(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5062967号
(P5062967)
(45)発行日　平成24年10月31日(2012.10.31)　(24)登録日　平成24年8月17日(2012.8.17)

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

請求項の数 10　(全 13 頁)

(21)出願番号　特願2005-160863(P2005-160863)
(22)出願日　平成17年6月1日(2005.6.1)
(65)公開番号　特開2006-339933(P2006-339933A)
(43)公開日　平成18年12月14日(2006.12.14)
審査請求日　平成20年3月28日(2008.3.28)
審判番号　不服2011-6812(P2011-6812/J1)
審判請求日　平成23年4月1日(2011.4.1)

(73)特許権者　504411166
アラクサラネットワークス株式会社
神奈川県川崎市幸区鹿島田８９０
(74)代理人　100100310
弁理士　井上　学
(72)発明者　鈴木　伸介
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　柴田　剛志
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　樋口　秀光
東京都品川区南大井六丁目２６番２号　アラクサラネットワークス株式会社内

最終頁に続く

(54)【発明の名称】ネットワークアクセス制御方法、およびシステム

(57)【特許請求の範囲】
【請求項１】
端末、認証サーバ、及び検疫サーバとに接続され、該端末が属するVLANを収容するLayer2スイッチであって、
認証サーバ、及び検疫サーバとにネットワークを介して接続されるインターフェースと、
上記端末から上記インターフェースを介してLayer2の認証用パケットを受信し、該パケットに基づいて上記端末の認証を行う認証手段と
上記認証手段におけるLayer2の認証が成功した後、上記端末から送信された上記端末のＬａｙｅｒ２のアドレスと収容するＶＬＡＮの識別子と上記Ｌａｙｅｒ２スイッチのＬａｙｅｒ３のアドレスとの対応付けを含む上記検疫サーバ宛のLayer3の検疫用パケットを上記検疫サーバに、上記インターフェースを介して転送する転送手段と、
上記検疫サーバにおけるLayer3の検疫で上記端末が正常と確認された後、上記端末のLayer2アドレスと変更された上記端末が収容するＶＬＡＮの識別子と当該Ｌａｙｅｒ２スイッチのＬａｙｅｒ３のアドレスとを対応付けに基づいて生成されたVLAN変更指示を上記検疫サーバから受け、上記ＶＬＡＮ変更指示に従って上記端末を収容するVLANを変更するＣＰＵと、を有することを特徴とするLayer2スイッチ。
【請求項２】
請求項１記載のLayer2スイッチであって、
上記ＣＰＵは、上記VLAN変更指示に従って、上記Layer3の検疫で正常と確認された端末

