2004－ＣＳＥＣ－26　(34)
2004／7／21

IPsec/IKE によるセキュアなシームレスローミング方式の試作

武仲 正彦† 藤本 真吾† 藤野 信次‡

† 富士通株式会社 〒674-8555 明石市大久保町西脇 64

‡ 富士通株式会社 〒211-8588 川崎市中原区上小田中 4-1-1

E-mail: †{ma, shingo_fujimoto}@jp.fujitsu.com, ‡fujino@jp.fujitsu.com

あらまし ユビキタス環境では移動端末にいつでもどこでも変わらないネットワーク接続を提供することが大変重要である．ユビキタス環境を支える技術に IPsec/IKE による VPN 技術がある．しかし，既存の VPN システムでは IP アドレスが頻繁に変化する移動端末は考慮されていなかった．このため，SCIS2004 で我々は IKE に独自の拡張を加えることで，移動端末へのサポートを強化する手法を提案していた．本論文では，先の提案を実証するプロトタイプの実装に成功したのでこれについて報告する．試作は，富士通の IPsec/IKE 規格に準拠した VPN 製品を元にしている．試作では，IP アドレスが頻繁に変化する移動端末に対しても，安全で接続の切れない VPN 接続，「セキュア・シームレスローミング」が実現可能であることを確認した．

キーワード IPsec/IKE，シームレスローミング，実装

Implementation of Secure Seamless Roaming Method by IPsec/IKE

Masahiko TAKENAKA†, Shingo FUJIMOTO† and Nobutsugu FUJINO‡

† FUJITSU LTD. 64 Nishiwaki, Ohkubo-cho, Akashi, Japan

‡ FUJITSU LTD. 1-1 Kamikodanaka 4-chome, Nakahara-ku, Kawasaki, Japan

E-mail: †{ma, shingo_fujimoto}@jp.fujitsu.com, ‡fujino@jp.fujitsu.com

Abstract It is most important requirement that the mobile nodes are connected with the network , anytime, anywhere, on the ubiquitous computing environment. The IPsec/IKE based VPN system is the one of the service elements of the ubiquitous computing. However, existing IPsec/IKE based VPN system didn't support mobile nodes, which IP address will quite often. In SCIS2004, we proposed the extension to the IKE protocol, which adds mobile node support. In this paper, we described the prototype implementation based on our past proposal. The implementation is based on Fujitsu VPN product which is compliant to IPsec/IKE protocol. As the result, we successfully added the mobile node support, we named as "Secure Seamless Roaming". This extension provides secure, persistent network connection, even if the node's IP address was changed.

Keyword IPsec/IKE, Seamless Roaming, Implementation

1. はじめに

近年，ユビキタスネットワークに注目が集まっている．ユビキタスネットワーク環境ではあらゆる機器がいつでも，どこでもネットワークに接続し利用可能であることが特徴である．特に Mobile 機器や車載機器など移動中にもネットワークを利用するような状況も考慮されるため，移動中でも通信・サービスが途切れることなく継続できるシームレスローミングは実現が必要な技術の一つである．

またユビキタスネットワーク環境では，ネットワークに接続された機器に対し，その物理的な位置情報や接続した時間情報といった，プライバシ保護上重要なデータの送信を行うことを前提としたサービスが検討されている．そのため，データ通信におけるプライバシ保護は非常に重要な問題であり，それを守るためのネットワークセキュリティ技術はユビキタス環境の実現において必須の技術の一つと位置づけられる．

本論文では，我々が「2004 年暗号と情報セキュリティシンポジウム(SCIS2004)」で提案した高いセキュリティを保ったままシームレスローミングを実現する手法について，その機能・性能について評価するための試作を行ったので報告する．提案手法は IKE(ISAKMP / IKE)プロトコルに準拠しながら，これをわずかに拡張し，シームレスローミング機能を実現するものである．本論文では，実際の IPsec セキュリティ GW 製品に対し提案手法を組込む試作を行い，提案手法の実現性を確認する．また，試作に対する評価を行い，性能について報告を行う．

