GSCIP における構成要素 GEA の検討

佐本　章悟

Researches on GEA；an element of GSCIP

Shogo Samoto

第1章.　はじめに

今日ネットワーク技術の進歩に伴い，あらゆる物，人がいつでもどこからでもネットワークに接続できるユビキタスな社会が現実的になっており，それに伴うネットワークセキュリティの重要性も高まっている．特に重要な情報を扱う企業では情報の保安は必須である．しかし近年の企業ネットワークでは，外部からの不正侵入，データの盗聴や改竄，漏洩といった脅威がある．また企業内部にも脅威は存在し，内部関係者による不正も多く報告されている．外部からの脅威の対処は通信の暗号化，ディジタル署名などのセキュリティ技術の利用やそれらをファイアウォールと併用するなど，様々な工夫がなされている．内部のセキュリティ対策としては，ユーザ名とパスワードによる簡単な認証，アクセス制御程度しか行われていないのが現状であり，有効な対策が必要とされる．このような状況に対応するためのネットワークセキュリティの代表技術として IPsec がある[1]．IPsec では個人単位でセキュリティ機能を実現するトランスポートモード，ドメイン単位でセキュリティ機能を実現するトンネルモードがある．トランスポートモードは通信しあうエンド端末にセキュリティ機能を実装することで実現し，トンネルモードは通信経路上にセキュリティ機能を実装したセキュリティゲートウェイ（以下 SGW）を設置し，SGW 配下のサブネットを保護することで実現する．しかし両者には互換性が無く，端末が個人単位とドメイン単位に混在するような環境への対応は向いていない．逆に IPsec で混在環境を可能にするにはエンド端末にトランスポートモードとトンネルモードの両方の設定が必要であり，システム構成が頻繁に変化するような環境では管理負荷が膨大になるといった課題もある．このため IPsec は，イントラネット内ではほとんど利用されていない．そこで我々は新たなネットワークの概念として，FPN（Flexible Private Network）[2]と呼ぶシステムを提案している．FPN では柔軟かつセキュアな通信グループの構築を可能とするシステムを目標としている．また FPN を実現する新たな通信アーキテクチャとして GSCIP（Grouping for Secure Communication for IP）[3]を検討している．GSCIP では通信グループを形成する構成要素を GE（GSCIP Element）と呼び，現状で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），サブネットを構成するルータに適用するタイプの GEN（GE for Network）の 2 タイプの種類がある．GEN は配下に存在する一般端末を一括して保護することができる．しかし，各タイプの GE を既存のネットワーク体系に導入することは，既存の端末やルータに手を加える必要があり，容易ではない．この課題を解決するためブリッジタイプの GEA（GE realized by Adapter）について検討したので報告する．

以下，第 2 章で FPN と GSCIP，第 3 章で GEA の提案と動作，第 4 章で GEA の実装について述べ，第 5 章でまとめる．

第2章.　FPN と GSCIP

2.1. FPN の概要

FPN は柔軟性とセキュリティとを兼ね備えた新たなネットワークの概念である．FPN では個人単位とドメイン単位の通信が混在する環境に対しても，通信グループを定義することでセキュアな通信を可能とするシステムであり，また端末が移動しても通信の継続が可能とされる移動透過性も実現できるシステムである．FPN の概念を図示したものを図 1 に示す．

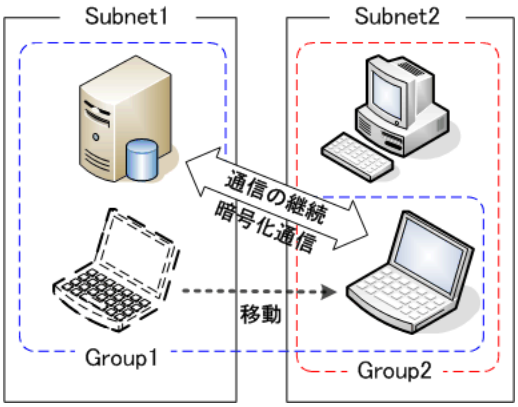

図 1　FPN の概要

同一通信グループ内の端末間通信は，通信グループごとに定義されている暗号鍵を用い暗号化し，異なる通信グループに属する端末からのアクセスは拒否することができる．通信の際に使用される暗号鍵は，通信開始時に自動的に生成されるため，複数のグループに帰属しているホストがいたとしてもグループの違いを意識することなく通信を継続することが可能である．

