通信アーキテクチャ GSCIP の管理運用評価

村 橋 孝 謙[†1]　鈴 木 秀 和[†2, †3]　渡 辺　晃[†1]

名城大学理工学部[†1]　名城大学大学院理工学研究科[†2]　日本学術振興会特別研究員 PD[†3]

１．はじめに

組織のネットワークにおいて，内部の関係者からの情報漏洩を防ぐ手段は重要である．しかし，実際に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．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．これを実現するための既存技術として IPsec が挙げられるが，IPsec で使用される鍵交換プロトコル IKE では設定項目が多くネットワーク構成が複雑な場合やシステム構成が変化した場合の管理負荷が大きくなる．ドメイン単位に IPsec を適用する方法もあるが，端末毎の細かな通信グループの定義が困難となる．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）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 の管理は GMS（Group Management Server）で行う．GMS では動作モード，通信グループを定義し，グループ鍵の生成，配送，更新を行う．

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比較し，GSCIP の有効性を検証した．

２．IPsec と GSCIP

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．IP パケットの暗号化により情報漏洩を防ぎ，認証データをパケット内に埋め込むことでパケットが改ざんされていないことを保証する．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（Internet Key Exchange）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．

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，通信グループを定義する場合は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．

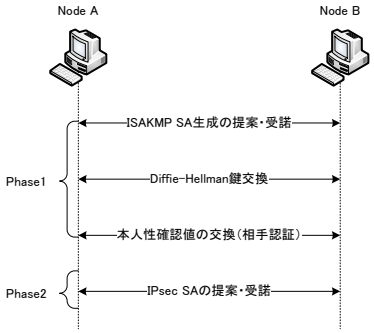


図１　IKE の動作シーケンス

2.2 GSCIP

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．

“Evaluation of management and use of communication architecture GSCIP”

†1 Takanori Murahashi and Akira Watanabe
Faculty of Science and Technology, Meijo University

†2 Hidekazu Suzuki
Graduate School of Science and Technology, Meijo University

†3 Hidekazu Suzuki
Research Fellow of the Japan Society for the Promotion of Science

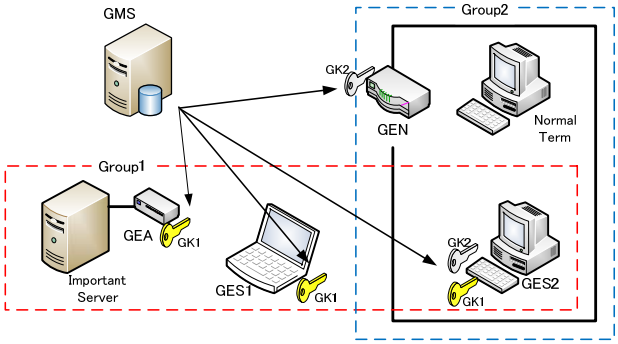


図２　GSCIP によるグループ構築例

GSCIP は，各 GE と管理サーバ GMS（Group Management Server）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）[1]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．

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３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．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．

GSCIP では各 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．

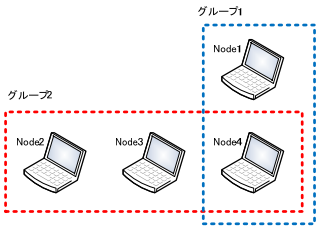


図３　想定するネットワーク構成

3.2　大規模システムの場合及びシステム構成変化時

図３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．追加ノード数と設定項目数の関係は図４のようになり，GSCIP が有利であることがわかる．

次にシステム構築後，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．

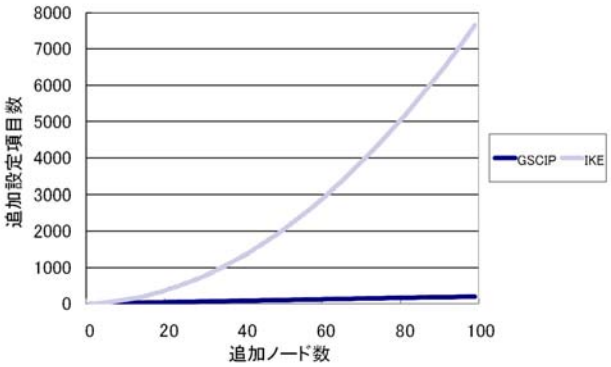


図４　ノード追加時の設定項目数の変化

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．今後はネットワークを構成するグループが階層的になっている場合についても比較する．また KINK（Kerberized Internet Negotiation of Keys）など，他の方式を含めた比較評価を行う．

参考文献

[1]　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)

