(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3962050号
(P3962050)
(45)発行日　平成19年8月22日(2007.8.22)　(24)登録日　平成19年5月25日(2007.5.25)

(51)Int.Cl.　F I
H04L 9/36 (2006.01)　H04L 9/00 685

請求項の数 4　(全 36 頁)

(21)出願番号	特願2004-291882(P2004-291882)	(73)特許権者	000003078
(22)出願日	平成16年10月4日(2004.10.4)		株式会社東芝
(62)分割の表示	特願平8-295116の分割		東京都港区芝浦一丁目１番１号
原出願日	平成8年11月7日(1996.11.7)	(74)代理人	100058479
(65)公開番号	特開2005-65322(P2005-65322A)		弁理士　鈴江　武彦
(43)公開日	平成17年3月10日(2005.3.10)	(74)代理人	100091351
審査請求日	平成16年10月4日(2004.10.4)		弁理士　河野　哲
(31)優先権主張番号	特願平7-312593	(74)代理人	100088683
(32)優先日	平成7年11月30日(1995.11.30)		弁理士　中村　誠
(33)優先権主張国	日本国(JP)	(74)代理人	100108855
(31)優先権主張番号	特願平7-313307		弁理士　蔵田　昌俊
(32)優先日	平成7年11月30日(1995.11.30)	(74)代理人	100075672
(33)優先権主張国	日本国(JP)		弁理士　峰　隆司
		(74)代理人	100109830
			弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】パケット暗号化方法及びパケット復号化方法

(57)【特許請求の範囲】

【請求項１】

所定の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、

通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、

暗号化未完了であり、かつ、署名情報が存在しない場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている送信元計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、

求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている、当該パケットの暗号化を行なうべきパケット処理装置から当該送信元計算機に至るネットワーク経路内に設置されたパケット処理装置の数を指定する暗号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を暗号化するとともに、該パケットに対して、前記暗号化情報を暗号化完了を示す内容にし、および暗号化を行った自装置の署名情報を付加することを特徴とするパケット暗号化方法。

【請求項２】

前記パケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の

内容、署名情報の有無、および暗号化レベル情報の内容の間に矛盾が存在する場合は、エラーを通知するように制御することを特徴とする請求項１に記載のパケット暗号化方法。

【請求項３】

所定の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置にて外部方向から通信されるパケットを復号化するパケット復号化方法において、

通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、

暗号化完了であり、かつ、署名情報が存在する場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている受信先計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、

求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている、当該パケットの復号化を行なうべきパケット処理装置から当該受信先計算機に至るネットワーク経路内に設置されたパケット処理装置の数を指定する復号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を復号化することを特徴とするパケット復号化方法。

【請求項４】

前記復号化レベル情報を、前記パケットの送信元計算機が暗号化を行なうパケット処理装置を指定するためのものである、当該パケットの暗号化を行なうべきパケット処理装置から当該送信元計算機に至るネットワーク経路内に設置されたパケット処理装置の数を指定する暗号化レベル情報と共通化したことを特徴とする請求項３に記載のパケット復号化方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、移動計算機を含む複数の計算機間でオープンなネットワークを介してデータ通信を行なう場合に、受信したパケットが正当な計算機もしくは利用者からのものであるかどうかを認証し、正当なパケットのみを転送制御し、さらには組織外部へのデータ転送にあたり外部への情報漏洩を防ぐためパケットの暗号化を行う、パケット暗号化方法及びパケット復号化方法に関する。

【背景技術】

【０００２】

インターネットの普及により、遠隔地の計算機にログインしたり、遠隔地の計算機に対しファイルを転送したりすることが可能となっている。電子メールやｗｏｒｌｄ ｗｉｄｅ ｗｅｂ（WWW）などのサービスも利用できる。その一方、インターネットではセキュリティを考慮したプロトコルやシステムの構築が遅れてきたため、悪意の利用者が遠隔ネットワークの計算機に侵入して機密情報を盗んだり、重要なファイルを消去したり、さらには外部への通信情報が盗聴されるといった不正行為が行われる可能性があった。

【０００３】

このような不正行為に対抗するため、企業などのネットワークにはファイアウォール、もしくはセキュリティゲートウェイと呼ばれるシステムが構築される場合が多い。ファイアウォールは企業のローカルなネットワークと広域なインターネットの接続点に設けられ、外部からの不正な侵入や情報漏洩を防止するために通信のフィルタリング（通信の遮断・通過の制御）を実現するシステムである。

【０００４】

ファイアウォールが危険な外部からの通信を遮断するので、内部のネットワーク（内部ネット）に接続された計算機（ホスト）には特別にセキュリティを強化するための仕組みを講じなくても済むという利点がある。

【０００５】
ファイアウォールの基本手法に、パケットフィルタがある。パケットフィルタは通信パケットに添付されている送信元ホストと受信元ホストのアドレスと利用サービス（遠隔ログイン（ｔｅｌｎｅｔ）、ファイル転送（ｆｔｐ）、電子メール（ＳＭＴＰ）、電子ニュース（ＮＮＴＰ）、WWWサービス（ｈｔｔｐなど）に対応するポート番号を基に許可された通信かどうかを判定し、許可されている通信のパケットのみをリレーする手法である。この手法ではパケット内のホスト・アドレスとサービス（ポート番号）を改変困難と仮定すれば十分なセキュリティ機能を提供するが、実際には送信ホストのアドレスを偽ってパケットを送出することは可能である。このような不正行為に対抗するために、暗号を利用した認証機能を用いてパケットのフィルタリングを実施するシステムがある。

【０００６】
暗号によるパケット認証には一般にＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）と呼ばれる手法が用いられる。これは、パケットの送信側と受信側が秘密の鍵情報を共有していることを前提とする。送信側は各パケットごとに、そのデータの全ビットと鍵Ｋに依存したダイジェスト情報を計算し、パケットに添付する。すなわち、ＭＡＣ＝ｆ（Ｋ，ｄａｔａ）を計算する。ここでｆはＭＡＣ計算アルゴリズム、ｄａｔａはパケットの内容を表す。一方、パケットの受信側は受け取ったパケットの内容と鍵Ｋから送信側と同じ計算を行い、計算したＭＡＣの値とパケットに添付されたＭＡＣが一致する場合には、送信者とパケット内容が送信データそのものであることを認証する。

【０００７】
ファイアウォールにＭＡＣによる認証機能を導入することは、例えば文献Ｊ．Ｉｏａｎｎｉｄｉｓ ａｎｄ Ｍ．Ｂｌａｚｅ，“Ｔｈｅ Ａｒｃｈｉｔｅｃｔｕｒｅ ａｎｄ Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ ｏｆ Ｎｅｔｗｏｒｋ－Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ ｕｎｄｅｒ Ｕｎｉｘ，”ＵＳＥＮＩＸ／４ｔｈＵＮＩＸ Ｓｅｃｕｒｉｔｙ ｓｙｍｐｏｓｉｕｍ，ｐｐ．２９－３９（１９９３）に示されている。

【０００８】
このようにすると、パケット中のアドレスやポート番号を偽った送信や伝送中のパケットの改ざんは検出できるため、ファイアウォールシステムの安全性が飛躍的に向上する。これを認証機能付きファイアウォールと呼ぶことにする。

【０００９】
しかし、従来の認証機能付きファイアウォールが対象としているのは、保護すべきネットワークが１階層の場合に限定されていた。すなわち、送信ホストもしくは送信ホストを収容するネットワークのファイアウォールがＭＡＣをパケットに添付し、受信ホストを収容するネットワークのファイアウォールをＭＡＣを検査する仕組みである。保護ネットワークが階層的になった場合には十分に対応できない。なぜなら受信側の保護ネットワークが２階層の場合、送信ホスト側のファイアウォールと受信側第１階層のファイアウォールは鍵Ｋを共有するため、ＭＡＣを検査することはできるが、受信側第２階層のファイアウォールは鍵Ｋを持たないので同じパケットを受け取ってもＭＡＣ検査ができないからである。

【００１０】
仮に受信側第１階層のファイアウォール、受信側第２階層のファイアウォール、送信側ファイアウォールが鍵Ｋを共有することにすると、受信側第１階層のファイアウォールから送信側ファイアウォールになりすまして受信側第２階層ファイアウォールへパケットを送り込むことができる。

【００１１】
最近では携帯型計算機を利用する場面も多くなっており、多部署のネットワークに携帯計算機を接続して、その移動計算機が本来所属しているネットワークのサーバ計算機や移動先の計算機などと通信する場面も増加している。このような場合でも従来の認証機能付きファイアウォールの機能では限界がある。すなわち、認証機能付きファイアウォールでは、訪問先のネットワークのファイアウォールと通信相手のネットワークのファイアウォ

ールの間でパケットの検査は行えるが、移動計算機と訪問先のファイアウォールとの認証や移動計算機と通信先のファイアウォールとの認証をどのようにして一貫して行うかは未解決のままである。

【００１２】

以上の説明した認証の問題以外に、通信パケット内容の保護という問題もある。すなわち、特に機密性の高いデータを外部ネットワークを介して通信する状況では、外部にデータパケットを送出する前にその内容を暗号化し、受信したサイトで復号化するという方法がある。この方法も保護すべきネットワークが１階層の場合にはパケットの方向性のみを暗号化・復号化の判定に利用すれば良いが、保護すべきネットワークが階層された場合や、移動計算機を利用したモバイル・コンピューティング環境では、暗号化・復号化の制御をどのマシンで、どのような判断基準で行うかという問題がある。特に、パケットを階層間に亘って転送する場合に各階層での復号・再暗号化の繰り返しによる処理効率の低下を回避しかつ安全性を確保することは困難であった。また、暗号通信すべき領域と平文で通信すべき領域を柔軟に制御しかつ安全性を確保することは困難であった。

【発明の開示】

【発明が解決しようとする課題】

【００１３】

以上のように、従来のシステムでは、保護すべきネットワークが階層化された計算機ネットワーク等では、各階層のネットワークを安全に保護することは困難であった。また、暗号通信を効率的かつ安全に行うことは困難であった。

【００１４】

本発明は、上記事情を考慮してなされたものであり、保護すべき計算機ネットワークが階層化された場合や移動計算機をサポートするモバイル・コンピューティング環境においても、通信されるデータ内容を効率的かつ安全に保護可能なパケット暗号化方法及びパケット復号化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】

【００１５】

本発明は、所定の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向に通信されるパケットを暗号化するパケット暗号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、暗号化未完了であり、かつ、署名情報が存在しない場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている送信元計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている、当該パケットの暗号化を行なうべきパケット処理装置から当該送信元計算機に至るネットワーク経路内に設置されたパケット処理装置の数を指定する暗号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を暗号化するとともに、該パケットに対して、前記暗号化情報を暗号化完了を示す内容にし、および暗号化を行った自装置の署名情報を付加することを特徴とする。

【００２１】

本発明によれば、重要な情報をネットワークを介して通信する際に、送信側でパケットを暗号化する処理をユーザの指定する箇所のパケット処理装置で１回のみ行うようにすることができ、暗号化の処理に起因するデータ転送効率の低下を防止することができる。

【００２２】

好ましくは、前記パケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容、署名情報の有無、および暗号化レベル情報の内容の間に矛盾が存在する場合は、エラーを通知するように制御するようにしてもよい。

【００２５】

本発明は、所定の計算機ネットワークと該計算機ネットワーク外部との接続点に設けられるパケット処理装置（例えば、セキュリティゲートウェイ）にて外部方向から通信されるパケットを復号化するパケット復号化方法において、通過するパケット内に書き込まれている暗号化完了または暗号化未完了を示す暗号化情報の内容および署名情報の有無を調べ、暗号化完了であり、かつ、署名情報が存在する場合、予め格納された、自装置の設置箇所から末端の計算機に至る下位ネットワークに接続されている計算機のアドレス情報と、各計算機に至るネットワーク経路内に設置されたパケット処理装置の数の情報との対応情報をもとに、前記パケット内に書き込まれている受信先計算機のアドレス情報から、対応するパケット処理装置の数の情報を求め、求められたパケット処理装置の数の情報と、前記パケット内に書き込まれている、当該パケットの復号化を行なうべきパケット処理装置から当該受信先計算機に至るネットワーク経路内に設置されたパケット処理装置の数を指定する復号化レベル情報とが等しい場合、前記パケット内のデータ本体の部分を復号化することを特徴とする。

【００２６】

本発明によれば、重要な情報をネットワークを介して通信する際に、受信側でパケットを暗号化する処理をユーザの指定する箇所のパケット処理装置で１回のみ行うようにすることができ、暗号化の処理に起因するデータ転送効率の低下を防止することができる。

【００２７】

好ましくは、前記復号化レベル情報を、前記パケットの送信元計算機が暗号化を行なう処理装置を指定するためのものである、当該パケットの暗号化を行なうべきパケット処理装置から当該送信元計算機に至るネットワーク経路内に設置されたパケット処理装置の数を指定する暗号化レベル情報と共通化ようにしてもよい。

【００２８】

パケット処理装置による相互接続は、外部ネットワークとの接続のみならず、組織内の小グループ間でも各組織内部の秘密情報の保護のため設置されるようになっていくと考えられ、その場合、末端の計算機から複数のパケット処理装置を通して各組織間の通信や外部ネットワークとの通信を行うようになる。本発明によれば、そのようなネットワーク構成において、データに含まれる情報を共有すべき最小のネットワーク範囲を認識し、必要なネットワーク階層で１回のみ暗号化、復号化を行い、かつ不要な多段階の暗号化を回避するよう制御することが可能になる。

【００３０】

なお、以上の各装置に係る発明は、方法に係る説明としても成立し、各方法に係る発明は、装置に係る説明としても成立する。

【００３１】

また、上記の発明は、コンピュータに上記の発明に相当する各手順を実行させるためのプログラムあるいはコンピュータを上記の発明に相当する各手段として機能させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【発明の効果】

【００３２】

本発明によれば、保護ネットワークが階層化され、各階層にパケット処理装置を配置する場合においても、重要な情報をネットワークを介して通信する際に、送信側でデータパケットを暗号化し、受信側で復号化する処理を、ユーザの指定する箇所で１回のみ行うことができ、暗号化、復号化の処理に起因するデータ転送効率の低下を防止することができる。さらに、そのようなネットワーク構成において、データに含まれる情報を共有すべき最小のネットワーク範囲を認識し、必要なネットワーク階層で１回のみ暗号化、復号化を行い、かつ不要な多段階の暗号化を回避するよう制御することが可能になる。

【００３３】

また、本発明によれば、各パケット処理装置で暗号化を行った際にデータパケットに暗号化完了を示す情報を付加し、この情報の付加されたデータパケットに対しては、その暗号化装置では暗号化を行わないように制御することができるので、各暗号化装置毎に複雑

