平成１７年度　特許流通支援チャート

電気３１

不正アクセス侵入検知防御技術

２００６年3月

独立行政法人　工業所有権情報・研修館

不正アクセスの侵入は、ファイアウォールだけでは防御できない

■ 不正アクセス侵入検知防御技術とは

ネットワークから情報セキュリティを喪失させるものとしては、不正アクセスとウイルスがある。ウイルスが間接的に攻撃をするのに対して、不正アクセスの攻撃は、成済ましやセキュリティホールを利用して侵入し、コンピュータの内部で直接ファイル等を破壊する場合と、サービス妨害攻撃(DoS 攻撃)でコンピュータを外部から直接攻撃し、コンピュータのサービスを不能にしてしまう場合がある。DoS 攻撃は、ファイアウォールでは防御できない。不正アクセスに対処する技術は、侵入を検知、解析、予防する技術と、侵入を防御する技術とがある。また 1999 年８月６日に「不正アクセス行為の禁止等に関する法律」いわゆる「不正アクセス防止法」が成立し 2000 年２月 13 日より施行されている。

■ 侵入検知解析の技術が技術開発の中心

1993 年から 2003 年 12 月までに出願された不正アクセス侵入検知防御技術に関する特許出願は、2,221 件である。93 年の出願件数は 32 件、出願人は 21 人であったが、この 10 年で出願件数は約 13 倍に、出願人は約 10 倍に増加した。

この中では、侵入検知解析技術(609 件、27%)とパケットフィルタリング技術(520 件、23%)に関する出願件数は、現在も増加傾向が続いている。侵入の防御技術であるアプリケーション中継技術(561 件、25%)、ホスト認証技術(277 件、13%)、トンネリング技術(255 件、12%)は 2000 年から出願が減少している。

■ 技術開発の課題の中心は「侵入防御の性能向上」

不正アクセス侵入検知防御技術の技術開発の課題では、「侵入防御の性能向上」が 350 件と最も多く、次いで「利用サービスの保護強化」、「デバイスの正当性向上」や「通信データの中継性能向上」も多い。

侵入防御の性能向上の中では、攻撃元のアドレスを特定する「アドレスフィルタの強化」やフィルタルールの設定作業を簡易化したり、動的なフィルタの設定を容易化したりする「フィルタルール設定の効率化」に関するものが多い。

■ 「データ構造の改良」が主要な解決手段

「利用サービスの保護強化」という課題について、最も多く用いられている解決手段は、「データ構造の改良」の中の具体的な解決手段である「アクセステーブルの改良」である。

次いで、「中継するデータの機密性向上」という課題について、多く用いられている解決手段は、「データ形式の改良」である。

さらに「侵入防御の性能向上」という課題について、多く用いられている解決手段は、「データ構造の改良」の中の具体的解決手段である「フィルタテーブルの改良」である。

ファイアウォールは古くから用いられている技術であるが、「侵入防御の性能向上」の課題に対する「フィルタテーブルの改良」は、最近３年の出願が多い。これは、侵入検知システム(IDS)とファイアウォールの連携によるフィルタの機能強化であり、不正アクセスの侵入を迅速に検知して、その結果を動的にフィルタに設定して、ただちに不正アクセスの防御を行うものである。

■ 通信サービスやコンピュータメーカーが主要出願人

不正アクセス侵入検知防御技術に関する特許出願の多い企業としては、日本電信電話(NTT)等の通信サービス企業と、日立製作所、日本電気、東芝、富士通等のコンピュータメーカーである。

NTT と日立製作所の２社は、それぞれ 150 件以上の出願があり、日本電気、東芝と富士通は、それぞれ 100 件以上の出願がある。

大学・公的研究機関の出願は少なく、科学技術振興機構が４件、産業技術総合研究所、宇宙航空研究開発機構、東京大学が各２件となっている。

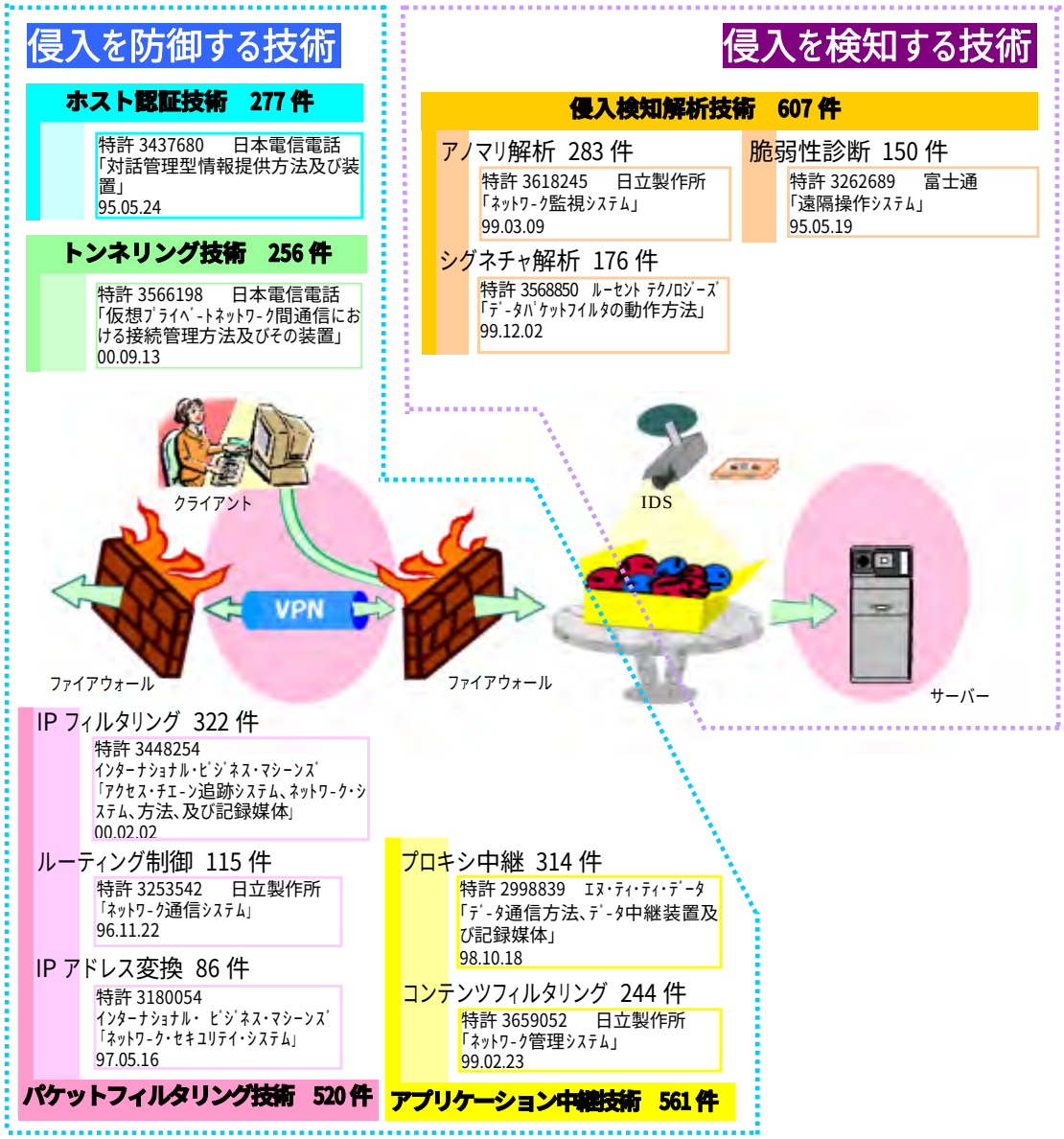
■ 開発拠点は

この分野の技術開発は、ソフト産業が発達している首都圏に多く、特に東京と神奈川に集中している。

不正アクセス侵入検知防御技術の特許分布と周辺技術

不正アクセス侵入検知防御技術に関して、1993 年 1 月以降、2003 年 12 月までの出願は 2,221 件である。不正アクセス侵入検知防御技術は、侵入を検知する技術と侵入を防御する技術に大別できる。侵入を検知する技術は、侵入検知解析技術が最も多く 607 件ある。これは、アノマリ解析技術(283 件)、シグネチャ解析技術(176 件)、及び脆弱性診断技術(150 件)から構成されている。一方、侵入を防御する技術は、パケットの通過の許諾を制御するアプリケーション中継技術(561 件)、パケットフィルタリング技術(520 件)、暗号技術を応用したホスト認証技術(277 件)及びトンネリング技術(256 件)から構成されている。

図 1.1.2 不正アクセス侵入検知防御技術の構成図

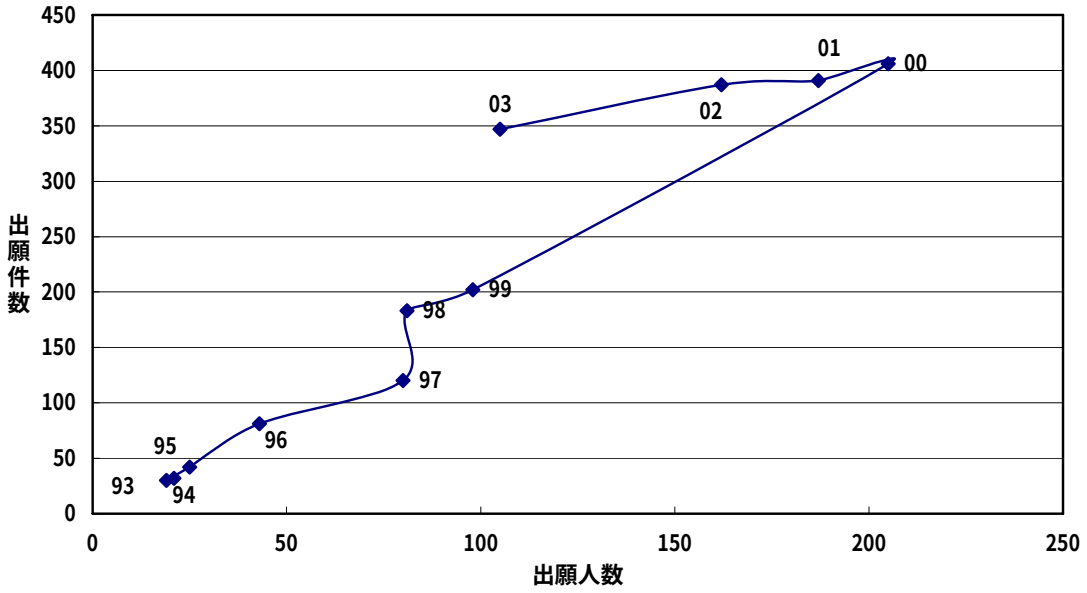


急増し続ける　侵入検知解析技術とパケットフィルタリング技術

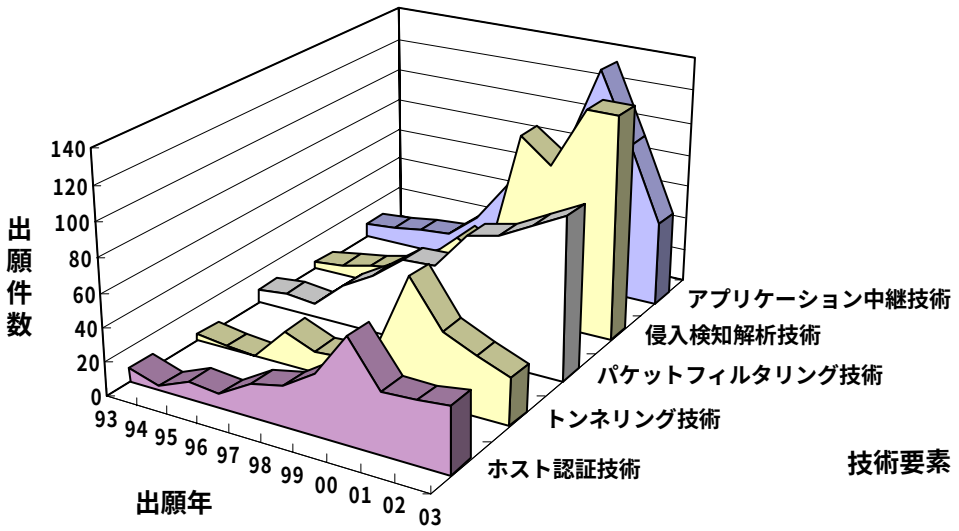
不正アクセス侵入検知防御技術の出願件数、出願人数は２０００年まで毎年大幅に増加し、その後は共に減少傾向を示している。

技術要素別にみると、侵入検知解析技術およびパケットフィルタリングの技術は依然として高い水準にあるのに対して、アプリケーション中継技術及びトンネリング技術が大幅に減少している。

不正アクセス侵入検知防御技術に関する出願人数－出願件数の推移



不正アクセス侵入検知防御技術に関する技術要素別の出願件数の推移



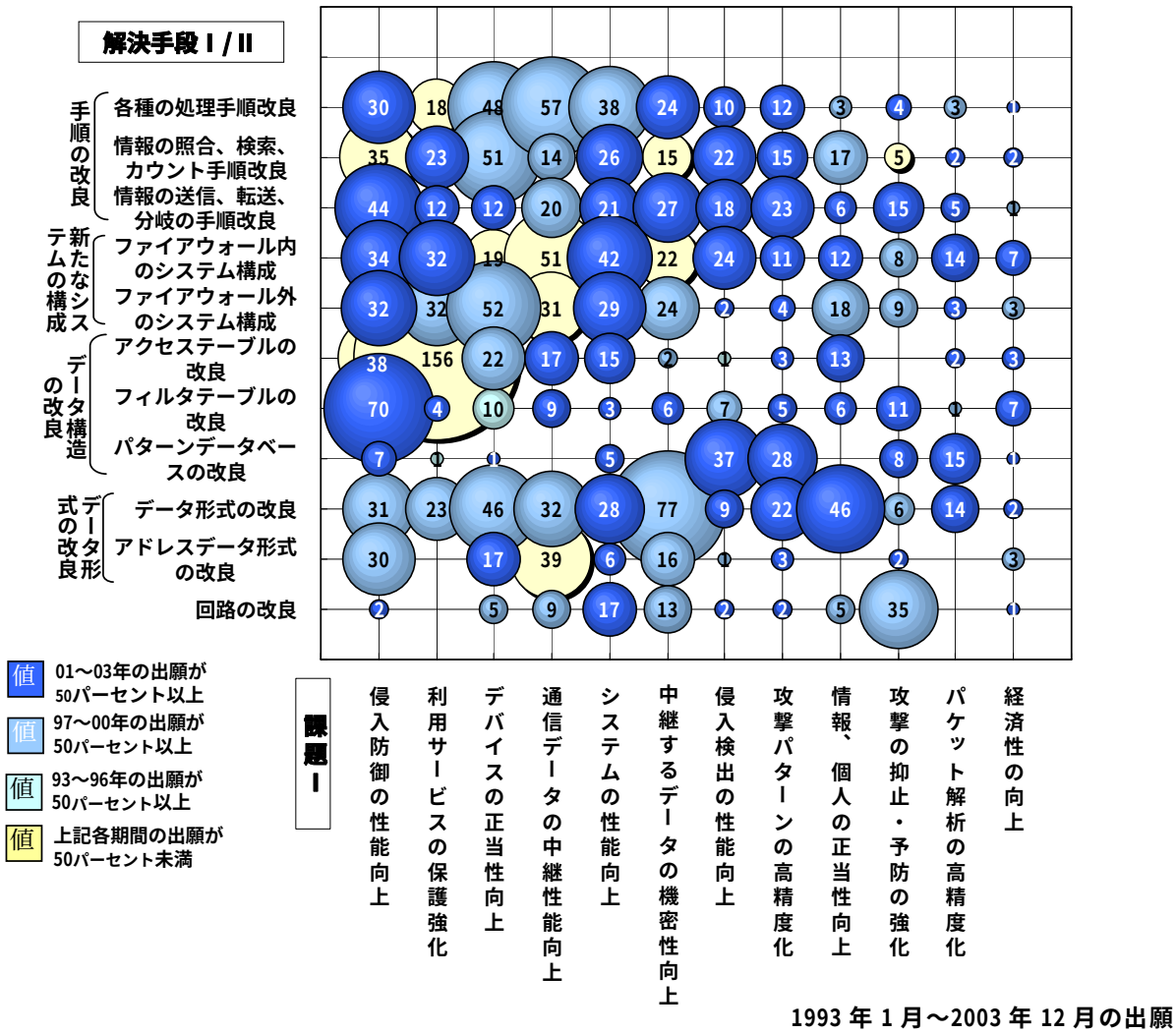
技術開発課題は「侵入防御の性能向上」

不正アクセス侵入検知防御技術の技術開発は、さまざまな課題に対して行われているが、最も出願の多い課題は「侵入防御の性能向上」である。この「侵入防御の性能向上」については、近年「フィルタテーブルの改良」、「情報の送信、転送、分岐の手順改良」及び「ファイアウォール内のシステム構成」を用いるものが多くなっている。

「利用サービスの保護強化」の課題については、「アクセステーブルの改良」によるものが最も多く、出願自体は安定している。

一方、「中継するデータの機密性向上」の課題については、「データ形式の改良」によるものが多いが、2001 年以降の出願は少なくなっている。

不正アクセス侵入検知防御技術の課題と解決手段の分布図



1993 年 1 月～2003 年 12 月の出願

広く分布している注目される特許

他の特許に引用されていたものは 2,205 件ある。このうち５回以上引用されていたものが 25 件ある。

最も引用回数の多かった特許は、日立製作所の「ネットワーク監視システム」(特許 3618245 号)で、侵入検出の性能向上を課題とするもので、ファイアウォール内のシステム構成で、おとりサーバーを構成配置するものである。

不正アクセス侵入検知防御技術に関する注目される特許の課題と解決手段および被引用回数（抜粋）

課題 I ＼ 解決手段 II	侵入防御の性能向上	通信データの中継性能向上	中継するデータの機密性向上	侵入検出の性能向上	攻撃の抑止・予防の強化
各種の処理手順の改良		特開平 11-234270 （日本電信電話） [7 回] 特開平 08-044643 （富士通） [5 回]			
情報の照合、検索、カウント手順の改良				特許 3483782 （ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ） [6 回]	特許 3549861 （日本電信電話） [8 回]
情報の送信、転送、分岐の手順の改良		特許 2998839 （ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ、ﾄﾞﾜﾝｺﾞ）（共願） [6 回]			特開平 09-269930 （日立製作所） [9 回]
ファイアウォールシステム内の構成		特開平 10-154110 (ﾀﾝﾌﾞﾙｳｨｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(米国)) [7 回] 特開 2000-354056 （東芝） [5 回]		特許 3618245 （日立製作所） [14 回] 特開 2002-007234 （三菱電機） [5 回]	
アクセステーブルの改良	特開平 09-026975 (ｴｲ･ﾃｨ･ｱﾝﾄﾞ･ﾃｨ(米国)) [5 回] 特開平 10-028144 （日立製作所） [5 回]			特開平 10-164064 （日立製作所） [7 回]	
フィルタテーブルの改良	特開 2001-273388 （日立製作所） [5 回]				
データ形式の改良	特許 3180054 （ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ（米国）） [6 回]	特開 2000-076218 （ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ） [6 回]	特開平 06-209313 （ﾌｼﾞｸﾗ） [5 回] 特許 3263877 （日本電信電話） [5 回]	特開 2002-063084 （東芝） [8 回]	
回路の改良					特許 3165366 （日立製作所） [7 回] 特開 2002-073433 （三菱電機） [5 回]
件数 回数	5 件 21 回	6 件 36 回	2 件 10 回	5 件 40 回	4 件 29 回

通信サービス企業やコンピュータメーカーが主要出願人

不正アクセス侵入検知防御技術の主要出願人は、日本電信電話（NTT）等の通信サービス企業、日立製作所、日本電気などのコンピュータメーカーである。

技術開発拠点は、東京や神奈川の首都圏が多い。また出願人構成比率を見ると、海外からの出願の割合が少なくなっていることがわかる。

図 3.1 不正アクセス侵入検知防御技術の主要企業の技術開発拠点

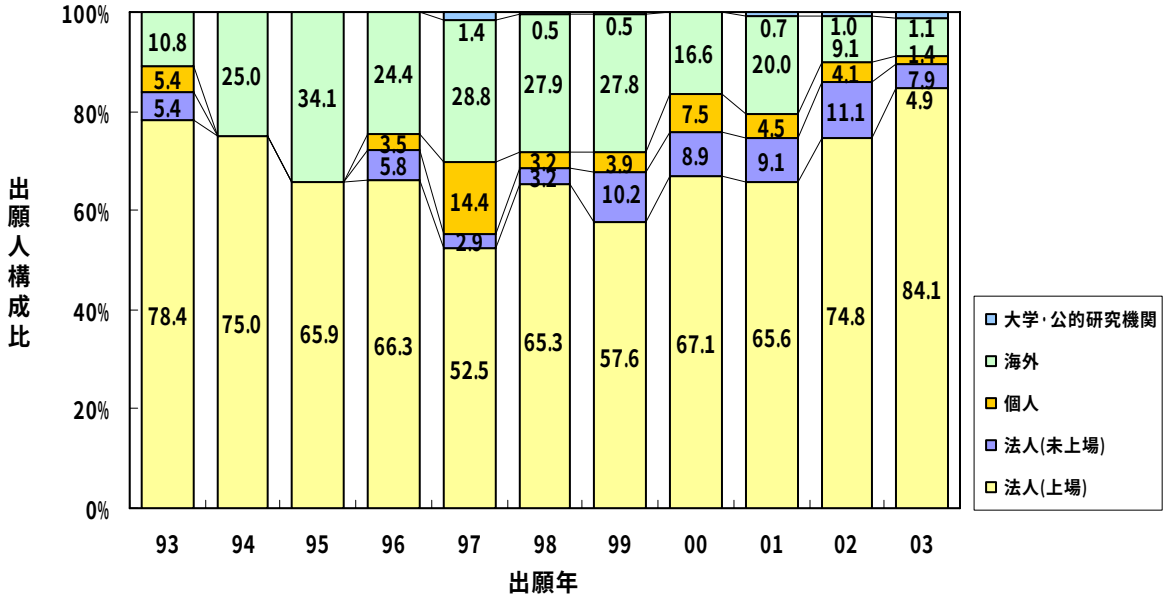
主要出願人

番号	出願人	出願件数
①	日本電信電話	197
②	日立製作所	152
③	日本電気	131
④	東芝	124
⑤	富士通	116

大学・公的研究機関出願人

番号	出願人	出願件数
⑥	科学技術振興機構	4
⑦	産業技術総合研究所	2
⑧	宇宙航空研究開発機構	2
⑨	東京大学	2

不正アクセス侵入検知防御技術に関する出願人構成比の推移



日本電信電話株式会社

出願状況

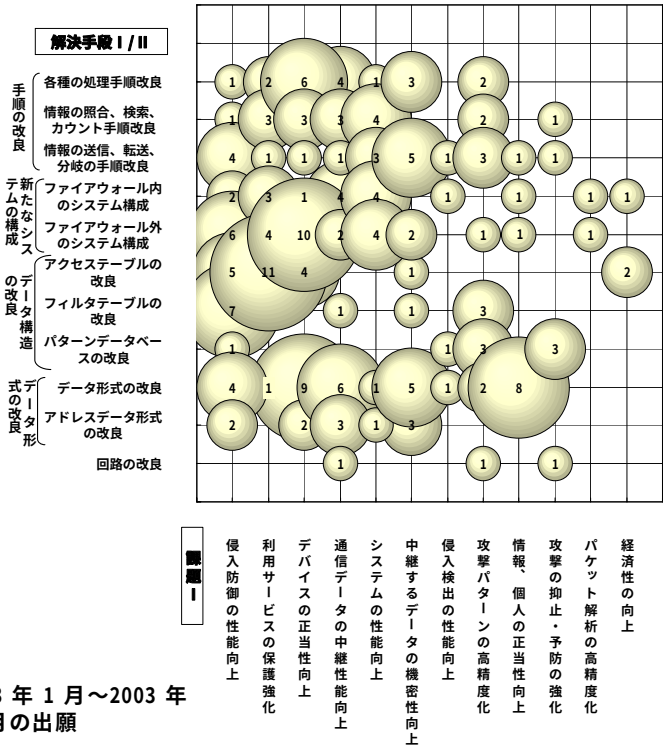
日本電信電話（NTT）の出願件数は 152 件であり、そのうち 06 年１月現在で、28 件が登録特許となっている。

デバイスの正当性向上の課題に関する出願が 36 件と多く、また侵入防御の性能向上の課題に関する出願も 33 件と多い。

利用サービスの保護強化の課題に対して、アクセステーブルの改良の解決手段で対応する出願が多くなっている。

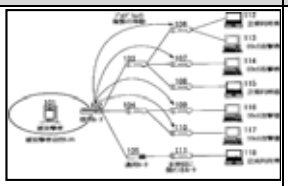
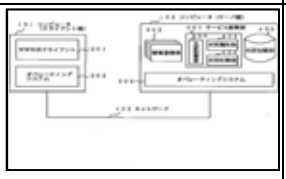
また、デバイスの正当性向上の課題に対して、ファイアウォール外のシステム構成で対応する出願や、またデータ形式の改良で対応する出願も多くなっている。

特許の課題と解決手段の分布



1993 年 1 月～2003 年 12 月の出願

保有特許例

特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要	課題Ⅰ	解決手段Ⅱ	技術要素Ⅲ
特許 3549861 01.09.10 H04L12/66 [被引用 8 回]	**分散型ｻｰﾋﾞｽ不能攻撃の防止方法および装置ならびにそのｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ**  通信装置を通過する通信ﾊﾟｹｯﾄを監視し分散型ｻｰﾋﾞｽ不能攻撃を検出するﾄﾗﾌｨｯｸ監視機能部と、攻撃元検索ﾓｼﾞｭｰﾙによって検索された攻撃元に近い上位側の通信装置の候補中から上位側の防御位置とする通信装置を抽出する攻撃元判断機能部とを備えﾓｼﾞｭｰﾙ送信部は、攻撃元判断機能部によって抽出された上位側の防御位置の通信装置に対して攻撃防御ﾓｼﾞｭｰﾙを送信するものであることを特徴とする通信装置。	攻撃の抑止・予防の強化	情報の照合、検索、カウント手順改良	アノマリ解析技術
特許 3437680 95.05.24 G06F15/00,330 [被引用 2 回]	**対話管理型情報提供方法及び装置**  ｸﾗｲｱﾝﾄ側からの情報取得要求受信時、初回の情報取得要求か、第 2 回目以降の情報取得要求かを判別し、情報をｸﾗｲｱﾝﾄ側へ送出し、ID の取得要求でない情報取得要求の場合、URL に対話 ID が付加されていれば、対話記憶部に対話 ID が記録されているかどうか検査し、記録されていればｱｸｾｽを記録し、送出すべき情報内の URL に対話 ID を付加し、情報をｸﾗｲｱﾝﾄ側へ送出し、URL に対話 ID が付加されていない場合、または、対話 ID が対話記憶部に記録されていない場合、ｱｸｾｽ拒否を行うことを特徴とする対話管理型情報提供方法。	データ形式の改良	デバイスの正当性向上	ホスト認証技術

株式会社　日立製作所

出願状況

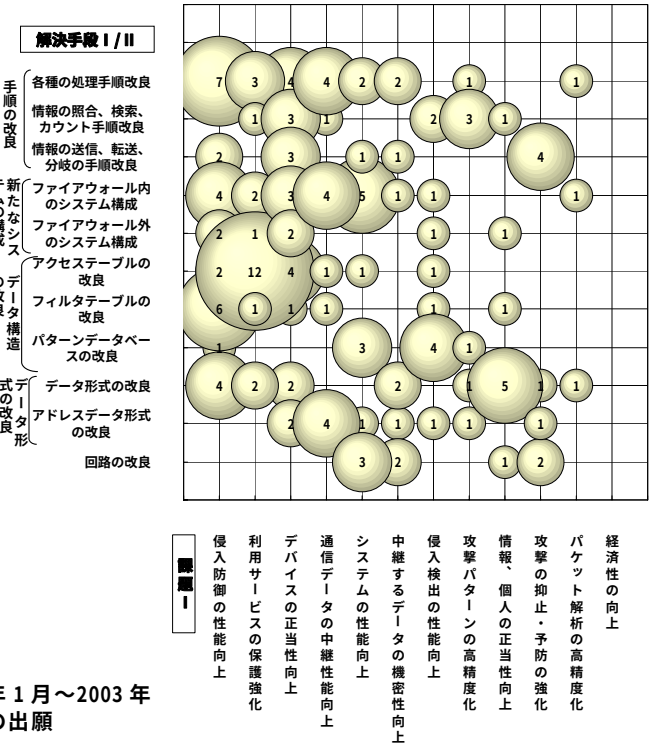
日立製作所の出願件数は152件あり、そのうち06年1月末現在で、15件が登録特許となっている。

侵入防御の性能向上の課題に関する出願が28件と多く、またデバイスの正当性向上の課題に関する出願も 24 件と多い。

利用サービスの保護強化の課題に対して、アクセステーブルの改良の解決手段で対応する出願が多くなっている。

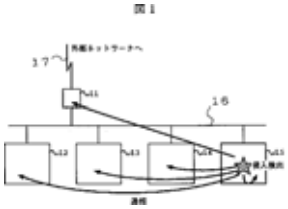
また、侵入防御の性能向上の課題に対して、各種の処理手順の改良で対応する出願も多くなっている。

特許の課題と解決手段の分布



1993年1月～2003年12月の出願

保有特許例

特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要	課題Ⅰ	解決手段Ⅱ	技術要素Ⅲ
特許 3618245 99.03.09 H04L12/46 [被引用 14 回]	**ネットワーク監視システム**  内部情報ネットワークを不正にアクセスするパケットを検出した時、ルータ装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と、受信パケットに応答して、パケットの送信元に、意図的な情報を含む応答パケットを送信する偽装サーバとを有し、ルータが、監視装置からの制御パケットの受信に応答して、不正パケットの識別情報を記憶するための手段を備え、外部ネットワークから受信されたパケットの中から識別情報に基づいて不正パケットを識別し、偽装サーバに転送することを特徴とするネットワーク監視システム。	侵入検出の性能向上	ファイアウォール内のシステム構成	アノマリ解析技術
特許 3165366 96.02.08 G06F13/00,351 [被引用 7 回]	**ネットワークセキュリティシステム**  計算機は、計算機の内部状態を監視し、異常の発生を検知する内部状態監視手段と、内部のリソースに対するアクセスの制御を行うアクセス制御手段とを備え、アクセス制御手段は、内部状態監視手段により異常の発生が検知されたとき、異常に関連した内部のリソースの保護処理を行うことを特徴とするネットワークセキュリティシステム。	攻撃の抑止・予防の強化	回路の改良	アノマリ解析技術

日本電気株式会社

出願状況

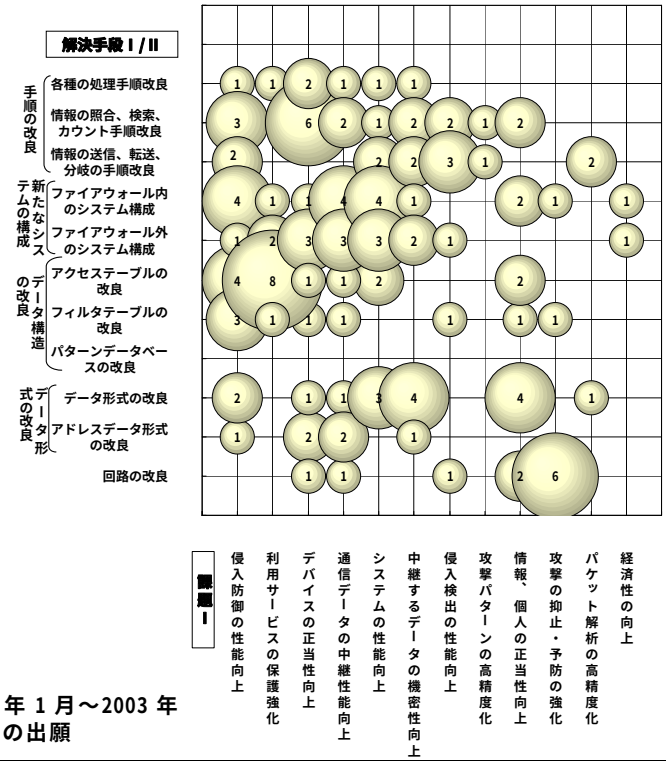
日本電気の出願件数は、131件であり、そのうち06年1月末現在で、33件が登録特許となっている。

侵入防御の性能向上の課題に関する出願が21件と多く、またデバイスの正当性向上の課題に関する出願も18件と多い。

利用サービスの保護強化の課題に対して、アクセステーブルの改良の解決手段で対応する出願が多くなっている。

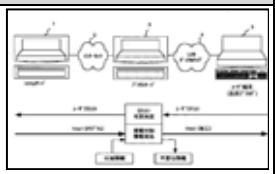
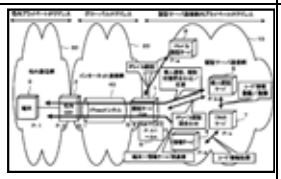
また、デバイスの正当性向上の課題に対して、情報の照合、検索、カウント手順改良で対応する出願や、攻撃の抑止・予防の強化対して、回路の改良で対応する出願も多くなっている。

特許の課題と解決手段の分布



1993年1月～2003年12月の出願

保有特許例

特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要	課題 I	解決手段 II	技術要素 III
特許 3250512 98.02.24 G06F13/00,540 [被引用 2 回]	**ﾌﾟﾛｷｼｻｰﾊﾞ**  ﾕｰｻﾞ端末に関する情報を一時的に保存するﾕｰｻﾞ端末情報格納部と、ﾕｰｻﾞのｱｸｾｽを禁止するｱｸｾｽ不可ﾘｽﾄを格納するｱｸｾｽ不可ﾘｽﾄ格納部と、ｻｰﾊﾞから送信された情報を受信する情報受信部と、ｱｸｾｽ不可ﾘｽﾄおよびﾕｰｻﾞ端末情報を参照して受信した情報を編集する情報編集部と、編集した情報をﾕｰｻﾞ端末に送信する情報送信部と、を備えていることを特徴とするﾌﾟﾛｷｼｻｰﾊﾞ。	侵入防御の性能向上	フィルタテーブルの改良	プロキシ中継技術
特許 3616570 01.01.04 H04L12/66	**ｲﾝﾀｰﾈｯﾄ中継接続方式**  ﾀﾞｲｱﾙｱｯﾌﾟによりIPに準拠するｱﾄﾞﾚｽが付与され、端末を含む宅内通信網とｸﾞﾛｰﾊﾞﾙｱﾄﾞﾚｽによりIPに基づく通信を行うｲﾝﾀｰﾈｯﾄ通信網との接続点に設けられた宅内ｹﾞｰﾄｳｪｲと、複数の認証ｻｰﾊﾞを含みIPに準拠するﾌﾟﾗｲﾍﾞｰﾄIPｱﾄﾞﾚｽにより制御される認証ｻｰﾊﾞ通信網とｲﾝﾀｰﾈｯﾄ通信網との接続点に設けられた認証ｻｰﾊﾞｹﾞｰﾄｳｪｲとを備えたｲﾝﾀｰﾈｯﾄ中継接続方式において、ｲﾝﾀｰﾈｯﾄ通信網の中に宅内ｹﾞｰﾄｳｪｲと認証ｻｰﾊﾞｹﾞｰﾄｳｪｲとの間に、IPsecﾄﾝﾈﾙを設定する手段を備えたことを特徴とするｲﾝﾀｰﾈｯﾄ中継接続方式。	デバイスの正当性向上	ファイアウォール外のシステム構成	ホスト認証技術

株式会社　東芝

出願状況

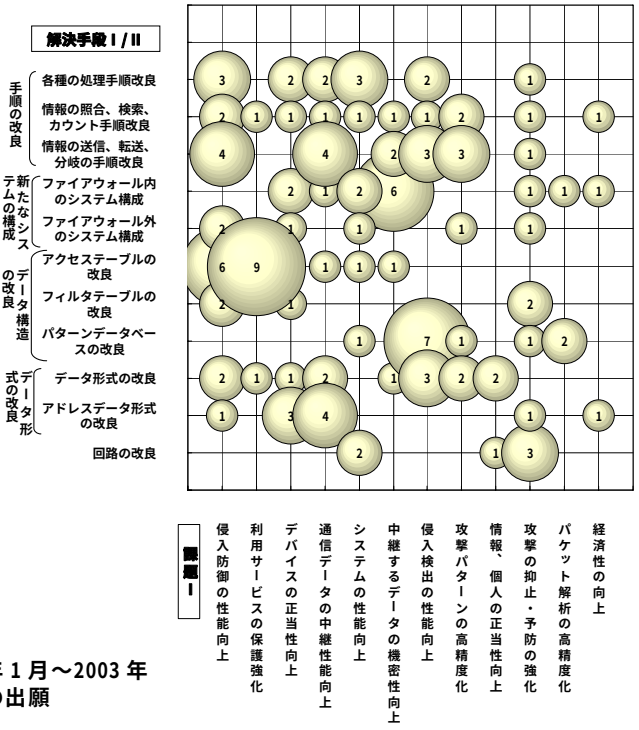
東芝の出願件数は、124 件であり、そのうち 06 年１月末現在で、17 件が登録特許となっている。

侵入防御の性能向上の課題に関する出願が 22 件と多く、また侵入検出の性能向上の課題に関する出願も 16 件と多い。

利用サービスの保護強化の課題に対して、アクセステーブルの改良の解決手段で対応する出願が多くなっている。

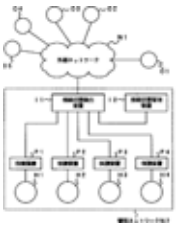
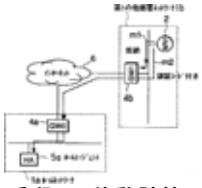
また、侵入検出の性能向上課題に対して、パターンデータベースの改良で対応する出願も多くなっている。

特許の課題と解決手段の分布



1993 年 1 月～2003 年 12 月の出願

保有特許例

特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要	課題Ⅰ	解決手段Ⅱ	技術要素Ⅲ
特許 3426832 96.01.26 G06F13/00,351 [被引用 2 回]	**ﾈｯﾄﾜｰｸｱｸｾｽ制御方法**  複数の計算機のいずれかを送信元または宛先とするすべてのﾊﾟｹｯﾄを監視可能な位置に設けられた接続状態検出手段により、ﾊﾟｹｯﾄの内容に基づいて、複数の計算機の他計算機との接続開始および接続終了を少なくとも検出し、複数の計算機対応に設けられた保護手段により、少なくとも検出された接続開始または接続終了の情報に基づいて、対応する計算機にﾊﾟｹｯﾄを受信させるか否かを決定することを特徴とするﾈｯﾄﾜｰｸｱｸｾｽ制御方法。	システムの性能向上	各種の処理手順改良	アノマリ解析技術
特許 3557056 96.10.25 H04L12/66	**ﾊﾟｹｯﾄ検査装置、移動計算機装置及びﾊﾟｹｯﾄ転送方法**  自装置の管理対象となる計算機以外の移動計算機から送信されたﾊﾟｹｯﾄに含まれる移動計算機識別情報に基づき、移動計算機から送信されたﾊﾟｹｯﾄのﾈｯﾄﾜｰｸ外への転送の可否を判定する判定手段と、この判定手段により転送を拒否すると判定した場合に、移動計算機に転送拒否を示すﾒｯｾｰｼﾞを返信する手段と、移動計算機から移動計算機識別情報を生成するための鍵情報を要求するﾒｯｾｰｼﾞを受信した場合に、移動計算機のﾕｰｻﾞに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する手段とを具備したことを特徴とするﾊﾟｹｯﾄ検査装置。	侵入防御の性能向上	データ形式の改良	コンテンツフィルタリング技術

富士通株式会社

出願状況

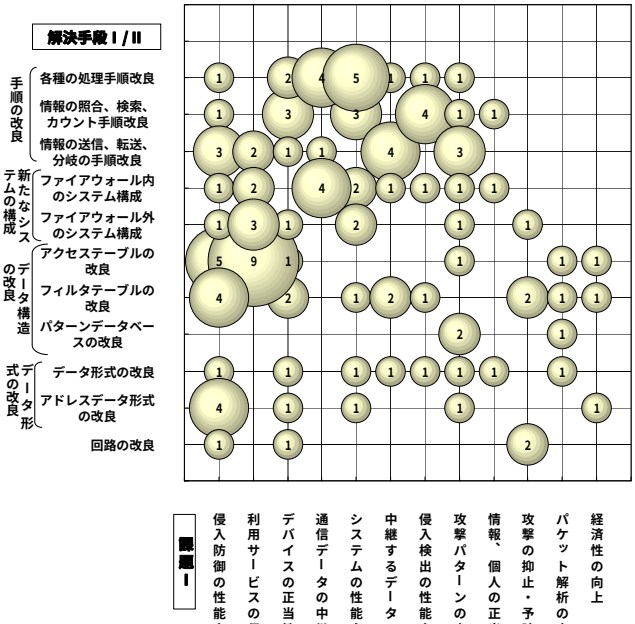
富士通の出願件数は、116件であり、そのうち06年1月末現在で、16件が登録特許となっている。

侵入防御の性能向上の課題に関する出願が22件と多く、また利用サービスの保護強化の課題に関する出願も16件と多い。

利用サービスの保護強化の課題に対して、アクセステーブルの改良の解決手段で対応する出願が多くなっている。

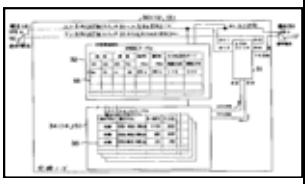
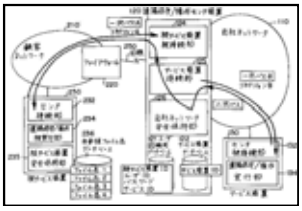
また、システムの性能向上の課題に対して、各種の処理手順の改良で対応する出願や、また侵入防御の性能向上対して、アクセステーブルの改良で対応する出願も多くなっている。

特許の課題と解決手段の分布



1993年1月～2003年12月の出願

保有特許例

特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要	課題Ⅰ	解決手段Ⅱ	技術要素Ⅲ
特許 3591753 97.01.30 H04L12/56 [被引用 4 回]	**ﾌｧｲｱｳｫｰﾙ方式およびその方法**  固定長ﾊﾟｹｯﾄを交換するとともに、受信した固定長ﾊﾟｹｯﾄのなかから第2のﾌﾟﾛﾄｺﾙによる第1の端末から第2の端末へのｱｸｾｽ要求を含んだ固定長ﾊﾟｹｯﾄを抽出する交換ﾉｰﾄﾞと、ﾈｯﾄﾜｰｸ内に設けられ、交換ﾉｰﾄﾞによって抽出された固定長ﾊﾟｹｯﾄに格納されている情報に基づいて第2の端末へのｱｸｾｽを許容するか否かを判断するｴｰｼﾞｪﾝﾄﾕﾆｯﾄと、を有するﾌｧｲｱｳｫｰﾙ方式。	システムの性能向上	各種の処理手順改良	脆弱性診断技術
特許 3262689 95.05.19 G06F13/00,351	**遠隔操作ｼｽﾃﾑ**  第一のﾌｧｲｱｳｫｰﾙが内部ﾈｯﾄﾜｰｸに接続されたｻｰﾋﾞｽ装置のアドレスを特定するための識別子を送信し、第二のﾌｧｲｱｳｫｰﾙ及び第一のﾌｧｲｱｳｫｰﾙを介して、ｻｰﾋﾞｽ装置との間にｺﾈｸｼｮﾝを確立し、ｺﾈｸｼｮﾝを介して該ｻｰﾋﾞｽ装置との間でﾊﾟｹｯﾄを送受信するﾊﾟｹｯﾄ通信手段と、ﾊﾟｹｯﾄ通信手段が受信したﾊﾟｹｯﾄから遠隔操作の指示情報を取り出し、指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、を備えたことを特徴とする被ｻｰﾋﾞｽ装置。	システムの性能向上	ファイアウォール内のシステム構成	脆弱性診断技術

Contents

目次

不正アクセス侵入検知防御技術

１．技術の概要

1.1 不正アクセス侵入検知防御技術 3
1.1.1 不正な侵入による攻撃 3
1.1.2 不正アクセス侵入検知防御技術 8
1.1.3 ファイアウォール 15
1.1.4 侵入検知システム(IDS) 18
1.1.5 ファイアウォールと IDS でトータルセキュリティ 20
1.1.6 特許からみた技術の進展 21
1.1.7 セキュリティソフトウエアの市場 28
1.2 不正アクセス侵入検知防御技術の特許情報へのアクセス ..32
1.3 技術開発活動の状況 37
1.3.1 不正アクセス侵入検知防御技術の技術開発活動 37
1.3.2 不正アクセス侵入検知防御技術の海外における技術開発活動 41
1.3.3 侵入検知解析技術 44
1.3.4 アプリケーション中継技術 47
1.3.5 パケットフィルタリング技術 49
1.3.6 ホスト認証技術 52
1.3.7 トンネリング技術 53
1.4 技術開発の課題と解決手段 54
1.4.1 不正アクセス侵入検知防御技術の技術要素と課題、および課題と解決手段 61
(1) 技術要素と課題 61
(2) 攻撃種別と課題 63
(3) 課題と解決手段 64
1.4.2 侵入検知解析技術の課題に対する解決手段 67
(1) アノマリ解析技術 68
(2) シグネチャ解析技術 74
(3) 脆弱性診断技術 79
1.4.3 アプリケーション中継技術の課題に対する解決手段 ..84
(1) プロキシ中継技術 85
(2) コンテンツフィルタリング技術 92

目　次

Contents

1.4.4 パケットフィルタリング技術の課題に対する解決手段 ..98
（1） IP フィルタリング技術 99
（2） ルーティング制御技術 105
（3） IP アドレス変換技術 110
1.4.5 ホスト認証技術の課題に対する解決手段 114
1.4.6 トンネリング技術の課題に対する解決手段 121
1.5 注目される特許 127
1.5.1 注目される特許の抽出 127
1.5.2 注目される特許の課題と解決手段 135
1.5.3 注目される特許の関連図 137

２．主要企業、大学・公的研究機関等の特許活動

2.1 日本電信電話(NTT) 142
2.1.1 企業の概要 142
2.1.2 製品例 142
2.1.3 技術開発拠点と研究者 143
2.1.4 技術開発課題対応特許の概要 143
2.2 日立製作所 170
2.2.1 企業の概要 170
2.2.2 製品例 170
2.2.3 技術開発拠点と研究者 171
2.2.4 技術開発課題対応特許の概要 171
2.3 日本電気 190
2.3.1 企業の概要 190
2.3.2 製品例 190
2.3.3 技術開発拠点と研究者 191
2.3.4 技術開発課題対応特許の概要 191
2.4 東芝 211
2.4.1 企業の概要 211
2.4.2 製品例 211
2.4.3 技術開発拠点と研究者 212
2.4.4 技術開発課題対応特許の概要 212
2.5 富士通 228
2.5.1 企業の概要 228
2.5.2 製品例 228
2.5.3 技術開発拠点と研究者 229
2.5.4 技術開発課題対応特許の概要 229

目　次

Contents

2.6 三菱電機 245
2.6.1 企業の概要 245
2.6.2 製品例 245
2.6.3 技術開発拠点と研究者 246
2.6.4 技術開発課題対応特許の概要 246
2.7 松下電器産業 258
2.7.1 企業の概要 258
2.7.2 製品例 258
2.7.3 技術開発拠点と研究者 259
2.7.4 技術開発課題対応特許の概要 259
2.8 ソニー 267
2.8.1 企業の概要 267
2.8.2 製品例 267
2.8.3 技術開発拠点と研究者 268
2.8.4 技術開発課題対応特許の概要 268
2.9 キヤノン 275
2.9.1 企業の概要 275
2.9.2 製品例 275
2.9.3 技術開発拠点と研究者 276
2.9.4 技術開発課題対応特許の概要 277
2.10 インターナショナル・ビジネス・マシーンズ(IBM).....284
2.10.1 企業の概要 284
2.10.2 製品例 284
2.10.3 技術開発拠点と研究者 285
2.10.4 技術開発課題対応特許の概要 285
2.11 富士ゼロックス 296
2.11.1 企業の概要 296
2.11.2 製品例 296
2.11.3 技術開発拠点と研究者 297
2.11.4 技術開発課題対応特許の概要 297
2.12 リコー 303
2.12.1 企業の概要 303
2.12.2 製品例 303
2.12.3 技術開発拠点と研究者 304
2.12.4 技術開発課題対応特許の概要 304

目　次

Contents

2.13 マイクロソフト 309
2.13.1 企業の概要 309
2.13.2 製品例 309
2.13.3 技術開発拠点と研究者 310
2.13.4 技術開発課題対応特許の概要 310
2.14 エヌ・ティ・ティ・データ(NTT データ) 315
2.14.1 企業の概要 315
2.14.2 製品例 315
2.14.3 技術開発拠点と研究者 316
2.14.4 技術開発課題対応特許の概要 316
2.15 沖電気工業 321
2.15.1 企業の概要 321
2.15.2 製品例 321
2.15.3 技術開発拠点と研究者 322
2.15.4 技術開発課題対応特許の概要 322
2.16 サン・マイクロシステムズ 327
2.16.1 企業の概要 327
2.16.2 製品例 327
2.16.3 技術開発拠点と研究者 328
2.16.4 技術開発課題対応特許の概要 328
2.17 横河電機 332
2.17.1 企業の概要 332
2.17.2 製品例 332
2.17.3 技術開発拠点と研究者 333
2.17.4 技術開発課題対応特許の概要 333
2.18 エヌ・ティ・ティ・ドコモ(NTT ドコモ) 337
2.18.1 企業の概要 337
2.18.2 製品例 337
2.18.3 技術開発拠点と研究者 338
2.18.4 技術開発課題対応特許の概要 338
2.19 セイコーエプソン 342
2.19.1 企業の概要 342
2.19.2 製品例 342
2.19.3 技術開発拠点と研究者 343
2.19.4 技術開発課題対応特許の概要 343

目　次

Contents

2.20 ヒューレット・パッカード 347
2.20.1 企業の概要 347
2.20.2 製品例 347
2.20.3 技術開発拠点と研究者 348
2.20.4 技術開発課題対応特許の概要 348
2.21 ルーセント テクノロジーズ 352
2.21.1 企業の概要 352
2.21.2 製品例 352
2.21.3 技術開発拠点と研究者 353
2.21.4 技術開発課題対応特許の概要 353
2.22 大学・公的研究機関 358
2.23 主要企業以外の特許番号一覧 361

３．主要企業の技術開発拠点

3.1 不正アクセス侵入検知防御技術の技術開発拠点 373

資 料

1．ライセンス提供の用意のある特許 379

本チャートに関する留意事項

1．一部の出願人の名称について略記を用いている場合がある。

2．特許リスト等における出願人については、作成時点での最新情報を反映させている。

3．本チャート掲載の製品名等は、各企業等が所有する商標または登録商標である。

4．掲載されている特許についてライセンスできるかどうかは各企業、大学・公的研究機関等の状況により異なる。

１．技術の概要

1.1 不正アクセス侵入検知防御技術
1.2 不正アクセス侵入検知防御技術の特許情報へのアクセス
1.3 技術開発活動の状況
1.4 技術開発の課題と解決手段
1.5 注目される特許

特許流通
支援チャート

1．技術の概要

不正アクセス侵入検知防御技術は、情報セキュリティ保護の中心的な技術であり、不正アクセスの侵入を検知する技術と、不正アクセスの侵入を防御する技術から構成されている。

1.1 不正アクセス侵入検知防御技術

1.1.1 不正な侵入による攻撃

(1) 情報セキュリティとは

情報セキュリティは、守秘性(Confidentiality)、完全性(Integrity)、可用性(Availability)の頭文字を取ったCIAとして知られ、CIAはISO/IEC 15408の情報セキュリティ評価基準で定められている。

(情報セキュリティ評価基準；http://www.ipa.go.jp/security/jisec/evalbs.html)

●守秘性(Confidentiality)

権限のない（認可されていない）ユーザーが情報にアクセスできないことを確保する。

●完全性(Integrity)

データとそれを格納する情報システムが正確で完全であることを確保する。

●可用性(Availability)

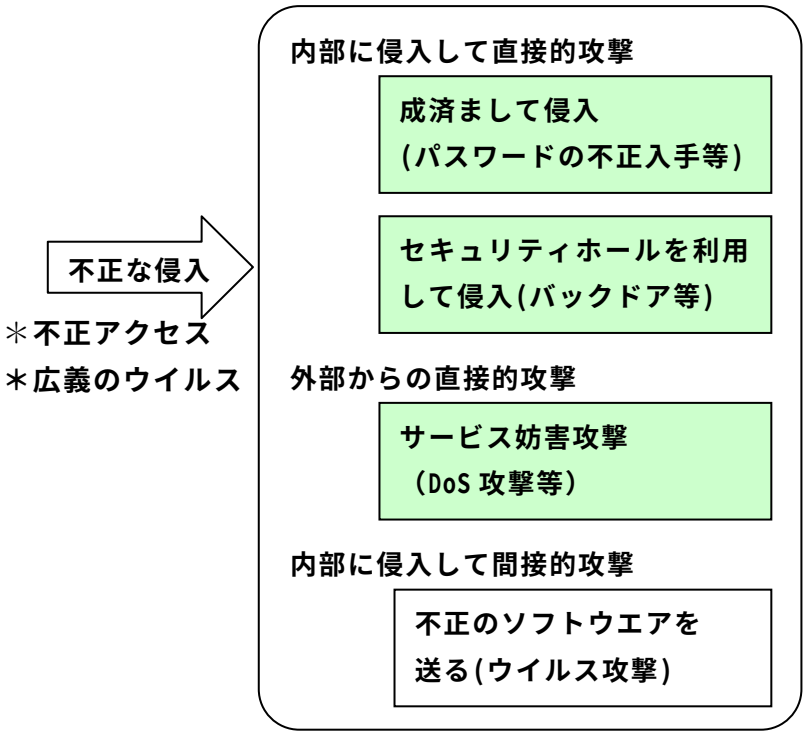
必要なときに適時にアクセス可能であり、利用可能であることを確保する。

(IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

(2) 不正アクセスとは

情報セキュリティを喪失させるコンピュータへの不正な侵入は、不正アクセスによる攻撃と広義のウイルスによる攻撃がある。図1.1.1に不正な侵入によるコンピュータへの攻撃方法を示す。

図1.1.1 不正な侵入によるコンピュータへの攻撃方法



不正アクセスによる攻撃は、コンピュータへの直接的な攻撃である。直接的な攻撃とは、悪意の第三者が自分のコンピュータを操作することで、ネットワークを経由してターゲットとなるコンピュータの内部に侵入し、ファイルなどを直接攻撃することをいう。

不正アクセスにより、内部に侵入して直接的攻撃を加える方法には、パスワードやIDなどを不正入手して、他人に成済まして侵入する方法、セキュリティホールを使用して内部に侵入する方法、メールサーバープログラムのセキュリティホールを利用して、暗号化パスワードファイルを自分宛に送り込む方法がある。別のセキュリティホールを利用して侵入する方法には、バックドア(裏口)の設置による侵入方法もある。管理者が、不正アクセスに気づき、正面の門である通信路を塞いでもバックドアから侵入が出来てしまう。バックドアからの侵入は全ての機能を使用可能とするので、攻撃の踏み台としても利用されてしまう。この不正アクセスが確認された場合は、バックドアを完全に消去するディスクのフォーマットを行い、OSを再インストールする必要がある。

不正アクセスによる外部からの直接的攻撃には、サービス妨害攻撃(DoS攻撃)がある。大量のデータをターゲットに送り込むため、一般ユーザーのサービスは使用できなくなる。

一方、広義のウイルスによる攻撃は、コンピュータへの間接的な攻撃である。間接的な攻撃とは、悪意の第三者が、メールの添付ファイルに不正なソフトウェアを付けてコンピュータに送り込み、受信者が添付ファイルを開くことによって、不正なソフトウェアを働かせ、ファイルなどを間接的に破壊する攻撃をいう。

●不正アクセス

システムを利用する者が、その者に与えられた権限によって許可された行為以外の行為をネットワークを介して意図的に行うこと。

●広義のウイルス

「コンピュータウイルス対策基準」においては、広義の定義を採用しており、自己伝染機能・潜伏機能・発病機能のいずれかをもつ加害プログラムをウイルスとしている。自己伝染機能については、他のファイルやシステムに寄生・感染するか、単体で存在するかを問わない定義になっているので「Worm(ワーム)」も含むことになる。他のファイルやシステムへの寄生・感染機能を持たないがユーザーが意図しない発病機能をもつ「Trojan Horse（トロイの木馬)」や、勝手にインストールされ害がもたらされる「スパイウエア」も、この広義の定義ではウイルスに含まれる。

●セキュリティホール

情報セキュリティ分野における「脆弱性」は、俗に「セキュリティホール」と呼ばれている。

●バックドア

本来、禁じられているアクセス（侵入）を可能とするための仕掛け。一度、侵入されたサイトに再侵入しやすくするために仕掛けられることがある。

●サービス妨害攻撃（DoS攻撃,DoS Attack,Denial of Service Attack）

コンピュータ資源やネットワーク資源が、本来のサービスを提供できない状態に陥れる攻撃。例えば、インターネットサーバーによって提供されている各種サービスを標的として妨害する攻撃が、一般に入手可能なツールを利用して行われている。このようなDoS攻撃には、次の種類がある。

・インターネットプロトコルの特性を悪用して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供することをできなくする攻撃 ：SYN flood attack(SYNフラッド攻撃)。

・ネットワークの帯域を渋滞させる攻撃：Smuff attack(Smuff攻撃)。

・サーバーアプリケーションの脆弱性を攻略し、サービスに例外処理をさせてサービスを提供することをできなくする攻撃。

(IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

(3) 情報セキュリティの保護技術の発展に寄与した重要な出来事や事件

インターネットがまだ普及していない1980年代始に早くも不正アクセスであるバックドアによる攻撃が行われていた。88年に、米国の大学院生であるロバート・モリス(Robert Morris)は、インターネットに接続していた6000台のコンピュータに(モリス)ワームをまき散らし、始めてインターネットを大規模に停止させた。このワームは、バッファオーバフロー攻撃など現在のワームやウイルスの基本的なコンセプトをすでに持っていた。これらの侵入を防御する技術として、インターネットとイントラネットの間に配置され、外部からのアクセスを遮断し、内部から外部へのアクセスを通過させる装置であるファイアウォールが開発された。

世界で最初の商用ファイアウォールは、米国ディジタル・イクイップメント社（現在のコンパック・コンピュータ社）の「SEAL」であるといわれており、1990年に発売された。SEALは、３台のコンピュータにファイアウォールの機能を分割して、セキュリティシステムを構築した。SEALの３機能は現在のファイアウォールの基本機能をなすものである。

SEALのゲートシステム(Gate System)は現在のパケットのフィルタリング技術である。またゲートキーパーシステム(Gatekeeper System)は現在のアプリケーションの中継技術である。さらにメールゲートシステム(Mailgate System)は現在の侵入検知解析の技術である。当時インターネット接続している企業は少なく、高いセキュリティを希望する限られた企業のみが導入した。

またモリスワームのような事例が繰返されることの懸念から、SEALの発売と同じ90年に、コンピュータユーザーにネットワークセキュリティ問題について警告するための機関CERT(Computer Emergency Response Team)が設立された。

1992年にWWW技術が開発され、インターネットは爆発的に普及していく中、99年にメール侵入型の不正アクセスが登場した。今までの侵入は、フロッピーディスクのような記録媒体経由の侵入であったが、このメールによる侵入は、ネットワークを介しての侵入になった。侵入速度が大幅に上がり、大規模な侵入がまたたく間に簡単に行われるようになった。不正アクセスは様変わりし、一部の情報管理者だけの問題でなく、社会問題化していった。

2000年代の今日の情報セキュリティは、ファイアウォールを設置しておけば大丈夫と必ずしも言えなくなった。

ひとつは、DoS 攻撃である。この攻撃は、ヤフー(Yahoo)社やイーベイ(eBay)社などの米国企業のサイトに仕掛けられ、一般ユーザーは接続不能になった。DoS攻撃とは、侵入し易いネットワークサーバーを探し、そこに侵入のバックドアとなるソフトをインストールして、そこを踏み台として、攻撃しようとするターゲットサイトに、例えば異常なパケットを送信して、機能停止に追い込んでしまうものである。このパケットは、踏み台から送信されているためファイアウォールを通過してしまう。

２つめは、01年に多く出回ったワームである。メール型でなくウェブ感染型のコードレッド(Code Red)ウイルスは、もはやファイアウォールでは、ウイルスによる不正侵入が防げないとわかったのも01年であった。ウイルスの不正侵入による攻撃に対して、予防や駆除の機能を持つワクチンプログラムの重要性が増し、ウイルスワクチンソフト技術が開発されていった。ウイルスワクチンソフト技術の基本機能は次の４つであると言われている。

＊ ウイルス検査機能：既知ウイルスの検出
＊ ファイルの変更チェック機能：未知ウイルスの検出
＊ 修復機能：発見したウイルスの駆除
＊ レポート機能：発見したウイルスの詳細調査

ほとんどのウイルスワクチンソフト技術は、これらの機能を持っているが、新種のウイルスが次々現れるので最新のバージョンにしておくことが重要である。万が一のウイルス被害に備えるために頻繁にバックアップを行うことも重要であり、プログラムには自動ダウンロード機能を備えるものもある。

02年には、ウィンドウズ(Windows)やウェブモジュールのセキュリティホールを利用し

た不正アクセスの攻撃で、サイトの改ざんなどの被害が深刻になってきた。これらの被害を防ぐために、侵入検知システムの技術が見直されている。この技術は、パケットの挙動を解析し、データベースにある攻撃パターンと比較照合したり、アルゴリズムで攻撃パケットと特定したりする技術である。またこの技術は、当初オフラインで解析し、攻撃元アドレスを特定していたので、新たな攻撃元アドレスをファイアウォールに設定するのにタイムラグが生じていた。最近では、ファイアウォールと不正侵入検知システムが連携して、不正侵入検知システムが攻撃を検知し、ただちにファイアウォールに解析結果が送られ、新たな攻撃を防御することが可能になってきている。

我が国においても、1988年末に不正侵入としてウイルスの被害が初めて報道され、その後対策や法整備が急ピッチで進められた。不正侵入の報告として、90年４月、当時の通産省から「コンピュータウイルス対策基準」が告示され、被害の届出の受付機関として当時の情報処理振興事業協会(IPA)が指定された。96年８月に「コンピュータ不正アクセス対策基準」が告示され、04年７月に、「ソフトウェア等脆弱性関連情報取り扱い基準」が告示された。不正アクセスの法整備として、99年８月に「不正アクセス行為の禁止等に関する法律(通称；不正アクセス防止法)」が成立し、2000年２月より施行された。対策基準、不正アクセス防止法、および届出情報などの関連資料は独立行政法人 情報処理推進機構(IPA)のセキュリティセンターのホームページで見ることができる。

(http://www.ipa.go.jp/security/)。

また、不正侵入の攻撃と対策は、米国のCERTと連携している、日本のJPCERTのホームページ(http://www.jpcert.or.jp/)にも詳しく記載されている。

●ワーム

自己複製し、自己増殖するコンピュータプログラム。広義のウイルスには含まれる。ワームは、狭義のウイルスとは異なり、単体でネットワーク環境において増殖するもの。いわゆるモリスワームを契機とする。

●ファイアウォール

特定のネットワークセグメントを他のネットワークとの接続部分において防護する考え方であり、外部のインターネットから内部のイントラネットを防護するのが典型的である。インターネットファイアウォールの場合、通常インターネットサーバーも運用されるので、単純な外部と内部をコントロールする関係にはならない。外部インターネットと内部イントラネットの間にDMZ(非武装地帯)と呼ばれる境界ネットワークを構築することがある。

●ウイルスワクチンソフト（ウイルス対策ソフト、アンチウイルスソフト）

ウイルスを検出・削除し、ウイルスに感染するのを未然に防ぐためのソフトウェアである。ウイルス対策ソフトやアンチウイルスソフトと同義語。ウイルスワクチンソフトウェア会社から市販されている。パソコンにプレインストールされているものもありが、その場合は3ヶ月等の有効期限があるため、継続して使用するには更新手続きをする必要がある。

(IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

1.1.2 不正アクセス侵入検知防御技術

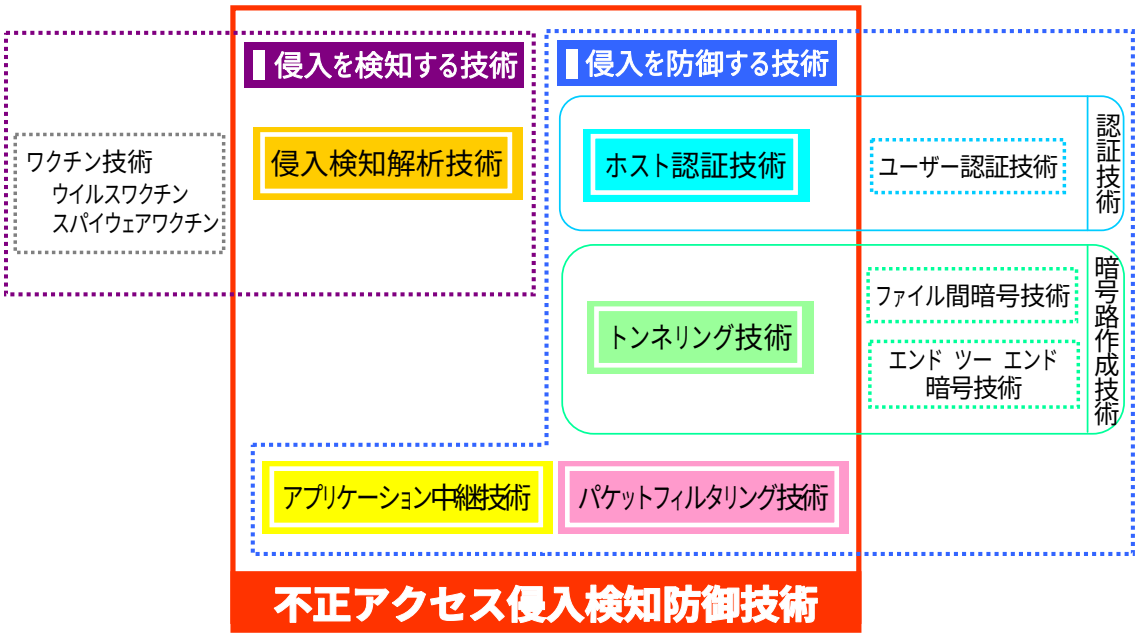
不正アクセス侵入検知防御技術は、インターネットからの不正アクセスによる侵入に対して、内部ネットワークの入り口でアクセスを検知して、正常な訪問者か、不正な侵入者かを解析して、その結果により、門を開け閉めして防御する技術である。

(1) 不正アクセス侵入検知防御技術の範囲

図1.1.2-1に、不正アクセス侵入検知防御技術の範囲を示す。太線で囲まれた部分が不正アクセス侵入検知防御技術の範囲である。不正アクセス侵入検知防御技術は、二つの技術に大別でき、不正アクセスの侵入を検知、解析、予防することで侵入を検知する技術と、不正アクセスによる攻撃被害の侵入を防御する技術である。

侵入を検知する技術は、侵入検知解析技術とワクチン技術がある。侵入検知解析技術は、ネットワーク上のパケットを監視して、ログを採取し、それを解析して、不正アクセスを検知する技術である。ワクチン技術は、広義のウイルスの侵入に対して、ウイルスを検知し、検知したウイルスを駆除する技術である。不正アクセス侵入検知防御技術は、不正アクセスを検知する侵入検知解析技術を解析対象範囲とする。

図 1.1.2-1 不正アクセス侵入検知防御技術の範囲



侵入を防御する技術は、パケットフィルタリング技術、アプリケーション中継技術、ホスト認証技術及びトンネリング技術がある。

パケットフィルタリング技術とアプリケーション中継技術は、ネットワーク上でこのアクセスは通過させる、このアクセスは破棄するとアクセス制御(Access Control)をする技術である。ネットワーク層の下位層であるIP層でアクセス制御をする技術をパケットフィ

ルタリング技術といい、上位層であるアプリケーション層でのアクセス制御をする技術をアプリケーション中継技術という。不正アクセス侵入検知防御技術は、この２つの直接侵入を防御する技術を解析対象範囲とする。

また、侵入を防御する技術には、パケットなどの情報のアクセスをする前に、侵入を防御することが可能な認証技術(Authentication)がある。認証とは、クライアントを使用しているユーザーが本当に本人か、ネットワークに接続されているクライアントやサーバーが本物かを確認することである。認証技術には、ユーザーとクライアント間のユーザー認証技術と、クライアントとネットワークを経由したサーバー間のホスト認証技術がある。不正アクセス侵入検知防御技術は、ネットワークをうまく利用したホスト認証技術を解析対象範囲とする。

さらに、侵入を防御する技術には、パケットなどの情報が不正に漏洩した後も、情報の内容を守秘可能にする暗号路作成技術がある。暗号路作成技術は、ネットワークのどの部位で情報を暗号化するかにより、３つに分けられる。それらは、ファイル間暗号技術、エンドツーエンド(コンピュータ間)暗号技術、トンネリング(通信機器間暗号)技術である。不正アクセス侵入検知防御技術は、IPアドレスを暗号化して包みこんでしまうトンネリング技術を解析対象範囲とする。

- アクセス制御（access control）

  コンピュータセキュリティにおいて、ユーザーがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすることをいい、典型的にはオペレーティングシステムにおいてACL（Access Control List：アクセスコントロールリスト）として実装される。MAC（Mandatory Access Control）方式、DAC（Discretionary Access Control）方式がある。また、インターネットセキュリティにおいて、送信元／宛先のIPアドレスとポートに対するパケットの通過の可否をコントロールするリストもACL（Access Control List：アクセスコントロールリスト）と呼ばれる。また、分散オブジェクト上にもACLは実装されている。何らかのコンピュータ／ネットワーク資源へのアクセスをコントロールすることを表現する広範な内容を表現するようになってきている。

- 認証(Authentication)

  認証もしくは本人認証は、ユーザーが本人であることを証明する過程をいう。認証のプロセスは、典型的には、本人であることの証拠として、 ユーザーの知識として自らの名前とパスワードやパスフレーズの入力を要求する。近年、ユーザーの持ち物（例： スマートカード）や、ユーザーの身体的特徴（バイオメトリクス）に基づく認証機構も普及しつつある。

  (IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

(2) 不正アクセス侵入検知防御技術を構成する技術要素

表1.1.2に不正アクセス侵入検知防御技術を構成する技術要素を示す。不正アクセス侵入検知防御技術は、「侵入を検知する技術」と「侵入を防御する技術」の２技術要素から構成されている。

侵入を検知する技術は、不正アクセスの侵入を検知、解析する「侵入検知解析技術」で構成されている。侵入を防御する技術は、「アプリケーション中継技術」、「パケットフィルタリング技術」、「ホスト認証技術」と「トンネリング技術」の５技術要素から構成されている。

侵入検知解析技術は、「アノマリ解析技術」、「シグネチャ解析技術」と「脆弱性診断技術」の３技術要素から構成されている。アプリケーション中継技術は、「プロキシ中継技術」と「コンテンツフィルタリング技術」の２技術要素から構成されている。パケットフィルタリング技術は、「IP フィルタリング技術」、「ルーティング制御技術」と「IP アドレス変換技術」の３技術要素から構成されている。

表 1.1.2 不正アクセス侵入検知防御技術を構成する技術要素

	技術要素 I	技術要素 II	技術要素 III
不正アクセス侵入検知防御技術	侵入を検知する技術	侵入検知解析技術	アノマリ解析技術
			シグネチャ解析技術
			脆弱性診断技術
	侵入を防御する技術	アプリケーション中継技術	プロキシ中継技術
			コンテンツフィルタリング技術
		パケットフィルタリング技術	IPフィルタリング技術
			ルーティング制御技術
			IPアドレス変換技術
		ホスト認証技術	
		トンネリング技術	

- アノマリ解析(anomaly detection)

  情報セキュリティ侵害検出方式のひとつで、通常ではない変則・異常なイベント、統計的に稀なイベントを検出する方法。「セキュリティ侵害行為を意味するイベントは、通常ではないイベントに含まれるはずである」という仮定に基づいている。

- シグネチャ解析(signature detection)

  情報セキュリティ侵害検出方法のひとつ。既知の侵害パターンに基づく情報とマッチングすることにより、該当侵害／ミスユース（悪用）の存在を検出する方法。この場合の signature（シグネチャ）は、既知の侵害パターンに基づく情報のことであり、署名のことではない。misuse detection（ミスユース検出法）ともいう。

  (IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

図1.1.2-2に不正アクセス侵入検知防御技術の構成図を示す。不正アクセス侵入検知防御技術を構成する技術要素が示されている。以下に、各技術要素を説明する。

図1.1.2-2 不正アクセス侵入検知防御技術の構成図

a 侵入検知解析技術

侵入検知解析技術は、アノマリ解析技術、シグネチャ解析技術と脆弱性診断技術から構成されている。

侵入検知解析技術は、不正アクセスの侵入を検知、解析する技術である。この技術は、コンビニェンスストアなどで使用している防犯カメラと同じ働きをしており、ネットワークを流れるパケットを監視し、ログを採取し、解析し、不正アクセスと特定する技術である。またこの技術は、監視カメラをネットワークのどの部分に配置するかにより、監視する情報の内容が違い、解析する技術も違ってくる。

・ **アノマリ解析技術**

アノマリ解析技術は、保護したいホストのアクティビティ（例えばログイン、ログアウトの時間、稼動していたアプリケーションなど）を監視するもので、ホストの前後に配置して、一定期間システムを運用し、ログ情報を採取し、統計的に解析して異常事態(アノマリ)を検知する技術である。

・ **シグネチャ解析技術**

シグネチャ解析技術は、過去に攻撃パケットと認識されたパケットの挙動をパターン化(シグネチャ)し、データベースに登録し、現在ネットワーク上を流れているパケットと比較照合して攻撃パケットを検知する技術である。

・ **脆弱性診断技術**

脆弱性診断技術は、最初にポートスキャンなどを行い、空いているポートから擬似的な不正アクセスによる攻撃を試みるものであり、システムの脆弱部分の試験、診断を行う技術である。可用性や冗長性を向上させる保守技術も含む。

●ポートスキャン

攻撃・侵入の前段階に行われる標的サイトの各ポートにおけるサービスの状態の調査。

(IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

b アプリケーション中継技術

アプリケーション中継技術は、プロキシ(Proxy;代理)中継技術とコンテンツフィルタリング技術から構成されている。

ネットワーク上を流れるパケットは、階層構造をしている。このアプリケーション中継技術は、パケットの上位階層であるアプリケーション層で、パケットの中味であるペイロードを確認して、パケットの通過・破棄のアクセス制御をする技術である。

・ **プロキシ中継技術**

プロキシ中継技術は、プロキシサーバーを配置して、クライアントからの要求を、プロキシサーバーが受けて外部に要求を出し、その応答をサーバーが受けてクライアントに返す技術である。この技術は、代理で処理を行うため、外部からは代理しか見えず、内部のネットワークを隠すことができ、機密性を高める技術である。またこの技術は、アプリケーション層でアプリケーションプロトコルごとのプロキシサーバーを配置して中継をする技術が主体であるが、トランスポート層でアプリケーションに依存せずに、プロキシサーバーを用いて中継するソックス(Socks)技術も含まれる。

・ **コンテンツフィルタリング技術**

コンテンツフィルタリング技術は、アプリケーション層で中継されたパケットの中身を

確認し、細かくアクセス制御をする技術である。この技術は、アクセスする物、アクセスする人を行列で設定（アクセスする主体をサブジェクト、アクセスする客体をオブジェクトとして行列を作成）し、さらにその行列にアクセス権を設定（アクセス権は例えば、見ることも書くことも出来ない、見ることは出来るが書くことはできない、見ることも書くことも出来るなどである）できる。この技術は、ユーザーの利用権限の制限、コンテンツの利用の制限を可能にするものである。

c パケットフィルタリング技術

パケットフィルタリング技術は、IP フィルタリング技術、ルーティング制御技術と IP アドレス変換技術から構成されている。

パケットフィルタリング技術は、パケットの下位階層である IP 層(ネットワーク層とトランスポート層)で、パケットヘッダのアドレスを確認して、パケットの通過・破棄のアクセス制御をする技術である。通過の許可、拒否を判断するための情報はフィルタに設定されており、フィルタとパケットのヘッダの情報を比較してアクセス制御を行う。フィルタ情報は、送信先アドレス、送信元アドレス、送信方向、プロトコル情報である。パケットフィルタリング技術は、簡単なアドレス処理によるアクセス制御を行っているので、処理時間が短い。しかしこの技術を大規模なネットワークで使用する場合、多数のパケットを処理するので、高速なアクセス制御が要求される。

• IPフィルタリング技術

IP フィルタリング技術は、インターネットの TCP/IP 層（OSI のネットワーク層とトランスポート層）で行われるパケットのフィリタリング技術である。IP 層のヘッダと TCP 層のヘッダを取り出し、フィルタにかけて、アクセス制御を行う。フィルタ情報は、送信先の IP アドレス、送信先のポート番号、送信元の IP アドレス、送信元のポート番号、プロトコル情報である。

• ルーティング制御技術

ルーティング制御技術は、IP 層において、IP アドレスの順番や組合せを規定することで、経路の絞込みをして、アクセス制御する技術である。データ転送を行う通信機器は、相手の通信機器の経路情報を知らせてもらい通信を行うが、外部と直接通信を行う機器は、内部の経路を一切教えないで経路の絞込みを行い、内部ネットワークの機密性を高めるための技術である。

• IPアドレス変換技術

IP アドレス変換技術は、グローバル IP アドレスをプライベート IP アドレスに変換する技術である。アドレス変換は、外部から内部または内部から外部へ直接のアドレスでパケットの通過をできなくして、内部ネットワークの機密性を高めることができる。IP アドレスにポート番号まで含めたアドレス変換技術も含まれる。

d ホスト認証技術

ホスト認証技術は、ネットワークをうまく利用した技術が取り入れられている。この技術は、他人や他の組織が認証した結果を信頼(Trust)して利用するものである。具体的にこの技術は、公的、私的な認証局が発行した証明書を見せてもらって相手を検証したり、システム全体で一箇所に配置した認証サーバーで相手を検証し登録し、その結果を使用する技術である。これらの認証技術は証明書を一度認証すれば、次回から証明書を見せるだけで認証の処理を省略できる特徴を持っている。パスワードを用いた認証技術は簡単なので多数使用されているが、ネットワークを経由している認証では固定したパスワードは、盗聴されやすく、またその情報を記録して後に成済まして使用されるリプレイ攻撃を受け易い。リプレイ攻撃を回避するには、パスワードは毎回異なるパスワード(ワンタイムパスワード)にしてかつ暗号化する必要がある。ワンタイムパスワードは、パスワードにタイムスタンプを付加したり、ハッシュ関数を付加したりして暗号化する方式がある。

●ハッシュ関数

メッセージ・ダイジェスト(MD)を生成するハッシュ関数は、元の平文に１ビットの変化があると、平均してメッセージ・ダイジェスト中の半分のビットが変化するような特殊な関数。また、メッセージ・ダイジェストから元の平文を生成することはできない。

(IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

eトンネリング技術

トンネリング技術は、IP パケットを別の IP パケットで包み込む技術をいう。この技術は、機密漏洩の目的でパケットを暗号化するが、宛先も分らなくしてしまう。またこの技術は、ファイアウォール間で、仮想の通信路を設定し、その両端の IP アドレスを付けて暗号化されたパケットを送信する技術である。トンネリング技術は、インターネット上で使用すると、あたかも専用線のように使用できる機能なので VPN(Virtual Private Network:仮想私設網)とも呼ばれている。ネットワーク層で設定する VPN とトランスポート層で設定する VPN がある。IPsec(Secure Architecture for IP)が代表的な方法である。トンネリング技術は、通信路上の全データを暗号化できるが、通信機器とコンピュータ間の暗号化はできない。

●VPN（Virtual Private Network：バーチャルプライベートネットワーク:仮想私設網）

インターネットのような公衆ネットワークをまたぐ複数のプライベートネットワークを、仮想的に統一されたプライベートなネットワークとして構築する技術。プライベートネットワーク間は、IPsec プロトコルのような暗号・認証機能をもつプロトコルで接続される。

(IPAの用語集；http://www.ipa.go.jp/security/glossary/glossary.html)

1.1.3 ファイアウォール

ファイアウォールは、不正アクセス侵入検知防御技術を適用した最もポピュラーな製品である。情報セキュリティを保護するセキュリティ機器やシステムは多数あるが、その中で最も利用されているのはファイアウォールである。大規模から小規模の内部ネットワークを保護するために、ファイアウォールの導入は今や必須になっている。ファイアウォールは、外部ネットワークと内部ネットワークを分離して、外部から内部へのアクセスを、内部ネットワークの入り口で食い止める機能をいい、この名前は延焼を食い止める「防火壁」に因んでいる。

ファイアウォールは、目的に応じてさまざまな不正アクセス侵入検知防御技術を適用した製品である。ルータなどの簡易通信機器に内蔵されたファイアウォールは、パケットフィルタリング技術の IP アドレス変換技術を適用している。大規模なネットワークのサーバーに内蔵されるファイアウォールは、高速処理を要求されるパケットフィルタリング技術をハードウェア回路で適用し、かつトンネリング技術も適用している。個々のサーバーのセキュリティを保護するため、例えば情報提供サーバーに内蔵されたファイアウォールは、緻密なコンテンツのアクセス制御を可能にするコンテンツフィルタリング技術を適用している。最近では個人によるインターネットへの常時接続が普及したため、単体のマシンを保護するプライベート用ファイアウォールは、侵入検知解析技術とパケットフィルタ技術を連携させて、新たな攻撃を解析し、検知し、ただちにパケットフィルタに設定し、攻撃を防御する統合形ファイアウォールである。

(1) ファイアウォールの機能要件

情報セキュリティの保護という観点で、屋台骨として内部ネットワークを支えているファイアウォールは、一般的に次の機能要件を持っことが必要であるといわれている。

- ＊ アクセス制御：外部ネットワークと内部ネットワークの間で転送されるデータ、又は利用ユーザーさらにはコンピュータなどのアクセス対象資源の制限を実施する機能を必要とする。
- ＊ 認証：利用を試みるホストが、確かに正当なアクセスが認められているホストであるかを検証する。この場合ホストの認証にIPアドレスを用いると効率の良い認証が可能になるがIPスプーフィング(Spoofing)などの不正技術を用いると簡単に成済ましが可能になってしまう。ホスト認証には、アドレス情報だけに頼るべきでなく、トランスポート層以上で行う認証機能と併用する必要がある。
- ＊ 暗号化：パスワードや転送データの暗号化を実施する。なおインターネットにおいてファイアウォール間の転送データを暗号化して安全に通信するためにあたかも専用線のように使用するVPNの機能を必要とする。
- ＊ 監視・監査：ネットワーク上のトラフィック量、ホストや通信機器の使用状況やアクセスログなどを採取し監視する。またアクセス制御が正当に実施されているか稼動状況を定期的に監査する機能を必要とする。

(2) ファイアウォールのアクセス制御

ファイアウォールのアクセス制御は、パケットフィルタリング技術とアプリケーション中継技術で行われる。

パケットフィルタリング技術によるアクセス制御は、送信元や送信先の IP アドレスやポート番号などによってパケットを通過させるかどうかを判断する。この技術は、ネットワーク層で動作させるのでチェックするデータが少なく高速な処理ができるが、ルールの定義が複雑になる。

アプリケーション中継技術によるアクセス制御は、通信を中継するプロキシプログラムを使用し社内ネットワークとインターネットを切離すことで行う。例えば、内部のクライアントが、WWW ブラウザで外部のウェブサーバーにアクセスする場合、ファイアウォールは、自動的に HTTP(Hyper Text Transfer Protocol の略；ウェブサーバーとクライアント間のデータの送受信するプロトコル)プロキシプログラムを起動し、このプログラムは WWW ブラウザであるかのようにして HTTP で外部のウェブサーバーをアクセスする。さらに、このプログラムはウェブサーバーからの返答を受取ると、要求元のクライアントに結果を返す。これにより社内のマシンは外部と直接接続することなく、セキュリティ的には安全にウェブサービスを利用できることになる。

ファイル転送のためには、FTP(File Transfer Protocol の略)のプロトコルを解釈できる FTP プロキシプログラムが必要になる。従ってパケットフィルタリング技術ではできなかった、次のようなアクセス制御が可能になる。

内部から外部 HTTP サーバーに対する「GET コマンド」は許可
内部から外部 FTP サーバーに対する「PUT コマンド」は拒否

「　」カッコで囲んだ部分がアプリケーション中継技術によるアクセス制御である。

アプリケーション中継技術には、プロキシ中継技術のようにアプリケーションごとにプロキシプログラムを準備したが、より汎用的に中継を行う仕組みが考えられている。そのひとつは、プロトコルに依存せずにトランスポート層でアプリケーションを中継するソックス(Socks)技術である。ソックス技術は、日本電気が開発した技術で、ただ単に中継を行うだけでなく、認証の機能も持っている。クライアントにソックスクライアント、ファイアウォールにソックスサーバーを持ち、ソックスクライアントはアプリケーションからのデータを横取りしてソックスサーバーにデータを送信する。ソックス技術は、外部の特定のアプリケーションを持つサーバーとデータのやり取りを行うため認証機能を持ち、パスワードやケロベロス認証機能を持っている。またこのソックス技術とパケットデータの暗号化技術により VPN 技術を構成することが可能になる。

(3) ファイアウォールのアドレス変換技術

ルータはアドレス変換技術で不正アクセスに対する防御を行う。インターネットに直接接続してない機器はプライベートな IP アドレスを使用できる。プライベートな IP アドレスを持つ機器とインターネットに接続されたグローバル IP アドレスを持つ機器の間ではルーティングが出来ない。ルータはこの機能を使用して内部機器を防御している。グローバル IP アドレスをプライベートな IP アドレスに変換する技術を NAT(Network Address

Translation)技術という。通常、内部接続しているホストが、同時にインターネットに接続する場合、台数分のグローバル IP アドレスが必要になってくる。通常グローバルアドレスを台数分確保することは出来ないので、ひとつのグローバル IP アドレスに、そのポート番号も含めてアドレス変換を行う NAT の拡張(IP Masquerade)機能がある。さらに規制を強めて、特定の IP アドレスで特定のポートにしか変換しない Port Forwarding 機能もある。これらアドレス変換の技術はインターネットにつながったルータに実装されており、身近なルータである ISDN 用のダイヤルアップルータは NAT 機能を持っている。

(4) ファイアウォールの弱点

ファイアウォールをどんな攻撃でも防ぐことができる魔法の壁のように思い、「うちはファイアウォールを導入したから大丈夫」というユーザーがいる。確かにファイアウォールは不正アクセスに対して強力な防御装置であるが、ファイアウォールの持つ機能に弱点があるということも知るべきである。ファイアウォールは、「通過を拒否された通信は完全に防御できるが、通過を許可された通信は防ぐことができない」という当たり前のことをしている。具体的には、インターネット向けに公開しなければならないサービスは、そのサービスへの通信を許可するようにファイアウォールは設定する。従ってそのサービスにセキュリティホールが存在した場合、通常のサービスを利用するためのアクセスとセキュリティホールを利用した攻撃による不正アクセスをファイアウォールは判別できない。

セキュリティホールの基本的な対策は、情報収集とそれに基づくパッチ(プログラム不具合の修正のため、ごく一部を書き換えること)とバージョンアップである。利用しているサービスに関するセキュリティ情報を日常的に収集し、問題があれば即座にパッチを適用し、バージョンアップするなどの対策を行うことが大切である。

(5) ファイアウォールの今後の機能

今やネットワークセキュリティの番人として位置が定着したファイアウォールであるが、今後必要とされる機能は、次のように考えられる。

- ＊ ファイアウォールの高速化：企業の業務システム(エンタプライズともいう)ではまだ必要性は少ないが、サービスプロバイダのバックボーンシステムでは、ギガビットのスループットが要求されている。ハードウェアによる、処理専用の集積回路の開発や、処理を並行に行うシステムの開発がなされると思われる。
- ＊ ファイアウォールの高可用性：電子商取引の運用に伴い 24 時間 365 日の継続したサービスの提供が必要である。バックアップシステムを始めとした保守性、信頼性の充実したシステムの開発がなされると思われる。

1.1.4 侵入検知システム(IDS)

侵入検知システム(IDS；Intrusion Detection System)は、門の前後に配置する監視カメラと同じ働きをする。監視カメラは通過する人間を常に記録しておき、後で必要になった時確認するが、IDSもネットワークを流れるパケットを監視し履歴を採取する監視技術が基本であり、この技術は昔からあった。IDSが行う処理は、情報を収集し、情報を解析し、さらにアクションとしての対応を行う技術である。IDSは、セキュリティ対策としてのファイアウォールやアンチウイルスソフトと比較すると認知度は低かった。

IDSは、情報の解析の仕方で２つ技術を適用している。シグネチャ解析技術は、過去に認識された攻撃パターン(シグネチャ)をデータベース化し、現在監視しているパケットを捕獲して、シグネチャと比較照合して、攻撃パケットであるかどうかを検知する技術である。アノマリ解析技術は、IDSを一定期間運用してシステムのプロファイルを作成する。プロファイルはユーザーのログイン、ログオフの時間、利用したアプリケーション名、トラフィック量などが含まれる。この通常プロファイルと異なるアクティビティがあれば異常事態(アノマリ)として検知する技術である。

IDSは、正しい検知か誤検知かが常に付きまとう。誤検知には、「正当なパケットを不正なパケットとする」場合と、「不正なパケットを正当なパケットとする」場合がある。誤検知が多いと、ログが満杯で捨てられたり、解析に時間がかかったりする。さらに正当なパケットを不正なパケットとした誤検知が多いと、警告を無視するようになる。そのため、不正なパケットの侵入を検知した本当の警告を見逃してしまう。正確なパターンの作成や、検知の閾値(しきいち：現象を起こすために越さなければならない最小値)を含めた検知ルール設定が重要になる。IDSは、試行錯誤しながら、いかに安定した運用まで持っていくかがセキュリティ管理者の腕の見せどころであるといわれている。

IDSのデバイスは、ファイアウォールの近くに配置し、ファイアウォールを補完するネットワーク型侵入検知システム(N-IDS)と、サーバーなどのホストの近くに配置するホスト型侵入検知システム(H-IDS)がある。

(1) ネットワーク型侵入検知システム(N-IDS)

N-IDSの特徴は、ファイアウォールでパケットが拒否されていて、どんな理由で拒否されているかを知ることができる。攻撃を検知したらファイアウォールにすぐフィードバックして防御できる。１台で全体を監視できるので、導入に容易であるなどの特徴を持つ。

N-IDSの情報収集は、ステルスモード(IPアドレスを定義せず、全パケットを透過させる)で設置する。これは外部の攻撃者からN-IDSの存在を隠しながら、ネットワーク上のパケットを捕獲するためである。N-IDSの存在が分れば、攻撃対象になってしまう。

N-IDSの情報の解析は、シグネチャ技術による解析をする製品が多い。ネットワークを流れる多量のパケットを処理するには、マッチング処理が最も効率がよいからである。セキュリティ・ベンダが作成したシグネチャが用意されている。処理の高速化のためシグネチャをカテゴリ別に分けた製品や、ユーザが作成したシグネチャが登録できる製品もある。通常時のパケットをプロファイリングして、このプロファイルを使用して、トラフィック状態の変化に基づき異常状態を検知する製品もある。

(2) ホスト型侵入検知システム(H-IDS)

H-IDSの特徴は、重要なホストを監視する。例えば、非武装地帯(DMZ:DeMilitalized Zone)であるDMZ上の公開用サーバーで、コンテンツの改ざんやメンテナンス用のログインアカウントの監視をする。またH-IDS はエンドポイント(IPアドレスとポート番号の組合せ)で監視するので、スイッチング環境、VPN環境で利用可能である。H-IDSは、保護すべきホストの近くに配置しているので、内部の悪意ある者が不正に情報を外部に送信したなどの異常状態の解析が可能である。外部からの不正アクセスより内部での不正アクセスが７割もあるといわれ、また個人情報保護法の施行により、このような特徴を持ったIDSが見直されている。

H-IDSの情報収集は、自分自身が作成するログ情報はもちろん、ホスト自身が作成するログ情報、コマンド履歴、レジストリ情報などを分析対象にすることができる。H-IDSの情報の解析は、アノマリ技術により統計的解析する製品が多い。一定期間をプロファイリング期間として、システムのアクティビティをプロファイルとして作成する。プロファイルの情報は、曜日、時間帯、利用アプリケーション名などである。ユーザーの取得したプロファイルが、極端に逸脱した振舞いを示した場合、異常事態としてアラートを発する。この手法を使用することにより、新種または未知の攻撃が検知できる。H-IDSのアクションは、ファイルやレジストリデータの復元機能であり、ウェブの改ざん対策として有効である。ただし保護したいファイルを指定して、オリジナルファイルを安全な領域に退避させておく必要がある。ファイルの更新中はこの機能を停止するので無防備な状態になるので注意が必要である。H-IDSは、防御したいアプリケーションに依存したOSごとにIDSソフトウェアを必要とする。またアプリケーションが同じでも利用形態が変わるとプロファイルも変化するので、利用形態に合わせたプロファイルを作成しないと誤検出が多量に出るので注意する必要がある。

H-IDSでは、セキュリティホールがあるように見せかけた脆弱なシステムを配置して、攻撃者の攻撃手法や手順のデータを取得する目的の、おとりサーバの技術を持つ製品がある。攻撃者は、スキャンポートで最もセキュリティの弱い部分を標的として攻撃してくる。これらのアクティビティを全て記録し、解析を行う。実際のシステムまで侵入を許すタイプと許可しないタイプがある。おとりサーバーでは、他のサイトの攻撃をするための踏み台になっていないか監視する必要があり、パスワードやアカウントも実際使用しているものは、使用しないことが肝要である。

(3) 今後の侵入検知システム

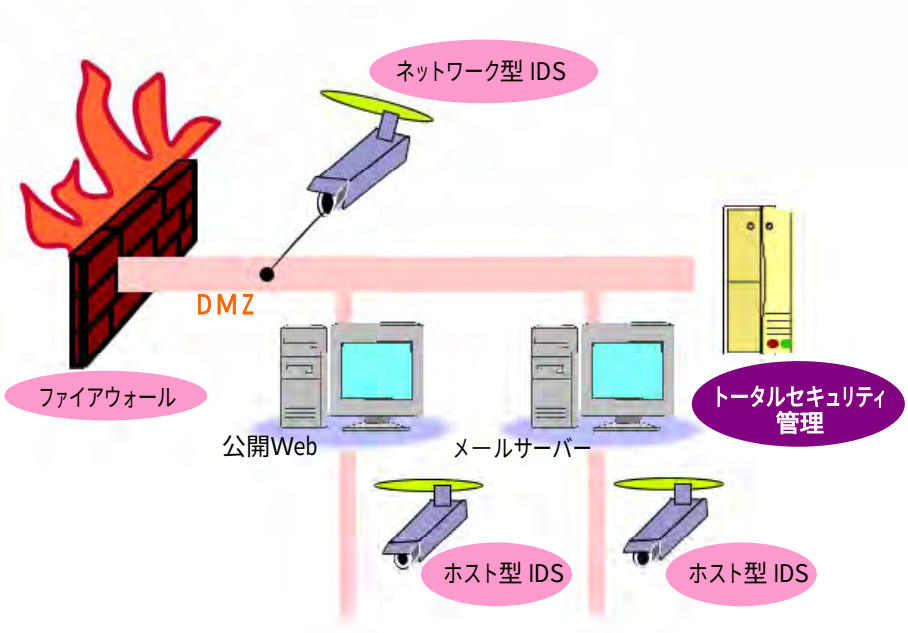
毎日のように報じられるウェブの改ざんに対応できるソリューションはIDSしか今のところは無い。従って今後より一層の期待が増してくるものと思われる。IDSは24時間365日の連続した監視が必要である。メンテナンスの停止中に攻撃されては意味がない。N-IDSには、タスクを分散して冗長性を増した製品も開発されつつある。これはまた分散することにより高速なネットワークやトラフィックの処理に対応可能にもなってくると思われる。またインターネットの常時接続の環境が整備され個人のコンピュータの情報流出や踏み台が多くなるので、個人向けIDSの製品が充実してくると思われる。特にファイアウォールとIDSが一緒になった統合型がパーソナルユースの主流になると思われる。

1.1.5 ファイアウォールとIDSでトータルセキュリティ

ファイアウォール、IDS にはメリットやデメリットがあるので、それを組み合わせて、理想的な構成が考えられる。特に DMZ 上でのサーバー群を監視するケースでは、ファイアウォールによるプロトコルの絞込みを前提し、ネットワークに対する無差別な攻撃をネットワーク型 IDS が監視し、ネットワーク型 IDS を回避するような攻撃に対しては、ホスト型 IDS がターゲットサーバ上で監視する構成をとれば理想的である。複数のセキュリティデバイスを併用することによりネットワーク全体を防御するトータルセキュリティの実現が重要である。

図 1.1.5 にネットワーク全体を防御するトータルセキュリティを示す。トータルセキュリティとは、ただ単にファイアウォールや IDS を配置したものではない。ファイアウォールや IDS で最も重要なことは、ソフトウェアで検出されたイベントに対するアクションである。つまり IDS で攻撃を検知した場合、それに対するアクションは、システム固有の情報伝達経路やセキュリティポリシによってかわってくる。

図 1.1.5 ネットワーク全体を防御するトータルセキュリティ



1.1.6 特許からみた技術の進展

(1) 侵入検知解析技術

a アノマリ解析技術

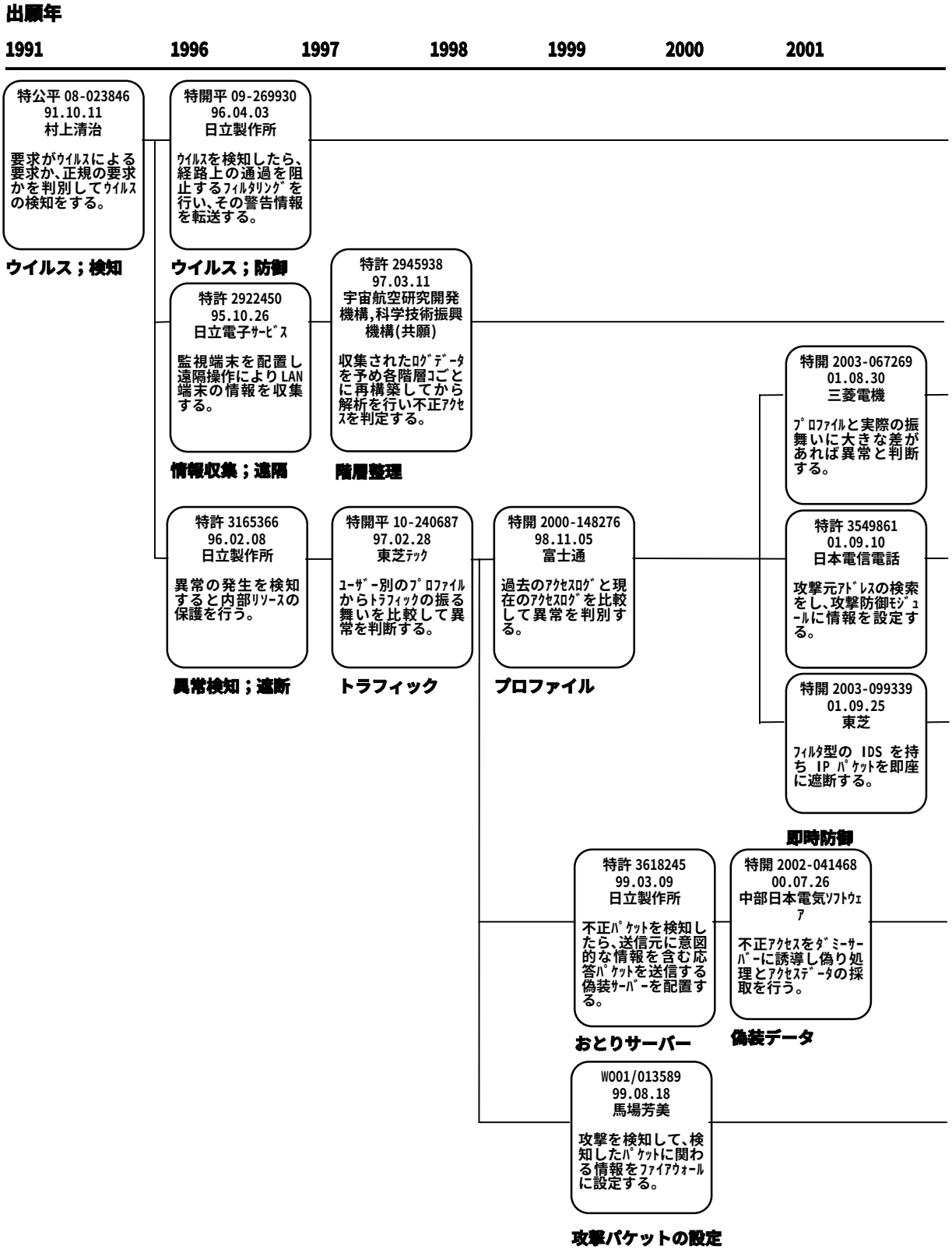
図1.1.6-1にアノマリ解析技術に関する進展を示す。ウイルスは、通常汚染して初めて特定されるが、特公平08-023846は、挙動を解析しウイルスを検知するものであり、特開平09-269930は検知して防御するものである。

特許2922450は遠隔で情報収集する技術であり、特許2945938で階層ごとにログを整理する技術に進展している。

トラフィックの異常を解析して各種アクションを行う技術は、特許3165366がアノマリを検出して通信路を遮断し、特開平10-240687がトラフィックの挙動からアノマリを検知し、特許3618245が、トラフィックのアノマリを検知し、おとりサーバーに不正アクセスを導き偽装応答し挙動を解析する技術に進展している。さらにWO01/013589はアノマリを検知しその結果をファイアウォールに設定する技術へと進展している。

通常ユーザプロファイルと比較してアノマリを検知する技術は、特開2000-148276が過去のログと照合してアノマリを検知し、特開2003-067269、特許3549861と特開2003-099339が即刻防御をしている。

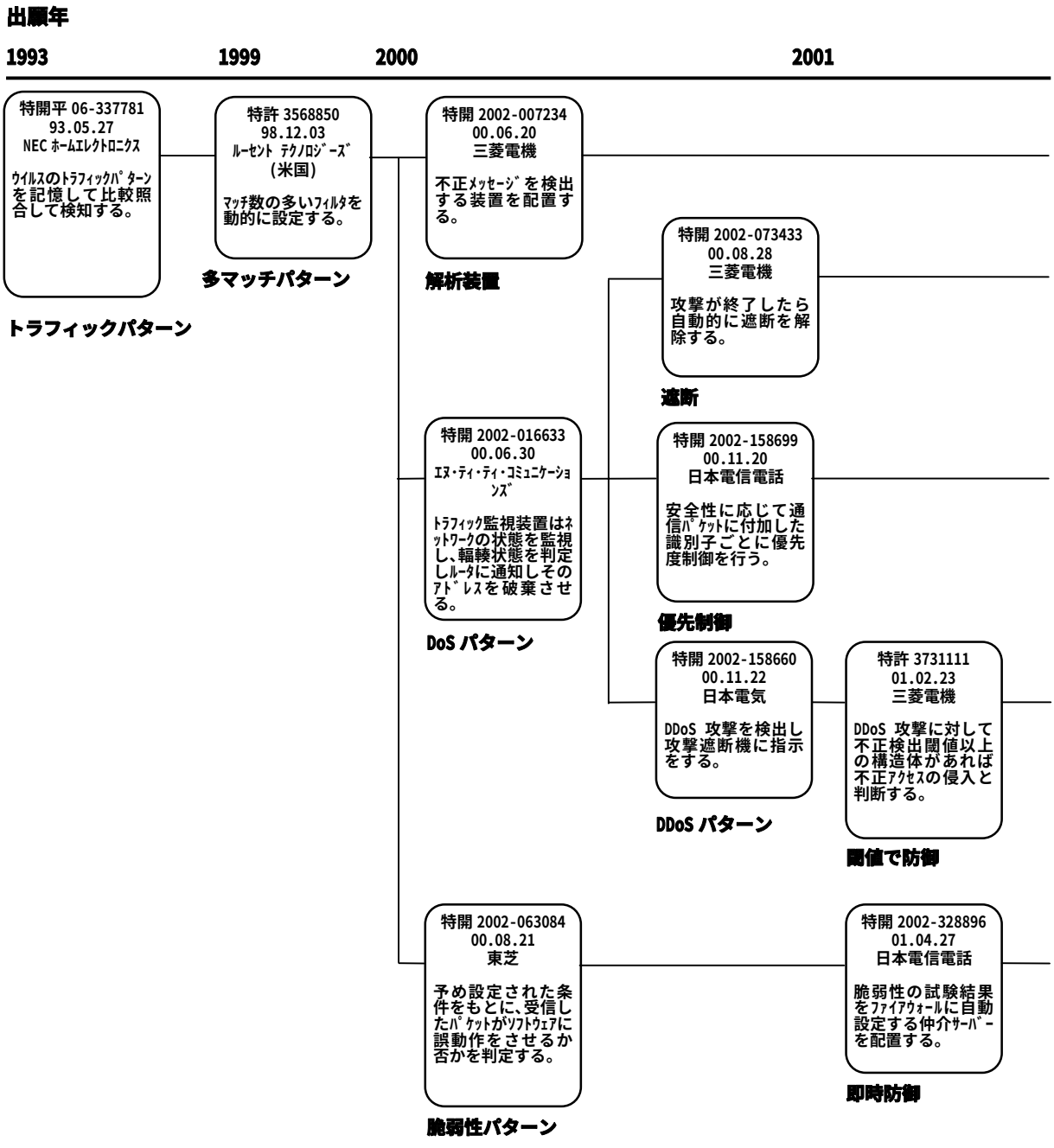
図1.1.6-1 アノマリ解析技術に関する進展



b シグネチャ解析技術

図1.1.6-2にシグネチャ解析技術に関する進展を示す。シグネチャ解析技術は、特開平06-337781で、ウイルスのシグネチャの照合から出発して、特許3568850にて、マッチの多いパターンを動的にシグネチャデータベースに設定し、特開2002-007234で解析装置に誘導させてパターン作成をする技術へと進展する。個々のパターン作成技術は、00年にほとんど同時に技術が見られ、特開2002-016633でDosパターンの作成、特開2002-158660でDDoSパターンの作成、特開2002-252654でDDoSの閾値による即時防御に技術が進展している。特開2002-063084は脆弱性パターンの作成、特開2002-328896では脆弱性パターンの即時防御に技術が進展している。

図1.1.6-2 シグネチャ解析技術に関する進展

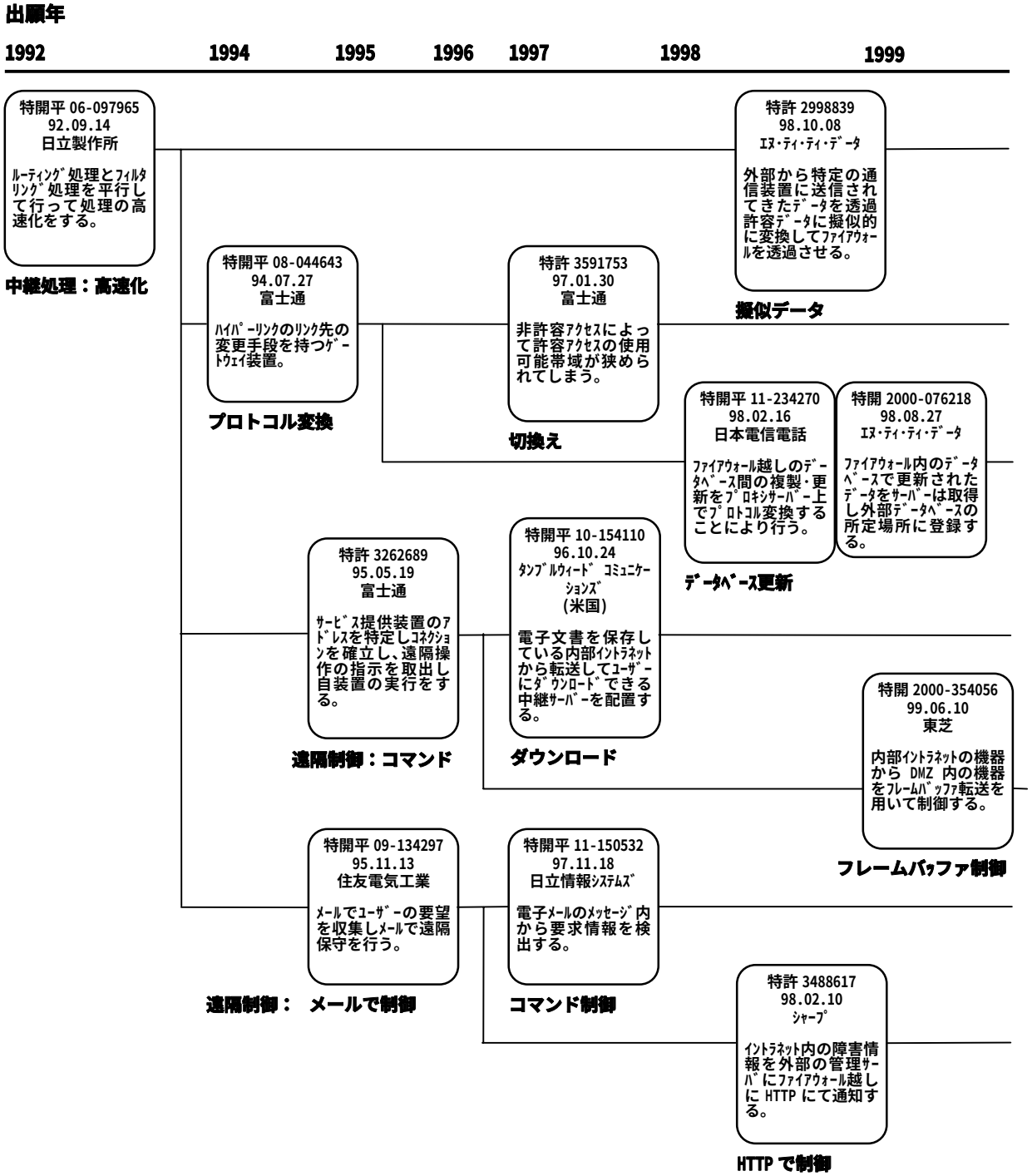


(2) アプリケーション中継技術

a プロキシ中継技術

図1.1.6-3にプロキシ中継技術に関する進展を示す。プロキシ中継技術では、遠隔制御の技術が中心になって進展している。特許3262689では、遠隔制御コマンドの認識と実行であり、特開平2000-354056はフレームバッファ内に遠隔制御をいれての制御である。特開平09-134297は、メールによる遠隔制御であり、特開平11-150532はメール内に遠隔コマンドを入れて制御するものである。さらに特許3488617はHTTPで遠隔制御するものである。

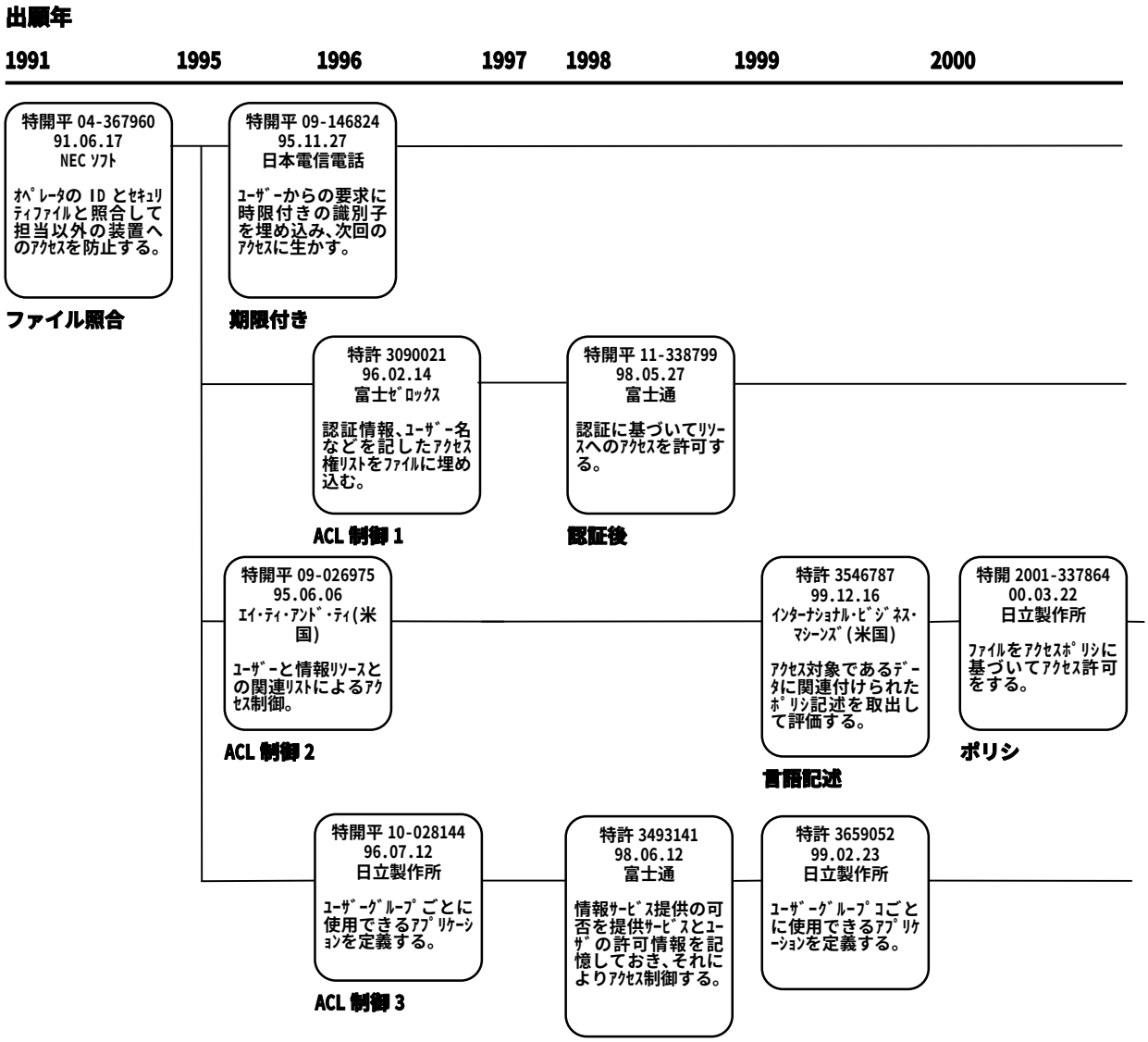
図1.1.6-3 プロキシ中継技術に関する進展



b コンテンツフィルタリング技術

図1.1.6-4にコンテンツフィルタリング技術に関する進展を示す。特開平04-367960はコンテンツとIDの照合でアクセス制御する技術で、96年に、特許3090021はアクセステーブル(ACL)にてコンテンツのアクセス制御をするようになり、さらに特開平10-28144のようにグループアクセス制御を行っている。特許3546787は、より詳細なアクセス制御のため言語を記述することにより可能にしている。

図1.1.6-4 コンテンツフィルタリング技術に関する進展

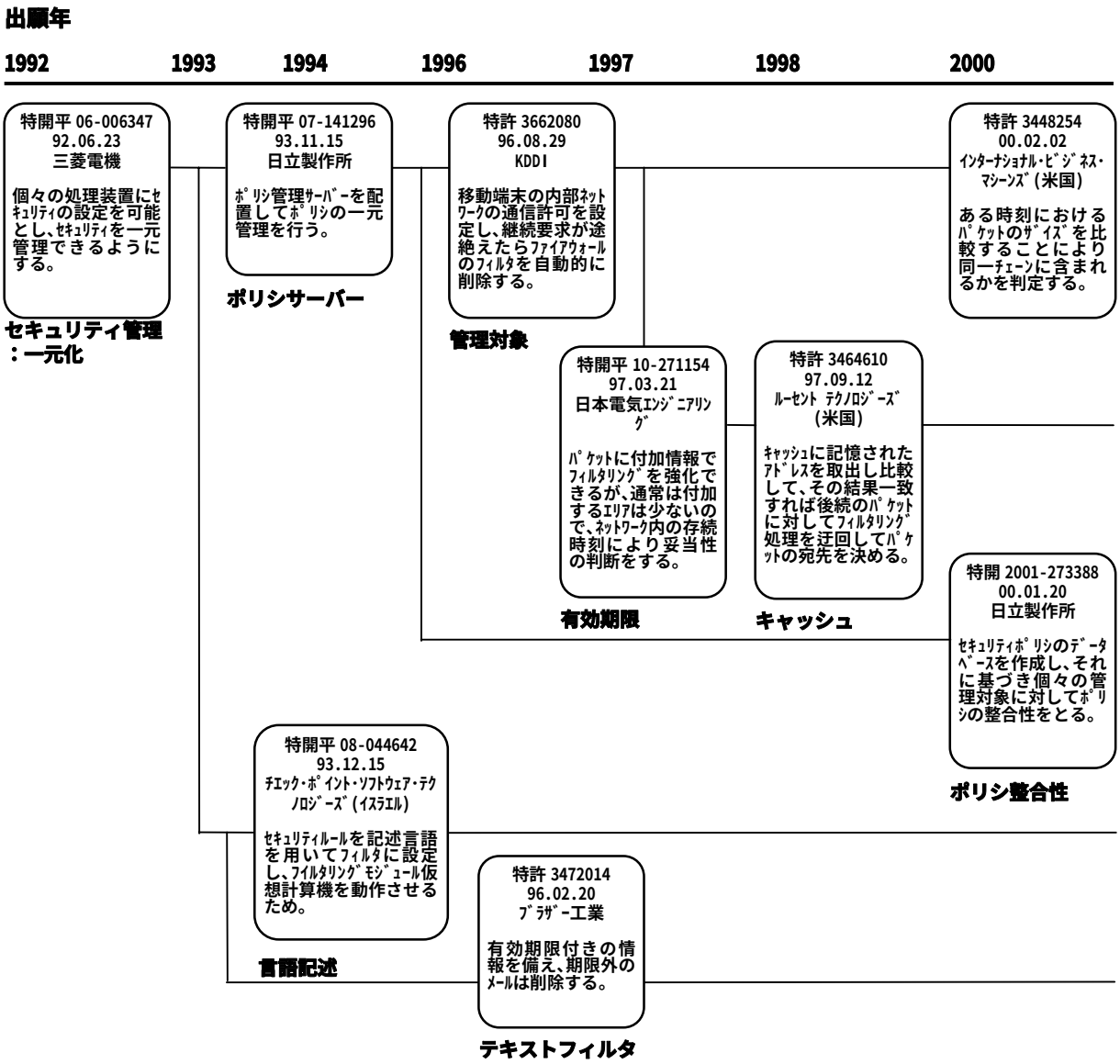


(3) パケットフィルタリング技術

a IPフィルタリング技術

図1.1.6-5にIPフィルタリング技術に関する進展を示す。セキュリティ管理の技術が主である。特開平06-006347、07-141296は、セキュリティの一元管理に関する技術である。激増するフィルタの削減の技術は特許3662080や特開平10-271154で対応している。特許3464610は、フィルタリングのキャッシュによる高速処理である。フィルタリングの内容強化として、詳細なフィルタリングのために言語記述する技術が、ファイアウォール大手のチェック・ポイント社(イスラエル)による特開平08-044642であり、激増するワームメール対策のフィルタリングとして、テキストフィルタリングを可能とした特許3472014がある。

図1.1.6-5 IPフィルタリング技術に関する進展

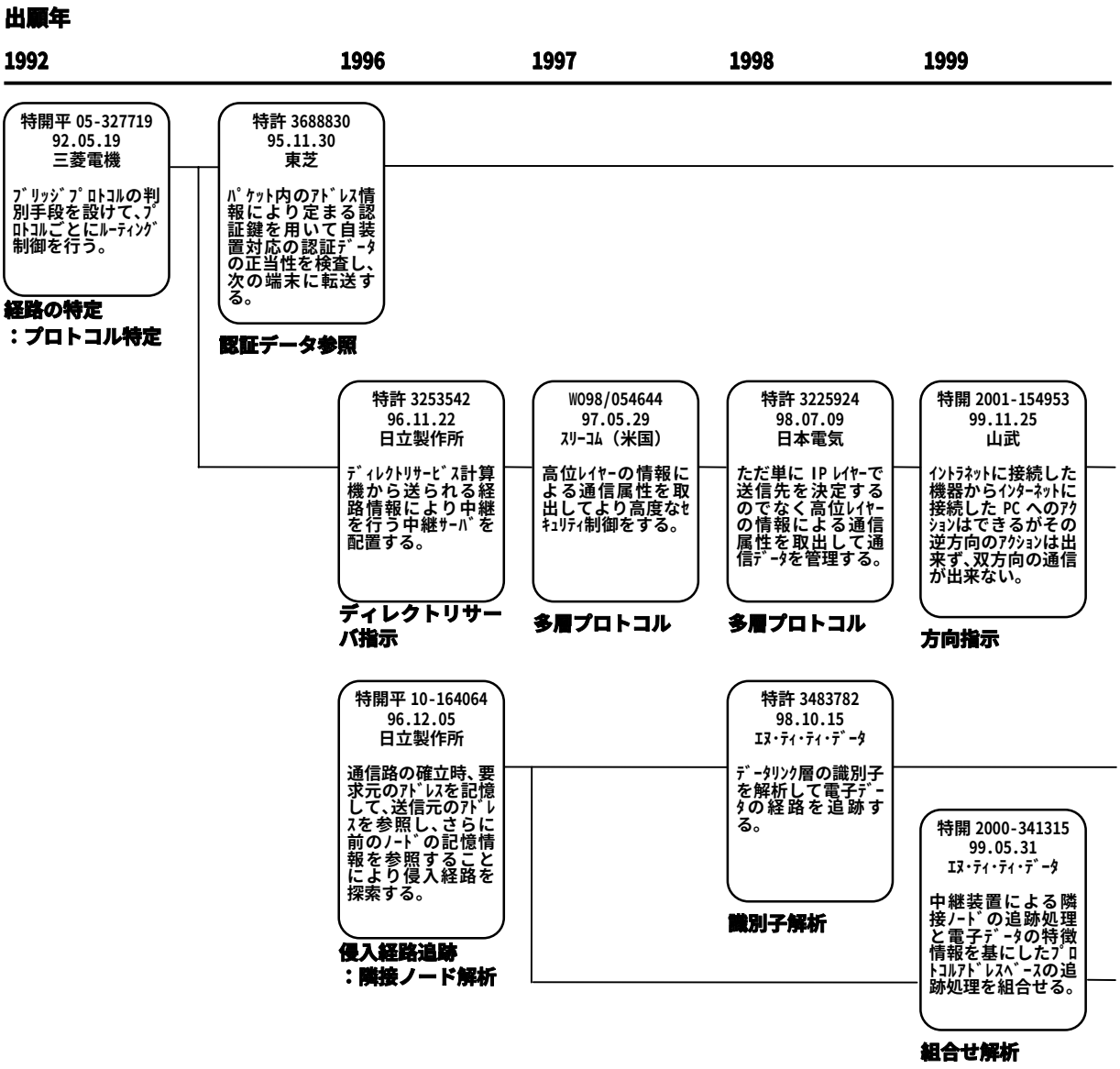


b ルーティング制御技術

図1.1.6-6にルーティング制御技術に関する進展を示す。特開平05-327719は、プロトコルごとにルートを定めておくものであり、特許3253542は中継サーバーでルートを定めておきそれ以外のルートのものはフィルタリングするものである。さらに詳細に上位プロトコルを使用するものが、WO98/054644や特許3225924である。

ルーティングによりフィルタリングはしないが、攻撃パケットの追跡のために侵入経路を追跡する技術が、隣接ノードを順番に追跡する技術として特開平10-164064にあり、リンク層の識別子の解析による技術が特許3483782で示されている。

図1.1.6-6 ルーティング制御技術に関する進展

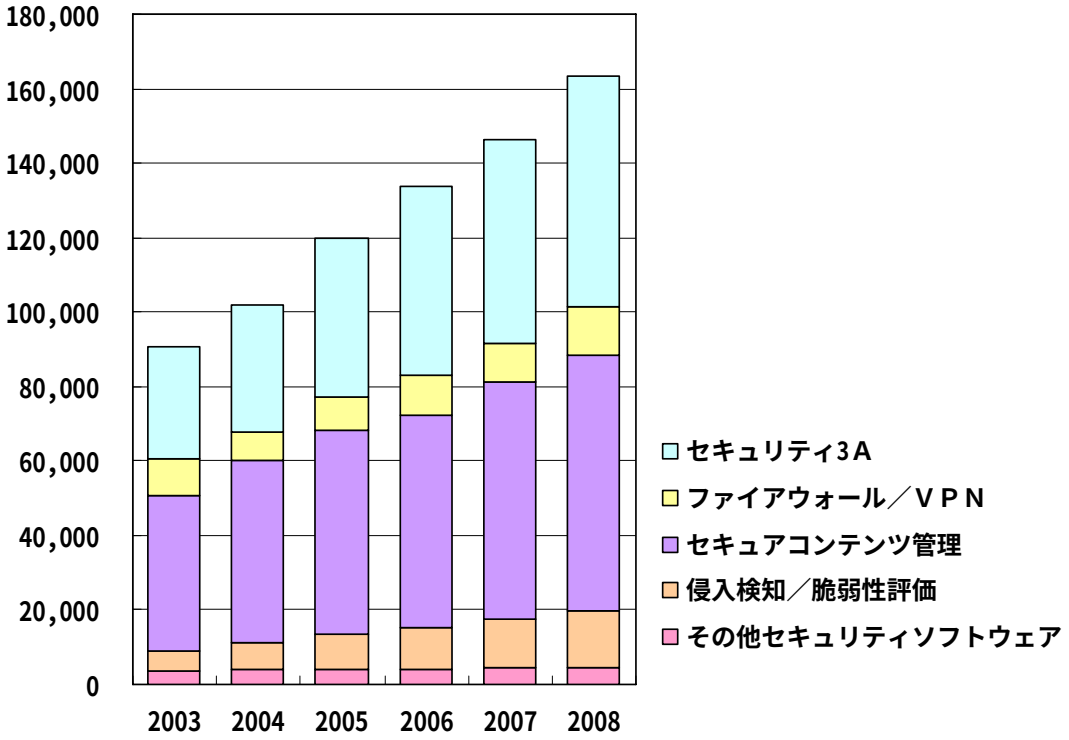


1.1.7 セキュリティソフトウェアの市場

(1) 市場規模

図1.1.7-1にマーケットのリサーチを専門に行うインタナショナル データ コーポレイション(International Data Corporation;IDC社)によるセキュリティソフトウェアの市場規模の推移を示す。2004年の実績は、約1000億円である。そのうちファイアウォール/VPNは約75億円で全体の7.5%、侵入検知/脆弱性評価は75億円で7.5%である。08年の予測は、セキュリティソフトウェア全体が約1600億円で伸び率が160%で、ファイアウォール/VPNは150億円で伸び率が200%、侵入検知/脆弱性評価は175億円で伸び率230%である。

(百万円)　　図 1.1.7-1 セキュリティソフトウェア市場規模の推移



(出典：http://www.idcjapan.co.jp/)

(2) 市場参加者・競争状況

ファイアウォールの主要製品の対応OSと機能を一覧表にして表1.1.7-1に示す。

イスラエルのチェック・ポイント・ソフトウエア・テクノロジーズ社(Check Point社、チェック・ポイント社)のファイアウォール製品であるFireWall-1(チェック・ポイント社の製品)は、世界で最も多く使用されている製品である。

表1.1.7-1　ファイアウォールの主要製品

製品名	FireWall-1	ISA 2000	Enterprise Firewall	PIX Firewall	SonicWall
会社名	Check Point	Microsoft	Symantec	Cisco System	SonicWall
対応OS					
WinNT/2000	○	○	○	―	―
Solaris	○	―	○	―	―
Linux	○	―	―	―	―
AIX	○	―	―	―	―
HP-UX	○	―	―	―	―
専用OS	○	―	○	○	○
機能					
ﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ	○	○	○	○	○
ﾌﾟﾛｷｼ	○	○	○	○	―
ｺﾝﾃﾝﾂ	△	△	○	△	○

△はオプション、○は対応

米国のインターネット セキュリティ システムズ社(ISS社)は、不正アクセス対策のIDS(Intrusion Detection System)商品で最も実績がある。RealSecure(ISS社の製品)はIDSとして今まで実績があり、最近Preventia(ISS社の製品)をIDSより進んだIPS(Intrusion Protection System)商品と称して販売している。InternetScanner(ISS社の製品)は、脆弱性診断システム商品として実績を持っている。

シスコ・システムズ社は、Cisco Secure IDS Sensor(シスコ・システムズ社の製品)を商品として販売し、またエンテラシス・ネットワーク社は、Dragon Sensor(エンテラシス・ネットワーク社の製品)を販売している。

またウイルスワクチンメーカーとして実績のある会社もIDSの商品を扱っている。コンピュータ・アソシエイツは、eTrust Intrusion Detection（コンピュータ・アソシエイツ社の製品）を販売、シマンテックは、Symantec ManHunt（シマンテック社の製品）を販売、日本ネットワークアソシエイツ社は、McAfee IntruShield(ネットワークアソシエイツ社の製品)を販売している。

(3) 標準化、法規制

ネットワークセキュリティに関する国内の標準規格、法規制としては以下のようなものがある。

・標準化

情報セキュリティの標準化は、ISO/IEC 15408に規定されている。守秘性(Confidentiality)、完全性(Integrity)、可用性 (Availability)の頭文字を取ったCIAとして知られる標準セキュリティ基準を定めている。この３基準は、機密に関わる情報の危険性を計り、セキュリティ方針を確立するための一般的に受け入れられる基準である。我が国では、この国際標準を基に、2000年７月にセキュリティ評価・認定制度という日本工業規格JIS X 5070として制定された。セキュリティ製品は、世界標準に基づいて評価される環境が整いつつある。以下にCIA基準の詳細を説明する。

＊ 守秘性(Confidentiality)：機密に関わる情報へのアクセスは事前設定された人物に限る。情報を不当に見られないようにする。

＊ 完全性(Integrity)：情報はそれ自体が不完全または不適当になるよう破壊や改ざんをされてはならない。許可のないユーザーには、機密に関わる情報の変更・消去の権限を限定する。

＊ 可用性(Availability)：情報は許可のあるユーザーには必要な時はいつでもアクセス可能にしておく。可用性は情報が合意している頻度とタイミングで入手できるという保証である。ISPと企業間で使用されるサービスレベル契約書のパーセンテージが同意事項にある。

・関連法規、基準

＊ 不正アクセス関連

コンピュータ不正アクセス対策基準(経産省)
(http://www.ipa.go.jp/security/ciadr/guide-crack.html)

不正アクセス行為の禁止等に関する法律(通称、不正アクセス防止法)
(http://www.ipa.go.jp/security/ciadr/law199908.html)

＊ 脆弱性関連情報

ソフトウエア等脆弱性関連情報取扱基準(経産省)
(http://www.meti.go.jp/feedback/downloadfiles/i40706dj.pdf)

情報セキュリティ早期警戒パートナーシップガイドライン(IPA)
(http://www.ipa.go.jp/security/ciadr/partnership_guide_200507.html)

「製品開発ベンダーにおける脆弱性情報取扱に関する体制と手順整備のためのガイドライン」JEITA・JISA
(http://it.jeita.or.jp/infosys/info/0407JEITA-guideline/index.html)

「製品開発ベンダーにおける脆弱性関連情報取扱に関する体制と手順整備のためのガイドライン」JPSA
(http://www.jpsa.or.jp/info/04/20041203_security.html)

(4) セキュリティ関連組織

表1.1.8-2セキュリティ関連組織を示す。ネットワーク侵入検知防御技術に関する情報源である。

表1.1.7-2 ネットワーク侵入検知防御技術に関する情報源

名称/ホームページURL	備考
(独) 情報処理推進機構(IPA)/ (http://www.ipa.go.jp/security/index.html)	・ウイルス、不正アクセス、脆弱性関連情報の届出先 ・情報セキュリティ対策の情報提供 ・セキュリティ用語集；本書で用いる用語の出典
コンピュータ緊急対応センター(JPCERT)/ (http://www.jpcert.or.jp/)	・インターネットを介した不正アクセスに関する情報を収集・公開する団体 ・セキュリティに関する啓蒙活動
(社) 情報サービス産業協会(JISA)/ (http://www.jisa.or.jp/)	・情報サービスに係る企業で組織する業界団体。
(社) 日本パーソナルコンピュータソフトウェア協会(JPSA)/(http://www.jpsa.or.jp/)	・パソコンソフトに係る企業で組織する業界団体でマーケティングサポートも行う
(社) 電子情報技術産業協会(JEITA)/ (http://www.jeita.or.jp/japanese/)	・電子機器、電子部品に係る企業で組織する業界団体。電子機器、電子部品国内出荷統計を提供

1.2 不正アクセス侵入検知防御技術の特許情報へのアクセス

● 国際特許分類(IPC)によるアクセス

不正アクセス侵入検知防御技術に関する技術は、国際特許分類(IPC)では、G06F、H04Lのサブクラスに分類されている。

不正アクセス侵入検知防御技術は、IPCメイングループで、下記に分類されている。

G06F13/00　メモリ、入力/出力装置または中央処理装置の間の情報または他の信号の相互接続または転送
G06F15/00　デジタル計算機一般
H04L9/00　秘密または安全な通信のための配置
H04L12/00　データ交換ネットワーク

● ファイル・インデックス(FI)によるアクセス

不正アクセス侵入検知防御技術に関する技術は、以下のファイル・インデックス(FI)によってアクセスができる。

G06F13/00,351　１以上の遠方ステーションからのデジタル入力、またはそのようなステーションへのデジタル出力
- A　・伝送制御
- B　・・プロトコル変換
- E　・転送内容に特徴を有するもの
- F　・・コマンド
- G　・・文書・テキスト・イメージ
- H　・・プログラム
- N　・監視・試験
- Z　・その他のもの（上位層のファイアウォール含む）

G06F13/00,353　通信制御装置；通信制御処理装置
- C　・通信処理、制御
- U　・監視・試験

G06F13/00,357　共通の転送媒体を介した情報転送
- A　・バス転送路

G06F15/00,310　オンライン端末システム
- D　・接続制御

G06F15/00,320　オンライン障害対策、モニタ
- K　・モニタ、トレース、状態表示

G06F15/00,330　オンライン機密保護
- A　・オンライン機密保護一般

H04L9/00,673　IDまたはパスワードに関するもの
- B　・端末IDに関するもの

H04L12/02　データ交換ネットワークの細部

H04L12/22　・データチャンネルから許可なくデータを取り出すことを防止するための配置
H04L12/26　・監視配置；試験配置
H04L12/46　・ネットワーク間の相互接続
B　・・LAN際の通信制御
H04L12/46,100　・・LAN間の中継装置に関する構成
A　・・・ブリッジ
B　・・・ゲートウェイ
H04L12/56　・パケット交換方式
A　・・アドレス管理
H04L12/56,100　・・ルーティング
Z　・・・その他のもの
H04L12/56,400　・・試験
Z　・・・その他のもの
H04L12/66　・異なる形式の交換方式を有するネットワーク間の接続のための配置
B　・・セキュリティ機能を有するゲートウェイ(下位層のファイアウォール)

● Fターム(FT)によるアクセス

不正アクセス侵入検知防御技術に関する技術は、以下のFターム(FT)によってアクセスができる。

テーマコード：5B089　計算機・データ通信
GA19　プロキシ/代理サーバー
JB16　監視情報
KA17　不正行為の防止/セキュリティ
KB13　アクセス権/セキュリティ
KC57　秘密・機密
KC58　署名・認証
KF05　プロトコル変換
KG08　ルーティング
MC08　データ監視
テーマコード：5B085　情報処理
AC14　ログジャーナル
AE04　端末ID
テーマコード：5K030　広域データ交換
GA15　セキュリティ、機密保護、暗号化、認証
LC18　不要なデータを消去、破棄するもの
MB09　トラフィック監視、通信量、稼動情報

テーマコード：5K032　　LAN
AA08　機密保護
CC02　プロトコル変換
CC05　トラフィック制御
CC07　アドレス変換

● キーワードによるアクセス

不正アクセス侵入検知防御技術に用いられるキーワードまたはフリーワードとしては、以下のものがある。

ファイアウォール、侵入検知システム(IDS)、侵入検出システム、不正アクセス侵入検知、不正アクセス侵入検出、不正侵入防御、不正侵入防衛、不正侵入防止

● 技術要素別のアクセス

不正アクセス侵入検知防御技術を構成する技術要素にアクセスする場合、それらの技術をカバーしているIPC、FIとこれをインデックスするFTを用いて、各技術要素を特定することができる。

表1.2に、不正アクセス侵入検知防御技術の技術要素別検索ツールの例を示す。

表1.2 不正アクセス侵入検知防御技術の技術要素別検索ツール(1/2)

技術要素		FIおよびFターム
侵入検知解析技術	アノマリ解析技術 シグネチャ解析技術 脆弱性診断技術	G06F13/00,351N G06F13/00,353N G06F15/00,320K H04L12/26 H04L12/56,400 5B089JB16 5B089MC08 5B085AC14 5K030MB09 5K032CC05
アプリケーション中継技術	プロキシ中継技術	G06F13/00,351E G06F15/00,330A 5B089GA19
	コンテンツフィルタリング技術	G06F13/00,351G G06F13/00,351H 5B089KB13

表1.2 不正アクセス侵入検知防御技術の技術要素別検索ツール(2/2)

技術要素		FIおよびFターム
パケットフィルタリング技術	IPフィルタリング技術	H04L12/46,100A H04L12/46,100B H04L12/66B 5B089KA17
	ルーティング制御技術	H04L12/46B H04L12/56,100 5B089KG08
	IPアドレス変換技術	H04L12/56A 5K032CC07
ホスト認証技術		H04L9/00,673B 5B089KC57 5B085AE04
トンネリング技術		H04L12/22 5B089KC57

● 米国特許分類(CL)によるアクセス

不正アクセス侵入検知防御技術に関する技術は、以下の米国特許分類(CL)によってアクセスができる。

Class 726　Information Security
- 726/001　Policy
- 726/002　Access control or Authentication
- 726/003　・Network
- 726/004　・・Authorization
- 726/005　・・Credential
- 726/011　・・Firewall
- 726/012　・・・Proxy server or gateway
- 726/013　・・・Packet filtering
- 726/014　・・・Security protocols
- 726/015　・・・・Virtual Private Network(VPN) or Virtual Terminal Protocol(VTP)
- 726/022　Monitoring or scanning of software or data including attack prevention
- 726/023　・Intrusion detection
- 726/025　・Vulnerability assessment

● 欧州特許分類(ECLA)によるアクセス

不正アクセス侵入検知防御技術に関する技術は、以下の欧州特許分類(ECLA)によってアクセスができる。

H04L29/02	Communication control; Communication processing
H04L29/06	・Characterised by a protocol
H04L29/06C6	・・Protocols or architecture for network security
H04L29/06C6A	・・・For the separating internal and external traffic, e.g. firewalls
H04L29/06C6B	・・・For the confidentiality of the information travelling over the network,e.g.encryption of data
H04L29/06C6C	・・・For allowing a denying access to network elements
H04L29/06C6C2	・・・・Using authentication protocols,e.g. Kerberos, Challenge-response
H04L29/06C6D	・・・Security provided by high-level applications, e.g. Java
H04L29/06C6E	・・・Maintaining multiple levels of security, e.g. classes,user profiles,policies
H04L29/06C6F	・・・Using different network or path for securing the traffic
H04L29/06C6G	・・・For guaranteeing the integrity of the information, e.g. digital signatures

1.3 技術開発活動の状況

1.3.1 不正アクセス侵入検知防御技術の技術開発活動

1993年１月～03年12月までに出願された不正アクセス侵入検知防御技術に関する特許出願は、2,221件である。

図1.3.1-1に、不正アクセス侵入検知防御技術に関する出願人数-出願件数の推移を示す。不正アクセス侵入検知防御技術に関する出願は、1993年においては、出願件数が32件、出願人が21人であったが2000年には、出願件数が約13倍に増加し、出願人数も約10倍に増加した。しかし、01年以降、出願人が大幅に減少している。

図1.3.1-1 不正アクセス侵入検知防御技術に関する出願人数－出願件数の推移

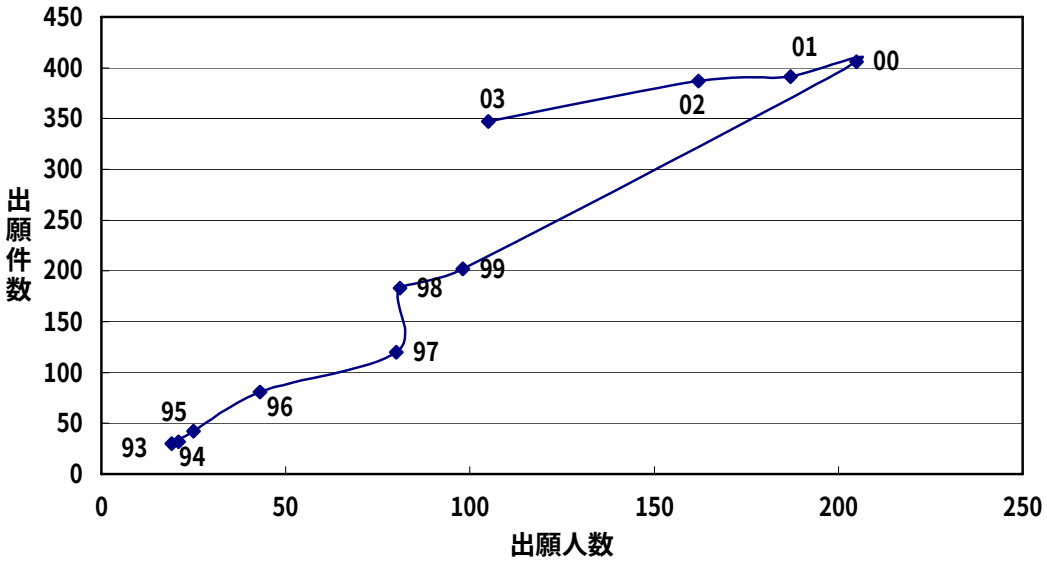


図1.3.1-2に、不正アクセス侵入検知防御技術に関する技術要素別の出願件数の推移を示す。侵入検知解析技術に関するものが607件(28%)、アプリケーション中継技術に関するものが561件(25%)、パケットフィルタリング技術に関するものが520件(23%)、ホスト認証技術に関するものが277件(12%)、トンネリング技術に関するものが255件(11%)である。

侵入検知解析技術とパケットフィルタリング技術は、依然として高い水準にあるのに対して、アプリケーション中継、ホスト認証技術とトンネリング技術は、2000年から01年をピークに減少に転じている。

図1.3.1-2 不正アクセス侵入検知防御技術に関する技術要素別の出願件数の推移

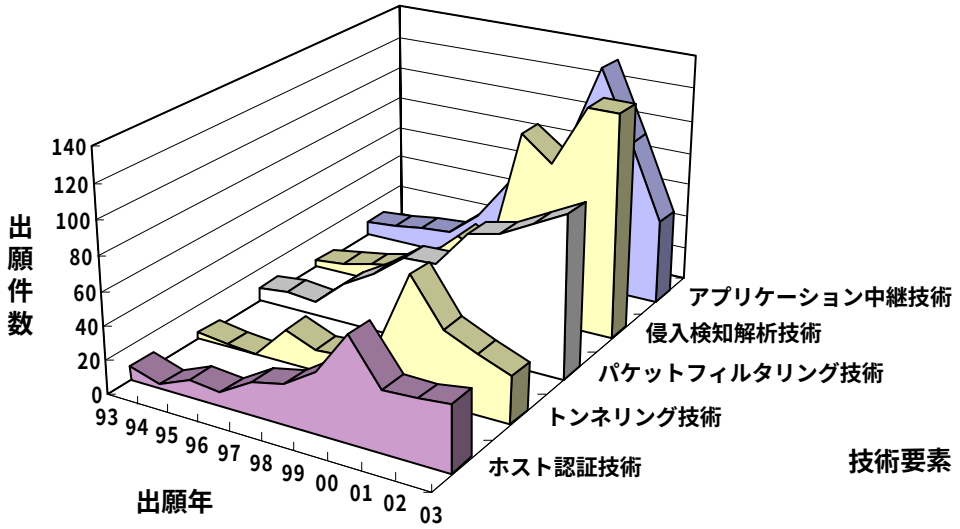


図1.3.1-3に、不正アクセス侵入検知防御技術に関する出願人構成比の推移を示す。上場法人の占める割合は、93年には80%と高かったが、海外からの出願の増加に伴い、徐々に減少した。その後2002年から増加傾向に転じ、03年には84%を占めている。大学、公的研究機関のものの構成比は、１%前後で少ない。

図1.3.1-3 不正アクセス侵入検知防御技術に関する出願人構成比の推移

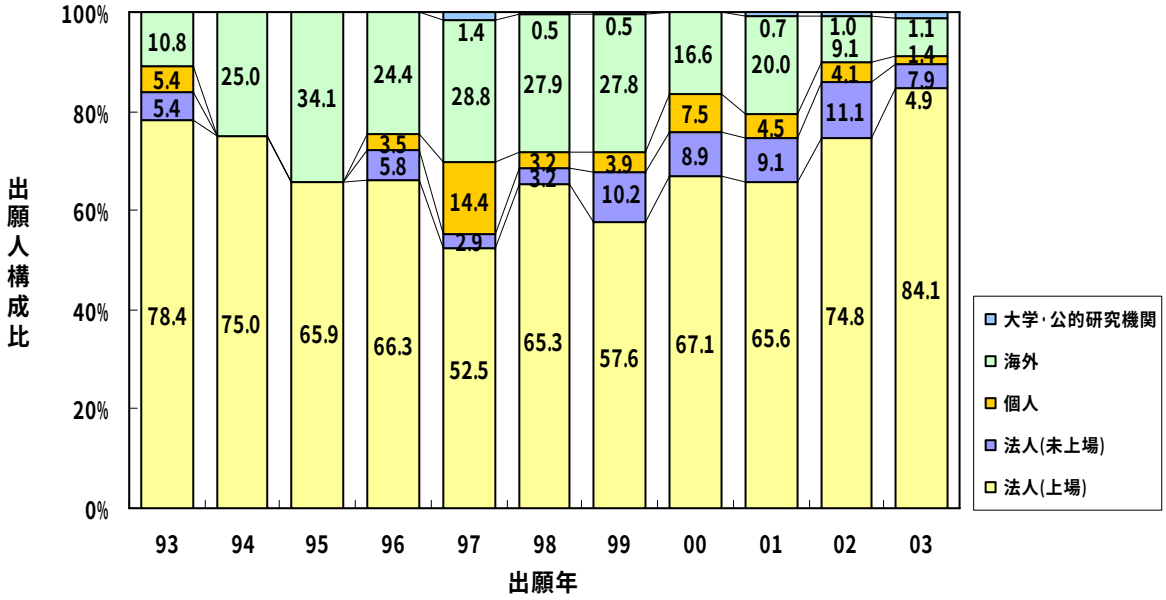


表1.3.1-1に、不正アクセス侵入検知防御技術に関する出願件数の多い出願人を示す。この分野での出願の多い企業は、NTT等の通信サービス企業と、日立製作所、日本電気、東芝、富士通等のコンピュータメーカーである。

出願件数でみると、NTTと日立製作所の２社が、それぞれ150件を越えている。最も出願件数の多いNTTは、1995年から５件と増え始め、98年以降10件以上の高い水準の出願を維持し、02年は44件、03年は55件と集中して出願している。

また日立製作所の出願は、93年には5件出願したが、96年に15件と急増し、以降20件前後の高い水準で落ち着いている。

これに続く日本電気は、93年には5件出願していたが、99年から10件以上に拡大した。2000年には27件となり、02年以降も20件前後の高い水準を維持している。

東芝は、96年から10件前後に増え始め、02年以降20件の水準を維持している。

富士通は、93年から５件前後の出願が続き、98年以降10件前後の多い出願を維持していたが、02年以降さらに出願を増加している。

三菱電機は、98年から10件と出願が増え、以降10件前後の高い水準を維持している。特に00年は、24件と集中して出願した。松下電器産業は、2000年以降、10件前後の出願を維持している。ソニーは、2000年以降、10件前後と多く出願していて、01年に15件と集中して出願した。

富士ゼロックスは、早い時期から出願、98年に４件と増やし、以降５件前後の水準を維持している。リコーは02年以降10件前後の高い水準が維持している。マイクロソフトは、

03年に15件と集中して出願した。サン・マイクロシステムズは、2000年以降の出願がなくなった。

表 1.3.1-1 不正アクセス侵入検知防御技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件推移											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	1	1	6	7	7	14	10	27	25	44	55	197
2	日立製作所	5	3	3	15	7	17	17	21	16	23	25	152
3	日本電気	5	2	0	4	3	9	16	27	24	22	19	131
4	東芝	2	2	1	8	13	10	7	12	19	22	28	124
5	富士通	4	5	9	3	7	10	4	17	13	21	23	116
6	三菱電機	0	4	0	2	3	10	8	24	17	9	13	90
7	松下電器産業	1	1	1	1	2	3	3	13	9	14	13	61
8	ソニー	1	0	1	1	1	2	2	9	15	13	7	52
9	キヤノン	2	1	0	1	1	6	4	8	9	7	9	48
10	インターナショナル･ビジネス･マシーンズ(米国)	3	3	3	3	4	2	7	7	11	3	2	48
11	富士ゼロックス	0	1	2	1	2	4	3	3	4	5	6	31
12	リコー	0	0	1	1	0	2	1	2	4	9	10	30
13	マイクロソフト(米国)	0	0	0	0	1	2	0	0	4	5	15	27
14	エヌ･ティ･ティ･データ	0	0	0	0	1	5	2	1	6	8	2	25
15	沖電気工業	0	0	0	1	4	2	3	0	4	4	5	23
16	サン･マイクロシステムズ(米国)	0	0	2	5	5	7	4	0	0	0	0	23
17	横河電機	0	0	0	0	0	0	0	4	4	8	6	22
17	エヌ･ティ･ティ･ドコモ	0	0	0	0	0	0	2	4	5	7	4	22
19	セイコーエプソン	0	0	0	0	0	2	0	3	6	6	4	21
19	ヒューレット･パッカード(米国)	0	0	0	0	0	3	2	3	10	3	0	21
19	ルーセント　テクノロジーズ(米国)	0	0	0	0	7	5	4	4	0	0	1	21
22	日立ソフトウェアエンジニアリング	2	0	1	2	2	3	1	0	3	2	1	17
23	シャープ	0	1	0	0	0	1	2	4	2	1	4	15
23	村田機械	0	0	0	0	0	0	0	6	9	0	0	15
23	エヌ･ティ･ティ･コムウェア	0	0	0	0	0	2	2	2	4	5	0	15
23	エヌ･ティ･ティ･コミュニケーションズ	0	0	1	0	1	0	1	5	3	1	3	15
27	東日本電信電話	0	0	0	0	0	1	1	8	1	1	1	13
28	大日本印刷	0	0	0	0	0	2	4	1	2	1	1	11
28	野村総合研究所	0	0	0	0	0	2	0	5	0	1	3	11
28	カシオ計算機	0	0	0	0	1	0	3	1	3	1	2	11
28	山武	0	0	0	0	0	1	2	1	1	5	1	11

表1.3.1-2に、不正アクセス侵入検知防御技術に関する大学・公的研究機関の出願件数を示す。不正アクセス侵入検知防御技術に関する大学・公的研究機関の出願件数は、少なく、その中で科学技術振興機構は、４件である。産業技術総合研究所、宇宙航空研究開発機構と東京大学は、各２件である。その他、関西ティー・エル・オー、産学連携機構九州、明治大学、東京理科大学、東京電機大学は、各１件である。

表 1.3.1-2 不正アクセス侵入検知防御技術に関する大学・公的研究機関の出願件数

No.	出願人名	出願年											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	科学技術振興機構	0	0	0	0	1	0	0	0	1	2	0	4
2	産業技術総合研究所	0	0	0	0	0	0	0	0	0	0	2	2
2	宇宙航空研究開発機構	0	0	0	0	1	1	0	0	0	0	0	2
2	東京大学	0	0	0	0	0	0	0	0	1	1	0	2
5	関西ティー･エル･オー	0	0	0	0	0	0	1	0	0	0	0	1
5	産学連携機構九州	0	0	0	0	0	0	0	0	0	0	1	1
5	明治大学	0	0	0	0	0	0	0	0	0	0	1	1
5	東京理科大学	0	0	0	0	0	0	0	0	1	0	0	1
5	東京電機大学	0	0	0	0	0	0	0	0	0	1	0	1

1.3.2 不正アクセス侵入検知防御技術の海外における技術開発活動

図1.3.2-1に、不正アクセス侵入検知防御技術に関する米国における出願件数の推移を示す。1999年米国特許法改正により出願公開制度が始まり、登録と公開でデータベースが異なるため集計は分けて示す。直近の５年間のデータであるが、2000年は公開特許で250件あり、01年で500件以上に激増し、日本の出願件数より100件多い。その後、減少傾向にあるが300件の高水準にあり、日本の出願件数とほぼ同じである。

