平成20年度　修士論文

邦文題目

セキュア通信アーキテクチャGSCIPを実現するグループ管理サーバの実装と運用評価

英文題目

Implementation and operational evaluation of Group Management Server which realize secure communication architecture GSCIP

情報科学専攻

(学籍番号: 073432006)

今村　圭佑

名城大学大学院理工学研究科

内容要旨

企業ネットワークでは企業が管理する個人情報の漏洩など，社員や内部関係者の不正による犯罪が多く報告されている．外部からの侵入防止には通信の暗号化やデジタル署名などのセキュリティ対策がなされている．しかしながら，イントラネット内部のセキュリティ対策はユーザ名とパスワードによる簡単な相手認証，アクセス制御程度しか行われていないのが現状である．そのため企業ネットワークにおいてセキュリティを確保するために，部門や業務に応じた通信グループを構築し，暗号通信を行うことは有効な手段である．そこで我々は柔軟性とセキュリティを兼ね備えたネットワークの概念として FPN（Flexible Private Network）と呼ぶシステムを提唱し，FPN を具体的に実現するための通信アーキテクチャとして GSCIP（Grouping for Secure Communication for IP）を検討してきた．GSCIP では端末が所属する通信グループ，および動作モードの組み合わせにより，通信の可否および暗号通信の有無を動的に決定することができる．GSCIP の管理はグループ管理サーバ GMS（Group Management Server）で行う．GMS では通信グループと動作モードの定義，およびグループ鍵の生成，更新を行い，クライアント起動時にこれらの情報を配送する．本稿ではグループ管理サーバ GMS を実装し，その成果をもとに適当なネットワークモデルにおける管理負荷を IPsec を用いた場合と比較し，有効性を確認する．

目 次

図 目 次

表 目 次

第1章　序論

企業ネットワークでは，不正侵入，データの盗聴，改ざんなどに対するセキュリティ対策が重要な課題となっている．外部からの侵入防止には通信の暗号化やデジタル署名など，セキュリティ強度の高い技術を駆使したり，ファイアウォールや IDS（Intrusion Detection System）などと併用したりするなど，様々な対策がなされている．しかし企業ネットワークのセキュリティの脅威は組織内部にも存在し，社員や内部関係者の不正による犯罪が多く報告されている [1]．企業ネットワーク内部のセキュリティ対策は，ユーザ名とパスワードによる簡単な相手認証，アクセス制御程度しか行われていないのが現状である．そのため企業ネットワークにおいてセキュリティを確保するために，部門や業務に応じた通信グループを構築し，暗号通信を行うことは有効な手段である．この方法によりネットワークインフラ環境をそのまま利用しながら，同一通信グループのメンバ間通信の安全性を確保することができる．

エンド端末同士でセキュリティを確保する既存の方法として IPsec [2] トランスポートモードがある．この方法ではきめ細かい通信グループの定義が可能であるが，すべての端末に機能を実装する必要があり，規模が大きくなると管理負荷が大きくなる．一方ドメイン単位にセキュリティを確保する既存の方法として IPsec トンネルモードを使用し，セキュリティゲートウェイ（以下 SGW）間に VPN（Virtual Private Network）を構築する方法がある．この方法では SGW だけにセキュリティ機能を実装すればよいが，きめ細かい通信グループを定義することができない．両者の利点を生かすためには，個人単位の通信グループとドメイン単位の通信グループを混在できることが望ましい．このような環境を以降混在環境と呼ぶ．たとえば特定のドメインの中に，別の通信グループの個人が存在するような混在環境が考えられる．企業ネットワークでは部門単位の業務グループと部門横断の個人単位の業務グループ（たとえばプロジェクト単位）が混在することがあり，混在環境においても通信グループを柔軟に定義できることが望まれる．

IPsec はトランスポートモードおよびトンネルモードの互換性がなく，上記のような混在環境への適応に向いていない．IPsec では通信経路上に同一モードの IPsec 機能を持つ装置が対で存在することが前提となっており，混在環境を実現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を設定しなければならないなど管理負荷が大きくなるという課題がある．

このような状況を考え，我々は柔軟性とセキュリティを兼ね備えた通信グループの構築を可能とする FPN（Flexible Private Network）と呼ぶシステムを提唱し，FPN を具体的に実現するための通信アーキテクチャとして GSCIP（Grouping for Secure Communication for IP；ジースキップ）[3] を検討してきた．GSCIP は通信グループと共通暗号鍵を一対一で対応させることにより，IP アドレスや物理的配置に依存しない通信グループを構成できるという特徴がある．GSCIP では端末が所属する通信グループ，および動作モードの組み合わせにより，通信の可否および暗号通信の有無

を動的に決定することができる．GSCIP の管理は，グループ管理サーバ GMS（Group Management Server）で行う．GMS では通信グループと動作モードの定義，およびグループ鍵の生成，更新を行い，クライアント起動時にこれらの情報を配送する．

文献 [3] では GSCIP の考え方が提案され，管理負荷が軽減されることが記述されているが限定的であり，IPsec との詳細な比較は行っていなかった．本稿ではグループ管理サーバ GMS を実装し，その成果をもとに GSCIP の管理負荷を IPsec を用いた場合と比較した．比較項目は初期設定時，ネットワークの構成変化時，および通信グループのメンバ構成変化時に分けて評価した．その結果，システム規模が大きく，構成が複雑になるほど GSCIP の管理負荷が相対的に軽くなることを定量的に示すことができた．また，GSCIP は通信開始時のオーバヘッドが極めて小さく，エンドユーザにとっても使いやすいシステムであることを示した．

以降，2 章 で比較技術について，3 章 でグループ管理サーバの動作について述べる．4 章 で管理負荷の比較評価結果と性能を述べ，5 章 でまとめる．

第2章　通信グループの管理方式

2.1　IPsecによる管理

2.1.1　IPsecの概要

IPsecは暗号技術を用いて，IP層においてデータの改ざん防止や秘匿機能を提供するプロトコルである．これによりアプリケーションを限定することなく，通信経路上での盗聴や改ざんを防止できる．

IPsecには通信相手のなりすましを防止するための本人性確認，データの改ざんを防止するための完全性保証を提供するAH（Authentication Header）[4]とAHの機能に加えデータの暗号化を行うESP（Encapsulating Security Payload）[5]の2つのセキュリティプロトコルがある．

IPsecは汎用性を重視しておりノード間の通信において，IPアドレス，ポート番号，プロトコルによって複数の暗号方式や暗号鍵，セキュリティプロトコルを指定することができる．ノード間のコネクションを管理するパラメータをIPsecではSA（Security Association）と呼び，SAを管理するデータベースをSAD（Security Association Database）と呼ぶ．すべてのIPsecパケットはSAに従って送受信が行われる．どのプロトコルでどのSADを使用するかを決めるのが，セキュリティポリシ（Security Policy：SP）で，そのセキュリティポリシを管理するデータベースをSPD（Security Policy Database）と呼ぶ．IPsecヘッダにはノードが所持するSAを示すID情報が付加される．これをSPI（Security Parameter Index）と呼ぶ．IPパケットを送信するノードは，そのIPパケットに合致するセキュリティポリシを探し，セキュリティポリシが示すSAの情報に基づいて暗号化の処理を行う．受信時はヘッダに含まれるID情報（SPI）からSAが検索されて復号/認証処理が行われ，その処理結果がセキュリティポリシで規定されるセキュリティ要求を満たしているか否かの判定が行われる．

IPsecを利用するにはSAをエンド端末同士で共有する必要がある．手作業でSAを設定する場合，暗号化に使用する共通秘密鍵やその他のパラメータを両端末にそれぞれ設定する必要がある．手作業でSAを設定するのはセキュリティ上好ましくないため，通常は鍵交換プロトコルを利用して自動でSAの設定を行う．SAを共有するのに必要な鍵情報の交換を安全に行うプロトコルとして以下に述べる，IKE（Internet Key Exchange）[6, 7]やKINK（Kerberized Internet Negotiation of Keys）[8]がある．

