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 System

AYUMU KUBOTA ,† ATSUSHI ITO † and TOHRU ASAMI†

As mobile computing and the use of the Internet are becoming common, it is nessesary 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 implementaion 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，高性能化に伴い，PCを携帯し，オフィスや外出先など，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 IP[1]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．

† 株式会社KDD研究所
KDD R&D Laboratories

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などを利用して，頻繁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など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など，移動に伴うネットワーク環境の変化を意識しなくて済むなどのメリットがある．

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 (Care of Address, 以下

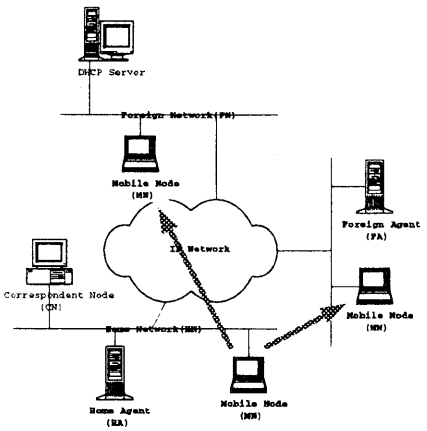


図 1 Mobile IP
Fig. 1 Mobile IP

CoA) 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 (Foreign Network, 以下 FN) 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 (Correspondent Node: 以下 CN) 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 Attack[6] などへの対策のため，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毎に 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全て CoA 発，HA 着のパケットにカプセル化する．更に，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など)において，送受信双方向ともに，更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も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全て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などに基づいて，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，IPSECの鍵管理と配送のプロトコルがまだドラフト段階である現状においては，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を形成することができず，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セグメント上に，MobileIP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など，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供に，標準

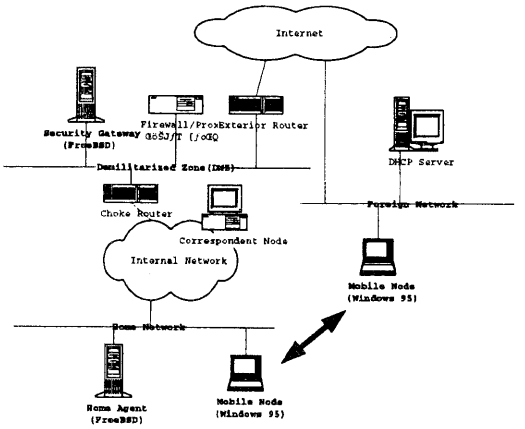


図2　システム構成
Fig. 2　System Configuration

(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，前述の通り，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なように，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更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，それらを設定することができる．

この条件の妥当性の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 Parameter 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 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ので，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．

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，AH を付加して送出する．(AH は設定により省略可．)

SGW は AH によるパケットの認証と 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，更に HA 発，SGW 着のパケットにカプセル化して送出する．

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

SGW ← MN

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

HA ← SGW

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

[Registration Reply Message のカプセル化手順]

SGW ← HA

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

MN ← SGW

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

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

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，更に IPSEC の AH(Authentication Header) を付加して CoA 宛てに送出する．

MN は SGW からのパケットを AH を用いて認証し，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．

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

図 5 に示す実験構成において，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 1,2 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 32Kbyte) 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

[Inbound Packet]

SGW ← MN

src=CoA dst=SGW	AH + ESP or ESP	src=CoA dst=HA	src=MN dst=CN	Upper layer protocol

HA ← SGW

src=SGW dst=HA	src=CoA dst=HA	src=MN dst=CN	Upper layer protocol

CN ← HA

src=MN dst=CN	Upper layer protocol

[Outbound Packet]

HA ← CN

src=CN dst=MN	Upper layer protocol

SGW ← HA

src=HA dst=SGW	src=HA dst=CoA	src=CN dst=MN	Upper layer protocol

MN ← SGW

src=SGW dst=CoA	AH + ESP or ESP	src=HA dst=CoA	src=CN dst=MN	Upper layer protocol

