第 12 部

モーバイルコンピューティングにおけるセキュリティ

第 1 章

IP Security を利用した安全な Mobile IP

1.1 はじめに

インターネットと携帯端末など移動通信機器の普及に伴い、組織内ネットワークにインターネットを介してアクセスを行う、モバイルコンピューティングへの期待が高まっている。このような通信では、組織内の機密性の高い情報に対し、(セキュリティ保証のない) インターネット経由でアクセスを行うため、セキュリティを考慮した通信サポートが必須である。

本章では、IETF で標準化が行われている IP セキュリティと Mobile IP を組み合わせることにより、セキュアなモバイルコンピューティング環境を IP 層処理で構築するアプローチについて提案する。提案システムは security/mobility 複合プロトコルを実装した Security Gateway と移動端末から構成される。特に移動先の端末からのセキュリティを保持したゲートウェイ透過方式について説明する。また、現在の実装状況も報告する。

1.2 Key Technologies

1.2.1 Mobile IP

IP version 4 では、IP アドレスはホスト識別子かつネットワーク上の位置識別子である。したがって、端末が IP ネットワーク上で移動した場合、それまでの IP address は使用し続けることは出来ない。よって端末が移動した場合は、その移動したネットワークに割り当てられた IP アドレスに変更して通信することが必要となる。一方、IP アドレスはホスト識別子でもあるので、移動により IP アドレス が変ることはユーザの利便性を損ねることになる。

Mobile IP [?] はこのような問題を解決するために提唱された。これは移動端末に対して一定の IP アドレスを利用することを可能にし、IP ネットワーク上での移動透過性を与える。Mobile IP の概略を以下に述べる。

- Mobile Node は 1 つの Home Address をもつ。Home Address は Mobile Node がネットワーク上の位置を変えても使用し続けることができる address である。

- Care-of-Address(CoA) は、Mobile Node が移動した先のネットワークにおいて使用する address である。CoA は Foreign Agent から指定される address か、もしくは DHCP などで直接 Mobile Node に割り当てられる address である。後者の場合は特に co-located care-of-address と呼ばれる。

- Home Agent は、Mobile Node から情報を受け取って、Mobile Node の現在位置 (care-of-address) 等を管理する。また、Mobile Node が移動した場合、Mobile Node の代わりにパケットを受取り、これを Mobile Node へ転送する役割を果たす。Home Agent は Mobile Node の Home Network に配置される。

- Foreign Agent は各移動先のネットワークに配置され、移動してきた Mobile Node に対して CoA を指示し、また Home Agent が転送してきたパケットを受け取って Mobile Node へと転送する役割を果たす。Mobile Node が co-located CoA を使用した場合には Foreign Agent は必要ない。

- Mobile Node は、移動するとまず CoA を取得する。CoA を取得したら、Home agent (Foreign Agent がいる場合には Foreign Agent) に対して登録を行う。これが成功すると、Home Agent は、 Mobile Node 宛 (すなわち destination address が Mobile Node の Home address) であるパケットを代わりに受け取り、CoA を destination として IPinIP でカプセル化 [?] し転送する。

- Mobile Node が co-located CoA を使用する場合には、Home Agent が転送したパケットは直接、移動した Mobile Node に到着するので、Mobile Node は自身でこれをデカプセル化し、自分の Home address 宛のパケットを得る (図 1.1)。

  Foreign Agent が存在する場合、Home Agent からの転送パケットは Foreign Agent に到着する。Foreign Agent はこれをデカプセル化し、得た Home Address 宛のパケットを (IP のルーティングによってではなく) link layer によって Mobile Node に転送する。

1.2.2 IP security

IP 層におけるセキュリティの要求に答えるために、IETF では IP security protocol(IPsec) が提案された [?]. IPsec では 2 つの機構を提供している。1 つは Authentication Header(AH)[?] と呼ばれるもので、AH は一般的にデータの完全性 (integrity) や、データ発信者の認証 (Authentication) を提供する。もう一つは Encapsulating Security Payload(ESP)[?] と呼ばれるもので、これは一般的に秘匿性 (confidentiality) と完全性および認証を提供する。

AH および ESP では、様々な暗号化および認証アルゴリズムが使用できる。実際にどのようなアルゴリズムが使用されるかは、セキュリティ・アソシエーションによって定まるとされている。これは認証アルゴリズムや暗号化アルゴリズム、その鍵といったパラメー

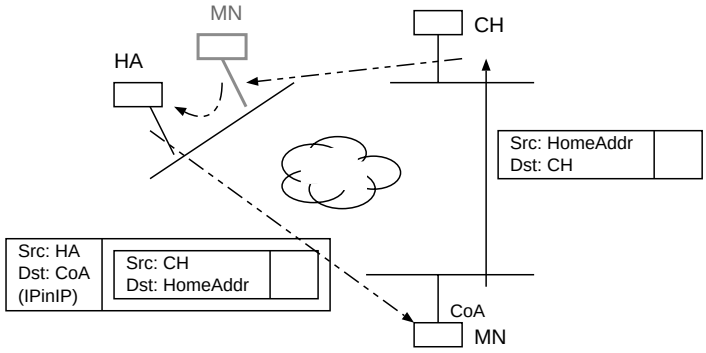


図 1.1: Mobile IP の動作

タの集合である。AH および ESP には Security Parameter Index(SPI) と呼ばれるパラメータがあり、セキュリティ・アソシエーションは SPI と destination address の組から一意に定まるものとされている。よって、IPsec を使用するためには、通信相手と事前にセキュリティ・アソシエーションの内容について合意しなければならない。セキュリティ・アソシエーションの管理は鍵管理プロトコルの果たすべき役割とされている。

1.3　解決すべき問題

前述のように Mobile IP により移動端末は IP ネットワーク上での移動透過性を得ることができる。しかし Mobile IP をそのまま使用して、移動先から組織内ネットワークにアクセスを行う場合、幾つかの危険性がある。

1.3.1　組織内ネットワークに入るパケットの問題

Mobile IP では、移動した Mobile Node が送信するパケットの source address は自分の Home Address である。このパケットは Mobile Node のホームネットワークから見ると、内部 address を詐称して外部からアクセスする IP アドレス偽造攻撃 (IP address spoofing attack) のパケットと区別が付かない。もし組織ネットの入口に防火壁が設置されている場合、このパケットは通過拒否されることがありうる。逆にこのパケットが通過できるなら、その組織のネットワークは IP アドレス偽造攻撃に対し無防備であることになり、非常に危険である。

Mobile IP の規定では、Home Agent と Mobile Node との間では暗号技術を使用した認証が行われるので Mobile Node へのなりすましは困難であるとされている。一方、Home Agent は Mobile Node の Home Address 宛のパケットについては処理を行うが、Home Address 発のパケットがネットワーク外部から第三者に送られてきても何もチェックする方法がない。

