(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-352719
(P2006-352719A)
(43)公開日　平成18年12月28日(2006.12.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/40	(2006.01)	H04L	12/40	M	5B089
H04L 12/66	(2006.01)	H04L	12/66	B	5K030
H04L 12/46	(2006.01)	H04L	12/46	M	5K032
G06F 13/00	(2006.01)	G06F	13/00	351N	5K033

審査請求 未請求　請求項の数 13　ＯＬ　（全 14 頁）

(21)出願番号　特願2005-178697 (P2005-178697)
(22)出願日　平成17年6月20日 (2005.6.20)

（特許庁注：以下のものは登録商標）
１．イーサネット

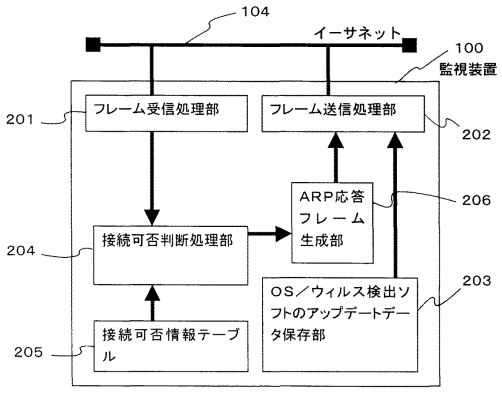
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(71)出願人　000153443
株式会社日立情報制御ソリューションズ
茨城県日立市大みか町５丁目２番１号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　吉川　秀之
茨城県日立市大みか町五丁目２番１号
株式会社日立製作所
情報制御システム事業部内

最終頁に続く

(54)【発明の名称】ネットワーク監視装置，ネットワーク監視方法，ネットワークシステム及びネットワーク監視方法及びネットワーク通信方法

(57)【要約】
【課題】
従来、検疫ネットワークを実現するためには、これに応じた機能を有する専用のスイッチングハブなどのハードウェアを導入するか、あるいは、ネットワーク全体をＤＨＣＰ環境とし、専用のＤＨＣＰサーバを導入するか、あるいは、ＬＡＮへの接続が予想される装置すべてに専用のパーソナル・ファイアウォール・プログラムをインストールする必要があった。
【解決手段】
本発明では、イーサネットのブロードキャストドメインに監視装置を置き、この監視装置が、検疫対象装置からのＡＲＰ要求を監視し、それに応じてＡＲＰ応答を返信することで特定の装置との通信のみ許可した検疫ネットワークを実現する。
【効果】
監視装置をイーサネットの各ブロードキャストドメインに接続する監視装置で実現することができる。
【選択図】図２

図 2



【特許請求の範囲】
【請求項１】
フレームを受信する受信処理部と、フレームを送信する送信処理部と、検疫対象のノードから送信されたフレームを受信した場合、検疫対象のノードに対する検疫に関する情報の通信を妨げないよう、他のノードについてのネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せが含まれないようにフレームを送信する処理部を有することを特徴とするネットワーク監視装置。
【請求項２】
請求項１において、検疫対象ノードのアドレスを記憶する可否情報テーブルを有し、前記フレームのアドレスを前記可否情報テーブルの記憶内容と比較することで検疫対象となるノードを特定することを特徴とするネットワーク監視装置。
【請求項３】
請求項１において、前記検疫情報は検疫サーバに格納されることを特徴とするネットワーク監視装置。
【請求項４】
請求項３において、前記検疫サーバのネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せを含むフレームを送信することを特徴とするネットワーク監視装置。
【請求項５】
請求項４において、ネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せを含む情報を要求するフレームが受信された場合に、前記フレームの送信処理がなされることを特徴とするネットワーク監視装置。
【請求項６】
請求項５において、自装置のネットワークアドレスと前記ネットワークより高い層における前記検疫対象のノードに相応するアドレスの組合せを含む情報を送信することを特徴とするネットワーク監視装置。
【請求項７】
請求項５において、自装置のネットワークアドレスと前記ネットワークより高い層における通信相手ノードに相応するアドレスの組合せを含む情報を送信することを特徴とするネットワーク監視装置。
【請求項８】
請求項３において、前記検疫サーバは他のネットワークに設置され、前記検疫サーバと、ＩＰパケットのフィルタリング機能を持つルータを介して接続されることを特徴とするネットワーク監視装置。
【請求項９】
請求項１において、ＯＳ或いはウィルス検出ソフトのアップデートデータを保存する保存部から、前記検疫対象のノードに前記アップデートデータが送信されようになすことを特徴とするネットワーク監視装置。
【請求項１０】
フレームを受信する受信処理部と、フレームを送信する送信処理部と、検疫対象のノードから送信されたフレームを受信した場合、検疫対象のノードが特定したノードにおけるネットワークアドレス或いは前記ネットワークより高い層におけるアドレスの少なくとも一方を該ノードに相応しないアドレスとしてフレームを送信する処理部を有することを特徴とするネットワーク監視装置。
【請求項１１】
検疫対象のノードからフレームが送信されると、監視ノードから、前記検疫対象のノードと検疫に関する情報を格納するノードとの通信を妨げないよう、他のノードについてのネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せが含まれないようにフレームを送信するネットワークシステム。
【請求項１２】

フレームを受信部で受信し、該受信が、検疫対象のノードから送信されたフレームである場合、検疫対象のノードに対する検疫に関する情報の通信を妨げないように、他のノードについてのネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せが含まれないよう演算処理し、送信部からフレームを送信するネットワーク監視方法。

【請求項１３】

検疫対象のノードからフレームが送信されると、監視ノードから、前記検疫対象のノードと検疫に関する情報を格納するノードとの通信を妨げないよう、他のノードについてのネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せが含まれないようにフレームを送信するネットワーク通信方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク監視装置，ネットワーク監視方法，ネットワークシステム及びネットワーク監視方法及びネットワーク通信方法に関する。

