(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4319609号
(P4319609)
(45)発行日　平成21年8月26日(2009.8.26)　(24)登録日　平成21年6月5日(2009.6.5)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66　B

請求項の数 7　(全 14 頁)

(21)出願番号　特願2004-325249 (P2004-325249)
(22)出願日　平成16年11月9日 (2004.11.9)
(65)公開番号　特開2006-135885 (P2006-135885A)
(43)公開日　平成18年5月25日 (2006.5.25)
審査請求日　平成19年6月15日 (2007.6.15)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　北澤　繁樹
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

審査官　玉木　宏治

最終頁に続く

(54)【発明の名称】攻撃経路解析装置及び攻撃経路解析方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
複数の中継装置を介して接続された複数のネットワークを監視対象とし、
いずれかのネットワークに対する攻撃パケットが検知された場合に、攻撃パケットの送信に用いられた攻撃経路の解析を行う攻撃経路解析装置であって、
中継装置間の接続関係を示す中継装置情報を記憶する中継装置情報記憶部と、
各ネットワークを流通するパケットを収集して得られた各パケットのヘッダ情報を各ネットワークより受信する流通パケットヘッダ情報受信部と、
前記流通パケットヘッダ情報受信部により受信された各ネットワークからのヘッダ情報を記憶するヘッダ情報記憶部と、
いずれかのネットワークに対する攻撃パケットが検知された場合に、検知された攻撃パケットのヘッダ情報を受信する攻撃パケットヘッダ情報受信部と、
前記中継装置情報記憶部に記憶されている中継装置情報と、前記ヘッダ情報記憶部に記憶されている各ネットワークからのヘッダ情報と、前記攻撃パケットヘッダ情報受信部により受信された攻撃パケットのヘッダ情報とに基づき、攻撃パケットの中継を行った可能性のある中継装置を導出し、攻撃経路を解析する攻撃経路解析部とを有することを特徴とする攻撃経路解析装置。
【請求項２】
前記中継装置情報記憶部は、
各中継装置のＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスが示され

た中継装置情報を記憶し、
前記ヘッダ情報記憶部は、
送信先ＭＡＣアドレス、送信元ＭＡＣアドレス、及びＴＴＬ（Ｔｉｍｅ　ｔｏ　Ｌｉｖｅ）データを含む各ネットワークからのヘッダ情報を記憶し、
前記攻撃パケットヘッダ情報受信部は、
送信先ＭＡＣアドレス、送信元ＭＡＣアドレス、及びＴＴＬデータを含む攻撃パケットのヘッダ情報を受信し、
前記攻撃経路解析部は、
送信先ＭＡＣアドレス、送信元ＭＡＣアドレス、及びＴＴＬデータ以外のデータが、攻撃パケットのヘッダ情報の送信先ＭＡＣアドレス、送信元ＭＡＣアドレス、及びＴＴＬデータ以外のデータと一致するヘッダ情報を前記ヘッダ情報記憶部に記憶されているヘッダ情報の中から抽出し、抽出したヘッダ情報の送信先ＭＡＣアドレス及びＴＴＬデータと、攻撃パケットのヘッダ情報の送信元ＭＡＣアドレス及びＴＴＬデータと、中継装置情報に示された各中継装置のＭＡＣアドレス及び中継装置間の接続関係とに基づき、攻撃パケットの中継を行った可能性のある中継装置を導出し、攻撃経路を解析することを特徴とする請求項１に記載の攻撃経路解析装置。
【請求項３】
前記中継装置情報記憶部は、
中継装置間の接続関係として、二つの中継装置ごとに、送信先中継装置及び送信元中継装置を示す中継装置情報を記憶していることを特徴とする請求項１に記載の攻撃経路解析装置。
【請求項４】
前記中継装置情報記憶部は、
中継装置間の接続関係として、監視対象のネットワーク上に存在する中継経路ごとに、それぞれの中継経路に含まれる中継装置及び中継の順序を示す中継装置情報を記憶していることを特徴とする請求項１に記載の攻撃経路解析装置。
【請求項５】
前記攻撃経路解析装置は、更に、
中継装置間の接続関係に変更が生じた際に、変更後の接続関係を示す中継装置情報をいずれかの中継装置から受信する中継装置情報受信部を有し、
前記中継装置情報記憶部は、
前記中継装置情報受信部により新たな中継装置情報が受信された際に、新たな中継装置情報を用いて中継装置情報の更新を行うことを特徴とする請求項１に記載の攻撃経路解析装置。
【請求項６】
複数の中継装置を介して接続された複数のネットワークを監視対象とし、
中継装置間の接続関係を示す中継装置情報を管理し、いずれかのネットワークに対する攻撃パケットが検知された場合に、攻撃パケットの送信に用いられた攻撃経路の解析を行う攻撃経路解析方法であって、
各ネットワークを流通するパケットを収集して得られた各パケットのヘッダ情報を各ネットワークより受信する流通パケットヘッダ情報受信ステップと、
前記流通パケットヘッダ情報受信ステップにより受信された各ネットワークからのヘッダ情報を記憶するヘッダ情報記憶ステップと、
いずれかのネットワークに対する攻撃パケットが検知された場合に、検知された攻撃パケットのヘッダ情報を受信する攻撃パケットヘッダ情報受信ステップと、
管理している中継装置情報と、前記ヘッダ情報記憶ステップにより記憶された各ネットワークからのヘッダ情報と、攻撃パケットヘッダ情報受信ステップにより受信された攻撃パケットのヘッダ情報とに基づき、攻撃パケットの中継を行った可能性のある中継装置を導出し、攻撃経路を解析する攻撃経路解析ステップとを有することを特徴とする攻撃経路解析方法。

