(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2019-41176
(P2019-41176A)
(43)公開日　平成31年3月14日(2019.3.14)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/46	(2006.01)	H04L 12/46	E	5K033

審査請求 未請求　請求項の数 11　ＯＬ　（全 18 頁）

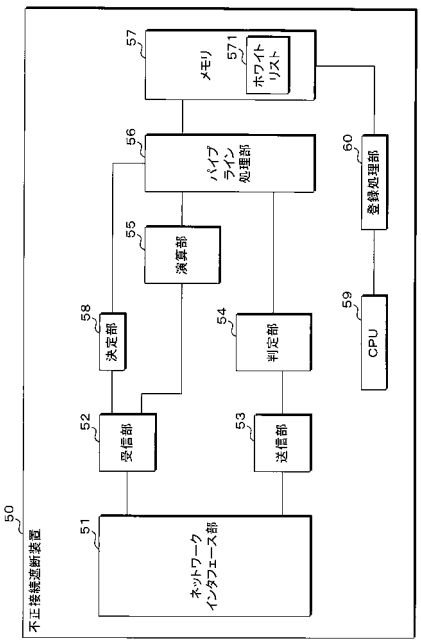
(21)出願番号　特願2017-160290 (P2017-160290)
(22)出願日　平成29年8月23日 (2017.8.23)

(71)出願人　316017343
株式会社ソフトクリエイト
東京都渋谷区渋谷二丁目１５番１号
(74)代理人　100114557
弁理士　河野　英仁
(74)代理人　100078868
弁理士　河野　登夫
(72)発明者　沼田　浩邦
東京都渋谷区渋谷２－１５－１　株式会社ソフトクリエイト内
(72)発明者　松谷　健史
東京都品川区北品川３－３－３　東和電業株式会社内

Ｆターム(参考)　5K033 AA09　DB20　EC03

(54)【発明の名称】不正接続遮断装置及び不正接続遮断方法

(57)【要約】
【課題】ネットワーク構成を変更することなく、ネットワークでの不正接続を遮断することができる不正接続遮断装置及び不正接続遮断方法を提供する。
【解決手段】不正接続遮断装置は、ネットワークでの不正接続を遮断する不正接続遮断装置であって、第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得する取得部と、取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する判定部と、第１アドレスが正当でないと判定した場合、第２装置が第２アドレスを第１装置へ送信する前に、所定のアドレスを第１装置へ送信する送信部とを備える。
【選択図】図２



【特許請求の範囲】
【請求項１】
ネットワークでの不正接続を遮断する不正接続遮断装置であって、
第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得する取得部と、
該取得部で取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する判定部と、
該判定部で前記第１アドレスが正当でないと判定した場合、前記第２装置が前記第２アドレスを前記第１装置へ送信する前に、所定のアドレスを前記第１装置へ送信する送信部と
を備える不正接続遮断装置。
【請求項２】
前記送信部は、
前記判定部で前記第１アドレスが正当であると判定した場合、前記所定のアドレスを前記第１装置へ送信しない請求項１に記載の不正接続遮断装置。
【請求項３】
複数の正当な第１アドレスを記憶した記憶部を備え、
前記判定部は、
取得した要求パケットに含まれる第１アドレスが前記記憶部に記憶した第１アドレスに一致するか否かに応じて、前記要求パケットに含まれる第１アドレスが正当であるか否かを判定する請求項１又は請求項２に記載の不正接続遮断装置。
【請求項４】
複数の正当な第１アドレスに対してハッシュ演算を行って得られたハッシュ値に基づくアドレスに複数の正当な第１アドレスを対応付けて記憶する記憶部と、
取得した要求パケットに含まれる第１アドレスに対して前記ハッシュ演算を行う演算部と
を備え、
前記判定部は、
前記演算部で演算して得られたハッシュ値に基づく前記記憶部のアドレスに正当な第１アドレスが記憶されていない場合、前記要求パケットに含まれる第１アドレスが正当ではないと判定する請求項１又は請求項２に記載の不正接続遮断装置。
【請求項５】
前記取得部で要求パケットを取得する都度、前記記憶部に記憶した正当な第１アドレスをパイプライン処理で読み出すパイプライン処理部を備え、
前記判定部は、
前記パイプライン処理部で読み出した結果に基づいて、取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する請求項３又は請求項４に記載の不正接続遮断装置。
【請求項６】
前記取得部は、
前記要求パケットを含む任意のパケットを取得し、
前記取得部で取得したパケットが要求パケットであるか否かに応じて前記パイプライン処理部の処理の実行・停止を決定する決定部を備える請求項５に記載の不正接続遮断装置。
【請求項７】
前記判定部又は演算部での処理は、ハードウェアで行う請求項１から請求項６のいずれか一項に記載の不正接続遮断装置。
【請求項８】
前記第１アドレスは、ＭＡＣアドレスである請求項１から請求項７のいずれか一項に記載の不正接続遮断装置。

【請求項９】
前記第２アドレスは、ＭＡＣアドレス又はＩＰアドレスである請求項１から請求項８のいずれか一項に記載の不正接続遮断装置。
【請求項１０】
前記所定のアドレスは、偽のＭＡＣアドレス又はＩＰアドレスである請求項１から請求項９のいずれか一項に記載の不正接続遮断装置。
【請求項１１】
ネットワークでの不正接続を遮断する不正接続遮断方法であって、
第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得部が取得し、
取得された要求パケットに含まれる第１アドレスが正当であるか否かを判定部が判定し、
前記第１アドレスが正当でないと判定された場合、前記第２装置が前記第２アドレスを前記第１装置へ送信する前に、所定のアドレスを前記第１装置へ送信部が送信する不正接続遮断方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不正接続遮断装置及び不正接続遮断方法に関する。
【背景技術】
【０００２】
様々な情報処理装置がネットワークに接続され、ネットワークを介して企業の情報の授受が行われている。このため、企業の情報を不正なアクセスから保護することが重要な課題になりつつあり、ネットワークにおける安全性の高いセキュリティ対策に対するニーズが高まっている。
【０００３】
ネットワークのセキュリティ対策には種々のものがある。例えば、特許文献１には、パケットを監視し、不正端末によるネットワークへの不正接続を検出した場合、セキュリティ強度が異なる複数の仮想ネットワークから一の仮想ネットワークを選択すべくネットワーク構成を変更して、不正アクセスが発生したネットワークを選択的に保護するネットワーク構成変更方法が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１５－５０７１７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかし、特許文献１のように、ネットワーク構成を変更する場合、ルータやスイッチなどの設定変更なども必要となり、適用箇所が多いときは、ネットワークの運用労力が多大となる。
【０００６】
本発明は、斯かる事情に鑑みてなされたものであり、ネットワーク構成を変更することなく、ネットワークでの不正接続を遮断することができる不正接続遮断装置及び不正接続遮断方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明の実施の形態に係る不正接続遮断装置は、ネットワークでの不正接続を遮断する不正接続遮断装置であって、第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得する取得部と、該取得部で取得した要求パケットに含

まれる第１アドレスが正当であるか否かを判定する判定部と、該判定部で前記第１アドレスが正当でないと判定した場合、前記第２装置が前記第２アドレスを前記第１装置へ送信する前に、所定のアドレスを前記第１装置へ送信する送信部とを備える。

【０００８】

本発明の実施の形態に係る不正接続遮断方法は、ネットワークでの不正接続を遮断する不正接続遮断方法であって、第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得部が取得し、取得された要求パケットに含まれる第１アドレスが正当であるか否かを判定部が判定し、前記第１アドレスが正当でないと判定された場合、前記第２装置が前記第２アドレスを前記第１装置へ送信する前に、所定のアドレスを前記第１装置へ送信部が送信する。