本論文では，２章で IKE を中心に IPsec/IKE のプロトコルの概略を，３章では従来の Mobile IP を使用したシームレスローミング手法とその問題点を，４章で提案手法について，５章で試作・及びその評価結果についてそれぞれ示し，６章でまとめる．

表 1 IPsec SA での管理情報

種別	情報
識別子	IPaddress
秘密情報	処理・暗号化方式，秘密鍵

表 2 ISAKMP SA での管理情報

種別	情報
識別子	IPaddress, Cookie
秘密情報	処理・暗号化方式，秘密鍵情報

2. IPsec/IKE

本提案では，IPsec/IKE 通信を使用する．本章では，IPsec/IKE について提案方式に関連する部分の概略のみを紹介する．IPsec/IKE についての詳細な内容については文献[1-3]を参照のこと．なお，本試作は，IPv4 を使用した IPsec セキュリティ GW をベースに行っているが，提案手法自体は IP プロトコルに依存しない IKE に適用したものであるため，IPv6 にも適用可能である．

2.1. IPsec

IPsec は IP 通信をセキュアにするプロトコルで，RFC2406 で規定されている[1]．IPsec では，パケット認証を行う IP Authentication Header (AH)，暗号化を行う IP Encapsulating Security Payload (ESP)等が規定されている．さらに，ESP ではカプセル化モードとしてトランスポートモードとトンネルモードが存在する．提案手法では，ESP のトンネルモードを使用する．トンネルモードの IPsec では，通信を行う二者間で暗号化 VPN トンネルを構成し，その中でプライベートアドレスを使用した通信が行われる．ESP トンネルモードの IPsec 通信において，Security Association (SA) で管理する情報を表 1 に示す．

2.2. IKE

IPsec では，秘密鍵を共有した二者間でのセキュアな通信を提供するが，インターネット上で秘密鍵を共有する手段は提供しない．これを補っているのが IKE(Internet Key Exchange:RFC2409)で，IPsec で使用する IPsec SA の折衝と共有秘密鍵と管理を自動で行う[2]．IKE プロトコルには，認証や IKE 通信で使用する ISAKMP(Internet Security Association and Key Management Protocol) SA の折衝を行う Phase1 と，IPsec SA 等の折衝を行う Phase2，及びその他の設定を行うフェースがある．また，Phase2 は IPsec SA の更新(鍵更新)にも使用される．

Phase1 には，3 ハンドシェーク(アグレッシブモード)，または 6 ハンドシェーク(メインモード)のモードがあり，それぞれのモードでの認証方式として，事前共有秘密鍵方式，デジタル署名方式，公開鍵暗号方式が存在する．本試作で使用した IPsec セキュア GW では，事前共有鍵方式のメインモードを使用した Phase1 通信を行っている．しかし，提案方式自体は，Phase1 が成立した後の状態を扱うため，Phase1 以前の通信はどの方式を選択しても良い．

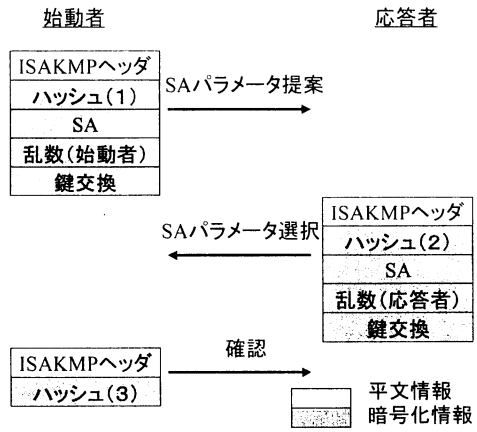

図 1 IKE Phase2 通信(PFS 有効，ID 無し)

表 3 IKE 通信の処理処理時間内訳(実測)

プロトコル	処理時間
独自拡張プロトコル	1 秒
Phase1	4 秒
Phase2(PFS 有効)	1 秒

一方，Phase2 は，3 ハンドシェークのクイックモード 1 種類であるが，オプションとして鍵情報の独立性を強化する PFS(Perfect Forward Security)を使用することができる．PFS を有効にすれば，高いセキュリティが保証されるが，Phase2 の度に DH(Diffie-Hellman)鍵交換を行うため，大きな処理オーバヘッドが必要である．一方，PFS を使用しない場合は，Phase1 で DH 鍵交換した情報を再利用する．そのため一度鍵情報が漏洩するとそれ以前の鍵情報も漏洩する危険があるが，オーバヘッドはほとんど無い．図 1 に PFS を有効にした場合(ID 無し)の Phase2 通信プロトコルを示す．

