モバイルコンピューティングとワイヤレス通信　20－10
(2002.　3.　8)

移動網を介したVPNに関する検討と性能評価

高橋 竜男†　　三浦　史光†　　西郷 悟†

†NTTドコモマルチメディア研究所
〒239-8536　神奈川県横須賀市光の丘3-5

E-mail: †{tatsuo,fm,saigosat}@mml.yrp.nttdocomo.co.jp

あらまし　筆者らは，これまで主としてPDC, PDC-P, PHSを対象として，これらを経由した企業LANへのリートアクセスに適したVPNプロトコル（モバイルVPN）の検討を行ってきた．しかしながら，IMT-2000のサービス開始により，今後はIMT-2000網を経由した利用環境を前提とする必要が生じている．このため，IMT-2000網とモバイルVPNの親和性を調査し，新たな要件に関して検討を行う必要がある．

このような立場から，本報告ではIMT-2000網の技術的特徴および今後想定されるこれを利用した新サービスへの対応という観点からモバイルVPNに対する要件を洗い出し，その解決策としてモバイルVPNに，セキュアなTCPアクセラレーション機能と，高速な系切り替えが可能な冗長化機能を追加することを提案し，それらを実装したプロトタイプに関する評価結果について述べる．

キーワード モバイルコンピューティング，IMT-2000, VPN，IPsec，VRRP

A Study of VPN Protocol over Mobile Communication Network and its Performance Evaluation

Tatsuo TAKAHASHI†, Fumiaki MIURA†, and Satoru SAIGO†

† Multimedia Laboratories, NTT DoCoMo, Inc
Hikarinooka 3-5, Yokosuka-shi, Kanagawa-ken, 239-8536 Japan

E-mail: †{tatsuo,fm,saigosat}@mml.yrp.nttdocomo.co.jp

Abstract　In previous research, we studied a VPN protocol customized for remote access to corporate LAN over PDC, PDC-P, and PHS networks (Mobile VPN). Since IMT-2000 commercial service was started, it is expected that many users will use Mobile VPN over IMT-2000 network in order to access to corporate LAN. In this situation, we studied the problems about the compatibility between Mobile VPN and IMT-2000 network. At the result of this, we found two requirements for Mobile VPN, TCP parameter conversion and redundancy support. In this paper, we describe these requirements and propose our solutions, called secure TCP accelerator and VRRP. We describe new Mobile VPN implementation including these functions and evaluation result of this.

Key words　**Mobile Computing, IMT-2000, VPN, IPsec, VRRP**

1. はじめに

IMT-2000の商用サービス開始により，モバイルコンピューティングにおけるインターネット接続環境は大幅に向上することが期待されている．また，近年頻発しているクラッキング事件によってユーザのセキュリティ意識は年々向上等している．これらより，今後モバイル環境におけるインターネットVPN（Virtual Private Network）の利用が急速に増加することが予想される．

筆者らは，これまでアクセス回線としてPDC，PDC-P，PHSを利用することを前提とし，移動網向けのチューニングを行ったVPNプロトコル(以下本報告ではモバイルVPNと称する)の提案と評価を行ってきた[1][2]．しかしながら，IMT-2000網の特性やその性能を生かした新しいアプリケーションへの対応を考えると，モバイルVPNをIMT-2000に適用するだけでは，網のポテンシャルを十分に引き出せない可能性がある．

本報告では，このような観点から，新たな問題点を抽出し，その解決方式を検討し，これを実装したプロトタイプの評価結果に関して述べる．

2. IMT網向けモバイルVPNの要件

2.1 共通要件

移動網を介したVPNの概要，メリットについて図1に示す．前回の報告[1]では，PDC，PDC-P，PHSへの適用を前提に，モバイル環境においてインターネットVPNがユーザに受け入れられるための条件として，以下の4点を挙げた．

(1)ユーザを，端末やアクセス網に縛らない
(2)セキュリティ機能
(3)競合する従来技術(RAS，企業LANとドコモ設備の専用線による直結等）と比較して十分に安価
(4)周期処理の排除（パケット課金の擬似時間課金化防止）

これら要件に対する解として，前回の報告では，IPsec（RFC1825-1829）[3]-[7]をベースとし，これに対して，安価なプラットフォームでも十分高速に鍵交換処理が可能な高速鍵交換アルゴリズムと，周期処理を用いないダイヤルアップVPNのセッション管理機能を追加することを提案した．

