

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4384236号
(P4384236)

(45) 発行日 平成21年12月16日(2009.12.16)

(24) 登録日 平成21年10月2日(2009.10.2)

(51) Int.Cl.

F I

H O 4 L 12/28 (2006.01)

H O 4 L 12/28 2 0 0 A

請求項の数 13 (全 30 頁)

(21) 出願番号 特願2008-130277 (P2008-130277)
 (22) 出願日 平成20年5月19日(2008.5.19)
 (62) 分割の表示 特願2004-69937 (P2004-69937)
 の分割
 原出願日 平成16年3月12日(2004.3.12)
 (65) 公開番号 特開2008-199675 (P2008-199675A)
 (43) 公開日 平成20年8月28日(2008.8.28)
 審査請求日 平成20年5月19日(2008.5.19)

早期審査対象出願

(73) 特許権者 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
 (73) 特許権者 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 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

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、ネットワーク監視用プログラム及びネットワーク監視用プログラムが格納された記録媒体

(57) 【特許請求の範囲】

【請求項1】

ネットワークに流れる情報を受信する受信手段と、

前記受信手段を介してアドレス解決プロトコルの要求を受取ると、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスと共に物理アドレスに基づいて、ローカルネットワークを構成する予め定められた許可端末に相当するかを判断する判断手段と、

前記許可端末に相当しないと判断された場合に、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスが、前記ローカルネットワークで保護すべき端末によって使用されているか判断する手段と、

前記ローカルネットワークで保護すべき端末によって使用されている場合は、前記端末で組として使用されているネットワークアドレスと物理アドレスを、アドレス解決プロトコルの要求に対する応答として、一方、前記ローカルネットワークで保護すべき端末によって使用されていない場合は、前記アドレス解決プロトコルを要求した端末のネットワークアドレスと所定の物理アドレスを、アドレス解決プロトコルの要求に対する応答として送信する送信手段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、端末に対応してネットワークへの接続可或は否に関する情報を登録する手段と、この登録された接続可或は否に関する情報と受信情報を比較することで、許可の可否を判断することを特徴とするネットワーク監視装置。

10

20

【請求項 3】

請求項 2 において、前記受信手段宛の情報とネットワークの複数端末宛のブロードキャスト情報あるいはマルチキャスト情報を受信、またはネットワークを流れる実質的に全ての情報を受信す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、該許可されないと判断された端末に切り離し専用手段が設置されるか否かにかかわらず、該端末がネットワークから切り離されるよう構成され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 1 において、接続を許可しない端末がネットワークに存在することを検出したことを、または、接続を許可しない端末をネットワークから切り離したことを、外部端末に通知する手段と、ネットワークに接続された端末の切り離し指示あるいは接続指示のうち少なくとも一つを外部端末から受け付ける手段と、受け付けた指示が切り離し指示の場合には、ネットワークアドレスの重複状態を発生させるための情報を生成する手段を有することを特徴とするネットワーク監視装置。

10

【請求項 6】

請求項 5 において、受け付けた指示が接続指示の場合には、ネットワーク内にネットワークアドレスの重複状態を解消させるための情報を生成する手段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 7】

20

請求項 1 乃至 6 のいずれかにおいて、ネットワークアドレスと物理層側アドレスを組み合わせ、ネットワークに接続された端末のアドレス情報を一意的に生成する手段と、生成された一意的なアドレス情報の要素分類に応じて外部から昇順もしくは降順に並べ替える手段と、生成された一意的なアドレス情報の個々の要素に対して外部から有効あるいは無効の設定を可能とする手段を設け、これらの手段により端末アドレス情報を生成し、端末に対するネットワークへの接続可否情報としてこの端末アドレス情報を使用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 1 乃至 6 のいずれかにおいて、該当ネットワークのネットワークアドレス体系のホスト番号部がとりうる最小値から最大値までの全てのホスト番号のうち、接続可否のチェックを行う端末のホスト番号の範囲とチェックを行うタイミング情報を設定する手段と、この範囲のホスト番号を使ったチェック用ネットワークアドレスを生成する手段と、このチェック用ネットワークアドレスを使って、相手端末からの応答を期待できる要求情報を生成する手段と、この要求情報を前記設定されたタイミング情報にもとづいたタイミングで監視装置から送出し、その応答の情報の存在またはその情報内容と、端末に対するネットワークへの接続可否情報とを比較して接続可否を判断することを特徴とするネットワーク監視装置。

30

【請求項 9】

請求項 8 において、相手端末からの応答を期待できる要求情報を生成する手段として、ICMP 要求情報あるいはアドレス要求情報を生成することを特徴とするネットワーク監視装置。

40

【請求項 10】

請求項 1 乃至 6 のいずれかにおいて、端末に対するネットワークへの接続可否情報として、端末のネットワークアドレスおよび物理層側アドレスのうち少なくとも一つを、あるいは、接続許可時間帯および接続不許可時間帯のうち少なくとも一つを、あるいは前回接続した時刻からある閾値以上の経過時間がたった場合にはその接続を拒否するために使用される時刻情報を、あるいは、前回接続した時刻からある閾値以上の経過時間がたった場合には現在接続されている端末を切り離すために使用される時刻情報を、あるいは、これまでに接続を許可されなかった回数、あるいは、許容されるネットワークトラフィックの閾値、あるいは端末のネットワークへの接続許可台数、あるいは端末の所有者情報、ある

50

いはこれらの少なくとも1つ以上を組み合わせたものを、使用することを特徴とするネットワーク監視装置。

【請求項11】

ネットワークに流れる情報を受信し、

前記受信としてアドレス解決プロトコルの要求を受取ると、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスと共に物理アドレスに基づいて、ローカルネットワークを構成する予め定められた許可端末に相当するかを判断し、

前記許可端末に相当しないと判断された場合に、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスが、前記ローカルネットワークで保護すべき端末によって使用されているか判断し、

前記ローカルネットワークで保護すべき端末によって使用されている場合は、前記端末で組として使用されているネットワークアドレスと物理アドレスを、アドレス解決プロトコルの要求に対する応答として、一方、前記ローカルネットワークで保護すべき端末によって使用されていない場合は、前記アドレス解決プロトコルを要求した端末のネットワークアドレスと所定の物理アドレスを、アドレス解決プロトコルの要求に対する応答として送信するネットワーク監視方法。

【請求項12】

ネットワークに流れる情報を受信させ、

前記受信としてアドレス解決プロトコルの要求を受取ると、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスと共に物理アドレスに基づいて、ローカルネットワークを構成する予め定められた許可端末に相当するかを判断させ、

前記許可端末に相当しないと判断された場合に、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスが、前記ローカルネットワークで保護すべき端末によって使用されているか判断させ、

前記ローカルネットワークで保護すべき端末によって使用されている場合は、前記端末で組として使用されているネットワークアドレスと物理アドレスを、アドレス解決プロトコルの要求に対する応答として、一方、前記ローカルネットワークで保護すべき端末によって使用されていない場合は、前記アドレス解決プロトコルを要求した端末のネットワークアドレスと所定の物理アドレスを、アドレス解決プロトコルの要求に対する応答として送信せることを電子計算機になさしめるプログラム。

【請求項13】

ネットワークに流れる情報を受信させ、

前記受信としてアドレス解決プロトコルの要求を受取ると、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスと共に物理アドレスに基づいて、ローカルネットワークを構成する予め定められた許可端末に相当するかを判断させ、

前記許可端末に相当しないと判断された場合に、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスが、前記ローカルネットワークで保護すべき端末によって使用されているか判断させ、

前記ローカルネットワークで保護すべき端末によって使用されている場合は、前記端末で組として使用されているネットワークアドレスと物理アドレスを、アドレス解決プロトコルの要求に対する応答として、一方、前記ローカルネットワークで保護すべき端末によって使用されていない場合は、前記アドレス解決プロトコルを要求した端末のネットワークアドレスと所定の物理アドレスを、アドレス解決プロトコルの要求に対する応答として送信せることを電子計算機になさしめるプログラムを格納した記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

10

20

30

40

50

本発明は、ネットワーク監視装置、ネットワーク監視方法、ネットワーク監視用プログラム及びネットワーク監視用プログラムが格納された記録媒体に関する。

【背景技術】

【0002】

許可されていない不正な端末がネットワークに接続されることを防止するために、不正端末の存在を検出し、さらにその不正端末がネットワーク上の他の装置と通信できなくなるようなネットワークシステムを実現することが求められている。IP (Internet Protocol) プロトコルを使用したネットワークにおいて、不正な端末の存在を監視するために、IETF (Internet Engineering Task Force) から発行されているRFC (Request For Comments) 2131に示されるDHCP (Dynamic Host Configuration Protocol) を応用した方式がある。この種の方式として、特開平8-186569号公報(特許文献1)に記載の技術では、アドレス管理装置がDHCPを使って割り当てたアドレス情報とネットワーク上を伝送されるパケットから抽出したアドレス情報を使って、アドレス管理装置がネットワーク内の不正な端末の存在を監視する。一方、特開2002-158701号公報(特許文献2)に記載の技術は、ケーブルモデム装置において、DHCPで割り当てたIPアドレスを管理しておき、割り当てたIPアドレス以外を使用したパケットがネットワークから入り込んできた場合に不正利用と判断し、そのパケットをケーブルモデム装置で廃棄する。

10

【0003】

また、OSI (Open Systems Intetconnection) 参照モデルにおける物理層のアドレス情報(IPアドレスなど)やデータリンク層のアドレス情報を使用せずに、監視装置とネットワークに接続された端末それぞれに予め専用ソフトウェアをインストールしておき、監視装置側の専用ソフトウェアと端末側の専用ソフトウェアが連携して、端末内の情報を取り出すことにより、監視装置が該当端末の状態を把握するシステムなどが知られている。

20

【0004】

【特許文献1】特開平8-186569号公報

【特許文献2】特開2002-158701号公報

【発明の開示】

【発明が解決しようとする課題】

30

【0005】

上記の従来の技術では、DHCPで割り当てたアドレス情報をもとに、ネットワーク上の不正な装置の存在を検出するものであるが、一般のネットワーク環境においてはDHCPでアドレスを割り当てる環境だけでなく、装置に固定的に割り付けたアドレスを使用するネットワーク環境も存在するのが一般的である。

【0006】

また、中継装置をネットワークの中に入れて、この中継装置で特定のフレームを常に廃棄することで、他の装置と通信をできなくする方式もあるが、このような中継装置を使うことによる、中継装置自体の障害時の考慮や、ネットワーク性能が中継性能に依存すること、あるいは、この不正な装置から送信されるフレームによるネットワークトラフィックなどについても考慮が必要となる。

40

【0007】

また、ネットワークに接続される装置の数が増えると、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担が大きくなるが、これらを軽減することについては考慮されていない。

【0008】

本発明の目的は、システム構成に大きく影響を受けずに、ネットワークを監視することが可能なものを提供することにある。DHCPでアドレスを割り当てる環境に限定せずに、装置に固定的に割り付けたアドレスを使用するネットワーク環境においても、許可されていない装置の存在を検出することである。その場合、許可されていない装置がネットワ

50

ークへ接続されたタイミングでその存在を検出することである。さらに、許可されていない装置の存在を検出するのみでなく、許可されていない装置自体がネットワークを使って他の装置と通信をできないようにさせること（以下、これを切り離しと呼ぶ）である。また、許可されていない装置と判断される装置を含めてネットワーク上に接続する装置に本発明に関わる専用ソフトウェアを予め入れておく必要が無いことによりネットワークセキュリティを強化することを目的とする。

【0009】

また、本発明は、許可されていない端末の存在を判断する際に使用するアドレス管理情報をネットワークのフレーム内の情報あるいはフレームの送信元アドレス情報から生成することにより、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担を軽減すること目的とする。

【0010】

また、本発明は、許可されていない装置として、一旦切り離れた装置を管理者等の判断で、外部から指示することにより、ネットワーク上の他の装置の使用者に影響を与えることなく、一旦切り離れた装置を使用できるようにすることである。また、同様に、接続されている装置を管理者等の判断で、外部からの指示することにより、ネットワーク上の他の装置の使用者に影響を与えることなく、接続されている装置を使用できなくなるように切り離すことである。これにより、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担を軽減すること目的とする。

