(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4072150号
(P4072150)

(45)発行日　平成20年4月9日(2008.4.9)　(24)登録日　平成20年1月25日(2008.1.25)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00　351Z
H04L 12/66 (2006.01)　　H04L 12/66　B

請求項の数 4　(全 16 頁)

(21)出願番号　特願2004-313993(P2004-313993)
(22)出願日　平成16年10月28日(2004.10.28)
(65)公開番号　特開2005-135420(P2005-135420A)
(43)公開日　平成17年5月26日(2005.5.26)
審査請求日　平成16年10月28日(2004.10.28)
(31)優先権主張番号　10/698197
(32)優先日　平成15年10月31日(2003.10.31)
(33)優先権主張国　米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】ホストベースのネットワーク侵入検出システム

(57)【特許請求の範囲】

【請求項１】

通信ネットワーク内のホスト・コンピュータ上で動作するホストベースのネットワーク侵入検出システムであって、

前記ホスト・コンピュータ内の処理装置に対するデータおよび命令を格納する前記ホスト・コンピュータ内の記憶装置と、

前記記憶装置に結合された前記処理装置であって、シグニチャのリポジトリからのシグニチャを使用して、前記通信ネットワークに関連するネットワーク・プロトコルのトランスポート層で処理されるデータ・パケットをスキャンし、前記スキャンしたデータ・パケットが悪意のあるものであるか否かを判定し、前記スキャンしたデータ・パケットが悪意がないと判定した場合は、悪意がないと判定した前記データ・パケットを前記トランスポート層と前記ネットワーク・プロトコルのアプリケーション層との間で機能する少なくとも１つのアプリケーション受信キュー（ＡＲＱ）に書き込むことにより、悪意がないと判定した前記データ・パケットを前記アプリケーション層に渡し、前記スキャンしたデータ・パケットが悪意があると判定した場合は、少なくとも１つのアクションを取るようにプログラムされた処理装置とを備え、

前記少なくとも１つのアクションが、

悪意があると判定した前記データ・パケットを前記少なくとも１つのアプリケーション受信キュー（ＡＲＱ）に書き込まないことにより、悪意があると判定した前記データ・パケットを前記アプリケーション層に渡さないこと、

悪意があると判定した前記データ・パケットに関するエラーのログを取ること、および
悪意があると判定した前記データ・パケットに関する既存の接続を前記トランスポート層が終了するように通知することを含むネットワーク侵入検出システム。
【請求項２】
通信ネットワーク内のホスト・コンピュータ上で動作するホストベースのネットワーク侵入検出システムであって、
前記ホスト・コンピュータ内の処理装置に対するデータおよび命令を格納する前記ホスト・コンピュータ内の記憶装置と、
前記記憶装置に結合された前記処理装置であって、シグニチャのリポジトリからのシグニチャを使用して、前記通信ネットワークに関連するネットワーク・プロトコルのトランスポート層で処理され且つ前記トランスポート層と前記ネットワーク・プロトコルのアプリケーション層との間で機能する少なくとも１つのアプリケーション受信キュー（ＡＲＱ）に書き込まれたデータ・パケットをスキャンし、前記スキャンしたデータ・パケットが悪意のあるものであるか否かを判定し、前記スキャンしたデータ・パケットが悪意がないと判定した場合は、悪意がないと判定した前記データ・パケットを前記少なくとも１つのアプリケーション受信キュー（ＡＲＱ）から前記アプリケーション層に渡し、前記スキャンしたデータ・パケットが悪意があると判定した場合は、少なくとも１つのアクションを取るようにプログラムされた処理装置とを備え、
前記少なくとも１つのアクションが、
悪意があると判定した前記データ・パケットに関するエラーのログを取ること、
悪意があると判定した前記データ・パケットに関する既存の接続を前記トランスポート層が終了するように通知すること、
前記ホスト・コンピュータのファイアウォール規則を変更することにより、悪意があると判定した前記データ・パケットのソースへのネットワーク・アクセスをブロックすること、
前記アプリケーション層のアプリケーションを終了すること、および
前記スキャンしたデータ・パケットが悪意があると判定されたことを前記アプリケーション層のアプリケーションに通知することを含むネットワーク侵入検出システム。
【請求項３】
前記プロトコルを監視する場合、前記処理装置が、スキャンのために１つまたは複数のハンドラに前記少なくとも１つのアプリケーション受信キュー（ＡＲＱ）に書き込まれたデータ・パケットをディスパッチするようにプログラムされる請求項２に記載のネットワーク侵入検出システム。
【請求項４】
前記処理装置が、偽応答を生成するようにプログラムされる請求項１又は請求項２に記載のネットワーク侵入検出システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にネットワーク・セキュリティの分野に関し、詳細には、通信ネットワークにおける侵入およびセキュリティ違反を検出するコンピュータ・ソフトウェアに関する。
【背景技術】
【０００２】
一般に通信ネットワーク・セキュリティ、具体的にはコンピュータ・ネットワーク・セキュリティはしばしば、ハッカーを含む無許可の侵入者による巧妙なアタックの対象となる。そのようなネットワークへの侵入者は、ネットワークの弱点を利用してアクセスおよび無許可特権を得ることにますます熟達してきており、そのようなアタックを検出し追跡することが難しくなっている。さらに、ウィルスやワームなどのセキュリティ脅威は人間の指示を必要とせず、複製し、他のネットワーク・システムに移動することができる。こ

うした侵入は、コンピュータ・システムに損傷を与える可能性があり、影響を受けるネットワークに関連するエンティティの主要部分に悪影響を及ぼす可能性がある。

【０００３】

プタセク，トーマス・エイチ（Ptacek, Thomas H.）およびニューシャム，ティモシー・エヌ（Newsham,Timothy N.）、「挿入、回避、およびサービス妨害：ネットワーク侵入検出の回避（Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection）」、（http://secinf.net/info/ids/idspaper/idspaper.html）には、ネットワーク侵入検出を含む詳細が説明されている。

【非特許文献１】プタセク，トーマス・エイチ（Ptacek, Thomas H.）およびニューシャム，ティモシー・エヌ（Newsham,Timothy N.）、「挿入、回避、およびサービス妨害：ネットワーク侵入検出の回避（Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection）」、（http://secinf.net/info/ids/idspaper/idspaper.html）