本試作で使用した IPsec セキュア GW では，Phase2 で PFS を常に使用するよう設定されている．IKE プロトコルにおいて ISAKMP SA で管理する情報を表 2 に示す．

本試作で使用した環境では，FW との連携のための独自拡張として，Phase1 通信の前に FW 通過のための認証や IP アドレスの通知，一部の IPsec パラメータの交換を行っている．本試作環境を含め多くの実装では，ISAKMP 上の識別子に IP アドレスを使用している．一般にリモートアクセス時に IKE プロトコルのみではメインモードでの事前共有秘密鍵認証が利用できない．これはリモート環境を前提とした場合，事前に IP アドレスを登録することが難しいためである.しかし本試作環境では，この独自拡張によりそれを可能にしている．試作環境での IKE の処理時間測定の結果を表 3 に示す．

表 4 IKE 通信の処理処理時間内訳(実測)

プロトコル	処理時間
Phase1	0.5～1 秒
XAUTH + ISAKMP-Config	0.5～1 秒
Phase2(PFS 無効)	0.1 秒

また，他の IPsec セキュア GW 環境では，Phase1，Phase2 以外のモードとして XAUTH, PIC(Pre-IKE Credential Provisioning Protocol)等のユーザ認証や，ISAKMP-Config，IPsec-DHCP 等の内部 IP アドレスの割り当てを行うモードを使用しているものも存在する．一例として，以下に示すリモートアクセス環境での IKE の処理時間測定の結果を表 4 に示す．

- 事前共有鍵方式アグレッシブモード
- XAUTH，ISAKMP-Config
- PFS 無効
- Pentium-M 700MH z クライアント
- ADSL1.5M 環境からリモートアクセス

表 3, 4 より，IKE 通信に置いては，Phase1 とその他のプロトコルが処理時間の大半をしめている．特に PFS を無効にすれば，Phase2 は 0.1 秒程度と無視できる処理時間となることが判る．

3. IPsec とシームレスローミング

ユビキタス環境においては，機器はいつでも何処でもネットワークに接続可能である．さらに携帯 IP 電話や車載機器等を考慮すれば，移動中でもネットワークが利用可能かつ，継続的にサービスが利用可能である必要がある．このことから，機器の接続するネットワークやアドレスが変化してもサービスが継続される，シームレスローミングは重要な技術であるといえる．

一方，ユビキタス環境では機器の物理的な位置情報や接続した時間情報を利用し，利用可能なサービスが変化するような方式も検討されている．それゆえ，通信内容の保護だけでなく，何時，何処から通信しているかというプライバシ情報の保護も重要な課題である．

一般に IP 通信をセキュアにするといえば，IPsec 等の暗号通信での実現を考える．しかし既存のプロトコルはローミングを考慮しておらず，ローミングが発生すると通信は切断してしまう．例えば表 3 で測定した IPsec 環境の場合，ローミングが発生すれば，再度認証フェーズから通信路の確立を行わなければならないため，最低でも 1 秒～2 秒は通信が切断されてしまう．

シームレスローミングの実現については Mobile IP を使用した方式が提案されている[10-11]．これは Mobile IP による気付アドレスが変化しないことを利用し，高速なハンドオーバ技術を導入することでシームレスローミングを実現すると言うものである．ここで，Mobile IP は，Internet 上でホスト移動性(mobility)を透過的にサポートし，サブネット間のローミングを行うプロトコルで，RFC2002～2006[4-8]で定義されている．本論文では Mobile IP についての紹介は行わない．詳しくは文献[4-9]を参照のこと．

Mobile IP のセキュア化については，文献[8]で検討されている．ここでは IPsec を使用することで Mobile IP の安全性を確保することが述べられている．つまり Mobile IP を IPsec でカプセル化するという考えである．しかし，Mobile IP を使用したシームレスローミングを IPsec でカプセル化を行うと，ローミング時に実 IP アドレスが変化するためにカプセル化している IPsec 通信が切断してしまう．そのため IPsec のローミングと同じ問題が発生し，Mobile IP を使用したシームレスローミングを使用した意味がない．

