# 通信アーキテクチャ GSCIP の管理運用評価

060427360　村橋 孝謙
渡邊研究室

## 1.　はじめに

組織内のネットワークは、ユーザ名とパスワードによる認証が行われている程度のもので情報漏えいが危惧される。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でセキュリティの確保が出来る．既存技術として IPsec が挙げられるが，設定項目が多く管理負荷が大きくなるという課題がある．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．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 で用いられる IKE では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．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全ての通信ペアに対しての設定が必要である．

### 2.2　GSCIP

GSCIP では同一のグループ鍵を所有する GE を同一のグループに属するメンバとして考える．基本的な GSCIP を用いた通信グループの構成を図１に示す．GSCIP におけるグループ構成要素を GE（GSCIP Element）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による認証と暗号化が行われる．

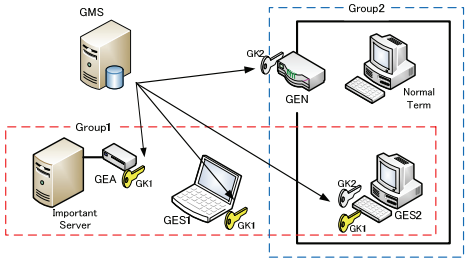



図１　GSCIP によるグループ構築例

## 3.　管理負荷の比較

GSCIP および IPsec 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．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．設定は全て管理装置で行い，その情報を各ノードに配送するものとした．

### 3.1　小規模システムの場合

図２に示す最も簡単なグループ構成を想定する． IPsec の場合は通信ペアごとに３の設定が必要であり，ペア数が４のため管理負荷は 12 である．GSCIP では各 GE ごとに２の設定が必要となり，ノード数が４のため管理負荷は８である．

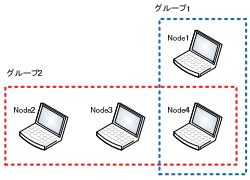



図２　想定するネットワーク構成

### 3.2　大規模システムの場合

図２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図３に示す．ノード数が増えると，IPsec の管理負荷が大幅に増加することがわかる．

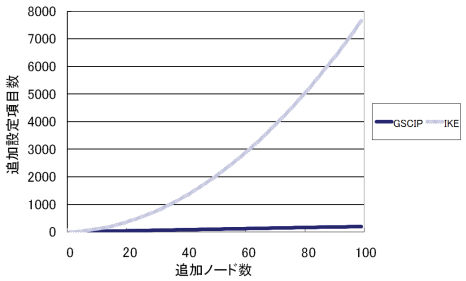



図３　ノード追加時の設定項目数の変化

## 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．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)

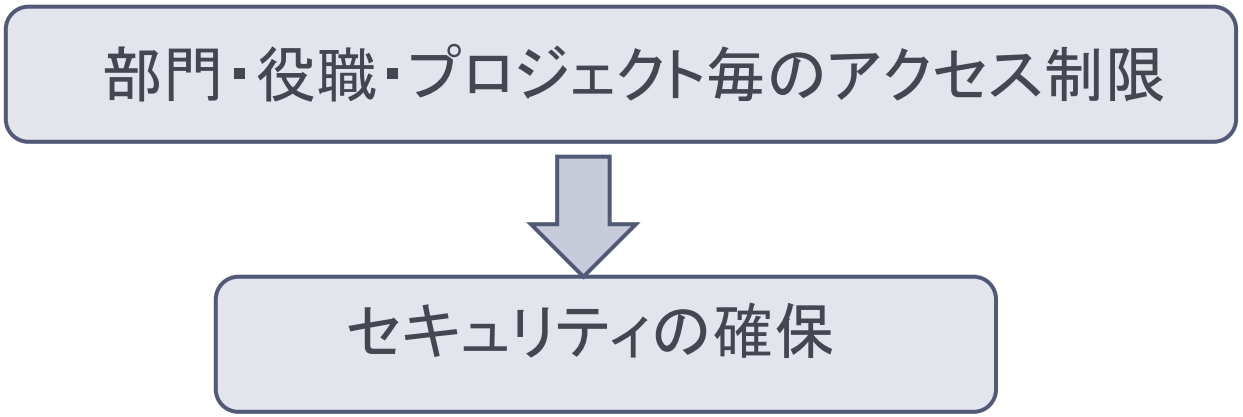
Watanabe Lab.