即ち Mobile IP の枠組では、前述の IP アドレス偽造攻撃の問題は防止できないといえる。

1.3.2 移動先ネットワークを出る際の問題

Mobile Node は移動先ネットワークの防火壁とも問題を起こすかも知れない。これはたとえば移動先のネットワークを保護する防火壁が、情報の流出を意識して、外部へでていくパケットに制限を科しているような場合である。

1.3.3 通信の秘匿性の問題

一般に、あるネットワークが防火壁によって守られている場合、そのネットワークは安全であると仮定しており、外部の人間に見られては困る秘密情報でも、暗号化などの保護を施すことなく通信することができる。

しかし Mobile Node が組織外に移動し、保護されているネットワークの中と通信を行うと、その秘密情報は組織外ネットワークに転送されるので、盗聴の危険が発生する。即ち Mobile Node に送られる情報は何らかの秘匿処理を行われることが必要である。

以上述べたように、Mobile IP を用いて組織内ネットワークへ安全にアクセスするためには、

(1) IP パケットの偽造からの防御
(2) 防火壁の安全な乗り越え方法
(3) 通信の秘匿性の確保

が必要である。

1.3.4 IPsec と Mobile IP を組み合わせた場合の問題

前節の要求はすべて IPsec によって解決出来る。IPsec では、AH および ESP により通信の完全性を、ESP により通信の秘匿性を保証する。

前節の要求 (1) に対しては、IPsec が AH で提供する完全性の性質によって、受け取ったパケットが確かに Mobile Node が送信したものであることを保証してやればよい。要求 (2) に対しても、Mobile Node と防火壁の間で AH を使用し、防火壁が受信したパケットが、それを乗り越えることができる Mobile Node から送られてきたパケットであること、またそれが改竄されていないことを保証してやればよい。要求 (3) については、 IPsec が ESP で提供する秘匿性の性質によって、通信を盗聴などから守ることができる。外部の Mobile Node に向かって流れるパケットについては防火壁と Mobile Node 間で ESP で暗号化し、第三者に盗聴されないようにすれば良い。

すなわち、上記の Mobile Node、防火壁間の課題は IPsec の導入で解決出来ると考えられる。IPsec と Mobile IP は IP プロトコル的には独立に設計されているので、互に干渉する部分はなく、両者をそのまま使用できる。

しかし、Mobile IP と IPsec を組み合わせることで新たな問題も発生する。Mobile Node が IP ネットワークを移動しながら、IPsec で通信するため、移動箇所によって IPsec の相手が変化するという問題である。たとえば図 1.2の場合において、Mobile Node がホスト H1 と通信する場合、位置 A にいたときには防火壁 FW を乗り越える必要があるが、位置 B に移動すればその必要はない。逆に、ホスト H2 と通信する場合にはその逆となる。

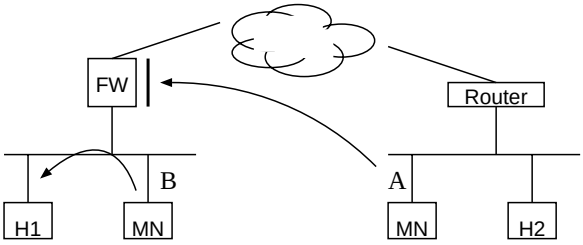


図 1.2: Mobile Node が移動した時の乗り越えるべき防火壁の変化

すなわち、Mobile Node は、位置を変更する度に、各通信相手宛の経路上で、どの防火壁を乗り越えなければならないのかを判断する必要がある。一般には乗り越えるべき防火壁は複数個ありうる。これは、組織内の一部署が防火壁を設置するような場合に相当する。

1.4　提案システム

提案システムの典型的な構成図を図 1.3に示す。IPsec を処理できる防火壁を Security Gateway(SGW) と呼ぶ。全ての防火壁は IPsec を処理できる SGW であるとする。SGW は通常の防火壁のように組織内ネットと外部との境界に置かれる。また、組織内の特定の部署などのネットワークを保護するために、入れ子状の配置も許すと仮定する。

Mobile Node のホーム (サブ) ネットワークには、Home Agent が配置される。また Mobile Node の通信相手 (CH で表わされている) は SGW のポリシーが許す限りにおいてはシステム内の任意の位置に存在して良い。

1.4.1　Security Gateway

前述の通り、SGW は、自分が保護するネットワークの各ホストに (IPsec 処理を含む) セキュリティサービスを提供する。各 SGW は適切に管理され、通信が許されているネットワーク間の SGW は、お互いの存在をあらかじめ知っているものとする。

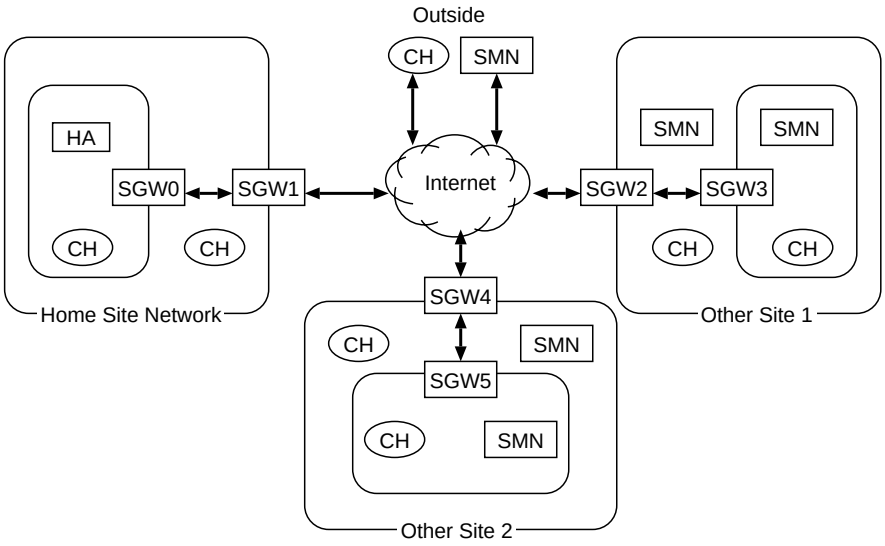


図 1.3: 典型的な構成図

1.4.2 Secure Mobile Node

Mobile Node も同様に IPsec を処理できなければならない。以後この Mobile Node を Secure Mobile Node(SMN) と呼ぶ。SMN は co-located care-of-address を使用する。すなわち、SMN は Home Agent が転送してきたパケットを自分でデカプセル化することができ、Foreign Agent は必要としない。

