モバイルコンピューティングにおけるVPNの研究

移動網を介したモバイルコンピューティングに適するVPNプロトコルについて検討した．
本稿では，その概要と実装および評価結果について報告する．

高橋 竜男　鶴巻 宏治　関口 克己　竹下 敦

1. まえがき

近年インターネットを利用したVPN（Virtual Private Network）が着目されている．

今後VPNは，移動体通信を利用したモバイルコンピューティングにおいても多く利用されるようになると考えられる．しかし，既存のVPNプロトコルは，固定網での利用を前提に検討されているため，移動体通信特有の問題が及ぼす影響を調査し，対策を検討する必要がある．

このような観点から，既存のVPN製品の評価を行うことで問題点を抽出し，その対策を施したモバイル向けVPNプロトコルの提案を行った[1]．

本稿は，これらの概要とその実装例および評価に関して報告するものである．

2. VPNの概要

2.1 VPNとは

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，あたかも専用線のように利用するための技術である．

モバイル環境下においてユーザは，図1に示すダイヤルアップ型VPNを利用することによって，以下のメリットを得ることができる．

(1) 通話料金の削減

PHSの通話料金は，距離に比例する部分が大きい．遠距離から企業LAN（Local Area Network）にアクセスする必要があるユーザはVPNを導入することにより，最も近いISP（Internet Service Provider）のアクセスポイントまでダイヤルアップし，そこからインターネット経由で企業LANにアクセスすることが可能になる．これにより企業LANのRAS（Remote Access Service）に直接ダイヤルアップする場

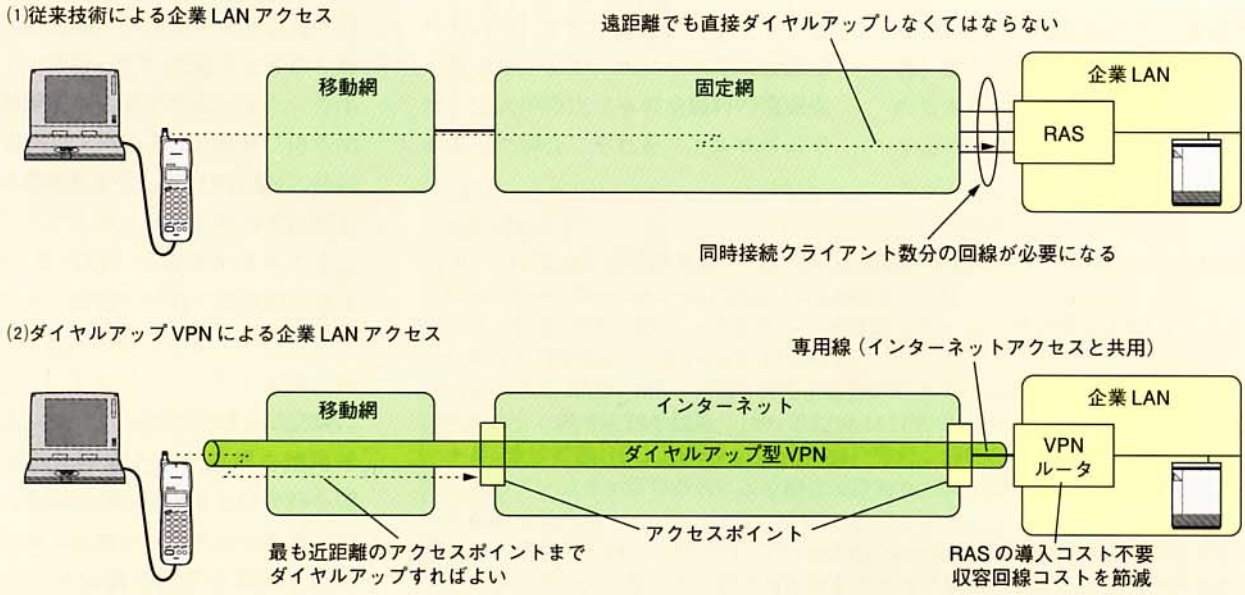


図1　VPNの概要

合に比較して，通話料金の距離比例分を節約することが可能になる．

(2) RASの導入，維持管理コストの削減

ディジタル方式自動車電話方式（PDC：Personal Digital Cellular）でRASに直接ダイヤルアップした場合，ユーザは9600bit/sでしか利用できないにもかかわらず，RAS側の固定電話回線1回線を占有してしまう．また，RAS側には，同時接続ユーザ数分の固定電話回線を導入する必要がある．VPNを導入すれば，これらの電話回線をインターネットへの接続回線で兼用することが可能になり，回線導入コスト，使用料を節減できる．また，RAS自体の導入および維持管理コストも不要となる．

