(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6356871号
(P6356871)
(45)発行日　平成30年7月11日(2018.7.11)　(24)登録日　平成30年6月22日(2018.6.22)

(51)Int.Cl.　F I
H04L 12/70 (2013.01)　H04L 12/70 100Z

請求項の数 1　(全 37 頁)

(21)出願番号	特願2017-103072 (P2017-103072)	(73)特許権者	000004226 日本電信電話株式会社 東京都千代田区大手町一丁目５番１号
(22)出願日	平成29年5月24日 (2017.5.24)	(73)特許権者	515130201 株式会社Ｐｒｅｆｅｒｒｅｄ　Ｎｅｔｗｏｒｋｓ 東京都千代田区大手町１丁目６番１号　大手町ビル２階
(62)分割の表示	特願2016-529415 (P2016-529415)の分割	(74)代理人	110002147 特許業務法人酒井国際特許事務所
原出願日	平成27年6月17日 (2015.6.17)	(72)発明者	濱田　貴広 東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(65)公開番号	特開2017-143583 (P2017-143583A)		
(43)公開日	平成29年8月17日 (2017.8.17)		
審査請求日	平成29年5月24日 (2017.5.24)		
(31)優先権主張番号	特願2014-125403 (P2014-125403)		
(32)優先日	平成26年6月18日 (2014.6.18)		
(33)優先権主張国	日本国(JP)		

最終頁に続く

(54)【発明の名称】ネットワークシステム

(57)【特許請求の範囲】
【請求項１】
通信装置と、ネットワークを介して前記通信装置と通信する制御装置とを備えたネットワークシステムであって、
前記通信装置は、
該通信装置を経由する通信を制御する通信制御部と、
前記通信に関する情報のうち、一部の情報を部分情報として構成して前記制御装置に送信する収集部と、
を備え、
前記制御装置は、
前記通信装置から受信した部分情報を用いて分析して前記通信に異常があるか否かを判断する分析部と、
前記分析部によって前記通信に異常があると判断された場合には、前記通信が前記通信装置から前記制御装置へ送信されるよう、前記通信制御部に対して通信経路を制御する制御判断部と、
通信経路の制御により送信されてきた通信が悪性の通信であるか否かを判定する解析部と、
を備えたことを特徴とし、
前記制御判断部は、
さらに、前記解析部によって前記通信が悪性の通信であると判定された場合には、前記

通信制御部に対して該悪性の通信を制限するよう制御し、
前記制御装置は、
前記部分情報を基にして生成される特徴空間を示す情報であって、前記分析部が行う分析に適用されるモデル情報を記憶する記憶部をさらに備え、
前記分析部は、さらに、複数の通信装置の各々を経由する通信に対応するモデル情報を共有して構成される共有モデル情報を前記記憶部に記憶させ、前記共有モデル情報を用いて、前記通信に異常があるか否かを判断する
ことを特徴とするネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークシステム、制御装置、通信装置、通信制御方法および通信制御プログラムに関する。
【背景技術】
【０００２】
近年、ネットワークを介した攻撃の手法が高度化し、従来の事前防御によるセキュリティ対策では対処が困難になってきている。高性能・高機能のセキュリティ機器によりこれらの攻撃手法に対処しようとしているが、機器の費用や運用・管理の手間を考慮すると一般のユーザ宅や中小企業への導入が難しい。このため、安価な機器の導入で高度なセキュリティ対策を実現することが望ましいが、そのような機器では性能・機能が限られている。
【０００３】
例えば、ホームＮＷ（Network）や中小の企業ＮＷ等のユーザＮＷには、最小限の機能を備える安価な機器のみを導入し、この機器とユーザＮＷの外部にある機能とが連携することで高度なセキュリティ対策を実現すること、つまりユーザＮＷのセキュリティのアウトソースが期待される。
【０００４】
例えば、セキュリティ対策として、ユーザＮＷと外部ＮＷとの間の通信トラフィック（通信パケット、通信フローも含む）全てをインターネット上のデータセンタなどに配置される外部機能を経由またはミラーリングさせることで、外部機能でユーザＮＷの通信トラフィックをもれなく監視する技術が考えられる。また、例えば、ユーザＮＷのトラフィックをサンプリングしてデータセンタなどに配置されている外部機能へ送信して異常検知する技術がある。
【０００５】
また、例えば、ユーザＮＷの外部でユーザＮＷから流れてくる通信トラフィックをＩＤＳ（Intrusion Detection System）にかけて宛先のアプリケーションサーバ（ＡＰサーバ）への不正通信であるか否かを判定して管理者へ通知する技術がある（例えば、特許文献１参照）。具体的には、特定のＡＰサーバへの不正アクセスが疑われる通信を、当該ＡＰサーバを担当するＩＳＰ（Internet Services Provider）内のＩＤＳを備えるパケット転送装置へ割り振り、そこで悪性と判定された場合は管理者へ通知する。これにより、転送装置は任意のＡＰサーバへの通信ではなく特定のサーバへの通信に特化してＩＤＳ処理を実現できるため、処理負荷が低減される。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００９－１１７９２９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、上記の従来技術では、ユーザ回線の帯域を圧迫することなく、また、精

度を低下させることなく、悪性通信を検知して、ユーザ通信を適切に保護することができないという課題があった。つまり、上記の通信トラフィック全てを監視する技術は、帯域が圧迫されるという問題があった。また、上記の全ての通信トラフィックを対象とせず、単純にサンプリングして異常検知するする技術では、精度が低下するという問題があった。

【０００８】

また、特定のＡＰサーバへの不正アクセスが疑われる通信トラフィックを、当該サーバが属するサービスプロバイダ（ISP、MSSP（Managed Security Service Provider）等）のＩＤＳに転送して悪性を判定する技術では、保護の対象がＡＰサーバのため、ユーザネットワークの通信が保護できないという問題点があった。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するために、本発明のネットワークシステムは、通信装置と、ネットワークを介して前記通信装置と通信する制御装置とを備えたネットワークシステムであって、前記通信装置は、該通信装置を経由する通信を制御する通信制御部と、前記通信に関する情報のうち、一部の情報を部分情報として構成して前記制御装置に送信する収集部と、を備え、前記制御装置は、前記通信装置から受信した部分情報を用いて分析して前記通信に異常があるか否かを判断する分析部と、前記分析部によって前記通信に異常があると判断された場合には、前記通信が前記通信装置から前記制御装置へ送信されるよう、前記通信制御部に対して通信経路を制御する制御判断部と、通信経路の制御により送信されてきた通信が悪性の通信であるか否かを判定する解析部と、を備えたことを特徴とし、前記制御判断部は、さらに、前記解析部によって前記通信が悪性の通信であると判定された場合には、前記通信制御部に対して該悪性の通信を制限するよう制御し、前記制御装置は、前記部分情報を基にして生成される特徴空間を示す情報であって、前記分析部が行う分析に適用されるモデル情報を記憶する記憶部をさらに備え、前記分析部は、さらに、複数の通信装置の各々を経由する通信に対応するモデル情報を共有して構成される共有モデル情報を前記記憶部に記憶させ、前記共有モデル情報を用いて、前記通信に異常があるか否かを判断することを特徴とする。

【発明の効果】

【００１０】

本発明によれば、ユーザネットワークの回線の帯域の圧迫や異常・悪性通信の検知に関する精度の低下を抑えて、悪性通信を検知して、ユーザネットワークの通信を適切に保護することができるという効果を奏する。

【図面の簡単な説明】

【００１１】

【図１】図１は、第一の実施の形態に係るネットワークシステムの構成を示す図である。

【図２】図２は、第一の実施の形態に係る通信装置の構成を示すブロック図である。

【図３】図３は、第一の実施の形態に係る制御装置の構成を示すブロック図である。

【図４】図４は、通信モードの遷移について説明する図である。

【図５】図５は、第一の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。

【図６】図６は、第一の実施の形態に係るネットワークシステムにおける通信制御処理の流れを示すシーケンス図である。

【図７】図７は、第一の実施の形態に係る収集装置における収集処理の流れを示すフローチャートである。

【図８】図８は、第一の実施の形態に係る制御装置の通常モードにおける通信制御処理の流れを示すフローチャートである。

【図９】図９は、第一の実施の形態に係る制御装置のミラーリングモードにおける通信制御処理の流れを示すフローチャートである。

【図１０】図１０は、第一の実施の形態に係る制御装置のインラインモードにおける通信

制御処理の流れを示すフローチャートである。
【図１１】図１１は、第二の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。
【図１２】図１２は、特徴ベクトル空間へのマッピングの概念図である。
【図１３】図１３は、異常判定処理に用いられる判定基準の一例を示す図である。
【図１４】図１４は、第二の実施の形態に係るネットワークシステムにおける通信制御処理の流れを示すシーケンス図である。
【図１５】図１５は、第二の実施の形態に係る制御装置の通常モードにおける通信制御処理の流れを示すフローチャートである。
【図１６】図１６は、第三の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。
【図１７】図１７は、第三の実施の形態に係るネットワークシステムにおける通信制御処理の流れを示すシーケンス図である。
【図１８】図１８は、第三の実施の形態に係る収集装置における収集処理の流れを示すフローチャートである。
【図１９】図１９は、第四の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。
【図２０】図２０は、集合の類似度の求め方を説明する図である。
【図２１】図２１は、第五の実施の形態に係るネットワークシステムにおいてミラーリングモードの際の通信制御処理の一連の流れを説明する図である。
【図２２】図２２は、第五の実施の形態に係るネットワークシステムにおいてインラインモードの際の通信制御処理の一連の流れを説明する図である。
【図２３】図２３は、第六の実施の形態に係るネットワークシステムにおける通信制御処理の一連の流れを説明する図である。
【図２４】図２４は、第六の実施の形態に係るアノマリ情報蓄積部に記憶される情報の一例を示す図である。
【図２５】図２５は、第六の実施の形態に係る通信制御装置が有するフローテーブルの一例を示す図である。
【図２６】図２６は、通信制御プログラムを実行するコンピュータを示す図である。
【発明を実施するための形態】
【００１２】
以下に、本願に係るネットワークシステム、制御装置、通信装置、通信制御方法および通信制御プログラムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態により本願に係るネットワークシステム、制御装置、通信装置、通信制御方法および通信制御プログラムが限定されるものではない。
【００１３】
［第一の実施の形態］
以下の実施の形態では、第一の実施の形態に係るネットワークシステムの構成、通信装置の構成、制御装置の構成、ネットワークシステムの全体の処理の流れ、通信装置および制御装置それぞれの処理の流れを順に説明し、最後に第一の実施の形態による効果を説明する。
【００１４】
［ネットワークシステムの構成］
図１は、第一の実施の形態に係るネットワークシステムの構成を示す図である。図１に示すネットワークシステム１００では、ユーザＮＷ３０内に設置された通信装置１０と、ユーザＮＷ３０の外に設置された制御装置２０とを有する。通信装置１０と制御装置２０とは、外部ＮＷ６０を介して接続される。
【００１５】
図１に示すように、通信装置１０の配置場所は、ユーザＮＷ３０側である。例えば、通信装置１０は、ユーザＮＷ３０側のインターネット通信するための外縁ルータに組込まれ

てもよいし、外縁ルータとユーザＮＷ３０内におけるＰＣなどの端末４０との間に置かれてもよい。後者の場合は、インライン型（トランスペアレント型）の接続となる。つまり、通信装置１０を経由する通信、またはその一部が処理の対象となる。また、通信装置１０は、収集装置１１と通信制御装置１２とから構成される。

【００１６】

収集装置１１は、ユーザＮＷ３０を流れて通信装置１０を経由する通信トラフィックの一部を収集して、通信トラフィックの部分情報として制御装置２０の収集管理装置２１に送信する。なお、収集装置１１は、収集した通信トラフィックの一部をそのまま収集管理装置２１に送信してもよいし、収集した通信トラフィックの一部のさらにその一部のみを部分情報として送信してもよいし、もしくは、集約または統計化した情報を通信トラフィックの部分情報として外部に送信してもよい。

【００１７】

通信制御装置１２は、制御装置２０から受けた制御命令にしたがって通信トラフィックを制御する。なお、後に詳述するが、通信トラフィックの制御処理として、通信モードの変更に伴う通信モード制御とセキュリティ制御（パケットフィルタリングなど）とがある。

【００１８】

制御装置２０の配置場所は、ユーザＮＷ３０の外部であって、制御ＮＷ７０側である。例えば、制御装置２０は、通信キャリアＮＷやＩＳＰのＮＷ、インターネット上のデータセンタに設置される。また、制御装置２０は、収集管理装置２１、分析装置２２、制御判断装置２３、解析装置２４、および、通信制御装置２５の５つの装置で構成される。なお、制御装置２０を一つの装置とし、収集管理装置２１、分析装置２２、制御判断装置２３、解析装置２４、および、通信制御装置２５それぞれの機能を一台で有してもよい。

【００１９】

収集管理装置２１は、収集装置１１から送信される部分情報を収集し、分析装置２２へ送信する。

【００２０】

分析装置２２は、収集管理装置２１から受信した部分情報に対して、例えば、機械学習の異常検知などによる分析を行い、その分析結果を制御判断装置２３に出力する。また分析結果を機械学習のモデル情報として記憶して以降の分析に適用する。入力として受け付けた部分情報を用いて構成される特徴ベクトルとモデル情報（たとえば、特徴ベクトル群で構成される、特徴ベクトル群を集約して構成される、特徴ベクトル空間または特徴空間など）を用いて分析し、この特徴ベクトルが異常であるか否かを分析結果として出力する。さらに、機械学習することで、この特徴ベクトルをモデル情報に反映することで更新させて以降の分析の精度を向上させる。

【００２１】

制御判断装置２３は、分析装置２２から受けた分析結果を基に通信モードを決定し、各通信制御装置１２、２５へ通信モードに従った通信モード制御を行うよう命令する。また、制御判断装置２３は、解析装置２４から受けた解析結果を基に通信モードやセキュリティ制御の内容を決定し、各通信制御装置１２、２５へこれらの決定に従った通信制御を行うよう命令する。

【００２２】

解析装置２４は、受信する通信トラフィックに対して深い解析を行い、マルウェア等に感染した悪性通信であるか否かを判定して判定結果を制御判断装置２３に出力する。例えば、解析装置２４は、悪性である「黒」、悪性ではない「白」、白黒判定できない「灰」のいずれであるかを判定する。なお、「灰」については、多段階であってもよく、例えばより黒に近い５から白に近い１までの５段階レベルで、判定しても良い。判定結果には、判定対象の通信のプロトコル番号、宛先や送信元アドレス・ポート番号等が含まれており、この情報を用いて各通信制御装置１２、２５へセキュリティ制御が行われる。

【００２３】

通信制御装置２５は、制御判断装置２３から受けた制御命令にしたがって通信トラフィックを制御する。なお、通信トラフィックの制御処理として、通信モードの変更に伴う通信モード制御とセキュリティ制御とがある。

【００２４】

ユーザＮＷ３０内には、ＰＣなどの通信機器である端末４０とインターネットと通信するためのルータ８０（または終端装置）とがある。通信装置１０は、端末４０とルータ８０の間に接続され、端末４０がインターネット通信する通信トラフィックはすべて通信装置１０を介してルータ経由で外部ＮＷ６０と送受信されるものとする。

【００２５】

ここで、各装置について具体例を挙げて説明すると、例えば、収集装置１１は、ｓＦｌｏｗエージェント、収集管理装置２１は、ｓＦｌｏｗコレクタ、各通信制御装置１２、２５は、ＯｐｅｎＦｌｏｗ（例えば、「https://www.opennetworking.org/」参照）対応スイッチ、およびＧＲＥやＬ２ＴＰなどのトンネリング機能を基に構成される。

【００２６】

また、例えば、分析装置２２は、異常検知処理として、オンライン機械学習並列分散処理フレームワークＪｕｂａｔｕｓ（例えば、ＮＴＴ技術ジャーナル　2012.10、pp.30-35、「http://www.ntt.co.jp/journal/1210/files/jn201210030.pdf」参照）の異常検知を行うことができる装置である。また、例えば、解析装置２４は、Ｄｅｅｐ　Ｐａｃｋｅｔ　Ｉｎｓｐｅｃｔｉｏｎを行えるレイヤ2からレイヤ7のアプリケーション通信までを識別して深く解析し、悪性通信の振る舞いを検出、遮断できる装置である。

