(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7150552号
(P7150552)

(45)発行日　令和4年10月11日(2022.10.11)

(24)登録日　令和4年9月30日(2022.9.30)

(51)国際特許分類
Ｈ０４Ｌ　12/22　(2006.01)

ＦＩ
Ｈ０４Ｌ　12/22

請求項の数　11　（全49頁）

(21)出願番号　特願2018-188227(P2018-188227)
(22)出願日　平成30年10月3日(2018.10.3)
(65)公開番号　特開2019-213182(P2019-213182A)
(43)公開日　令和1年12月12日(2019.12.12)
審査請求日　令和3年4月20日(2021.4.20)
(31)優先権主張番号　特願2017-230201(P2017-230201)
(32)優先日　平成29年11月30日(2017.11.30)
(33)優先権主張国・地域又は機関
日本国(JP)
(31)優先権主張番号　特願2018-107964(P2018-107964)
(32)優先日　平成30年6月5日(2018.6.5)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　514136668
パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ
Ｐａｎａｓｏｎｉｃ Ｉｎｔｅｌｌｅｃｔｕａｌ Ｐｒｏｐｅｒｔｙ Ｃｏｒｐｏｒａｔｉｏｎ ｏｆ Ａｍｅｒｉｃａ
アメリカ合衆国 ９０５０４ カリフォルニア州，トーランス，スイート ４５０，ウエスト　１９０ストリート ２０５０
(74)代理人　100109210
弁理士　新居 広守
(74)代理人　100137235
弁理士　寺谷 英作
(74)代理人　100131417
弁理士　道坂 伸一

最終頁に続く

(54)【発明の名称】　ネットワーク防御装置およびネットワーク防御システム

(57)【特許請求の範囲】

【請求項１】

複数のＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）のポートを備え、通信ネットワーク間の接続を行うスイッチを流れる、少なくとも送信元端末の情報と送信先端末の情報とを含む通信データを、プロミスキャスモードで前記スイッチを介して取得する通信データ取得部と、

前記通信データの脅威を検知する脅威検知部と、

脅威除去部と、

前記脅威検知部で脅威を検知した場合、前記脅威除去部を介さずに前記送信元端末と前記送信先端末とを接続する第１の通信経路を、前記脅威除去部を介して前記送信元端末と前記送信先端末とを接続した、前記第１の通信経路と異なる第２の通信経路に変更するように前記スイッチを操作する経路変更部と、を備え、

前記脅威除去部は、前記経路変更部が通信経路を変更した後に、前記通信データの脅威を除去する、

ネットワーク防御装置。

【請求項２】

前記スイッチは、前記送信元端末に接続された第１のＬＡＮのポートと、前記脅威除去部に接続された第２のＬＡＮのポートおよび第３のＬＡＮのポートと、前記送信先端末に接続された第４のＬＡＮのポートとを有し、

前記脅威検知部で脅威を検知していない場合、前記経路変更部は、前記第１のＬＡＮの

ポートに接続された前記送信元端末から、前記第４のＬＡＮのポートに接続された前記送信先端末までの前記第１の通信経路を、第１のＶＬＡＮ（Ｖｉｒｔｕａｌ　Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）に設定し、

前記脅威検知部で脅威を検知した場合、前記経路変更部は、前記第２の通信経路に含まれる、前記第１のＬＡＮのポートに接続された前記送信元端末から、前記第２のＬＡＮのポートに接続された前記脅威除去部までの経路を前記第１のＶＬＡＮと異なる第２のＶＬＡＮに設定し、前記第３のＬＡＮのポートに接続された前記脅威除去部から、前記第４のＬＡＮのポートに接続された前記送信先端末までの経路を前記第１のＶＬＡＮに設定する、

請求項１記載のネットワーク防御装置。

【請求項３】

さらに、前記脅威除去部を通過した前記通信データに含まれる通信ネットワークのＶＬＡＮ情報を書き換える書換部を備え、

前記スイッチは、前記送信元端末に接続された第５のＬＡＮのポートと、前記脅威除去部が接続された第６のＬＡＮのポートと、前記送信先端末に接続された第７のＬＡＮのポートとを有し、

前記脅威検知部で脅威を検知していない場合、前記経路変更部は、前記第５のＬＡＮのポートに接続された前記送信元端末と、前記第７のＬＡＮのポートに接続された前記送信先端末とを第１のＶＬＡＮに設定し、

前記脅威検知部で脅威を検知した場合、

前記経路変更部は、前記第２の通信経路に含まれる、前記第５のＬＡＮのポートに接続された前記送信元端末を前記第１のＶＬＡＮと異なる第２のＶＬＡＮに設定し、前記第７のＬＡＮのポートに接続された前記送信先端末を前記第１のＶＬＡＮに設定し、

前記書換部は、前記第６のＬＡＮのポートを介して、前記送信元端末が属する前記第２のＶＬＡＮを示すＶＬＡＮ情報を前記送信先端末が属する前記第１のＶＬＡＮを示すＶＬＡＮ情報に書き換え、書き換えられた通信データを、前記スイッチに出力する、

請求項１記載のネットワーク防御装置。

【請求項４】

前記第１のＶＬＡＮは、前記脅威除去部を介さない通常系ネットワークであり、

前記第２のＶＬＡＮは、前記脅威除去部が前記通信データの脅威を除去する検疫系ネットワークであり、

前記脅威検知部で脅威を検知した場合、前記経路変更部は、前記第１のＶＬＡＮの一部を前記通常系ネットワークから検疫系ネットワークに変更する、

請求項２又は３記載のネットワーク防御装置。

【請求項５】

前記脅威除去部において、前記通信データの脅威が除去されると、前記経路変更部は、前記通常系ネットワークから変更されていた前記検疫系ネットワークを、前記通常系ネットワークに戻す、

請求項４記載のネットワーク防御装置。

【請求項６】

前記通信データ取得部は、前記通信データのコピーを取得し、

前記脅威検知部は、前記通信データのコピーをプロミスキャスモードで監視する、

請求項１～５のいずれか１項に記載のネットワーク防御装置。

【請求項７】

前記脅威除去部は、脅威を検知した前記通信データから、脅威を含む不要なデータを除去する、

請求項１～６のいずれか１項に記載のネットワーク防御装置。

【請求項８】

前記脅威検知部は、検知した脅威内容に応じて、脅威が検知された送信元端末にスコアを付与し、

前記経路変更部は、前記脅威検知部で付与した前記スコアが第１の値を超えた場合、前

記スコアが付与された当該送信元端末に係る通信データを前記脅威除去部に経由させるように、前記スイッチに通信経路を変更させる、
請求項１～７のいずれか１項に記載のネットワーク防御装置。
【請求項９】
前記脅威検知部は、付与した前記スコアに対して、所定時間経過後に前記スコアを所定値減算し、
脅威が検知された前記送信元端末の前記スコアが第２の値を下回った場合、前記経路変更部は、前記送信元端末と前記送信先端末との接続を、前記脅威除去部を介さないように前記スイッチに通信経路を変更させる、
請求項８記載のネットワーク防御装置。
【請求項１０】
前記脅威検知部は、脅威が検知された前記送信元端末の前記スコアが前記第１の値より大きい第３の値を超えた場合、前記所定時間経過しても前記スコアを減算しない、
請求項９記載のネットワーク防御装置。
【請求項１１】
複数のＬＡＮのポートを備え、通信ネットワーク間の接続を行うスイッチを流れる、少なくとも送信元端末の情報と送信先端末の情報とを含む通信データを、プロミスキャスモードで前記スイッチを介して取得する通信データ取得部と、
前記通信データの脅威を検知する脅威検知部と、
脅威除去部と、
前記脅威検知部で脅威を検知した場合、前記脅威除去部を介さずに前記送信元端末と前記送信先端末とを接続する第１の通信経路を、前記脅威除去部を介して前記送信元端末と前記送信先端末とを接続した、前記第１の通信経路と異なる第２の通信経路に変更するように前記スイッチを操作する経路変更部と、を備え、
前記脅威除去部は、前記経路変更部が通信経路を変更した後に、前記通信データの脅威を除去する、
ネットワーク防御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、通信ネットワークを監視し、通信を制御するためのネットワーク防御装置およびネットワーク防御システムに関するものである。
【背景技術】
【０００２】
昨今、ネットワーク技術の発達に応じて、様々な機器がネットワークに接続されるようになっている。それに伴い、マルウェア感染、マルウェアの外部からの侵入などの攻撃による被害も増大し、セキュリティ対策が非常に重要になっている。
【０００３】
一般的にセキュリティ対策としては、ネットワークの境界を監視し外部ネットワークからのアクセスに対して防御する方法、端末自体を監視し防御する方法などが採られる。具体的には、インターネットとＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）の境界にＦＷ（Ｆｉｒｅ Ｗａｌｌ）、ＩＤＳ（Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ）、ＩＰＳ（Ｉｎｔｒｕｔｉｏｎ Ｐｒｅｖｅｎｔｉｏｎ Ｓｙｓｔｅｍ）、ＵＴＭ（Ｕｎｉｆｉｅｄ Ｔｈｒｅａｔ Ｍａｎａｇｅｍｅｎｔ）などのセキュリティ対策機器を設置することが挙げられる。また、ＬＡＮ内に設置している端末に対してマルウェア対策ソフトウェアをインストールし、オペレーティングシステムおよびアプリケーションソフトウェアに最新のセキュリティパッチを適用することなども挙げられる。
【０００４】
しかしながら、施設、工場などにおけるネットワークにおいて、無停止稼動が求められる端末、生産稼働の遅延に厳格であるために一切のソフトウェアの追加又は変更を許され

ない端末などといった、一般的な対策が困難な端末がネットワークに接続されている例が増えてきている。この様な端末は、セキュリティ対策ができず、マルウェアに容易に侵入されてしまい、マルウェア感染などの脅威に曝されるリスクが大きい。このため、ＬＡＮ内部にマルウェアが侵入した場合に更なる感染拡大が起こり、ＬＡＮ内部に様々な障害を起こす。そのため、この様な感染拡大を防ぐ新たなセキュリティ対策が求められている。

【０００５】

従来、第１のコンピュータおよび第２のコンピュータを含む複数のコンピュータと通信可能な対策機器であって、ＬＡＮ内部に対策機器を設置することで、対策機器が任意の時点で通信データを取得し、取得した通信データを第１のコンピュータまたは第２のコンピュータに送信するかを判断する。このように対策機器は、第１のコンピュータと第２のコンピュータとによる通信サービスを制限する技術が開示されている（例えば、特許文献１参照）。

【０００６】

また、スイッチ装置を通過する通信データを、プロミスキャスモードを備えるセキュリティ機器に送信して監視し、ＳＤＮ（Ｓｏｆｔｗａｒｅ Ｄｅｆｉｎｅｄ Ｎｅｔｗｏｒｋ）スイッチ装置で通信を制御する技術が開示されている（例えば、特許文献２参照）。

【先行技術文献】

【特許文献】

【０００７】

【文献】特許第４０８２６１３号公報
特許第６３６４２５５号公報

【非特許文献】

【０００８】

【文献】Ｗａｎｇ，Ｋｅ，ａｎｄ Ｓａｌｖａｔｏｒｅ Ｊ．Ｓｔｏｌｆｏ．“Ａｎｏｍａｌｏｕｓ ｐａｙｌｏａｄ ｂａｓｅｄ ｎｅｔｗｏｒｋ ｉｎｔｒｕｓｉｏｎ ｄｅｔｅｃｔｉｏｎ．”ＲＡＩＤ．Ｖｏｌ．４．２００４．

【発明の概要】

【発明が解決しようとする課題】

【０００９】

しかしながら、特許文献１では、ＬＡＮ内部全体を監視し、セキュリティの脅威を排除するためには、ＬＡＮ内部の全通信データを対策機器に取り込む必要がある。特許文献１の対策機器でこれを実現しようとすると、全ての端末の全組み合わせに対して通信制御パケットを送出し続ける必要があり、２乗のオーダーで制御する必要となるペアが増える。この場合、対策機器に通信が集中するため、通信が逼迫し対策機器の負荷が増大する。このため、前述の様な、遅延に厳格な端末に悪影響が発生する課題がある。

【００１０】

また、通信データを対策機器に取り込むための制御用通信パケットの送信頻度が不十分な場合といった状態では、通信データを対策機器に確実に取り込めない場合があるため、脅威を含む通信データを除去しきれないという課題もある。

【００１１】

また、特許文献２では、ＬＡＮ内部の脅威を監視するセキュリティ機器がＳＤＮスイッチ装置を制御することで通信を制限するため、セキュリティ機器に掛かる負荷が増大すると、脅威の検知が遅れる、或いは、通信全体が遅延する、という課題がある。

【００１２】

また、セキュリティ機器が脅威を検知した内容に応じて検知した端末に関する全ての通信データを正常な内容の通信データも含めて制限してしまうため、突発的な通信遮断などが生じてしまい、制御に悪影響を与えるという課題がある。

【００１３】

さらに、単一のセキュリティ機器のみで検知するため、誤検知および過検知による正常な通信への悪影響も懸念される。

【００１４】
本開示は、通信ネットワークを構成する端末の無停止稼動と通信遅延の最小化とを実現しながら、セキュリティレベルを向上させることを目的とする。
【課題を解決するための手段】
【００１５】
本開示の一態様に係るネットワーク防御装置は、複数のＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）のポートを備え、通信ネットワーク間の接続を行うスイッチを流れる、少なくとも送信元端末の情報と送信先端末の情報とを含む通信データを、プロミスキャスモードで前記スイッチを介して取得する通信データ取得部と、前記通信データの脅威を検知する脅威検知部と、脅威除去部と、前記脅威検知部で脅威を検知した場合、前記脅威除去部を介さずに前記送信元端末と前記送信先端末とを接続する第１の通信経路を、前記脅威除去部を介して前記送信元端末と前記送信先端末とを接続した、前記第１の通信経路と異なる第２の通信経路に変更するように前記スイッチを操作する経路変更部と、を備え、前記脅威除去部は、前記経路変更部が通信経路を変更した後に、前記通信データの脅威を除去する。
【００１６】
なお、これらの包括的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。
【発明の効果】
【００１７】
上記態様により、通信ネットワークを構成する端末の無停止稼動と通信遅延の最小化とを実現しながら、セキュリティレベルを向上させる。
【図面の簡単な説明】
【００１８】
【図１】図１は、実施の形態１におけるネットワーク防御装置が属する通信ネットワークの全体構成を示す図である。
【図２】図２は、実施の形態１における通信データの構成を示す図である。
【図３】図３は、実施の形態１における通信分析部の構成を示す図である。
【図４】図４は、実施の形態１における端末通信情報の構成を示す図である。
【図５】図５は、実施の形態１におけるスイッチ操作部の構成を示す図である。
【図６】図６は、実施の形態１におけるスイッチ初期設定情報の構成を示す図である。
【図７】図７は、実施の形態１におけるスイッチ情報の構成を示す図である。
【図８】図８は、実施の形態１における端末管理部の構成を示す図である。
【図９】図９は、実施の形態１における脅威スコア情報の構成を示す図である。
【図１０】図１０は、実施の形態１における端末一時情報の構成を示す図である。
【図１１】図１１は、実施の形態１における端末更新情報の構成を示す図である。
【図１２Ａ】図１２Ａは、実施の形態１における端末情報の構成を示す図である。
【図１２Ｂ】図１２Ｂは、実施の形態１における端末情報の構成を示す図である。
【図１３Ａ】図１３Ａは、実施の形態１におけるネットワーク全体構成の論理的なネットワークの構成を示す図である。
【図１３Ｂ】図１３Ｂは、実施の形態１におけるネットワーク全体構成の論理的なネットワークの構成を示す図である。
【図１４】図１４は、実施の形態１におけるネットワーク防御装置の動作を示すフローチャートである。
【図１５】図１５は、実施の形態１における脅威スコアの更新の動作を示すフローチャートである。
【図１６】図１６は、実施の形態１における端末情報の更新の動作を示すフローチャートである。

【図１７Ａ】図１７Ａは、実施の形態１の変形例１におけるネットワーク防御装置が属する別の通信ネットワークの全体構成を示す図である。
【図１７Ｂ】図１７Ｂは、実施の形態１の変形例１において、送信元端末と送信先端末とが検疫系ネットワークで通信を行う場合を示す図である。
【図１７Ｃ】図１７Ｃは、実施の形態１の変形例１において、送信元端末と送信先端末とが通常系ネットワークで通信を行う場合を示す図である。
【図１８】図１８は、実施の形態１の変形例２におけるネットワーク防御装置が属するさらに別の通信ネットワークの全体構成を示す図である。
【図１９】図１９は、実施の形態２におけるネットワーク防御装置が属する通信ネットワークの全体構成を示す図である。
【図２０】図２０は、実施の形態２における通信データの構成を示す図である。
【図２１】図２１は、実施の形態２における端末通信情報の構成を示す図である。
【図２２】図２２は、実施の形態２におけるスイッチ初期設定情報の構成を示す図である。
【図２３】図２３は、実施の形態２におけるスイッチ情報の構成を示す図である。
【図２４Ａ】図２４Ａは、実施の形態２における端末情報の構成を示す図である。
【図２４Ｂ】図２４Ｂは、実施の形態２における端末情報の構成を示す図である。
【図２５Ａ】図２５Ａは、実施の形態２におけるネットワーク全体構成の論理的なネットワークの構成を示す図である。
【図２５Ｂ】図２５Ｂは、実施の形態２におけるネットワーク全体構成の論理的なネットワークの構成を示す図である。
【図２６】図２６は、実施の形態２におけるネットワーク防御装置の動作を示すフローチャートである。
【図２７】図２７は、実施の形態２におけるパケット書換部の構成を示す図である。
【図２８】図２８は、実施の形態２の変形例１におけるネットワーク防御装置が属する別の通信ネットワークの全体構成を示す図である。
【図２９】図２９は、実施の形態２の変形例２におけるネットワーク防御装置が属するさらに別の通信ネットワークの全体構成を示す図である。
【発明を実施するための形態】
【００１９】
（本開示の基礎となった知見）
工場などにある産業機器などの制御端末には、設計および実装された時期が古く、インターネットへの接続を考慮されていない場合がある。この様な制御端末には、インターネットからのセキュリティの脅威に対して、なんら対策が講じられていない。
【００２０】
更に、この様な制御端末は、可用性が強く求められ、生産稼働の遅延の増大および稼動停止を極力防ぐ必要があるため、セキュリティ対策ソフトウェアの導入およびセキュリティパッチなど、オペレーションシステムを含むソフトウェアの変更が許容されない。
【００２１】
しかし現在、その様な制御端末を含む産業機器ネットワークは、インターネットに接続されるため、セキュリティの脅威に晒されている。
【００２２】
したがって、産業機器ネットワーク全体のセキュリティの脅威を監視し、生産稼働の遅延および停止を防ぎながらも、マルウェアによる攻撃の無害化および被害拡大を防ぐことが求められる。通信ネットワークデータを監視して攻撃を検知し、かつ、無害化する技術は、例えば、前述の特許文献１、２で開示されている。しかし、産業機器ネットワークに求められる、遅延増大および停止を防ぐことと、突然の通信遮断による制御への悪影響は想定されていない。
【００２３】
そこで、本開示では、工場など制御システムネットワークに必要な端末の無停止稼動と通信遅延の最小化を実現し、かつ、セキュリティレベルを向上させることを目的とする。

【００２４】
（本開示の一態様）
本開示の一様態に係るネットワーク防御装置は、複数のＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）のポートを備え、通信ネットワーク間の接続を行うスイッチを流れる、少なくとも送信元端末の情報と送信先端末の情報とを含む通信データを、プロミスキャスモードで前記スイッチを介して取得する通信データ取得部と、前記通信データの脅威を検知する脅威検知部と、脅威除去部と、前記脅威検知部で脅威を検知した場合、前記脅威除去部を介さずに前記送信元端末と前記送信先端末とを接続する第１の通信経路を、前記脅威除去部を介して前記送信元端末と前記送信先端末とを接続した、前記第１の通信経路と異なる第２の通信経路に変更するように前記スイッチを操作する経路変更部と、を備え、前記脅威除去部は、前記経路変更部が通信経路を変更した後に、前記通信データの脅威を除去する。
【００２５】
この構成により、スイッチを経由する通信データのコピーを通信分析部で監視し続けることで、脅威を検知することができる。脅威を検知すると、経路変更部は、スイッチの設定を変更することで、脅威を含みうる送信元端末が属する通信ネットワークと、送信先端末が属する通信ネットワークとを論理的に切り離し、脅威を含みうる送信元端末と送信先端末の間の経路に、脅威除去部を論理的に接続する様に変更する。こうして、送信元端末が送信した脅威を含みうる通信データから脅威を除去することができる。これにより、端末の運転を停止させることなく（正常な通信に悪影響を与えることなく）通信をすることができるとともに、脅威を監視しマルウェア等の拡散を防ぐことができる。
【００２６】
また、送信元端末が属する通信ネットワークと送信先端末が属する通信ネットワークとの正常な通信を継続するため、脅威を検知する通信分析部と脅威を除去する脅威除去部とを分離している。つまり、通信分析部と脅威除去部とを異なる処理部として分離しているため、それぞれの処理部の処理負荷を最小限にすることができる。これにより、通信分析部が探索行動などによって脅威に到る前に脅威を検知してから、脅威除去部による脅威の除去を適用することができる。その結果、より早期にセキュリティの脅威に対応することができる。
【００２７】
したがって、このネットワーク防御装置は、通信ネットワークを構成する端末の無停止稼動と通信遅延の最小化とを実現しながら、セキュリティレベルを向上させることができる。特に、既存の設備に影響を与えることなく、既存の設備の無停止稼動を実現することができる。
【００２８】
本開示の一様態に係るネットワーク防御システムは、複数のＬＡＮのポートを備え、通信ネットワーク間の接続を行うスイッチを流れる、少なくとも送信元端末の情報と送信先端末の情報とを含む通信データを、プロミスキャスモードで前記スイッチを介して取得する通信データ取得部と、前記通信データの脅威を検知する脅威検知部と、脅威除去部と、前記脅威検知部で脅威を検知した場合、前記送信元端末と前記送信先端末とを接続する第１の通信経路を、前記脅威除去部を介して前記送信元端末と前記送信先端末とを接続した、前記第１の通信経路と異なる第２の通信経路に変更するように前記スイッチを操作する経路変更部と、を備え、前記脅威除去部は、前記経路変更部が通信経路を変更した後に、前記通信データの脅威を除去する。
【００２９】
このネットワーク防御システムにおいても上述と同様の作用効果を奏する。
【００３０】
本開示の一様態に係るネットワーク防御装置において、前記スイッチは、前記送信元端末に接続された第１のＬＡＮのポートと、前記脅威検知部に接続された第２のＬＡＮのポートおよび第３のＬＡＮのポートと、前記送信先端末に接続された第４のＬＡＮのポート