(3) その他

DoPa（ドゥーパ）*1のLAN接続サービスにおいては，パケット関門中継処理装置（PGW：Packet Gateway Module）～企業LAN間に専用線を敷設する必要がある．しかし，VPNを利用することでこれをインターネットに置き換えても同等のサービスを実現することが可能となり，専用線敷設コスト・敷設までの期間・回線使用料を削減することが可能である．

2.2 VPNプロトコルの標準化動向

現在有力なVPNプロトコルについて概説する．

(1) L2TP（Layer Two Tunneling Protocol）[RFC2661]

L2TPパケットの構造を図2(a)に示す．PPP（Point to Point Protocol）のフレームをUDP（User Datagram Protocol）のパケットでカプセル化している点が特徴である．これにより，IP以外のパケットをIP網上で転送可能になることが利点となる．

反面，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直接規定されていない．

(2) IPsec（Internet Protocol Security）[RFC2401-2412，2451]

IPsecには，AH（Authentication Header）[RFC2402]とESP（Encapsulating Security Payload）[RFC2406]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．このなかで，代表的なものがトンネルモードESPである．

図2(b)にそのパケット構造を示す．

IPパケットをIPパケットでカプセル化している点が特徴である．これにより，企業LAN内のローカルなIPパケットを，インターネット上で転送することができる．

カプセル化の際，オリジナルのIPパケットは盗聴防止とLAN内サーバのIPアドレス秘匿のため，ヘッダ部ごと暗号化され（図2(b)①），VPNセッションを識別するESPヘッダ（②），パディングなどのESPトレイラ（③）が付加され，さらに受信側で改竄検出とパケット認証を行うため，①～③に鍵付ハッシュ関数を適用した結果をESP認証部（④）に付加されたうえで，新たなIPヘッダ（⑤）を付加される．このとき，新たなIPヘッダの送信先には，宛先企業LANのSGW（Security Gateway）*2のグローバルIPアドレス，またはVPNクライアント（IPsec終端機能を有するダイヤルアップ移動端末）のグローバルIPアドレスが指定される．

このように，IPsecは，セキュリティ機能が充実していることが大きな利点である．さらに，これらIPパケット単位のセキュリティを実現するため，ノード側（SGW，VPNクライアント）に以下の概念を導入している．

① SA（Security Association）[RFC2401]

IPsecにおけるVPNセッションは，SAと称する関係を構築することにより開設される．実装上，SAはパケットの送信元と受信元の双方で合意したセキュリティポリシー，暗号および認証鍵を格納するオブジェクトであり，次に述べる鍵交換時に更新される．

