(19)日本国特許庁(JP)

# 再公表特許(A1)

(11)国際公開番号
WO2015/174100

発行日　平成29年4月20日(2017.4.20)

(43)国際公開日　平成27年11月19日(2015.11.19)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L 12/741 | (2013.01) | H04L | 12/741 | | 5K030 |
| H04L 12/717 | (2013.01) | H04L | 12/717 | | 5K033 |
| H04L 12/46 | (2006.01) | H04L | 12/46 | 100R | |

審査請求 未請求　予備審査請求 未請求　（全 43 頁）

出願番号　特願2016-519125 (P2016-519125)
(21)国際出願番号　PCT/JP2015/050618
(22)国際出願日　平成27年1月13日(2015.1.13)
(31)優先権主張番号　特願2014-100321 (P2014-100321)
(32)優先日　平成26年5月14日(2014.5.14)
(33)優先権主張国　日本国(JP)

(71)出願人　800000068
学校法人東京電機大学
東京都足立区千住旭町５番
(74)代理人　100119677
弁理士　岡田　賢治
(74)代理人　100115794
弁理士　今下　勝博
(72)発明者　小林　浩
東京都足立区千住旭町５番　学校法人東京電機大学内
(72)発明者　末廣　友貴
東京都足立区千住旭町５番　学校法人東京電機大学内

最終頁に続く

(54)【発明の名称】パケット転送装置、パケット転送システム及びパケット転送方法

(57)【要約】
本発明では、不正に流入したパケットを廃棄すること、さらに、すり抜けてインターネットに流入した攻撃パケットや不正パケットについて以後のインターネットへの流出又は流入を阻止することを目的とする。
本発明にかかるパケット転送装置は、複数のポート又は複数のチャネルと、ポート又はチャネルの識別情報と、送信元物理アドレスと送信元論理アドレスとの対応関係を記憶しておくバインディングテーブルと、要請に応じて生成又は更新する廃棄テーブルと、送信元物理アドレスと送信元論理アドレスとの対がバンディングテーブルに存在するときは、次ホップノードへ転送し、バインディングテーブルに存在しないときはパケットを廃棄し、廃棄テーブルに該当するときはパケットを廃棄する転送部と、を備える。

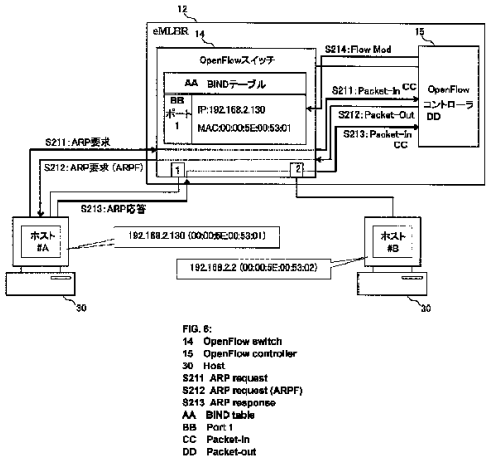



FIG. 6:
14 OpenFlow switch
15 OpenFlow controller
30 Host
S211 ARP request
S212 ARP request (ARPF)
S213 ARP response
AA BIND table
BB Port 1
CC Packet-In
DD Packet-out

【特許請求の範囲】
【請求項１】
互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルと、
前記ポート又は前記チャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと前記フレームをデカプセル化して取り出したパケットの送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルと、
前記フレームを受信した前記ポート又は前記チャネルをキーに前記マルチレイヤ・バインディングテーブルを検索し、前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記マルチレイヤ・バンディングテーブルに存在するときは、前記フレームから取り出されたパケットをフレームにカプセル化して前記パケットの送信先論理アドレスに向けて次ホップノードへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送部と、を備える
ことを特徴とするパケット転送装置。
【請求項２】
互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルと、
前記ポート又は前記チャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと前記フレームをデカプセル化して取り出したパケットの送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルと、
前記フレームを受信した前記ポート又は前記チャネルをキーに前記マルチレイヤ・バインディングテーブルを検索し、前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出されたパケットの送信先論理アドレスに向けて転送するルータへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送部と、を備える
ことを特徴とするパケット転送装置。
【請求項３】
前記パケット転送装置は、
予め接続された他のパケット転送装置に備わる前記転送部から、受信したポート又はチャネルの識別情報とともに送られてきた認証要求パケット又はフレームについて、認証サーバーへの認証要求を仲介し、前記認証サーバーが認証した認証結果を取得し、前記認証結果に基づいて決定した通信サービス品質を前記マルチレイヤ・バインディングテーブルの記憶の対象にし、
前記ポート又は前記チャネルを介して前記認証要求の要求元のノード又はエンティティの実在確認を行って、前記マルチレイヤ・バインディングテーブルを更新し、
前記マルチレイヤ・バインディングテーブルを他のパケット転送装置に備わる前記転送部に伝達する制御部を備え、
前記転送部は、
前記制御部が伝達してきた前記マルチレイヤ・バインディングテーブルを更新する
ことを特徴とする請求項１に記載のパケット転送装置。
【請求項４】
前記制御部は、
前記ポート又はチャネルに接続されるいずれかのノード又はエンティティからの廃棄要請を受け付け、或いは予め定められた所定のノード又はエンティティを定期的にアクセスし取得した廃棄要請に応じて前記転送部の廃棄テーブルを更新し、
前記転送部は、
前記廃棄テーブルに該当するフレーム又はパケットを廃棄する
ことを特徴とする請求項１から３のいずれかに記載のパケット転送装置。

【請求項５】
前記転送部と前記制御部は、互いに連携して、
前記ノード又は前記エンティティがブロードキャスト送信した自装置宛アドレス解決要求フレームに呼応して、前記ノード又は前記エンティティに対してアドレス解決要求フレームを同じポート又はチャネルからブロードキャスト送信し、
前記ポート又は前記チャネルを介して返ってきたアドレス解決応答フレームの送信元物理アドレスと送信元論理アドレスの対と、前記自装置宛アドレス解決要求フレームの送信元物理アドレスと送信元論理アドレスの対とを照合することによって、前記ノード又は前記エンティティの物理アドレスと論理アドレスの真正性を検証し認証する
ことを特徴とする請求項１から４のいずれかに記載のパケット転送装置。
【請求項６】
前記制御部及び前記転送部は、
前記ノード又は前記エンティティが固定のプロセス識別アドレスを有する場合、前記プロセス識別アドレスを前記マルチレイヤ・バインディングテーブルに記憶する対象にすることを特徴とする請求項１から５のいずれかに記載のパケット転送装置。
【請求項７】
ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、レイヤ２スイッチ及びＷ－ＬＡＮ（Ｗｉｒｅｌｅｓｓ Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）各機能の一部又はすべてを含めた一体構造である
ことを特徴とする請求項１から６のいずれかに記載のパケット転送装置。
【請求項８】
前記転送部または前記制御部は、
認証されたノード又はエンティティが送信したパケットを受信した場合、前記パケットの通信プロトコルに応じて予め定められた値を受信したパケットの所定のフィールドに書き込み、未認証のノード又はエンティティが送信したパケットを受信した場合、前記所定のフィールドをリセットする
ことを特徴とする請求項１から７のいずれかに記載のパケット転送装置。
【請求項９】
インターネット利用者側に配置されるパケット転送装置と、
請求項１から８のいずれかに記載のインターネット側に配置されるパケット転送装置と、を備え、インターネット側に配置される前記パケット転送装置は、インターネット利用者側に配置される前記パケット転送装置を迂回又はすり抜けてアドレス詐称パケットが送られても、インターネットへの流入を阻止する
ことを特徴とするパケット転送システム。
【請求項１０】
互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルを、フレームが送られてきたポート又はチャネルの識別情報をキーに検索し、
前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出したパケットをフレームにカプセル化して前記パケットの送信先論理アドレスに向けて次ホップノードへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送手順を有する
ことを特徴とするパケット転送方法。
【請求項１１】
互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと送信元論

理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルを、フレームが送られてきたポート又はチャネルの識別情報をキーに検索し、
前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出したパケットの送信先論理アドレスに向けて転送するルータへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送手順を有する
ことを特徴とするパケット転送方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、パケット転送装置、パケット転送システム及びパケット転送方法に関する。

【背景技術】

【０００２】

年々巧妙化・組織化しているサイバー攻撃は、２０１１年全世界で１兆米ドルの損害を与えたと言われるほど、地球規模での大きな脅威となってきた。とりわけ、ボットウィルスに感染した無数のＰＣでボットネットを形成し、それを操りＷｅｂサイトなどへ攻撃を仕掛けるＤＤｏＳ攻撃は、これまでの「自分を守ろうとするセキュリティ技術」では防ぐことができず、インターネット全体での対策が必要となっている。

【０００３】

ところで、警察庁の発表によれば、２０１２年中に観測されたボットネットによる攻撃では、約９７％がＳＹＮ（ＳＹＮｃｈｒｏｎｉｚｅ） ｆｌｏｏｄ攻撃とＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ） ｆｌｏｏｄ攻撃で、その大半が送信元ＩＰアドレスを詐称（以下、ＩＰアドレス詐称もしくはアドレス詐称）していたことが特徴となっている。ＩＰアドレス詐称対策を行うことが、サイバー攻撃対策として大きな効果を挙げるものと期待される。

【０００４】

ＩＰアドレス詐称が成功する背景には、インターネット上でのルーティングがパケットの宛先ＩＰアドレスだけを見ていることにある。ＩＰアドレス詐称パケットのインターネットへの流入を阻止しようとするイングレス・フィルタリング技術の一つに、受信したパケットの送信元アドレスが経路表に経路情報として存在するかを調べ、経路情報が見つかればそのパケットを転送し、見つからなければ廃棄するｕＲＰＦ（Ｕｎｉｃａｓｔ Ｒｅｖｅｒｓｅ Ｐａｔｈ Ｆｏｒｗａｒｄｉｎｇ）があるが、経路表に記載されたネットワークアドレスのアドレス空間内でのアドレス詐称パケットを中継転送としてしまう不完全性のため、広く導入するまでには至っていない。

【０００５】

また、予め決められた端末以外がネットワークにアクセスしないように認証によってポートに疎通許可を与えるＩＥＥＥ８０２．１Ｘ規格がある。これにＭＡＣアドレスベースのイングレス・フィルタング機能を付加して、たとえリピータハブを介して未認証端末からフレームが送信されても阻止できる製品もあるが、データリンク層での対策であるため、認証を受けた端末がボットウィルスなどに感染しＩＰアドレス詐称パケットを送信しても、認証ＬＡＮスイッチはそれを阻止することはできない。

【０００６】

さらに、企業などの内部ネットワーク向けに、ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）によるアドレス割り当てを監視し、それと整合しないパケットをフィルタリングするＤＨＣＰ ｓｎｏｏｐｉｎｇ技術や、単一のポリシーのもとに情報へのアクセス認可などをコントロールするＴｒｕｓｔｅｄ Ｎｅｔｗｏｒｋ Ｃｏｎｎｅｃｔ技術、他にもＩＰアドレス詐称パケットの発信源を特定しようとするＩＰ ｔｒａｃｅ ｂａｃｋ技術など、様々な試みや製品が出回っているが、いずれもサイバー攻撃を根絶する有効な解決手段とはなっていない（例えば、特許文献１を参照。）。

【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２００３－２８９３３８号公報
【特許文献２】国際公開第２０１２／０７７６０３号
【特許文献３】特開２００７－６８１９０号公報
【特許文献４】ＵＳ２００３／００４３８５３Ａ１
【発明の概要】
【発明が解決しようとする課題】
【０００８】
ところで、関連技術のネットワーク機器では、これまでハードウェアとソフトウェアの両方をベンダーが開発し、それを組み合わせてネットワーク装置として提供していた。ベンダーごとに様々な機能や特徴を持った機器が存在する一方、機器のソフトウェアとハードウェアが一体となっているため、ベンダーが想定するアーキテクチャ以外のネットワーク構成や機能追加ができないのが実情であった。これに対して、ＳＤＮ（Ｓｏｆｔｗａｒｅ　Ｄｅｆｉｎｅｄ　Ｎｅｔｗｏｒｋ）は、ネットワークの構成や機能、性能などをソフトウェアの操作だけで動的に設定・変更できるようにしようとするネットワークや概念を指し、各所で開発が進められている。
【０００９】
次に、インターネット文化とＩＰアドレス詐称対策との関わりにおける課題を説明する。インターネットは、様々なポリシーのもとにインターネットサービスプロバイダー（以下、ＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ））が自律的に運用しているネットワークを相互接続したものである。サイバー攻撃はインターネット全体の問題であり、ＩＰアドレス詐称対策を部分的に導入してもその効果は微々たるものである。無数に存在するＩＳＰや様々な組織、一般利用者のほぼすべてに対策の導入を求めることは極めて困難なことのように思えよう。
【００１０】
しかしながら、インターネット文化には、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）やＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）、メールなどのインターネット基盤技術開発の原動力となった「情報は共有されるべき」や、民主主義の根幹をなす「情報は広く公開されるべき」、政府や官僚、大企業の介入を嫌う「権力は横暴で信用できない」、とともに「クラッキング行為は戒めよ」がある。
【００１１】
すなわち、民主主義に根ざしたインターネットは、利用者の良識ある行為・行動を前提としており、利用を監視したり制限したりするメカニズムや組織はない。あるのはプロトコルの標準化を行うＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）や、ドメイン名やＩＰアドレスなどの有限なインターネット資源を管理するＩＣＡＮＮ（Ｉｎｔｅｒｎｅｔ　Ｃｏｒｐｏｒａｔｉｏｎ　ｆｏｒ　Ａｓｓｉｇｎｅｄ　Ｎａｍｅｓ　ａｎｄ　Ｎｕｍｂｅｒｓ）などのインターネットガバナンスだけである。すなわち、インターネットはオープンだが無防備であり、これを悪用したクラッキング行為は厳に戒めるべきとする考えが根底にある。
【００１２】
ＩＰアドレス詐称パケットは、本人が認識しているか否かはともかく、何等かのクラッキング行為を意図したパケットであることは明らかである。すなわち、ＩＰアドレス詐称パケットがインターネットに流入しないような対策を講じることは、インターネット文化の考え方に沿うものと言えよう。
【００１３】
そして、インターネットの世界は契約で成り立っており、限られた数の一次ＩＳＰの下に、二次／三次ＩＳＰさらに利用者が契約し接続している。従って、一次ＩＳＰが本発明

の費用対効果を認識し導入を決断すれば、下位のＩＳＰ／組織ユーザ／一般ユーザを含めた契約条項として導入を規定できる。

【００１４】

図１及び図２３に示すアドレス詐称対策の対象とすべきノードは（本明細書では、ユーザパケットを生成し送受信するホストと、ユーザパケットの生成は行わずパケットの中継転送を行うルータやスイッチを総称する用語として「ノード」を用いる）、利用者本人が意図としているか否かは別として、サイバー攻撃を行うもしくは加担させられるノードとして、いわゆる一般利用者が利用するＰＣ２６と、スマートフォン２４及び携帯端末２５や、サイバー攻撃の踏み台にされるサーバー１３などの他に、最近では遠隔操作によって不正プログラムが埋め込まれサイバー攻撃に加担されるデジタルテレビ２９や冷蔵庫、プリンタ、ＩＴＶカメラ、さらには既設の家庭用ブロードバンドルータなどがある。これらに加えて、ＩｏＴ（Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎｇｓ）と呼ばれるセンサーや機器などの「モノ」が、２０２０年には全世界で２６０億台がインターネットに接続されると予想されている。これらがウィルスに感染したり、製造工程でマルウェアが埋め込まれ、電力網や鉄道などの社会インフラがサイバー攻撃に曝され、インターネットのみならず社会全体が大混乱に陥ることも懸念されている。

【００１５】

このようなノードは、アドレス詐称による被害において、インターネット１０と接続して主としてマシン同士、すなわちＭ ｔｏ Ｍ型（Ｍａｃｈｉｎｅ ｔｏ Ｍａｃｈｉｎｅ）の端末が攻撃ターゲットとするＩＰアドレスに送信元ＩＰアドレスを詐称してＤＲＤｏＳ（Ｄｉｓｔｒｉｂｕｔｅｄ Ｒｅｆｌｅｃｔｉｏｎ Ｄｅｎｉａｌ ｏｆ Ｓｅｒｖｉｃｅ）攻撃に加担させられるケースも報告されている。さらにユーザ宅内に配置される家庭用ブロードバンドルータに当たる本発明のｅＭＬＢＲ１２であっても、迂回（バイパス）あるいはＷＡＮ回線に直接パソコンを接続し攻撃パケットを送り込むなどの仕掛けが施されればアドレス詐称パケットを外部（インターネット１０）に流出することになるため、これらもアドレス詐称対策の対象とすべきノードである。

【００１６】

また、ネットワークは、ｉＭＬＢＲ１１及びｅＭＬＢＲ１２が含まれるノードの集合であるが、このノードの集合すなわちネットワークをノードと見なし、さらにその集合をネットワークとして扱える、すなわちインターネット１０は階層的かつ回帰的な構造をなしている。したがって、上述の「なんでも繋がせる」ポリシーのネットワーク（Ｕｎｔｒｕｓｔｅｄ Ｉｎｔｅｒｎｅｔ２１）が、本発明（ｉＭＬＢＲ１１又はｅＭＬＢＲ１２）によらない既設ルータを介してインターネット１０に接続しても、それを信頼できないノードの一つと捉えれば良いことになる。なお、インターネット１０は、ホーム認証サーバーとして機能するＨＲＳ２３（Ｈｏｍｅ ＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ Ｓｅｒｖｅｒ）を有する。

【００１７】

しかしながら、多様なポリシーのもとで運用しているＩＳＰや様々な組織、一般利用者の行為・行動を監視・制御したり、ポリシーの強制もしくはＩＰ ｔｒａｃｅ ｂａｃｋに見られるようにＩＳＰのポリシーを抉り出したりするような対策は、受け入れられ難い。すなわち、発信元ＩＰアドレスを詐称しているか否かを利用者側の出口とインターネット１０の入り口とでチェックし、アドレス詐称パケットであればそれを確実に遮断する、さらにこうした対策をすり抜けてインターネットに流入しようとする攻撃パケットや不正パケットを遮断するための必要最小限にして汎用性のある、そして技術的に実現可能な対策であることが課題である。

【００１８】

これは、仮に「なんでも繋がせる」ポリシーのＩＳＰがいたとしても、その存在を否定するものではなく、同ＩＳＰが運用するネットワーク（Ｕｎｔｒｕｓｔｅｄ Ｉｎｔｅｒｎｅｔ２１）や「オニオンルーティング」と呼ばれる仮想回線接続により、通信を複数のノードを経由させることによって接続経路の匿名化を行う匿名ネットワークなどがあって

も、これらのネットワークとの接続点（ｉＭＬＢＲ１１）での検疫を強化し、さらに帯域を狭めることによって攻撃パケットや不正パケットのインターネット１０への流入を抑制すれば良いことを意味する。すなわち、上述の課題を満たし得る対策であれば、国際法の制定などを待たずに、民間ベースの契約で地球規模での導入が可能と考えられる。

【００１９】

前記課題を解決するために、本発明は、認証要求を行うサプリカントを有し、その真正性が認証された端末はもとより、サプリカントを有せずしかもＯＳのバージョンアップやファイアウォール機能を持たないまったく無防備な端末（デジタルテレビなどのスマート家電）から送出されるアドレス詐称パケットのインターネット１０への流出並びにインターネット１０への流入を阻止する。さらに、上記対策をすり抜けてインターネット１０に流入した攻撃パケットや不正パケットについても、これを検出したノードからの要請によって、以後、インターネット１０への流出並びにインターネット１０への流入を阻止する。

【課題を解決するための手段】

【００２０】

上記目的を達成するため、本発明では、パケット転送装置（ｉＭＬＢＲ及びｅＭＬＢＲ）のポート又はチャネルの識別情報と送信元物理（所謂ＭＡＣ）アドレスと送信元論理（所謂ＩＰ）アドレスとの対応関係を管理し、フレーム／パケットを受信したポート又はチャネルの識別情報をキーにこの対応関係が存在するかを調べ、対応関係が存在しないパケットをアドレス詐称パケットとみなして廃棄する。さらに、上記対策をすり抜けてインターネットに流入した攻撃パケットや不正パケットを検出したノードからの要請を受けて廃棄テーブルを生成・更新し、この廃棄テーブルに該当するパケットを廃棄する。