とを有し、前記脅威検知部で脅威を検知していない場合、前記経路変更部は、前記第１のＬＡＮのポートに接続された前記送信元端末から、前記第４のＬＡＮのポートに接続された前記送信先端末までの前記第１の通信経路を、第１のＶＬＡＮ（Ｖｉｒｔｕａｌ　Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）に設定し、前記脅威検知部で脅威を検知した場合、前記経路変更部は、前記第２の通信経路に含まれる、前記第１のＬＡＮのポートに接続された前記送信元端末から、前記第２のＬＡＮのポートに接続された前記脅威除去部までの経路を前記第１のＶＬＡＮと異なる第２のＶＬＡＮに設定し、前記第３のＬＡＮのポートに接続された前記脅威除去部から、前記第４のＬＡＮのポートに接続された前記送信先端末までの経路を前記第１のＶＬＡＮに設定する。

【００３１】

これによれば、脅威検知部で脅威を検知していない場合、送信元端末から送信先端末までを第１のＶＬＡＮ（第１の通信経路）に設定する。また、脅威検知部で脅威を検知した場合、送信元端末から脅威除去部までを第２のＶＬＡＮに設定し、脅威除去部から送信先端末までの経路を第１のＶＬＡＮに設定する（第１のＶＬＡＮと第２のＶＬＡＮとが第２の通信経路となる）。こうすることで、脅威を検知した場合に送信元端末から送信先端末までの間に脅威除去部を介することができる。

【００３２】

本開示の一様態に係るネットワーク防御装置は、さらに、前記脅威除去部を通過した前記通信データに含まれる通信ネットワークのＶＬＡＮ情報を書き換える書換部を備え、前記スイッチは、前記送信元端末に接続された第５のＬＡＮのポートと、前記脅威除去部が接続された第６のＬＡＮのポートと、前記送信先端末に接続された第７のＬＡＮのポートとを有し、前記脅威検知部で脅威を検知していない場合、前記経路変更部は、前記第５のＬＡＮのポートに接続された前記送信元端末と、前記第７のＬＡＮのポートに接続された前記送信先端末とを第１のＶＬＡＮに設定し、前記脅威検知部で脅威を検知した場合、前記経路変更部は、前記第２の通信経路に含まれる、前記第５のＬＡＮのポートに接続された前記送信元端末を第２のＶＬＡＮに設定し、前記第７のＬＡＮのポートに接続された前記送信先端末を前記第１のＶＬＡＮに設定し、前記書換部は、前記第６のＬＡＮのポートを介して、前記送信元端末が属する前記第２のＶＬＡＮを示すＶＬＡＮ情報を前記送信先端末が属する前記第１のＶＬＡＮを示すＶＬＡＮ情報に書き換え、書き換えられた通信データを、前記スイッチに出力する。

【００３３】

このように、脅威検知部で通信データの脅威を検知すると、送信元端末が第２のＶＬＡＮに設定され、送信先端末が第１のＶＬＡＮに設定される。脅威除去部は、第６のポートを介して取得した通信データに含まれる脅威を除去する。書換部は、脅威を除去した通信データに含まれる通信ネットワークのＶＬＡＮ情報を書き換える。つまり、第１のＶＬＡＮを示すＶＬＡＮ情報と第２のＶＬＡＮを示すＶＬＡＮ情報とが異なるため、書換部は、通信データに含まれるＶＬＡＮ情報を、送信先端末が接続されている第７ポートに対応するようにＶＬＡＮ情報を書き換える。これにより、異なるＶＬＡＮを通過する通信データであっても、送信元端末から送信先端末に送信することができる。

【００３４】

本開示の一様態に係るネットワーク防御装置において、前記第１のＶＬＡＮは、前記脅威除去部を介さない通常系ネットワークであり、前記第２のＶＬＡＮは、前記脅威除去部が前記通信データの脅威を除去する検疫系ネットワークであり、前記脅威検知部で脅威を検知した場合、前記経路変更部は、前記第１のＶＬＡＮの一部を前記通常系ネットワークから検疫系ネットワークに変更する。

【００３５】

これによれば、脅威を検知した場合に、通常系ネットワークから検疫系ネットワークに変更されるため、送信元端末が出力した通信データに含まれる脅威を、送信先端末に届く前に除去することができる。

【００３６】

本開示の一様態に係るネットワーク防御装置における、前記脅威除去部において、前記通信データの脅威が除去されると、前記経路変更部は、前記通常系ネットワークから変更されていた前記検疫系ネットワークを、前記通常系ネットワークに戻す。

【００３７】

通信データの脅威が除去された後も送信元端末と送信先端末との通信経路の間に脅威除去部を介していれば、両者の間で通信遅延が生じてしまう。しかし、このネットワーク防御装置では、通信データの脅威が除去されれば検疫系ネットワークを、通常系ネットワークに戻す。このため、送信元端末と送信先端末との間の通信遅延の発生を抑制することができる。

【００３８】

本開示の一様態に係るネットワーク防御装置において、前記通信データ取得部は、前記通信データのコピーを取得し、前記脅威検知部は、前記通信データのコピーをプロミスキャスモードで監視する。

【００３９】

例えば送信元端末と送信先端末との通信経路の間に脅威検知部を配置すれば、脅威検知部が全ての通信データを監視するため、両者の間で通信遅延が生じてしまう。しかし、このネットワーク防御装置では、通信経路上の通信データをコピーしてプロミスキャスモードで監視するため、送信元端末と送信先端末との間の通信遅延の発生を抑制することができる。

【００４０】

本開示の一様態に係るネットワーク防御装置において、前記脅威除去部は、脅威を検知した前記通信データから、脅威を含む不要なデータを除去する。

【００４１】

これによれば、送信先端末には通信データから脅威を含む不要なデータを除去した、脅威除去後の通信データが送信されるため、通信データの通信量を削減することができる。

【００４２】

本開示の一様態に係るネットワーク防御装置において、前記脅威検知部は、検知した脅威内容に応じて、脅威が検知された送信元端末にスコアを付与し、前記経路変更部は、前記脅威検知部で付与した前記スコアが第１の値を超えた場合、前記スコアが付与された当該送信元端末に係る通信データを前記脅威除去部に経由させるように、前記スイッチに通信経路を変更させる。

【００４３】

これによれば、脅威をスコアによって段階的に分類することで、脅威を含んでいる可能性の高い通信データだけを脅威除去部に経由させることができる。このため、脅威を含んでいる可能性の低い通信データを脅威除去部に経由させないようにすることができる。その結果、脅威除去部を経由する通信データの数が削減されるため、送信元端末と送信先端末との通信経路の間の通信遅延の発生を抑制することができる。

【００４４】

本開示の一様態に係るネットワーク防御装置において、前記脅威検知部は、付与した前記スコアに対して、所定時間経過後に前記スコアを所定値減算し、検知した脅威の前記スコアが第２の値を下回った場合、前記経路変更部は、前記送信元端末と前記送信先端末との接続を、前記脅威除去部を介さないように前記スイッチに通信経路を変更させる。

【００４５】

これによれば、通信データから検知された脅威の内容（スコア）を精度よく補正することができる。このため、時間の経過とともに脅威除去部を経由する通信データの数が削減されるため、送信元端末と送信先端末との通信経路での通信遅延の発生を抑制することができる。

【００４６】

本開示の一様態に係るネットワーク防御装置において、前記脅威検知部は、検知した脅威の前記スコアが前記第１の値より大きい第３の値を超えた場合、前記所定時間経過して

も前記スコアを減算しない。
【００４７】
これによれば、脅威を含んでいる可能性の非常に高い通信データについては、誤検知の可能性が低いと考えられるため、通信データから検知された脅威を示すスコアを変更することなく、スコアを維持する。このため、誤検知の発生を抑制するとともに、検知した脅威を脅威除去部によって確実に除去することができる。
【００４８】
なお、以下で説明する実施の形態は、いずれも本発明の一具体例を示すものである。これらの包括的または具体的な態様は、システム、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能な記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムまたは記録媒体の任意の組み合わせで実現されてもよい。以下の実施の形態で示される数値、形状、構成要素、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。また全ての実施の形態において、各々の内容を組み合わせることもできる。
【００４９】
（実施の形態１）
本実施の形態について、図面を参照しながら説明する。なお、各図面において同じ構成要素については同じ符号が用いられている。
【００５０】
１．通信ネットワークの全体構成
図１は、本実施の形態におけるネットワーク防御装置が属する通信ネットワークの全体構成を示す図である。本実施の形態の通信ネットワークでは、端末は、ＩＥＥＥ８０２．３で規定されるＥｔｈｅｒｎｅｔ（登録商標）上でＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）／ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）およびＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）／ＩＰなどアプリケーションに応じて、適切なプロトコルで通信を行う。
【００５１】
図１に示すように、通信ネットワークでは、インテリジェントスイッチ２０に対して、ネットワーク防御装置１０と、送信先端末３０１と、送信元端末３０２とがそれぞれＬＡＮケーブルで接続されて構成される。本実施の形態では、便宜上、送信元端末３０２が送信する後述する図２の通信データ１０１０の送信先を送信先端末３０１、および、送信先端末３０１に送信する通信データ１０１０の送信元を送信元端末３０２に定義しているが、送信先端末は送信元端末とも成りえ、その逆も成りえる。
【００５２】
インテリジェントスイッチ２０は、端末を接続するための複数のＬＡＮのポート（０～７）を備える。なお、以下では、ＬＡＮのポートのことを単にポートと呼ぶ。インテリジェントスイッチ２０において、インテリジェントスイッチ２０とＬＡＮケーブルとの接続点に記載されている数値は、ＬＡＮケーブルが接続されるポートの番号を示す。なお、以下で単に「端末」という場合は、送信元端末３０２および送信先端末３０１を総称していう。
【００５３】
また、インテリジェントスイッチ２０は、それぞれのポートにＶＬＡＮと呼ばれる論理的なネットワークを設定する機能を備える。インテリジェントスイッチ２０では、インテリジェントスイッチ２０を通過する通信データ１０１０のコピーを出力可能なミラー機能をポート０に備える。ポート１～７は、一般的なスイッチングハブのポートと同様の振る舞いをする。なお、ポート（ＬＡＮのポート）は、物理的ポートだけでなく論理的なソフトウェアポートを含んでいてもよい。ただし、ソフトウェアポートには、ＴＣＰ／ＩＰのようなポートを含めなくてもよい。

【００５４】
インテリジェントスイッチ２０のポート０～２は、それぞれＬＡＮケーブルを介して、ネットワーク防御装置１０に接続されている。また、インテリジェントスイッチ２０のポート４には、送信先端末３０１が接続されている。さらに、インテリジェントスイッチ２０のポート７には、送信元端末３０２が接続されている。ポート７は第１のポートの一例である。ポート４は第４のポートの一例である。
【００５５】
２．ネットワーク防御装置の構成
次にネットワーク防御装置１０の詳細について説明する。
【００５６】
ネットワーク防御装置１０は、通信データ取得部１０１と、通信分析部１０２と、スイッチ操作部１０３と、端末情報管理部１０４と、脅威除去部１０５とを備える。
【００５７】
通信データ取得部１０１は、複数のポートを備えたインテリジェントスイッチ２０を流れる通信データ１０１０をプロミスキャスモードで取得する。通信データ取得部１０１は、送信元端末３０２と送信先端末３０１との間で通信される通信データ１０１０を、ポート０からの出力によって受信（取得）し、通信分析部１０２に出力する機能を備える。
【００５８】
通信分析部１０２は、通信データ取得部１０１から出力された通信データ１０１０を分析する。通信分析部１０２は、分析結果を示す情報（後述する端末通信情報）を端末情報管理部１０４に出力する機能を備える。端末のポート番号は、端末がインテリジェントスイッチ２０に接続されているポートの数値である。
【００５９】
スイッチ操作部１０３は、インテリジェントスイッチ２０が保持している端末のポート番号および端末のアドレスを対応付けた情報（後述するスイッチ情報）を取得し、端末情報管理部１０４に通知する機能を備える。また、スイッチ操作部１０３は、端末情報管理部１０４から出力された情報（後述する端末情報）に基づいて、インテリジェントスイッチ２０のＶＬＡＮを、ＶＬＡＮ１からＶＬＡＮ２に、或いはＶＬＡＮ２からＶＬＡＮ１に切り換える（変更する）。つまり、スイッチ操作部１０３は、インテリジェントスイッチ２０に、ＶＬＡＮ１とＶＬＡＮ２とを相互に切り換えることを命令する機能を備える。ここで、ＶＬＡＮ１は、通常系ネットワークであり、ＶＬＡＮ２は、検疫系ネットワークである。ＶＬＡＮ１は、第１のＶＬＡＮの一例であり、ＶＬＡＮ２は、第２のＶＬＡＮの一例である。
【００６０】
端末情報管理部１０４は、通信分析部１０２から出力された分析結果を示す情報と、後述するスイッチ操作部１０３のスイッチ情報取得部１０３２から出力された情報とを統合し、端末情報として管理する。端末情報管理部１０４は、この端末情報をスイッチ操作部１０３に通知する機能を備える。
【００６１】
脅威除去部１０５は、送信先端末３０１から送信された通信データ１０１０を取得し、取得した通信データ１０１０から脅威を除去する機能を備える。つまり、脅威除去部１０５は、脅威を検知した通信データ１０１０から、脅威を含む不要なデータを除去する機能を備える。また、脅威除去部１０５は、脅威除去後の通信データを送信先端末３０１に出力する機能も備える。脅威除去部１０５は、通信データ１０１０そのものが脅威であれば、通信データ１０１０を除去し、通信データ１０１０に含まれる例えば文字列などが脅威であれば、その文字列を除去した通信データ１０１０を、インテリジェントスイッチ２０に出力する。
【００６２】
ここで、脅威とは、送信先端末３０１および送信先端末３０１に格納される情報に対して、破損、破壊、または、アクセス拒否などの有害なまたは望まれない影響を生じさせる

コンピュータプログラムであり、例えばマルウェア、ウイルス、または、スパイウェア等である。

【００６３】

２－１．通信データの構成

図２は、本実施の形態における通信データ１０１０の構成を示す図である。図２に示すように、通信データ１０１０には、少なくとも、送信元アドレス情報１０１１と送信先アドレス情報１０１２とペイロード１０１３とが含まれる。

【００６４】

送信元アドレス情報１０１１には、少なくとも、送信元ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス情報１０１１１と、送信元ＩＰアドレス情報１０１１２と、送信元ポート情報１０１１３とが含まれる。送信元アドレス情報１０１１は、送信元端末３０２の情報の一例である。

【００６５】

送信先アドレス情報１０１２には、少なくとも、送信先ＭＡＣアドレス情報１０１２１と、送信先ＩＰアドレス情報１０１２２と、送信先ポート情報１０１２３とが含まれる。送信先アドレス情報１０１２は、送信先端末の情報の一例である。

【００６６】

３．通信分析部の構成

次に通信分析部１０２の詳細について説明する。

【００６７】

図３は、本実施の形態における通信分析部１０２の構成を示す図である。図３に示すように、通信分析部１０２は、端末アドレス確認部１０２０と、通信フロー情報解析部１０２１と、通信データ解析部１０２２とを備える。

【００６８】

通信分析部１０２は、通信データ取得部１０１から通信データ１０１０を取得し、端末アドレス確認部１０２０と通信フロー情報解析部１０２１と通信データ解析部１０２２とを用いて、それぞれが通信データ１０１０を解析する。通信分析部１０２は、端末アドレス確認部１０２０、通信フロー情報解析部１０２１、および、通信データ解析部１０２２のそれぞれの脅威検知情報を纏めた端末通信情報１０２３を、端末情報管理部１０４に出力する。通信分析部１０２は、脅威検知部の一例である。

【００６９】

３－１．端末アドレス確認部の構成

図２および図３に示すように、端末アドレス確認部１０２０は、通信データ１０１０にある送信元アドレス情報１０１１のうち、少なくとも、送信元ＭＡＣアドレス情報１０１１１と送信元ＩＰアドレス情報１０１１２とを取得する。端末アドレス確認部１０２０は、取得した送信元アドレス情報１０１１に基づいて、アクセスが禁止されている送信元端末３０２のＭＡＣアドレス情報およびＩＰアドレス情報と、送信元ＭＡＣアドレス情報１０１１１および送信元ＩＰアドレス情報１０１１２とが一致するかどうかを判定し、判定した結果である脅威検知情報を出力する。

【００７０】

３－２．通信フロー情報解析部の構成

通信フロー情報解析部１０２１は、通信データ１０１０に含まれる送信先アドレス情報１０１２に基づいて脅威検知情報を生成する。通信フロー情報解析部１０２１は、送信先アドレス情報１０１２に基づいて脅威があるかどうかを判定し、判定した結果である脅威検知情報を出力する。通信フロー情報解析部１０２１は、ブラックリスト通信検知部１０２１１と、ホワイトリスト外通信検知部１０２１２と、ＩＰスキャン検知部１０２１３と、ポートスキャン検知部１０２１４とを含む。なお、通信フロー情報解析部１０２１は、上記の検知部を全て含まなくてもよく、一部の構成でもよいし、さらに別の検知部を含んでもよい。

【００７１】

ブラックリスト通信検知部１０２１１は、アクセスを禁止されている送信先アドレス情報と送信先アドレス情報１０１２とが一致するかどうかを判定し、一致する場合にセキュリティ異常として検知する。

【００７２】

ホワイトリスト外通信検知部１０２１２は、アクセスを許可されている送信先アドレス情報と送信先アドレス情報１０１２とが一致するかどうかを判定し、一致しない場合にセキュリティ異常として検知する。

【００７３】

ＩＰスキャン検知部１０２１３は、送信先アドレス情報１０１２に含まれる送信先ＩＰアドレス情報１０１２２から、通信ネットワーク内部における多数のＩＰアドレスへのアクセス試行の有無を判定する。ＩＰスキャン検知部１０２１３は、このようなアクセス試行がある場合に、セキュリティ異常として検知する。

【００７４】

ポートスキャン検知部１０２１４は、送信先アドレス情報１０１２に含まれる送信先ポート情報１０１２３から通信ネットワーク内部における特定のＩＰアドレスに対する多数のポートへのアクセス試行の有無を判定する。ポートスキャン検知部１０２１４は、このようなアクセス試行が有る場合に、セキュリティ異常として判定する。

【００７５】

通信フロー情報解析部１０２１は、ブラックリスト通信検知部１０２１１、ホワイトリスト外通信検知部１０２１２、ＩＰスキャン検知部１０２１３、および、ポートスキャン検知部１０２１４以外の別の検知部を用いてもよい。例えば、機械学習を用いて、アクセス先が妥当なものかどうかを点数評価し、一定の点数以上となるものをセキュリティ異常と判定する検知部、点数が最上位の端末から数台目までの端末をセキュリティ異常の疑いと判定する検知部などである。

【００７６】

３－３．通信データ解析部の構成

通信分析部１０２において、通信データ解析部１０２２は、通信データ１０１０に含まれるペイロード１０１３に基づいて脅威検知情報を生成する。通信データ解析部１０２２は、ペイロード１０１３に基づいて脅威があるかどうかを判定し、判定した結果である脅威検知情報を出力する。通信データ解析部１０２２は、脆弱性攻撃検知部１０２２１とマルウェア検知部１０２２２と認証失敗検知部１０２２３とを含む。

【００７７】

なお、通信データ解析部１０２２は、上記の脆弱性攻撃検知部１０２２１、マルウェア検知部１０２２２、および、認証失敗検知部１０２２３を全て含まなくてもよく、さらに別の検知部を含んでもよい。

【００７８】

脆弱性攻撃検知部１０２２１は、ペイロード１０１３の中において、端末に組み込まれているソフトウェアの脆弱性を攻撃するパターンの有無を判定する。脆弱性攻撃検知部１０２２１は、通信データ１０１０にソフトウェアの脆弱性を攻撃するパターンが有る場合に、セキュリティ異常として検知する。

【００７９】

マルウェア検知部１０２２２は、ペイロード１０１３にマルウェアを示すパターンが含まれているかどうかを判定する。マルウェア検知部１０２２２は、マルウェアを示すパターンが含まれる場合に、セキュリティ異常として検知する。

