

研究会推薦論文

Mobile IP 用セキュリティ・ゲートウェイの
実装とその機能評価窪田 歩[†] 伊藤 篤[†] 浅見 徹[†]

インターネット利用の爆発的普及と、PCを携帯して利用するユーザの増加により、インターネットにおける、移動サポートと、移動先からの安全な通信を保証するためのセキュリティ対策はますます重要になってきている。我々は、IPのための移動サポートのメカニズムとして IETF で標準化されている Mobile IP と、同じく IP 層での認証と暗号化のための IETF 標準である IPSEC を組み合わせることにより、ファイアウォールの外部へ移動した PC から、安全かつ位置透過的な内部ホストへのアクセスを可能にする Mobile IP 用セキュリティ・ゲートウェイを開発した。本稿では、セキュアな環境での Mobile IP の問題点、IETF ドラフトで提案されている解決策、本実装で用いた方式と IETF ドラフトとの相違点、および実装したシステムの性能評価と考察結果を述べる。

An Implementation and Evaluation of
Security Gateway for Mobile IP SystemAYUMU KUBOTA,[†] ATSUSHI ITO[†] and TOHRU ASAMI[†]

As mobile computing and the use of the Internet are becoming common, it is necessary to provide secure mobility support mechanism for the Internet. Using IETF standard Mobile IP and IPSEC, we implemented a secure Mobile IP system which enables mobile nodes to access internal hosts from outside of their firewalls. This paper presents the detail of the implementation and results of performance evaluation.

1. はじめに

インターネット利用の爆発的普及と、携帯型 PC の軽量化、高性能化にともない、PC を携帯し、オフィスや外出先等、様々な場所からインターネット/イントラネットを利用する人々も増加している。このため、インターネットにおける、移動サポートと、移動先からの安全な通信を保証するためのセキュリティ対策はますます重要になってきている。我々は、IP のための移動サポートのメカニズムとして IETF で標準化されている Mobile IP¹⁾ に対し、同じく IP 層での認証と暗号化のための IETF 標準である IPSEC^{2)~4)} を組み合わせ、ファイアウォール外部へ移動した PC からの、安全かつ位置透過的な内部ホストへのアクセスを可能にする Mobile IP 用セキュリティ・ゲートウェイを開発した⁵⁾。以下では、Mobile IP の概要とセキュ

アな環境での Mobile IP の問題点、IETF ドラフトで提案されている解決策、本実装で用いた方式、ならびに実装したシステムの性能評価と考察結果について述べる。

2. Mobile IP

Mobile IP は IETF で標準化された、IP のための移動サポート機構であり、移動する端末が、同一の IP アドレスを使いながら、ネットワーク間を移動することを可能にするものである。このため、無線 LAN 等を利用して、頻りに端末を移動させるユーザにとって、アドレス変更の煩雑さがなくなるほか、セッションを継続しながらの移動が可能になる等のメリットが大きい。また、無線 LAN を使用していない場合でも、端末のアドレスによる各種アクセス制限が課せられているような環境では、端末の移動によりアドレス変更を

[†] 株式会社 KDD 研究所
KDD R&D Laboratories

本論文の内容は 1998 年 5 月のモバイルコンピューティング研究会にて報告され、同研究会主催により情報処理学会論文誌への掲載が推薦された論文である。

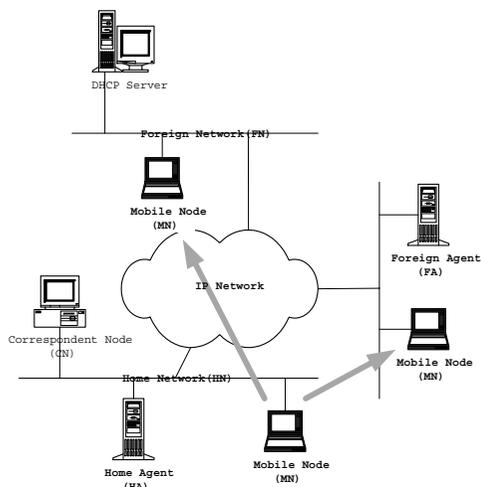


図 1 Mobile IP
Fig. 1 Mobile IP.

