

(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2006-120138

(P2006-120138A)

(43) 公開日 平成18年5月11日(2006.5.11)

(51) Int. Cl.		F I			テーマコード (参考)
G06F 13/00	(2006.01)	G06F 13/00	351Z		5B089
G06F 21/20	(2006.01)	G06F 15/00	330A		5B285
H04M 3/00	(2006.01)	H04M 3/00	B		5K201

審査請求 有 請求項の数 20 O L (全 15 頁)

(21) 出願番号	特願2005-287464 (P2005-287464)	(71) 出願人	500500044
(22) 出願日	平成17年9月30日 (2005. 9. 30)		アバイア テクノロジー コーポレーショ ン
(31) 優先権主張番号	10/955, 594		アメリカ合衆国, 07920 ニュージャ ーシー, バスキング リッジ, マウント エアリー ロード 211
(32) 優先日	平成16年9月30日 (2004. 9. 30)	(74) 代理人	100064447
(33) 優先権主張国	米国 (US)		弁理士 岡部 正夫
		(74) 代理人	100085176
			弁理士 加藤 伸晃
		(74) 代理人	100094112
			弁理士 岡部 譲
		(74) 代理人	100096943
			弁理士 臼井 伸一

最終頁に続く

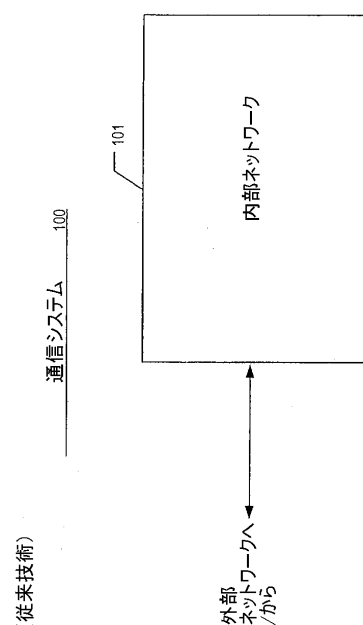
(54) 【発明の名称】 VoiceOver IP用のステートフルおよび相互プロトコルの侵入検知

(57) 【要約】

【課題】 2つ以上のプロトコルのメッセージを使用する侵入を検知する方法を提供すること。

【解決手段】 このような侵入はVoice over Internet Protocol (VoIP) システムだけでなく、2つ以上のプロトコルがVoIP以外の何らかのサービスをサポートするシステムでも発生しうる。本発明の例示されている実施形態では、ステートフルの侵入検知システムは、相互プロトコルの前提条件を持つルールを使用することができる。例示されている実施形態は、このようなルールを使用して、さまざまなVoIPベースの侵入の試みだけでなく、呼ハイジャック、BYE攻撃などを認識することができる。さらに、例示されている実施形態は、このようなルールを使用して、2つ以上のプロトコルがVoIP以外のサービスをサポートする他の種類の侵入の試みを認識することができる。例示されている実施形態は、さらに、相互プロトコルの前提条件とともにルールを使用することができるステートフルのファイアウォールも含む。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

