(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5204054号
(P5204054)

(45)発行日　平成25年6月5日(2013.6.5)　(24)登録日　平成25年2月22日(2013.2.22)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/46	(2006.01)	H04L	12/46	E
G06F 21/44	(2013.01)	G06F	21/20	144C

請求項の数 4　(全 14 頁)

(21)出願番号　特願2009-173216 (P2009-173216)
(22)出願日　平成21年7月24日 (2009.7.24)
(65)公開番号　特開2011-29900 (P2011-29900A)
(43)公開日　平成23年2月10日 (2011.2.10)
審査請求日　平成24年2月9日 (2012.2.9)

(73)特許権者　000155469
株式会社野村総合研究所
東京都千代田区丸の内一丁目６番５号
(74)代理人　100105924
弁理士　森下　賢樹
(72)発明者　川上　明浩
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内

審査官　浦口　幸宏

最終頁に続く

(54)【発明の名称】ネットワーク管理システムおよび通信管理サーバ

(57)【特許請求の範囲】
【請求項１】
パケットを送受信する端末と、
複数の入出力ポートを有するパケット交換装置であって、いずれかの入出力ポートを介して受け取ったパケットを、別の入出力ポートを介して前記端末または他のパケット交換装置に送出するよう構成されたパケット交換装置と、
前記端末および前記パケット交換装置で構成されるネットワークにおいて、該ネットワークへの接続が許可されていない不正端末による通信を防止する通信管理サーバと、を含むネットワーク管理システムであって、
前記端末は、固有の識別情報としての端末エージェントＩＤが割り当てられておりパケット送信時に前記端末エージェントＩＤをパケットに付加する通信エージェントを備え、
前記パケット交換装置は、前記端末からパケットを受け取りパケットから前記端末エージェントＩＤを取得し、該端末エージェントＩＤに基づき前記端末がネットワークへの接続が許可された正規端末であるか否かを問い合わせる確認メッセージを前記通信管理サーバに送信する確認部を備え、
前記通信管理サーバは、
全ての正規端末が備える通信エージェントの端末エージェントＩＤを記録する通信エージェント情報保持部と、
前記確認メッセージに含まれる前記端末エージェントＩＤが前記通信エージェント情報保持部に記録されているか否かに基づき、前記端末が正規端末であるか不正端末である

かを通知する回答メッセージを前記パケット交換装置に返信する通信制御部と、
端末毎にパケットの送受信が許可される宛先端末の識別情報を記録したアクセス許可リストを保持する許可リスト管理部と、
前記アクセス許可リストを前記端末に配信する許可リスト配信部と、を備え、
前記パケット交換装置は、前記回答メッセージに応答して、前記端末が正規端末であるときは該端末が接続された入出力ポートを開放し、前記端末が不正端末であるときは該端末が接続された入出力ポートをロックするポートロック部をさらに備え、
前記端末の通信エージェントは、
前記通信管理サーバから受け取った前記アクセス許可リストを保持する許可リスト保持部と、
パケットの送信時に、該パケット内の前記宛先端末の識別情報が前記アクセス許可リストに含まれているか否かを判定し、含まれているときに前記パケットを送信するよう構成されたパケット送受信部と、をさらに備える
ことを特徴とするネットワーク管理システム。
【請求項２】
前記ネットワーク内で複数のパケット交換装置が階層的に接続されている場合、
少なくとも一つの階層にあるパケット交換装置は、固有の識別情報としての交換装置エージェントＩＤが割り当てられておりパケット送信時に前記交換装置エージェントＩＤをパケットに付加する通信エージェントをさらに備え、
前記通信エージェント情報保持部は、ネットワークへの接続が許可されたパケット交換装置が備える通信エージェントの前記交換装置エージェントＩＤを記録しており、
上位の階層のパケット交換装置は、前記少なくとも一つの階層のパケット交換装置からパケットを受け取ると、パケットから前記交換装置エージェントＩＤを取得し、該交換装置エージェントＩＤに基づき前記少なくとも一つの階層のパケット交換装置についてネットワークへの接続が許可されているか否かを問い合わせる確認メッセージを前記通信管理サーバに送信することを特徴とする請求項１に記載のネットワーク管理システム。
【請求項３】
前記許可リスト管理部は、パケットの送受信が許可される宛先端末が異なる複数のアクセス許可リストを保持しており、前記許可リスト配信部は、配信時刻に応じて選択されるアクセス許可リストを前記端末に配信することを特徴とする請求項２に記載のネットワーク管理システム。
【請求項４】
固有の識別情報としてのエージェントＩＤが割り当てられておりパケット送信時に前記エージェントＩＤをパケットに付加する通信エージェントを備える端末と、
一つ以上の入出力ポートを有し、いずれかの入出力ポートを介して受け取ったパケットを、別の入出力ポートを介して前記端末または他のパケット交換装置に送出するよう構成されたパケット交換装置であって、前記端末からパケットを受け取りパケットから前記エージェントＩＤを取得し、該エージェントＩＤに基づき前記端末がネットワークへの接続が許可された正規端末であるか否かを問い合わせる確認メッセージを発するパケット交換装置と、
を組み合わせてなるネットワークにおいて、該ネットワークへの接続が許可されていない不正端末による通信を防止する通信管理サーバであって、
全ての正規端末が備える通信エージェントのエージェントＩＤを記録する通信エージェント情報保持部と、
前記パケット交換装置からの前記確認メッセージに含まれる前記エージェントＩＤが前記通信エージェント情報保持部に記録されているか否かに基づき前記端末が正規端末であるか不正端末であるかを判定し、前記端末が正規端末であるときは該端末が接続された入出力ポートを開放させ、不正端末であるときは該端末が接続された入出力ポートをロックさせる回答メッセージを前記パケット交換装置に返信する通信制御部と、
端末毎にパケットの送受信が許可される宛先端末の識別情報を記録したアクセス許可リ

