(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-104509
(P2007-104509A)
(43)公開日　平成19年4月19日(2007.4.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5B089
H04L 12/56	(2006.01)	H04L	12/56	B	5K030
G06F 13/00	(2006.01)	G06F	13/00	351Z	

審査請求 未請求　請求項の数 6　ＯＬ　（全 13 頁）

(21)出願番号　特願2005-294216 (P2005-294216)
(22)出願日　平成17年10月6日 (2005.10.6)

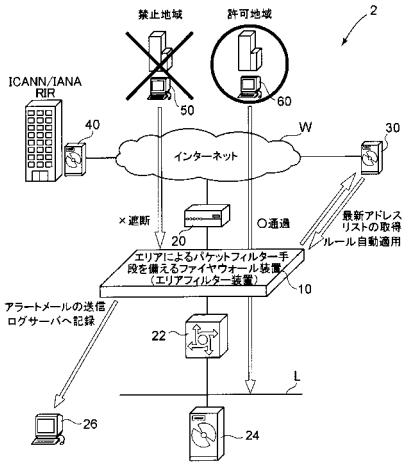
（特許庁注：以下のものは登録商標）
１．Ｌｉｎｕｘ

(71)出願人　305047214
日本エフ・セキュア株式会社
神奈川県横浜市西区高島２－１９－１２
スカイビル２３Ｆ
(74)代理人　100080230
弁理士　石原　詔二
(72)発明者　迎　博
神奈川県横浜市神奈川区金港町６－６　横浜みなと第一生命ビル８Ｆ　日本エフ・セキュア株式会社内

Ｆターム(参考)　5B089 GA11 GA21 GA31 HA06 HA10
HB02 KA17 KB13 KC54
5K030 GA15 HA08 HD03 HD06 KA05
KX24 LC15 MD10

(54)【発明の名称】エリアによるパケットフィルタリング方法及びファイヤウォール装置並びにファイヤウォールシステム

(57)【要約】
【課題】
不正アクセス等の目的の有無やパケットの内容とは無関係に送信元の端末が所属する国乃至地域の単位でパケットの通過の許可又は拒否を行い得るようにし、Ｗｅｂサーバ等の運営者が意図しない不必要な通信トラフィックを画一的に制御でき堅牢で確実な利便性の高いエリアによるパケットフィルタリング方法及びファイヤウォール装置並びにファイヤウォールシステムを提供する。
【解決手段】
グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールを設定し、該フィルタリングルールと受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの受容又は破棄を行うようにした。
【選択図】　図１



【特許請求の範囲】
【請求項１】
グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールを設定し、該フィルタリングルールと受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの受容又は廃棄を行うことを特徴とするエリアによるパケットフィルタリング方法。
【請求項２】
前記グローバルＩＰアドレスの割り当て地域情報は、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）によって割り当てられたグローバルＩＰアドレスの地域情報であることを特徴とする請求項１記載のエリアによるパケットフィルタリング方法。
【請求項３】
グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールを設定し、該フィルタリングルールと受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの受容又は廃棄を行うようにしたエリアによるパケットフィルター手段を備えることを特徴とするファイヤウォール装置。
【請求項４】
前記エリアによるパケットフィルター手段は、グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールが設定されたフィルタリングルール設定部と、該フィルタリングルール設定部から該フィルタリングルールを読み出して、該フィルタリングルールと前記受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの受容又は廃棄を行うように構成された地域情報に基づくフィルタリング処理部とを備えることを特徴とする請求項３記載のファイヤウォール装置。
【請求項５】
前記グローバルＩＰアドレスの割り当て地域情報は、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）によって割り当てられたグローバルＩＰアドレスの地域情報であることを特徴とする請求項３又は４記載のファイヤウォール装置。
【請求項６】
請求項３～５のいずれか１項記載のファイヤウォール装置を含むファイヤウォールシステムであって、割り当て地域情報を含むグローバルＩＰアドレスのアドレス範囲リストをアドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）のサイトから取得し、該アドレス範囲リストを前記ファイヤウォール装置におけるエリアによるパケットフィルター手段に対応した所定のフォーマットに整形して日付毎に保持すると共に、定期的又は不定期に任意で、該整形後のアドレス範囲リストを前記ファイヤウォール装置にインターネットを介して配信し、前記フィルタリングルールの更新を行わせしめる配信サーバを備えることを特徴とするファイヤウォールシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、フィルタリングルールに従ってパケットの選択的通過処理（フィルタリング）を行うパケットフィルタリング方法及びファイヤウォール装置並びにファイヤウォールシステムに関する。
【背景技術】
【０００２】
従来より、世界的なＴＣＰ／ＩＰ（Transmission Control Protocol／Internet Protocol）ネットワークであるインターネットにおけるネットワークセキュリティを確保するための技術として、ファイアウォール（防火壁）の技術が知られている。ファイアウォール

は、インターネット等の外部ネットワーク（ＷＡＮ：Wide Area Network）と、企業等の内部ネットワーク（ＬＡＮ：Local Area Network）やＷｅｂサーバ等の公開サーバ用のセグメントである非武装地帯（ＤＭＺ：DeMilitarized Zone）との間に配置され、予め決められた条件や基準に基づいて、流入する通信トラフィックを検査してデータ通信を許可するか否かを制御することにより、外部ネットワークから内部ネットワークへの不正アクセス等を阻止するための技術である。ファイヤウォールには、ファイヤウォール専用装置として提供される場合の他、異なるネットワーク間を相互接続するルータ等の一部機能として提供される場合、各端末にインストールするソフトウェアプログラムとして提供される場合等がある。

【０００３】

このようなファイアウォールには種々の方式のものがあるが、そのうち代表的な方式の一つにパケットフィルタリング（パケットの選択的通過処理）型のファイアウォールがある。インターネットは、ネットワーク層（ＯＳＩ基本参照モデルの３層）にＩＰ（Internet Protocol）を使用し、トランスポート層（ＯＳＩ基本参照モデルの４層）にＴＣＰ／ＵＤＰ（Transport Control Protocol／User Datagram Protocol）を使用したＴＣＰ／ＩＰネットワークであり、通信データを各層毎に所定バイト数にまとめた単位のパケットとして処理されており、パケットフィルタリング型のファイアウォールでは、このパケット毎にその通過を許可するか否かの制御を行うものであり、このような制御は予め定められたフィルタリングルールに従って行われ、一般的なフィルタリングルールでは、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコルの種類等によってフィルタリングの対象にするパケットが特定され、当該パケットに対し通過の許可又は拒否等の判定がされ、当該パケットの通過の受容又は廃棄が行われるようにされている（例えば、特許文献１～５参照）。その他、パケットフィルタリング型のファイアウォールでは阻止できない上位層への攻撃等や不正アクセス等を検出するための侵入検知システム（ＩＤＳ：Intrusion Detection System）や不正侵入検知・防御システム（ＩＤＰ：Intrusion Detection and Prevention）、不正侵入防止システム（ＩＰＳ：Intrusion Prevention System）等も知られている（例えば、特許文献６等参照）。