データ処理システムにおいて、

(i) 第 1 のセッションの第 1 のプロトコルの状態と、

(i i) 第 2 のセッションの第 2 のプロトコルの状態と、に基づいて信号を発生する処理を含む方法であって、

前記第 1 のプロトコルは前記第 2 のプロトコルと異なることを特徴とする方法。

【請求項 2】

前記信号は、潜在的侵入を示す請求項 1 に記載の方法。

【請求項 3】

前記信号は、その後前記データ処理システムで受信されたメッセージが宛先に届くのをブロックされることを示す請求項 1 に記載の方法。

【請求項 4】

前記第 1 のプロトコルおよび前記第 2 のプロトコルは、アプリケーション層プロトコルである請求項 1 に記載の方法。

【請求項 5】

前記第 1 のプロトコルおよび前記第 2 のプロトコルは、サービスをサポートする請求項 1 に記載の方法。

【請求項 6】

前記サービスは、Voice over Internet Protocol である請求項 5 に記載の方法。

【請求項 7】

前記第 1 のセッションおよび前記第 2 のセッションは、1つの呼に属す請求項 1 に記載の方法。

【請求項 8】

(a) 第 1 のプロトコルに従うメッセージをデータ処理システムで受信する処理と、

(b) 前記データ処理システムにおいて、

(i) 前記メッセージと、

(i i) セッションの第 2 のプロトコルの状態とに基づき信号を発生する処理とを含み、

前記第 1 のプロトコルは前記第 2 のプロトコルと異なることを特徴とする方法。

【請求項 9】

前記信号は、潜在的侵入を示す請求項 8 に記載の方法。

【請求項 10】

前記信号は、

(i) 前記メッセージがその宛先に届くのをブロックされることと、

(i i) 前記データ処理システムでその後受信されるメッセージがその宛先に届くのをブロックされることのうちの少なくとも一方を示す請求項 8 に記載の方法。

【請求項 11】

前記第 1 のプロトコルおよび前記第 2 のプロトコルは、アプリケーション層プロトコルである請求項 8 に記載の方法。

【請求項 12】

前記第 1 のプロトコルおよび前記第 2 のプロトコルは、サービスをサポートする請求項 8 に記載の方法。

【請求項 13】

前記サービスは、Voice over Internet Protocol である請求項 12 に記載の方法。

【請求項 14】

(a) 前記データ処理システムにおいて、

(i) 第 1 のプロトコルに従う第 1 のメッセージと、

10

20

30

40

50

(i i) 前記第1のプロトコルと異なる第2のプロトコルに従う第2のメッセージを受信する処理と、

(b) 前記データ処理システムにおいて、前記第1のメッセージおよび前記第2のメッセージに基づいて信号を発生する処理とを含む方法。

【請求項15】

前記信号は、潜在的侵入を示す請求項14に記載の方法。

【請求項16】

前記信号は、

(i) 前記第1のメッセージがその宛先に届くのをブロックされることと、

(i i) 前記第2のメッセージがその宛先に届くのをブロックされることと、

10

(i i i) 前記データ処理システムでその後受信されるメッセージがその宛先に届くのをブロックされることのうちの少なくとも1つを示す請求項14に記載の方法。

【請求項17】

前記第1のプロトコルおよび前記第2のプロトコルは、アプリケーション層プロトコルである請求項14に記載の方法。

【請求項18】

前記第1のプロトコルおよび前記第2のプロトコルは、サービスをサポートする請求項14に記載の方法。

【請求項19】

前記サービスは、Voice over Internet Protocolである請求項18に記載の方法。

20

【請求項20】

前記第1のメッセージは、第1のセッションに属し、前記第2のメッセージは、第2のセッションに属し、前記第1のセッションおよび前記第2のセッションは1つのトランザクションに属す請求項18に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般に、通信システムに関するものであり、より具体的には、ネットワーク・セキュリティに関するものである。

30

【背景技術】

【0002】

侵入とは、無許可ユーザ（例えば、「ハッカー」など）がコンピュータ・システムに侵入したり、コンピュータ・システムを悪用しよう（例えば、機密データを盗もうと）試みることである。侵入検知システム（IDS）は、コンピュータ・システムに入ってくるメッセージおよびコンピュータ・システムから出て行くメッセージ（例えば、パケットなど）を監視し、それらのメッセージに基づき、侵入が試みられているかどうかを判別しようとする。侵入検知システムでは、不規則な、または不審なメッセージ・シーケンスが出現した場合、またはメッセージ・シーケンスが知られている「侵入シグネチャ」と一致した場合に、侵入試行が進行中であると結論することができる。

40

【0003】

図1は、従来技術による通信システム100の概略図を示している。図1に示されているように、通信システム100は、外部ネットワーク（例えば、インターネットなど）を介してメッセージを受信し、外部ネットワークを介してメッセージを外部データ処理システムに送信する、内部ネットワーク101（例えば、企業首都圏ネットワーク、住宅ローカル・エリア・ネットワークなど）を含む。

【0004】

図2は、従来技術による内部ネットワーク101の要素の概略図を示している。図2に示されているように、内部ネットワーク101は、侵入検知システム202、ファイヤウォール203、およびNを正の整数としてコンピュータ・システム204-1から204

50

—Nを含み、図のように相互接続されている。

【0005】

$n \in 1, 2, K, N$ の場合それぞれのコンピュータ・システム 204-n は、パーソナル・コンピュータ、サーバ、ラップトップ・コンピュータ、無線ローカル・エリア・ネットワーク通信機能を備えるパーソナル・デジタル・アシスタント (PDA) とすることが可能である。

【0006】

$n \in 1, 2, K, N$ としてコンピュータ・システム 204-n に向けられた入メッセージは、最初に、メッセージを検査し、メッセージを宛先に届かないようにブロックするか、またはルール集合内のいくつかのルールに基づいてメッセージを通すかを決定するファイヤウォール 203 を通る。ルールの実施例としては、ドメイン badguys.com からすべてのメッセージをブロックする、特定のプロトコルタイプのメッセージを除くすべてのメッセージをブロックする、などがある。

10

【0007】

ファイヤウォール 203 で、入メッセージを通す場合、侵入検知システム 202 は、その後、メッセージを受信して検査する。侵入検知システム 202 は、ファイヤウォール 203 を通ることを許可された 1 つまたは複数のメッセージを含む侵入の試みを検知することにより追加セキュリティ層を用意する。例えば、ファイヤウォール 203 は、内部ネットワーク 101 内の Web サーバへの外部アクセスをポート 80 に制限することが可能であるが、侵入検知システムがないと、Web サーバソフトウェア (ColdFusion、Apache など) のバグのせいでポート 80 を通る正当なトラフィックを介して Web サーバ自体を攻撃することが可能な場合がありうる。類推として、ファイヤウォール 203 は、内部ネットワーク 101 を囲む「フェンス」と機能する。フェンスは、セキュリティを実現するが、誰かが (例えば、地下トンネルなどを掘って) 押し入ろうとしたときにそのことを検知する機能を持たない。しかし、侵入検知システム 202 は、ファイヤウォール 203 が検知できないいくつかの押し入り試行を認識することができる。

20

【0008】

Voice over Internet Protocol (VoIP) システムは、回路交換電話網 (例えば、公衆交換電話網など) の代わりにパケット交換インターネット・プロトコル (IP) データ・ネットワーク上で音声トラフィックを伝送する。通常、Voice over Internet Protocol システムは、H323 および Session Initiation Protocol (SIP) の 2 つの主要なプロトコルのうちの 1 つに基づく。両方のタイプのシステムにおいて、起呼側および被呼側通信端末 (例えば、ヘッドホン、ソフトホンなど) での VoIP ユーザ・エージェントは、Real-time Transport Protocol (RTP) による符号化音声信号を含むパケットを送受信する。さらに、VoIP ゲートウェイは、Media Gateway Control Protocol (MGCP) または MGACO/H.248 などのメディア管理プロトコルを採用し、IP ベースのネットワークと非 IP ベースのネットワークとの間 (例えば PSTN 電話と IP 電話との間など) のトラフィックを透過的に翻訳することも可能である。