なネットワーク構成の設定を行うことなく、１回のみ暗号、復号化を行うようにシステムを設定することが可能になる。

【発明を実施するための最良の形態】

【００３４】

以下、図面を参照しながら発明の実施の形態を説明する。

【００３５】

図１は、本発明を適用する計算機ネットワークの一例である。

【００３６】

セキュリティゲートウェイの保護および管理の対象となるネットワークを管理対象ネットワークと呼ぶ。

【００３７】

本実施形態においては、各々のセキュリティゲートウェイに対して、管理対象ネットワークとそれ以外である外部ネットワークが定義され、セキュリティゲートウェイは、外部ネットワークから管理ネットワークへの不審なパケットの侵入を防止し、さらには管理ネットワークから外部ネットワークへの不審なパケットの流出を防止する。例えば図１の計算機ネットワークでは、セキュリティゲートウェイＧＡ１の管理ネットワークは部所Ａ１ネットワークであり、セキュリティゲートウェイＧＡ１１の管理ネットワークは部所Ａ１１ネットワークである。

【００３８】

管理ネットワークに直接収容されている計算機とは、次のことを指す。ある計算機から見て外部ネットワークへの送信時に最初におよび外部からの受信時に最後に通過しなければならないセキュリティゲートウェイが存在するが、その計算機はそのセキュリティゲートウェイの管理ネットワークに直接収容されている（そのセキュリティゲートウェイが直接管理している）ものとする。例えば図１の計算機ネットワークでは、計算機Ｈ３は管理ネットワークＡ１に直接収容されており、計算機Ｈ４は管理ネットワークＡに直接収容されている。

【００３９】

本発明を適用する計算機ネットワークでは、パケットが送信元のホストから最終的な宛先ホストに到達するまでに幾つかのセキュリティゲートウェイを通過する。各セキュリティゲートウェイには、そこから外部へのパケット送出あるいは外部からのパケット流入にあたり、必要に応じてパケットの認証処理（認証情報の付与や検査）を実行する。

【００４０】

本発明１は、パケットの認証機能に関するものであり、パケットの通過パスに存在するセキュリティゲートウェイの間で通過パスに沿った形式でリンク・バイ・リンクに認証鍵を共有する。さらに、送信ホストを直接収容するネットワークのセキュリティゲートウェイ（これを発信側ゲートウェイと呼ぶことにする）は最終宛先ホストを直接収容するネットワークのセキュリティゲートウェイ（これを宛先側ゲートウェイと呼ぶことにする）との間でエンド・ツー・エンドで認証鍵を共有する。

【００４１】

発信側ゲートウェイは、パケット・データに対して、エンド・ツー・エンドで共有した認証鍵１による認証コード１と、次のセキュリティゲートウェイとの間で共有している認証鍵２による認証コード２の２つを計算し、パケットに添付して転送する。

【００４２】

次のセキュリティゲートウェイは共有している認証鍵２によりパケットに添付された認証コード２を検査し、検査に通ればさらに次のセキュリティゲートウェイとの間で共有している認証鍵３によりパケットデータに対する認証コード３を生成し、パケットから認証コード２を除去し、代わりに認証コード３を添付して転送する。このようにパケット経路の間に存在するセキュリティゲートウェイでは、隣のセキュリティゲートウェイとの間でパケット認証コードの検査・生成による付け替えを繰り返しながら、パケットの転送が行われる。このことにより各セキュリティゲートウェイは、パケットが経路に沿って隣のセ

キュリティゲートウェイから転送されていること、内容に改ざんがないことを確認できる。

【００４３】

また、宛先側ゲートウェイは、前段のセキュリティゲートウェイにより添付された認証コードの他に、発信側ゲートウェイにより添付された認証コード１を検査する。特に、認証コード１の検査によりパケットが発信側ゲートウェイにより発信されたものであること、内容に改ざんがないことを確認できる。

【００４４】

本発明２は、パケットの認証機能に関するものであり、パケットの通過パスに存在する個々のセキュリティゲートウェイと発信側ゲートウェイとの間でペア単位に別々の認証鍵を共有している。発信側ゲートウェイは、それぞれの認証鍵を用いて複数の認証コードを生成し、全てをパケットに添付して転送する。

【００４５】

パケットの経路に存在するセキュリティゲートウェイは、自らの装置に対応する認証コードの検査を行い、検査に通ればパケットを転送する。このことにより、パケットが発信側ゲートウェイにより発信されたものであること、内容に改ざんがないことを各経路上のセキュリティゲートウェイが確認できる。

【００４６】

本発明３は、パケットの暗号化機能に関するものであり、複数の計算機ネットワーク間で、データを通信する際に、通信データパケットを暗号化するセキュリティゲートウェイであって、各セキュリティゲートウェイは、自装置に直接接続されている計算機群のアドレス情報を管理する手段と、通過するデータパケットの送信元が自装置に直接接続されている計算機であるかどうかを判断する手段と、通過するデータパケットの受信先が自装置に直接接続されている計算機であるかどうかを判断する手段とを備え、通過するデータパケットの送信元が自装置に直接接続されている計算機であると判断された場合にのみデータを暗号化し、通過するデータパケットの受信先が、自装置に直接接続されている計算機であると判断された場合にのみデータを復号化するようにしたものである。

【００４７】

本発明４は、パケットの暗号化機能に関するものであり、複数の計算機ネットワーク間で、データを通信する際に、通信データパケットを暗号化するセキュリティゲートウェイであって、各セキュリティゲートウェイは、自装置が暗号化を行った際にデータパケットに暗号化完了を示す情報と自装置による署名情報とを付加する手段と、通過するデータパケットの暗号化完了を示す情報を検査し、もし暗号化完了でありデータに署名情報が付加されている場合には自装置では暗号化を行わないように制御し、もし暗号化完了でありデータに署名情報が付加されていない場合にはエラーを通知し、もし暗号化未完了であり、データに署名情報が付加されていない場合には、データを暗号化し、データ内に暗号化完了情報と自装置による署名情報を付加するように制御し、もし暗号化未完了であり、かつデータに署名情報が付加されている場合にはエラーを通知するように制御する手段と、自装置に直接接続されている計算機群のアドレス情報を管理する手段とを備え、データ到達先では、発明３のように、受信先計算機が、自装置に直接接続されている計算機であると判断された場合にのみデータを復号化するようにしたものである。

【００４８】

以下、本実施形態をさらに詳しく説明する。

【００４９】

図１は、本発明の一実施形態に係るセキュリティゲートウェイが用いられる計算機ネットワークの一構成例を示す。この計算機ネットワークは、複数の組織ネットワークを相互接続するインターネットなどの外部ネットワーク１０１、組織Ａネットワーク１０２、組織Ｂネットワーク１０３、組織Ｃネットワーク１０４、組織Ｄネットワーク１０５、組織Ａネットワーク内の部所ネットワークＡ１，Ａ２，Ａ３、部所ネットワークＡ１内の部所ネットワークＡ１１、組織Ｂネットワーク内の部所ネットワークＢ１，Ｂ２からなる。

【００５０】
また、本発明の一実施形態に係るセキュリティゲートウェイとして、組織Ａ用（ＧＡ）、部所Ａ１用（ＧＡ１）、部所Ａ１１用（ＧＡ１１）、組織Ｂ用（ＧＢ）、部所Ｂ１用（ＧＢ１）、組織Ｃ用（ＧＣ）、組織Ｄ用（ＧＤ）が、それぞれ図１の位置に配置される。
【００５１】
このようにセキュリティゲートウェイは、保護すべきネットワークとその外部のネットワークとの接続点に設置され、その保護ネットワーク内からの送信パケットおよび保護ネットワーク内への受信パケットは共にセキュリティゲートウェイを通過しなければならないように配置され、ファイアウォールと同様の機能を果たす。ファイアウォールとは、内部ホストから外部へのサービス要求と外部から内部ネットワークへのサービス要求を共に許可されたもの以外制限するものである。
【００５２】
なお、本実施例では、図１における「部所ネットワーク」を、本セキュリティゲートウェイで保護されたネットワークを単位に定義している。
【００５３】
まず最初に本発明のセキュリティゲートウェイの認証機能について説明する。
【００５４】
セキュリティゲートウェイの管理する対象である管理ネットワークとは、セキュリティゲートウェイの保護対象となるネットワークをいう。例えば図１の計算機ネットワークでは、セキュリティゲートウェイＧＡ１の管理ネットワークは部所Ａ１ネットワークであり、セキュリティゲートウェイＧＡ１１の管理ネットワークは部所Ａ１１ネットワークである。
【００５５】
さらに、管理ネットワークに直接収容されている計算機とは、次のことを指す。計算機から見て外部への送信時に最初におよび外部からの受信時に最後に通過しなければならないセキュリティゲートウェイが存在するが、そのセキュリティゲートウェイの管理ネットワークに直接収容されていると定義する。例えば図１の計算機ネットワークでは、管理ネットワークＡ１に直接収容されている計算機は例えばＨ３であり、計算機Ｈ４は管理ネットワークＡに直接収容されている。
【００５６】
なお、図１におけるホストＨ５はセキュリティゲートウェイの存在しないネットワークに接続されている。このようなホストＨ５と安全に通信を行う場合には、ホストＨ５自体がセキュリティゲートウェイの機能を備えている必要がある。
【００５７】
図２は、図１のネットワークにおけるパケットの流れの一例を説明するための図である。図１における部所ネットワークＡ１１内の計算機（ホストとも呼ぶ）Ｈ１から部所ネットワークＢ１内のホストＨ２宛てに送出されるパケットは、送信ホストＨ１→セキュリティゲートウェイＧＡ１１→ＧＡ１→ＧＡ→ＧＢ→ＧＢ１→受信ホストＨ２の経路を通る。
【００５８】
本実施形態では、ホストＨ２からホストＨ１宛てのパケットは、先の経路の逆順に流れる。ただし、場合によってはセキュリティゲートウェイを保護ネットワークに複数設置することも可能であり、その場合にはパケットの送信方向や通信相手により経由するセキュリティゲートウェイが異なることもある。
【００５９】
このようにパケット転送経路上に送信側と受信側で一対のセキュリティゲートウェイに限定されず、複数のセキュリティゲートウェイが存在する場合、従来では、個々のセキュリティゲートウェイがどのように連携してパケットを認証すれば良いかといった問題が発生する。本セキュリティゲートウェイでは、このような状況に対処し、各々のセキュリティゲートウェイがパケットの正当性を確認しながら自らの管理するネットワークを保護可能とするものである。

【００６０】
まず、第１の実施形態を説明する。
【００６１】
図３に、本実施形態に係るセキュリティゲートウェイの一構成例を示す。図３のように、セキュリティゲートウェイ３１０は、パケット受信部３０１、認証コード検査部３０２、認証鍵管理部３０３、パケットフィルタリング部３０４、認証コード生成部３０５、パケット整形部３０６、パケット転送部３０７を備えている。
【００６２】
パケット受信部３０１は、セキュリティゲートウェイ３１０の保護するネットワークを経由するパケットを受信する。
【００６３】
認証鍵管理部３０３は、認証鍵テーブルを管理し、認証コードの生成に用いられる証明用認証鍵、認証コードの検査に用いられる検査用認証鍵を記憶している。
【００６４】
認証コード検査部３０２は、認証鍵管理部３０３から得た検査用認証鍵を用いて、受信パケットの認証コードの正当性を検査する。
【００６５】
パケットフィルタリング部３０４は、受信されたパケットに含まれる送信元ホスト識別情報、受信先ホスト識別情報、コネクション識別情報を元にパケットの転送を認めるかどうかの判定を行う。
【００６６】
認証コード生成部３０５は、認証鍵管理部３０３から得た証明用認証鍵を用いて、次の転送先での検査に用いられる認証コードを生成する。
【００６７】
パケット整形部３０６は、パケットに添付され既に検査された認証コードの除去と新たに生成された認証コードの添付を行う。
【００６８】
パケット転送部３０７は経路情報に基づいてパケットの転送を行う。
【００６９】
なお、以上の構成部分のうち、パケットフィルタリング部３０４については、本セキュリティゲートウェイとは別にパケットフィルタリング装置として用意し、（パケットフィルタリング部３０４を除いた）セキュリティゲートウェイとパケットフィルタリング装置とが連係をとる形態にしても良い。この場合、セキュリティゲートウェイでは、認証コード検査部３０２の出力が認証コード生成部３０５の入力に結線された構造となる。
【００７０】
認証コード（MESSAGE AUTHENTICATION CODE ：略してＭＡＣと呼ばれる）の計算は、例えば次のような方法を用いる。第１の方法は、秘密鍵暗号であるＤＥＳ（DATA ENCRYPTION STANDARD）のＣＢＣ（CIPHER-BLOCK-CHAINING ）モードでパケットデータを暗号化し、その暗号文の最終ブロックである６４ビットデータを用いる方法（ISO/IEC JTC1/IS 9797に詳細な説明がある）である。第２の方法は、ハッシュ関数であるＭＤ５（MESSAGE DIGEST ALGORITHM 5）を用いて、パケットデータの前後に認証鍵を連結したデータを、圧縮した結果である、１２８ビットデータを用いる方法（IETF RFC1828に詳細な説明がある）などによる。
【００７１】
認証コードは、パケット内のフィールドにおいて転送途中で変化するもの（例えば、ルータに到着するごとにデクリメントされるTTL(TIME-TO-LIVE) フィールドなど）を除いた全てのデータを反映したものとする。
【００７２】
ここで、認証コードの生成・検査に用いられる認証鍵の設定単位について説明する。第１の方法は、送信元ホストアドレス、受信先ホストアドレスの組に対して１つの認証鍵を

設定することである。この場合には、同一ホスト間のパケットはどんなサービスでも同じ認証鍵によって認証コードが生成されることになる。

【００７３】

第２の方法は、送信元ホストアドレス、受信先ホストアドレス、送信元のポート番号、受信先のポート番号の組に対して設定することである。この場合、ポート番号の組はコネクションに対応するので、通信セッション単位に認証鍵を定義したことになる。

【００７４】

以下の説明では、送信ポート番号と受信先ポート番号といった情報をコネクションＩＤと定義して説明を行ない、認証鍵はコネクション単位に設定されるものと仮定する。ただし、他の設定単位でも同様な適用が可能である。

【００７５】

図４に、転送されるパケット・フォーマットの一例を示す。パケットは、送信元ホストアドレス（図中１５０１）、受信先ホストアドレス（１５０２）、コネクションＩＤ（１５０３）、認証コード（１５０４）、データ部（１５０５）の各領域を備える。認証コード（１５０４）は複数を添付することも可能であり、その場合には個々の認証コードを識別するための通し番号や認証コードＩＤがさらに付けられても良い。

【００７６】

図５に転送されるパケットフォーマットのより詳細な一例を示す。パケットのうち、データ部（図中のＤａｔａ）とＩＰヘッダ１（図中のＩＰ１）が送信元ホストから送出されるＩＰパケットである。このＩＰヘッダ１に送信元ホストアドレス、受信先ホストアドレスが含まれている。また認証コードは認証ヘッダ（ＡＨ）に含まれる。パケットに複数の認証コードを添付する場合には複数の認証ヘッダを用いる。認証ヘッダ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ）はＩＥＴＦ ＲＦＣ１８２６に詳しい。図５には認証ヘッダ１（図中のＡＨ１）の外側にＩＰヘッダ２（図中のＩＰ２）が、また認証ヘッダ２（図中のＡＨ２）の外側にＩＰヘッダ３（図中のＩＰ３）が挿入されている。これはＩＰヘッダ３により指定された宛先のノードで認証ヘッダ２内の認証コードが検査され、ＩＰヘッダ２により指定された宛先のノードで認証ヘッダ１内の認証コードが検査されることを意味する。

