(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5088517号
(P5088517)
(45)発行日　平成24年12月5日(2012.12.5)　(24)登録日　平成24年9月21日(2012.9.21)

(51)Int.Cl.　F I
H04L 12/46 (2006.01)　H04L 12/46 M
H04L 12/56 (2006.01)　H04L 12/46 V
H04L 12/56 H

請求項の数 10　(全 30 頁)

(21)出願番号　特願2010-221558(P2010-221558)
(22)出願日　平成22年9月30日(2010.9.30)
(65)公開番号　特開2012-80216(P2012-80216A)
(43)公開日　平成24年4月19日(2012.4.19)
審査請求日　平成22年9月30日(2010.9.30)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　110000682
特許業務法人ワンディーＩＰパートナーズ
(72)発明者　藤田　圭祐
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　玉木　宏治

最終頁に続く

(54)【発明の名称】検疫装置、検疫システム、検疫方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置であって、
前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、端末検出部と、
前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、
を備えていることを特徴とする検疫装置。
【請求項２】
前記ネットワークが、業務に利用される業務ネットワークと、前記検疫処理に用いられる検疫ネットワークとを備え、
前記スイッチ制御部が、前記第１のＶＬＡＮを前記業務ネットワークに接続させ、前記第２のＶＬＡＮを前記検疫ネットワークに接続させる、請求項１に記載の検疫装置。
【請求項３】
前記スイッチ制御部によって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエ

ージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす端末にのみ、当該端末が送信するイーサーネットフレームへの前記タグの付加を指示する、エージェント制御部を更に備えている、請求項１または２に記載の検疫装置。
【請求項４】
前記集線装置に接続された端末のうち、前記エージェントプログラムが導入されていない端末、及びセキュリティポリシーで設定されている要件を満たしていない端末に対して、検疫処理を実行する、隔離端末制御部を更に備えている、請求項３に記載の検疫装置。
【請求項５】
前記スイッチ制御部によって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入された端末を特定し、特定した端末が送信したイーサーネットフレームに、前記タグを付加する、ルーティング制御部を更に備えている、請求項１または２に記載の検疫装置。
【請求項６】
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置と、前記ネットワークに接続された複数の端末とを備え、
前記検疫装置は、
前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、前記複数の端末のうちの１台の端末が接続されている場合に、前記集線装置への別の端末の接続を検出する、端末検出部と、
前記別の端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、を備え、
前記集線装置に接続された端末は、前記検疫装置から指示された場合に、当該端末が送信するイーサーネットフレームに、前記タグを付加する、
ていることを特徴とする検疫システム。
【請求項７】
前記ネットワークが、業務に利用される業務ネットワークと、前記検疫処理に用いられる検疫ネットワークとを備え、
前記スイッチ制御部が、前記第１のＶＬＡＮを前記業務ネットワークに接続させ、前記第２のＶＬＡＮを前記検疫ネットワークに接続させる、請求項６に記載の検疫システム。
【請求項８】
前記検疫装置が、更に、エージェント制御部を備え、
前記エージェント制御部は、前記スイッチ制御部によって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす端末にのみ、当該端末が送信するイーサーネットフレームへの前記タグの付加を指示する、
請求項６または７に記載の検疫システム。
【請求項９】
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行うための検疫方法であって、
（ａ）前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、ステップと、
（ｂ）前記（ａ）のステップで前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、ステップと、

を有することを特徴とする検疫方法。
【請求項１０】
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として、コンピュータによって、検疫処理を行うためのプログラムであって、
前記コンピュータに、
（ａ）前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、ステップと、
（ｂ）前記（ａ）のステップで前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、ステップと、
を実行させるプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークに接続された端末を検疫するための検疫装置、検疫システム、更には、検疫方法、及びこれらを実現するためのプログラムに関する。
【背景技術】
【０００２】
近年、企業等においては、ネットワークを介して感染するワーム及びウイルスなどの増加に対応するため、検疫システムの導入が進められている（例えば、特許文献１参照。）。検疫システムは、ＯＳパッチファイル、ウイルス対策ソフトの定義ファイルが最新でないなど、予めセキュリティポリシーで設定されている要件を満たしていない端末を、業務ネットワークから隔離して、ネットワークのセキュリティを保持している。
【０００３】
このような検疫システムでは、一般に、ネットワークの制御をより厳密に行うために、ＶＬＡＮ（Virtual LAN）機能を有するレイヤー２スイッチが利用されている。レイヤー２スイッチは、インターネットプロトコルの通信に利用されるレイヤーよりも低いレイヤー（データリンク層）において、ネットワークを制御している。
【０００４】
具体的には、検疫システムにおいて、ＶＬＡＮ機能を有するレイヤー２スイッチは、予め、業務用のＶＬＡＮと隔離用のＶＬＡＮとを備えている。そして、検疫システムを構成する検疫サーバは、レイヤー２スイッチに接続された端末のセキュリティポリシーに従い、その端末をどちらかのＶＬＡＮに所属させる。
【０００５】
つまり、検疫サーバは、レイヤー２スイッチのいずれかのポートに端末が接続されると、ＳＮＭＰ（Simple Network Management Protocol）を利用して、端末のポートへの接続を検知する。そして、検疫サーバは、端末におけるエージェントプログラムのインストールのチェック、セキュリティポリシーのチェックなどを実行する。
【０００６】
その後、検疫サーバは、セキュリティポリシーを満たす安全な端末のみを業務用のＶＬＡＮに所属させ、業務ネットワークへの接続を許可する。また、検疫サーバは、セキュリティポリシーを満たさない端末を隔離用のＶＬＡＮによって隔離する。また、隔離用ＶＬＡＮに所属している端末は、検疫サーバ以外を通信対象として通信を行うことができず、検疫サーバのみと通信を行う。
【０００７】
更に、検疫サーバは、エージェントプログラムが未導入の端末、及びセキュリティポリシーを満たしていない端末に対して、エージェントプログラムのインストールといった、

セキュリティポリシーを満たすための処理を施してから、これらを業務用のＶＬＡＮに接続させる。この結果、ネットワークのセキュリティが保たれる。

【０００８】

また、上述の検疫システムでは、レイヤー２スイッチのポート毎に別々のＶＬＡＮ設定を行うことができ、この場合は、ポート単位での端末の隔離及び復旧を実現することができる。更に、端末毎に隔離用ＶＬＡＮを割り当てることもでき、この場合は、端末一台毎に検疫を行うこともできる。

【先行技術文献】

【特許文献】

【０００９】

【特許文献１】特開２００８－５４２０４号公報

【発明の概要】

【発明が解決しようとする課題】

【００１０】

ところで、上述の検疫システムでは、レイヤー２スイッチの各ポートには、１台の端末又は１台の情報機器が直接接続されることが、前提とされている。一方、実際には、例えば、レイヤー２スイッチのポートに、ＶＬＡＮ機能を持たないハブが接続され、更に、このＶＬＡＮ機能を持たないハブの配下に複数の端末が接続される場合がある。

【００１１】

上記の場合、ＶＬＡＮ機能を持たないハブの配下の端末は、全て同一のＶＬＡＮに所属することになる。従って、例えば、ＶＬＡＮ機能を持たないハブの配下に、セキュリティポリシーを満たした端末が１台目として接続されると、検疫サーバは、ＶＬＡＮ機能を持たないハブが接続されているポートを業務用のＶＬＡＮに接続させてしまう。

【００１２】

そして、ＶＬＡＮ機能を持たないハブの配下に、２台目の端末が接続されると、この端末は、エージェントプログラムが未導入であっても、又はエージェントプログラムは導入済みであるが、セキュリティポリシーで設定された要件を満たしていなくても、業務用のネットワークに接続できてしまう。上述の検疫システムには、レイヤー２スイッチのポートに、ＶＬＡＮ機能を持たないハブを介して、複数台の端末が接続された場合に、当該端末を個別に業務ネットワークから隔離及び復旧することができないという問題が存在している。

【００１３】

本発明の目的の一例は、上記問題を解消し、レイヤー２スイッチのポートに、ＶＬＡＮ機能を有していない集線装置を介して、複数の端末が接続された場合に、各端末に対して個別に検疫を実行し得る、検疫装置、検疫システム、検疫方法、及びプログラムを提供することにある。

【課題を解決するための手段】

【００１４】

上記目的を達成するため、本発明の一側面における検疫装置は、ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置であって、

前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、端末検出部と、

前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、

を備えていることを特徴とする。

【００１５】

上記目的を達成するため、本発明の一側面における検疫システムは、
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置と、前記ネットワークに接続された複数の端末とを備え、
前記検疫装置は、
前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、前記複数の端末のうちの１台の端末が接続されている場合に、前記集線装置への別の端末の接続を検出する、端末検出部と、
前記別の端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、を備え、
前記集線装置に接続された端末は、前記検疫装置から指示された場合に、当該端末が送信するイーサーネットフレームに、前記タグを付加する、
ことを特徴とする。

【００１６】

また、上記目的を達成するため、本発明の一側面における検疫方法は、ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行うための検疫方法であって、
（ａ）前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、ステップと、
（ｂ）前記（ａ）のステップで前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、ステップと、
を有することを特徴とする。

【００１７】

更に、上記目的を達成するため、本発明の一側面におけるプログラムは、ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として、コンピュータによって、検疫処理を行うためのプログラムであって、
前記コンピュータに、
（ａ）前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、ステップと、
（ｂ）前記（ａ）のステップで前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、ステップと、
を実行させることを特徴とする。

【発明の効果】

【００１８】

以上の特徴により、本発明によれば、レイヤー２スイッチのポートに、ＶＬＡＮ機能を有していない集線装置を介して、複数の端末が接続された場合に、各端末に対して個別に検疫を実行することができる。