ただし米国特許分類、欧州特許分類を利用して検索しているため件数の比較はその考慮を要する。

図1.3.2-1 不正アクセス侵入検知防御技術に関する米国における出願件数の推移

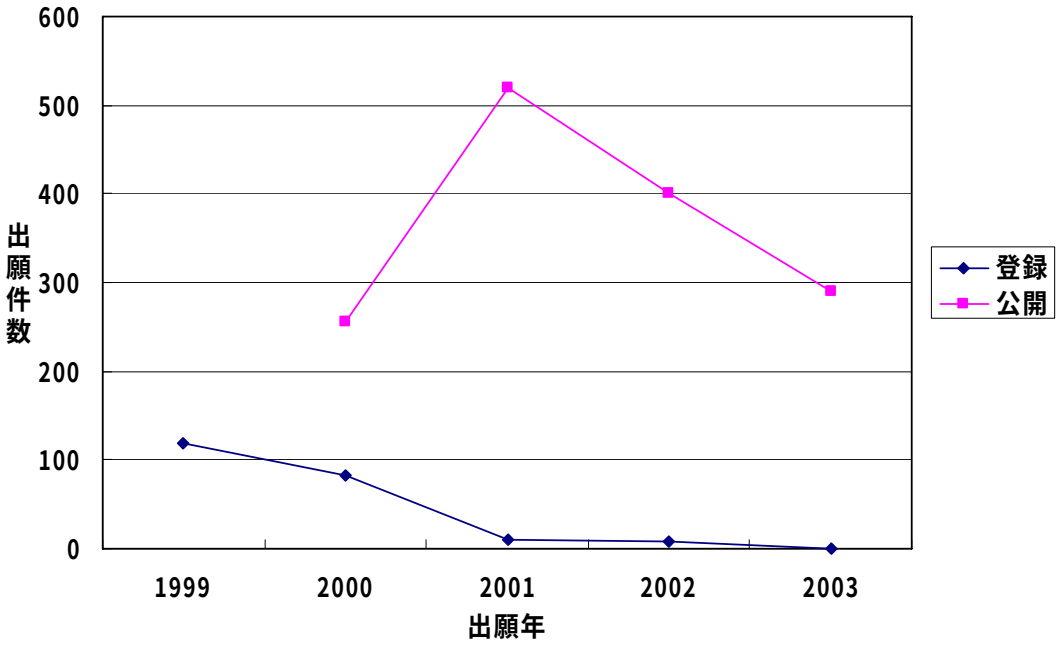


図1.3.2-2に、不正アクセス侵入検知防御技術に関する欧州における出願件数の推移を示す。2000年から増加傾向にあり、02年で130件の出願件数でピークとなった。欧州における不正アクセス侵入検知防御技術の出願件数は、米国や日本の出願の約４分の１である。

図1.3.2-2 不正アクセス侵入検知防御技術に関する欧州における出願件数の推移

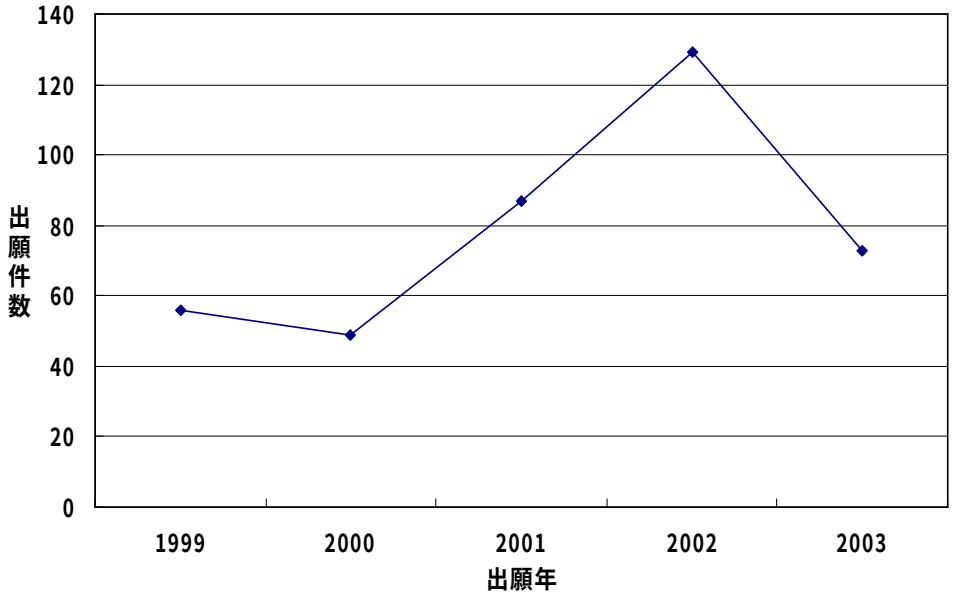


図1.3.2-2に、不正アクセス侵入検知防御技術に関する日本における出願件数の推移を示す。2000年以降、400件前後の安定した出願が続いている。

図1.3.2-2 不正アクセス侵入検知防御技術に関する日本における出願件数の推移

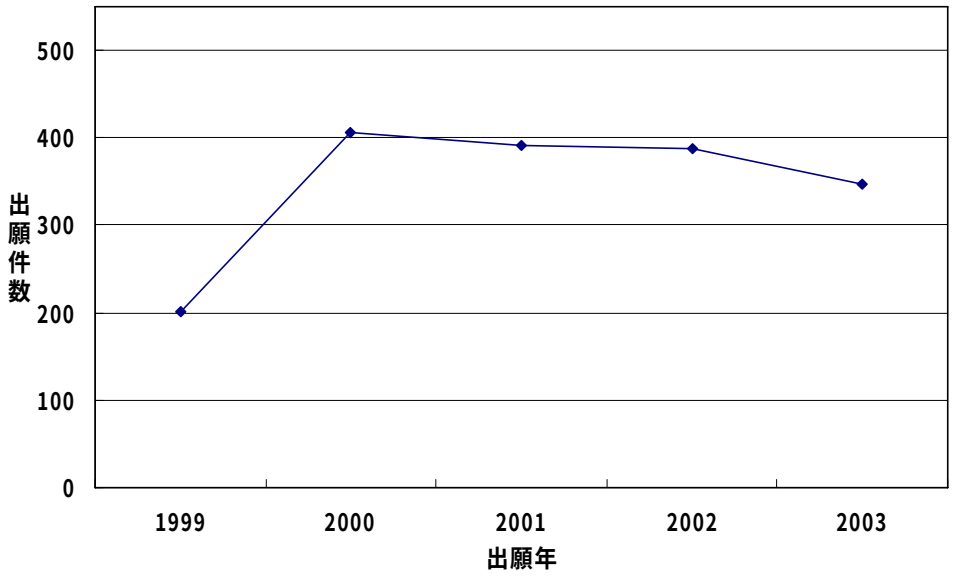


表1.3.2-1に、不正アクセス侵入検知防御技術に関する米国における登録件数の多い権利人を示す。IBMが32件と多く出願して、次いでシスコシステムが29件、サン・マイクロシステムズが23件、と多く出願している。

表 1.3.2-1 不正アクセス侵入検知防御技術に関する米国における登録件数の多い権利人

No.	登録件数	権利者
1	32	INTERNATIONAL BUSINESS MACHINES（米国）
2	29	CISCO SYSTEM（米国）
3	23	SUN MICROSYSTEMS（米国）
4	19	Microwave Communication inc（米国）
5	15	LUCENT TECHNOLOGIES（米国）

1999 年 1 月～2003 年 12 月の出願

表 1.3.2-2 に、不正アクセス侵入検知防御技術に関する米国における出願件数の多い出願人を示す。IBM が 80 件と多く出願、次いでマイクロソフトが 59 件、ヒューレット・パカードが 41 件、と多く出願している。

表 1.3.2-2 不正アクセス侵入検知防御技術に関する米国における出願件数の多い出願人

No.	出願件数	出願人
1	80	INTERNATIONAL BUSINESS MACHINES（米国）
2	59	MICROSOFT（米国）
3	41	HEWLETT PACKARD（米国）
4	25	TELEWARE（イギリス）
5	24	INTEL（米国）

1999 年 1 月～2003 年 12 月の出願

表 1.3.2-3に、不正アクセス侵入検知防御技術に関する欧州における出願件数の多い出願人を示す。マイクロソフトが30件、フランスのアルカテル社が14件、と多く出願している。

表 1.3.2-3 不正アクセス侵入検知防御技術に関する欧州における出願件数の多い出願人

No.	出願件数	出願人
1	30	MICROSOFT（米国）
2	14	CIT ALCATEL（フランス）
2	14	STONESOFT CORP（フィンランド）
2	14	SUN MICROSYSTEMS（米国）
5	13	ERICSSON（スウェーデン）

1999 年 1 月～2003 年 12 月の出願

1.3.3 侵入検知解析技術

図1.3.3-1に、侵入検知解析技術に関する出願人数-出願件数の推移を示す。侵入検知解析技術は、1999年までは、低迷していた。2000年に出願件数、出願人とも急増し、その後も増加傾向にある。99年と03年を比べると、出願件数で約５倍、出願人数で約５倍になっている。

図1.3.3-1 侵入検知解析技術に関する出願人数－出願件数の推移

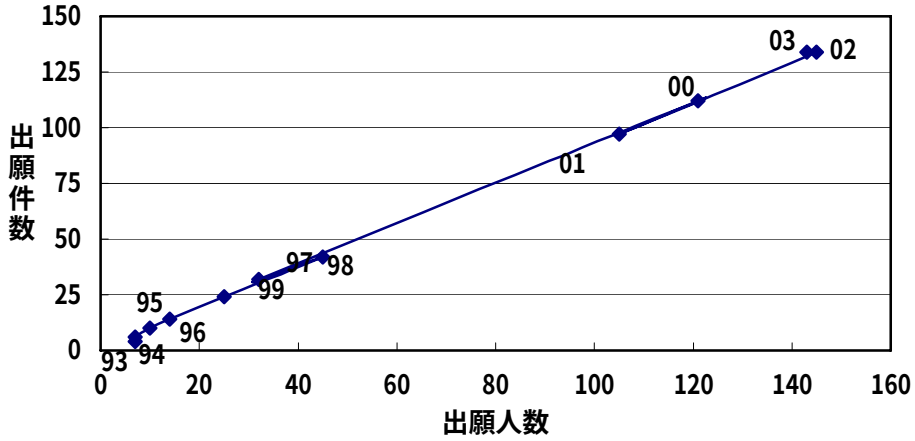


図1.3.3-2に、侵入検知解析技術に関する技術要素別の出願件数の推移を示す。３種の技術は、2000年に急増するほぼ同じ開発パターンを示している。しかしその後、シグネチャ解析技術とアノマリ解析技術は、現在でも増加傾向にあるが、脆弱性診断技術は、2000年をピークに減少傾向にある。

図 1.3.3-2 侵入検知解析技術に関する技術要素別の出願件数の推移

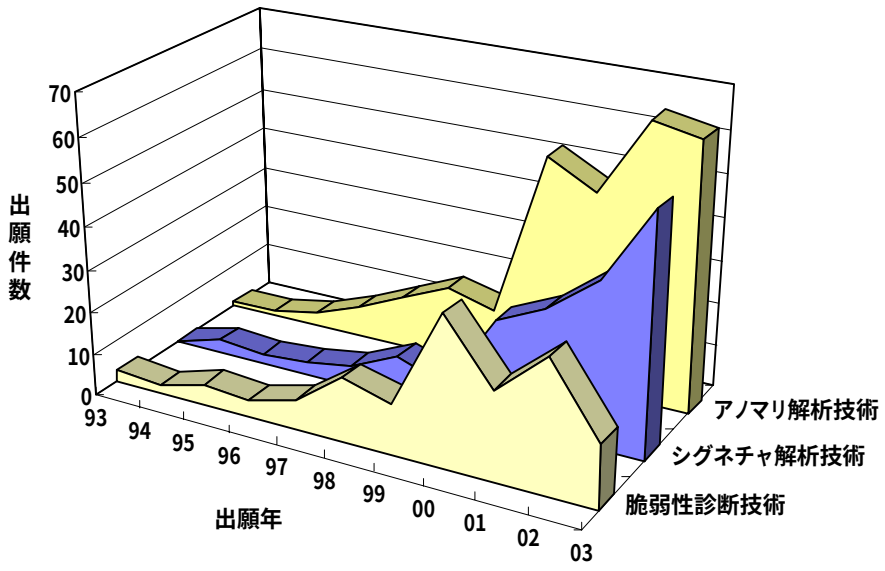


表1.3.3-1に、侵入検知解析技術に関する出願件数の多い出願人を示す。NTT、東芝、富士通、日立製作所は、総数の出願件数が44～45件とほぼ同じである。NTTは、03年に22件と集中して出願している。東芝は、01年に10件、03年に13件と集中して出願している。富士通は、01年に11件、03年に14件と集中して出願している。日立製作所は、早い時期の96年に８件、最近の02年と03年に各８件出願している。

表 1.3.3-1 侵入検知解析技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	1	1	0	0	1	0	5	6	9	22	45
1	東芝	0	2	0	1	0	5	3	3	10	8	13	45
1	富士通	0	0	3	0	4	4	2	2	5	11	14	45
4	日立製作所	1	1	1	8	2	3	4	6	2	8	8	44
5	三菱電機	0	1	0	0	1	1	3	11	8	6	7	38
6	日本電気	1	0	0	0	0	3	1	11	6	7	5	34
7	エヌ･ティ･ティ･データ	0	0	0	0	0	1	0	1	5	5	1	13
8	横河電機	0	0	0	0	0	0	0	2	2	6	2	12
9	沖電気工業	0	0	0	1	1	1	0	0	2	3	3	11
10	ルーセント テクノロジーズ(米国)	0	0	0	0	2	4	1	2	0	0	1	10
10	松下電器産業	0	0	0	0	0	1	0	2	2	1	4	10

表1.3.3-2に、アノマリ解析技術に関する出願件数の多い出願人を示す。日立製作所、東芝、日本電気、NTT、三菱電機と富士通は、各20件前後出願している。東芝とNTTは、03年に各７件と集中して出願している。

表 1.3.3-2 アノマリ解析技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日立製作所	0	1	1	4	2	1	2	4	0	2	4	21
2	東芝	0	0	0	1	0	0	2	2	4	4	7	20
2	日本電気	0	0	0	0	0	3	1	4	4	4	4	20
2	日本電信電話	0	0	1	0	0	0	0	3	3	6	7	20
5	三菱電機	0	0	0	0	0	1	2	5	3	5	3	19
6	富士通	0	0	0	0	2	1	0	1	2	7	5	18

表1.3.3-3に、シグネチャ解析技術に関する出願件数の多い出願人を示す。NTTと東芝は、総数で各18件と最も多く出願している。NTTは、03年に12件と集中して出願している。東芝は94年に２件の出願があり、その後2000年から出願が続いている。

表 1.3.3-3 シグネチャ解析技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	0	0	0	0	1	0	1	2	2	12	18
1	東芝	0	2	0	0	0	2	0	0	5	4	5	18
3	日立製作所	0	0	0	2	0	0	0	1	1	4	4	12
4	富士通	0	0	0	0	1	0	1	0	2	2	5	11
5	三菱電機	0	0	0	0	0	0	0	4	3	0	3	10
6	エヌ･ティ･ティ･データ	0	0	0	0	0	0	0	0	3	1	1	5
6	日本電気	0	0	0	0	0	0	0	3	0	1	1	5

表1.3.3-4に、脆弱性診断技術に関する出願件数の多い出願人を示す。富士通は、16件と最も多く出願している。95年の早い時期から出願が続いている。

表 1.3.3-4 脆弱性診断技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	富士通	0	0	3	0	1	3	1	1	1	2	4	16
2	日立製作所	1	0	0	2	0	2	2	1	1	2	0	11
3	三菱電機	0	1	0	0	1	0	1	2	2	1	1	9
3	日本電気	1	0	0	0	0	0	0	4	2	2	0	9
5	東芝	0	0	0	0	0	3	1	1	1	0	1	7
5	日本電信電話	0	1	0	0	0	0	0	1	1	1	3	7

1.3.4 アプリケーション中継技術

図1.3.4-1に、アプリケーション中継技術に関する出願人数-出願件数の推移を示す。アプリケーション中継技術は、1997年から増加し01年で出願件数、出願人ともにピークになり、その後02年、03年と出願件数、出願人とも減少傾向にある。

図1.3.4-1 アプリケーション中継技術に関する出願人数－出願件数の推移

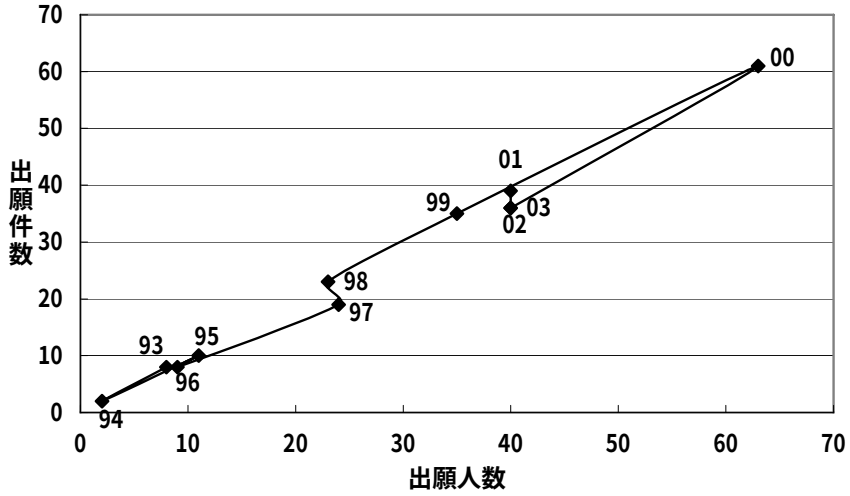


図1.3.4-2に、アプリケーション中継技術に関する技術要素別の出願件数の推移を示す。プロキシ中継技術とコンテンツフィルタリング技術の２つの技術とも、同じような開発パターンを示している。つまり97年から増加して、01年にピークとなり、以降減少傾向にある。

図 1.3.4-2 アプリケーション中継技術に関する技術要素別の出願件数の推移

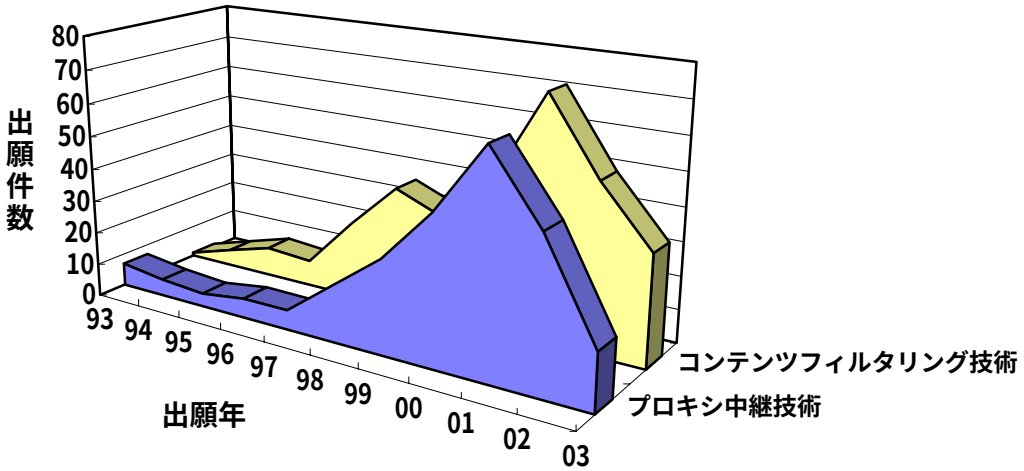


表1.3.4-1に、アプリケーション中継技術に関する出願件数の多い出願人を示す。NTTは、合計で49件と最も多く出願している。01年に11件、02年に13件と集中して出願している。次に多い日本電気は、01年に９件と集中した出願している。ソニーが、01年に７件の集中した出願している。

表 1.3.4-1 アプリケーション中継技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	1	0	2	2	1	7	1	8	11	13	3	49
2	日本電気	1	2	0	1	0	2	3	5	9	6	4	33
3	日立製作所	1	0	0	1	2	3	4	4	5	4	5	29
4	富士通	1	3	1	0	2	3	1	5	3	5	4	28
5	東芝	0	0	0	1	2	2	1	4	1	5	5	21
6	ソニー	0	0	0	0	1	0	1	3	7	6	2	20
6	キヤノン	1	1	0	1	1	1	2	2	6	4	1	20
8	インターナショナル･ビジネス･マシーンズ(米国)	0	1	1	0	2	1	3	0	5	2	0	15
9	リコー	0	0	1	1	0	0	0	0	3	2	6	13
9	松下電器産業	0	0	1	0	0	0	2	4	2	3	1	13
11	サン･マイクロシステムズ(米国)	0	0	1	3	2	2	3	0	0	0	0	11
12	ヒューレット･パッカード(米国)	0	0	0	0	0	1	1	1	5	2	0	10

表1.3.4-2に、プロキシ中継技術に関する出願件数の多い出願人を示す。NTTは、合計で27件と最も多く出願している。01年に７件と集中して出願した。

表 1.3.4-2 プロキシ中継技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	0	0	1	1	5	1	4	5	7	3	27
2	日本電気	0	0	0	0	0	2	3	2	5	3	3	18
3	富士通	0	3	1	0	1	1	0	1	0	5	2	14
3	日立製作所	0	0	0	1	1	1	0	3	2	3	3	14
5	東芝	0	0	0	0	2	1	1	1	1	3	3	12
6	ソニー	0	0	0	0	1	0	0	1	4	2	2	10

表1.3.4-3に、コンテンツフィルタリング技術に関する出願件数の多い出願人を示す。NTTは、合計で22件と最も多く出願している。01年と02年に各６件と集中して出願した。

図 1.3.4-3 コンテンツフィルタリング技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	1	0	2	1	0	2	0	4	6	6	0	22
2	日本電気	1	2	0	1	0	0	0	3	4	3	1	15
2	日立製作所	1	0	0	0	1	2	4	1	3	1	2	15
4	富士通	1	0	0	0	1	2	1	4	3	0	2	14
5	キヤノン	1	0	0	1	0	0	1	1	3	4	0	11
6	ソニー	0	0	0	0	0	0	1	2	3	4	0	10

1.3.5 パケットフィルタリング技術

図1.3.5-1に、パケットフィルタリング技術に関する出願人数-出願件数の推移を示す。パケットフィルタリング技術は、1996年までは、低迷していた。97年から出願件数、出願人ともに増加して、直近の03年まで、右肩上がりで増加し、出願件数で約10倍、出願人数で約４倍となっている。

図1.3.5-1 パケットフィルタリング技術に関する出願人数-出願件数の推移

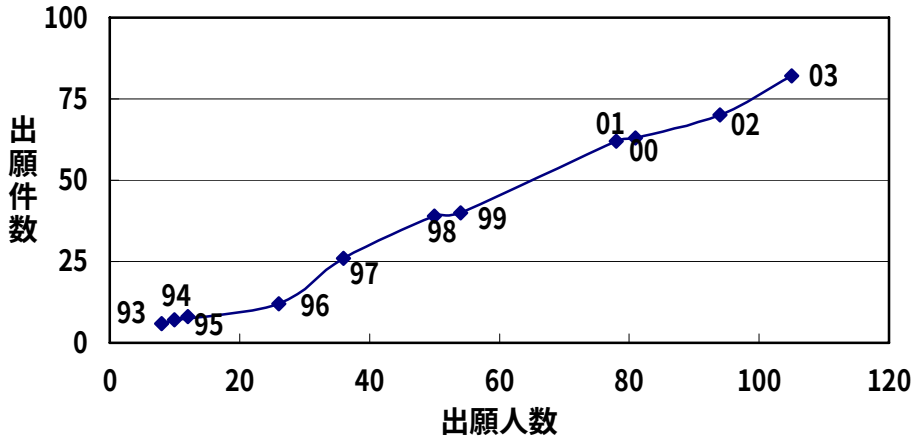


図1.3.5-2に、パケットフィルタリング技術に関する技術要素別の出願件数の推移を示す。３種の技術のうち、IPフィルタリング技術の件数は最も多い。IPフィルタリング技術は、95年から急激な増加をして現在も続いている。ルーティング制御技術は96年頃から20件前後に増加して、以降その水準を現在も維持している。IPアドレス変換技術は、少しずつ増加し00年頃20件前後に増加し、以降その水準を現在も維持している。

図1.3.5-2 パケットフィルタリング技術に関する技術要素別の出願件数の推移

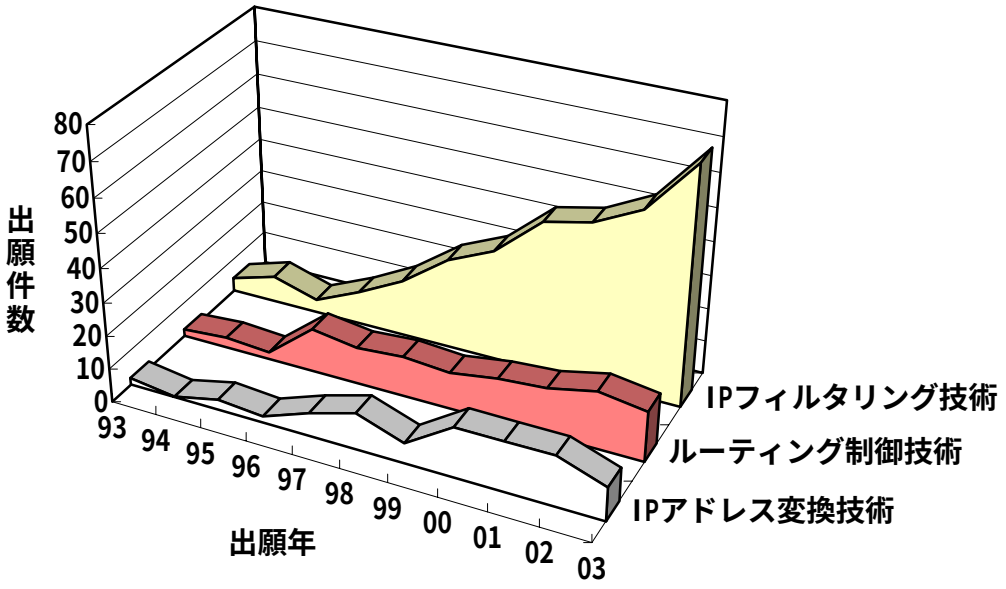


表1.3.5-1に、パケットフィルタリング技術に関する出願件数の多い出願人を示す。NTTは、1996年から出願が始まり、02年に15件、03年に18件と集中して出願している。日立製作所は、98年以降、５件以上の出願が続いている。東芝は、03年に10件と集中して出願している。日本電気は、99年に７件と集中して出願している。マイクロソフトは、03年に８件と集中して出願している。サン・マイクロシステムズも03年に８件と集中した出願をしている。

表 1.3.5-1 パケットフィルタリング技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	0	0	3	2	4	3	3	3	15	18	51
2	日立製作所	1	2	1	4	3	6	5	5	5	9	5	46
3	東芝	1	0	1	1	6	2	2	3	6	5	10	37
4	日本電気	0	0	0	2	2	3	7	4	2	3	6	29
5	富士通	1	1	3	1	0	2	1	6	4	3	3	25
6	三菱電機	0	2	0	0	0	2	0	4	3	2	4	17
6	松下電器産業	1	1	0	0	1	1	0	1	1	6	5	17
8	マイクロソフト(米国)	0	0	0	0	1	0	0	0	1	2	8	12
9	インターナショナル･ビジネス･マシーンズ(米国)	1	1	1	1	1	0	2	3	1	0	0	11
9	ソニー	0	0	0	1	0	0	1	2	1	3	3	11
11	サン･マイクロシステムズ(米国)	0	0	0	0	1	0	0	0	1	0	8	10

表1.3.5-2に、IPフィルタリング技術に関する出願件数の多い出願人を示す。日立製作所は、98年以降、５件前後の多い出願が続いている。NTTは、03年に11件と集中して出願している。東芝は、03年に９件と集中して出願している。マイクロソフトも03年に７件の集中した出願をしている。

表 1.3.5-2 IP フィルタリング技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日立製作所	1	1	0	1	1	6	4	3	5	7	5	34
2	日本電信電話	0	0	0	0	1	1	1	2	1	8	11	25
3	東芝	1	0	0	0	4	0	2	2	4	2	9	24
4	日本電気	0	0	0	2	2	2	5	2	0	2	4	19
5	富士通	0	1	2	0	0	2	0	2	2	1	3	13
6	マイクロソフト(米国)	0	0	0	0	1	0	0	0	1	2	7	11
7	松下電器産業	0	1	0	0	0	0	0	0	1	3	5	10
7	三菱電機	0	1	0	0	0	1	0	2	2	2	2	10

表1.3.5-3に、ルーティング制御技術に関する出願件数の多い出願人を示す。NTTは、合計で18件と他の出願人より多い出願をして、02年に７件と集中した出願をしている。

表 1.3.5-3 ルーティング制御技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	0	0	3	1	2	1	0	1	7	3	18
2	東芝	0	0	1	1	2	1	0	0	1	1	0	7
3	日立製作所	0	1	0	3	0	0	1	0	0	1	0	6
4	松下電器産業	1	0	0	0	1	1	0	1	0	1	0	5
4	富士通	0	0	0	1	0	0	1	1	1	1	0	5
4	日本電気	0	0	0	0	0	0	2	1	1	0	1	5

表1.3.5-4に、IPアドレス変換技術に関する出願件数の多い出願人を示す。NTTは、03年に４件の出願がある。富士通は、2000年に３件の出願がある。

表 1.3.5-4 IP アドレス変換技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	0	0	0	0	1	1	1	1	0	4	8
2	富士通	1	0	1	0	0	0	0	3	1	1	0	7
3	日立製作所	0	0	1	0	2	0	0	2	0	1	0	6
3	東芝	0	0	0	0	0	1	0	1	1	2	1	6
5	日本電気	0	0	0	0	0	1	0	1	1	1	1	5

1.3.6 ホスト認証技術

図1.3.6-1に、ホスト認証技術に関する出願人数-出願件数の推移を示す。2000年までは増加が続いていたが、02年、03年件数と出願人の減少傾向にある。

図1.3.6-1 ホスト認証技術に関する出願人－出願件数の推移

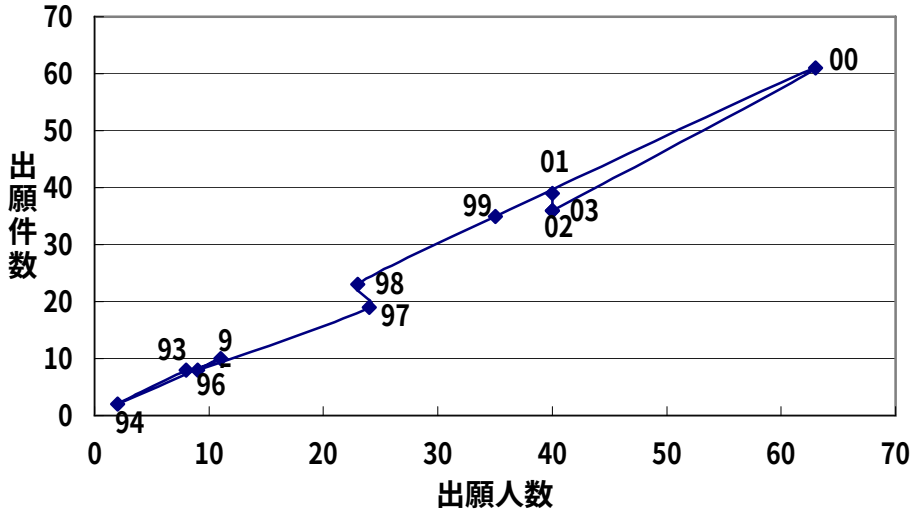


表1.3.6-1に、ホスト認証技術に関する出願件数の多い出願人を示す。NTTは、合計で33件と最も多く出願しており、03年に８件と集中した出願をしている。

表 1.3.6-1 ホスト認証技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	日本電信電話	0	0	3	2	3	0	4	4	4	5	8	33
2	日立製作所	2	0	1	1	0	4	1	3	4	1	4	21
3	日本電気	3	0	0	1	1	1	3	3	2	3	2	19
4	三菱電機	0	0	0	0	0	1	2	4	3	1	0	11
5	松下電器産業	0	0	0	0	0	0	1	4	0	2	2	9
6	富士通	0	1	2	2	0	0	0	1	0	0	2	8
6	東芝	1	0	0	1	2	1	1	0	1	1	0	8
8	富士ゼロックス	0	0	0	0	0	3	1	1	0	0	2	7
8	キヤノン	1	0	0	0	0	1	1	3	0	1	0	7

1.3.7 トンネリング技術

図1.3.7-1に、トンネリング技術に関する出願人数-出願件数の推移を示す。2000年までは増加が続いていたが、02年、03年件数と出願人の減少傾向にある。

図1.3.7-1 トンネリング技術に関する出願件数-出願人数の推移

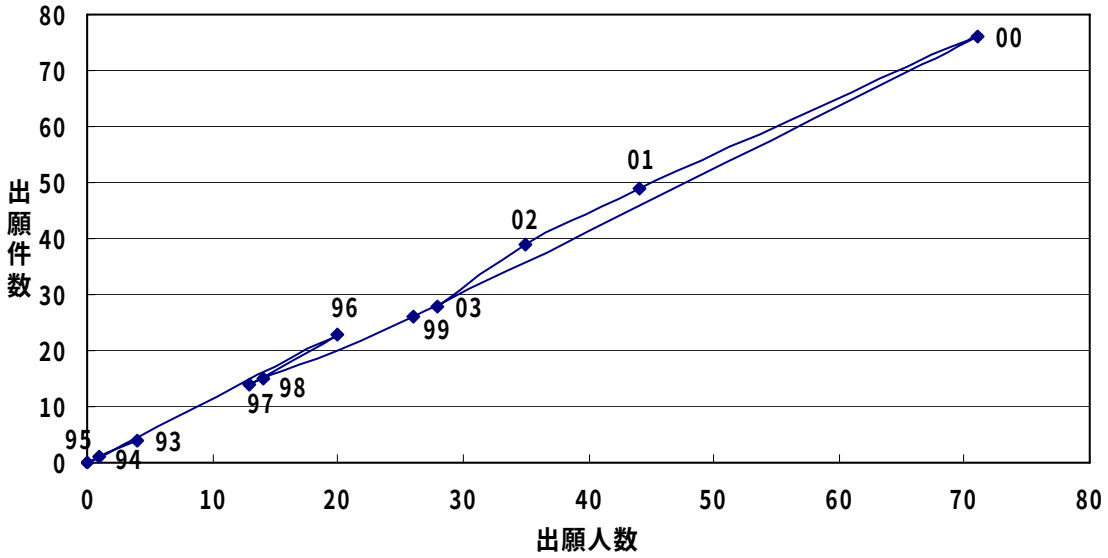


表1.3.7-1に、トンネリング技術に関する出願件数の多い出願人を示す。三菱電機は、2000年に５件と多い出願をしている。NTTも、2000年に７件と集中した出願をしている。日本電気は01年に５件と多い出願をしている。

表 1.3.7-1 トンネリング技術に関する出願件数の多い出願人

No.	出願人名	年次別出願件数											合計
		93	94	95	96	97	98	99	00	01	02	03	
1	三菱電機	0	0	0	2	2	4	2	5	3	0	1	19
1	日本電信電話	0	0	0	0	1	2	2	7	1	2	4	19
3	日本電気	0	0	0	0	0	0	2	4	5	3	2	16
4	東芝	0	0	0	4	3	0	0	2	1	3	0	13
5	日立製作所	0	0	0	1	0	1	3	3	0	1	3	12
5	松下電器産業	0	0	0	1	1	1	0	2	4	2	1	12
7	インターナショナル･ビジネス･マシーンズ(米国)	1	1	0	2	1	0	1	1	3	0	1	11
8	富士通	2	0	0	0	1	1	0	3	1	2	0	10

1.4 技術開発の課題と解決手段

不正アクセス侵入検知防御技術に関する特許出願の技術開発課題を、表1.4-1に示す。課題Ⅰ、課題Ⅱ、課題Ⅲの3階層に分けられている。

表 1.4-1 不正アクセス侵入検知防御技術に関する技術開発課題(1/4)

課題Ⅰ	課題Ⅱ	課題Ⅲ
侵入防御の性能向上	アドレスフィルタの強化	アドレス通過阻止強化
		フィルタの動的設定の簡略化
		異種 URL の阻止強化
		誤配信の防止
		マルチキャストの対処
		公開ポートの節約、制限
	フィルタルール設定の効率化	設定作業の簡略化
		動的設定の容易化
		設定誤りの防止
	フィルタルール適用の整合性	ルール適用の一元化
		個別ルール適用の容易性
		ルール適用範囲の見直し
		ルール適用の評価
	プロトコルフィルタの強化	不適切メールの阻止強化
		不適切ウェブの阻止強化
		プロトコル通過阻止強化
		異種ダイアログの阻止強化
	フイルタリング処理の効率化	照合など処理時間の短縮
		フィルタ処理の負荷軽減
		フィルタデータの見直し
		重複アドレスの見直し
利用サービスの保護強化	リソース保護の強化	利用コンテンツの保護
		アプリケーション利用の保護
		共有リソースの保護
		利用機器の保護
		データベースの保護
		オブジェクトの保護
	アクセス管理の効率化	アクセスセキュリティ強化
		アクセスルール設定の容易化
		アクセス管理の統合化
		アクセス管理の容易化
		アクセス許可範囲の適正化
		アクセス許可操作の簡便化
		アクセス速度の向上
		登録件数の節減
デバイスの正当性向上	成済ましの防止	デバイス ID の正当性
		アドレス詐称の防止
		送信元の正当性
		相互での正当性
		送信先の正当性
	認証処理の効率化	認証処理の簡略化
		認証入力の省略、煩雑性の解消
		適切な認証方法の選択
		認証回数の削減
		認証の更新

表 1.4-1 不正アクセス侵入検知防御技術に関する技術開発課題(2/4)

課題 I	課題 II	課題III
通信データの中継性能向上	アプリケーション層の中継機能拡大	アプリケーションの疎通化
		外部アクセスの疎通化
		データベース間の同期化
	経路生成の効率向上	適切な経路の確保
		送信者の匿名性向上
		エージェントに移動の保証
		プロトコルの選択性向上
		送信先の隠蔽性向上
		認証による経路の確保
	ネットワーク層の中継機能拡大	NAT 越えによる疎通化
		固定割付による枯渇防止
		中継処理時間の軽減
		ポート番号の簡単な設定
	トランスポート層の中継機能拡大	プロトコルの疎通化
		応答情報による疎通化
		正当者アドレスの疎通化
システムの性能向上	保守・信頼性の向上	遠隔からの安全性・制御性の向上
		装置の状態把握
		装置の接続把握
		VPN と一般通信路の選択
		攻撃からの迅速な回復
		保守性の向上
		故障のバックアップ
	システム負荷の軽減	処理時間の短縮
		トラフィックの集中排除
		処理能力の向上
		セキュリティ処理の簡便化
		通信資源の利用効率向上
		通信の高速化
		更新処理の簡略化
		トラフィックの軽減
		ネットワーク規模の拡大
		時間誤差、輻輳の防止
中継するデータの機密性向上	使い易いセキュア通信の確立	秘匿処理の簡便化
		VPN 設定の容易化
		VPN 設定の不整合防止
		障害時の SA の再確立
	機密性の適用範囲の拡大	経路毎の機密性向上
		機密性の喪失防止
		複数層への拡大
		NAT を使用する VPN 網
		秘匿処理の一元化
	暗号技術の強度向上	鍵の安全な配布
		不正解析の防止
		復号の正確性向上
	暗号処理の効率化	鍵管理の容易化
		動作不安定の防止
		パケット遅延の減少
		復号処理の容易化
		鍵交換回数の軽減

表 1.4-1 不正アクセス侵入検知防御技術に関する技術開発課題(3/4)

課題 I	課題 II	課題III
侵入検出の性能向上	未知攻撃検出の精度向上	攻撃元特定の正確化
		侵入経路の探求
		分析アルゴリズムによる特定
		不正操作の痕跡追求
	攻撃検出の精度向上	振る舞いの再現化
		踏み台に成った如くで対応
		検出器の精度向上
		不正アクセスの精度向上
		最新パターンの確保
		ビジブル化による判定の支援
		コネクションレスパケットの対応
		再送要求の詐称
		欺瞞パケット防止
	侵入検出処理の効率化	検出処理時間の短縮
		許容範囲の適正化
攻撃パターンの高精度化	資源消耗さす攻撃パターンの精度向上	過負荷攻撃の耐性向上
		同時複数攻撃からの防御
		バッファのオーバフローの防止
		帯域浪費の防止
	プログラム脆弱部からの攻撃パターンの精度向上	脆弱部の抽出性能向上
		自由アプリ脆弱部のパターン
		サブルーチン脆弱部のパターン
		バックドアの探索
	プログラムを利用する攻撃パターンの精度向上	オブジェクトのメソッドによる詐称
		エージェントによる詐称
		踏み台による詐称
		テストに託けた詐称
	機能停止をさせる攻撃パターンの精度向上	応答コマンドの正当性
		フォーマット異常の攻撃パターン
		無応答攻撃パターン
	攻撃パターン生成の効率化	更新処理の安全性向上
		生成時間の短縮
		生成処理の簡便化
情報、個人の正当性向上	情報の原本性向上	情報の改ざん防止
		送信先での改ざん防止
	個人認証による疎通化	パスワードの成済ましの防止
		ユーザーID の成りすましの防止
		パスワード、ID の強度向上
	通信データの正当性	証明書の正当性
		パケットの正当性
攻撃の抑止・予防の強化	新たな攻撃の予防	攻撃防御の迅速化
		二次感染の防止
		ブラックリストの衆知化
		パッチ操作の徹底
		手掛かり情報の撲滅
	速やかな攻撃からの回避	物理的に完全な回避
		不具合時の遮蔽方法
		回避処理時間の短縮

表 1.4-1 不正アクセス侵入検知防御技術に関する技術開発課題(4/4)

課題 I	課題 II	課題III
パケット解析の高精度化	パケット採取の適切化	蓋然性パケットの確保
		採取タイミングの適正化
		採取ログの適正化
		採取の見破り防止
	解析処理の効率化	ログ情報量の削減化
		診断精度の向上
		ログ情報の利用し易い形態
		解析時間の短縮
		ログ解析の支援
経済性の向上	装置コストの低減	ファイアウォールのコストダウン
		メモリの削減
	費用の低減	認証管理費用の低減
		通信費用の低減
		運用費用の低減

一方、このような課題を解決するために開発された解決手段を、表1.4-2に示す。解決手段Ⅰ、解決手段Ⅱ、解決手段Ⅲ、解決手段Ⅳの4階層に分けられている。

表1.4-2不正アクセス侵入検知防御技術の技術開発課題に対する解決手段(1/4)

解決手段 I	解決手段 II	解決手段III	解決手段IV
手順の改良	各種の処理手順改良	特定情報の記憶、登録手順	認証情報の記憶
			鍵情報の記憶
			アドレスの記憶
			ログ情報の記憶
			設定情報の記憶
			要求情報の記憶
		プロトコルの処理手順	プロトコル変換
			プロトコル切換
			多層プロトコルの処理
			プロトコル併用
			プロトコルの照合
			UDP の活用
		応答コマンドの処理手順	応答コマンドを要求コマンド
			応答情報の検証
			応答情報の無返却、制限
			応答コマンドにデータ添付
		各種処理の実行手順	特定情報の表示
			特定処理の実行
			並列処理の実行
			パターン、ルールの言語記述
		特定情報の取得手順	ステータスの取得
			ID 情報の取得
			アドレスの取得
			設定情報の取得

表1.4-2不正アクセス侵入検知防御技術の技術開発課題に対する解決手段(2/4)

解決手段 I	解決手段 II	解決手段III	解決手段IV
手順の改良	情報の照合、検索、カウント手順改良	特定情報の照合手順	ワンタイム ID
			認証情報の照合
			時間・期間情報
			ログ履歴情報の照合
			アドレスの照合
			識別子情報の照合
			順番号の検証
		特定情報の検索、抽出手順	メッセージの内容検索
			経路、中継サーバ
			遠隔制御コマンドの抽出
			アドレスの検索
		特定情報のカウント手順	エラー
			トラフィック
			パケット
			アクセス、セッション回数
			パケットのフィールド
			コマンド
			送信回数
			使用回数
	情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	警告情報
			鍵情報の送信
			擬似、ダミデータの送信
			障害情報の通知
			識別子、認証情報の送信
			更新差分情報の送信
			攻撃情報の通知
			アクセス許可情報
		情報転送の手順	ポリシ設定情報
			プログラム、スクリプト
			VPN 設定情報
			パターンのダウンロード
		設定値で分岐の手順	セキュリティレベル
			トラフィックの頻度、増加率
			ある閾値で分岐
			容疑レベル、悪性閾値
			送信方向
新たなシステムの配置	ファイアウォール内のシステム構成	イントラネット内に機器の配置	位置識別子の配置
			複数ファイアウォールの配置
			記憶領域の分割配置
			エージェントの配置
			バックアップサーバーの配置
			メモリの配置
			機器、モジュール配置
		DMZ に機器の配置	中継サーバの配置
			攻撃解析サーバーの配置
			情報提供サーバーの配置
			監視装置の配置
			収集器の配置

表 1.4-2 不正アクセス侵入検知防御技術の技術開発課題に対する解決手段(3/4)

解決手段 I	解決手段 II	解決手段III	解決手段IV
新たなシステムの配置	ファイアウォール外のシステム構成	セキュリティサーバーの配置	認証サーバーの配置
			ポリシサーバーの配置
			暗号処理サーバーの配置
			エッジノードにファイアウォール機能の分割配置
			アクセス制御サーバ配置
		サービスサーバーの配置	プロキシサーバーの配置
			メールサーバーの配置
			チェックサーバー配置
			DNS、DHCP サーバー配置
			仲介サーバー配置
データ構造の改良	アクセステーブルの改良	アプリケーションとの関連付け	ユーザー・グループ
			ファイル
			リソース
			業務・商品情報
			ゾーン
		アクセスルールとの関連付け	マシン・ホスト
			アドレス、ポート番号
			オブジェクトとサブジェクト
			時間、期限情報
			通信路
			役割の属性値
		認証情報との関連付け	ID 認証情報
			許可証明書
			鍵情報
	フィルタテーブルの改良	攻撃元アドレスの追加	IP アドレスの設定
			属性付与し登録
			ポート番号の登録
			自動登録
			IP アドレスの削除
		フイルタの追加	フィルタの付加
			フィルタのダウンロード
			フィルタの学習
		ポリシルールの追加、切換	ポリシルールの切換
			ポリシルールの追加、学習
			質問形式での追加、学習
			ポリシの削除
	パターンデータベースの改良	攻撃パターンの追加、切換	攻撃属性別パターンの追加
			アラートパターンの追加
			異常出現頻度パターンの追加
			パターンの廃棄
			パターンの切換
		攻撃情報の蓄積	不正アクセス履歴情報の蓄積
			ログ情報の蓄積
			ポートスキャン蓄積
			リターンアドレス蓄積
		攻撃パターンの学習	トラフィックデータの学習
			振舞い形式の学習
			特徴単語の学習
			HTTP の学習
		分析アルゴリズムの改良	脆弱度の算出
			類似度、相関度の算出
			各種アルゴリズムの改良
			帯域制限値の算出

表 1.4-2 不正アクセス侵入検知防御技術の技術開発課題に対する解決手段(4/4)

解決手段 I	解決手段 II	解決手段III	解決手段IV
データ形式の改良	データ形式の改良	データに情報付加	ヘッダに認証情報
			ヘッダに情報付加
			電子署名の付加
			ハッシュ値の付加
			タイムスタンプの付加
			コマンドに情報付加
			更新情報の付加
			電子透かしの埋め込み
			クッキに情報付加
		データの変換	データの暗号化
			データの分割、仕分け
			認証情報の変換
			フォーマットの変換
			鍵情報のパック化
			ペイロードの暗号化
			可変鍵の付加
			識別子情報の変換
			多重符号化で変換
			中間コードに変換
			データの圧縮化
		オブジェクトのデータ形式改良	パケットオブジェクトモデル
			オブジェクに認証情報埋め込み
			セキュリティオブジェクトモデル
			ポリシオブジェクトモデル
	アドレスデータ形式の改良	アドレスの変換	IP アドレスの変換
			パックアドレス
			URL ドメインの変換
			アドレスの暗号化
			ポート番号、NAT の変換
			情報の付加
		IP アドレスの割付	ポート番号の割付
			ソケットの割付
			IPv6 の割付
			相対アドレスの割付
			リダイレクトアドレスの割付
			ポート番号の停止、取消し
回路の改良	回路の改良	スイッチ回路の追加	回路の切換
			通信遮断回路
			専用線の活用
			ロック回路の追加
			複数通信路の配置
			無線との切換
		処理回路の改良	フィルタリング回路の改良
			プログラマブル素子の暗号回路
			同一チップ内のバス回路

1.4.1 不正アクセス侵入検知防御技術の技術要素と課題、および課題と解決手段

(1) 技術要素と課題

図1.4.1-1に、不正アクセス侵入検知防御技術の技術要素に対する課題の分布を示す。不正アクセス侵入検知防御技術の課題として、「侵入防御の性能向上」、「利用サービスの保護強化」、「デバイスの正当性向上」と「通信データの中継性能向上」が、300件前後の件数で多い。次いで「システムの性能向上」、「中継するデータの機密性向上」とする課題が200件強で続いている。

技術要素別に課題をみると、侵入検知解析技術では、「システムの性能向上」、「侵入検出の性能向上」と「攻撃パターンの高精度化」等の課題が、100件前後で分散している。アプリケーション中継技術は、「利用サービスの保護強化」の課題に集中しており、直近３年の出願が多い。パケットフィルタリング技術では、「侵入防御の性能向上」の課題に集中しており、直近３年の出願が多い。ホスト認証技術は、「デバイスの正当性向上」の課題に集中しており、出願は安定している。トンネリング技術は、「中継するデータの機密性向上」の課題に集中し、３年以上前の出願が多い。

図1.4.1-1 不正アクセス侵入検知防御技術の技術要素に対する課題の分布

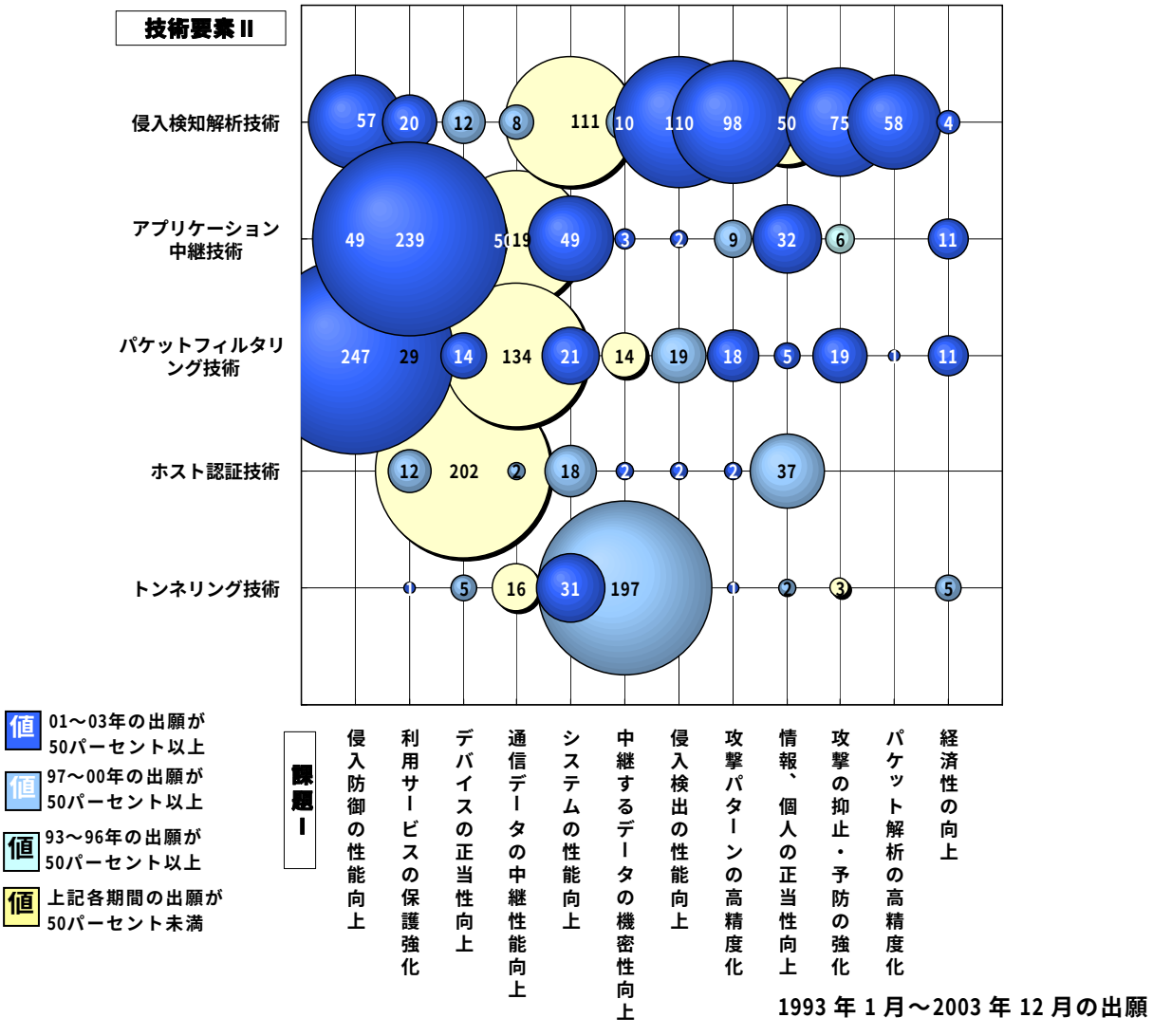


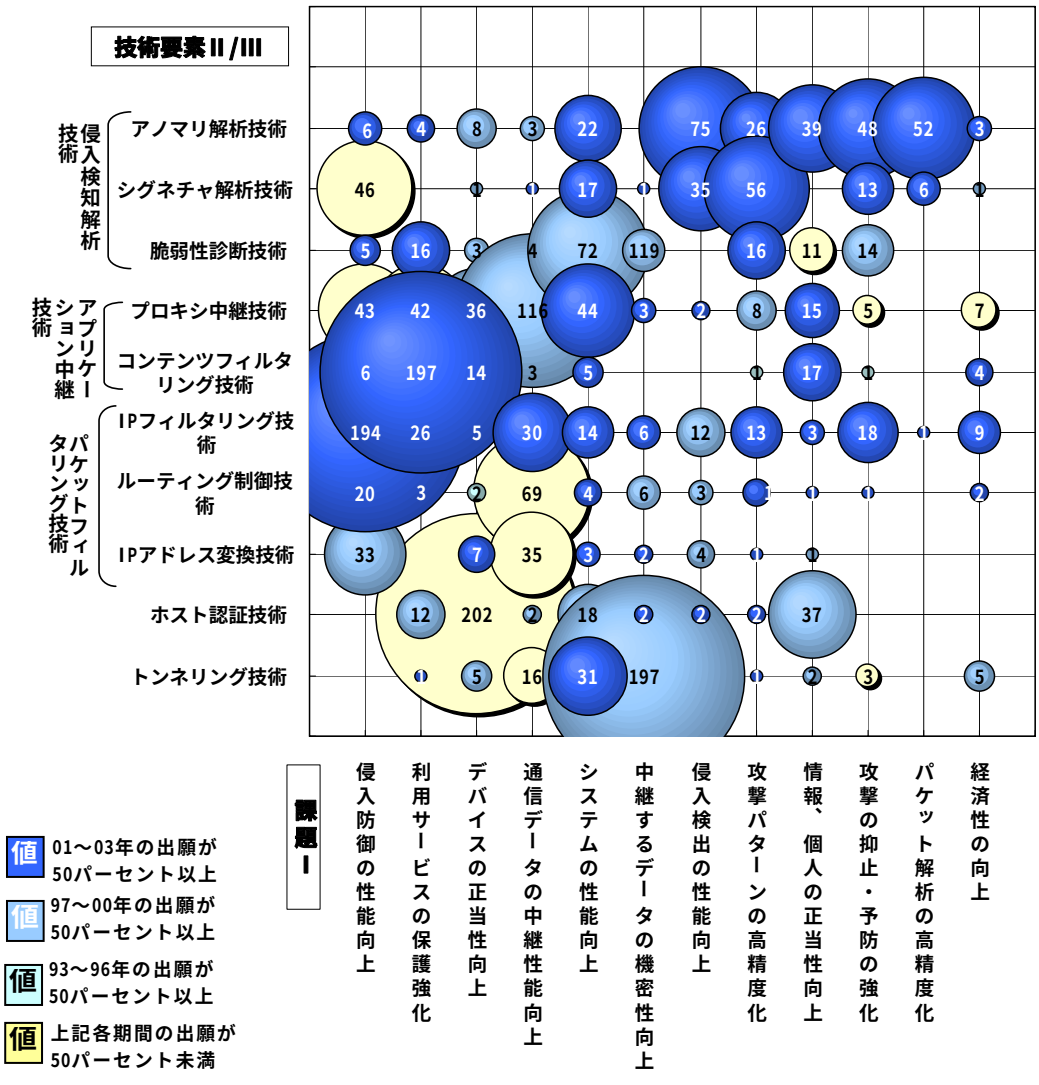
図1.4.1-2に、不正アクセス侵入検知防御技術の技術要素に対する課題の分布(詳細)を示す。これは、侵入検知解析技術、アプリケーション中継技術とパケットフィルタリング技術を詳細な技術要素にして、課題の分布を示したものである。

侵入検知解析技術のうち、アノマリ解析技術では、「侵入検出の性能向上」、「パケット解析の高精度化」や「攻撃の抑止・予防の強化」の課題が多い。シグネチャ解析技術では、「攻撃パターンの高精度化」や「侵入防御の性能向上」の課題に集中している。脆弱性診断技術では、「システムの性能向上」の課題に集中し、３年以上前の出願が多い。

アプリケーション中継技術のうち、プロキシ中継技術では、「通信データ中継性能向上」に集中し、３年以上前の出願が多い。コンテンツフィルタリング技術では、「利用サービスの保護強化」の課題に集中し、直近３年の出願が多い。

パケットフィルタリング技術のうち、IPフィルタリング技術では、「侵入防御の性能向上」に集中し、直近３年の出願が多い。ルーティング制御技術では、「通信データの中継性能向上」に集中している。

図1.4.1-2 不正アクセス侵入検知防御技術の技術要素に対する課題の分布(詳細)



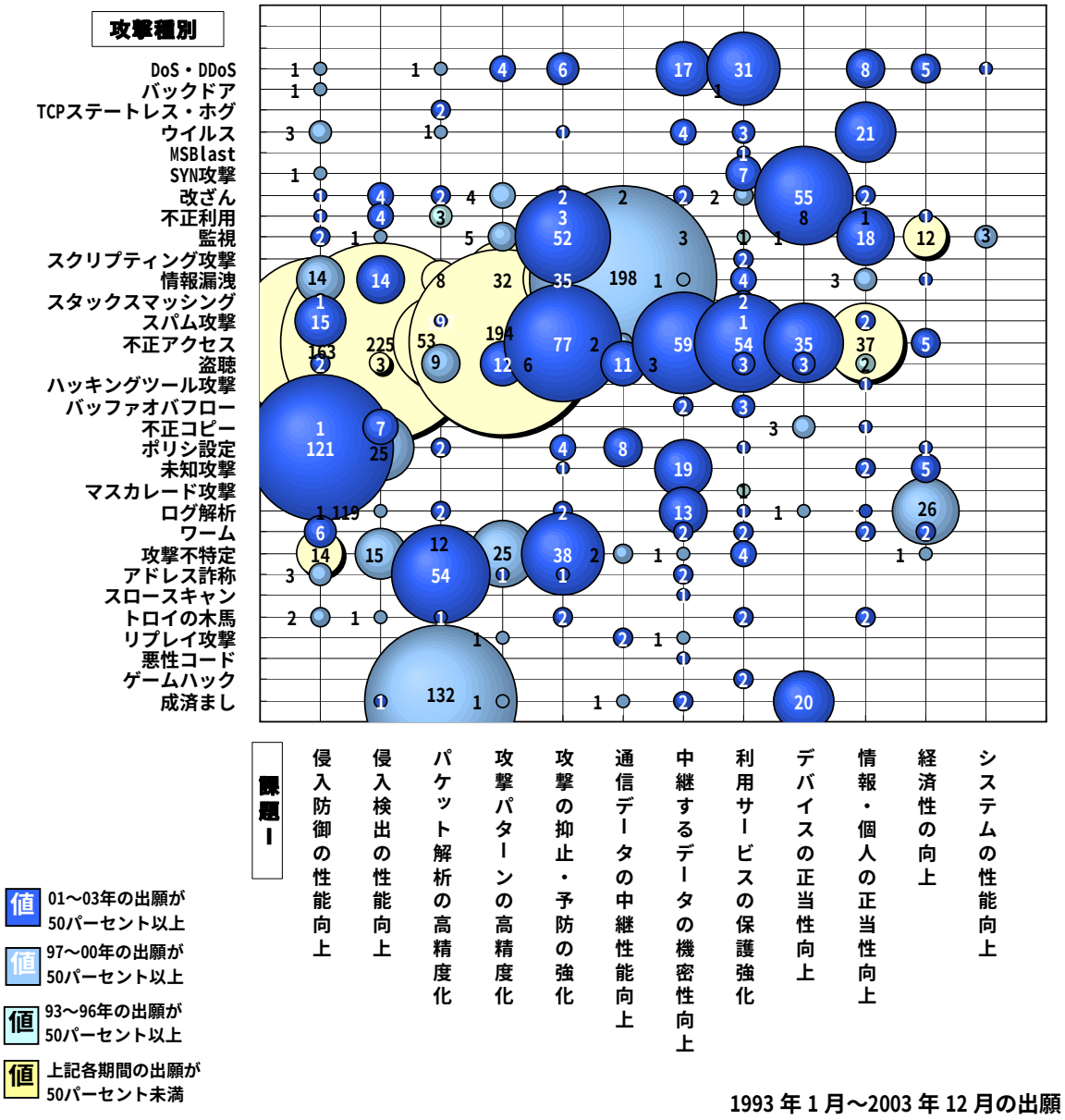
1993年1月～2003年12月の出願

(2) 攻撃種別と課題

図1.4.1-3に不正アクセス侵入検知防御技術の攻撃種別に対する課題の分布を示す。攻撃種別は、不正アクセスが最も多くほぼ900件、次いで情報漏洩が300件、成済ましやポリシ設定が160件、監視や攻撃不特定が100件、DoS・DDoSや改ざんやアドレス詐称が70件である。

課題別にみると攻撃種別は集中しているのが特徴である。具体的に、侵入検出の性能向上に対して「不正アクセス」攻撃に関するものが最も集中し、次いで通信データの中継性能向上に対して「情報漏洩」の攻撃に関するものが集中している。さらに、侵入防御の性能向上に対して「不正アクセス」攻撃に関するものも集中している。パケット解析の高精度化に対して「成済まし」攻撃に関するものも集中している。

図1.4.1-3不正アクセス侵入検知防御技術の攻撃種別に対する課題の分布



(3) 課題と解決手段

図1.4.1-4に、不正アクセス侵入検知防御技術の課題に対する解決手段の分布を示す。課題も解決手段も昇順に並べて示している。

「侵入防御の性能向上」の課題では、「データ構造の改良」で対応するものが最も多く、直近の３年の出願が多く、次いで「手順の改良」で対応するものが多い。

「利用サービスの保護強化」の課題では、「データ構造の改良」で対応するものが最も多く、平均化された安定した出願である。

「デバイスの正当性向上」の課題では、「手順の改良」で対応するものが最も多く、３年以上前に出願が多いものである。

「通信データの中継性能向上」の課題では、「手順の改良」で対応するものが最も多く、３年以上前に出願が多いものである。

「システムの性能向上」の課題では、「手順の改良」で対応するものが最も多く、直近の３年の出願が多い。

「中継するデータの機密性向上」の課題では、「データ形式の改良」で対応するものが最も多く、３年以上前に出願が多いものである。

図1.4.1-4不正アクセス侵入検知防御技術の課題に対する解決手段の分布

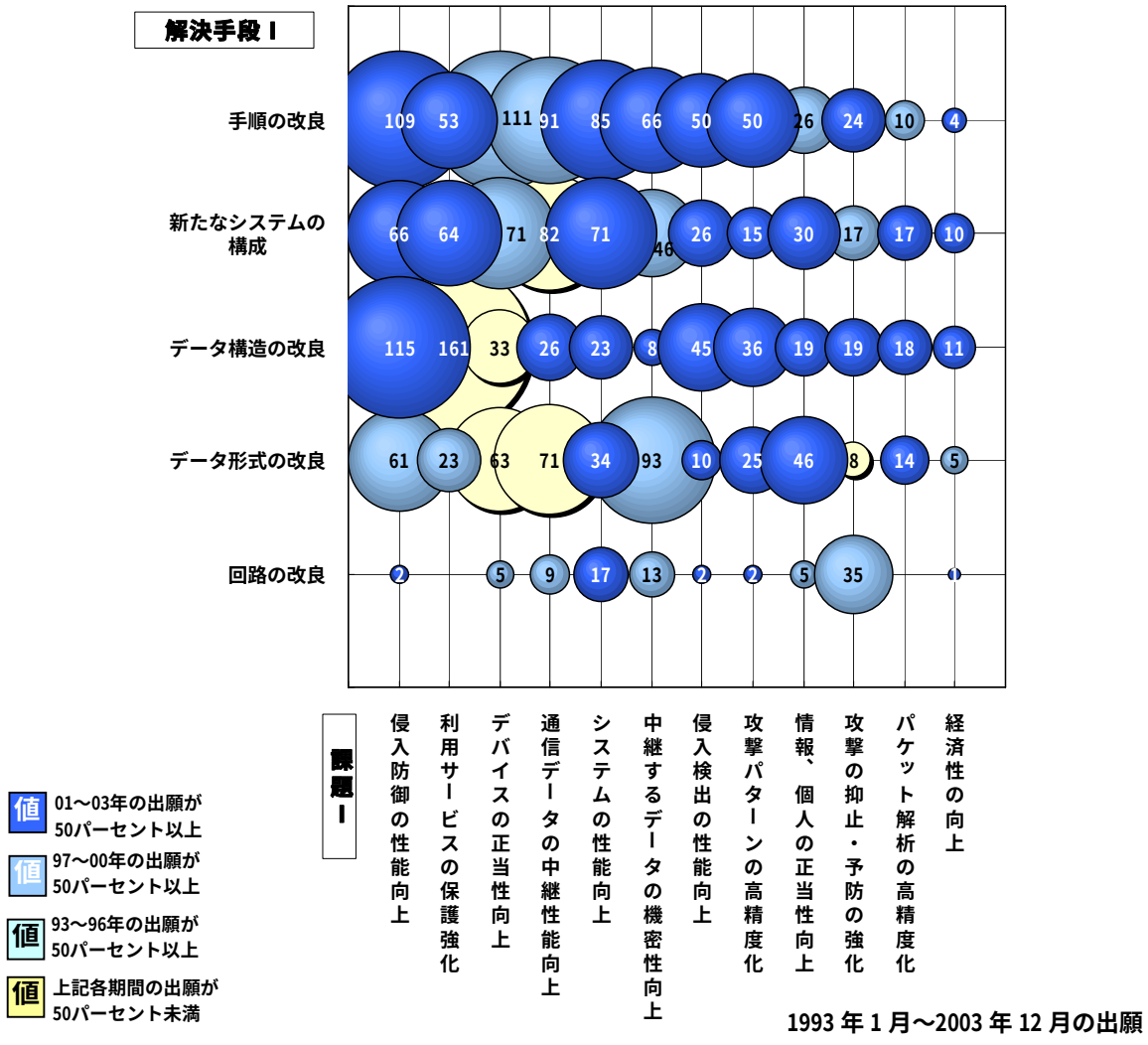


図1.4.1-5に、不正アクセス侵入検知防御技術の課題に対するさらに詳しい解決手段を示す。これは課題に対する詳細な解決手段の分布を示したものである。

課題別にみると、利用サービスの保護強化に対する解決手段は、「アクセステーブルの改良」に最も集中している。中継するデータの機密性向上に対する解決手段は、「データ形式の改良」が多い。なお、データ形式の改良を解決手段とする出願は、1997年～2000年で50%以上の出願となっており、最近の出願が少ない。

侵入防御の性能向上に対する解決手段は、「フィルタテーブルの改良」が多い。次いで「情報の送信、転送、分岐の手順改良」が多い。フィルタテーブルの改良や情報の送信、転送、分岐の手順改良を解決手段とする出願は、01年～03年で50%以上の出願となっており、最近の出願が多くなっている。

通信データの中継性能向上に対する解決手段は、「各種の処理手順の改良」が多く、次いで「ファイアウォール内のシステム構成」が多い。各種の処理手順の改良を解決手段とする出願は、97年～2000年で50%以上となっており、最近の出願が少ない。

デバイスの正当性向上に対する解決手段は、「ファイアウォール外のシステム構成」、「情報の照合、検索、カウント手順改良」、「各種の処理手順の改良」や「データ形式の改良」に分散している。これらの解決手段の出願は、97年～2000年で50%以上の出願となっており、最近の出願が少ない。

図1.4.1-5不正アクセス侵入検知防御技術の課題に対する解決手段の分布（詳細）

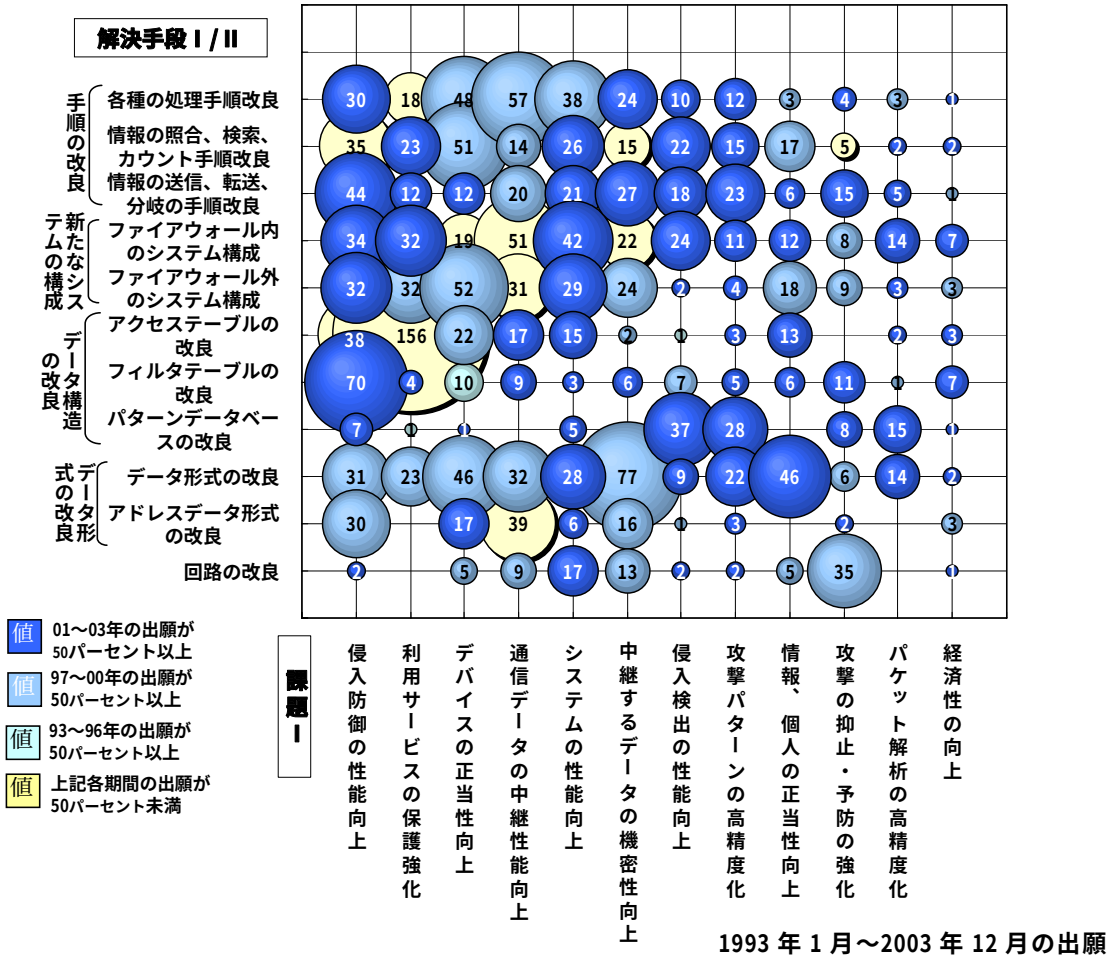


図1.4.1-6に不正アクセス侵入検知防御技術の課題に対する解決手段の分布(最近３年分)を、図1.4.1-7に不正アクセス侵入検知防御技術の課題に対する解決手段の分布(前８年分)を示す。

２つの図を比較して、前８年分で多数の出願が行われていて、引き続き最近３年も多数の出願が行われている主なものは以下の通りである。

・中継するデータの機密性向上に対して､｢データ形式の改良｣で対応している出願

・デバイスの正当性向上に対して、｢ファイアウォール外の新たなシステム構成｣、｢情報の照合、検索、カウント手順改良｣、｢各種の処理手順の改良｣と｢データ形式の改良｣で対応している出願

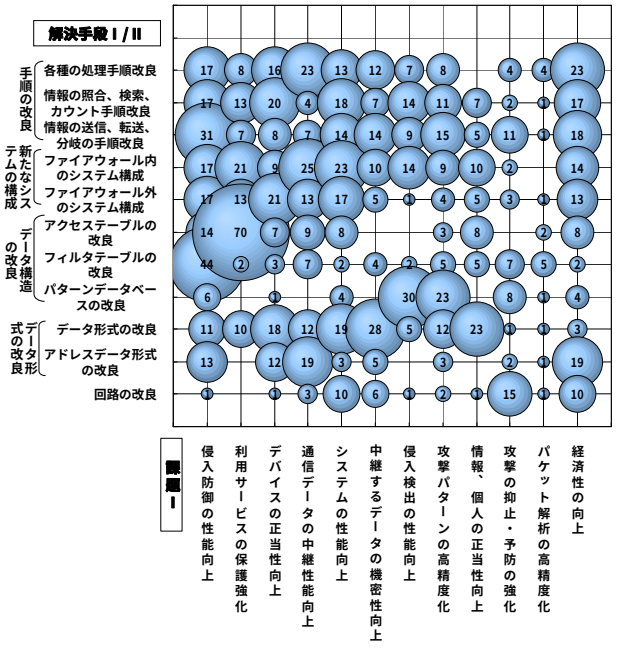
２つの図を比較して、前８年分で多数の出願が行われていたものは、以下の通りである。

・ 侵入防御の性能向上に対して、｢情報の照合、検索、カウント手順改良｣と｢フィルタテーブルの改良｣で対応している出願

・ 侵入検出の性能向上に対して、｢パターンデータベースの改良｣で対応している出願

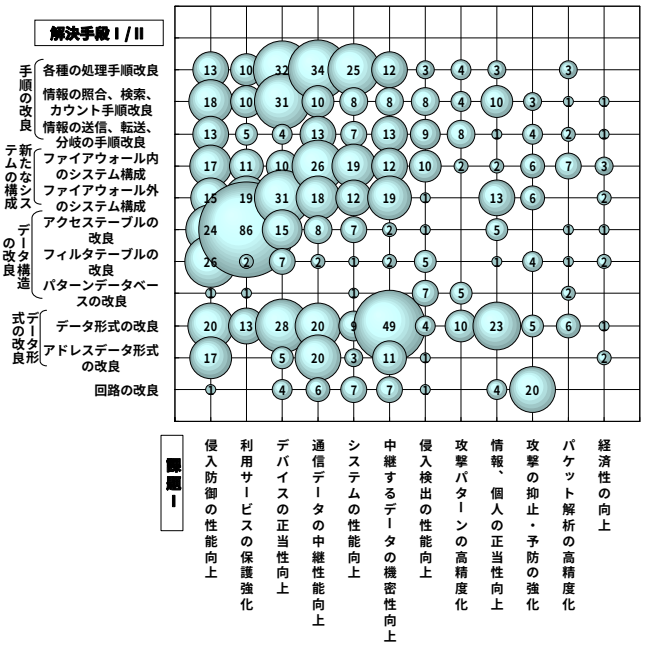
・ 攻撃パターンの高精度化に対して、｢パターンデータベースの改良｣で対応している出願

図 1.4.1-6 不正アクセス侵入検知防御技術の課題に対する解決手段の分布(最近３年分)



2001 年 1 月～2003 年 12 月の出願

図 1.4.1-7 不正アクセス侵入検知防御技術の課題に対する解決手段の分布(前８年分)



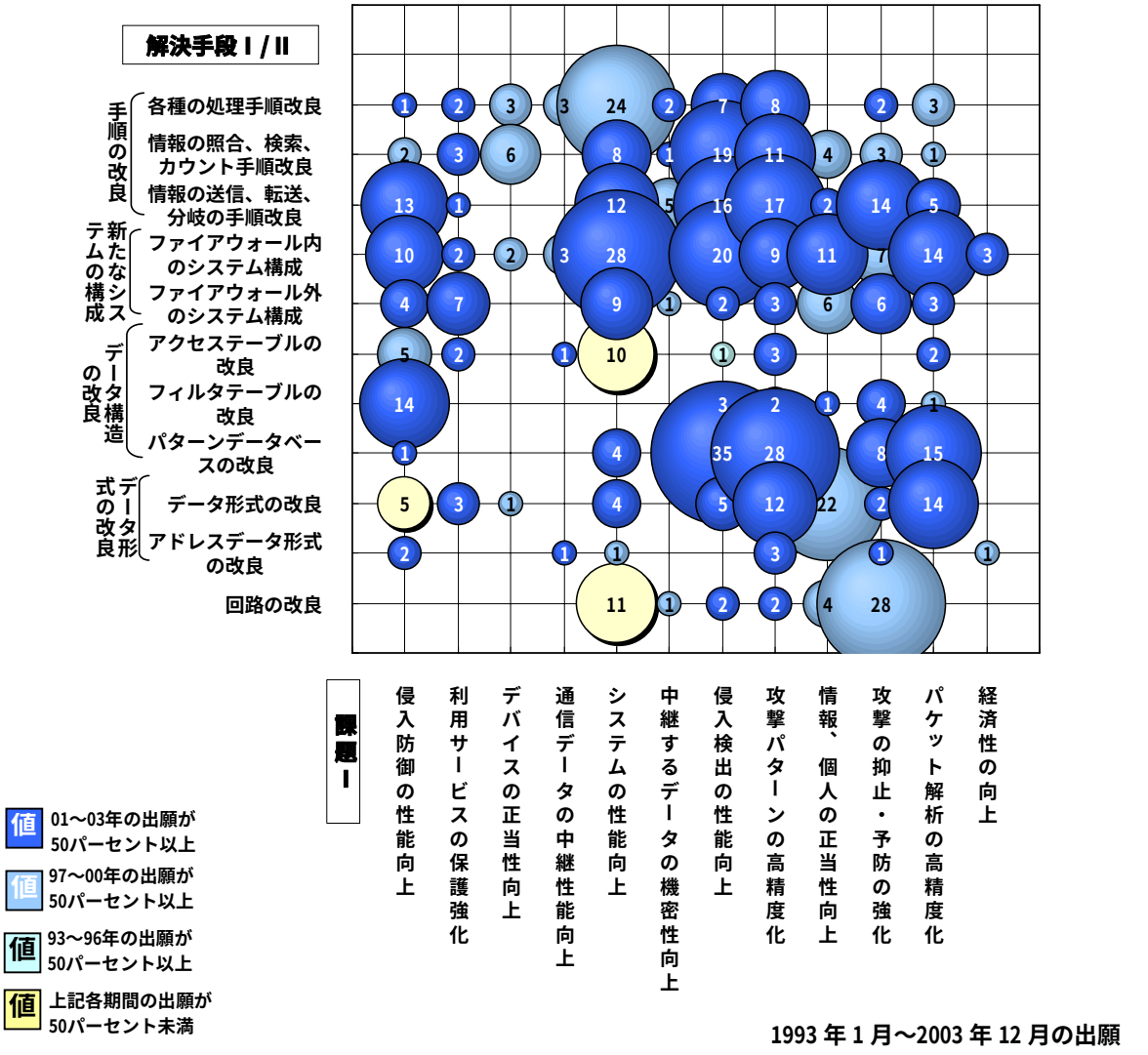
1993 年 1 月～2000 年 12 月の出願

1.4.2 侵入検知解析技術の課題に対する解決手段

図1.4.2-1に侵入検知解析技術の課題に対する解決手段の分布を示す。侵入検知解析技術において、多い課題は、「侵入検出の性能向上」で、次いで「攻撃パターンの高精度化」であり、さらに「システムの性能向上」となっている。

侵入検出の性能向上に対しては、「パターンデータベースの改良」で最も多く対応し、次いで攻撃パターンの高精度化に対しても「パターンデータベースの改良」で多く対応している。これらは、直近３年の出願が多い。システムの性能向上に対しては「ファイアウォール内のシステム構成」で対応して、直近３年の出願が多い。攻撃の抑止・予防強化に対しては「回路の改良」で対応して、3年以上前の出願が多い。

図1.4.2-1 侵入検知解析技術の課題に対する解決手段の分布



次に侵入検知解析技術をアノマリ解析技術、シグネチャ解析技術、脆弱性診断技術に分けて、技術ごとの課題に対する出願人の分布を示す。

(1) アノマリ解析技術

図1.4.2-2にアノマリ解析技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「侵入検出の性能向上」で、次いで「パケット解析の高精度化」である。

情報、個人の正当性向上に対して「データ形式の改良」で多く対応し、３年以上前の出願が多い。次いで侵入検出の性能向上に対しては、「パターンデータベースの改良」や「情報の照合、検索、カウント手順改良」や「ファイアウォール内のシステム構成」で対応し、さらに攻撃の抑止・予防の強化に対しては「回路の改良」で対応しているものが多く、どれも直近３年の出願が多いものである。

図1.4.2-2 アノマリ解析技術の課題に対する解決手段の分布

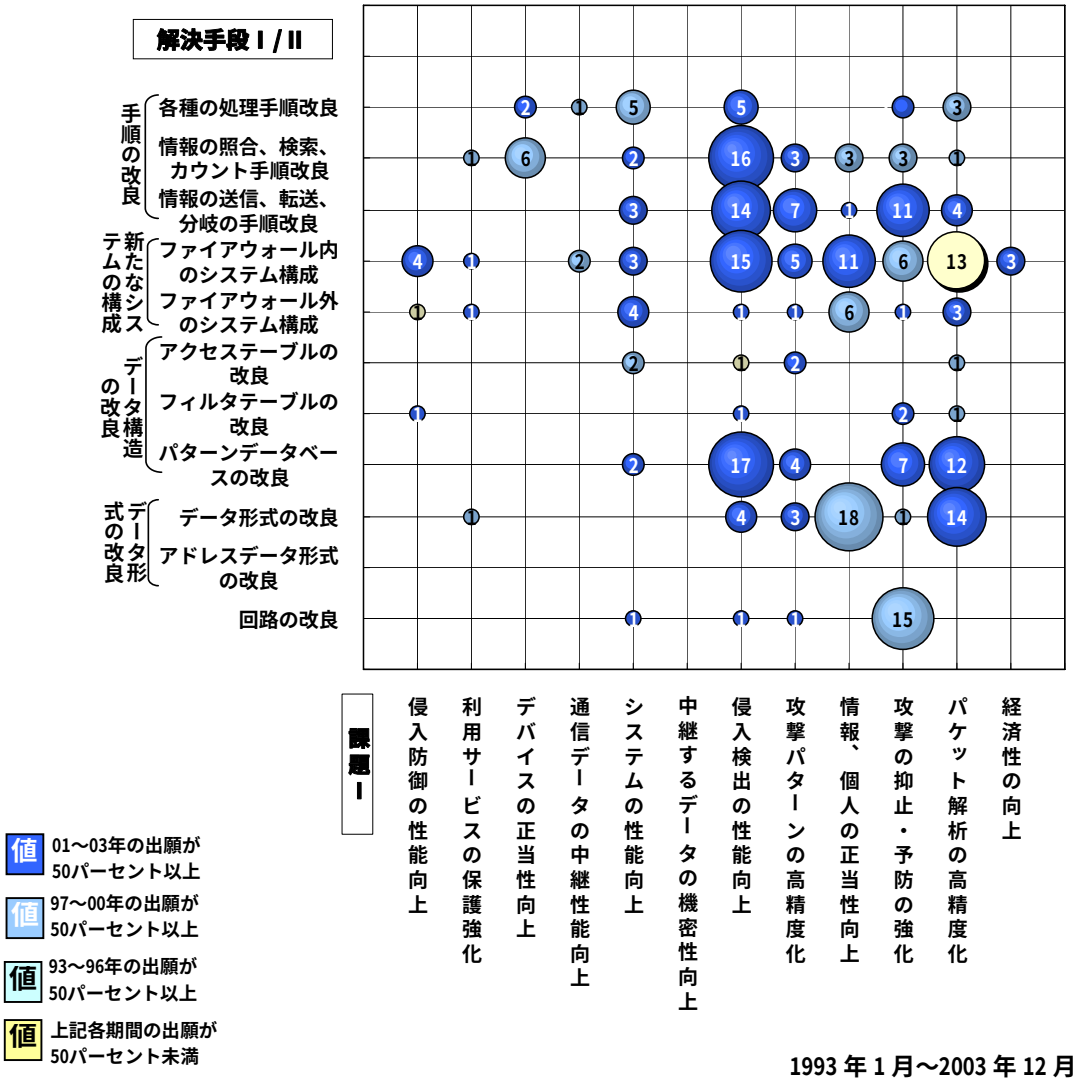


表1.4.2-1にアノマリ解析技術の課題に対する解決手段の詳細を示す。出願の多い課題は、侵入検出の性能向上の「未知攻撃検出の精度向上」と、情報・個人の正当性向上の「情報の原本性向上」と、攻撃の抑止・予防の強化の「新たな攻撃の予防」と、パケット解析の高精度化の「パケット採取の適切化」である。情報の原本性向上に対して、「データに情報付加」や「イントラネット内に機器の配置」で多く対応し、新たな攻撃の予防に対して「特定情報の通知・送信手順の改良」で多く対応している。

表1.4.2-1 アノマリ解析技術の課題に対する解決手段の詳細

課題 I / 課題 II / 解決手段 II	III	侵入防御の性能向上			サービス利用保護の強化		デバイスの正当性向上	データの中継性能向上		システムの性能向上		侵入検出の性能向上			攻撃パターンの高精度化					情報、個人の正当性向上		攻撃の抑止・予防の強化		パケット解析の高精度化		経済性の向上	
		アドレスフィルタの強化	フィルタルール適用の整合性	プロトコルフィルタの強化	リソース保護の強化	アクセス管理の効率化	成済ましの防止	アプリケーション層の中継機能拡大	トランスポート層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	未知攻撃検出の精度向上	攻撃検出の精度向上	侵入検出処理の効率化	資源消耗させる攻撃パターンの精度向上	プログラム脆弱部からの攻撃パターンの精度向上	プログラムを利用する攻撃パターンの精度向	機能停止をさせる攻撃パターンの精度向上	攻撃パターン生成の効率化	情報の原本性向上	個人認証による疎通化	新たな攻撃の予防	速やかな攻撃からの回避	パケット採取の適切化	解析処理の効率化	装置コストの低減	費用の低減
各種の処理手順改良	特定情報の記憶、登録手順												1											3			
	応答コマンドの処理手順						1	1				1										1					
	各種処理の実行手順									1		1	2									1					
	特定情報の取得手順						1			1	3	1															
情報の照合、検索、カウント手順改良	特定情報の照合手順					1	4					6	3							1	2	2		1			
	特定情報の検索、抽出手順						1					5										1					
	特定情報のカウント手順						1				2	1	1		3												
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順									2		4				2						10					
	情報転送の手順																			1					1		
	設定値で分岐の手順										1	4	5	1	3	1		1				1		1	2		
ファイアウォール内のシステム構成	イントラネット内に機器の配置				1			1	1		2	2								11		1	4	1	1		1
	DMZ に機器の配置	3		1							1	6	6	1	1	3		1				1		4	7	1	1
ファイアウォール外のシステム構成	セキュリティサーバーの配置		1							1	2							1		2	1	1			1		
	サービスサーバーの配置					1				1		1								3				1	1		
アクセステーブルの改良	アプリケーションとの関連付け									1																	
	アクセスルールとの関連付け									1		1			1		1								1		
フィルタテーブルの改良	攻撃元アドレスの追加																					2		1			
	ポリシルールの追加、切換	1										1															
パターンデータベースの改良	攻撃パターンの追加、切換											6	2		1	1						5		2	2		
	攻撃情報の蓄積									1		1				1								6			
	攻撃パターンの学習											2	3						1								
	分析アルゴリズムの改良										1	2	1										2	2			
データ形式の改良	データに情報付加											3			2					17		1		3	4		
	データの変換																1			1				2	5		
	オブジェクトのデータ形式改良				1							1															
回路の改良	スイッチ回路の追加									1		1			1							4	11				

1993 年 1 月～2003 年 12 月の出願

表1.4.2-2にアノマリ解析技術の課題に対する解決手段の出願人を示す。出願が最も多い情報、個人の正当性向上の具体的な課題「情報の原本性向上」に対する「データに情報の付加」に関しては、NTTと日立製作所が各３件、米国のIBMが２件と出願している。その他は各１件の出願であるが、大手企業である。

表1.4.2-2 アノマリ解析技術の課題に対する解決手段の出願人(1/4)

課題I / 課題II / 解決手段II III		侵入検出の性能向上 未知攻撃検出の精度向上	情報、個人の正当性向上 情報の原本性向上	攻撃の抑止・予防の強化 新たな攻撃の予防	パケット解析の高精度化 パケット採取の適切化
各種の処理手順改良	特定情報の記憶、登録手順				日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特許 3541872 日立製作所 特許 3537018 野村ﾎｰﾙﾃﾞｨﾝｸﾞｽ,野村総合研究所(共願) 特開 2002-041359
	応答コマンドの処理手順	東芝　特開 2003-173300		ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ,ｻｲﾊﾞｰｿﾘｭｰｼｮﾝｽﾞ(共願) 特開 2003-309607	
	各種処理の実行手順	東芝　特開 2004-274481		三菱電機　,三菱電機情報ﾈｯﾄﾜｰｸ(共願) 特開 2004-234208	
情報の照合、検索、カウント手順改良	特定情報の照合手順	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ 特開 2003-032252 ﾗｲﾌ技術研究所 特開 2001-005781 横河電機 特開 2004-120695 日本電気 特開 2003-006185 日立製作所 特開 2000-354036 野村総合研究所 特開 2004-213476	日本電気 特開 2002-176455	横河電機 特開 2003-304289 溝口 文雄 特開 2002-135248	宇宙航空研究開発機構,科学技術振興機構(共願)　特許 2945938
	特定情報の検索、抽出手順	ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ 特許 3483782 横河電機 特開 2003-298652 三菱電機 特開 2003-258910 富士通 (2) 特開 2002-342279 特開 2004-280724		日本電信電話 特許 3549861	
	特定情報のカウント手順	ｲﾝﾃﾘｼﾞｴﾝﾄ･ｺｽﾓｽ研究機構 特開 2005-094361			
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	ｶｼｵ計算機 特開 2004-159117 科学技術振興機構 特開 2003-288227 山武　特開 2003-309608 東芝　特開 2004-146931		NEC ﾌｨｰﾙﾃﾞｨﾝｸﾞ 特開 2005-122251 ｵﾑﾛﾝ　特開 2004-180048 ｷﾔﾉﾝ (2) 特開 2004-005030 特開 2004-265310 ｾｺﾑ上信越 特開 2005-109847 横河電機 特開 2004-005147 日本電信電話 特開 2004-320453 日立製作所 (3) 特開平 08-212164 特開平 09-269930 特開平 11-134190	

1993 年 1 月～2003 年 12 月の出願

表 1.4.2-2 アノマリ解析技術の課題に対する解決手段の出願人(2/4)

解決手段II / 課題II / 課題I		未知攻撃検出の精度向上 侵入検出の性能向上	情報の原本性向上 情報、個人の正当性向上	新たな攻撃の予防 攻撃の抑止・予防の強化	パケット採取の適切化 パケット解析の高精度化
情報の送信、転送、分岐の手順改良	情報転送の手順		ｺﾆｶﾐﾉﾙﾀﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2004-362385		
	設定値で分岐の手順	ﾄｯﾌﾟ ﾚｲﾔｰ ﾈｯﾄﾜｰｸｽ(米国) 特表 2004-507978 三菱電機 特開 2001-094602 日本電気 特開 2003-337797 日本電信電話 特開 2005-159551		日立製作所 特開 2004-246444	日本電気 特許 3225919
ファイアウォール内のシステム構成	イントラネット内に機器の配置	ﾄﾗｲｵﾌﾟｽ(韓国) 特表 2004-520654 三菱電機 特開 2003-076662	ｱｲｴｽｴｲ 特開 2003-076610 ｽｶﾗﾍﾞ・ｺｰﾎﾟﾚｰｼｮﾝ,高野直人(共願) 特開 2002-244941 ﾘﾝｸ 特開 2003-067253 高 振宇 特開 2002-175010 西谷 正,ｳｴｽﾀﾝ･ﾃｸﾉﾛｼﾞｰ(共願) 特開 2004-078860 日本電気 特開 2004-185182 日本電気 ,NEC ｿﾌﾄ(共願) 特開 2003-196141 日本電信電話 特開 2002-215583 日立国際電気 特開 2003-167786 富士通 特許 3484523 六舜実業股分(台湾) 特開 2004-078265	ｷﾈﾃｯｸ(ｲｷﾞﾘｽ) 特表 2004-518193	横河電機 特開 2002-111667
	DMZ に機器の配置	ｼﾞｪﾝｽﾞ 特開 2004-153485 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特開 2002-026907 横河電機 特開 2005-175993 三菱電機(2) 特開 2002-199024 特開 2004-328307 中部日本電気ｿﾌﾄｳｪｱ 特開 2002-041468		日本電気 特開 2003-162423	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2002-344519 ｻｲﾚﾝﾄﾗﾝﾅｰ (米国) 特表 2002-521748 沖電気工業 特開 2004-145687 資訊工業策進会(台湾) 特開 2002-073553
ファイアウォール外のシステム構成	セキュリティサーバーの配置		ﾌﾞﾚｲﾝｷｬｽﾄ,大岡 歩夢(共願) 特開 2002-044075 亜細亜証券印刷 ,ｼﾅｼﾞｰｲﾝｷｭﾍﾞｰﾄ(共願) 特開 2002-024177	松下電器産業 特開 2005-182311	

1993 年 1 月～2003 年 12 月の出願

表 1.4.2-2 アノマリ解析技術の課題に対する解決手段の出願人(3/4)

解決手段II / 課題I	解決手段III / 課題II	侵入検出の性能向上 未知攻撃検出の精度向上	情報、個人の正当性向上 情報の原本性向上	攻撃の抑止・予防の強化 新たな攻撃の予防	パケット解析の高精度化 パケット採取の適切化
ファイアウォール外のシステム構成	サービスサーバーの配置	日本電気 特開2002-207694	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ 特開2001-350721 科学技術振興機構,曽我正和(共願) 特許3450849 日本電信電話 特許3393521		ｵﾑﾛﾝ 特開2003-316965
	アクセスルールとの関連付け	日立製作所 特開平10-164064			
フィルタテーブルの改良	攻撃元アドレスの追加			東芝 特開2003-099339 富士通 特開2003-288282	富士通 特開2002-251374
	ポリシルールの追加、切換	富士通 特開2004-362075			
パターンデータベースの改良	攻撃パターンの追加、切換	三菱電機 (2) 特開2002-026906 特開2003-333092 東芝(3) 特開2003-150550 特開2005-011234 特開2005-085158 日立製作所 特開2004-318742		ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ,ｻｲﾊﾞｰ･ｿﾘｭｰｼｮﾝｽﾞ(共願) (2) 特開2004-030286 特開2004-030287 ｿﾆｰ 特開2003-023377 大阪瓦斯 特開2003-256230 東芝 特開2003-298628	ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ 特開2001-313640 石井 剛,宇宙航空研究開発機構,藤田 直行(共願) 特許3648520
	攻撃情報の蓄積	日立製作所 特開2001-350677			ｾｲｺｰｴﾌﾟｿﾝ 特開2005-056243 ﾆﾃﾞｯｸ 特開2005-025378 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開2004-364306 ﾗｯｸ 特開2005-025517 東芝 特開2005-025269 富士通 特開2004-007170
	攻撃パターンの学習	石田 賢治,井上 貴裕(共願) 特開2005-175714 東芝 特開2005-085157			
	分析アルゴリズムの改良	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開2004-128733 ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開2002-133388			KDDI 特開2005-151289 ｲﾝﾃﾘｼﾞｪﾝﾄ･ｺｽﾓｽ研究機構 特開2004-312064

1993年1月～2003年12月の出願

表 1.4.2-2 アノマリ解析技術の課題に対する解決手段の出願人(4/4)

解決手段II / 課題I	解決手段III / 課題II	侵入検出の性能向上 未知攻撃検出の精度向上	情報、個人の正当性向上 情報の原本性向上	攻撃の抑止・予防の強化 新たな攻撃の予防	パケット解析の高精度化 パケット採取の適切化
データ形式の改良	データに情報付加	ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ,ｻｲﾊﾞｰ･ｿﾘｭｰｼｮﾝｽﾞ(共願) 特開2004-147223 京ｾﾗｺﾐｭﾆｹｰｼｮﾝｼｽﾃﾑ 特開2003-330886 富士通 特開2004-096246	JFE ｼｽﾃﾑｽﾞ 特開2002-149603 ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) (2) 特開2002-009759 特許3210630 ｵｰﾌﾟﾝﾙｰﾌﾟ 特許3563649 ｶｼｵ計算機 特開2002-084275 ﾘｺｰﾘｰｽ,ﾘｺｰｼｽﾃﾑ開発(共願)　特開2002-099843 村田機械 特開2003-043916 大日本印刷 特開2003-022350 東芝　特表2005-515715 日本電気 特開2002-024147 日本電信電話 (3) 特開2002-024176 特開2002-132722 特許3578100 日立製作所 (3) 特開2002-049590 特開2002-156903 特開2004-102951 富士通 特開2004-110197	日本ｺﾝﾋﾟｭｰﾀ開発 特開2000-056968	三菱電機 特開2004-179999 日本電気 特許3584838 富士通 特開2005-109715
	データの変換		松下電器産業 特開2002-319935		ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ東海 特開2004-005046 三菱電機 特開2003-204358
	オブジェクトのデータ形式改良	三菱電機ﾋﾞﾙﾃｸﾉｻｰﾋﾞｽ 特開2002-049588			
回路の改良	スイッチ回路の追加	沖電気工業 特開2004-038557		細原 豪 特開2003-348113 日本ﾃﾚｺﾑ 特開2005-197815 日本電気 特開2005-012606 日立製作所 特許3165366	

1993 年 1 月～2003 年 12 月の出願

(2) シグネチャ解析技術

図1.4.2-3にシグネチャ解析技術の課題に対する解決手段の分布を示す。この技術において、最も出願の多い課題は、「攻撃パターンの高精度化」で、次いで「侵入防御の性能向上」であり、さらに「侵入検出の性能向上」となっている。侵入検出の性能向上に対して「パターンデータベースの改良」で最も多く対応し、攻撃パターンの高精度化に対しても、「パターンデータベースの改良」で多く対応している。

図1.4.2-3 シグネチャ解析技術の課題に対する解決手段の分布

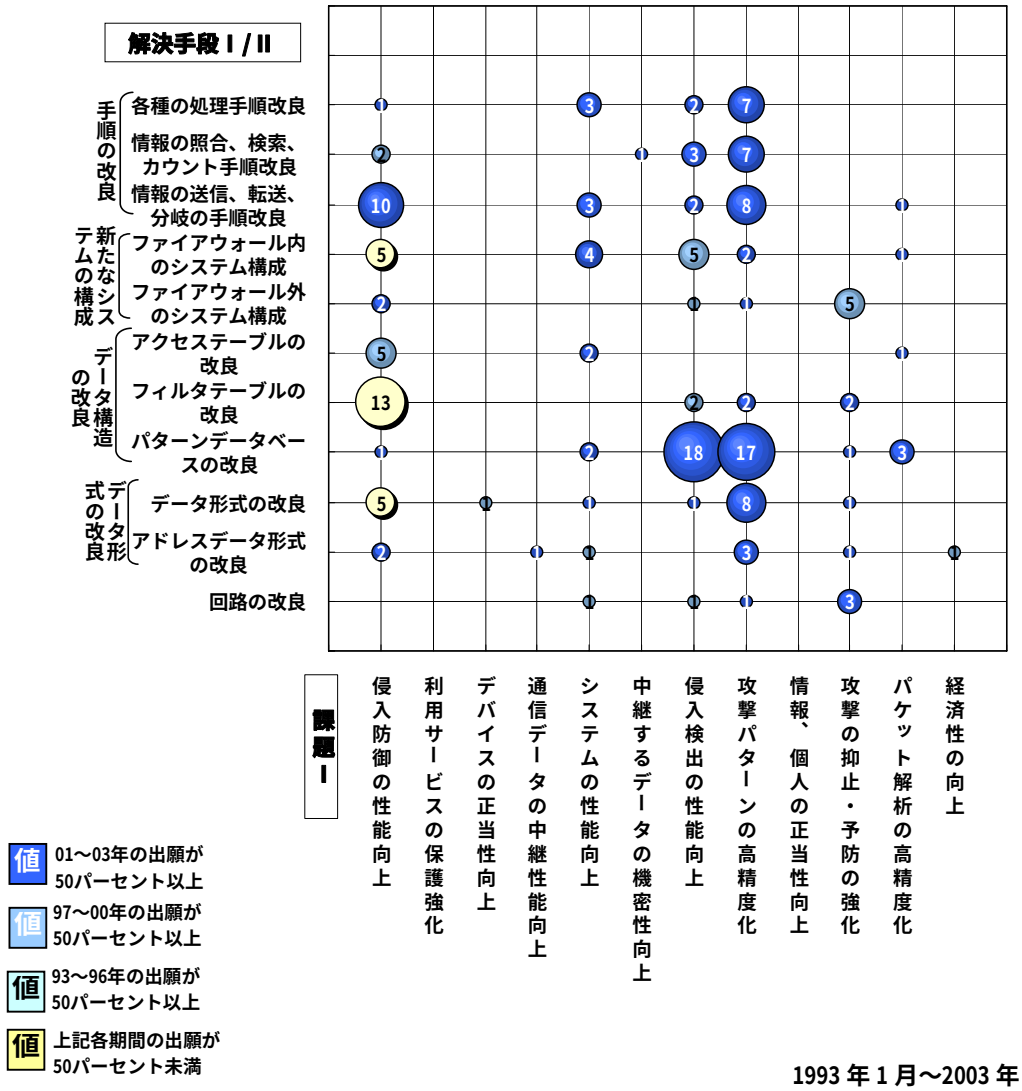


表1.4.2-3にシグネチャ解析技術の課題に対する解決手段の詳細を示す。出願が多い課題は、侵入防御の性能向上の「フィルタルール設定の効率化」と、侵入検出の性能向上の「攻撃検出の精度向上」と、攻撃パターンの高精度化の「資源消耗さす攻撃パターンの精度向上」と「プログラム脆弱性部からの攻撃パターンの精度向上」である。

フィルタルール設定の効率化に対して、「情報転送の手順改良」や「ポリシルールの追加、切換」で対応するものが多く、攻撃検出の精度向上に対して「攻撃パターンの追加、切換」や「攻撃パターンの学習」で対応するものも多い。

表 1.4.2-3 シグネチャ解析技術の課題に対する解決手段の詳細

課題 I / 課題 II / 解決手段 II	III	侵入防御の性能向上					デバイスの正当性向上	通信データの中継性能向上	システムの性能向上		中継するデータの機密性向上	侵入検出の性能向上			攻撃パターンの高精度化					攻撃の抑止・予防の強化		パケット解析の高精度化		経済性の向上
		アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	プロトコルフィルタの強化	フィルタリング処理の効率化	成済ましの防止	ネットワーク層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	機密性の適用範囲の拡大	未知攻撃検出の精度向上	攻撃検出の精度向上	侵入検出処理の効率化	資源消耗させる攻撃パターンの精度向上	プログラム脆弱部からの攻撃パターンの精度向上	プログラムを利用する攻撃パターンの精度向上	機能停止をさせる攻撃パターンの精度向上	攻撃パターン生成の効率化	新たな攻撃の予防	速やかな攻撃からの回避	パケット採取の適切化	解析処理の効率化	費用の低減
各種の処理手順改良	プロトコルの処理手順								1															
	応答コマンドの処理手順																	3						
	各種処理の実行手順				1								1			2								
	特定情報の取得手順								2			1				2								
情報の照合、検索、カウント手順改良	特定情報の照合手順	1									1		1			1								
	特定情報の検索、抽出手順		1												1									
	特定情報のカウント手順											1	1		4			1						
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	1							2			1	1				1							
	情報転送の手順		8																1			1		
	設定値で分岐の手順			1					1						4	2								
ファイアウォール内のシステム構成	イントラネット内に機器の配置			1		2			3						1									
	DMZ に機器の配置		2						1				4	1					1				1	
ファイアウォール外のシステム構成	セキュリティサーバーの配置											1						1						
	サービスサーバーの配置		2																	5				
アクセステーブルの改良	アプリケーションとの関連付け		4						1															
	アクセスルールとの関連付け			1																			1	
	認証情報との関連付け								1															
フィルタテーブルの改良	攻撃元アドレスの追加		3										2			1				1				
	フイルタの追加		4																	1				
	ポリシルールの追加、切換		5	1											1									
パターンデータベースの改良	攻撃パターンの追加、切換									2		1	6	1	5	2		1	3			1	1	
	攻撃情報の蓄積												3			2				1		1		
	攻撃パターンの学習	1											5		1									
	分析アルゴリズムの改良											2				3								
データ形式の改良	データに情報付加			1			1										2	3	2	1				
	データの変換								1			1												
	オブジェクトのデータ形式改良		4														1							
アドレスデータ形式の改良	アドレスの変換					1									1				1					
	IP アドレスの割付	1						1		1						1				1				1
回路の改良	スイッチ回路の追加								1				1		1					2	1			

1993 年 1 月～2003 年 12 月の出願

表 1.4.2-4 にシグネチャ解析技術の課題に対する解決手段の出願人を示す。出願が最も多い侵入防御の性能向上の「フィルタルール設定の効率化」課題に対する、「情報転送の手順」に関しては、コグニティブリサーチラボが２件出願している。その他は各１件の出願であるが、米国から１社、イギリスから１社の出願がある。

表 1.4.2-4 シグネチャ解析技術の課題に対する解決手段の出願人(1/3)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上	侵入検出の性能向上	攻撃パターンの高精度化	
		フィルタルール設定の効率化	攻撃検出の精度向上	資源消耗さす攻撃パターンの精度向上	プログラム脆弱部からの攻撃パターンの精度向上
各種の処理手順改良	各種処理の実行手順		富士通 特開 2004-302956		ｲﾝｶｲﾝﾀｰﾈｯﾄ(韓国) 特開 2005-166051 ﾊﾘｽ(米国) 特表 2003-523030
	特定情報の取得手順				ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2005-128933 井上 浩人,都築 浩,柏木 慎史(共願) 特開 2005-044021
情報の照合、検索、カウント手順改良	特定情報の照合手順		富士通 特開 2003-223365		三菱電機 特開 2001-236314
	特定情報の検索、抽出手順	東芝 特開平 08-153072		三菱電機 特開 2003-087333	
	特定情報のカウント手順		東芝 特開 2005-039591	ｱﾙｶﾃﾙ (ﾌﾗﾝｽ) 特開 2004-328726 沖電気工業,沖情報ｼｽﾃﾑｽﾞ(共願) 特開 2003-108450 三菱電機 特開 2002-252654 日本電信電話 特開 2004-343580	
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順		ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2005-135420		
	情報転送の手順	ｺｸﾞﾆﾃｨﾌﾞﾘｻｰﾁﾗﾎﾞ (2) 特開 2002-196944 特開 2002-196993 ｻﾞｸｿﾝｱｰﾙｱﾝﾄﾞﾃﾞｲ 特開 2003-085079 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2004-303242 ﾏﾙｺﾆ ﾕｰｹｲ ｲﾝﾃﾚｸﾁｭｱﾙﾌﾟﾛﾊﾟﾃｨｰ(ｲｷﾞﾘｽ) 特表 2004-522335 東芝 特開 2000-090048 東芝ﾃｯｸ 特開 2002-176424 日本ｻｲﾊﾞｰｻｲﾝ 特開 2003-132020			
	設定値で分岐の手順			ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ 特開 2002-016633 東芝 (3) 特開 2003-091465 特許 3566699 特許 3566700	ｺﾑｽｸｴｱ 特開 2003-216577 京ｾﾗｺﾐｭﾆｹｰｼｮﾝｼｽﾃﾑ 特開 2004-259020

1993 年 1 月～2003 年 12 月の出願

表 1.4.2-4 シグネチャ解析技術の課題に対する解決手段の出願人(2/3)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上 フィルタルール設定の効率化	侵入検出の性能向上 攻撃検出の精度向上	攻撃パターンの高精度化 資源消耗さす攻撃パターンの精度向上	攻撃パターンの高精度化 プログラム脆弱部からの攻撃パターンの精度向上
ファイアウォール内のシステム構成	イントラネット内に機器の配置			横河電機 特開 2004-140618	
	DMZ に機器の配置	日本電信電話 特開 2004-320644 日立製作所,日立ﾈｯﾄﾋﾞｼﾞﾈｽ(共願) 特開 2004-356787	ｴﾇ･ﾃｲ･ﾃｲ･ｿﾌﾄｳｴｱ 特開 2002-149602 KDDI 特開 2002-111727 三菱電機 特開 2002-007234 松下電器産業 特開 2002-328897		
ファイアウォール外のシステム構成	サービスサーバーの配置	沖電気工業 特開 2000-132473 日本電信電話 特開 2002-328896			
アクセステーブルの改良	アプリケーションとの関連付け	ｴｲ･ﾃｨ･ｱﾝﾄﾞ･ﾃｨ(米国) 特開平 09-026975 ﾃﾞﾙ･ﾕｰｴｽｴｲ･ｴﾙﾋﾟｰ(米国) 特開平 11-212921 東芝 特開平 11-308272 日本電信電話 特開平 11-313111			
フィルタテーブルの改良	攻撃元アドレスの追加	ﾘｯｼﾞｳｪｲ ｼｽﾃﾑｽﾞ ｱﾝﾄﾞ ｿﾌﾄｳｴｱ(ｲｷﾞﾘｽ) 特表 2004-505552 沖電気工業 特開平 09-284330 富士通 特開 2003-263376	KDDI 特開 2002-111726 三菱電機 特開 2001-350678		日本ﾃﾚｺﾑ 特開 2005-198267
	フイルタの追加	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3375071 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) (2) 特開平 11-353258 特許 3568850 日本電信電話 特開 2004-357234			
	ポリシルールの追加、切換	ｴｲ･ﾃｨ･ｱﾝﾄﾞ･ﾃｨ(米国) (2) 特開平 10-229418 特開平 10-243028 ﾙｰﾄﾚｯｸ･ﾈｯﾄﾜｰｸｽ 特開 2004-357026 松下電器産業 特開 2004-312416 日本電信電話 特開 2005-151492		日本電信電話 特開 2005-039721	

1993 年 1 月～2003 年 12 月の出願

表 1.4.2-4 シグネチャ解析技術の課題に対する解決手段の出願人(3/3)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上	侵入検出の性能向上	攻撃パターンの高精度化	
		フィルタルール設定の効率化	攻撃検出の精度向上	資源消耗さす攻撃パターンの精度向上	プログラム脆弱部からの攻撃パターンの精度向上
パターンデータベースの改良	攻撃パターンの追加、切換		ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ (2) 特開 2004-046742 特開 2004-336130 ﾅｶｶﾞﾜﾒﾀﾙ 特開 2003-218949 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2003-228552 三菱電機 特開 2003-085139 東芝 特開 2005-045649	ｻｲﾌｧｰﾄﾗｽﾄ 特表 2005-520230 ｿﾆｰ 特開 2004-139178 ﾄﾚﾝﾄﾞﾏｲｸﾛ 特開 2005-128792 日本電信電話 特許 3652661 富士通 特開 2004-289298	ｺﾑｽｸｴｱ 特開 2003-216576 ｿﾌﾃｯｸ 特開 2004-054706
	攻撃情報の蓄積		日本ｲﾝﾃﾘｼﾞｪﾝｽ 特開 2004-206683 日本電信電話 特開 2005-182187 日立製作所 特開 2004-038517		ｿﾆｰ 特開 2004-054470 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開 2004-102479
	攻撃パターンの学習		KDDI 特開 2005-057522 ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ 特開 2005-190484 ｺﾝﾋﾟｭｰﾀｰ ｱｿｼｴｲﾂ ｼﾝｸ(米国) 特表 2005-523539 ｼﾞｮｲｽ ｼﾞｪｰﾑｽﾞ ﾋﾞｰ(米国) 特表 2003-531430 東芝 特開 2002-300219	ﾃﾞｨｰﾌﾟ ﾅｲﾝｽﾞ(米国) 特表 2005-518764	
	分析アルゴリズムの改良				ｼﾞｪﾈﾗﾙ ﾀﾞｲﾅﾐｯｸｽ ｶﾞﾊﾞﾒﾝﾄ ｼｽﾃﾑｽﾞ(米国) 特表 2002-521775 ﾊﾘｽ(米国) 特表 2003-523140 ﾌｧｳﾝﾄﾞｽﾄｰﾝ(米国) 特表 2005-515541
データ形式の改良	オブジェクトのデータ形式改良	ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特開平 09-270788 ﾅｸﾞﾗﾋﾞｼﾞｵﾝ(ｽｲｽ) 特表 2005-502930 ﾏｲｸﾛｿﾌﾄ(米国) 特表 2002-513961 富士通 特開 2002-342278			
アドレスデータ形式の改良	アドレスの変換			ｷﾔﾉﾝ 特開 2004-343533	
	IP アドレスの割付				富士通 特開 2004-334455
回路の改良	スイッチ回路の追加		日本電気 特開 2002-158660	日本電信電話 特開 2003-087307	

1993 年 1 月～2003 年 12 月の出願

(3) 脆弱性診断技術

図1.4.2-4に脆弱性診断技術の課題に対する解決手段の分布を示す。この技術において、最も出願の多い課題は、「システムの性能向上」で、次いで「攻撃パターンの高精度化」となっている。システムの性能向上に対して「ファイアウォール内のシステム構成」で多く対応し、次いで「各種の処理手順改良」で多く対応している。

図1.4.2-4 脆弱性診断技術の課題に対する解決手段の分布

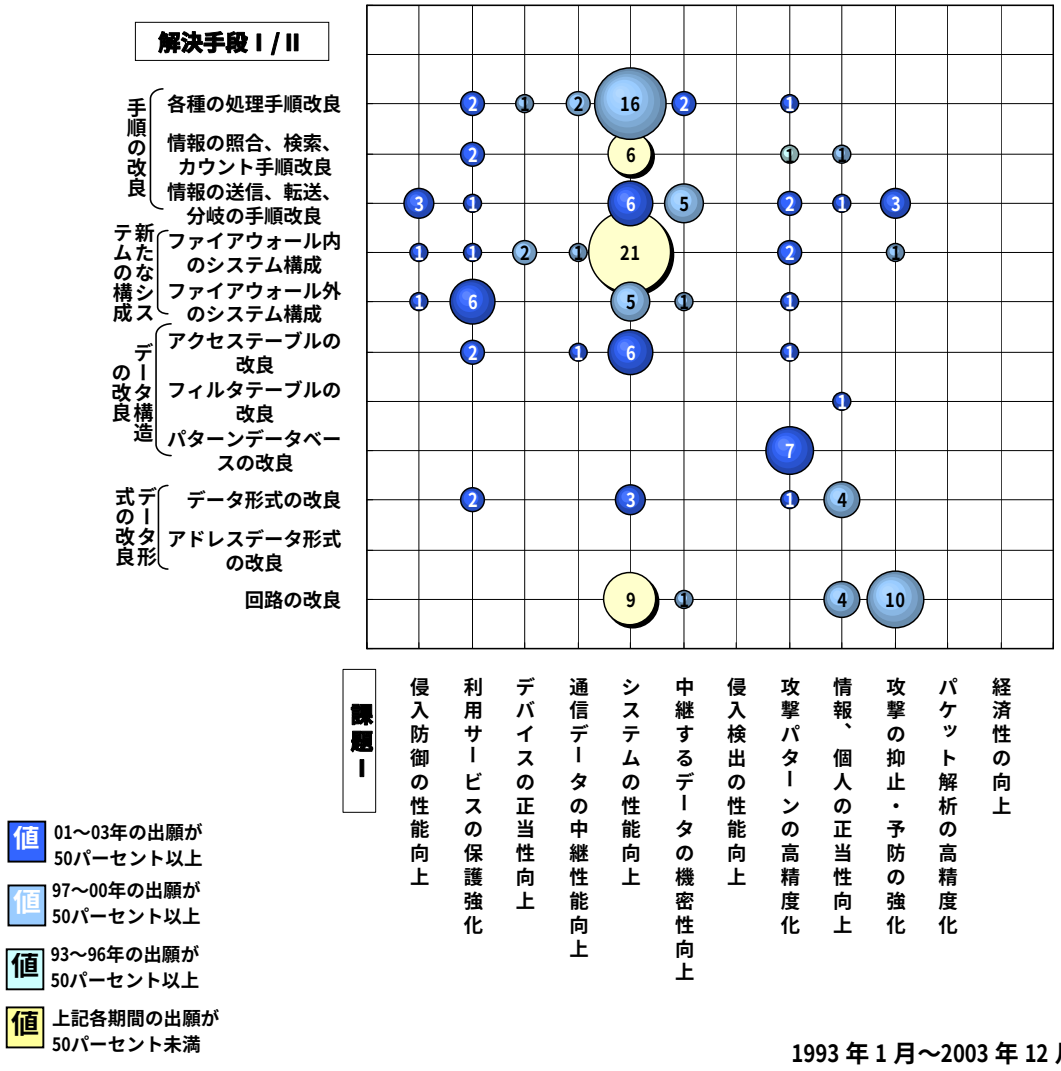


表1.4.2-5に脆弱性診断技術の課題に対する解決手段の詳細を示す。出願が多い課題は利用サービスの保護強化の「アクセス管理の効率化」と、システムの性能向上の「保守・信頼性の向上」と「システム負荷の軽減」で、さらに攻撃パターンの高精度化の「プログラム脆弱性部からの攻撃パターンの精度向上」である。

保守・信頼性の向上に対して、「イントラネット内に機器の配置」や「スイッチ回路の追加」で対応するものが多く、プログラム脆弱性部からの攻撃パターンの精度向上に対して「分析アルゴリズムの改良」で対応するものも多い。

表 1.4.2-5 脆弱性診断技術の課題に対する解決手段の詳細

解決手段 II	課題 I / 課題 II / III	侵入防御の性能向上		利用サービスの保護強化		デバイスの正当性向上		通信データの中継性能向上	システムの性能向上		中継するデータの機密性向上			攻撃パターンの高精度化	情報、個人の正当性向上		攻撃の抑止・予防の強化	
		フィルタルール設定の効率化	フィルタルール適用の整合性	リソース保護の強化	アクセス管理の効率化	成済ましの防止	認証処理の効率化	アプリケーション層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号処理の効率化	プログラム脆弱部からの攻撃パターンの精度向上	情報の原本性向上	個人認証による疎通化	新たな攻撃の予防	速やかな攻撃からの回避
各種の処理手順改良	特定情報の記憶、登録手順					1				1								
	プロトコルの処理手順								2	1								
	応答コマンドの処理手順							2	1	1				1				
	各種処理の実行手順				2				5	2	2							
	特定情報の取得手順								3									
情報の照合、検索、カウント手順改良	特定情報の照合手順			2					2					1				
	特定情報の検索、抽出手順								3									
	特定情報のカウント手順								1							1		
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順		1	1					3	2							3	
	情報転送の手順	1								1	5							
	設定値で分岐の手順		1											2		1		
ファイアウォール内のシステム構成	イントラネット内に機器の配置		1	1		1			15	2				1				1
	DMZ に機器の配置						1	1	4					1				
ファイアウォール外のシステム構成	セキュリティサーバーの配置		1		4					1			1					
	サービスサーバーの配置			1	1				4					1				
アクセステーブルの改良	アプリケーションとの関連付け			1	1													
	アクセスルールとの関連付け								5	1				1				
	認証情報との関連付け							1										
フィルタテーブルの改良	ポリシルールの追加、切換															1		
パターンデータベースの改良	分析アルゴリズムの改良													7				
データ形式の改良	データに情報付加				2					2				1	2			
	データの変換								1						1	1		
回路の改良	スイッチ回路の追加								8	1		1				4	1	9

1993 年 1 月～2003 年 12 月の出願

表1.4.2-6に脆弱性診断技術の課題に対する解決手段の出願人を示す。出願が最も多いシステムの性能向上の「保守・信頼性の向上」の課題に対する「イントラネット内に機器の配置」に関しては、NTTと三菱電機が各２件出願している。攻撃パターンの高精度化の「プログラム脆弱部からの攻撃パターンの高精度化」の課題に対する「分析アルゴリズムの改良」に関して、米国のインターネット セキュリティ システムズ社(ISS社)から１件の出願がある。

表 1.4.2-6 脆弱性診断技術の課題に対する解決手段の出願人(1/3)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化	システムの性能向上		攻撃パターンの高精度化
		アクセス管理の効率化	保守・信頼性の向上	システム負荷の軽減	プログラム脆弱部からの攻撃パターンの精度向上
各種の処理手順改良	特定情報の記憶、登録手順			富士通 特開 2000-267958	
	プロトコルの処理手順		ﾘｺｰ 特開 2003-101591 日本電気 ,ｴﾇｲｰｼｰｼｽﾃﾑﾃｸﾉﾛｼﾞｰ(共願) 特許 3555857	富士通 特許 3591753	
	応答コマンドの処理手順		三菱電機 特開 2005-100141	ﾘｺｰ 特開 2004-139566	富士通 特開 2005-056007
	各種処理の実行手順	日立製作所(2) 特開 2001-101135 特開 2003-258795	ｼｰﾒﾝｽ ｲﾝﾌｫﾒｲｼｮﾝ ｱﾝﾄﾞｺﾐｭﾆｹｲｼｮﾝ(米国) (3) 特開 2000-029835 特開 2000-082041 特開 2000-137679 東芝,東芝ｺﾝﾋﾟｭｰﾀｴﾝｼﾞﾆｱﾘﾝｸﾞ (共願) 特開平 11-345205 日本電気通信ｼｽﾃﾑ 特開 2001-357012	日立製作所 特開 2002-182560 富士通 特許 3542103	
	特定情報の取得手順		ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2004-510240 PFU 特開 2000-324154 富士通 特開平 11-259423		
情報の照合、検索、カウント手順改良	特定情報の照合手順		三菱電機ｼｽﾃﾑｳｴｱ ,三菱電機 (共願) 特許 3248658 富士通 特開平 08-249282		日立製作所 特開平 09-265443
	特定情報の検索、抽出手順		ｺﾝﾊﾟｯｸ･ｺﾝﾋﾟｭｰﾀ(米国) 特開平 11-134297 日本ﾃﾚｺﾑ 特開 2005-182640 日立情報ｼｽﾃﾑｽﾞ 特開平 11-150532		
	特定情報のカウント手順		日本電気 ,NECｱｸｾｽﾃｸﾆｶ(共願)特許 3592249		
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順		ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ 特許 3618681 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特開平 11-355271 日立製作所 特開 2003-141348	三菱電機 特表 2001-056223 日本電気 特開 2004-094850	
	情報転送の手順			NEC ﾓﾊﾞｲﾘﾝｸﾞ 特開 2001-331389	
	設定値で分岐の手順				富士通 (2) 特開 2004-258777 特開 2004-265286

1993 年 1 月～2003 年 12 月の出願

表 1.4.2-6 脆弱性診断技術の課題に対する解決手段の出願人(2/3)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化	システムの性能向上		攻撃パターンの高精度化
		アクセス管理の効率化	保守・信頼性の向上	システム負荷の軽減	プログラム脆弱部からの攻撃パターンの精度向上
ファイアウォール内のシステム構成	イントラネット内に機器の配置		ｱｲﾃｲｰﾏﾈｰｼﾞ 特許 3519696 ｲﾝﾃﾙ(米国) 特表 2005-521281 ｹﾝｳｯﾄﾞ 特開 2001-350679 ｻｰﾄﾞｳｴｱ 特開 2003-122609 ｾｲｺｰｴﾌﾟｿﾝ 特開 2004-129128 ｾｺﾑ 特開 2004-102408 ｿﾆｰ 特開 2003-124996 PFU 特開 2001-060184 三菱電機(2) 特開 2002-077174 特開 2003-345750 日本電気 特開 2002-259233 日本電信電話 (2) 特開 2005-128962 特開 2005-130399 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開平 10-107795 日立製作所 特開 2000-216830	ﾛｯｸｳｪﾙ ｻｲｴﾝｽ ｾﾝﾀｰ(米国) 特許 3184138 日本電信電話 特開 2001-244961	ﾋﾞｼﾞﾗﾝﾃｺﾑ(米国) 特表 2005-503053
	DMZに機器の配置		ﾘｺｰ,ﾘｺｰﾃｸﾉｼｽﾃﾑｽﾞ(共願) 特開 2005-027040 安川電機 特開 2001-344129 日立製作所 特開平 09-214493 富士通 特許 3262689		ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-334887
ファイアウォール外のシステム構成	セキュリティサーバーの配置	ｲﾝﾀｰﾅｼｮﾅﾙ・ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ 特開 2004-259197 ｴﾝ ｶﾞﾙﾃﾞ ｼｽﾃﾑｽﾞ(米国) 特表 2005-503047 ｺｻｲﾝ・ｺﾐｭﾆｹｰｼｮﾝｽﾞ(米国) 特表 2004-509523 三菱電機 特開 2003-030138		三菱電機 特開 2002-261829	
	サービスサーバーの配置	日本電信電話 特開 2002-335246	PFU 特開 2001-331596 ｲﾝﾀｰﾅｼｮﾅﾙ・ﾋﾞｼﾞﾈｽ・ﾏｼｰﾝｽﾞ(米国) 特開 2002-007332 ｶｼｵ計算機 特開 2000-332754 富士通 特開 2002-084326		東芝 特開 2004-318816
アクセステーブルの改良	アプリケーションとの関連付け	日立製作所 特開 2000-163375			

1993年1月～2003年12月の出願

表 1.4.2-6 脆弱性診断技術の課題に対する解決手段の出願人(3/3)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化	システムの性能向上		攻撃パターンの高精度化
		アクセス管理の効率化	保守・信頼性の向上	システム負荷の軽減	プログラム脆弱部からの攻撃パターンの精度向上
アクセステーブルの改良	アクセスルールとの関連付け		ﾊﾞｯﾌｧﾛｰ 特許 3679086 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特開 2001-237895 九州日本電気ｿﾌﾄｳｪｱ 特許 3005490 山武 特開 2003-203021 日本電気 特許 2105027	ﾌﾞﾗｻﾞｰ工業 特許 3654280	ﾘｺｰ 特開 2005-092456
パターンデータベースの改良	分析アルゴリズムの改良				ｲﾝﾀｰﾈｯﾄ ｾｷｭﾘﾃｨ ｼｽﾃﾑｽﾞ(米国) 特表 2004-509387 ｶｽﾀﾏ ｷｬｽﾄ(米国) 特表 2002-514823 ﾈｯﾄﾜｰｸ ｾｷｭﾘﾃｨｰ ｼｽﾃﾑｽﾞ(米国) 特表 2003-529254 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-164617 山武 特開 2003-256369 産業技術総合研究所 特開 2004-310267 富士通 特開 2004-303094
データ形式の改良	データに情報付加	富士ｾﾞﾛｯｸｽ (2) 特開 2004-151896 特開 2004-151897		ｴﾆｯｸｽ,ｺﾐｭﾆﾃｨｰｴﾝｼﾞﾝ(共願) 特開 2002-009837 日本電気 特開 2004-192351	ｿﾆｰ・ｺﾝﾋﾟｭｰﾀ・ｴﾝﾀﾃｲﾝﾒﾝﾄ・ｱﾒﾘｶ(米国) 特表 2005-522802
	データの変換		日立ﾊｲﾃｸﾉﾛｼﾞｰｽﾞ 特開 2003-347179		
回路の改良	スイッチ回路の追加		ｲﾝｽﾃｨﾃｭｰﾄ ﾌｪｱ ﾃﾚﾏﾃｲｸ ｴｰ ﾌｧｳ(ﾄﾞｲﾂ) 特表 2002-523979 ｲﾝﾀｰﾅｼｮﾅﾙ・ﾋﾞｼﾞﾈｽ・ﾏｼｰﾝｽﾞ(米国) 特許 3156820 ｵｾｰﾈ-ﾃﾞﾙﾗﾝﾄﾞ(ｵﾗﾝﾀﾞ) 特許 3002134 ｼﾞｮﾝｿﾝｺﾝﾄﾛｰﾙｽﾞ 特開 2004-110113 ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2003-529243 東芝 (2) 特開 2000-138703 特開 2002-207624 日立製作所 特開 2003-331373	日立製作所 特許 3599552	

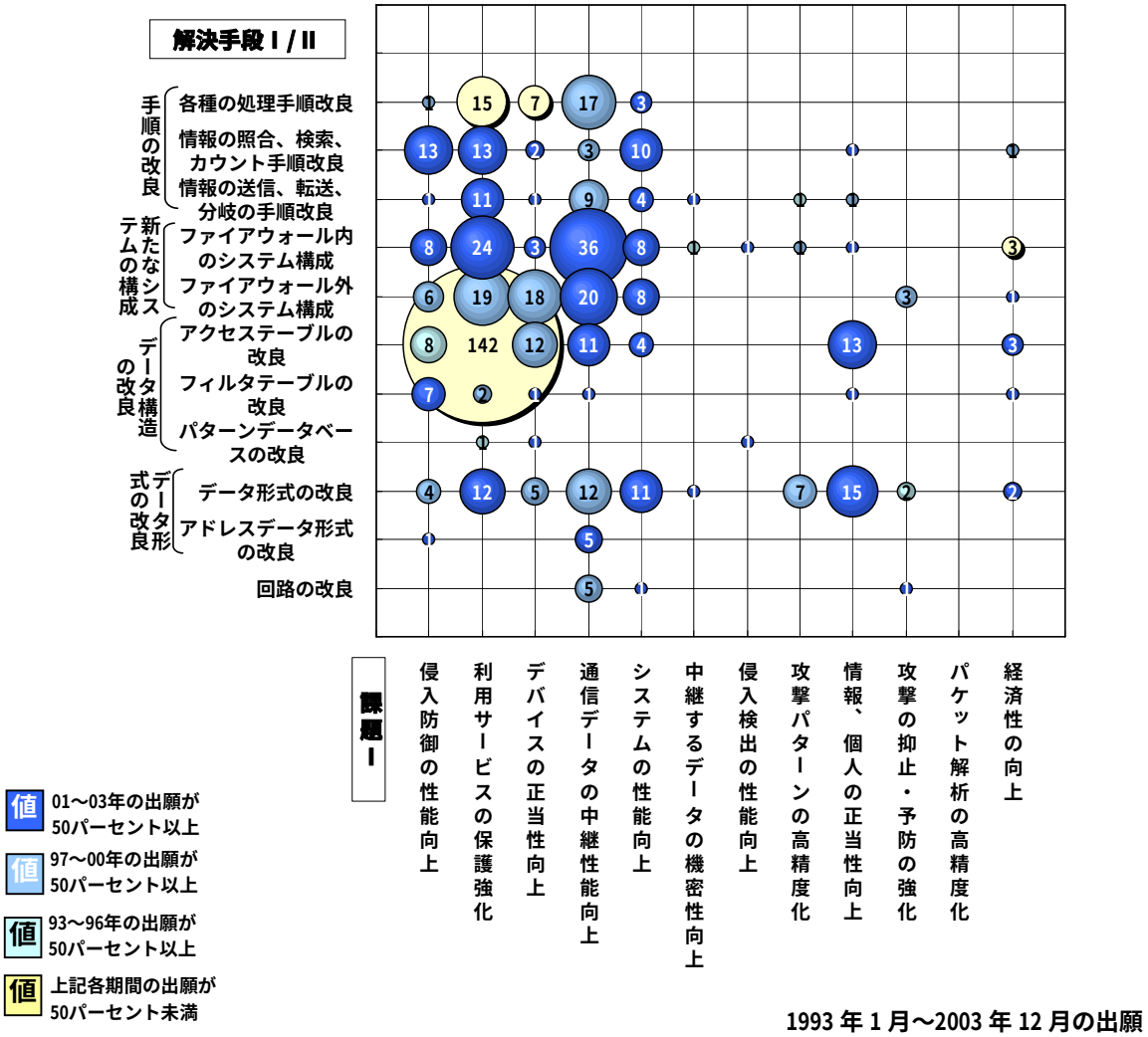
1993 年 1 月～2003 年 12 月の出願

1.4.3 アプリケーション中継技術の課題に対する解決手段

図1.4.3-1にアプリケーション中継技術の課題に対する解決手段の分布を示す。アプリケーション中継技術において、最も集中している課題は、「利用サービスの保護強化」で、次いで「通信データの中継性能向上」が多い。

利用サービスの保護強化に対しては、「アクセステーブルの改良」で最も集中し、「ファイアウォール内のシステム構成」や「ファイアウォール外のシステム構成」でも多く対応している。次いで通信データの中継性能向上に対しても「ファイアウォール内のシステム構成」や「ファイアウォール外のシステム構成」でも多く対応している。

図 1.4.3-1 アプリケーション中継技術の課題に対する解決手段の分布



次にアプリケーション中継技術をプロキシ中継技術とコンテンツフィルタリング技術に分けて、技術ごとの課題に対する出願人の分布を示す。

(1) プロキシ中継技術

図1.4.3-2にプロキシ中継技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「通信データの中継性能向上」で、次いで「システムの性能向上」である。通信データの中継性能向上に対して「ファイアウォール内のシステム構成」で最も多く、次いで「ファイアウォール外のシステム構成」でも多く対応している。

図 1.4.3-2 プロキシ中継技術の課題に対する解決手段の分布

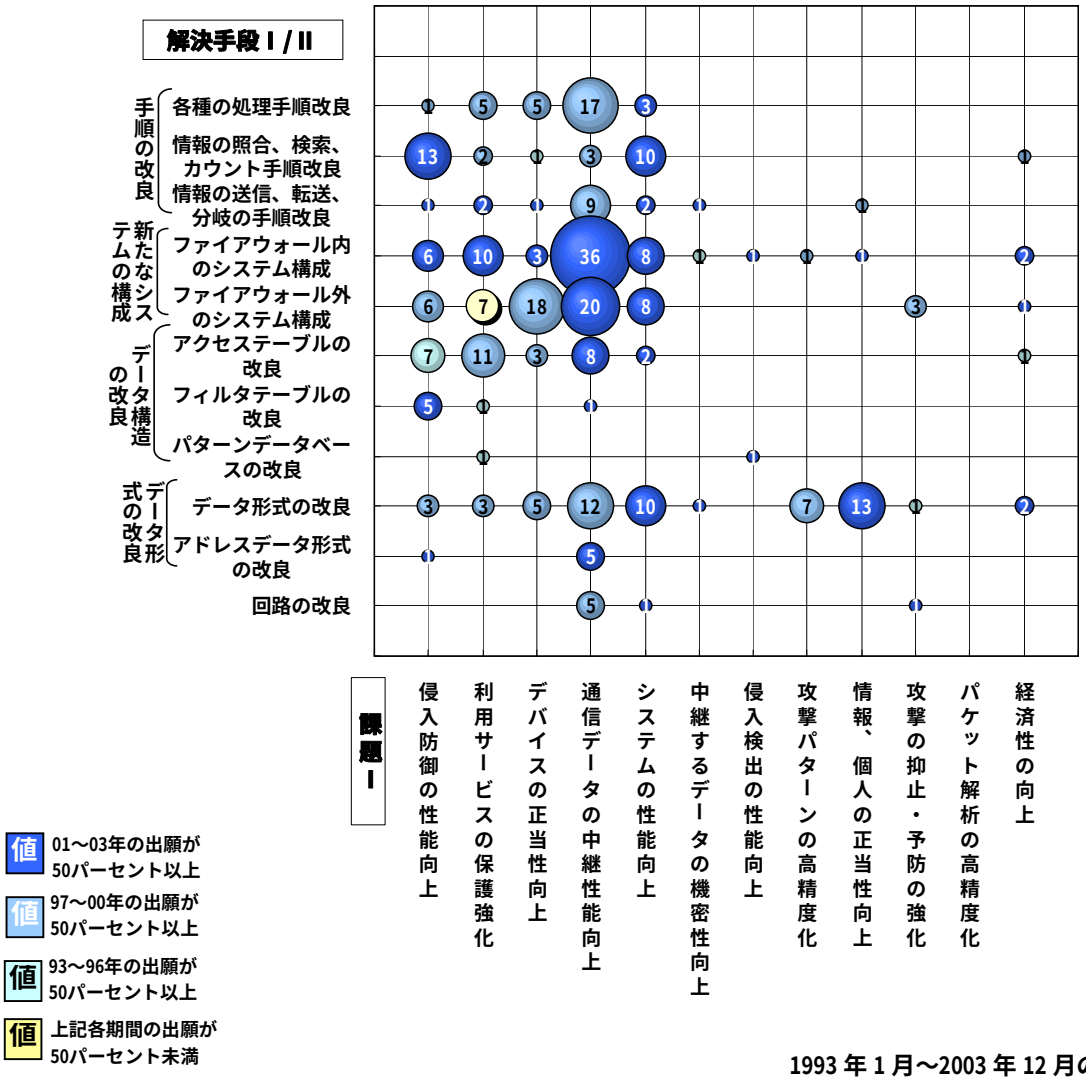


表1.4.3-1にプロキシ中継技術の課題に対する解決手段の詳細を示す。出願の多い課題は、利用サービスの保護強化の「リソース保護の強化」と、デバイスの正当性向上の「認証処理の効率化」と、通信データの中継性能向上の「アプリケーション層の中継機能拡大」と、システムの性能向上の「保守・信頼性の向上」である。

アプリケーション層の中継機能拡大に対して、「DMZに機器の配置」で最も多く、次いで「サービスサーバーの配置」で多く対応している。さらに認証処理の効率化に対して「セキュリティサーバーの配置」で対応しているものも多い。

表1.4.3-1 プロキシ中継技術の課題に対する解決手段の詳細

解決手段II / III	課題II / 課題I	アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	プロトコルフィルタの強化	フィルタリング処理の効率化	リソース保護の強化	アクセス管理の効率化	成済ましの防止	認証処理の効率化	アプリケーション層の中継機能拡大	経路生成の効率向上	ネットワーク層の中継機能拡大	トランスポート層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上	未知攻撃検出の精度向上	攻撃検出の精度向上	プログラムを利用する攻撃パターンの精度向	情報の原本性向上	個人認証による疎通化	通信データの正当性	新たな攻撃の予防	速やかな攻撃からの回避	装置コストの低減	費用の低減
各種の処理手順改良	特定情報の記憶、登録手順									4																			
	プロトコルの処理手順							3			6			1															
	応答コマンドの処理手順				1						2			7	1														
	各種処理の実行手順						1	1							1	1													
	特定情報の取得手順		0						1		1																		
情報の照合、検索、カウント手順改良	特定情報の照合手順	2			2		1				1					2													
	特定情報の検索、抽出手順				9		1			1	2				8														1
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順								1		5								1										
	情報転送の手順			1							3				2										1				
	設定値で分岐の手順						2					1																	
ファイアウォール内のシステム構成	イントラネット内に機器の配置				1			2		2	6				2		1					1							
	DMZ に機器の配置	1			3	1	6	2	1		29	1			4	2					1		1					2	
ファイアウォール外のシステム構成	セキュリティサーバーの配置			2			1	1		12	4				1	3													
	サービスサーバーの配置				3	1	3	2	4	2	16				1	3										3			1
アクセステーブルの改良	アプリケーションとの関連付け			1	1	2	8		1	2	5																	1	
	アクセスルールとの関連付け	1	1		1		3				1																		
	認証情報との関連付け										2				2														
フィルタテーブルの改良	攻撃元アドレスの追加	1			2		1																						
	フイルタの追加	1			1						1																		
パターンデータベースの改良	攻撃パターンの追加、切換						1													1									
データ形式の改良	データに情報付加	1			1		2		1	2	2	5		1	1	4						2	5	1	3			1	
	データの変換	1								2	3				2								1	1					
	オブジェクトのデータ形式改良							1			1				2	1		1				5	2			1			1
アドレスデータ形式の改良	アドレスの変換	1									2		1																
	IP アドレスの割付										2																		
回路の改良	スイッチ回路の追加										3	1	1														1		
	処理回路の改良															1													

1993 年 1 月～2003 年 12 月の出願

表1.4.3-2にプロキシ中継技術の課題に対する解決手段の出願人を示す。出願の多い通信データの中継性能向上の「アプリケーション層の中継機能拡大」の課題に対する「DMZに機器の配置」に関しては、村田機械が５件、日本電気とNTTが各３件、セイコーエプソン、富士通が各２件出願している。その他は各１件の出願であるが、大手電子機器メーカが多い。

表 1.4.3-2 プロキシ中継技術の課題に対する解決手段の出願人(1/5)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化 リソース保護の強化	デバイスの正当性向上 認証処理の効率化	通信データの中継性能向上 アプリケーション層の中継機能拡大	システムの性能向上 保守・信頼性の向上
各種の処理手順改良	特定情報の記憶、登録手順		NEC ﾋﾞｭｰﾃｸﾉﾛｼﾞｰ 特許 3570890 ｱﾗｲﾄﾞﾃﾚｼｽﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2003-018178 黄 全福(中国) 特開 2002-063136 日立製作所 特開 2002-278932		
	プロトコルの処理手順			ｷﾔﾉﾝ 特開平 11-003307 ﾄﾑｿﾝ ﾏﾙﾁﾒﾃﾞｨｱ(ﾌﾗﾝｽ) 特表 2002-518885 静岡日本電気 特開 2001-197125 日本電信電話 特開平 11-234270 富士通 (2) 特開 2004-005427 特開平 08-044643	
	応答コマンドの処理手順			ﾋﾞｼﾞｭｱﾙｼﾞｬﾊﾟﾝ 特開 2001-184307 ﾌﾞﾗｻﾞｰ工業 特開 2003-069569	山武 特開 2004-266689
	各種処理実行手順	ｿﾆｰ 特開 2002-141953			日立製作所 特開 2004-272319
	特定情報取得手順			ｲﾝﾃﾙ(米国) 特表 2005-525656	
情報の照合、検索、カウント手順改良	特定情報照合手順	ｱｸﾃｨﾌﾞ・ﾈｯﾄﾜｰｸ・ﾃﾞｻﾞｲﾝ 特開 2001-344208		NEC 情報ｼｽﾃﾑｽﾞ 特開 2002-149465	
	特定情報の検索、抽出手順	ﾌｭｰｼﾞｮﾝﾜﾝ(米国) 特開 2003-006074	富士ｾﾞﾛｯｸｽ 特許 3137173	ﾘｺｰ 特許 3501913 東芝 特開平 11-161321	ｷﾔﾉﾝ (2) 特開 2002-328886 特開 2002-328887 ｺﾆｶﾐﾉﾙﾀﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2003-050755 ｾﾝﾋﾞｯﾄﾞ(米国) 特表 2005-509977 ﾘｺｰ 特開 2003-330823 横河電機 特開 2002-305777 松下電工 特開 2003-167827 東京ｴﾚｸﾄﾛﾝ 特開 2003-229914
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順			ｴﾇ・ﾃｨ・ﾃｨ・ｺﾑｳｪｱ 特開 2001-155007 ｴﾇ・ﾃｨ・ﾃｨ・ﾃﾞｰﾀ,ﾄﾞﾜﾝｺﾞ(共願)特許 2998839 ｻﾝ・ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特表 2001-519059 ﾋﾞｽﾄ(米国) 特許 3474453 東芝 特開平 11-265347	
	情報転送の手順			ｻﾝｸﾀﾑ(ｲｽﾗｴﾙ) 特表 2003-513349 沖電気工業 特開 2000-215120 東芝 特開 2003-202930	ｺﾆｶﾐﾉﾙﾀﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2002-251356 ﾀﾞｲｷﾝ工業 特開 2004-005496

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-2 プロキシ中継技術の課題に対する解決手段の出願人(2/5)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化 リソース保護の強化	デバイスの正当性向上 認証処理の効率化	通信データの中継性能向上 アプリケーション層の中継機能拡大	システムの性能向上 保守・信頼性の向上
情報の送信、転送、分岐の手順改良	設定値で分岐の手順	日本電信電話 特開 2002-300191 富士ｾﾞﾛｯｸｽ 特開平 10-232844			
ファイアウォール内のシステム構成	イントラネット内に機器の配置		大阪瓦斯 特開 2003-110626 日本ﾃﾚｺﾑ 特開 2003-173324	ｲﾁﾚｲﾖﾝ 特開 2002-132569 ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2003-324484 ｼﾞｪｲﾋﾟｰﾓﾙｶﾞﾝ･ﾁｪｰｽ･ﾊﾞﾝｸ(米国) 特表 2003-500711 ｾﾞﾛｯｸｽ(米国) 特開 2003-050756 増沢 浩一 特開 2002-132716 日立製作所 特開 2002-123435	ｱﾌﾟﾚｯｿ 特開 2002-288052 ﾌﾞﾘﾃｨｯｼｭ･ﾃﾚｺﾐｭﾆｹｰｼｮﾝｽﾞ(ｲｷﾞﾘｽ) 特表 2002-503922
	DMZ に機器の配置	ｷﾔﾉﾝ 特開 2000-125062 ｿﾆｰ 特開 2003-067429 ﾘｺｰ 特開 2003-036335 高島 大樹 特開 2003-228551 日立製作所 (2) 特開 2003-050883 特開 2004-005705		ｲｻｵ 特開 2003-179648 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ 特開 2000-132525 ｶﾞｳﾞｧﾘ･ﾃﾞｼﾞﾀﾙ ｴﾝﾀﾃｲﾒﾝﾄ 特開 2001-005861 ｼｽｲﾝﾈｯﾄ 特開平 07-056795 ｼｬｰﾌﾟ 特開 2001-312536 ｾｲｺｰｴﾌﾟｿﾝ (2) 特開 2003-108449 特開 2004-318333 ｿﾆｰ 特開 2004-272632 ﾀﾝﾌﾞﾙｳｨｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(米国) 特開平 10-154110 三菱重工業 特開 2000-112855 山崎 文明 特開 2003-256370 松下電工 特開 2000-276410 村田機械 (5) 特開 2002-217942 特開 2002-217943 特開 2002-300159 特開 2002-300202 特開 2002-300220 東芝 特開 2000-354056 藤井 得生 特開 2002-007601 日本電気(3) 特開 2000-132475 特開 2002-351757 特開 2004-229187 日本電信電話 (3) 特開 2000-082032 特開 2000-099462 特開平 09-331327	ﾌﾞﾗﾄﾞｳ ﾁﾔﾄﾞ ｱｰﾙ(米国),ﾃﾞﾊﾞｲﾝ ｷｬﾛﾙ ﾜｲ(米国),ｼｭﾜﾙﾂ ｴﾄﾞﾜｰﾄﾞ(米国),ｼｬﾏｼｭ ｱﾘｰ(米国),ｼｮｳﾙﾊﾞｰｸﾞ ﾘﾁｬｰﾄﾞ ﾀﾞﾌﾞﾘｭ(米国),ｳﾞｫﾘｭﾋﾞﾙ(米国)(共願) 特表 2003-525475 ﾘｺｰ 特開 2004-287855 横河電機 特開 2004-220298 日本電信電話 特開 2003-271528

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-2 プロキシ中継技術の課題に対する解決手段の出願人(3/5)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化 リソース保護の強化	デバイスの正当性向上 認証処理の効率化	通信データの中継性能向上 アプリケーション層の中継機能拡大	システムの性能向上 保守・信頼性の向上
ファイアウォールのシステム構成	DMZ に機器の配置			富士ｾﾞﾛｯｸｽ情報ｼｽﾃﾑ 特開 2004-348669 富士写真ﾌｲﾙﾑ 特開平 11-073391 富士通 (2) 特開 2003-324485 特開 2004-228616	
ファイアウォール外のシステム構成	セキュリティサーバーの配置	日本電信電話 特開平 11-175475	ｱｰﾙｴｽｴｲ ｾｷｭﾘﾃｲｰ(米国) 特開 2000-357156 ｲﾝﾃﾞｨｺﾞ 特開 2001-244927 ｶｼｵ計算機 (2) 特開 2002-328854 特開 2002-374566 ｻﾝ・ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特開 2001-067317 ｿﾆｰ 特開 2003-271559 松下電器産業 特開 2001-326695 日本電気 特開 2003-330885 日本電信電話 (3) 特開 2000-322353 特開 2001-344205 特開 2002-123491 浜 勝巳 特開 2001-249984	ｴﾇ・ﾃｨ・ﾃｨ・ﾄﾞｺﾓ東海 特開 2002-278840 三菱電機 特開 2000-112860 日本電気 特開 2003-152805 富士ｾﾞﾛｯｸｽ 特開 2003-008661	ﾍﾞﾘｿﾞﾝ(米国) 特表 2001-511982
	サービスサーバーの配置	ｾｲｺｰｴﾌﾟｿﾝ(2) 特開 2002-312314 特開 2003-046580 日立ﾌﾟﾘﾝﾃｨﾝｸﾞｿﾘｭｰｼｮﾝｽ 特開 2001-296977	ｼｰﾃｲｰｱｲ,岩田 彰(共願) 特開 2001-251297 日本電気 特開 2001-344207	ｴﾇ・ﾃｨ・ﾃｨ・ﾃﾞｰﾀ (2) 特開 2000-151693 特開 2003-218867 ｴﾘｱﾋﾞｲｼﾞｬﾊﾟﾝ 特開 2002-140239 ｸﾞﾚﾈｲﾙ ｴﾚｸﾄﾛﾆｸｽ(米国) 特表 2003-527759 ｽﾀｰﾘﾝｸﾞ ｺﾏｰｽ(米国) 特表 2000-502825 ｾｲ ﾃｸﾉﾛｼﾞｰｽﾞ 特開 2000-163283 ﾄﾖﾀｹｰﾗﾑ,ｲﾝﾊﾟｸﾄｿﾌﾄ(米国)(共願) 特開 2003-099380 ﾋｭｰﾚｯﾄ・ﾊﾟｯｶｰﾄﾞ(米国)(2) 特開 2003-186764 特開 2004-005398 三菱重工業 特開 2002-063122 東日本電信電話 ,西日本電信電話(共願) (2) 特開 2000-148611 特開 2002-135335 日本電気 特開 2003-122513 日本電信電話 (2) 特開 2004-179770 特許 3672534 富士写真ﾌｲﾙﾑ 特開 2004-171422	ｾｲｺｰｴﾌﾟｿﾝ 特開 2003-018676

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-2 プロキシ中継技術の課題に対する解決手段の出願人(4/5)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化 リソース保護の強化	デバイスの正当性向上 認証処理の効率化	通信データの中継性能向上 アプリケーション層の中継機能拡大	システムの性能向上 保守・信頼性の向上
アクセステーブルの改良	アプリケーションと関連付け	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3381927 ﾋﾟｱﾚｽ ｼｽﾃﾑｽﾞ(米国) 特表 2005-523489 松下電器産業 特開 2001-273218 東芝(2) 特開 2002-342144 特開 2004-280401 NEC ｿﾌﾄｳｴｱ東北 特開 2000-276392 日本ｱｲﾋﾞｰｴﾑ 特開 2001-188699 富士通 特開 2003-323377	ｷﾔﾉﾝ 特開 2002-041477 日本電信電話 特開 2003-273868	ｿﾆｰ (3) 特開 2002-244755 特開 2002-244756 特開 2002-244868 三星電子(韓国) 特開 2003-296204 日本電気 特開 2000-276411	
	アクセスルールとの関連付け	ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ東海 特開 2003-234758 小林記録紙 特表 2001-095086 松下電器産業 特開 2001-060972		東芝 特開 2003-345690	
	認証情報との関連付け			大日本印刷 特開 2002-358274 本田技研工業 特開 2002-024072	ｿﾆｰ 特開 2004-046430 日立製作所 特開 2004-048642
フィルタテーブルの改良	攻撃元アドレスの追加	ﾘｺｰ 特開平 08-331267			
	フイルタの追加			日立製作所 特開 2005-010871	
パターンデータベースの改良	攻撃パターンの追加、切換	ｷﾔﾉﾝ 特開平 07-295934			
データ形式の改良	データに情報付加	ｲｰﾌｫｰｼｰﾘﾝｸ,ﾍﾞｰｽﾃｸﾉﾛｼﾞｰ,日立製作所,三菱化学ﾒﾃﾞｨｱ,ｾｲｺｰｲﾝｽﾂﾙﾒﾝﾂ(共願) 特開 2004-280227 ｷﾔﾉﾝ 特開 2001-045275	ｷﾔﾉﾝ 特開 2003-108520 ﾌｧｲﾌﾞｴﾆｰ 特開 2002-041380	ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ 特開 2000-076218 東芝 特開 2002-118554	ﾘｺｰ 特開 2004-289313
	データの変換		松下電器産業 特開 2003-242113 富士通 特許 3493141	ｸﾚﾃﾞｨｽ 特開 2002-163578 ｾｲｺｰｴﾌﾟｿﾝ 特開 2002-288145 ﾌｼﾞﾀ 特開 2001-306420	ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2002-328869 山田 純 特開 2003-218950
	オブジェクトのデータ形式改良			ﾄﾞｺﾓ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ﾗﾎﾞﾗﾄﾘｰｽﾞ ﾕｰ･ｴｽ･ｴｰ(米国) 特開 2004-192642	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2003-022253 ﾒｶﾞﾁｯﾌﾟｽ 特開 2003-150545

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-2 プロキシ中継技術の課題に対する解決手段の出願人(5/5)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化 リソース保護の強化	デバイスの正当性向上 認証処理の効率化	通信データの中継性能向上 アプリケーション層の中継機能拡大	システムの性能向上 保守・信頼性の向上
アドレスデータ形式の改良	アドレスの変換			ｻｲﾄｹｱ 特開 2004-252567 ﾃﾞｼﾞﾀﾙ 特開 2005-070826	
	IP アドレスの割付			ｵｰﾘｯｸ ｳｪﾌﾞ ｼｽﾃﾑｽﾞ(米国) 特許 3588323 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特許 3298832	
回路の改良	スイッチ回路の追加			住友重機械工業 特許 3597448 東日本電信電話 ,西日本電信電話(共願) 特開 2000-227869 日本電気 特許 3478200	

1993 年 1 月～2003 年 12 月の出願

(2) コンテンツフィルタリング技術

図1.4.3-3にコンテンツフィルタリング技術の課題に対する解決手段の分布を示す。コンテンツフィルタリング技術において、最も集中している課題は、「利用サービスの保護強化」である。利用サービスの保護強化に対して「アクセステーブルの改良」で最も集中して対応している。

