(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2007-325293
(P2007-325293A)
(43)公開日　平成19年12月13日(2007.12.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5B089
G06F 13/00	(2006.01)	G06F	13/00	351Z	5B285
G06F 21/20	(2006.01)	G06F	15/00	330A	5K030

審査請求 有　請求項の数 3　ＯＬ　（全 64 頁）

(21)出願番号　特願2007-179436 (P2007-179436)
(22)出願日　平成19年7月9日 (2007.7.9)
(62)分割の表示　特願2005-263858 (P2005-263858)の分割
原出願日　平成15年8月19日 (2003.8.19)
(31)優先権主張番号　特願2002-238989 (P2002-238989)
(32)優先日　平成14年8月20日 (2002.8.20)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2003-74781 (P2003-74781)
(32)優先日　平成15年3月19日 (2003.3.19)
(33)優先権主張国　日本国(JP)

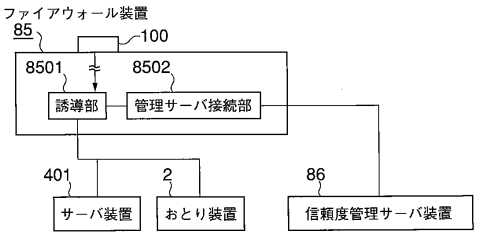
特許法第３０条第１項適用申請有り　２００２年１２月２０日　社団法人情報処理学会主催の「情報処理学会研究報告」において文書をもって発表

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100097157
弁理士　桂木　雄二
(72)発明者　中江　政行
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　山形　昌也
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B089 KA17
5B285 AA05 AA06 BA01 CA32 CA34 DA04
5K030 GA15 HA08 HD03 HD06 JA10 LC13 MA04 MC08

(54)【発明の名称】攻撃検知システムおよび攻撃検知方法

(57)【要約】
【課題】インターネットから内部ネットワークへのアクセスでＳＳＬなど通信路暗号化技術が用いられた場合であっても不正なアクセスを検知し有効に防御する攻撃検知システム及び方法を提供する。
【解決手段】ファイアウォール装置８５と、おとり装置２と、信頼度管理サーバ８６と、を有し、ファイアウォール装置８５は入力ＩＰパケットもしくはその一部のデータを含む要求メッセージを信頼度管理サーバ８６へ送信し、信頼度管理サーバ８６は、要求メッセージに応じて、当該要求メッセージに含まれるデータから入力ＩＰパケットに対する信頼度を生成し、信頼度を少なくとも含む応答メッセージをファイアウォール装置８５へ返信する。
【選択図】図６６



【特許請求の範囲】
【請求項１】
内部ネットワークと外部ネットワークとの境界に設置された攻撃防御システムにおいて、
ファイアウォール装置と、
おとり装置と、
少なくとも１つの信頼性管理サーバと、
を有し、
前記ファイアウォール装置は入力ＩＰパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、
前記信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力ＩＰパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、
ことを特徴とする攻撃防御システム。
【請求項２】
内部ネットワークと外部ネットワークとの境界に設置され、ファイアウォール装置と、おとり装置と、少なくとも１つの信頼性管理サーバと、を有する攻撃防御システムにおける攻撃防御方法において、
前記ファイアウォール装置は入力ＩＰパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、
前記信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力ＩＰパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、
ステップを有することを特徴とする攻撃防御方法。
【請求項３】
内部ネットワークと外部ネットワークとの境界に設置され、ファイアウォール装置と、おとり装置と、少なくとも１つの信頼性管理サーバと、を有する攻撃防御システムにおける前記信頼性管理サーバをコンピュータに実装するためのプログラムにおいて、
前記ファイアウォール装置から入力ＩＰパケットもしくはその一部のデータを含む要求メッセージを受信し、
前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力ＩＰパケットに対する信頼度を生成し、
前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、
ステップを有することを特徴とする攻撃防御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はコンピュータネットワークにおけるセキュリティ対策に係り、特に外部ネットワークからの攻撃に対して内部ネットワーク上の資源を保護するためのシステムおよび方法に関する。
【背景技術】
【０００２】
従来、外部ネットワークからの攻撃に対する防御技術として、（１）ファイアウォール、（２）侵入検知システム、（３）おとりシステム、といった手法があった。
【０００３】
ファイアウォールの一例は、たとえば特開平８－４４６４２号公報（特許文献１）に開示されている。外部のＩＰネットワークと内部のイーサネット（登録商標）との境界にファイアウォールを設置し、検査対象となるパケットを外部ネットワークから内部ネットワークに通過させてよいか否かを判定する。特に、ファイアウォールにパケットフィルタを設け、パケットのヘッダ情報（送信元アドレスや送信先アドレス）などの他、プロトコル

の種別（ＴＣＰ／ＵＤＰ／ＨＴＴＰなど）や、データ内容（ペイロード）なども参照しながら、所定のルールに従って、パケットの通過可否を判定する。適切なルールを設定しておけば、例えば、外部ネットワーク一般に公開されているＷｅｂサーバなどに対してワームなどを含む不正なパケットが進入することを遮断できる。

【０００４】

侵入検知システムの一例は、たとえば特開２００１－３５０６７８号公報（特許文献２）に開示されている。この従来の侵入検知システムは不正侵入判定ルール実行部を有し、アプリケーションごとの判定ルール、例えばＷＷＷサーバ用不正侵入判定ルールやＭＡＩＬサーバ用不正侵入判定ルールを備えている。まず、ＩＰアドレステーブル取得部は、内部ネットワーク上を流れるパケットの送信元ＩＰアドレスもしくは送信先ＩＰアドレスから、当該ＩＰアドレスを持つサーバにおいて現在動作中のアプリケーションを決定する。次に、不正侵入判定ルール実行部において、そのアプリケーションに応じた不正侵入判定ルールを実行し、当該パケットが不正であるか否かを判定する。こうすることにより、アプリケーションに依存したより精度の高い侵入検知が可能となる。

【０００５】

おとりシステムの第１例は、たとえば特開２０００－２６１４８３号公報（特許文献３）に開示されている。この従来のおとりシステムは、ルータ１０の下に構築された内部ネットワーク上に、トラフィック監視装置、攻撃パターンおよび偽装サーバを備える。まず、トラフィック監視装置において、内部ネットワーク上を流れるパケットを監視しながら、特定の攻撃パターンに合致するものを不正パケットとして検出し、その識別情報（送信元ＩＰアドレス、送信先ＩＰアドレスなどを含む）をルータに通知する。次に、ルータでは、後に続く外部ネットワークからのパケットについて、検出した識別情報に合致するパケットをすべて偽装サーバに転送する。偽装サーバは、転送されたパケットを適切に解釈し、内部ネットワーク上の正規のサーバをまねた偽の応答パケットを生成し、先に不正パケットを送信したホストへ向けて、その偽の応答パケットを送信する。こうすることで、外部ネットワーク上に存在する攻撃者に、内部ネットワークに悪影響のない形で、攻撃を続けさせることができ、逆探知によって攻撃者の身元を明らかにすることができる。

【０００６】

おとりシステムの第２例は、たとえば特開２００２－７２３４号公報（特許文献４）に開示されている。この従来のおとりシステムは、内部ネットワークと外部ネットワーク（インターネット）との境界に、いわゆるゲートウェイとして、不正検出サーバと、おとりサーバと、を備える。外部ネットワークから内部ネットワークへ流れるパケットを不正検出サーバで監視し、例えば、当該パケットのペイロードについて所定のパターンマッチング処理を行うなどして、不正か否かを判定する。不正であると判定されたパケットには、その旨を示す特殊なマークを加えた上で、当該パケットをおとりサーバもしくは内部ネットワーク上の情報処理サーバへ転送する。情報処理サーバへ不正パケットを転送する場合、予め情報処理サーバに不正回避処理部を持たせておき、特殊なマークのあるパケットを受信した際には、さらにおとりサーバへ当該パケットを転送するようにしておく。いずれにせよ、不正検出サーバで検出された不正パケットは、最終的におとりサーバへ到達する。その後、おとりサーバでは、偽の応答パケットを生成し、不正パケットの送信元ホストに向けて、当該応答パケットを送信する。こうすることで、不正と判定されたパケットを全ておとりサーバに閉じ込めることができる。

【０００７】

さらに、おとりシステムの第３例は、たとえば特開平０９－２２４０５３号公報（特許文献５）に記載されている。この従来のおとりシステムは、公衆ネットワーク（インターネット）と、プライベートネットワーク（内部ネットワーク）との境界に、スクリーン・システムおよび代行ネットワークを備える。スクリーン・システムは、自身に接続される各ネットワークからの着信パケットについて、パケットのヘッダに記載される情報や着信履歴など基にしたスクリーン基準に従い、フィルタリングを行う。ただし、スクリーン・システムの通信インタフェースはＩＰアドレスをもたず、ｔｒａｃｅｒｏｕｔｅなどを用

いた探索から自身を隠蔽することを特徴の１つとする。もう１つの特徴として、プライベートネットワークに向かう着信パケットについて、代行ネットワークに経路を変更することもできる。代行ネットワーク上には０台以上の代行ホストが設けられ、プライベートネットワーク上にあるホストの代理として動作させることもできる。こうすることで、公衆ネットワークからの攻撃からプライベートネットワークを保護できる。

【０００８】

【特許文献１】特開平８－４４６４２号公報（段落番号００２９～００３０、図５）

【特許文献２】特開２００１－３５０６７８号公報（段落番号００６２～００８４、図１）

【特許文献３】特開２０００－２６１４８３号公報（段落番号００２４～００３０、図１）

【特許文献４】特開２００２－７２３４号公報（段落番号００３６～００４０、図１、図２）

【特許文献５】特開平０９－２２４０５３号公報（段落番号００３７～００４３、００６６～００６７、図６）。

【発明の開示】

【発明が解決しようとする課題】

【０００９】

しかしながら、上記従来の技術は、いずれも、次に挙げるような問題点を持つ。

【００１０】

第１の問題点は、外部ネットワーク上の攻撃ホストと内部ネットワーク上のサーバとの間で、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）やＩＰＳｅｃ（ＲＦＣ２４０１記載）などの通信路暗号化技術が用いられた場合に、攻撃を有効に検知または防御できないということである。その理由は、攻撃検知のための主要なデータ（ペイロードなど）が暗号化されており参照できないためである。

【００１１】

第２の問題点は、攻撃検知部のパフォーマンスが、近年のネットワークの高速化に追随しきれず、検査から漏れるパケットが存在したり、ネットワークの高速性を損なったりする点にある。その理由は、攻撃検知の精度を向上するには、より多彩な、あるいはより複雑な判定ルールの実行が必要であるが、一方、ネットワークの高速化により、検査対象となるパケット量が飛躍的に増加しているためである。

【００１２】

また、特許文献２および特許文献３に記載された侵入検知システムやおとりシステムの第１例では、少なくとも１つの不正パケットが、内部ネットワーク上の保護すべきサーバに到達してしまう。その理由は、攻撃検知部が検査を行うのは、パケットのコピーでしかなく、当該パケットが不正と判定された場合でも、その内部ネットワーク上のパケット流通を遮断できないためである。

【００１３】

さらに、特許文献５に記載されたおとりシステムの第３例では、インターネットから到来したパケットを代行ネットワークに経路変更させる条件および方法については検討されていない。このために、正確にパケットを振り分けることができず、正常なアクセスが代行ネットワークへ、異常なアクセスが内部ネットワークへ導かれる可能性がある。

【００１４】

第３の問題点は、攻撃検知精度の向上が困難な点にある。近年のサーバ運用の形態は、遠隔からの保守作業が一般的であり、その作業はサーバ内のデータ修正やシステムの更新などであり、侵入検知システムはこうした保守作業をしばしば攻撃と誤って検知してしまう。

【００１５】

また、Webアプリケーション等で知られるように、サーバのサブシステムとして、データベース操作など様々なアプリケーションプログラムを動作させることが多く、そうした

サブシステムの脆弱性を突いて不正動作を行わせる攻撃も頻繁に見られるようになった。侵入検知システムは、一般によく知られるサーバまたはそのサブシステムへの攻撃パターンを知識として備えるが、サイト独自に作成されたサブシステムが存在する場合や、一般的なサーバまたはサブシステムであっても設定に不備がある場合には、前記攻撃パターンに当てはまらない、いわゆる未知攻撃を受ける危険性がある。

【００１６】

第４の問題点は、データベースやプラグインモジュールなどのサブシステムを備えるサーバシステムにおいて、クライアントとの通信プロトコルで、一定のアクセス手順が規定されている場合（すなわちステートフルプロトコルであった場合）、不審なアクセスのみをおとりサーバなど、正規のサーバ以外に誘導する方法では、おとりサーバと正規のサーバ双方でクライアントーサーバ通信が失敗する。特に、誤っておとりサーバへ誘導されたアクセスがあった場合には、正規のサーバ上であるべき処理が行われないため、サーバ障害を発生させることになる。

【００１７】

本発明の目的は、通信路暗号化技術を用いた通信システムに対しても、外部ネットワークからの攻撃を有効に防御できる攻撃検知方法ならびに攻撃防御システムを提供することにある。

【００１８】

本発明の他の目的は、高速ネットワーク環境に対応できる攻撃検知方法ならびに攻撃防御システムを提供することにある。

【００１９】

本発明のさらに他の目的は、保護すべきサーバに向けられた不正パケットを確実に遮断できる攻撃検知方法ならびに攻撃防御システムを提供することにある。

【課題を解決するための手段】

【００２０】

本発明による攻撃防御システムは、内部ネットワークと外部ネットワークとの境界に設置され、ファイアウォール装置と、おとり装置と、少なくとも１つの信頼性管理サーバと、を有し、前記ファイアウォール装置は入力ＩＰパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、前記信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力ＩＰパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、ことを特徴とする。

【００２１】

本発明による攻撃防御方法は、内部ネットワークと外部ネットワークとの境界に設置され、ファイアウォール装置と、おとり装置と、少なくとも１つの信頼性管理サーバと、を有する攻撃防御システムにおいて、前記ファイアウォール装置は入力ＩＰパケットもしくはその一部のデータを含む要求メッセージを前記信頼性管理サーバへ送信し、前記信頼性管理サーバは、前記要求メッセージに応じて、当該要求メッセージに含まれるデータから前記入力ＩＰパケットに対する信頼度を生成し、前記信頼度を少なくとも含む応答メッセージを前記ファイアウォール装置へ返信する、ステップを有することを特徴とする。

【発明の効果】

【００２２】

以上詳細に説明したように、本発明によれば、ＩＰアドレスの信頼度により、外部ネットワークから内部ネットワークへのアクセスにおいて通信路暗号化技術が用いられた場合でも、攻撃を検知および防御することができる。

【００２３】

いかなる通信路暗号化技術が用いられたとしても、少なくともＩＰヘッダに記載されたソースＩＰアドレスもしくはディスティネーションＩＰアドレスは暗号化されず、さらにファイアウォール装置による攻撃検知装置（おとり装置）への誘導は、これらＩＰヘッダに記載された情報を基に行うことができる。

【００２４】
また、本発明によれば、ファイアウォール装置によるおとり装置への誘導方法が少ないパラメータを基にした簡易なアルゴリズムで実現できるため、高速ネットワーク環境においても、ネットワーク性能を高いレベルで維持できる。
【００２５】
さらに、本発明によれば、おとり装置へ誘導されて攻撃が検出された全てのパケットについて、その送信元ホストからの以降のアクセスを拒否するように動的な防御を行うことで後続する攻撃を全てファイアウォール装置で防御することができる。このために内部ネットワークへの通信経路が無くなり、検出された攻撃用パケットが一切内部ネットワークに到達しない。
【発明を実施するための最良の形態】
【００２６】
（ネットワーク構成）
図１は、本発明による攻撃防御システムの概略的ブロック図である。本発明による攻撃防御システムは、基本的に、ファイアウォール装置１およびおとり装置２を有し、インターネット３と内部ネットワーク４との境界にファイアウォール装置１が設置されている。内部ネットワーク４は、ＷＷＷ（World-Wide Web）などのサービスを提供する１個以上のサーバ装置４０１を含む。ここではインターネット３に攻撃元ホスト３０１が想定されている。
【００２７】
ファイアウォール装置１は、通常の正規のパケットであれば、これを通過させて内部ネットワーク４へ送付し、不正パケットあるいは不審なパケットであれば、おとり装置２へ誘導する。おとり装置２は攻撃の有無を検知し、攻撃を検知した場合にはアラートをファイアウォール装置１へ出力する。また、不正パケットに対する偽の応答パケットを生成してファイアウォール装置１へ返してもよい。ファイアウォール装置１はその偽の応答パケットを不正パケットの送信元である攻撃元ホスト３０１へ送信する。
【００２８】
（第１実施形態）
１．１）構成
図２は、本発明の第１実施形態による攻撃防御システムのファイアウォール装置１およびおとり装置２の構成を示すブロック図である。ファイアウォール装置１は、外部通信インタフェース１００でインターネット３と接続され、第１の内部通信インタフェース１０４で内部ネットワーク４と接続される。
【００２９】
パケットフィルタ１０１は、外部通信インタフェース１００および誘導部１０３の間に接続され、アクセス制御リスト管理部１０２から取得したアクセス制御ルールに従ってパケットフィルタリングを行う。すなわち、後述するように、パケットフィルタ１０１は外部通信インタフェース１００および誘導部１０３の一方から受け取ったＩＰパケットを他方へ転送し、あるいは転送せずに廃棄する。
【００３０】
パケットフィルタ１０１で受理されたパケットは誘導部１０３へ送られ、誘導部１０３は、後述する誘導リスト（図５）を参照し、パケットフィルタ１０１から入力したＩＰパケットの宛先ＩＰアドレスに応じて当該パケットを第１の内部通信インタフェース１０４および第２の内部通信インタフェース１０５のいずれかへ誘導する。逆に、第１の内部通信インタフェース１０４または第２の内部通信インタフェース１０５からインターネット３に向かうＩＰパケットをパケットフィルタ１０１に転送する。
【００３１】
第１の内部通信インタフェース１０４は、誘導部１０３から入力したＩＰパケットを内部ネットワーク４に伝達し、内部ネットワーク４からインターネット３に向かうＩＰパケットを誘導部１０３へ伝達する。第２の内部通信インタフェース１０５は、誘導部１０３

によって誘導されたＩＰパケットをおとり装置２に伝達し、おとり装置２からインターネット３に向かうＩＰパケットを誘導部１０３に伝達する。

【００３２】

おとり装置２は、プロセッサ２０１と攻撃検知部２０２とを含む。プロセッサ２０１は、ＷＷＷやＴｅｌｎｅｔなどのネットワークサービスを提供するプロセスを実行しながら、当該プロセスの状況を攻撃検知部２０２へ随時伝達する。攻撃検知部２０２は、プロセッサ２０１から入力されるプロセス状況を監視しながら、攻撃の有無を検査し、攻撃が認められた場合には攻撃内容を報告するためのアラートを生成しファイアウォール装置１へ送出する。

【００３３】

制御インタフェース１０６を通してアラートを入力すると、防御ルール判定部１０７は、アラートの内容に従ってアクセス制御リスト管理部１０２のアクセス制御リストの更新等を指示する。

【００３４】

図３は、図２のファイアウォール装置１におけるアクセス制御リスト管理部１０２の模式的構成図である。アクセス制御リスト管理部１０２は、アクセス制御リストデータベース１０２１、検索部１０２２および更新処理部１０２３を有する。アクセス制御リストデータベース１０２１は、少なくとも「ソースＩＰアドレス」、「ディスティネーションＩＰアドレス」および「フィルタ処理方法」といったフィールドを有するエントリ（アドレス制御ルール）の集合を検索可能に保持する。検索部１０２２は、パケットフィルタ１０１からＩＰアドレスなどを含む問い合わせ（ＲＱ）を受けると、アクセス制御リストデータベース１０２１から対応するアクセス制御ルールを検索してパケットフィルタ１０１へ返す。更新処理部１０２３は、防御ルール判定部１０７から入力した更新用アクセス制御ルールに従ってアクセス制御リストデータベース１０２１の内容を更新（追加／修正）する。

【００３５】

図４は、アクセス制御リストデータベース１０２１の内容を例示した模式図である。アクセス制御リストデータベース１０２１には複数のアクセス制御ルールが所定の規則に従って格納される。各アクセス制御ルールは、図４に示すように、ソースＩＰアドレス（ＳＲＣ）やディスティネーションＩＰアドレス（ＤＳＴ）などのルール適合条件と、パケットの受理（ＡＣＣＥＰＴ）、拒否（ＤＥＮＹ）、廃棄（ＤＲＯＰ）などの所定の処理方法（ＰＲＯＣ）を示す識別子との組からなる。アクセス制御ルールは一般に複数設定されるので、その集合をアクセス制御リストデータベース１０２１で保持しておく。図４において、アスタリスク（＊）は任意のアドレスを示し、パケットフィルタ処理の“ＡＣＣＥＰＴ”はパケットの受理、“ＤＥＮＹ”はＩＣＭＰエラー通知をするパケット拒否、“ＤＲＯＰ”はＩＣＭＰエラー通知をしないパケット廃棄をそれぞれ示す。

【００３６】

図５は、誘導部１０３に設けられた誘導リストの一例を示す模式図である。誘導部１０３には、予め１つ以上のＩＰアドレスからなる誘導リストが保持されている。本実施例の誘導リストでは、内部ネットワーク４の未使用ＩＰアドレスが列挙されている。後述するように、未使用であるはずのＩＰアドレスを宛先とするパケットは、不審パケットである可能性が高い。

【００３７】

図６は、防御ルール判定部１０７に保持されている防御ルールスクリプトを例示した模式図である。詳しくは後述するが、防御ルール判定部１０７は、探査（RECON）、侵入(INTRUSION)、破壊(DESTRUCTION)などの攻撃種別ごとに、防御ルールを列挙し、例えばファイル形式で保持している。防御ルールは、所定の攻撃カテゴリに１対１対応する形式で、１つのアクセス制御ルールの雛型を指定する記述が用いられる。例えば、

ＩＮＴＲＵＳＩＯＮ：（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝、ＤＳＴ：＊、ＰＲＯＣ：ＤＲＯＰ）

といった記述が行ごとに攻撃種別ごとに列挙されている。この記述のうち「＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝」の部分が、後述するように、おとり装置２からのアラートに記載された情報（攻撃パケットのソースＩＰアドレス）で置き換えられる変数である。

【００３８】

１．２）動作

１．２．１）パケットフィルタリング

図７は、本発明の第１実施形態による攻撃防御システムの動作を示すフローチャートである。まず、ファイアウォール装置１において、インターネット３から内部ネットワーク４へ向けたＩＰパケットを外部通信インタフェース１００で捉えた後、当該ＩＰパケットをパケットフィルタ１０１へ転送する（ステップＡ１）。

【００３９】

次に、パケットフィルタ１０１は、当該ＩＰパケットのヘッダを参照し、そこに記載されているソースＩＰアドレスやディスティネーションＩＰアドレスなどの情報をアクセス制御リスト管理部１０２へ出力する。アクセス制御リスト管理部１０２は、上述したように、入力したＩＰアドレスを用いてアクセス制御リストデータベース１０２１を検索し、ヒットした最初のアクセス制御ルールをパケットフィルタ１０１へ返す。アクセス制御ルールを取得すると、パケットフィルタ１０１は、その処理方法に従って、当該ＩＰパケットを受理または廃棄する（ステップＡ２）。ＩＰパケットを受理した場合は、当該ＩＰパケットを誘導部１０３へ転送し、廃棄した場合は、直ちに次のパケットの処理へと制御を移す。

【００４０】

アクセス制御リスト管理部１０２におけるアクセス制御ルールの検索において、パケットフィルタ１０１から入力したソースＩＰアドレスを検索部１０２２が受け取ると、検索部１０２２は個々のアクセス制御ルールの適合条件と入力したソースＩＰアドレスとを照合し、適合条件を満たす最初のアクセス制御ルールを抽出し、パケットフィルタ１０１へ返す。

【００４１】

１．２．２）パケット誘導

次に、誘導部１０３では、パケットフィルタ１０１で受理されたＩＰパケットに対して、そのディスティネーションＩＰアドレスと予め設けられた誘導リストとを参照し、転送すべき内部通信インタフェース（１０４あるいは１０５）を決定する（ステップＡ３）。具体的には、図５に示すような誘導リストと、ディスティネーションＩＰアドレスとを照合し、合致するものがある場合には、第２の内部通信インタフェース１０５を介して当該ＩＰパケットをおとり装置２へ転送する。合致するものがない場合には、第１の内部通信インタフェース１０４を介して内部ネットワーク４へ当該ＩＰパケットを伝達する。

【００４２】

ＩＰパケットが内部ネットワーク４へ伝達された場合には、当該ＩＰパケットは内部ネットワーク４上の適切なサーバ装置３０１に到達し、所定のサービスを提供するための処理が行われる（ステップＡ４）。

【００４３】

一方、ＩＰパケットがおとり装置２へ伝達された場合には、そのプロセッサ２０１において、偽のサービスを提供するための処理を行いながら、入力データの内容や処理状況を逐次的に攻撃検知部２０２へ通知する（ステップＡ５）。この際、おとり装置２は、ファイアウォール装置１から伝達されたＩＰパケットを、そのディスティネーションＩＰアドレスの如何を問わず、受信することができる。具体的には、おとり装置２に複数のＩＰアドレスを割り当てられるような工夫を施してもよいし、あるいは図８に示すように、予め誘導部１０３にアドレス変換部１０３１を備えておき、入力ＩＰパケットのディスティネーションＩＰアドレスをおとり装置２のＩＰアドレスに書き換えた上で、おとり装置２に当該ＩＰパケットを伝達するような方法を用いてもよい。

