(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2005-197823
(P2005-197823A)
(43)公開日　平成17年7月21日(2005.7.21)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/66	H04L 12/66	B	5B089
G06F 13/00	G06F 13/00	351Z	5K030

審査請求 未請求　請求項の数 5　ＯＬ　（全 16 頁）

(21)出願番号　特願2003-435587 (P2003-435587)
(22)出願日　平成15年12月26日 (2003.12.26)

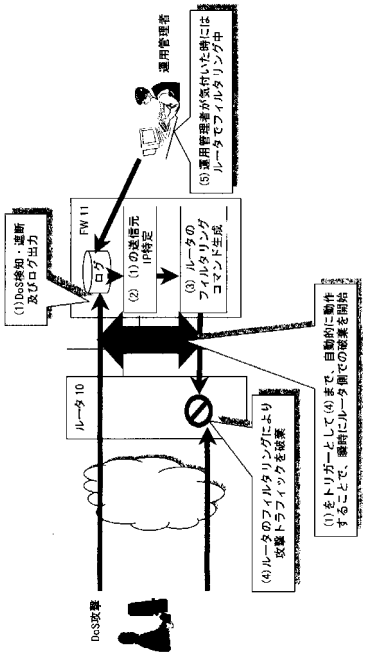
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100067987
弁理士　久木元　彰
(72)発明者　山崎　毅
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B089 GA31 JB10 KA17 KB06 KB13 KC54 KC59
5K030 GA15 HA08 HC01 HD03 HD09 JA10 KA05 LC18 MA13 MC09

(54)【発明の名称】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

(57)【要約】
【課題】　ファイアウォールとルータの連携により、高速、且つ、正常なアクセスを常に正常に処理できる不正アクセス制御装置を提供する。
【解決手段】　ＤＯＳ攻撃を検出したファイアウォール（ＦＷ）１１は、ＤＯＳ攻撃を遮断し、攻撃があったことを示すログを出力する。そして、ＤＯＳ攻撃の送信元のＩＰアドレスを特定する。そして、ルータ１０に、攻撃遮断のためのフィルタリングコマンドを生成して、ルータに送る。ルータ１０は、ＦＷ１１から送られてきたコマンドにより、指定されたＩＰアドレスから送信されてくるパケットをフィルタリングにより破棄する。
【選択図】図１

本発明の実施形態に従ったファイアウォールで
DOS攻撃検出時の動作を説明する図



【特許請求の範囲】
【請求項１】
外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御装置において、
アクセス元のアドレスを指定して、ハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータと、
設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータ手段に送信し、フィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールと、
を備えることを特徴とする不正アクセス制御装置。
【請求項２】
前記ルータに設定したフィルタリングのポリシーに基づき、該ルータ手段でのパケットの破棄状況について、前記ファイアウォールから定期的に情報収集することを特徴とする請求項１に記載の不正アクセス制御装置。
【請求項３】
前記ルータから収集した破棄情報を基に、破棄パケット数が所定の閾値を下回るか否かを判断し、下回った場合には、該ルータに対してパケット破棄を中止させることを特徴とする請求項２に記載の不正アクセス制御装置。
【請求項４】
外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御方法において、
アクセス元のアドレスを指定して、ルータのハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータステップと、
設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータに送信し、該ルータにフィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールステップと、
を備えることを特徴とする不正アクセス制御方法。
【請求項５】
外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御方法において、
アクセス元のアドレスを指定して、ルータのハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータステップと、
設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータに送信し、該ルータにフィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールステップと、
を備えることを特徴とする不正アクセス制御方法をコンピュータに実現させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ファイアウォール及びルータでの不正アクセス制御装置に関する。
【背景技術】
【０００２】
近年の通信技術の発達により、インターネットなどのネットワークに多くの情報処理端

末が接続されている。しかし、ネットワークに接続されている情報処理端末のユーザは良心的とは限らず、ハッカーと呼ばれる人たちがいる。ハッカーは、他人の情報処理端末に不正にアクセスし、秘匿性の高い情報を勝手に取得したり、侵入した情報処理端末をハッカーが勝手に操作するなどを行い、侵入された側の安全を脅かす。

【０００３】

このような、不正なアクセスに対処するため、今日、情報処理端末が接続されているネットワークの情報処理端末への入り口にファイアウォールとルータを設けることによって対処することが多く行われている。ファイアウォールは不正アクセスを検出して、不正アクセスを遮断し、ルータの場合は、ユーザがアクセス拒否のアドレスを設定して、当該アドレスからの不正アクセスを拒否するなどが行われる。

【０００４】

しかし、従来は、ファイアウォールは、レイヤ２～レイヤ７までの各レイヤでのアクセス制御ポリシーに基づき、アクセス制御を行うため、高度な制御を実現可能であるが、ネットワークを流れるパケットのデータの内部まで識別するために、高速な制御が困難であった。

【０００５】

ルータは、ハードレベルでのアクセス制御機能を実装し、高速な制御が可能であるが、レイヤ４～レイヤ７のレイヤでのアクセス制御が困難であった。

このため運用管理者が、ファイアウォールでのアクセス制御ログ情報を参照し、不正なアクセスを検知した場合に、ルータに該当トラフィックを拒否するフィルタリングポリシーを手動で設定する運用としていた。

【０００６】

特許文献１には、外部ネットワークから企業内情報ネットワークへの不正アクセスを検出し、不正パケットの送信元端値を可能とするネットワーク監視システムが開示されている。

【０００７】

特許文献２では、ルータ、スイッチ、ファイアウォール等の各機器の保有するフィルタリングポリシーレベルでフィルタリングを行っている。しかし、他の機器の異なるレイヤでのフィルタリングポリシーへの変換適用までは実施しておらず、フィルタリングポリシーの設定はセキュリティ運用管理者が入力する方式をとっている。

【０００８】

特許文献３では、複数のファイアウォール装置のフィルタリングヒット状況を外部の管理装置に自動転送し、各ファイアウォールからの情報を基に最適なフィルタリング情報を自動的に再更新し、各ファイアウォール装置に自動転送・反映する方式が開示されている。

【特許文献１】特開２０００－２６１４８３号公報
【特許文献２】特表２００２－５０７２９５号公報
【特許文献３】特開２００３－２３３６２３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

従来技術の場合、ファイアウォールとルータは別のノードであり、ファイアウォールでの異常検出をルータのフィルタリングポリシー設定に自動的に反映することができず、運用管理者による監視及び手動操作が必要であった。また、一時的にファイアウォールが過負荷状態となる問題があった。