【００８０】

認証失敗検知部１０２２３は、端末への認証試行情報を取得し、特定の端末に対して一定時間内に認証試行と認証失敗とが繰り返し発生しているかどうかを判定する。認証失敗検知部１０２２３は、認証失敗が繰り返して発生している場合に、セキュリティ異常として検知する。

【００８１】

通信データ解析部１０２２は、脆弱性攻撃検知部１０２２１、マルウェア検知部１０２２２、および、認証失敗検知部１０２２３以外の別の検知部を用いてもよい。別の検知部は、例えば、非特許文献１に開示されているような、ペイロード１０１３のビットパターンの一部を、機械学習を用いて点数評価したり、ペイロード１０１３の内容を解読して得た情報を、機械学習を用いて点数評価したりするなどして、ある一定以上の点数であればセキュリティ異常として検知する検知部、点数が上位の数パターンをセキュリティ異常として検知する検知部などが考えられる。

【００８２】

３－４．端末通信情報の構成

次に、端末通信情報１０２３の詳細について説明する。図４は、本実施の形態における端末通信情報１０２３の構成を示す図である。

【００８３】

図３および図４に示すように、端末アドレス確認部１０２０、通信フロー情報解析部１０２１、および、通信データ解析部１０２２は、通信データ１０１０を解析し、解析した結果を端末通信情報１０２３とする。図４に示すように、端末通信情報１０２３は、端末番号１０２３０とＩＰアドレス情報１０２３１とＭＡＣアドレス情報１０２３２と更新時刻情報１０２３３と脅威検知内容１０２３４とで構成される。

【００８４】

端末アドレス確認部１０２０は、送信元ＩＰアドレス情報１０１１２をＩＰアドレス情報１０２３１とし、送信元ＭＡＣアドレス情報１０１１１をＭＡＣアドレス情報１０２３２とする。また、通信フロー情報解析部１０２１と通信データ解析部１０２２との判定結果は脅威検知内容１０２３４とされる。ＩＰアドレス情報１０２３１、および、送信元のＭＡＣアドレス情報１０２３２を取得した時刻は、更新時刻情報１０２３３とされる。

【００８５】

４．スイッチ操作部の構成

次に、スイッチ操作部１０３の詳細について説明する。図５は、本実施の形態におけるスイッチ操作部１０３の構成を示す図である。

【００８６】

図５に示すように、スイッチ操作部１０３は、インテリジェントスイッチ２０に関する設定情報であるスイッチ初期設定情報１０３１を格納している。スイッチ操作部１０３は、スイッチ情報取得部１０３２と、経路変更部１０３３とを備える。

【００８７】

スイッチ情報取得部１０３２は、スイッチ初期設定情報１０３１に基づいてインテリジェントスイッチ２０が保持するスイッチ情報１０３２０を取得し、スイッチ情報１０３２０を端末情報管理部１０４に出力する。

【００８８】

経路変更部１０３３は、スイッチ初期設定情報１０３１と端末情報管理部１０４とからの通知に基づいてインテリジェントスイッチ２０の各ポートのＶＬＡＮ設定を変更する。

【００８９】

４－１．スイッチ初期設定情報の構成

次に、スイッチ初期設定情報１０３１の詳細について説明する。図６は、本実施の形態におけるスイッチ初期設定情報１０３１の構成を示す図である。図６に示すように、スイッチ初期設定情報１０３１は、スイッチ識別情報１０３１１とスイッチ制御用ＩＰアドレス１０３１２とが対応したスイッチ識別情報テーブル１０３１０、および、ＶＬＡＮ情報１０３１４とＶＬＡＮネットワーク種類１０３１５とが対応したＶＬＡＮ識別情報テーブル１０３１３で構成される。

【００９０】

スイッチ識別情報１０３１１は、個々のインテリジェントスイッチ２０を識別する情報である。

【００９１】

スイッチ制御用ＩＰアドレス１０３１２は、ＳＮＭＰ（Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）を用いてインテリジェントスイッチ２０のポート１を通じて、インテリジェントスイッチ２０を制御する場合に使用する。

【００９２】

ＶＬＡＮ情報１０３１４は、ＶＬＡＮを特定（識別）するための情報であり、本実施の形態では、ＶＬＡＮ１、および、ＶＬＡＮ２が存在する。

【００９３】

ＶＬＡＮネットワーク種類１０３１５は、ＶＬＡＮ情報１０３１４に対応付けられている。例えば、ＶＬＡＮ１は、ＶＬＡＮネットワーク種類１０３１５が通常系ネットワークを示し、ＶＬＡＮ２は、ＶＬＡＮネットワーク種類１０３１５が検疫系ネットワークを示す。

【００９４】

通常系ネットワークは、送信元端末３０２から送信先端末３０１までの間に、脅威除去部１０５を介さないネットワークである。

【００９５】

検疫系ネットワークは、送信元端末３０２から送信先端末３０１までの間に、脅威除去部１０５を介するネットワークである。

【００９６】

４－２．スイッチ情報の構成

次に、スイッチ情報１０３２０の詳細について説明する。図７は、本実施の形態におけるスイッチ情報１０３２０の構成を示す図である。スイッチ情報１０３２０は、スイッチ情報取得部１０３２により生成される。スイッチ情報取得部１０３２は、スイッチ初期設定情報１０３１から取得されたスイッチ識別情報１０３１１をスイッチ識別情報１０３２１とし、インテリジェントスイッチ２０から、スイッチ識別情報１０３２１に対応する接続ポート情報１０３２２、ＶＬＡＮ情報１０３２３、および、ＭＡＣアドレス情報１０３２４を取得する。

【００９７】

接続ポート情報１０３２２は、端末が接続されているインテリジェントスイッチ２０のポート番号を示す情報である。

【００９８】

５．端末情報管理部の構成

次に、ネットワーク防御装置１０の端末情報管理部１０４の詳細について説明する。図８は、本実施の形態における端末情報管理部１０４の構成を示す図である。図８に示すように、端末情報管理部１０４は、管理対象の通信ネットワークに存在する端末の情報である端末情報１０４１０を管理する。端末情報管理部１０４は、端末情報１０４１０を記憶する端末情報記憶部１０４１と、端末情報更新部１０４２と、端末管理設定部１０４３ａとを備える。

【００９９】

端末情報更新部１０４２は、通信分析部１０２から取得した図４の端末通信情報１０２３と、スイッチ操作部１０３から取得した図７のスイッチ情報１０３２０と、後述する図９の脅威加算スコア情報１０４３０とに基づいて端末一時情報１０４０を生成する。端末情報更新部１０４２は、端末一時情報１０４０と端末情報記憶部１０４１に記憶される端末情報１０４１０とに基づいて、端末更新情報１０４２０を生成する。端末情報更新部１０４２は、端末更新情報１０４２０を、スイッチ操作部１０３の経路変更部１０３３へ通知する。さらに、端末情報更新部１０４２は、端末更新情報１０４２０に基づいて、端末情報記憶部１０４１に記憶される端末情報１０４１０を更新する。

【０１００】

端末管理設定部１０４３ａは、端末管理部設定情報１０４３を格納している記憶部である。

【０１０１】

５－１．端末管理部設定情報の構成

次に、端末管理部設定情報１０４３の詳細について説明する。図９は、本実施の形態における端末管理部設定情報１０４３の構成を示す図である。図９に示すように、端末管理部設定情報１０４３は、脅威加算スコア情報１０４３０と、脅威スコアに基づいて各ポートのＶＬＡＮ設定を変更するために必要な端末管理部基準値情報１０４３１とを含む。

【０１０２】

脅威加算スコア情報１０４３０は、検知内容識別情報１０４３０１と、検知内容１０４３０２と、判定１０４３０３と、脅威加算スコア１０４３０４とを含む。

【０１０３】

検知内容識別情報１０４３０１は、通信分析部１０２が持つ端末アドレス確認部１０２０、通信フロー情報解析部１０２１、通信データ解析部１０２２などのいずれかで判定した結果を示す情報である。検知内容識別情報１０４３０１では、各処理部の符号で表し、図面に記載される符号は一例である。

【０１０４】

なお、検知内容識別情報１０４３０１は、どの処理部で判定した結果であるかを識別できるのであれば何でもよく、例えば、検知部の検知内容に対して識別可能な番号を付与しておき、その番号で識別するようにしてもよい。

【０１０５】

検知内容１０４３０２は、検知内容識別情報１０４３０１に対応付けられた検知内容を示している。検知内容１０４３０２は、例えば、検知内容識別情報１０４３０１の「１０２０」では、新規の送信元アドレス情報１０１１の端末情報記憶部１０４１に含まれていない「新規のＩＰアドレス、ＭＡＣアドレスが出現」したことを示す。

【０１０６】

判定１０４３０３は、検知内容１０４３０２で示す検知結果が脅威であると判定した場合をブラックとし、脅威の可能性があるが明確に脅威であるかは判定できない場合をグレーとし、脅威の可能性がない場合をホワイトと定義する。

【０１０７】

なお、判定１０４３０３は、検知結果を上記のように３つのレベルで定義するだけでなく、必要に応じて、さらに判定レベルを追加して用いてもよいし、ブラックとホワイトの２つのレベルで定義してもよい。

【０１０８】

なお、脅威加算スコア情報１０４３０は、上記の項目に限られず、さらに別の項目が含まれていてもよいし、一部の項目のみを利用してもよい。また、脅威加算スコア情報１０４３０の検知内容１０４３０２は、複数が組み合わされて用いられてもよい。また、脅威加算スコア情報１０４３０の脅威加算スコア１０４３０４は、全ての端末で同一である必要はなく、役割および種類に応じて異なる値が設定されていてもよい。

【０１０９】

端末管理部基準値情報１０４３１は、基準値内容１０４３１１と、基準値１０４３１２とを含む。基準値内容１０４３１１としては、「脅威スコア減算までの時間ｔ０」と、「ＶＬＡＮ１からＶＬＡＮ２へ変更する際の脅威スコア値Ｘ」と、「ＶＬＡＮ２からＶＬＡＮ１へ変更する際の脅威スコア値Ｙ」と、「脅威レベルの判定をグレーからブラックに変更するスコア値Ｚ」とを含む。脅威スコア値Ｘは、第１の値の一例である。脅威スコア値Ｙは、第２の値の一例である。スコア値Ｚは、第３の値の一例である。

【０１１０】

なお、端末管理部基準値情報１０４３１の基準値内容１０４３１１は、上記の内容に限定されるわけではなく、上記内容以外の項目が含まれていてもよいし、上記内容の一部を利用してもよい。「脅威スコア減算までの時間ｔ０」を用いる代わりに、例えば、「通信容量Ｍ０」、「一定の通信パケット数Ｐ０」、「一定のＴＣＰセッション数Ｓ０」などを用いてもよい。基準値内容１０４３１１が「通信容量Ｍ０」および「通信パケット数Ｐ０」とした場合、通信容量および通信パケット数によって、送信先端末３０１からの送信量

を計測してもよいし、送信元端末３０２および送信先端末３０１からの送受信量を計測してもよい。

【０１１１】

また、基準値内容１０４３１１では、「脅威スコア減算までの時間ｔ０」、「通信容量Ｍ０」、「一定の通信パケット数Ｐ０」および「一定のＴＣＰセッション数Ｓ０」のうちの任意の２つ以上を組み合わせて用いてもよい。また、端末管理部基準値情報１０４３１の基準値１０４３１２の値は全ての端末で同一である必要はなく、役割および種類に応じて、異なる値を設定してもよい。

【０１１２】

端末管理部設定情報１０４３は、通信ネットワーク稼動開始時に設定しておく必要があるが、通信ネットワークの稼動開始後には、状況に応じて変更を行ってもよい。図示はしないが、端末情報更新部１０４２に設定のための情報表示部と入力部とを備えて設定を行ってもよいし、例えば、機械学習を用いて自動的に脅威加算スコア１０４３０４および基準値１０４３１２を変更するなどをしてもよい。

【０１１３】

５－２．端末一時情報の構成

次に端末一時情報１０４０の詳細について説明する。図１０は、本実施の形態における端末一時情報１０４０の構成を示す図である。図１０に示すように、端末一時情報１０４０は、図８の端末情報管理部１０４により管理される。端末一時情報１０４０は、スイッチ識別情報１０４０１と、接続ポート情報１０４０２と、ＶＬＡＮ情報１０４０３と、ＭＡＣアドレス情報１０４０４と、ＩＰアドレス情報１０４０５と、更新時刻情報１０４０６と、脅威加算スコア１０４０７とを含む。

【０１１４】

５－３．端末更新情報の構成

次に、端末更新情報１０４２０の詳細について説明する。図１１は、本実施の形態における端末更新情報１０４２０の構成を示す図である。図１１は、送信元端末３０２からの脅威が検知された後の情報である。端末更新情報１０４２０は、端末情報管理部１０４により管理され、端末情報更新部１０４２により保持される。

【０１１５】

端末更新情報１０４２０は、スイッチ識別情報１０４２１と、接続ポート情報１０４２２と、ＶＬＡＮ情報１０４２３と、ＭＡＣアドレス情報１０４２４と、ＩＰアドレス情報１０４２５と、更新時刻情報１０４２６と、脅威スコア１０４２７とを含む。脅威スコア１０４２７は、図９の脅威加算スコアに基づいて算出された通信データ１０１０の脅威度を示す。脅威スコア１０４２７は、スコアの一例である。

【０１１６】

５－４．端末情報の構成

次に、端末情報１０４１０の詳細について説明する。図１２Ａおよび図１２Ｂは、本実施の形態における端末情報１０４１０の構成を示す図である。図１２Ａの端末情報１０４１０は、送信元端末３０２からの脅威が検知される前の情報を示し、図１２Ｂの端末情報１０４１０は、送信元端末３０２からの脅威が検知された後の情報を示している。

【０１１７】

図１２Ａおよび図１２Ｂに示すように、端末情報１０４１０は、端末情報管理部１０４により管理され、端末情報記憶部１０４１に記憶される。端末情報１０４１０は、管理ＩＤ情報１０４１１と、スイッチ識別情報１０４１２と、接続ポート情報１０４１３と、ＶＬＡＮ情報１０４１４と、ＭＡＣアドレス情報１０４１５と、ＩＰアドレス情報１０４１６と、更新時刻情報１０４１７と、脅威スコア１０４１８とを含む。

【０１１８】

管理ＩＤ情報１０４１１は、スイッチ識別情報１０４１２、接続ポート情報１０４１３、ＶＬＡＮ情報１０４１４、および、ＭＡＣアドレス情報１０４１５を１組として、他の組と識別する１つのＩＤを割り当てる。

【０１１９】
６．脅威検知前と脅威検知後の論理的なネットワークの構成
次に、送信元端末３０２からの脅威が検知される前と後のネットワーク全体構成の詳細について説明する。図１３Ａおよび図１３Ｂは、本実施の形態におけるネットワーク全体構成の論理的なネットワーク構成を示す図である。図１３Ａは、送信元端末３０２からの脅威が検知される前の論理的なネットワーク全体構成を示し、図１３Ｂは、送信元端末３０２からの脅威が検知された後の論理的なネットワーク構成を示す。図１３Ａおよび図１３Ｂに示すように、脅威除去部１０５は、ＶＬＡＮ１に含まれるインテリジェントスイッチ２０のポート１を介して接続し、かつ、ＶＬＡＮ２に含まれるインテリジェントスイッチ２０のポート２を介して接続している。なお、図１３Ａおよび図１３Ｂでは、便宜上、インテリジェントスイッチ２０のポート０とネットワーク防御装置１０とを接続するＬＡＮケーブルを省略している。
【０１２０】
図１３Ａは、送信元端末３０２からの脅威が検知される前、または、脅威が検知された後、かつ、異常状態から正常状態に変化した後の通常系ネットワークを示す。送信先端末３０１と送信元端末３０２とは、共にＶＬＡＮ１に含まれ、脅威除去部１０５を介さずに通信を行っている。つまり、図１３ＡのＶＬＡＮ１は、送信先端末３０１と送信元端末３０２とがインテリジェントスイッチ２０を介して接続されており、通信データ１０１０に対して脅威除去を行わない通常系ネットワークを構成している。異常状態から正常状態に変化とは、異常状態から正常状態に回復することを意味する。
【０１２１】
送信元端末３０２、インテリジェントスイッチ２０のポート７、ポート４、および、送信先端末３０１は、第１の通信経路の一例であり、ＶＬＡＮ１に属する。送信元端末３０２、インテリジェントスイッチ２０のポート７、ポート４、および、送信先端末３０１の経路は、検知前の正常状態である。
【０１２２】
図１３Ｂは、送信元端末３０２からの脅威が検知された後、かつ、異常状態から正常状態に変化する前の論理的な異常系ネットワークを示す。
【０１２３】
送信先端末３０１はＶＬＡＮ１に接続されたまま脅威除去部１０５に接続され、送信元端末３０２はＶＬＡＮ１からＶＬＡＮ２に接続が切り換えられて脅威除去部１０５に接続される。これにより、送信元端末３０２は、脅威除去部１０５を介して送信先端末３０１と通信を行う。脅威除去部１０５は、送信元端末３０２に係る通信データ１０１０から脅威を除去し、脅威除去後の通信データつまり修正後の通信データを、インテリジェントスイッチ２０を介して送信先端末３０１に送信する。
【０１２４】
ＶＬＡＮ２に属する、送信元端末３０２、インテリジェントスイッチ２０のポート７、ポート２、脅威除去部１０５、および、ＶＬＡＮ１に属する、脅威除去部１０５、インテリジェントスイッチ２０のポート１、ポート４、送信先端末３０１は、第２の通信経路の一例である。送信元端末３０２、インテリジェントスイッチ２０のポート７、ポート２、脅威除去部１０５、および、ＶＬＡＮ１に属する、脅威除去部１０５、インテリジェントスイッチ２０のポート１、ポート４、送信先端末３０１の経路は、検知前の異常状態である。ポート１およびポート２は、第２のポートおよび第３のポートの一例である。
【０１２５】
そして、ネットワーク防御装置１０のスイッチ操作部１０３は、図１３Ａで示すように異常状態の異常系ネットワークから正常状態の通常系ネットワークに変更する。そして、送信元端末３０２は、送信先端末３０１と正常な通信を行う。
【０１２６】
７．ネットワーク防御装置の動作
次に、ネットワーク防御装置１０の動作について詳細に説明する。図１４は、本実施の

形態におけるネットワーク防御装置１０の動作を示すフローチャートである。
【０１２７】
図１４等に示すように、ネットワーク防御装置１０は、送信元端末３０２と送信先端末３０１との間で通信される通信データ１０１０を取得する（ステップＳ００１）。具体的には、ネットワーク防御装置１０は、インテリジェントスイッチ２０のポート０に接続されたＬＡＮケーブルを介して、通信データ１０１０のコピーをプロミスキャスモードで取得する。
【０１２８】
ネットワーク防御装置１０の通信データ取得部１０１は、監視対象の通信ネットワーク上で取得した通信データ１０１０を、通信分析部１０２に出力する。
【０１２９】
通信分析部１０２は、通信データ１０１０を分析する（ステップＳ００２）。通信分析部１０２は、通信データ１０１０に基づいて、端末アドレス確認部１０２０と、通信フロー情報解析部１０２１と、通信データ解析部１０２２とを用いて、各々が判定した結果である各々の脅威検知情報を生成する。通信分析部１０２は、各々の脅威検知情報に基づいて端末通信情報１０２３を生成する。
【０１３０】
端末アドレス確認部１０２０は、通信データ１０１０から送信元端末３０２の端末通信情報１０２３を抽出し、送信元端末３０２のＩＰアドレス情報１０２３１とＭＡＣアドレス情報１０２３２と更新時刻情報１０２３３とを特定する。
【０１３１】
通信フロー情報解析部１０２１において、ブラックリスト通信検知部１０２１１は、送信先アドレス情報１０１２がアクセスを禁止されている送信先と一致する場合に、セキュリティ異常として検知する。また、ホワイトリスト外通信検知部１０２１２は、送信先アドレス情報１０１２がアクセスを許可されている送信先と一致しない場合にセキュリティ異常として検知する。さらに、ＩＰスキャン検知部１０２１３は、送信先ＩＰアドレス情報からネットワーク内部の多数のＩＰアドレスへのアクセス試行がある場合にセキュリティ異常と検知する。また、ポートスキャン検知部１０２１４は、送信先ポート情報からネットワーク内部の特定のＩＰアドレスに対して多数のポートのアクセス試行が有る場合にセキュリティ異常と検知する。
【０１３２】
通信データ解析部１０２２において、脆弱性攻撃検知部１０２２１は、ペイロード１０１３の中に、送信先端末３０１に組み込まれているソフトウェアの脆弱性を攻撃するパターンが有る場合に、セキュリティ異常と検知する。マルウェア検知部１０２２２は、ペイロード１０１３にマルウェアを示すパターンが含まれる場合にセキュリティ異常と検知する。認証失敗検知部１０２２３は、認証が必要な端末へ特定の端末から一定時間内に多数の認証試行と失敗の繰り返しが発生している場合にセキュリティ異常と検知する。
【０１３３】
そして、通信分析部１０２は、端末通信情報１０２３を端末情報管理部１０４に送信する。
【０１３４】
端末情報更新部１０４２は、端末通信情報１０２３と、端末情報１０４１０と、端末管理部設定情報１０４３の脅威加算スコア情報１０４３０とから、端末一時情報１０４０を生成する。
【０１３５】
ＭＡＣアドレス情報１０４０４は端末通信情報１０２３のＭＡＣアドレス情報１０２３２、ＩＰアドレス情報１０４０５は端末通信情報１０２３のＩＰアドレス情報１０２３１、更新時刻情報１０４０６は端末通信情報１０２３の更新時刻情報１０２３３を用いる。
【０１３６】
端末情報更新部１０４２は、端末情報１０４１０から、ＭＡＣアドレス情報１０４０４