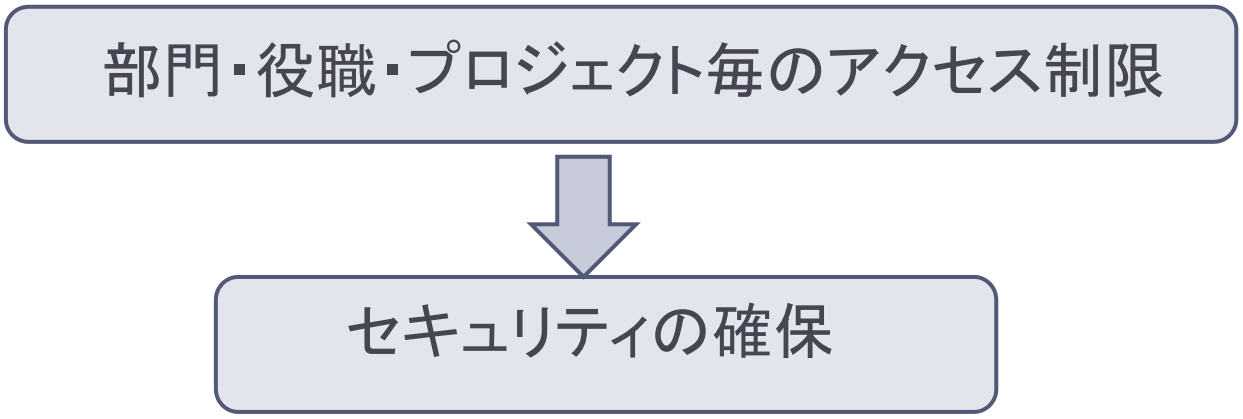
Watanabe Lab

通信アーキテクチャGSCIPの管理運用評価

名城大学　理工学部
村橋 孝謙　鈴木秀和　渡邊晃

研究背景

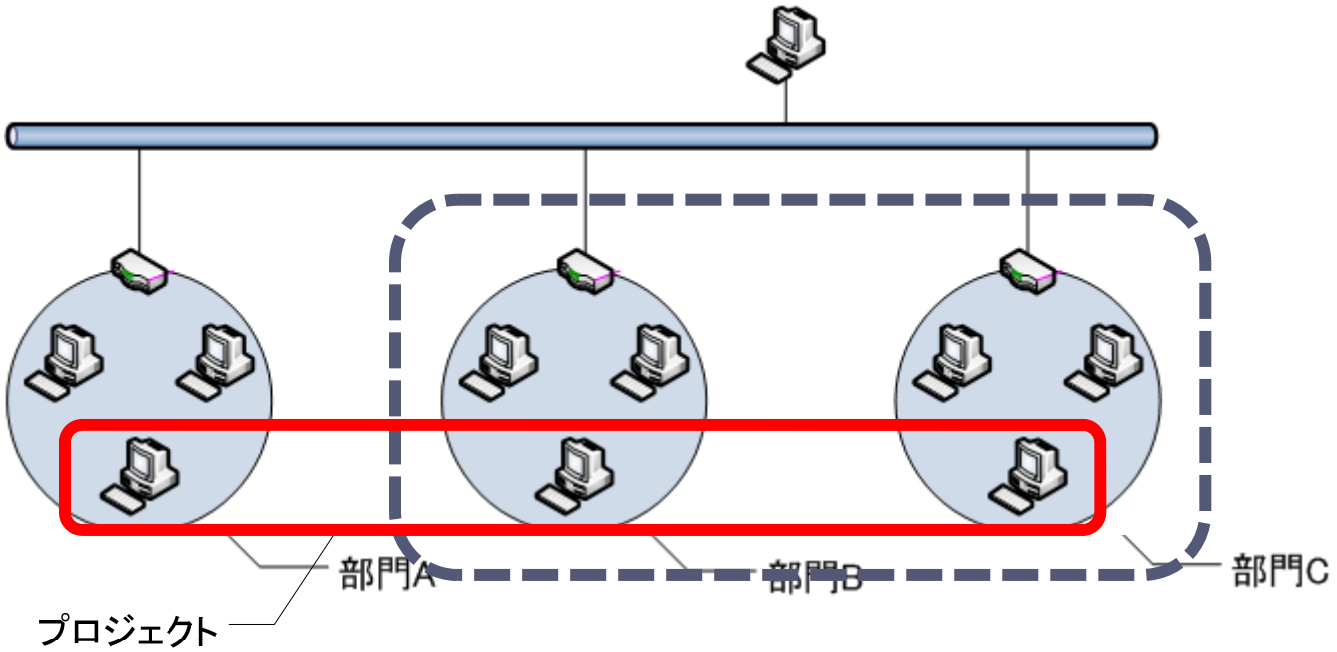
- ネットワークにおける，組織内部の関係者による情報漏洩の問題
  - 外部： ファイアウォール，IDS*等
  - 内部： ユーザ名，パスワードによる認証がほとんど



