通信アーキテクチャ GSCIP の管理運用評価

村　橋　孝　謙

Evaluation of management and use of communication architecture GSCIP

TAKANORI MURAHASHI

組織においてネットワーク内部の端末に自由にアクセスすることを許可すると，内部関係者による情報漏洩などの問題が発生する可能性がある．通信グループを定義する方法は，この問題を軽減するのに有効である．通信グループを構築する既存技術として IPsec があるが，管理が煩雑になるという課題がある．我々は柔軟なグルーピングを実現する技術として GSCIP を提案している．GSCIP では IP アドレスに依存しないグルーピングを実現でき，IPsec に比べ管理負荷が小さい．そこで特定のネットワーク構成を仮定し，IPsec と GSCIP の設定項目数を定量的に比較することにより GSCIP の有効性を確認する．

1. はじめに

組織内のネットワークは，外部からの侵入対策としてはファイアウォール，デジタル署名など多くの対策がなされているが，ネットワーク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認証が行われている程度であることが多く，内部関係者からの情報漏洩が危惧される．そこで部門等に応じた通信メンバのグループを定義し，グループメンバの認証と暗号化通信を行うことはセキュリティの確保に有効である．通信グループを実現できる既存技術として IPsec（Security Architecture for Internet Protocol）[1]が挙げられるが，IPsec で使用される鍵交換プロトコル IKE（Internet Key Exchange）[2]では設定項目が多い．また IPsec では通信ペア毎に端末に設定を行う必要があるため，管理負荷が大きくなるという課題がある．ドメイン単位に IPsec を適用する方法としてトンネルモードがあるが，端末毎の細かな通信グループの定義が困難である．IPsec では端末が移動しシステム構成が変化したときは，構成を再定義するために再度設定を行う必要がある．また端末単位で IPsec を適用する場合はトランスポートモードを使用するが，トンネルモードとトランスポートモードは互換性が無いため，これらを併用することは困難となる．

我々が提唱している通信アーキテクチャ GSCIP（Grouping for Secure Communication for IP）[3]では，通信グループと暗号鍵を１対１に対応させることにより，管理者が容易に通信グループの定義を行うことができる．GSCIP では通信グループの定義は IP アドレスに依存しないため，端末が移動しシステム構成が変化した

場合でもグループ構成の再定義が不要である．これにより IPsec では難しかった端末単位およびドメイン単位の混在した通信グループの構築が容易に可能となる．

本稿では，特定のネットワークモデルを想定し，IPsec および GSCIP によりセキュリティ対策を行った場合の管理負荷を定量的に比較し，GSCIP の有効性を検証した．

以降，２章で IPsec および GSCIP の概要について述べる．３章で各方式を用いた場合の管理負荷について述べ，４章で評価し５章でまとめる．

2. 既存技術

2.1 IPsec

IPsec は暗号化と認証により IP パケットを安全に運ぶための技術である．IPsec で使用されるセキュリティプロトコル ESP（Encapsulating Security Payload）[4]では IP パケットの暗号化が可能であり，IKE と組み合わせて使用することでパケットの改ざんに対する検知も可能である．これを用いることで情報漏洩を防ぐことが可能となる．

IPsec では暗号化方式等を定めた SA（Security Association）を通信端末間で共有する．SA の管理を手動で行うことは管理負荷やセキュリティの問題上好ましくないため，多くの場合は IKE が使用される．IKE は SA の自動的な生成，管理を行う．図１に IKE の動作シーケンス[5]を示す．IKE の動作は２つのフェーズに分けられる．フェーズ１では IKE の制御信号を安全にやりとりするための ISAKMP SA を生成する．これは ISAKMP SA 生成要求とその受諾，安全な暗号鍵の共有を実現する 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によって完成する．またフェーズ２では，フェーズ１で生成した ISAKMP SA を使用して IPsec SA を生成する．これにより相手認証と暗号化を実現することができる．

図１に示すように IPsec は通信ペアとして定義されており，通信グループの定義は IP アドレスに依存するため，必要となる全ての通信ペアに対しての設定が必要である．また IKE は暗号化アルゴリズム，認証アルゴリズム，パケットの処理方法等の必要な設定項目が多く，設定端末数が増加すると大幅に設定にかかる負荷が増大する．