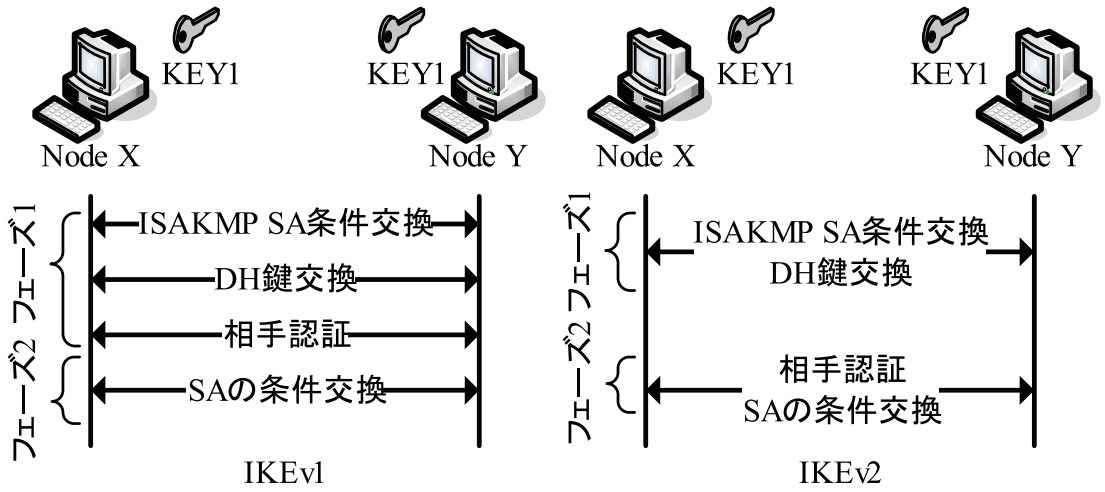

図 2.1　IKE ネゴシエーションシーケンス

2.1.2　IKE

IKE は 2 つのフェーズに分かれており，フェーズ 1 で SA の情報を交換するための SA（ISAKMP SA）[9] を生成する．フェーズ 2 でこの ISAKMP SA を使用して SA を生成するためのパラメータを交換する．IKE ネゴシエーションを図 2.1 に示す．IKEv1 は SA のパラメータをネゴシエートして決定する SA 条件交換，通信に使用する共通鍵を共有する DH（Diffie-Hellman）鍵交換，通信相手が本物であることを確認する相手認証からなる．IKE には IKEv1 と IKEv2 がある．IKEv2 には IKEv1 が複雑になってしまった反省から再定義されたものである．実現される機能は同じであるため，以降は IKEv2 について述べる．フェーズ 1 は 1 往復のネゴシエーションで ISAKMP SA の条件交換と DH 鍵交換を同時に行う．フェーズ 2 は 1 往復のネゴシエーションで相手認証と SA の条件交換を同時に行う．IKE は SA を生成するために，通信ペア毎に設定する必要がある．そのため通信ペアが増加すると大幅に設定による管理負荷が増加する．

2.1.3　KINK の概要

KINK は Kerberos [10] の認証機構を利用して IPsec を利用したいノードを認証し，各ノード同士が SA を共有するための設定情報を交換するプロトコルである．Kerberos は共通暗号鍵による認証方式の一つである．

Kerberos のチケットを発行する発行局を KDC（Key Distribution Center）と呼び，認証サーバ AS（Authentication Server）とチケット交付サーバ TGS（Ticket Granting Server）の機能で構成されている．KDC の管理領域をレルム（realm）と呼び，レルムに所属するノードの認証とチケットの発行を一手に受け持つ．レルムは 1 つの通信グループとみなすことができる．各ノードのユーザアカウントに相当するものはプリンシパル（Principal）と呼ばれる．各ノードは KDC に各自のプリンシパルと KDC との間で共有する暗号鍵を登録する．エンドノード同士が SA を交換する場合は，KDC から発行されたチケットを利用して相互認証を行い，チケットに含まれるセッション鍵を使用して SA のパラメータの設定と交換を行う．

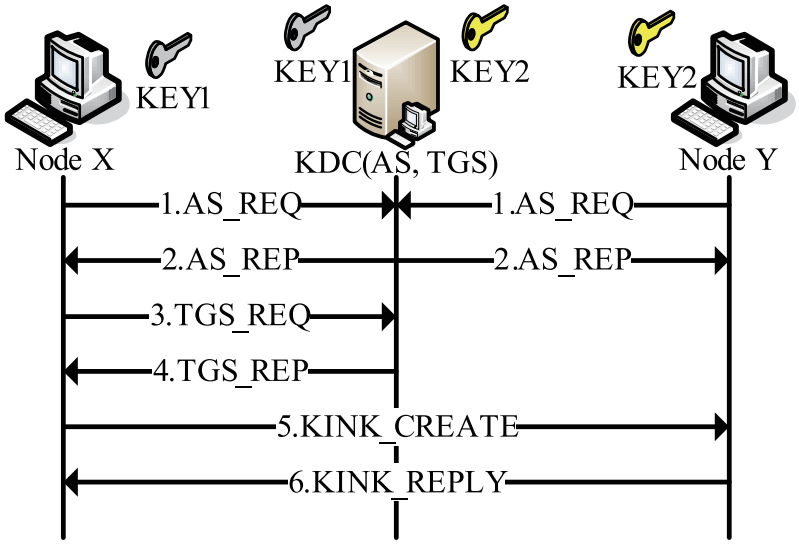

図 2.2　KINK ネゴシエーションシーケンス

図 2.2 に KINK ネゴシエーションのシーケンスを示す．ノード X と Y は起動時に AS_REQ を送信して，自身の認証と任意のチケットを取得するための TGT（Ticket Granting Ticket）を取得する．この TGT はそれぞれノード X と Y の共通鍵で暗号化されているため，他のノードは取得できない．ノード X が Y と SA を共有したいという要求が発生した場合は，ノード X が KDC に対してノード Y と KINK 交換を行うためのチケットを要求する．この要求には事前に取得した TGT を提示する必要がある．KDC はノード X に対してノード X と Y が通信するためのセッション鍵とチケットを X に送付する．これらの情報は KDC とノード X が共有している共通鍵で暗号化されているため他のノードは取得することができない．またこのチケットにはノード X の ID とセッション鍵が含まれており，これらは KDC とノード Y が共有している共通鍵で暗号化されているため，X を含む他のノードは復号できない．ノード X はチケット取得後，セッション鍵を使用してノード X と Y が通信するための SA 生成に使用する共通鍵を生成する．その後事前に設定してあるセキュリティポリシに基づき，自らの inbound に SA を設定する．ここで設定した SA 情報と暗号化されたままのチケットをノード Y に送信する．ノード Y ではチケットを自己の共通鍵で復号し，チケットに含まれるセッション鍵からノード Y の inbound の SA に使用する共通鍵を生成し，SA を設定する．ノード Y の outbound はノード X の inbound の設定を使用する．その後ノード Y は inbound の SA の情報をノード X に送信することにより SA の交換が終了する．

KINK は KDC と各ノードとの間で共通鍵を共有しておくため，IKE のように通信ペア毎に共通鍵を共有する必要がない．そのため通信相手が増加しても設定による管理負荷は大きく増加することはない．ただし，通信グループごとにレルムを構築する必要があり，通信グループが増加すると管理負荷が大きくなる．KINK は共通鍵ベースのシステムであるため，公開鍵演算を必要としないという特徴がある．そのためセンサネットワークなど CPU パワーが低いノードを利用する場合に有効である．

2.2 GSCIP

2.2.1 GSCIP の概要

我々が目指している FPN とは，以下の 3 つの透過性を実現するシステムである．ドメイン単位と個人単位が混在したネットワーク環境であっても容易にグループを定義できる位置透過性，またユーザはセキュリティを確保したまま自由に移動できる移動透過性，さらにユーザは，IPv4 グローバルアドレス空間，IPv4 プライベートアドレス空間，IPv6 アドレス空間の違いを意識する必要がないアドレス空間透過性である．GSCIP は FPN の中の位置透過性を実現する通信アーキテクチャである．本論文では位置透過性に絞って記述する．図 2.3 に GSCIP による通信グループの構築方法を示す．

GSCIP における通信グループの構成要素を GE（GSCIP Element）と呼ぶ．GE には端末に機能を実装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．GEA は変更が不可能なサーバやルータの直前に設置することで，配下のサーバやルータがグループの構成要素になることが可能である．そのため GSCIP は現在稼働しているサーバやルータと共存が可能である．

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．グループ鍵 GK を通信グループと一対一に対応させることにより，IP アドレスや物理的配置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，グループ鍵による相互認証と暗号通信が実行される．