【課題を解決するための手段】

【0011】

上記目的のうちの少なくとも1を達成するため、本発明では、ネットワークに流れる情報を受信し、前記受信としてアドレス解決プロトコルの要求を受取ると、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスと共に物理アドレスに基づいて、ローカルネットワークを構成する予め定められた許可端末に相当するかを判断し、前記許可端末に相当しないと判断された場合に、前記アドレス解決プロトコルの要求に含まれる送信元アドレスとしてのネットワークアドレスが、前記ローカルネットワークで保護すべき端末によって使用されているか判断し、前記ローカルネットワークで保護すべき端末によって使用されている場合は、前記端末で組として使用されているネットワークアドレスと物理アドレスを、アドレス解決プロトコルの要求に対する応答として、一方、前記ローカルネットワークで保護すべき端末によって使用されていない場合は、前記アドレス解決プロトコルを要求した端末のネットワークアドレスと所定の物理アドレスを、アドレス解決プロトコルの要求に対する応答として送信するように構成した。より具体的或いは代替的には、ネットワークに流れる情報を受信する受信手段と、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスがネットワークで用いられていることを示す情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置、ネットワークに接続された端末の切り離し指示あるいは接続指示を外部端末から受け付ける手段と、受け付けた指示が切り離し指示の場合には、該当端末を切り離すために、ネットワークにネットワークアドレスの重複状態を発生させるための情報を生成する手段を有することを特徴とするネットワーク監視装置、ネットワークに流れる情報を受信する受信手段と、ネットワークアドレス対となる該ネットワークアドレスより物理層側のアドレスを得るために送信された情報に基づいて、予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に、該ネットワークアドレス相当とは異なる物理層側アドレスを示す情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置、ネットワークに流れる情報を受信する受信手段と、複数の端末に順に情報が受信されるように、アドレスを含んだ情報を返信するよう要求する情報を送信し、返信された情報に基づいて、予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に、該ネットワークアドレス相当とは異なる該ネット

10

20

30

40

50

ワークアドレスより物理層側のアドレスを示す情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置あるいはネットワークに流れる情報を受信する受信手段と、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報が判断する判断手段と、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスについて重複状態を発生させるための情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置と構成し、また、接続を許可しない装置がネットワークに接続されたタイミングで、許可されていない装置の存在を検出し、さらに、ネットワークからこの許可されていない装置を切り離すことである。このとき、接続を行う装置側には本システム専用の処理を予め組み込んでおく必要が無いことを特徴とする。

10

【0012】

すなわち、具体的には、ネットワークに接続された複数の装置やネットワークの状態を監視する監視システムにおいて、監視システム宛フレームとネットワーク上のすべての装置宛のブロードキャストフレームを受信する手段またはネットワークを流れる全てのフレームを受信する手段と、装置に対するネットワークへの接続可否情報を登録する手段と、この登録された接続可否情報と前記フレームデータ内容を比較して接続可否を判断する手段と、接続を許可しないと判断した場合には該当装置を切り離すために、ネットワーク内にIPアドレスの重複状態を発生させるフレームを生成する手段と、監視システムからこのフレームをネットワークに送出し、ネットワーク内にIPアドレスの重複状態を発生させることにより該当装置をネットワークから切り離す手段を設けること、一方、切り離される該当装置には切り離しを行うための本システム専用処理を予め組み込んでおくことが不要であること、としたことを特徴とする。

20

【0013】

これにより、例えば、接続が許可されていない、個人の持ち込みPC (Personal Computer) がウイルスに汚染されていた場合においても、本監視システムはPCがネットワークに接続したことを検出し、物理層のレベルで該当PCを切り離す。これにより、汚染されたフレームはネットワークに送出されなくなり、ネットワーク上の他の装置に対するウイルス汚染の拡散防止に有効となる。一方、予め組み込まれた専用ソフトウェアと連携して、通信をさせないようにする方式では、この専用ソフトウェアが組み込まれていない許可されていないPCを接続された場合には効果が期待できない。しかし、本発明では許可されていないPCと判断される装置を含めてネットワーク上に接続する装置には本発明に関わる専用ソフトウェアを予め組み込んでおく必要が無いことから、予め組み込まれた専用ソフトウェアと連携して、通信をさせないようにする方式に比べて、ネットワークセキュリティを強化できる。

30

【0014】

さらに、上記目的を達成するための本発明の特徴はネットワーク監視システムがネットワークを監視することによって、ネットワークに接続された装置がもつアドレス情報を収集し、順次アドレス情報を順次作り上げていき、これをネットワークへの接続可否情報として使用することができるようにすることを特徴としている。

40

【0015】

具体的には、ネットワークに接続された複数の装置やネットワークの状態を監視する監視システムにおいて、監視システム宛フレームとネットワーク上のすべての装置宛のブロードキャストフレームを受信する手段またはネットワークを流れる全てのフレームを受信する手段と、装置に対するネットワークへの接続可否情報を登録する手段と、この登録された接続可否情報と前記フレームデータ内容を比較して接続可否を判断する手段と、接続を許可しないと判断した場合には該当装置を切り離すために、ネットワーク内にIPアドレスの重複状態を発生させるフレームを生成する手段と、監視システムからこのフレームをネットワークに送出し、ネットワーク内にIPアドレスの重複状態を発生させることに

50

より該当装置をネットワークから切り離す手段を設けること、一方、切り離される該当装置には切り離しを行うための本システム専用処理を予め組み込んでおくことが不要であること、さらに、監視システムはネットワーク上の全ての装置または指定された1つ以上の装置に対してARPフレームの発行を誘発するフレームを発行する手段と各装置から発行されたARPフレームからIPアドレスとMACアドレス情報を抽出する手段、のうち少なくとも一つの手段を設け、さらに、この抽出したIPアドレスとMACアドレスを組み合わせて、ネットワークに接続された装置のアドレス情報を一意的に生成する手段と、生成された一意的なアドレス情報の要素分類をキーにして外部から昇順もしくは降順に並べ替える手段と、生成された一意的なアドレス情報の個々の要素に対して外部から有効あるいは無効の設定を可能とする手段を設け、これらの手段により装置アドレス情報を生成し、装置に対するネットワークへの接続可否情報としてこの装置アドレス情報を使用することを特徴とする。

10

【0016】

これにより、ネットワークに接続される多くの装置のアドレス情報の作成において、例えば、別の手段により、接続許可申請書に記載されたアドレス情報をもとにネットワーク管理者が装置に対するネットワークへの接続可否情報を作成する場合に対して、ネットワーク管理者や装置所有者の申請処理等に関わる負担軽減に有効となる。

【0017】

また、上記目的を達成するための本発明の特徴は、許可されていない装置として、一旦切り離れた装置を管理者等の判断で、監視システムから指示することにより、ネットワーク上の他の装置の使用に与えることなく、該当装置を使用できるようにすること、また、逆に、接続されている装置を使用できなくなるように切り離すことである。

20

【0018】

すなわち、具体的には、監視システム宛フレームとネットワーク上のすべての装置宛のブロードキャストフレームを受信する手段またはネットワークを流れる全てのフレームを受信する手段と、装置に対するネットワークへの接続可否情報を登録する手段と、この登録された接続可否情報と前記フレームデータ内容を比較して接続可否を判断する手段と、接続を許可しないと判断した場合には、該当装置を切り離すために、ネットワーク内にIPアドレスの重複状態を発生させるフレームを生成する手段と、監視システムからこのフレームをネットワークに送出し、ネットワーク内にIPアドレスの重複状態を発生させることにより該当装置をネットワークから切り離す手段と、一旦切り離された装置を許可された装置に外部から変更するための手段と、一旦切り離された装置が他の装置と通信できるようにするための接続フレームを生成する手段と、監視システムからこの接続フレームをネットワーク上に接続されている全ての装置に対して送出することによって、一旦切り離された装置が他の装置と通信できるようにする手段と、接続されている装置を切り離すために外部から変更するための手段を備えたことであり、一方、切り離される該当装置には切り離しや接続を行うための本システム専用処理を予め組み込んでおくことが不要であることを特徴とする。

30

【0019】

これにより、例えば、接続が許可されていないために切り離れたPCに対して、所定の手続きが行われた後に、ネットワーク管理者が該当装置を許可する場合において、他の装置の使用にも負担をかけることなく、該当PCをネットワークに組み入れて使用できる環境を提供できることになり、ネットワーク管理者の負担軽減にも有効となる。

40

【0020】

上記した本発明の特徴および上記した以外の発明の特徴は、以下の記載によりさらに明確とされる。

【0021】

本発明では、ネットワーク監視システムはネットワーク内を流れるフレームデータのうち、ネットワークに接続した装置が発行するARPフレームを監視し、このARPフレームからARPフレームを送出した装置のIPアドレスとMACアドレスを抽出する手段を

50

使用する。また、装置に対するネットワークへの接続可否情報として、外部から、ネットワークへの接続を許可する装置のＩＰアドレスあるいはＭＡＣアドレスのうち少なくとも１つのアドレス情報が監視システムに登録されている。この登録手段により登録されたアドレス情報とＡＲＰフレームから抽出したアドレス情報を比較して、一致しない場合には、許可しない装置であるとみなし、該当装置を切り離す手段を実行する。該当装置を切り離すために、ＩＰアドレスの重複状態を発生させるフレームを生成する手段を使用して、前記ＡＲＰフレームから抽出した該当装置のＩＰアドレスとネットワーク監視システムのＭＡＣアドレスを組み合わせるフレームを生成する。その後、監視システムからこのフレームをネットワークに送出し、ネットワーク内にＩＰアドレスの重複状態を発生させる。本フレームを受け取った該当装置はＩＰアドレスの重複状態が発生したことを検知して、自律的にネットワークから離脱する。これにより、許可されていない該当装置がネットワークから切り離されることになる。

10

【００２２】

さらに、本発明では、ネットワーク監視システムはネットワーク内を流れるフレームデータのうち、ネットワークに接続された装置が自発的に発行するＡＲＰフレームを監視し、このＡＲＰフレームからＡＲＰフレームを送出した装置のＩＰアドレスとＭＡＣアドレスを抽出する手段を使用する。これにより、ネットワークに接続された装置のアドレス情報が順次作り上げられていく。一方、ネットワーク上の全ての装置または指定された１つ以上の装置に対してＡＲＰフレームの発行を誘発するフレームを発行することにより、各装置から発行されたＡＲＰフレームに対しても同様の処理を行い、ネットワークに接続された装置のアドレス情報を順次作り上げていく。また、この順次作り上げられたアドレス情報をもとに一意的に生成する手段を使って、一意的なアドレス情報を生成する。さらに、この生成された一意的なアドレス情報の要素分類をキーにした外部から昇順もしくは降順に並べ替える手段と、生成された一意的なアドレス情報の個々の要素に対して外部から有効あるいは無効の設定を可能とする手段を提供する。この提供された手段を使用して生成された、装置アドレス情報のＩＰアドレスあるいはＭＡＣアドレスのうち少なくとも１つのアドレス情報を装置に対するネットワークへの接続可否情報として使用する。

20

【００２３】

さらに、本発明では、許可されない装置として切り離された装置を許可された装置にするために、外部からの変更指示にもとづき、この切り離された装置が他の装置と通信できるようにするための接続フレームを生成する手段を使用する。このとき、この許可されていない装置が発行したＡＲＰフレームから抽出したＩＰアドレスとＭＡＣアドレスを、装置に対するネットワークへの接続可否情報として新たに登録すると同時に、これらのアドレスを組み合わせるフレームを生成する。その後、監視システムからこのフレームをネットワークに接続されている全ての装置宛てに送出し、各装置が通信を行うために持っているＩＰアドレスとＭＡＣアドレスの対応表を更新させる。これにより、一旦切り離された装置はネットワーク上の他の装置と通信ができる環境が整うことになる。また、接続されている装置を切り離すために、外部からの変更指示にもとづき、接続されている装置が他の装置と通信できないようにするためのＩＰアドレス重複状態発生フレームを生成する手段を使用する。その後、監視システムからこのフレームをネットワークに接続されている全ての装置宛てに送出する。これにより、これまで接続されていた装置をネットワーク上の他の装置と通信ができなくさせることができる。

30

40

【００２４】

また、ネットワークに流れる情報を受信する受信手段と、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスがネットワークで用いられていることを示す情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置を構成する（構成１）。

【００２５】

構成１において、端末に対応してネットワークへの接続可或は否に関する情報を登録す

50

る手段と、この登録された接続可或は否に関する情報と受信情報を比較することで、許可の可否を判断することを特徴とするネットワーク監視装置を構成する（構成2）。

【0026】

構成2において、前記受信手段宛の情報とネットワークの複数端末宛のブロードキャスト情報あるいはマルチキャスト情報を受信、またはネットワークを流れる実質的に全ての情報を受信することを特徴とするネットワーク監視装置を構成する（構成3）。

【0027】

構成3において、該許可されないと判断された端末に切り離し専用手段が設置されるか否かにかかわらず、該端末がネットワークから切り離されるよう構成されることを特徴とするネットワーク監視装置を構成する（構成4）。 10

【0028】

構成1において、接続を許可しない端末がネットワークに存在することを検出したことを、または、接続を許可しない端末をネットワークから切り離したことを、外部端末に通知する手段と、ネットワークに接続された端末の切り離し指示あるいは接続指示のうち少なくとも一つを外部端末から受け付ける手段と、受け付けた指示が切り離し指示の場合には、ネットワークアドレスの重複状態を発生させるための情報を生成する手段を有することを特徴とするネットワーク監視装置を構成する（構成5）。

【0029】

構成5において、受け付けた指示が接続指示の場合には、ネットワーク内にネットワークアドレスの重複状態を解消させるための情報を生成する手段を有することを特徴とするネットワーク監視装置を構成する（構成6）。 20

