通信アーキテクチャ CGSCIP の管理運用評価

村橋 孝謙[†1]　鈴木 秀和[†2]　渡邊 晃[†2]

企業などの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．

Evaluation of management and use of communication architecture GSCIP

TAKANORI MURAHASHI[†1]　HIDEKAZU SUZUKI[†1†2]
AKIRA WATANABE[†1]

Allow free access to internal network devices, organizations may cause information leakage by insiders. How to define communication groups is effective in reducing this problem. Existing technology to build a communication group that the IPsec have become complex management challenge. We are a technology that enables flexible grouping has been proposed GSCIP. GSCIP grouping can be achieved independent of the IP address, IPsec is lightly loaded compared to control. We assume a particular network configuration, IPsec GSCIP and quantitatively by comparing the number of configuration items to verify the validity of GSCIP.

1. はじめに

組織のネットワークは，外部からの侵入対策としてはファイアウォール，デジタル署名など確実な対策がなされている．しかし，組織内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．そこで部門やプロジェクトなど業務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．

安全な通信グループを実現できる既存技術の代表として IPsec[1]が挙げられる．個人単位に通信グループを実現するトランスポートモードではきめ細かい通信グループの定義が可能な反面，全ての通信ペアについて設定を行う必要があるため，グループの規模が大きくなると管理負荷が多くなる．サブネット単位に通信グループを定義するトンネルモードではセキュリティゲートウェイのみに設定を行えば良いため管理負荷は小さくなるが，個人単位のような小さなグループの構築は困難である．また両者の利点を生かすため個人単位とグループ単位の混在した環境を実現しようとすると，トランスポートモードとトンネルモードの互換性がないため設定は複雑になる．

我々は，GSCIP（Grouping for Secure Communication for IP）[2]と呼ぶ通信アーキテクチャを提案している．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．

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. 通信グループの構築方法

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．IKE（Internet Key Exchange）[3]では暗号鍵の自動交換を行い，ESP（Encapsulating Security Payload）[4]では IP パケットの暗号化とパケットの改ざん検知が可能である．

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 の設定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 を共有する．以上の

[†1] 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
[†2] 名城大学理工学部
Faculty of Science and Technology, Meijo University

手順により相手認証と暗号化通信の準備ができる．

IPsec で使用される鍵交換プロトコル IKE および暗号化通信プロトコル ESP は汎用性を重視したため，設定項目が多い．また IPsec では通信ペア毎に設定を行う必要があるため，大規模なシステムにおいては管理負荷が大きい．通信ペアの指定は IP アドレスで行うため，端末が移動すると設定を変更する必要がある．サブネット単位に IPsec を適用するトンネルモードと端末単位に IPsec を適用するトランスポートモードの間に互換性が無いため，これらを併用すると管理負荷が更に増加する．

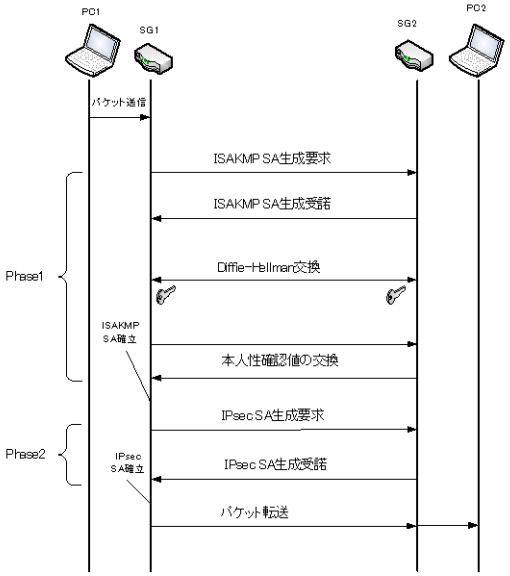


図 1　IKE の動作シーケンス

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．GSCIP を用いた通信グループの構成例を図 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．

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を許可する開放モードか，通信を一切禁止する閉域モードを選択することができる．一般にはクライアントは開放モード，GEN や GEA は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）によって実現される．[5] GMS は通信グループおよび各 GE の動作モードを定義する．GMS と各 GE の間の認証には PKI（public key infrastructure）など既存の認証技術を使用して確実な認証を行うものとする．GMS は各 GE に対しグループ番号，動作モードおよびグループ鍵をあらかじめ配送しておく．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．各 GE では通信の開始に先立ち，独自のプロトコル DPRP（Dynamic Process Resolution Protocol）[6]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．

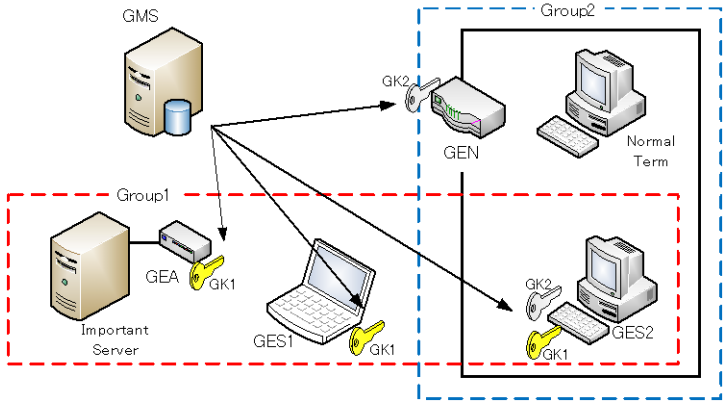


図 2　GSCIP によるグループ構築例

2.2.2 DPRP

DPRP は通信開始時に通信経路上の GE がグループ番号と動作モードを交換し，動作処理テーブル PIT（Process Information Table）を動的に生成する．PIT には送信元/宛先の IP アドレスとそれに対応した動作処理情報が記述される．

図３に DPRP の動作シーケンスを示す．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送信パケットを一旦カーネル内に退避させ DPRP を実行する．まず，終点 GE を探索するために DDE（Detect Destination End GE）と呼ぶ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，プロトコル番号を記述する．これに対し，受信側の端末は RGI（Report GE Information）と呼ぶ制御パケットを返送する．RGI には各 GE に配送されていた通信グループ番号，動作モードを記述する．経路上の GE は RGI に自らの設定情報を追加していく．始点 GE は RGI を受信すると，取得した情報から各 GE の動作処理情報を決定し，その内容を MPIT（Make Process Information Table）に記述して終点 GE に送信する．MPIT を受信した経路上の GE および終点 GE は MPIT に含まれる情報から自らの 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．始点 GE は退避していた通信パケットを元に戻し，PIT の内容に従って処理した後送信する．以降の通信パケットは PIT の内容に従って処理される．このように DPRP では GEN と GES 間の動作に互換性を持たせていり，サブネット単位と個人単位の通信グループを容易に構築できるようになっている．

3. 管理負荷の比較

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定量的に比較した．以下クライアントとサーバをまとめてホスト，ホストとルータをまとめてノードと呼ぶ．各ノードでの設定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．

3.1 個人単位の通信グループの場合

図４に示すようなクライアント／サーバシステムを想定する．IPsec ではサーバとクライアント間は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．GSCIP では全てのホストが GES の昨日を搭載し，同一のグループに属するものとする．いずれの場合もグループ定義は管理装置で行い，その設定情報を各ホストに配送するものとする．管理装置と各ホストとの間は確実な PKI（Public Key Infrastructure）