【請求項７】
複数の中継装置を介して接続された複数のネットワークを監視対象とし、
中継装置間の接続関係を示す中継装置情報をコンピュータに管理させるとともに、いずれかのネットワークに対する攻撃パケットが検知された場合に、攻撃パケットの送信に用いられた攻撃経路の解析をコンピュータに実行させるプログラムであって、
各ネットワークを流通するパケットを収集して得られた各パケットのヘッダ情報を各ネットワークより受信する流通パケットヘッダ情報受信処理と、
前記流通パケットヘッダ情報受信処理により受信された各ネットワークからのヘッダ情報を記憶するヘッダ情報記憶処理と、
いずれかのネットワークに対する攻撃パケットが検知された場合に、検知された攻撃パケットのヘッダ情報を受信する攻撃パケットヘッダ情報受信処理と、
管理している中継装置情報と、前記ヘッダ情報記憶処理により記憶された各ネットワークからのヘッダ情報と、前記攻撃パケットヘッダ情報受信処理により受信された攻撃パケットのヘッダ情報とに基づき、攻撃パケットの中継を行った可能性のある中継装置を導出し、攻撃経路を解析する攻撃経路解析処理とをコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークに対する攻撃パケットが検知された場合に、攻撃パケットの侵入経路を解析する侵入経路解析技術に関する。
【背景技術】
【０００２】
従来技術（特許文献１）では、図６に示すように、監視対象の各サブネットワークにパケット収集装置を配置するとともに、各ホストにホスト内部情報収集装置を設けている。パケット収集装置はそれぞれが接続されているサブネットワークを流れるパケットを捕捉し、パケットヘッダの内容をヘッダ情報として侵入経路解析装置２５１に通知する。また、ホスト内部情報収集装置はホスト内のプロセス管理情報を収集し、侵入経路解析装置２５１に通知する。侵入経路解析装置２５１では、パケット収集装置ならびにホスト内部情報収集装置からそれぞれ収集したヘッダ情報及びプロセス管理情報を、データベースへ格納しておく。また、侵入検知装置にて攻撃パケットの侵入を検知した場合には、侵入経路解析装置２５１において、３つの異なる解析手段（ホストレベル解析、ルータレベル解析、ホスト内部解析）をスケジューリングアルゴリズムによってスケジューリングすることにより、送信元ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスの詐称や踏み台ホストといった、真の攻撃元端末を隠蔽するような手段を用いた場合であっても、その侵入経路の特定を可能としている。
ルータレベル解析では、ヘッダ情報をキーとしたデータベース検索により抽出した複数の攻撃のパケットを、ＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）データによってソートをした後に、パケットの送受信ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスとネットワーク上のルータのＭＡＣアドレスを関連付けることで、パケットの送出元からあて先までの経路を特定する。これにより、送信元ＩＰアドレスを詐称されていた場合であっても攻撃の経路を特定可能である。
また、ホスト内部解析では、パケットを送出したプロセスの親子関係を辿り、親プロセスの中にリモートの端末と通信した履歴を持つものがあるかどうかを解析する。リモート端末との通信の履歴があった場合には、ホストレベル解析ならびにルータレベル追跡によって、リモートの端末までの経路を特定する。これにより、踏み台を含む侵入経路を追跡可能としている。
【０００３】
また、図７は、従来技術（特許文献２）の構成を表している。特許文献２では、パケットプリンティング装置３１１～３１３をネットワークの要所に設置して、パケットプリン

ティング装置が接続されているネットワークを通過するパケットの識別情報（パケットのハッシュ値やパケットの一部）（図７では、符号３２１～３２３で示している）をパケットプリンティング装置に保存しておく。侵入パケット検知装置（図７では図示していない）で攻撃パケットの侵入を検知した場合、その攻撃パケットの識別情報を生成し、各パケットプリンティング装置に、攻撃パケットの識別情報と一致するデータが保存されているか問い合わせを行うことにより、侵入経路を特定している。問い合わせの方法として、（１）全てのパケットプリンティング装置へ問い合わせる方式、（２）管理マネージャが、経路を辿りながら、逐次問い合わせる方式、（３）パケットプリンティング装置同士が、自律的に問い合わせを行う方式がある。

【０００４】

また、図８は、従来技術（特許文献３）の概要を表している。特許文献３では、認証サーバである一定以上のリソース消費を検知した場合に、ＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃と判断し、ＤｏＳ攻撃パケットのソースアドレスを持つパケットを、ＤｏＳ攻撃経路を遡りながら、ネットワーク上のルータでフィルタリングすることにより、ＤｏＳ攻撃を無効化する。ただし、ソースアドレスが詐称された場合は、正当なユーザの通信をフィルタリングしてしまうという問題点があり、これに対しては、ネットワーク・イングレス・フィルタリング技術（ＲＦＣ２８２７）と組み合わせることよって、回避するとしている。ネットワーク・イングレス・フィルタリング技術とは、ルータが他の装置からパケットを受信した際に、ソースアドレスが通常ありえないアドレス（プライベートＩＰアドレスや、ルータが接続されているサブネットに直接接続されている端末からサブネット以外のソースアドレス）であった場合に、ルータはそのパケットを破棄するというフィルタリング技術である。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

上述したように、従来技術（特許文献１）におけるルータレベル解析を行うためには、解析対象であるパケットを収集するために、パケット収集装置をネットワークの各サブネット上に設置する必要がある。しかしながら、ルータ間（例えば、ルータ２４１とルータ２４２の間）に配置されたパケット収集装置（例えば、パケット収集装置２３１）はルータ間に流れるパケットを収集するため、バックボーンネットワークのような広帯域ネットワークの場合は、パケット収集装置から集積されるパケットログ件数が多くなる。このため、侵入経路解析に必要な計算量が多くなり侵入経路解析に長時間を要するとの問題がある。また、集積するパケットログ件数が多いため、ログの転送処理やデータベースへの格納処理にかかるコスト、ならびに、ログを保存しておくための領域を多く必要とする。これらにより、監視対象ネットワークの規模が大きくなった場合には、対応できなくなってしまうという問題点がある。また、ルータレベル解析に関連した経路上のパケットが１つでも欠けており、またＩＰアドレスを詐称されていた場合には、経路を特定できないといった問題点もある。