本報告においても，上記要件とモバイルVPNの基本であるIPsecの採用に関しては，継承されるべきであると考えるが，IMT-2000網での利用に対応するため，技術面，利用環境面から新たな要件を追加が必要であると考える．以下これらについて述べる．

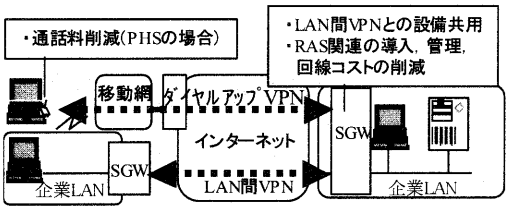

図1　モバイル環境におけるVPNとそのメリット

2.2 IMT網の技術面からの要件

IMT-2000網（W-CDMA網）は従来のアクセス回線と比較して，広帯域であるが，遅延が大きい等の特性があり，TCP/IPを利用する場合には，両端のTCPに対してパラメータチューニングが必要となる[8][9]．ユーザは，自分が所有している端末に対しては，これを行うことは可能であるが，それ以外の場合（主にサーバ側）には困難である．

この様な場合における性能向上策として，ネットワーク上にTCPを中継転送するプロキシを設置することにより，TCPのパラメータを強制的に変換するという手法が提案されている[10]-[13]．本報告ではこの様な動作を行う装置をTCPアクセラレータと称する．

ところで，VPNプロトコルとしてIPsecを利用する場合，IP層以上が暗号化されるため，暗号区間上にTCPアクセラレータが設置されてもこの恩恵を受けることができない．これに加えてIPsecパケットの組み立て分解による遅延という要素も加わるため，IPsecユーザが実効的に利用可能な帯域は，一般ユーザに比較して著しく制限され，エンドユーザに対するVPNおよびIMT-2000の利便性を著しく損なうことになる．

この問題を解決する手段として，VPNルータにおいて暗号化前のパケットに対して，TCPアクセラレーションを行うという手法が考えられる．しかしながら，このことは，VPNルータに対するTCPセッションハイジャックの危険が増すという新たなセキュリティ上の問題を生じる．以下その理由を述べる．

TCPセッションハイジャックは，TCPにおける送信元認証が，送信元のIPアドレスおよびRFC793[14]において規定される（TCPヘッダ中の）シーケンス番号のみによっておこなわれることを利

用する非常にポピュラーな攻撃方法である[15]. 概要を図 2に示す. 図の説明を以下に示す.

なお, 以下では, RFC793 に規定するシーケンス番号を, SN 値, 初期シーケンス番号を ISN 値と称する. また SYN (ISNi)は, 初期シーケンス番号 ISNi の SYN, ACK : ISNi は, 当該信号に対する ACK を表す.

①攻撃者 X が正規のクライアント A になりすまして (すなわち送信元 IP アドレスを A のアドレスでスプーフィングして)サーバ B に SYN(ISNx)を送る.
②B は, SYN (ISNb) ACK : ISNx を A に送る. X はこの信号を直接受信することはできない. しかしながら, 何らかの方法で ISN b を推測できたとする.
③X は, ACK : ISN b を B に送信する. この信号を B が受理した段階で, X から B への片方向の TCP セッションが設定され, X は B に対して任意のデータを送信することが可能になる.

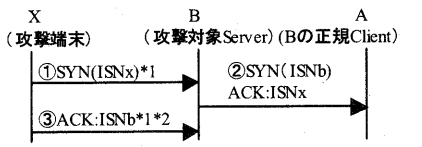

図 2 TCP セッションハイジャックの例

この攻撃を成功させるためには, ③において ISNb を推測しなくてはならないが, RFC793 によれば, ISN の値はタイマに連動してインクリメントされるので, X が直前に正規の手続きで B に TCP のセッションを設定し, ISNb0 を取得する等すれば, ISNb0 と, 時間差から ISN b を計算することが可能となる. 最近の OS では, ISN 生成のアルゴリズムをより複雑化し, 簡単にはこの値の推測できない実装になっているものもあるが[16][17], これらのアルゴリズムに関するセキュリティホールの指摘も後を絶たないため[18], 今後もこの実装には十分に注意する必要がある.