行った場合に生じる，ネットワーク資源へのアクセス拒否がなくなる等，移動にともなうネットワーク環境の変化を意識しなくてすむ等のメリットがある．

2.1 Mobile IP の概要

図 1 に示したように，Mobile IP では，端末の移動をサポートするために，移動端末（以下，MN: Mobile Node）が通常接続されている Home Network（以下，HN）に，MN の位置管理を行う Home Agent（以下，HA）を配置する．移動した MN は，移動先でのパケット受信に利用するアドレス（以下，CoA: Care of Address）を，パケットの転送先として HA に登録する．MN の移動先のネットワーク（以下，FN: Foreign Network）に Foreign Agent（以下，FA）が存在している場合，FA のアドレスを CoA として用い，FA 経由で HA への位置登録を行う．FA が存在しない場合には，DHCP 等により MN 自身が CoA を一時的に取得し，それを HA に登録する．位置登録の完了以降，HN に届く MN の通信相手端末（以下，CN: Correspondent Node）からの MN 宛てのパケット（オリジナルのパケット）は，代理 ARP を出して HA が MN の代わりに受信し，それを HA から CoA 宛てのパケットにカプセル化して送出する．オリジナルのパケットは，転送先で FA もしくは MN 自身によって復元され，MN の上位層プロトコルに渡される．MN から CN 宛てのパケットは，特別な処理を施さずにそのまま送出される．

2.2 セキュアな環境における Mobile IP の課題

Mobile IP では，パケットが宛先アドレスのみに基づいてルーティングされ，宛先に届くことを前提とし

ており，セキュリティのために各種の対策が施されている昨今のインターネット環境では以下の理由により有効に機能しない．

2.2.1 発信元アドレスによるフィルタリング

パケットのソースアドレスを偽造してリモート・ホストへの侵入を図る IP Spoofing Attack⁶⁾等への対策のため，プロバイダ等が管理しているインターネット上のルータにおいても，発信元アドレスに基づくフィルタリングを行って不正な発信元アドレスを持つパケットを廃棄することが一般的になっている．このため，MN から CN へのパケットのように，FN 発でありながら HN の発信元アドレスを持つようなパケットは，CN に届く前に廃棄される可能性がある．

2.2.2 ファイアウォール

HN とインターネットの間にファイアウォールが設けられているような場合，ファイアウォールによる外部からのパケットの廃棄により，MN が HA と通信できなくなるため，Mobile IP は使えない．また，ファイアウォール内部でプライベート・アドレスを利用している場合には，移動先の MN から内部ネットワークへ発せられたパケットが，宛先としてプライベート・アドレスを持つことから，そもそもインターネット上のルータでは配送不能であり，即刻廃棄される．

3. Mobile IP のセキュア環境への対応

上述の問題の発生する状況は，昨今のインターネット環境ではごく一般的なものであり，その対策は Mobile IP にとって必須である．以下では，IETF で提案されている対処法を簡単にまとめる．

3.1 IETF ドラフト⁷⁾の提案

Mobile IP のためのファイアウォール通過に関する IETF ドラフトでは，以下の仮定に基づき，トンネリングと IPSEC の利用によって，発信元アドレスに基づくフィルタリングとファイアウォールに対応した MobileIP を実現することを提案している．

- MN のドメイン内に存在するファイアウォールは複数あってもよいが，ドメインの最外のファイアウォールと，ドメイン外の FN に移動した MN の間にはファイアウォールはないものとし，かつ，FN から HN との間にある通過すべきファイアウォールの所在は既知とする（通信経路上のファイアウォールの動的な発見手法も提案されている⁸⁾）．
- ファイアウォール外へ移動した MN は FA を使わず，自分自身で CoA を取得して通信する．
- ファイアウォールは標準の IPSEC を実装する必

要はあるが、Mobile IP のメッセージを解釈する機構を実装する必要はない。

- プライベート・アドレスを利用している場合、HA はプライベートとパブリック・アドレスとの区別ができなければならない。

ファイアウォールを通過させるためには IPSEC による認証を利用し、必要であれば通信内容の機密保持のために暗号化も行う。IPSEC では各ノードが発信元アドレスと宛先アドレスの組ごとに Security Association (SA) を保持し、認証や暗号化を行うため、ファイアウォールは、MN が移動先で取得した CoA との間で SA を持つ必要がある。一般に MN が移動先で取得する CoA は既知でないので、鍵の管理・配送プロトコルを利用して、動的に SA を形成する必要がある。