【０００６】

特許文献２におけるパケットプリンティング装置は、サブネットごとに設置する必要はない。しかしながら、侵入経路を特定するために設置するパケットプリンティング装置の数を減らした場合に、攻撃パケットとパケット識別情報が偶然一致するパケットを保持しているパケットプリンティング装置があった場合には、誤った経路が導き出されてしまうという問題点がある。

【０００７】

また、特許文献３では、ネットワーク・イングレス・フィルタリング技術を回避するようなＩＰアドレスの詐称（同一サブネットの他の端末のＩＰアドレスによる詐称など）も可能であり、その場合には、攻撃経路を遡った正確なフィルタリングを行うことができないという問題点が残る。

【０００８】

この発明は上記のような問題点を解決するためになされたもので、ルータレベル解析で必要とする収集パケットの総量の削減および攻撃経路の特定性能の向上を目的とする。
【特許文献１】特開２００３－２５８９１０号公報
【特許文献２】特開２００４－１４５６８７号公報
【特許文献３】特開２００３－２９８９１５号公報
【課題を解決するための手段】
【０００９】
本発明に係る攻撃経路解析装置は、
複数の中継装置を介して接続された複数のネットワークを監視対象とし、
いずれかのネットワークに対する攻撃パケットが検知された場合に、攻撃パケットの送信に用いられた攻撃経路の解析を行う攻撃経路解析装置であって、
中継装置間の接続関係を示す中継装置情報を記憶する中継装置情報記憶部と、
各ネットワークを流通するパケットを収集して得られた各パケットのヘッダ情報を各ネットワークより受信する流通パケットヘッダ情報受信部と、
前記流通パケットヘッダ情報受信部により受信された各ネットワークからのヘッダ情報を記憶するヘッダ情報記憶部と、
いずれかのネットワークに対する攻撃パケットが検知された場合に、検知された攻撃パケットのヘッダ情報を受信する攻撃パケットヘッダ情報受信部と、
前記中継装置情報記憶部に記憶されている中継装置情報と、前記ヘッダ情報記憶部に記憶されている各ネットワークからのヘッダ情報と、攻撃パケットヘッダ情報受信部により受信された攻撃パケットのヘッダ情報とに基づき、攻撃パケットの中継を行った中継装置を特定し、攻撃経路を解析する攻撃経路解析部とを有することを特徴とする。
【発明の効果】
【００１０】
本発明によれば、中継装置間の接続関係を示す中継装置情報を用いて攻撃経路を解析するため、パケットの収集量を減らすことができ、これにより、攻撃経路解析に必要な計算量を削減することができ、より高速に侵入経路解析を行うことができる。また、パケットの収集量を減らすことにより、攻撃経路解析に使用するデータの格納や保存にかかるコストを抑えることも可能である。また、一定のパケットが欠けていた場合であっても、正確に攻撃経路を特定することができる。
【発明を実施するための最良の形態】
【００１１】
実施の形態１.
図１は、本実施の形態に係るシステム構成例を示す構成図である。図１において１０１はインターネットなどの広域ネットワークを表し、ルータ１２１～１２４は、異なるサブネットワーク間を接続して通信を中継する。ルータのそれぞれは、中継装置に相当する。ルータ１２１～１２４により接続されている各サブネットワーク（破線で表示）は、監視対象のネットワークに相当する。
侵入検知装置１３１は、接続されているサブネットワーク上を常時監視して攻撃パケットを検知した場合には、検知した攻撃の内容および検知したパケットのヘッダ情報を含む情報をアラートとして、侵入経路解析装置１７１へ通知する。アラートとして通知する内容には、パケット検知日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の送信元ＭＡＣアドレス、送信先ＭＡＣアドレス、ＩＣＭＰプロトコルヘッダのＴｙｐｅ、Ｃｏｄｅ、Ｃｈｅｃｋｓｕｍ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ、ＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）、Ｐｒｏｔｏｃｏｌ、発信元ＩＰアドレス、宛先ＩＰアドレス、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、Ｃｈｅｃｋｓｕｍ、ＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒなどの情報が含まれる。
【００１２】
パケット収集装置１４１～１４３では、接続された各サブネットワーク上を流通するパ

ケットを決められた収集ルールにしたがって、常時収集し、ヘッダの内容をヘッダ情報として記憶領域に記録する。記録するヘッダ情報には、パケットを識別するための情報が含まれる。例えば、侵入検知装置１３１がアラートとして侵入経路解析装置１７１に通知する内容と同じでもよい。具体的には、パケット取得日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の送信元ＭＡＣアドレス、送信先ＭＡＣアドレス、ＩＣＭＰプロトコルヘッダのＴｙｐｅ、Ｃｏｄｅ、Ｃｈｅｃｋｓｕｍ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ、ＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）、Ｐｒｏｔｏｃｏｌ、発信元ＩＰアドレス、宛先ＩＰアドレス、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、Ｃｈｅｃｋｓｕｍ、ＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒなどの情報が含まれる。

【００１３】

また、パケット収集装置１４１～１４３は、収集ルールによって、取得するパケットの種類をあらかじめ限定して収集することより、パケット情報件数を削減可能である。

たとえば、収集ルールとして、ＴＣＰ（Ｔｒａｎｃｅｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）のＳＹＮパケット、ＵＤＰ（Ｕｓｅｒ　Ｄａｔａ　Ｐｒｏｔｏｃｏｌ）パケット、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ　Ｐｒｏｔｏｃｏｌ）パケットのみを取得することとすれば、ＴＣＰにおけるＳＹＮパケット以外のパケットや、その他のプロトコルに関するパケットの分だけパケットログを削減可能である。収集ルールを特に指定しない場合は、全てのパケットを収集する。また、パケットのペイロード部分は、侵入経路の特定に直接影響を及ぼさないため、パケット取得時に破棄することでパケットログ１件あたりのデータ量を減らすこともできる。

