(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3557056号

(P3557056)

(45)発行日　平成16年8月25日(2004.8.25)　(24)登録日　平成16年5月21日(2004.5.21)

(51)Int.Cl.[7]	F I		
H04L 12/66	H04L	12/66	B
G06F 13/00	G06F	13/00	351M
G09C 1/00	G09C	1/00	640Z
H04L 12/56	H04L	12/56	100Z

請求項の数 11　(全 20 頁)

(21)出願番号　特願平8-283992
(22)出願日　平成8年10月25日(1996.10.25)
(65)公開番号　特開平10-136014
(43)公開日　平成10年5月22日(1998.5.22)
審査請求日　平成14年3月18日(2002.3.18)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100068814
弁理士　坪井　淳
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】パケット検査装置、移動計算機装置及びパケット転送方法

(57)【特許請求の範囲】

【請求項１】

自装置の管理するネットワークの内部の計算機がネットワーク外の計算機へ向けて送信するパケットを検査するパケット検査装置であって、

自装置の管理対象となる計算機以外の移動計算機から送信されたパケットに含まれる移動計算機識別情報に基づき、該移動計算機から送信されたパケットのネットワーク外への転送の可否を判定する判定手段と、

この判定手段により転送を拒否すると判定した場合に、前記移動計算機に転送拒否を示すメッセージを返信する手段と、

前記移動計算機から移動計算機識別情報を生成するための鍵情報を要求するメッセージを受信した場合に、該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する手段とを具備したことを特徴とするパケット検査装置。

【請求項２】

自装置がどの計算機を管理するかを示す管理対象計算機認識手段をさらに備え、

前記判定手段は、この管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理する計算機から送信されたものであることが示される場合は、該パケットをそのまま転送することを許可すると判定することを特徴とする請求項１に記載のパケット検査装置。

【請求項３】

自装置がどの計算機を管理するかを示す管理対象計算機認識手段をさらに備え、
前記判定手段は、この管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、このパケットが移動計算機識別子を含まない場合は、該パケットの転送を拒否すると判定することを特徴とする請求項１に記載のパケット検査装置。

【請求項４】

自装置がどの計算機を管理するかを示す管理対象計算機認識手段をさらに備え、
前記判定手段は、この管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、該パケットが移動計算機識別子を含む場合、該移動計算機識別子から該計算機の正当性が確認されたときのみ、該パケットを転送すると判定することを特徴とする請求項１に記載のパケット検査装置。

【請求項５】

相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機であって、
自装置が現在位置するネットワーク以外のネットワークに、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置が存在する場合に、該移動計算機管理装置へ向けて自装置の現在位置情報を含む登録メッセージを送信する第１の送信手段と、
自装置が現在位置するネットワーク内部から該ネットワーク外へのパケットを検査するパケット検査装置から、この第１の送信手段により送信された登録メッセージのパケット転送拒否を示すメッセージが返信された場合に、該パケット検査装置に移動計算機識別情報を生成するための鍵情報を要求する要求メッセージを送信する第２の送信手段と、
この第２の送信手段により送信された要求メッセージに応答して、前記パケット検査装置から鍵情報が返送された場合に、この鍵情報に基づいて生成した移動計算機識別情報を自装置が現在位置するネットワーク外へ向けて送信すべきパケットに付加して送信する第３の送信手段とを具備したことを特徴とする移動計算機装置。

【請求項６】

前記第３の送信手段は、前記移動計算機管理装置へ向けて、自装置の現在位置情報を含む登録メッセージを、前記移動計算機識別情報を付加して送信し、該移動計算機管理装置からの登録メッセージに対する受諾応答を受信した後、通信相手となる計算機へのデータパケットを、前記移動計算機識別情報を付加して送信するものであることを特徴とする請求項５に記載の移動計算機装置。

【請求項７】

前記第３の送信手段は、前記第１の送信手段により送信された前記登録メッセージのパケット転送拒否を示すメッセージが前記パケット検査装置から返信されなかった場合には、通信相手となる計算機へのデータパケットを、前記移動計算機識別情報を付加せずに送信することを特徴とする請求項５に記載の移動計算機装置。

【請求項８】

自装置の管理するネットワークの内部の計算機がネットワーク外の計算機へ向けて送信するパケットを検査するパケット検査装置のパケット転送方法であって、
自装置の管理対象となる計算機以外の移動計算機から送信されたパケットに含まれる移動計算機識別情報に基づき、該移動計算機から送信されたパケットのネットワーク外への転送の可否を判定し、
転送を拒否すると判定した場合に、前記移動計算機に転送拒否を示すメッセージを返信し、
前記移動計算機から移動計算機識別情報を生成するための鍵情報を要求するメッセージを受信した場合に、該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を該移動計算機へ返送することを特徴とするパケット転送方法。

【請求項９】
前記パケット検査装置は、自装置がどの計算機を管理するかを示す管理対象計算機認識手段を具備するものであり、
前記判定にあたっては、前記管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、該パケットが移動計算機識別子を含む場合、該移動計算機識別子から該計算機の正当性が確認されたときのみ、該パケットを転送すると判定することを特徴とする請求項８に記載のパケット転送方法。
【請求項１０】
相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機のパケット転送方法であって、
自装置が現在位置するネットワーク以外のネットワークに、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置が存在する場合に、該移動計算機管理装置へ向けて自装置の現在位置情報を含む登録メッセージを送信し、
自装置が現在位置するネットワーク内部から該ネットワーク外へのパケットを検査するパケット検査装置から、前記登録メッセージに対するパケット転送拒否を示すメッセージが返信された場合に、該パケット検査装置に移動計算機識別情報を生成するための鍵情報を要求する要求メッセージを送信し、
この要求メッセージに応答して、前記パケット検査装置から鍵情報が返送された場合に、この鍵情報に基づいて生成した移動計算機識別情報を自装置が現在位置するネットワーク外へ向けて送信すべきパケットに付加して送信することを特徴とするパケット転送方法。
【請求項１１】
前記移動計算機管理装置へ向けて送信された前記登録メッセージのパケット転送拒否を示すメッセージが前記パケット検査装置から返信されなかった場合には、前記自装置が現在位置するネットワーク外へ向けて送信すべきパケットであって通信相手となる計算機へのデータパケットを、前記移動計算機識別情報を付加せずに送信することを特徴とする請求項５に記載の移動計算機装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワーク内部から外に向けて転送されようとするパケットを検査するパケット検査装置及び相互に接続されたネットワーク間を移動して暗号通信を行うことが可能な移動計算機装置並びにそれらのパケット転送方法に関する。
【０００２】
【従来の技術】
計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、１組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（Ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。
【０００３】
また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持った

ユーザがネットワーク上を移動して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【０００４】

一般に移動通信を行う場合、移動計算機が所属していたネットワークに移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機が移動した場合、このホームエージェントに対して現在位置を示す登録メッセージを送る。登録メッセージが受け取られたら、移動計算機宛データの送信はそのホームエージェントを経由して、移動計算機の元のアドレス宛のＩＰパケットを移動ＩＰの現在位置アドレス宛パケット内にカプセル化することで移動計算機に対するデータの経路制御が行われる。例えば、図１５では、元々ホームネットワーク１ａに属していた移動計算機２が、他のネットワーク１ｂに移動し、ネットワーク１ｃ内の他の計算機（ＣＨ）３との間で通信を行う場合に、移動計算機２に対しホームエージェント５（ＨＡ）が上記の役割を行う。この方式は、インターネットの標準化団体であるＩＥＴＦのｍｏｂｉｌｅ－ＩＰワーキンググループで標準化が進められている移動ＩＰと呼ばれる方式である（文献：ＩＥＴＦ　ｉｎｔｅｒｎｅｔ　ｄｒａｆｔ，　ＩＰ　ｍｏｂｉｌｉｔｙ　ｓｕｐｐｏｒｔ　（Ｃ．Ｐｅｒｋｉｎｓ））。