B が通常のホスト PC の場合, 本攻撃により被害を被るのは, B のみに限定され, B のアクセス権を厳密に管理する等により, 一定の防御を行うことが可能である. しかしながら, B が TCP アクセラレーション機能を有する場合には, その ISN 値算出法が破られると, B が TCP セッションを集約している全てのサーバがセッションハイジャックの危険にさらされるという意味で, この問題は非常に深刻となる. さらに, 各サーバは TCP アクセラレータに対しては認証無しにセッションを設定しなくてはならないため, 個別のサーバ毎のアクセス権管理のみでは, ISN の予測を防止することができなくなる. インターネット上からの攻撃に対しては, IPsec の認証メカニズムにより防御することが可能であるが, 攻撃者 X が, 同一 LAN 内または, エクストラネット内に存在する場合には, この対策を行う必要がある.

このように, TCP アクセラレータの実装は必須であるが, セッションハイジャックの危険性が増大するような実装でないことが絶対条件となる.

2.3 IMT 網の利用環境からの要件

IMT-2000 によって, 移動体通信の用途は飛躍的に拡大することが期待される. モバイル VPN の利用形態も社内システム, 社内のメールサーバへのリモートアクセスといった用途のみでは無く, サーバの遠隔制御や[19], 有料のコンテンツ配信, 商取引等へ応用[20]されることが予想できる. さらに, これらサービスを行う ASP を想定した場合, ユーザの数も膨大になると想定される. これらを考慮すると, サービスの継続性が重要な問題となり, VPN ルータ自体の冗長化が必要となると考えられる.

VPN ルータの冗長化方式として, 最も単純には, 予備の VPN ルータを設置しておき, 通常利用している VPN ルータ (現用系) からレスポンスが無いなどの問題が発生した場合には, 予備系 (これも別のユーザは現用系として利用していて良い) の VPN ルータに新たに VPN を設定する等の方式を採ることが考えられる. しかしながら, この場合, 系の切り替え時に VPN ルータの IP アドレスが変更になるため, 負荷の高い鍵交換を全てやり直す必要があり, 多数のダイヤルアップ VPN ユーザが系切り替え時に同時に VPN セッションの再設定のために鍵交換を要求し, 予備系の VPN ルータに非常に大きな負荷がかかりサービスが長時間中断する可能性が高い.

このような問題を起こさないためには, 鍵の再交換を必要としない系切り替え方式が必要である. このためには, 現用系, 予備系とも同一の IP アドレスを有し, かつ現用系と予備系で SA 情報を共有することが可能な VPN ルータ冗長化方式を検討する必要がある.

3. 方式検討

3.1 ベースプロトコルの変更

ベースとする VPN プロトコルは，改訂版 IPsec (RFC2401- 2410, 2451 他) [21]-[31]とする．従来採用していた旧版の IPsec との違いは，鍵交換 (IKE) の規定や[29]，ESP 認証の追加等があるが[26]，前述の 4 条件を満たすことに変わりは無い．改訂版 IPsec には，AH (RFC2402) [22]，ESP (RFC2406) [26]があり，それぞれにトンネルモードとトランスポートモードがあるが，モバイル VPN の利用形態（図 1）との親和性および，暗号化機能を有することより，トンネルモード ESP を利用することとする．

前回の報告で提案した追加機能に関しては，IMT-2000 網においても，データ通信の主力はパケット課金方式であると考えられるため，周期処理を用いないダイヤルアップ VPN セッション管理方式を，サポートすることとした．これに対して，広帯域化により，相対的に鍵交換処理の比率が低下したこと，および前述の様に IKE が規定されたことなどから，鍵交換処理に関しては，IKE をそのまま利用することとした．

3.2 セキュア TCP アクセラレーション[32]

TCP アクセラレータは TCP を一旦終端する必要があるが，TCP セッションハイジャックに関連するのは，TCP ヘッダ中の SN 値に関する部分のみであるため，SN 値を擬似的に透過とすれば，本機能設置により ISN を予測される危険性が増大するという事態は避けられる．図 3 に本機能の実装例を示す．以下，簡単に説明する．TCP アクセラレータのクライアント側に SN 変換部を，サーバ側に ISN 読み取部を設置する．SN 変換部は，TCP アクセラレータのクライアント側 ISN 値（ISNc）を取得し，ISN 読み取り部は，サーバ（B）の ISN 値（ISNb）を取得して，SN 変換部に転送する．SN 変換部は，これらを基に両者の値の変換則を導出し，クライアント側には ISNb を通知し，ISNc は隠蔽する．セッション開設以降は，TCP アクセラレータとサーバ（B）間で直接同期をとるのではなく，SN 変換部で導出された ISN 値の変換則（新たに ISN_{Offset} 記憶部を設け，これを保管）を用いた差分計算により SN 値の整合性を保つこととする．本機能により，TCP セッションハイジャックの足掛りとなる ISN 値予測を困難とすることが可能となる．