パケット収集装置で収集したヘッダ情報は、侵入経路解析装置１７１からの記録データ送信要求発行後もしくは、定期的に侵入経路解析装置１７１へ送信される。

【００１４】

収集したパケット情報などのログの送信や管理用コマンド要求・応答などの管理通信は、別の管理用ネットワークを構築するか、もしくは、監視対象ネットワークを使用して行うことを考える。監視対象ネットワークを使用して送信する場合には、取得したパケットログが、管理通信パケットかどうかを収集ルールによって判別し、管理通信パケットであった場合には、当該パケットログを破棄する。これにより、ログの送信や管理用コマンド要求・応答などの管理通信パケットなどの余分なパケットログを取得しないようにすることにより、侵入経路解析に使用するデータの格納や保存にかかるコストを抑えられる。

【００１５】

管理通信パケットの識別の方式としては、たとえば、パケット収集装置や侵入経路解析装置など管理通信を行う装置のＩＰアドレスを送信元ＩＰアドレス、あるいは、宛先ＩＰアドレスとして持つパケットを取得しないようにすればよい。また、管理用通信パケットにそのパケットが管理用通信のためのパケットであることを示す識別子をパケットのヘッダ部分につけておくことでも識別可能である。

【００１６】

本実施の形態では、パケット収集装置１４１～１４３を最低限、ホスト１５１～１５２や利用者端末１６１～１６４など、通常の通信において、発信元または宛先となりうる端末が接続されているサブネットワークに設置する。つまり、本実施の形態に係る侵入経路解析装置１７１では、ルータ間を流通するパケットのヘッダ情報がなくても攻撃経路の解析が可能であり、このため、ルータ１２１とルータ１２２との間、ルータ１２１とルータ１２３との間、ルータ１２１とルータ１２４との間には、パケット収集装置は設置しなくてもよい。これにより、ルータ間を流通するパケットの収集を行わないので、パケット収集量を抑えることができる。

【００１７】

ホスト１５１～１５２では、何らかのネットワークサービスが提供されており、利用者端末１６１～１６３は、そのネットワークサービスを利用する端末である。ただし、ホス

ト間ならびに利用者端末間でも通信は可能とする。

【００１８】

侵入経路解析装置１７１は、パケット収集装置から受信したヘッダ情報を蓄積する。また、侵入経路解析装置１７１は、更に、ルータ情報を管理している。ルータ情報は、ルータ間の接続関係を示すルータ間接続情報と、各ルータのＭＡＣアドレスを示すルータＭＡＣアドレス情報からなる。ルータ間接続情報及びルータＭＡＣアドレス情報の詳細は後述する。

侵入検知装置１３１からアラートが通知された場合に、侵入経路解析装置１７１は、アラートに含まれている攻撃パケットのヘッダ情報を検索キーとして蓄積しているパケット収集装置からのヘッダ情報及びルータ情報を照合することにより攻撃パケットの中継を行ったルータを特定し、攻撃経路を解析する。侵入経路解析装置１７１は、攻撃経路解析装置に相当する。

【００１９】

図２は、侵入経路解析装置１７１の構成例を示す図である。

通信部は、パケット収集装置１４１～１４３、侵入検知装置１３１、及び各ルータ１２１～１２４との通信を行う。パケット収集装置１４１～１４３との間では、各パケット収集装置で収集されたパケットのヘッダ情報を受信する。侵入検知装置１３１との間では、攻撃パケットのヘッダ情報を含むアラートを受信する。また、各ルータ１２１～１２４との間では、動的にルータ間接続情報を管理する場合に、構成に変更のあったネットワークのルータからＩＰルーティングテーブルなどを受信する。通信部１７１１は、流通パケットヘッダ情報受信部、攻撃パケットヘッダ情報受信部、中継装置情報受信部に相当する。

【００２０】

アラート判断部１７１２は、通信部１７１１により受信されたデータの種類を判断し、侵入検知装置１３１からのアラートの場合は、受信されたアラートを侵入経路解析部１７１５に転送し、侵入経路解析部１７１５に侵入経路の解析を行わせる。パケット収集装置からのヘッダ情報である場合には、ヘッダ情報記憶部１７１４に転送し、ヘッダ情報記憶部１７１４にヘッダ情報の記憶を行わせる。ルータからのＩＰルーティングテーブルである場合は、ルータ情報記憶部１７１３に転送し、ルータ情報記憶部１７１３にＩＰルーティングテーブルの記憶を行わせる。

【００２１】

ルータ情報記憶部１７３は、ネットワーク上のルータ同士の接続関係を示すルータ間接続情報及び各ルータのＭＡＣアドレスを示すルータＭＡＣアドレス情報を、静的あるいは動的に管理する。動的にルータ間接続情報を作成および更新する場合は、ネットワーク構成に変更があった場合でも、侵入経路解析装置上のデータを変更する必要がなく、侵入経路解析装置の運用・管理コストの削減が可能となる。動的にルータ間接続情報を作成する手段としては、たとえば、ＳＮＭＰ（Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）などにより、ネットワーク上のルータが保持しているＩＰルーティングテーブルを収集することで実現可能である。

図３は、ルータ情報記憶部１７３が記憶するルータ間接続情報の例を示す。図３では、一例として、ルータ間接続情報の記述形式を（送信元ルータ、送信先ルータ）としており、図１のネットワーク構成におけるルータ間接続情報は、（ルータ１２１、ルータ１２２）、（ルータ１２１、ルータ１２３）、（ルータ１２１、ルータ１２４）、（ルータ１２２、ルータ１２１）、（ルータ１２３、ルータ１２１）、（ルータ１２４、ルータ１２１）のように、パケットの送受信が行われるルータの全ての組み合わせで表される。