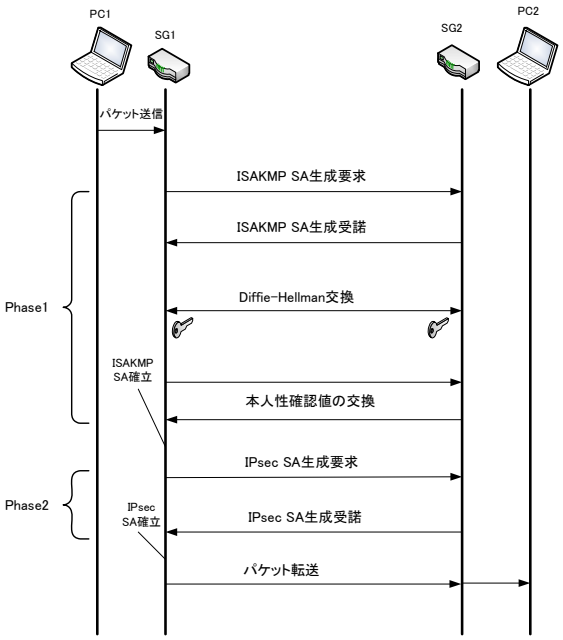

図１　IKE の動作シーケンス

2.2 GSCIP

2.2.1 GSCIP概要

GSCIP はセキュリティと柔軟性を兼ね備えた通信グループを構築するためのアーキテクチャの名称である．基本的な GSCIP を用いた通信グループの構成を図２に示す．GSCIP におけるグループ構成要素を GE（GSCIP Element）と呼ぶ．GE には各端末に機能を実装して使用するソフトウェアタイプの GES（GE realized by Software），ルータに機能を実装する GEN（GE for Network），重要なサーバの直前に設置しサーバに変更を加えずとも GES の機能を実現する GEA（GE realized by Adapter）がある．GSCIP では同一の暗号鍵を所有する GE を同一のグループに属するメンバとして考える．この暗号鍵をグループ鍵 GK（Group Key）と呼ぶ．

このようにグループ鍵と通信グループを１対１に対応させる仕組みにより，IP アドレスに依存しない通信グループを定義することが可能となる．同一グループ間の通信はグループ鍵 GK を用いた認証と暗号化が行われる．グループ外の端末との通信においては，管理者の設定により平文での通信または通信の禁止を選択することができる．グループ外の端末との通信は，一般にはクライアントは平文での通信が可能な開放モード，GEN や GEA はグループ外との通信を一切拒否する閉域モードが選択される．

GSCIP は，各 GE と管理サーバ GMS（Group Management Server）[6]によって実現される．GMS は各 GE の動作モードやグループ鍵の配送，グループ鍵の管理や GE と通信グループ番号の関連付けなどを行う．

グループ鍵 GK は通信グループに応じて生成され，定期的に更新を行う． GSCIP では通信の開始に先立ち，独自のプロトコル DPRP（Dynamic Process Resolution Protocol）[7]を実行し，通信経路上に存在する GE 同士の認証と動作処理情報の生成を行う．

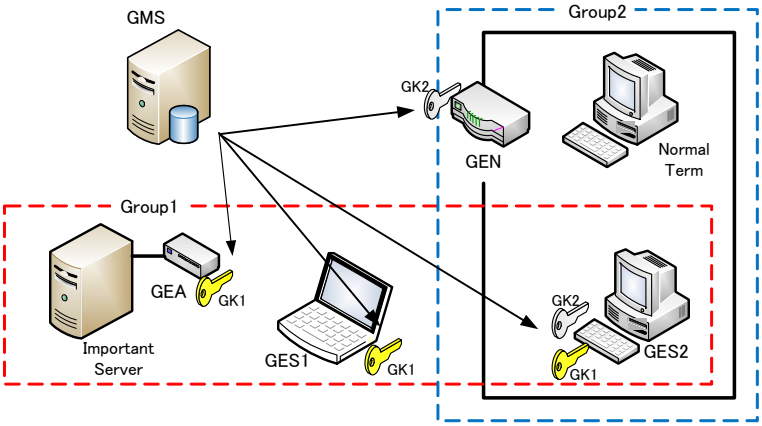

図２　GSCIP によるグループ構築例

2.2.2 DPRP概要

DPRP は GSCIP において，位置透過性すなわちネットワーク構成の変化時にも通信を可能とする機能を持つものである．

DPRP では, GE がネットワーク構成を学習することで動作処理テーブル PIT（Process Information Table）を生成し，各 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，動作処理情報等が記述されている．

パケット送信時には，PIT が既に存在するかを確認し，存在しない場合にはパケットを一旦カーネルに退避させ DPRP により PIT を生成する．図３に DPRP の動作シーケンスを示す．