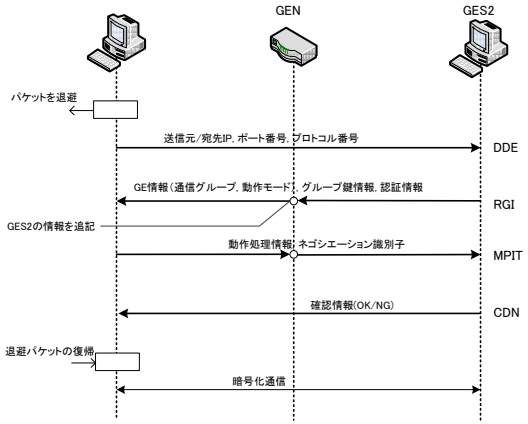


図３　DPRP の動作シーケンス

等の既存技術により認証と暗号化通信がされることを前提とする．管理装置と各ホスト間との通信に関わる管理負荷は GSCIP/DPRP および IPsec/IKE の直接的な比較には影響しないため，今回は比較対象から除外する．ESP，IKE では汎用性を重視して設定に必要な項目が多いが，通信グループの定義に関係しない内容は設定項目数の計算から除外した．

GSCIP ではホストごとに２項目の設定が必要である．具体的には動作モードとグループ番号を指定する．IPsec ではホストごとに３項目の設定が必要となる．具体的には通信ペアの相手となるノードの IP アドレス，処理内容および指定した通信相手以外との通信における処理内容である．

サーバ数を m，クライアント数を n としたとき，IPsec における管理負荷はサーバとクライアントがそれぞれ通信ペアを確立する必要があるため，$m \times n \times 3$ の式で求められる．それに対し GSCIP では各サーバおよびクライアントに対し 2 項目を設定するので，システム全体の管理負荷は $(m+n) \times 2$ の式で求められる．

通信グループ内のサーバ数が１台，３台，５台のとき，クライアントの数を１台から 100 台まで変化させた場合について管理負荷を比較した結果を図５に示す．

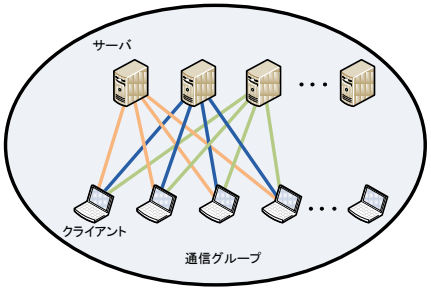


図４　クライアント／サーバシステムの例

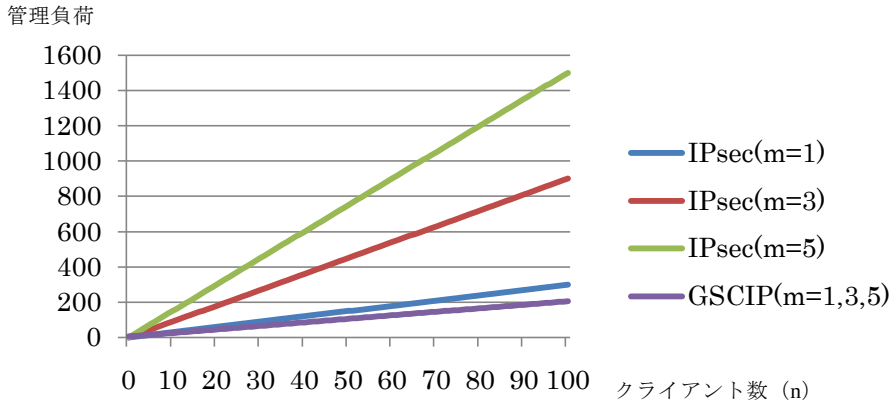


図５　個人単位の通信グループにおける管理負荷

サーバが１台の時は IPsec と GSCIP の管理負荷はほぼ同一であるが，同一グループ内のサーバの数が増加すると IPsec では管理負荷が比例して増加する．これは通信ペアごとの設定が必要であることに起因している．

3.2　端末が多重帰属する場合

図６（a）に通信グループが独立して２つ存在している場合を示す．このときグループ２に属する特定のクライアントが，グループ１に多重帰属する場合を考える（図６(b)）．ここで新たに必要となる設定数を IPsec および GSCIP において比較する．

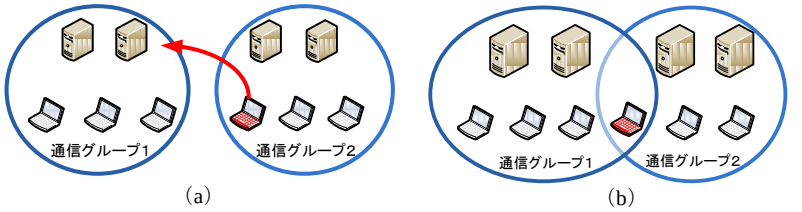


図６　多重帰属の例

IPsec では，クライアント１台を他グループにも帰属させるごとに，新たに接続するサーバの IP アドレス，処理内容を追加する．すなわち，新たに加入するグループ内のサーバ数を m，重複させるクライアント数を n とすると追加設定にかかる管理負荷は，$m \times n \times 2$ となる．それに対し GSCIP では，重複させるクライアントに新たに所属するグループ番号を追加するため，管理負荷は n となる．新たに所属するグループ内のサーバ数が１台，３台，５台のとき，重複帰属させるクライアントの数と追加設定にかかる管理負荷の関係を図７に示す．IPsec では増加する通信ペアを全て追加定義するが，GSCIP は重複帰属するクライアントのグループを追加するだけで良いため，IPsec に比べ管理負荷が小さくなる．

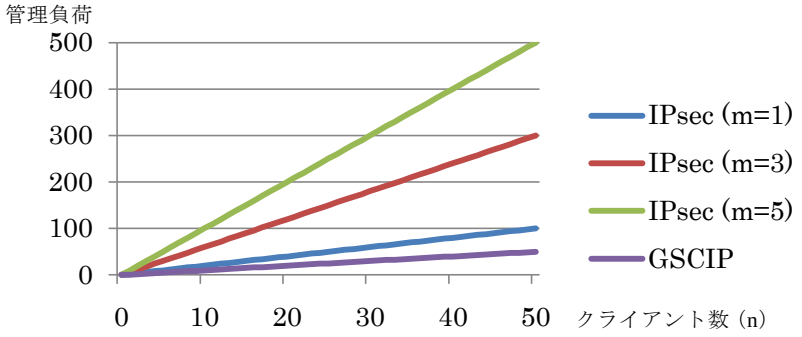


図７　端末が多重帰属する場合に追加される管理負荷

3.3　クライアントが移動する場合

システム構築後，クライアントが移動して IP アドレスが変化した場合を考える．IPsec では移動したクライアントとその通信ペアとなる全てのサーバの設定を変更しなければならない．すなわち，クライアントの移動時には１台移動するごとに，移動

したクライアントの所属する通信グループ内のサーバの数だけ設定の変更が必要となる．クライアント移動時にかかる管理負荷は，グループ内のサーバ数を m，移動するクライアントの数を n とすると， $m \times n \times 3$ の式で表すことができる．それに対し GSCIP では，グループの定義は IP アドレスに依存しないため設定負荷は発生しない．サーバ数が 1 台、3 台、5 台のときの移動クライアント数と管理負荷の関係を図 8 に示す．

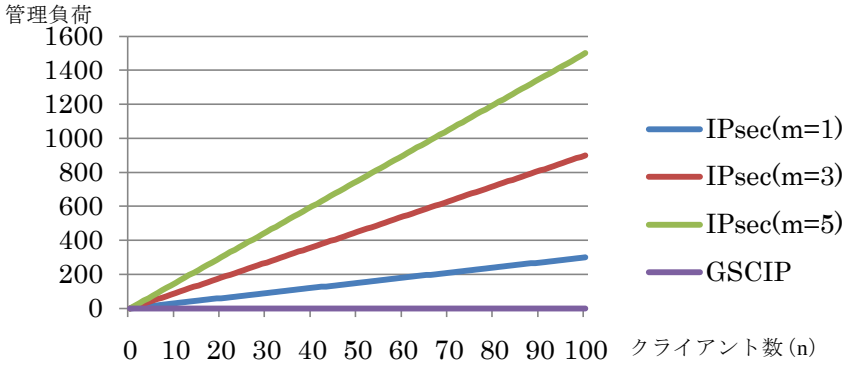


図 8　クライアントが移動する場合の管理負荷

3.4　サブネット単位の通信グループの場合

IPsec および GSCIP において，サブネット単位に相互に通信を許可する設定を行う場合について考える．図 9 のようなサブネット単位の通信において，IPsec ではサブネット毎に存在するルータ同士をトンネルモードを使用してマトリクス状に結合する．GSCIP においては 2.2.1 節に示した GEN を使用し，各 GEN にグループ番号を設定する．