【００４４】
１．２．３）偽サービス提供
ＩＰパケットを受信後、おとり装置２は、偽のサービスとして、ＷＷＷやＴｅｌｎｅｔなど１つ以上の任意のものを提供する。ただし、本実施形態においては、通信プロトコルさえ適切に処理すれば十分であり、実際のサービスで行われるような、ファイルシステムへのアクセスやデータベース処理などは一切行わなくともよい。具体的には、例えば、Ｔｅｌｎｅｔサービスの場合であれば、Ｌｏｇｉｎ／Ｐａｓｓｗｏｒｄプロンプトへの任意の入力に対して、すべてログインを許可し、ユーザに偽のメッセージを応答するような偽装シェルを起動するようにしてもよい。
【００４５】
１．２．４）攻撃検知
次に、おとり装置２の攻撃検知部２０２では、プロセッサ２０１から通知される処理状況について、正常動作定義との照合を行い、攻撃の有無を判定する（ステップＡ６）。正常動作定義とは、おとり装置２上で提供されるサービスの正しい振舞いに関する条件の集合である。具体的には、例えば、ＷＷＷサービスに対して「ＷＷＷサービスに対応するプロセスは自ら他のサーバ装置にネットワークアクセスをすることはない」というような条件や、「／ｕｓｒ／ｌｏｃａｌ／ｗｗｗ／ｌｏｇｓディレクトリ以外にファイルを書き込むことはない」というような条件などの集合である（詳しくは、図１２参照）。これらの各条件と通知された処理状況とを照合し、合致しない条件を少なくとも１つ検出した際に、「攻撃あり」と判断する。
【００４６】
攻撃を検出した際、違反した条件の意味に応じて、攻撃種別を決定し、その結果をアラートとしてファイアウォール装置１へ送信する（ステップＡ７）。
【００４７】
攻撃種別とは、当該攻撃に対する防御方法を導出するのに十分な分類をいい、例えば、
・「探査」：ポートスキャンやバナー攻撃などのいわゆる「フィンガープリンティング」
・「侵入」：トロイの木馬やアカウントの追加などのバックドア設置
・「破壊」：Ｐｉｎｇ　Ｏｆ　Ｄｅａｔｈなどのサービス不能攻撃
などを指す。その方法の一例として、正常動作定義の中の各条件について、違反時に想定される攻撃種別を予め併記しておけばよい。例えば、前記した「／ｕｓｒ／ｌｏｃａｌ／ｗｗｗ／ｌｏｇｓディレクトリ以外にファイルを書き込むことはない」という条件に違反するような攻撃については、バックドア設置の可能性が高いので、「侵入」を示す識別子を当該条件に併記しておく。
【００４８】
１．２．５）アクセス制御リストの更新
最後に、ファイアウォール装置１における防御ルール判定部１０７では、制御インタフェース１０６を介しておとり装置２から受信したアラートを参照し、防御ルールを用いてアクセス制御ルールを生成し、アクセス制御リスト管理部１０２へ当該アクセス制御ルールを追加するよう指示する（ステップＡ８）。
【００４９】
具体的には、防御ルール判定部１０７に、予め攻撃種別ごとに、図６のような防御ルールスクリプトを設定しておく。防御ルールスクリプトには、図６のような書式によって、攻撃種別と更新すべきアクセス制御ルールのひな型との組を記述する。アクセス制御ルールのひな型には、アラートに記載された情報を挿入するための変数が記述できる。たとえば、
（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝、ＤＳＴ：１．２．３．４、ＰＲＯＣ：ＤＲＯＰ）
と記述されている場合、「＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝」の箇所は、アラートに記載されたソースＩＰアドレスで置換され、

（ＳＲＣ：１２．３４．５６．７８、ＤＳＴ：１．２．３．４、ＰＲＯＣ：ＤＲＯＰ）といった完全な形式のアクセス制御ルールに変換される。そして、当該アクセス制御ルールは、アクセス制御リスト管理部１０２内の更新処理部１０２３へ伝達され、アクセス制御リストデータベース１０２１に適切に追加される。同じソースＩＰアドレスおよびディスティネーションＩＰアドレスの組をもつアクセス制御ルールが既にアクセス制御リストデータベース１０２１に登録されている場合には、更新処理部１０２３は、新たに追加されたアクセス制御ルールが有効になるように適切にアクセス制御リストデータベース１０２１を更新する。たとえば、アクセス制御リストデータベース１０２１の検索スキャン方向の先頭に位置するように追加される。

【００５０】

１．３）効果

第１実施形態のファイアウォール装置１では、誘導部１０３において、誘導リストとディスティネーションＩＰアドレスとの照合結果により、おとり装置２へ誘導する方法を用いている。このために、内部ネットワーク４の既存の構成を一切変更することなく、おとり装置２を設置可能となる。さらに、誘導リストに含めるＩＰアドレスとして、内部ネットワーク４における未使用のＩＰアドレス群を記載することで、１台のおとり装置２で、内部ネットワーク４上に複数のおとり装置２を設置するのと同じ効果が得られる。

【００５１】

通常、「ＣｏｄｅＲｅｄ」や「Ｎｉｍｄａ」などの自動感染機能をもつワームは、ある連続したＩＰアドレスの区間からランダムにＩＰアドレスを選択しながら、感染を試みるよう動作する。したがって、おとり装置２は設置台数が多ければ多いほど検知の確率が高くなる。本実施形態では、図５に示すような誘導リストの作成でその効果を得ることができる。

【００５２】

また、ファイアウォール装置１の外部通信インタフェース１００に割り当てられたＩＰアドレスを誘導リストに含めることで、インターネット３側からは、ファイルウォール装置１とおとり装置２との見分けがつかなくなる。一般に、インターネット３からの攻撃は、ファイアウォールの発見から始まるので、本実施形態はファイアウォール装置１を「隠す」という効果をもつ。

【００５３】

１．４）具体例

図９～図１１は第１実施形態の具体的動作例を説明するためのネットワーク構成図であり、図１２はおとり装置２における攻撃検知動作を説明するための模式図である。

【００５４】

図９に示すように、インターネット３上に攻撃元ホスト３０１（ＩＰアドレス：１２．３４．５６．７８）があり、内部ネットワーク４上にインターネットサーバ装置４０１がありものとする。さらに、インターネット３と内部ネットワーク４との境界にファイアウォール装置１が設置され、標準的なポート番号であるＴＣＰ８０番ポートにおいてＷＷＷサービスを提供するおとり装置２が設置されているものとする。また、内部ネットワーク４のネットワークアドレスとして、「１．２．３．ｘ／２４」が用いられており、サーバ装置４０１には「１．２．３．４」というＩＰアドレスが設定されているものとする。

【００５５】

今、攻撃元ホスト３０１はＷＷＷサービスに対する自動感染機能をもつワームに感染しており、当該ワームが次の感染先として、内部ネットワーク４に対応する「１．２．３．ｘ／２４」に狙いを定め、かつ「１．２．３．１」を第１の感染先として選択したものとする。このとき、攻撃元ホスト３０１から内部ネットワーク４に向けて、ＳＹＮパケット（ソースＩＰアドレス：１２．３４．５６．７８、ディスティネーションＩＰアドレス：１．２．３．１）が送信される。

【００５６】

当該ＳＹＮパケットは、まず、ファイアウォール装置１の外部通信インタフェース１０

０に到達した後、ただちにパケットフィルタ１０１に伝達される。パケットフィルタ１０１では、アクセス制御リスト管理部１０２に対して、少なくとも当該ＳＹＮパケットのソースＩＰアドレス「１２．３４．５６．７８」とディスティネーションＩＰアドレス「１．２．３．１」とを出力する。この他、アクセス制御ルールの粒度を高めるために、プロトコル番号「６」（ＴＣＰを示す）や、ポート番号「８０」などを出力できるようにしてもよいが、本実施例では例としてソースＩＰアドレスとディスティネーションＩＰアドレスだけを入力するものとする。

【００５７】

アクセス制御リスト管理部１０２におけるアクセス制御リストデータベース１０２１は、例えば、図４のようなテキスト形式で記述されたアクセス制御リストを保持しているものとする。上述したように、各行は１つのアクセス制御ルールを示しており、ＳＲＣフィールドとＤＳＴフィールドとの組が適合条件を、ＰＲＯＣフィールドがフィルタ処理方法をそれぞれ示す。

【００５８】

検索部１０２２では、パケットフィルタ１０１から入力として与えられたソースＩＰアドレス「１２．３４．５６．７８」およびディスティネーションＩＰアドレス「１．２．３．１」との組を検索キーとして、適切なアクセス制御ルールを抽出するために、アクセス制御リストデータベースの先頭行から順に各アクセス制御ルールを参照しながら、各ルールの適合条件と前記入力との比較を行い、適合する最初のアクセス制御ルールを抽出する。この時点では、「（ＳＲＣ：＊、ＤＳＴ：１．２．３．１、ＰＲＯＣ：ＡＣＣＥＰＴ）」（「ＰＲＯＣ：ＡＣＣＥＰＴ」は入力ＩＰパケットの受理を示す）というアクセス制御ルールが適合したとする。このとき、検索部１０２２は、「（ＳＲＣ：１２．３４．５６．７８、ＤＳＴ：１．２．３．１、ＰＲＯＣ：ＡＣＣＥＰＴ）」をパケットフィルタ１０１に返す。

【００５９】

アクセス制御ルールを受け取ったパケットフィルタ１０１は、当該ルールのＰＲＯＣフィールドを参照し、「ＡＣＣＥＰＴ」であることを確認すると、ただちに入力ＩＰパケットを後段の誘導部１０３へと伝達する。

【００６０】

続いて、誘導部１０３では、受け取った入力ＩＰパケットのディスティネーションＩＰアドレスと内部的に保持する誘導リストとを参照し、次の転送先を決定する。本実施例では、誘導リスト内に内部ネットワーク４の未使用ＩＰアドレスが列挙されており、その１つが「１．２．３．１」であるものとする。この場合、誘導部１０３は、入力ＩＰパケットのディスティネーションＩＰアドレス「１．２．３．１」が誘導リストに記載されているのを確認した後、当該入力ＩＰパケットをおとり装置２が接続されている第２の内部通信インタフェース１０５へと伝達する（図１０参照）。

【００６１】

おとり装置２は、第２の内部通信インタフェース１０５へ伝達された全てのＩＰパケットを、そのディスティネーションＩＰアドレスの如何によらず受け付ける。おとり装置２では偽のＷＷＷサービスが稼動しており、ワームが発したＳＹＮパケットを受け付けると共に、ＳＹＮ－ＡＣＫパケットをそのソースＩＰアドレス（すなわち攻撃元ホスト３０１）へ向けて出力する。

【００６２】

これ以降、ファイアウォール装置１で同様の処理が繰り返されて、攻撃元ホスト３０１とおとり装置２との間でＴＣＰ接続確立のための通信と、ワーム感染のための（不正な）通信が行われる。

【００６３】

おとり装置２では、プロセッサ２０１でＷＷＷサービスを攻撃元ホスト３０１へ提供する。それと並行して、プロセッサ２０１は、ファイルアクセスやネットワークアクセスなどの動作状況を、攻撃検知部２０２へ逐次的に通知する。攻撃元ホスト３０１上のワーム

は、おとり装置２上のＷＷＷサービスに対して、感染を試みる。具体的には、例えば、
「ＧＥＴ　／ｄｅｆａｕｌｔ．ｉｄａ？ＮＮＮＮＮＮＮＮＮＮＮＮ（２００バイト程度の繰り返し）…％ｕ００００％ｕ００＝ａ　ＨＴＴＰ／１．１」といった文字列から始まる、非常に大きなメッセージをＷＷＷサービスに対して入力し、いわゆる「バッファオーバーフロー」を引き起こすことで、任意のコマンドを実行しようとする。この際、一般的なワームは、ワーム自身のコードをディスク上のシステム領域にコピーした後、当該コードを実行するようなコマンドを発行する。したがって、ワームの侵入時に、プロセッサ２０１は、システム領域へファイルの書き出しが行われたこと、あるいは、当該ファイルの実行が行われたことを攻撃検知部２０２に伝達することになる。このとき、同時に、おとり装置２が受け付けた入力ＩＰパケットのコピーも併せて伝達する。

【００６４】

攻撃検知部２０２は、予めプロセッサ２０１上のＷＷＷサービスの適正な動作に関する情報を、正常動作定義ファイルとして保持している。正常動作定義ファイルは、例えば、図１２のような形式で記述されており、ファイルの読み込み、書き出し、実行などに関する条件が列挙されている。

【００６５】

ここで、前記ワームが自身のコピーを書き出す箇所を「Ｃ：￥Ｗｉｎｄｏｗｓ(登録商標）」ディレクトリだとすると、その動作は図１２に示す正常動作定義ファイル内の第２番目の条件である
「ＷＲＩＴＥ、Ｃ：￥Ｉｎｅｔｐｕｂ￥ｗｗｗｒｏｏｔ￥＿ｖｔｉ＿ｌｏｇ￥＊；ＩＮＴＲＵＳＩＯＮ」（「Ｃ：￥Ｉｎｅｔｐｕｂ￥ｗｗｗｒｏｏｔ￥＿ｖｔｉ＿ｌｏｇディレクトリ以下にのみファイル書き出しを行う」の意）
に違反する。このとき、攻撃検知部２０２は、当該条件の「；」以下を参照し、ＩＮＴＲＵＳＩＯＮ（侵入）カテゴリに属する攻撃があったと判定する。

【００６６】

続いて、攻撃検知部２０２は、少なくとも、入力ＩＰパケットに含まれるソースＩＰアドレスと、検出された攻撃のカテゴリが「ＩＮＴＲＵＳＩＯＮ」であることを知らせるためのアラートを生成し、ファイアウォール装置１の制御インタフェース１０６へ伝達する（図１１参照）。

【００６７】

制御インタフェース１０６で受信されたアラートは防御ルール判定部１０７へ伝達される。アラートの入力を受けた防御ルール判定部１０７は、上述したように、防御ルールを列挙したスクリプトを、例えばファイル形式で保持している。各防御ルールは、所定の各攻撃カテゴリに１対１対応する形式で、１つのアクセス制御ルールのひな型が指定されている（図６参照）。

【００６８】

具体的には、例えば、
ＩＮＴＲＵＳＩＯＮ：（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝、ＤＳＴ：＊、ＰＲＯＣ：ＤＲＯＰ）　　・・・（１）
といった記述が行ごとに列挙されている。ここで、アラートの入力を受けた防御ルール判定部１０７は、防御ルールの定義ファイルを行ごとに参照し、「ＩＮＴＲＵＳＩＯＮ」カテゴリに対応する防御ルールである式（１）を抽出する。そして、アクセス制御ルールの雛型に対して、当該アラートに記載されたソースＩＰアドレス「１２．３４．５６．７８」（すなわち攻撃元ホストのＩＰアドレス）によって、「＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝」を置換し、
（ＳＲＣ：１２．３４．５６．７８、ＤＳＴ：＊、ＰＲＯＣ：ＤＲＯＰ）
・・・（２）
というアクセス制御ルールを生成する（「ＤＳＴ：＊」は任意のディスティネーションＩＰアドレスに適合する）。そして、当該アクセス制御ルールをアクセス制御リスト管理部１０２へ伝達する。

【００６９】
アクセス制御リスト管理部１０２では、防御ルール判定部１０７からのアクセス制御ルールの入力について更新処理部１０２３で処理する。更新処理部１０２３では、式（２）で示されるアクセス制御ルールを、アクセス制御リストデータベース１０２１に伝達し、その追加を指示する。アクセス制御リストデータベース１０２１では、式（２）で示されるアクセス制御ルールを追加するように更新処理を行う。その際、アクセス制御リストデータベース１０２１は、それ以降の検索処理が最近の更新結果を反映するように適切に更新処理を行う。例えば、図４のようなテキスト形式で記述されたアクセス制御リストを用い、先頭行から順に検索処理を行うような場合であれば、式（２）を先頭行に追加すればよい。つまり、たとえ次式（３）といったようなアクセス制御ルールが予め設定されていたとしても、

（ＳＲＣ：１２．３４．５６．７８、ＤＳＴ：＊、ＰＲＯＣ：ＡＣＣＥＰＴ）
・・・（３）

当該更新処理以降、検索部１０２２がソースＩＰアドレス「１２．３４．５６．７８」を含む入力を受けた場合には、式（３）ではなく式（２）を検索結果として出力する（図１３参照）。

【００７０】
次に、攻撃元ホスト３０１上のワームが次の攻撃先として、「１．２．３．４」を選択したものとする。しかる後、先の攻撃と同様に、内部ネットワーク４上のサーバ装置４０１に向けたＳＹＮパケットがファイアウォール装置１に到達する。その場合、当該ＳＹＮパケットの入力をうけたパケットフィルタ１０１は、アクセス制御リスト管理部１０２から適合するアクセス制御ルールとして式（２）を受け取るので、ＰＲＯＣフィールドの指定「ＤＲＯＰ」に従い、当該ＳＹＮパケットを廃棄する（図１４参照）。

【００７１】
以上のような動作を行うことにより、本発明による攻撃防御システムは、攻撃元ホスト３０１上のワームからの攻撃から、内部ネットワーク４上のサーバ装置４０１を保護することができる。

【００７２】
（第２実施形態）
２．１）構成
図１５は、本発明の第２実施形態による攻撃防御システムのブロック図である。本実施形態のファイアウォール装置５は、図２に示す第１実施形態におけるファイアウォール装置１に信頼度管理部５０２を加え、さらに誘導部１０３に代えて、信頼度に依存してパケット誘導方向を決定できる誘導部５０１を有する。以下、図２に示すシステムと同じ機能ブロックについては、同一参照番号を付して詳細な説明は省略する。

【００７３】
図１５において、誘導部５０１は、パケットを入力すると、信頼度管理部５０２へ入力ＩＰパケットのソースＩＰアドレスを出力し、対応する信頼度を取得する。信頼度を受け取ると、誘導部５０１はその信頼度と所定のしきい値との比較を行い、その結果に応じて、当該入力ＩＰパケットを第1の内部通信インタフェース１０４および第２の内部通信インタフェース１０５のいずれかに出力する。

【００７４】
信頼度管理部５０２はＩＰアドレスと対応する信頼度との組の集合を管理する。誘導部５０１から要求があると、信頼度管理部５０２はそれに対応した信頼度を検索して誘導部５０１へ返し、後述するように信頼度の更新を行う。

【００７５】
２．２）動作
図１６は、本発明の第２実施形態による攻撃防御システムの動作を示すフローチャートである。

【００７６】

まず、第１実施形態のファイアウォール装置１と同様に、インターネット３からの入力ＩＰパケットを受信すると（ステップＡ１）、パケットフィルタ１０１は、アクセス制御リスト管理部１０２で保持されているアクセス制御ルールの内容に応じて、当該入力ＩＰパケットの受理または廃棄を行う（ステップＡ２）。受理されたＩＰパケットは誘導部５０１へ転送される。

【００７７】

２．２．１）信頼度管理

誘導部５０１は、入力ＩＰパケットに含まれる情報のうち少なくともソースＩＰアドレスを信頼度管理部５０２へ出力し、当該ＩＰアドレスに対する信頼度を取得する（ステップＣ１）。信頼度管理部５０２はＩＰアドレスとその信頼度との組の集合を保持し、ＩＰアドレスを入力すると、それに対応する信頼度を出力することができる。具体的には、例えば、「１．２．３．４：１０」などのように、「＜ＩＰアドレス＞：＜信頼度＞」といった形式をなす行で構成されるテキストファイルを用いることができる。

【００７８】

その他、検索および更新処理を効率的に行うために、リレーショナルデータベースを利用してもよい。いずれにせよ、任意のＩＰアドレスについて、対応する信頼度を適切に検索および更新できればよい。信頼度管理部５０２は、入力されたＩＰアドレスに対応するＩＰアドレスと信頼度との組が１つ見つかれば、当該信頼度を誘導部５０１へ出力する。もし適切なＩＰアドレスと信頼度の組が見つからなかった場合には、当該ＩＰアドレスに対する信頼度として初期値（例えば０）を設定し、当該初期値を誘導部５０１に出力するとともに、新たに「＜ＩＰアドレス＞：＜初期値＞」という組を保持内容に追加する。

【００７９】

続いて、信頼度管理部５０２は、信頼度を出力した後、当該信頼度を増加させるように保持内容を更新する（ステップＣ２）。具体的には、例えば次式（４）に示されるように、信頼度に定数Ｃ（≧１）を加算する。

ｃ［ｎ＋１］＝ｃ［ｎ］＋Ｃ　　・・・　（４）。

【００８０】

２．２．２）信頼度に基づくパケット誘導

誘導部５０１は、取得した信頼度に応じて、当該ＩＰパケットの転送先を決定する（ステップＣ３）。信頼度ｃの評価処理の好適な一例としては、予め誘導部５０１にあるしきい値Ｔを設定しておき、信頼度ｃとしきい値Ｔとの比較結果（大小関係）を評価する。

【００８１】

図１７は、本実施形態における信頼度とパケット転送先の関係を示すグラフである。ここでは、ｃ≧Ｔのときには、入力ＩＰパケットを「信頼できる」と判定し、当該ＩＰパケットを内部通信インタフェース１０４を介して内部ネットワーク４へ伝達する。一方、ｃ＜Ｔのときには、内部通信インタフェース１０５を介して、おとり装置２へ伝達する。

【００８２】

なお、これ以降の動作は、図７に示す処理（ステップＡ４～Ａ８）と同じである。

【００８３】

２．２．３）信頼度の更新方法

図１６のステップＣ２における信頼度の更新方法は、上述した式（４）の他に、別の方法もある。次式（５）に示すように、誘導部５０１からの入力の一部に、入力ＩＰパケットｐのバイト数Ｌ（ｐ）を含めておき、その逆数１／Ｌ（ｐ）を加算するようにしても良い。

ｃ［ｎ＋１］＝ｃ［ｎ］＋１／Ｌ（ｐ）　　・・・　（５）。

【００８４】

この方法は、大きなサイズをもつＩＰパケットほど信頼度が増加しにくくなるように、重みづけを行うものである。一般に、バッファオーバーフロー攻撃やサービス妨害（ＤｏＳ）攻撃を目的としたＩＰパケットは正常な通信内容をもつＩＰパケットに比べて大きなサイズをもつことが多いため、こうした重みづけを施すことで、これらの攻撃の可能性を

もつ入力ＩＰパケットを、できるだけ長い期間、おとり装置２へ誘導することが可能になる。その結果、本発明による攻撃防御システムの防御性能を高めることができる。

【００８５】

また、別の一例として、誘導部５０１からの入力の一部に、入力ＩＰパケットのプロトコル番号を含めておき、予め設定されたプロトコル番号に一致した場合のみ、信頼度を更新する方法を併用してもよい。たとえば、予めプロトコル番号「６」を設定しておくことで、入力ＩＰパケットがＴＣＰである場合にのみ、信頼度を更新する。こうすることで、本格的な攻撃の前に準備的に行われるスキャン攻撃による、不要な信頼度の増加を抑える効果が得られる。もちろん、更新処理の条件として、プロトコル番号だけでなく、その他ＩＰヘッダ、ＴＣＰヘッダ、ＵＤＰヘッダなどに含まれる任意の情報を用いてもよいし、複数の条件を組み合わせた論理式を用いるようにしてもよい。

【００８６】

さらに別の一例として、入力ＩＰパケットについて、一般に外れ値検知として知られるような、統計的に「異常であること」の確からしさを求める方法を用いてもよい。具体的には、図１８に示すように、ＩＰアドレスと信頼度との組の集合に代えて、特開２００１－１０１１５４公報（本出願人による特許出願）に記載の外れ値度計算装置を信頼度管理部５０２に組み込む。この場合、誘導部５０１からは実数値や属性を表す離散値などを含む多次元のベクトル、たとえば、ｘ＝（入力ＩＰパケットの到達時刻、入力ＩＰパケットのサイズ、プロトコル番号）を入力する。

【００８７】

このような多次元ベクトルを入力した外れ値度計算装置は、それまでの入力から生成した確率密度分布などを基に、１個の実数値として表される「スコア値」を算出する。このスコア値は「異常であること」の確からしさを表しており、その値が大きいほど攻撃である可能性が高い、言い換えれば信頼度が低い。したがって、スコア値の逆数でもって、入力ＩＰパケットに対する信頼度とすることができる。

【００８８】

図１８（Ａ）は、外れ値度計算を用いた信頼度管理部５０２の概略的構成図であり、（Ｂ）は、その一例を示す詳細なブロック図である。この外れ値度計算を用いる方法は、上述したような「決定的な」信頼度の評価方法では捉えきれない（すなわち予期されない）攻撃を「確率的に」検出するものである。したがって、将来現れうる未知の攻撃に対する防御が可能となる。

【００８９】

本発明の第２実施形態は、第１実施形態による効果に加えて、さらに「アクティブ・ターゲッティング」にも対応できるという効果が得られる。アクティブ・ターゲッティングとは、次に具体的に説明するように、予め特定のサーバ装置もしくはホスト装置に狙いを定めて行われる攻撃形態を指し、一般的には悪意をもった人間によって実行される。

【００９０】

２．３）具体例

図１９～図２１は、本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【００９１】

図１９に示すように、インターネット３上の攻撃元ホスト３０１を使うユーザが、内部ネットワーク４上のサーバ装置４０１の動作停止を目的として、Ｐｉｎｇ　Ｏｆ　ＤｅａｔｈなどのＤｏＳ攻撃を行う場合を考える。

【００９２】

このような場合、攻撃元ホスト３０１のＩＰアドレス「１２．３４．５６．７８」に対する信頼度が、誘導部５０１に設定されたしきい値以下であれば、図２０に示すように、ＤｏＳ攻撃を構成するＩＰパケットはおとり装置２へ誘導され、サーバ装置４０１は保護される。ＤｏＳ攻撃をしかけるような悪意をもった人間は、ターゲットを定めたしばらく後に、攻撃を開始すると考えられるので、前記しきい値を十分大きく設定しておくことで

、おとり装置２によるサーバ装置４０１の保護が達成される。

【００９３】

さらに、通常の（すなわち攻撃の意図がない）ユーザからのアクセスについては、安全に内部ネットワーク４上のサーバ装置４０１によるサービスを行うができる。たとえば、図２１に示すように、インターネット３上に通常のホスト３０２から、サーバ装置４０１へのアクセスがあった場合、前記例と同様に、ファイアウォール装置５の信頼度管理部５０２により、通常のホスト３０２のＩＰアドレスに対する信頼度が評価される。

【００９４】

もし、通常のホスト３０２の信頼度が不十分であれば、誘導部５０１により「不審」と判定され、おとり装置２へ当該アクセスを構成するＩＰパケットは誘導される。ここで、おとり装置２のプロセッサ２０１で、サーバ装置４０１上のＷＷＷサービスと同じ処理を行うよう、おとり装置２を設定しておく。すなわち、おとり装置２をサーバ装置４０１のミラーサーバとして動作させる。具体的には、WWWサービスの場合、HTMLファイルやJPEGファイルなどのコンテンツの複製をとればよい。したがって、通常のホスト３０２は目的のサービスを受けることができる。おとり装置２では正常なアクセスがなされる間は攻撃が検知されることがないので、通常のホスト３０２のＩＰアドレスに対する信頼度は上述した信頼度更新方法に従って増加していき、いずれ、しきい値Ｔを超える。信頼度ｃがしきい値Ｔを超えた後は、通常のホスト３０２からのアクセスを構成するＩＰパケットは内部ネットワーク４内のサーバ装置４０１へ誘導される。

