移動網を介したモバイル VPN 方式の提案と評価

高橋 修[†] 高橋竜男[†] 三浦史光[†]
西郷 悟[†] 水野忠則[††]

本論文では，W-CDMA 等の移動通信網を介して VPN を実現するモバイル VPN 方式ついて提案する．最初にモバイル VPN を実現するために考慮すべき要件と課題を明確にする．次に，これらの課題を解決する方式として，キープアライブによらない新しい VPN セッション管理方式，TCP セッションハイジャックを防御するセキュア TCP アクセラレータ方式，および VPN が実現するセキュリティ機能を低下させずにモバイル VPN を構成する冗長化されたルータ間（現用/予備）の切替えを短時間に効率的に行う方式を提案する．最後にこれらの方式を実現したプロトタイプによる評価システムとその評価結果について述べ，筆者らが提案するモバイル VPN 方式がモバイル環境に適用可能な実用的な方式であることを示す．

Secure and Efficient Architecture for Mobile VPN

Osamu Takahashi,[†] Tatsuo Takahashi,[†] Fumiaki Miura,[†]
Satoru Saigo[†] and Tadanori Mizuno[††]

In this paper, we propose the requirements and issues for mobile VPN architecture, firstly. And we propose the secure and efficient architecture for mobile VPN, which supports keep-alive less VPN session management method on the base of IPsec. And it also supports a secure TCP accelerator, and efficient VPN router redundancy method. Finally, we show evaluation results of prototype system of proposed mobile VPN architecture.

1. はじめに

第 3 世代の移動通信網である IMT-2000（W-CDMA）網の商用サービスが開始されたり，無線 LAN によるホットスポットサービスが本格的に普及されたりすることにより，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ますます向上している．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．固定網を前提とした VPN はすでに実用になっているが，移動通信網経由でサーバにアクセスするモバイル環境にそのまま適用しても，広帯域が特徴である W-CDMA 網のポテンシャルを十分に引き出せない等の可能性がある．このため，移動網特有の性質が VPN に及ぼす影響を明確にし，その対策を検討することがモバイル VPN を普及させるうえで重要である．

本論文では，最初にモバイル環境での VPN 利用の要件と課題を明確にする．具体的には，VPN を実現する際に標準的に使用されているプロトコル（IPsec）をモバイル環境に適用させるために考慮すべき課題，モバイル VPN ルータでのプロキシ機能（TCP アクセラレータ機能）の必要性とそれを実現する際のセキュリティ上の課題，さらに，信頼性向上のための仮想ルータ方式（VRRP: Virtual Router Redundancy Protocol）をモバイル VPN ルータに適用する際の課題について明確にする．

次に，これらの課題を解決する方式として，キープアライブによらない新しい VPN セッション管理方式，TCP セッションハイジャックを防御するセキュア TCP アクセラレータ方式，および VPN が実現するセキュリティ機能を低下させずにモバイル VPN を構成する冗長化されたルータ間（現用/予備）の切替えを短時間に効率的に行う方式を提案する．

さらに，これらの方式のプロトタイプによる評価システムとその評価結果について述べる．移動網として

† NTT ドコモマルチメディア研究所
Multimedia Laboratories, NTT DoCoMo, Inc
†† 静岡大学情報学部情報科学科
Faculty of Information, Shizuoka University

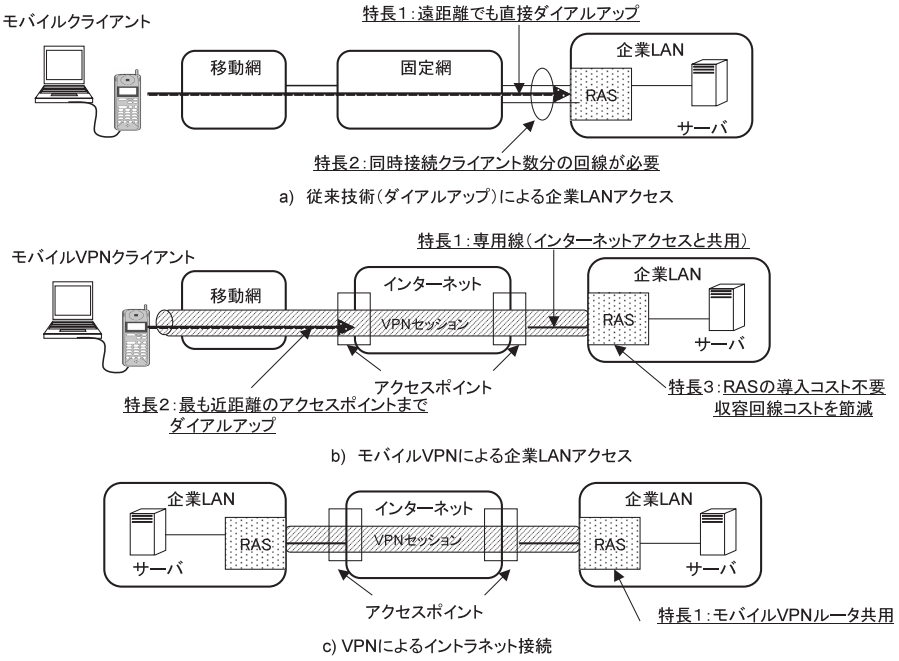


図 1 モバイル VPN の概要と特長
Fig. 1 Feature of mobile VPN.

W-CDMA を想定した評価結果から，提案した VPN セッション管理方式がキープアライブなしでも VPN セッションを維持できること，セキュア TCP アクセラレータ方式により TCP セッションハイジャックを防止しつつ，スループットを最大 3 倍程度向上できること，冗長化されたルータ間の系の切替えが 3 秒程度で行われ，ほぼ実アプリケーションに影響を与えず実現可能なこと等を示す．これらにより，本論文で提案するモバイル VPN 方式は，固定網とほぼ同じセキュリティレベルと移動網の特徴を最大限に活かす性能が得られ，モバイル環境に適用できる実用的なものであることを示す．最後に，残された課題と今後の検討計画について述べる．

2. VPN の概要

2.1 VPN の特長

VPN は，インターネットのように多数のユーザによって共用されるネットワークを，あたかも専用線と同等のセキュアな環境で利用するための技術である（**図 1**）．モバイル環境下においてユーザ（クライアント）は，移動網経由でダイヤルアップし VPN を利用する（以下では，この形態をモバイル VPN という）ことによって次のメリットを得ることができる．