30

40

【0009】

VoIP の主要な利点は、音声およびデータ・ネットワークの集中が可能になるという点である。しかし、音声トラフィックをデータ・ネットワークに移行させると、音声ネットワークは、プライバシー、サービスの品質、および正確な請求書作成を損なう侵入および他の攻撃 (例えば、サービス拒否攻撃、認証攻撃など) に対し脆弱になる。さらに、Voice over Internet Protocol システムの特性により、従来技術のいくつかの侵入検知システムでは、VoIP パケットを採用する侵入 (つまり、VoIP ベースの侵入) を採用する不適切なセキュリティが用意される。

必要なのは、VoIP ベースの侵入の試みだけでなく、VoIP ベースの侵入と同じ特性のいくつかを示す他の種類のいくつかの侵入の試みを検知できる侵入検知システムであ

50

る。

【発明の開示】

【発明が解決しようとする課題】

【0010】

本発明は、Voice over Internet Protocolトラフィックの特定の特性がある種の侵入検知システムによるVoIPベースの侵入の試みの認識を困難にさせる可能性があるという観察結果に基づく。

【課題を解決するための手段】

【0011】

特に、例示されている実施形態は、(i) Voice over Internet Protocolは、複数のプロトコル（例えば、SIP、RTPなど）によりサポートされるサービスであり、(ii) それらのプロトコルのうちの2つ以上にまたがる特定のメッセージ・シーケンスを介してデータ処理システムを攻撃する可能性があるという事実に基づく。

【0012】

例えば、呼ハイジャックはVoIPベースの侵入の一種である。呼ハイジャックでは、攻撃者は、被呼端末でSIP REINVITEメッセージをVoIPユーザ・エージェントに送信する。通常、REINVITEメッセージは、呼移送（例えば、有線電話から携帯電話などに呼を転送する）のために送信される。しかし、第三者攻撃者により送信される悪意あるREINVITEメッセージは、被呼端末に送信されたRTPトラフィックを他の何らかの端末にリダイレクトすることができる。

【0013】

VoIPベースの侵入の他の例は、BYE攻撃と呼ばれるもので、完了しないうちに呼を終了させることを目標とする。BYE攻撃では、攻撃者は、見せかけのSIP BYEメッセージを、VoIP呼に現在関わっているユーザ・エージェントAに送信する。ユーザ・エージェントAは、BYEメッセージを受信した後、リモート・パーティのユーザ・エージェント（ユーザ・エージェントB）がその呼を終了したと結論する。したがって、ユーザ・エージェントAは、出RTPメッセージ・ストリームを即座に停止するが、ユーザ・エージェントBは、第三者BYEメッセージに気づかず、RTPメッセージをユーザ・エージェントAに送信し続ける。

【0014】

これらの実施例の両方において、侵入は、SIPおよびRTPの2つのアプリケーション層プロトコルのメッセージに基づく。このような侵入は、本発明の例示されている実施形態では、侵入検知システムのルール・ベースに適切な相互プロトコル・ルールを含めることによりブロックすることができる（つまり、2つ以上のプロトコルを対象とする前提条件を持つルール）。当業者であれば理解するように、上述の例示されているVoIPベースの侵入は、プロトコルSIPおよびRTPを伴うが、ある種のVoIPベースの侵入は、他のプロトコルの組み合わせに基づく可能性もある。例えば、いくつかのインスタント・メッセージング攻撃は、SIPおよびIPメッセージの組み合わせに基づく。

【0015】

当業者にとっては明らかであるように、本発明の例示されている実施形態では、相互プロトコル・ルールを使用して、Voice over Internet Protocol以外のサービスに基づく侵入から保護することができる。さらに、上で例示されているように、相互プロトコル侵入（VoIPベースかどうかに関係なく）は、アプリケーション層の下のプロトコル（例えば、インターネット・プロトコルなど）とともに、アプリケーション層プロトコル（例えば、SIP、RTPなど）を使用する可能性がある。

【0016】

相互プロトコル・ルールを許すことのほかに、例示されている実施形態の侵入検知システムはステートフルである（つまり、特定のセッション内のプロトコルの状態に基づく前提条件を持つルールを使用できる）。当業ではよく理解されているように、セッション内

10

20

30

40

50

の特定の時点のプロトコルの状態は、そのセッション内の先立つイベントに基づくようにできる（例えば、メッセージ、タイムアウトなど）。さらに、相互プロトコル侵入は、通常、何らかの形で相互関係付けられている2つ以上のセッション（例えば、SIPセッションおよびRTPセッションなど）を伴う（例えば、セッションは、同じ呼に属す、同じトランザクションに属す、など）。

【0017】

本発明の例示されている実施形態では、ファイヤウォールは、侵入検知システムのように、ステートフルであり、相互プロトコル・ルールを使用することができる。しかし、当業者であれば理解するように、本発明のいくつかの実施形態では、ファイヤウォールはステートフルでない場合があるか、または侵入検知システムに似た相互プロトコル・ルールを採用できない場合がある。

10

【0018】

例示されている実施形態は、(i)第1のセッションにおける第1のプロトコルの状態、および(ii)第2のセッションにおける第2のプロトコルの状態に基づき、データ処理システム側で信号を発生することを含むが、ただし、第1のプロトコルは第2のプロトコルと異なる。

【発明を実施するための最良の形態】

【0019】

図3は、本発明の例示されている実施形態による、内部ネットワーク301の要素の概略図を示している。図3に示されているように、内部ネットワーク301は、侵入検知システム302、ファイヤウォール303、およびNを正の整数としてコンピュータ・システム204-1から204-Nを含み、図のように相互接続されている。

20

【0020】

コンピュータ・システム204-1から204-Nは、本発明の例示されている実施形態により、従来技術から何ら変わっていない。したがって、本発明の実施形態を作成し、使用するうえで、コンピュータ・システム204のソフトウェア、ハードウェアなどに変更はいっさい必要ない。