【００９５】

このような動作により、信頼ずみの通常のユーザからのアクセスについては、すべてサーバ装置４０１が応答する。したがって、おとり装置２が攻撃を受けて、その動作を停止したとしても、信頼ずみの通常のユーザは、サーバ装置４０１によりサービスを継続して受けることができるという効果をもつ。

【００９６】

なお、おとり装置２はサーバ装置４０１上の完全なミラーサーバとして設定してもよいし、例えば、ユーザ認証を要するような重要サービスは除いて、一般的なサービスだけをおとり装置２で提供するようにも設定できる。

【００９７】

（第３実施形態）

図２２は、本発明の第３実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図であり、図２３は、その一例を示す詳細なブロック図である。本実施形態のファイアウォール装置６は、ファイアウォール装置１における誘導部１０３に加えて、図５に示す第２実施形態の誘導部５０１および信頼度管理部５０２を有する。

【００９８】

具体的には、図２３に示すように、第１の誘導部１０３の後段として第２の誘導部５０１を設けても良い。逆に、第１の誘導部１０３の前段として第２の誘導部５０１を設けることもできる。

【００９９】

いずれの構成においても、ワームのようにランダムにＩＰアドレスを選択して行われる攻撃と、アクティブ・ターゲッティングによる攻撃の両方に対応できる、という効果が得られる。また、あるホストが、第２の誘導部５０１で一旦信頼された後、ワームに感染するなどした場合でも、おとり装置２にて攻撃の有無を検査することができる、という効果も得られる。

【０１００】

（第４実施形態）

４．１）構成

図２４は、本発明における第４実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。本実施形態よるファイアウォール装置７は、図１５のファイアウォール装置５における信頼度管理部５０２に代えて、信頼度管理部７０１が接

続されている。その他の機能ブロックは、図１５のものと同じであるから、同一参照番号を付して説明は省略する。

【０１０１】

図２４に示すように、信頼度管理部７０１は、リアルタイム信頼度データベース７０１１、複製処理部７０１２、長期信頼度データベース７０１３、および、更新処理部７０１４を備える。

【０１０２】

リアルタイム信頼度データベース７０１１は、ＩＰアドレス、それに対応する信頼度および最終更新時刻の組の集合を管理し、誘導部５０１からの問い合わせのＩＰアドレスに応じて、対応する信頼度を返す。複製処理部７０１２は、定期的に、リアルタイム信頼度データベース７０１１の内容を、長期信頼度データベース７０１３へ複製する。

【０１０３】

長期信頼度データベース７０１３は、ＩＰアドレス、それに対応する信頼度および最終更新時刻の組の集合を管理する。更新処理部７０１４は、定期的に長期信頼度データベース７０１３を参照し、所定の期間よりも古い最終更新時刻を有する項目について、その信頼度を減算する更新処理を実行する。

【０１０４】

４．２）信頼度管理

基本的には、入力ＩＰパケットをフィルタリングし、おとり装置２または内部ネットワーク３へ誘導するまでの処理は、第２実施形態のファイアウォール装置５と同一である（図１６のステップＡ１～Ａ２、Ｃ１～Ｃ３、Ａ４～Ａ８）。ただし、本実施形態の信頼度管理部７０１は、パケットの処理と並行して、以下にあげるような信頼度管理処理を行う。

【０１０５】

図２５は信頼度管理部７０１における信頼度参照処理を示すフローチャートである。まず、図１６のステップＣ１において信頼度の参照が行われたとき、信頼度管理部７０１は、リアルタイム信頼度データベース７０１１から、入力として与えられたＩＰアドレスに対応する項目が記録されているかどうかを調べる（図２５のステップＤ１）。当該ＩＰアドレスに対応する項目が記録されている場合（ステップＤ１のＹ）、さらにその信頼度を参照し、当該信頼度を誘導部５０１に出力する（ステップＤ２）。

【０１０６】

一方、ＩＰアドレスに対応する項目がリアルタイム信頼度データベース７０１１に記録されていない場合（ステップＤ１のＮ）、まず、長期信頼度データベース７０１３を参照して、当該ＩＰアドレスに対応する項目が記録されているかどうかを調べる（ステップＤ３）。記録されている場合（ステップＤ３のＹ）、長期信頼度データベース７０１３の該当項目の内容（ＩＰアドレス、信頼度および最終更新時刻）を、リアルイム信頼度データベース７０１１にコピーし（ステップＤ４）、信頼度を出力する（ステップＤ２）。長期信頼度データベース７０１３にも該当項目がない場合（ステップＤ３のＮ）、リアルタイム信頼度データベース７０１１に、所定の信頼度の初期値をもって、新たな項目を追加し（ステップＤ５）、信頼度を出力する（ステップＤ２）。

【０１０７】

そして、図１６のステップＣ２において信頼度の更新が行われたとき、信頼度管理部７０１は、ＩＰアドレスと、信頼度の更新に加えて、更新時刻をリアルタイム信頼度データベース７０１１に記録する。

【０１０８】

４．３）リアルタイム信頼度の複製処理

以上の処理に並行して、複製処理部７０１２は定期的に（例えば1日ごとに）リアルタイム信頼度データベース７０１１の全内容を走査しながら、各項目を長期信頼度データベース７０１３へコピーしていく。このとき、最終更新時刻を参照して、所定の期間（例えば1週間）以上、更新処理が行われなかった項目について、当該項目をリアルタイム信頼

度データベース７０１１から削除する処理を行っても良い。
【０１０９】
４．４）長期信頼度の更新処理
また、更新処理部７０１４は、定期的に（例えば１日ごとに）長期信頼度データベース７０１３の全内容を走査しながら、各項目の最終更新時刻を参照して、所定の期間（例えば１週間）以上、更新が行われなかった項目については、その信頼度を所定の値だけ減算する。もしくは、単に削除しても良い。
【０１１０】
４．５）効果
以上のような動作を行うことで、リアルタイム信頼度データベース７０１１の記憶容量を抑えることができるので、ＳＤＲＡＭなど、低容量で高速な記憶デバイスを用いることができる。一方、長期信頼度データベース７０１３はアクセス頻度が少ないので、ハードディスクデバイスなど、大容量で低速な記憶デバイスを用いることができる。
【０１１１】
また、更新処理部７０１４による長期信頼度データベース７０１３の更新処理により、たとえ１度、十分な信頼度を得たソースＩＰアドレスについても、ある一定期間以上、アクセスが途絶えた場合には再び「不審」と見なすことができる。これは、特に中古ＰＣの売買など、ソースＩＰアドレスに相当するホストの利用環境が大きく変化した場合などに、信頼度の再評価を自動的におこなうことができるという効果をもつ。
【０１１２】
（第５実施形態）
本発明の第５実施形態として、図２３に示す第３実施形態の信頼度管理部５０２に代えて、上述した第４実施形態の信頼度管理部７０１を用いたファイアウォール装置を構成することができる。基本的な構成は図２３と同じであり、信頼度管理部７０１の構成及び動作は、図２４、図２５および第４実施形態の項で説明した通りであるから、ここでは省略する。
【０１１３】
（第６実施形態）
６．１）構成
図２６は、本発明の第６実施形態による攻撃防御システムのファイアウォール装置９を示す概略的ブロック図である。ファイアウォール装置９では、第１実施形態のファイアウォール装置１における誘導部１０３に代えて、バッファ９０１１およびＩＣＭＰ監視部９０１２を有する誘導部９０１が設けられている。本実施形態では、第１実施形態のように誘導リストを設けることなく、ＩＣＭＰパケットを利用して同様の機能を実現できる。なお、簡略化のために、図２６では他の機能ブロックの表示が省略されている。
【０１１４】
バッファ９０１１は、次に述べるように、パケットフィルタ１０１より受け取ったパケットを一時的に蓄積し、第１内部通信インタフェース１０５を介して内部ネットワークへ転送すると共に、ＩＣＭＰ監視部９０１２からの求めに応じて、蓄積したパケットを第２の内部通信インタフェース１０５を介しておとり装置２へ再送信する。ＩＣＭＰ監視部９０１２は、第１の内部通信インタフェース１０４におけるＩＣＭＰパケットの受信を監視し、特定のＩＣＭＰエラーパケットを検出したとき、バッファ９０１１に適切なパケット再送を要求する。以下、本実施形態の動作を詳述する。
【０１１５】
６．２）動作
図２７は本実施形態によるファイアウォール装置９の動作を示すフローチャートである。まず、第１実施形態のファイアウォール装置１と同様に、外部通信インタフェース１００を介してインターネット４から受信した入力ＩＰパケットについて、パケットフィルタ１０１によるフィルタリングを行う（ステップＡ１、Ａ２）。
【０１１６】

受理されたＩＰパケットは誘導部９０１のバッファ９０１１に蓄積され（ステップＥ１）、無条件に第１の内部通信インタフェース１０４を介して内部ネットワーク３へ送出され（ステップＥ２）、通常のサービスが提供される（ステップＡ４）。この場合、たとえ不審パケットであっても内部ネットワークへ転送されてしまうが、実際の攻撃を実行する前に送信されるＴＣＰコネクション確立要求のＳＹＮパケットは攻撃要素が含まれていないために、ＳＹＮパケットであれば受け入れても問題はない。内部ネットワークにＳＹＮパケットが転送され宛先が存在しなければ、到達不能を知らせるＩＣＭＰパケット（タイプ３）が返される。

【０１１７】

ＩＣＭＰ監視部９０１２は、第１の内部通信インタフェース１０４でＩＣＭＰパケット（ＲＦＣ７９２記載）が受信されると、当該ＩＣＭＰパケットの内容を参照して、到達不能を知らせるエラー（すなわちＩＣＭＰタイプ３）であるか否かを調べる（ステップＥ３）。到達不能を知らせるエラーであれば（ステップＥ３のＹ）、そのＩＰヘッダ部をさらに参照し、少なくともソースＩＰアドレスもしくはディスティネーションＩＰアドレスを用いてバッファ９０１１に再送要求を行う（ステップＥ３）。その他のメッセージであった場合は、何もせず、監視を続ける。

【０１１８】

再送要求を受けたバッファ９０１１は、少なくともソースＩＰアドレスもしくはディスティネーションＩＰアドレスに従って、蓄積されたパケットから該当するパケットを抽出し、当該パケットを第２の内部通信インタフェース１０５を介して、おとり装置２へ再送する（ステップＥ４）。以下、すでに述べたステップＡ５～Ａ８が実行される。

【０１１９】

このように攻撃要素を含まないコネクション確立のためのパケットを利用することで、内部ネットワーク３の未使用ＩＰアドレスを誘導リストとして事前に設定することなしに、自動的に未使用ＩＰアドレス宛ての入力ＩＰパケットをおとり装置２へ誘導することができる。

【０１２０】

（第７実施形態）

７．１）構成

図２８は、本発明の第７実施形態による攻撃防御システムのファイアウォール装置１０を示す概略的ブロック図である。このファイアウォール装置１０は、上述した第２～第５実施形態によるファイアウォール装置における防御ルール判定部１０７およびアクセス制御リスト管理部１０２に代えて、有効期限付き防御ルール判定部１００１および有効期限付きアクセス制御リスト管理部１００２を設けている。

【０１２１】

防御ルール判定部１００１は、制御インタフェース１０６を介しておとり装置２から受け取ったアラートに応じて、信頼度管理部５０２および７０１に対して、対応する信頼度の再設定を指示する。あるいは、アラートに応じて、更新すべきアクセス制御ルールを決定し、アクセス制御リスト管理部１００２にその更新を指示する。

【０１２２】

信頼度管理部５０２および７０１は、防御ルール判定部１００１からの更新指示を受けて、新たな信頼度を決定し誘導部５０１へ出力する。アクセス制御リスト管理部１００２は、防御ルール判定部１００１からの更新指示を受けて、アクセス制御リストを更新し、パケットフィルタ１０１からの要求に応じてアクセス制御ルールを出力する。

【０１２３】

７．２）動作

本実施形態における攻撃防御システムの動作を、具体的な例を挙げながら詳細に説明する。

【０１２４】

まず、インターネット４から到達した入力ＩＰパケットが、ファイアウォール装置１０

によって、おとり装置２へ誘導され、おとり装置２において、当該入力ＩＰパケットによる攻撃が検知され、その旨を知らせるアラートが送信されるまでは、図１６のステップＡ１～Ａ７に示すように、第２～第５実施形態における攻撃防御システムと同様である。

【０１２５】

ファイアウォール装置１０の防御ルール判定部１００１には、防御ルール判定部１０７とは異なり、信頼度を更新するための防御ルールが予め設定されている。例えば、防御ルールとして、次式（６）のような形式の記述があれば、信頼度を１減算すると解釈されるものとする。

ＲＥＣＯＮ：ｃ（＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝）－＝１

・・・　（６）。

【０１２６】

たとえば、制御インタフェース１０６を通してソースＩＰアドレス「１２．３４．５６．７８」を示すアラートが受け取ると、防御ルール判定部１００１はＩＰアドレス「１２．３４．５６．７８」に対する信頼度を１減算すると解釈し、その旨を信頼度管理部５０２／７０１に指示する。すなわち、アラートを受け取ると、そのソースＩＰアドレスの信頼度を低減させる。信頼度管理部５０２は第２実施形態で説明したように信頼度を更新し、信頼度管理部７０１は第４実施形態で説明したように信頼度を更新するから、信頼度の低減処理を加えることで、よりきめ細かい信頼度管理ができる。

【０１２７】

また、ファイアウォール装置１０において、防御ルール判定部１００１内に、防御ルール判定部１０７と同様に、アクセス制御ルールのひな型としての防御ルールを予め設定してもよい。ただし、この場合のアクセス制御ルールは、新たに「有効期間」を表すフィールドを記載できる（したがって防御ルールにも記載可能）。例えば、次式（７）に示すように、前記式（１）の防御ルールにＥＸＰＩＲＥの項を追加し、「７日間有効」という制約をつけることができる。

ＩＮＴＲＵＳＩＯＮ：（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝、ＤＳＴ：＊、ＰＲＯＣ：ＤＲＯＰ、ＥＸＰＩＲＥ：＋７ＤＡＹ）　・・・（７）。

【０１２８】

したがって、アラートが制御インタフェース１０６を経由して防御ルール判定部１００１に伝達されると、防御ルール判定部１０７と同様の方法で、次式（８）に示すようにアクセス制御ルールが生成され、アクセス制御リスト管理部１００２に伝達される。

（ＳＲＣ：１２．３４．５６．７８、ＤＳＴ：＊、ＰＲＯＣ：ＤＲＯＰ、ＥＸＰＩＲＥ：＋７ＤＡＹ）　・・・　（８）。

【０１２９】

次に、アクセス制御リスト管理部１００２は、防御ルール判定部１００１から受け取ったアクセス制御ルールをアクセス制御リストデータベース１０２１に追加する。このとき、式（８）のようにＥＸＰＩＲＥフィールドがアクセス制御ルールに記載されている場合、アクセス制御リスト管理部１００２は、現在時刻に、ＥＸＰＩＲＥフィールドに指定された値を加算した時刻を算出した上で、データベースを更新する（図７のステップＡ８に対応する）。

【０１３０】

図２９は、アクセス制御リスト管理部１００２の管理動作を示すフローチャートである。アクセス制御リストデータベース１０２１が更新された後、再びソースアドレス「１２．３４．５６．７８」からの入力ＩＰパケットがファイアウォール装置１０に到達すると、パケットフィルタ１０１は当該ソースＩＰアドレスをアクセス制御リスト管理部１００２へ送付してアクセス制御ルールの取得要求を行う（ステップＡ２＿１）。

【０１３１】

アクセス制御リスト管理部１００２は、当該ソースＩＰアドレスに対応するアクセス制御ルールを検索する（ステップＡ２＿２、Ａ２＿３）。式（８）に相当するアクセス制御ルールを抽出すると、アクセス制御リスト管理部１００２は、ＥＸＰＩＲＥフィールドに

記載された有効期間と現在時刻とを比較する（ステップＡ２＿４）。

【０１３２】

現在時刻が有効期間を超過していた場合には（ステップＡ２＿４のＹＥＳ）、当該アクセス制御ルールをアクセス制御リストデータベース１０２１から削除し（ステップＡ２＿５）、デフォルトのアクセス制御ルールをパケットフィルタ１０１へ返す（ステップＡ２＿６）。逆に、有効期間内であれば（ステップＡ２＿４のＮＯ）、次式（９）に示すようなＥＸＰＩＲＥフィールドを除いたアクセス制御ルールをパケットフィルタ１０１へ返す（ステップＡ２＿７）。

（ＳＲＣ：１２．３４．５６．７８、ＤＳＴ：＊、ＰＲＯＣ：ＤＲＯＰ）

・・・（９）。

【０１３３】

こうして取得したアクセス制御ルールを用いて、パケットフィルタ１０１は受信ＩＰパケットの受理／廃棄の判定を行う（ステップＡ２）。

【０１３４】

上述したように、攻撃をおとり装置で検知した後の防御方法として、よりきめ細かな対策を講じることができる。具体例を挙げると、一般に攻撃者は、「侵入」もしくは「破壊」に相当する攻撃の準備として、ポートスキャンあるいはＴｒａｃｅｒｏｕｔｅなどの「探査」に相当する攻撃を行う。しかし、「探査」として検出されるアクセスが、全て攻撃であるとは限らないことも、よく知られる所である。したがって、「探査」に対する防御方法として、恒久的なアクセス遮断を行うことは不都合を生じる可能性がある。

【０１３５】

そこで、本実施形態では、有効期限付きのアクセス制御ルールを用いて時間制限を付けたアクセス遮断を行う。または、上述したように、アラーム発生によってそれまで蓄積された信頼度を低減させることで、信頼度がしきい値Ｔ（図１７参照）を超えないようにし、おとり装置への誘導を継続し、後で「侵入」もしくは「破壊」に相当する攻撃を検知してから恒久的なアクセス遮断へと対応を変えることもできる。

【０１３６】

（第８実施形態）

図３０は、本発明の第８実施形態による攻撃防御システムの概略的構成図である。第８実施形態では、単一のおとり装置２に代えて、２台以上のおとり装置２を含むおとりクラスタ２１が設けられている。

【０１３７】

本実施形態における各おとり装置２は、特定のディスティネーションＩＰアドレスをもつパケット、もしくは、特定のポート番号をもつパケットにしか偽のサービスを提供しないようにする。

【０１３８】

こうすることにより、内部ネットワーク４上の特定のサーバ装置に１対１対応するおとり装置２を設けたり、特定の偽のサービスだけを提供するおとり装置２を設けたりすることができる。したがって、攻撃者に対して正規のサーバ装置により近いサービスを提供することができ、また、特定のサービス向けの正常動作定義をもつことでより運用性を向上させることもできる。

【０１３９】

（第９実施形態）

第９実施形態のファイアウォール装置は、第１～第８実施形態における誘導部に加えて、出力パケット誘導部を有する。出力パケット誘導部は、内部ネットワーク３からインターネット４へ向けて送信される出力ＩＰパケットに対して、上述したパケットフィルタリングおよびおとり装置への誘導処理を行う。

【０１４０】

このような出力パケット誘導部を設けることで、内部ネットワーク３の運用規定として、インターネット４へのアクセスを禁じているような場合に、内部ネットワーク３からイ

ンターネット４への不法なアクセスを検知し、その記録をとることができる。

【０１４１】

（第１０実施形態）

上記第１～第９実施形態の説明では機能ブロック構成を用いたが、本発明はこれに限定されるものではなく、ソフトウエアにより同一の機能を実現することもできる。

【０１４２】

図３１は、本発明の第１０実施形態による攻撃防御システムの概略的構成図である。本実施形態のファイアウォール装置には、プログラム制御プロセッサ１１０１、上記第１～第９実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ１１０２、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース１１０３、および各種インタフェース１００、１０４～１０６が設けられている。同様に、本実施形態のおとり装置には、プログラム制御プロセッサ２１０１、上記第１実施形態で説明したおとり装置としての機能ブロックを実現するプログラムのセットを格納したプログラムメモリ２１０２およびファイアウォール装置とのインタフェースが設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第１～第９実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。

【０１４３】

（第１１実施形態）

上記第１～第１０実施形態では、ファイアウォール装置とおとり装置とが別ユニットになった攻撃防御システムを例示したが、本発明はこれに限定されるものではなく、ハードウエア的に１ユニットで構成することもできる。１ユニットは、取り扱いが容易であり小型化し易いというメリットがある。

【０１４４】

図３２は、本発明の第１１実施形態による攻撃防御ユニットの概略的構成図である。本実施形態の攻撃防御ユニットには、ファイアウォール装置用のプログラム制御プロセッサ１１０１、おとり装置用のプログラム制御プロセッサ２１０１、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース１１０３、上記第１～第９実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ１１０４、および各種インタフェース１００および１０４が設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第１～第９実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。また、プロセッサ１１０１とプロセッサ２１０１とを単一のプロセッサで構成しても良い。

【０１４５】

（第１２実施形態）

１２．１）構成

図３３は、本発明の第１２実施形態によるおとり装置のブロック図である。本実施形態におけるおとり装置３７は、第１～第１０実施形態におけるおとり装置２の攻撃検知部２０２に代えて、イベント管理部３７０１および攻撃検知部３７０２を備える。

【０１４６】

イベント管理部３７０１は、プロセッサ２０１から伝達されるプロセス状況（以下イベント）を内部的に備えたキューに一時格納しながら、所定の条件を満たす関係をもつ過去のイベントとの間にリンク付けを行い、当該イベントとリンクを攻撃検知部３７０２に伝達する。また、攻撃検知部３７０２からリンクの入力を受けて、リンク先またはリンク元イベントを返す。

【０１４７】

攻撃検知部３７０２は、イベントとリンクの組の伝達を受けて、必要に応じて、イベント管理部３７０１を用いてリンクを探索しながら、所定の攻撃検知ルールとの照合によって攻撃の有無を判定し、攻撃があった場合にファイアウォール装置にその旨を通知するた

めのアラームを送信する。

【０１４８】

１２．２）動作

図３４は、本発明の第１２実施形態によるおとり装置３７の動作を示すフローチャートである。

【０１４９】

１２．２．１）イベント伝達

まず、ファイアウォール装置１から転送された入力ＩＰパケットを受けて、プロセッサ２０１上の偽サービスを提供するためのプログラムが動作する。第１～第１０実施形態におけるおとり装置２とは異なり、この偽サービス提供は正規のサービス提供と全く同じように、ネットワーク入出力・プロセスの生成と停止（プロセス生滅）・ファイル入出力を行うものとする。

【０１５０】

プロセッサ２０１は、当該プログラムを動作させながら、さらに、ネットワーク入出力・プロセス生滅・ファイル入出力に係るイベントを、イベント管理部３７０１に随時伝達する（ステップＦ１）。

【０１５１】

イベントには、少なくとも、イベント名および引数の値や、イベントの返値や、当該イベントを発行したプロセスのプロセスＩＤが含まれる。この他、イベントの発生時刻などを含めてもよい。

【０１５２】

１２．２．２）イベント種別の判定

イベントの伝達を受けたイベント管理部３７０１では、まず所定のイベント種別判定ルールに従って、イベント種別を判定する（ステップＦ２）。イベント種別判定ルールは、少なくともネットワーク入出力・プロセス生滅・ファイル入出力を区別できれば十分である。たとえば、プロセッサ２０１が伝達するイベントの名前と、イベント種別との対応関係を定めたテーブル（図３５参照）を予め用意しておき、イベントが伝達されるたびに当該テーブルを検索して、イベント種別を導けばよい。

【０１５３】

１２．２．３）イベント管理キューへの追加

そして、イベント管理部３７０１は、前記イベントをキューに格納する（ステップＦ３）。キューは1本でもよいが、並列処理や後段の処理を簡単にするために、複数本を備えてもよい。ここでは、たとえば、イベント種別ごとに1本ずつのキューを備えるものとする（図３６参照）。この場合、前記イベント種別判定ルールによって求められたイベント種別について、対応するキューを選択し、その最後尾に前記イベントを追加する。

【０１５４】

１２．２．４）イベント間のリンク付け

さらに、イベント管理部３７０１は、最後にキューに追加したイベント（カレントイベント）について、所定のリンク付けルールにしたがって、関連イベントとの間にリンク付けを行う（ステップＦ４）。リンク付けルールは、少なくともイベントの発生源となったプロセスの生成イベントから、当該イベントへのリンクを生成できれば十分である（図４３参照）。関連イベントとのリンク付けを入力した攻撃検知部３７０２は、ＤＴ定義にしたがって攻撃の有無を判定する（ステップＦ５～Ｆ７）。詳しくは後述するが、関連イベントとのリンク付けとＤＴ定義に記載された各ルールとの照合を行い、合致するルールがあるか否かを判定し（ステップＦ６）、合致するルールがあれば（ステップＦ５のＹ）、さらに攻撃であるかどうかを判定する（ステップＦ７）。攻撃があれば、ただちにアラームを生成し、ファイアウォール装置１に送信する（ステップＦ８）。以下、さらに詳細に説明する。

【０１５５】

１２．２．４．１）基本的なリンク付けルール

図３７を参照しながら、より具体的な例として、もっとも基本的なリンク付けルールを示す。

【０１５６】

図３７において、まず、前記カレントイベントの発行源プロセスＩＤを抽出する（ステップＨ１）。そして、プロセスイベント管理キューの最後尾にあるイベントを参照する（ステップＨ２）。

【０１５７】

次に、現在参照しているイベントが、プロセス生成イベントか否かを判別する（ステップＨ３）。具体的には、例えば、予め定めたイベント名と、現在参照中のイベントに記載されたイベント名が一致するかどうかを検査する。

【０１５８】

そして、プロセス生成イベントではないと判定された場合は、参照先を１つ前方に移動させ、ステップＨ３へ戻る（ステップＨ４）。

【０１５９】

一方、プロセス生成イベントであると判定された場合は、現在参照しているイベントのプロセスＩＤを参照して、前記発行源プロセスＩＤと比較する（ステップＨ５）。一致する場合は、ステップＨ６に進み、一致しない場合は、ステップＨ４に戻る。