【００１０】

また、ファイアウォールでの異常検出を、ルータでのフィルタリングポリシー設定による不当ｐｋｔ（ｐｋｔはパケットの省略）の高速な破棄に連動することができない。

ルータでのフィルタリング動作によるパケット破棄状況と、ファイアウォールでのフィルタリング動作によるパケット破棄状況の双方を確認しないと不正アクセスの継続状況を

確認できないという問題もある。

【００１１】

更に、ファイアウォールで検出した異常状態に対し、ルータにフィルタリングポリシーを追加した場合、その解除可否の確認、および解除指示を運用管理者が、ルータにアクセスして行う必要がある。

【００１２】

ファイアウォールがＤＯＳ／ＤＤＯＳ攻撃を検知している状態において、ルータでのフィルタリングポリシー設定を行う際、ルータとファイアウォール間の通信路を使用すると、トラフィックが多くなってしまうため、操作ができない場合が発生し得る。

【００１３】

複数のルータを経由してファイアウォールと接続されている場合において、ＤＯＳ／ＤＤＯＳ攻撃の送信元トラフィックの入り口となっているルータを特定し、ルータのフィルタリングポリシーを適用するまでに時間がかかり、その間の業務が停止してしまう。

【００１４】

特許文献１では、ファイアウォールとルータの連携により不正アクセスを検知しているが、その不正アクセスを偽装サーバに到達させているため、大量の不正パケットが送られてくる場合、ファイアウォールとルータ間のネットワークがいっぱいになり、正しいパケットを受け付けられなくなる可能性が高い。特に、特許文献１の技術では、ＤＯＳ／ＤＤＯＳ攻撃時に、ファイアウォールや偽装サーバ、探知装置が動作不能となったり、トラフィック監視装置からファイアウォール、ルータへのフィルタリングルールの適用が、ＤＯＳ／ＤＤＯＳ攻撃での負荷によりファイアウォールからルータへ指示できない可能性が高い。

【００１５】

本発明の課題は、ファイアウォールとルータの連携により、高速、且つ、正常なアクセスを常に正常に処理できる不正アクセス制御装置を提供することである。

【課題を解決するための手段】

【００１６】

本発明の不正アクセス制御装置は、外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御装置において、アクセス元のアドレスを指定して、ハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータと、設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータ手段に送信し、フィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールとを備えることを特徴とする。

【００１７】

本発明によれば、ファイアウォールが不正アクセスを検出すると、ファイアウォールは、ルータが不正アクセス元のアドレスからのパケットを破棄するように自動的に設定する。ファイアウォールが自動的にルータの設定を行うことにより、ルータでのハードウェアによる高速なパケット破棄が実現できる。また、ルータとファイアウォールとの間の回線には不正アクセスのパケットが入り込まなくなるので、正規のアクセスを正常に受け付け続けることができる。

【発明の効果】

【００１８】

本発明によれば、ファイアウォールとルータを連携させた不正アクセス制御を行うので、高速且つ高度な不正アクセス拒否制御を行うことができる。

【発明を実施するための最良の形態】

【００１９】

本発明の実施形態では、以下の構成を採用する。

（１）ファイアウォールでの異常検出時、その送信元ＩＰアドレスを特定し、ＬＡＮ上に存在するルータに対し、そのルータの使用するフィルタリングコマンドでルータにフィルタリングポリシーを自動設定する機能を、ファイアウォールに実装する。
（２）ファイアウォールでのパケット破棄状況に関する統計情報として、ＬＡＮ上に存在するルータでのフィルタリング動作によるパケット破棄状況をコマンドにより入手し、上記統計情報に結合して、運用管理者に通知することで、ファイアウォールだけを監視することで、不当アクセス状況を確認する手段を設ける。
（３）（１）でルータに設定したフィルタリングポリシーに対し、（２）の動作により、異常状態の継続有無を定期的に確認し、事前に設定した異常状態脱出の閾値を下回った場合に、自動的に（１）で設定したフィルタリングポリシーを解除するコマンドを投入し、通常状態に復帰する機構を設ける。
（４）ルータとファイアウォール間で帯域を確保した専用の通信路（ＶＬＡＮ等）を確保し、（１）、（２）、（３）の動作を保証する。
（５）複数のルータを経由してファイアウォールと接続されている場合において、ファイアウォールに上記ルータを全て事前登録しておき、ＤＯＳ／ＤＤＯＳ（Denial Of Service/Distributed Denial Of Service）攻撃検出時に、登録された全てのルータに対して、（１）、（２）、（３）の動作を行う。

【００２０】

ＤＯＳ／ＤＤＯＳ攻撃により送られてくる不正パケットを破棄することにより、ルータとファイアウォールとの間の回線の容量が大きく消費されてしまうことを防ぎ、正当なアクセスを常に正常に受け付けることを可能としている。

【００２１】

以下、図面を用いて説明する。
図１は、本発明の実施形態に従ったファイアウォールでＤＯＳ攻撃検出時の動作を説明する図である。

【００２２】

ファイアウォール１１（以下、ＦＷ）が、事前設定されたフィルタリングポリシーをもとにＤＯＳ／ＤＤＯＳ攻撃を検出した場合（１）、ログ出力を行うと同時に、その不正アクセスパケットの送信元ＩＰアドレスを特定する（２）。

【００２３】

このＦＷ１１には、事前にルータ１０の外部接続ネットワークのインターフェース名、及びルータ１０のフィルタリングコマンド形式を登録しておき、（２）で特定した送信元ＩＰアドレスをキーとしたルータのフィルタリングコマンドを生成し、ルータにコマンド操作のためのリモート接続を行った後、当該コマンドをルータに設定する（３）。ルータ１０では、（３）で設定されたフィルタリングポリシーを元に、以降のＤＯＳ／ＤＤＯＳ攻撃パケットを遮断・破棄する（４）。以降、（１）～（４）までの動作を自動的に実施する。運用管理者がＦＷ１１のログを見て、不正アクセスを発見したときには、既に、ＦＷ１１とルータ１０が連携して、不正アクセスをフィルタリングしている状態になっている。

【００２４】

なお、今後、本発明の実施形態の説明において、ルータは、以下の構成をもっているものとする。
１）ルータは、送信元ＩＰアドレス指定によるパケット破棄をハードレベルで実現可能な環境を持ち、このパケット破棄指示を各ルータ固有のコマンド仕様で指定可能とする。また、各ルータは、外部ネットワークに対する接続インターフェースと、サーバ宛のパケットの中継点であるＦＷ側への接続インターフェース、及びルータ装置の運用管理（フィルタリングポリシー設定、状態確認）を行うための専用インターフェースを保持する。また、ルータは、複数台で構成可能で、かつ、異なるルータ機種でも組み合わせて構成可能である。
２）ルータ及びＦＷの運用管理インターフェースは、ルータとＦＷ間の、正当なユーザと