*IDS：Intrusion Detection System

研究背景

- 部門・役職・プロジェクト等に応じた通信グループを定義



研究背景

- 通信グループの定義

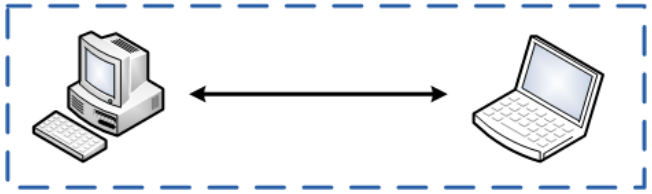
  確実な通信相手の認証　　通信の暗号化

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

既存技術 - IPsec

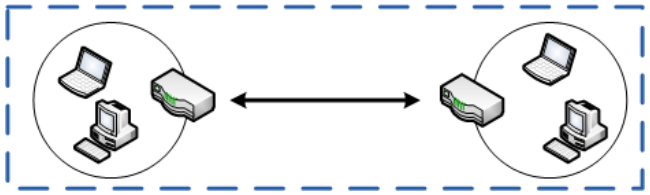
- IP層で定義されたセキュリティプロトコル
- アプリケーションに依存しない

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
- 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

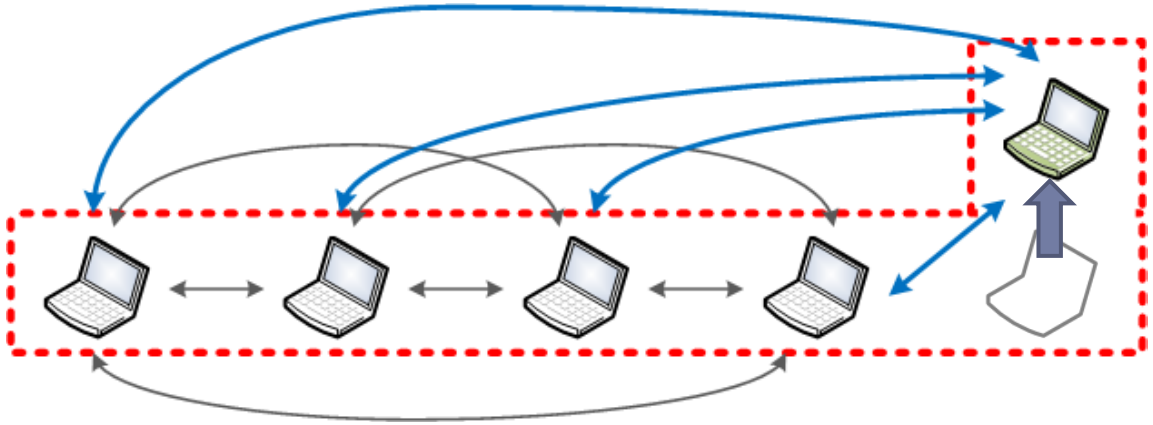
既存技術 - IPsec

- IPsec動作
  - ESP[1]（パケット毎の暗号化）
  - IKE[2]（通信開始時の認証）

IPsec，IKEは設定項目が多い

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

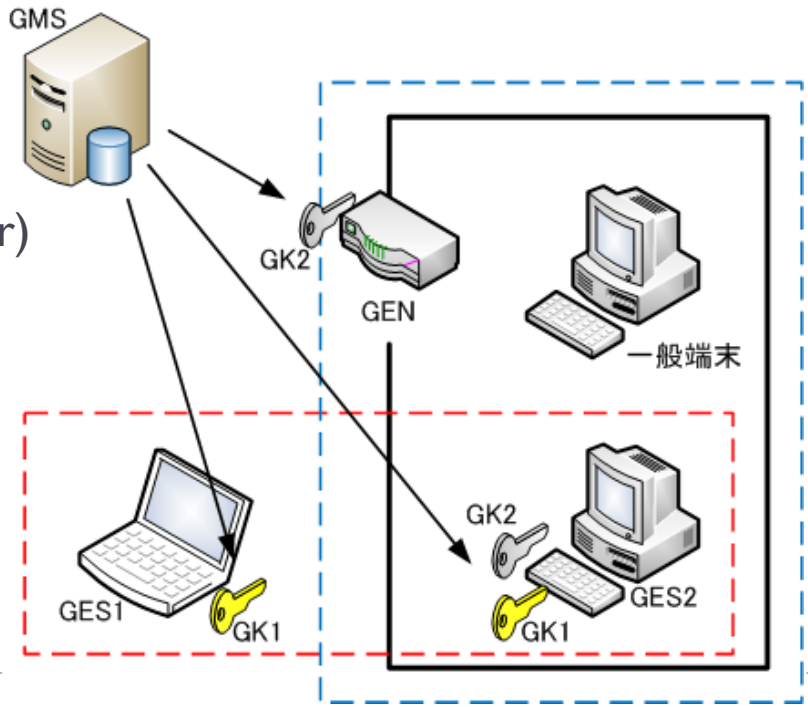


1：ESP (Encapsulated Security Payload)
2：IKE (Internet Key Exchange)

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)