# 通信アーキテクチャGSCIPの管理運用評価

渡邊研究室
060427360　村橋　孝謙

# 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

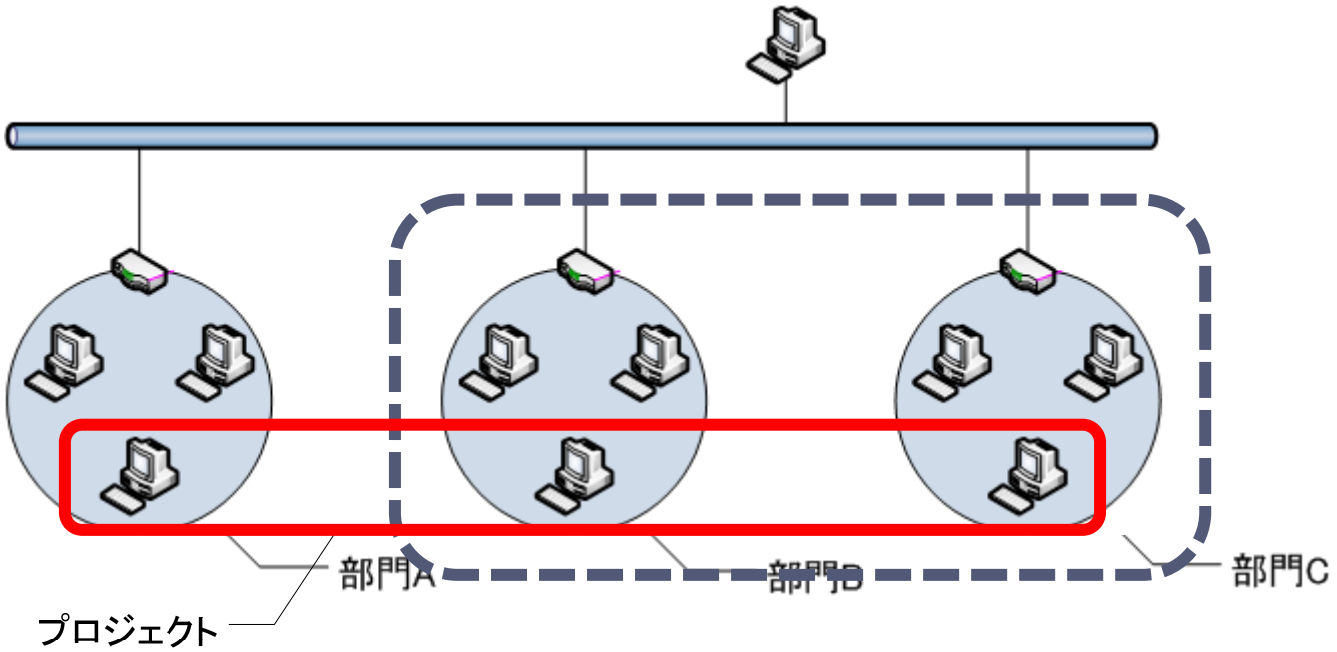





*IDS：Intrusion Detection System

# 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



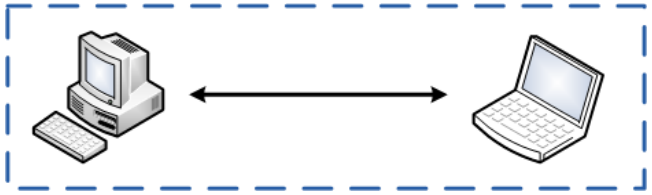
# 研究背景

- 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