【００２１】

具体的には、本発明に係るパケット転送装置は、

互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルと、

前記ポート又は前記チャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと前記フレームをデカプセル化して取り出したパケットの送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルと、

前記フレームを受信した前記ポート又は前記チャネルをキーに前記マルチレイヤ・バインディングテーブルを検索し、前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出されたパケットをフレームにカプセル化して前記パケットの送信先論理アドレスに向けて次ホップノードへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送部と、を備える。

【００２２】

具体的には、本発明に係るパケット転送装置は、

互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルと、

前記ポート又は前記チャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと前記フレームをデカプセル化して取り出したパケットの送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルと、

前記フレームを受信した前記ポート又は前記チャネルをキーに前記マルチレイヤ・バインディングテーブルを検索し、前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出されたパケットの送信先論理アドレスに向けて転送するルータへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送部と、を備える。

【００２３】

本発明に係るパケット転送装置は、
予め接続された他のパケット転送装置に備わる前記転送部から、受信したポート又はチャネルの識別情報とともに送られてきた認証要求パケット又はフレームについて、認証サーバーへの認証要求を仲介し、前記認証サーバーが認証した認証結果を取得し、前記認証結果に基づいて決定した通信サービス品質を前記マルチレイヤ・バインディングテーブルの記憶の対象にし、
前記ポート又は前記チャネルを介して前記認証要求の要求元のノード又はエンティティの実在確認を行って、前記マルチレイヤ・バインディングテーブルを更新し、
前記マルチレイヤ・バインディングテーブルを他のパケット転送装置に備わる前記転送部に伝達する制御部を備え、
前記転送部は、
前記制御部が伝達してきた前記マルチレイヤ・バインディングテーブルを更新してもよい。

【００２４】
本発明に係るパケット転送装置では、
前記ポート又はチャネルに接続されるいずれかのノード又はエンティティからの廃棄要請を受け付け、或いは予め定められた所定のノード又はエンティティを定期的にアクセスし取得した廃棄要請に応じて前記転送部の廃棄テーブルを更新し、
前記転送部は、
前記廃棄テーブルに該当するフレーム又はパケットを廃棄してもよい。

【００２５】
本発明に係るパケット転送装置では、
前記転送部と前記制御部は、互いに連携して、
前記ノード又は前記エンティティがブロードキャスト送信した自装置宛アドレス解決要求フレームに呼応して、前記ノード又は前記エンティティに対してアドレス解決要求フレームを同じポート又はチャネルからブロードキャスト送信し、
前記ポート又は前記チャネルを介して返ってきたアドレス解決応答フレームの送信元物理アドレスと送信元論理アドレスの対と、前記自装置宛アドレス解決要求フレームの送信元物理アドレスと送信元論理アドレスの対とを照合することによって、前記ノード又は前記エンティティの物理アドレスと論理アドレスの真正性を検証し認証してもよい。

【００２６】
本発明に係るパケット転送装置では、
前記制御部及び前記転送部は、
前記ノード又は前記エンティティが固定のプロセス識別アドレスを有する場合、前記プロセス識別アドレスを前記マルチレイヤ・バインディングテーブルに記憶する対象にしてもよい。

【００２７】
本発明に係るパケット転送装置では、
ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、レイヤ２スイッチ及びＷ－ＬＡＮ（Ｗｉｒｅｌｅｓｓ Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）各機能の一部又はすべてを含めた一体構造であってもよい。

【００２８】
本発明に係るパケット転送装置では、
前記転送部または前記制御部は、
認証されたノード又はエンティティが送信したパケットを受信した場合、前記パケットの通信プロトコルに応じて予め定められた値を受信したパケットの所定のフィールドに書き込みを行ってもよい。また、未認証のノード又はエンティティが送信したパケットを受信した場合、前記所定のフィールドをリセットしてもよい。

【００２９】
具体的には、本発明に係るパケット転送システムは、

インターネット利用者側に配置されるパケット転送装置と、
インターネット側に配置されるパケット転送装置と、を備え、インターネット側に配置される前記パケット転送装置は、インターネット利用者側に配置される前記パケット転送装置を迂回又はすり抜けてアドレス詐称パケットが送られても、インターネットへの流入を阻止する。

【００３０】

具体的には、本発明に係るパケット転送方法は、
互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルを、フレームが送られてきたポート又はチャネルの識別情報をキーに検索し、
前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出したパケットをフレームにカプセル化して前記パケットの送信先論理アドレスに向けて次ホップノードへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送手順を有する。

【００３１】

具体的には、本発明に係るパケット転送方法は、
互いにパケットをフレームにカプセル化して送受信する少なくとも一つのノード又は少なくとも一つのエンティティを収容する複数のポート又は複数のチャネルの識別情報と前記ノード又は前記エンティティが送信する前記フレームの送信元物理アドレスと送信元論理アドレスとの対応関係を記憶しておくマルチレイヤ・バインディングテーブルを、フレームが送られてきたポート又はチャネルの識別情報をキーに検索し、
前記フレームの送信元物理アドレスと送信元論理アドレスとの対が前記バンディングテーブルに存在するときは、前記フレームから取り出したパケットの送信先論理アドレスに向けて転送するルータへ転送し、前記マルチレイヤ・バインディングテーブルに存在しないときは前記パケットを廃棄する転送手順を有する。

【発明の効果】

【００３２】

本発明によるパケット転送装置を、インターネット１０の端部に所謂エッジルータ（ｉＭＬＢＲ１１）として配備すれば、アドレス詐称パケットや攻撃パケット、不正パケットのインターネット１０への流入を阻止する。さらに、本発明によるパケット転送装置を、インターネット利用者側で所謂ブロードバンドルータなど（ｅＭＬＢＲ１２）として配備すれば、アドレス詐称パケットや攻撃パケット、不正パケットのインターネット１０への流出を阻止する。

【図面の簡単な説明】

【００３３】

【図１】本実施形態に係るネットワークの構成図の一例を示す。
【図２】本実施形態に係るｅＭＬＢＲの構成図の一例を示す。
【図３】本実施形態に係るｉＭＬＢＲの構成図の一例を示す。
【図４】本実施形態に係る複数の通信機能を有するネットワークの構成要素の一例を示す。
【図５】本実施形態に係るＡＲＰリフレクションを用いたＩＥＥＥ８０２．１Ｘ非対応ノードとｅＭＬＢＲ間の認証及び上りパケットの転送シーケンスの一例を示す。
【図６】本実施形態に係る通信手順における構成図の一例を示す。
【図７】本実施形態に係る通信手順におけるテーブルの一例を示す。
【図８】本実施形態に係る通信手順におけるフローチャートの一例を示す。
【図９】本実施形態に係るパケット転送方法を適用した評価結果を示す。
【図１０】本実施形態に係るパケット転送方法を適用した評価結果を示す。

【図１１】本実施形態に係る複数の通信機能を有するネットワークの構成の一例を示す。
【図１２】本実施形態に係るＩＥＥＥ８０２．１Ｘ対応ノードとｅＭＬＢＲ間の認証及び上りパケットの転送シーケンスの一例を示す。
【図１３】本実施形態に係る複数の通信機能を有するネットワークの一例を示す。
【図１４】本実施形態に係るｅＭＬＢＲ－Ｒ（一般住宅向け）とｉＭＬＢＲ間の相互認証及び上りパケットの転送シーケンスの一例を示す。
【図１５】本実施形態に係る複数の通信機能を有するネットワークの構成の一例を示す。
【図１６】本実施形態に係る複数の通信機能を有するネットワークの構成の一例を示す。
【図１７】本実施形態に係る帯域制限によるＴＶオンラインデータサービスにおける応答性評価の評価環境の一例を示す。
【図１８】本実施形態に係るＴＶオンラインデータサービスの応答性評価のフローテーブルの一例を示す。
【図１９】本実施形態に係るＴＶオンラインデータサービスの応答性評価の評価結果を示す。
【図２０】本実施形態に係るＴＶオンラインデータサービスの応答性評価の評価結果を示す。
【図２１】本実施形態に係るＩＥＥＥ８０２．１Ｘ対応端末とｅＭＬＢＲ１２間のシーケンス動作の一例を示す。
【図２２】本実施形態に係るパケット転送システムにおけるＩＰｖ６の適応例の一例を示す。
【図２３】本実施形態に係るネットワークの構成図の一例を示す。
【発明を実施するための形態】
【００３４】
以下、本発明の実施形態について、図面を参照しながら詳細に説明する。なお、本発明は、以下に示す実施形態に限定されるものではない。これらの実施の例は例示に過ぎず、本発明は当業者の知識に基づいて種々の変更、改良を施した形態で実施することができる。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。
【００３５】
さらに、各実施形態で用いる以下に説明する用語は、すべての実施形態に共通に適用される。
【００３６】
インターネット：一般的にデジタル伝送媒体を介してコンピュータ同士を相互接続したものをコンピュータネットワークもしくは物理ネットワークと呼び、コンピュータネットワークを、パケット転送装置（ルータやレイヤ３スイッチ）を介して相互接続したものをインターネットワークという。ＩＳＰが運用するコンピュータネットワークを相互接続した全世界に開かれたインターネットワークの固有名詞が、インターネット（Ｔｈｅ Ｉｎｔｅｒｎｅｔ）であり、ＴＣＰ／ＩＰプロトコル体系を用いてパケット通信サービスを提供する。インターネットのパケット通信サービスを利用するには、利用者側ネットワークに配備される家庭用ルータなど（ｅＭＬＢＲ）と、専用回線または公衆アクセス回線（電話回線やＩＳＤＮ回線、ＡＤＳＬ回線、光回線、無線回線など）を介して、インターネットの端部に配備されるエッジルータ（ｉＭＬＢＲ）に接続する必要がある。なお、移動体通信網では、これまでＴＣＰ／ＩＰに準じた独自のプロトコル体系を用いていたが、スマートフォンなどの導入に伴ってＴＣＰ／ＩＰを用いたＩＰネットワークが運用されるようになり、またＮＧＮ（Ｎｅｘｔ Ｇｅｎｅｒａｔｉｏｎ Ｎｅｔｗｏｒｋ）でもＴＣＰ／ＩＰベースのパケット通信サービスが提供されている。本明細書では、これらもインターネットの構成要素として含める。
【００３７】
パケット：エンドノード間の通信を行うためのレイヤ３（ネットワーク層）における転送単位（ＰＤＵ： Ｐｒｏｔｏｃｏｌ Ｄａｔａ Ｕｎｉｔ）で、送信元論理アドレスと送

信先論理アドレスや、パケットの種別、ユーザーデータを含む。ＲＦＣ ７９１規格のＩＰパケットやＩＴＵ－Ｔ勧告のＸ．２５パケットなどを含む。

【００３８】

フレーム：デジタル伝送媒体を介して直接接続されている一つの物理ネットワーク内でのノード間の通信を行うためのレイヤ２（データリンク層）のＰＤＵで、パケットを所定のフォーマットにカプセル化（ＭＡＣヘッダやトレーラを付加したり、ＭＡＣｓｅｃなどによるＳｅｃＴＡＧの付加やペイロードの暗号化を含む）して送信する。受信側ではフレームをデカプセル（誤り検査、ＭＡＣｓｅｃなどによるメッセージ認証、暗号化されたペイロードの復号を含む）してパケットを取り出す。ＭＡＣフレームの他にＰＰＰ（Ｐｏｉｎｔ ｔｏ Ｐｏｉｎｔ Ｐｒｏｔｏｃｏｌ）フレーム、ＨＤＬＣ（Ｈｉｇｈ－Ｌｅｖｅｌ Ｄａｔａ Ｌｉｎｋ Ｃｏｎｔｒｏｌ）フレーム、ＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ Ｔｒａｎｓｆｅｒ Ｍｏｄｅ）セルなどを含む。

【００３９】

ノード：ユーザパケットを生成し送受信するホストと、ユーザパケットの生成は行わずパケットの中継転送を行うルータやレイヤ３スイッチを総称する用語として「ノード」を用いる。さらに、インターネットは階層的かつ回帰的な構造をなしているため、ノードの集合であるネットワークをノードとして扱うことができる。本明細書では、ネットワークも「ノード」の一つとして扱う。

【００４０】

エンティティ：利用者、プロセス、クライアント、サーバー、メールアカウントや、ＮＥＴＢＯＩＳ名、ホスト名などのなどのベンダー特有のエンティティ、およびそれらから構成されるグループ。

【００４１】

ポート：物理ポート（所謂ＬＡＮやルータのスイッチポート）や既存の物理接続を用いてソフトウェア的に構成される仮想ポート、外部とデータを入出力するためのインターフェースなどで、それぞれの装置ごとに識別情報によって識別され管理される。

【００４２】

チャネル：ＭＡＣｓｅｃのように共有鍵を用いて識別可能なセキュアチャネル（ＳＣＩ：Ｓｅｃｕｒｅ Ｃｈａｎｎｅｌ Ｉｄｅｎｔｉｆｉｅｒ）などのチャネル識別情報や送信元ＭＡＣアドレスをチャネル識別情報として用いてもよい。他に移動体通信などで用いられているＴＤＭＡやＣＤＭＡ、ＯＦＤＭＡなどにおけるタイムスロットや拡散符号、リソースブロックを用いてノードやエンティティに割り当てられるチャネルやスロット、コネクション、セッション、フローラベルなどを含み、それぞれの装置もしくは複数の装置に跨って識別され管理される。

【００４３】

マルチレイヤ・バインディング・ルータ（ＭＬＢＲ）： 本発明によるパケット転送装置の特徴を表す用語として用いるもので、さらに利用者側に配置されるアドレス詐称パケットや攻撃パケット、不正パケットの外部（インターネット）への流出を阻止するものをｅＭＬＢＲ（ｅｇｒｅｓｓ ＭＬＢＲ）、インターネットの端部に所謂エッジルータとして配置されアドレス詐称パケットや攻撃パケット、不正パケットのインターネットへの流入を阻止するものをｉＭＬＢＲ（ｉｎｇｒｅｓｓ ＭＬＢＲ）と称する。さらに、ｅＭＬＢＲは家庭に配置されるものをｅＭＬＢＲ－Ｒ（Ｒｅｓｉｄｅｎｃｅ）、企業などの組織に配置されるものをｅＭＬＢＲ－Ｏ（Ｏｒｇａｎｉｚａｔｉｏｎ）、データセンターなどに配置されるものをｅＭＬＢＲ－Ｃ（Ｄａｔａ Ｃｅｎｔｅｒ）、無線ＬＡＮスポットサービスなどに配置されるものをｅＭＬＢＲ－Ｗ（Ｗ－ＬＡＮ Ｓｐｏｔ Ｓｅｒｖｉｃｅ）、ワイヤレスセンサーネットワークやＩｏＴに配置されるものをｅＭＬＢＲ－Ｓ（Ｓｅｎｓｏｒ Ｎｅｔｗｏｒｋ）、移動体通信網に配置されるものをｅＭＬＢＲ－Ｍ（Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ）などと称し、様々な用途・形態に応じて適宜機能を取捨選択あるいは追加して適用することが可能である。

マルチレイヤ・バインディング・フィルタリング装置として、既設のルータの前段に配置

しても同様の効果が得られる。

【００４４】

マルチレイヤ・バインディング（ＭＬＢ）テーブル：　ポート又はチャネルの識別情報と、送信元物理アドレス（所謂ＭＡＣアドレスやＡＴＭで用いるＶＰＩ（Ｖｉｒｔｕａｌ Ｐａｔｈ Ｉｄｅｎｔｉｆｉｅｒ）／ＶＣＩ（Ｖｉｒｔｕａｌ Ｃｈａｎｎｅｌ Ｉｄｅｎｔｉｆｉｅｒ）などのレイヤ２（データリンク層）アドレス）と、送信元論理アドレス（所謂ＩＰｖ４アドレスやＩＰｖ６アドレスや通信事業者固有のレイヤ３（ネットワーク層）アドレスなど）との対応関係を記憶しておくテーブルで、所定の有効期限（例：４時間）を有する。サーバーの場合は、上記に加え送信元プロセス識別アドレス（所謂ｗｅｌｌ－ｋｎｏｗｎポート番号）もＭＬＢテーブルに加えてもよい。

【００４５】

廃棄テーブル：主にサイバー攻撃を受けている被害者ノードＲｅＮから、もしくはサイバー攻撃を受けていると判断したノードＲｅＮもしくはサイバー攻撃パケットと思われるパケットを検出したノードＲｅＮから送られてきたパケットを分析して攻撃又は被害を認定するノードＤｅＮから、もしくは廃棄要請情報をインターネット全体に配信するノードＳｈＮからの廃棄要請情報をもとに生成・更新されるテーブルで、送信先／送信元物理アドレスや送信先／送信元論理アドレス、送信先／送信元プロセス識別アドレスの一部又はすべての対、匿名アドレスとそれらの有効期間を管理するテーブル。

【００４６】

ＩＥＥＥ ８０２．１Ｘ：有線ＬＡＮや無線ＬＡＮへの接続時に使用する認証規格で、認証されたノードやエンティティ以外がネットワークに接続できないようにする規格。本発明では、ＩＥＥＥ ８０２．１Ｘによる認証をＬＡＮスイッチ（データリンク層）に限定するのではなく、レイヤ３スイッチやルータなどのパケット転送装置（ネットワーク層）へ適用する。ＩＥＥＥ８０２．１Ｘの認証方式には、本実施形態の説明の中で用いるＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）の他に、ＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ ５）やＬＥＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ＥＡＰ－ＦＡＳＴ（ＥＡＰ－Ｆｌｅｘｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｖｉａ Ｓｅｃｕｒｅ Ｔｕｎｎｅｌｉｎｇ）、ＴＴＬＳ（Ｔｕｎｎｅｌｅｄ Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）、ＰＥＡＰ（Ｐｒｏｔｅｃｔｅｄ ＥＡＰ）があり、認証方法や認証レベルは異なるものの、これらを適用してもよい。

【００４７】

サプリカント：ネットワーク上のノードやエンティティの認証において、認証を要求する側、認証される側、クライアント側の機器やソフトウェア、エンティティ。なお、Ｗｉｎｄｏｗｓ（Ｗｉｎｄｏｗｓは登録商標） ２０００（ＳＰ４）、Ｗｉｎｄｏｗｓ ＸＰ以降のＷｉｎｄｏｗｓ、及びＭａｃ ＯＳ ＸはＩＥＥＥ８０２．１Ｘ対応のサプリカント機能を標準で内蔵している。

【００４８】

オーセンティケータ：サプリカントからの要求を受けて、認証サーバーとのやり取りを仲介し、サプリカントの接続可否や通信サービス品質のレベルを決めるプロキシの役割を担う。

【００４９】

認証サーバー：クライアントＩＤとパスワードや、デジタル証明書を用いてノードもしくはエンティティの真正性を（相互に）検証し、クライアントからのアクセスを許可するかどうかをオーセンティケータに通知する。ＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ Ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）、移動体通信で用いられるＨＬＲ（Ｈｏｍｅ Ｌｏｃａｔｉｏｎ Ｒｅｇｉｓｔｅｒ ）やＭｉｃｒｏｓｏｆｔのＡｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙなどのベンダー特有の認証機構を含む

【００５０】

通信サービス品質（ＱｏＳ（Ｑｕａｌｉｔｙ ｏｆ Ｓｅｒｖｉｃｅ））：秘匿通信、帯域制限、帯域保証、遅延・ジッタ保証、検閲、送信先ＩＰアドレスの制限、通信可能プロトコルの制限、接続拒否、通信内容記録など。

【００５１】

ＯｐｅｎＦｌｏｗ：ネットワーク構成や機能、性能などをソフトウェアで動的に設定・変更できるネットワークやコンセプトをＳＤＮ（Ｓｏｆｔｗａｒｅ Ｄｅｆｉｎｅｄ Ｎｅｔｗｏｒｋ）と呼び、ＯｐｅｎＦｌｏｗはクラウドコンピューティングにおける負荷分散などを意図に開発が進められているＳＤＮを実現する技術規格の一つで、経路制御を司る「ＯｐｅｎＦｌｏｗコントローラ」と、データ転送機能を司る「ＯｐｅｎＦｌｏｗスイッチ」、そしてコントローラとスイッチがコミュニケーションをするための「ＯｐｅｎＦｌｏｗプロトコル」からなる。