【図面の簡単な説明】

【００１９】

【図１】図１は、本発明の実施の形態１における検疫システムの全体構成を示す図である。

【図２】図２は、本発明の実施の形態１における検疫システムを構築している検疫装置の構成を示すブロック図である。

【図３】図３は、本発明の実施の形態１における検疫システムを構築している端末の構成を示すブロック図である。
【図４】図４は、図１に示す端末情報データベースに格納されている端末情報の一例を示す図である。
【図５】図５は、図１に示すポート情報データベースに格納されているポート情報の一例を示す図である。
【図６】図６は、本発明の実施の形態１における検疫システムの動作を示すシーケンス図である。
【図７】図７は、本発明の実施の形態２における検疫システムの全体構成を示す図である。
【図８】図８は、本発明の実施の形態２における検疫システムを構築している検疫装置の構成を示すブロック図である。
【図９】図９は、本発明の実施の形態２における検疫システムの動作を示すシーケンス図である。
【図１０】図１０は、本発明の実施の形態における検疫装置を実現するコンピュータの一例を示すブロック図である。
【発明を実施するための形態】
【００２０】
（発明の概要）
通常、検疫装置（検疫用のサーバ装置）が監視対象としている、レイヤー２スイッチのポートは、アクセスポートに設定されている。これに対して、本発明では、検疫装置は、ポートに接続されたハブ（ＶＬＡＮ機能無）の配下に１台の端末が接続されている場合に、このハブの配下に更に２台目の端末が接続されると、それを検知したタイミングで、当該ポートをトランク（Trunk）ポートに設定する。
【００２１】
また、このトランクポートには、新たに、ＶＬＡＮが定義される。この新たに定義されたＶＬＡＮは、検疫装置とのみ通信が可能な隔離ネットワーク（以下「隔離ＮＷ（Net Work）」とする。）に接続され、更に、「ネイティブ（native）ＶＬＡＮ」として設定される。ここで、この新たに定義されたＶＬＡＮは、従来の１つポートに毎に設定された隔離用のＶＬＡＮとは異なるため、本明細書では、「隔離用ネイティブＶＬＡＮ」とする。
【００２２】
一般に、「ネイティブＶＬＡＮ」とは、ＶＬＡＮタグの無いイーサーネット（登録商標）フレームの通信を行うＶＬＡＮをいう。レイヤー２スイッチは、ＶＬＡＮタグが付加されたイーサーネットフレームを受け取ると、これを、ネイティブＶＬＡＮに所属しているものとして転送する。なお、ネイティブＶＬＡＮのＶＬＡＮ番号（VLAN ID）は、デフォルトでは、「１」に設定されていることが多いが、自由に変更することも可能である。
【００２３】
また、トランクに設定されたポートには、隔離ＮＷに接続される「隔離用ネイティブＶＬＡＮ」に加え、業務ネットワーク（以下「業務ＮＷ（Net Work）とする。）に接続される「業務用ＶＬＡＮ」も設定される。レイヤー２スイッチは、ＶＬＡＮタグの無いイーサーネットフレームを受け取った場合は、これを、業務用ＶＬＡＮに所属しているものとして転送する。このように、トランクに設定されたポートでは、隔離ＮＷと業務ＮＷとの通信のみが許可されるように設定が行われる。
【００２４】
上述のレイヤー２スイッチの設定により、トランクに設定したポートでは、ＶＬＡＮタグが付加されたイーサーネットフレームの通信と、ＶＬＡＮタグが付加されていないイーサーネットフレームの通信とが可能となる。そして、レイヤー２スイッチは、ＶＬＡＮタグの有無に応じて、イーサーネットフレームを、業務ＮＷ又は隔離ＮＷのいずれかに転送する。
【００２５】

従って、例えば、端末に導入されたエージェント（Agent）に、ＶＬＡＮタグ（以下「業務ＮＷ用ＶＬＡＮタグ」とする。）を付加する機能を持たせるようにする。この場合、エージェントが導入済みの端末（以下「正規端末」とする。）は、エージェントが、イーサーネットフレームに、業務ＮＷ用のＶＬＡＮタグを付加するため、業務ＮＷと通信することができる。

【００２６】

一方、エージェントが導入されていない端末（以下「不正端末」）は、イーサーネットフレームに業務ＮＷ用ＶＬＡＮタグを付加することができないため、「隔離用ネイティブＶＬＡＮ」での通信となる。そして、隔離用ネイティブＶＬＡＮでの通信では、端末は、隔離ＮＷを介して検疫サーバとしか通信できない状態となる。この端末が、業務ＮＷに接続するためには、検疫サーバと通信し、エージェントプログラムをインストールする必要がある。

【００２７】

以上により、ＶＬＡＮ機能を持たないハブの配下に、例えば、エージェントが未導入の端末、エージェントは導入されているが、セキュリティポリシーを満たしていない端末が、接続された場合であっても、この端末を個別に業務ＮＷから隔離し、更に、復旧することができる。

【００２８】

（実施の形態１）

以下、本発明の実施の形態１における検疫装置、検疫システム、検疫方法、及びプログラムについて、図１～図６を参照しながら説明する。最初に、本実施の形態１における検疫装置及び検疫システムの構成について図１及び図２を用いて説明する。図１は、本発明の実施の形態１における検疫システムの全体構成を示す図である。図２は、本発明の実施の形態１における検疫システムを構築している検疫装置の構成を示すブロック図である。

【００２９】

図１に示すように、本実施の形態１における検疫システム３０は、ネットワーク４０を対象として検疫処理を行う検疫装置１と、ネットワーク４０に接続された端末３及び４とを備えている。検疫装置１、端末３及び４は、ネットワーク４０を構成している。ここで、本実施の形態１において「検疫処理」には、ネットワークに接続された端末を業務ＮＷから隔離し、その後、エージェントプログラムの導入、パッチファイルの適用といった復旧処理を行うことだけでなく、既に隔離されている端末に対して復旧処理を行うことも含まれる。

【００３０】

また、ネットワーク４０は、レイヤー２スイッチ７を備えている。本実施の形態では、ネットワーク４０は、更に、検疫指示装置５、業務ネットワーク（業務ＮＷ）８、レイヤー２スイッチ７のポート７２に接続されたハブ６も備えている。

【００３１】

レイヤー２スイッチ７は、仮想的にネットワークを分割する機能、いわゆる「ＶＬＡＮ機能」を備えている。具体的には、レイヤー２スイッチ７は、国際標準であるＩＥＥＥ８０２．１Ｑに準拠したタグＶＬＡＮ機能を備えている。更に、レイヤー２スイッチ７は、ネットワーク管理プロトコルによって検疫装置１と通信する機能も備えている。ネットワーク管理プロトコルとしては、インターネット上の業界標準であるＲＦＣで規定されているＳＮＭＰ（Simple Network Management Protocol）等が挙げられる。

【００３２】

また、レイヤー２スイッチ７は、ポート７１～７６を備えている。このうち、ポート７１には、検疫装置１が接続されている。ポート７１は、複数のタグＶＬＡＮそれぞれに所属するイーサーネットフレームを送出可能なトランク（Trunk）ポートに設定されている。一方、ポート７２～ポート７６は、アクセスポートに設定されている。なお、ハブ６が接続されているポート７２は、後述するように、一定条件下でトランクポートに設定される。

【００３３】
ハブ６は、イーサーネットで構成されたネットワークで利用される集線装置であり、ＶＬＡＮ機能を有していない。ハブ６は、ＶＬＡＮ機能及びＳＮＭＰ機能を有していないレイヤー２のスイッチと同等であり、ハブ６をこれと置き換えることも可能である。
【００３４】
業務ネットワーク８は、イントラネット等の業務ネットワークであり、業務サーバ及びインターネットへの接続に利用される。また、業務ネットワーク８は、企業の上流ネットワークへのアクセス経路を含んでいても良い。
【００３５】
端末３及び端末４は、共に、ネットワーク４０の利用者が利用するコンピュータであり、レイヤー２スイッチ７のポート７２に、ＶＬＡＮ機能を有していないハブ６を介して接続されている。本実施の形態では、このうち、端末３が最初にハブ６に接続され、その後、端末４がハブ６に接続される。
【００３６】
ところで、レイヤー２スイッチ７の配下にＶＬＡＮ機能を持たないハブ６が接続され、このハブ６の配下に一台の端末３のみが接続されている場合は、レイヤー２スイッチ７のポートに、直接端末３が接続されている状態と同じである。従って、端末３にエージェントプログラムが導入されており、且つ、セキュリティポリシーで設定された要件が満たされている場合は、レイヤー２スイッチ７は、端末３を業務ネットワーク８に接続する。そして、この状態で、エージェントプログラムが導入されていない端末、又はエージェントプログラムは導入されているが、セキュリティポリシーで設定された要件を満たしていない端末がハブ６に接続されると、従来では、この端末までもが業務ネットワークに接続される。しかし、本実施の形態では、以下に説明するように、検疫装置１によって、この接続は阻止される。
【００３７】
図２に示すように、検疫装置１は、端末検出部１１と、スイッチ制御部１２とを備えている。このうち、端末検出部１１は、レイヤー２スイッチ７のポート７２に、ＶＬＡＮ機能を有していないハブ６を介して、１台の端末３が接続されている場合に、ハブ６への別の端末４の接続を検出する。
【００３８】
スイッチ制御部１２は、端末４の接続が検出された場合に、ハブ６が接続されているポート７２をトランクポートに設定する。また、スイッチ制御部１２は、隔離用のＶＬＡＮを定義すると共に、この隔離用のＶＬＡＮをネイティブＶＬＡＮ（隔離用ネイティブＶＬＡＮ）に設定する。更に、スイッチ制御部１２は、ポート７２に、業務用ＶＬＡＮと、隔離用ネイティブＶＬＡＮとを設定する。
【００３９】
業務用ＶＬＡＮは、発明の概要で上述したように、設定されたタグが付加されたイーサーネットフレームのみを転送するタグＶＬＡＮであり、業務ＮＷに接続される。また、隔離用ネイティブＶＬＡＮは、タグが付加されていないイーサーネットフレームのみを転送するネイティブＶＬＡＮであり、隔離ＮＷ（図１及び図２において図示せず）に接続される。なお、本実施の形態１では、業務用ＶＬＡＮのＶＬＡＮ番号（VLAN ID）は「１１」に設定され、隔離用ネイティブＶＬＡＮのＶＬＡＮ番号（VLAN ID）は「１０」に設定されている。
【００４０】
また、ハブ６に接続された端末３及び端末４は、検疫装置１から指示された場合に、当該端末が送信するイーサーネットフレームに、タグを付加する。つまり、検疫装置１が許可する場合にのみ、各端末は、業務ネットワーク８に接続でき、それ以外の場合では、隔離ＮＷに接続され、検疫装置１及び検疫指示装置５のみと通信を行う。
【００４１】
従って、検疫装置１及び検疫システム３０によれば、レイヤー２スイッチ７のポートに

、ＶＬＡＮ機能を有していない集線装置を介して、複数の端末が接続された場合であっても、各端末に対して個別に検疫を実行することができる。

【００４２】

なお、本実施の形態において、ネットワーク４０は、図１及び図２の例に限定されるものではない。図１の例では、２つの端末のみが例示されているが、端末の数は限定されるものではない。また、端末は、レイヤー２スイッチ７のいずれかのポートに直接接続されていても良い。更に、ハブ６に３つ以上の端末が接続されていても良い。加えて、図１の例では、１つのレイヤー２スイッチ７のみが例示されているが、レイヤー２スイッチ７の数も限定されるものではない。

【００４３】

ここで、本実施の形態における検疫装置１及び検疫システム３０の構成について、図３～図５を用いて、更に具体的に説明する。図３は、本発明の実施の形態１における検疫システムを構築している端末の構成を示すブロック図である。図４は、図１に示す端末情報データベースに格納されている端末情報の一例を示す図である。図５は、図１に示すポート情報データベースに格納されているポート情報の一例を示す図である。

【００４４】

本実施の形態では、端末３及び端末４のうち、端末３には、検疫装置１との通信を可能にするエージェントプログラムが導入されている。エージェントプログラムは、端末３において実行されると、図１及び図３に示すように、端末３の内部に、検疫エージェント２を構築する。

【００４５】

また、図３に示すように、検疫エージェント２は、検疫サーバ通信部２１と、タグ付加機能部２２とを備えている。そして、検疫エージェント２は、この構成により、端末３のセキュリティポリシーの収集、検疫指示サーバ５への収集結果の通知、検疫サーバ１との通信、イーサーネットフレームへのタグの付加を実行する。検疫サーバ通信部２１及びタグ付加機能部２２それぞれの機能については、後述する。

【００４６】

なお、本実施の形態では、端末３は、セキュリティレベルが設定基準を満たした端末（以下「正規端末」という。）であるのに対して、端末４は、セキュリティレベルが設定基準を満たしいていない端末（以下「不正端末」という。）である。「セキュリティレベルが設定基準を満たしている」とは、端末に、エージェントプログラムが導入され、且つ、端末が、セキュリティポリシーで設定されている要件を満たしている、ことを意味する。これらの条件が一つでも充足されていない場合は、端末のセキュリティレベルは、設定基準を満たしていないことになる。