【００７７】

例えば、図２に示した各ノードを介して送信元ホストＨ１がパケットを受信先ホストＨ２に送信する場合、ホストＨ１では、ＩＰヘッダ１はソースアドレス＝ホストＨ１、宛先アドレス＝ホストＨ２と設定したパケット（ＩＰヘッダ１とＤａｔａ部）を送る。セキュリティゲートウェイＧＡ１１ではこのパケットを受信し、認証ヘッダ１とＩＰヘッダ２を追加する。ここでＩＰヘッダ２のソースアドレス＝ゲートウェイＧＡ１１、宛先アドレス＝ゲートウェイＧＢ１とする。さらに、このパケットに認証ヘッダ２とＩＰヘッダ３を追加する。ＩＰヘッダ３のソースアドレス＝ＧＡ１１、宛先アドレス＝ＧＡ１とする。以下、パケットの中継を行うセキュリティゲートウェイではＩＰヘッダ３の内容を変更しながら、パケットを転送する。このとき各中継ゲートウェイでは認証ヘッダ２の検査・除去と新たな認証ヘッダ２の作成・添付が行われる。

【００７８】

図６に、認証鍵管理部３０３に記憶される認証鍵テーブルの一例を示す。認証鍵テーブルには、送信元ホストアドレス，受信先ホストアドレス，コネクションＩＤの組に対して検査用認証鍵と証明用認証鍵が登録される。検査用認証鍵と証明用認証鍵のどちらか一方は空欄の場合がある。すなわち、送信ホストが管理ネットワーク内にあれば検査用認証鍵は空欄となる。このとき、証明用認証鍵は最大２つが登録されることになる。一方、受信ホストが管理ネットワーク内であれば生成用認証鍵が空欄で、検査用認証鍵は最大２つが登録される。なお、検査用認証鍵と証明用認証鍵の両方が空欄となることはない。複数のセキュリティゲートウェイでの認証鍵の配送・共有方法については後で例を説明する。

【００７９】

以上のような装置がどのように連係してパケット転送を行うかを図７の例を基に説明す

る。前提として、パケット転送経路上のセキュリティゲートウェイであるＧＡ１１，ＧＡ１，ＧＡ，ＧＢ，ＧＢ１の間では次のように認証鍵を共有しているものとする。すなわち、ＧＡ１１とＧＡ１の間で認証鍵Ｋ１、ＧＡ１とＧＡの間で認証鍵Ｋ２、ＧＡとＧＢの間で認証鍵Ｋ３、ＧＢとＧＢ１の間で認証鍵Ｋ４、さらにはＧＡ１１とＧＢ１の間で認証鍵Ｋ０がそれぞれ共有されている。

【００８０】

セキュリティゲートウェイＧＡ１１は、ホストＨ１から受信したパケットに指定されている送信ホスト，受信ホスト，コネクションＩＤを調べ、対応する認証鍵Ｋ０でパケットの内容に相当するデータに対する認証コードＭＡＣ０を計算する。同様に、認証鍵Ｋ１を用いて認証コードＭＡＣ１を計算する。この２つの認証コードをパケットに添付して転送する。このパケットはルーティング処理に従って次のセキュリティゲートウェイＧＡ１に到着する。

【００８１】

セキュリティゲートウェイＧＡ１では、受信したパケットに添付されている送信ホスト，受信ホスト，コネクションＩＤを調べ、対応する認証鍵Ｋ１により認証コードＭＡＣ１を検査する。ＭＡＣ１の正当性が確認された場合には、認証鍵Ｋ２によりパケットデータに対する認証コードＭＡＣ２を計算し、パケットに添付されたＭＡＣ１を除去し、ＭＡＣ２を添付したパケットを転送する。

【００８２】

以下、セキュリティゲートウェイＧＡ，ＧＢでは、セキュリティゲートウェイＧＡ１と同様に認証コードの検査、認証コードの生成と置き換えを行いながらパケットを転送する。異常がなければパケットはセキュリティゲートウェイＧＢ１に到達する。

【００８３】

セキュリティゲートウェイＧＢ１では、まず、ＭＡＣ４を認証鍵Ｋ４で検査し、これに以上がなければＭＡＣ０を認証鍵Ｋ０で検査する。この検査に以上がなければ、受信したパケットはホストＨ１を収容するネットワークから発信され、途中で改ざんされることなく上位のセキュリティゲートウェイＧＢを経由して受信されたことが確認される。最後に、ＭＡＣ４とＭＡＣ０を除去したパケットをホストＨ２に転送することでパケットの転送は完了する。

【００８４】

なお、本実施形態の変形例として、セキュリティゲートウェイＧＢとＧＢ１の間では認証鍵Ｋ４を共有せずに、ＧＢではＧＡから転送されたパケットのＭＡＣ３を検査し、検査結果が異常でないときにはＭＡＣ３を取り除いたパケット（ＭＡＣ０が付加されているだけのパケット）をＧＢ１に転送するようにしても良い。この場合、ＧＢ１では認証鍵Ｋ０を用いてＭＡＣ０を検査するのみとなる。上述のセキュリティゲートウェイＧＢがＭＡＣ４を付ける実施形態は、受信パケットがセキュリティゲートウェイＧＢを経たものであることを最初に確認した上で、ホストＨ１を収容するネットワークのセキュリティゲートウェイＧＡ１１から発信されたものであることを確認する方式となるが、セキュリティゲートウェイＧＢ１にとって特に重要なのはＧＡ１１からの発信パケットであることの確認であるから、余分なＭＡＣ４の検査を省略しても良い。

【００８５】

さらに、外部からの管理ネットワークへの不正な侵入の防止だけを目的とする場合には、パケットの発信側のネットワークにおいて、セキュリティゲートウェイＧＡ１１とＧＡ１の間でのＭＡＣ１の生成・検査、およびセキュリティゲートウェイＧＡ１とＧＡの間でのＭＡＣ２の生成・検査は不要である。具体例としては、セキュリティゲートウェイＧＡ１１が鍵Ｋ０を用いてパケットにＭＡＣ０を添付し、セキュリティゲートウェイＧＡ１はパケットが外向き（すなわち内部ネットワークから外部ネットワーク向き）か内向き（すなわち外部ネットワークから内部ネットワーク向き）かだけを検査し、外向きの場合にはそのまま転送する。セキュリティゲートウェイＧＡはパケットが外向きか内向きかを検査し、外向きであれば鍵Ｋ３でＭＡＣ３を生成し、パケットに添付する。この場合には鍵Ｋ

１とＫ２の共有が不要となる。

【００８６】

以上に説明した第１の実施形態におけるセキュリティゲートウェイの処理手順を図８に示した。

【００８７】

本実施例のセキュリティゲートウェイは、パケットを受信すると（ステップＳ８０１）、まず、パケットの送信元ホストアドレスを調べ、直接収容する管理ネットワーク内ホストからの送信かどうかを検査する（ステップＳ８０２）。これは原理的には、セキュリティゲートウェイが管理ネットワークに直接収容されている全てのホストのアドレスの一覧表を保持しており、それと比較することで行う。ホストのアドレスが統一的に付けられていれば、アドレスの一部を検査すればよい。例えば、直接収容しているホストのアドレスがある範囲内にあるように設定されていれば、送信元アドレスがその範囲かどうかを調べれば良い。

【００８８】

ステップＳ８０２の検査の結果、直接収容する管理ネットワーク外のホストからの送信であれば、受信パケットには認証コードが添付されているはずであるから、認証コードの検査処理であるステップＳ８０３からＳ８０６の処理を行う。一方、そうでない場合、認証コードは添付されていないのでので、ステップＳ８０７以降の処理に移る。

【００８９】

認証コードの検査処理においては、まず、認証コードがパケットに添付されているかどうかを調べる（ステップＳ８０３）。

【００９０】

認証コードが添付されていない場合には、不正な通信パケットと判断してエラー処理に移る（ステップＳ８１２）。エラー処理の一例は、受信パケットの転送を行わず、ログに記録を残すことである。

【００９１】

認証コードが添付されている場合には、認証コードの検査を行う（ステップＳ８０４）。このとき図６に示した認証鍵テーブルの送信元ホスト，受信先ホスト，コネクションＩＤのエントリを調べ、検査用の認証鍵を用いる。認証コードの検査の結果、異常があればエラー処理に移る（ステップＳ８１２）。異常がなければ、受信パケットは正常とみなす。なお、ステップＳ８０３からＳ８０５までの認証コードの検査は、認証鍵テーブルの該当エントリに登録されている検査用認証鍵の個数だけ行う。

【００９２】

そして、全ての認証コードが正当な場合のみステップＳ８０６に移り、ここで検査した全ての認証コードを除去する。

【００９３】

ここまででパケットの完全性（ホストアドレスやポート番号などが改ざんされておらず、正規の送信ホストからのものであること）が確認されたので、ステップＳ８０７のパケットフィルタリング処理を行う。

【００９４】

ステップＳ８０７のパケットフィルタリング処理では、送信側と受信側双方のホストアドレス、ポート番号などを基にパケットの通過を認めてよいかどうかを判定する。この判定は、例えば、フィルタリングのルールを記述したテーブルを用意し、そのルール群と逐一照合することで行う。フィルタリング処理で通過を許可されないパケットに対しては転送を行わず、その行為をログに残すなどの処理を行う。なお、前述したようにパケットフィルタリング部３０４は別装置の機能に委ねることも可能であり、この場合にはこの処理は省略される。

【００９５】

次に、受信先ホストのアドレスから、直接収容する管理ネットワーク内ホストへの受信パケットかどうかを判断する（ステップＳ８０８）。そうであれば、そのままパケットの

転送処理を行う（ステップＳ８１１）。

【００９６】

一方、直接収容する管理ネットワーク外のホストへの受信パケットの場合には、以下の認証コードの生成処理に移る。認証コードの生成では、認証鍵テーブルから証明用の認証鍵を求め、該当エントリに登録されている全ての認証鍵を用いた認証コードを生成し（ステップＳ８０９）、それらをパケットに添付する（ステップＳ８１０）。その後、パケット転送を行う（ステップＳ８１１）。

【００９７】

以上の説明では、認証コードの生成・検査において転送途中で変化する特定のエリア以外の全てのビットを対象に認証コードを計算することを想定した。これは必ずしも必要ではない。この実施形態では、エンド・ツー・エンドの認証コードとリンク・バイ・リンクの認証コードが併用されている。エンド・ツー・エンドでは送信されたパケットが１ビットも改変されることなく受信されたことを保証する必要があるが、リンク・バイ・リンクでは必ずしも全てのビットが改変なく受信されたことまで保証する必要はなく、そのパケットの転送に隣のセキュリティゲートウェイが関与したことを保証すれば十分であるとも考えられるからである。

【００９８】

このリンク・バイ・リンクの認証子の生成対象のデータを図４のフォーマットで説明すれば、送信元ホストアドレス（１５０１）、受信先ホストアドレス（１５０２）、コネクションＩＤ（１５０３）、さらにエンド・ツー・エンドの認証コード（１５０４）までを対象にすればよい。

【００９９】

また、図５のフォーマットで説明すると、認証ヘッダ１（図中のＡＨ１）がエンド・ツー・エンドの認証コードを含むため、この中の認証コードの計算はＩＰヘッダ２（図中のＩＰ２）、認証ヘッダ１（ただし認証コードのエリアは“０”で置き換える）、ＩＰヘッダ１（図中のＩＰ１）、データ部（図中のＤａｔａ）を対象とする。一方、認証ヘッダ２（図中のＡＨ２）はリンク・バイ・リンクの認証コードを含むが、この部分の認証コードの計算はＩＰヘッダ３（図中のＩＰ３）、認証ヘッダ２、認証ヘッダ１を対象にすればよい。この認証コード１、２とその保護対象のデータの関係を図９に示した。

【０１００】

なお、このときにリンク・バイ・リンクの認証コードによる保護の対象は、図９にハッチングして示した領域の全てを含まなければならない訳ではない。少なくとも含めなければならないのは、エンド・ツー・エンドの認証コードの保護の対象外であるＩＰヘッダ３と認証ヘッダ２である。さらに、エンド・ツー・エンドの認証コードの保護対象のデータのうち毎回変化するデータを含めなければならない。例えば、必ずカウントアップされるシーケンス番号や、あるいは十分な長さのランダムなデータである。十分な長さとは例えば１２８ビットである。エンド・ツー・エンドの認証コードは、実用上１２８ビットのランダムデータと見なすことが可能であるため、先の説明ではこの認証コードを含む認証ヘッダ１を対象に含めている。

【０１０１】

このようにした場合のパケット転送処理の一例を図７で説明すると、ＭＡＣ１、ＭＡＣ２、ＭＡＣ３、ＭＡＣ４の生成・検査が効率化され、パケット転送の効率化につながる効果がある。

【０１０２】

以上に示したメッジセージ認証コードの多重化は、この第１の実施形態のみならず以降で説明する第２の実施形態などにも適用可能である。

【０１０３】

次に、第２の実施形態について説明する。

【０１０４】

本実施形態では、セキュリティゲートウェイの構成は、送信元のネットワークに接続さ

れたセキュリティゲートウェイ（図１０）とそのパケットの転送経路上のセキュリティゲートウェイ（図１１）の２種類に分けられる。ただし、図１０の構成と図１１の構成の必要部分を融合させて一つのセキュリティゲートウェイとした構成も考えられ、その場合には図３と同様の構成になる。

【０１０５】

図１０に示したように本実施形態に係る送信元のセキュリティゲートウェイ５１０は、パケット受信部５０１、パケット転送部５０２、認証鍵管理部５０３、認証コード生成部５０４、パケット整形部５０５、パケットフィルタリング部５０６を備える。

【０１０６】

パケット受信部５０１は、セキュリティゲートウェイ５１０の保護するネットワークから発信されるパケットを受信する。

【０１０７】

パケットフィルタリング部５０６は、受信されたパケットに含まれる送信元ホスト識別情報，受信先ホスト識別情報，コネクションＩＤ、および認証コードを元にパケットの転送を認めるかどうかなどの制御を行う。

【０１０８】

認証鍵管理部５０３は、送信元ホスト識別情報，受信先ホスト識別情報，コネクションＩＤの３つ組データに対応する証明用認証鍵を登録したテーブルを管理する。このとき、同一の３つ組データに対し、生成用認証鍵が複数記憶されている点が特徴である。これらの証明用認証鍵は、パケットが通過するセキュリティゲートウェイと１つずつ共有されている。