【0030】

また、ネットワークに接続された端末の切り離し指示あるいは接続指示を外部端末から受け付ける手段と、受け付けた指示が切り離し指示の場合には、該当端末を切り離すために、ネットワークにネットワークアドレスの重複状態を発生させるための情報を生成する手段を有することを特徴とするネットワーク監視装置を構成する（構成7）。

【0031】

構成7において、受け付けた指示が接続指示の場合には、ネットワーク内にネットワークアドレスの重複状態を解消させるための情報を生成する手段を有することを特徴とするネットワーク監視装置を構成する（構成8）。 30

【0032】

構成1乃至8において、ネットワークの端末から発行されるアドレス要求情報を監視し、このアドレス要求情報からネットワークアドレスと物理層側アドレス情報を抽出する手段と、ネットワーク上の全ての端末または指定された1つ以上の端末に対してアドレス要求情報の発行を誘発する情報を発行する手段と、各端末から発行されたアドレス要求情報からネットワークアドレスと物理層側アドレス情報を抽出する手段、のうち少なくとも一つの手段を設け、さらに、この抽出したネットワークアドレスと物理層側アドレスを組み合わせ、ネットワークに接続された端末のアドレス情報を一意的に生成する手段と、生成された一意的なアドレス情報の要素分類に応じて外部から昇順もしくは降順に並べ替える手段と、生成された一意的なアドレス情報の個々の要素に対して外部から有効あるいは無効の設定を可能とする手段を設け、これらの手段により端末アドレス情報を生成し、端末に対するネットワークへの接続可否情報としてこの端末アドレス情報を使用することを特徴とするネットワーク監視装置を構成する（構成9）。 40

【0033】

構成1乃至8において、切り離し手段として、許可されない端末がネットワークアドレスの重複状態を検出するために発行するアドレス要求情報に対して、特定の物理層側アドレスを設定したアドレス要求応答情報を生成する手段を有することを特徴とするネットワーク監視装置を構成する（構成10）。

【0034】

構成1乃至8において、切り離し手段として、許可されない端末がアドレス解決のため 50

に発行するアドレス要求情報に対して、特定の物理層側アドレスを設定したアドレス要求応答情報を生成する手段を有することを特徴とするネットワーク監視装置を構成する（構成11）。

【0035】

構成1乃至8において、該当端末をネットワークに接続する手段として、アドレス要求情報から得られた該当特定端末の物理層側アドレスと該当端末のネットワークアドレスとを使用して、アドレス要求応答情報を生成する手段を設け、このアドレス要求応答情報をネットワーク内の各端末に向けることを特徴とするネットワーク監視装置を構成する（構成12）。

【0036】

構成10または11において、特定の物理層側アドレスを設定したアドレス要求応答情報を生成する手段として、許可されない端末のネットワークアドレスがネットワーク内の他の端末で現在使用されているか否かを判断する手段を設け、このネットワークアドレスがすでに他の端末で使用されている場合にはアドレス要求応答情報内の送信元物理層側アドレスを端末同一ネットワークアドレスを使用している他の端末の物理層側アドレスとし、このネットワークアドレスが他の端末で使用されていない場合にはアドレス要求応答情報内の送信元物理層側アドレスを監視装置の物理層側アドレスもしくはネットワーク上に存在しえない物理層側アドレスを設定したアドレス要求応答情報を生成する手段を設け、このアドレス要求応答情報をネットワークに送出させることにより、許可されない端末にネットワークアドレス重複状態が発生したことを認識させ、許可されない端末がネットワーク上の許可されない端末以外の端末と通信ができない状態にするのと同時に、同一ネットワークアドレスをすでに使用していた端末とネットワーク上の許可されない端末以外の端末との通信が継続できることを特徴とするネットワーク監視装置を構成する（構成13）。

【0037】

構成1乃至8において、該当ネットワークのネットワークアドレス体系のホスト番号部がとりうる最小値から最大値までの全てのホスト番号のうち、接続可否のチェックを行う端末のホスト番号の範囲とチェックを行うタイミング情報を設定する手段と、この範囲のホスト番号を使ったチェック用ネットワークアドレスを生成する手段と、このチェック用ネットワークアドレスを使って、相手端末からの応答を期待できる要求情報を生成する手段と、この要求情報を前記設定されたタイミング情報にもとづいたタイミングで監視装置から送出し、その応答の情報の存在またはその情報内容と、端末に対するネットワークへの接続可否情報とを比較して接続可否を判断することを特徴とするネットワーク監視装置を構成する（構成14）。

【0038】

構成14において、相手端末からの応答を期待できる要求情報を生成する手段として、ICMP要求情報あるいはアドレス要求情報を生成することを特徴とするネットワーク監視装置を構成する（構成15）。

【0039】

構成1乃至8において、端末に対するネットワークへの接続可否情報として、端末のネットワークアドレスおよび物理層側アドレスのうち少なくとも1つを、あるいは、接続許可時間帯および接続不許可時間帯のうち少なくとも1つを、あるいは前回接続した時刻からある閾値以上の経過時間がたった場合にはその接続を拒否するために使用される時刻情報を、あるいは、前回接続した時刻からある閾値以上の経過時間がたった場合には現在接続されている端末を切り離すために使用される時刻情報を、あるいは、これまでに接続を許可されなかった回数、あるいは、許容されるネットワークトラフィックの閾値、あるいは端末のネットワークへの接続許可台数、あるいは端末の所有者情報、あるいはこれらの少なくとも1つ以上を組み合わせたものを、使用することを特徴とするネットワーク監視装置を構成する（構成16）。

【0040】

また、ネットワークに流れる情報を受信する受信手段と、ネットワークアドレスに対となる該ネットワークアドレスより物理層側のアドレスを得るために送信された情報に基づいて、予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に、該ネットワークアドレス相当とは異なる物理層側アドレスを示す情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置を構成する（構成１７）。

【００４１】

また、ネットワークに流れる情報を受信する受信手段と、複数の端末に順に情報が受信されるように、アドレスを含んだ情報を返信するよう要求する情報を送信し、返信された情報に基づいて、予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に、該ネットワークアドレス相当とは異なる該ネットワークアドレスより物理層側のアドレスを示す情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置を構成する（構成１８）。

10

【００４２】

また、ネットワークに流れる情報を受信する受信手段と、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報か判断する判断手段と、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスについて重複状態を発生させるための情報をネットワークに流す送信手段を有することを特徴とするネットワーク監視装置を構成する（構成１９）。

【００４３】

20

また、ネットワークに流れる情報を受信し、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報か判断し、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスがネットワークで用いられていること示す情報をネットワークに流すネットワーク監視方法を構成する（構成２０）。

【００４４】

また、ネットワークに流れる情報を受信し、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報か判断し、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスがネットワークで用いられていること示す情報をネットワークに流すことを電子計算機になさしめるプログラムを構成する（構成２１）。

30

【００４５】

また、ネットワークに流れる情報を受信し、ネットワーク接続のために送信された情報に基づいて予め定められた許可端末に相当する情報か判断し、許可端末に相当しないと判断された場合に前記情報を送信した端末を特定するアドレスがネットワークで用いられていること示す情報をネットワークに流すことを電子計算機になさしめるプログラムを格納した記録媒体を構成する（構成２２）。

【発明の効果】

【００４６】

本発明では、システム構成に大きく影響を受けずに、ネットワークを監視することが可能となる。

40

【発明を実施するための最良の形態】

【００４７】

以下、本発明の一実施例を図を用いて詳細に説明する。なお、以下、通信プロトコルはＩＰプロトコル（ＴＣＰ／ＩＰなど）、ネットワークはオフィス等で多く用いられているＬＡＮを使用するシステムを用いて説明する。

【００４８】

<システムの全体構成>

はじめに、本発明が対象とするネットワーク監視システムの全体構成を図２に示す。複数の装置２０１～２０３が標準的なＬＡＮ２１０に接続されている。ＰＣなどの各装置には業界標準的なＯＳ（Operating System）が搭載されており、このＯＳのなかには業界標

50

準の通信プロトコル（ＩＰプロトコルなど）が実装されており、このプロトコルに対応したネットワーク層のアドレス（ＩＰアドレス）や物理層のアドレス（ＭＡＣアドレス）が割り当てられている。各装置に搭載された業務プログラムはそれぞれの装置の業務プログラムと通信を行いながら、全体の業務を進める。一方、ネットワーク監視システム２００はこのＬＡＮに許可されていない装置が接続された場合、これを検出し、さらに、この装置をＬＡＮから切り離すために監視をしている。なお、「物理層側」とは対象層（例えばネットワーク層）、に対して物理層の側であることを示す。

【００４９】

装置が他の装置と通信を行うためには図３にあるようなＩＰフレーム３００を使ってＬＡＮ上にデータを送出するが、相手先にデータを到達させるためには宛先ＭＡＣアドレス 301 と ＩＰヘッダ 302 に含まれる宛先 ＩＰアドレス 303 の２つのアドレスが必要である。

10

【００５０】

一般に、ネットワークに接続された装置が立ち上がった段階では、該当装置においては宛先の装置のＩＰアドレスはわかっているものの、宛先装置のＭＡＣアドレスを所持していない。このため、この宛先装置のＭＡＣアドレスを取得するために、ＲＦＣ８２６で規定されたＡＲＰ（Address Resolution Protocol）プロトコルを用いる。図４にこのＡＲＰプロトコルフレーム４００のフォーマットを示す。

【００５１】

ＡＲＰフレームのフレームデータ４０１において、アドレス情報関連部は送信元ＭＡＣアドレス４０２，送信元ＩＰアドレス４０３，探索ＭＡＣアドレス４０４および探索ＩＰアドレス４０５で構成される。また、ＯＰ（オペレーションフィールド）において、ＡＲＰの種別（ＡＲＰ要求あるいはＡＲＰ応答）が区別される。

20

【００５２】

一方、このＡＲＰプロトコルを用いて宛先装置のＭＡＣアドレスを得るための典型的な通信例を図５に示す。ここでは装置ｄ５０４において、装置ｂ５０２宛にデータを送るイベント５０５が発生した場合、装置ｄ５０４は宛先装置ｂ５０２のＭＡＣアドレスを取得する必要がある。そのため、装置ｄ５０４は宛先ＩＰアドレスが装置ｂ５０２のＩＰアドレスＩＰｂを含むＡＲＰ要求フレーム５０６をネットワーク上の全ての装置宛にブローキャスト方式で送信する。それを受信した各装置はＡＲＰフレーム内のＩＰアドレスＩＰｂが自分自身に対する要求であると認識した場合には、自装置のＭＡＣアドレスを設定したＡＲＰ応答フレームを装置ｄ５０４に送り返す。本例では、装置ｂ５０２はＡＲＰフレーム内のＩＰアドレスＩＰｂをみて、これが自分自身に対する要求であると認識し、自装置のＭＡＣアドレスを設定したＡＲＰ応答フレーム５０７を装置ｄ５０４に送り返す。これにより、装置ｄ５０４は宛先である装置ｂ５０２のＭＡＣアドレス（ＭＡＣｂ）を取得することができたので、このＩＰアドレス（ＩＰｂ）とＭＡＣアドレス（ＭＡＣｂ）を使ってデータ通信５０８を行う。

30

【実施例１】

【００５３】

<構成>

40

以下、第１の実施例について説明する。

【００５４】

本発明のネットワーク監視システムの構成を図１に示す。ネットワーク監視システム２００はネットワーク１２０からフレームを受信するフレーム受信処理部１０２，ネットワークに接続される装置に対する接続可否情報を管理する接続可否情報管理処理部１０４，接続された装置が許可されている装置であるか否かを判断する接続可否判断処理部１０６，該当装置をネットワークから切り離すためのＩＰアドレス重複状態発生フレーム生成処理部１０５，生成されたフレームをネットワークへ送信するフレーム送信処理部１０１，フレームの送信タイミングを制御するタイミング情報管理処理部１０８，接続を許可されない装置を検出したことや該当装置を切り離したことを外部に通知するための外部通知処

50

理部107, 外部からの装置の切り離し指示や装置の接続指示等を受け付ける外部指示受付処理部109, いったん切り離された装置を接続するためのフレームを生成する接続用フレーム生成処理部110, 装置に対する接続可否チェック用IPアドレスを生成するための接続可否チェック用IPアドレス生成処理部112, そのIPアドレス生成のために予め登録されたアドレス管理情報113, 生成された接続可否チェック用IPアドレスのフレームを生成するためのチェック用フレーム生成処理部111, ネットワークから受信したフレーム内容からネットワークに接続されている装置のアドレス情報を生成するための装置アドレス情報生成処理部103, 外部から指示を行う外部装置114からなる。ここで、IPアドレス重複状態とは、ネットワークに接続された複数の装置が同一のIPアドレスを誤って使用している状態を指している。