【００４７】

また、図２に示すように、検疫装置１は、端末検出部１１及びスイッチ制御部１２に加えて、エージェント制御部１３と、隔離端末制御部１４と、端末情報データベース（以下「端末情報ＤＢ（Data Base）」）１５と、ポート情報データベース（以下「ポート情報ＤＢ（Data Base）」１６とを備えている。更に、本実施の形態１では、検疫装置１は、レイヤー２スイッチ７のハブ６が接続されたポート７２を監視対象としている。また、検疫装置１は、実際には、サーバコンピュータに導入されたプログラムによって実現されている。

【００４８】

端末情報ＤＢ１５は、図４に示すように、検疫サーバ１が監視対象としているレイヤー２スイッチ７の配下に接続された端末に関する情報（以下「端末情報」）を登録している。図４の例では、レイヤー２スイッチ７のポート７２に、ＶＬＡＮ機能を持たないハブ６を介して接続された、端末３及び端末４に関する情報が、端末情報として格納されている。端末情報は、端末毎の、端末ＩＤ、ＭＡＣアドレス、ＩＰアドレス、ＶＬＡＮ番号、ポート番号によって構成されている。

【００４９】

なお、図４において、端末ＩＤが「１０１」の端末が端末３であり、端末ＩＤが「１０２」の端末が端末４である。端末ＩＤが「１０２」の端末４には、上述したようにエージェントプログラムが導入されておらず、検疫エージェント２が構築されていないため、ＭＡＣアドレス及びＩＰアドレスは登録されていない。

【００５０】

ポート情報ＤＢ１６は、図５に示すように、検疫サーバ１が監視対象としているレイヤー２スイッチ７の各ポートに関する情報（以下「ポート情報」）を登録している。ポート情報は、ポート毎の、ポート番号、接続されるネットワークの種類、ＶＬＡＮ番号（VLAN ID）、ポート状態によって構成されている。

【００５１】

図５の例では、ポート番号６のポートは、ハブ６が接続されたポート７２であり、ポート番号１０のポートは、ポート７３であり、ポート番号２０のポートは、ポート７６である。また、図５の例では、ポート番号６のポート７２が、スイッチ制御部１２によって、トランクポートに設定された場合について情報が登録されている。具体的には、ポート情報ＤＢ１６において、ポート番号６のポート７には、隔離用ネイティブＶＬＡＮのＶＬＡＮ番号（VLAN ID=10）と、業務用ＶＬＡＮのＶＬＡＮ番号（VLAN ID=11）とが登録されている。このため、ポート７２に接続された端末は、業務ＮＷ８（VLAN ID=10）との通信、及び隔離ＮＷとの通信のうちいずれか一方が可能となる。

【００５２】

更に、図５の例では、ポート番号１０のポート７３はアクセスポートに設定されている。ポート７３に接続された端末は、ＶＬＡＮ番号（VLAN ID）が「２２」のＶＬＡＮにより、隔離ＮＷと通信する。また、ポート番号２０のポート７６も同様にアクセスポートに設定されているが、ポート７４に接続された端末は、ＶＬＡＮ番号（VLAN ID）が「１０」のＶＬＡＮにより、業務ＮＷ８と通信する。

【００５３】

なお、図５の例に限定されるものではなく、ポート番号１０のポート７３及びポート番号２０のポート７６の一方又は両方が、ポート番号６のポート７２と同様にトランクポートに設定されていても良い。また、この場合も、トランクポートに設定されたポートにおいては、隔離用ネイティブＶＬＡＮのＶＬＡＮ番号と、業務用ＶＬＡＮのＶＬＡＮ番号とが登録される。

【００５４】

端末検出部１１は、上述したように、レイヤー２スイッチ７のポート７２に、ＶＬＡＮ機能を有していないハブ６を介して、端末３が接続されている場合に、ハブ６に端末４が接続されると、これを検出する。このとき、本実施の形態１では、端末検出部１１は、ポート情報ＤＢ１６にアクセスし、ハブ６が接続されているポート７２のポート情報を取得し、これをスイッチ制御部１２に通知する。

【００５５】

具体的には、端末検出部１１は、例えば、次の処理を実行することによって、端末４の接続を検知することができる。先ず、端末検出部１１は、ハブ６に端末が接続されたときに、端末がブロードキャストで発信するＡＲＰパケットを検出し、その発信元のＭＡＣアドレスを特定する。更に、端末検出部１１は、レイヤー２スイッチ７のポートのうち、送信元のＭＡＣアドレスを含む複数のＭＡＣアドレスが登録されているポートの検出を行う。そして、複数のＭＡＣアドレスが登録されているポートが検出された場合は、端末検出部１１は、このポートに、２台以上の端末が接続されたと判断する。

【００５６】

スイッチ制御部１２は、本実施の形態１では、端末検出部１１からのポート情報の通知を受信すると、通知されたポートをトランクポートに設定し、更に、通知されたポートに、業務用ＶＬＡＮ及び隔離用ネイティブＶＬＡＮの設定を行う。また、スイッチ制御部１２は、ポート情報ＤＢ１６にアクセスし、ポート情報を更新する。更に、スイッチ制御部１２は、エージェント制御部１３に対し、トランクに設定されたポートの配下に接続され

た端末（本実施の形態１では、端末３及び４）の端末情報を送信する。

【００５７】

エージェント制御部１３は、スイッチ制御部１２によって、業務用ＶＬＡＮ及び隔離用ネイティブＶＬＡＮが設定されると、スイッチ制御部１２から送信された端末情報に基づき、ハブ６に接続された端末のうち、エージェントプログラムが導入された端末を特定する。本実施の形態１では、エージェント制御部１３は、エージェントプログラムが導入された端末として、端末３を特定する。

【００５８】

また、エージェント制御部１３は、エージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす、端末にのみ、それが送信するイーサーネットフレームへのタグの付加を指示する。

【００５９】

具体的には、本実施の形態１では、エージェント制御部１３は、端末３の検疫エージェント２に対して、後述の検疫指示装置５（図１参照）へセキュリティポリシーの診断要求を行うよう指示する。そして、検疫指示装置５による診断の結果、セキュリティポリシーが満たされている場合は、エージェント制御部１３は、検疫エージェント２に、イーサーネットフレームを業務ＶＬＡＮに所属させるためのタグ（ＶＬＡＮタグ）に関する情報を送信すると共に、タグを付加するように指示を行う。

【００６０】

また、検疫指示装置５による診断の結果、セキュリティポリシーで設定された要件が満たされていない場合は、エージェント制御部１３は、検疫指示装置５から、診断対象となった端末３に対する隔離の指示を受信する。そして、エージェント制御部１３は、端末３の検疫サーバ通信部２１（図３参照）に対して、タグ付加の停止の指示を送信する。なお、その後、端末３において、セキュリティポリシーで設定された要件が満たされた場合は、エージェント制御部１３は、先に述べたように、タグ（ＶＬＡＮタグ）に関する情報を送信すると共に、タグを付加するように指示を行う。更に、エージェント制御部１３は、上述した処理の終了後、端末情報ＤＢ１５にアクセスし、登録されている端末情報を更新する。

【００６１】

隔離端末制御部１４は、ハブ６に接続された端末のうち、エージェントプログラムが導入されていない端末、及びセキュリティ状態が設定基準を満たしていない端末に対して、検疫処理を実行する。具体的には、隔離端末制御部１４は、隔離用ネイティブＶＬＡＮに所属している端末４からの要求に応じて、検疫エージェント２を構築するためのエージェントプログラムを配布する。

【００６２】

また、隔離端末制御部１４は、隔離用ネイティブＶＬＡＮに所属している端末４が、セキュリティポリシーで設定されている要件を満たすための処理、例えば、パッチファイルの配布等も行う。更に、隔離端末制御部１４は、隔離用ネイティブＶＬＡＮに所属している端末４の通信を監視し、端末４からのサービス要求に対する応答を行うこともできる。

【００６３】

検疫指示装置５（図１参照）は、検疫エージェント２からの要求に応じて、検疫エージェント２が収集した端末のセキュリティポリシーをチェックし、端末がセキュリティポリシーで設定されている要件を満たしているかどうかを判定する。実際には、検疫指示装置５は、検疫装置１と同様に、サーバコンピュータに導入されたプログラムによって実現されている。

【００６４】

そして、判定の結果、端末がセキュリティポリシーで設定されている要件を満たしてない場合は、検疫指示装置５は、検疫装置１に端末の隔離を指示する。一方、判定の結果、端末がセキュリティポリシーで設定されている要件を満たしている場合は、検疫指示装置５は、検疫装置１にその旨を通知する。検疫指示装置５による指示又は通知が行われると

、上述したように、検疫装置１のエージェント制御部１３による処理が行われる。

【００６５】

図３を用いて上述したように、本実施の形態１では、検疫サーバ通信部２１と、タグ付加機能部２２とを備えている。検疫サーバ通信部２１は、検疫装置１からＶＬＡＮタグに関する情報を受信し、そして、受信した情報に基づいて、タグ付加機能部２２に、ＶＬＡＮタグを付加するように指示を行う。

【００６６】

タグ付加機能部２２は、まず、検疫サーバ通信部２１が受信した情報と、それからの指示とを受け取る。そして、タグ付加機能部２２は、受け取った指示に基づいて、端末のネットワーク・インターフェースカードから送出されるイーサーネットフレームに、これを業務用ＶＬＡＮで転送するためのＶＬＡＮタグを付加する。

【００６７】

本実施の形態１では、端末（正規端末）３から送出されたイーサーネットフレームには、ＶＬＡＮタグが付加されている。この場合、レイヤー２スイッチ７は、ＶＬＡＮタグから、このイーサーネットフレームが所属するＶＬＡＮのＶＬＡＮ番号は「１１」であると判定する。この結果、正規端末３は、業務ＮＷ８での通信が可能となる。

【００６８】

一方、エージェントプログラムが導入されていない端末（不正端末）４は、イーサーネットフレームに、ＶＬＡＮタグを付加する機能を備えていないため、不正端末４からは、ＶＬＡＮタグが付加されていないイーサーネットフレームが送信される。そして、レイヤー２スイッチ７は、このイーサーネットフレームを受信すると、これは隔離用ネイティブＶＬＡＮに所属していると判断し、このイーサーネットフレームを、隔離用ネイティブＶＬＡＮ（VLAN ID=11）に転送する。

【００６９】

隔離用ネイティブＶＬＡＮは、隔離ＮＷに接続されているため、この結果、不正端末４は、検疫サーバ１のみとしか通信ができない状態となる。但し、この状態であっても、不正端末４が、隔離用ＶＬＡＮで検疫装置１からエージェントプログラムを取得し、且つ、検疫装置１の検疫処理により、セキュリティポリシーで設定されている要件を満たせば、端末４による業務ＮＷ８での通信が可能となる。

【００７０】

次に、本発明の実施の形態１における検疫装置１及び検疫システム３０の動作について図６を用いて説明する。図６は、本発明の実施の形態１における検疫システムの動作を示すシーケンス図である。以下の説明においては、適宜図１～図５を参酌する。また、本実施の形態１では、検疫装置１を動作させることによって、検疫方法が実施される。よって、本実施の形態１における検疫方法の説明は、以下の検疫装置１の動作説明に代える。