【０１６０】

なお、カレントイベントがプロセス生成イベントである場合、ステップＨ２で参照されるイベントはカレントイベント自身である。しかし、どのオペレーティングシステムにおいても、プロセス生成の際に、同じプロセスＩＤが割り当てられることはあり得ない。したがって、ステップＨ５において、カレントイベントの発行源プロセスＩＤと、カレントイベントのプロセスＩＤは一致せず、必ずステップＨ４へ戻る。

【０１６１】

そして、当該プロセス生成イベントから、カレントイベントへの、順方向リンクをプロセス生成イベントに付加する（ステップＨ６）。さらに、カレントイベントからプロセス生成イベントへの、逆方向リンクをカレントイベントに付加する（ステップＨ７）。順方向および逆方向のリンクの一例は図４３に示される。

【０１６２】

こうして付加された順方向リンクは、イベント間の関係を時系列に沿った形で保持するためのものであり、逆方向リンクは、イベント間の関係を時系列とは逆順に保持するためのものである。以降の処理において、イベント間の時間的な関係を利用するので、同じイベントに付加された、順方向リンクと逆方向リンクはいつでも区別できるようにしておくことが望ましい。

【０１６３】

１２．２．４．２）イベント－コンテキスト対の伝達

その後、イベント管理部３７０１は、前記カレントイベントと、そのコンテキストとの組（イベント－コンテキスト対）を攻撃検知部３７０２へ出力する。図３８に示すように、コンテキストとは、カレントイベントに付加された全ての順方向リンクおよび逆方向リンクの集合を指す。

【０１６４】

１２．２．５）攻撃検知

図３９に、予め定められたドメイン－タイプ制約付きの正常動作定義（以下、ＤＴ定義という。）の一例を示す。イベント－コンテキスト対の入力を受けた攻撃検知部３７０２は、ＤＴ定義にしたがって攻撃の有無を判定する（図３４のステップＦ５）。

【０１６５】

１２．２．５．１）ドメイン－タイプ制約つきルールの判定

（ドメイン－タイプ制約つきルールの構成要素）

ＤＴ定義内の各ドメイン－タイプ制約つきルールは、少なくとも、

（１）ドメイン－タイプ制約（以下、ＤＴ制約）

（２）イベント制約
（３）判定値
という構成要素をもつ。
【０１６６】
（１）ＤＴ制約は、イベントの発生原因となったアクセスの送信元ホストもしくはそのネットワークドメインに関する制約（ドメイン制約）と、イベントの発生源となったプロセスおよびその先祖プロセスに関する制約（タイプ制約）とを論理積で組み合わせた制約条件を示しており、前記イベントがこの制約を満たす場合のみ、（２）イベント制約の判定を行う。
【０１６７】
ＤＴ制約について、より具体的に説明する。たとえば、以下のようにＤＴ制約が記述されているものとする。
・タイプ制約：「プログラムＴ１」「プログラムＴ２」
・ドメイン制約：「１３３．２０３．１．１２８」。
【０１６８】
図４０に示すように、これらの制約は以下の条件を指定する。
・イベントの発生源である何らかのプロセスの先祖として、「プログラムＴ　２」のプロセスが存在すること。
・「プログラムＴ２」の親プロセスとして「プログラムＴ１」のプロセスが存在すること。
・「サーバプログラム」がＩＰアドレス「１３３．２０３．１．１２８」のホストからアクセスを受けていること。
【０１６９】
なお、図４０は「サーバプログラム」が「プログラムＴ１」の先祖である場合を示しているが、一般的にはイベント発生源のプロセスおよびその先祖プロセスのいずれかが「サーバプログラム」であれば十分である。たとえば、「プロセスＴ１」または「プロセスＴ２」が「サーバプログラム」であってもよいし、イベント発生源のプロセスそのものが「サーバプログラム」であってもよい。
【０１７０】
（２）イベント制約と（３）判定値は、第１実施形態におけるおとり装置２の正常動作定義と同じ意味である。すなわち、前記（２）はイベント名とパラメータ値についての正規表現の組である。攻撃検知部３７０２は、それらが前記イベント－コンテキスト対におけるイベントの名前およびパラメータ値と、合致するかどうかを判定する。
【０１７１】
また、前記（３）は、前記イベントが前記（２）に合致した場合に、攻撃検知部３７０２がそれを正常と判定するか、攻撃と判定するか、を定める値である。たとえば、正常と判定する場合の判定値を「ＡＬＬＯＷ」、攻撃と判定する場合の判定値を「ＤＥＮＹ」とする。なお、攻撃と判定する場合の判定値については、第１実施形態におけるおとり装置２と同様の攻撃種別を用いても良い。
【０１７２】
以下、特にＤＴ制約について、より具体的な記述例と判定方法を示す。
【０１７３】
（ドメイン制約の記述例）
ドメイン制約は、例えば、ＩＰアドレスの集合として記述できる。具体的には、１つのＩＰアドレスを10進3桁の数の4組「xxx.yyy.zzz.www」として記述し、「．」で区切ってＩＰアドレス集合の要素を列挙する。またその便法として、「xxx.yyy.zzz.www/vvv」（vvvはビットマスク）などの表記を許してもよい。あるいは、正規表現を用いることもできる。
【０１７４】
（タイプ制約の記述例）

また、タイプ制約は、例えば、実行形ファイル名に関する正規表現をもちいて記述できる。また、実行形ファイル名の連結によって、プロセスの親子関係を表現できるようにして、その正規表現を用いてもよい。

【０１７５】

具体的には、プロセスの親子関係を「<F(1)><F(2)>(中略)<F(N)>」（各F(i)は実行形ファイル名）という形式で表すことができる。このとき、それぞれの「<F(i)>」は、プロセスに関する制約であり、これにマッチする名前をもつ実行形ファイルの起動後のプロセスに相当する。また、その列挙は前方に記述されたプロセスを親とし、後方に書かれたプロセスをその直接の子とすることを示す。

【０１７６】

したがって、実行形ファイル「Ａ」に相当するプロセスＡの子として、実行形ファイル「Ｂ」に相当するプロセスＢが、さらにその子として実行形ファイル「Ｃ」に相当するプロセスＣが起動されている場合、プロセスＡ、Ｂ、Ｃの親子関係は「<A><B><C>」という文字列で表記される。

【０１７７】

こうしたプロセスの親子関係に関する正規表現をもって、タイプ制約とすることができる。具体的には、「<A>.*<C>」というタイプ制約は、実行形ファイル「Ｃ」に相当するプロセスＣが起動しており、その親プロセス（直接でなくともよい）が実行形ファイル「Ａ」である場合に、マッチする。

【０１７８】

また特殊な例として、タイプ制約が「^」で始まる場合、その直後に記述されたプロセスが、プロセッサ２０１上のオペレーティングシステムの起動直後に生成されたプロセスである場合にマッチする。

【０１７９】

一般に、オペレーティングシステムは、唯一の初期プロセスをもち、起動直後のプロセスはすべて、その初期プロセスの直接の子となる。初期プロセスに相当する実行形ファイルが必ずしも存在するわけではないので、これを特殊記号「^」で表記することで、ＤＴ定義の汎用性を向上させることができる。

【０１８０】

別の特殊な例として、タイプ制約が「$」で終わる場合、「$」の直前に指定されたプロセス「<F(N)>」が、イベント発生源であることを示す。

【０１８１】

（ＤＴ制約とイベント－コンテキスト対の比較）

ＤＴ制約の判定において、前記イベント－コンテキスト対との比較を行うが、その方法について、詳細に説明する。

【０１８２】

タイプ制約の判定は、コンテキストに含まれる逆方向リンクのうち、前記プロセスイベント管理キュー内のイベントを指すもの（以下、プロセスリンク）を選択する。前記リンク付けルールに従えば、任意のイベントにはその発生源であるプロセスの生成イベントを指すプロセスリンクが必ず存在する。

【０１８３】

そして、当該プロセスリンクを辿り、その先のイベントを参照して、実行形ファイル名をスタックに積む。こうしたステップを、プロセスリンクが存在しないイベントに到達するまで繰り返す。

【０１８４】

一般的なオペレーティングシステムでは、任意のプロセスの先祖として初期プロセスが存在する。そのようなオペレーティングシステムがプロセッサ２０１上で動作している場合、初期プロセスは親プロセスをもたないため、かならず本ステップの繰り返しは終了する。

【０１８５】

もし、初期プロセスが存在しないようなオペレーティングシステムがプロセッサ２０１上で動作している場合、イベント管理部３７０１において、仮想的な初期プロセスの生成イベントを、プロセスイベント管理キューの先頭に配置するようにすればよい。

【０１８６】

前記ステップが終了した後、スタックに積まれた実行形ファイル名の系列は、前記初期プロセスから、前記イベント発生源のプロセスに至るまでのプロセス系列が得られる。当該プロセス系列は、プロセス間の親子関係を時系列順にならべたものに一致するので、当該プロセス系列と、タイプ制約とを比較することで、イベント系列とタイプ制約が合致するか否かを判定できる。

【０１８７】

また、ドメイン制約の判定は、タイプ制約と同様にプロセスリンクをたどりながら、順次ネットワークイベント管理キューへの順方向リンクを参照していく。順方向リンクの先に、接続要求の受信イベントが見つかれば、当該イベントに記載されているソースＩＰアドレスをアクセス元ホストのＩＰアドレスとみなし、探索を終了する。

【０１８８】

そして、前記ＩＰアドレスと、ドメイン制約とを比較して合致するか否かを判定する。

【０１８９】

１２．２．５．２）アラーム送信

以上のようにして、イベントーコンテキスト対とＤＴ定義に記載された各ルールとの照合を繰り返し行い、（１）ＤＴ制約および（２）イベント制約の全てに合致するかどうかを確認する（図３４のステップＦ６）。もし、両方の制約に合致するルールが１つも無い場合は、デフォルト値として予めＤＴ定義内に設定された判定値を採用する。

【０１９０】

合致するルールがあれば、当該ルールの（３）判定値を参照して、前記イベントーコンテキスト対が攻撃であるかどうかを判定する（ステップＦ７）。

【０１９１】

そして、採用された判定値が許可（ＡＬＬＯＷ）以外の場合、ただちにアラームを生成し、ファイアウォール装置１に送信する（ステップＦ８）。アラームの内容は第１実施形態におけるおとり装置２と同様に、少なくとも、前記アクセスのソースＩＰアドレスと、前記判定値を含み、その他、アクセス元のポート番号などを含めても良い。

【０１９２】

１２．３）効果

本実施形態におけるおとり装置３７は、プロセッサ２０１が発生するイベントについて、イベント管理部３７０１でイベント間の因果関係の分析と履歴管理を行っている。これを用いて、攻撃検知部３７０２でアクセス元ホストや、サブシステムの呼び出し関係などを含めた、より詳細な正常動作定義が可能となる。これにより、複雑なサブシステム構成をもつサーバに対する攻撃検知性能を向上させると共に、保守作業の誤検知を低減させることができる。

【０１９３】

１２．４）具体例

本実施形態におけるおとり装置３７の動作を具体例を用いて説明する。

【０１９４】

１２．４．１）構成

まず、おとり装置３７のプロセッサ２０１上で、偽サービスとしてＷＷＷサーバが動作しているものとする。そして、そのコンテンツ領域を、"C:\Inetpub\wwwroot" ディレクトリ以下とする。また、ＷＷＷサーバのサブシステムとして、以下の２つのＣＧＩモジュールを備えるものとする。

【０１９５】

（Ａ）登録ＣＧＩ：顧客情報を顧客データベースに登録するＣＧＩ
（パス名："C:\Inetpub\scripts\regist.exe"）

（Ｂ）出力ＣＧＩ：顧客データベースの内容をＨＴＭＬに変換し、ブラウザから閲覧するＣＧＩ（パス名："C:\Inetpub\scripts\view.exe"）。

【０１９６】

ただし、出力ＣＧＩは専ら保守作業の１つとして利用されることを目的としており、内部ネットワーク４上の管理ドメイン"１０．５６．３．０／２４"からのアクセスのみに応答することを要求されているものとする。また、別の保守作業として、ＦＴＰサーバを介したコンテンツの更新が想定されているものとする。

【０１９７】

以下、クライアントとサーバとの間で行われる接続開始から要求データ送信完了までのＩＰパケット送受信をまとめて「アクセス」と呼ぶ。同様に、応答データ送信開始から接続終了までのＩＰパケット送受信をまとめて「（当該アクセスに対する）応答」と呼ぶ。

【０１９８】

こうした構成に対するＤＴ定義の例として、図３９に示すファイル４１０１のような設定がなされているものとする。ただし、「#」で始まる行はコメント行であり、無視されるものとする。

【０１９９】

１２．４．２）動作例１

具体的な動作の一例として、外部ネットワーク３上のクライアント（１３３．２０１．５７．２）から、内部ネットワーク４上のＷＷＷサーバに対する不審アクセスがあって、それが正常である場合のおとり装置３７の動作例を示す。

【０２００】

このとき、第１～第１０実施形態のいずれかのファイアウォール装置によって、前記不審アクセスはおとり装置３７に誘導され、偽サービス処理が開始される。

【０２０１】

そして、おとり装置３７のプロセッサ２０１上のＷＷＷサーバでは、前記不審アクセスを受信を初めとして、以下のような処理を行う。

（Ａ）１３３．２０１．５７．２からのアクセスを受信する。

（Ｂ）子プロセスを生成する。

（Ｃ）子プロセスで、当該アクセスにおける要求データに応じて、

例えば、

（Ｃ－１）コンテンツ領域に対するファイル入出力

（Ｃ－２）データベース操作のためのファイル入出力

を行う。

【０２０２】

以下に、それぞれのステップごとにおとり装置３７の内部動作を説明する。

【０２０３】

１２．４．２．１）不審アクセスの受信

プロセッサ２０１上のＷＷＷサーバが、不審アクセスを受信した直後、プロセッサ２０１からイベント管理部３７０１に、イベント３５０１が伝達される（図４１参照）。

【０２０４】

イベント３５０１の内容には、少なくとも、イベント名（ＮＷ＿ＡＣＣＥＰＴ）、アクセス元ＩＰアドレス（１３３．２０１．５７．２）、当該イベントの発生源であるプロセスであるＷＷＷサーバのプロセスＩＤ（７０９）が記載される。この他、アクセス元のポート番号、ＴＣＰ／ＵＤＰなどのプロトコル種別、要求データなどの情報を含めてもよい。

【０２０５】

イベント３５０１を受け取ったイベント管理部３７０１は、直ちに図３５に示すような対応表を参照して、イベント名「ＮＷ＿ＡＣＣＥＰＴ」のイベント種別を「ネットワーク」であると判定し、前記イベントに追記する。そして、イベント種別「ネットワーク」に

対応するイベント管理キューに、イベント３５０１を追加する。さらに、所定のリンク付けルールに従いイベント３５０１と関連する過去のイベントとの間にリンク付けを行う。

【０２０６】

具体的には、図４２を参照すると、イベント種別「プロセス」に対応するイベント管理キューから、前記イベント内に記載されたプロセスＩＤ（７０９）に相当するイベント名「ＰＲＯＣ＿ＥＸＥＣ」または「ＰＲＯＣ＿ＦＯＲＫ」をもつイベント３６０１を検索する。このとき、最後尾から前方に向けてキュー走査を行い、最初にマッチするイベント３６０１を発見したとき、後の処理へ進む。

【０２０７】

そして、イベント３６０１に対して、イベント３５０１への順方向リンク（図４３の実線）を付加し、イベント３５０１に対して、イベント３６０１への逆方向リンク（図４３の破線）を付加する。以下、リンクを図示する際は、逆方向リンクを省略する。

【０２０８】

その後、イベント３５０１に関するイベント－コンテキスト対を、攻撃検知部３７０２に伝達する。

【０２０９】

攻撃検知部３７０２では、まず、所定のＤＴ定義ファイル４１０１を参照し、各ルールを抽出する。本例では、ＤＴ定義ファイル４１０１の先頭から前方に向かって1行ずつルールを抽出していく。なお、「＃」で始まる行はコメントを意味し、コメントと空行はスキップされる。

【０２１０】

まず、最初のルール（図３９のルール１）が抽出される。本例の場合、ドメイン制約は「0.0.0.0/0」であり、これは任意のネットワークドメインにマッチする。また、タイプ制約は「<inetinfo.exe>」であり、WWWサーバに相当するプロセスまたはその子プロセスにマッチする。

【０２１１】

前記ＤＴ制約とイベント３５０１との照合のために、攻撃検知部３７０２は、まず、イベント３５０１のコンテキスト内の逆方向リンクをイベント管理部３７０１に入力して、リンク先のイベント３６０１の出力を受ける。

【０２１２】

次に、イベント３６０１の内容を参照して、プロセスＩＤ「７０９」に相当するプログラム実行形ファイルのパス名「C:\Web\inetinfo.exe」を抽出する。さらに、イベント３６０１の逆方向リンクを先と同様にして、さらに親プロセスの生成イベントの取得を行おうとするが、本例では存在しない。したがって、イベント３６０１に相当するプロセスの親子関係を「<inetinfo.exe>」と判定し、前記タイプ制約「<inetinfo.exe>」にマッチすることを確認する。

【０２１３】

次に、ドメイン制約との照合を行うため、再びイベント３５０１の内容を参照する。まず、イベント３５０１のイベント種別が「ネットワーク」であることを確認して、さらにイベント名が「ＮＷ＿ＡＣＣＥＰＴ」であることを確認する。
これにより、イベント３５０１自身がドメイン制約の対象となるので、さらにソースＩＰアドレスを参照して、「１３３．２０１．５７．２」を取得する。この値は、前記ドメイン制約「0.0.0.0/0」にマッチする。

【０２１４】

続けて、イベント制約の判定を行う。イベント名「FILE_WRITE」と、イベント３５０１のイベント名「NW_ACCEPT」とを照合するが、この場合、一致しないので、当該ルールの照合処理を中断し、次のルール照合へ移る。

【０２１５】

以下、同様にして、ルール抽出、ＤＴ制約の照合、イベント制約の照合を繰り返すが、本例の場合、いずれのルールにも合致しないため、デフォルトルール「ＤＥＦＡＵＬＴ；

ＡＬＬＯＷ」が採用され、イベント３５０１を「正常」と判定し、ＤＴ定義全体の照合を終了する。

【０２１６】

１２．４．２．２）子プロセスの生成

次に、プロセッサ２０１上のＷＷＷサーバは前記不審アクセスの要求データを処理するために、子プロセスを生成する。一般に複数のアクセスを並行処理するサーバは、このように個々のアクセスに対する要求データ処理と応答処理を子プロセス側で行う。ただし、逐次的にアクセスを処理するサーバもあり、こうした場合には、直ちに要求データの処理に移る。また、子プロセスの代わりに子スレッドを作る場合もあるが、本例ではスレッドと厳密な意味でのプロセスとを同等に、「（広義の）プロセス」として扱う。

【０２１７】

プロセッサ２０１は、子プロセスの生成動作を受けて、イベント３８０１（図４４参照）をイベント管理部３７０１に伝達する。イベント３８０１の内容には、少なくとも、イベント名「PROC_FORK」と、実行形ファイルのパス名「C:\Web\inetinfo.exe」と、生成された子プロセスのプロセスＩＤ（８００）と、当該イベントの発生源であるプロセスＩＤ（７０９）が記載される。この他、スレッドと（狭義の）プロセスを区別するためのフラグなどを設けてもよい。

【０２１８】

イベント３８０１の伝達を受けたイベント管理部３７０１は、前記イベント３５０１と同様にして、イベント３８０１のイベント種別（「プロセス」）を判定し、プロセスイベント管理キューへイベント３８０１を追加した後、イベント３６０１からイベント３８０１への順方向リンクと、イベント３８０１からイベント３６０１への逆方向リンクをつける（図４４参照）。そして、イベント３８０１に関するイベント－コンテキスト対を攻撃検知部３２０２へ伝達する。

【０２１９】

攻撃検知部３７０２では、先と同様に、イベント３８０１に関するイベント－コンテキスト対のリンクを探索して、イベント３８０１のＤＴ判定を行う。その結果、イベント３８０１そのものがイベント種別「プロセス」であり、イベント３８０１の逆方向リンク先をイベント管理部３２０１から取得すると、イベント３６０１が得られる。したがって、イベント３８０１のタイプは「<inetinfo><inetinfo>」と判定される。

【０２２０】

そして、再びイベント３８０１を参照するが、そのイベント種別は「ネットワーク」ではないので、イベント３８０１の順方向リンクを参照しようとする。しかし、イベント３８０１にはネットワークイベント管理キューへの順方向リンクがないので、イベント３８０１の逆方向リンク先をイベント管理部３７０１から取得する。イベント３８０１にはネットワークイベント管理キューへの順方向リンクがあるので、さらにその先にあるイベント３５０１を、イベント管理部３２０１から取得する。イベント３５０１は、イベント名が「ＮＷ＿ＡＣＣＥＰＴ」、ソースＩＰアドレスが「１３３．２０１．５７．２」であるので、イベント３８０１のドメインを「１３３．２０１．５７．２」と判定する。

【０２２１】

なお、本例のように、プロセスの生成に係るイベントのドメイン決定時には、特別にその旨をイベント管理部３７０１に伝達して、イベント３８０１からイベント３５０１への逆方向リンクを付加するようにしてもよい。このようにすることで、ＷＷＷサーバが子プロセスの実行中に、新たなアクセスを受信した場合でも、当該子プロセスが発生する後続イベントのドメインを誤ることはない。

【０２２２】

次に、ＤＴ定義ファイル４４０１との照合を行うが、本例の場合、イベント３５０１と同様に、イベント３８０１は、いずれのルールにも完全に合致することなく、デフォルトの判定値（「ＤＥＦＡＵＬＴ；ＡＬＬＯＷ」）が採用されるので、「正常」と判定される。

【０２２３】
１２．４．２．３）コンテンツ領域に対するファイル入出力
次に、プロセッサ２０１上のＷＷＷサーバの子プロセスは前記不審アクセスの要求データを処理する。ここでは、まず、当該要求データが「GET /HTTP/1.0」である場合の動作例を示す。
【０２２４】
前記要求データに対して、前記子プロセスは、コンテンツ領域内のファイル「C:\Inetpub\wwwroot\default.htm」を読み込む。この動作を受けて、プロセッサ２０１はイベント３９０１（図４５参照）をイベント管理部３７０１に伝達する。イベント３９０１の内容には、少なくとも、イベント名「ＦＩＬＥ＿ＲＥＡＤ」、読み込むファイルのパス名「C:\Inetpub\wwwroot\default.htm」、当該イベントの発生源である子プロセスのプロセスＩＤ（８００）が記載される。この他、実際に読み込んだファイル内容などを含めても良い。
【０２２５】
次に、イベント管理部３７０１は、イベント３９０１のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント３９０１を追加する。その後、イベント３８０１からイベント３９０１への順方向リンクと、イベント３９０１からイベント３８０１への逆方向リンクを付加する（図４５参照）。その後、イベント３９０１に関するイベント－コンテキスト対を攻撃検知部３２０２に伝達する。
【０２２６】
そして、攻撃検知部３７０２は、イベント３９０１に関するイベント－コンテキスト対に対するＤＴ判定を行う。その結果、イベント３９０１のタイプを「<inetinfo.exe><inetinfo.exe>」、ドメインを「１３３．２０１．５７．２」と判定する。
【０２２７】
次に、攻撃検知部３７０２は、ＤＴ定義ファイル４１０１との照合を行う。本例の場合、以下のルール（図３９のルール２）に合致し、その判定値が「ＡＬＬＯＷ」であることから、「正常」と判定される。
【０２２８】
0.0.0.0/0、 <inetinfo.exe>、 FILE_READ、 C:\Inetinfo\.*;
ALLOW
１２．４．２．４）データベース操作
別の要求データの例として、「GET /cgi-bin/regist.exe?name=someoneHTTP/1.0」である場合の動作例を示す。
【０２２９】
（ア）ＣＧＩの起動
この要求データに対して、前記子プロセスは、まず、前記登録ＣＧＩを起動して、新たな孫プロセスを生成する。また、ＵＲＬパラメータ「name=someone」は環境変数「QUERY_STRING」に格納されているものとする。
【０２３０】
この動作を受けて、プロセッサ２０１はイベント４００１（図４６参照）をイベント管理部３７０１に伝達する。イベント４００１の内容には、少なくとも、イベント名「PROC_EXEC」と、実行形ファイルのパス名「C:\Inetpub\scripts\regist.exe」と、前記孫プロセスのプロセスＩＤ（８０１）と、当該イベントの発生源である前記子プロセスのプロセスＩＤ（８００）とが記載される。この他、環境変数の情報などを含めてもよい。
【０２３１】
次に、図４６を参照すると、イベント管理部３７０１は、イベント４００１のイベント種別を「プロセス」と判定し、プロセスイベント管理キューにイベント４００１を追加する。その後、イベント３８０１からイベント４００１への順方向リンクと、イベント４００１からイベント３８０１への逆方向リンクを付加し、イベント４００１に関するイベント－コンテキスト対を攻撃検知部３７０２に伝達する。