【背景技術】

【０００２】

社内ＬＡＮなど保護されたネットワークを保護するため、ネットワークへの接続を制限する、いわゆる、ネットワーク監視装置が知られている。このような技術は、例えば、特開２００３－３０３１１８号公報に記載されている。

【０００３】

【特許文献１】特開２００３－３０３１１８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

このような検疫ネットワークで、特に、外部から持ち込まれたコンピュータなどを、保護されたネットワークへの接続を許可する前に、当該コンピュータのオペレーティングシステムやウィルス検出ソフトがアップデートされているか確認し、アップデートされていない場合、当該コンピュータのオペレーティングシステムやウィルス検出ソフトのバージョンアップソフトを供給する必要がある。

【０００５】

そのためには、認証スイッチを利用することが考えられる。すなわち、外部から持ち込まれたコンピュータを社内ＬＡＮなどの保護されたネットワークに接続する際、検疫ネットワーク機能をサポートしたスイッチングハブがそのコンピュータが接続されたポートを、保護されたネットワークとは仮想的に切り離されたヴァーチャルＬＡＮ（ＶＬＡＮ）により構成された検疫ネットワークに接続した。そして、検疫ネットワーク上でオペレーティングシステム（ＯＳ）やウィルス検出ソフトのアップデートが完了すると、スイッチングハブが当該コンピュータが接続されたポートを保護されたネットワーク側に所属するようＶＬＡＮの設定を変更する。

【０００６】

しかしながら、保護されたネットワークにおいて、端末が接続するスイッチングハブから、検疫サーバが接続するスイッチングハブまで、その経路上のすべてのスイッチングハブが検疫ネットワーク機能をサポートすることが必要である。

【０００７】

また、認証ＤＨＣＰ方式を利用することが考えられる。すなわち、外部から持ち込まれたコンピュータがＤＨＣＰを用いてＩＰアドレスを取得する際、ＤＨＣＰサーバが検疫ネットワーク用のＩＰアドレスとデフォルトゲートウェイＩＰアドレスを当該コンピュータに割り当てる。検疫ネットワーク用のＩＰアドレスは保護されたネットワークとはＩＰアドレス体系が異なるため、当該コンピュータが保護されたネットワーク内の装置と通信す

ることはできない。当該コンピュータは検疫ネットワーク上でＯＳやウィルス検出ソフトのアップデートが完了すると、保護されたネットワークと接続可能なＩＰアドレスやデフォルトゲートウェイＩＰアドレスが再び割り当てられ、保護されたネットワーク内の装置と通信することが可能となる。

【０００８】

また、保護されたネットワークがＤＨＣＰを用いる環境でなら適用できるが、ＩＰアドレスを固定で割り振るネットワーク環境では適用することができず、また、ＤＨＣＰを用いる環境であってもＩＰアドレスを固定で割り当てた装置に対しては効果がない。

【０００９】

さらに、パーソナル・ファイアウォールを利用することが考えれえる。すなわち、保護されたネットワークと接続するコンピュータにあらかじめファイアウォール機能を持つソフトウェアをインストールしておく。当該コンピュータが保護されたネットワークに接続しようとした際は、ＯＳやウィルス検出ソフトのアップデートプログラムが保存された検疫サーバとのみ通信できるよう、パーソナル・ファイアウォールが通信を制限する。アップデートが完了するとパーソナル・ファイアウォールの制限が解除され、保護されたネットワーク内の装置と通信が可能になる。

【００１０】

しかしながら、保護されたネットワークに接続する可能性があるコンピュータにあらかじめパーソナル・ファイアウォールのソフトウェアをインストールする必要があり、これがインストールされていない装置に対しては効果がない。

【００１１】

本発明の目的は、上記した問題点の少なくとも１つを解決し、画可能なネットワーク監視装置，ネットワーク監視方法，ネットワークシステム及びネットワーク監視方法及びネットワーク通信方法を提供することにある。

【課題を解決するための手段】

【００１２】

上記目的を達成するために、本発明では、フレームを受信部で受信し、該受信が、検疫対象のノードから送信されたフレームである場合、検疫対象のノードと検疫情報を格納するノードとの通信を妨げず、他のノードについてのネットワークアドレスと前記ネットワークより高い層における相応するアドレスの組合せが含まれないよう演算処理し、送信部からフレームを送信するように構成した。

【００１３】

具体的には、イーサネット上のイーサフレームを受信するフレーム受信処理部と、イーサフレームを送信するフレーム送信処理部と、検疫ネットワークに接続する装置に関する情報を蓄える接続可否情報テーブルと、受信したイーサフレームと接続可否情報テーブルからＡＲＰフレーム送信を判断する接続可否判断処理部と、接続可否判断処理部からの指示に従いＡＲＰフレームを送信するＡＲＰ応答フレーム生成部と、検疫に必要となるソフトウェアを記憶するＯＳ／ウィルス検出ソフトのアップデートデータ保存部を備える、イーサネットのブロードキャストドメインに接続する監視装置を用い、検疫対象装置からのＡＲＰ要求に応じてＡＲＰ応答を送信することで検疫ネットワークを実現したものである。

【発明の効果】

【００１４】

本発明によれば、外部から持ち込まれたコンピュータ等のノードに対して、ネットワークのノードへの通信を許可する前に、コンピュータのオペレーティングシステムやウィルス検出ソフト等を適切なバージョンに保つすることが可能となる。

【発明を実施するための最良の形態】

【００１５】

以下、本発明の実施例を図面を用いて説明する。図１は本発明の検疫ネットワーク方式の実施例１である。本構成例では、イーサネットによる１つのブロードキャスト・ドメイ

ンからなるネットワーク１０４に、監視装置１００と、いくつかの装置１０１ａ～101ｂ、検疫対象装置１０３が接続されている。本実施例では、ＯＳ／ウィルス検出ソフトのアップデートデータを保持する検疫サーバを監視装置１００が兼ねる。