そこで，Mobile IP を使用したシームレスローミングでは，Mobile IP を IPsec でカプセル化せず，IPsec を Mobile IP でカプセル化することで，シームレスローミングを実現しながら，通信内容は IPsec で秘匿することが考えられる．しかし，この方式では通信内容は秘匿されるが，ローミングプロトコル自体は暗号化されないため，何時，何処からの通信かというプライバシ情報の保護までは実現できない．

4. 提案方式

本章では，今回試作した提案方式の紹介を行う．提案方式は IPsec/IKE プロトコルを拡張することで暗号通信による安全なネットワーク通信とシームレスローミングを同時に実現する手法である．

IPsec/IKE プロトコルでは，暗号通信を行う IPsec 暗号通信路(ESP)と鍵交換を行う IKE 暗号通信路との 2 つの暗号通信路を使用する．暗号通信の場合，通信を全て暗号化してしまうと送受信不可能になってしまうため，どの暗号化プロトコルでも識別子として使用できる平文の情報が付加されている．IPsec 暗号通信路では，表 1 に示すように，この識別子として通信ホストの IP アドレスを利用している．そのため，移動端末などでローミングによって IP アドレスが変化すると，識別子も変化してしまい送信者が識別不能となる．その結果 IPsec 通信路を保持することができず，通信は切断せざるをえない．

一方，IKE 通信では，表 2 に示すように，識別子として IP アドレスと Cookie を利用している．つまり IKE 通信では IP アドレスと Cookie の 2 つの識別子が使用可能である．このことから IKE 通信では，本来の識別氏である IP アドレスの代わりに Cookie を識別子として使用することで，ローミングが起っても，引き続き通信相手や通信データを識別することが可能である．

提案方式では，ローミングが起った場合，IKE 通信を利用してローミングが起ったことを通信相手に伝達し，高速に IPsec 暗号通信路を張り替える．言い換えれば，処理の大半を占める Phase1 や認証等のプロトコルを省略することで，シームレスローミングを実現するものである．

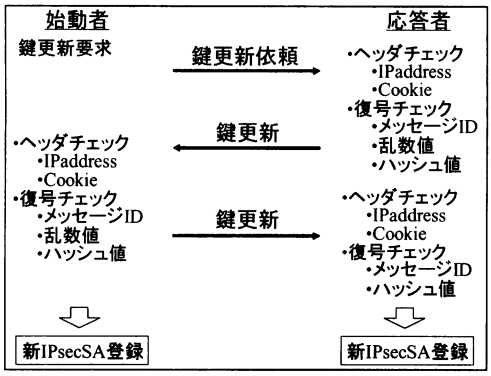

図 2 鍵更新処理概略

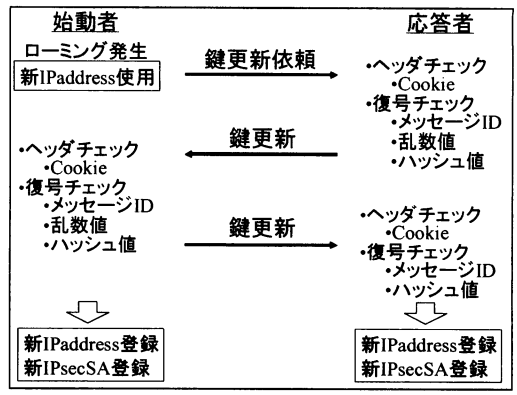

図 3 提案プロトコル処理概略

4.1. 提案プロトコル

本提案では，IKE の鍵更新プロトコルを拡張する．IKE 鍵更新プロトコルは IKE 通信の Phase2 を使用する．本論文では便宜上，Phase2 の最初の通信を鍵更新要求通信，それ以降を鍵更新通信と呼ぶ．

