モーバイルコンピューティング 10－7
（1999．10．7）

モバイル向けVPNプロトコルの検討

高橋 竜男† 竹下 敦† 関口 克己†

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．VPNは，今後移動体通信を利用したモバイルコンピューティングにも多く適用されるようになると考えられるが，移動通信網や，モバイルコンピューティングの特徴を陽に意識した標準ＶＰＮプロトコルは現在のところ存在しない．このような観点から，我々は，既存の標準ＶＰＮプロトコルであるIPSec (IP Security) を対象に問題点の抽出・確認と，対策の検討を行った．この結果，キープアライブパケットによる通信品質の悪化等や，鍵交換処理の過負荷が問題であると考え，これらを解決するモバイル向けVPNのための技術として，キープアライブを利用しないセッション管理方式と，ハッシュを利用した軽量な鍵交換プロトコルを提案する．

A Study of VPN Protocol for Mobile Computing

Tatsuo TAKAHASHI†, Atsushi TAKESHITA†, and Katsumi SEKIGUCHI†

Virtual Private Network (VPN) over Internet is paid much attention in recent years. It is expected that VPN will be more popular on mobile computing, therefore many people will use VPN over the mobile communication network. There are several standardized VPN protocols, however no one is designed for use on the mobile communication network. In this situation, we made experiments on establishing VPN over mobile communication network, using IPSec (IP Security), one of the major standard VPN protocol. We found two problems from the results of these experiments, deterioration of communication quality due to keep-alive packets, and load of Internet key exchange protocol. In this paper, we describe these problems and propose a session management algorithm without keep-alive packets and a lightweight key-exchanging algorithm, that is the solution of these problems.

1．はじめに

近年，インターネットの普及に伴い，小規模オフィスにもLANが導入され，オフィス間の接続を専用線よりも安価に実現する技術として，あるいは移動端末とオフィスとの接続をRAS（Remote Access Server）を利用することなく安価に実現する方法として，インターネット上に仮想的な専用線を張る，VPN（Virtual Private Network）技術が着目されている．このようなVPNは，今後移動体通信を利用したモバイルコンピューティングにも普及していくものと考えられる．しかしながら，既存のVPNプロトコルおよび製品は，基本的に固定通信を前提として設計されており，移動体通信の特性を陽に考慮して設計されているものは存在しない．また，既存のVPN製品は一般に導入価格が高く，SOHOユーザ等小規模企業ユーザがそのコスト的優位性を十分享受できな状況にある．

本報告では既存のプロトコルの問題点を洗い出し，モバイル向けVPNを処理能力の高くないハードウェア上で実現するための，VPNセッションの管理方式と，軽量な鍵交換方式を提案する．検討にあたっては，次世代移動体通信システム（IMT-2000）において，主流となると考えられている，パケット通信網の利用を前提とした．

† NTT DoCoMo マルチメディア研究所
NTT DoCoMo Multimedia Laboratories

2．VPNの概要

2．1 VPNを構成する技術

VPNはインターネット等のような，多数の利用者によって共用されるネットワークを，クローズドな専用線の様に利用するための技術である．このため，利用者の要求の側面から，その実現技術は以下

の様に大別される.

（1）カプセリング技術

専用線と同等の利便性を実現する技術. すなわち, グローバルな環境中においてローカルと同等のユーザの利用環境を実現するために, ローカル環境のカプセル化を行う.

（2）セキュリティ技術

以下の機能のうち, 必要に応じたものを提供する.

- 機密性確保：第三者による盗聴を防止する. 暗号化技術, 鍵交換などによって実現される.
- 完全性確保：第三者によってメッセージの内容を改ざんされることを防止する. 鍵付きハッシュ関数などが利用される.
- 否認防止：通信の事実を否認されることを防止する.
- 認証：ユーザ本人であることを認証する
- 秘匿性：通信の事実自体を秘匿する

（3）QoS 技術

専用線と同等の品質を実現するための技術. 現在のところ有効な QoS 機能を持った標準 VPN プロトコルは存在しない.