1.4.3 提案システムに関する仮定

提案システムの構成、各構成要素の動作、管理条件については、以下を仮定する。

- 提案システムでは、IP アドレスの重複はない、 即ち、1 つの IP アドレスに対して唯一つのホストが定まるものとする。

- SMN が Mobile IP を使用して通信できる相手ホストは、その Mobile Node が Home Network にいる時に通信できる (reachability がある) 相手であるとする。すなわち、SMN がどこに移動しても、(Mobile Node 宛のパケットを移動先へ中継する)Home Agent と、その通信相手となるホストとの通信は可能であるとする。

- SGW は専門知識を持つ管理者が管理することを期待することができるのに対して、SMN は一般のユーザが使用すると仮定する。このため、SMN が静的に持つ情報というのは出来るだけ少なくするべきである。

1.5　乗り越えるべき SGW の発見

前述のように、SMN が移動した場合、相手ホストへの経路が変化するために乗り越えるべき SGW もまた変化する。しかし、SMN 上にすべての SGW およびその SGW が保護するネットワークの集合をあらかじめ設定しておくというのは、SMN 上の情報を出来る限り少なくしたいという要求に反する。よって、ある宛先に対してどの SGW を乗り越えるかを動的に発見する必要がある。

1.5.1　動的な発見方法

基本方針は、SGW が SMN に対して、通過の際に何らかの認証が必要であることを伝えるというものである (たとえば [?], [?])。

通常の防火壁では、パケットを受信した時にそのパケットを受信 (あるいは転送) または破棄するかどうか決定する。これはその防火壁の持つセキュリティポリシーにしたがって決められる。SGW ではセキュリティポリシーの中に、“そのパケットを通過させても良いが、認証が必要である” という考え方を持っている。そして SGW がパケットを受信して、そのパケットに必要な認証がなされていない場合には、認証が必要であることをそのパケットの source address(これは通常 SMN である) に向けて通知する[1]。

各 SGW 間の認証要求は IPsec の AH 機能を使用できる。この認証要求を受けて、Mobile Node は乗り越えるべき SGW リストに認証要求の送信元の SGW を追加する。

Mobile Node MN が SGW S1 を乗り越えてホスト H と通信するという例で説明する (図 1.4).S1 は MN と H の間の経路上にある。まず MN は、通常の IP パケットをホスト H に向けて送信する。S1 はこのパケットを H へ転送するには認証子が必要と判断し、認証要求をパケットの source address、すなわち MN へ送信する。MN はこれを受けて、乗り越えるべき SGW のリストに S1 を追加する。

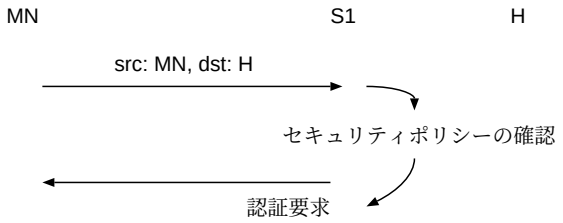


図 1.4: 動的なゲートウェイの発見

[1] この認証要求は、SMN の Home Address に向けて返される場合があるので、認証要求を出した SGW と SMN 間以外の経路を辿ることもある。ここでは SGW 間における認証要求の透過性は保証されていると仮定する

1.5.2 動的な発見と組織外ネットワーク

SGW を使用している組織では、組織内経路を組織外に流していない場合が多い。前節の動的 SGW 発見は、宛先の通信相手に対し、経路上の乗り越えるべき SGW にパケットが到着することを前提としている。よって Mobile Node の現在地から宛先に向けて経路が存在しなくてはいけないが、組織外ネットワークに移動した場合、これを期待することができない。

これを回避するために default border gateway を定義する。border gateway は組織内と組織外のネットワークの接点にいる SGW を指す。Mobile Node は最低 1 つ、次のような情報を持たなければならない。

(border gateway, 全組織内ネットワーク*)*

全組織内ネットワークは、組織中で使用しているネットワークであり、指定されている border gateway に限らず、いずれかの border gateway で保護されている、ネットワークアドレスのすべての集合である。たとえば、図 1.3では、Home Site Network、Other Site 1、Other Site 2 の 3 つのネットワークがこれにあたる。

このように指定された border gateway を default border gateway と呼ぶ。Mobile Node は、全組織内ネットワークの集合に自分の care-of-address が含まれておらず、かつ通信相手が全組織内ネットワークの集合に含まれている場合には、(動的な発見を行うことなく) この border gateway を Next-Hop の SGW とする。

ただし border gateway は、自分が誤った border gateway であった場合、すなわちパケットを受信して、IPsec の処理 (認証や復号) をしたが、その結果えたパケットの宛先が自分の保護するネットワークに該当せず、そのパケットを新たに他の border gateway へと転送しなければならない場合、border gateway 間でも適切な IPsec 機構を使用してこの転送を行わなければならない (図 1.5)。

default border gateway を使用する利点は以下のようなものである。

まず、Mobile Node がすべての border gateway(とその border gateway が保護するネットワークの集合) を知らなくても、組織外ネットワークから組織内ネットワークへの安全な通信を行う事が可能になる点である。また、すべての SGW が動的な発見に対応していれば、この default border gateway(と全組織内ネットワークの集合) だけを知ってれば良いことになる。

また、防火壁はその性質上、出来るだけ外部にその情報を与えない方がよい、という考え方が強い。よって多くの防火壁は不必要なパケットは出来るだけ出さず、“静か” であることが望まれている。これは、特に border gateway のような The Internet のあらゆる場所から攻撃される可能性がある場合に言える。一方、SMN は動的な SGW の発見のために、SGW からの応答を期待しているが、これは前述の考え方に反しているので何らかの折衝点を求めることが必要である。

本方式では、すべての SMN が (少なくとも 1 つの)default border gateway を知ることによって、SMN と default border gateway 間では動的な経路発見でなされるようなメッセー

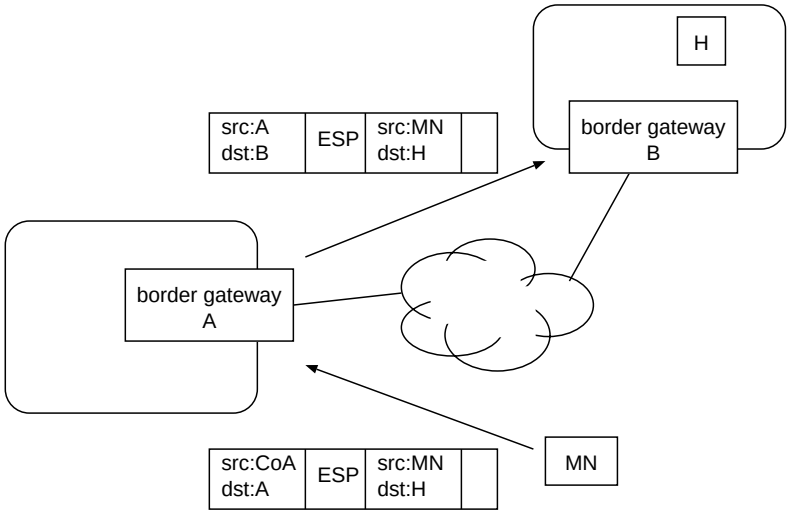


図 1.5: border gateway 間の転送

ジのやり取りは起こらない。従って SMN が組織外に移動した場合に、SMN、default border gateway 間の The Internet を流れるパケットを最小にし、border gateway をより安全に保つことができる。