【０２３２】
そして、攻撃検知部３７０２は、イベント４００１に関するイベント－コンテキスト対に対して、イベント３９０１と同様にＤＴ判定を行う。その結果、イベント４００１のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「１３３．２０１．５７．２」と判定する。
【０２３３】
次に、攻撃検知部３７０２は、ＤＴ定義との照合を行う。本例の場合、合致するルールがないので、デフォルトルールの判定値「ＡＬＬＯＷ」を採用して、正常と判定する。
【０２３４】
（イ）ＣＧＩの動作
続けて、前記登録ＣＧＩがデータベース出力を行う。本例では、登録ＣＧＩが操作するデータベースを「C:\data\client.db」ファイルとする。
【０２３５】
データベース出力の具体例として、登録ＣＧＩは前記環境変数「QUERY_STRING」の値を読み取り、その値「name=someone」に改行記号を加えた文字列を前記データベースの末尾に追記するものとする。
【０２３６】
この動作を受けて、プロセッサ２０１はイベント４１０１（図４７参照）をイベント管理部３７０１に伝達する。イベント４１０１の内容には、少なくとも、イベント名「FILE_WRITE」と、実行形ファイルのパス名「C:\data\client.db」と、当該イベント発生源である前記孫プロセスのプロセスＩＤ（８０１）とが記載される。この他、書き出したデータの内容などを含めてもよい。
【０２３７】
次に、図４７を参照すると、イベント管理部３７０１は、イベント４１０１のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント４１０１を追加する。その後、イベント４００１からイベント４１０１への順方向リンクと、イベント４１０１からイベント４００１への逆方向リンクを付加し、イベント４１０１に関するイベント－コンテキスト対を攻撃検知部３７０２に伝達する。
【０２３８】
そして、攻撃検知部３７０２は、イベント４１０１に関するイベント－コンテキスト対に対して、ＤＴ判定を行う。その結果、イベント４１０１のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「１３３．２０１．５７．２」と判定する。
【０２３９】
次に、攻撃検知部３７０２は、ＤＴ定義ファイル４１０１との照合を行う。本例の場合、以下のルール（図３９のルール３）に合致するので、その判定値「ＡＬＬＯＷ」を採用して、正常と判定する。
【０２４０】
0.0.0.0/0、 <Inetinfo.exe><regist.exe>$、 FILE_WRITE、
C:\data\client.db; ALLOW
１２．４．３）動作例２
具体的な動作の別の例として、外部ネットワーク３上のクライアント（１３３．２０１．５７．２）から、内部ネットワーク４上のＷＷＷサーバに対する不審アクセスがあって、それが攻撃である場合を示す。
【０２４１】
このとき、第１～第１０実施形態のいずれかのファイアウォール装置によって、前記不審アクセスはおとり装置３７に誘導され、偽サービス処理が行われる。
【０２４２】
その後、おとり装置３７のプロセッサ２０１上のＷＷＷサーバでは、前記不審アクセスを受信を初めとして、以下のような処理を行う。
（Ａ）１３３．２０１．５７．２からのアクセスを受信する。

（Ｂ）子プロセスを生成する。
（Ｃ）子プロセスで、当該アクセスにおける不正な要求データに応じて、所定の処理を行う。例えば、
（Ｃ－１）コンテンツ領域に対する不正ファイル書き出し
（Ｃ－２）データベースに対する不正アクセス
などを行う。
【０２４３】
上記（Ａ）、（Ｂ）は前記動作例１と同様であるため、ここでは攻撃時の動作（Ｃ－１）、（Ｃ－２）のみについて具体例を示す。
【０２４４】
１２．４．３．１）コンテンツ領域に対する不正ファイル書出し
ＷＷＷサーバまたはそのサブシステム（登録ＣＧＩ・出力ＣＧＩ）などに脆弱性が存在するものとする。今、登録ＣＧＩに脆弱性が存在し、「GET/cgi-bin/regist.exe?path=C:\Inetpub\wwwroot\default.htm&data=abcd」というアクセスがあった場合に、コンテンツ領域内のファイル「C:\Inetpub\wwwroot\default.htm」に対して、データ「abcd」が書き込まれるものとする。
【０２４５】
前記不正アクセスがあった場合、前記動作（Ｃ－１）が行われ、プロセッサ２０１はイベント４９０１（図４８参照）をイベント管理部３７０１に伝達する。イベント４９０１の内容には、少なくとも、イベント名「FILE_WRITE」と、実行形ファイルのパス名「C:\Inetpub\wwwroot\default.htm」と、当該イベント発生源である前記孫プロセスのプロセスＩＤ（８０１）とが記載される。
【０２４６】
次に、イベント管理部３７０１は、イベント４９０１のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント４９０１を追加する（図４８参照）。その後、イベント４００１からイベント４９０１への順方向リンクと、イベント４９０１からイベント４００１への逆方向リンクを付加し、イベント４９０１に関するイベント－コンテキスト対を攻撃検知部３７０２に伝達する。
【０２４７】
そして、攻撃検知部３７０２は、イベント４９０１に関するイベント－コンテキスト対に対してＤＴ判定を行う。その結果、イベント４９０１のタイプを「<inetinfo.exe><inetinfo.exe><regist.exe>」、ドメインを「１３３．２０１．５７．２」と判定する。
【０２４８】
次に、攻撃検知部３７０２は、ＤＴ定義との照合を行う。本例の場合、以下のルール（図３９のルール６）に合致するので、その判定値「ＤＥＮＹ」を採用し、攻撃があったものと判定する。
【０２４９】
0.0.0.0/0、 <inetinfo.exe>、 FILE_WRITE、 .*; DENY
そして、攻撃検知部３７０２は、攻撃元ホスト「１３３．２０１．５７．２」を含むアラームを直ちに生成して、前記ファイアウォール装置１へ送信する。
【０２５０】
なお、ＷＷＷサーバもしくはそのサブシステムの脆弱性を介した不正なファイル書き込みがあった場合、すべて前記と同様にして攻撃であると判定される。
【０２５１】
また、ＷＷＷサーバ以外のサーバ、例えばＦＴＰサーバを介したコンテンツ領域への書き込みがあった場合、以下のルール（図３９のルール５)に合致しない限り、すなわち、管理ドメインからの正当な保守作業でない限り、
10.56.192.0/24、 ^<ftpd.exe>+$、 FILE_WRITE、 C:\Inetpub\wwwroot\.*; ALLOW
以下のルール（図３９のルール８）により、攻撃であると判定される。
【０２５２】

0.0.0.0/0、 .*、 FILE_WRITE、 C:\Inetpub\wwwroot\.*; DENY

１２．４．３．２）データベースへの不正アクセス

ＷＷＷサーバまたはそのサブシステム（登録ＣＧＩ・出力ＣＧＩ）などに脆弱性が存在するものとし、「GET /cgi-bin/..%c1%c9../data/client.db HTTP/1.0」というアクセスによって、前記顧客データベースを窃取されるものとする。

【０２５３】

前記不正アクセスがあった場合、前記動作が行われたのを受けて、プロセッサ２０１はイベント５００１（図４９参照）をイベント管理部３７０１に伝達する。イベント５００１の内容には、少なくとも、イベント名「FILE_READ」と、実行形ファイルのパス名「C:\data\client.db」と、当該イベント発生源である前記子プロセスのプロセスＩＤ（８００）とが記載される。

【０２５４】

次に、イベント管理部３７０１は、イベント５００１のイベント種別を「ファイル」と判定し、ファイルイベント管理キューにイベント５００１を追加する。その後、イベント３８０１からイベント５００１への順方向リンクと、イベント５００１からイベント３８０１への逆方向リンクを付加し、イベント５００１に関するイベント－コンテキスト対を攻撃検知部３７０２に伝達する。

【０２５５】

そして、攻撃検知部３７０２は、イベント５００１のイベント－コンテキスト対に対してＤＴ判定を行う。その結果、イベント５００１のタイプを「<inetinfo.exe><inetinfo.exe>」、ドメインを「１３３．２０１．５７．２」と判定する。

【０２５６】

次に、攻撃検知部３７０２は、ＤＴ定義との照合を行う。本例の場合、以下のルール（図３９のルール７）に合致するので、その判定値「ＤＥＮＹ」を採用し、攻撃があったものと判定する。

【０２５７】

0.0.0.0/0、 .*、 FILE_READ|FILE_WRITE、 C:\data\.*; DENY

そして、攻撃検知部３７０２は、攻撃元ホスト「１３３．２０１．５７．２」を含むアラームを直ちに生成して、前記ファイアウォール装置１へ送信する。

【０２５８】

（第１３実施形態）

１３．１）構成

図５０は、本発明の第１３実施形態におけるファイアウォール装置のブロック図である。本実施形態におけるファイアウォール装置５１は、第２実施形態におけるファイアウォール装置５の誘導部５０３および信頼度管理部５０２に代えて、仮想サーバ部５１０１および信頼度管理部５１０２を備える。

【０２５９】

図５１を参照すると、仮想サーバ部５１０１は、接続管理部５２０１と、第１入力バッファ５２０２および第１出力バッファ５２０３と、第２入力バッファ５２０４および第２出力バッファ５２０５とを有する。

【０２６０】

接続管理部５２０１は、パケットフィルタ１０１から伝達された各アクセスに含まれる要求データを信頼度管理部５１０２に入力し、その信頼度を取得する。また、その信頼度に応じて、第１入力バッファ５２０２または第２入力バッファ５２０４への要求データ転送処理や、第１出力バッファ５２０３または第２出力バッファ５２０５からの応答データ読み取り処理などを行う。

【０２６１】

第１入力バッファ５２０２および第１出力バッファ５２０３は、第１の内部通信インターフェース１０４を内部ネットワーク４に接続されており、それぞれサーバ装置への要求データと、サーバ装置からの応答データを一時格納する。

【０２６２】
第２入力バッファ５２０４および第２出力バッファ５２０５は、おとり装置２に接続されており、それぞれおとり装置２への要求データと、おとり装置２からの応答データを一時格納する。また、信頼度管理部５１０２は、仮想サーバ部５１０１の接続管理部５２０１からの要求データ入力に応じて、その信頼度を出力する。
【０２６３】
１３．２）動作
図５２は、第１３実施形態におけるファイアウォール装置３３のフローチャートである。
【０２６４】
１３．２．１）仮接続
図５２において、まず、ファイアウォール装置３３がインタネット３上のあるホストから新たな接続を要求する入力ＩＰパケットを受信して、第２実施形態におけるファイアウォール装置５と同様に、パケットフィルタ１０１とアクセス制御リスト管理部１０２とによって、その通過を認められた場合には、仮想サーバ５１０１の接続管理部５１０１は、前記ホストとの間に仮の接続を確立する（ステップＧ１）。
【０２６５】
１３．２．２）要求データの一時格納
その後、前記インタネット３上のホストから内部ネットワーク４上のサーバに対する要求データを受信する（ステップＧ２）。そして、接続管理部５２０１は、当該要求データを第１入力バッファ５２０２と第２入力バッファ５２０４とに伝達して、一時格納する（ステップＧ３）。
【０２６６】
１３．２．３）信頼度判定
そして、前記要求データを信頼度管理部５１０２に入力し、その信頼度cを取得し（ステップＧ４）、所定の閾値Ｔと比較を行う（ステップＧ５）。
【０２６７】
信頼度管理部５１０２における信頼度の計算方法としては、例えば、要求データをバイトデータの系列パターンとみなして、統計的なパターン解析によって、「頻繁に見られる要求データ」との類似度を計算し、当該類似度をもって信頼度ｃとする方法がある。
【０２６８】
また、単に図５３に示すような、過去に入力された要求データと信頼度との組を管理するためのテーブルを保持し、新たな要求データの入力があるたびに、当該テーブルを参照して、信頼度を求める方法を用いてもよい。より具体的には、ステップＧ８－２でおとり装置２によって正常であることが確認された場合にのみ信頼度を１とし、それ以外の場合、特にステップＧ８－３において、攻撃であることが確認された場合には、信頼度を０とし、以降この信頼度を再利用する方法を用いてもよい。
【０２６９】
さらに、前記テーブルに要求データを直接格納するのではなく、要求データの一方向性ハッシュ関数値を格納する方法を用いてもよい。この場合、既知の要求データが再度入力された場合、その一方向性ハッシュ関数値としても一致するため、その信頼度を正しく取得できる。さらに、要求データのサイズが非常に大きなものになり得る場合でも、一方向性ハッシュ関数値は常に一定のサイズであるため、メモリ効率が良い。ただし、異なる要求データに対する一方向性ハッシュ関数値が一致する（＝衝突する）場合があるが、一般に一方向性ハッシュ関数値が一致する異なる２つの要求データ（特に、一方が正常でもう一方が攻撃であるような場合）を見つけることは困難とされるので、実用上の危険性は極めて小さい。
【０２７０】
１３．２．３．１）要求データを信頼した場合
もし、c≧Ｔであれば（ステップＧ５のＹ）、前記要求データを信頼できるものと判定

し、第１入力バッファ５２０２と、第２入力バッファ５２０４とに、要求データの転送を指示する（ステップＧ６－１）。この指示を受けた第1入力バッファ５２０２は、直ちに格納ずみ要求データを、第１の内部通信インターフェース１０４を介して、内部ネットワーク４上のサーバに転送する。同様に、第２入力バッファ５１０４は、格納ずみ要求データを、第２の内部通信インターフェース１０５を介して、おとり装置２に転送する。

【０２７１】

１３．２．３．２）応答データの確認

その後、第1の内部通信インターフェース１０４を介して、内部ネットワーク４上のサーバから応答データを受信したとき、第１出力バッファ５２０３は当該応答データを一時格納し、接続管理部５２０１に応答のあった旨を伝える（ステップＧ７－１）。

【０２７２】

１３．２．３．３）応答データの転送

接続管理部５２０１は、第１出力バッファ５２０３からデータ受信を伝達された後、直ちに前記ホストに向けて、第１出力バッファ５２０３に格納された応答データを転送する（ステップＧ８－１）。

【０２７３】

１３．２．４）要求データを不審とした場合

一方、ステップＧ５の後、c＜Ｔであれば（ステップＧ５のＮ）、前記要求データを不審であると判定し、第２入力バッファ５２０４のみに、要求データの転送を指示する（ステップＧ６－２）。第２入力バッファ５２０４は、この指示を受けて、直ちに第２の内部通信インターフェース１０５を介して、おとり装置２へ前記要求データを転送する。

【０２７４】

１３．２．４．１）攻撃検知

そして、おとり装置２は第２実施形態と同様にして、攻撃の有無を判定する（ステップＧ７－２）。

【０２７５】

１３．２．４．２）攻撃が検知された場合

攻撃があった場合には（ステップＧ７－２のＹ）、その旨を伝えるアラームを生成して、ファイアウォール装置５１へ送信する。制御インタフェース１０６を介して、当該アラームを受信したファイアウォール装置３３は、第２実施形態におけるファイアウォール装置5と同様に、防御ルール判定部１０７から、信頼度管理部５１０２に前記ホストから攻撃のあったことを伝達すると共に、アクセス制御リスト管理部１０２にアクセス制御ルールの更新を指示して、前記接続を遮断する（ステップＧ８－３）。

【０２７６】

１３．２．４．３）攻撃が検知されなかった場合

一方、所定のタイムアウト時間内に攻撃が検知されなかった場合には（ステップＧ７－２のＮ）、信頼度管理部５１０２は接続管理部５２０１へアラームを伝達する。接続管理部５２０１は、当該アラームを受けて、第１入力バッファ５２０２へ格納済み要求データの転送を指示する（ステップＧ８－２）。

【０２７７】

なお、前記タイムアウト時間は、５００ミリ秒程度の時間を設定すれば通常十分であるが、入力ＩＰパケットがファイアウォール装置５１に到達する時間間隔の平均値などをもって、適応的に変化させるようにしてもよい。

【０２７８】

その後、第1の内部通信インターフェース１０４を介して、内部ネットワーク４上のサーバから応答データを受信したとき、第1出力バッファ５２０３は当該応答データを一時格納し、接続管理部５２０１に応答のあった旨を伝える（ステップＧ７－１）。

【０２７９】

接続管理部５２０１は、第1出力バッファ５２０３からデータ受信を伝達された後、直ちに前記ホストに向けて、第１出力バッファ５２０３に格納された応答データを転送する

（ステップＧ８－１）。

【０２８０】

１３．３）効果

第１３実施形態におけるファイアウォール装置５１によれば、１回の接続について、複数の要求データr(1)、 r(2)、...、 r(n) があって、その途中のある要求データr(i) が不審とされるような場合、おとり装置２で当該要求データr(i) に対するサーバ動作から攻撃が検知されなかったとき、r(i) は内部ネットワーク４上の正規サーバへ必ず転送されるので、r(1)～r(n) の全要求データが正しい順序で正規サーバに到達することを保証できる。

【０２８１】

一方、おとり装置２で攻撃が検知されたとき、直ちに前記接続が遮断されるので、前記要求データr(i) を含め、それ以降の要求データは一切、前記正規サーバに到達しないことを保証できる。

【０２８２】

こうした性質は、データベースと連携するＷＷＷサーバ（いわゆる「３層システム」）や、Ｔｅｌｎｅｔサーバや、ＦＴＰサーバなどと、それぞれのクライアントとの間で行われるように、１回の接続につき、複数の要求と応答が繰り返されるようなプロトコル（＝ステートフルプロトコル）に従うサービスの保護に適する。

【０２８３】

こうしたサービスにおいては、要求データ系列の順序が異なると、正しいサービス提供が保証できない。また、前記のように、攻撃用データを要求データ系列の一部として含むような場合にも、それまでの要求データ系列の順序が異なると、当該攻撃用データによるサーバの異常動作が観測できない場合がある。

【０２８４】

したがって、本実施形態におけるファイアウォール装置５０とおとり装置２との組み合わせによる攻撃防御システムは、ステートフルプロトコルに従うサービスについて、その正常動作および異常動作を誤りなく判定し、攻撃を確実に防御することができる。

【０２８５】

また、ＷＷＷサーバによる静的コンテンツ提供のような、ステートレスプロトコルを対象とする場合でも、本実施例による誘導方法によれば、インタネット３上のホストに転送される応答データは常に正規サーバの出力する応答データである。したがって、静的コンテンツの改ざんなどがおとり装置２で発生していた場合でも、改ざんされたコンテンツが前記ホストに到達することが一切なく、常に正しいコンテンツの提供が保証できる。

【０２８６】

１３．４）具体例

１３．４．１）構成

図５４を参照すると、本実施例は、インターネット３上のＦＴＰクライアント３０２と、内部ネットワーク４上のＦＴＰサーバ４０２と、ファイアウォール装置５１と、おとり装置２とから構成される。

【０２８７】

ＦＴＰクライアント３０２は、ＦＴＰサーバ４０２に向けていくつかの要求データを送信するが、それらは全て、ファイアウォール装置５１で中継される。また、ファイアウォール装置５１は、ＦＴＰクライアント３０２から入力される要求データをおとり装置２へも転送する。さらに、おとり装置２のプロセッサ２０１上では、ＦＴＰサーバ４０２と同じＦＴＰサービスが提供されている。

【０２８８】

１３．４．２）動作

ＦＴＰクライアント３０２は、ＦＴＰサーバ４０２に向けて、要求データを順次送信するが、本実施例では、ＦＴＰクライアント３０２が、

１）匿名ログイン

２）ファイルアップロード
を行う場合の、ファイルウォール装置５１の動作例を示す。
【０２８９】
また、ＦＴＰサーバ４０２とおとり装置２とは、非常に長いファイル名を処理したときにバッファオーバーフローを起こして、シェルが不正に操作される、という共通の脆弱性をもつものとする。
【０２９０】
さらに、おとり装置２の攻撃検知部２０２には、プロセッサ２０１で動作するＦＴＰサーバがシェルを起動することを禁止するような正常動作定義がなされているものとする。
【０２９１】
１３．４．２．１）仮接続
まず、ＦＴＰクライアント３０２は、ＦＴＰサーバ４０２へのログインに先立って、所定のＴＣＰ接続を確立するため、ＦＴＰサーバ４０２に向けてＳＹＮパケットを送信する。
【０２９２】
当該ＳＹＮパケットが、ファイアウォール装置５１に到達したとき、ファイアウォール装置５１の仮想サーバ５１０１は、ＦＴＰサーバ４０２に代わって、前記ＳＹＮパケットに対応するＳＹＮ－ＡＣＫパケットを応答する。
【０２９３】
その後、ＦＴＰクライアント３０２は、さらにＡＣＫパケットをＦＴＰサーバ４０２へ向けて送信する。当該ＡＣＫパケットがファイアウォール装置５１に到達したとき、仮想サーバ５１０１は、新たなＴＣＰ接続が確立したものと判定する。
【０２９４】
そして、仮想サーバ５１０１の接続管理部５２０１は、ＦＴＰサーバ４０２と、おとり装置２とに対して、ＦＴＰクライアント３０２に代わって、個別にＴＣＰ接続を確立する。
【０２９５】
１３．４．２．２）匿名ログイン
次に、ＦＴＰクライアント３０２は、ＦＴＰサーバ４０２へ向けて、匿名ログインを行うための要求データを送信する。
【０２９６】
一般に、ＦＴＰサーバに対する匿名ログインは、以下のような２個の要求データを送信する。
・第１の要求データ（r1）：ユーザ名を示すものであり、一般に「anonymous」である。
・第２の要求データ（r2）：パスワードを示すものであり、一般に「user@domain」の形式をもつメールアドレスである。
【０２９７】
第１の要求データr1が、ファイアウォール装置５１に到達したとき、仮想サーバ５１０１の接続管理部５２０１は、まず、第１の要求データr1を第１入力バッファ５２０２と、第２入力バッファ５２０４とに伝達し、一時格納する。
【０２９８】
その後、第１の要求データr1を信頼度管理部５１０２に入力し、その信頼度を取得する。このとき、信頼度管理部５１０２は、例えば、図５３のような信頼度管理テーブルに対して、第１の要求データr1をキーとして信頼度を検索する。このとき、第１の要求データr1のエントリがあれば、その信頼度c1を、接続管理部５２０１に出力する。もし、第１の要求データr1のエントリが無ければ、信頼度の初期値「０」をもつ、新たなエントリを追加し（図５５の網掛け部）、信頼度０を接続管理部５２０１に出力する。本実施例では、すでに第１の要求データr1のエントリが存在し、その信頼度が「１」であるものとする。
【０２９９】
そして、接続管理部５２０１は、所定の閾値と前記信頼度を比較する。本実施例では、

閾値を１とする。したがって、接続管理部５２０１は、第１の要求データr1を信頼し、第１入力バッファ５２０２と、第２入力バッファ５２０４とに、第１の要求データr1の転送を指示する。

【０３００】

転送を指示された第１入力バッファ５２０２および第２入力バッファ５２０４は、それぞれ、ＦＴＰサーバ４０２およびおとり装置２へ、第１の要求データr1を転送する。

【０３０１】

その後、第１の要求データr1を受信したＦＴＰサーバ４０２は、パスワードの入力を求める応答データs1をＦＴＰクライアント３０２へ向けて送信する。応答データs1がファイアウォール装置５１に到達したとき、応答データs1は一旦第１出力バッファ５２０３に格納される。そして、第１出力バッファ５２０３は、新たな応答データを受信した旨を、接続管理部５２０１に伝達する。

【０３０２】

そして、接続管理部５２０１は、第１出力バッファ５２０３に格納された応答データs1を、ＦＴＰクライアント３０２に向けて転送する。なお、おとり装置２からも応答データs1が送信され、第２出力バッファ５２０５がs1を格納し、接続管理部５２０１に応答データ受信を伝達するが、本実施例における接続管理部５２０１は、これを無視する。

【０３０３】

以上のようにして、ＦＴＰクライアント３０２からＦＴＰサーバ４０２へ向けて送信された要求データr1は、適切にＦＴＰサーバ４０２およびおとり装置２へ転送される。

【０３０４】

次に、パスワード入力である要求データr2についても、信頼度管理部５１０２は、その信頼度を「１」と出力するものとする。したがって、r2はr1と同様にして、ＦＴＰサーバ４０２およびおとり装置２へ転送される。こうして、ＦＴＰクライアント３０２は、ＦＴＰサーバ４０２およびおとり装置２の双方に対して、匿名ログインを完了することができる。

【０３０５】

１３．４．２．３）ファイルアップロード

匿名ログインを完了したＦＴＰクライアント３０２は、ファイルアップロードを行う。ＦＴＰサービスにおけるファイルアップロードは、以下の形式のコマンドを要求データに含めることで行われる。

【０３０６】

「ＰＵＴ　＜ファイル名＞」。

【０３０７】

ここで、以下の２種類の要求データを考える。

（Ａ）ｒ３－１：「ＰＵＴ　ＦＩＬＥ．ＴＸＴ」

（Ｂ）ｒ３－２：「ＰＵＴ　ＸＸＸＸＸＸＸＸ・・・＜シェルコード＞」。

【０３０８】

ｒ３－１は、「ＦＩＬＥ．ＴＸＴ」という名前のファイルをＦＴＰサーバ４０２にアップロードしようとするものであり、正常な要求データであるとする。一方ｒ３－２は、ＦＴＰサーバ４０２にバッファオーバーフローを引き起こさせて、ファイル名の一部として含められたシェルコードを不正にＦＴＰサーバ４０２内のシェルに実行させようとするものであるとする。

【０３０９】

１３．４．２．３．１）正常な要求データｒ３－１が入力された場合

まず、ＦＴＰクライアント３０２から要求データｒ３－１が送信された場合を示す。

【０３１０】

要求データｒ３－１がファイアウォール装置５１に到達した際、前記要求データｒ１と同様にして、接続管理部５２０１によって、第１入力バッファ５２０２および第２入力バッファ５２０４とに格納され、要求データｒ３－１が信頼度管理部５１０２に入力される

。
【０３１１】
信頼度管理部５１０２は、前記信頼度管理テーブルを参照するが、このとき、要求データｒ３－１のエントリがないものとする。この場合、信頼度管理部５１０２は、信頼度管理テーブルに、要求データｒ３－１のエントリを新たに追加する。また、要求データｒ３－１の信頼度として、所定の初期値「０」を設定し、「０」を接続管理部５２０１に出力する。
【０３１２】
接続管理部５２０１は、要求データｒ３－１の信頼度「０」を取得したのち、閾値「１」との比較を行って、閾値より小さな信頼度であることを確認し、要求データｒ３－１を不審とみなす。そして、第２入力バッファ５２０４のみに、要求データｒ３－１の転送を指示する。
【０３１３】
第２入力バッファ５２０４は、前記転送指示を受けて、おとり装置２に要求データｒ３－１を転送する。
【０３１４】
おとり装置２は、要求データｒ３－１を受信して、ファイル「ＦＩＬＥ．ＴＸＴ」を保存した後、保存が完了した旨を伝える応答データｓ３－１を送信する。
【０３１５】
その後、応答データｓ３－１は、ファイアウォール装置５１に到達し、第２出力バッファ５２０５に格納され、第２出力バッファ５２０５は、その旨を接続管理部５２０１に通知する。そして、接続管理部５２０１は、信頼度管理部５１０２に要求データｒ３－１が正常であることを通知し、信頼度管理部５１０２は、前記信頼度管理テーブルを更新して、要求データｒ３－１の信頼度を「１」にする。
【０３１６】
さらに、接続管理部５２０１は、第１入力バッファ５２０２に要求データｒ３－１の転送を指示して、第１入力バッファ５２０２に要求データｒ３－１をＦＴＰサーバ４０２に転送させる。
【０３１７】
その後、ＦＴＰサーバ４０２は、ファイル「ＦＩＬＥ．ＴＸＴ」を保存し、その完了を伝える応答データｓ３－１を送信する。
【０３１８】
ＦＴＰサーバ４０２からの応答データｓ３－１は、第１出力バッファ５２０３に格納され、第１出力バッファ５２０３は、その旨を接続管理部５２０１に通知する。そして、接続管理部５２０１は、ｓ３－１をＦＴＰクライアント３０２に転送する（図５６参照）。
【０３１９】
以上のようにして、ＦＴＰクライアント３０２から送信されたファイル「ＦＩＬＥ．ＴＸＴ」は、ＦＴＰサーバ４０２およびおとり装置２に適切に保存される。
【０３２０】
１３．４．２．３．２）要求データｒ３－２が入力された場合
次に、ＦＴＰクライアント３０２から不正な要求データｒ３－２が送信された場合を示す。
【０３２１】
要求データｒ３－２がファイアウォール装置５１に到達した際、前記要求データｒ３－１と同様にして、接続管理部５２０１によって、第１入力バッファ５２０２および第２入力バッファ５２０４とに格納され、要求データｒ３－２が信頼度管理部５１０２に入力される。
【０３２２】
信頼度管理部５１０２は、前記信頼度管理テーブルを参照するが、このとき、やはり、要求データｒ３－２のエントリがないものとする。この場合、信頼度管理部５００２は、