【００２７】

また、解析装置２４は、悪性通信（黒）であると判定した場合は、該当するメッセージログを出力する。また、解析装置２４は、怪しい通信（灰）であると判定した場合は、該当するメッセージログを出力し、さらに怪しさにレベルがある場合には、そのレベルを示す情報もあわせて出力する。また、解析装置２４は、悪性通信でない（白）と判定した場合は、該当するメッセージログを出力する、またはメッセージログを出力しないことで、悪性通信でないことを外部の制御判断装置２３や利用者へ通知する。

【００２８】

制御判断装置２３は、分析装置２２や解析装置２４の結果を基に命令内容を判断してＯｐｅｎＦｌｏｗコントローラを介して、ＯｐｅｎＦｌｏｗ対応スイッチ（例えば、Ｏｐｅｎ　ｖＳｗｉｔｃｈ（http://openvswitch.org/））へ命令してもよく、通信制御装置１２、２５の間のトンネリングの構築と削除は別途命令することとしてもよい。

【００２９】

また、ＯｐｅｎＦｌｏｗコントローラを各通信制御装置１２、２５に組み込み、制御判断装置２３が、各ＯｐｅｎＦｌｏｗコントローラに対して制御命令を送信し、命令を受信したＯｐｅｎＦｌｏｗコントローラが対象のＯｐｅｎＦｌｏｗ対応スイッチに対してフローエントリの書き込みなどの制御を行うこととしてもよい。

【００３０】

［通信装置の構成］

次に、図２を用いて、図１に示した通信装置１０の構成を説明する。図２は、第一の実施の形態に係る通信装置の構成を示すブロック図である。図２に示すように、この通信装置１０は、収集装置１１と通信制御装置１２とで構成される。

【００３１】

収集装置１１は、通信に関する情報のうち、一部の情報を部分情報として構成して制御装置２０に送信する。または、ユーザネットワーク内の収集可能な全通信を収集して、その一部を部分情報として構成することとしてもよい。ここで、ユーザネットワーク内の通信とは、通信装置１０を経由する通信であって、たとえばユーザネットワーク内に閉じた通信やユーザネットワークとインターネットなどの外部のネットワークの間の通信を示す。収集装置１１は、抽出部１１ａと記憶部１１ｂとを有する。

【００３２】

記憶部１１ｂは、部分情報を収集するための規定が定義された収集ルールを記憶する。例えば、記憶部１１ｂは、収集ルールとして、抽出部１１ａが通信トラフィックを抽出するための条件を規定した抽出ルールや、抽出した部分情報を収集管理装置２１へ送信するための条件が規定された送信ルールを記憶する。

【００３３】

抽出部１１ａは、記憶部１１ｂに記憶された収集ルールに基づいて、通信トラフィックを抽出し、必要に応じて一時的に記憶部１１ｂに記憶させる。また、抽出部１１ａは、抽出ルールの要件を満たす部分情報を抽出し、送信ルールの要件を満たす契機で収集管理装置２１へ送信する。例えば、抽出部１１ａは、所定数のパケットを取得するごとに、収集ルールの要件を満たす部分情報を収集管理装置２１へ送信する。

【００３４】

通信制御装置１２は、記憶部１２ａとトンネル部１２ｂと通信制御部１２ｃとを有する。記憶部１２ａは、通信モード制御やセキュリティ制御に必要な制御ルールを記憶する。

【００３５】

ここで、抽出部１１ａの収集ルールについて説明する。収集装置１１の記憶部１１ｂに記憶される収集ルールは、異常検知などを行う分析装置２２への入力となる特徴ベクトルを構成する各要素の情報（例えば、通信方向ごとの時刻情報、通信セッションの持続時間、ユーザまたはユーザＮＷ３０を識別する識別情報、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、アプリケーション識別情報、データサイズ、名前解決のためのＤＮＳクエリ及びレスポンスの内容情報やこの問合せの時間間隔、回数や解決された名前のＴＴＬ（Time To Live）など）と、これらの情報をサンプリングやサンプリングに類する形式で集約する、または統計化する計算方法、さらに部分情報を収集管理装置２１へ送信させる契機（収集する時間間隔を契機、所定パケット数収集を契機とするなど）を示す情報から構成される。例えば、契機を示す情報として、所定の時間間隔を契機としてもよいし、所定パケット数を収集したことを契機としてもよい。

【００３６】

また、通信トラフィックの収集として、例えば、ＳＮＭＰやｓＦｌｏｗ、Ｎｅｔｆｌｏｗ、ＩＰＦＩＸで取得できるデータ、及び、そのサンプリング方法が一例として挙げられる。または、ＯｐｅｎＦｌｏｗで扱える統計情報を取得する仕組みを利用してもよい。この場合には、ＯｐｅｎＦｌｏｗ対応スイッチで収集される統計情報をＯｐｅｎＦｌｏｗの仕様に従ってＯｐｅｎＦｌｏｗコントローラに送信されることになる。例えば、制御判断装置２３にＯｐｅｎＦｌｏｗコントローラが組込まれている場合は、統計情報を収集した制御判断装置２３は収集管理装置２１へ転送し、また各通信制御装置（通信制御装置１２と通信制御装置２５）にＯｐｅｎＦｌｏｗコントローラが組込まれている場合は通信制御装置１２上で収集した統計情報を収集管理装置２１へ転送する（収集装置１１を経由してもよい）。また、通信に利用されているレイヤ７のアプリケーションを識別できる手段が組込まれている場合は、この識別情報を部分情報に含めてもよい。

【００３７】

その他にも任意の情報を任意の形式で集約する構成を組込んでもよい。フレームまたはパケットをキャプチャして分解することで必要な要素情報を抽出できる。また、収集ルールに該当する要件を満たす所定の通信トラフィックをそのまま送信させてもよいし、この通信トラフィックの一部を送信させてもよい。この場合は、後述する収集管理装置２１側で部分情報を生成するか、または、受信した情報から機械学習などに適用する特徴ベクトルを生成する。例えば、ｓＦｌｏｗの技術を適用した場合は、サンプリングベースの技術であり、エージェント（収集装置１１に相当）ではなくコレクタ（収集管理装置２１に相当）にて特徴ベクトルを生成する。

【００３８】

トンネル部１２ｂは、対向の制御装置２０の通信制御装置２５との間でトンネルを構築する。トンネル部１２ｂは、通信モードがミラーリングモードまたはインラインモードのときに、解析装置２４へ通信トラフィックを流すために対向の通信制御装置２５の通信制

御部２５ｃとの間でトンネルを構築する。通信制御部１２ｃは、通信装置１０を経由する通信を制御する。具体的には、通信制御部１２ｃは、通信モードに基づく通信モード制御と、パケットフィルタリングなどのセキュリティ制御を行う。

【００３９】

［制御装置の構成］

次に、図３を用いて、図１に示した制御装置２０の構成を説明する。図３は、第一の実施の形態に係る制御装置の構成を示すブロック図である。図３に示すように、この制御装置２０は、収集管理装置２１と分析装置２２と制御判断装置２３と解析装置２４と通信制御装置２５とで構成される。

【００４０】

制御装置２０は、通信装置１０を流れる通信トラフィックを観測し、異常な通信（悪性、または悪性と断定できないが正常な通信の振る舞いとは異なる通信）と判定した場合や悪性通信と判定した場合に通信モードを変更することで通信モード制御を、悪性であり通信遮断が必要であると判定した場合はセキュリティ制御を、通信装置１０の通信制御装置１２および／または制御装置２０の通信制御装置２５に対して命令する。

【００４１】

収集管理装置２１は、収集部２１ａおよび抽出制御部２１ｂを有する。収集部２１ａは、通信装置１０から部分情報を収集して分析装置２２へ送信する。抽出制御部２１ｂは、収集装置１１に対して予め収集ルールを送信する。

【００４２】

分析装置２２は、収集管理装置２１を介して通信装置１０から受信した部分情報を分析し、分析した分析結果を用いて、ユーザネットワーク内の通信に異常があるか否かを判断する。また、分析装置２２は、分析／学習部２２ａおよび記憶部２２ｂを有する。なお、記憶部２２ｂは、通信の異常を判断する判断基準となるルールを記憶する。

【００４３】

分析／学習部２２ａは、収集管理装置２１から受け取った部分情報を異常検知などの機械学習により分析し、その結果を制御判断装置２３へ通知する。また、分析／学習部２２ａは、機械学習の学習結果をモデル情報として更新し、更新したモデル情報を記憶部２２ｂに格納する。

【００４４】

分析／学習部２２ａは、分析および学習の方法として、例えば密度ベースの外れ値検出法であるＬＯＦ（Local Outlier Factor）等を利用してもよい。ここで、分析および機械学習について詳細に説明する。まず、特徴ベクトル化について、特徴ベクトルを構成する要素をあらかじめ定義し、分析装置２２に登録しておく。

【００４５】

通信パケットである場合、例えば、送信元／宛先ＩＰアドレスやＭＡＣアドレス、プロトコル番号（ＴＣＰ／ＵＤＰ等を示す番号）、ポート番号、データ部の認証情報（有りの場合は１、無しの場合は０とする等）、データサイズ、通信に利用されているアプリケーションを識別する識別情報など通信パケットから取得できるあらゆる情報のうち、分析・学習に必要な要素を予め定義しておき、パケットの入力を受付けた場合には、このパケットを分解して定義した必要な要素（ＩＰｖ４アドレスを例えば８ビットごとの要素とする複数要素で構成してもよい）を抽出し、この要素で構成される特徴ベクトル（要素がｎ個であればｎ次元の数値ベクトルとなる）を作成する。

【００４６】

これは、収集装置１１の収集ルールに基づいて抽出部１１ａで行ってもよく、とにかく特徴ベクトル化に必要な情報を部分情報として収集装置１１から収集管理装置２１へ送信し、収集管理装置２１がこの部分情報から特徴ベクトルを生成することとしてもよい。

【００４７】

異常判定（分析）について、分析装置２２の記憶部２２ｂが記憶するこれまでの学習結果であるモデル情報（例えば、特徴ベクトル群であって、所定の学習または分類アルゴリ

ズムで分類されている１以上の集合となる）に対して、特徴ベクトル化された入力情報を入力として与えた場合、空間の距離や密度に基づいて異常（またはアノマリ、通常モデルからの逸脱度合いで示されるもの）か非異常かを判定することができる。

【００４８】

学習について、特徴ベクトルを所定の記憶部２２ｂに記憶するとともに、記憶された特徴ベクトル群を、所定の学習アルゴリズムに基づいて分類する。異常検知の学習アルゴリズムとして、例えばＬＯＦが適用可能である。ここで学習とは、記憶部２２ｂに特徴ベクトル情報を記憶して、記憶部２２ｂに記憶されている特徴ベクトル情報群から集合の特徴情報（分類であれば集合を分類するために線引きする境界線など）を導出する。この特徴情報を用いることで分析が可能となる。学習により、より多様で多数の特徴ベクトルがモデル情報に反映されることで、モデル情報を用いた分析の精度を高くすることができる。

【００４９】

制御判断装置２３は、判断部２３ａ、制御命令部２３ｂおよび記憶部２３ｃを有する。記憶部２３ｃは、各通信制御装置１２、２５の状態情報等を記憶する。記憶部２３ｃは、状態情報として、例えば、どのユーザまたはユーザＮＷ３０のどの通信トラフィックをどの通信モードで経路制御しているか、また通信モードの遷移の履歴、どのようなセキュリティ制御を実施しているかをユーザまたはユーザＮＷ３０ごとに対応付けて記憶する。

【００５０】

判断部２３ａは、分析装置２２によって分析された分析結果を用いて、通信モードを判断する。具体的には、判断部２３ａは、分析装置２２から分析結果を受け取ると、分析結果を基に判断して通信制御装置１２の通信モードを決定する。

【００５１】

制御命令部２３ｂは、分析装置２２によって通信に異常があると判断された場合には、該異常と判断された通信に関する情報（分析結果として異常と判定された特徴ベクトルに該当・対応する通信）が通信制御装置１２から解析装置２４へ転送される（経由する、またはミラーリングされる）ようにユーザＮＷ３０内の通信制御装置１２に対して通信経路を制御する。また、制御命令部２３ｂは、解析装置２４によってユーザＮＷ３０内の通信が悪性の通信であると判定された場合には、該悪性の通信を制限するように制御する。

【００５２】

例えば、制御命令部２３ｂは、判断部２３ａが決定した通信モードが現在の通信モードと異なる場合は、各通信制御装置１２、２５に決定した通信モードに従うよう通信モード制御命令を送信する。また、制御命令部２３ｂは、解析装置２４から解析結果を受け取り、セキュリティ制御が必要であると判断した場合には、通信制御装置１２（および／または２５）にセキュリティ制御命令を送信する。

【００５３】

ここで、通信制御装置１２、２５の記憶部１２ａ、２５ｂに記憶される制御ルールについて説明する。制御ルールは、通信モードに基づく経路制御とセキュリティ制御のためのルールである。図４に示すように、通信モードには、通常モードとミラーリングモードとインラインモードとが規定されており、分析装置２２の分析結果を考慮した制御判断装置２３の判断結果に応じて、各通信制御装置１２、２５が各モードに遷移することとなる。

【００５４】

通信モードが通常モードの場合は、内部ＮＷ（ユーザＮＷ３０）と通信する通信インターフェース及び外部ＮＷ６０と通信する通信インターフェースを備える通信装置１０の通信制御装置１２に対してブリッジ／スイッチ、ルーティング処理により受信した通信トラフィックを宛先へそのまま転送されるように制御する経路制御ルールが設定される。

【００５５】

また、ミラーリングモードおよびインラインモードの場合には、通信制御装置１２と対向の通信制御装置２５との間でトンネルを構築する。このトンネルは静的に構築されているものでもよく、当該通信モードに切り替わる契機で未構築であれば動的にトンネルが構築されるものでもよい。この場合、通常モードに切り戻す契機で動的に構築済みトンネル

を削除することとすればよい。

【００５６】

ミラーリングモードの場合には、通信装置１０の通信制御装置１２に対して、内部ＮＷと通信する通信インターフェースや外部ＮＷ６０と通信する通信インターフェースから受信した通信トラフィックを宛先へそのまま転送するとともに、受信した通信トラフィックをトンネル対向側に向けてミラーリングしてトンネル経由で転送するように制御する経路制御ルールが設定される。一方、制御装置２０の通信制御装置２５に対して、トンネル対向側からトンネル経由で受信した通信トラフィックを解析装置２４へ転送するように制御する経路制御ルールが設定される。

【００５７】

インラインモードの場合には、通信装置１０の通信制御装置１２に対して、内部ＮＷと通信する通信インターフェースから受信した通信トラフィックをトンネル対向側に向けてトンネル経由で転送するように、外部ＮＷ６０と通信する通信インターフェースから受信した通信トラフィックをトンネル対向側に向けてトンネル経由で転送するように、トンネル対向側からトンネル経由で受信した通信トラフィックを元の宛先に対して転送するように制御する経路制御ルールが設定される。さらに、通信装置１０の通信制御装置１２は、制御装置２０の通信制御装置２５からトンネル経由で受信した通信トラフィックを当該通信トラフィックの宛先へ転送するように制御する経路制御ルールが設定される。

【００５８】

一方、制御装置２０の通信制御装置２５に対して、トンネル対向側からトンネル経由で受信した通信トラフィックを解析装置２４へ転送するように、解析装置２４から受信した通信トラフィックをトンネル対向側にトンネル経由で転送するように制御する経路制御ルールが設定される。

【００５９】

セキュリティ制御は、悪性通信や所定の条件を満たす、あやしい通信（白黒灰の判定において灰に相当）と判定された通信を遮断する。所定の条件を満たすあやしい通信の遮断は、安全サイドに倒して念のための遮断であり、遮断の後で正常通信であると判定された場合は、その時点でこの遮断を解除する制御命令を送信することとなる。制御判断装置２３が遮断すべきと判断した通信を遮断するよう通信制御装置１２および／または２５へ命令する。例えば、レイヤ３のＩＰアドレスやＩＰアドレスレンジのレベル、レイヤ４のＴＣＰ／ＵＤＰやポート番号のレベル、アプリケーションレイヤでの遮断の制御が可能な場合は、通信トラフィックから遮断するべき特定のアプリケーションを識別して該当するアプリケーションを識別可能な情報を用いて当該アプリケーション通信を遮断する。ＵＲＬフィルタを適用できる場合は、遮断するべき特定のＵＲＬやＦＱＤＮをフィルタに設定するよう制御してもよい。メールフィルタを適用できる場合は、遮断するべき特定のメールアドレスやドメインをフィルタに設定するよう制御してもよい。遮断等のセキュリティ制御の設定に必要な情報は、解析装置２４が出力する解析結果に含まれていて、制御判断装置２３は受け取った解析結果を用いて通信制御装置に命令して制御する。

