GSCIP と IPsec を併用したリモートアクセス方式の提案

030432017　今村　圭佑

A Proposal of a Remote Access Method using GSCIP and IPsec

Keisuke Imamura

第 1 章　　序論

インターネットの普及に伴い, 企業業務においてネットワークの利用が必須となってきている. 無線アクセスポイントの普及や, 在宅勤務者の増加などの要因により, インターネット経由で社外から社内ネットワークへのアクセスが頻繁に行われている. しかしインターネット空間には，盗聴，改ざん，成りすましといった脅威が存在する. それらの脅威から通信を保護するために，VPN（Virtual Private Network）を構築してリモートアクセスを行う方法がよく利用されている．リモートアクセス VPN を構築する手段として，PPTP（Point-to-Point Tunneling Protocol）[1], L2TP（Layer 2 Tunneling Protocol）[2]，IPsec（Security Architecture for Internet Protocol）[3], SSL（Secure Socket Layer）[4]などの手法が挙げられる．PPTP、L2TP は，暗号化強度が低く企業ネットワークで使用する場合にはセキュリティ強度に問題がある. そのため，近年よく利用される VPN 構築手法として，IPsec や SSL が注目されている．IPsec は，通信開始時に IKE（Internet Key Exchange）[5]を行い，お互いに共通暗号鍵を所持することで暗号化通信を可能にしている．しかし，IPsec は設定項目が多くユーザが増加すると管理が煩雑になる．また，SSL はトランスポート層とセッション層の間に実装されていることからアプリケーション限定されるといった課題が存在する. また両方式ともセキュリティを End-to-End で保護していない. 内部犯罪の増加で，盗聴，改ざん，成りすましといった脅威はイントラネット内にも存在する．そこで，我々は, イントラネットのセキュリティを確保しつつ，管理負荷の低減を目的として，GSCIP（Grouping for Secure Communication for IP；ジースキップ）[6]を検討している．本稿では，インターネット空間でセキュリティを確保する IPsec と GSCIP を組み合わせることで, 任意のアプリケーションが利用可能でかつ，End-to-End でセキュアな通信を可能としたリモートアクセス方式の提案を行う.

第 2 章　　既存技術とその問題

既存の VPN 構築方法として，PPTP，L2TP，IPsec，SSL などの手法が挙げられる．PPTP とは，リモートアクセス用に設計されたプロトコル PPP（Point-to-Point Protocol）を拡張した技術で，PPP パケットを IP データグラムでカプセル化し，インターネット上を転送可能にするプロトコルである．しかし，PPTP は暗号化強度が低く企業ネットワークで使用する場合にはセキュリティ強度に問題がある．L2TP は，インターネットなどの公衆回線網上に仮想的にトンネルを生成し，そこを通じて PPP 接続を確立することにより，VPN を構築するためのプロトコルである．L2TP も同様にセキュリティ強度の問題がある．そこで近年はリモートアクセス VPN の手段として IPsec と SSL が良く利用されている．以下 2.1 と 2.2 で IPsec と SSL を説明する．

2.1　IPsec-VPN

IPsec は，TCP/IP 上において，汎用的に利用できるセキュリティ・プロトコルである．ネットワーク層（第 3 層）に実装されており，IETF（Internet Engineering Task Force）で標準化されている．現在では VPN を構築するためによく利用されており，IPv6 では標準サポートされている．IPsec は，AH（Authentication Header）[7]と ESP（Encapsulating Security Payload）[8]の 2 つのプロトコルからなり，AH は，IP パケットの改ざんを防止するための機能を持つプロトコルである．ESP は，IP パケットの改ざん検出に加え，機密性を確保するための機能を持つプロトコルである．IPsec と共に使用されるプロトコルとして，IKE が存在する．IKE はアルゴリズムの種類や鍵などの情報を交換するプロトコルである．

図 1 に一般的な IPsec を利用したリモートアクセスの構成を示す．通常ゲートウェイ（以下 GW）に IPsec-VPN 装置を設置し，リモート端末は IPsec-VPN 装置に対し IKE を実行し，IPsec SA（Security Association）構築する．以後，社内 LAN 宛てのパケットは ESP 化される．