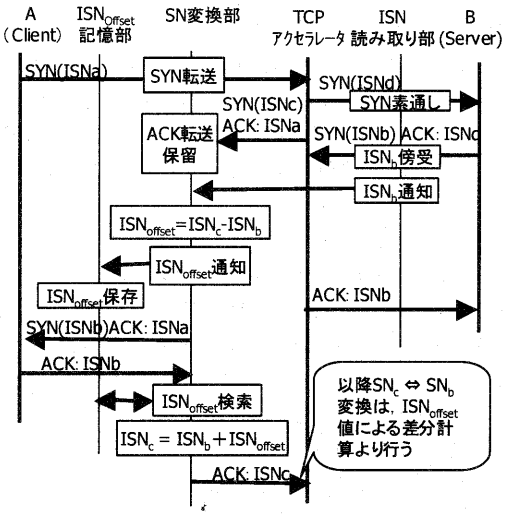

図 3　セキュア TCP アクセラレータの原理

3.3 冗長化 VPN ルータ[33]

従来，IP アドレスの変更を伴わないルータの冗長化方式として，VRRP (RFC2338 : Virtual Router Redundancy Protocol)が利用されている[34]．本報告では，この VRRP を，VPN ルータに適用する方式を提案する．提案する冗長化 VPN ルータの構成を図 4に示す．

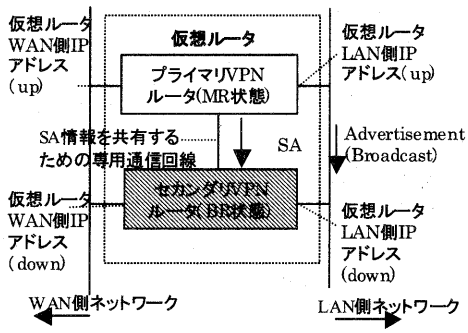

図 4　冗長化 VPN ルータ

現用系をマスター（MR），予備系をバックアップ（BR）と称する．また，MR，BR とは独立に各ルータには優先順位が設定されている．本報告では，優先順位が高い VPN ルータをプライマリ（PR），低い方をセカンダリ（SR)と称する．MR と BR は，RFC2338 に規定されている仮想 MAC アドレスを利用して，IP アドレスを共用している．2.3 で述べた SA の共有を実現するために，PR-SR 間に LAN,

WANとは独立した回線を設置し，鍵交換時にこの回線を介してSA情報を転送することとする．しかしながら，本回線のみによりVPNルータ全体の性能を低下させずにSA情報を完全に共有することは困難であると考えられる．以下，その理由と対策に関して述べる．

RFC2406では，VPNルータに対するリプライ攻撃対策が盛り込まれている．リプライ攻撃とは，正規の送信者が送信したパケットを，ネットワーク上でキャプチャ，複製し，受信者側のVPNルータに送る攻撃である．複製されたIPsecパケットには正規の認証情報が付与されているので，VPNルータの認証機構をすりぬけ，受信側のLANに擾乱を与える．RFC2406では，これを防ぐために，送信側において各送信パケットに1から順にシーケンス番号と称する番号を付与する．なお，RFC793のシーケンス番号と明確に区別するため，本報告では，以降RFC2406のシーケンス番号をSeq値と称する．

受信側では，パケットの受信履歴をこのSeq値で管理しており，以前受信したのと同じSeq値のパケットを受信した場合には，直ちに廃棄する．これにより，リプライ攻撃から受信側ネットワークを守ることが可能となっている．SA中のセキュリティポリシ，暗号，認証鍵等は，鍵交換時に送信側と受信側で共有されるのに対し，このパケットに付与されるSeq値に関する情報は，パケットを送受する毎に更新されるため，MR故障時の故障形態等を考えると，VPNルータの性能を落とさずに，この値を完全に共有することは困難である．