1.6　通信モデル

1.6.1　IPsec を使用した SGW の乗り越え方

乗り越えるべき SGW が分れば、SMN は各 SGW とのセキュリティ・アソシエーション (SA) の共有を行う。鍵交換の方法は本稿の範囲外であるが、SKIP[?] や ISAKMP[?] などの鍵管理プロトコルなどを使用することができる。

各 SGW に対して SA を設定するので、その結果にしたがって各 SGW のために IPsec の機構を用いる。たとえば、Secure Mobile Node SMN とホスト H が通信する場合で、乗り越えるべき SGW が順に S1, S2 だとする。S1, S2 それぞれと ESP を使用するように SA を設定したとする。SMN は、H へ送信するパケットを、まず S2 との SA を使用して S2 宛に ESP 化する。次に S2 宛のパケットを、S1 との SA を使用して S1 宛に ESP 化する。S1 はこのパケットを受信して処理し、デカプセル化したパケットを転送する。転送されたパケットは、IP ヘッダにしたがって S2 へと送られる。S2 も同様に ESP を処理し、デカプセル化したパケットを転送する。転送されたパケットは、IP ヘッダにしたがって H へと送られる。SMN が S1, S2 それぞれのために ESP をつけているので、S1, S2 ともに送信者が SMN であるということを認証することができる。動的な SGW の発見との手続きを合わせた通信の流れを図 1.6に示す。

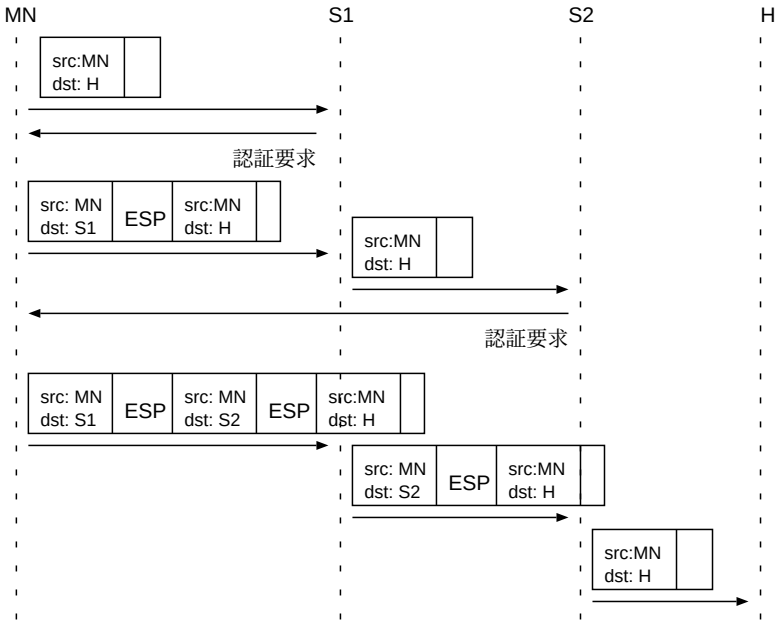


図 1.6: IPsec を用いて SGW を乗り越えるときのパケット

1.6.2 発見すべき SGW

乗り越えるべき SGW を発見しなければならない PATH は大きく 2 つに分けられる。1 つは、Mobile Node の移動地点から Home Agent までの PATH である。この PATH は登録要求/応答と、HA が転送してくれる IPinIP パケットが使用する。Mobile Node は、移動したらまずこの PATH を確保し、Home Agent に対して Mobile IP の登録を行う。

もう一つは、Mobile Node から、通信する相手への PATH である。この PATH は Mobile Node から通信相手へ向かうパケットが使用する。通信する相手から、Mobile Node 宛 (これは Home Agent が受け取る)PATH は、Mobile Node が Home Network にいるならば通信できる前提があるので、この PATH は意識する必要はない。

どちらの PATH においても、IPsec を使用する場合、SMN が外側の IP ヘッダに使用する address は ICMP unreachable 等のエラー情報を受け取る場合のことを考えると、care-of-address が望ましい。各 SGW は、そのパケットが Security Mobile Node からのものであるということを認識できなければならない。したがって、SMN は、care-of-address を使用しても各 SGW が SMN であると認識できるように SA の内容について合意する必要がある。

1.7　実装と性能

1.7.1　実装の現状

現在、プロトタイプシステムを BSD/OS 2.1 上で実装している。プロトタイプシステムは大きく以下の 3 つで構成される

- Mobile IP node
- Mobile IP home agent
- IPsec module

大部分は application として実装した。また実装した暗号化アルゴリズムは DES および Triple-DES であり、認証用のハッシュ関数は MD5 である。鍵管理プロトコルとしては SKIP を実装した。ただし、動的な SGW の発見はまだ実装していない。

1.7.2　性能

IPsec および Mobile IP のオーバヘッドを測定するために、TCP の bulk transfer rate を測定した。測定には Netperf[2] を使用した。テストに使用した環境を図 1.7に示す。また、結果を表 1.1に示した。fragment を起こさないようにするために、MTU = 1300 とした。

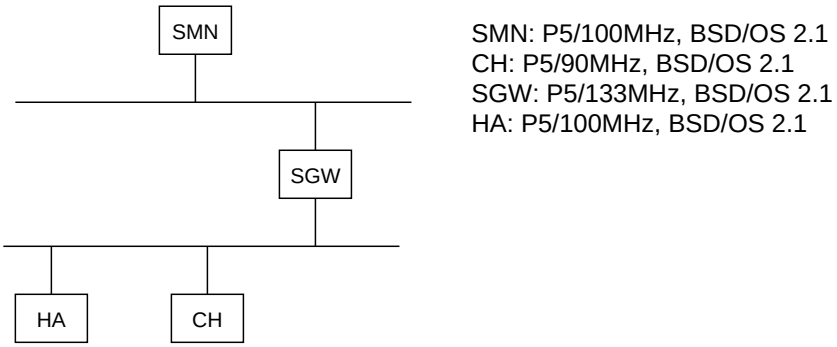


図 1.7: 性能測定に使用した環境

Plain IP(1) は、Mobile IP や IPsec を使用せずに計測した結果である。SGW はただの router として動作させた。Mobile IP(2) は Mobile IP だけを使用し、この時も SGW はただの router として動作させた。IPsec(3, 4) は鍵管理プロトコルに SKIP を使用し、AH だけの場合と、AH と ESP を同時に使用したものを計測した。IPsec は SGW と SMN の間で使用した。MIP+IPsec(5, 6) は、Mobile IP と IPsec を同時に使用して計測した。