PIT 生成時にはまず，終点 GE を探索するために DDE（Detect Destination End GE）と呼ばれる制御パケットを送信する．これには送信側および受信側の IP アドレス，ポート番号，プロトコル情報が含まれる. これに対し, 受信側の端末は RGI（Report GE Information）と呼ばれる制御パケットを返送する．RGI には各 GE の通信グループ, 動作モード, グループ鍵情報, 認証情報が含まれ，経路上の GE 情報をパケットに追加しながら始点 GE を探索する．これらにより始点 GE および終点 GE が確認されると，始点 GE は MPIT（Make Process Information Table）を送信し，受信した経路上の GE および終点 GE は MPIT に含まれる情報から PIT を仮生成する．終点 GE が MPIT を受信すると, 始点 GE へ CDN（Complete DPRP Negotiation）を送信しネゴシエーションの完了を通知する．CDN を受信した各 GE は，仮生成した PIT を確定する．これにより今後の PIT に従った暗号化通信が可能となる．

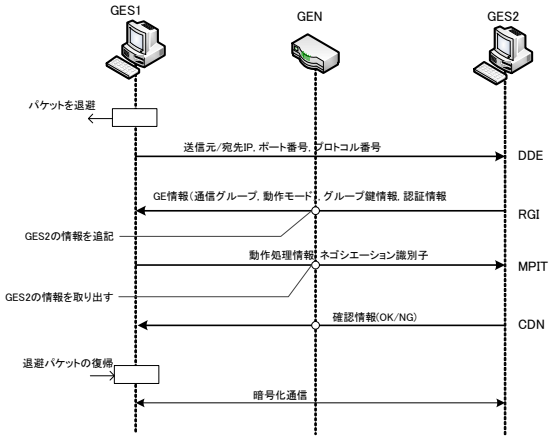

図３　DPRP の動作シーケンス

3. 管理負荷の比較

3.1 小規模システムの場合

GSCIP/DPRP および IPsec/IKE により通信グループを構築した場合の管理負荷を比較した．各ノード，サーバでの設定１項目あたりの管理負荷を１とし，設定項目数による管理負荷の違いを求めた．図４に示す最も簡単なグループ構成を想定する．ノード１，４がグループ１に，ノード２～４がグループ２に属している．GSCIP ではノード１～４が GES１～４に対応する．また IPsec の場合はグループ内の各ノード間でそれぞれトランスポートモードを使用した暗号化通信を行うものとする．いずれの場合もグループ定義は管理装置で行い，その設定情報を各ノードに配送するものと

する．管理装置と各ノードとの間は確実な認証と暗号化通信がされていることを前提とし，既存技術である PKI（Public Key Infrastructure）等を使用することを想定する．GSCIP/DPRP および IPsec/IKE の直接的な比較には影響しないため，管理装置と各ノード間との管理負荷は比較対象から除外する．また各ノードへの設定とは別に管理装置に設定すべき項目が存在するが，GE の台数によって設定項目数が変化しない項目については設定項目数の計算から除外した．また IKE においてノード数による設定項目数の変化にあまり影響のない項目についても比較から除外する．

GSCIP では GE ごとに２の設定が必要である．具体的には GE は動作モード，グループ番号を設定するだけで良い．よって GSCIP では合計８の設定が必要である．

IPsec では通信ペアごとに３の設定が必要となる．具体的には通信ペアとなる２台のノードの IP アドレス及び処理内容である．通信ペア数はグループ１で１，グループ２で３であるため，合計 12 の設定が必要である．

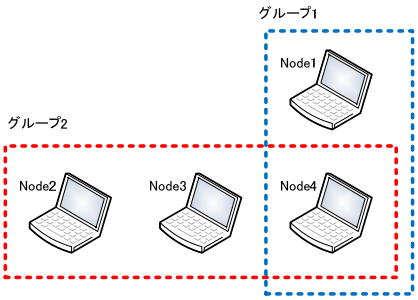

図４　想定するネットワーク構成

3.2 大規模システムの場合

図４の構成からグループ１のみに属するノードとグループ２のみに属するノードを同時に１台ずつ増加させた場合の構成において必要となる設定項目数を示す．GSCIP では追加ノードごとに動作モード，グループ番号の設定を行うだけで良いので，ノードが１台増えるごとに設定項目は２だけ増加する．

IPsec/IKE の場合は想定される通信ペアの数だけ設定が必要となる．そのためノード数が増加すると設定項目数が指数関数的に増大する．ノード追加時の設定項目数の変化を図５に示す．