発信元アドレスに基づくフィルタリングに対しては、トンネリングで対処する。まず、Mobile IP のリバース・トンネリング⁹⁾により MN から発せられるパケットもすべて CoA 発、HA 着のパケットにカプセル化する。さらに、MN から HA までの経路上の各区間 (MN からファイアウォール、ファイアウォール間、ファイアウォールから HA 等) において、送受信双方向ともに、さらなるトンネリングを行い、それぞれの区間において適正であるような発着アドレスを持つパケットへのカプセル化を行う。

以上により、ファイアウォールの外へ移動した MN も、Mobile IP を利用して、HN に接続されている場合と、通信速度や遅延の問題を除いて、同じ環境を利用することができる。ただし、以下の理由により現時点では、この方式が導入可能でない場合が多い。

3.2 導入における問題

IETF ドラフトで提案された方式は、通過すべきファイアウォールがすべて IPSEC に対応していることを前提にしている。しかしながら、現在一般的に用いられているファイアウォールでは、IP や上位層プロトコルのヘッダ情報やセッションの監視情報等に基づいて、ファイアウォール通過の可否を決定しており、IPSEC が利用されていることはまだ稀である。また、IPSEC 対応のファイアウォールであっても、現在の運用形態においては、通信相手がほぼ固定されたインターネット VPN 構築用に利用されている場合がほとんどで、鍵管理・配送プロトコルを利用して、不特定のアドレスを持つノードとの間で動的に SA を形成するような利用ができない場合が多い。

このため、IETF ドラフトで提案された方式を MN 上に実装したとしても、IPSEC 対応のためのファイアウォールの置換やアップグレードを行う必要があり、

HA や MN の機能拡張だけでは対応できないのが現状である。

4. Mobile IP 用セキュリティ・ゲートウェイの提案

先に述べたように、現状では HA や MN の機能拡張だけでは Mobile IP のファイアウォール対応は実現できないため、我々は、通常、外部に公開するサーバ等を配置するために設けられているファイアウォールの DMZ (DeMilitarized Zone : 非武装地帯・公開サーバ群を配置するためのセグメント) 上に、Mobile IP 用のセキュリティ・ゲートウェイ (以下、SGW) を設置する構成で、Mobile IP のファイアウォール対応を図った。Mobile IP 専用に SGW を開発したため、このゲートウェイ部分で標準的な IPSEC の処理の他に、Mobile IP のメッセージの解釈を行わせることも可能となり、これを利用して鍵配送機構の省略等、実装の簡略化を行っている。以下に、実装の詳細について述べる。

4.1 実装

MN を Windows 95 上に、HA と SGW を FreeBSD 上に実装し、MN と HA についてもファイアウォール通過のための機構を付加した。標準の Mobile IP としての動作をさせる場合には、RFC2002 準拠の MN、HA、FA との相互接続が可能であるが、ファイアウォールの通過が必要な場合には、MN と HA とともに、標準 (RFC2002) の Mobile IP に準拠した実装は使えない。基本的に、IETF ドラフトでの提案と同様、IPSEC とトンネリングを用いた実装を行ったが、前述のとおり、SGW 上に Mobile IP のメッセージを解釈させる機構を組み込んだことで、MN、SGW 間の SA の確立手順を省略している。

4.2 条件

Mobile IP 用の SGW の実装にあたり、以下の条件を仮定した。

- SGW はパブリック・アドレスを持ち、外部のノードとの間で、プロキシ等を介在させない直接の通信が可能のように、ファイアウォールやルータが設定されている。
- 内部ネットワーク上にさらに複数のファイアウォールが設置されている場合、SGW と HA との間でのプロキシ等を介在させない直接の通信ができるよう、内部のファイアウォールのパケット・フィルタリング・ルールを設定することができる。

2 点目の条件によって、SGW が外部からの侵入を受けた場合に、無条件で HA へのアクセスが可能とな

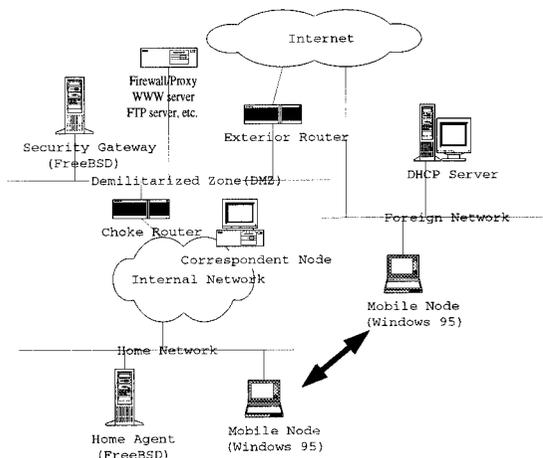


図2 システム構成
Fig. 2 System configuration.