ストを保持する許可リスト管理部と、
前記アクセス許可リストを前記端末の通信エージェントに配信し、該端末からのパケットの送信時にパケット内の前記宛先端末の識別情報が前記アクセス許可リストに含まれているときに前記パケットを送信させる許可リスト配信部と、
を備えることを特徴とする通信管理サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ネットワークへの不正なアクセスを防止するネットワーク管理システムおよび装置に関する。
【背景技術】
【０００２】
企業内で使用されるＬＡＮ（Local Area Network）では、情報の漏洩を防止するために、許可されていない端末とのデータの送受信を禁止する必要がある。特許文献１には、スイッチングハブまたはルータなどのパケット交換装置の入出力ポートに装置が接続されたとき、その装置の認証を行い、許可を与えられていない計算機による不正なネットワーク使用を防止するパケット交換装置が開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００１－１８６１８６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
特許文献１に記載の技術では、交換装置毎に計算機の認証を行っている。このような構成の場合、ネットワーク規模が大きくなり交換装置の数が増大すると、認証のための設定を交換装置毎に実施しなくてはならないため、作業量が膨大になりまた交換装置の管理も困難になる。
【０００５】
本発明はこうした状況に鑑みてなされたものであり、その目的は、ネットワークの不正使用を集中して管理する通信管理サーバを設けたネットワーク管理技術を提供することである。
【課題を解決するための手段】
【０００６】
本発明のある態様は、ネットワーク管理システムである。このシステムは、パケットを送受信する端末と、複数の入出力ポートを有するパケット交換装置であって、いずれかの入出力ポートを介して受け取ったパケットを、別の入出力ポートを介して端末または他のパケット交換装置に送出するよう構成されたパケット交換装置と、端末およびパケット交換装置で構成されるネットワークにおいて、該ネットワークへの接続が許可されていない不正端末による通信を防止する通信管理サーバと、を含む。端末は、固有の識別情報が割り当てられ、パケット送信時に識別情報をパケットに付加する通信エージェントを備える。パケット交換装置は、端末からパケットを受け取りパケットから通信エージェントの識別情報を取得し、該識別情報に基づき端末がネットワークへの接続が許可された正規端末であるか否かを問い合わせる確認メッセージを通信管理サーバに送信する確認部を備える。通信管理サーバは、全ての正規端末が備える通信エージェントの識別情報を記録する通信エージェント情報保持部と、確認メッセージに応答して、識別情報が通信エージェント情報保持部に記録されているか否かに基づき、端末が正規端末であるか不正端末であるかを通知する回答メッセージをパケット交換装置に返信する通信制御部と、を備える。パケット交換装置は、回答メッセージに応答して、端末が正規端末であるときは該端末が接続された入出力ポートを開放し、端末が不正端末であるときは該端末が接続された入出力ポ

ートをロックするポートロック部をさらに備える。

【０００７】

ここで、パケットとは、例えばＩＰパケットやＭＡＣフレームなどの宛先アドレス等の制御情報を付加されたデータ単位のことをいう。また、パケット交換装置は、ルータ、レイヤ３スイッチ、スイッチングハブ等を含む。

この態様によると、ネットワークへの接続が許可された正規端末の通信エージェントの識別情報が通信管理サーバで集中管理され、パケット交換装置に接続された端末が正規端末であるか不正端末であるかの判定を行う。したがって、正規端末間のみでパケットの送受信が可能になるとともに、ネットワーク構成の変更を行った場合でも、個別のパケット交換装置の設定を変更する必要がなく、ネットワーク全体の不正アクセスの管理が容易になる。

【０００８】

通信管理サーバは、端末毎にパケットの送受信が許可される宛先端末の識別情報を記録したアクセス許可リストを保持する許可リスト管理部と、アクセス許可リストを端末に配信する許可リスト配信部と、をさらに備えてもよい。端末の通信エージェントは、通信管理サーバから受け取ったアクセス許可リストを保持する許可リスト保持部と、パケットの送信時に、該パケットの宛先端末の識別情報がアクセス許可リストに含まれているか否かを判定し、含まれているときにパケットを送信するよう構成されたパケット送受信部と、をさらに備えてもよい。これによると、端末間でのパケットの送受信を制限できるとともに、アクセス許可リストが通信管理サーバで集中管理されているため、リストが端末毎に管理されている場合に比べてネットワーク全体のアクセス制御の管理が容易になる。

【０００９】

ネットワーク内で複数のパケット交換装置が階層的に接続されている場合、少なくとも一つの階層にあるパケット交換装置は、固有の識別情報が割り当てられ、パケット送信時に識別情報をパケットに付加する通信エージェントをさらに備えてもよい。通信エージェント情報保持部は、ネットワークへの接続が許可されたパケット交換装置が備える通信エージェントの識別情報を記録しており、上位の階層のパケット交換装置は、少なくとも一つの階層のパケット交換装置からパケットを受け取ると、パケットから通信エージェントの識別情報を取得し、該識別情報に基づき少なくとも一つの階層のパケット交換装置についてネットワークへの接続が許可されているか否かを問い合わせる確認メッセージを通信管理サーバに送信してもよい。これによると、上位階層のパケット交換装置が、下位階層のパケット交換装置が正規のものであるかを通信管理サーバに対して問い合わせる。したがって、通信管理サーバに対して正規端末か否かの確認を依頼する機能を有さないパケット交換装置を利用した不正アクセス行為を防止できる。

【００１０】

許可リスト管理部は、パケットの送受信が許可される宛先端末が異なる複数のアクセス許可リストを保持しており、許可リスト配信部は、配信時刻に応じて選択されるアクセス許可リストを端末に配信してもよい。これによると、時間帯別で異なるアクセス制御を実現できる。