【０００４】

しかしながら、不正アクセス等の原因の一つともなるＯＳ（Operatting System）やアプリケーションソフトウェアのセキュリティホール（脆弱性）は日々新たに発見され、新種のコンピュータウィルス、スパイウェアによる情報漏洩、Ｗｅｂサイトの改竄、サービス妨害（ＤｏＤ）攻撃、大量のスパムメール、クラッキングツールの蔓延、自サイトが他サイトへの不正アクセスの踏み台とされる等の被害は後を絶たず、ファイヤウォールやＩＤＳ等による対応は、後手からの対処療法的な様相を呈しているのが現状である。インターネットは全世界的ネットワークである上に匿名性も高いため、不正アクセス等の被害があってもその追跡調査は困難である場合が多い。近年では通信インフラが整備され、ブロードバンドや常時接続の環境が普及するに伴い、このような問題は増大傾向にある。特に中小企業や個人等がＷｅｂサーバやＦＴＰサーバ、メールサーバ等をインターネット上に公開することも比較的容易となったが、中小企業や個人等ではネットワークセキュリティに対する認識が希薄であったり、システム管理者のスキルが未熟であったりすることが原因で不正アクセス等に対し充分な対応策が講じられていないケースも多い。

【０００５】

他方、不正アクセス等の送信元は我国国内よりも国外の諸外国、特に特定の数カ国である場合が大半であり、また、我国国内の中小企業や個人等がＷｅｂサーバ等をインターネット上に公開する場合は我国国内からのみアクセス可能であれば必要充分であることも多いという現状もある。

【特許文献１】特開平９－２０５４５７号公報
【特許文献２】特開平９－２７０８１３号公報
【特許文献３】特開１０－１３３８７７号公報
【特許文献４】特開２０００－７８１９３号公報

【特許文献５】特開２００３－２７３９３６号公報
【特許文献６】特開２００４－３０２８６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、上記問題点に鑑みてなされたものであり、不正アクセス等の目的の有無やパケットの内容とは無関係に送信元の端末が所属する国乃至地域の単位でパケットの通過の許可又は拒否を行い得るようにし、Ｗｅｂサーバ等の運営者が意図しない不必要な通信トラフィックを画一的に制御でき堅牢で確実な利便性の高いエリアによるパケットフィルタリング方法及びファイヤウォール装置並びにファイヤウォールシステムを提供することを目的とする。
【課題を解決するための手段】
【０００７】
上記課題を解決するために、本発明のエリアによるパケットフィルタリング方法は、グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールを設定し、該フィルタリングルールと受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの通過の受容又は廃棄を行うことを特徴とする。なお、本明細書においては、上記本発明のエリアによるパケットフィルタリング方法を単に「エリアフィルタリング」という場合がある。
【０００８】
上記本発明方法におけるグローバルＩＰアドレスの割り当て地域情報は、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）によって割り当てられたグローバルＩＰアドレスの地域情報であることが好適である。
【０００９】
また、本発明のファイヤウォール装置は、グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールを設定し、該フィルタリングルールと受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの通過の受容又は廃棄を行うようにしたエリアによるパケットフィルター手段を備えることを特徴とする。なお、本明細書においては、上記本発明のファイヤウォール装置におけるエリアによるパケットフィルター手段のことを単に「エリアフィルター手段」と、また、この「エリアフィルター手段」を備えるファイヤウォール装置、即ち上記本発明のファイヤウォール装置のことを単に「エリアフィルター装置」という場合がある。
【００１０】
前記エリアによるパケットフィルター手段は、グローバルＩＰアドレスの割り当て地域情報に基づいてフィルタリングルールが設定されたフィルタリングルール設定部と、該フィルタリングルール設定部から該フィルタリングルールを読み出して、該フィルタリングルールと前記受信パケットにおける送信元のグローバルＩＰアドレスとを照合して、該受信パケットの通過の許可又は拒否を判定し、該受信パケットの通過を受容又は廃棄するように構成された地域情報に基づくフィルタリング処理部とを備えることが好ましい。
【００１１】
上記本発明装置におけるグローバルＩＰアドレスの割り当て地域情報は、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）によって割り当てられたグローバルＩＰアドレスの地域情報であることが好適である。
【００１２】
更に、本発明のファイヤウォールシステムは、前記ファイヤウォール装置を含むファイヤウォールシステムであって、割り当て地域情報を含むグローバルＩＰアドレスのアドレス範囲リストを地域アドレス管理機関（ＲＩＲ）のサイトから取得し、該アドレス範囲リストを前記ファイヤウォール装置におけるエリアによるパケットフィルター手段に対応した所定のフォーマットに整形して日付毎に保持すると共に、定期的又は不定期に任意的で

、該整形後のアドレス範囲リストを前記ファイヤウォール装置にインターネットを介して配信し、前記フィルタリングルールの更新を行わせしめる配信サーバを備えることを特徴とする。なお、本明細書においては、上記本発明のエリアによるパケットフィルター手段を備えるファイヤウォール装置（即ちエリアフィルター装置）を含むファイヤウォールシステムを単に「エリアフィルターシステム」という場合がある。

【発明の効果】

【００１３】

本発明によれば、不正アクセス等の目的の有無やパケットの内容とは無関係に、送信元のグローバルＩＰアドレスからその端末が所属する国乃至地域の単位でパケットの通過の許可又は拒否が行われるので、Ｗｅｂサーバ等の運営者が意図しない不必要な通信トラフィックを画一的に制御でき堅牢で確実な利便性の高いエリアによるパケットフィルタリング方法及びファイヤウォール装置並びにファイヤウォールシステムを提供することができるという大きな効果を奏する。

【発明を実施するための最良の形態】

【００１４】

以下に本発明の実施の形態を添付図面に基づいて説明するが、図示例は例示的に示されたもので、本発明の技術思想から逸脱しない限り種々の変形が可能なことはいうまでもない。