[2]URL: http://www.cup.hp.com/netperf/NetperfPage.html

	プロトコル	送信側→受信側	Mbit/sec
1	Plain IP (via router)	SMN → CH	7.04
	Plain IP (via router)	CH → SMN	6.96
2	Mobile IP	SMN → CH	5.72
	Mobile IP	CH → SMN	2.11
3	IPsec (AH only)	SMN → CH	3.22
	IPsec (AH only)	CH → SMN	2.42
4	IPsec (AH+ESP)	SMN → CH	1.97
	IPsec (AH+ESP)	CH → SMN	1.74
5	MIP+IPsec (AH only)	SMN → CH	2.08
	MIP+IPsec (AH only)	CH → SMN	1.09
6	MIP+IPsec (AH+ESP)	SMN → CH	1.33
	MIP+IPsec (AH+ESP)	CH → SMN	0.89

表 1.1: 性能測定の結果

(1), (2) を比較すると、特に CH から SMN への性能が悪い。これは、送信側から受信側へのパケットには payload がのり、逆側は Ack だけのパケットであるので、HA の転送オーバヘッドに加えて、CH からの大きな payload の乗ったパケットが HA でカプセル化されて SMN へ転送されるために、CH のいるリンクを 2 回通り、バンド幅を 2 重に消費するのが大きな原因であると考えられる。(5) を見ると、IPsec のオーバヘッドもかなり大きいことが分かる。

Mobile IP と IPsec を同時に使用した場合、計測する前には、IPsec だけを使用する場合に比べてそれほど大きく性能は劣化しないのではないかと考えていた。理由は以下の 2 点である。

- SMN から送られるパケットの、各ホストでの処理は、IPsec だけを使用した場合と変らない。
- SMN へと送られるパケットは、Mobile IP は HA、IPsec は SGW とそれぞれ分散して処理され、SMN では IPinIP をデカプセル化する処理が増えるだけである。よって IPsec 復号化などの処理オーバヘッドが支配的で、Mobile IP 分の影響は小さいと予測した

しかし (6) と (4) を比較する限り、無視できない性能の劣化が認められる。今後、この原因を究明していきたい。

本プロトタイプは、モジュールの大部分は user application で実装しているため、基本的に kernel〜user 空間のデータのコピーなどに多くのオーバヘッドがあると考えられる。

kernel 内で実装した場合には、より高速な結果が期待できる。

1.8　おわりに

本章では、Mobile IP と IP security を使用することによって、安全な mobility computing を可能とするシステムを提案した。提案システムは固定的に配置された組織や部署のネットワークを守るための SGW と、ネットワーク上の任意の点に移動できる Mobile Node、およびその移動をサポートする Home Agent からなる。Mobile Node はネットワーク上の任意の位置から通信したい相手の経路上にある乗り越えるべき SGW を自動的に発見し、発見した SGW それぞれに対して IPsec の機構を使用することで安全に各 SGW を乗り越えることができる。また、BSD/OS 上で本システムのプロトタイプを実装した。プロトタイプでは、高速な LAN 環境ではオーバヘッドが大きすぎるが、比較的低速な WAN を介した通信や、電話回線等を通した通信であれば十分使用に耐える速度であると考えられる。

今後は動的な SGW の発見の実装を行い、提案方式のの妥当性を検証していきたい。また、本稿ではすべての防火壁を SGW と仮定したが、すでに存在する防火壁との共存方式についても考えていきたい。現在、IETF においても Mobile IP の防火壁の乗り越えに関する議論は注目を集めている。これらの動向をふまえながらこの技術の確立および標準化に貢献していく。

第 2 章

VIPv3 における安全なファイアウォール通過機構

2.1 はじめに

筆者らは移動透過な通信機能を提供するプロトコルとして、1991 年に IP を拡張した Virtual Internet Protocol, version 1 (VIPv1)[?] を開発した。VIPv1 においては、不正なコンピュータが容易に他のコンピュータになりすますことができるため、1994 年に VIPv1 に認証機能を付加した VIPv2[?] を開発した。VIPv2 により、原理的には移動コンピュータとの移動透過な通信機能は実用段階に達したと言える。

しかし実際のインターネット環境においては、各組織は外部ネットワークとの接点にファイアウォールを設置し、組織内部のセキュリティを保っている。ファイアウォールは、一般的にある決められたサービスに関しては内側から外側への通信は可能であるが、外側から内側への通信は遮断する。このような環境では、プロトコルの点では移動透過な通信が可能であるにもかかわらず、外部に接続した移動コンピュータから自組織内部のコンピュータと通信することができない。一般的な利用形態では、移動コンピュータと自組織内のサーバコンピュータ (たとえばメールサーバ) との通信は頻繁に行われると考えられる。移動コンピュータと自組織内のコンピュータとの通信が遮断されると、移動コンピュータの通信機能の価値は半減してしまう。これはモーバイルコンピューティングにとっての大きな問題であった。

VIPv3 は安全なファイアウォール通過機能を実現するとともに、コンピュータ単体の移動透過性に加えてサブネット単位での移動透過性 [?] も実現した。サブネット単位での移動透過性に関しては別の機会に譲り、本稿では安全なファイアウォール通過機能に焦点を当てる。

以下、第 2.2節では VIP の概要を述べる。第 2.3節では VIPv3 に関して、ファイアウォール通過機構に焦点を当てて述べる。第 2.4節では VIPv3 の実装について述べる。第 2.5節ではファイアウォール通過機能の安全性について考察し、第 2.6節では関連研究について述べる。最後に第 2.7節で本稿をまとめる。

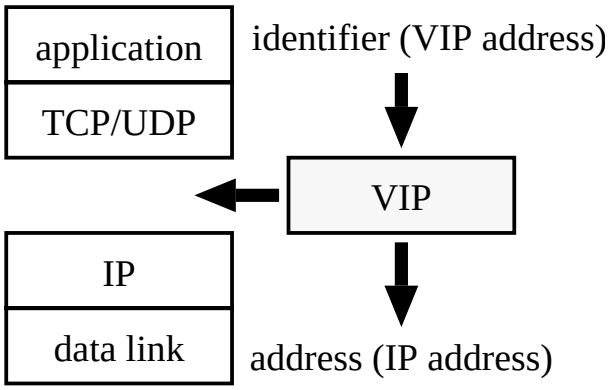


図 2.1: プロトコル階層

2.2　VIP の概要

2.2.1　VIP の原理

移動透過な通信とは、相手コンピュータの場所にかかわらず、一定不変の識別子を用いて相手コンピュータと通信ができ、TCP コネクションのような論理通信路が移動の前後で維持できることであると定義できる。インターネットにおいて移動透過な通信ができないのは、IP アドレスが持つアドレスと識別子という二重性のためである。