【００１１】

本発明の別の態様は、通信管理サーバである。この通信管理サーバは、固有の識別情報が割り当てられ、パケット送信時に識別情報をパケットに付加する通信エージェントを備える端末と、一つ以上の入出力ポートを有し、いずれかの入出力ポートを介して受け取ったパケットを、別の入出力ポートを介して端末または他のパケット交換装置に送出するよう構成されたパケット交換装置であって、端末からパケットを受け取りパケットから通信エージェントの識別情報を取得し、該識別情報に基づき端末がネットワークへの接続が許可された正規端末であるか否かを問い合わせる確認メッセージを発するパケット交換装置と、を組み合わせてなるネットワークにおいて、該ネットワークへの接続が許可されていない不正端末による通信を防止するサーバである。サーバは、全ての正規端末が備える通信エージェントの識別情報を記録する通信エージェント情報保持部と、パケット交換装置

からの確認メッセージに応答して、識別情報が通信エージェント情報保持部に記録されているか否かに基づき端末が正規端末であるか不正端末であるかを判定し、端末が正規端末であるときは該端末が接続された入出力ポートを開放させ、不正端末であるときは該端末が接続された入出力ポートをロックさせる回答メッセージをパケット交換装置に返信する通信制御部と、を備える。

【００１２】

なお、以上の構成要素の任意の組合せ、本発明の表現を装置、方法、システム、プログラム、プログラムを格納した記録媒体などの間で変換したものもまた、本発明の態様として有効である。

【発明の効果】

【００１３】

本発明によれば、ネットワークの不正使用を集中して管理する通信管理サーバを設けることで、不正使用を防止するための設定が容易になる。

【図面の簡単な説明】

【００１４】

【図１】一般的なネットワークの全体構成図である。

【図２】本発明の一実施形態による通信管理サーバを加えたネットワークを示す図である。

【図３】通信管理サーバの詳細な構成を説明する図である。

【図４】エッジスイッチの構成を示す図である。

【図５】端末に導入される通信エージェントの構成を示す図である。

【図６】本実施形態による不正端末の検出について説明するフローチャートである。

【図７】正規端末と不正端末を入れ替えたときの動作を説明するフローチャートである。

【発明を実施するための形態】

【００１５】

本発明の一実施形態は、企業内ＬＡＮ等のネットワークにおいて、接続が許可されていない端末がネットワークに接続されることによる情報漏洩を防止するネットワーク管理システムである。

【００１６】

図１は、一般的な企業内ネットワークシステムの全体構成図である。ネットワークシステム１００は、基本的に、コアスイッチ、中継スイッチ、エッジスイッチの三種類のスイッチからなる三層構造をなしている。このうち、コアスイッチ１４は、バックボーン・ネットワークを構成する最上位のスイッチである。コアスイッチ１４は、エッジスイッチ８４～８８から送出されたパケットを他のコアスイッチ１４に中継し、宛先のエッジスイッチまで転送する。エッジスイッチ８４～８８は、ネットワークの終端部に存在し、ＬＡＮケーブル等を用いて端末２６、２８が接続されるスイッチである。中継スイッチ１６は、コアスイッチ１４とエッジスイッチ８４～８８とを結びつける役割を有するスイッチである。図１では一層のみの中継スイッチ１６が描かれているが、ネットワークの規模に応じて中継スイッチを二層、三層と多層的に構成してもよいし、ネットワーク規模が小さい場合には中継スイッチを省いてもよい。

【００１７】

コアスイッチ１４、中継スイッチ１６、およびエッジスイッチ８４～８８は、典型的には複数の入出力ポートを備えるＥｔｈｅｒｎｅｔ（登録商標）スイッチングハブであるが、ルータまたはレイヤ３スイッチであってもよい。

なお、上記ではコアスイッチ、中継スイッチ、エッジスイッチをそれぞれ別個のものとして説明したが、ネットワークの規模やネットワーク要件に応じて、これらの一部が同一の機器であってもよい。

【００１８】

端末２６、２８は、ネットワークインタフェースカード（ＮＩＣ）を介してエッジスイッチ８４、８６のいずれかの入出力ポートに接続される。本明細書において「端末」とは

、デスクトップ型またはノートブック型のパーソナルコンピュータ、ラックマウント型サーバ、ブレードサーバなどを含む。

【００１９】

以下、図１のネットワークにおいて、端末Ａから別の端末Ｂへとパケットを送信する場合について説明する。

端末Ａ２６に接続されたエッジスイッチＡ８４は、端末ＡからＭＡＣ（Media Access Control）フレームやＩＰ（Internet Protocol）パケットなどのパケットを入出力ポートを介して受信すると、ヘッダに含まれる宛先アドレスを取得する。続いて、予め準備された宛先アドレスと入出力ポートとの対応が記載されたルーティングテーブルを参照して、その宛先アドレスを有する通信機器（各種スイッチまたは端末）が接続されているか、あるいはその宛先アドレスに到達可能な入出力ポートを選択する。そして、エッジスイッチＡは、選択した出力ポートにパケットを送出し、パケットはその入出力ポートに接続された中継スイッチまたは端末に送信される。中継スイッチにパケットが送信された場合は、中継スイッチが上記と同様にしてパケットを転送する入出力ポートを選択する。この処理によって、パケットは端末Ｂ２８側のエッジスイッチＢ８６に到達し、このエッジスイッチＢが受信したパケットを端末Ｂに出力する。このようなスイッチ間でのパケットの転送は周知技術であるから、本明細書ではこれ以上詳細な説明を省略する。

【００２０】

従来、図１のようなネットワークにおいて、接続が許可されていない端末のネットワーク接続を防止するためには、コアスイッチ、中継スイッチおよびエッジスイッチの各スイッチにおいて空きポートをソフトウェア的にまたはハードウェア的にブロックするといった対策が必要であった。また、各端末からのアクセス先を制限するためには、各スイッチにおいてアクセスが許可される宛先端末の識別情報を設定しておく必要であった。