【００１６】

図２は本実施例における監視装置１００の構成であり、ネットワーク１０４に接続するフレーム受信処理部２０１，フレーム送信処理部２０２，ＯＳ／ウィルス検出ソフトのアップデートデータ保存部２０３,接続可否判断処理部２０４,接続可否情報テーブル２０５，ＡＲＰ応答フレーム生成部２０６からなる。なお、ＡＲＰ（Address Resolution Protocol）は、ＴＣＰ／ＩＰプロトコルにおいて、ＩＰアドレスからＭＡＣアドレスを求めるためのプロトコルのことである。具体的には、自分のイーサーネットアドレスと自分のＩＰアドレス、そして通信先のＩＰアドレスの３つの組を、ＡＲＰ要求として、ＬＡＮ上へブロードキャストする。ＬＡＮ上の各ノードはＡＲＰ問い合わせのブロードキャストを監視しているので、自分のＩＰアドレスが指定されていれば、ＡＲＰ応答として、パケットに自分のＭＡＣアドレスを入れて応答を返す。このＡＲＰ要求と、ＡＲＰ応答によって、ＩＰアドレスからＭＡＣアドレスを得る。なお、ＭＡＣアドレスとは、イーサーネットでフレームの送受信を行うための物理的なアドレスであり、世界中で同じ物理アドレスを持つことがないように、すべて異なる固有のアドレスが割り当てられている。また、ＩＰアドレスは、ＴＣＰ／ＩＰプロトコルを使用しているネットワーク等で、サーバやクライアント，ルータなどのノードごとに割り振られた固有のアドレスであり、通信先の機器を指定するために使われる。

【００１７】

図８に接続可否情報テーブル２０５の構成を示す。本テーブルはネットワーク１０４に接続するそれぞれの装置に関するＭＡＣアドレス８１０，ＩＰアドレス８１１，ステータス８１２の組からなる。ステータス８１２が接続許可となっている装置間の通信については、監視装置１００は一切干渉しない。ステータス８１２が検疫対象となっている装置については、当該装置と監視装置１００との間の通信のみ可能となるよう監視装置１００が処理を行う。本テーブルにエントリーのない装置は接続を許可しない装置である。検疫対象装置１０３は外部から持ち込まれたコンピュータで、ネットワークとの接続は許可されているが、ＯＳ／ウィルス検出ソフトのアップデートが必要であるものとする。検疫対象装置１０３は他装置との通信のため、ＡＲＰ要求フレームをブロードキャストで送信する。

【００１８】

図３にＡＲＰ要求フレームを示す。検疫対象装置１０３がＡＲＰ要求フレームを送信する場合、送信元ＭＡＣアドレス３０１には検疫対象装置１０３のＭＡＣアドレスが、送信元ＩＰアドレス３０２には検疫対象装置１０３のＩＰアドレスが入る。宛て先ＭＡＣアドレス３０３には0が入る。宛て先ＩＰアドレスには検疫対象装置１０３が通信しようとする相手装置のＩＰアドレスが入る。

【００１９】

図４に監視装置１００内の接続可否判断処理部２０４の処理フローを示す。処理４０１で受信したフレームのプロトコル種別を判断し、ＡＲＰ以外なら処理を終了する。処理４０２で受信したＡＲＰの種別を判定し、ＡＲＰ応答なら処理を終了する。処理４０３で受信したＡＲＰ要求の送信元ＭＡＣアドレスが接続可否情報テーブル２０５に接続許可装置として登録されているか判断する。登録済みならば処理を終了する。処理４０４で受信したＡＲＰ要求の送信元ＩＰアドレスを使用している接続許可装置はあるかを判断する。なければ処理４０５を、あれば処理４０６を実施する。処理４０５では不正装置排除用ＡＲＰ応答ａをブロードキャスト送信することで、たとえば、装置１０１ａから検疫対象装置１０３への通信を防ぐ。処理４０６では不正装置排除用ＡＲＰ応答ｂをブロードキャスト送信する。これは検疫対象装置１０３がすでに他の装置に割り当てられているＩＰアドレスを使っているケースに対応するためである。すなわち検疫対象装置１０３がＡＲＰ要求を送信することによって当該ＩＰアドレス宛ての通信の宛て先が検疫対象装置１０３

宛てに書き換えられてしまうが、不正装置排除用ＡＲＰ応答ｂを送信することで、当該ＩＰアドレス宛ての通信を本来の装置宛てに修正する。処理４０７は不正装置排除用ARP応答ｃを検疫対象装置１０３宛てに送出することで、検疫対象装置１０３が通信相手としてＡＲＰ要求を送信した装置のＭＡＣアドレスを監視装置１００のＭＡＣアドレスで上書きすることにより、検疫対象装置からの通信を監視装置１００宛てにするためである。

【００２０】

図５に不正装置排除用ＡＲＰ応答ａを示す。送信元ＭＡＣアドレス５０１には監視装置１００のＭＡＣアドレスが、送信元ＩＰアドレス５０２には検疫対象装置のＩＰアドレスが、宛て先ＭＡＣアドレス５０３には検疫対象装置のＭＡＣアドレスが、宛て先ＩＰアドレス５０４には検疫対象装置のＩＰアドレスが入る。

【００２１】

図６に不正装置排除用ＡＲＰ応答ｂを示す。送信元ＭＡＣアドレス６０１には通信相手のＭＡＣアドレスが、送信元ＩＰアドレス６０２には通信相手のＩＰアドレスが、宛て先ＭＡＣアドレス６０３には検疫対象装置のＭＡＣアドレスが、宛て先ＩＰアドレス６０４には検疫対象装置のＩＰアドレスが入る。