のみを収容するVLANに上記端末を収容することを特徴とするLayer2スイッチ。
【請求項３】
端末、該端末が属するVLANを収容するLayer2スイッチ、さらに該VLANを収容するLayer3スイッチ、認証サーバ、及び検疫サーバが互いに接続されたネットワークシステムであって、
上記認証サーバにおける上記端末のLayer2の認証が成功した後、
上記Ｌａｙｅｒ２スイッチが、上記端末から送信された上記端末のＬａｙｅｒ２のアドレスと収容するＶＬＡＮの識別子と上記Ｌａｙｅｒ２スイッチのＬａｙｅｒ３のアドレスとの対応付けを含む上記検疫サーバ宛のLayer3の検疫用パケットを上記検疫サーバに、上記インターフェースを介して転送し、上記検疫サーバが、上記端末のLayer3の検疫を実行し、該Layer3の検疫で上記端末が正常と確認された後、上記端末のLayer2アドレスと上記端末を収容するＶＬＡＮの識別子と当該Ｌａｙｅｒ２スイッチのＬａｙｅｒ３のアドレスとを対応付け、
上記検疫サーバからのVLAN変更指示に従い、上記Layer2スイッチが該端末を収容するVLANを変更することを特徴とするネットワークシステム。
【請求項４】
請求項３記載のネットワークシステムであって、
上記Layer2スイッチは、上記検疫サーバからの上記VLAN変更指示に従って、上記Layer3の検疫で正常と確認された端末のみを収容するVLANに上記端末を収容することを特徴とするネットワークシステム。
【請求項５】
請求項４記載のネットワークシステムであって、
上記Layer3スイッチは、受信したフレームの送信元Layer2アドレスが該Layer3スイッチ自身のアドレスでなければ廃棄することを特徴とするネットワークシステム。
【請求項６】
請求項５記載のネットワークシステムであって、
上記Layer3スイッチは、さらにVLANごとに対応付けられるアクションを設定可能なことを特徴とするネットワークシステム。
【請求項７】
請求項３記載のネットワークシステムであって、
上記Layer2スイッチは、上記端末がネットワーク接続された際に、該端末のLayer2アドレス、および所属VLANの情報を上記検疫サーバへ送信し、
上記検疫サーバは、上記Layer2スイッチから受信した情報に基づき、上記端末と該端末を収容する上記Layer2スイッチとを対応付けて管理することを特徴とするネットワークシステム。
【請求項８】
請求項７記載のネットワークシステムであって、
上記検疫サーバは、複数のLayer2スイッチから同一端末の端末収容を通知された際に、いずれか一のLayer2スイッチを対応付けて管理することを特徴とするネットワークシステム。
【請求項９】
請求項８記載のネットワークシステムであって、
いずれか一のLayer2スイッチは、複数のＬａｙｅｒ２スイッチのうち優先度が最も高いものであり、上記検疫サーバは、上記一のＬａｙｅｒ２スイッチにのみ、上記端末のVLAN変更指示を送信することを特徴とするネットワークシステム。
【請求項１０】
請求項３記載のネットワークシステムであって、
上記Layer3スイッチが、上記端末がLayer2の認証のみに成功している場合、当該端末を収容するVLANからは上記検疫サーバとのみ通信できるようにすることを特徴とするネットワークシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネットにおける通信制御技術に関し、特にネットワークアクセス制御技術に関する。
【背景技術】
【０００２】
今日の企業網では、セキュリティ保全を図るために、企業網とインターネットとの境界にファイアウォールを設置し、外部から企業網への不正アクセスや攻撃を防止する。しかしながら持込端末やメールやWebなどを介した、ファイアウォール内でのウィルス拡散被害が広がっている今日、ファイアウォールだけでのセキュリティ保全は困難になってきている。
【０００３】
こうした潮流に対して、検疫ネットワークというコンセプトが提案されている。検疫ネットワークは、端末のネットワークアクセス認証を行う際に端末のセキュリティ状態をチェックし、ウィルス感染端末や資産管理ソフトなどがインストールされていない不正な端末を、正常な端末から隔離されたセグメント(検疫セグメント)へ収容するコンセプトである(非特許文献1)。このコンセプトの実現のためにはこれまで、IEEE802.1x連動方式とDHCP連動方式の2つの方法が用いられてきた。
【０００４】
IEEE802.1x連動方式は、端末がLayer2ネットワーク装置への接続許可をIEEE802.1xを用いて要請する際に、端末のセキュリティ状態に基づいた認証を行う方式である。Cisco社のNAC(Network Admission Control) (非特許文献2)が代表例である
一般にIEEE802.1xでは、ユーザ名とパスワードの組を端末から認証サーバへ送付することによりログイン認証を行う。これに対してIEEE802.1x連動方式を用いた検疫ネットワークでは、アンチウィルスソフトのバージョンなどの端末自体に関する情報を端末から認証サーバへ送付する。この情報に基づき、認証サーバが端末のセキュリティ状態に基づいた認証を行う。
【０００５】
DHCP連動方式は、ネットワークから端末に与えるアドレスとして仮IPアドレスと正規IPアドレスとを使い分けることにより、端末のセキュリティ状態に基づく認証を行う方式である。NEC社のVital QIPが代表例である。
【０００６】
端末がネットワークに接続されると、DHCPサーバは端末へまず仮IPアドレスを配布する。仮IPアドレスを用いて端末がウェブアクセスを行うと、検疫サーバはそのウェブアクセスを検知し、ウェブアクセスを行った端末へ検疫スクリプトを送り返す。検疫スクリプトは、端末のセキュリティ状態をチェックした結果を検疫サーバへ報告するように作られている。検疫スクリプトが端末はセキュアであると判定した場合、その報告を受けた検疫サーバはDHCPサーバへ指示して、その端末へ割り当てた仮IPアドレスを回収し正規のIPアドレスを割り当てる。逆にセキュアではないと判定した場合には、仮IPアドレスが割り当てられたままである。この仮IPアドレスでの通信範囲をルータやスイッチのフィルタ設定により制限することにより、端末のセキュリティ状態に応じて端末を異なるネットワークへ隔離することができる。
【０００７】
【非特許文献１】「検疫ネットワークで不正なパソコンを取り締まる」、日経Windows（登録商標）プロ2004年11月号 pp.78-89
【０００８】
【非特許文献２】“Network Admission Control”、http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdcont_0900aecd800fdd66.pdf
【発明の開示】