サーバ間通信のために使用するインターフェースとは独立したインターフェースで、かつ、サーバ間通信用インターフェースのトラフィックとは帯域を共有しない、例えば、異なる物理回線を使うとか、同一ケーブル上でＶＬＡＮを分け、かつ、帯域を運用管理専用に確保しているなどの方式を採用している。

【００２５】

図２は、本発明の実施形態に従ったファイアウォールでのＤＯＳ攻撃検出後の動作を説明する図である。

（１）で、ＦＷ１１からルータ１０に設定したフィルタリングポリシーに基づき、ルータ１０でＤＯＳ／ＤＤＯＳ攻撃パケットを遮断した後は、ＦＷ１１から定期的にルータ１０側のフィルタリング状態表示コマンドを投入することで、破棄パケット数の増加有無を確認し（３）、その状態表示コマンドで得た情報を、ＦＷ１１のファイルリングポリシー（ＤＯＳ／ＤＤＯＳ攻撃防御ポリシー）のルールに対応付けて蓄積しているため運用管理者が攻撃の継続を確認するために仮想ノードに対する確認コマンドを投入すると、破棄状態に関する統計情報として受け取る（４）ことができる。このため運用管理者は、ＦＷ１１がフィルタリング制御をルータにオフロード（パケットの破棄処理をＦＷ１１からルータ１０に移すこと）しているか否かを意識することなく、状態確認をＦＷ１１に対する操作だけで実施することが可能となる。

【００２６】

図３は、本発明の実施形態に従ったＤＯＳ攻撃停止時の動作を説明する図である。

（１）によりＦＷ１１からルータ１０にフィルタリングポリシーを設定し、（２）で、ルータにて攻撃トラフィックに該当するパケットを破棄している状況において攻撃が止まった場合（３）、ＦＷ１１に事前設定した攻撃状態の解除認識条件（攻撃パケットの時間あたりの数が閾値以下となって、指定した時間経過など）に適合した場合に、自動的に（１）で設定したポリシーを解除するコマンドをファイアウォール（ＦＷ１１）が投入することで、不要なアクセス制御ルールの残存による、定常状態での余分な負荷の継続を自動的に防止する。

【００２７】

図４は、本発明の実施形態の動作環境に関する説明図である。

なお、同図において、ハッカー１～５、外部ネットワーク、ルータ１～３、ＦＷ現用装置、ＦＷ待機装置、運用管理端末などに付されている数字や記号は、ＩＰアドレス等の装置を特定する識別子の例である。後の図において、これらのＩＰアドレス等を用いて説明を行う。

【００２８】

正当な利用者からのアクセスと、不当なアクセス（悪意あるアクセス）を行うハッカーが混在し得るインターネット等の外部接続ネットワーク１５と各ユーザからのアクセス先であるサーバまでの間に、本発明の実施形態で説明するルータ１０－１～１０－３及びＦＷ１１－１、１１－２が存在する。ルータ１０－１～１０－３は、送信元ＩＰアドレス指定によるパケット破棄をハード（チップ）のコマンド仕様で指定可能である。また、各ルータ１０－１～１０－３は、外部ネットワーク１５に対する接続インターフェース、及びルータ装置の運用管理（フィルタリングポリシー設定、状態確認）を行うための専用インターフェースを保持する。また、ルータ１０－１～１０－３は、複数台で構成可能、かつ、異なるルータ機種でも実現可能である。ＦＷ１１－１、１１－２は、１台または２台（ＦＷの信頼性を高める場合）で構成可能であり、ルータ１０－１～１０－３と直接接続されたインターフェース、サーバへの接続インターフェース、及びＦＷの運用管理（ＤＯＳ／ＤＤＯＳ攻撃防御ポリシー、ルータ連携環境設定、ＤＯＳ／ＤＤＯＳ攻撃防御状況確認）を行うための専用インターフェースを保有する。ルータ１０－１～１０－３及びＦＷ１１－１、１１－２の運用管理インターフェースは、ルータ１０－１～１０－３とＦＷ１１－１、１１－２間の、正当なユーザとサーバ間通信（以降、業務通信と略す）のために使用するインターフェースとは独立したインターフェースで、かつ、業務インターフェースのトラフィックとは帯域を共有しない方式（異なる物理結線または、同一ケーブル上でＶ

ＬＡＮを分け、かつ帯域を運用管理専用に確保）を保有する。

【００２９】

ＦＷ１１－１、１１－２は、２台でホットスタンバイ動作により使用することが可能であり、この場合、業務通信用インターフェースに関し、ルータ側およびサーバ側で、各々各ネットワークに共通な２台のファイアウォール（以降ＦＷと略す）に対し１つの共用ＩＰを付与し、本ＩＰを仮想ＩＰとして現用ＦＷ装置１１－１が通信に使用する機能を保持する。また、運用管理用インターフェースにおいても共用ＩＰを付与し、運用管理者は、本ＩＰを運用操作対象ＦＷとして運用操作することで、運用管理者に２台のＦＷの意識及びＦＷの動作状態（現用・待機）の意識を不用とする機能を保有する。

【００３０】

図５は、ファイアウォールに環境定義情報として運用管理者が設定する情報をテーブルとして表した図である。図５におけるテーブルの内容は、例として図４の情報を基に設定したものである。

【００３１】

連携対象ルータとは、外部ネットワークに接続されたルータであり、図４のルータ１～ルータ３を示す。また、これらの各ルータ単位に図５に示す各情報を設定する。制御用ＩＰアドレスとは、ＦＷからルータに対するコマンド制御を行うためのルータ側ＩＰであり、図４の運用管理用インターフェース上のルータ側ＩＰを示す。制御用アカウント・パスワードは、ＦＷから各ルータに対する運用管理操作を行うための接続を行う際、ルータ側の認証情報として、登録されているものを設定する。接続手順・接続ポート番号は、上記接続を行う際に使用するポート番号、及び、接続する場合telnetまたはｓｓｈのいずれの手順を使用するかを示し、接続手順は、ルータ側でサポートされているtelnet／sshのいずれかを設定する。

【００３２】

ルータ種別とは、後に図６で示すようにルータのメーカ、機種によりフィルタリング等の機能で提供するルータのコマンド仕様が相違する場合に、適切なコマンド仕様を選択するためのルータ種別識別情報であり、ＦＷ内に実装されている図６のテーブルに登録されたルータが本実施形態での対象ルータとなる。