【００５２】

ＡＲＰリフレクション（ＡＲＰＦ）：ＩＥＥＥ８０２．１Ｘに対応していないデジタルテレビなどの所謂スマート家電や既設の家庭用ルータ、ＩｏＴなど、ＩＥＥＥ８０２．１Ｘに非対応ノードもしくはエンティティの論理アドレスおよび物理アドレスの真正性を簡易的に検証し、アドレス詐称パケットを阻止するための本発明において定義する機能である。具体的には、ノードは他ネットワークとの通信を契機にデフォルトゲートウェイ（ＤＧＷ）のポート又はチャネルを介してアドレス解決（ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ））要求パケットを送信するが、ノードがアドレス詐称していなければ、ＤＧＷからのＡＲＰ要求に対してＡＲＰ応答を返すはずであることから、ＤＧＷとして機能するｅＭＬＢＲ又はｉＭＬＢＲが、ＡＲＰ要求を送ってきたノードに対して同じポート又はチャネルを介してＡＲＰ要求を送信することをＡＲＰリフレクションと呼ぶ。

【００５３】

本実施形態に係るイーグレス・マルチレイヤ・バインディング・パケット転送装置ｅＭＬＢＲの構成例を図２に示し、イングレス・マルチレイヤ・バインディング・パケット転送装置ｉＭＬＢＲの構成例を図３に示す。なお、本実施形態においてｅＭＬＢＲ１２及びｉＭＬＢＲ１１は、パケット転送装置として機能する。

【００５４】

図２は、利用者側に配備されるｅＭＬＢＲ１２に必要なほぼすべての機能を実装した例を示す図である。ｅＭＬＢＲ－ＲやｅＭＬＢＲ－Ｏ、ｅＭＬＢＲ－Ｃ、ｅＭＬＢＲ－Ｗ、ｅＭＬＢＲ－Ｓ、ｅＭＬＢＲ－Ｍなどは、その用途によって取捨選択して実装される。また、本実施形態に係るパケット転送装置は、ＤＨＣＰやＷ－ＬＡＮ、レイヤ２／ＶＬＡＮなど各機能を有した一体型構造でもよい。この場合、容易なネットワーク管理を実現するパケット転送装置を提供することができる。一方で、ネットワーク管理は煩雑になるが、ＤＨＣＰやＷ－ＬＡＮ、レイヤ２／ＶＬＡＮなどは、別の装置として配備してもよい。さらに、ルーティング機能は既設のルータを使用するケースでは、ルーティング機能に係る機能部を実装しないもしくは当該機能部を停止したイーグレス・マルチレイヤ・バインディング・フィルタリング装置として既設のルータの前段に配置してもよい。具体的には、パケット転送装置として機能するｅＭＬＢＲ１２の転送部１４では、フレーム／パケットを受信したポート又はチャネルをキーにＭＬＢテーブルを検索し、フレーム／パケットの送信元物理アドレスと送信元論理アドレスとの対がＭＬＢテーブルに存在するときは、パケットの送信先論理アドレスに向けて転送するルータへ転送し、ＭＬＢテーブルに存在しないときはパケットを廃棄してもよい。

【００５５】

ｅＭＬＢＲ１２は、制御部１５を備え、制御部１５はさらに受信したポート又はチャネルの識別情報とともに転送部１４から伝達されてきたＤＨＣＰ要求やアドレス解決要求、認証要求などのパケットやフレームを受け付ける処理要求受付部、デジタルテレビやＩｏＴなどのＩＥＥＥ８０２．１Ｘ非対応ノードに対するＡＲＰリフレクションを用いた認証や、ｉＭＬＢＲ１１との間でデジタル証明書の交換などを行って相互に認証し合う認証部

、オーセンティケータとして認証サーバーへの仲介を行う認証仲介部、前記認証部及び認証サーバーからの認証結果を取得する認証結果取得部、ポート又はチャネルの識別情報と送信元物理アドレスと送信元論理アドレスなどとの対応関係をＭＬＢテーブルとして有効期間を附して生成し更新するＭＬＢテーブル生成・更新部、通信を許可したノード又はエンティティの実在確認を行い上述のＭＬＢテーブルの有効期間を更新する実在確認部、ＭＡＣｓｅｃなどによる暗号鍵の生成・交換を行う暗号鍵生成・交換部、他のノードからの廃棄要請に基づいて有効期間を附して生成・更新する廃棄テーブル生成・更新部、認証結果（認証レベル）に基づいて通信サービス品質を決定するＱｏＳ決定部、ＤＨＣＰ要求を行ってきたノードに対してＩＰアドレスを割り当てたり、ネットマスクやＤＧＷのＩＰアドレスなど、ネットワークの接続に必要な情報を提供するＤＨＣＰ部、ｅＭＬＢＲ１２配下で用いられる論理アドレスやプロセス識別アドレスを外部ネットワークで用いる論理アドレスやプロセス識別アドレスに変換するためのＮＡＴテーブルを生成するＮＡＴテーブル生成部、これらの各機能部での処理結果や認証部で生成するＡＲＰリフレクション用のＡＲＰ要求パケットや実在確認部で生成する実在確認用のパケットなどを転送部１４に伝達するための処理結果伝達部、その他図には示していないが転送部１５の例えばレイヤ２／ＶＬＡＮスイッチ部などの制御に必要な機能や、ＩＰｓｅｃのトンネルモード対応機能、ｅＭＬＢＲ１２に不正侵入され制御プログラムやテーブルなどが改ざんされていなすかを検査するための完全性検査機能、実装後に発見されたセキュリティホールや新しい機能を追加するためのバージョンアップ機能などを有してもよい。

【００５６】

また、ｅＭＬＢＲ１２は、転送部１４をさらに備え、転送部１４はさらに有線系（Ｅｔｈｅｒｎｅｔ（Ｅｔｈｅｒｎｅｔは登録商標）や光信号など）／無線系（無線ＬＡＮ／移動体通信など）通信に必要な複数の物理ポートを提供するポート部、又は及び複数のチャネルを提供するチャネル部、物理信号受信・復号部、物理信号生成・送信部、暗号化／復号部、パケットもしくはフレームを一時的にバッファリングする受信バッファ部及び送信バッファ部、受信したフレームからパケットを取り出すフレームデカプセル化部、その逆を行うフレームカプセル化部、受信したフレーム及びパケットの送信元及び送信先物理アドレス、送信元及び送信先論理アドレス、送信元及び送信先プロセス識別アドレスを抽出するレイヤ２、３、４アドレス抽出部、ポート又はチャネルに対して指定された通信サービス品質を提供するＱｏＳ提供部、レイヤ２スイッチ及びＶＬＡＮ機能を提供するレイヤ２／ＶＬＡＮスイッチ部、ＭＬＢテーブルを格納するＭＬＢテーブル部、廃棄テーブルを格納する廃棄テーブル部、ＭＬＢテーブルや廃棄テーブルを検索してパケットを廃棄するパケット廃棄部、ルーティングテーブルを参照してパケットの転送処理を行うレイヤ３スイッチ部、ＤＨＣＰ要求やアドレス解決要求、認証要求などのフレームもしくはパケットを制御部１５の前記受付部へ伝達し処理を要求する処理要求伝達部、制御部１５から伝達されてきた処理結果を該当する各機能部に反映もしくは中継する処理結果受付部などを有してもよい。

【００５７】

図３は、インターネット１０側の端部に配備されるｉＭＬＢＲ１１に必要なほぼすべての機能を実装した例を示す図である。各機能部の機能は図２のｅＭＬＢＲ１２とほぼ同じであるので、詳しい説明は省略するが、ＮＡＴ機能やレイヤ２／ＶＬＡＮ機能は原則不要である。また、本実施形態に係るパケット転送装置は、ＤＨＣＰなど各機能を有した一体型構造でもよい。この場合、容易なネットワーク管理を実現するパケット転送装置を提供することができる。一方で、ネットワーク管理は煩雑になるが、ＤＨＣＰなどは、別の装置として配備してもよい。さらに、ルーティング機能は既設のルータを使用するケースでは、ルーティング機能に係る機能部を実装しないもしくは当該機能部を停止したイングレス・マルチレイヤ・バインディング・フィルタリング装置として既設のルータの前段に配置してもよい。具体的には、パケット転送装置として機能するｉＭＬＢＲ１１の転送部１４では、フレーム／パケットを受信したポート又はチャネルをキーにＭＬＢテーブルを検索し、フレーム／パケットの送信元物理アドレスと送信元論理アドレスとの対がバンディ

ングテーブルに存在するときは、パケットの送信先論理アドレスに向けて転送するルータへ転送し、ＭＬＢテーブルに存在しないときはパケットを廃棄してもよい。

【００５８】

ｉＭＬＢＲ１１は、制御部１５を備え、ＩＥＥＥ８０２．１Ｘ非対応ノードに対する認証や、ｅＭＬＢＲ１２とｉＭＬＢＲ１１との間でデジタル証明書の交換などを行って相互認証を行う。また、ｉＭＬＢＲ１１は、転送部１４を備え、物理信号受信・復号部／生成・送信部は、有線系（Ｅｔｈｅｒｎｅｔ（Ｅｔｈｅｒｎｅｔは登録商標）や光信号など）／無線系（無線ＬＡＮ／移動体通信など）に必要な機能を有する。

【００５９】

（実施形態１）

本実施形態では、ＡＲＰリフレクション（ＡＲＰＦ）によるデジタルテレビや、ファックスやスキャナー、プリンタなど複数の機能を搭載した複合機、さらにＩｏＴなどのＩＥＥＥ８０２．Ｘ非対応ホストのｅＭＬＢＲ１２による認証及び上りパケットの転送シーケンスの動作例を説明する。本実施形態に係るネットワークの構成を図４に示す。図４に示すネットワーク構成は、ｉＭＬＢＲ１１を含んだインターネット１０、ＩＥＥＥ８０２．１Ｘ非対応のノード及びｅＭＬＢＲ１２で構成している。

【００６０】

図５におけるシーケンス図は、ＡＲＰリフレクションを用いたデジタルテレビなどのＩＥＥＥ８０２．１Ｘ非対応ノードとｅＭＬＢＲ１２間の認証及び上りパケットの転送シーケンスを示した図である。図５では、ノードから外部ネットワーク（インターネット１０）に向けて送信されるユーザＭＡＣフレーム／ＩＰパケットに係わるものについて記述している。本実施形態におけるＤＨＣＰプロトコルのやり取りなどは、簡略化して記述している（例えば、ＤＨＣＰ　Ｄｉｓｃｏｖｅｒ⇒ＤＨＣＰ　Ｏｆｆｅｒ⇒ＤＨＣＰ　Ｒｅｑｕｅｓｔ⇒ＤＨＣＰ　ＡＣＫと４回やり取りする）。また、図及び説明が煩雑になるのを避けるため、各ステップに係わる転送部１４及び制御部１５の機能部の記述も省略している。

【００６１】

以下に、図５のシーケンス図の動作を説明する。ＩＥＥＥ８０２．１Ｘ非対応のノードが他ノードへ通信を開始する場合、ＤＨＣＰ要求パケットをブロードキャスト送信する（ステップＳ１１１）。ＤＨＣＰ要求を受信したｅＭＬＢＲ１２は、受信したポートの識別情報と前記ノードのＭＡＣアドレスとプライベートＩＰアドレスとして割り当てるＩＰアドレスの対応関係を記憶しておく制御部１５のＭＬＢテーブルＡに仮登録する（ステップＳ１１２）。ノードは、ｅＭＬＢＲ１２のネットマスクやＤＧＷのＩＰアドレスなど、ネットワークへの接続に必要な情報とともにＩＰアドレスを割り当てる旨のＤＨＣＰ応答パケットを受信する（ステップＳ１１３）。ＤＨＣＰ応答を受け取ったノードは、ＤＧＷのアドレスの解決要求する旨のＡＲＰ要求パケットをブロードキャスト送信する（ステップＳ１１４）。

【００６２】

ＡＲＰ要求パケットを受信したｅＭＬＢＲ１２は、ノードがアドレス詐称していなければ、ｅＭＬＢＲ１２からのＡＲＰ要求に対してＡＲＰ応答を返すはずであることから、ＡＲＰ要求パケット（ＡＲＰＦ要求）をノードにブロードキャスト送信し、ノードからのＡＲＰ応答パケットを受け取る（ステップＳ１１５及びステップＳ１１６）。ｅＭＬＢＲ１２において、ＡＲＰ応答パケットを受信したポートをキーに制御部１５のＭＬＢテーブルＡを検索し、ＡＲＰ応答の送信元ＩＰアドレスと送信元ＭＡＣアドレスの対が存在しない場合、ＭＬＢテーブルＡから仮登録した前記対応関係を削除する（ステップＳ１１７及びステップＳ１１８）。一方、ＭＬＢテーブルＡに存在する場合、ＱｏＳ（後述するように、例えば上り帯域を１０ｋｂｐｓ）を決定し、さらに有効期間（例えば４時間）を設定の上、転送部１４のＭＬＢテーブルＡに正登録する（ステップＳ１１９）。

【００６３】

次に、ｅＭＬＢＲ１２がノードからの最初のＡＲＰ要求（ＤＧＷのアドレス解決）（ス

テップＳ１１４）に対する応答として、ステップＳ１２０によるＡＲＰ応答を返した以降、ノードが送信したユーザＭＡＣフレーム／ＩＰパケットをｅＭＬＢＲ１２が受け取ると（ステップＳ１２１）、ｅＭＬＢＲ１２は、受け取ったユーザＭＡＣフレーム／ＩＰパケットの送信元ＩＰアドレス及び送信元ＭＡＣアドレスが転送部１４のＭＬＢテーブルＡに存在するか調べ（ステップＳ１２２）、存在しない場合、ノードが送信したパケットを破棄する（ステップＳ１２３）。

【００６４】

一方、転送部１４のＭＬＢテーブルＡに存在する場合、ステップＳ１１９で決定したＱｏＳで、かつＮＡＴテーブルを参照してプライベートＩＰアドレスからグローバルＩＰアドレスにアドレス変換して、次ホップノードであるｉＭＬＢＲ１１にＭＡＣフレームにカプセル化して転送し、ｉＭＬＢＲ１１がＭＡＣフレーム／ＩＰパケットを受け取る（ステップＳ１２４）。なお、ステップＳ１２０によるＡＲＰ応答は、ステップＳ１１５のＡＲＰ要求（ＡＲＰＦ要求）で既にノードがｅＭＬＢＲ１２のＭＡＣアドレスを知っているので、行わなくてもよい。

【００６５】

また、本実施形態におけるｅＭＬＢＲ１２が備える制御部１５は、転送部１４と連携してノードもしくはエンティティのポートもしくはチャネルでの実在確認を適宜（必ずしも定期的である必要はない）行い（ステップＳ１２８及びステップＳ１２９）、ステップＳ１３０で確認結果に応じてＭＬＢテーブルＡを更新（有効期間を延長）してもよい。

【００６６】

ｉＭＬＢＲ１１（ＩＳＰエッジルータ）は、ステップＳ１２４で転送されてきたパケットを受信したポートの識別情報をキーに、パケットのＩＰアドレス（ｅＭＬＢＲ１２に割り当てられたグローバルＩＰアドレス）と（ｅＭＬＢＲ１２の）ＭＡＣアドレスとの対が転送部１４のＭＬＢテーブルＢに存在するか調べ（ステップＳ１２５）、ＭＬＢテーブルＢに存在しない場合、パケットを廃棄する（ステップＳ１２６）。一方、転送部１４のＭＬＢテーブルＢに存在する場合、予めｅＭＬＢＲ１２の認証の際に決定されたＱｏＳ（ｅＭＬＢＲ１２がｉＭＬＢＲ１１によってＩＥＥＥ８０２．１Ｘノードとして認証されていれば、帯域制限されずに）で次ホップノードに転送する（ステップＳ１２７）。

【００６７】

本実施形態によるＡＲＰリフレクションで認証した場合は、ＩＤやパスワード、あるいはデジタル証明書を用いるＩＥＥＥ８０２．１Ｘ認証よりセキュアな端末とは言い切れない、すなわち認証レベルは低いため、ＱｏＳを例えばインターネット１０へ向かう上り方向の帯域を１０ｋｂｐｓ程度に制限しても、下り方向は帯域制限しなければ、テレビの利用者はリモコン操作によるテレビ局とのデータ通信や画面の遷移、その他のテレビを介したインターネット接続サービスに、違和感を持つことはない。

【００６８】

したがって、ＯＳのバージョンアップやファイアウォール機能を持たない無防備でサイバー攻撃の温床になりかねないスマート家電やＩｏＴなどが、たとえボットウィルスに感染もしくは製造工程でマルウェアが埋め込まれ、送信元ＩＰアドレスを攻撃ターゲットのＩＰアドレスに詐称して大量のパケットを送信するＤＲＤｏＳ攻撃、あるいは送信先ＩＰアドレスを攻撃ターゲットのＩＰアドレスに設定し、送信元ＩＰアドレスをランダムに変えながら大量のパケットを送信するＤＤｏＳ攻撃などに加担させられても、アドレス詐称パケットのインターネット１０への流出を阻止でき、たまたま端末の送信元ＩＰアドレスに一致した攻撃パケットだけがインターネット１０に流入するため、被害を最小限に抑えることができる。さらに、後述する実施形態５によって、攻撃パケットが長時間にわたってインターネット１０に流出／流入することを阻止することもできる。

【００６９】

なお、本実施形態では、ノードからのＡＲＰ要求に対してＡＲＰリフレクションを行うものとしているが、例えばノードがｅＭＬＢＲ１２のＩＰアドレスとＭＡＣアドレスをキャッシュし、ＩＣＭＰパケットを用いてｅＭＬＢＲ１２へエコー要求（疎通確認）し、こ

のパケット／フレームに対応するＭＬＢテーブルをｅＭＬＢＲ１２が保持していないとき、同ノードに対してエコー要求（エコーリフレクション）もしくはＡＲＰ要求を送り、その応答パケット／フレームとノードからのエコー要求パケット／フレームの送信元ＩＰアドレスと送信元ＭＡＣアドレスを照合し、一致していれば、制御部１５及び転送部１４のＭＬＢテーブルに登録するなど、色々なバリエーションでのＩＰアドレスおよびＭＡＣアドレスの真正性の検証による認証を用いてもよい。

【００７０】

ここで、ＯｐｅｎＦｌｏｗを用いたＡＲＰリフレクションの通信動作の実験例を図６に示す。ホスト＃ＡはｅＭＬＢＲ１２を介してホスト＃Ｂと通信しようとしている。ｅＭＬＢＲ１２は、ＯｐｅｎＦｌｏｗを実行し、本実施形態に係るパケット転送装置として機能する。ｅＭＬＢＲ１２は制御部１５であるＯｐｅｎＦｌｏｗコントローラ１５と、転送部１４であるＯｐｅｎＦｌｏｗスイッチ１４との二つから構成される。ＯｐｅｎＦｌｏｗスイッチ１４はＭＬＢテーブルを備えている。また、図６では、ホスト＃ＡがＤＧＷのアドレス解決のために送信するＡＲＰ要求（ステップＳ２１１）はＯｐｅｎＦｌｏｗコントローラ１５に送られ、同コントローラにてホスト＃Ａに対してＡＲＰ要求（ＡＲＰＦ）が生成され、ＯｐｅｎＦｌｏｗスイッチを介してホスト＃Ａに送られる（ステップＳ２１２）。これは、前述したように相手がアドレス詐称している場合ＡＲＰ応答を返さないだろうという仮定に基づくもので、相手がアドレス詐称していない場合ＡＲＰ応答を返し（ステップＳ２１３）、ＯｐｅｎＦｌｏｗコントローラにてステップＳ２１１で送ってきたＡＲＰ要求とステップＳ２１３で返してきたＡＲＰ応答のＩＰアドレスＭＡＣアドレスを照合することによってその真正性を検証し、一致していればＯｐｅｎＦｌｏｗコントローラ１５のＭＬＢテーブルに仮登録し、Ｆｌｏｗ ｍｏｄにてＯｐｅｎＦｌｏｗスイッチ１４のＭＬＢテーブルに正登録する。