【発明の開示】

【発明が解決しようとする課題】

【０００４】

既存のネットワーク侵入検出システム（ＮＩＤＳ）は、そのようなＮＩＤＳのアーキテクチャに固有の問題のために、ネットワーク中のあらゆるホスト上に配置するには不適切である。ＮＩＤＳは、無差別モード・キャプチャおよび分析を使用し、それによってシステム上で著しいオーバヘッドを引き起こし、挿入および回避アタックに対して脆弱となる。

【課題を解決するための手段】

【０００５】

本発明の一態様によれば、通信ネットワークにおける侵入を検出する方法が提供される。この方法は、シグニチャのリポジトリからのシグニチャを使用して、通信ネットワークに関連するネットワーク・プロトコルのトランスポート層で処理されるデータ・パケットをスキャンするステップと、スキャンしたデータ・パケットが悪意のあるものであるか否かを判定するステップと、何らかのデータ・パケットが悪意があると判定した場合、少なくとも１つのアクションを取るステップとを含む。

【０００６】

かかるアクションは、悪意があると判定した任意のデータ・パケットの、ネットワーク・プロトコルのアプリケーション層への伝送を中断すること、悪意があると判定した任意のデータ・パケットに関するエラーのログを取ること、何らかのデータ・パケットが悪意があると判定した場合にホスト・コンピュータのファイアウォール規則を変更すること、何らかのデータ・パケットが悪意があると判定されたことをネットワーク管理者に通知すること、悪意があると判定した任意のデータ・パケットに関する既存の接続をトランスポート層が終了するように通知すること、悪意があると判定した任意のデータ・パケットのソースへのネットワーク・アクセスをブロックすること、何らかのデータ・パケットが悪意があると判定した場合、アプリケーション層のアプリケーションを終了すること、および何らかのデータ・パケットが悪意があると判定した場合、アプリケーション層のアプリケーションに通知することのうち少なくとも１つを含むことができる。

【０００７】

この方法は、悪意がないと判定した任意のデータ・パケットをアプリケーション層に送るステップをさらに含むことができる。

【０００８】

この方法は、トランスポート層からのデータ・パケットを処理するステップをさらに含むことができる。

【０００９】

この方法は、プロトコルが監視されているか否かを判定するステップをさらに含むことができる。

【００１０】
スキャンするステップおよび判定するステップは、スキャン・モジュールを使用して実施することができる。
【００１１】
少なくとも１つのアプリケーション受信キュー（ＡＲＱ）は、トランスポート層とアプリケーション層との間で機能することができる。スキャンするステップは、トランスポート層と少なくとも１つのアプリケーション受信キュー（ＡＲＱ）の間で実施することができる。
【００１２】
この方法は、少なくとも１つのアプリケーション受信キュー（ＡＲＱ）からデータを得るステップをさらに含むことができる。この少なくとも１つのアプリケーション受信キューは、トランスポート層とアプリケーション層との間で直接機能することができる。スキャンするステップは、この少なくとも１つのアプリケーション受信キュー（ＡＲＱ）内のデータ・パケットに対して実施することができる。
【００１３】
この方法は、プロトコルを監視する場合、スキャンのために１つまたは複数のハンドラにデータ・パケットをディスパッチするステップをさらに含むことができる。
【００１４】
スキャンするステップおよび判定するステップは、スキャン・デーモンを使用して実施することができる。
【００１５】
この方法は、偽応答を生成するステップをさらに含むことができる。
【００１７】
本発明の別の態様によれば、上記の検出する方法を実施する、通信ネットワークにおける侵入を検出するシステムと、通信ネットワークにおける侵入を検出するように構成されたプログラム式命令を含むコンピュータ可読媒体とが開示される。
【００１９】
図面を参照しながら本発明の少数の実施形態を以下で説明する。
【発明を実施するための最良の形態】
【００２０】
通信ネットワークにおける侵入を検出する方法、システム、およびコンピュータ・プログラム製品が開示される。さらに、通信ネットワークにおける侵入を防止する方法、システム、およびコンピュータ・プログラム製品が開示される。以下の説明では、ネットワーク構成、ネットワーク・プロトコル、プログラミング言語などを含む多数の特定の詳細を説明する。しかし、この開示から、本発明の範囲および精神から逸脱することなく、修正または置換あるいはその両方を行えることは当業者には明らかであろう。他の環境では、本発明を不明瞭にしないように、特定の詳細を省略することがある。
【００２１】
通信ネットワークにおける侵入を検出する方法はモジュールとして実装することができる。同様に、通信ネットワークにおける侵入を防止する方法はソフトウェアとして実装することができる。モジュール、特にモジュールの機能は、ハードウェアまたはソフトウェアとして実装することができる。ソフトウェアの意味では、モジュールは、特定の機能または関係する機能を通常実施するプロセス、プログラム、またはその一部である。このようなソフトウェアは、例えばJava（登録商標）、Ｃ、Ｃ＋＋、Fortranとして実装することができるが、任意の数の他のプログラミング言語／システム、またはその組合せとして実装することもできる。ハードウェアの意味では、モジュールは、他の構成要素またはモジュールと共に使用するように設計された機能ハードウェア・ユニットである。例えば、モジュールは離散的電子構成部品を使用して実装することができ、またはモジュールは、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、特定用途向け集積回路（ＡＳＩＣ）などの電子回路全体の一部を形成することができる。物理的実装はまた、例えばＦ

ＰＧＡに関する構成データ、またはＡＳＩＣに関するレイアウトも含むことができる。さらに、物理的実装の記述は、EDIF_netlisting言語、構造ＶＨＤＬ、構造Verilogなどでよい。多数のその他の可能性も存在する。システムをハードウェア・モジュールとソフトウェア・モジュールの組合せとして実装できることを当業者は理解されよう。

【００２２】

ネットワーク内のあらゆるホスト上にネットワーク侵入検出システム（ＮＩＤＳ）を配置することにより、ネットワーク全体のセキュリティが大幅に向上する。本発明の実施形態は、ＨＮＩＤＳアーキテクチャが無差別モード・キャプチャを使用する受動プロトコル解析に対して機能せず、それによってネットワーク内のあらゆるホスト上でＮＩＤＳを使用することが容易になるという点で既存のＮＩＤＳアーキテクチャとは異なるアーキテクチャを開示する。以下で提示する実施形態は、本発明の可能な実施形態の完全なリストとなるよう意図されておらず、またはそのようにみなすべきではない。