【発明の効果】

【０００９】

本発明によれば、ネットワーク構成を変更することなく、ネットワークでの不正接続を遮断することができる。

【図面の簡単な説明】

【００１０】

【図１】本実施の形態の不正接続遮断装置が不正接続を検知・遮断するネットワークの構成の一例を示す模式図である。

【図２】本実施の形態の不正接続遮断装置の構成の一例を示すブロック図である。

【図３】本実施の形態のメモリのアドレスとアドレスに格納されるデータとの関係の一例を示す模式図である。

【図４】パイプライン処理部の処理を停止した場合の処理の一例を示す模式図である。

【図５】パイプライン処理部の処理を実行した場合の処理の一例を示す模式図である。

【図６】本実施の形態の不正接続遮断装置によるＡＲＰパケットの場合の不正接続遮断動作の一例を示す説明図である。

【図７】ＤＨＣＰパケットのイーサネットフレームの構成を示す模式図である。

【図８】本実施の形態の不正接続遮断装置によるＤＨＣＰパケットの場合の不正接続遮断動作の一例を示す説明図である。

【図９】本実施の形態の不正接続遮断装置による不正接続遮断処理の手順の一例を示すフローチャートである。

【発明を実施するための形態】

【００１１】

以下、本発明の実施の形態を図面に基づいて説明する。図１は本実施の形態の不正接続遮断装置５０が不正接続を検知・遮断するネットワークの構成の一例を示す模式図である。図１に示すように、ネットワーク通信線１には、情報処理装置２０、ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバ３０、不正接続遮断装置５０、スイッチ１０などが接続されている。不正接続遮断装置５０は、通信回線などを経由して管理サーバ１００に接続されている。なお、情報処理装置２０、スイッチ１０の数は図１の例に限定されない。

【００１２】

本明細書では、不正接続を行う情報処理装置を、正当な情報処理装置２０と区別するため、便宜上、不正装置２００として説明する。不正装置２００は、ネットワークに不正接続しようとしている。不正装置２００は、例えば、情報処理装置２０内の情報又は情報処理装置２０同士で送受される情報を不正に取得し、あるいは改ざんする行為を行う。また、不正装置２００は、情報処理装置２０内にマルウェアを侵入させる。不正装置２００は、例えば、パーソナルコンピュータ、タブレット、スマートフォンなどの装置を含む。

【００１３】

情報処理装置２０は、ネットワークへの接続が許可された正当な装置であり、例えば、パーソナルコンピュータ、タブレット、スマートフォンなどの装置を含む。

【００１４】

スイッチ１０は、Ｌ２スイッチであり、ＭＡＣアドレス（Media Access Control address）とポートとを関連付ける。スイッチ１０は、通信したい相手がどのポートに繋がっているかを記憶しており、パケットを転送することができる。より具体的には、スイッチ１０は、どのポートにどの情報処理装置２０が繋がっているかをＭＡＣアドレスによって管理する。

【００１５】

ＤＨＣＰサーバ３０は、サーバ又はルータ等で構成することができ、情報処理装置２０（ＤＨＣＰクライアントとも称する）が使用するＩＰアドレスを複数用意しておき、情報処理装置２０からの要求に応じて、一つのＩＰアドレスを割り当てる。

【００１６】

図２は本実施の形態の不正接続遮断装置５０の構成の一例を示すブロック図である。不正接続遮断装置５０は、不正装置２００がネットワークに不正に接続すること、及びネットワーク内の情報処理装置２０と通信を行うこと（両者を纏めて不正接続と称する）を検知し、不正接続を遮断する。

【００１７】

図２に示すように、不正接続遮断装置５０は、ネットワークインタフェース部５１、受信部５２、送信部５３、判定部５４、演算部５５、パイプライン処理部５６、記憶部としてのメモリ５７、決定部５８、ＣＰＵ５９、登録処理部６０などを備える。

【００１８】

メモリ５７は、複数の正当なＭＡＣアドレスのリストであるホワイトリスト５７１を記憶する。正当なＭＡＣアドレスは、例えば、ネットワーク上で情報処理装置２０との間の通信が許可された情報処理装置２０のＭＡＣアドレス、あるいはネットワークへの接続が許可された情報処理装置２０のＭＡＣアドレスとすることができる。

【００１９】

ネットワークインタフェース部５１は、ＯＳＩ（Open Systems Interconnection）参照モデルにおけるレイヤ１の物理層（Physical Layer）の処理を行う。ネットワークインタフェース部５１は、イーサネットＰＨＹとも称される。

【００２０】

受信部５２は、受信バッファ（不図示）を備え、ネットワークインタフェース部５１を経由してパケットを受信する。パケットは、情報処理装置間の通信に使用されるデータを送る単位であり、ＰＤＵ（プロトコル・データ・ユニット）と称する。パケットは、ＯＳＩ参照モデルにおけるカイヤ３のネットワーク層の通信で使われる。

【００２１】

受信部５２は、取得部としての機能を有し、第１アドレスを有する第１装置（例えば、不正装置２００）が第２装置（例えば、情報処理装置２０又はＤＨＣＰサーバ３０）に対して第２アドレスを要求する要求パケットを取得する。

【００２２】

第１アドレスは、ネットワークに接続される装置の識別に使用するアドレスであり、例えば、ＭＡＣアドレス（Media Access Control address）とすることができる。

【００２３】

要求パケットは、例えば、不正装置２００が情報処理装置２０と通信を行うためのＡＲＰ（Address Resolution Protocol）のパケット（ＡＲＰパケットとも称する）、あるいは、不正装置２００がネットワークに接続するのに必要なＩＰ（Internet Protocol）アドレスを要求するＤＨＣＰのパケット（ＤＨＣＰパケットとも称する）などを含む。

【００２４】

要求パケットがＡＲＰパケットである場合、第２アドレスはＭＡＣアドレスである。また、要求パケットがＤＨＣＰパケットである場合、第２アドレスはＩＰアドレスである。

【００２５】

判定部５４は、受信部５２で取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する。より具体的には、判定部５４は、第１装置の第１アドレスが、ホワ

イトリスト５７１に記録された正当な第１アドレスのいずれかと一致するか否かを判定し、一致する場合には、第１装置による接続は正当であると判定し、一致しない場合には、第１装置による接続は正当でないと判定する。これにより、不正接続を検知することができる。

【００２６】

図１の例では、不正装置２００は、ネットワークへの接続が許可されていない装置であり、ホワイトリスト５７１には、不正装置２００のＭＡＣアドレス（第１アドレス）が記録されていない。従って、判定部５４は、不正装置２００が接続を行うと、当該接続は正当でないと判定することができる。

【００２７】

送信部５３は、送信バッファ（不図示）を備え、ネットワークインタフェース部５１を経由してパケットを受信する。

【００２８】

送信部５３は、判定部５４で要求パケットに含まれる第１アドレスが正当でないと判定した場合、第２装置が第２アドレスを第１装置へ送信する前に、所定のアドレスを含む所定のパケットを第１装置へ送信する。

【００２９】

要求パケットがＡＲＰパケットである場合、第２装置は、第１装置が通信しようとする相手となる情報処理装置２０である。また、要求パケットがＤＨＣＰパケットである場合、第２装置は、ＤＨＣＰサーバ３０である。所定のアドレスは、例えば、ネットワーク上に存在しない偽のアドレスである。

【００３０】

情報処理装置２０又はＤＨＣＰサーバ３０が、不正装置２００の要求パケットに対して応答する場合、例えば、数百μｓから数ｍｓ程度の応答時間を要する。送信部５３は、情報処理装置２０（又はＤＨＣＰサーバ３０）がＭＡＣアドレス（又はＩＰアドレス）を不正装置２００へ送信する前（例えば、数μｓ程度の応答時間内）に所定のアドレスを不正装置２００へ送信する。要求パケットに対して最初に取得する応答を正しいものとして受け取ることに着目すると、不正装置２００が最初に取得する応答には、偽のアドレスが含まれている。このため、許可された情報処理装置２０以外の不正装置２００は、情報処理装置２０と通信することができず、あるいはネットワークに接続することができず、不正装置２００による不正接続を検知し遮断することができる。

【００３１】

送信部５３は、判定部５４で要求パケットに含まれる第１アドレスが正当であると判定した場合、第１装置は、正当な情報処理装置２０であるとして、所定のアドレスを送信しない。これにより、情報処理装置２０は、他の情報処理装置２０（又はＤＨＣＰサーバ３０））からＭＡＣアドレス（又はＩＰアドレス）を取得することができるので、正当な情報処理装置２０と他の情報処理装置２０との間の通信、あるいは正当な情報処理装置２０のネットワークへの接続を行わせることができる。