(1) 通話料金の削減

電話料金は距離に比例して高額になる．遠距離から企業 LAN にアクセスする必要がある場合 VPN によって最も近接の ISP のアクセスポイント経由で企業 LAN にアクセスすることが可能になる．企業 LAN の RAS（Remote Access Service）に直接ダイヤルアップする場合と比較して，通信料金の距離に比例する部分を節約することができる．

(2) RAS の導入，維持管理コストの削減

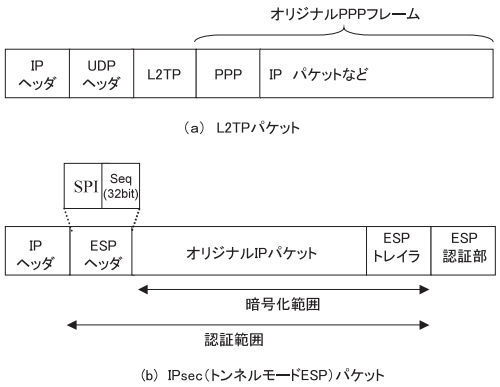
RAS を利用する際には，RAS 側で同時接続するユーザ数分だけ固定電話回線を導入する必要があるのに対して，VPN の場合は，これらの固定電話回線をインターネットとの接続回線で兼用することができ，回線導入コストを節減可能である．また，RAS そのものの導入および維持管理コストも削減できる．

2.2 VPN プロトコル

有力な VPN プロトコルとして L2TP（Layer two Tunneling Protocol）[1] と IPsec（Internet Protocol Security）[2)~12)] の 2 つのプロトコルがある．

(1) L2TP

L2TP は，PPP（Point to Point Protocol）[13] のフレームを UDP（User Datagram Protocol）[14] のパケットでカプセル化し，IP 以外のパケットも IP 網上で転送可能とするものである（**図 2**）．セキュリティ機能に関しては，トンネルの認証機能以外は規定されて



ESP : Encapsulating security Payload
IP : Internet Protocol
IPsec : Internet Protocol Security
SPI : Security Parameters Index
L2TP : Layer Two Tunneling Protocol
PPP : Point to Point Protocol
UDP : User Datagram Protocol
Seq : シーケンス番号

図 2 主要 VPN プロトコルのパケット構造
Fig. 2 Packet formats of VPN protocols.

表 1 主要 VPN プロトコルの機能比較
Table 1 Comparison of VPN protocols.

要件		L2TP	IPsec
トンネリング		○(レイヤ2)	○(レイヤ3) *1
セキュリティ	認証	○	○
	秘匿	×	○ *2
	改竄防止	×	○
	鍵交換	×	○

＊1:トンネルモードでサポート
＊2:ESP(Encapsulating Security Payload)でサポート

いない．

(2) IPsec

IPsec には，AH（Authentication Header）[3]と ESP（Enc apsulating security Payload）[7]があり，それぞれにトランスポートモードとトンネルモードがあるが，以下では，代表的なトンネルモード ESP について述べる．

トンネルモード ESP の特徴は IP パケットを IP パケットでカプセル化していることであり，これにより企業 LAN 内のローカルな IP パケットを，インターネットに転送できる．カプセル化の際に，オリジナルの IP パケットは盗聴防止と企業 LAN 内サーバの IP アドレス秘匿のためにすべて暗号化され，VPN セッションを識別するための ESP ヘッダと ESP トレイラが付加されるとともに，改ざん検出とパケット認証のための ESP 認証部を付加し，新たな IP ヘッダ付加する（図 2）．このように，IPsec はセキュリティ機能が充実しているのが特徴である．

(3) モバイル環境での VPN プロトコル

上記 2 つの VPN プロトコルの機能比較を**表 1** に示す．本論文では，セキュリティ機能の充足性を重視し，モバイル VPN のセキュリティプロトコルとして IPsec を選択した．さらに，IPsec の中から，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優先し，トンネルモード ESP をモバイル VPN のベースプロトコルとし，以下では，これを前提に検討する．

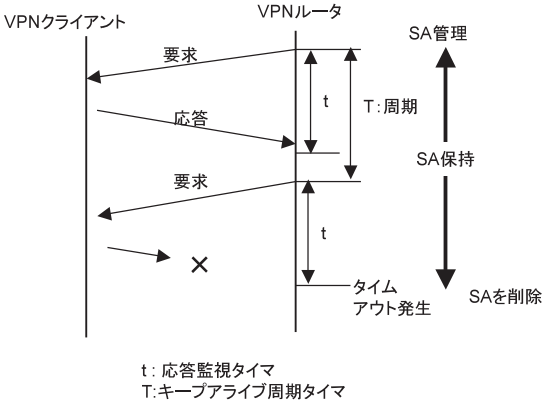


図 3 キープアライブによる SA 管理の例
Fig. 3 Example of SA management using keep-alive method.

3. モバイル VPN の要件

モバイル VPN を実現するうえで考慮すべき要件に以下のものがある．

3.1 モバイル VPN プロトコルへの要件

移動網経由でインターネットにダイヤルアップ接続を行う場合には，一般には接続するごとに，異なる IP アドレスが割り当てられる．IPsec では，通信相手（IP アドレス）ごとに SA（Security Association）を管理する必要がある．SA は，IP パケットの送受信元双方で合意したセキュリティポリシー，暗号鍵，認証鍵，IPsec パケットの ESP ヘッダ部にあるシーケンス番号値（Seq 値）等を格納するオブジェクトであり，VPN セション開設時に作成し，終了時に削除する必要がある．しかし，接続が異常終了した場合等には VPN ルータ側はこの状態を検出できない場合がある．このため，一般に VPN クライアントと VPN ルータ間でキープアライブパケットを送受し，状態を定期的に監視する必要がある（**図 3**）．しかし，モバイル VPN の場合には，キープアライブ方式には以下の問題がある．

(1) 誤切断

VPN クライアント側の電波状態の悪化により，一時的な遅延時間の増大が発生した場合，VPN ルータ

はキープアライブパケットが規定時間内に戻らないことにより，VPN クライアントが正常である場合でも，VPN セッションを切断してしまう可能性がある．

(2) 課金

クライアントが接続している移動網がパケット網の場合，パケット網は情報量課金が基本であるのにかかわらず，キープアライブパケット自体に課金されるため，接続する時間によって通信料金が増えてしまう問題がある．