【０００５】

ところで、移動ＩＰ方式では、移動計算機が新規の移動先に移った場合、現在位置の登録メッセージをホームエージェントに送ることが必要である。この場合、移動計算機がどのようなネットワークに移動したかによって、移動計算機の発するメッセージの扱いが変わってくる。

【０００６】

例えば、移動計算機のホームネットワークと親しいネットワークに移動して、そのネットワークの出口に置かれたゲートウェイ（ファイアウォール）が登録メッセージを自由に外部に送出させる場合は、移動ＩＰの規定のままで動作が可能である。

【０００７】

一方、移動計算機を外部から内部に滞在（または侵入）しているものとして扱う一般のネットワークでは、セキュリティ上の考慮から、移動計算機の発する登録メッセージを自由に外部に送出させることは危険であると判断する。この場合、移動計算機が、自分は現在自分を侵入者として扱うネットワークにいる、ということを認識し、ゲートウェイに対して身分証明に相当する処理を行って外部アクセス許可を得たうえで登録メッセージのホームエージェントへの送出を行うことが必要になる。また、登録メッセージ送出が完了したあとの実際のデータ転送においても、ゲートウェイに対する身分証明を保持しての通信が必要である。

【０００８】

しかし従来は、移動ＩＰ方式では、各通信ノードは一意なＩＰアドレスが付与され、自由に制御パケットをやりとりできるという仮定で、経路制御や移動計算機位置の登録などの規定を行っていたため、実際の運用に際しては、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定がなかった。このため、特にセキュリティを考慮し、内部計算機の自由な外部アクセスを許可しないようなネットワークに移動計算機が移動した場合、移動後に行う新規位置の登録メッセージさえも移動計算機のホームネットワーク上のホームエージェントに到達させることができず、移動ＩＰ方式の運用に障害を起こすことがあった。

【０００９】

【発明が解決しようとする課題】

従来の通信システムでは、各通信ノードには一意なＩＰアドレスが付与され、自由にパケットを送受信できるという仮定で、経路制御や移動計算機位置の登録などの規定を行っていたため、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機をサポートする場合、実際の運用に際しては、移動計算機がどのような組織に属するネットワークに移動したかというネットワーク運用ポリシーに関する動作規定がなかった。

【００１０】
このため特にセキュリティを考慮し内部計算機の自由な外部アクセスを許可しないようなネットワークに移動計算機が移動した場合、移動後に行う新規位置の登録メッセージさえも移動計算機のホームネットワーク上のホームエージェントに到達させることができず、移動計算機に関する運用に障害を起こすことがあった。
【００１１】
本発明は、上記事情を考慮してなされたもので、ネットワーク内部に移動してきた管理対象外の移動計算機のうち、正当と認識できる移動計算機からのパケットのみをネットワーク外部へ通過させる制御を行うことのできるパケット検査装置及びパケット転送方法を提供することを目的とする。
【００１２】
また、本発明は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機において、自装置を一旦侵入者とみなすネットワークに移動した場合に、パケット検査装置との間で自装置の正当性の確認を行い、該パケット検査装置から外部へパケットを通過させる制御を行うことのできる移動計算機装置及びパケット転送方法を提供することを目的とする。
【００１３】
【課題を解決するための手段】
本発明は、自装置の管理するネットワークの内部の計算機がネットワーク外の計算機へ向けて送信するパケットを検査するパケット検査装置（例えば、ゲートウェイ）であって、自装置の管理対象となる計算機以外の移動計算機から送信されたパケットに含まれる移動計算機識別情報に基づき、該移動計算機から送信されたパケットのネットワーク外への転送の可否を判定する判定手段と、この判定手段により転送を拒否すると判定した場合に、前記移動計算機に転送拒否を示すメッセージを返信する手段と、前記移動計算機から移動計算機識別情報（例えば、所定の鍵情報を使って生成する認証データを含む情報）を生成するための鍵情報を要求するメッセージを受信した場合に、該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する手段とを具備したことを特徴とする。
【００１４】
なお、パケット検査装置及び移動計算機が使用する移動計算機識別子として、例えば、転送パケット内容と生成鍵から生成される一方向ハッシュ関数値（例えば、Ｋｅｙｅｄ　ＭＤ５方式）などの認証データが利用できる。
【００１５】
好ましくは、自装置がどの計算機を管理するかを示す管理対象計算機認識手段をさらに備え、前記判定手段は、この管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理する計算機から送信されたものであることが示される場合は、該パケットをそのまま転送することを許可すると判定するようにしても良い。
【００１６】
好ましくは、自装置がどの計算機を管理するかを示す管理対象計算機認識手段をさらに備え、前記判定手段は、この管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、このパケットが移動計算機識別子を含まない場合は、該パケットの転送を拒否すると判定するようにしても良い。
【００１７】
好ましくは、自装置がどの計算機を管理するかを示す管理対象計算機認識手段をさらに備え、前記判定手段は、この管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、該パケットが移動計算機識別子を含む場合、該移動計算機識別子から該計算機の正当性が確認されたときのみ、該パケットを転送すると判定するようにしてもよい。
【００１８】

本発明では、パケット検査装置は、自装置の管理対象となる計算機以外の移動計算機から送信されたパケットに含まれる移動計算機識別情報に基づいて、該移動計算機から送信されたパケットのネットワーク外への転送を拒否すると判定した場合（例えば、パケット内に移動計算機識別情報が存在しない場合、あるいは移動計算機識別情報が正当なものでなかった場合）には、前記移動計算機に転送拒否を示すメッセージを返信する。

【００１９】

その後、この移動計算機から移動計算機識別情報を生成するための鍵情報を要求するメッセージを受信した場合、該移動計算機のユーザに関する情報（例えば、要求メッセージに含まれる）が所定の条件を満たすこと（例えば、予め登録されたユーザあるいは登録されたグループに属するユーザであること）を確認したならば、要求された鍵情報を返送する。

【００２０】

そして、この移動計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、このパケットが移動計算機識別子を含む場合、この移動計算機識別子を検査してその正当性が確認されたならば、該パケットを（必要な処理を施して）転送させる。

【００２１】

本発明によれば、ネットワーク内部に移動してきた管理対象外の移動計算機のうち、正当と認識できる移動計算機からのパケットのみをネットワーク外部へ通過させる制御を行うことができる。

【００２２】

この結果、移動計算機から当該ネットワーク外へのパケットの転送を当該ネットワークのセキュリティポリシーを守って正しく行え、また外部から訪問している正当な移動計算機を不正にネットワーク内に侵入して外部と通信を行う計算機とは明確に区別して外部への通信を許可することができるなど、セキュリティの高いかつ柔軟な移動計算機制御を可能とする。

【００２３】

また、本発明によれば、パケットに移動計算機識別情報を付与して画一的な処理を行うので、個々の移動計算機のテーブル管理などの処理が不要で、高速な認証手続きが可能である。特にパケットの暗号化や通信の末端同士でのパケット内容の認証といったＩＰセキュリティ処理を併用する場合に有効である。