【００７１】

図６に示すように、先ず、検疫装置１において、端末検出部１１は、レイヤー２スイッチ７のポートを監視する。そして、端末検出部１１は、レイヤー２スイッチ７の特定のポートに、ＶＬＡＮ機能を持たないハブ６が接続され、更に、ハブ６の配下に１台の端末３が接続されている状態で、ハブ６に新たな端末４が接続されると、そのことを検出する（ステップＡ１）。

【００７２】

次に、端末検出部１１は、レイヤー２スイッチ７から、そのポートにハブ６を介して接続された端末の端末情報（ＭＡＣアドレス、ＩＰアドレス、ポート番号等（図４参照））を取得する（ステップＡ２）。そして、端末検出部１１は、スイッチ制御部１２に、取得した端末情報を送信して、ハブ６に複数の端末が接続されていることを通知する（ステップＡ３）。

【００７３】

次に、スイッチ制御部１２は、端末検出部１１から受け取った端末情報に基づき、複数の端末が接続されているポートを特定する。そして、スイッチ制御部１２は、ポート情報

ＤＢ１６に対して、特定したポートに設定された業務用ＶＬＡＮのＶＬＡＮ番号を要求し（ステップＡ４）、その後、業務用ＶＬＡＮのＶＬＡＮ番号を取得する（ステップＡ５）。

【００７４】

次に、スイッチ制御部１２は、レイヤー２スイッチ７のＶＬＡＮ機能を持たないハブ６が接続されているポート７２に対して設定を行う（ステップＡ６）。具体的には、スイッチ制御部１２は、まず、検疫装置１とのみ通信が可能な隔離用ＶＬＡＮを新たに定義し、更に、その定義した隔離用ＶＬＡＮをネイティブＶＬＡＮ（隔離用ネイティブＶＬＡＮ）として設定する。続いて、スイッチ制御部１２は、ポート７２をトランクポートに設定する。最後に、スイッチ制御部１２は、トランクポートに設定したポート７２に、隔離ＮＷと接続するための隔離用ネイティブＶＬＡＮと、業務ＮＷ８と接続するための業務ＶＬＡＮとを設定し、ポート７２において二つのＮＷとの通信を許可する。

【００７５】

次に、スイッチ制御部１２は、ポート情報ＤＢ１６にアクセスし、ハブ６が接続されたポートのポート情報を更新する（ステップＡ７）。次に、スイッチ制御部１２は、ＶＬＡＮ機能を持たないハブ６の複数の端末が接続されたポート７２の情報、即ち、ポート番号、及び業務ＶＬＡＮのＶＬＡＮ番号を、エージェント制御部１３に出力し、ハブ６に複数の端末が接続されたことを通知する（ステップＡ８）。

【００７６】

次に、エージェント制御部１３は、エージェントプログラムが導入された正規端末３を特定し、正規端末３の検疫エージェント２に対し、検疫指示装置５にセキュリティポリシーの診断を要求するよう指示を行う（ステップＡ９）。次に、検疫エージェント２は、それが構築されている正規端末３のセキュリティポリシーを収集する。そして、検疫エージェント２は、収集したセキュリティポリシーに基づいて、検疫指示装置５に診断要求を行う（ステップＡ１０）。

【００７７】

次に、検疫指示装置５は、検疫エージェント２からの診断要求に基づいて、検疫エージェント２が導入されている正規端末３のセキュリティポリシーをチェックし、セキュリティポリシーで設定されている要件が満たされているかどうかを判定する。そして、判定の結果、合格である場合は、検疫指示装置５は、検疫エージェント２の検疫サーバ通信部２１に合格通知を送信する（ステップＡ１１）。

【００７８】

次に、検疫指示装置５は、検疫サーバ通信部２１に合格通知を出した後、エージェント制御部１３に対して、正規端末３が業務ＮＷ８に接続されるように指示を行う（ステップＡ１２）。そして、エージェント制御部１３は、検疫指示装置５から得た正規端末３の情報（ＭＡＣアドレス及びＩＰアドレス）と、スイッチ制御部１２から得た業務用ＶＬＡＮのＶＬＡＮ番号とに基づき、検疫エージェント２の検疫サーバ通信部２１に、業務ＮＷで用いるＶＬＡＮタグの情報とＶＬＡＮタグの付加の指示とを送信する（ステップＡ１３）。

【００７９】

次に、検疫エージェント２において、検疫サーバ通信部２１はエージェント制御部１３から受信した業務ＮＷで用いるＶＬＡＮタグの情報を、タグ付加機能部２２に出力する。更に、検疫サーバ通信部２１は、タグ付加機能部２２に、イーサーネットフレームが送出される時にＶＬＡＮタグを付加するように指示を行う（ステップＡ１４）。

【００８０】

ステップＡ１４の実行後、エージェント制御部１３は、タグ付加機能部２２から、ＶＬＡＮタグの付加の設定が完了したことを示す通知を受信する（ステップＡ１５）。次に、エージェント制御部１３は、端末情報ＤＢ１５にアクセスし、ステップＡ８でスイッチ制御部１２から受け取った情報に基づいて、ハブ６に接続されている端末の端末情報を更新する（ステップＡ１６）。

【００８１】
また、検疫エージェント２が導入されていない不正端末４に関しては、取得できる情報は限られている。よって、ステップＡ１６の実行時において、エージェント制御部１３は、図４に示されたように、不正端末４については、端末ＩＤ、ＶＬＡＮ番号、及びポート番号のみを登録する。端末情報ＤＢ１５を用いれば、検疫システム３０の管理者は、各端末の状態を把握することができる。
【００８２】
その後、検疫エージェント２のタグ付加機能部２２は、正規端末３を業務ＮＷ８において通信させるため、レイヤー２スイッチ７に対して、業務ＮＷ８用のＶＬＡＮタグを付加したイーサーネットフレームを送信する（ステップＡ１７）。ステップＡ１７が実行されると、レイヤー２スイッチ７は、正規端末３から送信されたイーサーネットフレームのＶＬＡＮタグを業務ＮＷ８のＶＬＡＮタグと判断し、そのイーサーネットフレームを業務ＮＷ８に転送させる。
【００８３】
一方、不正端末４には検疫エージェント２が導入されていないため、不正端末４からレイヤー２スイッチ７へと送信されたイーサーネットフレームには、ＶＬＡＮタグは付加されていない（ステップＡ１８）。従って、レイヤー２スイッチ７は、検疫エージェント２が未導入の不正端末４からのイーサーネットフレームは、隔離用ネイティブＶＬＡＮに所属すると判定し、このイーサーネットフレームを隔離ＮＷに転送させる（ステップＡ１９）。
【００８４】
また、検疫エージェント３が未導入の不正端末４は、業務ＮＷ８に接続するため、隔離用ネイティブＶＬＡＮを利用して検疫装置１と通信し、その隔離端末制御部１４からエージェントプログラムを取得する（ステップＡ２０）。その後、不正端末４の内部に、検疫エージェント２が構築される。その後、端末４についてステップＡ９～Ａ１６が実行されると、端末４は、業務ＮＷ８において通信を行うことが可能となる。
【００８５】
以上のように、本実施の形態１によれば、レイヤー２スイッチ７に、ＶＬＡＮ機能を持たないハブ６が接続された場合であっても、ハブ６の配下の危険性のある端末を業務ＮＷ８から隔離することができ、正常なＮＷ状態を維持することが可能となる。また、本実施の形態１では、ＶＬＡＮ機能を持たないハブ６の配下の端末は、検疫装置１によって管理されているため、検疫システム３０の管理者は、ＶＬＡＮ機能を持たないハブ６の配下の端末の状態を把握することができる。
【００８６】
更に、背景技術の欄で述べた検疫システムでは、集線装置としては、末端においてもＶＬＡＮ対応のレイヤー２スイッチを用いなければならなかったが、本実施の形態１によれば、レイヤー２スイッチとＶＬＡＮ機能を持たないハブとを併用できる。本実施の形態１では、ＶＬＡＮ機能持たないハブを末端に用いることができる。このため、検疫システムの導入にかかるコストを抑えることができ、企業等においては、機器が無駄になることを避けることができ、資産の有効活用を図ることができる。
【００８７】
また、本実施の形態１におけるプログラムは、サーバコンピュータ等のコンピュータに、図６に示すステップＡ１～Ａ９、Ａ１３、Ａ１６を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施の形態１における検疫装置１と検疫方法とを実現することができる。この場合、コンピュータのＣＰＵ（Central Processing Unit）は、端末検出部１１、スイッチ制御部１２、エージェント制御部１３、隔離端末制御部１４として機能し、処理を行なう。また、コンピュータに備えられたハードディスク等の記憶装置が、端末情報ＤＢ１５及びポート情報ＤＢ１６として機能する。
【００８８】

（実施の形態２）
次に、本発明の実施の形態２における検疫装置、検疫システム、検疫方法、及びプログラムについて、図７～図９を参照しながら説明する。最初に、本実施の形態２における検疫装置及び検疫システムの構成について図７及び図８を用いて説明する。図７は、本発明の実施の形態２における検疫システムの全体構成を示す図である。図８は、本発明の実施の形態２における検疫システムを構築している検疫装置の構成を示すブロック図である。
【００８９】
本実施の形態２においては、実施の形態１と異なり、正規端末に導入されている検疫エージェントがＶＬＡＮタグを付加する機能を備えていなくても、正規端末からのイーサーネットフレームは業務ＮＷへと転送される。
【００９０】
図７に示すように、本実施の形態２における検疫装置５０は、ルーティング制御部１７を備えている。ルーティング制御部１７は、検疫エージェント２が導入された正規端末３から、ＶＬＡＮタグが付加されていないイーサーネットフレームが送信されると、これを隔離用ネイティブＶＬＡＮから業務用ＶＬＡＮにルーティングする。この結果、実施の形態２においても、実施の形態１と同様の機能が実現される。
【００９１】
図８に示すように、本実施の形態２においては、ルーティング制御部１７は、エージェント制御部１３と隔離端末制御部１４とによって構成されている。エージェント制御部１３は、本実施の形態２では、レイヤー２スイッチ７のポート７２において、業務用ＶＬＡＮと隔離用ネイティブＶＬＡＮとが設定されると、ハブ６に接続された端末のうち、エージェントプログラムが導入された正規端末を特定する。
【００９２】
具体的には、エージェント制御部１３は、検疫指示装置５からの情報に基づいて、エージェントプログラムが導入された正規端末を特定する。そして、正規端末が特定されると、隔離端末制御部１４は、特定された端末が送信したイーサーネットフレームに、実施の形態１で説明したＶＬＡＮタグと同様のタグを付加し、このイーサーネットフレームをルーティングする。
【００９３】
また、本実施の形態２においては、実施の形態１と異なり、正規端末３に導入されている検疫エージェント２は、タグ付加機能部（図３参照）を備えておらず、ＶＬＡＮタグを付加する機能を有していない。それ以外の点では、本実施の形態２における検疫エージェント２は、実施の形態１における検疫エージェントと同様である。
【００９４】
次に、本発明の実施の形態２における検疫装置５０及び検疫システム６０の動作について図９を用いて説明する。図９は、本発明の実施の形態２における検疫システムの動作を示すシーケンス図である。以下の説明においては、適宜図７及び図８を参酌する。また、本実施の形態２では、検疫装置５０を動作させることによって、検疫方法が実施される。よって、本実施の形態２における検疫方法の説明は、以下の検疫装置５０の動作説明に代える。
【００９５】
最初に、本実施の形態２における検疫システム６０において、ステップＢ１～Ｂ１２が実行される。但し、ステップＢ１～Ｂ１２は、それぞれ、実施の形態１において図６に示したステップＡ１～Ａ１２の対応するステップと同一のステップである。従って、ステップＢ１２の実行後、エージェント制御部１３は、検疫指示装置５から、正規端末の情報（ＭＡＣアドレス及びＩＰアドレス）を取得し、スイッチ制御部１２からは、業務用ＶＬＡＮのＶＬＡＮ番号を取得している。
【００９６】
次に、検疫システム６０において、ステップＢ１２～Ｂ１８が実行される。ステップＢ１２～Ｂ１８は、実施の形態１において図６に示したステップとは異なるステップである