【００２２】

図７に不正装置排除用ＡＲＰ応答ｂを示す。送信元ＭＡＣアドレス７０１には監視装置１００のＭＡＣアドレスが、送信元ＩＰアドレス７０２には通信相手のＩＰアドレスが、宛て先ＭＡＣアドレス７０３には検疫対象装置のＭＡＣアドレスが、宛て先ＩＰアドレス７０４には検疫対象装置のＩＰアドレスが入る。

【００２３】

ここで、検疫対象装置１０３が監視装置１００以外の装置、たとえば装置１０１ａと通信する場合の動作を図４に示すフローと図１５に示すチャートに従い詳細に説明する。ここでは検疫対象装置１０３は他の装置とは重複しないＩＰアドレスを持つものとする。装置１０１ａとの通信を開始する前に、検疫対象装置１０３はＡＲＰ要求１５０１をブロードキャスト送信する。このとき、図３に示す通信相手のＩＰアドレス３０４には装置101aのＩＰアドレスが設定される。

【００２４】

このＡＲＰ要求に対し、装置１０１ａがＡＲＰ応答１５０２を返す。また、ＡＲＰ要求１５０１はブロードキャスト送信のため、監視装置１００も受信する。監視装置１００は図４に示すフローに従いこのフレームに対する処理を行う。すなわち、処理４０１はARPであるため処理４０２に進み、処理４０２は要求であるため処理４０３に進み、処理403では検疫対象装置１０３のＭＡＣアドレスは接続可否情報テーブル２０５上に検疫対象として登録されているため処理４０４に進む。

【００２５】

処理４０４では検疫対象装置１０３のＩＰアドレスは他の装置では使われていないため処理４０５に進む。処理４０５にて、監視装置１００は図１５の１５０３に示す不正装置排除用ＡＲＰ応答ａをブロードキャスト送信する。これにより、ネットワーク１０４に接続する装置は検疫対象装置１０３のＭＡＣアドレスとして監視装置１００のＭＡＣアドレスを記憶するので、検疫対象装置１０３宛ての通信は不可となる。

【００２６】

さらに、図４のフローに従い、監視装置１００は処理４０７にて図１５の１５０４に示す不正装置排除用ＡＲＰ応答ｃを検疫対象装置１０３宛てに送出する。これにより、検疫対象装置１０３は装置１０１ａのＭＡＣアドレスとして監視装置１００のＭＡＣアドレスを記憶するため、装置１０１ａ宛ての通信は不可となる。

【００２７】

次に、検疫対象装置１０３が監視装置１００との通信を試みる場合の動作を図４に示すフローと図１６に示すチャートに従い詳細に説明する。処理４０５までの動作は上記で説明した動作と違いはない。続く処理４０７で、監視装置１００は図１６の１６０４に示す不正装置排除用ＡＲＰ応答ｃを検疫対象装置１０３宛てに送出するが、この場合、検疫対

象装置１０３は監視装置１００のＭＡＣアドレスとして監視装置１００のＭＡＣアドレスを記憶する。つまり、検疫対象装置１０３は正しく監視装置１００のＩＰアドレスとMACアドレスの組合せを記憶するので、監視装置１００への通信は可能となる。これにより、検疫対象装置１０３は監視装置１００が有するＯＳ／ウィルス検出ソフトのアップデートデータを自装置に転送することが可能となり、ＯＳ／ウィルス検出ソフトのアップデートを実施することができる。本アップデートが完了したことを確認した上で、接続可否情報テーブル２０５上の検疫対象装置１０３のステータスを検疫対象から接続許可に書き換える。これにより、以後は検疫対象装置１０３も装置１０１ａ～１０１ｂと同等に通信することが可能となる。

【００２８】

以下、実施例２について説明する。

【００２９】

図９は本発明の実施例２の構成である。本実施例では、実施例１と異なり、監視装置１００は内部にＯＳ／ウィルス検出ソフトのアップデートデータ保存部２０３を持たず、替わりにこれらのデータを保持する検疫サーバ１０２を設置する。検疫サーバ１０２の役割は、検疫対象装置１０３からの要求により、ＯＳ／ウィルス検出ソフトのアップデートデータを検疫対象装置１０３へ転送することである。

【００３０】

図１０に実施例２の場合の監視装置１００内の接続可否判断処理部２０４の処理フローを示す。なお、ここでは図４と異なる部分のみ記述してある。処理４０１～処理４０３までは図４と同じである。処理４０３のあと処理１００１にて受信したＡＲＰ要求の送信元ＭＡＣアドレスが接続可否情報テーブル２０５に検疫対象として登録されているかどうかを判定する。登録されていなければ、図４の処理４０４へと進む。登録されている場合は処理１００２へと進む。処理１００２では受信したＡＲＰ要求の宛て先ＩＰアドレスが検疫サーバ１０２かどうかを判定する。検疫サーバ１０２以外ならば図４の処理４０４へと進む。検疫サーバ１０２宛てならば処理４０５を実行する。処理４０５にて不正装置排除用ＡＲＰ応答ａをブロードキャスト送信することで、たとえば、装置１０１ａから検疫対象装置１０３への通信を防ぐ。ただし、このままでは検疫サーバ１０２から検疫対象装置１０３への通信も不可となるため、続く処理１００３にて検疫装置アドレス修復用ＡＲＰ応答を検疫サーバ１０２宛てに送出する。

【００３１】

図１１に検疫装置アドレス修復用ＡＲＰ応答を示す。送信元ＭＡＣアドレス１１０１には検疫対象装置１０３のＭＡＣアドレスを、送信元ＩＰアドレス１１０２には検疫対象装置１０３のＩＰアドレスを、宛て先ＭＡＣアドレス１１０３には修復相手のＭＡＣアドレスを、宛て先ＩＰアドレス１１０４には修復相手のＩＰアドレスを設定し、修復相手宛てに送信する。

【００３２】

ここで、検疫対象装置１０３が検疫サーバ１０２との通信を試みる場合の動作を図１０に示すフローと図１７に示すチャートに従い詳細に説明する。ここでは検疫対象装置103は他の装置とは重複しないＩＰアドレスを持つものとする。