また、図４は、ルータ情報記憶部１７３が記憶するルータＭＡＣアドレス情報の例を示す。図４の例では、各ルータのネットワークインターフェースカードに割り振られているＭＡＣアドレスを、ルータ１２１（Ｍ１、Ｍ２、Ｍ３、Ｍ４）、ルータ１２２（Ｍ５、Ｍ６）、ルータ１２３（Ｍ７、Ｍ８）、ルータ１２４（Ｍ９、Ｍ１０）とする。

【００２２】

ヘッダ情報記憶部１７１４は、パケット収集装置１４１～１４４から受信したヘッダ情

報を、検索可能な形式でデータベースに格納しておく。格納するヘッダ情報は、前述したように、パケットヘッダ内の送信元ＭＡＣアドレス、送信先ＭＡＣアドレス、ＩＣＭＰプロトコルヘッダのＴｙｐｅ、Ｃｏｄｅ、Ｃｈｅｃｋｓｕｍ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ、ＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）、Ｐｒｏｔｏｃｏｌ、発信元ＩＰアドレス、宛先ＩＰアドレス、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、Ｃｈｅｃｋｓｕｍ、ＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒなどの情報である。

【００２３】

侵入経路解析部１７１５は、アラート判断部１７１２により侵入検知装置１３１からのアラートが転送されてきた場合に、アラートに含まれている攻撃パケットのヘッダ情報を検索キーとして、ヘッダ情報記憶部１７１４に蓄積されているヘッダ情報とルータ情報記憶部１７１３に記憶されているルータ間接続情報及びルータＭＡＣアドレス情報を照合することにより攻撃パケットの中継を行ったルータを特定し、攻撃経路を解析する。侵入経路解析部１７１５は、攻撃経路解析部に相当する。

【００２４】

本実施の形態に係る侵入経路解析装置１７１の動作を図５を参照しながら説明する。なお、以下では、攻撃者が利用者端末１６３（ＭＡＣアドレスとしてＭ１１を持つ）からホスト１５１（ＭＡＣアドレスとしてＭ１２を持つ）へ攻撃を行った場合を想定して、侵入経路解析装置１７１において攻撃経路を解析する際の手順を説明する。ただし、攻撃は侵入検知装置１３１で検知可能なものであると仮定する。また、各パケット収集装置では、取りこぼしなくパケットの収集が行われているものとする。また、侵入検知装置１３１で検知された攻撃パケットをＰ１、パケット収集装置１４３で収集された攻撃パケットをＰ２とする。また、これらのパケットを（送信元ＭＡＣアドレス、宛先ＭＡＣアドレス、ＴＴＬ）として表現し、端末からのパケット送出時のＴＴＬの初期値を１０と置くと、Ｐ１（Ｍ６、Ｍ１１、７）、Ｐ２（Ｍ１２、Ｍ１０、１０）と表される。

【００２５】

先ず、侵入検知装置１３１からのアラートが通知される前は、ステップＳ５０１において、例えば定期的に、通信部１７１１が、パケット収集装置からのヘッダ情報を受信する（流通パケットヘッダ情報受信ステップ）。

次に、アラート判断部１７１２が、受信されたデータがパケット収集装置からのヘッダ情報であると判断し、ステップＳ５０２において、ヘッダ情報記憶部１７１４がヘッダ情報を記憶する（ヘッダ情報記憶ステップ）。

また、アラート判断部１７１２は、通信部１７１１によりアラートが受信されたか否かを常にチェックしており侵入検知装置１３１からのアラートを受信した場合は（Ｓ５０３、攻撃パケットヘッダ情報受信ステップ）は、アラートを侵入経路解析部１７１５に転送する。

侵入経路解析部１７１５では、ステップＳ５０４において、アラート判断部１７１２からのアラートに含まれたヘッダ情報と侵入検知装置１３１でホスト１５１への攻撃を検知したときのパケットの検知時刻に基づき、ヘッダ情報記憶部１７１４に記憶されているヘッダ情報の検索を行い（攻撃経路解析ステップ）、ステップＳ５０５において、攻撃パケットのヘッダ情報とＭＡＣアドレス、ＴＴＬ以外のデータが一致するヘッダ情報を抽出する（攻撃経路解析ステップ）。検索キーとするパケットのヘッダ情報は、攻撃パケットの種類（プロトコル）に応じて、ＩＣＭＰプロトコルヘッダのＴｙｐｅ、Ｃｏｄｅ、Ｃｈｅｃｋｓｕｍ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ、Ｐｒｏｔｏｃｏｌ、発信元ＩＰアドレス、宛先ＩＰアドレス、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、Ｃｈｅｃｋｓｕｍ、ＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒなどの項目を組み合わせて使用する。パケットヘッダに含まれるこれらの情報は、攻撃元から宛先ホストにパケットが到着するまで変更されない値であり、攻撃パケットを識別可能な情報である。したがって、以上の検索により、攻撃対象であるホスト１５１へ届いたパケットＰ１に対して、

攻撃元である利用者端末１６３から送信されたパケットＰ２が得られる。しかしながら、この時点では、パケットＰ２が偶然検索でヒットしたものであるのかどうかは判定できない。

【００２６】

次に、侵入経路解析部１７１５では、ステップＳ５０６において、抽出したヘッダ情報のＭＡＣアドレス、ＴＴＬ、攻撃パケットのＭＡＣアドレス、ＴＴＬ、ルータ情報（ルータ間接続情報、ルータＭＡＣアドレス情報）により攻撃パケットを中継したルータを特定し、攻撃経路を解析する（攻撃経路解析ステップ）。図１に示す利用者端末１６３からホスト１５１に対して攻撃パケットが送信された場合に基づいて説明すると、ステップＳ５０５の抽出結果から、（Ａ）パケットＰ１の送信元ＭＡＣアドレスがＭ６であることから、Ｐ１はＭＡＣアドレスＭ６を持つルータ１２２から送信された、（Ｂ）Ｐ２の送信先ＭＡＣアドレスがＭ１０であることから、Ｐ２はＭＡＣアドレスＭ１０を持つルータ１２４へ送信された、（Ｃ）Ｐ２のＴＴＬとＰ１のＴＴＬの差（＝３）より、仮にＰ２を攻撃パケットと仮定した場合には、経路上に３つのルータが存在する（ＩＰプロトコルの仕様により、パケットがルータを通過するたびにＴＴＬが１減るため）ことが分かる。