【発明が解決しようとする課題】
【０００９】
上述の2つの従来技術にはそれぞれ異なる課題がある。IEEE802.1x連動方式の課題は、既存管理フレームワークからの移行の困難さである。DHCP連動方式の課題は、ネットワーク自体への攻撃を防げないことと端末再検疫の困難性である。以下それぞれについて説明する。
【００１０】
IEEE802.1x連動方式では、IEEE802.1xの認証セッション上でその管理ツールの認証機能を動かす必要がある。既にセキュリティ監視ツールや資産管理ツールを導入している企業網にとって、検疫ネットワーク導入のために既存の管理ツールを置き換えることは費用手間の両面から困難である。特に目的に応じて複数の管理ツールを用いている場合(例.資産管理とセキュリティ管理)、IEEE802.1x連動方式では全ての管理ツールの認証機能をまとめてIEEE802.1xの1つの認証セッション上で動かす必要があり、対応が困難である。
【００１１】
IEEE802.1xにおける認証セッション用のデータフォーマットは、RADIUSの属性値として事実上標準化されている。RADIUSはログイン認証に必要な情報(例.ユーザ名やパスワード)のフォーマットは標準化しているが、端末のセキュリティ状態の認証に必要な情報(例.アンチウィルスソフトのバージョン)は標準化していない。端末のセキュリティ状態の定義はサイトごとに異なるために、一般的な形で標準化することが困難なためである。セキュリティ情報を運ぶ手段に標準がないために、検疫ネットワークを構成するソフトウェアやネットワーク装置間の相互接続性を確保することは難しく、検疫ネットワークの導入をより困難にしている。
【００１２】
DHCP連動方式は、ネットワークアクセス制御をIPアドレスのサブネットに基づいて実現する技術である。この技術では、異なるIPサブネット間の通信は制御可能であるが、同一IPサブネット内での攻撃(例. ウィルス拡散やトラフィック飽和)を回避することは難しい。
【００１３】
またDHCP認証技術は、仮に割り振ったIPアドレスに対して端末のセキュリティ状態を監視する技術である。従って正規IPアドレス割当後に、端末のセキュリティ状態を継続監視することが困難である。
【課題を解決するための手段】
【００１４】
本発明では、端末のログイン認証と端末のセキュリティ状態の監視とを独立に実施し、それぞれの結果に基づき端末のLayer2的な接続性を制御することにより、上記の3つの問題を解決する。
本発明では、1つのIPサブネットを複数のVLANから構成し、VLAN間の直接通信ができないようにする。そして各VLANから通信可能な範囲を事前にVLAN毎に変えておく。
【００１５】
端末が上記のIPサブネットに接続するためのログイン認証を完了すると、端末はIPアドレスを与えられ、検疫サーバとだけ通信可能なVLANへ収容される。そしてその端末を収容するスイッチは、検疫サーバに対して、その端末の収容状況を通知する。
IPアドレスを与えられた端末は、検疫サーバに対して検疫開始要求を送信する。検疫サーバはその検疫開始要求を受けると、検疫開始要求を送信した端末に対するセキュリティ状態の確認を行う。
【００１６】
検疫サーバが端末を正常と判断した場合、検疫サーバはその端末を収容するスイッチに対して、その端末を正規な通信が可能なVLANへ収容するよう指示する。異常であると判断した場合には、端末を検疫サーバとだけ通信可能なVLANに収容したまま放置する。
【００１７】

端末は、正規な通信が可能なVLANに収容された後も、定期的に検疫サーバへ検疫開始要求を送信し、検疫サーバは上述の検疫作業を繰り返す。これにより端末の再認証を定期的に実施する。

【発明の効果】

【００１８】

上記の解決手段により、従来技術の3つの課題はそれぞれ以下のように解決される。本発明では、端末ログイン認証をIEEE802.1x等をそのまま用いて実現することができる。更に既存の資産管理やセキュリティ管理用のアプリケーションをそのまま動かし、管理サーバがその管理結果に基づいて、端末を収容するLayer2スイッチ設定を変更することにより、端末のセキュリティ状態に基づく検疫を行うことができる。そのため、既存の認証プロトコルや管理プロトコルを変更せずに、容易に検疫ネットワークを実現することができる。

【００１９】

本発明では、端末のLayer2接続性を変更するのみであり、端末のIPアドレスはセキュリティ状態の結果にかかわらず変わらない。従って、既存の管理プロトコルを動かし続けることにより、検疫を終えた端末を継続して監視することができる。さらに監視の結果異常が見つかった場合には、検疫サーバからLayer2スイッチへ指示を送ることにより、端末の接続するネットワークを変更することも可能である。

【００２０】

上記の解決手段では、端末のネットワーク接続性を端末のアドレスに基づいてLayer2レベルで制御している。従って、ネットワーク自体への攻撃を最小限に抑えることができる。

本発明は従来技術の3つの課題を解決するのみではなく、より柔軟なネットワークアクセス制御の実現にも役立つ。

【００２１】

通常検疫ネットワークでは、ユーザ認証や端末のセキュリティ状態監査などを単一のプロトコルだけ上で全て行う。これに対して本発明では、認証に基づくVLAN割当を複数独立動作させ、それぞれの中で必要な認証処理を実行させる。そのため複数の観点からの端末監視を容易に実現することができる。

【００２２】

例えば複数種類のセキュリティ監査プロトコルを動作させることにより、より厳しく端末のセキュリティ状態をチェックすることができる。また端末の通信ログ監査プロトコルとユーザ認証プロトコルとを同時動作させることにより、ネットワークへのアクセス権限は持っていても不正な情報漏洩を過去に過去に行ったユーザを、ネットワークから排除させることもできる。

【発明を実施するための最良の形態】

【００２３】

本発明は、端末を収容するLayer2スイッチと端末を監視する管理サーバの2箇所にて実施される。以下具体的な実現例について説明する。

【実施例１】

【００２４】

本実施例では送信元MACアドレスによりVLANを定めるMAC-VLANを用いた実施例を説明する。物理ポート単位で所属VLANを決定するポートVLANに対しても同様な方法を用いて、本発明は実現可能である。

【００２５】

図1にネットワークの物理構成を示す。本発明の制御の対象である端末160、161、162は、MAC-VLAN機能を有するLayer2スイッチ140、150に収容される。Layer3スイッチ130は、Layer2スイッチ140、150をそれぞれ2本の回線で収容し、端末160、161、162を収容するIPサブネット170を構成する。Layer3スイッチはIPサブネット170と同時に、外部ネット100、認証サーバ110、検疫サーバ120を収容する。認証サーバ110はLayer2スイッチと通信す