2．2　VPN の実現形態

VPN はその形態から, 以下の様に分類することができる.

（1）LAN 間 VPN

たとえば企業の本社の LAN と支社の LAN の間に専用線を引く場合などに, 直接専用線を引く代わりわりに VPN を利用する方式. 専用線は, 最寄の ISP のアクセスポイントまで引けばよいので, 一般的に通信コストを大幅に削減できる. 図 1 の例では, 本社 LAN, 支社 LAN のそれぞれに配置された SGW（セキュリティゲートウェイ）により VPN を終端している.

（2）ダイヤルアップ VPN

主として, 移動端末等から最寄の ISP などにダイヤルアップし, そこから VPN を経由して企業 LAN にアクセスする形態. 企業 LAN の ISP への既存の専用線を利用して, RAS 相当の機能を実現することができるので, その導入コストおよびランニングコストを削減することができる. 図 1 の例では, 移動端末に, VPN の Client としての機能を提供するソフトウェアを組み込み, 企業 LAN の SGW との間に VPN を設置している.

2．3　IPSec の概要

インターネット VPN プロトコルの一例として,

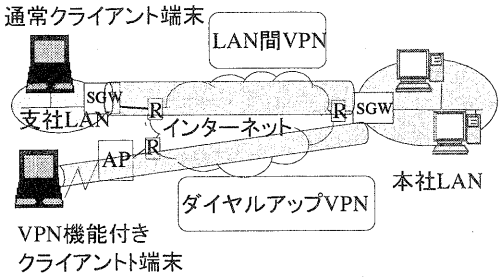

図 1　VPN の形態

現在最も有力なプロトコルの一つである IPSec（IP Security）について概説する. IPSec は, IP 層における VPN プロトコルであり, IP パケットに対して, カプセル化, 暗号化, 認証情報の付与等を行うセキュリティ重視型の VPN プロトコルである. 現在まで, IPSec バージョン 1（RFC1825-1829）[1][2], とバージョン 2（RFC2401-2410,2412,2451）が規定されており, それぞれ IPv4 と IPv6 の双方に対応している. 以下に, IPSec の主要な技術要件について概説する.

（1）IP パケットのカプセル化

図 2 (a)に示す様に, オリジナルの IP パケット（この場合ローカルアドレス）を新しい IP パケット（この場合グローバルアドレス）でカプセル化する.

（2）IP パケットの暗号化, 認証情報の付与

IPSec では, ESP と, AH という 2 つのモードを規定している.

・ESP：IP Encapsulating Security Payload

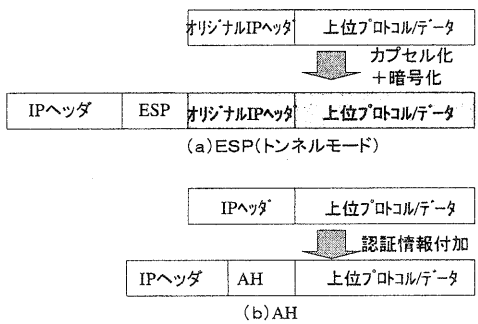

図 2　IPSec のパケットフォーマット

機密性を提供するため，IPパケットの暗号化機能を提供する．また，カプセル化された（ローカル）IPヘッダも暗号化されるので，弱い秘匿性も提供する．また，AHとの併用で完全性も提供する．

・AH: IP Authentication Header

ハッシュ関数を利用して，パケットの送信者の認証，完全性の検証を行う．

（3）SA（Security Association）

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を格納する．宛先IPアドレスと，擬似乱数値（Security Parameter Index）により管理される．また，SAは単方向であり，双方向通信を行うためには，2つのSAを必要とする．