【００２４】

また、本発明は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機であって、自装置が現在位置するネットワーク以外のネットワークに、自装置の移動位置情報（例えば、移動ＩＰプロトコルのホームエージェント）を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置が存在する場合に、該移動計算機管理装置へ向けて自装置の現在位置情報を含む登録メッセージを送信する第１の送信手段と、自装置が現在位置するネットワーク内部から該ネットワーク外へのパケットを検査するパケット検査装置（例えば、ゲートウェイ）から、この第１の送信手段により送信された登録メッセージのパケット転送拒否を示すメッセージが返信された場合に、該パケット検査装置に移動計算機識別情報（例えば、所定の鍵情報を使って生成する認証データを含む情報）を生成するための鍵情報を要求する要求メッセージを送信する第２の送信手段と、この第２の送信手段により送信された要求メッセージに応答して、前記パケット検査装置から鍵情報が返送された場合に、この鍵情報に基づいて生成した移動計算機識別情報を自装置が現在位置するネットワーク外へ向けて送信すべきパケットに付加して送信する第３の送信手段とを具備したことを特徴とする。

【００２５】

好ましくは、前記第３の送信手段は、前記移動計算機管理装置へ向けて、自装置の現在位置情報を含む登録メッセージを、前記移動計算機識別情報を付加して送信し、該移動計算機管理装置からの登録メッセージに対する受諾応答を受信した後、通信相手となる計算機

へのデータパケットを、前記移動計算機識別情報を付加して送信するようにしてもよい。

【００２６】

好ましくは、前記第３の送信手段は、前記第１の送信手段により送信された前記登録メッセージのパケット転送拒否を示すメッセージが前記パケット検査装置から返信されなかった場合には、通信相手となる計算機へのデータパケットを、前記移動計算機識別情報を付加せずに送信するようにしてもよい。

【００２７】

本発明では、移動計算機は、自装置が現在位置するネットワーク以外のネットワークに、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置が存在する場合（すなわち、ホームネットワーク外に移動した場合に）、まず、移動計算機管理装置へ向けて自装置の現在位置情報を含む登録メッセージを送信する。

【００２８】

これに対して自装置が現在位置するネットワーク内部から該ネットワーク外へのパケットを検査するパケット検査装置から、この登録メッセージのパケット転送拒否を示すメッセージが返信された場合、該パケット検査装置に移動計算機識別情報を生成するための鍵情報を要求する要求メッセージを送信する。

【００２９】

この要求メッセージに応答して、前記パケット検査装置から鍵情報が返送された場合、この鍵情報に基づいて生成した移動計算機識別情報を自装置が現在位置するネットワーク外へ向けて送信すべきパケットに付加して送信する。

【００３０】

本発明によれば、自装置を一旦侵入者とみなすネットワークに移動した場合に、パケット検査装置との間で自装置の正当性の確認を行い、該パケット検査装置から外部へパケットを通過させる制御を行うことができる。

【００３１】

また、本発明は、自装置の管理するネットワークの内部の計算機がネットワーク外の計算機へ向けて送信するパケットを検査するパケット検査装置のパケット転送方法であって、自装置の管理対象となる計算機以外の移動計算機から送信されたパケットに含まれる移動計算機識別情報に基づき、該移動計算機から送信されたパケットのネットワーク外への転送の可否を判定し、転送を拒否すると判定した場合に、前記移動計算機に転送拒否を示すメッセージを返信し、前記移動計算機から移動計算機識別情報を生成するための鍵情報を要求するメッセージを受信した場合に、該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を該移動計算機へ返送することを特徴とする。

好ましくは、前記パケット検査装置は、自装置がどの計算機を管理するかを示す管理対象計算機認識手段を具備するものであり、前記判定にあたっては、前記管理対象計算機認識手段により、ネットワーク内部の計算機から送信されたパケットが自装置の管理しない計算機から送信されたものであることが示され、かつ、該パケットが移動計算機識別子を含む場合、該移動計算機識別子から該計算機の正当性が確認されたときのみ、該パケットを転送すると判定するようにしてもよい。

【００３２】

また、本発明は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機のパケット転送方法であって、自装置が現在位置するネットワーク以外のネットワークに、自装置の移動位置情報を管理し自装置宛のパケットを自装置の現在位置に転送する手段を有する移動計算機管理装置が存在する場合に、該移動計算機管理装置へ向けて自装置の現在位置情報を含む登録メッセージを送信し、自装置が現在位置するネットワーク内部から該ネットワーク外へのパケットを検査するパケット検査装置から、前記登録メッセージに対するパケット転送拒否を示すメッセージが返信された場合に、該パケット検査装置に移動計算機識別情報を生成するための鍵情報を要求する要求メッセージを送信し

、この要求メッセージに応答して、前記パケット検査装置から鍵情報が返送された場合に、この鍵情報に基づいて生成した移動計算機識別情報を自装置が現在位置するネットワーク外へ向けて送信すべきパケットに付加して送信することを特徴とする。
好ましくは、前記移動計算機管理装置へ向けて送信された前記登録メッセージのパケット転送拒否を示すメッセージが前記パケット検査装置から返信されなかった場合には、前記自装置が現在位置するネットワーク外へ向けて送信すべきパケットであって通信相手となる計算機へのデータパケットを、前記移動計算機識別情報を付加せずに送信するようにしてもよい。

【００３３】

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する。
また、上記の発明は、相当する手順あるいは手段をコンピュータに実行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。

【００３４】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。
図１に、本実施形態に係る通信システムの基本構成の一例を示す。
図１の通信システムは、前述した図１５と同様に移動ＩＰなどにより移動計算機の通信をサポートしているものとする。なお、移動ＩＰプロトコルでは、移動先ネットワークで移動計算機に対するパケット配送を行うフォーリンエージェントというルータの存在を仮定するモードと、フォーリンエージェントを設けない（移動先計算機自身がフォーリンエージェントを兼ねる）ポップアップモードがあるが、本実施形態では、ポップアップモードを採用するものとして説明する。

【００３５】

図１では、ホームネットワーク１ａ、第１の他部署ネットワーク１ｂ、第２の他部署ネットワーク１ｃがインターネット６を介して相互に接続されており、移動計算機（ＭＮ）２、移動計算機の通信相手（ＣＨ）３は、これらネットワーク内に接続され、または外部ノードとしてインターネット６に接続される。ネットワーク１ａ，１ｂには、自装置の管理するネットワークの内部の計算機がネットワーク外の計算機へ向けて送信するパケットを検査するパケット検査装置（ゲートウェイ）４ａ，４ｂがそれぞれ設けられるものとする。なお、ネットワーク１ｃにも、必要に応じてゲートウェイ４ｃが設けられる。

【００３６】

本実施形態では、ネットワーク１ａの内部をホームポジションとする移動計算機２が他部署ネットワーク１ｂに移動した場合について説明する。
ゲートウェイ４ａ，４ｂ，４ｃは、パケット暗号化認証処理機能を持つものとする。また、移動計算機２は、少なくとも移動中には、パケット暗号化認証処理機能を持つものとする（図中、パケット暗号化認証処理機能を持つ移動計算機２をMN^{+}で表す）。なお、パケット暗号化認証処理における通信データの暗号化／復号は、例えば、文献（ＩＥＴＦ　ＲＦＣ１８２５，１８２７）に示される方式で実現できる。また、パケット暗号化認証処理における、認証データ（転送パケット内容と生成鍵から生成されるハッシュ関数値など）の付与／チェックは、例えば、文献（ＩＥＴＦ　ＲＦＣ１８２５，１８２６）に示される方式で実現できる。

【００３７】

ホームネットワーク１ａには、移動ＩＰプロトコルをサポートするために、移動計算機の移動先の現在位置の情報を管理するホームエージェント（ＨＡ）５が設けられる。管理対象とする移動計算機の台数は任意である。前述したように、移動中の移動計算機２宛に転送されてきたＩＰパケットは、そのホームエージェント５を経由し、移動計算機２の元のアドレス（ホームネットワーク１ａにおけるアドレス）宛のＩＰパケットを移動ＩＰの現在位置アドレス宛パケット内にカプセル化することで、移動計算機２に対するデータの経路制御を行うことができる。