【００３２】

次に、判定部５４による判定処理の詳細について説明する。

【００３３】

演算部５５は、受信部５２で受信した要求パケットに含まれるＭＡＣアドレスに対して所要のハッシュ関数によるハッシュ演算を行ってハッシュ値を算出する。所要のハッシュ関数は、適宜のハッシュ関数を用いることができる。ハッシュ関数としては、現在利用できるハッシュ関数を用いることができ、例えば、ＦＮＶ、ｈｓｉｅｈ、ｍｕｒｍｕｒ、ｊｅｎｋｉｎｓ、Ｂｕｚｈａｓｈ、ＰＪＷ ｈａｓｈ、ＭＤ４、ＭＤ５、ＲＩＰＥＭＤ、ＲＩＰＥＭＤ－１２８、ＲＩＰＥＭＤ－１６０、ＳＨＡ－１、ＳＨＡ－２２４、ＳＨＡ－２５６、ＳＷＩＦＦＴ、Ｗｈｉｒｌｐｏｏｌなどを用いることができるが、ハッシュ関数はこれらに限定されない。

【００３４】

図３は本実施の形態のメモリ５７のアドレスとアドレスに格納されるデータとの関係の一例を示す模式図である。図３に示すように、メモリ５７は、アドレス（番地）と当該アドレスに格納されるデータとによって構成されている。演算部５５がＭＡＣアドレスに対してハッシュ演算を行うことによって得られたハッシュ値を、例えば、ハッシュ値１、ハッシュ値２…とする。本実施の形態では、メモリ５７の他に不図示のキャッシュ（キャッシュメモリ）を備え、メモリ５７とキャッシュとの間のマッピング方式は、ダイレクトマップ方式でもよく、セットアソシアティブ方式でもよい。以下では、一例としてセットアソシアティブ方式とし、ｗａｙ数をｎで表す。なお、図３の例では、ｗａｙ数ｎを４としている。１エントリー当たりのバイト数をｓとする。バイト数ｓは、ＭＡＣアドレスを格納するバイト数（６バイト）及び関連情報を格納するバイト数の合計となる。以下では、便宜上、関連情報を格納するバイト数を０とする。従って、バイト数ｓは、ＭＡＣアドレスの長さの６バイトとなる。

【００３５】

図３に示すように、ハッシュ値１に基づくアドレスは、エントリー毎に、ハッシュ値１×ｓ×ｎ＋１ｓ、ハッシュ値１×ｓ×ｎ＋２ｓ、ハッシュ値１×ｓ×ｎ＋３ｓ、ハッシュ値１×ｓ×ｎ＋４ｓとなり、それぞれのエントリーに、ＭＡＣアドレス１１、ＭＡＣアドレス１２、ＭＡＣアドレス１３、ＭＡＣアドレス１４が格納されている。同様に、ハッシュ値２に基づくアドレスは、エントリー毎に、ハッシュ値２×ｓ×ｎ＋１ｓ、ハッシュ値２×ｓ×ｎ＋２ｓ、ハッシュ値２×ｓ×ｎ＋３ｓ、ハッシュ値２×ｓ×ｎ＋４ｓとなり、それぞれのエントリーに、ＭＡＣアドレス２１、ＭＡＣアドレス２２、ＭＡＣアドレス２３、ＭＡＣアドレス２４が格納されている。以下、他のハッシュ値に基づくアドレスについても同様である。

【００３６】

なお、図３の例では、ｗａｙ数ｎが４であるが、ｗａｙ数ｎは４に限定されるものではなく、２、８、１６等であってもよい。

【００３７】

すなわち、メモリ５７は、複数の正当なＭＡＣアドレスに対してハッシュ演算を行って得られたハッシュ値に基づくアドレスに複数のＭＡＣアドレスを対応付けて記憶する。具体的には、アドレスは、ハッシュ値×ｓ×ｎで表すことができる。ここで、ｓは１エントリー当たりのバイト数であり、ｎはｗａｙ数である。

【００３８】

ハッシュ演算によってＭＡＣアドレスのビット数よりも少ないビット数のハッシュ値を得ることができる。メモリ５７は、例えば、ＤＲＡＭ（Dynamic Random Access Memory）とすることができ、ハッシュ値に基づく値をアドレスに対応させ、当該アドレスにハッシュ値に対応するＭＡＣアドレス（ハッシュ演算によって当該ハッシュ値を得ることができたＭＡＣアドレス）を記憶する。これにより、メモリ５７のメモリ空間のどのアドレスを参照するかがハッシュ値によって決定される。

【００３９】

判定部５４は、演算部５５で演算して得られたハッシュ値に基づくメモリ５７のアドレスを参照し、参照したアドレスにＭＡＣアドレスが記憶されていない場合、要求パケットに含まれるＭＡＣアドレスが正当ではないと判定する。

【００４０】

メモリ５７のアドレスがハッシュ値に基づく値に対応し、当該アドレスに記憶したデータがＭＡＣアドレスに対応するので、演算部５５で演算して得られたハッシュ値に基づくアドレスにＭＡＣアドレスが記憶されていない場合、要求パケットに含まれるＭＡＣアドレスが正当ではないと判定することができる。

【００４１】

これにより、演算部５５で演算して得られたハッシュ値に基づくアドレスを１回アクセス（例えば、READコマンド）するだけで、要求パケットに含まれるＭＡＣアドレスが正当であるか否かを判定することができ、判定処理に要する時間を短縮することができ、受信

部５２で要求パケットを取得した時点から送信部５３で偽のアドレスを含む所定のパケットを送信する時点までの時間を数μｓ程度に短縮することができる。

【００４２】

また、（ｎ－ｗａｙ）方式を用いることによって、１つのハッシュ値に対応して複数（ｎ個）のＭＡＣアドレスが同時に得られるので、メモリ５７のアクセススピードが遅い場合でも、遅いアクセススピードを補完することができる。また、同一のハッシュ値に対してｗａｙ数（例えば、４など）に相当する数のＭＡＣアドレスを格納することができるので、ハッシュ値に対応するＭＡＣアドレスのコンフリクトをｗａｙ数の分だけ容認することができる。

【００４３】

パイプライン処理部５６は、受信部５２で要求パケットを取得する都度、メモリ５７に記憶したＭＡＣアドレスをパイプライン処理で読み出す。例えば、READコマンドによってＭＡＣアドレスを読み出す場合、パイプライン処理部５６は、READコマンドによってＭＡＣアドレスが読み出される前に当該READコマンドの次のREADコマンドを出力することができる。

【００４４】

判定部５４は、パイプライン処理部５６で読み出した結果に基づいて、要求パケットに含まれるＭＡＣアドレスが正当であるか否かを判定する。例えば、メモリ５７からＭＡＣアドレスが読み出された場合、要求パケットに含まれるＭＡＣアドレスは正当であると判定することができる。また、メモリ５７からＭＡＣアドレスを読み出すことができない場合、要求パケットに含まれるＭＡＣアドレスは正当でないと判定することができる。パイプライン処理部５６を備えることにより、要求パケットの取得頻度が高くなった場合でも、判定部５４による判定処理に要する時間を短縮することができる。

【００４５】

決定部５８は、受信部５２で取得したパケットが要求パケットであるか否かに応じてパイプライン処理部５６の処理の実行・停止を決定する。例えば、取得したパケットが要求パケットである場合、パイプライン処理部５６の処理を実行する。また、取得したパケットが要求パケット以外の任意のパケットである場合、パイプライン処理部５６の処理を停止することができる。これにより、要求パケットを取得したときだけ、パイプライン処理部５６の処理を実行して、判定部５４による判定処理に要する時間を短縮することができる。