【００６０】

解析装置２４は、制御判断装置２３の判断部２３ａによって通信に異常があると判断された場合には、ミラーリングモードで機能している場合はこれに基づく経路制御によって転送されてくる通信を受信し、この通信に対して解析を行い、ユーザＮＷ３０内の通信が悪性の通信であるか否かを判定する。

【００６１】

解析装置２４は、詳細解析部２４ａを有する。詳細解析部２４ａは、通信トラフィックの内容を深く解析して、通信が、白（正常通信）、黒（悪性通信）、灰（白黒断定できない通信）のいずれであるかを判定し、判定対象の通信を示す送信元・宛先のＩＰアドレスやポート番号、アプリケーション識別情報などのうち少なくとも１以上からなる組とともに判定結果として制御判断装置２３へ送信する。

【００６２】

通信制御装置２５は、トンネル部２５ａと記憶部２５ｂと通信制御部２５ｃとを有する。トンネル部２５ａは、対向の通信装置１０の通信制御装置１２との間でトンネルを構築する。例えば、トンネル部２５ａは、ミラーリングモードとインラインモードのときに、解析装置２４へ通信トラフィックを流すために対向の通信制御装置１２の通信制御部１２ｃとの間でトンネルを構築する。

【００６３】

記憶部２５ｂは、通信モード制御やセキュリティ制御に必要な制御ルールを記憶する。通信制御部２５ｃは、通信モードに基づく通信モード制御を行う。また、通信制御部２５ｃは、セキュリティ制御を行う。

【００６４】

ここで、図５を用いて、第一の実施の形態に係るネットワークシステム１００による通信制御処理の一連の流れを説明する。図５は、第一の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。

【００６５】

図５に示すように、収集装置１１は、ユーザＮＷ３０を流れて通信制御装置１２を経由する通信トラフィックまたはその一部を収集する（図５の（１）参照）。そして、収集装置１１は、通信トラフィックの部分情報として制御装置２０の収集管理装置２１に送信する（図５の（２）参照）。

【００６６】

続いて、収集管理装置２１は、収集装置１１から送信される部分情報を収集し、分析装置２２へ送信する（図５の（３）参照）。そして、分析装置２２は、収集管理装置２１から受信した部分情報に対して、例えば、機械学習の異常検知などによる分析を行い、その結果を制御判断装置２３に出力する（図５の（４）参照）。

【００６７】

その後、制御判断装置２３は、分析装置２２から受けた分析結果を基に通信モードを決定し、各通信制御装置１２、２５へ通信モードに従った通信モード制御を行うよう命令する（図５の（５）参照）。また、解析装置２４は、受信する通信トラフィックに対して深い解析を行い、マルウェア等に感染した悪性通信であるか否かを判定して判定結果を制御判断装置２３に出力する（図５の（６）参照）。

【００６８】

そして、制御判断装置２３は、解析装置２４から受けた解析結果を基に通信モードやセキュリティ制御の内容を決定し、各通信制御装置１２、２５へこれらの決定に従った通信制御を行うよう命令する（図５の（７）参照）。例えば、通信モードが通常モードの場合には、通信制御装置１２は、端末４０とインターネット上のサイト５０との間の通信をそのまま宛先へ転送する（図５の矢印Ａ参照）。また、例えば、通信モードがミラーリングモードの場合には、通信制御装置１２は、通信をそのまま宛先（インターネット上のサイト５０または端末４０）へ転送するとともに、この両方向の通信をミラーリングして制御装置２０の通信制御装置２５を介して解析装置２４へも転送する（図５の矢印Ｂ参照）。また、例えば、通信モードがインラインモードの場合には、通信制御装置１２は、端末４０とインターネット上のサイト５０との通信を、通信制御装置１２、通信制御装置２５および解析装置２４を経由させてユーザＮＷ３０側の外縁ルータを経て宛先へ転送する。より具体的には、端末４０からインターネット上のサイト５０宛の通信であれば、端末４０から通信制御装置１２、通信制御装置２５を経て解析装置２４を経由して、そこから折り返して通信制御装置２５、通信制御装置１２を経てインターネット上のサイト５０宛に送信される。インターネット上のサイト５０から端末４０宛の通信であれば、この逆向きの順序の通信となる（図５の矢印Ｃ参照）。

【００６９】

［ネットワークシステムの処理の一例］

次に、図６を用いて、第一の実施の形態に係るネットワークシステム１００における通信制御処理の流れについて説明する。図６は、第一の実施の形態に係るネットワークシス

テムにおける通信制御処理の流れを示すシーケンス図である。

【００７０】

図６に示すように、収集装置１１は、ユーザＮＷ３０を流れて通信制御装置１２を経由する通信トラフィックまたはその一部を収集し、通信トラフィックの部分情報として制御装置２０の収集管理装置２１に送信する（ステップＳ１０１）。続いて、収集管理装置２１は、収集装置１１から送信される部分情報を収集し、分析装置２２へ送信する（ステップＳ１０２）。

【００７１】

そして、分析装置２２は、収集管理装置２１から受信した部分情報に対して、例えば、機械学習の異常検知などによる分析を行う（ステップＳ１０３）。そして、分析装置２２は、分析結果を制御判断装置２３に出力する（ステップＳ１０４）。

【００７２】

その後、制御判断装置２３は、分析装置２２から受けた分析結果を基に制御内容として通信モードを判断し（ステップＳ１０５）、各通信制御装置１２、２５へ通信モードに従った通信モード制御を行うよう命令して（ステップＳ１０６）、各通信制御装置１２、２５に制御内容を通知する（ステップＳ１０７）。そして、各通信制御装置１２、２５は、通知された通信モード制御を設定する（ステップＳ１０８、Ｓ１０９）。

【００７３】

ここで、通信制御装置１２は、通信モードがミラーリングモードまたはインラインモードの場合には、解析装置２４へ通信トラフィックを送信する（ステップＳ１１０）。そして、解析装置２４は、受信する通信トラフィックに対して深い解析を行い（ステップＳ１１１）、マルウェア等に感染した悪性通信であるか否かを判定して解析結果を制御判断装置２３に出力する（ステップＳ１１２）。

【００７４】

そして、制御判断装置２３は、解析装置２４から受けた解析結果を基に通信モードやセキュリティ制御の内容を判断し（ステップＳ１１３）、各通信制御装置１２、２５へ判断結果に応じた通信制御を行うよう命令して（ステップＳ１１４）、通信モードやセキュリティ制御の内容を各通信制御装置１２、２５に通知する（ステップＳ１１５）。そして、各通信制御装置１２、２５は、通知された通信モードやセキュリティ制御を設定する（ステップＳ１１６、Ｓ１１７）。

【００７５】

このように、ユーザＮＷ３０の外部に配置される制御装置２０は、ユーザＮＷ３０を流れる通信トラフィックの一部または統計化された情報である部分情報を効率よく収集し、収集した通信トラフィックの部分情報に対して分析を行う。そして、分析により異常な通信の振る舞いであると判定した場合は、監視すべきユーザＮＷ３０の通信トラフィックが制御装置２０に流れるように通信モードを変更させる。

【００７６】

また、通信モード変更によって、ミラーリングモードやインラインモードで通信の経路制御をすることで部分情報ではない通信トラフィックそのもの（ペイロードも対象としてもよい）を観測することでより深い解析にかける。解析によりマルウェアなどに感染したことを示す悪性通信と判定した場合は、この通信トラフィックを一時的または恒久的に遮断するよう制御する。悪性ではなく、正常な振る舞いの通信であると判断した場合は通信モードを例えば通常モードへ変更する。

【００７７】

普段はユーザＮＷ３０の通信トラフィックのうちの部分情報を観測することで、ユーザＮＷ３０の通信性能への影響を低減する。そして、この観測で異常検知の判定を行う。これを所定の契機で継続する。異常であると判断した場合は、該当通信トラフィックを深く解析し、さらに悪性通信であると判定した場合には、当該通信トラフィックに対してセキュリティ制御を実施する。

【００７８】

［収集装置の処理の一例］
次に、図７を用いて、収集装置１１における収集処理の流れについて説明する。図７は、第一の実施の形態に係る収集装置における収集処理の流れを示すフローチャートである。
【００７９】
図７に示すように、収集装置１１は、通信トラフィックを観測し（ステップＳ２０１）、通信トラフィックが抽出ルールに該当するかを判定する（ステップＳ２０２）。この結果、抽出ルールに該当する場合には（ステップＳ２０２肯定）、通信に関する情報を抽出し、または、統計化する（ステップＳ２０３）。
【００８０】
そして、収集装置１１は、通信に関する情報を抽出し、または、統計化した際に、送信ルールに該当するか否かを判定する（ステップＳ２０４）。例えば、収集装置１１は、送信ルールに規定される所定の時間間隔が経過したか、もしくは、送信ルールに規定される所定パケット数を収集したかを判定する。
【００８１】
この結果、収集装置１１は、送信ルールに該当する場合には（ステップＳ２０４肯定）、部分情報を収集管理装置２１へ送信する（ステップＳ２０５）。また、抽出ルールに該当しない場合（ステップＳ２０２否定）、または、送信ルールに該当しない場合には（ステップＳ２０４否定）、ステップＳ２０１の処理に戻って処理を繰り返す。
【００８２】
［制御装置の処理の一例］
次に、図８、９、１０を用いて、制御装置２０における通信制御処理の流れについて説明する。図８は、第一の実施の形態に係る制御装置の通常モードにおける通信制御処理の流れを示すフローチャートである。図９は、第一の実施の形態に係る制御装置のミラーリングモードにおける通信制御処理の流れを示すフローチャートである。図１０は、第一の実施の形態に係る制御装置のインラインモードにおける通信制御処理の流れを示すフローチャートである。
【００８３】
まず、図８を用いて、通常モードにおける通信制御処理について説明する。図８に示すように、まず、制御装置２０の収集管理装置２１が、収集装置１１から送信される部分情報を収集する（ステップＳ３０１）。そして、分析装置２２は、収集管理装置２１から受信した部分情報に対して、例えば、機械学習の異常検知などによる分析を行う（ステップＳ３０２）。
【００８４】
そして、分析装置２２は、分析した分析結果を用いて、ユーザＮＷ３０内の通信に異常があるか否かを判断する（ステップＳ３０３）。この結果、分析装置２２は、通信に異常がないと判定した場合には（ステップＳ３０３否定）、ステップＳ３０１の処理に戻る。また、制御判断装置２３は、通信に異常があると判定された場合には（ステップＳ３０３肯定）、分析装置２２から受けた分析結果を基に制御内容として通信モードを判定する（ステップＳ３０４）。
【００８５】
ここで、制御判断装置２３は、通信の異常の度合いが所定の閾値より高いか否かを判定する（ステップＳ３０５）。この結果、制御判断装置２３は、通信の異常の度合いが所定の閾値より高い場合には（ステップＳ３０５肯定）、インラインモードへ遷移する通信モード制御を行うよう各通信制御装置１２、２５に命令する（ステップＳ３０６）。また、制御判断装置２３は、通信の異常の度合いが所定の閾値以下である場合には（ステップＳ３０５否定）、ミラーリングモードへ遷移する通信モード制御を行うよう各通信制御装置１２、２５に命令する（ステップＳ３０７）。そして、各通信制御装置１２、２５は、命令された通信モード制御を設定する（ステップＳ３０８）。なお、通信モードが通常モードと、ミラーリングモードまたはインラインモードの２つのみで実施される場合は、ステ

ップＳ３０５は省略されて、ステップＳ３０６またはステップＳ３０７のいずれかが択一的に選択されることとなる。

【００８６】

次に、図９を用いて、ミラーリングモードにおける通信制御処理について説明する。図９に示すように、解析装置２４は、ミラーリングモードにおいて、通信制御装置１２から受信する通信トラフィックに対して深い解析を行い（ステップＳ４０１）、通信が悪性である「黒」、悪性ではない「白」、白黒判定できない「灰」のいずれであるかを判定する（ステップＳ４０２）。

【００８７】

この結果、解析装置２４が「黒」と判定した場合には、制御判断装置２３は、パケットフィルタリングなどのセキュリティ制御を行うことを各通信制御装置１２、２５に命令し（ステップＳ４０３）、ステップＳ４０７に移行する。

【００８８】

また、解析装置２４が「白」と判定した場合には、制御判断装置２３は、通常モードへ遷移する通信モード制御を行うよう各通信制御装置１２、２５に命令し（ステップＳ４０４）、ステップＳ４０７に移行する。

【００８９】

また、解析装置２４が「灰」と判定した場合には、制御判断装置２３は、通信が要注意であるか、すなわち、「灰」という判定結果が所定のレベル以上であるか否かを判定する（ステップＳ４０５）。例えば、より黒に近い５から白に近い１までの５段階レベルである場合には、「３」以上であるか否かを判定する。

【００９０】

この結果、制御判断装置２３は、所定のレベル以上である場合には（ステップＳ４０５肯定）、インラインモードへ遷移する通信モード制御を行うよう各通信制御装置１２、２５に命令し（ステップＳ４０６）、ステップＳ４０７に移行する。また、所定のレベル以上でない場合には（ステップＳ４０５否定）、ステップＳ４０１の処理に戻って、上記の処理を繰り返す。そして、ステップＳ４０７において、通信制御装置２５は、命令された通信モードやセキュリティ制御を設定して、処理を終了する。なお、通信モードが通常モードとミラーリングモードの２つのみで実施される場合、ステップＳ４０５、ステップＳ４０６は省略され、ステップ４０２で灰判定となった場合はステップＳ４０１の処理に戻ってもよい。また、あらかじめ設定しておくことで、より安全性を高めるために灰判定を黒判定と同じ扱いとしてもよく、または過剰な通信遮断による弊害を避けるため、灰判定を白判定と同じ扱いとしてもよい。

【００９１】

次に、図１０を用いて、インラインモードにおける通信制御処理について説明する。図１０に示すように、解析装置２４は、インラインモードにおいて、通信制御装置１２から受信する通信トラフィックに対して深い解析を行い（ステップＳ５０１）、通信が悪性である「黒」、悪性ではない「白」、白黒判定できない「灰」のいずれであるかを判定する（ステップＳ５０２）。

【００９２】

この結果、解析装置２４が「黒」と判定した場合には、制御判断装置２３は、パケットフィルタリングなどのセキュリティ制御を行うことを各通信制御装置１２、２５に命令し（ステップＳ５０３）、ステップＳ５０７に移行する。

【００９３】

また、解析装置２４が「灰」と判定した場合には、制御判断装置２３は、通信が要注意であるか、すなわち、「灰」という判定結果が所定のレベル以上であるか否かを判定する（ステップＳ５０４）。例えば、より黒に近い５から白に近い１までの５段階レベルである場合には、「３」以上であるか否かを判定する。

【００９４】

この結果、制御判断装置２３は、所定のレベル以上でない場合には（ステップＳ５０４

否定）、ミラーリングモードへ遷移する通信モード制御を行うよう各通信制御装置１２、２５に命令し（ステップＳ５０５）、ステップＳ５０７に移行する。また、所定のレベル以上である場合には（ステップＳ５０４肯定）、ステップＳ５０１の処理に戻って、上記の処理を繰り返す。

【００９５】

また、解析装置２４が「白」と判定した場合には、制御判断装置２３は、通常モードへ遷移する通信モード制御を行うよう各通信制御装置１２、２５に命令し（ステップＳ５０６）、ステップＳ５０７に移行する。そして、ステップＳ５０７において、通信制御装置２５は、命令された通信モードやセキュリティ制御を設定して、処理を終了する。なお、通信モードが通常モードとインラインモードの２つのみで実施される場合、ステップＳ５０４、ステップＳ５０５は省略され、ステップ５０２で灰判定となった場合はステップＳ５０１の処理に戻ってもよい。また、あらかじめ設定しておくことで、より安全性を高めるために灰判定を黒判定と同じ扱いとしてもよく、または過剰な通信遮断による弊害を避けるため、灰判定を白判定と同じ扱いとしてもよい。