VIP は位置指示子 (アドレス) と識別子を明確に分離することにより移動透過性を実現している。具体的には、位置指示子である IP アドレスに加えて識別子として VIP アドレスを導入した。VIP アドレスと IP アドレスは同一のフォーマットを持っており、それだけではどちらであるのか区別がつかない。オペレーティングシステムの仮想記憶システムにおける仮想アドレスと物理アドレスの関係に対応付けられる。

プロトコル階層の観点からは、図 2.1に示すように IP 層と TCP/UDP 層の間に VIP 層を挿入する。TCP/UDP 層以上では VIP アドレス (識別子) でコンピュータを識別する。VIP 層が VIP アドレスを IP アドレス (位置指示子) にマッピングし、得られた IP アドレスに従って IP 層がパケットを配送するのである。

VIP アドレスから IP アドレスへのマッピングを効率よく行うために、VIP 層で AMT(Address Mapping Table) と呼ばれるキャッシュを持つ。AMT は複数のエントリから構成され、各エントリは 1 台の移動コンピュータに対応する。AMT エントリは、VIP アドレス、IP アドレス、バージョン番号、その他の管理情報から構成される。

移動コンピュータが送信するパケットのヘッダは送信コンピュータの VIP アドレスと IP アドレスを含んでいるので、途中のルータや最終的な受信コンピュータはヘッダから送信コンピュータの VIP アドレスと IP アドレスの関係を知り、AMT エントリを作成する。このように、原則として移動コンピュータが送信したパケットの経路に沿って AMT エント

リが拡散して行く。

2.2.2 VIPv2 における認証機構

VIP アドレスは位置に依存しない番号であるため、他のコンピュータの VIP アドレスを偽ること (なりすまし) は容易である。VIPv2 の認証機構は、不正なコンピュータによる他のコンピュータへのなりすましを防止することが目的である。

VIPv2 では keyed MD5 と呼ばれる方式を用いている。MD5[?] とは一種のチェックサム計算法であり、任意長のデータから 16 オクテットのデータ (MD: Message Digest) を生成する。MD5 の結果が特定な値を持つようなデータを生成することは非常に困難であるとされているため、MD5 は通常改竄防止に使われる。すなわち送信側で送信データに関して MD5 を計算し、計算結果をデータに付加して送信する。受信側はデータ部分に関して MD5 を計算し、計算結果を受信したものと比較する。両者が一致すれば、通信途中に改竄が行われていないことがわかる。

keyed MD5 では、送信側と受信側で秘密鍵を共有する。送信側ではデータに秘密鍵を付加したものについて MD5 を計算し、計算結果をデータに付加して送信する。受信側では受信したデータに秘密鍵を付加して MD5 を計算し、計算結果を受信したものと比較する。両者が一致すれば、通信途中に改竄が行われていないことがわかると同時に、送信側と受信側が秘密鍵を共有していることもわかる。第三者が秘密鍵を知らないと仮定すれば、受信者は送信者が “ほんもの” であることがわかる (認証できる)。

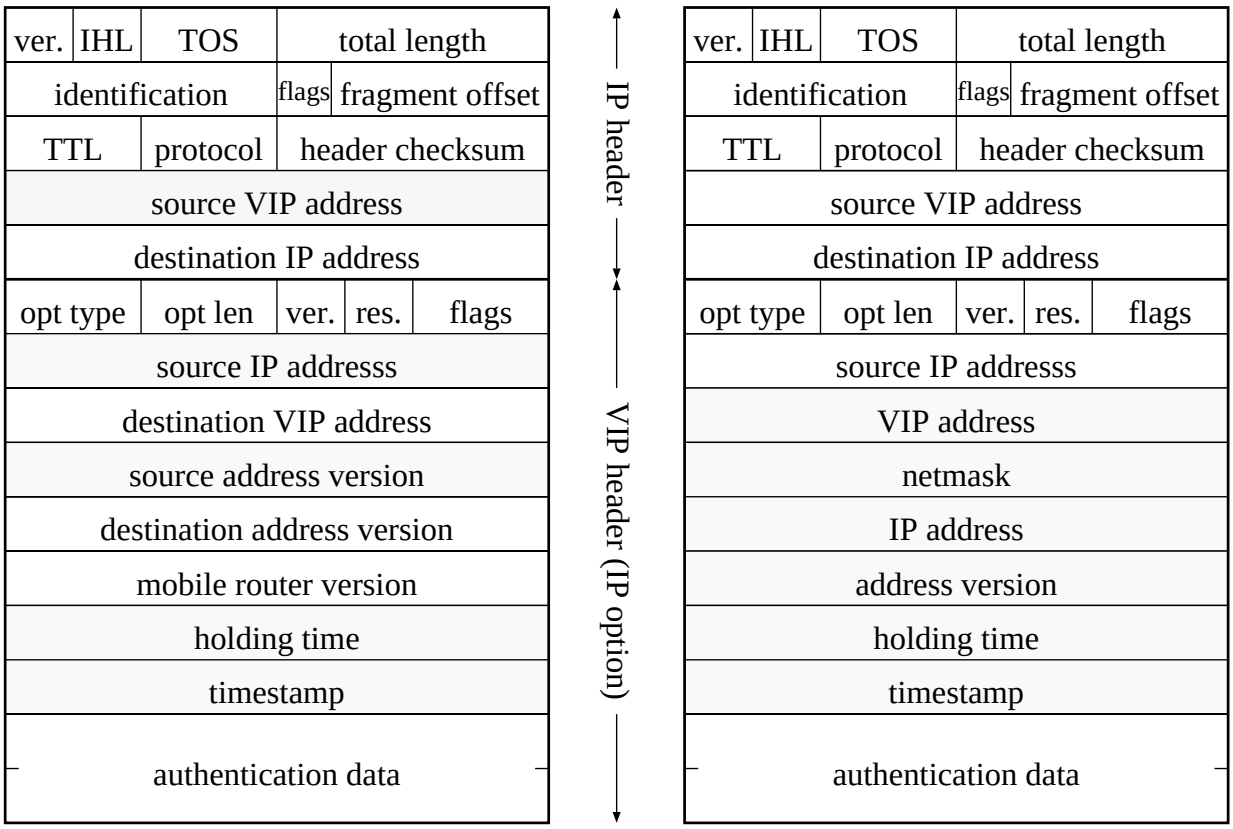
具体的に VIPv2 では、送信コンピュータは自分の VIP アドレス、IP アドレス、アドレスバージョン、AMT エントリ保持時間、タイムスタンプの合計 20 オクテットのデータに、128 ビット (16 オクテット) の秘密鍵を付加して MD5 の計算を行っている。