（4）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のサンプルデータがあれば，一定の時間をかければ解読できることが実証されている[6]．より長い鍵の共通鍵暗号方式も提案されているが，その分大きい処理能力を必要とするので，実用的ではない．これらより，通信を行う両者間では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 1では，自動鍵交換と手動鍵交換を実装することのみを規定しており，自動鍵交換のプロトコルに関しては，本来規定していない．しかしながら，現在市販されている多くのIPSec対応製品は，IPSec2で標準になっている鍵交換アルゴリズムであるIKE[7]（ISAKMP/Oakley）を自動鍵交換アルゴリズムとしてサポートしている．

3．モバイル向けVPNの要件

3．1　パケット通信方式の特性

（1）概要

パケット通信方式は，複数の端末が無線回線を共有する方式であり，インターネットアクセス等のように間欠的にトラフィックが生じる様なデータ通信において特に利用効率の高い方式である[8]．

（2）通信速度

IMT-2000では，384kbpsベストエフォート型パケット通信のサービスが提供予定であり，これがデータ通信の主流になると見込まれている．現状ではパケット通信として，ディジタル携帯電話の無線方式であるPDC方式をベースとしたPDC-P方式によって，最大28．8kbpsおよび9．6kbpsのパケット通信サービスが提供されている．

（3）課金方式

PHS，PDC等のような回線交換方式が，通信時間に比例した課金方式を取っているのに対し，現状では，パケット通信方式は，通信時間や距離とは無関係に，データ量従量制課金方式がとられる．

（4）IPアドレス管理方式

ClientのPCに付与するIPアドレスに関しては，移動機対応に固定のIPを割り当てるスタティックアサイン方式と，テンポラリなIPアドレスを付与するダイナミックアサイン方式が存在する[9]．パケット通信によりISPにアクセスする場合は一般にはダイナミックアサイン方式が用いられる．

3．2　モバイル特有の要因

我々は，モバイル向けVPNを，”移動通信を介しても快適に利用可能でかつ処理能力の高くないハードウェア上でも実現可能なVPNプロトコル”と定義する．以下これを実現するための要件を説明する．

（1）VPN形態

モバイルコンピューティングの形態は現在主として，ノートPC，PDAなどの携帯端末を持ち歩くユーザが，出先で企業LANのメール等各種Serverにアクセスする等の用途に使用するというのが一般であり，VPN形態としては，ダイヤルアップVPNに相当する．一方，企業LAN自体が本社LANと支社LANの間でLAN間VPNを設置する場合もあり，これら両形態のVPNを併用可能であることが望まれる．

（2）通信経路

通常の回線交換，パケット通信，PIAFS等，様々な方式が混在しており，IMT-2000サービス開始後もこの状況は当面続くと思われる，これら移動通信方式に，固定通信等を含めた中からコスト／スループット／接続性等の観点から最適なものをユーザは選択すると考えられる．同様に，インターネットへの接続ポイントもユーザは上記観点から最適なものを選択すると考えられる．

（3）通信品質の不安定性

移動端末は，その時々の電波状態や輻輳によって，スループットが著しく低下したり，また場合によっては，まったく通信が不可能になる場合がある．通常のインターネットにおいても，一時的な輻輳により，通信が困難になることは一般的であるが，移動体通信の問題で通信が困難になった場合には，ISPへのPPPコネクション自体が切断されてしまうという点が異なる．この場合，再認証，再接続を行い，

また，場合によっては，ISPから割り当てられているIPアドレス自体が変わってしまうという点で，通信中断によるペナルティはより重大となる．

（4）ClientとServerの処理能力の低さ

現在，携帯移動端末は，ノートPC,ハンドヘルドPC，PDA，メール専用端末，など様々な用途に用いられている．これら携帯移動端末は一部のものを除けば，デスクトップPCに比較すれば，大幅に性能が劣るプロセッサを利用している．加えて，導入コストを押さえるためには，SGW機能をルータ等に縮退することが必須であると考えられるが，一般に小規模企業ユーザを対象としたSOHOルータの場合，やはりPCのプロセッサに比較すれば大幅に性能が劣るものが使用されていることが多い．