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

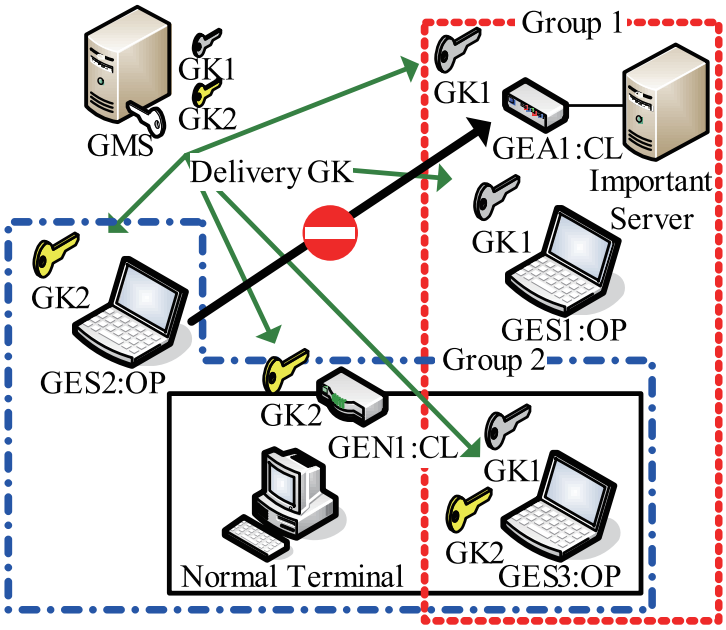

図 2.3　通信グループの構築方法

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 2.3 では，通信グループ 1 に所属する GES1 と GES3 間の通信はグループ鍵 1 で相手認証および暗号化が行われる．GES1 と GES2 の通信は同一の通信グループに所属していないが両者とも開放モードであるため平文での通信が行われる．GEA1 は通信グループ 1 に所属しており，かつ閉域モードであるためグループ外の GES2 からのアクセスを拒否する．

GE に必要な情報はグループ管理サーバ GMS で定義される．この情報を GE 情報と呼び，ユーザ ID と動作モード（OP または CL），および GE との共通鍵で構成される．また GMS では各 GE が所属する通信グループの定義を行う．通信グループは，物理的配置や IP アドレスに依存することなく決定することができ，個人単位，ドメイン単位の混在環境であったり，ユーザが複数の通信グループに重複帰属するようなケースでも柔軟に定義できる．サブネット内に存在する個人に対して，そのサブネットとは別の通信グループを定義することもできる．GMS では通信グループの定義のほかに，グループ鍵の生成，更新，配送などを行う．グループ鍵は GMS の設定に基づいて定期的に更新される．GMS と各 GE の間は確実な認証と暗号化が可能であることが前提である．

2.2.2 DPRP

DPRP（Dynamic Process Resolution Protocol）[3] は GSCIP を実現する一連のプロトコルの 1 つで，通信経路上の GE がネットワーク構成を学習することにより，自己の動作を決定する動作処理テーブル PIT（Process Information Table）を自律的に生成する．各 GE は自己の PIT に従いパケットの処理を行う．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番号，鍵バージョンが記述されている．DPRP はエンド端末間の通信に先立ち実行するネゴシエーションプロトコルである．端末はパケット送信時に PIT を検索し，PIT に従ってパケットを処理する．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カーネル内に退避し，DPRP を実行して PIT を動的に生成する．図 2.4 に DPRP のシーケンスを示す．図 2.4 はエンド端末 GES1，GES2 の間にルータタイプの GEN が存在する場合を示している．

DPRP には，ICMP をベースとして定義された DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）という 4 つの制御パケットからなる．DDE は終点 GE を探索するもので，DPRP のトリガーとなった通信パケットの CID（Connection ID；送信元/宛先 IP アドレス，ポート番号，プロトコルタイプ）が記述されており，宛先ノードへ送信される．図 2.4 では GES2 が終点 GE となり，RGI を返送する．RGI は始点 GE を探索し，かつ各 GE の設定情報を収集するためのものである．通信経路上の GE は RGI を中継する際，自身の設定情報（ID，動作モード：OM，所属する通信グループ番号：GKnum）をパケットに追加していく．図 2.4 では 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 PIT を決定する．GES1 は決定した動作処理情報を MPIT に記述して

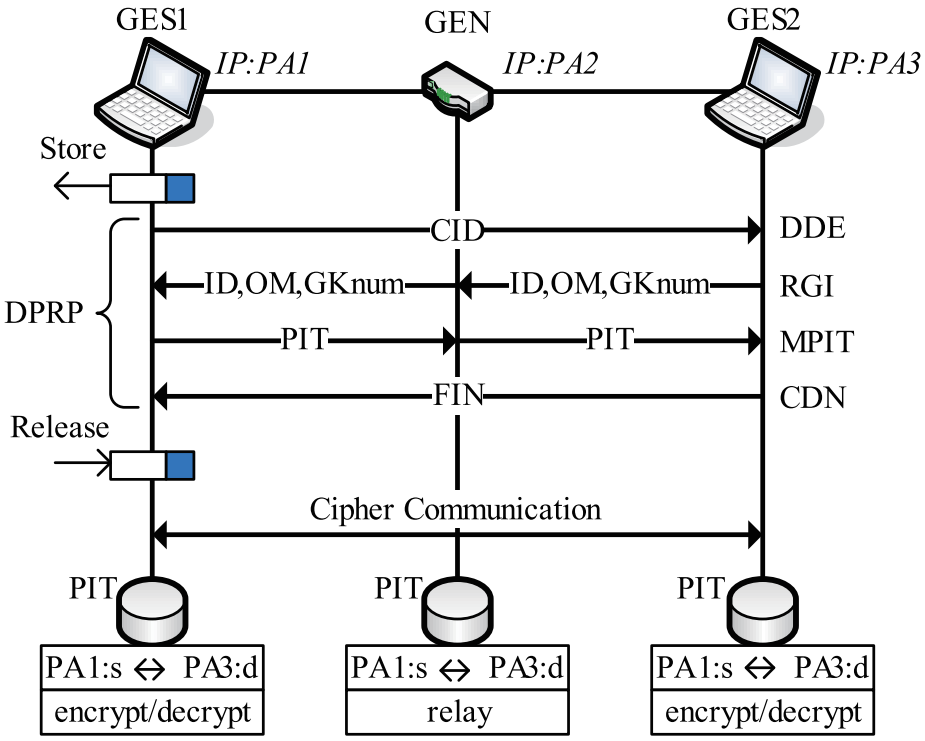

図 2.4　DPRP のシーケンス

GES2 に宛てて送信する．MPIT を受信した GEN，GES2 はパケットの内容から自身に関する動作処理情報を取り出し，PIT を仮生成する．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 GES1 へ送信する．CDN を受信した各 GE は PIT を確定させる．GES1 は待避していた通信パケットを復帰させる．以後の通信は各 GE において生成された，PIT に従った処理が実行される．

GE は PIT に記述されている動作処理情報によって，パケットの暗号化/復号，透過中継，破棄を行う．ここで通信暗号プロトコルとしては，IPsec ESP のような方式を適用することも可能であるが，GSCIP の中で定義された PCCOM（Practical Cipher Communication Protocol）[11] を使用すれば，高スループットの通信が可能である．

第3章　GSCIPにおけるGMSの役割

3.1　GMSの構成

図 3.1 に GMS（Group Management Server）の構成を示す．GMS は GE 情報やグループ鍵を格納するデータベース，各 GE に GE 情報やグループ鍵を配送したり，グループ鍵の更新などを行うサーバデーモン gmsd（Group Management Server Deamon），および GSCIP 管理者からの GE の追加登録や通信グループ構成の変更，グループ鍵の更新を受けつける Web アプリケーション PHP で構成されている．管理者は Web ブラウザを使用して GMS にアクセスし，操作を行うことができる．また各 GE には GMS からの情報を受け取り，GE の設定情報やグループ鍵をカーネルへセットするためのクライアント用デーモン gmcd（Group Management Client Deamon）が実装されている．

GMS で管理するデータベースを図 3.2 に示す．GE 情報テーブルは GE のユーザ ID，動作モード，GE との共通鍵，GE がオンラインかオフラインであるかの状態，GE が GMS に対して定期的に送出するパケットの受信時間を記録しておくチェック時間で構成されている．GMS はこのチェック時間を用い GE の状態を記録している．グループ鍵を更新する場合は，全てのオンライン GE に対してグループ鍵を配送する．通信グループ情報テーブルには，通信グループ番号，グループ鍵のバージョン，グループ鍵長，グループ鍵で構成されている．所属グループ情報テーブルはどの GE がどの通信グループに所属しているかを保持するテーブルで，ユーザ ID，通信グループ番号で構成されている．