② 鍵交換

共通鍵暗号方式では，送受信を行う両者間で同一の鍵を所有する必要がある．現在主流の56bit型の共通鍵暗号方式では暗号文

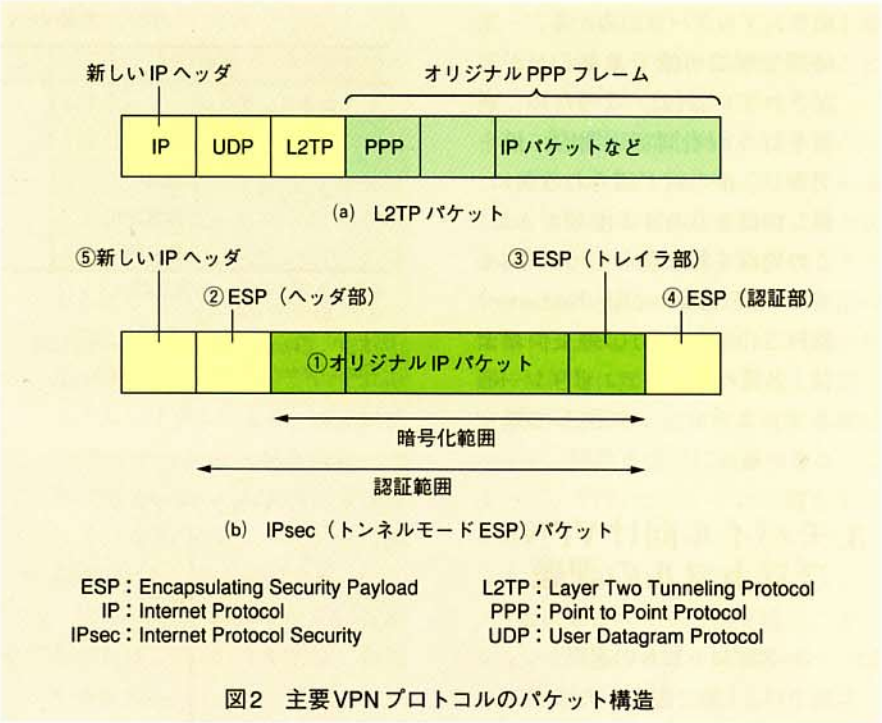


図2 主要VPNプロトコルのパケット構造

*1 DoPa（ドゥーパ）：データ端末をPDC-Pネットワークに接続し，PPPを用いてインターネットや企業LANなどの外部ネットワークと接続するサービスである．1997年3月に開始された

*2 SGW：Security Gateway企業LAN側でIPsecを終端するVPNルータなど

のサンプルデータのみから，一定時間で解読可能であることが実証されている[2]．このため，通信を行う両者間で定期的に鍵を更新し，前の鍵が破られる前に，新しい鍵を共有する必要がある．この処理を鍵交換という．IPsecでは，IKE (Internet Key Exchange) [RFC2409] により，鍵交換および，各種セキュリティポリシーのネゴシエーションに関して規定している．

3. モバイル向けVPNプロトコルの課題

3.1 ベースプロトコルの選択

本稿では2.1節で説明したモバイルでのVPN利用形態に着目し，既存のVPNプロトコルをベースとし，これを移動網経由で利用した場合における課題を整理し，それらを解決したものをモバイルVPNとして提案する．

2.2節で述べた主要VPNプロトコルの機能比較を表1に示す．

ベースとする既存VPNプロトコルとしては，セキュリティ機能の充足性を重視し，IPsec（トンネルモードESP）を採用することとした．

3.2 モバイル環境におけるIPsecの課題

(1) キープアライブ

IPsecでは，本来キープアライブを規定していない．しかし，IPsecをダイヤルアップ型VPNとして使用する場合，以下の理由によりキープアライブを実装する必要が生じる．

ISPにダイヤルアップ接続を行う場合，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，通信相手のIPアドレスをキーに，SAを管理する必要がある．そのため，ダイヤルアップ型VPNの場合，VPNセッション開設時に新規SAを作成し，VPNセッション終了時にはこれを削除しなくてはならない．しかし，VPNクライアントのISPへの接続が異常終了した場合に，SGWはこの状態を直接検出することができない．

このようなVPNセッション管理上の問題を解決するために，SGW～VPNのクライアント間で，キープアライブパケットを送受する必要が生じる(図3)．しかし，VPNクライアントが移動網を介してISPに接続している場合，この方式は以下の問題を生じる．

① 誤切断

クライアント側電波状況悪化による，一時的な遅延時間増大が発生した際，SGW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クライアントのISPへの接続が正常である場合でも，VPNセッションを切ってしまう場合がある．

② 課　金

移動網側がパケット網の場合，キープアライブパケット自体に課金が生じてしまうため，本来情報量課金であるはずのパケット網に，時間課金の要素が加わることになり，ユーザにとって極めて不利な状況となる．

(2) 鍵交換

結局のところ，2.1節で述べたVPNのメリットは，ユーザ側コストの削減ということになる．したがって，VPN導入にかかるコストは，削減されるコストと比較して，十分低くなくてはならない．