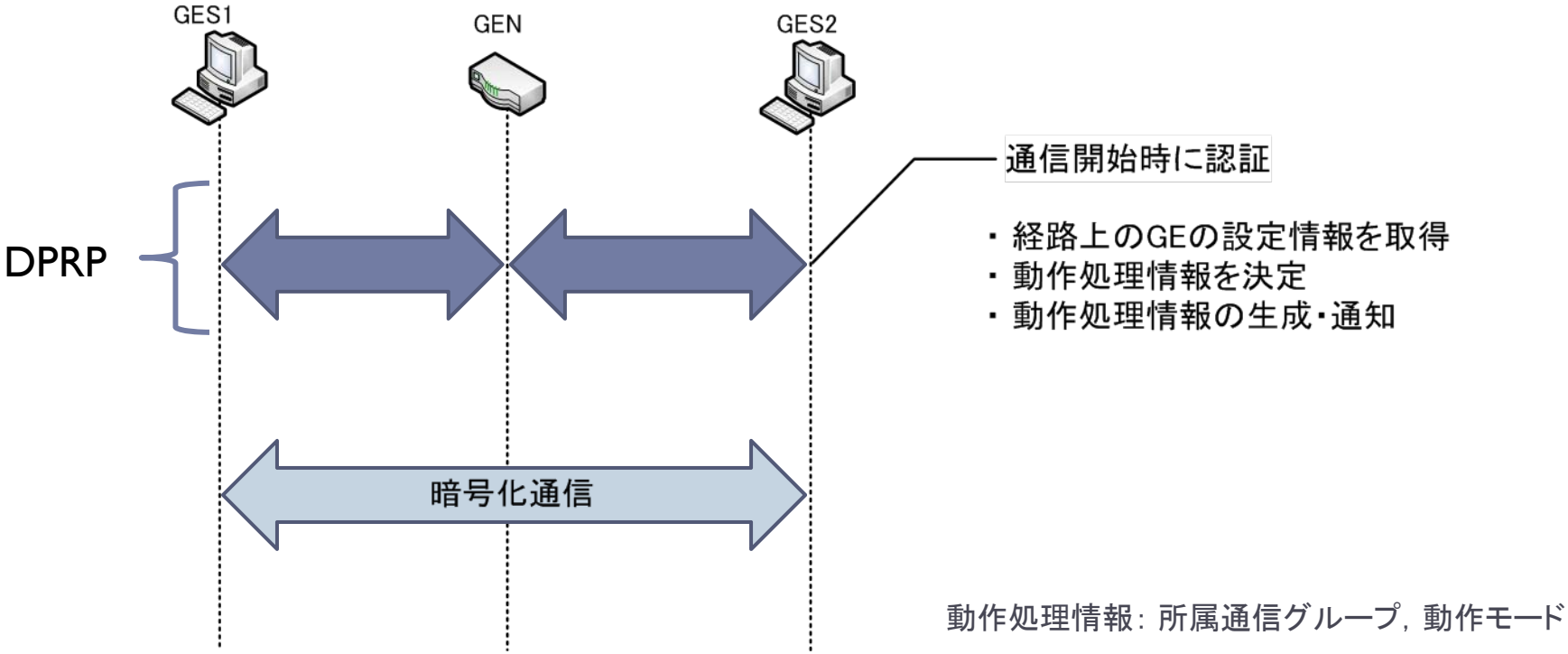


IPアドレス，システム構成が変化しても
グループ関係が維持される

DPRP
(Dynamic Process Resolution Protocol) 概要

- 通信開始時にDPRPを実行

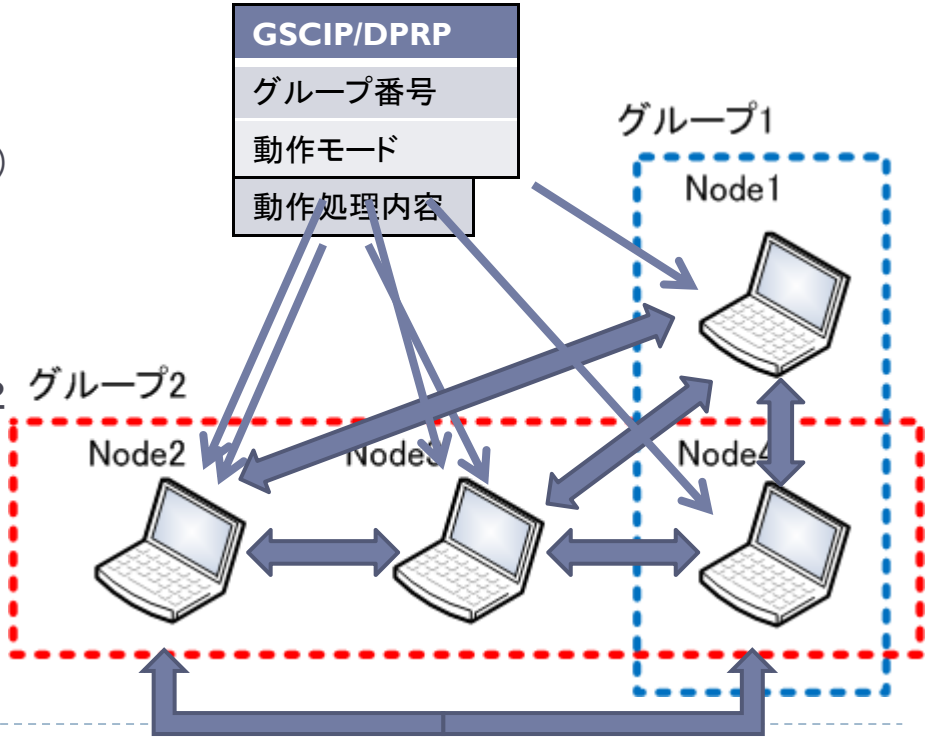
通信相手が同じグループ鍵を所持しているかを確認



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 – 小規模システム

- GSCIP，IPsec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
  - 必要設定コスト：通信ペア毎に3
    （通信ペアのIPアドレス，動作処理内容）
  - 通信ペア毎に設定する必要がある
- 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）
- 管理負荷
  - IPsec： $3 \times 6 = 18$
  - GSCIP： $(2+3) \times 2 = 10$