【００４６】

図４はパイプライン処理部５６の処理を停止した場合の処理の一例を示す模式図である。図４の例では、パケットを取得したときにメモリ５７のデータを読み出す処理が行われるとする。図４に示すように、要求パケット以外の他のパケットＡ１を取得すると、メモリ５７のデータを読み出すべくREADコマンドａ１が出力されるとする。また、パケットＡ１に後にパケットＡ２を取得したとし、メモリ５７のデータを読み出すべくREADコマンドａ２が出力されるとする。パイプライン処理部５６の処理を停止した場合、READコマンドａ２は、READコマンドａ１によりデータａ１が読み出された後に出力される。すなわち、複数回のREADコマンドでデータをメモリ５７から読み出す時間は比較的長くなる。

【００４７】

図５はパイプライン処理部５６の処理を実行した場合の処理の一例を示す模式図である。図５に示すように、短い時間の間に要求パケットＢ１、Ｂ２、Ｂ３を取得したとする。要求パケットＢ１を取得すると、メモリ５７のＭＡＣアドレスを読み出すべくREADコマンドｂ１が出力されるとする。要求パケットＢ２、Ｂ３についても同様に、READコマンドｂ２、ｂ３が出力されるとする。

【００４８】

パイプライン処理部５６の処理を実行した場合、READコマンドｂ２は、READコマンドｂ１によりデータｂ１が読み出されるのを待つことなく出力される。また、READコマンドｂ３は、READコマンドｂ２によりデータｂ２が読み出されるのを待つことなく出力される。

すなわち、複数回のREADコマンドでＭＡＣアドレスをメモリ５７から読み出す時間は短くなる。

【００４９】

本実施の形態では、判定部５４又は演算部５５での処理は、ハードウェアで行うことができる。例えば、判定部５４又は演算部５５をＦＰＧＡ（Field-Programmable Gate Array）又はＡＳＩＣ（Application Specific Integrated Circuit）等の半導体チップで構成することができる。

【００５０】

これにより、判定部５４又は演算部５５での処理をソフトウェアで実行する場合に比べて処理時間を大幅に短縮することができ、受信部５２で要求パケットを取得した時点から送信部５３で偽のアドレスを含む所定のパケットを送信する時点までの時間を数μｓ程度に短縮することができる。

【００５１】

次に、本実施の形態の不正接続遮断装置５０の動作について説明する。以下では、要求パケットをＡＲＰパケット、ＤＨＣＰパケットとして説明する。

【００５２】

図６は本実施の形態の不正接続遮断装置５０によるＡＲＰパケットの場合の不正接続遮断動作の一例を示す説明図である。ＡＲＰは、ＩＰアドレスからイーサネット（登録商標）のＭＡＣアドレスの情報が得られるプロトコロルであり、通信相手のＩＰアドレスから実際のＭＡＣアドレスを調べるために利用される。ＴＣＰ／ＩＰを利用したＬＡＮ通信では、ＩＰアドレスとＭＡＣアドレスの二つのアドレスが分かることで通信を行うことができる。

【００５３】

図６に示すように、不正装置２００のＩＰアドレスを、１９２．１６８．０．１とし、ＭＡＣアドレスを、００００．００００．１１１１とする。情報処理装置２０のＩＰアドレスを、１９２．１６８．０．５とし、ＭＡＣアドレスを００００．００００．５５５５とする。

【００５４】

不正装置２００は、情報処理装置２０と通信を行いたいとする。不正装置２００は、ＡＲＰリクエストをブロードキャストする（符号Ｐ１）。ブロードキャストは、ＡＲＰリクエストがネットワーク上の全ての装置に送信される。ＡＲＰリクエストは、情報処理装置２０（ＩＰアドレスが１９２．１６８．０．５のＭＡＣアドレスを要求する。

【００５５】

仮に、不正接続遮断装置５０がネットワークに接続されていないとすると、情報処理装置２０は、ＡＲＰリクエストを取得し、ＡＲＰリクエストにより探索しているＩＰアドレスが自分のＩＰアドレスと同一であると分かると、自身のＭＡＣアドレス：０００００．００００．５５５５を不正装置２００へ伝えるため、ＡＲＰリプライをユニキャストで送信する（符号Ｐ３）。ユニキャストは、特定の相手だけに送信される。情報処理装置２０が、ＡＲＰリクエストを取得してからＡＰＲリプライを送信するまでの時間は、数百μｓから数ｍｓ程度の時間である。

【００５６】

しかし、本実施の形態では、不正接続遮断装置５０がネットワークに接続されているので、不正接続遮断装置５０は、情報処理装置２０がＡＲＰリプライを送信する時点よりも相当前の時点でＡＲＰリプライをユニキャストで不正装置２００へ送信する（符号Ｐ２）。不正接続遮断装置５０が送信するＡＲＰリプライには、ＭＡＣアドレス：ｘｘｘｘ．ｙｙｙｙ．ｚｚｚｚ（存在しないＭＡＣアドレス）が含まれる。不正接続遮断装置５０が、ＡＲＰリクエストを取得してからＡＰＲリプライを送信するまでの時間は、数μｓ程度の時間である。

【００５７】

不正装置２００は、最初に取得するＡＲＰリプライが正しいパケットであると認識する

。このため、不正装置２００は、存在しないＭＡＣアドレス：ｘｘｘｘ．ｙｙｙｙ．ｚｚｚｚを用いても情報処理装置２０と通信を行うことができないので、不正接続を遮断することができる。

【００５８】

次に、要求パケットがＤＨＣＰパケットである場合について説明する。

【００５９】

図７はＤＨＣＰパケットのイーサネットフレームの構成を示す模式図である。図７に示すように、ＤＨＣＰパケットのイーサネットフレームは、イーサネットヘッダ、ＩＰヘッダ、ＵＤＰヘッダ及びＤＨＣＰメッセージの各要素で構成される。イーサネットヘッダには、宛先ＭＡＣアドレス及び送信元ＭＡＣアドレスなどが格納され、ＩＰヘッダには、送信元ＩＰアドレス及び宛先ＩＰアドレスなどが格納され、ＵＤＰ（User Datagram Protocol）ヘッダには、送信元ポート及び宛先ポートなどが格納される。ＤＨＣＰメッセージには、ＤＨＣＰDiscover(ＤＨＣＰディスカバー)、ＤＨＣＰOffer（ＤＨＣＰオファー）、ＤＨＣＰRequest（ＤＨＣＰリクエスト）、ＤＨＣＰAck（ＤＨＣＰアック）のいずれかが格納される。

【００６０】

図８は本実施の形態の不正接続遮断装置５０によるＤＨＣＰパケットの場合の不正接続遮断動作の一例を示す説明図である。ＤＨＣＰは、ネットワーク接続するのに必要なＩＰアドレスを自動的に割り当てるプロトコルであり、自身のＩＰアドレスを取得するために利用される。例えば、コンピュータ起動時、Ｗｉｆｉ接続時などに自動的に利用される。

【００６１】

図８に示すように、不正装置２００のＩＰアドレスを、０．０．０．０とし、ＭＡＣアドレスを、０００００．００００．１１１１とする。ＤＨＣＰサーバ３０のＩＰアドレスを、１９２．１６８．０．１０とし、ＭＡＣアドレスを０００００．００００．８８８８とする。

【００６２】

不正装置２００がネットワーク接続する場合、不正装置２００は、自身のＩＰアドレス（暫定的に０．０．０．０と表す）、及びＤＨＣＰサーバ３０のＩＰアドレスを知らない。そこで、不正装置２００は、ＤＨＣＰディスカバーをブロードキャストする（符号Ｐ１１）。ＤＨＣＰディスカバーは、ＩＰアドレスを要求するパケットである。

【００６３】

仮に、不正接続遮断装置５０がネットワークに接続されていないとすると、ＤＨＣＰサーバ３０は、ＤＨＣＰディスカバーを取得し、不正装置２００に割り当てるＩＰアドレスを含むＤＨＣＰオファーをブロードキャストで不正装置２００へ送信する（符号Ｐ１３）。ＤＨＣＰサーバ３０が、ＤＨＣＰディスカバーを取得してからＤＨＣＰオファーを送信するまでの時間は、数百μｓから数ｍｓ程度の時間である。