システム全体のサブネット数を n としたとき，IPsec においては全てのサブネット同士の設定を行うため，必要な管理負荷は $n \times (n-1) \div 2 \times 3$ である．これに対し，GSCIP では各 GEN を全て同一グループとする設定を行うので，管理負荷は $m \times 2$ である．このときの IPsec および GSCIP におけるグループ数と管理負荷の関係を図 10 に示す．

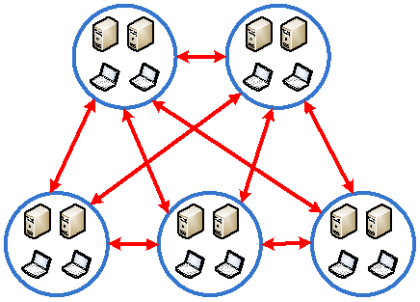


図 9　グループ単位のシステム構成例

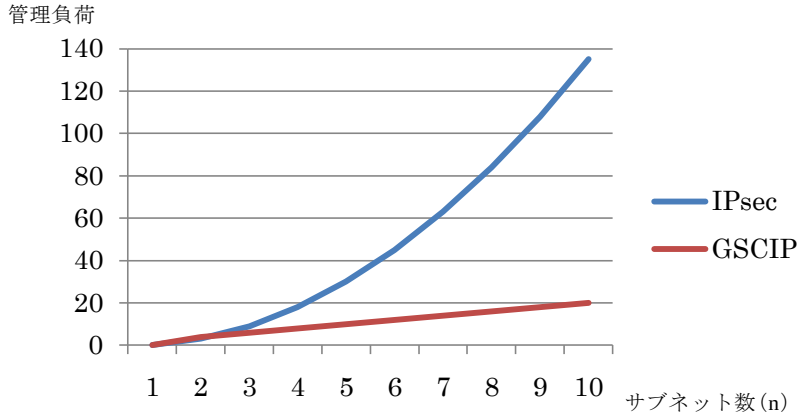


図 10　サブネット単位の通信グループにおける管理負荷

4.　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 をそれぞれ用いて通信グループを構築する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）[7]など，他の通信グループ構築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] 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
[3] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)” RFC2409, IETF, Nov. 1998
[4] R. Atkinson, “IP Encapsulating Security Payload (ESP)” RFC1827, IETF, Aug. 1995
[5] 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
[6] 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)
[7] Neuman, C., Yu, T., Hartman, S. and Raeburn, K: The Kerberos Network Authentication Service (V5),RFC4120 (2005)

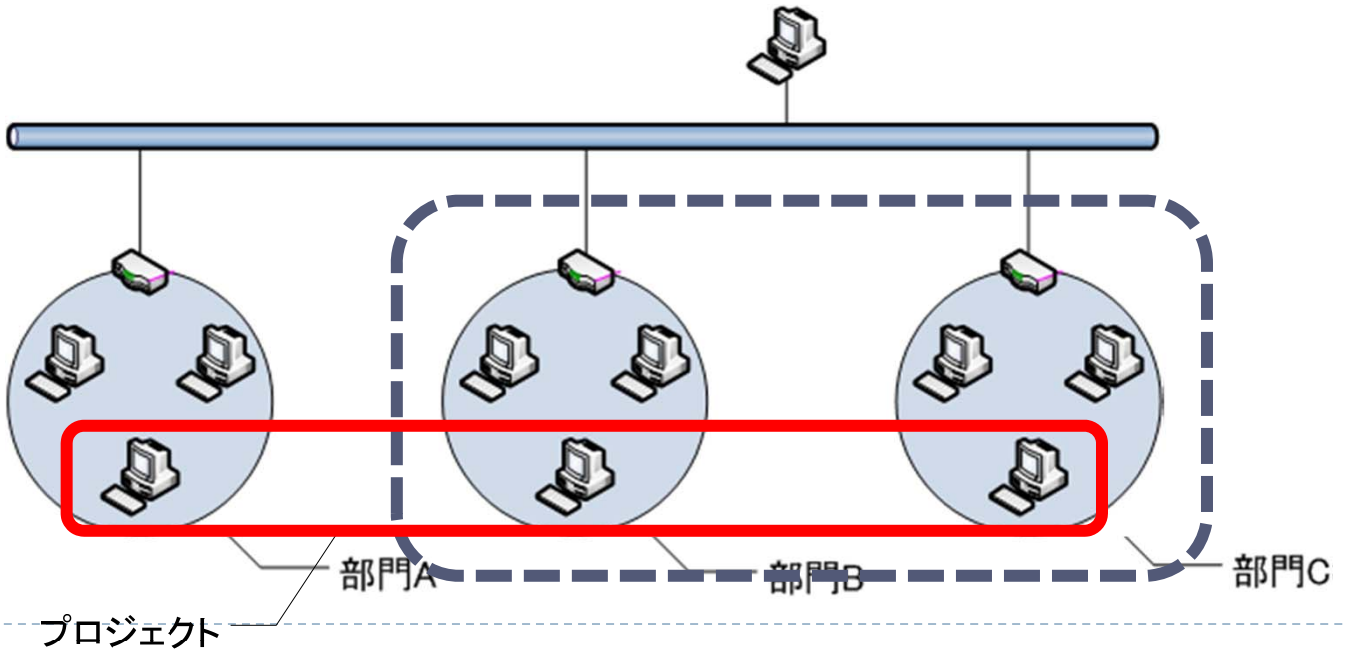
通信アーキテクチャGSCIPの管理運用評価

名城大学大学院　理工学研究科
村橋 孝謙　鈴木秀和　渡邊晃

研究背景

- ネットワークにおける，組織内部の関係者による情報漏洩の問題
  - 重要なサーバ等：ユーザ名，パスワードによる認証がほとんど

部門・役職・プロジェクト単位の通信グループ



研究背景

- 通信グループの定義

  確実な通信相手の認証　　通信の暗号化

- セキュリティを確保したグルーピング技術
  - IPsec（IKE, KINK）
  - GSCIP
    （Grouping for Secure Communication for IP）
    - 管理負荷の比較を行う