【００２３】

概説

本発明の実施形態は、ネットワーク内の各ホストがアンチウィルス・ソフトウェアと類似の方式でネットワーク侵入検出ソフトウェアを実行することを可能にする「ホストベースのネットワーク侵入検出システム」（ＨＮＩＤＳ）を開示する。このアーキテクチャにより、ネットワーク上のあらゆるシステムが、侵入を検出および管理する際に自律エンティティとして振る舞うことが可能となる。

【００２４】

ネットワークを介して通信することができるあらゆるシステムは、通信プロトコル（例えばＴＣＰ／ＩＰプロトコルが一般的かつ広範に使用されている）を使用しなければならない。ネットワーク層（ＴＣＰ／ＩＰプロトコルの場合にはＩＰ）は断片化を処理し、通信プロトコルのトランスポート層（ＴＣＰ／ＩＰプロトコルの場合にはＴＣＰおよびＵＤＰ）は、必要に応じてパケットの並び換えおよび再組立てを処理する。この処理が完了すると、データがアプリケーション層にサブミットされる。ネットワーク層およびトランスポート層がデータの処理を完了した後、ＨＮＩＤＳは、プロトコル・スタックの挙動を活用し、悪意のあるコンテンツを求めてデータをスキャンする。したがって、ＨＮＩＤＳは、データ全体に対して働き、それによって挿入および回避アタックの問題ならびに既存のＮＩＤＳに関連する待ち時間およびオーバヘッドが緩和される。ＨＮＩＤＳは、ＨＮＩＤＳを使用するシステムに向かうデータだけをスキャンし、受動プロトコル解析および無差別モード・キャプチャを使用しない。

【００２５】

このアーキテクチャの詳細をさらに説明するため、２つの異なるＨＮＩＤＳの実施形態を説明する。一実施形態では、ＨＮＩＤＳは、データがトランスポート層でアプリケーションにサブミットされる前にデータをスキャンする。論理的には、ＨＮＩＤＳは、通信プロトコル（例えばＴＣＰ／ＩＰ）のトランスポート層とアプリケーション層の間に位置する。別の実施形態では、ＨＮＩＤＳは、着信データを求めてアプリケーション受信キュー（ＡＲＱ）を監視し、データが到着したとき、悪意のあるコンテンツを求めてデータをスキャンする。

【００２６】

ＨＮＩＤＳは、先を見越して侵入を防止するための機能を有し、それによって「侵入防止システム」として動作する。このことは、「アイドル時間」の概念を導入し、それによってネットワーク・インターフェースがアイドル時間の満了後に使用不能にされることによって達成される。アイドル時間は、システムからパケットが送信されない期間である。インターフェースが使用不能にされるので、システムはネットワークからのどんなパケットも処理しない。実質上、このことは、システムをネットワークから取り除き、誰もシステムを使用していない閑散時の間（例えば夜間）に、侵入に関係する活動を防止することと同じである。ユーザが存在し、何らかのネットワーク関係の活動を実施していることを示す、ネットワークに送信すべきパケットが存在するとき、ネットワーク・インターフェ

ースが再び使用可能にされる。結果として得られる「アイドル時間」機能を有するシステムは、「ホストベースのネットワーク侵入検出／防止システム」とも呼ぶことができる。

【００２７】

最近では、（アタッカをわなに誘い込むように）偽サービスを使用することが重要となりつつある。ＨＮＩＤＳは、偽サービスをセットアップするための備えも有することができる。

【００２８】

本発明の実施形態は、無差別モード・キャプチャおよび受動プロトコル解析に関連する問題に対処するＨＮＩＤＳアーキテクチャを含む。

【００２９】

このアーキテクチャは、

１）「挿入」および「回避」アタックの防止、

２）パケットごとの解析、および悪意のあるコンテンツの検出時の応答、

３）ユーザの意図を判断するために欺瞞機構（deception mechanisms）を使用することを容易にすること、および

４）ネットワークのセキュリティ全体の改善を実現する。

【００３０】

一般的概念

図１は、本発明の実施形態によるＨＮＩＤＳ１００の機能ブロック図である。ＨＮＩＤＳ１００は、ネットワークに結合されたホスト・コンピュータ上で動作するスキャン・モジュール（ＳＭ）１０１およびアイドル時間処理モジュール（ＩＴＰＭ）１０２を含む。スキャン・モジュール（ＳＭ）はスキャン・デーモン（ＳＤ）でよい。ＳＭおよびＳＤの詳細を、図２および図３を参照しながらより詳細に説明する。図９にＩＴＰＭに関する流れ図を示す。モジュール１０１および１０２は、別々の機能を有する独立なモジュールである。

【００３１】

ＩＴＰＭモジュールはアイドル時間機能を担う。ＨＮＩＤＳはこれなしで機能することができる。ＩＴＰＭは侵入防止機能を提供する。

【００３２】

ＨＮＩＤＳ１００がシステムにとってローカルであるので、ＨＮＩＤＳ１００は外部世界とは直接インターフェースしない。

【００３３】

ＨＮＩＤＳ１００は、ホスト上にインストールされる別個のアプリケーションでよく、またはＨＮＩＤＳ１００はホストのネットワーク実装の一部でよい。

【００３４】

ＩＴＰＭ１０２は、ネットワーク・インターフェースを使用可能および使用不能にするためのプログラム・コードを含むことができる。アイドル時間が満了したとき、ＩＴＰＭ１０２はネットワーク・インターフェースを使用不能にする。インターフェースは、ネットワークにパケットを送信する必要があるときに使用可能にされる。ネットワーク・インターフェースを使用可能および使用不能にすることは、当技術分野で周知である。図面には、ネットワーク・インターフェース（物理的アダプタ）を図示していない。ＩＴＰＭ１０２は、ネットワーク・インターフェースを使用可能／使用不能にするためのコードを含む。この作業を実施する方法は、当業者にとって周知である。

【００３５】

このことは、ネットワーク・ドライバ・ソフトウェアでインターフェース（ＩＯＣＴＬ－入出力制御エントリポイントなど）を設け、ネットワーク・インターフェースを使用可能／使用不能にすることによって実施することができる。