るが、HA が中継を行うのは Mobile IP の認証に成功した MN のパケットのみであるので、即、侵入の被害が内部に及ぶことはない。ただし、HA には SGW が侵入を受けた場合に備えて、外部からの攻撃に対するセキュリティの強化等、通常、公開用のサーバ等に施すセキュリティ対策を施す必要である。

以上の条件の妥当性に関する考察については後で述べることとし、以下ではシステム構成、Mobile IP の各パケットの通過の仕組みについて説明する。

4.3 システム構成

図 2 に示したように、本システムは IPSEC を用いた Mobile IP 用の SGW、HA、MN から構成されている。インターネット上のホストと SGW 間の通信と、SGW と HA 間の通信はルータやファイアウォールの設定であらかじめ許可されている。SGW と MN は相互の IPSEC による通信のための SPI (Security Parameters Index) 値と鍵を共有する。現バージョンでは IPSEC の AH (Authentication Header) 用には keyed MD5 を、ESP (Encapsulating Security Payload) 用には DES のみを実装している。この構成で、MN は HA、CN との間の通信を以下のように行う。

4.4 MN と SGW 間の SA の確立

インターネット上に移動した MN は DHCP 等により自分自身で CoA を取得し、この CoA を用いて SGW との通信を行うため、SGW はこの CoA に対して SA を確立しなければならない。今回、SGW を Mobile IP 用として開発したため、SGW に Mobile IP の登録メッセージを読み取らせる機能も組み込み、Mobile IP の登録の成否によって SA の確立を決定することとし、IPSEC の鍵管理プロトコルの実装は省

[Registration Request Message のカプセル化手順]

SGW ← MN			
src=CoA	src=CoA	UDP	Registration request
dst=SGW	dst=HA	header	

HA ← SGW			
src=SGW	src=CoA	UDP	Registration request
dst=HA	dst=HA	header	

[Registration Reply Message のカプセル化手順]

SGW ← HA			
src=HA	src=HA	UDP	Registration reply
dst=SGW	dst=CoA	header	

MN ← SGW			
src=SGW	src=HA	UDP	Registration reply
dst=CoA	dst=CoA	header	

図3 MN、HA 間の Mobile IP 登録メッセージ
Fig. 3 Mobile IP registration message between MN and HA.

略した。このため、SGW は、Mobile IP 登録メッセージ用の UDP ポートを用いた外部ホスト-HA 間のパケットは、認証ヘッダなしで無条件に中継する。

4.5 Mobile IP 登録メッセージ

Mobile IP 登録メッセージが、MN から SGW、SGW から HA 等のパケットにカプセル化されて MN、HA 間で送受される様子を図 3 に示す。まず MN は HA への登録メッセージを SGW 宛てのパケットにカプセル化して送出する。SGW は受信したパケットの中身が、あらかじめ登録された HA 宛ての Mobile IP 登録メッセージである場合のみ、IPSEC の認証ヘッダなしでもパケットの転送を行う。HA への転送の際にオリジナルのパケットをそのまま内部ネットワーク上に流すと、発信元アドレスが CoA となり、内部ネットワーク上のルータの発信元アドレスに基づくフィルタリングによって廃棄される可能性があるため、これを SGW 発、HA 着のパケットにカプセル化して送出する。

HA は登録メッセージに対し Mobile IP の認証処理を行い、CoA に宛てた応答メッセージを作成するが、これを SGW 宛てのパケットにカプセル化して送出する。SGW は応答メッセージの内容を読み取り、HA による MN の認証が成功した場合には、4.3 節で述べたように MN に対してあらかじめ用意した SPI と鍵を用いて、CoA との間での SA を設定した後、オリジナルの応答メッセージを SGW 発、MN 着のパケットにカプセル化して送出する。