これにより、上記（Ａ）とルータ間接続情報より、ルータ１２２を送信先とする可能性のあるルータはルータ１２１であることが分かる。

次に、ルータ１２１を送信先とする可能性のあるルータは、ルータ１２２、ルータ１２３、ルータ１２４であることが分かる。

ここまでの処理で、（ルータ１２２→ルータ１２１→ルータ１２２）、（ルータ１２３→ルータ１２１→ルータ１２２）、（ルータ１２４→ルータ１２１→ルータ１２２）がルータを３つ含む経路の候補となる。このうち、Ｐ２を攻撃パケットと仮定した場合、（ルータ１２４→ルータ１２１→ルータ１２２）の経路により（Ａ）、（Ｂ）、（Ｃ）に矛盾なく経路を構成可能であることがわかる。よって、攻撃元から送信されたＰ２は、ルータ１２４、ルータ１２１、ルータ１２２を経由して、ホスト１５１への攻撃パケットＰ１として検知されたと断定する。

ここで、もし、矛盾なく経路を構成できなかった場合には、Ｐ２は、攻撃パケットではないことが分かり、その時点で経路の解析を終了する（侵入経路は未確定）。

また、経路に矛盾がない経路が複数導き出された場合には、それら全てを侵入経路とする。

【００２７】

このように、本実施の形態では、ルータ間接続情報を含むルータ情報を用いて、攻撃パケットの転送経路を特定するため、従来技術で必要であったルータ間を流れるパケットを収集する必要がなくなる。つまり、従来必要であった図１のルータ１２１とルータ１２２との間（ルータ１２１とルータ１２３との間、ルータ１２１とルータ１２４との間も同様である）のパケットの収集が不要になる。このため、収集するパケットの総量を減らすことが可能である。これにより、侵入経路解析に必要な計算量を削減することができ、より高速に侵入経路解析を行うことができる。また、収集するパケットの総量を減らすことにより、侵入経路解析に使用するデータの格納や保存にかかるコストを抑えることも可能である。

また、本実施の形態によれば、ルータ間接続情報を含むルータ情報を用いるため、ルータレベル解析に関連した経路上のパケットが欠けていた場合であっても、正確に攻撃経路を特定可能となる。

【００２８】

実施の形態２.

実施の形態１では、ルータ間接続情報を（送信元ルータ、送信先ルータ）という接続されたルータのペアで保持していたが、端末が繋がっているサブネットワーク間の経路をあらかじめ特定して、

テーブルとして持つことにより、侵入経路追跡の解析手順を簡略化可能である。

たとえば、図面１の場合は、（ルータ１２２⇔ルータ１２１⇔ルータ１２３）、（ルー

タ１２２⇔ルータ１２１⇔ルータ１２４）、（ルータ１２３⇔ルータ１２１⇔ルータ１２４）という情報をあらかじテーブルとしてもっていれば、侵入経路解析でＰ１、Ｐ２が得られたときに、利用者端末１６３からホスト１５１へ、３つのルータ（ルータ１２４、ルータ１２１、ルータ１２２）を含む経路を構成可能であることが分かる。このように、本実施の形態では、ルータ間接続情報として、監視対象のサブネットワーク上に存在する中継経路ごとに、それぞれの中継経路に含まれるルータ及び中継の順序を示す情報を記憶することにより、実施の形態１に比べて、侵入経路の解析に要する時間を短縮することができる。

【００２９】

ただし、監視対象ネットワークが大規模ネットワークであった場合には、この方式ではルータ間接続情報のテーブルが巨大になってしまうことが考えられるため、ネットワークの規模により、ルータ間接続情報の持ち方を選択可能とする。

【００３０】

なお、本実施の形態では、ルート間接続情報の内容が異なるのみであり、全体のシステム構成、侵入経路解析装置の構成例、侵入経路解析装置の動作例などは、実施の形態１と同様である。

【００３１】

このように、実施の形態２によれば、ルータ間接続情報を経路の候補となるデータ列として保持しておくことによって、より高速かつ簡単な手順で侵入経路の特定が可能となる。

【００３２】

前述した各実施の形態で、侵入経路解析装置１７１は、コンピュータで実現できるものである。

図示していないが、侵入経路解析装置１７１は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を備えている。

【００３３】

例えば、ＣＰＵは、バスを介して、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、通信ボード、表示装置、Ｋ／Ｂ（キーボード）、マウス、ＦＤＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ　Ｄｒｉｖｅ）、ＣＤＤ（コンパクトディスクドライブ）、磁気ディスク装置、光ディスク装置、プリンタ装置、スキャナ装置等と接続していてもよい。

ＲＡＭは、揮発性メモリの一例である。ＲＯＭ、ＦＤＤ、ＣＤＤ、磁気ディスク装置、光ディスク装置は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。

前述した各実施の形態の侵入経路解析装置１７１が扱うデータや情報は、記憶装置あるいは記憶部に保存され、侵入経路解析装置１７１の各部により、記録され読み出されるものである。