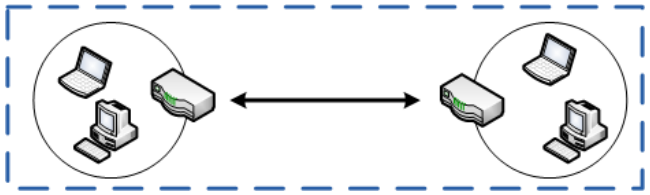
- IP層で定義されたセキュリティプロトコル
- アプリケーションに依存しない

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

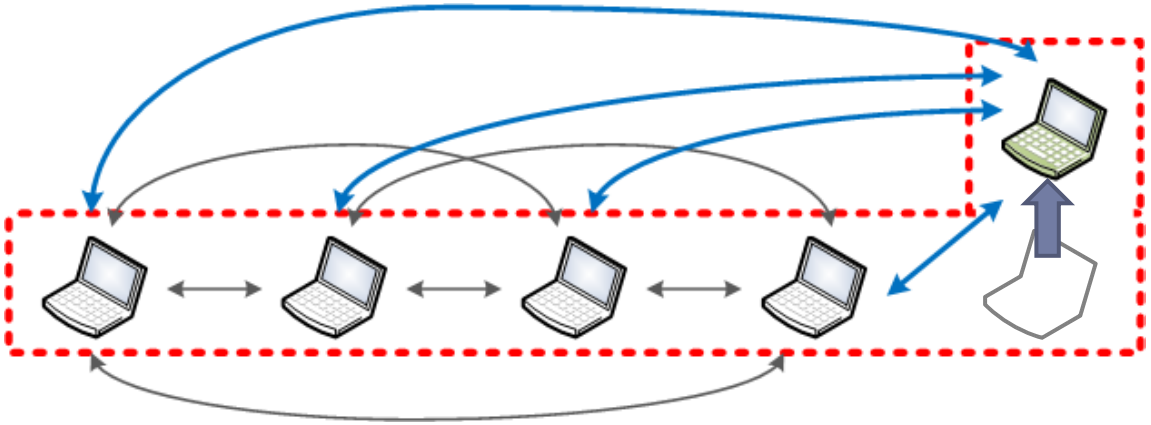
# 既存技術 - IPsec

- 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



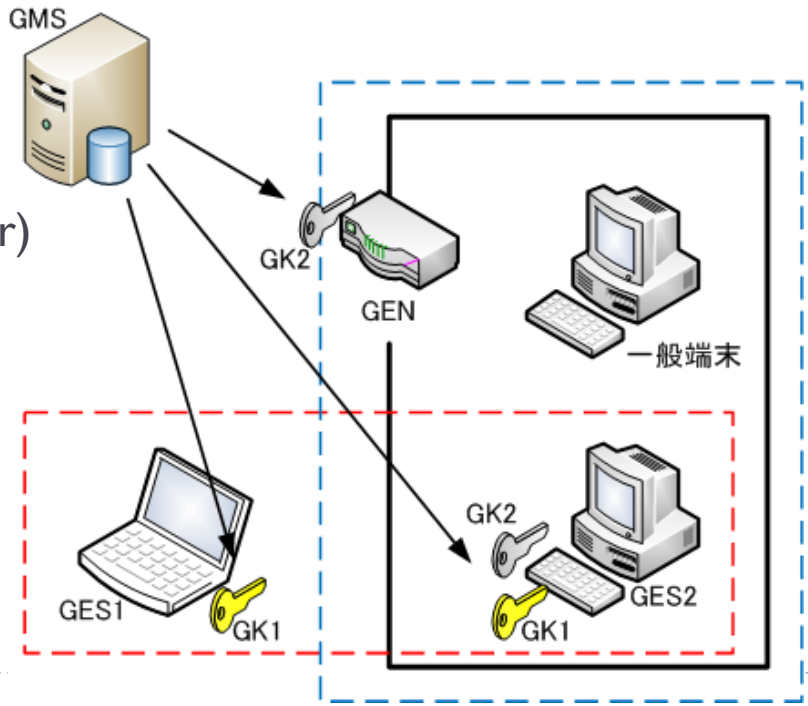


1：ESP (Encapsulated Security Payload)
2：IKE (Internet Key Exchange)