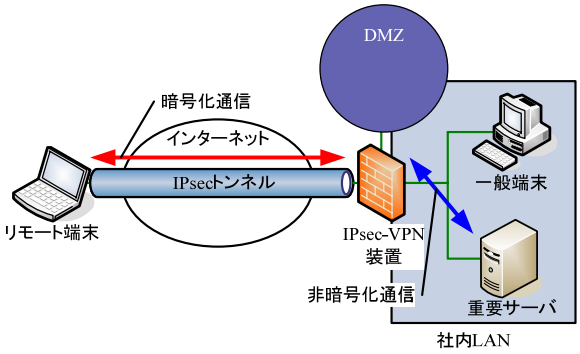

図 1：IPsec を利用したリモートアクセス

社内 LAN で使用する内部ネットワーク情報をリモートアクセス端末に自動設定する仕組みとして，多くの IPsec-VPN 装置で IKE を拡張した mode-cfg（IKE-CFG）[9]が利用されている．mode-cfg を使用することで，社内 LAN に関するネットワーク情報をリモートアクセス端末に通知し，社内 LAN へ接続できるようになる．ユーザ認証機能として，ワンタイムパスワードやチャレンジレスポンスなどの PKI を使用しないレガシー認証システムが多く利用されている．しかし，IKE はこういった認証システムを利用する機能を持たない．したがって，相手認証には，IKE を拡張した XAUTH（Extended Authenticati on within IKE）が利用されている．XAUTH では，通常のパスワードによる認証のほか，RADIUS（Remote Authentication Dial In User Service）[10]，CHAP（Challenge Handshake Authentication Protocol）

および，OTP（One-Time Password Authentication System）[11]などの認証方式を利用できる．

IPsec を用いたリモートアクセス VPN の問題点として，End-to-End セキュア通信を確保しにくい点と管理負荷が高いという 2 点がある．通常 IPsec を用いたリモートアクセスでは，VPN 装置に対し IPsec トンネルを構築するので，VPN 装置と社内 LAN の端末間は暗号化通信を行わない．End-to-End のセキュリティを確保する方法として IPsec トランスポートモードが存在するが，UDP カプセル化より，IPsec が持つセキュリティレベルを確保できないといった問題がある．

2.2 SSL-VPN

SSL は公開鍵暗号や秘密鍵暗号，デジタル証明書，ハッシュ関数などのセキュリティ技術を組み合わせ，データの盗聴や改ざん，なりすましを防ぐことが可能である．セッション層（第 5 層）とトランスポート層（第 4 層）の境界で動作し，HTTP や FTP などの上位のプロトコルを利用するアプリケーションソフトからは，特に意識することなく透過的に利用できる．

SSL-VPN とは，暗号化に SSL を利用する VPN 技術である．多くの Web ブラウザやメールソフトは標準で SSL に対応しており，リモートアクセスに利用できる．図 2 に SSL を利用したリモートアクセスの構成を示す．