各 GE は gmcd 起動時に GMS に対し GE 情報とグループ鍵を要求する．GMS は GE の確実な認証を行った後，GE 情報と所属する通信グループのグループ鍵を暗号化して配送する．認証の方法については現時点の実装では GMS と各 GE 間で共通暗号鍵を共有する方式を適用している．今

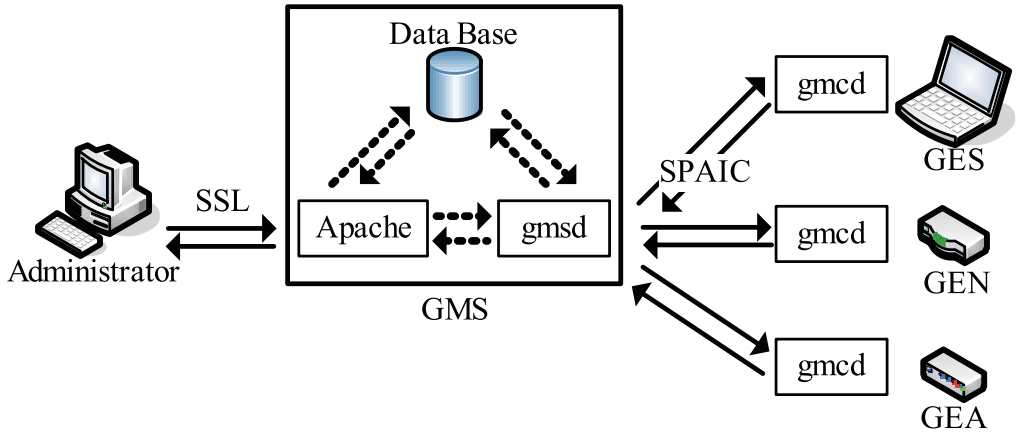

図 3.1　GSCIP におけるグループ管理システムの構成

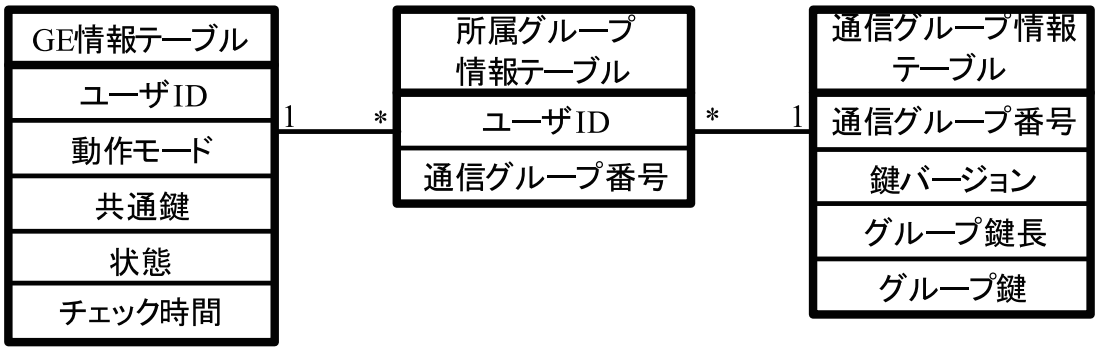

図 3.2　GMS データベース

後は公開鍵による認証方式，SPAIC（Secure Protocol for Authentication with IC card） [12] を検討中である．GSCIP の場合 GMS と GE 間の認証が必要になるのは，GE の立ち上げ時だけであるため，公開鍵による認証方式を採用しても通信に影響を与えることはほとんどない．以降の比較では，GMS と GE 間の認証に共通鍵暗号方式を適用した場合について記述する．

3.2　配送シーケンス

図 3.3 に GMS から GE への配送シーケンスを示す．GE はクライアントデーモン起動時に SPAIC に GMS から GE 毎に定義されている情報を取得する．この情報には DPRP で使用するシステム共通暗号鍵 CK と GE の動作モード，所属する通信グループのグループ鍵情報が含まれる．これらの情報を受信した gmcd はカーネルへシステム共通暗号鍵と動作モード，グループ鍵をセットする．

GMS では定期的あるいは管理者の指示でシステム共通暗号鍵，グループ鍵の更新を行う．これらの鍵が更新された場合は，全てのオンライン GE に即座に配送し，カーネルへセットする．また

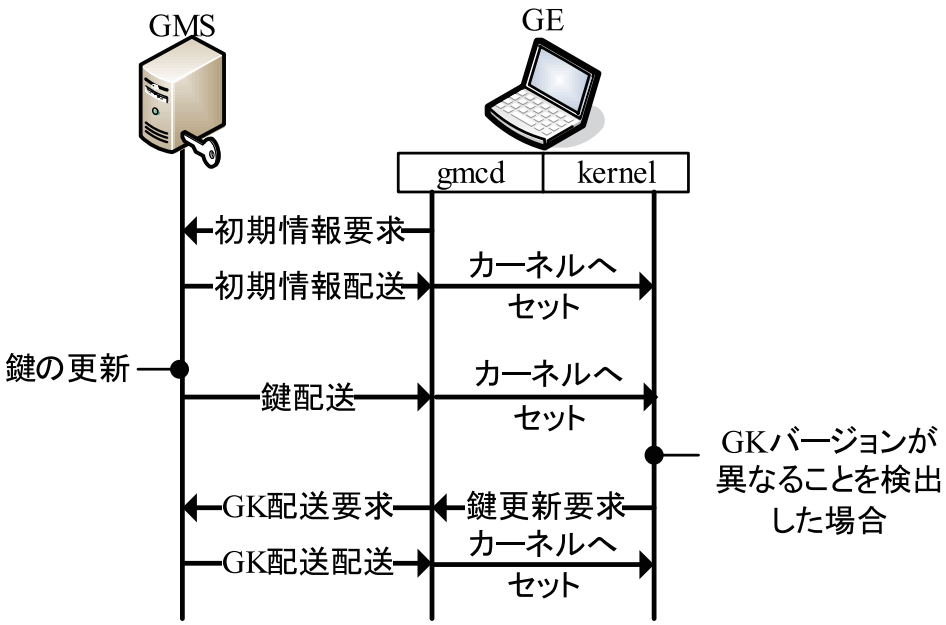

図 3.3　GMS から GE への配送シーケンス

GE が DPRP ネゴシエーション中にグループ鍵のバージョンが異なることを検出した場合はカーネルから鍵配送要求を gmcd に対して指示し，GMS から最新のグループ鍵を取得する．

第4章　各方式の比較

4.1　管理負荷の比較

各方式を使用した場合の管理負荷について比較評価した．通信アーキテクチャ GSCIP，鍵配送サーバを GMS，ネゴシエーションに DPRP を使用する場合を以下 GSCIP，通信アーキテクチャ IPsec，鍵交換ネゴシエーションに IKE を使用する場合を以下 IKE，鍵配送サーバ Kerberos，鍵交換ネゴシエーションに KINK を使用する場合を以下 KINK とする．

4.1.1　評価方法

特定のネットワーク構成を想定した上で，各ノードおよびサーバで行う設定 1 つあたりに必要な項目を負荷 1 と定義し，設定の項目数の違いにより管理負荷の違いを比較する．また，ノード数および通信グループ数をパラメータとして管理負荷の変化を比較する．

想定するネットワーク構成を図 4.1，図 4.2 に示す．図 4.1 の構成では，ノード 1 と 4 で通信グループ 1 を構成し，ノード 2，3 および 4 で通信グループ 2 を構成する．同じ通信グループに所属するノードは暗号通信を行い，他の端末とは一切通信を行わないものとする．この想定環境において初期導入時に必要な管理負荷およびノードを増加させていく場合の管理負荷について比較する．

図 4.2 では実際のネットワーク環境に近い形で，ノード 1，2，SGW および SGW 配下の一般端末で通信グループ 1 を構成し，ノード 2，3 で通信グループ 2 を構成する．図 4.2 は本論文でも必要性が高いとしている混在環境に相当するもので，その中でも最も小規模なシステムである．こ