【００７１】

ＯｐｅｎＦｌｏｗコントローラ１５の開発フレームワークとしてＴｒｅｍａ－ｅｄｇｅをパソコン（ＯＳ：Ｕｂｕｎｔｕ１２．０４（Ｘ６４）、ＣＰＵ：Ｃｅｌｅｒｏｎ４４０@２．００ＧＨｚ、メモリ：２ＧＢ）に実装し、ＯｐｅｎＦｌｏｗスイッチ１４にはＯｐｅｎ ｖＳｗｉｔｃｈ ２．０．０を同じ仕様の別のパソコンに実装し、レイヤ３スイッチとして動作させた。このプログラムでは、スイッチの各ポートが受け入れるＩＰアドレスとＭＡＣアドレスの対応関係をＯｐｅｎＦｌｏｗコントローラ１５のＭＬＢテーブルに仮登録し、ＯｐｅｎＦｌｏｗスイッチ１４のＭＬＢテーブルに正登録する。

【００７２】

次に、図６、図７及び図８を用いて、本実施形態の動作を説明する。フローテーブルの構成を図７、さらにフローテーブルの遷移を図８に示す。スイッチとして機能するＯｐｅｎＦｌｏｗスイッチ１４に到着したＡＲＰ要求やＡＲＰＦに係わるパケットは、すべてＯｐｅｎＦｌｏｗコントローラ１５へＰａｃｋｅｔ－Ｉｎ（図７及び図８のテーブル：０）で処理方法を問い合わせるものとし、他のパケットは複数のフローテーブル遷移（パイプライン処理）を通過したもののみがルーティング処理されるか、Ｐａｃｋｅｔ－Ｉｎとしてコントローラへの問い合わせが発生する（同テーブル：１８０）。

【００７３】

ホスト＃Ａが送信したＡＲＰ要求をポート１で受信したＯｐｅｎＦｌｏｗスイッチ１４は、図７及び図８に示したテーブル：０において、ＯｐｅｎＦｌｏｗコントローラ１５に対しＰａｃｋｅｔ－Ｉｎ動作を行う（ステップＳ２１１及びステップＳ３１１）。ＯｐｅｎＦｌｏｗコントローラ１５は受信したポート１をキーに、受信したＡＲＰ要求フレーム／パケットの送信元ＩＰアドレスと送信元ＭＡＣアドレスの対をコントローラ内のＭＬＢテーブルに仮登録する。次いで、ＯｐｅｎＦｌｏｗコントローラ１５は、ＡＲＰリフレクションとしてＯｐｅｎＦｌｏｗスイッチ１４に対してＡＲＰ要求をＰａｃｋｅｔ－Ｏｕｔし、スイッチはこれをホスト＃Ａへポート１から送る（ステップＳ２１２）。ホスト＃Ａが返してきたＡＲＰ応答をポート１で受け取ったＯｐｅｎＦｌｏｗスイッチ１４は、再度コントローラへＰａｃｋｅｔ－Ｉｎを発生させる（ステップＳ２１３及びステップＳ３１

２）。コントローラは、ポート１をキーにコントローラ内のＭＬＢテーブルを検索し、ホスト＃ＡからのＡＲＰ応答の送信元ＩＰアドレスと送信元ＭＡＣアドレスの対が存在すれば、同対のノードが実在すると判定し認証する。コントローラはスイッチに対してＦｌｏｗ Ｍｏｄ動作を行って（ステップＳ２１４）、「ポート：１」をマッチ条件とするフローエントリを物理ポートテーブル（テーブル：６０）に、同対をマッチ条件とするフローエントリをＭＬＢテーブル（テーブル：１０１）に書き込む（正登録する）。これにより、ポート１に上記対以外のＩＰパケットが受信されたときは、廃棄されることになる。

以上の処理フローに則りホスト＃Ａがコントローラによって認証され、各フローエントリがスイッチ内の該当テーブルに書き込まれたことを、フローエントリ確認コマンドを用いて確認した。

【００７４】

ＯｐｅｎＦｌｏｗスイッチ１４では、パイプライン処理を活用して、受信したパケットを処理する過程で受信したポートのＭＬＢテーブルに遷移させる（図７及び図８のテーブル：６０及び１０１）。同ポートのＭＬＢテーブルに送信元ＩＰ／ＭＡＣアドレスがあれば、ルーティング動作（図７ テーブル：１８０、ステップＳ３１６）に進めるが、ＭＬＢテーブルにないときは廃棄する（図７及び図８のテーブル：１０１及び１０２）。

【００７５】

本実装例の有効性を検証するために、簡易攻撃ツールｈｐｉｎｇ３を用いてＳＹＮ ｆｌｏｏｄ攻撃実験を行った。送信元ＩＰアドレスをネットワークアドレス（１９２．１６８．２．０／２４）の範囲内でランダムに変更しながら、１０，０００パケットを攻撃先に送信する実験を複数回行った。その結果、攻撃先に到達できたのは１０，０００パケット中、平均して約３０パケット（ １０，０００÷２５６；攻撃元ホスト本来のＩＰアドレス）で、残りの約９，９７０パケットは廃棄されたことがスイッチ上のログで確認できた。

【００７６】

また、ホスト＃Ａからホスト＃Ｂ宛にＩＣＭＰエコー要求パケットを２．５ｋｐｐｓから１６０ｋｐｐｓまで送信レートを変えて送信したところ、図９及び図１０の各々に示すようにＭＬＢテーブル機能オン（図７のすべてのテーブルを活性化）とオフ（図７のテーブル：１８０のみ活性化）共に、送信レートが高くなるほどホスト＃ＡでのＩＣＭＰ応答パケットの未着率が増えることが観測されたが、ＯｐｅｎＦｌｏｗスイッチ１４のＣＰＵ使用率は１％未満で、スイッチでのパケットロスも観測されなかった。これは、ＩＣＭＰエコー要求パケットを生成・送信しながら、応答パケットの受信を行おうとするホスト＃Ａが過負荷状態に陥り、応答パケットを取りこぼしているためである。

【００７７】

以上から、本実装がＩＰアドレス詐称に対し有効に機能し、少なくとも家庭用のｅＭＬＢＲ１２として十分な性能を有し得ることが確認できた。

【００７８】

また、図１７には帯域制限によるＴＶオンラインデータサービスの応答性評価の評価環境を示し、図１８にはＴＶオンラインデータサービスの応答性評価のフローテーブルを示す。図１８では、ＮＡＰＴ交換は、Ｐａｋｅｔ－Ｉｎが多発する。そこでスイッチ内に閉じたＮＡＰＴ交換モジュールの実装が必要である。図１９及び２０は、ＴＶオンラインデータサービスの応答性評価の評価結果を示す。図１９は、帯域（Ｋｂｐｓ）を縦軸とし時間（ｓｅｃ）を横軸として評価結果を示し、表示時間（ｓｅｃ）を縦軸とし帯域（Ｋｂｐｓ）を横軸として評価結果を示した。

【００７９】

（実施形態２）

本実施形態では、ＩＥＥＥ８０２．１Ｘを用いたパソコンなどのＩＥＥＥ８０２．１Ｘ対応ノードとｅＭＬＢＲ１２間での認証及び上りパケットの転送シーケンスの動作例を説明する。本実施形態に係るネットワーク構成を図１１に示した。図１１に示すネットワーク構成は、ｉＭＬＢＲ１１とＨＲＳ２３とを含んだインターネット１０、ノード及びｅＭ

ＬＢＲ１２で構成している。なお、図１や図１１、図２３などでは、ＨＲＳ２３がインターネットの内部に配置されるように記されているが、不正侵入などによって認証データやプログラムなどが改ざんされないよう、ＩＳＰなど信頼できる機関がＨＲＳ２３を厳重管理することを意味するものであって、ｉＭＬＢＲ１１やｅＭＬＢＲ１２を介して、インターネットの外側に配置されてもよい。以下も同様である。

【００８０】

図１２は、パソコンなどのＩＥＥＥ８０２．１Ｘ対応ノードとｅＭＬＢＲ１２間のシーケンス動作の例を示す。なお、図１２では、ノードから外部ネットワーク（インターネット１０）に向けて送信されるＭＡＣフレーム／ＩＰパケットに係わるものについて説明する。また、本実施形態におけるＤＨＣＰプロトコルや、オーセンティケータによるＥＡＰメッセージとＲＡＤＩＵＳメッセージの変換・中継処理などを含むＥＡＰ／ＲＡＤＩＵＳプロトコルのやり取り、ＭＡＣｓｅｃによる鍵の生成／交換／ＭＡＣフレームの暗号化／復号などは、簡略化もしくは省略している。また、各ステップに係わる転送部１４及び制御部１５の機能部の記述も省略している。なお、無線ＬＡＮ機能を搭載したｅＭＬＢＲ－Ｗなども、基本シーケンスは同じである。

【００８１】

なお、ＥＡＰメッセージを含んだＭＡＣフレームはマルチキャストアドレスで送信されるため、ＥｇＥＲの配下にスイッチングハブが配置されている場合、オーセンティケータに届かない。ＥＡＰメッセージ用に特定のＭＡＣアドレスを割り当てるなど、ＩＥＥＥ８０２．１Ｘ規格の変更が必要である。

【００８２】

以下に、図１２のシーケンス図の動作を説明する。ＩＥＥＥ８０２．１Ｘ対応ノードのサプリカントは、拡張認証プロトコルである（ＥＡＰ：Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）ＥＡＰＯＬ（ＥＡＰ ｏｖｅｒ ＬＡＮ）により、ＥＡＰメッセージフレームをｅＭＬＢＲ１２のオーセンティケータに送る（ステップＳ４１１）。ＥＡＰＯＬを受け取ったｅＭＬＢＲ１２は、ＥＡＰ要求（ＴＬＳ）をＩＥＥＥ８０２．１Ｘ対応ノードに送出し（ステップＳ４１２）、ノードびｅＭＬＢＲ１２間でＥＡＰメッセージ交換を行い（ステップＳ４１３）、ｅＭＬＢＲ１２はこれをホーム認証サーバーとして機能するＲＡＤＩＵＳサーバー２３へ仲介する（ステップＳ４１４）。認証結果をＲＡＤＩＵＳサーバーがｅＭＬＢＲ１２へ送信する（ステップＳ４１５）。ｅＭＬＢＲ１２のオーセンティケータは、認証結果を判別（ステップＳ４１６）し、認証に失敗した場合はノードにＥＡＰ失敗を告げ処理を終了する（ステップＳ４１７）。

【００８３】

認証に成功した場合、ノードにＥＡＰ成功を伝える（ステップＳ４１８）とともに、ノードとｅＭＬＢＲ１２との間で、ＩＥＥＥ８０２．１Ｘで定められたＭＡＣｓｅｃ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ（ＭＫＡ）プロトコルによる共有鍵の生成・交換を行い、セキュアチャネルを確立する（ステップＳ４１９）。以下、ノードとｅＭＬＢＲ１２との間の通信では、同規格の定める共有鍵暗号を用いた秘匿通信が行われるとともに、通信中にデータが改ざんされていないかを検査するメッセージ認証が行われる。

【００８４】

認証に成功したノードがＤＨＣＰ要求をブロードキャスト送信する（ステップＳ４２０）と、ｅＭＬＢＲ１２は、通信サービス品質（ＱｏＳ）レベルを決定し、さらに有効期間（例えば４時間）を設定するとともに、セキュアチャネルの識別情報をキーに、ノードのＭＡＣアドレスとノードに固定的（前回と同じ）あるいは動的に割り当てる（プライベート）ＩＰアドレスとの対応関係を、制御部１５のＭＬＢテーブルＡに仮登録し（ステップＳ４２１）、さらに転送部１４のＭＬＢテーブルＡに正登録する（ステップＳ４２２）。その上で、ノードに対して、ネットマスクやＤＧＷのＩＰアドレスなど、ネットワークへの接続に必要な情報とともにＩＰアドレスを割り当てるＤＨＣＰ応答を送信する（ステップＳ４２３）。

【００８５】

ノードは、以後、ｅＭＬＢＲ１２との間に確立したセキュアチャネルを介して、すなわちペイロード（ユーザパケット）を、上記共有鍵を用いて暗号化しＭＡＣフレームにカプセル化したユーザＭＡＣフレームを送信し（ステップＳ４２４）、ｅＭＬＢＲ１２は暗号化ユーザＭＡＣフレームをデカプセル化／復号／メッセージ認証を行った後、セキュアチャネルの識別情報をキーに、転送部１４のＭＬＢテーブルＡを検索し（ステップＳ４２５）、送信元ＩＰアドレス及びＭＡＣアドレスの対が存在しない場合、同フレーム／パケットを破棄する（ステップＳ４２６）。

【００８６】

一方、ＭＬＢテーブルＡに送信元ＩＰアドレス及び送信元ＭＡＣアドレス対が存在する場合、ステップＳ４２３で決定したＱｏＳで、ステップＳ４２１でプライベートＩＰアドレスを割り当てた場合にはｅＭＬＢＲ１２のグローバルＩＰアドレスに変換（ＮＡＴ）してから、ｅＭＬＢＲ１２とｉＭＬＢＲ１１間ですでに確立しているセキュアチャネルを介して、すなわちｅＭＬＢＲ１２とｉＭＬＢＲ１１間の共有鍵を用いてユーザパケットを暗号化しＭＡＣフレームにカプセル化してから次ホップノードであるｉＭＬＢＲ１１に転送し、ｉＭＬＢＲ１１（ＩＳＰエッジルータ）が暗号化ユーザＭＡＣフレームを受け取る。

【００８７】

また、本実施形態におけるｅＭＬＢＲ１２が備える制御部１５と転送部１４は連携して、ノード及びｅＭＬＢＲ１２間で暗号鍵の更新による実在確認を適宜行い（ステップＳ４３２）、ステップＳ４３３で確認結果に応じてＭＬＢテーブルＡを更新、すなわちＭＬＢテーブルＡの有効期間を延長してもよい。

【００８８】

ｉＭＬＢＲ１１（ＩＳＰエッジルータ）は、ステップＳ４２７で転送されたＭＡＣフレームをデカプセル化／復号／メッセージ認証してから、ｅＭＬＢＲ１２とｉＭＬＢＲ１１間のセキュアチャネル識別情報をキーに転送部１４のＭＬＢテーブルＢを検索し、（ステップＳ４２８）、送信元ＩＰアドレス及び送信元ＭＡＣアドレスの対が存在しない場合、パケットを廃棄する（ステップＳ４２９）。一方、ＭＬＢテーブルＢに送信元ＩＰアドレス及び送信元ＭＡＣアドレス対が存在する場合、指定されたＱｏＳで宛先ＩＰアドレスに向けて次ホップノードにユーザＭＡＣフレームを転送する（ステップＳ４３０及びステップＳ４３１）。

【００８９】

なお、本実施形態ではノード又はエンティティの認証にＩＥＥＥ８０２．１Ｘ規格に基づき、認証サーバーとしてＲＡＤＩＵＳサーバーを用いているが、ＬＤＡＰなど他の認証サーバー／規格を用いて認証を行ってもよい。

【００９０】

さらに、ノード又はエンティティの認証もしくは実在確認の際に、ＯＳのバージョンアップ状態や、ファイアウォールの設定状態、ウィルス検知ソフトウェアのパターンファイル、広く利用されサイバー攻撃の対象にされ易いパッケージ型のアプリケーションプログラムやＪａｖａ仮想マシンなどのミドルウェアの更新状態などを調べ、認証レベルすなわち通信サービス品質の決定に反映させてもよい。この結果を利用者に伝えることによって、利用者に対して端末をよりセキュアな状態に保つよう促すことも可能になる。

【００９１】

（実施形態３）

本実施形態では、ＩＥＥＥ８０２．１Ｘに対応したｅＭＬＢＲ－Ｒ１２（一般住宅向け）とｉＭＬＢＲ１１間の相互認証及び上りパケットの転送シーケンスの動作例を説明する。本実施形態に係るネットワーク構成を図に示す。図１３に示すネットワーク構成は、ｉＭＬＢＲ１１とＨＲＳ２３とを含んだインターネット１０、ホスト３０及びｅＭＬＢＲ－Ｒ１２で構成している。

【００９２】

ノードから外部ネットワーク（インターネット１０）に向けて送信されるＭＡＣフレーム／パケットに係わるものについて説明する。なお、本実施形態におけるオーセンティケ

ータによるＥＡＰメッセージとＲＡＤＩＵＳメッセージの変換・中継処理などを含むＥＡＰ／ＲＡＤＩＵＳプロトコルのやり取り、ＭＡＣｓｅｃによる鍵の生成／交換／ＭＡＣフレームの暗号化／復号などは、簡略化もしくは省略している。また、各ステップに係わる転送部１４及び制御部１５の機能部の記述も省略している。

【００９３】

以下に、図１４のシーケンス図の動作を説明する。ネットワークに接続したＩＥＥＥ８０２．１Ｘ対応のｅＭＬＢＲ－Ｒ１２のサプリカントは、まずＥＡＰＯＬにより、ＥＡＰメッセージフレームをｉＭＬＢＲ１１のオーセンティケータに送る（ステップＳ５１１）。ＥＡＰＯＬを受け取ったｉＭＬＢＲ１１は、ＥＡＰ要求（ＴＬＳ）をｅＭＬＢＲ－Ｒ１２に送出し（ステップＳ５１２）、ｅＭＬＢＲ－Ｒ１２及びｉＭＬＢＲ１１間でＥＡＰメッセージ交換を行い（ステップＳ５１３）、ｉＭＬＢＲ１１はこれをホーム認証サーバーとして機能するＲＡＤＩＵＳサーバー２３へ仲介する（ステップＳ５１４）。認証結果をＲＡＤＩＵＳサーバーがｉＭＬＢＲ１１へ送信する（ステップＳ５１５）。ｉＭＬＢＲ１１のオーセンティケータは、認証結果を判別（ステップＳ５１６）し、認証に失敗した場合はｅＭＬＢＲ－Ｒ１２にＥＡＰ失敗を告げ処理を終了する（ステップＳ５１７）。

【００９４】

認証に成功した場合、ｅＭＬＢＲ－Ｒ１２にＥＡＰ成功を伝える（ステップＳ５１８）とともに、ｅＭＬＢＲ－Ｒ１２とｉＭＬＢＲ１１との間で、ＭＫＡプロトコルによる共有鍵の生成・交換を行い、セキュアチャネルを確立する（ステップＳ５１９）。以下、ｅＭＬＢＲ－Ｒ１２とｉＭＬＢＲ１１との間の通信では、共有鍵暗号を用いた秘匿通信が行われるとともに、途中でデータが改ざんされていないかを検査するメッセージ認証が行われる。

【００９５】

認証に成功したｅＭＬＢＲ－Ｒ１２がＤＨＣＰ要求をブロードキャスト送信する（ステップＳ５２０）と、ｉＭＬＢＲ１１は、通信サービス品質（ＱｏＳ）レベルを決定し、さらに有効期間（例えば４時間）を設定するとともに、セキュアチャネルの識別情報をキーに、ｅＭＬＢＲ－Ｒ１２のＭＡＣアドレスと、ｅＭＬＢＲ－Ｒ１２に固定的あるいは動的に割り当てるＩＰアドレスとの対応関係を記憶しておく制御部１５のＭＬＢテーブルＡに仮登録し（ステップＳ５２１）、さらに転送部のＭＬＢテーブルＡに正登録する（ステップＳ５２２）。その上で、ｅＭＬＢＲ－Ｒ１２に対して、ネットマスクやＤＧＷのＩＰアドレスなど、ネットワークへの接続に必要な情報とともにＩＰアドレスを割り当てるＤＨＣＰ応答を返す（ステップＳ５２３）。