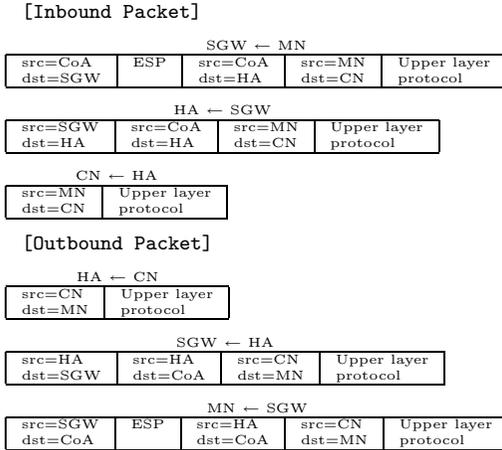


図4 Mobile IP登録後のメッセージ
Fig. 4 Message after mobile IP registration.

4.6 MNとCN間のパケット

登録完了後のMN, CN間の通信はHAとSGWを経由して行い, MN-SGW間ではIPSECを用いた認証と暗号化を行う.

図4に示すように, MNからのCN宛てパケットの場合, MNはCN宛てのパケットを, CoA発, HA着のパケットにカプセル化した後, これをCoA発, SGW着のパケットのESPとして暗号化して送出する.

SGWはESPの復号を行い, 取り出したパケットを, 発信元アドレスによるフィルタリング対策のため, SGW発, HA着のパケットにカプセル化して送出する.

HAはSGWから受け取ったパケットよりオリジナルのパケットを取り出して送出し, これがHome Networkから発せられたMN発, CN着のパケットとして配送されて最終的にCNまでパケットが届く.

CNからMN宛てのパケットは, HAが代理ARPを出してMNの代わりに受信し, これをCoA宛てのパケットにカプセル化した後, さらにHA発, SGW着のパケットにカプセル化して送出する.

HAからのパケットを受け取ったSGWは, HA発, CoA着のパケットを取り出し, これをCoA宛てのパケットのIPSECのESPとして暗号化し, CoA宛てに送出する.

MNはSGWからのパケットを受信し, ESPの復号を行った後, オリジナルのCN発, MN着のパケットのペイロード部分を上位層プロトコルに渡す.

以上により, インターネット上に移動したMNとCNとの間の通信がSGWとHAを経由して行われる.

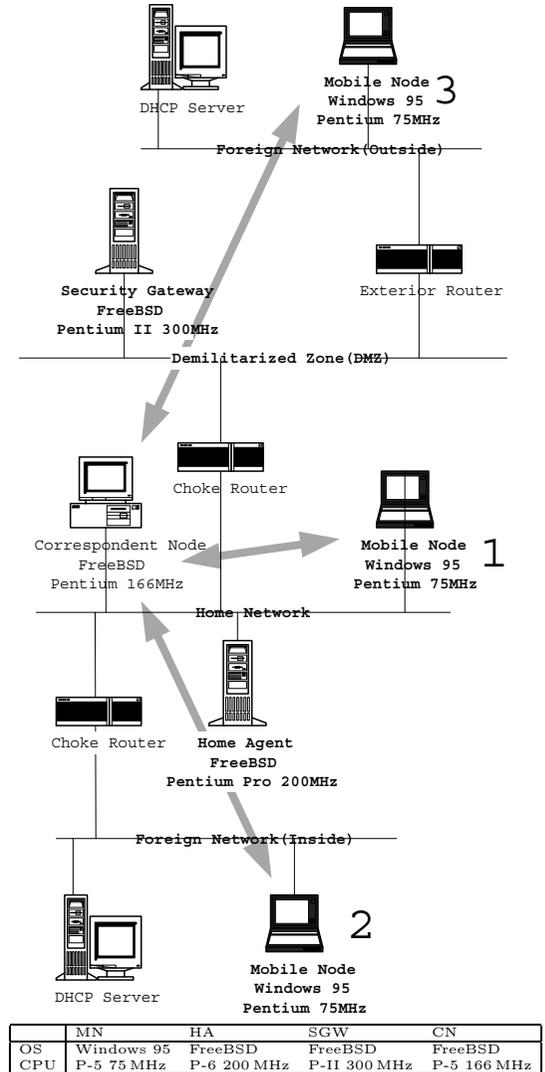


図5 実験構成
Fig. 5 Testing configuration.