【００３６】

一実施形態

図２に、スキャン・モジュール（ＳＭ）２００をより詳細に示す。スキャン・モジュー

ル２００は、スキャニング・エンジン２０２、シグニチャ・データベース２０１、およびログ・データベース２０３を含む。

【００３７】

シグニチャ・データベース２０１は、周知のアタック・シグニチャのリストを含む。これは、アンチウィルス・システムで使用されるウィルス・シグニチャ・データベースと類似している。スキャニング・エンジン２０２は、シグニチャ・データベース２０１中のシグニチャを使用して侵入を検出する。シグニチャ・データベース２０１は、シグニチャのリストを含むプレーンＡＳＣＩＩファイルでよいが、その他のファイル・フォーマットも実施することができる。シグニチャはａｒａｃｈＮＩＤＳデータベースから取得することができる。

【００３８】

シグニチャの例を表１に与える。ただし、バイト・コード・フォーマットの２進データを囲むのに「｜」を使用する。

【００３９】

【表１】

表１

"|eb 02 eb 02 eb 02|"	このイベントは、アタッカがデーモンの１つを、jmp0x02「ステルス nop」でオーバーフローしようと試みたことを示す。
"GetInfo|0d|"	このイベントは、アタッカが NetBus リモート管理ツールを照会しようと試みていることを示す。この正当な管理ツールは、しばしばアタッカによりトロイの木馬として使用される。
"|5c|IPC$|00 41 3a 00|"	このイベントは、リモート・ユーザが IPC# シェアを使用して、名前付きパイプを開こうと試みている可能性があることを示す。
"|0b 00 00 00 07 00 00 00|Connect"	このイベントは、リモート・ユーザが Windows(R)上で動作するダガー1.4.0 トロイの木馬サーバに接続するよう試みたことを示す。この接続試行は、既存の危険を示す可能性がある。

【００４０】

シグニチャ・データベース２０１の設計は、記載の実施形態通りに限定されるのではなく、どんな適切な実施形態も使用することができる。例えば、プレーンＡＳＣＩＩファイルの代わりに、Microsoft Excel（商標）ファイルおよびMySQL（商標）やPostgreSQL（商標）などのデータベースのうち１つまたは複数にシグニチャを格納することもできる。

【００４１】

スキャニング・エンジン２０２は、シグニチャ・データベース２０１を使用して、シグニチャの存在を求めてデータをスキャンし、何らかのシグニチャが見つかった場合に適切なアクションを取るためのプログラム・コードを含む。図２の実施形態では、関係する詳細をログ・データベース２０３に記録することができる。悪意のあるデータの発見後に取るべきアクションは、エラーの記録だけに限定されない。他の可能なアクションには、デスクトップ・ファイアウォール規則の変更、およびリモート管理者への通知が含まれる。さらに、他のアクションを単独で、または組み合わせて実施することができる。

【００４２】

図３に、スキャン・デーモン（ＳＤ）３００を示す。アプリケーション受信キュー（ＡＲＱ）は、アプリケーションがアプリケーションのデータを取得するキューである。スキャン・デーモン３００は、データを求めてＡＲＱを監視し、その後にデータを解析するためのプログラム・コード３０２を含む。通常、コード３０２は、異なるアプリケーション・プロトコルに対応するプロトコル・ハンドラ３０２ａ．．．３０２ｎを含む。ハンドラ３０２ａ．．．３０２ｎは、監視するように構成されたプロトコル・ポートに関してのみ活動化される。例えば、ＨＴＴＰ３０２ａおよびＦＴＰ３０２ｂが監視するように構成された場合、これらのプロトコルに関するハンドラ３０２ａ、３０２ｂだけが活動化される。これらのハンドラ３０２ａ、３０２ｂは、シグニチャ・データベース３０１を使用してデータをスキャンする。合致が見つかった場合、ログ・データベース３０３に適切なエラーを記録することができる。

【００４３】

図３の実施形態は、スキャン・デーモン３００に関して可能な唯一の実施形態ではない。行われる他のアクションには、例えばファイアウォール規則を変更して問題のホストからパケットを受信することを防止すること、および既存の接続を切断するようにトランスポート層に通知することを含めることができる。

【００４４】

図４に、プロトコル・スタック４００の上方に向かうパケットの流れを示す。単に例示の目的で、ＴＣＰ／ＩＰプロトコル・スタックを示す。実施することのできるその他のプロトコル・スタックには、トランスポート層とアプリケーション層の間に明確な区分を有する階層化モデルに従う任意のプロトコル・スタックが含まれる。

【００４５】

物理媒体４１０は、リンク層４１２にパケットを与え、リンク層４１２は、パケットをネットワーク層処理４１４に与える。そこから、パケットはトランスポート層処理４１６に進む。トランスポート層４１６は、データをアプリケーション受信キュー４１８にコピーする。アプリケーション受信キュー４１８は通常はソケット・キューである。次いでアプリケーション層４２０が、ＡＲＱ４１８からデータをコピーし、データを使用する。

【００４６】

図５に、本発明の実施形態を示す。物理媒体５１０、リンク層５１２、ネットワーク層５１４、およびトランスポート層５１６は、それぞれ図４の機能４１０、４１２、４１４、および４１６に対応する。リンク層５１２は、イーサネット（商標）、トークン・リング、ワイヤレス・ネットワーク、およびその他の適切なネットワークでよく、イーサネット（商標）およびトークン・リングは単に例示のために挙げたに過ぎない。リンク層は、通常はそうであるが、ネットワーク実装のトランスポート層とアプリケーション層が明確に区分されることを条件として、いくつかのネットワークのいずれでもよい。ネットワーク層５１４はＩＰでよい。トランスポート層５１６はＴＣＰ／ＵＤＰでよい。ホストベースのネットワーク侵入検出システム（ＨＮＩＤＳ）５３０は、トランスポート層５１６とアプリケーション層５２０の間で機能する。ＨＮＩＤＳ５３０は、この実施形態では図２のスキャン・モジュール（ＳＭ）２００を使用する。ＨＮＩＤＳ５３０は、トランスポート層５１６とＡＲＱ５１８の間をインターフェースすることが好ましい。