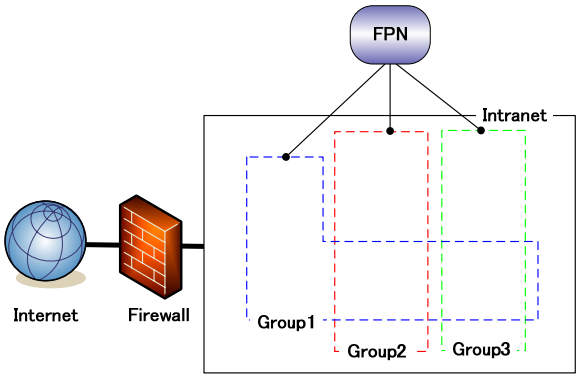

図 2　FPN の適用範囲：イントラネット

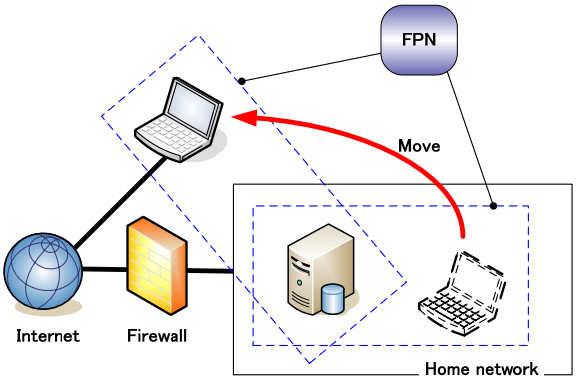

図 3　FPN の適用範囲：ホームネットワーク

FPN の適用範囲は図 2，図 3 に示すようにイントラネット内部，およびホームネットワークを含むインターネット上を想定している．前者ではインターネットとイントラネットの間に強固なファイアウォール（以下 FW）が存在しセキュリティポリシーが厳密なため，イントラネットをインターネット上まで適応することは想定していない．一方後者では，ホームネットワークとインターネットの間にホームネットワークを保護する FW は存在するが，前述したほどの強固な FW ではなく，ある程度の自由度を持たせた FW であると考えられ，インターネットの延長に近いと考えることができる．

2.2. GSCIP

FPN を実現するためには様々な方式があり得る．厳重なセキュリティを求めるのならば IPsec を用いればよいが，IPsec は FPN で要求される柔軟性に富んだ技術ではない．そこで我々は，FPN の概念を実現するための通信アーキテクチャとして GSCIP を提唱している．GSCIP は，一連の通信プロトコルの総称であり，システム構成が変化しても動的に動作処理情報を生成する DPRP（Dynamic Process Resolution Protocol）[4]，通信中に IP アドレスが変化した場合の処理を行う Mobile PPC（Mobile Peer-to-Peer Communication）[5]，NAT（Network Address Translation）を介していてもグローバル空間からプライベート空間への通信を可能とする NAT-f（NAT-free）[6]などがある．