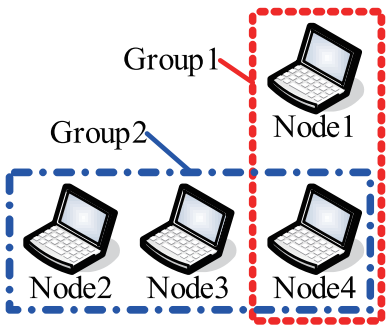

図 4.1　想定するネットワーク構成 1

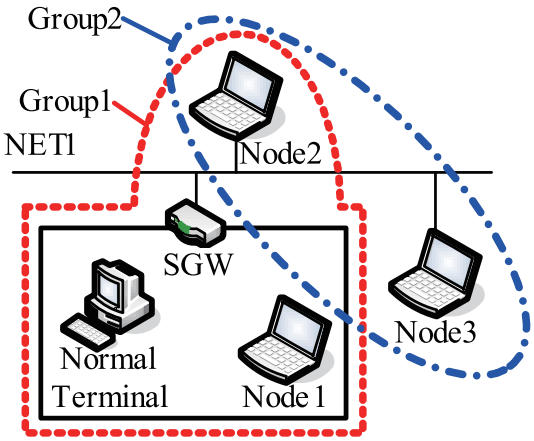

図 4.2　想定するネットワーク構成 2

の想定環境における初期導入時に必要な管理負荷，ネットワークの構成変化時に発生する管理負荷，通信グループのメンバ構成変化時に発生する管理負荷を以下に比較する．ここで構成変化とは，人事異動や出張，引越しなどオフラインでの移動による変化であり，通信中の移動は含まない．

4.1.2 ネットワーク構成 1 の初期管理負荷

GSCIP を利用するために GMS に必要な設定項目を表 4.1 に示す．GE 情報にはユーザ ID，動作モード，および GE との共通鍵の 3 項目が必要である．グループ鍵情報には通信グループ番号とグループ鍵のバージョン，鍵長，グループ鍵の 4 項目必要となる．さらに所属通信グループ情報には各 GE が所属する通信グループを定義するため，ユーザ ID と通信グループ番号のペアが必要である．GE にはユーザ ID と GMS との共通鍵，GMS のアドレスを設定する．

GSCIP で想定環境を構築する場合を考える．ノード 1〜4 は GES1〜4 と置き換えると，各 GE が所持するグループ鍵は表 4.2 となる．GSCIP では通信グループとグループ鍵を一対一で対応させて管理しているため，通信グループ 1 はグループ鍵 GK1 を使用しグループを構成している．同様に通信グループ 2 はグループ鍵 GK2 を使用し構成する．図 4.1 の環境では，GE の台数が 4 台であるため GMS との共通鍵の設定として各 GE にユーザ ID，共通鍵，GMS のアドレスの設定が必要となり合計 12 である．GMS には各 GE の動作モード，共通鍵の設定が必要であり合計 12 である．さらに通信グループ数は 2 であり，グループ鍵情報の設定項目として合計 8 必要となる．また各 GE が所属する通信グループは GES1，GES2，GES3 が 1 グループ，GES4 が 2 グループである．そのため所属通信グループの設定はユーザ ID と通信グループ番号のペアで 10 必要である．よって想定する環境における初期管理負荷の合計は 42 である．

一方，事前共有鍵方式を用い IKE を利用する場合の各設定 1 つあたりに必要な設定項目数表 4.4 に示す．事前共有鍵方式では，ノード間で事前に共有した事前共有鍵と通信相手の事前共有鍵識別子を設定し，設定項目数は 2 である．セキュリティポリシの設定は，通信ペアの IP アドレスを inbound と outbound の双方設定し，暗号プロトコル，IPsec モード，ポリシレベル，SA に使用する暗号アルゴリズム，ハッシュルアルゴリズムの設定が必要である．パケットの処理内容により設定項目数が異なり，トンネルモードはさらにエンドノードの IP アドレスをペアで設定する必要があり，設定項目数は 16，トランスポートモードでは 14 になる．パケットを破棄する Discard，中継する Bypass は暗号アルゴリズム等の設定が不要であり，設定項目数は 8 である．IKE の設定は，通信相手の識別子，ISAKMP SA で使用する暗号アルゴリズム，ハッシュアルゴリズム，DH

表 4.1 GMS の設定項目

	GE 情報	グループ鍵情報	所属通信グループ情報
設定内容	ユーザ ID 動作モード 共通鍵	通信グループ番号 鍵バージョン 鍵長 グループ鍵	ユーザ ID 通信グループ番号

表 4.2　各ノードが所持するグループ鍵

ノード	所持するグループ鍵
GES1	GK1
GES2	GK2
GES3	GK2
GES4	GK1，GK2

表 4.3　各ノードの設定項目数

GSCIP/GMS ＋ DPRP				
	GE の設定			
GES1	3			
GES2	3			
GES3	3			
GES4	3			
	GE 情報	グループ鍵情報	所属通信グループ情報	合計
GMS	12	8	10	30
合計	24	8	5	42
IPsec/IKE				
	事前共有鍵情報	セキュリティポリシ	IKE	合計
Node1	2	IPsec,Transport:14	11	27
Node2	4	IPsec,Transport:16	12	32
Node3	4	IPsec,Transport:16	12	32
Node4	6	IPsec,Transport:18	13	37
合計	16	64	48	128
IPsec/Kerberos ＋ KINK				
	KDC との共通鍵	セキュリティポリシ	KINK	合計
Node1	3	IPsec,Transport:14	1	18
Node2	3	IPsec,Transport:16	2	21
Node3	3	IPsec,Transport:16	2	21
Node4	5	IPsec,Transport:18	3	26
KDC	ノードとの共通鍵：15			15
合計	14	64	8	101

グループの設定が必要であり，設定項目数は 11 である．

IKE を利用して図 4.1 と同様な環境を実現する場合の設定項目数を表 4.3 に示す．通信グループ 1 を構築するために，ノード 1，4 に事前共有鍵の識別子と事前共有鍵を設定する．同様にノード 2，3，4 がそれぞれ事前共有鍵を共有する．ゆえにノード 1 の事前共有鍵による設定項目数はノード 1 が 2，ノード 2，3 は 4，ノード 4 は 6 であり，管理負荷の合計は 14 である．またノード 1 はノード 4 への通信は IPsec トランスポートモードを使用し，暗号化するといったセキュリティポリシを設定する．この設定項目数は 14 である．同様にノード 2 はノード 3，4 に対して行う．セ

表 4.4　ノードに必要な IKE の設定項目数

	事前共有鍵情報	セキュリティポリシ	IKE
設定項目	事前共有鍵識別子 事前共有鍵	通信ペア IP アドレス 処理内容（IPsec/Discard/Bypass） 暗号プロトコル（ESP/AH） モード（Transport/Tunnel） ポリシレベル（require/use） 暗号アルゴリズム ハッシュアルゴリズム　etc.	通信相手識別子 暗号アルゴリズム ハッシュアルゴリズム DH グループ 相手認証方法 etc.
項目数	2	IPsec,Transport:14 IPsec,Tunnel:16 Discard/Bypass:8	11

表 4.5　ノードに必要な KINK の設定項目数

	KDC との共通鍵	セキュリティポリシ	KINK
設定項目	プリンシパル 共通鍵 KDC の IP アドレス	通信ペア IP アドレス 処理内容（IPsec/Discard/Bypass） 暗号プロトコル（ESP/AH） モード（Transport/Tunnel） ポリシレベル（require/use） 暗号アルゴリズム ハッシュアルゴリズム　etc.	通信相手プリンシパル
項目数	3	IPsec,Transport:14 IPsec,Tunnel:16 Discard/Bypass:8	1

キュリティポリシの設定は通信相手の数によって異なり，合計 64 である．さらに各ノードと IKE を行うための設定をそれぞれノードに行い，その設定による管理負荷は通信相手の数により異なり合計 48 である．ゆえに IKE を利用する場合の初期設定の管理負荷はノード 1 が 27，ノード 2，3 は 32，ノード 4 は 37 合計 128 である．

KINK を利用する場合の各設定 1 つあたりに必要な設定項目数表 4.5 に示す．KINK を使用する場合には KDC との共通鍵の設定として自己のプリンシパル，KDC との共通鍵，KDC の IP アドレスが必要であり，設定項目数は合計 3 である．セキュリティポリシの設定は IKE を使用する場合と同様で，パケットの処理内容によって異なりそれぞれ 14，16，8 である．KINK の設定は通信相手のプリンシパルのみを設定すれば良く，設定項目数は 1 である．

KINK を利用して図 4.1 と同様な環境を実現する場合の設定項目数を表 4.3 に示す．KINK を利用する場合は IKE と異なり KDC との共通秘密鍵と自己のプリンシパル，KDC の IP アドレスの設定が必要である．ノード 1〜3 は一つの通信グループにのみ所属しているのでプリンシパルと共通鍵のペアは 1 つであり，その設定項目数は 3 である．ノード 4 は 2 つの通信グループに所属してい