とＩＰアドレス情報１０４０５とを含む組み合わせを検索する。該当する組み合わせが有る場合、端末情報更新部１０４２は、スイッチ識別情報１０４０１をスイッチ識別情報１０４１２とし、接続ポート情報１０４０２を接続ポート情報１０４１３とし、ＶＬＡＮ情報１０４０３をＶＬＡＮ情報１０４１４とする。端末管理設定部１０４３ａは、脅威加算スコア情報１０４３０に基づいて、脅威加算スコア１０４０７を脅威検知内容１０２３４と一致する検知内容１０４３０２に該当する脅威加算スコア１０４３０４とする（ステップＳ０２１）。

【０１３７】

端末情報更新部１０４２は、端末情報１０４１０から、ＭＡＣアドレス情報１０４０４とＩＰアドレス情報１０４０５とを含む組み合わせを検索する。該当する組み合わせが無い場合、端末情報更新部１０４２は、端末管理部設定情報１０４３の脅威加算スコア情報１０４３０で示される検知内容１０４３０２の「新規ＩＰ：ＭＡＣ出現」に該当する脅威加算スコア１０４３０４である「１０００」を、脅威加算スコア１０４０７とする（ステップＳ０２１）。ここでは、スイッチ識別情報１０４０１と接続ポート情報１０４０２とＶＬＡＮ情報１０４０３とは未定のままである。

【０１３８】

通信分析部１０２は、脅威を検知したかどうかを判定する（分岐Ｂ００３）。具体的には、脆弱性攻撃検知部１０２２１は通信データ１０１０にソフトウェアの脆弱性を攻撃するパターンが有る場合、マルウェア検知部１０２２２はマルウェアを示すパターンが含まれる場合、認証失敗検知部１０２２３は認証失敗の繰り返しが発生している場合に、セキュリティ異常として検知する。

【０１３９】

脅威が検知されない場合（分岐Ｂ００３でＮの場合）、つまり、脅威スコアがスコア値Ｚ未満である場合、端末情報管理部１０４は、端末更新情報１０４２０を生成し、脅威加算スコア１０４０７の値から次のステップを判定する。

【０１４０】

端末情報管理部１０４は、端末一時情報１０４０と端末情報１０４１０とに基づいて端末更新情報１０４２０を生成する。このとき、スイッチ識別情報１０４２１はスイッチ識別情報１０４０１となり、接続ポート情報１０４２２は接続ポート情報１０４０２となり、ＶＬＡＮ情報１０４２３はＶＬＡＮ情報１０４０３となり、ＭＡＣアドレス情報１０４２４はＭＡＣアドレス情報１０４０４となり、ＩＰアドレス情報１０４２５はＩＰアドレス情報１０４０５となり、更新時刻情報１０４２６は更新時刻情報１０４０６となる。端末情報管理部１０４は、脅威加算スコア１０４０７に脅威スコア１０４１８を加算した脅威スコア１０４２７を算出する。

【０１４１】

端末情報管理部１０４の端末情報更新部１０４２は、端末更新情報１０４２０の脅威スコア１０４２７が０より大きいか否かを判定する（分岐Ｂ０３０）。脅威スコア１０４２７が０である場合（分岐Ｂ０３０でＮの場合）、端末情報更新部１０４２は、ステップＳ００１に戻り次の通信データ１０１０の取得を行う。また、脅威スコア１０４２７が０よりも大きい場合（分岐Ｂ０３０でＹの場合）、端末情報更新部１０４２は、脅威スコア１０４２７が、脅威レベルの判定をグレーからブラックに変更するスコア値Ｚ（以下、スコア値Ｚとする）未満であるか否かを判定する（分岐Ｂ０３１）。

【０１４２】

脅威スコア１０４２７がスコア値Ｚ以上であれば（分岐Ｂ０３１でＮの場合）、端末情報更新部１０４２は、脅威レベルをブラックと判定し、ステップＳ００１に戻り次の通信データ１０１０の取得を行う。脅威スコア１０４２７がスコア値Ｚ未満であれば（分岐Ｂ０３１でＹの場合）、端末情報更新部１０４２は、脅威レベルをグレーと判定し、端末情報１０４１０の更新時刻情報１０４１７と端末更新情報１０４２０の更新時刻情報１０４２６を比較し、前回の更新時刻から時間ｔ０が経過しているかどうかを判定する（分岐Ｂ０３２）。

【０１４３】
ここで、時間ｔ０は、端末管理部基準値情報１０４３１の基準値内容１０４３１１で定義したものと同一であり、通信稼動前に定めておく必要がある値である。時間ｔ０は、例えば５分として、一定値にしてもよいし、通信稼動後に状況の変化に応じて何らかの基準を設けて変更してもよい。
【０１４４】
また、分岐Ｂ０３２の判定の代わりに、例えば通信容量Ｍ０、一定の通信パケット数Ｐ０、一定のＴＣＰセッション数Ｓ０を用いて判定してもよい。通信容量Ｍ０および通信パケット数Ｐ０の場合、通信容量および通信パケット数が、送信元端末３０２からの送信量を計測してもよいし、送信元端末３０２および送信先端末３０１からの送受信量を計測してもよい。
【０１４５】
また、分岐Ｂ０３２の判定において、時間ｔ０、通信容量Ｍ０、一定の通信パケット数Ｐ０および一定のＴＣＰセッション数Ｓ０を組み合わせて用いてもよい。また、端末管理部基準値情報１０４３１の基準値１０４３１２の値は、一例であり、役割によってそれぞれ異なる値を設定してもよい。
【０１４６】
時間ｔ０が経過していない場合（分岐Ｂ０３２でＮの場合）、端末情報更新部１０４２は、ステップＳ００１に戻り次の通信データ１０１０の取得を行う。前回の更新時刻から時間ｔ０が経過している場合（分岐Ｂ０３２でＹの場合）、端末情報更新部１０４２は、端末更新情報１０４２０の脅威スコア１０４２７を端末情報１０４１０の脅威スコア１０４２７から１を減じた値にする（ステップＳ０３３）。
【０１４７】
ここで、減じる値を１としているが、検知した脅威の種類および端末の役割に応じて減じる数値を変更してもよいし、減じる数値を脅威スコアの一定割合としてもよく、減じる値は１に限定されない。
【０１４８】
脅威が検知された場合（分岐Ｂ００３でＹの場合）、つまり、脅威スコアがスコア値Ｚ以上である場合、スイッチ操作部１０３のスイッチ情報取得部１０３２は、インテリジェントスイッチ２０から、最新のスイッチ情報１０３２０を取得する（ステップＳ００４）。スイッチ情報取得部１０３２は、最新のスイッチ情報１０３２０を端末情報管理部１０４に出力する。端末情報更新部１０４２は、端末更新情報１０４２０のスイッチ識別情報１０４２１と接続ポート情報１０４２２とＶＬＡＮ情報１０４２３とを更新する。
【０１４９】
ここで、スイッチ情報取得部１０３２は、例えばＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）などにより、インテリジェントスイッチ２０のポート１を通じて、最新のスイッチ情報１０３２０を取得することができる。なお、スイッチ情報取得部１０３２は、ＳＮＭＰ以外にも専用の通信線などによって最新のスイッチ情報１０３２０を取得してもよい。
【０１５０】
端末情報更新部１０４２は、端末更新情報１０４２０のＶＬＡＮ情報１０４２３がＶＬＡＮ１であるかどうかを判定する（分岐Ｂ００５）。ＶＬＡＮがＶＬＡＮ２である場合（分岐Ｂ００５でＮの場合）、分岐Ｂ００６に進み、ＶＬＡＮがＶＬＡＮ１である場合（分岐Ｂ００５でＹの場合）、分岐Ｂ００７に進む。
【０１５１】
端末情報更新部１０４２は、端末更新情報１０４２０の脅威スコア１０４２７が、ＶＬＡＮ２からＶＬＡＮ１へ変更する際の脅威スコア値Ｙよりも大きいかどうかを判定する（分岐Ｂ００６）。
【０１５２】
脅威スコア１０４２７が脅威スコア値Ｙよりも大きい場合（分岐Ｂ００６でＹの場合）

、経路変更部１０３３が接続ポート情報１０４２２の属するＶＬＡＮを切り換えることなくステップＳ００８へ進み、脅威スコア１０４２７が脅威スコア値Ｙ以下の場合（分岐Ｂ００６でＮの場合）、ステップＳ０６１へ進む。

【０１５３】

端末情報更新部１０４２は、端末更新情報１０４２０の脅威スコア１０４２７が、ＶＬＡＮ１からＶＬＡＮ２へ切り換える際の脅威スコア値Ｘよりも小さいかどうかを判定する（分岐Ｂ００７）。脅威スコア１０４２７が脅威スコア値Ｘよりも小さい場合（分岐Ｂ００７でＹの場合）、ステップＳ００８へ進み、脅威スコア１０４２７が脅威スコア値Ｘ以上の場合（分岐Ｂ００７でＮの場合）、ステップＳ０７１へ進む。

【０１５４】

ここで、分岐Ｂ００６と分岐Ｂ００７に用いる脅威スコア値Ｘおよび脅威スコア値Ｙは、同じ値であってもよいし、異なる値であってもよい。

【０１５５】

図５、図１１および図１４に示すように、端末更新情報１０４２０のＶＬＡＮ情報１０４２３に基づいて、経路変更部１０３３は、接続ポート情報１０４２２の属するＶＬＡＮをＶＬＡＮ２からＶＬＡＮ１に切り換える（ステップＳ０６１）。ステップＳ０６１は、検疫対象であった送信元端末３０２を、検疫系ネットワークから通常系ネットワークに戻す処理であり、図１３Ｂの送信元端末３０２の属するＶＬＡＮ２から図１３ＡのＶＬＡＮ１に属するように切り換える処理である。

【０１５６】

図１３Ａは、送信元端末３０２からの脅威が検知される前であり、端末管理部基準値情報１０４３１の脅威スコアが図９の脅威スコア値Ｘを下回っている状態、または、端末管理部基準値情報１０４３１の脅威スコアが、図９の脅威スコア値Ｙを上回る状態から脅威スコア値Ｙ以下の状態に変化した後の論理的なネットワークを示す。

【０１５７】

経路変更部１０３３は、例えばＳＮＭＰなどにより、インテリジェントスイッチ２０のポート１を通じて、スイッチのポートのＶＬＡＮを設定することができる。なお、経路変更部１０３３は、ＳＮＭＰ以外にも専用の通信線などを用いて設定してもよい。

【０１５８】

端末更新情報１０４２０のＶＬＡＮ情報１０４２３に基づいて経路変更部１０３３は、接続ポート情報１０４２２の属するＶＬＡＮをＶＬＡＮ１からＶＬＡＮ２に切り換える（ステップＳ０７１）。

【０１５９】

ステップＳ０７１は、通常系ネットワークに属していた送信元端末３０２を、検疫系ネットワークに属するように切り換える処理であり、図１３Ａの送信元端末３０２の属するＶＬＡＮ１から図１３ＢのＶＬＡＮ２に属するように切り換える処理である。

【０１６０】

また、図１３Ｂは、送信元端末３０２からの脅威が検知された後であり、端末管理部基準値情報１０４３１の脅威スコアが、図９の脅威スコア値Ｘを下回る状態から脅威スコア値Ｘ以上の状態に変化し、かつ、端末管理部基準値情報１０４３１の図９の脅威スコア値Ｙを上回ったままの状態での論理的なネットワークを示す。

【０１６１】

端末情報更新部１０４２は、端末更新情報１０４２０に基づいて、端末情報１０４１０を更新する（ステップＳ００８）。具体的には、端末情報更新部１０４２は、スイッチ識別情報１０４１２とスイッチ識別情報１０４２１と、接続ポート情報１０４１３が接続ポート情報１０４２２と、ＶＬＡＮ情報１０４１４がＶＬＡＮ情報１０４２３と、ＭＡＣアドレス情報１０４１５がＭＡＣアドレス情報１０４２４と、ＩＰアドレス情報１０４１６がＩＰアドレス情報１０４２５と一致しているかどうかを、それぞれ確認する。これら全て一致する場合、端末情報更新部１０４２は、一致する組み合わせを持つ管理ＩＤの更新時刻情報１０４１７を更新時刻情報１０４２６に、脅威スコア１０４１８を脅威スコア１

０４２７に、それぞれ更新する。一方、これら全て一致するわけでない場合、端末情報更新部１０４２は、新しい管理ＩＤを割り当て、スイッチ識別情報１０４１２をスイッチ識別情報１０４２１に、接続ポート情報１０４１３を接続ポート情報１０４２２に、ＶＬＡＮ情報１０４１４をＶＬＡＮ情報１０４２３に、ＭＡＣアドレス情報１０４１５をＭＡＣアドレス情報１０４２４に、ＩＰアドレス情報１０４１６をＩＰアドレス情報１０４２５に、更新時刻情報１０４１７を更新時刻情報１０４２６に、脅威スコア１０４１８を脅威スコア１０４２７に設定する。端末情報更新部１０４２は、このように更新した後に、ステップＳ００１に戻り次の通信データ１０１０の取得を行う。図１２Ｂは、図１２Ａの状態の端末情報１０４１０が、図１１の端末更新情報１０４２０によって更新された場合を示す。そして、端末情報更新部１０４２は、処理をステップＳ００１に戻す。

【０１６２】

７－１．脅威スコアの更新動作

次に、脅威スコアの更新の動作の詳細について説明する。図１５は、本実施の形態における脅威スコアを更新する処理を示すフローチャートである。図１５は、図１４の分岐Ｂ００３における、端末更新情報１０４２０の脅威スコア１０４２７の更新処理を示す。

【０１６３】

図１５等に示すように、端末情報更新部１０４２は、スイッチ識別情報１０４１２とスイッチ識別情報１０４２１とが全て一致しているかどうかを確認する。この確認は、端末情報更新部１０４２がステップＳ１０２からステップＳ１０６を繰り返す以下のループ処理によって行われる（Ｓ１０１）。具体的には、端末情報更新部１０４２は、端末情報１０４１０の管理ＩＤの全てに対して、端末一時情報１０４０のスイッチ識別情報１０４０１と接続ポート情報１０４０２とＶＬＡＮ情報１０４０３とＭＡＣアドレス情報１０４０４とＩＰアドレス情報１０４０５との組み合わせが含まれているかどうかを確認する。

【０１６４】

端末情報更新部１０４２は、スイッチ識別情報１０４０１とスイッチ識別情報１０４１２とが一致しているかどうかを判定する（ステップＳ１０２）。一致していなければ（ステップＳ１０２でＮの場合）、含まれている管理ＩＤが無い、つまり、端末一時情報１０４０が端末情報１０４１０に含まれていないことが示される。端末情報更新部１０４２は、脅威加算スコア１０４０７を端末更新情報１０４２０の脅威スコア１０４２７とする（ステップＳ１０８）。そして、端末情報更新部１０４２は、処理を終了する。

【０１６５】

一致していれば（ステップＳ１０２でＹの場合）、端末情報更新部１０４２は、スイッチ識別情報１０４０２ａとスイッチ識別情報１０４１３ａとが一致しているかどうかを判定する（ステップＳ１０３）。一致していなければ（ステップＳ１０３でＮの場合）、端末情報更新部１０４２は、ステップＳ１０８に進む。

【０１６６】

一致していれば（ステップＳ１０３でＹの場合）、端末情報更新部１０４２は、スイッチ識別情報１０４０３ａとスイッチ識別情報１０４１４ａとが一致しているかどうかを判定する（ステップＳ１０４）。一致していなければ（ステップＳ１０４でＮの場合）、端末情報更新部１０４２は、ステップＳ１０８に進む。

【０１６７】

一致していれば（ステップＳ１０４でＹの場合）、端末情報更新部１０４２は、スイッチ識別情報１０４０４ａとスイッチ識別情報１０４１５ａとが一致しているかどうかを判定する（ステップＳ１０５）。一致していなければ（ステップＳ１０５でＮの場合）、端末情報更新部１０４２は、ステップＳ１０８に進む。

【０１６８】

一致していれば（ステップＳ１０５でＹの場合）、端末情報更新部１０４２は、スイッチ識別情報１０４０５ａとスイッチ識別情報１０４１６ａとが一致しているかどうかを判定する（ステップＳ１０６）。一致していなければ（ステップＳ１０６でＮの場合）、端末情報更新部１０４２は、ステップＳ１０８に進む。

【０１６９】
一致していれば（ステップＳ１０６でＹの場合）、端末情報更新部１０４２は、該当する管理ＩＤの脅威スコア１０４１８と、端末一時情報１０４０の脅威加算スコア１０４０７との和を、端末更新情報１０４２０の脅威スコア１０４２７とする（ステップＳ１０７）。そして、端末情報更新部１０４２は、処理を終了する。
【０１７０】
７－２．端末情報の更新動作
次に、端末情報１０４１０の更新の動作について詳細に説明する。図１６は、本実施の形態における端末情報を更新する処理を示すフローチャートである。図１６は、図１４のＳ００９の端末情報１０４１０の更新処理を示す。図１５と同様の処理については同一の符号を付してその説明を適宜省略する。
【０１７１】
図１６等に示すように、端末情報更新部１０４２は、ステップＳ１０２からステップＳ１０６を繰り返す以下のループ処理を行う（Ｓ１０１）。ステップＳ１０２からステップＳ１０６の処理において、端末情報１０４１０の管理ＩＤの全てが一致する場合（ステップＳ１０６でＹの場合）、端末情報更新部１０４２は、該当する管理ＩＤにおける図１２Ａの更新時刻情報１０４１７を更新時刻情報１０４２６に基づいて更新し、図１２Ａの脅威スコア１０４１８を脅威スコア１０４２７に基づいて更新する（ステップＳ１１７）。そして、端末情報更新部１０４２は、処理を終了する。
【０１７２】
端末情報更新部１０４２は、含まれている管理ＩＤが無い場合（端末一時情報１０４０が端末情報１０４１０に含まれていない場合）、新たな管理ＩＤを追加して端末更新情報を登録する（ステップＳ１１８）。そして、端末情報更新部１０４２は、処理を終了する。
【０１７３】
８．脅威除去部の動作
脅威除去部１０５は、ＶＬＡＮ１とＶＬＡＮ２との双方に接続されている。脅威除去部１０５は、ＶＬＡＮ１に属する送信先端末３０１とＶＬＡＮ２に属する送信元端末３０２との間の通信から、脅威を含む通信データ１０１０を除去する。或いは、脅威除去部１０５は、ＶＬＡＮ１に属する送信先端末３０１とＶＬＡＮ２に属する送信元端末３０２との間の通信から、脅威を含む通信データ１０１０を無害化するために通信データ１０１０の有害な部分を破棄、或いは、無害なものに書き換えた正常な通信データ１０１０を通過させる機能を有する。
【０１７４】
脅威除去部１０５は、トランスペアレントモードといわれる脅威除去部１０５が通信ネットワーク上で端末として存在しないようにふるまう形態としてもよく、この場合には送信元端末３０２のＶＬＡＮを切り換えた場合にもそのまま通信を継続することができる。
【０１７５】
また、ネットワーク防御装置１０は、ＶＬＡＮ１とＶＬＡＮ２との間のルータとして振る舞う形態としてもよく、この場合には、送信先端末３０１から送信元端末３０２に通信する際には脅威除去部１０５が送信元端末３０２のように振るまい、送信元端末３０２から送信先端末３０１に通信する際には脅威除去部１０５が送信先端末３０１のように振る舞えばよい。具体的には、ＡＲＰコマンドを用いてもよい。
【０１７６】
９．実施の形態の効果
本実施の形態により、インテリジェントスイッチ２０を経由する通信データ１０１０のコピーを通信分析部１０２で監視し続けることで、脅威を検知することができる。また、脅威を検知すると、スイッチ操作部が、脅威を含みうる送信先端末３０１が属する通信ネットワーク（ＶＬＡＮ２）と、送信元端末３０２、３０４が属する通信ネットワーク（ＶＬＡＮ１）とを論理的に切り離すことができる。つまり、脅威を含みうる送信元端末３０２、３０４が属するＶＬＡＮ２と送信先端末３０１が属するＶＬＡＮ１との境界に、脅威

除去部１０５を論理的に接続する。こうして、脅威を含みうる送信元端末３０２、３０４が送信した通信データ１０１０から脅威を除去することができる。これにより、正常な通信に悪影響を与えることなくセキュリティ異常の拡散を防ぐことができる。

【０１７７】

また、送信元端末３０２、３０４が属する通信ネットワークと送信先端末３０１が属する通信ネットワークとの正常な通信を継続するため、脅威を検知する通信分析部１０２と脅威を除去する脅威除去部１０５とを分離している。このため、それぞれの処理部の処理負荷を最小限にすることができる。これにより、通信分析部１０２が探索行動などによって脅威に到る前に脅威を検知してから、脅威除去部１０５による脅威の除去を適用することができる。その結果、より早期にセキュリティの脅威に対応することができる。