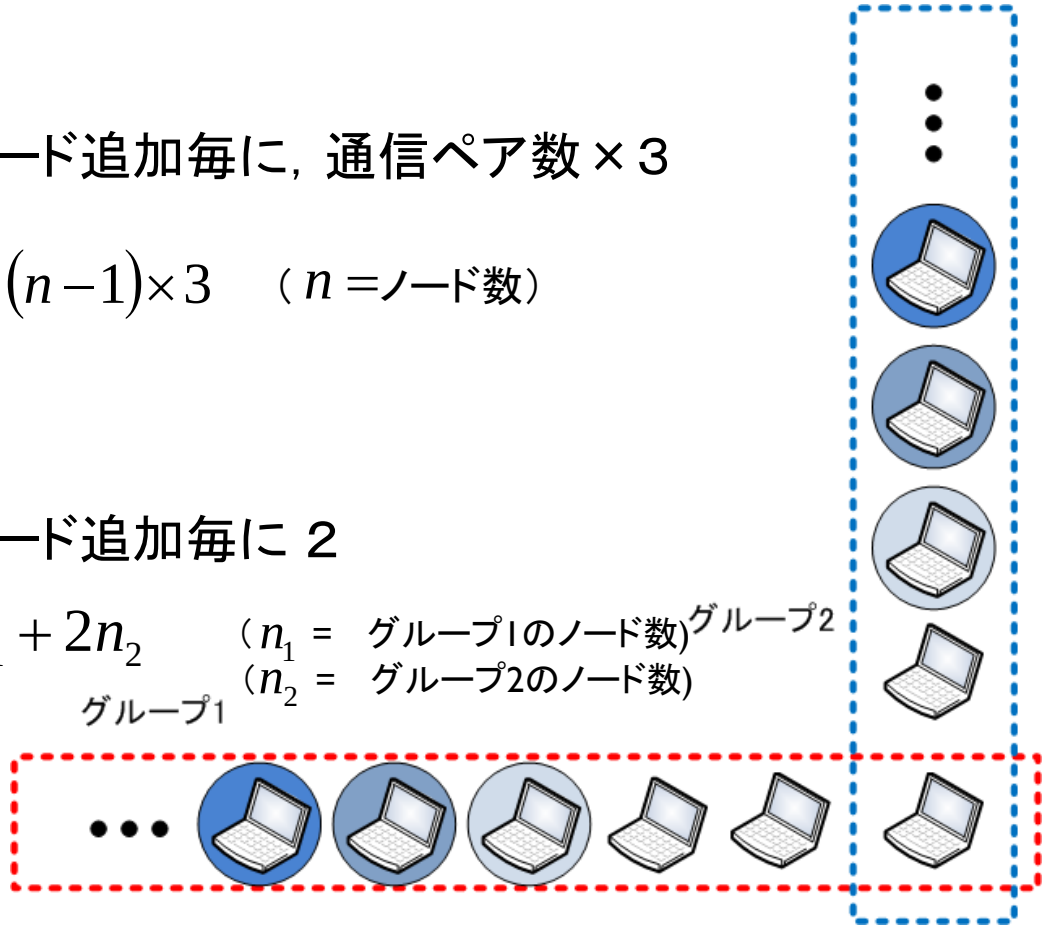
管理負荷の比較 – 大規模システム

- 管理負荷
  - IPsec
    - 必要設定コスト：ノード追加毎に，通信ペア数×３

      必要設定数合計： $n \times (n-1) \times 3$ （n =ノード数）