【００３３】

ＤＯＳ防御インターフェースは、ルータにフィルタリングルールを適用する際、インターフェースの指定が可能であるかを示すものであり、指定可能な場合には、更に、外部ネットワーク接続インターフェース名を指定する。また、この指定はルータによっては、任意の指定が可能であることが考えられるが、この場合、ルータ側の処理能力により、特に問題が無ければ、外部ネットワークだけでなく、全インターフェースを対象とすることもできるものと想定する。

【００３４】

フィルタリングルール番号は、ルータに対するフィルタリングルールをコマンドにより設定する際に、複数のルールを識別するための番号を、ＦＷ側で保持するものである。また、ルータへのフィルタリングルールは、本実施形態によるＦＷからの自動設定以外にも、運用管理者が事前設定するケースもあるため、本テーブルで設定した番号の範囲を、ＦＷからの自動設定で使用すると共に、その他の番号の範囲をユーザの手動設定で使用することし、これにより、ＦＷでの自動設定と、運用管理者の手動設定で、ルール番号の重複が発生することを回避する。

【００３５】

図６は、本発明の実施形態に従った、ＦＷ装置のファームウェア、あるいは、ソフトウェアとして装置自身に登録されている情報の例を示す図である。

図６のテーブルは、運用管理者は操作しない内部テーブルである。

【００３６】

図６のテーブルは、ＦＷ装置が本実施形態で連携可能なルータ装置（機種）に対し、その識別情報をルータ種別という形で与える。ＦＷは、本実施形態での連携ルータ機種を拡

張する場合には、本テーブルにルータ種別を新規に追加し、他のテーブル内容に、追加したルータ仕様に基づいた情報を付加する。これにより、新たなルータに対しても本実施形態を適用することができるようになる。

【００３７】

フィルタリングルールコマンド、ルール適用コマンド、状態参照コマンド、フィルタリングルール解除コマンド、ルール適用解除コマンド、インターフェース指定コマンドには、ルータ種別毎に、そのルータの仕様に沿ったコマンドsyntaxを設定する。

【００３８】

図７は、運用管理者が、ＦＷ装置に対して、ＦＷ装置が提供するＤＯＳ／ＤＤＯＳ防御機能の使用の有無をポリシーとして設定したＦＷ内部のテーブルの例を示す図である。

検出ＤＯＳ攻撃種別は、ＦＷ装置が提供するＤＯＳ防御機能の一覧であり、図７に不正ＩＰパケット受信、不正ＴＣＰパケット受信、Ping of Death攻撃、Nimudaワーム、ＩＬＯＶＥ ＹＯＵ攻撃と列挙されているように、各種別単位で、詳細なＤＯＳ攻撃としての検出対象／内容が、検出ＤＯＳ攻撃内容詳細として設定されている。ユーザは、不正ＩＰバージョンなどの一意に識別可能な情報を指定する場合において、ＧＵＩ（Graphic User Interface）、ＣＬＩ（Command Line Interface）でユニークな識別子を選択するだけで指定可能な場合や、図７のNimudaワームの詳細検出内容のように複数の識別情報を同様にＧＵＩ、ＣＬＩで識別子選択・指定する場合、及び、ユーザ自身がこれらの詳細情報を、識別パターンとして個別に設定する場合のいずれでも指定可能である。

【００３９】

異常検出閾値は、ＦＷ装置としてデフォルト値を保有し、運用管理者が特に指定しない場合は、この値を使用し、運用管理者が特別に、各ルールに対し指定した場合には、指定値が採用され、本テーブルに反映される。設定内容としては、秒あたりの該当ｐｋｔ受信数を指定し、その数を上回った場合に検知する方法と、１ｐｋｔでも受信した場合には即座に異常とみなす即時検出（実質的に１ｐｋｔ／ｓと同等）の２つの方法がある。

【００４０】

遮断可否の情報は、攻撃パターンを異常検出閾値以上のｐｋｔ数受信時に、異常と認識し遮断する（ｐｋｔ破棄する）か否かを示す。この情報を遮断と指定した場合に、異常検出、閾値異常のｐｋｔ受信時に、異常発生のメッセージ出力と同時に、ルータに対する動的なフィルタリング指示を行う。

【００４１】

遮断解除時間とは、異常検出後、遮断状態を解除するまでの時間である。

なお、異常検出時時点から遮断解除時間経過時に、その間のルータでのｐｋｔ廃棄状況を確認し、その破棄数が異常検出閾値以上であった場合には、遮断時間解除時間経過後であってもルータに対するフィルタリングの解除指示は行わず、この時点から再度、遮断時間解除時間が経過するまで、ルータでのフィルタリング状態を継続する。

【００４２】

図８は、ＤＯＳ／ＤＤＯＳ攻撃をＦＷで検出している状態、及び、ルータに対する指示状態を管理するためにＦＷ内部に保持するテーブルの例を示す図である。

図７で示すＦＷのポリシーテーブルを基に、ＤＯＳ／ＤＤＯＳ攻撃を検出した場合に、その検出時間、及び検出時の該当ｐｋｔの送信元ＩＰアドレスと、そのＩＰアドレスでルータにフィルタリング指示を行った場合の各ルータに対して発行したフィルタリング適用指示コマンドのルール番号をルータ毎に保持している。

【００４３】

本テーブル情報を基に、ＦＷは、ＤＯＳ／ＤＤＯＳ攻撃検出時に、ルータに対して発行したフィルタリング指示コマンドに対応付けて、攻撃解除時にフィルタリング適用解除指示コマンドを発行するための情報、及び、攻撃の継続状態の確認を行うための情報として使用する。

【００４４】

本情報は、ＦＷの現用装置で状態更新が行われるが、更新時には、その差分情報をＦＷ

待機装置に転送し、常にＦＷ現用・待機装置間で状態の同期（一致性保証）が行われる。
図９は、ＦＷでのＤＯＳ／ＤＤＯＳ攻撃検出からルータへのフィルタリング指示までのＦＷ側での動作の流れを示すフローチャートである。

【００４５】
各ルータは、ＦＷから指示されたフィルタリング指示コマンドを、コマンド操作として動的に受け付け、その状態参照コマンドに対して、フィルタリング指示コマンドによるｐｋｔ破棄状態通知、および、フィルタリング適用解除指示コマンドの受け付けを行う。ルータでは、状態が、通常状態→フィルタリング適用中（状態確認コマンド受け付け）→通常状態（フィルタリング適用解除指示コマンド受け付け）の遷移を行う。

【００４６】
以下に、図９の流れについて説明する。
ステップＳ１０において、ＦＷはパケット（ｐｋｔ）を受信すると、検出対象のＤＯＳ攻撃に一致したか否かの判定を行う。一致しなかった場合には、ステップＳ１１において、全ＤＯＳ攻撃対象のチェックが完了したか否かについて判断する。ステップＳ１１の判断がＮＯの場合には、ステップＳ１０に戻る。ステップＳ１１の判断がＹＥＳの場合には、処理を終了する。