【０１７８】

したがって、工場など制御システムネットワークに必要な端末の無停止稼動と通信遅延の最小化とを実現することができる。また、通信ネットワーク内の脅威を監視したり、脅威の拡散を抑制したりすることで、セキュリティレベルを向上させることができる。

【０１７９】

１０．実施の形態１のその他の変形例

本開示を上記実施の形態に基づいて説明してきたが、本開示は、上記実施の形態１に限定されず、以下のような、実施の形態１の変形例１、実施の形態１の変形例２も本開示に含まれる。

【０１８０】

実施の形態１の変形例１（以下、本変形例）について説明する。ネットワークの全体構成として、図１では、ネットワーク防御装置１０に１つのインテリジェントスイッチ２０を接続する構成としたが、複数のインテリジェントスイッチを接続する構成であってもよい。図１７Ａは、本変形例におけるネットワーク防御装置１０が属する通信ネットワークの全体構成を示す図である。

【０１８１】

図１７Ａに示すように、通信ネットワークは、ネットワーク防御装置１０、インテリジェントスイッチ２０、送信先端末３０１、送信元端末３０２に加え、インテリジェントスイッチ２１、送信先端末３０３、送信元端末３０４がＬＡＮケーブルで接続されて構成される。

【０１８２】

この通信ネットワークでは、インテリジェントスイッチ２０のポート３とインテリジェントスイッチ２１のポート０とをＬＡＮケーブルを介して接続する。また、この通信ネットワークでは、ネットワーク防御装置１０をインテリジェントスイッチ２１のポート１とポート３とに、それぞれＬＡＮケーブルを介して接続する。

【０１８３】

インテリジェントスイッチ２１は、送信元端末３０４と送信先端末３０３との通信稼動開始時に、インテリジェントスイッチ２１のポート０とポート４とポート７とをＶＬＡＮ１に、ポート１をＶＬＡＮ２に、ネットワーク防御装置１０に接続したポート３をミラー機能に設定する。通信データ取得部１０１は、インテリジェントスイッチ２１のポート３からも通信データ１０１０を取得する。ネットワーク防御装置１０とインテリジェントスイッチ２１のポート１との間では、例えばインテリジェントスイッチ２１の制御用コマンドが通信される。

【０１８４】

送信元端末３０４と送信先端末３０３とが通常系ネットワークで通信を行う場合は、上述の図１３Ａと同様である。通信分析部１０２により、通信データ１０１０から脅威が検知された場合、図１７Ｂのように、検疫系ネットワークで通信を行う。図１７Ｂは、本変形例において、送信元端末と送信先端末とが検疫系ネットワークで通信を行う場合を示す図である。スイッチ操作部１０３は、脅威を含みうる送信元端末３０４が属する通信ネットワーク（ＶＬＡＮ２）と、送信先端末３０３が属する通信ネットワーク（ＶＬＡＮ１）

とを論理的に切り離す。

【０１８５】

具体的には、スイッチ操作部１０３は、送信元端末３０４がインテリジェントスイッチ２１のポート７、ポート１を介してネットワーク防御装置１０の脅威除去部１０５に接続するＶＬＡＮ２と、ネットワーク防御装置１０の脅威除去部１０５がインテリジェントスイッチ２０のポート２、ポート３、インテリジェントスイッチ２１のポート０、ポート４、を介して送信先端末３０３に接続するＶＬＡＮ１となるように、切り換える。こうして、送信元端末３０４は、インテリジェントスイッチ２１のポート７、ポート１、ネットワーク防御装置１０、インテリジェントスイッチ２０のポート２、ポート３、インテリジェントスイッチ２１のポート０、ポート４を介して送信先端末３０３と接続される。

【０１８６】

また、図１７Ｃのように、送信元端末３０４と送信先端末３０１とが通常系ネットワークで通信を行う場合、送信元端末３０４は、インテリジェントスイッチ２１のポート７、ポート０、インテリジェントスイッチ２０のポート３、ポート４を介して送信先端末３０１と接続される。図１７Ｃは、実施の形態１の変形例１において、送信元端末と送信先端末とが通常系ネットワークで通信を行う場合を示す図である。図示はしないが、送信元端末３０４と送信先端末３０１とが検疫系ネットワークで通信を行う場合、スイッチ操作部１０３は、送信元端末３０４がインテリジェントスイッチ２１のポート７、ポート０、インテリジェントスイッチ２０のポート３、ポート２を介してネットワーク防御装置１０の脅威除去部１０５に接続するＶＬＡＮ２と、ネットワーク防御装置１０の脅威除去部１０５がインテリジェントスイッチ２０のポート０、ポート４を介して送信先端末３０１に接続するＶＬＡＮ１となるように、切り換える。

【０１８７】

このような構成を採ることで、本変形例のネットワーク防御装置１０は、通信ネットワークを構成する端末の無停止稼動を実現し、かつ、送信元端末３０２、３０４と送信先端末３０１、３０３と間のような、複数の端末間における通信遅延の最小化も実現しながら、セキュリティレベルを向上させることができる。

【０１８８】

図１７Ｂのように太い実線の経路は第２の通信経路の一例であり、図１７Ｃのように太い実線の経路は第１の通信経路の一例である。

【０１８９】

実施の形態１の変形例２（以下、本変形例）について説明する。通信ネットワークの全体構成として、ネットワーク防御装置１０に複数のインテリジェントスイッチを接続する図１７Ａとは別の構成であってもよい。図１８は、本実施の形態におけるネットワーク防御装置１０が属する通信ネットワークの全体構成を示す図である。

【０１９０】

図１８に示すように、通信ネットワークは、ネットワーク防御装置１０、インテリジェントスイッチ２０、送信先端末３０１、送信元端末３０２に加え、インテリジェントスイッチ２１、送信先端末３０３、送信元端末３０４がＬＡＮケーブルで接続されて構成される。

【０１９１】

この通信ネットワークでは、インテリジェントスイッチ２０のポート３とインテリジェントスイッチ２１のポート０とをＬＡＮケーブルを介して接続する。必要に応じて、インテリジェントスイッチ２１に接続されていないポートをミラー機能として設定し、ネットワーク防御装置１０に接続してもよい。

【０１９２】

インテリジェントスイッチ２１は、送信元端末３０４と送信先端末３０３との通信稼動開始時に、インテリジェントスイッチ２０のポート３とインテリジェントスイッチ２１のポート０とをトランクラインとして設定し、インテリジェントスイッチ２１のポート４とポート７とをＶＬＡＮ１に設定する。

【０１９３】
送信元端末３０４と送信先端末３０３とが通常系ネットワークで通信を行う場合は、上述の図１３Ａと同様である。検疫系ネットワークで通信を行う場合、スイッチ操作部１０３は、送信元端末３０４がインテリジェントスイッチ２１のポート７、ポート０を介してネットワーク防御装置１０の脅威除去部１０５に接続するＶＬＡＮ２（太い実線で示す）と、ネットワーク防御装置１０の脅威除去部１０５がインテリジェントスイッチ２０のポート１、ポート３、インテリジェントスイッチ２１のポート０、ポート４、を介して送信先端末３０３に接続するＶＬＡＮ１となるように、切り換える。図１８のような経路が第１の通信経路の一例となる。
【０１９４】
このような構成を採ることで、ネットワーク防御装置１０は、複数のインテリジェントスイッチ（本実施の形態では、インテリジェントスイッチ２０およびインテリジェントスイッチ２１）に接続される通信ネットワークを防御することができる。
【０１９５】
（実施の形態２）
［構成］
本実施の形態における他の構成は、特に明記しない場合は、実施の形態１と同様であり、同一の構成については同一の符号を付して構成に関する詳細な説明を省略する。
【０１９６】
２１．通信ネットワークの全体構成
ネットワーク防御装置１０は、通信データ取得部１０１、通信分析部１０２、スイッチ操作部１０３、端末情報管理部１０４、および、脅威除去部１０５の他に、さらにパケット書換部１０６を備える。
【０１９７】
インテリジェントスイッチ２０のポート０は、インテリジェントスイッチ２０を通過する通信データ１０１０のコピーを出力可能なミラー機能を備える。ポート１は、通信データ１０１０にＶＬＡＮグループを区別するタグ情報を付加するタグポート機能を備える。ポート２～７は、一般的なスイッチングハブのポートと同様の振る舞いをする通常ポートである。ポート１は、第６のポートの一例である。
【０１９８】
また、ネットワーク防御装置１０は、インテリジェントスイッチ２０のポート０、ポート１に接続される。送信先端末３０１はポート４に接続され、送信元端末３０２はポート７に接続され、送信先端末３０３はポート５に接続され、送信元端末３０４はポート６に接続されている。ポート７は、第５のポートの一例である。ポート４は、第７のポートの一例である。
【０１９９】
また、送信元端末３０２から、インテリジェントスイッチ２０のポート４、ポート７、および、送信先端末３０１は、ＶＬＡＮ１ａに属している。送信元端末３０４から、ポート５、ポート６、および、送信先端末３０１は、ＶＬＡＮ１ａとは異なるＶＬＡＮ１ｂに属している。送信元端末３０２、３０４および送信先端末３０１、３０３は、同一のインテリジェントスイッチ２０に接続されているが、異なるＶＬＡＮ間、すなわち、ＶＬＡＮ１ａとＶＬＡＮ１ｂとの間は、通信できない。
【０２００】
また、インテリジェントスイッチ２０のポート１とネットワーク防御装置１０を接続する通信路は、トランクラインであり、複数のＶＬＡＮグループ、例えば、ＶＬＡＮ１ａとＶＬＡＮ１ｂとを区別して通信データ１０１０を送受信する。この通信データ１０１０には、ＶＬＡＮグループを特定するタグ情報が挿入される。なお、本実施の形態では、インテリジェントスイッチ２０のポート２とネットワーク防御装置１０とは接続されていない。
【０２０１】
インテリジェントスイッチ２０は、通常ポートであるポート４～７が通信データ１０１

０を受信すると、通信データ１０１０に含まれるアドレスの送信先端末３０１が、ポートの所属するＶＬＡＮ（以降、所属ＶＬＡＮと呼ぶ）と同一のポートに接続されていない場合、送信先端末３０１の所属ＶＬＡＮを示すタグ情報を通信データ１０１０に付加し、タグポートであるポート１からこの通信データ１０１０を送信する。

【０２０２】

また、インテリジェントスイッチ２０は、タグポートであるポート１が通信データ１０１０を受信すると、通信データ１０１０に含まれる所属ＶＬＡＮを示すタグ情報を参照し、タグ情報に対応するＶＬＡＮグループに属する通常ポートを選択する。インテリジェントスイッチ２０は、通信データ１０１０からタグ情報を除去し、送信先端末３０１に接続されたポートを介し、送信先端末３０１に通信データ１０１０を送信する。

【０２０３】

２２．ネットワーク防御装置の構成

次にネットワーク防御装置１０の詳細について説明する。

【０２０４】

スイッチ操作部１０３は、ポートのＶＬＡＮを切り換える際、例えば、ＶＬＡＮ１ａまたはＶＬＡＮ１ｂからＶＬＡＮ２ａまたはＶＬＡＮ２ｂ（図２５Ａ、２５Ｂで後に示す）に、或いは、ＶＬＡＮ２ａまたはＶＬＡＮ２ｂからＶＬＡＮ１ａまたはＶＬＡＮ１ｂに切り換える。ここで、ＶＬＡＮ１ａとＶＬＡＮ１ｂは、通常系ネットワークであり、ＶＬＡＮ２ａとＶＬＡＮ２ｂとは、検疫系ネットワークである。例えば、送信先端末３０１がＶＬＡＮ１ａに属し、送信元端末３０２がＶＬＡＮ２ａに属し、送信先端末３０３がＶＬＡＮ１ｂに属し、送信元端末３０４がＶＬＡＮ２ｂに属する。

【０２０５】

脅威除去部１０５は、ＶＬＡＮ２ａまたはＶＬＡＮ２ｂに属する端末に係る通信データ１０１０を受信し、通信データ１０１０から脅威を除去した上で本来の送信先端末３０１または送信先端末３０３に出力する機能を備える。

【０２０６】

パケット書換部１０６は、脅威除去部１０５を通過した脅威除去後の通信データに含まれる通信ネットワークのＶＬＡＮ情報を書き換える。具体的には、パケット書換部１０６は、ポート１から入力され脅威除去部１０５を通過した脅威除去後の通信データの所属ＶＬＡＮ情報１０１１ａをＶＬＡＮ１ａまたはＶＬＡＮ１ｂからＶＬＡＮ２ａまたはＶＬＡＮ２ｂへ、或いは、ＶＬＡＮ２ａまたはＶＬＡＮ２ｂからＶＬＡＮ１ａまたはＶＬＡＮ１ｂへ書き換える（変更する）。このように書き換えた後に、パケット書換部１０６は、再びインテリジェントスイッチ２０のポート１に、書き換えられた通信データを送信する。パケット書換部１０６は、書換部の一例である。

【０２０７】

２２－１．通信データの構成

図２０は、本実施の形態における通信データ１０１０の構成を示す図である。通信データ１０１０には、少なくとも、所属ＶＬＡＮ情報１０１１ａと送信元アドレス情報１０１１と送信先アドレス情報１０１２とペイロード１０１３とが含まれる。

【０２０８】

所属ＶＬＡＮ情報１０１１ａは、例えばＩＥＥＥ８０２．１Ｑで規定されているタグ情報であり、Ｅｔｈｅｒｎｅｔフレームに挿入されてＶＬＡＮの識別に利用される。

【０２０９】

２３．端末通信情報の構成

次に、端末通信情報１０２３の詳細について説明する。図２１は、本実施の形態における端末通信情報１０２３の構成を示す図である。

【０２１０】

図２１に示すように、端末通信情報１０２３は、端末番号１０２３０とＩＰアドレス情報１０２３１とＭＡＣアドレス情報１０２３２とＶＬＡＮ情報１０２３２ａと更新時刻情報１０２３３と脅威検知内容１０２３４とで構成される。

【０２１１】
端末アドレス確認部１０２０から取得した所属ＶＬＡＮ情報１０１１ａはＶＬＡＮ情報１０２３２ａとされる。ＩＰアドレス情報１０２３１、送信元ＭＡＣアドレス情報１０２３２、および、ＶＬＡＮ情報１０２３２ａを取得した時刻は、更新時刻情報１０２３３とされる。
【０２１２】
２４．スイッチ初期設定情報の構成
次に、スイッチ初期設定情報１０３１の詳細について説明する。図２２は、本実施の形態におけるスイッチ初期設定情報１０３１の構成を示す図である。
【０２１３】
図２２に示すように、スイッチ初期設定情報１０３１は、スイッチ識別情報１０３１１とスイッチ制御用ＩＰアドレス１０３１２とが対応したスイッチ識別情報テーブル１０３１０と、ＶＬＡＮ情報１０３１４とＶＬＡＮグループ情報１０３１４ａとＶＬＡＮネットワーク種類１０３１５とがそれぞれ対応したＶＬＡＮ識別情報テーブル１０３１３とで構成される。
【０２１４】
ＶＬＡＮ識別情報テーブル１０３１３にて定義されたＶＬＡＮ情報１０３１４は、インテリジェントスイッチ２０のポート１であるトランクラインについて、通信データ１０１０の出力対象となるＶＬＡＮとして設定する。
【０２１５】
ＶＬＡＮグループ情報１０３１４ａは、ＶＬＡＮ１ａ、ＶＬＡＮ１ｂ、ＶＬＡＮ２ａ、および、ＶＬＡＮ２ｂにそれぞれ割り得てられた所属するグループを示す情報である。ＶＬＡＮグループ情報１０３１４ａは、あらかじめネットワークに割り当てられていたＶＬＡＮ情報１０３１４にそれぞれ対応付けられる。
【０２１６】
なお、ＶＬＡＮグループ情報１０３１４ａは、通信分析部１０２によって、それぞれ異なる検知内容で検知された情報であってもよい。また、特定のＶＬＡＮグループ情報１０３１４ａでのみ脅威を検知するように、通信分析部１０２が設定されていてもよい。
【０２１７】
端末管理部基準値情報１０４３１は、基準値内容１０４３１１と基準値１０４３１２とを含む。基準値内容１０４３１１としては、「脅威スコア減算までの時間ｔ０」と、「ＶＬＡＮネットワーク種類が通常系から検疫系へ変更する際の脅威スコア値Ｘ」と、「ＶＬＡＮネットワーク種類が検疫系ネットワークから通常系ネットワークへ変更する際の脅威スコア値Ｙ」と、「脅威レベルの判定をグレーからブラックに変更するスコア値Ｚ」とを含む。
【０２１８】
２５．端末情報の構成
次に、端末情報１０４１０の詳細について説明する。図２４Ａおよび図２４Ｂは、本実施の形態における端末情報１０４１０の構成を示す図である。図２４Ａの端末情報１０４１０は、送信元端末３０２からの脅威が検知される前の情報を示し、図２４Ｂの端末情報１０４１０は、送信元端末３０２からの脅威が検知された後の情報を示している。
【０２１９】
２６．脅威検知前と脅威検知後の論理的なネットワークの構成
次に、送信元端末３０２からの脅威が検知される前と後のネットワーク全体構成の詳細について説明する。図２５Ａおよび図２５Ｂは、本実施の形態におけるネットワーク全体構成の論理的なネットワーク構成を示す図である。図２５Ａは、送信元端末３０２からの脅威が検知される前の論理的なネットワーク構成を示し、図２５Ｂは、送信元端末３０２からの脅威が検知された後の論理的なネットワーク構成を示す。図２５Ａおよび図２５Ｂに示すように、脅威除去部１０５およびパケット書換部１０６は、トランクラインＴＲＵＮＫ１に設定されたインテリジェントスイッチ２０のポート１を介して接続している。な

お、図２５Ａおよび図２５Ｂでは、便宜上、インテリジェントスイッチ２０のポート０とネットワーク防御装置１０とを接続するＬＡＮケーブルを省略している。

【０２２０】

図２５Ａは、送信元端末３０２または送信元端末３０４からの脅威が検知される前であり、端末管理部基準値情報１０４３１の脅威スコアが図９の脅威スコア値Ｘを下回っている状態、または、端末管理部基準値情報１０４３１の脅威スコアが図９の脅威スコア値Ｙを上回る状態から脅威スコア値Ｙ以下の状態に変化した後の論理的なネットワークを示す。送信先端末３０１と、ポート４と、ポート７と、送信元端末３０２とは、共にＶＬＡＮ１ａに含まれ、送信先端末３０３と、ポート５と、ポート６と、送信元端末３０４とは共にＶＬＡＮ１ｂ含まれ、脅威除去部１０５およびパケット書換部１０６を介さずに通信を行っている。

【０２２１】

送信先端末３０１は、ＶＬＡＮ１ａに接続されたままである。スイッチ操作部１０３がインテリジェントスイッチ２０に接続しているポート７をＶＬＡＮ１ａからＶＬＡＮ２ａに切り換えることで、送信元端末３０２は、ＶＬＡＮ２ａに接続される。送信先端末３０１および送信元端末３０２は、脅威除去部１０５とパケット書換部１０６とを介して通信を行う。

【０２２２】

また、送信先端末３０３は、ＶＬＡＮ１ｂに接続されたままである。送信元端末３０４は、インテリジェントスイッチ２０に接続しているポート６をＶＬＡＮ１ｂからＶＬＡＮ２ｂに切り換えることで、送信元端末３０４は、ＶＬＡＮ２ｂに接続される。送信先端末３０３および送信元端末３０４は、脅威除去部１０５とパケット書換部１０６とを介して通信を行う。

【０２２３】

図２５Ａのように太い実線の経路、および、太い破線の経路は、第１の通信経路の一例である。

【０２２４】

図２０、および、図２５Ｂに示すように、ポートのＶＬＡＮ設定が切り換わると、インテリジェントスイッチ２０は、ポート７、或いは、ポート６から入力された通信データ１０１０に所属ＶＬＡＮ情報１０１１ａを挿入（タグ付け）し、ポート１からトランクラインＴＲＵＮＫ１を介してネットワーク防御装置１０に出力する。

【０２２５】

ネットワーク防御装置１０の脅威除去部１０５は、送信元端末３０２および送信元端末３０４に係る通信データ１０１０から脅威を除去する。脅威を除去した後、パケット書換部１０６は、脅威除去後の通信データの所属ＶＬＡＮ情報１０１１ａについて、ＶＬＡＮ識別情報テーブル１０３１３を参照し、ＶＬＡＮ１ａからＶＬＡＮ２ａまたはＶＬＡＮ２ａからＶＬＡＮ１ａ、或いはＶＬＡＮ１ｂからＶＬＡＮ２ｂまたはＶＬＡＮ２ｂからＶＬＡＮ１ｂなどと、通常系ネットワークから検疫系ネットワークまたは検疫系ネットワークから通常系ネットワークへのＶＬＡＮ情報に書き換えを行う。

【０２２６】

ＶＬＡＮ情報を書き換えられた通信データは、トランクラインＴＲＵＮＫ１を通ってインテリジェントスイッチ２０のポート１に戻る。インテリジェントスイッチ２０は、書き換えられた通信データの所属ＶＬＡＮ情報１０１１ａを参照して書き換えられた通信データの送信先ポートを決定するとともに、所属ＶＬＡＮ情報１０１１ａを書き換えられた通信データより削除する。インテリジェントスイッチ２０は、所属ＶＬＡＮ情報１０１１ａを削除した通信データを送信先ポートから送信する。