【００３３】

検疫サーバ１０２との通信を開始する前に、検疫対象装置１０３はＡＲＰ要求１７０１をブロードキャスト送信する。このとき、図３のＡＲＰ要求フレームの通信相手のＩＰアドレス３０４には検疫サーバ１０２のＩＰアドレスが設定される。このＡＲＰ要求により、検疫サーバ１０２はＡＲＰ応答１７０２を送信する。また、ＡＲＰ要求１７０１はブロードキャスト送信のため、監視装置１００も受信し、図１０に示すフローに従いこのフレームに対する処理を行う。ただし、処理４０１～処理４０２は実施例１の処理と同じため説明は割愛する。

【００３４】

続く処理４０３では検疫対象装置１０３のＭＡＣアドレスは接続可否情報テーブル205

上に接続許可としては登録されていないため処理１００１に進む。処理１００１では検疫対象装置１０３のＭＡＣアドレスは接続可否情報テーブル２０５上に検疫対象として登録されているため処理１００２に進む。処理１００２では受信したＡＲＰ要求の宛て先ＩＰアドレスは検疫サーバ１０２であるため処理４０５に進む。処理４０５にて、監視装置１００は不正装置排除用ＡＲＰ応答ａ　１７０３をブロードキャスト送信する。これにより、ネットワーク１０４に接続する装置は検疫対象装置１０３のＭＡＣアドレスとして監視装置１００のＭＡＣアドレスを記憶するので、検疫対象装置１０３宛ての通信は不可となる。続く処理１００３で監視装置１００は検疫装置アドレス修復用ＡＲＰ応答１７０４を検疫サーバ１０２宛てに送出する。このとき、宛て先ＭＡＣアドレス１１０３には検疫サーバ１０２のＭＡＣアドレスが、宛て先ＩＰアドレス１１０４には検疫サーバ１０２のＩＰアドレスが設定される。これにより、検疫サーバ１０２は検疫対象装置１０３のMACアドレスとして正しいＭＡＣアドレスを記憶するので、検疫サーバ１０２と検疫対象装置１０３間の通信が可能となる。よって、検疫対象装置１０３は検疫サーバ１０２が有するＯＳ／ウィルス検出ソフトのアップデートデータを自装置に転送することが可能となり、ＯＳ／ウィルス検出ソフトのアップデートを実施することができる。これに続く動作は実施例１と同様である。

【００３５】

以下、実施例３について説明する。

【００３６】

図１２は本発明の実施例３の構成である。本実施例では、実施例２とは異なり、検疫サーバ１０２はルータ１０６を介した別ネットワーク１０５に接続される。ルータ１０６はこれを通過するＩＰパケットに対し条件によりフィルタリングする機能を有するものとする。フィルタリング機能そのものは従来から存在する一般的な技術である。

【００３７】

図１３にルータ１０６のフィルタリング設定テーブルの例を示す。フィルタリング設定テーブル１３０１は、条件となる送信元ＩＰアドレス１３０２、および、宛て先ＩＰアドレス１３０３と、その条件を満たすＩＰパケットに対するアクション１３０４からなる。本実施例では、ネットワーク１０４から別ネットワーク１０５へ向けてルータ１０６を通過するＩＰパケットに対し本フィルタを適用する。その設定値は、送信元ＩＰアドレスには検疫対象装置１０３のＩＰアドレスを設定する。検疫対象装置が複数ある場合は検疫対象装置１０３ａ～１０３ｃのように複数のエントリを作成する。宛て先ＩＰアドレスには検疫サーバ１０２以外を条件として設定する。アクションは廃棄を設定する。

【００３８】

また、本実施例では、検疫対象装置のデフォルト・ゲートウェイとしてルータ１０６のネットワーク１０４側ＩＰアドレスを設定する。

【００３９】

図１４に実施例３の監視装置１００内の接続可否判断処理部２０４の処理フローを示す。なお、ここでは図１０と異なる部分のみ記述してある。処理４０１～処理１００１までは図１０と同じである。処理１００１のあと、処理１４０２では受信したＡＲＰ要求の宛て先ＩＰアドレスがルータ１０６かどうかを判定する。ルータ１０６以外ならば図４の処理４０４へと進む。ルータ１０６宛てならば処理４０５を実行する。処理４０５にて不正装置排除用ＡＲＰ応答をブロードキャスト送信することで、たとえば、装置１０１ａから検疫対象装置１０３への通信を防ぐ。ただし、このままではルータ１０６から検疫対象装置１０３への通信も不可となるため、続く処理１４０３にて検疫装置アドレス修復用ARP応答をルータ１０６宛てに送出する。

【００４０】

ここで、検疫対象装置１０３が検疫サーバ１０２との通信を試みる場合の動作を図１４に示すフローと図１８に示すチャートに従い詳細に説明する。ここでは検疫対象装置103は他の装置とは重複しないＩＰアドレスを持つものとする。検疫サーバ１０２との通信を開始する前に、検疫対象装置１０３はＡＲＰ要求１８０１をブロードキャスト送信する。

このとき、図３のＡＲＰ要求フレームの通信相手のＩＰアドレス３０４には検疫対象装置のデフォルト・ゲートウェイとして設定されたルータ１０６のＩＰアドレスが設定される。このＡＲＰ要求により、ルータ１０６はＡＲＰ応答１８０２を送信する。また、ＡＲＰ要求１８０１はブロードキャスト送信のため、監視装置１００も受信し、図１４に示すフローに従いこのフレームに対する処理を行う。ただし、処理４０１～処理１００１は実施例２の処理と同じため説明は割愛する。続く処理１４０２では受信したＡＲＰ要求の宛て先ＩＰアドレスはルータ１０６であるため処理４０５に進む。