【００９６】

［第一の実施の形態の効果］

このように、第一の実施の形態に係るネットワークシステム１００は、通信装置１０は、該通信装置１０を経由する通信に関する情報のうち、一部の情報または統計化された情報を部分情報として制御装置２０に送信する。そして、制御装置２０は、通信装置１０から受信した部分情報を分析し、分析された分析結果を用いて、ユーザＮＷ３０内の通信に異常があるか否かを判断する。そして、制御装置２０は、ユーザＮＷ３０内の通信に異常があると判断された場合には、通信モードを変更することで経路制御を行い、ユーザＮＷ３０を流れる通信を用いて解析を行い、ユーザＮＷ３０内の通信が悪性の通信であるか否かを判定する。制御装置２０は、ユーザＮＷ３０内の通信に異常があると判断された場合には、該異常と判断された通信に関する情報（例えば、異常と判定された特徴を持つ通信トラフィック）が通信装置１０から解析装置２４へ転送されるようにユーザＮＷ３０内の通信装置１０を制御する。そして、解析装置２４によってユーザＮＷ３０内の通信が悪性の通信であると判定された場合には、該悪性の通信を制限するように制御する。

【００９７】

これにより、第一の実施の形態に係るネットワークシステム１００は、ユーザＮＷ３０から外部ＮＷ６０であるインターネットなどへアクセスするための通信回線の帯域の圧迫や異常・悪性通信の検知に関する精度の低下を抑えて、悪性通信を検知して、ユーザ通信を適切に保護することが可能である。つまり、通常時は、通信装置１０で収集した部分情報を制御装置２０が分析を行って異常を検知する処理を行い、異常を検知した場合にはユーザＮＷ３０の通信に関する情報を解析装置２４へ転送させ、転送された全データに対してＩＤＳやＩＰＳ（Intrusion Prevention System）等で深い解析を行うことにより悪性通信を判定して悪性通信を対処する。これにより、ユーザＮＷ回線の帯域の圧迫や異常・悪性通信の検知に関する精度の低下を抑えて、悪性通信を判定し、悪性通信を対処することが可能となる。

【００９８】

［第二の実施の形態］

上記の第一の実施の形態では、部分情報を異常検知などの機械学習により分析し、さらに機械学習の結果をモデル情報として更新する場合を説明したが、解析装置２４の解析結果を分析装置２２のモデル情報に反映または付加することで、モデル情報を更新してもよい。

【００９９】

例えば、分析装置２２における異常検知の学習結果であるモデル情報では、モデル情報を構成する特徴ベクトル群の密度や距離などに基づいて所定の閾値により、異常となる空間領域であるか否か判定される。ここで異常とは、通常とは異なるものであって、この時点では必ずしも悪性通信であると断定できるものではない。

【０１００】
そこで、第二の実施の形態では、解析装置２４で得られた判定結果であるラベル（白／黒／灰）と、この判定結果に該当する通信トラフィックから構成される特徴ベクトルとを組として、モデル情報にマッピング（写像）させる場合を例にして説明する。なお、第一の実施の形態と同様の処理については説明を省略する。
【０１０１】
図１１は、第二の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。図１１に示すように、第二の実施の形態に係る制御装置２０において、分析装置２２は、機械学習の異常検知などによる分析を行うと、その結果を制御判断装置２３に出力するとともに（図１１の（４）参照）、分析結果を機械学習のモデル情報として記憶する。
【０１０２】
そして、制御判断装置２３は、解析装置２４から受けた解析結果を基に通信モードやセキュリティ制御の内容を決定し、各通信制御装置１２、２５へこれらの決定に従った通信制御を行うよう命令した後（図１１の（７）参照）、解析装置２４から受け取った解析結果を分析装置２２に送信する。そして、分析装置２２は、解析装置２３から受けた解析結果を分析装置２２のモデル情報の空間上にマッピングする（図１１の（８）参照）。
【０１０３】
ここで、解析結果をモデル情報の空間上にマッピングする処理について、図１２の例を用いて説明する。図１２は、特徴ベクトル空間へのマッピングの概念図である。図１２に示すように、特徴ベクトル空間においては、通常モードにおける分析装置２２による異常検知の特徴ベクトルと、解析装置２４の判定結果に対応する特徴ベクトルとが存在する。
【０１０４】
この解析装置２４の判定結果に対応する特徴ベクトルには、解析装置２４の判定結果を示すラベルが付されている。そして、解析装置２４の判定結果に対応する特徴ベクトルを含む所定の領域に該当する特徴ベクトルは、ラベルに基づく判定基準による制御が行われる。例えば、「異常」と判定された空間領域に「黒」と判定された結果がラベルとしてマッピングされている場合には、異常ではなく悪性通信と判定する。なお、黒、白、灰の全てのラベルを付する場合に限定されるものではなく、黒および／または白と判定されたもののみをラベル付することとしてもよい。
【０１０５】
また、例えば、ラベル付された特徴ベクトルと所定の距離や密度を満たす特徴ベクトルに対しては、ラベルに基づいた判定をしてもよい。また、例えば、判断基準を示す制御ルールをあらかじめ決めておき、これに従って制御内容を決定することとしてもよい。
【０１０６】
ここで判断基準の一例について図１３を用いて説明する。図１３は、異常判定処理に用いられる判定基準の一例を示す図である。図１３に例示するように、解析装置２４の解析結果である「マッピング情報」と、分析装置２２の分析結果である「モデル情報」との組み合わせごとに、通信モードが規定されている。
【０１０７】
例えば、モデル情報が「異常と判定された空間領域」であり、この領域の中に「白判定」を示すマッピング情報が該当している場合には、この領域に該当する通信（特徴ベクトル）を分析により検知した時、「通常モード」による通信モード制御が行われる。つまり、異常と判定された空間領域ではあるが、悪性通信ではない「白」と判定されたラベルであるため、通常モードのままとしている。なお、図１３において、括弧に「（またはミラーリングモード）」と記載されており、括弧内の通信モードが決定されてもよく、通常モードとするかミラーリングモードとするかはユーザや管理者に予め選択させておけばよい。
【０１０８】
また、例えば、モデル情報が「異常と判定されない空間領域」であり、この領域の中に

「黒判定」を示すマッピング情報が該当している場合には、この領域に該当する通信（特徴ベクトル）を分析により検知した時、「セキュリティ制御」が行われる。つまり、異常と判定されない空間領域であっても、悪性通信ではある「黒」と判定されたラベルであるため、セキュリティ制御に遷移する。

【０１０９】

第一の実施の形態では、通常モードからセキュリティ制御へ遷移することはなかったが、第二の実施の形態では、上記したようにラベルを適用することで、異常の内容を反映することが可能となるため、例えば、悪性通信（黒）であるから異常であるなどと判断できるため、通常モードからセキュリティ制御へ遷移させることができる。

【０１１０】

なお、異常検知だけではなく、例えばクラスタリングの機械学習にも適用することができる。セキュリティ判定結果を機械学習によって分類された各クラスタにマッピングさせることで、各クラスタにラベル付けをすることができる。ここで、クラスタリングとは、機械学習において、特徴量の関連性・類似性が高いものをグルーピングすることであり、分類対象の集合を、内的結合と外的分離が達成されるような部分集合に分割する。

【０１１１】

このマッピング処理に使用するラベルと特徴ベクトルの組は、解析装置２４に別途収集装置１１と同等の装置を組込む、または解析装置２４の手前（解析装置２４と通信制御装置２５の間など）にインライン接続の形態で収集装置１１を置く、もしくは解析装置２４に流れてくる通信トラフィックに対してミラーリング接続の形態で収集装置１１を置くことで、解析装置２４に流れてくる通信トラフィックに関する情報を収集する。

【０１１２】

そして、収集装置１１相当の装置が部分情報を抽出して特徴ベクトルを構成し、さらに、解析装置２４のセキュリティ判定結果であるラベル相当の情報を特徴ベクトルに対応付けて、分析装置２２のモデル情報にマッピングさせる。この対応付けした特徴ベクトルとラベル情報は、制御判断装置２３を介して分析装置２２の記憶部２２ｂに記憶してもよい。また制御判断装置２３の記憶部２３ｃに記憶してもよく、この場合は分析装置２２から出力される分析結果と組み合せてセキュリティ制御判断に適用してもよい。

【０１１３】

つまり、分析結果である特徴ベクトルの空間領域に対して意味づけ（ラベルづけ）を行うことによって、異常検知／分析結果を基に通信モードの変更を省略してセキュリティ制御を行うことができる。または、異常検知／分析結果を基に通常モードからミラーリングモード、インラインモードへ遷移するところを、ミラーリングモードを省略して通常モードからインラインモードへ遷移させる判断をとってもよい。

【０１１４】

次に、図１４を用いて、第二の実施の形態にかかるネットワークシステム１００における通信制御処理の流れについて説明する。図１４は、第二の実施の形態に係るネットワークシステムにおける通信制御処理の流れを示すシーケンス図である。なお、図１４におけるステップＳ６０１～Ｓ６１７の処理は、図６で説明した第一の実施の形態に係るネットワークシステム１００における通信制御処理のステップＳ１０１～Ｓ１１７と同様であるため、説明を省略する。

【０１１５】

各通信制御装置１２、２５は、通知された通信モードやセキュリティ制御を設定した後（ステップＳ６１６、Ｓ６１７）、制御判断装置２３は、解析装置２４から受け取った解析結果を分析装置２２に送信する（ステップＳ６１８）。そして、分析装置２２は、解析装置２４から受けた解析結果を分析装置２２のモデル情報の空間上にマッピングする（ステップＳ６１９）。

【０１１６】

次に、図１５を用いて、制御装置２０における通信制御処理の流れについて説明する。図１５は、第二の実施の形態に係る制御装置の通常モードにおける通信制御処理の流れを

示すフローチャートである。

【０１１７】

図１５に示すように、制御判断装置２３は、分析装置２２から受けた分析結果を基に制御内容として通信モードを判定する際に（ステップＳ７０４）、解析結果照合に該当するか否かを判定する（ステップＳ７０５）。ここで、例えば、上記の分析結果である特徴ベクトルによる空間領域（クラスタリングされた空間領域または異常／通常を分ける空間領域）にラベル付された特徴ベクトルが該当する場合は、この空間領域全体またはこの空間領域内であってラベル付された特徴ベクトルから所定の距離・範囲内の空間領域を、そのラベルで代表される空間領域とみなす。この空間領域に該当するか否か、さらに該当するラベルは何なのかを分析装置２２が判定する。この結果、解析結果照合に該当する場合には（ステップＳ７０５肯定）、パケットフィルタリングなどのセキュリティ制御を行うことを各通信制御装置１２、２５に命令する（ステップＳ７０６）。

【０１１８】

つまり、上述したように、解析装置２４の解析結果（判定結果）に対応する特徴ベクトルには、さらに、解析装置２４の判定結果を示すラベルが付されている。このため、解析装置２４の判定結果に対応する特徴ベクトルを含む所定の領域に該当する部分情報の特徴ベクトルは、ラベルに基づく判定基準による制御が行われる。例えば、「異常」と判定された空間領域に「黒」と判定された結果がラベルとしてマッピングされている場合には、異常ではなく悪性通信と判定し、パケットフィルタリングなどのセキュリティ制御を行う。

【０１１９】

このように、第二の実施の形態に係るネットワークシステムでは、解析装置２４の解析結果と該当する特徴ベクトルを分析装置２２のモデル情報に反映し、モデル情報を更新することで、機械学習の結果であるモデル情報に意味づけをして、制御判断の材料にすることが可能となる。

【０１２０】

［第三の実施の形態］

上記の第一の実施の形態では、記憶部１１ｂに記憶された収集ルールに基づいて、通信トラフィックの部分情報を収集管理装置へ送信する場合を説明したが、この収集ルールを適宜更新するようにしてもよい。そこで、以下の第三の実施形態では、制御判断装置２３が収集ルールを適宜更新する場合について説明する。なお、第一の実施の形態と同様の処理については説明を省略する。

【０１２１】

図１６は、第三の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。図１６に示すように、制御判断装置２３は、更新した収集ルールを収集管理装置２１を介して収集装置１１に送信する（図１６の（８）参照）。そして、収集装置１１は、記憶部１１ｂに記憶している収集ルールを更新する（図１６の（９）参照）。その後、収集装置１１は、更新された収集ルールに基づいて部分情報を収集管理装置２１へ送信する（図１６の（２）参照）。

【０１２２】

このように、第三の実施の形態に係るネットワークシステムでは、より精度の高い判定をするために、制御判断装置２３が収集ルールを更新することで、収集すべき部分情報を更新する。

【０１２３】

収集ルールの更新について、例えば、任意の送信元又は宛先ＩＰアドレスを対象としていたところを、自国に割り当てられているＩＰアドレスではない海外の、または海外の特定国・地域のＩＰアドレスとの通信を対象とすることとしてもよい。また、特定のＩＳＰが管理するＩＰアドレスとの通信を対象としてもよい。

【０１２４】

また、部分情報を収集する時間間隔や、何パケット毎に、または特定の宛先や送信元毎

に何パケット毎に部分情報を収集するかを示すサンプリングレートを更新してもよい。例えば、１０分間隔で部分情報を収集していたところを１分間隔で収集することとしてもよいし、サンプリングレートを大きくすることとしてもよい。また、サンプリング対象のプロトコルやポート番号を指定してもよいし、これらのプロトコルやポート番号の通信トラフィックの１００パケット毎の収集を１０パケット毎にするなどサンプリングレートを高くすることとしてもよい。

【０１２５】

また、更新するルールの決定方法について、機械学習の学習結果である異常検知のモデル情報を取得することにより、特徴ベクトル空間上において、特徴ベクトルの集合の密度や特徴ベクトル及び特徴ベクトルで構成される集合と集合の間の距離などを基に異常と判定される特徴ベクトルまたは空間領域を特定できるため、この空間領域に該当する特徴ベクトルに該当する通信トラフィックをより多く効率的に収集できるルールへ更新することが考えられる。または、多様な特徴ベクトルにてモデル情報を構成するため、特徴ベクトル空間上においてまだ特徴ベクトルがない、またはまばらな空間に該当する部分情報を収集できるようにする更新することとしてもよい。

【０１２６】

また、解析結果を基に収集ルールを更新する場合は、例えば、所定期間内に所定回数以上の黒判定を結果として出力された場合を条件として、収集の時間間隔を短くする、またはサンプリングレートを上げることでより多くの部分情報を収集することとしてもよい。また、例えば、所定期間内に同一または類似する種類の黒判定が所定回数以上結果として出力された場合を条件として、この黒判定の種類を特徴づける情報（黒判定となっているアドレスに該当する国のアドレス、サービスを示すポート番号、アプリケーションなど）を抽出し、これらの情報の収集割合を高くする収集ルールに更新して部分情報を収集することとしてもよい。その後、同じまたは別の所定期間黒判定を結果として出力されなかった場合に更新した収集ルールを元に戻すこととしてもよい。また、分析結果と解析結果を組合せて適用して収集ルールを更新してもよい。

【０１２７】

また、分析装置２２のモデル情報および／または解析装置２４の判定結果を基にして、一般的に機械学習は固定の特徴ベクトルに基づいて分析・学習の処理されるものが多い。したがって、特徴ベクトルを構成する要素の追加や削除、変更を伴う収集ルールの更新は、これまでの学習結果であるモデル情報と整合しないため学習がうまく機能しなくなる場合がある。ただし、特徴ベクトルを構成する要素の動的な追加や削除、変更を許容できる学習アルゴリズムを適用する場合はこの限りでない。

【０１２８】

次に、図１７を用いて、第三の実施の形態にかかるネットワークシステム１００における通信制御処理の流れについて説明する。図１７は、第三の実施の形態に係るネットワークシステムにおける通信制御処理の流れを示すシーケンス図である。なお、図１７におけるステップＳ８０４～Ｓ８２０の処理は、図６で説明した第一の実施の形態に係るネットワークシステム１００における通信制御処理のステップＳ１０１～Ｓ１１７と同様であるため、説明を省略する。

【０１２９】

図１７に示すように、まず最初に、収集管理装置２１が、収集ルールを生成し（ステップＳ８０１）、収集ルールを収集装置１１に送信する（ステップＳ８０２）。そして、収集装置１１は、収集ルールを設定し（ステップＳ８０３）、設定された収集ルールに基づいて部分情報を収集管理装置２１へ送信する（ステップＳ８０４）。

【０１３０】

その後、各通信制御装置１２、２５が、通知された通信モードやセキュリティ制御を設定した後（ステップＳ８１９、Ｓ８２０）、制御判断装置２３は、収集ルールを更新し（ステップＳ８２１）、収集ルールを収集装置１１に送信する（ステップＳ８２２）。そして、収集装置１１は、更新された収集ルールを設定する（ステップＳ８２３）。