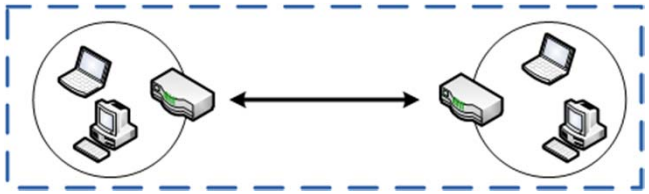
既存技術 - IPsec

- IP層で定義されたセキュリティプロトコル
- アプリケーションに依存しない

個人単位に実現

IPsecトランスポートモード
- プロジェクト単位のグルーピング
- １対１の通信ペア定義のため、規模が大きくなると管理負荷が増大

ドメイン単位に実現



IPsecトンネルモード
- 部門単位のグルーピング
- 細かい通信グループの定義が困難

互換性がなく，混在環境の実現は困難

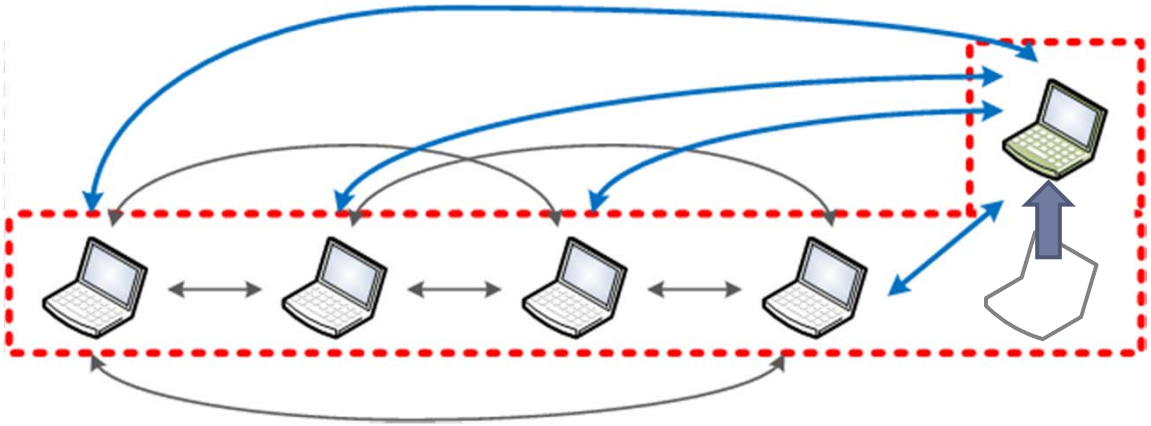
既存技術 - IPsec

- IPsec動作
  - IKE[1], KINK[2]（通信開始時の認証）

全ての通信ペアに対して設定が必要

ノード移動時に再設定が必要

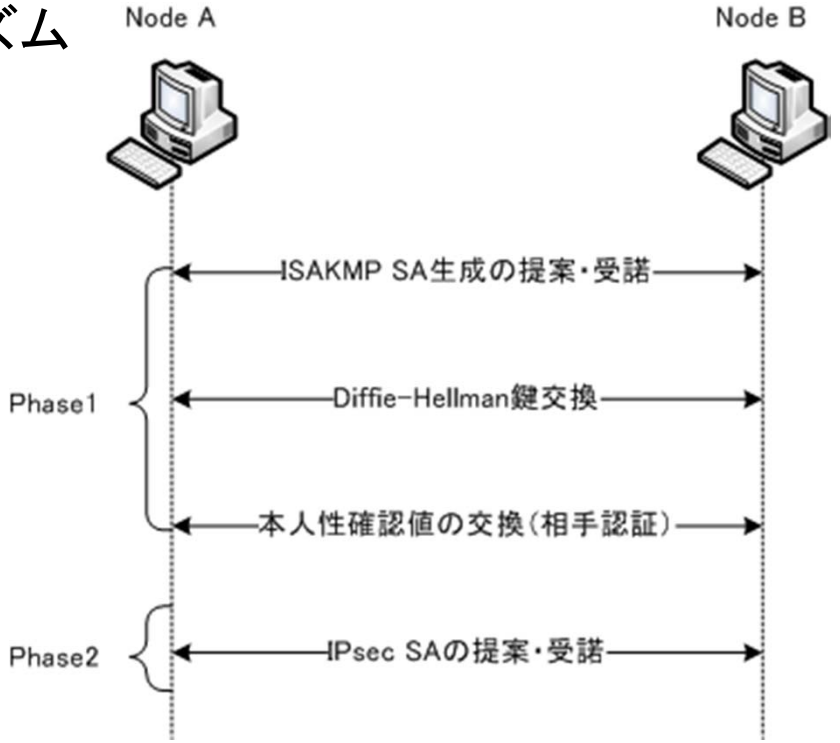
設定項目が多い



1 : IKE (Internet Key Exchange)
2 : KINK(Kerberized Internet Negotiation of Keys)

通信開始時の認証 - IKE (Internet Key Exchange)

- 最も一般的な鍵交換プロトコル
  - 自動的なSA（Security Association）の生成・管理
- 動作モード，認証方式，鍵交換アルゴリズム
  暗号アルゴリズム，認証アルゴリズム等
- 多台数間の設定にかかる負荷が大きい

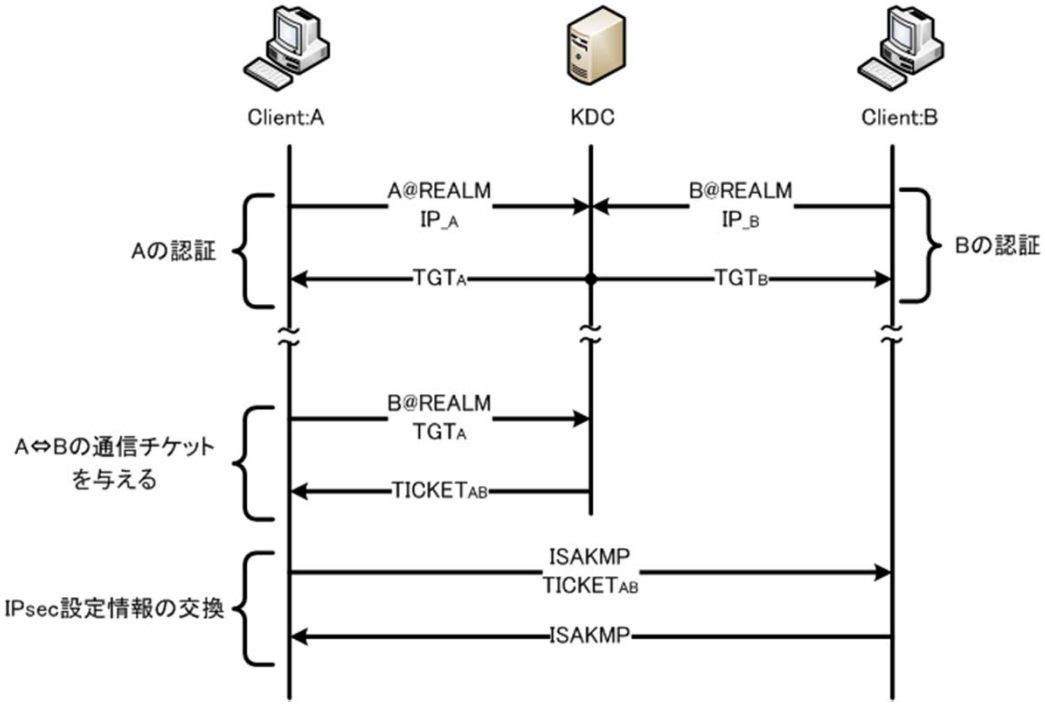


通信開始時の認証 – KINK (Kerberized Internet Negotiation of Keys)

- Kerberosの認証機構を使用したSA交換手法
  - KINKサービスチケットを使用した認証

1. ログイン時にクライアントの情報登録，TGTの取得
2. Bと通信するための$TICKET_{AB}$を取得
3. $TICKET_{AB}$を提示してSAを設定

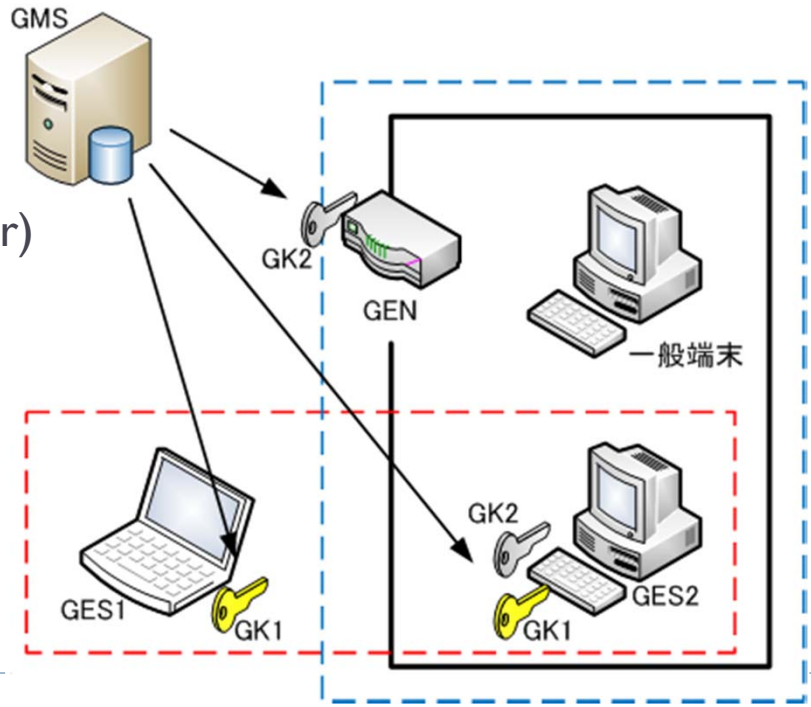
グループ毎にKDCが必要



GSCIP概要

グループの定義方法

- 通信グループとグループ鍵を1：1に対応づける
- 管理装置から鍵を配送
  - GE: GSCIP対応装置
    - GES(Software型)
    - GEN(Network型)
  - GMS(Group Management Server)