【００２１】

しかしながら、上記のようにスイッチ毎にポートのブロックやアクセス先制限を設定する仕組みを取ると、ネットワークが大規模になりスイッチ数が増大すると、各スイッチで設定を行う作業が非常に煩雑になるという問題がある。また、スイッチの階層構造が複雑になりネットワーク全体の把握が困難になるので、アクセス制限の設定ミスが起こりやすくなり、想定通りの挙動が得られなくなる場合がある。さらに、スイッチ数が増えるほどアクセス制限に要する処理量が増大し、本来のルーティング機能が低下するおそれがある。

【００２２】

そこで、本実施形態では、ネットワークに接続される各端末に通信エージェントを導入し、これら通信エージェントに関する情報を通信管理サーバで一括して管理するようにした。さらに、端末が接続された入出力ポートを開放するか否かの判定を、通信管理サーバで実施することにした。

【００２３】

図２は、本発明の一実施形態による通信管理サーバを備えたネットワークシステム１００’を示す。通信管理サーバ１０は、ネットワーク内のいずれかのコアスイッチ１４に接続され、ネットワーク内での不正端末の検出および端末間のアクセス制御を実行する。通信管理サーバ１０は、プログラムにしたがって各種処理を実行するプロセッサと、一時的にデータやプログラムを記憶するメモリと、サーバの再起動があっても記録内容が失われないハードディスクドライブ、ＤＶＤドライブなどの記憶装置と、ネットワークに接続し各種の入出力処理を実行するネットワークインタフェースと、これらを相互接続するバスを少なくとも備える。なお、通信管理サーバ１０は、帯域が広い部分に接続されることが好ましいので、コアスイッチに接続されるのが最適であるが、エッジスイッチと通信が可能であればネットワーク内の任意の箇所にあってよい。

【００２４】

本実施形態では、ネットワークへの接続が許可される端末２８、ファイルサーバ２２およびメールサーバ２４には、通信エージェント９０が導入される。この通信エージェント

９０は、好適にはソフトウェアにより提供される機能であり、端末上で常時起動されている。通信エージェントは、端末で送受信される全てのパケットが必ず通信エージェントを通じて送受信されるように機能する。各端末の通信エージェント９０には固有の識別情報としてのエージェントＩＤが付与されている。ネットワークへの接続が許可される端末のエージェントＩＤは、通信管理サーバ１０に記録される。以下、通信エージェントが導入済みであり、かつエージェントＩＤが通信管理サーバに記録された端末を「正規端末」と呼び、それ以外の端末を「不正端末」と呼ぶ。以下では、端末Ａ２６を「不正端末」として、端末Ｂ２８、ファイルサーバ２２およびメールサーバ２４を「正規端末」として説明する。

【００２５】

通信エージェント機能をソフトウェアで提供することで、ネットワークへの接続が必要な任意の端末に、通信エージェントソフトウェアが記録されたＣＤ、ＤＶＤ等の任意の記録媒体を通じて、またはネットワーク配信によって、通信エージェントソフトウェアをインストールすることができる。代替的に、通信エージェント機能を有するハードウェアが予め組み込まれた端末を使用してもよいし、またはハードウェアとソフトウェアの組合せで通信エージェント機能を提供してもよい。

【００２６】

本実施形態のエッジスイッチ４４～４８は、入出力ポートを開放またはロックするポート制御部を備える。エッジスイッチ４４～４８のポート制御部は、自身のいずれかの入出力ポートに端末２８が接続されると、その端末のＩＰアドレス、ＭＡＣアドレス、またはエージェントＩＤなどの端末情報を取得する。そして、この端末が、ネットワークへの接続が許可された正規端末であるか否かを通信管理サーバ１０に確認する。

【００２７】

通信管理サーバ１０は、端末間のアクセス制御を管理するとともに、通信エージェントがインストールされていない端末（以下、「不正端末」という）がネットワークを介してデータを送受信することを防止する。通信管理サーバ１０は、エッジスイッチからの問い合わせに応じて端末が正規のものであるか否かを確認し、その結果をエッジスイッチに返す。正規端末でない場合、エッジスイッチ４４～４６は、その端末が接続された入出力ポートをロックして、ネットワークとの間でのデータの送受信を防止する。

【００２８】

図３は、通信管理サーバ１０の詳細な構成を説明する図である。これらの構成は、ハードウェア的には、任意のコンピュータのＣＰＵ、メモリ、その他のＬＳＩで実現でき、ソフトウェア的にはメモリにロードされたプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。

【００２９】

通信管理サーバは、送受信部４０、通信制御部４２、リスト転送部３８および通信管理マスタ部５０を含む。

送受信部４０は、接続された端末が正規端末であるか否かの確認メッセージをエッジスイッチ４４～４６から受け取り、またその確認結果を回答メッセージとしてエッジスイッチ４４～４６に返信する。通信制御部４２は、通信管理マスタ部５０内の情報を参照して、端末が正規端末であるか否かを確認する。

【００３０】

通信管理マスタ部５０は、通信エージェント情報保持部５２、許可リスト管理部５４、端末情報保持部５６を含む。

通信エージェント情報保持部５２は、ネットワーク内の接続が許可された正規端末で動作する通信エージェントのエージェントＩＤを保持する。ネットワークの管理者は、端末に新たに通信エージェントをインストールした場合には、その通信エージェントのエージェントＩＤを情報保持部５２に登録する。

許可リスト管理部５４は、正規端末毎に、データの送受信が許可される宛先端末の識別情報が記録されたアクセス許可リストを保持する。アクセス許可リストに記録される識別情報は、宛先端末のＮＩＣに割り振られているＩＰアドレス、ＭＡＣアドレス、またはエージェントＩＤの少なくとも一つである。識別情報として、ポート情報も含めたＴＣＰ／ＩＰアドレス、ＶＬＡＮ情報を用いてもよい。このアクセス許可リストは各端末の通信エージェントに送信され、アクセスの可否を判定するために使用される。このアクセス許可リストによって、例えば端末Ｂ２８について、メールサーバ２４とのデータ送受信は許可するがファイルサーバ２２とのデータ送受信は拒否するといったアクセス制御を実現することができる。