10

【0055】

＜許可されていない装置の切り離し処理＞

図1を用いて、許可されていない装置の切り離し処理を説明する。

【0056】

ネットワーク監視システムはブロードキャスト方式を使ってネットワーク120上のすべての装置宛に送られるARP要求フレームをフレーム受信処理部102で受信する。そして、ARP要求フレームを発行した装置を特定するために、このフレームから該当装置のアドレス情報であるIPアドレスとMACアドレスを抽出する。一方、このネットワークに接続することを許可されている装置のアドレス情報は接続可否情報管理処理部104に予め格納されているので、接続可否判断処理部106において前記ARPフレームから抽出したアドレス情報が、接続可否情報として登録されているか否かのチェックが行われる。もし、登録されていない場合には許可されていない装置が接続されたと判断し、該当装置をネットワークから切り離す処理を実行する。本処理を実行するために、IPアドレス重複状態発生フレーム生成処理部105において、該当装置と同じIPアドレスをもった装置を論理的にネットワーク内に生成するためのフレームをつくり、フレーム送信処理部101を経由して、このフレームをネットワーク120内の全装置宛に送信し、ネットワーク内をIPアドレス重複状態とする。このとき、ネットワークへの送信タイミングはタイミング情報管理処理部108に従い送信される。このフレームを受信した該当装置（前記ARP要求フレームを発行した装置）はネットワーク内に自装置と同じIPアドレスをもった他装置が存在する（IPアドレス重複状態）と判断し、自律的にネットワークから離脱する。

20

30

【0057】

これにより、許可されていない装置をネットワークから切り離すことができる。

【0058】

＜許可された装置の外部からの切り離し処理＞

一方、前記切り離し処理は接続可否判断処理部106から実行されたが、この切り離し処理は外部装置114からの指示を受けて実行されることもある。これについては実施例3で説明する。

【0059】

以上、切り離し処理について述べたが、フレーム受信処理においては監視システム宛フレームもしくはネットワーク上のすべての装置宛のブロードキャストフレームのみを受信しているが、ネットワーク上を流れるすべてのフレームを受信して、その後、本発明で必要なフレームを抽出してもよい。

40

【0060】

＜構成処理部＞

以下、許可されていない装置の切り離し処理に関する構成処理部について詳細に説明する。

【0061】

接続可否情報管理処理部104で管理される情報を図6に示す。接続可否情報600はネットワークへの接続を許可する装置のMACアドレス601と接続を許可する装置のI

50

Pアドレス602の組み合わせで構成されており、ネットワークに装置が接続された場合、接続可否判断処理部106において、接続されたこの装置のIPアドレスとMACアドレスと、接続可否情報の内容とが比較されることにより、該当装置の接続可否判断がなされる。この接続可否情報はあらかじめ外部から登録されたものを使用してもよいし、監視システムが動作中に外部から更新されたものでもよい。また、装置アドレス情報生成処理部103から生成された情報も接続可否情報として使用できる。

【0062】

図6ではMACアドレスとIPアドレスの1対1の組み合わせであるが、図7に示すように接続可否情報700としてMACアドレス(MAC1)とIPアドレス(IP1)の組み合わせ701、IPアドレス(IP2)のみの場合702、MACアドレス(MAC3)のみの場合703、あるいはIPアドレスの範囲指定(IP4~IP5)の場合704などとすることができる。これらはネットワークのセキュリティポリシーやネットワーク環境あるいは、運用方針などに従って使い分けられることになる。

【0063】

また、図8に示すように、接続可否情報800として、装置毎にネットワークへの接続許可時間帯801、接続不許可時間帯802および所有者情報803を使用することもできる。例えば、ネットワークへの接続が許可されている装置1の場合804では、時刻aから時刻bの間だけは接続を許可するが、これ以外の時間帯は許可をしない。逆に、装置3の場合805では時刻eから時刻fの間はネットワークへの接続を許可しない場合などである。なお、図8では装置毎に時間帯を設定しているが、これらは装置毎でなくとも、例えばネットワーク全体で決めてもよい。所有者情報803は装置の使用者を特定し、例えば、その使用者権限によりネットワークへの接続を許可したり、許可しなかったりする場合の判断材料に使用するものである。これらの、所有者権限については、例えば、ディレクトリシステムと連携することで、さらにきめ細かな接続可否判断が可能となる。

【0064】

また、図9に示すように、接続可否情報900は装置毎に、前回の接続時刻901と、前回接続した時刻からある閾値以上の経過時間がたった場合には新たな接続を拒否するために使用される接続拒否用経過時間902と、前回接続した時刻からある閾値以上の経過時間がたった場合には現在接続されている装置を切り離すために使用される接続中断用経過時間903と、接続を許可されなかった回数904などをもつこともできる。これはたとえば、許可されているPCなどの装置であっても、一定期間以上、ネットワークに接続されていない装置は、例えば、ウイルスチェックパターンが最新のものに更新されていないため、最近のウイルスに汚染されている場合も想定される。そのような場合において、前回接続してからの経過時間が接続拒否用経過時間902を超えている場合には、ネットワークへの接続を許可しないことにより、ネットワークへの悪影響を及ぼす可能性を下げるうえで有効である。同様に、たとえば、許可されている装置であっても、例えば、サービス運用に合わせて、連続して接続をした状態を維持する時間に制限をつけたい場合がある。そのような場合において、今回接続した時刻からの経過時間が接続中断用経過時間903を超えた場合には該当装置を切り離すことにより、きめこまかなネットワーク運用が可能となる。例えば、装置1の場合905においては、接続拒否用経過時間(時間1)以上たった後は装置1をネットワークに接続しようとしてもできないし、一方、装置1をネットワークに接続した後、接続中断用経過時間(時間a)がたつとネットワークから切り離されることになる。

【0065】

なお、接続可否情報900においては接続拒否用経過時間902および接続中断用経過時間903を装置毎にもっているがそれぞれをシステム全体でもってかまわない。

【0066】

また、図では示していないが、ネットワークへ接続される装置の全台数を一定以下に抑えることで、ネットワークトラフィックを一定以下に抑えることを目的に、接続可否情報として、装置のネットワークへの接続許可台数やネットワークトラフィック状態も利用す

10

20

30

40

50

ることができる。

【0067】

タイミング情報管理処理部108はネットワークに送出するフレームの送出タイミングを制御するものである。図10に示すように、タイミング情報1000はフレーム種別毎に送信タイミング1001, 1002, 1003, 1004とフレームの送出繰り返し回数1005のうち少なくとも1つ以上を組み合わせた形で使用されている。

【0068】

例えば、IPアドレス重複状態発生用フレーム1010の場合には、フレーム送出要求があると、即時にネットワークへ送出される。アドレス収集用フレーム1040の場合には、T5秒のインターバル1とT6秒インターバル2従って、ネットワークへ送出される。

10

【0069】

どの送信タイミングでネットワークへ送出されるかはセキュリティ管理やネットワークシステムの運用方針等で決まるものである。これにより、ネットワークの負荷状態や装置の使用状況に応じたきめこまかな制御が可能となる。なお、このタイミング情報はあらかじめ外部から登録されたものを使用してもよいし、監視システムが動作中に外部から更新されたものであってもよい。

【0070】

IPアドレス重複状態発生フレーム生成処理部105はネットワーク上にIPアドレスが重複した状態、すなわち、同一IPアドレスを複数の装置が使用している状態を作るために、該当フレームを作成するものである。

20

【0071】

例えば、PCをネットワークに接続して、該当PCを立ち上げると、該当PCのIPアドレスが他の装置に使用されていないことを該当PCのOS (Operating System) がチェック処理 (IPアドレスの重複チェック処理) を行う。

【0072】

このとき、図11に示すようなARP要求フレーム1100が該当PCからネットワークに対してブロードキャストされる。このとき、送信元アドレス1101のIPアドレスは該当PCのIPアドレス (IP1) 1112を、MACアドレスは該当PCのMACアドレス (MAC1) 1111である。一方、探索アドレス1102のIPアドレスは該当PCのIPアドレス (IP1) 1114を、MACアドレス1113は0が設定される。監視システムでは受信したこのARP要求フレーム1100を利用して、図12に示すようにIPアドレス重複状態発生フレーム-a1200もしくは、IPアドレス重複状態発生フレーム-b1250を生成する。具体的に以下に詳細に説明する。ここでのポイントは許可されていないPC (装置) がネットワークに接続したときのネットワーク内の他の装置への影響、つまり、他の装置間の通信への影響を見極めることである。許可されていないPCがどのようなIPアドレスを使ってネットワークに接続してくるかによってその影響が決まる。例えば、許可されていないPCがネットワーク内の他の装置が使用しているIPアドレスを使用していた場合には、ネットワーク内の他の装置が通信時に使用している各装置内のARP管理テーブル内の情報が破壊され、通信ができなくなる。そのため、該当PCをネットワークから切り離すだけでなく、同時に、各装置がもつ破壊されたARP管理テーブルを修復し、他の装置間の通信が継続できるようにすることがポイントである。すなわち、許可されていないPCがネットワーク内の他の装置が使用しているIPアドレスを使用していなかった場合にはIPアドレス重複状態発生フレーム-a1200を生成する。具体的には、このとき、送信元アドレス1201のIPアドレスは該当PCのIPアドレス (IP1) 1212を、MACアドレスは監視システムのMACアドレス (MACx) 1211とする。一方、探索アドレス1202のIPアドレスは該当PCのIPアドレス (IP1) 1214を、MACアドレスは該当PCのMACアドレス (MAC1) 1213を設定する。なお、ここでは送信元アドレス1201のMACアドレスとして監視システムのMACアドレス (MACx) 1211を使用した。このMACアド

30

40

50

レスはネットワーク内の他の装置が使用しないMACアドレスのビットパターンであってもよい。

【0073】

一方、許可されていないPCがネットワーク内の他の装置が使用しているIPアドレスを使用していた場合にはIPアドレス重複状態発生フレーム-bを生成する。具体的には、このとき、送信元アドレス1251のIPアドレスは該当PCのIPアドレス(IP1)1262を、MACアドレスは同一IPアドレスを使っていた他の装置のMACアドレス(MACy)1261とする。一方、探索アドレス1252のIPアドレスは該当PCのIPアドレス(IP1)1264を、MACアドレスは該当PCのMACアドレス(MAC1)1263を設定する。

10

【0074】

このように設定したフレームをネットワーク内の全装置宛に送出することにより、ネットワーク内にIPアドレス重複状態を発生させる。ネットワークから本フレームを受信した該当PCは自分が使用したIPアドレスは重複状態であることを認識(自装置以外の装置が同一のIPアドレスを使用していることを認識)し、ネットワークから自律的に離脱する。また、同時に、破壊された各装置がもつARP管理テーブルを修復し、他の装置間の通信が継続できるようにする。

【0075】

なお、本処理部は接続可否判断処理部106で接続を許可しないと判断された場合、あるいは、外部装置114から特定の装置を切り離す要求指示を外部指示受付処理部109で受け付けた場合にも実行される。

20

【0076】

図13に許可されていない装置の切り離し処理の一例をフローチャートに示す。この例では処理1300で受信したフレームを特定するためにフレームヘッダ内のプロトコル種別をチェックし、プロトコルがARP以外の場合には処理を終了する。なお、このプロトコル種別は図3のIPフレーム300内のタイプ304で識別することができる。ARPの場合には処理1310において監視システム自身が発行したARPについては処理対象外として処理を終了する。処理1320において、受信したARPの種別がARP要求フレームであるか、ARP応答フレームであるかを判断し、ARP要求フレームのみを以降の処理対象とする。処理1330において該当ARPフレーム1100から送信元のIPアドレスと送信元のMACアドレスを抽出し、処理1340において該当アドレスが接続可否情報テーブル900に登録されているか、さらに、処理1350において接続可否情報テーブル900の許可条件を満足しているか否かをチェックして、登録されていない場合、あるいは満足していない場合には該当装置を切り離し対象として選択する。

30

【0077】

処理1360において、許可されていない装置のIPアドレスがネットワーク内の他の装置で現在使用しているかどうかをチェックし、他の装置で使用されていない場合には処理1370において、ネットワーク内にIPアドレス重複状態を発生させるためにIPアドレス重複状態発生フレーム-aを生成する。このとき、送信元MACアドレスを監視システムのMACアドレスとする。許可されていない装置のIPアドレスがネットワーク内の他の装置で現在使用されている場合には処理1380において、ネットワーク内にIPアドレス重複状態を発生させるためにIPアドレス重複状態発生フレーム-b1250を生成する。このとき送信元MACアドレスを、同一IPアドレスを現在使用している他の装置のMACアドレスとする。処理1390においてタイミング管理情報テーブル1000からフレーム送信タイミング情報を抽出し、このタイミング情報を使用して処理1400において上記で生成したIPアドレス重複状態発生フレーム(IPアドレス重複状態発生フレーム-aもしくはIPアドレス重複状態発生フレーム-b1250を)をネットワークへ送信する。ここで、処理1340において接続可否情報テーブル900の代わりに接続可否情報テーブル600, 700, 800を用いてもよい。