図1.4.3-3 コンテンツフィルタリング技術の課題に対する解決手段の分布

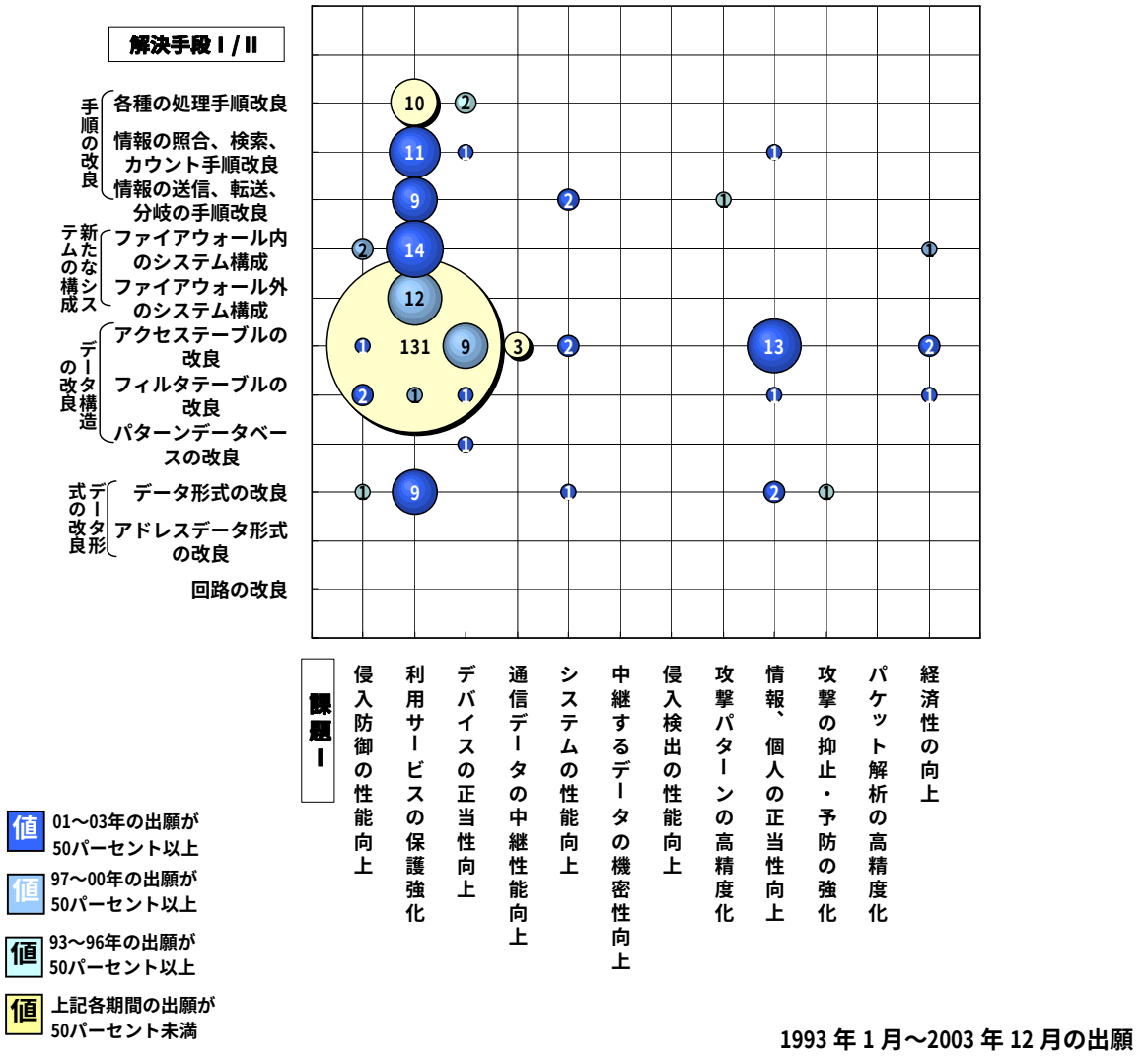


表1.4.3-3にコンテンツフィルタリング技術の課題に対する解決手段の詳細を示す。出願の多い課題は、利用サービスの保護強化であり具体的には「リソース保護の強化」と「アクセス管理の効率化」である。

リソース保護の強化に対して、「アプリケーションとの関連付け」の具体的には「ユーザー・グループ」との関連付けで最も多く、次いで「ファイル」との関連付けで多く対応し、さらに「認証情報との関連付け」でも多く対応している。アクセス管理の効率化に対して、アプリケーションとの関連付けの「ユーザー・グループ」で多く対応し、次いで「アクセスルールとの関連付け」でも多く対応している。

表1.4.3-3 コンテンツフィルタリング技術の課題に対する解決手段の詳細

課題 I / 課題 II / 解決手段 II　III			侵入防御の性能向上			利用サービスの保護強化		デバイスの正当性向上		通信データの中継性能向上	システムの性能向上		攻撃パターンの高精度化	情報、個人の正当性向上			攻撃の抑止・予防の強化	経済性の向上	
			アドレスフィルタの強化	フィルタルール適用の整合性	プロトコルフィルタの強化	リソース保護の強化	アクセス管理の効率化	成済ましの防止	認証処理の効率化	アプリケーション層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	プログラムを利用する攻撃パターンの精度向上	情報の原本性向上	個人認証による疎通化	通信データの正当性	速やかな攻撃からの回避	装置コストの低減	費用の低減
各種の処理手順改良	特定情報の記憶、登録手順					2	2												
	プロトコルの処理手順						1												
	応答コマンドの処理手順					1													
	各種処理の実行手順					2	2												
	特定情報の取得手順							2											
情報の照合、検索、カウント手順改良	特定情報の照合手順					8			1							1			
	特定情報の検索、抽出手順					2													
	特定情報のカウント手順						1												
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順					1					1	1	1						
	情報転送の手順						3												
	設定値で分岐の手順					4	1												
ファイアウォール内のシステム構成	イントラネット内に機器の配置					7	4												1
	DMZ に機器の配置			2		1	2												
ファイアウォール外のシステム構成	セキュリティサーバーの配置					1	10												
	サービスサーバーの配置					1													
アクセステーブルの改良	アプリケーションとの関連付け　ユーザー・グループ					29	18	1	1	1					5				
	アプリケーションとの関連付け　ファイル					20	1	1		1									
	アプリケーションとの関連付け　リソース					8	2	1				1							
	アプリケーションとの関連付け　業務・商品情報					1	3	1											
	アプリケーションとの関連付け　ゾーン						1												
	アクセスルールとの関連付け		1			13	15		2						1				
	認証情報との関連付け					18	2	2		1	1				6	1		2	
フィルタテーブルの改良	攻撃元アドレスの追加				1														
	フイルタの追加				1													1	
	ポリシルールの追加、切換						1	1							1				
パターンデータベースの改良	攻撃情報の蓄積							1											
データ形式の改良	データに情報付加			1		3	2					1		1	1				
	データの変換					3	1										1		

1993 年 1 月～2003 年 12 月の出願

表1.4.3-4にコンテンツフィルタリング技術の課題に対する解決手段の出願人を示す。出願が最も集中している利用サービスの保護強化の具体的な課題「リソース保護の強化」に対し、アプリケーションとの関連付けの「ユーザー・グループ」での対応に関しては、日立製作所が３件、IBM、キヤノン、日本電気、富士通が各２件出願している。その他は各１件の出願であるが、米国からはIBMを除いて５社、フランスから１社の出願がある。

表1.4.3-4 コンテンツフィルタリング技術の課題に対する解決手段の出願人(1/4)

課題Ⅰ / 課題Ⅱ / 解決手段Ⅱ Ⅲ		利用サービスの保護強化	
		リソース保護の強化	アクセス管理の効率化
各種の処理手順改良	特定情報の記憶、登録手順	ｷﾔﾉﾝ 特許 3501485 日立ｻｲｴﾝｽｼｽﾃﾑｽﾞ 特開 2003-173359	ｸﾎﾞﾀ 特開 2002-297544 ﾋﾞｽﾄ(米国) 特表 2002-523973
	プロトコルの処理手順		日本電信電話 特開 2002-032333
	応答コマンドの処理手順	ｾﾞﾛｯｸｽ(米国) 特開 2004-007589	
	各種処理の実行手順	ｷﾔﾉﾝ 特開 2002-073554 ｻﾝ・ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特表 2002-517053	ﾘｺｰ 特開 2004-280727 日本電気 特許 2932945
情報の照合、検索、カウント手順改良	特定情報の照合手順	ｴﾇ・ﾃｨ・ﾃｨ・ﾄﾞｺﾓ 特表 2002-042920 ｿﾆｰ 特開 2002-278838 ﾊﾟｰｳﾞｪｲｼｳﾞ ｾｷｭﾘﾃｨｰ ｼｽﾃﾑｽﾞ(米国) 特開 2003-228520 ﾌﾞﾗｻﾞｰ工業 特開 2005-164638 医学書院 特開 2003-345453 杉原 修 特開 2003-092567 日本電信電話(2) 特開 2002-297542 特許 3611470	
	特定情報の検索、抽出手順	ｲﾝﾀｰﾅｼｮﾅﾙ・ﾋﾞｼﾞﾈｽ・ﾏｼｰﾝｽﾞ(米国) 特表 2004-533046 ｸﾞﾛｰﾊﾞﾙ・ﾍﾞﾛｼﾃｨｰ(米国) 特表 2005-507126	
	特定情報のカウント手順		ｳｪﾌﾞｾﾝｽ(米国) 特表 2005-512211
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	ｿﾆｰ 特開 2004-102663	
	情報転送の手順		ｴﾇ・ﾃｨ・ﾃｨ・ﾃﾞｰﾀ 特許 3440206 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2003-208404 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特許 3443529
	設定値で分岐の手順	ｲﾝﾀｰﾅｼｮﾅﾙ・ﾋﾞｼﾞﾈｽ・ﾏｼｰﾝｽﾞ(米国) 特開 2003-316650 ﾗｳﾞｪﾝﾊﾟｯｸ(ﾄﾞｲﾂ) 特表 2003-518683 東洋通信機 特開 2002-318738 富士通 特開 2002-197060	富士通 特開 2004-234378
ファイアウォール内のシステム構成	イントラネット内に機器の配置	ｳｪｲﾌﾞ ｼｽﾃﾑｽﾞ(米国) 特表 2002-530765 ｼｰｲｰｼｰ 特開 2004-013909 ｾｲｺｰｴﾌﾟｿﾝ 特開 2004-206620 ｾｲｺｰｲﾝｽﾂﾙﾒﾝﾂ 特開 2003-296194 東日本電信電話 特開 2003-186777 日本電信電話 特開 2002-342277 富士通 特開 2003-099400	瀬口 哲夫,ｳﾗｼﾞﾐｰﾙ ﾊﾟﾅｼｳｸ(共願) 特開 2001-265727 日本電信電話 (2) 特開 2003-122717 特許 3557152 本田技研工業 特開 2002-024104
	DMZに機器の配置	富士通 特開 2003-006032	ｾﾌﾞﾝｽ ﾅｲﾄ(米国) 特表 2005-508059 日本電気 特開 2004-287810

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-4 コンテンツフィルタリング技術の課題に対する解決手段の出願人(2/4)

課題 I / 課題 II / 解決手段 II III IV			利用サービスの保護強化	
			リソース保護の強化	アクセス管理の効率化
ファイアウォール外のシステム構成	セキュリティサーバーの配置		富士通,富士通ヴィエルエスアイ(共願) 特開 2003-085147	ｵｰﾋﾞｯｸﾋﾞｼﾞﾈｽｺﾝｻﾙﾀﾝﾄ 特許 3577494 ｿﾆｰ 特開 2002-014929 ﾘｺｰ (2) 特開 2004-252954 特開 2004-252955 日本ﾃﾞｼﾞﾀﾙ研究所 特開 2001-203690 日本電気 特許 3630087 日本電信電話 特開 2003-345742 日立製作所 特開 2001-022755 富士通 特許 3565720 富士通,富士通周辺機(共願) 特開 2002-149475
	サービスサーバーの配置		ｱｲｻﾞｯｸ 特開 2002-288133	
アクセステーブルの改良	アプリケーションとの関連付け	ユーザー・グループ	NEC ｲﾝﾌﾛﾝﾃｨｱ 特開 2003-308452 ｱﾒﾘｶﾝ･ｴｸｽﾌﾟﾚｽ･ﾄﾗﾍﾞﾙ･ﾘﾚｲﾃｯﾄﾞ･ｻｰﾋﾞｼｽﾞ(米国) 特表 2004-502232 ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国)(2) 特開 2003-050707 特許 3611297 ｳｪﾌﾞｾﾝｽ(米国) 特表 2003-521065 ｷﾔﾉﾝ (2) 特開 2003-333067 特開 2004-096161 ｺﾆｶﾐﾉﾙﾀﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2002-171503 ｿﾆｰ 特開 2004-013600 ﾄﾞｺﾓ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ﾗﾎﾞﾗﾄﾘｰｽﾞ ﾕｰ･ｴｽ･ｴｰ(米国) 特開 2003-233589 ﾊﾟｰｳﾞｪｲｼｳﾞ ｾｷｭﾘﾃｨｰ ｼｽﾃﾑｽﾞ(米国) 特開 2003-228519 ﾊﾞﾘﾃﾞｨ(ﾌﾗﾝｽ) 特表 2004-519762 ﾋﾞｰｲｰｴｲ ｼｽﾃﾑｽﾞ(米国) 特表 2004-533075 ﾘｺｰ 特開 2003-167852 稲田 吉伸 特開 2004-220546 三井住友海上火災保険 特開 2004-078515 三洋電機 特開 2003-069595 山武,ｴﾇ･ﾃｨ･ﾃｨ･ﾌｧｼﾘﾃｨｰｽﾞ(共願) 特開 2001-111704 住友林業,日本電気 ,住友林業情報ｼｽﾃﾑ (共願) 特開 2002-328890 新日鉄ｿﾘｭｰｼｮﾝｽﾞ 特開 2000-267996 川鉄情報ｼｽﾃﾑ 特開 2000-347943 日本電気(2) 特開 2004-046460 特許 2843768 日本電信電話 特開 2003-283549 日立製作所 (3) 特開 2002-318633 特許 3659019 特許 3659052 富士通 (2) 特許 2741726 特許 3494590	ｲﾝﾀｰ･ﾁｬｲﾅ･ﾈｯﾄﾜｰｸ･ｿﾌﾄｳｪｱ(中国) 特表 2004-534297 ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国)(2) 特表 2000-508153 特表 2004-531817 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ(2) 特開 2001-290719 特開 2001-290771 ﾊﾞﾘｰ ﾋﾞｰ ﾚｲﾘｰ(米国),ﾁﾖﾄﾞﾛﾈｸ ﾏｰｸ ｴｰ(米国),ﾃﾞﾛｰｽﾞ ｴﾘｯｸ(米国),ｺﾞﾝｻﾞﾚｽ ﾏｰｸ ｴﾇ(米国),ｼﾞｪｲﾑｽ ｱﾝｼﾞｪﾗ ｱｰﾙ(米国),ﾚﾋﾞｰ ﾘｰﾝ(米国) (共願) 特表 2003-522342 ﾋﾟｭｱ ﾏﾄﾘｯｸｽ(米国) 特表 2004-529432 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特表 2004-537095 ﾗﾝﾄﾞﾙﾌﾗﾝﾄﾞ.ｺﾑ ｴﾙｴﾙｼｰ(米国) 特表 2004-537883 東芝 (4) 特開 2002-032255 特開 2003-216582 特許 3526435 特許 3576008 日本電気 特開平 09-319448 富士通 (3) 特開 2001-306513 特開 2002-014862 特表 2000-019326 野村総合研究所 特開 2000-148688

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-4 コンテンツフィルタリング技術の課題に対する解決手段の出願人(3/4)

課題 I / 課題 II / 解決手段 II III IV			利用サービスの保護強化	
			リソース保護の強化	アクセス管理の効率化
アクセステーブルの改良	アプリケーションとの関連付け	ファイル	ｱｯﾊﾟﾙ-ｻ ｲﾝﾀ-ｱｸﾃｲﾌﾞ(米国) 特表 2001-503178 ｷﾔﾉﾝ (2) 特開 2001-117744 特開 2003-108419 ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特開 2002-318715 ｻｲｴﾝﾃｨﾌｨｯｸｰｱﾄﾗﾝﾀ(米国) 特表平 10-510408 ｼｰﾒﾝｽ(ﾄﾞｲﾂ) 特開 2001-034538 ﾃﾞｨｳﾞｧｲﾝ ﾃｸﾉﾛｼﾞｰ ｳﾞｪﾝﾁｬｰｽﾞ(米国) 特表平 11-507752 ﾉﾏﾃﾞｨｯｸｽ(米国) 特表 2003-513514 ﾊﾟﾜｰﾌﾟﾘﾝﾄ 特開 2002-083019 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2004-005451 松下電器産業 特開 2000-315191 新日鉄ｿﾘｭｰｼｮﾝｽﾞ 特開 2000-267959 大阪瓦斯 特開 2005-167793 電通,ｱｲｴｽｲｰﾈｯﾄ(共願) 特開 2003-030031 日本電気 特開 2004-118433 日本電気 ,NEC ｼｽﾃﾑﾃｸﾉﾛｼﾞｰ(共願)(2) 特開 2003-186747 特開 2004-054846 日本電信電話 特許 3678128 日立製作所 特開 2001-297179 堀 健太 特開 2002-236522	三菱電機ｼｽﾃﾑｳｴｱ 特開 2000-305776
		リソース	ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ,ｻｲﾊﾞｰ･ｿﾘｭｰｼｮﾝｽﾞ(共願) 特開 2003-308296 ｶｼｵ計算機 特開 2001-101198 ｽﾃｱﾘﾝｸﾞ ｺﾏｰｽ(米国) 特表平 11-506241 ｾｲｺｰｲﾝｽﾂﾙﾒﾝﾂ 特開 2003-296193 ﾄﾗｽﾄｺﾋﾟｰ･ﾋﾟｰﾃｨｰ(ｼﾝｶﾞﾎﾟｰﾙ) 特開 2002-169681 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-005638 日本ﾃﾚｺﾑ 特開 2003-058423 富士通 特許 3657755	ｸｫｱﾙｺﾑ(米国) 特表 2005-502128 日本ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ 特開 2001-325224
		業務・商品情報	ｾｲｺｰｴﾌﾟｿﾝ 特開 2004-086686	日本電信電話 特開平 09-231173 日立製作所 特開 2004-282662 富士ｾﾞﾛｯｸｽ 特開 2004-287912
		ゾーン		ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2003-018167

1993 年 1 月～2003 年 12 月の出願

表 1.4.3-4 コンテンツフィルタリング技術の課題に対する解決手段の出願人(4/4)

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化	
		リソース保護の強化	アクセス管理の効率化
アクセステーブルの改良	アクセスルールとの関連付け	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特表 2003-500923 ｳｪｲｳﾞ ｼｽﾃﾑｽﾞ(米国) 特表 2004-513585 ｸﾛｽﾛｼﾞｯｸｽ(米国) 特表 2002-528815 ｺﾝﾋﾟｭｰﾀｰ ｱｿｼｴｲﾂ ｼﾝｸ(米国) 特表 2002-527841 ﾊﾟﾗﾛﾝ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表平 09-508246 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特表 2003-511783 ﾌﾟﾛﾋﾞｯｸｽ(米国) 特表 2004-509398 ﾏｲｸﾛｿﾌﾄ(米国) 特表 2002-517852 松下電器産業 特開 2001-337917 東京電子設計 特開 2000-330734 東芝 特開 2004-274159 日立製作所 特開 2002-318700 富士ｾﾞﾛｯｸｽ 特開 2004-151163	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3074638 ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特開平 10-326256 ﾄﾞﾙﾌｨｱﾝ(ﾌﾗﾝｽ) 特表 2004-537819 ﾘｺｰ 特開 2002-359631 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国)特許 3545303 沖電気工業,日本電信電話(共願) 特許 3504150 三菱電機 特許 3349978 松下電器産業 特表 2001-082086 大日本印刷 特開 2000-163149 東芝 特開 2002-108729 日本電気 特許 3649180 日本電信電話 特許 3398530 日立製作所(3) 特開 2001-075920 特開 2004-192601 特許 3228182
	認証情報との関連付け	ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2002-278860 ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ,ｹｲ･ﾗﾎﾞﾗﾄﾘｰ(共願)(2) 特開 2003-337630 特開 2003-337716 ｶｼｵ計算機 特開 2002-278770 ｷﾔﾉﾝ 特許 3566478 ｹﾝｳｯﾄﾞ,ｹｲ･ﾌﾛﾝﾃｨｱ(共願) 特開 2003-162505 ｿﾆｰ (3) 特開 2003-132030 特開 2004-015530 特開 2004-118455 ﾋﾟｨﾋﾟｨﾋﾟｨﾃﾞｻﾞｲﾝ 特開 2003-044342 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-213632 松下電器産業 特開 2004-038486 東芝 特開 2004-194212 日本電信電話 (4) 特開 2003-218951 特開 2003-228550 特開 2003-256315 特開 2003-258919 日立製作所 特開 2002-374237	ﾕﾆﾃﾞﾝ 特開 2002-118590 日本電信電話 特開 2004-062417
フィルタテーブルの改良	ポリシルールの追加、切換		日本電気 特許 3637857
データ形式の改良	データに情報付加	ｻｰﾄﾗｽﾄ 特開 2004-227191 ﾋﾞﾃﾞｨｳｽ(米国) 特表 2004-533677 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特表 2004-535611	日本電信電話 特許 3528065 日立製作所 特表 2000-013097
	データの変換	ｻｲﾄｻｳﾝﾄﾞ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表 2004-513453 ｾｲｺｰｴﾌﾟｿﾝ 特開 2004-029938 東芝 特開 2004-282414	ｼﾏﾝﾃｯｸ(米国) 特表 2004-533179

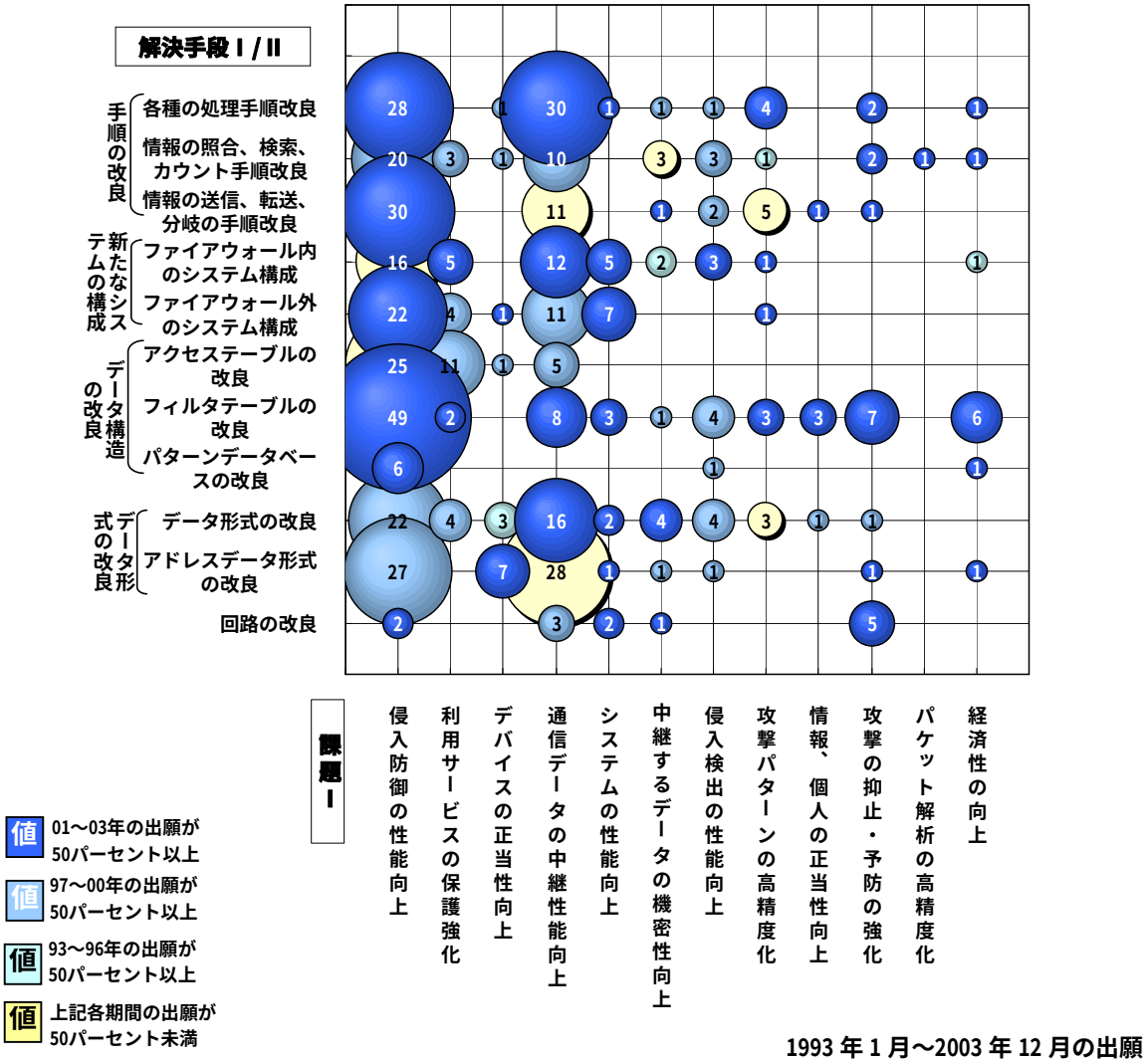
1993 年 1 月～2003 年 12 月の出願

1.4.4 パケットフィルタリング技術の課題に対する解決手段

図1.4.4-1にパケットフィルタリング技術の課題に対する解決手段の分布を示す。パケットフィルタリング技術において、出願の多い課題は、「侵入防御の性能向上」で、次いで「通信データの中継性能向上」である。

侵入防御の性能向上に対しては、「フィルタテーブルの改良」で多く対応し、「情報の送信、転送、分岐の手順改良」や「各種の処理手順改良」や「アドレスデータ形式の改良」でも多く対応している。次いで通信データの中継性能向上に対しては、「各種の処理手順改良」や「アドレスデータ形式の改良」で多く対応をしている。

図1.4.4-1 パケットフィルタリング技術の課題に対する解決手段の分布



次にパケットフィルタリング技術をIPフィルタリング技術、ルーティング制御技術とIPアドレス変換技術に分けて、技術ごとの課題に対する出願人の分布を示す。

(1) IPフィルタリング技術

図1.4.4-2にIPフィルタリング技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「侵入防御の性能向上」である。

侵入防御の性能向上に対して「フィルタテーブルの改良」で多く対応し、次いで「情報の送信、転送、分岐の手順改良」、「アクセステーブルの改良」や「各種の処理手順改良」でも多く対応している。

図1.4.4-2 IPフィルタリング技術の課題に対する解決手段の分布

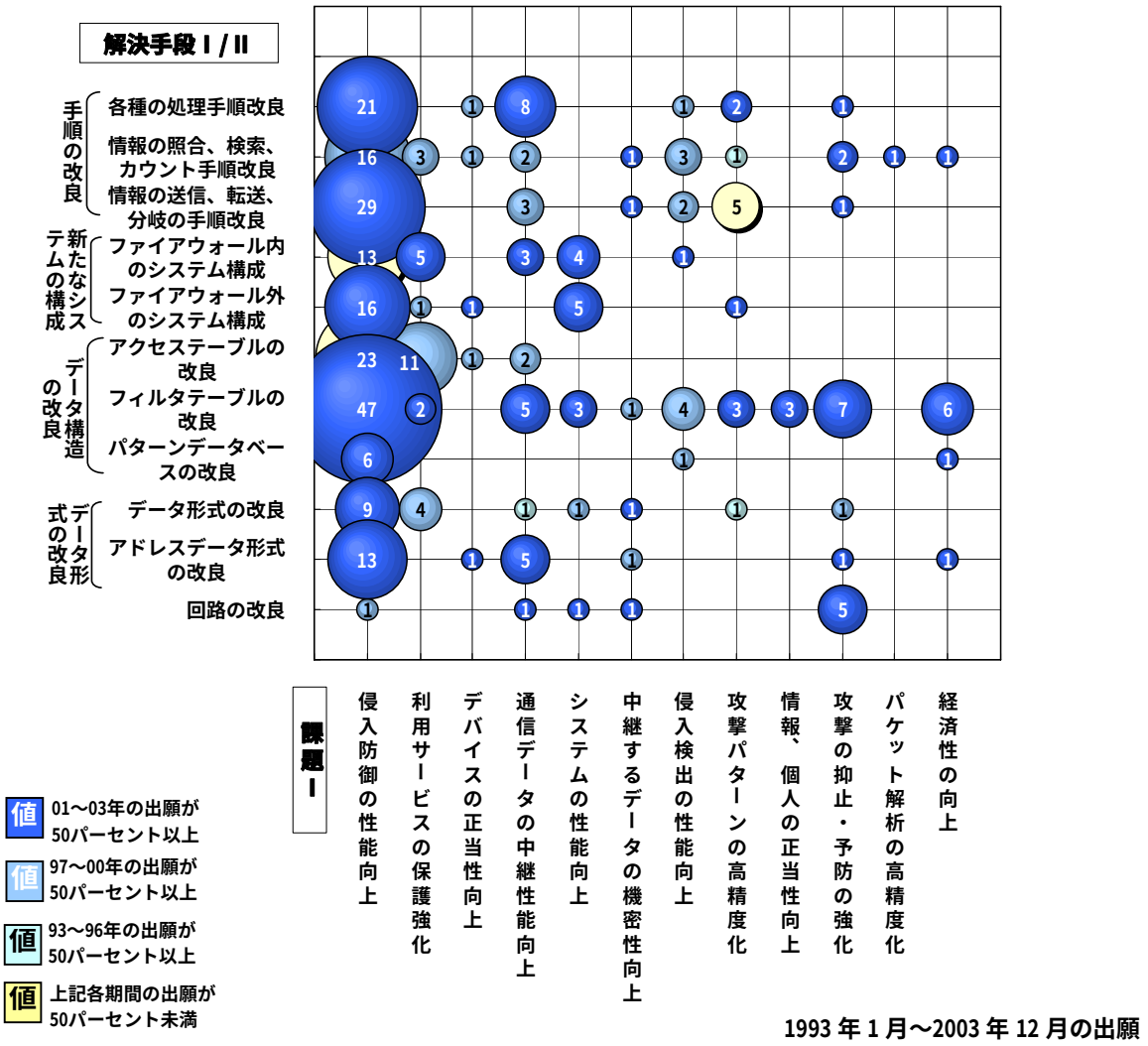


表1.4.4-1にIPフィルタリング技術の課題に対する解決手段の詳細を示す。出願の多い課題は、侵入防御の性能向上の「アドレスフィルタの強化」と、「フィルタルール設定の効率化」と、「フィルタルール適用の整合性」と、「フィルタリング処理の効率化」である。

アドレスフィルタの強化に対して、「攻撃元アドレスの追加」で多く、次いで「IPアドレスの割付」で多く対応している。さらにフィルタルール設定の効率化に対して「情報転送の手順」の改良でも多く対応している。

表1.4.4-1 IPフィルタリング技術の課題に対する解決手段の詳細

解決手段II	III	課題II: アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	プロトコルフィルタの強化	フィルタリング処理の効率化	リソース保護の強化	アクセス管理の効率化	成済ましの防止	認証処理の効率化	アプリケーション層の中継機能拡大	経路生成の効率向上	ネットワーク層の中継機能拡大	トランスポート層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号処理の効率化	未知攻撃検出の精度向上	攻撃検出の精度向上	侵入検出処理の効率化	資源消耗させる攻撃パターンの精度向上	機能停止をさせる攻撃パターンの精度向上	情報の原本性向上	新たな攻撃の予防	速やかな攻撃からの回避	解析処理の効率化	装置コストの低減
各種の処理手順改良	特定情報の記憶、登録手順	1	1	1																									
	プロトコルの処理手順	1		2		1					1		1	2															
	応答コマンドの処理手順	2			1	1			1		1			3								1		2		1			
	各種処理の実行手順		6	1		2																							
	特定情報の取得手順			1																									
情報の照合、検索、カウント手順改良	特定情報の照合手順	6		1	2		1	1	1				1	1				1				1							
	特定情報の検索、抽出手順			1	5															1								1	
	特定情報のカウント手順					1	1													1				1		2			1
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	2	1											2						1	1					1			
	情報転送の手順	3	11	6																			2						
	設定値で分岐の手順	5		1									1					1					3						
ファイアウォール内のシステム構成	イントラネット内に機器の配置	3		2	2	4	1	4			1		1	1	1	2				1									
	DMZ に機器の配置		1	1												1													
ファイアウォール外のシステム構成	セキュリティサーバーの配置	1	6	6						1						3							1						
	サービスサーバーの配置		1		1	1	1								1	1													
アクセステーブルの改良	アプリケーションとの関連付け		2	7		1	9	1	1					1															
	アクセスルールとの関連付け	3	3	3		3	1					1																	
	認証情報との関連付け		1																										
フィルタテーブルの改良	攻撃元アドレスの追加	22	3	1	1	3					4						1			3	1		1			5			1
	フイルタの追加	2	1	2	1	1	1	1			1					3							2		3	1	1		4
	ポリシルールの追加、切換	2	1	5		2																							1
パターンデータベースの改良	攻撃パターンの追加、切換		1	1		1																							1
	攻撃パターンの学習				2	1														1									
データ形式の改良	データに情報付加	1			1										1											1			
	データの変換	2	1		1		3	1				1						1						1					
	オブジェクトのデータ形式改良	1	2																										
アドレスデータ形式の改良	IP アドレスの割付	12	1						1				5				1									1			1
回路の改良	スイッチ回路の追加										1								1								5		
	処理回路の改良					1										1													

1993 年 1 月～2003 年 12 月の出願

表1.4.4-2にIPフィルタリング技術の課題に対する解決手段の出願人を示す。出願の多い課題である侵入防御の性能向上の「アドレスフィルタの強化」に対する、「攻撃元アドレスの追加」に関しては、オービックビジネスコンサルタント,三菱電機、東芝テック、日本電気、日立製作所が各２件出願している。その他は各１件の出願であるが、米国から５社、中国から１社の出願がある。

表1.4.4-2 IPフィリタリング技術の課題に対する解決手段の出願人(1/4)

課題Ⅰ / 課題Ⅱ / 解決手段Ⅱ Ⅲ		侵入防御の性能向上			
		アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	フイルタリング処理の効率化
各種の処理手順改良	特定情報の記憶、登録手順	日本電信電話 特開 2003-324457	東芝 特開 2004-282786	ﾆﾌﾃｨ 特開 2004-040164	
	プロトコルの処理手順	ﾈｯﾄｽｸﾘｰﾝ･ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表 2005-505175		ｷﾔﾉﾝ 特開 2005-101741 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-364315	日本放送協会,ﾚｸｻｽ(共願) 特開 2005-157682
	応答コマンドの処理手順	大成建設 特開平 11-053310 東洋通信機 特開 2003-067268			日立製作所 特開 2005-018186
	各種処理の実行手順		ｼｬｰﾌﾟ 特開平 07-234836 ｿﾆｰ 特開 2004-078507 ﾁｪｯｸ･ﾎﾟｲﾝﾄ･ｿﾌﾄｳｪｱ･ﾃｸﾉﾛｼﾞｰｽﾞ(ｲｽﾗｴﾙ) 特表平 10-504168 松下電器産業 特開 2003-333084 日立製作所 (2) 特開 2004-038819 特開 2004-139372	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ 特開 2002-108818	日本電気 特開 2000-293493 日立製作所 特開 2000-083055
	特定情報の取得手順			日立製作所 特開 2002-352062	
情報の照合、検索、カウント手順改良	特定情報の照合手順	ｼｬｰﾌﾟ 特開 2004-289311 ﾘｺｰ 特開 2000-134403 東芝 特開 2005-175689 日本電気 特開平 11-346214 富士ｾﾞﾛｯｸｽ 特許 3656418 富士通 特開平 09-036977		日立ﾋﾞﾙｼｽﾃﾑ 特開 2003-141078	
	特定情報の検索、抽出手順			日本電気 特開 2005-196728	
	特定情報のカウント手順				松下電器産業 特開 2005-051588
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	日本電信電話 特開 2003-324460 富士通 特表 2002-067512	日本電信電話 特開 2004-254010		
	情報転送の手順	ﾄﾞｺﾓ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ﾗﾎﾞﾗﾄﾘｰｽﾞ ﾕｰ･ｴｽ･ｴｰ(米国) 特開 2004-185622 ﾌﾞﾙｰﾌｧｲｱ ｾｷｭﾘﾃｨ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表 2004-535714 日本電気 特開 2000-156711	KDDI 特開 2005-073151 ﾏｲｸﾛｿﾌﾄ(米国) (2) 特開 2005-018769 特開 2005-085279 ﾔﾏﾊ 特開 2003-216148 ﾘｺｰ 特開 2004-133821 伊藤 徳之 特開 2004-040155 松下電器産業 特開 2004-032364 東芝 特開 2000-259521 日本電気 特開 2004-348292	ｱﾒﾘｶ ｵﾝﾗｲﾝ(米国) 特表 2003-513579 ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開平 07-250058 ｸﾞﾙｰﾌﾟ･ﾈｯﾄﾜｰｸｽ(米国) 特表 2004-501547 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2003-203011 ﾘｺｰ 特開 2004-102907 野村総合研究所 特開 2005-092485	

1993 年 1 月～2003 年 12 月の出願

表 1.4.4-2 IP フィリタリング技術の課題に対する解決手段の出願人(2/4)

解決手段II / 課題II / 課題I		侵入防御の性能向上			
		アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	フイルタリング処理の効率化
情報の送信、転送、分岐の手順改良	情報転送の手順		日立製作所 特開 2004-02166 富士通 特開平 09-116534		
	設定値で分岐の手順	三菱電機 特開 2004-185483 川鉄情報ｼｽﾃﾑ 特開 2001-144755 東芝 特開 2002-232487 日本電信電話 特開 2004-145583 富士ｾﾞﾛｯｸｽ 特開 2002-084324		東芝 特開 2003-224554	
ファイアウォール内のシステム構成	イントラネット内に機器の配置	ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2004-180155 ｻﾌｪｲ(韓国) 特表 2004-535096 馬場 芳美 特開 2001-057554		ｼﾞｪﾑﾌﾟﾘｭｽ(ﾌﾗﾝｽ) 特表 2004-532543 日本電信電話 特開 2004-187208	ｲﾌﾞﾘｯｸｽ ｱｸﾁｴﾝｹﾞｾﾞﾙｼｬﾌﾄ(ﾄﾞｲﾂ) 特表 2003-528484 ﾃﾞｼﾞﾀﾙ 特表 2003-525557 ﾏｲｸﾛｿﾌﾄ(米国) 特許 3399928 日本電気 特開 2000-261487
	DMZ に機器の配置		日本電気 特開 2005-107663	日立製作所 特開平 07-141296	
ファイアウォール外のシステム構成	セキュリティサーバーの配置	ﾌｧｰｽﾄﾄﾗｽﾄ 特開 2003-273936	ｿﾆｰ 特開 2003-186831 ﾘｺｰ (2) 特開 2004-094401 特開 2004-094405 東芝(2) 特開 2002-281093 特開 2005-072636 日本電信電話 特開 2005-086381	ｱﾙｶﾃﾙ･ｲﾝﾀｰﾈｯﾄﾜｰｷﾝｸﾞ(米国) 特表 2003-502757 ｱﾙｶﾃﾙ(ﾌﾗﾝｽ) 特開 2001-022665 ｳｫｯﾁｶﾞｰﾄﾞ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表 2002-544607 日本電信電話 (2) 特開 2001-358716 特開 2004-062416 富士電機ﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2005-004549	
	サービスサーバーの配置		ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特表 2002-518726		ﾌﾗﾝｽ･ﾃﾚｺﾑ(ﾌﾗﾝｽ) 特開平 08-331168
アクセステーブルの改良	アプリケーションとの関連付け		日本電気 特開平 11-025045 日本電信電話 特開 2004-187206	東芝 (2) 特開 2001-256123 特開 2001-256136 日本電気 特開平 09-293052 日本電信電話 特開 2004-260470 日立製作所 特開平 10-028144 富士ｾﾞﾛｯｸｽ 特開平 07-319820 富士通 特開平 07-244639	日本電気 特開 2000-232476

1993 年 1 月～2003 年 12 月の出願

表 1.4.4-2 IP フィリタリング技術の課題に対する解決手段の出願人(3/4)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上			
		アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	フイルタリング処理の効率化
アクセステーブルの改良	アクセスルールとの関連付け	ﾋﾞｱｾｽ(ﾌﾗﾝｽ) 特表 2005-526329 松下電器産業 特開 2004-185498 大阪瓦斯 特開 2004-179690	横河電機 特開 2004-054488 日本電気 特開 2004-342072 日本電信電話 特開 2002-064543	日本電信電話 特開 2003-242112 日立製作所 特開 2000-216780 富士通 特開 2005-197826	ｱﾙｶﾃﾙ (ﾌﾗﾝｽ) 特開 2002-077277 東芝 (2) 特開平 11-112514 特開平 11-136274
	認証情報との関連付け		ｾｲｺｰｴﾌﾟｿﾝ 特開 2004-297759		
フィルタテーブルの改良	攻撃元アドレスの追加	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特表 2005-513660 ｵｰﾋﾞｯｸﾋﾞｼﾞﾈｽｺﾝｻﾙﾀﾝﾄ (2) 特開 2002-133058 特開 2002-133059 ｸﾚﾃﾞﾝｽ ｼｽﾃﾑｽﾞ(米国) 特開 2002-203760 ｻﾝ・ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国),ﾓﾄﾛｰﾗ(米国)(共願) 特表 2001-506093 ﾋｭｰﾚｯﾄ・ﾊﾟｯｶｰﾄﾞ(米国) 特表 2005-505828 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-110774 華為技術(中国) 特表 2005-516544 三菱電機 (2) 特開 2000-115228 特開 2002-251336 松下電器産業 特開 2004-221879 石油ｺﾝﾋﾞﾅｰﾄ高度統合運営技術研究組合,鹿島石油 ,三菱化学(共願) 特開 2004-264963 中央ｺﾝﾋﾟｭｰﾀｰ 特開 2002-064532 東芝ﾃｯｸ (2) 特開 2004-264995 特開 2004-265116 東芝ﾗｲﾃｯｸ 特開 2004-206210 日本電気 (2) 特開 2001-345802 特許 2982727 日本電信電話 特開 2004-220120 日立製作所 (2) 特開 2004-185178 特開 2004-247800 馬場 芳美 特開 2000-354034	ｿﾆｰ 特開 2004-343497 日立製作所 特開 2003-348116 日立電線 特開平 08-331166	日立製作所 特開 2005-167864	KDDI 特許 3662080 東芝 特開 2005-086691 富士通 特開 2002-158701
	フイルタの追加	ｻﾝ・ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特表 2001-510603 東芝 特開 2004-180020	ｾｲｺｰｴﾌﾟｿﾝ 特開 2003-244243	新日鉄ｿﾘｭｰｼｮﾝｽﾞ 特開 2004-320794 富士通 特開 2005-136629	ｱﾙｶﾃﾙ ｼﾄ(ﾌﾗﾝｽ) 特開 2005-130489

1993 年 1 月～2003 年 12 月の出願

表 1.4.4-2 IP フィリタリング技術の課題に対する解決手段の出願人(4/4)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上			
		アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	フイルタリング処理の効率化
フィルタテーブルの改良	ポリシルールの追加、切換	PFU 特開平 10-133977 松下電器産業 特開平 08-163177	日立製作所 特開 2003-196476	ｱｽﾞｼﾞｪﾝﾄ 特開 2005-004679 三菱電機 特開 2002-261788 日本電信電話 特開 2004-274552 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開 2003-099602 日立製作所 特開 2002-247033	ｿﾆｰ 特開 2004-139177 日本電信電話 特開 2003-244247
パターンデータベースの改良	攻撃パターンの追加、切換		NEC ﾌｨｰﾙﾃﾞｨﾝｸﾞ 特開 2005-071218	三菱電機 特開 2005-025523	ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-364305
	攻撃パターンの学習				日本電信電話 特開 2005-027218
データ形式の改良	データに情報付加	日本電気 特開 2004-172931			
	データの変換	ｼｬｰﾌﾟ 特開 2005-142915 三菱電機 特開 2004-040476	日立製作所 特開平 11-259367		
	オブジェクトのデータ形式改良	ｺｸﾞﾆﾃｨﾌﾞﾘｻｰﾁﾗﾎﾞ 特開 2003-108255	ｱﾙｶﾃﾙ・ｲﾝﾀｰﾈｯﾄﾜｰｷﾝｸﾞ(米国) 特開 2005-065305 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2005-184836		
アドレスデータ形式の改良	IP アドレスの割付	NEC ｿﾌﾄ 特開 2003-099562 ｴﾇｹｰｴﾙ ﾉﾙﾄｳﾞｴｽﾄﾄﾞｲﾁｴｸﾗｳｾﾝﾛﾃﾘｰ(ﾄﾞｲﾂ) 特表 2004-522218 ｴﾑｹｰ精工 特開 2001-319273 ﾎｴｰﾙ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(ｲｽﾗｴﾙ) 特表 2002-507080 ﾜﾝﾏｰｹｯﾄ 特開 2002-169716 古河電気工業,東京電力(共願) 特開 2002-325144 松下電器産業 特開 2002-259309 島津製作所 特開 2003-099307 東芝 特開 2002-261790 日本電気 特許 3546771 富士通 特開 2004-032523 野村ﾎｰﾙﾃﾞｨﾝｸﾞｽ,野村総合研究所(共願) 特開 2001-312466	ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ (米国) 特開 2005-086807		
回路の改良	処理回路の改良				富士通 特開 2001-333093

1993 年 1 月～2003 年 12 月の出願

(2) ルーティング制御技術

図1.4.4-3にルーティング制御技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「通信データの中継性能向上」である。通信データの中継性能向上に対して「各種の処理手順改良」で多く対応し、次いで「データ形式の改良」、「アドレスデータ形式の改良」や「情報の照合、検索、カウントの手順改良」で多く対応している。

図1.4.4-3ルーティング制御技術の課題に対する解決手段の分布

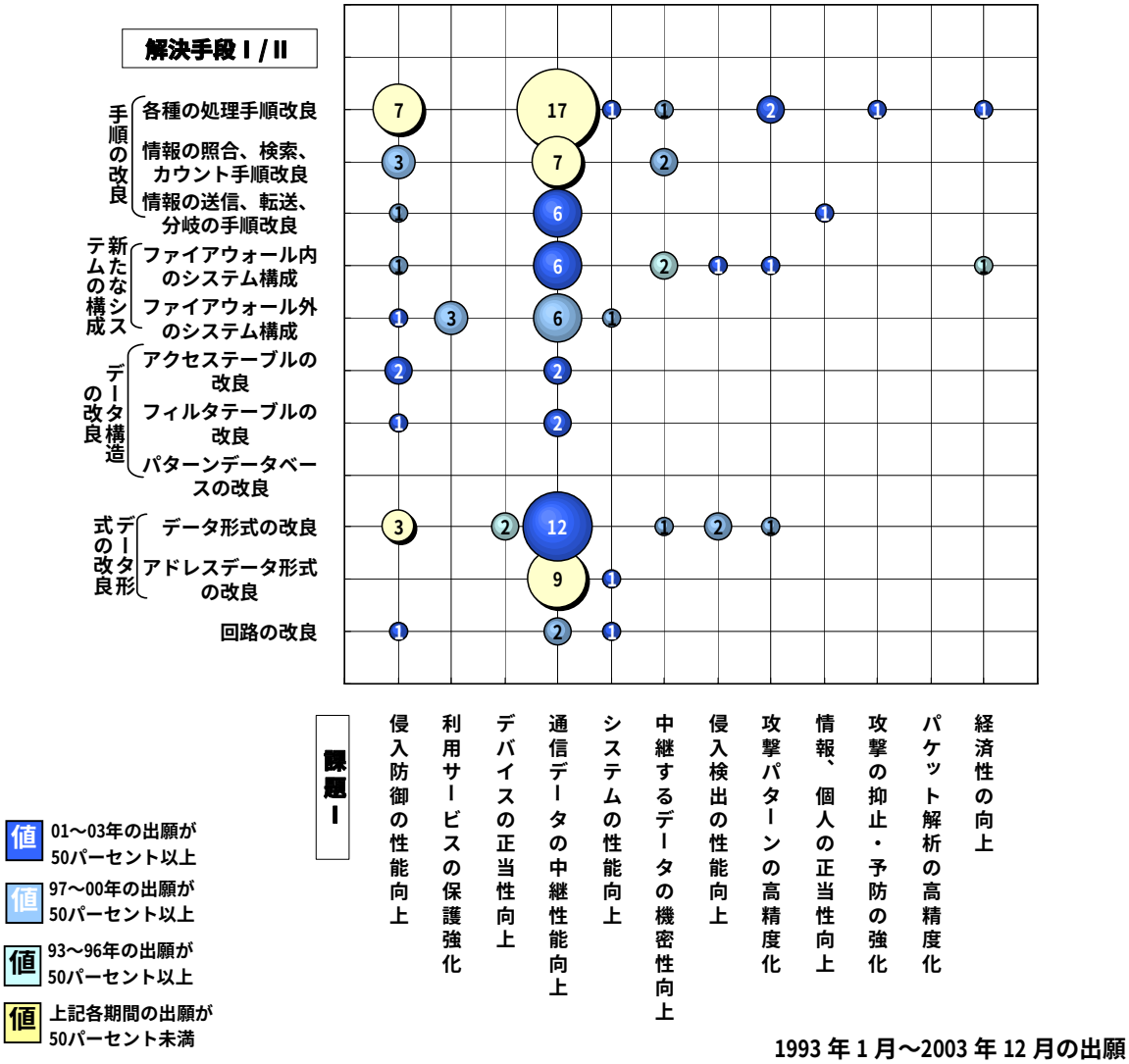


表1.4.4-3にルーティング制御技術の課題に対する解決手段の詳細を示す。出願の多い課題は、侵入防御の性能向上の「プロトコルフィルタの強化」と、通信データの中継性能向上の「アプリケーション層の中継機能拡大」、「経路生成の効率向上」と「トランスポート層の中継機能拡大」である。トランスポート層の中継機能拡大に対して、「プロトコルの処理手順」で多く、次いで経路生成の効率向上に対して「データに情報付加」や「特定情報の検索、抽出手順」や「アドレスの変換」で多く対応している。さらにプロトコルフィルタの強化に対して「プロトコルの処理手順」の改良でも多く対応している。

表 1.4.4-3 ルーティング制御技術の課題に対する解決手段の詳細

解決手段II	解決手段III	課題I: 侵入防御の性能向上				利用サービスの保護強化		デバイスの正当性向上	通信データの中継性能向上				システムの性能向上		中継するデータの機密性向上			侵入検出の性能向上		パターン攻撃の高精度化		情報、個人の正当性向	攻撃の抑止・予防の強	経済性の向上
		課題II: アドレスフィルタの強化	フィルタルール適用の整合性	プロトコルフィルタの強化	フィルタリング処理の効率化	リソース保護の強化	アクセス管理の効率化	成済ましの防止	アプリケーション層の中継機能拡大	経路生成の効率向上	ネットワーク層の中継機能拡大	トランスポート層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上	未知攻撃検出の精度向上	攻撃検出の精度向上	プログラムを利用する攻撃パターンの精度向	機能停止をさせる攻撃パターンの精度向上	通信データの正当性	新たな攻撃の予防	費用の低減
各種の処理手順改良	特定情報の記憶、登録手順											1			1									
	プロトコルの処理手順			6					2		2	8	1							1	1			1
	応答コマンドの処理手順				1				1			2												
	各種処理の実行手順									1													1	
情報の照合、検索、カウント手順改良	特定情報の照合手順									1							1							
	特定情報の検索、抽出手順	1		2						6						1								
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順									1		1										1		
	情報転送の手順								1	1														
	設定値で分岐の手順				1					2														
ファイアウォール内のシステム構成	イントラネット内に機器の配置									2	1				1			1		1				1
	DMZ に機器の配置			1						2		1				1								
ファイアウォール外のシステム構成	セキュリティサーバーの配置					1	2			1				1										
	サービスサーバーの配置	1							2	1	1	1												
アクセステーブルの改良	アプリケーションとの関連付け		1						1	1														
	アクセスルールとの関連付け	1																						
フィルタテーブルの改良	攻撃元アドレスの追加									1	1													
	ポリシルールの追加、切換			1																				
データ形式の改良	データに情報付加		1					2		7								1	1	1				
	データの変換				1					4		1			1									
	オブジェクトのデータ形式改良			1																				
アドレスデータ形式の改良	アドレスの変換									6	1			1										
	IP アドレスの割付									2														
回路の改良	スイッチ回路の追加			1						1		1	1											

1993 年 1 月～2003 年 12 月の出願

表1.4.4-4にルーティング制御技術の課題に対する解決手段の出願人を示す。出願の多い通信データの中継性能向上の具体的な課題「トランスポート層の中継機能拡大」に対する、「プロトコルの処理手順」の改良に関しては、米国からの出願が２社から各１件づつ、オランダからの出願が１社１件ある。

表 1.4.4-4 ルーティング制御技術の課題に対する解決手段の出願人(1/3)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上	通信データの中継性能向上		
		プロトコルフィルタの強化	アプリケーション層の中継機能拡大	経路生成の効率向上	トランスポート層の中継機能拡大
各種の処理手順改良	特定情報の記憶、登録手順				松下電器産業 特開 2002-164951
	プロトコルの処理手順	ｺﾛﾝﾋﾞﾃｯｸ(ｽｳｪｰﾃﾞﾝ) 特表 2004-524601 ﾃﾞｼﾞﾀﾙ 特開 2000-137662 ﾃﾚｺﾑ・ｲﾀﾘｱ・ｴｯｾ・ﾋﾟｰ・ｱｰ(ｲﾀﾘｱ) 特表 2004-538678 三菱電機ｲﾝﾌｫﾒｰｼｮﾝﾃｸﾉﾛｼﾞｰ 特許 3604131 東芝 特開 2004-201288 日立製作所 特開 2001-034553	日立製作所,日立情報制御ｼｽﾃﾑ(共願) 特開平 08-008974 富士電機ﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2001-292176		ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2005-520389 ｿﾆｰ 特開 2004-126715 ﾃｸｸﾌｧｰﾑ 特開 2002-091850 ﾎﾞｰｲﾝｸﾞ(米国) 特表 2005-502228 ﾏﾂｼﾀ･ｴﾚｸﾄﾘｯｸ(米国) 特許 3009737 山武 特開 2000-172597 富士ｾﾞﾛｯｸｽ 特開 2003-058459 富士通 特開 2002-027012
	応答コマンドの処理手順		ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特許 3375934		ｿﾆｰ 特開 2005-080003 山武 特開 2001-154953
	各種処理の実行手順			日立製作所 特開 2003-229913	
情報の照合、検索、カウント手順改良	特定情報の照合手順			日本電信電話 特開 2004-005690	
	特定情報の検索、抽出手順	ｻﾝｸﾀﾑ(ｲｽﾗｴﾙ) 特表 2003-504723 ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2003-504773			ﾄﾖﾀ自動車 特開 2004-229171 東洋通信機 特開 2000-151715 日本電信電話 (2) 特開 2004-015693 特開 2004-242161 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開 2002-325088 日立製作所 特開 2001-251367	
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順			東芝 特開 2003-044299	三菱電機 特開平 07-264178
	情報転送の手順		横河電機 特開 2004-341975	日本電信電話 特開 2004-248185	
	設定値で分岐の手順			ﾈｯﾄ ｱｲ ﾄﾗｽﾄ(米国) 特表 2002-527801 三菱電機 特開 2002-111722	

1993 年 1 月～2003 年 12 月の出願

表 1.4.4-4 ルーティング制御技術の課題に対する解決手段の出願人(2/3)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上	通信データの中継性能向上		
		プロトコルフィルタの強化	アプリケーション層の中継機能拡大	経路生成の効率向上	トランスポート層の中継機能拡大
ファイアウォール内のシステム構成	イントラネット内に機器の配置			日本電気 特開 2000-207357 日本電信電話 特開 2004-088657	
	DMZ に機器の配置	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ 特開平 11-338798		ｾﾝﾄﾗﾙﾘｰｽ,ｼｰｷｭｰﾌﾞ(共願)　特開 2002-223254 日立製作所 特許 3253542	富士通 特開 2004-064490
ファイアウォール外のシステム構成	セキュリティサーバーの配置			ｿﾆｰ　特表 2002-027503	
	サービスサーバーの配置		ｷﾞﾌｫｰﾄﾞ ﾃﾞｨｳﾞｨｯﾄﾞ ｹｲ(米国) 特表 2001-508258 川崎製鉄 特開平 07-202944	横河電機 特開 2001-290785	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ 特許 3208115
アクセステーブルの改良	アプリケーションとの関連付け		松下電器産業 特開平 07-191918	戸田建設 特開 2003-085238	
フィルターテーブルの改良	攻撃元アドレスの追加			日本電気 特許 3594009	
	ポリシルールの追加、切換	三菱電機 特開 2004-312176			
データ形式の改良	データに情報付加			ｵﾑﾛﾝｴﾝﾀﾃｲﾝﾒﾝﾄ 特開 2000-155746 ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2001-519062 ﾄﾞｺﾓ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ﾗﾎﾞﾗﾄﾘｰｽﾞ ﾕｰ･ｴｽ･ｴｰ(米国) 特開 2003-234740 PFU 特開 2002-073434 日本電気 特開 2004-355234 日本電信電話 (2) 特開 2001-188757 特開 2004-248030	
	データの変換			ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2001-518271 日本電信電話 特開 2003-316742 桧垣 博章,ｴﾙｳｲﾝｸﾞ(共願)　特開 2004-147029 富士通ﾌﾟﾗｲﾑｿﾌﾄﾃｸﾉﾛｼﾞ 特開 2005-159912	ﾕｰｼﾞｰｴｽ ﾋﾟｰｴﾙｴﾑ ｿﾘｭｰｼｮﾝｽﾞ(米国) 特表 2005-502929
	オブジェクトのデータ形式改良	日本電信電話 特許 3657569			

1993 年 1 月～2003 年 12 月の出願

表 1.4.4-4 ルーティング制御技術の課題に対する解決手段の出願人(3/3)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上	通信データの中継性能向上		
		プロトコルフィルタの強化	アプリケーション層の中継機能拡大	経路生成の効率向上	トランスポート層の中継機能拡大
アドレスデータ形式の改良	アドレスの変換			ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2003-069626 ｻｲｴﾝｽ ｱﾌﾟﾘｹｰｼｮﾝｽﾞ (米国)(2) 特表 2002-529779 特表 2002-529965 東芝 特許 3581251 日本電信電話(2) 特開 2003-069605 特開平 11-177629	
	IP アドレスの割付			ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) (2) 特許 3285882 特許 3330377	
回路の改良	スイッチ回路の追加	岡沢 広知 特開 2003-030064		ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特表 2003-505934	松下電器産業 特開平 11-261640

1993 年 1 月～2003 年 12 月の出願

(3) IPアドレス変換技術

図1.4.4-4にIPアドレス変換技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「通信データの中継性能向上」であり、次いで「侵入防御の性能向上」である。

侵入防御の性能向上に対して「アドレスデータ形式の改良」で多く対応し、さらに「データ形式の改良」でも多く対応している。通信データの中継性能向上に対して「アドレスデータ形式の改良」で多く対応している。

図 1.4.4-4 IP アドレス変換技術の課題に対する解決手段の分布

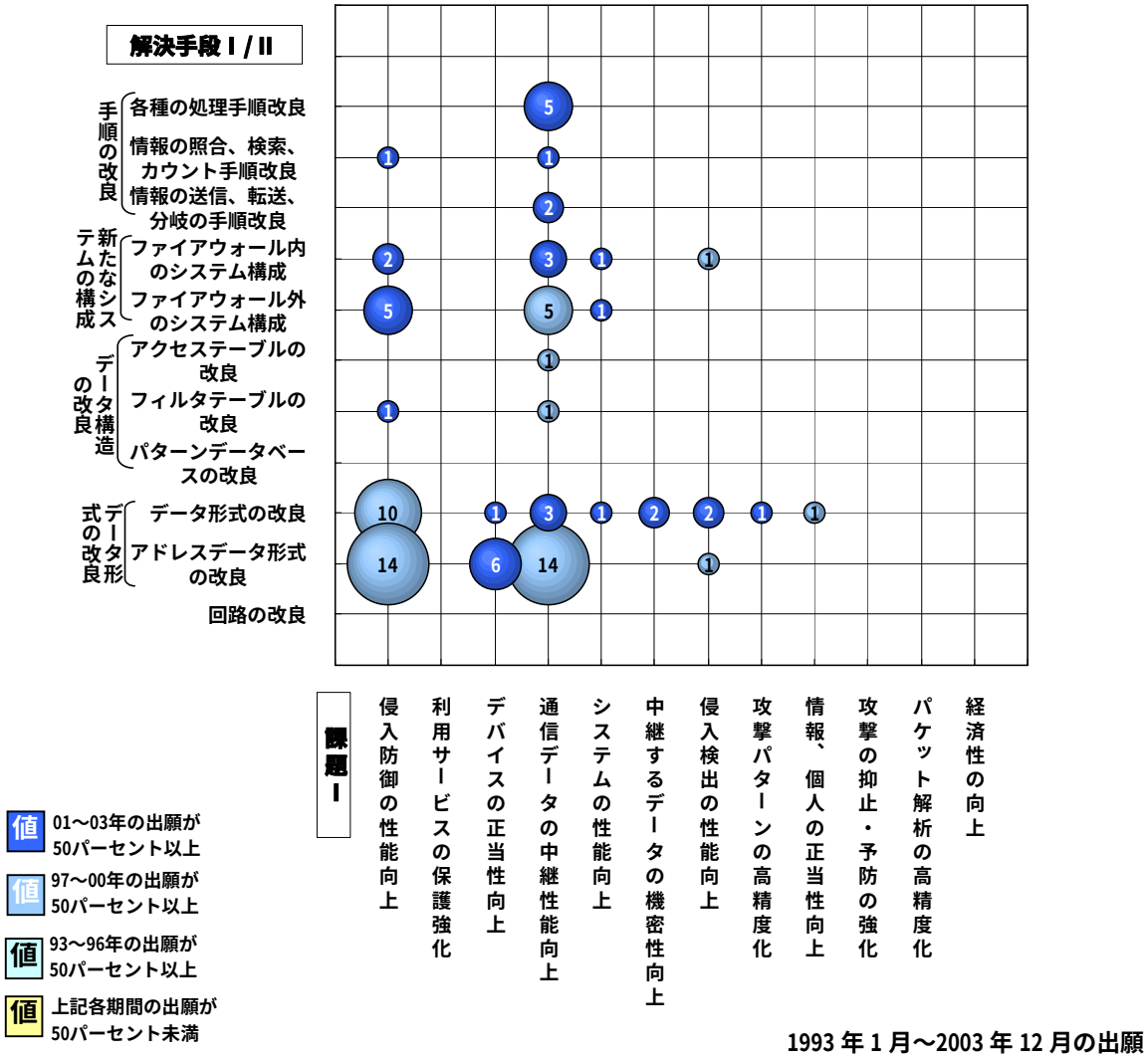


表1.4.4-5にIPアドレス変換技術の課題に対する解決手段の詳細を示す。出願の多い課題は、侵入防御の性能向上の「アドレスフィルタの強化」と、通信データの中継性能向上の「ネットワーク層の中継機能拡大」である。

アドレスフィルタの強化に対して、「アドレスの変換」で多く対応し、次いで通信データの中継性能向上に対して「アドレスの変換」や「IPアドレスの割付」で多く対応している。

表 1.4.4-5 IP アドレス変換技術の課題に対する解決手段の詳細

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上					デバイスの正当性向上	通信データの中継性能向上				システムの性能向上		中継するデータの機密性向上		検出向侵入性能上		攻撃パターンの高精度化	情報、個人の正当性向上
		アドレスフィルタの強化	フィルタルール設定の効率化	フィルタルール適用の整合性	プロトコルフィルタの強化	フィルタリング処理の効率化	成済ましの防止	アプリケーション層の中継機能拡大	経路生成の効率向上	ネットワーク層の中継機能拡大	トランスポート層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	機密性の適用範囲の拡大	暗号技術の強度向上	未知攻撃検出の精度向上	攻撃検出の精度向上	プログラムを利用する攻撃パターンの精度向上	情報の原本性向上
各種の処理手順改良	特定情報の記憶、登録手順									1									
	プロトコルの処理手順									1									
	応答コマンドの処理手順									3									
情報の照合、検索、カウント手順改良	特定情報の照合手順	1								1									
情報の送信、転送、分岐の手順改良	設定値で分岐の手順									2									
ファイアウォール内のシステム構成	イントラネット内に機器の配置									2									
	DMZ に機器の配置	1		1				1					1				1		
ファイアウォール外のシステム構成	サービスサーバーの配置	5								5		1							
アクセステーブルの改良	アクセスルールとの関連付け									1									
フィルタテーブルの改良	攻撃元アドレスの追加	1																	
	フイルタの追加									1									
データ形式の改良	データに情報付加	3	2		3		1		2		1		1	1	1	2		1	1
	データの変換	2																	
アドレスデータ形式の改良	アドレスの変換	9				1	6		2	6							1		
	IP アドレスの割付	3	1							6									

1993 年 1 月～2003 年 12 月の出願

表1.4.4-6にIPアドレス変換技術の課題に対する解決手段の出願人を示す。出願の多い侵入防御の性能向上の「アドレスフィルタの強化」の課題に対する「アドレスの変換」に関しては、富士通が３件出願している。その他は各１件の出願であるが、フランス、スウェーデン、米国から１社の出願がある。

表 1.4.4-6 IP アドレス変換技術の課題に対する解決手段の出願人(1/2)

課題 I / 課題 II / 解決手段 II III		侵入防御の性能向上 アドレスフィルタの強化	通信データの中継性能向上 ネットワーク層の中継機能拡大
各種の処理手順改良	特定情報の記憶、登録手順		ﾗﾝﾃﾞｯｸ 特開 2003-162461
	プロトコルの処理手順		ｱｽｱｽﾎｰ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ｾｷｭﾘﾃｨ(ﾌｨﾝﾗﾝﾄﾞ) 特許 3457645
	応答コマンドの処理手順		ｱﾘｴﾙ・ﾈｯﾄﾜｰｸ 特開 2004-023597 ﾈｯﾄﾂｰｺﾑ 特開 2004-015442 松下電器産業 特許 3445986
情報の照合、検索、カウント手順改良	特定情報の照合手順	ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2005-515534	日本電気 特開 2004-070757
情報の送信、転送、分岐の手順改良	設定値で分岐の手順		ﾌﾞﾗｻﾞｰ工業 特開 2004-120708 富士通 特許 3593762
ファイアウォール内のシステム構成	イントラネット内に機器の配置		ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2004-046681 日立製作所 特開 2004-015773
	DMZ に機器の配置	富士ｾﾞﾛｯｸｽ 特開平 09-062627	
ファイアウォール外のシステム構成	サービスサーバーの配置	ｴﾘ･ｱﾋﾞﾙ(米国) 特表 2005-502239 住友電気工業 特開 2004-192277 東日本電信電話 特開 2001-320418 日本電気 特開 2002-251504 富士通 特開 2004-180211	ｱｲﾎﾞｰﾙ ﾈｯﾄﾜｰｸｽ(ｶﾅﾀﾞ) 特表 2004-528748 ﾉｰﾃﾙ ﾈｯﾄﾜｰｸｽ(ｶﾅﾀﾞ) 特表平 11-508753 沖電気工業 特許 3436471 三菱電機 特許 3482863 日本電気 特開 2001-326696
アクセステーブルの改良	アクセスルールとの関連付け		日立製作所,日立情報制御ｼｽﾃﾑ(共願) 特開 2001-244996
フィルタテーブルの改良	攻撃元アドレスの追加	ﾆｰｽﾞｸﾘｴｲﾀ 特開 2003-037601	
	フイルタの追加		日本電信電話 特許 3591426
データ形式の改良	データに情報付加	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3180054 ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2004-507905 馬場 芳美 特開 2002-124996	
	データの変換	NEC ｱｸｾｽﾃｸﾆｶ 特許 3626743 ｶﾅﾙ ﾌﾟﾗｽ ｿｼｴﾃ ｱﾉﾆﾑ(ﾌﾗﾝｽ) 特表 2002-518896	

1993 年 1 月～2003 年 12 月の出願

表 1.4.4-6 IP アドレス変換技術の課題に対する解決手段の出願人(2/2)

課題 I / 課題 II / 解決手段 II　III		侵入防御の性能向上 アドレスフィルタの強化	通信データの中継性能向上 ネットワーク層の中継機能拡大
アドレスデータ形式の改良	アドレスの変換	ｱﾙｶﾃﾙ(ﾌﾗﾝｽ) 特開 2001-211175 ｴﾌﾈｯﾄ ｸﾞﾙｰﾌﾟ(ｽｳｪｰﾃﾞﾝ) 特表 2002-520892 ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特開 2000-207320 ｼﾞｬﾊﾟﾝﾒﾃﾞｨｱｼｽﾃﾑ 特開 2000-222323 新潟日本電気ｿﾌﾄｳｴｱ 特許 3001489 富士ｾﾞﾛｯｸｽ 特開 2000-276443 富士通 (3) 特開 2001-352337 特開 2002-077252 特開平 07-162454	ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特開 2000-049867 ﾈｸｽﾗﾝﾄﾞ(米国) 特開 2001-313679 ﾌｫｰﾄﾚｽ ﾃｸﾉﾛｼﾞｰｽﾞ (米国) 特表 2001-508627 日立製作所 特開 2002-132596 日立超ｴﾙ･ｴｽ･ｱｲ･ｼｽﾃﾑ 特開 2005-182250 野村総合研究所 特開 2001-298473
	IP アドレスの割付	ｲﾉﾒﾃﾞｨｱ ﾌﾟﾗｲﾍﾞｰﾄ(ｼﾝｶﾞﾎﾟｰﾙ) 特表 2004-528774 ﾕｰｼﾞｰｴｽ ﾋﾟｰｴﾙｴﾑ ｿﾘｭｰｼｮﾝｽﾞ(米国) 特表 2004-531782 安川電機 特開 2002-236627	ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特表 2002-522964 ｿﾌﾄﾌﾛﾝﾄ 特開 2002-271418 ﾃﾙｺｰﾃﾞｨｱ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表 2005-518117 ﾌｧｲｱﾌﾞﾘｯｼﾞ ｼｽﾃﾑｽﾞ ﾋﾟｰﾃｨｰﾜｲ(ｵｰｽﾄﾗﾘｱ) 特表 2004-531941 ﾘｺｰ 特開 2002-176462 日立製作所 特開平 11-032088

1993 年 1 月～2003 年 12 月の出願

1.4.5 ホスト認証技術の課題に対する解決手段

図1.4.5-1にホスト認証技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「デバイスの正当性向上」で、次いで「情報、個人の正当性向上」である。

デバイスの正当性向上に対しては、「情報の照合、検索、カウント手順改良」で多く対応し、「各種の処理手順改良」や「データ形式の改良」や「ファイアウォール外のシステム構成」でも多く対応している。

図 1.4.5-1 ホスト認証技術の課題に対する解決手段の分布

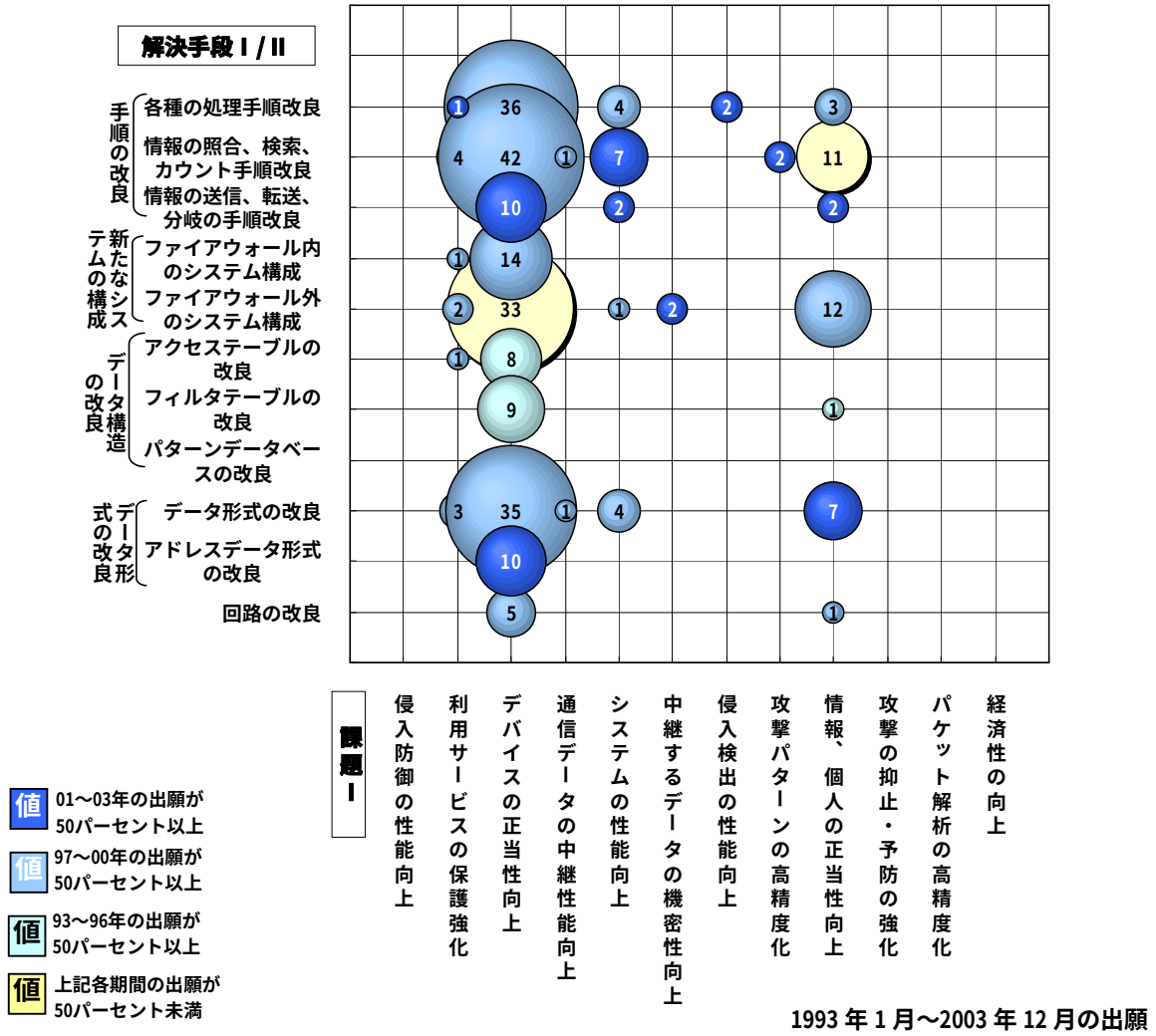


表1.4.5-1にホスト認証技術の課題に対する解決手段の詳細を示す。出願の多い課題は、デバイスの正当性向上の「成済ましの防止」と「認証処理の効率化」であり、さらに情報、個人の正当性向上の「個人認証による疎通化」である。

成済ましの防止に対して、「セキュリティサーバーの配置」で多く、次いで「特定情報の照合手順」の改良と「データに情報付加」で多く対応している。さらに認証処理の効率化に対して「特定情報の記憶、登録手順」と「特定情報の照合手順」でも多く対応している。

表 1.4.5-1 ホスト認証技術の課題に対する解決手段の詳細

解決手段 II	III	課題 I: 利用サービスの保護強化		デバイスの正当性向上		通信データの中継性能向上		システムの性能向上		中継するデータの機密性向上	侵入検出の性能向上	攻撃パターンの高精度化		情報、個人の正当性向上		
		課題 II: リソース保護の強化	アクセス管理の効率化	成済ましの防止	認証処理の効率化	経路生成の効率向上	ネットワーク層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	使い易いセキュア通信の確立	攻撃検出の精度向上	資源消耗さす攻撃パターンの精度向上	プログラムを利用する攻撃パターンの精度向上	情報の原本性向上	個人認証による疎通化	通信データの正当性
各種の処理手順改良	特定情報の記憶、登録手順		1	7	16				1						1	
	プロトコルの処理手順				1											
	応答コマンドの処理手順			3	1						1				1	
	各種処理の実行手順								3							
	特定情報の取得手順			8							1				1	
情報の照合、検索、カウント手順改良	特定情報の照合手順	3	1	27	12	1		1	6			1	1		5	3
	特定情報のカウント手順			2	1										3	
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順			3	1				2						2	
	情報転送の手順			3	3											
ファイアウォール内のシステム構成	イントラネット内に機器の配置			9	1											
	DMZ に機器の配置		1	3	1											
ファイアウォール外のシステム構成	セキュリティサーバーの配置	2		28	3				1	2				1	8	2
	サービスサーバーの配置			2											1	
アクセステーブルの改良	アプリケーションとの関連付け			1												
	アクセスルールとの関連付け	1		3	1											
	認証情報との関連付け			1	2											
フィルタテーブルの改良	攻撃元アドレスの追加			9											1	
データ形式の改良	データに情報付加	2		23	3		1	1	3					1	1	2
	データの変換	1		8	1										3	
アドレスデータ形式の改良	アドレスの変換			7												
	IP アドレスの割付			2	1											
回路の改良	スイッチ回路の追加			4	1										1	

1993 年 1 月～2003 年 12 月の出願

表1.4.5-2にホスト認証技術の課題に対する解決手段の出願人を示す。出願の多いデバイスの正当性向上の具体的な課題「成済ましの防止」に対する「セキュリティサーバーの配置」に関しては、NTTが６件出願している。その他は各１件の出願であるが、海外から米国３社、オランダと韓国から各１社ずつの出願がある。

表 1.4.5-2 ホスト認証技術の課題に対する解決手段の出願人(1/5)

課題 I / 課題 II / 解決手段 II III		デバイスの正当性向上		情報、個人の正当性向上
		成済ましの防止	認証処理の効率化	個人認証による疎通化
各種の処理手順改良	特定情報の記憶、登録手順	ﾒﾃﾞｨｱﾄﾞｳ 特開 2002-366516 住友電気工業 特開 2003-324458 東芝 特開 2001-118038 日本電信電話(3) 特開 2001-350722 特開 2003-169069 特開 2004-260401 日立製作所 特開平 11-331142	ｱｲﾃｨﾌｫｰ 特開 2003-091504 ｴｲﾃﾞｨｼｰﾃｸﾉﾛｼﾞｰ 特開 2001-092891 ｼｬｰﾌﾟ (2) 特開 2001-352411 特開 2004-259000 ﾌｫﾝﾄﾞｯﾄ ｺﾑｼﾞｬﾊﾟﾝ 特開 2000-148685 ﾘｺｰ 特開 2004-287492 りそなﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開 2002-163231 安川電機 特開 2002-124978 沖電気工業 特開 2001-092782 三菱ﾏﾃﾘｱﾙ 特開 2003-318958 三菱電機 特許 3587045 大和証券ｸﾞﾙｰﾌﾟ本社 特開 2002-132719 日本電気 特許 3436165 日本電信電話 特開 2000-236342 日立製作所 特開 2000-029833 富士ｾﾞﾛｯｸｽ 特開 2000-057056	武田 英夫 特開平 11-066004
	プロトコルの処理手順		ｷﾔﾉﾝ 特開 2004-054893	
	応答コマンドの処理手順	山武 特開 2002-237821 住商情報ｼｽﾃﾑ 特開 2002-312316 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開平 10-136025	富士通 特許 3463399	日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開 2001-103049
	特定情報の取得手順	ｱﾌﾞｿﾘｭｰﾄ ｿﾌﾄｳｪｱ(ｶﾅﾀﾞ) 特表平 10-508735 ﾉｷｱ ﾈｯﾄﾜｰｸｽ(ﾌｨﾝﾗﾝﾄﾞ) 特表 2002-520708 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特表 2004-508619 東芝 特開平 11-175476 東洋通信機 特開平 11-088325 凸版印刷 特開平 11-331181 日本電信電話 特開 2003-173417 富士通 特開 2005-184639		ﾌｧｰｽﾄ ﾃﾞｰﾀ(米国) 特表 2004-506361
情報の照合、検索、カウント手順改良	特定情報の照合手順	NEC ｿﾌﾄ 特開 2002-014924 ｱﾙｶﾃﾙ (ﾌﾗﾝｽ) 特開 2001-236015 ｴﾑ ｱｲ ｼｰ ｼｽﾃﾑｽﾞ(ｵﾗﾝﾀﾞ) 特表 2003-504739 ｷﾔﾉﾝ 特開 2000-209562 ｼｬｰﾌﾟ 特開 2001-144756 ｼｭﾀﾙｸ 特開 2005-078462 ｿﾆｰ 特開 2002-344444 ﾉｷｱ ﾈｯﾄﾜｰｸｽ(ﾌｨﾝﾗﾝﾄﾞ) (2) 特表 2004-517517 特表 2004-518309 ﾋﾞｼﾞﾈｽ･ﾌﾞﾚｰｸｽﾙｰ 特開 2000-341340 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2003-223416 ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特開 2002-084276 ﾜﾝﾀﾞｰﾌｧｰﾑ 特開 2002-055954 横河電機 特開 2004-178361	ｿﾆｰ (2) 特開 2005-064683 特開平 08-263384 ﾏｲｸﾛｿﾌﾄ(米国) 特開 2003-099401 前田 勇 特開 2002-032342 日新電機 特開平 11-203248 日本電気(3) 特開 2001-237820 特開 2004-258997 特開平 07-064912 日本電信電話,ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ(共願) 特開平 08-223293 富士通ｴﾌ･ｱｲ･ﾋﾟｰ 特開 2003-273855 野村総合研究所 (2) 特開 2001-282676 特開 2004-227451	ﾍﾞﾘｽﾀｰ(米国) 特表平 11-511882 ﾒﾄﾛ 特開 2001-175599 三菱電機 特開 2001-320366 日本電気 特開 2004-070814 日本電気ｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開 2000-259569

1993 年 1 月～2003 年 12 月の出願

表 1.4.5-2 ホスト認証技術の課題に対する解決手段の出願人(2/5)

課題 I / 課題 II / 解決手段 II III		デバイスの正当性向上		情報、個人の正当性向上
		成済ましの防止	認証処理の効率化	個人認証による疎通化
情報の照合、検索、カウント手順改良	特定情報の照合手順	松下電器産業 (3) 特開 2001-265677 特開 2002-140298 特開 2004-040717 杉山 彰 特開 2001-022272 大阪瓦斯 特開 2002-223312 通信 放送機構,日立製作所 (共願) 特開 2003-143126 日本ﾋﾞｸﾀｰ 特開 2002-024179 日本電気 特開 2005-159688 日本電気ﾃﾚｺﾑｼｽﾃﾑ ,日本電気 (共願) 特許 2972637 日本電信電話 特開 2002-344474 日立製作所 特開 2001-060183 富士ｾﾞﾛｯｸｽ 特開 2000-057097 富士通 特開 2005-072639		
	特定情報のカウント手順	ﾃｨｰ･ﾃｨｰ･ﾃｨｰ 特開 2004-102524 富士ｾﾞﾛｯｸｽ 特開 2005-044277	ｱｲ･ﾃｨｰ･ｻｰﾋﾞｽ 特開 2000-322380	沖電気工業 特開 2004-220123 三菱電機 特開 2002-297543 富士ｾﾞﾛｯｸｽ 特開 2005-190348
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順	NEC ｿﾌﾄ 特開 2002-140241 ｾｷｭｱｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ 特開 2004-023662 東芝ｷｬﾘｱ 特開 2001-285962	ｴﾑ･ｼｰ･ｴﾑ ｼﾞｬﾊﾟﾝ 特開 2002-374308	山武 特開 2003-203051 日本電信電話 特開 2003-244125
	情報転送の手順	ｱｸﾃｨﾌﾞｶｰﾄﾞ(ﾌﾗﾝｽ) 特表 2002-517049 住友電気工業 特開 2003-324459 日立製作所 特開 2004-272724	三星電子(韓国) 特開 2003-289299 日本電信電話 特許 3656194 日立製作所 特開 2001-202332	
ファイアウォール内のシステム構成	イントラネット内に機器の配置	ｱﾄﾞﾊﾞﾝｽﾄ･ﾏｲｸﾛ･ﾃﾞｨﾊﾞｲｼｽﾞ(米国) 特表 2004-535641 ｵﾗｸﾙ(米国) 特表 2001-522115 ｿﾘｭｰｼｮﾅﾘｰ(米国) 特表 2004-525446 ﾃﾞﾝｿｰ 特開 2002-232955 積水ﾊｳｽ 特開 2002-183008 東芝 (2) 特開平 11-085687 特許 3651721 日本電気 特許 3501051 日立製作所 特開 2004-274521	KDDI 特開 2002-108820	
	DMZ に機器の配置	日本電信電話 特開 2005-117466 日立製作所 特開 2003-124926 富士ｾﾞﾛｯｸｽ 特開 2000-057112	日立製作所 特開 2002-132714	

1993 年 1 月～2003 年 12 月の出願

表 1.4.5-2 ホスト認証技術の課題に対する解決手段の出願人(3/5)

課題 I / 課題 II / 解決手段 II III		デバイスの正当性向上		情報、個人の正当性向上
		成済ましの防止	認証処理の効率化	個人認証による疎通化
ファイアウォール外のシステム構成	セキュリティサーバーの配置	ｱｲﾋﾞｯｸｽ 特開 2000-222359 ｲｰﾁﾔｰｼﾞ(米国) 特表 2003-534593 ｲﾝﾃﾙ(米国) 特表 2004-527816 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ 特開 2002-101459 ｷﾔﾉﾝ 特開平 07-021127 ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2004-533194 ｾｿﾞﾝ情報ｼｽﾃﾑｽﾞ 特開 2001-217826 ｿﾆｰ 特開 2003-069559 ﾆｰﾓﾆｯｸｾｷｭﾘﾃｨ 特開 2005-071202 ﾋｱﾕｰｱｰ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(米国) 特表 2004-505383 ﾋﾞｰｲﾝｸﾞ 特開平 11-272615 ﾏｲ･ﾃﾚﾋﾞ 特開 2001-357014 横河電機 特開 2003-085140 沖電気工業 特開 2005-191830 三星電子(韓国) 特開 2003-234786 三菱電機 特開 2000-216903 松下電器産業 特開 2004-363884 鷹山 特開 2003-288326 東芝 特開平 11-345214 日本電信電話 (6) 特開 2002-132721 特開 2004-023166 特開 2004-363874 特開平 10-312362 特許 3496482 特許 3670242 日立製作所 特開 2004-140779 富士通 特開平 10-105516 野上 優 特開 2001-290723	三菱電機 特開 2003-085144 日本電信電話 特開 2001-273258 富士通ｿｰｼｱﾙｻｲｴﾝｽﾗﾎﾞﾗﾄﾘ 特開 2003-296428	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3426091 ｴｽ･ﾃｨｰ･ｴﾙ 特開 2001-265220 ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2002-049589 ﾌﾗﾝｽ ﾃﾚｺﾑ(ﾌﾗﾝｽ) 特開 2004-246895 ﾓﾝｷｰ(旧香港) 特開平 10-341224 東洋通信機 特開平 11-187016 日立製作所 特開 2003-178025 富士ｾﾞﾛｯｸｽ 特開 2002-091917
	サービスサーバーの配置	ﾍﾞｸﾀｰ 特開 2002-049770 日本電気 ,ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ(共願) 特許 3616570		住友電気工業 特開平 11-239169
アクセステーブルの改良	アプリケーションとの関連付け	ﾏｲｸﾛｿﾌﾄ(米国) 特開 2004-310774		
	アクセスルールとの関連付け	ｴｲ ｼﾞｰ ｺﾐｭﾆｹｲｼｮﾝ ｼｽﾃﾑｽﾞ(米国) 特開平 11-146018 日本電信電話 特開平 09-307580 日立製作所,日立ｺﾝﾋﾟｭｰﾀｴﾝｼﾞﾆｱﾘﾝｸﾞ(共願) 特開平 09-244976	日本電気 ,ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ(共願) 特許 3645844	
	認証情報との関連付け	日立製作所 特開平 06-274431	三菱電機 特開 2003-030063 富士通 特開平 07-295926	

1993 年 1 月～2003 年 12 月の出願

表 1.4.5-2 ホスト認証技術の課題に対する解決手段の出願人(4/5)

課題 I / 課題 II / 解決手段 II　III		デバイスの正当性向上		情報、個人の正当性向上
		成済ましの防止	認証処理の効率化	個人認証による疎通化
フィルタテーブルの改良	攻撃元アドレスの追加	JFE ﾎｰﾙﾃﾞｨﾝｸﾞｽ,ｴｸｻ(共願) 特開平 10-269293 PFU　特開 2005-134972 ｺﾆｶﾐﾉﾙﾀﾎｰﾙﾃﾞｨﾝｸﾞｽ 特開平 06-324959 東芝　特開平 07-038599 東日本電信電話 特開 2004-304281 日本電気　特開平 07-028754 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開平 09-046335 日立製作所 特開平 07-079243 富士通　特開平 09-172450		日本電気　特開平 07-013930
データ形式の改良	データに情報付加	ｱﾊﾞｲｱ ﾃｸﾉﾛｼﾞｰ(米国) 特表 2005-515550 ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ (2) 特開 2004-072631 特開 2004-194196 ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2004-519882 ｺﾘﾝｽﾞ ﾗｲｱﾙ ｼﾄﾞﾆｰ(ｵｰｽﾄﾗﾘｱ) 特表 2002-532741 ｼｰﾒﾝｽ(ﾄﾞｲﾂ) 特表 2004-514310 ｼﾞｪﾈﾗﾙ･ｲﾝｽﾂﾙﾒﾝﾄ(米国) 特表 2002-535740 ｽｶｲｺﾑ,ﾈｯﾄﾜﾝｼｽﾃﾑｽﾞ(共願) 特開 2004-040650 ｾｲｺｰｴﾌﾟｿﾝ 特開 2004-094630 ﾈｯﾄﾋﾞﾚｯｼﾞ 特開平 10-240689 ﾉｷｱ ﾈｯﾄﾜｰｸｽ(ﾌｨﾝﾗﾝﾄﾞ) 特表 2002-541685 ﾌﾗﾝｾｰｽﾞ ﾃﾞｭ ﾗﾃﾞｨｵﾃﾚﾌｫﾝﾇ(ﾌﾗﾝｽ)　特開 2004-120755 ﾘｺｰ　特開 2000-330898 三菱電機　特開 2001-148715 松下電器産業 (2) 特開 2004-088148 特開 2004-220339 大日本印刷 特開 2005-100123 日本電気　特開 2001-318889 日本電信電話 (4) 特開 2005-080242 特開 2005-141654 特開 2005-142719 特開平 10-327144 日立製作所 特許 3678009	森元 信吉　特開 2001-312467 日本電信電話(2) 特開 2004-240819 特許 3437680	NEC ｿﾌﾄ　特開 2005-165418

1993 年 1 月～2003 年 12 月の出願

表 1.4.5-2 ホスト認証技術の課題に対する解決手段の出願人(5/5)

課題 I / 課題 II / 解決手段 II III		デバイスの正当性向上		情報、個人の正当性向上
		成済ましの防止	認証処理の効率化	個人認証による疎通化
データ形式の改良	データの変換	ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2004-512735 ｻﾝ･ﾏｲｸﾛｼｽﾃﾑｽﾞ(米国) 特開平 11-167536 ｼﾞｪﾑﾌﾟﾘｭｽ(ﾌﾗﾝｽ) 特表 2002-523923 ﾊﾝﾁﾝ ﾘｱｵ(米国),ｽﾃｨｰｳﾞﾝ ｴｽﾎﾞｲﾙ(米国),ﾋﾟｰﾀｰ ｴﾌ ｷﾝｸﾞ(米国),ﾌﾞﾙｰｽ ｳﾞｨ ｼｭﾜﾙﾂ(米国)(共願) 特開平 11-275069 産学連携機構九州,ｾｷｭｱｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(共願) 特開 2004-282295 大野 治夫,長岡 俊治(共願) 特開 2001-357011 日本ﾃﾞｼﾞﾀﾙ研究所 特開平 11-195004 日立製作所 特開平 08-335207	日本電信電話 特開 2000-250409	NEC ｿﾌﾄ 特開 2003-249931 ｾｲｺｰｴﾌﾟｿﾝ 特開 2002-132715 日本電信電話 特開 2000-244481
アドレスデータ形式の改良	アドレスの変換	SAP 特開 2005-191879 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ 特開 2002-288134 ｾｲｺｰｴﾌﾟｿﾝ 特開 2005-026825 東日本電信電話 特開 2004-134855 日本電気 特開平 09-205457 日本電信電話 (2) 特開 2001-273257 特開平 09-016494		
	IP アドレスの割付	横河電機 特開 2005-006147 日立製作所 特開 2004-289257	東芝 特開 2003-091503	
回路の改良	スイッチ回路の追加	ｷﾔﾉﾝ 特開 2001-352330 沖電気工業 特開平 11-025046 三菱電機 特開 2001-298774 富士通 特許 3431745	日本電気 特開 2004-048234	日本電気 特開 2002-163030

1993 年 1 月～2003 年 12 月の出願

1.4.6 トンネリング技術の課題に対する解決手段

図1.4.6-1にトンネリング技術の課題に対する解決手段の分布を示す。この技術において、出願の多い課題は、「中継するデータの機密性向上」で、次いで「システムの性能向上」である。

中継するデータの機密性向上に対しては、「データ形式の改良」で集中して対応し、「各種の処理手順改良」や「ファイアウォール外のシステム構成」や「情報の送信、転送、分岐の手順改良」でも多く対応している。

図1.4.6-1 トンネリング技術の課題に対する解決手段の分布

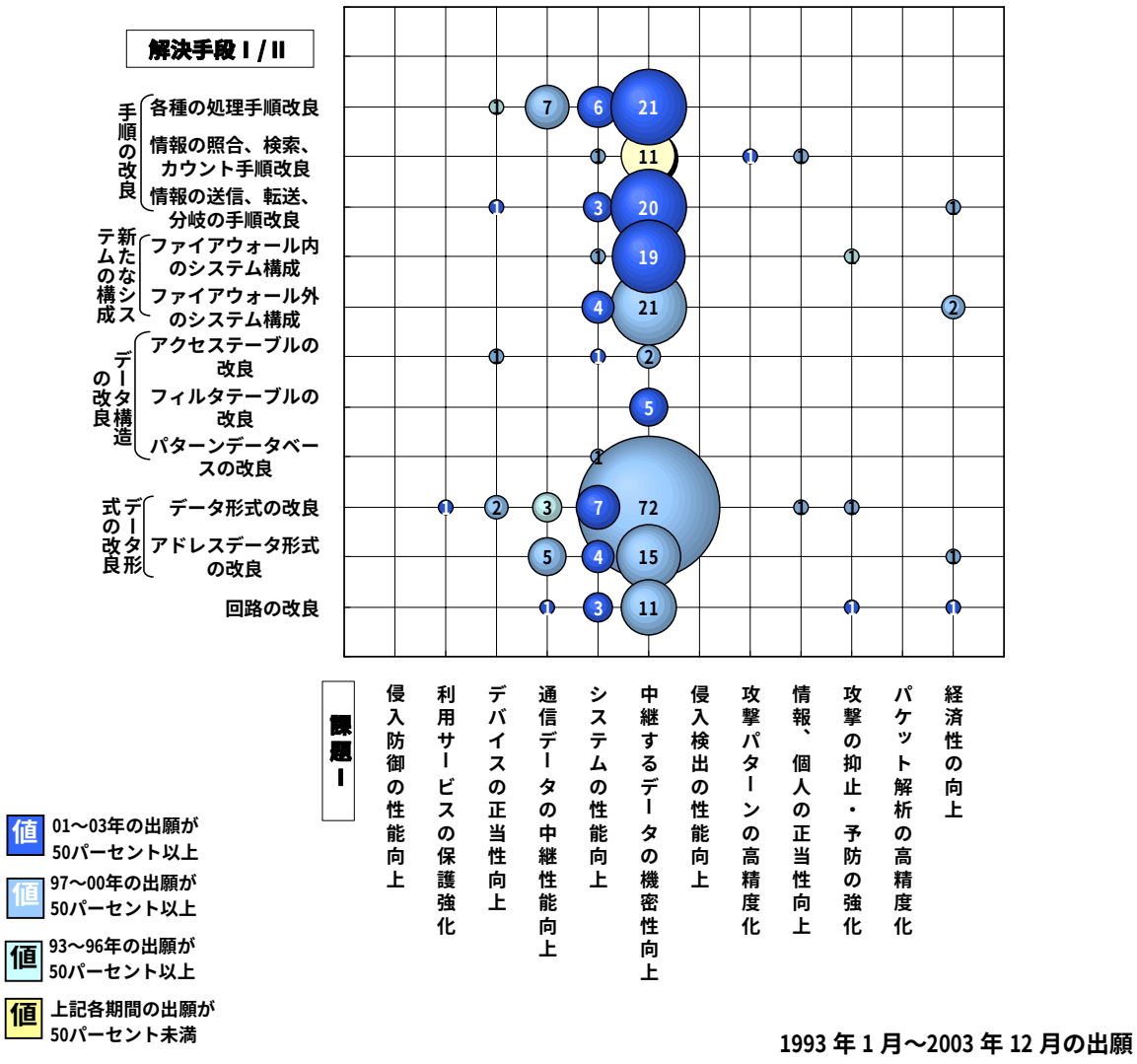


表1.4.6-1にトンネリング技術の課題に対する解決手段の詳細を示す。出願の多い課題は、中継するデータの機密性向上であり具体的には「使い易いセキュア通信の確立」と「機密性の適用範囲の拡大」と「暗号技術の強度向上」であり、さらにシステムの性能向上の「システム負荷の軽減」である。

使い易いセキュア通信の確立、機密性の適用範囲の拡大と暗号技術の強度向上の各課題に対して「データの変換」で多く対応している。

表 1.4.6-1 トンネリング技術の課題に対する解決手段の詳細

課題 I / 課題 II / 解決手段 II III		利用サービスの保護強化	デバイスの正当性向上	通信データの中継性能向上				システムの性能向上		中継するデータの機密性向上				攻撃パターンの高精度化	情報、個人の正当性向上	攻撃の抑止・予防の強化		経済性の向上	
		リソース保護の強化	成済ましの防止	アプリケーション層の中継機能拡大	経路生成の効率向上	ネットワーク層の中継機能拡大	トランスポート層の中継機能拡大	保守・信頼性の向上	システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上	暗号処理の効率化	プログラムを利用する攻撃パターンの精度向	情報の原本性向上	新たな攻撃の予防	速やかな攻撃からの回避	装置コストの低減	費用の低減
各種の処理手順改良	特定情報の記憶、登録手順								3	3	1	2	4						
	プロトコルの処理手順				6					1		1							
	応答コマンドの処理手順						1			1									
	各種処理の実行手順								2	1	1		2						
	特定情報の取得手順		1						1	3	1								
情報の照合、検索、カウント手順改良	特定情報の照合手順							1		1	2	5		1	1				
	特定情報の検索、抽出手順									2									
	特定情報のカウント手順												1						
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順		1							5	1	8	2						1
	情報転送の手順							2		3	1								
	設定値で分岐の手順								1										
ファイアウォール内のシステム構成	イントラネット内に機器の配置								1	8	2	2					1		
	DMZ に機器の配置									1	4		2						
ファイアウォール外のシステム構成	セキュリティサーバーの配置							1	3	8	5		4						1
	サービスサーバーの配置									4								1	
アクセステーブルの改良	アプリケーションとの関連付け		1																
	アクセスルールとの関連付け								1										
	認証情報との関連付け											1	1						
フィルタテーブルの改良	フイルタの追加									2									
	ポリシルールの追加、切換									1	2								
パターンデータベースの改良	攻撃パターンの追加、切換								1										
データ形式の改良	データに情報付加		1		3			1	1	6	2	2			1				
	データの変換	1	1						5	26	16	14	3			1			
	オブジェクトのデータ形式改良										1	1	1						
アドレスデータ形式の改良	アドレスの変換			1	2	2			3	7	3	2	1						1
	IP アドレスの割付							1			2								
回路の改良	スイッチ回路の追加				1			1		4	1	4					1	1	
	処理回路の改良								2			2							

1993 年 1 月～2003 年 12 月の出願

表1.4.6-2にトンネリング技術の課題に対する解決手段の出願人を示す。出願の多い中継するデータの機密性向上の「使い易いセキュア通信の確立」の課題に対する「データの変換」に関しては、キヤノンが３件、ソニーが２件出願している。その他は各１件の出願であるが、米国から６社の出願がある。

表 1.4.6-2 トンネリング技術の課題に対する解決手段の出願人(1/4)

課題 I / 課題 II / 解決手段 II　III		システムの性能向上	中継するデータの機密性向上		
		システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上
各種の処理手順改良	特定情報の記憶、登録手順	NEC ｿﾌﾄ,ﾌｼﾞﾀﾋﾞｼﾞﾈｽｼｽﾃﾑ,ｺｱ･ｼｽﾃﾑﾃﾞｻﾞｲﾝ,ﾌｼﾞﾀ(共願)特開 2003-309557 東芝　特許 3420002 富士ｾﾞﾛｯｸｽ 特開 2003-318873	ｿﾆｰ･ﾃﾞｨｽｸｱﾝﾄﾞﾃﾞｼﾞﾀﾙｿﾘｭｰｼｮﾝ 特開 2002-271313 日立製作所 (2) 特開 2004-056325 特開 2004-221922	三菱電機 ,日本電信電話(共願) 特開平 11-243388	ﾊﾟﾝﾌﾟｷﾝﾊｳｽ 特表 2002-087146 富士通 特許 3644579
	プロトコルの処理手順		ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2004-507977		ﾌｧｳｪｲ ﾃｸﾉﾛｼﾞｰｽﾞ(中国) 特開 2004-032744
	応答コマンド処理手順		日本電信電話 特開 2001-273256		
	各種処理の実行手順	ﾙｰｾﾝﾄ ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特許 3545988 松下電器産業 特開 2004-180234	ﾅｸﾞﾗﾋﾞｼﾞｵﾝ(ｽｲｽ) 特表 2004-537764	日本電気 特許 3575360	
	特定情報の取得手順	三菱電機 特開 2001-203678	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開平 10-200530 ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2005-110302 松下電器産業 特開 2005-184368	日本電信電話 特開 2005-149337	
情報の照合、検索、カウント手順改良	特定情報の照合手順		松下電工 特開 2005-117246	ｱｸｾﾚﾚｰｼｮﾝ ｿﾌﾄｳｪｱ ｲﾝﾀｰﾅｼｮﾅﾙ(米国),ｿｰｽﾈｸｽﾄ(共願) 特開 2002-204230 ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2005-072668	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) (2) 特許 2628619 特許 3024053 ﾄﾞｲﾂﾁｪ ﾃﾚｺﾑ(ﾄﾞｲﾂ) 特開平 10-020782 東芝　特開平 11-110353 日立国際電気 特開 2001-237896
	特定情報の検索、抽出手順		ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2002-304335 ｷﾔﾉﾝ　特開 2005-167608		
情報の送信、転送、分岐の手順改良	特定情報の通知、送信手順		三菱電機 特開 2002-344443 東芝　特開 2004-166238 日本電気 特許 3651424 日立製作所 特開 2005-020215 富士通 特開平 06-266670	富士通 特開 2003-101523	ｼｬｰﾌﾟ 特開 2002-271309 三菱電機 特開 2001-237824 松下電器産業 特開 2001-292135 村田機械 (2) 特開 2001-285273 特開 2001-285274 日本ﾋﾞｸﾀｰ 特開 2001-337921 日本電信電話 特開 2002-252607 富士ｾﾞﾛｯｸｽ 特開 2005-080249
	情報転送の手順		松下電器産業 特開 2003-304227 日本電信電話 特許 3566198 富士通 特開 2003-318992	日本電気 特開 2004-104542	
	設定値で分岐の手順	日本電気 特許 3603830			

1993 年 1 月～2003 年 12 月の出願

表 1.4.6-2 トンネリング技術の課題に対する解決手段の出願人(2/4)

課題 I / 課題 II / 解決手段 II III		システムの性能向上	中継するデータの機密性向上		
		システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上
ファイアウォール内のシステム構成	イントラネット内に機器の配置	日立製作所 特開 2001-331380	ｼﾞｪﾑﾌﾟﾘｭｽ(ﾌﾗﾝｽ) 特表 2005-518039 ｿﾆｰ 特開 2001-249899 九電情報ｻｰﾋﾞｽ 特開 2004-133804 三菱電機 (2) 特開 2004-328230 特開平 09-282281 東芝 (2) 特開平 11-122262 特開平 11-161618 富士通 特開 2002-044141	ｺﾞｰﾙﾄﾞｽﾀｲﾝ ﾍﾞﾝｼﾞｬﾐﾝ ﾃﾞｲ(米国) 特表 2001-507837 ﾎﾞﾙﾃｰﾙ・ｱﾄﾞﾊﾞﾝｽﾄ・ﾃﾞｰﾀ ・ｾｷｭﾘﾃｨ(ｲｽﾗｴﾙ) 特表 2001-506783	光電製作所 特開 2003-114853 東芝 特許 3629237
	DMZ に機器の配置		日本電気 特開 2004-328688	ｸﾎﾞﾀｼｽﾃﾑ開発 特許 3665311 村田機械 (2) 特開 2003-032236 特開 2003-032310 東芝 特開 2004-178486	
ファイアウォール外のシステム構成	セキュリティサーバーの配置	ﾄﾞｺﾓ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ﾗﾎﾞﾗﾄﾘｰｽﾞ ﾕｰ･ｴｽ･ｴｰ(米国) 特開 2003-338850 日本電信電話 特開 2004-312517 富士通 特開 2001-249866	ｴｲ･ﾃｨ･ｱﾝﾄﾞ･ﾃｨ(米国) 特開平 10-124427 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ 特開 2005-160005 ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ 特開平 11-041280 ｼｽﾃﾑ工学,高木 相(共願) 特開平 10-084338 三菱電機 (3) 特開 2001-320365 特開平 11-088436 特開平 11-308264 東日本電信電話 ,日立ｼｽﾃﾑｱﾝﾄﾞｻｰﾋﾞｽ(共願) 特開 2002-208921	ｻﾝ電子 特開 2001-306515 ﾕﾆｼｽ(米国) 特表 2003-514414 ﾘｺｰ 特開 2004-085627 村田機械 特開 2002-124940 日本電信電話 特開 2000-312203	
	サービスサーバーの配置		ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3489988 日本電気 (2) 特開 2002-033760 特許 3637863 日本電信電話 特開 2004-304532		
	アクセスルールとの関連付け	東芝 特開 2004-151964			
	認証情報との関連付け				東芝 特開 2002-149569
フィルタテーブルの改良	フイルタの追加		ﾏｲｸﾛｿﾌﾄ(米国) 特開 2005-027312 富士通 特開 2005-229651		
	ポリシルールの追加、切換		日本電信電話 特開 2005-063132	ｲﾝﾃﾙ(米国) 特開 2003-196567 ｹﾞｰｴﾑﾃﾞｰﾌｫﾙｼｭﾝｸﾞｽﾂｪﾝﾄﾙﾑｲﾝﾌｫﾙﾏ(ﾄﾞｲﾂ),富士通(共願) 特開 2002-101096	

1993 年 1 月～2003 年 12 月の出願

表 1.4.6-2 トンネリング技術の課題に対する解決手段の出願人(3/4)

課題 I / 課題 II / 解決手段 II III		システムの性能向上	中継するデータの機密性向上		
		システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上
パターンデータベースの改良	攻撃パターンの追加、切換	日立製作所 特許 3632167			
データ形式の改良	データに情報付加	三菱電機 特開 2003-179627	ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2005-174304 ﾔﾝ･ﾋﾟｰﾀｰ･ｸﾘｽﾃｨｱｰﾝ･ｽﾍﾟﾙﾄ･ﾌｧﾝ･ｳｰﾙ(ｵﾗﾝﾀﾞ) 特表 2003-526283 日本電気 特開 2003-143124 日本電信電話 特許 3457259 日立製作所 特開平 10-111855 富士通 特開平 07-030568	ｷﾔﾉﾝ 特開 2001-245163 ｼﾃｨﾊﾞﾝｸ ｴﾇ.ｴｲ.(米国) 特開 2001-060235	ｷﾔﾉﾝ 特開 2004-355471 ｼﾞｬﾊﾟﾝ･ｲﾝﾌｫﾒｰｼｮﾝ･ﾃｸﾉﾛｼﾞｰ,石ざき 利和(共願) 特開 2004-165976
	データの変換	KDDI 特開 2004-048479 ｼｬｰﾌﾟ 特開 2004-152278 ﾘｺｰ 特開 2003-304229 三菱電機 特開 2002-044135 日本電気 特開 2003-204326	ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ 特開 2002-319936 ｷﾔﾉﾝ (3) 特開 2002-009865 特開 2002-084318 特開 2002-353965 ｺｱｴｯｸｽﾒﾃﾞｨｱ(米国) 特表 2004-523937 ｻｲｴﾝｽ ｱﾌﾟﾘｹｰｼｮﾝｽﾞ ｲﾝﾀｰﾅｼｮﾅﾙ(米国) 特表 2004-507909 ｼﾞｪﾈﾗﾙ･ｲﾝｽﾂﾙﾒﾝﾄ(米国) 特表 2003-521834 ｽﾀｰﾘﾝｸﾞ ｺﾏｰｽ(米国) 特表 2004-508768 ｾｶﾞ 特開 2002-237812 ｾﾌﾞﾝ ﾈｯﾄﾜｰｸｽ(米国) 特表 2005-515664 ｿﾆｰ (2) 特開 2003-169055 特開 2005-027183 ﾃｸﾉﾌﾟﾛｼﾞｪｸﾄ 特開 2002-099511 ﾊﾟﾝﾌﾟｷﾝﾊｳｽ 特開平 11-168460 PFU 特開 2001-103096 ﾌﾟﾛﾑﾅｰﾄﾞ 特開 2003-244124 ﾏﾙｺｰﾆ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(米国) 特開平 10-233786 沖ﾃﾞｰﾀ 特開平 11-068735 三菱電機 特開平 09-252315 松下電器産業 特開 2002-176421	ｲﾙﾃﾞﾄ･ｱｸｾｽ(ｵﾗﾝﾀﾞ) 特表 2004-504765 ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特開 2003-132021 ｴｸｼﾝｸﾞ,ﾌﾞﾗｻﾞｰ工業(共願) 特許 3654712 ｵｰﾙﾀｰﾜﾝ(米国) 特許 3586203 ｻﾌｧｿﾌﾄ(韓国) 特表 2003-535398 ｾｲｺｰｴﾌﾟｿﾝ 特開平 11-252161 ｿﾆｰ 特開 2002-374245 ﾅｶﾖ通信機 特開 2005-159959 ﾊﾟｲｵﾆｱ 特開 2004-220399 ﾜｲﾄﾞﾊﾞｲﾝ･ﾃｸﾉﾛｼﾞｰｽﾞ(米国) 特表 2004-511931 沖電気工業 特開 2001-094600 関西ﾃｨｰ･ｴﾙ･ｵｰ 特開 2001-160092 松下電器産業 (2) 特開 2003-110603 特開 2003-198544 日立電線 ,大阪ﾒﾃﾞｨｱﾎﾟｰﾄ(共願) 特開 2002-271417 富士ｾﾞﾛｯｸｽ 特開 2002-190832	ｴﾇ･ﾃｨ･ﾃｨ･ﾌｧｼﾘﾃｨｰｽﾞ 特開 2004-110163 ｸｫｱﾙｺﾑ(米国) 特表 2004-521521 ｺｰﾆﾝｸﾚｯｶ ﾌｨﾘｯﾌﾟｽ ｴﾚｸﾄﾛﾆｸｽ(ｵﾗﾝﾀﾞ) 特表 2002-536888 ｽﾄﾚｲｼﾞ･ﾃｸﾉﾛｼﾞｰ(米国) 特表 2002-538702 ｿﾆｰ 特開平 11-355268 ﾀﾝﾌﾞﾙｳｨｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(米国) 特表 2002-521893 ﾄﾘﾆﾃｨｰｾｷｭﾘﾃｨｰｼｽﾃﾑｽﾞ 特開 2002-055604 ﾅｼﾌﾟﾆ ｳﾞﾗﾃﾞｲﾐｰﾙ ｳﾞﾗﾃﾞｲﾐﾛｳﾞｲﾂﾁ(ﾛｼｱ),ｸﾞﾛﾌ ｹﾞｵﾙｷﾞｰ ﾎﾞﾘｿｳﾞｨｯﾁ(ﾛｼｱ),ﾛﾊﾞﾉﾌ ｹﾞﾅﾃﾞｨ ﾊﾘﾄﾉｳﾞｨｯﾁ(ﾛｼｱ),ﾅｻﾞﾛﾌ ｳﾞﾗﾃﾞｨﾐｰﾙ ｳﾞｧｼﾘｴｳﾞｨｯﾁ(ﾛｼｱ)(共願) 特表 2004-534333 ﾌｧﾙｺﾝｼｽﾃﾑｺﾝｻﾙﾃｲﾝｸﾞ,白井 力(共願) 特開 2002-198955 三星電子(韓国) 特開 2004-282751 村田機械 (2) 特開 2001-285278 特開 2001-285280 日本電気 特開 2001-144773 矢崎総業 特開 2002-135240

1993 年 1 月～2003 年 12 月の出願

表 1.4.6-2 トンネリング技術の課題に対する解決手段の出願人(4/4)

課題 I / 課題 II / 解決手段 II III		システムの性能向上	中継するデータの機密性向上		
		システム負荷の軽減	使い易いセキュア通信の確立	機密性の適用範囲の拡大	暗号技術の強度向上
データ形式の改良	データの変換		松下電工 特開 2002-044068 鷹山 特開 2002-040939 中部日本電気ｿﾌﾄｳｪｱ 特開平 09-321749 日本電気 特開 2004-165761 日立製作所 特開 2001-337918 平野 宏一 特開 2002-077139		
	オブジェクトのデータ形式改良			ｱﾙｶﾃﾙ(ﾌﾗﾝｽ) 特開 2001-268074	日本電信電話 特開 2004-015582
アドレスデータ形式の改良	アドレスの変換	松下電器産業 特開 2002-344927 東日本電信電話 特開 2002-135313 日立製作所 特開 2000-232480	ｺﾝﾊﾟｯｸ･ｺﾝﾋﾟｭｰﾀ(米国) 特許 3343064 ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ(米国) 特開 2003-198561 古河電気工業 特開 2002-232450 三菱電機(2) 特開 2002-185540 特許 3259724 東洋通信機 特開 2001-333076 日本電気 特許 3596676	三菱電機 特開平 11-203222 日本電信電話 (2) 特開 2002-141939 特許 3597756	ﾌﾞﾘﾃｨｯｼｭ･ﾃﾚｺﾐｭﾆｹｰｼｮﾝｽﾞ(ｲｷﾞﾘｽ) 特表 2004-533749 日立製作所 特開 2000-349747
	IP アドレスの割付			ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国) 特許 3636095 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ 特開 2005-151295	
回路の改良	スイッチ回路の追加		三菱ﾏﾃﾘｱﾙ 特開 2002-271317 藤井 裕崇 特開 2004-178533 藤野 浩三 特開 2002-217996 福原 正樹 特開 2002-101085	ﾃﾚﾌｫﾝｱｸﾁｰﾎﾞﾗｹﾞｯﾄ ｴﾙ ｴﾑ ｴﾘｸｿﾝ(ｽｳｪｰﾃﾞﾝ) 特表 2001-517396	ｴﾇ･ﾃｨ･ﾃｨ･ﾄﾞｺﾓ (2) 特開 2001-177514 特開 2002-247113 三菱電機 特開 2001-274812 志賀 道夫 特開 2002-092499
	処理回路の改良	NEC ｴﾚｸﾄﾛﾆｸｽ 特開 2003-324423 日本電気ｴﾝｼﾞﾆｱﾘﾝｸﾞ 特開 2003-348171			ｱﾀﾞﾌﾟﾃｯｸ(米国) 特表 2005-503699 日立製作所 特表 2000-057290

1993 年 1 月～2003 年 12 月の出願

1.5 注目される特許

1.5.1 注目される特許の抽出

ここでは、本チャートが対象とする特許等において、①出願人自身により引用された文献公知発明、②特許公報・公告公報上に参考文献として掲載された特許文献、および③特許庁審査官の拒絶理由通知書に記載された先行技術文献の中で、引用頻度が５件以上の高い特許（外国特許および1993年以前の出願を含む）を紹介する。注目される特許を表1.5.1に示す。

表 1.5.1 注目される特許リスト(1/8)

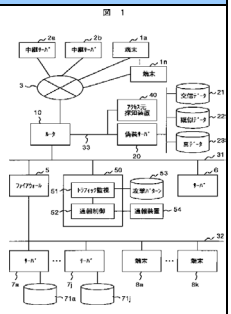
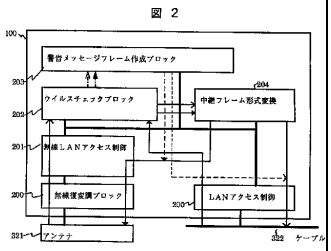
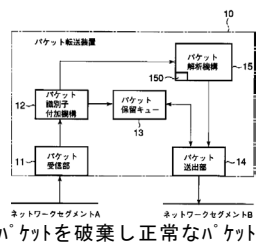
No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
1	特許 3618245 日立製作所 ネットワーク監視システム 99.03.09	14	0	14	三菱電機(3) 横河電機(3) 日本電気(2) 東芝(1) 富士通(1) KDDI(1) カシオ計算機(1) NEC フィールディング(1) ジェンズ(1)	外部ネットワークからルータを通過して流入するパケットのトラフィックを監視し内部情報ネットワークを不正にアクセスするパケットを検出した時ルータ装置宛に不正パケットの識別情報を示す制御パケットを送信するトラフィック監視装置と受信パケットに応答してパケットの送信元に意図的な情報を含む応答パケットを送信する偽装サーバとを有しルータが監視装置からの制御パケットの受信に応答して不正パケットの識別情報を記憶するための手段を備え外部ネットワークから受信されたパケットの中から識別情報に基づいて不正パケットを識別し、偽装サーバに転送することを特徴とするネットワーク監視システム 
2	特開平 09-269930 日立製作所 ネットワークシステムの防疫方法及びその装置 96.04.03	9	1	8	東芝(3) 日本電気(1) 富士通，エフ・エフ・シー(1) 富士通(1) 井上浩人，都築浩，柏木慎史(1) 野村総合研究所(1)	伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップとウイルスチェックステップにおいてウイルスが含まれると判断したデータの伝送路上の通過を阻止するフィルタリングステップとウイルスチェックステップで伝送路を流れるデータ中にウイルスを検出した場合警告メッセージをネットワークシステム上に送出する警告通報ステップと警告通報ステップによる警告メッセージジを受信し受信した警告メッセージに基づいてウイルスが検出されたことをユーザに知らせるための情報をコンピュータ上に表示する提示ステップとウイルスのフィルタリングステップにより阻止されたデータが受信先に到達しないことによる影響を処理する後処理ステップとを有することを特徴とするネットワークシステムの防疫方法。 
3	特開 2002-063084 東芝 パケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体 00.08.21	8	7	1	三菱電機(1)	第１のネットワークセグメントを介して受信した受信パケットを第２のネットワークセグメントに送出する際に予め設定された条件をもとに受信パケットの情報に第２のネットワークセグメントに接続された装置のソフトウエアに対し誤動作させる要因を含んでいるか否かを解析するパケット解析手段と解析手段によって前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に不正パケットを破棄し正常なパケットと判定した受信パケットのみを第２のネットワークセグメントに送出する手段とを具備してなることを特徴とするパケット転送装置。 

表 1.5.1 注目される特許リスト(2/8)

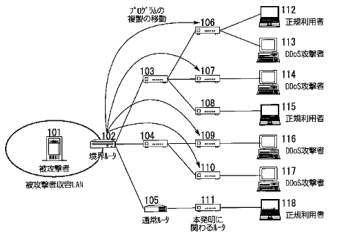
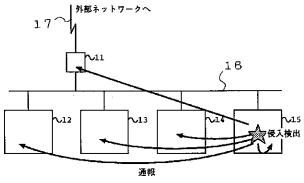
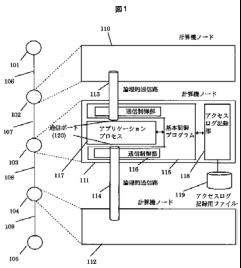
No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
3	特許 3549861 日本電信電話 分散型サービス不能攻撃の防止方法および装置ならびにそのコンピュータプログラム 00.09.12	8	3	5	富士通(2) 横河電機(1) 三菱電機(1) 東芝(1)	 分散型サービス不能攻撃を防止するための通信装置であって、通信装置を通過する通信パケットを監視し分散型サービス不能攻撃を検出するトラフィック監視機能部と、分散型サービス不能攻撃が検出された際に分散型サービス不能攻撃の通信パケットを破棄する攻撃防御モジュールと、攻撃元に近い上位側の通信装置のアドレスを検索する処理を行う攻撃元検索モジュールと、上位側の防御位置の通信装置に対して攻撃元検索モジュールを送信するモジュール送信部と、攻撃元検索モジュールによって検索された攻撃元に近い上位側の通信装置の候補中から上位側の防御位置とする通信装置を抽出する攻撃元判断機能部とを備え、モジュール送信部は、攻撃元判断機能部によって抽出された上位側の防御位置の通信装置に対して攻撃防御モジュールを送信するものであることを特徴とする通信装置。
5	特許 3165366 日立製作所 ネツトワークセキユリテイシステム 96.02.08	7	1	6	日立超ｴﾙ･ｴｽ･ｱｲ･ｼｽﾃﾑ(1) 横河電機(1) ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ（米国）(1) 日本電気(1) 日本電信電話(1) ｿﾆｰ(1)	図 1  ネットワークに接続された計算機を有するネットワークセキュリティシステムであって、計算機は、計算機の内部状態を監視し、異常の発生を検知する内部状態監視手段と、内部のリソースに対するアクセスの制御を行うアクセス制御手段とを備え、アクセス制御手段は、内部状態監視手段により異常の発生が検知されたとき、異常に関連した内部のリソースの保護処理を行うことを特徴とするネットワークセキュリティシステム。
5	特開平 10-164064 日立製作所 ネットワーク侵入経路追跡方式 96.12.05	7	1	6	横河電機(2) ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ(1) 三菱電機(1) ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ(1) ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ（米国）(1)	図1  通信ﾉｰﾄﾞ間を双方のﾉｰﾄﾞ上の通信ﾎﾟｰﾄのﾍﾟｱで接続する論理的通信路で構成するﾈｯﾄﾜｰｸｼｽﾃﾑにおいて、第一のﾉｰﾄﾞで、第二のﾉｰﾄﾞからの論理的通信路が確立したときに、第一のﾉｰﾄﾞは第二のﾉｰﾄﾞに対して通信路を確立したﾌﾟﾛｾｽの識別子とﾕｰｻﾞﾌﾟﾛｾｽが第三のﾉｰﾄﾞから論理的通信路を介して起動されたものである場合、通信ﾎﾟｰﾄの識別子と前記第三のﾉｰﾄﾞの識別子を要求し、これらの情報と第一のﾉｰﾄﾞ上で第二のﾉｰﾄﾞからの論理的通信路に対応する前記通信ﾎﾟｰﾄの識別子と対応するﾌﾟﾛｾｽの識別子とともに記録し、第一のﾉｰﾄﾞでｾｷｭﾘﾃｨ上の問題を検出した場合、第一のﾉｰﾄﾞ上の前記記録情報を参照することで、第二のﾉｰﾄﾞからの接続であることを認識し、第一のﾉｰﾄﾞ上の記録情報と第二のﾉｰﾄﾞ上で記録した同種の情報のうち第二のﾉｰﾄﾞに関するﾌﾟﾛｾｽの識別子と通信ﾎﾟｰﾄの識別子および通信相手ﾉｰﾄﾞの識別子を突き合わせて、一致したものを対応する記録情報とみなして第三のﾉｰﾄﾞの前記と同種の記録情報を参照にいくという手順を繰り返し侵入経路を特定することを特徴とするﾈｯﾄﾜｰｸ侵入経路追跡方式。

表 1.5.1 注目される特許リスト (3/8)

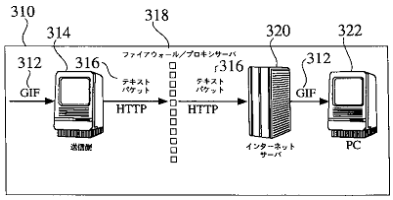
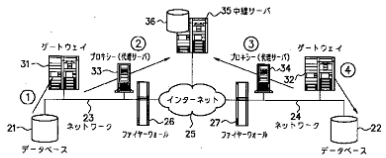
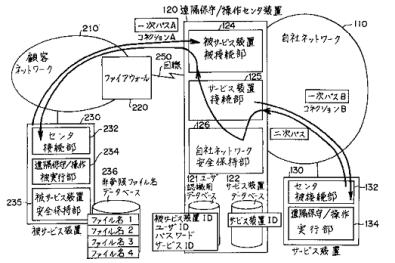
No	被引用特許文献番号 出願人 発明の名称 出願日 (対応日本特許)	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
5	特開平 10-154110 タンブルウィード コミュニケーションズ(米国) 電子文書引渡しシステム 96.10.24	7	1	6	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ (2) ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ (1) 山武(1) ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国)(1) 日立製作所(1)	 電子文書を引渡す装置であって、送信側コンピュータと、受信側コンピュータと、上記送信側コンピュータと受信側コンピュータとの間に挿入されているサーバと、を備え、電子文書が送信側コンピュータから上記サーバへ転送されると、サーバは上記電子文書の通知を受信側コンピュータへ送り、そして受信側コンピュータは転送された電子文書をサーバからダウンロードすることを特徴とする装置。
5	特開平 11-234270 日本電信電話 ネットワーク間のデータベースの複製･更新方法 98.02.16	7	0	7	ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ (1) ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ (1) ﾌｼﾞﾀ(1) ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ(米国)(1) 山武(1) 日本電気(1) 住友重機械工業(1)	 ファイヤーウォールにより中継ネットワークから分離された複数のネットワーク上のデータベース間でデータを複製・更新するネットワーク間のデータベースの複製・更新方法において、各ネットワーク上のゲートウェイを用いてデータベースの複製・更新のためのプロトコルと、ファイヤーウォールを越えてアクセス可能なプロトコルとの変換を行い、各ネットワーク上のプロキシー（代理サーバ）を経由し、中継ネットワーク上の中継サーバを介してデータを複製・更新することを特徴とするネットワーク間のデータベースの複製・更新方法。
9	特許 3262689 富士通 遠隔操作システム 95.05.19	6	0	6	日本電気(2) 東芝(1) 横河電機(1) NEC ｴﾝｼﾞﾆｱﾘﾝｸﾞ(1) 沖電気工業(1)	 外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置によって、外部ネットワークを介して遠隔操作サービスを実施される、外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、第二のファイアウォール及び第一のファイアウォールを介して、サービス装置との間にコネクションを確立し、コネクションを介してサービス装置との間でパケットを送受信するパケット通信手段と、パケット通信手段が受信したパケットから遠隔操作の指示情報を取り出し、指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、を備えたことを特徴とする被サービス装置。

表 1.5.1 注目される特許リスト(4/8)

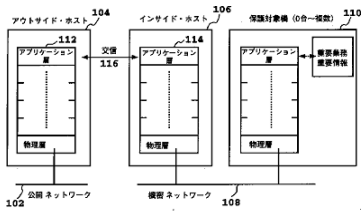
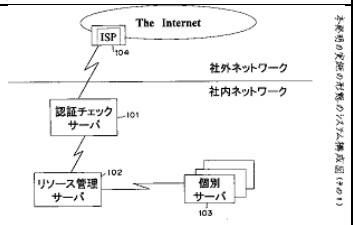
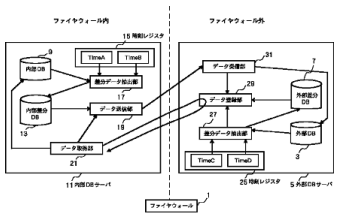
No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
9	特許 3180054 インターナショナル･ビジネス･マシーンズ(米国) ネツトワーク・セキユリテイ・システム 97.05.16	6	0	6	富士通(1) 日立国際電気(1) ｾｿﾞﾝ情報ｼｽﾃﾑｽﾞ(1) 中部日本電気ｿﾌﾄｳｪｱ(1) 日本電気(1) ｼｰｲｰｼｰ(1)	 外部のネットワークと接続されているシステムにおいて、外部ネットワークとの間でヘッダ付きパケットを送受信する第１のコンピュータと、第１のコンピュータと専用の通信路で接続されている第２のコンピュータとを含み、第１のコンピュータは、専用通信路を介してヘッダ付きパケットからヘッダを落としたパケットを第２のコンピュータに送信し、第２のコンピュータから専用通信路を介して受け取ったパケットにヘッダを付加して外部ネットワークに対して送信することを特徴とするネットワーク・セキュリティ・システム
9	特開平 11-338799 富士通 ネットワーク接続制御方法及びシステム 98.05.27	6	0	6	ｿﾆｰ(2) 松下電器産業(1) 日本電気(1) 東芝(1) 富士ｾﾞﾛｯｸｽ(1)	 外部ネットワークとローカルエリアネットワークを相互に接続するネットワーク接続制御方法であって、外部ネットワーク内のユーザによるローカルエリアネットワークへのアクセス時に、ユーザに対する認証チェックを実行し、認証チェックの結果に基づいて、ローカルエリアネットワーク内のリソースにアクセスするためのリソース要求をユーザから受信し、リソース要求と認証チェックの結果に基づいて、リソース要求によって要求されているローカルエリアネットワーク内のリソースに対するアクセス権を算出し、算出されたアクセス権に基づいてリソースにアクセスする、過程を含むことを特徴とするネットワーク接続制御方法。
9	特開 2000-076218 エヌ･ティ･ティ･データ データベース間の同期化システム 98.08.27	6	0	6	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ(2) NEC 情報ｼｽﾃﾑｽﾞ(2) 本田技研工業(1) 日本電気(1)	 ファイヤウォールによって互いに隔てられた内部データベースと外部データベースとを同期化するためのシステムにおいて、ファイヤウォール内に配置された内部データベースサーバと、ファイヤウォール外に配置された外部データベースサーバとを備え、内部データベースサーバが、内部データベース内で更新された内部データを外部データベースサーバへ提供するデータ提供部と、ﾌｧｲﾔｳｫｰﾙ外の所定場所に登録されている外部ﾃﾞｰﾀを、ﾌｧｲﾔｳｫｰﾙ内から主導的に取得し、取得した外部ﾃﾞｰﾀにより内部ﾃﾞｰﾀﾍﾞｰｽを更新するﾃﾞｰﾀ取得部とを有し、外部データベースサーバが、データ提供部が提供する内部データを受取り、受け取った内部データにより外部データベースを更新するデータ受取部と、前記外部データベース内で更新された外部データを、ファイヤウォール外の所定場所に登録するデータ登録部とを有したデータベース同期化システム。

表 1.5.1 注目される特許リスト(5/8)

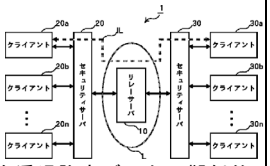
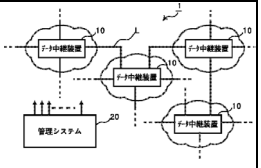
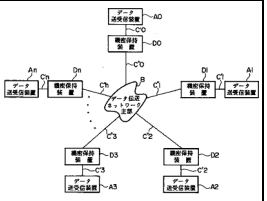
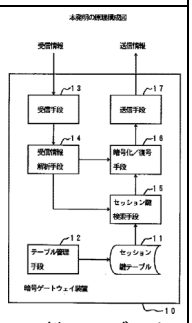
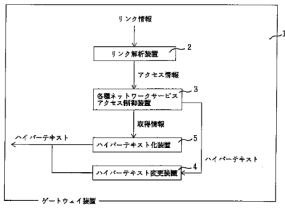
No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
9	特許 2998839 エヌ･ティ･ティ データ、 ドワンゴ(共願) データ通信方法、データ中継装置及び記録媒体 98.10.08	6	0	6	村田機械(5) 日本電気(1)	配下にある１又は複数の通信装置との間で所定形態の透過許容データのみの透過を許容するセキュリティ装置が介在する環境下で行うデータ通信方法であって、外部装置から特定の通信装置宛に送信された通信データを透過許容データに擬似的に変換してセキュリティ装置を透過させることを特徴とする 
9	特許 3483782 エヌ･ティ･ティ･データ 電子データの追跡システム及びデータ中継装置 98.10.15	6	2	4	三菱電機(2) ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ(1) 富士通(1)	電子データを流通させる装置が連鎖状に接続されたネットワーク上で電子データを運ぶデータリンク層の識別子を解析し、電子データが通過した装置を前記識別子の解析結果に基づいて特定する過程を含む、電子データの追跡方法。 
15	特開平 06-209313 フジクラ 機密保持装置およびその方法 93.01.12	5	0	5	三菱電機(2) 九州日本電気ｿﾌﾄｳｪｱ(1) 東芝(1) 三菱電機 ，日本電信電話(1)	複数のデータ送受信装置間でパケット通信を行うデータ伝送ネットワークにおいて、データ送受信装置と前記ネットワークの通信回線との間に接続され、データ送受信装置から通信回線へ向けて伝送されるパケットをパケットの宛先アドレスに対応した暗号化鍵を用いて暗号化する手段と、通信回線からデータ送受信装置へ向けて伝送されるパケットをパケットの送信元アドレスに対応した復号化鍵を用いて復号化する手段とを具備することを特徴とする機密保持装置。 
15	特許 3263877 日本電信電話 暗号ゲートウェイ装置 93.10.06	5	0	5	東芝(1) 三菱電機 ，日本電信電話（共願）(1) ﾜｰﾙﾄﾞﾄｰｸ（米国）(1) 日本電気(1) 三菱電機 (1)	受信情報を送信端末から受信し受信情報を暗号化又は復号し暗号化又は復号された送信情報を受信端末に送信する暗号ゲートウェイ装置において送信端末及び受信端末の識別情報と暗号化又は復号のためのセッション鍵の組を保持するセッション鍵テーブルと送信端末及び受信端末の識別情報とセッション鍵を該セッション鍵テーブルに登録するテーブル管理手段と受信情報から送信端末及び受信端末の識別情報と通信文を抽出する受信情報解析手段と抽出された識別情報を検索キーとしてセッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と抽出された識別情報と該当するセッション鍵に応じて通信文を暗号化又は復号して送信情報を作成する暗号化復号手段とから成りセッション鍵検索手段による検索の結果セッション鍵テーブルに該当するセッション鍵が無い場合には通信文を原文のまま送信する構成としたことを特徴とする暗号ゲートウェイ装置。 
15	特開平 08-044643 富士通 ゲートウェイ装置 94.07.27	5	1	4	日本電気(1) ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ(1) ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ（米国）(1) 日本電信電話(1)	ハイパーテキストのリンクの置き換えをするリンク置き換え処理手段と、リンクの変更をするリンク変更処理手段とをハイパーテキスト変更装置に備え、リンク置き換え処理手段がハイパーテキストを受け取ると、リンク変更処理手段でハイパーテキスト中のリンク情報を特定の処理手段に従って変更した後、リンク置き換え処理手段がリンク情報変更後のハイパーテキストを出力するようにするハイパーテキスト変更装置を備えることを特徴としたゲートウェイ装置。 

表 1.5.1 注目される特許リスト(6/8)

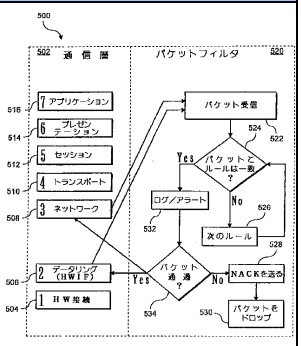
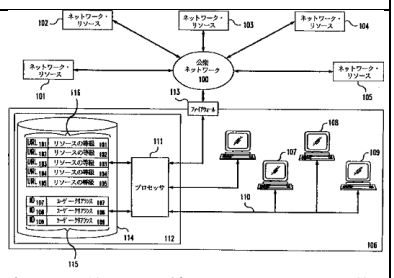
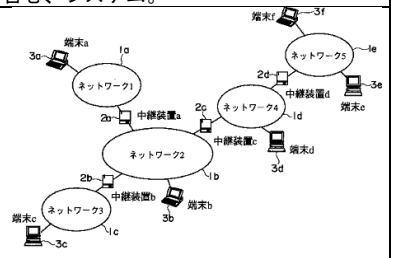
No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
15	特開平 08-044642 チエック･ポイント･ソフトウェア･テクノロジーズ（イスラエル） コンピュータネツトワークの制御方法及び保安システム 93.12.15	5	0	5	松下電器産業(2) 日本電気(1) 日本電信電話(1) ルーセント テクノロジーズ（米国）(1)	データがデータパケットとして扱われるコンピュータネットワークにおけるデータパケットの伝送を保安ルールに従って制御するための、下記段階を含む方法：ａ）保安ルールにより制御されるネットワークの夫々のアスペクトの定義を発生する段階；  ｂ）アスペクトの内の少くとも一つを制御するためにアスペクト定義で保安ルールを発生する段階； ｃ）データパケットの伝送を制御するパケットフィルタリングモジュールの動作を制御するために保安ルールをーセットのフィルタ言語命令に変換する段階； ｄ）ルールに従ってデータパケットの伝送を制御するために、パケットフィルタリング仮想計算機をつくるパケットフィルタモジュールを少くとも一つのネットワークエンティティに設ける段階； ｅ）ネットワーク内の上記パケットの伝送を許可または拒否するためにパケットフィルタリングモジュール仮想計算機を動作させるためにモジュールが命令を読取りそして実行する段階。
15	特開平 09-026975 エイ･ティ･アンド･ティ（米国） データベース・アクセス管理のためのシステムと方法 95.06.06	5	0	5	日本電気(2) 日立製作所(1) NEC ソフト(1) アッパ ルーサ インターアクティヴ（米国）(1)	 １つかそれ以上の、それ以外の点では公衆の情報リソースへのアクセスを選択的に制限するためのシステムであって、複数のリソースの識別子の各々を少なくとも１つのリソースの等級と関連させる第１の記憶されたリストと、複数のユーザー識別コードの各々を少なくとも１つのユーザー・クリアランスの等級と関連させる第２の記憶されたリストとを含む関連データベースと、リソースの識別子とユーザー識別コードを含む、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの要求を受信するために適用され、さらに関連データベースの中の第１、第２リストを照会し、第１リストの中の受信されたリソースの識別子と関連して示されたリソースの等級と、第２リストの中の受信されたユーザー識別コードと関連して示されたユーザー・クリアランスの等級との相関として、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの要求を実行するために適用されたプロセッサとを含む、システム。
15	特開平 10-028144 日立製作所 アクセス制御機能付きネツトワーク構成方式 96.07.12	5	0	5	日本電気(2) アテンションシステム(1) エヌ･ティ･ティ･データ(1) ルーセント テクノロジーズ（米国）(1)	 少なくとも一の計算機が接続された複数のネットワークを中継装置を介して接続したネットワーク構成方式において、ユーザが保有する諸属性に応じて、ユーザ毎にアクセス可能な計算機および／またはネットワーク等の利用領域を定義することができる手段を設けたことを特徴とするアクセス制御機能付きネットワーク構成方式。

表 1.5.1 注目される特許リスト(7/8)

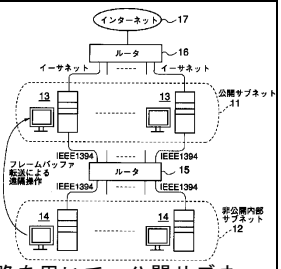
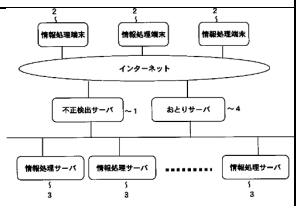
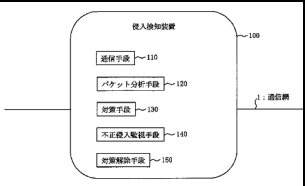
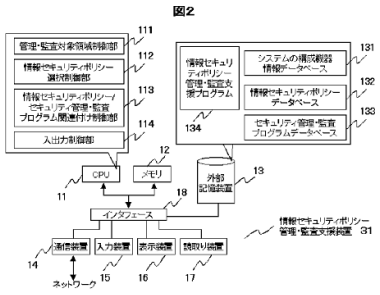
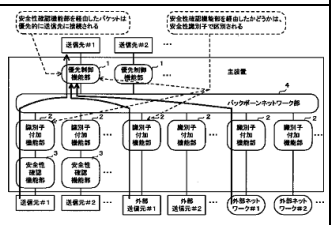
No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
15	特開 2000-354056 東芝 計算機ネツトワークシステムおよびそのアクセス制御方法 99.06.10	5	0	5	住友重機械工業(1) 日本電気(1) 日新電機(1) 日本放送協会,ﾚｸｻｽ(1) ﾀﾞｲｷﾝ工業(1)	 外部ネットワークに接続された公開サブネットと、この公開サブネットを介して外部ネットワークのサービスを受ける非公開内部サブネットとに分割された計算機ネットワークシステムにおいて、リードトランザクションとライトトランザクションが定義された通信路を用いて、公開サブネットと非公開内部サブネット間を接続する接続手段と、非公開内部サブネット内の計算機から前記外部ネットワークのサービスを利用できるようにするために、画面情報および入力情報を共有するためのフレームバッファ転送を用いて、非公開内部サブネット内の計算機から公開サブネット内の計算機を遠隔操作する遠隔操作手段とを具備し、遠隔操作手段は、フレームバッファ転送を用いた遠隔操作を、非公開内部サブネット内の計算機から公開サブネット内の計算機へのリードトランザクションおよびライトトランザクションによって実行することを特徴とする計算機ネットワークシステム。
15	特開 2002-007234 三菱電機 不正メツセージ検出装置、不正メツセージ対策システム、不正メツセージ検出方法、不正メツセージ対策方法、及びコンピュータ読み取り可能な記録媒体 00.06.20	5	1	4	KDDI(1) ﾗｯｸ(1) 日本電気(1) ｼﾞｪﾝｽﾞ(1)	 第一の情報処理装置と第二の情報処理装置とに接続され、第二の情報処理装置を送信先として第一の情報処理装置から送信されたメッセージを受信し、受信したメッセージから、第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置であって、第一の情報処理装置から送信されたメッセージを受信する通信手段と、通信手段により受信されたメッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段とを有することを特徴とする不正メッセージ検出装置。
15	特開 2002-073433 三菱電機 侵入検知装置及び不正侵入対策管理システム及び侵入検知方法 00.08.28	5	1	4	沖電気工業(2) KDDI(1) ｷｰｳｪｱ ｿﾘｭｰｼｮﾝｽﾞ,ｾｷｭｱﾌｨｯｸｽ(1)	 パケットを送受信する通信部と、通信部が受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析部と、パケット分析部が不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策部とを備えることを特徴とする侵入検知装置。

表 1.5.1 注目される特許リスト(8/8)

No	被引用特許文献番号 出願人 発明の名称 出願日 （対応日本特許）	被引用回数	自社特許数	他社特許数	引用した特許の出願人	概要
15	特開 2001-273388 日立製作所 セキュリティ管理システムおよび方法 00.01.20	5	0	5	ﾘｺｰ(3) 三菱電機(1) 三菱電機 ,三菱電機情報ﾈｯﾄﾜｰｸ(共願)(1)	 情報システムを構成する複数の被管理対象システムのセキュリティ状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理システムであって、少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、対応する被管理対象システムのセキュリティ状態を、対応する情報セキュリティポリシーに整合するように制御する、複数の管理手段と、情報セキュリティポリシー、被管理対象システムおよび管理手段の対応を登録したデータベースと、ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付手段と、データベースから、セキュリティ内容受付手段が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている管理手段を抽出する抽出手段と、抽出手段が抽出した管理手段に、管理手段に対応する被管理対象システムのセキュリティ状態を、管理手段に対応する情報セキュリティポリシーに整合するように変更させる管理制御手段と、を有することを特徴とするセキュリティ管理システム。
15	特開 2002-158699 日本電信電話 DoS 攻撃防止方法および装置およびシステムおよび記録媒体 00.11.20	5	2	3	横河電機(1) 富士通(1) ｿﾆｰ(1)	 通信パケットに対して施した安全性確認の度合いに応じて、通信パケットに異なる種類の安全性識別子を付加し、通信パケットの配送経路上で前記安全性識別子に応じた優先度制御を行うことを特徴とするＤｏＳ攻撃防止方法。

1.5.2 注目される特許の課題と解決手段

1.5.1で抽出した25件の注目される特許における技術開発の課題と解決手段の関係を表1.5.2に示す。注目される特許は、課題と解決手段で集中したものはなく、幅広く分布している。

表 1.5.2 注目される特許の課題と解決手段および被引用回数(1/2)

課題Ⅰ / 解決手段Ⅱ	侵入防御の性能向上	利用サービスの保護強化	デバイスの正当性向上	通信データの中継性能向上	システムの性能向上
各種の処理手順の改良				特開平 11-234270 （日本電信電話） [7 回] 特開平 08-044643 （富士通） [5 回]	
情報の照合、検索、カウント手順の改良					
情報の送信、転送、分岐の手順の改良				特許 2998839 （ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ、ﾄﾞﾜﾝｺﾞ）（共願） [6 回]	
ファイアウォール内のシステム構成				特開平 10-154110 （ﾀﾝﾌﾞﾙｳｨｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ（米国）） [7 回] 特開 2000-354056 （東芝） [5 回]	特許 3262689 （富士通） [6 回]
アクセステーブルの改良	特開平 09-026975 （ｴｲ･ﾃｨ･ｱﾝﾄﾞ･ﾃｨ（米国）） [5 回] 特開平 10-028144 （日立製作所） [5 回]	特開平 11-338799 （富士通） [6 回]			
フィルタテーブルの改良	特開 2001-273388 （日立製作所） [5 回]				
データ形式の改良	特許 3180054 （ｲﾝﾀｰﾅｼｮﾅﾙ･ﾋﾞｼﾞﾈｽ･ﾏｼｰﾝｽﾞ（米国）） [6 回]		特開 2002-158699 （日本電信電話） [5 回]	特開 2000-076218 （ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ） [6 回]	
回路の改良					
件数 回数	5 件 21 回	1 件 6 回	1 件 5 回	6 件 36 回	1 件 6 回

表 1.5.2 注目される特許の課題と解決手段および被引用回数(2/2)

課題Ⅰ ＼ 解決手段Ⅱ	中継するデータの機密性向上	侵入検出の性能向上	攻撃パターンの高精度化	攻撃の抑止・予防の強化	件数 被引用回数
各種の処理手順改良					2 件 12 回
情報の照合、検索、カウント手順改良		特許 3483782 （ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ） [6 回]		特許 3549861 （日本電信電話） [8 回]	2 件 14 回
情報の送信、転送、分岐の手順改良			特開平 08-044642 (ﾁｪｯｸ･ﾎﾟｲﾝﾄ･ｿﾌﾄｳｪｱ･ﾃｸﾉﾛｼﾞｰｽﾞ（ｲｽﾗｴﾙ)) [5 回]	特開平 09-269930 （日立製作所） [9 回]	3 件 20 回
ファイアウォール内のシステム構成		特許 3618245 （日立製作所） [14 回] 特開 2002-007234 （三菱電機） [5 回]			5 件 37 回
アクセステーブルの改良		特開平 10-164064 （日立製作所） [7 回]			4 件 23 回
フィルタテーブルの改良					1 件 5 回
データ形式の改良	特開平 06-209313 （ﾌｼﾞｸﾗ） [5 回] 特許 3263877 （日本電信電話） [5 回]	特開 2002-063084 （東芝） [8 回]			6 件 35 回
回路の改良				特許 3165366 （日立製作所） [7 回] 特開 2002-073433 （三菱電機） [5 回]	2 件 12 回
件数 回数	2 件 10 回	5 件 40 回	1 件 5 回	4 件 29 回	

1.5.3 注目される特許の関連図

図1.5.3-1に、特許3618245の引用関連図を示す。この特許の出願人は日立製作所で、発明の名称は「ネットワーク監視システム」で、不正アクセスを検知する基礎となる監視の技術に関するものである。引用された出願の多い出願人は、横河電機(３件)、三菱電機(３件)、日本電気(２件)である。

図 1.5.3-1 特許 3618245 の引用特許関連図

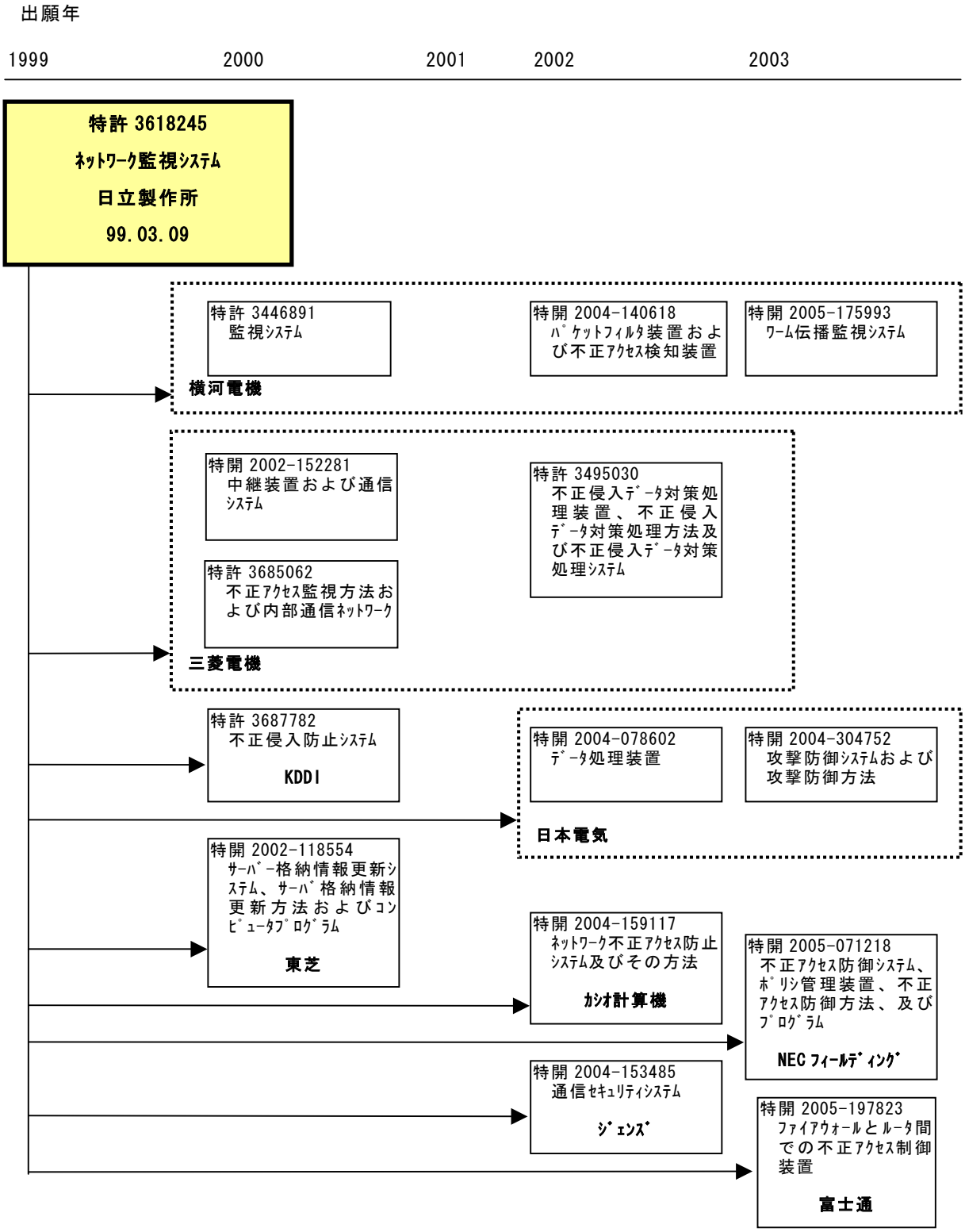


図1.5.3-2に、特開平09-269930の引用関連図を示す。この特許の出願人は日立製作所で、発明の名称は「ネットワークシステムの防疫方法及びその装置」で、不正アクセスを検知する基礎となるウイルスの検知の技術に関するものである。引用された出願の多い出願人は、東芝(３件)である。