上記問題を解決するために，キープアライブをしない新しい VPN セッション（SA）の管理方式の検討が必要である．

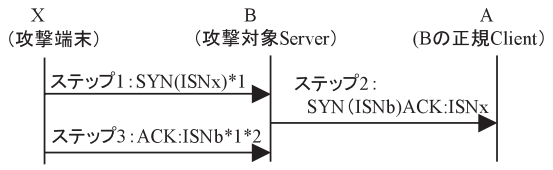
3.2 モバイル VPN ルータへの機能要件

3.2.1 W-CDMA 網の特性からの要件

1) TCP アクセラレータ機能の必要性

W-CDMA 網では高速パケット交換サービス（上り 64 Kbps，下り 384 Kbps）が提供されており，従来よりも高速なモバイルインターネットアクセスが可能となっている．このパケットチャネルの特性として一般に無線区間を含む網内伝送遅延時間が，転送速度に比較して大きな値になることが分かっており，既存の TCP を利用した各種アプリケーションが十分なスループットを得られない等の性能低下を生じることが明らかになっている．この対策として，受信バッファサイズの拡大等の TCP パラメータの最適化が必要になる[15),16)]．さらに，IPsec パケットの組立て/分解によるオーバヘッドが加わるため，モバイル VPN で実効的に利用可能な帯域は，通常の利用形態に比較して著しく制限され，利便性を損なうことになる．これらの理由により，TCP パラメータの最適化は必須となる．ユーザが所有している端末側は，TCP パラメータの最適化は自分自身で実施できるが，サーバ側は一般には困難である．この場合の性能向上策として，ネットワーク上にゲートウェイ（GW）を設置することにより，クライアント側と GW 間，GW とサーバ間で TCP セッションを独立に設定し，クライアント側と GW 間の TCP パラメータを移動網の特性に合った最適値に設定という手法が提案されている[17)~20)]．以下では，この方式を TCP アクセラレータと称し，これをモバイル VPN ルータで実現する際の課題について検討する．

一般に 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，たとえ暗号通信区間に TCP アクセラレータが設置されたとしてもそのままではこの機能を利用できない．このため，IPsec を処理するモバイル 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ことが必須となる．



注）＊1：送信元IPアドレスをAのIPアドレスに設定する
＊2：直接ISNbを知ることはできないが，何らかの方法で推定

図 4 TCP セッションハイジャックの例
Fig. 4 Example of TCP session highjacking.

2) TCP アクセラレータ実現上の課題

モバイル VPN ルータで TCP アクセラレータを実現する際には新たなセキュリティ問題を考慮する必要がある．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 TCP ヘッダ中のシーケンス番号[21)]のみによって行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[22)]．概要を以下に示す（**図 4**）．なお，以下では TCP（RFC793）のシーケンス番号を SN 値，初期シーケンス番号を ISN 値と記す．また SYN（ISNi）は初期シーケンス番号 ISNi の SYN，ACK:ISNi は SYN（ISNi）要求に対する応答（ACK）を示す．

［**ステップ 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．

［**ステップ 2**］B 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 ISNb を推測できたとする．

［**ステップ 3**］X は，ACK:ISNb 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．

この攻撃を成功させるためには，［ステップ 3］において ISNb を推測しなくてはならないが，TCP では 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，そのときの ISN 値を取得する等によりこの値と経過時間から ISNb を計算し推測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[23),24)]，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[25)]，危険性は依然として残されている．

Bが通常のホストサーバの場合，本攻撃により被害を被るのは，Bのみに限定される．しかし，BがTCPアクセラレーション機能を有するモバイルVPNルータの場合には，そのISN値算出法がいったん破られると，BがTCPセッションを集約しているすべ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VPNルータに対しては特別な認証なしに接続するので，サーバごとの個別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．

このように，通常のインターネットからの攻撃に対しては，IPsecの認証メカニズムにより防御可能である．しかし，VPNルータを異種企業間等のLAN間通信で利用する場合（図1(c)参照）には，攻撃者XがLAN内に存在する可能性があり，Xが遠隔のLAN内からVPNを通じてTCPセッションハイジャックを試みた場合，どちらのVPNルータもそれを検出ないし防御することは困難であり，この対策をモバイルVPNルータで行う必要がある．

3.2.2 モバイルVPNルータ冗長構成の要件

モバイルVPNの利用形態は，W-CDMAに出現によってますます多様化，高度化し，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なく，サーバの遠隔制御や有料のコンテンツ配信，商取引等へ応用[26]され，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，信頼性向上のためモバイルVPNルータ自体の冗長化が必要になる．

モバイルVPNルータの冗長化方式として，最も単純には，予備のルータを設置しておき，通常利用しているルータ（現用系）からレスポンスがない等の問題が発生した場合に，予備系に切り替え新たにVPNセッションを設定し直す方式等が考えられる．しかし，この場合，系の切替え時にルータ自身のIPアドレスが変更になるため，このルータは接続しているすべてのモバイルVPNクライアントと鍵交換をやり直す必要があり，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．このため，鍵の再交換を必要としない系切替え方式として，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．

4. モバイルVPN方式の提案

本章では，3章で述べた各要件を解決する実現方式を提案する．

4.1 モバイルVPNプロトコル

IPsecをモバイルVPNに適用するために，以下の新しいVPNセッション管理方式を提案する．提案方式は，周期的なキープアライブによるリアルタイムのVPNセッション管理（SA情報管理）を行わずに，VPNセッション管理上問題が発生したときのみに，モバイルVPNルータからクライアントに状態確認のための確認要求パケットを送信するようにISsecを拡張することでVPNセッション管理を行う[27]．

具体的には，モバイルVPNルータは，クライアントからVPNセッション設定要求を受け，SAを作成する（VPNセッションが上限数に達するまで，要求を受け付ける）．VPNセッション数が同時接続上限に達した場合，モバイルVPNルータは，そのとき廃棄すべき無効なSA情報が存在しないか以下の手順で確認する．

1) FIFO（First in First out）かLRU（Least Recently Used）のいずれかのアルゴリズムにより，廃棄候補のVPNセッションを選択し，当該VPNセッションのSAに登録されているクライアントに状態確認パケットを送信する．
2) クライアントから応答がなければ，当該SAを削除し，資源を解放する．
3) クライアントから応答があれば次の廃棄候補を選択し，上記1)の処理を継続する．