端末情報保持部５６は、通信管理サーバ１０の管理対象となる端末および各スイッチの識別情報、例えばＩＰアドレスまたはＭＡＣアドレスが記録される。

【００３１】

リスト転送部３８は、所定のタイミング、正規端末２８からのリクエスト時、またはアクセス許可リストの更新時に、最新のアクセス許可リストを端末２８に送信する。

【００３２】

図４は、エッジスイッチ４４～４８の構成を示す図である。図４でも、これらの構成は、ハードウェア的には、任意のコンピュータのＣＰＵ、メモリ、その他のＬＳＩで実現でき、ソフトウェア的にはメモリにロードされたプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。

【００３３】

エッジスイッチは、通信部６０、ポート制御部７０、パケット処理部８２を含む。

通信部６０は、端末または他のスイッチなどの通信機器との間でパケットの送受信を行うために通信ケーブルと接続される一つ以上の入出力ポート６２を備える。

ポート制御部７０は、確認部７２とポートロック部７４を含む。確認部７２は、入出力ポートを介してエッジスイッチと他の通信機器とが接続され通電したときに、いずれのポートに通信機器が接続されたかを認識することができるよう構成される。そして、接続された端末が正規端末であるか否かの確認メッセージを通信管理サーバ１０に送信する。ポートロック部７４は、通信管理サーバ１０から回答メッセージを受け取り、正規端末であるか不正端末であるかに応じて、端末の接続された入出力ポートを開放するか、またはロックする。

【００３４】

パケット処理部８２は、入出力ポートと宛先アドレスの対応関係が記載されたルーティングテーブルを有しており、周知のルーティング技術にしたがって、入出力ポートを介して受け取ったパケットを送出する入出力ポートを決定し、他の通信機器との間でパケットを交換する。

【００３５】

図５は、正規端末、すなわち端末２８およびサーバ２２、２４に導入される通信エージェント９０の構成を示す図である。上述のように、本実施形態では、ネットワークに接続される端末には通信エージェントがインストールされ、通信エージェントを経由してのみ他の端末との通信が可能になる。

通信エージェント９０は、パケット送受信部９２、許可リスト受信部９４、および許可リスト保持部９６を含む。許可リスト受信部９４は、通信管理サーバ１０から自身の端末に突いてのアクセス許可リストを受け取り、許可リスト保持部９６に記憶させる。許可リスト受信部９４は、通信管理サーバ１０が所定のタイミングで送信する最新のアクセス許可リストを受け取るようにしてもよいし、許可リスト受信部９４が所定のタイミングで最新のリストを要求してもよい。アクセス許可リストの全体が更新されてもよいし、前回との差分のみが更新されてもよい。代替的に、許可リスト受信部９４は、他の端末と通信するたびにアクセス許可リストの更新の有無を通信管理サーバ１０に問い合わせてもよい。

【００３６】

このように、本実施形態ではアクセス許可リストを通信管理サーバで集中管理するので

、アクセス許可リストが端末毎に管理されている場合に比べて、ネットワークの構成変更等に伴う宛先端末変更の作業が容易になる。

【００３７】

パケット送受信部９２は、他の端末との間でのパケットの送受信を制御する。パケット送受信部９２は、パケットを送信する際に、パケットのヘッダに記載された宛先端末の識別情報を参照する。そして、宛先端末の識別情報がアクセス許可リストに含まれる場合にはそのパケットを送信し、含まれない場合にはパケットを送信しない。また、パケット送受信部９２は、パケットを送信する際に、エージェントＩＤをパケットのヘッダに追加する。別法として、エージェントＩＤをパケットのボディに追加してもよい。

【００３８】

図６は、本実施形態によるネットワークに接続された不正端末の検出について説明するフローチャートである。

【００３９】

まず、ネットワーク管理者は、接続を許可する端末に通信エージェントを導入したときに、通信管理サーバ１０内の通信エージェント情報保持部５２にエージェントＩＤを記録しておく。また、その端末の識別情報を端末情報保持部５６に記録しておく。

【００４０】

ある端末がエッジスイッチ４０～４８のいずれかの入出力ポートに接続され、不正端末からパケットの送信が試みられるとする。エッジスイッチは、不正端末が入出力ポートに接続されると（Ｓ１０）、通信管理サーバ１０に対し、接続された端末が正規端末であるか否かを確認する確認メッセージを送信する（Ｓ１２）。この確認メッセージには、端末のエージェントＩＤが含まれる。

【００４１】

通信管理サーバ１０は、確認メッセージを受け取ると、通信エージェント情報保持部５２を参照して、エージェントＩＤが記録されているか否かに基づき、端末が正規端末であるか不正端末であるかを判定する（Ｓ１４）。そして、正規端末であるか不正端末であるかを記載した回答メッセージとしてエッジスイッチに送信する（Ｓ１６）。エッジスイッチは、正規端末と確認された場合、端末が接続された入出力ポートを開放する（Ｓ１８）。これによって、端末はパケットの送受信が可能になる。不正端末と確認された場合、エッジスイッチは端末が接続された入出力ポートをロックする（Ｓ１８）。これによって、許可されていない不正端末とのパケットの送受信が不可能になる。

【００４２】

このように、エッジスイッチは自身の入出力ポートを監視し、不正端末であることが通信管理サーバにより確認されると、その端末が接続された入出力ポートをロックする。したがって、不正端末への情報漏洩が防止され、または不正端末からのパケット送信によるトラフィックの占有が回避される。

また、本実施形態では、コアスイッチ、中間スイッチ、エッジスイッチにおいては端末が正規端末であるか不正端末であるかの判定を行わず、通信管理サーバに任せている。したがって、スイッチ毎に上記判定を行わせるための設定をする必要がなくなり、ネットワークの管理も容易になる。