40

【0078】

50

接続可否チェック用 I P アドレス生成処理部 1 1 2 について説明する。

【0079】

これまでの説明ではブロードキャスト方式を使ってネットワーク 1 2 0 上のすべての装置宛に送られてくる A R P 要求フレームに対する処理の流れを説明したが、この処理を補完するために下記処理を行う。これは例えば、監視システムを何らかの理由で一度停止し、再度立ち上げた場合を想定すると、監視システムが停止中に許可されていない装置がネットワークに接続された場合にはこの許可されていない装置の存在を検出することが遅れることがある。図 1 を使って以下説明する。監視システムが許可されていない装置の存在を能動的に検出するために、ネットワーク上の全ての装置または指定された 1 つ以上の装置に対して A R P フレームの発行を誘発するためのフレームを発行する。そのために、発行対象となる装置の決定はアドレス管理情報 1 1 3 にあらかじめ登録されているものを使用する。ここには、例えば、対象となる装置の I P アドレスの範囲指定やチェック用フレーム送出のタイミング情報が登録されている。また、I P アドレスの範囲指定がされていない場合には該当ネットワークのアドレス体系およびネットマスク情報をもとにネットワーク上のすべてのホストの I P アドレスを生成して発行することになる。例えば、図 1 8 に示すような該当ネットワークの I P アドレスやネットマスク情報をもとにネットワーク上のすべてのホストの I P アドレスを生成して発行することになる。図 1 8 においては、I P アドレス 1 8 0 0 は 1 7 2 . 2 0 . 1 0 0 . 5 2、サブネットマスク 1 8 0 1 は 2 5 5 . 2 5 5 . 2 5 5 . 1 9 2 であるため、ネットワークアドレス部は 2 6 ビット、ホスト部は 6 ビットである。次に、アドレス管理情報 1 1 3 をもとに接続可否チェック用 I P アドレス生成処理部 1 1 2 で順次、I P アドレスを生成し、その I P アドレスを使って、チェック用フレーム生成処理部 1 1 1 でチェック用フレームを生成する。このとき、図 2 2 に示すように、R F C 7 9 2 で規定された I C M P プロトコル 2 2 0 0 を使用する。ここで、タイプ 2 2 0 1 が 8 である I C M P エコー要求フレームを生成した後、フレーム送信処理部 1 0 1 を使ってこのフレームをネットワークへ送信する。これをアドレス管理情報 1 1 3 の内容に従い繰り返す。このとき、ネットワークのトラフィック負荷を上昇させないようにアドレス管理情報 1 1 3 に登録された送信間隔でフレームをネットワークへ送信する。ネットワークに接続された装置はこの I C M P エコー要求フレームに対する応答を I C M P エコー応答フレームで本監視システム宛に返してくるので、この情報をフレーム受信処理部 1 0 2 で受信する。その後、この応答フレームの送信元装置の I P アドレスと M A C アドレスを組み合わせたアドレス情報を使って、接続可否判断が行われる。その後の接続可否判断処理以降の処理は前記処理と同じである。

【0080】

なお、ここではチェック用に I C M P エコー要求フレームを使った例を示したが、I C M P エコー要求フレームでなくても、接続可否チェックをされる装置から応答が返えされるフレームであればよい。たとえば、図 2 2 に示す I C M P タイムスタンプ要求や I C M P アドレスマスク要求、あるいは、A R P 要求フレームなどであってもよい。

【0081】

次に、図 2 3 に接続可否チェック処理のための一例をフローチャートに示す。

【0082】

図 2 3 の処理は一度起動されると動き続ける例を示している。処理 2 3 0 1 ~ 2 3 0 3 は初期化処理である。まず、処理 2 3 0 1 ではアドレス管理情報 1 1 3 から接続可否チェック用に使用する装置の I P アドレスの範囲情報（例えば、I P x から I P y の範囲のアドレス情報を収集する場合にはその範囲）および、フレーム送信タイミングを読み込む。フレーム送信タイミングについてはタイミング管理情報 1 0 0 0 に設定される。また、監視システムが接続されているネットワークのアドレス体系情報を把握するための I P アドレスとサブネットマスク情報を読み込む。次に、処理 2 3 0 3 において、フレームを出すタイミングを規定したタイミング管理情報テーブル 1 0 0 0 から、チェック用 1 0 3 0 の送信タイミング b（インターバル 1）T 3 および送信タイミング c（インターバル 2）T 4 を取り込む。処理 2 3 0 4 において、処理 2 3 0 5 ~ 2 3 0 9 の処理で使用するインデ

ックスを初期化する。すなわち、ホスト番号を1つずつ更新するためのホスト番号管理用インデックス、および、範囲指定されたIPアドレスを1つずつ更新するためのアドレス範囲管理用インデックスを初期化する。処理2305においては、処理2301で読み込んだ情報にしたがい、接続可否チェック用IPアドレスが範囲指定されていた場合には処理2308で該当IPアドレスを選択し、処理2309において次の選択用にインデックスを更新する。接続可否チェック用IPアドレスが範囲指定されていない場合には処理2306でサブネットマスクに従いホスト番号部を抽出し、ホスト番号を生成する。処理2307において次のホスト番号を生成するためにインデックスを更新する。処理2310ではIPアドレスを生成し、処理2311ではこのIPアドレスを使用したICMPエコー要求フレームを生成し、処理2312ではこのフレームを送信する。処理2313では指定された全てのホスト（装置）に対してアドレス収集用のICMPエコー要求フレームを発行したかを判断し、全てが完了した場合には処理2114でインターバル2の間休止し、以後処理を続行する。一方、全てが完了していない場合にはインターバル1の間休止し、次のホスト（装置）に対する処理を続行する。

10

【0083】

本実施例によればネットワークに接続を許可される装置情報を予め登録しておくことにより、ネットワークへの接続を許可されていない装置がネットワークに接続されたタイミングで、監視システムはその存在を検出し、さらに、許可されていない装置自体が他の装置と通信をできなくするように、許可されていない装置をネットワークから切り離すことができる。また、許可されていない装置を切り離す際には、許可されていない装置が使用したIPアドレスのネットワーク内での使用状況により、許可されていない装置の切り離し方法を変え、これにより、ネットワーク内の他の装置間の通信を継続できるようにしていることである。また、許可されていない装置がネットワークに接続された後に、監視システムを起動させた場合においても、該当装置の存在を検知し、さらに、該当装置をネットワークから切り離すことができる。また、許可されていない装置と判断される装置を含めてネットワーク上に接続される装置には本発明に関わる専用ソフトウェアを予め入れておく必要が無いことからネットワークセキュリティを強化することができる。

20

【実施例2】

【0084】

以下、実施例2について説明する。

30

【0085】

<構成>

本発明のネットワーク監視システムの構成のうち、特徴部を図15に示す。なお、その他の部分は概略、図1と同じである。図15において、ネットワーク監視システム200はネットワーク120からフレームを受信するフレーム受信処理部102、受信したフレームのうち、ネットワーク上の各装置から自発的あるいは誘発的に発行されたARPフレームからIPアドレスとMACアドレス情報を抽出するARPフレームのアドレス情報抽出処理部1501、この抽出したIPアドレスとMACアドレスを組み合わせ、ネットワークに接続された装置のアドレス情報を一意的に生成するアドレス情報生成処理部1502、生成された一意的なアドレス情報の要素分類をキーにして外部から昇順もしくは降順に並べ替えを行い、さらに、このアドレス情報の個々の要素に対して、外部から有効あるいは無効の設定を行うための外部装置114、その設定結果に従って生成される、ネットワークに接続された装置の装置アドレス情報生成処理部103、ネットワーク上の全ての装置または指定された1つ以上の装置に対して、ARPフレームの発行を誘発するフレームを発行するためのアドレス情報収集用IPアドレス生成処理部1505、そのIPアドレス生成のために予め登録されたアドレス管理情報113、アドレス情報収集用フレーム生成処理部1504、生成されたフレームをネットワークへ送信するフレーム送信処理部101からなる。なお、接続可否情報管理処理部104および本図に記載されていない他の処理部は図1と同様である。

40

【0086】

50

＜装置アドレス情報生成処理＞

図15を用いて、装置アドレス情報生成処理を説明する。

【0087】

ネットワーク監視システム200はブロードキャスト方式を使ってネットワーク120上のすべての装置宛に送られてくるARP要求フレームを受信処理部102で受信する。そして、ARP要求フレームを発行した装置を特定するために、ARPフレームのアドレス情報抽出処理部1501において、受信したARPフレームから該当装置のアドレス情報であるIPアドレスとMACアドレスを抽出する。アドレス情報生成処理部1502においては抽出したアドレス情報がすでに登録されていないかをチェックし、登録されていない場合のみ、今回受信したアドレス情報を登録する。この結果、本処理部1502を処理することで、ネットワークに接続された装置のアドレス情報が一意的に作成される。ここで、以上の処理が一定時間実施された場合にはアドレス生成情報として、図16に示すアドレス情報1600ができる。いずれも、アドレス情報としてIPアドレスとMACアドレスの組み合わせを基本に、さらに、時刻情報をもつこともある。ここで、この情報をそのまま接続可否情報管理処理部104で用いるのではなく、ネットワークシステムの運用等に照らし合わせて、装置アドレス情報生成処理部103で処理を行う。例えば、DHCPサーバ環境の場合、時間の経過とともに同一IPアドレスが複数の装置に割り当てられるので、IPアドレスとMACアドレスを1対1に対応付けることはできない。そのような場合には図17に示す装置アドレス情報1700における装置3のようにMACアドレス(MAC3)のみを登録1703する。また、装置によってはLANアダプタの故障等によるLANアダプタの交換でMACアドレスが変更になる場合を考慮して、装置2のようにIPアドレス(IP2)のみを登録1702することもある。

【0088】

このようなネットワークシステムの運用等に照らし合わせた設定が必要となることから、外部装置114に対しては、生成された一意的なアドレス情報の要素分類をキーにして、外部から昇順もしくは降順に並べ替えを行うことができるインタフェースおよび、一意的なアドレス情報の個々の要素に対する有効あるいは無効の設定を行うためのインタフェースが提供されている。

【0089】

したがって、外部装置114からこのインタフェースを使用して図17に示すような装置アドレス情報1700を生成する。例えば、図16を例に説明する。要素分類としてIPアドレス1601をキーに、昇順に並べ替え、要素としてMAC2を無効とする。図17における、装置2の情報1702はこのケースを示している。MAC2を無効としたため、MAC部は空白となっている。ここで生成された情報は接続可否情報として接続可否情報管理処理部104で使用できることになる。接続可否情報管理処理部104以降の処理の流れは図1と同じである。

【0090】

図19にアドレス情報を受動的に収集して、アドレス情報を生成する一例をフローチャートに示す。本処理は装置アドレス情報生成処理を行うための前処理である、アドレス情報生成の一例である。この例では処理1901において停止要求があるまでネットワークからアドレス情報を収集している。処理1902では受信したフレームのプロトコル種別を調べて、それがARPフレームの場合のみを以降の処理対象としている。処理1903は監視システムが発行したARPフレームは処理対象外とするものである。処理1904において、受信したARPフレームからIPアドレスとMACアドレスを抽出し、処理1905においてこのアドレス情報がすでに登録されているか否かをチェックし、未登録のアドレス情報のみを図16のアドレス情報テーブル1600に登録することにより一意的なアドレス情報を生成する。

【0091】

次に、図20において外部からの指示に従って、図17の装置アドレス情報1700を生成するための一例をフローチャートに示す。ここでは前記の処理で生成されたアドレス

情報1600をもとに装置アドレス情報1700を生成する。処理2010では、アドレス情報1600を編集するために、外部から、アドレス部であるMACアドレスやIPアドレスをキーにした並べ替えを行う指示があるか否かを判断する。並べ替えを行う指示がある場合には、処理2011において、IPアドレスやMACアドレスをキーにした昇順あるいは降順の並べ替えを行う。処理2012においては、各アドレス部に対する有効、あるいは無効の指示を取り込み、その指示に従ってアドレス情報1600をもとに装置アドレス情報1700を生成するための判断を行う。処理2013はMACアドレスのみを有効とした装置アドレス情報1700を作成する。処理2014はIPアドレスのみを有効とした装置アドレス情報1700を作成する。また、処理2015はMACアドレスとIPアドレスの双方を有効とした装置アドレス情報1700を作成する。処理2016において、全ての装置に対する編集が終われば処理を終了する。

10

【0092】

一方、前記はブロードキャスト方式を使ってネットワーク120上のすべての装置宛に送られてくるARP要求フレームに対する処理の流れを説明したが、この処理を補完するために下記処理を行う。これは例えば、監視システムを何らかの理由で一度停止し、再度立ち上げた場合には、その時点ですでにネットワークに接続された全ての装置のアドレス情報を生成することが困難となる場合を想定したものである。