# GSCIP概要

## グループの定義方法

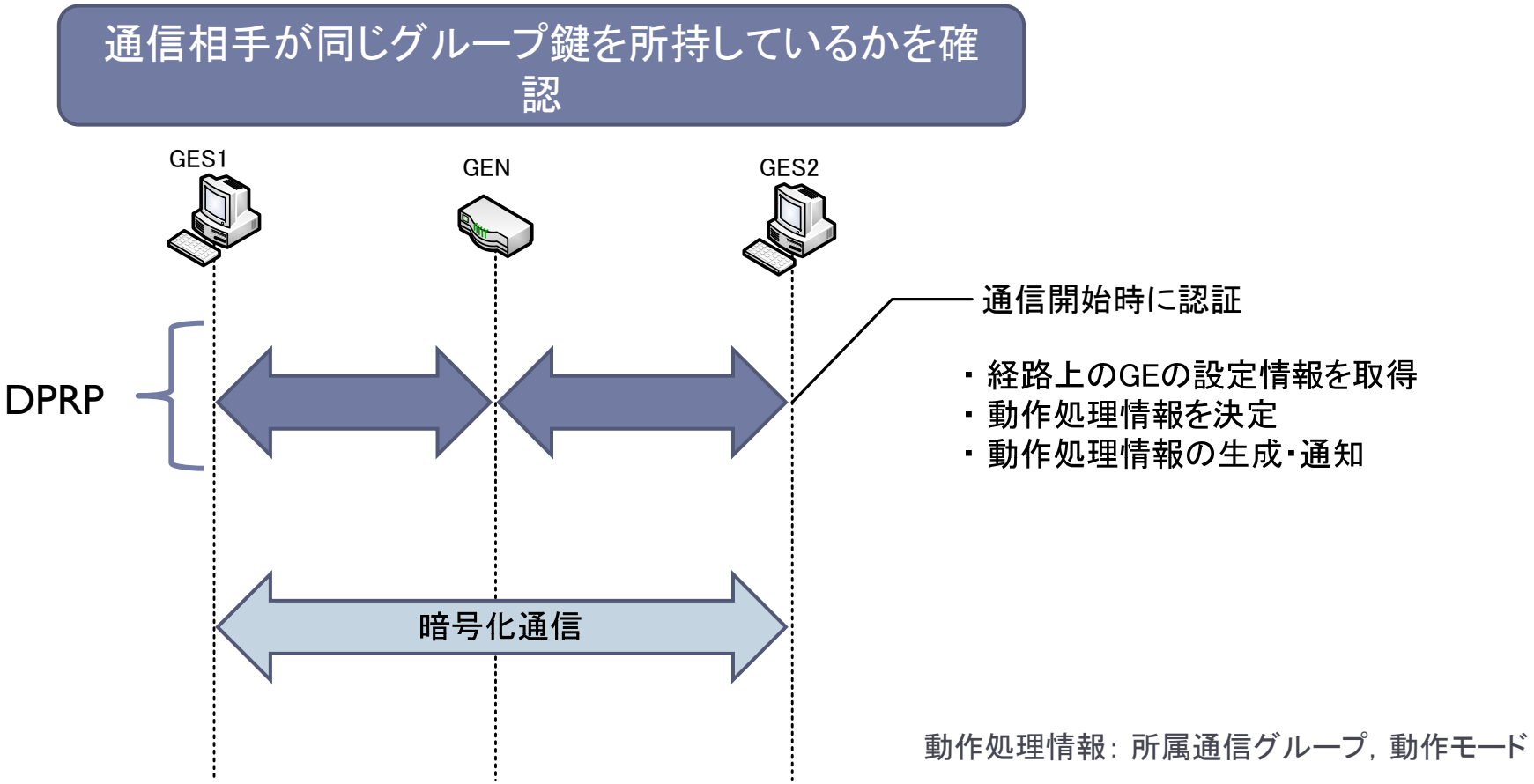
- 通信グループとグループ鍵を1：1に対応づける
- 管理装置から鍵を配送
  - GE: GSCIP対応装置
    - GES(Software型)
    - GEN(Network型)
  - GMS(Group Management Server)