次にこの問題の対策について述べる．RFC2406では，Seq値の扱いに関して，送信側は送信パケットにシーケンシャルにSeq値を付与すると規定しているのに対し，受信側は，当該Seq値が以前に利用されたかどうかの履歴を管理する（すなわちSeq値の順序に関しては関知しない）と規定している．この性質を利用すれば以下の対策が可能になる．

・32bitのSeq値の領域を4つの30bitブロック b_{00}, b_{01}, b_{10}, b_{11} に分割する．

・PRをVPNルータ0，SRをVPNルータ1とした場合，各ノードは自ノードでVPNルータiがMR，対向ノードでVPNルータjがMRの時，送信SNのブロックに，bij，受信Seq値のブロックにbjiを利用する．

・各VPNルータは，割り当てられたブロックの範囲内でのみSeq値を利用する．例えば，ブロック b_{00} を利用している際には，Seq値が0~3FFFFFFFの範囲を超える前に鍵交換を行い，Seq値を初期値に戻す．これらブロック分割を利用した系切り替え時の処理手順を，図5を利用して説明する．

①2重化ノードAとBがVPNセッションを設定しており，それぞれPR，SRがMRとなっている．この場合，ノードA，Bはそれぞれ送信ブロックとして b_{01}，b_{10} を利用する（図5上）．

②ノードAのPRが故障し，SRがMRとなり，送信ブロックを b_{11} に切り替える．次にSRは自らがノードAのMRとなったことをノードBに通知する．

③この通知を受け取ったノードBのMR(SR)は，ノードA向けの送信ブロックを b_{11} に変更する．また，ノードAのMR (SR)は②の間，旧ブロック (b_{10}) に送られてきたパケットは全て廃棄する．この再送は上位プロトコルによる（図5下）．

これにより，Seq値に関する情報をリアルタイムに共有せずとも，Seq値のチェックが可能となる．

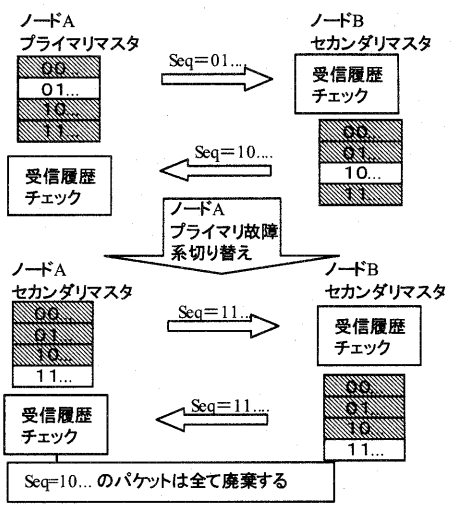

図5　シーケンス番号の領域切り替え

4. 評価

4.1 セキュアTCPアクセラレーション

上記各機能を実装したVPNルータを試作した．その評価系を図6に示す．本項目ではHTTPプロトコルを利用して，実験用HPから，500KBのjpegファイルのダウンロードに要する時間をスニファ②（IPsec対応）を利用して測定した．また，スニファ

③（IPsec 対応），④を利用して，３ウェイハンドシェイク時のアクセラレータの動作を確認した．

TCP アクセラレーション機能 ON／OFF それぞれの場合における，RTT とスループットの関係（クライアントが最初に送信した SYN から，WWW サーバが送信した最後のデータパケットまでの時間差から算出）を図７に示す．また，同データから３ウェイハンドシェイクのオーバーヘッドを排除したグラフ（WWW サーバが送信した最初と最後のデータパケットの時間差から算出）を図８に示す．

TCP アクセラレータにおける，３ウェイハンドシェイクの処理シーケンスを図９に示す．ただし，スニファ③，④の内部タイマを完全に同期させることは不可能であったため，各々最初の SYN のキャプチャ時刻を０とし，各セグメント到着時刻はその相対時間で表してある．また，スニファ③側のデータは実際には，ESP 形式により，カプセル化，暗号化されているが，図では略している．

4.2 冗長化 VPN ルータ

本項目では，図６の評価系において，FTP プロトコルで１MB のバイナリファイルのダウンロードを開始後，手動で MR の電源断を行った．このとき，BR が MR に切り替わり，FTP の転送シーケンスが正常終了する様子をスニファ①で確認した．また，スニファ④は，このときの，２重化 VPN ルータの LAN 側で MR がブロードキャストする VRRP の ADVERTISEMENT メッセージを収集した．