【０１３１】
次に、図１８を用いて、収集装置１１における収集処理の流れについて説明する。図１８は、第三の実施の形態に係る収集装置における収集処理の流れを示すフローチャートである。
【０１３２】
図１８に示すように、収集装置１１は、制御判断装置２３から更新された収集ルールを受け付けると、収集ルールを更新する（ステップＳ９０１）。そして、収集装置１１は、通信トラフィックを観測し（ステップＳ９０２）、通信トラフィックが更新された抽出ルールに該当するかを判定する（ステップＳ９０３）。この結果、抽出ルールに該当する場合には（ステップＳ９０３肯定）、通信に関する情報を抽出し、または、統計化する（ステップＳ９０４）。その後、第一の実施の形態に係る収集装置１１と同様の処理を行って、部分情報を収集管理装置２１へ送信する（ステップＳ９０６）。
【０１３３】
このように、第三の実施の形態に係るネットワークシステムでは、より精度の高い判定をするために、制御判断装置２３が収集ルールを動的に更新することで、収集すべき部分情報を適切に収集することが可能である。
【０１３４】
［第四の実施の形態］
上記の第一の実施の形態では、１つのユーザＮＷ３０の分析結果および／または解析結果を基に判定することとしていたが、各ユーザＮＷ３０の分析結果であるモデル情報を統合・共有してもよい。これにより、より多数で多様な特徴ベクトル群にてモデル情報を構成することができ、一般に異常検知の精度の向上が見込まれる。この場合、分析装置２２は、各ユーザＮＷ３０の特徴ベクトルを１つの機械学習にかけて１つのモデル情報を構築する構成とする。
【０１３５】
そこで、第四の実施の形態では、各ユーザＮＷ３０の分析結果であるモデル情報を統合し、分析装置２２でユーザごとのモデル情報を共有する場合を例として説明する。なお、第一の実施の形態と同様の処理については説明を省略する。
【０１３６】
図１９は、第四の実施の形態に係るネットワークシステムによる通信制御処理の一連の流れを説明する図である。図１９に示すように、分析装置２２は、各ユーザＮＷ３０の特徴ベクトルを１つの機械学習にかけて１つのモデル情報を構築し、ユーザごとのモデル情報を共有する（図１９の（８）参照）。
【０１３７】
また、一律に共有するのではなく、各ユーザＮＷ３０の分析結果であるモデル情報をクラスタリングして、モデル情報が類似するユーザＮＷ３０のモデル情報の間でのみを共有することとしてもよい。元のモデル情報を単純に統合して多様化するのではなく、元のモデル情報に類似するモデル情報、つまり通信の振る舞いが類似するユーザＮＷ３０に該当するモデル情報間で共有することで、ユーザＮＷ３０の通信の傾向に沿ったモデル情報を構成することができる。ユーザＮＷ３０ごとの局所的な通信の傾向や振る舞いの特徴が類似するユーザＮＷ３０間のモデル情報を共有することで、この特徴を活かしつつ、学習のための情報を増やすことができ、また異常検知の精度の向上が見込まれる。
【０１３８】
この場合、分析装置２２は、ユーザＮＷ３０ごとに対応づけてモデル情報を記憶部２２ｂに記憶する。さらに、所定の契機でモデル情報の間の類似度を計算し、類似すると判定したモデル情報を統合して共有する。この場合、ユーザＮＷ３０ごとのモデル情報を記憶しつつ、統合されたモデル情報をさらに記憶することとしてもよい。
【０１３９】
モデル情報の類似性の判定の際に用いる集合間の類似度の求め方としては、例えば、図２０に例示するような計算が挙げられる。分析装置２２は、計算した係数「ｓｉｍ」とし

て、ジャッカード係数、ダイス係数、シンプソン係数を求め、計算した係数「ｓｉｍ」が所定の閾値以上であれば、類似すると判定する。なお、ジャッカード係数、ダイス係数、シンプソン係数の３つの係数を求めて類似性を判定しても良いし、いずれか１つまたは２つの係数を求めて類似性を判定しても良い。

【０１４０】

また、各ユーザＮＷ３０の学習モデル、各クラスタの学習モデルを保持ししつつ、ユーザＮＷ３０の学習モデル間、クラスタの学習モデル間の傾向分析やモデル情報単位での異常判定をすることにより、モデル情報内の特徴ベクトルの異常判定にとどまらず、モデル情報そのものの異常を判定することも可能となるため、この判定結果を分析結果として適用してもよい。この場合、あるモデル情報内では異常ではない特徴ベクトル群であっても、他のモデル情報と比較することで、このモデル情報そのものが異常な特徴ベクトルが多数を占める集合であるということも検知することができる。

【０１４１】

［第五の実施の形態］

上記の第一の実施の形態では、通信の異常の度合いに応じて、ミラーリングモードへ遷移するかインラインモードへ遷移するかを制御する場合を説明したが、これに限定されるものではない。例えば、分析装置２２で異常を検知された通信が、暗号化されている通信である場合には、インラインモードへ遷移させることとし、平文通信である場合には、ミラーリングモードへ遷移させるように各通信制御装置１２、２５を制御してもよい。

【０１４２】

つまり、分析装置２２で異常が検知された通信が、暗号化されている通信である場合には、ミラーリングモードへ遷移して解析装置２４に通信を引き込んだとしても、暗号化されているため、解析装置２４でＤＰＩ（Deep Packet Inspection）による深い解析を実施できない。

【０１４３】

そこで、第五の実施の形態では、分析装置２２で異常を検知された通信が、暗号化されている通信である場合には、インラインモードへ遷移させることとし、平文通信である場合には、ミラーリングモードへ遷移させるように各通信制御装置１２、２５を制御する場合を例として説明する。また、第五の実施の形態のネットワークシステムでは、端末４０から受信した暗号通信を復号し、復号した通信を解析装置２２へ送信するとともに、再び暗号化して宛先へ送信する暗号通信検査装置２６を新たに有する例を説明する。なお、第一の実施の形態と同様の処理については説明を省略する。

【０１４４】

制御判断装置２３は、暗号通信と平文通信の識別について、例えば、パケットの送信元や宛先のポート番号を用いるようにしてもよい。例えば、ＨＴＴＰＳ（Hypertext Transfer Protocol Secure）の通信において、宛先のポート番号が「４４３」のポート（https（http protocol over TLS/SSL）：443）の場合や、ＦＴＰＳ（File Transfer Protocol over SSL/TLS)の通信において、ポート番号が「９８９」のポート（ＦＴＰデータ転送ポート）または「９９０」のポート（ＦＴＰ制御ポート）の場合には、暗号通信と判定する。

【０１４５】

なお、暗号通信検査装置２６が復号できない暗号通信があって、復号できないことが既知である場合は、ミラーリングモードへ遷移させることとしてもよい。この既知の復号不可の暗号通信の識別もまたポート番号を用いる。また、特定の宛先とＶＰＮ通信をすることが事前に分かっている場合は、宛先ＩＰアドレスを用いて識別することとしてもよい。また、ポート番号やＩＰアドレスの情報は、例えば制御判断装置２３の中の記憶部２３ｃに記憶されている。

【０１４６】

例えば、図２１に例示するように、制御判断装置２３は、分析装置で異常が検知された通信が、平文通信であると判定した場合には、ミラーリングモードへ遷移させる。ミラー

リングモードに遷移した後は、第一の実施の形態と同様に、通信制御装置２５が、受信した通信を解析装置２４へ転送する。

【０１４７】

また、図２２に例示するように、制御判断装置２３は、分析装置で異常が検知された通信が、暗号通信であると判定した場合には、インラインモードへ遷移させる。ここで、一般的に、ユーザＮＷ３０内の端末４０に暗号通信検査装置２６のＣＡ（認証局：certificate authority）証明書がインポートされていることが前提となる。

【０１４８】

インラインモードにおいては、暗号通信検査装置２６は、端末４０との間、Ｗｅｂサーバ９０との間にそれぞれＳＳＬ／ＴＬＳ等の暗号通信のセッションを張る。そして、暗号通信検査装置２６は、受信した暗号通信を復号し、復号した通信を解析装置２２へ送信するとともに、再び暗号化して宛先であるＷｅｂサーバ９０へ送信する。なお、暗号通信検査装置２６は、一般にＳＳＬインスペクション装置などと呼ばれる装置である。なお、暗号通信検査装置２６と解析装置２４は同一の装置で構成されるものであってもよい。

【０１４９】

このように、第５の実施の形態では、分析装置２２で異常を検知された通信が、暗号化されている通信である場合には、インラインモードへ遷移させることとし、平文通信である場合には、ミラーリングモードへ遷移させるように各通信制御装置１２、２５を制御するので、異常を検知された通信が暗号通信である場合であっても、該通信を解析装置２４が解析することが可能である。

【０１５０】

［第六の実施の形態］

上記の第一の実施の形態では、通常モードでユーザＮＷ３０側の通信制御装置１２を流れている通信に関する部分情報を収集し、分析して異常を検出した際に、該当する通信をミラーリングモードまたはインラインモードへ遷移させる場合を説明したが、これに限定されるものではない。例えば、分析装置２２において異常通信として過去に検出された情報を蓄積させ、蓄積された情報を用いて、初出のパケットに対して、ミラーリングモードまたはインラインモードへ遷移させる制御を行うようにしてもよい。

【０１５１】

例えば、ＯｐｅｎＦｌｏｗの仕様に基づく場合、ＯｐｅｎＦｌｏｗ対応スイッチのフローテーブルに該当しない未登録のパケットは、このパケットまたこのパケットの所定の一部の情報をＯｐｅｎＦｌｏｗコントローラへ転送することができる。そして、ＯｐｅｎＦｌｏｗコントローラ側でこのパケットの処理を決定し、この処理に従うようＯｐｅｎＦｌｏｗ対応スイッチのフローテーブルへフローエントリを設定することができる。このようなＯｐｅｎＦｌｏｗの仕様において、ＯｐｅｎＦｌｏｗコントローラへ転送されたパケットに対して、分析装置２２において異常通信として過去に検出された情報を用いてミラーリングモードまたはインラインモードへ遷移させる制御または該当する通信を遮断する制御を行うようにしてもよい。

【０１５２】

ここで、以下の第六の実施の形態では、ＯｐｅｎＦｌｏｗの仕様において、ＯｐｅｎＦｌｏｗコントローラへ転送されたパケットに対して、分析装置２２において異常通信として過去に検出された情報を用いてミラーリングモードまたはインラインモードへ遷移させる制御を行う場合について説明する。なお、第一の実施の形態と同様の処理については説明を省略する。

【０１５３】

図２３を用いて、第六の実施の形態に係るネットワークシステムの一例について説明する。図２３は、第六の実施の形態に係るネットワークシステムにおける通信制御処理の一連の流れを説明する図である。図２３に示すように、第六の実施の形態に係るネットワークシステムでは、アノマリ情報蓄積部２７をさらに有する点が第一の実施の形態と異なる。アノマリ情報蓄積部２７は、分析装置２２によって分析された結果に基づいて、異常が

ある通信を示す情報（以下、適宜「アノマリ情報」と記載）を蓄積する。

【０１５４】

また、制御判断装置２３は、ＯｐｅｎＦｌｏｗ対応スイッチ機能を備える、通信制御装置１２からＯｐｅｎＦｌｏｗコントローラ１４を経由してパケットを受信した場合に、該パケットに含まれる情報がアノマリ情報蓄積部２７に蓄積されたアノマリ情報と一致するか否かを判定し、異常があると判断された場合には、ミラーリングモードまたはインラインモードへ遷移させる制御を通信制御装置１２、または通信制御装置１２、２５に対して行うことで、通信が通信制御装置１２から解析装置２４へ転送されるように通信制御装置１２を制御する。なお、通信制御装置２５もＯｐｅｎＦｌｏｗ対応スイッチ機能を備えていることとする。

【０１５５】

ここでアノマリ情報について具体的に説明する。アノマリ情報蓄積部２７は、例えば、図２４に例示するように、各エントリを識別する「ＩＤ」と、プロトコル番号、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号および宛先ポート番号の「５タプル情報」と、該５タプル情報に該当した場合の制御の内容である「制御内容」とを対応付けて記憶する。図２４の具体的を挙げて説明すると、アノマリ情報蓄積部２７は、例えば、ＩＤ「１」と、プロトコル番号「６（ＴＣＰ）」と、送信元ＩＰアドレス「Ａ．Ｂ．Ｃ．Ｄ」と、宛先ＩＰアドレス「Ｅ．Ｆ．Ｇ．Ｈ」と、送信元ポート番号「１００００」と、宛先ポート番号「８０」と、制御内容「ミラーリングモード」とを対応付けて記憶する。なお、５タプル情報について、ＩＰアドレスのレンジなどの範囲指定する情報であってもよい。

【０１５６】

ここで、図２４の例において、ＩＤ１、２では、プロトコル番号、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、および宛先ポート番号について、それぞれ情報を記憶しており、通信の双方向の情報を記憶していることを意味する。また、ＩＤ１、２については、５タプルの全項目と、処理対象のパケットの５タプルの全項目の情報が一致した場合に、異常がある通信に「該当」するとみなす。

【０１５７】

また、ＩＤ３、５では、プロトコル番号、宛先ＩＰアドレスおよび宛先ポート番号の３つと処理対象のパケットの情報が一致した場合に、異常がある通信に「該当」するとみなす。ＩＤ４、６では、プロトコル番号、宛先ＩＰアドレスの２つと処理対象のパケット上の情報が一致した場合に、異常がある通信に「該当」するとみなす。なお、ＩＤ３～６についても、ＩＤ１、２と同様に双方向の情報が記憶されていてもよい。

【０１５８】

通信制御装置１２は、フローエントリと呼ばれる規則に従ってパケットの転送処理を行う。フローエントリには、どういったパケットをどう処理するかに関するパケット処理の規則情報が記憶されている。例えば、通信制御装置１２が有するフローエントリには、図２５に例示するように、フローエントリを識別する「ＩＤ」と、受信したパケットにマッチするか否かを判定する条件である「マッチ条件」と、パケットがマッチ条件に合致した場合に行う処理である「アクション」と、パケットに関する統計情報である「カウンタ」とが対応付けて記憶されている。なお、図２５のテーブルをフローテーブルと呼び、フローテーブルにおける各行をフローエントリと呼ぶ。統計情報とは、パケット数やバイト数、フローエントリが登録されてからの継続時間等である。

【０１５９】

マッチ条件には、５タプルの全項目に設定されていてもよく、１以上の任意の項目のみに設定されていてもよい。さらに、マッチ条件には、パケットが入力されたＯｐｅｎＦｌｏｗ対応スイッチの入力ポートや５タプル以外のパケットヘッダ情報の項目が設定されていてもよい。また、アクションには、主に、マッチ条件にマッチしたパケットの出力先ポート、マッチしたパケットを破棄、マッチしたパケットのヘッダ内の指定のフィードを書き換える、といった処理等が設定されている。なお、フローエントリにおける統計情報に

ついては、ＯｐｅｎＦｌｏｗ対応スイッチ機能を有する通信制御スイッチ１２からＯｐｅｎＦｌｏｗコントローラ１４を介して、部分情報として分析装置２２に送信され、統計情報以外の部分情報については、収集管理装置２１または通信制御装置２５を経由して分析装置２２に送信される。

【０１６０】

図２３の説明に戻って、第六の実施の形態に係るネットワークシステムにおける通信制御処理の一連の流れを説明する。図２３に示すように、通信制御装置１２は、受信したパケットがフローテーブルに該当する規則情報がない未登録の場合（または所定のパケットに対してあらかじめ指定していた場合）、通知メッセージ（Packet　Inメッセージ）をＯｐｅｎＦｌｏｗコントローラ１４へ通知する（図２３の（１）参照）。ここで、Packet　Inメッセージとは、フローテーブル中にマッチするフローがなかった場合、受信パケットをＯｐｅｎＦｌｏｗコントローラ１４へと送るメッセージである。

【０１６１】

そして、ＯｐｅｎＦｌｏｗコントローラ１４は、制御判断装置２３へ通知メッセージに含まれる該当パケットの５タプル情報を通知する（図２３の（２）参照）。続いて、制御判断装置２３は、アノマリ情報蓄積部２７のアノマリ情報を参照して、受けた通知と照合する（図２３の（３）参照）。

【０１６２】

そして、制御判断装置２３は、５タプル情報がアノマリ情報に該当した場合には、該当する制御（ミラーモード、インラインモード、またはセキュリティ制御）を実行するよう制御命令をＯｐｅｎＦｌｏｗコントローラ１４へ送り、該当しなかった場合には、通常モードの制御を実行するよう制御命令をＯｐｅｎＦｌｏｗコントローラ１４へ送る（図２３の（４）参照）。