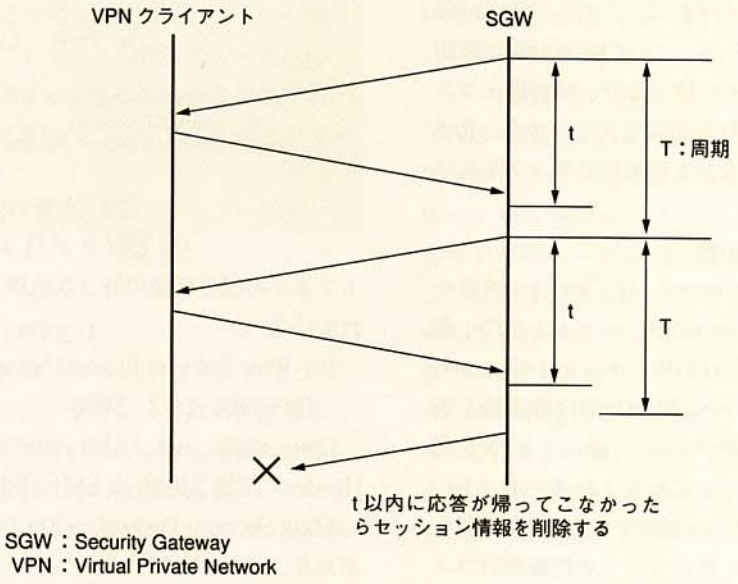
このことより，VPN機能は廉価なSOHO用ルータなどに収容する必要があるが，一般にこのようなルータにお

表1　主要VPNプロトコルの機能比較

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でサポート

ESP：Encapsulating Security Payload
IPsec：Internet Protocol Security



SGW：Security Gateway
VPN：Virtual Private Network

図3　キープアライブの例

いては，PCなどに比較すると処理能力が劣るプロセッサが使用されている．そのため，VPN機能の収容にあたっては，プロセッサ負荷について十分な検討を要する．

IPsec関連の処理は，以下のように分類することができる．

① 情報量に比例する分…暗号，復号処理
② パケット数に比例する分…トンネリング，パケット認証処理，パケット配送処理
③ VPNセッション数に比例する分…鍵交換処理

鍵交換処理は，一般的には数十分から数時間に1度と頻度は少ない．しかし，IKEが採用している「Diffie-Hellman」の鍵交換アルゴリズム[RFC2631]は，廉価なプロセッサで行った場合，1分以上を要することもあり，この時間はログオン時の待ち時間に追加される．

また，モバイル環境下では，無線リンク断によってVPNセッションが中断された場合にSAを作成し直さなければならないため，SAの平均寿命が短くなることや，固定網の場合よりも帯域が狭くなることなどから，相対的に①，②の処理よりも③の処理の比重が大きくなると考えられる．

これらより，鍵交換の処理負荷軽減について検討する必要がある．

4. モバイルVPN

4.1 キープアライブを利用しないVPNセッション管理方式

周期的なキープアライブパケットによるリアルタイムのVPNセッション管理を行わず，VPNセッション管理上問題が発生したときに，SGWがVPNクライアントに状態確認のパケットを送り，問題を解決するという方式を採用する．

以下に詳細を述べる．

① VPN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）．
② 新たなVPNクライアントから，VPNセッション設定要求を受けるが，VPNセッション数が上限値に達しているため，SGWの資源不足などの問題が発生する．
③ FIFO（First in First out）[*3]，LRU（Least Recently Used）[*4]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VPNクライアントに状態確認パケットを送信する．
④ VPNクライアントから応答がなければ，当該SAを削除，資源を解放する．
⑤ VPNクライアントから応答があれば，次の廃棄候補を選択し③の処理を続ける．

これにより，周期的なキープアライブを利用せずに，3.2節(1)で述べたVPNセッションの管理上の問題を解決する．

また，VPNクライアントがSAに登録してあるものとは異なるIPアドレスで，新しいVPNセッション設定を要求してきた場合には（当然再度認証は行われる），以前の当該ユーザのSAを削除し，新規SAを作成する．この場合，上記手順③～⑤による削除を待たずに早期に無効なVPNセッションを検出削除することが可能になる．