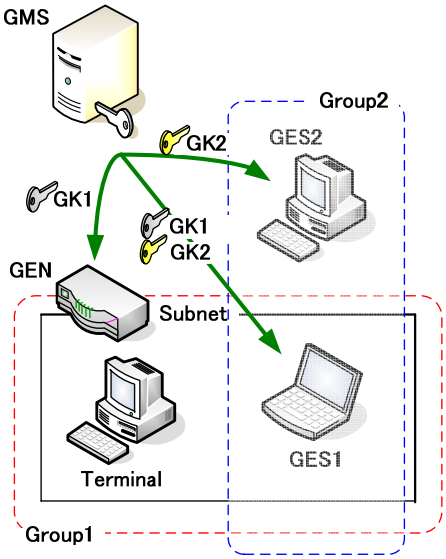

図 4　通信グループの定義方法

GSCIP における通信グループの定義方法を図 4 に示す．GSCIP の機能を実装している要素を GE（GSCIP Element）と呼ぶ．現状 GE には 2 タイプの装置がある．端末にソフトウェアをインストールするタイプの GES（GE realized by Software）と，サブネットを構成するルータに適用するタイプの GEN（GE for Network）である.GEN の配下に位置する端末は，GEN により一括して保護される．GSCIP では同一の暗号鍵を所持する GE を同一の通信グループとして定義している．この暗号鍵をグループ鍵 GK（Group Key）と呼ぶ．グループ鍵 GK と通信グループを 1 対 1 に対応付けることで IP アドレスに依存しない通信グループを定義でき，ネットワークのシステム環境が変化してもグループ情報が維持できる．同一の通信グループにおける GE 間の通信はグループ鍵 GK を用いて暗号化される．また GE には異なる通信グループとの通信を一切禁止する閉域モード CL（Closed Mode）と，平文であれば通信が可能な開放モード OP（Open Mode）という 2 つの動作モードがある．これらにより GSCIP では，通信の可否および暗号化の有無を柔軟に決定することができる．グループ鍵 GK は，電源投入時などの初期状態において，管理装置 GMS（Group Management Server）から通信グループの情報と共に配送される．

この時の GMS と各 GE 間の通信は，公開鍵を用いた確実な認証と暗号化が行われる．グループ鍵 GK は GMS から定期的に，およびネットワークのシステム構成が変化した際に更新される．

GSCIP では端末間の通信は，GE 自身が所持している動作処理情報テーブル PIT（Process Information Table）の内容に沿って処理を行う．PIT には送信元/宛先の IP アドレス，ポート番号，プロトコル番号，グループ鍵の識別情報，および通信パケットの暗号化/復号/透過中継/破棄といった処理内容が記述されている．この PIT は DPRP により生成される．

2.3. DPRP

DPRP では端末間の通信開始に先立ち，通信経路上に存在する全 GE に設定されている定義情報を取得するため，ネゴシエーションを行う．図 5 に DPRP の動作概要について示す．