【０１６３】

そして、ＯｐｅｎＦｌｏｗコントローラ１４は、通知メッセージ（Packet　Inメッセージ）を受けたユーザＮＷ３０側の通信制御装置１２または通信制御装置２５へフローエントリを設定するメッセージ（Ｆｌｏｗ　Ｍｏｄメッセージ）を通知する（図２３の（５）参照）。そして、通信制御装置１２や通信制御装置２５は、メッセージ（Ｆｌｏｗ　Ｍｏｄメッセージ）を受け取ると、通信制御装置１２や通信制御装置２５のフローエントリ／フローテーブルを更新する。さらに、ＯｐｅｎＦｌｏｗコントローラ１４は、通知メッセージを送ってきた通信制御装置１２へパケット処理メッセージ（Packet　Outメッセージ）を通知する。そして、通信制御装置１２は、該パケット処理メッセージ（Packet　Outメッセージ）に従った処理をする。

【０１６４】

以降、通信制御装置１２は、更新されたフローテーブルに該当するパケットを受信した場合、ＯｐｅｎＦｌｏｗコントローラ１４へ通知することなくフローテーブルの規則情報に従ったパケット処理をする。ここで、Packet　OutメッセージとはPacket　InでＯｐｅｎＦｌｏｗコントローラ１４に送られてきたパケットを所定の宛先に送る（またはドロップするなど）ために、通信制御装置１２側へと送り返す際に用いられるメッセージである。

【０１６５】

また、ＯｐｅｎＦｌｏｗコントローラ１４は、必要に応じて、制御ＮＷ７０側の通信制御装置２５に対して該当する制御（ミラーモード、インラインモードまたはセキュリティ制御）に相当するフローエントリを設定するメッセージ（Flow　Modメッセージ：フローエントリの追加・更新・削除）を通知する（図２３の（６）参照）。制御ＮＷ７０側の通信制御装置２５のフローテーブルに静的に制御（ミラーモード、インラインモード）が設定されている場合はこの通知は不要であるが、動的に制御（ミラーモード、インラインモード）を設定する場合は、通信制御装置１２への通知とともに、この通知を行う。

【０１６６】

なお、図２３におけるネットワークシステムの構成は一例であり、これに限定されるも

のではなく、例えば、アノマリ情報蓄積部２７は制御判断装置２３に含まれていてもよいし、ＯｐｅｎＦｌｏｗコントローラ１４は制御判断装置２３に含まれていてもよいし、両者が制御判断装置２３に含まれていてもよい。

【０１６７】

このように、第六の実施の形態では、分析装置２２において異常通信として過去に検出された情報を蓄積させ、蓄積された情報を用いて、ミラーリングモードまたはインラインモードへ遷移させる制御を行うことで、初出のパケットに対しても、適切にミラーリングモードまたはインラインモードへ遷移させる制御を行うことが可能である。

【０１６８】

なお、上記した各実施の形態に記載の発明を任意に組合せて適用してよい。また、第一の実施の形態～第五の実施の形態においても、第六の実施の形態と同様に分析結果であるアノマリを示すアノマリ情報を蓄積しておいてもよく、この蓄積されたアノマリ情報を用いて、制御判断装置２３が、通信制御装置１２や２５に設定を通知して通信を制御してもよい。この場合、制御判断装置２３が通信制御装置１２から現在有効な通信（ＯｐｅｎＦｌｏｗ対応スイッチのフローテーブルに登録されている通信）に関する情報（５タプル情報など）を定期的にまたは所定の契機毎に収集して、アノマリ情報に該当する通信がある場合は、この通信を制御の対象としてもよい。また、ＯｐｅｎＦｌｏｗ対応スイッチのフローテーブルは、例えば通信制御装置１２の記憶部１２ａ、通信制御装置２５の２５ｂが該当することとなる。

【０１６９】

以上、本発明をいくつかの実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に多様な変更または改良を加えることが可能であることが当業者には明らかである。また、そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【０１７０】

［セキュリティ制御］

例えば、上記の実施の形態では、通信制御装置１２でパケットをフィルタリングすることとしていたが、該当通信を行っている端末を図示しない検疫ＮＷに接続させて、端末内部のセキュリティチェックを実施して、必要に応じてマルウェア除去やセキュリティのアップデートを強制することとしてもよい。

【０１７１】

通常モードとミラーリングモードの場合、セキュリティ制御は、通信装置１０の通信制御装置１２に対して制御命令を送信し、この通信制御装置１２で実施する。一方、インラインモードの場合、悪性通信や怪しい通信と判定された場合、解析装置２４でまず遮断してそのあとで、通信装置１０の通信制御装置１２にセキュリティ制御を反映させる制御命令を送信することとしてもよい。この場合、判定から遮断までのタイムラグがなくなる。または、セキュリティ制御を通信装置１０の通信制御装置１２で行うこととする場合は、通常モードやミラーリングモードと同様の扱いとしてもよい。また、あるユーザＮＷ３０の通信において解析結果で黒判定となった場合のセキュリティ制御は、当該ユーザＮＷ３０だけではなく他のユーザＮＷ３０にも適用されてもよい。制御判断装置２３によりセキュリティ制御の対象を通信制御装置１２、２５として説明してきたが、少なくとも通信制御装置１２のみを対象とするものであってもよい。なお、インラインモードにおける解析装置２４の位置は、端末４０とインターネット上のサイト５０の間にインライン接続する形で配置されるため、解析装置２４が受信した通信トラフィックはそのまま透過して送信されるが（解析装置２４が悪性通信であると判断した場合は自らその通信を遮断してもよい）、ミラーリングモードでは、ミラーリングコピーされた通信トラフィックを解析装置２４が受信するため解析後は破棄されることとなる。

【０１７２】

［通信モードの遷移］

通信モードの遷移については、通常モードとミラーリングモードとインラインモードの３つのモード間を遷移する構成でもよいし、通常モードとミラーリングモード、通常モードとインラインモードの２つのモード間を遷移する構成でもよい。３つのモード間を遷移する場合には、任意のモードから任意のモードへ遷移する構成でもよく、この任意の遷移の構成から、インラインモードからミラーリングモードへの遷移を除く構成でもよく、また、この任意の遷移の構成から、通常モードからインラインモードへの遷移やインラインモードからミラーリングモードへの遷移を除く構成でもよい。図４中の実線・破線は遷移の推移を示す一例であり、破線の遷移は省略されることとしてもよい。または、これらを組み合わせた構成でもよい。

【０１７３】

また、セキュリティ制御命令の後について、命令に該当する通信を遮断したのち、即時通常モードに戻してもよい。または、該当通信を遮断したあと、インラインモード（またはミラーリング）を継続し、解析装置２４において白判定が所定期間続いた場合や黒や灰の判定が所定期間出力されなかった場合に通常モードに戻すこととしてもよい。また、収集装置１１と収集管理装置２１の間の部分情報や収集ルールに関する通信や、通信制御装置１２と２５の間の通信は、それぞれ暗号化されていてもよい。

【０１７４】

［特徴ベクトルの生成］

上記の実施形態では、収集装置１１が特徴ベクトルを生成して、収集管理装置２１に送信する場合を説明したが、これに限定されるものではない。例えば、収集装置１１が特徴ベクトル化に必要な情報を収集管理装置２１に送信し、これを受信した収集管理装置が特徴ベクトル化して分析装置へ渡すこととしてもよい。

【０１７５】

［ミラーリングモードやインラインモード］

通信装置１０を経由する全通信トラフィックをこれらの通信モードの通信制御対象としてもよいが、ユーザＮＷ３０内の端末同士の通信は安全であるなどとみなして、内部ＮＷと外部ＮＷとの間の通信のみを通信モード制御の対象とすることとしてもよい。また特定の宛先および／または送信元との通信や特定のプロトコル、サービス、アプリケーションの通信のみを通信モード制御の対象とすることとしてもよい。この場合の対象外の通信トラフィックは、通常モードと同様に、送信元と宛先の間を通信装置１０を介して通信する。これらは、制御判断装置２３からの制御命令の内容に基づいて対象が決定される。なお、収集する通信についても、内部ＮＷと外部ＮＷとの間の通信のみを収集の対象とすることとしてもよく、収集ルールに内部ＮＷと外部ＮＷとの間の通信のみを収集するルールが記述されていてもよい。

【０１７６】

３つの通信モード制御の設定について、制御判断装置２３にＯｐｅｎＦｌｏｗコントローラが配置され、通信制御装置１２、２５にＯｐｅｎＦｌｏｗ対応スイッチが配置されている場合の制御について、説明する。

【０１７７】

基本となる通常モードでは、通信制御装置１２は一般的なスイッチングの機能を実現する。通常モードでは通信制御装置２５は特に動作することはない。ミラーリングモードでは、ＯｐｅｎＦｌｏｗコントローラからの命令により、通信制御装置１２の記憶部１２ａには、内部ＮＷと通信する通信インターフェースや外部ＮＷと通信する通信インターフェースから受信した通信トラフィックを宛先に転送するとともに、トンネル対向（通信制御装置２５側）にも転送するよう制御するためのフローエントリが書き込まれる。通信制御装置２５の記憶部２５ｂには、トンネル対向（通信制御装置１２側）から受信する通信トラフィックを解析装置２４側に転送するよう制御するためのフローエントリが書き込まれる。

【０１７８】

インラインモードでは、通信制御装置１２の記憶部１２ａには、内部ＮＷと通信する通

信インターフェースが受信した通信トラフィックまたは外部ＮＷと通信する通信インターフェースが受信した通信トラフィック（トンネル対向からの通信トラフィックではない）をトンネル対向（通信制御装置２５側）へ転送し、トンネル対向（通信制御装置２５側）から受信した通信トラフィックを当該通信トラフィックの宛先へ転送するよう制御するためのフローエントリが書き込まれる。通信制御装置２５の記憶部２５ｂには、トンネル対向（通信制御装置１２側）から受信した通信トラフィックを解析装置２４側へ転送し、解析装置２４側から戻ってきた通信トラフィックをトンネル対向（通信制御装置１２側）へ転送するよう制御するためのフローエントリが書き込まれる。

【０１７９】

ここで、フローエントリとは、ＯｐｅｎＦｌｏｗコントローラから受け付ける制御ルールであり、マッチングルールとアクションを含む構成であって、入力された通信トラフィックがマッチングルールに設定された条件に該当する場合、この通信トラフィックはこのマッチングルールに対応するアクションに設定されている制御が実行される。例えば、マッチングルールには、主にレイヤ１からレイヤ４の情報である、パケットが入力されたＯｐｅｎＦｌｏｗ対応スイッチのポート、パケットの送信元や宛先のＭＡＣアドレス、ＩＰアドレス、ポート番号といった情報のうちの１以上の組を条件として記述できる。また、アクションには、マッチングルールに該当したパケットを指定した出力先のポートへ転送する、または該当したパケットを転送せずにドロップする等といった動作を指定できる。

【０１８０】

なお、ミラーリングモードやインラインモードにおいて、全通信トラフィックを制御対象としてもよいが、特定の宛先や送信元、サービス（ポート番号）の通信トラフィックのみを制御の対象としてもよい。フローエントリに設定をすることで個別の制御は可能である。この場合、これらの個別の制御対象以外の通信トラフィックは通常モードとして制御されることになる。

【０１８１】

通信トラフィックのパケットの宛先アドレス等を書き換えて変更するのではなく、転送先のポートを指定することで転送の制御を行えるようにするのが望ましい。これはパケットを書き換えてしまうと適切な解析を阻害する可能性があるためである。したがって、例えばトンネル構築にはトンネル用のポートまたは通信インターフェースを用意するのが望ましい。

【０１８２】

通信モードを変更する場合、ＯｐｅｎＦｌｏｗコントローラは制御したい通信モードに該当するフローエントリを書き込むよう各ＯｐｅｎＦｌｏｗ対応スイッチに命令することなる。

【０１８３】

ＯｐｅｎＦｌｏｗコントローラが制御判断装置２３ではなく各通信制御装置に配置される構成の場合は、制御判断装置２３は、これらの制御をするよう各ＯｐｅｎＦｌｏｗコントローラに命令することになる。そして、各ＯｐｅｎＦｌｏｗコントローラは同じ装置内のＯｐｅｎＦｌｏｗ対応スイッチに対してフローエントリを書き込むことになる。

【０１８４】

セキュリティ制御では、解析結果として、制限すべきと判定された通信の宛先や送信元のＩＰアドレスやポート番号などを基にこの通信を遮断するため、これらの情報を用いてフィルタリングの設定をする。ＯｐｅｎＦｌｏｗの仕様を利用する場合はＯｐｅｎＦｌｏｗコントローラからＯｐｅｎＦｌｏｗ対応スイッチに対してこの設定に該当するフローエントリを書き込むこと、ＯｐｅｎＦｌｏｗ対応スイッチはフィルタリングを実施する。

【０１８５】

また、上記実施の形態では、異常検知やクラスタリングといった機械学習を基にして適用する通信モードを判断したが、これに限らず、部分情報を基に所定の条件を満たす通信であると分析した場合は、通信モードを変更する構成をとってもよい。例えば、この所定の条件をルールとして記述して、分析装置２２の記憶部２２ｂに記憶しておき、分析／学

習部２２ａがこのルールと入力される部分情報を照合することで分析結果を出力し、制御判断装置２３がこの分析結果を基に通信モードを判断することとしてもよい。これは明示的なルール、例えば、最近よくサイバー攻撃に悪用されているＵＲＬやＦＱＤＮ、ドメイン、またはＩＰアドレスやそのレンジ、国や地域やとの通信を示す部分情報を受付けた場合は、このルールに適合するため、通常モードからミラーリングモードまたはインラインモードへ変更することとしてもよい。また、これらも含めて異常として扱うこととしてもよい。機械学習でクラスタリングを適用する場合、特定のクラスタに分類された入力情報を異常として扱うこととしてもよい。

【０１８６】

［部分情報等］

また、部分情報は、ユーザＮＷ３０側の通信装置を流れる通信トラヒックの一部の通信であればよい。例えば、５タプルを組として該当する通信の開始時間、終了時間、その間に流れた総パケット数、総データサイズ等の統計情報でもよい。また、例えば、端末Ａ、Ｂ間の通信において、通信の向き毎（Ａ→Ｂ、Ｂ→Ａ）に統計情報を算出してもよい。なお、この情報はOpenFlowの仕様で収集可能な情報であるものとする。

【０１８７】

また、部分情報は、端末が送受信する通信のうちの特定の通信そのものでもよい。例えば、ＤＮＳ等の通信は常に収集管理装置または分析装置へミラーリングされることとしてもよい。この場合、要求パケットと応答パケットから解決したい名前と解決されたＩＰアドレスを含む情報を対応付けて記憶する。または特徴ベクトルを構成してもよいし、名前やＩＰアドレスを分析や機械学習の対象とすることとしてもよい。

【０１８８】

また、部分情報は、上記したユーザＮＷ側の通信装置を流れる通信トラヒックの一部の通信と、特定の通信そのものの組み合わせでもよい。また、OpenFlowを基に説明したが、これに限らず代替可能なＳＤＮ（Software Defined Networking）技術または本発明を実現できる機能を有する技術であれば代替してもよい。

【０１８９】

［装置構成等］

通信装置１０や制御装置２０は、内包する各機能（装置）を物理的・仮想的に分散可能であり、その際は両装置内の各機能（装置）が各々一つの単位として分散されることとしてもよい。また、例えば、収集管理装置２１は省略可能であり、収集部２１ａは分析装置２２に、抽出制御部２１ｂは制御判断装置２３に組み込まれることとしてもよい。また各装置内の各部は、有効に機能する程度において別の各装置に組み込まれる構成をとってもよい。

【０１９０】

［プログラム］

また、上記実施の形態に係る通信装置１０や制御装置２０が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。この場合、コンピュータがプログラムを実行することにより、上記実施の形態と同様の効果を得ることができる。さらに、かかるプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータに読み込ませて実行することにより上記実施の形態と同様の処理を実現してもよい。以下に、通信装置１０や制御装置２０と同様の機能を実現する通信制御プログラムを実行するコンピュータの一例を説明する。