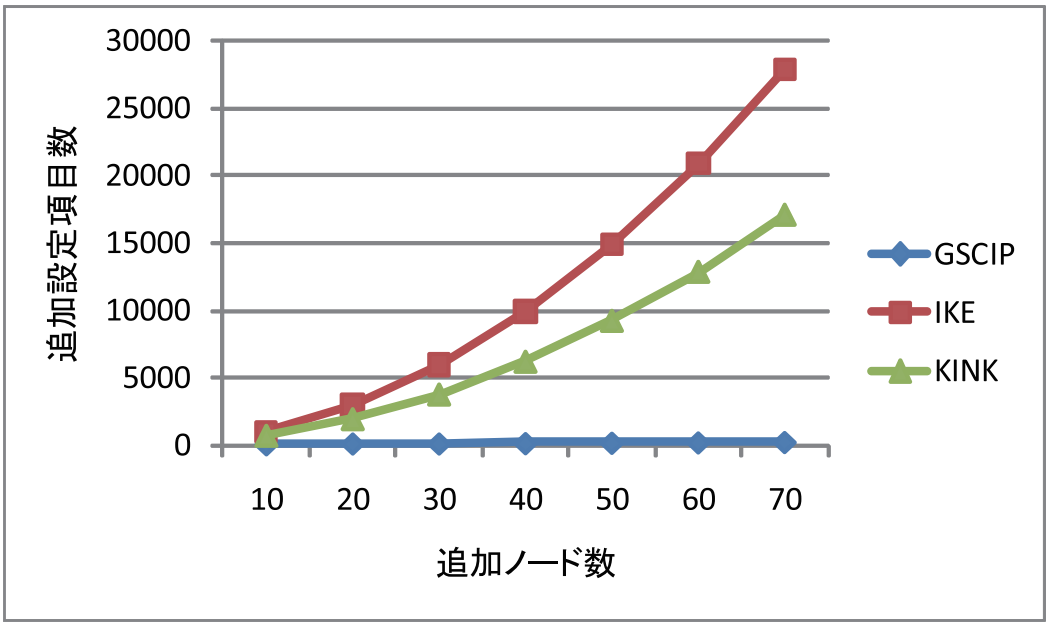

図 4.3　ノード追加による管理負荷の増加数

るため，プリンシパルと共通鍵のペアが 2 つ必要である．そのため設定項目数は 5 である．KDC にも各ノードのプリンシパルと共通鍵のペアをレルム（通信グループ）毎に設定する必要があり，合計 15 である．セキュリティポリシは IKE と同様な設定が必要であり，合計 64 である．さらに各ノードと KINK を行うため，通信相手のプリンシパル名を設定する必要がある．設定項目数は通信相手の数によって異なり，合計 8 である．ゆえに KINK を利用する場合の初期設定の管理負荷はノード 1 が 18，ノード 2，3 は 21，ノード 4 は 26，KDC は 15，合計 101 である．

4.1.3　ノード増加時の管理負荷

図 4.1 の環境において通信グループ 2 に所属する端末を増加させた場合の管理負荷について評価する．図 4.3 に各方式を用いてノード数を増加させた場合の管理負荷を示す．GSCIP のノード 1 台追加による追加設定はクライアントには GE の設定，GMS には GE 情報と所属通信グループに追加するだけで良い．そのため増加量はこれらの合計 8 に比例する．IKE のノード 1 台追加による追加設定は事前共有鍵情報，セキュリティポリシ，IKE の設定が追加するノードと現存するノードに対して必要である．IKE ではすべてのノードと事前共有鍵を共有するため，ノード数を n とすると $2n^2 - 2n$ の事前共有鍵の設定が必要となる．またセキュリティポリシには通信ペアの IP アドレスの設定が必要であるため各アルゴリズムの設定に加えて，$2n^2 - 2n$ の追加設定が必要である．さらに IKE で通信相手識別子を設定する必要があり n 個の追加設定が必要である．よって追加設定項目数は 2 乗のオーダで増加する．KINK のノード 1 台追加による追加ノードの設定は，KDC との共通鍵，セキュリティポリシ，KINK の設定である．さらに現存するノードに IKE と同様なセキュリティポリシの追加，追加ノードのプリンシパルを設定する必要がある．このように IKE，KINK を利用する場合は，各ノードに対する設定項目が多く，ノード数が増加すると管理負

表 4.6　各ノードの設定項目数

GSCIP/GMS ＋ DPRP				
	GE の設定			
GES1	3			
GES2	3			
GES3	3			
GES	3			
	GE 情報	グループ鍵情報	所属通信グループ情報	合計
GMS	12	8	8	28
合計	24	8	8	40
IPsec/IKE				
	事前共有鍵情報	セキュリティポリシ	IKE	合計
Node1	2	IPsec,Transport:14	11	27
Node2	6	IPsec,Transport:14+2	13	51
		IPsec,Tunnel:16		
Node3	2	IPsec,Transport:14	11	27
SGW	2	None:8, Bypass:8	11	29
合計	12	76	46	134
IPsec/Kerberos ＋ KINK				
	KDC との共通鍵	セキュリティポリシ	KINK	合計
Node1	3	IPsec,Transport:14	1	18
Node2	5	IPsec,Transport:14+2	2	39
		IPsec,Tunnel:16	1	
Node3	3	IPsec,Transport:14	1	18
SGW	3	None:8, Bypass:8	1	20
KDC	ノードとの共通鍵：15			15
合計	14	76	6	96

荷が増大する．

4.1.4　ネットワーク構成 2 の初期管理負荷

GE の台数が 4 台であるため GMS との共通鍵の設定として各 GE にユーザ ID，共通鍵，GMS のアドレスの設定が必要となり合計 12 である．GMS には各 GE の動作モード，共通鍵の設定が必要であり合計 12 である．さらに通信グループ数は 2 であり，グループ鍵情報の設定項目として合計 8 必要となる．また各 GE が所属する通信グループは GES1，GES2，GES3 が 1 グループ，GES4 が 2 グループである．そのため所属通信グループの設定はユーザ ID と通信グループ番号のペアで 10 必要である．よって想定する環境における初期管理負荷の合計は 42 である．

GSCIP を使用して図 4.2 の環境を構築する場合を考える．ノード 1〜3 を GES1〜3，SGW を GEN と置き換え，通信グループ 1，2 をそれぞれグループ鍵 1，2 を用いて構成する．設定項目数を表 4.6 に示す．GE の台数が 4 台であるため GMS との共通鍵の設定として各 GE にユーザ ID，共

表 4.7　各ノードの設定変更数

IPsec/IKE				
	事前共有鍵情報	セキュリティポリシ	IKE	合計
Node1	1	IPsec,Tunnel:16 + 2	1	20
Node2	1	2	1	3
SGW	1	2	1	4
合計	3	22	3	27
IPsec/Kerberos ＋ KINK				
	KDC との共通鍵	セキュリティポリシ	KINK	合計
Node1	0	IPsec,Tunnel:16 + 2	1	19
Node2	0	2	0	2
SGW	0	2	1	3
合計	0	22	2	24

通鍵，GMS のアドレスの設定が必要となり合計 12 である．GMS には各 GE の動作モード，共通鍵の設定が必要であり合計 12 である．さらに通信グループ数は 2 であり，グループ鍵情報の設定項目として合計 8 必要となる．また各 GE が所属する通信グループは GES1，3，GEN が 1 グループ GES2 が 2 グループである．そのため所属通信グループの設定はユーザ ID と通信グループ番号のペアで 10 必要である．よって想定する環境における初期管理負荷の合計は 40 である．

IKE を利用して図 4.2 の環境を実現する場合の設定項目数を表 4.6 に示す．ノード 1 とノード 2 は互いにトランスポートモードのセキュリティポリシの設定が必要である．ノード 2 とノード 3 も同様にトランスポートモードのセキュリティポリシの設定が必要である．またノード 2 が SGW 配下の一般端末と通信するために，ノード 2 と SGW にトンネルモードの設定が必要になる．ゆえに IKE を利用する場合の初期設定の管理負荷は，ノード 1，ノード 3 に 27，ノード 2 に 51，SGW に 29，合計 134 である．

KINK を利用して図 4.2 の環境を実現する場合の設定項目数を表 4.6 に示す．KINK を利用する場合は IKE と異なり KDC との共通鍵と自分のプリンシパル，KDC の IP アドレスの設定が必要である．セキュリティポリシは IKE と同様な設定が必要であり，合計 76 必要である．KINK では鍵交換に必要な設定は通信相手のプリンシパルだけで良いため，合計 6 である．ゆえに KINK を利用する場合の初期設定の管理負荷は，ノード 1，ノード 3 に 18，ノード 2 に 39，SGW に 20，KDC に 15，合計 96 である．