信頼度管理テーブルに、要求データｒ３－１のエントリを新たに追加する。また、要求データｒ３－２の信頼度として、所定の初期値「０」を設定し、「０」を接続管理部５２０１に出力する。

【０３２３】

接続管理部５２０１は、要求データｒ３－２の信頼度「０」を取得したのち、閾値「１」との比較を行って、閾値より小さな信頼度であることを確認し、要求データｒ３－２を不審とみなす。

【０３２４】

そして、第２入力バッファ５２０４のみに、要求データｒ３－２の転送を指示する。第２入力バッファ５２０４は、前記転送指示を受けて、おとり装置２に要求データｒ３－２を転送する。

【０３２５】

おとり装置２が要求データｒ３－２を受信すると、プロセッサ２０１上で、（偽の）ＦＴＰサーバはバッファーオーバーフローによってシェルを起動し、要求データｒ３－２に含まれる不正なシェルコードを実行しようとする。おとり装置２の攻撃検知部２０２は、当該シェル起動を攻撃と検知し、直ちにアラームをファイアウォール装置５１に送信する。

【０３２６】

前記アラームを受信したファイアウォール装置５１は、まず、防御ルール判定部１０７と、アクセス制御リスト管理部１０２と、パケットフィルタ１０１とによって、第１実施形態におけるファイアウォール装置１と同様に、ＦＴＰクライアント３０２からの以降のアクセスを遮断する。また、防御ルール判定部１０７は、アラームの受信を接続管理部５２０１にも通知する。

【０３２７】

アラーム受信通知を受けた接続管理部５２０１は、ただちにＦＴＰクライアント３０２との接続を遮断する。また、望ましくは、第１入力バッファ５２０２に格納されたｒ３－２を消去する。

【０３２８】

以上のようにして、不正な要求データｒ３－２は、到達するとしてもおとり装置２に限られ、ＦＴＰサーバ４０２に到達しない（図５７参照）。

【０３２９】

（第１４実施形態）

図５８に示すように、内部ネットワーク４上のサーバ（例えばＦＴＰサーバ４０２）からおとり装置２へ少なくともファイルシステムの内容を複写するミラーリング装置５９０１をさらに備えてもよい。

【０３３０】

おとり装置２で攻撃が検知されファイアウォール装置５１の防御ルール判定部１０７にアラームが伝達された際、防御ルール判定部１０７は、さらにミラーリング装置５９０１にもアラーム受信を通知する。

【０３３１】

当該通知を受けたミラーリング装置５９０１は、前記内部ネットワーク４上のサーバのファイルシステム４０２１を読み取り、その内容をおとり装置２上のファイルシステム２０１１へ複写する。こうすることにより、おとり装置２上で不正なファイル書込みが発生しても、その被害をリアルタイムに復旧することができる。

【０３３２】

本実施形態ではファイルシステムを具体例として挙げたが、その他に、さらにメモリモジュールの内容を複写するようにしてメモリ内の異常を復旧するようにしてもよい。また、おとり装置２から送信されるアラームに、書換えられたファイルのパス名、あるいは、メモリ領域を記載するようにして、被害を受けた部分のみを複写できるようにしてもよい。

【０３３３】
（第１５実施形態）
図５９は、本発明の第１５実施形態におけるファイアウォール装置の概略的構成図である。本実施形態におけるファイアウォール装置６２は、第１３実施形態におけるファイアウォール装置５１の仮想サーバ５１０１の前段に暗号処理部６２０１を備える。
【０３３４】
暗号処理部６２０１は、パケットフィルタ１０１から得られた暗号化入力ＩＰパケットを復号し、復号された入力ＩＰパケットを仮想サーバ５１０１に伝達する。また、仮想サーバ５１０１から得られた出力ＩＰパケットを暗号化し、暗号化出力ＩＰパケットをパケットフィルタ１０１に伝達する。
【０３３５】
このようにすることで、インタネット３および内部ネットワーク４との間で暗号化通信が行われる場合にも、おとり装置への誘導を行うことができる。
【０３３６】
（第１６実施形態）
上記第１～第１５実施形態では、誘導部（または仮想サーバ部）、防御ルール判定部、パケットフィルタ、および、アクセス制御リスト管理部が一つのユニットになったファイアウォール装置を例示したが、本発明はこれに限定されるものではない。
【０３３７】
たとえば、次のようにハードウェア的に２ユニットで構成し、それらをネットワークで接続することもできる。
【０３３８】
・少なくともパケットフィルタおよびアクセス制御リスト管理部を有するファイアウォール装置
・少なくとも誘導部（または仮想サーバ部）および防御ルール判定部を有するスイッチ装置。
【０３３９】
従来のファイアウォール装置は、遠隔からアクセス制御リストの部分的更新を行う機能を有していることが多いので、既に設置ずみのファイアウォール装置に加えて、上記スイッチ装置を設置することで、第１～第１４実施形態における１ユニットのファイアウォール装置と同等の機能を実現できるというメリットがある。
【０３４０】
図６０は本発明の第１６実施形態による攻撃防御システムの概略的構成図である。本実施形態において、ファイアウォール装置７００１にはパケットフィルタ１０１およびアクセス制御リスト管理部１０２が設けられ、スイッチ装置７００２には誘導部５０１、信頼度管理部５０２および防御ルール判定部１０７が設けられている。パケットフィルタ１０１と誘導部５０１との間、および、アクセス制御リスト管理部１０２と防御ルール判定部１０７との間をネットワークを介して接続することで、第１～第１５実施形態による攻撃防御システムを実現することができる。
【０３４１】
（第１７実施形態）
１７．１）構成
図６１は、本発明の第１７実施形態による攻撃防御システムの概略的構成図である。本実施形態における攻撃防御システムは、ファイアウォール装置８０と、サーバ装置４０１と、複数のおとり装置２（１）～２（ｋ）から構成されるおとりクラスタ２１と、から構成される。
【０３４２】
ファイアウォール装置８０は、少なくとも誘導部８００１、サーバ管理部８００２、および、信頼度管理部５０２を有する。誘導部８００１は、すでに述べた手順により、新規に受信したアクセスに関する信頼度を信頼度管理部５０２からを受け取り、さらに、当該

信頼度をサーバ管理部８００２へ渡して適切なおとり装置２（ｉ）の識別子を受け取る。誘導部８００１は、受け取った識別子で指示されたおとり装置２（ｉ）もしくは内部ネットワークへ受信したアクセスを転送する。

【０３４３】

サーバ管理部８００２は、おとりクラスタ２１に含まれるおとり装置２（１）～２（ｋ）の識別子と必須信頼度との対応関係を示す参照表８００３を内部的に備えており、誘導部８００１からの信頼度の入力を受けて、参照表から適切な識別子を選択し、選択された識別子を誘導部８００１へ返す。

【０３４４】

図６２は、サーバ管理部８００２が有する参照表８００３の一例を示す模式図である。ここでは、おとり装置２（１）～２（ｋ）にそれぞれ対応するサーバ識別子Ｄ１～Ｄｋと必須信頼度Ｍ１～Ｍｋとの対応が格納されている。

１７．２）動作

図６３は、本発明の第１７実施形態による攻撃防御システムの動作を示すフローチャートである。ファイアウォール装置８０がサーバ装置４０１へ向かうパケットｐを受信すると、誘導部８００１は、まず入力パケットｐの少なくともヘッダを信頼度管理部５０２へ出力し、パケットｐに対する信頼度τ[p]を受け取る（ステップＩ１）。

【０３４５】

続いて、誘導部８００１は、信頼度τ[p]をサーバ管理部８００２へ出力し、少なくとも１つの識別子を受け取る。このとき、サーバ管理部８００２は、参照表８００３の必須信頼度の列を走査し、受け取った信頼度τ[p]以下の必須信頼度に対応する識別子を検索する（ステップＩ２およびＩ３）。

【０３４６】

対応する識別子を発見できなかった場合は（ステップＩ３のＮ）、少なくともサーバ装置４０１に割り当てられた所定の識別子および必須信頼度Ｎの組を仮の検索結果としてする（ステップＩ４）。この場合、さらに、おとりクラスタ２１上の全てのおとり装置の識別子Ｄ１～Ｄｋの系列を検索結果に加えてもよい。なお、サーバ装置４０１の必須信頼度Ｎは、参照表８００３の必須信頼度Ｍ１～Ｍｋの最大値を越える値であるものとする（Ｎ＞max[M1, M2, …, Mk]）。

【０３４７】

対応する識別子が１以上抽出された場合は（ステップＩ３のＹ）、抽出された識別子を誘導部８００１へ返す（ステップｉ５）。このとき、複数の識別子が抽出された場合は、必須信頼度が最大である識別子を１つだけ誘導部８００１へ戻してもよいし、全ての識別子を戻してもよい。誘導部８００１は、サーバ管理部８００２から入力した識別子に対応するおとり装置２またはサーバ装置４０１へパケットｐを転送する（ステップＩ６）。

【０３４８】

サーバ装置４０１がパケットｐを受信すると、サーバ装置４０１上のサーバプログラムによりパケットｐの処理が行われる。一方、おとり装置２がパケットｐを受信すると、すでに述べたように、プロセッサ上でサーバプログラムを動作させ、攻撃検知部でそのふるまいを監視する（ステップＩ７）。

【０３４９】

そして、転送先のおとり装置２もしくはサーバ装置４０１上のサーバプログラムが出力したレスポンスは、誘導部８００１を経て、パケットｐの送信元ホストへと返送される（ステップＩ８）。なお、転送先であるおとり装置２が複数である場合、レスポンスも複数得られるが、誘導部８００１は必須信頼度が最大であるおとり装置２から得られたレスポンスのみをアクセス元へ転送する。ただし、転送先にサーバ装置４０１が含まれる場合には、必ずサーバ装置４０１からのレスポンスを採用して転送する。

【０３５０】

１７．３）効果

上述したように、おとりサーバに必須信頼度を割り当てておき、この必須信頼度に応じ

て、様々な重要度をもつコンテンツの配置・非配置を決定することができる。これにより、おとりサーバ上で被害が発生した場合でも、予め想定したレベル以下に抑制することができる。

【０３５１】

（第１８実施形態）

これまで述べてきた実施形態における信頼度管理部は、おとり装置２からのアラートに基づいて信頼度を調整するものであったが、本発明はこれに限定されるものではなく、外部の一般的な攻撃検知システムから攻撃検知通知に基づいて信頼度調整を行うこともできる。これにより、他のサイトで発生した攻撃事例を基に予防的な防御を行うことが可能となる。

【０３５２】

１８．１）構成

図６４は、本発明の第１８実施形態による攻撃防御システムの概略的構成図である。本実施形態における攻撃防御システムは、ファイアウォール装置８１と、内部ネットワーク８１０３および外部ネットワーク８１０４上にある１つ以上の攻撃検知システムAD_1～AD_Nと、を備える。

【０３５３】

ファイアウォール装置８１は、少なくとも信頼度管理部８１０１とアラート変換部８１０２とを有する。信頼度管理部８１０１は、アラート変換部８１０２によって変換されたアラートを入力すると、すでに述べた手順により、後続する入力パケットの信頼度を減算する。なお、攻撃検知システムAD_1～AD_Nは、それぞれのシステムに依存した構文のアラートを送信するから、攻撃検知システムごとにアラームを解釈するための解釈モジュールがアラート変換部８１０２に設けられている。

【０３５４】

アラート変換部８１０２は、外部ネットワーク８１０４または内部ネットワーク８１０３上にある各種攻撃検知システムからシステム依存アラートを受信し、それらのアラート構文を解釈して変換し、信頼度管理部８１０１へ出力する。

【０３５５】

攻撃検知システムAD_1～AD_Nは、ネットワークトラフィックまたはサーバプログラムの動作あるいはログファイルなどを監視し、攻撃を検知した際には、少なくとも攻撃元ＩＰアドレスおよび攻撃対象ＩＰアドレスを含むアラートをファイアウォール装置８１のアラート変換部８１０２へ送信する。

【０３５６】

１８．２）動作

図６５は、本発明の第１８実施形態による攻撃防御システムの動作を示すフローチャートである。まず、アラート変換部８１０２は、外部ネットワークまたは内部ネットワーク上にある各種攻撃検知システムからアラートを受信すると、当該アラートの構文を解釈する（ステップＪ１）。上述したように受信アラートは送信元の攻撃検知システムに依存した構文をもっているため、アラート変換部８１０２内に備えられた攻撃検知システムごとの解釈モジュールを適切に選択し、選択された解釈モジュールにより受信アラートの構文を解釈する。解釈モジュールの選択にあたっては、たとえば、アラートの送信元ＩＰアドレスを基に攻撃検知システムの種類を特定すればよい。そして、解釈結果から、少なくとも攻撃パケットの送信元ＩＰアドレスと宛先ＩＰアドレスとを抽出する（ステップＪ２）。

【０３５７】

続いて、アラート変換部８１０２は、解釈結果から、受信アラートの深刻度を算出する（ステップＪ３）。深刻度の算出方法の具体例としては、例えばアノーマリ型攻撃検知システムによるアラートであれば異常さを示す数値が記載されているので、それを深刻度として採用する。また、シグネチャ型攻撃検知システムによるアラートであれば、攻撃方法を示す識別子から予め対応づけられた深刻度を求めるようにしてもよい。

【０３５８】
そして、少なくとも送信元ＩＰアドレス、宛先ＩＰアドレス、および、深刻度という３つの値を１組として生成し、変換ずみアラートとして信頼度管理部８１０１へ出力する（ステップＪ４）。
【０３５９】
変換済みアラートを入力した信頼度管理部８１０１は、送信元ＩＰアドレスまたは宛先ＩＰアドレス、あるいは（もし取得可能であれば）攻撃データに対する信頼度から深刻度を減算することで、信頼度の更新を行う（ステップＪ５）。
【０３６０】
（第１９実施形態）
第１～第１８実施形態におけるファイアウォール装置では、信頼度管理部を内部に有していたが、本発明はこれに限定されるものではなく、信頼度管理部を別ユニットで構成することもできる。これにより、ファイアウォール装置が多数存在する場合にも、少数の信頼度管理用ユニットでファイアウォール装置の動作を制御できるようになり、運用コストが低減するというメリットがある。
【０３６１】
１９．１）構成
図６６は、本発明の第１９実施形態による攻撃防御システムの概略的ブロック図である。本実施形態による攻撃防御システムは、ファイアウォール装置８５と、信頼度管理サーバ装置８６と、少なくとも１つのおとり装置２もしくは攻撃検知システムを備えている。ファイアウォール装置８５は、少なくとも誘導部８５０１および管理サーバ接続部８５０２を有する。誘導部８５０１は、外部ネットワークから受信した入力ＩＰパケットを管理サーバ接続部８５０２へ渡して信頼度を取得し、入力ＩＰパケットを内部ネットワーク上のサーバ装置４０１またはおとり装置２へ転送する。
【０３６２】
管理サーバ接続部８５０２は、少なくとも１つの信頼度管理サーバ装置８６に接続されており、誘導部８５０１から入力した入力ＩＰパケットの全てまたは一部を含む信頼度要求メッセージを信頼度管理サーバ装置８６へ送信する。信頼度管理サーバ装置８６から信頼度を含む応答メッセージを受信すると、管理サーバ接続部８５０２は当該信頼度を誘導部８５０１へ返す。
【０３６３】
信頼度管理サーバ８６は、ファイアウォール装置８５から信頼度要求メッセージを受信すると、所定の方法により算出された信頼度を含む応答メッセージを当該ファイアウォール装置８５へ返信する。
【０３６４】
１９．２）動作
図６７は、本発明の第１９実施形態による攻撃防御システムの動作を示すフローチャートである。ファイアウォール装置８５は、まず、新たに外部ネットワークから受信した入力ＩＰパケットを誘導部８５０１へ転送する（ステップＫ１）。
【０３６５】
誘導部８５０１から入力ＩＰパケットを受け取ると、管理サーバ接続部８５０２は、当該入力ＩＰパケットから信頼度要求メッセージを生成し、所定の信頼度管理サーバ装置８６へ送信する（ステップＫ２）。なお、所定の信頼度管理サーバ装置８６は、１台とは限らず、複数であってもよい。また、信頼度要求メッセージは入力ＩＰパケットの全てを含むものでもよいし、ヘッダやペイロードなどの一部を含むものであってもよい。信頼度要求メッセージに含めるべき情報は、信頼度管理サーバ装置８６における信頼度の算出方法に依存するので、複数の信頼度管理サーバ装置がある場合には、各信頼度管理サーバ装置に応じて、信頼度要求メッセージのフォーマットを定めるようにしてもよい。
【０３６６】
次に、信頼度要求メッセージを受信すると、信頼度管理サーバ装置８６は、当該信頼度

要求メッセージに含まれる入力ＩＰパケットの全てまたは一部を抽出し（ステップＫ３）、当該入力ＩＰパケットに対する信頼度τ[p]を算出する（ステップＫ４）。なお、信頼度算出方法は、すでに説明した信頼度管理部の動作など信頼度としての数値を算出するものであれば任意の方法を用いてよい。あるいは、そうした信頼度管理手段を、信頼度管理モジュールとしてモジュール化しておき、動的に変更可能なようにしてもよい。こうすることにより、いわゆる「プラグイン機能」や「アップデート機能」を提供することができ、信頼度管理サーバ装置の保守性を向上させることができる。

【０３６７】

続いて、信頼度管理サーバ装置８６は、信頼度τ[p]を含む応答メッセージを管理サーバ接続部８５０２へ送信する（ステップＫ５）。なお、応答メッセージは、少なくとも信頼度を数値として含むものであれば、ほかにどのような情報が付加されていてもよい。そして、応答メッセージを受信した管理サーバ接続部８５０２は、当該応答メッセージから信頼度を抽出した後、当該信頼度を誘導部８５０１へ出力する（ステップＫＪ６）。

【０３６８】

なお、複数の信頼度管理サーバ装置８６から応答メッセージを受信した場合には、管理サーバ接続部８５０２で所定の関数Ｈにより、１つの信頼度にまとめあげた上で、誘導部８５０１へ出力する。関数Ｈの具体例としては、複数の信頼度のうち最小のものを返す関数あるいは平均値を返す関数などを用いることができる。

【０３６９】

信頼度を受け取った誘導部８５０１は、当該信頼度と所定の振り分け条件とを照合した結果に基づいて、入力ＩＰパケットをサーバ装置４０１およびおとり装置２のいずれかへと転送する（ステップK７）。

【図面の簡単な説明】

【０３７０】

【図１】本発明による攻撃防御システムの概略的ブロック図である。

【図２】本発明の第１実施形態による攻撃防御システムのファイアウォール装置１およびおとり装置２の構成を示すブロック図である。

【図３】図２のファイアウォール装置１におけるアクセス制御リスト管理部１０２の模式的構成図である。

【図４】アクセス制御リストデータベース１０２１の内容を例示した模式図である。

【図５】誘導部１０３に設けられた誘導リストの一例を示す模式図である。

【図６】防御ルール判定部１０７に保持されているアクセス制御ルールのひな型を例示した模式図である。

【図７】本発明の第１実施形態による攻撃防御システムの動作を示すフローチャートである。

【図８】本発明の第１実施形態のファイアウォール装置でアドレス変換処理を行う際の好適な一例を示すブロック図である。

【図９】第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１０】第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１１】第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１２】おとり装置２における攻撃検知動作を説明するための模式図である。

【図１３】第１実施形態におけるアクセス制御リストの更新動作例を説明するための模式図である。

【図１４】第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１５】本発明の第２実施形態による攻撃防御システムのブロック図である。

【図１６】本発明の第２実施形態による攻撃防御システムの動作を示すフローチャートである。

【図１７】本実施形態における信頼度とパケット転送先の関係を示すグラフである。

【図１８】（Ａ）は、外れ値度計算を用いた信頼度管理部５０２の概略的構成図であり、（Ｂ）は、その一例を示す詳細なブロック図である。

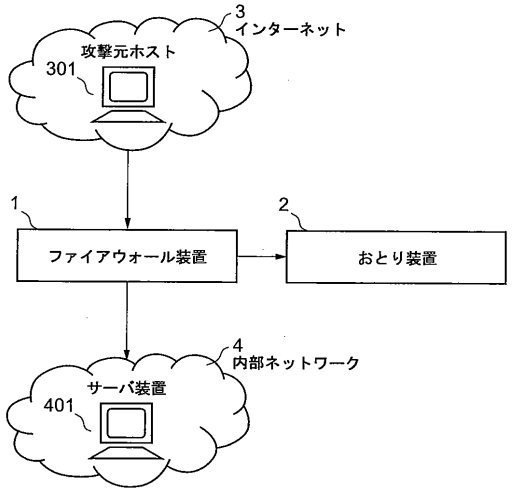
【図１９】本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。
【図２０】本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。
【図２１】本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。
【図２２】本発明の第３実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図である。
【図２３】第３実施形態による攻撃防御システムのファイアウォール装置の一例を示す詳細なブロック図である。
【図２４】本発明における第４実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。
【図２５】信頼度管理部７０１における信頼度参照処理を示すフローチャートである。
【図２６】本発明の第６実施形態による攻撃防御システムのファイアウォール装置９を示す概略的ブロック図である。
【図２７】本実施形態によるファイアウォール装置９の動作を示すフローチャートである。
【図２８】本発明の第７実施形態による攻撃防御システムのファイアウォール装置１０を示す概略的ブロック図である。
【図２９】アクセス制御リスト管理部１００２の管理動作を示すフローチャートである。
【図３０】本発明の第８実施形態による攻撃防御システムの概略的構成図である。
【図３１】本発明の第１０実施形態による攻撃防御システムの概略的構成図である。
【図３２】本発明の第１１実施形態による攻撃防御ユニットの概略的構成図である。
【図３３】本発明の第１２実施形態におけるおとり装置の構成を示すブロック図である。
【図３４】第１２実施形態におけるおとり装置の全体的動作を示すフローチャートである。
【図３５】第１２実施形態において使用されるプロセス種別判定テーブルの一例を示す図である。
【図３６】イベント管理部におけるイベント管理キューの一例を示す図である。
【図３７】第１２実施形態におけるイベント管理部が行うリンク付け処理の１例を示すフローチャートである。
【図３８】第１２実施形態におけるイベント管理部が出力するイベント－コンテキスト対の概念図である。
【図３９】ドメイン－タイプ制約つき正常動作定義（ＤＴ定義）ファイルの一例を示す図である。
【図４０】第１２実施形態における攻撃検知部が解釈するドメイン－タイプ制約の概念図である。
【図４１】第１２実施形態におけるおとり装置のイベント管理部が行うネットワークイベント追加の具体例を示す模式図である。
【図４２】第１２実施形態におけるおとり装置のイベント管理部が行うプロセスイベント走査の具体例を示す模式図である。
【図４３】第１２実施形態におけるおとり装置のイベント管理部が行うリンク付けの具体例を示す模式図である。
【図４４】第１２実施形態におけるおとり装置のイベント管理部が行う子プロセス生成イベントの追加およびリンク付けの具体例を示す模式図である。
【図４５】第１２実施形態におけるおとり装置のイベント管理部が行う子プロセスが発生させたファイルイベントの追加およびリンク付けの具体例を示す模式図である。
【図４６】第１２実施形態におけるおとり装置のイベント管理部が行う孫プロセス生成イベントの追加およびリンク付けの具体例を示す模式図である。
【図４７】第１２実施形態におけるおとり装置のイベント管理部が行う孫プロセスが発生

させたファイルイベントの追加およびリンク付けの具体例を示す模式図である。
【図４８】第１２実施形態のおとり装置における攻撃発生時のイベント管理キュー状態を示す具体例を示す模式図である。
【図４９】第１２実施形態のおとり装置における攻撃発生時のイベント管理キュー状態を示す別の具体例を示す模式図である。
【図５０】本発明の第１３実施形態におけるファイアウォール装置の構成を示すブロック図である。
【図５１】第１３実施形態におけるファイアウォール装置の仮想サーバ部の詳細なブロック図である。
【図５２】第１３実施形態におけるファイアウォール装置の動作を示すフローチャートである。
【図５３】第１３実施形態におけるファイアウォール装置の信頼度管理部に格納される信頼度管理テーブルの一例を示す図である。
【図５４】第１３実施形態におけるファイアウォール装置の動作を説明するための攻撃防御システムの概略的ブロック図である。
【図５５】第１３実施形態における信頼度管理部が行う信頼度管理テーブルへの新規エントリ追加の具体例を示す図である。
【図５６】第１３実施形態におけるファイアウォール装置が行う正常動作確認時の動作の具体例を示す図である。
【図５７】第１３実施形態におけるファイアウォール装置が行う、攻撃検知時の動作の具体例を示す図である。
【図５８】本発明の第１４実施形態による攻撃防御システムの概略的ブロック図である。
【図５９】本発明の第１５実施形態におけるファイアウォール装置の概略的ブロック図である。
【図６０】本発明の第１６実施形態による攻撃防御システムの概略的構成図である。
【図６１】本発明の第１７実施形態による攻撃防御システムの概略的構成図である。
【図６２】サーバ管理部８００２が有する参照表８００３の一例を示す模式図である。
【図６３】本発明の第１７実施形態による攻撃防御システムの動作を示すフローチャートである。
【図６４】本発明の第１８実施形態による攻撃防御システムの概略的構成図である。
【図６５】本発明の第１８実施形態による攻撃防御システムの動作を示すフローチャートである。
【図６６】本発明の第１９実施形態による攻撃防御システムの概略的ブロック図である。
【図６７】本発明の第１９実施形態による攻撃防御システムの動作を示すフローチャートである。
【符号の説明】
【０３７１】
１　ファイアウォール装置
１００　外部通信インタフェース
１０１　パケットフィルタ
１０２　第１のアクセス制御リスト管理部
１０２１　アクセス制御リストデータベース
１０２２　検索処理部
１０２３　更新処理部
１０３　誘導部
１０３１　アドレス変換部
１０４　第１の内部通信インタフェース
１０５　第２の内部通信インタフェース
１０６　制御インタフェース
１０７　防御ルール判定部