5. 評価と考察

ここでは実装したシステムを用いて行った性能評価の結果と考察について述べる.

5.1 性能評価

10MbpsのEthernetで構成した図5に示す実験ネットワークにおいて, HN上に配置したCNとMNとの間で行ったスループット測定の結果を表1に示す. MNをHN(図5中の1)からファイアウォール内部のFN(図5中の2)およびファイアウォール外部のFN(図5中の3)に移動させ, それぞれの場合について, RTTは100回のpingの平均値を, パケット・サイズ64バイトで測定し, MN-SGW間については, パケッ

表 1 性能測定結果

Table 1 Results of performance measurement.

64 byte RTT (msec)	HN	FN (Inside)	FN (Outside)
without encryption	1.16	3.38	—
with encryption	—	4.19	8.93

n byte RTT (msec)	64	300	600	900	1200
MN-SGW	8.93	15.63	19.57	23.30	27.34

Throughput (Mbps)	HN	FN (Inside)	FN (Outside)
without encryption	5.75	3.44	—
with encryption	—	1.57	1.49

トサイズを変化させて測定を行った。スループットは netperf による測定値 (TCP_STREAM テスト, メッセージ・サイズ 32 Kbyte) である。ファイアウォール内部の FN への移動時については, MN-HA 間通信の暗号化を行う場合と行わない場合それぞれについて測定を行った。RTT に関しては, パケットサイズが 64 バイトの場合, SGW と HA を経由させ, 暗号化も行った場合でも, パケット・サイズ 64 バイトで 9ms 弱, パケット・サイズ 1200 バイトで 27ms 弱と, 実用上問題のない程度である。スループットは DES を用いた暗号化による影響が大きく, SGW 経由での通信を行う場合, HN 上での通信時に比べ 1/4 程度に低下するが, 約 1.5 Mbps という値は, ファイアウォール外からのリモート・アクセス時のスループットとしては十分といえる。

5.2 考 察

本実装は, Ishiyama らの実装⁸⁾と同等のシステム構成をとっているが, Mobile IP の登録メッセージに基づいて SGW と MN の SA を設定するため, 鍵交換の手順を省略しており, MN がファイアウォールの外部へ移動した場合, HA への登録のオーバーヘッドは小さくなっている。ただし, 鍵の更新作業等はマニュアルで行う必要があるため, 今後鍵管理プロトコルの実装についても検討する予定である。

以下では, 実装にあたり仮定した条件の妥当性についての考察を行う。ファイアウォール内部のネットワークでプライベート・アドレスを利用している場合でも, 公開サーバ等を配置するために, パブリック・アドレスを持ち, 外部からのアクセスを許可する DMZ セグメントを配置している場合が多い。そのため, 4.2 節に示した条件の 1 点目は, 一般的なパケット・フィルタリング型ファイアウォール利用時の条件に反するものではない。ただし, 内部と外部ネットワークとの間のいっさいの IP 転送を禁止し, プロキシのみによって内部-外部間の通信を実現している場合は本実装のファイアウォールとの共存は不可である。これは 2 点目の

条件についても同様であり, このような場合, ファイアウォール上に Mobile IP 用のプロキシを実装する必要がある。

条件の 2 点目は内部ネットワーク上での設定に関するものなので, 技術的には問題がないが, SGW, HA 間の通信を固定的に許可することの妥当性は問題となる。本来, MN は通過すべきすべてのファイアウォールとの間で個別に認証されることが望ましいので, すべてのファイアウォールが IPSEC 対応であれば, MN が送出するパケットに各ファイアウォールごとの認証ヘッダを付加することによって, パケットの通過を許可させるべきである。我々の実装では, この部分を省略し, SGW と HA 間に存在しているファイアウォールは, SGW と HA 間の通信を無条件で許可するものとしたため, HA の行う MN の認証結果のみによってインターネット上のホストから発せられたパケットの, 各ファイアウォールの通過が可能となる。ただし, これによって許可されるのは MN からホーム・ネットワークへの通信のみであり, HA を経由した後に CN へ向けて発せられる MN 発のパケットが内部のファイアウォールを通過する際には, 各ファイアウォールで独立に定められたセキュリティ・ポリシーに基づいて, 通過の可否が決定されることになる。このため, 必ずしも各ファイアウォールの持つセキュリティ・ポリシーの独自性が失われることにはならない。今後は各ファイアウォールごとに個別の認証を行う機構の実装についても検討する予定である。