【０２２７】

図２５Ｂのように太い実線の経路、および、太い破線の経路は、第２の通信経路の一例である。

【０２２８】

以上より、端末側の処理を変更することなく送信元端末３０２は送信先端末３０１と、送信元端末３０４は送信先端末３０３と、それぞれ正常な通信を行うことができる。

【０２２９】

なお、本実施の形態では、送信元端末３０２および送信元端末３０４からの脅威が同時に検知される場合について説明したが、これに限られない。例えば、送信元端末３０２または送信元端末３０４のいずれか一方による脅威が検知される場合に、論理的なネットワーク構成を変更するようにしてもよい。

【０２３０】

２７．ネットワーク防御装置の動作

次に、ネットワーク防御装置１０の動作について詳細に説明する。図２６は、本実施の形態におけるネットワーク防御装置の動作を示すフローチャートである。

【０２３１】

図２６の動作は実施の形態１の図１４と同様であり、図１４と同様の処理については同一の符号を付してその説明を適宜省略する。

【０２３２】

図２６に示すように、ネットワーク防御装置１０は、通信データ１０１０を取得する（ステップＳ００１）。通信分析部１０２は、通信データ１０１０を分析する（ステップＳ００２）。端末情報管理部１０４は、脅威スコア１０４２７を算出する（ステップＳ０２１）。通信分析部１０２は、脅威を検知したかどうかを判定する（分岐Ｂ００３）。

【０２３３】

脅威が検知された場合（分岐Ｂ００３でＹの場合）、スイッチ情報取得部１０３２は、インテリジェントスイッチ２０から、最新のスイッチ情報１０３２０を取得する（ステップＳ００４）。そして、処理は、分岐Ｂ１０５に進む。

【０２３４】

脅威が検知されない場合（分岐Ｂ００３でＮの場合）、端末情報管理部１０４は、脅威スコア１０４２７が０より大きいか否かを判定する（分岐Ｂ０３０）。脅威スコア１０４２７が０である場合（分岐Ｂ０３０でＮの場合）、ステップＳ００１に戻る。また、脅威スコア１０４２７が０よりも大きい場合（分岐Ｂ０３０でＹの場合）、端末情報更新部１０４２は、脅威スコア１０４２７が、脅威レベルの判定をグレーからブラックに変更するスコア値Ｚ（以下、スコア値Ｚとする）未満であるか否かを判定する（分岐Ｂ０３１）。

【０２３５】

脅威スコア１０４２７がスコア値Ｚ以上であれば（分岐Ｂ０３１でＮの場合）、ステップＳ００１に戻る。脅威スコア１０４２７がスコア値Ｚ未満であれば（分岐Ｂ０３１でＹの場合）、端末情報更新部１０４２は、前回の更新時刻から時間ｔ０が経過しているかどうかを判定する（分岐Ｂ０３２）。

【０２３６】

時間ｔ０が経過していない場合（分岐Ｂ０３２でＮの場合）、ステップＳ００１に戻る。前回の更新時刻から時間ｔ０が経過している場合（分岐Ｂ０３２でＹの場合）、端末情報更新部１０４２は、脅威スコア１０４２７から１を減じた値にする（ステップＳ０３３）。

【０２３７】

端末情報更新部１０４２は、ＶＬＡＮ情報１０４２３とＶＬＡＮ識別情報テーブル１０３１３とから、ＶＬＡＮネットワーク種類が通常系ネットワークであるかどうかを判定する（分岐Ｂ１０５）。

【０２３８】

検疫系ネットワークの場合（分岐Ｂ１０５でＮの場合）は、分岐Ｂ００６に進み、ＶＬＡＮネットワーク種類が通常系ネットワークである場合（分岐Ｂ１０５でＹの場合）は、分岐Ｂ００７に進む。

【０２３９】

端末情報更新部１０４２は、脅威スコア１０４２７が検疫系ネットワークから通常系ネ

ットワークへ切り換えする際の脅威スコア値Ｙよりも大きいかどうかを判定する（分岐Ｂ００６）。

【０２４０】

脅威スコア１０４２７が脅威スコア値Ｙよりも大きい場合（分岐Ｂ００６でＹの場合）、経路変更部１０３３が接続ポート情報１０４２２の属するＶＬＡＮを切り換えることなくステップＳ００８へ進み、脅威スコア１０４２７が脅威スコア値Ｙ以下の場合（分岐Ｂ００６でＮの場合）、ステップＳ１６１へ進む。

【０２４１】

端末情報更新部１０４２は、脅威スコア１０４２７が、通常系ネットワークから検疫系ネットワークへ切り換える際の脅威スコア値Ｘよりも小さいかどうかを判定する（分岐Ｂ００７）。脅威スコア１０４２７が脅威スコア値Ｘよりも小さい場合（分岐Ｂ００７でＹの場合）、ステップＳ００８へ進み、脅威スコア１０４２７が脅威スコア値Ｘ以上の場合（分岐Ｂ００７でＮの場合）、ステップＳ１７１へ進む。

【０２４２】

端末更新情報１０４２０のＶＬＡＮ情報１０４２３から、ＶＬＡＮ識別情報テーブル１０３１３のＶＬＡＮグループ情報１０３１４ａに対応するＶＬＡＮ情報１０３１４に基づいて、パケット書換部１０６は、接続ポート情報１０４２２の属するＶＬＡＮ情報を通常系ネットワークのＶＬＡＮ情報に書き換える（ステップＳ１６１）。

【０２４３】

ステップＳ１６１は、検疫対象であった送信元端末３０２、３０４を、検疫系ネットワークから通常系ネットワークに戻す処理である。ステップＳ１６１は、図２５Ｂの送信元端末３０２の接続しているインテリジェントスイッチ２０のポートの属するＶＬＡＮ情報が、ＶＬＡＮ２ａから図２５ＡのＶＬＡＮ１ａに属するように書き換える処理である。または、ステップＳ１６１は、図２５Ｂの送信元端末３０４の接続しているインテリジェントスイッチ２０のポートの属するＶＬＡＮ情報がＶＬＡＮ２ｂから図２５ＡのようにＶＬＡＮ１ｂに属するように書き換える処理である。

【０２４４】

端末更新情報１０４２０のＶＬＡＮ情報１０４２３から、ＶＬＡＮ識別情報テーブル１０３１３のＶＬＡＮグループ情報１０３１４ａに対応するＶＬＡＮ情報１０３１４に基づいて、パケット書換部１０６は、接続ポート情報１０４２２の属するＶＬＡＮを検疫系ネットワークのＶＬＡＮ情報に書き換える（ステップＳ１７１）。

【０２４５】

ステップＳ１７１は、通常系ネットワークに属していた送信元端末３０４を、検疫系ネットワークに属するように書き換える処理であり、図２５Ａの送信元端末３０２の接続しているインテリジェントスイッチ２０のポートの属するＶＬＡＮ情報がＶＬＡＮ１ａから図２５ＢのＶＬＡＮ２ａに属するように書き換える処理である。または、ステップＳ１７１は、図２５Ｂの送信元端末３０４の接続しているインテリジェントスイッチのポートの属するＶＬＡＮ情報がＶＬＡＮ１ｂから図２５ＢのようにＶＬＡＮ２ｂに属するように書き換える処理である。

【０２４６】

端末情報更新部１０４２は、端末情報１０４１０を更新する（ステップＳ００８）。そして、端末情報更新部１０４２は、処理をステップＳ００１に戻す。

【０２４７】

２８．脅威除去部の動作

脅威除去部１０５は、トランクラインを介して接続されている。脅威除去部１０５は、ＶＬＡＮ１ａに属する送信先端末３０１とＶＬＡＮ２ａに属する送信元端末３０２との間、および、ＶＬＡＮ１ｂに属する送信先端末３０３とＶＬＡＮ２ｂに属する送信元端末３０４との間で行われる通信から、脅威となる通信データ１０１０を除去し、正常な通信データ１０１０を通過させる機能を有する。

【０２４８】

脅威除去部１０５は、トランスペアレントモードといわれる脅威除去部１０５が通信ネットワーク上で端末として存在しないように振る舞う形態としてもよい。この場合には、送信元端末３０２および送信元端末３０４のＶＬＡＮを切り換えた場合にもそのまま通信を継続することができる。

【０２４９】

また、脅威除去部１０５は、通常系ネットワークと検疫系ネットワークとの間のルータとして振る舞う形態としてもよい。この場合には、送信先端末３０１から送信元端末３０２に通信する際には脅威除去部１０５が送信元端末３０２のように振る舞い、送信元端末３０２から送信先端末３０１に通信する際には脅威除去部１０５が送信先端末３０１のように振る舞い、或いは、送信先端末３０３から送信元端末３０４に通信する際には脅威除去部１０５が送信元端末３０４のように振る舞い、送信元端末３０４から送信先端末３０３に通信する際には脅威除去部１０５が送信先端末３０３のように振る舞うようになればよい。具体的には、ＡＲＰコマンドを用いてもよい。

【０２５０】

２９．パケット書換部の動作

次に、パケット書換部１０６の構成について、詳細に説明する。図２７は、本実施の形態におけるパケット書換部１０６の構成を示す図である。

【０２５１】

図２７に示すように、パケット書換部１０６は、インテリジェントスイッチ２０のポート１のトランクラインＴＲＵＮＫ１と脅威除去部１０５との間に設けられ、脅威除去部１０５で脅威除去後の通信データのＶＬＡＮ所属情報を書き換える機能を有する。

【０２５２】

脅威除去部１０５に入力されるパケットの通信データ１０１０は、所属ＶＬＡＮ情報が通常系ネットワークのＶＬＡＮ情報と検疫系ネットワークのＶＬＡＮ情報とで異なる。そのため、脅威除去部１０５からインテリジェントスイッチ２０に脅威除去後の通信データを送信するだけでは、送信先端末３０１、３０３が所属ＶＬＡＮ情報に示されるポートに接続されていないため、インテリジェントスイッチ２０と送信先端末３０１、３０３との間で通信が成立しない。そこでパケット書換部１０６は、脅威除去部１０５に入力されるパケットについてＶＬＡＮ識別情報テーブル１０３１３を参照し、同一のＶＬＡＮグループ情報に含まれるＶＬＡＮ情報に相互変換する。

【０２５３】

これにより、送信元端末３０２から送信先端末３０１に通信する際、脅威除去部１０５を通過した脅威除去後の通信データは、所属ＶＬＡＮ情報がＶＬＡＮ２ａからＶＬＡＮ１ａに、パケット書換部１０６によって書き換えられる。そして、インテリジェントスイッチ２０のポート１が受信した書き換えられた通信データの送信先は、送信先端末３０１が接続されているＶＬＡＮ１ａのポート４になる。

【０２５４】

また、送信先端末３０１から送信元端末３０２に通信する際に、脅威除去部１０５を通過した脅威除去後の通信データは、所属ＶＬＡＮ情報がＶＬＡＮ１ａからＶＬＡＮ２ａに、パケット書換部１０６によって書き換えられる。そして、インテリジェントスイッチ２０のポート１が書き換えられた通信データの送信先は、送信元端末３０２が接続されているＶＬＡＮ２ａのポート７になる。

【０２５５】

こうして、送信元端末３０２と送信先端末３０１との間で、通信が維持される。

【０２５６】

また、送信元端末３０４から送信先端末３０３に通信する際に、脅威除去部１０５を通過した脅威除去後の通信データは、所属ＶＬＡＮ情報がＶＬＡＮ２ｂからＶＬＡＮ１ｂに、パケット書換部１０６によって書き換えられる。そして、インテリジェントスイッチ２０のポート１が受信した書き換えられた通信データの送信先は、送信先端末３０３が接続されているＶＬＡＮ１ａのポート５になる。

【０２５７】
　また、送信先端末３０３から送信元端末３０４に通信する際に、脅威除去部１０５を通過した脅威除去後の通信データの所属ＶＬＡＮ情報がＶＬＡＮ１ｂからＶＬＡＮ２ｂに、パケット書換部１０６によって書き換えられ、インテリジェントスイッチ２０のポート１が受信した書き換えられた通信データの送信先は、送信元端末３０４が接続されているＶＬＡＮ２ｂのポート６になる。
【０２５８】
　こうして、送信元端末３０４と送信先端末３０３との間で、通信が維持される。
【０２５９】
　３０．実施の形態２のその他の変形例
　本開示を上記実施の形態に基づいて説明してきたが、本開示は、上記実施の形態に限定されず、以下のような、実施の形態２の変形例１、実施の形態２の変形例２場合も本開示に含まれる。
【０２６０】
　実施の形態２の変形例１（以下、本変形例）について説明する。図２８に示すように、インテリジェントスイッチ２０のポート３とインテリジェントスイッチ２１のポート０とは、トランクラインＴＲＵＮＫ２で接続される。ネットワーク防御装置１０は、トランクラインＴＲＵＮＫ１を介してインテリジェントスイッチ２０のポート１に接続する。
【０２６１】
　インテリジェントスイッチ２１は、送信元端末３０４と送信先端末３０３との通信稼動開始時に、インテリジェントスイッチ２１のポート４とポート７とをＶＬＡＮ１ａに設定する。また、ＬＡＮケーブルを介してネットワーク防御装置１０とインテリジェントスイッチ２１の任意のポートとを接続したミラー機能に設定してもよい。このとき、通信データ取得部１０１は、インテリジェントスイッチ２１の任意のポートからも通信データ１０１０を取得する。
【０２６２】
　送信元端末３０４と送信先端末３０３とが通常系ネットワークで通信を行う場合は、上述の図１３Ａと同様である。また、送信元端末３０４と送信先端末３０３とが検疫系ネットワークで通信を行う場合は、上述の図１７Ｂと同様である。図２８のように太い実線の経路は、第２の通信経路の一例である。
【０２６３】
　このような構成を採ることで、本変形例のネットワーク防御装置１０は、インテリジェントスイッチ２０およびインテリジェントスイッチ２１に接続されるネットワークを防御することができる。
【０２６４】
　実施の形態２の変形例２（以下、本変形例）について説明する。ネットワークの全体構成として、図２８では、１つのネットワーク防御装置１０に１つのインテリジェントスイッチ２０を接続する構成としたが、ネットワーク防御装置１０の機能を分散させて、複数のネットワーク防御装置を備える構成であり、さらに図２９のように複数のインテリジェントスイッチ２０を接続する構成であってもよい。図２９は、本実施の形態におけるネットワーク防御装置１０、１１が属する通信ネットワークの全体構成を示す図である。
【０２６５】
　図２９に示すように、通信ネットワークは、ネットワーク防御装置１０、１１、インテリジェントスイッチ２０、送信先端末３０１、送信元端末３０２に加え、インテリジェントスイッチ２１、送信先端末３０３、送信元端末３０４がＬＡＮケーブルで接続されて構成される。インテリジェントスイッチ２１では、インテリジェントスイッチ２１を通過する通信データ１０１０のコピーを出力可能なミラー機能をポート３に備える。また、インテリジェントスイッチ２１では、ポート１とネットワーク防御装置１１とがＬＡＮケーブルで接続されて構成される。ネットワーク防御装置１０とインテリジェントスイッチ２１のポート１との間では、例えばインテリジェントスイッチ２１の制御用コマンドが通信さ

れる。

【０２６６】

この通信ネットワークでは、インテリジェントスイッチ２１に接続されるネットワーク防御装置１１は、通信データ取得部１１１、通信分析部１１２、端末情報管理部１１４から構成される。

【０２６７】

送信元端末３０４と送信先端末３０３とが通常系ネットワークで通信を行う場合は、上述の図１３Ａと同様である。検疫系ネットワークで通信を行う場合、スイッチ操作部１０３は、送信元端末３０４がインテリジェントスイッチ２１のポート７、ポート０、インテリジェントスイッチ２０のポート３、ポート１、を介してネットワーク防御装置１０の脅威除去部１０５に接続するＶＬＡＮ２ｂと、ネットワーク防御装置１０の脅威除去部１０５がインテリジェントスイッチ２０のポート１、ポート３、インテリジェントスイッチ２１のポート０、ポート４、を介して送信先端末３０３に接続するＶＬＡＮ１ｂとなるように、切り換える。このとき、パケット書換部１０６は、脅威除去部１０５を通過した通信データ１０１０の所属ＶＬＡＮ情報を、パケット書換部１０６がＶＬＡＮ１ｂからＶＬＡＮ２ｂに書き換える。なお、インテリジェントスイッチ２１のポート１はミラー機能として設定されている。図２９のように太い実線の経路は、第２の通信経路の一例である。

【０２６８】

このような構成をとることで、複数のインテリジェントスイッチ２０、２１から構成されるネットワークにおいて脅威検知を分散して実行することで、各々のインテリジェントスイッチ２０、２１を通過する通信データ１０１０について１台のネットワーク防御装置に集中して脅威検知することがなくなるため、ネットワークの負荷を軽減することができる。

【０２６９】

３１．その他の変形例

（１）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、図示はしないが、ネットワーク防御装置１０には、端末情報管理部１０４で管理する全ての情報の中から端末情報１０４１０など任意の情報を取得し適切に表示してもよい。また、ネットワーク防御装置１０は、必要に応じて利用者が情報を更新し設定を行うための入力部を備えてもよい。

【０２７０】

例えば、スイッチ初期設定情報１０３１および端末管理部設定情報１０４３は、通信稼動前にいったん設定する必要があるが、表示部と入力部を用いて確認できるように設定してもよく、ネットワーク防御装置１０によって通信稼働中に設定変更できるようにしてもよい。

【０２７１】

また、ネットワーク防御装置１０は、利用者が特定の端末の脅威スコアを高めるための入力がされることで、その端末が接続されるポートのＶＬＡＮを切り換える設定を行えるような、表示部と入力部とを備えていてもよい。

【０２７２】

またこのとき、ネットワーク防御装置１０は、端末情報１０４１０の脅威スコア１０４１８を時系列にグラフ化して表示することで、端末の脅威を可視化し、設定変更する基準として用いてもよい。

【０２７３】

（２）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、図１のネットワーク防御装置１０は、１つの装置として図示されているが、インテリジェントスイッチ２０と一体となった装置でもよい。また、ネットワーク防御装置１０の全ての機能を単一の機器のみで実現する必要はなく、ネットワーク防御装置１０は、複数の機器を用いて構成されていてもよい。また、インテリジェントスイッチ２０は、例えばＳＤＮスイッチを用いてもよく、ＯｐｅｎＦｌｏｗの様な制御用通信プロトコルを活用してもよい。

【０２７４】
（３）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、各機能はコンピュータプログラムとして構成してもよく、また、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）と呼ばれる専用のＬＳＩ（Ｌａｒｇｅ Ｓｃａｌｅ Ｉｎｔｅｇｒａｔｅｄ－ｃｉｒｃｕｉｔ：集積回路）として構成してもよく、また、ＰＬＤ（Ｐｒｏｇｒａｍｍａｂｌｅ Ｌｏｇｉｃ Ｄｅｖｉｃｅ）およびＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）の様な、機能変更可能なＬＳＩを用いて構成してもよく、また、これらを含む複数の方法を組み合わせて構成してもよい。また、ネットワーク防御装置１０に含まれる複数の機能或いは全ての機能を単一のＳｏＣ（Ｓｙｓｔｅｍ ｏｎ ａ Ｃｈｉｐ：システムＬＳＩ）と呼ばれるＬＳＩとして構成してもよい。また、これらのような、コンピュータプログラム、ＬＳＩ、ＦＰＧＡ、ＳｏＣと同等の機能を実現する技術があれば、それらを用いて構成してもよい。

【０２７５】
（４）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、図３における通信フロー情報解析部１０２１または通信データ解析部１０２２の一部または全部は、市販されるＩＤＳを活用してもよい。

【０２７６】
（５）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、図３における通信分析部１０２の、通信フロー情報解析部１０２１に含まれる１０２１１～１０２１４と、通信データ解析部１０２２に含まれる１０２２１～１０２２３に関して、これらの一部のみを用いてもよく、また、これら以外の分析部を用いてもよい。

【０２７７】
例えば、機械学習を用いたパターン解析結果を点数評価してから判定する方法、通信分析部１０２が含む全ての方法の中から任意の方法を選択し相関を判定する方法、過去の通信を分析した結果との相関を判定する方法、過去からの通信のパターンを抽出しそこから外れる度合いを点数評価して判定する方法などが考えられる。

【０２７８】
（６）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、脅威除去部１０５は、一般的に市販されるＩＰＳ、ＦＷ、ＵＴＭなどを用いてもよい。

【０２７９】
（７）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、脅威除去部１０５は、ＩＰＳのように脅威となる通信データ１０１０のみをシグネチャ方式と呼ばれる方法で除去するようにしてもよいし、最低限通過させなければいけない通信情報をホワイトリストとして準備し、ホワイトリストに合致しない通信データの一切を除去するとしてもよい。

【０２８０】
（８）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、ＩＰアドレスを固定で記載しているが、例えば、ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）を用いてもよい。

【０２８１】
（９）上記の実施の形態１、２および実施の形態１、２の変形例１、２では、脅威除去部１０５は、通信データ１０１０に含まれる脅威を除去するとしているが、通信データそのものを除去してもよい。この場合、送信先端末には、通信データの送信はされなくてもよい。

【０２８２】
以上のように、一つまたは複数の態様に係るネットワーク防御装置およびネットワーク防御システムについて、実施の形態１、２および実施の形態１、２の変形例１、２に基づいて説明したが、本開示は、この実施の形態１、２および実施の形態１、２の変形例１、２に限定されるものではない。本開示の趣旨を逸脱しない限り、当業者が思いつく各種変

形を本実施の形態１、２および実施の形態１、２の変形例１、２に施したもの、および、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