4.1.5　ネットワーク構成変化時に発生する管理負荷

図 4.2 においてノード 1 が SGW 配下から NET1 へ移動した際に必要な設定項目を評価する．GSCIP では端末が移動してもその都度 DPRP により動作処理情報を新しく生成するため，ユーザや管理者が行う作業はいっさい発生しない．

一方，IKE で同様の変更を実現しようとすると，ノード 1 は移動により IP アドレスが変化する

表 4.8　各ノードの設定変更数

GSCIP/GMS ＋ DPRP				
	GE の設定			
GES1	3			
	GE 情報	グループ鍵情報	所属通信グループ情報	合計
GMS	3	-	2	5
合計	6	0	2	8
IPsec/IKE				
	事前共有鍵情報	セキュリティポリシ	IKE	合計
Node1	2	2	1	5
Node2	2	2	1	5
Node4	6	IPsec,Transport:14 + 2 IPsec,Tunnel:16	11 + 2	51
SGW	2	2	1	5
合計	12	38	16	66
IPsec/Kerberos ＋ KINK				
	KDC との共通鍵	セキュリティポリシ	KINK	合計
Node1	0	2	1	3
Node2	0	2	1	3
Node4	3	IPsec,Transport:14 + 2 IPsec,Tunnel:16	3	38
SGW	0	2	1	3
KDC	ノードとの共通鍵：3			3
合計	3	38	6	50

ため，通信を識別するための識別子を変更する必要がある．そのためノード 1 は自己の IP アドレスの変更と通信相手のノード 2 にも IP アドレスの変更が必要であり，合計 4 である．さらに通信グループ 1 に所属する一般端末と通信するために，SGW に対してトンネルモードの設定を追加する必要がある．その管理負荷は事前共有鍵情報，セキュリティポリシと IKE の設定で，合計 18 である．よってノード 1 の移動による管理負荷は合計 27 となる．図 4.2 の構成はシンプルであるため，SGW が 1 台しか存在しないが，ノード 1 が複数の通信グループに所属し，SGW が複数ある場合は設定による管理負荷が大きく増加する，

また，KINK で同様の変更を実現する場合は，ノード 1 は移動により IP アドレスが変化するため，IKE と同様なセキュリティポリシの変更が必要である．またノード 1 と SGW 間で KINK を利用するため，通信相手のプリンシパルをそれぞれ追加する必要がある．ゆえにネットワーク構成変化時の設定コストは合計 24 である．

4.1.6　通信グループのメンバ構成変化時に発生する管理負荷

図 4.2 において通信グループ 1 に所属するノード 4（GSCIP では GES4）を新たに NET1 上に配置する場合の管理負荷を評価する．GSCIP では管理者が GMS にて GES4 の GE 情報を追加定義す

る．その情報は GES4 のユーザ ID，動作モードおよび所属通信グループ番号のみである．GES4 は電源投入時に定義された GE 情報とグループ鍵を GMS から取得し，自動に設定される．通信を行う際には DPRP により動作処理情報を動的に決定する．よって新しく端末を追加した場合の管理負荷は GES4 の GE 情報のみで合計 8 である．

一方 IKE では，ノード 4 に事前共有鍵情報，セキュリティポリシ，および IKE の設定をノード 1，2 および SGW に対して行う必要があり，合計 51 である．さらにノード 1，2 および SGW はノード 4 に対する事前共有鍵情報，セキュリティポリシ，および IKE の設定を追加する設定する必要がある（合計 66）．実際の環境では，通信グループに多くのメンバがいることが想定されるため，さらに設定追加による管理負荷が増加する．

また，KINK を利用する場合は，ノード 4 の KDC との共通鍵と IKE を使用する場合と同様なセキュリティポリシの設定，KINK の設定として通信相手のプリンシパルの設定が必要である．ゆえに通信グループのメンバ構成変化時に発生する管理負荷は合計 50 である．

これらのことから，GSCIP は初期導入時や端末の移動，メンバの追加に伴う管理負荷がわずかであるため，FPN を実現する有効な方法であるといえる．

4.2 性能評価

GSCIP/GMS ＋ DPRP，IPsec/IKE，IPsec/Kerberos ＋ KINK の各方式を用い，2 台の端末間のネゴシエーションによるオーバヘッドと通信性能を測定した．IPsec ESP は FreeBSD に実装されている KAME [13] を使用し，ネゴシエーションアプリケーションは racoon2 [14] を使用した．また Kerberos のアプリケーション KDC には，Heimdal [15] を使用した．オーバヘッドの測定には Wireshark [16] を用いた．

1. **ネゴシエーションによる初期遅延**

   図 4.4 に各方式のネゴシエーションの測定範囲を示す．[1] ネゴシエーション時間は，最初のネゴシエーションパケットが送信されてからネゴシエーションが終了するまでの時間である．[2] 通信開始までの時間は，最初のネゴシエーションパケットが送信されてから最初の TCP/UDP パケットが送信されるまでの時間である．なお GMS ＋ DPRP および Kerberos ＋

表 4.9　オーバヘッド測定結果

	GMS ＋ DPRP	IKEv1	IKEv2	Kerberos ＋ KINK
(0) サーバとの通信時間	6.11	—	—	0.89
(1) ネゴシエーション時間	0.38	1542.72	264.09	3.07
(2) 通信開始までの時間（TCP）	1.78	3038.23	2862.15	3037.98
(2) 通信開始までの時間（UDP）	1.89	1797.16	429.92	16.03

Unit : [ms]

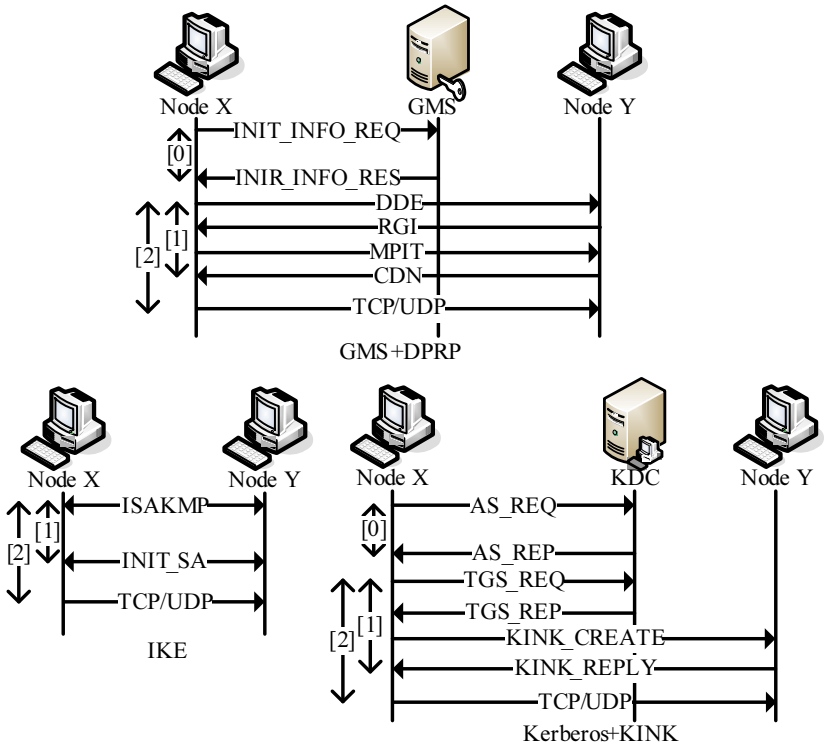

図 4.4　各方式のネゴシエーション測定

KINK は，端末起動時に [0] サーバとの通信が必要であるが，これは通信の要求が発生する前に実行されるため通信開始までの時間には含めない．オーバヘッドの測定結果を表 4.9 に示す．GMS ＋ DPRP はグループ鍵などの配送にかかるサーバとの通信時間は 6.11 ミリ秒，DPRP のネゴシエーションに 0.38 ミリ秒，通信開始までの時間は TCP で 1.78 ミリ秒となった．IKEv1 および IKEv2 は，ネゴシエーションにそれぞれ 1542.72 ミリ秒（約 1.5 秒），264.09 ミリ秒，通信開始までの時間は，TCP で 3038.23 ミリ秒（約 3 秒），2862.15 ミリ秒（約 2.8 秒）となった．Kerberos ＋ KINK はサーバとの通信時間に 0.89 ミリ秒，ネゴシエーションに 3.07 ミリ秒，通信開始までの時間は，TCP で 3037.98（約 3 秒）となった．