図 1.5.3-2 特開平 09-269930 の引用特許関連図

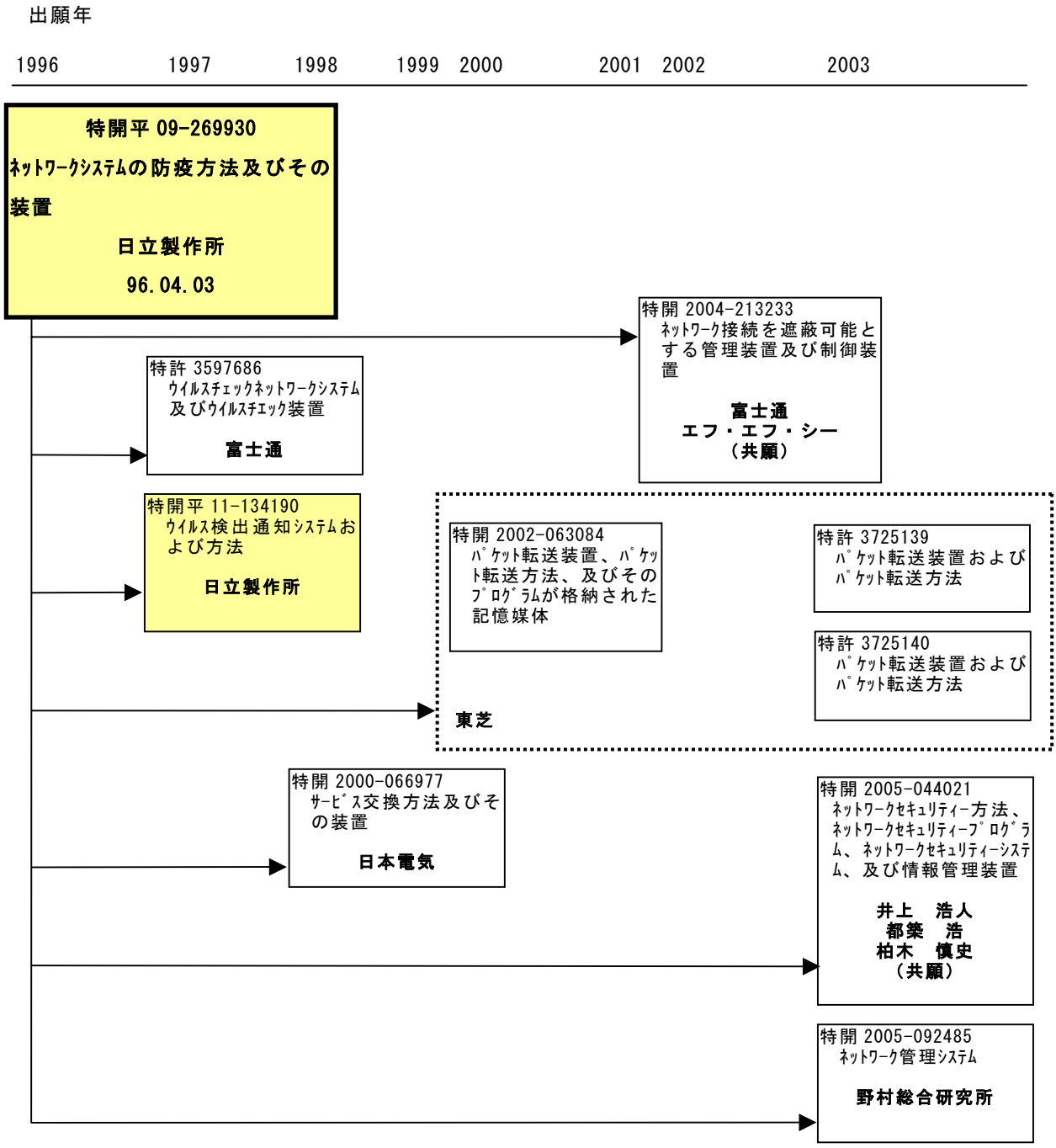
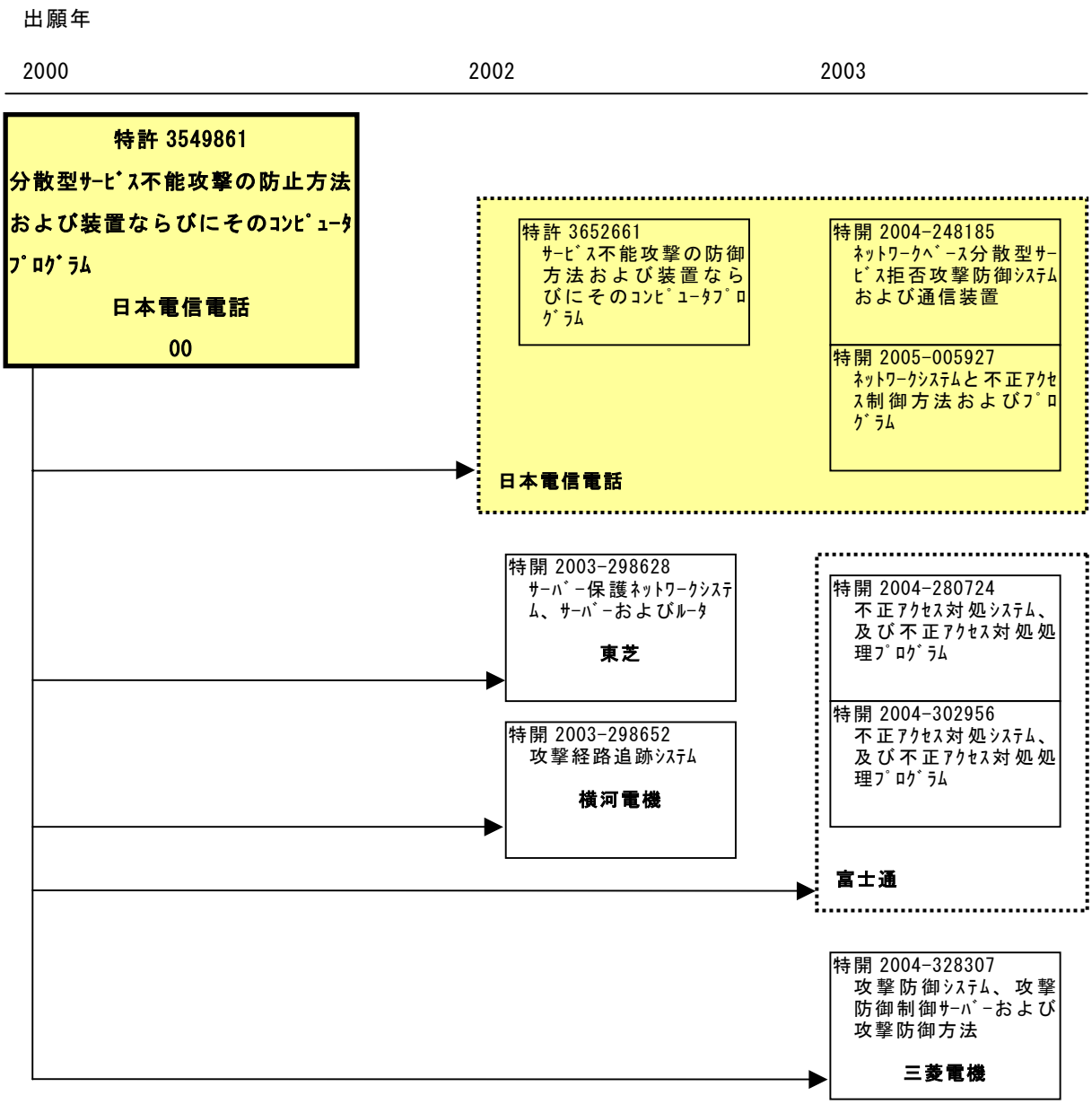


図1.5.3-3に、特許3549861の引用関連図を示す。この特許の出願人はNTTで、発明の名称は「分散型サービス不能攻撃の防止方法および装置ならびにそのコンピュータプログラム」で、DDOS攻撃の検知とその防御の技術に関するものである。引用された出願の多い出願人は、NTT(３件)、富士通(２件)である。

図 1.5.3-3 特許 3549861 の引用特許関連図



２．主要企業、大学・公的研究機関等の特許活動

2.1　日本電信電話(NTT)
2.2　日立製作所
2.3　日本電気
2.4　東芝
2.5　富士通
2.6　三菱電機
2.7　松下電器産業
2.8　ソニー
2.9　キヤノン
2.10 インターナショナル・ビジネス・マシーンズ(IBM、米国)
2.11 富士ゼロックス
2.12 リコー
2.13 マイクロソフト(米国)
2.14 エヌ・ティ・ティ・データ(NTT データ)
2.15 沖電気工業
2.16 サン・マイクロシステムズ(米国)
2.17 横河電機
2.18 エヌ・ティ・ティ・ドコモ(NTT ドコモ)
2.19 セイコーエプソン
2.20 ヒューレット・パッカード(米国)
2.21 ルーセント　テクノロジーズ(米国)
2.22 大学・公的研究機関
2.23 主要企業等以外の特許番号一覧

特許流通
支援チャート

2．主要企業、大学・公的研究機関等の特許活動

主要企業、大学・公的研究機関ごとに、製品や研究内容の紹介をし、保有している不正アクセス侵入検知防御技術の特許をリストにして示す。

1993年１月から2003年12月までに出願された不正アクセス侵入検知防御技術に関し、出願件数が20件以上の出願人は21社あり、表２に示す。この主要企業21社の出願件数は1,282件で、全体の58%を占めている。そのうち登録された特許は165件である。

ここでは、表２に示した主要企業21社について、下記のような紹介や解析を行う。

1) 企業概要、不正アクセス侵入検知防御技術に関する取扱い例、不正アクセス侵入検知防御技術に関係する主要製品・技術の紹介を行う。

2) 主要企業が保有する特許の発明者とその住所から、主要企業の発明者数と開発拠点を示す。なお、開発拠点については、公報に記載の発明者の住所を参考にした。

3) 主要企業が保有する特許を、技術要素と課題の分布と課題と解決手段の分布を作成して示す。

4) 主要企業が保有する特許を、技術要素別の課題対応のリストにして示す。

一方、大学・公的研究機関等の出願は少なく、21社の後にまとめて全出願を紹介する。

主要企業の技術要素別課題対応特許のリストで登録された出願は、概要と図入りで示されている。経過情報については、2006年１月末の状況を掲載しており、最近特許になったものは特許番号のみを表示している。主要企業以外の技術要素別課題対応特許のうち、登録された特許も、概要入りで示されている。

本書に掲載されている各企業の保有特許は、すべてがライセンス可能な開放特許であるとは限らない。開放特許にするか、ライセンスの可能性のない非開放特許にするかは、各企業の特許戦略による。

表2 不正アクセス侵入検知防御技術の主要出願人21社

№	出願人名	出願件数	№	出願人名	出願件数
1	日本電信電話	197	12	リコー	30
2	日立製作所	152	13	マイクロソフト(米国)	27
3	日本電気	131	14	エヌ･ティ･ティ･データ	25
4	東芝	124	15	沖電気工業	23
5	富士通	116	16	サン・マイクロシステムズ(米国)	23
6	三菱電機	90	17	横河電機	22
7	松下電器産業	61	18	エヌ･ティ･ティ･ドコモ	22
8	ソニー	52	19	セイコーエプソン	21
9	キヤノン	48	20	ヒューレット・パッカード(米国)	21
10	インターナショナル・ビジネス・マシーンズ(米国)	48	21	ルーセント テクノロジーズ(米国)	21
			22	大学・公的研究機関等	15
11	富士ゼロックス	31			

2.1 日本電信電話

2.1.1 企業の概要

商号	日本電信電話　株式会社
本社所在地	〒100-8116　東京都千代田区大手町 2-3-1
設立年	1985 年（昭和 60 年）
資本金	9,379 億 50 百万円（2005 年 3 月末）
従業員数	2,792 名（2005 年 3 月末）（連結：201,486 名）
事業内容	NTT グループ会社の発行株式の引き受け・保有、NTT グループ会社への助言・あっせん・援助、電気通信技術に関する研究、これらの付帯業務

日本電信電話(NTT)は、NTT 東日本、NTT 西日本や NTT コミュニケーション等の持株会社であり、電気通信の基盤となる電気通信技術に関する研究を行っている。研究開発活動では、次世代ネットワークの構築に向けた基盤技術の創出と先端基礎技術の開発に取組んでいる。(出典：http://www.ntt.co.jp/)

2.1.2 製品例

NTT は、電話から IP へのパラダイムシフトに対応し、長い歴史のある電話事業で培ってきたネットワーク技術と最先端の IP 技術とを融合して、品質、セキュリティが保証された信頼性の高い､インターネットと電話網のメリットを兼ね備えた次世代 IP ネットワークの実現に向けた研究開発を進めている。表 2.1.2 に研究開発例を示す。

表 2.1.2 NTT の不正アクセス侵入検知防御技術に関する研究開発例

研究開発	概要・特徴
HIKARI GATE (NTT の登録商標)	① ネットワークのことを知らないユーザに使用してもらうため簡単、快適、安全なホームゲートウェイで、ネットワーク自動設定、フィルタの動的設定をするファイアウォールを実装している。 ② 保守は、VPN を用いたリモートメインテナンス。 ③ 映像配信の広帯域の要求、VOIP の低遅延の要求に対応する QOS(Quality Of Service)。
Moving Firewall 技術の実地検証	米国で Ddos 攻撃対策で豊富な経験を持つ Verio 社の協力を得て Web サイトでのトライアルを米国で行った。
世界最高速処理ﾌｧｲｱｳｫｰﾙの研究	① 10Gbit/s の高速処理が可能なファイアウォール機能を実現した。 ② Ddos 攻撃やワーム攻撃など多量のパケットを識別､転送処理をするボードで、新しい攻撃に対応する機能変更や追加を容易にした。

(出典：http://www.ntt.co.jp/)

2.1.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

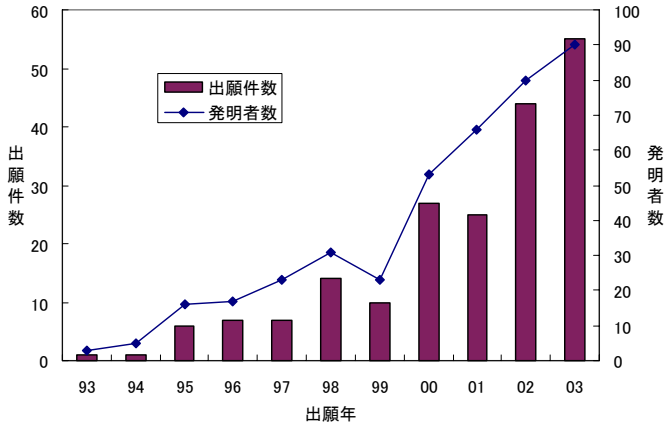
東京都新宿区西新宿 3 丁目 19 番 2 号 日本電信電話株式会社内

東京都千代田区大手町 2 丁目 3 番 1 号 日本電信電話株式会社内

東京都千代田区内幸町 1 丁目 1 番 6 号 日本電信電話株式会社内

図 2.1.3 に、NTT の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。1999 年までは 10 件前後の出願件数であったが、以降急激に増加し、03 年には 50 件を越え、発明者は 90 人に達している。

図 2.1.3 NTT の不正アクセス侵入検知防御技術に関する出願件数と発明者数



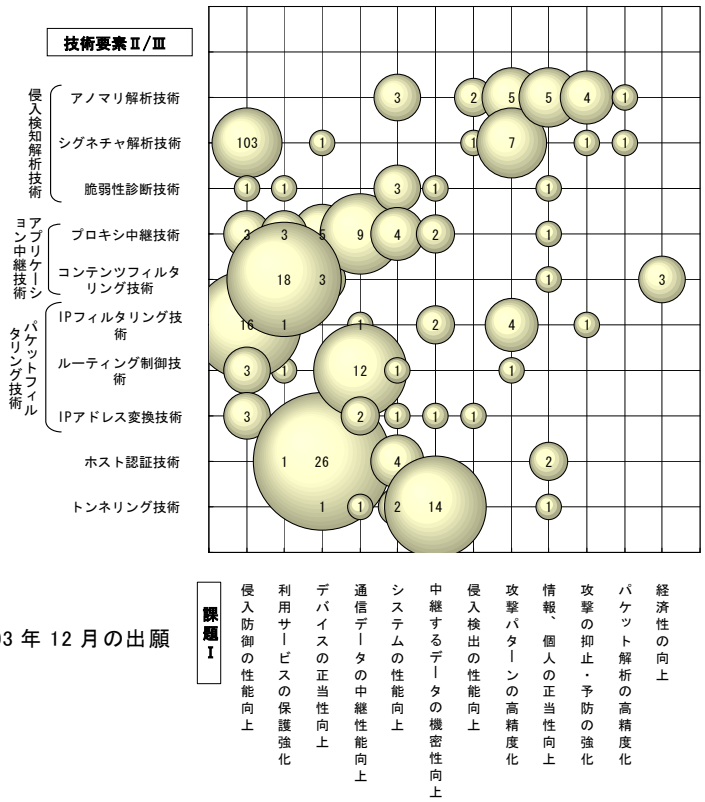
2.1.4 技術開発課題対応特許の概要

図 2.1.4-1 に、NTT の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図 2.1.4-2 に、NTT の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

ホスト認証技術が最も多く出願され、次いでプロキシ中継技術、IP フィルタリング技術とコンテンツフィルタリング技術に関する出願が多い。これらの出願のうち、最も多い課題は、「デバイスの正当性向上」であり、次いで多い課題は「侵入防御の性能向上」である。

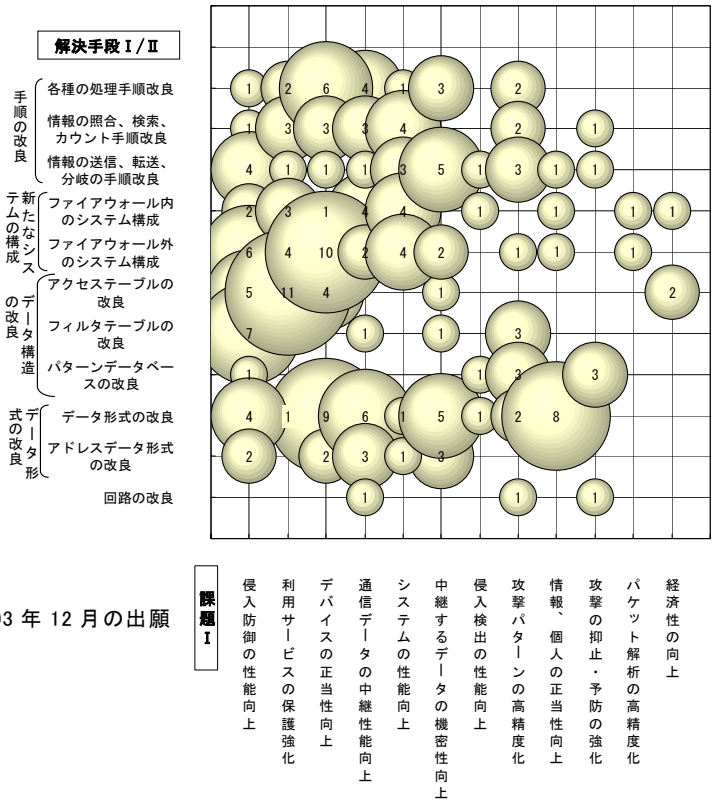
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。次いで「デバイスの正当性向上」の課題に対しては、「ファイアウォール外のシステム構成」で多く対応し、さらに「データ形式の改良」でも多く対応している。

図 2.1.4-1 NTT の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993 年 1 月～2003 年 12 月の出願

図 2.1.4-2 NTT の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993 年 1 月～2003 年 12 月の出願

表 2.1.4 NTT の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は 197 件で、そのうち 28 件が登録特許である。なお、表 2.1.4 では図 2.1.4-2 の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表 2.1.4 NTT の技術要素別課題対応特許(1/25)

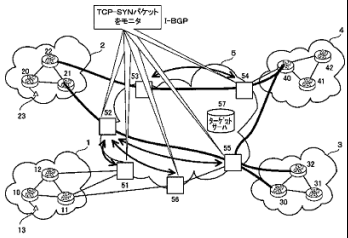
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	システムの性能向上	情報の照合、検索、 ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾄﾗﾌｨｯｸ	特開 2003-298655 02.04.05 H04L12/56,400	ｻｲﾄ領域内ﾎﾞﾄﾙﾈｯｸ特定方法
		情報の送信、転送、 分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開 2004-166029 02.11.14 H04L12/66	分散型ｻｰﾋﾞｽ拒絶防御方法およびｼｽﾃﾑ、ならびにそのﾌﾟﾛｸﾞﾗﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特開 2004-120498 02.09.27 H04L12/56,400	違法ﾄﾗﾋｯｸ防止ｼｽﾃﾑおよびｻｰﾊﾞおよびｴｯｼﾞﾙｰﾀ
	侵入検出の性能向上	情報の送信、転送、 分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開 2005-159551 03.11.21 H04L12/66	ﾈｯﾄﾜｰｸ攻撃対策方法およびそのﾈｯﾄﾜｰｸ装置、ならびにそのﾌﾟﾛｸﾞﾗﾑ
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開 2004-355287 03.05.28 G06F13/00,351	不正要求防御装置および方法
	攻撃パターンの高精度化	情報の照合、検索、 ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾊﾟｹｯﾄ	特開 2004-320636 03.04.18 H04L12/56,100	DoS 攻撃元検出方法、DoS 攻撃阻止方法、ｾｯｼｮﾝ制御装置、ﾙｰﾀ制御装置、ﾌﾟﾛｸﾞﾗﾑおよびその記録媒体
		情報の送信、転送、 分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開 2002-247114 01.02.14 H04L12/66	ｹﾞｰﾄｳｪｲ装置における過負荷防御方法及びその装置
			特許 3643087 02.03.28 H04L12/66	通信網およびﾙｰﾀおよび分散型ｻｰﾋﾞｽ拒絶攻撃検出防御方法 ﾎﾞｰﾀﾞﾙｰﾀは、自通信網に流入するｺﾈｸｼｮﾝ確立要求を含む TCP-SYN ﾊﾟｹｯﾄを監視する手段を備え、この監視する手段は、同一宛先ｱﾄﾞﾚｽを有する TCP-SYN ﾊﾟｹｯﾄの個数を計数する手段と、この計数する手段の計数結果を他ﾎﾞｰﾀﾞﾙｰﾀに通知する手段と、他ﾎﾞｰﾀﾞﾙｰﾀからの前記計数する手段の計数結果を受け取る手段と、この受け取る手段により受け取った他ﾎﾞｰﾀﾞﾙｰﾀにおける計数結果および前記計数する手段による自ﾎﾞｰﾀﾞﾙｰﾀの計数結果に基づき計数結果を集計する手段とを備え、この集計する手段は、前記計数結果の所定時間内の増加率を検出する手段と、この検出する手段の検出結果が閾値を超えるときには前記同一宛先ｱﾄﾞﾚｽの情報を含む警報を発出する手段とを備えたことを特徴とする通信網。 
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 ﾘﾀｰﾝｱﾄﾞﾚｽ蓄積	特開 2004-334607 03.05.09 G06F15/00,330 [被引用回数 1]	不正ｱｸｾｽ対処ﾙｰﾙ生成方法及びその装置と、不正ｱｸｾｽ対処方法及びその装置と、不正ｱｸｾｽ対処ﾙｰﾙ生成ﾌﾟﾛｸﾞﾗﾑ及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体

表 2.1.4 NTT の技術要素別課題対応特許(2/25)

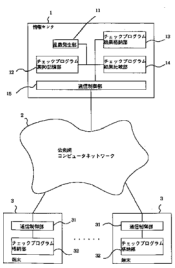
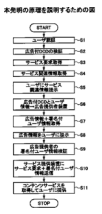
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開 2004-320461 03.04.16 H04L12/66	**ﾈｯﾄﾜｰｸ攻撃防止方法、ﾈｯﾄﾜｰｸ攻撃防止装置、ﾈｯﾄﾜｰｸ攻撃防止ﾌﾟﾛｸﾞﾗﾑ及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開 2002-215583 （拒絶確定） 01.01.18 G06F15/00,330	**簡易端末用情報開示装置、方法、及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特許 3393521 95.10.19 G06F1/00	**端末ﾌﾟﾛｸﾞﾗﾑ改ざん検出方法、および情報ｾﾝﾀ**  情報ｾﾝﾀと、該ｾﾝﾀにﾈｯﾄﾜｰｸを介して接続する複数の端末で構成されたｼｽﾃﾑにおいて、上記ｾﾝﾀは、前記の各端末で使用されるｱﾌﾟﾘｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾑの特徴をあるﾁｪｯｸﾌﾟﾛｸﾞﾗﾑによって計測し、計測に用いた各ﾁｪｯｸﾌﾟﾛｸﾞﾗﾑの識別子、および各ｱﾌﾟﾘｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾑが改ざんされていないことが保証された状態での、前記計測の結果である基準結果の組を保持し、上記端末は、前記ﾁｪｯｸﾌﾟﾛｸﾞﾗﾑの識別子、およびそれに対応するﾁｪｯｸﾌﾟﾛｸﾞﾗﾑの組を複数保持し、あるｱﾌﾟﾘｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾑを使用する際に、該端末から上記ｾﾝﾀに、前記ﾁｪｯｸﾌﾟﾛｸﾞﾗﾑの識別子を要求すると、上記ｾﾝﾀは、端末からの要求に応じて、該ｾﾝﾀに保持されたﾁｪｯｸﾌﾟﾛｸﾞﾗﾑの識別子のうちの 1 つをﾗﾝﾀﾞﾑに選択して、要求のあった端末に送信し、上記端末は、該ｾﾝﾀから送信されたﾌﾟﾛｸﾞﾗﾑの識別子に対応したﾁｪｯｸﾌﾟﾛｸﾞﾗﾑを実行し、その計測結果をｾﾝﾀに送信し、上記ｾﾝﾀは、送られてきた計測結果と、予め保持していた前記基準結果を比較し、異なる場合には前記端末のｱﾌﾟﾘｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾑが改ざんされたと判断することを特徴とする端末ﾌﾟﾛｸﾞﾗﾑ改ざん検出方法。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特許 3578100 01.03.23 G06F17/60,326	**ｺﾝﾃﾝﾂ提供方法及びｼｽﾃﾑ及びｺﾝﾃﾝﾂ提供ﾌﾟﾛｸﾞﾗﾑ及びｺﾝﾃﾝﾂ提供ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**  ｺﾝﾃﾝﾂ及び該ｺﾝﾃﾝﾂﾃﾞｰﾀに対する情報やｻｰﾋﾞｽをﾕｰｻﾞに提供するためのｺﾝﾃﾝﾂ提供方法において、任意の認証方法により、前記ﾕｰｻﾞの認証を行い、ｺﾝﾃﾝﾂ ID やｺﾝﾃﾝﾂの属性情報などのﾃﾞｰﾀ集合である DCD に広告情報を付与した広告付 DCD に付与されたﾃﾞｨｼﾞﾀﾙ署名をﾃﾞｨｼﾞﾀﾙ署名に対応する検証方法で検証し、該広告付 DCD の内容が正当なものであることを検証し、前記ﾕｰｻﾞから前記広告付 DCD に対するｻｰﾋﾞｽ要求を取得し、ｺﾝﾃﾝﾂ関連情報を提供するｺﾝﾃﾝﾂ関連情報提供装置に前記ｻｰﾋﾞｽ要求を送信し、該ｻｰﾋﾞｽ要求に対応するｺﾝﾃﾝﾂに関するｻｰﾋﾞｽ関連情報を受信し、前記ｻｰﾋﾞｽ関連情報を送信し、ﾕｰｻﾞにより選定されたｻｰﾋﾞｽ関連情報と前記広告付 DCD と該ﾕｰｻﾞに関するﾕｰｻﾞ情報を広告提供者装置に送信し、前記広告提供者装置から前記 DCD に付与されている広告情報と、広告提供者のﾃﾞｨｼﾞﾀﾙ署名が付与されたﾕｰｻﾞ情報を取得し、前記 DCD に付与されている広告情報を前記ﾕｰｻﾞに提示し、前記広告提供者のﾃﾞｨｼﾞﾀﾙ署名が付与されたﾕｰｻﾞ情報を該ﾃﾞｨｼﾞﾀﾙ署名を行った方法に基づいて検証し、前記広告提供者のﾃﾞｨｼﾞﾀﾙ署名が付与されたﾕｰｻﾞ情報とｺﾝﾃﾝﾂに対するｻｰﾋﾞｽ要求をｻｰﾋﾞｽ提供者装置に送信し、前記ｻｰﾋﾞｽ提供者装置から取得したｺﾝﾃﾝﾂｻｰﾋﾞｽを前記ﾕｰｻﾞに提供することを特徴とするｺﾝﾃﾝﾂ提供方法。

表 2.1.4 NTT の技術要素別課題対応特許(3/25)

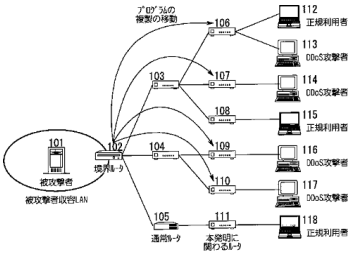
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
アノマリ解析技術	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開 2002-132722 00.10.30 G06F15/00,330	**代行認証方法、その各装置、その装置の処理方法、及びﾌﾟﾛｸﾞﾗﾑ記録媒体**
			特開 2002-024176 （拒絶確定） 00.07.04 G06F15/00,330	**ﾃﾞｰﾀ通信ｼｽﾃﾑ、送信者装置、仲介者装置、受信者装置および記録媒体**
	攻撃の抑止・予防の強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ｱﾄﾞﾚｽの検索	特許 3549861 00.09.12 H04L12/66 [被引用回数 8]	**分散型ｻｰﾋﾞｽ不能攻撃の防止方法および装置ならびにそのｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ**  通信装置を通過する通信ﾊﾟｹｯﾄを監視し分散型ｻｰﾋﾞｽ不能攻撃を検出するﾄﾗﾌｨｯｸ監視機能部と、分散型ｻｰﾋﾞｽ不能攻撃が検出された際に分散型ｻｰﾋﾞｽ不能攻撃の通信ﾊﾟｹｯﾄを破棄する攻撃防御ﾓｼﾞｭｰﾙと、攻撃元に近い上位側の通信装置のｱﾄﾞﾚｽを検索する処理を行う攻撃元検索ﾓｼﾞｭｰﾙと、上位側の防御位置の通信装置に対して攻撃元検索ﾓｼﾞｭｰﾙを送信するﾓｼﾞｭｰﾙ送信部と、攻撃元検索ﾓｼﾞｭｰﾙによって検索された攻撃元に近い上位側の通信装置の候補中から上位側の防御位置とする通信装置を抽出する攻撃元判断機能部とを備え、ﾓｼﾞｭｰﾙ送信部は、攻撃元判断機能部によって抽出された上位側の防御位置の通信装置に対して攻撃防御ﾓｼﾞｭｰﾙを送信するものであることを特徴とする通信装置。
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開 2004-320453 03.04.16 H04L12/56,100	**不正ｱｸｾｽ警告装置とそのﾌﾟﾛｸﾞﾗﾑ**

表 2.1.4 NTT の技術要素別課題対応特許(4/25)

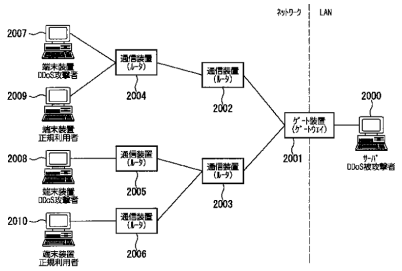
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
アノマリ解析技術	攻撃の抑止・予防の強化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 帯域制限値の算出	特許 3609381 02.03.22 H04L12/56,200	**分散型ｻｰﾋﾞｽ不能攻撃防止方法及びｹﾞｰﾄ装置、通信装置ならびにﾌﾟﾛｸﾞﾗﾑ**  ｹﾞｰﾄ装置は、入力される通信ﾄﾗﾋｯｸから攻撃容疑ﾄﾗﾋｯｸを検出した場合に、ｹﾞｰﾄ装置における攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値と、ｹﾞｰﾄ装置の 1 つ上流にある通信装置数とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、通信装置は、攻撃容疑ﾄﾗﾋｯｸの伝送帯域を下流のｹﾞｰﾄ装置または通信装置から受信した伝送帯域制限値に制限すると共に、受信した伝送帯域制限値と、通信装置の 1 つ上流にある通信装置数とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、攻撃容疑ﾊﾟｹｯﾄ送出元の最上流の通信装置に達するまで再帰的に、攻撃容疑ﾊﾟｹｯﾄの伝送帯域の制限と、攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値送信との処理を行い、ｹﾞｰﾄ装置は、上流の通信装置へ攻撃容疑ﾄﾗﾋｯｸの平均入力伝送帯域を問合せを送信する処理を行い、上流の通信装置は、下流のｹﾞｰﾄ装置または通信装置から攻撃容疑ﾄﾗﾋｯｸの平均入力伝送帯域問合せを受信して、通信装置における攻撃容疑ﾄﾗﾋｯｸの平均入力伝送帯域値を下流のｹﾞｰﾄ装置または通信装置へ送信する処理を行い、ｹﾞｰﾄ装置は、ｹﾞｰﾄ装置における攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値と、上流の通信装置から受信した攻撃容疑ﾄﾗﾋｯｸの平均入力伝送帯域値とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値を算出して上流の通信装置へ送信する処理を行い、通信装置は、攻撃容疑ﾄﾗﾋｯｸの伝送帯域を下流のｹﾞｰﾄ装置または通信装置から受信した伝送帯域制限調整値に制限すると共に、上流の通信装置へ前記攻撃容疑ﾄﾗﾋｯｸの平均入力伝送帯域を問合せを送信する処理と、下流の通信装置から受信した伝送帯域制限調整値と、上流の通信装置から受信した前記攻撃容疑ﾄﾗﾋｯｸの平均入力伝送帯域値とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値を算出して上流の通信装置へ送信する処理とを行い、攻撃容疑ﾊﾟｹｯﾄ送出元の最上流の前記通信装置に達するまで再帰的に、伝送帯域制限調整値に攻撃容疑ﾊﾟｹｯﾄの伝送帯域の制限と共に、攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値の送信との処理を行う、ことを特徴とする分散型ｻｰﾋﾞｽ不能攻撃防止方法。

表 2.1.4 NTT の技術要素別課題対応特許(5/25)

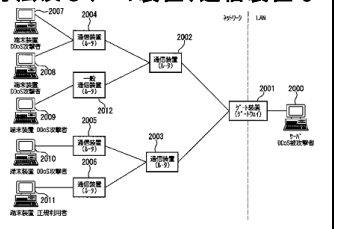
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
アノマリ解析技術	攻撃の抑止・予防の強化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 帯域制限値の算出	特許 3609382 02.03.22 H04L12/66	**分散型ｻｰﾋﾞｽ不能攻撃防止方法及びｹﾞｰﾄ装置、通信装置ならびにﾌﾟﾛｸﾞﾗﾑ**  ｹﾞｰﾄ装置は、入力される通信ﾄﾗﾋｯｸから攻撃容疑ﾄﾗﾋｯｸを検出した場合に、当該ｹﾞｰﾄ装置における攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値と、ｹﾞｰﾄ装置の１つ上流にある通信装置数とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値を下流のｹﾞｰﾄ装置または通信装置から受信した伝送帯域制限値に制限すると共に、受信した伝送帯域制限値と、通信装置の１つ上流にある通信装置数とを基に、上流の通信装置へ通知する前記攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値を算出して上流の通信装置へ送信する処理を行い、攻撃容疑ﾊﾟｹｯﾄ送出元の最上流の通信装置に達するまで再帰的に、攻撃容疑ﾊﾟｹｯﾄの伝送帯域の制限と、攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限値送信との処理を行い、最上流の通信装置は、通信装置に入力される前記攻撃容疑ﾄﾗﾋｯｸの合計入力伝送帯域値を下流の通信装置へ送信する処理を行い、合計入力伝送帯域値を受信した下流の通信装置は、上流の通信装置を介さずに通信装置に入力される攻撃容疑ﾄﾗﾋｯｸの伝送帯域値と、受信した攻撃容疑ﾄﾗﾋｯｸの合計入力伝送帯域値とを合計した、通信装置における攻撃容疑ﾄﾗﾋｯｸの合計入力伝送帯域値を下流の通信装置または前記ｹﾞｰﾄ装置へ送信し、ｹﾞｰﾄ装置に達するまで再帰的に攻撃容疑ﾄﾗﾋｯｸの合計入力伝送帯域値の送信する処理を行い、ｹﾞｰﾄ装置は、ｹﾞｰﾄ装置における攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値と、上流の通信装置を介さずにｹﾞｰﾄ装置に入力される攻撃容疑ﾄﾗﾋｯｸの伝送帯域値と、上流の通信装置から受信した攻撃容疑ﾄﾗﾋｯｸの合計入力伝送帯域値とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値を算出して上流の通信装置へ送信する処理を行い、通信装置は、攻撃容疑ﾄﾗﾋｯｸの伝送帯域を下流のｹﾞｰﾄ装置または通信装置から受信した伝送帯域制限調整値に制限すると共に、受信した伝送帯域制限調整値と、上流の通信装置を介さずに通信装置に入力される攻撃容疑ﾄﾗﾋｯｸの伝送帯域値と、上流の通信装置から受信した前記攻撃容疑ﾄﾗﾋｯｸの合計入力伝送帯域値とを基に、上流の通信装置へ通知する攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値を算出して上流の通信装置へ送信する処理とを行い、攻撃容疑ﾊﾟｹｯﾄ送出元の最上流の通信装置に達するまで再帰的に、伝送帯域制限調整値に前記攻撃容疑ﾊﾟｹｯﾄの伝送帯域の制限と共に、攻撃容疑ﾄﾗﾋｯｸの伝送帯域制限調整値の送信との処理を行う、ことを特徴とする分散型ｻｰﾋﾞｽ不能攻撃防止方法。
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開 2005-157421 03.11.20 G06F13/00	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ維持方法，接続許可ｻｰﾊﾞ及び接続許可ｻｰﾊﾞ用ﾌﾟﾛｸﾞﾗﾑ**
シグネチャ解析技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開 2004-320644 03.04.18 H04L12/66	**ﾌｧｲｱｳｫｰﾙ検査ｼｽﾃﾑ、ﾌｧｲｱｳｫｰﾙ検査方法、ﾌｧｲｱｳｫｰﾙ検査用ﾌﾟﾛｸﾞﾗﾑ、及びﾌｧｲｱｳｫｰﾙ検査用記録媒体**

表 2.1.4 NTT の技術要素別課題対応特許(6/25)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	発明の名称 概要
シグネチャ解析技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 仲介ｻｰﾊﾞｰ配置	特開 2002-328896 01.04.27 G06F15/00,330 〔被引用回数 3〕	不正ｱｸｾｽ対処ﾙｰﾙ自動設定装置
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開平 11-313111 （みなし取下） 98.04.28 H04L12/66 〔被引用回数 3〕	情報通過制御方法、ｹﾞｰﾄｳｴｲ装置及び記録媒体
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｲﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開 2004-357234 03.05.30 H04L12/66	ｾｷｭﾘﾃｨ管理装置、ｾｷｭﾘﾃｨ通信装置、ﾌｧｲｱｳｫｰﾙ設定方法、ﾌｧｲｱｳｫｰﾙ設定用ﾌﾟﾛｸﾞﾗﾑ、及びﾌｧｲｱｳｫｰﾙ設定用記録媒体。
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの切換	特開 2005-151492 03.11.20 H04L12/66	不正ｱｸｾｽ対処ﾙｰﾙ生成方法，不正ｱｸｾｽ対処方法，不正ｱｸｾｽ対処ﾙｰﾙ生成装置，不正ｱｸｾｽ対処装置およびｽﾀｯｸｽﾏｯｼﾝｸﾞ攻撃対策ｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの追加、学習	特開 2004-274654 03.03.12 H04L12/66	ｾｷｭﾘﾃｨ自動設定装置、ｾｷｭﾘﾃｨ自動設定方法および記録媒体
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IP ｱﾄﾞﾚｽの変換	特開 2005-122656 03.10.20 G06F15/00,330	ﾃﾞｰﾀ送信分散制御方法、ﾈｯﾄﾜｰｸ転送装置、ﾕｰｻﾞ端末、ｻｰﾋﾞｽ管理ｻｰﾊﾞおよび記録媒体
	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開 2002-158699 （拒絶確定） 00.11.20 H04L12/56 〔被引用回数 5〕	DoS 攻撃防止方法および装置およびｼｽﾃﾑおよび記録媒体
	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 不正ｱｸｾｽ履歴情報の蓄積	特開 2005-182187 03.12.16 G06F13/00,351	不正ｱｸｾｽ検知方法、不正ｱｸｾｽ検知ｼｽﾃﾑ及び不正ｱｸｾｽ検知ﾌﾟﾛｸﾞﾗﾑ
	攻撃パターンの高精度化	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開 2005-124055 03.10.20 H04L12/66	ﾈｯﾄﾜｰｸ攻撃の防御装置
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾄﾗﾌｨｯｸ	特開 2004-343580 03.05.19 H04L12/66	ｹﾞｰﾄｳｴｲ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの切換	特開 2005-039721 03.07.18 H04L12/66	DDoS 防御方法及び DDoS 防御機能付きﾙｰﾀ装置

表 2.1.4 NTT の技術要素別課題対応特許(7/25)

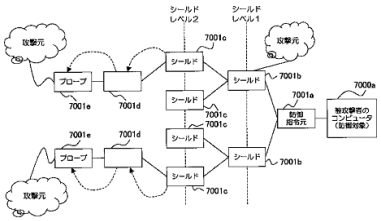
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
シグネチャ解析技術	攻撃パターンの高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特許 3652661 02.03.20 H04L12/66	**ｻｰﾋﾞｽ不能攻撃の防御方法および装置ならびにそのｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ**  複数の通信装置によって構成されるﾈｯﾄﾜｰｸに接続された防御対象ｺﾝﾋﾟｭｰﾀをｻｰﾋﾞｽ不能攻撃から防御するための防御方法であって､前記防御対象ｺﾝﾋﾟｭｰﾀに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて､当該境界通信装置から所定の段数分の範囲内に接続されているｼｰﾙﾄﾞ通信装置が､当該ｼｰﾙﾄﾞ通信装置に到着する通信ﾊﾟｹｯﾄを分析する分析処理を行い､この分析処理の結果に応じて当該通信ﾊﾟｹｯﾄが前記防御対象ｺﾝﾋﾟｭｰﾀに対する攻撃の通信ﾊﾟｹｯﾄである可能性に応じて当該通信ﾊﾟｹｯﾄの優先度を決定してこの優先度に応じて当該通信ﾊﾟｹｯﾄを転送先に転送するとともに､前記分析処理の結果当該通信ﾊﾟｹｯﾄが確実に前記防御対象ｺﾝﾋﾟｭｰﾀに対する攻撃の通信ﾊﾟｹｯﾄであることが判明した場合には当該通信ﾊﾟｹｯﾄを破棄するｼｰﾙﾄﾞ過程を有することを特徴とするｻｰﾋﾞｽ不能攻撃の防御方法。
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開 2004-363785 03.06.03 H04L12/66	**ﾈｯﾄﾜｰｸ間接続装置**
		ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｵﾌﾞｼﾞｪｸに認証情報埋め込み	特開 2004-227410 03.01.24 G06F15/16,620	**ﾓﾊﾞｲﾙｴｰｼﾞｪﾝﾄｼｽﾃﾑ､及びﾓﾊﾞｲﾙｴｰｼﾞｪﾝﾄ方法､その方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開 2003-087307 01.09.12 H04L12/56	**ﾉｰﾄﾞ装置及びﾉｰﾄﾞ制御装置**
	攻撃の抑止・予防の強化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 不正ｱｸｾｽ履歴情報の蓄積	特開 2003-330887 (みなし取下) 02.05.15 G06F15/00,330	**不正ｱｸｾｽ警告装置､ｻｰﾊﾞ装置及び不正ｱｸｾｽ警告ﾌﾟﾛｸﾞﾗﾑ**
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開 2005-005927 03.06.11 H04L12/56,400	**ﾈｯﾄﾜｰｸｼｽﾃﾑと不正ｱｸｾｽ制御方法およびﾌﾟﾛｸﾞﾗﾑ**
脆弱性診断技術	侵入防御の性能向上	情報の送信､転送､分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開 2004-080272 02.08.14 H04L12/66	**通信ﾈｯﾄﾜｰｸｼｽﾃﾑ､ｻｰﾋﾞｽ処理制御方法､ﾌﾟﾛﾊﾞｲﾀﾞｻｰﾊﾞおよびｻｰﾋﾞｽ処理装置**
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特開 2002-335246 01.05.10 H04L12/26 〔被引用回数 2〕	**ﾈｯﾄﾜｰｸﾍﾞｰｽ侵入検査方法及び装置並びにﾈｯﾄﾜｰｸﾍﾞｰｽ侵入検査用ﾌﾟﾛｸﾞﾗﾑ及びその記録媒体**

表 2.1.4 NTT の技術要素別課題対応特許(8/25)

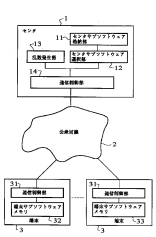
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開 2005-130399 03.10.27 H04L12/66	**侵入検知ｼｽﾃﾑ、侵入検知方法および記録媒体**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開 2005-128962 03.10.27 G06F13/00,351	**侵入検知ｼｽﾃﾑ、侵入検知方法および記録媒体**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開 2001-244961 00.03.01 H04L12/54	**電子私書箱方式**
	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 情報転送の手順 VPN 設定情報	特開 2004-343522 （特許 3732835） 03.05.16 H04L12/66	**通信ﾌﾟﾛﾌｧｲﾙ管理装置及び通信装置、ならびに通信ﾌﾟﾛﾌｧｲﾙ提供方法**
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特許 3463963 94.04.28 G06F1/00	**ｿﾌﾄｳｪｱ解析保護方法**  ｾﾝﾀと、該ｾﾝﾀに接続された複数の端末で構成されたｼｽﾃﾑにおいて、端末で使用されるｿﾌﾄｳｪｱが端末で解析されないように保護するｿﾌﾄｳｪｱ解析保護方法であって、端末で使用されるｿﾌﾄｳｪｱを分割したｿﾌﾄｳｪｱ部分を端末とｾﾝﾀとに分配して保持し、端末において前記ｿﾌﾄｳｪｱを使用する毎に、端末からｾﾝﾀに保持されたｿﾌﾄｳｪｱ部分を要求し、端末からの要求に応じてｾﾝﾀに保持されたｿﾌﾄｳｪｱ部分を端末に送信し、ｾﾝﾀから送信されたｿﾌﾄｳｪｱ部分をﾒﾓﾘ上の端末に保持されたｿﾌﾄｳｪｱ部分中の欠落部分にﾛｰﾄﾞすることにより、前記ｿﾌﾄｳｪｱの前記ﾒﾓﾘ上に展開された配置ﾊﾟﾀｰﾝを前記ｿﾌﾄｳｪｱが端末で使用される毎に変更しながら、前記ｿﾌﾄｳｪｱを端末上で動作可能とし、前記ﾒﾓﾘ上に展開された前記ｿﾌﾄｳｪｱを端末上で動作させる、ことからなるｿﾌﾄｳｪｱ解析保護方法。
プロキシ中継技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開 2004-282115 03.03.12 H04L12/66	**SIP 通信方法及び SIP 通信ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開平 11-252067 （みなし取下） 98.03.03 H04L9/32 〔被引用回数 2〕	**ｾｷｭﾘﾃｨｵﾍﾟﾚｰｼｮﾝ制御方法およびその記録媒体**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開 2005-175635 03.12.08 H04L12/46	**ﾈｯﾄﾜｰｸ間接続制御方法及びｼｽﾃﾑ装置**

表 2.1.4 NTT の技術要素別課題対応特許(9/25)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	利用サービスの保護強化	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 多層ﾌﾟﾛﾄｺﾙの処理	特開 2004-259102 03.02.27 G06F15/00,310	ｱｸｾｽ統合制御方法及びｱｸｾｽ統合制御装置と当該装置を用いたﾈｯﾄﾜｰｸ利用統合制御ｼｽﾃﾑ
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開 2002-300191 01.04.02 H04L12/56	複数ｻｰﾋﾞｽ種別提供方法及びその実施ｼｽﾃﾑ並びにその処理ﾌﾟﾛｸﾞﾗﾑと記録媒体
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開平 11-175475 (拒絶確定) 97.12.11 G06F15/00,330	ｱｸｾｽ制御方法およびｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開 2000-322353 99.05.13 G06F13/00,351	情報提供装置、情報提供ｻｰﾋﾞｽ認証方法及び情報提供ｻｰﾋﾞｽ認証ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
			特開 2002-123491 00.10.13 G06F15/00,330 〔被引用回数 3〕	認証代行方法、認証代行装置、及び認証代行ｼｽﾃﾑ
			特開 2001-344205 00.05.31 G06F15/00,330	ｻｰﾋﾞｽ提供ｼｽﾃﾑおよびｻｰﾋﾞｽ提供方法ならびに記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開 2003-273868 02.03.15 H04L12/22	認証ｱｸｾｽ制御ｻｰﾊﾞ装置と、ｹﾞｰﾄｳｴｲ装置と、認証ｱｸｾｽ制御方法と、ｹﾞｰﾄｳｴｲ制御方法と、認証ｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑ及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開 2000-163346 98.11.27 G06F13/00,353	ｾｯｼｮﾝ識別方法およびｾｯｼｮﾝ管理方法、ならびにそれを実現するための情報提供ｼｽﾃﾑとそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開平 11-234270 (みなし取下) 98.02.16 H04L12/22 〔被引用回数 7〕	ﾈｯﾄﾜｰｸ間のﾃﾞｰﾀﾍﾞｰｽの複製･更新方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 中継ｻｰﾊﾞｰの配置	特開 2000-099462 (拒絶確定) 98.09.25 G06F15/00,310	遠隔操作方法、ｼｽﾃﾑ、および遠隔操作ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
			特開平 09-331327 (みなし取下) 96.06.13 H04L12/24	ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 収集器の配置	特開 2000-082032 (拒絶確定) 98.09.04 G06F13/00,354	ｻｰﾋﾞｽ利用情報転送方法、ｻｰﾋﾞｽ利用情報収集･集計ｼｽﾃﾑ、ｻｰﾋﾞｽ利用情報配送ﾌﾟﾛｸﾞﾗﾑ、ｻｰﾋﾞｽ利用情報集計ﾌﾟﾛｸﾞﾗﾑをそれぞれ記録した記録媒体
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開 2004-179770 02.11.25 H04L12/66	ｱｸｾｽ制御方法、ｼｽﾃﾑ、およびﾌﾟﾛｸﾞﾗﾑとその記録媒体

表 2.1.4 NTT の技術要素別課題対応特許(10/25)

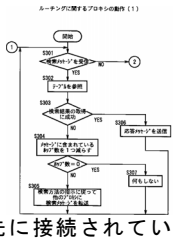
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	発明の名称 概要
プロキシ中継技術	通信データの中継性能向上	ファイアウォール外のシステム構成 サービスサーバーの配置 プロキシサーバーの配置	特許 3672534 02.02.13 H04L12/56,100	**ルーチング制御方法及びルーチング制御装置並びに記録媒体及び制御プログラム**  プロキシが配置された各ノードの制御に用いるルーチング制御方法であって、各々のアプリケーションプログラム及び各々のプロキシを特定するサービスアドレス、並びに各々の通信を表すセッションを管理し、各々のアプリケーションプログラムの所在及び各々のプロキシの所在をリソーステーブルとして管理し、宛先のアプリケーションプログラムを表す第 1 のサービスアドレスと、前記宛先に接続されている通信経路上で自プロキシの次ホップに位置する他のプロキシを表す第 2 のサービスアドレスとの対応関係をプロキシルーチングテーブルとして管理し、各ノードに存在する通信デバイスのネットワークアドレスをロケーションテーブルとして管理し、自ノードで管理されている情報が更新された場合、もしくは自ノードに存在しない情報の検索が必要になった場合に、前記リソーステーブルもしくはロケーションテーブルで管理されている他のノードに対してメッセージを送信し、自ノードが他ノードからの検索を要求するメッセージを受信し、要求された情報が自ノードに存在する場合には、検索の結果をメッセージの発信元に送信し、自ノードが他ノードからの検索を要求するメッセージを受信し要求された情報が自ノードに存在しない場合、もしくは情報の更新を示すメッセージを受信した場合には、メッセージの発信元からのホップ数が制限値を超えていなければ、受信したメッセージの内容を前記リソーステーブルもしくはロケーションテーブルで管理されている他のノードに対して転送することを特徴とするルーチング制御方法。
		データ形式の改良 データに情報付加 ヘッダに認証情報	特開 2001-331446 00.05.24 G06F15/00,330 〔被引用回数 1〕	**セキュアエージェント実現方法とセキュアエージェントシステムとセキュアエージェント管理装置**
		データ形式の改良 データに情報付加 電子署名の付加	特開 2001-209613 00.01.25 G06F15/00,330	**匿名アプリケーション格納方法及びシステム及び匿名アプリケーション格納プログラムを格納した記憶媒体**
		回路の改良 スイッチ回路の追加 複数通信路の配置	特開 2003-150468 01.11.14 G06F13/00,353 〔被引用回数 1〕	**通信方法および装置**
	システムの性能向上	情報の照合、検索、カウント手順改良 特定情報の照合手順 順番号の検証	特開 2002-312261 01.04.09 G06F13/00,353	**ネットワークサービス中継方法及び中継装置**
		ファイアウォール内のシステム構成 DMZ に機器の配置 情報提供サーバーの配置	特開 2003-271528 02.03.15 G06F13/00,630	**イントラネット内装置制御システム，イントラネット内装置制御方法，イントラネット内の装置を制御する制御装置およびその方法，並びにイントラネット内装置制御用プログラ**
		ファイアウォール外のシステム構成 セキュリティサーバーの配置 認証サーバの配置	特開 2003-318889 （みなし取下） 02.04.26 H04L9/32	**ユーザ認証方法、通信システム、認証サーバ装置、サーバ装置及びユーザ端末装置**
		ファイアウォール外のシステム構成 セキュリティサーバーの配置 アクセス制御サーバ-配置	特開 2003-242109 02.02.15 G06F15/00,310 〔被引用回数 1〕	**認証アクセス制御サーバ装置と、ゲートウエイ装置と、認証アクセス制御方法と、ゲートウエイ制御方法と、認証アクセス制御プログラム及びそのプログラムを記録した記録媒体**

表 2.1.4 NTT の技術要素別課題対応特許(11/25)

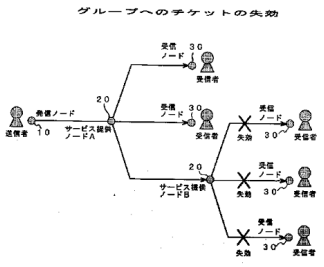
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
プロキシ中継技術	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開 2002-247021 01.02.15 H04L9/08	**ｱｸｾｽ制限付ｺﾝﾃﾝﾂ表示方法およびその装置**
		ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｾｷｭﾘﾃｨｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特開 2003-345931 02.05.28 G06F17/60,140	**個人情報流通管理方法,個人情報流通管理ｼｽﾃﾑにおける個人情報認証装置,個人情報利用環境認証装置,個人情報提供装置,個人情報利用装置および開示利用規定判断ﾌﾟﾛｸﾞ**
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｵﾌﾞｼﾞｪｸに認証情報埋め込み	特開 2002-245013 01.02.19 G06F15/16,620	**ｾｷｭﾘﾃｨ実現方法及びｾｷｭﾘﾃｨ実現ﾌﾟﾛｸﾞﾗﾑ及びｾｷｭﾘﾃｨ実現ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**
コンテンツフィルタリング技術	利用サービスの保護強化	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開 2002-032333 (拒絶確定) 00.07.18 G06F15/00,310	**ﾃﾞｰﾀ管理ｼｽﾃﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑ ID	特開 2002-297542 01.04.02 G06F15/00,330	**ｺﾝﾃﾝﾂ時限開示方法、ｼｽﾃﾑ、ｾｷｭﾘﾃｨﾃﾞﾊﾞｲｽ**
			特許 3611470 98.09.22 H04L12/18	**通信ｻｰﾋﾞｽﾁｹｯﾄの失効ﾘｽﾄ管理方法**  通信ﾈｯﾄﾜｰｸ上で単一の送信者から複数の受信者へｸﾞﾙｰﾌﾟ通信を行い、送信者は複数の受信者の指定をｸﾞﾙｰﾌﾟを示す識別子で行い、前記識別子で指定されたｸﾞﾙｰﾌﾟは、ｻｰﾋﾞｽ提供者により管理される機器(以下ｻｰﾋﾞｽ提供ﾉｰﾄﾞと呼ぶ)により階層的に別のｸﾞﾙｰﾌﾟまたは受信者に展開されることによって、送信者のﾒｯｾｰｼﾞが最終的な受信者に伝達され、ｺﾐｭﾆｹｰｼｮﾝの制御をｺﾐｭﾆｹｰｼｮﾝを行う権利を有する事をあらわすﾁｹｯﾄの発行による許可と該ﾁｹｯﾄの失効による禁止によって行い、ﾁｹｯﾄの失効を要求する主体として、受信者、ｻｰﾋﾞｽ提供者、及びそれ以外の第三者が存在し、失効要求に基づいて失効情報のﾘｽﾄである失効ﾘｽﾄを作成し失効を実施する失効実施者として受信者及びｻｰﾋﾞｽ提供者が存在し、失効を要求する各主体に応じて、失効により利益を得る失効受益者が異なるような通信ｼｽﾃﾑにおいて、各失効実施者が各々の失効ﾘｽﾄを持ち、その失効ﾘｽﾄには必須失効情報とｵﾌﾟｼｮﾅﾙ失効情報の二つに分類され、必須失効情報は失効実施者と失効受益者が等しく必ず失効を実施する失効情報であり、ｵﾌﾟｼｮﾅﾙ失効情報は失効実施者と失効受益者が異なり実施者の判断により実施する失効情報であり、失効要求者は受益者である実施者の管理する機器(以下失効実施ﾉｰﾄﾞと呼ぶ)に対し失効要求として失効したいﾁｹｯﾄの情報及び受信者やｸﾞﾙｰﾌﾟなどの宛先を示す識別子を送り、前記失効実施ﾉｰﾄﾞは前記失効要求をもとに、必須失効情報として前記失効実施ﾉｰﾄﾞが参照する失効ﾘｽﾄに登録する事を特徴とする通信ｻｰﾋﾞｽﾁｹｯﾄの失効ﾘｽﾄ管理方法。

表 2.1.4 NTT の技術要素別課題対応特許(12/25)

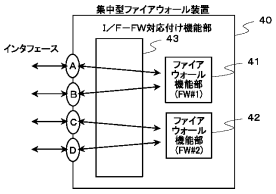
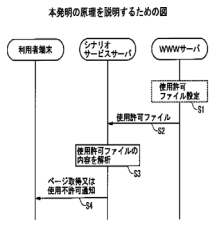
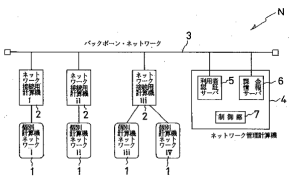
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特許 3557152 00.04.27 G06F13/00,351 〔被引用回数 1〕	**集中型ﾌｧｲｱｳｫｰﾙ装置**  複数のﾕｰｻﾞ網間接続を行うﾈｯﾄﾜｰｸに設置されるﾌｧｲｱｳｫｰﾙ装置であって、個々のﾕｰｻﾞ網と接続する複数のｲﾝﾀﾌｪｰｽと、ﾕｰｻﾞ網間毎に独立したﾌｧｲｱｳｫｰﾙ機能を提供する複数のﾌｧｲｱｳｫｰﾙ機能部と、各ｲﾝﾀﾌｪｰｽを複数のﾌｧｲｱｳｫｰﾙ機能部のいずれかに対応付ける対応付け機能部とを備えたことを特徴とする集中型ﾌｧｲｱｳｫｰﾙ装置。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特開 2002-342277 01.05.21 G06F15/00,330	**ｻｰﾋﾞｽ連携ｼｽﾃﾑおよび連携ｻｰﾊﾞおよびｾｷｭｱﾄｰｸﾝおよびﾌﾟﾛｸﾞﾗﾑおよび記録媒体**
			特開 2003-122717 (みなし取下) 01.10.12 G06F15/00,330	**ｱｸｾｽ許可装置及び方法、並びにｱｸｾｽ許可ﾌﾟﾛｸﾞﾗﾑ及び記録媒体**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｱｸｾｽ制御ｻｰﾊﾞｰ配置	特開 2003-345742 02.05.28 G06F15/00,310	**CUG(ClosedUserGroup)管理方法及び CUG 提供ｼｽﾃﾑ及び CUG 提供ﾌﾟﾛｸﾞﾗﾑ及び CUG 提供ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開 2003-283549 (特許 3706350) 02.03.22 H04L12/56,100	**ｺﾝﾃﾝﾂﾌｨﾙﾀﾘﾝｸﾞ装置及び方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特許 3678128 00.09.13 G06F15/00,310	**ｼﾅﾘｵｻｰﾋﾞｽ提供方法及びｼﾅﾘｵｻｰﾋﾞｽｻｰﾊﾞ及びｼﾅﾘｵｻｰﾋﾞｽ提供ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**  WWWｼｽﾃﾑにおいて、利用者が利用者端末から、ﾍﾟｰｼﾞの提示順序を制御するためのｼﾅﾘｵ情報に従って利用者に提示するﾍﾟｰｼﾞを選択するｼﾅﾘｵｻｰﾋﾞｽｻｰﾊﾞを経由して、WWWｻｰﾊﾞに公開されているﾍﾟｰｼﾞを取得するｼﾅﾘｵｻｰﾋﾞｽ提供方法において、WWWｻｰﾊﾞ上に、ﾍﾟｰｼﾞがｼﾅﾘｵｻｰﾋﾞｽｻｰﾊﾞを経由して利用されることを許可するか、あるいは、不許可とするかを記載した使用許可ﾌｧｲﾙを設け、ｼﾅﾘｵｻｰﾋﾞｽ提供時に、ｼﾅﾘｵｻｰﾋﾞｽｻｰﾊﾞにおいて、ﾍﾟｰｼﾞを利用する前に、WWW ｻｰﾊﾞから該使用許可ﾌｧｲﾙを取得し、使用許可ﾌｧｲﾙの内容を解析し、解析結果において、利用が許可されている場合には、ﾍﾟｰｼﾞを取得して、利用者端末に提供し、利用が許可されていない場合には、ﾍﾟｰｼﾞが利用不許可であることを利用者端末に通知することを特徴とするｼﾅﾘｵｻｰﾋﾞｽ提供方法。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開平 09-231173 (みなし取下) 96.02.21 G06F15/00,330	**ｱｸｾｽﾚﾍﾞﾙによる HMI 端末の利用機能のﾏｽｸ方法及びｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特許 3398530 95.08.23 H04L12/28,200	**ﾈｯﾄﾜｰｸｼｽﾃﾑとその運用処理方法および使用ｱｸｾｽ方法**  ｻｰﾊﾞ装置とｸﾗｲｱﾝﾄ装置からなる個別ﾈｯﾄﾜｰｸの 1 又は複数をﾈｯﾄﾜｰｸ接続用装置に接続し、該ﾈｯﾄﾜｰｸ接続用装置の複数をﾊﾞｯｸﾎﾞｰﾝ･ﾈｯﾄﾜｰｸに接続するとともに当該ﾊﾞｯｸﾎﾞｰﾝ･ﾈｯﾄﾜｰｸにﾈｯﾄﾜｰｸ管理装置を設け、該ﾈｯﾄﾜｰｸ管理装置に該ﾊﾞｯｸﾎﾞｰﾝ･ﾈｯﾄﾜｰｸ全体の制御機能を持たせた、ことを特徴とするﾈｯﾄﾜｰｸｼｽﾃﾑ。

表 2.1.4 NTT の技術要素別課題対応特許(13/25)

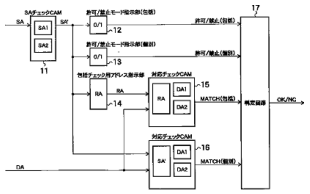
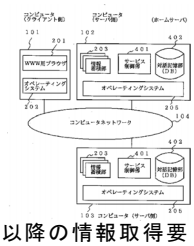
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特許 3504150 98.07.23 H04L12/22 沖電気工業	**ｺﾈｸｼｮﾝﾚｽ交換装置及びｱｸｾｽﾁｪｯｸ回路**  ﾒｯｾｰｼﾞに付されたｱﾄﾞﾚｽ情報に基づいて､ﾒｯｾｰｼﾞのｱｸｾｽ可否を判定するｱｸｾｽﾁｪｯｸ回路において､ｸﾞﾙｰﾌﾟ単位のｱﾄﾞﾚｽ情報に基づいて､ｱｸｾｽ可否を判定する包括ﾁｪｯｸ機能部と､端末単位のｱﾄﾞﾚｽ情報に基づいて､ｱｸｾｽ可否を判定する個別ﾁｪｯｸ機能部と､包括ﾁｪｯｸ機能部及び個別ﾁｪｯｸ機能部の双方又は一方の判定結果に基づいて､判定可否を最終判断する判定部とを備えたことを特徴とするｱｸｾｽﾁｪｯｸ回路。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID 認証情報	特開 2003-256315 02.02.27 G06F13/00,540	**複数のﾌﾛｰから構成されるｺﾝﾃﾝﾂ配信ｻｰﾋﾞｽ向けｹﾞｰﾄｳｪｲ装置､ﾏﾈｰｼﾞｬｻｰﾊﾞ装置､ｺﾝﾃﾝﾂ配信ｻｰﾊﾞ装置､およびｺﾝﾃﾝﾂ配信ｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID 認証情報	特開 2003-218951 01.08.28 H04L12/66	**ｹﾞｰﾄｳｪｲ装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID 認証情報	特開 2003-258919 02.02.27 H04L12/66	**複数ﾌﾛｰから構成されるｺﾝﾃﾝﾂ配信ｻｰﾋﾞｽ向けｹﾞｰﾄｳｪｲ装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開 2003-228550 02.02.05 G06F15/00,310	**違法ｺﾝﾃﾝﾂの配信制限方法およびｴｯｼﾞﾙｰﾀ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開 2004-062417 02.07.26 G06F15/00,330	**認証ｻｰﾊﾞ装置､ｻｰﾊﾞ装置､およびｹﾞｰﾄｳｪｲ装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特許 3528065 95.08.04 G06F15/00,330	**ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ上の対話継承型ｱｸｾｽ制御方法**  情報提供用のWorld-Wide Web を有するｻｰﾊﾞｺﾝﾋﾟｭｰﾀとWorld-Wide Web からの情報取得のためのﾌﾞﾗｳｻﾞを有するｸﾗｲｱﾝﾄｺﾝﾋﾟｭｰﾀを含むｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸにおけるｻｰﾊﾞ側のｱｸｾｽ制御方法であって、ｸﾗｲｱﾝﾄ側からの情報取得要求受信時、初回の情報取得要求か、第2 回目以降の情報取得要求かを判定し、初回の情報取得の場合は、ID 取得要求付き情報要求をもつ初期画面のﾊｲﾊﾟｰﾃｷｽﾄをｸﾗｲｱﾝﾄ側に返送し、第2 回目以降の情報取得要求の時､ID の取得要求があり情報提供条件を満たしたﾕｰｻﾞからの要求であった場合には、発行元ｻｰﾊﾞの明記された対話 ID を生成し、該対話 ID を対話記憶部に登録し、該対話 ID を付加したﾊｲﾊﾟｰﾃｷｽﾄをｸﾗｲｱﾝﾄに側に返送し、ID 取得要求でない情報取得要求の場合は､情報取得要求内の対話 ID を抽出し、該対話 ID から判明する発行元ｻｰﾊﾞに問い合わせを行い、該発行元ｻｰﾊﾞからのﾕｰｻﾞ認証の結果に基づき情報提供の可否の判定を行い、対話 ID が存在しない場合、または正規の対話 ID でない場合、または、正規の対話 ID でもﾕｰｻﾞの属性により情報提供を認めない場合には、ｱｸｾｽ拒否を行うことを特徴とするｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ上の対話継承型ｱｸｾｽ制御方法。

表 2.1.4 NTT の技術要素別課題対応特許(14/25)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	デバイスの正当性向上	各種の処理手順改良 特定情報の取得手順 ID 情報の取得	特開平 07-182287 (みなし取下) 93.12.22 G06F15/00,330	**ｱｸｾｽ制御方式**
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑ ID	特開 2003-069562 01.08.28 H04L9/32	**実行許可ﾁｹｯﾄを用いた認証ｼｽﾃﾑ及び方法､認証ﾌﾟﾛｸﾞﾗﾑ及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開 2002-163233 (特許 3741963) 00.09.13 G06F15/00,330	**ﾃﾞｰﾀ配送方法および装置およびﾌﾟﾛｸﾞﾗﾑおよび記録媒体**
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開 2002-297541 01.03.30 G06F15/00,330	**不正利用通知方法､不正利用通知装置および不正利用通知ﾌﾟﾛｸﾞﾗﾑ**
	経済性の向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特許 3557152 00.04.27 G06F13/00,351 〔被引用回数 1〕	**集中型ﾌｧｲｱｳｫｰﾙ装置** 概要は技術要素「ｺﾝﾃﾝﾂﾌｨﾙﾀﾘﾝｸﾞ」、課題「利用ｻｰﾋﾞｽの保護強化」の項参照
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID 認証情報	特開 2003-256315 02.02.27 G06F13/00,540	**複数のﾌﾛｰから構成されるｺﾝﾃﾝﾂ配信ｻｰﾋﾞｽ向けｹﾞｰﾄｳｪｲ装置､ﾏﾈｰｼﾞｬｻｰﾊﾞ装置､ｺﾝﾃﾝﾂ配信ｻｰﾊﾞ装置､およびｺﾝﾃﾝﾂ配信ｼｽﾃﾑ** 概要は技術要素「ｺﾝﾃﾝﾂﾌｨﾙﾀﾘﾝｸﾞ」、課題「利用ｻｰﾋﾞｽの保護強化」の項参照
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID 認証情報	特開 2003-258919 02.02.27 H04L12/66	**複数ﾌﾛｰから構成されるｺﾝﾃﾝﾂ配信ｻｰﾋﾞｽ向けｹﾞｰﾄｳｪｲ装置** 概要は技術要素「ｺﾝﾃﾝﾂﾌｨﾙﾀﾘﾝｸﾞ」、課題「利用ｻｰﾋﾞｽの保護強化」の項参照
ＩＰフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開 2003-324457 (みなし取下) 02.05.01 H04L12/46	**ｱｸｾｽ制御装置､方法､ﾌﾟﾛｸﾞﾗﾑおよび記録媒体**
		情報の送信、転送､分岐の手順改良 特定情報の通知、送信手順 警告情報	特開 2003-324460 (みなし取下) 02.05.08 H04L12/56	**ｱｸｾｽ制御時のｴﾗｰﾒｯｾｰｼﾞ表示方法およびｹﾞｰﾄｳｪｲ装置**
		情報の送信、転送､分岐の手順改良 特定情報の通知、送信手順 識別子､認証情報の送信	特開 2004-254010 03.02.19 H04L12/56	**SIP 通信制御装置**
		情報の送信、転送､分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開 2004-145583 02.10.24 G06F13/00,351	**ﾌｨﾙﾀﾘﾝｸﾞｼｽﾃﾑ**

表 2.1.4 NTT の技術要素別課題対応特許(15/25)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開 2004-187208 02.12.06 H04L12/66	ﾌｧｲｱｳｫｰﾙ多重装置およびﾊﾟｹｯﾄ振分け方法
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開 2001-358716 00.06.12 H04L12/24	論理閉域網管理方法及び装置ならびにﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
			特開 2004-062416 02.07.26 G06F13/00,351	不正ｱｸｾｽ防止方法、ｾｷｭﾘﾃｨﾎﾟﾘｼｰﾀﾞｳﾝﾛｰﾄﾞ方法、PC、およびﾎﾟﾘｼｰｻｰﾊﾞ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開 2005-086381 03.09.08 H04L12/56	ﾈｯﾄﾜｰｸ接続機器、通信方法、ﾌﾟﾛｸﾞﾗﾑおよびﾌﾟﾛｸﾞﾗﾑを記憶した記憶媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開 2004-187206 02.12.06 H04L12/66	ﾊﾟｰｿﾅﾙﾌｨﾙﾀﾘﾝｸﾞｼｽﾃﾑ及びﾊﾟｰｿﾅﾙﾌｨﾙﾀﾘﾝｸﾞ方法
			特開 2004-260470 03.02.25 H04L12/46	ﾎﾟﾘｼ制御装置
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開 2002-064543 00.08.14 H04L12/56	ﾊﾟｹｯﾄ処理方法及びその装置並びにﾊﾟｹｯﾄ処理ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特開 2003-242112 02.02.13 G06F15/00,330	ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ及び方法、ｾｷｭﾘﾃｨ管理ﾌﾟﾛｸﾞﾗﾑ及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 自動登録	特開 2004-220120 03.01.09 G06F15/00,330	ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｼｽﾃﾑ、ｱｸｾｽ制御方法、認証機構、ﾌｧｲｱｳｫｰﾙ機構、認証機構ﾌﾟﾛｸﾞﾗﾑ、ﾌｧｲｱｳｫｰﾙ機構ﾌﾟﾛｸﾞﾗﾑ及びその記録媒体
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼﾙｰﾙの追加、切換 ﾎﾟﾘｼﾙｰﾙの切換	特開 2003-244247 (みなし取下) 02.02.15 H04L12/66	ﾊﾟｹｯﾄﾌｨﾙﾀ分散方法及び分散化ﾊﾟｹｯﾄﾌｨﾙﾀｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼﾙｰﾙの追加、切換 ﾎﾟﾘｼﾙｰﾙの追加、学習	特開 2004-274552 03.03.11 H04L12/56,200	ｺﾝﾋﾟｭｰﾀ通信ｼｽﾃﾑおよびﾘｿｰｽ管理方法とﾌﾟﾛｸﾞﾗﾑおよび記録媒体
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 ﾄﾗﾌｨｯｸﾃﾞｰﾀの学習	特開 2005-027218 03.07.02 H04L12/66	ﾊﾟｹｯﾄ経路制御装置およびﾌｧｲｱｳｫｰﾙ負荷軽減方法
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開平 11-242625 (特許 3753535) 97.04.07 G06F12/00,537	WWW ｻｰﾊﾞのﾃﾞｰﾀ参照制限方法及びそのためのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体

表 2.1.4 NTT の技術要素別課題対応特許(16/25)

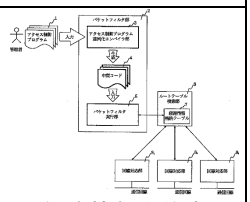
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開 2000-099428 （拒絶確定） 98.09.25 G06F13/00,353 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ間における情報の収集方法及びこれに用いるﾈｯﾄﾜｰｸ管理装置**
	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開 2005-005854 03.06.10 H04L12/56,100	**通信経路設定方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IP ｱﾄﾞﾚｽの割付 ｿｹｯﾄの割付	特開 2000-228674 99.02.04 H04L12/56	**複数拠点間通信におけるｱﾄﾞﾚｽ割り当て方法及び複数拠点間の通信方法並びにその接続装置**
	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開 2004-355285 03.05.28 G06F15/00,330	**ｾｷｭﾘﾃｨﾎﾟﾘｼ設定方法、装置およびﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞの配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特開 2004-363915 03.06.04 H04L12/22	**DoS 攻撃対策ｼｽﾃﾑおよび方法およびﾌﾟﾛｸﾞﾗﾑ**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開 2005-151039 03.11.13 H04L12/66	**攻撃ﾊﾟｹｯﾄ防御ｼｽﾃﾑ**
			特開 2005-130190 03.10.23 H04L12/66	**攻撃ﾊﾟｹｯﾄ防御ｼｽﾃﾑ**
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開 2002-335242 01.05.08 H04L9/38	**光信号伝送方法、WDM ﾈｯﾄﾜｰｸ伝送装置、及び光通信ﾈｯﾄﾜｰｸｼｽﾃﾑ**
ルーティング制御技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開 2003-244231 （特許 3712983） 02.02.13 H04L12/56,260	**ﾏﾙﾁｷｬｽﾄ通信制御方法及び通信制御装置並びに記録媒体及び制御ﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 中間ｺｰﾄﾞに変換	特許 3219186 96.08.27 H04L12/56 〔被引用回数 1〕	**ﾊﾟｹｯﾄ処理装置**  複数種類の比較ﾊﾟﾗﾒｰﾀからなるﾊﾟｹｯﾄ条件、および、ﾊﾟｹｯﾄ条件に一致したﾊﾟｹｯﾄの転送、あるいは、廃棄を定義する複数行のｱｸｾｽ制御規則からなるｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを入力し、該ｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑに従ってﾊﾟｹｯﾄのﾍｯﾀﾞを解析し、ﾊﾟｹｯﾄの転送、または、廃棄を決定するﾊﾟｹｯﾄﾌｨﾙﾀ部と、経路情報を検索して、転送ﾊﾟｹｯﾄの回線を決定するﾙｰﾄﾃｰﾌﾞﾙ検索部を有するﾊﾟｹｯﾄ処理装置において、前記ﾊﾟｹｯﾄﾌｨﾙﾀ部がｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑｺﾝﾊﾟｲﾗ部とﾊﾟｹｯﾄﾌｨﾙﾀ実行部とからなり、ｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑｺﾝﾊﾟｲﾗ部は、ｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを変換して中間ｺｰﾄﾞを生成する手段を有し、ﾊﾟｹｯﾄﾌｨﾙﾀ実行部は、前記中間ｺｰﾄﾞを解釈して、通信回線から受信したﾊﾟｹｯﾄのﾍｯﾀﾞ部分と比較し、比較結果に従ってﾊﾟｹｯﾄの転送あるいは廃棄を決定する手段を有することを特徴とするﾊﾟｹｯﾄ処理装置。

表 2.1.4 NTT の技術要素別課題対応特許(17/25)

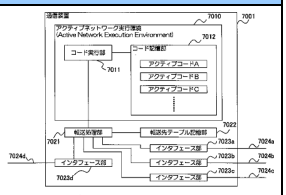
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
ルーティング制御技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾊﾟｹｯﾄｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特許 3657569 02.03.20 H04L12/56,100	**ﾊﾟｹｯﾄ処理方法および通信装置**  ﾊﾟｹｯﾄの送信元ｱﾄﾞﾚｽまたは宛先ｱﾄﾞﾚｽまたはそれら両方のｱﾄﾞﾚｽのﾊﾟﾀｰﾝとﾊﾟﾀｰﾝに対応するﾌﾟﾛｸﾞﾗﾑの情報とを予め転送先ﾃｰﾌﾞﾙに登録しておき、ﾊﾟｹｯﾄを受信した際に、この受信ﾊﾟｹｯﾄの送信元ｱﾄﾞﾚｽまたは宛先ｱﾄﾞﾚｽに基づいて転送先ﾃｰﾌﾞﾙを参照し、転送先ﾃｰﾌﾞﾙに登録されていたｱﾄﾞﾚｽのﾊﾟﾀｰﾝと、受信ﾊﾟｹｯﾄの送信元ｱﾄﾞﾚｽまたは宛先ｱﾄﾞﾚｽとがﾏｯﾁした場合に、ﾊﾟﾀｰﾝに対応するﾌﾟﾛｸﾞﾗﾑを起動して、起動されたﾌﾟﾛｸﾞﾗﾑに受信ﾊﾟｹｯﾄを渡すことを特徴とするﾊﾟｹｯﾄ処理方法。
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開平 11-282805 （みなし取下） 98.03.27 G06F15/00,330	**資源ｱｸｾｽ制御方法及びｼｽﾃﾑ及び資源ｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ併用	特開平 09-214540 （みなし取下） 96.02.02 H04L12/44	**ﾈｯﾄﾜｰｸおよびそのｸﾞﾙｰﾌﾟ管理方式**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑ ID	特開 2004-005690 98.03.26 G06F13/00,610	**ﾒｰﾙｱｸｾｽ制御方法、通信ｼｽﾃﾑ、およびﾒｰﾙｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開 2004-242161 03.02.07 H04L12/56	**ﾃﾞｰﾀ通信網ｼｽﾃﾑおよびﾃﾞｰﾀ通信網接続制御方法**
			特開 2004-015693 02.06.11 H04L12/56,260	**ﾊﾟｹｯﾄ転送方法および装置、ﾊﾟｹｯﾄ転送ﾌﾟﾛｸﾞﾗﾑおよびﾊﾟｹｯﾄ転送ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開 2004-248185 03.02.17 H04L12/56,100	**ﾈｯﾄﾜｰｸﾍﾞｰｽ分散型ｻｰﾋﾞｽ拒否攻撃防御ｼｽﾃﾑおよび通信装置**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開 2004-088657 （みなし取下） 02.08.28 H04L12/22	**ｱﾄﾞﾎｯｸﾈｯﾄﾜｰｸの無線端末及びｱﾄﾞﾎｯｸﾈｯﾄﾜｰｸ無線通信方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開 2001-188757 99.12.28 G06F15/00,330	**証明書を用いたｻｰﾋﾞｽ提供方法**
			特開 2004-248030 03.02.14 H04L12/56	**発信端末、着信端末、ﾊﾟｹｯﾄﾌｨﾙﾀｰ装置、通信制御装置、通信ｼｽﾃﾑ、通信方法、及びﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 識別子情報の変換	特開 2003-316742 （みなし取下） 02.04.24 G06F15/00,330	**ｼﾝｸﾞﾙｻｲﾝｵﾝ機能を有する匿名通信方法および装置**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IP ｱﾄﾞﾚｽの変換	特開 2003-069605 （特許 3696816） 01.08.28 H04L12/56	**ｱﾄﾞﾚｽ秘匿通信方法、ｼｽﾃﾑおよびﾌﾟﾗｲﾊﾞｼｰｹﾞｰﾄｳｪｲ**

表 2.1.4 NTT の技術要素別課題対応特許(18/25)

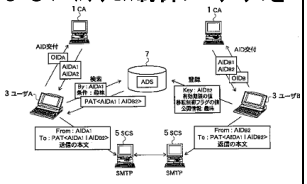
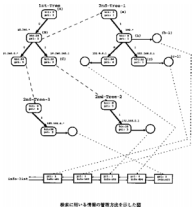
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 URL ﾄﾞﾒｲﾝの変換	特開平 11-177629 （拒絶確定） 97.12.11 H04L12/66	ｾｷｭﾘﾃｨｹﾞｰﾄｳｴｲｻｰﾊﾞおよび該ｻｰﾊﾞを用いた WWW ｻｰﾊﾞ URL 隠蔽方法と WWW ｻｰﾊﾞ URL 隠蔽ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾎﾟｰﾄ番号、NAT の変換	特開 2003-244245 （特許 3714549） 02.02.15 H04L12/66	ｹﾞｰﾄｳｴｲ装置及びそれによる通信方法
	システムの性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IP ｱﾄﾞﾚｽの変換	特開 2004-032453 （みなし取下） 02.06.26 H04L12/56,200	ﾊﾟｹｯﾄ通信ｼｽﾃﾑとこのｼｽﾃﾑで使用されるﾊﾟｹｯﾄ転送装置及びﾊﾟｹｯﾄ転送制御ﾌﾟﾛｸﾞﾗﾑ
	攻撃パターンの高精度化	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開平 10-126437 （みなし取下） 96.10.17 H04L12/54	分散ｵﾌﾞｼﾞｪｸﾄ通信方法
IP アドレス変換技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特許 3449941 98.03.26 H04L12/58,100 〔被引用回数 1〕	ﾒｰﾙｱｸｾｽ制御方法、通信ｼｽﾃﾑ、およびﾒｰﾙｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体  着信者にﾒｰﾙの送信を希望する発信者により着信者をﾒｰﾙの宛先として指定するために提示され、発信者識別子と着信者識別子を対応付けて含んだ個別化ｱｸｾｽﾁｹｯﾄを、発信者と着信者間の通信を接続するｾｷｭｱ･ｺﾐｭﾆｹｰｼｮﾝ･ｻｰﾋﾞｽにおいて受け取るｽﾃｯﾌﾟと、該ｾｷｭｱ･ｺﾐｭﾆｹｰｼｮﾝ･ｻｰﾋﾞｽにおいて、該個別化ｱｸｾｽﾁｹｯﾄに基づいて発信者の着信者に対するｱｸｾｽ権を検証することにより発信者と着信者間のｱｸｾｽを制御するｽﾃｯﾌﾟと、を有することを特徴とするﾒｰﾙｱｸｾｽ制御方法。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開 2005-031720 03.07.07 G06F13/00,351 ｴﾇ･ﾃｨ･ﾃｨ･ｱﾄﾞﾊﾞﾝｽﾃｸﾉﾛｼﾞ	高速検索対応高多重ﾕｰｻﾞ収容ﾌｧｲｱｳｫｰﾙ装置
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IP ｱﾄﾞﾚｽの変換	特開 2004-312483 03.04.09 H04L12/56,230	ﾒﾃﾞｨｱ通信方法及びﾒﾃﾞｨｱ通信ｼｽﾃﾑ
	通信データの中継性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの学習	特許 3591426 00.05.30 H04L12/66	ﾌﾟﾚﾌｨｯｸｽを含む複数ｱﾄﾞﾚｽによる連想情報探索方法及び装置  ｱﾄﾞﾚｽのﾌﾟﾚﾌｨｯｸｽの 2 つの組により指定され、かつ優先度付けがなされた情報の中から、あるｱﾄﾞﾚｽの組にﾏｯﾁする情報を優先度を考慮して探索する、ﾌﾟﾚﾌｨｯｸｽを含む複数ｱﾄﾞﾚｽによる連想情報探索方法であって、1 番目のﾌﾟﾚﾌｨｯｸｽにより 1 段目の 2 分木を構成し、1 段目の 2 分木の各葉に 1 番目のﾌﾟﾚﾌｨｯｸｽが該当するもののみによる 2 番目のﾌﾟﾚﾌｨｯｸｽによる 2 段目の 2 分木を構成し、2 段目の 2 分木の各葉には優先度付けされた情報を特定するものを線形ﾘｽﾄにより保持することにより情報を管理し、これを用いてｱﾄﾞﾚｽの組から情報の探索を行うことを特徴とする探索方法。

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(19/25)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPアドレス変換技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開 2005-159683 03.11.25 H04L12/66	情報通過制御ｼｽﾃﾑ、情報通過制御装置、ﾌﾟﾛｸﾞﾗﾑ及び記録媒体
	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開 2002-319938 （特許 3723896） 01.04.19 H04L12/22	ﾊﾟｹｯﾄ通信ﾈｯﾄﾜｰｸｼｽﾃﾑとｾｷｭﾘﾃｨ制御方法およびﾙｰﾃｨﾝｸﾞ装置ならびにﾌﾟﾛｸﾞﾗﾑと記録媒体
	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開 2001-111612 99.10.05 H04L12/56 〔被引用回数 1〕	情報漏洩防止方法およびｼｽﾃﾑ並びに情報漏洩防止ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
	侵入検出の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開 2005-005994 03.06.11 H04L12/66	ﾈｯﾄﾜｰｸ攻撃防止装置、ﾈｯﾄﾜｰｸ攻撃防止方法、ﾈｯﾄﾜｰｸ攻撃防止ﾌﾟﾛｸﾞﾗﾑ及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
ホスト認証技術	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑ ID	特開 2000-215165 99.01.26 G06F15/00,330	情報ｱｸｾｽ制御方法および装置と情報ｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開 2001-350722 （特許 3694219） 00.06.07 G06F15/00,330	情報表示ｼｽﾃﾑ及びｹﾞｰﾄｳｴｲ装置及び情報表示装置
			特開 2000-236342 99.02.17 H04L12/28	無線 LAN ｼｽﾃﾑ
		各種の処理手順改良 特定情報の記憶、登録手順 ｱﾄﾞﾚｽの記憶	特開 2003-169069 01.12.04 H04L12/44,300	IP ｱﾄﾞﾚｽを端末ｱｲﾃﾞﾝﾃｨﾃｨとして使用可能な IP ﾈｯﾄﾜｰｸ
		各種の処理手順改良 特定情報の記憶、登録手順 ﾛｸﾞ情報の記憶	特開 2004-260401 03.02.25 H04L9/08	通信制御ｼｽﾃﾑと通信制御方法およびﾌﾟﾛｸﾞﾗﾑと管理装置ならびに通信端末装置
		各種の処理手順改良 特定情報の取得手順 ID 情報の取得	特開 2003-173417 01.12.05 G06F17/60,332	料金代行徴収装置
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑ ID	特開平 08-223293 （拒絶確定） 95.02.20 H04M3/42 ｴﾇ・ﾃｨ・ﾃｨ・ｺﾐｭﾆｹｰｼｮﾝｽﾞ	通信回線を用いた情報提供ｻｰﾋﾞｽにおけるﾊﾟｽﾜｰﾄﾞ接続方法

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(20/25)

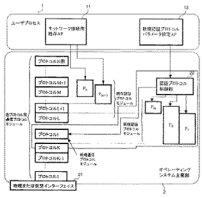
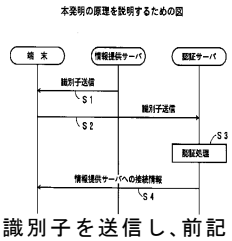
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開 2002-344474 01.05.14 H04L12/46	**CUG の構築方法、ﾈｯﾄﾜｰｸへの偽装ﾊﾟｹｯﾄ流入防止方法および偽装ﾊﾟｹｯﾄ流入防止機能付きﾈｯﾄﾜｰｸ**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特許 3656194 02.09.13 H04L29/06	**認証ﾌﾟﾛﾄｺﾙ処理方法、計算機端末、認証ﾌﾟﾛﾄｺﾙ処理ﾌﾟﾛｸﾞﾗﾑ、および記録媒体**  既存認証ﾌﾟﾛﾄｺﾙﾓｼﾞｭｰﾙから開始された認証ﾌﾟﾛﾄｺﾙ開始ﾊﾟｹｯﾄ、または前記既存認証ﾌﾟﾛﾄｺﾙﾓｼﾞｭｰﾙからの認証開始通知を、前記既存認証ﾌﾟﾛﾄｺﾙより下位で 1 つまたは複数の通信ﾌﾟﾛﾄｺﾙを処理する新規通信ﾌﾟﾛﾄｺﾙﾓｼﾞｭｰﾙの 1 つまたは複数で検出したことを新規認証ﾌﾟﾛﾄｺﾙの開始契機とし、1 つまたは複数の新規認証ﾌﾟﾛﾄｺﾙを実行するために必要な、新規認証ﾌﾟﾛﾄｺﾙ間の依存関係を管理し、前記依存関係に基づいた順序に従って前記新規認証ﾌﾟﾛﾄｺﾙの開始･実行を行ない、前記新規認証ﾌﾟﾛﾄｺﾙの開始契機として認証ﾌﾟﾛﾄｺﾙ開始ﾊﾟｹｯﾄを用いた場合には、新規認証ﾌﾟﾛﾄｺﾙの実行を完了できるまでの間、前記認証ﾌﾟﾛﾄｺﾙ開始ﾊﾟｹｯﾄを格納しておき、新規認証ﾌﾟﾛﾄｺﾙの実行完了後に前記認証ﾌﾟﾛﾄｺﾙ開始ﾊﾟｹｯﾄを新規通信ﾌﾟﾛﾄｺﾙの下位の通信ﾌﾟﾛﾄｺﾙに伝達し、既存認証ﾌﾟﾛﾄｺﾙの終了ﾊﾟｹｯﾄまたは認証終了通知を前記新規通信ﾌﾟﾛﾄｺﾙﾓｼﾞｭｰﾙの 1 つまたは複数で検出したことを契機として、前記依存関係に基づいた順序の逆順に前記新規認証ﾌﾟﾛﾄｺﾙの終了を行う認証ﾌﾟﾛﾄｺﾙ処理方法。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 情報提供ｻｰﾊﾞｰの配置	特開 2005-117466 03.10.09 H04L12/66	**通信制御ｼｽﾃﾑ、通信制御方法および通信制御ﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開 2002-132721 (拒絶確定) 00.10.27 G06F15/00,330	**ｻｰﾋﾞｽ提供方法、ｻｰﾋﾞｽ提供ｼｽﾃﾑ、ｻｰﾋﾞｽ提供ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体。**
			特開平 10-312362 (みなし取下) 97.05.14 G06F15/00,330	**ｱｸｾｽ制御ｼｽﾃﾑおよびｱｸｾｽ制御装置**
			特許 3496482 97.10.30 G06F15/00,330	**通信ﾈｯﾄﾜｰｸにおけるﾌｧｲﾙ識別方法及びｼｽﾃﾑ及び通信ﾈｯﾄﾜｰｸにおけるﾌｧｲﾙ識別ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**  ﾌｧｲﾙの提供を行うｻｰﾊﾞと、該ﾌｧｲﾙに含まれる情報について照合を行う機能を有したｻｰﾊﾞ(以下、認証ｻｰﾊﾞ)と、該ﾌｧｲﾙの受信を行う端末から構成される通信ﾈｯﾄﾜｰｸにおいて、該ﾌｧｲﾙの識別を行う通信ﾈｯﾄﾜｰｸにおけるﾌｧｲﾙ識別方法において、前記端末が前記情報提供ｻｰﾊﾞに要求したﾌｧｲﾙの受信を行う場合に、該情報提供ｻｰﾊﾞから該端末にﾌｧｲﾙの識別子を送信し、前記端末は前記ﾌｧｲﾙの識別子を前記認証ｻｰﾊﾞに転送し、前記認証ｻｰﾊﾞは、前記ﾌｧｲﾙの識別子に基づいて認証し、認証できた場合には前記端末が前記情報提供ｻｰﾊﾞに接続するための情報を該端末に送信することを特徴とする通信ﾈｯﾄﾜｰｸにおけるﾌｧｲﾙ識別方法。
			特開 2001-273258 (拒絶確定) 00.03.23 G06F15/00,330	**ﾕｰｻﾞ認証ｼｽﾃﾑ**

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(21/25)

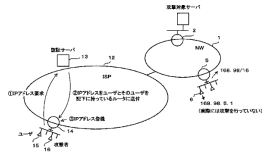
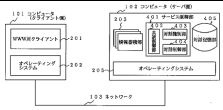
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
ホスト認証技術	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開 2004-023166 02.06.12 H04L12/28,310	**ﾓﾊﾞｲﾙ通信ｻｰﾋﾞｽｼｽﾃﾑ**
			特開 2004-363874 03.06.04 H04M1/663	**IP ﾈｯﾄﾜｰｸにおける通信端末登録方法、通信ｾｯｼｮﾝ確立方法、および端末**
			特許 3670242 02.02.15 H04L12/66	**送信元偽り攻撃制限ｻｰﾋﾞｽ方式およびﾙｰﾀ装置**  ﾕｰｻﾞ端末を IP 網に接続するﾙｰﾀと、このﾙｰﾀを介したﾕｰｻﾞ端末からの接続要求に対して IP ｱﾄﾞﾚｽを割り振る認証ｻｰﾊﾞとを備え、前記認証ｻｰﾊﾞは、前記接続要求に対して、認証済みの IP ｱﾄﾞﾚｽを要求元のﾕｰｻﾞ端末に加えてそのﾕｰｻﾞ端末を配下にもつﾙｰﾀに送付し、認証済みの IP ｱﾄﾞﾚｽが送付されたﾙｰﾀは、その IP ｱﾄﾞﾚｽを登録して保持するとともに、配下のﾕｰｻﾞ端末からのﾊﾟｹｯﾄの送信元 IP ｱﾄﾞﾚｽを監視し、登録された IP ｱﾄﾞﾚｽと異なるときには、そのﾊﾟｹｯﾄを廃棄するか、あるいは送信元偽りがあったことを保守者に通知することを特徴とする送信元偽り攻撃制限ｻｰﾋﾞｽ方式。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特開平 09-307580 （拒絶確定） 96.05.10 H04L12/46	**不正ﾊﾟｹｯﾄ防止方法およびﾌﾟﾘｯｼﾞ装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特許 3437680 95.05.24 G06F15/00,330 〔被引用回数 2〕	**対話管理型情報提供方法及び装置**  ｸﾗｲｱﾝﾄ側からの情報取得要求受信時、初回の情報取得要求か、第 2 回目以降の情報取得要求かを判別し、初回の情報取得要求の場合は、ID 取得要求付情報取得要求の URL を発行する初期画面をｸﾗｲｱﾝﾄ側に返送し、第 2 回目以降の情報取得要求の時、ID の取得要求があれば、対話 ID を生成し、対話 ID を対話記憶部に登録し、取得要求の情報内の URL に該対話 ID を付加し、情報をｸﾗｲｱﾝﾄ側へ送出し、ID の取得要求でない情報取得要求の場合､URL に対話 ID が付加されていれば、対話記憶部に対話 ID が記録されているかどうか検査し、記録されていればｱｸｾｽを記録し、送出すべき情報内の URL に対話 ID を付加し、情報をｸﾗｲｱﾝﾄ側へ送出し、URL に対話 ID が付加されていない場合、または、対話 ID が対話記憶部に記録されていない場合、ｱｸｾｽ拒否を行うことを特徴とする対話管理型情報提供方法。
			特開 2005-141654 03.11.10 G06F13/00	**情報通過制御ｼｽﾃﾑ、情報通過制御装置、ｻｰﾋﾞｽ提供装置、ﾌﾟﾛｸﾞﾗﾑ及び記録媒体**
			特開 2004-240819 03.02.07 G06F15/00,310	**認証機能付きﾊﾟｹｯﾄ通信装置、ﾈｯﾄﾜｰｸ認証ｱｸｾｽ制御ｻｰﾊﾞ、ｱﾌﾟﾘｹｰｼｮﾝ認証ｱｸｾｽ制御ｻｰﾊﾞ、および分散型認証ｱｸｾｽ制御ｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開 2005-142719 03.11.05 H04L9/32	**ﾒｯｾｰｼﾞ検証ｼｽﾃﾑ、ﾒｯｾｰｼﾞ検証方法およびﾒｯｾｰｼﾞ検証ﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開平 10-327144 （みなし取下） 97.05.22 H04L9/32	**仲介者認証方法及びその装置**
			特開 2005-080242 03.09.03 H04L9/32	**IP ｲﾝﾀﾌｪｰｽ情報の付与方法,その付与装置及びその付与ﾌﾟﾛｸﾞﾗﾑ並びにｱｸｾｽ認証装置**

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(22/25)

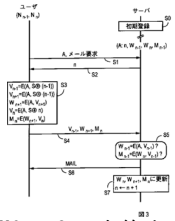
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
ホスト認証技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特開 2000-250409 99.03.04 G09C1/00,640	**情報利用･提供方法、そのｼｽﾃﾑ、装置及びﾌﾟﾛｸﾞﾗﾑ記録媒体**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IP ｱﾄﾞﾚｽの変換	特開 2001-273257 00.03.23 G06F15/00,330	**代理認証ｻｰﾊﾞ**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開平 09-016494 (拒絶確定) 95.06.26 G06F13/00,353	**ﾃﾞｰﾀ通信方法及びﾃﾞｰﾀ通信用ﾀｰﾐﾅﾙｱﾀﾞﾌﾟﾀ**
	システムの性能向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特許 3374716 96.09.11 H04L9/32	**ﾕｰｻﾞ認証機能を有する情報送受信制御方法及びその方法を記録した記録媒体**  ﾈｯﾄﾜｰｸ上でﾕｰｻﾞが利用するﾕｰｻﾞ端末装置と、認証者の認証者装置との間で認証処理を行うための情報送受信制御方法であり、以下のｽﾃｯﾌﾟを含む:(a) 初期登録手順として、上記ﾕｰｻﾞが、自分の識別子 A と、秘密に保持しているﾊﾟｽﾜｰﾄﾞ S から、次回認証ﾃﾞｰﾀ W0、次々回認証ﾃﾞｰﾀ W1、上記次々回認証ﾃﾞｰﾀ W1 の正当性検証ﾃﾞｰﾀ M0 の 3 つを算出し、認証回数 n の初期値 n=1 と共に上記認証者装置に上記識別子 A と対応して登録し、(b) 次に、n を正の整数とすると、第 n 回目の認証において、上記認証者装置は、上記ﾕｰｻﾞ端末装置からｻｰﾋﾞｽ起動要求と上記ﾕｰｻﾞの識別子 A の通知を受けて、そのﾕｰｻﾞの認証回数 n を読みだし、そのﾕｰｻﾞ端末装置へ通知し、(c) 上記ﾕｰｻﾞ端末装置では、上記ﾕｰｻﾞの識別子 A、送られてきた上記認証回数 n 及び秘密に保持しているﾊﾟｽﾜｰﾄﾞ S を用いて、今回の被認証ﾃﾞｰﾀ Vn-1、次々回の認証ﾃﾞｰﾀ Wn+1、次々回認証ﾃﾞｰﾀ Wn+1 の正当性検証ﾃﾞｰﾀ Mn を算出し、送信したいｺﾝﾃﾝﾂﾃﾞｰﾀがある場合にはそのﾃﾞｰﾀと共に上記認証者装置に通知し、(d) 上記認証者装置では、上記ﾕｰｻﾞの識別子 A と上記ｽﾃｯﾌﾟ(c) で送付されてきた今回の被認証ﾃﾞｰﾀ Vn-1 とから算出した今回の認証ﾃﾞｰﾀ Wn-1 を、登録されている認証ﾃﾞｰﾀ Wn-1 と比較し、かつ登録されている次回認証ﾃﾞｰﾀ Wn と、上記今回の被認証ﾃﾞｰﾀ Vn-1 とから計算した正当性検証ﾃﾞｰﾀ Mn-1 を、登録されている正当性検証ﾃﾞｰﾀ Mn-1 と比較し、(e) 上記ｽﾃｯﾌﾟ(d) の比較の結果、一致した場合、上記認証者装置ではそのﾕｰｻﾞを正当とし、上記ﾕｰｻﾞが要求したｻｰﾋﾞｽ情報の送受信を行うとともに、前回受けた次回認証ﾃﾞｰﾀ Wn と、今回送付されてきた次々回認証ﾃﾞｰﾀ Wn+1、と次々回認証ﾃﾞｰﾀの正当性検証ﾃﾞｰﾀ Mn を、前回登録した Wn-1, Wn, Mn-1 と置き換えて登録し、認証回数 n をｲﾝｸﾘﾒﾝﾄし、(f) 上記ｽﾃｯﾌﾟ(d) の比較の結果、一致しない場合、そのﾕｰｻﾞを不当とし以降の情報送受信を拒否し、前回登録したﾃﾞｰﾀ Wn-1, Wn, Mn 及び n をそのまま保持する。
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間･期間情報	特開 2003-134109 (特許 3754342) 01.10.30 H04L9/32	**公開鍵証明書の有効性検証ｼｽﾃﾑ**
			特開 2003-298580 02.04.05 H04L9/32	**失効公開鍵証明書ﾘｽﾄ生成装置、失効公開鍵証明書ﾘｽﾄ生成方法、ｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑおよびｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開 2004-248169 03.02.17 H04L12/66	**通信制御ｼｽﾃﾑと通信制御方法およびﾌﾟﾛｸﾞﾗﾑと通信端末装置**

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(23/25)

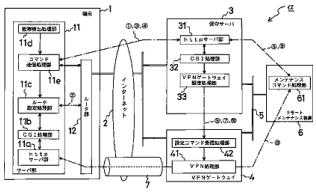
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
ホスト認証技術	情報、個人の正当性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開 2003-244125 （みなし取下） 02.02.15 H04L9/08	**情報伝達方法及び情報伝達装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特開 2000-244481 99.02.18 H04L9/32 〔被引用回数 1〕	**ｱｸｾｽ制御方法および装置とｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
トンネリング技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開 2000-165377 98.11.30 H04L9/14	**暗号ﾌﾟﾛﾄｺﾙ変換装置および方法と暗号ﾌﾟﾛﾄｺﾙ変換ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特開 2002-215576 01.01.17 G06F15/00,310	**遠隔処理呼び出し方法**
	システムの性能向上	情報の送信、転送、分岐の手順改良 情報転送の手順 VPN 設定情報	特許 3585411 00.01.05 H04L12/24	**端末-保守ｻｰﾊﾞ間認証鍵共有方法及び端末ﾘﾓｰﾄﾒﾝﾃﾅﾝｽ実施方法**  ｲﾝﾀｰﾈｯﾄに端末型ﾀﾞｲﾔﾙｱｯﾌﾟ接続された複数の端末と単一の保守ｻｰﾊﾞとの間で、OSI参照ﾓﾃﾞﾙのﾈｯﾄﾜｰｸ層において VPN ｾｯｼｮﾝを実現する IPsec の認証鍵を共有するに当り、前記端末の設置時に、当該端末と前記保守ｻｰﾊﾞとで事前に共有される第1の共有認証情報に基づいて前記保守ｻｰﾊﾞ内で前記端末の認証を行い、この認証が成功した場合に、当該保守ｻｰﾊﾞ内で前記 IPsec の認証鍵及び第 2 の共有認証情報をﾗﾝﾀﾞﾑに生成すると共に、これら生成した認証鍵及び第 2 の共有認証情報を、公開鍵暗号方式を用いて前記端末へ受け渡す設置通知処理と、該設置通知処理の完了に伴い、前記保守ｻｰﾊﾞから前記端末へ受け渡された前記認証鍵の設定を、当該端末のﾙｰﾀ部に書き込む端末 VPN 鍵設定処理と、を実行する、ことを特徴とする端末-保守ｻｰﾊﾞ間認証鍵共有方法。
		ﾌｧｲｱｳｫｰﾙﾀﾄのｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開 2004-312517 03.04.09 H04L12/56,100	**経路最適化ｼｽﾃﾑと方法およびﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開平 11-243388 98.02.26 H04L9/08 三菱電機	**暗号通信ｼｽﾃﾑ**
		各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開 2001-273256 00.03.23 G06F15/00,330	**情報伝達ｼｽﾃﾑ及び情報伝達方法**

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(24/25)

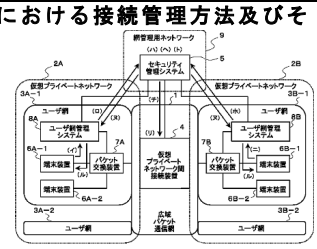
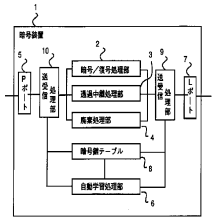
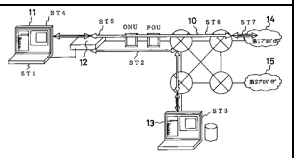
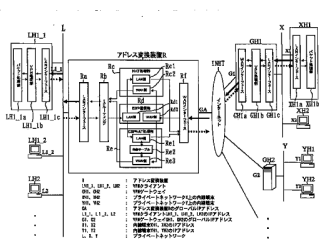
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 共同出願人 [被引用回数]	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	各種の処理手順改良 特定情報の取得手順 設定情報の取得	特開 2005-149337 03.11.19 G06F15/00	**ｹﾞｰﾄｳｪｲ装置**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開 2002-252607 00.12.22 H04L9/08	**情報配送方法及びその実施装置並びにその処理ﾌﾟﾛｸﾞﾗﾑと記録媒体**
		情報の送信、転送、分岐の手順改良 情報転送の手順 VPN 設定情報	特許 3566198 00.09.13 H04L12/24 〔被引用回数 2〕	**仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ間通信における接続管理方法及びその装置**  仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸを管理する管理者が該仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸに属するﾕｰｻﾞ網を管理するﾕｰｻﾞ網管理ｼｽﾃﾑに対して設定した仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ間通信の開設や設定変更のためのﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞやｱﾄﾞﾚｽ変換等に関する接続ﾙｰﾙを、該ﾕｰｻﾞ網管理ｼｽﾃﾑからｾｷｭﾘﾃｨ管理ｼｽﾃﾑへ送り、ｾｷｭﾘﾃｨ管理ｼｽﾃﾑでは一のﾕｰｻﾞ網管理ｼｽﾃﾑから送られた接続ﾙｰﾙを、該接続ﾙｰﾙにおける一の仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸの接続相手である他の仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸに属するﾕｰｻﾞ網を管理する他のﾕｰｻﾞ網管理ｼｽﾃﾑから送られた接続ﾙｰﾙと照合し、一致する接続ﾙｰﾙが存在する場合、該接続ﾙｰﾙを仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ間接続装置への設定情報に変換して配信することを特徴とする仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ間通信における接続管理方法。
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開 2000-312203 99.04.27 H04L9/08 〔被引用回数 1〕	**暗号通信の通過制御方法およびｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞの配置 ﾌﾟﾛｷｼｻｰﾊﾞの配置	特開 2004-304532 03.03.31 H04L12/56	**公開用管理ﾈｯﾄﾜｰｸ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 鍵情報	特許 3595145 97.06.02 H04L12/22 三菱電機 〔被引用回数 1〕	**暗号通信ｼｽﾃﾑ**  通信ﾈｯﾄﾜｰｸに収容された通信端末間を暗号装置が中継して暗号通信を行う暗号通信ｼｽﾃﾑにおいて、通信ﾃﾞｰﾀを中継する中継経路上の暗号装置は、中継する通信ﾃﾞｰﾀの送信元端末と宛先端末の組み合わせ(以下端末ﾍﾟｱと称す)に対応する暗号鍵情報が前記暗号装置の暗号鍵ﾃｰﾌﾞﾙに登録されていない場合、暗号鍵情報を収集するための鍵探索ﾊﾟｹｯﾄが前記中継経路上の各暗号装置自身の暗号情報を収集し、その収集した暗号情報を鍵探索応答ﾊﾟｹｯﾄが前記中継経路上の前記各暗号装置に通知し、通知を受けた前記各暗号装置は、収集した前記暗号鍵情報に基づいて、前記端末ﾍﾟｱに対応して通信ﾃﾞｰﾀを、暗号化するか、復号するか、透過中継するか、廃棄するか、いずれの処理を行うかを指定する暗号鍵情報を前記暗号鍵ﾃｰﾌﾞﾙに登録し、その端末ﾍﾟｱからの通信ﾃﾞｰﾀを中継する前記各暗号装置は前記暗号鍵ﾃｰﾌﾞﾙの暗号鍵情報に基づいて通信ﾃﾞｰﾀを処理することを特徴とする暗号通信ｼｽﾃﾑ。

表 2.1.4 NTT の技術要素Ⅱ別課題対応特許(25/25)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの切換	特開 2005-063132 03.08.12 G06F15/00,330	**分散ｼｽﾃﾑにおけるｾｷｭﾘﾃｨｱｿｼｴｰｼｮﾝ確立方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特許 3457259 00.05.30 H04L12/56,100	**ﾌﾟﾛﾊﾞｲﾀﾞ切換可能通信方法及びその装置**  仮想ﾛｰｶﾙｴﾘｱ･ﾈｯﾄﾜｰｸで構成されたﾊﾞｯｸﾎﾞｰﾝﾈｯﾄﾜｰｸを介して、ﾌﾟﾛﾊﾞｲﾀﾞとﾕｰｻﾞ端末との間で通信を行なう場合において、前記ﾕｰｻﾞ端末を前記ﾊﾞｯｸﾎﾞｰﾝﾈｯﾄﾜｰｸに接続するための装置をなす端末装置によって、当該ﾕｰｻﾞ端末から当該ﾌﾟﾛﾊﾞｲﾀﾞへ向けて送信された送信情報に、当該ﾌﾟﾛﾊﾞｲﾀﾞのIPｱﾄﾞﾚｽに対応した情報を含むVLANﾀｸﾞを付与し、当該VLANﾀｸﾞを用いて、当該送信情報を前記ﾊﾞｯｸﾎﾞｰﾝﾈｯﾄﾜｰｸを介して配送する、ことを特徴とするﾌﾟﾛﾊﾞｲﾀﾞ切換可能通信方法。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開 2003-229915 02.02.06 H04L12/66 〔被引用回数 2〕	**事業者 IP ﾈｯﾄﾜｰｸにおける IP 電話ｻｰﾋﾞｽ提供方法、およびｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾊﾟｹｯﾄｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特開 2004-015582 （みなし取下） 02.06.10 H04L12/66	**ｱｸﾃｲﾌﾞﾊﾟｹｯﾄにおけるﾊﾟｹｯﾄ認証および暗号化方法、ﾙｰﾀ装置、処理方法、ﾌﾟﾛｸﾞﾗﾑ、並びに記録媒体**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IP ｱﾄﾞﾚｽの変換	特開 2002-141939 （拒絶確定） 00.10.31 H04L12/56	**ｺﾝﾃﾝﾂ配信方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ｱﾄﾞﾚｽの暗号化	特許 3597756 00.06.09 H04L12/56 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ変換装置および VPN ｸﾗｲｱﾝﾄ多重化ｼｽﾃﾑ**  ﾊﾟｹｯﾄをﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸとｸﾞﾛｰﾊﾞﾙﾈｯﾄﾜｰｸとの間で送受信する際にﾈｯﾄﾜｰｸｱﾄﾞﾚｽを変換する方法において、受信したﾊﾟｹｯﾄがESP(Encapsulating Security Payload)か否かを判断するｽﾃｯﾌﾟと、ESPと判断された場合にｾｷｭﾘﾃｨｰﾊﾟﾗﾒｰﾀｲﾝﾃﾞｯｸｽと前記ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ上の端末のIPｱﾄﾞﾚｽとを対応付けた内部ﾃｰﾌﾞﾙを参照することにより、ESPのﾊﾟｹｯﾄにｱﾄﾞﾚｽ変換を施すｽﾃｯﾌﾟとを有することを特徴とするﾈｯﾄﾜｰｸｱﾄﾞﾚｽ変換方法。
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開 2000-232443 99.02.09 H04L9/32	**情報通過制御方法、ｹﾞｰﾄｳｪｲ装置及び記録媒体**

2.2 日立製作所

2.2.1 企業の概要

商号	株式会社　日立製作所
本社所在地	〒101-8010　東京都千代田区神田駿河台4-6 〒100-8280　東京都千代田区丸の内1-6-6
設立年	1920年（大正9年）
資本金	2,820億33百万円（2005年3月末）
従業員数	41,069名（2005年3月末）（連結：347,424名）
事業内容	総合電機（情報・通信システム、電子デバイス、電力・産業システム、デジタルメディア、民生機器等の製造・販売・サービス）

ネットワークのセキュリティに「網の目」は許されないとして、日立グループでセキュリティソリューションに対応したホームページ(Secureplaza)を開設し、セキュリティのサービス体系、セキュリティ製品やセキュリティ情報等を紹介している。

(出典：http://www.hitachi.co.jp/Prod/comp/Secureplaza/index.html)

2.2.2 製品例

Secureplazaに紹介されているファイアウォールやIDSの製品は下記のようになっており、表2.2.2に、製品例とその概要を示す。

表2.2.2 日立製作所の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
Astaro ファイアウォールソリュージョン	①　ファイアウォール,ウイルスソフト、スパムプロテクション、VPNやプロキシ機能を統合したオールインワン・ソフトウエア ②　PIX FireWall,FireWALL-1,NOKIA IP,NetScreen,CyberGuardを使用してファイアウォール運用管理、総合セキュリティソリューション、ファイアウォールマネジメントサービス
SWANStor VPNソリューション	柔軟なアクセスコントロールを有し、SSL-VPNによるセキュアリモートアクセスを実現するソフトウエア
侵入検知/IDSソリューション	①　Dragon,RealSecureなどを使用して不正検知システム ②　不正アクセス監視サービス ③　遠隔監視サービス
認証ソリューション	①　PKIのソリューション ②　シングルサインオンのソリューション

(出典：http://www.hitachi.co.jp/Prod/comp/Secureplaza/index.html)

2.2.3 技術開発拠点と研究者

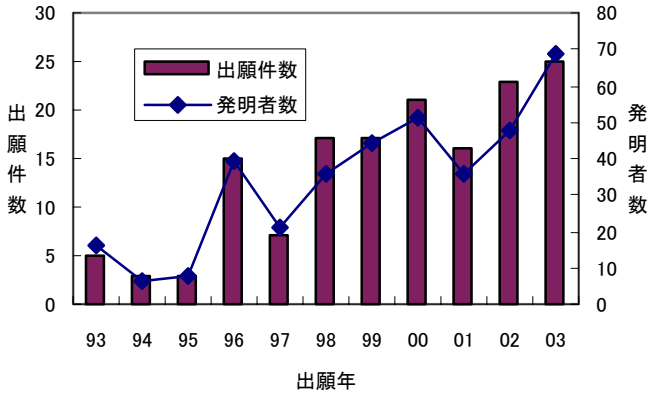
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

茨城県ひたちなか市稲田1410番地 株式会社日立製作所デジタルメディア事業部内
茨城県日立市幸町3丁目1番1号 株式会社日立製作所火力・水力事業部内
茨城県日立市大みか町7丁目2番1号 株式会社日立製作所内
埼玉県比企郡鳩山町赤沼2520番地 株式会社日立製作所基礎研究所内
神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所内
神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所内
神奈川県横浜市都筑区加賀原2丁目2番 株式会社日立製作所内
神奈川県海老名市下今泉810番地 株式会社日立製作所内
神奈川県小田原市国府津2820番地株式会社日立製作所ストレージシステム事業部内
神奈川県秦野市堀山下1番地 株式会社日立製作所内
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所内
神奈川県川崎市麻生区王禅寺1099株式会社日立製作所内
東京都江東区新砂1丁目6番27号 株式会社日立製作所内
東京都国分寺市東恋ヶ窪1丁目280番地 株式会社日立製作所中央研究所内
イギリス ケンブリッジ

図2.2.3に、日立製作所の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。出願件数は1996年以降、増加傾向にあり、03年に25件になり、発明者は60人に達している。

図2.2.3 日立製作所の不正アクセス侵入検知防御技術に関する出願件数と発明者数



2.2.4 技術開発課題対応特許の概要

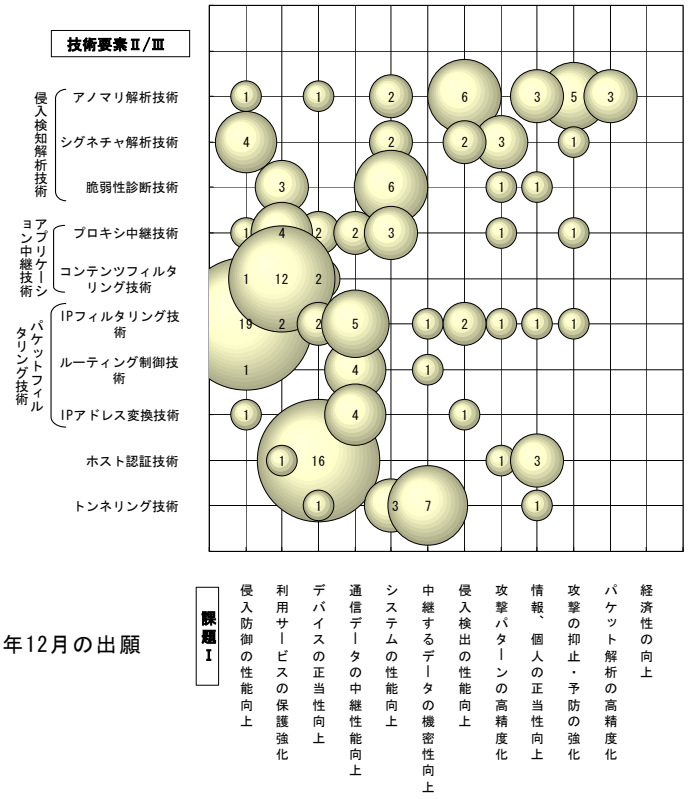
図2.2.4-1に、日立製作所の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.2.4-2に、日立製作所の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

IPフィルタリング技術が最も多く出願され、次いでアノマリ解析技術とホスト認証技術に関する出願が多い。これらの出願のうち、最も多い課題は、「侵入防御の性能向上」であり、次いで多い課題は「デバイスの正当性向上」である。

「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対

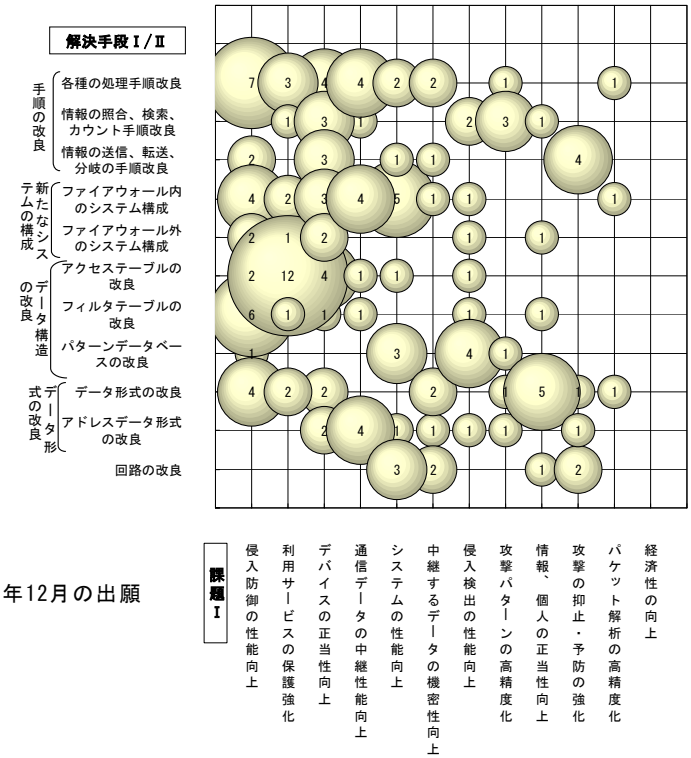
応している。次いで「侵入防御の性能向上」の課題に対しては、「各種の処理手順改良」で多く対応し、さらに「フィルタテーブルの改良」でも多く対応している。

図2.2.4-1 日立製作所の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.2.4-2日立製作所の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.2.4 日立製作所の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は152件で、そのうち15件が登録特許である。なお、表2.2.4では図

2.2.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段Ⅲと Ⅳまで分析している。

表2.2.4 日立製作所の技術要素別課題対応特許(1/17)

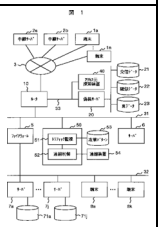
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開平07-262135 (拒絶確定) 94.03.17 G06F15/00,330 〔被引用回数 1〕	**ｾｷｭﾘﾃｨ管理装置**
	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2001-306514 00.04.24 G06F15/00,330	**ﾎｰﾑﾍﾟｰｼﾞ真正性維持方法及びその実施装置並びにその処理ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
	システムの性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 不正ｱｸｾｽ履歴情報の蓄積	特開2004-021572 02.06.17 G06F15/00,320	**ｱｸｾｽ情報管理ｻｰﾊﾞによるｼｽﾃﾑ稼動管理方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 帯域制限値の算出	特開2004-242222 03.02.10 H04L12/66	**ﾈｯﾄﾜｰｸ制御方法及びﾈｯﾄﾜｰｸ制御装置**
	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2000-354036 99.06.11 H04L12/24 〔被引用回数 1〕	**操作履歴ﾌｧｲﾙの保護方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特許3618245 99.03.09 H04L12/46 〔被引用回数14〕	**ﾈｯﾄﾜｰｸ監視ｼｽﾃﾑ**  外部ﾈｯﾄﾜｰｸからﾙｰﾀを通過して流入するﾊﾟｹｯﾄのﾄﾗﾌｨｯｸを監視し、内部情報ﾈｯﾄﾜｰｸを不正にｱｸｾｽするﾊﾟｹｯﾄを検出した時、ﾙｰﾀ装置宛に不正ﾊﾟｹｯﾄの識別情報を示す制御ﾊﾟｹｯﾄを送信するﾄﾗﾌｨｯｸ監視装置と、受信ﾊﾟｹｯﾄに応答して、ﾊﾟｹｯﾄの送信元に、意図的な情報を含む応答ﾊﾟｹｯﾄを送信する偽装ｻｰﾊﾞとを有し、ﾙｰﾀが、監視装置からの制御ﾊﾟｹｯﾄの受信に応答して、不正ﾊﾟｹｯﾄの識別情報を記憶するための手段を備え、外部ﾈｯﾄﾜｰｸから受信されたﾊﾟｹｯﾄの中から識別情報に基づいて不正ﾊﾟｹｯﾄを識別し、偽装ｻｰﾊﾞに転送することを特徴とするﾈｯﾄﾜｰｸ監視ｼｽﾃﾑ。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開平10-164064 (みなし取下) 96.12.05 H04L12/24 〔被引用回数 7〕	**ﾈｯﾄﾜｰｸ侵入経路追跡方式**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2004-318742 03.04.21 G06F13/00,351	**分散型ｻｰﾋﾞｽ不能攻撃を防ぐﾈｯﾄﾜｰｸｼｽﾃﾑ**
			特開2005-038116 03.07.18 G06F15/00,320	**不正侵入分析装置**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 ﾛｸﾞ情報の蓄積	特開2001-350677 00.06.06 G06F13/00,351	**ﾒﾀ情報を利用した通信の監視,検査ｼｽﾃﾑおよび通信の監視,検査方法、ならびにこれらの方法を記録した記録媒体**

表2.2.4 日立製作所の技術要素別課題対応特許(2/17)

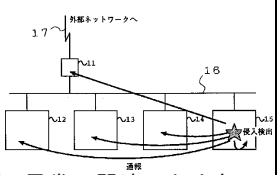
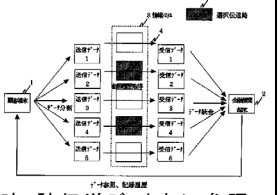
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
アノマリ解析技術	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2002-049590 00.08.04 G06F15/00,330 〔被引用回数 1〕	**電子公証ｼｽﾃﾑ**
			特開2004-102951 02.09.13 G06F15/00,330	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2002-156903 （特許3725020） 00.11.22 G09C1/00,640	**電子ﾃﾞｰﾀの内容証明方法及びそのｼｽﾃﾑ**
	攻撃の抑止・予防の強化	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開平09-269930 （拒絶確定） 96.04.03 G06F15/00,330 〔被引用回数 9〕	**ﾈｯﾄﾜｰｸｼｽﾃﾑの防疫方法及びその装置**
			特開平08-212164 （みなし取下） 95.02.02 G06F15/00,330	**情報処理方式**
			特開平11-134190 （拒絶確定） 97.10.31 G06F9/06,550 〔被引用回数 2〕	**ｳｲﾙｽ検出通知ｼｽﾃﾑおよび方法**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 容疑ﾚﾍﾞﾙ悪性閾値	特開2004-246444 03.02.12 G06F15/00,330	**ｾｷｭﾘﾃｨ基準検証方法及びその実施装置並びにその処理ﾌﾟﾛｸﾞﾗﾑ**
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特許3165366 96.02.08 G06F13/00,351 〔被引用回数 7〕	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｲｼｽﾃﾑ** 図１  計算機は計算機の内部状態を監視し異常の発生を検知する内部状態監視手段と、内部のﾘｿｰｽに対するｱｸｾｽの制御を行うｱｸｾｽ制御手段とを備えｱｸｾｽ制御手段は内部状態監視手段により異常の発生が検知されたとき、異常に関連した内部のﾘｿｰｽの保護処理を行うことを特徴とする。
	パケット解析の高精度化	各種の処理手順改良 特定情報の記憶、登録手順 ﾛｸﾞ情報の記憶	特許3537018 96.09.17 G06F17/60,240	**ﾃﾞｰﾀ伝送方法および情報ｼｽﾃﾑ**  顧客端末、金融機関端末および情報ｼｽﾃﾑの少なくとも1つに、伝送中の機密保護を要する情報の参照･記録の履歴情報を取得する参照履歴ﾌﾟﾛｸﾞﾗﾑを伝送ﾃﾞｰﾀとともに送信する送信手段と、該該機密情報が参照された時、該伝送ﾃﾞｰﾀ中に参照･履歴ﾃﾞｰﾀを記録する記録手段と、該参照履歴ﾌﾟﾛｸﾞﾗﾑを保持する保持手段と、情報管理者により確認された後に、該伝送ﾃﾞｰﾀ中の該機密情報を消去する消去手段とを具備することを特徴とする電子商取引におけるﾃﾞｰﾀ伝送ｼｽﾃﾑ。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2000-151602 98.11.18 H04L12/24	**ﾈｯﾄﾜｰｸ設定検査ｼｽﾃﾑ**

表2.2.4 日立製作所の技術要素別課題対応特許(3/17)

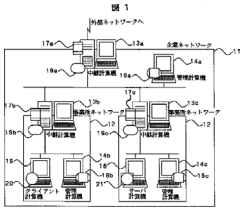
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	パケット解析の高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特許3497338 97.01.08 G06F13/00,351	**分散ﾛｸﾞ一括管理機能付きﾈｯﾄﾜｰｸｼｽﾃﾑ**  複数の中継装置に各々分散されて記録されているﾛｸﾞを一括管理するための管理装置を備え、計算機は、自身が属するﾈｯﾄﾜｰｸとは異なるﾈｯﾄﾜｰｸに属する計算機との間の通信経路を確立する際に、このとき確立すべき通信経路で行われる通信を識別するための識別子を生成する識別子生成手段と、通信経路の一部を自身との間で確立すべき中継装置に、識別子生成手段が生成した識別子を送信する識別子送信手段とを有し、中継装置は、計算機または他の中継装置から識別子が送信されてきた場合に、識別子が示す通信が行われる通信経路の一部を自身との間で確立すべき別の中継装置があるならば、識別子を別の中継装置に送信する識別子転送手段と、自身が中継する通信に係るﾛｸﾞを、通信の識別子を付加した形式で記録するﾛｸﾞ記録手段とを有し、管理装置は、ﾛｸﾞ調査の指示を受付ける受付手段と、受付手段がﾛｸﾞ調査の指示を受付けた場合に、自身と同じﾈｯﾄﾜｰｸに属する中継装置に、指示されたﾛｸﾞ調査を要求するﾛｸﾞ調査要求手段と、ﾛｸﾞ調査要求手段がﾛｸﾞ調査を要求した中継装置から調査結果が返送されてきた場合に、調査結果を出力する出力手段とを有し、中継装置は、さらに、管理装置または他の中継装置からﾛｸﾞ調査が要求された場合に、ﾛｸﾞ記録手段の記録内容のうちから、ﾛｸﾞ調査の対象として特定される通信の識別子に対応する内容を、調査結果として取得するﾛｸﾞ調査手段と、管理装置または他の中継装置から要求されたﾛｸﾞ調査の対象として特定される通信が行われた通信経路の一部を自身との間で確立した別の中継装置があるならば、ﾛｸﾞ調査を別の中継装置に要求するﾛｸﾞ調査要求転送手段と、ﾛｸﾞ調査要求転送手段が別の中継装置にﾛｸﾞ調査を要求しなかったならば、ﾛｸﾞ調査手段が取得した調査結果を、自身へのﾛｸﾞ調査の要求元に返送し、ﾛｸﾞ調査要求転送手段が別の中継装置にﾛｸﾞ調査を要求したならば、別の中継装置から調査結果が返送されてきた後で、返送されてきた調査結果とﾛｸﾞ調査手段が取得した調査結果とを合わせて、自身へのﾛｸﾞ調査の要求元に返送するﾛｸﾞ調査結果送信手段とを有することを特徴とする、分散ﾛｸﾞ一括管理機能付きﾈｯﾄﾜｰｸｼｽﾃﾑ。
シグネチャ解析技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2004-185455 02.12.05 G06F15/00,330	**情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの監査支援方法および装置**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開平09-218836 （みなし取下） 96.02.13 G06F13/00,351	**ﾈｯﾄﾜｰｸ用ｾｷｭﾘﾃｨ確保方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2004-356787 03.05.28 H04L12/66 日立ﾈｯﾄﾋﾞｼﾞﾈｽ	**ｾｷｭﾘﾃｨ検査ｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2002-290900 01.03.23 H04N5/91	**情報安全化装置及び情報保証ｼｽﾃﾑ**

表2.2.4 日立製作所の技術要素別課題対応特許(4/17)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
シグネチャ解析技術	システムの性能向上	ファイアウォール内のシステム構成 イントラネット内に機器の配置 位置識別子の配置	特開2005-142690 03.11.05 H04B7/26	情報処理装置及びその報知方法
		ファイアウォール内のシステム構成 イントラネット内に機器の配置 エージェントの配置	特開2005-141391 03.11.05 G06F11/30 日立電子サービス	エージェント駆動型監視システム及び方法
	侵入検出の性能向上	ファイアウォール外のシステム構成 セキュリティサーバーの配置 エッジノードにファイアウォール機能の分割配置	特開2001-345832 00.05.31 H04L12/54	メールシステム、メールガードド装置、操作端末
		パターンデータベースの改良 攻撃情報の蓄積 不正アクセス履歴情報の蓄積	特開2004-038517 (みなし取下) 02.07.03 G06F13/00,351	アクセス制御システム及び方法、プログラム
	攻撃パターンの高精度化	各種の処理手順改良 応答コマンドの処理手順 応答情報の検証	特開平09-266475 (みなし取下) 96.03.28 H04L12/22 〔被引用回数 4〕	アドレス情報管理装置およびネットワークシステム
		パターンデータベースの改良 攻撃パターンの追加、切換 アラートパターンの追加	特開2004-152251 02.09.04 G06F15/00,330	セキュリティに関する情報を更新する方法、クライアント、サーバ、及び管理端末
		アドレスデータ形式の改良 アドレスの変換 ポート番号、NATの変換	特開2005-005820 03.06.10 H04L12/46	フィルタリング装置に対するフィルタ設定情報管理方法
	攻撃の抑止・予防の強化	アドレスデータ形式の改良 IPアドレスの割付 ポート番号の割付	特開2003-281003 (みなし取下) 02.03.27 G06F13/00,351	システム稼動保証支援方法
脆弱性診断技術	利用サービスの保護強化	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2001-101135 99.09.29 G06F15/00,330 〔被引用回数 2〕	セキュリティ評価方法および装置、セキュリティ施策の作成支援方法および装置
		各種の処理手順改良 各種処理の実行手順 特定処理の実行	特開2003-258795 (みなし取下) 02.02.28 H04L12/22	コンピュータ集合体運用方法及びその実施システム並びにその処理プログラム
		アクセステーブルの改良 アプリケーションとの関連付け 業務・商品情報	特開2000-163375 98.11.30 G06F15/00,330	複数EDIシステム間でのアクセス権限管理方法
	システムの性能向上	各種の処理手順改良 各種処理の実行手順 特定処理の実行	特開2002-182560 00.12.12 G09C1/00,620	暗号処理機能を備えた情報サーバ装置

表2.2.4 日立製作所の技術要素別課題対応特許(5/17)

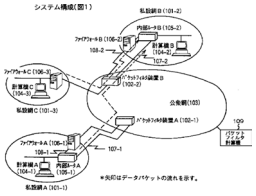
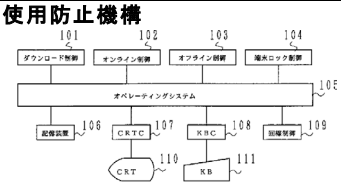
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
脆弱性診断技術	システムの性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 識別子、認証情報の送信	特開2003-141348 01.11.06 G06F17/60,176	**ﾌﾞﾘｯｼﾞﾒﾃﾞｨｱを用いた電子機器および通信方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数FWの配置	特開2000-216830 99.01.22 H04L12/66 〔被引用回数 1〕	**多段ﾌｧｲｱｳｫｰﾙｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開平09-214493 （みなし取下） 96.02.08 H04L12/24 〔被引用回数 2〕	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特許3599552 98.01.19 H04L12/66 〔被引用回数 2〕	**ﾊﾟｹｯﾄﾌｨﾙﾀ装置、認証ｻｰﾊﾞ、ﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ方法及び記憶媒体**  公衆網に接続される公衆接続部と、私設網に直接接続される私設接続部と、ﾌｧｲｱｳｫｰﾙに接続されるﾌｧｲｱｳｫｰﾙ接続部と、私設接続部で受信したﾃﾞｰﾀﾊﾟｹｯﾄにあらかじめ定めた認証情報を付加して公衆接続部から公衆網に送信し、ﾌｧｲｱｳｫｰﾙ接続部で受信したﾃﾞｰﾀﾊﾟｹｯﾄを公衆接続部から公衆網に送信するﾊﾟｹｯﾄ転送手段と、公衆接続部で受信したﾃﾞｰﾀﾊﾟｹｯﾄが、認証情報が付加されたﾃﾞｰﾀﾊﾟｹｯﾄであるかないかを判断し、認証情報が付加されたﾃﾞｰﾀﾊﾟｹｯﾄであれば、認証情報を取り除き、私設接続部からﾃﾞｰﾀﾊﾟｹｯﾄを送信し、認証情報が付加されたﾃﾞｰﾀﾊﾟｹｯﾄでなければﾌｧｲｱｳｫｰﾙ接続部からﾃﾞｰﾀﾊﾟｹｯﾄを送信するﾊﾟｹｯﾄ振り分け手段とを有することを特徴とするﾊﾟｹｯﾄﾌｨﾙﾀ装置。
	システムの性能向上	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2003-331373 02.05.14 G08B25/08	**警備ｼｽﾃﾑ**
	攻撃パターンの高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平09-265443 （みなし取下） 96.03.29 G06F13/00,357	**WWWｹﾞｰﾄｳｴｲｼｽﾃﾑ**
	情報、個人の正当性向上	回路の改良 ｽｲｯﾁ回路の追加 ﾛｯｸ回路の追加	特許2947448 93.12.27 G06F15/00,330 中部日立ｴﾚｸﾄﾘｯｸ,日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ，鉄道情報ｼｽﾃﾑ	**端末制御装置における不正使用防止機構**  端末制御装置は少なくとも ﾎｽﾄｺﾝﾋﾟｭｰﾀからのﾒｯｾｰｼﾞ受信を制御するﾀﾞｳﾝﾛｰﾄﾞ制御手段、ｵﾝﾗｲﾝ動作を制御するｵﾝﾗｲﾝ制御手段、ｵﾌﾗｲﾝ動作を制御するｵﾌﾗｲﾝ制御手段、および端末ﾛｯｸを制御する端末ﾛｯｸ制御手段とを有し、端末ﾛｯｸ制御手段に設定／解除が可能な端末ﾛｯｸﾌﾗｸﾞを設け、端末ﾛｯｸﾌﾗｸﾞが設定されているときにはｵﾝﾗｲﾝ制御手段の機能を抑止するとともにﾀﾞｳﾝﾛｰﾄﾞ制御手段の機能およびｵﾌﾗｲﾝ制御手段の機能を有効にするようにしたことを特徴とする端末制御装置における不正使用防止機構。

表2.2.4 日立製作所の技術要素別課題対応特許(6/17)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開2002-132718 00.10.20 G06F15/00,330	ｴﾝﾀｰﾌﾟﾗｲｽﾞｼｽﾃﾑにおける優先Web業務管理方法
	利用サービスの保護強化	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2003-256144 02.02.28 G06F3/06,301	記憶装置
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2003-050883 01.08.08 G06F17/60,138	技術支援ｺﾐｭﾆｹｰｼｮﾝｼｽﾃﾑ及び、技術支援方法
			特開2004-005705 00.02.09 G06F17/60,172	技術支援ｱﾝｻｰｼｽﾃﾑ及び、技術支援方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子透かしの埋め込み	特開2004-280227 03.03.13 G06F3/12 ｲｰﾌｫｰｼｰﾘﾝｸ,ﾍﾞｰｽﾃｸﾉﾛｼﾞｰ,三菱化学ﾒﾃﾞｨｱ,ｾｲｺｰｲﾝｽﾂﾙﾒﾝﾂ	文書管理ｼｽﾃﾑ
	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 ｱﾄﾞﾚｽの記憶	特開2002-278932 01.03.22 G06F15/00,330	情報処理装置および起動制御方法
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開平11-328117 （みなし取下） 98.05.14 G06F15/00,330 〔被引用回数 2〕	認証ｼｽﾃﾑにおけるﾕｰｻﾞ管理方法
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾊﾞｯｸｱｯﾌﾟｻｰﾊﾞｰの配置	特開2002-123435 00.10.17 G06F13/00,351	情報提供装置および方法
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2005-010871 03.06.17 G06F13/00,353	計算機通信制御方法およびｼｽﾃﾑ
	システムの性能向上	各種の処理手順改良 各種処理の実行手順 ﾊﾟﾀｰﾝ、ﾙｰﾙの言語記述	特開2004-272319 03.03.05 G06F12/14,320	ｾｷｭﾘﾃｨ性向上と管理容易化のための装置をもつた計算機と方法
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2004-048642 02.12.09 H04L12/66	宅内機器の制御方法、制御ｼｽﾃﾑ、宅内機器及びｹﾞｲﾄｳｪｲ
		回路の改良 処理回路の改良 ﾌｨﾙﾀﾘﾝｸﾞ回路の改良	特開2003-304293 （みなし取下） 02.04.10 H04L12/66	ﾊﾟｹｯﾄ中継装置

表2.2.4 日立製作所の技術要素別課題対応特許(7/17)

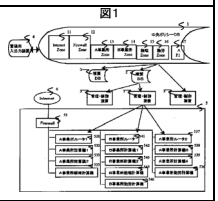
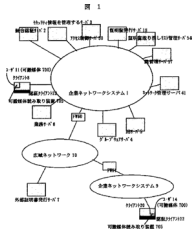
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開平10-269186 (みなし取下) 97.03.25 G06F15/16,370	**ｴｰｼﾞｪﾝﾄのｾｷｭﾘﾃｨ保護方式**
	攻撃の抑止・予防の強化	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｾｷｭﾘﾃｨｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	WO97-036246 96.03.22 G06F15/00,330	**ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸの管理方法および装置**
コンテンツフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2001-014239 99.06.29 G06F13/00,351	**多重ｼｽﾃﾑ並列稼働計算機によるｾｷｭﾘﾃｨｼｽﾃﾑ**
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開2001-022755 99.07.05 G06F17/30	**業務ﾃﾞｰﾀの検索処理方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ・ｸﾞﾙｰﾌﾟ	特許3659052 99.02.23 H04L12/66 〔被引用回数 3〕	**ﾈｯﾄﾜｰｸ管理ｼｽﾃﾑ**  ﾃﾞｰﾀﾍﾞｰｽに記憶される運用ﾎﾟﾘｼｰが、該ﾈｯﾄﾜｰｸを構成する機器で実行される業務内容の記述であり、業務内容の記述が適当な処理に基づきﾈｯﾄﾜｰｸを構成する機器の制御情報に変換されることを特徴とするﾈｯﾄﾜｰｸ管理ｼｽﾃﾑ。
			特開2002-318633 01.04.20 G06F1/00	**ﾌﾟﾛｸﾞﾗﾑ実行制限方法及び制限装置**
			特許3659019 98.09.29 G06F15/00,330	**可搬媒体を用いたｼﾝｸﾞﾙﾛｸﾞｲﾝ制御方法および該方法を実現するためのﾌﾟﾛｸﾞﾗﾑを格納した記録媒体および装置**  複数の業務に対するﾕｰｻﾞ認証処理を1回にするために、ﾕｰｻﾞが所持する可搬媒体に対するｱｸｾｽ可否判定手段、ｱｸｾｽ可否判定手段によりｱｸｾｽが許可された場合には、ﾕｰｻﾞ認証処理が必要な度に前記可搬媒体からｸﾗｲｱﾝﾄ側のﾕｰｻﾞ認証画面にﾕｰｻﾞ識別情報を送信する手段、ｱｸｾｽ可否判定手段によりｱｸｾｽが拒否された場合には、可搬媒体を無効にする手段、前記可搬媒体を用いたﾕｰｻﾞ認証処理を行なわないﾕｰｻﾞに対しては、業務のﾕｰｻﾞ認証処理ごとにﾕｰｻﾞ認証画面を表示する手段を備えることを特徴とするｼﾝｸﾞﾙﾛｸﾞｲﾝ方式のための画面制御方法。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2001-297179 00.02.09 G06F17/60,172 〔被引用回数 1〕	**技術支援ｱﾝｻｰｼｽﾃﾑ及び、技術支援方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開2004-282662 03.03.19 H04L12/66	**ﾎﾟﾘｼｰﾍﾞｰｽｼｽﾃﾑ設定支援装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開2002-318700 01.04.19 G06F9/46,350	**仮想計算機ｼｽﾃﾑの運用管理情報提供制御方法および仮想計算機ｼｽﾃﾑ**

表2.2.4 日立製作所の技術要素別課題対応特許(8/17)

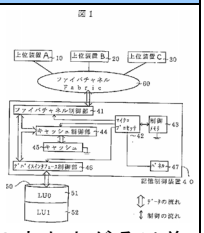
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特許3228182 97.05.29 G06F3/06,304	**記憶ｼｽﾃﾑ及び記憶ｼｽﾃﾑへのｱｸｾｽ方法**  ANSIX3T11で標準化されたﾌｧｲﾊﾞﾁｬﾈﾙを､上位装置と記憶制御装置間のｲﾝﾀﾌｪｰｽとし､上位装置､記憶制御装置､及び､記憶制御装置配下の磁気ﾃﾞｨｽｸﾄﾞﾗｲﾌﾞで構成された記憶装置から成るｺﾝﾋﾟｭｰﾀｼｽﾃﾑにおいて､上位装置から発行される､上位装置を一意に識別する情報であるN_Port_Name情報を､上位装置の立ち上がる以前に記憶制御装置に設置しておき､記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有し､上位装置が立ち上がった後､上位装置が､N_Port_Name情報を格納したﾌﾚｰﾑを記憶制御装置に対して発行し､記憶制御装置がこれを受領した際､既に設定され､保持されている上位装置を一意に識別するN_Port_Name情報と､受領したﾌﾚｰﾑに格納されたN_Port_Name情報とを比較する手段を有し､比較により一致した場合､当該ﾌﾚｰﾑの指示に基づく処理を継続し､不一致の場合､受領した当該ﾌﾚｰﾑを拒絶するLS_RJT(LinkService Reject)ﾌﾚｰﾑを上位装置に返し､上位装置からの不正ｱｸｾｽを抑止する手段を有することを特徴とするﾌｧｲﾊﾞﾁｬﾈﾙ接続記憶制御装置。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特開2004-192601 02.10.17 G06F12/14,310	**ﾎﾟﾘｼｰ設定支援ﾂｰﾙ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 時間､期限情報	特開2001-075920 99.09.07 G06F15/00,310	**ｻｰﾋﾞｽ取次装置を利用するｵﾝﾗｲﾝｻｰﾋﾞｽ提供方法及び取次装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 鍵情報	特開2002-374237 01.06.18 H04L9/08	**情報提供方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	WO00-013097 98.08.28 G06F17/30	**情報のｱｸｾｽ制御のためのｼｽﾃﾑ**
	デバイスの正当性向上	各種の処理手順改良 特定情報の取得手順 ID情報の取得	特開平07-121422 （みなし取下） 93.10.22 G06F12/00,537 日立ﾏｲｸﾛｿﾌﾄｳｪｱｼｽﾃﾑｽﾞ 〔被引用回数 1〕	**ﾌｧｲﾙｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開2004-334521 03.05.07 G06F12/14,310	**ｱｸｾｽ制御ｼｽﾃﾑ**
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却､制限	特開2000-267957 99.03.16 G06F13/00,351 〔被引用回数 1〕	**制御系用ﾌｧｲｱｳｫｰﾙ**

表2.2.4 日立製作所の技術要素別課題対応特許(9/17)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2005-018186 03.06.24 G06F15/00,330	ｱｸｾｽ管理方法及び装置並びにその処理ﾌﾟﾛｸﾞﾗﾑ
		各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2004-139372 02.10.18 G06F15/00,330	ﾌﾞﾗｳｻﾞｰ関連のｾｷｭﾘﾃｨﾁｪｯｸﾌﾟﾛｸﾞﾗﾑ
		各種の処理手順改良 各種処理の実行手順 特定処理の実行	特開2004-038819 02.07.08 G06F13/00,351	ｾｷｭﾘﾃｨｳｵｰﾙｼｽﾃﾑおよびそのﾌﾟﾛｸﾞﾗﾑ
		各種の処理手順改良 各種処理の実行手順 並列処理の実行	特開2000-083055 98.09.04 H04L12/56	ﾙｰﾀ
		各種の処理手順改良 特定情報の取得手順 設定情報の取得	特開2002-352062 01.05.24 G06F17/60,174	ｾｷｭﾘﾃｨ評価装置
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2004-021666 02.06.18 G06F15/00,310	ﾈｯﾄﾜｰｸｼｽﾃﾑ、ｻｰﾊﾞ、およびｻｰﾊﾞ設定方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開平07-141296 （みなし取下） 93.11.15 G06F15/00,330 〔被引用回数 3〕	ｵｰﾌﾟﾝな分散環境におけるｾｷｭﾘﾃｨ管理装置
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開平10-028144 （拒絶確定） 96.07.12 H04L12/66 〔被引用回数 5〕	ｱｸｾｽ制御機能付きﾈｯﾄﾜｰｸ構成方式
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開2000-216780 （特許3736173） 98.05.19 H04L12/24 〔被引用回数 2〕	ﾈｯﾄﾜｰｸ管理ｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2005-167864 03.12.05 H04L12/28	列車情報無線配信ｼｽﾃﾑ
			特開2004-247800 03.02.12 H04L29/06	ｹﾞｰﾄｳｴｲ装置、適応通信ｼｽﾃﾑ及びそれらの動作ﾌﾟﾛｸﾞﾗﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 ﾎﾟｰﾄ番号の登録	特開2003-348116 02.05.28 H04L12/46	家庭内ﾈｯﾄﾜｰｸ向けｱﾄﾞﾚｽ自動設定方式

表2.2.4 日立製作所の技術要素別課題Ⅰ対応特許(10/17)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの削除	特開2004-185178 02.12.02 G06F13/00,351	ﾌｨﾙﾀﾘﾝｸﾞ技術を用いたﾈｯﾄﾜｰｸｱｸｾｽ管理方法、ｼｽﾃﾑ及びﾌﾟﾛｸﾞﾗﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの追加、学習	特開2003-196476 01.12.27 G06F17/60,174	ｾｷｭﾘﾃｨﾎﾟﾘｼｰの作成支援ｼｽﾃﾑおよびｾｷｭﾘﾃｨ対策決定支援ｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 質問形式での追加､学習	特開2002-247033 (特許3744361) 01.02.16 H04L12/24 〔被引用回数 2〕	ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 特徴単語の学習	特開2000-122959 98.10.20 G06F13/00,354	通信ﾃﾞｰﾀのﾌｨﾙﾀﾘﾝｸﾞ方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子透かしの埋め込み	特開2001-005757 99.06.23 G06F13/00,351	電子透かしを利用したﾃﾞｰﾀのﾌｨﾙﾀﾘﾝｸﾞｼｽﾃﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開平11-259367 (みなし取下) 98.03.10 G06F12/14,320	ﾈｯﾄﾜｰｸｺﾝﾋﾟｭｰﾀｰ端末装置
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2000-029830 (みなし取下) 98.07.09 G06F15/00,310	ﾃﾞｰﾀ管理ｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2003-140994 01.11.01 G06F13/00,351	ﾌｧｲｱｳｵｰﾙ計算機ｼｽﾃﾑ
	デバイスの正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開2000-010930 (みなし取下) 98.06.24 G06F15/00,330	ﾈｯﾄﾜｰｸｼｽﾃﾑでのｱｸｾｽ制御方法
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 IPv6の割付	特開2003-115880 01.10.04 H04L12/66 〔被引用回数 1〕	ﾌｧｲｱｳｵｰﾙ装置、情報機器および情報機器の通信方法
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開2001-237829 00.02.24 H04L12/18	映像配送ｼｽﾃﾑにおけるﾋﾞﾃﾞｵｻｰﾊﾞ装置
		各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開平11-032086 (みなし取下) 97.07.09 H04L12/66	ﾈｯﾄﾜｰｸ間中継処理方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数FWの配置	特開2004-048520 (みなし取下) 02.07.15 H04L12/66	ﾎﾟｰﾄｱｸｾｽ制御ｼｽﾃﾑ
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2004-192044 02.12.06 G06F13/00,351	ﾌｧｲｱｳｵｰﾙ,及びﾎﾟｰﾄ番号切替えﾌﾟﾛｸﾞﾗﾑを記憶した記憶媒体

表2.2.4 日立製作所の技術要素別課題Ⅰ対応特許(11/17)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	中継するデータの機密性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の停止、取消し	特開2000-349821 99.06.08 H04L12/56 〔被引用回数 2〕	ﾎﾟｰﾄｱｸｾｽ制御ｼｽﾃﾑとFTPﾃﾞｰﾀｺﾈｸｼｮﾝ確立方法およびﾌｧｲｱｳｫｰﾙ
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2004-259225 03.02.28 G06F15/00,330 日立ｴﾝｼﾞﾆｱﾘﾝｸﾞ	ｽﾄﾘｰﾑ配信計算機、ﾌﾟﾛｸﾞﾗﾑ、NAS装置
	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開2000-215164 99.01.26 G06F15/00,330 〔被引用回数 2〕	ｺﾝﾋﾟｭｰﾀ不正利用者の接続元追跡方法
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2001-236278 00.02.25 G06F13/00,351 日立情報制御ｼｽﾃﾑ	計算機ｼｽﾃﾑ
	攻撃パターンの高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾊﾟｹｯﾄのﾌｨｰﾙﾄﾞ	特開平08-130538 (みなし取下) 94.10.31 H04L12/22	ﾊﾟｹｯﾄ中継の方法およびｲﾝﾀﾈｯﾄﾜｰｸ装置
	情報、個人の正当性向上	ﾌｨﾙﾀTBLの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2005-151437 03.11.19 H04L12/66	記憶装置、記憶装置ｼｽﾃﾑ、および、通信制御方法
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2002-084306 00.06.29 H04L12/46 〔被引用回数 1〕	ﾊﾟｹｯﾄ通信装置及びﾈｯﾄﾜｰｸｼｽﾃﾑ
ルーティング制御技術	侵入防御の性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙの照合	特開2001-034553 99.07.26 G06F13/00,351 〔被引用回数 3〕	ﾈｯﾄﾜｰｸｱｸｾｽ制御方法及びその装置
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開平08-008974 (みなし取下) 94.06.16 H04L12/66 日立情報制御ｼｽﾃﾑ 〔被引用回数 1〕	経路制御装置
		各種の処理手順改良 各種処理の実行手順 ﾊﾟﾀｰﾝ、ﾙｰﾙの言語記述	特開2003-229913 02.02.04 H04L12/66	ﾈｯﾄﾜｰｸ接続ｼｽﾃﾑ、ﾈｯﾄﾜｰｸ接続方法、および、それらに用いられるﾈｯﾄﾜｰｸ接続装置
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開2001-251367 (特許3692943) 96.10.18 H04L12/66 〔被引用回数 2〕	通信ｸﾗｲｱﾝﾄ装置

表2.2.4 日立製作所の技術要素別課題Ｉ対応特許(12/17)