【００９６】

以後、ＩＥＥＥ８０２．１Ｘ対応ノード（パソコンなど）は、実施形態２で述べた方法で認証を受け、ｅＭＬＢＲ－Ｒ１２との間でセキュアチャネルを確立し、セキュアチャネル識別情報をキーにノードのＩＰアドレスとＭＡＣアドレス及びＱｏＳの対を転送部１４のＭＬＢテーブルＢに正登録されてから、ｅＭＬＢＲ１２に対し暗号化ユーザＭＡＣフレームを送信し（ステップＳ５２４）、ｅＭＬＢＲ－Ｒ１２ではセキュアチャネルの識別情報をキーに転送部１４のＭＬＢテーブルＢを検索し、同フレーム／パケットの送信元ＩＰアドレスと送信元ＭＡＣアドレスの対が存在しない場合、ｅＭＬＢＲ１２は、ノードが送信したパケットを破棄する（ステップＳ５２６）。一方、ＭＬＢテーブルＢに存在する場合、予め設定されたＱｏＳで、また送信元プライベートＩＰアドレスをグローバルＩＰアドレスに変換し、ｅＭＬＢＲ１２とｉＭＬＢＲ１１間のセキュアチャネルを介して、すなわちｅＭＬＢＲ１２とｉＭＬＢＲ１１間の共有鍵を用いてユーザパケットを暗号化しＭＡＣフレームにカプセル化してから次ホップノードであるｉＭＬＢＲ１１に、指定されたＱｏＳで転送する（ステップＳ５２７）。

【００９７】

ｉＭＬＢＲ１１は、ステップＳ５２７で転送されてきたフレーム／パケットについて、ｅＭＬＢＲ１２とｉＭＬＢＲ１１間のセキュアチャネルの識別情報をキーに転送部１４のＭＬＢテーブルＡを検索し（ステップＳ５２８）、ＭＬＢテーブルＡに送信元ＩＰアドレ

ス及び送信元ＭＡＣアドレスが存在しない場合、同フレーム／パケットを廃棄する（ステップＳ５２９）。一方、ＭＬＢテーブルＡに存在する場合、指定されたＱｏＳで次ホップノードに、ユーザＭＡＣフレームを転送する（ステップＳ５３０）。また、本実施形態におけるｉＭＬＢＲ１１が備える制御部１５及び転送部１４は連携して、ｉＭＬＢＲ１１及びｅＭＬＢＲ１２間で暗号鍵の更新による、実在確認を適宜行い（ステップＳ５３２）、ステップＳ５３３で確認結果に応じてＭＬＢテーブルＡを更新、すなわちＭＬＢテーブルＡの有効期間を延長してもよい。

【００９８】

（実施形態４）

上記実施形態では、ｅＭＬＢＲ１２はＩＥＥＥ８０２．１Ｘに則ってｉＭＬＢＲ１１を介してＲＡＤＩＵＳサーバーで認証を受けることとしているが、図１５に示す本実施形態では、ｅＭＬＢＲ１２とｉＭＬＢＲ１１各々が予め信頼できる認証局（ＣＡ局）から認証を受け、その真正性を証明するデジタル証明書を取得していれば、これを直接交換し合い相互に認証してもよい。

【００９９】

以上に述べた実施形態に基づいたアドレス詐称対策を適用することによって、たとえＩＰｓｅｃを用いたトランスポートモードあるいはトンネルモードによる暗号化通信が行われても、すべてのフレーム／パケットについてｅＭＬＢＲ１２及びｉＭＬＢＲ１１でポート又はチャネルをキーに送信元ＩＰアドレスと送信元ＭＡＣアドレスの対がＭＬＢテーブルに存在するかチェックするため、インターネット１０へのアドレス詐称パケットの流出／流入を阻止できる。そして、これを適用したネットワーク（プロバイダー）が広がっていくにつれてＤＤｏＳやＤＲＤｏＳなど、様々なアドレス詐称を前提としたサイバー攻撃やサーバーなどへの不正侵入などが激減するものと思われる。

【０１００】

また、たとえ一部の「何でも繋がせる」プロバイダーもしくはネットワークや匿名ネットワークなどがあっても、これらのネットワークとの接続点に配備するｉＭＬＢＲ１１ではＭＬＢテーブルに記述されたネットワークアドレス空間から外れたパケットを遮断(前述のｕＲＰＦとして機能する)することができ、さらに廃棄要請と組み合わせることによって被害者ＩＰアドレスなどと対で攻撃者のＩＰアドレスあるいはアドレス空間内でランダムにアドレス詐称しているパケットを遮断することができる。さらに、ｉＭＬＢＲ１１の収容ポートの通信サービス品質（帯域を狭め、検疫（アノマリ検出によるＳＹＮ ｆｌｏｏｄ攻撃パケットなどの廃棄や、ウィルス検知ソフトによるウィルス混入パケットの廃棄、暗号化パケットの廃棄、スパムメールの廃棄など）を強化するなど）を限定することによって、インターネット１０全体の安心・安全性が格段に高まるものと考えられる。

【０１０１】

しかし、クラッカーから見ればｅＭＬＢＲ１２やｉＭＬＢＲ１１が新たな攻撃対象となる。このためには、これらのパケット転送装置へ不正侵入されないよう頑健な作りにする必要がある。また、たとえ侵入されプログラムやルーティングテーブル、ＭＬＢテーブルなどが改ざんされてもそれを検出できるように完全性検査機能、またＥＡＰ ｆｌｏｏｄ攻撃やＡＲＰ ｆｌｏｏｄ攻撃など、制御部１５のソフトウェア処理系に対する攻撃が行われても、それらを転送部１４で遮断するような自己防御機能を備えておく必要がある。さらに、ｅＭＬＢＲ１２やｉＭＬＢＲ１１に新たなセキュリティホールが見つかった場合や、新たなサイバー攻撃の出現に対応した機能を制御部１５や転送部１４に追加できるようバージョンアップ機能を備えておく必要がある。

【０１０２】

本実施形態に係るパケット転送装置はＩＰｖ４に限定されるものではなく、ＩＰｖ６も扱ってもよい。また、グローバルＩＰアドレス既得ユーザに対しては、届け出のあったアドレス空間を制御部１５のＭＬＢテーブルに仮登録しておき、ＩＥＥＥ８０２．１Ｘ認証を経てＩＰアドレス単位に、転送部１４のＭＬＢテーブルに正登録してもよい。

【０１０３】

さらに、ｉＭＬＢＲ１１又はｅＭＬＢＲ１２が、サーバー１３を収容する場合には、サーバー１３を収容するポートもしくはチャネルの識別情報をキーに、（別設置のＤＨＣＰもしくは自装置内のＤＨＣＰから、あるいはユーザが保有するアドレス空間から）サーバー１３に割り当てられたＩＰアドレスとサーバー１３のＭＡＣアドレスに加え、サーバー１３上で起動するプロセスを識別する固定のプロセス識別アドレス（ｗｅｌｌ－ｋｎｏｗｎポート番号）もバインディングの対象にしてもよい。これによって、たとえ悪意ある攻撃者によって不正侵入用のポートが作られても、同ポートからの情報流失などを防ぐことが可能になる。

【０１０４】

また、ＡＲＰリフレクションを適用する場合は、前述したように認証レベルが低いことから、例えば、当該端末を他のエンドノードから隔離したＶＬＡＮを構成し、帯域制限を施したブリッジを介して外部ネットワークに接続する、またＩＴＶ（Ｉｎｄｕｓｔｒｉａｌ　ＴｅｌｅＶｉｓｉｏｎ）などの監視カメラであれば、接続先は限定されるため、宛先ＩＰアドレスをＭＬＢテーブルに追加するなどの対策を施すことによって、インターネット１０に不正パケットが流出することを阻止できる。

【０１０５】

さらに、ｉＭＬＢＲ１１又はｅＭＬＢＲ１２が備える制御部１５は、ノードもしくはエンティティが収容されているポートもしくはチャネルでの実在確認を適宜（必ずしも定期的である必要はない）行い、通信サービス品質を維持更新（ＩＥＥＥ８０２．１Ｘにおけるｍａｃｓｅｃの使用、物理的接続の確認、共有鍵の更新、一定時間実在確認応答がなければＭＬＢテーブルからエントリーを削除し通信サービスを停止する、ノードが別のポートもしくはチャネルに移動したときは元のポートもしくはチャネルでの不在を確認してから、新たに認証し直しＭＬＢテーブルのポートもしくはチャネルのみ変更するなど）してもよい。

【０１０６】

なお、一つのポート又はチャネルが収容するノードもしくはエンティティは複数であってもよい。この場合には、該ポート又はチャネルの識別情報をキーとするＭＬＢテーブルには、複数の送信元ＩＰアドレスと送信元ＭＡＣアドレスの対が登録されることになる。

【０１０７】

また、ｅＭＬＢＲ１２は、ユーザ側ネットワークにおいてインターネット１０に向けて一台もしくは複数台が多段的に配備されてもよい。さらに、ｅＭＬＢＲ１２は、インターネット１０の端部に配備されている複数台のｉＭＬＢＲ１１に対して、接続（マルチホーミング）されてもよい。

【０１０８】

（実施形態５）

上記の実施形態の導入によって、アドレス詐称パケットのインターネット１０への流入、ひいてはサイバー攻撃が激減するものと考えられるが、アドレス詐称を伴わない攻撃（例えば、送信元ＩＰアドレスをランダムに変えながらＳＹＮ　ｆｏｏｄ攻撃する場合には、一定の確率で真の送信元ＩＰアドレスで攻撃パケットがインターネット１０へ流出／流入する。また、ウィルスに感染したパソコンや遠隔操作されたデジタルテレビなどから、利用者が知らない間にアドレス詐称せずに攻撃に加担させられる。）は、防ぐことができない。さらに、ＤＤｏＳ攻撃などの首謀者が所謂Ｃ＆Ｃ（Ｃｏｍｍａｎｄ　ａｎｄ　Ｃｏｎｔｒｏｌ）サーバーを介してボットに指令を発信する際に、匿名ネットワーク（例えば、Ｔｏｒ：Ｔｈｅ　Ｏｎｉｏｎ　Ｒｏｕｔｅｒなど）を経由して送信元ＩＰアドレスを隠ぺい化（以下、匿名ＩＰアドレスと呼ぶ）する行為が広く行われているが、匿名ＩＰアドレスパケットはアドレス詐称パケットではないため、アドレス非詐称パケットと同様に、インターネット１０への流出／流入を防ぐことができない。ただし、Ｔｏｒネットワークであれば、数千台あるとされているＴｏｒノードのアドレス（匿名ＩＰアドレス）は、インターネット上で公開されており、ブラックリスト化が可能である。

【０１０９】

本実施形態は、上記問題に対する対策で、他のノードからの要請によってｉＭＬＢＲ１１やｅＭＬＢＲ１２が廃棄テーブルを生成・更新し、それに合致したパケットを廃棄する動作例について説明する。

【０１１０】

具体的には、図１６に示すように、不正アクセス監視システム／侵入検知システムＩＤＳ（Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ）や侵入防止システムＩＰＳ（Ｉｎｔｒｕｓｉｏｎ Ｐｒｅｖｅｎｔｉｏｎ Ｓｙｓｔｅｍ）、匿名ネットワークもしくは匿名ＩＰアドレス検出システムなどを稼働させた対処要請ノードもしくは対処要請エンティティとして機能するＲｅＮ４０（Ｒｅｑｕｅｓｔ Ｎｏｄｅ）は、インターネット１０の要所やサービスを提供しているデータセンターや組織内ネットワーク、ＤＭＺ（ＤｅＭｉｌｉｔａｒｉｚｅｄ Ｚｏｎｅ）、サーバー内でトラフィックを監視し、明確な攻撃や攻撃によると推定される輻輳、匿名ＩＰアドレスを検知するとＤｅＮ４２（Ｄｅｌｉｖｅｒ Ｎｏｄｅ）へ攻撃パケットと推測されるパケットを送り対処を要請するノードである。また、ＤｅＮ４２は、ＲｅＮ４０から送られた攻撃パケットを収集・分析・集約し、攻撃と判定したときに廃棄要請情報を発信する機関のノードである。ＳｈＮ４３（Ｓｈａｒｅ Ｎｏｄｅ）は、ＤｅＮ４２が発信した廃棄要請情報を、廃棄対象パケットを中継転送しているｉＭＬＢＲ１１又はｅＭＬＢＲ１２へ、大規模な攻撃であればインターネット１０全体に配送するノードである。なお、図１６には、ＤｅＮ４２やＳｈＮ４３などが、インターネットの内部に配置されるように記されているが、前述のＨＲＳ２３と同様に、不正侵入などによって廃棄要請情報やプログラムなどが改ざんされないよう、ＩＳＰなど信頼できる機関がこれらを厳重管理することを意味するものであって、ｉＭＬＢＲ１１やｅＭＬＢＲ１２を介して、インターネットの外側に配置されてもよい。

【０１１１】

ＤｅＮ４２が発信する廃棄要請情報には、廃棄対象（攻撃や匿名ＩＰアドレス、情報漏洩など）パケットの送信元ＭＡＣアドレス／送信元ＩＰアドレス／ポート番号と送信先ＭＡＣアドレス／送信先ＩＰアドレス／ポート番号の一部又はすべての対と有効期間が、ＤｅＮ４２のデジタル証明書もしくは電子署名とともに記述されている。これを受取ったＳｈＮ４３は、廃棄要請情報に記述されている攻撃元ＩＰアドレス及び被害者ノードのＩＰアドレスそれぞれまでの経路情報を調べるｔｒａｃｅｒｏｕｔｅコマンドなどを応用して廃棄要請先のｉＭＬＢＲ１１やｅＭＬＢＲ１２のＩＰアドレスを割り出（アドレス解決）し、該当するｉＭＬＢＲ１１又はｅＭＬＢＲ１２へ廃棄要請情報を配送する。具体的には、ＴＴＬを１ずつ増やしながらＩＣＭＰエコー要求パケットを送信することによって経路情報を取得するが、ＴＴＬが１のＩＣＭＰエコー要求パケットをＭＬＢＲが受信すると、ＩＣＭＰ時間超過パケットのオプションフィールドにＭＬＢＲの属性情報（例えば、エッジルータとして配備するｉＭＬＢＲ、ＭＬＢＲ未導入のプロバイダーとの境界に配備するｉＭＬＢＲ、家庭用のｅＭＬＢＲ－Ｒ、無線ＬＡＮ用のｅＭＬＢＲ－Ｗ、データセンター用のｅＭＬＢＲ－Ｃなどの種別や、収容するノードやネットワークの属性など）を書き込んで経路情報の調査元（ＳｈＮ４３）に返すことによって、転送経路上に存在するｉＭＬＢＲ１１やｅＭＬＢＲ１２のＩＰアドレスとその属性情報を取得してもよい。その後、ＨＴＴＰやＳＭＴＰなどの転送プロトコルを用いて当該ｉＭＬＢＲ１１やｅＭＬＢＲ１２へ廃棄要請情報を送信してもよい。被害者ノードを収容するｉＭＬＢＲ１１やｅＭＬＢＲ１２についても、同様にすればよい。ＩＣＭＰパケットとＨＴＴＰやＳＭＴＰなどの転送プロトコルを用いることによって、転送経路上にファイアウォールがあっても遮断されることなくファイアウォールを通過できる。

【０１１２】

廃棄要請情報を受取ったｉＭＬＢＲ１１又はｅＭＬＢＲ１２の制御部１５では、添付されているデジタル証明書から廃棄要請情報の真正性を確認してから、廃棄要請情報に基づいて廃棄テーブルを生成・更新し、転送部１４に伝達する。転送部１４では、以後、受信したフレーム／パケットについてＭＬＢテーブルと照会してアドレス詐称パケットでないことを確認した後、廃棄テーブルに該当する送信元ＩＰアドレス／ポート番号と送信先Ｉ

Ｐアドレス／ポート番号などの対もしくはブラックリストとして登録されている匿名ＩＰアドレスに該当しないかを調べ、該当する場合は廃棄する（廃棄テーブルと照合してからＭＬＢテーブルに照会してもよい）。該当しない場合は、ルーティング処理に進む。

【０１１３】

本実施形態において、ＲｅＮ４１はＩＤＳ又はＩＰＳ相当の機能あるいはウィルス検知ソフトを実装したパソコン、タブレット端末、スマートフォン、デジタルテレビなどであってもよい。また、ＲｅＮ４０がＤｅＮ４２及びＳｈＮ４３相当の攻撃パケットの分析機能や配送機能などを有し、攻撃者のＩＰアドレスを特定できる場合には、直接、前述のｔｒａｃｅｒｏｕｔｅコマンドを応用したＩＣＭＰエコー要求パケットを用いることによって、ＲｅＮ４１から攻撃者までの転送経路上に存在するｉＭＬＢＲ１１やｅＭＬＢＲ１２のＩＰアドレスとその属性情報、さらにＩＣＭＰ時間超過パケットが返ってくる順序から、ｉＭＬＢＲ１１やｅＭＬＢＲ１２の位置関係(被害者ノードを収容するＭＬＢＲか攻撃者ノードを収容するＭＬＢＲかの判別)を把握することができる。その後、ＨＴＴＰやＳＭＴＰなどの転送プロトコルを用いて、当該ｉＭＬＢＲ１１又はｅＭＬＢＲ１２へ廃棄要請情報を配送してもよい。さらに、攻撃元が限られた範囲である場合は、ＤｅＮ４２はＳｈＮ４３の機能を代行し直接該当するｉＭＬＢＲ１１又はｅＭＬＢＲ１２へ上述の方法で廃棄要請情報を配送してもよい。また、ｉＭＬＢＲ１１及びｅＭＬＢＲ１２はＲｅＮ４０の機能を実装し、ＲｅＮ４０として機能してもよい。

加えて、上記実施形態では、ｉＭＬＢＲ１１及びｅＭＬＢＲ１２はＤｅＮ２３やＳｈＮ４３などからの廃棄要請によって廃棄テーブルを更新するとしているが、ＤｅＮ２３やＳｈＮ４３からの通知によってｉＭＬＢＲ１１及びｅＭＬＢＲ１２がＤｅＮ２３やＳｈＮ４３などに廃棄要請情報を取りにいく、あるいは定期的にｉＭＬＢＲ１１及びｅＭＬＢＲ１２がＤｅＮ２３やＳｈＮ４３などをアクセスし、自己に関係する新たな廃棄要請情報があればそれを取得してもよい。

【０１１４】

本実施形態によって、アドレス詐称を伴わない攻撃や、前述の匿名ネットワークの端部ノード（Ｔｏｒノード）のＩＰアドレスを、同ノードを収容するｉＭＬＢＲ１１又はｅＭＬＢＲ１２の廃棄テーブルに（ブラックリストとして）登録しておくことによって、「何でも繋がせる」ネットワークと匿名ネットワークを経由してきた攻撃パケットを廃棄することが可能になり、インターネット１０への流入／流出を阻止することができる。さらに、被害者ノードのＩＰアドレスとＬ４ポート番号、送信先ＩＰアドレスなどの対を、被害者ノードを収容するｉＭＬＢＲ１１やｅＭＬＢＲ１２の廃棄テーブルに登録しておくことによって、以後、情報漏洩パケットの流出やＣ＆Ｃサーバーへのアクセスなどを阻止することができる。

【０１１５】

（実施形態６）

本実施形態では、マルチレイヤ・バインディング・ルータ（ＭＬＢＲ）によるサイバー攻撃の対策について以下に述べる。まず、本実施形態では、クラッキング意図パケットを対策の対象とする。クラッキング意図パケットは、ＩＰアドレス詐称（成りすましを含む）パケット、匿名ＩＰアドレスパケット及びＩＰアドレス非詐称攻撃パケットを示す。

【０１１６】

本実施形態に係るＭＬＢＲの機能を以下（１）～（６）に示す。

（１）ノードもしくはエンティティからの接続要求があった時、その真正性と健全性を認証・検疫するとともに、認証・検疫レベルに応じて提供するＱｏＳを決定する。

（２）物理ポートｏｒ（セキュア）チャネルをキーに、ノードもしくはエンティティのＩＰアドレスとＭＡＣアドレスとの対応関係をＭＬＢテーブルに登録する。

（３）パケットを受信した物理ポート又はチャネルをキーにＭＬＢテーブルを検索し、パケットの送信元ＩＰアドレスとＭＡＣアドレスの対が存在するときは、次ホップノードへ指定されたＱｏＳで転送し、存在しないときはアドレス詐称ｏｒ成りすましパケットとみなして破棄する。