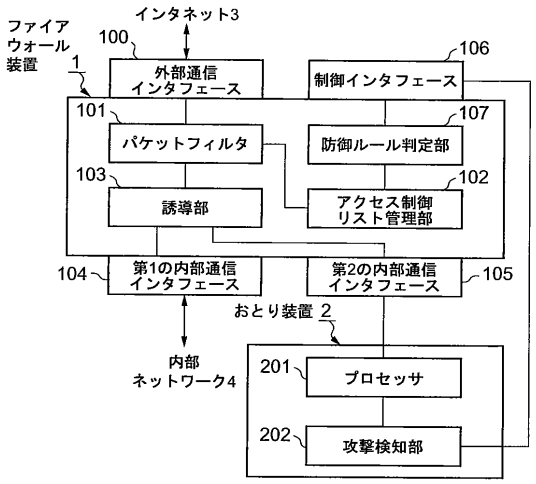
２　おとり装置
２１　おとりクラス
２０１　プロセッサ
２０１１　ファイルシステム
２０２　攻撃検知部
３　インターネット
３０１　攻撃元ホスト
３０２　通常のホスト
４　内部ネットワーク
４０１　サーバ装置
５　ファイアウォール装置
５０１　誘導部
５０２　信頼度管理部
５０２１　外れ値検知部
６　ファイアウォール装置
７　ファイアウォール装置
７０１　信頼度管理部
７０１１　リアルタイム信頼度データベース
７０１２　複製処理部
７０１３　長期信頼度データベース
７０１４　更新処理部
８　ファイアウォール装置
９　ファイアウォール装置
９０１　誘導部
９０１１　バッファ
９０１２　ＩＣＭＰ監視部
１０　ファイアウォール装置
１００１　防御ルール判定部
１００２　アクセス制御リスト管理部
２１　おとりクラスタ
３７　第２のおとり装置
３７０１　イベント管理部
３７０２　第２の攻撃検知部
４１０１　ドメイン－タイプ制約つき正常動作定義ファイル
３５０１　第１のイベント
３６０１　第２のイベント
３８０１　第３のイベント
３９０１　第４のイベント
４００１　第５のイベント
４１０１　第６のイベント
４９０１　第７のイベント
５００１　第８のイベント
５１　第８のファイアウォール装置
５１０１　仮想サーバ部
５１０２　第３の信頼度管理部
５２０１　接続管理部
５２０２　第１入力バッファ
５２０３　第１出力バッファ
５２０４　第２入力バッファ
５２０５　第２出力バッファ

６２　第９のファイアウォール装置
６２０１　暗号処理部
３０３　ＦＴＰクライアント
４０２　ＦＴＰサーバ
４０２１　ファイルシステム
６９０１　ミラーリング装置
７００１　ファイアウォール装置
７００２　スイッチ装置
８０　ファイアウォール装置
８００１　誘導部
８００２　サーバ管理部
８００３　参照表
８１　ファイアウォール装置
８１０１　信頼度管理部
８１０２　アラート変換部
８５０１　誘導部
８５０２　管理サーバ接続部
８６　信頼度管理サーバ装置

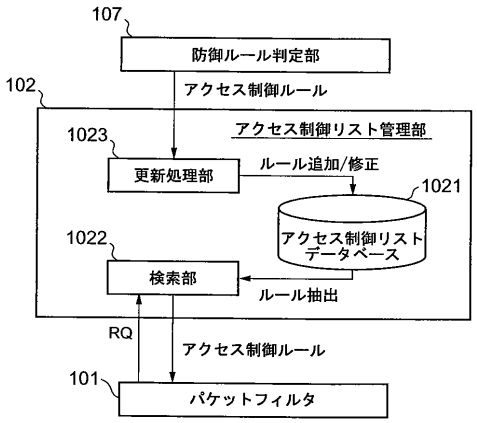
【図１】



【図２】



【図３】



【図４】

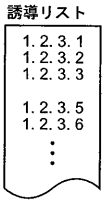
1021

アクセス制御リストデータベース

ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

*…任意のアドレスにマッチ
ACCEPT…パケットの受理
DENY…パケットの拒否(ICMPエラーを通知)
DROP…パケットの廃棄(ICMPエラーを通知しない)

【図５】



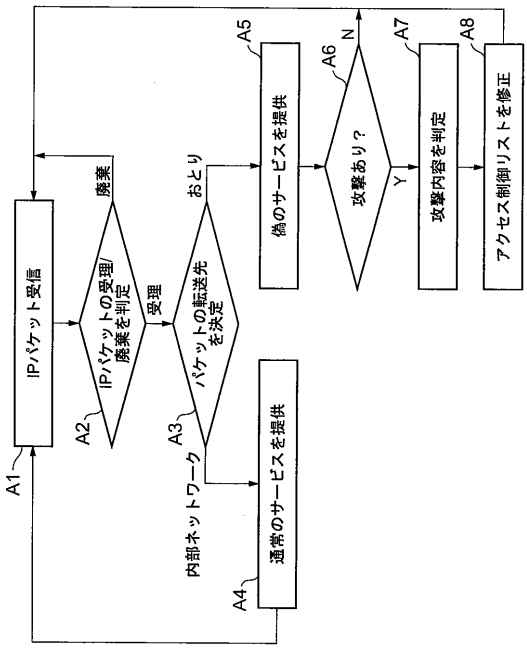
【図６】

107 防御ルール判定部

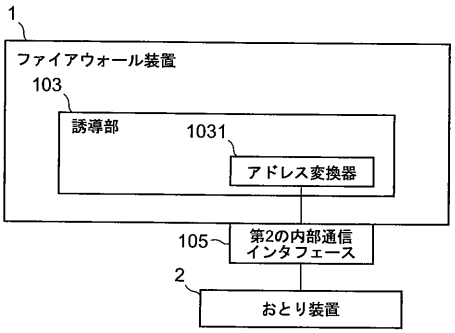
攻撃種別	ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
RECON	—	—	—
INTRUSION	${SRC_IP_ADDRESS}	*	DROP
DESTRUCTION	${SRC_IP_ADDRESS}	*	DROP

—…無指定(何もしない)
${}…置換用変数

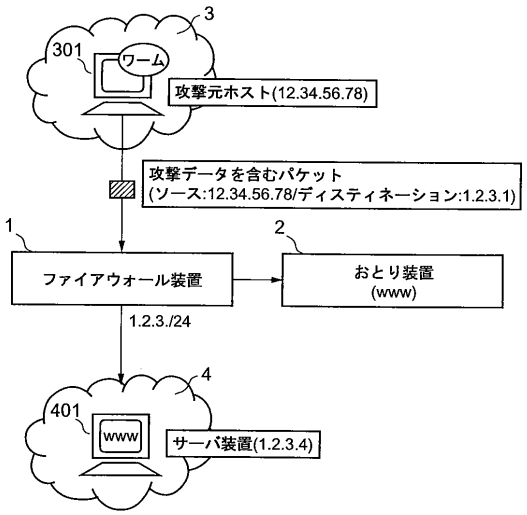
【図７】



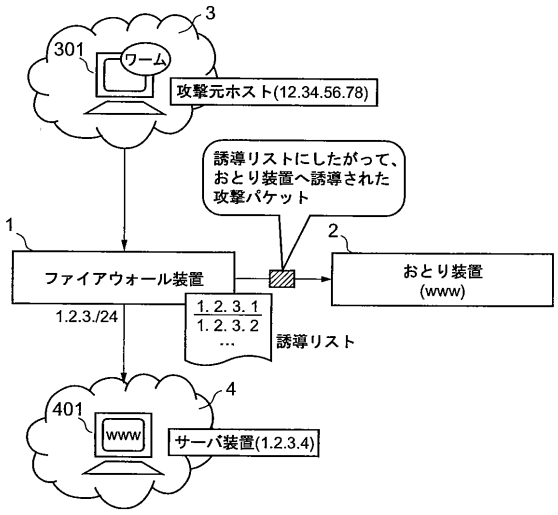
【図８】


1
ファイアウォール装置
103
誘導部
1031
アドレス変換器
105
第2の内部通信
インタフェース
2
おとり装置

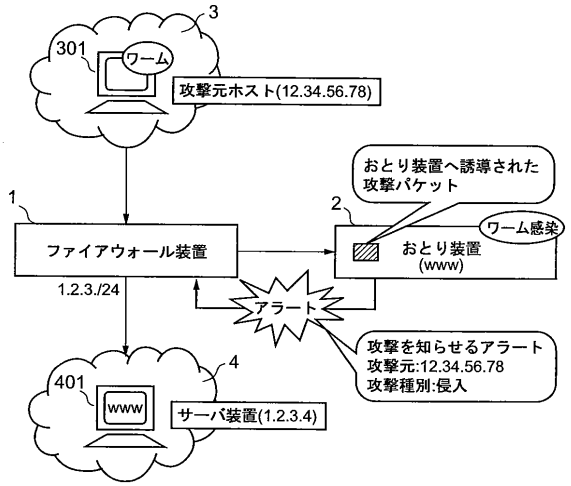
【図９】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
攻撃データを含むパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.1)
1
ファイアウォール装置
2
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

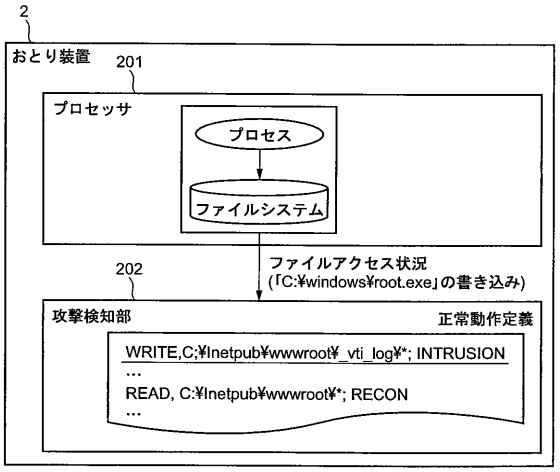
【図１０】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
誘導リストにしたがって、
おとり装置へ誘導された
攻撃パケット
1
ファイアウォール装置
2
おとり装置
(www)
1.2.3./24
1. 2. 3. 1
1. 2. 3. 2
…
誘導リスト
4
401
www
サーバ装置(1.2.3.4)

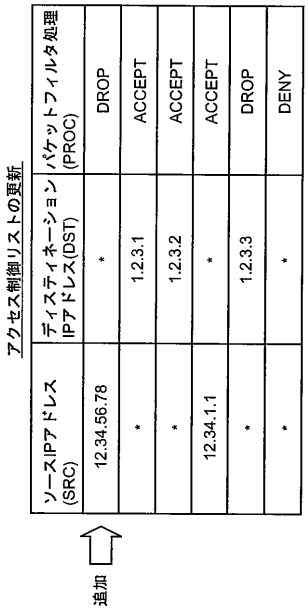
【図１１】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
おとり装置へ誘導された
攻撃パケット
1
ファイアウォール装置
2
ワーム感染
おとり装置
(www)
1.2.3./24
アラート
攻撃を知らせるアラート
攻撃元:12.34.56.78
攻撃種別:侵入
4
401
www
サーバ装置(1.2.3.4)