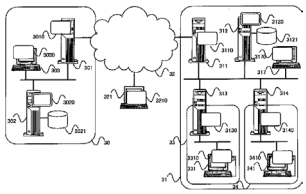
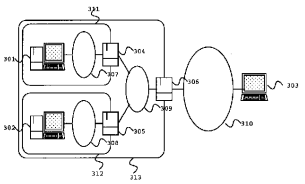
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
ルーティング制御技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特許3253542 96.11.22 G06F13/00,351 〔被引用回数 4〕	**ﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ** 図1  ﾃﾞｨﾚｸﾄﾘｻｰﾋﾞｽ計算機は、ﾈｯﾄﾜｰｸを構成する各計算機を識別するための識別情報と、各計算機にｱｸｾｽ可能なﾕｰｻﾞを規定したﾕｰｻﾞ情報と、各計算機の前記ﾈｯﾄﾜｰｸにおける通信経路を規定した経路情報とが格納されたﾃﾞｰﾀﾍﾞｰｽと、ｸﾗｲｱﾝﾄ計算機から、ｻｰﾊﾞ計算機の識別情報と、ｸﾗｲｱﾝﾄ計算機のﾕｰｻﾞを指定する情報とを受け付ける手段と、受け付けた情報を基に、ﾃﾞｰﾀﾍﾞｰｽに格納された識別情報およびﾕｰｻﾞ情報を検索して、ｸﾗｲｱﾝﾄ計算機のﾕｰｻﾞがｻｰﾊﾞ計算機の正当なﾕｰｻﾞであるか否かを判定する判定手段と、ｸﾗｲｱﾝﾄ計算機のﾕｰｻﾞがｻｰﾊﾞ計算機の正当なﾕｰｻﾞである場合、ﾃﾞｰﾀﾍﾞｰｽに格納された経路情報の内の、中継ｻｰﾊﾞ計算機からｻｰﾊﾞ計算機に到る通信経路を規定した経路情報を中継ｻｰﾊﾞ計算機へ送る手段とを有し、中継ｻｰﾊﾞ計算機は、ﾃﾞｨﾚｸﾄﾘｻｰﾋﾞｽ計算機から送られた経路情報で示される通信経路でｸﾗｲｱﾝﾄ計算機の通信を中継する手段を有することを特徴とするﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ。
	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特許3587633 96.10.18 H04L12/22 〔被引用回数 4〕	**ﾈｯﾄﾜｰｸ通信方法および装置** 図3  ｸﾗｲｱﾝﾄ上の通信ｸﾗｲｱﾝﾄﾌﾟﾛｸﾞﾗﾑとｻｰﾊﾞ上の通信ｻｰﾊﾞﾌﾟﾛｸﾞﾗﾑとの通信中継機能を備えた通信中継ﾌﾟﾛｸﾞﾗﾑを有する中継ｻｰﾊﾞをﾈｯﾄﾜｰｸ上に配置し、中継ｻｰﾊﾞとｸﾗｲｱﾝﾄに、ｻｰﾊﾞｱﾄﾞﾚｽとｻｰﾊﾞへの通信を中継する前記中継ｻｰﾊﾞのｱﾄﾞﾚｽとの対応関係を記憶した中継経路制御ﾃｰﾌﾞﾙを備え、中継ｻｰﾊﾞおよびｸﾗｲｱﾝﾄは、ﾌｧｲｱｳｫｰﾙにより直接通信できないｻｰﾊﾞとの通信時に、前記中継経路ﾃｰﾌﾞﾙを参照して中継に使用する中継ｻｰﾊﾞを選択し、中継ｻｰﾊﾞ網によるﾈｯﾄﾜｰｸを利用して通信を行なうことを特徴とするﾈｯﾄﾜｰｸ通信方法。

表2.2.4 日立製作所の技術要素別課題Ⅰ対応特許(13/17)

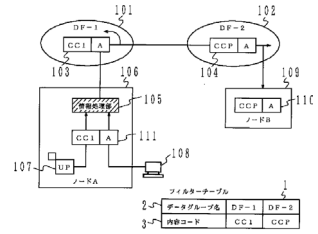
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPアドレス変換技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特許3097525 95.11.10 H04L12/46 日立ﾌﾟﾛｾｽｺﾝﾋﾟｭｰﾀｴﾝｼﾞﾆｱﾘﾝｸﾞ	**情報ﾌｨﾙﾀﾘﾝｸﾞ処理を行うﾃﾞｰﾀ伝送方法**  複数の属性を有するﾃﾞｰﾀを計算機Aから伝送路に送信する場合、伝送路内の伝送ﾃﾞｰﾀには、伝送ﾃﾞｰﾀの属性に対応するﾃﾞｰﾀの送信範囲を決定する情報を指定するｴﾘｱと、ﾃﾞｰﾀを受信する計算機の受信の可否を判定する条件となる情報を指定するｴﾘｱとを設け、ﾃﾞｰﾀを送信する計算機A内のﾕｰｻﾞﾌﾟﾛｸﾞﾗﾑは、受信の可否を判定する条件となる情報と、ﾃﾞｰﾀが持つ属性で設定されるﾃﾞｰﾀｸﾞﾙｰﾌﾟを示す情報と、ﾃﾞｰﾀの内容を指定して計算機Aに送出し、計算機Aは、指定された受信計算機での受信の可否を判定する条件となる情報と、ﾃﾞｰﾀｸﾞﾙｰﾌﾟを基に、ﾃﾞｰﾀが持つ他の属性に対応するﾃﾞｰﾀｸﾞﾙｰﾌﾟの情報と、ﾃﾞｰﾀｸﾞﾙｰﾌﾟでの受信計算機での受信の可否を判定する条件となる情報とを対応させ、かつﾃﾞｰﾀｸﾞﾙｰﾌﾟのﾃﾞｰﾀを送信する全ての計算機が共有するﾌｨﾙﾀｰ情報を有し、計算機Aは、ﾌｨﾙﾀｰ情報を基に、ﾃﾞｰﾀｸﾞﾙｰﾌﾟ毎の受信計算機での受信の可否を判定する条件となる情報を取得し、各ﾃﾞｰﾀｸﾞﾙｰﾌﾟ毎にそのﾃﾞｰﾀ送信範囲情報と、受信計算機での受信の可否を判定する条件となる情報の両方を付加して伝送路に送信し、ｼｽﾃﾑ内の各伝送路間を結ぶ計算機Bは、伝送ﾃﾞｰﾀが該伝送路を流れる時には、伝送ﾃﾞｰﾀに付加された送信範囲情報を基に、伝送ﾃﾞｰﾀを該ﾃﾞｰﾀ内で指定された送信範囲に中継送信し、計算機A,B以外の計算機Cは、伝送ﾃﾞｰﾀが複数の属性を有することを意識することなく、伝送ﾃﾞｰﾀの送信範囲内にある場合のみ、かつ伝送ﾃﾞｰﾀに指定された受信計算機での受信の可否を判定する条件となる情報に示された条件が一致する場合のみ、伝送ﾃﾞｰﾀを受信することを特徴とする情報ﾌｨﾙﾀﾘﾝｸﾞ処理を行うﾃﾞｰﾀ伝送方法。
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2004-015773 02.06.12 H04L9/32	**ﾈｯﾄﾜｰｸ上の位置情報を取得するｻｰﾊﾞ、およびｻｰﾋﾞｽ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2001-244996 00.02.29 H04L12/66 日立情報制御ｼｽﾃﾑ	**ﾈｯﾄﾜｰｸのｾｷｭﾘﾃｨ保護方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾎﾟｰﾄ番号、NATの変換	特開2002-132596 00.10.27 G06F13/00,351	**ﾎﾟｰﾄ番号の収束、展開方法及びそのｹﾞｰﾄｳｪｲｻｰﾊﾞ**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ｿｹｯﾄの割付	特開平11-032088 (みなし取下) 97.07.11 H04L12/66 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**

表2.2.4 日立製作所の技術要素別課題Ⅰ対応特許(14/17)

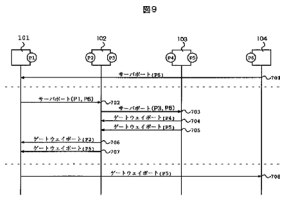
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPアドレス変換技術	侵入検出の性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾎﾟｰﾄ番号、NATの変換	特許3354433 97.04.25 H04L12/56 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ**  各代理ｻｰﾊﾞ計算機は、ｻｰﾊﾞ計算機の通信ｱﾄﾞﾚｽおよび割り振ったﾎﾟｰﾄ番号を、ｸﾗｲｱﾝﾄ計算機から、ｻｰﾊﾞ計算機に接続される代理ｻｰﾊﾞ計算機にかけて転送する手段と、転送に応じて、自代理ｻｰﾊﾞ計算機の通信ｱﾄﾞﾚｽおよび割り振ったﾎﾟｰﾄ番号を返送する手段と、ｻｰﾊﾞ計算機に接続される代理ｻｰﾊﾞ計算機から返送された通信ｱﾄﾞﾚｽおよび割り振ったﾎﾟｰﾄ番号を識別し、通信ｱﾄﾞﾚｽおよび割り振ったﾎﾟｰﾄ番号をｸﾗｲｱﾝﾄ計算機にかけて転送する手段とを備え、ｸﾗｲｱﾝﾄ計算機は、前記ｻｰﾊﾞ計算機との間で、ｻｰﾊﾞ計算機の通信ｱﾄﾞﾚｽおよび割り振ったﾎﾟｰﾄ番号と、ｻｰﾊﾞ計算機に接続される代理ｻｰﾊﾞ計算機の通信ｱﾄﾞﾚｽおよび割り振ったﾎﾟｰﾄ番号とを交換する手段とを備えることを特徴とするﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ。
ホスト認証技術	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2003-108519 01.09.27 G06F15/00,330	**ﾌｧｲﾙ転送ｼｽﾃﾑ及びﾌﾟﾛｸﾞﾗﾑ**
	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開平11-331142 （みなし取下） 98.05.08 H04L9/08	**公開鍵証書管理方法および装置**
		各種の処理手順改良 特定情報の記憶、登録手順 要求情報の記憶	特開2000-029833 98.07.14 G06F15/00,330	**ﾃﾞｰﾀのｱｸｾｽ方法**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2001-060183 99.08.24 G06F15/00,330	**記憶装置及びﾎｽﾄ装置**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 順番号の検証	特開2003-143126 （みなし取下） 01.11.05 H04L9/08 通信・放送機構	**ｾｷｭﾘﾃｨ保持方法及びその実施ｼｽﾃﾑ並びにその処理ﾌﾟﾛｾｽ**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2004-272724 03.03.11 G06F15/00,330	**ﾋﾟｱｰﾂｰﾋﾟｱ通信装置および通信方法**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特開2001-202332 00.01.17 G06F15/00,330	**認証ﾌﾟﾛｸﾞﾗﾑ管理ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2004-274521 03.03.11 H04L9/32	**ｻｰﾊﾞ装置、端末制御装置及び端末認証方法**

表2.2.4 日立製作所の技術要素別課題対応特許(15/17)

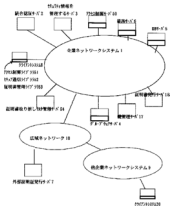
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2003-124926 01.10.15 H04L9/32	**暗号化通信ｼｽﾃﾑにおける認証処理方法及びそのｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2002-132714 00.10.27 G06F15/00,310 〔被引用回数 1〕	**ｻｰﾋﾞｽ提供方法および装置**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2004-140779 02.10.18 H04L12/28,310	**ｼｽﾃﾑおよび通信方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特開平09-244976 (みなし取下) 96.03.08 G06F13/00,351 日立ｺﾝﾋﾟｭｰﾀｴﾝｼﾞﾆｱﾘﾝｸﾞ 〔被引用回数 3〕	**ｾｷｭﾘﾃｨｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開平06-274431 (みなし取下) 93.03.17 G06F13/00,357 〔被引用回数 1〕	**異機種接続環境における認証および認可方法**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平07-079243 (みなし取下) 93.07.13 H04L12/40	**ﾈｯﾄﾜｰｸ接続装置およびﾈｯﾄﾜｰｸ接続方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特許3678009 98.07.23 H04L9/32	**通信方法**  ﾈｯﾄﾜｰｸを介してｸﾗｲｱﾝﾄ､業務ｻｰﾊﾞ及び証明書取り消しﾘｽﾄを管理するｻｰﾊﾞが接続され､証明書を利用して相互認証することにより通信可能なﾈｯﾄﾜｰｸｼｽﾃﾑにおいて､ﾕｰｻﾞが通信相手を認証するために証明書を取得する手段と､ﾕｰｻﾞが前記証明書を取得した通信相手を記憶する手段と､前記記憶された通信相手に関する証明書取り消しﾘｽﾄを前記ﾕｰｻﾞに自動的に配送する手段､あるいは前記ﾕｰｻﾞから前記記憶された通信相手に関する証明書取り消しﾘｽﾄを問い合わせる手段を備えることを特徴とする証明書取り消しﾘｽﾄの管理方法。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 鍵情報のﾊﾟｯｸ化	特開平08-335207 (みなし取下) 95.06.07 G06F15/00,330	**ﾈｯﾄﾜｰｸﾕｰｻﾞ認証方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 IPv6の割付	特開2004-289257 03.03.19 H04L12/66	**ﾈｯﾄﾜｰｸ認証装置及びﾈｯﾄﾜｰｸ認証ｼｽﾃﾑ**
	攻撃パターンの高精度化	情報の照合､検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 識別子情報の照合	特開平11-212933 (みなし取下) 98.01.30 G06F15/16,430	**分散協調型ｼｽﾃﾑにおける協調ﾌﾟﾛﾄｺﾙ管理及び協調処理実行ｼｽﾃﾑ**

表2.2.4 日立製作所の技術要素別課題対応特許(16/17)

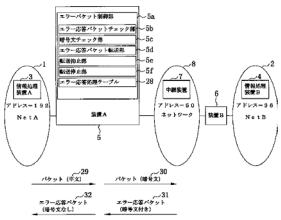
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ホスト認証技術	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2003-178025 01.12.11 G06F15/00,330	**ﾕｰｻﾞ認証方法及びﾕｰｻﾞ認証装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-272669 03.03.10 G06F17/60,132	**ｸﾞﾘｯﾄﾞｺﾝﾋﾟｭｰﾃｨﾝｸﾞにおける課金管理方法及び課金管理装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2001-282619 00.03.30 G06F12/14,310	**ｺﾝﾃﾝﾂ改竄検知方法及びその実施装置並びにその処理ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**
トンネリング技術	デバイスの正当性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 障害情報の通知	特開2005-065004 03.08.18 H04L9/08	**暗号化通信ﾃﾞｰﾀ検査方法、暗号化通信ﾃﾞｰﾀ検査装置及び暗号化通信ﾃﾞｰﾀ検査ﾌﾟﾛｸﾞﾗﾑ**
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開2001-331380 00.05.23 G06F12/16,310	**計算機ｼｽﾃﾑおよびﾃﾞｰﾀ復号化方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ﾊﾟﾀｰﾝの廃棄	特許3632167 98.01.30 H04L12/66 〔被引用回数 1〕	**暗号通信装置**  第1のﾈｯﾄﾜｰｸと第2のﾈｯﾄﾜｰｸとの間でﾊﾟｹｯﾄﾃﾞｰﾀを暗号化して通信するﾈｯﾄﾜｰｸｼｽﾃﾑにおける暗号通信装置であって、前記第1のﾈｯﾄﾜｰｸから前記第2のﾈｯﾄﾜｰｸ宛に送信されたﾊﾟｹｯﾄﾃﾞｰﾀを受信し暗号化して前記第2のﾈｯﾄﾜｰｸ宛に送信する手段と、前記第1のﾈｯﾄﾜｰｸ宛に前記ﾈｯﾄﾜｰｸｼｽﾃﾑ内の他のﾈｯﾄﾜｰｸから送信されたﾊﾟｹｯﾄﾃﾞｰﾀの受信に応じて前記暗号化したﾊﾟｹｯﾄﾃﾞｰﾀに対するｴﾗｰ応答ﾊﾟｹｯﾄを検出する手段と、前記検出したｴﾗｰ応答ﾊﾟｹｯﾄの情報部の暗号化部分を削除して前記第1のﾈｯﾄﾜｰｸに送信する手段とを有することを特徴とする暗号通信装置。
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開2000-232480 99.02.10 H04L12/56	**ﾊﾟｹｯﾄﾍｯﾀﾞ変換装置および通信ﾉｰﾄﾞ装置**
	中継するデータの機密性向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開2004-056325 02.07.18 H04L12/66	**ﾎｰﾑｹﾞｰﾄｳｴｲおよびﾎｰﾑﾈｯﾄﾜｰｸの通信方法**
		各種の処理手順改良 特定情報の記憶、登録手順 設定情報の記憶	特開2004-221922 03.01.15 H04L12/66	**ﾈｯﾄﾜｰｸ管理装置**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 障害情報の通知	特開2005-020215 03.06.25 H04L9/36	**ｾｷｭｱ通信における障害復旧方法及びｼｽﾃﾑ**

表2.2.4 日立製作所の技術要素別課題対応特許(17/17)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
トンネリング技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開平10-111855 96.10.04 G06F15/00,330	**通信ﾃﾞｰﾀ監査方法および装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2001-337918 00.05.26 G06F15/00,330	**情報管理ｼｽﾃﾑおよび情報通信ｼｽﾃﾑ**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 URLﾄﾞﾒｲﾝの変換	特開2000-349747 99.06.02 H04L9/08	**公開鍵管理方法**
		回路の改良 処理回路の改良 同一ﾁｯﾌﾟ内のﾊﾞｽ回路	WO00-057290 (却下) 99.03.19 G06F15/00,330	**情報処理装置**
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2001-203687 00.01.18 H04L9/32	**ﾃﾞｰﾀ伝送方法**

2.3 日本電気

2.3.1 企業の概要

商号	日本電気　株式会社
本社所在地	〒108-8001　東京都港区芝5-7-1
設立年	1899年（明治32年）
資本金	3,378億円（2005年9月末）
従業員数	23,552名（2005年9月末）（連結：148,540名）
事業内容	システムインテグレーションサービス・インターネットサービスの提供、情報・通信システム・機器および電子デバイス等の設計・製造・販売、他

効率的な情報セキュリティの連携で、経営資産を守り抜くことが必要であるとして、これからの情報セキュリティ対策は、見えにくいリスクをしっかりと把握し、情報セキュリティ連携による見える管理が不可欠であると、NECセキュリティソーリューションのホームページを開設して、セキュリティ情報等の紹介をしている。

（出典：http://www.sw.nec.co.jp/security/）

2.3.2 製品例

製品＆サービスのホームページにセキュリティ製品が紹介されており、表2.3.2に、製品例とその概要を示す。

表2.3.2 日本電気の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
CX5000/Firewall Pack	CX5000にCheck Point社製のVPN-1/FireWall-1をバンドルしたファイアウォールパック製品。短期間でファイアウォールを構築することが可能。
WebSAM RealSecure	① 統合システム運用管理(WebSAM)のミドルウエアに、不正アクセス侵入検知ソフトであるRealSecureの Sensor(Network,Server)やDesktop Protectorをバンドルする。 ② WebSAMに、脆弱性診断ソフトであるRealSecureのScannerをバンドルする。
Symantec Host IDS	ホストベースの侵入検知システム。ホストコンピュータ上で、ログやファイル、プロセス等を常時監視し、セキュリティ違反をリアルタイムで検出して、ポリシーに基づく対応を自動的に実行。

（出典：http://www.sw.nec.co.jp/products/soft/security.html）

2.3.3 技術開発拠点と研究者

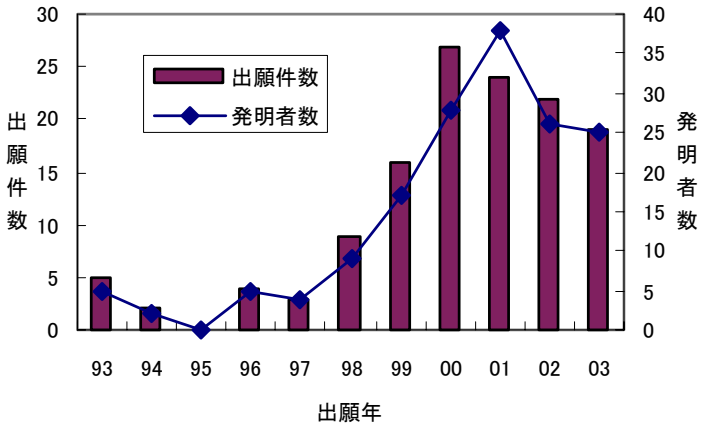
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都港区芝5丁目7番1号 日本電気株式会社内

図2.3.3に、日本電気の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。2000年以降の出願件数は、20件前後で、発明者も30人前後で安定している。

図2.3.3 日本電気の不正アクセス侵入検知防御技術に関する出願件数と発明者数



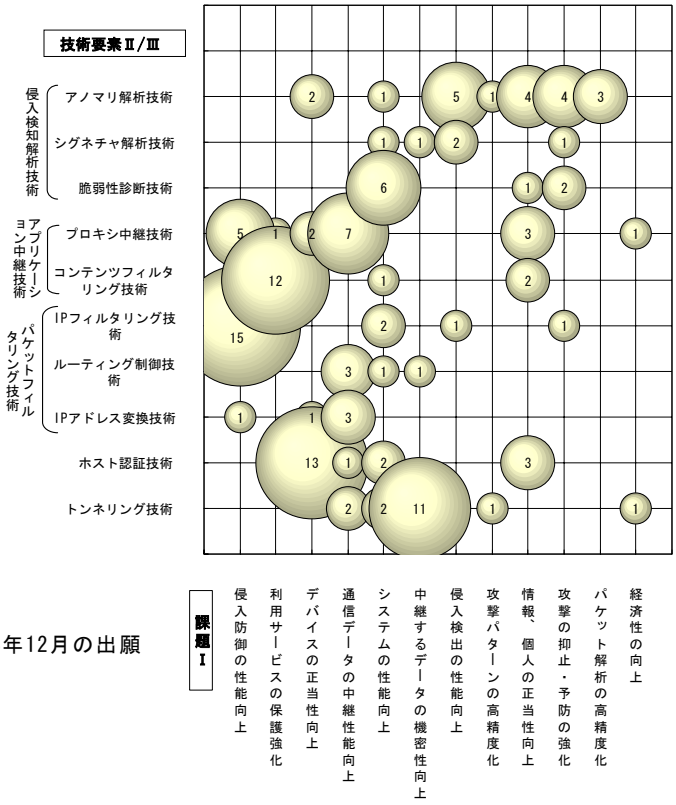
2.3.4 技術開発課題対応特許の概要

図2.3.4-1に、日本電気の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.3.4-2に、日本電気の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術が最も多く出願され、次いでIPフィルタリング技術とホスト認証技術に関する出願が多い。これらの出願のうち、最も多い課題は、「侵入防御の性能向上」であり、次いで多い課題は「デバイスの正当性向上」である。

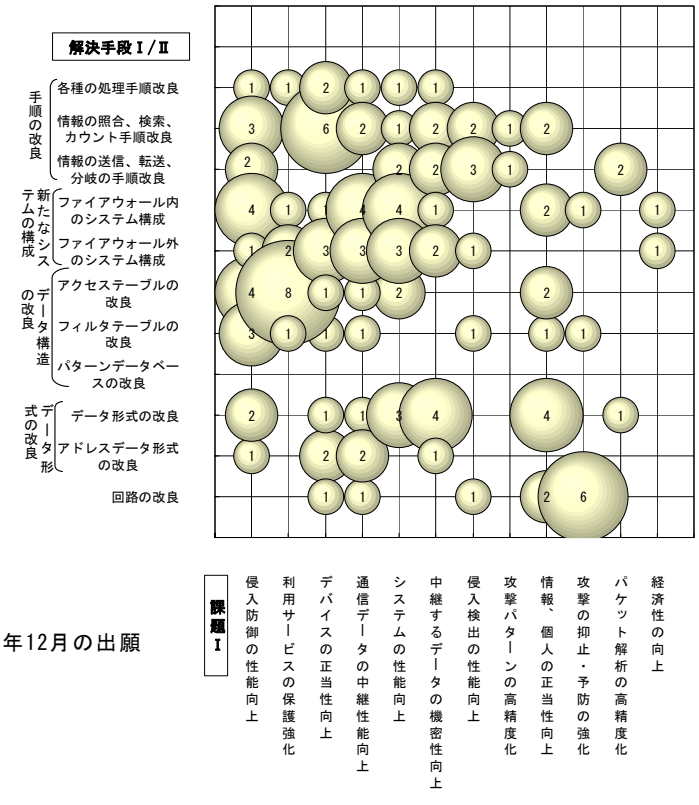
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。次いで「デバイスの正当性向上」の課題に対しては、「情報の照合、検索、カウント手順改良」で多く対応し、さらに「攻撃の抑止・予防の強化」の課題に対しては、「回路の改良」で多く対応している。

図2.3.4-1 日本電気の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.3.4-2 日本電気の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.3.4 日本電気の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は133件で、そのうち33件が登録特許である。なお、表2.3.4では図2.3.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.3.4 日本電気の技術要素別課題対応特許（1/18）

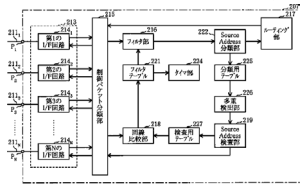
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
アノマリ解析技術	デバイスの正当性向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特許3584877 00.12.05 H04L12/66	**ﾊﾟｹｯﾄ転送制御装置、ﾊﾟｹｯﾄ転送制御方法およびﾊﾟｹｯﾄ転送制御ｼｽﾃﾑ**  ﾈｯﾄﾜｰｸを介して送られてきたﾊﾟｹｯﾄを受信する複数のﾎﾟｰﾄと、これらのﾎﾟｰﾄの幾つかに同一の送信元を示すﾊﾟｹｯﾄが時間的に並列して入力されたことを条件として不正ｱｸｾｽを検出する不正ｱｸｾｽ検出手段と、この不正ｱｸｾｽ検出手段が不正ｱｸｾｽを検出したときこれらのﾊﾟｹｯﾄの送信元を宛先としてﾊﾟｹｯﾄの返信を要求するための送信元検査用ﾊﾟｹｯﾄを送出する送信元検査用ﾊﾟｹｯﾄ送出手段と、この送信元検査用ﾊﾟｹｯﾄ送出手段によって送出された送信元検査用ﾊﾟｹｯﾄについての応答ﾊﾟｹｯﾄが送り返されてきたとき、この応答ﾊﾟｹｯﾄの送り返されてきたﾎﾟｰﾄ以外であって前記同一の送信元のﾊﾟｹｯﾄが入力されたﾎﾟｰﾄから前記同一の送信元のﾊﾟｹｯﾄが受信されたときその転送を禁止する特定ﾊﾟｹｯﾄ転送禁止手段とを具備することを特徴とするﾊﾟｹｯﾄ転送制御装置。
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2004-348456 03.05.22 G06F15/00,330	**認証記録確認ｼｽﾃﾑ**
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2004-254088 03.02.20 H04L12/26 NECｿﾌﾄ	**ﾌﾟﾛｾｽ監視ｼｽﾃﾑ、及び、ﾌﾟﾛｾｽ監視方法**
	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2003-006185 01.06.20 G06F17/21,570	**ｱｸｾｽ管理ｼｽﾃﾑおよびﾌﾞﾗｳｻﾞのﾌﾟﾛｸﾞﾗﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｱｸｾｽ、ｾｯｼｮﾝ回数	特開2004-266483 03.02.28 H04L12/66	**不正ｱｸｾｽ防止方法、装置、ﾌﾟﾛｸﾞﾗﾑ**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 容疑ﾚﾍﾞﾙ、悪性閾値	特開2003-337797 02.05.17 G06F15/00,330	**Webｻｲﾄ安全度認証ｼｽﾃﾑ、方法及びﾌﾟﾛｸﾞﾗﾑ**
			特開2004-078602 （みなし取下） 02.08.19 G06F13/00,351	**ﾃﾞｰﾀ処理装置**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特開2002-207694 01.01.05 G06F15/00,310	**情報転送追跡装置、個人情報管理ｼｽﾃﾑ、その方法及びﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**

表2.3.4 日本電気の技術要素別課題対応特許（2/18）

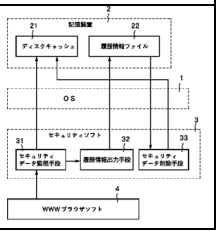
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2004-126874 02.10.01 G06F15/00,330	公開ｻｰﾊﾞのｾｷｭﾘﾃｨﾚﾍﾞﾙ診断方法、診断ﾌﾟﾛｸﾞﾗﾑ、診断装置および診断ｼｽﾃﾑ
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開2002-176455 （拒絶確定） 00.12.06 H04L12/66	ｾｷｭﾘﾃｨｼｽﾃﾑ及びそれに用いる音声ﾃﾞｰﾀｾｷｭﾘﾃｨ方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾊﾞｯｸｱｯﾌﾟｻｰﾊﾞｰの配置	特開2004-185182 02.12.02 G06F15/00,330	遠隔管理ｼｽﾃﾑ、ｻｰﾊﾞ及びﾌﾟﾛｸﾞﾗﾑ
			特開2003-196141 01.12.26 G06F12/00,537 NECｿﾌﾄ	ｲﾝﾀｰﾈｯﾄ上に公開するｺﾝﾃﾝﾂの登録ｼｽﾃﾑ、登録方法、及びﾌﾟﾛｸﾞﾗﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2002-024147 （拒絶確定） 00.07.05 G06F13/00,610 〔被引用回数 1〕	ｾｷｭｱﾒｰﾙﾌﾟﾛｷｼｼｽﾃﾑ及び方法並びに記録媒体
	攻撃の抑止・予防の強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2003-162423 01.11.27 G06F11/00	通信ｼｽﾃﾑ用のｳｲﾙｽ除去方法とそのﾌﾟﾛｸﾞﾗﾑ及びこれらを用いた通信ｼｽﾃﾑ、ｻｰﾊﾞ
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2000-066977 （拒絶確定） 98.08.20 G06F13/00,351	ｻｰﾋﾞｽ交換方法及びその装置
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2000-010887 （拒絶確定） 98.06.19 G06F13/00,353 〔被引用回数 3〕	ｾｷｭﾘﾃｨｽｲｯﾁ付きﾈｯﾄﾜｰｸｲﾝﾀﾌｪｰｽﾓｼﾞｭｰﾙ
			特開2005-012606 03.06.20 H04L12/26	ﾈｯﾄﾜｰｸ遮断ｼｽﾃﾑ及びﾈｯﾄﾜｰｸ遮断判定装置並びにﾌﾟﾛｸﾞﾗﾑ
	パケット解析の高精度化	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特開2000-250844 （拒絶確定） 99.03.03 G06F13/00,355	遠隔監視方式
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特許3225919 98.05.07 G06F13/00,540	ｾｷｭﾘﾃｨｼｽﾃﾑ WWWﾌﾞﾗｳｻﾞｿﾌﾄを使用するﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀにおいて、前記WWWﾌﾞﾗｳｻﾞｿﾌﾄによりWWWを閲覧しているときに前記ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀの記憶装置に書き込まれたｾｷｭﾘﾃｨ対象のﾃﾞｰﾀを、前記記憶装置から削除することを特徴とするｾｷｭﾘﾃｨｼｽﾃﾑ。 

表2.3.4 日本電気の技術要素別課題対応特許（3/18）

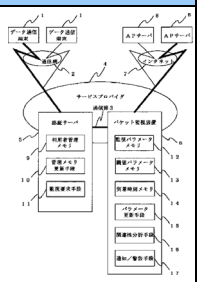
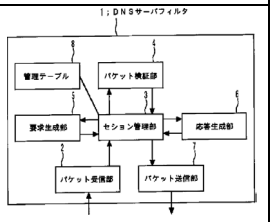
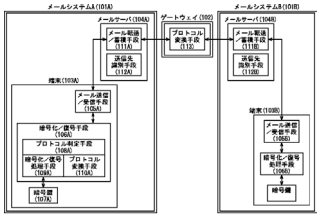
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	パケット解析の高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾀｲﾑｽﾀﾝﾌﾟの付加	特許3584838 00.02.22 H04L12/14	**ﾊﾟｹｯﾄ監視ｼｽﾃﾑ、ﾊﾟｹｯﾄ監視方法及びそのﾌﾟﾛｸﾞﾗﾑを記録した記録媒体**  ｱﾌﾟﾘｹｰｼｮﾝｻｰﾊﾞと該ｱﾌﾟﾘｹｰｼｮﾝｻｰﾊﾞを利用するｻｰﾋﾞｽ利用者とを接続する通信路上で送受信されるﾊﾟｹｯﾄを監視するﾊﾟｹｯﾄ監視ｼｽﾃﾑであって、前記ｻｰﾋﾞｽ利用者を認証する認証ｻｰﾊﾞ装置と、該認証ｻｰﾊﾞ装置からの依頼により、前記通信路上で送受信されるﾊﾟｹｯﾄを監視するﾊﾟｹｯﾄ監視装置と、を有することを特徴とするﾊﾟｹｯﾄ監視ｼｽﾃﾑ。
シグネチャ解析技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2005-159974 03.11.28 H04L12/66	**接続環境自動判別ｾｷｭﾘﾃｨｼｽﾃﾑ，ｾｷｭﾘﾃｨ方法およびｾｷｭﾘﾃｨﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開2004-304752 02.08.20 H04L12/66	**攻撃防御ｼｽﾃﾑおよび攻撃防御方法**
	侵入検出の性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 障害情報の通知	特開2002-141902 （拒絶確定） 00.11.06 H04L12/22	**ｲﾝﾀｰﾈｯﾄﾓﾆﾀﾘﾝｸﾞ方法**
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2002-158660 （拒絶確定） 00.11.22 H04L12/22 〔被引用回数 4〕	**不正ｱｸｾｽ防御ｼｽﾃﾑ**
	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特許3596400 00.01.21 H04L12/66	**DNSｻｰﾊﾞﾌｨﾙﾀ**  受信したDNS(Domain Name System)ﾊﾟｹｯﾄについて、該ﾊﾟｹｯﾄをDNSｻｰﾊﾞに渡すまえに、該ﾊﾟｹｯﾄの内容に異常があるか否か検査するﾊﾟｹｯﾄ検証手段を備え、異常を検出した際にｴﾗｰ応答ﾊﾟｹｯﾄを生成して要求元に返す、ことを特徴とするDNSｻｰﾊﾞﾌｨﾙﾀ装置。
脆弱性診断技術	システムの性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特許3555857 00.03.14 H04L12/58,100 NECｼｽﾃﾑﾃｸﾉﾛｼﾞｰ	**暗号ﾒｰﾙ送受信ｼｽﾃﾑ**  相互に異なった通信ﾌﾟﾛﾄｺﾙの下に制御される第1電子ﾒｰﾙｼｽﾃﾑおよび第2電子ﾒｰﾙｼｽﾃﾑと、該第1，第2電子ﾒｰﾙｼｽﾃﾑの間で送受するﾒｰﾙを、相手先の通信ﾌﾟﾛﾄｺﾙに変換するｹﾞｰﾄｳｪｲ装置とを有してなり、前記第1，第2電子ﾒｰﾙｼｽﾃﾑの夫々は、ﾒｰﾙを相手先に送信するﾒｰﾙ送信手段および前記ｹﾞｰﾄｳｪｲにより自己の通信ﾌﾟﾛﾄｺﾙに変換後のﾒｰﾙを受信するﾒｰﾙ受信手段とを夫々有してなる端末装置とを備えた電子ﾒｰﾙ送受信ｼｽﾃﾑにおいて、前記端末装置は、送信するﾒｰﾙを送信先通信ﾌﾟﾛﾄｺﾙに変換後、暗号鍵により暗号化する暗号化手段と、受信した暗号化ﾒｰﾙを自己の通信ﾌﾟﾛﾄｺﾙに変換して復号する復号化手段とを備えたことを特徴とする暗号ﾒｰﾙ送受信ｼｽﾃﾑ。

表2.3.4 日本電気の技術要素別課題対応特許（4/18）

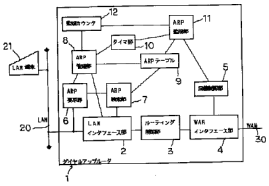
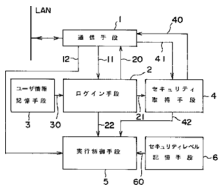
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
脆弱性診断技術	システムの性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾊﾟｹｯﾄ	特許3592249 01.03.15 H04L12/46 NECｱｸｾｽﾃｸﾆｶ	**ﾀﾞｲﾔﾙｱｯﾌﾟﾙｰﾀ及び回線接続抑制方法**  LANを構成する端末のうち、通信中の端末のMACｱﾄﾞﾚｽ及びIPｱﾄﾞﾚｽが一時的に登録されるARPﾃｰﾌﾞﾙと、MACｱﾄﾞﾚｽ及びIPｱﾄﾞﾚｽをARPﾃｰﾌﾞﾙに登録し、登録された該MACｱﾄﾞﾚｽ及びIPｱﾄﾞﾚｽを所定の登録時間経過後にARPﾃｰﾌﾞﾙから削除するARP管理部と、登録時間よりも短い周期から成る監視時間毎にその値が更新される監視ｶｳﾝﾀと、監視時間毎にARPﾃｰﾌﾞﾙの内容を監視し、ARPﾃｰﾌﾞﾙにMACｱﾄﾞﾚｽ及びIPｱﾄﾞﾚｽが1件も登録されていない場合は監視ｶｳﾝﾀの値をｶｳﾝﾄｱｯﾌﾟし、ARPﾃｰﾌﾞﾙに前記MACｱﾄﾞﾚｽ及びIPｱﾄﾞﾚｽが登録されている場合は監視ｶｳﾝﾀの値を零にｸﾘｱし、監視ｶｳﾝﾀの値が予め設定されたしきい値を超えた場合はWANに繋がる回線との接続を禁止するための回線接続禁止通知を出力するARP監視部と、ARP監視部から回線接続禁止通知を受け取った場合に、回線との接続要求があっても回線との接続を停止し、回線と既に接続されている場合は接続を切断する回線制御部と、を有するﾀﾞｲﾔﾙｱｯﾌﾟﾙｰﾀ
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 ｱｸｾｽ許可情報	特開2004-094850 02.09.04 G06F12/00,537	**排他制御装置および排他制御方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾊﾞｯｸｱｯﾌﾟｻｰﾊﾞｰの配置	特開2002-259233 01.03.05 G06F13/00,351	**ｺﾝﾃﾝﾂ提供ｼｽﾃﾑおよびｺﾝﾃﾝﾂ提供ﾌﾟﾛｸﾞﾗﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 通信路	特許2105027 93.05.28 G06F15/00,330	**ﾛｸﾞｲﾝ方式**  ﾛｸﾞｲﾝ先に設けられ、ﾛｸﾞｲﾝ要求元に付与されたﾛｸﾞｲﾝ名とそのﾊﾟｽﾜｰﾄﾞおよびﾛｸﾞｲﾝ名に対応するｾｷｭﾘﾃｨﾚﾍﾞﾙを記憶するﾕｰｻﾞ情報記憶手段、ﾛｸﾞｲﾝ先に設けられ、ﾛｸﾞｲﾝ要求元から送られてきたﾛｸﾞｲﾝ要求に付属するﾛｸﾞｲﾝ名とそのﾊﾟｽﾜｰﾄﾞとをﾕｰｻﾞ情報記憶手段に照合してﾛｸﾞｲﾝの許可を判定し、ﾛｸﾞｲﾝを許可すると判定したときはﾛｸﾞｲﾝを許可する信号を出力するﾛｸﾞｲﾝ手段、このﾛｸﾞｲﾝ手段の出力するﾛｸﾞｲﾝを許可する信号に応じて、通信路ｾｷｭﾘﾃｨﾚﾍﾞﾙを問い合わす問い合わせ信号をﾛｸﾞｲﾝ要求元に当て出力するようﾛｸﾞｲﾝ先に設けられるｾｷｭﾘﾃｨ取得手段、このｾｷｭﾘﾃｨ取得手段からの問い合わせ信号と上記ﾛｸﾞｲﾝ手段からのﾛｸﾞｲﾝを許可する信号とをﾛｸﾞｲﾝ要求元宛送信する通信手段、この通信手段から送信された問い合わせ信号に対する回答からｾｷｭﾘﾃｨ取得手段において通信路のｾｷｭﾘﾃｨﾚﾍﾞﾙを決定する通信路ｾｷｭﾘﾃｨﾚﾍﾞﾙ決定手段、ﾛｸﾞｲﾝ先に設けられ、ｺﾏﾝﾄﾞの実行のために要求されるｾｷｭﾘﾃｨﾚﾍﾞﾙを記憶するｾｷｭﾘﾃｨﾚﾍﾞﾙ記憶手段、ﾛｸﾞｲﾝ要求元から通信手段を介して入力されるｺﾏﾝﾄﾞに対応するｾｷｭﾘﾃｨﾚﾍﾞﾙをｾｷｭﾘﾃｨﾚﾍﾞﾙ記憶手段から読み出し、この読み出したｾｷｭﾘﾃｨﾚﾍﾞﾙと通信路ｾｷｭﾘﾃｨﾚﾍﾞﾙ決定手段で決定された通信路のｾｷｭﾘﾃｨﾚﾍﾞﾙおよびﾛｸﾞｲﾝ名に対応してﾕｰｻﾞ情報記憶手段から読み出されたｾｷｭﾘﾃｨﾚﾍﾞﾙとを対照してｺﾏﾝﾄﾞ実行の可否を決定する実行制御手段、を備えたことを特徴とするﾛｸﾞｲﾝ方式。

表2.3.4 日本電気の技術要素別課題対応特許（5/18）

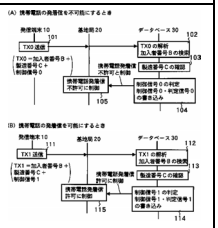
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
脆弱性診断技術	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-192351 02.12.11 G06F15/00,310	**既存ｼｽﾃﾑへの機能追加方法および機器設定方法ならびに情報機器**
	情報、個人の正当性向上	回路の改良 ｽｲｯﾁ回路の追加 ﾛｯｸ回路の追加	特許3478240 00.05.15 H04Q7/38	**無線通信ｼｽﾃﾑ及び携帯端末**  加入者番号及び加入者番号に対応した固有番号と共に、加入者番号に該当する所定の携帯端末の発着信制御信号とをそれぞれ無線送信する発信端末と、発信端末から送信された加入者番号、固有番号及び発着信制御信号を受信し、外部から入力された判定信号に基づいて指示された加入者番号の携帯端末の発着信を制御する基地局と、基地局により受信された加入者番号、固有番号及び発着信制御信号を基地局から入力として受け、入力された加入者番号及び固有番号を予め記憶している加入者番号及び固有番号と照合して認証する認証手段と、該認証手段により存在が認証されたときに、入力された発着信制御信号の値に基づいて判定した発着信許可又は発着信不許可を示す値の判定信号を加入者番号と共に前記基地局に通知する判定手段とを備えたﾃﾞｰﾀﾍﾞｰｽとを有し、基地局は発着信不許可を示す値の判定信号がﾃﾞｰﾀﾍﾞｰｽから入力されたときには、入力された加入者番号の携帯端末への発着信を不可能に動作することを特徴とする無線通信ｼｽﾃﾑ。
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2002-077272 （拒絶確定） 00.08.28 H04L12/66	**情報公開ｻｰﾊﾞのﾒﾝﾃﾅﾝｽｼｽﾃﾑとそのﾒﾝﾃﾅﾝｽ方法**
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2002-175224 （拒絶確定） 00.12.06 G06F13/00,351 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ接続ｼｽﾃﾑ、及び装置**
プロキシ中継技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開2004-207783 02.12.20 H04L12/46	**ﾈｯﾄﾜｰｸｼｽﾃﾑ、ｱｸｾｽ制限方法、及びｱｸｾｽ制限ﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2002-082907 00.09.11 G06F15/00,330	**ﾃﾞｰﾀ通信におけるｾｷｭﾘﾃｨ機能代理方法、ｾｷｭﾘﾃｨ機能代理ｼｽﾃﾑ、及び、記録媒体**
			特開2004-295166 03.03.25 G06F13/00,351	**ﾘﾓｰﾄｱｸｾｽｼｽﾃﾑおよびﾘﾓｰﾄｱｸｾｽ方法**

表2.3.4 日本電気の技術要素別課題対応特許（6/18）

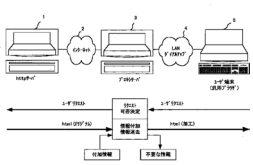
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
プロキシ中継技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの削除	特許3250512 98.02.24 G06F13/00,540 〔被引用回数 2〕	**ﾌﾟﾛｷｼｻｰﾊﾞ**  ﾕｰｻﾞからのﾘｸｴｽﾄを受信するﾘｸｴｽﾄ受信部と、ｱｸｾｽ不可ﾘｽﾄを参照してﾕｰｻﾞからのﾘｸｴｽﾄの可否を決定するﾘｸｴｽﾄ可否決定部と、ﾕｰｻﾞからのﾘｸｴｽﾄをｻｰﾊﾞへ送信するﾘｸｴｽﾄ送信部と、ﾕｰｻﾞ端末に関する情報を一時的に保存するﾕｰｻﾞ端末情報格納部と、ﾕｰｻﾞのｱｸｾｽを禁止するｱｸｾｽ不可ﾘｽﾄを格納するｱｸｾｽ不可ﾘｽﾄ格納部と、ｻｰﾊﾞから送信された情報を受信する情報受信部と、ｱｸｾｽ不可ﾘｽﾄおよびﾕｰｻﾞ端末情報を参照して受信した情報を編集する情報編集部と、編集した情報をﾕｰｻﾞ端末に送信する情報送信部と、を備えていることを特徴とするﾌﾟﾛｷｼｻｰﾊﾞ。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2002-314611 （特許3705148） 01.04.12 H04L12/58,100	**電子ﾒｰﾙ転送方法、ﾒｰﾙｻｰﾊﾞ及び電子ﾒｰﾙ転送ﾌﾟﾛｸﾞﾗﾑ**
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2000-285061 （拒絶確定） 99.03.31 G06F13/00,354 〔被引用回数 1〕	**ﾌﾟﾛｷｼｱｸｾｽ制御ｼｽﾃﾑ**
	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2003-330885 02.05.08 G06F15/00,330	**ﾃﾞｨﾚｸﾄﾘｻｰﾊﾞﾊﾟｽﾜｰﾄﾞ変更ｼｽﾃﾑ、方法、ﾌﾟﾛｸﾞﾗﾑ及びﾊﾟｽﾜｰﾄﾞ変更管理ｻｰﾊﾞ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2001-344207 （拒絶確定） 00.05.31 G06F15/00,330	**認証ｼｽﾃﾑおよび認証方法**
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2002-351757 （拒絶確定） 01.05.25 G06F13/00,351	**ﾈｯﾄﾜｰｸ透過ｼｽﾃﾑおよびﾈｯﾄﾜｰｸ透過方法**
			特開2004-229187 03.01.27 H04L12/66	**HTTPﾌﾟﾛｷｼ装置およびHTTPﾌﾟﾛｷｼｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特開2000-132475 （拒絶確定） 98.10.26 G06F13/00,351 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙｼｽﾃﾑ及びその情報取得方法ならびに情報取得処理制御ﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2003-152805 （拒絶確定） 01.11.13 H04L12/66	**公衆ｱｸｾｽｼｽﾃﾑおよび装置、ｻｰﾊﾞ**
			特開2003-122513 01.10.17 G06F3/12	**ｲﾝﾀﾈｯﾄ印刷ｼｽﾃﾑ及びｲﾝﾀﾈｯﾄ印刷方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2000-276411 （拒絶確定） 99.03.26 G06F13/00,351	**ftpにおける転送中ﾌｧｲﾙの排他制御方法**

表2.3.4 日本電気の技術要素別課題対応特許（7/18）

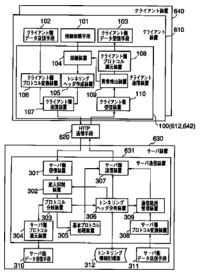
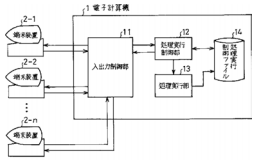
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
プロキシ中継技術	通信データの中継性能向上	回路の改良 ｽｲｯﾁ回路の追加 複数通信路の配置	特許3478200 99.09.17 H04L12/56	**ｻｰﾊﾞ・ｸﾗｲｱﾝﾄ間双方向通信ｼｽﾃﾑ**  ｻｰﾊﾞ装置と各ｸﾗｲｱﾝﾄ装置間で、ﾃﾞｰﾀの送受信が行われる以前に、ｸﾗｲｱﾝﾄ装置からｻｰﾊﾞ装置に対するﾃﾞｰﾀ送信をﾘｱﾙﾀｲﾑに行うことを可能にするための、HTTPのPOSTﾒｿｯﾄﾞを用いた上り回線と、ｻｰﾊﾞ装置からｸﾗｲｱﾝﾄ装置に対するﾃﾞｰﾀ送信をﾘｱﾙﾀｲﾑに行うことを可能にするための、HTTPのGET ﾒｿｯﾄﾞを用いた下り回線との計2回線をあらかじめ作成するようにしたことを特徴とする、ｻｰﾊﾞおよび複数のｸﾗｲｱﾝﾄ間の双方向通信ｼｽﾃﾑ。
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2004-355083 03.05.27 G06F12/14,310	**ﾊﾞｯｸｱｯﾌﾟｼｽﾃﾑおよびﾊﾞｯｸｱｯﾌﾟﾌﾟﾛｸﾞﾗﾑ**
			特開2003-051857 01.08.06 H04L12/66	**ﾃﾞｰﾀ通信ｼｽﾃﾑ、ﾃﾞｰﾀ通信端末及びそれに用いるﾃﾞｰﾀ通信方法並びにそのﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2003-338815 02.05.21 H04L9/32	**電子署名ｼｽﾃﾑおよび電子署名方法**
	経済性の向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2004-295166 03.03.25 G06F13/00,351	**ﾘﾓｰﾄｱｸｾｽｼｽﾃﾑおよびﾘﾓｰﾄｱｸｾｽ方法** 概要は技術要素「ﾌﾟﾛｷｼ中継技術」、課題「侵入防御の性能向上」の項参照
コンテンツフィルタリング技術	利用サービスの保護強化	各種の処理手順改良 各種処理の実行手順 並列処理の実行	特許2932945 94.08.12 G06F11/00,340	**不正処理実行防止方式**  2台の端末装置と、該2台の端末装置の各々から同一の処理内容が入力されることにより、前記処理内容に従った処理の実行を指示する処理実行制御部と、該処理実行制御部からの指示に応答して前記処理内容に従った処理を実行する処理実行部とを備えたことを特徴とする不正処理実行防止方式。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2004-287810 03.03.20 G06F15/00,330	**不正ｱｸｾｽ防止ｼｽﾃﾑ、不正ｱｸｾｽ防止方法、および不正ｱｸｾｽ防止ﾌﾟﾛｸﾞﾗﾑ**

表2.3.4 日本電気の技術要素別課題対応特許（8/18）

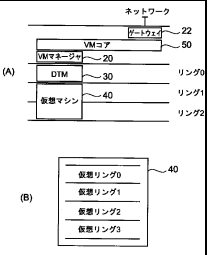
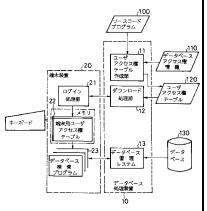
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特許3630087 00.05.10 G06F9/46,350 〔被引用回数 1〕	**自動ﾃﾞｰﾀ処理装置**  実ﾘﾝｸﾞﾌﾟﾛﾊﾟﾃｨを変更する処理が制限された最上位特権の実ﾘﾝｸﾞと、第2位特権の実ﾘﾝｸﾞと、残りの実ﾘﾝｸﾞと、からなる実環境と、最上位特権の実ﾘﾝｸﾞで動作する仮想ﾏｼﾝﾏﾈｰｼﾞｬと、残りの実ﾘﾝｸﾞおよびﾒﾓﾘの一部をからなる仮想ﾏｼﾝ環境と、第2位特権の実ﾘﾝｸﾞで動作し、仮想ﾏｼﾝ環境を出入りする情報転送を処理する第1ﾃﾞｰﾀ転送ﾏﾈｰｼﾞｬと、仮想ﾏｼﾝ環境内にある階層仮想特権ﾘﾝｸﾞと、仮想ﾏｼﾝ環境内の情報に対する特権ﾘﾝｸﾞの関連づけを含み、仮想ﾏｼﾝ環境内に形成された仮想環境ﾃﾞｨｽｸﾘﾌﾟﾀﾃｰﾌﾞﾙと、からなり、仮想ﾏｼﾝ環境内の情報は階層仮想特権ﾘﾝｸﾞに関連づけられ、ﾒﾓﾘの一部内に記憶され、自動ﾃﾞｰﾀ処理装置によって処理される情報は、同位または下位の特権の実ﾘﾝｸﾞに関連づけられたｼｽﾃﾑﾘｿｰｽおよび情報にｱｸｾｽ可能であり、仮想ﾏｼﾝ環境内の情報は、自動ﾃﾞｰﾀ処理装置によって処理される場合、同位または下位の特権の仮想特権ﾘﾝｸﾞに関連づけられたｼｽﾃﾑﾘｿｰｽおよび情報にｱｸｾｽ可能であるとともに、仮想ﾏｼﾝ環境のﾒﾓﾘの一部内のﾒﾓﾘﾛｹｰｼｮﾝにのみｱｸｾｽ可能であり、仮想特権ﾘﾝｸﾞに関連づけられた情報にとって利用可能な実特権は、自動ﾃﾞｰﾀ処理装置によって処理される場合、残りの実ﾘﾝｸﾞのうち仮想ﾏｼﾝ環境を含む実ﾘﾝｸﾞを超える実特権へのｱｸｾｽが要求されるときに仮想ﾏｼﾝﾏﾈｰｼﾞｬによって制御され、ﾒﾓﾘの一部は主ﾒﾓﾘおよび補助記憶領域を含む、ことを特徴とする自動ﾃﾞｰﾀ処理装置。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特許2843768 94.08.22 G06F12/00,537	**ﾃﾞｰﾀﾍﾞｰｽｱｸｾｽ制御方式**  ﾃﾞｰﾀﾍﾞｰｽ検索ﾌﾟﾛｸﾞﾗﾑのｿｰｽｺｰﾄﾞﾌﾟﾛｸﾞﾗﾑ中のﾃﾞｰﾀﾍﾞｰｽ操作言語による検索文とﾃﾞｰﾀﾍﾞｰｽｱｸｾｽ権情報とに基づいてﾕｰｻﾞｱｸｾｽ権ﾃｰﾌﾞﾙを作成するﾃﾞｰﾀﾍﾞｰｽ処理装置上のﾕｰｻﾞｱｸｾｽ権ﾃｰﾌﾞﾙ作成部と、端末装置でのﾛｸﾞｲﾝ時にﾃﾞｰﾀﾍﾞｰｽ処理装置からのﾀﾞｳﾝﾛｰﾄﾞﾃﾞｰﾀに基づいてﾛｸﾞｲﾝに係るﾕｰｻﾞに対応する端末用ﾕｰｻﾞｱｸｾｽ権ﾃｰﾌﾞﾙを端末装置内のﾒﾓﾘ上に生成する端末装置上のﾛｸﾞｲﾝ処理部と、ﾕｰｻﾞｱｸｾｽ権ﾃｰﾌﾞﾙ作成部により作成されたﾕｰｻﾞｱｸｾｽ権ﾃｰﾌﾞﾙに基づくﾀﾞｳﾝﾛｰﾄﾞﾃﾞｰﾀを端末装置でのﾛｸﾞｲﾝ時にﾃﾞｰﾀﾍﾞｰｽ処理装置から端末装置に送信するﾃﾞｰﾀﾍﾞｰｽ処理装置上のﾀﾞｳﾝﾛｰﾄﾞ処理部と、ﾕｰｻﾞから投入されたﾃﾞｰﾀﾍﾞｰｽ検索要求に基づいて起動され、ﾃﾞｰﾀﾍﾞｰｽ検索要求に対応するﾃﾞｰﾀﾍﾞｰｽ検索処理の実行の可否をﾕｰｻﾞから投入されたﾕｰｻﾞ識別子とﾛｸﾞｲﾝ処理部によって生成された端末用ﾕｰｻﾞｱｸｾｽ権ﾃｰﾌﾞﾙとを使用して検査し、この検査で「実行可」と判断した場合にのみﾃﾞｰﾀﾍﾞｰｽ検索処理を実行する端末装置上のﾃﾞｰﾀﾍﾞｰｽ検索ﾌﾟﾛｸﾞﾗﾑとを有することを特徴とするﾃﾞｰﾀﾍﾞｰｽｱｸｾｽ制御方式。
			特開平09-319448 （拒絶確定） 96.05.28 G06F1/00,370	**制御ｼｽﾃﾑ**
			特開2004-046460 02.07.10 G06F15/00,330	**ﾌｧｲﾙ管理ｼｽﾃﾑにおけるｱｸｾｽ制御方式**
			特開2002-328890 01.04.27 G06F15/00,310 住友林業，住友林業情報ｼｽﾃﾑ	**ｳｪﾌﾞｺﾝﾋﾟｭｰﾃｨﾝｸﾞｼｽﾃﾑ**

表2.3.4 日本電気の技術要素別課題対応特許（9/18）

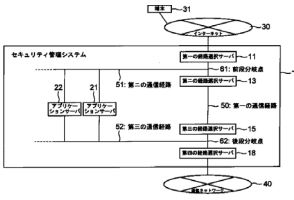
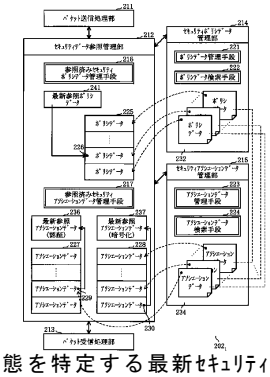
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2004-118433 02.09.25 G06F1/00	**外部ﾌﾟﾛｸﾞﾗﾑの動作制御方法、動作制御ﾌﾟﾛｸﾞﾗﾑ、動作制御装置、及び、動作制御ﾌﾟﾛｸﾞﾗﾑ提供装置**
			特開2003-186747 01.12.14 G06F12/14,310 NECｼｽﾃﾑﾃｸﾉﾛｼﾞｰ	**ｱｸｾｽ権管理ｼｽﾃﾑ、その管理方法及びそのﾌﾟﾛｸﾞﾗﾑ**
			特開2004-054846 02.07.24 G06F1/00 NECｼｽﾃﾑﾃｸﾉﾛｼﾞｰ	**ﾗｲｾﾝｽ管理ｼｽﾃﾑおよびﾗｲｾﾝｽ管理方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 通信路	特許3649180 01.12.06 H04L12/66	**ｾｷｭﾘﾃｨ管理ｼｽﾃﾑおよび経路指定ﾌﾟﾛｸﾞﾗﾑ** 通信ﾈｯﾄﾜｰｸからのﾃﾞｰﾀを通過させる複数の経路と、複数の経路上に配置され、通信ﾈｯﾄﾜｰｸからのﾃﾞｰﾀに対してｾｷｭﾘﾃｨの確認を行ってﾃﾞｰﾀを中継するｾｷｭﾘﾃｨ手段と、通信ﾈｯﾄﾜｰｸからのﾃﾞｰﾀを通過させる経路を定める経路設定手段とを備えたことを特徴とするｾｷｭﾘﾃｨ管理ｼｽﾃﾑ。 
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの追加、学習	特許3637857 00.09.08 H04L9/14	**ｾｷｭﾘﾃｨ処理形態検索管理装置**  通信ﾈｯﾄﾜｰｸに送出するそれぞれのﾊﾟｹｯﾄについてｾｷｭﾘﾃｨ処理の適用の有無等の採用しうるｾｷｭﾘﾃｨ処理の形態としての各種のｾｷｭﾘﾃｨ処理形態を格納したｾｷｭﾘﾃｨ処理形態ﾃﾞｰﾀﾍﾞｰｽと、このｾｷｭﾘﾃｨ処理形態ﾃﾞｰﾀﾍﾞｰｽの中から最近利用したｾｷｭﾘﾃｨ処理形態を抜き出して格納したｾｷｭﾘﾃｨ処理形態一時記憶手段と、このｾｷｭﾘﾃｨ処理形態一時記憶手段に格納した各種のｾｷｭﾘﾃｨ処理形態の中で直前に利用したｾｷｭﾘﾃｨ処理形態を特定する最新ｾｷｭﾘﾃｨ処理形態特定手段と、送信するﾊﾟｹｯﾄに対するｾｷｭﾘﾃｨ処理形態がまず最新ｾｷｭﾘﾃｨ処理形態特定手段で特定されたｾｷｭﾘﾃｨ処理形態と一致するかどうかを判別する第1段階ｾｷｭﾘﾃｨ処理形態検索手段と、この第1段階ｾｷｭﾘﾃｨ処理形態検索手段による検索ではｾｷｭﾘﾃｨ処理形態が一致しなかったとき前記ｾｷｭﾘﾃｨ処理形態一時記憶手段に格納された残りのセキュリティ処理形態を検索する第２段階セキュリティ処理形態検索手段と、この第２段階セキュリティ処理形態検索手段による検索ではセキュリティ処理形態が一致しなかったとき前記セキュリティ処理形態データベースを検索する第３段階セキュリティ処理形態検索手段とを具備することを特徴とするセキュリティ処理形態検索管理装置。

表2.3.4 日本電気の技術要素別課題対応特許（10/18）

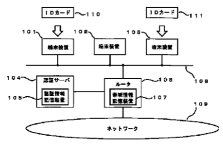
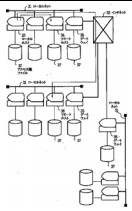
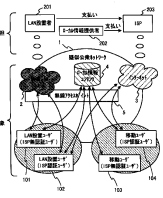
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	システムの性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特許3620452 01.02.13 H04L12/56,200	**通信帯域制御方式**  暗号化され使用者に固有の使用者識別情報を記憶した携帯可能な使用者識別情報記憶手段と、ﾃﾞｰﾀ通信に先立って、使用者識別情報記憶手段に記憶された使用者識別情報を送信する複数の端末装置と、各端末装置から受信した使用者識別情報を解読して、正規の使用者識別情報か否かを判別すると共に使用者名を判別する認証手段と、使用者名と割当て通信帯域とを対応付けした複数の通信帯域情報を記憶した通信帯域情報記憶手段と、認証手段で判別された使用者名および通信帯域情報に基づいて、端末装置に通信帯域を割り当てる通信帯域制御手段とを備え、通信帯域制御手段は、認証手段が正規の使用者識別情報であると判別すると共に端末装置の使用者名を判別したことを受けて、認証手段で判別された使用者名および通信帯域情報に基づいて使用者名に対する通信帯域を選定し、通信帯域を前記端末装置に割り当てることを特徴とする通信帯域制御方式。
	情報、個人の正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特許2082076 93.05.21 G06F13/00,351	**ﾈｯﾄﾜｰｸ･ｾｷｭﾘﾃｨ管理方法**  利用者がﾛｰｶﾙﾎｽﾄのｱｸｾｽ権を有しているか否かの確認を行うﾛｸﾞｲﾝｽﾃｯﾌﾟと、ﾛｸﾞｲﾝｽﾃｯﾌﾟによる確認により利用者がﾛｰｶﾙﾎｽﾄのｱｸｾｽ権を有する場合はｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸｼｽﾃﾑのﾛｰｶﾙﾈｯﾄならびにｲﾝﾀﾈｯﾄを使用する権限を有しているか否かの確認を行うﾘﾓｰﾄｱｸｾｽ確認ｽﾃｯﾌﾟと、ﾘﾓｰﾄｱｸｾｽ確認ｽﾃｯﾌﾟによる確認により利用者が前記ﾈｯﾄﾜｰｸのｱｸｾｽ権を有する場合はﾘﾓｰﾄﾎｽﾄのｱｸｾｽ権を有しているか否かの確認を行うﾘﾓｰﾄﾛｸﾞｲﾝｽﾃｯﾌﾟとを備えることを特徴とするﾈｯﾄﾜｰｸ･ｾｷｭﾘﾃｨ管理方法。
			特許3601434 00.10.13 H04L12/46	**擬似公衆無線ｱｸｾｽｻｰﾋﾞｽ**  ISPが、自営LAN設置者とｲﾝﾀｰﾈｯﾄ接続契約を締結してｲﾝﾀｰﾈｯﾄ接続ｻｰﾋﾞｽを行うとともに、自営LAN内に無線ｱｸｾｽﾎﾟｲﾝﾄを設置し、自営LAN設置ﾕｰｻﾞ以外の無線ｱｸｾｽﾕｰｻﾞに対しても前記無線ｱｸｾｽﾎﾟｲﾝﾄを介してｲﾝﾀｰﾈｯﾄへ接続するｻｰﾋﾞｽを提供することを特徴とする擬似公衆無線ｱｸｾｽｻｰﾋﾞｽ方法。
ＩＰフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 各種処理の実行手順 並列処理の実行	特開2000-293493 （拒絶確定） 99.04.02 G06F15/00,330	**ｾｷｭﾘﾃｨﾁｪｯｸの分散処理方法及びその装置並びに情報記録媒体**
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開平11-346214 （拒絶確定） 98.06.02 H04L12/22	**同報配信ｼｽﾃﾑ**
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路､中継ｻｰﾊﾞｰ	特開2005-196728 03.12.11 G06F15/00,330	**ｾｷｭﾘﾃｨ検証ｼｽﾃﾑ､装置､方法､およびｾｷｭﾘﾃｨ検証用ﾌﾟﾛｸﾞﾗﾑ**

表2.3.4 日本電気の技術要素別課題対応特許（11/18）

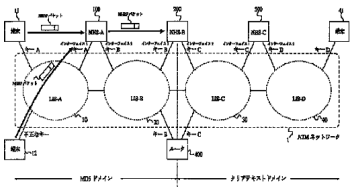
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2004-348292 03.05.20 G06F13/00,351	ｻｲﾊﾞｰｾｷｭﾘﾃｲｼｽﾃﾑ、ｻｲﾊﾞｰｾｷｭﾘﾃｲ提供方法及び制御ﾌﾟﾛｸﾞﾗﾑ
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特開2000-156711 （拒絶確定） 98.11.18 H04L12/66 〔被引用回数 3〕	ﾌｧｲｱｰｳｫｰﾙとその方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特開2000-261487 （拒絶確定） 99.03.10 H04L12/46	ﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ装置およびﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2005-107663 03.09.29 G06F15/00,310	接続支援ｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ・ｸﾞﾙｰﾌﾟ	特開2000-232476 （拒絶確定） 99.02.09 H04L12/56	ｹﾞｰﾄｳｴｲ装置
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開平09-293052 （拒絶確定） 96.04.26 G06F15/00,330 〔被引用回数 2〕	複数ﾈｯﾄﾜｰｸ間の権限管理方法およびｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開平11-025045 （拒絶確定） 97.06.30 G06F15/00,330	ｱｸｾｽ制御方法とその装置及び属性証明書発行装置並びに機械読み取り可能な記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2004-342072 03.04.24 G06F15/00,330	ｾｷｭﾘﾃｲ管理支援ｼｽﾃﾑ、ｾｷｭﾘﾃｲ管理支援方法およびﾌﾟﾛｸﾞﾗﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特許2982727 96.08.15 H04L12/56	**認証方法**  ｱﾄﾞﾚｽ解決を行なう機能を提供するNHRPｻｰﾊﾞがn個のｻﾌﾞﾈｯﾄﾜｰｸに所属するためのn個のｲﾝﾀﾌｪｰｽを有している場合、NHRPｻｰﾊﾞが前記ｎ個のｲﾝﾀﾌｪｰｽに各々割り当てられている認証ｷｰおよびそのﾀｲﾌﾟを保持し、NHRPｻｰﾊﾞが、n個のｲﾝﾀﾌｪｰｽのうちあるｲﾝﾀﾌｪｰｽからNHRPﾊﾟｹｯﾄを受けとった場合、ｲﾝﾀﾌｪｰｽに割り当てられている認証ｷｰを用いてNHRPﾊﾟｹｯﾄの認証を行ない、認証が不正の場合にNHRPﾊﾟｹｯﾄを破棄することを特徴とするNHRPﾊﾟｹｯﾄの認証方法。
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2001-345802 00.06.05 H04L12/02	ｲﾝﾀｰﾈｯﾄ接続におけるｾｷｭﾘﾃｲ方法およびﾀｰﾐﾅﾙｱﾀﾞﾌﾟﾀ装置
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾀｲﾑｽﾀﾝﾌﾟの付加	特開2004-172931 02.11.20 H04L12/66	動的IPｱﾄﾞﾚｽ割り当てに対応したﾌｧｲｱｳｫｰﾙｼｽﾃﾑ

表2.3.4 日本電気の技術要素別課題対応特許（12/18）

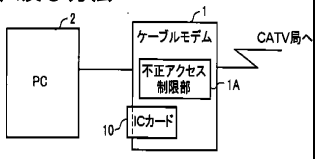
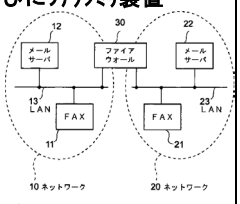
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特許3546771 99.09.07 H04L12/56	**ｹｰﾌﾞﾙﾓﾃﾞﾑの不正ｱｸｾｽ制限ｼｽﾃﾑ及び方法**  CATV局のﾍｯﾄﾞｴﾝﾄﾞﾓﾃﾞﾑ配下のﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀにｱｸｾｽするｹｰﾌﾞﾙﾓﾃﾞﾑの不正ｱｸｾｽ制限ｼｽﾃﾑにおいて、ｱｸｾｽを許可するｱｸｾｽ許可IPｱﾄﾞﾚｽが登録され前記ｹｰﾌﾞﾙﾓﾃﾞﾑに実装されるICｶｰﾄﾞと、ｱｸｾｽ要求元のIPｱﾄﾞﾚｽが前記ICｶｰﾄﾞに登録されているｱｸｾｽ許可IPｱﾄﾞﾚｽと一致しない場合には不正ｱｸｾｽとしてｱｸｾｽを拒否する不正ｱｸｾｽ制限部とを備えることを特徴とするｹｰﾌﾞﾙﾓﾃﾞﾑの不正ｱｸｾｽ制限ｼｽﾃﾑ。
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開2000-330897 （拒絶確定） 99.05.17 G06F13/00,351 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙ負荷分散ｼｽﾃﾑ、ﾌｧｲｱｳｫｰﾙ負荷分散方法および記録媒体**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特開2004-064694 02.07.31 H04L12/56,400 NECｼｽﾃﾑﾃｸﾉﾛｼﾞｰ	**通信ﾈｯﾄﾜｰｸにおけるﾊﾟｹｯﾄ収集の負荷分散方法及びその装置**
	侵入検出の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2001-222513 （拒絶確定） 00.02.08 G06F15/16,620 〔被引用回数 1〕	**情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑにおける接続要求管理装置および方法ならびに接続要求管理処理ﾌﾟﾛｸﾞﾗﾑを記録した情報通信ﾈｯﾄﾜｰｸｼｽﾃﾑにおける記録媒体**
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開平11-073384 （拒絶確定） 97.08.29 G06F13/00,351 〔被引用回数 2〕	**ｳｲﾙｽ対応ﾈｯﾄﾜｰｸ接続ｺﾝﾋﾟｭｰﾀ**
ルーティング制御技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開2000-207357 （拒絶確定） 99.01.20 G06F15/00,310	**ｾｷｭﾘﾃｨ実装ｴｰｼﾞｪﾝﾄｼｽﾃﾑ**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 ﾎﾟｰﾄ番号の登録	特許3594009 01.10.31 H04N1/00,104	**ﾌｧｸｼﾐﾘﾃﾞｰﾀ通信ｼｽﾃﾑ及びその方法並びにﾌｧｸｼﾐﾘ装置**  第一のLANと第二のLANとが、通信経路が制限される通信網を介して接続され、これ等各LAN内にはｲﾝﾀｰﾈｯﾄ標準ﾌﾟﾛﾄｺﾙを実行するﾌｧｸｼﾐﾘ装置が設けられており、これ等ﾌｧｸｼﾐﾘ装置同士が互いにﾃﾞｰﾀ通信をなすようにしたﾌｧｸｼﾐﾘﾃﾞｰﾀ通信ｼｽﾃﾑであって、送信元ﾌｧｸｼﾐﾘ装置は、前記通信網の経路制限を受けない通信経路を探索する経路探索手段と、この探索結果により通信可能と判定され時にこの通信経路によりﾃﾞｰﾀ通信をなす手段とを有することを特徴とするﾌｧｸｼﾐﾘﾃﾞｰﾀ通信ｼｽﾃﾑ。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-355234 03.05.28 G06F13/00,353	**遠隔管理ｼｽﾃﾑおよびﾘﾓｰﾄｹﾞｰﾄｳｪｲ装置並びにﾌﾟﾛｸﾞﾗﾑ**
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特開2001-326693 （拒絶確定） 00.05.17 H04L12/66	**通信装置及び通信制御方法並びに制御ﾌﾟﾛｸﾞﾗﾑ記録媒体**

表2.3.4 日本電気の技術要素別課題対応特許（13/18）

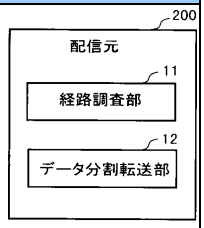
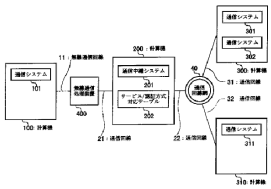
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ルーティング制御技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特許3465258 99.10.13 H04L12/56,100	**ﾃﾞｰﾀ配信経路制御ｼｽﾃﾑ及び方法** 配信元から配信先までの複数のﾙｰﾀから経路情報を探し出し、探し出された経路情報の信頼度を評価する配信元の経路調査部と、経路調査部により信頼度が評価された複数の経路を経由して、ﾃﾞｰﾀを分割して転送する配信元のﾃﾞｰﾀ分割転送部とを備えることを特徴とするﾃﾞｰﾀ配信経路制御ｼｽﾃﾑ。 
ｱﾄﾞﾚｽ変換技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 DNS、DHCPｻｰﾊﾞｰ配置	特開2002-251504 （拒絶確定） 01.02.22 G06F17/60,154	**ﾎﾞﾗﾝﾃｨｱ情報ﾈｯﾄﾜｰｸｼｽﾃﾑ**
	デバイスの正当性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開平11-355302 （拒絶確定） 98.06.11 H04L12/28	**IPｱﾄﾞﾚｽ変換装置及びその変換方法**
	通信データの中継性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2004-070757 02.08.07 G06F15/00,330	**参照権限管理ｼｽﾃﾑ、方法、及びｼｽﾃﾑのﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 DNS、DHCPｻｰﾊﾞｰ配置	特開2001-326696 （拒絶確定） 00.05.18 H04L12/66 〔被引用回数 3〕	**ｱｸｾｽ制御方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2004-328029 03.04.21 H04L12/66	**ﾈｯﾄﾜｰｸｱｸｾｽｼｽﾃﾑ**
ホスト認証技術	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特許3436165 99.01.07 H04L12/66	**通信中継ｼｽﾃﾑ** 通信ｼｽﾃﾑを持った複数の計算機を無線通信回線および通信回線網を含む通信回線によって接続する通信中継ｼｽﾃﾑであって、計算機毎にｻｰﾋﾞｽ階級および認証方式階級が記憶されたｻｰﾋﾞｽ/認証方式対応ﾃｰﾌﾞﾙに基づいて認証を行い接続することを特徴とする通信中継ｼｽﾃﾑ。 
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平07-064912 （拒絶確定） 93.08.31 G06F15/00,330	**不正接続防止機能を有するｵﾝﾗｲﾝｼｽﾃﾑ**
			特開2001-237820 （拒絶確定） 00.02.25 H04L9/08	**認証用証明書書き換えｼｽﾃﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2005-159688 03.11.26 H04L12/56	**ﾈｯﾄﾜｰｸ、通信ﾉｰﾄﾞ及びそれらに用いるｾｷｭﾘﾃｨ方法並びにそのﾌﾟﾛｸﾞﾗﾑ**
			特開2004-258997 03.02.26 G06F15/00,330	**ﾈｯﾄﾜｰｸ上での認証ｼｽﾃﾑ及び該認証ｼｽﾃﾑに用いるｻｰﾊﾞ**

表2.3.4 日本電気の技術要素別課題対応特許（14/18）

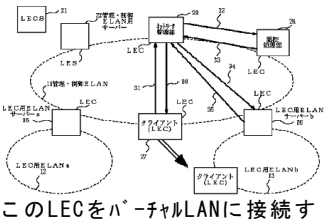
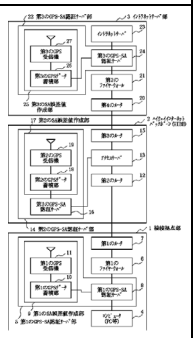
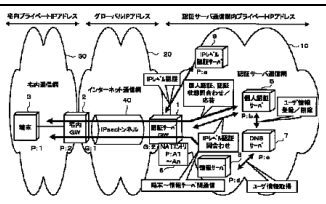
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特許2972637 97.04.03 H04L12/28 NEC通信ｼｽﾃﾑ	**ﾊﾞｰﾁｬﾙLANにおけるｸﾗｲｱﾝﾄの接続方式**  LECがﾊﾞｰﾁｬﾙLANに接続を希望するとき、LECを識別するための識別情報とLECを認証するための認証情報とをLECが前記ﾊﾞｰﾁｬﾙLANに出力し、ﾊﾞｰﾁｬﾙLANが識別情報及び認証情報によりLECを認証したときこのLECをﾊﾞｰﾁｬﾙLANに接続するようにしたことを特徴とするﾊﾞｰﾁｬﾙLANにおけるｸﾗｲｱﾝﾄの接続方式。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特許3501051 99.11.24 H04L12/22	**ｲﾝﾀｰﾈｯﾄ認証ｼｽﾃﾑ**  転送するときの時刻に対応する前記格納しておいたGPS-TimeとこのGPS-Timeに対応する格納しておいたSA誤差値とをIPﾊﾟｹｯﾄの前記IPﾍｯﾀﾞに記録して転送する接続拠点部と、GPS衛星から時々刻々送られてくる衛星の位置とGPS-Timeとを含む衛星情報より前記SA誤差値を時々刻々求め前記GPS-TimeとこのGPS-Timeに対応した前記SA誤差値とを格納しておき、接続拠点部が転送したIPﾊﾟｹｯﾄを受けたときに、このIPﾊﾟｹｯﾄのIPﾍｯﾀﾞに記録されたGPS-TimeとSA誤差値とが格納しておいたGPS-TimeとSA誤差値との中にあるか否かを調べ、格納しておいた中にあるときにはIPﾊﾟｹｯﾄを通過させ、格納しておいた中にないときにはIPﾊﾟｹｯﾄを破棄するﾊｲｳｪｲｲﾝﾀｰﾈｯﾄﾊﾞｯｸﾎﾞｰﾝと、GPS衛星から時々刻々送られてくる衛星の位置とGPS-Timeとを含む前記衛星情報よりSA誤差値を時々刻々求めGPS-TimeとこのGPS-Timeに対応したSA誤差値とを格納しておき、ﾊｲｳｪｲｲﾝﾀｰﾈｯﾄﾊﾞｯｸﾎﾞｰﾝが転送したIPﾊﾟｹｯﾄを受けたときに、このIPﾊﾟｹｯﾄの転送先のIPｱﾄﾞﾚｽを識別し、このIPｱﾄﾞﾚｽが予め登録されていないときにはIPﾊﾟｹｯﾄを破棄し、このIPｱﾄﾞﾚｽが予め登録されているときにはIPﾊﾟｹｯﾄの前記IPﾍｯﾀﾞに記録されたGPS-TimeとSA誤差値とが格納しておいたGPS-TimeとSA誤差値との中にあるか否かを調べ、格納しておいた中にないときにはIPﾊﾟｹｯﾄを破棄し、格納しておいた中にあるときにはIPﾊﾟｹｯﾄを受けるｲﾝﾄﾗﾈｯﾄｻｰﾊﾞ部と、を備えたことを特徴とするｲﾝﾀｰﾈｯﾄ認証ｼｽﾃﾑ。
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 DNS、DHCPｻｰﾊﾞｰ配置	特許3616570 01.01.04 H04L12/66 ｴﾇ・ﾃｨ・ﾃｨ・ｺﾐｭﾆｹｰｼｮﾝｽﾞ 〔被引用回数 1〕	**ｲﾝﾀｰﾈｯﾄ中継接続方式**  ﾀﾞｲｱﾙｱｯﾌﾟによりIPに準拠するｱﾄﾞﾚｽが付与され、端末を含む宅内通信網とｸﾞﾛｰﾊﾞﾙｱﾄﾞﾚｽによりIPに基づく通信を行うｲﾝﾀｰﾈｯﾄ通信網との接続点に設けられた宅内GWと、複数の認証ｻｰﾊﾞを含みIPに準拠するﾌﾟﾗｲﾍﾞｰﾄIPｱﾄﾞﾚｽにより制御される認証ｻｰﾊﾞ通信網とｲﾝﾀｰﾈｯﾄ通信網との接続点に設けられた認証ｻｰﾊﾞGWとを備えたｲﾝﾀｰﾈｯﾄ中継接続方式において、ｲﾝﾀｰﾈｯﾄ通信網の中に宅内GWと認証ｻｰﾊﾞGWとの間に、IPsecﾄﾝﾈﾙを設定する手段を備えたことを特徴とするｲﾝﾀｰﾈｯﾄ中継接続方式。

表2.3.4 日本電気の技術要素別課題対応特許（15/18）

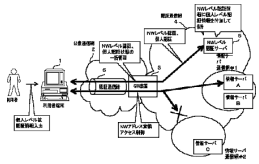
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特許3645844 01.09.12 H04L12/66 ｴﾇ・ﾃｨ・ﾃｨ・ｺﾐｭﾆｹｰｼｮﾝｽﾞ	**中継接続方式およびﾈｯﾄﾜｰｸﾚﾍﾞﾙ認証ｻｰﾊﾞおよびｹﾞｰﾄｳｪｲ装置および情報ｻｰﾊﾞおよびﾌﾟﾛｸﾞﾗﾑ**  ﾈｯﾄﾜｰｸﾚﾍﾞﾙの認証情報に個人ﾚﾍﾞﾙの認証情報を付加した認証情報を保持するﾈｯﾄﾜｰｸﾚﾍﾞﾙ認証ｻｰﾊﾞが設けられ、前記ﾈｯﾄﾜｰｸﾚﾍﾞﾙ認証ｻｰﾊﾞは、前記認証情報と併せて個人ﾚﾍﾞﾙのｱｸｾｽ制御情報も付加して保持する手段と、前記ｹﾞｰﾄｳｪｲ装置から認証要求として受信した被認証情報を検証しその認証結果に前記ｱｸｾｽ制御情報を付加して前記ｹﾞｰﾄｳｪｲ装置に返送する手段とを備え、前記ｹﾞｰﾄｳｪｲ装置は、ﾈｯﾄﾜｰｸﾚﾍﾞﾙの被認証情報に個人ﾚﾍﾞﾙの被認証情報を付加した被認証情報および利用者識別子とこの被認証情報の有効期限情報とを前記利用者端末から受信して前記有効期限を検証して前記被認証情報の有効性を確認する手段と、前記利用者識別子および前記被認証情報を用いて前記ﾈｯﾄﾜｰｸﾚﾍﾞﾙ認証ｻｰﾊﾞに対して前記認証要求を送信する手段と、認証の完了時に認証通信網内部で使用するﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸｱﾄﾞﾚｽを前記利用者端末の利用者に割当てこのﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸｱﾄﾞﾚｽと前記ﾈｯﾄﾜｰｸﾚﾍﾞﾙ認証ｻｰﾊﾞから前記認証結果として返送されたﾈｯﾄﾜｰｸﾚﾍﾞﾙの認証情報および個人ﾚﾍﾞﾙの認証情報としての前記利用者の公衆通信網におけるｱﾄﾞﾚｽであるﾈｯﾄﾜｰｸｱﾄﾞﾚｽおよび利用者識別子をそれぞれ保持するとともにこれらに対応して前記ﾈｯﾄﾜｰｸﾚﾍﾞﾙ認証ｻｰﾊﾞから前記認証結果とともに返送された前記個人ﾚﾍﾞﾙのｱｸｾｽ制御情報を保持する手段と、認証の完了時に、前記利用者との間に相互に秘密情報を共有してこの秘密情報を利用した暗号通信路である認証通信路を前記利用者端末との間に生成する手段と、前記利用者からの認証通信網内へのｱｸｾｽについては前記認証通信路に限定して許容するとともに前記公衆通信網におけるﾈｯﾄﾜｰｸｱﾄﾞﾚｽと前記認証通信網内部で利用するﾌﾟﾗｲﾍﾞｰﾄｱﾄﾞﾚｽとの間でｱﾄﾞﾚｽ変換を行う手段と、前記利用者からの前記認証通信網へのｱｸｾｽ時に前記利用者のﾈｯﾄﾜｰｸｱﾄﾞﾚｽから該当する前記ｱｸｾｽ制御情報を検索しこのｱｸｾｽ制御情報にしたがって前記利用者の前記情報ｻｰﾊﾞに対するｱｸｾｽを制御する手段とを備えたことを特徴とする中継接続方式。
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平07-028754 （拒絶確定） 93.07.14 G06F15/00,330	**ﾎｽﾄｺﾝﾋﾟｭｰﾀにおける多重機密保護方式**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2001-318889 （拒絶確定） 00.05.11 G06F15/00,330 〔被引用回数 1〕	**ﾃﾞｨﾚｸﾄﾘｼｽﾃﾑ**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開平09-205457 （拒絶確定） 96.01.29 H04L12/46 〔被引用回数 1〕	**ｾｷｭﾘﾃｨｼｽﾃﾑ**
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2004-048234 02.07.10 H04L12/46	**ﾕｰｻﾞ認証ｼｽﾃﾑおよびﾕｰｻﾞ認証方法**

表2.3.4 日本電気の技術要素別課題対応特許（16/18）

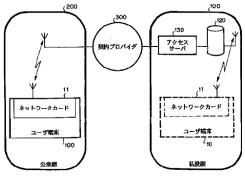
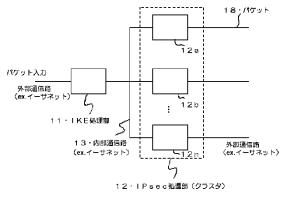
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
ホスト認証技術	通信データの中継性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平11-261731 （拒絶確定） 98.03.13 H04M11/00,303	**移動通信ｼｽﾃﾑ、移動通信ｼｽﾃﾑにおける接続方法及びこれが書き込まれた記憶媒体**
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2000-311138 （拒絶確定） 99.04.28 G06F15/00,330 〔被引用回数 1〕	**ｻｰﾊﾞの分散認証ｼｽﾃﾑ及び方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-048586 02.07.15 H04L12/56,100	**ﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ、ﾈｯﾄﾜｰｸ通信方法及び認証ﾗﾍﾞﾙｻｰﾊﾞ**
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2004-070814 02.08.08 G06F15/00,330	**ｻｰﾊﾞｾｷｭﾘﾃｨ管理方法及び装置並びにﾌﾟﾛｸﾞﾗﾑ**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平07-013930 （拒絶確定） 93.06.24 G06F15/00,330	**ｵﾝﾗｲﾝｼｽﾃﾑにおけるｾｷｭﾘﾃｨ制御方式**
		回路の改良 ｽｲｯﾁ回路の追加 無線との切換	特開2002-163030 （拒絶確定） 00.11.22 G06F1/00,370	**ｺﾝﾋﾟｭｰﾀ装置管理ｼｽﾃﾑ及びｺﾝﾋﾟｭｰﾀ装置管理方法**
トンネリング技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2002-094572 （拒絶確定） 00.09.12 H04L12/66	**通信ｼｽﾃﾑ及び通信方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特許3344421 00.12.06 H04L12/56	**仮想私設網**  相互に接続されている複数の独立したﾈｯﾄﾜｰｸと、前記ﾈｯﾄﾜｰｸにｱｸｾｽでき、新たに取得した送信元IPｱﾄﾞﾚｽを用いたIPｶﾌﾟｾﾙ通信及び暗号化機能を持つ端末と、前記ﾈｯﾄﾜｰｸのいずれかに接続されたﾃﾞｰﾀﾍﾞｰｽと、前記ﾃﾞｰﾀﾍﾞｰｽへのｱｸｾｽを管理制御しIPｶﾌﾟｾﾙ通信及び暗号化機能を持つｱｸｾｽｻｰﾊﾞとを備え、前記端末がいずれのﾈｯﾄﾜｰｸからでも前記ﾃﾞｰﾀﾍﾞｰｽにIPｶﾌﾟｾﾙ暗号化通信により秘匿性を保ったままｱｸｾｽする仮想私設網。
	システムの性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 容疑ﾚﾍﾞﾙ、悪性閾値	特許3603830 01.09.28 H04L12/66	**ｾｷｭﾘﾃｨｹﾞｰﾄｳｪｲ装置**  IPｾｷｭﾘﾃｨ通信に必要なﾊﾟﾗﾒｰﾀを対向するｾｷｭﾘﾃｨｹﾞｰﾄｳｪｲとの間でﾈｺﾞｼｴｰﾄするﾈｺﾞｼｴｰｼｮﾝ処理を行う認証ｷｰ交換手段と、前記認証ｷｰ交換手段と内部通信路で接続されており、前記認証ｷｰ交換手段から送られてきたﾊﾟｹｯﾄに対してIPｾｷｭﾘﾃｨ処理を実行するIPｾｷｭﾘﾃｨ処理手段と、からなるｾｷｭﾘﾃｨｹﾞｰﾄｳｪｲ装置。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特開2003-204326 02.01.09 H04L9/36	**通信ｼｽﾃﾑと暗号処理機能付きLAN制御装置、及び通信制御ﾌﾟﾛｸﾞﾗﾑ**

表2.3.4 日本電気の技術要素別課題対応特許（17/18）

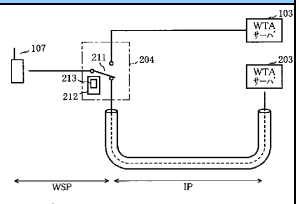
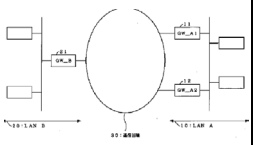
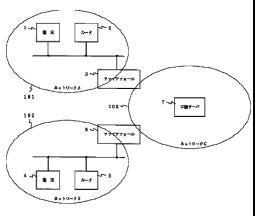
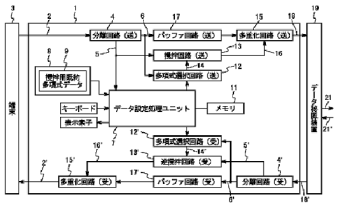
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	各種の処理手順改良 各種処理の実行手順 特定処理の実行	特許3575360 99.12.24 H04L12/22	**通信方法および通信ｼｽﾃﾑ**  ﾈｯﾄﾜｰｸ上のｺﾝﾃﾝﾂを取得してこれを表示する機能を備えた携帯型情報端末とこの携帯型情報端末と電話網で接続するｹﾞｰﾄｳｪｲとの間では、電話網上で通信の安全性を確保するための処理を実現する所定のﾌﾟﾛﾄｺﾙで暗号化したﾃﾞｰﾀの伝送を行い、ｹﾞｰﾄｳｪｲと前記ﾈｯﾄﾜｰｸ上のｺﾝﾃﾝﾂを格納したｻｰﾊﾞとの間はこの暗号化したﾃﾞｰﾀをﾄﾝﾈﾘﾝｸﾞ処理することを特徴とする通信方法。
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾄﾗﾌｨｯｸ	特開2004-328298 03.04.24 H04L12/66	**通信ｼｽﾃﾑ､通信装置及びその動作制御方法**
		情報の送信、転送､分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特許3651424 01.08.28 H04L12/46,100	**大規模IPSecVPN構築方法､大規模IPSecVPNｼｽﾃﾑ､ﾌﾟﾛｸﾞﾗﾑ及び鍵共有情報処理装置**  大規模LANのｹﾞｰﾄｳｪｲのｲﾝﾀｰﾈｯﾄｷｰｴｸｽﾁｪﾝｼﾞ部が、このｹﾞｰﾄｳｪｲのIPSec部に鍵設定を行うとともに、このｹﾞｰﾄｳｪｲの鍵転送部に鍵転送を要求し、前記ｹﾞｰﾄｳｪｲの鍵転送部が、前記要求に応じて、前記大規模LANの他のｹﾞｰﾄｳｪｲの鍵転送部に鍵転送を行い、前記他のｹﾞｰﾄｳｪｲの鍵転送部が、この転送されてきた鍵を用いて、前記他のｹﾞｰﾄｳｪｲのIPSec部に鍵設定を行うことを特徴とする大規模IPSec VPNの構築方法。
		情報の送信、転送､分岐の手順改良 情報転送の手順 VPN設定情報	特開2004-104542 02.09.11 H04L12/66	**ﾈｯﾄﾜｰｸ､IPsec設定ｻｰﾊﾞ装置､IPsec処理装置及びそれらに用いるIPsec設定方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2004-328688 03.04.30 H04L12/56	**ﾈｯﾄﾜｰｸ間接続装置の自動設定ｼｽﾃﾑ及びそれに用いる自動設定方法**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特許3637863 00.11.01 H04L12/66 〔被引用回数 1〕	**仮想ﾈｯﾄﾜｰｸ及び仮想ﾈｯﾄﾜｰｸ接続方式**  第1及び第2のﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ内に配設されかつ中継ｻｰﾊﾞに中継先相手を通知して中継先相手とのﾃﾞｰﾀ送受信を行う第1及び第2のﾙｰﾀを有し、中継ｻｰﾊﾞは、第1及び第2のﾙｰﾀから各々通知された中継先相手にしたがって第1のﾙｰﾀからのﾃﾞｰﾀを第2のﾙｰﾀに中継しかつ第2のﾙｰﾀからのﾃﾞｰﾀを第1のﾙｰﾀにそれぞれ中継するようにしたことを特徴とする仮想ﾈｯﾄﾜｰｸ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2002-033760 （拒絶確定） 00.07.14 H04L12/54	**電子ﾒｰﾙのｾｷｭﾘﾃｨを代行して保証する方法及びｼｽﾃﾑ並びに記録媒体**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2003-143124 （拒絶確定） 01.10.31 H04L9/08	**電文送受信ｼｽﾃﾑ､電文送受信方法および電文送受信用ﾌﾟﾛｸﾞﾗﾑ**

表2.3.4 日本電気の技術要素別課題対応特許（18/18）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾌｫｰﾏｯﾄの変換	特開2004-165761 02.11.11 H04L12/56	**通信ｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 多重符号化で変換	特開2001-144773 （拒絶確定） 99.11.12 H04L12/28	**ﾃﾞｰﾀ秘匿装置及びﾃﾞｰﾀ秘匿通信方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ｱﾄﾞﾚｽの暗号化	特許3596676 01.06.29 H04L12/56	**IPﾃﾞｰﾀ撹拌装置、IPﾃﾞｰﾀ秘匿ｼｽﾃﾑ、及び、IPﾃﾞｰﾀ撹拌方法**  送信対象IPﾃﾞｰﾀを送信対象ﾍｯﾀﾞ部分と送信対象ﾃﾞｰﾀ部分とに分離する送信用分離回路と、前記送信対象ﾍｯﾀﾞ部分を撹拌用既約多項式に基づいて撹拌する送信用撹拌回路と、前記送信用撹拌回路により撹拌された撹拌後送信対象ﾍｯﾀﾞ部分と前記送信対象ﾃﾞｰﾀ部分を多重化する送信用多重化回路とを含み、前記送信用多重化回路により多重化された多重化IPﾃﾞｰﾀを暗号化のために出力するIPﾃﾞｰﾀ撹拌装置。
	攻撃パターンの高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2003-050641 （拒絶確定） 01.08.07 G06F1/00	**ﾌﾟﾛｸﾞﾗﾑ管理ｼｽﾃﾑ、そのﾌﾟﾛｸﾞﾗﾑ管理方法、及び情報管理ﾌﾟﾛｸﾞﾗﾑ**
	経済性の向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特許3637863 00.11.01 H04L12/66 〔被引用回数 1〕	**仮想ﾈｯﾄﾜｰｸ及び仮想ﾈｯﾄﾜｰｸ接続方式** 概要は技術要素「ﾄﾝﾈﾘﾝｸﾞ技術」、課題「中継するﾃﾞｰﾀの機密性向上」の項参照

2.4 東芝

2.4.1 企業の概要

商号	株式会社　東芝
本社所在地	〒105-8001　東京都港区芝浦1-1-1
設立年	1904年（明治37年）
資本金	2,749億円（2005年3月末）
従業員数	30,810名（2005年3月末）（連結：160,038名）
事業内容	情報通信システム、社会システム、重電システム、デジタルメディア、家庭電器、電子デバイス等の製造・販売・エンジニアリング・サービス、他

セキュリティが経営を、ビジネスを加速させるとして、セキュリティソリューションに対応したホームページを開設し、セキュリティのサービス体系、セキュリティ製品やセキュリティ情報等を紹介している。

（出典：http://www.toshiba-sol.co.jp/nsd/sec/index_j.htm）

2.4.2 製品例

情報セキュリティの製品のホームページに紹介されている製品例を表2.4.2に示す。

表2.4.2 東芝の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
AntiHacker-Pro	①　インライン設置型アーキテクチャにより不正アクセスを検知し、確実に遮断 ②　脆弱性情報により不正アクセスを検知し、直ちに遮断 ③　Dos/Ddos防御機能の搭載 ④　L7パラメトリック方式による未知攻撃検知の機能搭載
IDSソリューション RealSecure	Sensor,Protector,ScannerなどRealSecure商品を使用したIDSのソリューション

（出典：http://www.toshiba-sol.co.jp/products/info_sec.htm）

2.4.3 技術開発拠点と研究者

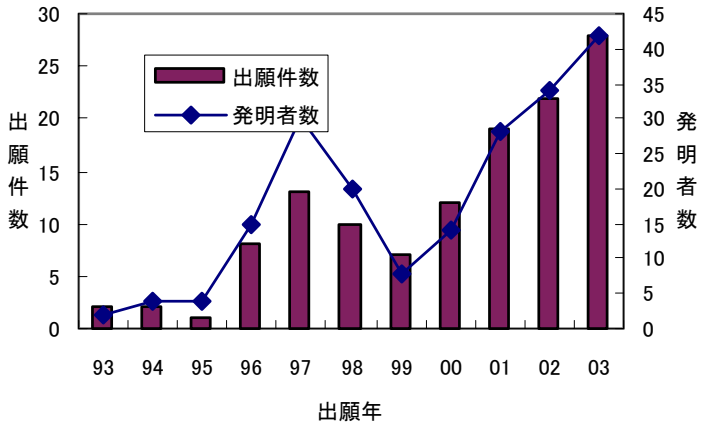
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都港区芝浦1丁目1番1号 株式会社東芝本社事務所内
東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内
東京都日野市旭が丘3丁目1番地1 株式会社東芝日野工場内
東京都府中市東芝町1番地 株式会社東芝府中工場内
神奈川県横浜市磯子区新杉田町8番地 株式会社東芝横浜事業所内
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝小向工場内
神奈川県川崎市川崎区日進町7番地1東芝情報システム株式会社内
石川県金沢市平和町2丁目28番60号B39-12
アメリカ合衆国カリフォルニア州アーバイン
アメリカ合衆国ニュージャージー州コンベント

図2.4.3に、東芝の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。1999年以降、出願件数は増加傾向で、03年では25件を越え、発明者数は40人を越えた。

図2.4.3 東芝の不正アクセス侵入検知防御技術に関する出願件数と発明者数



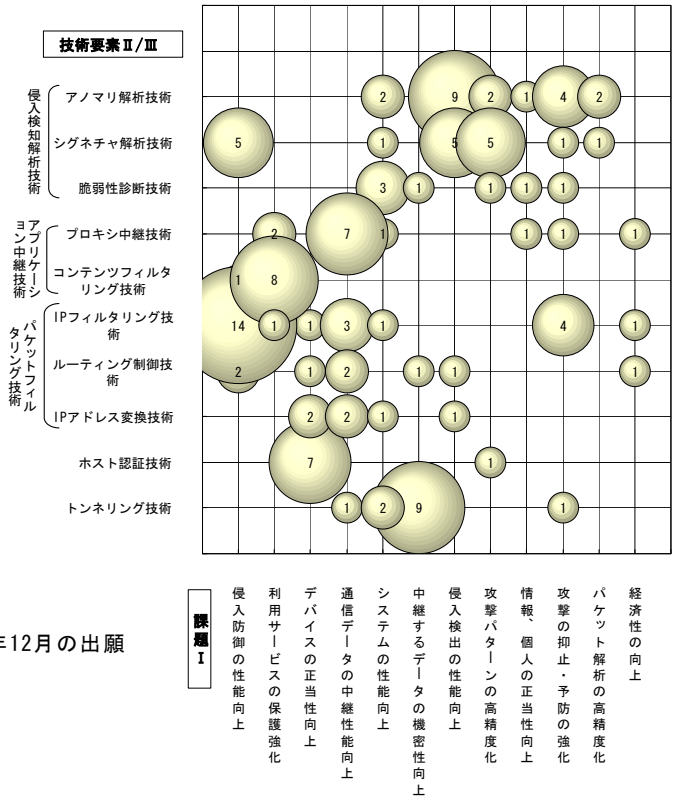
2.4.4 技術開発課題対応特許の概要

図2.4.4-1に、東芝の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.4.4-2に、東芝の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

IPフィルタリング技術が最も多く出願され、次いでアノマリ解析技術に関する出願が多い。これらの出願のうち、最も多い課題は、「侵入防御の性能向上」であり、次いで多い課題は「侵入検出の性能向上」である。

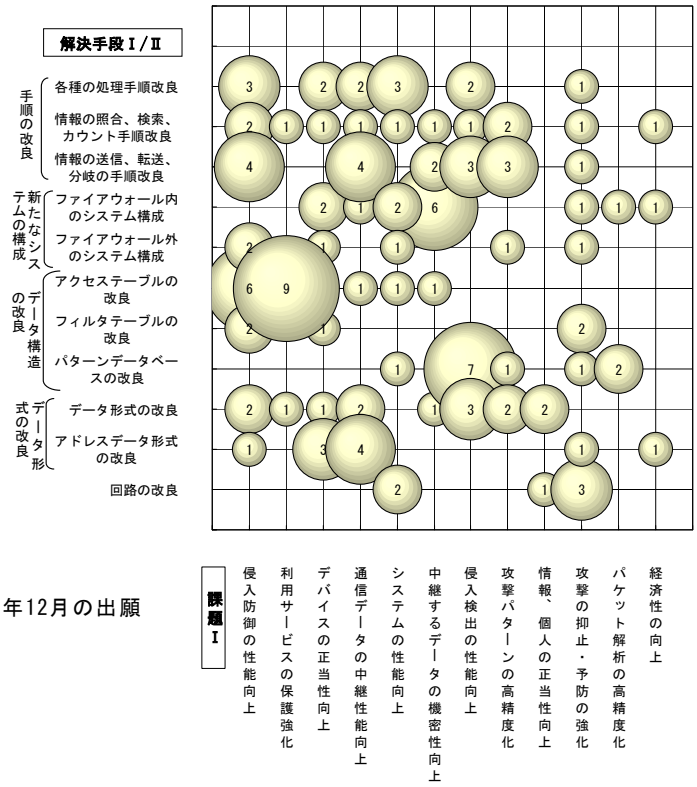
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。次いで「侵入検出の性能向上」の課題に対しては、「パターンデータベースの改良」で多く対応している。

図2.4.4-1 東芝の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.4.4-2 東芝の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.4.4 東芝の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は124件で、そのうち17件が登録特許である。なお、表2.4.4では図2.4.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.4.4 東芝の技術要素別課題対応特許（1/14）

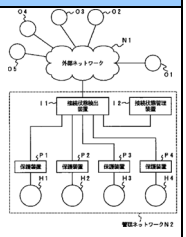
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	システムの性能向上	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特許3426832 96.01.26 G06F13/00,351 〔被引用回数 2〕	**ﾈｯﾄﾜｰｸｱｸｾｽ制御方法**  複数の計算機のいずれかを送信元または宛先とするすべてのﾊﾟｹｯﾄを監視可能な位置に設けられた接続状態検出手段により、ﾊﾟｹｯﾄの内容に基づいて、複数の計算機の他計算機との接続開始および接続終了を少なくとも検出し、複数の計算機対応に設けられた保護手段により、少なくとも検出された接続開始または接続終了の情報に基づいて、対応する計算機にﾊﾟｹｯﾄを受信させるか否かを決定することを特徴とするﾈｯﾄﾜｰｸｱｸｾｽ制御方法。
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 送信回数	特開2004-164553 02.09.26 G06F13/00,351	**ｻｰﾊﾞ計算機保護装置、ｻｰﾊﾞ計算機保護方法、ｻｰﾊﾞ計算機保護ﾌﾟﾛｸﾞﾗﾑ及びｻｰﾊﾞ計算機**
	侵入検出の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開2003-173300 01.09.27 G06F13/00,351 〔被引用回数 2〕	**ｻｰﾊﾞｰ計算機保護装置、ｻｰﾊﾞｰ計算機保護方法、ｻｰﾊﾞｰ計算機保護ﾌﾟﾛｸﾞﾗﾑ及びｻｰﾊﾞｰ計算機**
		各種の処理手順改良 各種処理の実行手順 特定処理の実行	特開2004-274481 03.03.10 H04L12/22	**発信源追跡装置及びﾌﾟﾛｸﾞﾗﾑ**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 攻撃情報の通知	特開2004-146931 （特許3689079） 02.10.22 H04L12/56,400	**ﾊﾟｹｯﾄ転送装置およびﾊﾟｹｯﾄ転送装置の不正ｱｸｾｽ検知時に於ける情報通知方法**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特開2003-348169 （特許3725139） 00.08.21 H04L12/66	**ﾊﾟｹｯﾄ転送装置およびﾊﾟｹｯﾄ転送方法**
			特開2003-348170 （特許3725140） 00.08.21 H04L12/66	**ﾊﾟｹｯﾄ転送装置およびﾊﾟｹｯﾄ転送方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 異常値出現頻度	特開2005-011234 03.06.20 G06F13/00,351	**不正ｱｸｾｽ検出装置、不正ｱｸｾｽ検出方法およびﾌﾟﾛｸﾞﾗﾑ**
			特開2003-150550 01.11.14 G06F15/00,330	**情報処理ｼｽﾃﾑ**
			特開2005-085158 03.09.10 G06F13/00,351	**不正ｱｸｾｽ検出装置およびｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ上に於ける異常ﾃﾞｰﾀ検出方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 HTTPの学習	特開2005-085157 03.09.10 G06F15/00,330	**不正ｱｸｾｽ検出装置、不正ｱｸｾｽ検出方法、および管理端末**
	攻撃パターンの高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ｱﾗｰﾄﾊﾟﾀｰﾝの追加	特開2003-108521 01.09.29 G06F15/00,330	**脆弱性評価ﾌﾟﾛｸﾞﾗﾑ、方法及びｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2005-072724 03.08.20 H04L12/56,100	**通信制御装置、通信制御ｼｽﾃﾑ、通信制御方法および通信制御ﾌﾟﾛｸﾞﾗﾑ**

表2.4.4 東芝の技術要素別課題対応特許（2/14）

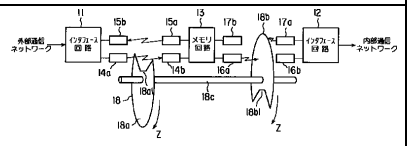
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特表2005-515715 02.01.17 H04L9/08	**ﾃﾞｰﾀ伝送ﾘﾝｸ**
	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開2003-099339 01.09.25 G06F13/00,351 〔被引用回数 3〕	**侵入検知･防御装置及びﾌﾟﾛｸﾞﾗﾑ**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 ﾊﾟﾀｰﾝの廃棄	特開2003-298628 02.03.29 H04L12/56	**ｻｰﾊﾞ保護ﾈｯﾄﾜｰｸｼｽﾃﾑ､ｻｰﾊﾞおよびﾙｰﾀ**
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特許3507718 99.01.11 H04L12/28	**ﾈｯﾄﾜｰｸ接続装置**  第1の通信ﾈｯﾄﾜｰｸとｲﾝﾀﾌｪｰｽをとる第1のｲﾝﾀﾌｪｰｽ手段と、第2の通信ﾈｯﾄﾜｰｸとｲﾝﾀﾌｪｰｽをとる第2のｲﾝﾀﾌｪｰｽ手段と、第1のｲﾝﾀﾌｪｰｽ手段と前記第2のｲﾝﾀﾌｪｰｽ手段との間に位置し､ﾃﾞｰﾀ信号を格納する記憶手段と、第1のｲﾝﾀﾌｪｰｽ手段と記憶手段との間に設けられ、第1のｲﾝﾀｰﾌｪｰｽ手段から出力されるﾃﾞｰﾀ信号のみを通し､記憶手段から出力されﾃﾞｰﾀ転送に必要な制御信号のみを通す信号経路を形成する第1の信号経路形成手段と､記憶手段と前記第2のｲﾝﾀﾌｪｰｽ手段との間に設けられ､記憶手段から読み出されたﾃﾞｰﾀ信号のみを通し､第2のｲﾝﾀﾌｪｰｽ手段から出力されﾃﾞｰﾀ転送に必要な制御信号のみを通す信号経路を形成する第2の信号経路形成手段とを具備してなることを特徴とするﾈｯﾄﾜｰｸ接続装置。
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2005-128784 03.10.23 G05B23/02	**監視制御ﾈｯﾄﾜｰｸｼｽﾃﾑ**
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2000-207238 99.01.11 G06F11/20,310	**ﾈｯﾄﾜｰｸｼｽﾃﾑおよび情報記録媒体**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 ﾎﾟｰﾄｽｷｬﾝ蓄積	特開2005-025269 03.06.30 G06F15/00,330	**ﾈｯﾄﾜｰｸ中継装置及びｾｷｭﾘﾃｨ検査方法**
シグネチャ解析技術	侵入防御の性能向上	各種の処理手順改良 各種処理の実行手順 ﾊﾟﾀｰﾝ､ﾙｰﾙの言語記述	特開2004-240766 03.02.06 G06F17/30,340	**ﾊﾟﾀｰﾝ検出処理ﾌﾟﾛｸﾞﾗﾑ生成ｼｽﾃﾑおよびﾊﾟﾀｰﾝ検出処理ﾌﾟﾛｸﾞﾗﾑ生成方法**
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路､中継ｻｰﾊﾞｰ	特開平08-153072 94.09.30 G06F15/00,330 〔被引用回数 3〕	**計算機ｼｽﾃﾑ及び計算機ｼｽﾃﾑ管理方法**
		情報の送信、転送､分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2000-090048 98.09.10 G06F15/00,310	**ｾｷｭﾘﾃｨ情報更新ｼｽﾃﾑ及び記録媒体**

表2.4.4 東芝の技術要素別課題対応特許（3/14）

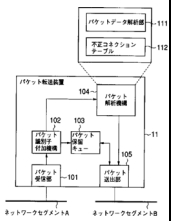
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
シグネチャ解析技術	侵入防御の性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開平11-308272 98.04.23 H04L12/56	**ﾊﾟｹｯﾄ通信制御ｼｽﾃﾑ及びﾊﾟｹｯﾄ通信制御装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開平08-006899 （みなし取下） 94.06.17 G06F15/00,330	**監視制御装置**
	システムの性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 ﾊﾟﾀｰﾝの廃棄	特許3581345 01.12.13 H04L12/66	**ﾊﾟｹｯﾄ転送装置およびﾊﾟｹｯﾄ転送方法**  ﾈｯﾄﾜｰｸｾｸﾞﾒﾝﾄ上のﾊﾟｹｯﾄを受信するﾊﾟｹｯﾄ受信手段と､ﾊﾟｹｯﾄ受信手段で受信した受信ﾊﾟｹｯﾄを一時保留するﾊﾟｹｯﾄ保留手段と､不正ｱｸｾｽに関わるﾊﾟｹｯﾄであると判定されたﾊﾟｹｯﾄのｺﾈｸｼｮﾝ識別情報が登録されるｺﾈｸｼｮﾝ識別情報記憶手段と､前記ﾊﾟｹｯﾄ受信手段により受信した受信ﾊﾟｹｯﾄのｺﾈｸｼｮﾝ識別情報が前記ｺﾈｸｼｮﾝ識別情報記憶手段に登録されているか否かを判別して､不正ｱｸｾｽに関わるﾊﾟｹｯﾄであるか否かを判定する第1の判定手段と､前記受信ﾊﾟｹｯﾄのｺﾈｸｼｮﾝ識別情報が前記ｺﾈｸｼｮﾝ識別情報記憶手段に登録されていないと判別した場合､前記受信ﾊﾟｹｯﾄのﾃﾞｰﾀを解析して､当該受信ﾊﾟｹｯﾄが正常なﾊﾟｹｯﾄか不正ｱｸｾｽに関わるﾊﾟｹｯﾄであるかを判定する第2の判定手段と､および前記受信ﾊﾟｹｯﾄのﾃﾞｰﾀ解析によって不正ｱｸｾｽに関わるﾊﾟｹｯﾄであると判定した場合､当該受信ﾊﾟｹｯﾄのｺﾈｸｼｮﾝ識別情報を前記ｺﾈｸｼｮﾝ識別情報記憶手段に登録する手段とを有するﾊﾟｹｯﾄ解析手段と､前記ﾊﾟｹｯﾄ解析手段の前記判定結果に基づき､前記ﾊﾟｹｯﾄ保留手段に一時保留されている前記受信ﾊﾟｹｯﾄのうち､前記不正ｱｸｾｽに関わるﾊﾟｹｯﾄは破棄し､正常な受信ﾊﾟｹｯﾄのみを送信先のﾈｯﾄﾜｰｸｾｸﾞﾒﾝﾄへ送出するﾊﾟｹｯﾄ送出手段とを具備することを特徴とするﾊﾟｹｯﾄ転送装置。
	侵入検出の性能向上	情報の照合､検索､ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2005-039591 03.07.16 H04L12/66	**不正ｱｸｾｽ防御装置及びﾌﾟﾛｸﾞﾗﾑ**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2005-045649 （特許3730642） 03.07.24 H04L12/56,100	**攻撃ﾊﾟｹｯﾄ検出装置及び方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 ﾊﾟﾀｰﾝの切換	特開2003-092603 01.09.17 H04L12/56,400 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ侵入検知ｼｽﾃﾑ､装置及びﾌﾟﾛｸﾞﾗﾑ**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 ﾄﾗﾌｨｯｸﾃﾞｰﾀの学習	特開2002-300219 01.03.30 H04L12/66	**ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ､IDS欺瞞防止装置､IDS欺瞞防止方法およびそのﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの圧縮化	特開2005-085159 03.09.10 G06F15/00,330	**不正ｱｸｾｽ検知装置および不正ｱｸｾｽ検出方法**

表2.4.4 東芝の技術要素別課題対応特許（4/14）

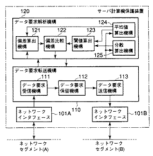
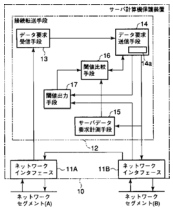
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
シグネチャ解析技術	攻撃パターンの高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾊﾟｹｯﾄのﾌｨｰﾙﾄﾞ	特許3651610 03.01.24 H04L12/66	**ｻｰﾊﾞ計算機保護装置、同装置のﾃﾞｰﾀ要求解析方法およびﾌﾟﾛｸﾞﾗﾑ**  ｸﾗｲｱﾝﾄから送出されたﾃﾞｰﾀ要求をｻｰﾊﾞ計算機に代わり受信して、当該受信したﾃﾞｰﾀ要求が不正ｱｸｾｽに関わるものか否かを解析するﾃﾞｰﾀ要求解析機構と、当該ﾃﾞｰﾀ要求解析機構の判定に従い前記ｸﾗｲｱﾝﾄから送出されたﾃﾞｰﾀ要求の前記ｻｰﾊﾞ計算機への転送を制御するﾃﾞｰﾀ要求転送機構とを備えたｻｰﾊﾞ計算機保護装置に於いて、前記ﾃﾞｰﾀ要求解析機構は、前記ｻｰﾊﾞ計算機が過去の一定期間内に受信したﾃﾞｰﾀ要求のﾒｯｾｰｼﾞ長の平均値を算出する平均値算出手段と、前記ｻｰﾊﾞ計算機が過去の一定期間内に受信したﾃﾞｰﾀ要求のﾒｯｾｰｼﾞ長の分散を算出する分散算出手段と、前記平均値算出手段が算出した平均値と前記分散算出手段が算出した分散から、前記ﾒｯｾｰｼﾞ長の偏差の閾値を算出する閾値算出手段と、前記平均値算出手段が算出した平均値と前記解析の対象にある受信したﾃﾞｰﾀ要求のﾒｯｾｰｼﾞ長からﾒｯｾｰｼﾞ長の偏差を算出する偏差算出手段と、前記閾値算出手段が算出した閾値と前記偏差算出手段が算出した偏差を比較し、偏差が閾値を超えたとき、前記解析の対象にある受信したﾃﾞｰﾀ要求は不正ｱｸｾｽに関わるものであると判定する偏差比較手段とを具備し、前記ﾃﾞｰﾀ要求転送機構は、前記偏差比較手段の判定に従いｸﾗｲｱﾝﾄから送出されたﾃﾞｰﾀ要求のｻｰﾊﾞ計算機への転送を制御することを特徴とするｻｰﾊﾞ計算機保護装置。
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開2003-091465 01.09.17 G06F13/00,351	**防御ｼｽﾃﾑ、装置及びﾌﾟﾛｸﾞﾗﾑ**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特許3566699 02.01.30 H04L12/66	**ｻｰﾊﾞ計算機保護装置および同装置のﾃﾞｰﾀ転送制御方法**  ｸﾗｲｱﾝﾄから送出されたﾃﾞｰﾀ要求をｻｰﾊﾞに代わり受信し、当該受信したｸﾗｲｱﾝﾄからｻｰﾊﾞ計算機へのﾃﾞｰﾀ要求について、当該ｻｰﾊﾞ計算機が過去の一定期間内に受信した前記ﾃﾞｰﾀ要求の回数を計測して、当該計測したﾃﾞｰﾀ要求の回数を閾値と比較し、当該比較の結果に応じて前記受信したﾃﾞｰﾀ要求を保留し若しくは要求先のｻｰﾊﾞ計算機に転送するｻｰﾊﾞ計算機保護装置に於いて、前記受信したﾃﾞｰﾀ要求の保留状態と前記ﾃﾞｰﾀ要求をｻｰﾊﾞに送出した際のｻｰﾊﾞからの応答状態をもとに前記閾値を動的に可変制御する手段を具備したことを特徴とするｻｰﾊﾞ計算機保護装置。

表2.4.4 東芝の技術要素別課題対応特許（5/14）

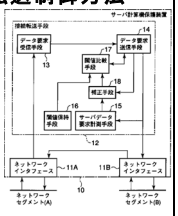
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
シグネチャ解析技術	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特許3566700 02.01.30 H04L12/66	**ｻｰﾊﾞ計算機保護装置および同装置のﾃﾞｰﾀ転送制御方法**  複数のﾈｯﾄﾜｰｸｲﾝﾀﾌｪｰｽを持ち、ｸﾗｲｱﾝﾄと一台あるいは複数台のｻｰﾊﾞ計算機との間に挿入されるｻｰﾊﾞ計算機保護装置に於いて、ｸﾗｲｱﾝﾄから送出されたﾃﾞｰﾀ要求をｻｰﾊﾞに代わり受信する要求受信手段と、前記要求受信手段が受信したｸﾗｲｱﾝﾄからｻｰﾊﾞ計算機へのﾃﾞｰﾀ要求について、前記ｻｰﾊﾞ計算機が過去の一定期間内に受信した前記ﾃﾞｰﾀ要求の回数を計測する計測手段と、前記計測手段で計測されたﾃﾞｰﾀ要求の回数を当該ﾃﾞｰﾀ要求の形態に応じて定められた補正条件をもとに補正する補正手段と、前記補正手段で補正されたﾃﾞｰﾀ要求の回数を予め定められた閾値と比較する比較手段と、前記比較手段による比較の結果、前記ﾃﾞｰﾀ要求の回数が前記閾値を超えた場合に当該ﾃﾞｰﾀ要求を破棄し、前記ﾃﾞｰﾀ要求の回数が前記閾値を超えない場合に当該ﾃﾞｰﾀ要求を要求先のｻｰﾊﾞ計算機に転送する転送制御手段とを具備したことを特徴とするｻｰﾊﾞ計算機保護装置。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2002-288051 01.03.27 G06F13/00,351	**ﾈｯﾄﾜｰｸｼｽﾃﾑ、不正ｱｸｾｽ防御装置及び方法並びに不正ｱｸｾｽ防御ﾌﾟﾛｸﾞﾗﾑ**
	攻撃の抑止・予防の強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特開2003-241989 02.02.15 G06F11/00	**ｺﾝﾋﾟｭｰﾀｳｲﾙｽ発生検出装置、方法、およびﾌﾟﾛｸﾞﾗﾑ**
	パケット解析の高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2003-223375 （拒絶確定） 02.01.30 G06F13/00,351 〔被引用回数 1〕	**不正ｱｸｾｽ検知装置および不正ｱｸｾｽ検知方法**
脆弱性診断技術	システムの性能向上	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開平11-345205 （みなし取下） 98.06.03 G06F15/00,330 東芝ｺﾝﾋﾟｭｰﾀｴﾝｼﾞﾆｱﾘﾝｸﾞ	**ｺﾝﾋﾟｭｰﾀｼｽﾃﾑおよびそのｳｴｲｸｱｯﾌﾟ制御方法**
		回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特開2002-207624 01.01.12 G06F12/00,531	**ﾃﾞｰﾀﾊﾞｯｸｱｯﾌﾟｼｽﾃﾑ、ﾃﾞｰﾀﾊﾞｯｸｱｯﾌﾟ装置、ﾃﾞｰﾀﾊﾞｯｸｱｯﾌﾟ方法**
		回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特開2000-138703 98.10.30 H04L12/54	**情報提供装置及び記憶媒体**
	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 情報転送の手順 VPN設定情報	特開2000-022681 （みなし取下） 98.07.03 H04L9/14	**暗号化通信情報の管理ｼｽﾃﾑ及び記録媒体**
	攻撃パターンの高精度化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2004-318816 03.03.31 G06F1/00	**通信中継装置、通信中継方法及びﾌﾟﾛｸﾞﾗﾑ**

表2.4.4 東芝の技術要素別課題対応特許（6/14）

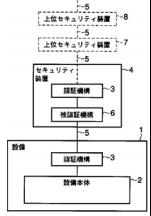
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
脆弱性診断技術	情報、個人の正当性向上	回路の改良 ｽｲｯﾁ回路の追加 ﾛｯｸ回路の追加	特許3600469 99.02.26 E05B49/00	**盗難防止機能付き設備及びｾｷｭﾘﾃｨ装置**  相手方に自己装置が正当なものであることを認証させる被認証機構を備えたｾｷｭﾘﾃｨ装置と、前記被認証機構との認証処理により前記ｾｷｭﾘﾃｨ装置が正当なものであるか否かを確認し、認証が成立した場合にのみ稼動許可信号を出力する認証機構と、当該稼動許可信号を受信した場合にのみ稼働状態となる設備本体とを備えた設備とからなることを特徴とする盗難防止機能付き設備。
	攻撃の抑止・予防の強化	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開2002-091916 00.09.18 G06F15/00,330 〔被引用回数 2〕	**不正ｱｸｾｽ通知ｼｽﾃﾑ**
プロキシ中継技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開2004-280401 03.03.14 G06F15/00,330	**ｺﾝﾃﾝﾂ配信ｼｽﾃﾑ、装置及びﾌﾟﾛｸﾞﾗﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2002-342144 01.05.21 G06F12/00,537	**ﾌｧｲﾙ共有ｼｽﾃﾑ、ﾌﾟﾛｸﾞﾗﾑおよびﾌｧｲﾙ受渡し方法**
	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2004-227121 03.01.21 G06F13/00,357	**ｻｰﾊﾞ装置、通信制御ｼｽﾃﾑ、通信方法及びｻｰﾊﾞﾌﾟﾛｸﾞﾗﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 遠隔制御ｺﾏﾝﾄﾞの抽出	特開平11-161321 （拒絶確定） 97.11.28 G05B23/02	**ﾌﾟﾗﾝﾄ監視装置**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 擬似、ﾀﾞﾐﾃﾞｰﾀの送信	特開平11-265347 （みなし取下） 98.01.16 G06F15/00,330 〔被引用回数 1〕	**分散ﾈｯﾄﾜｰｸｺﾝﾋﾟｭｰﾃｨﾝｸﾞｼｽﾃﾑ、及びこのｼｽﾃﾑに用いられる情報交換装置、情報交換方法、並びに情報交換方法のﾌﾟﾛｸﾞﾗﾑ情報を格納したｺﾝﾋﾟｭｰﾀ読取**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特開2003-202930 （みなし取下） 02.01.09 G06F1/00	**実行権限管理ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2000-354056 99.06.10 H04L12/46 〔被引用回数 5〕	**計算機ﾈｯﾄﾜｰｸｼｽﾃﾑおよびそのｱｸｾｽ制御方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開2003-345690 （みなし取下） 02.05.23 G06F13/00,510	**ﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ及びﾈｯﾄﾜｰｸ通信方法**

表2.4.4 東芝の技術要素別課題対応特許（7/14）

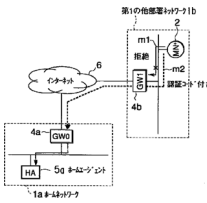
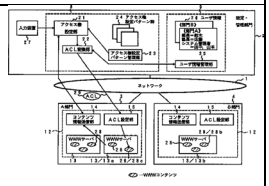
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
プロキシ中継技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 更新情報の付加	特開2002-118554 00.10.05 H04L12/22	**ｻｰﾊﾞ格納情報更新ｼｽﾃﾑ、ｻｰﾊﾞ格納情報更新方法およびｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ**
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開平11-073398 （みなし取下） 97.12.17 G06F15/16,370	**分散ﾈｯﾄﾜｰｸｺﾝﾋﾟｭｰﾃｨﾝｸﾞｼｽﾃﾑ、同ｼｽﾃﾑに用いられる情報交換装置、同ｼｽﾃﾑに用いられるｾｷｭﾘﾃｨ機能を有する情報交換方法、この方法を格納したｺ**
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-213339 02.12.27 G06F1/00	**ｿﾌﾄｳｴｱ無線機及びその制御方法**
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2004-274444 03.03.10 H04L12/66	**ｹﾞｰﾄｳｴｲｼｽﾃﾑ、情報伝送方法**
	経済性の向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 遠隔制御ｺﾏﾝﾄﾞの抽出	特開平11-161321 （拒絶確定） 97.11.28 G05B23/02	**ﾌﾟﾗﾝﾄ監視装置** 概要は技術要素「ﾌﾟﾛｷｼ中継」、課題「通信データの中継性能向上」の項参照
コンテンツフィルタリング技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特許3557056 96.10.25 H04L12/66 〔被引用回数 1〕	**ﾊﾟｹｯﾄ検査装置、移動計算機装置及びﾊﾟｹｯﾄ転送方法**  自装置の管理対象となる計算機以外の移動計算機から送信されたﾊﾟｹｯﾄに含まれる移動計算機識別情報に基づき、移動計算機から送信されたﾊﾟｹｯﾄのﾈｯﾄﾜｰｸ外への転送の可否を判定する判定手段と、この判定手段により転送を拒否すると判定した場合に、移動計算機に転送拒否を示すﾒｯｾｰｼﾞを返信する手段と、移動計算機から移動計算機識別情報を生成するための鍵情報を要求するﾒｯｾｰｼﾞを受信した場合に、移動計算機のﾕｰｻﾞに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する手段とを具備したことを特徴とするﾊﾟｹｯﾄ検査装置。
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ・ｸﾞﾙｰﾌﾟ	特許3576008 98.10.09 G06F15/00,330	**ｱｸｾｽ制御設定ｼｽﾃﾑ及び記憶媒体**  計算機上のﾘｿｰｽに対するｱｸｾｽ権の設定を行うためのｱｸｾｽ制御設定ｼｽﾃﾑにおいて、前記ﾘｿｰｽへのｱｸｾｽ許諾を受ける者及びそのｱｸｾｽ権内容を記述したｱｸｾｽ権設定ﾊﾟﾀｰﾝを1以上格納するｱｸｾｽ権設定ﾊﾟﾀｰﾝ格納部と、前記ｱｸｾｽ権の設定を行うために、前記ｱｸｾｽ権設定ﾊﾟﾀｰﾝの何れかを選択する選択手段とを備えたことを特徴とするｱｸｾｽ制御設定ｼｽﾃﾑ。
			特開2002-032255 00.07.17 G06F12/00,537	**ﾕｰｻﾞ情報管理ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体及びﾃﾞｰﾀﾍﾞｰｽ管理ｼｽﾃﾑのﾕｰｻﾞ情報管理装置**

表2.4.4 東芝の技術要素別課題対応特許（8/14）

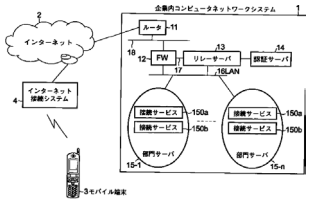
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特許3526435 00.06.08 G06F15/00,310	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**  内部ﾈｯﾄﾜｰｸと、前記内部ﾈｯﾄﾜｰｸと外部ﾈｯﾄﾜｰｸとを分離し、外部ﾈｯﾄﾜｰｸを介する端末からの内部ﾈｯﾄﾜｰｸへのｱｸｾｽの許可･不許可の制御を行うﾈｯﾄﾜｰｸ装置と、前記端末からのｱｸｾｽ要求に応じてｱｸｾｽされるｱﾌﾟﾘｹｰｼｮﾝを提供する複数のｻｰﾊﾞとを備えたｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸｼｽﾃﾑにおいて、前記端末から前記ﾈｯﾄﾜｰｸ装置を介して前記ｱﾌﾟﾘｹｰｼｮﾝへのｱｸｾｽ要求を受け取り、このｱｸｾｽ要求をしたﾕｰｻﾞの認証を行う認証手段と、前記認証手段により認証されたﾕｰｻﾞによる前記端末からのｱｸｾｽ要求が当該ﾕｰｻﾞに予め許されているｱﾌﾟﾘｹｰｼｮﾝへのｱｸｾｽ要求である場合に当該ｱｸｾｽ要求に対するｱｸｾｽを許可するｱｸｾｽ許可制御手段とを具備することを特徴とするｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸｼｽﾃﾑ。
			特開2003-216582 （みなし取下） 02.01.25 G06F15/00,330	**情報ﾈｯﾄﾜｰｸｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 時間、期限情報	特開2002-108729 00.09.29 G06F13/00,351	**ﾈｯﾄﾜｰｸ接続装置及び同装置に適用されるﾌｧｲｱｳｫｰﾙ制御ﾌﾟﾛｸﾞﾗﾑを記憶したｺﾝﾋﾟｭｰﾀ読み取り可能な記憶媒体**
			特開2004-274159 （拒絶確定） 03.03.05 H04N5/765	**情報機器及び資源制御方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2004-194212 02.12.13 H04N7/16	**受信装置、配信装置、受信方法、配信方法およびﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾍﾟｲﾛｰﾄﾞの暗号化	特開2004-282414 03.03.17 H04L12/56,100	**ｺﾝﾃﾝﾂ送信装置、ｺﾝﾃﾝﾂ受信装置、ｺﾝﾃﾝﾂ送信方法及びｺﾝﾃﾝﾂ受信方法**
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 特定情報の記憶、登録手順 ｱﾄﾞﾚｽの記憶	特開2004-282786 97.07.11 H04L12/46,100	**ﾙｰﾀ装置及びﾗﾍﾞﾙｽｲｯﾁﾝｸﾞﾊﾟｽの設定方法**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開2005-175689 03.12.09 H04L12/56	**通信装置、通信ｼｽﾃﾑおよび通信制御ﾌﾟﾛｸﾞﾗﾑ**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2000-259521 （特許3732672） 99.03.10 G06F13/00,351	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨﾙｰﾙ管理ｼｽﾃﾑ及びﾈｯﾄﾜｰｸｾｷｭﾘﾃｨﾙｰﾙ管理装置**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2002-232487 （特許3749129） 01.02.01 H04L12/58,100	**電子ﾒｰﾙｼｽﾃﾑ及び電子ﾒｰﾙ送信制御方法並びに中継装置**
			特開2003-224554 02.01.28 H04L9/08 〔被引用回数 1〕	**通信接続ｼｽﾃﾑ、方法、ﾌﾟﾛｸﾞﾗﾑ及び電子投票ｼｽﾃﾑ**

表2.4.4 東芝の技術要素別課題対応特許（9/14）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開2002-281093 01.03.19 H04L12/66 〔被引用回数 1〕	ﾈｯﾄﾜｰｸに適用するﾌﾟﾛﾌｧｲﾙ配信方法及びﾈｯﾄﾜｰｸｼｽﾃﾑ
			特開2005-072636 03.08.21 H04L12/66	通信ｼｽﾃﾑ、同通信ｼｽﾃﾑにおけるｾｷｭﾘﾃｨﾎﾟﾘｼｰの配布方法、ｻｰﾊﾞ装置、ならびにｾｷｭﾘﾃｨﾎﾟﾘｼｰの配布ﾌﾟﾛｸﾞﾗﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開2001-256136 00.03.09 G06F13/00,351 〔被引用回数 1〕	ﾈｯﾄﾜｰｸｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開2001-256123 （特許3684131） 00.03.10 G06F13/00,351	ｻｰﾊﾞｺﾝﾋﾟｭｰﾀ、電子商取引方法、及び記憶媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開平11-136274 （みなし取下） 97.10.28 H04L12/46	通信管理ｼｽﾃﾑ、通信管理装置、ﾉｰﾄﾞ及び通信管理ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
			特開平11-112514 97.10.06 H04L12/28	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ監視装置
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 ﾎﾟｰﾄ番号の登録	特開2005-086691 （特許3721182） 03.09.10 H04L12/66	不正ﾊﾟｹｯﾄ解析装置および不正ﾊﾟｹｯﾄ解析方法
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2004-180020 02.11.27 H04L12/66	通信中継装置、通信ｼｽﾃﾑ及び通信制御ﾌﾟﾛｸﾞﾗﾑ
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2002-261790 01.02.28 H04L12/46,100	ﾋﾟｰｸﾙ･ﾌﾟﾗｯﾄﾌｫｰﾑとしての車載ﾈｯﾄﾜｰｸｼｽﾃﾑ
	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開2005-108215 03.09.30 G06F13/00,353 東芝ﾃｯｸ	印刷装置のためのSNMPﾊﾟｹｯﾄﾌｨﾙﾀ処理
	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2001-186186 99.12.27 H04L12/56	ﾊﾟｹｯﾄ交換装置、ﾈｯﾄﾜｰｸｼｽﾃﾑ、およびﾊﾟｹｯﾄ交換方法
	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開2004-260295 03.02.24 H04L12/66	通信制御装置、通信制御方法、通信制御付ｻｰﾊﾞ装置、通信制御付ｻｰﾊﾞ装置による通信制御方法及び通信制御ﾌﾟﾛｸﾞﾗﾑ
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 IPv6の割付	特開2004-236096 03.01.31 H04L12/56	中継装置及び通信制御方法
			特開2004-289782 03.09.30 H04L12/66 東芝ﾃｯｸ	ｹﾞｰﾄｳｪｲ装置及びIPv6ﾈｯﾄﾜｰｸｼｽﾃﾑ

表2.4.4 東芝の技術要素別課題対応特許（10/14）

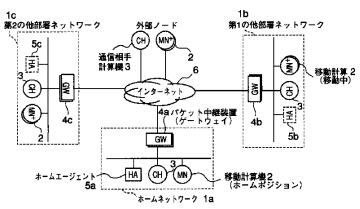
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
IPフィルタリング技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｱｸｾｽ制御ｻｰﾊﾞｰ配置	特開2002-312338 01.04.16 G06F15/177,674	**ｲﾝﾄﾗﾈｯﾄ業務ｻｰﾊﾞ、ｲﾝﾄﾗﾈｯﾄ業務ｼｽﾃﾑおよびﾌﾟﾛｸﾞﾗﾑ**
	攻撃の抑止・予防の強化	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2005-025252 03.06.30 G06F15/00,330 東芝ﾃｯｸ	**会員登録装置、会員登録方法、および会員登録ﾌﾟﾛｸﾞﾗﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開平07-093254 （みなし取下） 93.09.21 G06F15/00,330	**ﾈｯﾄﾜｰｸｼｽﾃﾑの悪用防止方法及び装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平11-167533 （みなし取下） 97.12.03 G06F13/00,351 東芝情報ｼｽﾃﾑ	**電子ﾒｰﾙﾌｧｲｱｳｫｰﾙ装置**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2004-320330 03.04.15 H04M3/00	**IP電話通信における不正ｱｸｾｽ防止ｼｽﾃﾑおよび方法**
	経済性の向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2004-320330 03.04.15 H04M3/00	**IP電話通信における不正ｱｸｾｽ防止ｼｽﾃﾑおよび方法** 概要は技術要素「IPﾌｨﾙﾀﾘﾝｸﾞ」、課題「攻撃の抑止・予防の強化」の項参照
ルーティング制御技術	侵入防御の性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 多層ﾌﾟﾛﾄｺﾙの処理	特開2004-201288 02.11.19 H04L9/32	**ﾈｯﾄﾜｰｸ通信のためのﾚｲﾔ間の高速認証または再認証**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特許3472098 97.09.08 H04L12/46	**移動計算機装置、中継装置及びﾃﾞｰﾀ転送方法**  装置が移動前に属していたﾈｯﾄﾜｰｸから、ｾｷｭﾘﾃｨ保持関係を保って通信できる通信相手のｱﾄﾞﾚｽの範囲を示すｱﾄﾞﾚｽ範囲情報を保持する記憶手段と、自装置が現在位置する移動先ﾈｯﾄﾜｰｸから、自装置の属していたﾈｯﾄﾜｰｸ内の宛先計算機に、自装置の属していたﾈｯﾄﾜｰｸの入口に設置された第1の中継装置に対する折衝情報を付加したﾃﾞｰﾀを送信する手段と、宛先計算機に至る経路途中の第2の中継装置から、送信ﾃﾞｰﾀに対する通過拒否ﾒｯｾｰｼﾞが返信された場合、第2の中継装置のｱﾄﾞﾚｽ情報と、記憶手段に保持されるｱﾄﾞﾚｽ範囲情報とを照合する手段と、この照合の結果、第2の中継装置のｱﾄﾞﾚｽ情報がｱﾄﾞﾚｽ範囲情報に含まれるものではない場合は、通過拒否された送信ﾃﾞｰﾀに付加した折衝情報の前に、第2の中継装置に対する折衝情報を付加し、第2の中継装置のｱﾄﾞﾚｽ情報がｱﾄﾞﾚｽ範囲情報に含まれるものである場合は、通過拒否された送信ﾃﾞｰﾀに付加した折衝情報の後に、第2の中継装置に対する折衝情報を付加して、ﾃﾞｰﾀを再度送信する手段とを備えたことを特徴とする移動計算機装置。

表2.4.4 東芝の技術要素別課題対応特許（11/14）

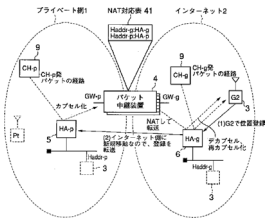
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
ルーティング制御技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開平09-214556 （特許3688830） 95.11.30 H04L12/56 〔被引用回数 4〕	**ﾊﾟｹｯﾄ転送方法及びﾊﾟｹｯﾄ処理装置**
	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 ｱｸｾｽ許可情報	特開2003-044299 01.07.30 G06F9/46,360	**情報処理方法および情報処理装置およびﾌﾟﾛｸﾞﾗﾑ**
	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特許3581251 98.06.16 H04L12/56	**通信ｼｽﾃﾑ、ﾃﾞｰﾀﾊﾟｹｯﾄ転送方法、ﾙｰﾀ装置及びﾊﾟｹｯﾄ中継装置**  第1のﾈｯﾄﾜｰｸと第2のﾈｯﾄﾜｰｸとの境界に設置されたﾊﾟｹｯﾄ中継装置と、第1のﾈｯﾄﾜｰｸに設置された第1のﾙｰﾀ装置と、第2のﾈｯﾄﾜｰｸに設置された第2のﾙｰﾀ装置とを備え、ﾊﾟｹｯﾄ中継装置は、第1のﾈｯﾄﾜｰｸ側に第1のｲﾝﾀﾌｪｰｽを持つとともに、第2のﾈｯﾄﾜｰｸ側に第2のｲﾝﾀﾌｪｰｽを持つものであり、第1のﾙｰﾀ装置および第2のﾙｰﾀ装置は、それぞれ、自装置が設置されているﾈｯﾄﾜｰｸをﾎｰﾑﾈｯﾄﾜｰｸとするﾓﾊﾞｲﾙ端末に対して割り当てられた、ﾓﾊﾞｲﾙ端末を識別するためのﾎｰﾑｱﾄﾞﾚｽの情報を管理するための第1の管理手段と、ﾓﾊﾞｲﾙ端末の現在位置を識別するため、ﾓﾊﾞｲﾙ端末から動的に通知される現在位置ｱﾄﾞﾚｽの情報を管理するための第2の管理手段と、第1の管理手段に格納されたﾓﾊﾞｲﾙ端末のﾎｰﾑｱﾄﾞﾚｽ宛に転送されてきたﾃﾞｰﾀﾊﾟｹｯﾄを代理受信し、ﾃﾞｰﾀﾊﾟｹｯﾄを第2の管理手段に格納された該ﾓﾊﾞｲﾙ端末の現在位置ｱﾄﾞﾚｽに応じてｶﾌﾟｾﾙ化して転送するための転送手段とを備えるものであることを特徴とする通信ｼｽﾃﾑ。
	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開平09-214543 （みなし取下） 96.02.05 H04L12/46 〔被引用回数 1〕	**通信経路制御方法および通信経路制御装置**
	侵入検出の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開平10-276241 （みなし取下） 97.03.28 H04L29/08	**ﾃﾞｰﾀ通信方法及びそのｼｽﾃﾑ**
	経済性の向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開平09-214543 （みなし取下） 96.02.05 H04L12/46 〔被引用回数 1〕	**通信経路制御方法および通信経路制御装置** 概要は技術要素「ﾙｰﾃｨﾝｸﾞ制御」、課題「中継するデータの機密性向上」の項参照
IPアドレス変換技術	デバイスの正当性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2004-222181 （特許3742390） 03.01.17 H04L12/46	**HTTPﾄﾝﾈﾘﾝｸﾞｻｰﾊﾞを用いた通信方法および通信装置、ﾌﾟﾛｸﾞﾗﾑ**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 情報の付加	特開2004-166002 02.11.13 H04L12/66	**通信装置、境界ﾙｰﾀ装置、ｻｰﾊﾞ装置、通信ｼｽﾃﾑ、通信方法、ﾙｰﾃｨﾝｸﾞ方法、通信ﾌﾟﾛｸﾞﾗﾑ及びﾙｰﾃｨﾝｸﾞﾌﾟﾛｸﾞﾗﾑ**

表2.4.4 東芝の技術要素別課題対応特許（12/14）

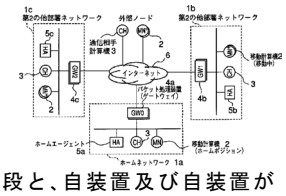
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPアドレス変換技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2000-196616 98.12.28 H04L12/28 〔被引用回数 1〕	**情報通信ﾈｯﾄﾜｰｸを用いた暗号化方式**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2004-112041 02.09.13 H04L12/22	**通信装置及びﾌﾟﾛｸﾞﾗﾑ並びに方法**
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2003-037591 01.07.25 H04L9/32	**中継機器及び方法**
	侵入検出の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2002-063084 （拒絶確定） 00.08.21 G06F13/00,351 〔被引用回数 8〕	**ﾊﾟｹｯﾄ転送装置、ﾊﾟｹｯﾄ転送方法、及びそのﾌﾟﾛｸﾞﾗﾑが格納された記憶媒体**
ホスト認証技術	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 要求情報の記憶	特開2001-118038 （拒絶確定） 99.10.18 G06K17/00	**計算装置及び記録媒体**
		各種の処理手順改良 特定情報の取得手順 ID情報の取得	特開平11-175476 （みなし取下） 97.12.16 G06F15/00,330	**ｾｷｭﾘﾃｨﾁｪｯｸ方法ならびに認証ｼｽﾃﾑ、及び同方法のﾌﾟﾛｸﾞﾗﾑが記録される記録媒体**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開平11-085687 97.09.05 G06F15/00,310	**移動計算機装置、読出制御方法及びﾒｯｾｰｼﾞ送出制御方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特許3651721 96.11.01 H04L9/32	**移動計算機装置、ﾊﾟｹｯﾄ処理装置及び通信制御方法**  自装置が、自装置の移動位置情報を管理し自装置宛のﾊﾟｹｯﾄを自装置の現在位置に転送する手段を有する移動計算機管理装置の設置されたﾈｯﾄﾜｰｸの内部に位置するか外に位置するかを認識する第1の認識手段と、自装置及び自装置が通信相手とする計算機の少なくとも一方につき、その送信するﾊﾟｹｯﾄを暗号化認証処理対象とするﾊﾟｹｯﾄ処理装置が存在するか否かを認識する第2の認識手段と、これら第1及び第2の認識手段の認識結果に基づき、送信すべきﾊﾟｹｯﾄの暗号化認証処理を含む所定の通信処理を行う手段とを具備することを特徴とする移動計算機装置。
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開平11-345214 （みなし取下） 98.06.02 G06F15/16,380	**分散ﾈｯﾄﾜｰｸｺﾝﾋﾟｭｰﾃｨﾝｸﾞｼｽﾃﾑ、同ｼｽﾃﾑに於ける負荷分散/ｾｷｭﾘﾃｨ保証方法、及び記憶媒体**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平07-038599 （みなし取下） 93.07.20 H04L12/46 〔被引用回数 3〕	**LAN間接続装置**

表2.4.4 東芝の技術要素別課題対応特許（13/14）

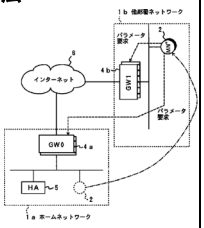
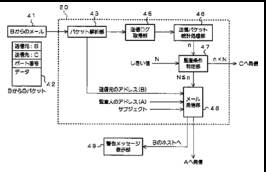
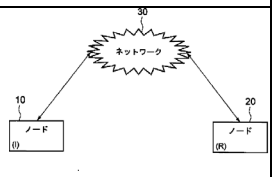
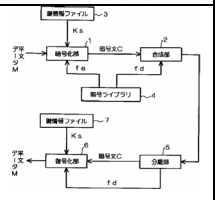
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
ホスト認証技術	デバイスの正当性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2003-091503 01.09.14 G06F15/00,330	**ﾎﾟｰﾄｱｸｾｽを利用した認証方法及び同方法を適用するｻｰﾊﾞ機器**
	攻撃パターンの高精度化	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 識別子情報の照合	特開2004-151886 02.10.29 G06F13/00,351	**ｾｷｭｱ通信ｼｽﾃﾑ､方法及びﾌﾟﾛｸﾞﾗﾑ**
トンネリング技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特許3492865 96.10.16 H04L9/12	**移動計算機装置及びﾊﾟｹｯﾄ暗号化認証方法**  自装置に入出力するﾊﾟｹｯﾄを暗号化認証処理する､ｵﾝ･ｵﾌ可能なﾊﾟｹｯﾄ暗号化認証手段と､自装置が現在位置するﾈｯﾄﾜｰｸに､このﾈｯﾄﾜｰｸに位置する計算機と他のﾈｯﾄﾜｰｸに位置する計算機との間で転送されるﾊﾟｹｯﾄを所定のｾｷｭﾘﾃｨﾊﾟﾗﾒｰﾀに基づいて暗号化認証処理して中継するﾊﾟｹｯﾄ処理装置が存在する場合に､このﾊﾟｹｯﾄ処理装置が持つｾｷｭﾘﾃｨﾊﾟﾗﾒｰﾀと､自装置に適したｾｷｭﾘﾃｨﾊﾟﾗﾒｰﾀとを比較し､この比較結果に基づいて前記ﾊﾟｹｯﾄ処理装置及び前記ﾊﾟｹｯﾄ暗号化認証処理手段の少なくとも一方を選択して､暗号化認証処理を行わせる制御手段とを具備したことを特徴とする移動計算機装置。
	システムの性能向上	各種の処理手順改良 特定情報の記憶､登録手順 鍵情報の記憶	特許3420002 96.09.13 H04L12/66 〔被引用回数 1〕	**通信監査装置及び通信監査方法**  送信元と送信先の組をｷｰとして送信履歴を収集する手段と､収集された送信履歴から得られる所定の統計量が予め定められた所定の条件を満たすものとなった送信元と送信先の組を持つ情報が送信されようとする場合､情報を該送信先に転送せずに､予め定められた特定の宛先に転送する手段とを備えたことを特徴とする通信監査装置。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開2004-151964 02.10.30 G06F13/00,353	**ﾄﾝﾈﾘﾝｸﾞ通信ｼｽﾃﾑ､HTTPﾄﾝﾈﾘﾝｸﾞｻｰﾊﾞ､HTTP通信ﾗｲﾌﾞﾗﾘ､ﾄﾝﾈﾘﾝｸﾞ通信方法及びﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平11-110353 （みなし取下） 97.09.30 G06F15/00,330	**情報交換用ｸｰﾎﾟﾝ､情報交換方法および情報交換ｼｽﾃﾑ**
		情報の送信、転送､分岐の手順改良 特定情報の通知､送信手順 鍵情報の送信	特開2004-166238 02.08.30 H04L9/32	**安全なﾃﾞｰﾀ通信ﾘﾝｸのための方法と装置**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開平11-122262 97.10.17 H04L12/28	**分散ﾈｯﾄﾜｰｸｺﾝﾋﾟｭｰﾃｨﾝｸﾞｼｽﾃﾑ､情報交換装置､情報交換方法､及び記憶媒体**

表2.4.4 東芝の技術要素別課題対応特許（14/14）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開平11-161618 97.09.05 G06F15/16,620	**移動計算機管理装置、移動計算機装置及び移動計算機登録方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特許3629237 01.12.28 H04L12/56	**ﾉｰﾄﾞ装置及び通信制御方法**  ﾊﾟｹｯﾄ通信における宛先ｱﾄﾞﾚｽ及び宛先ｱﾄﾞﾚｽについて一意の識別情報並びにﾊﾟｹｯﾄ通信で用いる暗号処理に関するﾊﾟﾗﾒｰﾀ情報を含むｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝ情報を交換するための交換手続きを行う交換手続き処理手段と、交換手続きにより交換されたｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝ情報を記憶する記憶手段と、記憶手段に記憶された各々のｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝ情報について、宛先ｱﾄﾞﾚｽ及び識別情報並びにｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝ情報の有効期限に関する情報を含む管理情報を、所定の不揮発性のﾒﾃﾞｨｱに記憶して管理する管理手段と、所定のｾｷｭﾘﾃｨ･ﾌﾟﾛﾄｺﾙに従う自ﾉｰﾄﾞ宛の受信ﾊﾟｹｯﾄのﾍｯﾀﾞに含まれる識別情報及び自ﾉｰﾄﾞを示す宛先ｱﾄﾞﾚｽにより特定されるｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝ情報が記憶手段に有効に存在せず、かつ、ｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝ情報に対応する管理情報が所定の不揮発性のﾒﾃﾞｨｱに有効に存在する場合に、その旨を通信相手となるﾉｰﾄﾞへ通知するために、宛先ｱﾄﾞﾚｽ及び識別情報を含む通知ﾒｯｾｰｼﾞを通信相手となるﾉｰﾄﾞへ送信するﾊﾟｹｯﾄ処理手段とを備えたことを特徴とするﾉｰﾄﾞ装置。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2001-333110 （特許3730480） 00.05.23 H04L12/66 〔被引用回数 1〕	**ｹﾞｰﾄｳｪｲ装置**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2004-178486 02.11.29 G06F15/00,330	**監視ｻｰﾊﾞおよび監視方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 鍵情報	特開2002-149569 00.11.07 G06F13/00,610	**暗号通信ｼｽﾃﾑ、暗号通信方法およびｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｾｷｭﾘﾃｨｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特許3537959 96.07.26 H04L9/14 岡本 栄司	**情報復号化装置**  情報の送り手により選択された複数の暗号ｱﾙｺﾞﾘｽﾞﾑのうちの1つと、鍵情報を用いて平文情報を暗号化して暗号文を生成し、この暗号文と選択された暗号ｱﾙｺﾞﾘｽﾞﾑに対応する復号化ﾌﾟﾛｸﾞﾗﾑを合成し、情報の受け手側で合成された暗号文と復号化ﾌﾟﾛｸﾞﾗﾑをﾈｯﾄﾜｰｸあるいは記録媒体を介して受け取ると、これらを分離し、暗号文を復号化ﾌﾟﾛｸﾞﾗﾑと鍵情報を用いて平文情報に復号することを特徴とする情報暗号化復号化方法。
	攻撃の抑止・予防の強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開平10-161935 96.09.19 G06F12/14,320	**ｾｷｭﾘﾃｨｼｽﾃﾑ及びｾｷｭﾘﾃｨ方法**

2.5 富士通

2.5.1 企業の概要

商号	富士通　株式会社
本社所在地	〒105-7123　東京都港区東新橋1-5-2　汐留シティセンター
設立年	1935年（昭和10年）
資本金	3,246億25百万円（2005年3月末）
従業員数	33,792名（2005年3月末）（連結：150,970名）
事業内容	通信システム、情報処理システム、電子デバイス等の製造・販売およびこれらに関するサービスの提供

トップページのサポート情報内にセキュリティ情報があり、各種セキュリティ情報の紹介を行っているページにリンクできる。

（出典：http://jp.fujitsu.com/support/security/）

2.5.2 製品例

ソリューションの中でセキュリティ製品とサービスを紹介している。表2.5.2に、製品例とその概要を示す。

表2.5.2 富士通の不正アクセス侵入検知防御技術に関連する製品例(1/2)

製品名	概要・特徴
ファイアウォール VPN-1/FireWALL-1	導入および管理が容易で、ファイアウォールやVPN機能を標準装備し、ネットワーク層ならびにアプリケーション層に対する攻撃の防御と、マルチサイトの集中管理を可能にする。
ファイアウォール IPCOM　Sシリーズ	IPネットワークに必要な機能を一台に集約した。負荷分散、帯域制御、ファイアウォール、VPN/IPsec・SSLを機能に持つサーバ。
ファイアウォール Interstage Security Director	インターネットでの企業間取引や顧客への情報公開を行うサーバに対する強固なセキュリティを確保する機能を提供し、インターネットビジネスの基盤に不可欠な安定したネットワーク環境を実現。 ファイアウォール機能に加え、SSL認証、モバイルのアクセス制御にも対応。
ファイアウォール NOKIA IPシリーズ	ノキアのプラットフォームは、チェック・ポイント社の業界をリードするファイアウォールとVPNのソフトウェアを、ハイ・パフォーマンスで導入の簡易なセキュリティ装置に統合。 リモート設定および管理機能により、ネッワークの規模に関係なく、容易な設定や管理が可能。
ファイアウォール NetShelter/FWシリーズ	ブロードバンド、VPN、VoIPなど最新のネットワーク技術に対応したオールインワンタイプのセキュリティ専用装置。 既存のネットワークに低コストで導入することができ、用途や事業所規模に応じて、最適で無駄のないセキュリティ環境を構築。
侵入検知 DefensePro	ファイアウォールでは制御出来ない高レイヤでの不正アクセスを、3Gのスループットを確保しつつ防御。 これまで性能的に導入が難しかったキャリア・ISPなどへも適用が可能。
侵入検知 PacketBlackHole	ネットワークを流れるすべてのパケットを完全に記録することで、いつ、誰が、どのようなメールを誰に出したか、誰がどういうWebページをいつ見たか、何か不正なアクセスはあったか、などのネットワークの運用状況を管理、監視するソリューション。