るRADIUSプロトコルのサーバであり、端末160、161、162のLayer2スイッチ140への接続をログイン名とパスワードの組で認証する。検疫サーバ120は端末160、161、162に組み込まれたソフトウェアと通信し、これらの端末が検疫に合格したか否かを判定するサーバである。検疫内容の具体例としてはウィルス感染の有無、所定のソフトウェアのインストール状態などがあるが、検疫の内容及び検疫に用いる通信プロトコルはどのようなものでも構わない。

【００２６】

図2は図1のネットワークの論理構成を示した図である。端末160、161、162はユーザ認証をパスすると検疫VLAN180に収容される。更に検疫サーバ120の検疫に合格すると通常VLAN181、183に収容される。どちらのVLANも同一IPサブネット170上に存在するし、Layey3スイッチ130がそのIPサブネットのデフォルトゲートウェイとして振舞う。

【００２７】

Layer3スイッチ130はIPサブネット170に入出力されたパケットを、図3のアルゴリズムに従い中継及び廃棄する。入力パケットに対しては、宛先Layer3アドレスが検疫サーバ120のアドレスのパケット(ステップ430)、宛先Layer3アドレスがLayer3スイッチ自身もしくはLayer3スイッチを含むマルチキャストアドレスであるパケット(ステップ440)ならばどのVLANから入力されたとしても中継する。それ以外のパケットが入力された場合には、それが通常VLANから入力された場合のみ中継する(ステップ450)。Layer3スイッチからIPサブネット170へパケット出力する場合は、そのパケットのLayer2アドレスがLayer3スイッチ自身であるパケットのみを中継する(ステップ420)。

【００２８】

Layer3スイッチは入力されたパケットがどちらのVLANに所属するかを、パケットが入力されたポートにより判定する。図1及び図2では通常VLANと検疫VLANがそれぞれ異なる物理ポートでLayer3スイッチ130に接続されているように描いているが、IEEE802.1qのような論理的なポート多重技術を用いても構わない。

【００２９】

本アルゴリズムにより、通常VLANから入力されたパケットは外部ネット100、検疫サーバ120、認証サーバ110へ通信可能となる。一方検疫VLANから入力されたパケットは検疫サーバ120とLayer3スイッチ130へのみ通信可能となる。検疫VLAN上の端末は検疫サーバ120と異なるIPサブネットに所属しているが、検疫VLAN上の端末はLayer3スイッチ自身へは通信可能であるため、Layer3スイッチを経由することにより検疫サーバ120へ通信可能となる。従って検疫VLANに所属した端末は、不正に外部ネット100への通信及び、Layer3スイッチ経由で通常VLANに所属する端末への通信を行うことができない。

【００３０】

検疫VLANに所属した端末が同じVLANに所属する他の端末と通信できることは、セキュリティ上問題になる可能性がある。例えばウィルスに感染したために通常VLANに所属できなかった端末が、ユーザ認証が完了し検疫サーバの検疫を待っている端末にウィルスを感染させることもあるためである。検疫VLANに所属することに伴う問題を防ぐために、Layer2スイッチ140、150においては、検疫VLANでの端末間の直接通信を防止するフィルタを設定する。フィルタの内容を以下に説明する。

【００３１】

検疫VLANへ入力されたパケットがLayer3スイッチ130と接続される物理ポートから入力された場合には、そのパケットは検疫VLAN内端末からのパケットではないため通過させる。検疫VLANへ入力されたパケットが同じ物理ポートへ出力される場合も、そのパケットは検疫VLAN内端末へのパケットではないため通過させる。この2つのいずれにも該当しない検疫VLANへ入力されたパケットは、全て検疫VLAN内端末から他の検疫VLAN内端末へのパケットであるため、廃棄する。以上のフィルタ設定により、検疫VLAN内での端末間通信を防止することができる。