【００６４】

しかし、本実施の形態では、不正接続遮断装置５０がネットワークに接続されているので、不正接続遮断装置５０は、ＤＨＣＰサーバ３０がＤＨＣＰオファーを送信する時点よりも相当前の時点でＤＨＣＰオファーをブロードキャストで不正装置２００へ送信する（符号Ｐ１２）。不正接続遮断装置５０が送信するＤＨＣＰオファーには、隔離されたＩＰアドレスが含まれる。隔離されたＩＰアドレスとは、例えば、ネットワークに全くアクセスすることができないＩＰアドレス、あるいは所定の認証処理が要求されるＩＰアドレスである。不正接続遮断装置５０が、ＤＨＣＰディスカバーを取得してからＤＨＣＰオファーを送信するまでの時間は、数μｓ程度の時間である。

【００６５】

同様に、不正接続遮断装置５０は、不正装置２００が送信したＤＨＣＰリクエスト（ＩＰアドレスを使用する旨を通知するパケット）に対して（符号Ｐ１４）、ＤＨＣＰサーバ３０がＤＨＣＰアックを送信する時点（符号Ｐ１６）よりも相当前の時点（符号Ｐ１５）で、ＤＨＣＰアックを送信する。

【００６６】
不正装置２００は、最初に取得するＤＨＣＰオファー、ＤＨＣＰアックが正しいパケットであると認識する。このため、不正装置２００は、隔離されたＩＰアドレスを用いてネットワーク接続を試みてもネットワークに接続することができず、不正接続を遮断することができる。
【００６７】
上述では、要求パケットとしてＡＲＰパケット及びＤＨＣＰパケットについて説明したが、要求パケットは、ＡＲＰパケット及びＤＨＣＰパケットに限定されるものではない。例えば、ＩＰｖ６のＩＰアドレス設定方法の一つとしてステートレス自動設定の場合にも本実施の形態を適用することができる。
【００６８】
ステートレス自動設定の場合、不正装置２００は、ＩＰアドレスを取得するため、ＲＳ（Router Solicitation）メッセージをネットワーク上のルータ宛に送信する。なお、要求パケットは、ＲＳメッセージを含むものとする。
【００６９】
仮に、不正接続遮断装置５０がネットワークに接続されていないとすると、ルータは、ＩＰアドレスの設定に必要な情報が含まれたＲＡ（Router Advertisement）メッセージを不正装置２００へ送信する。
【００７０】
しかし、本実施の形態では、不正接続遮断装置５０がネットワークに接続されているので、不正接続遮断装置５０は、ルータがＲＡメッセージを送信する時点よりも相当前の時点でＲＡメッセージを不正装置２００へ送信する。不正接続遮断装置５０が送信するＲＡメッセージには、隔離されたＩＰアドレスが含まれる。
【００７１】
不正装置２００は、最初に取得するＲＡメッセージが正しいメッセージであると認識する。このため、不正装置２００は、隔離されたＩＰアドレスを用いてネットワーク接続を試みてもネットワークに接続することができず、不正接続を遮断することができる。
【００７２】
次に、ホワイトリスト５７１（正当なＭＡＣアドレスのリスト）のメモリ５７への登録方法について説明する。
【００７３】
管理サーバ１００は、ホワイトリスト５７１の追加、削除、更新などの管理を行うサーバである。最新のホワイトリスト５７１は、管理サーバ１００から不正接続遮断装置５０へ送信される。
【００７４】
登録処理部６０は、正当アドレス取得部としての機能を有し、管理サーバ１００が送信したホワイトリスト５７１を取得し、取得したホワイトリスト５７１をメモリ５７に登録（記憶）する。登録処理部６０は、ホワイトリスト５７１を登録する場合、メモリ５７のアドレスをＭＡＣアドレスのハッシュ値とし、当該アドレスに格納されるデータをＭＡＣアドレスとする。
【００７５】
図９は本実施の形態の不正接続遮断装置５０による不正接続遮断処理の手順の一例を示すフローチャートである。不正接続遮断装置５０は、パケットを受信（取得）したか否かを判定し（Ｓ１１）、パケットを受信していない場合（Ｓ１１でＮＯ）、ステップＳ１１の処理を続ける。
【００７６】
パケットを受信した場合（Ｓ１１でＹＥＳ）、不正接続遮断装置５０は、受信したパケットがＡＲＰリクエスト又はＤＨＣＰディスカバーであるか否かを判定する（Ｓ１２）。受信したパケットがＡＲＰリクエスト又はＤＨＣＰディスカバーである場合（Ｓ１２でＹＥＳ）、不正接続遮断装置５０は、受信したパケットに含まれる送信元のＭＡＣアドレス

を取得する（Ｓ１３）。
【００７７】
不正接続遮断装置５０は、取得したＭＡＣアドレスに対してハッシュ演算を行い（Ｓ１４）、パイプライン処理をオン（実行する）とし（Ｓ１５）、ハッシュ演算によって得られたハッシュ値に基づくアドレスに格納されたＭＡＣアドレスを読み出すことによって、メモリ５７のホワイトリスト５７１からＭＡＣアドレスを読み出す（Ｓ１６）。
【００７８】
不正接続遮断装置５０は、ＭＡＣアドレスを読み出すことができたか否かに応じて、送信元のＭＡＣアドレスが正当であるか否かを判定する（Ｓ１７）。送信元のＭＡＣアドレスが正当ではない場合（Ｓ１７でＮＯ）、不正接続遮断装置５０は、偽のＭＡＣアドレスを付加してＡＲＰリプライを送信、あるいは偽のＩＰアドレスを付加してＤＨＣＰオファー送信する（Ｓ１８）。
【００７９】
不正接続遮断装置５０は、ＤＨＣＰリクエストを受信したか否かを判定し（Ｓ１９）、ＤＨＣＰリクエストを受信した場合（Ｓ１９でＹＥＳ）、ＤＨＣＰアックを送信し（Ｓ２０）、処理を終了する。
【００８０】
受信したパケットがＡＲＰリクエスト又はＤＨＣＰディスカバーでない場合（Ｓ１２でＮＯ）、送信元のＭＡＣアドレスが正当ではない場合（Ｓ１７でＮＯ）、あるいは、ＤＨＣＰリクエストを受信していない場合（Ｓ１９でＮＯ）、不正接続遮断装置５０は、処理を終了する。
【００８１】
上述のとおり、本実施の形態によれば、ネットワーク構成を変更することなく、ネットワークでの不正接続を検知・遮断することができる。
【００８２】
不正装置を遮断する方法として、以下のような手法も考えられる。すなわち、端末装置からのパケットを検出し、検出したパケットに含まれるＭＡＣアドレスがホワイトリストに存在しない場合、当該端末装置を不正装置として検知する。次に、偽のＭＡＣアドレスを含むＡＲＰリプライ（ＧＡＲＰ：Gratuitous ARP）を当該不正装置に対して送信することにより、当該不正装置のＡＲＰキャッシュを更新する。これにより、当該不正装置はネットワーク上の情報処理装置と通信することができなくなる。このような手法は、ＡＲＰ Poisoningとも称されている。しかし、このような手法への対策が行われ始めており、また攻撃者が盗聴などを行うため用いる攻撃手法でもある。かかる手法は、ＡＲＰのみ対応可能であるが、本実施の形態によれば、ＡＲＰだけでなくＤＨＣＰにも対応することができ、不正接続の検知・遮断を広範囲に適用することができる。
【００８３】
本実施の形態に係る不正接続遮断装置は、ネットワークでの不正接続を遮断する不正接続遮断装置であって、第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得する取得部と、該取得部で取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する判定部と、該判定部で前記第１アドレスが正当でないと判定した場合、前記第２装置が前記第２アドレスを前記第１装置へ送信する前に、所定のアドレスを前記第１装置へ送信する送信部とを備える。
【００８４】
本実施の形態に係る不正接続遮断方法は、ネットワークでの不正接続を遮断する不正接続遮断方法であって、第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得部が取得し、取得された要求パケットに含まれる第１アドレスが正当であるか否かを判定部が判定し、前記第１アドレスが正当でないと判定された場合、前記第２装置が前記第２アドレスを前記第１装置へ送信する前に、所定のアドレスを前記第１装置へ送信部が送信する。
【００８５】