【００４７】

図６は、図５の実施形態に関するプロセス６００を要約する流れ図である。ステップ６０１では、ＨＮＩＤＳ５３０により、トランスポート層５１６からパケットを受信する。ステップ６０２では、ＨＮＩＤＳ５３０は、ネットワーク・プロトコルを監視するか否かを検証する。プロトコルを監視しない場合（ＮＯ）、ステップ６０３で、ＨＮＩＤＳ５３０は対応するアプリケーション５２０にデータを渡す。プロトコルを監視する場合（ＹＥＳ）、ステップ６０４で、スキャニング・エンジン２０２が、シグニチャ・データベース２０１を使用してデータをスキャンする。判定ステップ６０５では、データが悪意のあるものか否かについてチェックを行う。データが悪意のあるものである場合（ＹＥＳ）、データはアプリケーション５２０に渡されず（データはＡＲＱにプットされない）、ステッ

プ６０６で、関連する接続をドロップし、エラーを記録する。接続をドロップすることは、リモート・ホストとのネットワーク接続を終了することを意味する。このシステムは、他の既存の／新しい接続に対する要求を引き続きサービスすることができる。しかし、ステップ６０６において、これらは、データが悪意のあるものと判明したときに取ることができる唯一の可能なアクションではない。他の可能なアクションには、攻撃側ホストへのアクセスのブロック、攻撃側ホストからのネットワーク・アクセスのブロック、システム管理者への通知が含まれる。さらに別のアクションも実施することができる。データが悪意のあるものでない場合（ＮＯ）、ステップ６０７で、対応するアプリケーション５２０にデータを渡す。

【００４８】

別の実施形態

図７に別の実施形態を示す。図７の物理的媒体７１０および層７１２、７１４、７１６は、それぞれ図４の媒体４１０および層４１２、４１４、４１６に対応する。データは、アプリケーション層７２０に渡される前に、トランスポート層７１６からアプリケーション受信キュー（ＡＲＱ）７１８に渡される。この別の実施形態のＨＮＩＤＳ７３０は、ＨＮＩＤＳ７３０とＡＲＱ７１８の間の矢印で示すように、アプリケーション受信キュー（ＡＲＱ）７１８を監視する。ＨＮＩＤＳ７３０からトランスポート層７１６への矢印は、ＨＮＩＤＳ７３０が、望ましい場合、リモート・ホストとの接続を終了する（または何らかの他の適切なアクションを開始する）ようにトランスポート層７１６に通知／命令できることを示す。ＨＮＩＤＳ７３０からアプリケーション層７２０への矢印は、ＨＮＩＤＳ７３０が、必要ならパケットを処理しないように、特定の悪意のある接続に関連する資源をリセット／解放するように、さらにはアプリケーション７２０をキルするようにアプリケーション７２０に通知／命令できることを示す。ＨＮＩＤＳ７３０は、この実施形態では図３のスキャン・デーモン３００を使用する。

【００４９】

図８は、上記の実施形態によるプロセス８００を要約する流れ図である。ステップ８０１では、データが到着したとき、ＨＮＩＤＳ７３０は、ＡＲＱ７１８からデータをピックアップし、データを解析する。判定ステップ８０２では、ＨＮＩＤＳ７３０は、プロトコルを監視するか否かを判定する。プロトコルを監視しない場合（ＮＯ）、ＨＮＩＤＳ７３０は、ステップ８０３では何も行わない。プロトコルを監視する場合（ＹＥＳ）、ステップ８０４では、スキャニング・デーモン３００が、適切なプロトコル・ハンドラ３０２ａ．．．３０２ｎをディスパッチして、シグニチャ・データベース３０１を使用してデータをスキャンする。判定ステップ８０５では、データが悪意のあるものか否かを判定するチェックを行う。データが悪意のあるものでない場合（ＮＯ）、ハンドラは、ステップ８０６では何も行わない。すなわちステップ８０６ではアクションは不要である。データが悪意のあるものである場合（ＹＥＳ）、ステップ８０７で、プロトコル・ハンドラは、適切な接続を終了する、アプリケーションをキルする、アプリケーションに通知する、攻撃側ホストからネットワーク・アクセスをブロックする、関連する詳細を記録するなどの適切なアクションを取る。こうしたアクションのうち任意の１つまたは複数を実施することができる。他のアクションを実施することもできる。

【００５０】

アイドル時間処理モジュール

図９は、図１のアイドル時間処理モジュール１０２に関するプロセス９００を要約する流れ図である。ステップ９０１でアイドル時間が満了したとき、ステップ９０２でネットワーク・インターフェースを使用不能にする。判定ステップ９０３では、送信すべきパケットが存在するか否かを判定するためにチェックを行う。送信すべきパケットについての指示がある場合（ＹＥＳ）、ステップ９０４で、ネットワーク・インターフェースを再び使用可能にする。ネットワーク・インターフェースを使用可能および使用不能にすることは当技術分野で周知である。そうではなく、ステップ９０３で送信すべきパケットが存在しない場合（ＮＯ）、処理はステップ９０３に戻る。