【００１５】

図１は、本発明のファイヤウォールシステム（エリアフィルターシステム）の全体的な機器構成の一例を概念的に示す説明図である。図２は、本発明のファイヤウォール装置）（エリアフィルター装置）のハードウェア構成の一例を示すブロック図である。図３は、本発明のエリアによるパケットフィルタリング方法（ホワイトリスト型）の一例を示すフローチャートである。図４は、本発明のエリアによるパケットフィルタリング方法（ブラックリスト型）の一例を示すフローチャートである。図５は、本発明システムにおける配信サーバの最新アドレス情報の取得動作の一例を示すフローチャートである。図６は、本発明システムにおけるファイヤウォール装置のフィルタリングルールの更新動作の一例を示すフローチャートである。図中、符号２は本発明のファイヤウォールシステム、符号１０は本発明のファイヤウォール装置、符号Ｗはインターネット、符号ＬはＬＡＮ、符号Ｐはパケットである。

【００１６】

なお、以下の説明において、アドレスやＩＰアドレスという用語は特に明示のない限り、グローバルＩＰアドレスを意味しており、プライベートＩＰアドレスやドメイン名、ＭＡＣアドレス、メールアドレス、地理的住所等の意味ではない。また、パケットとしては原則として受信したＩＰパケットである場合を説明するが、送信元のグローバルＩＰアドレスをヘッダー情報に有する受信パケットであればよい。

【００１７】

まず、本発明でいう「グローバルＩＰアドレスの割り当て地域情報」という概念について説明する。グローバルＩＰアドレスの割り当て地域情報とは、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）によって割り当てられたグローバルＩＰアドレスの地域情報のことである。

【００１８】

即ち、現在、世界的なＴＣＰ／ＩＰ（Transmission Control Protocol／Internet Protocol）ネットワークであるインターネットにおいて、グローバルＩＰアドレスは、世界的にアドレス管理等を行うアドレス管理機関であるＩＣＡＮＮ／ＩＡＮＡ（Internet Corporation for Assigned Names and Numbers：http://www.icann.org／Internet Assigned Numbers Authority：http://www.iana.org）がアドレス範囲（アドレスレンジやアドレスブロックともいう）を地域アドレス管理機関（ＲＩＲ：Regional Internet Registry）に割り振り、地域アドレス管理機関（ＲＩＲ）では割り当てられたアドレス範囲を更に分割して、直接にＩＳＰ（Internet Services Provider）等のＬＩＲ（Local Internet Regis

try：ＩＰアドレス管理指定事業者）に割り当てたり、国別アドレス管理機関（ＮＩＲ：National Internet Registry）通じてＩＳＰ（Internet Services Provider）等に割り当てたりしたものをエンドユーザが利用する仕組みとなっている。

【００１９】

地域アドレス管理機関（ＲＩＲ）には、現在の処、北米地域のＡＲＩＮ（http://www.arin.net）、欧州地域のＲＩＰＥ ＮＣＣ（http://www.ripe.net）、アジア太平洋地域のＡＰＮＩＣ（http://www.apnic.net）、南米カリブ海地域のＬＡＣＮＩＣ（http://lacnic.net）、アフリカ地域のＡｆｒｉＮＩＣ（http://www.afrinic.net）がある。また、国別アドレス管理機関（ＮＩＲ）には、例えばＡＰＮＩＣの管理下にあるアジア太平洋地域であれば、日本のＪＰＮＩＣ、中国のＣＮＮＩＣ、韓国のＫＲＮＩＣ、台湾のＴＷＮＩＣ、ベトナムのＶＮＮＩＣ、インドネシアのＡＰＪＩＩがある。

【００２０】

地域アドレス管理機関（ＲＩＲ）では、ある団体（ＬＩＲ又はＮＩＲ）に割り当てたアドレス範囲について、その管轄ＲＩＲ名、所属するエリア（国名又は地域名）、開始ＩＰアドレスとその個数、割当開始日、割当方法（再分配の可否）等を管理しており、その割り当て情報をアドレス情報ファイルとして各ＲＩＲのＷｅｂサイト又はＦＴＰサイト上で公開している。当該情報はＲＩＲの上位機関であるＩＣＡＮＮ／ＩＡＮＡからも入手可能である。このアドレス情報ファイルのフォーマットは統一されており、例えば無作為に一例を挙げると、

apnic ｜JP｜ipv4｜210.196.xxx.xxx｜ 65536｜19990609｜allocated
arin ｜US｜ipv4｜209.198.xxx.xxx｜131072｜19980209｜allocated
ripencc｜DE｜ipv4｜217.199.xxx.xxx｜ 32768｜20010507｜allocated

といった如くのものであり、各欄の意味する処は、

管轄RIR｜エリア｜ip種別｜開始IPアドレス｜アドレス数｜割当開始日｜割当方法

となっている。

【００２１】

管轄ＲＩＲとは、前述したＡＲＩＮ、ＲＩＰＥ ＮＣＣ、ＡＰＮＩＣ、ＬＡＣＮＩＣ、ＡｆｒｉＮＩＣの中のいずれの機関が管轄しているかを表している。エリアとは、ＩＳＯ３１６６－１規定によるもので、国乃至地域的に区別可能な領域につき、夫々アルファベット２文字のユニークな略語（例えば日本国はＪＰ）で表記したものである。ｉｐ種別とは、ＩＰのバージョン、即ちＩＰｖ４かＩＰｖ６かを表している。開始ＩＰアドレスとは、割り当てられたＩＰアドレス範囲の最初のＩＰアドレスを表している。アドレス数とは、割り当てられた指定可能なホストのＩＰアドレスの数を表している。このアドレス数はＣＩＤＲ（Classless InterDomain Routing）等のネットマスク表記と相関関係にあり、例えばアドレス数「６５５３６」はＣＩＤＲ表記なら「／１６」、ネットマスク（１０進数）表記なら「２５５．２５５．０．０」（クラスＢネットワーク）であり、アドレス数「１３１０７２」はＣＩＤＲ表記なら「／１５」、ネットマスク（１０進数）表記なら「２５５．２５４．０．０」であり、アドレス数「３２７６８」はＣＩＤＲ表記なら「／１７」、ネットマスク（１０進数）表記なら「２５５．２５５．１２８．０」である。割当開始日は、そのアドレスブロックが割り当てられた開始日である。割当方法には、allocatedとassignedがあり、再配分の可否に違いがある。