【0021】

侵入検知システム302は、本発明の例示されている実施形態により、何らかの侵入の試みから内部ネットワーク301を保護することができる。特に、侵入検知システム302は、ルール・ベースにステートフルの相互プロトコル侵入シグネチャを格納することができ、また以下で、図4および5に関して説明されているように、それらのシグネチャのうちの1つまたは複数と一致する侵入の試みを認識することができる。

30

【0022】

ファイヤウォール303は、本発明の例示されている実施形態により、選択された入メッセージが内部ネットワーク301にさらに入り込まないように防止することができる。以下で、図6および7に関して説明されているように、ファイヤウォール303は、ルール・ベースにステートフルの相互プロトコル・ルールを格納することができ、またそれに応じてそれらのルールのうちの1つまたは複数に基づき入メッセージをブロックすることができる。

40

【0023】

当業者であれば理解するように、いくつかの実施形態では、侵入検知システム302およびファイヤウォール303の一方または両方は、さらに、内部ネットワーク301から出るメッセージを検査することも可能である。このような実施形態では、出メッセージはブロックされるか（例えば、ファイル転送プロトコル・セッションを開くためのメッセージなど）、または侵入アラートが、その出メッセージ（例えば、スプーフィングされた出VoIPメッセージなど）に基づいて生成するようにすることも可能である。

【0024】

さらに当業者であれば理解するように、いくつかの実施形態では、侵入検知システム302は、プロセッサおよびメモリを備えるハードウェアベースの「アプライアンス」とす

50

ることが可能であるが、他のいくつかの実施形態では、侵入検知システム302は、サーバ、パーソナル・コンピュータなどの上で実行されるプログラムとすることも可能である。同様に、いくつかの実施形態では、ファイヤウォール303は、プロセッサおよびメモリを備えるハードウェア・アプライアンスとすることが可能であるが、他のいくつかの実施形態では、ファイヤウォール303は、サーバ、パーソナル・コンピュータなどの上で実行されるプログラムとすることも可能である。当業者であればさらに理解するように、いくつかの実施形態では、侵入検知システム302およびファイヤウォール303は、単一のハードウェア・アプライアンスに属するか、または単一のプラットフォーム上で実行されるプログラムとすることが可能である。

【0025】

10

図4は、本発明の例示されている実施形態による、侵入検知システム302の論理的アーキテクチャを示す。図4に示されているように、侵入検知システム302は、メッセージ・プロセッサ410、状態生成器420、イベント生成器430、およびルール照合エンジン440の4つのプログラム・モジュール、およびトレイル・ヒストリ415、トレイル状態425、イベント・ヒストリ435、およびルール・ベース445の4つのデータを備える。入メッセージが侵入検知システム302に届いたときに発生する制御およびデータフロー・イベントのシーケンスは、図4では、イベント407、413、417、422、423、427、432、433、437、442、443、および447により表されている。

【0026】

20

侵入検知システム302に届く入メッセージ（データフロー・イベント407）は、メッセージ・プロセッサ410により受信される。メッセージ・プロセッサ410は、以下を行える。

(i) 適切なプロトコル（例えば、インターネット・プロトコルなど）による断片化および再組み立て、

(ii) プロトコル復号化、および

(iii) フットプリント（つまり、メッセージに関する情報）をトレイル・ヒストリ415に格納すること（データフロー・イベント413）。

【0027】

トレイル・ヒストリ415は、フットプリントを特定のセッション／プロトコルの組み合わせを表すトレイルに編成する（例えば、第1のSIPトレイル、第2のSIPトレイル、第1のRTPトレイルなど）。

【0028】

その後、制御は状態生成器420に渡る（制御イベント417）。状態生成器420は、更新されたトレイル・ヒストリ415を読み込み（データフロー・イベント422）、1つまたは複数のトレイル状態を発生し（例えば、既存のトレイルの状態を更新し、新規作成されたトレイルの状態を初期化する、など）、それに応じてトレイル状態425の中の情報を更新する（データフロー・イベント423）。

【0029】

その後、制御はイベント生成器430に渡る（制御イベント427）。イベント生成器430は、更新されたトレイル状態425を読み込み（データフロー・イベント432）、この情報に基づき1つまたは複数のイベントを発生する。イベントは、フットプリント内の情報の相関関係を求める抽象化の1つの層であり、その情報を単一の記述的エンティティに集中させる。イベントは、(i) ルール照合プロセス（後述）のいくつかの詳細を隠し、(ii) 入フットプリント毎にではなく注目する瞬間にルール照合をトリガし、それにより性能を改善できるという面があるため有利である。その後、イベント生成器は、それに応じて、イベント・ヒストリ435を更新し（データフロー・イベント423）を更新し、制御権がルール照合エンジン440に渡る（制御イベント437）。

【0030】

ルール照合エンジン440は、更新されたイベント・ヒストリ435（データフロー・

50

イベント 4 4 2) およびルール・ベース 4 4 5 (データフロー・イベント 4 4 3) をロードし、ルール・ベース 4 4 5 のルールと突き合わせて 1 つまたは複数のイベントの照合を試みる。例えば、ルール・ベース 4 4 5 は、以下のルールを含むことが可能である。