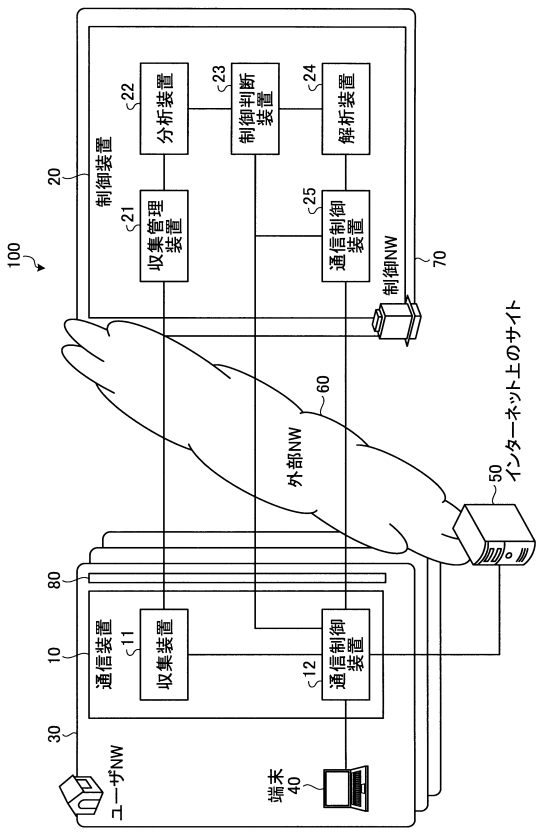
【０１９１】

図２６は、通信制御プログラムを実行するコンピュータを示す図である。図２６に示すように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有する。これらの各部は、バス１０８０によって接続される。

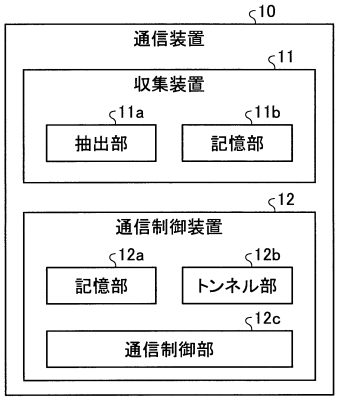
【０１９２】
メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１およびＲＡＭ（Random Access Memory）１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、ハードディスクドライブ１０９０に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１０４１に接続される。ディスクドライブ１０４１には、例えば、磁気ディスクや光ディスク等の着脱可能な記憶媒体が挿入される。シリアルポートインタフェース１０５０には、例えば、マウス１１１０およびキーボード１１２０が接続される。ビデオアダプタ１０６０には、例えば、ディスプレイ１１３０が接続される。
【０１９３】
ここで、図２６に示すように、ハードディスクドライブ１０９０は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３およびプログラムデータ１０９４を記憶する。上記実施の形態で説明した各テーブルは、例えばハードディスクドライブ１０９０やメモリ１０１０に記憶される。
【０１９４】
また、通信制御プログラムは、例えば、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、ハードディスクドライブ１０９０に記憶される。具体的には、上記実施の形態で説明したネットワークシステムの各装置が実行する各処理が記述されたプログラムモジュールが、ハードディスクドライブ１０９０に記憶される。
【０１９５】
また通信制御プログラムによる情報処理に用いられるデータは、プログラムデータとして、例えば、ハードディスクドライブ１０９０に記憶される。そして、ＣＰＵ１０２０が、ハードディスクドライブ１０９０に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出して、上述した各手順を実行する。
【０１９６】
なお、通信制御プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０９０に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ１０４１等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、通信制御プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ＬＡＮ（Local Area Network）やＷＡＮ（Wide Area Network）等のネットワークを介して接続された他のコンピュータに記憶され、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。
【符号の説明】
【０１９７】
１０　通信装置
１１　収集装置
１１ａ　抽出部
１１ｂ、１２ａ、２２ｂ、２３ｃ、２５ｂ　記憶部
１２、２５　通信制御装置
１２ｂ、２５ａ　トンネル部
１２ｃ、２５ｃ　通信制御部
１４　ＯｐｅｎＦｌｏｗコントローラ
２０　制御装置
２１　収集管理装置
２１ａ　収集部
２１ｂ　抽出制御部

２２　分析装置
２２ａ　分析／学習部
２３　制御判断装置
２３ａ　判断部
２３ｂ　制御命令部
２４　解析装置
２４ａ　詳細解析部
２６　暗号通信検査装置
２７　アノマリ情報蓄積部
１００　ネットワークシステム

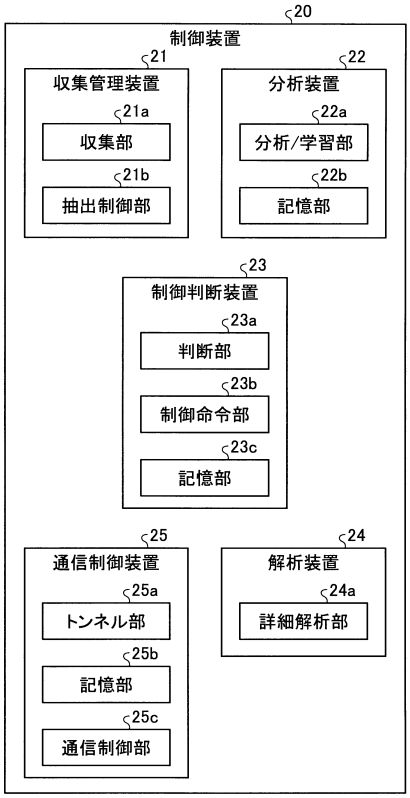
【図１】



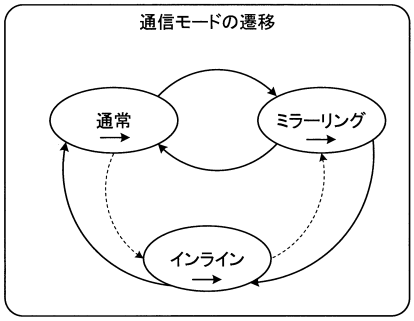
【図２】



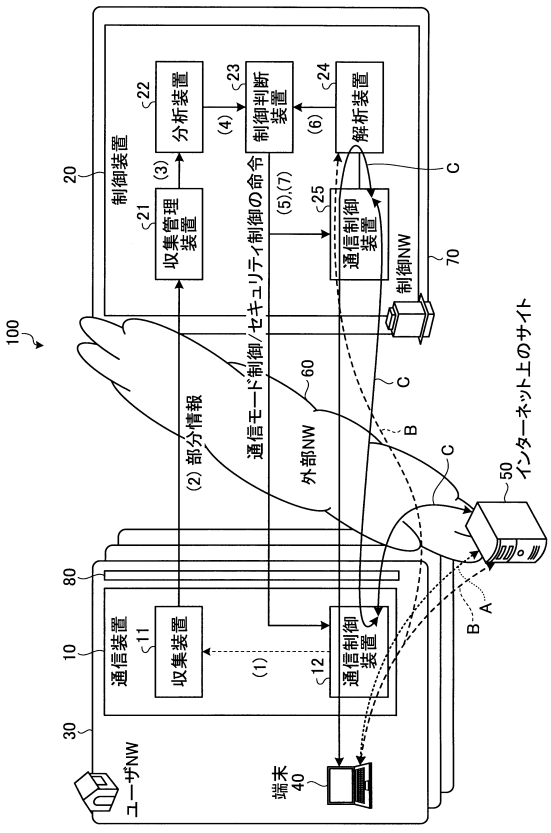
【図３】


20
制御装置
21
収集管理装置
21a
収集部
21b
抽出制御部
22
分析装置
22a
分析/学習部
22b
記憶部
23
制御判断装置
23a
判断部
23b
制御命令部
23c
記憶部
25
通信制御装置
25a
トンネル部
25b
記憶部
25c
通信制御部
24
解析装置
24a
詳細解析部

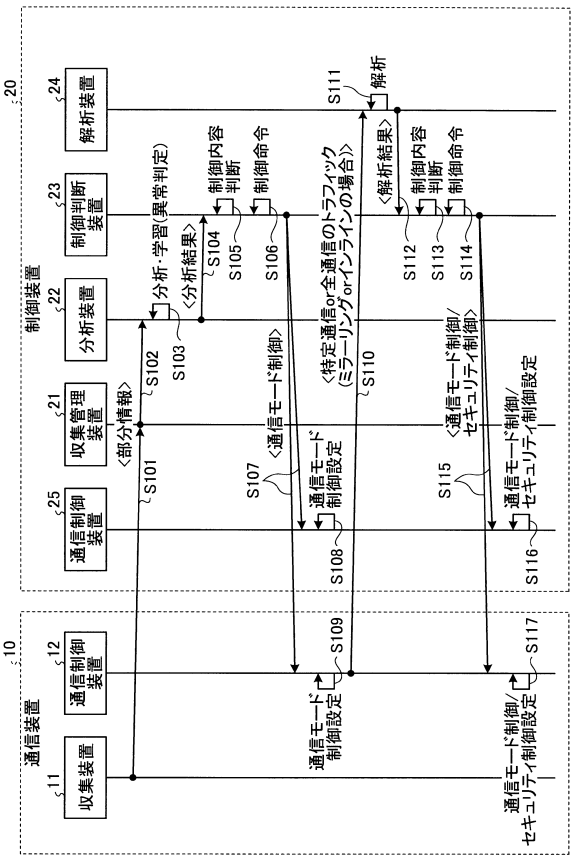
【図４】


通信モードの遷移
通常
ミラーリング
インライン

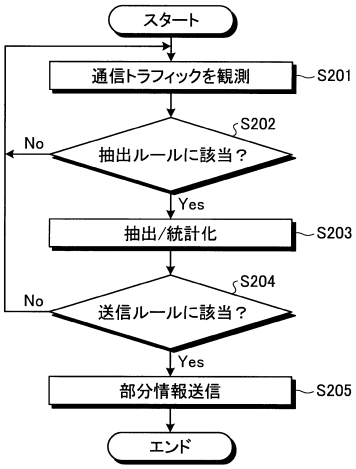
【図５】


100
制御装置
20
収集管理装置
21
分析装置
22
制御判断装置
23
解析装置
24
通信制御装置
25
制御NW
70
外部NW
60
通信モード制御/セキュリティ制御の命令
(1)
(2) 部分情報
(3)
(4)
(5),(7)
(6)
通信装置
10
収集装置
11
通信制御装置
12
80
30
ユーザNW
端末
40
インターネット上のサイト
50
A
B
C

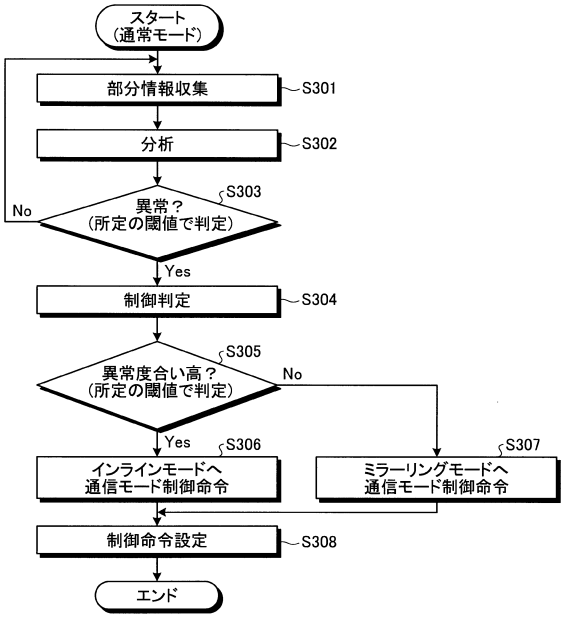
【図６】


制御装置
20
通信装置
10
収集管理装置
21
分析装置
22
制御判断装置
23
解析装置
24
通信制御装置
25
収集装置
11
通信制御装置
12
〈部分情報〉
分析・学習(異常判定)
〈分析結果〉
制御内容判断
制御命令
〈通信モード制御〉
通信モード制御設定
〈特定通信or全通信のトラフィック(ミラーリングorインラインの場合)〉
解析
〈解析結果〉
通信モード制御/セキュリティ制御
通信モード制御/セキュリティ制御設定
S101
S102
S103
S104
S105
S106
S107
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117

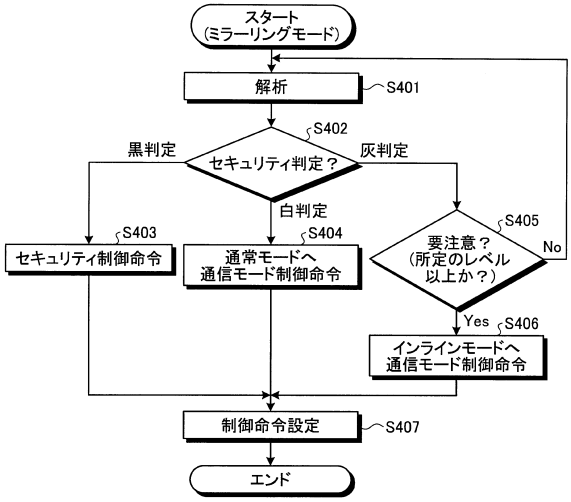
【図７】


スタート
通信トラフィックを観測
S201
S202
抽出ルールに該当？
No
Yes
抽出/統計化
S203
S204
送信ルールに該当？
No
Yes
部分情報送信
S205
エンド

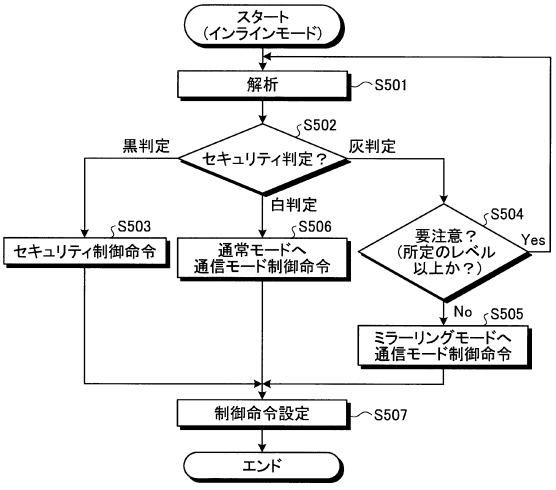
【図８】


スタート
(通常モード)
部分情報収集
S301
分析
S302
S303
異常？
(所定の閾値で判定)
No
Yes
制御判定
S304
S305
異常度合い高？
(所定の閾値で判定)
No
Yes
S306
インラインモードへ
通信モード制御命令
S307
ミラーリングモードへ
通信モード制御命令
制御命令設定
S308
エンド

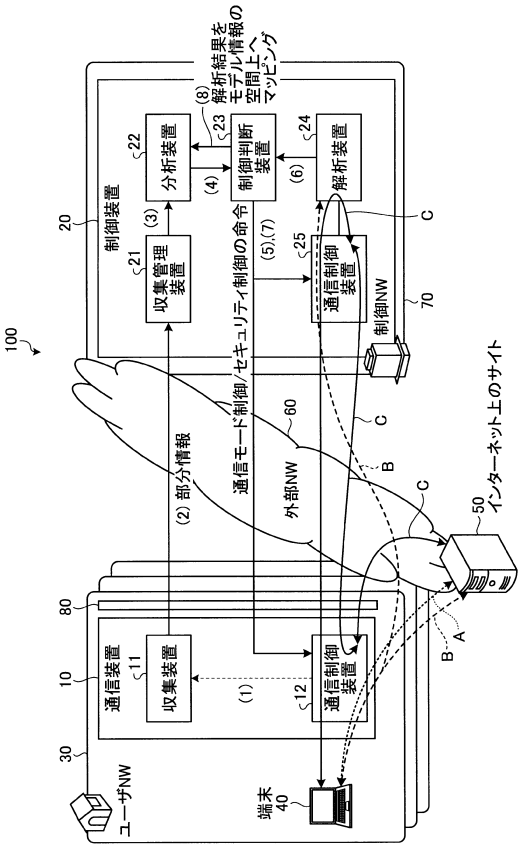
【図９】


スタート
(ミラーリングモード)
解析
S401
S402
セキュリティ判定？
黒判定
灰判定
白判定
S403
セキュリティ制御命令
S404
通常モードへ
通信モード制御命令
S405
要注意？
(所定のレベル
以上か？)
No
Yes
S406
インラインモードへ
通信モード制御命令
制御命令設定
S407
エンド