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

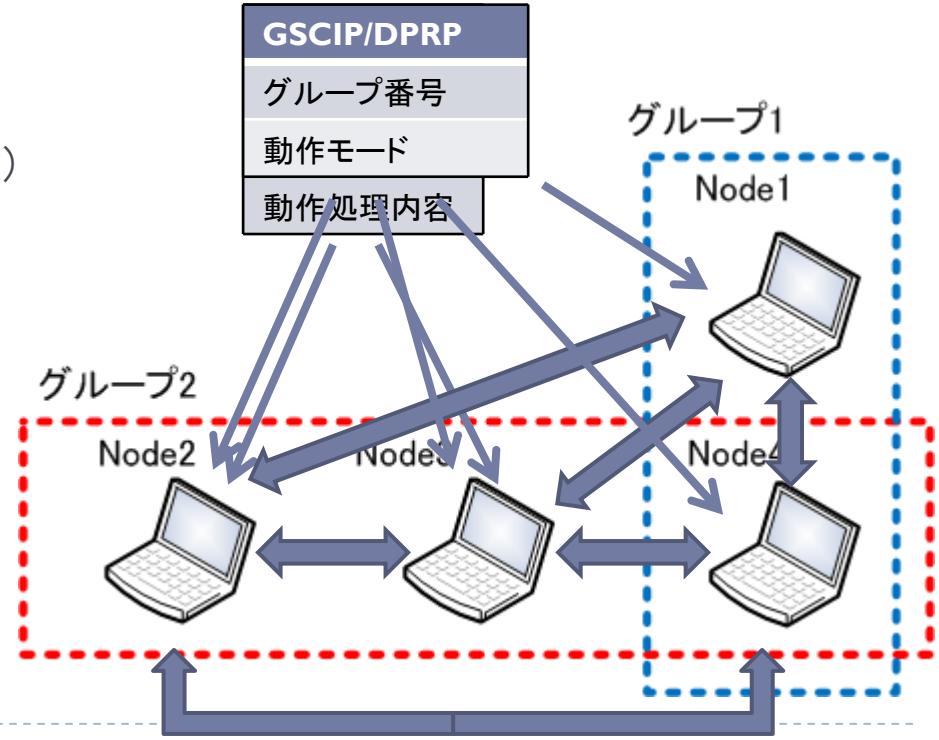
- 通信開始時にDPRPを実行




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：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： $2 \times 4 = 8$