ユーザ・エージェント A からの S I P B Y E メッセージの後にユーザ・エージェント A からの R T P メッセージが受信された場合

呼ハイジャック侵入アラートを発生する

【0 0 3 1】

当業者にはよく知られているように、ルール・ベース内のルールを表現し、そのようなルールと突き合わせて情報 (例えば、論理述語、記号表現など) を照合する方法は多数ある。ルール照合エンジン 4 4 0 が照合ルールを見つけた場合、図 4 においてイベント 4 4 7 として表されている出力信号により示されているようにルールは「発火」される (例えば、侵入アラートが生成される、入メッセージがブロックされる、新しいルールがルール・ベース 4 4 5 に追加される、など)。照合ルールが見つからない場合、イベント 4 4 7 で、入メッセージは内部ネットワーク 3 0 1 の適切な宛先コンピュータ・システム 2 0 4 に出力される。(上述のように、いくつかの実施形態では、侵入検知システム 3 0 2 で受信されたメッセージは、実際には、内部ネットワーク 3 0 1 からの出メッセージである可能性があり、その場合、メッセージはイベント 4 4 7 でファイアウォール 3 0 3 に受け渡される。)

10

【0 0 3 2】

当業者であれば理解するように、侵入検知システム 3 0 2 のいくつかの実施形態では、知識表現の代替え方法を、例示されている実施形態のルール・ベース・システムの代わりに使用することができる。例えば、いくつかの実施形態では、決定木、ベイジアン推論ネットワーク、ニューラル・ネットワークなどを使用することが可能である。当業者であればさらに理解するように、本発明のいくつかの実施形態では、侵入検知システム 3 0 2 は、イベント単独の代わりに、イベント、トレイル状態、および個別のフットプリントの何らかの組み合わせに基づくルールを使用することが可能である。本明細書を読んだ後、そのような実施形態を作成し、使用する方法が当業者に明らかになるであろう。

20

図 5 は、侵入検知システム 3 0 2 の顕著なタスクを流れ図の形で示している。

【0 0 3 3】

タスク 5 1 0 で、プロトコル P に従うメッセージ M が、よく知られている方式で受信される。

30

タスク 5 2 0 は、(i) メッセージ M が属すセッションと (i i) プロトコル P との組み合わせに対応するトレイル・ヒストリ 4 1 5 内にすでにトレイルがあるかどうかをチェックする。もしあれば、実行はタスク 5 4 0 から続き、そうでなければ、実行はタスク 5 3 0 に進む。

【0 0 3 4】

タスク 5 3 0 で、上記の (i) と (i i) の組み合わせに対応する新しいトレイルがトレイル・ヒストリ 4 1 5 内に作成される。

タスク 5 4 0 で、メッセージ M に関する情報 (例えば、メッセージの送信者、メッセージの宛先、メッセージのタイプ、メッセージの内容など) が、トレイル・ヒストリ 4 1 5 の適切なトレイル内のフットプリントによく知られている方法で格納される。

40

【0 0 3 5】

タスク 5 5 0 で、トレイル・ヒストリ 4 1 5 内の各トレイルに対する更新された状態は、トレイル・ヒストリ 4 1 5 内の先立つ状態およびタスク 5 4 0 の追加されたフットプリントに基づいて、よく知られている方法により生成される (例えば、状態遷移図などを介して)。

タスク 5 6 0 で、イベント E は、トレイル・ヒストリ 4 1 5 の更新されたトレイル状態に基づいて生成され、イベント・ヒストリ 4 3 5 に格納される。当業者であれば理解するように、タスク 5 6 0 は、状態遷移の円弧を出力イベントに関連付けるなどのさまざまな方法により遂行することができる。

50

【0036】

タスク570では、ルール・ベース445内のルールの侵入シグネチャが、新規生成されたイベントEを含むイベント・ヒストリ435のイベントと一致するかどうかをチェックする。一致する場合、実行はタスク580に進み、一致しない場合、実行はタスク595から続く。

【0037】

タスク580では、タスク570で一致したルールに従って、アラートが発行されるか、またはアクションが実行されるか、またはその両方が実行される。

タスク590では、メッセージMがブロックされる（つまり、侵入検知システム302から出ないようにされる）かどうかをチェックする。もしそうであれば、実行はタスク510に戻って続行し、そうでなければ、実行はタスク595から続く。

タスク595で、メッセージMは、よく知られている方法で、侵入検知システム302から出力される。タスク595の後、実行はタスク510に戻って継続する。

【0038】

図6は、本発明の例示されている実施形態による、ファイヤウォール303の論理的アーキテクチャを示す。図6に示されているように、ファイヤウォール303は、メッセージ・プロセッサ610、状態生成器620、およびルール照合エンジン630の3つのプログラム・モジュール、およびトレイル・ヒストリ615、トレイル状態625、およびルール・ベース645の3つのデータを備える。入メッセージがファイヤウォール303に届いたときに発生する制御およびデータフロー・イベントのシーケンスは、図6では、イベント607、613、617、622、623、627、642、643、および647により表されている。

【0039】

ファイヤウォール303に届く入メッセージ（データフロー・イベント607）は、メッセージ・プロセッサ610により受信される。メッセージ・プロセッサ610は、以下を行える。

(i) 適切なプロトコル（例えば、インターネット・プロトコルなど）による断片化および再組み立て、

(ii) プロトコル復号化、および

(iii) メッセージに対するフットプリントをトレイル・ヒストリ615に格納すること（データフロー・イベント613）。

【0040】

その後、制御は状態生成器620に渡る（制御イベント617）。状態生成器620は、更新されたトレイル・ヒストリ615（データフロー・イベント622）を読み込み、1つまたは複数のトレイル状態を生成し、それに応じてトレイル状態625内の情報を更新する（データフロー・イベント623）。