【００４３】

上述の実施形態では、エッジスイッチは、端末からパケットを受け取る毎に通信管理サーバに対して確認メッセージを送信する。しかしながら、このようにすると、エッジスイッチと通信管理サーバ間でのパケットの送受信量が増大し、トラフィックが混雑する上にスイッチの処理速度も低下する。そこで、エッジスイッチは、一旦正規端末であると確認された端末からパケットを受け取った場合、確認メッセージを発することなく転送することが好ましい。正規端末であると確認されてから所定の期間だけ、その端末からのパケットを転送するようにしてもよい。

【００４４】

エッジスイッチに端末を接続し、通信管理サーバによってその端末が正規端末として確

認された後、その端末を不正端末に入れ替えてネットワーク接続を試みるという不正行為が考えられる。この対策として、エッジスイッチは、入出力ポートへのケーブルの抜き差しがあった場合は常に、その端末からのパケット送信が通信エージェント経由でなされているか否かを確認する機能を備えていてもよい。通信エージェント経由でない場合、エッジスイッチは、その端末の接続されたポートをロックする。これによって、不正端末から通信を行うことが不可能になる。例えば、端末の通信エージェントが、パケットを送信するときに通信エージェントを経由したことを示す情報をヘッダに書き込むようにしておけば、エッジスイッチはパケット送信が通信エージェント経由であるか否かを判定することができる。エッジスイッチは、いずれかの入出力ポートをロックした場合、そのポートに接続された端末の識別情報を通信管理サーバに通知してもよい。

【００４５】

また、例えば違法コピーなどによって入手した通信エージェントをインストールした端末（「違法コピー端末」という）を、正規端末と入れ替えて接続を試みるという不正行為も考えられる。この対策として、エッジスイッチは、入出力ポートへのケーブルの抜き差しがあった場合には、そのポートに接続された端末が正規端末であるか否かの確認をするように構成されてもよい。

【００４６】

図７は、正規端末と違法コピー端末を入れ替えたときの動作を説明するフローチャートである。

ユーザは、以前に正規端末と確認された端末を、不正に入手した通信エージェントがインストールされた違法コピー端末と入れ替え（Ｓ３０）、エッジスイッチの入出力ポートとをケーブルで接続する（Ｓ３２）。エッジスイッチは、入出力ポートへの接続がなされたことを認識し、通信管理サーバ１０に対し、接続された端末が正規端末であるか否かを確認する確認メッセージを送信する（Ｓ３４）。

【００４７】

通信管理サーバ１０は、確認メッセージを受け取ると、通信エージェント情報保持部５２を参照して、エージェントＩＤが記録されているか否かに基づき、端末が正規端末であるか不正端末であるかを判定する（Ｓ３６）。この場合、端末の通信エージェントは不正に入手されたものなので、通信エージェント情報保持部５２には記録されていない。したがって、通信管理サーバ１０は、端末が不正端末である旨を記載した回答メッセージをエッジスイッチに送信する（Ｓ３８）。回答メッセージに応じて、エッジスイッチは違法コピー端末が接続された入出力ポートをロックする（Ｓ４０）。これによって、違法コピー端末からのパケットの送受信が不可能になる。

【００４８】

さらに、正規端末と確認された端末をそのままエッジスイッチに接続しておき、正規端末の別のポートに不正端末をつないで、正規端末の通信エージェントを経由してネットワークへのアクセスを試みる不正行為も考えられる。この対策として、端末上で動作する通信エージェントは、エッジスイッチを経由しないパケット送信を受け取った場合、そのパケットが正規端末の通信エージェントを経由して送信されたか否かを、パケットのヘッダに記録された情報から判断してもよい。通信エージェント経由でない場合、そのパケットの転送を拒否してもよいし、エッジスイッチに対してその旨を報告してもよい。エッジスイッチは、報告のあった端末が接続された入出力ポートをロックするようにしてもよい。

このように、端末上の通信エージェントにもパケットが正規端末から送信されたか否かの否かの判定をさせることで、正規端末を間にかませた不正アクセスを防止することができる。

【００４９】

また、既存のエッジスイッチと入れ替えて、通信管理サーバに対して正規端末か否かの確認を依頼する機能を有さないエッジスイッチ（以下、「不正エッジスイッチ」という）を利用する不正行為も考えられる。この場合、不正エッジスイッチに不正端末を接続しても、正規端末か否かの確認がなされないまま不正端末によるデータの送受信が可能になっ

てしまう。

【００５０】

そこで、別の実施形態では、エッジスイッチにも通信エージェントを導入し、エッジスイッチで転送される全てのパケットが通信エージェントを経由してなされるように構成してもよい。この場合、エッジスイッチの通信エージェントのＩＤを、通信エージェント情報保持部５２に記録しておく。この場合、エッジスイッチの上位の中継スイッチまたはコアスイッチに、下位のエッジスイッチからパケットを受け取ったとき、そのエッジスイッチが正規のものであるか否かを通信管理サーバに確認する確認部と、エッジスイッチが不正であると確認された場合、その不正エッジスイッチが接続された入出力ポートをロックするポートロック部とを設けておく。これにより、不正エッジスイッチを経由させた不正端末からのデータ送受信が不可能になる。

【００５１】

以上説明したように、本実施形態によれば、接続が許可され通信エージェントを導入した全ての端末について、エージェントＩＤを通信管理サーバで集中管理する。エッジスイッチは、端末に通信エージェントが導入されているか否かによらず、通信管理サーバに正規端末であるか否かの問い合わせをする。これにより、エージェントが導入されかつ通信管理サーバに登録された端末間のみで通信が可能になる。

また、スイッチ間の接続変更等のネットワーク構成の変更を行った場合でも、個別のスイッチの設定を変更する必要がなく、通信管理サーバ内のエージェントＩＤのみ変更すればよい。したがって、ネットワーク全体の不正アクセスの管理が容易になる。