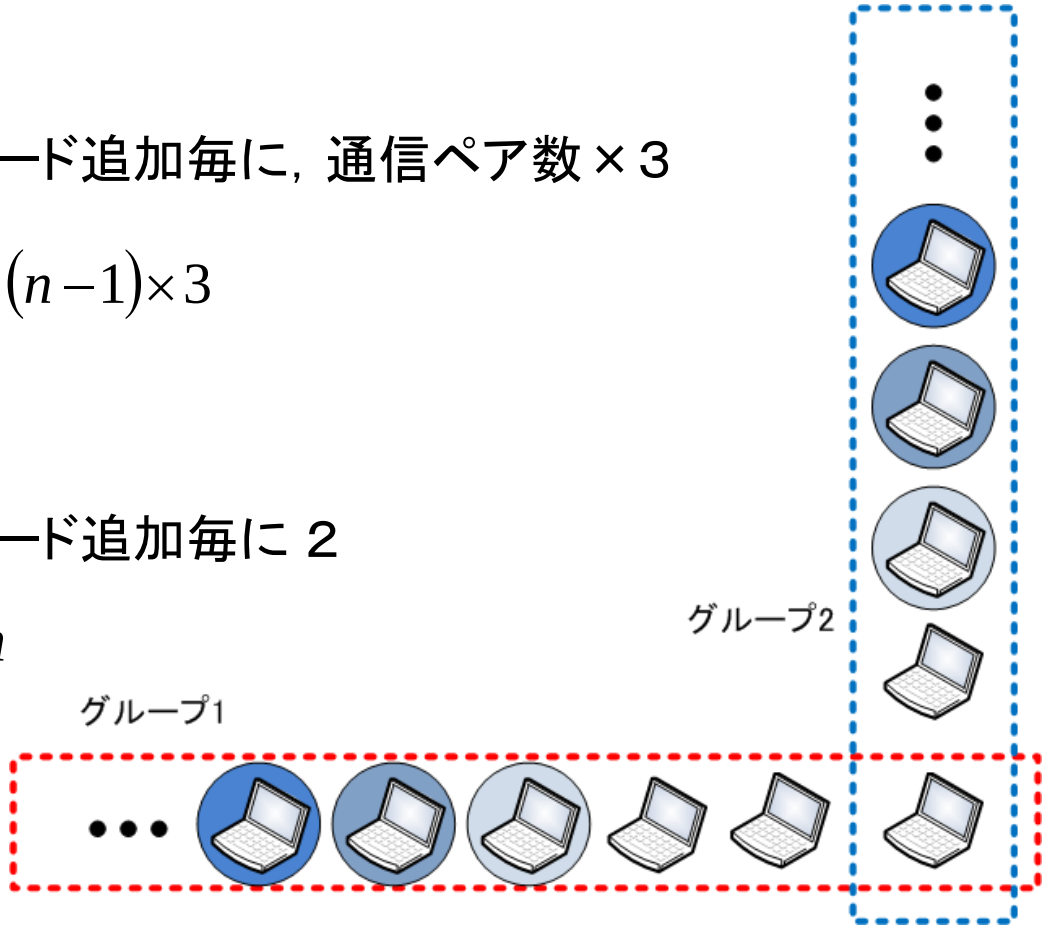


# 管理負荷の比較 – 大規模システム

- 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

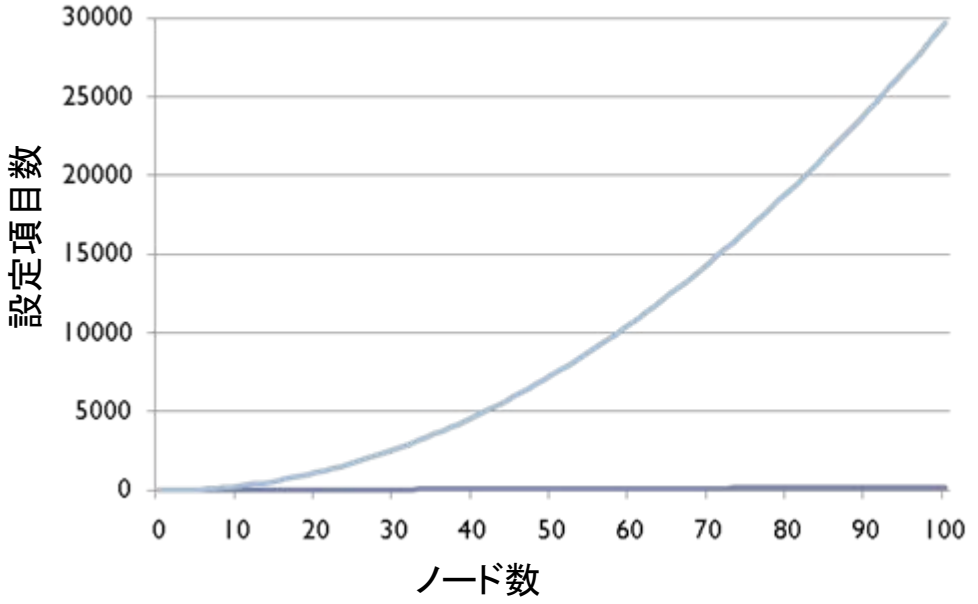
      必要設定数合計： $n \times (n-1) \times 3$
  - GSCIP
    - 必要設定コスト：ノード追加毎に２