通常の IKE 鍵更新は，運用ポリシで定められた IPsec 通信に使用する秘密鍵の有効期限が切れた場合に行われる．IKE による鍵更新要求通信を受けたホストでは，その IP アドレス，Cookie で送信者を識別し，対応する IKE-SA の情報を使用して暗号化パケットの復号を行い，乱数情報，ハッシュ値等でパケットの改竄や再送攻撃が行われていないことを確認(メッセージ認証)する．これらの処理後，受信者は鍵更新を開始し，IKE 鍵更新が完了する．IKE 鍵更新が完了すれば，新しい IPsec の SA が作成されるので，新しい鍵での IPsec 通信が可能となる．図 2 に鍵更新の処理概略を示す．

これに対して提案方式では，ローミングが起きた場合にも，新しい IP アドレスで鍵更新要求を行うことが特徴である．この場合，鍵更新要求を受けたホスト(IPsec GW)では，送信者(移動端末)の IP アドレスは無視して，Cookie で送信者を識別し，IKE 秘密鍵でパケットを復号後，乱数情報，ハッシュ値等でパケットの改竄や再送攻撃が行われていないことを確認(メッセージ認証)する．確認が出来たならば，受信者は自分の持つ送信者の IP アドレス情報を更新し，鍵更新を開始，新しい IP アドレスでの IKE 鍵更新が完了する．新しい IP アドレスでの IKE 鍵更新が完了すれば，新しい送信者 IP アドレスを持つ新しい IPsec の SA が作成されるので，新しい IP アドレスと鍵での IPsec 通信継続が可能となる．これにより，IKE の認証(Phase1)やその他のモード処理を行うことなくローミングが可能となる．図 3 に提案方式のプロトコル概略を示す．

4.2. 提案方式の安全性

提案方式のセキュリティについて検討する．提案方式は，IKE の Phase2 の一部を拡張しているため，ここでは拡張部分について安全性検討を行う．

提案方式は，通常の鍵更新プロトコルにおける IP アドレスでの識別を，ローミング時には行わないという拡張を行っている．

IKE で使用できる識別子は，表 2 に示すように IP アドレスと Cookie である．もともと IP アドレスと Cookie はヘッダとして平文で送信されるため，攻撃者にとって偽造は容易である．そのため通所の鍵更新と比較して提案方式の安全性の低下はほとんど無い．

その他の部分では，通常の鍵更新と提案方式は共に，暗号化によるメッセージ認証，乱数情報とメッセージ ID による再送攻撃対策等で安全性を保っており，同等の安全性であるといえる．

以上から，IP アドレスと Cookie の 2 情報による識別から，Cookie の 1 情報による識別の影響を，どちらも平文で送られる情報であるので，ほぼ同等と見なせば，通常の鍵更新と同じ安全性であると言える．言い換えれば，提案方式の安全性は IKE と同等であるといえる．

次に，ローミングプロトコルについては，拡張した IKE の Phase 2 を利用している．そのためローミング情報は全て IKE 暗号通信路で暗号化されている．表 5 に示すように IPsec を Mobile IP でカプセル化する方式がローミングプロトコルを平文通信することと比較すれば，提案方式はより高い安全性を実現しているといえる．その結果，提案方式は通信内容及びローミングプロトコル自身の安全性が IPsec/IKE プロトコルと同等であることが保障できる．

5. 試作

提案方式の試作には，IPsec セキュリティ GW の試作を，富士通製品の Interstage Security Director[10]の改造により実施した．IPsec クライアントの試作については富士通製品の Safegate Client[11]の改造により実施した．また，クライアントのローミング検出機能は富士通製品 Seamlesslink Client[12]に含まれる Network Agent ライブラリ[13-14]を使用した．評価環境の詳細については表 6 を参照．

表 5 提案方式と従来方式との安全性比較

方式	提案方式	通常の IPsec/IKE	IPsec の Mobile IP カプセル化
同一アドレス使用方式	IPsec ESP カプセルモード	IPsec ESP カプセルモード	Mobile IP
通信の秘匿	IPsec ESP	IPsec ESP	IPsec ESP
ローミング方式	拡張 IKE	なし	Mobile IP
ローミング通信	暗号化通信	-	平文通信
ローミングの安全性	IKE と同等	-	低い