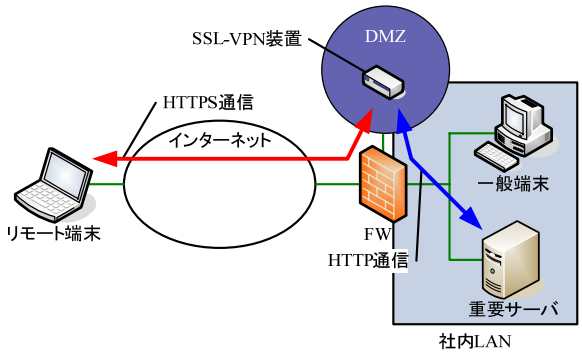

図 2：SSL を用いたリモートアクセス

SSL を利用してリモートアクセス VPN を構築する際は，通常 DMZ（DeMilitarized Zone）に SSL-VPN サーバを設置し，リモート端末は Web ブラウザを使用して SSL-VPN サーバにアクセスする．ユーザ認証をパスすると，そのユーザが利用できるリソースへのリンクが表示される．ユーザが利用できるリソースには，Web ベースのアプリケーション以外に，FTP や Windows ファイル共有などを利用するアプリケーションも含まれる．ユーザがリンクを選択すると，SSL-VPN サーバは該当する内部サーバに対して，それぞれのアプリケーションプロトコルを使用してアクセスする．その後，得られた結果を HTTP に変換してクライアントに転送する．リモート端末と SSL-VPN サーバの間は HTTPS が用いられるため，セキュリティが確保される．この方式では，クライアントは Web ブラウザだけを使用すればよく，手軽に VPN を利用できるというメリットがある．しかし，SSL-VPN サーバ上でプロトコル変換機能が必要であるため，利用できるアプリケーションが限られる．特に，UDP を使用するアプリケーションや動的な TCP ポートを使用するアプリケーション，複数の TCP セッションを使用するアプリケーションが利用できない．在宅勤務などでは，通常の企業業務で使用しているアプリケーションをそのまま利用したい要求があり，このような用途では利用できない．

第 3 章　　提案方式

3.1　提案方式の目的

イントラネットでは，認証は ID，パスワードだけに頼るなど脆弱である. また暗号化通信は，通常行われていない．しかし，盗聴，改ざん, 成りすましといった脅威はイントラネット内にも存在し, 近年内部犯罪の増加が懸念されている．認証，暗号化通信を可能にする技術として IPsec がある．しかし，IPsec はトンネルモード, トランスポートモードに互換性がない. また, 通信系路上のすべてにセキュリティポリシの設定を行わなければならない. 上記のような理由により, イントラネットのセキュリティを IPsec で確保するとユーザ数増加により管理負荷が増大する．そこで我々は，管理負荷の低減とセキュリティを兼ね備えた通信アーキテクチャ GSCIP を検討している．

また, IPsec を用いたリモートアクセスでは，トンネルモードを使用するためリモート拠点から GW である IPsec-VPN 装置間の暗号化しか行っていない. End-to-End で暗号化を可能にする技術としてトランスポートモードが存在するが，UDP カプセル化を行うため本来の IPsec のセキュリティ強度が得られないといった問題がある．そこで，GSCIP と組み合わせることでイントラネット内の暗号化を実現し，End-to-End でセキュア通信を可能とする．3.2 にグループ通信方式 GSCIP の原理を説明する．

3.2　GSCIP の原理

GSCIP とは柔軟性とセキュリティを兼ね備えたネットワークセキュリティアーキテクチャである．図 3 に GSCIP のグルーピングの原理を示す．GSCIP における通信グループの構成要素を GE(GSCIP Element)と呼ぶ．GE には端末にソフトウェアをインストールして実現するホストタイプの GES（GE realized by Software），ルータに機能を実装したルータタイプの GEN（GE for Network），重要なサーバの直前に設置して，GES と同じ役割を果たすブリッジタイプの GEA（GE realized by Adapter）の 3 種類がある．GEN の配下に存在する一般端末は，GEN により一括して保護される．GSCIP では，同一の共通暗号鍵を所持する GE の集合を同一の通信グループとして定義する．この共通暗号鍵をグループ鍵 GK（Group Key）と呼ぶ．GK を通信グループと一対一で対応させることにより IP アドレスに依存しない通信グループを構成することが可能となる．同一の通信グループ間の通信は，GK により暗号化される．GE には動作モードが定義されており, 同一通信グループに帰属しない端末との通信を一切禁止する閉域モード CL（Closed Mode）と，異なる通信グループの端末とは平文での通信が可能な開放モード OP（Open Mode）がある．一般に GEN，GEA およびサーバとして使用する GES には閉域モードが定義され，クライアントとして使用する GES には開放モードが定義される．図 3 では GEA はグループ 2 に所属しており，グループ外の GES3 からのアクセスを拒否することが可能となる．通信グループは，管理装置 GMS(Group Management Server)で定義し, GMS から各 GE へグループ情報とそれに対応する GK を配送する．この際，公開鍵を用いた確実な認証が行われる. GK は定期的に更新される．