【００５２】

一般的に、スイッチに書き込めるアクセス制御に関する情報量は限られているので、ネットワークが大規模になり各スイッチに接続される通信機器数が増加すると、詳細なアクセス制御内容をスイッチに書き込めなくなるおそれがある。また、アクセス制御の内容が複雑になるほど、スイッチでの処理量も増大し、本来のルーティング性能が低下するおそれがある。本実施形態では、端末毎のアクセス許可リストを通信管理サーバで集中管理するようにしたので、スイッチのルーティング性能の低下を抑制することができる。また、スイッチのベンダーによってアクセス制御の設定方法が異なることがあるが、通信管理サーバでアクセス許可リストを一括管理していれば、そのようなスイッチ毎の相違点を考慮する必要がなくなる。さらに、アクセス許可リストを一括管理しているため、大規模のネットワークでも端末間でのきめの細かいアクセス制御の設定が容易になる。

【００５３】

上述の実施形態では、ネットワークに対して単一の通信管理サーバを設けたが、ネットワークまたはトラフィックの規模に応じて通信管理サーバを階層構成にしてもよい。この場合、通信管理サーバをコアスイッチ毎にまたは中継スイッチ毎に設け、各通信管理サーバはサブネット内のエッジスイッチからの確認メッセージに回答するようにしてもよい。これによって、通信管理サーバの負荷を軽減することができる。

【００５４】

上述の実施形態では、エッジスイッチは、接続された端末が正規端末であるか否かを通信管理サーバに確認することを述べた。しかしながら、エッジスイッチ自身で正規端末であるか否かを確認してもよい。この場合、通信管理サーバの通信エージェント情報保持部は、所定のタイミングで、またはエッジスイッチの確認部からのリクエスト時に、登録済みのエージェントＩＤのリストをエッジスイッチに送信する。エッジスイッチの確認部は、このリストに基づき正規端末であるか否かを判定する。

【００５５】

上述の実施形態では、端末をエッジスイッチの入出力ポートに接続したとき、正規端末であるか否かの確認を通信管理サーバに対して行うことを述べた。しかしながら、エッジスイッチは、入出力ポートに接続されている全ての端末について、正規端末であるか否かの確認を定期的に実施してもよいし、ネットワークの管理者により随時実行されてもよい。

【００５６】

管理サーバの許可リスト管理部は、アクセス制御の設定が異なる複数のアクセス許可リストを保持しておき、時刻または時間帯に応じたアクセス許可リストを選択して端末の通信エージェントに送信するように構成されていてもよい。例えば、企業の営業時間中と営業時間外とで異なるアクセス許可リストを許可リスト管理部に準備しておき、管理サーバは、時間帯に応じたリストを選択して端末に送信するようにしてもよい。こうすると、例えば営業時間中には業務に必要な様々な通信機器に全ての端末が接続できるが、営業時間外には一部の端末のみ接続を許可したりすることができる。代替的に、アクセス制御の設定が異なる複数のアクセス許可リストを予め管理サーバから各端末の通信エージェントに送信しておき、通信エージェントが時刻に応じたアクセス許可リストを選択するように構成してもよい。

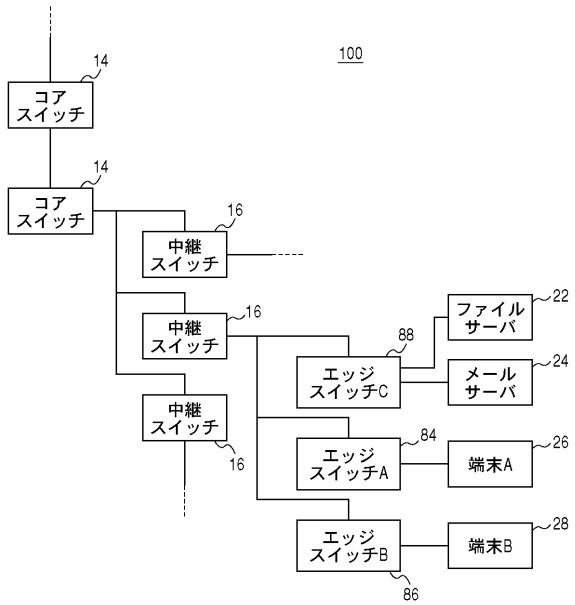
さらに、アクセス許可リストに有効期限を設けておいてもよい。各端末は、許可リスト保持部内のアクセス許可リストの有効期限が切れると、通信管理サーバに対して新たなリストを要求するように構成してもよい。

【符号の説明】

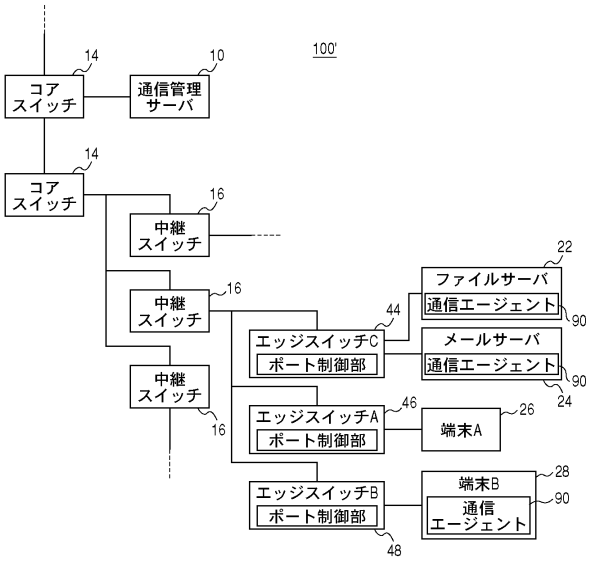
【００５７】

１０　通信管理サーバ、　１４　コアスイッチ、　１６　中継スイッチ、　２８　端末、　３８　リスト転送部、　４２　通信制御部、　４４～４８　エッジスイッチ、　５０　通信管理マスタ部、　５２　通信エージェント情報保持部、　５４　許可リスト管理部、　５６　端末情報保持部、　６０　通信部、　６２　入出力ポート、　７０　ポート制御部、　７２　確認部、　７４　ポートロック部、　８２　パケット処理部、　９０　通信エージェント、　９２　パケット送受信部、　９４　許可リスト受信部、　９６　許可リスト保持部。