【００３２】

以下に、端末をLayer2スイッチ140、150にて通常VLANまたは検疫VLANに振り分ける方法

を示す。
そのためにまずLayer2スイッチの構成を説明する。図4にLayer2スイッチのハードウェア構成を示す。Layer2スイッチは、物理インタフェース143、144、145間のフレーム中継をCPU142にて制御する装置である。CPUにおけるフレーム制御方法はプログラムにて実現されており、そのプログラムは記憶装置142に収容されている
図5にLayer2スイッチのソフトウェア構成を示す。物理インタフェースに入力されたフレームはフレーム中継処理プログラム200により適切な物理インタフェースに出力される。以下フレーム中継処理プログラム200の動作を説明する。
Layer2フレーム中継部220はフレームが入力されると、VLANデータベース230の物理インタフェース情報232と送信元MACアドレス情報233とマッチングを取ることにより、そのフレームがどのVLANに所属するかを決定する。IEEE802.1qの場合はフレーム内に含まれるtagの値により所属VLANが決まり、MAC-VLANの場合はフレーム内に含まれる送信元MACアドレスにより所属VLANを決まる。VLANデータベース230は、ネットワーク管理者がフレーム制御プログラム250を経由して設定するものである。
【００３３】
フレームの所属するVLANが決まると、Layer2フレーム中継部220はそのフレームの送信元MACアドレスが上で決まった所属VLAN上の物理インタフェースに存在することを、MAC学習データベース260へ反映する。同時にそのフレームを送信先MACアドレスが存在する物理インタフェースへ送信する。但しフレームフィルタ270のフローパターン271にマッチするフレームである場合には、その送信先MACアドレスが存在する物理インタフェースではなく該当するエントリのアクション272に従ってフレームを送信する。IEEE802.1xのような認証用のフレームは、フレームフィルタ270により、Layer2プロトコル処理部240を介してユーザ認証プログラム252へ送信される。フレームフィルタ270も、VLANデータベース230と同様に、ネットワーク管理者がフレーム制御プログラム250を経由して設定するものである。　Layer2フレーム中継部220は、送信先MACアドレスから物理インタフェースを発見するために、MAC学習データベース260とVLANデータベース230を用いる。フレームのVLAN番号と送信先MACアドレスとが、MAC学習データベース260上のVLANフィールド262とMACフィールド261にそれぞれマッチするエントリが存在する場合には、該当するエントリのポート情報262に示された物理インタフェースを出力先とする。ポート情報262に装置自身が指定されている場合、そのフレームはLayer2プロトコル処理部240へ渡される。MAC学習データベースにマッチするエントリが存在しない場合は、VLANデータベース230に示される物理インタフェースの全てを出力先とする。MAC学習データベースのエントリのマッチの有無に関わらず、あるVLANに所属するフレームは他のVLANには到達しないため、検疫VLANと通常VLANとはLayer2スイッチ内では相互に通信できない。
【００３４】
端末収容通知プログラム251は、Layer2スイッチに新たな端末が収容されたときに、その端末のMACアドレスとIPアドレスと所属VLANとを、事前に指定されたサーバへ送信するプログラムである。送信に用いるプロトコルはSNMP Trapなど任意のプロトコルでかまわない。送信を行う契機は、MAC学習データベース260の内容に変化が発生したとき、ユーザ認証プログラム252がユーザ認証を完了したとき、DHCPプロトコルに基づき端末へアドレス配布が行われたときなどである。端末のIPアドレスが不明な場合は、0.0.0.0というアドレスを通知する。
【００３５】
以下、上述のLayer2スイッチを制御する検疫サーバ120について説明する。図6にその物理構成を示す。検疫サーバ120は物理インタフェース123を介して、Layer2スイッチを制御する。具体的な制御アルゴリズムはCPU122にて実行され、そのプログラムは記憶装置121に格納されている。
【００３６】
図7に検疫サーバ120のソフトウェア構成を示す。検疫サーバ120上では、端末収容通知受信プログラム610と収容VLAN通知プログラム620と検疫作業プログラム630とが動作して

いる。そしてそれらの動作をサポートする端末情報データベース650とLayer2スイッチデータベース640とが存在する。端末情報データベース650は端末収容通知受信プログラム610を介して管理され、Layer2スイッチデータベース640は管理者がネットワークの構成に従い静的に定義する。

【００３７】

検疫作業プログラム630は、端末上にインストールされた検疫作業プログラムクライアントから情報を取得することにより端末の検疫を実際に行うプログラムである。検疫作業プログラム630は、端末のIPアドレスとその検疫結果との対応付けを収容VLAN通知プログラム620へ通知できなければならない。取得すべき内容や端末の検疫の判断基準は、ネットワーク管理者が任意に定めて構わない。

【００３８】

端末収容通知受信プログラム610の動作を、図8のフローチャートを用いて説明する。Layer2スイッチ上のユーザ認証プログラムがIEEE802.1xでの端末ログイン成功を検知すると、端末を検疫VLANへ収容すると同時に、端末収容通知プログラム251を用いて端末のMACアドレスとIPアドレス(0.0.0.0)と収容VLAN番号と自らのIPアドレスとの対応付けを端末収容通知受信プログラム610へ通知する(ステップ320)。端末収容受信プログラム610はこの通知に基づき、端末のMACアドレスとIPアドレスと所属VLANと収容スイッチとの対応付けを、端末情報データベース650に反映する(ステップ322)。IEEE802.1xでのLayer2スイッチへの接続に成功すると、端末はIPサブネット内のLayer3スイッチに対してDHCPやRouter SolicitationによりIPアドレスの配布を要求する(ステップ324)。Layer3スイッチはそのIPアドレス配布要求に従い端末へIPアドレスを配布すると(ステップ326)、端末は検疫サーバ120に対して自らの検疫を要求する(ステップ328)。検疫サーバは端末からの検疫要求を検疫作業プログラム630にて受け、要求を受けたIPアドレスに対して検疫作業を行い、その端末が検疫に合格するか否かを判定する(ステップ330)。検疫の結果に応じて、検疫作業プログラム630は収容VLAN通知プログラムへ、検疫を要求したIPアドレスの端末を通常VLAN(ステップ339)もしくは検疫VLANへ(ステップ338)へ収容するよう要請する。ステップ328からの検疫作業は定期的に行われるため、ログイン後の端末の検疫も可能となる(ステップ340)。