取得部は、第１アドレスを有する第１装置が第２装置に対して第２アドレスを要求する要求パケットを取得する。第１アドレスは、ネットワークに接続される装置の識別に使用するアドレスであり、例えば、ＭＡＣアドレス（Media Access Control address）とすることができる。要求パケットは、例えば、第１装置が第２装置と通信を行うためのＡＲＰ（Address Resolution Protocol）パケット、あるいは、第１装置がネットワークに接続するのに必要なＩＰ（Internet Protocol）アドレスを要求するＤＨＣＰ（Dynamic Host Configuration Protocol）パケットなどを含む。要求パケットがＡＲＰパケットである場合、第２アドレスはＭＡＣアドレスである。また、要求パケットがＤＨＣＰパケットである場合、第２アドレスはＩＰアドレスである。

【００８６】

判定部は、取得部で取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する。予め、ネットワークへの接続が許可された複数の装置の第１アドレスのリスト（ホワイトリストとも称する）を記憶しておく。判定部は、第１装置の第１アドレスが、リストに記録された正当な第１アドレスのいずれかと一致するか否かを判定し、一致する場合には、第１装置による接続は正当であると判定し、一致しない場合には、第１装置による接続は正当でないと判定する。

【００８７】

送信部は、判定部で第１アドレスが正当でないと判定した場合、第２装置が第２アドレスを第１装置へ送信する前に、所定のアドレスを第１装置へ送信する。要求パケットがＡＲＰパケットである場合、第２装置は、第１装置が通信しようとする相手である。また、要求パケットがＤＨＣＰパケットである場合、第２装置は、ＤＨＣＰサーバである。所定のアドレスは、例えば、ネットワーク上に存在しない偽のアドレスである。

【００８８】

第２装置が、第１装置の要求パケットに対して応答する場合、例えば、数百μｓから数ｍｓ程度の応答時間を要する。送信部は、第２装置が第２アドレスを第１装置へ送信する前、例えば、数μｓ程度の応答時間内に所定のアドレスを第１装置へ送信する。第１装置は、要求パケットに対して最初に取得する応答を正しいものとして受け取る。しかし、最初に取得する応答には、偽のアドレスが含まれているため、第１装置は、第２装置と通信することができず、あるいはネットワークに接続することができず、不正な第１装置による不正接続を遮断することができる。

【００８９】

本実施の形態に係る不正接続遮断装置において、前記送信部は、前記判定部で前記第１アドレスが正当であると判定した場合、前記所定のアドレスを前記第１装置へ送信しない。

【００９０】

送信部は、判定部で第１アドレスが正当であると判定した場合、所定のアドレスを第１装置へ送信しない。これにより、第１装置は、第２装置から第２アドレスを取得することができるので、正当な第１装置と第２装置との間の通信、あるいは正当な第１装置のネットワークへの接続を行わせることができる。

【００９１】

本実施の形態に係る不正接続遮断装置は、複数の正当な第１アドレスを記憶した記憶部を備え、前記判定部は、取得した要求パケットに含まれる第１アドレスが前記記憶部に記憶した第１アドレスに一致するか否かに応じて、前記要求パケットに含まれる第１アドレスが正当であるか否かを判定する。

【００９２】

記憶部は、複数の正当な第１アドレスを記憶する。正当な第１アドレスは、例えば、ネットワーク上で他の装置との間の通信が許可された装置の第１アドレス、あるいはネットワークへの接続が許可された装置の第１アドレスとすることができる。

【００９３】

判定部は、取得した要求パケットに含まれる第１アドレスが記憶部に記憶した第１アド

レスに一致するか否かに応じて、要求パケットに含まれる第１アドレスが正当であるか否かを判定する。これにより、許可された装置以外の装置が不正に接続しようとしても、不正接続を遮断することができる。

【００９４】

本実施の形態に係る不正接続遮断装置は、複数の正当な第１アドレスに対してハッシュ演算を行って得られたハッシュ値に基づくアドレスに複数の正当な第１アドレスを対応付けて記憶する記憶部と、取得した要求パケットに含まれる第１アドレスに対して前記ハッシュ演算を行う演算部とを備え、前記判定部は、前記演算部で演算して得られたハッシュ値に基づく前記記憶部のアドレスに正当な第１アドレスが記憶されていない場合、前記要求パケットに含まれる第１アドレスが正当ではないと判定する。

【００９５】

記憶部は、複数の正当な第１アドレスに対してハッシュ演算を行って得られたハッシュ値に基づくアドレスに複数の正当な第１アドレスを対応付けて記憶する。ハッシュ演算によって第１アドレスのビット数よりも少ないビット数のハッシュ値を得ることができる。記憶部は、例えば、ＤＲＡＭ（Dynamic Random Access Memory）とすることができ、ハッシュ値に基づく値をアドレスに対応させ、当該アドレスにハッシュ値に対応する第１アドレス（ハッシュ演算によって当該ハッシュ値を得ることができた第１アドレス）を記憶する。これにより、メモリ空間のどのアドレスを参照するかがハッシュ値によって決定される。

【００９６】

演算部は、取得した要求パケットに含まれる第１アドレスに対して当該ハッシュ演算を行う。これにより、第１アドレスに対応するハッシュ値を得ることができる。

【００９７】

判定部は、演算部で演算して得られたハッシュ値に基づく記憶部のアドレスに正当な第１アドレスが記憶されていない場合、要求パケットに含まれる第１アドレスが正当ではないと判定する。記憶部のアドレスがハッシュ値に基づく値に対応し、当該アドレスに記憶したデータが第１アドレスに対応するので、演算部で演算して得られたハッシュ値に基づくアドレスに第１アドレスが記憶されていない場合、要求パケットに含まれる第１アドレスが正当ではないと判定することができる。これにより、演算部で演算して得られたハッシュ値に基づくアドレスを１回アクセス（例えば、READコマンド）するだけで、要求パケットに含まれる第１アドレスが正当であるか否かを判定することができ、判定処理に要する時間を短縮することができる。

【００９８】

本実施の形態に係る不正接続遮断装置は、前記取得部で要求パケットを取得する都度、前記記憶部に記憶した正当な第１アドレスをパイプライン処理で読み出すパイプライン処理部を備え、前記判定部は、前記パイプライン処理部で読み出した結果に基づいて、取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する。

【００９９】

パイプライン処理部は、取得部で要求パケットを取得する都度、記憶部に記憶した正当な第１アドレスをパイプライン処理で読み出す。例えば、READコマンドによって第１アドレスを読み出す場合、パイプライン処理部は、READコマンドによって第１アドレスが読み出される前に当該READコマンドの次のREADコマンドを出力することができる。

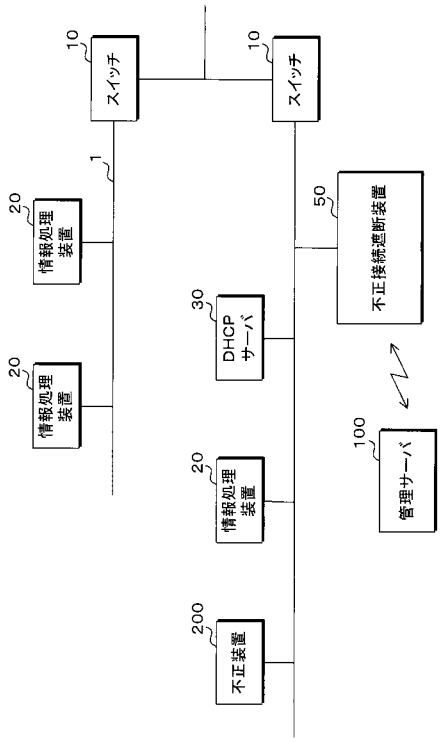
【０１００】

判定部は、パイプライン処理部で読み出した結果に基づいて、取得した要求パケットに含まれる第１アドレスが正当であるか否かを判定する。例えば、第１アドレスが読み出された場合、要求パケットに含まれる第１アドレスが正当であると判定することができる。また、第１アドレスが読み出されない場合、要求パケットに含まれる第１アドレスが正当でないと判定することができる。パイプライン処理部を備えることにより、要求パケットの取得頻度が高くなった場合でも、判定部による判定処理に要する時間を短縮することができる。