【００３８】

なお、第１の他部署ネットワーク１ｂ、第２の他部署ネットワーク１ｃにも、必要に応じて、ホームエージェント５ｂ，５ｃが設けられる。
ゲートウェイ４ａ，４ｂ，４ｃは、自装置が管理対象とする送信元計算機を認識する管理対象計算機認識部（図示せず）を持つ。例えば、通信システム内のいずれかの場所（分散していても良い）に、各ゲートウェイがどの計算機を管理対象とするかを示す情報のデータベース（具体例としては各ゲートウェイのネットワークアドレスと、その管理対象となる計算機群のネットワークアドレスの対応情報）を管理するサーバ装置を設置し、移動計算機が該データベースを検索することにより実現できる。あるいは、各ゲートウェイが、自装置の管理対象となる計算機群のネットワークアドレスの情報を保持することで実現できる。

【００３９】
ゲートウェイ４ａ，４ｂ，４ｃは、ネットワーク内部の計算機から送信されたパケットが自装置の管理する計算機から送信されたものである場合は、該パケットをそのまま転送するが、該パケットが自装置の管理しない計算機から送信されたものである場合は、該パケット内に正当な移動計算機識別情報が含まれれば該パケットに必要な処理を施した上で通過させるが、該パケット内に所定の情報が含まれなければ該パケットの転送を拒否する。

【００４０】
また、ゲートウェイ４ａ，４ｂ，４ｃは、パケットの転送を拒否された計算機から上記移動計算機識別情報を生成するために必要な鍵の情報を要求された場合には、要求メッセージから求められる該移動計算機のユーザに関する情報が所定の条件を満たすことを確認したならば、要求された鍵情報を返送する。

【００４１】
移動計算機２は、自装置を管理するホームエージェント５ａの設置されたネットワーク（ホームネットワーク）１ａ外に位置することを認識する位置認識部（図示せず）を持つ。位置認識部は、例えば、ホームエージェント５が定期的に発信する広告メッセージを受信できるか否かをもとに、自装置がホームネットワーク内にいるかどうかを判定することで実現できる。

【００４２】
移動計算機２は、位置認識部により、自装置がホームネットワーク外に移動したと判断された場合には、移動先のネットワーク（ここでは１ｂ）において、例えばＤＨＣＰやＰＰＰなどのプロトコルにより移動先ネットワークで使用するアドレスを獲得する。

【００４３】
アドレスを獲得したら、移動計算機２は、ホームネットワーク１ａのホームエージェント５ａに現在位置の情報を含む登録メッセージを送信する。
ここで、移動計算機２がゲートウェイ４ｂの管理対象である場合には、登録メッセージはそのままゲートウェイ４ｂを通過するが、移動計算機２がゲートウェイ４ｂの管理対象でない場合には、登録メッセージは一旦通過拒否されるので、移動計算機２は、ゲートウェイ４ｂに鍵情報を要求し、鍵情報が入手できれば、これを使って生成した計算機識別情報を付加して再度登録メッセージを送信する。この結果、再度送信された登録メッセージは、ゲートウェイ４ｂを通過する（なお、ゲートウェイ４ｂの管理対象でない計算機が、鍵情報を入手できなければ、この計算機は、ゲートウェイ４ｂから外にパケットを通過させることはできない）。

【００４４】
なお、ゲートウェイ及び移動計算機が使用する移動計算機識別子として、例えば、転送パケット内容と生成鍵から生成される一方向ハッシュ関数値（例えば、Ｋｅｙｅｄ　ＭＤ５方式）などの認証データが利用できる。

【００４５】
そして、登録メッセージが移動計算機２のホームネットワーク１ａのホームエージェント５ａに到着すると、その管理表には、移動計算機２の全ネットワーク中における位置を一意に特定可能な情報が登録される（この時点で、ホームエージェント５ａは、移動計算機

２がホームネットワーク１ａ外に移動したことを認識する）。また、ネットワーク１ａでは、ゲートウェイ４ｂの管理表に、インターネット６側からその移動計算機２宛に転送されてきたパケットをホームエージェント５ａに転送するように設定がなされる。

【００４６】

これによって、インターネット６から移動計算機２のホームネットワーク１ａに転送されてきた移動計算機２宛のパケットは、一旦ホームエージェント５ａに渡され、ここから、移動計算機２の移動先に宛てて転送される。その際、ホームエージェント５ａにて、例えば、前述したように、移動計算機２の元のアドレス（ホームネットワーク１ａにおけるアドレス）宛のＩＰパケットを移動ＩＰの現在位置アドレス宛パケット内にカプセル化する処理が行われる。

【００４７】

そして、移動計算機２は、登録メッセージに対して一旦転送拒否を示すメッセージを受信した後に鍵情報と計算機識別情報のやり取りによって応答受諾を受信した場合には、通信相手となる計算機３へのパケットに計算機識別情報を付加して送信する。登録メッセージに対して転送拒否されずに応答受諾を受けた場合には、通信相手となる計算機３へのパケットを通常通り送信する。

【００４８】

以下、さらに詳しく本実施形態を説明していく。

図２に、移動計算機２の現在位置を検出する処理手順の一例を示す。

ここで、移動ＩＰの規定にあるように各ホームエージェントはその処理するサブネット内に定期的にエージェント広告メッセージを送出するものとする。また、各ゲートウェイは、各々が検査対象とする計算機のアドレスのリストを公開しており、ある計算機について、その送信パケットのチェックを司るゲートウェイを検索可能であるとする。

【００４９】

移動計算機２側では、まず、自装置がホームネットワーク１ａの内部に位置するか外に位置するかを判定する。自装置を管理するホームエージェント５ａの送出するエージェント広告メッセージを受信し、ホームネットワーク内部に位置するか外に位置するかを検知する。自装置の属するホームネットワーク１ａのホームエージェント５ａによるエージェント広告メッセージを受信した場合にはホームネットワーク１ａ内部に位置すると判定する。それ以外のホームエージェントによるエージェント広告メッセージを受信した場合、あるいはエージェント広告メッセージを受信できない場合にはホームネットワークの外に位置すると判定する（ステップＳ１１）。

【００５０】

移動計算機２は、自装置がホームネットワークの外に位置すると判定された場合（ステップＳ１２）、移動ＩＰのケア・オブ・アドレス（Ｃａｒｅ－ｏｆアドレス）をＤＨＣＰなどの手段により取得する（ステップＳ１３）。

【００５１】

さらに、移動計算機２は、そのＣａｒｅ－ｏｆアドレスを保護するゲートウェイ（ＧＷ＿ＭＨ）を検索する（ステップＳ１４）。

ここで、検索されたゲートウェイ（ＧＷ＿ＭＨ）とホームネットワークのゲートウェイが一致している場合（例えばホームネットワーク１ａ内で他のサブネットに移動した場合）には、自装置はホームドメイン内に位置すると判定する［ＭＮ－ｈｏｍｅ］。そうでない場合には、ホームドメイン外に位置すると判定する［ＭＮ－ｆｏｒｅｉｇｎ］。ホームドメイン内に位置すると判定された場合には、以下に示す一連の位置登録処理は実行せず、通常のＩＰパケット形式で登録要求を送る。