【０１０９】

認証コード生成部５０４は、認証鍵管理部５０３から得た複数の証明用認証鍵を用いて、パケットの転送先での検査に用いられる複数の認証コードを生成する。

【０１１０】

パケット整形部５０５は、認証コード生成部５０４により得られる複数の認証コードを、転送経路での検査の順番に従ってパケットに添付する。

【０１１１】

パケット転送部５０２は、経路情報に基づいてパケットの転送を行う。

【０１１２】

図１１に示したように本実施形態に係る転送経路上のセキュリティゲートウェイ（送信元以外のもの）６１０は、パケット受信部６０１、パケット転送部６０２、認証鍵管理部６０３、認証コード検査部６０４、パケット整形部６０５、パケットフィルタリング部６０６を備える。

【０１１３】

パケット受信部６０１、パケット転送部６０２、パケットフィルタリング部６０６の構成・動作は、図１６および図１０と同様である。相違するのは、以下の点である。認証鍵管理部６０３が送信元ホストアドレス、受信先ホストアドレス、コネクションＩＤの３つ組データに対応する検査用認証鍵（１つ）を登録したテーブルを管理しており、認証コード検査部６０４はこの検査用認証鍵を用いてパケットに添付されている認証コードを検査する。パケット整形部６０５は、このセキュリティゲートウェイで検査された認証コード１つを除去する。

【０１１４】

なお、図１０と図１１の構成部分のうち、パケットフィルタリング部５０６や６０６はセキュリティゲートウェイとは別にパケットフィルタリング装置を用意し、セキュリティゲートウェイとパケットフィルタリング装置とが連係をとる形態にしても良い。この場合、パケットフィルタリング部５０６や６０６は不要となる。

【０１１５】

次に、本セキュリティゲートウェイを用いたパケット転送の流れを図１２を用いて説明する。

【０１１６】
前提として、パケット転送経路上のセキュリティゲートウェイであるＧＡ１１，ＧＡ１，ＧＡ，ＧＢ，ＧＢ１の間では次のように認証鍵を共有しているものとする。すなわち、ＧＡ１１とＧＡ１の間で認証鍵Ｋ１、ＧＡ１１とＧＡの間で認証鍵Ｋ２、ＧＡ１１とＧＢの間で認証鍵Ｋ３、ＧＡ１１とＧＢ１の間で認証鍵Ｋ４がそれぞれ共有される。
【０１１７】
セキュリティゲートウェイＧＡ１１は、受信したパケットに指定されている送信元ホストアドレス、受信先ホストアドレス、コネクションＩＤを調べ、対応する認証鍵Ｋ１でパケットの内容に相当するデータに対する認証コードＭＡＣ１を計算する。同様に、認証鍵Ｋ２，Ｋ３，Ｋ４を夫々用いて認証コードＭＡＣ２，ＭＡＣ３，ＭＡＣ４を計算する。これら４つの認証コードを全てパケットに添付して転送する。
【０１１８】
このパケットはルーティング処理に従って次のセキュリティゲートウェイＧＡ１に到着する。
【０１１９】
セキュリティゲートウェイＧＡ１では、受信したパケットに指定されている送信元ホストアドレス、受信先ホストアドレス、コネクションＩＤを調べ、対応する認証鍵Ｋ１により認証コードＭＡＣ１を検査する。ここで、認証コードＭＡＣ１が添付されていない場合やＭＡＣ１の正当性が確認されない場合にはエラー処理に移る。ＭＡＣ１の正当性が確認された場合には、パケットに添付されたＭＡＣ１を除去してパケットを転送する。
【０１２０】
以下、セキュリティゲートウェイＧＡ、ＧＢではセキュリティゲートウェイＧＡ１と同様に認証コードの検査と除去を行いながらパケットを転送する。異常がなければパケットはセキュリティゲートウェイＧＢ１に到達する。
【０１２１】
セキュリティゲートウェイＧＢ１では、ＭＡＣ４を認証鍵Ｋ４で検査し、これに異常がなければ、受信したパケットはホストＨ１を収容するネットワークから発信され、途中で改ざんされることなく受信されたことが確認される。最後にＭＡＣ４を除去したパケットをホストＨ２に転送することでパケットの転送は完了する。
【０１２２】
なお、本実施形態の変形例として、外部からの不正な侵入の防止だけを目的とする場合には、パケットの発信側のネットワークにおいて、セキュリティゲートウェイＧＡ１１とＧＡ１の間でのＭＡＣ１の生成・検査、およびセキュリティゲートウェイＧＡ１とＧＡの間でのＭＡＣ２の生成・検査は不要である。具体例としては、セキュリティゲートウェイＧＡ１１とＧＢが鍵Ｋ３を共有し、ＧＡ１１とＧＢ１が鍵Ｋ４を共有しておく。セキュリティゲートウェイＧＡ１１はパケットに対し、鍵Ｋ３で認証コードＭＡＣ３を、鍵Ｋ４で認証コードＭＡＣ４をそれぞれ生成し、パケットに添付して転送する。セキュリティゲートウェイＧＡ１とＧＡではパケットの方向だけを監視し、方向が外向きならばそのまま転送する。以下、セキュリティゲートウェイＧＢとＧＢ１の処理は元の実施形態と同じである。この場合には鍵Ｋ１とＫ２の共有が不要となる。
【０１２３】
さらに、元の実施形態や上記の変形例において、転送経路上のセキュリティゲートウェイにおいて、検査された認証コードの除去を行わない構成があげられる。この場合、検査された認証コードの除去は行わないため、パケットの長さは送信元のセキュリティゲートウェイ（図１２の例ではＧＡ１１）から受信先のセキュリティゲートウェイ（図１２の例ではＧＢ１）まで不変である。
【０１２４】
図１３にセキュリティゲートウェイ内の認証鍵管理部５０３，６０３に登録されている認証鍵テーブルの一例を示す。認証鍵テーブルには送信元ホストアドレス、受信元ホストアドレス、コネクションＩＤの組に対して検査用認証鍵と証明用認証鍵が登録される。検

査用認証鍵と証明用認証鍵のどちらか一方は常に空欄であるが、両方が空欄となることはない。すなわち、送信ホストが管理ネットワーク内にあれば検査用認証鍵は空欄となり、証明用認証鍵は一般に複数登録されるが、最大でも経路に存在する他のセキュリティゲートウェイの個数だけとなる。それ以外の場合で、自らのセキュリティゲートウェイが経路上にある場合には、検査用認証鍵が１つ登録される。

【０１２５】

以上に説明した第２の実施形態におけるセキュリティゲートウェイの処理手順を図１４に示した。

【０１２６】

本実施形態のセキュリティゲートウェイは、パケットを受信すると（ステップＳ９０１）、まず、パケットの送信元ホストアドレスを調べ、直接収容する管理ネットワーク内ホストからの送信かどうかを判断する（ステップＳ９０２）。

【０１２７】

直接収容する管理ネットワーク外のホストからの送信であれば、ステップＳ９０３からＳ９０６の認証コードの検査を行う。

【０１２８】

まず、受信パケットに認証コードが添付されているかどうかを調べる（ステップＳ９０３）。認証コードが添付されていない場合には、不正な通信パケットと判断してエラー処理に移る（ステップＳ９０９）。認証コードが添付されている場合には、認証コードの検査を行う（ステップＳ９０４）。このとき認証鍵テーブルの送信ホスト，受信ホスト，コネクションＩＤのエントリを調べ、検査用の認証鍵を用いる。認証コードの検査の結果異常があればエラー処理に移る（ステップＳ９０９）。異常がなければ受信パケットは正常とみなし、検査した認証コードを除去し（ステップＳ９０６）、パケットのフィルタリング処理を行なう（ステップＳ９０７）。フィルタを通過したパケットのみを転送する（ステップＳ９０８）。

【０１２９】

一方、ステップＳ９０２において直接収容する管理ネットワーク内ホストからの送信の場合には、さらに受信ホストも直接収容する管理ネットワーク内かどうかを判断する（ステップＳ９０７）。もしそうであれば管理ネットワーク内の通信パケットなのでセキュリティゲートウェイは何も処理を行わずに終了する。

【０１３０】

受信ホストが直接収容する管理ネットワークの外の場合には、まずパケットのフィルタリング処理を行なう（ステップＳ９１１）。フィルタを通過したパケットに対してステップＳ９１２からＳ９１３の認証コード生成処理を行う。このとき、図１３に示した認証鍵テーブルに記録された全ての認証鍵を用いて複数の認証コードを生成し（ステップＳ９１２）、生成した全ての認証コードをパケットに添付して（ステップＳ９１３）、パケットを転送する（ステップＳ９１４）。なお、先に説明したようにパケットフィルタリング部５０６，６０６は別装置の機能に委ねることも可能であり、この場合にはフィルタリング処理（ステップＳ９０７，Ｓ９１１）は省略される。

【０１３１】

次に、経路途上のセキュリティゲートウェイの処理量を削減する実施形態を幾つか説明する。

【０１３２】

図１５に、第３の実施形態におけるパケット転送の流れを示す。

【０１３３】

第３の実施形態は、第１の実施形態を変形したものに相当し、例えば図７の例において転送経路上のセキュリティゲートウェイ（ＧＡ１、ＧＡ、ＧＢ）で検査するための認証コード（これを通過用認証コードと呼ぶことにする）は全て同一とし、一方エンドのセキュリティゲートウェイでは別途エンド・ツー・エンドの認証コード（これを受信用認証コードと呼ぶことにする）を検査することにする。従って、例えば図１５のように、送信側ゲ

ートウェイであるＧＡ１１は証明用認証鍵Ｋ０とＫ１を所持し、宛先側ゲートウェイであるＧＢ１は検査用認証鍵Ｋ０（さらには検査用認証鍵Ｋ１）を所持し、経路途上のセキュリティゲートウェイであるＧＡ１、ＧＡ、ＧＢは検査用認証鍵Ｋ１を共有する。

【０１３４】

送信側ゲートウェイは、パケットに対し、受信用認証コードＭＡＣ０と通過用認証コードＭＡＣ１を生成し、パケットに添付して送信する。経路途上のセキュリティゲートウェイは通過用認証コードＭＡＣ１のみを検査し、検査に通ればそのままパケットを転送する。最後に受信側ゲートウェイは、受信用認証コードＭＡＣ０（さらには通過用認証コードＭＡＣ１）を検査し、検査に通れば認証コードを除去して受信ホスト宛に転送する。

【０１３５】

本実施形態では、送信側ゲートウェイは図１０と同じ構成であり、受信側ゲートウェイは図１１と同じ構成である。転送経路上のセキュリティゲートウェイは図１１においてパケット整形部６０５のない構成となる。

【０１３６】

図１６および図１７に、第３の実施形態によるセキュリティゲートウェイの処理手順を示す。

【０１３７】

本セキュリティゲートウェイは、パケットを受信すると（ステップＳ１３０１）、最初にパケットの送信元ホストアドレスを調べ、直接収容する管理ネットワーク内ホストからの送信かどうかを判断する（ステップＳ１３０２）。

【０１３８】

直接収容する管理ネットワーク外のホストからの送信であれば、以下の認証コードの検査処理を行う。

【０１３９】

まず、パケットの受信先ホストアドレスを調べ、直接収容する管理ネットワーク内ホストへの受信パケットかどうかを判断する（ステップＳ１３０３）。直接収容する管理ネットワーク内ホストへの受信パケットであれば、自装置は宛先側ゲートウェイであるから、ステップＳ１３０９からＳ１３１４までの受信用認証コードの検査処理を行う。受信用認証コードの検査処理では、最初に受信用認証コードの有無を検査し（ステップＳ１３０９）、受信用認証コードの検査を行う（ステップＳ１３１０）。これに異常がなければ認証コード（通過用も受信用も全て）を除去し（ステップＳ１３１２）、フィルタリング処理（ステップＳ１３１３）を行い、フィルタを通過したパケットのみを転送する（ステップＳ１３１４）。

【０１４０】

一方、直接収容する管理ネットワーク外ホストへのパケットであれば、自装置は経路上となるのでステップＳ１３０４からＳ１３０８までの通過用認証コードの検査処理を行う。通過用認証コードの検査処理では、最初に通過用認証コードの有無を検査し（ステップＳ１３０４）、通過用認証コードの検査（ステップＳ１３０５）を行う。これに異常がなければフィルタリング処理（ステップＳ１３０７）を行い、フィルタを通過したパケットのみを転送する（ステップＳ１３０８）。

【０１４１】

上記の認証コードの検査過程（ステップＳ１３０４，Ｓ１３０６，Ｓ１３０９，Ｓ１３１１）で異常が発見された場合は、エラー処理（ステップＳ１３２０）を行い、終了する。

【０１４２】

また、ステップＳ１３０２の判定において直接収容する管理ネットワーク内のホストからの送信であれば、受信アドレスを調べ、受信先も直接収容する管理ネットワーク内かどうかを調べる（ステップＳ１３１５）。もしそうであれば、直接収容する管理ネットワーク内での送受信であるので何もせずに終了する（ステップＳ１３２１）。

【０１４３】

受信先が直接収容する管理ネットワーク外であれば、自装置は送信側ゲートウェイであるからステップＳ１３１６からＳ１３１９までの認証コード生成処理を行う。まず、パケットのフィルタリング処理（ステップＳ１３１６）を行い、フィルタを通過したパケットに対して認証コードの生成処理を行う（ステップＳ１３１７）。そして、生成した認証コードをパケットに添付して（ステップＳ１３１８）、転送する（ステップＳ１３１９）。このとき、経路上に宛先側ゲートウェイ以外が存在しない場合以外は、２種類の認証コード（受信用認証コードと通過用認証コード）を生成する。

【０１４４】

なお、先に説明したようにパケットフィルタリング部は別装置の機能に委ねることも可能であり、この場合にはフィルタリング処理（ステップＳ１３０７，Ｓ１３１３、Ｓ１３１６）は省略される。

【０１４５】

第４の実施形態は、転送経路上のセキュリティゲートウェイの認証処理をさらに簡略化するものである。図１８にホストＨ１からホストＨ２へのパケット転送とそのときの認証処理を例示した。前提として、ホストＨ１，Ｈ２を収容する管理ネットワークのセキュリティゲートウェイＧＡ１１、ＧＢ１が認証鍵Ｋを共有しているものとする。また、各セキュリティゲートウェイは他のセキュリティゲートウェイのネットワーク上の位置を把握しており、受信先ホストアドレスからその管理ネットワークのセキュリティゲートウェイのアドレスの対応が分かるものとする。例えば、通信可能な全てのホストアドレスとそれに対応するセキュリティゲートウェイの一覧をテーブルに管理しているものとする。

【０１４６】

まず、ホストＨ１からパケットを受信したセキュリティゲートウェイＧＡ１１は受信先ホストアドレスＨ２からそれに対応するセキュリティゲートウェイＧＢ１のアドレスを求める。次に、パケット全体をデータとみなして、送信元アドレスとしてセキュリティゲートウェイＧＡ１１のアドレス、受信先アドレスとしてセキュリティゲートウェイＧＢ１のアドレスを添付したパケットを作成する。この処理はカプセル化と呼ばれる。さらに、認証鍵Ｋで元の受信パケットに対する認証コードを計算し、これをカプセル化したパケットに添付して転送する。