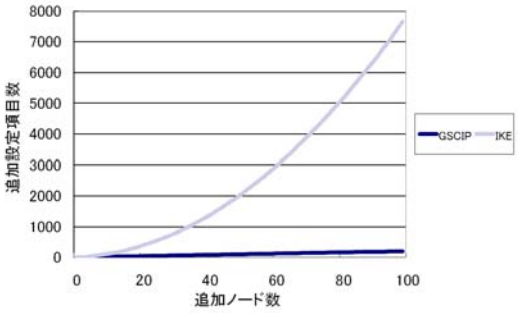

図５　ノード追加時の設定項目数の変化

3.3 システム構成変化時

システム構築後，ノードが移動して IP アドレスが変化した場合を考える．GSCIP ではグループ定義と IP アドレスが独立しており，設定負荷は発生しない．それに対し IPsec では移動したノードとその通信ペアとなる全てのノードの設定を変更しなければならない．すなわち，ノードの移動時には１台移動するごとに，移動したノードの所属する通信グループ内のノードの

数だけ設定の変更が必要となる．

3.4 個人単位･ドメイン単位の混在時

IPsec には個人単位で設定するトランスポートモードとドメイン単位で設定するトンネルモードの互換性がないため，両方式の混在時には双方それぞれの設定が必要となる．図６に示す構成を考える．

ノード１から３およびノード４から６は，それぞれ個人単位のグループに属している．またグループ１にノード１から３，グループ２にノード４，５が属しておりグループ間の通信が可能であるとする．

IPsec の管理負荷を考える．ここでは個人単位の通信ペアが６組あるため，合計 18 の設定が必要である．また IPsec ではグループ毎に IPsec 装置を別途用意する必要があり，装置間のペアが１組なので３の設定が必要である．これより IPsec における設定項目数の合計は 21 である．

次に GSCIP の管理負荷を考える．図６では６のノードがあり，それぞれに２の設定が必要なため，GSCIP 全体では 12 の設定が必要である．

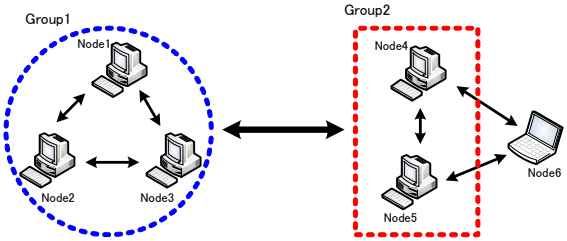

図６　混在環境の構成例

4. 評価

小規模なシステム構成の場合，GSCIP および IPsec において管理負荷にあまり差はない．図５にある通り IKE に必要な設定項目はノード数の増加に応じて指数関数的に増大するが，小規模のシステム構成においてはあまり影響がないといえる．また逆に大規模なシステム構成の場合は，IPsec を使用した場合の管理負荷が非常に高くなり運用が困難である．大規模な構成時において GSCIP を使用した場合は IPsec に比べ管理負荷が非常に小さく，セキュリティの実現が容易だといえる．

ノードが移動して IP アドレスが変化した場合，IPsec では IP アドレスが変化する度にグループ内の全てのノードの設定を変更する必要があるため，グループ内に頻繁に移動するノードがあるとき IPsec を用いた運用は困難となる．

個人単位とドメイン単位のグループの混在時では，図６の構成では管理負荷に大きな差は無かった．一般的な環境ではドメイン単位よりも個人単位のペア数の方が多いことを推定すると，混在環境においても管理負荷は個人単位のペア数に強く影響されると考えられる．

5. まとめ

本稿では特定のネットワーク構成を想定して，GSCIP と IPsec をそれぞれ用いてグループ通信を行う場合に発生する管理負荷について比較した．その結果，GSCIP は IPsec に比べ小さな管理負荷に抑えられることを示した．今後はより複雑な通信モデルにおける比較を行う．また KINK（Kerberized Internet Negotiation of Keys）[8] など，他の方式を含めた比較評価を行う．

参考文献

[1] S. Kent and K. Seo, “Security Architecture for the Internet Protocol “RFC4301, IETF, December. 2005

[2] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)” RFC2409, IETF, Nov. 1998

[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, 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

[4] R. Atkinson, “IP Encapsulating Security Payload (ESP)” RFC1827, IETF, Aug. 1995

[5] Hoffman, P.: Algorithms for Internet Key Exchange version 1(IKEv1), RFC4109 (2005).

[6] 今村圭佑, 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 pp. 1516 - 1522

[7] 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)

[8] Neuman, C., Yu, T., Hartman, S. and Raeburn, K: The Kerberos Network Authentication Service (V5),RFC4120 (2005)