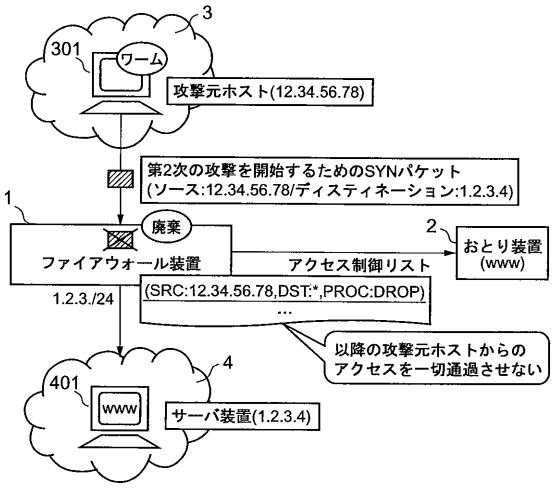
【図１２】



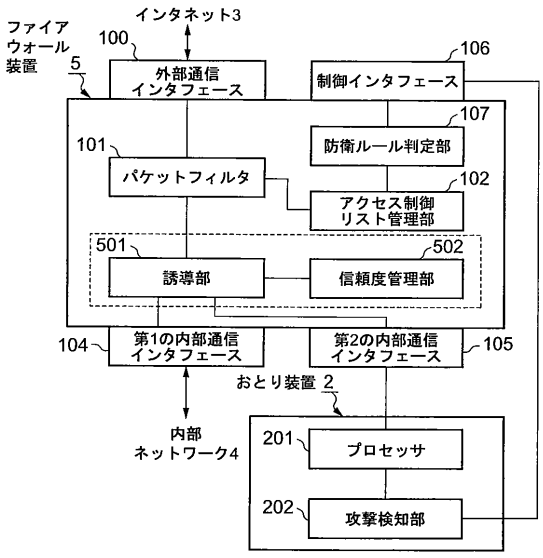
【図１３】



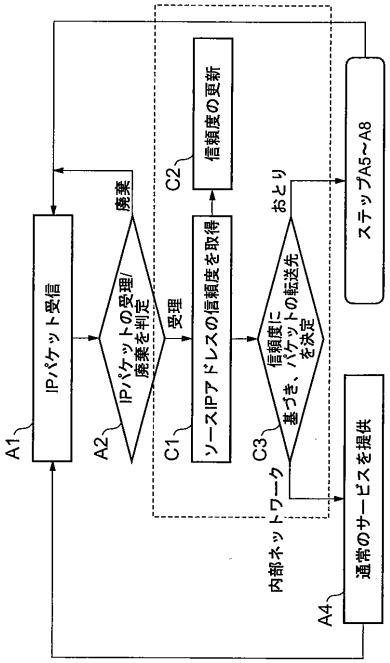
【図１４】



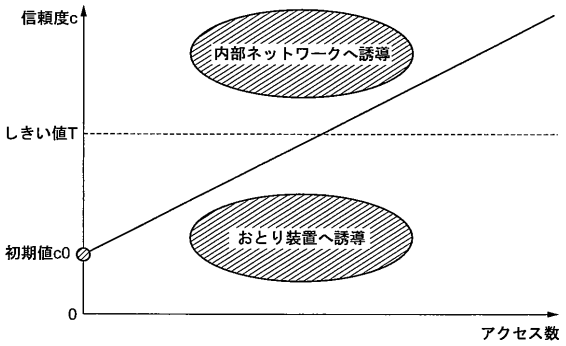
【図１５】



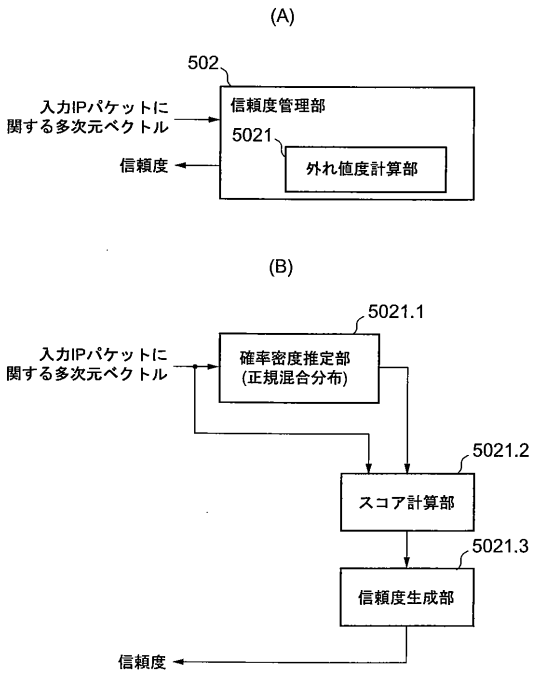
【図１６】



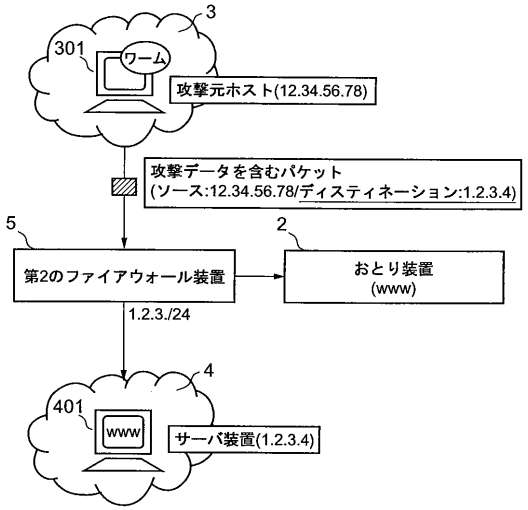
【図１７】



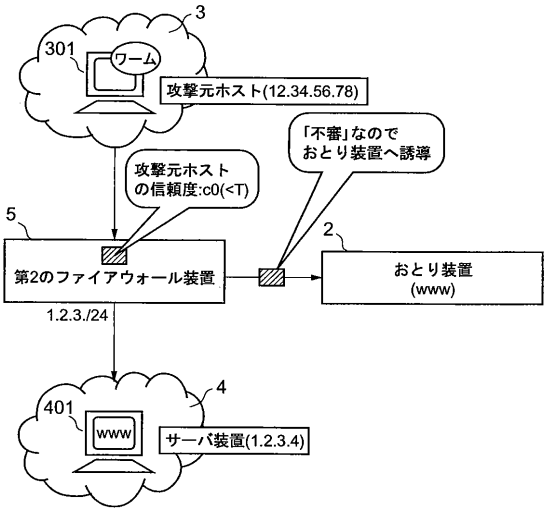
【図１８】



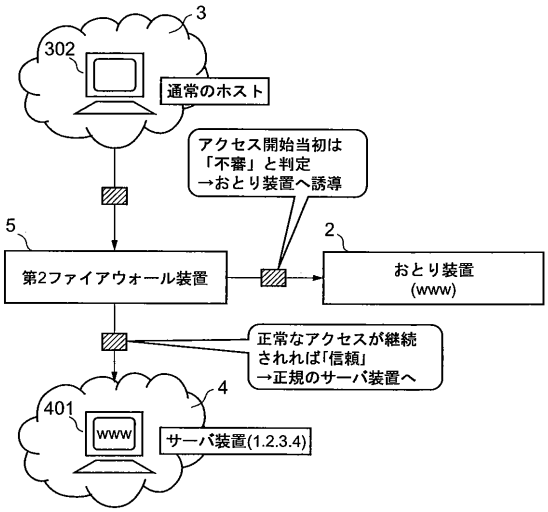
【図１９】



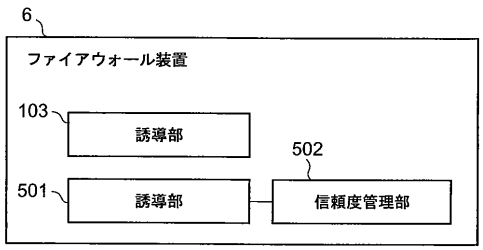
【図２０】



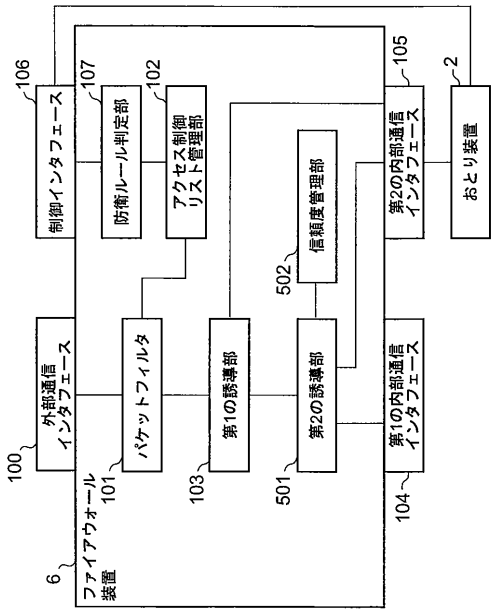
【図２１】



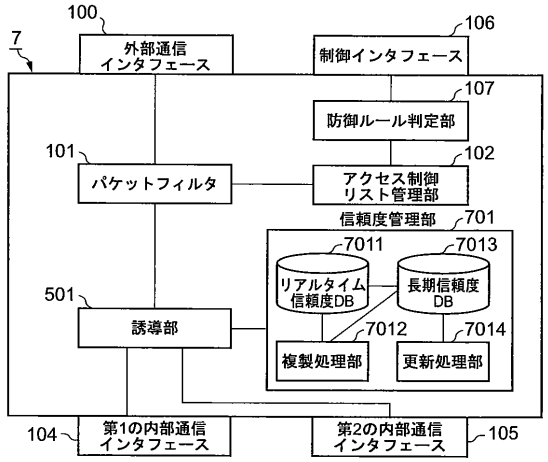
【図２２】



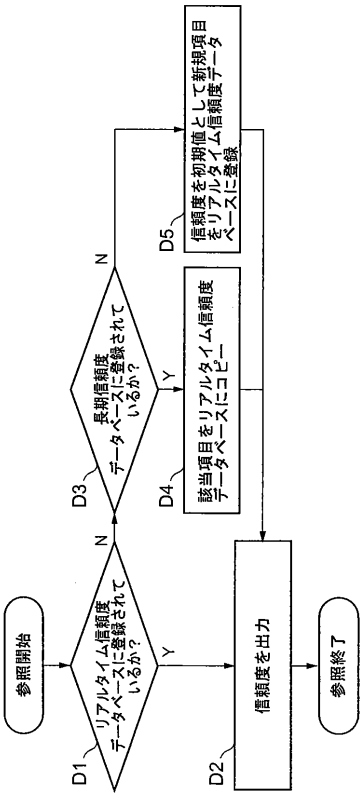
【図２３】



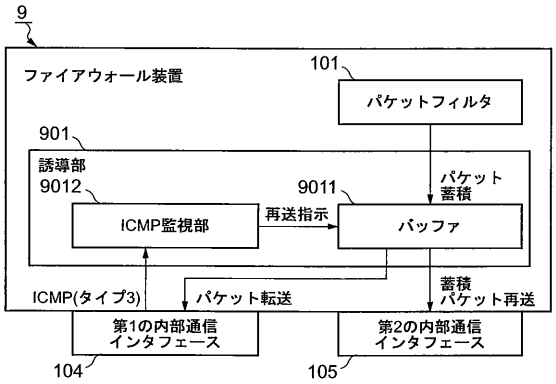
【図２４】



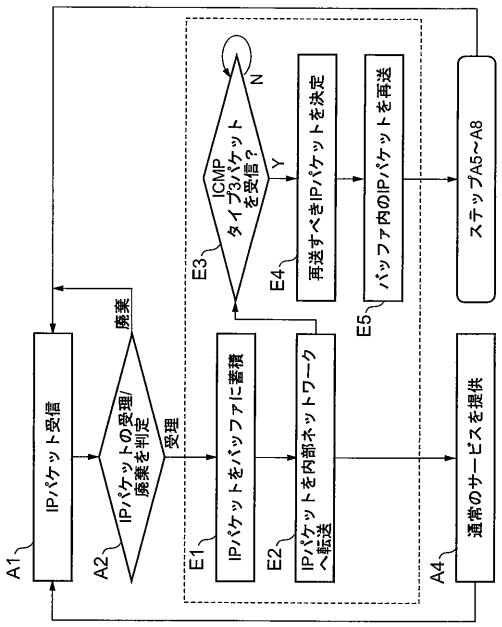
【図２５】



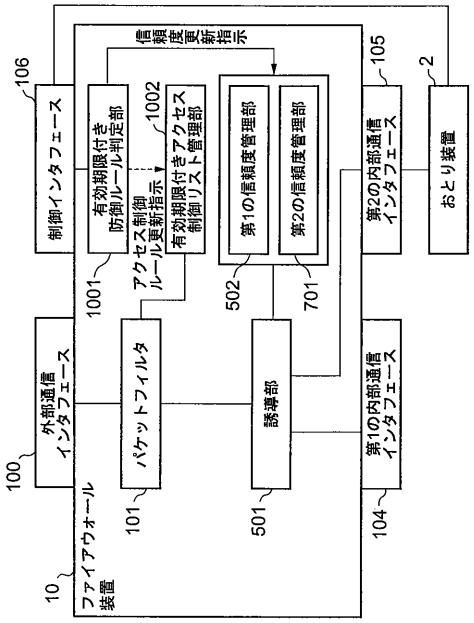
【図２６】



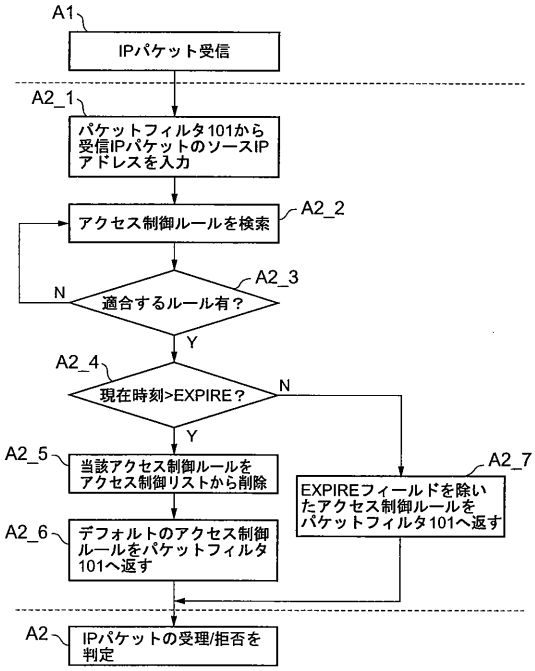
【図２７】



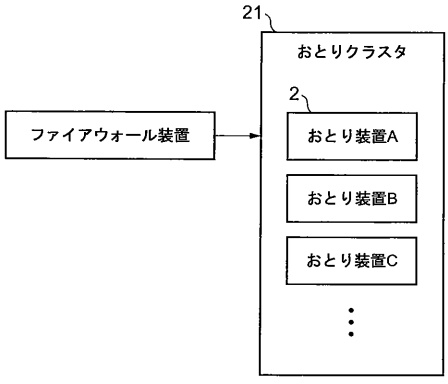
【図２８】



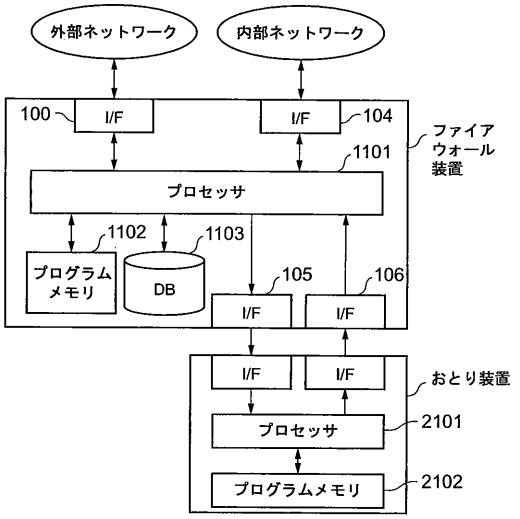
【図２９】



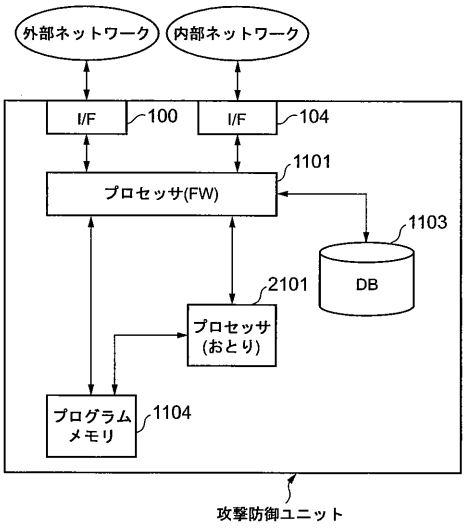
【図３０】



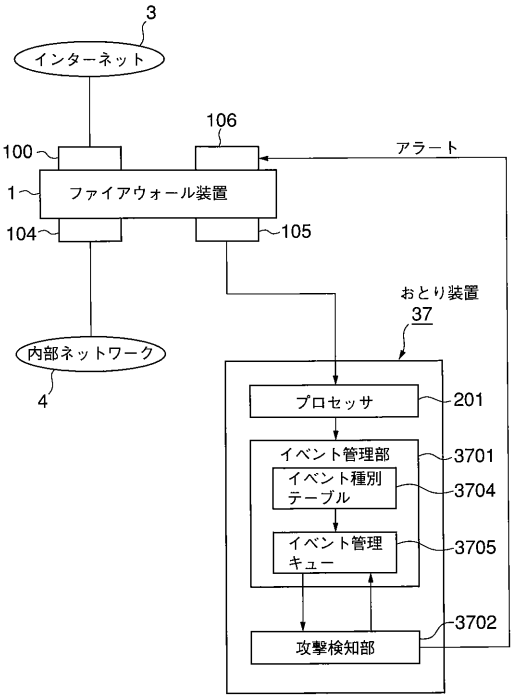
【図３１】



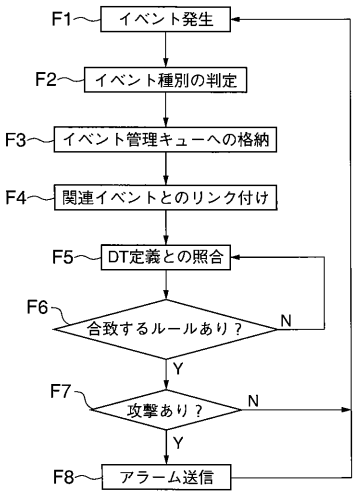
【図３２】



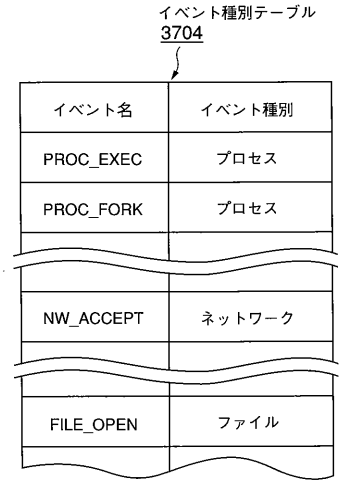
【図３３】



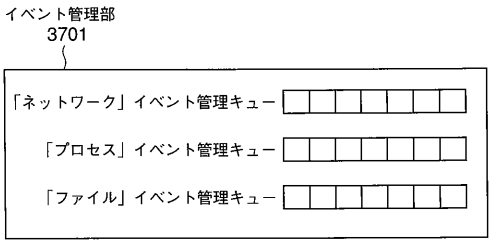
【図３４】



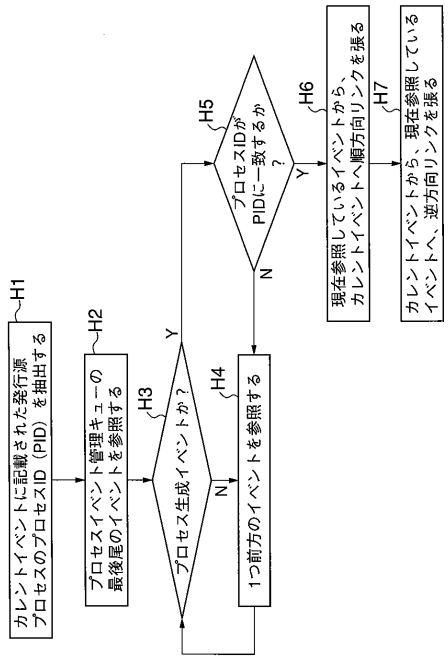
【図３５】



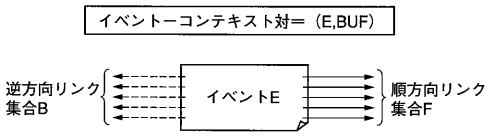
【図３６】



【図３７】



【図３８】

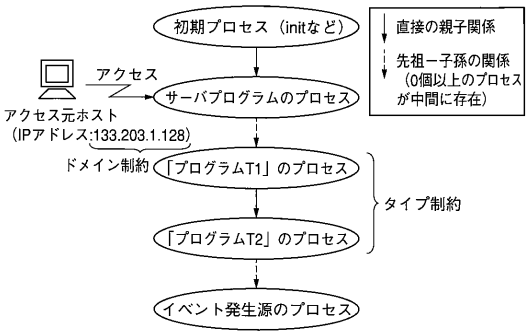


【図３９】

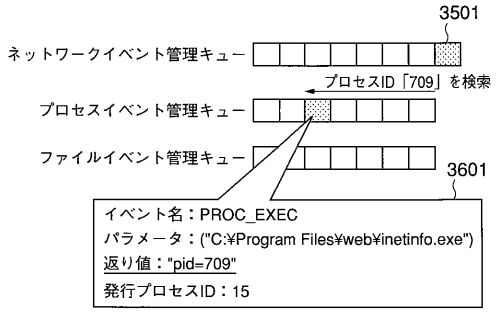
4101 DT定義ファイル

```
#（ルール1）WWWサーバによるログの書き出しを許可する
0.0.0.0/0,<Inetinfo.exe>,FILE_WRITE,C:¥winnt¥system32¥LogFiles¥.*;ALLOW
#（ルール2）WWWサーバによるコンテンツ領域の読込みを許可する。
0.0.0.0/0,<Inetinfo.exe>,FILE_READ,C:¥Inetpub¥wwwroot¥,*;ALLOW

#（ルール3）WWWサーバのサブシステムである登録CGIはデータベースを更新してよい。
0.0.0.0/0,<Inetinfo.exe><regist.exe>$,FILE_WRITE,C:¥data¥client.db;ALLOW
#（ルール4）WWWサーバのサブシステムである出力CGIによるデータベース読込みを許可。
0.0.0.0/0,<Inetinfo.exe><view.exe>$,FILE_READ,C:¥data¥client.db;ALLOW

#（ルール5）FTPサーバはコンテンツ領域に書き出し可能
#ただし、管理者ドメイン10.56.192.0/24からのアクセスに限る
10.56.192.0/24.^<ftpd.exe>+$,FILE_WRITE,C:¥Inetpub¥wwwroot¥.*;ALLOW

#（ルール6）WWWサーバは、特に許可されていない限り、ファイル書き出しを行わない。
0.0.0.0/0,<inetinfo.exe>.FILE_WRITE,.*;DENY
#（ルール7）許可されたプログラム以外によるデータベース領域のアクセスを禁止する。
0.0.0.0/0,.*,.*,FILE_READ|FILE_WRITE,C:¥data¥.*;DENY
#（ルール8）許可されたプログラム以外によるコンテンツ領域の書換えは攻撃である。
0.0.0.0/0,.*,.*,FILE_WRITE,C:¥Inetpub¥wwwroot¥.*;DENY

#（デフォルトルール）どのルールにもマッチしない場合は「許可」
DEFAULT;ALLOW
```

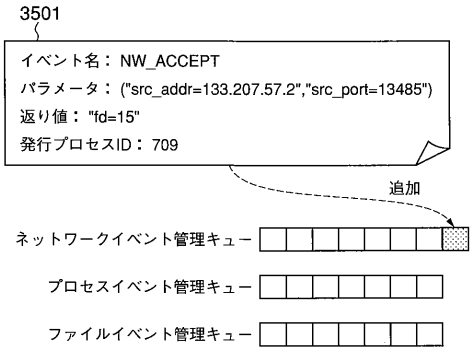
【図４０】



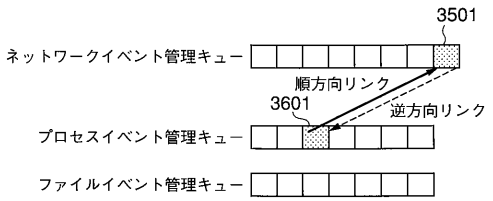
【図４２】



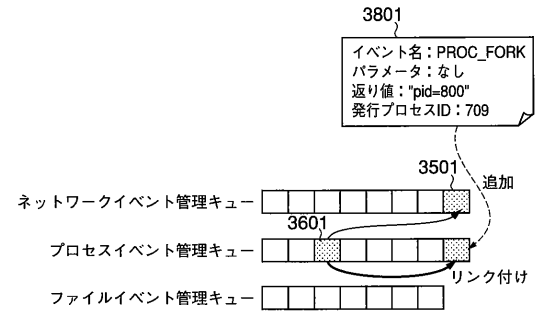
【図４１】



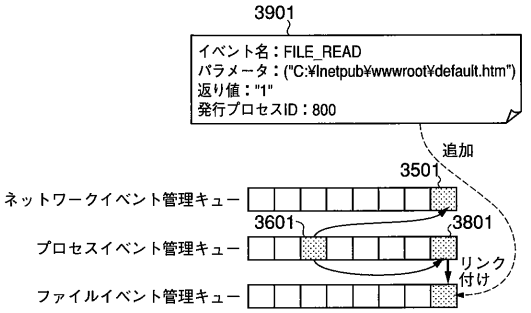
【図４３】



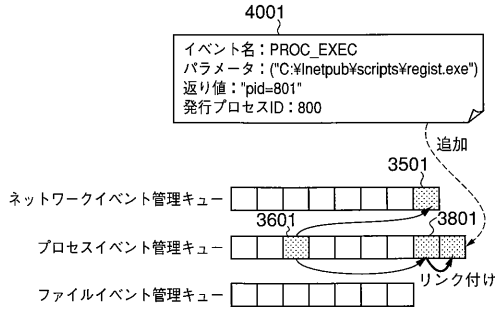
【図４４】



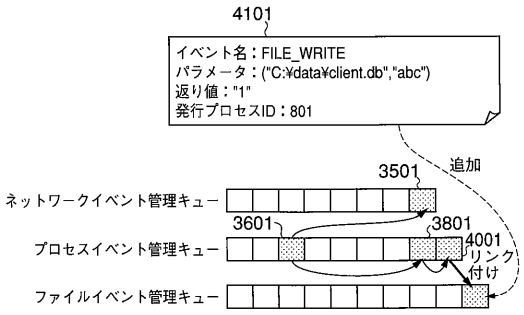
【図４５】



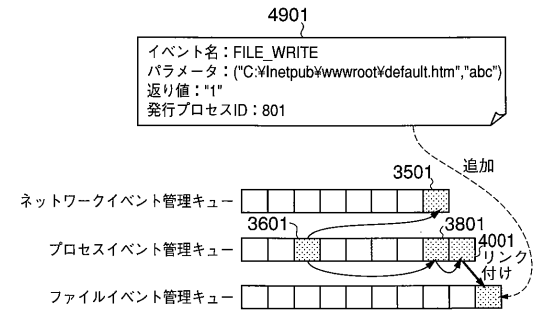
【図４６】



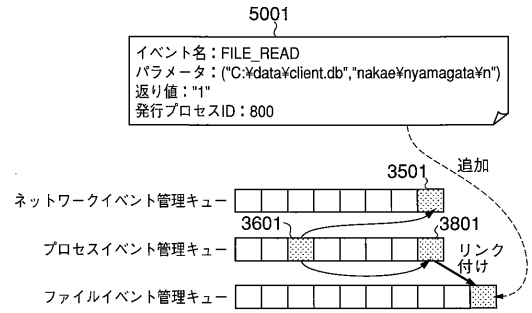
【図４７】



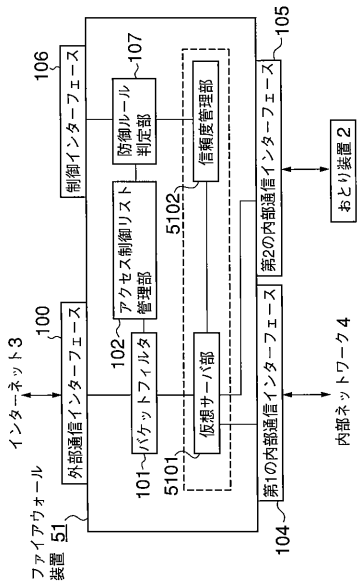
【図４８】



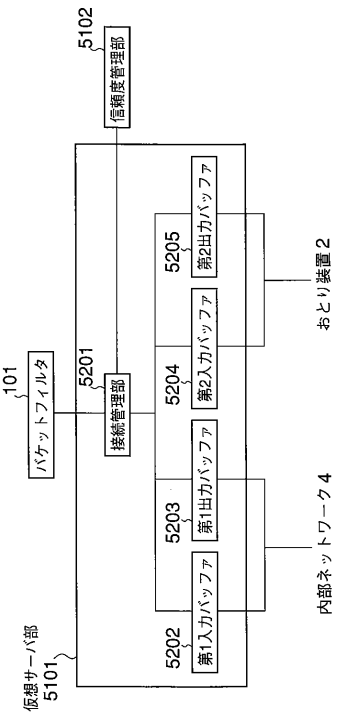
【図４９】



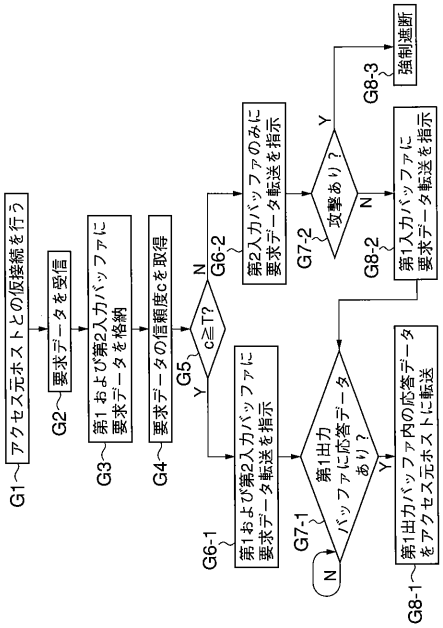
【図５０】



【図５１】



【図５２】



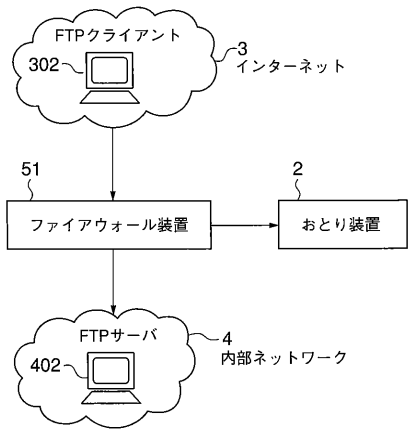
【図５３】

要求データ	信頼度
D0	1
D1	0
・・・	・・・
Dn	1

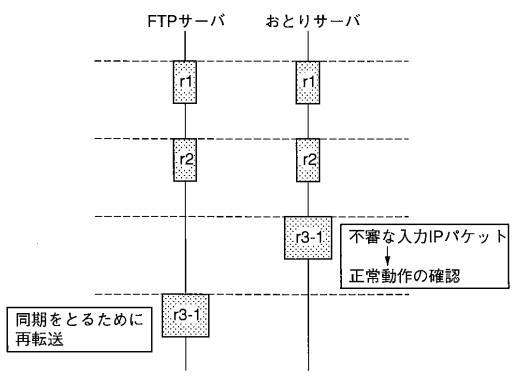
【図５５】

要求データ	信頼度
D0	1
D1	0
・・・	・・・
1	0

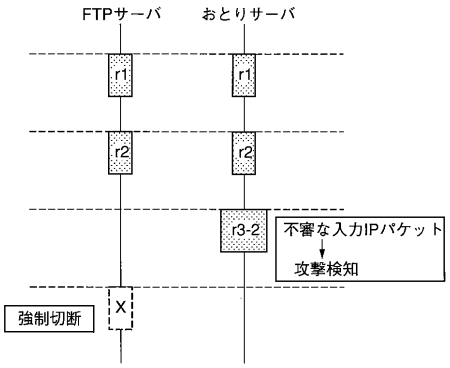
【図５４】



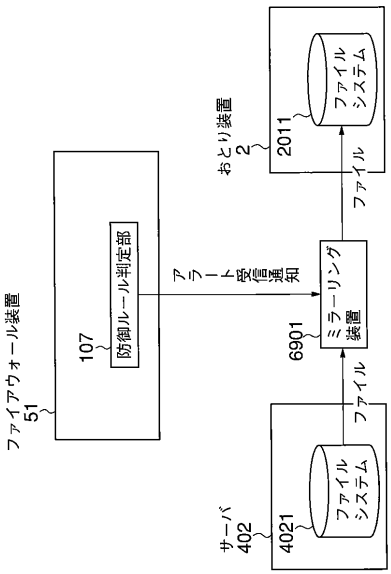
【図５６】



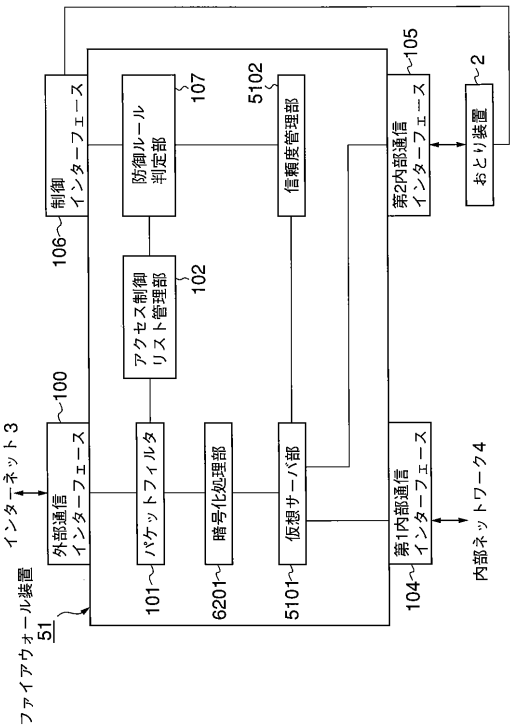
【図５７】



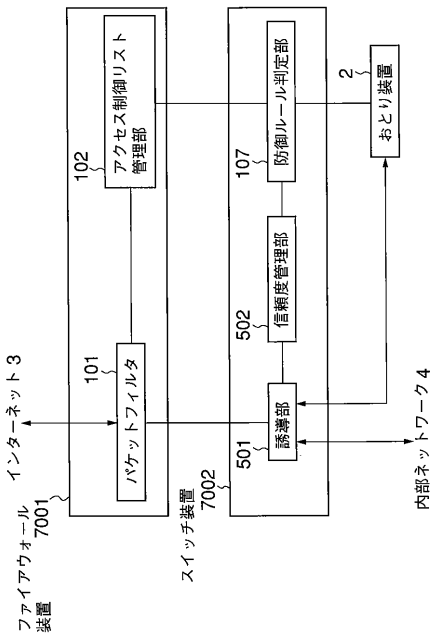
【図５８】



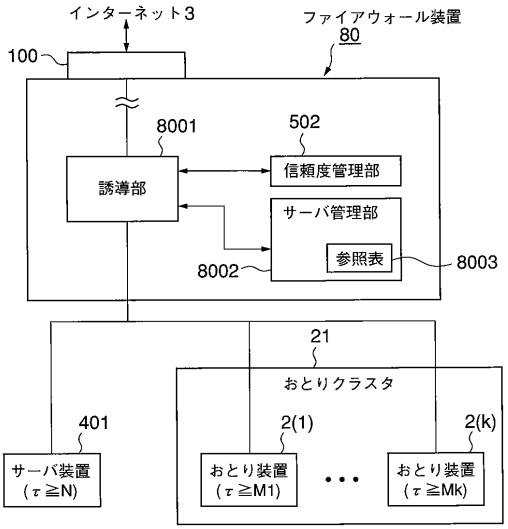
【図５９】



【図６０】



【図６１】

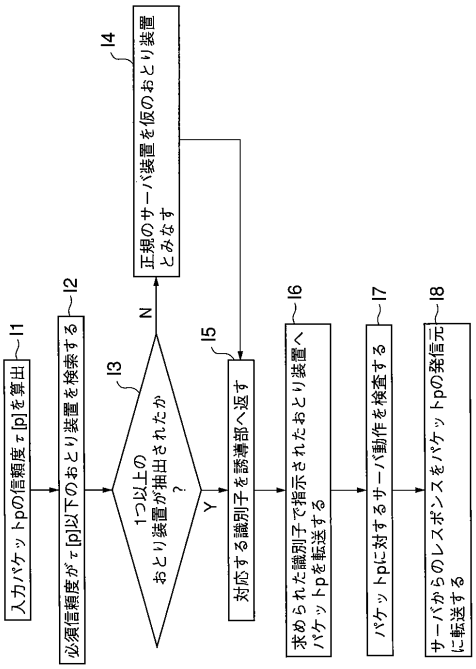


【図６２】

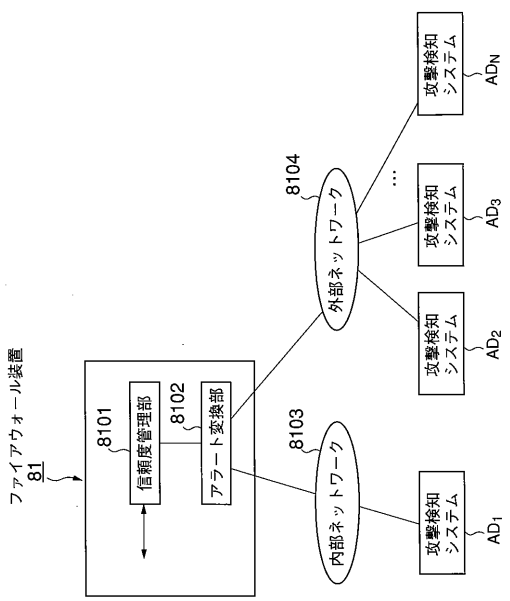
8003 参照表

サーバ識別子	必須信頼度
D1	M1
D2	M2
・・・	・・・
Dk	Mk

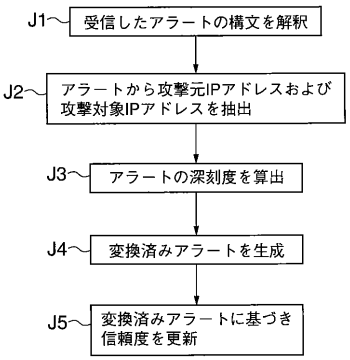
【図６３】



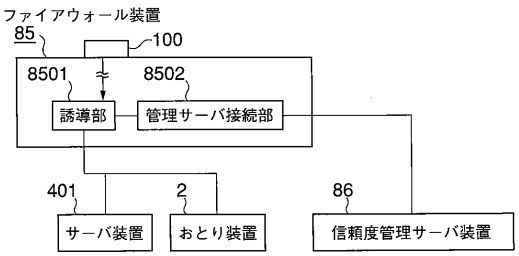
【図６４】



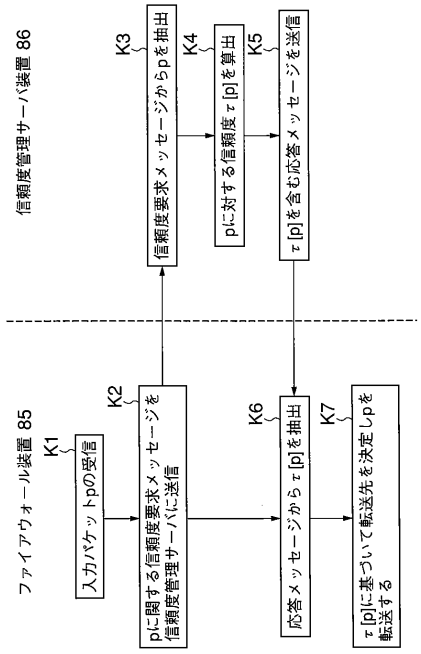
【図６５】



【図６６】



【図６７】


信頼度管理サーバ装置 86
ファイアウォール装置 85
K1
入力パケットpの受信
K2
pに関する信頼度要求メッセージを
信頼度管理サーバに送信
K3
信頼度要求メッセージからpを抽出
K4
pに対する信頼度τ[p]を算出
K5
τ[p]を含む応答メッセージを送信
K6
応答メッセージからτ[p]を抽出
K7
τ[p]に基づいて転送先を決定しpを
転送する