【０１４７】

パケットはルーティング処理によりセキュリティゲートウェイＧＡ１に到着するが、セキュリティゲートウェイＧＡ１では受信先のアドレスがセキュリティゲートウェイであることを認識すると、そのまま転送する。このパケットは同様にしてセキュリティゲートウェイＧＡ、ＧＢに到着するが、これらも受信先がセキュリティゲートウェイであればそのまま転送する。

【０１４８】

最後にカプセル化されたパケットの宛先であるセキュリティゲートウェイＧＢ１ではまず送信元アドレス、受信先アドレス、認証コードなどのヘッダを除去してデカプセル化を行い、その後のパケットに対して認証鍵Ｋで認証コードを検査する。認証に成功すればパケットを転送してホストＨ２に届ける。

【０１４９】

これは、宛先がセキュリティゲートウェイであれば、宛先側ゲートウェイでパケットの正当性が検査されるため、途中のセキュリティゲートウェイでは正当性の検査を簡略化したものである。

【０１５０】

ここで、複数のセキュリティゲートウェイの間で認証鍵を共有する方法の一例を示す。

【０１５１】

以下で説明する方法は公開鍵暗号をベースにしている。前提として、各セキュリティゲートウェイには固有の秘密鍵と公開鍵が割り当てられているものとする。また、各セキュリティゲートウェイはネットワーク内での全てのセキュリティゲートウェイの位置を把握しており、パケットを転送するにあたりどのセキュリティゲートウェイを経由して受信先

まで届くかが分かっているものとする。さらに、全てのセキュリティゲートウェイの公開鍵を登録したテーブルを所持しているものとする。

【０１５２】

このような前提の下で、送信側のセキュリティゲートウェイが認証鍵をランダムに決定し、受信側のセキュリティゲートウェイの公開鍵で暗号化したデータを作成し、パケットと一緒に転送する。受信側では自らの秘密鍵でこれを復号して認証鍵を得る。

【０１５３】

具体的には、第１の実施形態（図７）において、ＧＡ１１が認証鍵Ｋ０とＫ１を決定し、Ｋ０をＧＢ１の公開鍵で暗号化したデータＣＫ０と、Ｋ１をＧＡ１の公開鍵で暗号化したデータＣＫ１を計算し、これらをコネクション確立時の最初のパケットに添付して送信する。このパケットを受信したＧＡ１はＣＫ１を自分の秘密鍵で復号して認証鍵Ｋ１を得る。さらにＧＡ１は認証鍵Ｋ２をランダムに決定し、Ｋ２をＧＡの公開鍵で暗号化したデータＣＫ２を作成し、パケットからＣＫ１を削除しＣＫ２を添付して送信する。以上のことをセキュリティゲートウェイＧＢ１まで行えば図７に示したようにコネクションに対応した認証鍵が共有される。

【０１５４】

第２の実施形態（図１２）でも、ＧＡ１１が認証鍵Ｋ１，Ｋ２，Ｋ３，Ｋ４をランダムに決定し、これらを配布先のセキュリティゲートウェイの公開鍵で暗号化してコネクション確立のパケットに添付して転送すれば良い。このパケットを受信した各セキュリティゲートウェイは自分宛の暗号化データを自分の秘密鍵で復号して認証鍵を得る。

【０１５５】

第３の実施形態および第４の実施形態に関しても同様にして認証鍵を共有できる。

【０１５６】

なお、鍵共有の前提条件を緩和するためには、例えば経路上のゲートウェイ問い合わせプロトコルを用意すればよい。すなわち、送信パケットを受信したセキュリティゲートウェイＧＡ１１が、最初に経路上のゲートウェイ問い合わせ要求を受信先に向かって発信し、この問い合わせ要求を受信した経路上のセキュリティゲートウェイが自らの公開鍵とアドレスを問い合わせパケットに添付しながら転送し、最終的に問い合わせパケットを受け取ったセキュリティゲートウェイＧＢ１が、このパケット自体を応答として送信元のセキュリティゲートウェイＧＡ１１に向かって返すことにする。問い合わせ要求パケットを受信したセキュリティゲートウェイは、経路上の１つ手前のセキュリティゲートウェイのアドレスと公開鍵を認識できる。さらに、応答パケットをも受信することで、経路上の１つ先のセキュリティゲートウェイのアドレスと公開鍵も認識できる。

【０１５７】

以上の説明では、セキュリティゲートウェイと送受信ホストを区別してきたが、これを同一とする構成も可能である。すなわち、送受信パケットの認証機構を一般のホストに搭載することもできる。この場合には、パケット認証機構の保護対象はそれを搭載したホストとなる。例えば、これまでに説明した第１～第４の実施形態の場合、いずれにおいても送信側ゲートウェイ（図２におけるＧＡ１１）の機能をホストＨ１に、宛先側ゲートウェイ（図２におけるＧＢ１）の機能をホストＨ２に持たせれば良い。

【０１５８】

次に、図１９に送信側および受信側のパケット認証機構を搭載したホストの一構成を示す。

【０１５９】

本ホストは、アプリケーション処理部１６０１、トランスポート処理部１６０２、インターネットプロトコル（ＩＰ）処理部１６０３、パケット認証処理部１６０４、ネットワークインタフェース１６０５から構成される。このうち、１６０１～１６０３および１６０５はＴＣＰ／ＩＰによるプロトコルモジュールそのものである。

【０１６０】

パケット認証処理部１６０４は、認証コード検査部１６１１、受信パケット整形部１６

１２、認証鍵管理部１６１３、認証コード生成部１６１４、送信パケット整形部１６１５から構成される。

【０１６１】

パケット認証処理部の動作は、送信時の処理と受信時の処理の２つに分けられる。

【０１６２】

まず、上位層から要求のあったパケットに認証子を生成し、送信する処理においては、上位層からのパケットに添付されている送信先アドレスとコネクションＩＤにより認証鍵管理部１６１３のテーブルを検索し、そのエントリに登録されている全ての証明用認証鍵を用いてパケットに対する認証コードを生成し、それをパケットに添付する。

【０１６３】

一方、受信したパケットの認証を行ない、上位層に渡す処理においては、受信パケットに添付されている送信元アドレスとコネクションＩＤにより認証鍵管理部１６１３のテーブルを検索し、そのエントリに登録されている検査用認証鍵を用いて認証コードを検査する。認証に成功したパケットのみを上位層に渡す。認証に失敗したパケットに対してはエラー処理を行なう。

【０１６４】

このようにセキュリティゲートウェイ機能を送受信ホストにて動作させる構成は移動計算機を用いるモバイル・コンピューティングにおいて必須となる。このような状況での本実施形態のセキュリティゲートウェイの動作を以下で説明する。

【０１６５】

図１におけるホストＨ４が外部ネットに移動し、ホストＨ５の位置に移動したものとする。ホストＨ５の位置から元の組織Ａネットのあるホストと通信するためにはセキュリティゲートウェイＧＡを通過するためのパケット認証子を添付したパケットを生成しなければならない。外部ネットはセキュリティゲートウェイで保護されていないため、認証子の生成・検査は移動ホスト自身が行う必要がある。

【０１６６】

図２０におけるホストＨ４が組織Ｂネットのホスト Ｈ２の位置に移動し、組織Ａネットのホスト Ｈ３へパケットを送信する場合のセキュリティゲートウェイの動作例を示した。図２０の例は、ホストＨ４からセキュリティゲートウェイＧＡ１へのエンド・ツー・エンドの認証子ＭＡＣ０とリンク・バイ・リンクの認証子ＭＡＣ１をパケットに添付して送信する第１の実施例（図７）に相当するものである。図７との違いは送信ホストであるＨ４自身がパケット認証子を生成して送信する点にある。セキュリティゲートウェイＧＢ１にとっては、受信したパケットの送信ホストを認証する必要があり、このために移動ホストＨ４が認証子ＭＡＣ１を生成することを要求することになる。

【０１６７】

セキュリティゲートウェイが移動ホストをも収容する場合、その移動ホストの正当性が確認されることは、モバイル環境でのホストのなりすましを防ぐ上で極めて重要な意味を持つ。従って、本発明の骨子である、多数のセキュリティノードを介して安全にデータを転送する方法は、移動ホストの混在するイントラネット構築において効果的である。

【０１６８】

次に、本発明の他の実施形態に係るセキュリティゲートウェイの暗号処理機能について説明する。

【０１６９】

以下では、このセキュリティゲートウェイ（ファイアウォール）をデータ暗号化、復号化の制御方式とそれに伴うデータパケットの形式の相違をもとに４タイプに分け、各々の実現方法を説明する。

【０１７０】

（タイプ１）

まず、図２１と図２２を参照しながら、本実施形態に係るセキュリティゲートウェイの構成および動作について説明する。

【０１７１】
図２１に、本実施形態のセキュリティゲートウェイ（タイプ１）の基本構成を示す。図２１に示すように、タイプ１のセキュリティゲートウェイ２は、暗号化部１１、復号化部１２、暗号鍵記憶部１３、ホストアドレス管理部１４、ホストアドレス比較部１５を備える。
【０１７２】
図２２は、本セキュリティゲートウェイを通過するデータパケットの形式の一例を示す。データパケットは、送信元ホストアドレス（図中２１）、受信先ホストアドレス（２２）、データ属性（２３）、データ本体（２４）から構成される。送信元ホストアドレス（２１）は送信元ホスト計算機を、受信先ホストアドレス（２２）は受信先ホスト計算機を、それぞれ一意に示す識別子で、例えばネットワークアドレスを使用する。データ属性（２３）は、例えば複数のビットで構成されるフラグ情報である。なお、データ属性（２３）は、タイプ１のセキュリティゲートウェイでは使用しないので、ネットワーク内にタイプ１のセキュリティゲートウェイ２のみを設ける場合には、データ属性（２３）のフィールドは、他の用途で使用しない限り、不要である。
【０１７３】
図２１のセキュリティゲートウェイにおいて、暗号化部１１は、データ本体（２４）を暗号化する。復号化部１２は、データ本体（２４）を復号化する。暗号鍵記憶部１３は、データの暗号化、復号化に使用される暗号鍵の管理、記憶を行う。暗号鍵記憶部１３には、例えばシステム管理者によって必要な暗号鍵情報が格納される。ホストアドレス管理部１４は、自セキュリティゲートウェイに直接接続されているホスト計算機のホストアドレスを格納している。ホストアドレス比較部１５は、ホストアドレス管理部１４内に格納されているホスト計算機のホストアドレスと、データパケット内の送信元ホストアドレス（２１）および受信先ホストアドレス（２２）とを比較する。
【０１７４】
図２３に、本セキュリティゲートウェイがデータパケットを受けとった際の動作を示す。もしホストアドレス比較部１５にて送信元ホストアドレス２１の示すホスト計算機がホストアドレス管理部１４に登録されていると判断したなら（ステップＳ１１，Ｓ１２）、本セキュリティゲートウェイ２は暗号化部１１でデータ本体（２４）を暗号化する（ステップＳ１３）。そして、データパケットを次段に転送する（ステップＳ１７）。
【０１７５】
また、ホストアドレス比較部１５が、受信先ホストアドレス２２の示すホスト計算機がホストアドレス管理部１４に登録されていると判断したなら（ステップＳ１４，Ｓ１４）、復号化部１２でデータ本体（２４）を復号化する（ステップＳ１６）。そして、データパケットを次段に転送する（ステップＳ１７）。
【０１７６】
また、上記以外の条件の場合には、セキュリティゲートウェイ２はデータパケットに何も処理を行わず通過させる（ステップＳ１７）。
【０１７７】
なお、ホストアドレス管理部１４およびホストアドレス比較部１５でのアドレスの比較は、前述の方法の他に、このセキュリティゲートウェイの下位に構築されているサブネットワークアドレスをホストアドレス管理部１４に登録しておき、これとデータパケット内の送信元ホストアドレス２１および受信先ホストアドレス２２とを比較するといったように、他の構成を取ることも可能である。
【０１７８】
以上のような動作の結果、データパケットは、図２４に示すように、送信元ホスト３ｓを出て最初のセキュリティゲートウェイ２ｂで暗号化され、受信先ホストの直前のセキュリティゲートウェイ２ｔで復号化されることになる。すなわち、データは１回のみ暗号化、復号化され、一度セキュリティゲートウェイを通過した後は暗号化されていることになる。

【０１７９】
（タイプ２）
図２５に、本実施形態のセキュリティゲートウェイ（タイプ２）の基本構成を示す。タイプ２のセキュリティゲートウェイ２は、図２１の構成に暗号化判定部１６を付加したものである。
【０１８０】
本セキュリティゲートウェイを通過するデータパケットの形式の一例は、先に説明した図２２のものと同様である。
【０１８１】
本セキュリティゲートウェイは、上述したタイプ１のセキュリティゲートウェイと同様の機能を、図２２のデータ属性（２３）に基づく処理で実現したものである。すなわち、本実施形態では、データパケット内のデータ属性（２３）として１ビットの暗号化ビットをビット０（最下位ビット）に設け、その値が１の場合データは暗号化されており、０の場合は暗号化されていないこと（非暗号化）を示すものとする。暗号化判定部１６にて暗号化ビットが１か０かを調べることにより、容易に暗号化されているか否かを判定することができる。
【０１８２】
ここでは、各セキュリティゲートウェイは、暗号化されていないデータパケットが来た場合、ホストアドレス管理部１４を参照することなく、暗号化するようにしており、送信元を出て最初のセキュリティゲートウェイに到達した時点でデータは暗号化される。そして受信先ホストの１つ前のセキュリティゲートウェイではタイプ１と同様に、受信先ホストアドレス２２の示すホスト計算機がホストアドレス管理部１４に登録されているなら、復号化部１２でデータ本体２４を復号化する。本セキュリティゲートウェイは、先のタイプ１のものに比較し、ホストアドレス管理部１４の検索、データ内のホストアドレスとの比較処理が１回で済むので、より効率の良いデータ転送が期待できる。
【０１８３】
ただし、ここでは、データ転送の安全性を保持するために、データ暗号化ビットの転送途中での改ざんに対応することを考慮する。すなわち、転送経路でのデータ改ざんに対処するため、データを暗号化したセキュリティゲートウェイは、暗号化ビットを１にすると同時に、データパケット内の署名フィールドを自身の署名情報（例えば、デジタル署名）で置き換える。これは、例えばデータ属性（２３）の一部のフィールドを使用してもよいし、個別に設けてもよい。
【０１８４】
もし経路途中で、何者かによって本来０（未暗号化）のデータが１（暗号化）に改ざんされた場合、署名情報は元データのままであるので、次の段階のセキュリティゲートウェイはデータの矛盾を指摘でき、エラーとして転送を中止できる。よって未暗号化のデータをそのまま外部ネットワークに送出してしまう事態を回避できる。
【０１８５】
また、本来、１（暗号化）の暗号化ビットが０に改ざんされた場合、署名情報がないと、次の暗号化装置で２回目の暗号化が行われてしまう。このケースは情報が外に洩れることはないが、受信先で正しく復号できないという事態を招く。しかし、このケースもデフォルト以外の署名情報が付いているのに暗号化ビットが０であるという矛盾を検出することでエラー処理に入ることができる。
【０１８６】
以上のようなタイプ２のセキュリティゲートウェイの処理を図２６に示す。
【０１８７】
本セキュリティゲートウェイでは、データパケットを受け取ると（ステップＳ２０）、まず、暗号化判定部１６にて、暗号化ビットと署名情報を参照し、次のステップＳ２１，Ｓ２２，Ｓ２３，Ｓ２４の判断が行なわれる。
【０１８８】