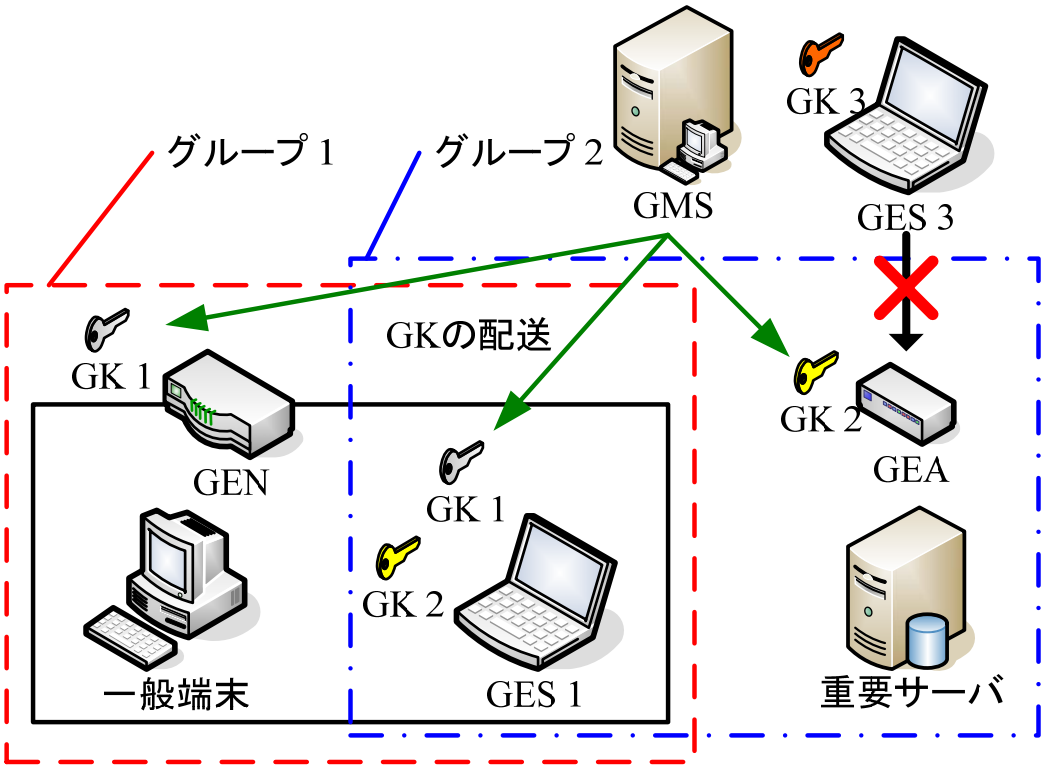

図 3：GSCIP におけるグルーピングの原理

3.3 DPRP の概要

各 GE は，自身が保持する動作処理テーブル PIT(Process Information Table)に従いパケットの処理を行う．PIT には送信先/宛先の IP アドレス，ポート番号，プロトコルタイプと，これらに一致するパケットの処理内容を規定した動作処理情報（暗号化/復号/透過中継/破棄），およびグループ鍵の識別情報が記述されている．PIT の検索には通信パケットの送信元/宛先 IP アドレス，ポート番号，およびプロトコルタイプの組を用いる．これらの情報を CID（Connection Identification)と呼ぶ．該当する PIT が存在しない場合には，送信パケットを一時的に退避し，動作処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）[14]を用いて PIT を動的に生成する．一般に DPRP は端末間の通信に先立ち実行される．

図 4 に DPRP のシーケンス図を示す．DPRP には，ICMP をベースとした DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）という 4 つの制御パケットを用いる．DDE には，DPRP のトリガーとなった通信パケットの CID がセットされ，通信パケットの宛先へ送信する．DDE を受信した GES2 が終点 GE となり，RGI を生成する．RGI には，GE のユーザ ID，動作モード，グループ鍵情報などの設定情報，および GE を認証するために用いる識別子（以下 aID）がセットされる．RGI は宛先を CID に記載されている送信元 IP アドレス「PA1」として送信される．中間 GE が RGI を転送する際，始点 GE と同様に自身の設定情報などをパケットに追加していく．RGI を受信した GES1 が始点 GE となり，収集した情報から各 GE の動作処理情報を決定する．GES1 は決定した動作処理情報を MPIT にセットして終点 GE，即ち GES2 へ送信する．MPIT を受信した GEN,