。図９に示す破線による囲みは、ステップＢ１２～Ｂ１８を示している。以下に、ステップＢ１２以降について説明する。

【００９７】

ステップＢ１２の終了後、エージェント制御部１３は、検疫指示装置５から取得した情報に基づき、ＶＬＡＮ機能を持たないハブ６の配下に接続され、且つ、検疫エージェント２が導入された、正規端末として、端末３を特定する。そして、エージェント制御部１３は、隔離端末制御部１４に対し、特定した正規端末３からのイーサーネットフレームを、隔離用ネイティブＶＬＡＮから業務用ＶＬＡＮにルーティングするように指示を行う（ステップＢ１３）。

【００９８】

次に、隔離端末制御部１４は、ルーティングを実行するための設定を行い、設定が完了した場合は、エージェント制御部１３に対して、完了の通知を送信する（ステップＢ１４）。次に、エージェント制御部１３は、完了の通知を受信すると、端末情報ＤＢ１５（図４参照）にアクセスし、ハブ６の配下に接続された端末の端末情報を更新する（ステップＢ１５）。

【００９９】

その後、正規端末３からイーサーネットフレームが送信されると、レイヤー２スイッチ７はこれを受信する（ステップＢ１６）。このとき、受信されたイーサーネットフレームには、実施の形態１と異なり、ＶＬＡＮタグは付加されていない。従って、レイヤー２スイッチ７は、受信されたイーサーネットフレームを、不正端末からのＶＬＡＮタグが付加されていないイーサーネットフレームと同様に扱い、これを隔離用ネイティブＶＬＡＮ介して隔離端末制御部１４に送信する（ステップＢ１７）。

【０１００】

隔離端末制御部１４は、隔離用ネイティブＶＬＡＮに所属している端末の通信を監視している。そして、ステップＢ１７が実行されると、隔離端末制御部１４は、受信したイーサーネットフレームに、業務ＮＷ用のＶＬＡＮタグを付加し、このイーサーネットフレームを業務ＮＷ８へとルーティングする（ステップＢ１８）。ステップＢ１８の実行により、結果、検疫エージェント２が導入済みの正規端末３は、業務ＮＷ８と通信することが可能となる。

【０１０１】

なお、図９に示すステップＢ１９～Ｂ２１は、それぞれ、実施の形態１において図６に示したステップＡ１８～Ａ２０の対応するステップと同一のステップである。ステップＢ１９～Ｂ２１が実行されると、不正端末からのイーサーネットフレームは、隔離用ネイティブＶＬＡＮにより、隔離ＮＷに転送される。また、検疫装置５０は、不正端末にエージェントプログラムを導入させる。

【０１０２】

以上のように、本実施の形態２によれば、検索エージェント２がＶＬＡＮタグを付加する機能を備えていなくても、実施の形態１において述べた効果と同様の効果を得ることができる。本実施の形態２は、ＶＬＡＮタグを付加できる端末とＶＬＡＮタグを付加できない端末とが混在しているネットワーク、及びＶＬＡＮタグを付加できない端末のみが存在しているネットワークにも適用でき、検疫システムの導入をいっそう促進することができる。

【０１０３】

また、本実施の形態１におけるプログラムは、サーバコンピュータ等のコンピュータに、図９に示すステップＢ１～Ｂ９、Ｂ１３～Ｂ１５、Ｂ１８を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施の形態２における検疫装置５０と検疫方法とを実現することができる。この場合、コンピュータのＣＰＵ（Central Processing Unit）は、端末検出部１１、スイッチ制御部１２、エージェント制御部１３、隔離端末制御部１４として機能し、処理を行なう。また、コンピュータに備えられたハードディスク等の記憶装置が、端末情報ＤＢ１５及びポー

ト情報ＤＢ１６として機能する。

【０１０４】

ここで、実施の形態１及び２におけるプログラムを実行することによって、検疫装置を実現するコンピュータについて図１０を用いて説明する。図１０は、本発明の実施の形態における検疫装置を実現するコンピュータの一例を示すブロック図である。

【０１０５】

図１０に示すように、コンピュータ１１０は、ＣＰＵ１１１と、メインメモリ１１２と、記憶装置１１３と、入力インターフェイス１１４と、表示コントローラ１１５と、データリーダ／ライタ１１６と、通信インターフェイス１１７とを備える。これらの各部は、バス１２１を介して、互いにデータ通信可能に接続される。

【０１０６】

ＣＰＵ１１１は、記憶装置１１３に格納された、本実施の形態におけるプログラム（コード）をメインメモリ１１２に展開し、これらを所定順序で実行することにより、各種の演算を実施する。メインメモリ１１２は、典型的には、ＤＲＡＭ（Dynamic Random Access Memory）等の揮発性の記憶装置である。また、本実施の形態におけるプログラムは、コンピュータ読み取り可能な記録媒体１２０に格納された状態で提供される。なお、本実施の形態におけるプログラムは、通信インターフェイス１１７を介して接続されたインターネット上で流通するものであっても良い。

【０１０７】

また、記憶装置１１３の具体例としては、ハードディスクの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス１１４は、ＣＰＵ１１１と、キーボード及びマウスといった入力機器１１８との間のデータ伝送を仲介する。表示コントローラ１１５は、ディスプレイ装置１１９と接続され、ディスプレイ装置１１９での表示を制御する。データリーダ／ライタ１１６は、ＣＰＵ１１１と記録媒体１２０との間のデータ伝送を仲介し、記録媒体１２０からのプログラムの読み出し、及びコンピュータ１１０における処理結果の記録媒体１２０への書き込みを実行する。通信インターフェイス１１７は、ＣＰＵ１１１と、他のコンピュータとの間のデータ伝送を仲介する。

【０１０８】

また、記録媒体１２０の具体例としては、ＣＦ（Compact Flash）及びＳＤ（Secure Digital）等の汎用的な半導体記憶デバイス、フレキシブルディスク（Flexible Disk）等の磁気記憶媒体、又はＣＤ－ＲＯＭ（Compact Disk Read Only Memory）などの光学記憶媒体が挙げられる。

【０１０９】

上述した実施の形態の一部又は全部は、以下に記載する（付記１）～（付記１９）によって表現することができるが、以下の記載に限定されるものではない。

【０１１０】

（付記１）

ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置であって、

前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、端末検出部と、

前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、

を備えていることを特徴とする検疫装置。

【０１１１】

（付記２）

前記ネットワークが、業務に利用される業務ネットワークと、前記検疫処理に用いられ

る検疫ネットワークとを備え、
前記スイッチ制御部が、前記第１のＶＬＡＮを前記業務ネットワークに接続させ、前記第２のＶＬＡＮを前記検疫ネットワークに接続させる、付記１に記載の検疫装置。
【０１１２】
（付記３）
前記スイッチ制御部によって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす端末にのみ、当該端末が送信するイーサーネットフレームへの前記タグの付加を指示する、エージェント制御部を更に備えている、付記１または２に記載の検疫装置。
【０１１３】
（付記４）
前記集線装置に接続された端末のうち、前記エージェントプログラムが導入されていない端末、及びセキュリティポリシーで設定されている要件を満たしていない端末に対して、検疫処理を実行する、隔離端末制御部を更に備えている、付記３に記載の検疫装置。
【０１１４】
（付記５）
前記スイッチ制御部によって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入された端末を特定し、特定した端末が送信したイーサーネットフレームに、前記タグを付加する、ルーティング制御部を更に備えている、付記１または２に記載の検疫装置。
【０１１５】
（付記６）
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置と、前記ネットワークに接続された複数の端末とを備え、
前記検疫装置は、
前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、前記複数の端末のうちの１台の端末が接続されている場合に、前記集線装置への別の端末の接続を検出する、端末検出部と、
前記別の端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、を備え、
前記集線装置に接続された端末は、前記検疫装置から指示された場合に、当該端末が送信するイーサーネットフレームに、前記タグを付加する、
ていることを特徴とする検疫システム。
【０１１６】
（付記７）
前記ネットワークが、業務に利用される業務ネットワークと、前記検疫処理に用いられる検疫ネットワークとを備え、
前記スイッチ制御部が、前記第１のＶＬＡＮを前記業務ネットワークに接続させ、前記第２のＶＬＡＮを前記検疫ネットワークに接続させる、付記６に記載の検疫システム。
【０１１７】
（付記８）
前記検疫装置が、更に、エージェント制御部を備え、
前記エージェント制御部は、前記スイッチ制御部によって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす端末にのみ、当該端末が送信するイーサーネットフレ

ームへの前記タグの付加を指示する、
付記６または７に記載の検疫システム。
【０１１８】
（付記９）
前記検疫装置が、更に、隔離端末制御部を備え、
隔離端末制御部は、前記集線装置に接続された端末のうち、前記エージェントプログラムが導入されていない端末、及びセキュリティポリシーで設定されている要件を満たしていない端末に対して、検疫処理を実行する、隔離端末制御部を更に備えている、付記８に記載の検疫システム。
【０１１９】
（付記１０）
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行うための検疫方法であって、
（ａ）前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、ステップと、
（ｂ）前記（ａ）のステップで前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、ステップと、
を有することを特徴とする検疫方法。
【０１２０】
（付記１１）
前記ネットワークが、業務に利用される業務ネットワークと、前記検疫処理に用いられる検疫ネットワークとを備え、
前記（ｂ）のステップにおいて、前記第１のＶＬＡＮを前記業務ネットワークに接続させ、前記第２のＶＬＡＮを前記検疫ネットワークに接続させる、付記１０に記載の検疫方法。
【０１２１】
（付記１２）
（ｃ）前記（ｂ）のステップによって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす端末にのみ、当該端末が送信するイーサーネットフレームへの前記タグの付加を指示する、ステップを更に有する、付記１０または１１に記載の検疫方法。
【０１２２】
（付記１３）
（ｄ）前記集線装置に接続された端末のうち、前記エージェントプログラムが導入されていない端末、及びセキュリティポリシーで設定されている要件を満たしていない端末に対して、検疫処理を実行する、ステップを更に有する、付記１２に記載の検疫方法。
【０１２３】
（付記１４）
（ｅ）前記（ｂ）のステップによって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入された端末を特定し、特定した端末が送信したイーサーネットフレームに、前記タグを付加する、ステップを更に有する、付記１０または１１に記載の検疫方法。
【０１２４】
（付記１５）
ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として、コンピ

ュータによって、検疫処理を行うためのプログラムであって、
前記コンピュータに、
（ａ）前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、ステップと、
（ｂ）前記（ａ）のステップで前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネットフレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネットフレームのみを転送する第２のＶＬＡＮを設定する、ステップと、
を実行させるプログラム。

【０１２５】
（付記１６）
前記ネットワークが、業務に利用される業務ネットワークと、前記検疫処理に用いられる検疫ネットワークとを備え、
前記（ｂ）のステップにおいて、前記第１のＶＬＡＮを前記業務ネットワークに接続させ、前記第２のＶＬＡＮを前記検疫ネットワークに接続させる、付記１５に記載のプログラム。