暗号化ビットが０で意味のある署名情報がついているか（ステップＳ２１，Ｓ２３）、暗号化ビットが１で意味のある署名情報がついていない場合（ステップＳ２２，Ｓ２４）は、エラー処理となる（ステップＳ３０）。

【０１８９】

暗号化ビットが０で意味のある署名情報がついていない場合（ステップＳ２１，Ｓ２３）、データ本体（２４）を暗号化して（ステップＳ２５）、次段に転送する（ステップＳ２９）。

【０１９０】

暗号化ビットが１で意味のある署名情報がついている場合（ステップＳ２２，Ｓ２４）、受信先ホストアドレス（２２）がホストアドレス管理部１４内に登録されているか判定し（ステップＳ２６）、登録されているときは（ステップＳ２７）、データ本体（２４）を復号化して（ステップＳ２８）、次段に転送し（ステップＳ２９）、一方、登録されていないときは（ステップＳ２７）、何も処理をせずに、次段に転送する（ステップＳ２９）。

【０１９１】

ただし、この場合、暗号化ビットを１から０に変え、かつ、署名情報を取り去ってしまうような改ざんを受けてしまうと適当なエラー検出はできない。そのため、そのように改ざんされたデータをセキュリティゲートウェイが受けとると、そのデータに２度目の暗号化処理を施してしまうことになる。この場合、受け手が正しくデータ内容を得られない不具合が生じるが、データ内容の漏洩は起こらない。

【０１９２】

（タイプ３，タイプ４）

次に、タイプ３，タイプ４のセキュリティゲートウェイについて説明する。

【０１９３】

上記のタイプ１およびタイプ２のセキュリティゲートウェイの動作例では、図２４に示すように、転送されるデータが送信元、受信先の小組織のみの秘密情報であり、経路途中のいかなる他の部署（たとえ上位階層の部署であっても）にも開示されないことを保証するものであった。

【０１９４】

しかし、一般にネットワークを介して通信を行う場合、よりネットワークの外側でデータの暗号化、復号化を行いたい場合がある。

【０１９５】

ここでは、一例として、図２７に示すようなネットワークにおいて、マルチキャスト通信で複数の受信先にデータを通信する場合、具体的には、ホストｘから自組織内の他部署のホストａ、ｂと外部組織内のホストｃ、ｄ、ｅにデータを転送する場合を考える。

【０１９６】

この場合、自組織内では、送信元ホストから２つのセキュリティゲートウェイを通して接続されている部署ａ、ｂに同じデータを送信するので、暗号化はセキュリティゲートウェイＡ（送信元から３つめのセキュリティゲートウェイ）で行うようにすると、自組織内部署への送信は暗号化、復号化処理を行わずに高速に行うことができる。

【０１９７】

また、外部組織側では、セキュリティゲートウェイＢ（受信先ホストから２つめのセキュリティゲートウェイ）で復号化を一度行えば、部署ｃ、ｄ、ｅの各々の入口のセキュリティゲートウェイでの復号化処理を回避でき、やはり転送効率を高めることが可能である。

【０１９８】

この例における暗号化、復号化を行うセキュリティゲートウェイから送信元、受信先ホストへの経路数を暗号化、復号化レベルと定義し、所定の暗号化、復号化レベルのセキュリティゲートウェイで暗号化、復号化処理されることをユーザが指定する場合の構成、動作を考える。

【０１９９】
まず、タイプ３のセキュリティゲートウェイについて説明する。
【０２００】
図２８に、上記要求に応じるためのタイプ３のセキュリティゲートウェイの構成例である。図２８の各構成部分の基本的な機能は、図２１と同様である。
【０２０１】
各データパケットには図２９に示すようにデータ属性（図２２中の２３）内にそのデータパケットの発信者が要求する暗号化レベルおよび復号化レベルをコード化して与えておく。各セキュリティゲートウェイ内では、ホストアドレス管理部１４内の管理情報に、そのセキュリティゲートウェイから下位にある全てのホストアドレスおよびそれらのホストに到達するレベル数を記録しておく。例えば、図２７のセキュリティゲートウェイＡに含まれるセキュリティゲートウェイ内のホストアドレス管理部１４には、図２８に示すような情報が登録される。
【０２０２】
本セキュリティゲートウェイでは、これらのデータパケット内に与えられた暗号化、復号化レベル要求およびホストアドレス管理部１４内の情報を元に以下のように動作する。
【０２０３】
本セキュリティゲートウェイは、データパケットの送信元ホストがホストアドレス管理部１４に登録されており、かつ、そのホストのレベル数がデータパケット内に示された暗号化レベルに等しい場合に、暗号化部１１でデータの暗号化を行う。また、受信先ホストがホストアドレス管理部１４に登録されており、かつ、そのホストのネストレベルがデータパケット内に示された復号化レベルに等しい場合に、復号化部１２でデータの復号化を行う。従って、図２９に示す形式のデータパケットが図２７のネットワーク構成でホストｘから発信された場合、セキュリティゲートウェイＡで暗号化され、セキュリティゲートウェイＢで復号化されることになる。
【０２０４】
次に、タイプ４のセキュリティゲートウェイについて説明する。
【０２０５】
本セキュリティゲートウェイの構成は、図２８のタイプ３のものと同様である。ただし、本セキュリティゲートウェイでは、データパケット内の暗号化、復号化レベルを１つの共通の情報で扱うと仮定し、１つのデータフィールドを共有して使用する。従って、ここでは、扱うデータパケットの形式は図３０のようになる。
【０２０６】
各セキュリティゲートウェイでは、送信元ホストがホストアドレス管理部１４に登録されており、かつ、そのホストのレベル数がデータパケット内に示された暗号化、復号化レベルに等しい場合に暗号化部１１でデータの暗号化を行う。また、受信先ホストがホストアドレス管理部１４に登録されており、かつ、そのホストのレベル数がデータパケット内に示された暗号化、復号化レベルに等しい場合に復号化部１２でデータの復号化を行う。
【０２０７】
このタイプ３、タイプ４の２つの実施形態では、暗号化されていないデータがネットワークの複数のパスを通るので、タイプ１、２に比べセキュリティ的に劣ってしまうことが考えられる。また、データパケット内のデータについては、タイプ２で示した暗号化ビットの改ざんだけでなく、暗号化、復号化レベル情報も改ざんされる可能性があることを考慮しなくてはいけない。これを防ぐには、タイプ２で説明したと同様の、暗号化を行ったセキュリティゲートウェイの署名機構、データのチェック機構を付加し、各ネットワーク経路上でデータの整合性をチェックし、もし矛盾のあるデータパケットが入力された場合はエラー処理を行うようにすればよい。
【０２０８】
一例として図３１でホストｘから暗号化レベル３でデータが送出され、このデータがセキュリティゲートウェイＢ、Ｃ間で改ざんされ、暗号化レベルが２に変えられてしまう場

合を考える。この場合、セキュリティゲートウェイＡで暗号化されるはずであったにもかかわらず、セキュリティゲートウェイＡに到達するとホストｘはレベル３であるから自装置では暗号化しない、と判断してしまい、暗号化されていないデータが外部に洩れていってしまうことになる。ここで、タイプ２の実施形態で説明したような暗号化ビットと暗号化署名情報を使い、セキュリティゲートウェイＡで判定を行うと、そのような未暗号化情報の外部への漏洩が防止できる。すなわち、そのようなデータがセキュリティゲートウェイＡに到達した場合、暗号化署名情報が元データのままであるから、ネットワークの下位では暗号化されていないことになり、暗号化レベルの情報と矛盾する。また、暗号化ビットも１になっていないので、その点でも矛盾がある。従ってセキュリティゲートウェイＡはデータの内容が途中経路で改ざんされたと判定でき、エラー処理を行うことができる。

【０２０９】

以上は、暗号化レベルが小さく改ざんされた場合であるが、暗号化レベルが大きく改ざんされる場合（エラー判定しないと、２重の暗号化がされてしまう）も同様に処理できる。

【０２１０】

図３２には、改ざんに対処できるタイプ３、タイプ４のセキュリティゲートウェイでの判定処理を示す。なお、ここでは、図２５の暗号化判定部１６の判定処理を最初に行なうものとしている。

【０２１１】

本セキュリティゲートウェイでは、データパケットを受け取ると（ステップＳ４０）、まず、暗号化判定部１６にて、暗号化ビットと署名情報を参照し、次のステップＳ４１，Ｓ４２，Ｓ４３，Ｓ４６の判断が行なわれる。

【０２１２】

暗号化ビットが０で意味のある署名情報がついているか（ステップＳ４１，Ｓ４３）、暗号化ビットが１で意味のある署名情報がついていない場合（ステップＳ４２，Ｓ４６）は、エラー処理となる（ステップＳ５０）。

【０２１３】

暗号化ビットが０で意味のある署名情報がついていない場合（ステップＳ４１，Ｓ４３）、データの暗号化レベルが登録された送信ホストのレベル数と同じならば（ステップＳ４４）、ここで暗号化し（ステップＳ４７）、データの暗号化レベルが登録された送信ホストのレベル数より大きいならば（ステップＳ４５）、上位で暗号化し（ステップＳ４８）、データの暗号化レベルが登録された送信ホストのレベル数より小さいならば、エラー処理となる（ステップＳ５０）。

【０２１４】

暗号化ビットが１で意味のある署名情報がついている場合（ステップＳ４２，Ｓ４６）、既に暗号化完了と判断する（ステップＳ４９）。

【０２１５】

なお、ステップ４７のようにここで暗号化すると判定された場合、暗号化した後に次段に転送する。また、ステップ４８のように上位で暗号化すると判定された場合、またはステップ４９のように既に暗号化完了と判定された場合、何も処理せずに次段に転送する。

【０２１６】

本実施形態では、暗号化ビットの改ざんについてはタイプ２のセキュリティゲートウェイの場合と同様に処理することができる。

【０２１７】

ここで、暗号化、復号化レベル情報や暗号化ビットなどの制御情報に、データ本体（２４）とは別の暗号化を行い、実際に暗号化、復号化を行うセキュリティゲートウェイのみがこれらの情報を復号化できるようにして、よりセキュリティを高めることも可能である。

【０２１８】

なお、タイプ３、４の実施形態における暗号化鍵の配布については、転送経路の全ての

ノード間で暗号化鍵を予め交換しておく方法や、転送要求が発生した際にデータ転送の前に送信元と受信先の間で鍵の交換を行うなどの方法が考えられるが、適当な方法を選択して行うものと仮定する。

【０２１９】

さらに、本実施形態では、パケット暗号処理機能はセキュリティゲートウェイに一体化されているが、送信ホストもしくは受信ホストにもパケット暗号処理機能を内蔵することも可能である。特に、移動計算機を用いるモバイル・コンピューティング環境で必要となる。例えば、図１におけるホストＨ４が外部ネットに移動し、ホストＨ５の位置に移動したものとする。外部ネットはセキュリティゲートウェイで保護されていないため、送信パケットの暗号化および受信パケットの復号を移動ホスト自身が行う必要がある。

【０２２０】

パケット暗号処理機能を送受信ホストに搭載した一構成例としては、図１７において認証コード検査部（１６１１）をパケット復号部に、認証鍵管理部（１６１３）を暗号鍵管理部に、認証コード生成部（１６１４）をパケット暗号化部に、それぞれ置き換えたものとなる。

【０２２１】

第１～第４の実施形態で説明した認証処理機能に係る発明と他の実施形態で説明した暗号処理機能に係る発明とは、独立実施可能である。すなわち、ゲートウェイにいずれかの認証処理機能およびいずれかの暗号処理機能の一方を設けてセキュリティゲートウェイとすることも、ゲートウェイにいずれかの認証処理機能およびいずれかの暗号処理機能の両方を設けてセキュリティゲートウェイとすることも可能である。

【０２２２】

また、本実施形態では、全ゲートウェイに認証処理機能および／または暗号処理機能を設けてセキュリティゲートウェイとしているが、本発明を適用するネットワークに応じて、認証処理機能および／または暗号処理機能を設けないセキュリティゲートウェイが一部存在していても構わない。

【０２２３】

また、本実施形態の各セキュリティゲートウェイの機能や計算機の機能は、プログラムとして実現することが可能である。

【０２２４】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【図面の簡単な説明】

【０２２５】

【図１】本発明の実施の形態に係るセキュリティゲートウェイが用いられる計算機ネットワークの一構成例を示す図

【図２】図１の計算機ネットワークにおけるパケットの流れの一例を説明するための図

【図３】本発明の第１の実施形態に係るセキュリティゲートウェイの構成を示す図

【図４】パケットフォーマットの一例を示す図

【図５】パケット認証機能を実施するためのパケットフォーマットの一例を示す図

【図６】同本実施形態における認証鍵テーブルの一例を示す図

【図７】同本実施形態の動作を説明するための図

【図８】同本実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート

【図９】メッセージ認証子の多重化を効率化する方法におけるメッセージ認証子の計算対象データの一例を示す図

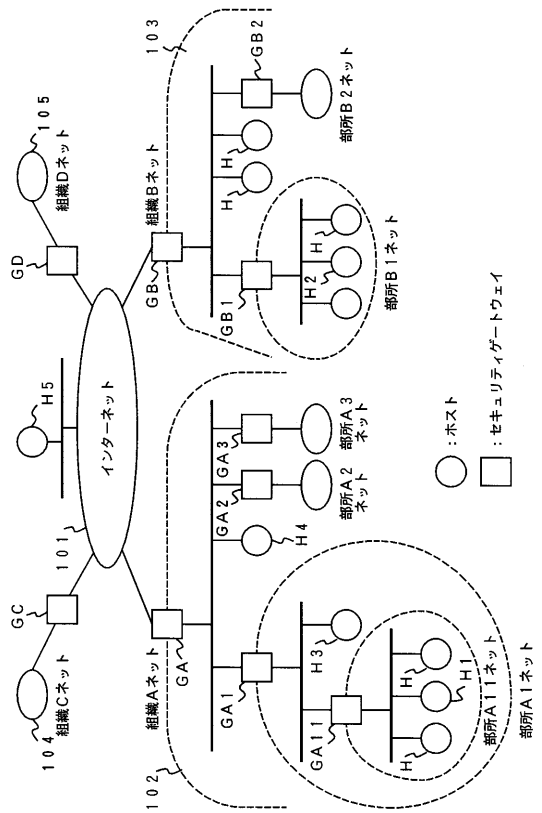
【図１０】本発明の第２の実施形態に係る送信側のセキュリティゲートウェイの構成を示す図