4.2 高速鍵交換アルゴリズム

(1) 鍵交換の要件

鍵交換アルゴリズムの満たすべき要件として，以下の点が挙げられる．

① ネットワークで交換される情報から，第三者が鍵を計算できないようにする
② ある鍵から，次回以降の鍵を取得または導出することができないようにする
③ 鍵交換は鍵交換時点でのVPNクライアント，SGW双方の合意に基づいて行い，いずれの側も新しい鍵を一方的に決定することができないようにする

(2) 提案する鍵交換アルゴリズム

4.2(1)で示した，①～③の要件を満たし，かつ計算量の少ない鍵交換方式を検討した．本方式は，VPNクライアント，SGW双方で事前に2つの秘密の情報（S1，S2）を共有し（これは，外部には絶対に知られないことを前提とする），これに一方向性を有する鍵付ハッシュ関数を交互に適用することによって，VPNセッションの鍵を生成する．

本プロトコルは，標準となるフェーズ1およびフェーズ2鍵交換と，オプションとなるログオン時鍵交換（フェーズ0）よりなる．

・フェーズ1

フェーズ1は，ハッシュの更新値を合意するもので，4.2(1)の鍵交換の要件③を満たすため，どちらか一方があらかじめすべての鍵を決定しておいたり，相手の更新値を見てから自分の更新値を決定したりすることができないようにするためのシーケンスである．

図4にそのシーケンス概要を，以下に詳細を説明する．

・フェーズ2

① VPNクライアント，SGW双方独立にそれぞれ乱数n11，n12を発生する（1－1）．
② SGWは自身が発生した乱数n12に，VPNクライアント，SGW間で事前に合意しているハッシュ関数を適用し，その結果H（n12）をVPNクライアントに送る（1－2）．
③ 上記ハッシュ値を受け取ったら，VPNクライアントは自身が発生した乱数n11を平文でSGWに送る（1－3）．

＊3 FIFO：最も古く作成されたVPNセッションを削除する
＊4 LRU：最も古く使用されたVPNセッションを削除する

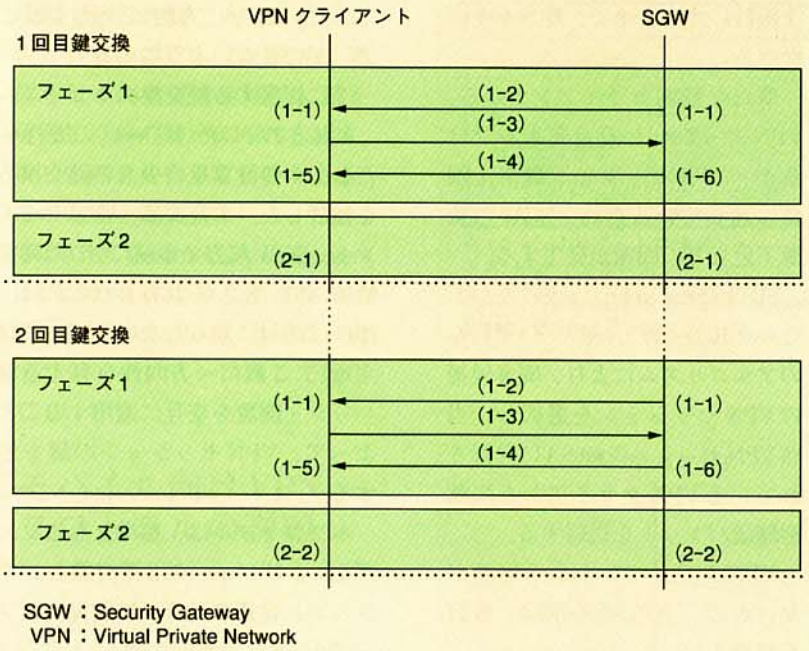


図4　鍵交換シーケンス

④　SGWはn11を受け取ったら，n12を平文でVPNクライアント送る（1－4）．

⑤　VPNクライアントはn12にハッシュ関数を適用し，②で取得した値と比較し，一致すればn11とn12に事前に合意した論理演算を適用し，更新値n1を計算し，フェーズ2に入る（1－5）．

⑥　SGWは③で取得したn11と自身で発生させたn12から，事前にVPNクライアント，SGW間で合意していた論理演算を適用し，鍵の更新値n1を計算し，フェーズ2に入る（1－6）．