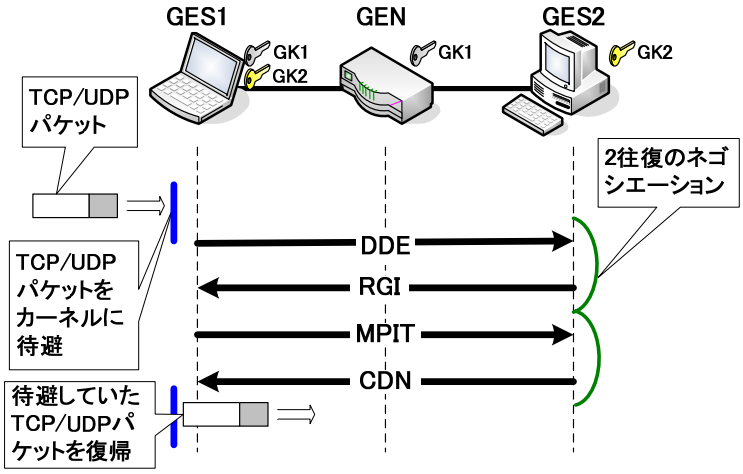

図 5　DPRP の動作概要

GES 1 は GEN の配下に帰属し，GES2 とは同一のグループに属している．GES1 から GES2 に対し通信が開始される場合の動作について説明する．GES1 は TCP/UDP パケットを送受信する際，自身の PIT を検索する．検索の結果 PIT がある場合は PIT の内容に従いパケットを処理する．PIT が無い場合は，TCP/UDP パケットをカーネルに一時的に待避させ，DPRP による 2 往復のネゴシエーションを行う．DPRP ネゴシエーションで使用する制御パケットは 4 つあり，順に DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）であり，それぞれ ICMP Echo パケットをベースに作られている．GES1 は終点 GE を決定するために通信相手（GES2）に向けて DDE を送信する．DDE を受け取った GES2 は終点 GE となり，RGI を生成する．終点 GE（GES2）は通信経路上の全 GE の各定義情報を収集し始点 GE を決定するため，DDE の送信元（GES1）に向け RGI を送信する．GES1 が RGI を受信すると GES1 が始点 GE となる．始点 GE（GES1）では収集した定義情報から全 GE の動作処理情報を決定し，PIT を生成する．そして通信経路上の他の GE に決定した動作処理情報を伝えるため，終点 GE（GES2）に MPIT を送信する．MPIT を受信した中間 GE（GEN）と終点 GE（GES2）は，自身に該当する動作処理情報を取得し，PIT の生成を行う．終点 GE（GES2）は DPRP のネゴシエーションが完了したことを始点 GE（GES1）に通知する．始点 GE（GES1）は一時的に待避していた TCP/UDP パケットを復帰させることにより TCP/UDP 通信が PIT の内容に基づいて開始される．

2.4. GE の課題

GE は現在 GES，GEN の 2 タイプがあるが，現状のままでは既存のネットワークに GE を導入することは困難であると考えられる．その理由として以下のことがあげられる．

- 既存のネットワークに GES や GEN を導入することは，既存の端末やルータに手を加える必要があり困難な場合がある
- 企業ネットワークなどでは新しくルータが入るとアドレス体系が変わり導入が難しい
- 現状の GE は GSCIP の機能を IP 層で実装しており，既存端末（サーバ等）に変更を加えることはカーネルを操作するので GES 等を導入することは許されない場合がある

第3章. GEA の提案と動作

上記課題を解決するため，ブリッジ型の GEA（GE realized by Adapter）を導入する．GEA はブリッジに GSCIP の機能を実装させ実現する．GEA を端末やルータの直前に設置することで, GES, GEN と同じ役割を果たすことができる. スイッチの直前に GEA を設置すれば，スイッチに接続された端末を一括してグルーピングすることも可能であり，より柔軟に既存のネットワークに対応することができる．

GEA が既存のネットワークに新たに導入されても，通信グループの定義方法に変わりはない．図 6 に GEA により構成されるネットワークの一例を示す.

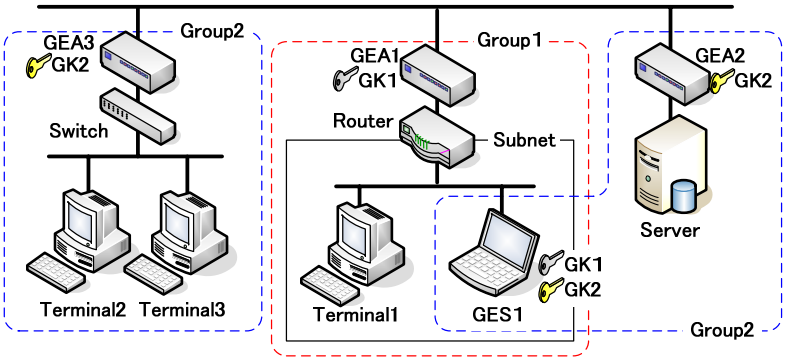

図 6　GEA により構成されるネットワークモデル

図 6 では，GEA1 によりルータ配下のサブネットを保護しており，GEA1 とルータで GEN の役割を果たしている．GEA2 により配下のサーバを保護し GES と同じ役割を果たしている．また GEA3 をスイッチの直前に設置し，配下の端末を一括してグルーピングしている．