2. スループット

測定方法は 100BASE-TX と 1000BASE-TX の Ethernet ネットワーク環境下において Netperf [17] を用いてスループットを測定した．測定結果を表 4.10 に示す．1000BASE-TX の Ethernet ネットワーク環境下で PCCOM は 229.37Mbps，IPsec ESP は 129.42Mbps となった．

これらの測定結果から GSCIP/GMS ＋ DPRP は通信開始までの時間も短く，スループットも IPsec ESP に比べて高速であることがわかる．GMS ＋ DPRP では通信に使用する暗号鍵を事前に配送するためネゴシエーション時間が大幅に短い．IKE では通信に使用する暗号鍵をネゴシエーション中に DH 鍵交換を用い生成するため，DPRP に比べ遅い．Kerberos ＋ KINK は共通鍵をベースに通信に使用する暗号鍵を生成するため IKE に比べ早い．通信開始までの時間は GSCIP ではネゴシ

表 4.10　スループット測定結果

	Normal	PCCOM	IPsec ESP
100BASE-TX	94.14	94.14	94.14
1000BASE-TX	941.46	229.37	129.42

Unit : [Mbps]

表 4.11

	GSCIP/GMS ＋ DPRP	IPsec/IKE	IPsec/Kerberos ＋ KINK
オーバヘッド	◎	×	×
スループット	○	×	×
セキュリティ強度	○	◎/△	◎/△
NAT/FW との共存	○	×/△	×/△
	管理負荷		
1 対 1 の通信	×	◎	×
大規模システム	◎	×	△
構成変化時	○	×	△
端末移動時	○	×	△

エーションのトリガーとなったパケットをカーネルに待避させ，ネゴシエーション終了後に送信するため高速である．しかし，IPsec ではトリガーとなったパケットは破棄され，TCP の再送制御に頼っているため秒オーダの時間がかかる．

4.3　総合評価

表 4.11 に各方式の比較評価を示す．通信開始時のオーバヘッドは GSCIP では，端末起動時に通信に使用する暗号鍵を配送するため他の方式に比べネゴシエーション早い．IPsec は TCP の再送に頼って最初のパケットを送信するため，秒オーダの時間が必要である．スループットは GSCIP 独自のパケット長を変えない暗号方式 PCCOM を使用しているため，IPsec ESP に比べ高速である．PCCOM では NAT やファイアウォールと共存できる方式であるため，IP ヘッダ，TCP/UDP ヘッダが平文である．トラヒックの内容を解析される恐れがあるが，NAT とファイアウォールの共存を考えるとヘッダ部分は平文であることが必須である．しかしヘッダは完全性保証の範囲であるため改ざんの検知は可能である．IPsec ESP では TCP/UDP ヘッダが暗号化部分に含まれているため NAT やファイアウォールを通過することができない．NAT を通過するために UDP ヘッダでカプセル化する方法があるが，UDP ヘッダ部分が改ざん可能であるためセキュリティ強度が低下する．

各方式の管理負荷は大規模システムになるほど図 4.3 のように GSCIP が有効である．拠点間をつなぐため VPN で良く使用される IPsec/IKE は一対一で通信する場合は，DPRP，KINK に比べ第 3 のサーバが必要でないため，有効である．ネットワーク構成の変化や端末移動時の管理負荷は，

IPsec では IP アドレスで管理しているため管理負荷がかかる．しかし GSCIP ではグループ鍵で通信グループを管理しているため管理負荷が低い．

これらのことから我々がめざす柔軟性とセキュリティを兼ね備えた FPN を実現する方式として GSCIP/GMS ＋ DPRP は有効な手段である．

第5章　むすび

本稿では FPN を実現するための GSCIP の概要とその管理方法を示した．GSCIP を管理するグループ管理サーバの実装を行い，特定のネットワーク構成を想定して GSCIP を運用する場合と IPsec を運用する場合の管理負荷について評価した．この結果，GSCIP では管理負荷を抑えつつ運用が可能であることを示した．特にノード数が増加する場合に GSCIP は有効であり，大規模なネットワーク環境でも利用できる．今後は，イントラネットのみならずインターネット空間でも GSCIP を運用出来るような GMS の分散化や連携を検討し，有効性を確認する．

謝辞

本研究を遂行するにあたり，多大なる御指導そして御協力を頂きました，名城大学大学院理工学研究科　渡邊晃教授に心より厚く御礼申し上げます．

本研究を遂行するにあたり，多大なる御指導そして御協力を頂きました，名城大学大学院理工学研究科　柳田康幸教授，宇佐見庄五准教授に心より厚く御礼申し上げます．

本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，名城大学理工学研究科情報科学科渡邊研究室の鈴木秀和氏，後藤裕司氏に心より感謝いたします．

また本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，名城大学理工学研究科情報科学科渡邊研究室の皆様に心より感謝いたします．

参考文献

[1] NPO 日本ネットワークセキュリティ協会：2007 年度情報セキュリティインシデントに関する調査報告書 Ver.1.5. http://www.jnsa.org/.

[2] Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).

[3] 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 (2006).

[4] Kent, S.: IP Authentication Header, RFC 4302, IETF (2005).

[5] Kent, S.: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).

[6] Harkins, D. and Carrel, D.: The Internet Key Exchange (IKE), RFC 2409, IETF (1998).

[7] Kaufman, C.: Internet Key Exchange (IKEv2) Protocol, RFC 4306, IETF (2005).

[8] Sakane, S., Kamada, K., Thomas, M. and Vilhuber, J.: Kerberized Internet Negotiation of Keys (KINK), RFC 4430, IETF (2006).

[9] Maughan, D., Schertler, M., Schneider, M. and Turner, J.: Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, IETF (1998).

[10] Neuman, C., Yu, T., Hartman, S. and Raeburn, K.: The Kerberos Network Authentication Service (V5), RFC 4120, IETF (2005).

[11] 増田真也，鈴木秀和，岡崎直宣，渡邊　晃：NAT やファイアウォールと共存できる暗号通信方式 PCCOM の提案と実装，情報処理学会論文誌， Vol. 47, No. 7, pp. 2258–2266 (2006).

[12] 束　長俊，鈴木秀和，渡邊　晃：非接触型 IC カードを用いた認証方式 SPAIC の提案，マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム論文集，Vol. 2007, No. 1, pp. 1332–1337 (2007).

[13] The KAME project: KAME. http://www.kame.net/.

[14] The Racoon2 Project: Racoon2. http://www.racoon2.wide.ad.jp/.

[15] The Heimdal: Heimdal. http://www.h5l.org/.

[16] The Wireshark: Wireshark. http://www.wireshark.org/.

[17] The Netperf: Netperf. http://www.netperf.org/.

研究業績

学術論文

なし

国際会議

1. K. Imamura, H. Suzuki and A. Watanabe, “A Proposal for a Remote Access Method using GSCIP and IPsec,” Proceedings of the IEEE International Region 10 Conference 2007 (TENCON2007), WeCM-O4.2, 219, pp.1–4, Taipei, Taiwan, Oct. 2007.

国内会議

1. 今村圭祐, 鈴木秀和, 後藤裕司, 渡邊晃, “セキュア通信アーキテクチャ GSCIP を実現するグループ管理サーバの実装と運用評価,” マルチメディア, 分散, 協調とモバイル（DICOMO2008）シンポジウム論文集, Vol.2008, No.1, pp.1516–1522, Jul. 2008.
2. 今村圭祐, 鈴木秀和, 渡邊晃, “GSCIP と IPsec を併用したリモートアクセス方式の提案と評価,” マルチメディア, 分散, 協調とモバイル（DICOMO2007）シンポジウム論文集, Vol.2007, No.1, pp.468–472, Jun. 2007.

研究会・大会等

1. 今村圭祐, 鈴木秀和, 渡邊晃, “GSCIP と IPsec を併用したリモートアクセス方式の提案,” 電子情報通信学会 2007 年総合大会講演論文集, B-7-134, p.224, Mar. 2007.
2. 今村圭祐, 伊藤将志, 渡邊晃, “GSCIP と IPsec を併用したリモートアクセス方式の提案,” 平成 18 年度電気関係学会東海支部連合大会論文集, O-425, Sep. 2006.

受賞歴

1. 2007 年 7 月　マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム　ヤングリサーチャー賞