【０１２６】
（付記１７）
（ｃ）前記（ｂ）のステップによって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入され、且つ、セキュリティポリシーで設定されている要件を満たす端末にのみ、当該端末が送信するイーサーネットフレームへの前記タグの付加を指示する、ステップを更に前記コンピュータに実行させる、付記１５または１６に記載のプログラム。

【０１２７】
（付記１８）
（ｄ）前記集線装置に接続された端末のうち、前記エージェントプログラムが導入されていない端末、及びセキュリティポリシーで設定されている要件を満たしていない端末に対して、検疫処理を実行する、ステップを更に前記コンピュータに実行させる、付記１７に記載のプログラム。

【０１２８】
（付記１９）
（ｅ）前記（ｂ）のステップによって、前記第１のＶＬＡＮと前記第２のＶＬＡＮとが設定された場合に、前記集線装置に接続された端末のうち、当該検疫装置との通信を可能にするエージェントプログラムが導入された端末を特定し、特定した端末が送信したイーサーネットフレームに、前記タグを付加する、ステップを更に前記コンピュータに実行させる、付記１５または１６に記載のプログラム。

【産業上の利用可能性】

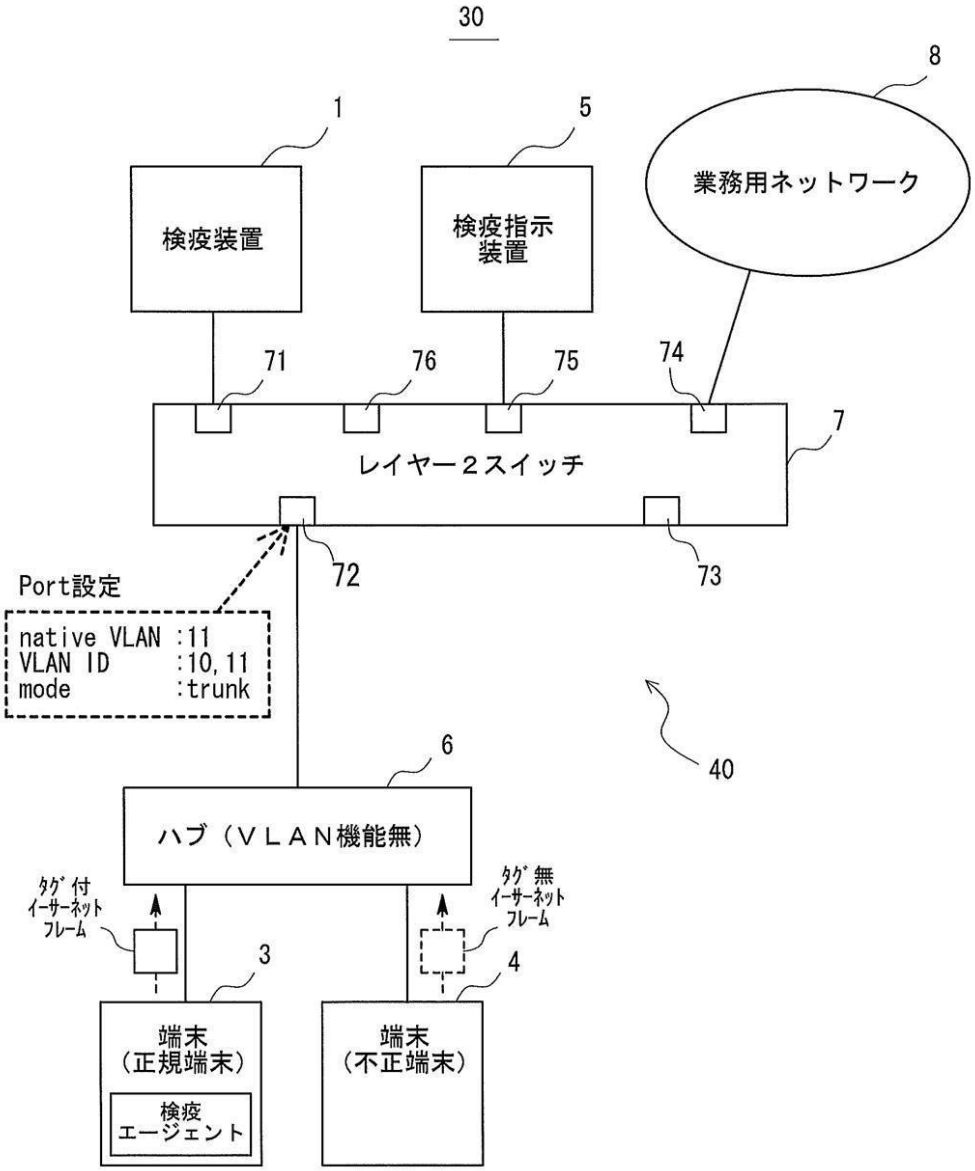
【０１２９】
以上のように、本発明によれば、レイヤー２スイッチのポートに、ＶＬＡＮ機能を有していない集線装置を介して、複数の端末が接続された場合であっても、各端末に対して個別に検疫を実行することができる。本発明は、ＶＬＡＮ機能を有していない集線装置と、ＶＬＡＮ機能を有しているレイヤー２スイッチとが混在している、ネットワークに、特に有用である。

【符号の説明】

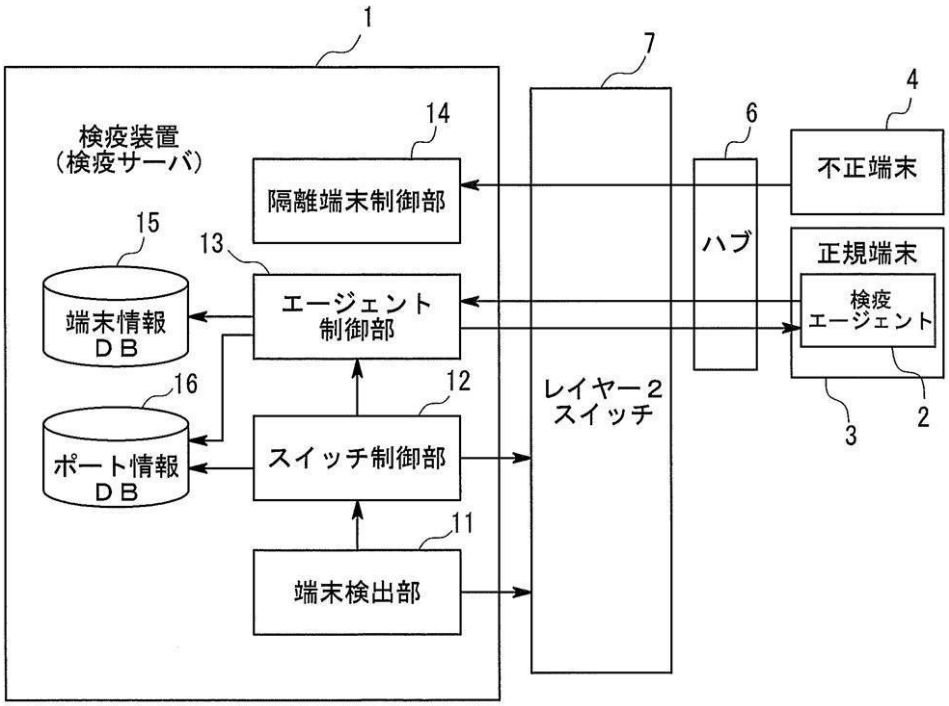
【０１３０】
１　検疫装置（実施の形態１）
２　検疫エージェント
３　端末（正規端末）

４　端末（不正端末）
５　検疫指示装置
６　ハブ
７　レイヤー２スイッチ
８　業務ネットワーク
１１　端末検出部
１２　スイッチ制御部
１３　エージェント制御部
１４　隔離端末制御部
１５　端末情報データベース
１６　ポート情報データベース
１７　ルーティング制御部
３０　検疫システム（実施の形態１）
４０　ネットワーク
５０　検疫装置（実施の形態２）
６０　検疫システム（実施の形態２）
１１０　コンピュータ
１１１　ＣＰＵ
１１２　メインメモリ
１１３　記憶装置
１１４　入力インターフェイス
１１５　表示コントローラ
１１６　データリーダ／ライタ
１１７　通信インターフェイス
１１８　入力機器
１１９　ディスプレイ装置
１２０　記録媒体
１２１　バス

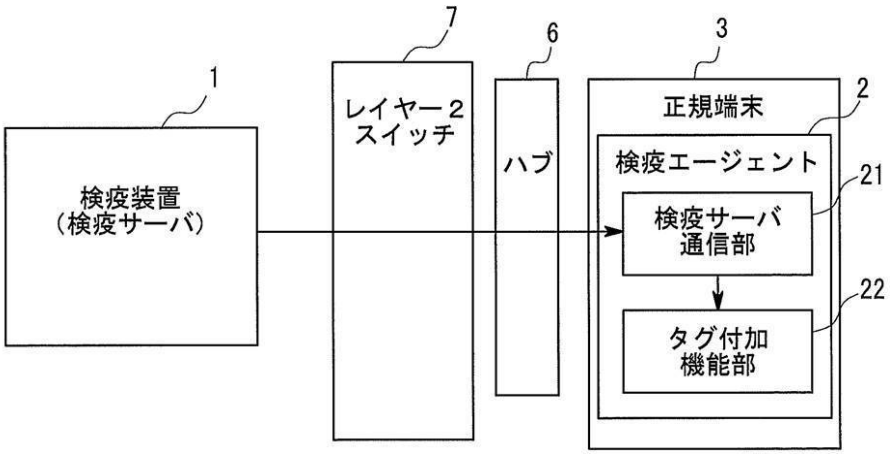
【図１】


30
8
1
5
検疫装置
検疫指示
装置
業務用ネットワーク
71
76
75
74
7
レイヤー２スイッチ
72
73
Port設定
native VLAN :11
VLAN ID :10,11
mode :trunk
40
6
ハブ（ＶＬＡＮ機能無）
ﾀｸﾞ付
ｲｰｻｰﾈｯﾄ
ﾌﾚｰﾑ
ﾀｸﾞ無
ｲｰｻｰﾈｯﾄ
ﾌﾚｰﾑ
3
4
端末
（正規端末）
検疫
エージェント
端末
（不正端末）