【００５１】
ＩＴＰＭとスキャン・モジュールは別々のモジュールである。ＩＴＰＭはアイドル時間機能を担う。ＨＮＩＤＳはこれなしで機能することができる。ＩＴＰＭは侵入防止機能を提供する。
【００５２】
ＩＴＰＭモジュールは、ＨＮＩＤＳ内の侵入防止機能を提供する任を担うＨＮＩＤＳの別個の構成要素である。システムからかなりの期間パケットが送信されない場合、ＩＴＰＭはホストをオフラインにする。
【００５３】
別の実施形態
図１０は、サービスを装う能力を有するＨＮＩＤＳ１０００の機能ブロック図である。ＨＮＩＤＳ１０００は、アイドル時間処理モジュール１００１、スキャン・モジュール（ＳＭ）またはスキャン・デーモン（ＳＤ）１００２、および偽サービスデーモン（ＦＳＤ）１００３を含む。モジュール１００１、１００２、および１００３は、それ自体の特定の機能を有する独立なモジュールである。モジュール１００１および１００２は、図１に関して説明したのと同じものである。
【００５４】
ＦＳＤ１００３は、サービスを装うためのプログラム・コードを含む。フェークする必要があるサービスは構成可能である。構成する偽サービスに応じて、ＦＳＤ１００３は適切なハンドラを作成する。こうしたハンドラは、実際には、接続要求に関する適切なポートをリスンする偽デーモンである。こうしたデーモンは、完全なアプリケーションではないが、アタッカをだまし、関係する詳細を記録するための偽応答を生成するのに使用される。一例を挙げると、ＨＴＴＰサーバを偽サービスとして構成することができる。ＦＳＤ１００３は、偽ＨＴＴＰデーモンを作成し、偽ＨＴＴＰデーモンは、ＨＴＴＰポート（８０）上の接続要求をリスンする。接続要求がこのポート上に到着したとき、ソースＩＰアドレス、ハードウェア・アドレスなどの関連する詳細を記録し、（偽）応答を要求側ホストに送信する。
【００５５】
本発明の少数の実施形態を詳細に説明したが、その他の実施形態も可能である。
【００５６】
コンピュータ実装
本発明の実施形態はコンピュータを使用して実装することができる。具体的には、上記で説明し、図１～１０に示した処理または機能は、コンピュータ上で実行されるソフトウェアまたはコンピュータ・プログラムとして実装することができる。通信ネットワークにおける侵入を検出するための開示の方法またはプロセス・ステップは、コンピュータによって実施されるソフトウェア中の命令で実施される。同様に、通信ネットワークにおける侵入を防止するための開示の方法またはプロセス・ステップは、コンピュータで実施されるソフトウェア中の命令で実施することができる。ソフトウェアは、プロセス・ステップを実施するための１つまたは複数のモジュールとして実装することができる。モジュールは、特定の機能または関係する機能を通常は実施するコンピュータ・プログラムの一部である。さらに、モジュールは、他の構成要素またはモジュールと共に使用するためのパッケージ化機能ハードウェア・ユニットでよい。
【００５７】
具体的には、ソフトウェアは、以下で説明する記憶装置を含むコンピュータ可読媒体に格納することができる。ソフトウェアは、コンピュータ可読媒体からコンピュータにロードされ、次いでコンピュータによって実施されることが好ましい。コンピュータ・プログラム製品は、コンピュータ・プログラム製品によって実施することができる媒体上に記録されたこのようなソフトウェアまたはコンピュータ・プログラムを有するコンピュータ可読媒体を含む。好ましくは、コンピュータでのコンピュータ・プログラム製品の使用は、本発明の実施形態に従って通信ネットワークにおける侵入を検出する有利なシステムを実

施する。同様に、通信ネットワークにおける侵入を防止するシステムも実装することができる。

【００５８】

コンピュータ・システムは、モデム通信経路、コンピュータ・ネットワークなどの適切な通信チャネルを使用して、通信インターフェースを介して１つまたは複数の他のコンピュータに接続することができる。コンピュータ・ネットワークは、ローカル・エリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、イントラネット、またはインターネット、あるいはそれらの組合せを含むことができる。コンピュータは、中央演算処理装置（以下では単にプロセッサと呼ぶ）、ランダム・アクセス・メモリ（ＲＡＭ）および読取り専用メモリ（ＲＯＭ）を含むことができるメモリ、入出力（ＩＯ）インターフェース、ビデオ・インターフェース、および１つまたは複数の記憶装置を含むことができる。記憶装置は、フロッピィ・ディスク、ハード・ディスク・ドライブ、光磁気ディスク・ドライブ、ＣＤ－ＲＯＭ、ＤＶＤ、磁気テープ、または当業者にとって周知のその他のいくつかの不揮発性記憶装置のうち１つまたは複数を含むことができる。通信ネットワークにおける侵入を検出するプログラムは、そのような記憶装置上に記録することができ、コンピュータによってメモリ内に読み込むことができる。同じことが、このような侵入を防止するプログラムにも当てはまる。コンピュータの各構成要素は通常、バスを介して他の装置のうち１つまたは複数に接続される。バスは、データ・バス、アドレス・バス、および制御バスを含むことができる。プロセッサを使用するシステムを説明したが、本発明の範囲および精神から逸脱することなく、データを処理することができ、演算を実施することのできるその他の処理装置を代わりに使用できることを当業者は理解されよう。ＨＮＩＤＳ１００のアイドル時間処理モジュール１０２およびスキャン・モジュール１０１は、このようなコンピュータを使用して実装することができる。

【００５９】

記載のコンピュータ・システムは単に例示的目的で与えたに過ぎず、本発明の範囲および精神から逸脱することなく、その他の構成も利用することができる。実施形態を実施することができるコンピュータには、ＩＢＭ－ＰＣ／ＡＴまたはその互換機、ＰＣのMacintosh（商標）ファミリの１つ、Sun Sparcstation（商標）、ワークステーションなどが含まれる。上記は、本発明の実施形態を実施することができるコンピュータのタイプの単なる例に過ぎない。通常、以下で説明する実施形態のプロセスは、ハード・ディスク・ドライブ上にコンピュータ可読媒体として記録されたソフトウェアまたはプログラムとして常駐し、プロセッサを使用して読み取られ、制御される。プログラムおよび中間データおよびネットワークから取り出された任意のデータの中間記憶は、恐らくはハード・ディスク・ドライブと協働する半導体メモリを使用して実施される。

【００６０】

ある場合には、ＣＤ－ＲＯＭまたはフロッピィ・ディスク上に符号化されたコンピュータ・プログラムをユーザに供給することができ、あるいはコンピュータ・プログラムは、例えばコンピュータに接続されたモデム装置を介してユーザがネットワークから読み取ることもできる。さらに、ソフトウェアは、磁気テープ、ＲＯＭまたは集積回路、光磁気ディスク、コンピュータと他の装置間の無線／赤外線伝送チャネル、ＰＣＭＣＩＡカードなどのコンピュータ可読カード、Ｅメール送信やウェブ・サイト上に記録された情報を含むインターネットおよびイントラネットなどを含む他のコンピュータ可読媒体からコンピュータ・システムにロードすることもできる。上記は、関連するコンピュータ可読媒体の一例に過ぎない。本発明の範囲および精神から逸脱することなく、他のコンピュータ可読媒体も実施することができる。

【００６１】

上記のように、通信ネットワークにおける侵入を検出する方法、システム、およびコンピュータ・プログラム製品を開示した。さらに、通信ネットワークにおける侵入を防止する方法、システム、およびコンピュータ・プログラム製品も開示した。この詳細な説明は、単に好ましい例示的実施形態を与えたに過ぎず、本発明の範囲、適用可能性、または構

成、あるいはそれらの組合せを限定することを意図するものではない。むしろ、好ましい例示的実施形態の詳細な説明は、本発明の好ましい例示的実施形態を実施することができる説明を当業者に与えるものである。添付の特許請求の範囲に記載の本発明の範囲および精神から逸脱することなく、要素の機能および構成に様々な変更または置換あるいはその両方を行えることを理解されたい。