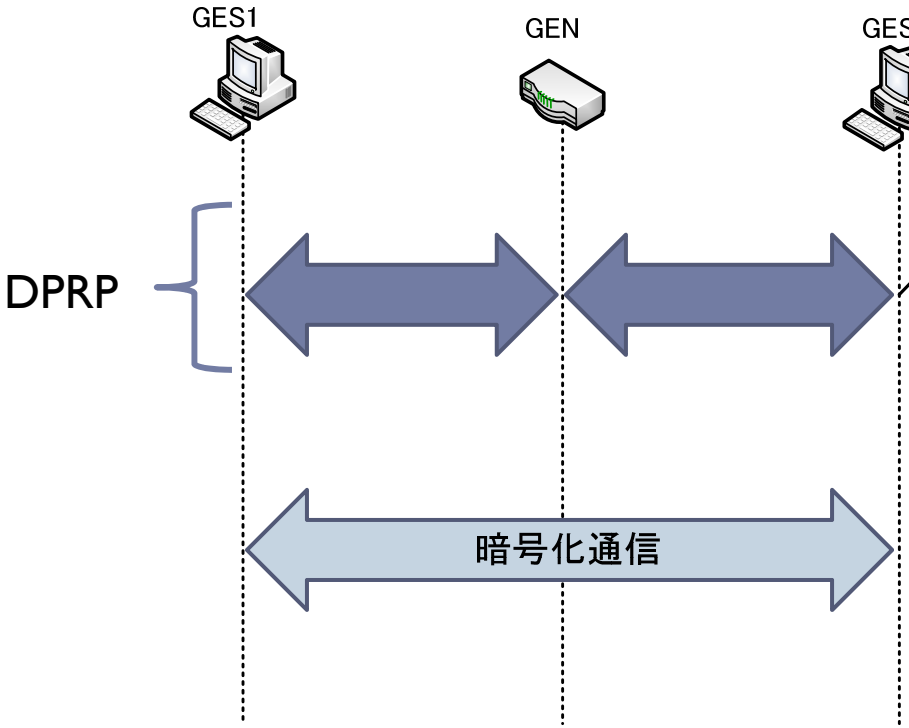


IPアドレス，システム構成が変化しても
グループ関係が維持される

DPRP
(Dynamic Process Resolution Protocol) 概要

- 通信開始時にDPRPを実行

通信相手が同じグループ鍵を所持しているかを確認



通信開始時に認証

- 経路上のGEの設定情報を取得
- 動作処理情報を決定
- 動作処理情報の生成・通知

動作処理情報：所属通信グループ，動作モード

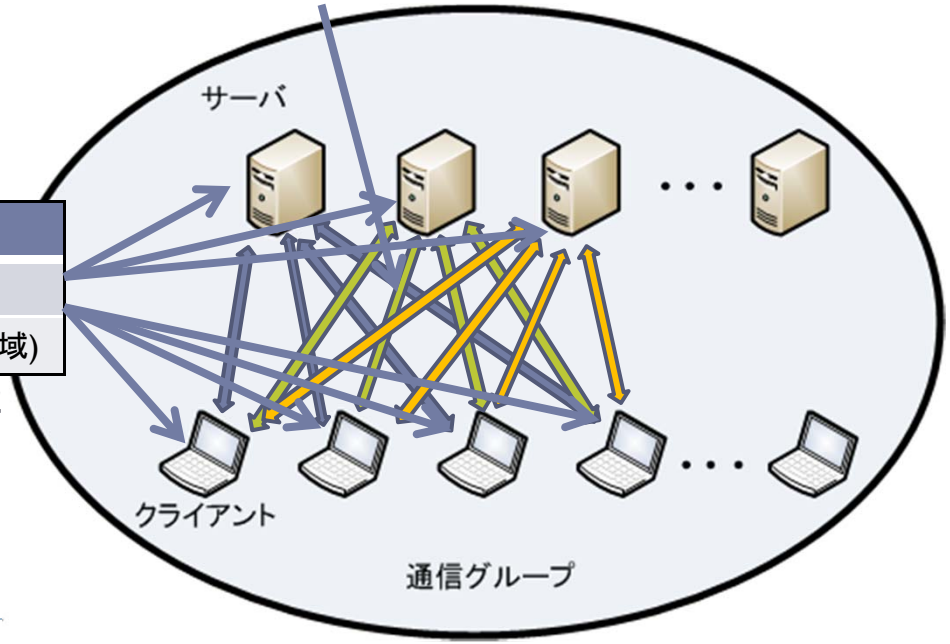
管理負荷の比較 – 個人単位の通信グループ

GSCIP，IPsec(IKE, KINK)の管理負荷の比較
- ネットワーク構成を想定
- 各ノードでの設定1項目あたりの管理負荷を1とする
- **システム全体で固定可能な設定については考えない**

- IPsec(IKE)
  - 必要設定コスト：通信ペア毎に3
    （宛先IPアドレス，動作処理内容，
    指定した相手以外に対する処理内容）
  - 通信ペア毎に設定する
- GSCIP
  - 必要設定コスト：グループ内のノード毎に2
    （グループ番号，動作モード）

IPsec/IKE
宛先IP
動作処理内容（IPsec, none, discard）
指定相手以外に対する動作処理内容

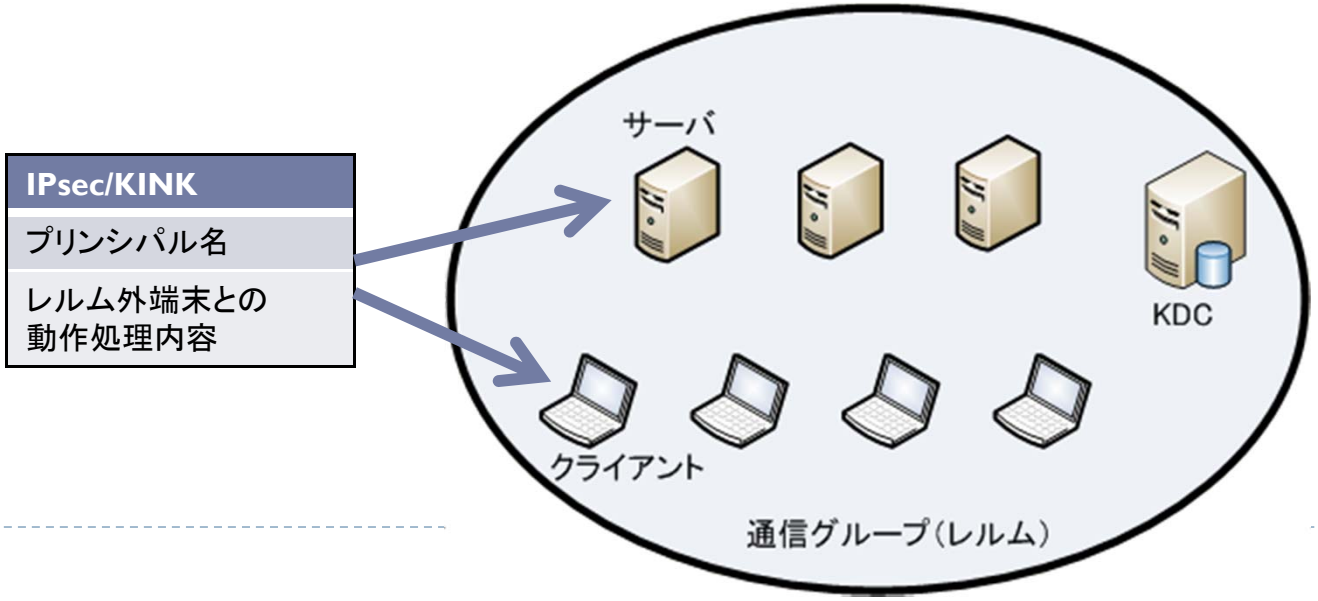
GSCIP/DPRP
グループ番号
動作モード(開放/閉域)