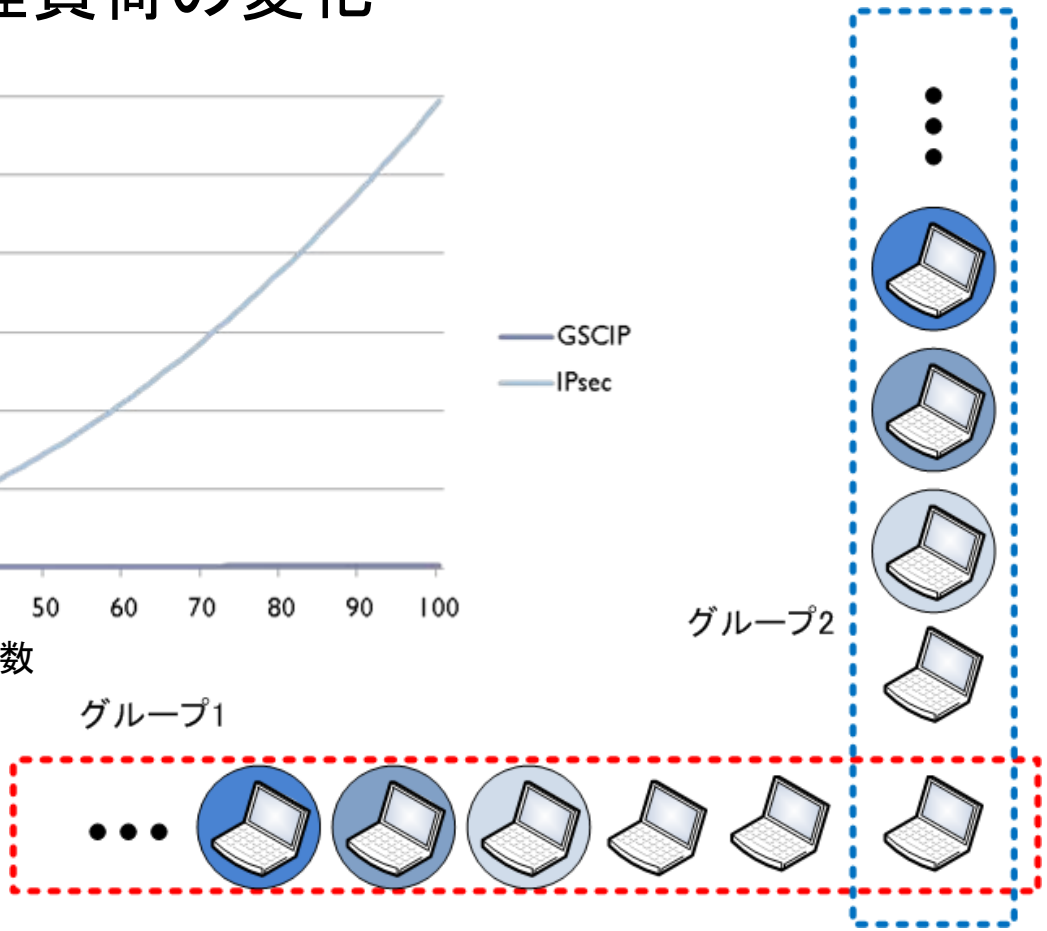
      必要設定数合計： $2n$



# 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



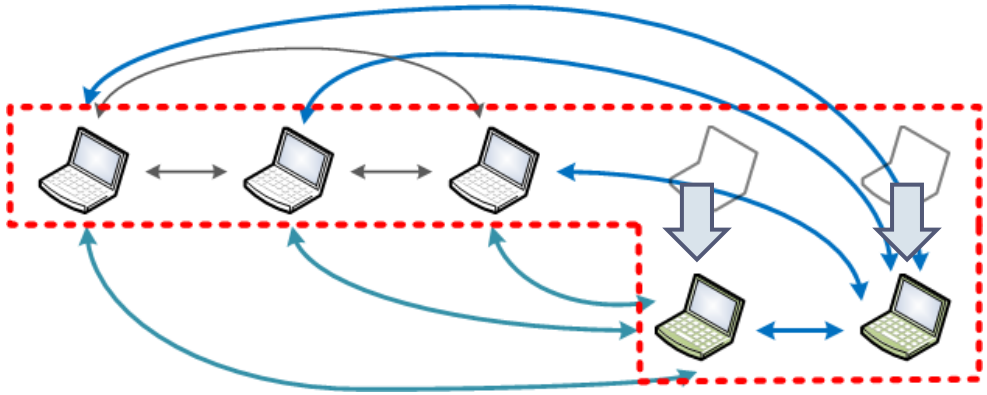




IPsec : $n \times (n-1) \times 3$

GSCIP : $2n$

# 管理負荷の比較 – システム構成変化時

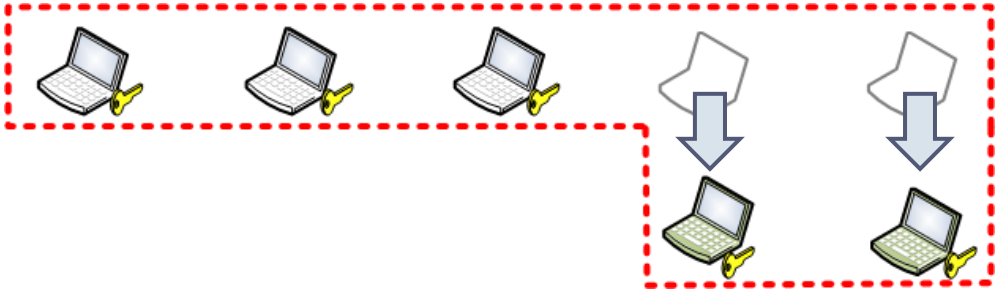
- ノードが移動した場合（IPsec）



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

# 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 | |