【００４１】

処理４０５にて、監視装置１００は示す不正装置排除用ＡＲＰ応答ａ　１８０３をブロードキャスト送信する。これにより、ネットワーク１０４に接続する装置は検疫対象装置１０３のＭＡＣアドレスとして監視装置１００のＭＡＣアドレスを記憶するので、検疫対象装置１０３宛ての通信は不可となる。続く処理１４０３で監視装置１００は検疫装置アドレス修復用ＡＲＰ応答１８０４をルータ１０６宛てに送信する。このとき、宛て先MACアドレス１１０３にはルータ１０６のＭＡＣアドレスが、宛て先ＩＰアドレス１１０４にはルータ１０６のＩＰアドレスが設定される。これにより、ルータ１０６は検疫対象装置１０３のＭＡＣアドレスとして正しいＭＡＣアドレスを記憶するので、ルータ１０６と検疫対象装置１０３間の通信が可能となる。検疫対象装置１０３から検疫サーバ１０２宛てのＩＰパケットがルータ１０６を通る際、フィルタリング設定テーブル１３０１と比較される。この例では、送信元ＩＰアドレスが検疫対象装置１０３、宛て先ＩＰアドレスが検疫サーバであるので、ＩＰパケットはルータ１０６を通り、別ネットワーク１０５へ、さらに検疫サーバ１０２に到達することができる。よって、検疫対象装置１０３は検疫サーバ１０２が有するＯＳ／ウィルス検出ソフトのアップデートデータを自装置に転送することが可能となり、ＯＳ／ウィルス検出ソフトのアップデートを実施することができる。これに続く動作は実施例２と同様である。

【００４２】

次に、検疫対象装置１０３が別ネットワーク１０５に接続する検疫サーバ１０２以外の装置と通信する場合の動作を詳細に説明する。この場合も、前記の検疫対象装置１０３と検疫サーバ１０２間の通信同様、ネットワーク１０４内での検疫対象装置１０３の通信相手はルータ１０６のため、たとえ宛て先が検疫サーバ１０２以外の装置であったとしても、監視装置１００は検疫対象装置１０３とルータ１０６間の通信を許可する。しかし、ルータ１０６のフィルタリングテーブル１３０１との比較において、宛て先ＩＰアドレスが検疫サーバ１０２以外であるためＩＰパケットは破棄される。よって、検疫対象装置103が別ネットワーク１０５に接続する検疫サーバ１０２以外の装置との通信は不可となる。

【００４３】

本実施例によれば、検疫ネットワーク機能をサポートする専用のスイッチングハブは不要であり、また、一般的なリピータ・ハブを用いても検疫ネットワークを構成できるので、既存のネットワークのハードウェア構成を変更する必要がない。また、ＤＨＣＰ環境においても固定ＩＰアドレス環境においても同様に動作するので、既存ネットワーク環境を変更する必要がない。さらに、すべての端末に対するパーソナル・ファイアウォールなどの専用ソフトウェアのインストールも不要であり、より簡便に検疫ネットワークを実現することができる。

【図面の簡単な説明】

【００４４】

【図１】実施例１のシステム全体構成図。

【図２】監視装置の構成図。

【図３】ＡＲＰ要求フレームの説明図。

【図４】実施例１の監視装置の動作を示すフローチャート。

【図５】検疫対象装置への通信が不可となるよう監視装置が送信するＡＲＰ応答１。

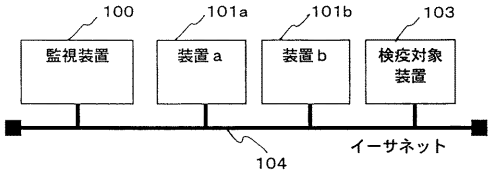
【図６】検疫対象装置への通信が不可となるよう監視装置が送信するＡＲＰ応答２。

【図７】検疫対象装置からの通信が不可となるよう監視装置が送信するＡＲＰ応答。

【図８】接続可否情報テーブルの構成。
【図９】実施例２のシステム構成図。
【図１０】実施例２の監視装置の動作を示すフローチャート。
【図１１】一部の装置に対し、検疫対象装置への通信が可能となるよう監視装置が送信するＡＲＰ応答。
【図１２】実施例３のシステム構成図。
【図１３】ルータのフィルタリング設定テーブル。
【図１４】実施例３の監視装置の動作を示すフローチャート。
【図１５】実施例１において検疫対象装置が監視装置以外の装置との通信を試みた場合のチャート。
【図１６】実施例１において検疫対象装置が監視装置と通信する場合のチャート。
【図１７】実施例２において検疫対象装置が検疫サーバと通信する場合のチャート。
【図１８】実施例３において検疫対象装置がルータを経由し検疫サーバと通信する場合のチャート。
【符号の説明】
【００４５】
１００…監視装置、１０２…検疫サーバ、１０３…検疫対象装置、１０４…監視装置や検疫対象装置が接続するネットワーク、１０５…ルータを介した別ネットワーク、１０６…ルータ、２０１…フレーム受信処理部、２０２…フレーム送信処理部、２０３…ＯＳ／ウィルスソフトのアップデートデータ保存部、２０４…接続可否判断処理部、２０５…接続可否情報テーブル、２０６…ＡＲＰ応答フレーム生成部。