GES2 は動作処理情報から自身に関する動作処理情報を取り出し，aID を用いた認証処理後に PIT を生成する．GES2 は PIT 生成後，DPRP ネゴシエーションの完了を通知するために CDN を生成し，始点 GE，即ち GES1 へ送信する．CDN を受信した GES1 は待避していた通信パケットを元に戻し，生成された PIT に基づいて通信が開始される．

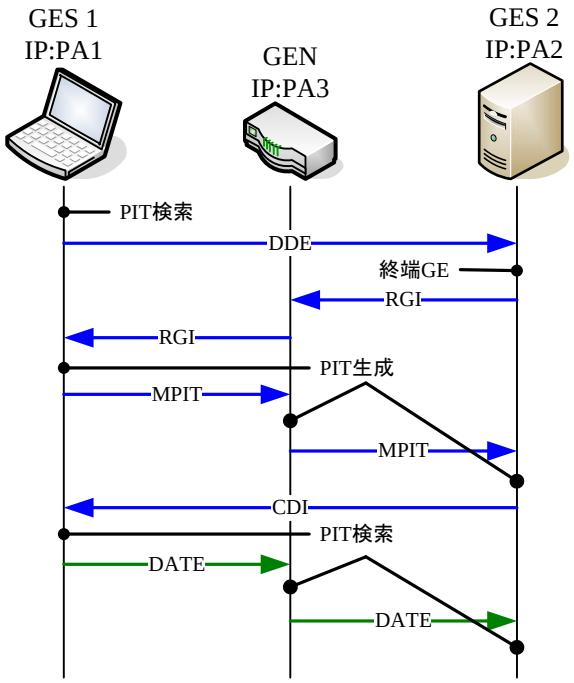

図 4：DPRP ネゴシエーション

3.4　提案方式のよるリモートアクセス

図 5 に GSCIP と IPsec を併用したリモートアクセス方式の構成を示す．まず，リモート GES は IPsec-VPN に対して IKE を実行し IPsec トンネルの構築を行う．その後リモート GES は鍵管理サーバ GMS に対してグループ鍵配送依頼を行う．GMS とリモート GES 間は公開鍵認証によって確実に認証され，該当するグループ情報とそれに対する GK が各 GES に配送される．グループ鍵が配送された後は，DPRP によって PIT が生成され，PIT に従った通信が開始される．