・フェーズ2

フェーズ2は，フェーズ1で合意したハッシュの更新値から鍵を計算するシーケンスである．

①　VPNクライアント，SGW双方で，S1を入力値として，2変数ハッシュ関数H（A，B）を利用して，VPNクライアント，SGW双方で以下の2つの値を計算する（2－1）．

$K01 = H_{n1-1}$（K00，S1）

$K1 = H_{n1}$（K00，S1）

このK1を1回目の共有鍵とする．また，K00は，事前共有値である．

ここで，添字の意味は，$H_1 = H$（A，B），$H_2 = H$（H_1，B），$H_3 = H$（H_2，B）と，添え字の回数ハッシュ計算を繰り返すこと示す．

また，2変数ハッシュ関数の計算法としては，HMAC（Keyed Hashing for Message Authentication）[RFC2104] を利用する．

②　次に鍵交換周期が来たときには，両者間で新たにフェーズ1を起動して新しい更新値n2を合意した後，

$K02 = H_{n2-1}$（K01，S2）

$K2 = H_{n2}$（K01，S2）

を計算し，K2を2回目の共有鍵とし，K02を内部に保存する（2－2）．

以下同様に，

鍵$K3 = H_{n3}$（K02，S1）

内部保存$K03 = H_{n3-1}$（K02，S1）

鍵$K4 = H_{n4}$（K03，S2）

内部保存$K04 = H_{n4-1}$（K03，S2）

……と，鍵交換を続ける．

秘密情報S1，S2を交互に使う理由は，たとえば1つの秘密情報Sを使い続けて同様のやり方を行うと，前の鍵に有限回数ハッシュを適用したものが次の鍵と等しくなり，総当り的にSの値を推察されてしまう可能性があるためである．4.2(1)の鍵交換の要件②を満たすために，2つの秘密情報S1，S2を交互に使い，前の鍵を直接新しい鍵計算のための入力値に使用するのではなく，1つ前のハッシュ値（K0x）を入力値とすることによって，ハッシュの一方向性の性質を利用して前の鍵から次の鍵を推察することを難しくしている．また，ネットワーク上を交換される情報は，ハッシュの計算回数を合意するための情報のみであるので，S1，S2を十分な長さとすることによって，4.2(1)の鍵交換の要件①を満たすことができる．

・フェーズ0（ログオン時鍵交換）

一般に廉価なSOHO用ルータにおいては，最低限の主記憶とフラッシュメモリが搭載されている程度で，次回鍵の種となるK0xの保存領域として適当な場所がない．このような場合，ログオフ時にK0xを廃棄し，再ログオン時には再度K00（固定値）から計算を開始する方式をとる必要があるが，この場合，最初の鍵のバリエーションは高々max（n1）通りになってしまい，セキュリティ上重大な問題が生じる．このような場合にオプションとして考案したのがログオン時鍵交換である．