【0093】

図15を使って以下説明する。監視システムがアドレス情報を能動的に生成するために、ネットワーク上の全ての装置または指定された1つ以上の装置に対してARPフレームの発行を誘発するためのフレームを発行する。そのために、発行対象となる装置の決定はアドレス管理情報113にあらかじめ登録されているものを使用する。ここには、例えば、対象となるIPアドレスの範囲指定や個別指定されたIPアドレスリストがある。また、アドレス指定されていない場合には、例えば、図18に示すような該当ネットワークのIPアドレスやネットマスク情報をもとにネットワーク上のすべてのホストのIPアドレスを生成して発行することになる。図18においては、IPアドレス1800は172.20.100.52、サブネットマスク1801は255.255.255.192であるため、ネットワークアドレス部は26ビット、ホスト部は6ビットである。アドレス管理情報113をもとにアドレス情報収集用IPアドレス生成処理部で順次、IPアドレスを生成し、そのIPアドレスを使って、アドレス情報収集用フレーム生成処理部1504で生成されたARP要求フレームをフレーム送信処理部101からネットワークへ送信する。これをアドレス管理情報113の内容に従い繰り返す。ネットワークに接続された装置はこのARP要求フレームに対する応答をARP応答フレームとして本監視システム宛に返してくるので、この情報をフレーム受信処理部102で受信する。その後の処理は前記処理と同じである。図21にアドレス情報を能動的に収集して、アドレス情報を生成する一例をフローチャートに示す。図21の処理は一度起動されると動き続ける例を示している。処理2101～2103は初期化処理である。まず、処理2101ではアドレス管理情報113からアドレス収集用に使用する装置のIPアドレスの範囲情報（例えば、IPxからIPyの範囲のアドレス情報を収集する場合にはその範囲）および、フレーム送信タイミングを読み込む。フレーム送信タイミングについてはタイミング管理情報1000に設定される。また、監視システムが接続されているネットワークのアドレス体系情報を把握するためのIPアドレスとサブネットマスク情報を読み込む。次に、処理2103において、フレームを出すタイミングを規定したタイミング情報管理テーブル1000から、アドレス収集用1040の送信タイミングb（インターバル1）T5および送信タイミングc（インターバル2）T6を取り込む。処理2104において、処理2105～2109の処理で使用するインデックスを初期化する。すなわち、ホスト番号を1つずつ更新するためのホスト番号管理用インデックス、および、範囲指定されたIPアドレスを1つずつ更新するためのアドレス範囲管理用インデックスを初期化する。処理2105においては、処理2101で読み込んだ情報にしたがい、アドレス情報収集用IPアドレスが範囲指定されていた場合には処理2108で該当IPアドレスを選択し、処理2109に

20

30

40

50

において次回の選択用にインデックスを更新する。アドレス情報収集用 I P アドレスが範囲指定されていない場合には処理 2 1 0 6 でサブネットマスクに従いホスト番号部を抽出し、ホスト番号を生成する。処理 2 1 0 7 において次回のホスト番号を生成するためにインデックスを更新する。処理 2 1 1 0 では I P アドレスを生成し、処理 2 1 1 1 ではこの I P アドレスを使用した A R P 要求フレームを生成し、処理 2 1 1 2 ではこのフレームを送信する。処理 2 1 1 3 では指定された全てのホスト（装置）に対してアドレス収集用の A R P 要求フレームを発行したかを判断し、全てが完了した場合には処理 2 1 1 4 でインターバル 2 の間休止し、以後処理を続行する。一方、全てが完了していない場合にはインターバル 1 の間休止し、次のホスト（装置）に対する処理を続行する。

【0094】

本実施例によれば、ネットワークに接続されている装置が自発的にネットワークに送出するアドレス情報を含んだフレームを監視することにより、ネットワークに接続されている装置のアドレス情報を生成する（受動的）ことに加えて、さらに、接続された装置にアドレス情報の送出を誘発させるフレームをネットワーク内の装置に送出することによりアドレス情報を生成する（能動的）。この 2 つの方式により生成されたアドレス情報をもとにして、ネットワークシステムの運用方針等に従ったきめ細かな管理情報を生成することができ、これを、許可されていない端末の存在を判断する際に使用するアドレス管理情報とすることができる。これにより、これら多数の装置の管理情報を、例えば、手作業で作成しなくてもよく、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担を軽減することができる。

【実施例 3】

【0095】

以下、実施例 3 について説明する。

【0096】

<構成>

本発明のネットワーク監視システムの構成を図 1 に示す。

【0097】

ネットワークに接続された装置の接続状態を管理し、一旦切り離された装置を許可された装置に外部から変更するための手段および、許可された装置を切り離すために外部から変更するための手段を提供する接続情報管理処理部 1 1 5、この処理部で管理される接続状態情報に対して、装置の接続状態情報やアドレス情報の要素分類をキーにして外部から昇順もしくは降順に並べ替えを行い、さらに、この接続状態に対して、外部から「接続」あるいは「切り離し」の設定を行うための外部装置 1 1 4、この設定指示を受け付ける外部指示受付処理部 1 0 9、一旦切り離された装置を他の装置と通信できるようにするための接続フレームを生成する接続用フレーム生成処理部 1 1 0、許可された装置を切り離すためのフレームを生成するための I P アドレス重複状態発生フレーム生成処理部 1 0 5、生成されたフレームをネットワークへ送信するフレーム送信処理部 1 0 1 からなる。

【0098】

図 1 および図 2 4 を用いて、一旦切り離された装置に対する接続処理および、許可されていた装置の切り離し処理を説明する。

【0099】

接続情報管理処理部 1 1 5 ではネットワークに接続された装置の接続状態を管理している。外部から、一旦切り離された装置を許可された装置に変更する場合、あるいはその逆に、許可されていた装置を切り離す装置に変更する場合には、外部装置 1 1 4 から接続あるいは切り離し指示が行われる。

【0100】

この接続指示あるいは切り離し指示は外部指示受付処理部 1 0 9 で受け付けられ、接続可否情報 7 0 0 と接続可否判断処理部 1 0 6 の結果に従った接続状態情報 2 4 0 0 がまず作成される。次に、この指示内容にしたがい接続情報管理処理部 1 1 5 で管理される接続状態情報 2 4 0 0 が変更される。外部装置 1 1 4 に対しては、接続状態およびアドレス情

報の要素分類をキーにして、外部から昇順もしくは降順に並べ替えを行うことができるインタフェースおよび、この接続情報に対応した装置に対して、接続あるいは切り離しの設定を行うためのインタフェースが提供されており、このインタフェースを使用して外部から該当装置の接続あるいは切り離し指示を行う。例えば、要素分類として接続状態情報 2401 をキーに、昇順に並べ替え、切り離された複数の装置、または接続状態の装置を抽出する。この複数の装置から接続を行う装置あるいは切り離しを行う装置を選択して、該当装置を接続状態あるいは切り離し状態とする指示を行う。

【0101】

＜一旦切り離された装置に対する外部からの接続処理＞

図 24 に接続情報管理処理部 115 で管理される接続状態情報 2400 を示す。接続状態情報 2400 は装置ごとに現在の接続状態 2401, MAC アドレス 2402, IP アドレス 2403 をもっている。たとえば、装置 1 2404 は「接続」状態を、装置 2 2405 は「停止」中の状態を、装置 3 2406 は「切り離し」状態を示している。

10

【0102】

一旦切り離された装置に対する外部からの接続処理一例を図 25 のフローチャートに示す。処理 2501 では外部装置 114 からの指示を取り込むものである。処理 2502 において、切り離し指示を外部指示受付処理部 109 で受け付けた後、接続可否情報 700 と接続可否判断処理部 106 の結果に従った接続状態情報 2400 を作成する。処理 2503 においては、要素分類として接続状態情報 2401 をキーに昇順あるいは降順に並べ替え要求があれば、処理 2504 でその処理を行い、切り離された複数の装置を抽出し、この複数の装置から接続を行う装置選択する。

20

【0103】

この後、処理 2505 において、選択された装置の接続状態情報 2400 が「切り離し」状態から「接続」状態に設定変更されると、処理 2506 において該当装置のアドレス情報を生成する。処理 2507 において接続用フレームを全装置宛に送る接続用フレーム 1400 (ARP 応答フレーム) を生成する。処理 2508 において、全装置宛にフレームをネットワークへ送信する。

【0104】

ここで、図 1 において接続用フレーム生成処理部 110 の処理について詳細に説明する。本処理部は一旦、切り離された特定の装置を再度、ネットワークに接続するために、該当接続フレームを作成するものである。

30

【0105】

このときのポイントは接続フレームを該当装置のみに送信するだけでは不十分である。つまり、ネットワークに接続されているすべての装置が個々に管理している IP アドレスと MAC アドレスの対応表のうち、今回接続を許可する装置の IP アドレスと MAC アドレスの対応関係を正しく直さなければならない。

【0106】

そのために、図 14 に示す接続用フレーム 1400 を作成する。具体的には、送信元アドレス 1401 の IP アドレスは接続しようとする該当装置の IP アドレス (IP1) 1412 とし、MAC アドレスは該当装置の MAC アドレス (MAC1) 1411 とする。一方、探索アドレス 1402 の IP アドレスは監視システムの IP アドレス (IPx) 1414 を、MAC アドレスは監視システムの MAC アドレス (MACx) 1413 を設定する。これを該当装置宛ではなく、ネットワークに接続されているすべての装置に対して送出し、各装置が持っている ARP 管理テーブル内の IP アドレスと MAC アドレスの対応関係も正しくなるように更新する。これにより、切り離されていた装置は他の装置と通信を行うことができるようになる。

40

【0107】

以上は、接続情報管理処理部 115 で管理される接続状態情報 2400 を外部から変更することで、切り離された装置の接続処理について述べたが、この接続処理は外部装置 114 からの直接の指示を受けて実行されることもある。そのときは、接続状態情報を使用

50

せずに、外部装置 114 から接続対象装置の IP アドレスを直接指定する。

【0108】

外部指示受付処理部ではこの IP アドレスに対応したこの装置の MAC アドレスを接続可否情報 700 から取り出し、この IP アドレスと MAC アドレスを組み合わせた接続用フレームの生成を接続用フレームの生成処理部 110 に依頼する。以後の処理は前記接続処理と同じである。これにより、外部から指定された装置をネットワークに接続することができる。

【0109】

＜接続されている装置に対する外部からの切り離し処理＞

一方、外部装置から、許可されている装置を切り離すための指示が行われた場合には、同様に外部指示受付処理部 109 を介して、接続状態情報に変更され、切り離し処理が実行される。このとき、実施例 1 で説明した切り離し処理が行われる。

【0110】

以上は、接続情報管理処理部 115 で管理される接続状態情報を外部から変更することで、接続されている装置を切り離す処理であるが、この切り離し処理は外部装置 114 からの直接の指示を受けて実行されることもある。そのときは、接続状態情報を使用せずに、外部装置 114 から切り離し対象装置の IP アドレスを直接指定する。

【0111】

外部指示受付処理部ではこの IP アドレスに対応したこの装置の MAC アドレスを接続可否情報 700 から取り出し、この IP アドレスと MAC アドレスを組み合わせた IP アドレス重複状態発生フレームの生成を IP アドレス重複状態発生フレーム生成処理部 105 に依頼する。以後の処理は実施例 1 と同じである。これにより、外部から、指定された装置を切り離すことができる。

【0112】

例えば、ネットワーク内のウイルス攻撃などを監視しているセキュリティ装置が、攻撃を検知した後、攻撃をしているネットワーク内の装置の切り離しや、あるいは、攻撃を受けているサーバを守るために、このサーバを切り離す場合などにも使用される。

【0113】

なお、本実施例では外部装置 114 とネットワーク監視システム 200 が直接接続されている図 1 の構成を使って説明したが、外部装置と監視システムがネットワークを介して接続されている場合であってもよい。

【0114】

本実施例によれば、許可されていない装置として一旦切り離した装置を、管理者等の判断で、ネットワーク上の他の装置の使用者に影響を与えることなく、外部から指示することにより、再度、使用できるようにすることができる。また、接続されている装置の切り離しについても、管理者等の判断で、ネットワーク上の他の装置の使用者に影響を与えることなく、外部から指示することにより、接続されている装置を切り離すことができるようになる。これにより、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担を軽減することができる。

【0115】

以上のように、DHCP でアドレスを割り当てる環境に限定せずに、装置に固定的に割り付けたアドレスを使用するネットワーク環境においても、ネットワークへの接続を許可されていない装置がネットワークに接続されたタイミングで、監視システムはその存在を検出し、さらに、許可されていない装置自体が他の装置と通信をできなくするように、許可されていない装置をネットワークから切り離すことができる。また、許可されていない装置を切り離す際には、許可されていない装置が使用した IP アドレスのネットワーク内での使用状況により、許可されていない装置の切り離し方法を変え、これにより、ネットワーク内の他の装置間の通信を継続できるようにしていることである。また、許可されていない装置がネットワークに接続された後に、監視システムを起動させた場合においても、該当装置の存在を検知し、さらに、該当装置をネットワークから切り離すことができる

10

20

30

40

50

。また、許可されていない装置と判断される装置を含めてネットワーク上に接続される装置には本発明に関わる専用ソフトウェアを予め入れておく必要が無いことからネットワークセキュリティを強化することができる。