以上の手続きにより，リモート GES は社内 LAN に存在する GE と同様グループに取り込まれ End-to-End のセキュア通信が可能となる．

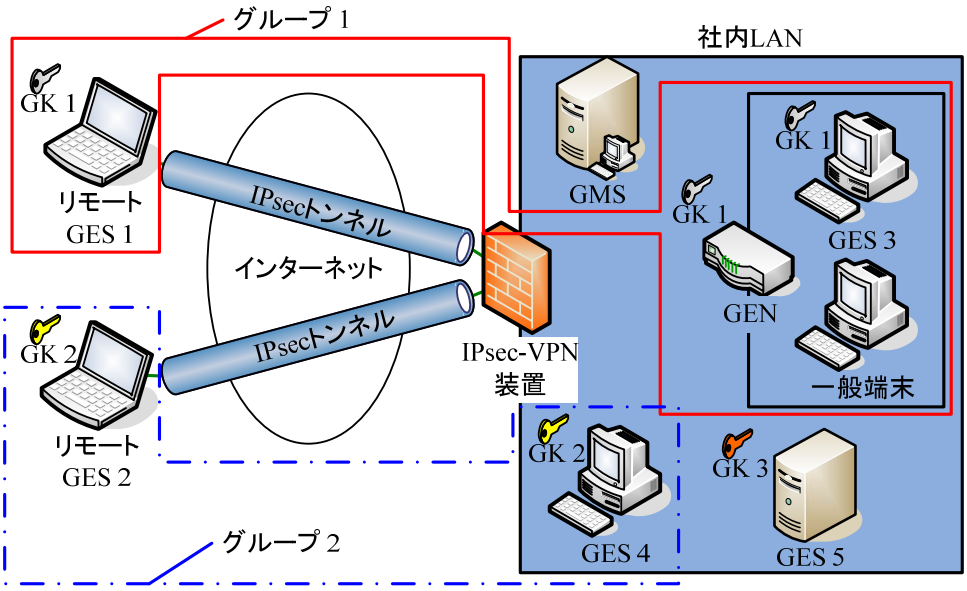

図 5：GSCIP と IPsec を併用したリモートアクセス方式

第 4 章　　評価

表 1 に既存技術と提案方式の比較を行った．IPsec を用いたリモートアクセスは，リモート端末から VPN 装置である GW までの暗号化でありイントラネット内のセキュリティの脆弱性が存在する．End-to-End で IPsec を構築する方法として IPsec トランスポートモードがあるが，UDP カプセル化によるセキュリティ強度の低下が懸念される．また，SSL はセッション層とトランスポート層の間に実装されていることから任意のアプリケーションが利用できないという問題が存在する．しかし，提案方式では GSCIP によってイントラネット内の暗号化通信を可能にしつつ，DPRP による動的に設定することで管理負荷の低減を可能にしている．また，GSCIP は IP 層に実装されているため任意のアプリケーションが利用可能である．

表 1：既存技術と提案方式の比較

	IPsec トンネルモード	SSL-VPN	提案方式
End-to-End 暗号化	× End-to-GW	× End-to-GW	○ End-to-End
利用可能なアプリケーション	○ 任意のアプリケーション	× アプリケーションが限定される	○ 任意のアプリケーション
管理負荷	○ トンネル構築の設定のみ	△ きめ細かい設定は可能であるが管理負荷が増大	△ GK の配送後，動的にポリシーの設定を行う

第 5 章　　まとめ

本論文では，GSCIP と IPsec を併用したリモートアクセス方式の提案を行った．IPsec のみによるリモートアクセスに比べ管理負荷増加を抑えつつ End-to-End セキュア通信が可能となる．今後は実装を行い，性能測定と実運用を試みる．

参考文献

[1] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn, “Point-to-Point Tunneling Protocol (PPTP)”RFC2637, IETF, July. 1999.

[2] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn and B. Palter,“Layer Two Tunneling Protocol "L2TP"”RFC2661, IETF, August. 1999.

[3] S. Kent and K. Seo,“Security Architecture for the Internet Protocol”RFC4301, IETF,

December. 2005.
[4] T. Dierks and C. Allen,“The TLS Protocol, Version 1.0”RFC2246, IETF, Jan. 1999.
[5] D. Harkins and D. Carrel,“The Internet Key Exchange (IKE)”RFC2409, IETF, Nov. 1998.
[6] 鈴木 秀和，竹内 元規，加藤 尚樹，増田 真也，渡邊 晃：フレキシブルプライベートネットワークを実現するセキュア通信アーキテクチャ GSCIP の提案，マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム論文集，Vol.2005，No.6，pp.441-444，Jul.2005.
[7] S. Kent,“IP Authentication Header”RFC4302, IETF, December. 2005.
[8] S. Kent,“IP Encapsulating Security Payload (ESP)”RFC4303, IETF, December. 2005.
[9] D. Dukes and R. Pereira,“The ISAKMP Configuration Method”Internet Draft, IETF, September. 2001.
draft-dukes-ike-mode-cfg-02.txt
[10] C. Rigney, A. Rubens, W. Simpson and S. Willens,“Remote Authentication Dial In User Service (RADIUS)”RFC2138, IETF, April. 1997.
[11] N. Haller, C. Metz, P. Nesser and M. Straw,“A One-Time Password System”RFC2289, IETF, February. 1998.
[12] 鈴木 秀和，渡邊 晃：フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の実装と評価，情報処理学会論文誌，Vol.47，No.11，pp.2976-2991，Nov.2006.

謝辞

本研究を遂行するにあたり，多大なるご指導，ご鞭撻を賜りました渡邊晃教授に心より感謝します．また有益なご助言，ご検討いただきました渡邊研究室の学部生，学院生の皆様に深く感謝いたします.