【0041】

その後、制御はルール照合エンジン640に渡る（制御イベント627）。ルール照合エンジン640は、トレイル状態625（データフロー・イベント642）およびルール・ベース645（データフロー・イベント643）をロードし、ルール・ベース645のルールと突き合わせて1つまたは複数のイベントの照合を試みる。当業者にはよく知られているように、ルール・ベース内のルールを表現し、そのようなルールと突き合わせて情報（例えば、論理述語、記号表現など）を照合する方法は多数ある。ルール照合エンジン640が照合ルールを見つけた場合、図6においてイベント647として表されている出力信号により示されているようにルールは「発火」される（例えば、侵入アラートが生成される、入メッセージがブロックされる、新しいルールがルール・ベース645に追加される、など）。照合ルールが見つからない場合、イベント647で、入メッセージは侵入検知システム302に出力される。（上述のように、いくつかの実施形態では、ファイヤウォール303で受信されたメッセージは、実際には、侵入検知システム302が調査後ファイヤウォール303に転送した内部ネットワーク301からの出メッセージである可

能性がある。そのような場合、メッセージは外部ネットワークを介してその宛先に送信される。))

【0042】

当業者であれば理解するように、ファイヤウォール303のいくつかの実施形態では、知識表現の代替え方法を、例示されている実施形態のルール・ベース・システムの代わりに使用することが可能である。例えば、いくつかの実施形態では、決定木、ベイジアン推論ネットワーク、ニューラル・ネットワークなどを使用することが可能である。当業者であればさらに理解するように、本発明のいくつかの実施形態では、ファイヤウォール303は、侵入検知システム202の例示されている実施形態の場合のように、トレイル状態の代わりの、またはトレイル状態と組み合わせたイベントに基づくルールを使用することが可能である。本明細書を読んだ後、そのような実施形態を作成し、使用方法が当業者に明らかになるであろう。

10

【0043】

図7は、本発明の例示されている実施形態による、ファイヤウォール303の顕著なタスクの流れ図である。

タスク710で、プロトコルPに従うメッセージMが、よく知られている方式で受信される。

タスク720は、(i)メッセージMが属すセッションと(ii)プロトコルPとの組み合わせに対応するトレイル・ヒストリ615内にすでにトレイルがあるかどうかをチェックする。もしあれば、実行はタスク740から続き、そうでなければ、実行はタスク730に進む。

20

【0044】

タスク730で、上記の(i)と(ii)の組み合わせに対応する新しいトレイルがトレイル・ヒストリ615内に作成される。

タスク740で、メッセージMに関する情報(例えば、メッセージの送信者、メッセージの宛先、メッセージのタイプ、メッセージの内容など)が、トレイル・ヒストリ615の適切なトレイル内のフットプリントによく知られている方法で格納される。

【0045】

タスク750で、トレイル・ヒストリ615内の各トレイルに対する更新された状態は、トレイル・ヒストリ615内の先立つ状態およびタスク740の追加されたフットプリントに基づいて、よく知られている方法により生成される(例えば、状態遷移図などを介して)。

30

【0046】

タスク770で、トレイル状態およびルール・ベース645に基づいて、メッセージMがファイヤウォール303を通過することを許されるかどうかをチェックする。許可される場合、実行はタスク780に進み、許可されない場合、実行はタスク795から続く。

タスク780で、メッセージMがブロックされたという指示は、よく知られた方法でログに記録される。タスク780の後、実行はタスク710に戻って継続する。

タスク795で、メッセージMは、よく知られている方法で、ファイヤウォール303から出力される。タスク795の後、実行はタスク710に戻って継続する。

40

【0047】

図8は、本発明の例示されている第2の実施形態による、内部ネットワーク301の要素の概略図を示している。この第2の例示されている実施形態では、第1の例示されている実施形態における侵入検知システム302の機能は、メッセージ・プロセッサ801、侵入検知システム802、およびメッセージ・プロセッサ804-1から804-Nに分散される。

【0048】

侵入検知システム802の論理アーキテクチャは、メッセージ・プロセッサ410がないことを除き、侵入検知システム302(つまり、図4)のと同様している。メッセージ・プロセッサ410の機能は、メッセージ・プロセッサ801およびメッセージ・プロセ

50

ッサ 804-1 から 804-N が代わって実行する。メッセージ・プロセッサ 801 およびメッセージ・プロセッサ 804-1 から 804-N（つまり、フットプリント）の出力は侵入検知システム 802 に送信され、侵入検知システム 302 の残りの機能（つまり、状態生成器 420、イベント生成器 430、およびルール照合エンジン 440）が実行される。

【0049】

第2の例示されている実施形態の利点は、内部ネットワーク 301 全体にメッセージ処理を分散させることにより、内部通信（例えば、2つのコンピュータ・システム 204-i と 204-j との間の V o I P 呼など）に対する攻撃を検出することができることにある。しかし、第2の例示されている実施形態の欠点は、分散アーキテクチャを展開し維持することがますます複雑化することである。さらに、第2の例示されている実施形態で複数のメッセージ・プロセッサを拡散させることにより、ハードウェアのコストがかなり高くなる可能性がある。当業者には、第2の例示されている実施形態のメッセージ・プロセッサ 801、侵入検知システム 802、およびメッセージ・プロセッサ 804-1 から 804-N を作成し、使用方法が明らかであろう。

10

【0050】

上述の実施形態は、単に本発明を例示しているだけであり、当業者であれば、上述の実施形態の多くの変更形態を、本発明の範囲から逸脱することなく考案できることは理解されるであろう。例えば、本明細書では、本発明の例示されている実施形態を完全に説明し、理解できるようにするために、多数の具体的詳細を述べている。ただし、当業者であれば、本発明は、特定の詳細の1つまたは複数を使用せずに、または他の方法、材料、コンポーネントなどを使用して、実践できることを理解するであろう。