3．3　モバイル向けVPNの要件

前節より，移動端末を利用したモバイルコンピューティングの特徴を考慮すると，モバイル向けVPNの要件として以下の点が挙げられる．

（1）VPN形態

ダイヤルアップ型，LAN間型双方のVPN形態を実現可能であること．

（2）VPN終端方式

モバイル向けVPNにおいては，前節（2）で述べたように通信経路に依存しないことが必要とされる．

一般のダイヤルアップVPNのモデルには，ISPアクセスポイントにVPN終端装置を設置するセンタ型と，エンドユーザ側でソフト／ハードのVPN終端装置を設置するエンドーエンド型がある．センタ型でVPNを利用するためには，移動中および移動前後に使用しうる全てのISPアクセスポイント，およびパケット通信を利用している場合はパケット通信網におけるPPP終端機能を提供している部分に当該VPN終端機能を提供する必要があり，これは実現困難である．したがってエンドーエンド型が適していると考える．

（3）セッション管理

一般に，VPNを設定する際には，IPアドレス等通信を行うのに必要な情報や，セキュリティポリシ等をお互いに交換し管理する必要がある．以下，この関係をVPNセッションと呼ぶ．

ここで，エンドーエンド型ダイヤルアップVPNを考える．Clientは移動網またはISPとPPP接続した時にIPアドレスをダイナミックアサインされ，このIPアドレスをもってSGW側にVPNセッションの確立を要求する．このVPNセション確立後に，移動網の不安定性により，VPNセッション終了の正常な手続きを経ずにPPP接続が切断された場合を考える．Client側はISPへの接続が切断されたことから，VPNセッションも利用不可能であることを直ちに認識できるが，この状態をSGWに通知するシーケンスが存在しないと，SGW側にいつまでもVPNセッションの塵が残り，結果SGWのメモリ資源を圧迫する．

上位のプロトコルのシーケンスが起動していれば，SGWは間接的にこの状態を知ることができるが，それ以外の場合に，SGW側でVPNセッション情報を削除する契機が無い．これらより，SGW側の資源管理上の問題が生じるのみではなく，Clientが再度PPP接続し，前回とは異なるIPアドレスをアサインされ，当該IPアドレスをもって，SGW側にVPNセッションの再設定を要求した場合におけるセッション管理法などが問題となる．

この問題を回避するための一般的な方法として，SGW，Client間でVPNセッションの状態を管理するためのキープアライブパケットの交換が行われている．図3にその一例を示す．SGWは，周期T毎に，Clientに対して，状態確認パケットを送信する．Clientは，そのパケットを受信したらただちに，返信する．SGWは，Clientから，規定時間t以内に返信パケットを受信したら，Clientは正常であると認識し，VPNセッションを維持する．もし，t以内に返信を受け取らなかったら，ClientはVPNセッションを終了したものと判断し，SGWは当該VPNセッション情報を削除する．

このように，ユーザが直接意識しないパケットがVPNセッションを維持するために送受されることは，新たに以下の問題を引き起こす．

- 通信品質の不安定性に基づく誤ったVPNセッション削除
- 周期的なキープアライブパケットへの課金

特に後者の場合，データ量従量制課金のパケット通信に時間課金的要素が加わり，ユーザにとっての利点が減少する．また，この比率を少なくするために，周期Tを長くするという対策をとると，Clientが一時的な問題により接続を切断された後，再接続をこころみても最大Tの間再接続を拒絶されるという問題が発生する．これら問題を解決するために，パケットの送受を行わないVPNセッションの管理方式が必要となる．

（4）プロセッサ負荷

モバイル向けVPNプロトコルは安価なプロセッ

サでも十分に実現できる程度に，プロセッサ負荷の軽いものである必要がある．一般に，プロセッサ負荷の圧迫要因は以下の様に分解することができる．

- パケット数比例分　主としてパケット暗号化処理に必要なプロセッサ負荷
- 鍵交換による分　共通鍵暗号を利用して暗号通信を行うためには，通信を行う者同志で鍵交換処理を行う必要がある．この処理のための負荷