【0116】

また、ネットワークに接続されている装置が自発的にネットワークに送出するアドレス情報を含んだフレームを監視することにより、ネットワークに接続されている装置のアドレス情報を生成する（受動的）ことに加えて、さらに、接続された装置にアドレス情報の送出を誘発させるフレームをネットワーク内の装置に送出することによりアドレス情報を生成する（能動的）。この2つの方式により生成されたアドレス情報をもとにして、ネットワークシステムの運用方針等に従ったきめ細かな管理情報を生成することができ、これを、許可されていない端末の存在を判断する際に使用するアドレス管理情報とすることができる。これにより、これら多数の装置の管理情報を、例えば、手作業で作成しなくてもよく、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担を軽減することができる。

10

【0117】

また、許可されていない装置として、一旦切り離れた装置を管理者等の判断で、外部から指示することにより、ネットワーク上の他の装置の使用者に影響を与えることなく、一旦切り離れた装置を使用できるようにすることができる。また、接続されている装置の切り離しについても、管理者等の判断で、外部から指示することにより、ネットワーク上の他の装置の使用者に影響を与えることなく、接続されている装置を切り離すことができる。これにより、ネットワークの管理や維持に関わる作業やそれに伴う費用、あるいはネットワーク管理者の負担を軽減することができる。

20

【図面の簡単な説明】

【0118】

【図1】ネットワーク監視システムの構成図。

【図2】ネットワーク監視システムの全体構成図。

【図3】IPフレームのフォーマット。

【図4】ARPプロトコルのフォーマット。

【図5】ARPプロトコルによるアドレス解決の通信例。

【図6】実施例1の接続可否情報を示す図（1）。

30

【図7】実施例1の接続可否情報を示す図（2）。

【図8】実施例1の接続可否情報を示す図（3）。

【図9】実施例1の接続可否情報を示す図（4）。

【図10】実施例1のフレーム送出タイミング管理情報。

【図11】実施例1のARP要求フレームフォーマット。

【図12】実施例1のIPアドレス重複状態発生フレームフォーマット。

【図13】実施例1の装置の切り離し処理のフローチャート。

【図14】実施例3の接続用フレームフォーマット。

【図15】実施例2のネットワーク監視システムの構成図（装置アドレス情報生成）。

【図16】実施例2のアドレス情報を示す図。

40

【図17】実施例2の装置アドレス情報を示す図。

【図18】実施例1、2のアドレス体系を示す図。

【図19】実施例2の受動的なアドレス情報生成処理のフローチャート。

【図20】実施例2の装置アドレス情報生成処理のフローチャート。

【図21】実施例2の能動的なアドレス情報生成処理のフローチャート。

【図22】実施例1のICMPプロトコルのフレームフォーマット。

【図23】実施例1の接続可否チェック処理のフローチャート。

【図24】実施例3の切り離された装置を外部から接続、切り離す場合に使用する接続状態情報の図。

【図25】実施例3の切り離された装置を外部から接続する処理のフローチャート。

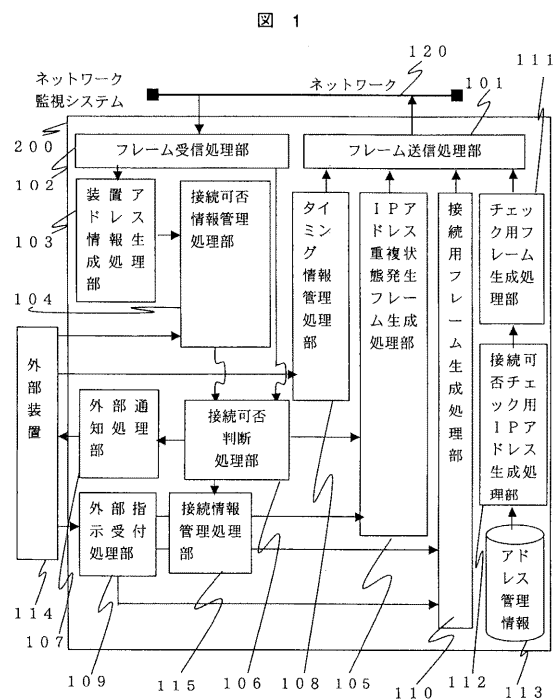
50

【符号の説明】

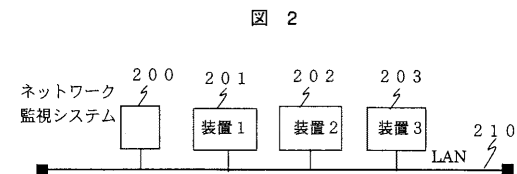
【0119】

101…フレーム送信処理部、102…フレーム受信処理部、103…装置アドレス情報生成処理部、104…接続可否情報管理処理部、105…IPアドレス重複状態発生フレーム生成処理部、106…接続可否判断処理部、107…外部通知処理部、108…タイミング情報管理処理部、109…外部指示受付処理部、110…接続用フレーム生成処理部、111…チェック用フレーム生成処理部、112…接続可否チェック用IPアドレス生成処理部、113…アドレス管理情報、114…外部装置、115…接続情報管理処理部、120…ネットワーク、200…ネットワーク監視システム。