20

【0051】

さらに、いくつかの場合には、例示されている実施形態の態様をわかりにくくしないため、よく知られている構造、材料、またはオペレーションについては、示されていないか、または詳述されていない。図に示されているさまざまな実施形態は例示するものであり、必ずしもスケール通りに描かれていないことも理解されるであろう。「一実施形態」または「いくつかの実施形態」と記述されている場合、これは、（複数の）実施形態に関して説明されている特定の機能、構造、材料、または特性は、本発明の少なくとも一実施形態に含まれるが、必ずしもすべての実施形態に含まれるわけではないことを意味する。したがって、「一実施形態では」または「いくつかの実施形態では」という語句が明細書のさまざまな箇所に記載されていても、必ずしもすべて同じ実施形態を参照しているとは限らない。さらに、特定の機能、構造、材料、または特性は、1つまたは複数の実施形態において、適当な方法により組み合わせることができる。したがって、このような変更形態は、請求項およびその等価物の範囲内に含まれることが意図される。

30

【図面の簡単な説明】

【0052】

【図1】従来技術による通信システムを示す概略図である。

【図2】従来技術による、図1に示されているような、内部ネットワーク 101 の要素を示す概略図である。

40

【図3】本発明の例示されている実施形態による、内部ネットワークの要素を示す概略図である。

【図4】本発明の例示されている実施形態による、図3に示されているような、侵入検知システム 302 の論理的アーキテクチャを示す図である。

【図5】本発明の例示されている実施形態による、侵入検知システム 302 の顕著なタスクの流れ図である。

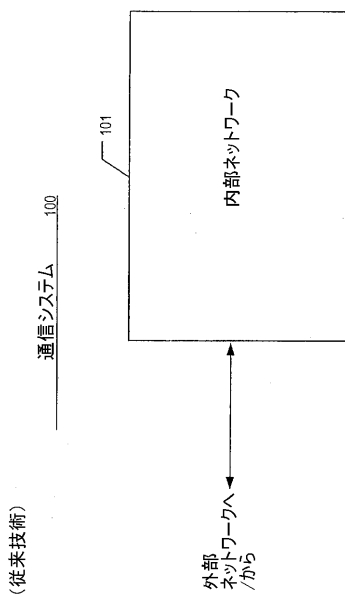
【図6】本発明の例示されている実施形態による、図3に示されているような、ファイヤウォール 303 の論理的アーキテクチャを示す図である。