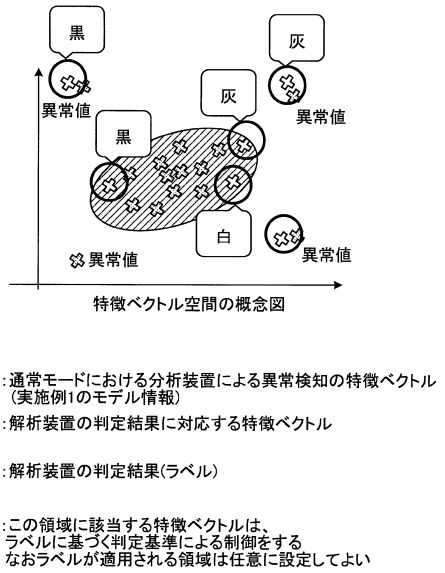
【図１０】


スタート
(インラインモード)
解析
S501
S502
セキュリティ判定？
黒判定
灰判定
白判定
S503
セキュリティ制御命令
S506
通常モードへ
通信モード制御命令
S504
要注意？
(所定のレベル
以上か？)
Yes
No
S505
ミラーリングモードへ
通信モード制御命令
制御命令設定
S507
エンド

【図１１】



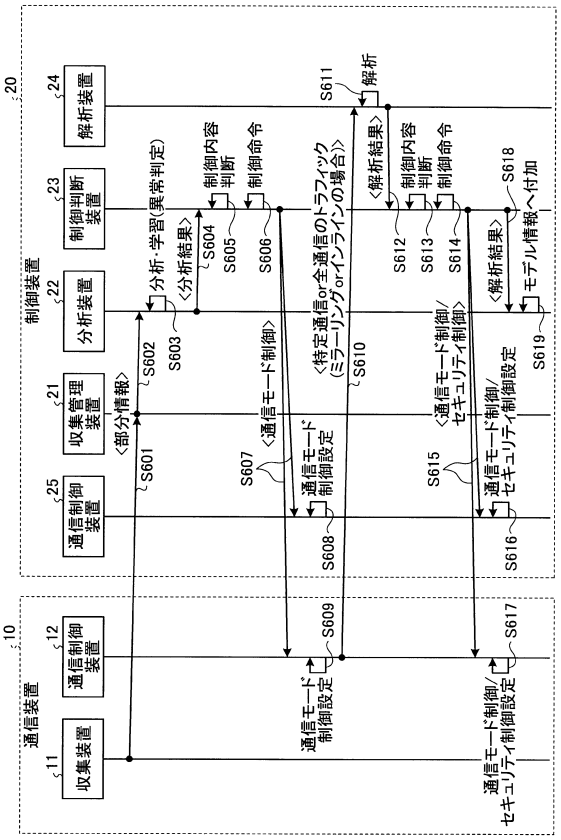
【図１２】



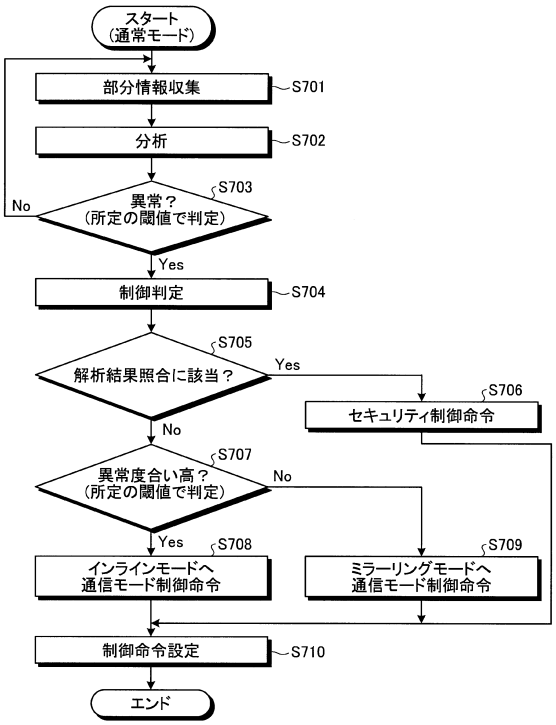
【図１３】

		モデル情報	
		異常と判定される空間領域	異常と判定されない空間領域
マッピング情報	白判定	通常モード（またはミラーリングモード）	通常モード
	灰判定	インラインモード（またはミラーリングモード）	ミラーリングモード（またはインラインモード）
	黒判定	セキュリティ制御（またはインラインモード、ミラーリングモード）	セキュリティ制御（またはインラインモード、ミラーリングモード）

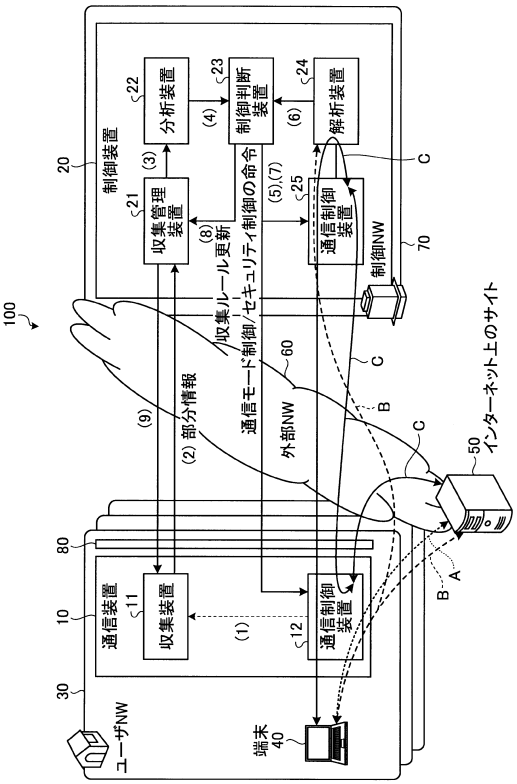
【図１４】



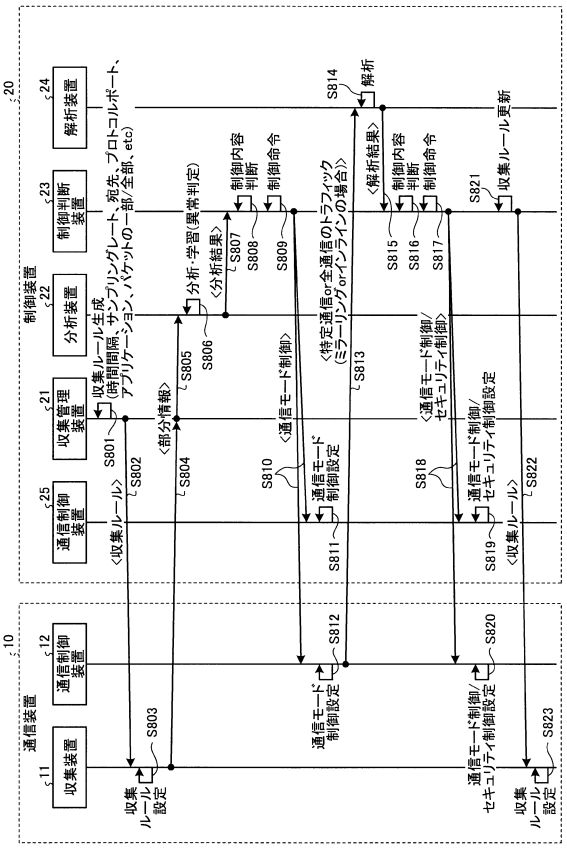
【図１５】



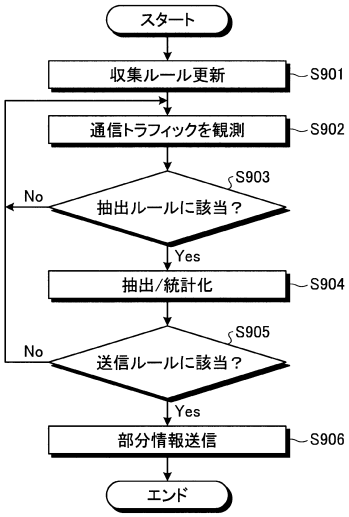
【図１６】



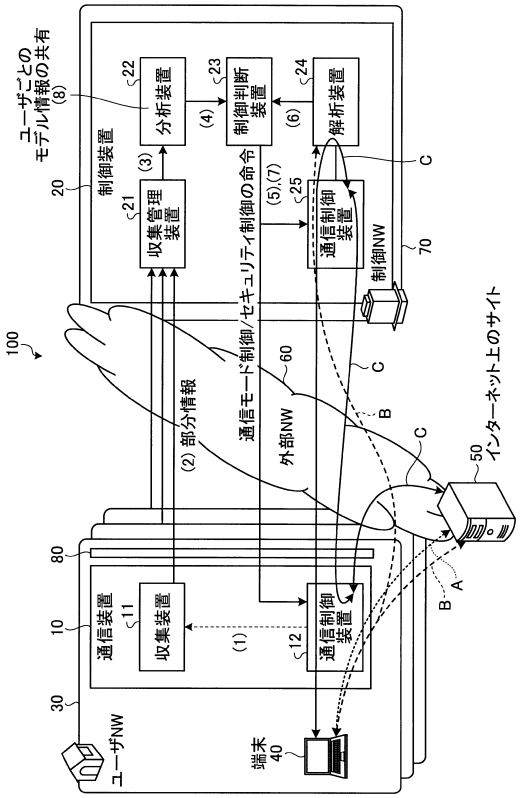
【図１７】



【図１８】



【図１９】



【図２０】

集合の類似度

次に示す3つの類似性指標は、もともと2つの集合の要素の一致度を示すものであるが、コサイン類似度に似た定義式をもっており、ある種のベクトルの類似度としても使うことができる

・ジャッカード係数
集合XとYの共通要素数を少なくとも1方にある要素の総数で割ったもの

$$sim=|X\cap Y|/|X\cup Y|$$

を、ジャッカード係数という
今、X∪Yの要素をz1,z2,…,znとして、ベクトルx=(x1,x2,…,xn)を、
xi=1 (if zi∈X),xi=0 (otherwise)として定める
ベクトルyも同様に定めると、ジャッカード係数は、

$$sim= x\cdot y/(\Sigma xi+\Sigma yi-x*y)$$

とあらわされる

・ダイス係数
集合XとYの共通要素数を各集合の要素数の平均で割ったもの

$$sim=2*|X\cap Y|/(|X|+|Y|)$$

を、ダイス係数という
X,Yに対応するベクトルx,yを使えば、

$$sim= 2*x\cdot y/(\Sigma xi+\Sigma yi)$$

とあらわされる

・シンプソン係数
集合XとYの共通要素数を各集合の要素数の最小値で割ったもの

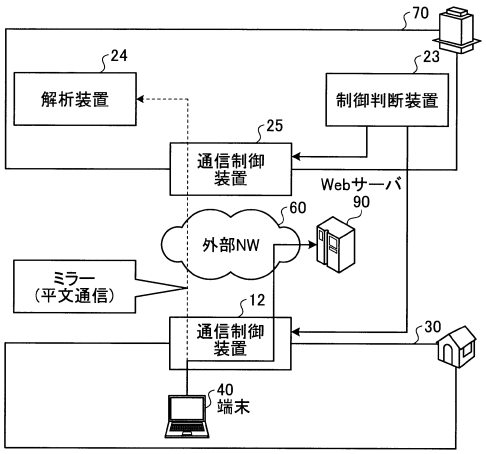
$$sim=|X\cap Y|/min(|X|,|Y|)$$

を、シンプソン係数という
X,Yに対応するベクトルx,yを使えば、

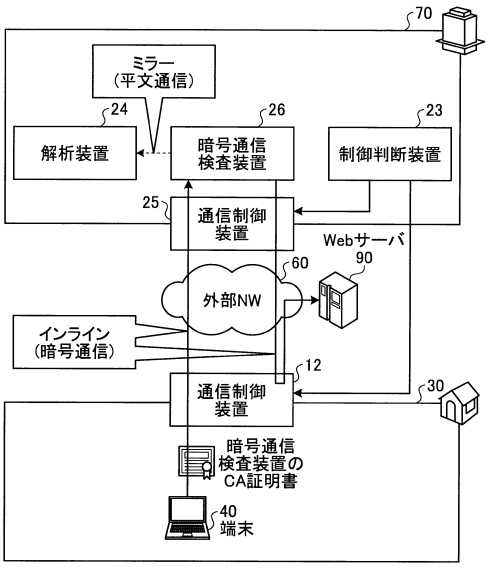
$$sim= x\cdot y/min(\Sigma xi, \Sigma yi)$$

とあらわされる

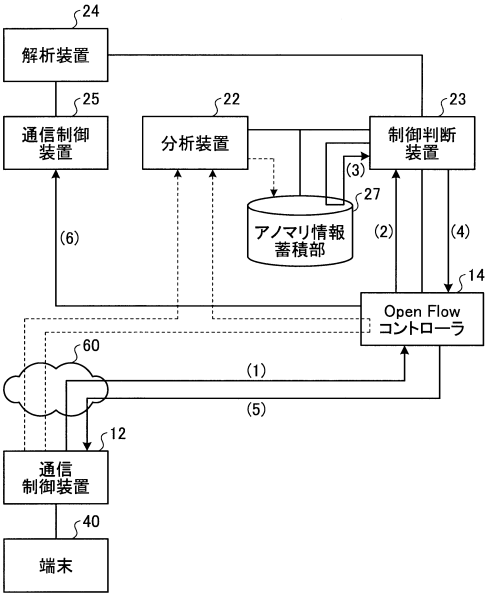
【図２１】



【図２２】



【図２３】



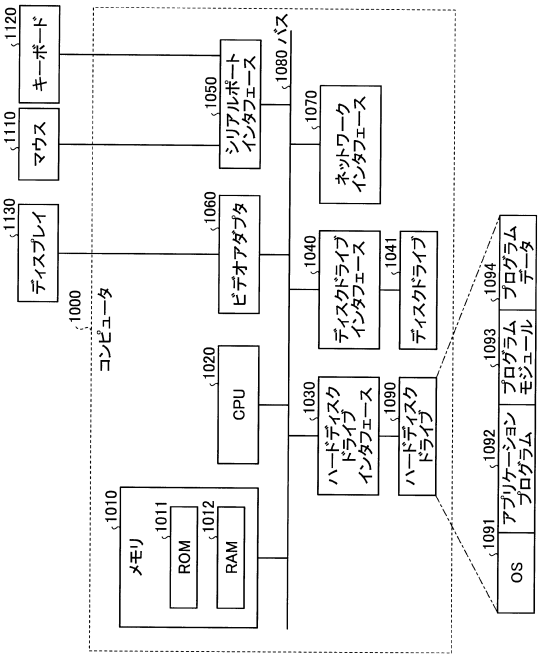
【図２４】

ID	5タプル情報					制御内容
	プロトコル番号	送信元IPアドレス	宛先IPアドレス	送信元ポート番号	宛先ポート番号	
1	6(TCP)	A.B.C.D	E.F.G.H	10000	80	ミラーリングモード
2	6(TCP)	E.F.G.H	A.B.C.D	80	10000	ミラーリングモード
3	6(TCP)		I.J.K.L		80	ミラーリングモード
4	17(UDP)		M.N.O.P			インラインモード
5	6(TCP)		Q.R.S.T		443	インラインモード
6	6(TCP)		U.V.W.X			セキュリティ制御（パケットドロップ（遮断））
…						

【図２５】

ID	マッチ条件										カウンタ(統計情報)				アクション
	パケットを受信したスイッチのポート番号	送信元MACアドレス	宛先MACアドレス	プロトコル番号	送信元IPアドレス	宛先IPアドレス	送信元ポート番号	宛先ポート番号	…		受信パケット数	受信バイト数	フローが有効になってからの経過時間	…	
1															
2															
3															
…															

【図２６】



フロントページの続き

(72)発明者　五十嵐　弓将
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　比戸　将平
アメリカ合衆国,　カリフォルニア州　９４４０２,　サン・マテオ,　サウス・エル・カミノ・リアル　５２０，スイート　６５５,　プリファード　ネットワークス　アメリカ社内

審査官　衣鳩　文彦

(56)参考文献　特開２００９－１１７９２９（ＪＰ，Ａ）
特開２０１３－１９２１２８（ＪＰ，Ａ）
特開２００７－２４３４５９（ＪＰ，Ａ）
濱田　貴広　他，ホームネットワーク仮想化システムのネットワークセキュリティに関する一考察，電子情報通信学会２０１４年総合大会講演論文集　通信2，２０１４年　3月　4日，p.224
小宮　康裕　他，クラウドコンピューティングにおけるセキュリティＳａａＳの基本検討，情報処理学会研究報告　平成２２年度１　［ＣＤ－ＲＯＭ］　情報処理学会研究報告　コンピュータセキュリテ，２０１０年　6月１５日，p.1～6，3ページ左欄～5ページ左欄「４．提案方式」

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　１２／００～１２／９５５