【００２２】

従って、このようなグローバルＩＰアドレスの割り当て情報から、ある特定のグローバルＩＰアドレスがどこの国乃至地域（エリア）に割り当てられているアドレスであるかを判別できるので、あるパケットのヘッダー情報に含まれる送信元アドレスから当該パケットがどこの国乃至地域（エリア）を発信源とするものであるかを判定できるのである。

【００２３】

図１は、本発明のファイヤウォールシステム（エリアフィルターシステム）２の全体的な機器構成の一例を概念的に示す説明図である。本発明システム２は、本発明のファイヤウォール装置（エリヤフィルター装置）１０を含むシステムであり、本発明装置１０の上

流側にルータ２０、下流側にスイッチ２２が配置され、これらを介してＷｅｂサーバ等の公開サーバ２４がインターネットWに接続されている。なお、図示例では内部ネットワークＬに公開サーバ２４が配置されている場合を示したが、公開サーバ用のセグメントとしての非武装地帯（ＤＭＺ）に配置されるようにしてもよい。

【００２４】

本発明システム２は配信サーバ３０を含み、インターネットWを介して、本発明装置１０と通信可能であると共にアドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）のサーバ４０とも通信可能とされている。配信サーバ３０は、割り当て地域情報を含むグローバルＩＰアドレスのアドレス範囲リストをアドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）のサイトから取得し、該アドレス範囲リストを前記ファイヤウォール装置におけるエリアによるパケットフィルター手段に対応した所定のフォーマットに整形して日付毎に保持すると共に、定期的又は不定期に任意で、該整形後のアドレス範囲リストを前記ファイヤウォール装置にインターネットを介して配信し、本発明装置１０におけるフィルタリングルールの更新を行うためのものである。また、本発明装置１０からのアラートメールやログを受け取るための管理端末２６を内部ネットワークＬ又はインターネットWを介して適宜設けるようにしてもよい。

【００２５】

ルータ２０は、公知のいわゆるセキュリティルータであり、インターネットWと内部ネットワークＬとの境界に設けられている。必要に応じて、ＮＡＴ（Network Address Translator）やＩＰマスカレード等を利用する。また、公開サーバ２４の種類（Ｗｅｂサーバかｆｔｐサーバかメールサーバか等々）に応じて各ポートの開閉を行い、一般的なパケットフィルタリングを行うように設定される。スイッチ２２は、公知のいわゆるレイヤ２スイッチやレイヤ３スイッチ或いはレイヤ４スイッチであり、必要に応じて設ければよく、特に限定されない。

【００２６】

図２は、本発明のファイヤウォール装置（エリヤフィルター装置）１０のハードウェア構成の一例を示すブロック図である。本発明装置１０は、その筐体内に、ＣＰＵ（Central Processing Unit）１１とＲＡＭ（Random Access Memory）１２とＲＯＭ（Read Only Memory）１３と入力ネットワークインターフェイス１４と出力ネットワークインターフェイス１６と補助記憶装置１８とを備え、夫々がバス１７に接続されている。なお、必要に応じて制御用のＲＳ２３２ＣポートやＵＳＢポート等を設けてもよい。

【００２７】

ＣＰＵ１１は、演算・制御を行う中央処理装置であり、その種類等に特段の制限はないが、本発明装置１０に求められる性能等に応じて適宜選択される。ＲＡＭ１２は、メインメモリ（主記憶装置）であり、メモリ容量等は本発明装置１０に求められる性能等に応じて適宜選択される。ＲＯＭ１３はのファームウェア等を記憶しておくための読み出し専用の記憶装置である。

【００２８】

入力ネットワークインターフェイス１４は、ＬＡＮケーブル等の伝送路に接続されてパケットＰが入力されるパケット入力部である。図示例では、伝送路を介してルータ２０に接続されており、ルータ２０を通過したパケットＰが入力されるようになっている。また、出力ネットワークインターフェイス１６は、ＬＡＮケーブル等の伝送路に接続されてパケットＰが出力されるパケット出力部である。図示例では、伝送路を介してスイッチ２２に接続されており、本発明装置１０によってエリアフィルタリングされたパケットＰがスイッチ２２に向けて出力されるようになっている。なお、入力ネットワークインターフェイス１４及び出力ネットワークインターフェイス１６は有線でもよいし無線でもよい。

【００２９】

補助記憶装置１８としてはハードディスクやフラッシュメモリ等を利用できる。補助記憶装置１８には、ＯＳ１００と、その管理下で動作するソフトウェアプログラムとしてのエリアによるパケットフィルター手段（エリヤフィルター手段）１１０が設けられ、必要

に応じて公知のＩＤＳやＩＤＰ等のその他の不正判別手段１２０が設けられる。ＯＳ１００としては特に限定されないが、各種Ｌｉｎｕｘや各種ＢＳＤ等のＵＮＩＸ（登録商標）系ＯＳを好適に用いることができる。

【００３０】

エリアによるパケットフィルター手段（エリヤフィルター手段）１１０は、フィルタリング処理部１１２とフィルタリングルール設定部１１４とからなる。フィルタリング処理部１１２としては、パケットフィルタリング機能を備えるソフトウェアプログラムであれば特に限定はないが、例えば、Ｌｉｎｕｘ系ＯＳであればｉｐｃｈａｉｎｓ、ｉｐｔａｂｌｅｓ等、ＢＳＤ系ＯＳであればｉｐｆｗ等がある。フィルタリングルール設定部１１４は、上記フィルタリング処理部１１２に対するフィルタリングルールを設定したルールファイルである。即ち、上記フィルタリング処理部１１２に応じた書式（フォーマット）で、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）のサイトから取得した割り当て地域情報を含むグローバルＩＰアドレスのアドレス範囲リストに基づいて、ホワイトリスト（パケットの通過許可アドレス一覧表）又はブラックリスト（パケットの拒否アドレス一覧表）として作成したものである。

【００３１】

例えば、日本国内の端末からのみ公開サーバ２４にアクセス可能としたい場合であれば、送信元のグローバルＩＰアドレスの割り当て地域情報（エリア）が日本国（ＪＰ）であるパケットのみを通過許可し（ホワイトリスト）、その他のエリアに属するグローバルＩＰアドレスを送信元とするパケットは全て通過拒否（パケット廃棄）するようにフィルタリングルールを設定すればよい。これによれば、許可地域（例えば日本国）にある端末６０のみが公開サーバ２４にアクセス可能となり、その他の地域は全て禁止地域となるので、禁止地域にある端末５０からは公開サーバ２４にアクセス不能となる。