【００４７】
すなわち、図７のテーブルを使用し、一致するものがあるか否かを図７の全行（以降エントリと呼ぶ）に対して行い、存在しなかった場合は、ＤＯＳ／ＤＤＯＳ攻撃検出処理を終了し、通常のｐｋｔ受信処理を行う。

【００４８】
ステップＳ１０で、一致するものがあった場合には、そのｐｋｔ受信数を＋１し、図７のテーブルに保持する。この際、ＰＫＴ受信数が図７の異常検出閾値以上となった場合には、図５を参照し、図５の連携対象ルータへのフィルタリング適用指示動作を開始する。

【００４９】
異常検出を行った場合には、この異常ＰＫＴを以降ルータ側で破棄する必要があるか否かを図５のテーブルを用いて判断する。図５にエントリが１つでも存在した場合には、各エントリに指定されたルータに対するフィルタリング適用指示を開始する（ステップＳ１２）。

【００５０】
ステップＳ１２の処理において、各ルータにフィルタリング適用指示をコマンドとして指示するための準備処理として、図５のテーブルを用いて、各ルータへのtelnetまたはｓｓｈによる接続を行う。このときの、ルータに対する接続手順、ポート番号、制御用ＩＰアドレス、アカウント・パスワード情報は、全て図５の情報を使用する（ステップＳ１３及びＳ１４）。

【００５１】
上記処理で、図５の現在処理中のエントリに対応するルータとの接続が完了した場合には、そのルータの種別を図５より抽出し、その種別情報をキーとして図６のエントリを検索し、該当ルータ種別エントリのフィルタリングルールコマンドsyntaxを図５より求める（ステップＳ１５）。

【００５２】
図５のルータフィルタリング番号より、図８で現在当該ルータに使用しているルール番号以外の番号を抽出し、ステップＳ１５で求めたコマンドsyntaxに本番号と、ステップＳ１０で異常検出した受信ＰＫＴの送信元ＩＰアドレスをフィルタリング対象として適用し、そのルータが解釈可能なフィルタリングルールコマンドとして発行を行い、当該ルータへのルール設定を完了する（ステップＳ１６）。

【００５３】
更に、このフィルタリングルールコマンドを、当該ルールで破棄動作の適用として登録するために、フィルタリング適用コマンドを発行する必要があるが、この際ルータによっては、図５のＤＯＳ防御対象インターフェースの説明で記述したように、特定のインター

フェースに適用する必要がある場合と、ルータの全インターフェースに適用可能な場合があるため、その設定がどうなっているかを図５の当該情報を参照し判断する（ステップＳ１７）。ステップＳ１７の判断がＮＯの場合には、ステップＳ２０に進み、ステップＳ１７の判断がＹＥＳの場合には、ステップＳ１８に進む。

【００５４】

図５のＤＯＳ防御対象インターフェースでインターフェース指定となっていた場合には、本フィールドからインターフェース名を抽出し、かつ、図６のインターフェースコマンド指定形式を当該ルータのルータ種別の一致するエントリから抽出し、当該ルータに対し、インターフェース指定コマンドを発行する（ステップＳ１８及びＳ１９）。

【００５５】

当該ルータに対し、そのルータのフィルタリング適用コマンドsyntaxを図６のルータ種別の一致するエントリから抽出し、ステップＳ１６で設定したフィルタリングルールコマンドのルール番号と合わせて、ルータに適用指示を行う（ステップＳ２０及びＳ２１）。

【００５６】

ステップＳ２１の処理を完了した場合、更に図５のエントリで未実施のルータがあれば、ステップＳ１２の処理から処理を繰り返し実施し、図５の全エントリに対する処理が完了した場合に、本処理を完了する。

【００５７】

図１０及び図１１は、図９において、ＦＷでのＤＯＳ／ＤＤＯＳ攻撃検出からルータへのフィルタリング指示を行った後に、その継続状態の確認及び攻撃がおさまった場合の解除までの流れを示すフローチャートである。

【００５８】

ＦＷは予め決められた監視時間間隔（運用管理者による設定変更可能）で、ＤＯＳ／ＤＤＯＳ攻撃の継続の有無を確認する（ステップＳ２５）ステップＳ２５において、監視時間間隔が経過していない場合には、処理を終了する。ステップＳ２５において、監視時間間隔が経過したと判断された場合には、ステップＳ２６に進む。

【００５９】

ＦＷ装置内の図８のテーブルにおいて、検出時刻の設定されたエントリが存在するか否かを判断する（ステップＳ２６）。ステップＳ２６の判断がＮＯの場合には処理を終了する。ステップＳ２６の判断がＹＥＳの場合には、ステップＳ２7に進む。

【００６０】

ＦＷ装置内の図８のテーブルにおいて、検出時刻の設定されたエントリが存在する場合、その検出ルールとして該当する図７のエントリを参照し、遮断解除時間を確認し、手動となっていないエントリであるかを確認する（ステップＳ２７）

ステップＳ２７で自動解除となっていた場合には、図８の該当エントリの検出時間に図７の該当エントリの遮断解除時間を加えたものが、現時刻以上となっているかを確認する（ステップＳ２８）。ステップＳ２7で自動解除となっていなかった場合には、ステップＳ２６に戻って、次のエントリの処理を行う。

【００６１】

ステップＳ２８で指定時間経過していた場合は、図５に保持する連携対象ルータで、現在、図８で確認中のエントリに対する攻撃が継続しているかを確認するための処理を開始する（ステップＳ２9）。ステップＳ２８において、指定時間経過していない場合には、ステップＳ２６に進み、次エントリの処理に進む。

【００６２】

ステップＳ２9における判断がＮＯの場合には、ステップＳ３５に進む。

ステップＳ３０～Ｓ３１で、図５の各ルータに対しても接続を図９のステップＳ１３～Ｓ１４と同様に行い、図６の該当ルータエントリの状態参照コマンドのsyntaxを抽出し、コマンドを発行する（ステップＳ３２及びＳ３３）。

【００６３】

上記で発行した状態参照コマンドの内容から、図８の当該エントリに対する図５での当

該ルータからのｐｋｔ削除数を取り出し、図８で前回当該ルータから取り出したｐｋｔ削除数と比較し、その増加分を図８の当該エントリに書き込む（ステップＳ３４）。

【００６４】

上記処理を図５の全ルータに対し実施した後、ステップＳ３３で求めた図８の当該エントリでの各ルータのｐｋｔ破棄数の総和が、図７の当該エントリの異常検出閾値未満であるかを確認し、閾値未満である場合には、破棄解除状態への遷移を行うため、以下の処理を行う。また、閾値以上であった場合には、破棄状態を継続する必要があるため、何もせず、図８の次のエントリに対する確認処理を継続するため、ステップＳ２６に戻る。