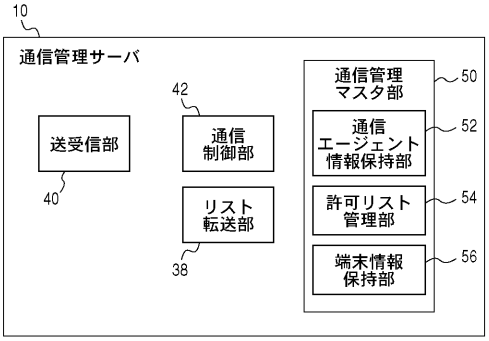
【図１】



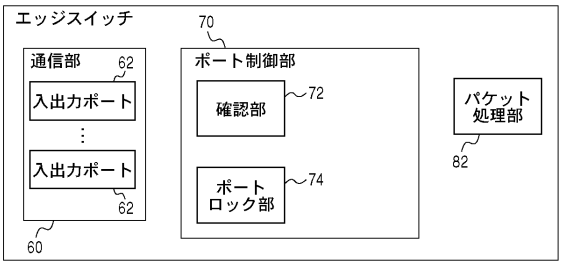
【図２】



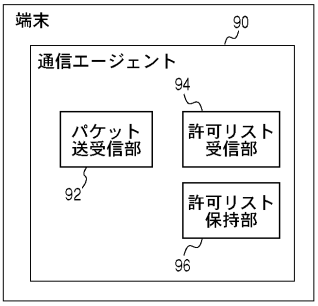
【図３】


10
通信管理サーバ
送受信部
40
42
通信制御部
リスト転送部
38
通信管理マスタ部
50
通信エージェント情報保持部
52
許可リスト管理部
54
端末情報保持部
56

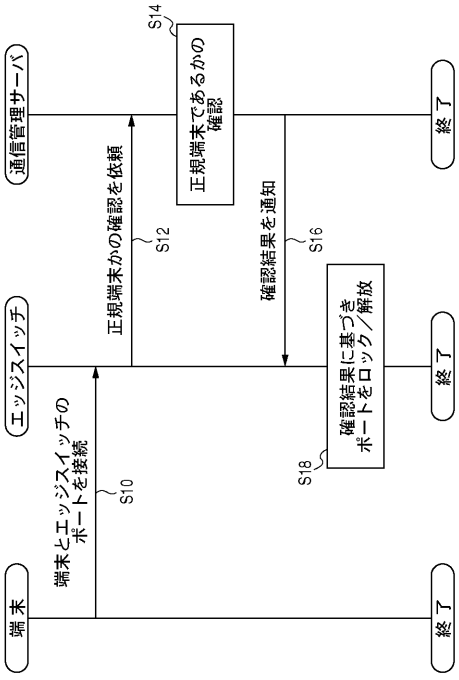
【図４】


エッジスイッチ
通信部
62
入出力ポート
入出力ポート
62
60
70
ポート制御部
確認部
72
ポートロック部
74
パケット処理部
82

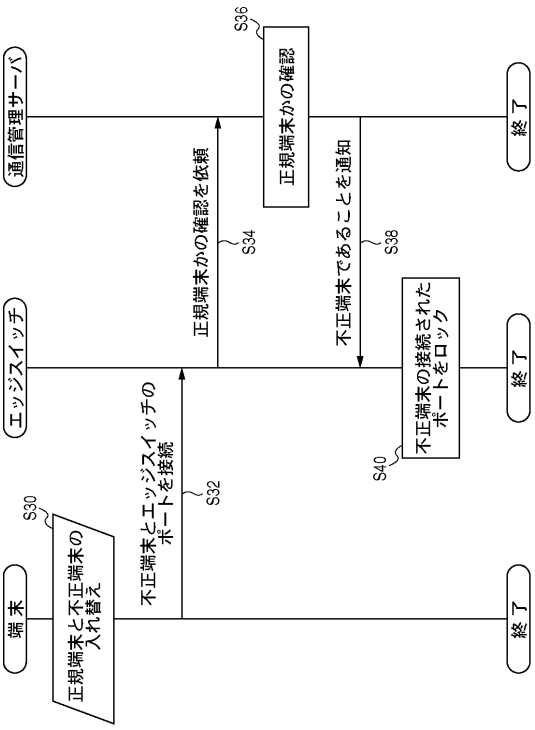
【図５】


端末
90
通信エージェント
94
パケット送受信部
92
許可リスト受信部
許可リスト保持部
96

【図６】


通信管理サーバ
エッジスイッチ
端末
端末とエッジスイッチのポートを接続
S10
正規端末かの確認を依頼
S12
S14
正規端末であるかの確認
確認結果を通知
S16
確認結果に基づきポートをロック／解放
S18
終了
終了
終了

【図７】


通信管理サーバ
エッジスイッチ
端末
S30
正規端末と不正端末の入れ替え
不正端末とエッジスイッチのポートを接続
S32
正規端末かの確認を依頼
S34
S36
正規端末かの確認
不正端末であることを通知
S38
不正端末の接続されたポートをロック
S40
終了
終了
終了

フロントページの続き

(56)参考文献 特開２００８－２７６６８６（ＪＰ，Ａ）
特開平１１－２１２９３３（ＪＰ，Ａ）
特開２００４－２４８２２２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １３／００
Ｇ０６Ｆ ２１／００
Ｇ０６Ｆ ２１／２０
Ｈ０４Ｌ １２／００－１２／２８
Ｈ０４Ｌ １２／４４－１２／９５５