【００３２】

また例えば、日本国外のＡ国、Ｂ国、Ｃ国等があり、そのうちＣ国の端末からのみ公開サーバ２４にアクセス不能としたい場合であれば、送信元のグローバルＩＰアドレスの割り当て地域情報（エリア）がＣ国であるパケットの通過を全て拒否（パケット廃棄）し（ブラックリスト）、その他のエリアに属するグローバルＩＰアドレスを送信元とするパケットは通過許可するようにフィルタリングルールを設定すればよい。これによれば、禁止地域（例えばＣ国）にある端末５０のみが公開サーバ２４にアクセス不能となり、その他の地域は全て許可地域となるので、許可地域にある端末６０からは公開サーバ２４にアクセス可能である。

【００３３】

なお、フィルタリングルールはポート番号毎に設定可能であり、例えば複数の公開サーバ２４として、Ｗｅｂサーバ（８０番ポート）とＦＴＰサーバ（２１番ポート）とＳＭＴＰサーバ（２５番ポート）とＤＮＳサーバ（５３番ポート）とがあるような場合はポート番号毎に夫々別々に本発明装置１０におけるエリヤフィルター手段１１０を適用することもできる。

【００３４】

また、フィルタリングルールの適用にあたっては、ユーザ（管理者）は国又は地域の名称（エリア名）を選択すればそのエリアに割り当てられている全てのグローバルＩＰアドレスを自動的に適用できるように構成される（この点については後述する）。

【００３５】

更に、前記のように日本国内の端末からのみアクセス可能としたり、特定の国乃至地域の端末からのアクセスを全て拒否した場合でも、別途ＶＰＮ（Viertual Private Network）等の技術を用いれば、禁止地域内であっても特定の海外支社等の端末からのアクセスだけは本発明装置１０におけるエリヤフィルター手段１１０の適用外とすることも可能であるので、エリアによる画一的なパケットフィルタリングを行うことによる不都合は少ない。

【００３６】

図３は、本発明のエリアによるパケットフィルタリング方法（ホワイトリスト型）の一例を示すフローチャートである。上述した本発明のファイヤウォール装置（エリヤフィルター装置）１０の入力ネットワークインターフェイス１４にパケットＰが入力されると、エリアによるパケットフィルター手段（エリヤフィルター手段）１１０がこれを取得する（ステップ２００）。パケットＰのヘッダ情報を抽出して、フィルタリングルールで指定された（フィルタリングの対象とされた）アプリケーション（宛先ポート番号）か否かを判定する（ステップ２０１）。該当しない場合は、そのままパケットＰを通過させ（ステップ２０２）、公開サーバ２４へ送信するか、又は、必要であればＩＤＳやＩＤＰ等のその他の不正判別手段１２０に転送する（ステップ２０５）。他方、該当する場合は、パケットＰがフィルタリングルールで許可された送信元アドレス（即ちエリア）であるか否かを判定する（ステップ２０３）。それが許可されたアドレス（エリア）ならばパケットＰを通過させ（ステップ２０４）、公開サーバ２４へ送信するか、又は、必要であればＩＤＳやＩＤＰ等のその他の不正判別手段１２０に転送する（ステップ２０５）。

【００３７】

パケットＰが許可されていない送信元アドレス（即ちエリア）からのものである場合は、このパケットＰを廃棄（ドロップ）する（ステップ２０６）。廃棄した場合は、ログファイルへ不正ログとして情報を補助記憶装置１８に記録する（ステップ２０７）。このログ記録は、Ｌｉｎｕｘ系ＯＳやＢＳＤ系ＯＳでは標準的に実装されているプログラムであるＳＹＳＬＯＧによればよい。記録されたログは、ログ転送の設定状態（転送先のログサーバが設定されているかどうか等）を確認し（ステップ２０８）、設定されているならば、そのログサーバにログを転送する（ステップ２０９）。このログサーバは図示例では管理端末２６でＳＹＳＬＯＧデーモンを動作させている。他方、設定されていない場合はステップ２０９をスキップする。

【００３８】

アラートメールの設定状態（アラートメールを送信するホストのメールアドレスが設定されているかどうか等）を確認し（ステップ２１０）、設定されているならば、記録された不正ログから送信元グローバルＩＰアドレスを抽出して、ＷＨＯＩＳを実行し、当該アドレスの使用元を検索し記録する（ステップ２１２）。指定されているメールアドレスへ不正ログの情報及び当該アドレスの使用元情報を記録したアラートメールを作成して送信する（ステップ２１３）。アラートメールを送信するホストは図示例では管理端末２６である。他方、設定されていない場合は何もしないで処理を終了する（Ｓ２１１）。

【００３９】

以上の処理をパケット毎に繰り返すことにより、ホワイトリスト型のエリアフィルタリングが可能である。次に、ブラックリスト型のエリアフィルタリングについて説明する。図４は、本発明のエリアによるパケットフィルタリング方法（ブラックリスト型）の一例を示すフローチャートである。ホワイトリスト型（図３）とブラックリスト型（図４）の違いは、ホワイトリスト型ではフィルタリングルールで許可された送信元アドレス（エリア）であるか否かを判定しているのに対し（図３、ステップ２０３）、ブラックリスト型では、フィルタリングルールで禁止された送信元アドレス（エリア）であるか否かを判定している点にある（図４、ステップ３０３）。従って、以下の説明では重複した説明を省略している。

【００４０】

即ち、前述した本発明装置１０の入力ネットワークインターフェイス１４にパケットＰが入力されると、エリヤフィルター手段１１０がこれを取得し（ステップ３００）、パケットＰのヘッダ情報を抽出して、フィルタリングルールで指定されたアプリケーション（宛先ポート番号）か否かを判定する（ステップ３０１）。該当しない場合は、そのままパケットＰを通過させ（ステップ３０２）、公開サーバ２４へ送信するか、又は、必要であればＩＤＳやＩＤＰ等のその他の不正判別手段１２０に転送する（ステップ３０５）。他方、該当する場合は、パケットＰがフィルタリングルールで禁止された送信元アドレス（即ちエリア）であるか否かを判定する（ステップ３０３）。それが禁止されていないアド

レス（エリア）ならばパケットＰを通過させ（ステップ３０４）、公開サーバ２４へ送信するか、又は、必要であればＩＤＳやＩＤＰ等のその他の不正判別手段１２０に転送する（ステップ２０５）。