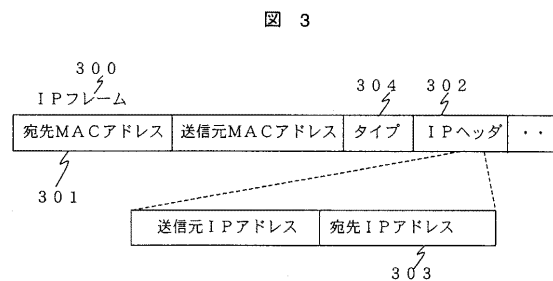
【図1】



【図2】



【図3】



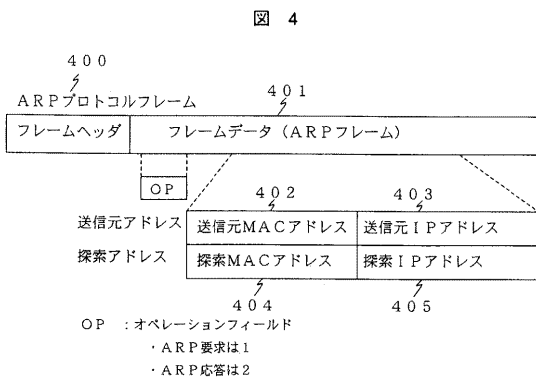
(a) タイプ： プロトコル種別を示す。

・ARP : 0806

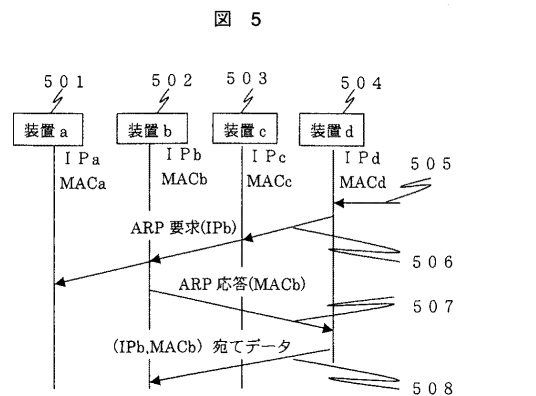
・IP : 0800

(b) ICMPフレームはIPヘッダ内のプロトコルフィールドの値で識別される。

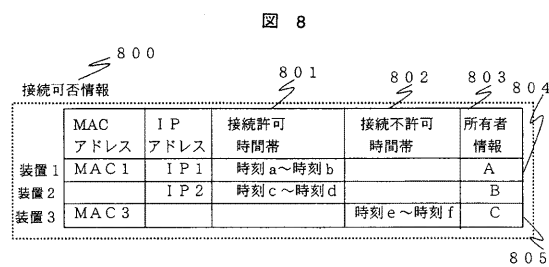
【図 4】



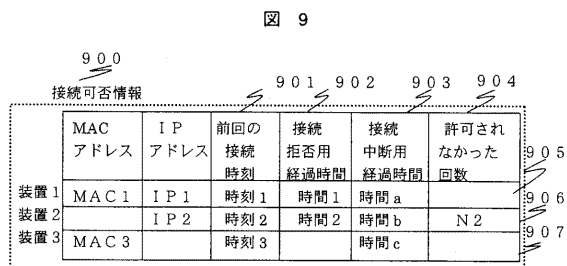
【図 5】



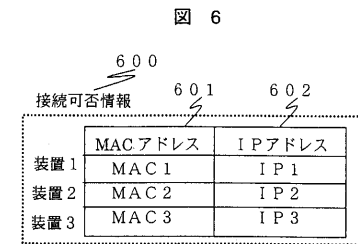
【図 8】



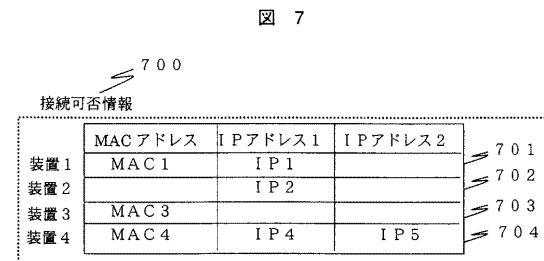
【図 9】



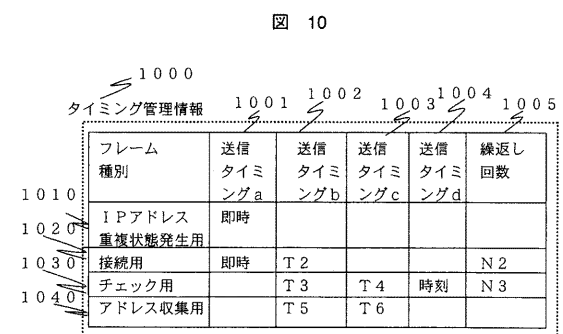
【図 6】



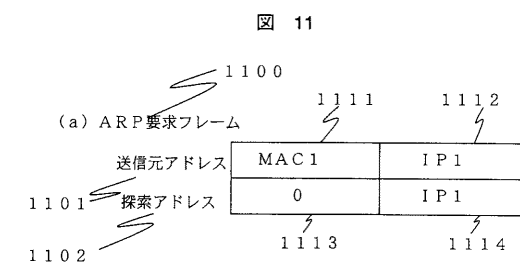
【図 7】



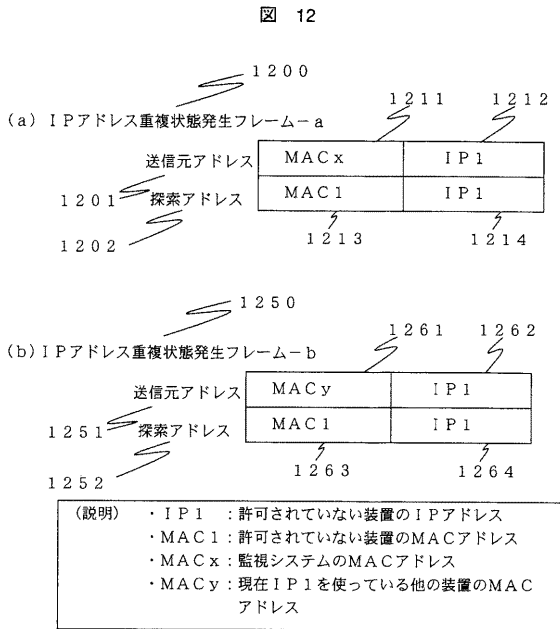
【図 10】



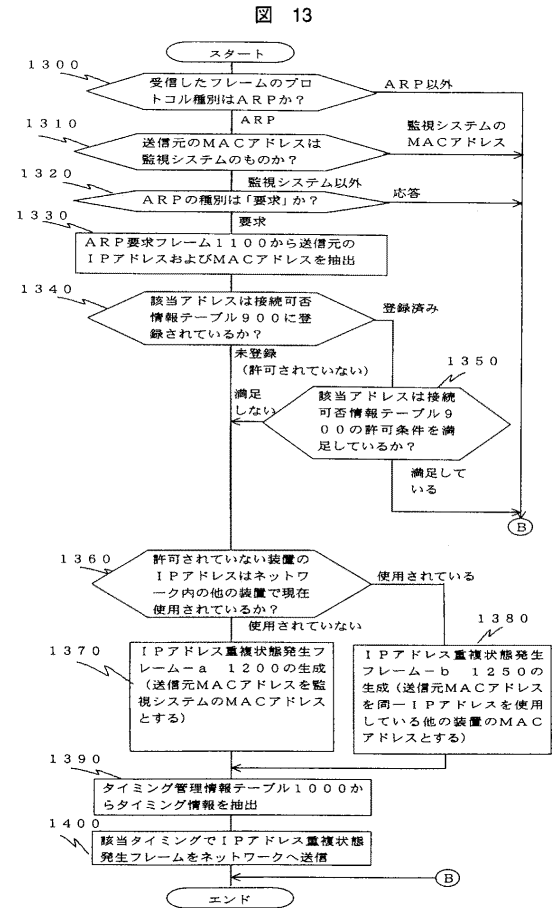
【図 11】



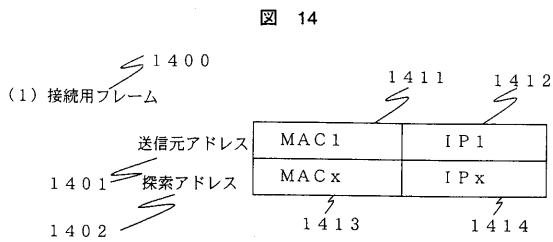
【図 12】



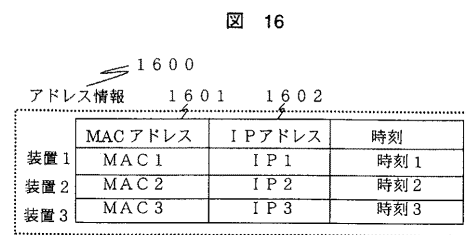
【図 13】



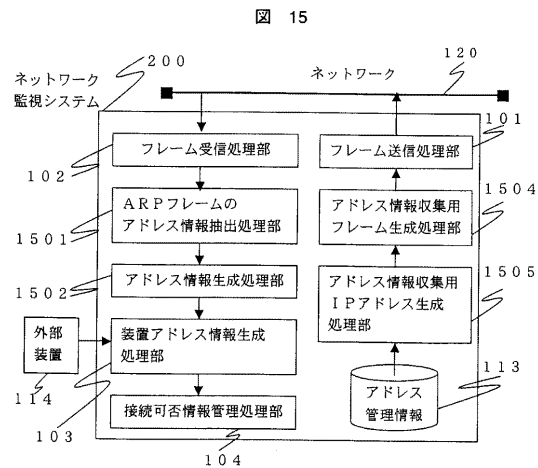
【図 14】



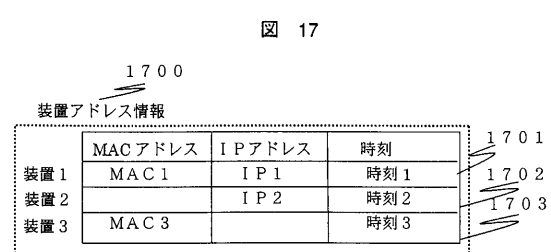
【図 16】



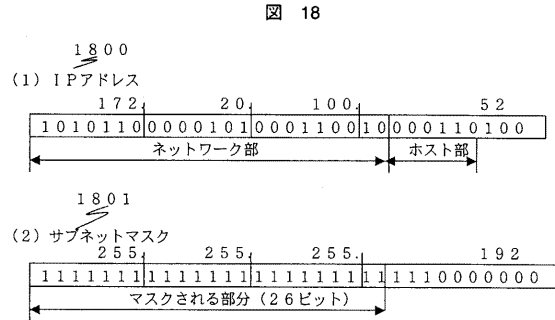
【図 15】



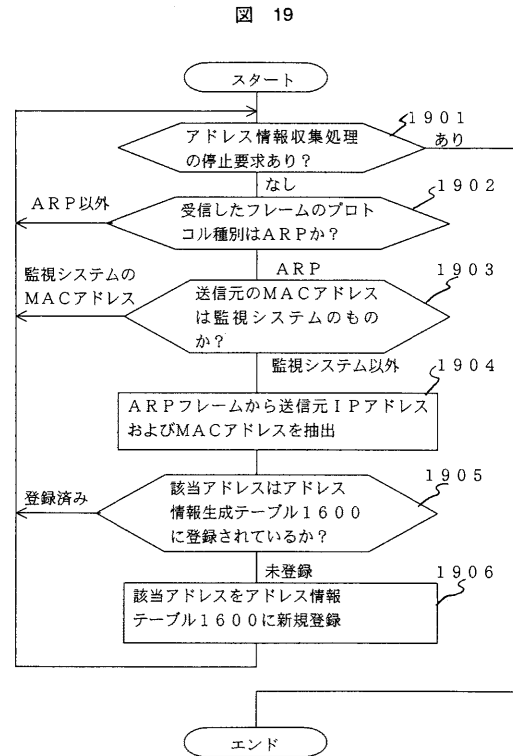
【図 17】



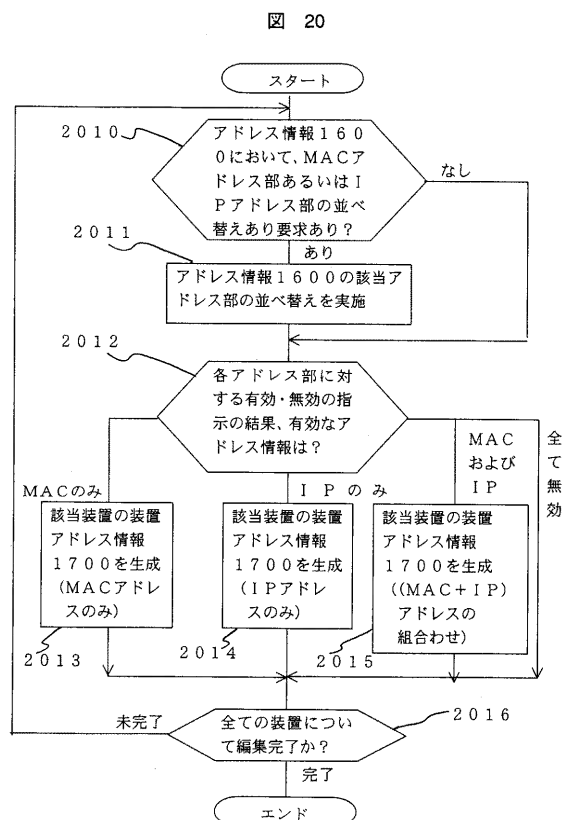
【図 18】



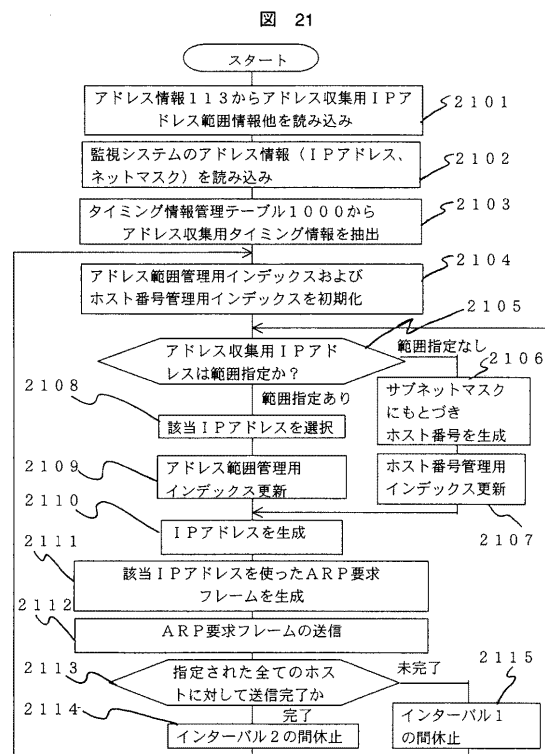
【図 19】



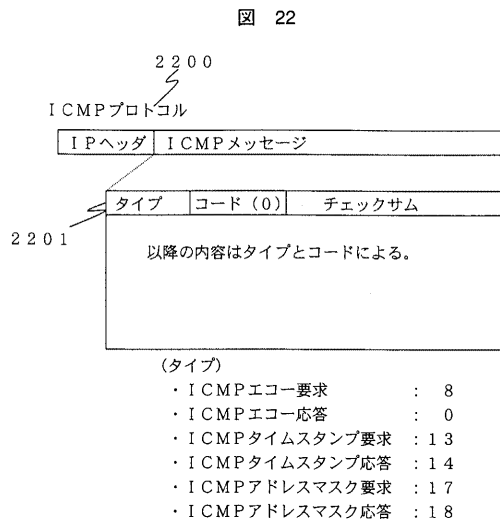
【図 20】



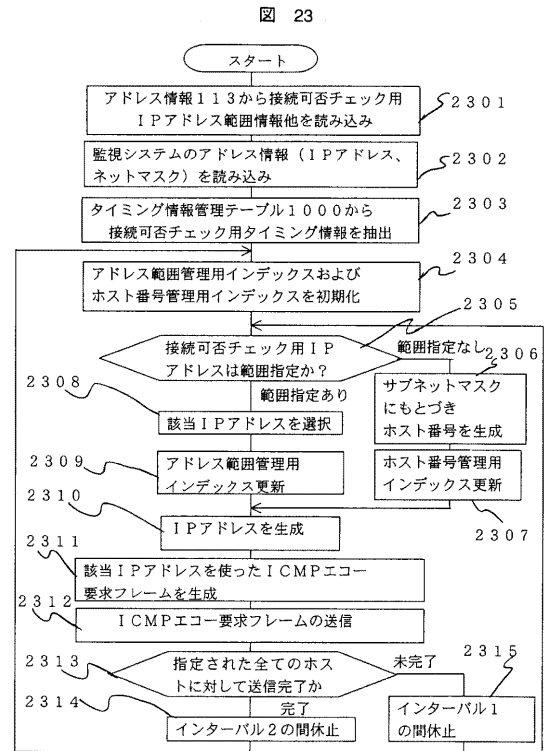
【図 21】



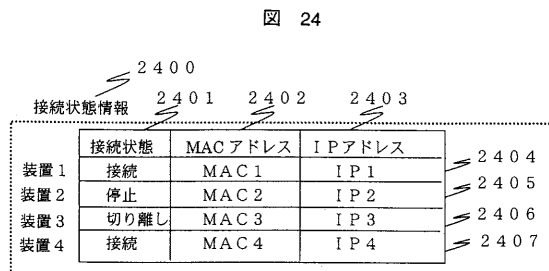
【図 22】



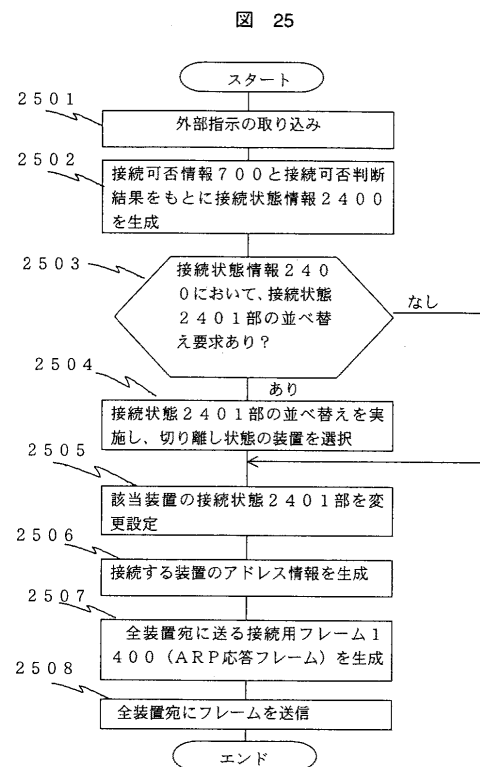
【図 23】



【図 24】



【図 25】



フロントページの続き

- (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
システム事業部内
株式会社 日立製作所 情報制御
- (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 浪岡 良光
茨城県日立市大みか町五丁目2番1号
システム事業部内
株式会社 日立製作所 情報制御
- (72)発明者 亀田 貴之
茨城県日立市大みか町五丁目2番1号
システム事業部内
株式会社 日立製作所 情報制御
- (72)発明者 菊池 久雄
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

審査官 脇水 佳弘

- (56)参考文献 特開平08-186569 (JP, A)
特開平02-004040 (JP, A)
特開2005-198090 (JP, A)
未承認マシンの不正接続防止, WebSAM SecureVisor, 2004年 2月 5
日, URL, [http://web.archive.org/web/20040205171541/www.sw.nec.co.jp/middle/WebSAM/p
roducts/SecureVisor/fn_jam.html](http://web.archive.org/web/20040205171541/www.sw.nec.co.jp/middle/WebSAM/products/SecureVisor/fn_jam.html)
WebSAM SecureVisor Ver. 1.3 ご説明資料, WebSAM Sec
ureVisor, 2003年10月 8日, URL, [http://web.archive.org/web/200407312
25655/http://www.sw.nec.co.jp/middle/WebSAM/products/SecureVisor/download/031008.Secur
eVisor.ppt](http://web.archive.org/web/20040731225655/http://www.sw.nec.co.jp/middle/WebSAM/products/SecureVisor/download/031008.SecureVisor.ppt)
塩月誠人, 堂々と公開されている“禁断のテクニック”パスワードクラック／ネットワーク盗聴
／ぜい弱性攻撃を阻め! 社内不正ユーザー撃退法 敵はLAN上にあり!, Windows
Server World 2003年8月号, 日本, (株)IDGジャパン, 2003年 8
月 1日, 第8巻第8号, pp. 102-106, 第2のケース ネットワーク盗聴

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