我々の実験によればパケット数比例分は，移動端末側および，小規模LANではSGW側のインターネット接続点のスループットがボトルネックとなり送受されるパケット数が制限されることから，大きな問題にならないことが明らかになった．これに対して，鍵交換による分はこのボトルネックとは無関係に，SGWに結合されているユーザ数に比例して多くなる．加えて，前節の通信品質の不安定性を考慮すると，再設定に伴う新たな鍵交換処理などが頻発する．

先述の鍵交換アルゴリズムIKEでは，Diffie-Hellman[10]の鍵交換アルゴリズムをベースとしているため，膨大な計算量が必要になり，SOHO向けなど小規模ルータに搭載されているようなプロセッサでは，過負荷が生じる．このため，軽量な鍵交換アルゴリズムの実装が必要になる．

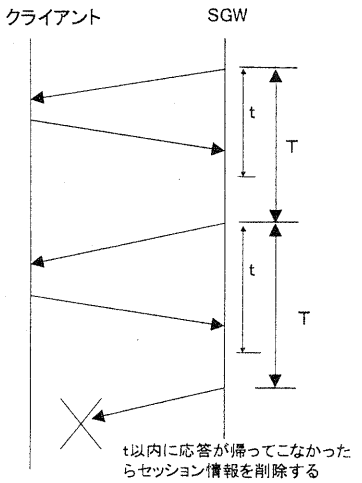

図3キープアライブの例

4．モバイル向けVPNの方式検討

前章で述べた要件より，モバイル向けVPNプロトコルの詳細について検討する．

4．1　ベースプロトコルの選択

現在すでにRFC化が行われている，あるいは近々行われる予定があるVPNプロトコルを，前章の各要件および一般的にVPNに求められる要件から比較した結果を表1に示す．セキュリティ機能が豊富なこと，VPN形態および，VPN終端方式の点で，我々の要求条件を満たしていることから，IPsecをプロトコルのベースとして検討することとした．また，IPSecの問題点として挙げられる，キープアライブ，プロセッサ負荷の点に関して改良を加えることとした．

4．2　IPSecのバージョン

ベースとするIPSecのバージョン／モードについて以下に規定する．

・IPSecバージョン1　(RFC1825-1829)

現状評価に使用できるIPSecバージョン2サポート製品が少ないため，バージョン1を使用する．

・IPv4版

当面IPv6が急激に普及する見込みが無いためIPv4版を前提とする．

・トンネルモード

IPSecには，IPパケットのIPパケットへのカプセル化を行うトンネルモードと，行わないトランスポートモードに分けられる．VPN機能があるのは，トンネルモードであるためトンネルモードを使用する．

4．3　モバイル向きVPNセッション管理方法の提案

キープアライブパケットの送受は行わずに，SGWで資源が不足した時点で以下のシーケンスを起動することによりVPNセッション情報の更新を行う．

表1　ベースプロトコルの選択

要件		L2TP	IPSec
一般的な要件	ﾄﾝﾈﾘﾝｸﾞ ﾚｲﾔ	ﾚｲﾔ2 (PPP)	ﾚｲﾔ3(IP)
	ｾｷｭﾘﾃｨ	認証	暗号，認証等
	ｺｽﾄ	導入時＋利用料	導入時
ﾓﾊﾞｲﾙ向け要件	VPN形態	ﾀﾞｲﾔﾙｱｯﾌﾟ	LAN間ﾀﾞｲﾔﾙｱｯﾌﾟ
	VPN終端方式	ISP内又はISP-ｴﾝﾄﾞ	ｴﾝﾄﾞ-ｴﾝﾄﾞ
	ｷｰﾌﾟｱﾗｲﾌﾞ	問題無し	対策必要
	ﾌﾟﾛｾｯｻ負荷	問題無し	対策必要