スニファ①，④で収集したシーケンスより，データ転送時の SN 値（RFC793 のシーケンス番号）プロットおよび，ADVERTISEMENT メッセージのプロットを図１０，図１１に示す．図１０は，本報告において提案する VRRP による IP アドレス共有を行うが，Seq 値のブロック化を行わなかった場合．図１１は，これらを同時に行った場合である

5. 考察

5.1 セキュア TCP アクセラレータ

図７より，提案方式による TCP アクセラレーション機能を利用することにより，十分な性能改善効果が得られることが明らかとなった．遅延時間０のデータのみ，性能改善効果がマイナスになっているが，これは，セッション開設時に，図３のシーケンスが実行されるため，サー側 ISN のキャプチャや，ISN_{Offset} の計算等の処理がオーバーヘッドになっているためであると考えられる．図７と図８を比較すると，図７では TCP アクセラレーション ON の場合でもグラフがやや右肩下がりとなっているが，図８では，バッファサイズ／RTT 値で算出される理論限界値に到達するまで，ほぼ最大性能が得られている．これは，提案の方式では，最初の SYN,SYNACK に関しては，クライアントとサーバが同期する必要性があるため，RTT の影響が直接現れているためと考えられる．

図９より，セグメント③，⑤を比較すると，サーバ側の ISN 値を透過としたまま，初期ウィンドウサイズのみを拡張することに成功していることが判る．これにより，本装置に対する TCP セッションハイジャックは防止することができる．

TCP セッションに対する攻撃法としては，この他にも，送受信間の SN 値の同期を崩す方式[35]等が知られているが，これらに関しては，TCP アクセラレータの有無に関わらず危険度は同一であり，本報告における検討対象としていない．また，LAN 内の個々のホストに対する ISN 値予測に関しても同様である．

5.2 冗長化 VPN ルータ

図１０より，提案する VPN ルータ冗長化方式（図４）により，上位アプリケーションに影響を与えずに，系切り替えが可能となっていることが明らかとなった．SA の共有が行われないため，系切り替え時には，鍵の再交換が必要となっているが，提案方式により，故障の前後で IP アドレスが変わらない為，負荷の高い IKE フェーズ１を行う必要は無く，フェーズ２（Quick モード）のみで対応可能となっている．図１１より，これに提案する Seq 値切り替え方式（図５）を併せて利用することにより，系切り替え時間をさらに３割以上短縮している．また，両図中の ADVERTISEMENT メッセージの有無より，VRRP ルータとしての中断時間を測定すると，図１０で約３．０秒，図１１で約３．６秒となる（ただし，評価システムでは，ADVERTISEMENT メッセージの周期が１秒であったため，電源断のタイミングと周期の関係で，実際の中断時間は，この値よりも最大で約１秒短い）．図１０の例では，VRRP ルータとしては回復した後でも，鍵交換のために，VPN セッションの回復に時間を要しているため，パケット送受がしばらく中断していることがわかる．