【００３９】

収容VLAN通知プログラム620の動作を、図9を用いて説明する。あるIPアドレスの端末を通常VLANに収容することになった場合、収容VLAN通知プログラムは端末情報データベース650から端末IPアドレスフィールド651が与えられたIPアドレスに合致するエントリを求める(ステップ510)。端末情報データベースに該当するIPアドレスが存在しない場合は、DHCPサーバや資産管理データベースやLayer3スイッチ130など外のサーバにそのIPアドレスとMACアドレスの対応付けを問い合わせ(ステップ520)、端末情報データベース650から見つかったMACアドレスを端末MACアドレスフィールド652に含むエントリを求める(ステップ550)。ステップ550でエントリが見つからなかった場合、もしくはステップ520でMACアドレスが見つからなかった場合は、収容通知指示自体を無効とみなし、何もせずプログラムは収容する(ステップ540)。

【００４０】

与えられたIPアドレスに対応する端末情報データベースエントリが複数見つかったときは、各エントリの端末収容スイッチIPアドレスフィールド654のアドレスに関して、Layer2スイッチデータベース640の端末収容スイッチIPアドレスフィールド641とマッチングを取る。そして各エントリの優先度フィールド644の値を比較し、最も値が大きいエントリを採用する(ステップ560)。

【００４１】

以上の作業により与えられたIPアドレスに対応する端末情報データベースエントリと、それに対応するLayer2スイッチデータベース640のエントリが一意に確定する。そのとき、収容VLAN通知プログラム620は、端末収容スイッチIPアドレスフィールド641のスイッチに対して、端末MACアドレスフィールド652のMACアドレスを通常VLAN IDフィールド642に

示されたVLANへ収容するように指示する(ステップ565)。VLAN収容の指示は、指定されたLayer2スイッチへリモートログインしMAC-VLAN設定コマンドを実行することにより実現する。

【００４２】

以上述べた、Layer2スイッチ上の端末収容通知プログラム251から検疫サーバ上の端末収容通知受信プログラム610間への通信と、検疫サーバ上の収容VLAN通知プログラム620からLayer2スイッチへのMAC-VLAN構成定義命令により、端末のログイン認証と端末のセキュリティ状態の検疫とを独立に実施し、それぞれの結果に基づき端末のLayer2的な接続性を制御することが可能となる。

【００４３】

以上の説明ではユーザ認証プロトコルとしてIEEE802.1xを用いた事例を説明したが、DHCPにてユーザ認証付きアドレス配布を行っても全く同様な手順で端末のログイン認証と端末のセキュリティ状態の検疫とを独立に実施できる。またユーザ認証が不要な場合には、Layer2スイッチからMAC学習テーブル650の内容変化を通知することにより、端末のセキュリティ状態の検疫のみを同じアルゴリズムで実現することができる。

【００４４】

更に、異なる検疫作業プログラム630を有する検疫サーバを設置し、そのサーバからも上述の制御を行うことにより、端末の検疫を複数の観点から実施することが可能になる。例えば複数種類のセキュリティ監査プロトコルを動作させることにより、特定のセキュリティ監査プロトコルの誤判定によるセキュリティ被害を軽減することができる。
またセキュリティ監査プロトコルとして更に端末の通信ログ監査プロトコルを動作させることにより、ネットワークへのアクセス権限は持ちセキュリティ上安全な端末であっても、過去に不正な情報漏洩を過去に過去に行った場合ネットワーク接続を制限することもできる。

【図面の簡単な説明】

【００４５】

【図１】本発明の対象となるネットワークの物理構成図である。
【図２】本発明の対象となるネットワークの論理構成図である。
【図３】図2のネットワークにおけるLayer3スイッチのフィルタリングルールである。
【図４】Layer2スイッチの物理構成図である。
【図５】Layer2スイッチのソフトウェアブロック図である。
【図６】検疫サーバの物理構成図である。
【図７】検疫サーバのソフトウェアブロック図である。
【図８】検疫サーバが端末収容VLANを変更するアルゴリズムのフローチャートである。
【図９】検疫サーバが端末収容VLANを通知するアルゴリズムのフローチャートである。

【符号の説明】

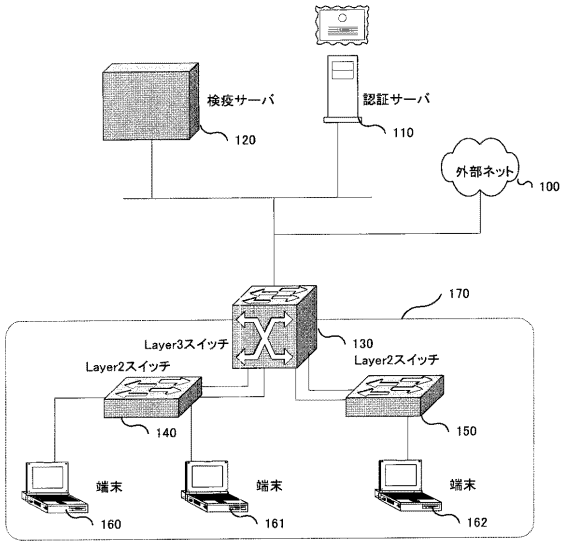
【００４６】

100 外部ネット
110 認証サーバ
120 検疫サーバ
121 記憶装置
122 CPU
123 物理インタフェース
130 Layer3スイッチ
140 Layer2スイッチ
141 記憶装置
142 CPU
143 物理インタフェース
144 物理インタフェース
145 物理インタフェース