管理負荷の比較 – 個人単位の通信グループ

- IPsec(KINK)について
  - 各ノードは自身の名前(プリンシパル名), レルム外の端末との動作処理内容を持つ(IPsec/none/discard)
    - KDC:レルム内のプリンシパル一覧
      レルム内端末同士の動作処理内容

    必要設定コスト:グループ内のノード毎に2



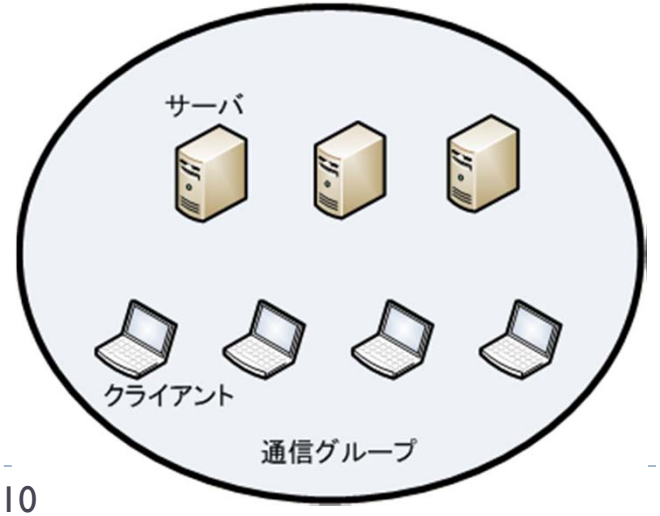
管理負荷の比較 – 個人単位の通信グループ

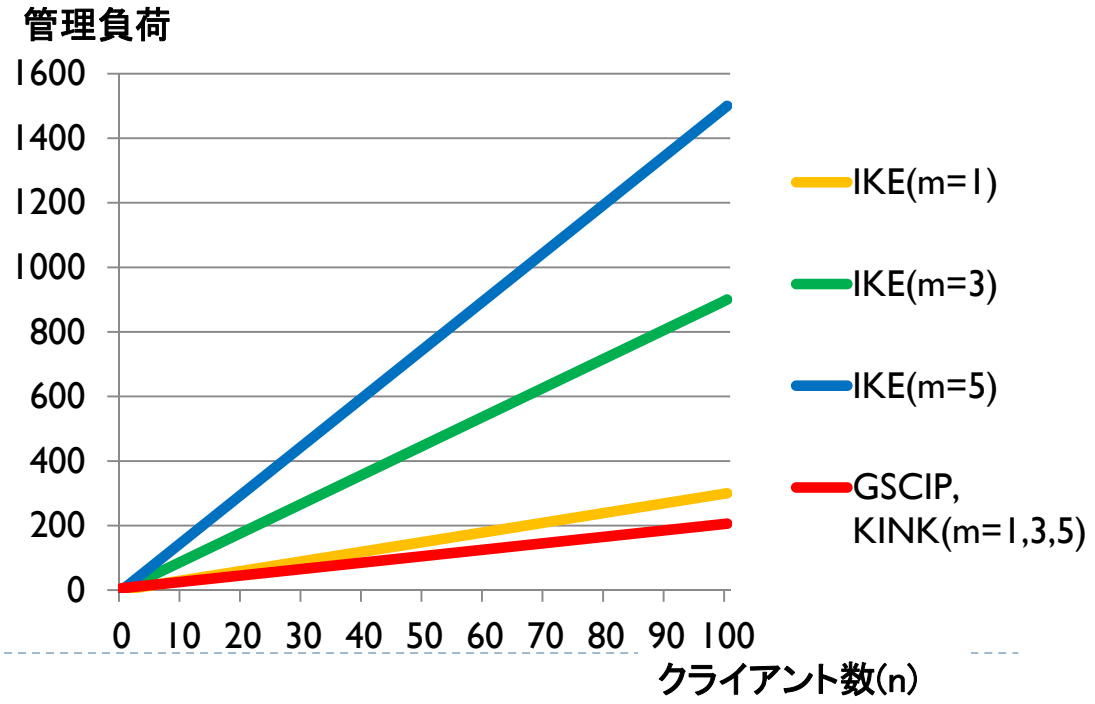
- 管理負荷
  - IPsec（IKE）： $m \times n \times 3$

    （宛先IP，動作処理内容， 指定以外の相手の処理）
  - GSCIP，IPsec(KINK)：

    $(m+n) \times 2$

    （グループ番号，動作モード / GSCIP）
    （プリンシパル名，レルム外端末との
    動作処理内容 / KINK）
    （m =サーバ数， n =クライアント数）