また，クライアントがすでにSAに登録してあるものとは異なる新たなIPアドレスでVPNセッションを要求してきた場合には，当該クライアントのすでにあるSAを削除し，新たなSAを作成する．これにより，上記1)〜3)による削除を待たずに早期に無効なVPNセッションを検出し，削除することを可能とする．

4.2 セキュアTCPアクセラレータの実現方式

TCPセッションハイジャックに関連するのは，3.2.1項で述べたようにTCPヘッダ中のSN値に関する部分のみである．このため，モバイルVPNルータで分割された2つのTCPセッションで使用するISN値を擬似的に透過（同じ値）になるように変換できれば，モバイルVPNルータでTCPアクセラレータを実現したとしても，ISN値が予測されハイジャックされる危険性の増大を避けることが可能となる[28]．

提案するTCPアクセラレータ実現方式を**図5**に示す．TCPアクセラレータは，以下のTCP処理部とSN値透過変換処理部から構成される．

(1) TCP処理部

サーバとVPNルータ間のTCPは，通常実装されているTCPをそのまま利用する．また，モバイルVPN

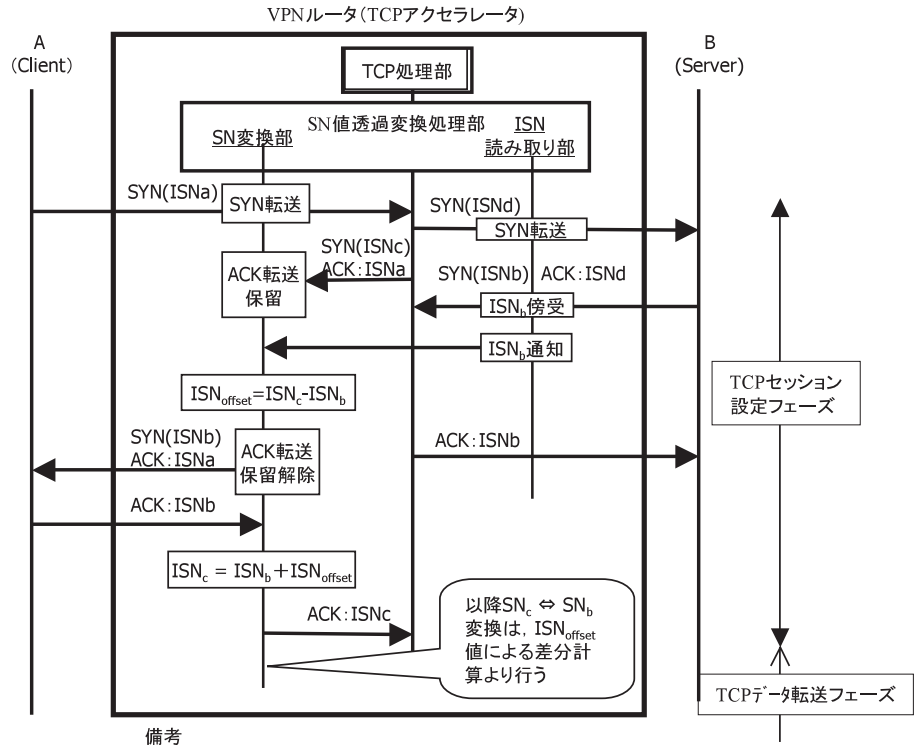


図 5 セキュア TCP アクセラレータにおける SN 値変換原理
Fig. 5 SN values translation method for secure TCP accelerator.

クライアントとモバイル VPN ルータ間の TCP には W-TCP（Wireless TCP）[15]と呼ばれる以下の TCP パラメータの拡張を行ったものを使用する．

- TCP バッファサイズの拡張
- 初期ウィンドウサイズの拡張
- 選択的応答確認
- 最大転送パケット長（MTU: Maximum Transfer Unit）の拡張

(2) SN 値透過変換処理部

SN 値透過変換処理部は，ISN 読み取り機能と SN 変換機能からなる．ISN 読み取り部は，サーバ側に位置し，サーバ（B）の ISN 値（ISNb）を取得して，SN 変換部に通知する．SN 変換部は，クライアント側に位置し，TCP プロトコル処理部のクライアント側（A）の ISN 値（ISNc）とサーバ側（B）の ISN 値（ISNb）を取得し，これらの値から ISN 値および SN 値の変換規則（ISNoffset 値=ISNc-ISNb）を生成するとともに，その規則に従って変換を実行する．すなわち，TCP セッション開設時には，クライアント側 TCP プロトコル処理部が送信した SYN(ISNc)ACK:ISNa の ISNc をサーバ（B）側の ISN 値である ISNb に変換し，クライアント（A）の ISN 値とサーバ（B）の ISN 値を同じ値にする．また，データ転送時は，クライアント（A）から受信した SN に ISNoffset 値を加え，TCP プロトコル処理部から受信した SN には ISNoffset 値を引く．

これにより，分割された TCP の各々の ISN 値をエンド–エンドレベルで透過性を確保することが可能になり，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できる．

4.3 冗長化モバイル VPN ルータ実現方式

(1) 基本方式

ルータの冗長化方式として，VRRP（RFC2338: Virtual Router Redundancy Protocol）がある[30]．VRRP は，現用系ルータ（MR: Master Router）と予備系ルータ（BR: Backup Router）を 1 つの仮想ルータとして動作させるためのプロトコルである．すなわち，通信相手には 1 つの IP アドレスに見せ，BR は MR の運用状態を監視し，MR の障害を検出すると BR が自動的に MR に切り替わるメカニズムを実

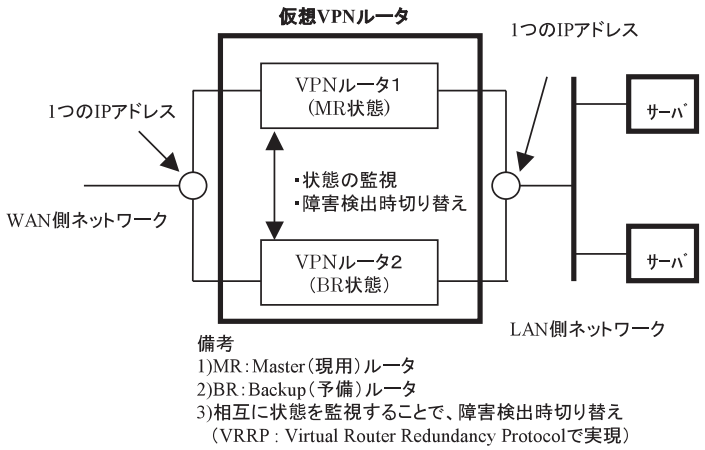


図 6 VRRP による仮想 VPN ルータ構成
Fig. 6 Virtual VPN router configuration using VRRP.