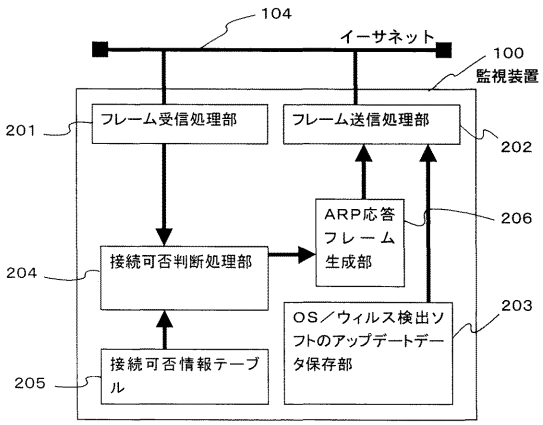
【図１】

図 1



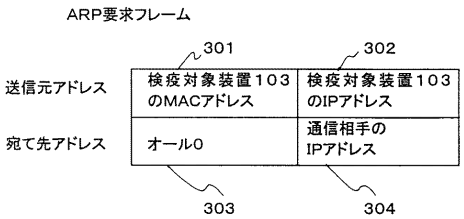
【図２】

図 2



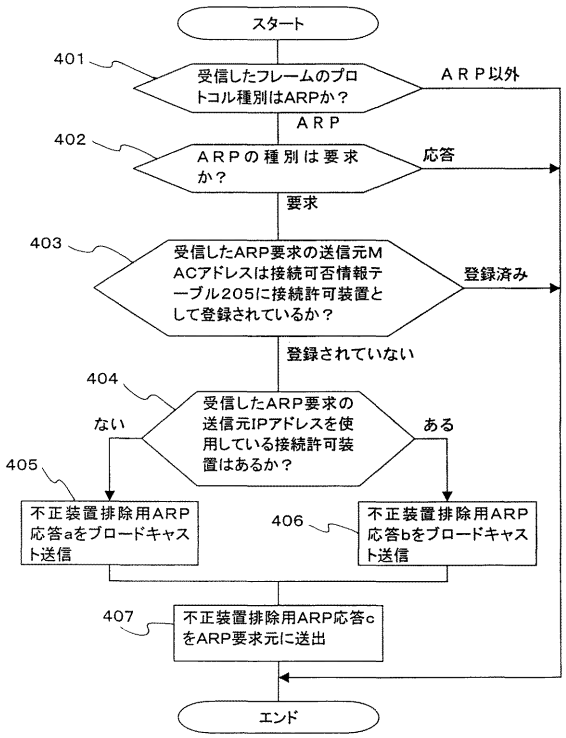
【図３】

図 3



【図４】

図 4



【図５】

図 5

不正装置排除用ARP応答a

	501	502
送信元アドレス	監視装置103のMACアドレス	検疫対象装置のIPアドレス
宛て先アドレス	検疫対象装置のMACアドレス	検疫対象装置のIPアドレス
	503	504

【図６】

図 6

不正装置排除用ARP応答b

	601	602
送信元アドレス	通信相手のMACアドレス	通信相手のIPアドレス
宛て先アドレス	検疫対象装置のMACアドレス	検疫対象装置のIPアドレス
	603	604

【図７】

図 7

不正装置排除用ARP応答c

	701	702
送信元アドレス	監視装置100のMACアドレス	通信相手のIPアドレス
宛て先アドレス	検疫対象装置のMACアドレス	検疫対象装置のIPアドレス
	703	704

【図８】

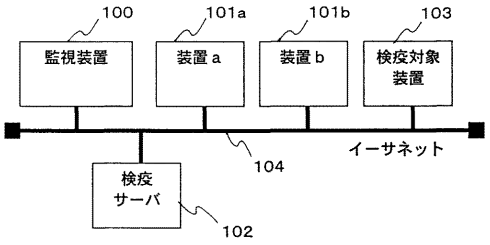
図 8

接続可否情報テーブル205の構成

	MACアドレス	IPアドレス	ステータス
装置101a	MAC801	IP804	接続許可
装置101b	MAC802	IP805	接続許可
検疫対象装置103	MAC803	IP806	検疫対象
	810	811	812

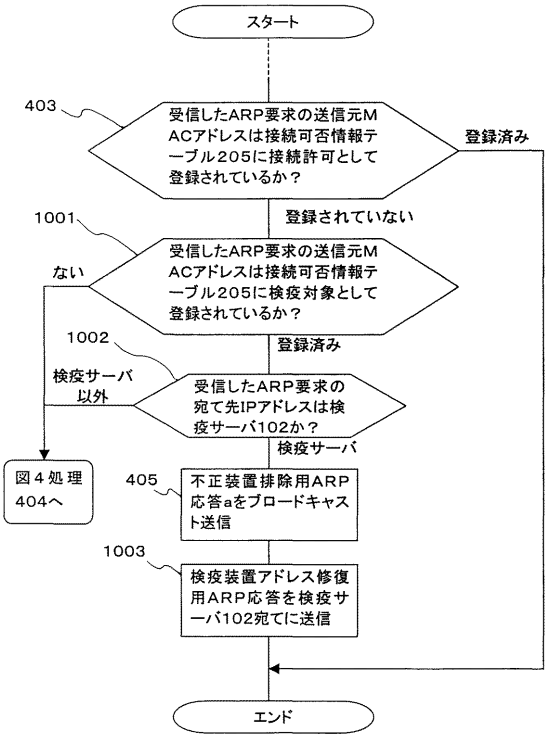
【図９】

図 9



【図１０】

図 10



【図１１】

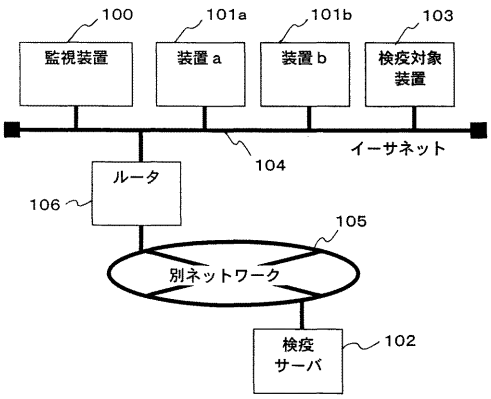
図 11

検疫装置アドレス修復用ARP応答

	1101	1102
送信元アドレス	検疫対象装置103のMACアドレス	検疫対象装置103のIPアドレス
宛て先アドレス	修復相手のMACアドレス	修復相手のIPアドレス
	1103	1104