【図１１】同実施形態に係る転送経路上のセキュリティゲートウェイの構成を示す図

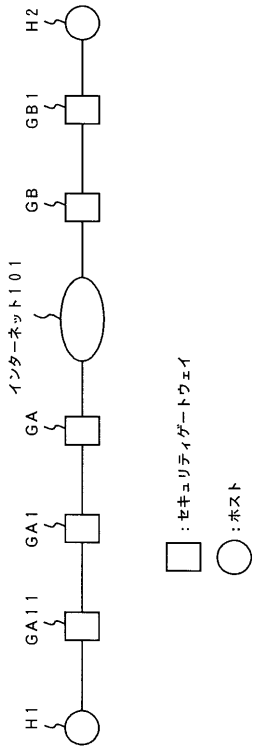
【図１２】同実施形態の動作を説明するための図

【図１３】同本実施形態における認証鍵テーブルの一例を示す図
【図１４】同本実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート
【図１５】本発明の第３の実施形態の動作を説明するための図
【図１６】同実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート
【図１７】同実施形態におけるセキュリティゲートウェイの処理手順を示すフローチャート
【図１８】本発明の第４の実施形態の動作を説明するための図
【図１９】パケット認証機構を送受信ホストに搭載した場合の構成を示す図
【図２０】移動計算機を送信ホストとした場合のパケット認証機能の動作を説明するための図
【図２１】本発明の他の実施形態に係るセキュリティゲートウェイ（タイプ１）の基本構成を示す図
【図２２】同実施形態におけるデータパケットの一形式を示す図
【図２３】同実施形態に係るセキュリティゲートウェイ（タイプ１）がデータパケットを受けとった際の動作手順を示すフローチャート
【図２４】同実施形態に係るセキュリティゲートウェイにより実現される暗号化通信を示す概念図
【図２５】データ属性に基づいて暗号化処理を行うセキュリティゲートウェイ（タイプ２）の基本構成を示す図
【図２６】同実施形態に係るセキュリティゲートウェイ（タイプ２）がデータパケットを受けとった際の動作手順を示すフローチャート
【図２７】同実施形態に係るセキュリティゲートウェイによりマルチキャスト通信を行う際のネットワーク基本構成およびデータ転送形態の一例を示す図
【図２８】ユーザが暗号化、復号化レベルを個別に指定するセキュリティゲートウェイ（タイプ３）の基本構成を示す図
【図２９】同実施形態に係るセキュリティゲートウェイ（タイプ３）におけるデータパケットのデータ属性の一形式を示す図
【図３０】同実施形態に係るセキュリティゲートウェイ（タイプ４）におけるデータパケットのデータ属性の一形式を示す図
【図３１】暗号化レベル情報が改ざんされる場合を説明するための図
【図３２】同実施形態に係るセキュリティゲートウェイ（タイプ３，タイプ４）で暗号化レベル情報の改ざんの有無を判定するための処理の流れを示すフローチャート
【符号の説明】
【０２２６】
１０１…インターネット、１０２…組織Ａネットワーク、１０３…組織Ｂネットワーク、１０４…組織Ｃネットワーク、１０５…組織Ｄネットワーク、３０１，５０１，６０１…パケット受信部、３０２，６０４…認証コード検査部、３０３，５０３，６０３…認証鍵管理部、３０４，５０６，６０６…パケットフィルタリング部、３０５，５０４…認証コード生成部、３０６，５０５，６０５…パケット整形部、３０７，５０２，６０２…パケット転送部、ＧＡ，ＧＡ１，ＧＡ１１，ＧＢ，ＧＢ１，ＧＣ，ＧＤ，３１０…セキュリティゲートウェイ、５１０…（送信元）セキュリティゲートウェイ、６１０…（転送経路上）セキュリティゲートウェイ、１５０１…送信元ホストアドレス、１５０２…受信先ホストアドレス、１５０３…コネクションＩＤ、１５０４…認証コード、１５０５…データ部、Ｈ，Ｈ１，Ｈ２，Ｈ３，Ｈ４…ホスト、２，２ａ，２ｂ，２ｔ…セキュリティゲートウェイ、３，３ｓ，３ｄ，ｈｏｓｔ ａ～ｈｏｓｔ ｅ，ｈｏｓｔ ｖ～ｈｏｓｔ ｘ…ホスト、１１…暗号化部、１２…復号化部、１３…暗号鍵記憶部、１４…ホストアドレス管理部、１５…ホストアドレス比較部、１６…暗号化判定部、２１…送信元ホストアドレス、２２…受信先ホストアドレス、２３…データ属性、２４…データ本体

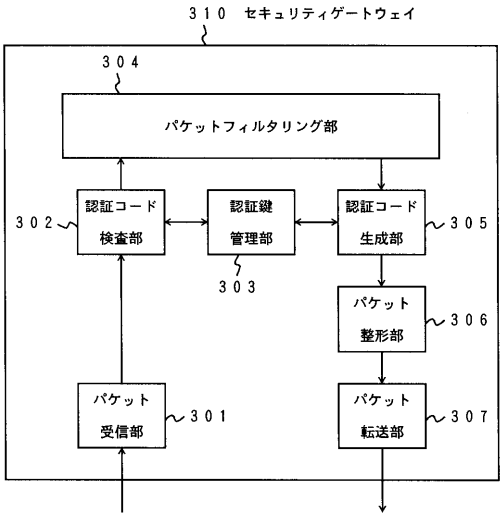
【図１】



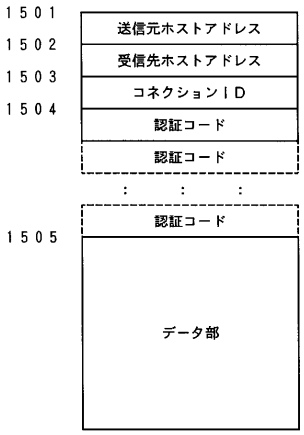
【図２】



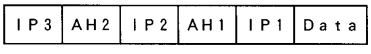
【図３】



【図４】



【図５】



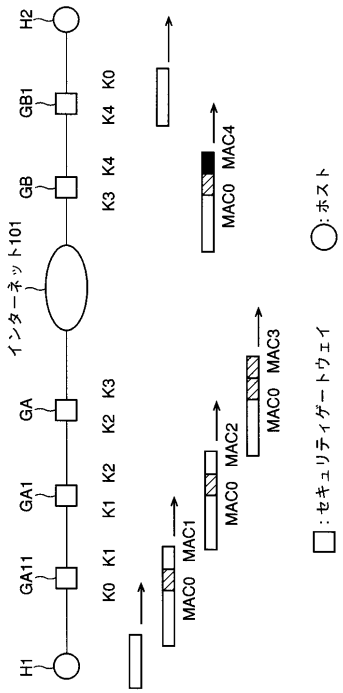
ＩＰ：ＩＰヘッダ

ＡＨ：認証ヘッダ

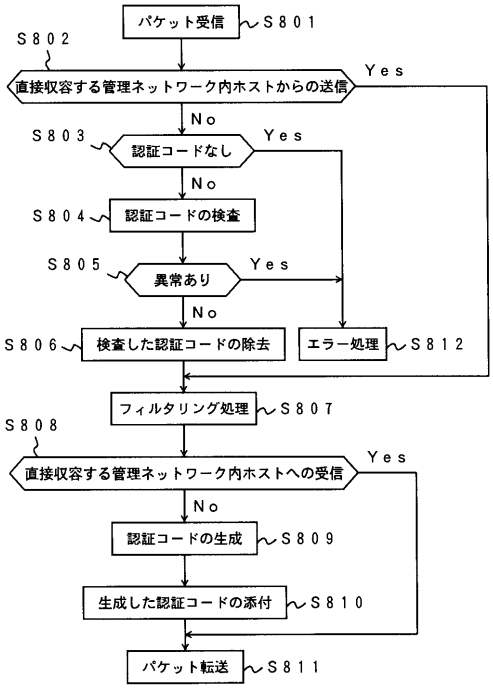
【図６】

送信元ホストアドレス	受信先ホストアドレス	コネクションＩＤ	検査用認証鍵	証明用認証鍵
Ｈ１	Ｈ２	ＩＤ１	Ｋ１	Ｋ２
Ｈ３	Ｈ２	ＩＤ１	…	Ｋ３，Ｋ４
Ｈ１	Ｈ４	ＩＤ２	Ｋ５	Ｋ６
Ｈ５	Ｈ３	ＩＤ３	Ｋ７，Ｋ８	…

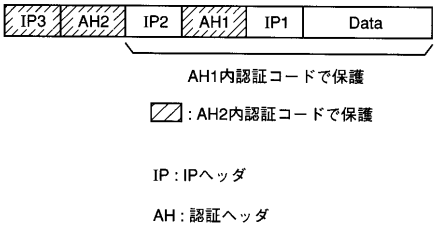
【図７】



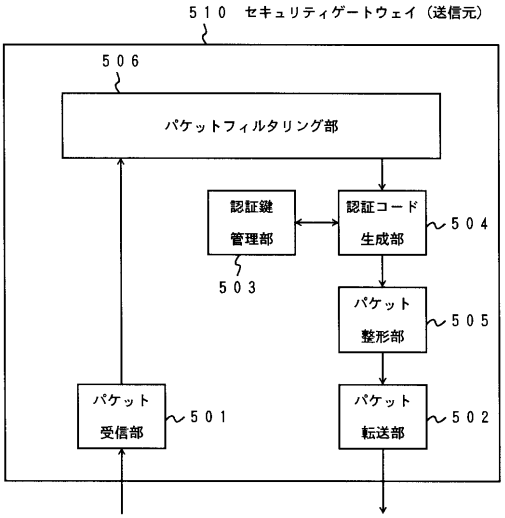
【図８】



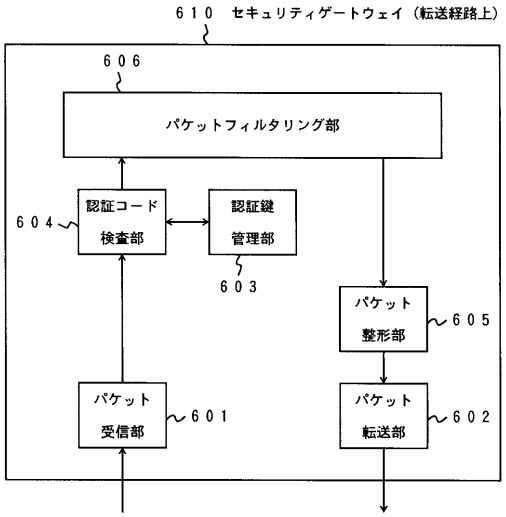
【図９】



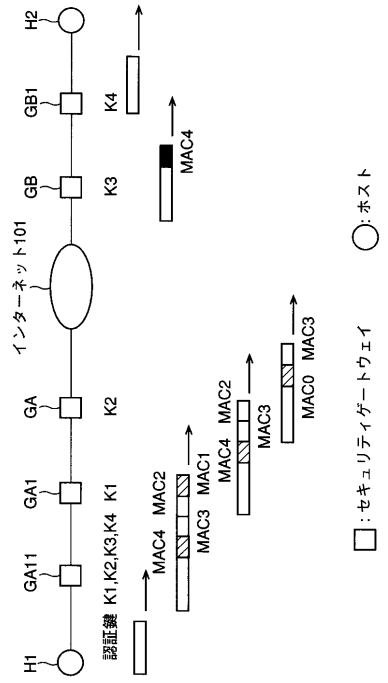
【図１０】



【図１１】



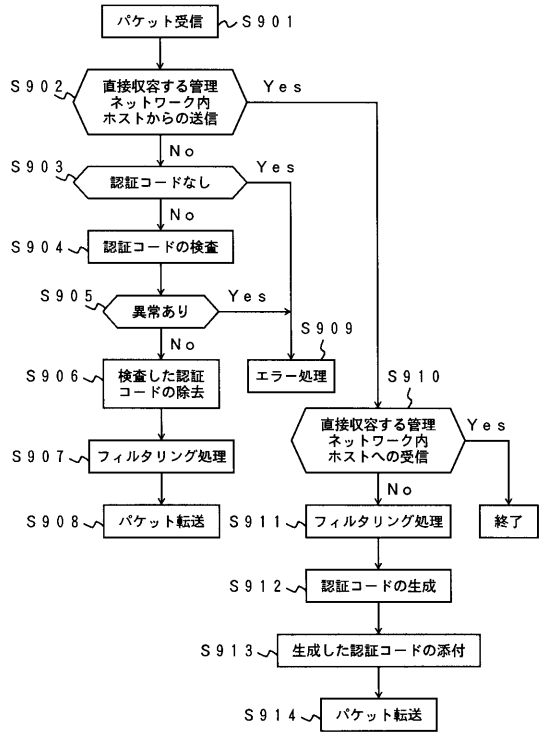
【図１２】



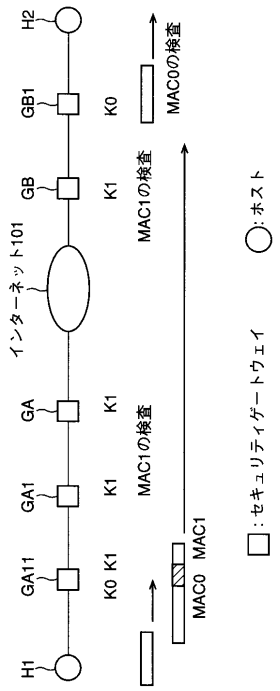
【図１３】

送信元ホストアドレス	受信先ホストアドレス	コネクションＩＤ	検査用認証鍵	証明用認証鍵
Ｈ１	Ｈ２	ＩＤ１	Ｋ１	…
Ｈ３	Ｈ２	ＩＤ１	…	Ｋ2, Ｋ3, Ｋ4, Ｋ5
Ｈ１	Ｈ４	ＩＤ２	Ｋ６	…
Ｈ５	Ｈ３	ＩＤ３	Ｋ７	…