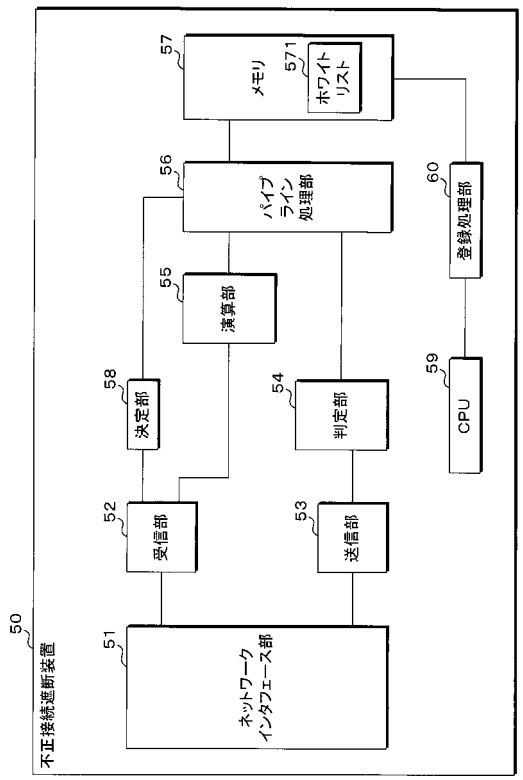
【０１０１】
本実施の形態に係る不正接続遮断装置において、前記取得部は、前記要求パケットを含む任意のパケットを取得し、前記取得部で取得したパケットが要求パケットであるか否かに応じて前記パイプライン処理部の処理の実行・停止を決定する決定部を備える。
【０１０２】
取得部は、要求パケットを含む任意のパケットを取得する。すなわち、取得部は、要求パケットだけでなく、他の任意のパケットも取得する。
【０１０３】
決定部は、取得部で取得したパケットが要求パケットであるか否かに応じてパイプライン処理部の処理の実行・停止を決定する。例えば、取得したパケットが要求パケットである場合、パイプライン処理部の処理を実行し、取得したパケットが要求パケットでない場合、パイプライン処理部の処理を停止することができる。これにより、要求パケットを取得したときだけ、パイプライン処理部の処理を実行して、判定部による判定処理に要する時間を短縮することができる。
【０１０４】
本実施の形態に係る不正接続遮断装置において、前記判定部又は演算部での処理は、ハードウェアで行う。
【０１０５】
判定部又は演算部での処理は、ハードウェアで行う。例えば、判定部又は演算部をＦＰＧＡ（field-programmable gate array）又はＡＳＩＣ（application specific integrated circuit）等の半導体チップで構成することができる。これにより、判定部又は演算部での処理をソフトウェアで実行する場合に比べて処理時間を大幅に短縮することができる。
【０１０６】
本実施の形態に係る不正接続遮断装置において、前記第１アドレスは、ＭＡＣアドレスである。
【０１０７】
第１アドレスは、ＭＡＣアドレスである。これにより、ネットワークに接続しようとしている不正な装置を特定することができる。
【０１０８】
本実施の形態に係る不正接続遮断装置において、前記第２アドレスは、ＭＡＣアドレス又はＩＰアドレスである。
【０１０９】
第２アドレスは、ＭＡＣアドレス又はＩＰアドレスである。これにより、ネットワークへの接続のためにＭＡＣアドレス又はＩＰアドレスを要求する不正な装置による不正接続を遮断することができる。
【０１１０】
本実施の形態に係る不正接続遮断装置において、前記所定のアドレスは、偽のＭＡＣアドレス又はＩＰアドレスである。
【０１１１】
所定のアドレスは、偽のＭＡＣアドレス又はＩＰアドレスである。偽のＭＡＣアドレスは、例えば、ネットワーク上に存在しないＭＡＣアドレスである。また、偽のＩＰアドレスは、隔離されたＩＰアドレスであり、例えば、ネットワークに全くアクセスすることができないＩＰアドレス、あるいは所定の認証処理が要求されるＩＰアドレスである。これにより、不正な第１装置は、ネットワーク上の他の装置との通信を行うことができない、あるいは、ネットワークに接続することができないので、不正接続を遮断することができる。
【符号の説明】
【０１１２】
１　ネットワーク通信線

１０　スイッチ
２０　情報処理装置
３０　ＤＨＣＰサーバ
５０　不正接続遮断装置
５１　ネットワークインタフェース部
５２　受信部
５３　送信部
５４　判定部
５５　演算部
５６　パイプライン処理部
５７　メモリ
５７１　ホワイトリスト
５８　決定部
５９　ＣＰＵ
６０　登録処理部
１００　管理サーバ
２００　不正装置