2.3 VIPv3 の機能

VIPv3 の特徴は、移動コンピュータ単体のみでなくサブネット単位での移動透過性の実現と、安全なフィアウォール通過機構である。VIPv3 は VIPv2 の上位互換であり、VIPv3 を実装しているコンピュータは VIPv2 パケットを正しく処理することができる。

2.3.1 サブネット移動透過性

コンピュータ単体の移動透過性実現のために識別子 (VIP アドレス) と位置指示子 (IP アドレス) を分離し、それぞれが仮想メモリシステムにおける論理アドレスと物理アドレスに対応づけられることは前に述べた。サブネット移動透過性実現のためにこの考えを発展させ、論理サブネット番号と物理サブネット番号という考え方を導入した。位置に依存しないサブネット全体の識別子が論理サブネット番号であり、移動サブネットの実際の位置を示すのが物理サブネット番号である。VIPv3 では、具体的にはパケットヘッダにネット



(a) data packet　　(b) control packet

図 2.2: パケットフォーマット

マスクのフィールドを導入することによって論理/物理サブネット番号を表現している。サブネット移動透過性に関する詳述は別の機会に譲る。

2.3.2　ファイアウォール通過機構

VIPv2 の認証機能は送受信コンピュータ間で行うことを目的として導入したが、VIPv3 ではこれをファイアウォールに応用した。移動コンピュータとファイアウォールで秘密鍵を共有し、送信コンピュータが本当に自組織に属する移動コンピュータであることが確認できたときにのみ、ファイアウォールは外側から内側へ IP パケットを中継するのである。

図 2.2に VIPv3 のパケットフォーマットを示す。以前のバージョンと同様に、VIPv3 も VIP ヘッダを IP オプションとして実装している。これは既存の IP との互換性を保つためである。

移動コンピュータは認証データを次のように計算する。図 2.2で、影付きのフィールドに 128 ビットの秘密鍵を付加した合計 36 オクテット (コントロールパケット場合は 40 オクテット) のデータについて MD5 を計算する。MD5 は 16 オクテットのデータを生成するが、パケットヘッダ長の制限により、16 オクテットのデータを 8 オクテットずつに分けて

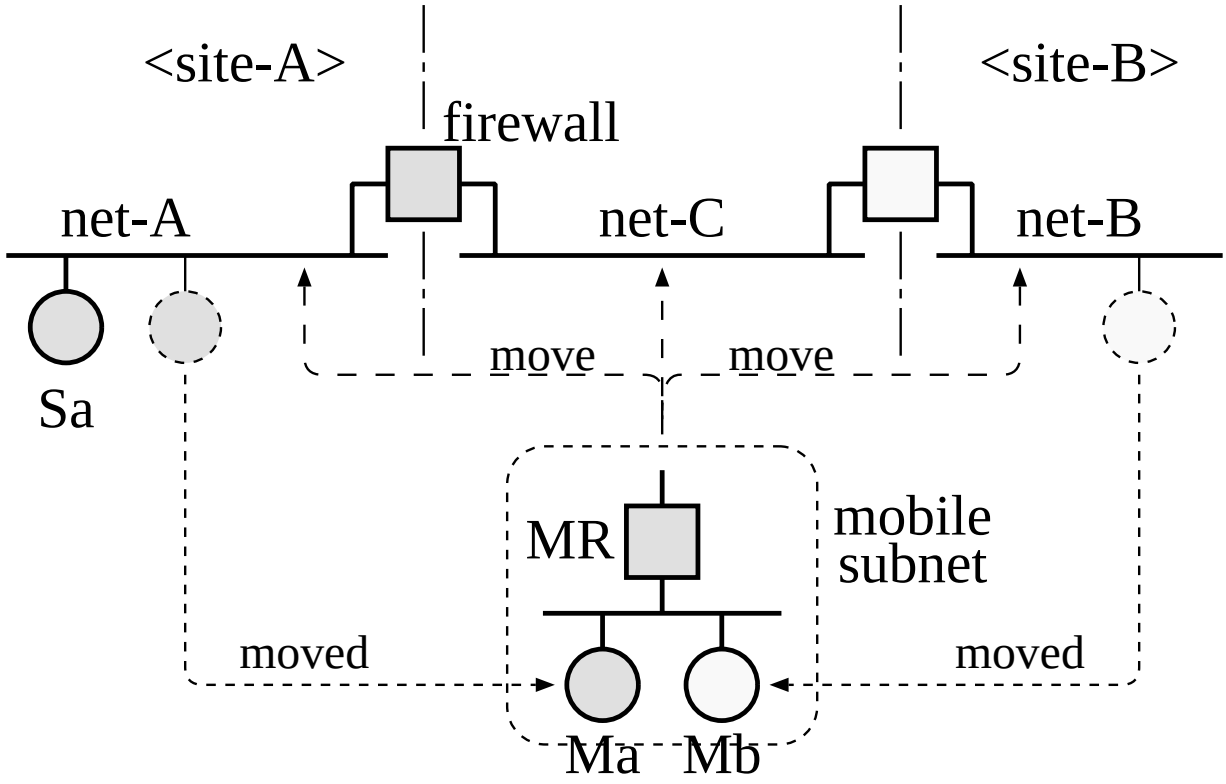


図 2.3: 実験環境

排他的論理和をとることによって 8 オクテットのデータに縮約し、ヘッダの Authentication Data フィールドに代入する。

ファイアウォールでは、移動コンピュータと共有している鍵を用いて送信側と同様の計算を行い、計算結果をパケットの Authentication Data フィールドの値と比較する。両者が一致すれば、移動コンピュータの VIP アドレスは正しく (移動コンピュータは “ほんもの” であり)、通信途中にヘッダが改竄されていないことがわかる。なお、VIPv3 は鍵配送プロトコルを含んでいない。

2.4 実装

現在 VIPv3 は IBM-PC 互換機で動作する UNIX である BSD/OS-2.1 上で動作している。VIPv3 の実装はオペレーティングシステムカーネルの変更、ユーザモードで動作するデーモンプロセスが 1 つ、およびいくつかのコマンドからなる。カーネルファイル (/bsd) の大きさは、VIPv3 を実装することにより約 14.4kbyte 大きくなっている (774.2kbyte から 788.6kbyte に増加)。