表2.5.2 富士通の不正アクセス侵入検知防御技術に関連する製品例(2/2)

製品名	概要・特徴
侵入検知 RealSecure	国内シェア No.1(2002 富士キメラ総研調べ)を誇り、多くの企業で導入実績があるISS社の不正侵入検知・防御ソリューション。
脆弱性診断 InternetScanner	ネットワーク上の脆弱性を検出し、その対処方法をアドバイスします。侵入者が不正侵入に利用するオペレーティングシステムやアプリケーションのセキュリティホール、あるいは脆弱な構成を検出して報告。

(出典：http://segroup.fujitsu.com/secure/solution/sol4.html)

2.5.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

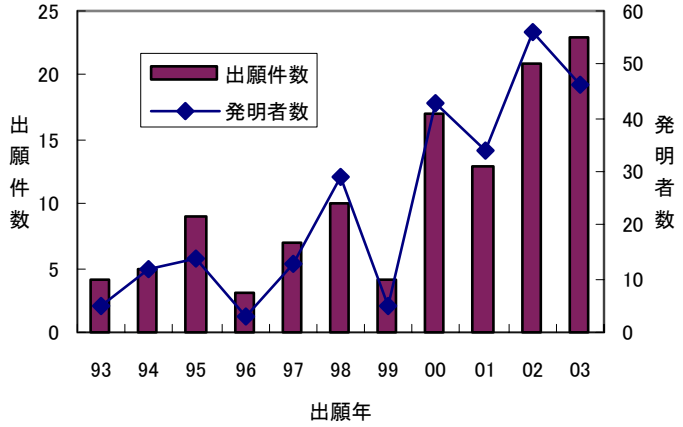
神奈川県横浜市港北区新横浜3丁目9番18号富士通内

神奈川県川崎市中原区上小田中1015番地 富士通株式会社内

アメリカ合衆国メリーランド州シルヴァースプリング

図2.5.3に、富士通の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の４年間の平均は、出願件数が17件、発明者が40人前後で安定している。

図2.5.3 富士通の不正アクセス侵入検知防御技術に関する出願件数と発明者数



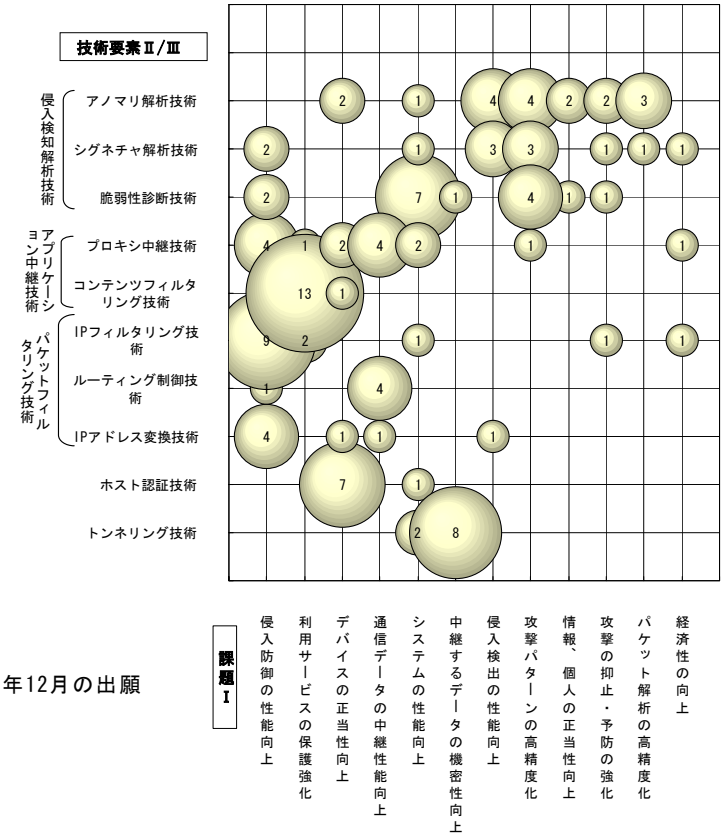
2.5.4 技術開発課題対応特許の概要

図2.5.4-1に、富士通の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.5.4-2に、富士通の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術が最も多く出願され、次いで脆弱性診断技術とホスト認証技術に関する出願が多い。これらの出願のうち、最も多い課題は、「侵入防御の性能向上」であり、次いで多い課題は「利用サービスの保護強化」である。

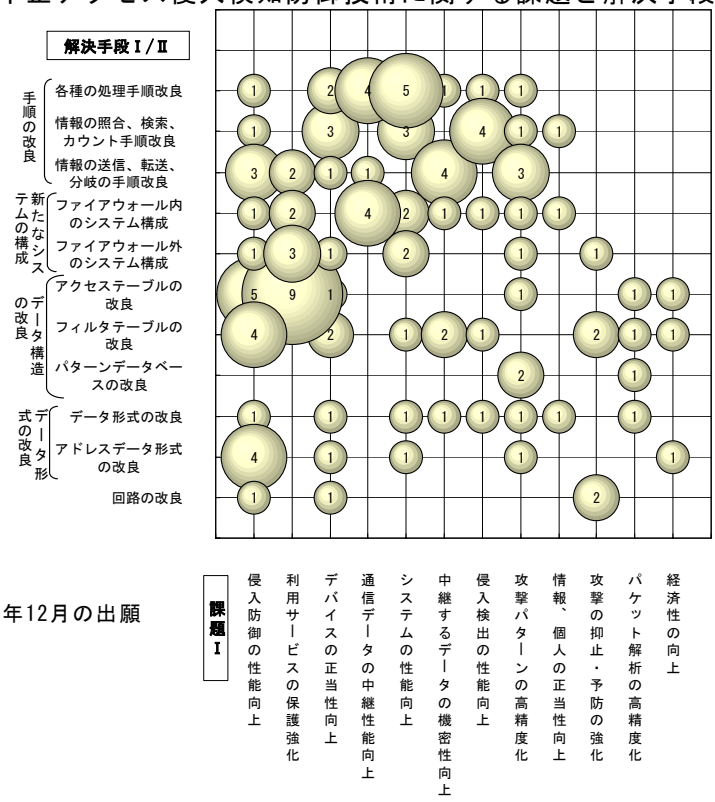
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。次いで「侵入防御の性能向上」の課題に対しては、「アクセステーブルの改良」で多く対応し、さらに「システムの性能向上」に対しては、「各種の処理手順改良」でも多く対応している。

図2.5.4-1 富士通の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.5.4-2富士通の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.5.4 富士通の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は116件で、そのうち16件が登録特許である。なお、表2.5.4では図2.5.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.5.4 富士通の技術要素別課題対応特許（1/14）

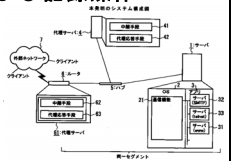
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平11-031129 （特許3717135） 97.07.14 G06F15/00,330 〔被引用回数 2〕	複数WWWｻｰﾊﾞ連携ｼｽﾃﾑ、複数WWWｻｰﾊﾞ連携方法、および記録媒体
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2000-148276 98.11.05 G06F1/00,370 〔被引用回数 3〕	ｾｷｭﾘﾃｨ監視装置，ｾｷｭﾘﾃｨ監視方法およびｾｷｭﾘﾃｨ監視用ﾌﾟﾛｸﾞﾗﾑ記録媒体
	システムの性能向上	各種の処理手順改良 各種処理の実行手順 特定処理の実行	特開2003-263413 02.03.07 G06F15/00,330	ﾃﾞｰﾀｻｰﾊﾞへの不正侵入対処方法、及びﾌﾟﾛｸﾞﾗﾑ
	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開2002-342279 01.03.13 G06F15/00,330 〔被引用回数 2〕	ﾌｨﾙﾀﾘﾝｸﾞ装置、ﾌｨﾙﾀﾘﾝｸﾞ方法およびこの方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑ
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開2004-280724 03.03.18 G06F13/00,351	不正ｱｸｾｽ対処ｼｽﾃﾑ、及び不正ｱｸｾｽ対処処理ﾌﾟﾛｸﾞﾗﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 質問形式での追加、学習	特開2004-362075 03.06.02 G06F15/00,320	ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ及びその制御方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2004-096246 02.08.29 H04L12/56,400	ﾃﾞｰﾀ伝送方法、ﾃﾞｰﾀ伝送ｼｽﾃﾑ及びﾃﾞｰﾀ伝送装置
	攻撃パターンの高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾄﾗﾌｨｯｸ	特開2005-025679 03.07.03 G06F11/00	ｳｲﾙｽ隔離ｼｽﾃﾑ
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 擬似、ﾀﾞﾐﾃﾞｰﾀの送信	特開2002-208986 01.01.12 H04L29/08 〔被引用回数 1〕	通信装置、通信方法、および媒体
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特許3648211 02.03.28 H04L12/56	ﾊﾟｹｯﾄ中継ﾌﾟﾛｸﾞﾗﾑ、ﾊﾟｹｯﾄ中継装置および記録媒体  中継ｻｰﾊﾞに、ｻｰﾊﾞからの確立要求/確立要求の確認応答ﾊﾟｹｯﾄを受信するｽﾃｯﾌﾟと、確立要求/確立要求の確認応答ﾊﾟｹｯﾄの受信に基づき、外部ﾈｯﾄﾜｰｸに該確立要求/確立要求の確認応答ﾊﾟｹｯﾄを中継すると共に、ｻｰﾊﾞに該確立要求/確立要求の確認応答ﾊﾟｹｯﾄに対応する確認応答ﾊﾟｹｯﾄを返信するｽﾃｯﾌﾟとを動作させることを特徴とするﾊﾟｹｯﾄ中継ﾌﾟﾛｸﾞﾗﾑ。

表2.5.4 富士通の技術要素別課題対応特許（2/14）

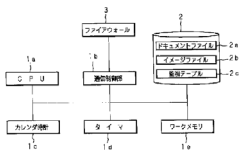
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
アノマリ解析技術	攻撃パターンの高精度化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特開2003-271474 02.03.13 G06F13/00,351	**外部ﾈｯﾄﾜｰｸからの不正侵入防止方法､およびﾌﾟﾛｸﾞﾗﾑ**
	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾊﾞｯｸｱｯﾌﾟｻｰﾊﾞｰの配置	特許3484523 97.11.19 G06F15/00,330 〔被引用回数 1〕	**改竄修正装置，及び改竄修正方法** ﾈｯﾄﾜｰｸ上の所定のﾛｹｰｼｮﾝで開示されているｺﾝﾃﾝﾂを定期的に入手して、その都度前記ｺﾝﾃﾝﾂの内容が改竄されているか否かを判定し、改竄されたと判定したとき、元の内容に修正することを特徴とする改竄修正方法。 
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2004-110197 02.09.13 G06F12/14,310	**ｾﾝﾀ･ｼｽﾃﾑにおける情報処理方法及びｱｸｾｽ権限管理方法**
	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開2003-288282 02.03.28 G06F13/00,351	**不正ｱｸｾｽ防止ﾌﾟﾛｸﾞﾗﾑ**
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2004-350090 03.05.23 H04L12/66	**ｲﾝﾀﾌｪｰｽ装置**
	パケット解析の高精度化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開2002-251374 00.12.20 G06F15/00,330	**情報管理ｼｽﾃﾑ､情報管理方法､およびその方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑ､並びにそのﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 不正ｱｸｾｽ履歴情報の蓄積	特開2004-007170 02.05.31 H04L12/66	**ﾈｯﾄﾜｰｸ中継装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2005-109715 03.09.29 H04L12/66	**ﾃﾞｰﾀ中継装置およびﾃﾞｰﾀ中継方法**
シグネチャ解析技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2003-263376 02.03.08 G06F13/00,351	**ﾌｧｲｱｳｫｰﾙのｾｷｭﾘﾃｨ管理方法及びその管理ﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾎﾟﾘｼｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特開2002-342278 01.05.22 G06F15/00,330	**情報処理装置およびｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ**
	システムの性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の停止、取消し	特開2001-016273 99.06.29 H04L12/66	**自動機監視装置､自動機､及び記録媒体**
	侵入検出の性能向上	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2004-302956 03.03.31 G06F15/00,330	**不正ｱｸｾｽ対処ｼｽﾃﾑ､及び不正ｱｸｾｽ対処処理ﾌﾟﾛｸﾞﾗﾑ**

表2.5.4 富士通の技術要素別課題対応特許（3/14）

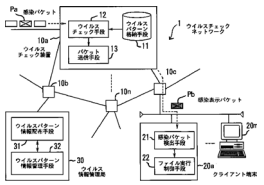
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
シグネチャ解析技術	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2003-223365 02.01.31 G06F12/14,310	ﾃﾞｰﾀ管理機構及びﾃﾞｰﾀ管理機構を有する装置又はｶｰﾄﾞ
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2002-269040 01.03.12 G06F15/00,330	不正ｸﾗｲｱﾝﾄ判別装置
	攻撃パターンの高精度化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2005-117656 03.10.03 H04Q7/38	自己組織化ﾏﾙﾁﾎｯﾌﾟ無線ｱｸｾｽﾈｯﾄﾜｰｸ用の装置、方法及び媒体
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ﾊﾟﾀｰﾝの廃棄	特開2004-289298 03.03.19 H04L12/66	ﾃﾞｰﾀ処理装置
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾘﾀﾞｲﾚｸﾄｱﾄﾞﾚｽの割付	特開2004-334455 03.05.07 G06F15/00,330	ｻｰﾊﾞ装置
	攻撃の抑止・予防の強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特許3597686 97.12.02 G06F11/00 〔被引用回数 2〕	ｳｨﾙｽﾁｪｯｸﾈｯﾄﾜｰｸｼｽﾃﾑ及びｳｨﾙｽﾁｪｯｸ装置  ｳｨﾙｽﾁｪｯｸを行って、ｳｨﾙｽ侵入を防止するｳｨﾙｽﾁｪｯｸﾈｯﾄﾜｰｸにおいて、ｳｨﾙｽﾊﾟﾀｰﾝを格納するｳｨﾙｽﾊﾟﾀｰﾝ格納手段と、受信したﾊﾟｹｯﾄを前記ｳｨﾙｽﾊﾟﾀｰﾝにもとづいて、ｳｨﾙｽに感染している感染ﾊﾟｹｯﾄか否かの前記ｳｨﾙｽﾁｪｯｸをﾈｯﾄﾜｰｸ側で行うｳｨﾙｽﾁｪｯｸ手段と、前記感染ﾊﾟｹｯﾄを検知した場合は、感染を示すﾊﾟｹｯﾄ内のﾋﾞｯﾄを立てて感染表示ﾊﾟｹｯﾄとして送信するﾊﾟｹｯﾄ送信手段と、から構成される複数のｳｨﾙｽﾁｪｯｸ装置と、前記ﾋﾞｯﾄにもとづいて、前記感染ﾊﾟｹｯﾄを検出する感染ﾊﾟｹｯﾄ検出手段と、前記感染ﾊﾟｹｯﾄに対応するﾌｧｲﾙを実行不可にするﾌｧｲﾙ実行制御手段と、から構成されるｸﾗｲｱﾝﾄ端末と、ｳｨﾙｽﾊﾟﾀｰﾝ情報をﾏﾙﾁｷｬｽﾄで前記ｳｨﾙｽﾁｪｯｸ装置に配布するｳｨﾙｽﾊﾟﾀｰﾝ情報配布手段と、前記ｳｨﾙｽﾊﾟﾀｰﾝ情報を一元管理するｳｨﾙｽﾊﾟﾀｰﾝ情報管理手段と、から構成されるｳｨﾙｽ情報管理局と、を有することを特徴とするｳｨﾙｽﾁｪｯｸﾈｯﾄﾜｰｸ。
	パケット解析の高精度化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開2005-136526 03.10.28 H04L12/66	不正ｱｸｾｽ検知装置、不正ｱｸｾｽ検知方法および不正ｱｸｾｽ検知ﾌﾟﾛｸﾞﾗﾑ
	経済性の向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の停止、取消し	特開2001-016273 99.06.29 H04L12/66	自動機監視装置、自動機、及び記録媒体 概要は技術要素「ｼｸﾞﾈﾁｬ解析」、課題「ｼｽﾃﾑの性能向上」の項参照

表2.5.4 富士通の技術要素別課題対応特許（4/14）

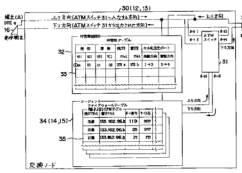
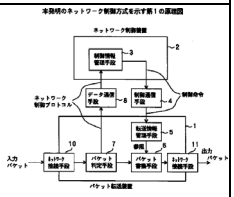
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
脆弱性診断技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2002-261839 01.02.28 H04L12/66	**通信ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ及びそのﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2003-288275 02.03.28 G06F12/14,320	**情報ｾｷｭﾘﾃｨ管理方法、この方法を実行するﾌﾟﾛｸﾞﾗﾑ、及び情報ｾｷｭﾘﾃｨ管理装置**
	システムの性能向上	各種の処理手順改良 特定情報の記憶、登録手順 要求情報の記憶	特開2000-267958 99.03.18 G06F13/00,351	**中継装置および記録媒体**
		各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特許3591753 97.01.30 H04L12/56 〔被引用回数 4〕	**ﾌｧｲｱｳｫｰﾙ方式およびその方法**  固定長ﾊﾟｹｯﾄを交換するとともに、受信した固定長ﾊﾟｹｯﾄのなかから第2のﾌﾟﾛﾄｺﾙによる第1の端末から第2の端末へのｱｸｾｽ要求を含んだ固定長ﾊﾟｹｯﾄを抽出する交換ﾉｰﾄﾞと、ﾈｯﾄﾜｰｸ内に設けられ、交換ﾉｰﾄﾞによって抽出された固定長ﾊﾟｹｯﾄに格納されている情報に基づいて第2の端末へのｱｸｾｽを許容するか否かを判断するｴｰｼﾞｪﾝﾄﾕﾆｯﾄと、を有するﾌｧｲｱｳｫｰﾙ方式。
		各種の処理手順改良 各種処理の実行手順 並列処理の実行	特許3542103 98.09.08 H04L12/56,100	**ﾈｯﾄﾜｰｸ制御方式**  ﾈｯﾄﾜｰｸの制御を行うﾈｯﾄﾜｰｸ制御方式において、ﾈｯﾄﾜｰｸ制御情報を含む制御ﾊﾟｹｯﾄを処理してﾈｯﾄﾜｰｸ制御情報の管理と伝播を行う制御情報管理手段を備えた一台または複数のﾈｯﾄﾜｰｸ制御装置と、ﾈｯﾄﾜｰｸ制御装置の制御情報管理手段からの制御情報を格納した転送情報管理手段及びこの転送情報管理手段に格納した制御情報に従って転送ﾊﾟｹｯﾄの内容を書き換えるﾊﾟｹｯﾄ書換手段を備えた一台または複数のﾊﾟｹｯﾄ転送装置と、を備えるとともに、送信されてくるﾊﾟｹｯﾄがﾈｯﾄﾜｰｸ制御情報を含む制御ﾊﾟｹｯﾄであるかそれ以外の転送ﾊﾟｹｯﾄであるか否かを判定するﾊﾟｹｯﾄ判定手段を備え、このﾊﾟｹｯﾄ判定手段で制御ﾊﾟｹｯﾄであると判定されたﾊﾟｹｯﾄを前記ﾈｯﾄﾜｰｸ制御装置に送り制御情報管理手段で処理し、制御ﾊﾟｹｯﾄ以外の転送ﾊﾟｹｯﾄであると判定されたﾊﾟｹｯﾄをﾊﾟｹｯﾄ転送装置のﾊﾟｹｯﾄ書換手段で書き換えることを特徴とするﾈｯﾄﾜｰｸ制御方式。
		各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特開平11-259423 98.03.10 G06F15/00,330	**伝送装置のｾｷｭﾘﾃｨｼｽﾃﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間・期間情報	特開平08-249282 （みなし取下） 95.03.15 G06F15/00,330	**不正ｱｸｾｽ検出機能を持つ端末**

表2.5.4 富士通の技術要素別課題対応特許（5/14）

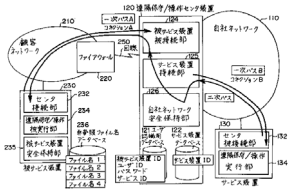
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特許3262689 95.05.19 G06F13/00,351 〔被引用回数 6〕	**遠隔操作ｼｽﾃﾑ**  第一のﾌｧｲｱｳｫｰﾙが内部ﾈｯﾄﾜｰｸに接続されたｻｰﾋﾞｽ装置のアドレスを特定するための識別子を送信し、第二のﾌｧｲｱｳｫｰﾙ及び第一のﾌｧｲｱｳｫｰﾙを介して、ｻｰﾋﾞｽ装置との間にｺﾈｸｼｮﾝを確立し、ｺﾈｸｼｮﾝを介して該ｻｰﾋﾞｽ装置との間でﾊﾟｹｯﾄを送受信するﾊﾟｹｯﾄ通信手段と、ﾊﾟｹｯﾄ通信手段が受信したﾊﾟｹｯﾄから遠隔操作の指示情報を取り出し、指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、を備えたことを特徴とする被ｻｰﾋﾞｽ装置。
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特開2002-084326 （拒絶確定） 01.06.11 H04L12/66	**被ｻｰﾋﾞｽ装置、ｾﾝﾀ装置、及びｻｰﾋﾞｽ装置**
	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 情報転送の手順 VPN設定情報	特開2002-073513 00.08.29 G06F13/00,650	**仮想空間のｾｷｭﾘﾃｲ方法**
	攻撃パターンの高精度化	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2005-056007 03.08.08 G06F15/00,330	**入力ﾃﾞｰﾀ制限ﾌﾟﾛｸﾞﾗﾑおよび入力ﾃﾞｰﾀ制限方法**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2004-265286 03.03.04 G06F15/00,330	**環境に応じて選択されたｾｷｭﾘﾃｲ・ﾎﾟﾘｼｰに従うﾓﾊﾞｲﾙ機器の管理**
			特開2004-258777 03.02.24 G06F15/00,330	**ｾｷｭﾘﾃｲ管理装置、ｾｷｭﾘﾃｲ管理ｼｽﾃﾑ、ｾｷｭﾘﾃｲ管理方法、ｾｷｭﾘﾃｲ管理ﾌﾟﾛｸﾞﾗﾑ**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 脆弱度の算出	特開2004-303094 03.03.31 G06F13/00,351	**ﾈｯﾄﾜｰｸｼｽﾃﾑﾃｽﾄ方法、ﾈｯﾄﾜｰｸｼｽﾃﾑﾃｽﾄﾌﾟﾛｸﾞﾗﾑ及びﾈｯﾄﾜｰｸ装置**
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2005-216291 98.03.10 G06F15/00,330	**伝送装置のｾｷｭﾘﾃｲｼｽﾃﾑ**
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2004-213233 02.12.27 G06F13/00,351 ｴﾌ・ｴﾌ・ｼｰ	**ﾈｯﾄﾜｰｸ接続を遮蔽可能とする管理装置及び制御装置**

表2.5.4 富士通の技術要素別課題対応特許（6/14）

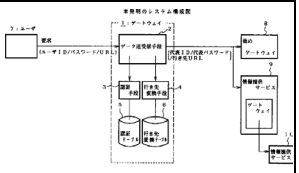
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
プロキシ中継技術	侵入防御の性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開平08-292930 95.02.23 G06F15/00,390	**ｸﾞﾙｰﾌﾟ間資源利用制御装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開平08-137798 （みなし取下） 94.11.14 G06F15/00,330	**情報処理装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開平08-137795 94.11.15 G06F15/00,310	**ﾃﾞｰﾀ独立型ｺﾝﾋﾟｭｰﾀｼｽﾃﾑにおけるﾃﾞｰﾀｱｸｾｽ権管理方式**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開2004-046739 02.07.15 G06F13/00,510	**ﾃﾞｰﾀ送信方法、ﾃﾞｰﾀ送信ｼｽﾃﾑ、中継装置、ｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ、及び記録媒体**
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開2003-323377 02.05.02 G06F13/00,560	**掲示板情報共有ｼｽﾃﾑ**
	デバイスの正当性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 識別子、認証情報の送信	特開2004-287802 03.03.20 G06F17/30,110	**横断検索方法及び横断検索ﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特許3493141 98.06.12 G06F15/00,330 〔被引用回数 3〕	**ｹﾞｰﾄｳｪｲｼｽﾃﾑおよび記録媒体**  ﾕｰｻﾞからの他のｼｽﾃﾑが実施するｻｰﾋﾞｽの要求を中継するｹﾞｰﾄｳｪｲｼｽﾃﾑにおいて、ﾕｰｻﾞからの上記ｻｰﾋﾞｽ要求を受信してﾕｰｻﾞの認証を行う手段と、要求のあったｻｰﾋﾞｽに対応するﾘﾝｸ情報と認証情報を用いてｻｰﾋﾞｽ要求を代行する手段と、ｻｰﾋﾞｽ要求に対応する返信のﾃﾞｰﾀのﾘﾝｸ情報に当該ｹﾞｰﾄｳｪｲｼｽﾃﾑのﾘﾝｸ情報を含める手段とを備えたことを特徴とするｹﾞｰﾄｳｪｲｼｽﾃﾑ。
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開平08-044643 （みなし取下） 94.07.27 G06F13/00,353 〔被引用回数 5〕	**ｹﾞｰﾄｳｪｲ装置**
			特開2004-005427 02.03.29 G06F13/00,353	**ﾎｽﾄ端末ｴﾐｭﾚｰｼｮﾝﾌﾟﾛｸﾞﾗﾑ、中継用ﾌﾟﾛｸﾞﾗﾑ、ﾎｽﾄ端末ｴﾐｭﾚｰｼｮﾝ方法、通信ﾌﾟﾛｸﾞﾗﾑ、通信方法およびｸﾗｲｱﾝﾄｺﾝﾋﾟｭｰﾀ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞの配置	特開2004-228616 （特許3698701） 03.01.17 H04L12/66	**DMZを介したｲﾝﾄﾗﾈｯﾄおよび外部ﾈｯﾄﾜｰｸ上の呼の確立**
			特開2003-324485 （特許3698698） 02.02.26 H04L12/66	**DMZを介したｲﾝﾄﾗﾈｯﾄおよび外部ﾈｯﾄﾜｰｸ上の呼の確立**
			特開2001-209596 00.01.27 G06F13/00,351	**情報集配信ｼｽﾃﾑ**

表2.5.4 富士通の技術要素別課題対応特許（7/14）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ｸｯｷに情報付加	特開2004-163999 02.11.08 G06F13/00,520	**中継装置**
	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開平10-254840 97.03.13 G06F15/16,430	**ﾓｰﾊﾞｲﾙｺｰﾄﾞ実行ｼｽﾃﾑ**
	経済性の向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開平08-137798 （みなし取下） 94.11.14 G06F15/00,330	**情報処理装置** 概要は技術要素「ﾌﾟﾛｷｼ中継」、課題「侵入防御の性能向上」の項参照
コンテンツフィルタリング技術	利用サービスの保護強化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2002-197060 00.12.27 G06F15/00,330	**ｾｷｭﾘﾃｨﾚﾍﾞﾙ設定支援ｼｽﾃﾑ及び方法**
			特開2004-234378 03.01.30 G06F15/00,330	**ｾｷｭﾘﾃｨ管理装置及びｾｷｭﾘﾃｨ管理方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2003-099400 01.09.26 G06F15/00,330	**ｾｷｭﾘﾃｨ管理装置及びｾｷｭﾘﾃｨ管理方法並びにｾｷｭﾘﾃｨ管理用ﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2003-006032 01.06.19 G06F12/00,546	**分散ﾌｧｲﾙ共有ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2003-085147 01.09.14 G06F15/00,330 富士通ｳﾞｨｴﾙｴｽｱｲ	**情報処理ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｱｸｾｽ制御ｻｰﾊﾞｰ配置	特開2002-149475 00.11.15 G06F12/00,546 富士通周辺機	**ﾈｯﾄﾜｰｸｻｰﾊﾞ、ﾊｲﾊﾟｰﾃｷｽﾄの送信制御方法、およびﾊｲﾊﾟｰﾃｷｽﾄを記録した記録媒体**

表2.5.4 富士通の技術要素別課題対応特許（8/14）

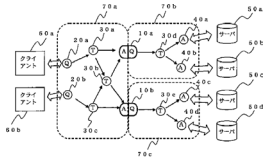
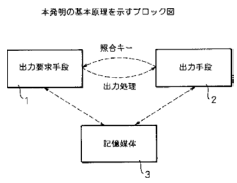
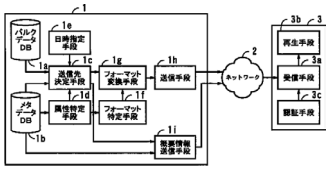
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｱｸｾｽ制御ｻｰﾊﾞｰ配置	特許3565720 98.08.20 G06F13/00,355	**分散構成による仲介装置および仲介装置に用いるﾃﾞｭｱﾙｾﾙ装置および仲介装置に用いる統合ｾﾙ装置**  仲介装置を構成するｾﾙ装置のうち少なくとも一つが、要求を出す質問者として振る舞うﾌﾟﾛｾｽを処理する質問ｾﾙ装置と要求の回答を出す回答者として振る舞うﾌﾟﾛｾｽを処理する回答ｾﾙ装置を兼ね備えたﾃﾞｭｱﾙｾﾙ装置であって、ﾃﾞｭｱﾙｾﾙ装置が、ｻｰﾊﾞ装置に対しては質問ｾﾙ装置として振る舞って質問者からの要求内容を前記ｻｰﾊﾞ装置に中継し、ｸﾗｲｱﾝﾄ装置に対しては要求に対する回答ｾﾙ装置と振る舞ってｻｰﾊﾞ装置からの回答をｸﾗｲｱﾝﾄ装置に中継する2つのｾﾙの役割を兼ね備えるｾﾙ装置であることを特徴とする分散構成による仲介装置。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特許2741726 93.06.21 G06F15/00,330	**共用出力手段のｾｷｭﾘﾃｨ確保方法及びｾｷｭﾘﾃｨ確保ｼｽﾃﾑ**  所定の出力手段（2）に対して出力処理を指示する出力要求手段（1）を有し、該出力手段（2）は、該出力要求手段（1）から指示された前記出力処理を受け付けて実行するような出力手段の共用構成に関する共用出力手段のｾｷｭﾘﾃｨ確保方法であって、前記出力要求手段（1）が前記出力処理を前記出力手段（2）に指示すると、前記出力手段（2）は、該出力処理を受け付けて該出力処理の実行を保留し、所定の照合ｷｰを生成して前記出力要求手段（1）に通知し、前記出力要求手段（1）は、該通知された照合ｷｰを記憶媒体（3）に記録し、前記出力手段（2）は、前記記憶媒体（3）の記憶内容を検索して前記照合ｷｰを見つけると、該照合ｷｰに対応する前記の保留した出力処理を実行することを特徴とする共用出力手段のｾｷｭﾘﾃｨ確保方法。
			特開2001-306513 00.04.21 G06F15/00,330	**情報管理装置および記憶媒体**
			特許3494590 99.06.18 H04L29/06	**送受信ｼｽﾃﾑおよび送信装置**  送信装置側に登録されたﾃﾞｰﾀを、少なくとも1以上の受信装置に対して送信する送受信ｼｽﾃﾑにおいて、前記送信装置は、送信対象となるﾃﾞｰﾀの属性を特定する属性特定手段と、前記属性特定手段によって特定された属性に応じた送信先を決定する送信先決定手段と、前記送信先決定手段によって決定された送信先に対して前記ﾃﾞｰﾀを送信する送信手段と、を有し、前記受信装置は、前記送信手段によって送信された前記ﾃﾞｰﾀを受信する受信手段と、前記受信手段によって受信された前記ﾃﾞｰﾀを再生する再生手段と、を有する、ことを特徴とする送受信ｼｽﾃﾑ。
			WO00-019326 98.09.29 G06F15/00,330	**ｱｸｾｽ要求処理方法及び装置**
			特開2002-014862 00.06.28 G06F12/00,537	**情報ｱｸｾｽ制御装置および情報ｱｸｾｽ制御方法**

表2.5.4 富士通の技術要素別課題対応特許（9/14）

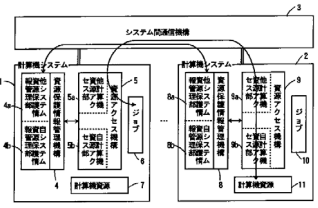
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特許3657755 97.11.25 G06F9/50	**複合型計算機ｼｽﾃﾑ及び計算機ｼｽﾃﾑ間の資源保護方法**  複数の計算機ｼｽﾃﾑと各計算機ｼｽﾃﾑを接続するｼｽﾃﾑ間通信機構から構成され、ｼﾞｮﾌﾞが他の計算機ｼｽﾃﾑ管理下の計算機資源に対するｱｸｾｽ処理を行う複合型計算機ｼｽﾃﾑにおいて、計算機ｼｽﾃﾑは、自計算機ｼｽﾃﾑの計算機資源を保護するための資源保護情報、及び他の計算機ｼｽﾃﾑ管理下の計算機資源を保護するための資源保護情報を管理する資源保護情報管理手段と、該資源保護情報管理手段にて管理する資源保護情報に基づいて、自計算機ｼｽﾃﾑ管理下の計算機資源に対するｱｸｾｽ処理、及び他の計算機ｼｽﾃﾑ管理下の計算機資源に対するｱｸｾｽ処理を行う資源ｱｸｾｽ手段とを有し、該資源ｱｸｾｽ手段にて計算機ｼｽﾃﾑ間のｱｸｾｽ処理の違いを吸収することにより、他の計算機ｼｽﾃﾑ管理下の計算機資源に対するｱｸｾｽ処理時の資源保護を、自計算機ｼｽﾃﾑ管理下の計算機資源に対するｱｸｾｽ処理と同様の処理で実行することを特徴とする複合型計算機ｼｽﾃﾑ。
	デバイスの正当性向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの追加、学習	特開2004-295504 03.03.27 G06F15/00,330	**ｾｷｭﾘﾃｨ管理ﾌﾟﾛｸﾞﾗﾑおよびｾｷｭﾘﾃｨ管理方法**
IPフィルタリング技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開平09-036977 （みなし取下） 95.07.18 H04M11/00,303	**ISDN端末装置**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 識別子、認証情報の送信	WO02-067512 01.02.19 H04L12/66	**通信のｾｷｭﾘﾃｨを確保するためのﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ方法およびﾊﾟｹｯﾄ通信ｼｽﾃﾑ**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開平09-116534 95.10.19 H04L9/32 〔被引用回数 1〕	**ｾｷｭﾘﾃｨﾚﾍﾞﾙ制御装置及びﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開平07-244639 （みなし取下） 94.03.03 G06F15/00,330	**ｱｸｾｽ権管理装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2005-197826 03.12.26 H04L12/24	**ﾈｯﾄﾜｰｸ上の複数ﾉｰﾄﾞの一元管理装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 自動登録	特開2002-158701 00.11.20 H04L12/56	**ｹｰﾌﾞﾙﾓﾃﾞﾑ装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2005-136629 03.10.29 H04L12/66	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**

表2.5.4 富士通の技術要素別課題対応特許（10/14）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2004-032523 （みなし取下） 02.06.27 H04L12/56,100	ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ方法および装置
		回路の改良 処理回路の改良 ﾌｨﾙﾀﾘﾝｸﾞ回路の改良	特開2001-333093 00.05.22 H04L12/56	ﾈｯﾄﾜｰｸｺﾈｸｼｮﾝﾌｨﾙﾀｼｽﾃﾑ
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2000-004225 98.06.17 H04L9/32	ﾈｯﾄﾜｰｸｼｽﾃﾑ、送受信方法、送信装置、受信装置、および、記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開平11-338799 98.05.27 G06F13/00,351 〔被引用回数 6〕	ﾈｯﾄﾜｰｸ接続制御方法及びｼｽﾃﾑ
	システムの性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2002-344530 01.05.17 H04L12/66 〔被引用回数 2〕	ﾊﾟｹｯﾄ転送装置、半導体装置、ﾊﾟｹｯﾄ転送ｼｽﾃﾑ
	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2005-197823 03.12.26 H04L12/66	ﾌｧｲｱｳｫｰﾙとﾙｰﾀ間での不正ｱｸｾｽ制御装置
	経済性の向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2002-344530 01.05.17 H04L12/66 〔被引用回数 2〕	ﾊﾟｹｯﾄ転送装置、半導体装置、ﾊﾟｹｯﾄ転送ｼｽﾃﾑ 概要は技術要素「IPﾌｨﾙﾀﾘﾝｸﾞ」、課題「ｼｽﾃﾑの性能向上」の項参照
ルーティング制御技術	侵入防御の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞにﾃﾞｰﾀ添付	特開平09-214550 （みなし取下） 96.01.30 H04L12/56	中継装置
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ併用	特開2002-027012 00.07.03 H04L29/06	ﾈｯﾄﾜｰｸ接続装置

表2.5.4 富士通の技術要素別課題対応特許（11/14）

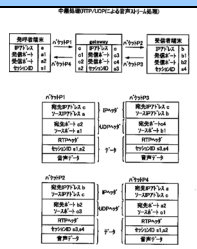
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 UDPの活用	特許3660285 01.08.30 H04L12/66	**通信制御方法、中継方法及び中継装置**  中継端末を介して第1通信端末T1と第2通信端末T2とが通信を行うに先立ち、第1通信端末T1が、自端末と前記中継端末との間の通信を識別するための第1通信識別情報S1を決定する第1決定ｽﾃｯﾌﾟと、中継端末を介して第1通信端末T1と第2通信端末T2とが通信を行うに先立ち、中継端末が、自端末と第1通信端末T1との間の通信を識別するための第2通信識別情報S2を決定する第2決定ｽﾃｯﾌﾟと、中継端末を介して第1通信端末T1と第2通信端末T2とが通信を行うに先立ち、中継端末が、自端末と第2通信端末T2との間の通信を識別するための第3通信識別情報S3を決定する第3決定ｽﾃｯﾌﾟと、中継端末を介して第1通信端末T1と第2通信端末T2とが通信を行うに先立ち、第2通信端末T2が、自端末と中継端末との間の通信を識別するための第4通信識別情報S4を決定する第4決定ｽﾃｯﾌﾟと、第1通信端末T1と中継端末とが、第1通信識別情報S1及び第2通信識別情報S2を含む第1ﾃﾞｰﾀの送受信を行う第1通信ｽﾃｯﾌﾟと、第2通信端末T2と前記中継端末とが、第3通信識別情報S3及び第4通信識別情報S4を含む第2ﾃﾞｰﾀの送受信を行う第2通信ｽﾃｯﾌﾟと、中継端末が、第1通信端末T1から受信した第1ﾃﾞｰﾀを第2通信端末T2に送信する場合に、第1ﾃﾞｰﾀのうち第1通信識別情報S1及び第2通信識別情報S2を第3通信識別情報S3及び第4通信識別情報S4に書き換える第1中継ｽﾃｯﾌﾟと、中継端末が、第2通信端末T2から受信したﾃﾞｰﾀを第1通信端末T1に送信する場合に、ﾃﾞｰﾀのうち第3通信識別情報S3及び第4通信識別情報S4を、第1通信識別情報S1及び第2通信識別情報S2に書き換える第2中継ｽﾃｯﾌﾟとを含む通信制御方法。
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開2000-332750 99.05.24 H04L12/14	**ﾈｯﾄﾜｰｸｱｸｾｽｴｰｼﾞｪﾝﾄによる集中課金・精算ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2004-064490 02.07.30 H04L29/06	**ﾃﾞｰﾀ通信ｼｽﾃﾑ**
IPアドレス変換技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 DNS、DHCPｻｰﾊﾞｰ配置	特開2004-180211 02.11.29 H04L12/56,100 〔被引用回数 1〕	**代理ﾈｯﾄﾜｰｸ制御装置**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 URLﾄﾞﾒｲﾝの変換	特開2001-352337 00.04.04 H04L12/46	**通信ﾃﾞｰﾀ中継装置、及び方法**
			特開2002-077252 00.08.28 H04L12/56	**ﾈｯﾄﾜｰｸ間通信ｾｷｭﾘﾃｨﾌﾟﾛｸﾞﾗﾑを記録した媒体および装置**
	侵入防御の性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 情報の付加	特開平07-162454 （拒絶確定） 93.12.03 H04L12/54	**電子ﾒｰﾙ連携方法および装置**
	デバイスの正当性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾎﾟｰﾄ番号、NATの変換	特開2003-078545 01.09.04 H04L12/56	**伝送装置およびﾌﾚｰﾑ転送方法**

表2.5.4 富士通の技術要素別課題対応特許（12/14）

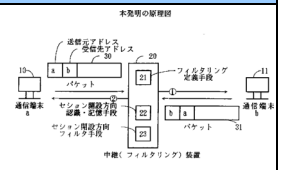
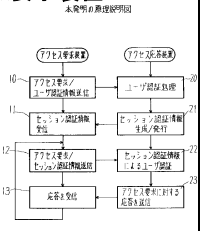
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
IPアドレス変換技術	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 送信方向	特許3593762 95.11.08 H04L12/66 〔被引用回数 2〕	**中継装置**  ﾈｯﾄﾜｰｸ上の通信端末間に置かれたﾌｨﾙﾀﾘﾝｸﾞ機能を有する中継装置に於いて、両通信端末間の通信をﾌｨﾙﾀﾘﾝｸﾞすることを、該通信端末ｱﾄﾞﾚｽによるｾｼｮﾝ開設方向で規定する定義手段と、該中継装置に入力されたﾊﾟｹｯﾄから該ｾｼｮﾝ開設方向を認識し、これを記憶管理するｾｼｮﾝ管理手段と、ｾｼｮﾝ開設後の通信について、前記ｾｼｮﾝ管理手段と前記定義手段とによりﾌｨﾙﾀﾘﾝｸﾞの是非を決めるﾌｨﾙﾀﾘﾝｸﾞ手段とを備えたことを特徴とする中継装置。
	侵入検出の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2002-185539 （特許3723076） 00.12.15 H04L12/66 〔被引用回数 3〕	**不正侵入防御機能を有するIP通信ﾈｯﾄﾜｰｸｼｽﾃﾑ**
ホスト認証技術	デバイスの正当性向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特許3463399 95.03.13 G06F13/00,353 〔被引用回数 1〕	**通信ｼｽﾃﾑおよびｱｸｾｽ応答装置およびｱｸｾｽ要求装置**  ｱｸｾｽ応答装置が保持するﾃﾞｰﾀまたはｻｰﾋﾞｽに対してｱｸｾｽ制限が課せられたものである場合には、ｱｸｾｽ要求の毎にｱｸｾｽ応答装置側がｱｸｾｽ要求装置側ﾕｰｻﾞの認証処理を行う通信ｼｽﾃﾑにおいて、ｱｸｾｽ要求装置は実行するｾｯｼｮﾝに係わる最初のｱｸｾｽ要求時だけｱｸｾｽ応答装置に対してﾕｰｻﾞ認証情報を送出し、ｱｸｾｽ応答装置はﾕｰｻﾞ認証処理によりｱｸｾｽ要求装置によるｱｸｾｽを許可した際は、今回のｾｯｼｮﾝに限り有効なｾｯｼｮﾝ認証情報を発行し、以後ｱｸｾｽ要求装置はｾｯｼｮﾝが終了するまでに発生するｱｸｾｽ要求毎にｾｯｼｮﾝ認証情報を前記ｱｸｾｽ応答装置に送出し、ｱｸｾｽ応答装置はｾｯｼｮﾝ認証情報を用いてﾕｰｻﾞ認証処理を行うように構成したことを特徴とする通信ｼｽﾃﾑ。
		各種の処理手順改良 特定情報の取得手順 ｱﾄﾞﾚｽの取得	特開2005-184639 03.12.22 H04L12/66	**接続管理ｼｽﾃﾑ、接続管理装置及び接続管理方法**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間・期間情報	特開2005-072639 03.08.21 H04L12/46	**識別子割当装置、方法及びﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開平10-105516 96.05.07 G06F15/00,330 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ認証ｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開平07-295926 （特許3685504） 94.04.28 G06F15/00,310	**情報管理装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 ﾎﾟｰﾄ番号の登録	特開平09-172450 （みなし取下） 95.12.19 H04L12/44 〔被引用回数 1〕	**ｱﾄﾞﾚｽｾｷｭﾘﾃｨ制御方式**

表2.5.4 富士通の技術要素別課題対応特許（13/14）

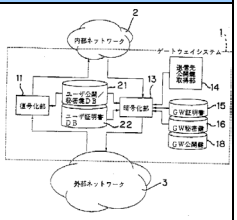
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
ホスト認証技術	デバイスの正当性向上	回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特許3431745 96.01.08 H04L12/46	**ｹﾞｰﾄｳｴｲｼｽﾃﾑ**  第1の通信回線、および該第1の通信回線を経由してﾃﾞｰﾀ通信を行なう複数の第1の端末を有する第1のﾈｯﾄﾜｰｸと、第2の通信回線、および該第2の通信回線を経由してﾃﾞｰﾀ通信を行なう複数の第2の端末を有する第2のﾈｯﾄﾜｰｸとの間のﾃﾞｰﾀ通信の橋渡しを行なうｹﾞｰﾄｳｪｲｼｽﾃﾑにおいて、前記第2の通信回線を経由して通信されてきたﾃﾞｰﾀを受信する第1の受信手段と、前記第1の通信回線にﾃﾞｰﾀを送信する第1の送信手段と、前記第1の端末それぞれに対応する、相互に異なる秘密鍵が登録された第1のﾃﾞｰﾀﾍﾞｰｽと、前記第2の通信回線を経由し前記第1の端末のうちのいずれかの第1の受信端末に向けて送信されてきた、該第1の受信端末の公開鍵で暗号化されたﾃﾞｰﾀを、前記第1のﾃﾞｰﾀﾍﾞｰｽから読み出した該第1の受信端末の秘密鍵で復号化して前記第1の送信手段に渡す復号化手段とを備えたことを特徴とするｹﾞｰﾄｳｪｲｼｽﾃﾑ。
	システムの性能向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2001-326632 00.05.17 H04L9/32	**分散ｸﾞﾙｰﾌﾟ管理ｼｽﾃﾑおよび方法**
トンネリング技術	システムの性能向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開平11-008627 97.06.16 H04L12/28	**認証機能を有する交換機**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特開2001-249866 00.03.06 G06F13/00,351	**ﾌｧｲｱｳｫｰﾙ機能を分散させたﾈｯﾄﾜｰｸ、ﾌｧｲｱｳｫｰﾙ分散機能を有するﾌｧｲｱｳｫｰﾙｻｰﾊﾞ、及びﾌｧｲｱｳｫｰﾙ機能を有するｴｯｼﾞﾉｰﾄﾞ**
	中継するデータの機密性向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特許3644579 98.10.29 H04L9/08 〔被引用回数 1〕	**ｾｷｭﾘﾃｨ強化方法及び装置**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開2003-101523 01.09.21 H04L9/08	**秘匿機能を有する通信ﾈｯﾄﾜｰｸ･ｼｽﾃﾑおよび通信方法**
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 擬似､ﾀﾞﾐﾃﾞｰﾀの送信	特開平06-266670 （拒絶確定） 93.03.11 G06F15/00,330	**暗号化仮想端末初期化装置**
		情報の送信、転送、分岐の手順改良 情報転送の手順 VPN設定情報	特開2003-318992 02.04.26 H04L12/66	**ｹﾞｰﾄｳｴｲ、通信端末装置、および通信制御ﾌﾟﾛｸﾞﾗﾑ**

表2.5.4 富士通の技術要素別課題対応特許（14/14）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
トンネリング技術	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2002-044141 00.07.26 H04L12/56 〔被引用回数 1〕	ﾓﾊﾞｲﾙIPﾈｯﾄﾜｰｸにおけるVPNｼｽﾃﾑ及びVPNの設定方法
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2005-229651 02.08.09 H04L12/56	仮想閉域網ｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙの追加、切換 ﾎﾟﾘｼｰﾙの切換	特開2002-101096 01.05.17 H04L12/22 ｹﾞｰ ｴﾑ ﾃﾞｰ ﾌｫﾙｼｭﾝｸﾞｽﾂｪﾝﾄﾙﾑ ｲﾝﾌｫﾙﾏ(ﾄﾞｲﾂ)	ｾｷｭﾘﾃｲｻｰﾋﾞｽ・ﾚｲﾔｰ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開平07-030568 （みなし取下） 93.06.24 H04L12/42	ﾙｰﾌﾟ型ﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸのｾｷｭﾘﾃｲ方式

2.6 三菱電機

2.6.1 企業の概要

商号	三菱電機　株式会社
本社所在地	〒100-8310　東京都千代田区丸の内2-2-3
設立年	1921年（大正10年）
資本金	1,758億20百万円（2005年3月末）
従業員数	27,319名（2005年3月末）（連結：97,661名）
事業内容	重電システム、産業メカトロニクス、情報通信システム、電子デバイス、家庭電器等の製造・販売、他

トップページで、セキュリティにリンクできる統合セキュリティのホームページを開設している。セキュリティを物理セキュリティ、情報セキュリティと統合セキュリティに体系化して、セキュリティ製品やセキュリティ情報等を紹介している。その中でも、「MISTY(R)」を紹介しており、暗号の解読に必要な暗号化鍵の長さを128ビット（DESは56ビット）とし、現時点でのもっとも強力な3つの暗号解読法に対して高い安全性を持っている。また、高速処理が可能なことも大きな特徴である。発表以来「MISTY(R)」は、国内外から安全性と高速性に関して高い評価を得ている。三菱電機は、「MISTY(R)」の基本特許を無償公開している。

（出典：http://www.mitsubishielectric.co.jp/security/index.html）

2.6.2 製品例

情報セキュリティの製品の中で不正アクセス侵入検知防御技術に関する製品やサービスを、表2.6.2に示す。

表2.6.2 三菱電機の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
MistyGuard(R)<CryptoSign(R)>	社内の機密情報や他社との契約書といった重要なビジネス文書を電子メールで送るのは心配である。こうした不安を、電子メールの持つ即時性や簡易性をビジネスに活用するための強力なソリューションとして、メッセージ暗号ソフトウェアMistyGuard(R)<CryptoSign(R)>を考案し、世界トップレベルの共通鍵暗号アルゴリズムで解決した。
不正アクセス対策ソリューション 脆弱性診断	業内システムや外部サービスシステムの安全性を保つためには、不正アクセスに対する脆弱性を定期的に診断する必要がある。セキュリティ診断ツールで重要なことは、実際に侵入者の立場となって評価対策を立て、診断する事が出来るかである。侵入者の視点で実際にクラッキングに利用される可能性があるセキュリティホールを効率的に診断・検出する。

（出典：http://www.mitsubishielectric.co.jp/security/info/）

2.6.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

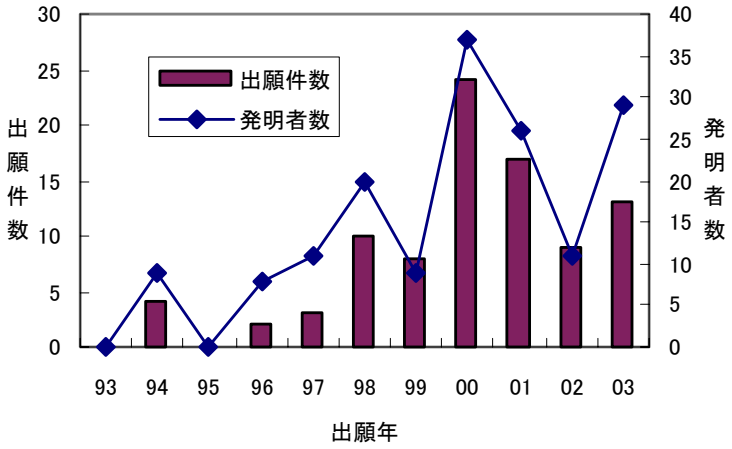
東京都千代田区丸の内2丁目2番3号 三菱電機株式会社内

神奈川県鎌倉市上町屋325番地 三菱電機株式会社情報システム製作所内

神奈川県鎌倉市大船5丁目1番1号 三菱電機株式会社通信システム研究所内

図2.6.3に、三菱電機の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の４年間の平均は、出願件数が15件、発明者数が25人である。

図2.6.3 三菱電機の不正アクセス侵入検知防御技術に関する出願件数と発明者数



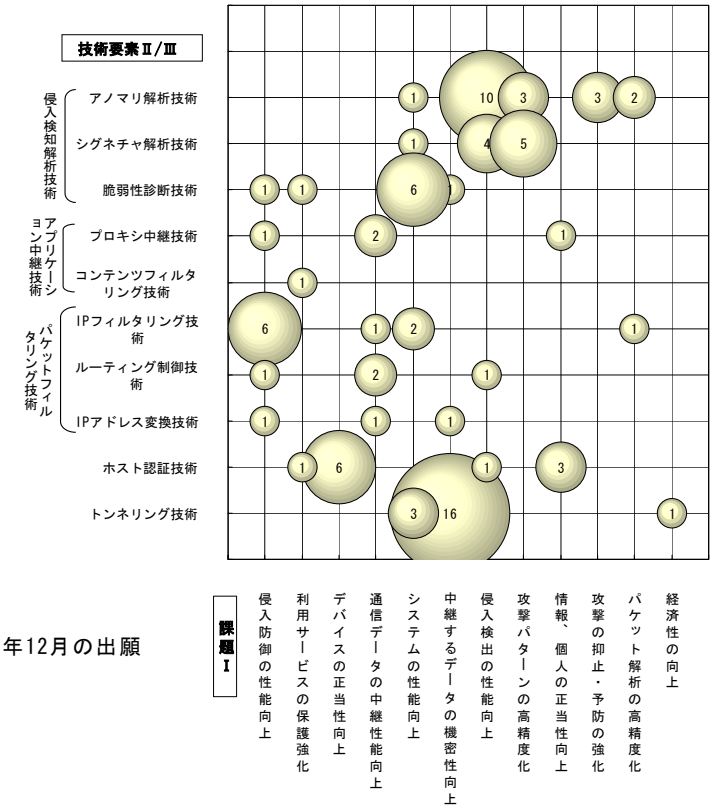
2.6.4 技術開発課題対応特許の概要

図2.6.4-1に、三菱電機の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.6.4-2に、三菱電機の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術とトンネリング技術が最も多く出願されている。これらの出願のうち、最も多い課題は、「中継するデータの機密性向上」であり、次いで多い課題は「侵入検出の性能向上」である。

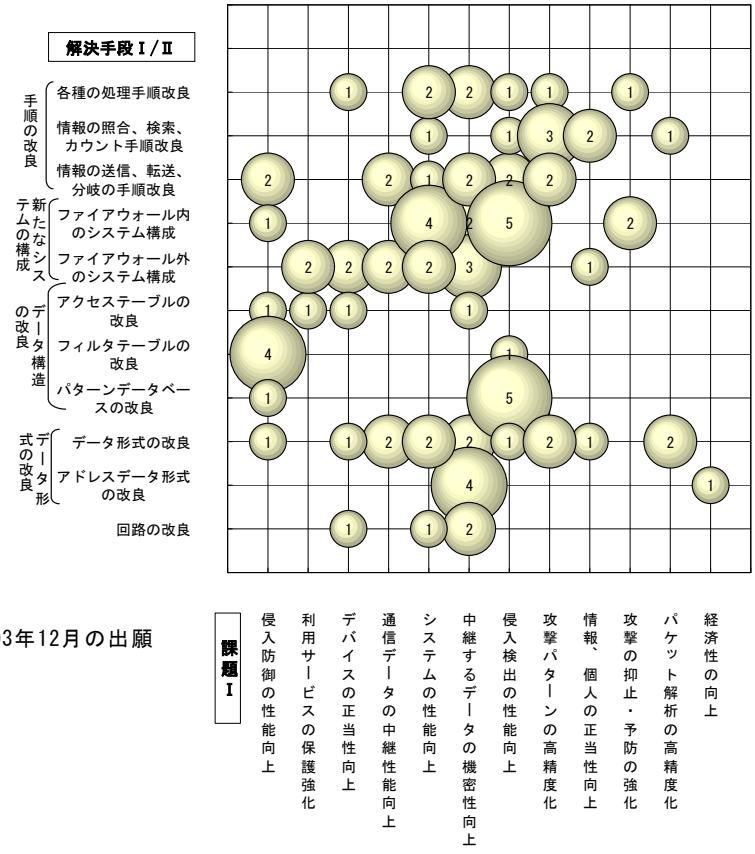
「侵入検出の性能向上」の課題に対しては、「ファイアウォール内のシステム構成」と「パターンデータベースの改良」で多く対応している。次いで「侵入防御の性能向上」に対しては、「フィルタテーブルの改良」で、「システムの向上」に対しては、「ファイアウォール内のシステム構成」で、さらに「中継するデータの機密性向上」に対しては、「アドレスデータ形式の改良」で対応している。

図2.6.4-1 三菱電機の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.6.4-2 三菱電機の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.6.4 三菱電機の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は90件で、そのうち７件が登録特許である。なお、表2.6.4では図2.6.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.6.4 三菱電機の技術要素別課題対応特許（1/10）

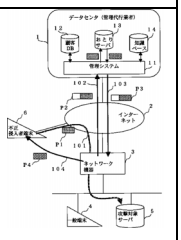
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2003-264595 02.03.08 H04L12/66 〔被引用回数 1〕	ﾊﾟｹｯﾄ中継装置、ﾊﾟｹｯﾄ中継ｼｽﾃﾑおよびｵﾄﾘ誘導ｼｽﾃﾑ
	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開2003-258910 02.03.04 H04L12/56,400	不正ｱｸｾｽ経路解析ｼｽﾃﾑ及び不正ｱｸｾｽ経路解析方法
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2001-337919 00.05.24 G06F15/00,330 〔被引用回数 1〕	ｾｷｭﾘﾃｨﾎｰﾙ診断方式
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開2001-094602 99.09.24 H04L12/56 〔被引用回数 1〕	不正ｱｸｾｽ検知装置
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開2003-076662 01.09.05 G06F15/00,330	情報漏洩追跡ｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2002-199024 （特許3685062） 00.12.27 H04L12/66 〔被引用回数 1〕	不正ｱｸｾｽ監視方法および内部通信ﾈｯﾄﾜｰｸ
			特開2004-328307 03.04.24 H04L12/66	攻撃防御ｼｽﾃﾑ、攻撃防御制御ｻｰﾊﾞおよび攻撃防御方法
			特許3495030 01.02.14 G06F13/00,351 〔被引用回数 1〕	不正侵入ﾃﾞｰﾀ対策処理装置、不正侵入ﾃﾞｰﾀ対策処理方法及び不正侵入ﾃﾞｰﾀ対策処理ｼｽﾃﾑ  所定の内部通信ﾈｯﾄﾜｰｸ外に配置され、前記内部通信ﾈｯﾄﾜｰｸに不正に侵入する目的で前記内部通信ﾈｯﾄﾜｰｸ外に配置されたいずれかのﾃﾞｰﾀ通信装置より送信された不正侵入ﾃﾞｰﾀを受信し、受信した前記不正侵入ﾃﾞｰﾀに対する対策処理を行うことを特徴とする不正侵入ﾃﾞｰﾀ対策処理装置。
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2002-026906 00.07.03 H04L12/22	ﾃﾞｰﾀ配信装置
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2003-333092 （みなし取下） 02.05.14 H04L12/56,400	ﾈｯﾄﾜｰｸｼｽﾃﾑ、攻撃ﾊﾟｹｯﾄ追跡方法および攻撃ﾊﾟｹｯﾄ防御方法

表2.6.4 三菱電機の技術要素別課題対応特許（2/10）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 振舞い形式の学習	特開2003-067269 01.08.30 G06F13/00,351 〔被引用回数 4〕	**不正ｱｸｾｽ検知装置及び不正ｱｸｾｽ検知方法**
	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ﾄﾗﾌｨｯｸの頻度、増加率	特開2002-199025 00.12.26 H04L12/66 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ防御装置**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特開2004-282262 03.03.13 H04L12/66	**負荷攻撃防御装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2001-344206 （拒絶確定） 00.05.31 G06F15/00,330	**ｾｷｭﾘﾃｨ診断ｼｽﾃﾑおよび方法**
	攻撃の抑止・予防の強化	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2004-234208 03.01.29 G06F15/00,330 三菱電機情報ﾈｯﾄﾜｰｸ	**ｾｷｭﾘﾃｨ対策運用管理装置**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開2000-276457 99.03.25 G06F15/177,682	**ﾃﾞｰﾀ共有ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ及びｸﾗｲｱﾝﾄ**
			特開2000-112890 98.09.30 G06F15/00,330 〔被引用回数 1〕	**不正操作防止と追跡装置**
	パケット解析の高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2004-179999 02.11.27 H04L12/66	**侵入検知装置およびその方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2003-204358 02.01.07 H04L12/56,400	**不正侵入検知装置及び不正侵入検知方法及び不正侵入検知ﾌﾟﾛｸﾞﾗﾑ**
シグネチャ解析技術	システムの性能向上	回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2002-073433 00.08.28 G06F13/00,351 〔被引用回数 5〕	**侵入検知装置及び不正侵入対策管理ｼｽﾃﾑ及び侵入検知方法**
	侵入検出の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2002-007234 00.06.20 G06F13/00,351 〔被引用回数 5〕	**不正ﾒｯｾｰｼﾞ検出装置、不正ﾒｯｾｰｼﾞ対策ｼｽﾃﾑ、不正ﾒｯｾｰｼﾞ検出方法、不正ﾒｯｾｰｼﾞ対策方法、及びｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**

表2.6.4 三菱電機の技術要素別課題対応特許（3/10）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
シグネチャ解析技術	侵入検出の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2001-350678 00.06.07 G06F13/00,351 〔被引用回数 1〕	不正侵入検知ｼｽﾃﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2003-085139 01.09.10 G06F15/00,330	侵入検知管理ｼｽﾃﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 類似度、相関度の算出	特開2004-220373 03.01.15 G06F15/00,320	不正ｱｸｾｽ検知ﾛｸﾞ情報分析支援装置、不正ｱｸｾｽ検知ﾛｸﾞ情報分析支援方法及びｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ
	攻撃パターンの高精度化	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開2005-004617 03.06.13 G06F13/00,351	不正侵入対策処理ｼｽﾃﾑ、攻撃分析･応答装置およびﾈｯﾄﾜｰｸ遮断･模擬装置並びに不正侵入対策処理方法
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2001-236314 （特許3748192） 00.02.24 G06F15/00,330	不正通信ｿﾌﾄｳｴｱ検出方法
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開2003-087333 01.09.10 H04L12/66	ﾃﾞｰﾀ中継装置、ﾃﾞｰﾀ中継方法、ﾃﾞｰﾀ中継処理ﾌﾟﾛｸﾞﾗﾑ及びﾃﾞｰﾀ中継処理ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ｱｸｾｽ、ｾｯｼｮﾝ回数	特開2002-252654 （特許3731111） 01.02.23 H04L12/66 〔被引用回数 3〕	侵入検出装置およびｼｽﾃﾑならびにﾙｰﾀ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2005-149205 03.11.17 G06F15/16	ﾓﾊﾞｲﾙｴｰｼﾞｪﾝﾄｼｽﾃﾑ
脆弱性診断技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 ｱｸｾｽ許可情報	特開2003-345749 02.05.23 G06F15/00,330	認証情報の管理配信方法およびｼｽﾃﾑ
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開2003-030138 01.07.11 G06F15/00,310 〔被引用回数 1〕	ｲﾝﾀｰﾈｯﾄ接続ｼｽﾃﾑ、管理ｻｰﾊﾞ装置、ｲﾝﾀｰﾈｯﾄ接続方法およびその方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑ
	システムの性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開2005-100141 03.09.25 G06F15/00,330	ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ、ｾｷｭﾘﾃｨ管理方法、ｾｷｭﾘﾃｨ管理ﾌﾟﾛｸﾞﾗﾑ及び記録媒体

表2.6.4 三菱電機の技術要素別課題対応特許（4/10）

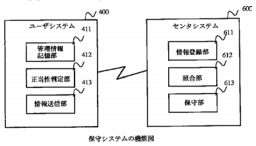
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
脆弱性診断技術	システムの性能向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特許3248658 94.11.02 G06F11/30 三菱電機ｼｽﾃﾑｳｴｱ	**保守ｼｽﾃﾑ及び遠隔保守方式及び遠隔保守ｼｽﾃﾑ**  以下のﾕｰｻﾞｼｽﾃﾑとｾﾝﾀｼｽﾃﾑを備えた保守ｼｽﾃﾑ（1）以下の要素を備えたﾕｰｻﾞｼｽﾃﾑ（a1）ﾕｰｻﾞｼｽﾃﾑの管理情報を記憶する管理情報記憶部、（a2）上記管理情報をﾁｪｯｸすることによりｼｽﾃﾑの正当性を判定する正当性判定部、（a3）上記正当性判定部の判定結果に基づいて、ｾﾝﾀｼｽﾃﾑにﾕｰｻﾞｼｽﾃﾑの情報を送信する情報送信部、（b）以下の要素を備えたｾﾝﾀｼｽﾃﾑ（b1）保守の対象となるﾕｰｻﾞｼｽﾃﾑの情報を記憶する情報登録部、（b2）上記情報送信部により送信された情報を受信し、情報登録部に記憶された情報と照合する照合部、（b3）上記照合部の照合結果に基づいて、ﾕｰｻﾞｼｽﾃﾑの保守を開始する保守部。
		情報の送信、転送､分岐の手順改良 特定情報の通知、送信手順 更新差分情報の送信	WO01-056223 00.01.28 H04L12/22	**通信管理ﾃｰﾌﾞﾙ転送ｼｽﾃﾑ及び管理装置及び暗号装置及び通信管理ﾃｰﾌﾞﾙ転送方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2003-345750 97.01.27 G06F15/00,330	**情報提供ｼｽﾃﾑ及び情報提供方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開2002-077174 00.08.25 H04L12/28	**移動体電子装置**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開2002-261829 01.02.27 H04L12/56,400	**階層管理ｼｽﾃﾑ及び階層管理方法**
	中継するデータの機密性向上	回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特開2003-319067 （特許3682049） 99.11.30 H04M3/00	**通話装置ｱﾀﾞﾌﾟﾀ及び中継ｻｰﾊﾞ及びｲﾝﾀｰﾈｯﾄ電話ﾈｯﾄﾜｰｸｼｽﾃﾑ**
プロキシ中継技術	侵入防御の性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開平08-050559 （みなし取下） 94.08.04 G06F12/00,537	**ﾌｧｲﾙ記憶保護装置**
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開2000-112860 98.10.01 G06F13/00,354	**安全な情報発信･共有ｻｰﾋﾞｽ方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-240596 03.02.05 G06F15/00,330	**Webｼｽﾃﾑ**

表2.6.4 三菱電機の技術要素別課題対応特許（5/10）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特開2000-148630 98.11.11 G06F13/00,351	**情報伝送ｼｽﾃﾑ**
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 役割の属性値	特許3349978 99.02.10 G06F12/00,537	**計算機ｼｽﾃﾑにおけるｱｸｾｽ制御方法**  ｻﾌﾞｼﾞｪｸﾄが役割に関連付けられ、計算機ｼｽﾃﾑ内のｵﾌﾞｼﾞｪｸﾄに対するｻﾌﾞｼﾞｪｸﾄのｱｸｾｽ権を各ｵﾌﾞｼﾞｪｸﾄに関連付けられたｱｸｾｽ制御ﾘｽﾄを用いて制御し、ｱｸｾｽ制御ﾘｽﾄにおけるｻﾌﾞｼﾞｪｸﾄの指定方法として、ｻﾌﾞｼﾞｪｸﾄの識別子、ｻﾌﾞｼﾞｪｸﾄの属性、ｻﾌﾞｼﾞｪｸﾄと関連付けられた役割の識別子、ｻﾌﾞｼﾞｪｸﾄと関連付けられた役割の属性を任意に含んだｻﾌﾞｼﾞｪｸﾄ照合条件式を利用する拡張役割ﾍﾞｰｽ･ｱｸｾｽ制御方式の計算機ｼｽﾃﾑにおけるｱｸｾｽ制御方法であって、属性の名称と属性取得ﾌｧﾝｸｼｮﾝの宣言の列からなる属性定義情報を与えられ、属性の値を解釈するｽﾃｯﾌﾟが前記属性定義情報を解釈して属性の値を得るための属性取得ﾌｧﾝｸｼｮﾝの宣言を得るｽﾃｯﾌﾟを含み、属性の値を取得するｽﾃｯﾌﾟが前記属性取得ﾌｧﾝｸｼｮﾝの宣言を解釈することによって属性の値を取得することを特徴とする計算機ｼｽﾃﾑにおけるｱｸｾｽ制御方法。
IPフィルタリング技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 送信方向	特開2004-185483 02.12.05 G06F13/00,351	**単方向通信装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開2002-251336 01.02.21 G06F13/00,351	**ﾈｯﾄﾜｰｸ管理装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの削除	特開2000-115228 98.10.06 H04L12/54	**電子ﾒｰﾙ用ﾒｰﾙｻｰﾊﾞ及びﾒｰﾙｸﾗｲｱﾝﾄ**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの追加、学習	特開2002-261788 01.02.27 H04L12/46 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙ管理装置および方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2005-025523 03.07.02 G06F15/00,330	**情報ｾｷｭﾘﾃｨ管理支援装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2004-040476 02.07.03 H04L12/46	**ｱﾄﾞﾚｽ変換装置**
	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開平08-097860 （みなし取下） 94.09.22 H04L12/66	**網間中継装置の経路情報交換方法**

表2.6.4 三菱電機の技術要素別課題対応特許（6/10）

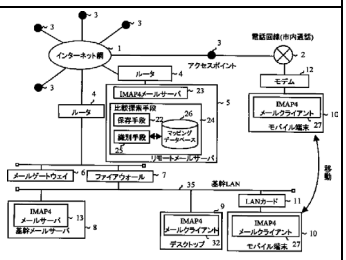
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	システムの性能向上	ファイアウォール内のシステム構成 イントラネット内に機器の配置 複数ファイアウォールの配置	特開2002-152281 （放棄） 00.11.09 H04L12/66	**中継装置および通信システム**
		ファイアウォール外のシステム構成 サービスサーバーの配置 メールサーバーの配置	特開2002-073509 00.08.31 G06F13/00,630	**遠隔監視制御システム**
	パケット解析の高精度化	情報の照合、検索、カウント手順改良 特定情報の検索、抽出手順 経路、中継サーバー	特開2004-304516 03.03.31 H04L12/56	**パケット送信元特定方法、パケット中継装置及びパケット受信装置**
ルーティング制御技術	侵入防止の性能向上	フィルターテーブルの改良 ポリシールールの追加、切換 ポリシールールの切換	特開2004-312176 03.04.03 H04L12/66	**メッセージ判定処理装置**
	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開平07-264178 （拒絶確定） 94.03.23 H04L9/00 〔被引用回数 3〕	**セキュリティ方式**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 トラフィックの頻度、増加率	特開2002-111722 00.09.27 H04L12/56	**データ中継装置、及びデータ中継方法**
	侵入検出の性能向上	データ形式の改良 データに情報付加 ヘッダに情報付加	特開2001-308918 00.04.20 H04L12/56 〔被引用回数 1〕	**攻撃経路追跡システム及びルータ装置**
IPアドレス変換技術	侵入防止の性能向上	ファイアウォール内のシステム構成 DMZに機器の配置 情報提供サーバーの配置	特開2005-056339 03.08.07 G06F13/00,540	**情報フィルタリング装置及び情報フィルタリングシステム**
	通信データの中継性能向上	ファイアウォール外のシステム構成 サービスサーバーの配置 メールサーバーの配置	特許3482863 98.03.16 H04L12/54 〔被引用回数 2〕	**電子メール管理システム**  異なったメールサーバ間でメールを識別するための識別手段と、メールヘッダと暗号化の有無とメールの未読/既読とメールの更新日時のメール状態情報を記憶する記憶手段と、記憶したメール状態情報を最新なものに更新する更新手段と、更新された新しいメール状態情報を基にメールの整合性をとることでメールサーバ間のメールの同期を行う同期手段と、特定のユーザが暗号化したメールの本文を特定のユーザだけが復号化できる暗号/復号手段と、更新手段による最新のメールのメール状態情報と暗号/復号手段で暗号化したメールの本文をリモートメールサーバにメール送信することによって、メール本体の同期を行う同期手段とを有しファイアウォール内に接続された基幹メールサーバと、比較探索手段を有しファイアウォール外に接続されたリモートメールサーバとを備え、比較探索手段はリモートメールサーバで割り当てられたユニークIDから基幹メールサーバで割当てられるユニークIDを獲得し、インターネット網を介してファイアウォール外にあるリモートメールサーバ内のメールを読むことによって、リモートメールサーバ内のメールと対応した基幹メールサーバ内のメールを読むことになることを特徴とする。

表2.6.4 三菱電機の技術要素別課題対応特許（7/10）

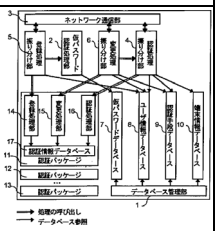
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPアドレス変換技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2003-008651 01.06.21 H04L12/58,100	**ﾊﾟｹｯﾄ通信方法及びﾊﾟｹｯﾄ通信ｼｽﾃﾑ**
ホスト認証技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2002-041467 00.07.25 G06F15/00,330	**証明書ｱｸｾｽｼｽﾃﾑ**
	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特許3587045 98.02.04 G06F15/00,330	**認証管理装置及び認証管理ｼｽﾃﾑ**  1又は複数の認証情報を入力する複数の端末とﾈｯﾄﾜｰｸを介して接続され、上記複数の端末の認証を管理する認証管理装置において、少なくとも、上記複数の端末に入力される認証情報に応じて認証処理を行う1又は複数の認証手段と、上記ﾕｰｻﾞの認証情報に対応する情報が登録されるﾕｰｻﾞ情報ﾃﾞｰﾀﾍﾞｰｽと、上記認証手段に対応する情報が登録される認証手段ﾃﾞｰﾀﾍﾞｰｽと、上記認証手段を任意に組み合わせた認証条件に対応する情報が登録される端末情報ﾃﾞｰﾀﾍﾞｰｽとを備えることを特徴とする認証管理装置。
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2000-216903 99.01.22 H04M11/00,303	**認証ｺｰﾙﾊﾞｯｸ接続ｼｽﾃﾑ**
			特開2003-085144 01.09.12 G06F15/00,330	**ﾈｯﾄﾜｰｸｼｽﾃﾑ、ﾈｯﾄﾜｰｸ用ｺﾝﾋﾟｭｰﾀ端末、代理認証装置および代理認証方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2003-030063 01.07.16 G06F13/00,351 〔被引用回数 1〕	**OA管理ｼｽﾃﾑ及びOA管理方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2001-148715 （拒絶確定） 99.11.19 H04L12/56 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**
		回路の改良 ｽｲｯﾁ回路の追加 無線との切換	特開2001-298774 00.04.13 H04Q7/38	**無線電話使用認証方法**
	侵入検出の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞにﾃﾞｰﾀ添付	特開2002-044074 00.07.25 H04L9/32	**通信ﾃﾞｰﾀ管理ｼｽﾃﾑ、通信ﾃﾞｰﾀ管理方法、通信ﾃﾞｰﾀ管理ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読取可能な記録媒体および双方向通信ﾃﾞｰﾀ管理装置**
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2001-320366 00.05.11 H04L9/32	**携帯型情報端末への情報供給方式**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2002-297543 01.04.02 G06F15/00,330	**不正ﾛｸﾞｲﾝ検出装置**

表2.6.4 三菱電機の技術要素別課題対応特許（8/10）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
ホスト認証技術	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2004-179724 02.11.25 H04L9/08	ｻｰﾊﾞ装置及び証明書検証方法及びﾌﾟﾛｸﾞﾗﾑ及びﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体
トンネリング技術	システムの性能向上	各種の処理手順改良 特定情報の取得手順 ID情報の取得	特開2001-203678 00.01.19 H04L9/08	暗号鍵配送ｼｽﾃﾑおよび暗号鍵配送方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2003-179627 01.12.10 H04L12/56	ﾊﾟｹｯﾄ通信装置及びﾊﾟｹｯﾄ通信方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2002-044135 00.07.25 H04L12/56	暗号装置及び暗号通信ｼｽﾃﾑ
	中継するデータの機密性向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開平11-243388 98.02.26 H04L9/08 日本電信電話	暗号通信ｼｽﾃﾑ
		各種の処理手順改良 各種処理の実行手順 特定処理の実行	特開2003-115834 01.10.05 H04L9/08	ｾｷｭﾘﾃｨｱｿｼｴｰｼｮﾝ切断/継続方法および通信ｼｽﾃﾑ
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開2001-237824 00.02.22 H04L9/14	情報通信中継装置
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 障害情報の通知	特開2002-344443 01.05.15 H04L9/32	通信ｼｽﾃﾑおよびｾｷｭﾘﾃｨｱｿｼｴｰｼｮﾝ切断/継続方法
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開2004-328230 03.04.23 H04L12/46	VPN環境導入支援ｼｽﾃﾑ、そのｼｽﾃﾑに使用される端末装置およびｻｰﾊﾞ装置
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 機器、ﾓｼﾞｭｰﾙ配置	特開平09-282281 （みなし取下） 96.09.12 G06F15/00,330	ﾃﾞｰﾀｾｷｭﾘﾃｨ方法およびｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2001-320365 00.05.10 H04L9/32	認証局ｻｰﾊﾞ及び電子署名装置及び電子署名検証装置及びﾌﾟﾗｲﾊﾞｼｰ情報鍵管理ｻｰﾊﾞ及びﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開平11-308264 （みなし取下） 98.04.17 H04L12/46 〔被引用回数 1〕	暗号通信ｼｽﾃﾑ

表2.6.4 三菱電機の技術要素別課題対応特許（9/10）

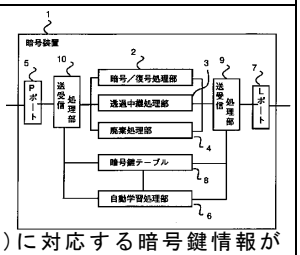
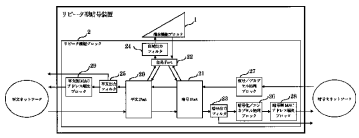
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開平11-088436 97.09.16 H04L12/56 〔被引用回数 2〕	**情報提供ｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 鍵情報	特許3595145 97.06.02 H04L12/22 日本電信電話 〔被引用回数 1〕	**暗号通信ｼｽﾃﾑ**  通信ﾈｯﾄﾜｰｸに収容された通信端末間を暗号装置が中継して暗号通信を行う暗号通信ｼｽﾃﾑにおいて、通信ﾃﾞｰﾀを中継する中継経路上の暗号装置は、中継する通信ﾃﾞｰﾀの送信元端末と宛先端末の組み合わせ（以下端末ﾍﾟｱと称す）に対応する暗号鍵情報が前記暗号装置の暗号鍵ﾃｰﾌﾞﾙに登録されていない場合、暗号鍵情報を収集するための鍵探索ﾊﾟｹｯﾄが前記中継経路上の各暗号装置自身の暗号情報を収集し、その収集した暗号情報を鍵探索応答ﾊﾟｹｯﾄが前記中継経路上の前記各暗号装置に通知し、通知を受けた前記各暗号装置は、収集した前記暗号鍵情報に基づいて、前記端末ﾍﾟｱに対応して通信ﾃﾞｰﾀを、暗号化するか、復号するか、透過中継するか、廃棄するか、いずれの処理を行うかを指定する暗号鍵情報を前記暗号鍵ﾃｰﾌﾞﾙに登録し、その端末ﾍﾟｱからの通信ﾃﾞｰﾀを中継する前記各暗号装置は前記暗号鍵ﾃｰﾌﾞﾙの暗号鍵情報に基づいて通信ﾃﾞｰﾀを処理することを特徴とする暗号通信ｼｽﾃﾑ。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾍﾟｲﾛｰﾄﾞの暗号化	特開平09-252315 （放棄） 96.03.14 H04L12/46 〔被引用回数 1〕	**暗号通信ｼｽﾃﾑおよび暗号装置**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開2000-183967 98.12.16 H04L12/56 〔被引用回数 1〕	**ﾊﾟｹｯﾄ通信装置及びﾊﾟｹｯﾄ通信ｼｽﾃﾑ**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特許3259724 99.11.26 H04L12/66	**暗号装置、暗号化器および復号器**  平文ﾈｯﾄﾜｰｸから受信した平文ﾃﾞｰﾀを暗号化すると共に、ｱﾄﾞﾚｽと他の暗号装置との予め定められた対応関係に基づいて、平文ﾃﾞｰﾀのﾍｯﾀﾞに設定されたｱﾄﾞﾚｽに対応する暗号装置を決定し、決定した他の暗号装置に基づいて新規にﾍｯﾀﾞを設定するｴﾝｶﾌﾟｾﾙ処理を行って生成した暗号ﾃﾞｰﾀを平文ﾈｯﾄﾜｰｸと同一IPｻﾌﾞﾈｯﾄの暗号文ﾈｯﾄﾜｰｸへ送信する暗号化/ｴﾝｶﾌﾟｾﾙ処理部と、暗号文ﾈｯﾄﾜｰｸから受信した暗号ﾃﾞｰﾀを平文ﾃﾞｰﾀに復号すると共に、平文ﾃﾞｰﾀのﾍｯﾀﾞに設定されたｱﾄﾞﾚｽに基づいてﾍｯﾀﾞを再設定するﾃﾞｶﾌﾟｾﾙ処理を行って生成した平文ﾃﾞｰﾀを暗号文ﾈｯﾄﾜｰｸと同一IPｻﾌﾞﾈｯﾄの平文ﾈｯﾄﾜｰｸへ送信する復号/ﾃﾞｶﾌﾟｾﾙ処理部とを備えたことを特徴とする暗号装置。
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開2002-185540 （放棄） 99.11.26 H04L12/66	**暗号装置、暗号化器および復号器**

表2.6.4 三菱電機の技術要素別課題対応特許（10/10）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ｱﾄﾞﾚｽの暗号化	特開平11-203222 （みなし取下） 98.01.19 G06F13/00,351 〔被引用回数 1〕	**暗号通信方法**
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2001-274812 00.03.28 H04L12/28	**暗号通信ｼｽﾃﾑおよび暗号装置**
	経済性の向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開2000-183967 98.12.16 H04L12/56 〔被引用回数 1〕	**ﾊﾟｹｯﾄ通信装置及びﾊﾟｹｯﾄ通信ｼｽﾃﾑ** 概要は技術要素「ﾄﾝﾈﾘﾝｸﾞ」、課題「中継するﾃﾞｰﾀの機密性向上」の項参照

2.7 松下電器産業

2.7.1 企業の概要

商号	松下電器産業　株式会社
本社所在地	〒571-8501　大阪府門真市大字門真1006
設立年	1935年（昭和10年）
資本金	2,587億40百万円（2005年3月末）
従業員数	47,867名（2005年3月末）　（連結：334,752名）
事業内容	電気機械器具の製造・販売・サービス（映像・音響機器、情報通信機器、家庭電化・住宅設備機器、産業機器、電子部品）

多発する犯罪、続発する情報流出。今やビジネスの世界でも行政機関においてもセキュリティ対策は急務の課題である。パナソニックでは、従来のように個々のセキュリティシステムを提供するだけでなく、それらを一つのネットワーク上に統合、連携･融合させ、一段と高度なセキュリティ環境を実現する、「シナプスネット」を開発した。

（出典：http://panasonic.biz/sinapse-net/index.html）

2.7.2 製品例

シナプスネットの製品やシステムのうち、不正アクセス侵入検知防御技術に関係する製品やサービスを、表2.7.2に示す。

表2.7.2 松下電器産業の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
ネットワーク映像監視システム	光ネットワークや専用回線を使って遠隔地を結び、鮮明な監視映像を送受信。
デジタルディスクレコーダー	監視カメラの映像を高画質デジタル記録する、ハードディスク録画方式を採用。

（出典：http://panasonic.biz/security/index.html）

2.7.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

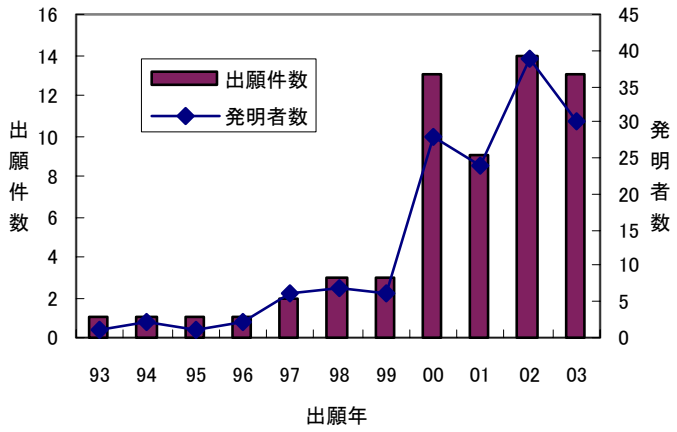
開発拠点：

大阪府門真市大字門真1006番地 松下電器産業株式会社内

アメリカ合衆国ニュージャージー州サマーセット

図2.7.3に、松下電器産業の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の４年間の平均では、出願件数が12件、発明者数が30人である。

図2.7.3 松下電器産業の不正アクセス侵入検知防御技術に関する出願件数と発明者数



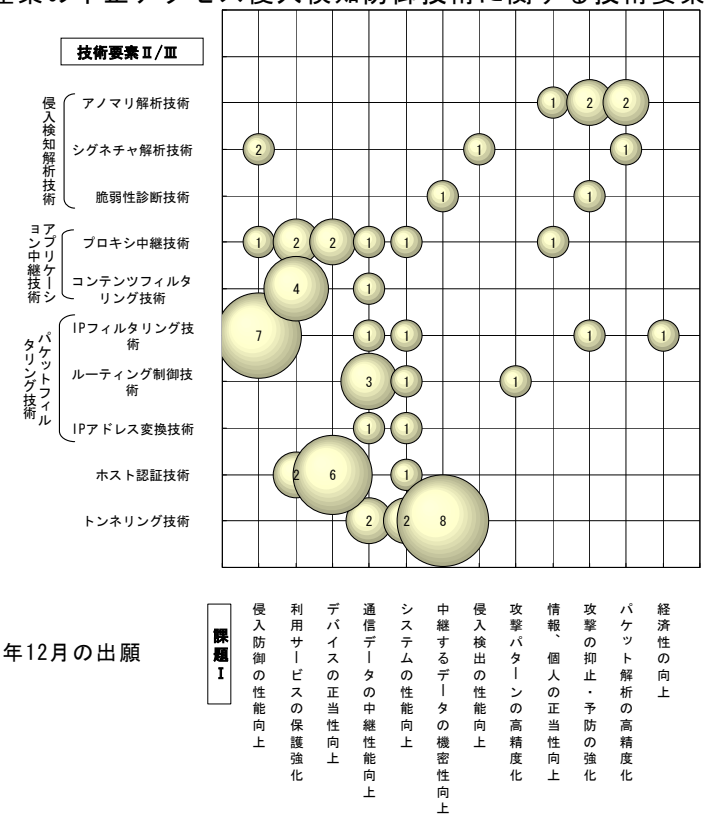
2.7.4 技術開発課題対応特許の概要

図2.7.4-1に、松下電器産業の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.7.4-2に、松下電器産業の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

トンネリング技術が最も多く出願され、次いでIPフィルタリング技術に関する出願が多い。これらの出願のうち、最も多い課題は、「侵入防御の性能向上」、「通信データの中継性能向上」と「中継するデータの機密性向上」である。

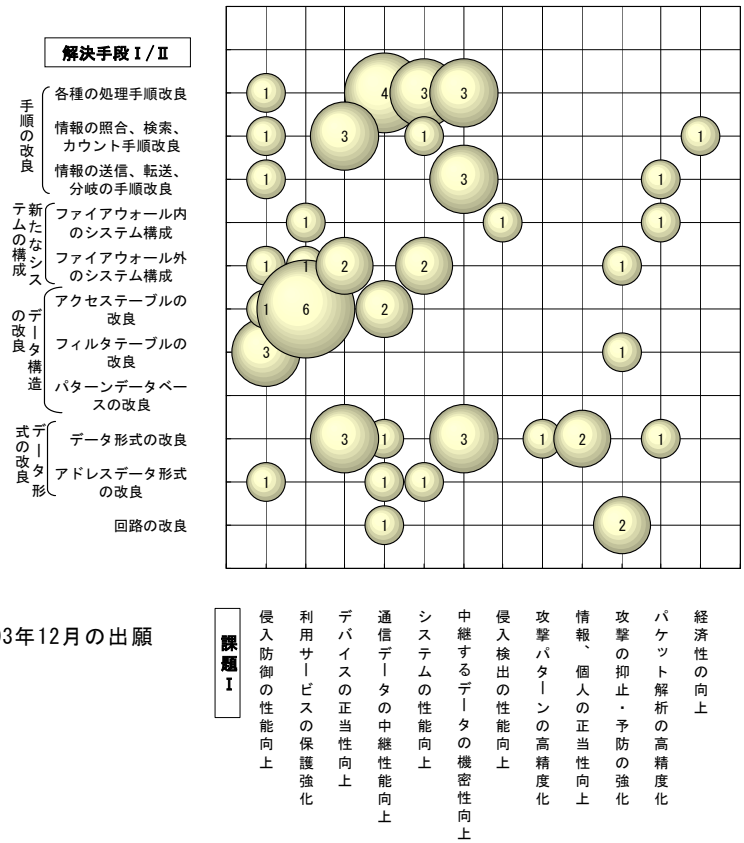
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。次いで「通信データの中継性能向上」の課題に対しては、「各種の処理手順改良」で多く対応している。

図2.7.4-1 松下電器産業の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.7.4-2 松下電器産業の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.7.4 松下電器産業の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は61件で、そのうち１件が登録特許である。なお、表2.7.4では図2.7.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.7.4 松下電器産業の技術要素別課題対応特許（1/6）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2002-319935 01.01.19 H04L9/32	ﾃﾞｰﾀ処理装置
	攻撃の抑止・予防の強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2005-182311 03.12.17 G06F15/00,330	端末管理支援方法及びﾊﾟｯﾁ確認ｻｰﾊﾞ
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2000-105621 98.09.28 G06F1/00,370	ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀ
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾊﾞｯｸｱｯﾌﾟｻｰﾊﾞｰの配置	特開2004-259262 03.02.07 G06F12/14,320	端末装置及びそれを備えたﾃﾞｰﾀ保護ｼｽﾃﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2004-080743 02.06.11 H04L12/56,400	ｺﾝﾃﾝﾂ通信履歴解析ｼｽﾃﾑ及びﾃﾞｰﾀ通信制御装置
シグネチャ解析技術	侵入検出の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼｰﾙｰﾙの追加、切換 ﾎﾟﾘｼｰﾙｰﾙの切換	特開2004-312416 03.04.08 H04L12/66	ｱｸｾｽ制御方法、中継装置及びｻｰﾊﾞ
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2002-328897 01.04.27 G06F15/00,330 〔被引用回数 1〕	ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｼｽﾃﾑ
	パケット解析の高精度化	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾊﾟﾀｰﾝのﾀﾞｳﾝﾛｰﾄﾞ	特開2005-157650 03.11.25 G06F13/00	不正ｱｸｾｽ検知ｼｽﾃﾑ
脆弱性診断技術	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 情報転送の手順 VPN設定情報	特開2001-298449 00.04.12 H04L9/14 〔被引用回数 2〕	ｾｷｭﾘﾃｨ通信方法、通信ｼｽﾃﾑ及びその装置
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2002-014928 （拒絶確定） 00.06.30 G06F15/00,330	ﾈｯﾄﾜｰｸ機器不正使用防止装置、ﾈｯﾄﾜｰｸ機器不正使用防止方法、及びﾈｯﾄﾜｰｸ機器不正使用防止ﾌﾟﾛｸﾞﾗﾑ記録媒体
プロキシ中継技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開平09-146887 95.11.24 G06F15/00,330	情報取り込み装置

表2.7.4 松下電器産業の技術要素別課題対応特許（2/6）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開2001-273218 00.03.24 G06F13/00,354	情報配信方法及び情報配信ｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特開2001-060972 （拒絶確定） 99.08.19 H04L12/66 〔被引用回数 1〕	ﾈｯﾄﾜｰｸ接続装置及びﾈｯﾄﾜｰｸ接続方法
	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2001-326695 （特許3714850） 00.05.18 H04L12/66 〔被引用回数 2〕	ｹﾞｰﾄｳｴｲ装置、接続ｻｰﾊﾞ装置、ｲﾝﾀｰﾈｯﾄ端末、ﾈｯﾄﾜｰｸｼｽﾃﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特開2003-242113 02.02.18 G06F15/00,330	通信ｼｽﾃﾑ、通信方法、ﾌﾟﾛｸﾞﾗﾑおよびｻｰﾊﾞ装置
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2003-209579 02.01.17 H04L12/56,300	情報処理ｼｽﾃﾑおよび情報処理方法
	システムの性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2003-030143 01.04.30 G06F15/00,330	携帯用記憶装置を用いるｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸｾｷｭﾘﾃｲｼｽﾃﾑ
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2005-167816 03.12.04 H04L9/36	中継装置、中継ｼｽﾃﾑ、中継方法及び中継ﾌﾟﾛｸﾞﾗﾑ
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2000-315191 99.05.06 G06F15/00,330	ｵｰﾄﾊﾟｲﾛｯﾄｼｽﾃﾑ及びｵｰﾄﾊﾟｲﾛｯﾄ方法並びに記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	WO01-082086 00.04.24 G06F12/14,310	ｱｸｾｽ権設定装置及び管理者端末
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 時間、期限情報	特開2001-337917 00.05.30 G06F15/00,310	GUI装置端末装置、ﾘｿｰｽ制御装置、ﾈｯﾄﾜｰｸｼｽﾃﾑ、媒体及び情報集合体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2004-038486 02.07.02 G06F1/00	発行許可装置、発行申請装置、配信装置、ｱﾌﾟﾘｹｰｼｮﾝ実行装置及び方法
	通信データの中継性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2003-085059 01.03.16 G06F13/00,351	ﾌｧｲｱｳｫｰﾙ設定方法およびその装置

表2.7.4 松下電器産業の技術要素別課題対応特許（3/6）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 各種処理の実行手順 ﾊﾟﾀｰﾝ、ﾙｰﾙの言語記述	特開2003-333084 （みなし取下） 02.05.09 H04L12/56,100	ﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞﾙｰﾙ設定方法
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順、ｺﾏﾝﾄﾞ	特開2005-051588 03.07.30 H04L12/56,100	自動ﾌｨﾙﾀﾘﾝｸﾞ方法、および機器
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2004-032364 02.06.26 H04L12/66	ﾈｯﾄﾜｰｸｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開2004-185498 02.12.05 G06F13/00,351	ｱｸｾｽ制御装置
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 自動登録	特開2004-221879 03.01.14 H04L12/66	通信方法、通信ﾌﾟﾛｸﾞﾗﾑおよび中継装置
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼﾙｰﾙの追加、切換 ﾎﾟﾘｼﾙｰﾙの切換	特開平08-163177 （みなし取下） 94.12.09 H04L12/66	ﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸﾌﾚｰﾑﾘﾚｰ網間ﾌﾟﾘｯｼﾞ装置
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の停止、取消し	特開2002-259309 01.02.27 G06F13/00,630	電子ﾒｰﾙを用いた処理ｼｽﾃﾑ
	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2004-312084 03.04.02 H04N7/173,610	映像配信ｼｽﾃﾑ
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特開2004-266516 03.02.28 H04L12/22	ﾈｯﾄﾜｰｸ管理ｻｰﾊﾞ、通信端末、ｴｯｼﾞｽｲｯﾁ装置、通信用ﾌﾟﾛｸﾞﾗﾑ並びにﾈｯﾄﾜｰｸｼｽﾃﾑ
	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開2004-287790 03.03.20 G06F13/00,610	通信ｱﾀﾞﾌﾟﾀｰ及びｹﾞｰﾄｳｪｲ装置
	経済性の向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順、ｺﾏﾝﾄﾞ	特開2005-051588 03.07.30 H04L12/56,100	自動ﾌｨﾙﾀﾘﾝｸﾞ方法、および機器
ルーティング制御技術	通信データの中継性能向上	各種の処理手順改良 特定情報の記憶、登録手順 要求情報の記憶	特開2002-164951 00.11.24 H04L29/06	ｸﾗｲｱﾝﾄ装置、ﾃﾞｰﾀ送受信ｼｽﾃﾑ及びﾌﾟﾛｸﾞﾗﾑ記録媒体

表2.7.4 松下電器産業の技術要素別課題対応特許（4/6）

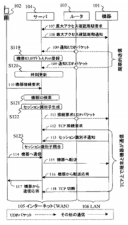
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開平07-191918 （拒絶確定） 93.12.27 G06F13/00,351	ｺﾝﾋﾟｭｰﾀｼｽﾃﾑおよびﾈｯﾄﾜｰｸ運用ｼｽﾃﾑ
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開平11-261640 （みなし取下） 98.03.13 H04L12/56 〔被引用回数 2〕	動的手段/経路変更方式及びﾈｯﾄﾜｰｸｼｽﾃﾑ
	システムの性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開2004-088768 02.08.06 H04L12/66	ﾊﾟｹｯﾄﾃﾞｰﾀ中継装置及びその方法
	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ｺﾏﾝﾄﾞに情報付加	特開平10-289106 （みなし取下） 97.04.15 G06F9/44,530	情報処理装置
IPアドレス変換技術	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特許3445986 02.09.27 H04L12/56	ｲﾝﾀｰﾈｯﾄに接続するｻｰﾊﾞ、機器および通信ｼｽﾃﾑ  ｲﾝﾀｰﾈｯﾄに接続された少なくとも1つの機器と、ｲﾝﾀｰﾈｯﾄに接続可能な少なくとも1つの端末との間の通信を転送する、ｲﾝﾀｰﾈｯﾄに接続されたｻｰﾊﾞであって、機器からの定期的な通知UDPﾊﾟｹｯﾄを受信し、端末からの機器に対する転送要求があった場合、通知UDPﾊﾟｹｯﾄの応答として接続要求UDPﾊﾟｹｯﾄを機器に送信し、接続要求UDPﾊﾟｹｯﾄに応答して機器からｻｰﾊﾞへ送信されたTCP接続要求を受諾し、TCP接続確立後、そのTCP接続上で端末と機器間の通信を転送することを特徴とするｻｰﾊﾞ。
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 DNS、DHCPｻｰﾊﾞｰ配置	特開2003-249941 （みなし取下） 02.02.26 H04L12/46	遠隔制御ｼｽﾃﾑの設定方法とその遠隔制御ｼｽﾃﾑ、及びその処理側分散制御ｼｽﾃﾑ
ホスト認証技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2001-051948 （拒絶確定） 99.08.16 G06F15/00,330	ｱｸｾｽ制御装置及びｱｸｾｽ制御ｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2001-222508 00.02.14 G06F15/00,330	携帯電話端末からのｲﾝﾄﾗﾈｯﾄｱｸｾｽ方式
	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2001-265677 00.03.21 G06F13/00,351	通信網におけるﾊｲﾊﾟｰﾃｷｽﾄｱｸｾｽ制御方式
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間・期間情報	特開2002-140298 00.10.31 G06F15/00,330	認証方法

表2.7.4 松下電器産業の技術要素別課題対応特許（5/6）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 識別子情報の照合	特開2004-040717 02.07.08 H04L9/32	機器認証ｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2004-363884 03.06.04 H04M11/00,303	情報処理ｼｽﾃﾑおよびｻｰﾋﾞｽ提供方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-220339 03.01.15 G06F15/00,330	情報供給ｼｽﾃﾑ、情報盤、使用者ｻｰﾊﾞ、供給者ｻｰﾊﾞおよび管理ｻｰﾊﾞ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-088148 02.08.22 H04L12/28,300	無線LANｼｽﾃﾑ、移動体通信ｼｽﾃﾑ及び無線端末、並びに、端末認証方法
	システムの性能向上	各種の処理手順改良 各種処理の実行手順 並列処理の実行	特開2002-287620 00.12.25 G09C1/00,610	ｾｷｭﾘﾃｨ通信ﾊﾟｹｯﾄ処理装置及びその方法
トンネリング技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2000-082028 97.12.18 G06F13/00,351	ﾒｯｾｰｼﾞ受信装置およびﾒｯｾｰｼﾞ送信装置
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開平10-021302 96.07.04 G06F17/60	利用者情報収集ｼｽﾃﾑ
	システムの性能向上	各種の処理手順改良 各種処理の実行手順 並列処理の実行	特開2004-180234 02.11.29 H04L9/14	暗号ﾊﾟｹｯﾄ処理装置
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ｱﾄﾞﾚｽの暗号化	特開2002-344927 （拒絶確定） 01.05.14 H04N7/173,610	画像伝送方法、画像伝送ﾌﾟﾛｸﾞﾗﾑおよび画像伝送装置
	中継するデータの機密性向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開平11-289326 98.04.01 H04L9/16	ﾃﾞｰﾀ送信装置、及びﾃﾞｰﾀ受信装置
		各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開2003-037587 01.07.26 H04L9/08	ｾｯｼｮﾝ鍵生成方法
		各種の処理手順改良 特定情報の取得手順 ｱﾄﾞﾚｽの取得	特開2005-184368 03.12.18 H04L12/56	通信制御装置、通信制御方法、およびﾈｯﾄﾜｰｸｶﾒﾗｼｽﾃﾑ

表2.7.4 松下電器産業の技術要素別課題対応特許（6/6）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開2001-292135 00.04.07 H04L9/08	**鍵交換ｼｽﾃﾑ**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特開2003-304227 （みなし取下） 02.04.08 H04L9/08	**暗号通信装置、暗号通信方法及び暗号通信ｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2002-176421 00.09.26 H04L9/14	**ﾃﾞｰﾀ転送方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2003-110603 01.09.28 H04L12/56	**ﾊﾟｹｯﾄ処理装置及びそのﾊﾟｹｯﾄ処理方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 多重符号化で変換	特開2003-198544 01.10.19 H04L9/32	**機器認証ｼｽﾃﾑおよび機器認証方法**

2.8 ソニー

2.8.1 企業の概要

商号	ソニー　株式会社
本社所在地	〒141-0001　東京都品川区北品川6-7-35
設立年	1946年（昭和21年）
資本金	6,217億8百万円（2005年3月末）
従業員数	151,400名（2005年3月末）
事業内容	音響・映像・情報・通信関係の各種電子・電気機械器具・部品の製造・販売、他

bit-driveは、ソニーが提供するブロードバンドソリューションである。ビジネス向けの高品質な光ファイバーやADSLインターネット接続サービス事業を核に、多様なソリューションを提供する。(出典：http://www.bit-drive.ne.jp/index.html)

2.8.2 製品例

bit-drive に紹介されているもののうち、不正アクセス侵入検知防御技術に関連する製品やサービスを、表2.8.2に示す。

表2.8.2 ソニーの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
セキュアサーバー DigitalGate	リモートアクセスやVPNなど多彩な機能を搭載したオールインワンサーバー。ファイアウォール、不正アクセス対策、セキュリティホールに対する自動パッチなどにより、セキュリティ対策の運用負荷を軽減。
DigitalGate VPNプラス	DigitalGateとの組み合わせにより、更に低コストなインターネットVPN環境の構築を実現するネットワークサーバーパックのオプションサービス。

(出典：http://www.bit-drive.ne.jp/index.html)

2.8.3 技術開発拠点と研究者

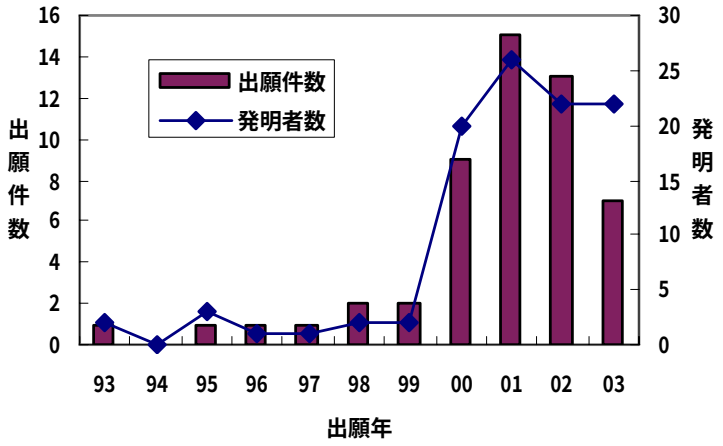
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都品川区北品川6丁目7番35号 ソニー株式会社内

図2.8.3に、ソニーの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の４年間の平均では、出願件数が10件、発明者数が20人である。

図2.8.3 ソニーの不正アクセス侵入検知防御技術に関する出願件数と発明者数



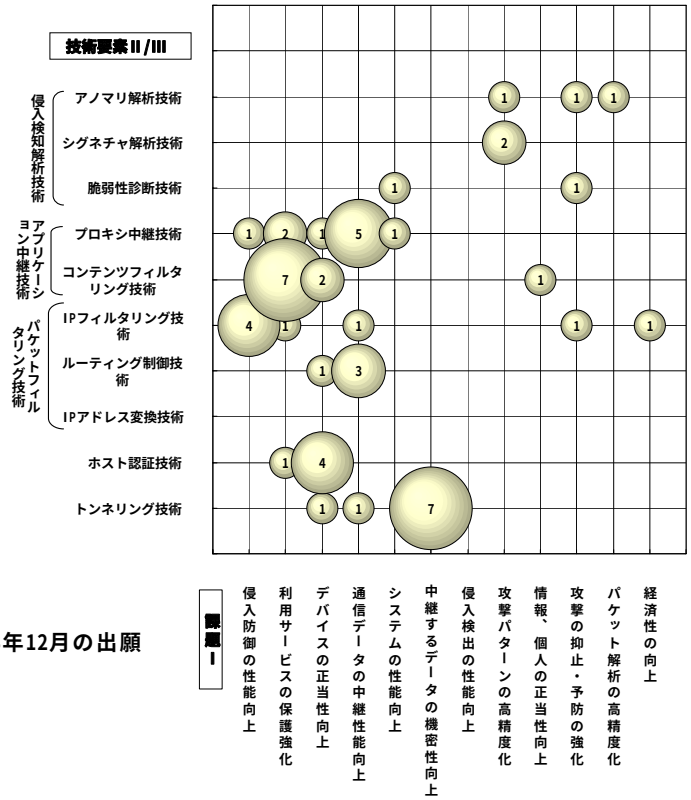
2.8.4 技術開発課題対応特許の概要

図2.8.4-1に、ソニーの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.8.4-2に、ソニーの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

コンテンツフィルタリング技術とプロキシ中継技術が最も多く出願され、次いでトンネリング技術に関する出願が多い。これらの出願のうち、最も多い課題は、「利用サービスの保護強化」であり、次いで多い課題は「通信データの中継性能向上」である。

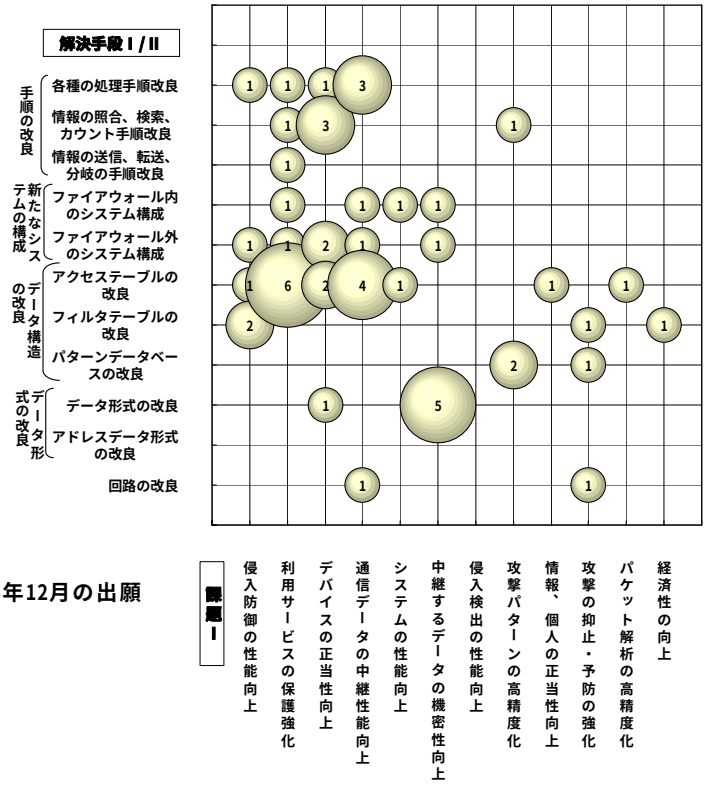
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。次いで「中継するデータの機密性向上」の課題に対しては、「データ形式の改良」で多く対応している。

図2.8.4-1 ソニーの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.8.4-2 ソニーの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.8.4 ソニーの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は52件である。なお、表2.8.4では図2.8.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.8.4 ソニーの技術要素別課題対応特許（1/5）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	攻撃パターンの高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ 手順 ﾊﾟｹｯﾄ	特開2004-140524 02.10.16 H04L12/66	DoS攻撃検知方法、DoS攻撃検知装置及びﾌﾟﾛｸﾞﾗﾑ
	攻撃の抑止・予防の強化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ｱﾗｰﾄﾊﾟﾀｰﾝの追加	特開2003-023377 01.07.09 H04B3/54	電力線通信におけるｳｲﾙｽの除去方法および装置
	パケット解析の高精度化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開平11-353276 (みなし取下) 98.06.09 G06F15/00,330	ｱｸｾｽ制御装置
シグネチャ解析技術	攻撃パターンの高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 異常値出現頻度	特開2004-139178 02.10.15 G06F13/00,351	情報処理装置及び方法、並びにﾌﾟﾛｸﾞﾗﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 ﾘﾀｰﾝｱﾄﾞﾚｽ蓄積	特開2004-054470 02.07.18 G06F15/00,330	ﾈｯﾄﾜｰｸ・ｾｷｭﾘﾃｲ・ｼｽﾃﾑ、情報処理装置及び情報処理方法、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2003-124996 (みなし取下) 01.10.10 H04L12/56,400	端末装置監視ｼｽﾃﾑ及び端末装置監視方法
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2002-271360 01.03.09 H04L12/46	ﾙｰﾀ装置
プロキシ中継技術	侵入防御の性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開2005-032059 03.07.08 G06F13/00,351	ﾃﾞｰﾀ処理方法、ﾌﾟﾛｸﾞﾗﾑおよびｺﾝﾋﾟｭｰﾀ
	利用サービスの保護強化	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2002-141953 00.11.06 H04L12/66 〔被引用回数 2〕	通信中継装置、通信中継方法、および通信端末装置、並びにﾌﾟﾛｸﾞﾗﾑ記憶媒体
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2003-067429 01.05.09 G06F17/50,624	情報公開ｼｽﾃﾑ、ｻｰﾊﾞ、ｸﾗｲｱﾝﾄ装置、および、ﾌﾟﾛｸﾞﾗﾑ
	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2003-271559 02.03.18 G06F15/00,330	情報処理ｼｽﾃﾑ、情報処理装置および方法、並びにﾌﾟﾛｸﾞﾗﾑ
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2004-272632 03.03.10 G06F13/00,357	情報処理装置、および情報処理方法、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ

表2.8.4 ソニーの技術要素別課題対応特許（2/5）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	通信データの中継性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰｸﾞﾙｰﾌﾟ	特開2002-244755 01.02.16 G06F1/00	ﾃﾞｰﾀ処理方法、半導体回路およびﾌﾟﾛｸﾞﾗﾑ
			特開2002-244868 01.02.16 G06F9/46,340	ﾃﾞｰﾀ処理方法、半導体回路およびﾌﾟﾛｸﾞﾗﾑ
			特開2002-244756 01.02.19 G06F1/00	ﾃﾞｰﾀ処理方法、半導体回路および認証用装置
		回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特開平11-055329 (みなし取下) 97.08.07 H04L12/66 〔被引用回数 1〕	ﾃﾞｰﾀ伝送装置およびﾃﾞｰﾀ伝送方法、ｻｰﾊﾞ装置
	システムの性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2004-046430 02.07.10 G06F15/00,330	ﾘﾓｰﾄｱｸｾｽｼｽﾃﾑ及びﾘﾓｰﾄｱｸｾｽ方法
コンテンツフィルタリング技術	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2002-278838 01.03.15 G06F12/14,310	ﾒﾓﾘｱｸｾｽ制御ｼｽﾃﾑ、ﾃﾞﾊﾞｲｽ管理装置、ﾊﾟｰﾃｲｼｮﾝ管理装置、ﾒﾓﾘ搭載ﾃﾞﾊﾞｲｽ、およびﾒﾓﾘｱｸｾｽ制御方法、並びにﾌﾟﾛｸﾞﾗﾑ記憶媒体
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 ｱｸｾｽ許可情報	特開2004-102663 02.09.10 G06F15/00,330	ｱｸｾｽ制御ｼｽﾃﾑ、ｱｸｾｽ制御方法、端末装置およびﾈｯﾄﾜｰｸ機器
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｱｸｾｽ制御ｻｰﾊﾞｰ配置	特開2002-014929 00.04.26 G06F15/00,330	ｱｸｾｽ制御ｼｽﾃﾑ、ｱｸｾｽ制御方法、およびﾃﾞﾊﾞｲｽ、ｱｸｾｽ制御ｻｰﾊﾞ、ｱｸｾｽ制御ｻｰﾊﾞ登録ｻｰﾊﾞ、ﾃﾞｰﾀ処理装置、並びにﾌﾟﾛｸﾞﾗﾑ記憶媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰｸﾞﾙｰﾌﾟ	特開2004-013600 02.06.07 G06F15/00,330	ﾃﾞｰﾀ処理ｼｽﾃﾑ、ﾃﾞｰﾀ処理装置、および方法、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2003-132030 (みなし取下) 01.10.24 G06F15/00,330	情報処理装置および方法、記録媒体、並びにﾌﾟﾛｸﾞﾗﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2004-118455 02.09.25 G06F12/14,320	ﾃﾞｰﾀ交換ｼｽﾃﾑ、ﾃﾞｰﾀ交換方法、ﾃﾞｰﾀ交換ﾌﾟﾛｸﾞﾗﾑ、及びﾃﾞｰﾀ交換ﾌﾟﾛｸﾞﾗﾑが記録された記録媒体
			特開2004-015530 02.06.07 H04L12/66	ｱｸｾｽ権限管理ｼｽﾃﾑ、中継ｻｰﾊﾞ、および方法、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
	デバイスの正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2000-322352 99.05.06 G06F13/00,351	情報交換装置、情報交換方法及び情報交換機能を有するﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な情報記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2002-281061 01.03.19 H04L12/56 〔被引用回数 1〕	ﾈｯﾄﾜｰｸｼｽﾃﾑ、接続装置、接続方法、ﾈｯﾄﾜｰｸ、ﾌﾟﾛｸﾞﾗﾑおよび記録媒体

表2.8.4 ソニーの技術要素別課題対応特許（3/5）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 (経過情報) 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
コンテンツフィルタリング技術	情報、個人の正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2001-357013 00.06.15 G06F15/00,330	特定多数向けｺﾝﾃﾝﾂの提供方法、特定多数向けｺﾝﾃﾝﾂ閲覧処理装置および特定多数向けｺﾝﾃﾝﾂ閲覧ｼｽﾃﾑ。
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 各種処理の実行手順 ﾊﾟﾀｰﾝ、ﾙｰﾙの言語記述	特開2004-078507 (みなし取下) 02.08.16 G06F13/00,351	ｱｸｾｽ制御装置及びｱｸｾｽ制御方法、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開2003-186831 (みなし取下) 01.12.13 G06F15/00,310	ﾈｯﾄﾜｰｸｼｽﾃﾑ、情報処理装置および方法、記録媒体、並びにﾌﾟﾛｸﾞﾗﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 自動登録	特開2004-343497 03.05.16 H04L12/28,200	情報処理装置、およびｱｸｾｽ制御処理方法、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼﾙｰﾙの追加、切換 ﾎﾟﾘｼの削除	特開2004-139177 02.10.15 G06F1/00	情報検査方法及び装置、並びにﾌﾟﾛｸﾞﾗﾑ
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2001-136507 99.11.05 H04N7/167	ﾃﾞｰﾀ処理装置およびﾃﾞｰﾀ処理方法、並びに記録媒体
	通信データの中継性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2001-251362 00.03.02 H04L12/66	通信ﾈｯﾄﾜｰｸｼｽﾃﾑ、ｹﾞｰﾄｳｴｲ、およびﾃﾞｰﾀ通信方法、並びにﾌﾟﾛｸﾞﾗﾑ提供媒体
	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2004-336619 03.05.12 H04L12/66	機器間認証ｼｽﾃﾑ及び機器間認証方法、通信機器、並びにｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
	経済性の向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾎﾟﾘｼﾙｰﾙの追加、切換 ﾎﾟﾘｼの削除	特開2004-139177 02.10.15 G06F1/00	情報検査方法及び装置、並びにﾌﾟﾛｸﾞﾗﾑ 概要は技術要素「IPﾌｨﾙﾀﾘﾝｸﾞ」、課題「侵入防御の性能向上」の項参照
ルーティング制御技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開平09-252323 96.12.25 H04L12/56 〔被引用回数 3〕	通信ｼｽﾃﾑ、並びに通信装置および方法
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2004-126715 02.09.30 G06F13/00,351	ﾃﾞｰﾀ交換装置、ﾃﾞｰﾀ交換方法、ﾃﾞｰﾀ交換ﾌﾟﾛｸﾞﾗﾑ及び、ﾃﾞｰﾀ交換ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能なﾌﾟﾛｸﾞﾗﾑ格納媒体

表2.8.4 ソニーの技術要素別課題対応特許（4/5）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞにﾃﾞｰﾀ添付	特開2005-080003 03.09.01 H04L12/66	ｱｸｾｽ制御方法、通信ｼｽﾃﾑ、ｻｰﾊﾞ及び通信端末
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞ-の配置 認証ｻｰﾊﾞ-の配置	WO02-027503 00.09.27 G06F13/00,351	ﾎｰﾑﾈｯﾄﾜｰｸｼｽﾃﾑ
ホスト認証技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2002-152279 00.11.10 H04L12/66 〔被引用回数 1〕	ﾈｯﾄﾜｰｸ接続制御装置及びその方法
	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平08-263384 (みなし取下) 95.03.24 G06F12/14,320	情報処理装置
			特開2005-064683 03.08.08 H04L9/32	情報処理装置および方法、ﾌﾟﾛｸﾞﾗﾑ、並びに記録媒体
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間・期間情報	特開2002-344444 01.05.18 H04L9/32	情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証ｼｽﾃﾑ、記録媒体、並びにﾌﾟﾛｸﾞﾗﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞ-の配置 認証ｻｰﾊﾞ-の配置	特開2003-069559 01.08.23 H04L9/32	ｺﾝﾃﾝﾂ保護ｼｽﾃﾑ及びｺﾝﾃﾝﾂ保護方法
トンネリング技術	デバイスの正当性向上	各種の処理手順改良 特定情報の取得手順 ID情報の取得	特開平06-268639 (拒絶確定) 93.03.16 H04L9/00	通信装置
	中継するデータの機密性向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2004-080645 (みなし取下) 02.08.21 H04L12/66	ﾙｰﾀ装置、閉域網接続方法、閉域網接続ﾌﾟﾛｸﾞﾗﾑ
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特開2001-249899 00.03.07 G06F15/00,330	通信手段を介したｻｰﾋﾞｽ提供ｼｽﾃﾑ、ｻｰﾋﾞｽ提供方法、およびｻｰﾋﾞｽ仲介装置、並びにﾌﾟﾛｸﾞﾗﾑ提供媒体
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞ-の配置 暗号処理ｻｰﾊﾞ-の配置	特開2001-256194 00.03.14 G06F15/00,330	情報提供装置および方法、情報処理装置および方法、並びにﾌﾟﾛｸﾞﾗﾑ格納媒体
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2001-358707 00.06.15 H04L9/10	暗号鍵ﾌﾟﾛﾄｸｸを用いた情報処理ｼｽﾃﾑおよび情報処理方法、並びにﾌﾟﾛｸﾞﾗﾑ提供媒体

表2.8.4 ソニーの技術要素別課題対応特許（5/5）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
トンネリング技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2003-169055 (みなし取下) 01.12.03 H04L12/22	情報通信方法及び情報通信装置、情報通信ｼｽﾃﾑ、並びに記憶媒体
			特開2005-027183 03.07.04 H04L9/14	ｹﾞｰﾄｳｴｲ機器及び暗号方式変換方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2002-374245 01.06.14 H04L9/36	暗号・復号処理方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 鍵情報のﾊﾟｯｸ化	特開平11-355268 (みなし取下) 98.06.09 H04L9/32	情報処理装置および方法、情報処理ｼｽﾃﾑ、並びに提供媒体

2.9 キヤノン

2.9.1 企業の概要

商号	キヤノン　株式会社
本社所在地	〒146-8501　東京都大田区下丸子3-30-2
設立年	1937年（昭和12年）
資本金	1,738億64百万円（2004年12月末）
従業員数	21,300名（2004年12月末）
事業内容	事務機（複写機、スキャナ等のコンピュータ周辺機器、ファクシミリ等の情報・通信機器）、カメラ、光学機器等の開発・製造

トップページで「make it possible with canon」のアイデンティティーを掲げその中で、デジタルネットワークで世界がより狭小になった現在、共生する星の一市民として、キヤノンはどんな貢献ができるのか。社員一人ひとりが自覚を持って、製品やサービス、そこから生まれるソリューション、また環境保全において、イノベーションをめざすために、新たなスローガンを掲げたとある。そこのソリューションにリンクする。

（出典：http://web.canon.jp/solution/index.html）

2.9.2 製品例

ソリューションを支える製品・サービスの中にセキュリティが紹介されている。そのうち不正アクセス侵入検知防御技術に関連した製品やサービスを、表2.9.2に示す。

表2.9.2 キヤノンの不正アクセス侵入検知防御技術に関連する製品例(1/2)

製品名	概要・特徴
セキュリティマネジメント	① ISMSコンサルティングサービス；セキュリティポリシーの策定から各種認証取得、教育や監査といった運用に至るまで、情報セキュリティ対策をサポートするコンサルティングサービス ② Symantec Enterprise Security Manager; セキュリティポリシーに基づく脆弱性の評価と遵守状況の監査をホストベースで行うセキュリティ監査ツール
コンテンツフィルタリング	① GUARDIANWALL; 織内のメールサーバに導入して、送受信記録の保存と、内容のフィルタリングを行う電子メールの情報セキュリティ管理ツール ② GUARDIANWALL ASPサービス；メールに対する内部情報漏洩の監査チェックや送受信メールの保存、メールのウィルスチェックの各機能をASPで提供するサービス ③ GUARDIANAUDIT; サーバーが送受信する電子メールの内容をパケットモニタ方式で監視、内容を分析する電子メールの情報セキュリティ管理ツール ④ WEBGUARDIAN; Web利用におけるアクセスログと外部送信情報を保存し、キーワードによるフィルタリングを行うWebの情報セキュリティ管理ツール

表2.9.2 キヤノンの不正アクセス侵入検知防御技術に関連する製品例(2/2)

製品名	概要・特徴
コンテンツフィルタリング	⑤ URLGUARDIAN; 不適切なWebアクセスを制限したり、利用状況をレポートするURLフィルタリングツール ⑥ PCLGUARDIAN; ファイルアクセス情報およびログオン／ログオフ操作などを記録しアクセス管理を行うクライアント情報セキュリティ管理ツール
ファイアウォール/VPN	① FireWall-1; アクセス・コントロール、攻撃防衛、コンテンツ・セキュリティ認証、NATなどの技術を提供しネットワークを確実に保護するソフトウエア ② VPN-1; インターネットなどの公衆網を仮想的に専用網であるかのように利用するためのセキュリティ製品 ③ Outpost Firewall Pro; 悪質なハッカーによる不正アクセスを防ぎ、個人情報流出などのあらゆる危険からパソコンを保護するファイアウォールソフト ④ CyberGuard; UNIX OSをカーネルレベルで強化したセキュアOSを採用した、ファイアウォール/VPNアプライアンス ⑤ SonicWALL; ファイアウォール・VPNの基本機能に加え、侵入検知/防御、コンテンツフィルタリング等の機能が追加できる、セキュリティ・アプライアンス ⑥ NetScreen; FireWall、VPN、トラフィック管理を統合化したセキュリティシステム ⑦ NGSecureWeb for Linux; ファイアウォール技術とIDS（侵入検知システム）を統合した、Linux Webサーバー(Apache)に対するアプリケーションファイアウォール ⑧ SecureSoft; ファイアウォール・VPNの基本機能に加え、侵入検知/防御等の機能が追加できる、セキュリティ・アプライアンス
不正侵入検知(IDS)/防御(IPS)	① ISS検査サービス；ISS SAFEsuiteを用い、対象ネットワーク及びシステムに対し擬似攻撃をしかけ、その結果をレポート、報告、対処するサービス ② Internet Scanner; ネットワーク上のデバイスの脆弱性を自動的に発見し、改善アドバイスや包括的な傾向分析、リスク管理レポートを提供する脆弱性検査・監査ソリューション ③ RealSecure Network Sensor; 不正アクセスと思われるパケットを発見した際にアラームを表示したり、当該セッションを切断したりする不正侵入検知システム ④ SecureⅡS Web; Microsoft IIS Webサーバーを既知または未知の攻撃から守るセキュリティソフト ⑤ WALL Scanner Web; Webサーバーの脆弱性調査（有無・原因・対策）を自動的におこなうセキュリティ・ツール ⑥ Sourcefire; オープンソースの不正侵入検知ソフトウエア「Snort(TM)」の技術をベースに最適化された、IDSアプライアンス

（出典：http://cweb.canon.jp/solution/product/security/secu-manage.html）

2.9.3 技術開発拠点と研究者

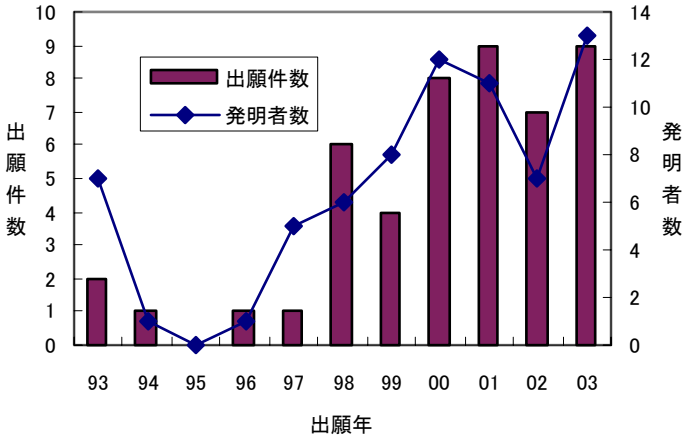
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

図2.9.3に、キヤノンの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の４年間の平均は、出願件数は８件、発明者は11人である。

図2.9.3 キヤノンの不正アクセス侵入検知防御技術に関する出願件数と発明者数



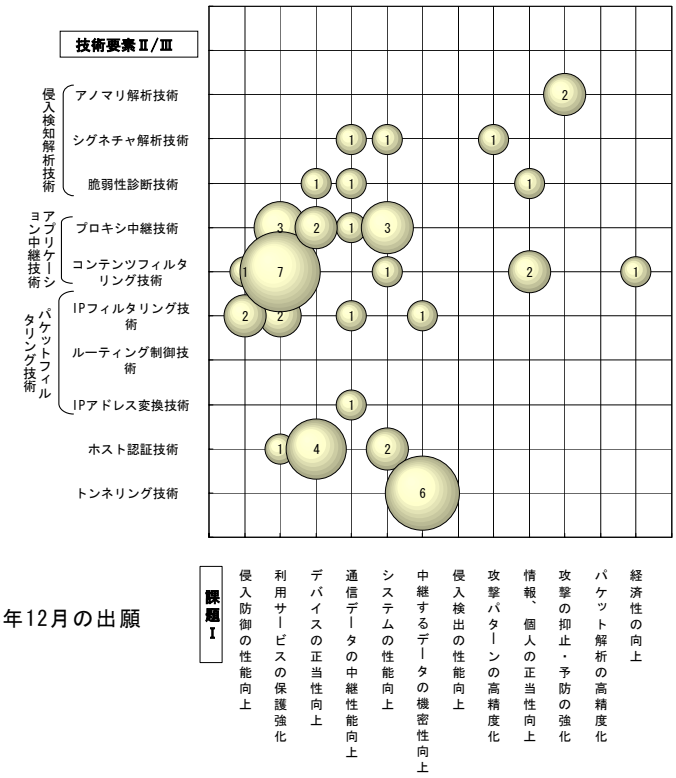
2.9.4 技術開発課題対応特許の概要

図2.9.4-1に、キヤノンの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.9.4-2に、キヤノンの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

コンテンツフィルタリング技術が最も多く出願され、次いでプロキシ中継技術に関する出願が多い。これらの出願のうち、最も多い課題は、「利用サービスの保護強化」である。

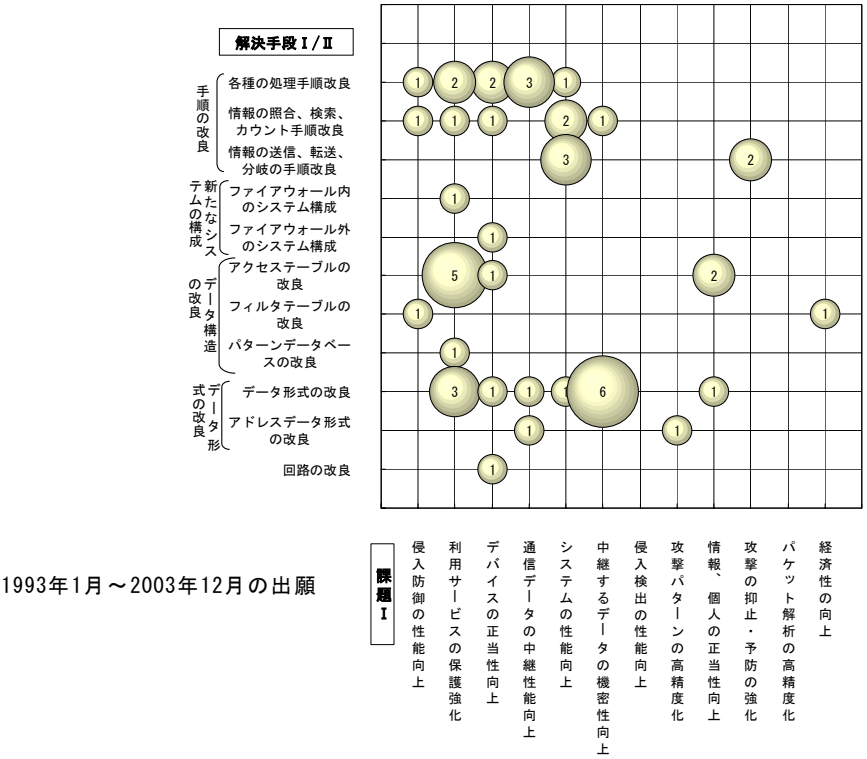
「中継するデータの機密性向上」の課題に対しては、「データ形式の改良」で多く対応している。次いで「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。

図2.9.4-1 キヤノンの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.9.4-2 キヤノンの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.9.4 キヤノンの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は48件で、そのうち３件が登録特許である。なお、表2.9.4では図2.9.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.9.4 キヤノンの技術要素別課題対応特許（1/5）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	攻撃の抑止・予防の強化	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開2004-265310 03.03.04 G06F15/00,330	家庭用ﾈｯﾄﾜｰｸ記憶装置
			特開2004-005030 （みなし取下） 02.05.30 G06F3/12	ﾈｯﾄﾜｰｸ機器及びその制御方法、ｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ
シグネチャ解析技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2004-341922 03.05.16 G06F13/00,353	受信装置、設定装置、接続要求装置、方法、及び、ﾌﾟﾛｸﾞﾗﾑ
	システムの性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特開2003-018235 01.06.29 H04L29/08	通信ｼｽﾃﾑ、通信方法、及び制御ﾌﾟﾛｸﾞﾗﾑ
	攻撃パターンの高精度化	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2004-343533 03.05.16 H04L12/66	受信装置、設定装置、接続要求装置、方法、及び、ﾌﾟﾛｸﾞﾗﾑ
脆弱性診断技術	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開2000-098819 98.09.22 G03G21/00,396	画像処理装置及び画像処理装置制御方法
	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特開2002-135858 00.10.20 H04Q9/00,301 〔被引用回数 2〕	遠隔操作ｼｽﾃﾑ及びその遠隔操作方法、並びに記憶媒体
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-180278 02.11.15 H04L9/32	情報処理装置、ｻｰﾊﾞ装置、電子ﾃﾞｰﾀ管理ｼｽﾃﾑ、情報処理ｼｽﾃﾑ、情報処理方法、ｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ及びｺﾝﾋﾟｭｰﾀ読み取り可能な記憶媒体
プロキシ中継技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2000-125062 98.10.15 H04N1/00,104	ﾃﾞｰﾀ通信ｼｽﾃﾑ及びﾃﾞｰﾀ通信装置及びその制御方法及び記憶媒体
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ﾊﾟﾀｰﾝの廃棄	特開平07-295934 （みなし取下） 94.04.20 G06F15/00,330 〔被引用回数 1〕	情報処理装置及びその制御方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子透かしの埋め込み	特開2001-045275 99.08.03 H04N1/387	ﾈｯﾄﾜｰｸｼｽﾃﾑを構成可能な画像形成装置、ﾃﾞﾊﾞｲｽ端末装置、画像形成ｼｽﾃﾑ、画像形成方法及び記憶媒体

表2.9.4 キヤノンの技術要素別課題対応特許（2/5）

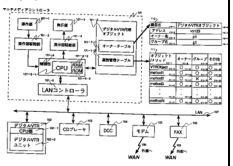
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
プロキシ中継技術	デバイスの正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開2002-041477 00.07.27 G06F15/00,330	ﾈｯﾄﾜｰｸｼｽﾃﾑ、ｺﾝﾋﾟｭｰﾀ接続方法及び装置、及び記録媒体
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ｸｯｷに情報付加	特開2003-108520 01.09.28 G06F15/00,330	情報提供ｻｰﾊﾞ、端末装置及びその制御方法並びに情報提供ｼｽﾃﾑ
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開平11-003307 97.06.13 G06F13/00,357	情報処理装置および方法
	システムの性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 遠隔制御ｺﾏﾝﾄﾞの抽出	特開2002-328887 01.04.27 G06F15/00,310 〔被引用回数 2〕	遠隔操作ｼｽﾃﾑ、遠隔操作方法、被操作装置、操作端末、ﾌﾟﾛｸﾞﾗﾑおよび記憶媒体
			特開2002-328886 01.04.27 G06F15/00,310	遠隔操作ｼｽﾃﾑ、遠隔操作方法、被操作装置、操作端末、ﾌﾟﾛｸﾞﾗﾑおよび記憶媒体
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開2004-240755 03.02.06 G06F15/00,330	表示ｼｽﾃﾑ、表示方法及び記憶媒体
コンテンツフィルタリング技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2003-006064 01.06.25 G06F13/00,351	ｱｸｾｽ規制装置、情報処理装置およびｱｸｾｽ規制ｼｽﾃﾑ
	利用サービスの保護強化	各種の処理手順改良 特定情報の記憶、登録手順 設定情報の記憶	特許3501485 93.12.24 G06F15/00,310	ﾏﾙﾁﾒﾃﾞｨｱ機器の管理ｼｽﾃﾑおよび管理方法  ﾏﾙﾁﾒﾃﾞｨｱ機器と、該ﾏﾙﾁﾒﾃﾞｨｱ機器を管理・制御するﾏﾙﾁﾒﾃﾞｨｱｺﾝﾄﾛｰﾗとを備えたﾏﾙﾁﾒﾃﾞｨｱ機器の管理ｼｽﾃﾑであって、前記ﾏﾙﾁﾒﾃﾞｨｱｺﾝﾄﾛｰﾗと前記ﾏﾙﾁﾒﾃﾞｨｱ機器との間でﾒｯｾｰｼﾞを授受し、当該ﾏﾙﾁﾒﾃﾞｨｱ機器のｵｰﾅｰについては所定の名称を自動設定すると共に、属性については所定のものに自動設定するかあるいは手動で設定する処理手段を具備し、前記属性の内容に応じて当該ﾏﾙﾁﾒﾃﾞｨｱ機器へのｱｸｾｽ権の有無を判別することを特徴とするﾏﾙﾁﾒﾃﾞｨｱ機器の管理ｼｽﾃﾑ。
		各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2002-073554 00.06.12 G06F15/00,330	ﾈｯﾄﾜｰｸｼｽﾃﾑ、Webｻｰﾊﾞへのｱｸｾｽ制限方法、記憶媒体、ﾈｯﾄﾜｰｸﾃﾞﾊﾞｲｽ及びその制御方法、並びにﾌﾟﾛｸﾞﾗﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特開2003-333067 （みなし取下） 02.05.15 H04L12/46	情報処理ｼｽﾃﾑ、情報処理装置およびその処理方法ならびにﾌﾟﾛｸﾞﾗﾑ、記憶媒体
			特開2004-096161 （みなし取下） 02.08.29 H04N1/00	画像処理方法及び画像処理装置及び画像処理装置の制御ﾌﾟﾛｸﾞﾗﾑ及び記憶媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2001-117744 99.10.15 G06F3/12 〔被引用回数 1〕	印刷ｼｽﾃﾑ、印刷方法及び記録媒体
			特開2003-108419 01.09.28 G06F12/00,537	ｻｰﾊﾞ装置及びその制御方法

表2.9.4 キヤノンの技術要素別課題対応特許（3/5）

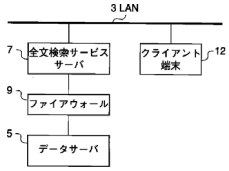
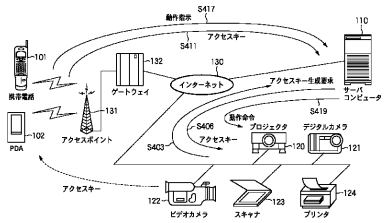
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特許3566478 96.12.27 G06F12/14,520	**文書ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ、文書ｾｷｭﾘﾃｨ管理方法および文書検索装置**  ﾈｯﾄﾜｰｸを介してｸﾗｲｱﾝﾄ端末に接続された文書検索ｻｰﾋﾞｽｻｰﾊﾞと、該文書検索ｻｰﾋﾞｽｻｰﾊﾞを通じて前記ﾈｯﾄﾜｰｸに接続され、文書を蓄積するﾃﾞｰﾀｻｰﾊﾞとを備え、前記文書検索ｻｰﾋﾞｽｻｰﾊﾞは前記ｸﾗｲｱﾝﾄ端末から指定された文字列にしたがって前記ﾃﾞｰﾀｻｰﾊﾞに蓄積されている文書を検索する文書ｾｷｭﾘﾃｨ管理ｼｽﾃﾑにおいて、前記文書検索ｻｰﾋﾞｽｻｰﾊﾞは、ｱｸｾｽ制限文字列およびそのﾊﾟｽﾜｰﾄﾞを設定する設定手段と、検索時、前記ｸﾗｲｱﾝﾄ端末から前記ｱｸｾｽ制限文字列およびそのﾊﾟｽﾜｰﾄﾞの指定がない場合、該ｱｸｾｽ制限文字列を含む文書へのｱｸｾｽを禁止する禁止手段とを備えたことを特徴とする文書ｾｷｭﾘﾃｨ管理ｼｽﾃﾑ。
	システムの性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 ｱｸｾｽ許可情報	特許3610341 02.02.19 H04L12/46	**ﾈｯﾄﾜｰｸ機器及び遠隔制御中継ｻｰﾊﾞ**  ﾈｯﾄﾜｰｸに接続されたﾈｯﾄﾜｰｸ機器を携帯端末から遠隔制御するための遠隔制御中継ｻｰﾊﾞであって、前記遠隔制御を許可するための許可関連情報の生成要求を前記ﾈｯﾄﾜｰｸ機器から受信する第1の受信手段と、前記生成要求に基づいて許可関連情報を生成する生成手段と、前記生成された許可関連情報を前記ﾈｯﾄﾜｰｸ機器に出力させるべく、該生成された許可関連情報を該ﾈｯﾄﾜｰｸ機器に送信する送信手段と、前記許可関連情報を前記携帯端末から受信する第2の受信手段と、前記許可関連情報に対応するﾈｯﾄﾜｰｸ機器を特定する特定手段と、前記特定されたﾈｯﾄﾜｰｸ機器に対して前記携帯端末からの動作指示に基づいた動作命令を発行する発行手段と、を含むことを特徴とする遠隔制御中継ｻｰﾊﾞ。
	情報、個人の正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2004-164415 02.11.14 G06F15/00,330	**ﾛｸﾞｲﾝ制限方法**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2002-207663 01.01.12 G06F13/00,540	**情報管理ｼｽﾃﾑ及び該情報管理ｼｽﾃﾑにおけるｱｸｾｽ管理方法、並びに記憶媒体**
	経済性の向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2003-006064 01.06.25 G06F13/00,351	**ｱｸｾｽ規制装置、情報処理装置およびｱｸｾｽ規制ｼｽﾃﾑ** 概要は技術要素「ｺﾝﾃﾝﾂﾌｨﾙﾀﾘﾝｸﾞ」、課題「侵入防御の性能向上」の項参照
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2005-101741 03.09.22 H04L12/66	**通信装置、方法、機器制御装置、方法、及び、ﾌﾟﾛｸﾞﾗﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開平11-313105 （みなし取下） 98.04.24 H04L12/54	**ｻｰﾊﾞ、ｸﾗｲｱﾝﾄ、ｻｰﾊﾞの制御方法、ｸﾗｲｱﾝﾄの制御方法、ｸﾗｲｱﾝﾄｻｰﾊﾞｼｽﾃﾑおよび記憶媒体**

表2.9.4 キヤノンの技術要素別課題対応特許（4/5）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	利用サービスの保護強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 識別子情報の変換	特開平11-212918 98.01.28 G06F15/00,330	情報処理ｼｽﾃﾑ及び装置及びそれらの方法
			特開平11-205307 （みなし取下） 98.01.16 H04L9/32 〔被引用回数 1〕	情報処理装置及びﾈｯﾄﾜｰｸｼｽﾃﾑ並びにﾘｿｰｽ識別子変換方法及び記憶媒体
	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2003-018181 01.06.29 H04L12/56	通信ｼｽﾃﾑ、通信方法、及び制御ﾌﾟﾛｸﾞﾗﾑ
	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2005-101740 03.09.22 H04L12/56,100	ｾｷｭﾘﾃｨ制御装置
IPアドレス変換技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2005-191646 03.12.24 H04L9/36	遮断装置、匿名公開鍵証明書発行装置、ｼｽﾃﾑ、および、ﾌﾟﾛｸﾞﾗﾑ
ホスト認証技術	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2001-202314 00.01.21 G06F13/00,354	ﾃﾞｰﾀ配信端末装置、ﾃﾞｰﾀ受信端末装置、ﾃﾞｰﾀ通信端末装置、ﾃﾞｰﾀ通信ｼｽﾃﾑ、ﾃﾞｰﾀ通信方法及び記憶媒体
	デバイスの正当性向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2004-054893 02.05.29 G06F15/00,330	画像形成装置の制御方法
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2000-209562 99.01.12 H04N7/16	課金装置、情報伝送ｼｽﾃﾑ、課金方法、及び記憶媒体
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開平07-021127 （取下） 93.06.30 G06F15/00,330	認証確認ｼｽﾃﾑ
		回路の改良 ｽｲｯﾁ回路の追加 無線との切換	特開2001-352330 00.06.07 H04L12/28	通信制御装置
	システムの性能向上	各種の処理手順改良 各種処理の実行手順 並列処理の実行	特開2000-083021 98.09.04 H04L9/32	分散認証のための装置および方法、分散認証ｼｽﾃﾑ、記録媒体
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開2001-251336 00.03.08 H04L12/46	無線ﾃﾞｰﾀ管理装置及び無線ﾃﾞｰﾀ管理ｼｽﾃﾑ

表2.9.4 キヤノンの技術要素別課題対応特許（5/5）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ｱﾄﾞﾚｽの検索	特開2005-167608 03.12.02 H04L12/66	**暗号通信装置､暗号通信方法､ｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ､及びｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2001-245163 99.07.13 H04N1/44	**通信装置および方法ならびに記憶媒体**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ｺﾏﾝﾄﾞに情報付加	特開2004-355471 03.05.30 G06F15/00,330	**不正ｱｸｾｽ防止方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2002-353965 01.05.25 H04L12/22	**出力ｼｽﾃﾑ及び出力ｼｽﾃﾑの制御方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割､仕分け	特開2002-009865 00.06.16 H04L29/04	**ﾃﾞｰﾀ伝送装置､ﾃﾞｰﾀ伝送ｼｽﾃﾑ､ﾃﾞｰﾀ伝送方法および記録媒体**
			特開2002-084318 00.09.08 H04L12/56	**ﾃﾞｰﾀ処理装置､ﾃﾞｰﾀ処理ｼｽﾃﾑ､ﾃﾞｰﾀ処理方法､及び記憶媒体**

2.10 インターナショナル・ビジネス・マシーンズ

2.10.1 企業の概要

社名	International Business Machines Corporation
本社所在地	New Orchard Road, Armonk, NY 10504 U.S.A.
設立年	1911年
資本金	16,269百万米ドル（2003年12月末）
従業員数	319,273名（連結：2003年12月末）
事業内容	コンピュータ関連のサービス、ハード、ソフトの提供

セキュリティやプライバシへの取り組みは、今やビジネスには欠かせないことは周知の事実である。また、強い経営基盤を支えるITにも必須の要素である。セキュリティやプライバシへの対策は、ビジネスにトータル・ソリューションで対応している。（出典：http://www.ibm.com/solutions/jp/）

2.10.2 製品例

ソリューションのうち、セキュリティ/プライバシに紹介されている不正アクセス侵入検知防御技術に関連する製品やサービスを、表2.10.2に示す。

表2.10.2 IBMの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
セキュリティ管理ミドルウエア IBM Tivoli	① IBM Tivoli Access Manager for e-business; インターネット経由のアクセスに対する認証／許可ポリシーの共通フレームワークを提供し、シングル・サインオン環境を実現。 ② IBM Tivoli Access Manager for OS; UNIX® リソースのセキュリティを強化し、不正アクセスを遮断。 ③ IBM Tivoli Identity Manager; ユーザと IT リソースの集中管理によって、管理者負担を軽減。 ④ IBM Tivoli Directory Integrator; アイデンティティ情報に対し、柔軟性に富むデータ同期機能の提供。 ⑤ IBM Tivoli Directory Server; 強力で信頼性の高いディレクトリーの構築を実現。 ⑥ IBM Tivoli Security Compliance Manager; システム内のセキュリティ・ポリシ違反を検出し、事前のリスク対応をサポート。
セキュリティサーバ IBM e-Server	① x-Server;インテル・アーキテクチャー・サーバ ② p-Server;UNIXサーバ・セキュリティ ③ i-Server;統合アプリケーション・サーバ・セキュリティ機能 ④ i-Server;統合アプリケーション・サーバ・セキュリティ・ソリューション ⑤ z-Server;オープン・メインフレーム・サーバ
PCセキュリティ	① PCセキュリティソリューション ② IBMエンベッド・セキュリティ・サブシステム ③ 不正使用の防止；ユーザ認証 ④ IBM Clieent Security Software;認証、データ暗号

（出典：http://www-06.ibm.com/jp/services/security/index.html）

2.10.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

アメリカ合衆国：ニューヨーク州、インディアナ州、カリフォルニア州、コネティカット州
コロラド州、ニューヨーク州、ノースカロライナ州、フロリダ州
ペンシルバニア州

イギリス：オックスフォード

イスラエル：テルアビブ

イタリア：ローマ

インド：カルナータ

カナダ：オンタリオ州トロント

スイス：ウルドルフ、チューリッヒ

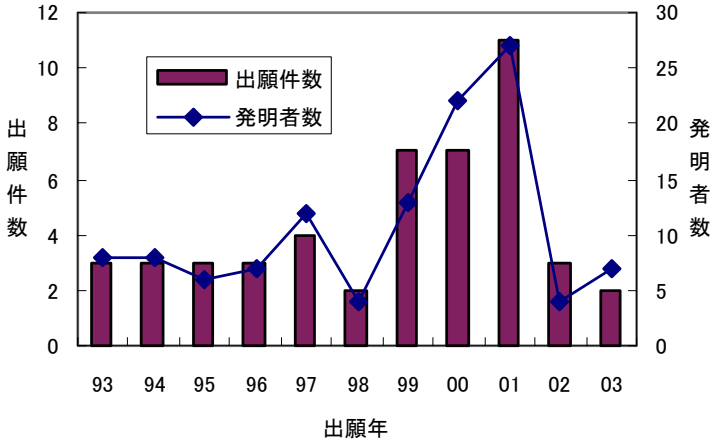
ドイツ：ディー、フランクフルト

フランス：ニース

神奈川県大和市下鶴間1623番地14 日本IBM株式会社 内

図2.10.3に、IBMの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。３年前までの平均は、出願件数が８件、発明者が20人ぐらいであった。

図2.10.3 IBMの不正アクセス侵入検知防御技術に関する出願件数と発明者数



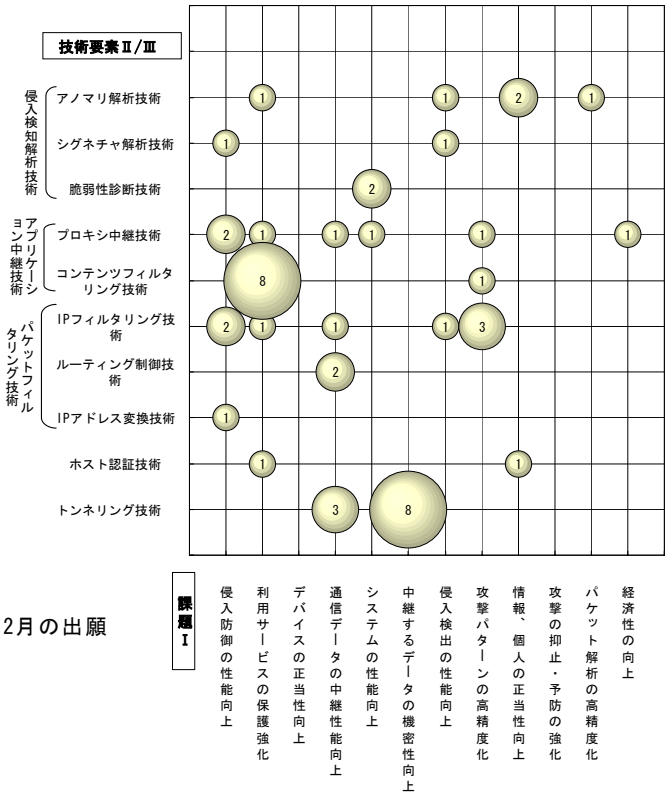
2.10.4 技術開発課題対応特許の概要

図2.10.4-1に、IBMの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.10.4-2に、IBMの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

トンネリング技術が最も多く出願され、次いでコンテンツフィルタリング技術に関する出願が多い。これらの出願のうち、最も多い課題は、「利用サービスの保護強化」であり、次いで多い課題は「中継するデータの機密性向上」である。

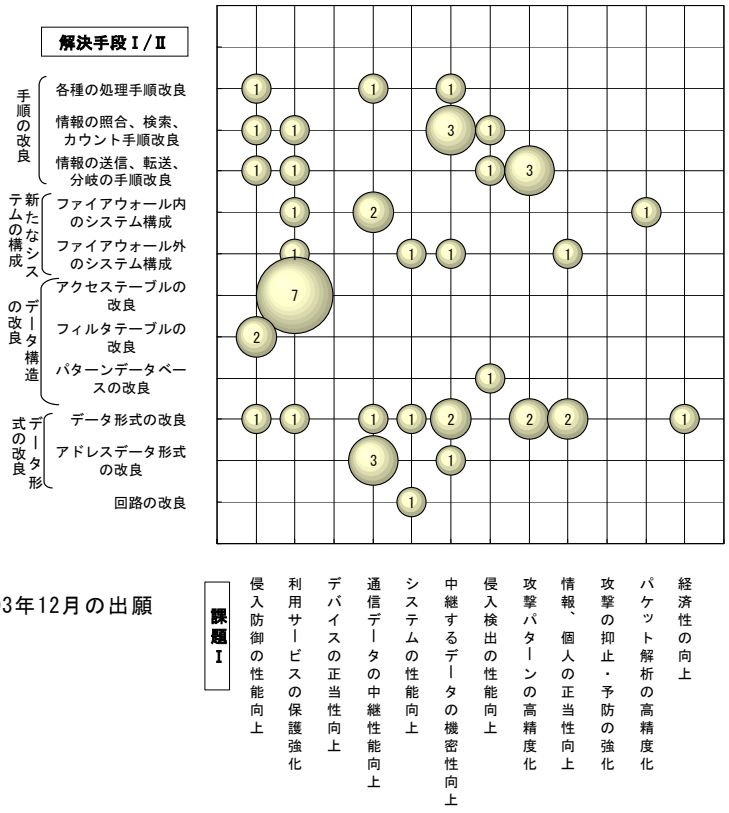
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で多く対応している。

図2.10.4-1 IBMの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.10.4-2 IBMの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.10.4 IBMの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は48件で、そのうち21件が登録特許である。なお、表2.10.4では図2.10.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.10.4 IBMの技術要素別課題対応特許（1/9）