【００５２】

なお、Ｃａｒｅ－ｏｆアドレスを保護するゲートウェイが存在しない場合、移動計算機２は外部ノードである。

さて、移動ＩＰ方式では、移動計算機が新規の移動先に移った場合、現在位置の情報を含む登録メッセージを、自装置を管理するホームエージェントに送ることが必要である。こ

の場合、移動計算機がホームネットワークと親しいネットワークに移動して、そのゲートウェイが自装置の送信する登録メッセージやデータパケットを自由に外部に送出させる場合には、移動ＩＰの規定のままで動作が可能である。しかし、一般に移動計算機を外部から内部に滞在しているものとして扱うネットワークでは、セキュリティ上の考慮から、移動計算機の発するメッセージを自由に外部に送出させることは危険であることから、ゲートウェイは自装置が管理対象とする計算機以外の移動計算機の送信する登録メッセージやデータパケットを一旦通過拒否する。このような場合、移動計算機は、現在自装置を侵入者として扱うネットワークに位置することを認識し、そのゲートウェイとの間で身分証明に相当する手続きを行って外部アクセス許可を得た後に登録メッセージをホームエージェントへ送信することが必要になる。

【００５３】

以下、登録メッセージに関する処理手順の一例を説明する。なお、ここでは、パケット内のデータ部の暗号化はしない例を示す。

まず、移動計算機２がホームドメインにいる［ＭＮ－ｈｏｍｅ］の場合は、

・ホームエージェント（ＨＡ）のＩＰアドレス

・移動計算機（ＭＮ）のＩＰアドレス

を調べ、移動計算機を送信元、ホームエージェントを宛先とする通常のＩＰパケット形式で登録要求を送り、ホームエージェントからのＩＰパケット形式の応答を受信するだけでよいので、登録メッセージの送出は不要である。

【００５４】

なお、ここでは、ホームエージェントと移動計算機のＩＰアドレスは、ホームネットでのプライベート・アドレス（Ｐｒｉｖａｔｅアドレス）とする。

次に、移動計算機２がホームドメイン外［ＭＮ－ｆｏｒｅｉｇｎ］に移動している場合について説明する。

【００５５】

例えば、図３に示すように移動計算機２が第１の他部署ネットワーク１ｂに移動している場合、まず、第１の登録メッセージを送る。

図４に第１の登録メッセージの一例を示す。ＩＰヘッダでは、送信元を移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレス、宛先をホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレスとする。

【００５６】

これに対し、移動計算機２がホームネットワーク１ａと親しいネットワークに移動して、そのゲートウェイが登録メッセージを自由に外部に送出させる場合には、問題なく、受諾応答が返るだけであるが、もしゲートウェイ４ｂが、管理対象でない計算機から自装置宛でないパケットを受信したならば、登録メッセージの通過を拒否するメッセージを返すような場合には、通過拒否メッセージが返送される。

【００５７】

図５に、通過拒否メッセージの一例として、ＴＣＰ／ＩＰ通信のＩＣＭＰメッセージを拡張した形式で実現したものを示す。ＩＰヘッダでは、送信元をゲートウェイ４ｂ（ＧＷ１）のグローバル・アドレス（Ｇｌｏｂａｌアドレス）、宛先を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレスとする。

【００５８】

この場合、移動計算機２は、通過拒否メッセージ中に含まれるゲートウェイ４ｂのＧｌｏｂａｌアドレスを用いて、ゲートウェイ４ｂに対し鍵要求メッセージを送信して、公開鍵の問い合わせを行う。

【００５９】

図６に、鍵要求メッセージの一例を示す。ＩＰヘッダでは、送信元を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、宛先をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレスとする。

【００６０】

この鍵要求メッセージに対し、ゲートウェイ４ｂが公開鍵情報を渡すか否かの判断は、ゲートウェイ４ｂのサイトのシステム管理のポリシーに依存する。
例えば、
・鍵要求情報に所定の書式で付加されたユーザ識別情報を調べ、社内ユーザであれば、鍵情報を返す。
・社外ユーザであれば、所定の組織であれば鍵情報を渡す。
・それ以外の場合、予め登録されたユーザであれば、鍵情報を渡す。
といった規則をゲートウェイ４ｂに登録しておく。

【００６１】

ゲートウェイ４ｂに対するユーザ登録方法などはシステムの性質に応じ任意に設定すれば良い。
公開鍵要求に対し、ゲートウェイ４ｂの公開鍵が得られたら、移動計算機２は、以下の２度目の登録要求（ｒｅｇｉｓｔｒａｔｉｏｎ　ｒｅｑｕｅｓｔ）を送る。

【００６２】

図７に、第２の登録メッセージの一例を示す。
ＩＰヘッダ１では、送信元を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、宛先をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレスとし、ＫＥＹ情報と、ＡＨ情報を付加する。

【００６３】

ＫＥＹ情報は、ＩＰヘッダ１の送信元ノードと宛先ノードとの間（ここでは、移動計算機２～ゲートウェイ４ｂ間）で共有する鍵情報を含むヘッダ情報である。

【００６４】

ＡＨ情報は、上記鍵を使って生成された認証データを含むヘッダ情報である。また、内部ＩＰヘッダ（登録要求）では、送信元を移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレス、宛先をホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレスとする。

【００６５】

この登録メッセージは、ゲートウェイ４ｂ宛でかつゲートウェイ４ｂに対する認証データを含むＡＨ情報（移動計算機識別情報）が付与されているので、ゲートウェイ４ｂは認証処理を行い、これに成功すれば登録メッセージは通過できる。

【００６６】

この結果、ゲートウェイ４ｂは、次段のゲートウェイ４ａ宛に登録メッセージを転送する。
そして、登録メッセージは、インターネット６からゲートウェイ４ａを介してホームエージェント５ａに到着し、必要な登録処理が行われる。また、ホームエージェント５ａは、移動計算機２に対して登録応答メッセージを送信する。

【００６７】

ホームエージェント５ａから送信される登録応答メッセージは、ゲートウェイ４ａにて中継され、ゲートウェイ４ｂに到達する。
ゲートウェイ４ｂでは、これを図８に示すように変形して移動計算機宛に転送する。図８において、ＩＰヘッダ１では、送信元をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレス、宛先を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレスとし、ＫＥＹ情報と、ＡＨ情報を付加する。また、内部ＩＰヘッダ（登録応答）では、送信元をホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレス、宛先を移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレスとする。

【００６８】

またその代わりに、ゲートウェイ４ｂでは、パケットを図８からＩＰヘッダ１、ＫＥＹ情報、ＡＨ情報を取り除いた形式のパケットで移動計算機宛に転送するようにしても良い。

【００６９】

なお、ゲートウェイ４ａとゲートウェイ４ｂの間で経路認証を行う場合には、各ゲートウェイは、パケットに前述の次段に対するＫＥＹ情報とＡＨ情報とＩＰヘッダを付加すれば

良い（前段とのＫＥＹ情報等がパケットに付加されていた場合には次段に対するものに置換される）。

【００７０】

以上の登録処理が完了したら、それ以降、移動計算機２が訪問ネットワーク１ｂ外に位置する通信相手計算機２とデータ通信を行う場合も、上記の移動計算機２～ゲートウェイ４ｂ間の認証データをパケットに付加して転送する。この認証データ付加があるか否かによって、ゲートウェイ４ｂにて正しく認識されている訪問ノードであるか否かを正しく判定し、セキュリティに正しい移動計算機のメッセージ制御を行うことが可能である。

【００７１】

以下、登録メッセージに関する処理手順の他の例を説明する。なお、ここでは、パケット内のデータ部を暗号化する場合が含まれる例を示す。本例では、各パケット検査装置は、パケット暗号化ゲートウェイとして働く。

【００７２】

ここでは、前述したような経路間での認証を、ＩＰセキュリティと呼ばれる仕様を用いたパケット内容の暗号化および末端同士でのパケット認証（参考文献：ＩＥＴＦ　ＲＦＣ１８２５～１８２９）と併せて定義した形式を採用する通信システムに本発明を適用した場合について説明する。