【図面の簡単な説明】

【００６２】

【図１】ホストベースのネットワーク侵入検出システム（ＨＮＩＤＳ）の機能ブロック図である。

【図２】図１のスキャン・モジュール（ＳＭ）の機能ブロック図である。

【図３】図１のスキャン・デーモン（ＳＤ）の機能ブロック図である。

【図４】プロトコル・スタックの上方に向かうパケットの通常の流れと、各層で行われる処理とを示す図である。

【図５】ＨＮＩＤＳがトランスポート層とアプリケーション層の間に位置する、プロトコル・スタックの上方に向かうパケットの通常の流れを示す図である。

【図６】図５の実施形態に関するプロセスを示す流れ図である。

【図７】図５と同様であるが、ＨＮＩＤＳがアプリケーション受信キュー（ＡＲＱ）を監視する図である。

【図８】図７に示す実施形態に関するプロセスを示す流れ図である。

【図９】図１のアイドル時間処理モジュール（ＩＴＰＭ）に関するプロセスを示す流れ図である。

【図１０】偽サービスを備えるＨＮＩＤＳの機能ブロック図である。

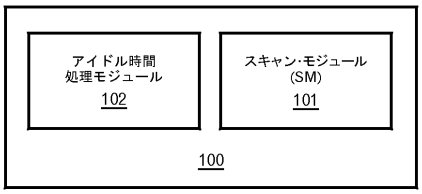
【符号の説明】

【００６３】

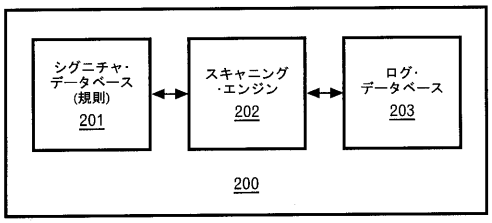
１００　ＨＮＩＤＳ
１０１　スキャン・モジュール（ＳＭ）
１０２　アイドル時間処理モジュール（ＩＴＰＭ）
２００　スキャン・モジュール（ＳＭ）
２０１　シグニチャ・データベース
２０２　スキャニング・エンジン
２０３　ログ・データベース
３００　スキャン・デーモン（ＳＤ）
３０２　プログラム・コード
３０２ａ　ＨＴＴＰ
３０２ｂ　ＦＴＰ
３０３　ログ・データベース
４００　プロトコル・スタック
４１０　物理媒体
４１２　リンク層
４１４　ネットワーク層処理
４１６　トランスポート層
４１８　アプリケーション受信キュー
４２０　アプリケーション層
５１０　物理媒体
５１２　リンク層
５１４　ネットワーク層
５１６　トランスポート層
５１８　ＡＲＱ
５２０　アプリケーション
５３０　ＨＮＩＤＳ

１０００　ＨＮＩＤＳ
１００１　アイドル時間処理モジュール
１００２　スキャン・モジュール（ＳＭ）またはスキャン・デーモン（ＳＤ）
１００３　偽サービスデーモン（ＦＳＤ）

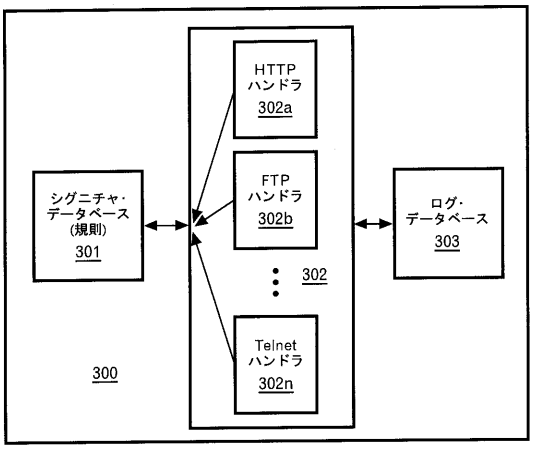
【図１】



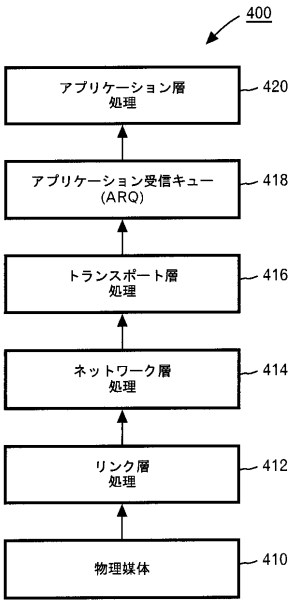
【図２】



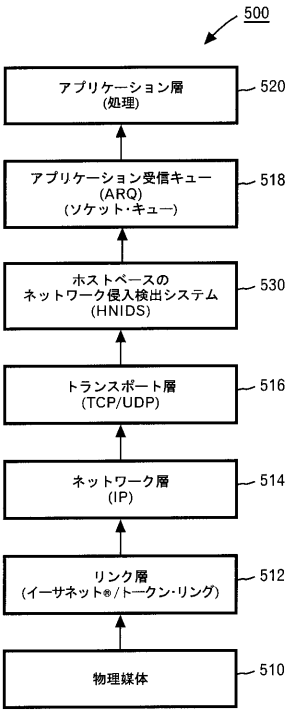
【図３】



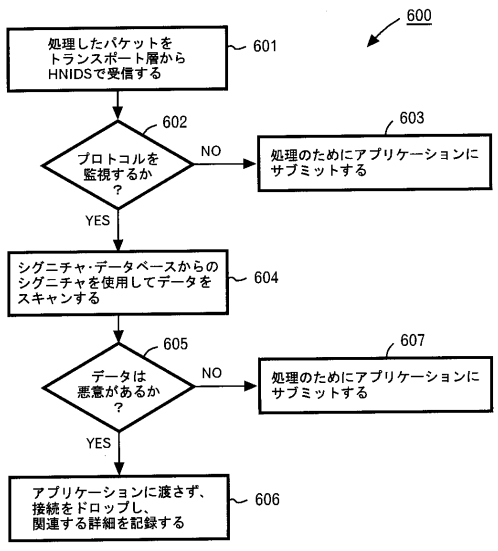
【図４】


400
アプリケーション層
処理
420
アプリケーション受信キュー
(ARQ)
418
トランスポート層
処理
416
ネットワーク層
処理
414
リンク層
処理
412
物理媒体
410