表 2.1: keyed MD5 の実行時間

CPU	実行時間
Pentium 166MHz	22 μsec
i486-DX4 75MHz	74 μsec

2.4.1　実験環境

図 2.3に実験環境を示す。実験環境は以下のように構成されている。2 台のルータが 3 つのネットワーク (net-A, net-B, net-C) を接続している。組織-A (net-A) と組織-B (net-B) が広域ネットワーク (net-C) に接続しているという想定である。組織-A はファイアウォールを介して広域ネットワークに接続している。組織-A には固定コンピュータ Sa が接続している。移動コンピュータ Ma は組織-A に属し、図では移動サブネットに接続している。移動コンピュータ Mb は組織-B に属し、同じく移動サブネットに接続している。移動サブネットは移動ルータ MR を介して net-A, net-B, net-C 間を移動する。さらに Ma, Mb は移動サブネットから離れて、単体で net-A, net-B, net-C 間を移動する。ファイアウォールと移動コンピュータ Ma は秘密鍵を共有している。

以上のような構成で、以下の動作の確認を行った。

- Ma, Mb の接続位置にかかわらず、それぞれの VIP アドレスを指定することによって、ファイアウォールと Ma, Mb それぞれとの間に TCP コネクションを確立することができる。
- その後、Ma, Mb それぞれ単体での移動、および移動サブネットに接続しての移動を行っても、TCP コネクションが維持され、データ通信を正しく行うことができる。
- Ma, Mb 双方が移動サブネットに接続し、移動サブネットが net-C に接続している状態で、Ma と Sa はファイアウォールを介して通信を行うことができるが、Mb は Sa と通信することはできない。
- Mb に Ma の VIP アドレスを割り当て (Mb が Ma になりすまし)、Sa と通信しようとしても失敗する。この状態でも、Ma と Sa は正しく通信することができる。

2.4.2　認証の実行時間

今回の実装では、ファイアウォールとして Pentium (166MHz) を CPU として持つコンピュータを用いた。また、移動コンピュータとしては i486-DX4 (75MHz) を CPU として持つコンピュータを用いた。それぞれのコンピュータでの keyed MD5 の実行時間の実測値を表 2.1に示す。

ファイアウォール通過のためには移動コンピュータとファイアウォール双方で keyed MD5 の計算を行う必要がある。したがって、実験環境における MD5 の計算によるオーバーヘッドは、96 μsec となる。一般的にインターネットでの通信時間は最低でも 10 msec のオーダーとなるので、MD5 の計算によるオーバーヘッドは無視できる。

IP に対する VIPv3 のオーバーヘッドを考えると、MD5 の計算時間に加えて送信側において VIP ヘッダを作成する時間、および受信側において VIP ヘッダを解析する時間も考慮する必要がある。残念ながら今回の実験環境においてはこれらの時間はまだ測定していない。過去の実測値から推測するとこれらの時間は合計 100 μsec 以下となり、通信時間に比較した VIPv3 のオーバーヘッドは無視し得るほど小さい。

2.5 考察

2.5.1 認証機構の強度

VIPv3 においては、第三者が通信中の VIPv3 パケットを盗み見ることにより、keyed MD5 の計算に使用されているデータ (秘密鍵を除く) と計算結果を得ることができる。すなわち keyed MD5 において元データと計算結果が既知の場合における秘密鍵の解読の困難さが VIPv3 の認証機構の強度となる。

MD5 は任意長のデータから 16 オクテットのデータを生成するため、計算結果から元データを逆計算で求めることはできない。したがって、全数計算以外に秘密鍵を求める方法はない。秘密鍵は 128 ビットであるので、鍵の総数は $2^{128} = 3.4 \times 10^{38}$ 個である。期待値は 1/2 となるので、1.7×10^{38}回 MD5 の計算をする必要がある。第 2.4.2節の測定結果から、現在の PC クラスの計算機で 1.7×10^{38}回 MD5 の計算を行うと、3.7×10^{33}秒 $\approx 10^{26}$年かかることがわかる。仮に PC の 100 万倍高速なスーパーコンピュータで計算しても、10^{20} 年かかることになる。したがって、VIPv3 の認証機構は十分な強度を持っていると言える。

2.5.2 鍵配送

VIPv3 は秘密鍵配送のプロトコルを含んでいない。すなわち手動でファイアウォールと移動コンピュータに共通の秘密鍵を設定する必要がある。前節での議論でわかるとおり、VIPv3 の認証機構は十分な強度を持っているので、実用上はある程度の間隔 (たとえば 1ヶ月) で秘密鍵の変更を手動で行えばよい。運用面から考えると、ファイアウォールと移動コンピュータは同一組織内に属するものであるので、手動で設定することはさほど問題にはならないと思われる。

インターネットにおけるプロトコルの標準化動向を見ると、いくつもの鍵配送プロトコルが提案されており、いずれ標準プロトコルが決まるものと思われる。標準プロトコルが決まったら、それを使用することも可能である。

2.6　関連研究

2.6.1　Mobile-IP

IETF という組織がインターネットにおけるプロトコルの標準化作業を行っている。IETF で標準化作業が行われている移動透過性プロトコルを通称 Mobile-IP[?] と呼ぶ。Mobile-IP では、移動コンピュータは通常の IP パケットを送信する。したがって、Mobile-IP のみでは VIPv3 のようにファイアウォールで移動コンピュータを認証することはできない。さらに Mobile-IP には移動コンピュータとの通信において経路が冗長になる等の問題点がある。

2.6.2　IP Security

IP のためのセキュリティメカニズム [?] も提案されている。この中には、IP データグラムの改竄防止および送信ノードの認証を目的とした認証ヘッダ [?] も定義されている。この認証機構は送受信コンピュータ間でセキュリティアソシエーションと呼ばれる関係を確立する必要があり、通信経路の途中に存在するファイアウォールが移動コンピュータを認証することは考慮されていない。

2.7　おわりに

ノートブックコンピュータを持ち歩き、行く先々で自組織のメールサーバにアクセスしてメールの読み書きをしているユーザーも多いと思われる。Windows95 には IP アドレスを自動的に取得するプロトコルである DHCP[?] が実装されており、このような利用形態も容易に実現できるようになってきた。しかしファイアウォールが設置されている環境では、このような利用をすることができない。

VIPv3 では各パケットには送信コンピュータの識別子とその認証のためのデータが含まれており、ファイアウォールにおいて移動コンピュータからのパケットを安全に自組織内へ中継することができる。認証機構は十分な強度を持っており、認証のためのオーバーヘッドは無視できるほど小さい。さらに VIPv3 はコンピュータ単体での移動透過性だけでなく、サブネット単位の移動透過性も実現している。今後は VIPv3 をさまざまプラットフォームに実装する予定である。