【００７３】

ＩＥＴＦではＩＰパケットへの認証コード付与方式をＩＰセキュリティ標準（文献：ＩＥＴＦ　ＲＦＣ１８２６，１８２８）として規定しているが、この方法を利用し、移動計算機の身分証明のための処理としてデータパケットに移動計算機と移動先ネットワークのゲートウェイ間での認証データを付加し、ゲートウェイでは受信したパケットの認証コードを確認してから、外部にパケットを通過させるようにする。これによって、たとえ組織外のユーザが入って来てネットワーク外部に対しデータパケットを送信したいと要求しても、予め所定の方法で認証鍵を交換し身分保証を行った移動計算機のみに外部アクセスを許可することが可能となる。

【００７４】

図９に各ゲートウェイ（パケット暗号化ゲートウェイ）で処理されるパケット形式を示す。

（ａ）は、通常のＩＰパケット形式である。

【００７５】

（ｂ）は、暗号化／末端認証形式であり、末端のゲートウェイ間または末端のゲートウェイ～移動計算機間でパケットの暗号化および認証を行う形式である。（ｃ）は、暗号化／経路間認証形式である。途中経路間でのゲートウェイ間、途中経路のゲートウェイ～移動計算機間の認証を必要とする場合にはこの形式を使用する。

【００７６】

（ｄ）は、移動ＩＰ形式であり、ホームエージェントで移動計算機宛に経路制御されるパケット形式である。

まず、移動計算機２がホームドメインにいる［ＭＮ－ｈｏｍｅ］の場合は、前述した場合と同様であり、

ホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレス

・移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレス

を調べ、通常のＩＰパケット形式で登録要求を送り、ＩＰパケット形式の応答を受信するだけでよいので、登録メッセージの送出は不要である。

【００７７】

移動計算機２がホームドメイン外［ＭＮ－ｆｏｒｅｉｇｎ］に移動している場合、まず、

・ホームネットワークのゲートウェイ（ＧＷ０）のｇｌｏｂａｌアドレス

・ホームネットワークのゲートウェイ（ＧＷ０）の公開鍵

・移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、Ｐｒｉｖａｔｅアドレス

・ホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレス

を調べ、第１の登録メッセージを送る。
【００７８】
図１０に第１の登録メッセージの一例を示す。
ＩＰヘッダでは、送信元を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、宛先をゲートウェイ４ａ（ＧＷ０）のＧｌｏｂａｌアドレスとし、ＫＥＹ情報と、ＡＨ情報と、ＥＳＰ情報を付加する。
【００７９】
ＫＥＹ情報は、ＩＰヘッダの送信元ノードと宛先ノードとの間（ここでは、移動計算機２～ゲートウェイ４ａ間）で共有する鍵情報を含むヘッダ情報である。ＡＨ情報は、上記鍵を使って生成された認証データを含むヘッダ情報である。
【００８０】
ＥＳＰ情報は、暗号化された内部データ（ここでは、内部ＩＰヘッダとそのデータ部）を復号するアルゴリズムを指定する情報を含むヘッダ情報である。
また、内部ＩＰヘッダ（登録要求）では、送信元を移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレス、宛先をホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレスとする。
【００８１】
これに対し、移動計算機２がホームネットワーク１ａと親しいネットワークに移動して、そのゲートウェイが登録メッセージを自由に外部に送出させる場合には、問題なく、受諾応答が返るだけであるが、もしゲートウェイ４ｂが、管理対象でない計算機から自装置宛でないパケットを受信したならば、登録メッセージの通過を拒否するメッセージを返すような場合には、通過拒否メッセージが返送される。
【００８２】
図１１に、通過拒否メッセージの一例として、ＴＣＰ／ＩＰ通信のＩＣＭＰメッセージを拡張した形式で実現したものを示す。ＩＰヘッダでは、送信元をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレス、宛先を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレスとする。
【００８３】
この場合は、移動計算機２は、通過拒否メッセージ中に含まれるゲートウェイ４ｂのｇｌｏｂａｌアドレスを用いて、ゲートウェイ４ｂに対し鍵要求メッセージを送信して、公開鍵の問い合わせを行う。
【００８４】
図１２に、鍵要求メッセージの一例を示す。ＩＰヘッダでは、送信元を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、宛先をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレスとする。
【００８５】
なお、前述したように、この鍵要求メッセージに対し、ゲートウェイ４ｂが公開鍵情報を渡すか否かの判断は、ゲートウェイ４ｂのサイトのシステム管理のポリシーに依存する。
【００８６】
この鍵要求メッセージに対し、ゲートウェイ４ｂの公開鍵が得られたら、移動計算機２は、以下の２度目の登録要求を送る。
図１３に、第２の登録メッセージの一例を示す。
【００８７】
ＩＰヘッダ１では、送信元を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、宛先をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレスとし、ＫＥＹ情報と、ＡＨ情報を付加する。
【００８８】
ＫＥＹ１情報は、ＩＰヘッダ１の送信元ノードと宛先ノードとの間（ここでは、移動計算機２～ゲートウェイ４ｂ間）で共有する鍵情報を含むヘッダ情報である。
【００８９】
ＡＨ情報は、上記鍵を使って生成された認証データを含むヘッダ

２では、送信元を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレス、宛先をゲートウェイ４ａ（ＧＷ０）のＧｌｏｂａｌアドレスとし、ＫＥＹ情報と、ＡＨ情報と、ＥＳＰ情報を付加する。

【００９０】

ＫＥＹ２情報は、ＩＰヘッダ２の送信元ノードと宛先ノードとの間（ここでは、移動計算機２～ゲートウェイ４ａ間）で共有する鍵情報を含むヘッダ情報である。

【００９１】

ＡＨ情報は、上記鍵を使って生成された認証データを含むヘッダ情報である。ＥＳＰ情報は、暗号化された内部データ（ここでは、内部ＩＰヘッダとそのデータ部）を復号するアルゴリズムを指定する情報を含むヘッダ情報である。

【００９２】

また、内部ＩＰヘッダ（登録要求）では、送信元を移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレス、宛先をホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレスとする。

【００９３】

この登録メッセージは、ゲートウェイ４ｂ宛でかつゲートウェイ４ｂに対する認証データを含むＡＨ情報（移動計算機識別情報）が付与されているので、ゲートウェイ４ｂは認証処理を行い、これに成功すればメッセージは通過できる。

【００９４】

この結果、ゲートウェイ４ｂは、次段のゲートウェイ４ａ宛に登録メッセージを転送する。

そして、登録メッセージは、インターネット６からゲートウェイ４ａを介してホームエージェント５ａに到着し、必要な登録処理が行われる。また、ホームエージェント５ａは、移動計算機２に対して登録応答メッセージを送信する。

【００９５】

ホームエージェント５ａから送信される登録応答メッセージ（ＫＥＹ２情報とＡＨ情報とＩＰヘッダ２にカプセル化されたもの）、ゲートウェイ４ａにて中継され、ゲートウェイ４ｂに到達する。

【００９６】

ゲートウェイ４ｂでは、これを図１４に示すように変形して移動計算機宛に転送する。

図１４において、ＩＰヘッダ１では、送信元をゲートウェイ４ｂ（ＧＷ１）のＧｌｏｂａｌアドレス、宛先を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレスとし、ＫＥＹ１情報と、ＡＨ情報を付加する。ＩＰヘッダ２では、送信元をゲートウェイ４ａ（ＧＷ０）のＧｌｏｂａｌアドレス、宛先を移動計算機（ＭＮ）のＣａｒｅ－ｏｆアドレスとし、ＫＥＹ２情報と、ＡＨ情報と、ＥＳＰ情報を付加する。また、内部ＩＰヘッダ（登録要求）では、送信元をホームエージェント（ＨＡ）のＰｒｉｖａｔｅアドレス、宛先を移動計算機（ＭＮ）のＰｒｉｖａｔｅアドレスとする。