【００４１】

パケットＰが禁止されている送信元アドレス（即ちエリア）からのものである場合は、このパケットＰを廃棄する（ステップ３０６）。廃棄した場合は、ログファイルへ不正ログとして情報を補助記憶装置１８に記録し（ステップ３０７）、ログ転送の設定状態を確認し（ステップ３０８）、設定されているならば、そのログサーバにログを転送する（ステップ３０９）。他方、設定されていない場合はステップ２０９をスキップする。

【００４２】

アラートメールの設定状態を確認し（ステップ３１０）、設定されているならば、記録された不正ログから送信元グローバルＩＰアドレスを抽出して、ＷＨＯＩＳを実行し、当該アドレスの使用元を検索及び記録し（ステップ３１２）、指定されているメールアドレスへ不正ログの情報及び当該アドレスの使用元情報を記録したアラートメールを作成して送信する（ステップ３１３）。他方、設定されていない場合は何もしないで処理を終了する（Ｓ３１１）。以上の処理をパケット毎に繰り返すことにより、ブラックリスト型のエリアフィルタリングが可能である。

【００４３】

次に、本発明システム２における配信サーバ３０について説明する。配信サーバ３０のハードウェア構成は一般的なサーバコンピュータと同様であり、インターネットWに適宜接続されている。図５は、本発明システム２における配信サーバ３０の最新アドレス情報の取得動作の一例を示すフローチャートであり、配信サーバ３０上で動作するソフトウェアプログラムであるアドレス取得手段（不図示）によって行われる。

【００４４】

まず、配信サーバ３０では、アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）のサイトから最新の割り当て地域情報を含むグローバルＩＰアドレスのアドレス範囲リストが記録されたアドレス情報ファイルをダウンロードする（ステップ４００）。

【００４５】

アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ）又は地域アドレス管理機関（ＲＩＲ）から得られるアドレス情報ファイルは、前述した如く、例えば

apnic｜JP｜ipv4｜210.196.xxx.xxx｜ 65536｜19990609｜allocated

というような形式のリストの羅列であり、エリア別にも分けられてもいないので、これをＩＰアドレス／ネットマスクの形式に変換するのである。上記例で言えば、開始アドレス２１０．１９６．ｘｘｘ．ｘｘｘからアドレス数が６５５３６個であるので、ＣＩＤＲ表記で２１０．１９６．ｘｘｘ．ｘｘｘ／１６と変換した上で、エリアはＪＰなので日本国に対応したエリアファイルに保存する。

【００４６】

なお、このように各国別に全てのグローバルＩＰアドレスが列挙されたエリアファイルを用意することで、本発明装置１０のユーザ（管理者）は国又は地域の名称（エリア名）を選択すれば、このエリアファイルに基づいてそのエリアに割り当てられている全てのグローバルＩＰアドレスを自動的に適用できるので、ユーザ（管理者）は具体的なグローバルＩＰアドレスを意識する必要は無く、極めて利便性の高いものとなる。

【００４７】

保存された各エリアファイルのアドレス記述フォーマットのチェックを行い（ステップ４０２）、正常なフォーマットか否かを判定する（ステップ４０３）。正常でないならば、処理を中断して（ステップ４０４）、最初から再度繰り返すようにする。正常ならば、当該処理の日付からバージョン情報ファイルを自動生成し（ステップ４０５）、各エリアファイルとバージョン情報ファイルをアーカイブして圧縮する（ステップ４０６）。このアーカイブと圧縮は常法により行えばよく特に限定はないが、例えばＬｉｎｕｘ系ＯＳや

ＢＳＤ系ＯＳではアーカイブはＴＡＲ等、圧縮はＧＺＩＰ等のプログラムによればよい。アーカイブされ圧縮された各エリアファイル及びバージョン情報ファイルを含む圧縮アーカイブファイルは更に暗号化して（ステップ４０７）、この暗号化ファイルを所定のファイル名に変更して（ステップ４０８）、本発明装置１０が配信サーバ３０にアクセスして当該暗号化ファイルをダウンロード可能なように所定のパス（ディレクトリ）に移動せしめる（ステップ４０９）。なお、この暗号化は秘密鍵暗号方式でも公開鍵暗号方式でもよいし両者を組み合わせてもよい。

【００４８】

図６は、本発明システム２におけるファイヤウォール装置（エリアフィルター装置）１０のフィルタリングルールの更新動作の一例を示すフローチャートであり、本発明装置１０上で動作するソフトウェアプログラムであるルール更新手段（不図示）によって行われる。まず、本発明装置１０では、定期的又は不定期に任意で、指定された配信サーバ３０にインターネットWを介して接続し（ステップ５００）、既にダウンロード済みの暗号化ファイルと配信サーバ３０からダウンロードしようとする暗号化ファイルとを比較して新しいものか否かを判定する（ステップ５０１）。新しいものでないか同じであるならば、処理を中断し（ステップ５０２）、後日又は時間をおいて最初から再度繰り返すようにする。

【００４９】

新しいものであるならば、当該暗号化ファイルのダウンロードを実行する（ステップ５０３）。そして、暗号化ファイルの復号化を実行し（ステップ５０４）、復号化に成功したか否かを判定する（ステップ５０５）。成功していない場合は処理を中断し（ステップ５０６）、最初から再度繰り返すようにする。成功した場合は、暗号化されていない圧縮アーカイブファイルが生成されているはずなので、当該圧縮アーカイブファイルの展開及び解凍を実行し（ステップ５０７）、展開及び解凍に成功したか否かを判定する（ステップ５０８）。成功していない場合は処理を中断し（ステップ５０９）、最初から再度繰り返すようにする。成功した場合は、アーカイブも圧縮もされていないエリアファイルとバージョン情報ファイルが生成されているはずなので、各エリアファイルのアドレス記述フォーマットのチェックを行い（ステップ５１０）、正常なファーマットか否かを判定する（ステップ５１１）。正常でないならば、処理を中断し（ステップ５１２）、最初から再度繰り返すようにする。

【００５０】

正常ならば、バージョン情報ファイルと既存のバージョンとの比較を行い（ステップ５１３）、新しいバージョンでないなら、後日又は時間をおいて最初から再度繰り返すようにする。新しいバージョンならば、既存のエリアファイルを上書き更新する（ステップ５１６）。そして、現在使用しているエリア毎のフィルタリングルールを識別（許可か拒否か、ボート番号によって異なる設定をしているか等）し、新しいバージョンのエリアファイルに基づいて、新たなフィルタリングルールを再作成する（ステップ５１７）。最後に、エリアによるパケットフィルター手段（エリヤフィルター手段）１１０の再起動を行い、フィルタリングルールの更新が完了する（ステップ５１８）。