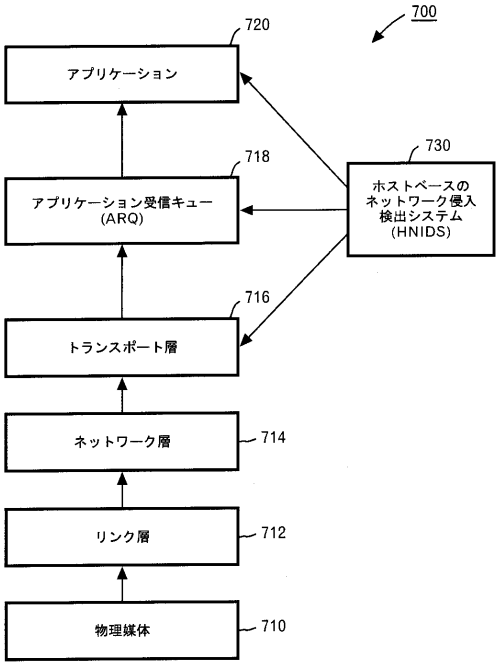
【図５】


500
アプリケーション層
(処理)
520
アプリケーション受信キュー
(ARQ)
(ソケット・キュー)
518
ホストベースの
ネットワーク侵入検出システム
(HNIDS)
530
トランスポート層
(TCP/UDP)
516
ネットワーク層
(IP)
514
リンク層
(イーサネット®/トークン・リング)
512
物理媒体
510

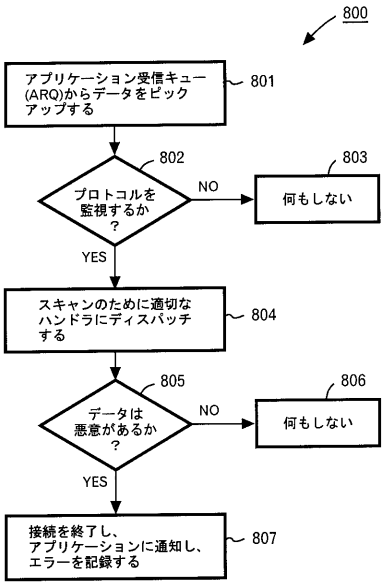
【図６】


600
処理したパケットを
トランスポート層から
HNIDSで受信する
601
プロトコルを
監視するか
?
602
NO
処理のためにアプリケーションに
サブミットする
603
YES
シグニチャ・データベースからの
シグニチャを使用してデータを
スキャンする
604
データは
悪意があるか
?
605
NO
処理のためにアプリケーションに
サブミットする
607
YES
アプリケーションに渡さず、
接続をドロップし、
関連する詳細を記録する
606

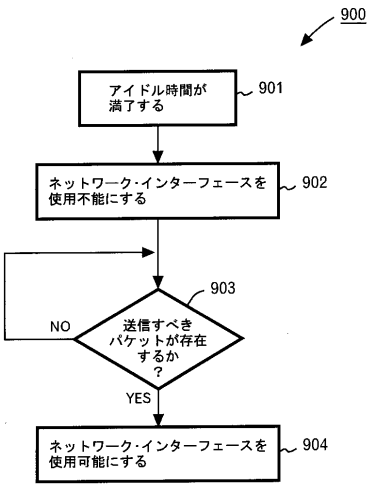
【図７】


700
720
アプリケーション
718
アプリケーション受信キュー
(ARQ)
730
ホストベースの
ネットワーク侵入
検出システム
(HNIDS)
716
トランスポート層
714
ネットワーク層
712
リンク層
710
物理媒体

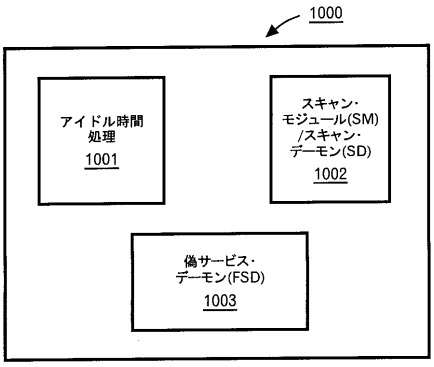
【図８】


800
アプリケーション受信キュー(ARQ)からデータをピックアップする
801
802
プロトコルを監視するか？
NO
803
何もしない
YES
スキャンのために適切なハンドラにディスパッチする
804
805
データは悪意があるか？
NO
806
何もしない
YES
接続を終了し、アプリケーションに通知し、エラーを記録する
807

【図９】


900
アイドル時間が満了する
901
ネットワーク・インターフェースを使用不能にする
902
903
NO
送信すべきパケットが存在するか？
YES
ネットワーク・インターフェースを使用可能にする
904

【図１０】


1000
アイドル時間処理
1001
スキャン・モジュール(SM)/スキャン・デーモン(SD)
1002
偽サービス・デーモン(FSD)
1003

フロントページの続き

(72)発明者　プラディプタ・クマル・バネルジー
インド　５６００１７　カルナータカ　バンガロール　フォース・クロス　ＨＡＬ　ＩＩＩ・ステージ　ハウスナンバー　２４５３
(72)発明者　アナント・ナラヤン・マヴィナカヤナハリー・グルラジャ
インド　５６００７０　バンガロール　パドマナバナガル　ラダ・クリシュナ・レイアウト・セカンド・ステージ　テンス・メイン　１４

審査官　田内　幸治

(56)参考文献　特開２００２－１１１７２７（ＪＰ，Ａ）
特開２００２－２５２６５４（ＪＰ，Ａ）
特開２００４－１０４７３９（ＪＰ，Ａ）
勝野　秀樹，新人管理者のためのセキュリティの基礎（応用編）　第3回　ＩＤＳ（侵入検知システム）の正しい使い方，日経オープンシステム，日本，日経ＢＰ社，２００２年１１月２６日，第１１６号，Ｐ．１７０～Ｐ．１７７
三宅　康夫，ワーム対策完全マニュアル，ＵＮＩＸ　ＵＳＥＲ，日本，ソフトバンクパブリッシング株式会社，２００２年　4月　1日，第１１巻第4号，Ｐ．４５～Ｐ．５０

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　１５／００
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　１２／６６