表 6 試作・評価環境

	セキュリティ GW	クライアント
使用機器	Sun Blade 2000	FMV7090MT4
OS	Solaris 8	Windows XP
開発環境	Sun One Studio7	Microsoft Visual C++ V6.0
IPsec/IKE	富士通 Interstage Security Director	富士通 Safegate Client
ローミング検出機能	_	富士通 Network Agent ライブラリ

5.1. 開発概要

試作に使用した Interstage Security Director，及び Safegate Client は IPsec セキュリティ GW 機能だけではなく，FW 機能や動的な FW 通過等と連携して動作する．そのため，試作にあたっては提案手法の組込みだけではなく，FW 関連についての改造も行った．

5.1.1. FW 関連機能の実現

Interstage Security Director は FW 機能と IPsec セキュリティ GW 機能を同時に実現しているため，リモートアクセスする場合，独自拡張のプロトコルを使用し，外部からの通信のほとんどを遮断している FW 機能に対して IPsec 通信の通過を要求している．このプロトコルの概略を図 4 に示す．

提案手法の場合，ローミング発生時にクライアントはセキュリティ GW に対し，新しいアドレスで IKE 通信を行う．しかし，試作環境では，IP アドレスを変更すると FW 機能によりパケットがフィルタリングされて，セキュリティ GW 機能にアドレス変更通信が届かないという問題が発生した．そこで，本試作においては，この独自拡張プロトコルに対しても改造を行った．ローミングが発生すると IKE 通信を行う前に FW 機能に対して FW 通過要求を行い，パケットの通過許可を取った後，改めて新しい IP アドレスで IKE 通信を行うこととした．また，接続時の独自拡張プロトコルではユーザ認証やフィルタリングルール等の FW パラメータ通知を行っているが，ローミング発生時は IP アドレス通知のみとすることで本プロトコルの処理時間の低減を図った．(図 5 参照)

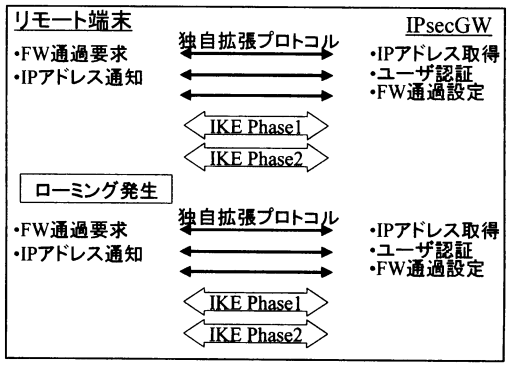

図 4 使用環境でのリモートアクセスプロトコル

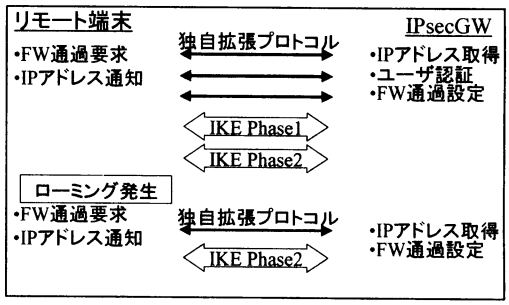

図 5 試作によるローミングの高速化

5.1.2. ローミング検出機能の実現

ローミング検出機能には，文献[10-11]で提案されている，富士通 Network Agent ライブラリを使用した．ここでは「バックアップ回線モード」と呼ばれる切り替えモードを使用する．これは PHS パケット網等狭帯域だが接続性の高い予備回線と，常に接続できるとは限らないが広帯域な優先回線との 2 回線を前提としている．予備回線側は常時接続としておき，優先側の回線が接続されたときは優先回線に，優先側の回線が切断した場合は予備回線に短時間に切り替えることが可能である．ライブラリはローミングが発生すると同時にクライアントアプリケーションへローミングイベントを通知することが出来る．

本試作においては，富士通 Safegate client に Network Agent ライブラリを組み込むことにより，ローミング

表 7 ローミング時の処理処理時間内訳(実測)

処理内容	試作結果	改造前
独自拡張プロトコル	0.1 秒	1 秒
Phase1	-	4 秒
Phase2(PFS 有効)	1 秒	1 秒

発生イベントの取得とネットワークの切替えの実現を行った.