（４）物理ポートまたはチャネルを介して適宜ノードもしくはエンティティの実在及び健全性確認を行い、ＭＬＢテーブルを更新（有効期間を延長）する。
（５）他のノードからの正当な廃棄要請を受けて破棄テーブルを更新し、以後、廃棄テーブルに該当する匿名のアドレスパケットやアドレス非詐称攻撃パケットを廃棄する。
（６）利用者（ｅｇｒｅｓｓ）に配置するｅＭＬＢＲ１２と、インターネット側（ｉｎｇｒｅｓｓ）に配備するｉＭＬＢＲ１１により、クラッキング意図パケットのインターネットへの流出及び流出を阻止する。

【０１１７】

本実施形態に係るＭＬＢＲにおけるサイバー攻撃の対策の対象となるノードをについて以下に具体的なノードを列挙する。

・ホストとルータの総称をノードとしてもよい。この場合、ノードの集合であるネットワークもノードとなる。
・ＩＥＥＥ８０２．１Ｘ対応端末（ＰＣやスマートフォン等）この場合、認証・検疫におけるクラッキング行為の抑止と端末の健全性確保に有効である。しかし、匿名ネットワーク経由で悪事を行っても特定され難く、ボットに感染すればＤＤｏＳ攻撃に加担し。また、遠隔操作や成りすましされ（見かけ上）アドレス詐称せずに悪事加担も考えられる。
・ＩＥＥＥ８０２．１Ｘ非対応端末（テレビ等のスマート家電やＩｏＴ）。この場合ＯＳのアップデートやＦＷはなく、サイバー攻撃の温床になることも考えられる。
・家庭用ルータ。遠隔操作され、攻撃に加担も考えられる。
・何でもつながせるポリシーのＩＳＰ。この場合、すべてのＩＳＰが対策を導入することは考えにくい。
・匿名ネットワーク及びＴｏｒ等。この場合、匿名アドレスであって、アドレス詐称ではない。
・成りすまし端末。

【０１１８】

ここで、上述したＩＥＥＥ８０２．１Ｘ対応端末とｅＭＬＢＲ１２間のシーケンス動作の例を図２１に示す。本実施形態に係る図２１のシーケンスでは、実施形態２における図１２のシーケンスとは、サーバーを２つ備える点で相違する。具体的には、サーバーは、検疫サーバー３１及びＲＡＤＩＵＳサーバー２３を別々に備えてもよい。また、ステップＳ５１４では、ｅＭＬＢＲ１２はこれをホーム認証サーバーとして機能するＲＡＤＩＵＳサーバー２３又は検疫サーバー３１へ仲介する際、健全性ステートメント交換も行う点で実施形態２における図１２のシーケンスと相違する。また、上述の構成の違いにより、図１４に対し図２１では、ステップＳ５１５において、認証結果及び検疫結果をそれぞれのサーバーがｅＭＬＢＲ１２へ送信することができる。

【０１１９】

以下に、具体的なケースを用いながら本実施形態に係るサイバー攻撃に対応策を説明する。第１のケースでは、標的型メール攻撃に対する対応策について以下に示す。標的型メール攻撃では、偽装メールを不用意に開封した社員の端末がコネクトバックで踏み台にされ、以後、Ｃ＆Ｃサーバーを介して攻撃者が指令を送り複数の端末を巻き込みながら基幹サーバーにバックドアを作り、機密情報を盗み出す攻撃である。

【０１２０】

第１のケースに係る標的型メール攻撃に対し、本実施形態では４つの対応例を述べる。１つ目は、攻撃者の多くがＣ＆Ｃサーバーに指令を送るときに匿名アドレスを用いるが、本対策では匿名ネットワークの使用を不能にする。２つ目は、基幹サーバーは、自己のポート番号を含めてＭＬＢテーブルに登録しておくことによって、バックドアからの情報漏洩を防ぐ。

【０１２１】

３つ目は、ＩＤＳなどで組織ネットワーク内での攻撃若しくは攻撃の兆候を検出次第Ｃ＆Ｃサーバーのアドレスと自組織のＩＰアドレスを記述した廃棄要請を自組織のｅＭＬＢＲ１２及びＣ＆Ｃサーバーを収容しているｅＭＬＢＲ１２とｉＭＬＢＲ１１に送り、

以後、Ｃ＆Ｃサーバーとの間の指令パケットのやり取りを阻止する。４つ目は、漏洩情報の送信先ＩＰアドレスを記述した廃棄要請を自組織のｅＭＬＢＲ１２とｉＭＬＢＲ１１に送り、以後の情報漏洩を阻止する。

【０１２２】

次に、第２のケースでは、ワイヤレスセンサーネットワーク攻撃に対する対応策について以下に示す。ワイヤレスセンサーネットワーク攻撃では、アドホック型のセンサーネットワークを形成しているＩＯＴが次々にマルウェアに感染もしくはＩｏＴの製造工程でマルウェアが埋め込まれ、攻撃者がＣ＆Ｃサーバーを介してＩＯＴに様々な指令を送り、データの改ざん、情報の盗み出し、機器や社会インフラの暴走などを行わせ、システムを制御不能状態にする攻撃である。

【０１２３】

第２のケースに係るワイヤレスセンサーネットワーク攻撃に対し、本実施形態では３つの対応例を述べる。１つ目は、匿名アドレスの使用を不能する。２つ目は、センサーネットワークを収容しているｅＭＬＢＲ１２のＱｏＳとして、インターネット接続先ＩＰアドレスを限定しておけばＩｏＴがＣ＆Ｃサーバーなどへアクセスすることを阻止できる。３つ目は、ＱｏＳとして帯域制限しておけば、ＩｏＴの帯域攻撃等への使用を不能にする。

【０１２４】

次に、第３のケースでは、ＤＮＳキャッシュポイズニングに対する対応策について以下に示す。ＤＮＳキャッシュポイズニングでは、ＩＰＳ、企業、大学などのキャッシュＤＮＳサーバーに対して偽のＤＮＳ情報をキャッシュさせる攻撃である。偽のＤＮＳ情報をキャッシュさせることにより、そのキャッシュＤＮＳサーバーを参照するＩＳＰの顧客、企業の社内ユーザ、大学の学生などクライアントを偽のサイトに誘導させるなどの行為が可能となる攻撃である。

【０１２５】

第３のケースに係るＤＮＳキャッシュポイズニングに対する対応例を以下に述べる。ＡＣＬ（Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ Ｌｉｓｔ）が適切に施されていないＩＳＰや企業、大学などでは、本来クライアントではない外部からの問い合わせに対して応答を返してしまっている。こういったキャッシュＤＮＳサーバーをオープンリゾルバと呼ぶ。オープンリゾルバは外部から任意の問い合わせができるため、毒を入れやすい状況にあるといえる。また、本来のクライアントであっても、ウイルスに感染してポット化されているようなケースでは任意の問い合わせが可能である。

【０１２６】

従って、適切な対応設定が施されていないキャッシュＤＮＳサーバーは、これを利用するクライアントに１台でも悪意あるクライアント若しくは遠隔操作されたクライアントがいた場合にキャッシュポイズニング攻撃を受けて、成功するとそのキャッシュＤＮＳサーバーを利用するすべてのクライアントに影響を与える可能性がある。

【０１２７】

キャッシュポイズニングの具体的な手法としては、以下のようなものが挙げられる。例えば、カミンスキーメソッド、委任インジェクション攻撃、移転インジェクション攻撃である。現在行われている対策としては、キャッシュＤＮＳサーバーに適切なＡＣＬを設定し、オープンリゾルバでなくすこと、外部へ問い合わせを行う際の送信元ポート番号を固定（又はインクリメンタル）せず、ランダマイズ化する実装若しくは設定を導入すること。

【０１２８】

また、近年では、キャッシュＤＮＳサーバー自身はランダマイズしていても、インターネットへ出ていく途中経路にＮＡＴ装置やＦｉｒｅｗａｌｌが存在した場合、その装置がポート番号を固定若しくはインクリメンタルマッピングしてしまうケースも見られるため、そういった中継に介在する装置のケアも必要である。昨今のＩＳＰではＩＰアドレスの枯渇に対応するため、ＬＳＮ（Ｌａｒｇｅ Ｓｃａｌｅ ＮＡＴ）を採用しているケースもあり、それらの実装の中にもポートのマッピングがきちんとランダマイズ化されない実

装があるという。このように、現在行われている対策は、キャッシュＤＮＳサーバーだけにとどまらず、ＩＳＰや企業、大学内のネットワーク全体にわたって、高度な専門知識を持ったネットワーク管理者が注意深く設定し管理運用しなければならないのが実情である。

【０１２９】

これに対して、ＭＬＢＲによる対策では、ＤＮＳキャッシュポイズニング、攻撃者が権威ＤＮＳサーバーのＩＰアドレスに詐称して直接キャッシャＤＮＳサーバーに毒を入れるか、遠隔操作で善良な利用者のＰＣなどから権威ＤＮＳサーバーのＩＰアドレスに詐称して毒を入れることが考えられるが、その際に攻撃者はＴｏｒネットワークなどを使って送信元ＩＰアドレスを匿名化する。ＭＬＢＲでは、匿名アドレスパケットはインターネットへの流入／流出を阻止する。またＩＰアドレス詐称パケットはＭＬＢＲ内で破棄するので、高度な設定など必要とせずにＤＮＳキャッシュポイズニングを防ぐことができる。

【０１３０】

次に、第４のケースでは、ＤＮＳリフレクション攻撃（ＤＮＳ　Ａｍｐ）に対する対応策について以下に示す。ＤＮＳリフレクション攻撃では、一般にはＤＮＳは問い合わせよりも応答のほうがデータサイズが大きい。これを悪用し送信元アドレスをターゲットのアドレスに偽装して大量の問い合わせを行うことでターゲットのアドレスに向かって大量の応答が返る攻撃である。

【０１３１】

第４のケースに係るＤＮＳリフレクション攻撃に対する対応例を以下に述べる。どんな相手からの問い合わせでも応答するということから先ほどのオープンリゾルバが踏み台とされるケースは多い。また、家庭用ブロードバンドルータを代表とするＣＰＥ（Ｃｕｓｔｏｍｅｒ　Ｐｒｅｍｉｓｅｓ　Ｅｑｕｉｐｍｅｎｔ）が踏み台とされるケースも多々ある。

【０１３２】

これはオープンリゾルバ若しくはオープンフォワーダー（どこからの問い合わせでもその機器でフォワード設定しているＤＮＳサーバーへ問い合わせフォワードする）となっているＣＰＥ実装が多く出回っており、攻撃者が悪用すると折り返しトラフィックなども含めてより大きなトラフィックを発生させることができる。

【０１３３】

対策として国内ＩＳＰやＣＡＴＶ業者が現在取り組みを始めつつあるものとして、ＩＰ５３Ｂ（Ｉｎｂｏｕｎｄ　Ｐｏｒｔ　５３　Ｂｌｏｃｋｉｎｇ）がある。これはＩＳＰから顧客のポート５３へのトラフィックを遮断するというものである。これにより、オープンリゾルバやオープンフォワーダーへのトラフィックを抑止することができるが、これを実施した場合の弊害（顧客がＤＮＳサーバーを立てていた場合にサービス妨害となる）を考慮して慎重な導入が進められている。これに対して、ＭＬＢＲによる対策としては、ＤＮＳリフレクション攻撃（ＤＮＳ　Ａｍｐ）では、アドレス詐称パケットがベースとなるので、これも高度な専門知識など必要とせずにＭＬＢＲで妨ぐことができる。

【０１３４】

第１の関連技術では（例えば、特許文献２参照。）、コンピュータシステム、コントローラ、及びネットワーク監視方法における、データセンターでのアドレス詐称対策が用いられている。具体的には、詐称アドレスを利用した不正アクセスや妨害に対するセキュリティ強度を向上させる。第１の関連技術によるコンピュータシステムは、コントローラと、コントローラによって設定されたフローエントリに適合する受信パケットに対し、当該フローエントリで規定された中継動作を行うスイッチと、スイッチに接続されたコントローラを具備する。

【０１３５】

スイッチは、自身に設定されたフローエントリに適合しない受信パケットの送信元アドレス情報を、コントローラに通知（Ｐａｃｋｅｔ－Ｉｎ）する。コントローラは、正当なホスト端末のアドレス情報と送信元アドレス情報とが一致しない場合、受信パケットの送

信元アドレスが詐称されていると判定し、廃棄フローエントリをスイッチに設定する。したがって、本実施形態に係る発明と比べ、第１の関連技術では、新たなアドレス詐称パケットを受信するごとに処理負荷が重いＰａｃｋｅｔ－Ｉｎが発生する。すなわち、この発明では大量のアドレス詐称パケット攻撃によって、スイッチは過負荷状態に陥り動作不能に陥る。

【０１３６】

第２の関連技術では、ＩＰアドレスとＭＡＣアドレスを対応付けてテーブルに格納し、端末から送られたパケットのＩＰアドレスとＭＡＣアドレスがテーブルにない時は破棄する。具体的には、端末は、通信に先立って初段ルータのアドレス解決のため、ＡＲＰ要求パケットを必ずブロードキャスト送信する。このＡＲＰ要求パケットには、送信元のＭＡＣアドレスとＩＰアドレスとが記述されている。このため、悪人がたとえ異なる物理ポートからであってもＡＲＰ要求パケットをＷｉｒｅｓｈａｒｋなどでキャプチャし、ＩＰアドレスとＭＡＣアドレス対を盗み見、他人のＰＣに成りすますことができる。

【０１３７】

一方本実施形態に係る発明では、物理ポート又は（セキュア）チャネルをキーにＩＰアドレスとＭＡＣアドレス対をＭＬＢテーブルで管理するため、他ポート又はチャネルからＡＲＰ要求パケットを盗み見て成りすまししても、成りすまし端末からのパケットを破棄できる。なお、これまではＮＩＣの製造メーカで付与したＭＡＣアドレスを書き換えることは事実上不可能であったが、ＯｐｅｎＦｌｏｗなどのＳＤＮ技術の出現によって、任意に書き換えられるようになった。したがって、本実施形態に係る発明と比べ、第２の関連技術では、物理ポートまたは（セキュア）チャネルをキーに管理する機能を有しない点でセキュリティ上の問題がある。

【０１３８】

第３の関連技術では（例えば、特許文献３及び特許文献４参照。）、ＭＡＣアドレスとＩＰアドレスを合わせて記憶して、ユーザがＩＳＰから付与されたＩＰアドレスを端末に設定したり、故意に他の端末と同一のＩＰアドレスに改ざんするユーザに対して、予め付与されたＩＰアドレスを設定していない端末からのパケットは受信してもブリッジ内で破棄する。具体的には、ＭＡＣアドレスとＩＰアドレスを対応付けて管理するテーブルを具備する。しかし、これは、ＩＰアドレスが付与された端末に対してＭＡＣブリッジがＡＲＰ要求パケットを送信し、返送されてきたＡＲＰ応答パケットに記述されているＭＡＣアドレスを取得する際に生成される副産物であり、以後のフィルタリングで参照するのは送信元ＭＡＣアドレスのみである。

【０１３９】

したがって、例えば端末がマルウェアに感染しＩＰアドレス詐称パケットを送信しても阻止できず、第３の関連技術では、ＭＡＣブリッジ（レイヤ２のパケット転送装置）であり、基本的にＭＡＣアドレスしか参照しないことによる問題が発生する。一方、本実施形態に係る発明では、物理ポート又は（セキュア）チャネルをキーにＭＡＣアドレスとＩＰアドレスの対がＭＬＢテーブルに存在するか否かをチェックするもので、フィルタリングで参照する対象が異なる。これによって、たとえ端末の所有者がＩＰアドレスやＭＡＣアドレスの詐称を行っていなくても、マルウェアに感染しＤＤｏＳ攻撃などに加担させられてＩＰアドレス詐称パケットを送信しても、インターネットへの流出と流入を阻止できる。

【０１４０】

ここで、本実施形態に係るパケット転送システムにおけるＡＲＰリフレクションのＩＰｖ６版の適応を具体的に述べる。ＩＰｖ６では、ＩＰｖ４用のＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）の代わりにＮＤＰ（Ｎｅｉｇｈｂｏｒ Ｄｉｓｃｏｖｅｒｙ Ｐｒｏｔｏｃｏｌ）を用いる。ＮＤＰには、リンク上に存在する近隣ノードのＭＡＣアドレスの判別やアドレスの変更・停止検出、近隣ノードへの到達性のチェック、リンク上にいるルータの検出及びパケットの転送先としての設定などの機能があり、各々で用いるパケットの呼称が異なる。また、ＮＤＰには、ブロード送信がないため、

代わりにマルチキャスト送信を用いる。また、図２２は、本実施形態に係るパケット転送システムにおけるＩＰｖ４版のＡＲＰリフレクションをＩＰｖ６の適応した場合の対比を示している。

【０１４１】

ＩＰｖ６版の適応で用いられる機能の用語を以下に挙げる。

・ＲＳパケット（ルータ要請パケット（ＲＳ：Ｒｏｕｔｅｒ Ｓｏｌｉｃｉｔａｔｉｏｎ））：ノードが初段ルータのアドレス解決に用いるパケット

・ＲＡパケット（ルータ応答パケット（ＲＡ：Ｒｏｕｔｅｒ Ａｄｖｅｒｔｉｓｅｍｅｎｔ））：ＲＳパケットに対してルータが返すパケット

・ＮＳパケット（近隣要請パケット（ＮＳ：Ｎｅｉｇｈｂｏｒ Ｓｏｌｉｃｉｔａｔｉｏｎ））：特定のノードのＭＡＣアドレスを解決するパケット。ＩＰｖ４のＡＲＰパケットとほぼ同じ。

・ＮＡパケット（近隣通知パケット（ＮＡ：Ｎｅｉｇｈｂｏｒ Ａｄｖｅｒｔｉｓｅｍｅｎｔ））ＮＳパケットに対する応答パケット

【０１４２】

なお、前述したように本発明によるＭＬＢＲをインターネット全体並びにすべての利用者サイドに配備することは、事実上不可能である。このための対策として、ｅＭＬＢＲ１２を介して所定の認証や検疫を受けて接続を許可されたノードまたはエンティティが送信したパケットでｅＭＬＢＲ１２で廃棄されなかったものについて、例えば転送部１４または制御部１５において、ＩＰｖ４であれば例えばＩＰヘッダのサービスタイプフィールドの未定義ビット（最後方の２ビット）に、ＩＰｖ６であればトラフィッククラスフィールドの所定ビット（最後方の２ビット）に認証フラグとして“１”を書き込むことによってその真正性を表示するようにしてもよい。さらに、未認証のノードまたは未認証のエンティティが送信したパケット、すなわちｅＭＬＢＲ１２を通っていないパケットについては、これらのパケットを中継転送してきたネットワークとの境界に設置されるｉＭＬＢＲ１１にて、前記所定ビットの認証フラグをリセット(“０”)するようにしてもよい。これによって、ＭＬＢＲ未導入のプロバイダのネットワークから送られてきたパケットや、ｅＭＬＢＲ１２をバイパスしてインターネットに流入させようとしたパケットは、これを受信したｉＭＬＢＲ１１や、パケットの送信先ノードを収容するｉＭＬＢＲ１１やｅＭＬＢＲ１２でパケットが認証を受けたノードまたはエンティティから送信されたものか否かを確認することが可能になり、認証フラグが“０”のパケットについては検疫サイトに配送し、クラッキング意図パケットか否かを詳細に検査する、あるいはその扱い(廃棄するか詳細な検疫検査を行うなど)を受信者に委ねることが可能になる。なお、認証フラグが“１”のパケットは、認証を受けたノードまたはエンティティから送信されたことを示すものであって、同パケットがマルウェアに感染していない、すなわち安全性が保証されていることを意味するものではない。