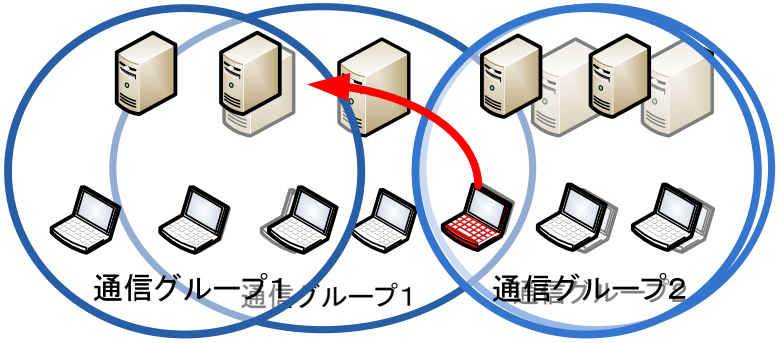


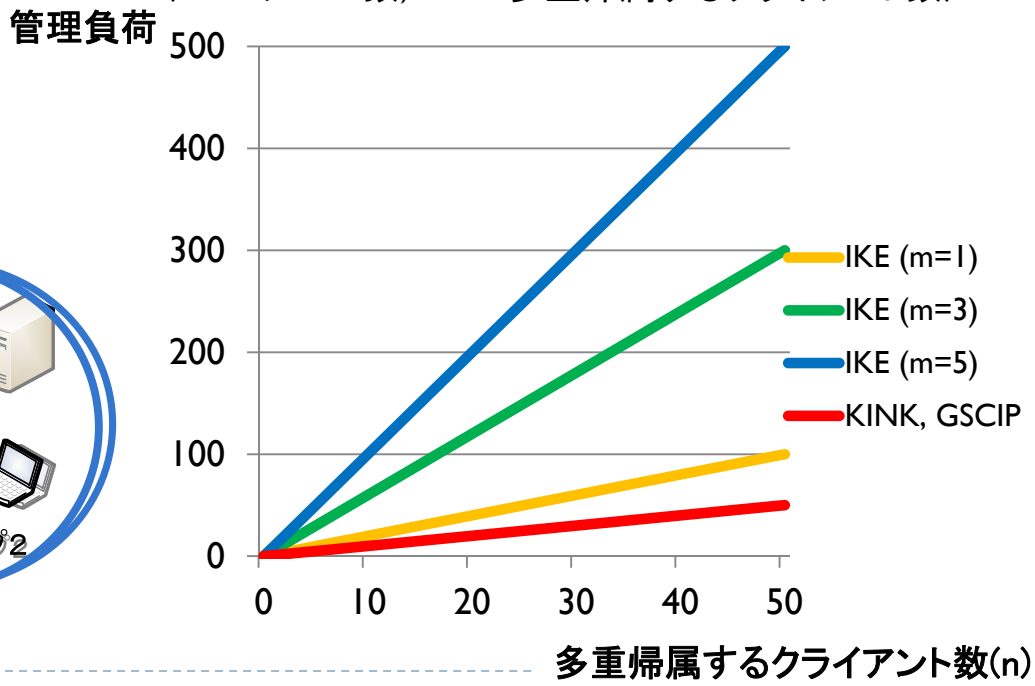
管理負荷の比較 – 端末が多重帰属する場合

- 2つの通信グループが存在するとき，
  特定の端末を多重帰属させる

必要追加設定数　IPsec（IKE）：$m \times n \times 2$（新たに接続するサーバのIP，処理内容）
IPsec（KINK）：n（新たに接続するレルムでのプリンシパル名）
GSCIP：n（グループ番号を追加）

（m＝サーバ数，n＝ 多重帰属するクライアント数）





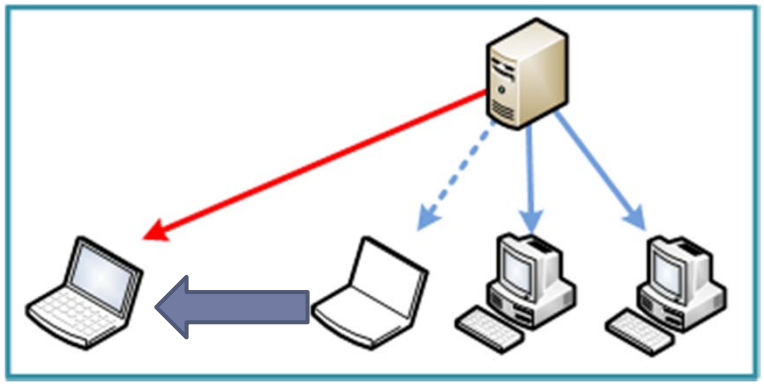
管理負荷の比較 – クライアントが移動する場合

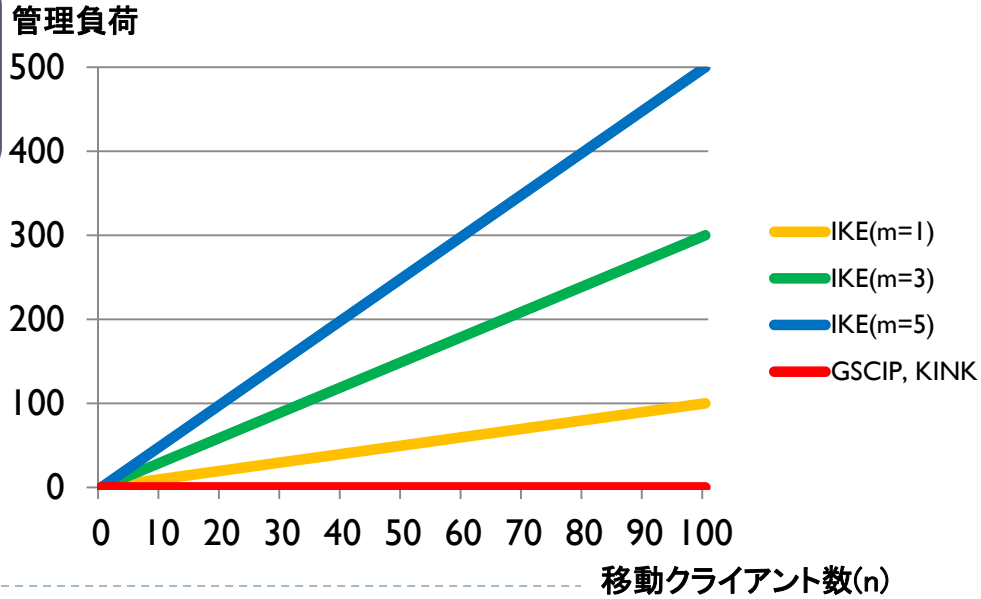
- システム構築後，クライアントが移動して
  IPアドレスが変化した場合

必要設定変更数（IKE）：　$m \times n$　（m ＝サーバ数，n ＝移動クライアント数）
（宛先IPアドレス）

（GSCIP, KINK）：　設定変更不要

GSCIP, KINKはIPアドレスに依存しない
グループ定義が可能





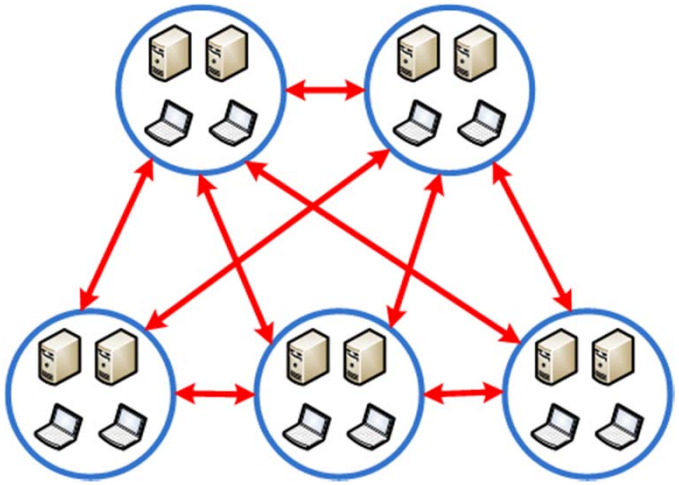
管理負荷の比較 – サブネット単位の通信グループ

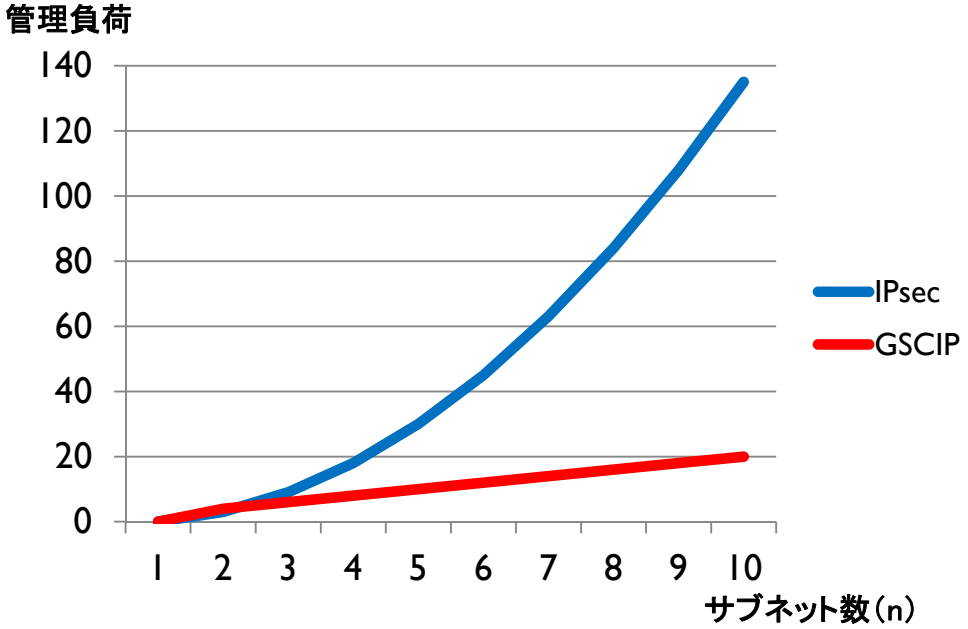
- サブネット毎に存在するルータ同士で通信を行う
  - GSCIPではGENを使用，各GENにグループ番号を指定