5.1.3. 提案機能の実現

提案機能の実現にはサーバ,クライアントの IKE-SA と IPsec-SA の管理に関する改造が必要であった. 試作に用いた富士通 Interstage Security Director 及び富士通 Safegate Client はこれらの SA 管理を独自に行っている. 本試作においては, IKE-SA 管理部分に対して IP アドレス更新機能の追加, IPsec-SA に対しては従来の鍵更新イベント以外からの SA 更新機能の追加を行うことで, 提案機能時実現を行った.

5.2. 試作評価

試作したプログラムにおけるローミング時 IKE 通信の処理時間の内訳を表 7 に示す. 比較のため, ローミング発生時に通信が切断されたと仮定して, 改造前クライアントで再接続を行った処理時間も同時に示す.

表 7 より, 提案手法を用いることでローミング発生時に IKE の Phase1 を行わずに接続維持が可能であることが実証できた. また, Phase1 を行わないため, ローミング時間を一秒程度に短縮することが可能であることが実証できた. Phase1 の前に利用した開発環境独自のプロトコルで FW 制御用の通信を行うが, 本試作では, プロトコルについてもローミング時間を短縮することが出来た.

次に, 提案手法を表 4 の環境に適用することを評価する. 提案手法ではローミング時に Phase1 の他 XAUTH や ISAKMP-Config の省略も可能であることから, 表 4 の環境に提案手法を導入すればローミング時間を 1 秒～2 秒から 0.1 秒程度に短縮可能である. ローミング時間が 0.1 秒程度だと, ストリーミング通信においてもほとんど無視できる遅延時間であるため, シームレスローミングが実現可能であると言える.

6. まとめ

SCIS2004 で提案した IPsec/IKE を使用したシームレスローミング手法の試作を行い, 提案手法の実現性を実証した. また試作結果の評価を行いローミング時間の短縮が可能であることを実証し, シームレスローミングの実現可能性を示した. 提案方式は IPsec とわずかに拡張した IKE のみを使用して, 通信の秘匿だけではなくローミングプロトコル自体の安全性を保ったままシームレスローミングの実現が可能である. 安全性についても, 提案方式は, 通常の IPsec/IKE と同等の十分な安全性確保が可能となる. このことから本誌策により, 提案手法が高い安全性とシームレスローミングとを両立可能であることを実証した.

謝辞

本研究は, 平成 15 年度総務省委託研究(ユビキタスネットワーク制御・管理技術の研究開発)により実現したものであります. 関係各位に深謝致します.

文　献

[1] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC2406, November 1998.

[2] D. Harkins and D. Carrel, "The Internet Key Exchange," RFC2409, November 1998.

[3] 馬場達也, "マスタリング IPsec," オライリー・ジャパン, 2001

[4] C. Perkins, "IP Mobility Support," RFC 2002, October 1996.

[5] C. Perkins, "IP Encapsulation within IP," RFC 2003, October 1996.

[6] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, October 1996.

[7] C. Perkins, "Applicability Statement for IP Mobility Support," RFC 2005, October 1996.

[8] C. Perkins, "The Definitions of Managed Objects for IP Mobility Support using SMIv2," RFC 2006, October 1996.

[9] J. Solomon, "Mobile IP: The Internet Unplugged," Prentice-Hall, 1998.

[10] 富士通, "Interstage Security Director," http://interstage.fujitsu.com/jp/v6/sd/

[11] 富士通, "Safegate client V2.0 L21," http://software.fujitsu.com/jp/product/PC/guide/win32/security/0jm01000.html

[12] 富士通, "Seamlesslink V2.0," http://software.fujitsu.com/jp/seamlesslink/

[13] 原 政博, 飯塚史之, 野口祐一郎, 藤野信次, "エージェントによる異種網シームレスローミング -コンセプトとアーキテクチャ-," 情報処理学会第 15 回全国大会, 2003

[14] 光延秀樹, 中川 格, 飯塚史之, 藤野信次, "エージェントによる異種網シームレスローミング -ローミング手法と評価-," 情報処理学会第 15 回全国大会, 2003