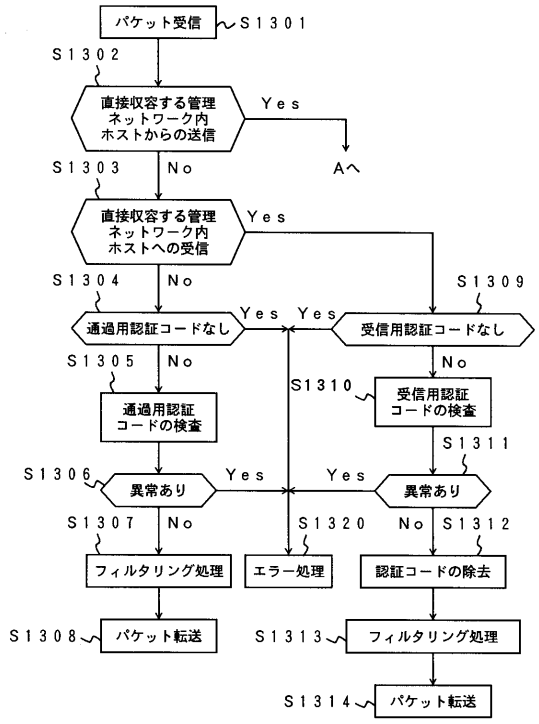
【図１４】



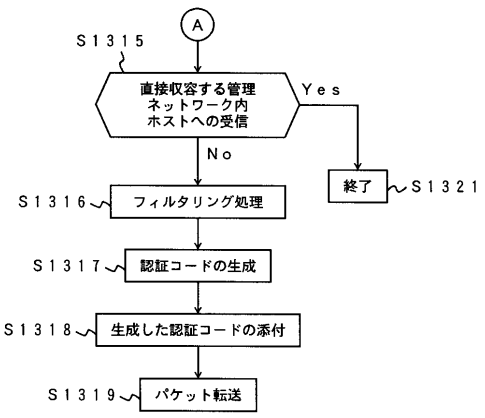
【図１５】



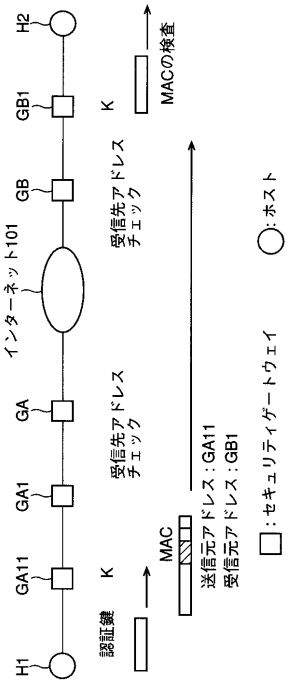
【図１６】



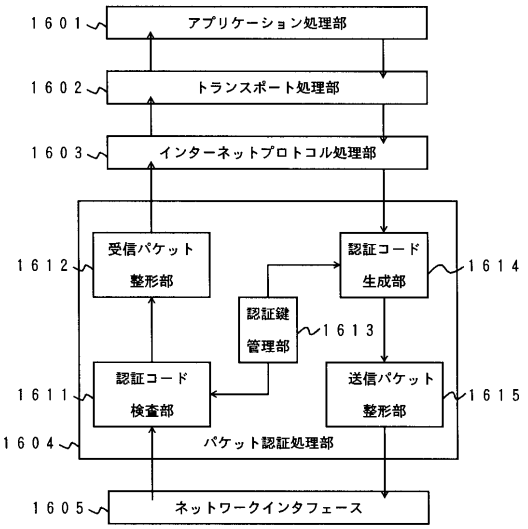
【図１７】



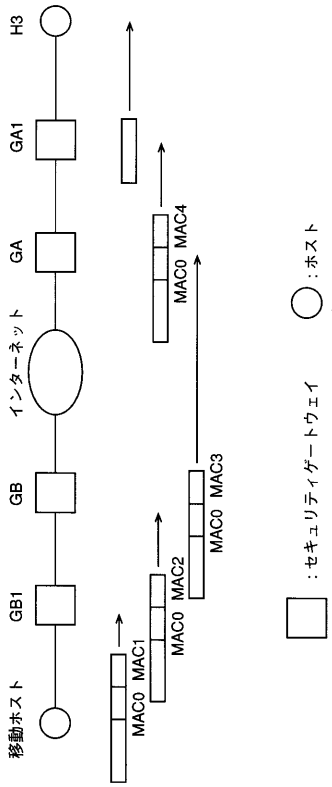
【図１８】



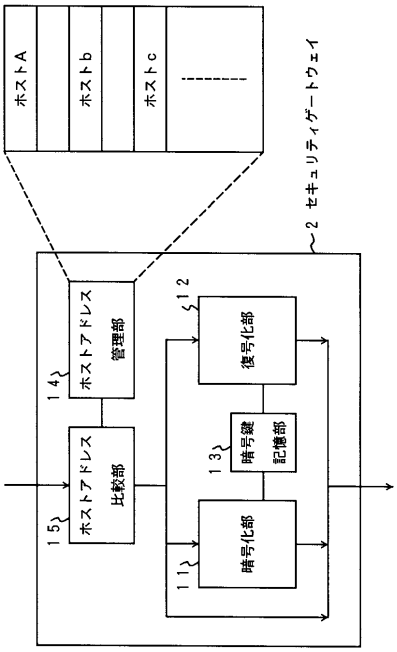
【図１９】



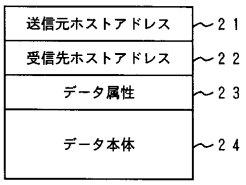
【図２０】



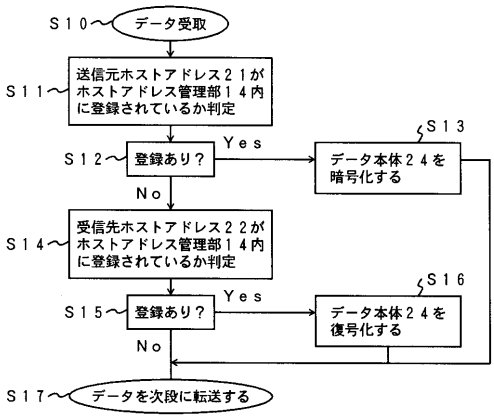
【図２１】



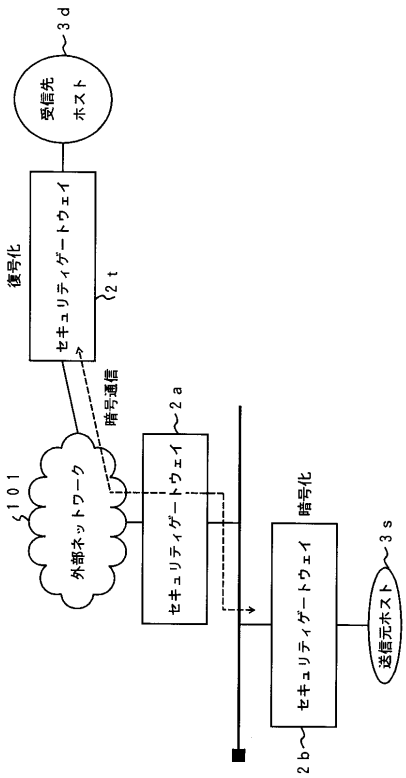
【図２２】



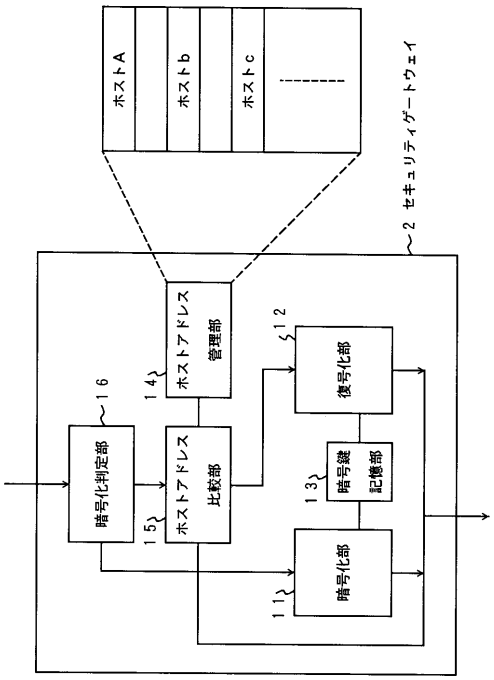
【図２３】



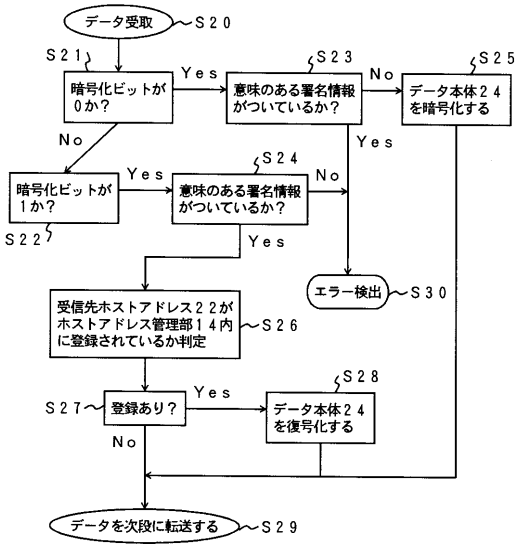
【図２４】



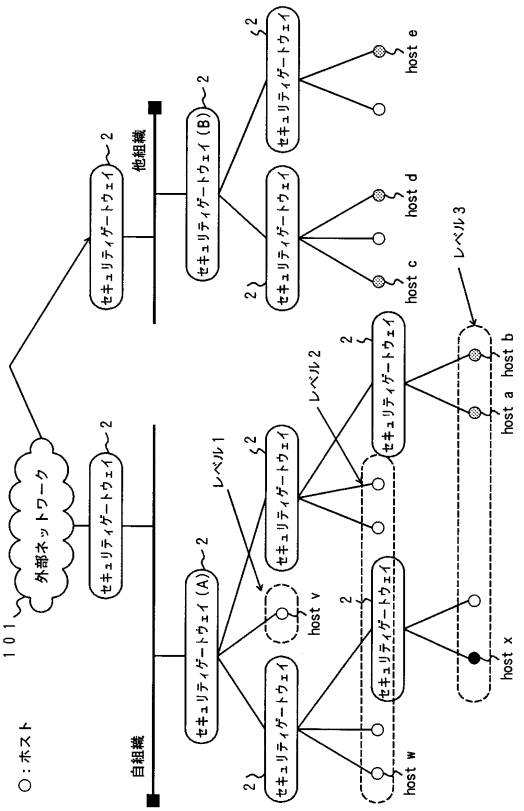
【図２５】



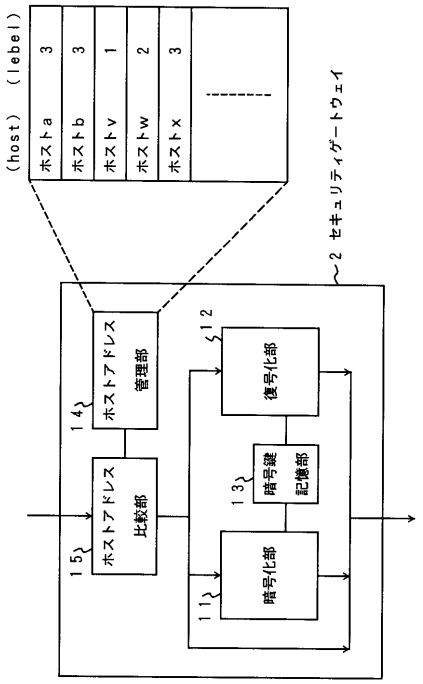
【図２６】



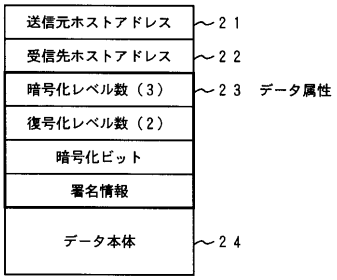
【図２７】



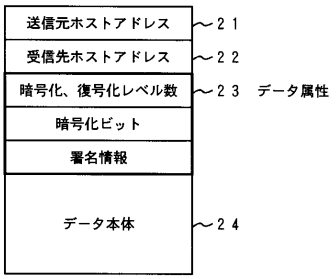
【図２８】



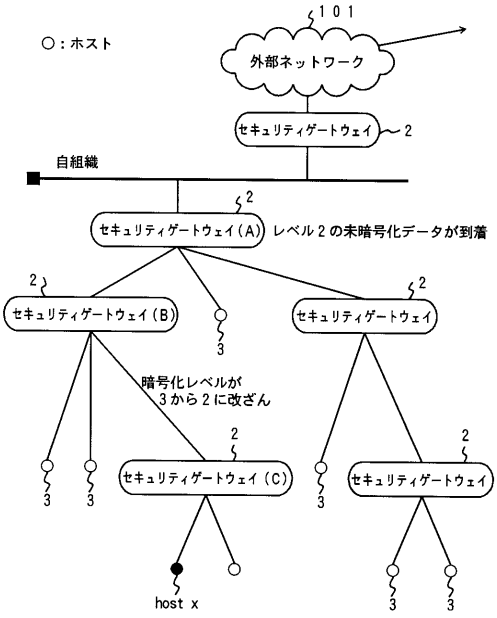
【図２９】



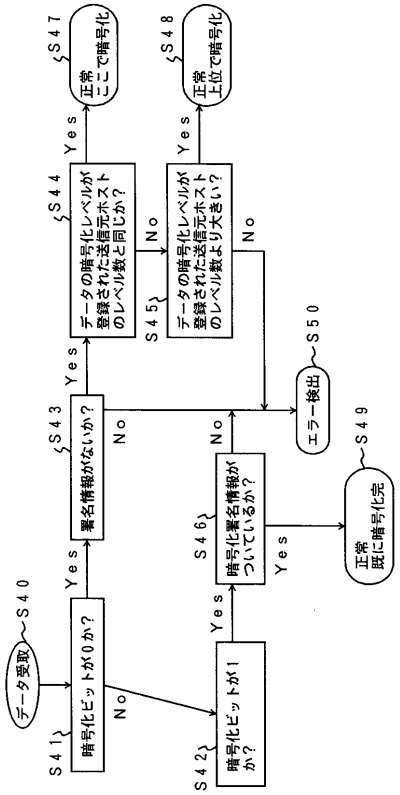
【図３０】



【図３１】



【図３２】


データ受取
S40
暗号化ビットが0か？
S41
Yes
No
署名情報がないか？
S43
Yes
No
データの暗号化レベルが登録された送信元ホストのレベル数と同じか？
S44
Yes
No
正常ここで暗号化
S47
データの暗号化レベルが登録された送信元ホストのレベル数より大きい？
S45
Yes
No
正常上位で暗号化
S48
暗号化ビットが1か？
S42
Yes
No
暗号化署名情報がついているか？
S46
Yes
No
エラー検出
S50
正常既に暗号化完
S49

フロントページの続き

(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎
(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　井上　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

審査官　速水　雄太

(56)参考文献　特開平０７－１０７０８２（ＪＰ，Ａ）
特開平０７－１７０２８０（ＪＰ，Ａ）
特開平０９－０２７８０４（ＪＰ，Ａ）
特開平０６－０７７９５４（ＪＰ，Ａ）
米国特許第０５４４４７８２（ＵＳ，Ａ）
妹尾尚一郎，馬場義昌，渡辺晃，厚井裕司，ネットワークセキュリティのためのパケット暗号化方式に関する一考察，第５１回（平成７年後期）全国大会講演論文集（１） 基礎理論及び基礎技術　ネットワーク　教育　応用，社団法人情報処理学会，１９９５年　９月２２日，第２３１－２３２頁
John Ioannidis, Matt Blaze, The Architecture and Implementation of Network-Layer Security Under Unix, 4th UNIX Security Symposium, １９９３年１０月，ＵＲＬ，http://citeseer.ist.psu.edu/371795.html

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３６