【００６５】

ステップＳ３５において、破棄状態解除が必要となった場合には、図５内の各ルータに対し、接続・フィルタリング適用解除コマンド投入・フィルタリングルール解除コマンドの投入を行う。

【００６６】

すなわち、図１１のステップＳ３６において、連携対象ルータがあるか否かを判断する。ステップＳ３６の判断がＮＯの場合には、図１０のステップＳ２６に戻る。ステップＳ３６の判断がＹＥＳの場合、ステップＳ37において、連携対象のルータでアカウント、パスワード、接続手順、接続ポート番号を抽出し、対象ルータに接続する。ステップＳ３８において、連携対象のルータでＤＯＳ防御インターフェースの指示があるか否かを判断する。ステップＳ３８の判断がＮＯの場合には、ステップＳ４０に進み、ＹＥＳの場合には、ステップＳ39に進む。

【００６７】

ステップＳ39においては、対象ルータのインターフェースをコマンド指示する。ステップＳ４０においては、対象ルータのフィルタリング適用解除指示コマンドを生成及び投入する。ステップＳ４１において、ルータでのフィルタリングルール解除コマンドを生成及び投入し、ステップＳ３６に戻る。　本発明の実施形態によれば、以下のような効果がある。

【００６８】

ファイアウォールでの異常検出時、自動的にルータに当該トラフィックの廃棄を指示するため、ＤＯＳ攻撃が長時間継続しても、ファイアウォールの性能が劣化することなく、通信を継続することが可能となる。

【００６９】

本発明の実施形態によれば、以下の効果が得られる。

運用管理者は、ファイアウォールのパケット破棄状態を確認するだけで、不当アクセスの継続可否を判断でき、複数の装置を確認した結果から判断を下す必要が無くなり、確認に要する時間の短縮及び、判断誤りを減少することが可能となる。

【００７０】

運用管理者が、事前に設定した不当アクセス状態解除条件（時間、閾値）を設定するだけで、ファイアウォールの判断により、ファイアウォール自身及びルータでのパケット廃棄状態から、自動的に正常状態に復帰するため、運用管理者の管理コストを削減できる。

【００７１】

ファイアウォールがＤＯＳ／ＤＤＯＳ攻撃を検知し、通信路上でトラフィックが多発している状態においても、ルータに対するフィルタリングポリシーの設定を保証でき、運用停止となる時間を防止することが可能となる。

【００７２】

複数のルータを経由してファイアウォールと接続されている場合において、ＤＯＳ／ＤＤＯＳ攻撃をファイアウォールで検出時に全ルータにフィルタリングポリシーを適用することにより、運用停止となる時間を防止することが可能になる。

（付記１）外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御装置において、

アクセス元のアドレスを指定して、ハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータと、
設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータ手段に送信し、フィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールと、
を備えることを特徴とする不正アクセス制御装置。

【００７３】

（付記２）前記ルータに設定したフィルタリングのポリシーに基づき、該ルータ手段でのパケットの破棄状況について、前記ファイアウォールから定期的に情報収集することを特徴とする付記１に記載の不正アクセス制御装置。

【００７４】

（付記３）前記ルータから収集した破棄情報を基に、破棄パケット数が所定の閾値を下回るか否かを判断し、下回った場合には、該ルータに対してパケット破棄を中止させることを特徴とする付記２に記載の不正アクセス制御装置。

【００７５】

（付記４）前記ルータとファイアウォール間で該ファイアウォールから該ルータへのパケット破棄の自動設定をするための専用通信を設けることを特徴とする付記１に記載の不正アクセス制御装置。

【００７６】

（付記５）１つの前記ファイアウォールが、複数の前記ルータのパケット破棄設定を行うことを特徴とする付記１または４に記載の不正アクセス制御装置。
（付記６）前記ファイアウォールは、現用装置と待機装置からなり、現用装置がダウンした場合には、待機装置が現用装置に代わって現用装置の機能を果たすことを特徴とする付記１に記載の不正アクセス制御装置。

【００７７】

（付記７）前記ファイアウォールは、パケットを受信し、前記不正なアクセスの攻撃があったか否かを判断し、該ファイアウォールと連携したルータがあるか否かを判断し、連携対象のルータにおいて、防御すべきインターフェースが指定されているかを判断し、該ルータにパケットの破棄処理を設定することを特徴とする付記１に記載の不正アクセス制御装置。

【００７８】

（付記８）前記ファイアウォールは、前記ルータへのフィルタリング指示後に、攻撃の継続状態及び攻撃が収まったか否かを監視することを特徴とする付記１に記載の不正アクセス制御装置。

【００７９】

（付記９）外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御方法において、
アクセス元のアドレスを指定して、ルータのハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータステップと、
設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータに送信し、該ルータにフィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールステップと、
を備えることを特徴とする不正アクセス制御方法。

【００８０】

（付記１０）外部のネットワークに接続されたルータとルータに接続されたファイアウォールとが連携して不正アクセスを制御する不正アクセス制御方法において、

アクセス元のアドレスを指定して、ルータのハードウェアのレベルで、当該アドレスから送られてくるパケットを破棄するルータステップと、
設定されたアクセス制御ポリシーに基づいて、不正アクセスを検出し、検出した不正アクセスの発信元のアドレスを特定し、不正アクセスの発信元のアドレスを遮断するための該ルータへのコマンドを該ルータに送信し、該ルータにフィルタリングのポリシー設定をすることによって、該ルータが不正アクセスのアドレスからのパケットを破棄するよう自動的に設定するファイアウォールステップと、
を備えることを特徴とする不正アクセス制御方法をコンピュータに実現させるプログラム。