【図１２】

図 12



【図１３】

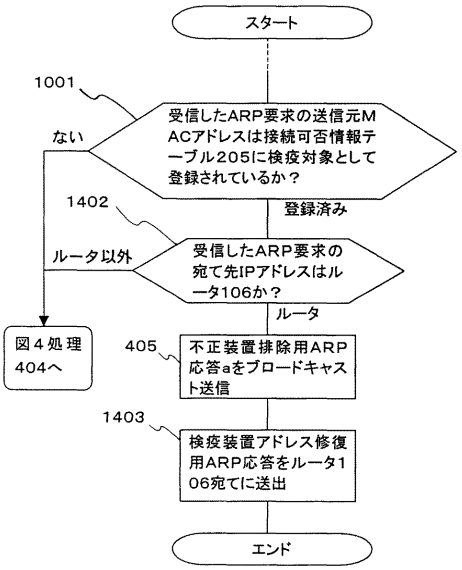
図 13

ルータ106のフィルタリング設定テーブル

1301	送信元ＩＰアドレス (1302)	宛て先ＩＰアドレス (1303)	アクション (1304)
	検疫対象装置１０３ａ	検疫サーバ以外	廃棄
	検疫対象装置１０３ｂ	検疫サーバ以外	廃棄
	検疫対象装置１０３ｃ	検疫サーバ以外	廃棄

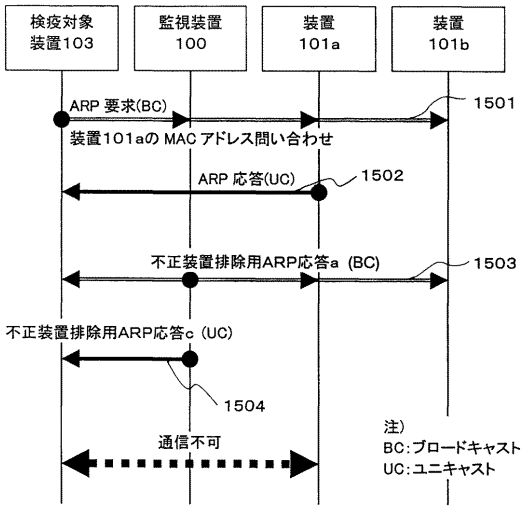
【図１４】

図 14



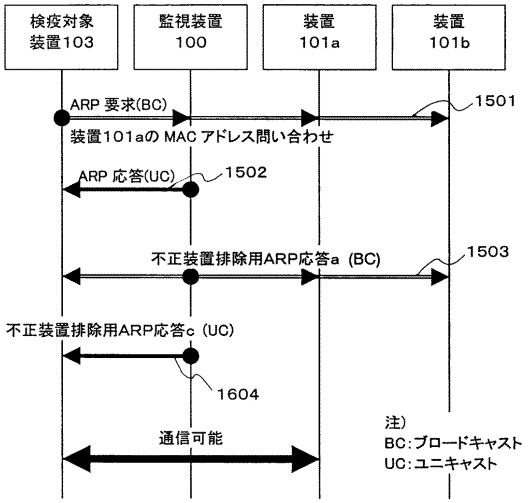
【図１５】

図 15



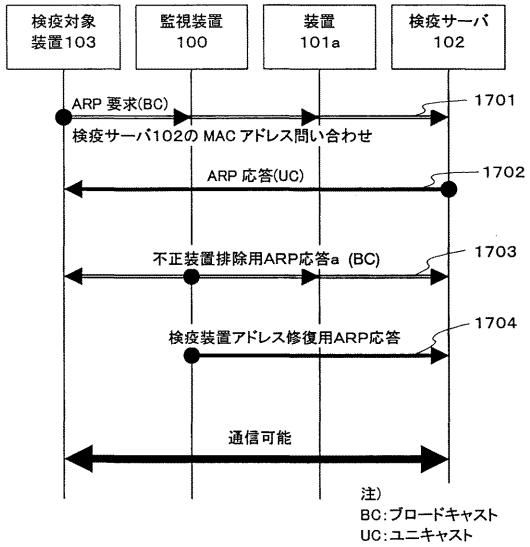
【図１６】

図 16



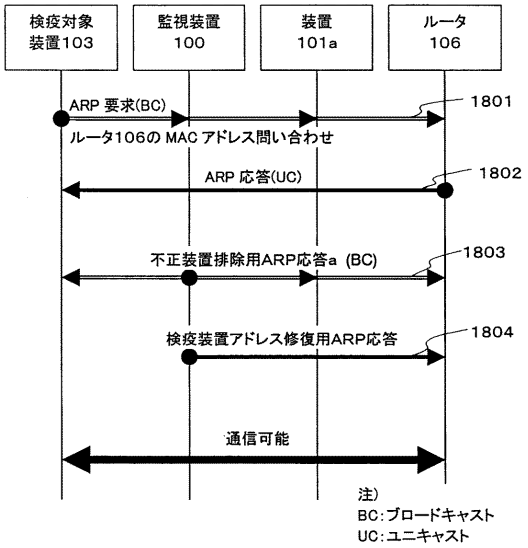
【図１７】

図 17



【図１８】

図 18



フロントページの続き

(72)発明者　足達　芳昭
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所情報制御システム事業部内
(72)発明者　外岡　秀樹
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所情報制御システム事業部内
(72)発明者　鴨志田　弘司
茨城県日立市大みか町五丁目２番１号　株式会社日立ハイコス内
(72)発明者　武富　浩二
茨城県日立市大みか町五丁目２番１号　株式会社日立ハイコス内

Ｆターム(参考)　5B089 GA32 KA17 MC01
5K030 GA15 HA08 HD03 JA10 KA05
5K032 AA08 BA08 CC10 CD01 DA01 DA06 DB28 EA07
5K033 AA08 BA08 CB01 CB08 DA01 DB12 DB16 DB20 EA07