図 4 Mobile IP 登録後のメッセージ

Fig. 4 Message after Mobile IP Registration

表 1 性能測定結果

Table 1 Results of performance measurement

64byte 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

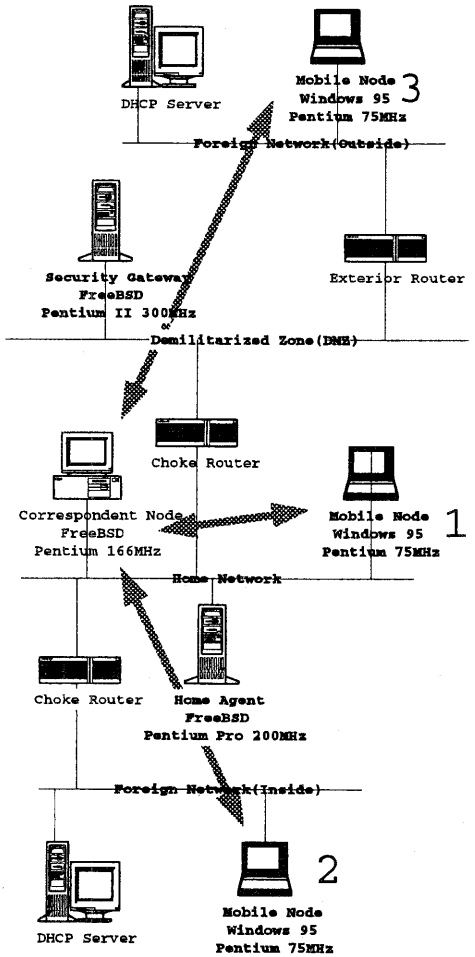
間通信の暗号化を行う場合と行わない場合それぞれについて測定を行った．RTT に関しては，パケットサイズが 64 バイトの場合，SGW と HA を経由させ，暗号化も行った場合でも，パケット・サイズ 64 バイトで 9ms 弱，パケット・サイズ 1200 バイトで 27ms 弱と，実用上問題のない程度である．スループットは DES を用いた暗号化による影響が大きく，SGW 経由での通信を行う場合，HN 上での通信時に比べ 1/4 程度に低下するが，約 1.5Mbps という値は，ファイアウォール外からのリモート・アクセス時のスループットとしては十分と言える．

5.2 考　　察

本実装は，石山らの実装[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の，HA への登録のオーバ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一切の 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



	MN	HA	SGW	CN
OS	Windows 95	FreeBSD	FreeBSD	FreeBSD
CPU	P-5 75MHz	P-6 200MHz	P-II 300MHz	P-5 166MHz

図 5 実験構成

Fig. 5 Testing configuration

る．本来，MN は通過すべき全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，全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毎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．だだし，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毎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 に分散することなどにより，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挙げられる．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 研究所の皆様に，謹んで感謝の意を表する．

参考文献

1) C. Perkins, "IP Mobility Support", RFC 2002, October 1996.
2) R.Atkinson, "Security Architecture for the Internet Protocol", RFC 1825, August 1995.
3) R.Atkinson, "IP Authentication Header", RFC 1826, August 1995.
4) R.Atkinson, "IP Encapsulating Payload", RFC 1827, August 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, p8, 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) V. Gupta, "Firewall Traversal for Mobile IP: Guidelines for Firewalls and Mobile IP entities", Draft <draft-ietf-mobileip-firewall-trav-00.txt>, work in progress, March 1997
8) Masahiro Ishiyama , Atsushi Inoue , Atsushi Fukumoto and Toshio Okamoto, "Design and Implementation of Mobile IP System with Security Consideration", Worldwide Computing and Its Applications-WWCA '98, 1998
9) G. Montenegro, "Bi-directional Tunneling for Mobile IP", Draft <draft-ietf-mobileip-tunnel-reverse-00.txt>, work in progress, Feb. 1997.