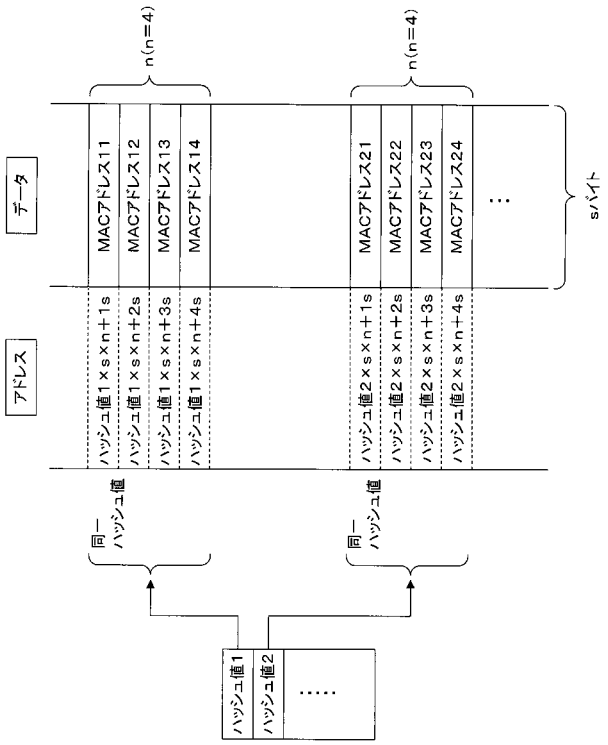
【図１】



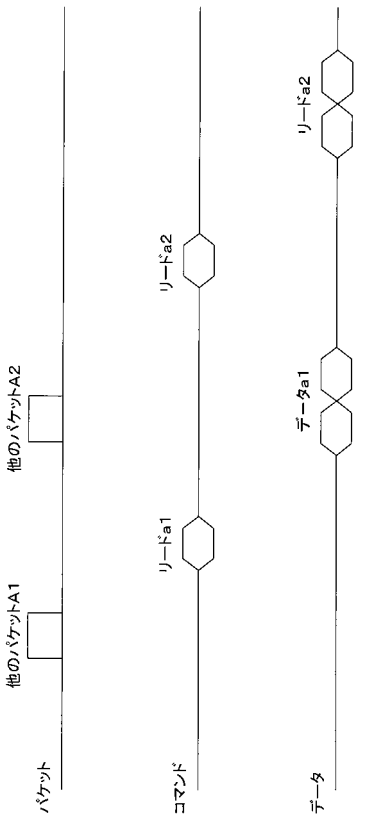
【図２】



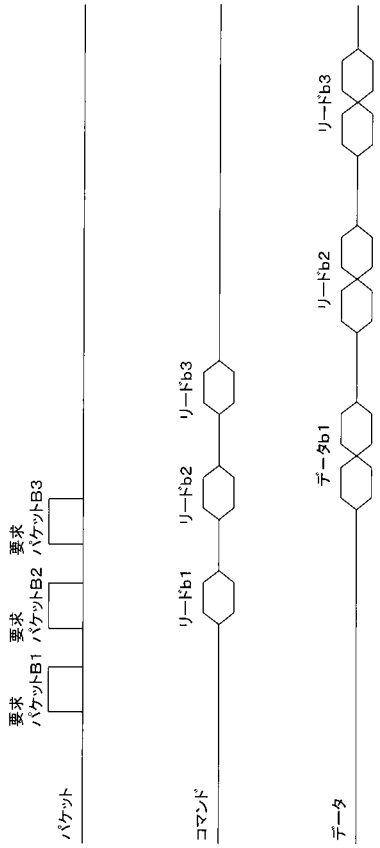
【図３】


データ
アドレス
n(n=4)
n(n=4)
MACアドレスX11
MACアドレスX12
MACアドレスX13
MACアドレスX14
MACアドレスX21
MACアドレスX22
MACアドレスX23
MACアドレスX24
…
sバイト
ハッシュ値1×s×n+1s
ハッシュ値1×s×n+2s
ハッシュ値1×s×n+3s
ハッシュ値1×s×n+4s
ハッシュ値2×s×n+1s
ハッシュ値2×s×n+2s
ハッシュ値2×s×n+3s
ハッシュ値2×s×n+4s
同一ハッシュ値
同一ハッシュ値
ハッシュ値1
ハッシュ値2
……

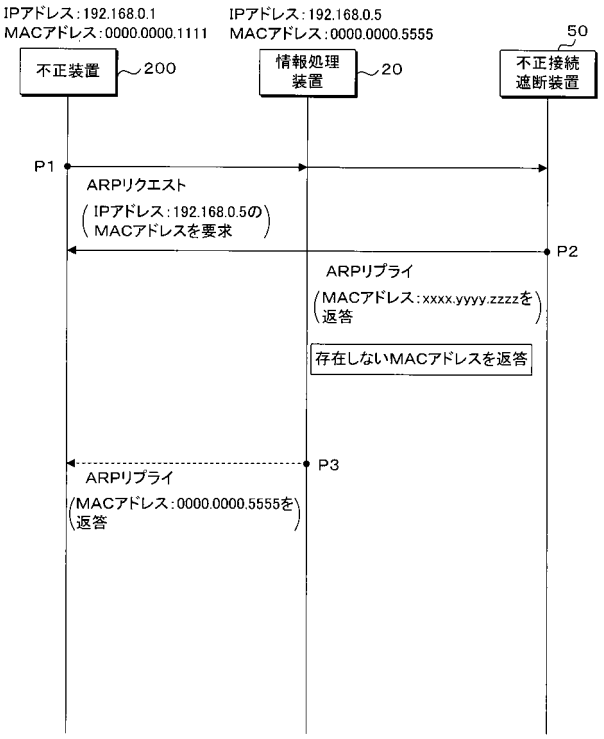
【図４】


他のパケットA2
他のパケットA1
パケット
リードa2
リードa1
コマンド
リードa2
データa1
データ

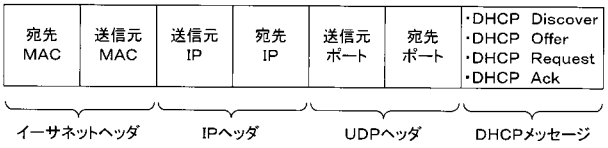
【図５】


要求パケットB3
要求パケットB2
要求パケットB1
パケット
リードb3
リードb2
リードb1
コマンド
リードb3
リードb2
データb1
データ

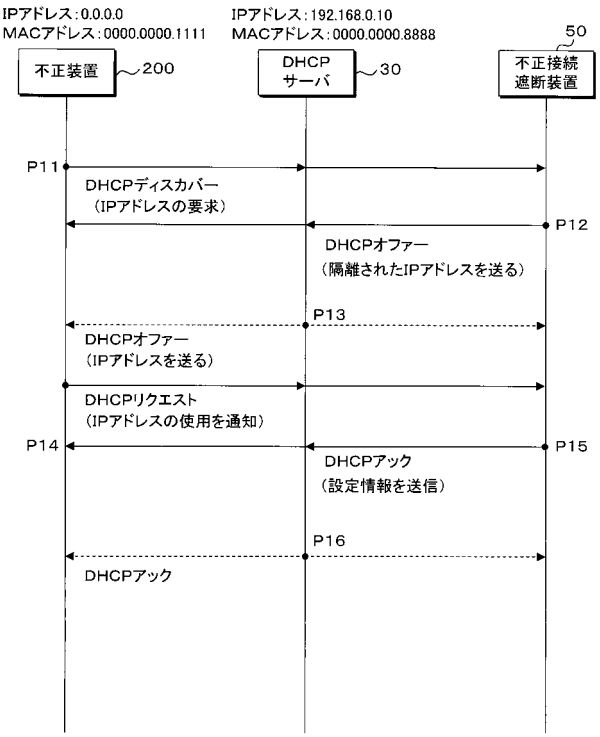
【図６】


IPアドレス:192.168.0.1
MACアドレス:0000.0000.1111
IPアドレス:192.168.0.5
MACアドレス:0000.0000.5555
50
不正装置
200
情報処理装置
20
不正接続遮断装置
P1
ARPリクエスト
(IPアドレス:192.168.0.5のMACアドレスを要求
P2
ARPリプライ
(MACアドレス:xxxx.yyyy.zzzzを返答
存在しないMACアドレスを返答
P3
ARPリプライ
(MACアドレス:0000.0000.5555を返答

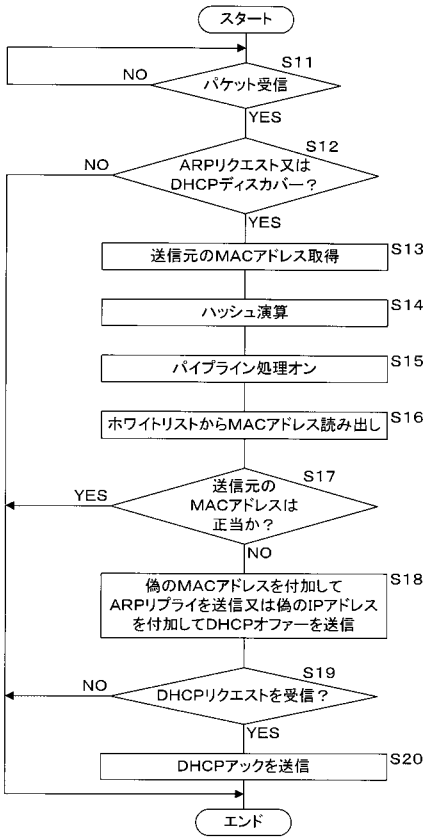
【図７】


宛先 MAC
送信元 MAC
送信元 IP
宛先 IP
送信元 ポート
宛先 ポート
・DHCP Discover
・DHCP Offer
・DHCP Request
・DHCP Ack
イーサネットヘッダ
IPヘッダ
UDPヘッダ
DHCPメッセージ

【図８】


IPアドレス：0.0.0.0
MACアドレス：0000.0000.1111
IPアドレス：192.168.0.10
MACアドレス：0000.0000.8888
50
不正装置
200
DHCP サーバ
30
不正接続 遮断装置
P11
DHCPディスカバー
（IPアドレスの要求）
P12
DHCPオファー
（隔離されたIPアドレスを送る）
P13
DHCPオファー
（IPアドレスを送る）
DHCPリクエスト
（IPアドレスの使用を通知）
P14
P15
DHCPアック
（設定情報を送信）
P16
DHCPアック

【図９】


スタート
S11
パケット受信
NO
YES
S12
ARPリクエスト又は DHCPディスカバー？
NO
YES
送信元のMACアドレス取得
S13
ハッシュ演算
S14
パイプライン処理オン
S15
ホワイトリストからMACアドレス読み出し
S16
S17
送信元の MACアドレスは 正当か？
YES
NO
偽のMACアドレスを付加して ARPリプライを送信又は偽のIPアドレス を付加してDHCPオファーを送信
S18
S19
DHCPリクエストを受信？
NO
YES
DHCPアックを送信
S20
エンド