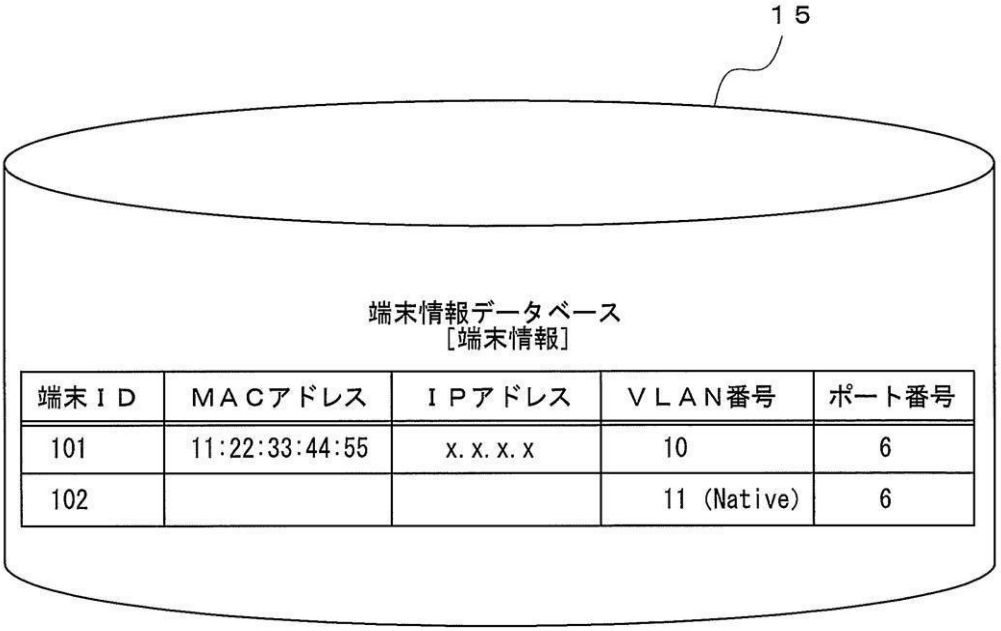
【図２】


1
検疫装置
（検疫サーバ）
14
隔離端末制御部
15
端末情報
ＤＢ
13
エージェント
制御部
16
ポート情報
ＤＢ
12
スイッチ制御部
11
端末検出部
7
レイヤー２
スイッチ
6
ハブ
4
不正端末
正規端末
検疫
エージェント
3
2

【図３】


1
検疫装置
（検疫サーバ）
7
レイヤー２
スイッチ
6
ハブ
3
正規端末
2
検疫エージェント
21
検疫サーバ
通信部
22
タグ付加
機能部

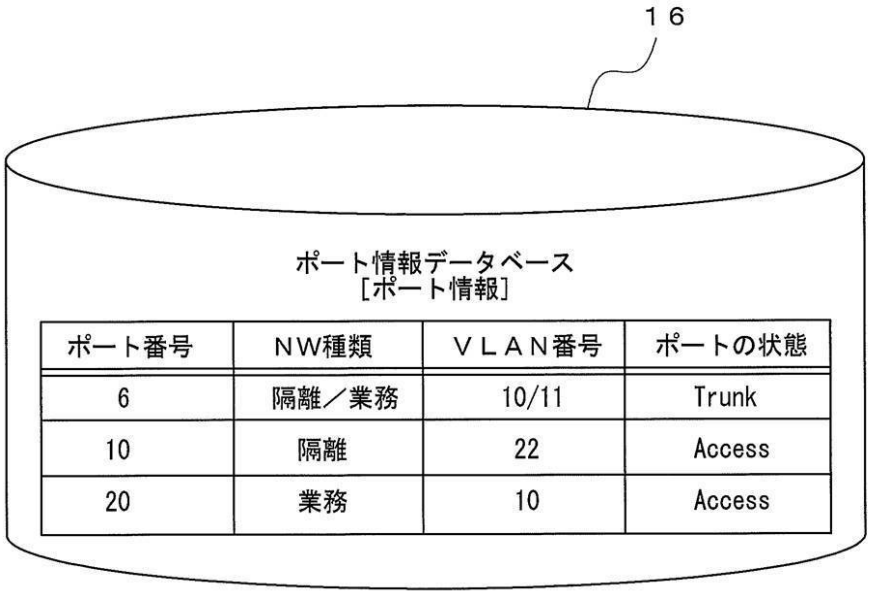
【図４】



端末情報データベース
［端末情報］

端末ＩＤ	ＭＡＣアドレス	ＩＰアドレス	ＶＬＡＮ番号	ポート番号
101	11:22:33:44:55	x.x.x.x	10	6
102			11 (Native)	6