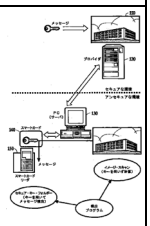
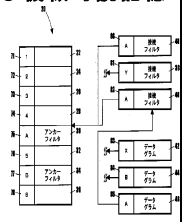
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開2002-342280 （拒絶確定） 01.03.08 G06F15/00,330	**区分処理ｼｽﾃﾑ、区分処理ｼｽﾃﾑにおけるｾｷｭﾘﾃｨを設ける方法、およびそのｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ**
	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 類似度、相関度の算出	特開2004-128733 02.09.30 H04L12/56,400	**通信監視ｼｽﾃﾑ及びその方法、情報処理方法並びにﾌﾟﾛｸﾞﾗﾑ**
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2002-009759 00.03.14 H04L9/18	**ｾｷｭｱ情報を含むWebﾍﾟｰｼﾞを作成する方法及びｼｽﾃﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子透かしの埋め込み	特許3210630 98.10.23 G09C5/00	**付加情報検出方法およびｼｽﾃﾑ**  耐ﾀﾝﾊﾟ性ﾃﾞﾊﾞｲｽおよびｻｰﾊﾞを用いて、ﾃﾞｰﾀに埋め込まれた付加情報を検出するｼｽﾃﾑであって、該ｼｽﾃﾑが、(1)ｻｰﾊﾞが、付加情報の埋め込まれたﾃﾞｰﾀを読み込む手段と、(2)前記ｻｰﾊﾞから、前記ｻｰﾊﾞに接続された耐ﾀﾝﾊﾟ性ﾃﾞﾊﾞｲｽへ、付加情報の埋め込み判定を依頼する手段と、(3)前記耐ﾀﾝﾊﾟ性ﾃﾞﾊﾞｲｽが、該耐ﾀﾝﾊﾟ性ﾃﾞﾊﾞｲｽに内包された秘密鍵を用いて、付加情報の埋め込み判定を行なう手段と、を有することを特徴とする、付加情報検出ｼｽﾃﾑ。
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特開2002-344519 （拒絶確定） 01.03.02 H04L12/56,400	**共用ﾈｯﾄﾜｰｸ・ｼｽﾃﾑにおけるﾙｰﾀを分析するためのｼｽﾃﾑ及び方法**
シグネチャ解析技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの学習	特許3375071 99.01.29 H04L12/56,100	**接続ﾌｨﾙﾀの動的ﾏｲｸﾛ配置方法、ｼｽﾃﾑおよび機械可読記憶媒体**  ﾌｨﾙﾀのｾｯﾄ内に接続ﾌｨﾙﾀを動的に配置する方法であって、ﾎﾟﾘｼｰ・ﾌｨﾙﾀを含めるためにﾌｨﾙﾀ・ｾｯﾄを初期設定するｽﾃｯﾌﾟと、前記接続ﾌｨﾙﾀを前記ﾌｨﾙﾀ・ｾｯﾄ内のﾌｨﾙﾀと順次に突き合わせるｽﾃｯﾌﾟと、前記接続ﾌｨﾙﾀと突き合わせﾎﾟﾘｼｰ・ﾌｨﾙﾀとの一致を検出するのに応答して、少なくとも1つの他の接続ﾌｨﾙﾀが前記突き合わせﾎﾟﾘｼｰ・ﾌｨﾙﾀに対応するか否かを判断し、対応する場合、前記他の接続ﾌｨﾙﾀとの衝突があるか否かを判断するｽﾃｯﾌﾟと、前記他の接続ﾌｨﾙﾀとの衝突がない場合、前記接続ﾌｨﾙﾀを前記ﾌｨﾙﾀ・ｾｯﾄ内の前記突き合わせﾎﾟﾘｼｰ・ﾌｨﾙﾀの前に配置し、衝突がある場合、前記接続ﾌｨﾙﾀを拒否するｽﾃｯﾌﾟとを含む方法。
	侵入検出の性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 攻撃情報の通知	特開2005-135420 03.10.31 G06F13/00,351	**ﾎｽﾄﾍﾞｰｽのﾈｯﾄﾜｰｸ侵入検出ｼｽﾃﾑ、方法、およびｺﾝﾋﾟｭｰﾀ可読媒体**
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰの配置	特開2002-007332 （みなし取下） 00.05.16 G06F15/00,310	**ｺﾝﾋﾟｭｰﾀ・ﾈｯﾄﾜｰｸ上のｺﾝﾋﾟｭｰﾀにｾｷｭﾘﾃｨを提供する方法及びｺﾝﾋﾟｭｰﾀｼｽﾃﾑ**

表2.10.4 IBMの技術要素別課題対応特許（2/9）

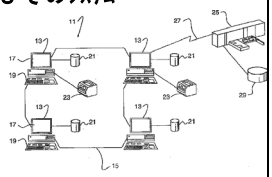
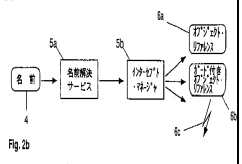
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
脆弱性診断技術	システムの性能向上	回路の改良 ｽｲｯﾁ回路の追加 ﾛｯｸ回路の追加	特許3156820 93.10.07 G06F15/00,330 〔被引用回数 1〕	**ﾛｰｶﾙ･ｴﾘｱ･ﾈｯﾄﾜｰｸのｾｷｭﾘﾃｨ方法及びそのｼｽﾃﾑ**  それぞれが1又は複数のｴﾚﾒﾝﾄを含む複数のﾃﾞｰﾀ処理システムのﾈｯﾄﾜｰｸを遠隔的に安全確保する方法であって、a）ﾎｽﾄ･ﾃﾞｰﾀ処理ｼｽﾃﾑにおいて、ﾈｯﾄﾜｰｸによりﾎｽﾄ･ﾃﾞｰﾀ処理システムと相互接続されたﾀｰｹﾞｯﾄ･ﾃﾞｰﾀ処理ｼｽﾃﾑの組をﾀｰｹﾞｯﾄとするｾｷｭﾘﾃｨ要求を受入れるｽﾃｯﾌﾟと、b）ﾈｯﾄﾜｰｸ上で相互接続された全てのﾃﾞｰﾀ処理ｼｽﾃﾑに対してﾎｽﾄ･ﾃﾞｰﾀ処理ｼｽﾃﾑから前記ｾｷｭﾘﾃｨ要求を通信するｽﾃｯﾌﾟと、c）たﾀｰｹﾞｯﾄ･ﾃﾞｰﾀ処理ｼｽﾃﾑの組においてｾｷｭﾘﾃｨを認識するｽﾃｯﾌﾟと、d）認識されたｾｷｭﾘﾃｨ要求に応答してたﾀｰｹﾞｯﾄ･ﾃﾞｰﾀ処理ｼｽﾃﾑのｴﾚﾒﾝﾄのﾛｯｸ状態を変更するｽﾃｯﾌﾟとを有するﾈｯﾄﾜｰｸを遠隔的に安全確保する方法。
プロキシ中継技術	侵入防御の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特表2003-503963 （拒絶確定） 99.06.30 H04L9/08	**ﾄﾗﾝｽｺｰﾃﾞｨﾝｸﾞ･ﾌﾟﾛｷｼでの複数の起点ｻｰﾊﾞへの動的接続**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開2003-030142 01.03.29 G06F15/00,330	**ﾈｯﾄﾜｰｸ･ｻｰﾊﾞのｾｷｭﾘﾃｨ方法および装置**
	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特許3381927 97.01.17 G06F9/46,360	**分散ｺﾝﾋﾟｭｰﾀ･ｼｽﾃﾑにおいて資源を保護する方法**  資源(2a....2n)、例えば、ﾌｧｲﾙ又は他のｵﾌﾞｼﾞｪｸﾄを未承認のｱｸｾｽから保護するための方法にして、資源は第1ｴﾝﾃｨﾃｨ、即ち、呼出元ｴﾝﾃｨﾃｨ(7)によってｺｰﾙされ、第2ｴﾝﾃｨﾃｨ、即ち、呼出先ｴﾝﾃｨﾃｨ(9)によって供給されるものであり、資源へのｱｸｾｽはｼﾝﾎﾞﾘｯｸ･ﾈｰﾑを使用して呼出元ｴﾝﾃｨﾃｨ(7)によって呼び出され、ｼﾝﾎﾞﾘｯｸ･ﾈｰﾑ全体はｴﾝﾃｨﾃｨに対する仮のﾈｰﾑ･ｽﾍﾟｰｽを形成し、名前解決ﾌﾟﾛｾｽはｵﾌﾞｼﾞｪｸﾄ･ﾘﾌｧﾚﾝｽをｼﾝﾎﾞﾘｯｸ･ﾈｰﾑに割り当て、ｵﾌﾞｼﾞｪｸﾄ･ﾘﾌｧﾚﾝｽ全体は許容された資源を反映するｴﾝﾃｨﾃｨに対する具体的なﾈｰﾑ･ｽﾍﾟｰｽを形成し、後者はｼｽﾃﾑのすべての資源のｻﾌﾞｾｯﾄであり、呼出元ｴﾝﾃｨﾃｨ(7)は、呼出先ｴﾝﾃｨﾃｨ(9)における具体的なﾈｰﾑ･ｽﾍﾟｰｽに対するｱｸｾｽだけを許容される 方法。
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開2003-324484 02.04.26 H04L12/66	**ｾｯｼｮﾝ中継ｼｽﾃﾑ、ｸﾗｲｱﾝﾄ端末、ｾｯｼｮﾝ中継方法、ﾘﾓｰﾄｱｸｾｽ方法、ｾｯｼｮﾝ中継ﾌﾟﾛｸﾞﾗﾑ及びｸﾗｲｱﾝﾄﾌﾟﾛｸﾞﾗﾑ**
	システムの性能向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｵﾌﾞｼﾞｪｸに認証情報埋め込み	特開2003-022253 01.06.26 G06F15/00,330	**ｻｰﾊﾞ、情報処理装置及びそのｱｸｾｽ制御ｼｽﾃﾑ並びにその方法**
	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｵﾌﾞｼﾞｪｸに認証情報埋め込み	特開平11-282753 98.03.06 G06F12/14,320	**ｵﾌﾞｼﾞｪｸﾄへのｱｸｾｽ方法及び装置、ｵﾌﾞｼﾞｪｸﾄへのｱｸｾｽを制御するﾌﾟﾛｸﾞﾗﾑを格納した記憶媒体**

表2.10.4 IBMの技術要素別課題対応特許（3/9）

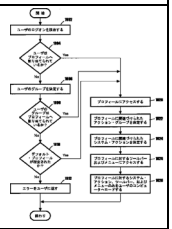
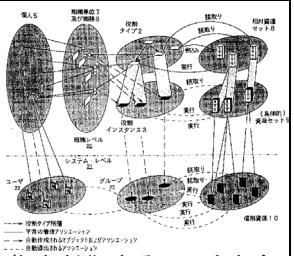
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
プロキシ中継技術	経済性の向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ｵﾌﾞｼﾞｪｸに認証情報埋め込み	特開2003-022253 01.06.26 G06F15/00,330	**ｻｰﾊﾞ、情報処理装置及びそのｱｸｾｽ制御ｼｽﾃﾑ並びにその方法** 概要は技術要素「ﾌﾟﾛｷｼ中継」、課題「ｼｽﾃﾑの性能向上」の項参照
コンテンツフィルタリング技術	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 遠隔制御ｺﾏﾝﾄﾞの抽出	特表2004-533046 01.03.21 G06F15/00,330	**ﾌﾟﾗｸﾞ対応認可ｼｽﾃﾑに対するｻｰﾊﾞｻﾎﾟｰﾄ方法およびｼｽﾃﾑ**
		情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ｾｷｭﾘﾃｨﾚﾍﾞﾙ	特開2003-316650 02.04.18 G06F12/14,310	**ｺﾝﾋﾟｭｰﾀ装置、携帯情報機器、ｾｷｭﾘﾃｨ切り替え方法、およびﾌﾟﾛｸﾞﾗﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特表2000-508153 97.02.14 H04L9/32	**ﾈｯﾄﾜｰｸ･ｺﾝﾋﾟｭｰﾀに関する汎用のﾕｰｻﾞ認証方法**
			特許3611297 99.09.16 G06F15/00,330	**ｾｷｭﾘﾃｨを役割ﾍﾞｰｽで割り振るﾃﾞｰﾀ処理ｼｽﾃﾑ、方法、及びｺﾝﾋﾟｭｰﾀ･ﾌﾟﾛｸﾞﾗﾑ製品** ﾌﾟﾛﾌｨｰﾙ構成によってｾｷｭﾘﾃｨを役割ﾍﾞｰｽで割り振るためﾃﾞｰﾀ処理ｼｽﾃﾑで実現される方法であって、ﾌﾟﾛﾌｨｰﾙを作成し、ﾌﾟﾛﾌｨｰﾙにｱﾌﾟﾘｹｰｼｮﾝを関連づけ、ﾌﾟﾛﾌｨｰﾙに基づいてｱﾌﾟﾘｹｰｼｮﾝの機能性をﾀﾞｳﾝﾛｰﾄﾞすることを含む方法。 
			特表2004-531817 01.04.30 G06F15/177,674	**ｸﾗｽﾀ化ｺﾝﾋﾟｭｰﾀ･ｼｽﾃﾑにおけるｸﾞﾙｰﾌﾟ･ｱｸｾｽ専用化**
			特開2003-050707 01.05.29 G06F9/46,340	**ｳｲﾝﾄﾞｳ･ﾍﾞｰｽのｸﾞﾗﾌｨｶﾙ･ｲﾍﾞﾝﾄを処理する方法およびｼｽﾃﾑ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ･ﾎｽﾄ	特表2003-500923 （拒絶確定） 99.05.21 H04L9/32	**ｾｷｭｱ通信をｲﾆｼｬﾗｲｽﾞし、装置を排他的にﾍﾟｱﾘﾝｸﾞする方法、ｺﾝﾋﾟｭｰﾀ･ﾌﾟﾛｸﾞﾗﾑおよび装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特許3074638 94.08.15 G06F12/14,310 〔被引用回数 2〕	**ｱｸｾｽ制御方法**  ｻﾌﾞｼﾞｪｸﾄ1が少なくとも1つの役割に関連づけられていることを特徴とする、ｺﾝﾋﾟｭｰﾀ･ｼｽﾃﾑ内の少なくとも1つのｵﾌﾞｼﾞｪｸﾄ4に対する少なくとも1つのｻﾌﾞｼﾞｪｸﾄ1のｱｸｾｽ権を制御する方法であって、前記ｻﾌﾞｼﾞｪｸﾄ1の前記役割への所属に応じて前記ｱｸｾｽ権を制御するｽﾃｯﾌﾟを含み、役割ﾀｲﾌﾟ2が提供され、前記役割が役割ｲﾝｽﾀﾝｽ3として表現されることを特徴とし、前記方法が前記役割ﾀｲﾌﾟ2を前記役割ｲﾝｽﾀﾝｽ3にｲﾝｽﾀﾝｽ化するｽﾃｯﾌﾟである前記役割ﾀｲﾌﾟ2から前記役割ｲﾝｽﾀﾝｽ3を導き出す事前ｽﾃｯﾌﾟをさらに含む方法。

表2.10.4 IBMの技術要素別課題対応特許（4/9）

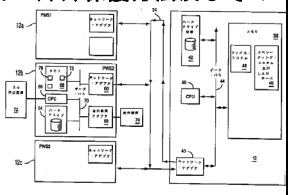
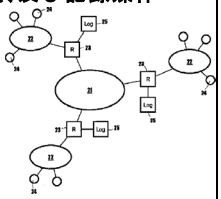
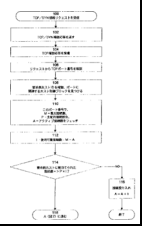
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
コンテンツフィルタリング技術	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 擬似、ﾀﾞﾐﾃﾞｰﾀの送信	特許3466025 95.10.12 G06F15/00,330	**ｺﾝﾋﾟｭｰﾀ・ﾈｯﾄﾜｰｸにおけるﾏｽｶﾚｰﾄﾞ・ｱﾀｯｸ保護方法及びその装置**  ｺﾝﾋﾟｭｰﾀ・ﾈｯﾄﾜｰｸにおいてﾏｽｶﾚｰﾄﾞ・ｱﾀｯｸ保護を行う方法であって、第1のﾏｼﾝによりﾀｲﾑｽﾀﾝﾌﾟと該第1のﾏｼﾝに固有の1又は複数のﾊｰﾄﾞｳｪｱ特性との関数としてｾｯｼｮﾝ・ｷｰを作成するｽﾃｯﾌﾟと、前記ﾈｯﾄﾜｰｸを介して前記ｾｯｼｮﾝ・ｷｰを前記第1のﾏｼﾝから第2のﾏｼﾝへ伝送するｽﾃｯﾌﾟと、前記第2のﾏｼﾝにより前記ﾀｲﾑｽﾀﾝﾌﾟと前記ﾊｰﾄﾞｳｪｱ特性との関数として複数のﾛｯｸを作成するｽﾃｯﾌﾟと、ｾｯｼｮﾝ・ｷｰが前記複数のﾛｯｸの1つに一致するか否かを第2のﾏｼﾝが検査するｽﾃｯﾌﾟと、ｾｯｼｮﾝ・ｷｰが複数のﾛｯｸの1つに一致する場合に第1のﾏｼﾝから第2のﾏｼﾝへのｱｸｾｽを許可するｽﾃｯﾌﾟとを含むﾏｽｶﾚｰﾄﾞ・ｱﾀｯｸ保護方法。
IPフィルタリング技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開平07-250058 （拒絶確定） 94.03.03 H04L9/00	**安全保護装置及びﾃﾞｰﾀ通信ﾈｯﾄﾜｰｸ**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特表2005-513660 01.12.21 G06F15/00,330	**ｲﾝﾀｰﾈｯﾄ上での電子ﾋﾞｼﾞﾈｽ・ﾄﾗﾝｻﾞｸｼｮﾝｾｷｭｱな処理の方法およびｼｽﾃﾑ**
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2000-357176 （拒絶確定） 99.04.30 G06F17/30,414	**ｺﾝﾃﾝﾂ索引付け検索ｼｽﾃﾑ及び検索結果提供方法**
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 機器、ﾓｼﾞｭｰﾙ配置	特開2000-259595 99.03.05 G06F15/177,678 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙ・ｻｰﾊﾞを動的に選択する方法**
	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ﾊﾟｹｯﾄのﾌｨｰﾙﾄﾞ	特許3448254 00.02.02 H04L12/24 〔被引用回数 4〕	**ｱｸｾｽ・ﾁｪｰﾝ追跡ｼｽﾃﾑ、ﾈｯﾄﾜｰｸ・ｼｽﾃﾑ、方法、及び記録媒体**  複数のﾎｽﾄを含む網内の少なくとも一つのﾌｧｲｱｳｫｰﾙに対するｺﾝﾌｨｷﾞｭﾚｰｼｮﾝﾌｧｲﾙを生成する方法であって、ﾎｽﾄがﾊﾟｹｯﾄを送信および受信する能力を指定する複数の役割に対する定義を受信するｽﾃｯﾌﾟ；前記役割の前記網内の前記複数のﾎｽﾄへの割当てを受信するｽﾃｯﾌﾟ；および前記指定された役割に基づいて前記ﾎｽﾄに対する規則を生成するｽﾃｯﾌﾟであって、前記規則がﾊﾟｹｯﾄが宛先ﾎｽﾄに通過できるか否かを決定するものであるｽﾃｯﾌﾟを含むことを特徴とする方法。
	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特許3560553 00.02.11 G06F13/00,351 〔被引用回数 1〕	**ｻｰﾊﾞへのﾌﾗｯﾄﾞ攻撃を防止する方法及び装置**  ﾈｯﾄﾜｰｸ・ｻｰﾊﾞのﾎﾟｰﾄ番号への接続に関して多数のﾘｸｴｽﾄが受信されるｻｰﾊﾞへのﾌﾗｯﾄﾞ攻撃を防ぐ方法であって、ｻｰﾊﾞのﾎﾟｰﾄ番号への接続に対するﾎｽﾄからのﾘｸｴｽﾄに応答して、ﾎｽﾄに割当てられたﾎﾟｰﾄとの接続の数が既定しきい値を超えるかどうかを判定し、超える場合は、接続ﾘｸｴｽﾄを拒否するｽﾃｯﾌﾟを含む、方法。

表2.10.4 IBMの技術要素別課題対応特許（5/9）

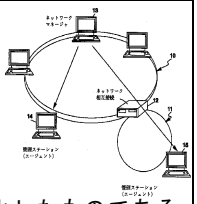
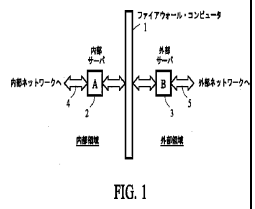
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	攻撃パターンの高精度化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 ある閾値で分岐	特許3560552 00.02.11 G06F13/00,351 〔被引用回数 1〕	**ｻｰﾊﾞへのﾌﾗｯﾄﾞ攻撃を防止する方法及び装置**  ﾈｯﾄﾜｰｸ･ｻｰﾊﾞのﾎﾟｰﾄ番号に対するｷｭｰに配置するため多数のｺﾈｸｼｮﾝﾚｽ･ﾃﾞｰﾀｸﾞﾗﾑが受信されるｻｰﾊﾞへのﾌﾗｯﾄﾞ攻撃を防ぐ方法であって、ｻｰﾊﾞのﾎﾟｰﾄ番号に対するﾎｽﾄからのﾃﾞｰﾀｸﾞﾗﾑの着信に応答して、ﾎﾟｰﾄ番号へのｷｭｰにすでに待機しているﾎｽﾄからのﾃﾞｰﾀｸﾞﾗﾑの数が既定しきい値を超えるかどうかを判定し、超える場合は、ﾃﾞｰﾀｸﾞﾗﾑを破棄するｽﾃｯﾌﾟを含む、方法。
IPフィルタリング技術	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特許2610107 93.08.25 H04L12/42 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸを管理する方法および装置**  通信ﾈｯﾄﾜｰｸにおけるﾈｯﾄﾜｰｸを管理する方法であって、ﾈｯﾄﾜｰｸ管理命令および機密保護ﾌｨｰﾙﾄﾞを含む管理ﾌﾚｰﾑを使用し、上記機密保護ﾌｨｰﾙﾄﾞが、直前の起点のﾀｲﾑｽﾀﾝﾌﾟである第1のｻﾌﾞﾌｨｰﾙﾄﾞと、ﾀｲﾑｽﾀﾝﾌﾟと該管理命令に基づく機能を暗号鍵を使用して暗号化したものである第2のｻﾌﾞﾌｨｰﾙﾄﾞを含み、A）ﾈｯﾄﾜｰｸに管理ﾌﾚｰﾑを送信するｽﾃｯﾌﾟと、B）管理ﾌﾚｰﾑをﾈｯﾄﾜｰｸから受信するｽﾃｯﾌﾟと、C）受信管理ﾌﾚｰﾑに含まれる管理命令およびﾀｲﾑ･ｽﾀﾝﾌﾟを読むｽﾃｯﾌﾟと、D）受信管理ﾌﾚｰﾑに含まれるﾀｲﾑ･ｽﾀﾝﾌﾟおよび管理命令に基づく機能を、暗号鍵を使用して暗号化するｽﾃｯﾌﾟと、E）暗号化ｽﾃｯﾌﾟD）の結果が受信管理ﾌﾚｰﾑの第2のｻﾌﾞﾌｨｰﾙﾄﾞと一致するかどうかを決定するｽﾃｯﾌﾟと、を含む方法。
ルーティング制御技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ｿｹｯﾄの割付	特許3285882 96.10.31 H04L12/66 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙを通過するｺﾝﾋﾟｭｰﾀ資源への外部ｱｸｾｽ**  FIG.1 ﾌｧｲｱｳｫｰﾙが内部領域と外部領域を規定し、外部領域内のｵﾌﾞｼﾞｪｸﾄが内部領域内のｵﾌﾞｼﾞｪｸﾄへのｱｸｾｽを直接開始するのを防止するｾｷｭﾘﾃｨ障壁を形成すると同時に、内部領域内のｵﾌﾞｼﾞｪｸﾄが外部領域内のｵﾌﾞｼﾞｪｸﾄへのｱｸｾｽを直接開始し、ｱｸｾｽを獲得することを許すﾌｧｲｱｳｫｰﾙ(1)を含むﾃﾞｰﾀ通信ﾈｯﾄﾜｰｸのためのﾄﾝﾈﾙ装置であって、ﾌｧｲｱｳｫｰﾙ(1)と外部領域内のｵﾌﾞｼﾞｪｸﾄとの間のｲﾝﾀﾌｪｰｽをとる、外部領域内の外部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀ(3)と、ﾌｧｲｱｳｫｰﾙ(1)と内部領域内のｵﾌﾞｼﾞｪｸﾄとの間のｲﾝﾀﾌｪｰｽをとる、内部領域内の内部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀ(2)と、内部と外部の両方のｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀにおいて、外部領域からのｱｸｾｽが許可されている内部領域内の所定のﾄﾗｽﾃｯﾄﾞ･ｵﾌﾞｼﾞｪｸﾄの識別情報を確認する手段と、外部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀにおいて、外部領域内のｵﾌﾞｼﾞｪｸﾄから送られた要求に応答して、確認手段と協調して、要求がﾄﾗｽﾃｯﾄﾞ･ｵﾌﾞｼﾞｪｸﾄのうちの1つのｵﾌﾞｼﾞｪｸﾄに宛てられたものであるか否かを判断し、要求がそのように宛てられたものである場合、要求を内部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀにﾙｰﾃｨﾝｸﾞする手段と、内部と外部の両方のｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀにおいて、ﾄﾗｽﾃｯﾄﾞ･ｵﾌﾞｼﾞｪｸﾄのうちの1つのｵﾌﾞｼﾞｪｸﾄに宛てられた要求に応答して、ﾄﾗｽﾃｯﾄﾞ･ｵﾌﾞｼﾞｪｸﾄのうちの1つのｵﾌﾞｼﾞｪｸﾄとそれぞれの要求を送った外部ｵﾌﾞｼﾞｪｸﾄとの間のﾃﾞｰﾀ通信接続を形成する手段とを含み、ﾃﾞｰﾀ通信接続のうちの内部領域にあるｾｸﾞﾒﾝﾄとﾌｧｲｱｳｫｰﾙを通って延びるｾｸﾞﾒﾝﾄが内部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀの排他的制御下で形成され、ﾃﾞｰﾀ通信接続のうちの外部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀから要求を送ったｵﾌﾞｼﾞｪｸﾄまでのｾｸﾞﾒﾝﾄが外部ｲﾝﾀﾌｪｰｽ･ｺﾝﾋﾟｭｰﾀの制御下で形成されるﾄﾝﾈﾙ装置。

表2.10.4 IBMの技術要素別課題対応特許（6/9）

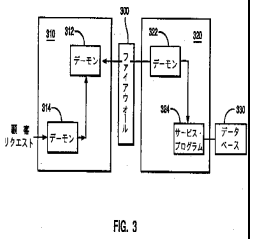
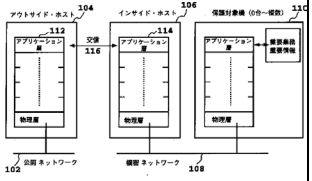
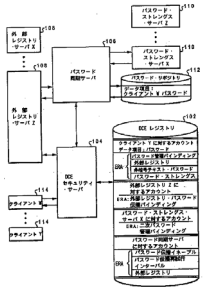
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ｿｹｯﾄの割付	特許3330377 95.10.31 G06F13/00,351	**保護されたｹﾞｰﾄｳｴｲ・ｲﾝﾀｰﾌｪｰｽ**  FIG. 3 内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑ(320)と外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑ(310)との間のｾｷｭﾘﾃｨ・ﾌｧｲｱｳｫｰﾙ(300)に違反することなく内部資源(330)を使用して前記外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑがﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄ(2)を開始することを可能にするように前記内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑに指示するための方法にして、前記内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑと前記外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑとの間の前記内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって開始される接続を認証し、それによって認証済み接続を確立するｽﾃｯﾌﾟ(451)と、前記外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって受け取られたﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄを前記外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって呼び出すｽﾃｯﾌﾟ(461)と、前記ﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄの呼出しに応答して、ﾌﾟﾛｾｽ環境変数を含むｵﾘｼﾞﾅﾙ・ﾌﾟﾛｾｽ環境を前記外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって作成し、ﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄを実行するためにﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄ及びﾌﾟﾛｾｽ環境変数を含むｽﾄﾘﾝｸﾞを作成するｽﾃｯﾌﾟと 認証済み接続を通して内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑに前記ｽﾄﾘﾝｸﾞを外部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって送るｽﾃｯﾌﾟ(435、436、437)と、ﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄを内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって検証するｽﾃｯﾌﾟ(454)と、ｵﾘｼﾞﾅﾙ・ﾌﾟﾛｾｽ環境を内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって再作成するｽﾃｯﾌﾟ(471)と、ﾄﾗﾝｻﾞｸｼｮﾝ・ﾘｸｴｽﾄを内部ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑによって実行し(472)、それによって出力を発生するｽﾃｯﾌﾟ(482)と、を含む方法。
IPアドレス変換技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特許3180054 97.05.16 G06F13/00,351 〔被引用回数 6〕	**ﾈｯﾄﾜｰｸ・ｾｷｭﾘﾃｨ・ｼｽﾃﾑ**  外部のﾈｯﾄﾜｰｸと接続されているｼｽﾃﾑにおいて、外部ﾈｯﾄﾜｰｸとの間でﾍｯﾀﾞ付きﾊﾟｹｯﾄを送受信する第1のｺﾝﾋﾟｭｰﾀと、第1のｺﾝﾋﾟｭｰﾀと専用の通信路で接続されている第2のｺﾝﾋﾟｭｰﾀとを含み、前記第1のｺﾝﾋﾟｭｰﾀは、前記専用通信路を介して前記ﾍｯﾀﾞ付きﾊﾟｹｯﾄからﾍｯﾀﾞを落としたﾊﾟｹｯﾄを第2のｺﾝﾋﾟｭｰﾀに送信し、前記第2のｺﾝﾋﾟｭｰﾀから専用通信路を介した受け取ったﾊﾟｹｯﾄにﾍｯﾀﾞを付加して外部ﾈｯﾄﾜｰｸに対して送信することを特徴とするﾈｯﾄﾜｰｸ・ｾｷｭﾘﾃｨ・ｼｽﾃﾑ。
ホスト認証技術	利用サービスの保護強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2001-282105 （拒絶確定） 00.03.27 G09C1/00,640	**電子ｺﾝﾃﾝﾂの証明方法、ｼｽﾃﾑおよびﾌﾟﾛｸﾞﾗﾑが記録された媒体**
	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特許3426091 95.11.13 G06F15/00,330	**ﾊﾟｽﾜｰﾄﾞ同期を与えるｼｽﾃﾑ**  ﾒｲﾝ・ﾃﾞｰﾀ記憶装置及び複数の二次ﾃﾞｰﾀ記憶装置の間にﾊﾟｽﾜｰﾄﾞ同期を与えるﾈｯﾄﾜｰｸ・ｼｽﾃﾑ・ｻｰﾊﾞにして、ﾒｲﾝ・ﾃﾞｰﾀ記憶装置に接続されたｾｷｭﾘﾃｨ・ｻｰﾊﾞと、ｾｷｭﾘﾃｨ・ｻｰﾊﾞに接続され、ﾒｲﾝ・ﾃﾞｰﾀ記憶装置をｱｸｾｽするための複数のｸﾗｲｱﾝﾄであって、各々が固有の修正可能なﾊﾟｽﾜｰﾄﾞを維持するものと、ｾｷｭﾘﾃｨ・ｻｰﾊﾞ及び複数の二次ﾃﾞｰﾀ記憶装置に接続され、ﾕｰｻﾞが複数の二次ﾃﾞｰﾀ記憶装置の間で単一の固有のﾊﾟｽﾜｰﾄﾞを維持することができるよう複数のｸﾗｲｱﾝﾄの1つと関連するﾕｰｻﾞから二次ﾃﾞｰﾀ記憶装置の各々にﾊﾟｽﾜｰﾄﾞ伝播同期を与えるﾊﾟｽﾜｰﾄﾞ同期ｻｰﾊﾞと、を含むﾈｯﾄﾜｰｸ・ｼｽﾃﾑ・ｻｰﾊﾞ。

表2.10.4 IBMの技術要素別課題対応特許（7/9）

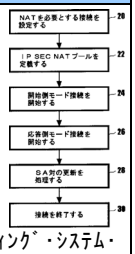
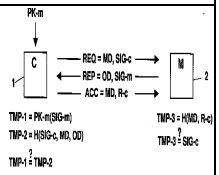
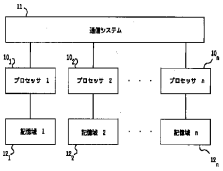
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ併用	特許3393836 99.01.29 H04L12/46 〔被引用回数 1〕	**仮想ﾌﾟﾗｲﾍﾞｰﾄ･ﾈｯﾄﾜｰｸの動作方法およびｼｽﾃﾑ**  ﾈｯﾄﾜｰｸ･ｱﾄﾞﾚｽ変換(NAT)をIP Sec処理と統合するIP Secに基づく仮想ﾌﾟﾗｲﾍﾞｰﾄ･ﾈｯﾄﾜｰｸ(VPN)を動作させる方法であって、NAT IPｱﾄﾞﾚｽ･ﾌﾟｰﾙを設定するｽﾃｯﾌﾟと、NAT IPｱﾄﾞﾚｽ･ﾌﾟｰﾙを使用するためにVPN接続を設定するｽﾃｯﾌﾟと、NAP IPｱﾄﾞﾚｽ･ﾌﾟｰﾙから特定のIPｱﾄﾞﾚｽを入手し、特定のIPｱﾄﾞﾚｽをVPN接続に割り振るｽﾃｯﾌﾟと、VPN接続を開始するｽﾃｯﾌﾟと、ｵﾍﾟﾚｰﾃｨﾝｸﾞ･ｼｽﾃﾑ･ｶｰﾈﾙにVPN接続のためのｾｷｭﾘﾃｨ･ｱｿｼｴｰｼｮﾝと接続ﾌｨﾙﾀをﾛｰﾄﾞするｽﾃｯﾌﾟと、VPN接続のためのIPﾃﾞｰﾀｸﾞﾗﾑを処理するｽﾃｯﾌﾟと、IPﾃﾞｰﾀｸﾞﾗﾑにVPN NATを適用するｽﾃｯﾌﾟとを含む方法。
トンネリング技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特許3346772 96.01.12 H04L9/32	**ﾈｯﾄﾜｰｸにおける安全な匿名情報交換**  Fig.2B 例えば入札またはｵｰｸｼｮﾝなど送信側と受信側の間での匿名の証明可能な情報交換の方法であって、送信側Cが主題または商品の説明MDおよびCのﾃﾞｨｼﾞﾀﾙ署名SIG-cのあるｵﾌｧｰ要求REQREQ=(MD,SIG-c)を作成するｽﾃｯﾌﾟと、REQが匿名通信ﾁｬﾈﾙ経由で少なくとも1つの受信側Mに送信されるｽﾃｯﾌﾟと- 受信側Mがｵﾌｧｰの説明ODと、少なくともMD、OD、SIG-cのうちの1つを含む選択された情報に関して計算されたﾃﾞｨｼﾞﾀﾙ署名SIG-mとを備えた応答REPREP=(OD,SIG-m)を作成し、任意選択でさらにMの公開ｷｰPK-mまたは公開ｷｰ証明書Cert-mを含ませるｽﾃｯﾌﾟと、送信側Cが応答REPを受信すると、既知の、送信された、または公開ｷｰ証明書Cert-mから抽出されたMの公開ｷｰPK-mを使って受信SIG-mを暗号化して第1の一時値TMP-1TMP-1=PK-m(SIG-m)を決定するｽﾃｯﾌﾟと、署名SIG-mの基になっている選択された情報の連結を計算して、第2の一時値TMP-2TMP-2=H(SIG-c/MD/OD)を決定するｽﾃｯﾌﾟとを含み、- これによって一時値TMP-1と一時値TMP-2が一致するとｵﾌｧｰの真正性が示される方法。
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2003-018142 01.06.20 H04L9/08	**情報の提供方法、情報の提供ｼｽﾃﾑおよびﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	各種の処理手順改良 特定情報の取得手順 設定情報の取得	特開平10-200530 96.12.23 H04L12/24 〔被引用回数 2〕	**管理方法およびｼｽﾃﾑ**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間･期間情報	特許3024053 94.03.01 H04L9/08	**通信における安全保護のための方法**  ﾌﾟﾛｾｯｻ用の記憶域から古い秘密ｷｰを読み取る段階と、記憶域から読み取った古い秘密ｷｰに基づいて、各ﾌﾟﾛｾｯｻごとに中間値を計算する段階と、計算した中間値を、1組のｻｰﾊﾞのうちの対応するｻｰﾊﾞに伝送する段階と、1組のｻｰﾊﾞにおいて他のｻｰﾊﾞから中間値を受け取る段階と、受け取った中間値を使って新しい秘密ｷｰを計算する段階と、計算された新しい秘密ｷｰを、ﾌﾟﾛｾｯｻ用の記憶域に記憶する段階と、その後に記憶域から古い秘密ｷｰを消去する段階と、を含む方法。

表2.10.4 IBMの技術要素別課題対応特許（8/9）

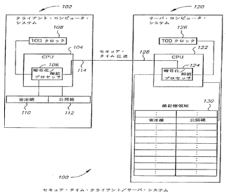
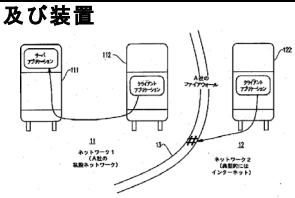
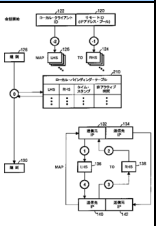
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
トンネリング技術	中継するデータの機密性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間・期間情報	特許2628619 93.07.22 G06F1/00,370	**ｾｷｭｱ・ﾀｲﾑｷｰﾋﾟﾝｸﾞ装置およびｾｷｭｱ・ﾀｲﾑ・ｻｰﾊﾞ**  物理的に安全確保されたﾊﾟｯｹｰｼﾞ内に設置された中央演算処理装置と電子記憶装置とを含むｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑにおいて用いるｾｷｭｱ(安全確保された)・ﾀｲﾑｷｰﾋﾟﾝｸﾞ装置であって、時刻伝送及び日付伝送を暗号化しかつ解読するために専用鍵を識別するときに用いる公開鍵を保有する公開鍵ﾚｼﾞｽﾀと、前記専用鍵を保有する専用鍵ﾚｼﾞｽﾀと、前記専用鍵を用いて暗号化された時刻及び日付の情報を受信する入力と、前記専用鍵を用いて受信された時刻及び日付の情報を解読するﾃﾞｰﾀ解読手段と、前記解読された時刻及び日付の情報を受信するための入力及び暗号化されていない時刻及び日付の情報を与えるための出力を備え、時刻ｸﾛｯｸと日付ｶﾚﾝﾀﾞｰとを含む日時(time-of-day:TOD)ｸﾛｯｸとを有するｾｷｭｱ・ﾀｲﾑｷｰﾋﾟﾝｸﾞ装置。
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特開2002-304335 01.01.16 G06F13/00,353	**通信方法、通信ｼｽﾃﾑ、通信のためのﾌﾟﾛｸﾞﾗﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特許3489988 97.03.28 H04L12/56 〔被引用回数 3〕	**ｾｷｭﾘﾃｨ保護通信ﾄﾝﾈﾘﾝｸﾞの方法及び装置**  ｻｰﾊﾞ・ｱﾌﾟﾘｹｰｼｮﾝを稼働させる少なくとも1つのｻｰﾊﾞを含む第1のﾈｯﾄﾜｰｸと、ｸﾗｲｱﾝﾄ・ｱﾌﾟﾘｹｰｼｮﾝを稼働させる少なくとも1つのｸﾗｲｱﾝﾄを含む第2のﾈｯﾄﾜｰｸと、第1のﾈｯﾄﾜｰｸと第2のﾈｯﾄﾜｰｸのうちの一方のﾈｯﾄﾜｰｸのｺﾝﾋﾟｭｰﾀ資源を保護し、第1のﾌｧｲｱｳｫｰﾙが第1のﾌｧｲｱｳｫｰﾙの内部から外部への接続を行うことができるようにするｿﾌﾄｳｪｱ・ｱﾌﾟﾘｹｰｼｮﾝを含む、第1のﾌｧｲｱｳｫｰﾙと、相互にｱﾄﾞﾚｽ可能なｻｰﾊﾞ終端ﾌﾟﾛｷｼ及びｻｰﾊﾞ・ｱﾌﾟﾘｹｰｼｮﾝと、相互にｱﾄﾞﾚｽ可能なｸﾗｲｱﾝﾄ終端ﾌﾟﾛｷｼ及びｸﾗｲｱﾝﾄ・ｱﾌﾟﾘｹｰｼｮﾝと、第1のﾌｧｲｱｳｫｰﾙの外部にあり、第1のﾈｯﾄﾜｰｸと第2のﾈｯﾄﾜｰｸの間の非信頼ﾈｯﾄﾜｰｸ内にある中間ﾌﾟﾛｷｼとを含み、ｻｰﾊﾞ終端ﾌﾟﾛｷｼとｸﾗｲｱﾝﾄ終端ﾌﾟﾛｷｼがそれぞれ第1のﾌｧｲｱｳｫｰﾙを介して中間ﾌﾟﾛｷｼとの接続を行い、中間ﾌﾟﾛｷｼがｻｰﾊﾞ終端ﾌﾟﾛｷｼからの接続とｸﾗｲｱﾝﾄ終端ﾌﾟﾛｷｼからの接続とを接続してｸﾗｲｱﾝﾄとｻｰﾊﾞの間にﾊﾟｽ・ｽﾙｰ通信ﾄﾝﾈﾙを確立する、ﾊﾟｹｯﾄ交換ﾈｯﾄﾜｰｸ通信ｼｽﾃﾑ。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2005-174304 03.11.12 G06F17/60	**電子取引において収集されたﾌﾟﾗｲﾊﾞｼｰ・ﾎﾟﾘｼｰをﾃﾞｨｼﾞﾀﾙ的に検証するための方法、ｼｽﾃﾑ、およびｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開2003-132021 01.08.30 G06F15/00,330	**機構に無関係のｸﾗｽﾀ・ｾｷｭﾘﾃｨ・ｻｰﾋﾞｽを提供する方法**

表2.10.4 IBMの技術要素別課題対応特許（9/9）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
トンネリング技術	中継するデータの機密性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特許3636095 00.05.23 H04L12/56 〔被引用回数 1〕	**VPN接続のｾｷｭﾘﾃｨ**  ﾈｯﾄﾜｰｸ･ｱﾄﾞﾚｽ変換(NAT)とIPｾｷｭﾘﾃｨ(IPSec)処理とを統合するIPSecに基づいて、仮想私設網(VPN)を操作する方法であって、NAT IPｱﾄﾞﾚｽ･ﾌﾟｰﾙを構成するｽﾃｯﾌﾟと、前記NAT IPｱﾄﾞﾚｽ･ﾌﾟｰﾙを使用するようにVPN接続を構成するｽﾃｯﾌﾟと、前記NAT IPｱﾄﾞﾚｽ･ﾌﾟｰﾙから特定のIPｱﾄﾞﾚｽを取得し、その特定のIPｱﾄﾞﾚｽを前記VPN接続に割り当てるｽﾃｯﾌﾟと、前記VPN接続を開始するｽﾃｯﾌﾟと、前記VPN接続用のｾｷｭﾘﾃｨ連合および接続ﾌｨﾙﾀをｵﾍﾟﾚｰﾃｨﾝｸﾞ･ｼｽﾃﾑのｶｰﾈﾙにﾛｰﾄﾞするｽﾃｯﾌﾟと、前記VPN接続に対してIPﾃﾞｰﾀｸﾞﾗﾑを処理するｽﾃｯﾌﾟと、前記IPﾃﾞｰﾀｸﾞﾗﾑにVPN NATを適用するｽﾃｯﾌﾟとを備えた方法。

2.11 富士ゼロックス

2.11.1 企業の概要

商号	富士ゼロックス　株式会社
本社所在地	〒107-0052　東京都港区赤坂2-17-22　赤坂ツインタワー東館
設立年	1962年（昭和37年）
資本金	200億円（2005年3月末）
従業員数	14,413名（2005年3月末）（連結：36,396名）
事業内容	オフィス機器（複写機、プリンター等）の製造・販売、ソリューション・ドキュメント処理サービスの提供、教育プログラム・教材の開発・制作・販売、他

ドキュメントという企業の中でも最も付加価値の高い情報資産の機密性、完全性および可用性を確保し維持するためには、紙と電子をシームレスにマネジメントすることを前提に、ドキュメント・ライフサイクルの各場面に応じたセキュリティ対策が必要である。富士ゼロックスでは、4つの視点による技術的対策アプローチを組み合わせることにより、ドキュメント・ライフサイクル上での最適なセキュリティ・ソリューションを提案している。(出典：http://www.fujixerox.co.jp/solution/security/index.html)

2.11.2 製品例

セキュリティ・ソリューションでの４つの視点は、コンサルティング、ネットワーク支援、ドキュメントセキュリティと運用監視支援であるとしている。これらのソリューションの中から、不正アクセス侵入検知防御技術に関係する製品やサービスを表2.11.2に示す。

表2.11.2 富士ゼロックスの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
セキュアなネットワークインフラ構築支援ソリューション	①　超高速ファイアウォールシステム；通信量の増加と共にネットワークインフラ機器の重要性が上がり、帯域の増加に伴う機器のパフォーマンス不足に対処。 ②　SSL-VPNシステム；セキュアなリモートアクセス環境の提供。 ③　社外取引先情報共有システム；文書管理システムとVPNの組合せ。
セキュリティ検査/監視ソリューション	①　ネットワークセキュリティ監視システム；24時間365日のネットワーク監視と、疑わしいログ発見時にアナリスト解析。 ②　ネットセキュリティ検査サービス；ツールや擬似ハッキングを使用して安全性の検査。

(出典：http://www.fujixerox.co.jp/solution/security/solution/infra.html)

2.11.3 技術開発拠点と研究者

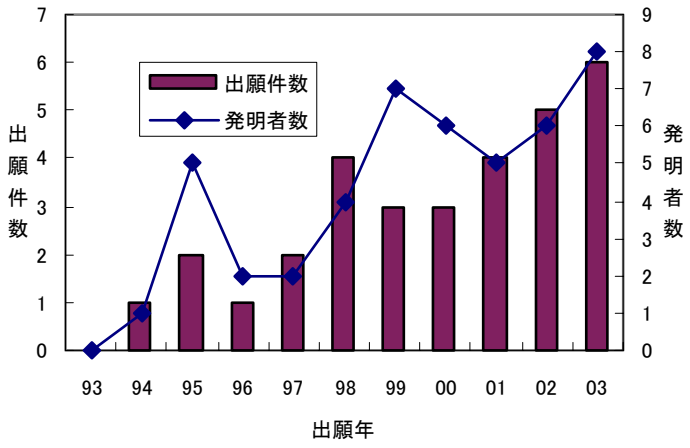
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都港区赤坂2丁目17番22号 富士ゼロックス株式会社内
神奈川県海老名市本郷2274番地 富士ゼロックス株式会社内
神奈川県川崎市高津区坂戸3丁目2番1号 ＫＳＰ Ｒ＆Ｄ富士ゼロックス株式会社内
神奈川県足柄上郡中井町境430 グリーンテクなかい 富士ゼロックス株式会社内
埼玉県岩槻市府内3丁目7番1号 富士ゼロックス株式会社岩槻事業所内

図2.11.3に、富士ゼロックスの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の３年間で、出願件数は増加傾向で03年には６件あり、発明者数は８人である。

図2.11.3 富士ゼロックスの不正アクセス侵入検知防御技術に関する出願件数と発明者数



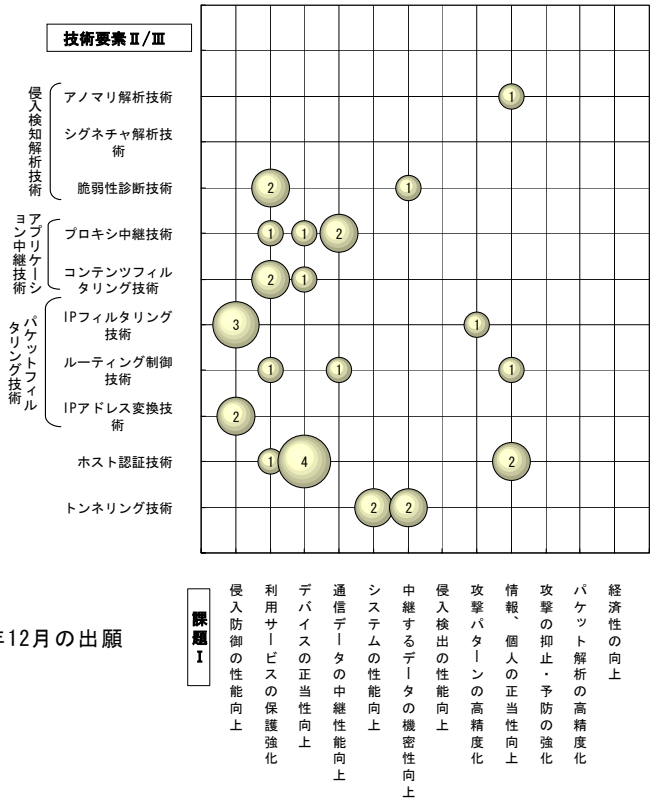
2.11.4 技術開発課題対応特許の概要

図2.11.4-1に、富士ゼロックスの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.11.4-2に、富士ゼロックスの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

ホスト認証技術に関する出願が多い。これらの出願のうち、最も多い課題は、「利用サービスの保護強化」であり、次いで多い課題は「デバイスの正当性向上」である。

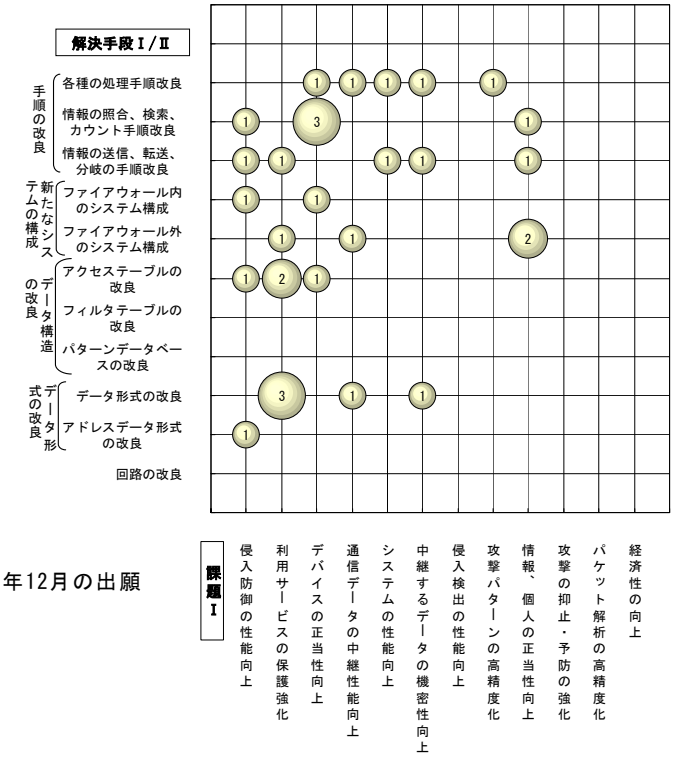
「利用サービスの保護強化」の課題に対しては、「データ形式の改良」で３件対応している。さらに「デバイスの正当性向上」の課題に対しては、「情報の照合、検索、カウント手順改良」で３件対応している。

図2.11.4-1 富士ゼロックスの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.11.4-2 富士ゼロックスの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.11.4 富士ゼロックスの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は31件で、そのうち４件が登録特許である。なお、表2.11.4では図2.11.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.11.4 富士ゼロックスの技術要素別課題対応特許（1/4）

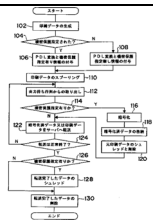
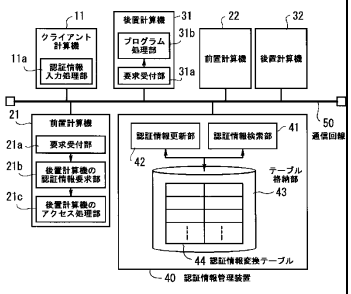
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
アノマリ解析技術	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2002-351836 01.05.30 G06F15/00,330	**固有ﾃﾞｰﾀ発行装置および方法**
脆弱性診断技術	利用サービスの保護強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-151897 02.10.29 G06F15/00,330	**ｼﾞｮﾌﾞ処理制御装置及びｼﾞｮﾌﾞ処理制御方法**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-151896 02.10.29 G06F15/00,330	**ｼﾞｮﾌﾞ処理制御装置及びｼﾞｮﾌﾞ処理制御方法**
	中継するデータの機密性向上	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特許3379411 97.11.10 G06F3/12	**ﾌﾟﾘﾝﾀｻｰﾊﾞ、及びﾌﾟﾘﾝﾀ**  ﾈｯﾄﾜｰｸを介して互いに接続されたｸﾗｲｱﾝﾄ装置、ﾌﾟﾘﾝﾄｻｰﾊﾞ及びﾌﾟﾘﾝﾀを含んで構成され、前記ｸﾗｲｱﾝﾄ装置から転送された印刷ﾃﾞｰﾀが前記ﾌﾟﾘﾝﾄｻｰﾊﾞで一旦受信された後ﾌﾟﾘﾝﾀへ転送され、又は前記ｸﾗｲｱﾝﾄ装置からの印刷ﾃﾞｰﾀが前記ﾌﾟﾘﾝﾀへ直接転送され、該ﾌﾟﾘﾝﾀが受信した印刷ﾃﾞｰﾀを印刷するﾈｯﾄﾜｰｸｼｽﾃﾑであって、前記ｸﾗｲｱﾝﾄ装置は、機密保護対象とする印刷ﾃﾞｰﾀを指定するための機密保護指定手段と、前記機密保護指定手段により機密保護対象として指定された印刷ﾃﾞｰﾀに、機密保護対象を示す機密属性情報を付加する情報付加手段と、前記属性情報付加手段により機密属性情報が付加された印刷ﾃﾞｰﾀを、該印刷ﾃﾞｰﾀが不要となった時点で判読不能なﾃﾞｰﾀに加工する第1の加工手段と、を有し、前記ﾌﾟﾘﾝﾀ及び前記ﾌﾟﾘﾝﾄｻｰﾊﾞの各々は、受信した印刷ﾃﾞｰﾀに機密属性情報が付加されているか否かを判定する判定手段と、前記判定手段により機密属性情報が付加されていると判定された印刷ﾃﾞｰﾀを、該印刷ﾃﾞｰﾀが不要となった時点で判読不能なﾃﾞｰﾀに加工する第2の加工手段と、を有するﾈｯﾄﾜｰｸｼｽﾃﾑ。
プロキシ中継技術	利用サービスの保護強化	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 容疑ﾚﾍﾞﾙ、悪性閾値	特開平10-232844 （拒絶確定） 97.02.19 G06F13/00,354	**情報処理装置**
	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特許3137173 95.07.20 G06F13/00,357 〔被引用回数 1〕	**認証情報管理装置**  ｸﾗｲｱﾝﾄ計算機と、ｸﾗｲｱﾝﾄ計算機から直接ｱｸｾｽされる前置計算機と、ｸﾗｲｱﾝﾄ計算機から前記前置計算機を介して間接的にｱｸｾｽされる後置計算機とがﾈｯﾄﾜｰｸで接続された計算機ｼｽﾃﾑにて、認証情報を管理する認証情報管理装置であって、前記後置計算機毎にﾕｰｻﾞに対応した認証情報を記憶する記憶手段と、前記前置計算機のｱｸｾｽ後に当該前置計算機を介して間接的に後置計算機をｱｸｾｽする際に受け取る当該後置計算機の識別情報とﾕｰｻﾞ情報とを基に前記記憶手段から該当する後置計算機の認証情報を検索する検索手段と、前記検索手段で検索された認証情報を当該前置計算機に返信する通信手段と、を具備することを特徴とする認証情報管理装置。

表2.11.4 富士ゼロックスの技術要素別課題対応特許（2/4）

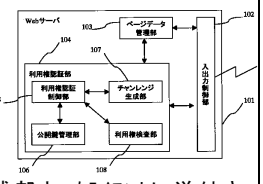
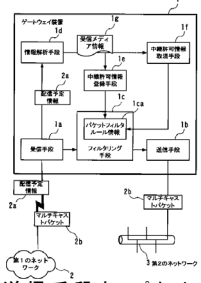
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ｱｸｾｽ制御ｻｰﾊﾞｰの配置	特開2003-008661 01.06.19 H04L12/66	**ﾈｯﾄﾜｰｸ接続中継制御方法および装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2005-182623 03.12.22 G06F12/00,546	**文書収集装置、文書収集方法及びﾌﾟﾛｸﾞﾗﾑ**
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開2004-287912 03.03.24 G06F15/00,330	**処理ｻｰﾋﾞｽ提供装置**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特開2004-151163 02.10.28 G09C1/00,660	**文書管理ｼｽﾃﾑおよび方法、機密化装置および方法並びにﾌﾟﾛｸﾞﾗﾑ、閲覧装置および方法並びにﾌﾟﾛｸﾞﾗﾑ**
	デバイスの正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特許3593979 01.01.11 G06F15/00,330	**利用権制御を伴うｻｰﾊﾞおよびｸﾗｲｱﾝﾄならびにｻｰﾋﾞｽ提供方法および利用権証明方法**  ｻｰﾊﾞが提供するｻｰﾋﾞｽ毎に割り当てられた公開鍵を記憶する公開鍵記憶部と、ｸﾗｲｱﾝﾄからのｻｰﾋﾞｽ要求を受けた際に、ｻｰﾊﾞからｸﾗｲｱﾝﾄに対して送付するﾁｬﾚﾝｼﾞを生成するﾁｬﾚﾝｼﾞ生成部と、ｸﾗｲｱﾝﾄに送付されたﾁｬﾚﾝｼﾞと、ﾁｬﾚﾝｼﾞに対してｸﾗｲｱﾝﾄから送り返されたﾚｽﾎﾟﾝｽとが所定の関係にあることを公開鍵を使って検査する利用権認証部とを備え、ｻｰﾊﾞが提供するｻｰﾋﾞｽに対するｸﾗｲｱﾝﾄの利用権を認証する際に、ｸﾗｲｱﾝﾄに対してﾁｬﾚﾝｼﾞ生成部で生成されたﾁｬﾚﾝｼﾞを送付し、ｸﾗｲｱﾝﾄからから送り返されたﾁｬﾚﾝｼﾞに対するﾚｽﾎﾟﾝｽを受け取り、利用権検査部で、そのﾁｬﾚﾝｼﾞとﾚｽﾎﾟﾝｽとが所定の関係にあることを、公開鍵記憶部に記憶されたｻｰﾋﾞｽに割り当てられた公開鍵を使用して検査し、検査に成功した場合にのみ該ｻｰﾋﾞｽをｸﾗｲｱﾝﾄに提供することを特徴とするｻｰﾊﾞ。
IPフィルタリング技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間･期間情報	特許3656418 98.07.15 H04L12/56,260	**ｹﾞｰﾄｳｪｲ装置及びﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄ中継ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**  ﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄが配信される期間が示された配信予定情報とﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄとを、第1のﾈｯﾄﾜｰｸから受信する受信手段と、ﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄを中継するための条件が登録されたﾊﾟｹｯﾄﾌｨﾙﾀﾙｰﾙ情報を保持しており、ﾊﾟｹｯﾄ受信手段が受信したﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄの中継がﾊﾟｹｯﾄﾌｨﾙﾀﾙｰﾙ情報において許されているか否かを判断するﾌｨﾙﾀﾘﾝｸﾞ手段と、ﾌｨﾙﾀﾘﾝｸﾞ手段により中継が許可されていると判断されたﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄを、第2のﾈｯﾄﾜｰｸ上へ送信するﾊﾟｹｯﾄ送信手段と、ﾊﾟｹｯﾄ受信手段が受信した配信予定情報に基づいて、ﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄの宛先ｱﾄﾞﾚｽと、宛先となるｱﾌﾟﾘｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾑの識別子との組からなる宛先情報、及び配信期間を示す配信期間情報を含む受信ﾊﾟｹｯﾄ情報を生成する情報解析手段と、情報解析手段が生成した受信ﾊﾟｹｯﾄ情報の宛先情報に合致するﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄが中継されるように、ﾊﾟｹｯﾄﾌｨﾙﾀﾙｰﾙ情報の内容を更新する中継許可情報登録手段と、情報解析手段が生成した受信ﾊﾟｹｯﾄ情報に示された配信期間が過ぎたﾏﾙﾁｷｬｽﾄﾊﾟｹｯﾄが中継されないように、ﾊﾟｹｯﾄﾌｨﾙﾀﾙｰﾙ情報の内容を更新する中継許可情報取消手段と、を有することを特徴とするｹﾞｰﾄｳｪｲ装置。

表2.11.4 富士ゼロックスの技術要素別課題対応特許（3/4）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 容疑ﾚﾍﾞﾙ、悪性閾値	特開2002-084324 00.09.08 H04L12/66 〔被引用回数 1〕	ﾈｯﾄﾜｰｸ接続制御方法および装置
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開平07-319820 （拒絶確定） 94.05.26 G06F15/00,330	情報処理ｼｽﾃﾑおよび情報処理ｼｽﾃﾑにおける作業支援方法
	攻撃パターンの高精度化	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開2000-235528 99.02.17 G06F13/00,351 〔被引用回数 1〕	ﾈｯﾄﾜｰｸ上において遠隔手続き呼び出しを実行するための方法
ルーティング制御技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開平09-293036 （拒絶確定） 96.04.26 G06F13/00,354 〔被引用回数 3〕	ﾌﾟﾘﾝﾄ処理装置
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開2003-058459 01.08.10 G06F13/00,547	ｲﾝﾀｰﾈｯﾄ印刷方法、そのｼｽﾃﾑ、ﾌﾟﾛｷｼ装置及びﾌﾟﾘﾝﾄｻｰﾊﾞ
	情報、個人の正当性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 識別子、認証情報の送信	特開2004-288112 03.03.25 G06F15/00,310	情報処理装置及び方法
IPアドレス変換技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開平09-062627 （拒絶確定） 95.08.23 G06F15/00,330 〔被引用回数 1〕	情報処理装置
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 URLﾄﾞﾒｲﾝの変換	特開2000-276443 99.03.24 G06F15/00,330	文書表示装置
ホスト認証技術	利用サービスの保護強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2001-117823 99.10.15 G06F12/14,320	ｱｸｾｽ資格認証機能付きﾃﾞｰﾀ記憶装置
	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開2000-057056 98.08.13 G06F12/14,310	ﾃﾞｰﾀ処理装置およびﾃﾞｰﾀ処理方法

表2.11.4 富士ゼロックスの技術要素別課題対応特許（4/4）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間・期間情報	特開2000-057097 （みなし取下） 98.08.13 G06F15/00,330	**画像処理装置**
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｺﾏﾝﾄﾞ	特開2005-044277 03.07.25 G06F15/00,330	**不正通信検出装置**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2000-057112 98.08.11 G06F15/16,620	**ﾈｯﾄﾜｰｸ上で遠隔手続き呼び出しを実行するための方法、及び、遠隔手続き呼び出しを実行可能なﾈｯﾄﾜｰｸ・ｼｽﾃﾑ**
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2005-190348 03.12.26 G06F12/14,320	**情報処理装置**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2002-091917 00.09.12 G06F15/00,330 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ装置および接続管理方法**
トンネリング技術	システムの性能向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開2003-318873 02.04.22 H04L9/08	**ﾃﾞｰﾀ処理装置、ﾃﾞｰﾀ処理方法およびﾃﾞｰﾀ処理ﾌﾟﾛｸﾞﾗﾑ**
		情報の送信、転送、分岐の手順改良 情報転送の手順 VPN設定情報	特開2004-201039 02.12.18 H04L12/22	**通信端末、方法および通信ﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 鍵情報の送信	特開2005-080249 03.09.04 H04L9/08	**ﾃﾞｰﾀ通信ｼｽﾃﾑ**

2.12 リコー

2.12.1 企業の概要

商号	株式会社　リコー
本社所在地	〒104-8222 東京都中央区銀座8-13-1　リコービル
設立年	1936年（昭和11年）
資本金	1,353億64百万円（2005年3月末）
従業員数	連結：75,100名（2005年3月末）
事業内容	事務機器（複写機、ファクシミリ、プリンタ等）、光学機器（カメラ、光学レンズ等）、光ディスク応用製品、半導体等の製造・販売、他

不正侵入防止、ウィルス対策など、ネットワーク上のセキュリティを強固に保つことはもちろん大切である。その上で、リコーは、ドキュメントに関わる情報物全般のセキュリティを強化することが、企業の責任として今後ますます重要であると考えている。

（出典：http://ext.ricoh.co.jp/security/）

2.12.2 製品例

ドキュメント・セキュリティとして、社内で培ってきたノウハウを商品・システムとして提供する。そのうち、不正アクセス侵入検知防御技術に関係すると思われる商品やサービスを、表2.12.2に示す。

表2.12.2 リコーの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
TrustyCabinet V1TrustyCabinet UX V1	電子文書の原本性確保支援システム；紙と同様に、電子文書の原本性保障・確保できる環境を構築
Ridoc IO Gate	統合プリント管理システム；不要な印刷を抑止
Imagio Neo 753/603/453/353シリーズ	不正コピーガード機能；全体にマスクパターンを埋め込んで出力できます。その原本をコピーした場合、「コピー禁止」等の牽制文字を浮き上がらせ、不正なコピーや情報漏えいを抑止。

（出典：http://ext.ricoh.co.jp/security/document/）

2.12.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

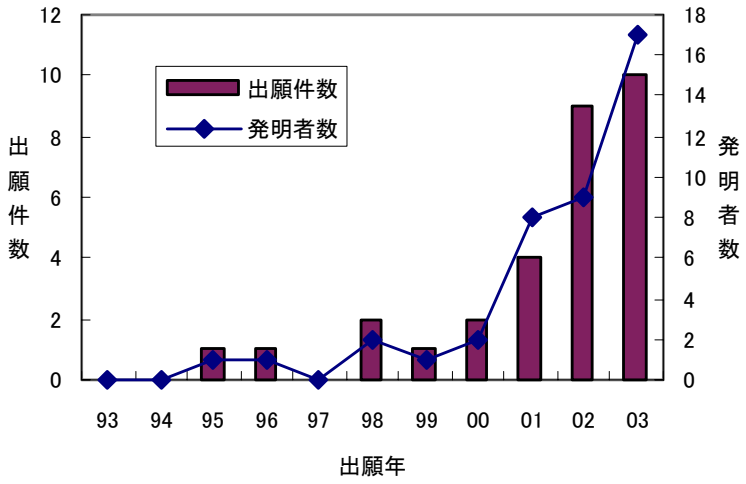
開発拠点：

東京都大田区中馬込1丁目3番6号 株式会社リコー内

アメリカ合衆国カリフォルニア州

図2.12.3に、リコーの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。2000年以降、出願件数は増加傾向にあり、03年の出願件数は10件になっており、発明者数も15人になっている。

図2.12.3 リコーの不正アクセス侵入検知防御技術に関する出願件数と発明者数



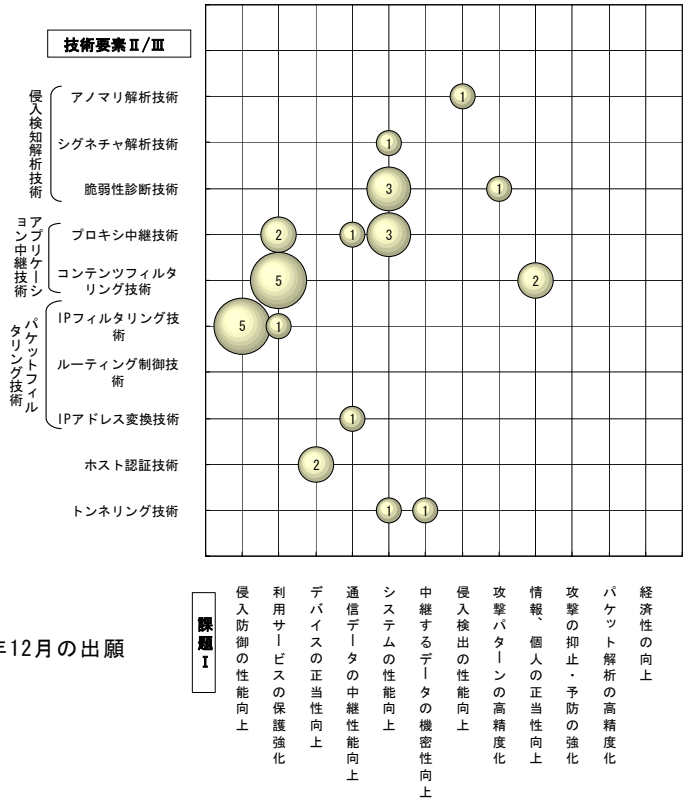
2.12.4 技術開発課題対応特許の概要

図2.12.4-1に、リコーの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.12.4-2に、リコーの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

コンテンツフィルタリング技術が7件出願され、次いでプロキシ中継技術とIPフィルタリング技術が6件出願されている。これらの出願のうち、多い課題は、「利用サービスの保護強化」と「システムの性能向上」である。

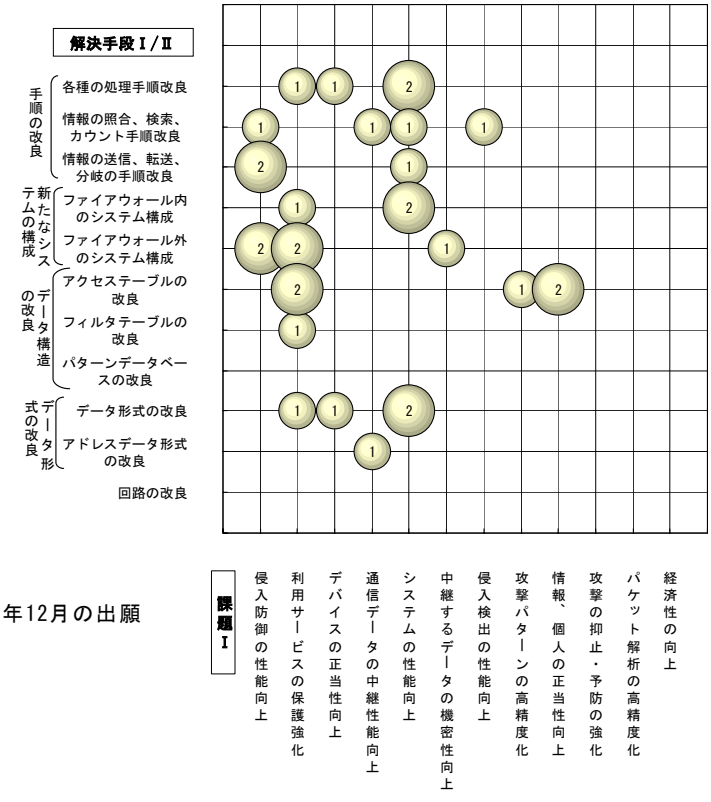
「利用サービスの保護強化」の課題に対しては、種々の分散した解決手段で対応している。システムの性能向上の課題に対しても、種々の分散した解決手段で対応している。

図2.12.4-1 リコーの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.12.4-2 リコーの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.12.4 リコーの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は30件で、そのうち１件が登録特許である。なお、表2.12.4では図2.12.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.12.4 リコーの技術要素別課題対応特許（1/3）

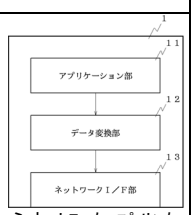
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2001-243091 00.02.04 G06F11/30	ﾛｸﾞﾌｧｲﾙによる事務機器保守ｼｽﾃﾑ
シグネチャ解析技術	システムの性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 障害情報の通知	特開2004-248256 03.01.24 H04M11/00,301	管理装置、遠隔管理ｼｽﾃﾑ、管理方法、およびﾌﾟﾛｸﾞﾗﾑ
脆弱性診断技術	システムの性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特開2003-101591 01.09.19 H04L12/66	ｾｷｭﾘﾃｨ方法およびｾｷｭﾘﾃｨ装置並びに遠隔診断保守ｼｽﾃﾑ
		各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特開2004-139566 02.09.19 G06F13/00,351	通信装置、通信ｼｽﾃﾑ、通信装置の制御方法、ﾌﾟﾛｸﾞﾗﾑ及び記録媒体
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2005-027040 03.07.02 H04L12/56 ﾘｺｰﾃｸﾉｼｽﾃﾑｽﾞ	監視方法、監視ﾌﾟﾛｸﾞﾗﾑ及び集中監視ﾌﾟﾛｸﾞﾗﾑ
	攻撃パターンの高精度化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ、ﾎﾟｰﾄ番号	特開2005-092456 03.09.16 G06F15/00,330	ﾈｯﾄｻｰﾋﾞｽ機能を有する情報処理装置およびﾈｯﾄｻｰﾋﾞｽ提供方法
プロキシ中継技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2003-036335 01.07.25 G06F17/60,154	行政文書目録公開ｼｽﾃﾑ、行政文書目録公開方法、その方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑおよびそのﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平08-331267 95.06.05 H04M11/00,301	被ﾓﾆﾀｰ装置とﾓﾆﾀｰ装置との間の通信方法，その通信ｼｽﾃﾑおよびｺﾝﾋﾟｭｰﾀ・ﾌﾟﾛｸﾞﾗﾑ製品
	通信データの中継性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特許3501913 96.12.20 G06F3/12	ﾌﾟﾘﾝﾀおよびﾈｯﾄﾜｰｸ・ﾌﾟﾘﾝﾀｼｽﾃﾑ SMTPを備えﾈｯﾄﾜｰｸ上で電子ﾒｰﾙを送受信する手段を有する端末と、印刷処理を行う手段とSMTPを備え、かつﾒｰﾙｻｰﾊﾞ機能を有するﾈｯﾄﾜｰｸ・ﾌﾟﾘﾝﾀとから構成されるﾈｯﾄﾜｰｸにおいて、前記端末は、ｱﾌﾟﾘｹｰｼｮﾝからの印刷ﾃﾞｰﾀを電子ﾒｰﾙ形式に変換する手段を備え、SMTPを使用して端末からﾈｯﾄﾜｰｸ・ﾌﾟﾘﾝﾀに対して印刷を行うことを特徴とするﾈｯﾄﾜｰｸ・ﾌﾟﾘﾝﾀｼｽﾃﾑ。 
	システムの性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 遠隔制御ｺﾏﾝﾄﾞの抽出	特開2003-330823 02.02.26 G06F13/00,353	画像形成装置管理ｼｽﾃﾑ、画像形成装置管理方法、管理装置、画像形成装置管理ﾌﾟﾛｸﾞﾗﾑ及び記録媒体

表2.12.4 リコーの技術要素別課題対応特許（2/3）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
プロキシ中継技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2004-287855 03.03.20 G06F13/00,351	監視方法、監視ｼｽﾃﾑ及びﾌﾟﾛｸﾞﾗﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ｺﾏﾝﾄﾞに情報付加	特開2004-289313 03.03.19 H04N1/00,106	画像処理装置管理ｼｽﾃﾑ、画像処理装置および画像処理装置の管理方法
コンテンツフィルタリング技術	利用サービスの保護強化	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2004-280727 03.03.18 G06F12/14,310	電子掲示板ｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2004-252954 03.01.27 G06F15/00,330	併合情報提供装置、情報提供装置、管理装置、併合情報提供方法、情報提供方法、管理方法、併合情報提供ﾌﾟﾛｸﾞﾗﾑ、情報提供ﾌﾟﾛｸﾞﾗﾑ、管理ﾌﾟﾛｸﾞﾗﾑ及び記録媒体
			特開2004-252955 03.01.27 G06F15/00,330	併合情報提供装置、情報提供装置、管理装置、併合情報提供方法、情報提供方法、管理方法、併合情報提供ﾌﾟﾛｸﾞﾗﾑ、情報提供ﾌﾟﾛｸﾞﾗﾑ、管理ﾌﾟﾛｸﾞﾗﾑ及び記録媒体
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ・ｸﾞﾙｰﾌﾟ	特開2003-167852 01.11.29 G06F15/00,330	情報提供ｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特開2002-359631 01.05.24 H04L12/46	ｺﾈｸｼｮﾝｾｷｭﾘﾃｨに基づいてﾈｯﾄﾜｰｸﾘｿｰｽへのｱｸｾｽを制御する方法及びｼｽﾃﾑ
	情報、個人の正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2004-046532 02.07.11 G06F15/00,330	情報処理装置、情報処理方法および記録媒体
			特開2005-085154 03.09.10 G06F15/00,330	ﾈｯﾄﾜｰｸｼｽﾃﾑおよび端末装置
IPフィルタリング技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2000-134403 98.10.28 H04N1/00,107	ﾘｱﾙﾀｲﾑｲﾝﾀｰﾈｯﾄﾌｧｸｼﾐﾘ装置の制御方法
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2004-133821 02.10.11 G06F15/00,330	情報機器および情報機器管理ｼｽﾃﾑ
			特開2004-102907 02.09.12 G06F17/60,154	ｾｷｭﾘﾃｨﾎﾟﾘｼｰ記述方法、記録媒体、及び伝送装置
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 ﾎﾟﾘｼｻｰﾊﾞｰの配置	特開2004-094401 02.08.29 G06F15/00,330	ｾｷｭﾘﾃｨﾎﾟﾘｼｰ配布ｼｽﾃﾑ、ｾｷｭﾘﾃｨﾎﾟﾘｼｰに基づき動作する装置、ｾｷｭﾘﾃｨﾎﾟﾘｼｰ配布方法、ｾｷｭﾘﾃｨﾎﾟﾘｼｰ配布ﾌﾟﾛｸﾞﾗﾑ、及びﾌﾟﾛｸﾞﾗﾑを記
			特開2004-094405 02.08.29 G06F15/00,330	ｾｷｭﾘﾃｨﾎﾟﾘｼｰ管理装置、ｾｷｭﾘﾃｨﾎﾟﾘｼｰ配布ｼｽﾃﾑ、ｾｷｭﾘﾃｨﾎﾟﾘｼｰ配布方法、ｾｷｭﾘﾃｨﾎﾟﾘｼｰ配布ﾌﾟﾛｸﾞﾗﾑ、及びﾌﾟﾛｸﾞﾗﾑを記録した記録媒
	利用サービスの保護強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開平11-259424 （みなし取下） 98.03.13 G06F15/00,330 〔被引用回数 1〕	ﾃﾞｰﾀ提供装置およびﾃﾞｰﾀ提供方法，並びにﾃﾞｰﾀ提供方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑを記録した機械読み取り可能な記録媒体

表2.12.4 リコーの技術要素別課題対応特許（3/3）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPアドレス変換技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾎﾟｰﾄ番号の割付	特開2002-176462 00.09.29 H04L29/08	**ｾｯｼｮﾝ確立方法**
ホスト認証技術	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開2004-287492 03.03.19 G06F15/00,330	**通信装置**
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2000-330898 99.05.20 G06F13/00,351	**電子文書管理ｼｽﾃﾑ、電子文書管理方法およびその方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**
トンネリング技術	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2003-304229 02.04.09 H04L9/08	**暗号化ﾃﾞｰﾀ通信装置、管理装置、暗号化ﾃﾞｰﾀ通信装置管理ﾌﾟﾛｸﾞﾗﾑ、管理装置管理ﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開2004-085627 （みなし取下） 02.08.22 G09C1/00,660	**暗号化制御ｼｽﾃﾑ、暗号化制御装置および暗号化制御ｻｰﾊﾞ**

2.13 マイクロソフト

2.13.1 企業の概要

商号	Microsoft Corporation
本社所在地	One Microsoft Way, Redmond, WA 98052, U.S.A.
設立年	1975年
資本金	56,396百万米ドル（2004年6月末）
従業員数	約57,000名（連結：2004年6月末）
事業内容	コンピュータ向けソフトウエアの開発、製作、ライセンス供与、サポート・サービスの提供

「コンピュータを守るため最低限の必要なこと」として、「①インターネット ファイアウォールを入手する、②Microsoft Update を使用する、③ウイルス対策ソフトウェアを入手する、④スパイウェア対策ソフトウェアを入手する」とホームページに記載され、その必要性を含めてセキュリティを易しく、詳細に解説している。（出典：http://www.microsoft.com/japan/athome/security/protect/windows2000/Default.mspx）

2.13.2 製品例

Windows2000XPではファイアウォールは組込まれており、その他のWindows2000でも上記②のUPDATEをダウンロードすれば、ファイアウォールは設定できる。一方Windows Server Systemでは、セキュリティ製品として紹介されており、表2.13.2に、製品例とその概要を示す。

表2.13.2 マイクロソフトの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
ISA Server 2000	① セキュアで管理の容易な高速インターネット接続を提供。 ② 拡張可能なマルチレイヤ エンタープライズ ファイアウォールとスケーラブルな高性能 Web キャッシュの統合。 ③ Windows セキュリティを基盤とした本製品は、ポリシー ベースのセキュリティ、アクセラレーションなどの管理を実現
Microsoft Client Protection	スパイウェアやウイルス等の「悪意のあるソフトウェア」の脅威からビジネス デスクトップ、ラップトップ、およびファイルサーバーを保護するセキュリティソリューション。
Sybari Software	ウイルス、ワーム、およびスパムからメッセージングとコラボレーションサーバを保護するセキュリティソリューション。
セカンダリファイアウォール ソリューション	従来のファイアウォールでは、対応する事が困難な課題、「情報漏えいの原因の特定」、「ウイルスの感染拡大」、「外部から接続するクライアントの検疫」、「Exchange Server の安全な公開」の解決。
企業におけるセキュリティ対策と運用管理	製品自体の脆弱性を削減すると共に、顧客によるセキュリティ対策とその維持を支援する。

（出典：http://www.microsoft.com/japan/windowsserversystem/security/default.mspx）

2.13.3 技術開発拠点と研究者

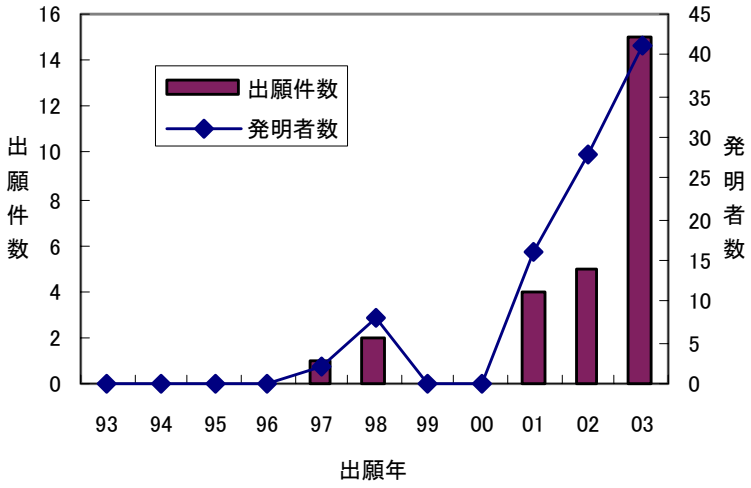
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

アメリカ合衆国ワシントン州

図2.13.3に、マイクロソフトの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。01年以降、出願件数が増加傾向にあり、03年に急激な増加をして14件の出願がなされ、発明者数も40人になった。

図2.13.3　マイクロソフトの不正アクセス侵入検知防御技術に関する出願件数と発明者数



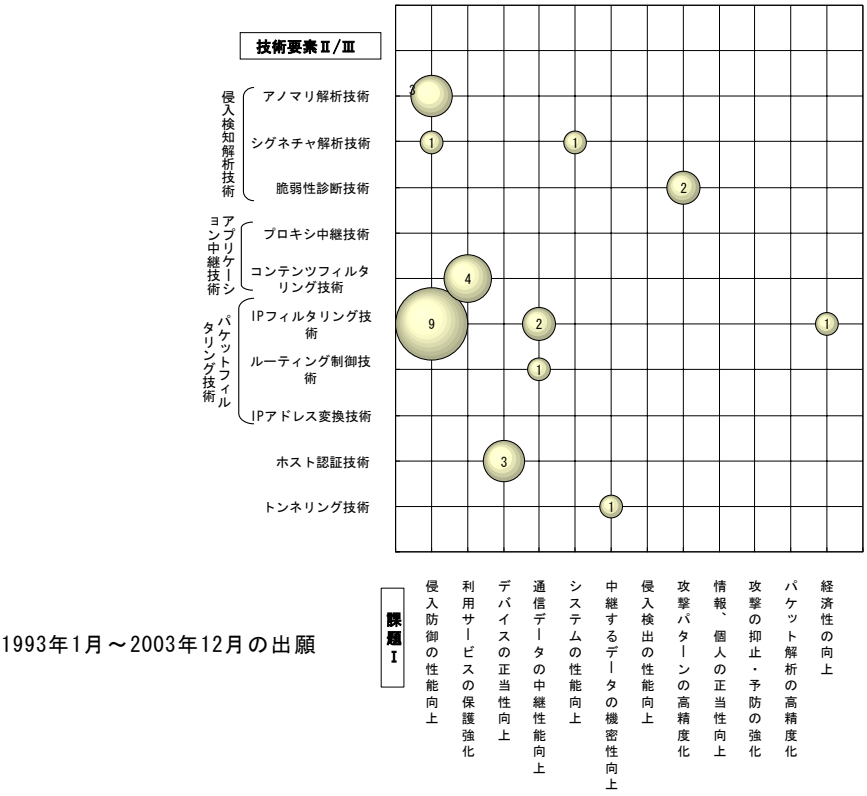
2.13.4 技術開発課題対応特許の概要

図2.13.4-1に、マイクロソフトの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.13.4-2に、マイクロソフトの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

IPフィルタリング技術が最も多く出願されている。これらの出願のうち、多い課題は、「侵入防御の性能向上」である。

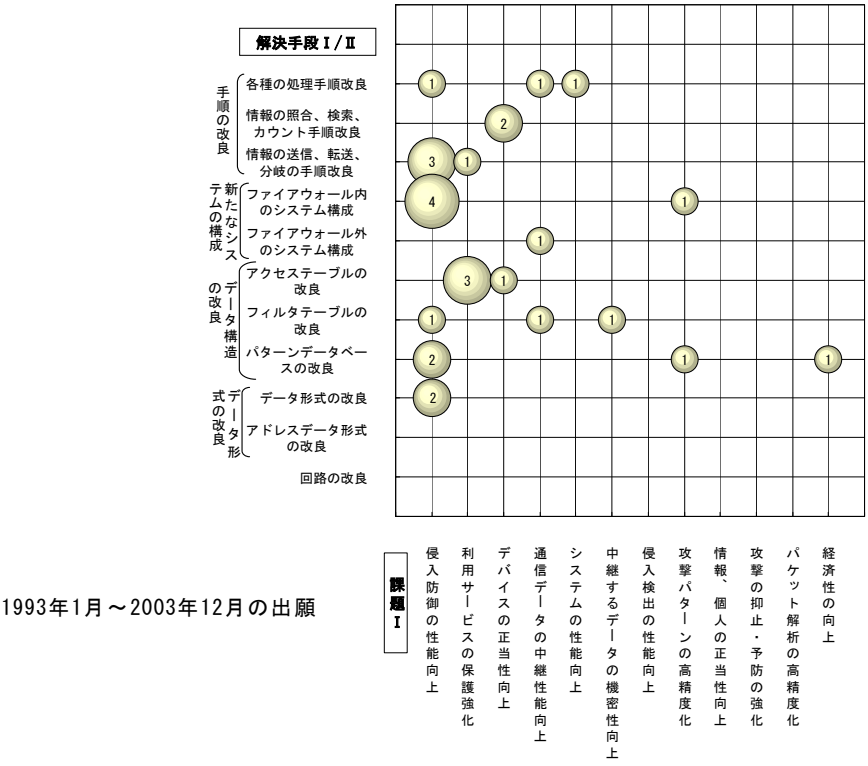
「侵入防御の性能向上」の課題に対しては、「ファイアウォール内のシステム構成」で多く対応している。

図2.13.4-1 マイクロソフトの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.13.4-2 マイクロソフトの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.13.4 マイクロソフトの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は27件で、そのうち１件が登録特許である。なお、表2.13.4では図2.13.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段Ⅲ とⅣまで分析している。

表2.13.4 マイクロソフトの技術要素別課題対応特許（1/3）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2005-011326 03.06.20 G06F13/00,610	ｽﾊﾟﾑﾌｨﾙﾀの不明瞭化
			特開2004-362581 03.06.06 G06F13/00,351	ﾏﾙﾁﾚｲﾔｰﾌｧｲｱｳｫｰﾙｱｰｷﾃｸﾁｬ
			特開2004-362590 03.06.06 G06F13/00,351	ﾈｯﾄﾜｰｸﾌｧｲｱｳｫｰﾙを実装するための多層ﾍﾞｰｽの方法
シグネチャ解析技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾎﾟﾘｼｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特表2002-513961 98.05.01 G06F15/00,330	ｲﾝﾃﾘｼﾞｪﾝﾄﾗｽﾄﾏﾈｼﾞﾒﾝﾄの方法およびｼｽﾃﾑ
	システムの性能向上	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特開2004-362594 03.06.06 G06F13/00,357	外部ﾈｯﾄﾜｰｸﾃﾞﾊﾞｲｽを自動的に発見および構成する方法
脆弱性診断技術	攻撃パターンの高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 情報提供ｻｰﾊﾞｰの配置	特開2004-334887 03.05.09 G06F12/14,530	ｾｷｭｱ・ﾃﾞｰﾀに対するWEBｱｸｾｽ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 脆弱度の算出	特開2004-164617 02.11.12 G06F15/00,330	ｸﾛｽｻｲﾄｽｸﾘﾌﾟﾃｨﾝｸﾞ脆弱性の自動検出
コンテンツフィルタリング技術	利用サービスの保護強化	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2003-208404 01.10.05 G06F15/00,330	ﾈｯﾄﾜｰｸﾕｰｻﾞｾｯｼｮﾝのためのｸﾞﾗﾆｭﾗ認証
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開2004-005638 02.05.09 G06F15/00,330	ｽﾃｰﾄﾚｽ環境でｱｸｾｽされるﾘｿｰｽに対する認証状態の維持
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 時間、期限情報	特表2002-517852 98.06.12 G06F1/00	信頼できないｺﾝﾃﾝﾄを安全に実行するための方法およびｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2004-213632 02.12.06 G06F15/00,330	ｺﾝﾋﾟｭｰﾀｼｽﾃﾑがﾈｯﾄﾜｰｸにｱｸｾｽするように準備する際に自動化のﾚﾍﾞﾙを高める方法、ｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ及び記録媒体
IPフィルタリング技術	侵入防御の性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 多層ﾌﾟﾛﾄｺﾙの処理	特開2004-364315 03.06.06 H04L12/66	複数のﾈｯﾄﾜｰｸ・ﾎﾟﾘｼｰを統合するための方法とﾌﾚｰﾑﾜｰｸ
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2003-203011 01.10.16 G06F12/14,310	仮想分散ｾｷｭﾘﾃｨｼｽﾃﾑ

表2.13.4 マイクロソフトの技術要素別課題対応特許（2/3）

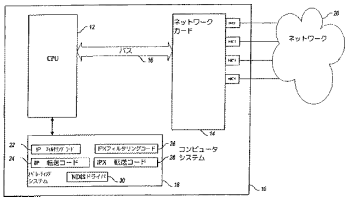
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
IPフィルタリング技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼｰ設定情報	特開2005-085279 03.09.08 G06F13/00,353	**ｾｷｭﾘﾃｨｺﾝﾌﾘｸﾄを回避する、調整されたﾈｯﾄﾜｰｸｲﾆｼｴｰﾀ管理**
		情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特開2005-018769 03.06.25 G06F13/00,351	**ｱﾌﾟﾘｹｰｼｮﾝのﾌｧｲｱｳｫｰﾙ横断を支援する方法**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特許3399928 97.07.10 H04L12/46,200	**ｺﾝﾋﾟｭｰﾀｼｽﾃﾑにおけるﾈｯﾄﾜｰｸﾊﾟｹｯﾄの高速転送及びﾌｨﾙﾀﾘﾝｸﾞ**  ｿｰｽﾈｯﾄﾜｰｸから宛先ﾈｯﾄﾜｰｸにﾃﾞｰﾀのﾊﾟｹｯﾄを転送するためのｺﾝﾋﾟｭｰﾀｼｽﾃﾑにおける方法において、各ﾊﾟｹｯﾄがﾒｯｾｰｼﾞの一部であり、ｺﾝﾋﾟｭｰﾀｼｽﾃﾑが、ﾊﾞｽを介してﾈｯﾄﾜｰｸｶｰﾄﾞに接続されたﾒｲﾝ中央演算処理装置を備え、ﾈｯﾄﾜｰｸｶｰﾄﾞがｿｰｽ及び宛先ﾈｯﾄﾜｰｸに接続され、ﾈｯﾄﾜｰｸｶｰﾄﾞが、ｷｬｯｼｭﾒﾓﾘを備え、ｺﾝﾋﾟｭｰﾀｼｽﾃﾑが、ﾒｲﾝ中央演算処理装置によって実行される命令を備えるｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑを備える、方法であって、ﾈｯﾄﾜｰｸｶｰﾄﾞの制御下で、ｿｰｽﾈｯﾄﾜｰｸからﾊﾟｹｯﾄを受信し、ｷｬｯｼｭﾒﾓﾘがﾊﾟｹｯﾄに関するﾙｰﾃｨﾝｸﾞ情報を包含するかどうか判断し、ｷｬｯｼｭﾒﾓﾘがかかるﾙｰﾃｨﾝｸﾞ情報を包含するとき、ﾙｰﾃｨﾝｸﾞ情報に従って宛先ﾈｯﾄﾜｰｸの受信したﾊﾟｹｯﾄを伝送し、ｷｬｯｼｭﾒﾓﾘがかかるﾙｰﾃｨﾝｸﾞ情報を包含しないとき、受信されたﾊﾟｹｯﾄをｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑに送信し、ｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑの制御下で、送信されたﾊﾟｹｯﾄを受信し、受信されたﾊﾟｹｯﾄがﾌｨﾙﾀﾘﾝｸﾞ情報に基づいてﾄﾞﾛｯﾌﾟされるかどうか判断し、受信されたﾊﾟｹｯﾄがﾄﾞﾛｯﾌﾟされなかったとき、受信ﾊﾟｹｯﾄが宛先ﾈｯﾄﾜｰｸに伝送されることを示すﾙｰﾃｨﾝｸﾞ情報を検索し、ﾙｰﾃｨﾝｸﾞ情報をﾈｯﾄﾜｰｸｶｰﾄﾞに送信し、ﾈｯﾄﾜｰｸｶｰﾄﾞの制御下で、送信ﾙｰﾃｨﾝｸﾞ情報を受信し、次のﾊﾟｹｯﾄがｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑに送信されることなく、該次のﾊﾟｹｯﾄが宛先ﾈｯﾄﾜｰｸに伝送されるように、受信されたﾙｰﾃｨﾝｸﾞ情報をﾒﾓﾘｷｬｯｼｭにｽﾄｱし、ﾙｰﾃｨﾝｸﾞ情報に従って宛先ﾈｯﾄﾜｰｸに受信されたﾊﾟｹｯﾄが伝送され、同じﾊﾟｹｯﾄ識別子を備えるﾊﾟｹｯﾄが、ｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑによる処理なしで宛先ﾈｯﾄﾜｰｸに転送され、他のﾊﾟｹｯﾄ識別子を備えるﾊﾟｹｯﾄが、ｵﾍﾟﾚｰﾃｨﾝｸﾞｼｽﾃﾑのﾌｨﾙﾀﾘﾝｸﾞ基準処理に基づいてﾄﾞﾛｯﾌﾟされる、ことを特徴とする方法。
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 自動登録	特開2004-110774 02.06.28 G06F15/00,310	**ﾍﾟｱﾚﾝﾀﾙ･ｺﾝﾄﾛｰﾙのｶｽﾀﾏｲｽﾞおよび通知**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ﾊﾟﾀｰﾝの廃棄	特開2004-364305 03.06.06 H04L12/66	**ﾈｯﾄﾜｰｸﾌｨﾙﾀﾍﾞｰｽのﾎﾟﾘｼｰを管理するための方法**
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 特徴単語の学習	特開2005-018745 03.06.23 G06F13/00,610	**高度なｽﾊﾟﾑ検出技法**

表2.13.4 マイクロソフトの技術要素別課題対応特許（3/3）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾎﾟﾘｼｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特開2005-184836 03.12.19 H04L12/66	ﾌｧｲｱｳｵｰﾙｻｰﾋﾞｽを管理するためのｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ
	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2004-265419 03.02.28 G06F15/00,330	ﾘｿｰｽの遅延割振りのための方法およびｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2004-056784 02.06.10 H04L9/32	ｾｷｭﾘﾃｨｹﾞｰﾄｳｪｲで実行する方法、記録媒体及びｼｽﾃﾑ
	経済性の向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ﾊﾟﾀｰﾝの廃棄	特開2004-364305 03.06.06 H04L12/66	ﾈｯﾄﾜｰｸﾌｨﾙﾀﾍﾞｰｽのﾎﾟﾘｼｰを管理するための方法 概要は技術要素「IPﾌｨﾙﾀﾘﾝｸﾞ」、課題「侵入防御の性能向上」の項参照
ルーティング制御技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2005-012775 03.06.06 H04L12/66	ﾘﾓｰﾄ･ｸﾗｲｱﾝﾄをﾛｰｶﾙ･ｸﾗｲｱﾝﾄ･ﾃﾞｽｸﾄｯﾌﾟに接続するためのｱｰｷﾃｸﾁｬ
ホスト認証技術	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2003-099401 01.06.20 G06F15/00,330	認証信用証明書の委任の有効範囲を制御するための方法とｼｽﾃﾑ
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2003-223416 01.11.13 G06F15/00,330	認証可能なｹﾞｰﾑｼｽﾃﾑを製造するためのｱｰｷﾃｸﾁｬ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ｿﾞｰﾝ	特開2004-310774 03.04.01 G06F13/00,351	ﾈｯﾄﾜｰｸｿﾞｰﾝ
トンネリング技術	中継するデータの機密性向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開2005-027312 03.06.30 H04L12/56	透過仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸを用いたﾈｯﾄﾜｰｸ構成の複雑さの低減

2.14 エヌ・ティ・ティ・データ

2.14.1 企業の概要

商号	株式会社　エヌ・ティ・ティ・データ
本社所在地	〒135-6033　東京都江東区豊洲3-3-3豊洲センタービル
設立年	1988年(昭和63年)
資本金	1,425億2,000万円(2005年９月末)
従業員数	8,077名(2005年９月末)　（連結：20,445名）
事業内容	電気通信業、データ通信システムの開発および保守の受託、販売並びに賃貸

IT社会が普及・拡大する現在、情報システムの世界は加速度的に変化している。時代に勝ち残っていくためには、ITトレンドの変化を読み取り、個々のシステムや技術の中身を理解し、いち早くビジネスにとり入れていくことが重要である。NTTデータはこれらITにおけるトレンドやキーワードを網羅した数々のサービスを提供し、IT社会の拡大と推進を目指している。(出典：http://www.nttdata.co.jp/service/s1109.html)

2.14.2 製品例

紹介されているファイアウォールやIDSの製品は下記のようになっており、表2.14.2に、製品例とその概要を示す。

表2.14.2 NTTデータの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
情報セキュリティコンサルティングサービス	単なるセキュリティポリシー策定やあるべき論の押し付けではなく、NTTデータが自らポリシー策定から情報セキュリティを遵守する風土に仕向けていくプロセスを経験してきた中から学んだ実態を踏まえてお客様の状況に合わせて情報セキュリティマネージメントの行き届いた組織する
SecureAccess	デバイスレベル(BIOS)の厳格なPC認証を用い、組織の管理の行き届かない不明なPCのネットワーク接続を防止。 イントラネット、リモートアクセスVPN等への適用が可能。 ユーザ認証と組み合わせて使うことで、より強力な認証基盤を実現。
SecureSeal	電子的な指紋「ハッシュ値」により原本性と作成時刻を厳密に保証する、究極の電子文書セキュリティサービス。NTTデータが2000年4月より他社に先駆けて始めた実績のあるサービス。特徴としては、タイムスタンプの効果が超長期に渡って保証できること。
SecureVISTA	ファイアウォール、IDSなどのログや、ネットワークを構成する機器からの管理情報を、リアルタイムに一元集約、統合分析。それらの情報を様々な角度からグラフィカルに表示することで、システムの全体状況把握を的確にし、より高度な意思決定をサポート。
SecureFort	「セキュリティ診断」「セキュリティ監視」を通常運用メニューとして用意するほか、セキュリティに関するオプションメニューを豊富に提供できるため、外部からの侵入を未然に防止。
セキュリティ・ソリューション SEER	(1)セキュリティ診断サービス (2)クライアントセキュリティ管理(SEER INNER) (3)ログ情報管理ソリューション(SEER Under-Cover,Tracker,LogHost) (4)セキュリティ eラーニング(ASP)

(出典：http://www.nttdata.co.jp/service/s1109.html)

2.14.3 技術開発拠点と研究者

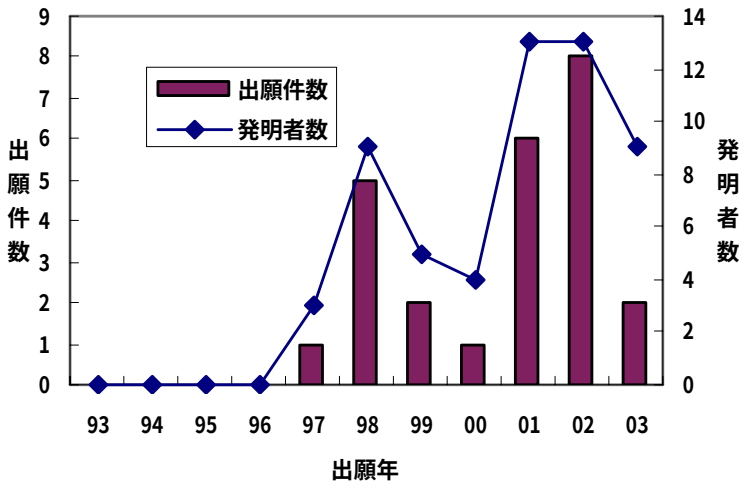
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都江東区豊洲3丁目3番3号 株式会社NTTデータ内

図2.14.3に、NTTデータの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。2001年、02年の平均は、出願件数が７件、発明者が13人であったが、03年に減少した。

NTTデータの不正アクセス侵入検知防御技術に関する出願件数と発明者数



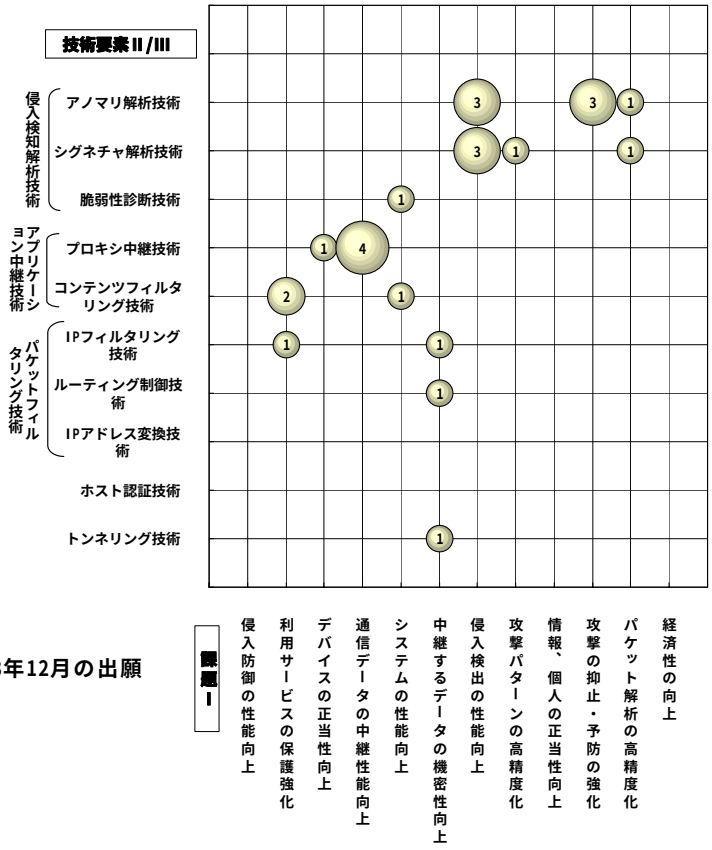
2.14.4 技術開発課題対応特許の概要

図2.14.4-1に、NTTデータの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.14.4-2に、NTTデータの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術に関する出願が多い。これらの出願のうち、最も多い課題は、「侵入検出の性能向上」である。

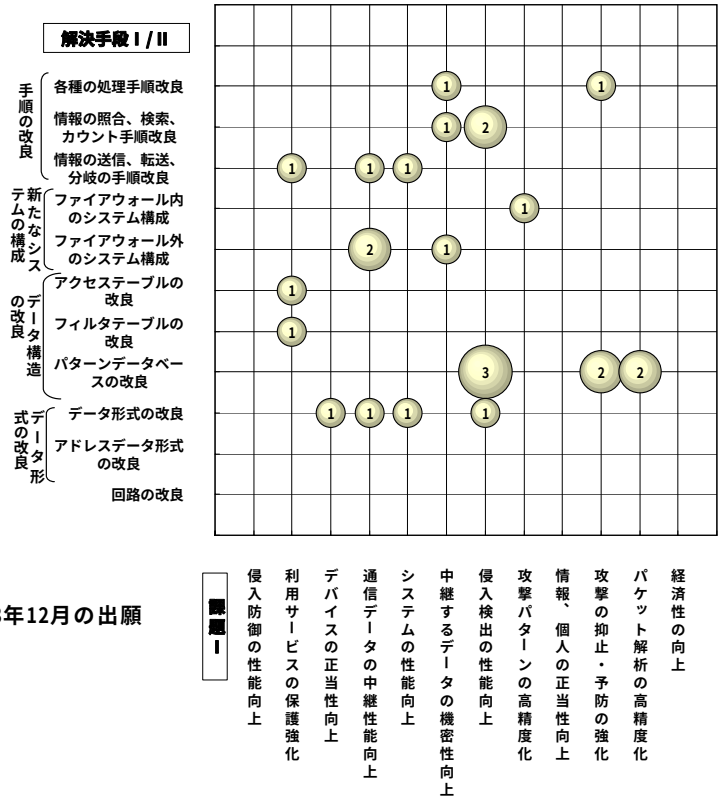
「侵入検出の性能向上」の課題に対しては、「パターンデータベースの改良」で３件対応している。

図2.14.4-1 NTTデータの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.14.4-2 NTTデータの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.14.4 NTTデータの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は25件で、そのうち５件が登録特許である。なお、表2.14.4では図2.14.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.14.4 NTTデータの技術要素別課題対応特許（1/3）

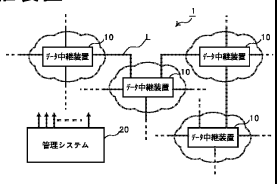
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	侵入検出の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2002-334061 01.05.08 G06F15/00,320 〔被引用回数 1〕	不正ｱｸｾｽ監視ｼｽﾃﾑおよびそのﾌﾟﾛｸﾞﾗﾑ
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 経路、中継ｻｰﾊﾞｰ	特許3483782 98.10.15 H04L12/56,400 〔被引用回数 6〕	電子ﾃﾞｰﾀの追跡ｼｽﾃﾑ及びﾃﾞｰﾀ中継装置 電子ﾃﾞｰﾀを流通させる装置が連鎖状に接続されたﾈｯﾄﾜｰｸ上で前記電子ﾃﾞｰﾀを運ぶﾃﾞｰﾀﾘﾝｸ層の識別子を解析し、当該電子ﾃﾞｰﾀが通過した前記装置を前記識別子の解析結果に基づいて特定する過程を含む、電子ﾃﾞｰﾀの追跡方法。 
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾀｲﾑｽﾀﾝﾌﾟの付加	特開2004-147223 02.08.30 H04L12/56,400 ｻｲﾊﾞｰ・ｿﾘｭｰｼｮﾝｽﾞ	ﾊﾟｹｯﾄ通過ﾙｰﾄ探索方法、不正ｱｸｾｽ攻撃元特定方法およびこれらの方法をｺﾝﾋﾟｭｰﾀに実行させるﾌﾟﾛｸﾞﾗﾑ
	攻撃の抑止・予防の強化	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の無返却、制限	特開2003-309607 02.04.17 H04L12/66 ｻｲﾊﾞｰ・ｿﾘｭｰｼｮﾝｽﾞ	ｱﾝﾁﾌﾟﾛﾌｧｲﾘﾝｸﾞ装置およびｱﾝﾁﾌﾟﾛﾌｧｲﾘﾝｸﾞﾌﾟﾛｸﾞﾗﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 異常値出現頻度	特開2004-030286 02.06.26 G06F15/00,330 ｻｲﾊﾞｰ・ｿﾘｭｰｼｮﾝｽﾞ	侵入検知ｼｽﾃﾑおよび侵入検知ﾌﾟﾛｸﾞﾗﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 異常値出現頻度	特開2004-030287 02.06.26 G06F13/00,351 ｻｲﾊﾞｰ・ｿﾘｭｰｼｮﾝｽﾞ	双方向型ﾈｯﾄﾜｰｸ侵入検知ｼｽﾃﾑおよび双方向型侵入検知ﾌﾟﾛｸﾞﾗﾑ
	パケット解析の高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2001-313640 00.05.02 H04L12/24 〔被引用回数 3〕	通信ﾈｯﾄﾜｰｸにおけるｱｸｾｽ種別を判定する方法及びｼｽﾃﾑ、記録媒体
シグネチャ解析技術	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ｱﾗｰﾄﾊﾟﾀｰﾝの追加	特開2004-046742 02.07.15 G06F13/00,351	攻撃分析装置、ｾﾝｻ、攻撃分析方法及びﾌﾟﾛｸﾞﾗﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ｱﾗｰﾄﾊﾟﾀｰﾝの追加	特開2004-336130 （特許3697249） 03.04.30 H04L12/66	ﾈｯﾄﾜｰｸ状態監視ｼｽﾃﾑ及びﾌﾟﾛｸﾞﾗﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 振舞い形式の学習	特開2005-190484 01.05.08 G06F15/00,330	不正ｱｸｾｽ監視ｼｽﾃﾑおよびそのﾌﾟﾛｸﾞﾗﾑ

表2.14.4 NTTデータの技術要素別課題対応特許（2/3）

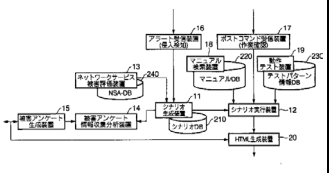
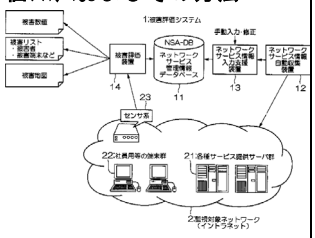
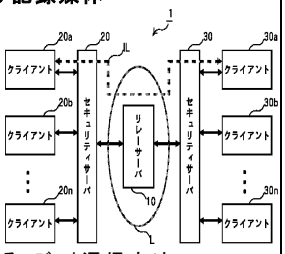
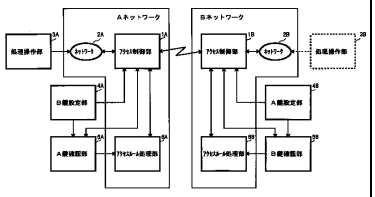
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
シグネチャ解析技術	攻撃パターンの高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特許3618682 01.05.01 G06F15/00,320	**ﾏﾆｭｱﾙの自動生成および動作確認ｼｽﾃﾑならびにその方法** ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨに起因する被害状況、ならびにその対応についてのﾕｰｻﾞ要求を得、回復のための対応手順を決定してその内容を生成するｼﾅﾘｵ生成装置と、作業ｽﾃｯﾌﾟ毎に構造化して記述されたｼﾅﾘｵにおいて、その作業ｽﾃｯﾌﾟ単位に作業確認を得、その作業ｽﾃｯﾌﾟ単位で回復箇所のﾃｽﾄを行ない前記ｼﾅﾘｵに反映させるｼﾅﾘｵ実行装置とを備えたことを特徴とするﾏﾆｭｱﾙの自動生成および動作確認ｼｽﾃﾑ。 
	パケット解析の高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ﾊﾟﾀｰﾝの切換	特開2002-342276 01.05.17 G06F15/00,330 ｻｲﾊﾞｰ・ｿﾘｭｰｼｮﾝｽﾞ 〔被引用回数 2〕	**ﾈｯﾄﾜｰｸ侵入検知ｼｽﾃﾑおよびその方法**
脆弱性診断技術	システムの性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 障害情報の通知	特許3618681 01.05.01 G06F15/00,320 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨに関する被害評価ｼｽﾃﾑおよびその方法** ﾊｰﾄﾞｳｪｱから業務ﾚﾍﾞﾙに至る全業務に関する各ﾈｯﾄﾜｰｸ要素の関連性を統一したﾌｫｰﾏｯﾄに基づき電子的に記述したﾈｯﾄﾜｰｸｻｰﾋﾞｽ管理情報ﾃﾞｰﾀﾍﾞｰｽと、前記ﾈｯﾄﾜｰｸに対する不正侵入や攻撃を受けて停止した前記あるﾈｯﾄﾜｰｸ要素を起点に前記ﾈｯﾄﾜｰｸｻｰﾋﾞｽ管理情報ﾃﾞｰﾀﾍﾞｰｽを検索することにより被害が及ぶ関連範囲を特定し、前記関連範囲におけるﾈｯﾄﾜｰｸ要素毎あらかじめ定義された想定被害数値を累積演算する被害評価装置とを備えたことを特徴とするﾈｯﾄﾜｰｸｾｷｭﾘﾃｨに関する被害評価ｼｽﾃﾑ。 
プロキシ中継技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2000-331101 （拒絶確定） 99.05.17 G06F19/00	**医療関連情報管理ｼｽﾃﾑ及びその方法**
	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 擬似、ﾀﾞﾐﾃﾞｰﾀの送信	特許2998839 98.10.08 H04L12/22 ﾄﾞﾜﾝｺﾞ 〔被引用回数 6〕	**ﾃﾞｰﾀ通信方法、ﾃﾞｰﾀ中継装置及び記録媒体** 配下にある1又は複数の通信装置との間で所定形態の透過許容ﾃﾞｰﾀのみの透過を許容するｾｷｭﾘﾃｨ装置が介在する環境下で行うﾃﾞｰﾀ通信方法であって、外部装置から特定の前記通信装置宛に送信された通信ﾃﾞｰﾀを前記透過許容ﾃﾞｰﾀに擬似的に変換して当該ｾｷｭﾘﾃｨ装置を透過させることを特徴とする、ﾃﾞｰﾀ通信方法。 
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2000-151693 （拒絶確定） 98.11.05 H04L12/56 〔被引用回数 1〕	**ﾌｧｲﾔｳｫｰﾙを隔てたｼｽﾃﾑ制御方式及び方法**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2003-218867 （拒絶確定） 02.01.28 H04L12/18	**ﾃﾞｰﾀ配信ｼｽﾃﾑ、ﾃﾞｰﾀ配信装置、ﾃﾞｰﾀ配信方法及びﾌﾟﾛｸﾞﾗﾑ**

表2.14.4 NTTデータの技術要素別課題対応特許（3/3）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
プロキシ中継技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 更新情報の付加	特開2000-076218 （拒絶確定） 98.08.27 G06F15/177,682 〔被引用回数 5〕	**ﾃﾞｰﾀﾍﾞｰｽ間の同期化ｼｽﾃﾑ**
コンテンツフィルタリング技術	利用サービスの保護強化	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特許3440206 98.06.10 H04L12/46	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｼｽﾃﾑ、相互ｱｸｾｽ制御方法及び記録媒体**  ｱｸｾｽ制御によるｾｷｭﾘﾃｨが施されたﾈｯﾄﾜｰｸｼｽﾃﾑにおいて、所定のｱｸｾｽﾙｰﾙに基づいて自ﾈｯﾄﾜｰｸに対するｱｸｾｽを制御するｱｸｾｽ制御手段と、自ﾈｯﾄﾜｰｸにて鍵を設定する鍵設定手段と、相手先のﾈｯﾄﾜｰｸにて鍵が設定されたことを確認する鍵設定確認手段と、前記鍵設定手段及び前記鍵設定確認手段により、自ﾈｯﾄﾜｰｸ及び相手先ﾈｯﾄﾜｰｸの両者にて鍵が設定された場合に前記ｱｸｾｽ制御手段を制御して通常時と異なるｱｸｾｽﾙｰﾙを設定するｱｸｾｽﾙｰﾙ処理手段と、を具備することを特徴とするﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｼｽﾃﾑ。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開2003-308296 02.04.17 G06F15/00,330 ｻｲﾊﾞｰ・ｿﾘｭｰｼｮﾝｽﾞ	**ﾈｯﾄﾜｰｸｱｸｾｽ制御ｼｽﾃﾑおよびﾈｯﾄﾜｰｸｱｸｾｽ制御ﾌﾟﾛｸﾞﾗﾑ**
	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特開2004-171274 02.11.20 G06F15/00,330	**分散型認証ｼｽﾃﾑ及び分散型認証ﾌﾟﾛｸﾞﾗﾑ**
IPフィルタリング技術	利用サービスの保護強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2002-351567 01.05.28 G06F1/00	**ﾌﾟﾛｸﾞﾗﾑ制御装置および方法、ならびにﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2005-175825 03.12.10 H04L12/66	**暗号化ﾊﾟｹｯﾄﾌｨﾙﾀﾘﾝｸﾞ装置およびそのﾌﾟﾛｸﾞﾗﾑ、ならびにﾎｽﾄ装置**
ルーティング制御技術	中継するデータの機密性向上	各種の処理手順改良 特定情報の記憶、登録手順 鍵情報の記憶	特開2000-341324 99.05.26 H04L12/56	**暗号通信方法及びｼｽﾃﾑ**
トンネリング技術	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 暗号処理ｻｰﾊﾞｰの配置	特開平11-041280 （みなし取下） 97.07.15 H04L12/56 〔被引用回数 3〕	**通信ｼｽﾃﾑ、VPN中継装置、記録媒体**

2.15 沖電気工業

2.15.1 企業の概要

商号	沖電気工業　株式会社
本社所在地	〒105-8460　東京都港区虎ノ門1-7-12
設立年	1949年（昭和24年）
資本金	678億77百万円（2005年3月末）
従業員数	5,389名（2005年3月末）
事業内容	情報システム（金融・ITS等）、通信システム（IP電話・映像配信等）の製造・販売・工事・保守、電子デバイス（LSI等）の製造・販売、他

トップページから製品をリンクすると、その中に「セキュリティ・認証」がある。そこには、個人情報をはじめとした重要情報を守る、強固な情報セキュリティシステムの紹介として、アイリス認識応用製品と情報セキュリティ製品をあげている。

(出典：http://www.oki.com/jp/Home/JIS/PROD/index.html#link9)

2.15.2 製品例

情報セキュリティ製品に紹介されているもののうち、不正アクセス侵入検知防御技術に関係する製品やサービスを、表2.15.2に示す。

表2.15.2 沖電気工業の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
eすぷりっと	企業間における重要情報の受け渡しを、割符の技術により、情報を分割・ 暗号化し、異なるルートで配送することにより、情報配送時の情報漏洩を防止する情報漏洩対策ソフト
SplitSafe	PCパソコンやノートパソコン上の機密ファイルの漏洩・盗難を防止するセキュリティソフトウェア。分散情報管理によってファイルを2つの断片に分離し、物理的に異なる1片は内蔵ハードディスク、もう1片をUSBメモリなどの外部媒体に保存。従来の鍵暗号によるファイルの暗号化とは異なり、パソコンとUSBメモリなど、2つの物理的な媒体が揃わなければファイルを復元することができないため、より高いセキュリティレベルで秘密ファイルを保護。
Trusted Exchange Manager V2	情報の流れをコントロールしながら、情報を漏らさず 共有を可能にする、新時代のファイルサーバ
Secure Traffic Probe	Secure Traffic Probe（異常トラフィック監視システム）は、ネットワーク管理者の業務支援を目的としたアプライアンス製品です。

(出典：http://www.oki.com/jp/NBC/sec.html)

2.15.3 技術開発拠点と研究者

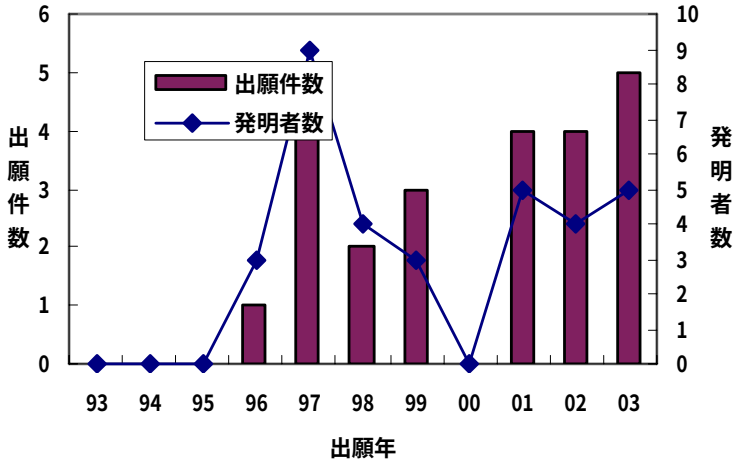
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

図2.15.3に、沖電気工業の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の３年間の平均は、出願件数が４件で、発明者が７人である。

図2.15.3 沖電気工業の不正アクセス侵入検知防御技術に関する出願件数と発明者数



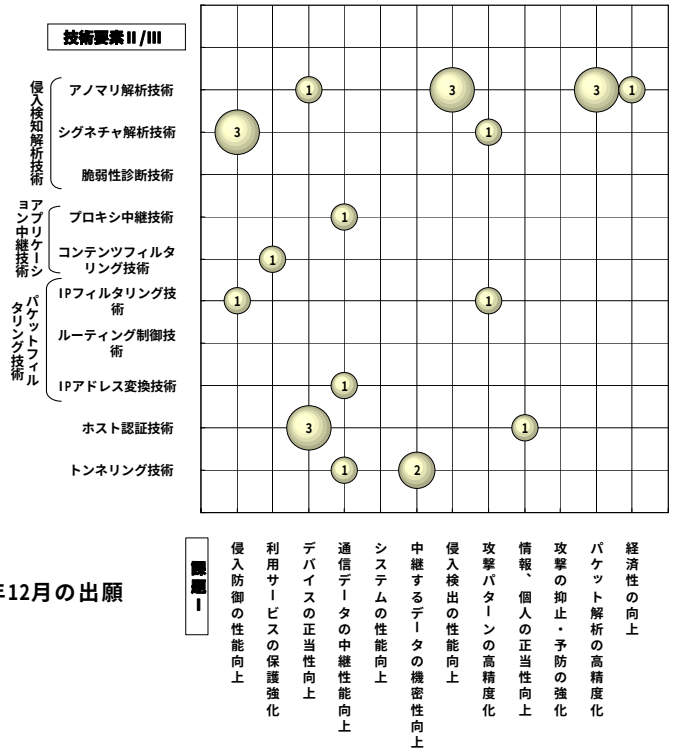
2.15.4 技術開発課題対応特許の概要

図2.15.4-1に、沖電気工業の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.15.4-2に、沖電気工業の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術に関する出願が8件されている。これらの出願のうち、「侵入防御の性能向上」と「デバイスの正当性向上」の課題が各４件である。

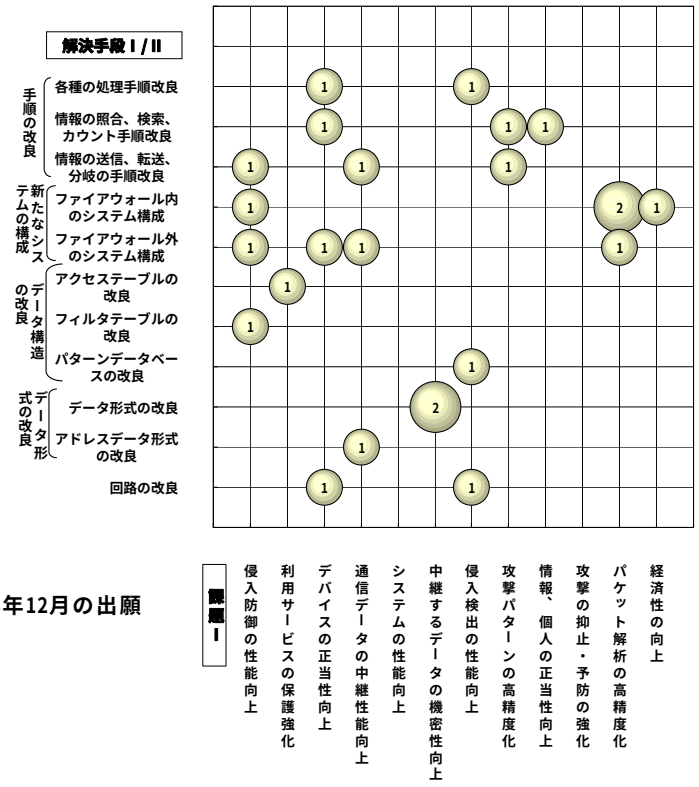
「中継するデータの機密性向上」の課題に対しては、「データ形式の改良」で２件対応している。さらに「パケット解析の高精度化」の課題に対しては、「ファイアウォール内のシステム構成」で２件対応している。

図2.15.4-1 沖電気工業の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.15.4-2 沖電気工業の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.15.4 沖電気工業の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は23件で、そのうち２件が登録特許である。なお、表2.15.4では図2.15.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.15.4 沖電気工業の技術要素別課題対応特許（1/3）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	デバイスの正当性向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開平11-032075 (みなし取下) 97.07.08 H04L12/56	ｺﾝﾋﾟｭｰﾀのｻｰﾋﾞｽ提供ｼｽﾃﾑ
	侵入検出の性能向上	各種の処理手順改良 特定情報の記憶、登録手順 ﾛｸﾞ情報の記憶	特開2004-013553 02.06.07 G06F13/00,351	被害判別装置､被害判別方法及び被害判別ｼｽﾃﾑ
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 振舞い形式の学習	特開2005-165541 03.12.01 G06F15/00	被害判定装置､被害解析装置､被害判別ｼｽﾃﾑ､被害判定ﾌﾟﾛｸﾞﾗﾑ及び被害解析ﾌﾟﾛｸﾞﾗﾑ
		回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2004-038557 02.07.03 G06F13/00,351	不正ｱｸｾｽ遮断ｼｽﾃﾑ
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特開2004-145687 02.10.25 G06F13/00,351	攻撃検知ｼｽﾃﾑ及び攻撃検知方法
			特開2005-117100 03.10.02 H04L12/66	侵入検知ｼｽﾃﾑおよびﾄﾗﾋｯｸ集約装置
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2005-130178 03.10.23 H04L12/46	通信装置の保守方法
	経済性の向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特開2004-145687 02.10.25 G06F13/00,351	攻撃検知ｼｽﾃﾑ及び攻撃検知方法 概要は技術要素「ｱﾉﾏﾘ解析」､課題「ﾊﾟｹｯﾄ解析の高精度化」の項参照
シグネチャ解析技術	侵入防御の性能向上	情報の送信、転送､分岐の手順改良 特定情報の通知、送信手順 擬似､ﾀﾞﾐﾃﾞｰﾀの送信	特開2003-198624 01.12.28 H04L12/56,400	装置間導通試験方法および装置
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2000-132473 98.10.23 G06F13/00,351	ﾌｧｲｱｳｫｰﾙ動的制御方式を用いたﾈｯﾄﾜｰｸｼｽﾃﾑ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特開平09-284330 (みなし取下) 96.04.18 H04L12/46	ﾈｯﾄﾜｰｸ間接続装置
	攻撃パターンの高精度化	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 使用回数	特開2003-108450 01.09.27 G06F13/00,353 沖情報ｼｽﾃﾑｽﾞ	TCP/IPのﾎﾟｰﾄ使用効率を向上させた端末装置および接続処理方法
プロキシ中継技術	通信データの中継性能向上	情報の送信、転送､分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ､ｽｸﾘﾌﾟﾄ	特開2000-215120 99.01.22 G06F13/00,351	分散型非同期ﾜｰｸﾌﾛｰ装置

表2.15.4 沖電気工業の技術要素別課題対応特許（2/3）

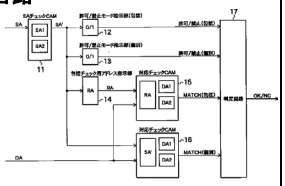
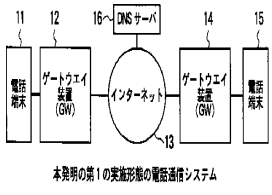
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	**発明の名称** 概要
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特許3504150 98.07.23 H04L12/22 日本電信電話	**ｺﾈｸｼｮﾝﾚｽ交換装置及びｱｸｾｽﾁｪｯｸ回路**  ｯｾｰｼﾞのｱｸｾｽ可否を判定するｱｸｾｽﾁｪｯｸ回路において､ｸﾞﾙｰﾌﾟ単位のｱﾄﾞﾚｽ情報に基づいて､ｱｸｾｽ可否を判定する包括ﾁｪｯｸ機能部と､端末単位のｱﾄﾞﾚｽ情報に基づいて､ｱｸｾｽ可否を判定する個別ﾁｪｯｸ機能部と､上記包括ﾁｪｯｸ機能部及び個別ﾁｪｯｸ機能部の双方又は一方の判定結果に基づいて､判定可否を最終判断する判定部とを備えたことを特徴とするｱｸｾｽﾁｪｯｸ回路。
IPフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開2003-186632 01.12.20 G06F3/12	**遠隔端末接続ｼｽﾃﾑ**
IPフィルタリング技術	攻撃パターンの高精度化	情報の送信､転送､分岐の手順改良 情報転送の手順 ﾎﾟﾘｼ設定情報	特開2004-086880 02.06.27 G06F15/00,330	**警戒ｼｽﾃﾑ､広域ﾈｯﾄﾜｰｸ防護ｼｽﾃﾑ､不正ｱｸｾｽ追跡方法､不正ｱｸｾｽ検知ｼｽﾃﾑ､ｾｷｭﾘﾃｨ管理方法及び攻撃防護方法**
IPアドレス変換技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 DNS､DHCPｻｰﾊﾞｰ配置	特許3436471 97.05.26 H04L12/66	**電話通信方法及び電話通信ｼｽﾃﾑ**  本発明の第1の実施形態の電話通信システム ｲﾝﾀｰﾈｯﾄを介して各ｹﾞｰﾄｳｪｲ装置に接続され､ｲﾝﾀｰﾈｯﾄに接続されている各ｹﾞｰﾄｳｪｲ装置の名前､名前に対応するｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽ､及び該各ｹﾞｰﾄｳｪｲ装置にそれぞれ割付けられた電話番号中の局番を管理する名前ｻｰﾊﾞを設けておき､各電話端末のうちの第1の電話端末から第2の電話端末に対する接続要求があった時､第1の電話端末の発呼に基づき､各ｹﾞｰﾄｳｪｲ装置のうちの第1の電話端末を収容している第1のｹﾞｰﾄｳｪｲ装置が制御用回線の第1のﾁｬﾈﾙを介して前記名前ｻｰﾊﾞへｱｸｾｽし､各ｹﾞｰﾄｳｪｲ装置のうちの第2の電話端末を収容している第2のｹﾞｰﾄｳｪｲ装置の局番に対応した名前を用いて第2のｹﾞｰﾄｳｪｲ装置のｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽを問い合わせる相手先問い合わせ処理と､名前ｻｰﾊﾞが第2のｹﾞｰﾄｳｪｲ装置のｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽを第1のﾁｬﾈﾙを介して第1のｹﾞｰﾄｳｪｲ装置へ応答する問い合わせ応答処理と､第1のｹﾞｰﾄｳｪｲ装置が自装置に接続されている音声用回線のｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽを選択し､且つ制御用回線の第2のﾁｬﾈﾙを介して第2のｹﾞｰﾄｳｪｲ装置に対して呼接続要求を行う呼接続要求処理と､第2のｹﾞｰﾄｳｪｲ装置が前記第2の電話端末が使用中か否かを判定し､不使用であれば音声用回線のｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽを選択し､選択したｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽを第1のｹﾞｰﾄｳｪｲ装置に返送して第1の電話端末と第2の電話端末とを接続する接続応答処理と､第1のｹﾞｰﾄｳｪｲ装置が第1の電話端末から送出された音声信号を音声用回線を介して第2のｹﾞｰﾄｳｪｲ装置へ伝送し､第2のｹﾞｰﾄｳｪｲ装置が伝送された音声信号を第2の電話端末へ送出する通話処理とを､行うことを特徴とする電話通信方法。

表2.15.4 沖電気工業の技術要素別課題対応特許（3/3）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
ホスト認証技術	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特開2001-092782 99.09.20 G06F15/00,330	情報ﾈｯﾄﾜｰｸ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2005-191830 03.12.25 H04M11/00,303	認識ｼｽﾃﾑおよび情報端末装置の認識方法
		回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特開平11-025046 (みなし取下) 97.07.03 G06F15/00,330	通信情報の保護方法
	情報、個人の正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報のｶｳﾝﾄ手順 ｴﾗｰ	特開2004-220123 03.01.09 G06F17/60,172	渉外員支援ｼｽﾃﾑおよびそのﾌﾟﾛｸﾞﾗﾑ
トンネリング技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開平10-224409 (拒絶確定) 97.02.07 H04L12/66 〔被引用回数 1〕	通信ｼｽﾃﾑ
	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 鍵情報のﾊﾟｯｸ化	特開2001-094600 99.09.24 H04L12/56	ﾒｯｾｰｼﾞ転送ﾉｰﾄﾞ及びﾈｯﾄﾜｰｸ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 識別子情報の変換	特開2003-110553 (みなし取下) 01.10.01 H04L9/32	ﾃﾞｰﾀ出力ｼｽﾃﾑおよびﾃﾞｰﾀ出力方法

2.16 サン・マイクロシステムズ

2.16.1 企業の概要

商号	Sun Microsystems, Inc.
本社所在地	4150 Network Circle, Santa Clara, CA 95054, U.S.A.
設立年	1982年
資本金	6,607百万米ドル（2004年6月末）
従業員数	約35,000名（連結：2004年9月）
事業内容	ネットワーク・コンピューティングの基盤となるコンピュータ・システム、ソフトウェア、関連機器および保守・教育等関連サービスの提供

「The Network is The Computer」はSunの創業当時から使われていて、Sunのビジョンを最も端的に表すフレーズである。ネットワークこそがコンピュータであり、ネットワークに接続されていないコンピュータには価値がない。今日であれば、この理念に賛同されない方はいらっしゃらないでしょうが、20年以上も前から「The Network is The Computer」と言い続けていたところにSunの先見性があると紹介されている。

(出典：http://jp.sun.com/company/#)

2.16.2 製品例

セキュリティ関連製品に紹介されているなかから、不正アクセス侵入検知防御技術に関連する製品やサービスを、表2.16.2に示す。

表2.16.2 サン・マイクロシステムズの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
Sun Crypto Accelerator 4000	セキュリティ・アクセラレータ機能（SSLおよびIPsec/IKEのためのコプロセッサ）と1つのGigabit Ethernetポート（1000BASE-SXまたは1000BASE-T）を1枚のPCI拡張カードで提供する製品。PCI拡張スロットを効率的に利用しながら高スループットの安全な通信を実現。
Sun Crypto Accelerator 1000	Eコマース等で標準的に使用されるSSLトランザクション処理を高速化するコプロセッサを提供するPCI拡張カード。さらにSolaris 9 4/03以降ではIPsec/IKEからも利用でき、ホストCPUの負荷を軽減しながら高スループットの安全な通信を実現。
Sun Crypto Accelerator 500	Sun Crypto Accelerator 1000の機能を、Sun Fire V210およびSun Fire V240に対するドータカード（メザニンカード）として実装したセキュリティ・アクセラレータ。薄型サーバでは貴重な資源であるPCI拡張スロットを使用することなく、SSL、IPsec/IKEのアクセラレーション機能を利用可能。

(出典：http://jp.sun.com/products/networking/sslaccel/)

2.16.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

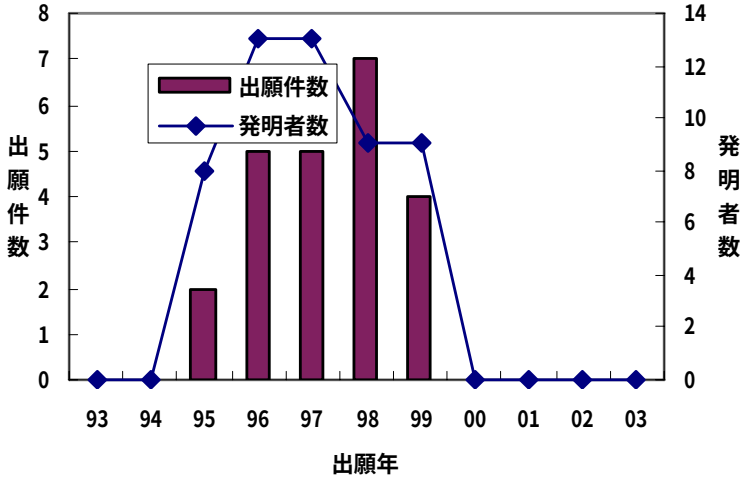
開発拠点：

アメリカ合衆国：カリフォルニア州、マサチューセッツ州

パキスタン：イスラマバード

図2.16.3に、サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。５年前までの平均は、出願件数が５件、発明者が11人であったが、ここ４年の出願がなされていない。

図2.16.3　サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する出願件数と発明者数



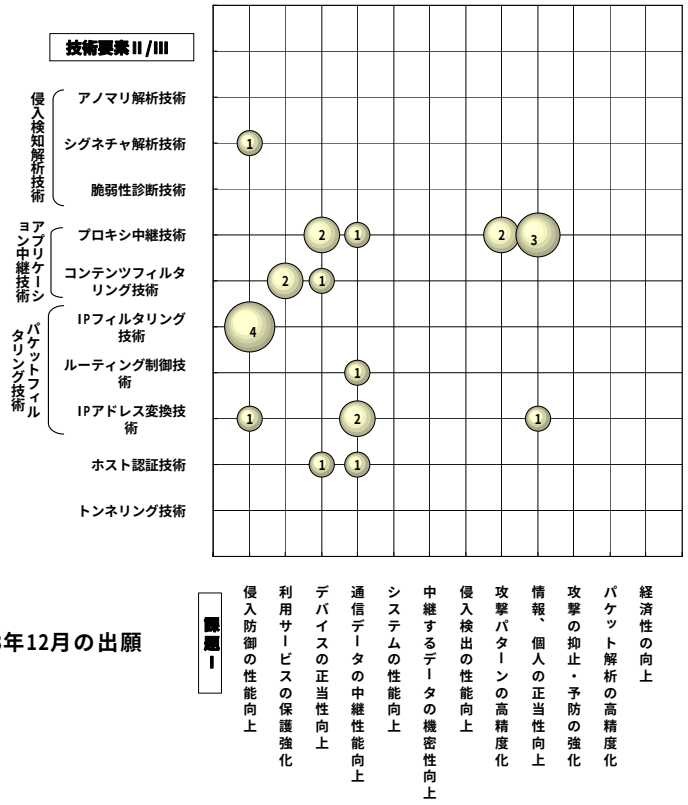
2.16.4 技術開発課題対応特許の概要

図2.16.4-1に、サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.16.4-2に、サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

プロキシ中継技術に関する出願が多い。これらの出願のうち、「侵入防御の性能向上」の課題が６件であり、「通信データの中継性能向上」が５件ある。

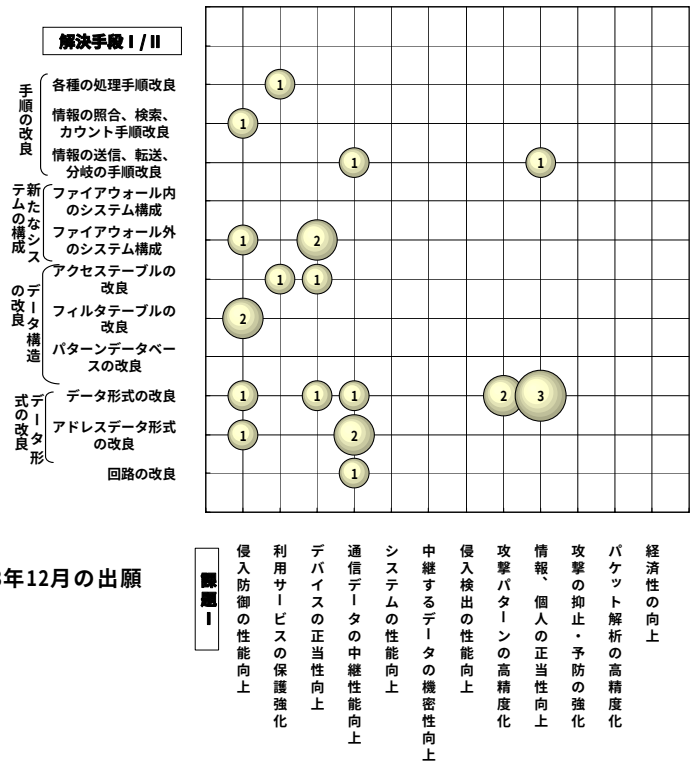
「情報、個人の正当性向上」の課題に対しては、「データ形式の改良」で３件対応している。

図2.16.4-1 サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.16.4-2 サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.16.4 サン・マイクロシステムズの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は23件である。なお、表2.16.4では図2.16.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.16.4 サン・マイクロシステムズの技術要素別課題対応特許（1/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
シグネチャ解析技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾊﾟｹｯﾄｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特開平09-270788 95.10.26 H04L9/32 〔被引用回数 1〕	ｾｷｭｱ・ﾈｯﾄﾜｰｸ・ﾌﾟﾛﾄｺﾙ・ｼｽﾃﾑ及び方法
プロキシ中継技術	デバイスの正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2001-067317 99.06.14 G06F15/00,330	ｻｰﾌﾞﾚｯﾄｴﾝｼﾞﾝにｶｽﾀﾏｲｽﾞ可能なｾｷｭﾘﾃｨおよびﾛｷﾞﾝｸﾞﾌﾟﾛﾄｺﾙを提供するための方法および装置
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開平09-224053 (取下) 95.05.18 H04L12/66 〔被引用回数 2〕	ｺﾝﾋﾟｭｰﾀ・ﾈｯﾄﾜｰｸ・ｲﾝﾀﾌｪｰｽにおけるﾃﾞｰﾀ・ﾊﾟｹｯﾄのﾊﾟｹｯﾄ・ﾌｨﾙﾀﾘﾝｸﾞ・ｼｽﾃﾑ
	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 更新差分情報の送信	特表2001-519059 (みなし取下) 97.03.31 G06F15/00,330	ｲﾝﾀｰﾈｯﾄを利用した安全な事象駆動電子ﾃﾞｰﾀ交換取引処理
	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾊﾟｹｯﾄｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特開平11-149456 97.06.19 G06F15/16,430	ﾘﾓｰﾄｵﾌﾞｼﾞｪｸﾄ呼出し用ｼｽﾃﾑ及び方法
			特開平10-116195 96.06.26 G06F9/44,530	ｾｷｭｱ方式にてｵﾌﾞｼﾞｪｸﾄの位置を見出すための機構
	情報、個人の正当性向上	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ、ｽｸﾘﾌﾟﾄ	特表2002-541578 99.04.08 G06F1/00	ﾀﾞｳﾝﾛｰﾄﾞしたﾌﾟﾛｷｼｺｰﾄﾞの信頼性を確立するためのﾒｿｯﾄﾞおよびｼｽﾃﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特開平10-133925 (みなし取下) 96.06.10 G06F12/00,531	ﾊﾟｽｸｱｳﾌﾟを第三者預託する方法およびｼｽﾃﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特表2002-512487 98.04.20 H04L12/56	ﾈｯﾄﾜｰｸでﾊﾟｹｯﾄをﾌｨﾙﾀﾘﾝｸﾞするためにﾃﾞｼﾞﾀﾙ署名を使用する方法および装置
コンテンツフィルタリング技術	利用サービスの保護強化	各種の処理手順改良 各種処理の実行手順 ﾊﾟﾀｰﾝ、ﾙｰﾙの言語記述	特表2002-517053 98.05.22 G06F13/00,351	ｺﾝﾋﾟｭｰﾀ/通信ﾈｯﾄﾜｰｸで実行可能ｺｰﾄﾞのﾈｯﾄﾜｰｸ・ｾｷｭﾘﾃｨを講じるための装置、方法及びｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特開平10-326256 (みなし取下) 96.12.18 G06F15/00,330	ﾏﾙﾁﾚﾍﾞﾙｾｷｭﾘﾃｨﾎﾟｰﾄ方法、装置、及びｺﾝﾋﾟｭｰﾀﾌﾟﾛｸﾞﾗﾑ製品
	デバイスの正当性向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開2001-067315 99.06.14 G06F15/00,330	ｴﾝﾀｰﾌﾟﾗｲｽﾞ・ｺﾝﾋﾟｭｰﾀ・ｼｽﾃﾑ内の異なる複数の認証ｼｽﾃﾑを扱う分散認証ﾒｶﾆｽﾞﾑ

表2.16.4 サン・マイクロシステムズの技術要素別課題対応特許（2/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開2000-123097 (みなし取下) 97.02.06 G06F19/00 〔被引用回数 2〕	ﾌｧｲｱｳｫｰﾙを介するｾｷｭｱな取引を許容するための方法及び装置
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞ-の配置 ﾌﾟﾛｷｼｻｰﾊﾞ-の配置	特表2002-518726 98.06.19 G06F12/00,546 〔被引用回数 1〕	ﾌﾟﾗｸﾞｲﾝﾌｨﾙﾀを用いた拡張性の高いﾌﾟﾛｷｼｻｰﾊﾞ
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 自動登録	特表2001-506093 96.12.09 H04L12/56 ﾓﾄﾛｰﾗ(米国)	動的ﾊﾟｹｯﾄ・ﾌｨﾙﾀ割り当て方法及び装置
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特表2001-510603 96.12.09 G06F13/00,351	分散型ﾏﾙﾁｻｰﾊﾞ・ﾈｯﾄﾜｰｸ環境におけるｱｸｾｽ制御方法および装置
ルーティング制御技術	通信データの中継性能向上	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特表2003-505934 99.07.15 H04L12/66	安全なﾈｯﾄﾜｰｸ・ｽｲｯﾁ
IPアドレス変換技術	侵入防御の性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2000-207320 98.06.30 G06F13/00,351	ﾘﾓｰﾄｱｸｾｽ方法
	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2000-049867 98.05.29 H04L12/56 〔被引用回数 1〕	ｲﾝﾀｰﾈｯﾄなどの公衆ﾈｯﾄﾜｰｸに接続された装置とﾈｯﾄﾜｰｸに接続された装置の間の通信を容易にするｼｽﾃﾑおよび方法
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 相対ｱﾄﾞﾚｽの割付	特表2002-522964 98.08.03 H04L12/46	ﾓﾊﾞｲﾙIPに関する連鎖ﾚｼﾞｽﾀﾚｰｼｮﾝ
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開平11-008620 (みなし取下) 97.04.18 H04L9/32	通信ﾁｬﾈﾙの認証を効率的に実施し、不正な変更の検出を容易にするｼｽﾃﾑおよび方法
ホスト認証技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 認証情報の変換	特開平11-167536 (拒絶確定) 97.06.27 G06F13/00,351	ｺﾝﾋﾟｭｰﾀ・ﾈｯﾄﾜｰｸを利用したｸﾗｲｱﾝﾄ/ﾎｽﾄ間の通信方法と装置
	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特表2002-521962 98.07.31 H04L9/08	認証ﾄｰｸﾝを使用して共有秘密を確立する方法及びｼｽﾃﾑ

2.17 横河電機

2.17.1 企業の概要

商号	横河電機　株式会社
本社所在地	〒180-8750　東京都武蔵野市中町2-9-32
設立年	1920年（大正9年）
資本金	323億06百万円（2005年3月末）
従業員数	5,112名（2005年3月末）（連結：18,972名）
事業内容	計測・制御機器の製造・販売、生産管理システム・医療情報システムの設計・製造・販売、他

YOKOGAWAは、産業界に先端マザーツール、先端技術基盤を提供することが使命である。自ら培ってきたパワーでYOKOGAWAの強みを生かし、お客様のビジネスを深く理解し、お客様にソリューション提案を行い、最大限の付加価値創造を実現することが豊かな人間社会に貢献することにつながると考えている。(出典：http://www.yokogawa.co.jp/)

2.17.2 製品例

IPネットワーク事業で紹介されているネットワークセキュリティ製品のうち、不正アクセス侵入検知防御技術に関連する製品やサービスを、表2.17.2に示す。

表2.17.2 横河電機の不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
SecureTicket	強力・安全な“ユーザ認証”をベースに多彩な機能を搭載した他に類のない高コストパフォーマンスの統合セキュリティソフト。認証、SSL-VPN、リバースプロキシの３機能を軸にエクストラネットや会員制サイト構築の支援。
ネットワーク侵入センサ ISシリーズ	世界・国内で圧倒的シェアを誇るインターネットセキュリティシステムズ株式会社のRealSecure® Network Sensorを実装したIDSアプライアンス。
Proventiaシリーズ	ISS社のRealSecureの技術をベースに、さらにパワフルになった防御エンジンと、ISS社の情報力の源である セキュリティ情報組織「X-Force」のナレッジ、そして世界に複数の拠点を持ち、実際にインターネットの脅威から24時間 365日、ネットワークを守り続けているセキュリティ監視センター（SOC：Security Operation Center）の防御ノウハウを結集。Proventiaシリーズは、セキュリティパッチを適用できない間も、仮想的にセキュリティパッチを適用した状態「Virtual Patch」を作り、重要なサーバ群やネットワークを防御。

(出典：http://www.yokogawa.co.jp/ipnet/index.htm)

2.17.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

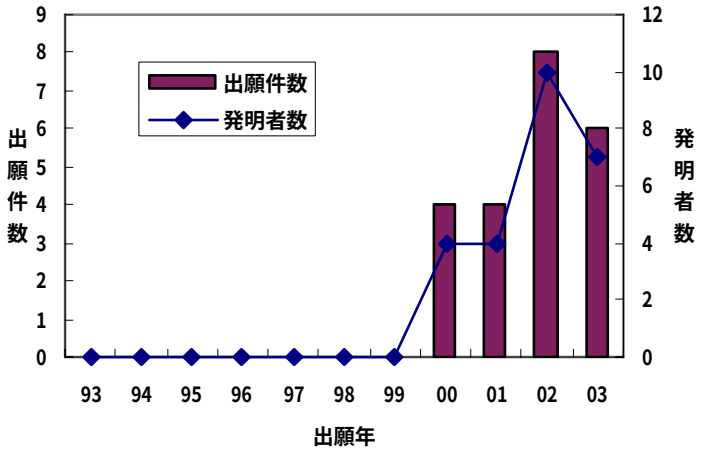
開発拠点：

東京都武蔵野市中町2丁目9番32号 横河電機株式会社内

山梨県甲府市高室町155番地　横河電機株式会社甲府事業所内

図2.17.3に、横河電機の不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。この４年間の出願のみで、平均で５件の出願件数であり、６人の発明者数である。

図2.17.3 横河電機の不正アクセス侵入検知防御技術に関する出願件数と発明者数



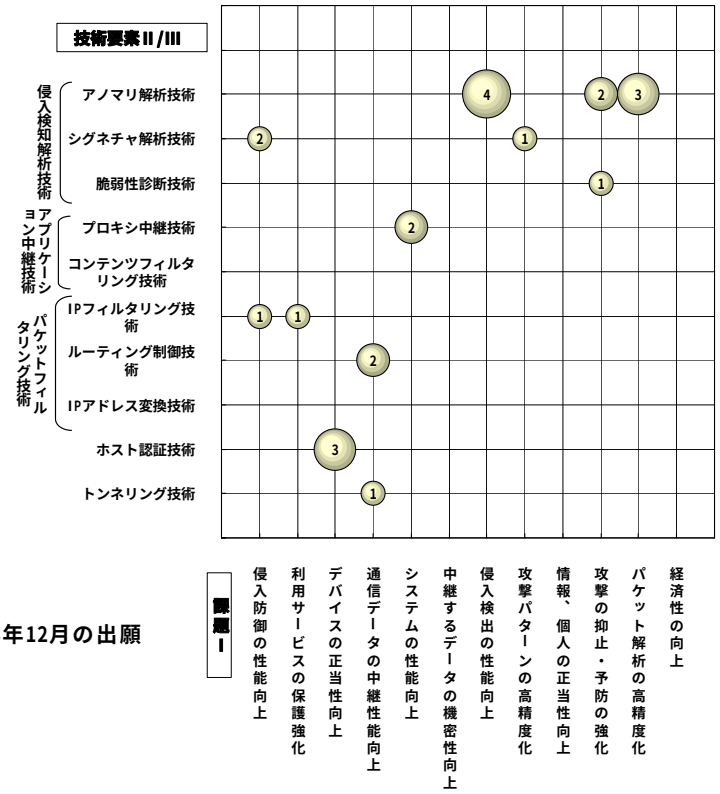
2.17.4 技術開発課題対応特許の概要

図2.17.4-1に、横河電機の不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.17.4-2に、横河電機の不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術に関する出願が多い。これらの出願のうち、「侵入検出の性能向上」の課題が４件ある。

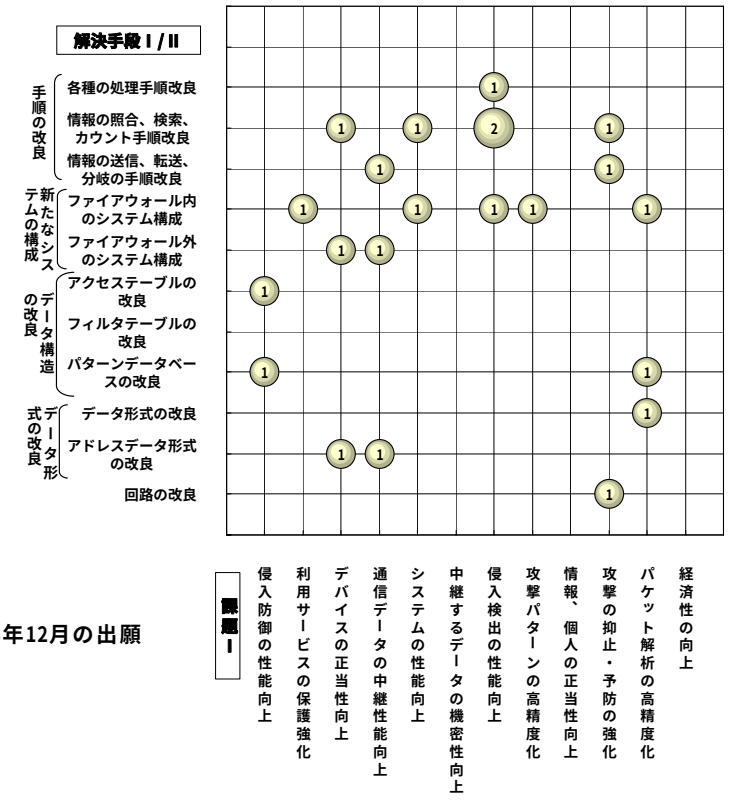
「侵入検出の性能向上」の課題に対して、「情報の照合、検索、カウント手順改良」で２件対応している。