【００５１】

このようにして、本発明によれば、不正アクセス等の目的の有無やパケットの内容とは無関係に、送信元のグローバルＩＰアドレスからその端末が所属する国乃至地域の単位でパケットの通過の許可又は拒否が行われるので、Ｗｅｂサーバ等の運営者が意図しない不必要な通信トラフィックを画一的に制御でき堅牢で確実な利便性の高いエリアによるパケットフィルタリング方法及びファイヤウォール装置並びにファイヤウォールシステムを提供することができるという大きな効果を奏する。

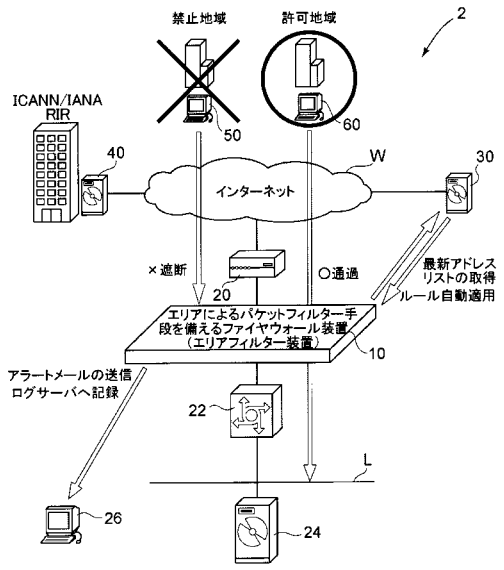
【図面の簡単な説明】

【００５２】

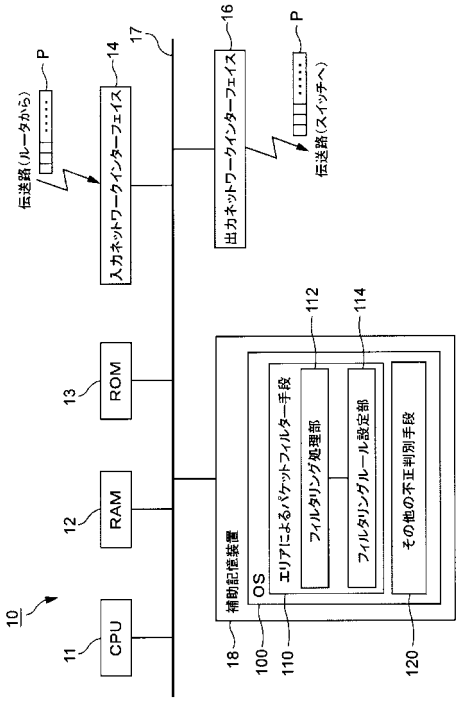
【図１】本発明のファイヤウォールシステム（エリアフィルターシステム）の全体的な機器構成の一例を概念的に示す説明図である。

【図２】本発明のファイヤウォール装置（エリヤフィルター装置）のハードウェア構成の一例を示すブロック図である。
【図３】本発明のエリアによるパケットフィルタリング方法（ホワイトリスト型）の一例を示すフローチャートである。
【図４】本発明のエリアによるパケットフィルタリング方法（ブラックリスト型）の一例を示すフローチャートである。
【図５】本発明システムにおける配信サーバの最新アドレス情報の取得動作の一例を示すフローチャートである。
【図６】本発明システムにおけるファイヤウォール装置のフィルタリングルールの更新動作の一例を示すフローチャートである。
【符号の説明】
【００５３】
２：本発明のファイヤウォールシステム（エリアフィルターシステム）、１０：本発明のファイヤウォール装置（エリヤフィルター装置）、１４：入力ネットワークインターフェイス、１６：出力ネットワークインターフェイス、１７：バス、１８：補助記憶装置、２０：ルータ、２２：スイッチ、２４：公開サーバ、２６：管理端末、３０：配信サーバ、４０：アドレス管理機関（ＩＣＡＮＮ／ＩＡＮＡ，ＲＩＲ）のサーバ、５０：禁止地域の端末、６０：許可地域の端末、１１０：エリヤフィルター手段、１１２：フィルタリング処理部、１１４：フィルタリングルール設定部、１２０：その他の不正判別手段、Ｌ：内部ネットワーク、Ｐ：パケット、Ｗ：インターネット。