【産業上の利用可能性】

【０１４３】

本発明は情報通信産業に適用することができる。

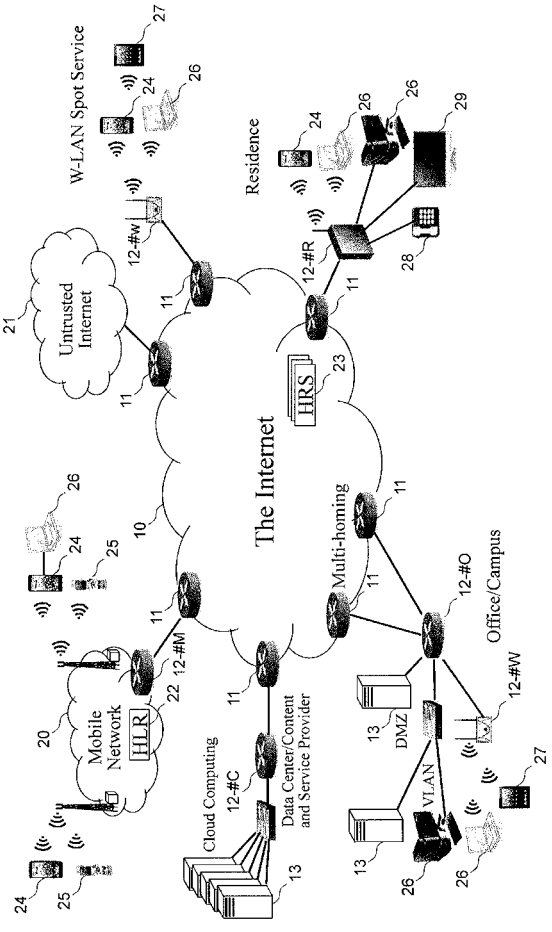
【符号の説明】

【０１４４】

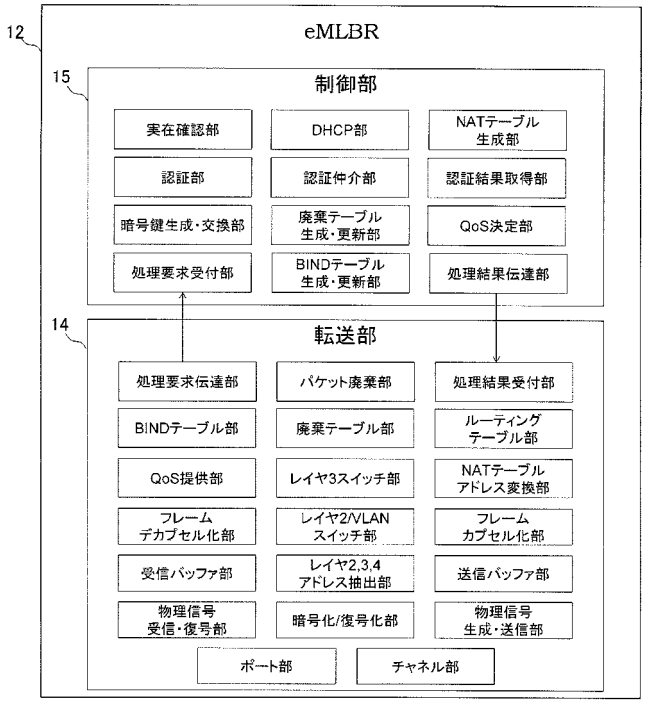
１０：インターネット
１１：ｉＭＬＢＲ
１２：ｅＭＬＢＲ
１３：サーバー
１４：転送部（Ｏｐｅｎ Ｆｌｏｗ Ｓｗｉｔｃｈ）
１５：制御部（Ｏｐｅｎ Ｆｌｏｗ Ｃｏｎｔｒｏｌｌｅｒ）
２０：Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ
２１：Ｕｎｔｒｕｓｔｅｄ Ｉｎｔｅｒｎｅｔ
２２：ＨＬＲ

２３：ＨＲＳ
２４：スマートフォン
２５：携帯電話
２６：ＰＣ
２７：タブレットＰＣ
２８：電話器
２９：デジタルテレビ
３０：ホスト
３１：検疫サーバー
４０：ＲｅＮ（Ｒｅｑｕｅｓｔ　Ｎｏｄｅ）
４１：ホスト／ＲｅＮ
４２：ＤｅＮ（Ｄｅｌｉｖｅｒ　Ｎｏｄｅ）
４３：ＳｈＮ（Ｓｈａｒｅ　Ｎｏｄｅ）

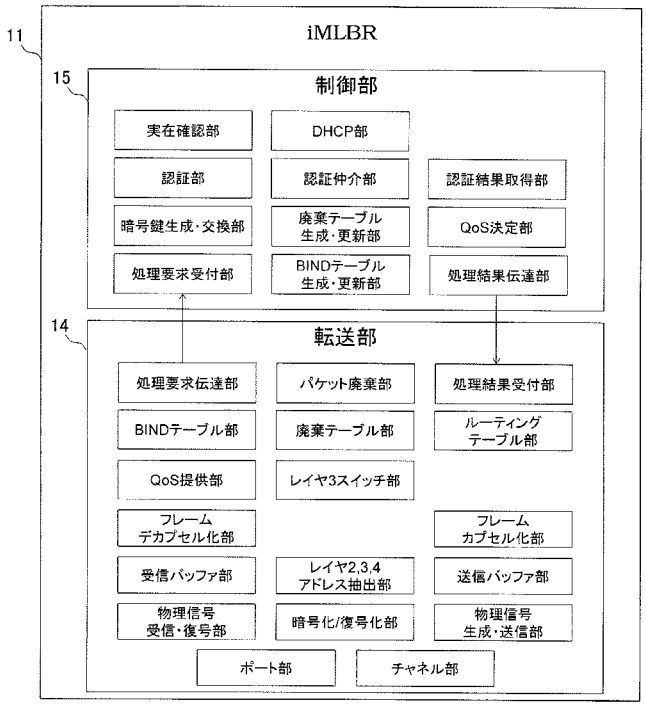
【図１】



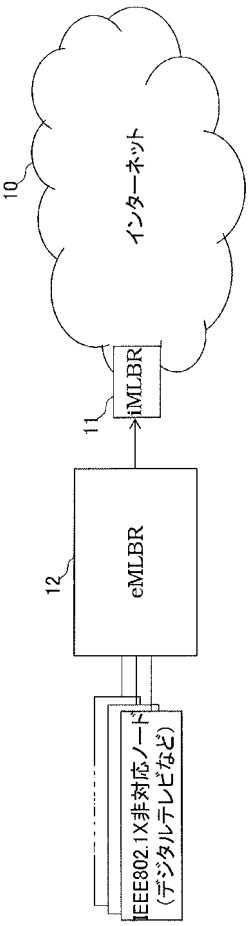

【図２】



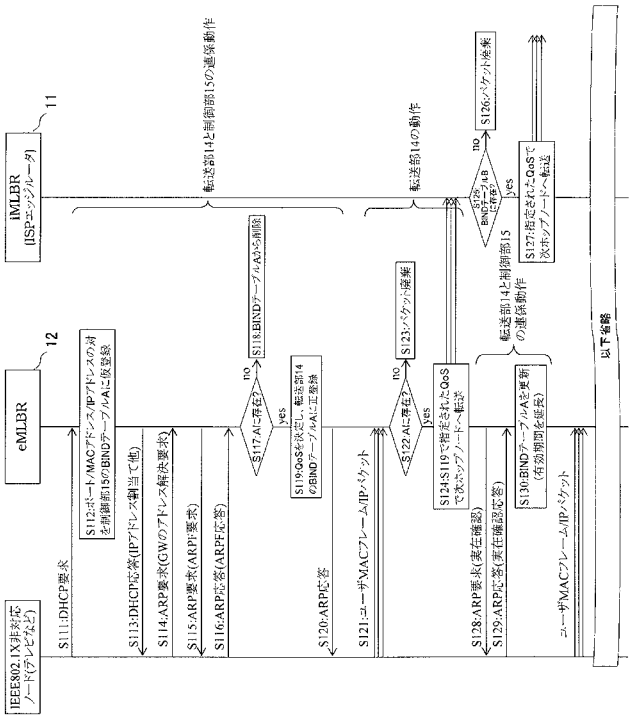
【図３】


11
iMLBR
15
制御部
実在確認部
DHCP部
認証部
認証仲介部
認証結果取得部
暗号鍵生成・交換部
廃棄テーブル生成・更新部
QoS決定部
処理要求受付部
BINDテーブル生成・更新部
処理結果伝達部
14
転送部
処理要求伝達部
パケット廃棄部
処理結果受付部
BINDテーブル部
廃棄テーブル部
ルーティングテーブル部
QoS提供部
レイヤ3スイッチ部
フレームデカプセル化部
フレームカプセル化部
受信バッファ部
レイヤ2,3,4アドレス抽出部
送信バッファ部
物理信号受信・復号部
暗号化/復号化部
物理信号生成・送信部
ポート部
チャネル部

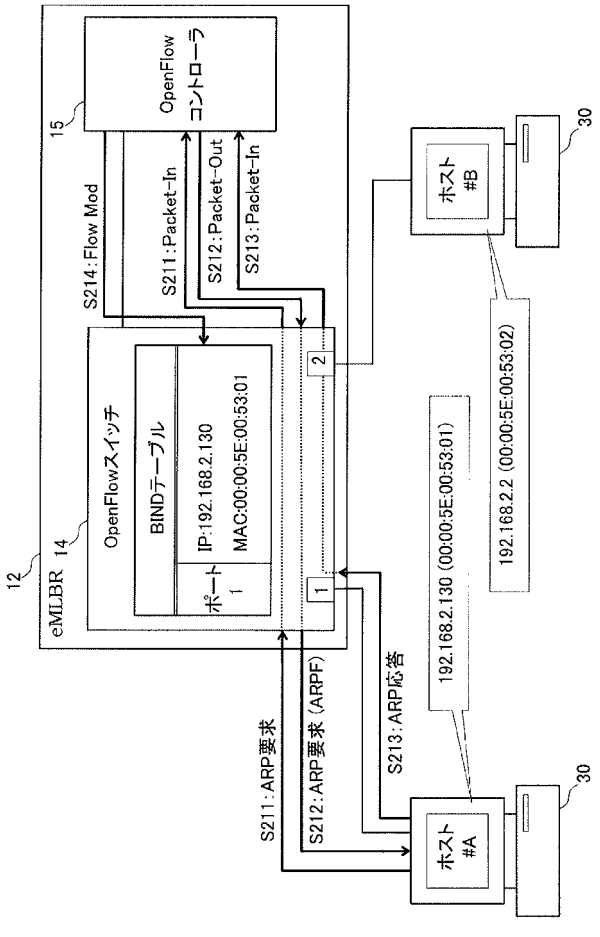
【図４】


10
インターネット
11
iMLBR
12
eMLBR
IEEE802.1X非対応ノード
(デジタルテレビなど)

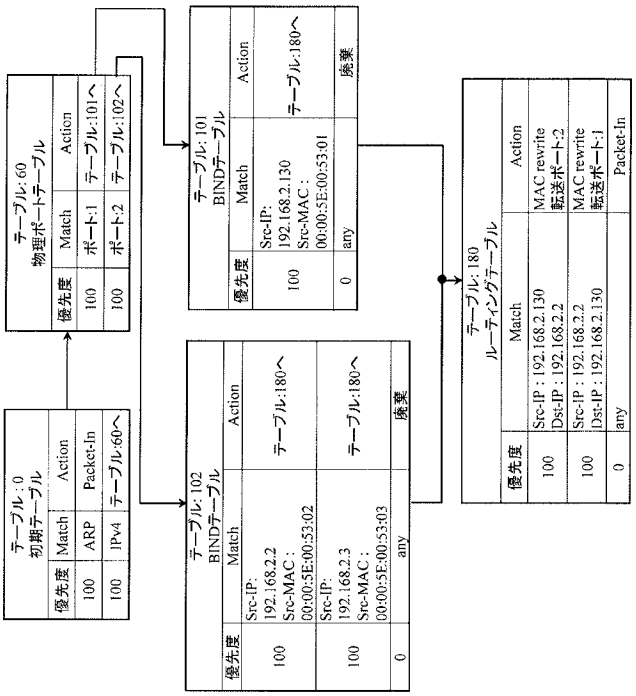
【図５】


IEEE802.1X非対応ノード(テレビなど)
11
iMLBR
(ISPエッジルータ)
12
eMLBR
転送部14と制御部15の連係動作
転送部14の動作
S111:DHCP要求
S112:ポート/MACアドレス/IPアドレスの対を制御部15のBINDテーブルAに仮登録
S113:DHCP応答(IPアドレス割当て他)
S114:ARP要求(GWのアドレス解決要求)
S115:ARP要求(ARPF要求)
S116:ARP応答(ARPF応答)
S117:Aに存在?
S118:BINDテーブルAから削除
S119:QoSを決定し、転送部14のBINDテーブルAに正登録
S120:ARP応答
S121:ユーザMACフレーム/IPパケット
S122:Aに存在?
S123:パケット廃棄
S124:S119で指定されたQoSで次ホップノードへ転送
S125:BINDテーブルB(IPアドレス)
S126:パケット廃棄
S127:指定されたQoSで次ホップノードへ転送
転送部14と制御部15の連係動作
S128:ARP要求(実在確認)
S129:ARP応答(実在確認応答)
S130:BINDテーブルAを更新(有効期間を延長)
ユーザMACフレーム/IPパケット
以下省略

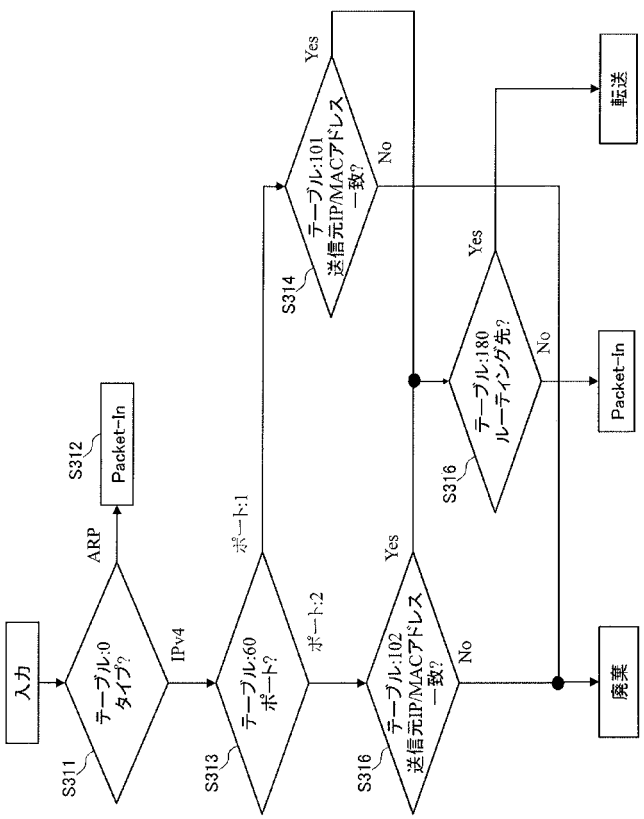
【図６】


12
eMLBR
14
OpenFlowスイッチ
BINDテーブル
ポート1
IP:192.168.2.130
MAC:00:00:5E:00:53:01
15
OpenFlow
コントローラ
S214:Flow Mod
S211:Packet-In
S212:Packet-Out
S213:Packet-In
1
2
ホスト#B
30
192.168.2.2 (00:00:5E:00:53:02)
192.168.2.130 (00:00:5E:00:53:01)
S211:ARP要求
S212:ARP要求(ARPF)
S213:ARP応答
ホスト#A
30

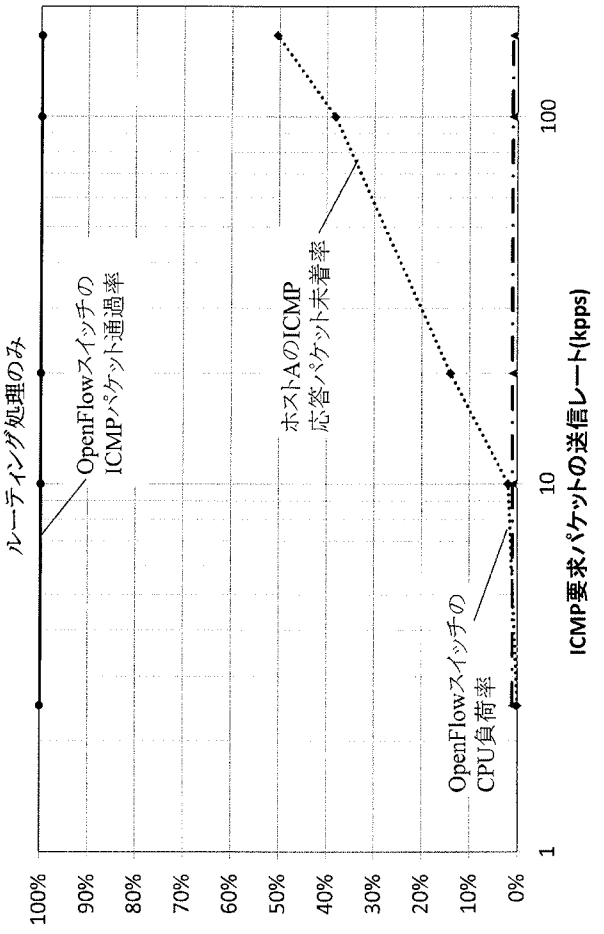
【図７】


テーブル:0
初期テーブル
優先度 Match Action
100 ARP Packet-In
100 IPv4 テーブル:60へ
テーブル:60
物理ポートテーブル
優先度 Match Action
100 ポート:1 テーブル:101へ
100 ポート:2 テーブル:102へ
テーブル:101
BINDテーブル
優先度 Match Action
100 Src-IP: 192.168.2.130 Src-MAC: 00:00:5E:00:53:01 テーブル:180へ
0 any 廃棄
テーブル:102
BINDテーブル
優先度 Match Action
100 Src-IP: 192.168.2.2 Src-MAC: 00:00:5E:00:53:02 テーブル:180へ
100 Src-IP: 192.168.2.3 Src-MAC: 00:00:5E:00:53:03 テーブル:180へ
0 any 廃棄
テーブル:180
ルーティングテーブル
優先度 Match Action
100 Src-IP : 192.168.2.130 Dst-IP : 192.168.2.2 MAC rewrite 転送ポート:2
100 Src-IP : 192.168.2.2 Dst-IP : 192.168.2.130 MAC rewrite 転送ポート:1
0 any Packet-In

【図８】


入力
S311
テーブル:0 タイプ?
ARP
S312
Packet-In
IPv4
S313
テーブル:60 ポート?
ポート:1
ポート:2
S314
テーブル:101 送信元IP/MACアドレス 一致?
Yes
No
S316
テーブル:102 送信元IP/MACアドレス 一致?
Yes
No
S316
テーブル:180 ルーティング先?
Yes
No
廃棄
Packet-In
転送

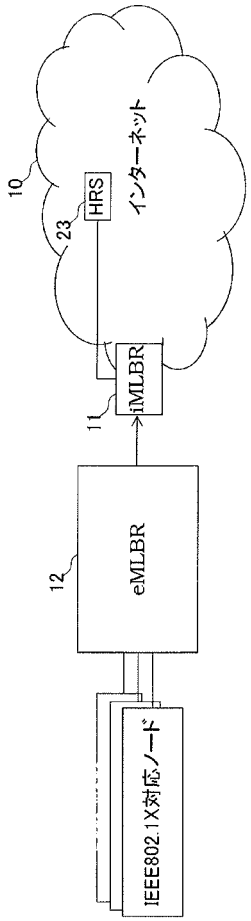
【図９】


ルーティング処理のみ
OpenFlowスイッチの ICMPパケット通過率
ホストAのICMP 応答パケット未着率
OpenFlowスイッチの CPU負荷率
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
1
10
100
ICMP要求パケットの送信レート(kpps)