現する．本論文では，VRRP をモバイル VPN に適用することを冗長化のための基本方式とした（**図 6**）．以下では，VRRP を前提に系の切替え時の課題と提案方式について述べる．

(2) SA 情報共有の課題

SA 情報には，セキュリティポリシィ，暗号鍵，認証鍵，および IPsec パケットの ESP ヘッダにあるシーケンス番号（以下では Seq 値と称する，図 2 参照）等がある．これらの情報は，3.2.2 項で述べたように MR と BR で共有されている必要がある．なお，この両者での SA 情報のやりとりは，機密性保持のためローカルな通信手段で行われるものとする．

モバイル VPN ルータの受信側では，リプレイ攻撃を避けるために，IPsec パケットの受信履歴を Seq 値で管理し，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，ただちに廃棄する必要がある．このため SA 情報のうちセキュリティポリシ，暗号鍵，認証鍵等は，鍵交換時（数分から数時間の頻度）に更新されるのに対し，IPsec 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ごとに更新されるので，MR と BR で Seq 値を VPN ルータの性能を落とさずに完全に共有することは困難であり，新しい切替え方式が必要である．

(3) 系切替え方式

IPsec 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[7]．この性質を利用し，IPsec パケット送信側での Seq 値の付与範囲を仮想 VPN ルータを構成する各ルータごとに限定使用することによって，通信する相手ごとに Seq 値の使用範囲を異なる範囲とし，系切替え時に Seq 情報の引き継ぎを不要にできる．また，この Seq フィールドは 32 ビットあるので，複数に分割してもその範囲は十分大きいのでデータ転送に関する実質的な影響はほとんどないと予想される．筆者らが提案しているモバイル VPN ルータは，モバイルクライアントと LAN（モバイル VPN ルータ），および LAN（モバイル VPN ルータ）相互間に適用することを想定している．このため，Seq 値の付与範囲は，LAN 相互間通信を考慮し以下の 4 つの領域に分割することとした[29]．

領域 1：`"00000000"-"3FFFFFFF"`
領域 2：`"40000000"-"7FFFFFFF"`
領域 3：`"80000000"-"BFFFFFFF"`
領域 4：`"C0000000"-"FFFFFFFF"`

また，本提案方式では，通信する相手ごとに Seq 値の付与範囲を変更するため，系を切り替えたモバイル VPN ルータは，そのことを陽に相手に通知する必要がある．このため，系が切り替わった際に VPN ルータ（新たに MR となったルータ）は，鍵交換プロトコルで規定される任意の情報の送受信が可能な通知情報フィールド（Notification Payload）[10]に新たな通知メッセージを定義し，相手側にそのことを通知することとした．具体的な処理手順を LAN（モバイル VPN ルータ）相互間通信を例に説明する（**図 7**）．

1) LAN（A）の VPN ルータ a1（MR）と LAN（B）の VPN ルータ b1（MR）が VPN セッションを設定し IPsec で通信している．この場合，ルータ a1，b1 はそれぞれ Seq 値として，`"00000000"-"3FFFFFFF"` の範囲を使用する．

2) LAN（B）の b1 が故障した場合，系が切り

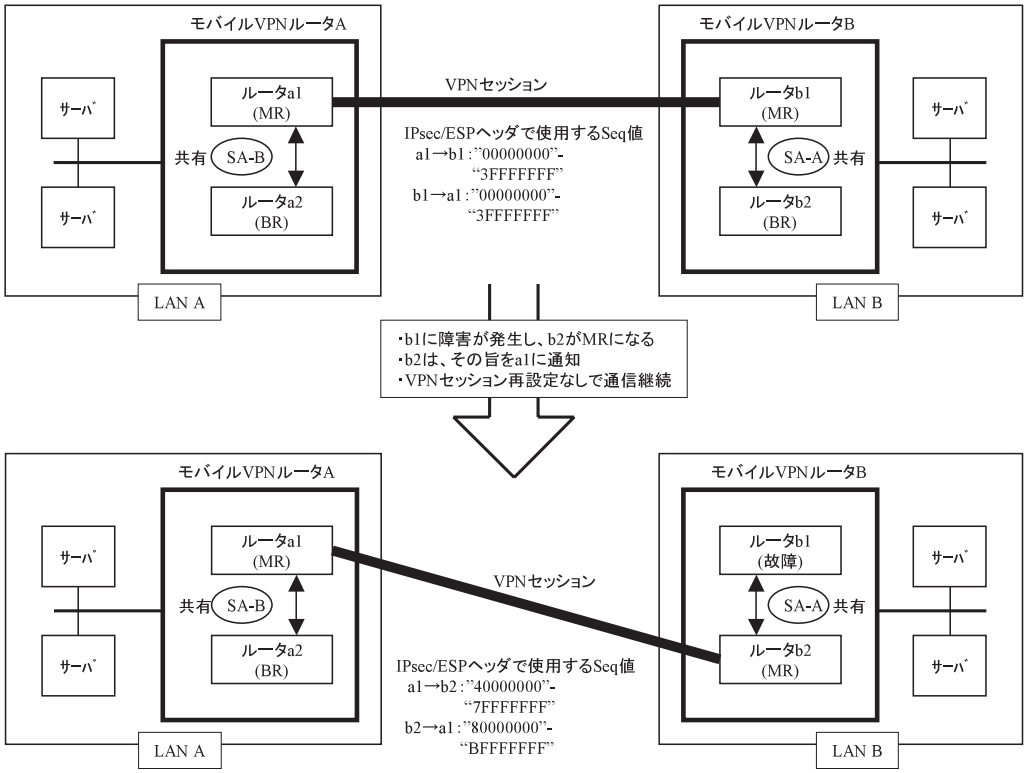


図 7 提案方式によるルータ切替え手順
Fig. 7 Proposed router switching method.