【図面の簡単な説明】

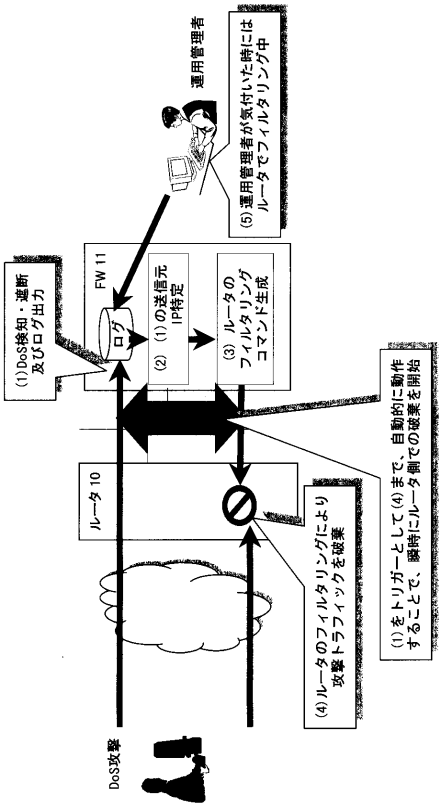
【００８１】
【図１】本発明の実施形態に従ったファイアウォールでＤＯＳ攻撃検出時の動作を説明する図である。
【図２】本発明の実施形態に従ったファイアウォールでのＤＯＳ攻撃検出後の動作を説明する図である。
【図３】本発明の実施形態に従ったＤＯＳ攻撃停止時の動作を説明する図である。
【図４】本発明の実施形態の動作環境に関する説明図である。
【図５】ファイアウォールに環境定義情報として運用管理者が設定する情報をテーブルとして表した図である。
【図６】本発明の実施形態に従った、ＦＷ装置のファームウェア、あるいは、ソフトウェアとして装置自身に登録されている情報の例を示す図である。
【図７】運用管理者が、ＦＷ装置に対して、ＦＷ装置が提供するＤＯＳ／ＤＤＯＳ防御機能の使用の有無をポリシーとして設定したＦＷ内部のテーブルの例を示す図である。
【図８】ＤＯＳ／ＤＤＯＳ攻撃をＦＷで検出している状態、及び、ルータに対する指示状態を管理するためにＦＷ内部に保持するテーブルの例を示す図である。
【図９】ＦＷでのＤＯＳ／ＤＤＯＳ攻撃検出からルータへのフィルタリング指示までのＦＷ側での動作の流れを示すフローチャートである。
【図１０】図９において、ＦＷでのＤＯＳ／ＤＤＯＳ攻撃検出からルータへのフィルタリング指示を行った後に、その継続状態の確認及び攻撃がおさまった場合の解除までの流れを示すフローチャート（その１）である。
【図１１】図９において、ＦＷでのＤＯＳ／ＤＤＯＳ攻撃検出からルータへのフィルタリング指示を行った後に、その継続状態の確認及び攻撃がおさまった場合の解除までの流れを示すフローチャート（その２）である。

【符号の説明】

【００８２】
１０　ルータ
１０－１　ルータ１
１０－２　ルータ２
１０－３　ルータ３
１１　ファイアウォール（ＦＷ）
１１－１　ファイアウォール現用
１１－２　ファイアウォール待機
１５　外部ネットワーク

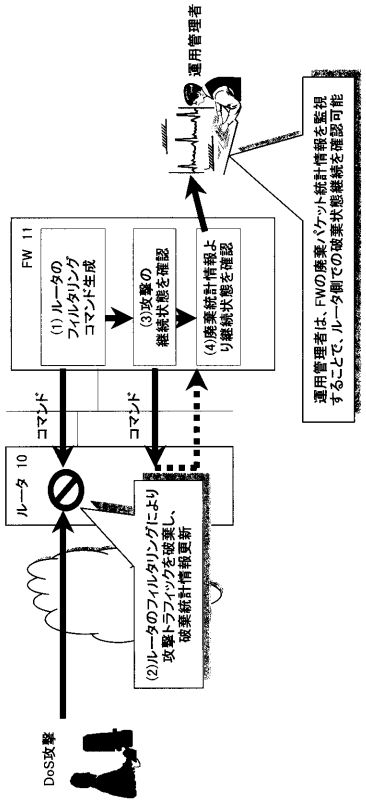
【図１】

本発明の実施形態に従ったファイアウォールで
DOS攻撃検出時の動作を説明する図



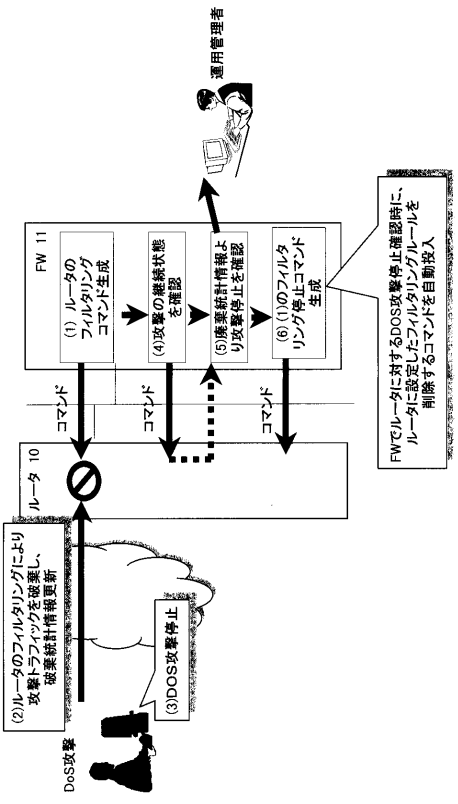
【図２】

本発明の実施形態に従ったファイアウォールでの
DOS攻撃検出後の動作を説明する図



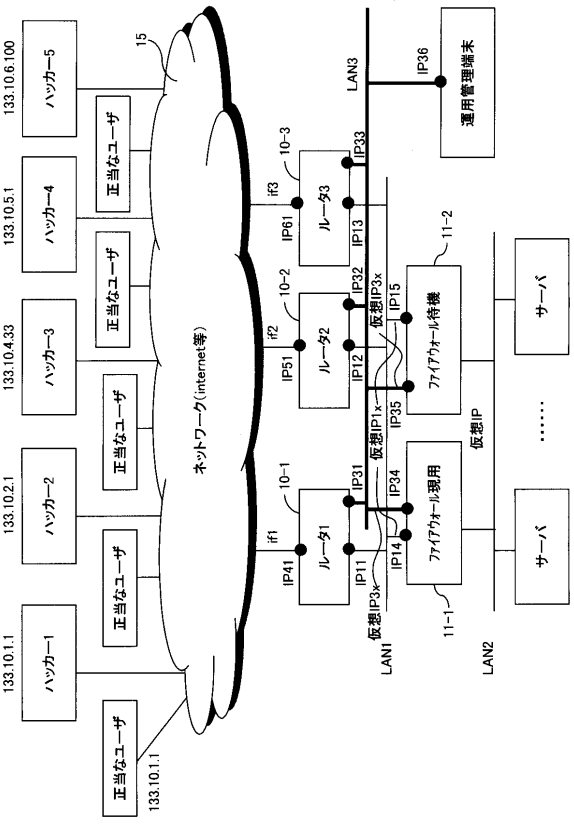
【図３】

本発明の実施形態に従った
DOS攻撃停止時の動作を説明する図



【図４】

本発明の実施形態の動作環境に関する説明図



【図５】

ファイアウォールに環境定義情報として運用管理者が設定する情報をテーブルとして表した図

連携対象ルータ	制御用IPアドレス	制御用アカウント	制御用パスワード	ルータ種別	DOS防御対象インタフェース	フィルタリングルール番号	接続手順	接続ポート番号
ルータ1	IP31	admin1	adminpwd1	routerA	if1	1000-1099	telnet	23
ルータ2	IP32	admin2	adminpwd2	routerB	if2	1200-1399	ssh	22
ルータ3	IP33	admin3	adminpwd3	routerC	特定せず	1000-1909	ssh	10022