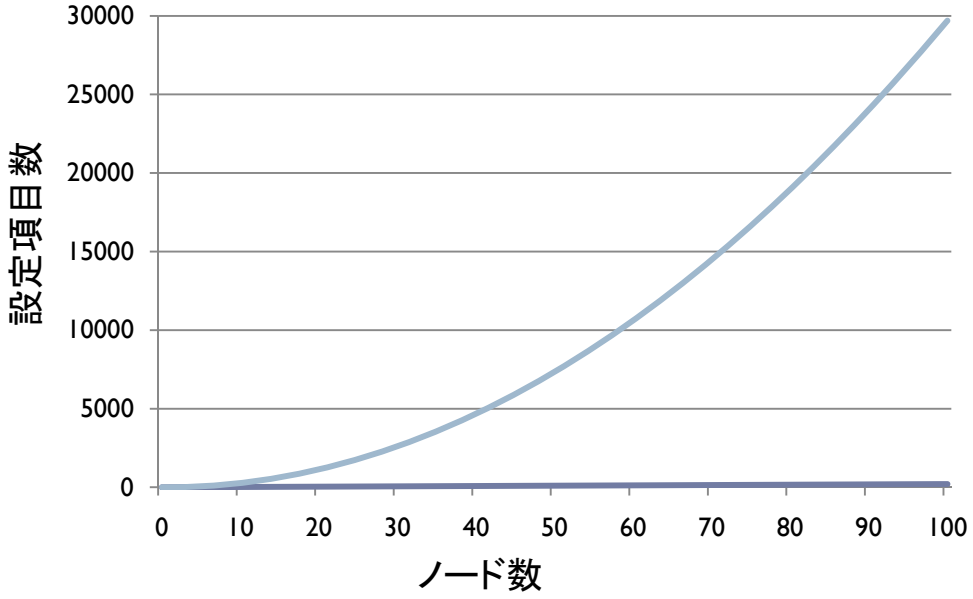
  - GSCIP
    - 必要設定コスト：ノード追加毎に２

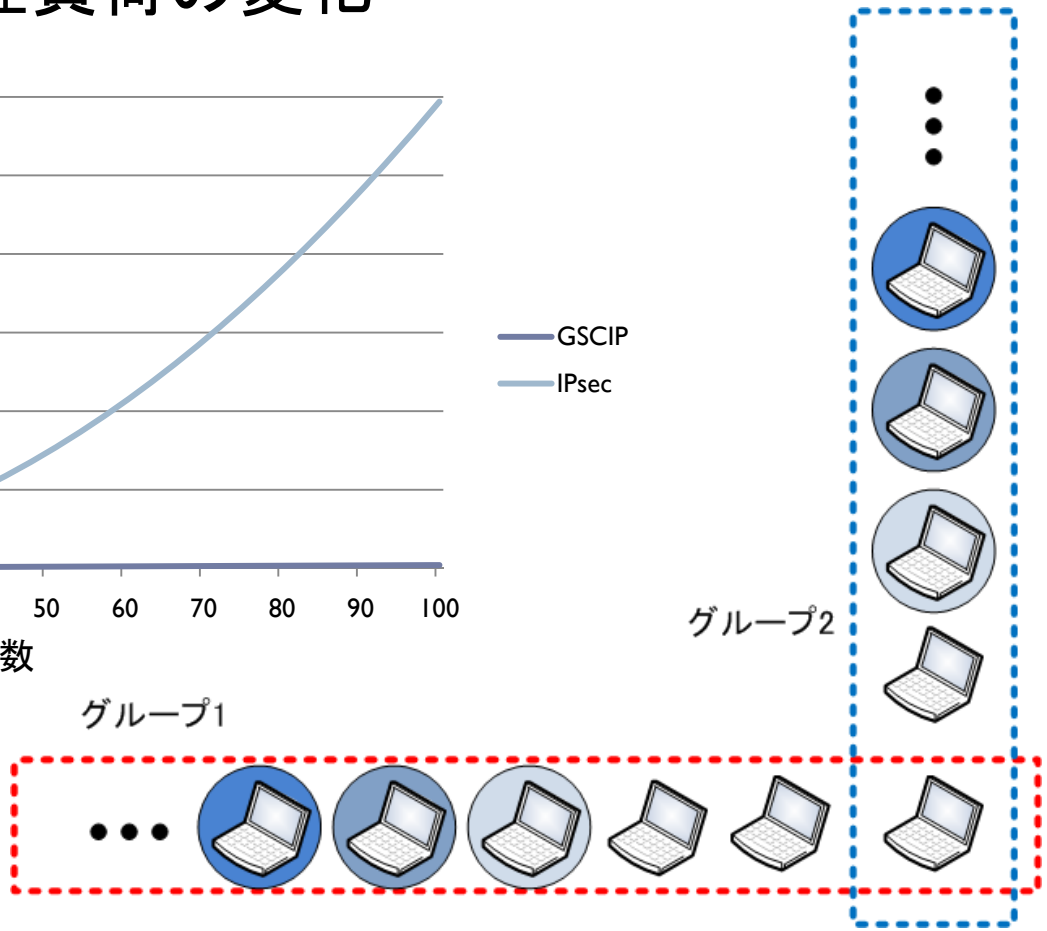
      必要設定数合計： $2n_1 + 2n_2$ （n_1 = グループ1のノード数）（n_2 = グループ2のノード数）