（1）Client から，VPN セッション設定要求があり，VPN セッション情報を作成する（セッション数が制限一杯になる）．
（2）他の Client から，VPN セッション設定要求があり，資源が不足する．
（3）以下に示す２種類のアルゴリズムのいずれかにより，廃棄してよい可能性が高い VPN セッションを選択する

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

当該 VPN セッションに状態確認パケットを送信し現在の状態を確認する．
（4）当該 VPN セッションに関して，Client 側から応答が無ければ，当該 VPN セッション情報を削除，資源を解放する．
（5）当該 VPN セッションから応答があれば，それを廃棄候補の最後尾に再配置し，（3）の処理を続ける．

これにより，３．３節（3）のセッション管理の問題点を解決する．また，削除する場合は無効になっている可能性が高い VPN セッションから順次確認しつつ，削除していくため，削除ミスの可能性を極めて小さくすることができる．また，Client が登録してある VPN セッション情報とは異なる 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 VPN セッション情報を新しい VPN セッション情報で上書きする．これにより，VPN セッション管理上の問題を解決することができる．また，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．

４．４　軽量鍵交換アルゴリズムの提案

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することが極めて困難であること．
（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こと．
（3）鍵交換は鍵交換時点での Client，SGW 双方の合意に基づいて行い，いずれの側も鍵の更新値を一方的に決定することが可能であってはならない．

これら要件を満たし，かつ計算量の少ない鍵交換方式を検討した．これを図４に示す．本方式は，Client，SGW 双方で事前に秘密の情報，S_1, S_2 を共有し，これに，一方向性を有するハッシュ関数を交互に適用することによって，新しい鍵を生成する．さらに，上述の鍵交換の要件（2）を満たすため，ハッシュの一方向性を利用している．また，S_1, S_2 は暗号通信を行う２者以外には絶対に知られないことを前提とする．

本アルゴリズムは２つのフェーズから構成される．
（フェーズ１）Client－SGW 間でハッシュの更新値を合意するフェーズ
(1-1)Client，SGW 双方独立にそれぞれ乱数 n_{11}，n_{12} を発生する．
(1-2)SGW は自身が発生した乱数 n_{12} に，Client，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（n_{12})を Client に送る．
(1-3)上記ハッシュ値を受け取ったら Client は自身が発生した乱数 n_{11} を平文で SGW に送る．
(1-4)SGW は，n_{11} を受け取ったら，n_{12} を平文で Client 送る．
(1-5)Client は，n_{12} にハッシュ関数を適用し，(1-2)で取得した値と比較し，一致すれば n_{11} と n_{12} に事前に合意した論理演算を適用し，更新値 n_1 を計算しフェーズ２に入る．
(1-6) SGW は(1-3)で取得した n_{11} と自身で発生させた n_{12} から，事前に Client，SGW 間で合意していた論理演算を適用し，鍵の更新値 n_1 を計算し，フェーズ２に入る．

フェーズ１は上述の鍵交換の要件（3）を満たすため，どちらか一方があらかじめ全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．
（フェーズ２）ハッシュ更新値から，鍵を計算するフェーズ
(2-1) Client，SGW 双方で，S1 を入力値とし，フェーズ１で合意した更新値 n_1 回ハッシュ関数の計算を繰り返し（これを $K_1=Hn_1(S_1)$ と表す）１回目の共有鍵 K_1 を生成する．
(2-2)次に鍵交換周期が来た時には，両者間で新たにフェーズ１を起動して新しい更新値 n_2 を合意した後，以下の計算を行う．