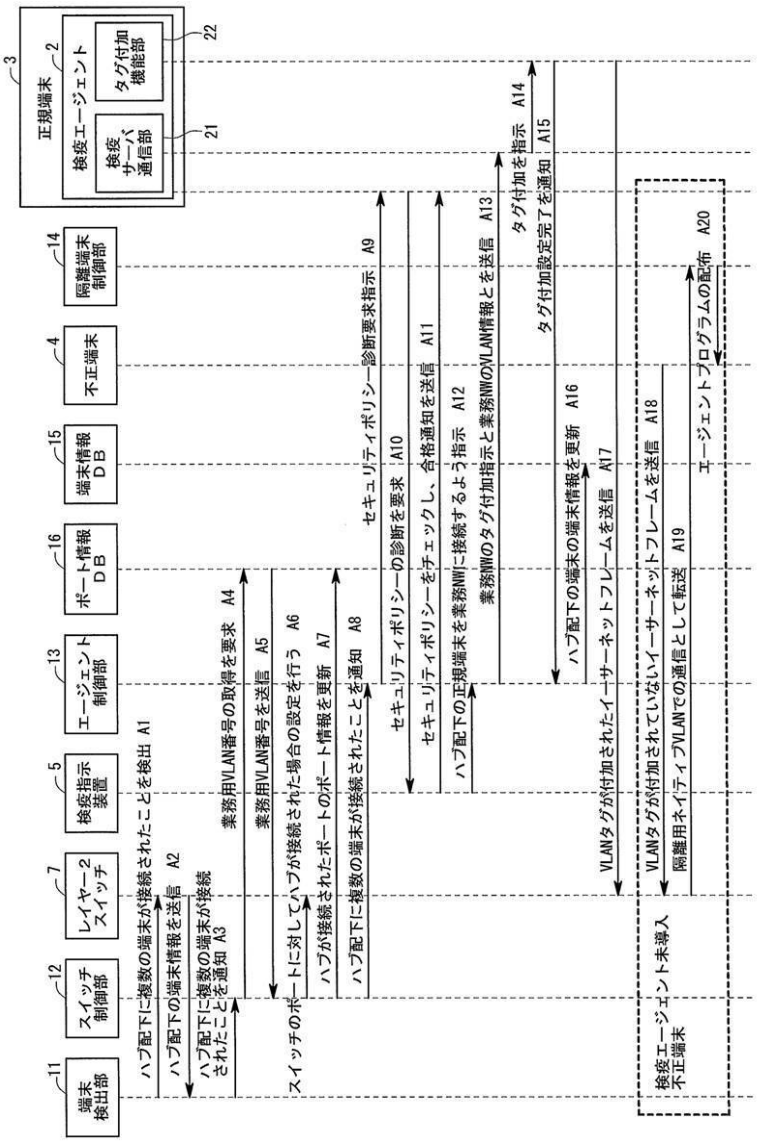
【図５】



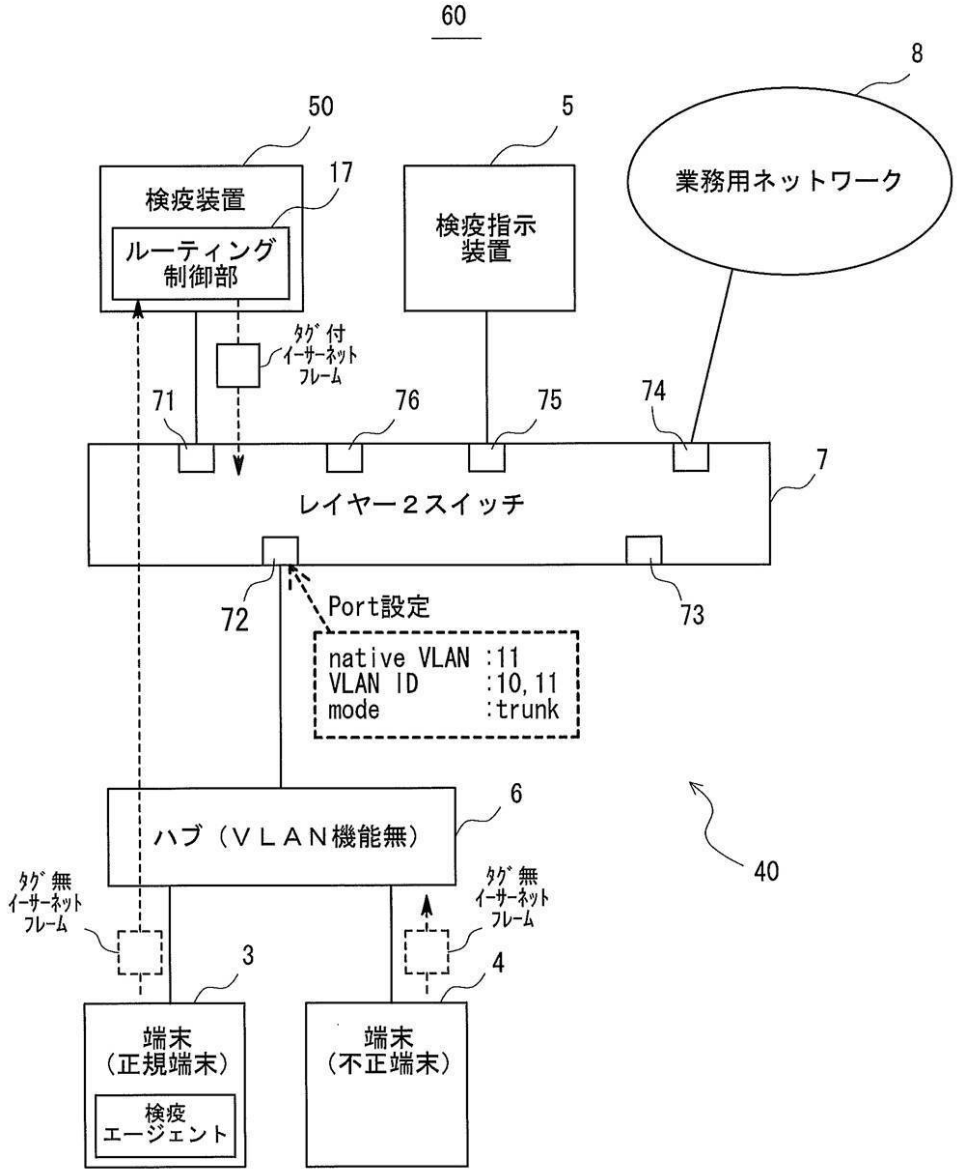
ポート情報データベース
［ポート情報］

ポート番号	ＮＷ種類	ＶＬＡＮ番号	ポートの状態
6	隔離／業務	10/11	Trunk
10	隔離	22	Access
20	業務	10	Access

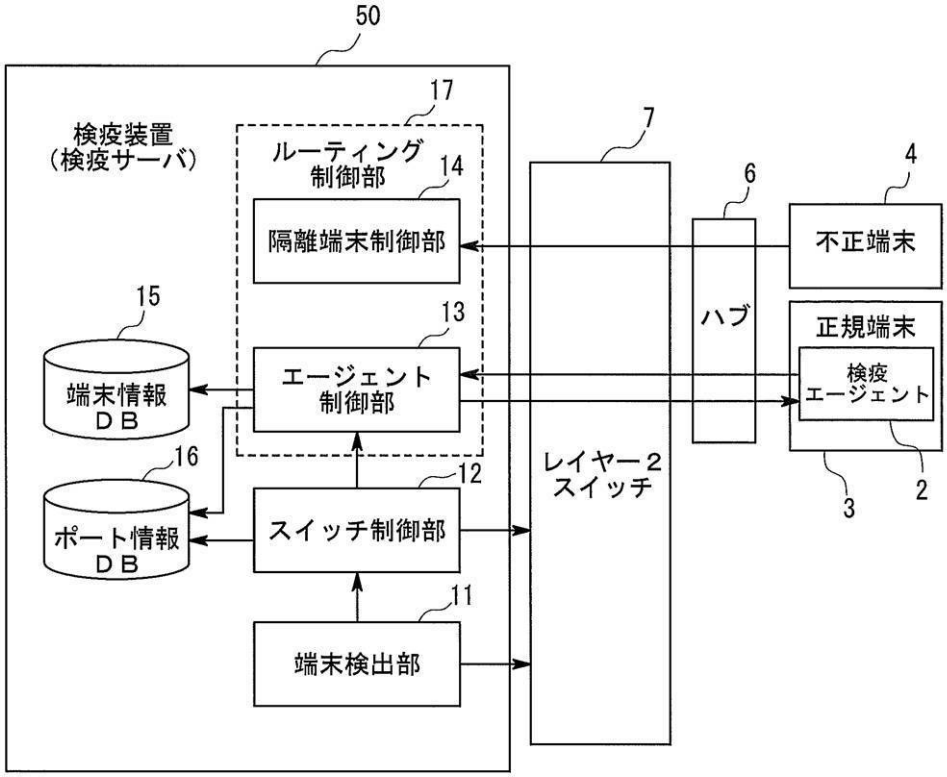
【図６】


11 端末検出部
12 スイッチ制御部
7 レイヤー2スイッチ
5 検疫指示装置
13 エージェント制御部
16 ポート情報DB
15 端末情報DB
4 不正端末
14 隔離端末制御部
3 正規端末
2 検疫エージェント
検疫サーバ通信部 21
タグ付加機能部 22
ハブ配下に複数の端末が接続されたことを検出 A1
ハブ配下の端末情報を送信 A2
ハブ配下に複数の端末が接続されたことを通知 A3
業務用VLAN番号の取得を要求 A4
業務用VLAN番号を送信 A5
スイッチのポートに対してハブが接続された場合の設定を行う A6
ハブが接続されたポートのポート情報を更新 A7
ハブ配下に複数の端末が接続されたことを通知 A8
セキュリティポリシー診断要求指示 A9
セキュリティポリシーの診断を要求 A10
セキュリティポリシーをチェックし、合格通知を送信 A11
ハブ配下の正規端末を業務NWに接続するよう指示 A12
業務NWのタグ付加指示と業務NWのVLAN情報とを送信 A13
タグ付加を指示 A14
タグ付加設定完了を通知 A15
ハブ配下の端末情報を更新 A16
VLANタグが付加されたイーサーネットフレームを送信 A17
VLANタグが付加されていないイーサーネットフレームを送信 A18
隔離用ネイティブVLANでの通信として転送 A19
エージェントプログラムの配布 A20
検疫エージェント未導入不正端末

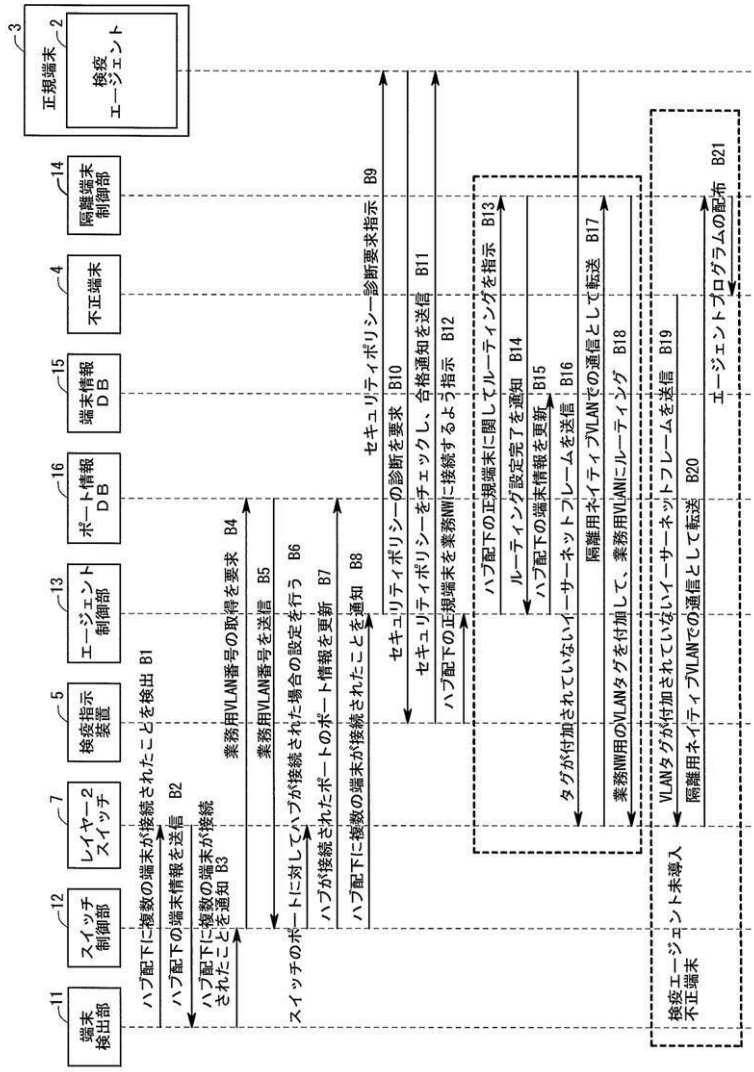
【図７】


60
8
50
5
検疫装置
17
ルーティング
制御部
検疫指示
装置
業務用ネットワーク
ﾀｸﾞ付
ｲｰｻｰﾈｯﾄ
ﾌﾚｰﾑ
71
76
75
74
7
レイヤー２スイッチ
72
Port設定
73
native VLAN :11
VLAN ID :10,11
mode :trunk
6
ハブ（ＶＬＡＮ機能無）
40
ﾀｸﾞ無
ｲｰｻｰﾈｯﾄ
ﾌﾚｰﾑ
ﾀｸﾞ無
ｲｰｻｰﾈｯﾄ
ﾌﾚｰﾑ
3
4
端末
（正規端末）
検疫
エージェント
端末
（不正端末）

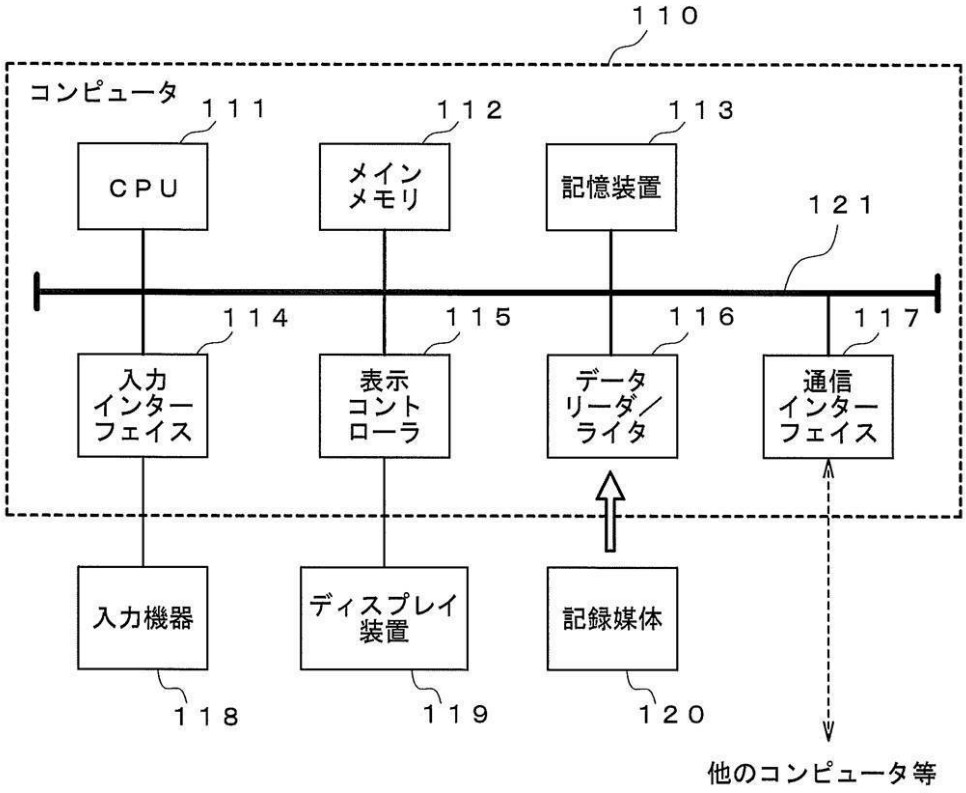
【図８】


50
検疫装置
（検疫サーバ）
17
ルーティング
制御部
14
隔離端末制御部
15
端末情報
ＤＢ
13
エージェント
制御部
16
ポート情報
ＤＢ
12
スイッチ制御部
11
端末検出部
7
レイヤー２
スイッチ
6
ハブ
4
不正端末
正規端末
検疫
エージェント
3
2

【図９】


正規端末
検疫エージェント
端末検出部
スイッチ制御部
レイヤー2スイッチ
検疫指示装置
エージェント制御部
ポート情報DB
端末情報DB
不正端末
隔離端末制御部
ハブ配下に複数の端末が接続されたことを検出 B1
ハブ配下の端末情報を送信 B2
ハブ配下に複数の端末が接続されたことを通知 B3
業務用VLAN番号の取得を要求 B4
業務用VLAN番号を送信 B5
スイッチのポートに対してハブが接続された場合の設定を行う B6
ハブが接続されたポートのポート情報を更新 B7
ハブ配下に複数の端末が接続されたことを通知 B8
セキュリティポリシー診断要求指示 B9
セキュリティポリシーの診断を要求 B10
セキュリティポリシーをチェックし、合格通知を送信 B11
ハブ配下の正規端末を業務NWに接続するよう指示 B12
ハブ配下の正規端末に関してルーティングを指示 B13
ルーティング設定完了を通知 B14
ハブ配下の端末情報を更新 B15
タグが付加されていないイーサーネットフレームを送信 B16
隔離用ネイティブVLANでの通信として転送 B17
業務NW用のVLANタグを付加して、業務用VLANにルーティング B18
検疫エージェント未導入
不正端末
VLANタグが付加されていないイーサーネットフレームを送信 B19
隔離用ネイティブVLANでの通信として転送 B20
エージェントプログラムの配布 B21

【図１０】


１１０
コンピュータ
１１１
ＣＰＵ
１１２
メイン
メモリ
１１３
記憶装置
１２１
１１４
入力
インター
フェイス
１１５
表示
コント
ローラ
１１６
データ
リーダ／
ライタ
１１７
通信
インター
フェイス
入力機器
ディスプレイ
装置
記録媒体
１１８
１１９
１２０
他のコンピュータ等

フロントページの続き

(56)参考文献 特開２００８－２８９０４０（ＪＰ，Ａ）
特開２００８－１９３２３１（ＪＰ，Ａ）
特開２００８－６０７６６（ＪＰ，Ａ）
特開２００６－３３９９３３（ＪＰ，Ａ）
「セキュリティ機能」の差はどこで見分ける？，NETWORK WORLD，２００７年 2月 1日，第12巻、第2号，pp.48-50，Windows Server World 2月号別冊
検疫とネットワーク認証がLANを脅威から守る砦，日経コミュニケーション，２００６年 5月 1日，第461号，pp.54-57
北井 彦久 他，IPCOM Lシリーズ 認証機能，PFU・テクニカルレビュー，２００６年１１月１日，第17巻、第2号，pp.39-46

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／００－６６