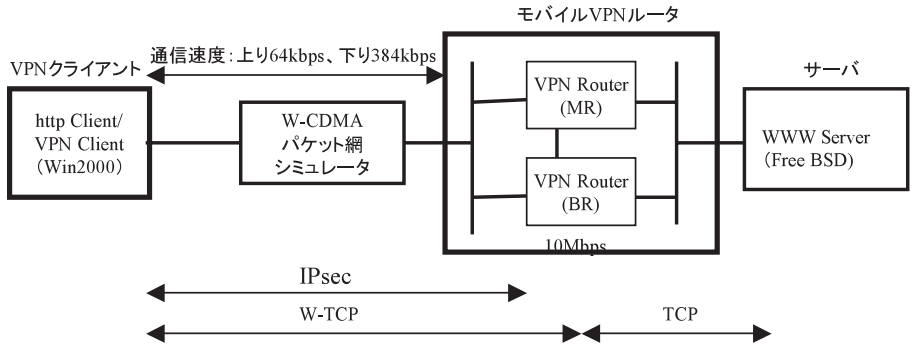


図 8 モバイル VPN 方式のプロトタイプ評価試験システム構成
Fig. 8 Mobile VPN prototype system for evaluation.

替わり新たに b2 が MR となり，b2 はそのことを LAN（A）に通知する．b2 は Seq 値として"80000000"-"BFFFFFFF"の範囲を使用する．なお，b2 は以降，"00000000"-"3FFFFFFF"の範囲の Seq 値を持つ受信 IP パケットはすべて廃棄する．

3) 上記の通知を受け取った LAN（A）の a1 は，以降 LAN（B）向けの Seq 値として"40000000"-"7FFFFFFF"の範囲を使用する．

クライアントと LAN（モバイル VPN ルータ）間の場合も同等の手順をとることになる．この方式によって，冗長化されたルータ相互間で Seq 値に関する情報を共有せずに，Seq 値のチェックが可能となり，リプレイ攻撃に対して十分な防御が可能となる．

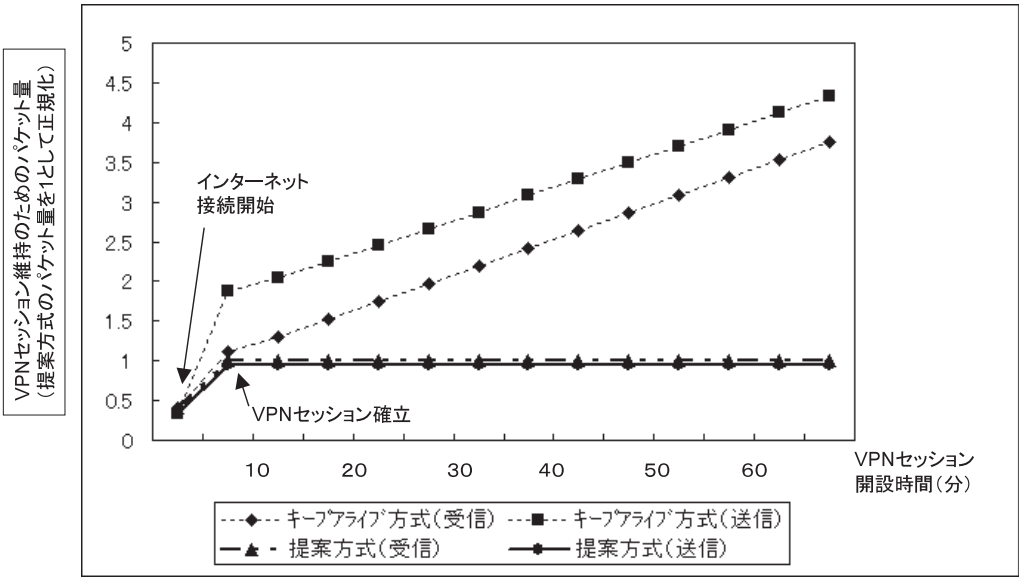


図 9 提案方式によるパケット数削減効果
Fig. 9 Amount of packets for VPN session maintenance.

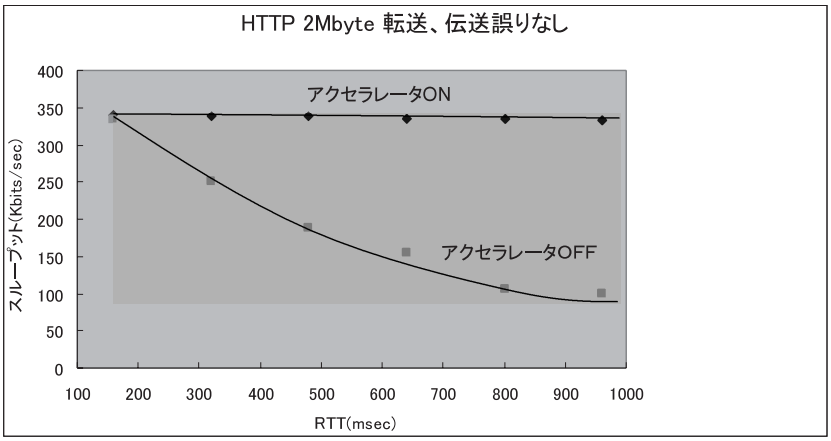


図 10 TCP アクセラレータの効果（スループット）
Fig. 10 Throughput evaluation of TCP accelerator.

5. 実 装 評 価

4 章で提案したモバイル VPN 方式のプロトタイプシステムによる実装評価結果について述べる．

5.1 評価システムの構成

試作したモバイル VPN ルータとモバイル VPN クライアントのプロトタイプシステムを使用し，提案方式の有効性を評価した．その評価系を**図 8** に示す．モバイル VPN ルータとクライアント間は，W-CDMA シミュレータ[16]を介して接続し，擬似的な通信環境とした．

5.2 VPN セッション管理方式の評価

VPN セッション管理方式の有効性を確認するため，提案方式とキープアライブ方式を採用している既存製品との VPN 維持パケット量の比較を行った．VPN セッション設定済みの状態で，上位のアプリケーションをいっさい起動せずに放置した場合に各々で送受された情報量を比較した結果を**図 9** に示す．提案方式では，VPN セッション維持のために，無用なパケットが流れていないことが確認できる．なお，1 時間放置した後，それぞれローカル IP で ping を行って，VPN セッションが維持されていることも確認している．

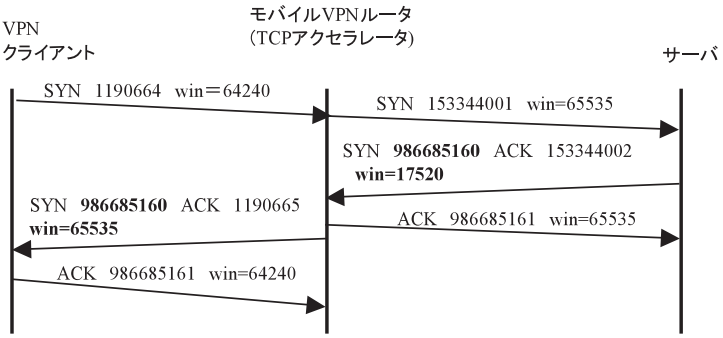


図 11 TCP セッション設定時の実測シーケンス例
Fig. 11 Example of TCP session set up sequence logs.