$K_2=Hn_2(Hn_1\text{-}1(S_1), S_2)$

以下

$K_3=Hn_3(Hn_2\text{-}1, S_1)$

$K_4=Hn_4(Hn_3\text{-}1, S_2)$

……

と鍵交換を続ける．

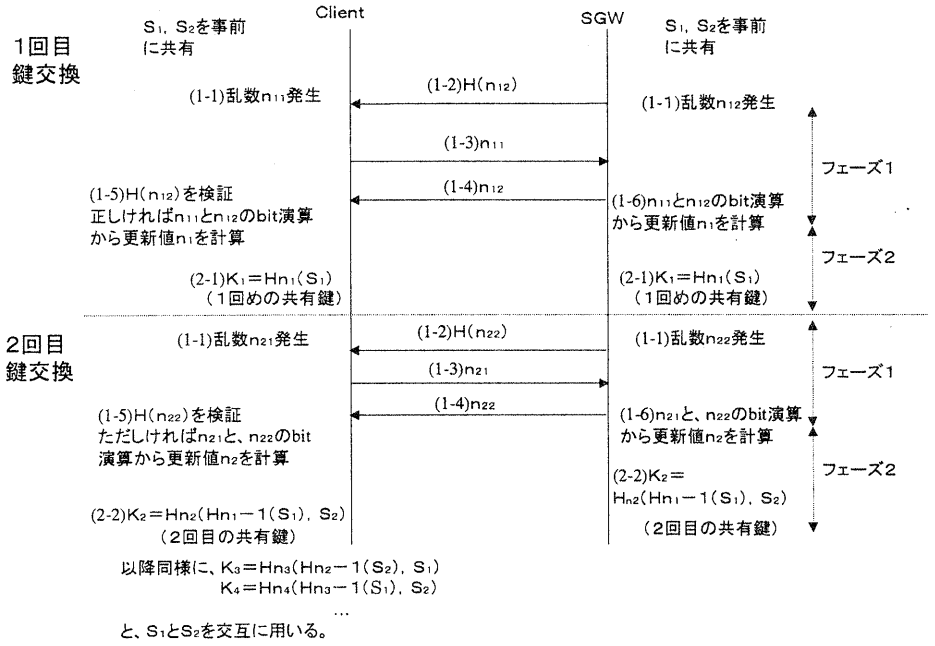

図4　提案する鍵交換アルゴリズム

秘密情報S_1, S_2を交互に使う理由は，例えば1つの秘密情報Sを使い続けて同様のやりかたを行うと，前の鍵に有限回数ハッシュを適用したものが次の鍵に等しくなり，(K_{n+1}=Hm (K_n)，mは有限整数) 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．2つの秘密情報S_1，S_2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無く，1つ前のハッシュ値を入力値にするため，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できる．

5．まとめと今後の課題

モバイル向けVPNプロトコルの満たすべき要件を抽出した．ただし，IPSecを利用した場合には，無線区間上をVPN維持のためのパケットが通ること，鍵交換処理の負荷が著しく大きくなることが問題となるため，これらに対する解決策として，パケット送受を伴わないVPNセッション管理方式，軽量鍵交換アルゴリズムを提案した．

今後，実際に本方式の評価を行う予定である．

参　考　文　献

[1]R. Atkinson, "Security Architecture for the Internet Protocol, "RFC 1825, Aug. 1995.
[2]R. Atkinson, "IP Authentication Header, "RFC 1826, Aug. 1995.
[3]R. Atkinson, "IP Encapsulating Security Payload (ESP),"RFC 1827, Aug. 1995.
[4]P. Metzger, W. Simpson, "IP Authentication using Keyed MD5,"RFC 1828, Aug. 1995.
[5]P. Karn, P. Metzger, W. Simpson, "The ESP DES-CBC Transform," RFC1829, Aug. 1995.
[6] Electric Frontier Foundation, Cracking DES, O' REILLY, May, 1998.
[7]D. Harkins, D. Carrel, "The Internet Key Exchange (IKE),"RFC2409, Nov. 1998.
[8]移動パケット通信システム特集, NTT DoCoMo テクニカルジャーナル, Vol.5, No.2. Jul. 1997.
[9]中村他, "PDC移動パケット通信システムにおけるIPアドレスダイナミックアサイン方式の開発," NTT DoCoMo テクニカルジャーナル, Vol.5, No.3, Oct. 1997.
[10] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Inform. Theory, Nov. 1976.