【００９７】

またその代わりに、ゲートウェイ４ｂでは、パケットを図１４からＩＰヘッダ１、ＫＥＹ１情報、ＡＨ情報を取り除いた形式のパケットで移動計算機宛に転送するようにしても良い。

【００９８】

なお、ゲートウェイ４ａとゲートウェイ４ｂの間で経路認証を行う場合には、各ゲートウェイ４ａは、パケットに前述の次段に対するＫＥＹ１情報とＡＨ情報とＩＰヘッダ１を付加すれば良い（前段とのＫＥＹ情報等がパケットに付加されていた場合には次段に対するものに置換される）。

【００９９】

以上の登録処理が完了したら、それ以降、移動計算機２が訪問ネットワーク外に位置する通信相手計算機２とデータ通信を行う場合も、上記の移動計算機２～ゲートウェイ４ｂ間の認証データをパケットに付加して転送する（これもＩＰＳＥＣの拡張で実装できる）。

この認証データ付加があるか否かによって、ゲートウェイ４ｂにて正しく認識されている

訪問ノードであるか否かを正しく判定し、セキュリティに正しい移動計算機のメッセージ制御を行うことが可能である。

【０１００】

なお、上記した各例では、移動先ネットワークにおいてそのゲートウェイから一旦パケットの通過を拒否された場合、所定の手順の後、認証データをパケットに付加して送信するものであったが、その代わりに、ゲートウェイにて認証に成功した移動計算機を管理対象として管理テーブルに登録し、以降はその移動計算機については認証を省くようにしても良い（この場合、登録後は、移動計算機は認証データをパケットに付加せずに送信することができる）。

【０１０１】

さて、従来、移動ＩＰ方式では、各ネットワークノードは一意なＩＰアドレスが付与され、自由に制御パケットをやりとりできるという仮定でのみ、経路制御や移動計算機位置の登録などの規定を行っていたが、本実施形態によれば、実際の運用に際して、移動計算機がどのような組織に属するネットワークに移動したか、というネットワーク運用ポリシーに関する動作規定を考慮することができる。

【０１０２】

特に、セキュリティを考慮し、内部計算機の自由な外部アクセスを許可しないようなネットワークに移動計算機が移動した場合にも、移動後に行う新規位置の登録メッセージの送信や通常の通信データの送信に際し、移動計算機が自身が外部組織のネットワークにいるということを認識して、移動先ネットのゲートウェイに対して自分の身分証明を行う処理を行ってから外部アクセスを行う手段を提供できるので、正規の処理を経た移動計算機発のパケットのみを選択的に通過させ、セキュリティの高い、かつ柔軟な移動計算機制御を行うことができる。

【０１０３】

また、本実施形態では、パケット自体に対し認証コードを付与して画一的な処理を移動計算機およびゲートウェイで行うことができるので、移動計算機個々をテーブル管理したりといった処理が不要で、高速な認証が可能である。特に、パケットの暗号化や通信の末端同士でのパケット内容の認証といったＩＰセキュリティ処理を併用する場合に有効である。

【０１０４】

以上の各機能、例えば移動計算機に搭載するパケット暗号化認証部などは、ハードウェアとしてもソフトウェアとして実現可能である。また、上記した各手順あるいは手段をコンピュータに実行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実施することもできる。

【０１０５】

なお、本実施形態では、ポップアップモードによる通信システムについて説明したが、本発明は、フォーリンエージェントの存在を仮定した通信システムにも適用可能である。

【０１０６】

また、本発明は、現在種々提案されている移動通信プロトコル、暗号化通信プロトコル、暗号鍵交換プロトコルに対しても適用可能である。

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。

【０１０７】

【発明の効果】

本発明に係るパケット検査装置によれば、ネットワーク内部に移動してきた管理対象外の移動計算機のうち、正当と認識できる移動計算機からのパケットのみをネットワーク外部へ通過させる制御を行うことができる。

【０１０８】

本発明に係る移動計算機装置によれば、自装置を一旦侵入者とみなすネットワークに移動した場合に、パケット検査装置との間で自装置の正当性の確認を行い、該パケット検査装

置から外部へパケットを通過させる制御を行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るシステムの基本構成の一例を示す図