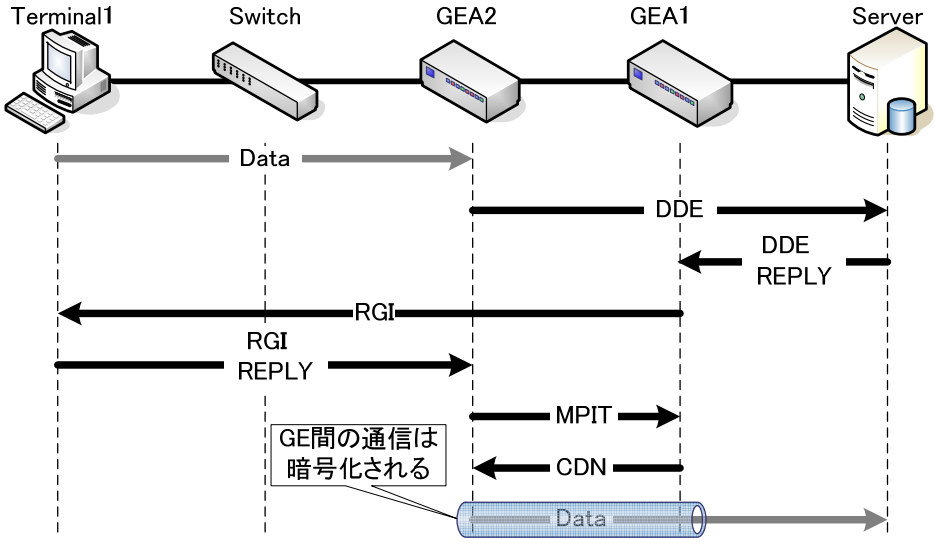

図 7　GEA により構成されるネットワークモデル

図 6 のネットワーク構成を想定した際の通信動作の一例を図 7 に示す．図 7 は端末 2 がサーバに通信を開始する際のシーケンスである．端末 2 とサーバはそれぞれ GEA2，GEA3 により保護され同一の通信グループ 2 に帰属している．端末 2 と，スイッチは GSCIP の機能を実装していないため DPRP を意識することなく通信パケットをサーバに向け送信する．通信パケットを受け取った初めの GE（GEA3）が DPRP ネゴシエーションを開始する．GEA3 は宛先をサーバとしたまま DDE を生成し送信する．サーバもまた GSCIP の機能を実装していないため DPRP を意識することはない．GSCIP を実装していない端末が DPRP の制御パケットを受信すると，通常の ICMP Echo Reply 応答をする．これは 4 つの制御パケットが ICMP Echo パケットをベースに作られているためである．DPRP では DDE に対する ICMP Echo Reply を DDE REPLY，RGI に対する ICMP Echo Reply を RGI REPLY とそれぞれ定義している．そこで GSCIP の機能を実装していないサーバが DDE を受信すると宛先を端末 2 とし,DDE REPLY を送信する．GEA2 はサーバからの DDE REPLY を最初に受信する．DDE の宛先が一般端末であった場合は DDE REPLY を最初に受信した GE（GEA2）が終点 GE となる．GEA2 は宛先を端末 2 としたまま RGI を生成し送信する．端末 2 は一般端末であるため RGI を受信すると RGI REPLY を応答する．RGI の宛先が一般端末であった場合は RGI REPLY を最初に受信した GE（GEA3）が始点 GE となる．始点 GE（GEA3）は終点 GE（GEA2）に対し MPIT を送信し，終点 GE（GEA2）は始点 GE（GEA3）に CDN を送信することで DPRP ネゴシエーションは完了する．この後の端末間通信は GEA3 と GEA2 により保護されたセキュアな通信となる．

第4章.　GEA の実装

GSCIP を実現するモジュール群のことを GPACK（Gscip PACKage）と呼び，DPRP はその一部を構成する．現状 GES，GEN の実装は IP 層で行っており，入出力関数 ip_input(), ip_output()から GPACK を呼び出してパケットの処理を行っている．GEA では現状の GPACK は改造せず, GPACK の呼び出し元である箇所をデータリンク層に変更することにより GEA の実装を実現させる．OS にはデータリンク層の情報が豊富な FreeBSD を選択した．図 8 に GEA の実装箇所の概要を図示する．