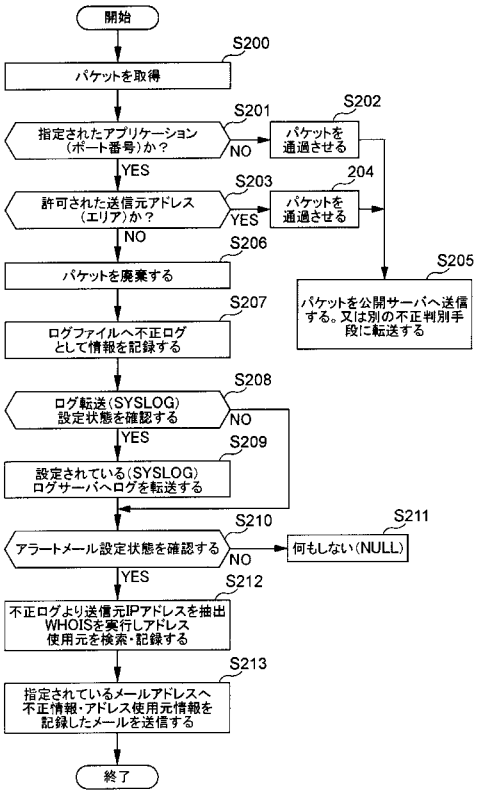
【図１】



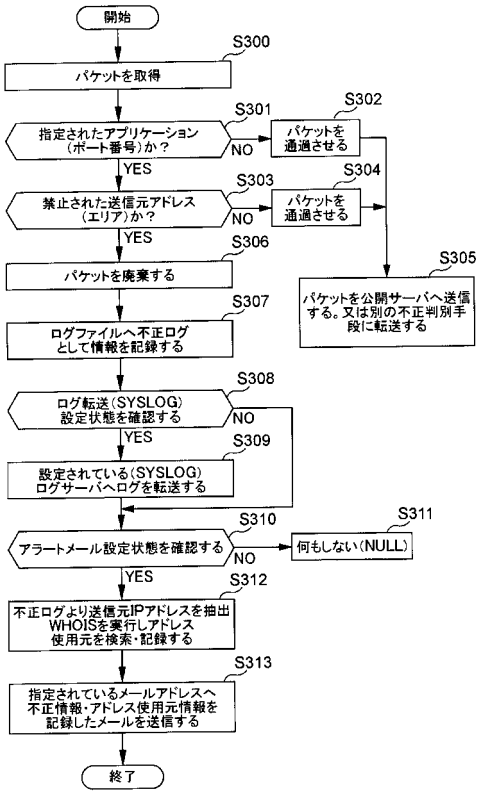
【図２】



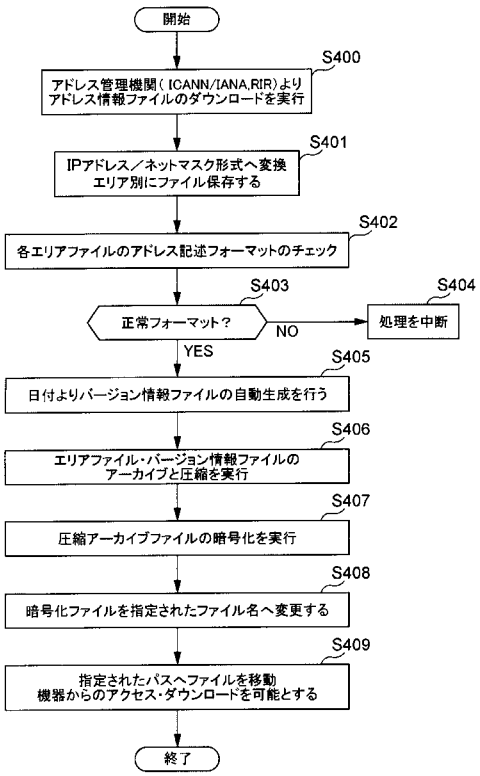
【図３】


開始
S200
パケットを取得
S201
指定されたアプリケーション（ポート番号）か？
NO
S202
パケットを通過させる
YES
S203
許可された送信元アドレス（エリア）か？
YES
204
パケットを通過させる
NO
S206
パケットを廃棄する
S205
パケットを公開サーバへ送信する。又は別の不正判別手段に転送する
S207
ログファイルへ不正ログとして情報を記録する
S208
ログ転送（SYSLOG）設定状態を確認する
NO
YES
S209
設定されている（SYSLOG）ログサーバへログを転送する
S210
アラートメール設定状態を確認する
NO
S211
何もしない（NULL）
YES
S212
不正ログより送信元IPアドレスを抽出 WHOISを実行しアドレス使用元を検索・記録する
S213
指定されているメールアドレスへ不正情報・アドレス使用元情報を記録したメールを送信する
終了

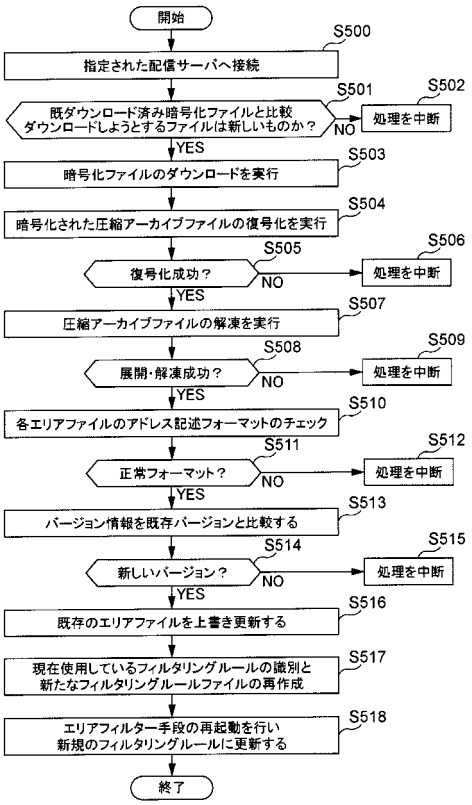
【図４】


開始
S300
パケットを取得
S301
指定されたアプリケーション（ポート番号）か？
NO
S302
パケットを通過させる
YES
S303
禁止された送信元アドレス（エリア）か？
NO
S304
パケットを通過させる
YES
S306
パケットを廃棄する
S305
パケットを公開サーバへ送信する。又は別の不正判別手段に転送する
S307
ログファイルへ不正ログとして情報を記録する
S308
ログ転送（SYSLOG）設定状態を確認する
NO
YES
S309
設定されている（SYSLOG）ログサーバへログを転送する
S310
アラートメール設定状態を確認する
NO
S311
何もしない（NULL）
YES
S312
不正ログより送信元IPアドレスを抽出 WHOISを実行しアドレス使用元を検索・記録する
S313
指定されているメールアドレスへ不正情報・アドレス使用元情報を記録したメールを送信する
終了

【図５】


開始
S400
アドレス管理機関（ICANN/IANA,RIR）よりアドレス情報ファイルのダウンロードを実行
S401
IPアドレス／ネットマスク形式へ変換 エリア別にファイル保存する
S402
各エリアファイルのアドレス記述フォーマットのチェック
S403
正常フォーマット？
NO
S404
処理を中断
YES
S405
日付よりバージョン情報ファイルの自動生成を行う
S406
エリアファイル・バージョン情報ファイルのアーカイブと圧縮を実行
S407
圧縮アーカイブファイルの暗号化を実行
S408
暗号化ファイルを指定されたファイル名へ変更する
S409
指定されたパスへファイルを移動 機器からのアクセス・ダウンロードを可能とする
終了

【図６】


開始
S500
指定された配信サーバへ接続
S501
既ダウンロード済み暗号化ファイルと比較 ダウンロードしようとするファイルは新しいものか？
NO
S502
処理を中断
YES
S503
暗号化ファイルのダウンロードを実行
S504
暗号化された圧縮アーカイブファイルの復号化を実行
S505
復号化成功？
NO
S506
処理を中断
YES
S507
圧縮アーカイブファイルの解凍を実行
S508
展開・解凍成功？
NO
S509
処理を中断
YES
S510
各エリアファイルのアドレス記述フォーマットのチェック
S511
正常フォーマット？
NO
S512
処理を中断
YES
S513
バージョン情報を既存バージョンと比較する
S514
新しいバージョン？
NO
S515
処理を中断
YES
S516
既存のエリアファイルを上書き更新する
S517
現在使用しているフィルタリングルールの識別と新たなフィルタリングルールファイルの再作成
S518
エリアフィルター手段の再起動を行い新規のフィルタリングルールに更新する
終了