5.3 セキュア TCP アクセラレーションの評価

HTTP プロトコルを利用して，2 MByte のファイルのダウンロードに要する時間を測定した．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，遅延時間（RTT: Round Trip Time）とスループットの関係を**図 10** に示す．アクセラレータ ON の場合，W-TCP（受信バッファサイズの拡大等）の効果が顕著にあり，ほぼ理論限界値に近い最大性能が得られおり，十分有効であることが分かった．

TCP アクセラレータにおける，TCP セッション設定時（3 ウェイハンドシェイク）の処理シーケンスログを**図 11** に示す．図 11 より，サーバ側 TCP の ISN 値を透過としたまま，クライアント側 TCP の初期ウィンドウサイズを拡張する（W-TCP の設定）ことに成功しており，TCP セッションハイジャック攻撃に有効に働くことが分かった．なお，TCP セッションに対する攻撃法としては，このほかにも，送受信間の SN 値の同期を崩す方式[31]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かかわらず危険度は同一であり，本論文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．

5.4 冗長化モバイル VPN ルータ方式の評価

通信中に擬似的に VPN ルータに障害を発生させ，その後系が切り替わり通信が正常に継続できるか否かの検証実験を行った．FTP プロトコルで 1 MByte のファイルのダウンロードを実行中に，VPN ルータの MR の電源を手動で切った場合のクライアント側での TCP シーケンス番号（SN 値）の時刻変化を**図 12** に示す．なお，提案方式の効果を明確にするため，VRRP 方式（SA 情報の共有を行わない場合）の同様の評価結果を**図 13** に示す．

図 12 より，提案するモバイル VPN ルータ冗長化方式により，3–4 秒程度で系の切替えが可能であることが分かった．切替え時間がこの程度であれば，上位アプリケーションに致命的な影響を与えず十分実用に耐えるといえる．また，図 13 と比較すると 3 割以上切替え時間を短縮していることが分かる．ただし，本評価においては，VPN セッションは 1 つのみで行ったが，複数の VPN セッションの場合（多数のユーザが同時に利用している環境）では，鍵交換処理のオーバヘッドが VPN セション数に比例して高くなり，提案方式の効果がより顕著になると考えられる．特に，鍵交換処理でオプションとなっている Diffie-Hellman 法[32]を利用する場合には，その処理負荷はより高くなることが分かっており，IPsec のセキュリティ機能を低下させずに冗長化ルータ構成を可能とする提案方式は，このようなモバイル VPN 利用形態では必須になるといえる．

6. おわりに

本論文では，VPN を W-CDMA 網に適用する場合のモバイル VPN 方式について提案した．提案した方式は，VPN として広く使用されている IPsec をベー

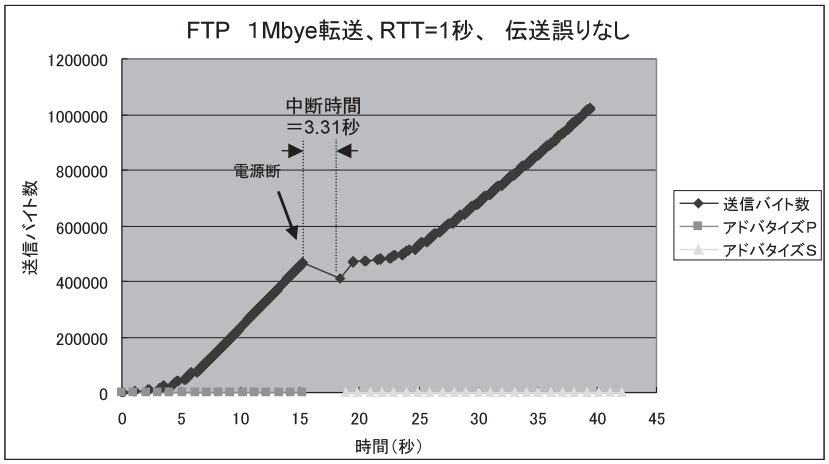


図 12 提案方式による系切替え時の TCP シーケンス
Fig. 12 TCP sequence logs of proposed router switching method.

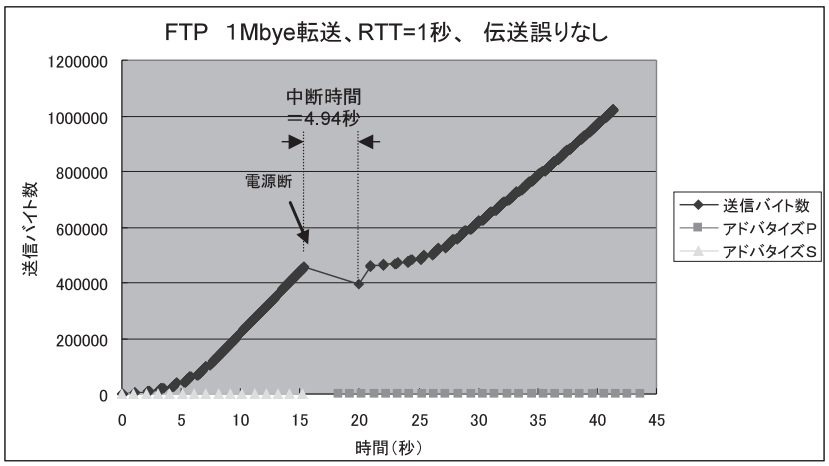


図 13 VRRP 方式（SA 情報の共有なし）による系切替え時の TCP シーケンス
Fig. 13 TCP sequence logs of original VRRP method.