【図２】同実施形態に係る移動計算機の位置判定処理の流れを示すフローチャート

【図３】同実施形態に係る移動登録メッセージ送信手順を説明するための図

【図４】同実施形態に係る第１の登録メッセージのフォーマットの一例を示す図

【図５】同実施形態に係る通過拒否メッセージのフォーマットの一例を示す図

【図６】同実施形態に係る鍵要求メッセージのフォーマットの一例を示す図

【図７】同実施形態に係る第２の登録メッセージのフォーマットの一例を示す図

【図８】同実施形態に係るデータパケットのフォーマットの一例を示す図

【図９】ＩＰセキュリティに基づくパケット形式の一例を示す図

【図１０】同実施形態に係る第１の登録メッセージのフォーマットの他の例を示す図

【図１１】同実施形態に係る通過拒否メッセージのフォーマットの他の例を示す図

【図１２】同実施形態に係る鍵要求メッセージのフォーマットの他の例を示す図

【図１３】同実施形態に係る第２の登録メッセージのフォーマットの他の例を示す図

【図１４】同実施形態に係るデータパケットのフォーマットの他の例を示す図

【図１５】移動計算機を含む通信システムの基本構成を説明するための他の図

【符号の説明】

１ａ…ホームネットワーク

１ｂ，１ｃ…他部署ネットワーク

２…移動計算機

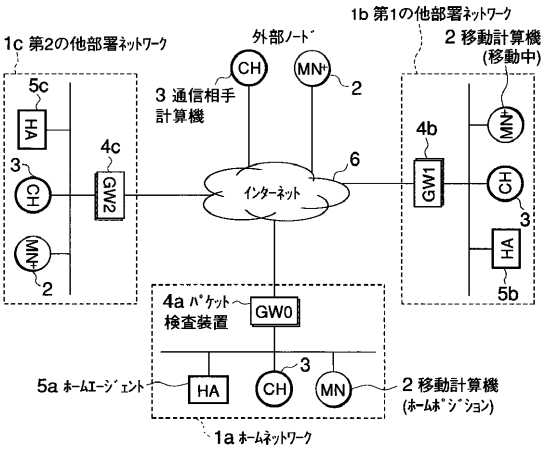
３…通信相手計算機

４ａ，４ｂ，４ｃ…パケット検査装置（ゲートウェイ）

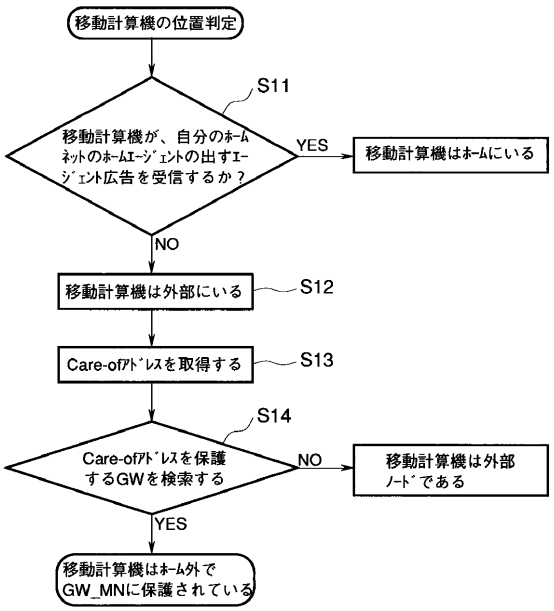
５ａ，５ｂ，５ｃ…ホームエージェント

６…インターネット

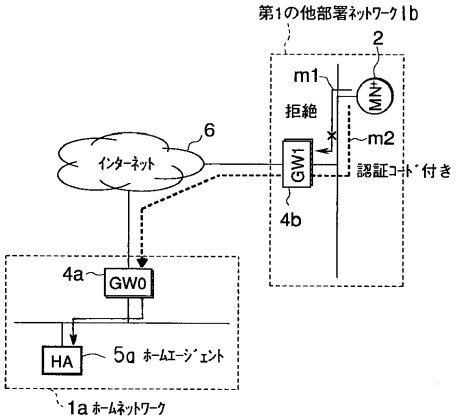
【図１】



【図２】



【図３】



【図４】

IPﾍｯﾀﾞ	data（登録要求）

IPﾍｯﾀﾞ（登録要求）
送信元＝MNのﾌﾟﾗｲﾍﾞｰﾄ･ｱﾄﾞﾚｽ
宛先＝HAのﾌﾟﾗｲﾍﾞｰﾄ･ｱﾄﾞﾚｽ

【図５】

IPﾍｯﾀﾞ	ICMP（通過拒否ﾒｯｾｰｼﾞ）

IPﾍｯﾀﾞ
送信元＝GW1のｸﾞﾛｰﾊﾞﾙ･ｱﾄﾞﾚｽ
宛先＝MNのｹｱ･ｵﾌﾞ･ｱﾄﾞﾚｽ

【図６】

IPﾍｯﾀﾞ	data（鍵要求）

IPﾍｯﾀﾞ
送信元＝MNのｹｱ･ｵﾌﾞ･ｱﾄﾞﾚｽ
宛先＝GW1のｸﾞﾛｰﾊﾞﾙ･ｱﾄﾞﾚｽ

【図７】

IPﾍｯﾀﾞ1	KEY	AH	内部IPﾍｯﾀﾞ	data（登録要求）

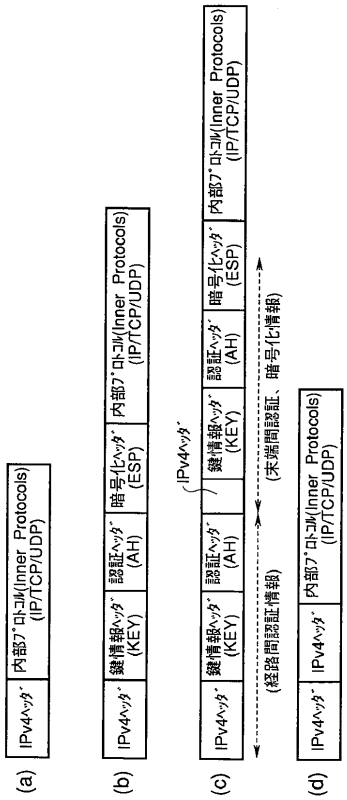
IPﾍｯﾀﾞ1
送信元＝MNのｹｱ･ｵﾌﾞ･ｱﾄﾞﾚｽ
宛先＝GW1のｸﾞﾛｰﾊﾞﾙ･ｱﾄﾞﾚｽ
内部IPﾍｯﾀﾞ（登録要求）
送信元＝MNのﾌﾟﾗｲﾍﾞｰﾄ･ｱﾄﾞﾚｽ
宛先＝HAのﾌﾟﾗｲﾍﾞｰﾄ･ｱﾄﾞﾚｽ

【図８】

IPﾍｯﾀﾞ1	KEY	AH	内部IPﾍｯﾀﾞ	data（登録応答）

IPﾍｯﾀﾞ1
送信元＝GW1のｸﾞﾛｰﾊﾞﾙ･ｱﾄﾞﾚｽ
宛先＝MNのｹｱ･ｵﾌﾞ･ｱﾄﾞﾚｽ
内部IPﾍｯﾀﾞ（登録応答）
送信元＝HAのﾌﾟﾗｲﾍﾞｰﾄ･ｱﾄﾞﾚｽ
宛先＝MNのﾌﾟﾗｲﾍﾞｰﾄ･ｱﾄﾞﾚｽ

【図９】



【図１０】

IPﾍｯﾀﾞ	KEY	AH	ESP	内部IPﾍｯﾀﾞ	data（登録要求）

IPﾍｯﾀﾞ(KEY)
送信元＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ
宛先＝GW0のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ
内部IPﾍｯﾀﾞ（登録要求）
送信元＝MNのﾌﾟﾗｲﾍﾞｰﾄ・ｱﾄﾞﾚｽ
宛先＝HAのﾌﾟﾗｲﾍﾞｰﾄ・ｱﾄﾞﾚｽ

【図１１】

IPﾍｯﾀﾞ	ICMP（通過拒否ﾒｯｾｰｼﾞ）

IPﾍｯﾀﾞ
送信元＝GW1のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ
宛先＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ

【図１２】

IPﾍｯﾀﾞ	data（鍵要求）

IPﾍｯﾀﾞ
送信元＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ
宛先＝GW1のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ

【図１３】

IPﾍｯﾀﾞ1	KEY1	AH	IPﾍｯﾀﾞ2	KEY2	AH	ESP	内部IPﾍｯﾀﾞ	data(登録要求)

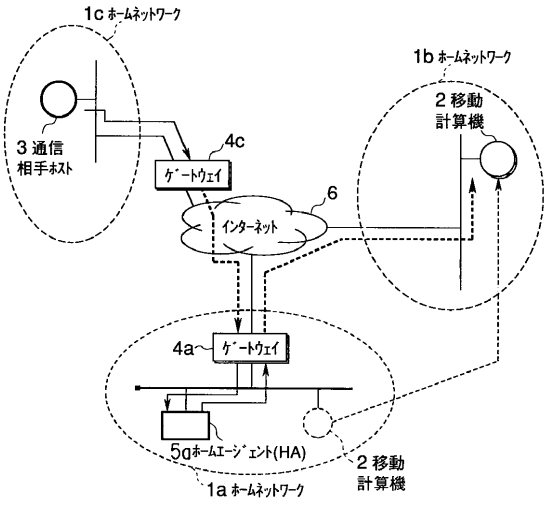
IPﾍｯﾀﾞ1
送信元＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ
宛先＝GW1のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ
IPﾍｯﾀﾞ2
送信元＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ
宛先＝GW0のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ
内部IPﾍｯﾀﾞ（登録要求）
送信元＝MNのﾌﾟﾗｲﾍﾞｰﾄ・ｱﾄﾞﾚｽ
宛先＝HAのﾌﾟﾗｲﾍﾞｰﾄ・ｱﾄﾞﾚｽ

【図１４】

IPﾍｯﾀﾞ1	KEY1	AH	IPﾍｯﾀﾞ2	KEY2	AH	ESP	内部IPﾍｯﾀﾞ	data(登録応答)

IPﾍｯﾀﾞ1
送信元＝GW1のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ
宛先＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ
IPﾍｯﾀﾞ2
送信元＝GW0のｸﾞﾛｰﾊﾞﾙ・ｱﾄﾞﾚｽ
宛先＝MNのｹｱ・ｵﾌﾞ・ｱﾄﾞﾚｽ
内部IPﾍｯﾀﾞ（登録応答）
送信元＝HAのﾌﾟﾗｲﾍﾞｰﾄ・ｱﾄﾞﾚｽ
宛先＝MNのﾌﾟﾗｲﾍﾞｰﾄ・ｱﾄﾞﾚｽ

【図１５】



フロントページの続き

(74)代理人 100070437
弁理士 河井 将次
(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 福本 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 津田 悦幸
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 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 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 衣鳩 文彦

(56)参考文献 特開平０９－２１４５５６（ＪＰ，Ａ）
特開平9-252323（ＪＰ，Ａ）
特開平10-126405（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
H04L 12/00
G09C 1/00
H04L 9/00