150 Layer2スイッチ
160 端末
161 端末
162 端末
170 IPサブネット
180 検疫MAC-VLAN
181 通常MAC-VLAN
182 検疫MAC-VLAN
183 通常MAC-VLAN
200 フレーム中継処理プログラム
220 Layer2フレーム中継部
230 VLANデータベース
240 Layer2プロトコル処理部
250 フレーム中継制御プログラム
251 端末収容通知プログラム
252 ユーザ認証プログラム
260 MAC学習データベース
270 フレームフィルタ
610 端末収容通知受信プログラム
620 収容VLAN通知プログラム
630 検疫作業プログラム
640 Layer2スイッチデータベース
650 端末情報データベース。

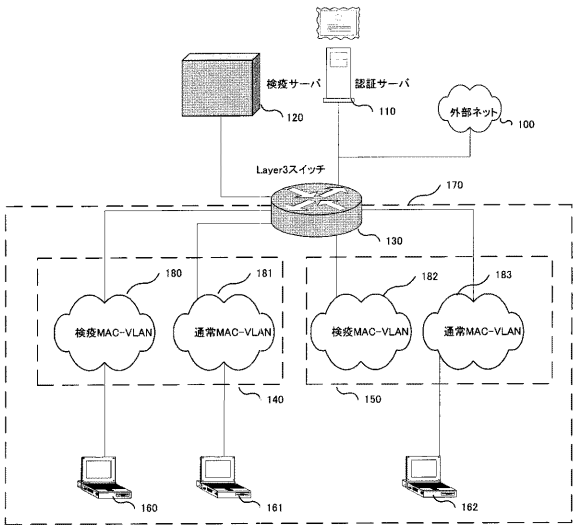
【図１】

図1



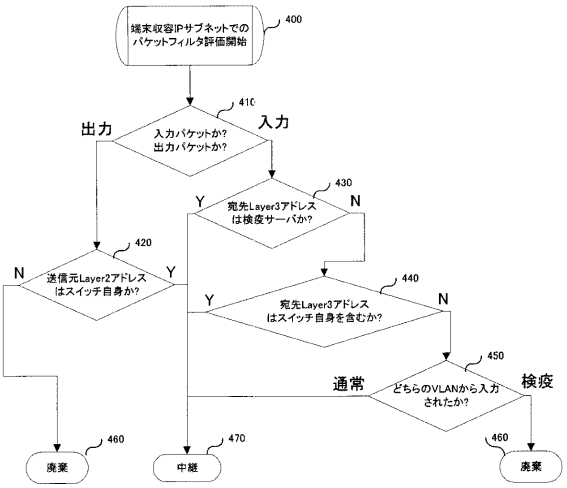
【図２】

図2



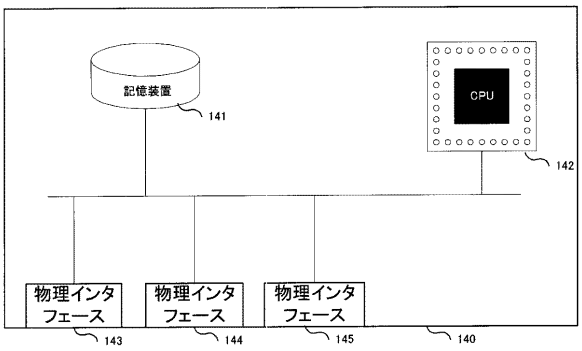