以下，このシーケンスを説明する．

①　VPNクライアントは，SGWにログオン要求を行う．

②　SGWは，任意の乱数K00を発生する．

③　SGWは，乱数K00を事前共有鍵で暗号化し，VPNクライアントに送付する．

以下，VPNクライアントは，K00を復号し，基本モードと同様のフェーズ1，フェーズ2を繰り返す．

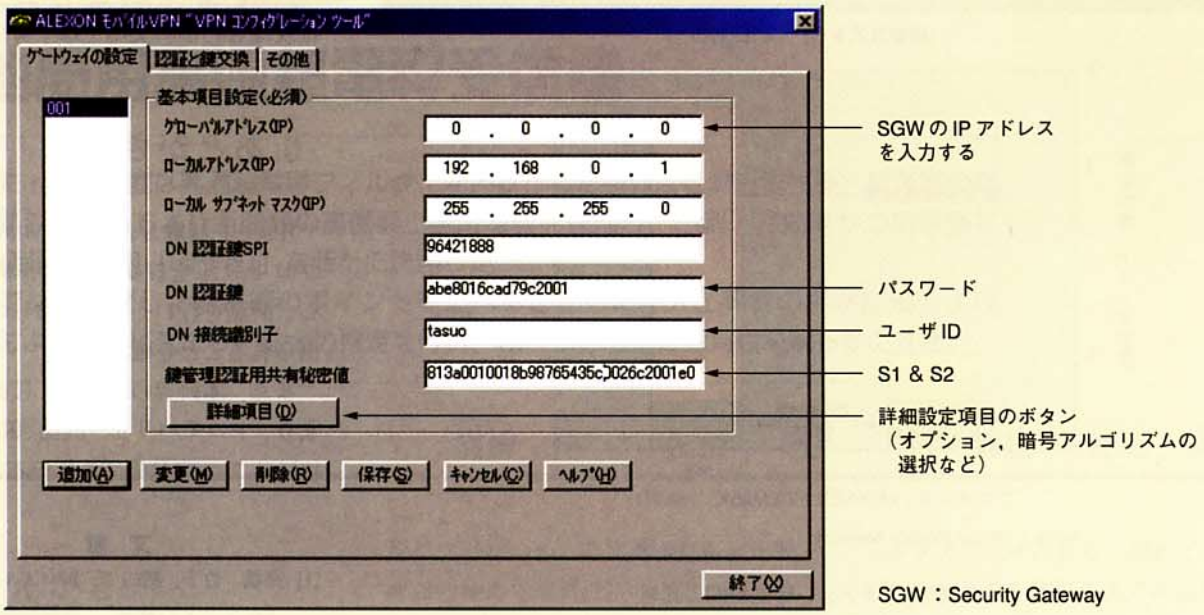


写真1　モバイルVPNクライアント設定画面例

K00を乱数とすることによって，発生し得る鍵のバリエーションを増やしている．また，K00を暗号化して，VPNクライアントに送る理由は，最初の種S1が破られやすくなることを防止するためである．

5. 実装と評価

提案したモバイルVPNプロトコルの試作機への実装と評価について概説する．なお，標準化時期の問題から，試作機は改定前のIPsec［RFC1825-1829］準拠とした．2.2節で述べた改定後のIPSecとの大きな違いは，IKEが規定されていないことが挙げられるが，この点に関してはIKEを先取りして実装したため，機能的には大きな差分はない．

5.1 実　装

(1) 高速鍵交換方式

セキュリティポリシーのネゴシエーションに関する機能をそのまま流用するため，IKE，ISAKMP［RFC2408］のmainモードのフレームワーク中に高速鍵交換方式を埋め込んで実装することとした．ただし，IKEでは，鍵情報を送受するためのペイロードを2つしか含んでいないため，SAネゴシエーションのペイロードを拡張して対応することとした．