図2.17.4-1横河電機の不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.17.4-2横河電機の不正アクセス侵入検知防御技術に関する課題と解決手段の分布



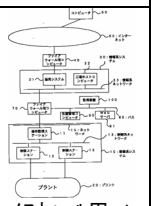
1993年1月～2003年12月の出願

表2.17.4横河電機の不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は22件で、そのうち１件が登録特許である。なお、表2.17.4では図2.17.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.17.4 横河電機の技術要素別課題対応特許（1/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	侵入検出の性能向上	各種の処理手順改良 各種処理の実行手順 特定情報の表示	特開2005-012312 03.06.17 H04L12/66	ｲﾍﾞﾝﾄﾛｸﾞ表示方法及びこれを用いた侵入検知ｼｽﾃﾑ
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特開2004-120695 02.09.30 H04L12/22	ﾊﾟｹｯﾄ経路追跡ｼｽﾃﾑ
		情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ｱﾄﾞﾚｽの検索	特開2003-298652 (拒絶確定) 02.03.29 H04L12/56,400	攻撃経路追跡ｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 収集器の配置	特開2005-175993 03.12.12 H04L12/22	ﾜｰﾑ伝播監視ｼｽﾃﾑ
	攻撃の抑止・予防の強化	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開2003-304289 (特許3700671) 02.04.10 H04L12/56,400	ｾｷｭﾘﾃｲ管理ｼｽﾃﾑ
		情報の送信、転送､分岐の手順改良 特定情報の通知、送信手順 警告情報	特開2004-005147 02.05.31 G06F15/00,330	ｱｸｾｽ制御機能を備えた装置
	パケット解析の高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開2002-111667 00.10.02 H04L12/24	ﾛｸﾞ保存装置
		ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加､切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特開2003-060712 01.08.20 H04L12/66	侵入監視ｼｽﾃﾑ及び侵入監視方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2004-128545 02.09.30 H04L12/22	ﾊﾟｹｯﾄﾛｸﾞ記録装置
シグネチャ解析技術	侵入防御の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 ﾄﾗﾌｨｯｸﾃﾞｰﾀの学習	特開2003-188893 (みなし取下) 01.12.19 H04L12/44,300	不正ｱｸｾｽ検知装置
	攻撃パターンの高精度化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特開2004-140618 02.10.18 H04L12/66	ﾊﾟｹｯﾄﾌｨﾙﾀ装置および不正ｱｸｾｽ検知装置

表2.17.4 横河電機の技術要素別課題対応特許（2/2）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
脆弱性診断技術	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 通信遮断回路	特開2001-273210 （取下） 00.03.27 G06F13/00,351 〔被引用回数 1〕	**外部ﾈｯﾄﾜｰｸからの侵入防止方法およびその装置**
プロキシ中継技術	システムの性能向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 遠隔制御ｺﾏﾝﾄﾞの抽出	特開2002-305777 01.04.06 H04Q9/00,301	**ﾘﾓｰﾄﾒﾝﾃﾅﾝｽ･ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 監視装置の配置	特開2004-220298 03.01.15 G05B23/02	**操作･監視ｼｽﾃﾑ**
IPフィルタリング技術	侵入防御の性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特開2004-054488 02.07.18 G06F13/00,351	**ﾌｧｲｱｳｫｰﾙ装置**
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特許3446891 00.12.14 G05B23/02 〔被引用回数 1〕	**監視ｼｽﾃﾑ**  監視対象への不正ｱｸｾｽを監視する監視ｼｽﾃﾑにおいて、監視対象を管理する情報系ｼｽﾃﾑと監視対象を制御する制御系ｼｽﾃﾑとの間に介在し、前記情報系ｼｽﾃﾑから制御系ｼｽﾃﾑへのｱｸｾｽを制限するﾌｧｲｱｳｫｰﾙの機能を果たすﾌｧｲｱｳｫｰﾙ用ｺﾝﾋﾟｭｰﾀと、このﾌｧｲｱｳｫｰﾙ用ｺﾝﾋﾟｭｰﾀに結合されたﾊﾞｽ上に接続されたｺﾝﾋﾟｭｰﾀと、前記ﾊﾞｽ上の通信を監視し、ﾌｧｲｱｳｫｰﾙ用ｺﾝﾋﾟｭｰﾀを通過したｱｸｾｽが前記ｺﾝﾋﾟｭｰﾀへのｱｸｾｽであるときは正当なｱｸｾｽとし、このｱｸｾｽが前記ｺﾝﾋﾟｭｰﾀへのｱｸｾｽでないときは不正なｱｸｾｽとする監視装置と、を有することを特徴とする監視ｼｽﾃﾑ。
ルーティング制御技術	通信データの中継性能向上	情報の送信、転送､分岐の手順改良 情報転送の手順 ﾌﾟﾛｸﾞﾗﾑ､ｽｸﾘﾌﾟﾄ	特開2004-341975 03.05.19 G06F9/445	**ﾌｧｲﾙ編集ｼｽﾃﾑ及び編集方法**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2001-290785 00.04.04 G06F15/16,620	**ORBｼｽﾃﾑ及びｴｰｼﾞｪﾝﾄｼｽﾃﾑの構築方法**
ホスト認証技術	デバイスの正当性向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾜﾝﾀｲﾑID	特開2004-178361 02.11.28 G06F15/00,330	**ﾕｰｻﾞｰ認証方式及びこれを用いたﾕｰｻﾞｰ認証ｼｽﾃﾑ**
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2003-085140 01.09.13 G06F15/00,330	**ｸﾗｲｱﾝﾄ認証方法**
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 IPv6の割付	特開2005-006147 03.06.13 H04L12/56	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**
トンネリング技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2005-064928 03.08.14 H04L12/22	**ｾｷｭﾘﾃｨ通信方法及びこれを用いた装置**

2.18 エヌ・ティ・ティ・ドコモ

2.18.1 企業の概要

商号	株式会社　エヌ・ティ・ティ・ドコモ
本社所在地	〒100-6150　東京都千代田区永田町2-11-1　山王パークタワー
設立年	1992年（平成4年）
資本金	9,496億79百万円（2005年3月末）
従業員数	5,856名（2005年3月末）（連結：21,527名）
事業内容	携帯電話サービス、パケット通信サービス、衛星電話サービス、国際電話サービスと各サービスの端末機器の販売

環境の変化を予測し、常に確信的なサービスを提供してきたNTTドコモ。ユーザの課題を正確に把握し、最適な携帯端末の選定とソリューションのご提案を実現する。様々なビジネスシーンに活用できるセキュリティ課題を重点的に強化したソリューションメニュー、これらのサービスは、セキュリティ・安全性の確保を基本とし、多様な要望に対応する。偽造・変造されにくく、高い安全性を保ちながらスピーディな送受信を実現する、非接触ICカード技術「FeliCa」をはじめ、PCにFOMA端末を接続して利用することも可能な、電子認証サービス「FirstPass」や電話番号による認証機能、そしてオールロック、遠隔ロック、指紋認証による盗難、紛失時の情報漏洩防止機能など携帯端末自体に高度なセキュリティ技術。これらの機能とさまざまなプラットフォーム、ソフトウェアなどとの組み合わせにより、会社の内外で携帯端末、PCを利用したイントラネットへのリモートアクセスにおける安全性の確保や、社内営業所などへの不正侵入者を防止する入退室認証、社内PC、プリンターなど機密を扱う機器の情報漏洩防止など、各種セキュリティシステムが驚くほど簡易に構築・利用を可能としている。

(出典；http://www.docomo.biz/html/product/security/)

2.18.2 製品例

表2.18.2に製品例とその特徴を示す。

表2.18.2 NTTドコモの不正アクセス侵入検知防御技術に関連する製品例(1/2)

製品名	概要・特徴
リモートアクセス利用時のセキュリティ　携帯版	①　紛失や盗難による情報漏洩 ②　なりすまし、盗聴防止；FirstPassサービス ③　セキュリティスキャン機能
リモートアクセス利用時のセキュリティ　PC版	①　セキュリティの基礎とも言える認証・暗号化；FirstPass＋セキュリティソフト ②　簡単にPC本体にPCロック ③　なりすまし、盗聴防止；FirstPassサービス ④　高度な盗聴防止策；アクセスmopera

表2.18.2 NTTドコモの不正アクセス侵入検知防御技術に関連する製品例(2/2)

製品名	概要・特徴
無線LAN利用時のセキュリティ	① なりすまし、盗聴などの不正アクセスに対して ② 高度なセキュリティ環境の構築

(出典：http://www.docomo.biz/html/product/security/sc/rmt_mb.html)

2.18.3 技術開発拠点と研究者

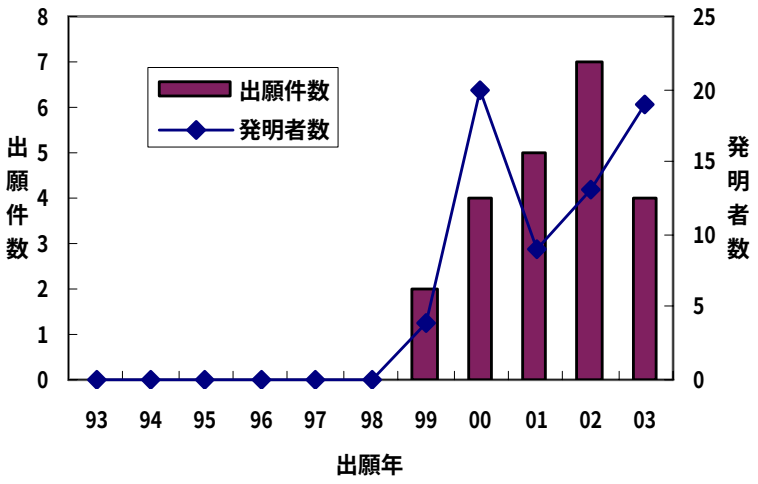
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

東京都千代田区永田町2丁目11番1号 株式会社NTTドコモ内

図2.18.3に、NTTドコモの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の５年間の平均は、出願件数で４件、発明者数が12人である。

図2.18.3 NTTドコモの不正アクセス侵入検知防御技術に関する出願件数と発明者数



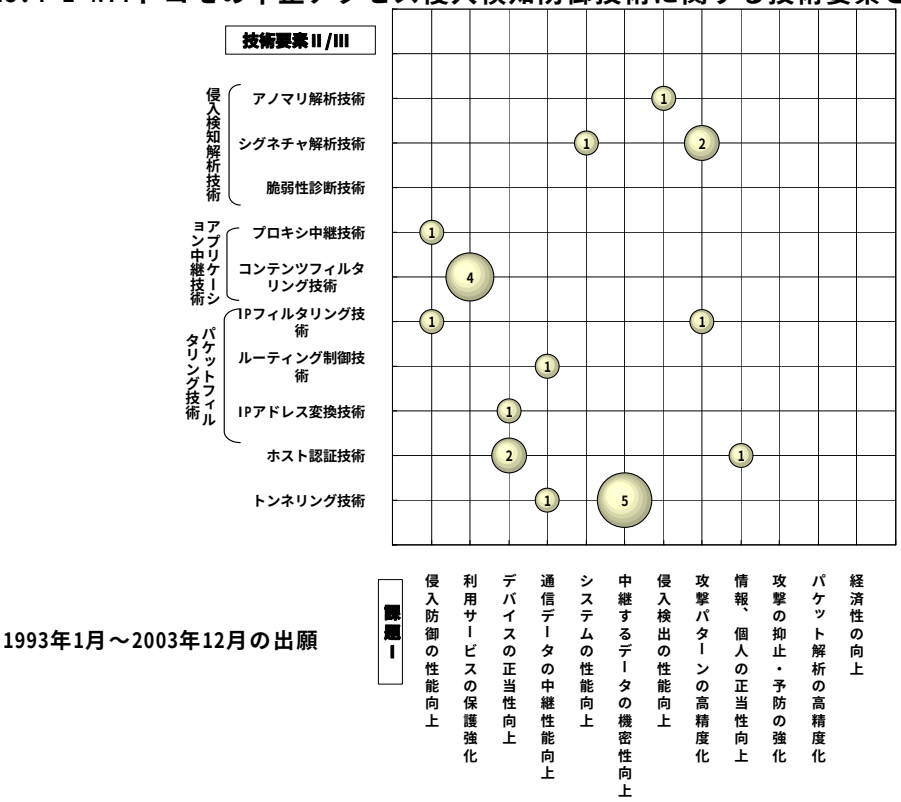
2.18.4 技術開発課題対応特許の概要

図2.18.4-1に、NTTドコモの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.18.4-2に、NTTドコモの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

トンネリング技術に関する出願が６件ある。「中継するデータの機密性向上」の課題に対する出願が５件ある。

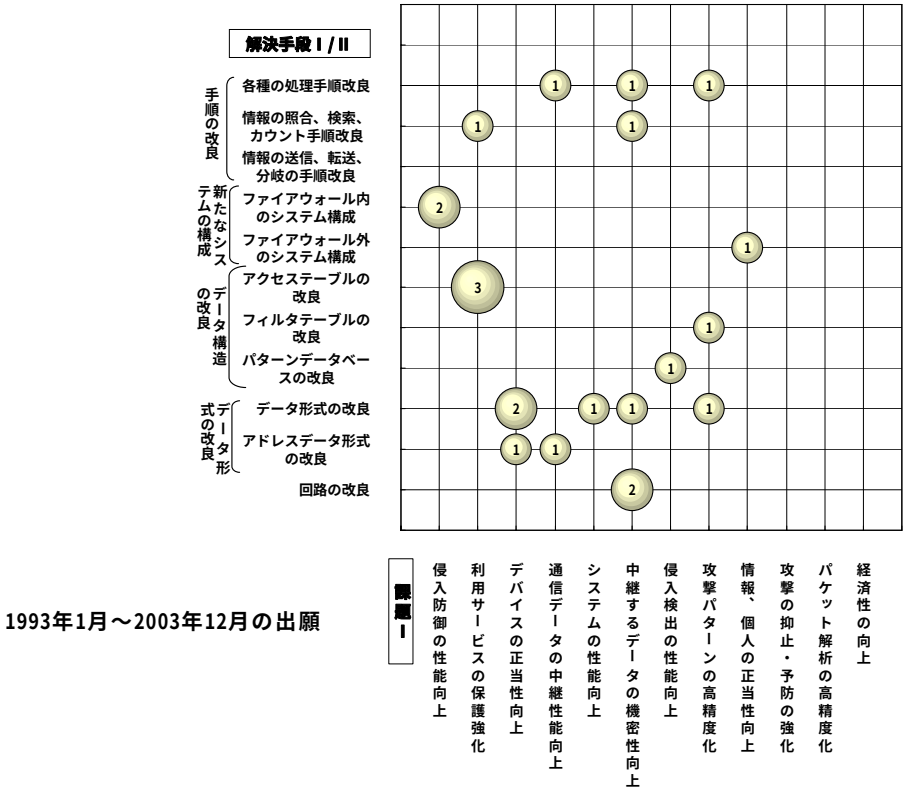
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で３件対応している。

図2.18.4-1 NTTドコモの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.18.4-2 NTTドコモの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.18.4 NTTドコモの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は22件である。なお、表2.18.4では図2.18.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.18.4 NTTドコモの技術要素別課題対応特許（1/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 各種ｱﾙｺﾞﾘｽﾞﾑの改良	特開2002-133388 00.10.25 G06N3/00	異種因子検出方法及びｼｽﾃﾑ
シグネチャ解析技術	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾌｫｰﾏｯﾄの変換	特開2004-086464 02.08.26 G06F13/00,351	監視ｼｽﾃﾑ、監視対象管理装置及び監視方法
	攻撃パターンの高精度化	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特開2005-128933 03.10.27 G06F1/00	情報処理装置、不正侵入検出方法及び不正侵入検出ﾌﾟﾛｸﾞﾗﾑ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ｺﾏﾝﾄﾞに情報付加	特開2004-302516 03.03.28 G06F15/00,330	端末装置およびﾌﾟﾛｸﾞﾗﾑ
プロキシ中継技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞ-の配置	特開2004-126735 02.09.30 G06F13/00,351	通信ｼｽﾃﾑ、中継装置及び通信制御方法
コンテンツフィルタリング技術	利用サービスの保護強化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	WO02-042920 00.11.22 G06F9/54	ﾈｯﾄﾜｰｸへのｱｸｾｽを管理する方法および装置
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2002-278860 01.03.16 G06F13/00,520	中継装置、通信装置、通信制御方法、通信制御ﾌﾟﾛｸﾞﾗﾑおよび通信制御ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
			特開2003-337630 02.05.17 G06F1/00 Klab	通信端末、ﾌﾟﾛｸﾞﾗﾑ、記録媒体、通信端末のｱｸｾｽ制御方法およびｺﾝﾃﾝﾂの提供方法
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け 許可証明書	特開2003-337716 02.05.20 G06F11/00 Klab	電子機器、ﾃﾞｰﾀ共用方法、ﾌﾟﾛｸﾞﾗﾑ及び記憶媒体
IPフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ｴｰｼﾞｪﾝﾄの配置	特開2004-180155 02.11.28 H04L12/56,100 〔被引用回数 1〕	通信制御装置、ﾌｧｲｱｳｫｰﾙ装置、通信制御ｼｽﾃﾑ、及び、ﾃﾞｰﾀ通信方法
	攻撃パターンの高精度化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開2005-039371 03.07.16 H04M3/42	中継装置
ルーティング制御技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2003-069626 01.08.28 H04L12/56,100	通信ｼｽﾃﾑ、通信方法及び通信制御装置

表2.18.4 NTTドコモの技術要素別課題対応特許（2/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPアドレス変換技術	デバイスの正当性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 IPｱﾄﾞﾚｽの変換	特開2002-247112 01.02.20 H04L12/66	TCP中継装置及びｼｰｹﾝｽ番号変換方法
ホスト認証技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-072631 02.08.08 H04Q7/38	無線通信における認証ｼｽﾃﾑ、認証方法及び端末装置
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾊｯｼｭ値の付加	特開2004-194196 02.12.13 H04L12/66	ﾊﾟｹｯﾄ通信認証ｼｽﾃﾑ、通信制御装置及び通信端末
	情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞｰの配置 認証ｻｰﾊﾞｰの配置	特開2002-049589 (拒絶確定) 00.08.02 G06F15/00,330	認証装置およびﾘﾓｰﾄｱｸｾｽ認証ｼｽﾃﾑ
トンネリング技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ切換	特開2002-111747 (特許3701866) 00.07.24 H04L12/66	中継装置、通信端末、及びｻｰﾊﾞ装置
	中継するデータの機密性向上	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特開2005-110302 99.08.27 H04L12/66	ｾｯｼｮﾝ情報管理方法およびｾｯｼｮﾝ情報管理装置
		情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ｱﾄﾞﾚｽの照合	特開2005-072668 03.08.26 H04L12/56	VPN通信ｼｽﾃﾑ及びVPNﾄﾝﾈﾙ形成方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾍﾟｲﾛｰﾄﾞの暗号化	特開2002-319936 01.04.20 H04L9/36	ﾃﾞｰﾀ安全化通信装置及びその方法
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特開2001-177514 99.12.17 H04L9/08	通信方法および通信装置
		回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特開2002-247113 01.02.22 H04L12/66	暗号化通信ｼｽﾃﾑ及び暗号化通信方法

2.19 セイコーエプソン

2.19.1 企業の概要

商号	セイコーエプソン　株式会社
本社所在地	〒392-8502　長野県諏訪市大和3-3-5
設立年	1942年（昭和17年）
資本金	532億4百万円（2005年3月末）
従業員数	12,828名（2005年9月末）（連結：98,480名）
事業内容	情報関連機器（PC、ﾌﾟﾘﾝﾀ・ｽｷｬﾅ等ｺﾝﾋﾟｭｰﾀ周辺機器、液晶ﾌﾟﾛｼﾞｪｸﾀｰ等映像機器）、電子ﾃﾞﾊﾞｲｽ、精密機器（ｳｵｯﾁ、眼鏡ﾚﾝｽﾞ）等の開発・製造・販売

個人情報保護法の施行をはじめとし、企業は情報の管理へ細心の注意を払わなくてはならない時代がやってきた。エプソンは出力時の情報管理・保護への課題を解決するため、オフィリオシナジーウェア[セキュリティ]を提供する。オフィスのセキュリティポリシや認証方法、印刷環境に合わせたフレキシブルな印刷セキュリティシステムの構築が可能となり、一般ユーザーはもちろん管理者や経営者にも、快適なオフィス環境を提供する。

(出典：http://www.i-love-epson.co.jp/products/offirio/sw/security/index.htm)

2.19.2 製品例

オフィリオシナジーウェア[セキュリティ]に紹介されているもののうち、不正アクセス侵入検知防御技術に関連する製品やサービスを、表2.19.2に、製品例とその概要を示す。

表2.19.2 セイコーエプソンの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
認証印刷	顧客情報や社員の査定表・給与明細など、たとえ社内ではあっても、他人に見られてはいけない情報がある。こうした情報が掲載されたドキュメントを印刷する際に、他の印刷物に紛れ込んでしまったり、間違って持っていかれたりすることなどを防止
印刷履歴管理	プリンタを利用する各ユーザーから印刷ログを自動収集。管理者は「誰が」「何を」「いつ」「何枚」印刷したかをチェックすることで、トレーサビリティを確保
不正コピー抑止	原本と複製を明確に区別する仕組みや、誰の出力物なのかを明確にすることで、不正な持ち出しや不正利用を抑止

(出典：http://www.i-love-epson.co.jp/products/oen/x_terminator/index.htm)

2.19.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

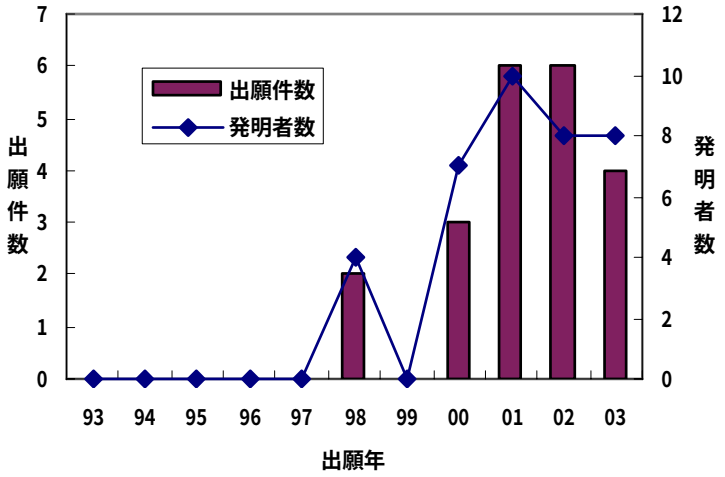
開発拠点：

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

長野県松本市芳川村井町1059番地 株式会社エプソンソフト開発センター内

図2.19.3に、セイコーエプソンの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。最近の４年間の平均は、出願件数が４件、発明者数が８人である。

図2.19.3 セイコーエプソンの不正アクセス侵入検知防御技術に関する出願件数と発明者数



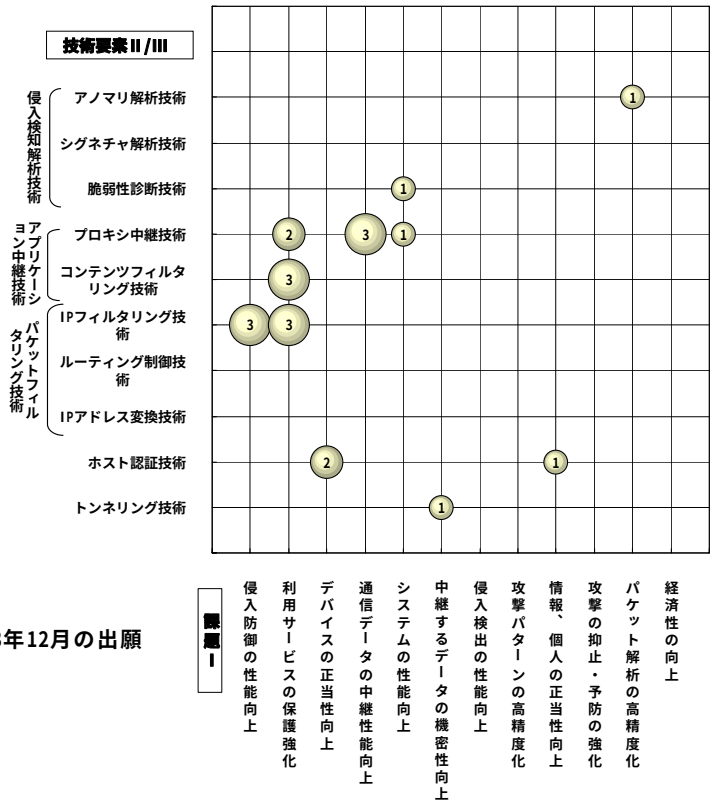
2.19.4 技術開発課題対応特許の概要

図2.19.4-1に、セイコーエプソンの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.19.4-2に、セイコーエプソンの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

プロキシ中継技術とIPフィルタリング技術に関する出願が各６件ある。これらの出願のうち、多い課題は、「利用サービスの保護強化」である。

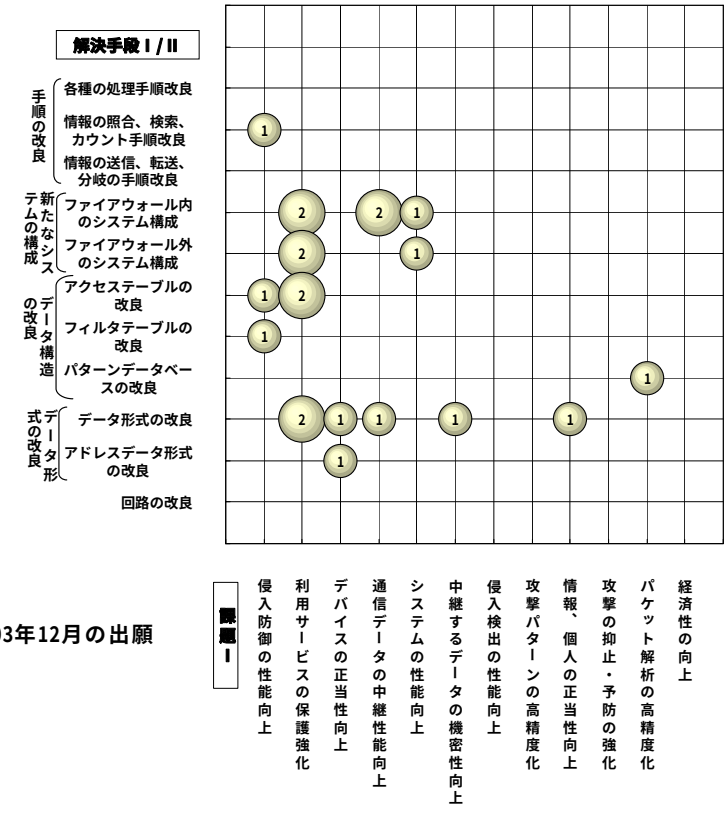
「利用サービスの保護強化」の課題に対しては、「ファイアウォール内のシステム構成」、「ファイアウォール外のシステム構成」、「アクセステーブルの改良」と「データ形式の改良」で各２件づつ対応している。

図2.19.4-1 セイコーエプソンの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.19.4-2 セイコーエプソンの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.19.4 セイコーエプソンの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は21件である。なお、表2.19.4では図2.19.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.19.4 セイコーエプソンの技術要素別課題対応特許（1/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	パケット解析の高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃情報の蓄積 ﾛｸﾞ情報の蓄積	特開2005-056243 03.08.06 G06F15/00,330	ﾜｰﾑの感染防止ｼｽﾃﾑ
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2004-129128 02.10.07 H04L12/22	ﾈｯﾄﾜｰｸ接続端子管理ｼｽﾃﾑとﾈｯﾄﾜｰｸ接続端子管理ﾌﾟﾛｸﾞﾗﾑ
プロキシ中継技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2002-312314 01.04.13 G06F15/00,310	ｻｰﾋﾞｽ提供ｼｽﾃﾑ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 仲介ｻｰﾊﾞｰ配置	特開2003-046580 01.04.05 H04L12/66	出力装置用のｾｷｭﾘﾃｨｼｽﾃﾑ
	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特開2003-108449 01.10.02 G06F13/00,351	ﾈｯﾄﾜｰｸに接続された仲介装置
			特開2004-318333 03.04.14 G06F13/00,357	接続機器情報開覧ｻｰﾊﾞｰ、接続機器情報管理ｻｰﾊﾞｰ、構内情報開覧ｻｰﾊﾞｰ、構内情報管理ｻｰﾊﾞｰ、接続機器情報開覧方法、構内情報開覧方法およびそれらの方法をｺﾝﾋﾟ
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2002-288145 01.03.28 G06F15/16,620	情報通信ｼｽﾃﾑおよびそのｲﾍﾞﾝﾄ処理方法並びに情報通信ｼｽﾃﾑにおけるｲﾍﾞﾝﾄ処理ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2003-018676 01.06.29 H04Q9/00,301	表示機器遠隔制御ｼｽﾃﾑ、表示機器及び表示機器用ﾌﾟﾛｸﾞﾗﾑ、並びに表示機器遠隔制御方法
コンテンツフィルタリング技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2004-206620 02.12.26 G06F3/12	印刷ｼｽﾃﾑ、及び、その制御方法
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開2004-086686 (みなし取下) 02.08.28 G06F15/00,330	情報提供装置および情報管理方法
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2004-029938 02.06.21 G06F3/12	ﾌﾟﾘﾝﾀ及び印刷ｼｽﾃﾑ、並びに、ﾃﾞｰﾀ受信装置及びﾃﾞｰﾀ送受信ｼｽﾃﾑ
IPフィルタリング技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開平11-252158 (取下) 98.02.27 H04L12/54	電子ﾒｰﾙ情報管理装置及び方法
		ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2004-297759 03.03.11 H04L12/28,300	無線通信ﾈｯﾄﾜｰｸｼｽﾃﾑにおける接続認証

表2.19.4 セイコーエプソンの技術要素別課題対応特許（2/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2003-244243 (みなし取下) 02.02.13 H04L12/66	ﾌｧｲﾙﾀﾘﾝｸﾞ機能を有するﾈｯﾄﾜｰｸ接続装置
	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特開2003-167802 01.11.29 G06F13/00,351	二重ｻｰﾊﾞｼｽﾃﾑおよびこれに用いるｻｰﾊﾞ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾘｿｰｽ	特開2001-282645 00.03.29 G06F13/00,351	処理端末、出力端末、ｻｰﾋﾞｽ利用支援ｼｽﾃﾑ及び出力ﾌﾟﾛｸﾞﾗﾑを記憶した記憶媒体
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2001-282644 00.03.29 G06F13/00,351	ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｼｽﾃﾑ
ホスト認証技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開2004-094630 (みなし取下) 02.08.30 G06F15/00,330	自動接続ｼｽﾃﾑ、自動接続方法、自動接続機能を有する自動接続ﾌﾟﾛｸﾞﾗﾑ、自動接続機能を有する自動接続ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な情報記録媒体及
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ｱﾄﾞﾚｽの暗号化	特開2005-026825 03.06.30 H04L12/28,200	ﾈｯﾄﾜｰｸﾃﾞｰﾀ転送における機密保持方法
	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開2002-132715 (取下) 00.10.30 G06F15/00,310	会員用端末、ｻｰﾊﾞ装置およびｻｰﾋﾞｽ提供方法
トンネリング技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開平11-252161 (取下) 98.03.04 H04L12/54	情報付加装置及び情報付加方法

2.20 ヒューレット・パッカード

2.20.1 企業の概要

商号	Hewlett-Packard Company
本社所在地	3000 Hanover Street, Palo Alto, CA 94304 U.S.A.
設立年	1947年
資本金	22,158百万米ドル（2004年10月末）
従業員数	約151,000名（連結：2004年10月末）
事業内容	印刷機器、パソコン、ワークステーション、サーバ等の製造・販売およびコンサルティング等のITサービス提供

ヒューレット・パッカードが提唱する「アダプティブ・エンタープライズ」のセキュリティは、安全で安定した基盤を構築する重要な役割を担う。重大なダメージを回避しながら変化を有利に導くには、柔軟で強固なセキュリティ・システムが不可欠になる。ビジネス・パートナーやユーザーとのスムーズな連携を可能にするためにも、適切なタイミングで、適切な人に、適切な情報を安全に提供するITやその運用形態、人の意識までを含めた「仕組み」が求められる。ヒューレット・パッカードのセキュリティ・ソリューションは、「アダプティブ・エンタープライズ」の実現に欠かせないセキュリティ・システムをトータルでマネジメントする。IT基盤の堅牢性を高めるセキュリティ対策こそ、企業の競争力強化に貢献する。

(出典：http://h50146.www5.hp.com/solutions/infrastructure/security/)

2.20.2 製品例

セキュリティ・ソリューションに紹介されているもののうち、不正アクセス侵入検知防御技術に関連する製品やサービスを、表2.20.2に示す。

表2.20.2 ヒューレット・パッカードの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
HP Quarantine System	① 証接続制御ソリューション；ネットワークに接続可能なクライアントをITが管理する情報に基づいて認証し、ネットワーク接続を許可/拒否。 ② 検疫接続制御ソリューション；ウィルスやワームに感染する可能性の高いクライアントのネットワーク接続を阻止。
HP IceWall SSO 8.0	フォーム認証、日本語ファイル名のサポート強化、エージェントの増強により、非常に複雑な環境に対しても、 柔軟な Web 認証導入が可能。さらに、通常リバースプロキシでは URL 変換が行われる為、SSO 導入後は既存のWebアプリケーションで使用していた URL を使用してのアクセスはできなかったが、Ver.8.0 からはApache HTTP サーバの Virtual Host 機能の利用により、SSO 導入前のURL を使用してのアクセス可能。

(出典：http://h50146.www5.hp.com/products/software/security/icewall/iw_80.html)

2.20.3 技術開発拠点と研究者

特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

アメリカ合衆国：コロラド州、アイダホ州、オレゴン州、カリフォルニア州、テキサス州
ニュージャージー州、ニューハンプシャー州、ニューヨーク州
ノースカロライナ州、バーモント州

イギリス：ブリストル、ロンドン

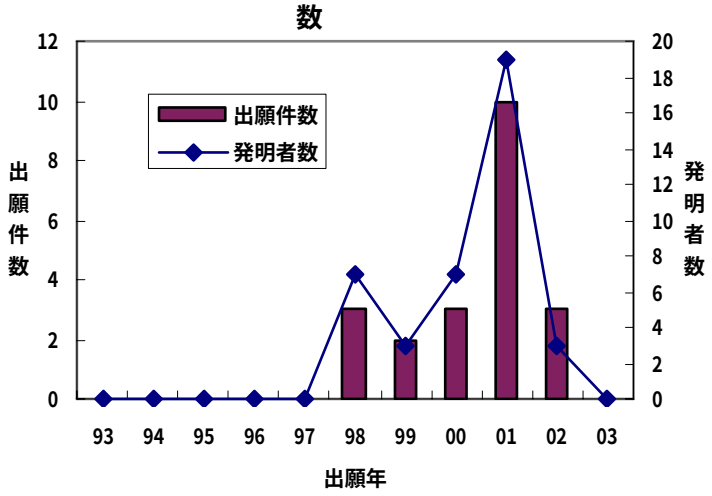
シンガポール：アッパーブキット、ネプチューンコート

ドイツ：ナフリンゲン

東京都杉並区高井戸東3丁目29番21号　日本ヒューレット・パッカード株式会社内

図2.20.3に、ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。2001年に10件と集中した出願がなされたが、平均的には毎年３件で発明者数も６人である。

図2.20.3 ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する出願件数と発明者数



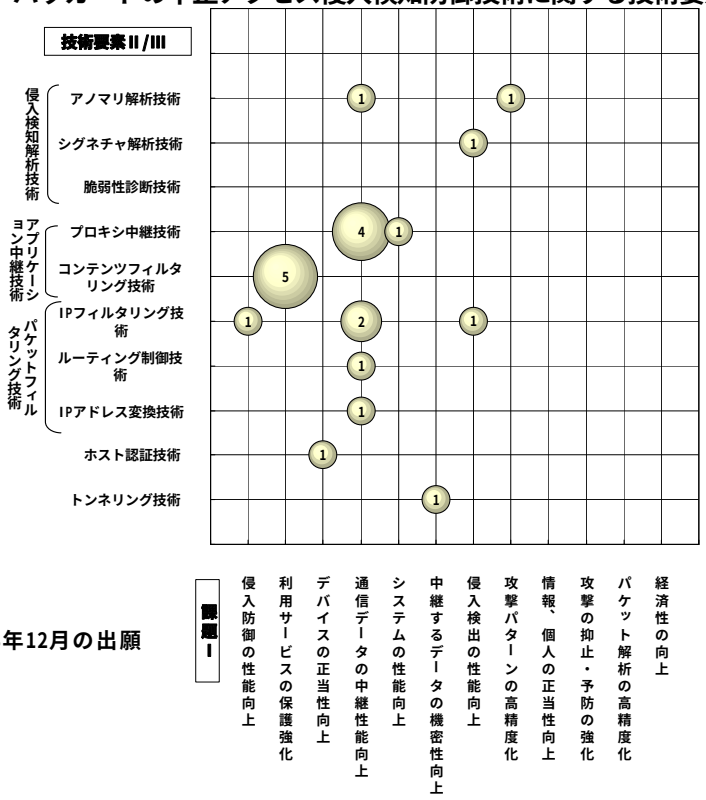
2.3.4 技術開発課題対応特許の概要

図2.20.4-1に、ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.20.4-2に、ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

コンテンツフィルタリング技術とプロキシ中継技術に関する出願が各５件ある。これらの出願のうち、多い課題は、「通信データの中継性能向上」である。

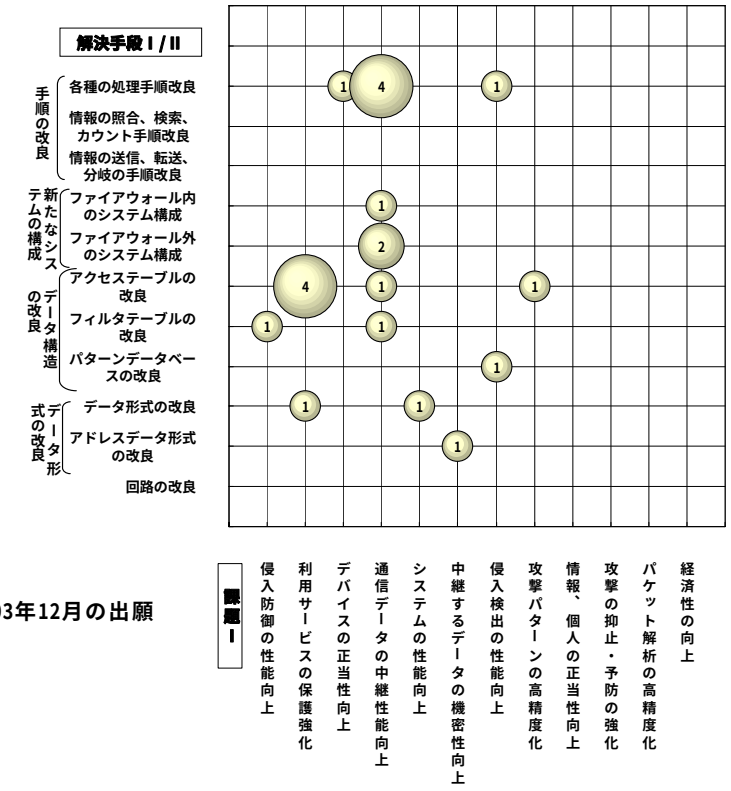
「利用サービスの保護強化」の課題に対しては、「アクセステーブルの改良」で４件対応している。さらに「通信データの中継性能向上」の課題に対しては、「各種の処理手順改良」で４件対応している。

図2.20.4-1 ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.20.4-2 ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



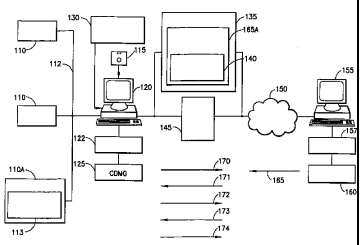
1993年1月～2003年12月の出願

表2.20.4 ヒューレット・パッカードの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は21件で、そのうち１件が登録特許である。なお、表2.20.4では図2.20.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.20.4 ヒューレット・パッカードの技術要素別課題対応特許（1/2）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 共同出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特開2001-273211 00.02.15 G06F13/00,351 〔被引用回数 1〕	ﾌｧｲﾔｳｫｰﾙ内部の装置を外部から制御する方法及び装置
	攻撃パターンの高精度化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特開2003-271560 01.10.31 G06F15/00,330	分散ﾈｯﾄﾜｰｸｻｰﾋﾞｽにおけるｱｸｾｽ制御装置およびﾎﾟﾘｼｰ実施装置
シグネチャ解析技術	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 ｱﾗｰﾄﾊﾟﾀｰﾝの追加	特開2003-228552 01.10.31 G06F15/00,330	不正侵入検出を提供するﾓﾊﾞｲﾙ通信ﾈｯﾄﾜｰｸのためのﾓﾊﾞｲﾙ機器
プロキシ中継技術	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞにﾃﾞｰﾀ添付	特開2000-003348 98.04.01 G06F15/177,678	遠隔的にｺﾏﾝﾄﾞを実行する装置
			特開2001-325164 00.03.28 G06F13/00,351	通信ｼｽﾃﾑおよび通信方法
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2003-186764 01.09.27 G06F13/00,351	ｳｴﾌﾞ資源へｱｸｾｽが制御される通信ﾈｯﾄﾜｰｸ
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾒｰﾙｻｰﾊﾞｰの配置	特開2004-005398 02.01.17 G06F13/00,630	ｻｰﾋﾞｽを提供するｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸおよびｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸによりｻｰﾋﾞｽを提供する方法
	システムの性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾌｫｰﾏｯﾄの変換	特開2002-328869 01.02.28 G06F13/00,547 〔被引用回数 1〕	ﾓﾊﾞｲﾙ機器によりﾌｧｲｱｳｫｰﾙを通してﾘﾓｰﾄで情報を適用する方法及び装置
コンテンツフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ・ｸﾞﾙｰﾌﾟ	特表2004-537095 01.04.24 G06F15/00,330	情報ｾｷｭﾘﾃｲｼｽﾃﾑ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特開2004-005451 02.02.28 G06F3/12	装置固有のﾌｧｲｱｳｫｰﾙ
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ｿﾞｰﾝ	特開2003-018167 01.05.07 H04L12/28,300	選択的無線通信ｱｸｾｽを制御する方法
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｵﾌﾞｼﾞｪｸﾄとｻﾌﾞｼﾞｪｸﾄ	特表2003-511783 99.09.17 G06F9/445	ｺﾝﾋﾟｭｰﾃｲﾝｸﾞ・ﾌﾟﾗｯﾄﾌｫｰﾑにおける信用状態の動作
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに情報付加	特表2004-535611 01.01.31 G06F13/00,351	高信頼性ｹﾞｰﾄｳｴｲｼｽﾃﾑ

表2.20.4 ヒューレット・パッカードの技術要素別課題対応特許（2/2）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
IPフィルタリング技術	侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特表2005-505828 01.10.11 G06F17/60,318	**周辺装置の消耗品供給管理**
	通信データの中継性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け 業務･商品情報	特開2000-112848 98.07.06 G06F13/00,351	**ﾃﾞｰﾀ交換管理ｼｽﾃﾑ及びﾃﾞｰﾀ交換方法**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの設定	特表2005-524123 01.10.11 G06F13/00,351	**ｳｪﾌﾞ統合のためのﾕｰｻﾞと装置の対話**
	侵入検出の性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答情報の検証	特開平11-338824 (特許3754230) 98.04.15 G06F15/00,330 〔被引用回数 1〕	**ｳｪﾌﾞﾘｿｰｽの保護方法**
ルーティング制御技術	通信データの中継性能向上	各種の処理手順改良 応答ｺﾏﾝﾄﾞの処理手順 応答ｺﾏﾝﾄﾞを要求ｺﾏﾝﾄﾞ	特許3375934 99.04.26 H04L12/46	**通信方法**  ﾛｰｶﾙﾌﾟﾛｾｯｻに接続された機器の制御をﾘﾓｰﾄﾌﾟﾛｾｯｻから行うことができるようにする通信方法であって、前記ﾘﾓｰﾄﾌﾟﾛｾｯｻが、ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸと、前記ﾛｰｶﾙﾌﾟﾛｾｯｻと前記ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸとの間に作動的に介挿された前記ﾛｰｶﾙﾌﾟﾛｾｯｻから前記ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸにﾒｯｾｰｼﾞをﾙｰﾃｨﾝｸﾞし、許可された場合にのみ前記ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸから前記ﾛｰｶﾙﾌﾟﾛｾｯｻにﾒｯｾｰｼﾞをﾙｰﾃｨﾝｸﾞするﾌﾟﾛｷｼﾏｼﾝと、を介して前記ﾛｰｶﾙﾌﾟﾛｾｯｻに接続されており、前記ﾌﾟﾛｷｼﾏｼﾝの存在に関係なく前記ﾘﾓｰﾄﾌﾟﾛｾｯｻが前記機器の動作の制御を行えるようにする方法を前記ﾛｰｶﾙﾌﾟﾛｾｯｻが実行し、前記通信方法は以下のｽﾃｯﾌﾟ(a)から(c)を設けたことを特徴とする通信方法：(a)前記ﾘﾓｰﾄﾌﾟﾛｾｯｻにﾒｯｾｰｼﾞを送信し、前記ﾌﾟﾛｷｼﾏｼﾝに対し、前記ﾘﾓｰﾄﾌﾟﾛｾｯｻから前記ﾛｰｶﾙﾌﾟﾛｾｯｻにﾒｯｾｰｼﾞをﾙｰﾃｨﾝｸﾞすることを許可する；(b)前記ﾘﾓｰﾄﾌﾟﾛｾｯｻから、前記ﾌﾟﾛｷｼﾏｼﾝによってﾙｰﾃｨﾝｸﾞされたところの、前記ﾛｰｶﾙﾌﾟﾛｾｯｻが実行するｺﾏﾝﾄﾞを示す前記ﾒｯｾｰｼﾞを受信する；(c)前記ｺﾏﾝﾄﾞを実行する。
ネットワークアドレス変換技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 機器､ﾓｼﾞｭｰﾙ配置	特開2004-046681 02.07.15 G06F13/00,547	**ｺﾝﾃﾝﾂ出力ｼｽﾃﾑ､ｺﾝﾃﾝﾂ出力要求中継ｻｰﾊﾞ､及びｺﾝﾃﾝﾂ出力装置**
ホスト認証技術	デバイスの正当性向上	各種の処理手順改良 特定情報の取得手順 ID情報の取得	特表2004-508619 00.08.18 G06F15/00,330	**ﾄﾗｽﾃｯﾄﾞ･ﾃﾞﾊﾞｲｽ**
トンネリング技術	中継するデータの機密性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特開2003-198561 01.12.21 H04L12/28,300	**ﾓﾊﾞｲﾙﾈｯﾄﾜｰｸｱｸｾｽ方法**

2.21 ルーセント　テクノロジーズ

2.21.1 企業の概要

商号	Lucent Technologies Inc.
本社所在地	600 Mountain Ave. Murray Hill,NJ
設立年	1869年
資本金	―　　（売上高94.4億ドル：2005年）
従業員数	約30,200名（2005年12月末）
事業内容	IPサービス、VoIPサービス 光学機器

(出典：ルーセントのホームページ http://www.lucent.com/corpinfo/)

ルーセントは、本社を米国ニュージャージー州マレーヒルに置く通信ネットワーク装置の世界的なサプライヤーである。主に通信事業者用のインターネット・インフラ、光通信ネットワーク、無線ネットワーク、及び通信ネットワーク・サポート・サービスの分野においてトップの座を誇っている。今後も発展を続けるため、ベル研究所の研究費の 3 分の 2 は、次世代プラットフォームの開発に使われている。(出典：日本ルーセントのホームページ http://www.lucent.co.jp/)

2.21.2 製品例

製品・サービスの通信事業者向けサービス内にセキュリティのリンクがありそこに紹介されているもののうち、不正アクセス侵入防止技術に関連のある製品やサービスを、表2.21.2に示す。

表2.21.2 ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関連する製品例

製品名	概要・特徴
VPN Firewall Brick Lucent Security Management Server (LSMS)	Lucent IPSec Client ソフトウェアと組み合わせて使用することにより、迅速なプロビジョニングを提供し、単一のコンソールから数千のユーザを対象に、セキュリティ、VPN、QoS サービスなどの各種機能を提供するマネージド・セキュリティ・サービスのプラットフォーム。
VPN Firewall Brick 1100	①1.0 GbpsのVPN（3DES時）スループット、②統合型高速ファイアウォール③VLANおよび仮想ファイアウォール機能 ④QoSおよび帯域管理
VPN Firewall Brick 500	975 Mbps のファイアウォール・パフォーマンス
VPN Firewall Brick 350	787 Mbpsのファイアウォール・パフォーマンス
VPN Firewall Brick 150	350 Mbps のファイアウォール･パフォーマンス
VPN Firewall Brick 80	190 Mbps のファイアウォール・パフォーマンス
VPN Firewall Brick 20	140 Mbps のファイアウォール・パフォーマンス
Lucent IPSec Client	ビルトイン・ファイアウォール、強力なパケット暗号化、各種認証方式

(出典：http://www.lucent.co.jp/jp/products/ipservice/index.html)

2.21.3 技術開発拠点と研究者

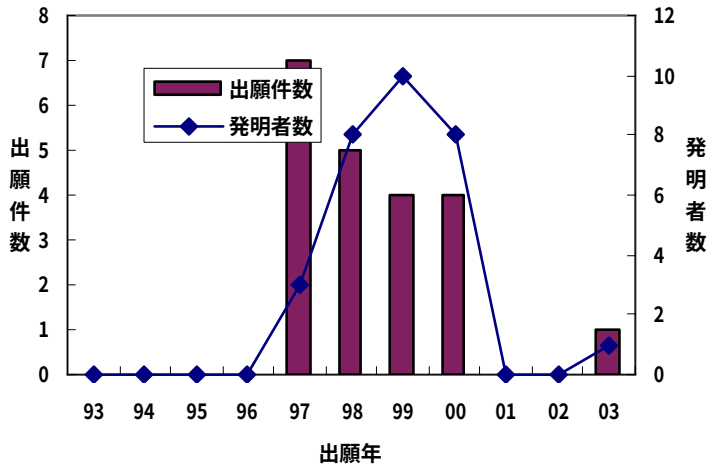
特許公報に記載された発明者の住所から抽出した技術開発拠点を以下に示す。

開発拠点：

アメリカ合衆国：ニュージャージー州、イリノイス州、テキサス州、ニューヨーク州

図2.21.3に、ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する出願件数と発明者数を示す。４年前までは平均で、出願件数が５件、発明者数が８人であったが、ここ３年の出願は、03年に１件と少ない。

図2.21.3 ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する出願件数と発明者数



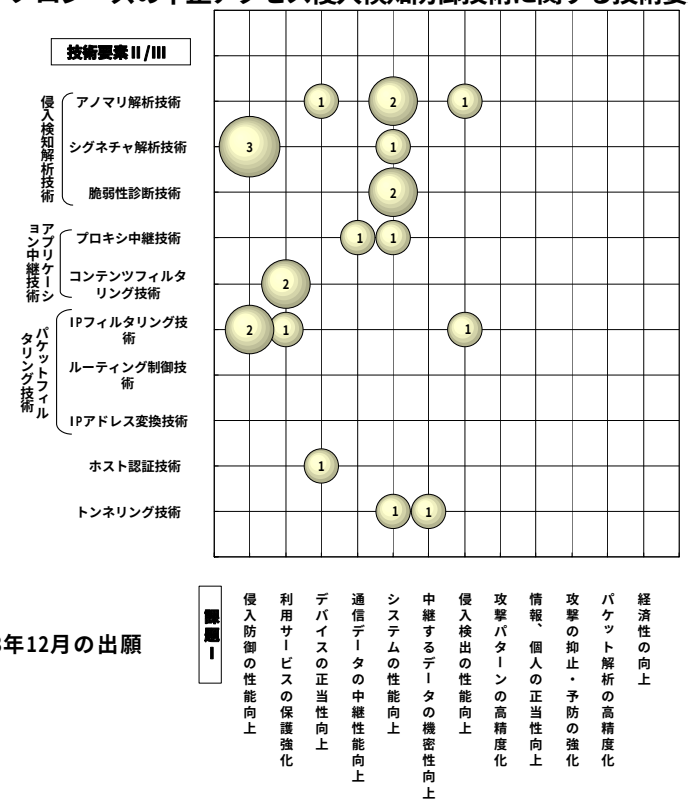
2.21.4 技術開発課題対応特許の概要

図2.21.4-1に、ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する技術要素と課題の分布を示す。図2.21.4-2に、ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する課題と解決手段の分布を示す。

アノマリ解析技術、シグネチャ解析技術とIPフィルタリング技術に関する出願が各４件ある。これらの出願のうち、「システムの性能向上」の課題が７件ある。

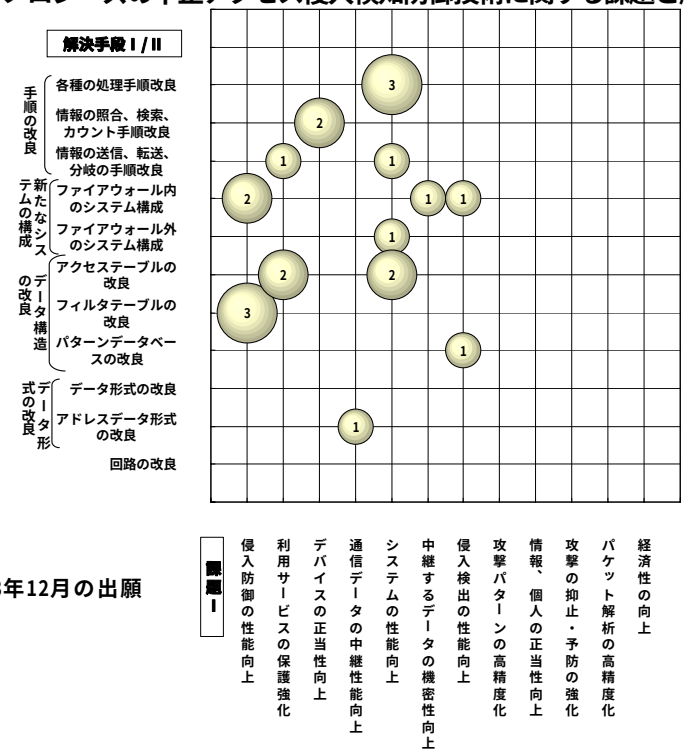
「侵入防御の性能向上」の課題に対しては、「フィルタテーブルの改良」で３件対応している。「システムの性能向上」の課題に対しては、「各種の処理手順改良」で３件対応している。

図2.21.4-1 ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する技術要素と課題の分布



1993年1月～2003年12月の出願

図2.21.4-2 ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する課題と解決手段の分布



1993年1月～2003年12月の出願

表2.21.4 ルーセント　テクノロジーズの不正アクセス侵入検知防御技術に関する技術要素別課題対応特許を示す。出願件数は21件で、そのうち９件が登録特許である。なお、表2.21.4では図2.21.4-2の解決手段Ⅰ/Ⅱを細展開した解決手段ⅢとⅣまで分析している。

表2.21.4 ルーセント　テクノロジーズの技術要素別課題対応特許（1/3）

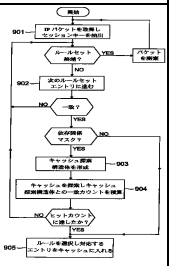
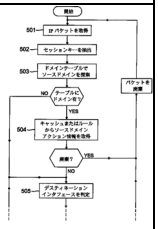
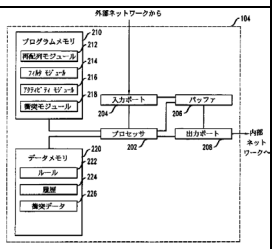
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
アノマリ解析技術	デバイスの正当性向上	情報の照合、検索､ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ｱﾄﾞﾚｽの検索	特開2005-073272 03.08.25 H04L12/66	**TCPｽﾃｰﾄﾚｽ･ﾎｸﾞによるTCPｻｰﾊﾞに対する分散ｻｰﾋﾞｽ妨害攻撃を防御する方法および装置**
	システムの性能向上	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特許3459183 97.09.12 H04L12/66 〔被引用回数 1〕	**ﾊﾟｹｯﾄ検証方法**  ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸﾌｧｲｱｳｫｰﾙにおけるﾊﾟｹｯﾄ検証方法において、該方法は、a.与えられたﾈｯﾄﾜｰｸｾｯｼｮﾝのﾊﾟｹｯﾄに対するｾｯｼｮﾝｷｰを取得するｽﾃｯﾌﾟと、b.前記ﾌｧｲｱｳｫｰﾙによって以前に処理されたﾊﾟｹｯﾄに関する情報を含むｷｬｯｼｭ内に前記ｾｯｼｮﾝｷｰとの一致が見つからない場合、ﾙｰﾙにおいて該ｷｬｯｼｭへの問合せを指定する問合せ部分を処理するｽﾃｯﾌﾟと、c.前記ｷｬｯｼｭへの問合せの結果に応じて前記ﾙｰﾙのｱｸｼｮﾝ部分を処理するｽﾃｯﾌﾟとからなることを特徴とするﾊﾟｹｯﾄ検証方法。
			特許3464610 97.09.12 H04L12/56 〔被引用回数 3〕	**ﾊﾟｹｯﾄ検証方法**  ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸﾌｧｲｱｳｫｰﾙにおけるﾊﾟｹｯﾄ検証方法において、ﾈｯﾄﾜｰｸｾｯｼｮﾝにおける与えられたﾊﾟｹｯﾄにﾙｰﾙｾｯﾄの少なくとも一部を適用した結果をｷｬｯｼｭに記憶するｽﾃｯﾌﾟと、記憶されている結果を利用して、前記与えられたﾊﾟｹｯﾄと同様の特性を有する少なくとも1つの後続のﾊﾟｹｯﾄを処理するﾊﾟｹｯﾄ処理ｽﾃｯﾌﾟとからなることを特徴とするﾊﾟｹｯﾄ検証方法。
	侵入検出の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開2002-026907 00.05.25 H04L12/22	**通信ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ方法および通信ﾈｯﾄﾜｰｸのﾈｯﾄﾜｰｸｾｷｭﾘﾃｨを分析するための方法および通信ｼｽﾃﾑおよびｾｷｭﾘﾃｨﾎｽﾄｺﾝﾋﾟｭｰﾀおよび**
シグネチャ解析技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 機器､ﾓｼﾞｭｰﾙ配置	特開平11-316677 98.01.29 G06F9/06,550	**ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸの保安方法**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀのﾀﾞｳﾝﾛｰﾄﾞ	特開平11-353258 （拒絶確定） 98.03.24 G06F13/00,351	**ﾌｧｲｱｳｫｰﾙｾｷｭﾘﾃｨ方法および装置**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの学習	特許3568850 98.12.03 H04L12/56 〔被引用回数 3〕	**ﾃﾞｰﾀﾊﾟｹｯﾄﾌｨﾙﾀの動作方法**  複数の順序づけられたﾙｰﾙを順次評価することによってﾃﾞｰﾀﾊﾟｹｯﾄをﾌｨﾙﾀﾘﾝｸﾞすることによりｾｷｭﾘﾃｨﾎﾟﾘｼｰを実現するﾃﾞｰﾀﾊﾟｹｯﾄﾌｨﾙﾀの動作方法において、該方法は、前記順序づけられたﾙｰﾙを自動的に再配列する再配列ｽﾃｯﾌﾟを有することを特徴とするﾃﾞｰﾀﾊﾟｹｯﾄﾌｨﾙﾀの動作方法。
	システムの性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID認証情報	特開2001-044992 （拒絶確定） 99.05.20 H04L12/22 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸ動作方法、ﾈｯﾄﾜｰｸﾉｰﾄﾞ、ﾈｯﾄﾜｰｸ装置、及び通信ﾈｯﾄﾜｰｸ**

表2.21.4 ルーセント　テクノロジーズの技術要素別課題対応特許（2/3）

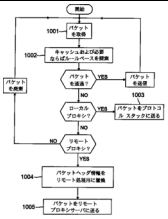
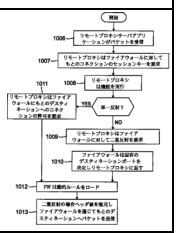
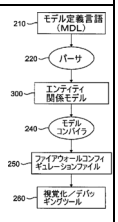
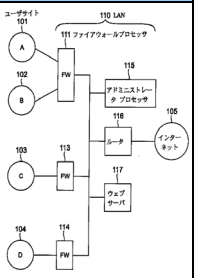
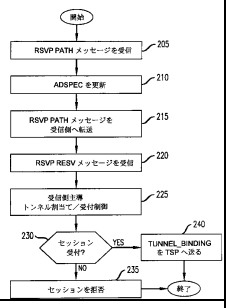
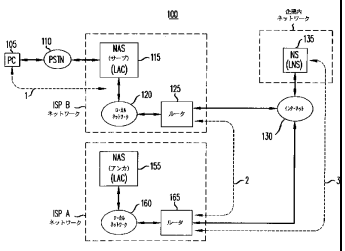
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	発明の名称 概要
脆弱性診断技術	システムの性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特開平11-355271 98.05.08 H04L12/22	**移動ﾎﾟｲﾝﾄ･ﾂｰ･ﾎﾟｲﾝﾄ･ﾌﾟﾛﾄｺﾙ**
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ｱﾄﾞﾚｽ､ﾎﾟｰﾄ番号	特開2001-237895 00.01.18 H04L12/56	**ﾈｯﾄﾜｰｸｹﾞｰﾄｳｴｲの解析方法及び装置**
プロキシ中継技術	通信データの中継性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 ﾘﾀﾞｲﾚｸﾄｱﾄﾞﾚｽの割付	特許3298832 97.09.12 G06F13/00,351	**ﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽ提供方法**  ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸでﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽを提供する方法において、該方法は、ﾌｧｲｱｳｫｰﾙにおいて、ｿｰｽからﾃﾞｽﾃｨﾈｰｼｮﾝまでのｾｯｼｮﾝを求める要求を受信するｽﾃｯﾌﾟと、前記ﾌｧｲｱｳｫｰﾙが前記要求を許可するには、ﾘﾓｰﾄｻｰﾊﾞが実行可能なｻｰﾋﾞｽが必要であるかどうかを確認する確認ｽﾃｯﾌﾟと、ﾘﾓｰﾄｻｰﾊﾞが実行可能なｻｰﾋﾞｽが必要である場合、前記ﾘﾓｰﾄｻｰﾊﾞを介して前記要求を実行する実行ｽﾃｯﾌﾟとからなることを特徴とするﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽ提供方法。
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾌﾟﾛｷｼｻｰﾊﾞｰの配置	特開2002-215478 97.09.12 G06F13/00,351	**ﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽ提供方法**
コンテンツフィルタリング技術	利用サービスの保護強化	情報の送信、転送、分岐の手順改良 情報転送の手順 ﾎﾟﾘｼｰ設定情報	特許3443529 97.09.12 G06F13/00,351 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽを提供する方法と、ﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽを提供するｺﾝﾋﾟｭｰﾀｼｽﾃﾑ**  ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸでﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽを提供する方法において、該方法は、初期ﾙｰﾙｾｯﾄをﾛｰﾄﾞするｽﾃｯﾌﾟと、前記初期ﾙｰﾙｾｯﾄを消去することなくﾙｰﾙｾｯﾄを修正する修正ｽﾃｯﾌﾟとからなることを特徴とするﾌｧｲｱｳｫｰﾙｻｰﾋﾞｽ提供方法。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 役割の属性値	特許3545303 99.01.29 H04L12/56 〔被引用回数 1〕	**ﾌｧｲｱｳｫｰﾙを管理するための方法および装置**  複数のﾎｽﾄを含む網内の少なくとも一つのﾌｧｲｱｳｫｰﾙに対するｺﾝﾌｨｷﾞｭﾚｰｼｮﾝﾌｧｲﾙを生成する方法であって、ﾎｽﾄがﾊﾟｹｯﾄを送信および受信する能力を指定する複数の役割に対する定義を受信するｽﾃｯﾌﾟ；前記役割の前記網内の前記複数のﾎｽﾄへの割当てを受信するｽﾃｯﾌﾟ；および前記指定された役割に基づいて前記ﾎｽﾄに対する規則を生成するｽﾃｯﾌﾟであって、前記規則がﾊﾟｹｯﾄが宛先ﾎｽﾄに通過できるか否かを決定するものであるｽﾃｯﾌﾟを含むことを特徴とする方法。
IPフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 位置識別子の配置	特開2001-053741 （拒絶確定） 99.05.27 H04L9/08	**受信ﾒｯｾｰｼﾞへのｱｸｾｽを制御するｼｽﾃﾑ**
		ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 ﾌｨﾙﾀの追加 ﾌｨﾙﾀの付加	特開2002-189643 00.08.31 G06F13/00,351	**通信ﾄﾗﾋｯｸを走査するための方法および装置**

表2.21.4 ルーセント　テクノロジーズの技術要素別課題対応特許（3/3）

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主IPC 共同出願人 ［被引用回数］	**発明の名称** 概要
IPフィルタリング技術	利用サービスの保護強化	ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾕｰｻﾞｰ･ｸﾞﾙｰﾌﾟ	特許3492920 97.09.12 H04L12/66 〔被引用回数 1〕	**ﾊﾟｹｯﾄ検証方法** ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸにおけるﾊﾟｹｯﾄを検証する方法において、該方法は、前記ﾊﾟｹｯﾄに対するｾｯｼｮﾝｷｰを導出するｽﾃｯﾌﾟと、前記ｾｯｼｮﾝｷｰの関数として複数のｾｷｭﾘﾃｨﾎﾟﾘｼｰのうちから少なくとも1つのｾｷｭﾘﾃｨﾎﾟﾘｼｰを選択する選択ｽﾃｯﾌﾟと、選択されたｾｷｭﾘﾃｨﾎﾟﾘｼｰを用いて前記ﾊﾟｹｯﾄを検証するｽﾃｯﾌﾟとからなることを特徴とするﾊﾟｹｯﾄ検証方法。 
	侵入検出の性能向上	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの学習 ﾄﾗﾌｨｯｸﾃﾞｰﾀの学習	特開2003-198637 （却下） 97.09.12 H04L12/66	**ﾊﾟｹｯﾄ検証方法**
ホスト認証技術	デバイスの正当性向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 認証情報の照合	特開2002-084276 （拒絶確定） 00.06.13 H04L9/32	**ﾕｰｻﾞ加入識別ﾓｼﾞｭｰﾙの認証についての改善された方法**
トンネリング技術	システムの性能向上	各種の処理手順改良 各種処理の実行手順 特定処理の実行	特許3545988 99.02.26 H04L12/56	**通信方法および通信装置** ﾄﾝﾈﾙﾃﾞｽﾃｨﾈｰｼｮﾝﾎﾟｲﾝﾄとして作用するﾊﾟｹｯﾄｻｰﾊﾞにおいて使用される通信方法において、RSVPﾍﾟｰｽのｼｸﾞﾅﾘﾝｸﾞを受信するｽﾃｯﾌﾟと、受信したRSVPﾍﾟｰｽのｼｸﾞﾅﾘﾝｸﾞに応答して、ｴﾝﾄﾞﾂｰｴﾝﾄﾞRSVPｾｯｼｮﾝをﾄﾝﾈﾙにﾏｯﾋﾟﾝｸﾞするｽﾃｯﾌﾟとを有することを特徴とする通信方法。 
	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞｰの配置	特許3470882 98.05.08 H04L12/56 〔被引用回数 1〕	**多重ﾎｯﾌﾟ･ﾎﾟｲﾝﾄ･ﾂｰ･ﾎﾟｲﾝﾄ･ﾌﾟﾛﾄｺﾙ** ﾊﾟｹｯﾄ･ｻｰﾊﾞで使用される方法であって、該方法が、他のﾊﾟｹｯﾄ終端間に多重ﾎｯﾌﾟ･ﾊﾟｹｯﾄ･ﾄﾝﾈﾙを確立する段階と、多重ﾎｯﾌﾟ･ﾊﾟｹｯﾄ･ﾄﾝﾈﾙを通じて他のﾊﾟｹｯﾄ終端間でﾒｯｾｰｼﾞを中継する段階とからなることを特徴とする方法。 

2.22　大学、公的研究機関

大学、公的研究機関の技術要素別課題対応特許等について下記に紹介する。

表 2.22 大学、公的研究機関等の技術要素別課題対応特許一覧(1/3)

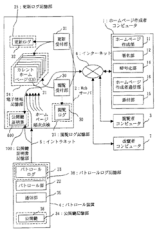
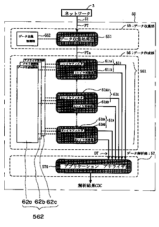
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 出願人 ［被引用回数］	**発明の名称** 概要
アノマリ解析技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開 2002-247068 01.02.21 H04L12/46 科学技術振興機構	**ﾈｯﾄﾜｰｸｼｽﾃﾑ**
経済性の向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特開 2002-247068 01.02.21 H04L12/46 科学技術振興機構	**ﾈｯﾄﾜｰｸｼｽﾃﾑ** 概要は技術要素「ｱﾉﾏﾘ解析」、課題「ｼｽﾃﾑの性能向上」の項を参照
侵入検出の性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 擬似、ﾀﾞﾐﾃﾞｰﾀの送信	特開 2003-288227 02.01.25 G06F11/00 科学技術振興機構	**ｺﾝﾋﾟｭｰﾀｳｲﾙｽの駆除方法及びｺﾝﾋﾟｭｰﾀｳｲﾙｽの検出表示方法**
情報、個人の正当性向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 ﾁｪｯｸｻｰﾊﾞｰ配置	特許 3450849 02.09.30 G06F12/14,310 科学技術振興機構，曽我　正和（共願）	**ﾊﾟﾄﾛｰﾙ装置及びﾊﾟﾄﾛｰﾙ方法**  電子情報と電子情報が真正であるか否かをﾁｪｯｸするための署名情報とを記憶する電子情報記憶部と、電子情報記憶部が記憶した電子情報を作成した電子機器の識別情報を含む更新ﾛｸﾞを記憶する更新ﾛｸﾞ記憶部と、署名情報を使用して電子情報の改竄の有無をﾊﾟﾄﾛｰﾙするﾊﾟﾄﾛｰﾙ部と、ﾊﾟﾄﾛｰﾙ部がﾊﾟﾄﾛｰﾙしたﾊﾟﾄﾛｰﾙﾛｸﾞを記憶するﾊﾟﾄﾛｰﾙﾛｸﾞ記憶部とを備え、ﾊﾟﾄﾛｰﾙ部は、電子情報に改竄有りと判断した場合には、更新ﾛｸﾞ記憶部が記憶した更新ﾛｸﾞとﾊﾟﾄﾛｰﾙﾛｸﾞ記憶部が記憶したﾊﾟﾄﾛｰﾙﾛｸﾞとから電子情報を改竄した改竄者の電子機器を特定する捕捉部を有するﾊﾟﾄﾛｰﾙ装置。
パケット解析の高精度化	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 ﾛｸﾞ履歴情報の照合	特許 2945938 97.03.11 H04L12/22 宇宙航空研究開発機構，科学技術振興機構（共願） 〔被引用回数 4〕	**ﾈｯﾄﾜｰｸ不正解析方法及びこれを利用したﾈｯﾄﾜｰｸ不正解析装置並びにﾈｯﾄﾜｰｸ不正解析ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**  ﾈｯﾄﾜｰｸ上で伝送されているﾊﾟｹｯﾄを取り込むﾃﾞｰﾀ収集工程と、階層化されたﾌﾟﾛﾄｺﾙに応じた階層化ﾓｼﾞｭｰﾙのﾊﾟﾗﾒｰﾀを予め読み込んでおいたｺﾝﾌｨｸﾞﾚｰｼｮﾝﾌｧｲﾙで指定された情報に基づいて設定し、ﾃﾞｰﾀ収集工程からのﾊﾟｹｯﾄを各階層化ﾓｼﾞｭｰﾙでﾌｨﾙﾀﾘﾝｸﾞしてﾊﾟｹｯﾄの細分化されたﾃﾞｰﾀを元の単位に再構築することにより解析ﾃﾞｰﾀを作成するﾃﾞｰﾀ作成工程と、予め読み込んでおいたｺﾝﾌｨｸﾞﾚｰｼｮﾝﾌｧｲﾙで指定された内容を基にﾃﾞｰﾀ作成工程からの解析ﾃﾞｰﾀに不正が発生しているか判定するﾃﾞｰﾀ解析工程とを備えたことを特徴とするﾈｯﾄﾜｰｸ不正解析方法。

表 2.22 大学、公的研究機関等の技術要素別課題対応特許一覧(2/3)

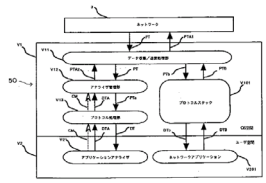
技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 （経過情報） 出願日 主 IPC 出願人 ［被引用回数］	発明の名称 概要
アノマリ解析技術	パケット解析の高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 攻撃ﾊﾟﾀｰﾝの追加、切換 攻撃属性別ﾊﾟﾀｰﾝの追加	特許 3648520 98.09.11 G06F13/00,353 石井 剛，宇宙航空研究開発機構，藤田 直行(共願) 〔被引用回数 2〕	**ﾈｯﾄﾜｰｸ通信の監視･制御方法及びこれを利用した監視･制御装置並びにﾈｯﾄﾜｰｸ通信の監視･制御ﾌﾟﾛｸﾞﾗﾑを記録したｺﾝﾋﾟｭｰﾀ読み取り可能な記録媒体**  情報通信ｽﾃｰｼｮﾝの間で階層化されたﾌﾟﾛﾄｺﾙにより通信を行うように構築されたﾈｯﾄﾜｰｸにおける不正を解析する方法であって、前記ﾈｯﾄﾜｰｸに対してﾊﾟｹｯﾄを送受信できるﾃﾞｰﾀ収集/送信処理工程と、制御ﾒｯｾｰｼﾞによって書き換えられるｱﾅﾗｲｻﾞ管理情報を基に前記ﾃﾞｰﾀ収集/送信処理工程との間でﾊﾟｹｯﾄ通信を行うとともに、通信に不正が検知されたときには前記ﾊﾟｹｯﾄでもって通信当事者と個々に通信して通信当事者間の通信をﾊｲｼﾞｬｯｸするﾊｲｼﾞｬｯｸ機能を備えたｱﾅﾗｲｻﾞ管理工程と、前記ｱﾅﾗｲｻﾞ管理工程から得たﾊﾟｹｯﾄから解析ﾃﾞｰﾀを再構築するとともに、制御ﾒｯｾｰｼﾞ及びﾃﾞｰﾀを前記ｱﾅﾗｲｻﾞ管理工程に伝送するﾌﾟﾛﾄｺﾙ処理工程と、前記ﾌﾟﾛﾄｺﾙ処理工程から取り込んだ解析ﾃﾞｰﾀに不正がないか判断するとともに、その判断結果に応じて制御ﾒｯｾｰｼﾞ及びﾃﾞｰﾀを作成してﾌﾟﾛﾄｺﾙ処理工程に送出するｱﾅﾗｲｻﾞ工程とを備えたことを特徴とするﾈｯﾄﾜｰｸ通信の監視･制御方法。
シグネチャ解析技術	侵入検出の性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZ に機器の配置 攻撃解析ｻｰﾊﾞｰの配置	特開 2004-302538 03.03.28 G06F13/00,351 明治大学	**ﾈｯﾄﾜｰｸｾｷｭﾘﾃｲｼｽﾃﾑ及びﾈｯﾄﾜｰｸｾｷｭﾘﾃｲ管理方法**
	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 更新情報の付加	特開 2003-208315 (みなし取下) 01.11.08 G06F9/445 米沢 明憲(東京大学)，日本総合研究所(共願)	**ｿﾌﾄｳｴｱの安全な自動組み込みｼｽﾃﾑおよびｿﾌﾄｳｴｱの安全な自動組み込みﾌﾟﾛｸﾞﾗﾑ**
	攻撃の抑止・予防の強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 ﾍｯﾀﾞに認証情報	特開 2003-208325 (みなし取下) 02.01.11 G06F11/00 米沢 明憲 (東京大学)，日本総合研究所(共願)	**ﾈｯﾄﾜｰｸ免疫ｼｽﾃﾑおよびﾈｯﾄﾜｰｸ免疫ﾌﾟﾛｸﾞﾗﾑ**
脆弱性診断技術	攻撃パターンの高精度化	ﾊﾟﾀｰﾝﾃﾞｰﾀﾍﾞｰｽの改良 分析ｱﾙｺﾞﾘｽﾞﾑの改良 脆弱度の算出	特開 2004-310267 03.04.03 G06F15/00,330 産業技術総合研究所	**ｳｴﾌﾞｻｲﾄの検査装置**
プロキシ中継技術	侵入防御の性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の検索、抽出手順 ﾒｯｾｰｼﾞの内容検索	特開 2003-173315 01.12.05 G06F13/00,610 溝口 文雄(東京理科大学)，斉藤 孝道(共願)	**通信管理装置及び管理ﾌﾟﾛｸﾞﾗﾑ**
IPフィルタリング技術	攻撃の抑止・予防の強化	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 属性付与し登録	特開 2005-174265 03.11.18 G06F13/00 産業技術総合研究所	**電子ﾒｰﾙ管理方法、電子ﾒｰﾙｼｽﾃﾑおよびﾀｸﾞ管理者側装置**

表 2.22 大学、公的研究機関等の技術要素別課題対応特許一覧(3/3)

技術要素Ⅲ	課題Ⅰ	解決手段Ⅱ 解決手段Ⅲ 解決手段Ⅳ	特許番号 (経過情報) 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特開 2004-147029 02.10.23 H04L12/56,100 桧垣 博章(東京電機大学),ｴﾙｳｲﾝｸﾞ(共願)	**ﾃﾞｰﾀ転送方法及びその装置**
トンネリング技術	デバイスの正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 可変鍵の付加	特開 2004-282295 03.03.14 H04L9/32 産学連携機構九州,ｾｷｭｱｰﾄﾞ ｺﾐｭﾆｹｰｼｮﾝｽﾞ(共願)	**ﾜﾝﾀｲﾑ ID の生成方法、認証方法、認証ｼｽﾃﾑ、ｻｰﾊﾞ、ｸﾗｲｱﾝﾄおよびﾌﾟﾛｸﾞﾗﾑ**
	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特開 2001-160092 (拒絶確定) 99.12.02 G06F17/60 関西ﾃｨｰ･ｴﾙ･ｵｰ	**通信保険契約方法、通信保険契約ｼｽﾃﾑ、送信装置、中継装置、及び記録媒体**

2.23　主要企業等以外の特許番号一覧

前掲の主要 21 社、大学、公的研究機関等以外の技術要素別課題対応特許について下記に紹介する。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（1/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	通信データの中継性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 記憶領域の分割配置	特許 3309758 97.03.07 G06F13/00,560 ﾉｰﾘﾂ	**ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸにおける情報の管理方法および情報管理ｼｽﾃﾑ** 一定の目的に供せられる情報を特定の管理者を立てて管理する方法であって、ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ上に配され、かつ管理者の管理下に置かれるｻｰﾊﾞに対して新規のﾕｰｻﾞからｱｸｾｽがなされると、ｻｰﾊﾞ内に当該新規のﾕｰｻﾞに対応した個別の情報ﾎﾞｯｸｽを設定し、それ以後のﾕｰｻﾞと管理者との情報の授受が全てこの情報ﾎﾞｯｸｽを介して行われることを特徴とするｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸにおける情報の管理方法。
	システムの性能向上	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特許 3585801 00.01.13 H04L12/24 ﾈｸｽﾄｺﾑ	**電子ﾚﾎﾟｰﾃｨﾝｸﾞｼｽﾃﾑ** 管理対象機器から送信される情報を監視し、監視している情報を利用者に逐次報告する必要性があるか否かを判断し、判断結果に基づき情報を利用者に逐次報告する必要性があると判断した場合には、情報を所定の通信媒体を介して利用者に逐次配信し、判断結果に基づき情報を逐次報告する必要性がないと判断した場合には、利用者により指定された報告内容に基づいて情報に関する報告書を作成し、作成した報告書を前記所定の通信媒体を介して利用者に定期的に配信することを特徴とする電子ﾚﾎﾟｰﾃｨﾝｸﾞｼｽﾃﾑ。
		情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 警告情報	特許 3587000 96.11.01 H04L12/28,200 ﾔﾏﾊ	**不正ｺﾋﾟｰ防止ｼｽﾃﾑ、監視ﾉｰﾄﾞ及び送受信ﾉｰﾄﾞ** 暗号化処理などのﾃﾞｰﾀ処理を施すことなくそのままの形でﾃﾞｨｼﾞﾀﾙﾃﾞｰﾀを入出力する通常ﾃﾞｰﾀ入出力動作ﾓｰﾄﾞと、不正ﾉｰﾄﾞがﾃﾞｨｼﾞﾀﾙﾃﾞｰﾀを取り込むことができないようにするﾌﾟﾛﾃｸﾄﾃﾞｰﾀ入出力動作ﾓｰﾄﾞとを具えた複数の正規ﾉｰﾄﾞ群と、この複数の正規ﾉｰﾄﾞ群を接続し、それぞれの正規ﾉｰﾄﾞ間でﾃﾞｰﾀの入出力動作を自由に行えるように構成された通信ﾈｯﾄﾜｰｸと、通信ﾈｯﾄﾜｰｸに接続されており、通信ﾈｯﾄﾜｰｸに不正ﾉｰﾄﾞが新たに接続されたことを検出した場合に、複数の正規ﾉｰﾄﾞ群に対してﾌﾟﾛﾃｸﾄﾃﾞｰﾀ入出力動作ﾓｰﾄﾞでﾃﾞｰﾀの入出力動作を行うように指令を出す監視ﾉｰﾄﾞとを具備することを特徴とする不正ｺﾋﾟｰ防止ｼｽﾃﾑ。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱﾌﾟﾘｹｰｼｮﾝとの関連付け ﾌｧｲﾙ	特許 2922450 95.10.26 G06F15/00,320 日立電子ｻｰﾋﾞｽ 〔被引用回数 3〕	**LAN 端末情報の収集方法** LAN に接続される 1 端末として、LAN 端末情報を収集するための専用の監視端末を設け、各監視対象端末の採取対象情報の実ﾌｧｲﾙ名を遠隔運用管理ｼｽﾃﾑ側から見た一般的な情報名と対応づける情報対応ﾃｰﾌﾞﾙを監視端末内に設け、LAN の障害発生時に、遠隔運用管理ｼｽﾃﾑから公衆網を介して監視端末に情報採取対象の端末名および採取対象情報の一般的な情報名を送信し、送信を受けた監視端末は、採取対象情報の一般的な情報名を前記情報対応ﾃｰﾌﾞﾙにより対応する実ﾌｧｲﾙ名に変換し、情報採取対象の端末名で指定された端末の実ﾌｧｲﾙ名のﾌｧｲﾙにｱｸｾｽすることにより、目的の LAN 端末情報を採取し、採取された LAN 端末情報を一般的な情報名で遠隔運用管理ｼｽﾃﾑに返送する、ことを特徴とする LAN 端末情報の収集方法。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（2/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
アノマリ解析技術	情報、個人の正当性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 電子署名の付加	特許 3563649 99.10.08 H04L12/54 ｵｰﾌﾟﾝﾙｰﾌﾟ	**通信制御装置及び記録媒体** ｸﾗｲｱﾝﾄﾏｼﾝより取得した送信用ﾃﾞｰﾀに基づいて、送信用ﾃﾞｰﾀの発信者及び/又は当該発信者が所属するｸﾞﾙｰﾌﾟを特定する送信元特定手段と、送信元特定手段が特定した発信者及び/又はｸﾞﾙｰﾌﾟに対応付けられた秘密鍵を用いて、送信用ﾃﾞｰﾀにﾃﾞｼﾞﾀﾙ署名を施す署名手段と、署名手段がﾃﾞｼﾞﾀﾙ署名を施した送信用ﾃﾞｰﾀをﾈｯﾄﾜｰｸに送出するﾃﾞｰﾀ送信手段と、を備える、ことを特徴とする通信制御装置。
	パケット解析の高精度化	各種の処理手順改良 特定情報の記憶、登録手順 ﾛｸﾞ情報の記憶	特許 3541872 98.08.19 G06F15/00,330 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ	**ﾈｯﾄﾜｰｸｱｸｾｽ検証ｼｽﾃﾑ** 端末利用者を認証情報に基づき、ｱｸｾｽ許可を識別し、ﾕｰｻﾞ識別子とﾕｰｻﾞの端末利用時間などのﾕｰｻﾞ情報を記録するﾕｰｻﾞ履歴記録手段と、記録されたﾕｰｻﾞ情報を管理端末に送信する履歴ﾃﾞｰﾀ送信手段とを有するｸﾗｲｱﾝﾄ端末と、内部ﾈｯﾄﾜｰｸの通信端末から送られてくる情報取得要求を要求された外部ﾈｯﾄﾜｰｸの通信端末へ転送し、外部ﾈｯﾄﾜｰｸの通信端末からの応答を要求元の内部ﾈｯﾄﾜｰｸの通信端末へ転送し、転送した内部ﾈｯﾄﾜｰｸの通信端末と情報取得要求などのｱｸｾｽ情報を記録する通信中継手段と、記録されたｱｸｾｽ情報を管理端末に送信する履歴ﾃﾞｰﾀ送信手段とを有するｹﾞｰﾄｳｪｲ端末と、内部ﾈｯﾄﾜｰｸの通信端末やｹﾞｰﾄｳｪｲ端末からのﾕｰｻﾞ情報やｱｸｾｽ情報を受信する管理端末上の履歴ﾃﾞｰﾀ収集手段と、履歴ﾃﾞｰﾀ収集手段によって収集されたﾕｰｻﾞ情報と前記ｱｸｾｽ情報と管理者が指定する情報取得要求から対応するﾕｰｻﾞを特定する履歴ﾃﾞｰﾀ分析手段を有する管理端末からなり、管理端末で特定の情報取得要求を指定することで、ﾕｰｻﾞ履歴記録手段と履歴ﾃﾞｰﾀ収集手段からのﾃﾞｰﾀを参照し、履歴ﾃﾞｰﾀ分析手段によって情報取得要求を発行したﾕｰｻﾞ及びﾕｰｻﾞが利用したｸﾗｲｱﾝﾄ端末を特定することを特徴とするﾈｯﾄﾜｰｸｱｸｾｽ検証ｼｽﾃﾑ。
シグネチャ解析技術	侵入検出の性能向上	各種の処理手順改良 特定情報の取得手順 ｽﾃｰﾀｽの取得	特許 3404032 02.04.09 G06F11/30 さくら情報ｼｽﾃﾑ	**ｺﾝﾋﾟｭｰﾀｳｲﾙｽ対策ｼｽﾃﾑ及びｺﾝﾋﾟｭｰﾀｳｲﾙｽ対策方法** ｱﾝﾁｳｨﾙｽ機能を有しており、ｱﾝﾁｳｨﾙｽ機能によりｺﾝﾋﾟｭｰﾀｳｨﾙｽの攻撃を受けたﾌｧｲﾙを含む検疫情報を取得し、検疫情報をｻｰﾊﾞに転送するｸﾗｲｱﾝﾄ端末と、ｸﾗｲｱﾝﾄ端末の機器情報を少なくとも記憶するﾃﾞｰﾀﾍﾞｰｽと、検疫情報に基づいて、ﾃﾞｰﾀﾍﾞｰｽよりｸﾗｲｱﾝﾄ端末の機器情報を読み出し、検疫情報と機器情報とを取得情報として統括して一元的に管理し、取得情報に基づき、ｳｨﾙｽ対策に係る所定情報をﾎﾟｰﾀﾙｻｲﾄにて提供するｻｰﾊﾞと、を具備することを特徴とするｺﾝﾋﾟｭｰﾀｳｨﾙｽ対策ｼｽﾃﾑ。
	攻撃の抑止・予防の強化	回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特許 3381055 97.01.27 G06F15/00,330 若山 裕典	**ｳｲﾙｽの侵入防止方法、及びｳｲﾙｽの侵入防止機構** 通信回線を介して得られたﾃﾞｰﾀからなるﾌｧｲﾙを読み書き可能なﾒﾓﾘ内に格納し、ﾒﾓﾘに格納したﾌｧｲﾙ内にｳｲﾙｽが存在する時又はその可能性があると判断した時に、ﾌｧｲﾙを格納しているﾒﾓﾘの電源をｵﾌするようにしたことを特徴とするｳｲﾙｽの侵入防止方法。
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 複数ﾌｧｲｱｳｫｰﾙの配置	特許 3519696 00.07.18 H04L12/26 ｱｲﾃｲｰﾏﾈｰｼﾞ	**監視ｼｽﾃﾑおよび監視方法** ｻｰﾋﾞｽ提供装置と通信し、前記ｻｰﾋﾞｽ提供装置の状態を監視する監視装置と、公開通信網とは別に設けられた、監視装置とｻｰﾋﾞｽ提供装置との間で情報を送受信するための監視用通信網と、ｻｰﾋﾞｽ提供装置から前記監視装置へ監視用通信網を介して第一の情報を送信するときに、第一の情報の送信元ｱﾄﾞﾚｽを変換する第一のｱﾄﾞﾚｽ変換装置と、監視装置からｻｰﾋﾞｽ提供装置へ監視用通信網を介して第二の情報を送信するときに、第二の情報の送信元ｱﾄﾞﾚｽを変換する第二のｱﾄﾞﾚｽ変換装置と、を備えたことを特徴とする監視ｼｽﾃﾑ。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（3/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
脆弱性診断技術	システムの性能向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 ｲﾝﾄﾗﾈｯﾄ内に機器の配置 ﾒﾓﾘの配置	特許 3184138 96.12.04 H04L12/28 ﾛｯｸｳｪﾙ ｻｲｴﾝｽ ｾﾝﾀｰ(米国)	**非同期式転送ﾓｰﾄﾞｼｽﾃﾑと通信するｼｽﾃﾑのためにﾌｧｲﾔｰ・ｳｫｰﾙ保護を提供するための装置および方法** ｺﾈｸｼｮﾝ型ｼｽﾃﾑに結合されるように適用されるｺﾈｸｼｮﾝ型ｼｽﾃﾑｲﾝﾀﾌｪｰｽと、複数の記憶場所を有するﾒﾓﾘと、ｺﾈｸｼｮﾝに関連づけられたﾃﾞｰﾀをﾒﾓﾘ・ｽﾛｯﾄへ転送するためにｺﾈｸｼｮﾝ型ｼｽﾃﾑ・ｲﾝﾀﾌｪｰｽとﾒﾓﾘとに結合される制御回路と、を備え、制御回路は記憶要素を含み、記憶要素は該ｺﾈｸｼｮﾝの各ｺﾈｸｼｮﾝによって使用されている記憶場所の数を格納し、制御回路はｺﾈｸｼｮﾝの各ｺﾈｸｼｮﾝによって使用されている記憶場所の数に応じてﾃﾞｰﾀを転送する、ｴｯｼﾞﾃﾞﾊﾞｲｽ。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け ﾏｼﾝ・ﾎｽﾄ	特許 3654280 02.09.27 G06F1/00,370 ﾌﾞﾗｻﾞｰ工業	**電子機器、及びﾌﾟﾛｸﾞﾗﾑ** 自己が以前に接続されていたﾈｯﾄﾜｰｸと異なるﾈｯﾄﾜｰｸに接続されたか否かを判断する判断手段と、判断手段により異なるﾈｯﾄﾜｰｸに接続されたと判断された場合、電子機器自身が記憶している記憶内容の利用を禁止する禁止手段と、を備えたことを特徴とする電子機器。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 通信路	特許 3005490 97.03.27 H04L12/56 九州日本電気ｿﾌﾄｳｪｱ 〔被引用回数 1〕	**HUB 間ﾃﾞｰﾀ暗号化によるﾃﾞｰﾀｾｷｭﾘﾃｨ確保装置と方法** HUB に直接接続している終端装置からﾊﾟｹｯﾄを受け取った場合に、ﾊﾟｹｯﾄがｺﾈｸｼｮﾝ型かｺﾈｸｼｮﾝﾚｽ型かに関係なく、ﾊﾟｹｯﾄの宛先終端装置を見て、暗号化するべきﾊﾟｹｯﾄかどうかを決定する暗号化判断部と、暗号化および復号化処理部と、暗号化を行った際にﾊﾟｹｯﾄの宛先ｱﾄﾞﾚｽおよび送信元ｱﾄﾞﾚｽの直後に暗号化を行ったという意味のﾌﾗｸﾞを ON にｾｯﾄし、復号化の際に必要となる情報があればそれを付加した上で暗号化ﾃﾞｰﾀのｶﾌﾟｾﾙ化を行うｶﾌﾟｾﾙ化部を備え、また、HUB が直接接続している終端装置ではなく外部からﾊﾟｹｯﾄを受け取った場合には、まずﾊﾟｹｯﾄの宛先物理ｱﾄﾞﾚｽが HUB に直接接続している終端装置かどうかを判断し、直接接続している場合には上述の暗号化判断部にてそのﾊﾟｹｯﾄが暗号化ﾃﾞｰﾀであるかどうかの判断を行い、暗号化ﾃﾞｰﾀである場合には、復号化を行った上でﾃﾞｰﾀの最終宛先である HUB に直接接続している終端装置に対してﾊﾟｹｯﾄを送出することを特徴とする HUB 間ﾃﾞｰﾀ暗号化によるﾃﾞｰﾀｾｷｭﾘﾃｨ確保装置。
		ｱｸｾｽﾃｰﾌﾞﾙの改良 ｱｸｾｽﾙｰﾙとの関連付け 通信路	特許 3679086 02.10.10 H04L12/46 ﾊﾞｯﾌｧﾛｰ	**無線 LAN 中継装置、無線 LAN ｻｰﾋﾞｽの提供方法および無線 LAN ｻｰﾋﾞｽの提供ﾌﾟﾛｸﾞﾗﾑを記録した媒体** ｱｸｾｽ要求における上記暗号化の有無を判断する暗号化判断手段と、この暗号化判断手段にて暗号化が有ると判断されたときにはｱｸｾｽ制限ｴﾘｱとｱｸｾｽ非制限ｴﾘｱへのｱｸｾｽを許容するとともに、ｱｸｾｽ要求判断手段にて暗号化が無いと判断されたときにはｱｸｾｽ非制限ｴﾘｱへのｱｸｾｽだけを許容するｱｸｾｽ対象制限手段とを具備することを特徴とする無線 LAN 中継装置。
		回路の改良 ｽｲｯﾁ回路の追加 回路の切換	特許 3002134 95.05.16 B41J29/38 ｵｾｰﾈ-ﾃﾞﾙﾗﾝﾄﾞ(ｵﾗﾝﾀﾞ) 〔被引用回数 1〕	**通信制御装置を持つ印刷ｼｽﾃﾑ** 第１ネットワークを経由してプリントデータを受けとるために第１ネットワークに接続可能な印刷装置(2)と、印刷装置(2)に接続された通信制御装置(3)とを備え、通信制御装置(3)が、第２ネットワーク(4)を介して外部ステーションと通信をおこなうための外部通信手段(12,21)と、印刷装置(2)と通信を行うための内部通信手段(11,18)とを備える印刷システムであって、通信制御装置(3)が、さらに、印刷装置(2)が前記第１ネットワーク(1)と機能的に接続されないときのみに外部通信手段(12,21)が外部前記外部ステーション(5)と通信することができるようにする手段(16,20)を備える印刷システム。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（4/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	デバイスの正当性向上	各種の処理手順改良 特定情報の記憶、登録手順 認証情報の記憶	特許 3570890 98.04.24 G06F15/00,330 NEC ﾋﾞｭｰﾃｸﾉﾛｼﾞｰ	**ｲﾝﾀｰﾈｯﾄ端末におけるﾎｰﾑﾍﾟｰｼﾞの閲覧方法および装置** ｱｸｾｽしたｻｰﾊﾞのﾎｰﾑﾍﾟｰｼﾞの閲覧にあたって、ｻｰﾊﾞ側から ID およびまたはﾊﾟｽﾜｰﾄﾞの要求を受けたか否かを判定する要求判定ｽﾃｯﾌﾟと、要求判定ｽﾃｯﾌﾟにおいて、ｻｰﾊﾞ側から ID およびまたはﾊﾟｽﾜｰﾄﾞの要求を受けたと判定した場合に、ｲﾝﾀｰﾈｯﾄﾌﾞﾗｳｻﾞにおいて構築されたﾌﾞｯｸﾏｰｸに格納された URL に対応する ID およびまたはﾊﾟｽﾜｰﾄﾞを検索する検索ｽﾃｯﾌﾟと、検索ｽﾃｯﾌﾟにおいてﾌﾞｯｸﾏｰｸ領域より検索された ID およびまたはﾊﾟｽﾜｰﾄﾞをｻｰﾊﾞ側に送信する通信処理ｽﾃｯﾌﾟとをｲﾝﾀｰﾈｯﾄ端末において実行させるようにしたことを特徴とするｲﾝﾀｰﾈｯﾄ端末におけるﾎｰﾑﾍﾟｰｼﾞの閲覧方法。
	通信データの中継性能向上	情報の送信、転送、分岐の手順改良 特定情報の通知、送信手順 更新差分情報の送信	特許 3474453 98.09.04 G06F12/00,533 ﾋﾞｽﾄ(米国) 〔被引用回数 1〕	**ﾈｯﾄﾜｰｸにおけるﾜｰｸｽﾍﾟｰｽｴﾚﾒﾝﾄの多数のｺﾋﾟｰを安全に同期させる方法およびｼｽﾃﾑ** (a)防火壁内の第 1 の記憶部に格納された第 1 のﾜｰｸｽﾍﾟｰｽｴﾚﾒﾝﾄが変更されたか否かを示す第 1 のﾊﾞｰｼﾞｮﾝ情報から、第 1 の検査結果を発生するｽﾃｯﾌﾟと、(b)第 1 のﾜｰｸｽﾍﾟｰｽｴﾚﾒﾝﾄの個別に変更可能なｺﾋﾟｰであって防火壁の外の第 2 の記憶部に格納されたものが変更されたか否かを示す第 2 のﾊﾞｰｼﾞｮﾝ情報から、第 2 の検査結果を発生するｽﾃｯﾌﾟと、(c)所定の規準が満たされたとき、防火壁内から前記ｽﾃｯﾌﾟ(a)および(b)を起動するｽﾃｯﾌﾟと、(d)第 1 の検査結果および第 2 の検査結果に基づき、第 1 のﾜｰｸｽﾍﾟｰｽｴﾚﾒﾝﾄおよびｺﾋﾟｰから好ましいﾊﾞｰｼﾞｮﾝを発生するｽﾃｯﾌﾟと、(e)好ましいﾊﾞｰｼﾞｮﾝを第 1 の記憶部および第 2 の記憶部に格納するｽﾃｯﾌﾟとを具備するｺﾝﾋﾟｭｰﾀに基づく方法。
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IP ｱﾄﾞﾚｽの割付 ﾘﾀﾞｲﾚｸﾄｱﾄﾞﾚｽの割付	特許 3588323 98.05.04 H04L12/58,100 ｵｰﾘｯｸ ｳｪﾌﾞ ｼｽﾃﾑｽﾞ(米国)	**ﾕｰｻﾞ専用のﾃﾞｰﾀﾘﾀﾞｲﾚｸｼｮﾝｼｽﾃﾑ、および、ﾕｰｻﾞ専用のﾃﾞｰﾀﾘﾀﾞｲﾚｸｼｮﾝを実行する方法** 複数のﾕｰｻﾞ ID の各々を各ﾕｰｻﾞ専用の規則ｾｯﾄに相関させる項目を含むﾃﾞｰﾀﾍﾞｰｽと、ﾕｰｻﾞのｺﾝﾋﾟｭｰﾀからﾕｰｻﾞ ID を受け取るﾀﾞｲｱﾙｱｯﾌﾟ・ﾈｯﾄﾜｰｸ・ｻｰﾊﾞと、ﾀﾞｲｱﾙｱｯﾌﾟ・ﾈｯﾄﾜｰｸ・ｻｰﾊﾞに接続されているﾘﾀﾞｲﾚｸｼｮﾝ・ｻｰﾊﾞと、ﾃﾞｰﾀﾍﾞｰｽとﾀﾞｲｱﾙｱｯﾌﾟ・ﾈｯﾄﾜｰｸ・ｻｰﾊﾞとﾘﾀﾞｲﾚｸｼｮﾝ・ｻｰﾊﾞとに接続されている認証および課金ｻｰﾊﾞとを含むﾕｰｻﾞ専用の自動ﾃﾞｰﾀﾘﾀﾞｲﾚｸｼｮﾝｼｽﾃﾑであって、ﾀﾞｲｱﾙｱｯﾌﾟ・ﾈｯﾄﾜｰｸ・ｻｰﾊﾞは、第 1 のﾕｰｻﾞ ID と第 1 のﾕｰｻﾞ ID のための一時割当てﾈｯﾄﾜｰｸｱﾄﾞﾚｽとを認証および課金ｻｰﾊﾞに伝送し、認証および課金ｻｰﾊﾞはﾃﾞｰﾀﾍﾞｰｽにｱｸｾｽし、ﾕｰｻﾞ ID と相関する各ﾕｰｻﾞ専用の規則ｾｯﾄと一時割当てﾈｯﾄﾜｰｸｱﾄﾞﾚｽとを前記ﾘﾀﾞｲﾚｸｼｮﾝ・ｻｰﾊﾞに伝送する、ﾕｰｻﾞ専用の自動ﾃﾞｰﾀﾘﾀﾞｲﾚｸｼｮﾝｼｽﾃﾑ。
		回路の改良 ｽｲｯﾁ回路の追加 専用線の活用	特許 3597448 00.05.12 H04L12/54 住友重機械工業	**情報ｱｸｾｽ方法及びﾈｯﾄﾜｰｸｼｽﾃﾑ** ﾌｧｲｱｳｫｰﾙで保護されたﾈｯﾄﾜｰｸ内に第 1 ｻｰﾊﾞを配備し、第 1 ｻｰﾊﾞとﾈｯﾄﾜｰｸの外側に存する第 2 ｻｰﾊﾞとを専用回線又は仮想専用回線を介して接続するとともに、第 1 ｻｰﾊﾞ及び第 2 ｻｰﾊﾞが保有するﾌｧｲﾙの少なくとも一部を互いに共通内容に維持された共通ﾌｧｲﾙとし、第 1 ｻｰﾊﾞの共通ﾌｧｲﾙに対する情報のｱｸｾｽを受容することで、第 2 ｻｰﾊﾞの共通ﾌｧｲﾙ内の情報をｱｸｾｽの発信端末で知得可能にすることを特徴とする、情報ｱｸｾｽ方法。
	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾊﾟｹｯﾄｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特許 3576000 98.09.17 G06F15/16,620 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ 〔被引用回数 1〕	**ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ** ﾈｯﾄﾜｰｸ上に分散して存在する複数のｸﾗｲｱﾝﾄｺﾝﾋﾟｭｰﾀが使用するｸﾗｲｱﾝﾄﾌﾟﾛｸﾞﾗﾑを、ﾈｯﾄﾜｰｸおよび所定のｾｷｭﾘﾃｨｼｽﾃﾑを中継してｻｰﾊﾞｺﾝﾋﾟｭｰﾀから取得して実行するｼｽﾃﾑにおいて、ｾｷｭﾘﾃｨｼｽﾃﾑ上で稼働する分散ｵﾌﾞｼﾞｪｸﾄ間通信を中継する中継ﾌﾟﾛｸﾞﾗﾑを、ｸﾗｲｱﾝﾄｺﾝﾋﾟｭｰﾀがｻｰﾊﾞｺﾝﾋﾟｭｰﾀからｸﾗｲｱﾝﾄﾌﾟﾛｸﾞﾗﾑを入手する時に、ｻｰﾊﾞｺﾝﾋﾟｭｰﾀからｾｷｭﾘﾃｨｼｽﾃﾑのｺﾝﾋﾟｭｰﾀに送信して自動的に構築することを特徴とする分散ｵﾌﾞｼﾞｪｸﾄ間通信中継ｼｽﾃﾑ。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（5/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 出願人 [被引用回数]	発明の名称 概要
プロキシ中継技術	攻撃パターンの高精度化	ﾃﾞｰﾀ形式の改良 ｵﾌﾞｼﾞｪｸﾄのﾃﾞｰﾀ形式改良 ﾊﾟｹｯﾄｵﾌﾞｼﾞｪｸﾄﾓﾃﾞﾙ	特許 3575978 98.03.27 G06F15/16,620 日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ	**ｺﾝﾋﾟｭｰﾀｼｽﾃﾑ** ﾈｯﾄﾜｰｸ上で複数の異なるｺﾝﾋﾟｭｰﾀが接続され、ｺﾝﾋﾟｭｰﾀ上で稼動する分散ｵﾌﾞｼﾞｪｸﾄ間の通信の中継を行なうｼｽﾃﾑにおいて、ｾｷｭﾘﾃｨ対策を講じる中継ｺﾝﾋﾟｭｰﾀ上で実行可能な分散ｵﾌﾞｼﾞｪｸﾄ間の通信を中継するﾌﾟﾛｸﾞﾗﾑを、通信先のｻｰﾊﾞﾌﾟﾛｸﾞﾗﾑのｵﾌﾞｼﾞｪｸﾄ定義から自動生成することを特徴とする分散ｵﾌﾞｼﾞｪｸﾄ間通信中継ﾌﾟﾛｸﾞﾗﾑ自動生成ｼｽﾃﾑ。
コンテンツフィルタリング技術	利用サービスの保護強化	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞ-の配置 ｱｸｾｽ制御ｻｰﾊﾞ-の配置	特許 3577494 00.11.29 G06F15/00,310 ｵｰﾋﾞｯｸﾋﾞｼﾞﾈｽｺﾝｻﾙﾀﾝﾄ	**ｲﾝﾀｰﾈｯﾄを介する業務ｿﾌﾄｻｰﾋﾞｽｼｽﾃﾑ** ｸﾗｲｱﾝﾄ端末は、少なくとも Web ﾌﾞﾗｳｻﾞと、前記仲介ｻｰﾋﾞｽ処理装置より送られた業務ｿﾌﾄ Web 画面にﾃﾞｰﾀを入力し生成した処理結果を蓄積･更新できる業務ｿﾌﾄ処理結果記録部を備え、仲介ｻｰﾋﾞｽ処理装置は、少なくとも利用者が処理入力画面にﾃﾞｰﾀを入力した処理結果をその記憶部に書込む処理結果書込実行ﾌｧｲﾙを送信し実行させる実行ﾌｧｲﾙ送信手段を備えることを特徴とするｲﾝﾀｰﾈｯﾄを介する業務ｿﾌﾄｻｰﾋﾞｽｼｽﾃﾑ。
	システムの性能向上	ｱｸｾｽﾃｰﾌﾞﾙの改良 認証情報との関連付け ID 認証情報	特許 3568832 99.08.24 G06F15/00,330 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾑｳｪｱ	**遠隔操作認証方法及び遠隔操作認証ﾌﾟﾛｸﾞﾗﾑを記録した記録媒体** 遠隔操作認証ｼｽﾃﾑは、作業者が遠隔操作を行う運用端末と、運用端末からの依頼に応じて作業者に対する認証及び運用端末からの遠隔操作に対する認証を行う認証ｻｰﾊﾞと、遠隔操作が認証ｻｰﾊﾞから認証された場合にこの遠隔操作に応じて業務ｼｽﾃﾑに対して監視･運用を行うｲﾍﾞﾝﾄを運用端末に代わって発行する監視ｻｰﾊﾞと、を備えたことを特徴とする遠隔操作認証ｼｽﾃﾑ。
	攻撃の抑止・予防の強化	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの暗号化	特許 3400480 93.01.20 G06F15/00,330 ｼｰｴｽｹｲ	**ﾌﾟﾛｸﾞﾗﾑ解析防止装置** 上位装置と、上位装置に通信回線を介して接続した端末装置とからなり、上位装置は、所定の規則にしたがってﾌﾟﾛｸﾞﾗﾑを暗号化する暗号化ｷｰを入力するｷｰ入力部と、該ｷｰ入力部より入力した暗号化ｷｰを記憶し保持する暗号化ｷｰ記憶部と、暗号化ｷｰにしたがって暗号化されたﾌﾟﾛｸﾞﾗﾑを復号化する編集ﾌﾟﾛｸﾞﾗﾑを記憶したﾌﾟﾛｸﾞﾗﾑ編集部と、ｷｰ入力部、暗号化ｷｰ記憶部及びﾌﾟﾛｸﾞﾗﾑ編集部を制御する制御部とを備えてなり、端末装置は、動作ﾌﾟﾛｸﾞﾗﾑを記憶し保持するﾌﾟﾛｸﾞﾗﾑ記憶部と、上位装置からﾀﾞｳﾝﾛｰﾄﾞされた暗号化ｷｰを記憶し保持する暗号化ｷｰ記憶部と、暗号化ｷｰにしたがってﾌﾟﾛｸﾞﾗﾑを暗号化する編集ﾌﾟﾛｸﾞﾗﾑを記憶したﾌﾟﾛｸﾞﾗﾑ編集部と、ﾌﾟﾛｸﾞﾗﾑ記憶部、暗号化ｷｰ記憶部及びﾌﾟﾛｸﾞﾗﾑ編集部を制御して、上位装置との接続が断たれた場合にﾌﾟﾛｸﾞﾗﾑ編集部に動作ﾌﾟﾛｸﾞﾗﾑの暗号化を行なわせ、かつその後ﾌﾟﾛｸﾞﾗﾑ編集部の編集ﾌﾟﾛｸﾞﾗﾑを消去すると共に、上位装置との接続が復旧した場合に暗号化した動作ﾌﾟﾛｸﾞﾗﾑを上位装置にｱｯﾌﾟﾛｰﾄﾞする制御部とを備えてなることを特徴とするﾌﾟﾛｸﾞﾗﾑ解析防止装置。
IPフィルタリング技術	侵入防御の性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞ-の配置 ﾒｰﾙｻｰﾊﾞ-の配置	特許 3472014 96.02.20 H04L12/58,100 ﾌﾞﾗｻﾞｰ工業 〔被引用回数 4〕	**電子ﾒｰﾙ転送装置** ﾛｰｶﾙﾈｯﾄﾜｰｸと広域ﾈｯﾄﾜｰｸとの間でﾈｯﾄﾜｰｸ中継手段を介してﾒｰﾙの送受信を行うことが可能な電子ﾒｰﾙ転送装置において、ﾛｰｶﾙﾈｯﾄﾜｰｸに接続され、かつﾒｰﾙの送受信を行う第一のﾒｰﾙｻｰﾋﾞｽ手段と、広域ﾈｯﾄﾜｰｸに接続され、かつﾒｰﾙの送受信を行う第二のﾒｰﾙｻｰﾋﾞｽ手段とを備え、第一のﾒｰﾙｻｰﾋﾞｽ手段は、ﾒｰﾙを受信するﾕｰｻﾞを指定するﾕｰｻﾞ指定手段と、ﾒｰﾙを送信するための期間を指定する期間指定手段と、ﾕｰｻﾞ指定手段により指定されたﾕｰｻﾞに対し、期間指定手段により指定された期間内に第一のﾒｰﾙｻｰﾋﾞｽ手段に対して送られたﾒｰﾙを第二のﾒｰﾙｻｰﾋﾞｽ手段に転送するﾒｰﾙ転送手段とを備えたことを特徴とする電子ﾒｰﾙ転送装置。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（6/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 出願人 [被引用回数]	発明の名称 概要
IPフィルタリング技術	経済性の向上 侵入防御の性能向上	ﾌｨﾙﾀﾃｰﾌﾞﾙの改良 攻撃元ｱﾄﾞﾚｽの追加 IPｱﾄﾞﾚｽの削除	特許 3662080 96.08.29 H04L12/56,100 KDDI 〔被引用回数 3〕	**ﾌｧｲｱｳｫｰﾙ動的制御方法** ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞにﾀﾞｲｱﾙｱｯﾌﾟにより接続中の端末がｲﾝﾀｰﾈｯﾄを経由してﾌｧｲｱｳｫｰﾙ内の内部ﾈｯﾄﾜｰｸにｱｸｾｽする際に、前記ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞから前記内部ﾈｯﾄﾜｰｸに前記端末のﾕｰｻﾞ情報を送ること、前記内部ﾈｯﾄﾜｰｸはこのﾕｰｻﾞ情報を基に前記端末が同内部ﾈｯﾄﾜｰｸから移動した移動端末か否かを判断すること、前記端末が移動端末である場合に同端末と内部ﾈｯﾄﾜｰｸとの通信を許可するようにﾌｧｲｱｳｫｰﾙのﾌｨﾙﾀを設定することを特徴とするﾌｧｲｱｳｫｰﾙ動的制御方法。
	システムの性能向上	ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｾｷｭﾘﾃｨｻｰﾊﾞ-の配置 ｴｯｼﾞﾉｰﾄﾞにﾌｧｲｱｳｫｰﾙ機能の分割配置	特許 3654847 01.03.30 H04L12/56,260 ﾃﾗｲﾃｯﾄﾞ ｲﾝﾀｰﾅｼｮﾅﾙ(米国)	**層 2 の同報ﾈｯﾄﾜｰｸにおける広帯域ｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｻｰﾋﾞｽを管理する装置及び方法** 層2の同報ﾈｯﾄﾜｰｸにおける広帯域ｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｻｰﾋﾞｽを管理する装置であって、外部からのﾄﾗﾌｨｯｸを受け、前記ﾈｯﾄﾜｰｸ上でｻｰﾋﾞｽの情報を広告しかつ提供する少なくとも1つのｴﾝﾄﾞ装置に該ﾄﾗﾌｨｯｸを転送し、前記ｴﾝﾄﾞ装置からの応答のﾄﾗﾌｨｯｸを前記外部に転送する少なくとも 1 つの中間装置と、前記ﾈｯﾄﾜｰｸ上のすべての装置からの登録を処理し、前記ﾈｯﾄﾜｰｸ上で特定のｻｰﾋﾞｽのためのｻｰﾊﾞﾘｽﾄを検索する新規の装置の要求に応答し、前記ﾈｯﾄﾜｰｸのための割り当て番号の権限ｻｰﾊﾞとして作動し、登録されたすべての装置を管理する管理ｴｰｼﾞｪﾝﾄとして作動する少なくとも 1 つの監視装置とを含み、前記中間装置は、該中間装置が前記ｴﾝﾄﾞ装置によるｻｰﾋﾞｽの広告から認識する利用可能な前記ｴﾝﾄﾞ装置にｻｰﾋﾞｽの要求のﾊﾟｹｯﾄを転送し、前記ｴﾝﾄﾞ装置は、出所からのﾄﾗﾌｨｯｸを他の前記ｴﾝﾄﾞ装置に転送するように前記中間装置に命じることを前記ｴﾝﾄﾞ装置が決定したとき、流れの情報を他の前記中間装置に広告することができ、前記ｻｰﾋﾞｽの情報は前記ﾈｯﾄﾜｰｸ上で前記ｴﾝﾄﾞ装置によって広告され、前記中間装置は常に前記ｴﾝﾄﾞ装置によって広告された流れに基づいたﾊﾟｹｯﾄを転送し、前記ｴﾝﾄﾞ装置は前記ﾈｯﾄﾜｰｸにおいて他の装置を中断させることなくかつ前記ｻｰﾋﾞｽに影響を及ぼすことなく負荷を共有するためにｵﾝｻﾞﾌﾗｲで追加され、ｵﾝｻﾞﾌﾗｲで停止される、層 2 の同報ﾈｯﾄﾜｰｸにおける広帯域ｲﾝﾀｰﾈｯﾄﾌﾟﾛﾄｺﾙｻｰﾋﾞｽを管理する装置。
ルーティング制御技術	侵入防御の性能向上	情報の送信、転送、分岐の手順改良 設定値で分岐の手順 送信方向	特許 3251220 97.10.24 H04L12/66 NEC 通信ｼｽﾃﾑ	**ｲﾝﾀｰﾈｯﾄとｲﾝﾄﾗﾈｯﾄのｱﾄﾞﾚｽ重複時の通信方式** IP ﾌﾟﾛﾄｺﾙに準拠したｲﾝﾄﾗﾈｯﾄとｲﾝﾀｰﾈｯﾄとを接続するｹﾞｰﾄｳｪｲﾙｰﾀを備え、前記 IP ﾌﾟﾛﾄｺﾙの IP ｱﾄﾞﾚｽのﾌｨｰﾙﾄﾞはﾈｯﾄﾜｰｸ部とﾎｽﾄ部とを含む通信方式において、前記ｲﾝﾄﾗﾈｯﾄ内に接続されている第1の装置が前記ｹﾞｰﾄｳｪｲﾙｰﾀを介して送信先である第 2 の装置に送信する場合前記ｹﾞｰﾄｳｪｲﾙｰﾀは、あらかじめﾃﾞｰﾀﾍﾞｰｽに登録された前記ｲﾝﾄﾗﾈｯﾄ内使用の IP ｱﾄﾞﾚｽのﾈｯﾄﾜｰｸ部の値と受信した IP ﾊﾟｹｯﾄﾍｯﾀﾞの送信先ｱﾄﾞﾚｽのﾈｯﾄﾜｰｸ部の値とを比較する比較手段と、前記比較手段において一致するﾈｯﾄﾜｰｸ部の値があれば送信元の前記第1の装置へ送信種別を問い合わせる問い合せ手段と、前記問い合せ手段による前記第1の装置からの問い合わせ応答によりｲﾝﾄﾗﾈｯﾄの内または外へ送信先を決定する決定手段とを有することを特徴とするｲﾝﾀﾈｯﾄとｲﾝﾄﾗﾈｯﾄのｱﾄﾞﾚｽ重複時の通信方式。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（7/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
ルーティング制御技術	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特許 3009737 94.12.07 H04L12/66 ﾏﾂｼﾀ･ｴﾚｸﾄﾘｯｸ(米国)	**相互接続ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸの機密保護装置** 第 1 のｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸおよび第 2 のｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ間の未公認の通信を防止するための機密保護装置において、第 1 のﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞおよび第 2 のﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞであって、該第 1 および第 2 のﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞが各々上記第 1 および第 2 のｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸとそれぞれ通信するためのﾈｯﾄﾜｰｸｲﾝﾀﾌｪｰｽｱﾀﾞﾌﾟﾀを有する上記第 1 のﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞおよび第 2 のﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞを備え、上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞの各々が更に転送ｱﾀﾞﾌﾟﾀを有し、該転送ｱﾀﾞﾌﾟﾀは上記他方のﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞの上記転送ｱﾀﾞﾌﾟﾀと通信するためのもので、同一で且つ整合されており、上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞの各々は上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞ各々の上記ﾈｯﾄﾜｰｸｲﾝﾀﾌｪｰｽｱﾀﾞﾌﾟﾀおよび上記転送ｱﾀﾞﾌﾟﾀ間のﾙｰﾄｻｰﾋﾞｽ情報の伝送を防止するためのﾈｯﾄﾜｰｸｵﾍﾟﾚｰﾃｨﾝｸﾞｿﾌﾄｳｪｱを有し、上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞの各々は上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞ各々の上記ﾈｯﾄﾜｰｸｲﾝﾀﾌｪｰｽｱﾀﾞﾌﾟﾀおよび上記転送ｱﾀﾞﾌﾟﾀ間のﾙｰﾄｻｰﾋﾞｽ情報の伝送を防止するためのﾈｯﾄﾜｰｸｵﾍﾟﾚｰﾃｨﾝｸﾞｿﾌﾄｳｪｱを有し、上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞの各々は更に上位ﾚﾍﾞﾙ層ﾌﾟﾛﾄｺﾙ情報および発生ｿｰｽ･宛先ｱﾄﾞﾚｽ情報を上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞ各々の上記ﾈｯﾄﾜｰｸｲﾝﾀﾌｪｰｽｱﾀﾞﾌﾟﾀおよび上記転送ｱﾀﾞﾌﾟﾀ間で通過させないようにするﾌﾟﾛﾄｺﾙ変換ｿﾌﾄｳｪｱを有し、上記ﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞの少なくとも 1 つは、該少なくとも 1 つのﾈｯﾄﾜｰｸﾏｻﾞｰﾎﾞｰﾄﾞに接続されたｺﾝﾋﾟｭｰﾀへｱﾌﾟﾘｹｰｼｮﾝﾚﾍﾞﾙ通信ｻｰﾋﾞｽを提供するためのｱﾌﾟﾘｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾐﾝｸﾞｲﾝﾀﾌｪｰｽ(API)ｼﾑｿﾌﾄｳｪｱを有する機密保護装置。
		ﾌｧｲｱｳｫｰﾙ外のｼｽﾃﾑ構成 ｻｰﾋﾞｽｻｰﾊﾞｰの配置 仲介ｻｰﾊﾞｰ配置	特許 3208115 97.11.20 H04L12/58,200 ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ 〔被引用回数 1〕	**ﾌｧｸｼﾐﾘ通信ﾈｯﾄﾜｰｸｼｽﾃﾑおよび通信方法** 電話網およびﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸに接続され、前記ﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸから受信したﾃﾞｰﾀを FAX 端末に配信する、前記ﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸ上の FAX ｻｰﾊﾞと、ﾙｰﾀおよび中継網を介して前記ﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸに接続され、加入者ﾃﾞｰﾀを一元的に収容･管理し、ｻｰﾋﾞｽ制御を行う統括ｻｰﾊﾞを有するﾌｧｸｼﾐﾘ通信ﾈｯﾄﾜｰｸｼｽﾃﾑ。
IPアドレス変換技術	侵入防御の性能向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特許 3626743 02.05.16 H04L12/66 NEC ｱｸｾｽﾃｸﾆｶ	**ﾊﾟｹｯﾄ転送装置、ﾊﾟｹｯﾄ転送方法及びﾊﾟｹｯﾄ転送ﾌﾟﾛｸﾞﾗﾑ** 第 1 のﾈｯﾄﾜｰｸと第 2 のﾈｯﾄﾜｰｸに接続され、ﾈｯﾄﾜｰｸｱﾄﾞﾚｽとﾎｽﾄｱﾄﾞﾚｽから構成されるｿｰｽｱﾄﾞﾚｽを有するﾊﾟｹｯﾄを、前記第 1 のﾈｯﾄﾜｰｸから前記第 2 のﾈｯﾄﾜｰｸへ転送するﾊﾟｹｯﾄ転送装置であって、前記第 1 のﾈｯﾄﾜｰｸに接続された 1 又は 2 以上のｸﾗｲｱﾝﾄ端末のﾈｯﾄﾜｰｸｱﾄﾞﾚｽ及び当該ｸﾗｲｱﾝﾄ端末のﾎｽﾄｱﾄﾞﾚｽを記憶するﾒﾓﾘと、前記第 1 のﾈｯﾄﾜｰｸに接続されたｸﾗｲｱﾝﾄ端末から送信された前記ﾊﾟｹｯﾄを受信する受信手段と、前記受信されたﾊﾟｹｯﾄからｿｰｽｱﾄﾞﾚｽを抽出する抽出手段と、前記ｿｰｽｱﾄﾞﾚｽを、ﾈｯﾄﾜｰｸｱﾄﾞﾚｽとﾎｽﾄｱﾄﾞﾚｽとに分割する分割手段と、前記分割されたﾈｯﾄﾜｰｸｱﾄﾞﾚｽ及びﾎｽﾄｱﾄﾞﾚｽのそれぞれについて、前記ﾒﾓﾘに記憶されたﾈｯﾄﾜｰｸｱﾄﾞﾚｽ及びﾎｽﾄｱﾄﾞﾚｽと比較を行う比較手段と、前記比較手段の比較結果に基づいて、前記受信されたﾊﾟｹｯﾄを前記第 1 のﾈｯﾄﾜｰｸから前記第 2 のﾈｯﾄﾜｰｸへ転送するか否か決定する決定手段と、前記決定手段により前記第 1 のﾈｯﾄﾜｰｸから前記第 2 のﾈｯﾄﾜｰｸへ転送すると決定された場合に、前記受信されたﾊﾟｹｯﾄを前記第 2 のﾈｯﾄﾜｰｸへ転送する転送手段と、を備えることを特徴とするﾊﾟｹｯﾄ転送装置。
		ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 URL ﾄﾞﾒｲﾝの変換	特許 3001489 98.01.16 H04L12/54 NEC ｿﾌﾄ	**TCP/IP 通信網ﾌﾞﾗｳｻﾞ装置** TCP/IP 通信網を通じたﾃﾞｰﾀ通信によるﾎｰﾑﾍﾟｰｼﾞ閲覧を Web ﾌﾞﾗｳｻﾞでのｿﾌﾄｳｪｱ処理によって行う TCP/IP 通信網ﾌﾞﾗｳｻﾞ装置において、受取側の Web ﾌﾞﾗｳｻﾞへの URL の設定によって、送出側の Web ﾍﾟｰｼﾞにおける特定の URL へのｱｸｾｽを規制する制御を行うｱｸｾｽ規制制御手段を備えることを特徴とする TCP/IP 通信網ﾌﾞﾗｳｻﾞ装置。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（8/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主IPC 出願人 [被引用回数]	発明の名称 概要
IPアドレス変換技術	侵入防御の性能向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 IPｱﾄﾞﾚｽの割付 相対ｱﾄﾞﾚｽの割付	特許 3310851 96.02.27 H04L12/46 PFU 〔被引用回数 2〕	**ﾌｨﾙﾀﾘﾝｸﾞ装置に対するﾌｨﾙﾀﾘﾝｸﾞ条件設定方法** 送信元IPｱﾄﾞﾚｽと送信元ﾈｯﾄﾏｽｸを有する始点ｱﾄﾞﾚｽ、着信先IPｱﾄﾞﾚｽと着信先ﾈｯﾄﾏｽｸを有する終点ｱﾄﾞﾚｽ、ﾌﾟﾛﾄｺﾙ、始点ﾎﾟｰﾄ、終点ﾎﾟｰﾄ、通過または非通過の処理方法の設定項目を持つﾌｨﾙﾀﾘﾝｸﾞ条件設定ﾌｧｲﾙ(11)と、ｱﾌﾟﾘｹｰｼｮﾝｹﾞｰﾄｳｪｲが中継するﾌﾟﾛﾄｺﾙとﾎﾟｰﾄからなるｻｰﾋﾞｽ情報、ｱﾌﾟﾘｹｰｼｮﾝｹﾞｰﾄｳｪｲのﾌｨﾙﾀﾘﾝｸﾞ装置との相対位置とIPｱﾄﾞﾚｽからなるｲﾝｽﾄｰﾙ位置の設定情報を持つｱﾌﾟﾘｹｰｼｮﾝｹﾞｰﾄｳｪｲ定義ﾌｧｲﾙ(12)とを使用することでﾌｨﾙﾀﾘﾝｸﾞ条件設定を行うことを特徴とするﾌｨﾙﾀﾘﾝｸﾞ装置に対するﾌｨﾙﾀﾘﾝｸﾞ条件設定方法。
	通信データの中継性能向上	各種の処理手順改良 ﾌﾟﾛﾄｺﾙの処理手順 ﾌﾟﾛﾄｺﾙ変換	特許 3457645 97.12.31 H04L12/66 ｴｽ ｴｽ ｴｲﾁ ｺﾐｭﾆｹｰｼｮﾝｽﾞ ｾｷｭﾘﾃｨ(ﾌｨﾝﾗﾝﾄﾞ)	**ﾈｯﾄﾜｰｸ･ｱﾄﾞﾚｽ変換とﾌﾟﾛﾄｺﾙ変換が存在する場合のﾊﾟｹｯﾄ認証の方法** ﾈｯﾄﾜｰｸにおいて送信ﾉｰﾄﾞ(903)と受信ﾉｰﾄﾞ(902)の間の適用可能なｾｷｭﾘﾃｨ･ﾎﾟﾘｼｰによってﾊﾟｹｯﾄ認証を達成する方法であって、前記送信ﾉｰﾄﾞと前記受信ﾉｰﾄﾞの間で転送されるﾊﾟｹｯﾄに対して行われる変換を動的に発見するｽﾃｯﾌﾟ(1003、1004)と、前記適用可能なｾｷｭﾘﾃｨ･ﾎﾟﾘｼｰに基づいて前記発見された変換が許容可能であることを検査するｽﾃｯﾌﾟ(1004)と、前記送信ﾉｰﾄﾞから前記受信ﾉｰﾄﾞに送信されるﾊﾟｹｯﾄを認証する前に、前記動的に発見された許容可能な変換を補償するｽﾃｯﾌﾟ(1004、1006)とを含むことを特徴とする方法。
ホスト認証技術	システムの性能向上	情報の照合、検索、ｶｳﾝﾄ手順改良 特定情報の照合手順 時間･期間情報	特許 3648159 00.12.29 G06F17/60,140 あいおい損害保険	**認証ｼｽﾃﾑ** ｻｰﾋﾞｽ提供者のｻｰﾋﾞｽ提供者ｻｰﾊﾞと認証者の認証者ｻｰﾊﾞとｸﾗｲｱﾝﾄのｸﾗｲｱﾝﾄ端末とがﾈｯﾄﾜｰｸを介して接続され、前記ｸﾗｲｱﾝﾄ端末は、前記ｻｰﾋﾞｽ提供者ｻｰﾊﾞの提供するｻｰﾋﾞｽに関する取扱情報を画面に表示する取扱情報表示手段と、前記ｻｰﾋﾞｽ提供者ｻｰﾊﾞが前記認証者ｻｰﾊﾞに認証されたことを示す認証情報を、前記取扱情報と同一の表示画面内の別々の表示領域で表示する認証情報表示手段とを備え、前記ｻｰﾋﾞｽ提供者ｻｰﾊﾞは、前記取扱情報を記憶する記憶手段と、前記ｸﾗｲｱﾝﾄ端末へ前記取扱情報を送信する取扱情報送信手段と、前記認証者ｻｰﾊﾞから受信した認証情報を前記ｸﾗｲｱﾝﾄ端末の表示画面内で前記取扱情報と別々の表示領域で表示させるよう送信する認証情報送信手段とを備え、前記認証者ｻｰﾊﾞは、前記ｻｰﾋﾞｽ提供者ｻｰﾊﾞの認証状態を記録した認証登録情報を格納する認証登録情報ﾃﾞｰﾀﾍﾞｰｽと、前記ｻｰﾋﾞｽ提供者に対応する前記認証情報を前記ｻｰﾋﾞｽ提供者ｻｰﾊﾞに送信する送信手段とを備える認証ｼｽﾃﾑ。
		ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀに情報付加 更新情報の付加	特許 3673660 98.11.06 H04L12/24 NEC ｴﾝｼﾞﾆｱﾘﾝｸﾞ	**遠隔管理ｼｽﾃﾑ** ｲﾝﾀｰﾈｯﾄ等の外部にｵｰﾌﾟﾝなﾈｯﾄﾜｰｸを介して接続されたﾕｰｻﾞﾛｰｶﾙﾈｯﾄﾜｰｸと管理会社ﾛｰｶﾙﾈｯﾄﾜｰｸとを備え、該管理会社ﾛｰｶﾙﾈｯﾄﾜｰｸは、前記ﾕｰｻﾞﾛｰｶﾙﾈｯﾄﾜｰｸ内装置に、ﾌｧｲｱｳｫｰﾙを越えて管理情報を収集解析可能とし、前記ﾕｰｻﾞﾛｰｶﾙﾜｰｸ内にﾈｯﾄﾜｰｸ管理装置を不要とすることを特徴とする遠隔管理ｼｽﾃﾑ。
トンネリング技術	中継するデータの機密性向上	ﾌｧｲｱｳｫｰﾙ内のｼｽﾃﾑ構成 DMZに機器の配置 中継ｻｰﾊﾞ-の配置	特許 3665311 02.10.11 H04L12/56 ｸﾎﾞﾀｼｽﾃﾑ開発	**通信ｼｽﾃﾑ** 公衆通信網に接続する接続装置を備える通信ｼｽﾃﾑにおいて、前記接続装置と通信する通信装置を備え、前記接続装置は、公衆通信網に接続する不特定の装置と通信を行う手段を備え、前記通信装置は、公衆通信網に接続する特定の顧客装置と、保護された情報の通信を行う手段を備えることを特徴とする通ｼｽﾃﾑ。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（9/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
トンネリング技術	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾃﾞｰﾀの分割、仕分け	特許 3654712 96.07.01 H04L12/22 ｴｸｼﾝｸﾞ,ﾌﾞﾗｻﾞｰ工業(共願)	**送信側ﾃﾞｰﾀ通信装置** 送信側ﾃﾞｰﾀ通信装置から前記受信側ﾃﾞｰﾀ通信装置に対して接続要求があると、接続要求に対して接続を許可する接続許可手段と、接続許可手段によって接続を許可した結果、送信側ﾃﾞｰﾀ通信装置との間に複数の回線が確立された後、元のﾃﾞｰﾀを単独では実質的に使用不可能に分割した分割ﾃﾞｰﾀが、送信側ﾃﾞｰﾀ通信装置から確立された複数の回線のそれぞれに割り当てられて送信されてきた場合には、分割ﾃﾞｰﾀを受信する受信手段と、受信手段によって受信した分割ﾃﾞｰﾀを記憶する記憶手段と、記憶手段に記憶された分割ﾃﾞｰﾀを読み出し、元のﾃﾞｰﾀに復元する復元手段とを備えたことを特徴とする受信側ﾃﾞｰﾀ通信装置。
	中継するデータの機密性向上	ﾃﾞｰﾀ形式の改良 ﾃﾞｰﾀの変換 ﾍﾟｲﾛｰﾄﾞの暗号化	特許 3586203 00.07.10 H04L12/66 ｵｰﾙﾀｰﾜﾝ(米国)	**高品質のｻｰﾋﾞｽのｲﾝﾀｰﾈｯﾄを利用したﾜｲﾄﾞｴﾘｱﾈｯﾄﾜｰｸ** ｿｰｽのﾌｧｲﾔｰｳｫｰﾙの一つの回線と、ｲﾝﾀｰﾈｯﾄのｻｰﾋﾞｽを提供する他の参加している ISX/ISP ﾌﾟﾛﾊﾞｲﾀﾞｰの持つ一つまたはそれ以上のﾙｰﾀｰで、これらのﾙｰﾀｰは一つの終端の地点の参加しているISX/ISPﾌﾟﾛﾊﾞｲﾀﾞｰにある一つのﾙｰﾀｰを含み、一つまたはそれ以上のﾙｰﾀｰは、一つ目のISX/ISPの一つのﾙｰﾀｰを終端の地点の参加しているISX/ISPﾌﾟﾛﾊﾞｲﾀﾞｰの一つのﾙｰﾀｰへと該参加している ISX/ISP ﾌﾟﾛﾊﾞｲﾀﾞｰの該一つまたはそれ以上のﾙｰﾀｰを通って結合する、あらかじめ定められたﾌﾟﾗｲﾍﾞｰﾄなﾄﾝﾈﾙの一つのﾃﾞｰﾀﾊﾟｽを構築する機能を果たす、一つまたはそれ以上のﾙｰﾀｰと、目的地の一つのﾙｰﾀｰで、目的地のﾙｰﾀｰへか、その一部へと結合された一つのﾁｬﾝﾈﾙｻｰﾋﾞｽﾕﾆｯﾄを含み、ﾁｬﾝﾈﾙｻｰﾋﾞｽﾕﾆｯﾄおよび二つ目の専用ﾗｲﾝを通じて終端の地点の ISX/ISP ﾌﾟﾛﾊﾞｲﾀﾞｰのﾙｰﾀｰへと結合された目的地のﾙｰﾀｰと、目的地ﾙｰﾀｰへと直接または一つのﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸを通じて結合された WAN ｲﾝﾀｰﾌｪｰｽを一つ持ち、ﾜｲﾄﾞｴﾘｱﾈｯﾄﾜｰｸ上での通信が望まれる一つの装置へと、直接または一つのﾛｰｶﾙｴﾘｱﾈｯﾄﾜｰｸを通じて結合するための二つ目のﾎﾟｰﾄを持つ持つ目的地のﾌｧｲﾔｰｳｫｰﾙの一つの回線で、ﾌｧｲﾔｰｳｫｰﾙが、ｿｰｽのﾙｰﾀｰへのﾌﾟﾗｲﾍﾞｰﾄなﾄﾝﾈﾙを介しての送信のために、WAN ｲﾝﾀｰﾌｪｰｽを通じて目的地のﾙｰﾀｰへと送信されるｱｯﾌﾟｽﾄﾘｰﾑのWANﾊﾟｹｯﾄのﾍﾟｲﾛｰﾄﾞを、ｿｰｽのﾌｧｲﾔｰｳｫｰﾙが利用するものと同じ暗号化の方法を利用し、ﾕｰｻﾞｰが設定できる一つまたは複数の鍵でｿｰｽのﾌｧｲﾔｰｳｫｰﾙの回線が利用するものと同じものを利用して暗号化する機能を果たし、ﾌｧｲﾔｰｳｫｰﾙは、終端の地点の参加しているISX/ISP ﾌﾟﾛﾊﾞｲﾀﾞｰから到着する、ｿｰｽのﾙｰﾀｰから入り来るﾊﾟｹｯﾄ全てを、ｿｰｽのﾌｧｲﾔｰｳｫｰﾙが利用するものと同じ暗号化ﾌﾟﾛﾄｺｰﾙを利用し、またﾕｰｻﾞｰが設定できる鍵でｿｰｽのﾌｧｲﾔｰｳｫｰﾙ回線が利用するものと同じものを利用して解読するためのもので、および解読されたﾊﾟｹｯﾄを二つ目の装置へと送信するためのﾌｧｲﾔｰｳｫｰﾙである、目的地のﾌｧｲﾔｰｳｫｰﾙの一つの回線と、から成る、ﾜｲﾄﾞｴﾘｱﾈｯﾄﾜｰｸ。

表 2.23 主要企業、大学、公的研究機関等以外の技術要素別課題対応特許一覧（10/10）

技術要素III	課題I	解決手段II 解決手段III 解決手段IV	特許番号 （経過情報） 出願日 主 IPC 出願人 [被引用回数]	発明の名称 概要
トンネリング技術	中継するデータの機密性向上	ｱﾄﾞﾚｽﾃﾞｰﾀ形式の改良 ｱﾄﾞﾚｽの変換 ﾊﾟｯｸｱﾄﾞﾚｽ	特許 3343064 96.10.25 H04L12/56 ｺﾝﾊﾟｯｸ・ｺﾝﾋﾟｭｰﾀ(米国)	**ﾌﾚｰﾑを捕獲、ｶﾌﾟｾﾙ化及び暗号化するための擬似ﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀ** 仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸを備えた擬似ﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀにおいて、上記仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸを経て送信するためにﾛｰｶﾙ通信ﾌﾟﾛﾄｺﾙｽﾀｯｸからﾊﾟｹｯﾄを捕獲するｲﾝﾀｰﾌｪｲｽを備え、このｲﾝﾀｰﾌｪｲｽは、上記ﾛｰｶﾙ通信ﾌﾟﾛﾄｺﾙｽﾀｯｸには、上記仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸに接続されたﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀのためのﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀﾃﾞﾊﾞｲｽﾄﾞﾗｲﾊﾞとして見え、上記仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸを経て送信するために上記ﾛｰｶﾙ通信ﾌﾟﾛﾄｺﾙｽﾀｯｸからﾊﾟｹｯﾄを捕獲する上記ｲﾝﾀｰﾌｪｲｽにより捕獲された第 1 要求ﾊﾟｹｯﾄに応答して第 1 応答ﾊﾟｹｯﾄを与える第 1 ｻｰﾊﾞｴﾐｭﾚｰﾀを備え、上記第 1 要求ﾊﾟｹｯﾄは、上記擬似ﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀのためのﾈｯﾄﾜｰｸﾚｲﾔｱﾄﾞﾚｽを要求し、そして上記第 1 応答ﾊﾟｹｯﾄは、上記擬似ﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀのためのﾈｯﾄﾜｰｸﾚｲﾔｱﾄﾞﾚｽを指示し、更に、上記仮想ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸを経て送信するために上記ﾛｰｶﾙ通信ﾌﾟﾛﾄｺﾙｽﾀｯｸからﾊﾟｹｯﾄを捕獲する上記ｲﾝﾀｰﾌｪｲｽにより捕獲された第 2 要求ﾊﾟｹｯﾄに応答して第 2 応答ﾊﾟｹｯﾄを与える第 2 ｻｰﾊﾞｴﾐｭﾚｰﾀを備え、上記第 2 要求ﾊﾟｹｯﾄは、ﾘﾓｰﾄｻｰﾊﾞﾉｰﾄﾞに位置された第 2 擬似ﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀのﾈｯﾄﾜｰｸﾚｲﾔｱﾄﾞﾚｽに対応するﾌｨｼﾞｶﾙｱﾄﾞﾚｽを要求し、そして上記第 2 応答ﾊﾟｹｯﾄは、所定の指定済のﾌｨｼﾞｶﾙｱﾄﾞﾚｽを指示することを特徴とする擬似ﾈｯﾄﾜｰｸｱﾀﾞﾌﾟﾀ。

３．主要企業の技術開発拠点

3.1 不正アクセス侵入検知防御技術の技術開発拠点

特許流通
支援チャート

３．主要企業の技術開発拠点

不正アクセス侵入検知防御技術の技術開発拠点は、関東地方に集中が顕著である。特に東京都と神奈川県への集中が、顕著である。

3.1 不正アクセス侵入検知防御技術の技術開発拠点

図3.1に不正アクセス侵入検知防御技術の主要企業21社の技術開発拠点を示し、表3.1には技術開発拠点の住所一覧を示す。この図や表は、主要企業が保有している特許の公報から発明者の住所を集計したものである。

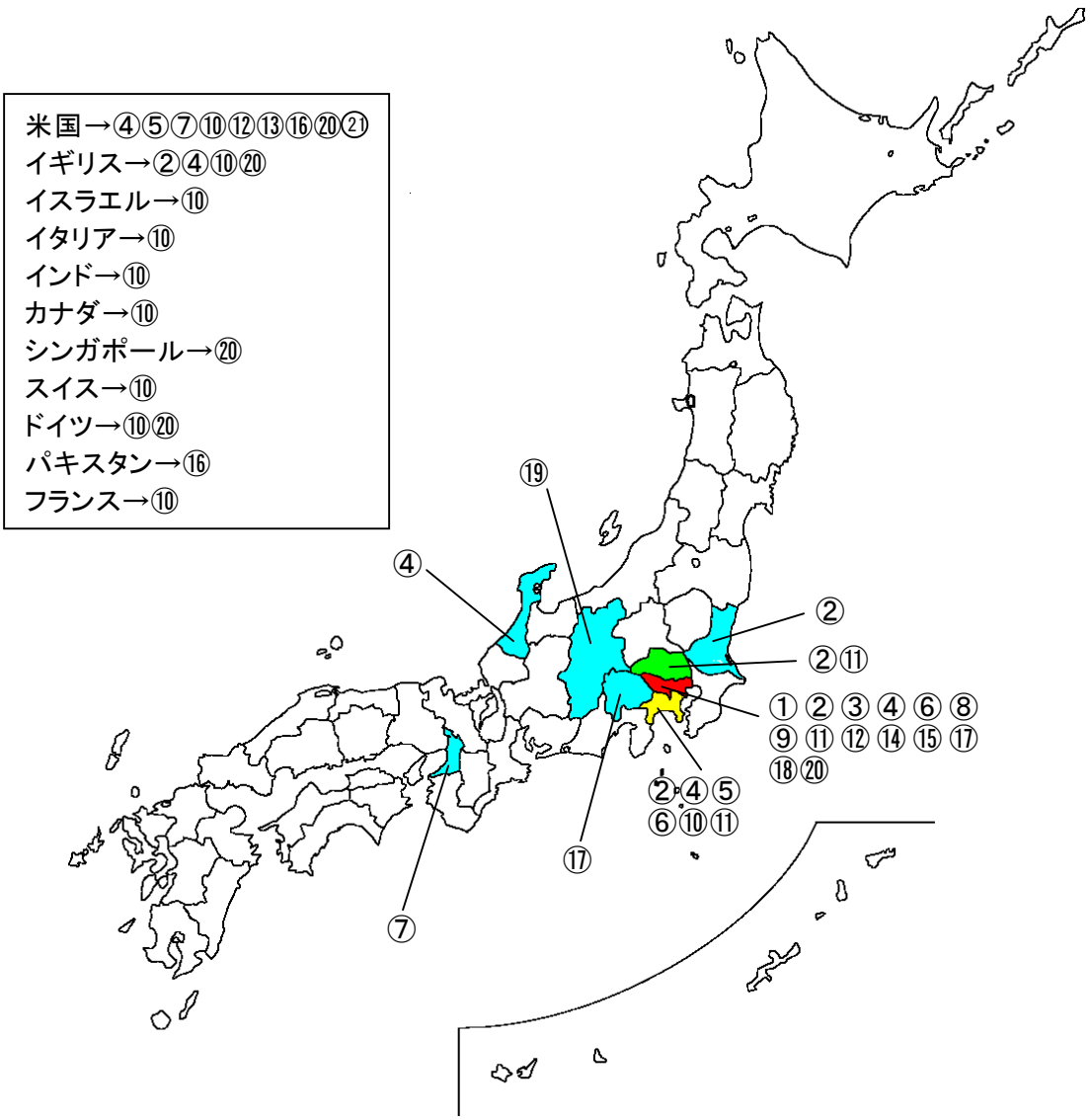
集計の結果は、東京都が14社20拠点、神奈川県が６社13拠点、埼玉県が２社２拠点、茨城県が１社３拠点、長野県が１社２拠点、山梨県が１社１拠点、石川県が１社１拠点、大阪府が１社１拠点である。

不正アクセス侵入検知防御技術の主要企業21社の開発拠点は、関東地方に集中している。特に東京都と神奈川県への集中が顕著である。

不正アクセス侵入検知防御技術の主要企業21社のうち、外国企業は、IBM(米国)、マイクロソフト(米国)、サン・マイクロシステムズ(米国)、ヒューレット・パッカード(米国)とルーセント テクノロジーズ(米国)の５社である。IBMは米国国内に10拠点、海外にイギリス、イスラエル、イタリア、インド、カナダ、スイス、ドイツ、フランスと日本に開発拠点を持っている。マイクロソフトは米国のワシントン州が開発拠点である。サン・マイクロシステムズは、米国国内に２拠点、パキスタンに１拠点ある。ヒューレット・パッカードは、米国国内に10拠点、海外にイギリス、シンガポール、ドイツと日本にある。ルーセント テクノロジーズは、米国国内に４拠点ある。

日本企業で海外に開発拠点を持つ会社は５社あり、それは米国に３社、イギリスに２社である。

図 3.1 不正アクセス侵入検知防御技術の主要企業の技術開発拠点



1993 年 1 月～2003 年 12 月の出願

表3.1 不正アクセス侵入検知防御技術の主要企業の技術開発拠点住所一覧(1/2)

No.	企業名	住所	
		都道府県または国名	所在地・事業所名
①	日本電信電話	東京都	新宿区西新宿 3 丁目 19 番 2 号 日本電信電話株式会社内
			千代田区大手町 2 丁目 3 番 1 号 日本電信電話株式会社内
			千代田区内幸町 1 丁目 1 番 6 号 日本電信電話株式会社内
②	日立製作所	茨城県	ひたちなか市稲田 1410 番地 株式会社日立製作所デジタルメディア事業部内
			日立市幸町 3 丁目 1 番 1 号 株式会社日立製作所火力・水力事業部内
			日立市大みか町 7 丁目 2 番 1 号 株式会社日立製作所内
		埼玉県	比企郡鳩山町赤沼 2520 番地 株式会社日立製作所基礎研究所内
		神奈川県	横浜市戸塚区吉田町 292 番地 株式会社日立製作所内
			横浜市戸塚区戸塚町 5030 番地 株式会社日立製作所内
			横浜市都筑区加賀原 2 丁目 2 番 株式会社日立製作所内
			海老名市下今泉 810 番地 株式会社日立製作所内
			小田原市国府津 2820 番地株式会社日立製作所ストレージシステム事業部内
			秦野市堀山下 1 番地 株式会社日立製作所内
			川崎市幸区鹿島田 890 番地 株式会社日立製作所内
			川崎市麻生区王禅寺 1099 株式会社日立製作所内
		東京都	江東区新砂 1 丁目 6 番 27 号 株式会社日立製作所内
			国分寺市東恋ヶ窪 1 丁目 280 番地 株式会社日立製作所中央研究所内
		イギリス	ケンブリッジ
③	日本電気	東京都	港区芝 5 丁目 7 番 1 号 日本電気株式会社内
④	東芝	東京都	港区芝浦 1 丁目 1 番 1 号 株式会社東芝本社事務所内
			青梅市末広町 2 丁目 9 番地 株式会社東芝青梅工場内
			日野市旭が丘 3 丁目 1 番地 1 株式会社東芝日野工場内
			府中市東芝町 1 番地 株式会社東芝府中工場内
		神奈川県	横浜市磯子区新杉田町 8 番地 株式会社東芝横浜事業所内
			川崎市幸区小向東芝町 1 番地 株式会社東芝小向工場内
			川崎市川崎区日進町 7 番地 1 東芝情報システム株式会社内
		石川県	金沢市平和町 2 丁目 28 番 60 号 B39-12
		アメリカ合衆国	カリフォルニア州アーバイン
			ニュージャージー州コンベント
		イギリス	ブリストル
⑤	富士通	神奈川県	横浜市港北区新横浜 3 丁目 9 番 18 号富士通内
			川崎市中原区上小田中 1015 番地 富士通株式会社内
		アメリカ合衆国	メリーランド州シルヴァースプリング
⑥	三菱電機	東京都	千代田区丸の内 2 丁目 2 番 3 号 三菱電機株式会社内
		神奈川県	鎌倉市上町屋 325 番地 三菱電機株式会社情報システム製作所内
			鎌倉市大船 5 丁目 1 番 1 号 三菱電機株式会社通信システム研究所内
⑦	松下電器産業	大阪府	門真市大字門真 1006 番地 松下電器産業株式会社内
		アメリカ合衆国	ニュージャージー州サマーセット
⑧	ソニー	東京都	品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内
⑨	キヤノン	東京都	大田区下丸子 3 丁目 30 番 2 号 キヤノン株式会社内
⑩	インターナショナル・ビジネス・マシーンズ (IBM,米国)	アメリカ合衆国	ニューヨーク州
			インディアナ州
			カリフォルニア州
			コネティカット州
			コロラド州
			テキサス州
			ニューヨーク州
			ノースカロライナ州
			フロリダ州
			ペンシルバニア州
			ミネソタ州
			フロリダ州
		イギリス	オックスフォード
		イスラエル	テルアビブ
		イタリア	ローマ
		インド	カルナータ
		カナダ	オンタリオ州トロント
		スイス	ウルドルフ
			チューリッヒ
		ドイツ	ディー
			フランクフルト
		フランス	ニース
		神奈川県	大和市下鶴間 1623 番地 14 日本アイ・ビー・エム株式会社 内

1993年1月～2003年12月の出願

表3.1 不正アクセス侵入検知防御技術の主要企業の技術開発拠点住所一覧(2/2)

No.	企業名	住所	
		都道府県または国名	所在地・事業所名
⑪	富士ゼロックス	東京都	港区赤坂 2 丁目 17 番 22 号 富士ゼロックス株式会社内
		神奈川県	海老名市本郷 2274 番地 富士ゼロックス株式会社内
			川崎市高津区坂戸 3 丁目 2 番 1 号 ＫＳＰ Ｒ＆Ｄ富士ゼロックス株式会社内
			足柄上郡中井町境 430 グリーンテクなかい 富士ゼロックス株式会社内
		埼玉県	岩槻市府内 3 丁目 7 番 1 号 富士ゼロックス株式会社岩槻事業所内
⑫	リコー	東京都	大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
		アメリカ合衆国	カリフォルニア州
⑬	マイクロソフト(米国)	アメリカ合衆国	ワシントン州
⑭	エヌ・ティ・ティ・データ	東京都	江東区豊洲 3 丁目 3 番 3 号 株式会社エヌ ティ ティ データ内
⑮	沖電気工業	東京都	港区虎ノ門 1 丁目 7 番 12 号 沖電気工業株式会社内
⑯	サン・マイクロシステムズ(米国)	アメリカ合衆国	カリフォルニア州
			マサチューセッツ州
		パキスタン	イスラマバード
⑰	横河電気	東京都	武蔵野市中町 2 丁目 9 番 32 号 横河電機株式会社内
		山梨県	甲府市高室町 155 番地　横河電機株式会社甲府事業所内
⑱	エヌ・ティ・ティ・ドコモ	東京都	千代田区永田町 2 丁目 11 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内
⑲	セイコーエプソン	長野県	諏訪市大和 3 丁目 3 番 5 号 セイコーエプソン株式会社内
			松本市芳川村井町 1059 番地 株式会社エプソンソフト開発センター内
⑳	ヒューレット・パッカード(米国)	アメリカ合衆国	コロラド州
			アイダホ州
			オレゴン州
			カリフォルニア州
			テキサス州
			ニュージャージー州
			ニューハンプシャー州
			ニューヨーク州
			ノースカロライナ州
			バーモント州
		イギリス	ブリストル
			ロンドン
		シンガポール	アッパーブキット
			ネプチューンコート
		ドイツ	ナフリンゲン
		東京都	杉並区高井戸東 3 丁目 29 番 21 号　日本ヒューレット・パッカード株式会社内
㉑	ルーセント テクノロジーズ(米国)	アメリカ合衆国	ニュージャージー州
			イリノイス州
			テキサス州
			ニューヨーク州

1993年1月～2003年12月の出願

資料

1．ライセンス提供の用意のある特許

資料１．ライセンス提供の用意のある特許

不正アクセス侵入検知防御技術に関連する技術で、ライセンス提供の用意のある特許を、特許流通データベース（独立行政法人工業所有権情報・研修館のホームページ http://www.ncipi.go.jp/を参照）による検索結果を以下に示す。

なお、検索キーワード「不正アクセス」、「侵入検知」、「侵入防御」、「ファイアウォール」でヒットしたものを、選択した。

ライセンス提供の用意のある特許リスト

順番号	ライセンス番号	特許番号 出願日 特許権利者	発明の名称
1	L20030000367	特許3262689 95.05.19 富士通	遠隔操作システム

特許流通支援チャート　電気 31

不正アクセス侵入検知防御技術

2006 年 3 月 31 日発行

企画・発行　　独立行政法人 工業所有権情報・研修館©
〒100-0013　東京都千代田区霞が関 3-4-3
電話 03-3580-6949（直通）

編　　集　　社団法人 発明協会
〒105-0001　東京都港区虎ノ門 2-9-14
電話 03-3502-5440（直通）