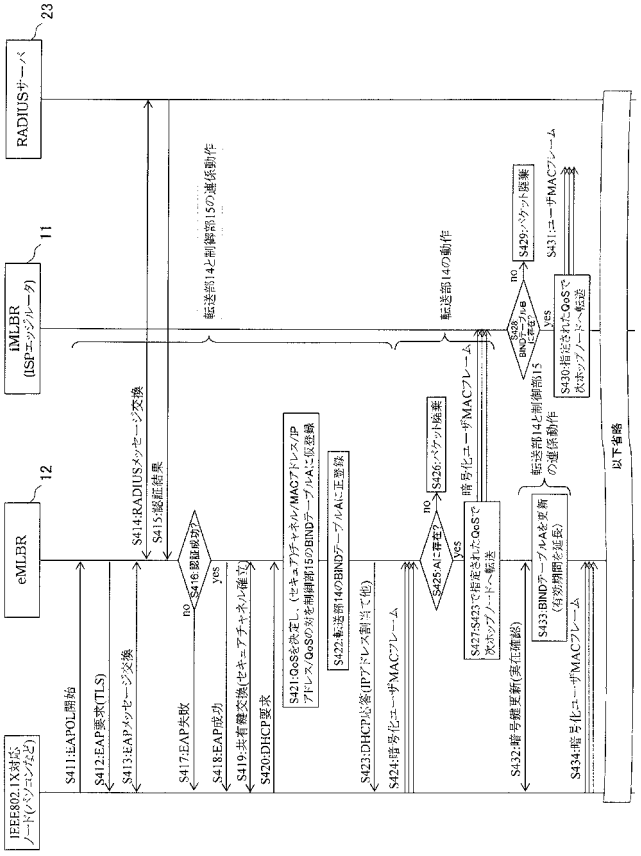
【図１０】


アドレス詐称検査+ルーティング処理
OpenFlowスイッチの ICMPパケット通過率
ホストAのICMP 応答パケット未着率
OpenFlowスイッチの CPU負荷率
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
1
10
100
ICMP要求パケットの送信レート(kpps)

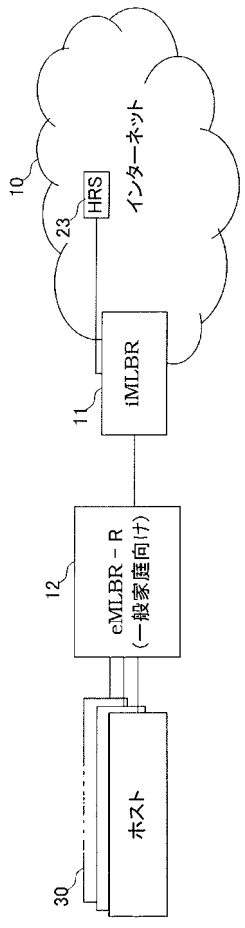
【図１１】



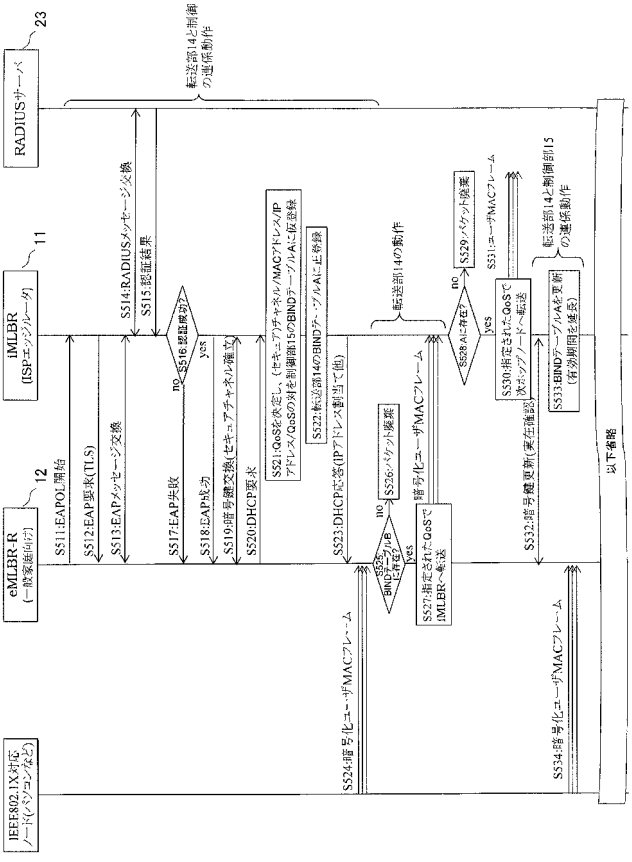

【図１２】



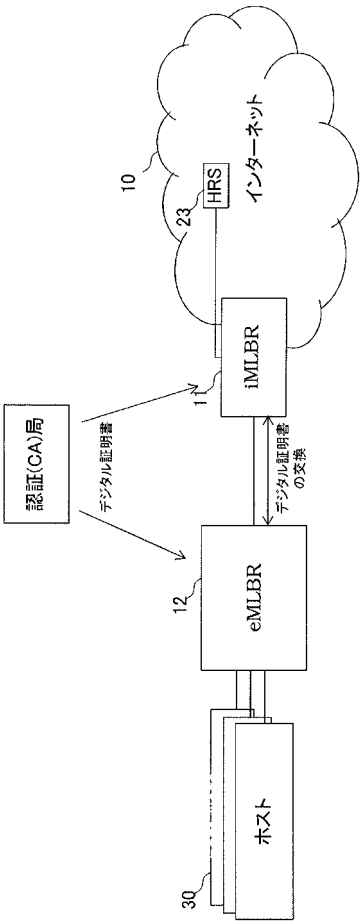

【図１３】



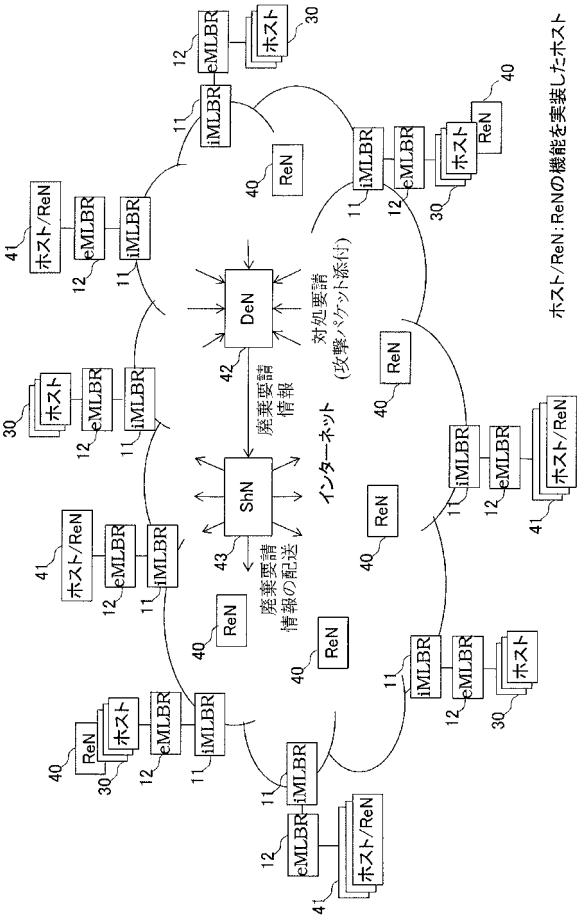

【図１４】



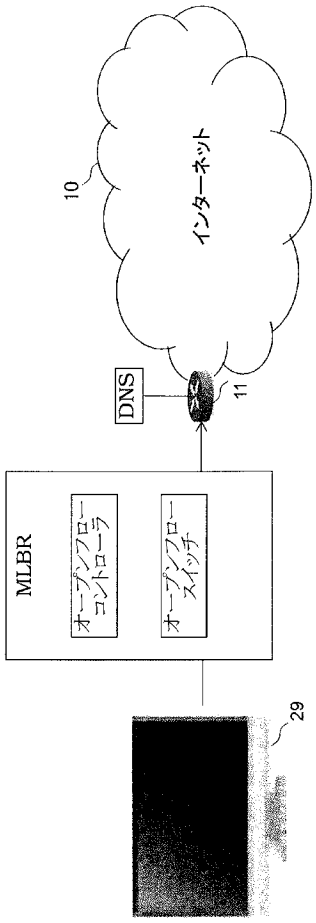
【図１５】



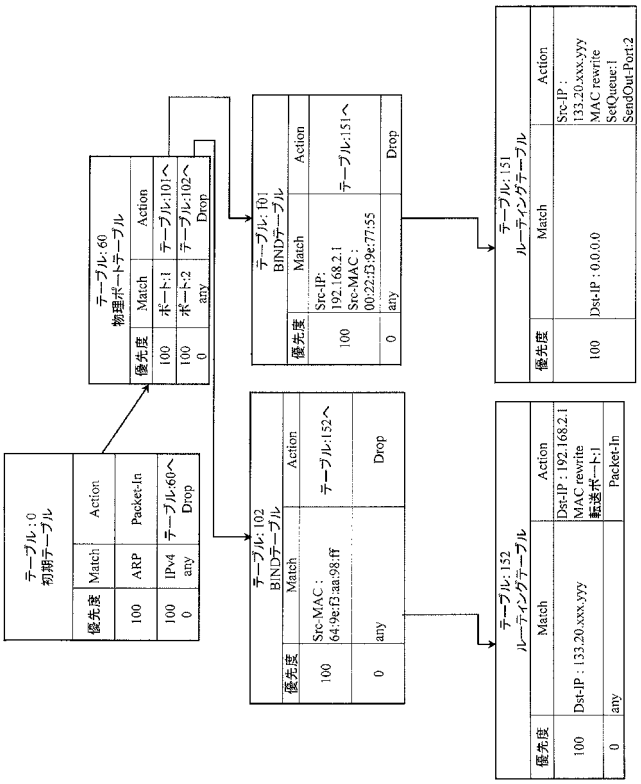

【図１６】



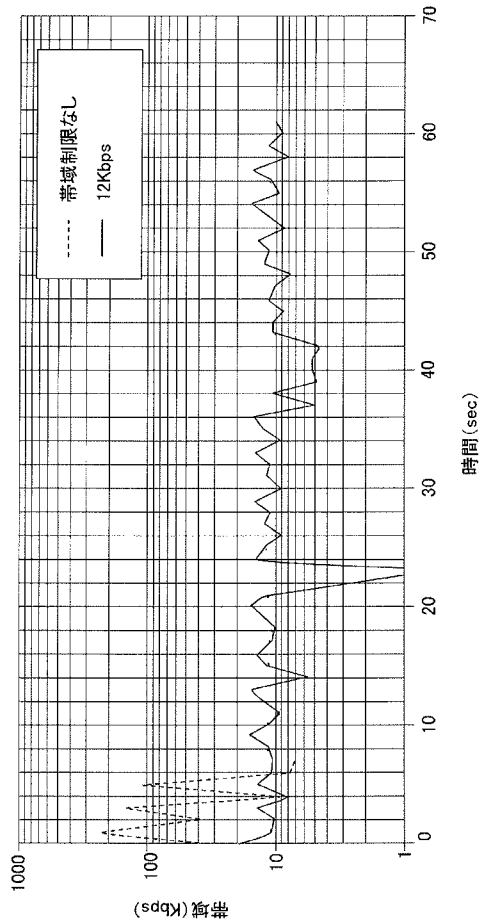

【図１７】



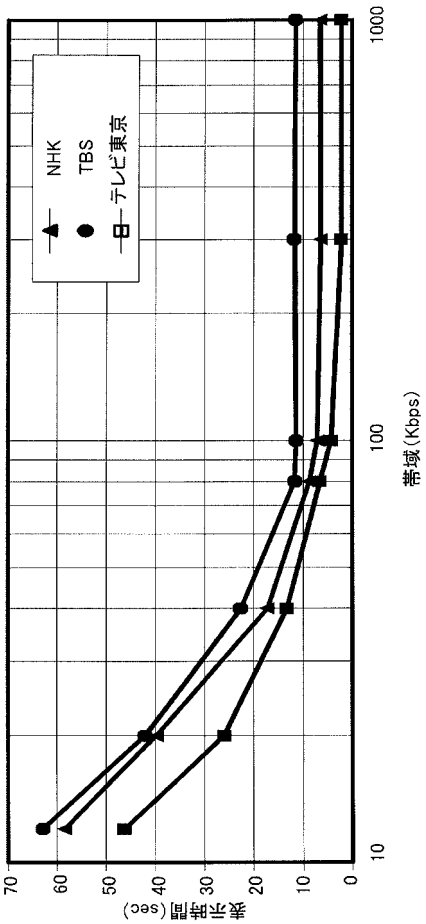

【図１８】



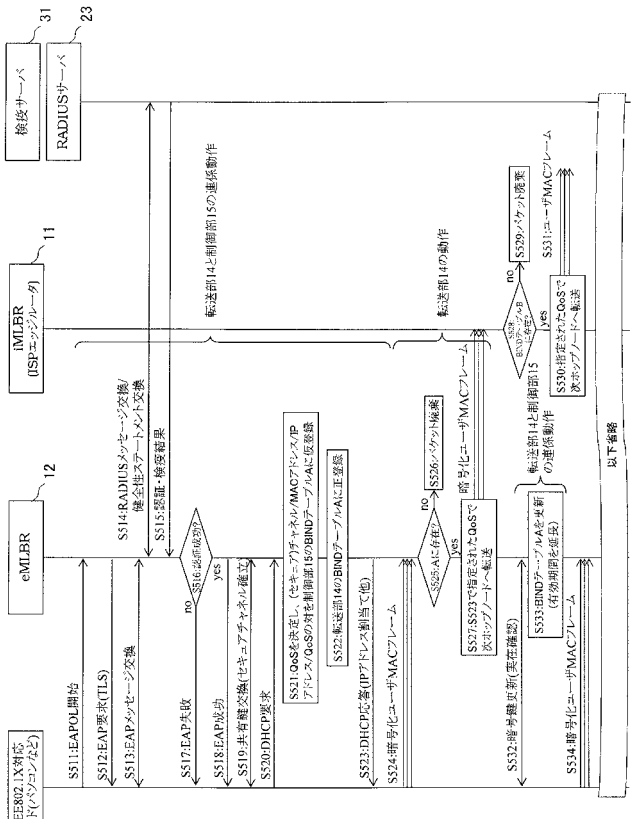
【図１９】




【図２０】

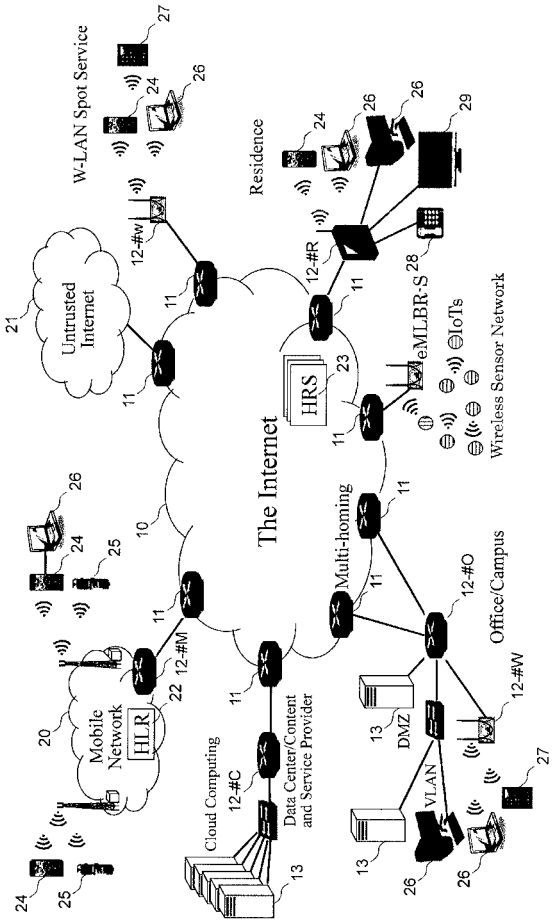



【図２１】




【図２２】

【図２３】


W-LAN Spot Service
Residence
Untrusted Internet
The Internet
HRS
eMLBR·S
IoTs
Wireless Sensor Network
Multi-homing
Office/Campus
Mobile Network
HLR
Cloud Computing
Data Center/Content and Service Provider
DMZ
VLAN
12-#w
12-#R
12-#O
12-#W
12-#M
12-#C

【国際調査報告】

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2015/050618

A. CLASSIFICATION OF SUBJECT MATTER
*H04L12/66*(2006.01)i, *H04L12/46*(2006.01)i, *H04L12/717*(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/66, H04L12/46, H04L12/717

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2015
Kokai Jitsuyo Shinan Koho 1971-2015 Toroku Jitsuyo Shinan Koho 1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y<br>A | WO 2012/153913 A1 (Estsoft Corp.),<br>15 November 2012 (15.11.2012),<br>fig. 1 to 5<br>& JP 2014-517593 A & US 2014/0325651 A | 1-4,6-11<br>5 |
| Y<br>A | JP 2012-175482 A (Fujitsu Ltd.),<br>10 September 2012 (10.09.2012),<br>paragraphs [0008] to [0009]<br>(Family: none) | 1-4,6-11<br>5 |
| Y | WO 2011/081104 A1 (NEC Corp.),<br>07 July 2011 (07.07.2011),<br>fig. 1, 2<br>& US 2011/0314517 A1 | 3 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 07 April 2015 (07.04.15) | 21 April 2015 (21.04.15) |
| Name and mailing address of the ISA/<br>Japan Patent Office<br>3-4-3,Kasumigaseki,Chiyoda-ku,<br>Tokyo 100-8915,Japan | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (July 2009)

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2015/050618

Claim 3 is not sufficiently supported by the description.
In particular, which statement in the description "a control unit which transmits the above-mentioned multilayer binding table to the above-mentioned transfer unit of another packet transfer device" corresponds to is unclear.

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１５／０５０６１８

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. H04L12/66(2006.01)i, H04L12/46(2006.01)i, H04L12/717(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. H04L12/66, H04L12/46, H04L12/717

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|---|---|
| 日本国実用新案公報 | １９２２－１９９６年 |
| 日本国公開実用新案公報 | １９７１－２０１５年 |
| 日本国実用新案登録公報 | １９９６－２０１５年 |
| 日本国登録実用新案公報 | １９９４－２０１５年 |

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求項の番号 |
|---|---|---|
| Y | WO 2012/153913 A1（イーストソフト　コーポレーション）2012.11.15, 図１－５ | 1-4,6-11 |
| A | & JP 2014-517593 A & US 2014/0325651 A | 5 |
| Y | JP 2012-175482 A（富士通株式会社）2012.09.10, 段落［０００８］－［０００９］ | 1-4,6-11 |
| A | （ファミリーなし） | 5 |

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| 国際調査を完了した日 | 国際調査報告の発送日 |
|---|---|
| ０７．０４．２０１５ | ２１．０４．２０１５ |

| 国際調査機関の名称及びあて先 | 特許庁審査官（権限のある職員） | | |
|---|---|---|---|
| 日本国特許庁（ＩＳＡ／ＪＰ）<br>郵便番号１００－８９１５<br>東京都千代田区霞が関三丁目４番３号 | 上田　翔太 | ５Ｘ | ４４４９ |
| | 電話番号　０３－３５８１－１１０１　内線　３５９６ | | |

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００９年７月）

| 国際調査報告 | 国際出願番号 PCT／JP2015／050618 |
|---|---|

C（続き）． 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求項の番号 |
|---|---|---|
| Y | WO 2011/081104 A1（日本電気株式会社）2011.07.07,<br>図１，２<br>& US 2011/0314517 A1 | 3 |

請求項３は、明細書によって十分に裏付けされていない。
特に、「前記マルチレイヤ・バインディングテーブルを他のパケット転送装置に備わる前記転送部に伝達する制御部」が明細書のどの記載に対応するのか不明である。

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

特許法第３０条第２項適用申請有り　平成２５年度卒業研究・開発型プロジェクト梗概集（ＣＤ－ＲＯＭ）　平成２６年1月１６日

（特許庁注：以下のものは登録商標）
１．ＪＡＶＡ

(72)発明者　八槇　博史
東京都足立区千住旭町５番　学校法人東京電機大学内
(72)発明者　佐々木　良一
東京都足立区千住旭町５番　学校法人東京電機大学内
(72)発明者　上野　洋一郎
東京都足立区千住旭町５番　学校法人東京電機大学内
(72)発明者　佐野　香
東京都足立区千住旭町５番　学校法人東京電機大学内
Ｆターム(参考) 5K030 GA15 HD03 HD06 HD10 KX24 LB07 LC15 LC18
5K033 AA05 CB11 DA06 DB18 EC04

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。