IPsec（IKE）：$n \times (n-1) \div 2 \times 3$（全ての組合せに対して，宛先IP，動作処理内容，指定以外の相手の処理）

GSCIP：$n \times 2$　（グループ番号，動作モード）

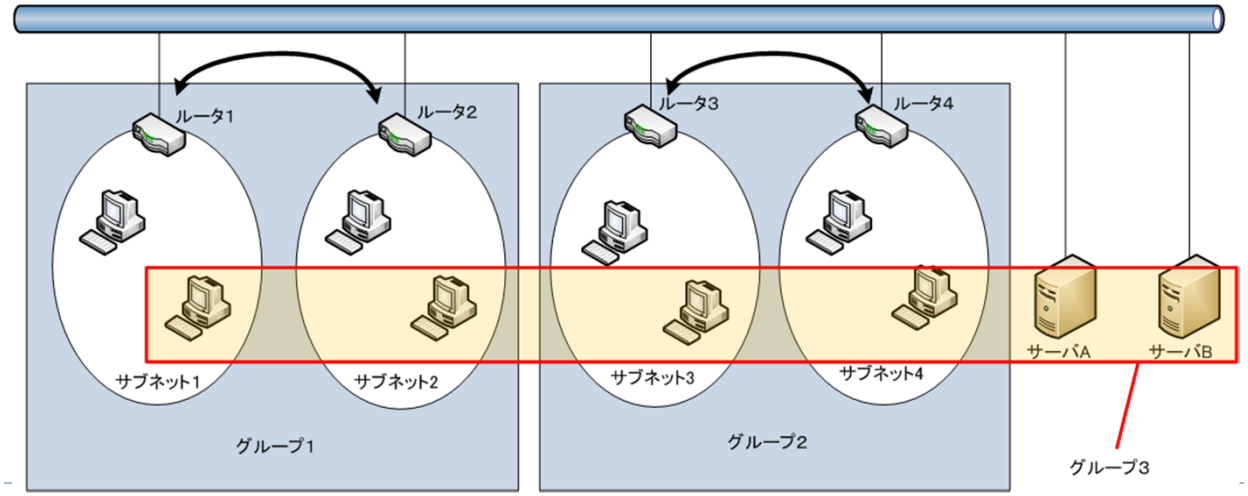
（n = サブネット数）





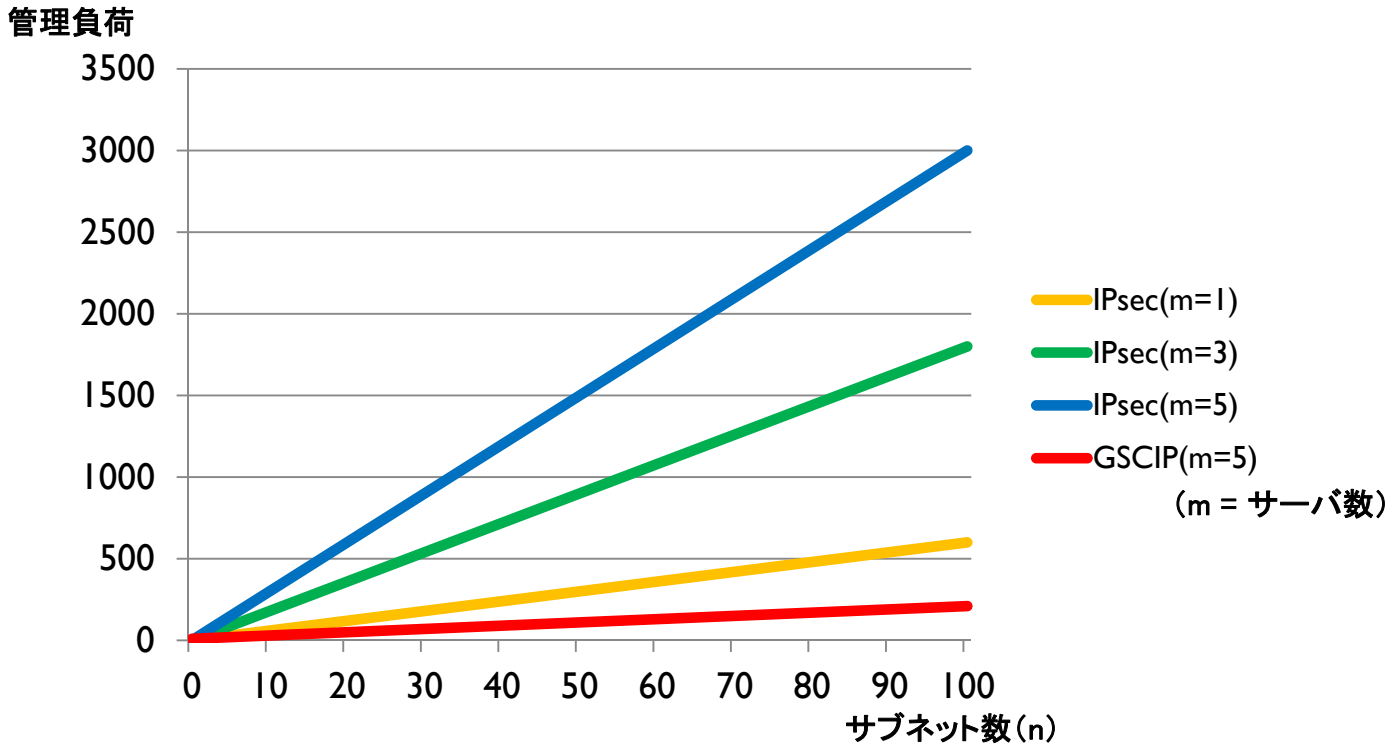
管理負荷の比較 – グループ・個人の混在環境

- グループ単位，個人単位の混在した通信グループ
  - グループ1，2が存在するとき，新たにグループ3を定義する場合
    - IPsec（IKE）：サーバとクライアントのペア毎に3の設定
      ＋ペア毎にルータに通信許可設定（送信元，宛先，処理内容のセット）
      $m \times n \times 3 + m \times n \times 3$
    - GSCIP：端末毎に2（グループ番号，動作モード）
      $(m+n) \times 2$　　（ m ＝サーバ数，n ＝グループ3のクライアント数 ）



管理負荷の比較 – グループ・個人の混在環境

- グループ単位，個人単位の混在した通信グループ



Watanabe Lab.

まとめ

- GSCIPは通信グループとグループ鍵を1対1に対応させることで，IPsecに比べ管理不可を大幅に抑えられる
  - IPアドレスに依存しないグルーピングが可能なため，IPアドレスが変化しても管理不可が発生しない
- IPsecおよびGSCIPにおける通信グループ構成時の管理負荷を定量的に比較した

付録

付録 - IPsec, IKEの設定項目

IPsecの設定項目
送信元IP，ポート番号
宛先IP，ポート番号
通信方向(in, out)
プロトコル(TCP, UDP, etc)
処理内容(Discard, None, IPsec)
セキュリティプロトコル(ESP, AH)
セレクタ
Lifetime
暗号化アルゴリズム
認証アルゴリズム
エンドノードのIPアドレス　等

IKEの設定項目
IKE相手のIPアドレス
交換タイプ(Main, Aggressive)
Situation
自身のID
IKE相手のID
Lifetime(ISAKMP SA)
暗号化アルゴリズム
ハッシュアルゴリズム
認証方式
DHグループ　等

付録 - GSCIPの設定項目

GEの設定	GMSの設定		
GE設定	GE情報	グループ鍵情報	所属通信グループ情報
ユーザID	ユーザID	通信グループ番号	ユーザID
GMSとの共通鍵	動作モード	鍵バージョン	通信グループ番号
GMSのIPアドレス	GEとの共通鍵	鍵長	
		グループ鍵	