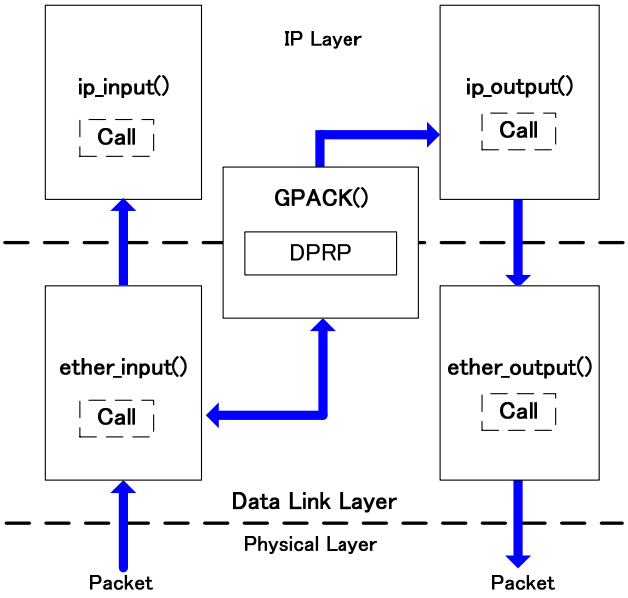

図 8　GEA の実装箇所

実装の基本的な考えは，GES，GEN と変わらず入出力関数から GPACK を呼び出し，DPRP などの処理を行った後，パケットを元の場所に差し戻す方式である．この方式では既存のデータリンク層の処理は GPACK の影響を一切受けることがない．

GEA では GPACK をデータリンク層の入力関数である ether_input()からのみ呼び出している．元々ブリッジの機能にはフレームをフィルタリングする機能が存在し，ether_input()においてフレームの中継等の判断がなされている箇所がある．今回の実装ではその箇所から GPACK の呼び出しを行っている．呼び出された GPACK では，受け取った通信パケットの種類を判別してから，適切なモジュールを選択し実行する．受信パケットが ICMP の場合，GPACK で処理を行わずにデータリンク層へ戻す．受信パケットが DPRP の制御パケットの場合，DPRP モジュールに渡され処理される．受信パケットが TCP/UDP パケットの場合，PIT の検索が行われ，PIT が存在する場合は PIT の内容に従いパケットが処理され，PIT がない場合は DPRP モジュールに処理が渡され，DPRP モジュールは DDE を生成して ip_output()に渡し送信する．GEA はブリッジであるため，常になんらかの通信経路上の中間に位置している．このため GEA 自身から通信を開始することは想定しておらず，データリンク層の出力関数 ether_output()から GPACK を呼び出すことはない．

第5章.　まとめ

ユビキタス社会において FPN の概念はネットワークのあるべき姿であり，今後 FPN を既存のネットワークに導入することは十分にあり得る．その際 GEA は大きな役割を果たすことになると考えられる．本論文ではブリッジ型の GE である GEA の提案をし，GEA の動作，GEA の実装について述べた．現状の GE の課題をあげ，GEA の必要性と効果について検討し既存のネットワークにも柔軟に対応できることを示した．今後は実機による動作確認を行い，GEA がネットワークに与えるスループットを測定し評価をしていく．

参　考　文　献

[1] 小早川知昭，西田晴彦：IPsec 徹底入門，翔泳社出版（2002）
[2] 名城大学理工学部情報工学科，渡邊研究室：http://www.wata-lab.meijo-u.ac.jp/
[3] 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，DICOMO2005 シンポジウム論文集，Vol.2005，No.6，pp.441-444，Jul.2005
[4] 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
[5] 竹内元規，鈴木秀和，渡邊晃：エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，情報処理学会論文誌，Vol.47，No.12，pp.3244-3257，Dec.2006
[6] 鈴木秀和，渡邊晃：アドレス空間透過性を実現する NAT-f の実装と評価，DICOMO2006 シンポジウム論文集(I)，Vol.2006，No.6，pp.453-456，Jul.2006