スとし，キープアライブをしない VPN セッション管理方式を提案した．また，TCP の性能問題を解決するためプロキシ機能をモバイル VPN ルータ上で実現することとし，その際に新たに発生する TCP セッションハイジャック問題を防止するセキュア TCP アクセラレータの実現方式を提案した．さらに，信頼性を向上させるための冗長化ルータ構成を実現するため標準的なプロトコルである VRRP をベースにセキュリティレベルを保持したまま，効率良く系の切替えを実現する方式を提案した．また，本方式を実装したプロトタイプシステムを構築し，W-CDMA 網を疑似するシミュレータを使用して，実測評価した．

この結果，提案した方式の機能が有効に働き，かつ性能上も TCP スループットを最大 3 倍向上させるとともに，モバイル VPN ルータの障害時に系の切替え時間が 3 秒程度であり，十分実用的な方式であることを示した．

今後は，FOMA 網等の実際のモバイル環境での評価を継続するとともに，複数のクライアントが同時接続している場合の系の切替え時間等の性能を明確にし，本提案方式に基づくモバイル VPN ルータを実用化する際のハードウェア条件等を設計指針として確立する予定である．

謝辞 日頃，御指導いただく（株）NTT ドコモマルチメディア研究所中野博隆所長，評価実験に協力していただいた（株）NTC 功刀氏に感謝する．

参 考 文 献

1) Townsley, W., Valencia, A., et al.: Layer Two Tunneling Protocol L2TP, IETF, RFC2661 (Aug. 1999).
2) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, IETF, RFC2401 (Nov. 1998).
3) Kent, S. and Atkinson, R.: IP Authentication Header, IETF, RFC2402 (Nov. 1998).
4) Madson, C. and Glenn, R.: The Use of HMAC-MD5-96 within ESP and AH, IETF, RFC2403 (Nov. 1998).
5) Madson, C. and Glenn, R.: The Use of HMAC-SHA-1-96 within ESP and AH, IETF, RFC2404 (Nov. 1998).
6) Madson, C. and Doraswamy, N.: The ESP DES-CBC Cipher Algorithm With Explicit IV, IETF, RFC2405 (Nov. 1998).
7) Kent, S. and Atkinson, R.: IP Encapsulating Security Payload (ESP), IETF, RFC2406 (Nov. 1998).
8) Piper, D.: The Internet IP Security Domain of Interpretation for ISAKMP, IETF, RFC2407 (Nov. 1998).
9) Maughan, D., et al.: Internet Security Association and Key Management Protocol (ISAKMP), IETF, RFC2408 (Nov. 1998).
10) Harkins, D. and Carrel, D.: The Internet Key Exchange (IKE), IETF, RFC2409 (Nov. 1998).
11) Glenn, R. and Kent, S.: The NULL Encryption Algorithm and Its Use With IPsec, IETF, RFC2410 (Nov. 1998).
12) Pereira, R. and Adams, R.: The ESP CBC-Mode Cipher Algorithms, IETF, RFC2451 (Nov. 1998).
13) Simpson, W.: The Point-to-Point Protocol (PPP), IETF, RFC1661 (July 1994).
14) Postel, J.: User Datagram Protocol, IETF, RFC768 (Aug. 1980).
15) Inmura, H., et al.: TCP over 2.5 G and 3 G Wireless Networks, IETF, draft-ietf-pilc-2.5g3g-10 (July 2002).
16) 石川太朗，稲村　浩，高橋　修：W-CDMA 向け TCP プロファイル，情報処理学会研究会報告，MBL15-3 (Nov. 2000).
17) 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).
18) Kojo, M., Raatikainen, K. and Alanko, T.: *Connecting Mobile Workstations to the Internet over a Digital Cellular Telephone Network*, University of Helsinki, Helsinki (Sep. 1994).
19) Border, J., et al.: Performance Enhancing Proxies Intended to Multigate Link-Related Degradations, IETF, RFC3135 (Jun. 2002).
20) 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, p.153 (Oct. 1998).
21) Postel, J.: Transmission Control Protocol, IETF, RFC793 (Sep. 1981).
22) Morris, R.T.: A Weakness in the 4.2BSD UNIX TCP/IP Software, Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ (Feb. 1985).
23) 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).
24) Bellovin, S.: Defending Against Sequence Number Attacks, IETF, RFC1948 (May 1996).
25) Statistical Weakness in TCP/IP Initial Sequence Numbers, CERT Advisory, CA-2001-09 (May 2001).
26) 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).
27) 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，情報処理学会研究会報告，MBL10-7 (Oct. 1999).
28) 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, p.329 (2001).
29) 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, p.329 (2001).
30) Knight, S., et al.: Virtual Router Redundancy Protocol, IETF, RFC2338 (Apr. 1998).
31) Joncheray, L.: *Simple Active Atack Against TCP*, Merit Network Inc. (1996).
32) Rescorla, E.: Diffie-Hellman Key Agreement Method, IETF, RFC2631 (Jun. 1999).

(平成 14 年 3 月 26 日受付)
(平成 14 年 10 月 7 日採録)

高橋　修（正会員）

1951 年生．1975 年 3 月北海道大学大学院工学研究科修士課程修了，同年 4 月電電公社（現 NTT）入社．情報通信研究所でコンピュータネットワークアーキテクチャの研究開発，および OSI の標準化に従事．1999 年 NTT ドコモに異動．マルチメディア研究所にてモバイルインターネットの研究開発に従事．電子情報通信学会会員．

高橋　竜男

1964年生．1989年3月東海大学大学院工学研究科修士課程修了，同年4月NTT入社．交換システム研究所にてノードシステム用制御系アーキテクチャ，分散プラットフォームの研究開発に従事．1998年NTTドコモに異動．マルチメディア研究所にてモバイルインターネットの研究開発に従事．電子情報通信学会会員．

三浦　史光（正会員）

1962年生．1990年3月京都大学大学院工学研究科修士課程修了，同年4月NTT入社．ソフトウェア研究所，情報通信研究所にて分散処理・DB・VOD等の研究に従事．1999年NTTドコモに異動．マルチメディア研究所にてセキュリティの研究開発に従事．

西郷　　悟（正会員）

1974年生．2000年3月北海道大学大学院理学研究科修士課程修了，同年4月NTTドコモ入社．マルチメディア研究所にてモバイルインターネット向けのセキュリティ技術の研究開発に従事．

水野　忠則（正会員）

1945年生．1968年名古屋工業大学経営工学科卒業．同年三菱電機（株）入社．1993年静岡大学工学部情報知識工学科教授，現在，同大学情報学部情報科学科教授．工学博士．情報ネットワーク，モバイルコンピューティング，放送コンピューティングに関する研究に従事．著書としては「プロトコル言語」（カットシステム），「コンピュータネットワーク概論」（ピアソン・エデュケーション）等がある．電子情報通信学会，IEEE，ACM各会員．当会フェロー．