管理負荷の比較 – 大規模システム

- ノード数による管理負荷の変化



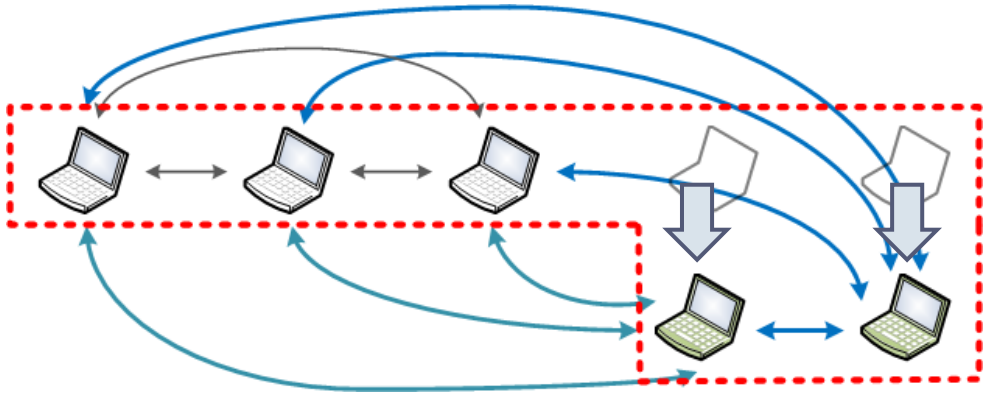


IPsec : $n \times (n-1) \times 3$

GSCIP : $2n_1 + 2n_2$

管理負荷の比較 – システム構成変化時

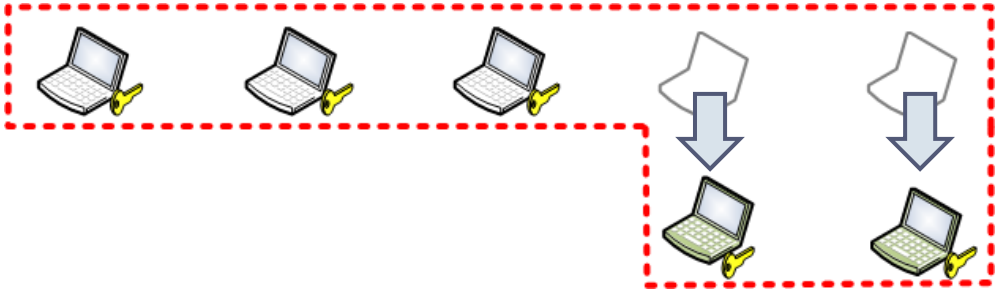
- ノードが移動した場合（IPsec）



必要設定数合計： $m \times (n-1) \times 3$

移動した数：m
グループメンバの数：n

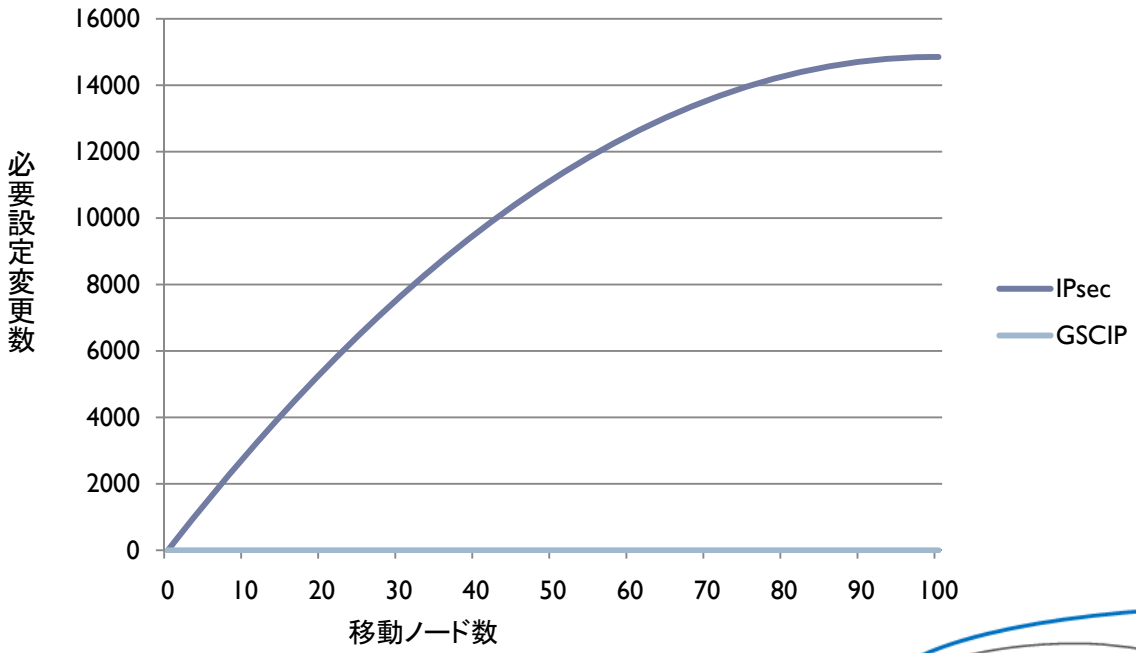