【図６】

本発明の実施形態に従った、FW装置のファームウェア、あるいは、ソフトウェアとして装置自身に登録されている情報の例を示す図

ルータ種別	フィルタリングルールコマンド	ルール適用コマンド	状態参照コマンド	フィルタリングルール解除コマンド	ルール適用解除コマンド	インタフェース指定コマンド
routerA	access-list <NUM> deny <IF> src <ADDR>	filter-list <NUM> in	Show access-list <NUM> statistics	no access-list <NUM>	no filter-list <NUM>	interface
routerB	Access deny <NUM> ownip <IP> host <ADDR>	filter <NUM> <IF> in	show Access	no access <NUM>	no filter <NUM>	if

【図７】

運用管理者が、FW装置に対して、FW装置が提供するDOS／DDOS防御機能の使用の有無をポリシーとして設定したFW内部のテーブルの例を示す図

検出DOS攻撃種別	検出DOS攻撃内容詳細	異常検出閾値	遮断可否	遮断解除時間
不正IPパケット受信	不正IPバージョン	10PKT/S	遮断	24H
不正TCPパケット受信	不正ポート番号	—	遮断せず	—
…	…	…	…	…
Ping of Death攻撃	Ping of Death攻撃	20PKT/S	遮断	24H
Nimudaワーム	http_path[に“/cmd.exe?”, “/root.exe?”, “/readme.exe?” を含むURI存在	即時	遮断	手動
I LOVE YOU ウィルス	SMTP subject:=“I LOVE YOU”	即時	遮断	48H

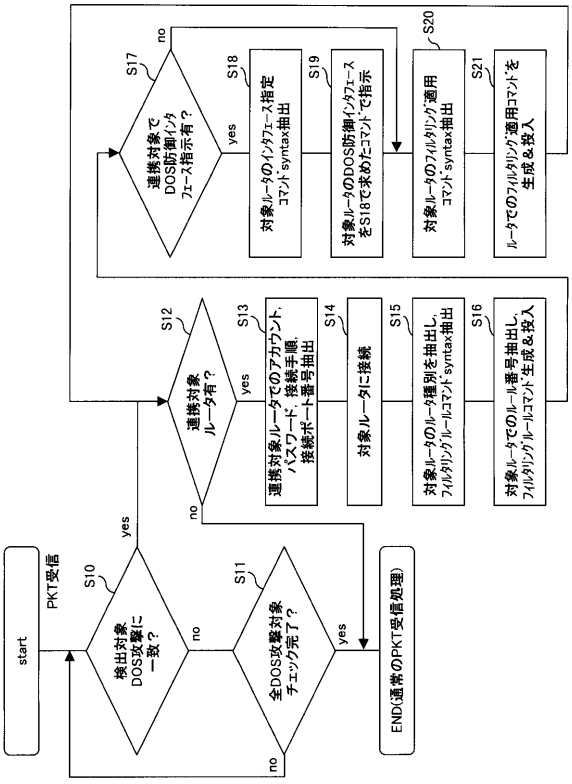
【図８】

DOS／DDOS攻撃をFWで検出している状態、及び、ルータに対する指示状態を管理するためにFW内部に保持するテーブルの例を示す図

検出DOS攻撃種別	検出DOS攻撃内容詳細	検出時刻	検出対象IPアドレス	ルータ1ルール番号	ルータ2ルール番号	ルータ3ルール番号
不正IPパケット受信	不正IPバージョン	2003.11.01 11:01:11	133.10.1.1	1000	1200	1000
不正TCPパケット受信	不正ポート番号	—	—	—	—	—
…	…	…	…	…	…	…
Ping of Death攻撃	Ping of Death攻撃	2003.11.01 12:22:01	133.10.2.1 133.10.4.33 133.10.5.1	1001 1002 1003	1201 1202 1203	1001 1002 1003
Nimudaワーム	http_path[に“/cmd.exe?”, “/root.exe?”, “/readme.exe?” を含むURI存在	none	none	—	—	—
I LOVE YOU ウィルス	SMTP subject:=“I LOVE YOU”	2003.11.01 16:33:00	133.10.6.100	1004	1204	1004

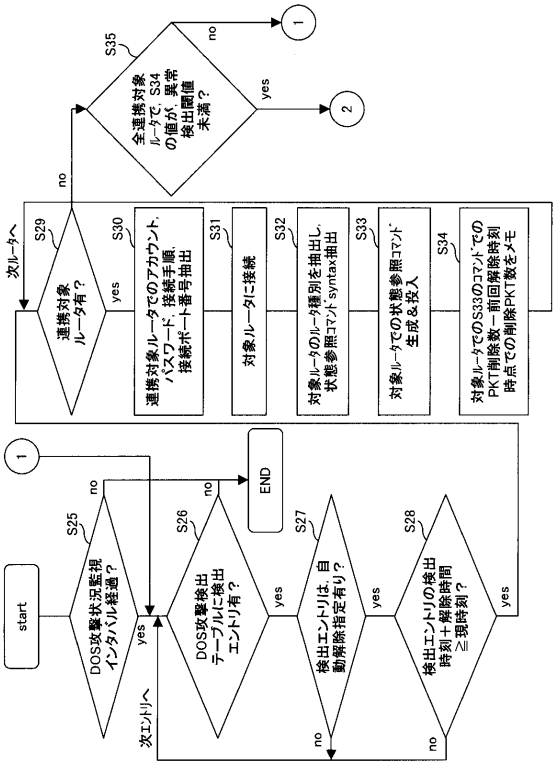
【図９】

FWでのDOS／DDOS攻撃検出からルータへのフィルタリング指示までのFW側での動作の流れを示すフローチャート



【図１０】

図9において、FWでのDOS／DDOS攻撃検出からルータへのフィルタリング指示を行った後に、その継続状態の確認及び攻撃がおさまった場合の解除までの流れを示すフローチャート（その1）



【図１１】

図9において、FWでのDOS／DDOS攻撃検出からルータへのフィルタリング指示を行った後に、その継続状態の確認及び攻撃がおさまった場合の解除までの流れを示すフローチャート（その2）