【００３４】

また、通信ボードは、例えば、ＬＡＮ、インターネット、或いはＩＳＤＮ等のＷＡＮ（ワイドエリアネットワーク）に接続されている。

【００３５】

磁気ディスク装置には、オペレーティングシステム（ＯＳ）、ウィンドウシステム、プログラム群、ファイル群（データベース）が記憶されている。

プログラム群は、ＣＰＵ、ＯＳ、ウィンドウシステムにより実行される。

【００３６】

上記侵入経路解析装置１７１の各部は、一部或いはすべてコンピュータで動作可能なプログラムにより構成しても構わない。或いは、ＲＯＭに記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

【００３７】

上記プログラム群には、実施の形態の説明において「～部」として説明した処理をＣＰＵに実行させるプログラムが記憶される。これらのプログラムは、例えば、Ｃ言語やＨＴＭＬやＳＧＭＬやＸＭＬなどのコンピュータ言語により作成される。

【００３８】

また、上記プログラムは、磁気ディスク装置、ＦＤ（Ｆｌｅｘｉｂｌｅ　Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等のその他の記録媒体に記憶され、ＣＰＵにより読み出され実行される。

【図面の簡単な説明】

【００３９】

【図１】実施の形態１、２に係るシステム構成例を示す図。

【図２】実施の形態１、２に係る侵入経路解析装置の構成例を示す図。

【図３】実施の形態１に係るルータ間接続情報の例を示す図。

【図４】実施の形態１、２に係るルータＭＡＣアドレス情報の例を示す図。

【図５】実施の形態１、２に係る侵入経路解析装置の動作例を示す図。

【図６】従来技術を説明する図。

【図７】従来技術を説明する図。

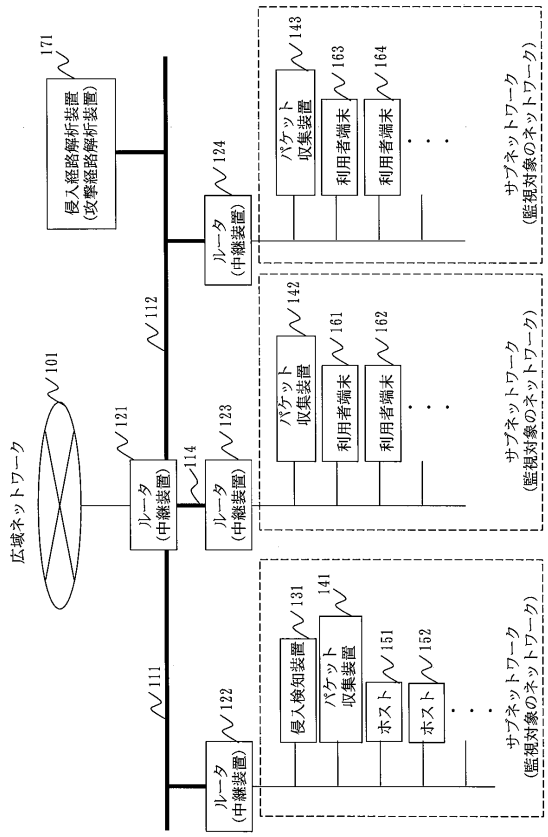
【図８】従来技術を説明する図。

【符号の説明】

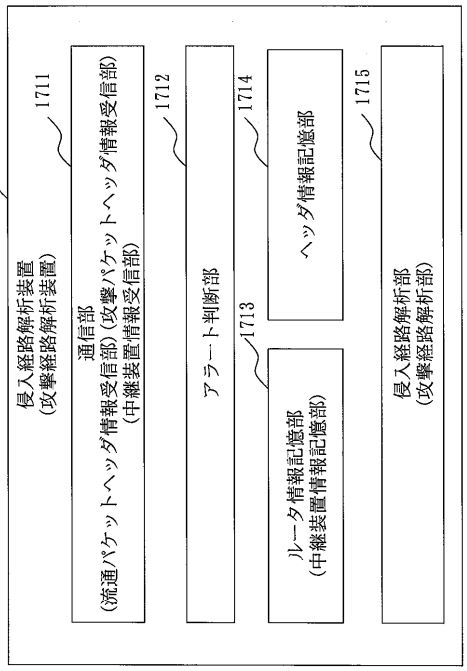
【００４０】

１０１　広域ネットワーク、１２１　ルータ、１２２　ルータ、１２３　ルータ、１２４　ルータ、１３１　侵入検知装置、１４１　パケット収集装置、１４２　パケット収集装置、１４３　パケット収集装置、１５１　ホスト、１５２　ホスト、１６１　利用者端末、１６２　利用者端末、１６３　利用者端末、１６４　利用者端末、１７１１　通信部、１７１２　アラート判断部、１７１３　ルータ情報記憶部、１７１４　ヘッダ情報記憶部、１７１５　侵入経路解析部。

【図１】



【図２】



【図３】

ルータ間接続情報

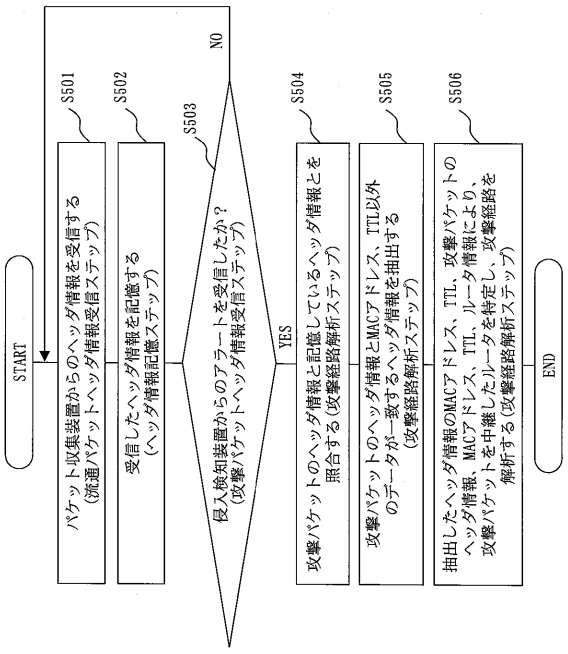
送信元ルータ	送信先ルータ
ルータ121	ルータ122
ルータ121	ルータ123
ルータ121	ルータ124
ルータ122	ルータ121
ルータ123	ルータ121
ルータ124	ルータ121