(2) セッション管理方式

サーバ側でセッションの最大数を入力し，この値を超えたVPN設定要求があった場合に，SGWは無効なVPNセッションを検索するためのパケットを送信することとした．

(3) VPNクライアント

VPNクライアントの設定画面を写真1に示す．S1，S2は，ユーザによる手入力とした．

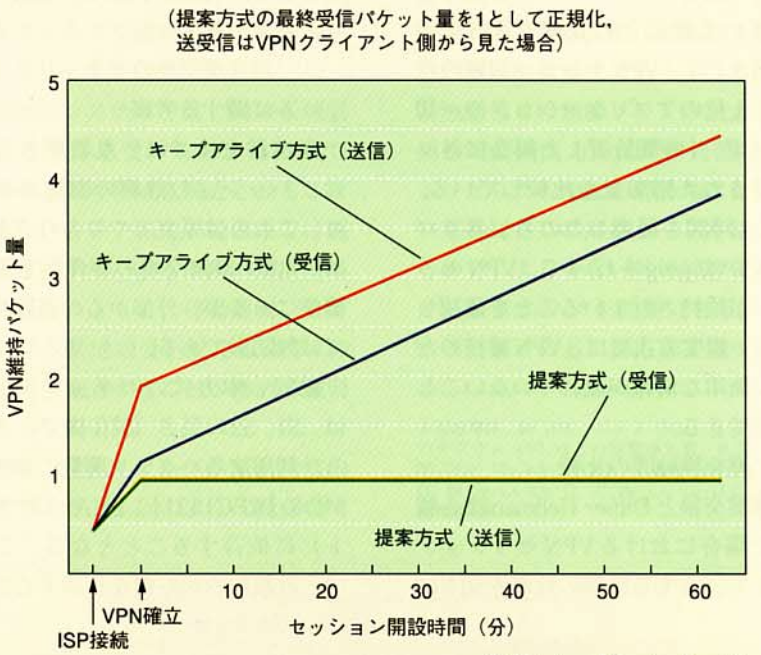


図5　提案方式によるパケット数削減効果

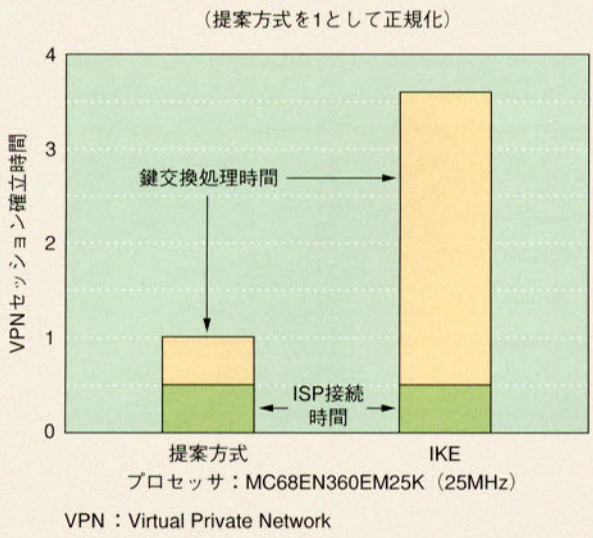


図6　VPNセッション確立時間の比較

5.2　評　　価

(1)　セッション管理方式

提案方式とキープアライブ方式を採用している製品との比較を図5に示す．図5では，VPNセッション開設状態で，上位のアプリケーションを一切起動せず，1時間放置した場合に各々で送受された情報量を比較している．また，1時間を経過したのち，各々ローカルIPでpingを行って，VPNセッションが維持されていることを確認している．提案方式では，VPN維持のために，無用な情報が流れていないことが確認できる．

(2)　鍵交換時間の比較

高速鍵交換とDiffie-Hellman法を利用した場合におけるVPNセッション開設までに要する時間の比較を図6に示す．図6より高速鍵交換を利用することにより，VPNセッションを確立するまでの時間を約1/4に短縮できたことが分かる．

(3)　高速鍵交換のセキュリティレベルに関する考察

高速鍵交換では，乱数値となるのは，ハッシュの計算の回数のみであり，これらは平文でやりとりされるため，4.2(1)の鍵交換の要件③を満たす機能はあるが，外部からの盗聴に対しては無防備である．

結局，本方式のセキュリティ強度は，S1，S2の長さ（試作機では256bit）と，利用するハッシュ関数の強度（同MD5［RFC1321］，SHA-1をサポート）に依存することとなる．この点で，乱数のみから鍵を合意するDiffie-Hellman法に，セキュリティレベルでは及ばないが，実用上は十分であると考えられる．

6. あとがき

IPsecを基礎したモバイル向けVPNプロトコルを提案し，試作機に実装し，評価を行い，予想どおりの効果が得られることを確認した．

また，本研究の成果は，技術開示により，ドコモバリュー商品（RDM700）[3]として，商品化されている．

文　献

[1] 高橋，竹下，関口：“モバイル向けVPNプロトコルの検討”，情報処理学会モバイルコンピューティング研究会 99-MBL-10-7，1999.

[2] Electric Frontier Foundation, Cracking DES, O' REILLY, May, 1998.

[3] “Mobile VPN Router RDM700”，http://www.alexon.co.jp/rdm700/index.html, 2000.

用語一覧

AH：Authentication Header
ESP：Encapsulating Security Payload
FIFO：First in First out
HMAC：Keyed Hashing for Message Authentication
IKE：Internet Key Exchange
IP：Internet Protocol
IPsec：Internet Protocol Security
ISP：Internet Service Provider
LAN：Local Area Network（構内通信網）
LRU：Least Recently Used
L2TP：Layer Two Tunneling Protocol
PDC：Personal Digital Cellular（ディジタル自動車電話方式）
PGW：Packet Gateway Module（パケット関門中継処理装置）
PPP：Point to Point Protocol
RAS：Remote Access Service
SA：Security Association
SGW：Security Gateway
UDP：User Datagram Protocol
VPN：Virtual Private Network