- ノードが移動した場合（GSCIP）

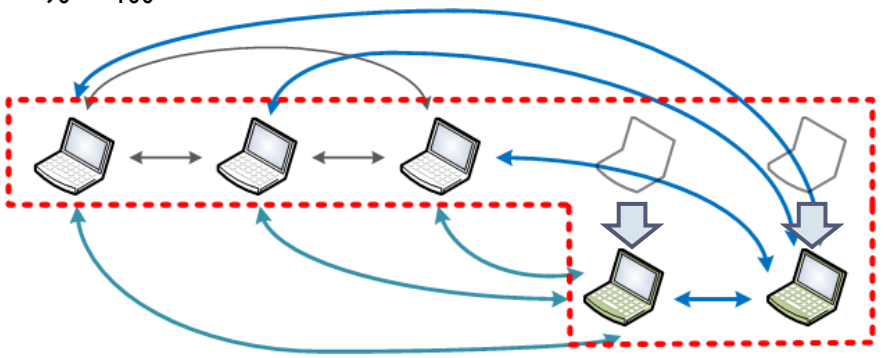


設定変更は不要

管理負荷の比較 – システム構成変化時

- ノードが移動した場合 $(n = 100)$





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，IPアドレスに依存しないグルーピングが可能
  - GSCIPはIPsecに比べ管理負荷を大幅に抑えられる

- 今後
  - 個人単位･ドメイン単位の混在環境における比較
  - 他の方式を含めた比較

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	