【図４】

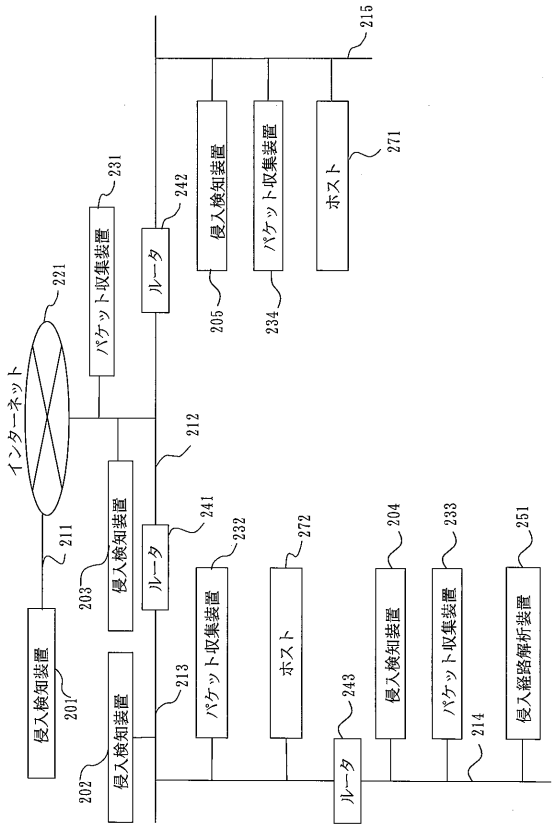
ルータMACアドレス情報

ルータ	MACアドレス
ルータ121	M1, M2, M3, M4
ルータ122	M5, M6
ルータ123	M7, M8
ルータ124	M9, M10

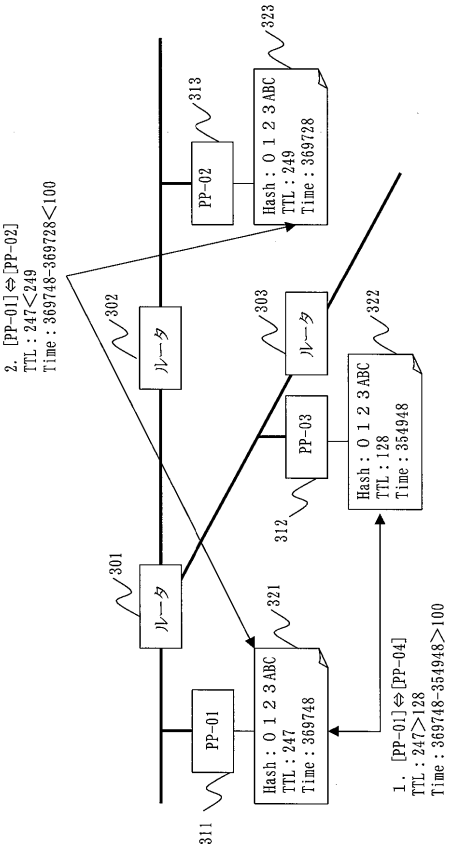
【図５】



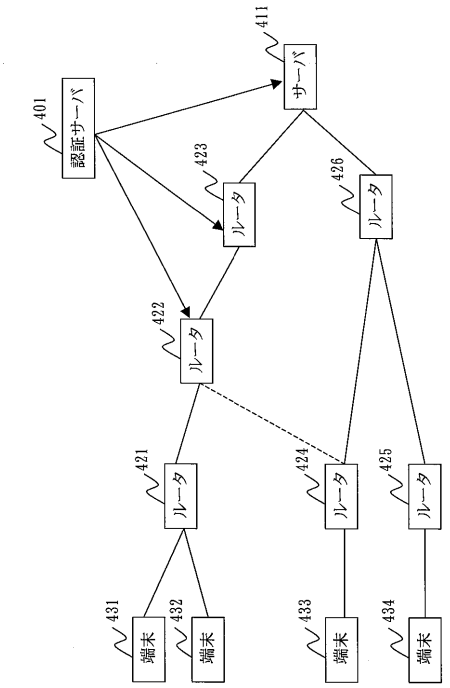
【図６】


インターネット
221
211
侵入検知装置
201
侵入検知装置
202
侵入検知装置
203
パケット収集装置
231
ルータ
241
ルータ
242
ルータ
243
侵入検知装置
204
パケット収集装置
233
侵入経路解析装置
251
212
213
214
215
侵入検知装置
205
パケット収集装置
232
ホスト
272
パケット収集装置
234
ホスト
271

【図７】


2. [PP-01]⇔[PP-02]
TTL : 247<249
Time : 369748-369728<100
301
ルータ
302
ルータ
303
ルータ
311
PP-01
312
PP-03
313
PP-02
321
Hash : 0 1 2 3 ABC
TTL : 247
Time : 369748
322
Hash : 0 1 2 3 ABC
TTL : 128
Time : 354948
323
Hash : 0 1 2 3 ABC
TTL : 249
Time : 369728
1. [PP-01]⇔[PP-04]
TTL : 247>128
Time : 369748-354948>100

【図８】


401
認証サーバ
411
サーバ
422
ルータ
423
ルータ
426
ルータ
421
ルータ
424
ルータ
425
ルータ
431
端末
432
端末
433
端末
434
端末

フロントページの続き

(56)参考文献 特開２００３－２５８９１０（ＪＰ，Ａ）
北澤 繁樹 他，侵入経路追跡システムの実装と評価，情報処理学会第66回（平成16年）全国大会 講演論文集（３） 3J-2，２００４年 3月 9日，pp.3-283～3-284

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／００－６６