【産業上の利用可能性】

【０２８３】

本開示は、サブネットワーク内の端末間の通信から脅威、或いは、脅威の疑いを検知し、脅威のある通信データを除去することが可能であり、脅威の検知と脅威の除去とを分離した処理を行うことで、より早期の検知とより確実な端末の隔離とを実現できる。また、通信および制御の遅延を最小化し、施設、工場などの制御システムの誤動作リスクを最小化しながら、サブネットワーク内のセキュリティレベルを高めることが可能である。

【符号の説明】

【０２８４】

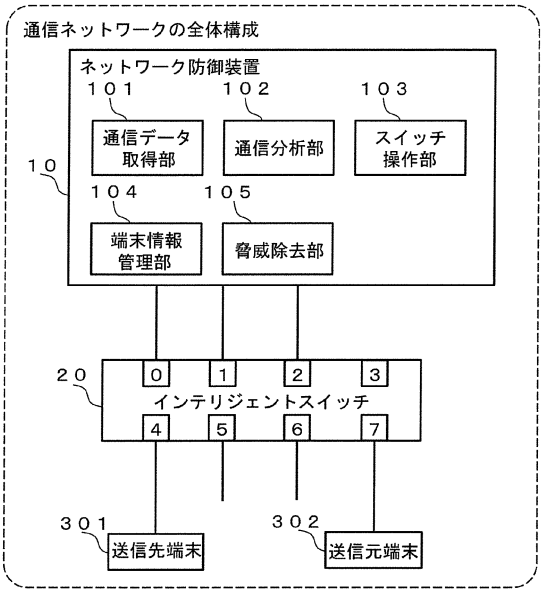
１０、１１　ネットワーク防御装置
１０１、１１１　通信データ取得部
１０１０　通信データ
１０１１　送信元アドレス情報
１０１１ａ　所属ＶＬＡＮ情報
１０１２　送信先アドレス情報
１０１１１　送信元ＭＡＣアドレス情報
１０１１２　送信元ＩＰアドレス情報
１０１１３　送信元ポート情報
１０１３　ペイロード
１０１２１　送信先ＭＡＣアドレス情報
１０１２２　送信先ＩＰアドレス情報
１０１２３　送信先ポート情報
１０２、１１２　通信分析部（脅威検知部）
１０２０　端末アドレス確認部
１０２１　通信フロー情報解析部
１０２１１　ブラックリスト通信検知部
１０２１２　ホワイトリスト外通信検知部
１０２１３　ＩＰスキャン検知部
１０２１４　ポートスキャン検知部
１０２２　通信データ解析部
１０２２１　脆弱性攻撃検知部
１０２２２　マルウェア検知部
１０２２３　認証失敗検知部
１０２３　端末通信情報
１０２３０　端末番号
１０２３１　ＩＰアドレス情報
１０２３２　ＭＡＣアドレス情報
１０２３２ａ　ＶＬＡＮ情報
１０２３３　更新時刻情報
１０２３４　脅威検知内容
１０３　スイッチ操作部（経路変更部）
１０３１　スイッチ初期設定情報
１０３１０　スイッチ識別情報テーブル
１０３１１　スイッチ識別情報
１０３１２　スイッチ制御用ＩＰアドレス
１０３１３　ＶＬＡＮ識別情報テーブル
１０３１４　ＶＬＡＮ情報

１０３１４ａ　ＶＬＡＮグループ情報
１０３１５　ＶＬＡＮネットワーク種類
１０３２　スイッチ情報取得部
１０３２０　スイッチ情報
１０３２１　スイッチ識別情報
１０３２２　接続ポート情報
１０３２３　ＶＬＡＮ情報
１０３２４　ＭＡＣアドレス情報
１０３３　経路変更部
１０４、１１４　端末情報管理部
１０４０　端末一時情報
１０４０１　スイッチ識別情報
１０４０２　接続ポート情報
１０４０２ａ　スイッチ識別情報
１０４０３　ＶＬＡＮ情報
１０４０３ａ　スイッチ識別情報
１０４０４　ＭＡＣアドレス情報
１０４０４ａ　スイッチ識別情報
１０４０５　ＩＰアドレス情報
１０４０５ａ　スイッチ識別情報
１０４０６　更新時刻情報
１０４０７　脅威加算スコア
１０４１　端末情報記憶部
１０４１０　端末情報
１０４１１　管理ＩＤ情報
１０４１２　スイッチ識別情報
１０４１３　接続ポート情報
１０４１３ａ　スイッチ識別情報
１０４１４　ＶＬＡＮ情報
１０４１４ａ　スイッチ識別情報
１０４１５　ＭＡＣアドレス情報
１０４１５ａ　スイッチ識別情報
１０４１６　ＩＰアドレス情報
１０４１６ａ　スイッチ識別情報
１０４１７　更新時刻情報
１０４１８　脅威スコア
１０４２　端末情報更新部
１０４２０　端末更新情報
１０４２１　スイッチ識別情報
１０４２２　接続ポート情報
１０４２３　ＶＬＡＮ情報
１０４２４　ＭＡＣアドレス情報
１０４２５　ＩＰアドレス情報
１０４２６　更新時刻情報
１０４２７　脅威スコア
１０４３　端末管理部設定情報
１０４３ａ　端末管理設定部
１０４３０　脅威加算スコア情報
１０４３０１　検知内容識別情報
１０４３０２　検知内容

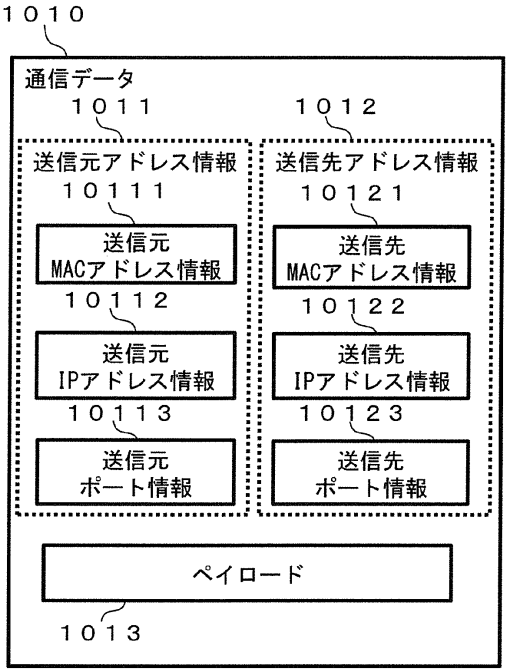
１０４３０３　判定
１０４３０４　脅威加算スコア
１０４３１　端末管理部基準値情報
１０４３１１　基準値内容
１０４３１２　基準値
１０５　脅威除去部
１０６　パケット書換部（書換部）
２０、２１　インテリジェントスイッチ
３０１、３０３　端末
３０２、３０４　攻撃端末

【図面】

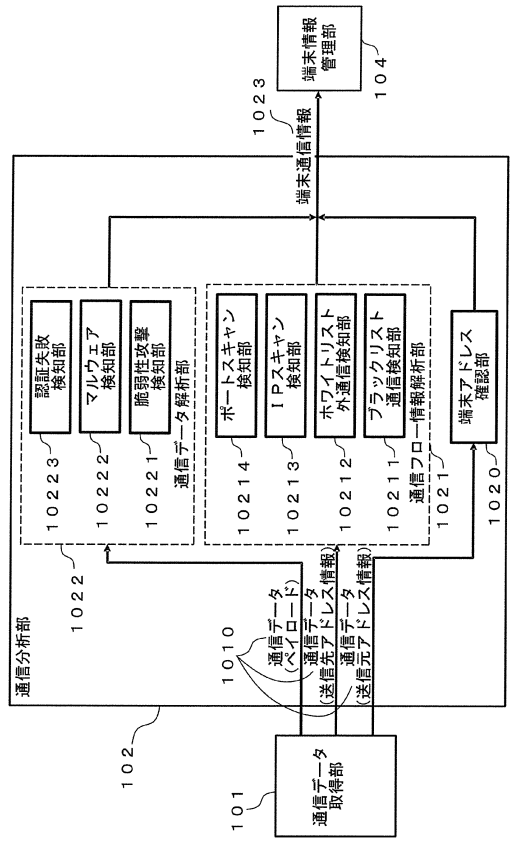
【図１】



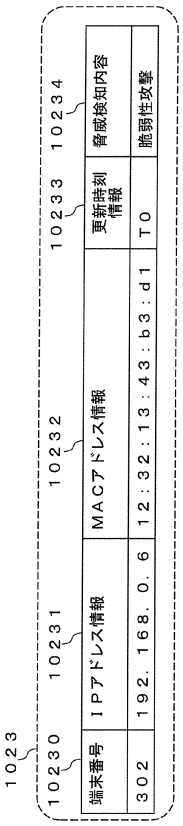
【図２】



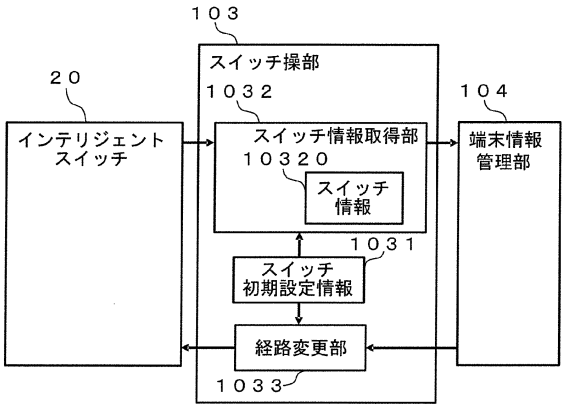
【図３】


端末情報管理部
104
1023
端末通信情報
通信分析部
認証失敗検知部
マルウェア検知部
脆弱性攻撃検知部
通信データ解析部
10223
10222
10221
1022
ポートスキャン検知部
IPスキャン検知部
ホワイトリスト外通信検知部
ブラックリスト通信検知部
通信フロー情報解析部
10214
10213
10212
10211
1021
端末アドレス確認部
1020
1010
通信データ（ペイロード）
通信データ（送信先アドレス情報）
通信データ（送信元アドレス情報）
102
101
通信データ取得部

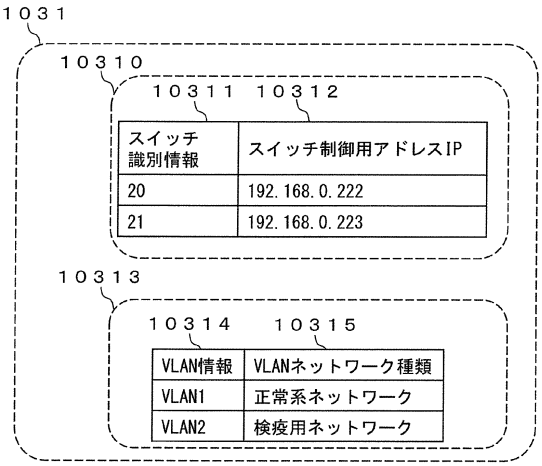
【図４】


1023
10230
端末番号
302
10231
IPアドレス情報
192.168.0.6
10232
MACアドレス情報
12:32:13:43:b3:d1
10233
更新時刻情報
T0
10234
脅威検知内容
脆弱性攻撃

【図５】


103
スイッチ操部
20
インテリジェントスイッチ
1032
スイッチ情報取得部
10320
スイッチ情報
104
端末情報管理部
1031
スイッチ初期設定情報
経路変更部
1033

【図６】

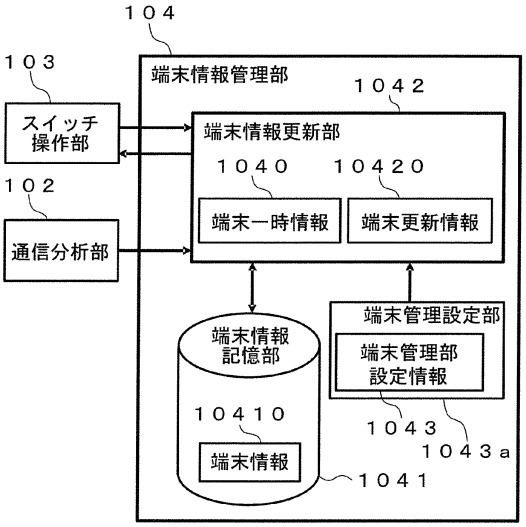

1031
10310
10311
10312
スイッチ識別情報
スイッチ制御用アドレスIP
20
192.168.0.222
21
192.168.0.223
10313
10314
10315
VLAN情報
VLANネットワーク種類
VLAN1
正常系ネットワーク
VLAN2
検疫用ネットワーク

【図７】

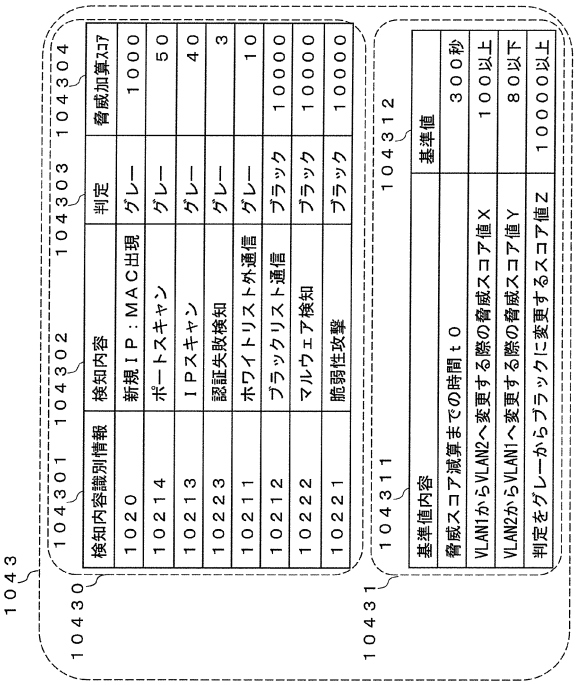
10320

	10321 スイッチ識別情報	10322 接続ポート情報	10323 VLAN情報	10324 MACアドレス情報
301	20	4	VLAN1	12:32:13:43:a5:s6
302	20	7	VLAN2	12:32:13:43:b3:d1