本システムの運用上の問題として, SGW をファイアウォールとは別に設けることや, MN の認証情報と鍵が, 内部ネットワークに存在する各 HA 上と SGW に分散すること等により, HA や MN の数が増加した場合に, セキュリティの適切な管理が困難になることがあげられる。このため, SGW と複数の HA の設定を連携させ, 一元的に管理できるようなツールの開発も必要と考えられる。

6. おわりに

Mobile IP の実用化においてはファイアウォール対策が必須であるが, IETF ドラフトの提案方式は, IPSEC 対応ファイアウォールが一般化していない現時点での導入には問題があるため, 既存ファイアウォールと共存させる構成で, Mobile IP のファイアウォール通過機構を提案し, その実装結果について評価を行った。今後実ネットワークでの利用を通して問題点を洗い出し, 改修や機能拡張を施していく予定である。

謝辞 日頃ご指導いただく KDD 研究所の皆様へ,

謹んで感謝の意を表する。

参 考 文 献

- 1) Perkins, C.: IP Mobility Support, RFC 2002 (Oct. 1996).
- 2) Atkinson, R.: Security Architecture for the Internet Protocol, RFC 1825 (Aug. 1995).
- 3) Atkinson, R.: IP Authentication Header, RFC 1826 (Aug. 1995).
- 4) Atkinson, R.: IP Encapsulating Payload, RFC 1827 (Aug. 1995).
- 5) 窪田 歩: SOHO ネットワークとセキュリティ, *ON THE LINE*, 3月号, p.8 (1998).
- 6) CERT Advisory CA-96.21: TCP SYN Flooding and IP Spoofing Attacks. available at ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding.
- 7) Gupta, V.: Firewall Traversal for Mobile IP: Guidelines for Firewalls and Mobile IP entities, Draft <draft-ietf-mobileip-firewall-trav-00.txt>, work in progress (Mar. 1997).
- 8) Ishiyama, M., Inoue, A., Fukumoto, A. and Okamoto, T.: Design and Implementation of Mobile IP System with Security Consideration, *Worldwide Computing and Its Applications, WWCA '98* (1998).
- 9) Montenegro, G.: Bi-directional Tunneling for Mobile IP, Draft <draft-ietf-mobileip-tunnel-reverse-00.txt>, work in progress (Feb. 1997).

(平成 10 年 11 月 25 日受付)

(平成 11 年 12 月 2 日採録)

推 薦 文

インターネットにおける移動サポートと、移動先からの安全案通信を保証することは、必須の技術項目である。本論文では、移動先から安全に自分のホストへのアクセスを可能にする方法を提案しており、その提案手法に基づき、実験システムを作成し、実用化が可

能であることを示している。今後、実際のネットワーク上での運用が期待でき、本論文は高く評価できる。(モバイルコンピューティング研究会主査 水野忠則)



窪田 歩 (正会員)

1993年3月, 京都大学工学部情報工学科卒業, 1995年3月, 同大学大学院情報工学専攻修了, 同年国際電信電話(株)に入社。以来, KDD研究所において, IPモビリティ, ネットワーク管理, ポリシー・ベース・ネットワーク等の研究に従事。



伊藤 篤

1981年3月, 名古屋大学工学部電子工学科卒業, 1983年3月, 同大学大学院情報工学専攻修了, 同年国際電信電話(株)に入社。1985~1999年, KDD研究所において仕様記述言語, 通信ソフトウェア開発環境, IN, インターネット等の研究に従事。1991~1992年, スタンフォード大学 CSLI 客員研究員。現在, 先端技術ビジネス推進部所属。



浅見 徹 (正会員)

1974年京都大学工学部電子工学科卒業, 1976年同工学大学院修士課程修了。同年国際電信電話(株)入社。以来, ファクシミリ通信, データ通信, ネットワーク障害診断システムの研究実用化に従事。現在(株)KDD研究所取締役, (株)KDD コミュニケーションズ取締役。IEEE, 電子情報通信学会, 情報処理学会各会員。第43回前島賞受賞。