【図３】

図3



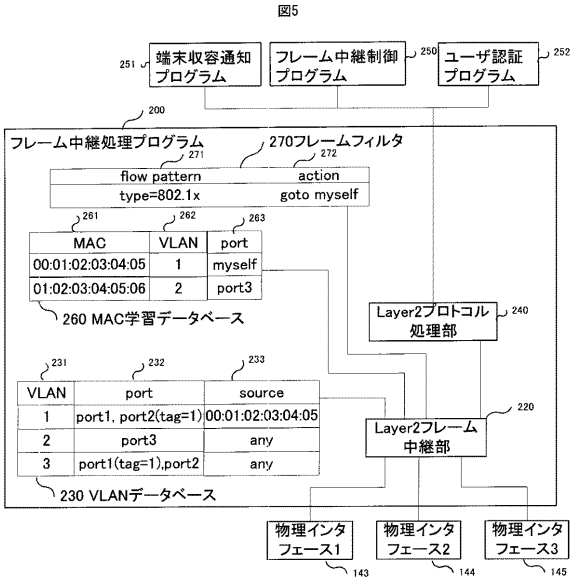
【図４】

図4



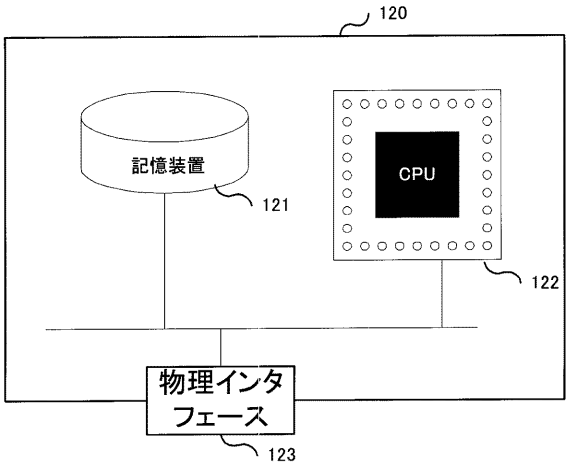
【図５】

図5



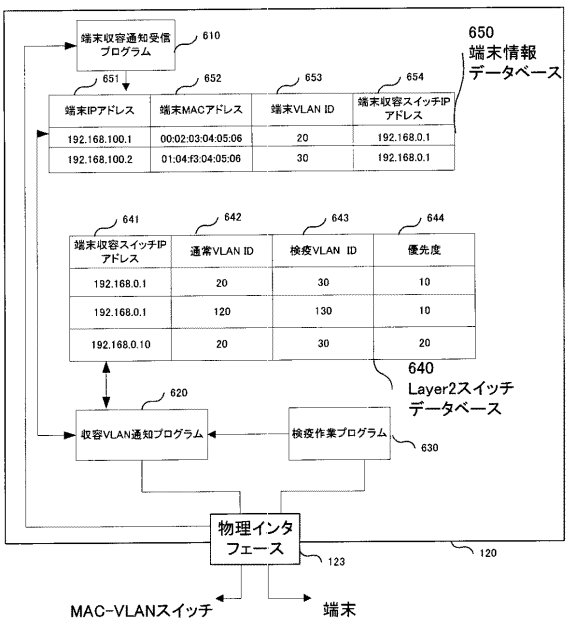
【図６】

図6



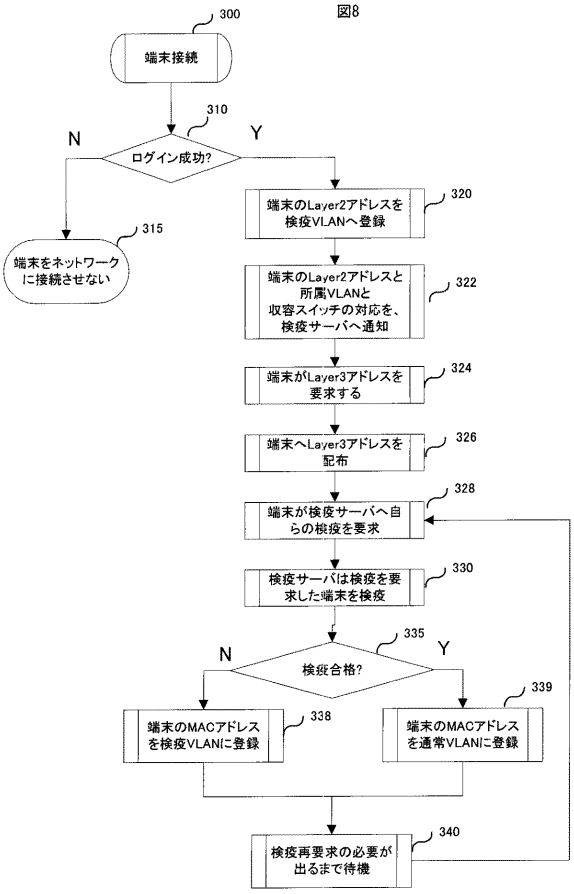
【図７】

図7



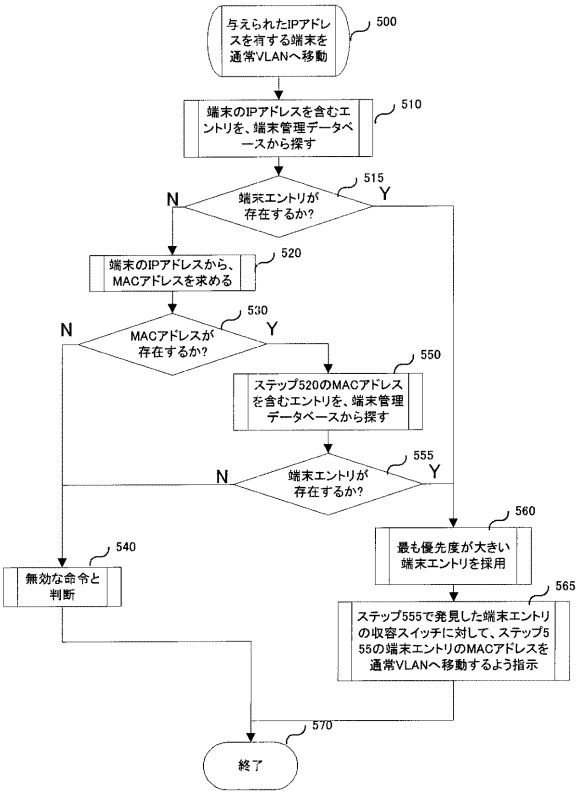
【図８】

図8



【図９】

図9



フロントページの続き

(72)発明者　宮部　隆夫
東京都品川区南大井六丁目２６番２号　アラクサラネットワークス株式会社内

合議体
審判長　石井　研一
審判官　矢島　伸一
審判官　神谷　健一

(56)参考文献　特開２００６－２５２２５６（ＪＰ，Ａ）
特開２００５－２５０７６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/28 - 12/46