これらより，本評価系において，提案している

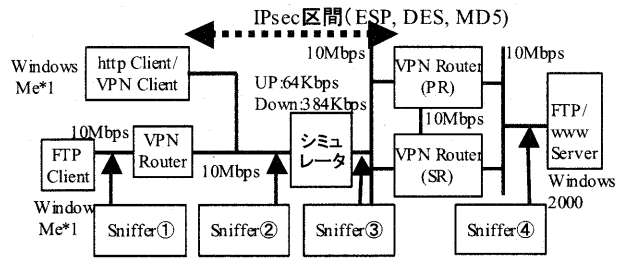

図６　評価系構成図

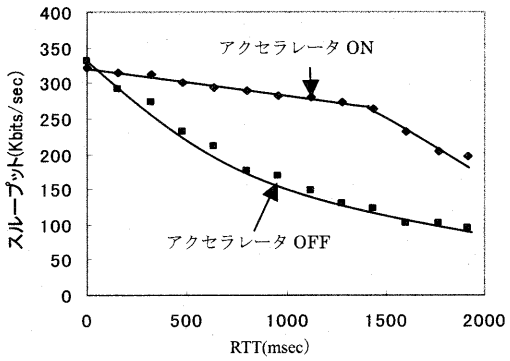

図７　セキュア TCP アクセラレーションの効果
（SYN-最終パケット受信）

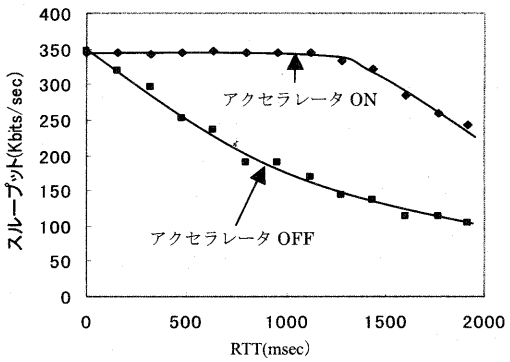

図８　セキュア TCP アクセラレーションの効果
（データパケット受信開始-最終パケット受信）

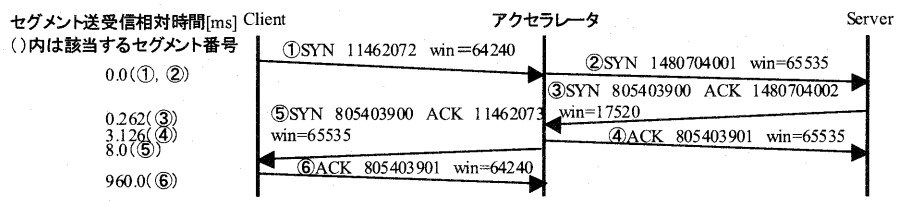

図９　３ウェイハンドシェイクシーケンス

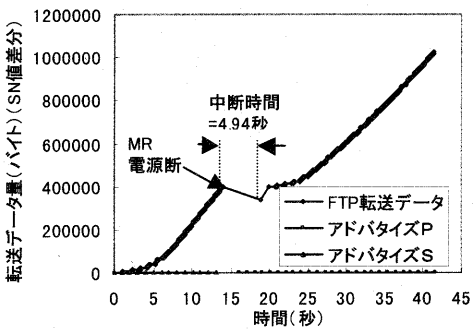

図１０　系切り替え時の処理シーケンス
（VRRP のみ利用）

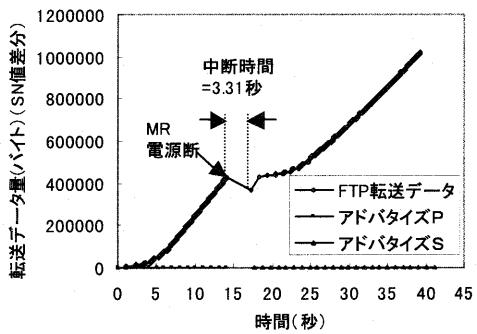

図１１　系切り替え時の処理シーケンス
（VRRP，Seq 値ブロック切り替え併用）

VPN ルータ冗長化方式，Seq 値切り替え方式を併用することの有効性を確認できた．また，本評価においては，VPN セッションは１つのみで行ったが，前提条件で示したように，非常に多数のユーザが同時に利用している環境では，Quick モードによる鍵交換処理のオーバーヘッドの比率がさらに高くなり，両方式併用による効果がさらに高くなると考えられる．これに加えて，Quick モードではオプションとなっている Diffie-Hellman 法[36]を利用する場合，鍵交換処理のオーバーヘッドは非常に大きくなり，Seq 値切り替え方式の併用は必須になると考えられる．

6. おわりに

モバイル VPN を IMT-2000 網に適用した場合に生じる新たな問題点について示し，その解決策として，セキュア TCP アクセラレーション機能，VRRP による VPN ルータ冗長化機能を提案し，これらを実装したプロトタイプに対する評価結果を示した．今後，実際のサービス環境での評価を行う．

文　献

[1] 高橋竜男，竹下敦，関口克己，”モバイル向け VPN プロトコルの検討，” 情処研究会，MBL10-7，Oct. 1999.

[2] 高橋竜男，鶴巻宏治，関口克己，竹下敦，”モバイルコンピューティングにおける VPN の研究，” NTT DoCoMo テクニカル・ジャーナル,Vol.8,No.4,pp.58-64,Jan. 2001.

[3] R. Atkinson, "Security Architecture for the Internet Protocol," IETF, RFC 1825, Aug. 1995.

[4] R. Atkinson, "IP Authentication Header," IETF, RFC 1826, Aug. 1995.

[5] R. Atkinson, "IP Encapsulating Security Payload (ESP)," IETF, RFC 1827, Aug. 1995.

[6] P. Metzger, and W. Simpson, "IP Authentication using Keyed MD5," IETF, RFC 1828, Aug. 1995.