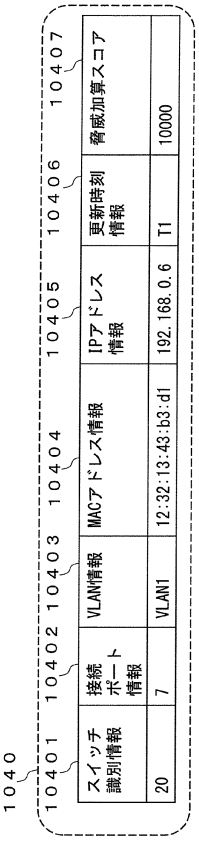
【図８】



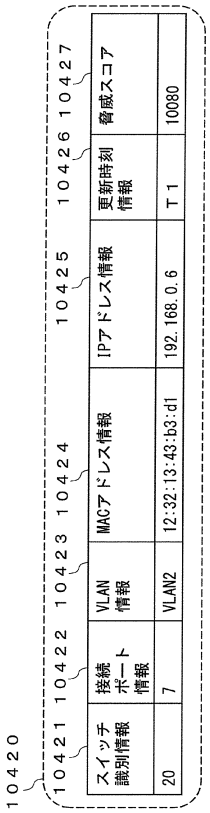
【図９】



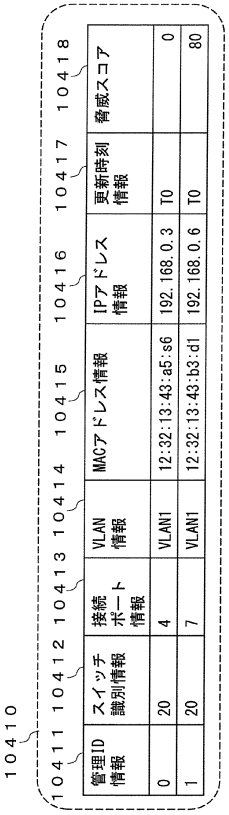
【図１０】



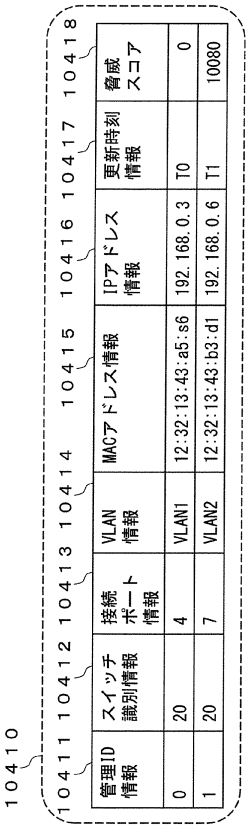
【図１１】



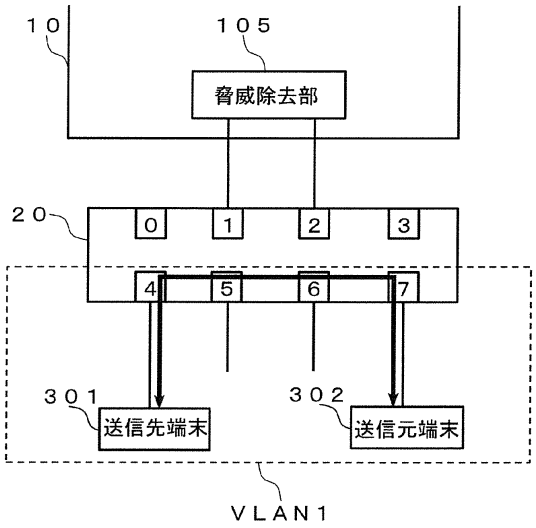
【図１２Ａ】



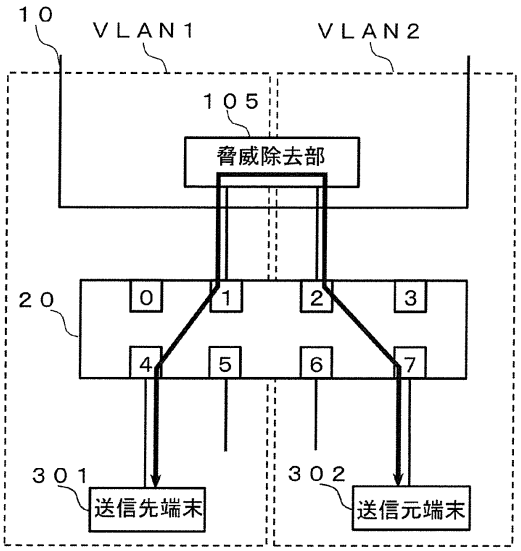
【図１２Ｂ】



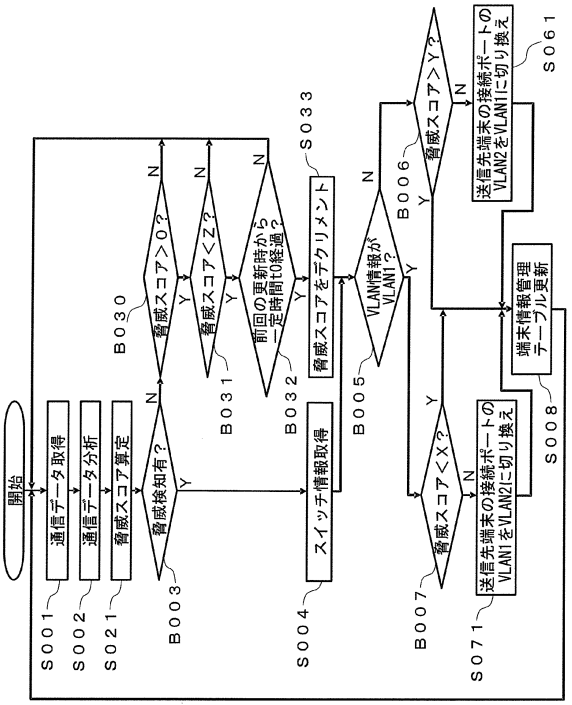
【図１３Ａ】



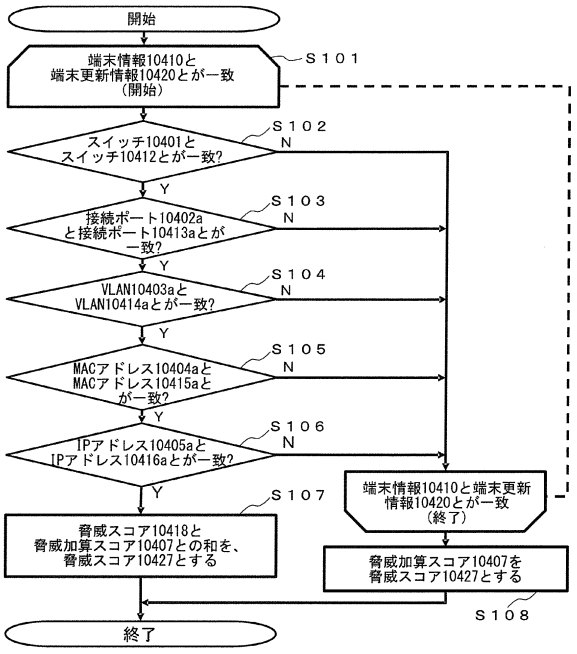
【図１３Ｂ】



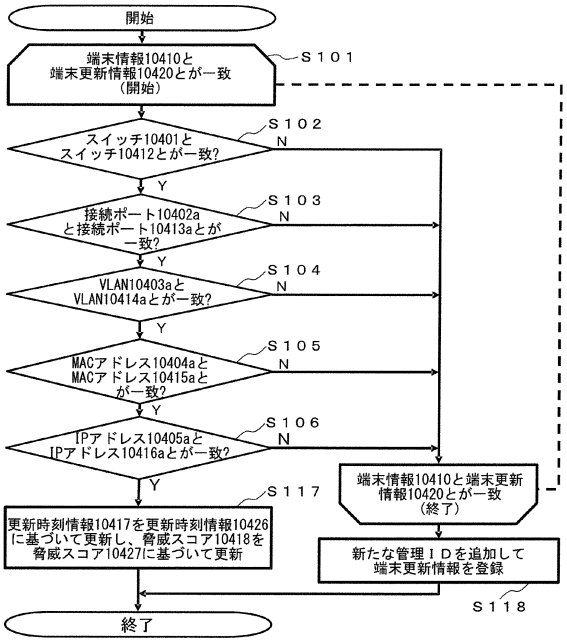
【図１４】



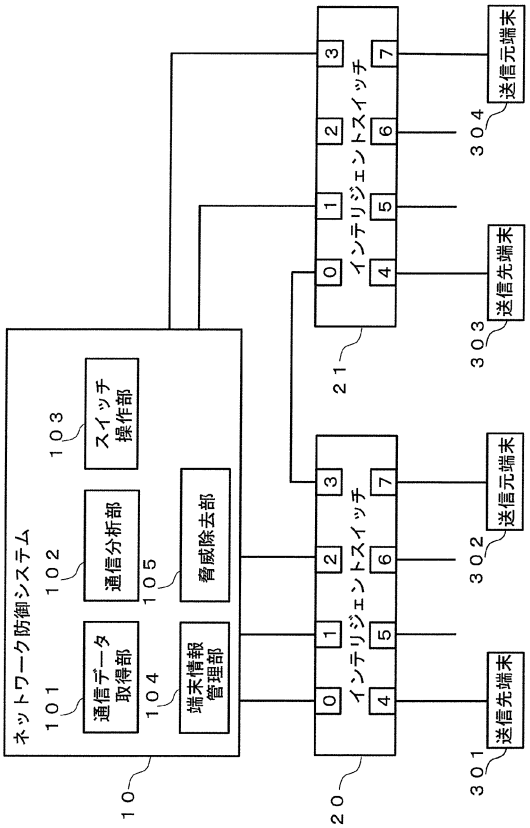
【図１５】



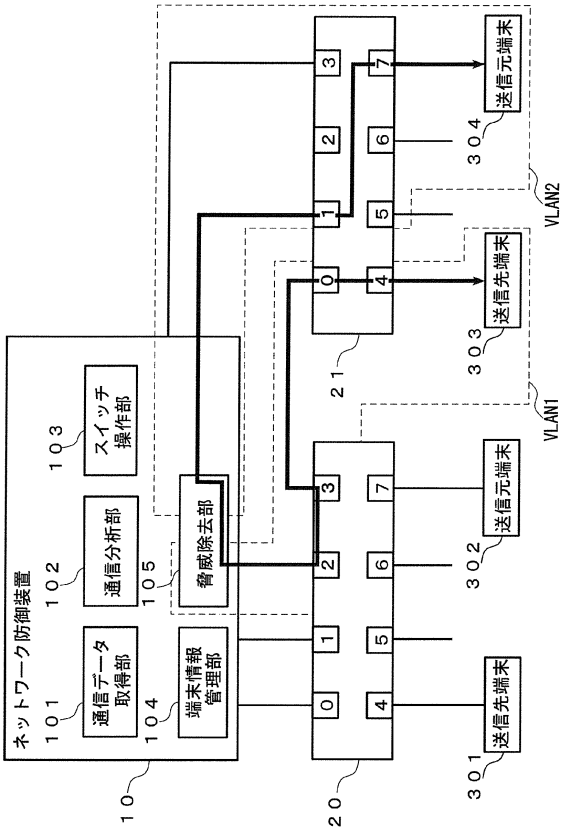
【図１６】



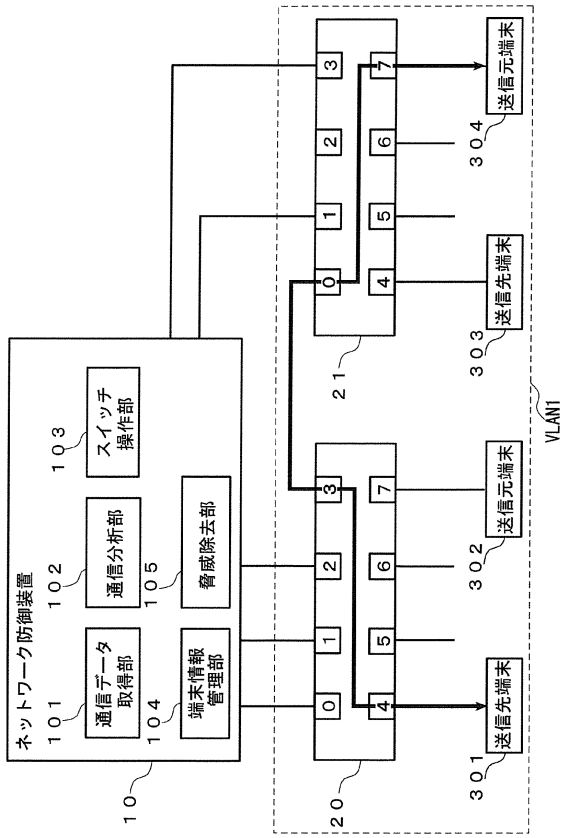
【図１７Ａ】



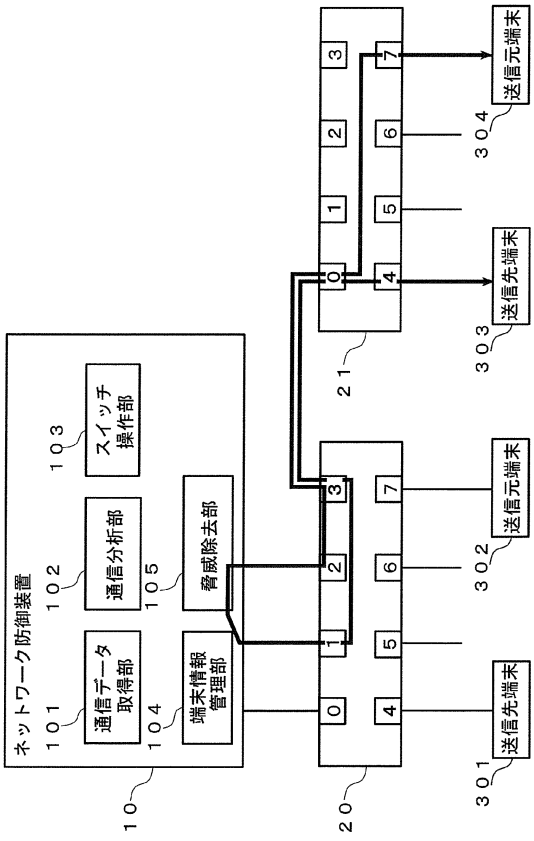
【図１７Ｂ】



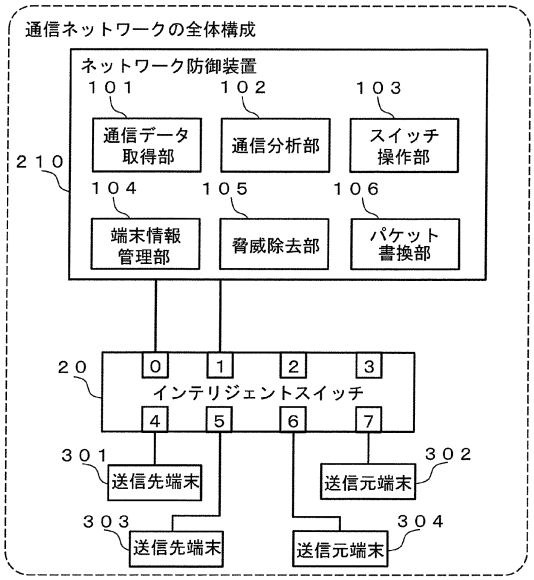
【図１７Ｃ】



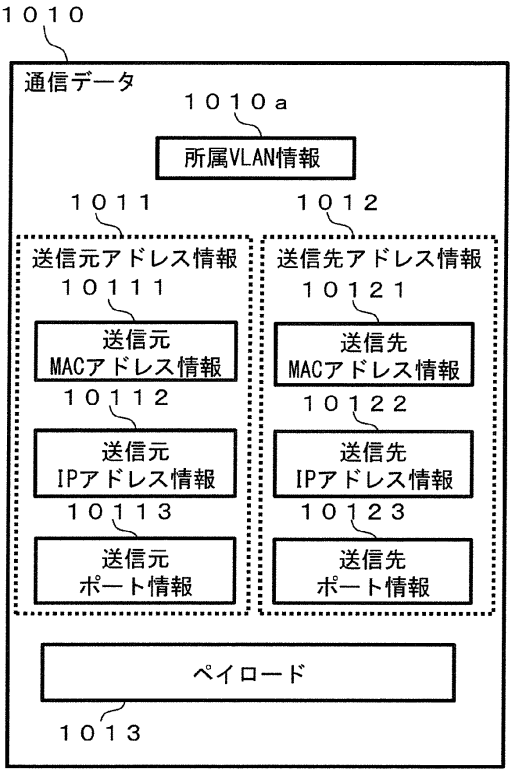
【図１８】



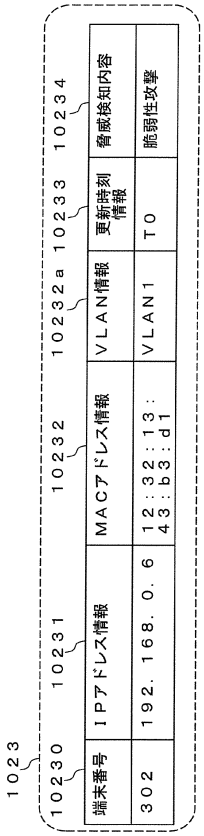
【図１９】



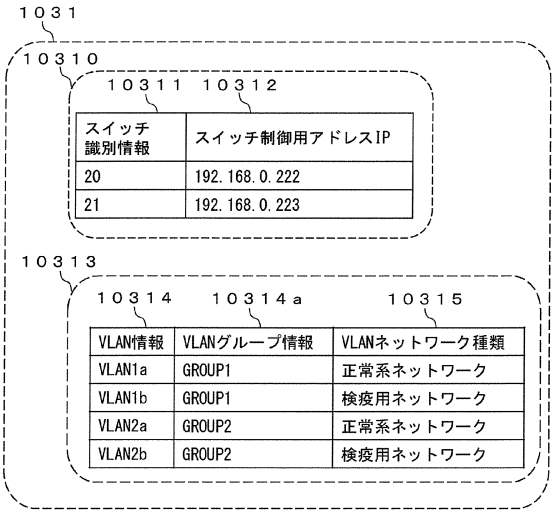
【図２０】



【図２１】



【図２２】



【図２３】

10320

	10321 スイッチ識別情報	10322 接続ポート情報	10323 VLAN情報	10324 MACアドレス情報
301	20	4	VLAN1a	12:32:13:43:a5:s6
302	20	7	VLAN1b	12:32:13:43:b3:d1
303	20	5	VLAN2a	12:32:13:23:00:01
304	20	6	VLAN2b	12:32:13:89:ec:01

【図２４Ａ】

10410

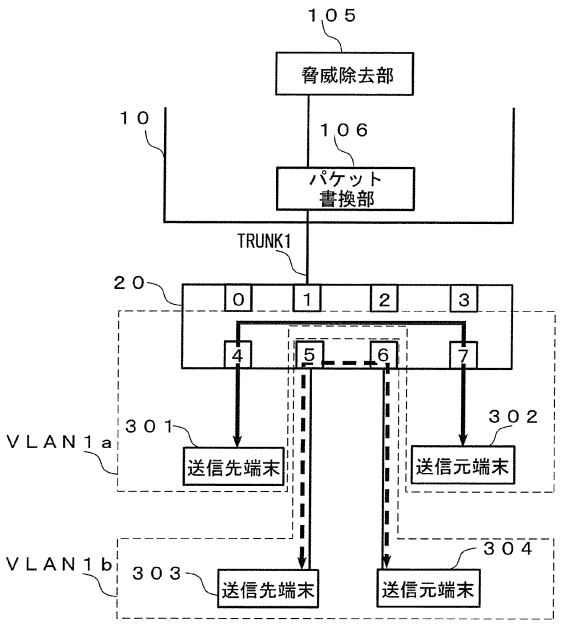
10411 管理ID情報	10412 スイッチ識別情報	10413 接続ポート情報	10414 VLAN情報	10415 MACアドレス情報	10416 IPアドレス情報	10417 更新時刻情報	10418 脅威スコア
0	20	4	VLAN1a	12:32:13:43:a5:s6	192.168.0.3	T0	0
1	20	7	VLAN1b	12:32:13:43:b3:d1	192.168.0.6	T0	80
2	20	5	VLAN2a	12:32:13:23:00:01	192.168.10.5	T0	0
3	20	6	VLAN2b	12:32:13:89:ec:01	192.168.10.8	T0	30

【図２４Ｂ】

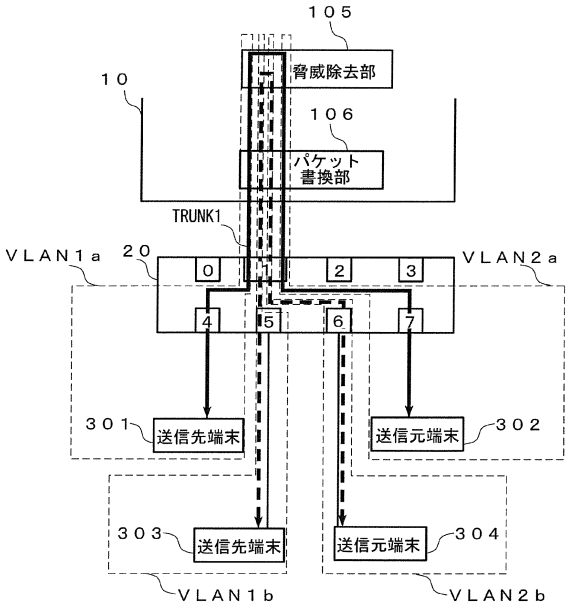
10410

10411 管理ID情報	10412 スイッチ識別情報	10413 接続ポート情報	10414 VLAN情報	10415 MACアドレス情報	10416 IPアドレス情報	10417 更新時刻情報	10418 脅威スコア
0	20	4	VLAN1a	12:32:13:43:a5:s6	192.168.0.3	T0	0
1	20	7	VLAN1b	12:32:13:43:b3:d1	192.168.0.6	T1	10080
2	20	5	VLAN2a	12:32:13:23:00:01	192.168.10.5	T0	0
3	20	6	VLAN2b	12:32:13:89:ec:01	192.168.10.8	T2	10030

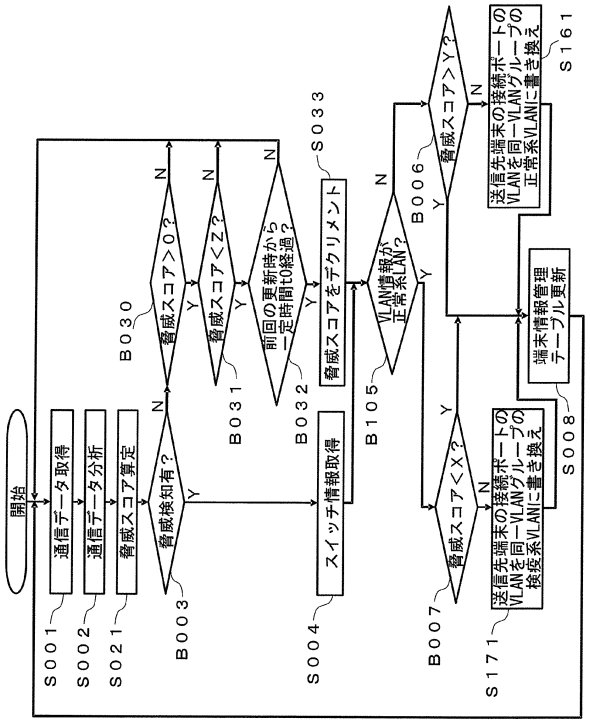
【図２５Ａ】



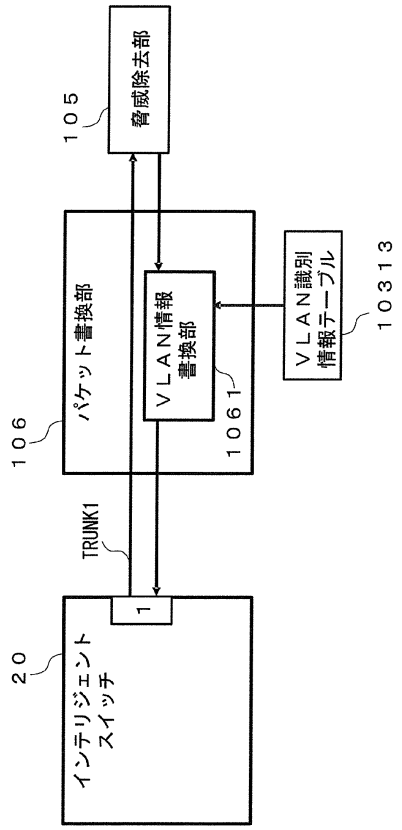
【図２５Ｂ】



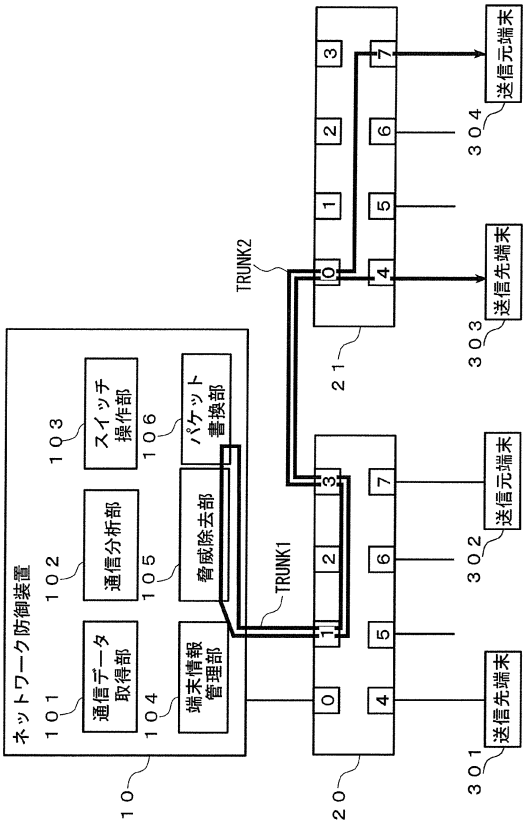
【図２６】



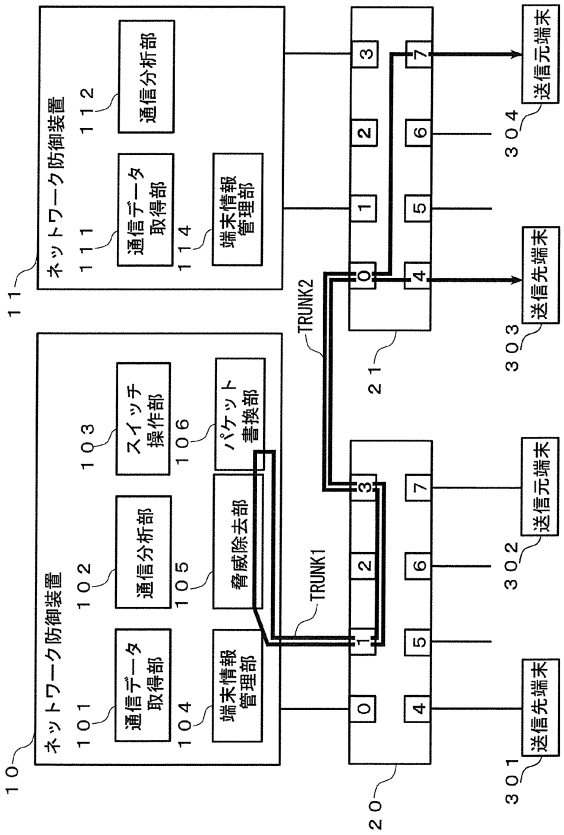
【図２７】



【図２８】



【図２９】


ネットワーク防御装置
１１
１１１
通信データ取得部
１１２
通信分析部
１１４
端末情報管理部
ネットワーク防御装置
１０
１０１
通信データ取得部
１０２
通信分析部
１０３
スイッチ操作部
１０４
端末情報管理部
１０５
脅威除去部
１０６
パケット書換部
TRUNK1
TRUNK2
２０
２１
３０１
送信先端末
３０２
送信元端末
３０３
送信先端末
３０４
送信元端末

フロントページの続き

(72)発明者　越智 直紀
大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　平本 琢士
大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　織田 智宏
大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　大庭 達海
大阪府門真市大字門真１００６番地 パナソニック株式会社内

審査官　羽岡 さやか

(56)参考文献　特開２０１７－１０８２２１（ＪＰ，Ａ）
特表２０１０－５３２６３３（ＪＰ，Ａ）
米国特許出願公開第２００６／０２５６７３０（ＵＳ，Ａ１）
米国特許第０８２５５９９６（ＵＳ，Ｂ２）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２２
Ｈ０４Ｌ　４１／４０