【図7】本発明の例示されている実施形態による、ファイヤウォール 303 の顕著なタスクの流れ図である。

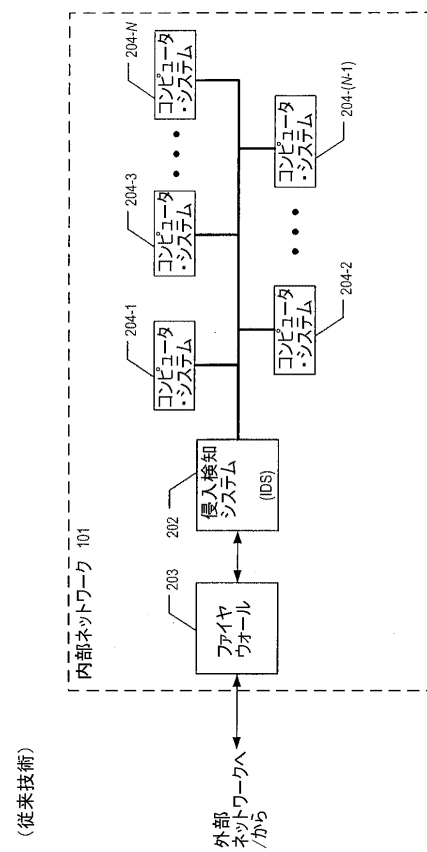
50

【図 8】 本発明の例示されている実施形態による、図 3 に示されているような、内部ネットワーク 301 の要素を示す概略図である。

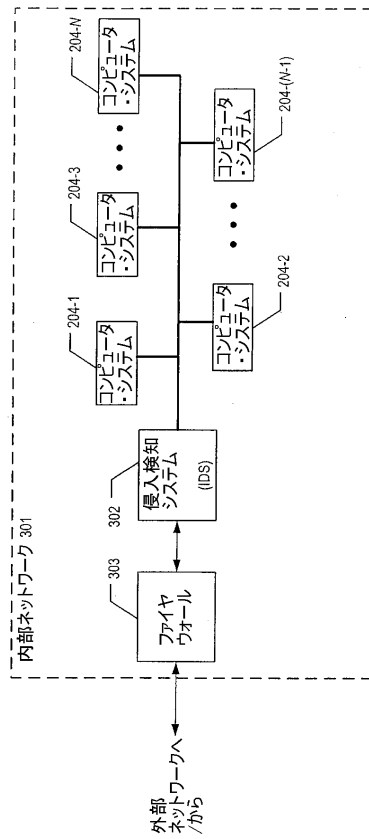
【図 1】



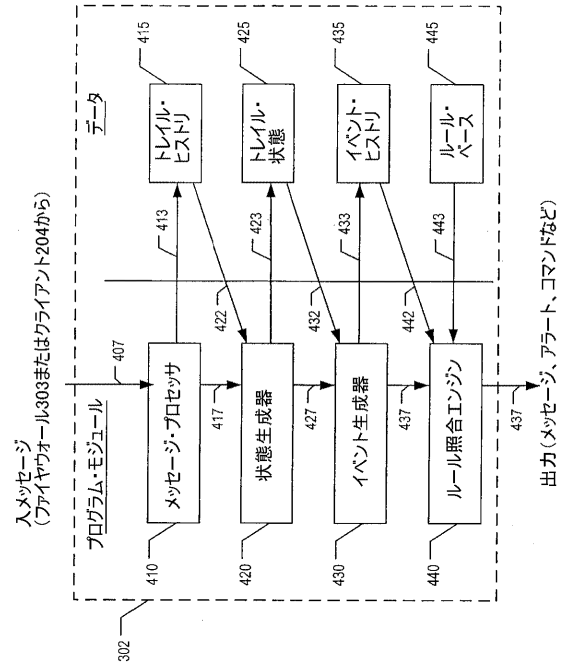
【図 2】



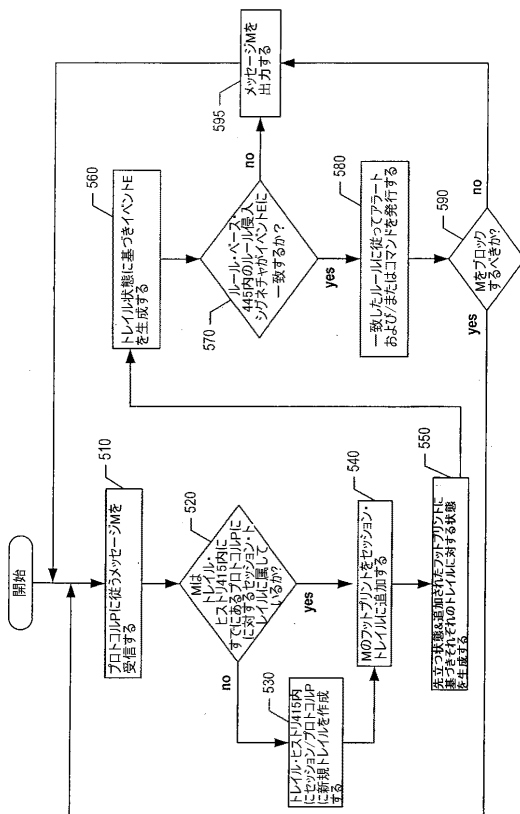
【図 3】



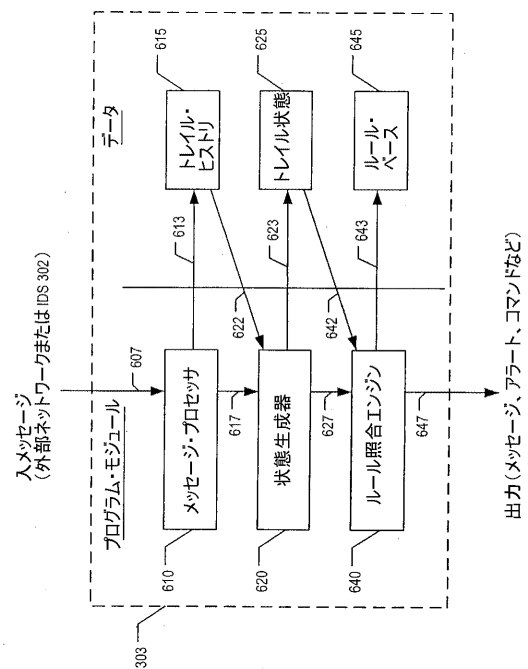
【図 4】



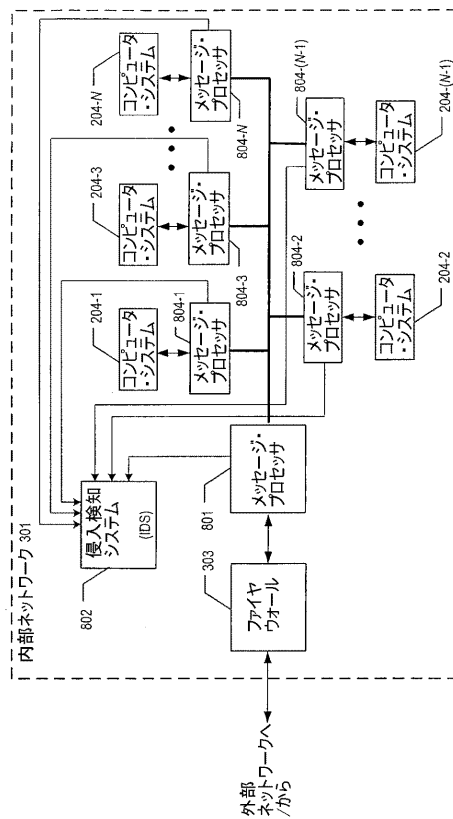
【図 5】



【図 6】



【図 8】



フロントページの続き

- (74)代理人 100101498
弁理士 越智 隆夫
- (74)代理人 100096688
弁理士 本宮 照久
- (74)代理人 100104352
弁理士 朝日 伸光
- (74)代理人 100128657
弁理士 三山 勝巳
- (72)発明者 サチン ガーグ
アメリカ合衆国 08812 ニュージャージー, グリーン ブルーク, シャドウラウン ドライ
ヴ 1033
- (72)発明者 ナブヨット サイン
アメリカ合衆国 07834 ニュージャージー, デンヴィーレ, マウント プリーセント ター
ンパイケ 33
- (72)発明者 ティモシー コーチー ツサイ
アメリカ合衆国 95002 カリフォルニア, アルビソ, アーチエンジェル ドライヴ 510
2
- (72)発明者 ユーサン ウー
アメリカ合衆国 47906 インディアナ, ウェスト ラフェイット, ピーチリーフ ドライヴ
2769
- (72)発明者 サラブー バグチ
アメリカ合衆国 47909 インディアナ, ラフェイット, エグレス ウエイ ドライヴ 31
72, アpartment 1742
- Fターム(参考) 5B089 JA40 JB14 KA17 KB13
5B285 AA04 AA06 BA01 DA05
5K201 AA07 BC23 CD07 EA05