[7] P. Karn, P. Metzger, and W. Simpson, "The ESP DES-CBC Transform," IETF, RFC1829, Aug. 1995.

[8] H.Inmura, et al., "TCP over 2.5G and 3G Wireless Networks," IETF, draft-ietf-pilc-2.5g3g-05, Nov. 2001.

[9] 石川太朗，稲村浩，高橋修，” W-CDMA 向け TCP プロファイル，” 情処研究会，MBL15-3，Nov. 2000.

[10] 渋谷尚久，加藤紀康，高木雅祐，” ハイブリット MMAC システムでの TCP スループット向上の一検討と性能評価，” (DICOMO 2001)シンポジウム論文集，pp.79-84，Jun. 2001.

[11] M. Kojo, K.Raatikainen, and T.Alanko, Connecting Mobile Workstations to the Internet over a Digital Cellular Telephone Network,University of Helsinki, Helsinki, Sep. 1994.

[12] J.Border, et al., "Performance Enhancing Proxies Intended to Multigate Link-Related Degradations," IETF RFC3135, Jun. 2002.

[13] 加藤紀康，鎌形英二，” 非対称無線リンク用 TCP ゲートウェイ，” 信学通信ソ大，分冊 2，No.B-7-32，pp.153，Oct.1998.

[14] "TRANSMISSION CONTROL PROTOCOL," IETF, RFC793, Sep. 1981.

[15] Robert T. Morris, "A Weakness in the 4.2BSD UNIX TCP/IP Software," Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, Feb. 1985.

[16] 久米原栄，” TCP/IP セキュリティ，” pp.159-160，ソフトバンクパブリッシング，2000.

[17] S.Bellovin, "Defending Against Sequence Number Attacks," IETF, RFC1948, May 1996.

[18] "Statistical Weakness in TCP/IP Initial Sequence Numbers," CERT Advisory , CA-2001-09, May 2001.

[19] Norman SU, Masahiko TSUKAMOTO, and Shojiro NISHIO, "Rajicon:A system for Remote PC Access through a Cellular Phone," (DICOMO2001)シンポジウム論文集，pp.349-354，Jun. 2001.

[20] モバイル・インターネット最前線：ｉモードから次世代システム IMT-2000 まで，日経コミュニケーション，日経ニューメディア（共編），Sep. 2000.

[21] S.Kent, and R. Atkinson, "Security Architecture for the Internet Protocol," IETF, RFC2401, Nov. 1998.

[22] S.Kent, and R. Atkinson, "IP Authentication Header," IETF, RFC2402, Nov. 1998.

[23] C.Madson, and R.Glenn, "The Use of HMAC-MD5-96 within ESP and AH," IETF, RFC2403, Nov. 1998.

[24] C.Madson, and R.Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH," IETF, RFC2403, Nov. 1998.

[25] C.Madson, and N.Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV," IETF, RFC2405, Nov. 1998.

[26] S.Kent, and R.Atkinson, "IP Encapsulating Security Payload (ESP)," IETF, RFC2406, Nov. 1998.

[27] D.Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," IETF, RFC2407, Nov. 1998.

[28] D.Maughan, et al., "Internet Security Association and Key Management Protocol (ISAKMP)," IETF, RFC2408, Nov. 1998.

[29] D.Harkins, and D.Carrel, "The Internet Key Exchange (IKE)," IETF, RFC2409, Nov. 1998.

[30] R. Glenn, and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec," IETF, RFC2410, Nov. 1998.

[31] R. Pereira, and R.Adams, "The ESP CBC-Mode Cipher Algorithms," IETF, RFC2451, Nov. 1998.

[32] 西郷悟，高橋竜男，三浦史光，高橋修，” TCP アクセルレータにおける TCP ハイジャック防止対策，”信学総大，分冊通信２，No.B-7-196, PP.329, 2001.

[33] 高橋竜男，三浦史光，西郷悟，” VPN ルータ冗長化に関する一検討，” 信学総大，分冊通信２，No.B-7-186, PP.329, 2001.

[34] S.Knight, et al., "Virtual Router Redundancy Protocol," IETF, RFC2338, Apr. 1998.

[35] Laurent Joncheray, "Simple Active Atack Against TCP," Merit Network Inc., 1996.

[36] E. Rescorla, "Diffie-Hellman Key Agreement Method," IETF, RFC2631, Jun. 1999.