# 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

073432006　今村圭佑
渡邊研究室

## 1　はじめに

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あるべき姿の概念として FPN（Flexible Private Network）と呼ぶシステムを提唱してきた．また 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．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，配送を行う．端末は通信開始時に GSCIP 独自のネゴシエーションを行い，パケットの処理方法を動的に決定し暗号化/平文通信が可能である．

既存の暗号通信技術として IPsec があげられる．鍵交換プロトコルとして IKE，KINK があるが，セキュリティポリシの設定，ネゴシエーションの設定と設定項目が多く，複雑なネットワーク構成や通信する端末が増加すると設定による負荷が大きい．そのため管理負荷が少なくかつ部門や業務に応じた通信グループを柔軟に構築できる GSCIP が有効である．文献 [1] で GSCIP，IPsec の管理負荷について記述されているが，詳細な比較は行われていなかった．そこで本研究では，GMS を実装し GSCIP の実運用を試みた．その成果をもとに，適当なネットワークモデルにおける GSCIP と IPsec の管理負荷を比較評価し有効性を確認した．

## 2　比較技術

### 2.1　IPsec

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，通信経路上で通信内容の盗聴や改ざんを防止できる．IPsec を利用するには SA（Security Association）を両端末で共有する必要がある．SA を共有するために必要な鍵情報の交換を安全に行うプロトコルの代表的なものに，IKE や KINK があげられる．

IKE は SA の条件交換，DH 鍵交換，相手の認証の 3 つの基本機能を通して SA を生成する．図 1 に IKE のシーケンスを示す．IKE は 2 つのフェーズに分かれており，IKE_SA_INIT で SA の情報を交換するための SA を生成する．IKE_AUTH でこの SA を生成するためのパラメータの交換と相手認証を行う．IKE を実行するには，鍵交換アルゴリズム，暗号アルゴリズム．認証アルゴリズムなど事前設定項目が多く，端末が増加すると設定に負担がかかる．KINK は Kerberos 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．KINK では Kerberos が発行するセッション鍵を用いて相手認証と SA の交換を行うため IKE に比べ設定による負荷が少ない．

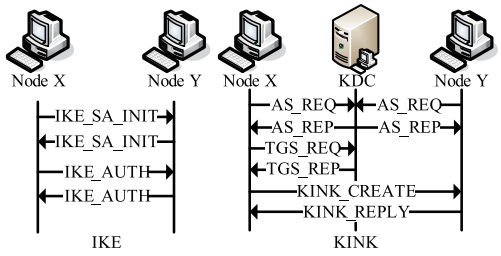



図 1: IKE，KINK のネゴシエーションシーケンス

### 2.2　GSCIP

GSCIP はセキュリティと柔軟性を兼ね備えた通信アーキテクチャである．図 2 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 には端末にソフトウェアをインストールして実現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．

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

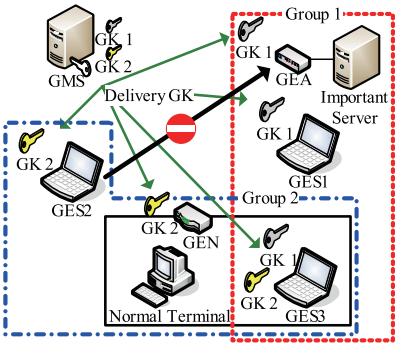



図 2: 通信グループの構築方法

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 に必要な情報はグループ管理サーバ GMS で定義される．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．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．通信の際は通信に先立ち，GE 間で GSCIP 独自のプロトコル DPRP（Dynamic Process Resolution Protocol） [1] を実行し，相手認証と通信の可否および暗号通信の有無を動的に決定する．

## 3　グループ管理サーバの実現

GSCIP を管理するグループ管理サーバ GMS の実装を行った．GMS は GE の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（動作モード）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．GE にはクライアントデーモンがあり，GMS からのグループ鍵取得や設定を行う．GMS の実装により，実際に GSCIP の運用管理が可能であることを確認した．

## 4　各方式の比較

### 4.1　管理負荷の比較

GSCIP/GMS + DPRP，IPsec/IKE，IPsec/Kerberos + KINK の管理負荷について比較評価した．各ノードおよびサーバで行う各設定 1 つあたりに必要な項目を負荷 1 と定義し，設定項目数により管理負荷の違いを求めた．想定するネットワーク環境を図 3 に示す．図 3 の想定環境では，ノード 1 と 4 で通信グループ 1 を構成し，ノード 2〜4 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，他の端末との通信は拒否できる．

GSCIP ではノード 1〜4 は GES1〜4 に対応づけられる．各 GE が所持するグループ鍵は GES1，4 がグループ鍵 1，GES2〜4 がグループ鍵 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 1 を使用しグループを構成し，通信グループ 2 はグループ鍵 2 を使用する．GSCIP では GE 起動時に GMS が確実な認証を行った後，グループ鍵番号とグループ鍵を配送する．他のノードと通信を開始する場合はまず DPRP を実行し，グループ鍵を用いて相手の認証を行う．そのためユーザが設定する負荷は少なく，想定環境を実現する場合の設定項目数は，各 GE にユーザ ID，GMS との共通鍵，GMS のアドレスの 3，GMS にはグループ鍵の設定が 8，各 GE が所属する通信グループの設定に 13，合計 33 である．

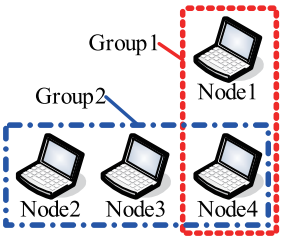



図 3: 想定するネットワーク構成

表 1: 各ノードの設定項目数

| | GSCIP | IPsec/IKE | IPsec/KINK |
|---|---|---|---|
| Node1 | 3 | 27 | 18 |
| Node2 | 3 | 29 | 18 |
| Node3 | 3 | 29 | 18 |
| Node4 | 3 | 31 | 21 |
| Server | 13，8 | − | 15 |
| 合計 | 33 | 116 | 90 |

IKE を用いる方法では，すべてのノードの通信には 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．また通信グループ 1 を構築するために，ノード 1，4 に事前共有鍵を共有する．同様に通信グループ 2 を構築するためにノード 2〜4 で事前共有鍵を共有する．さらに各ノードと IKE を行うための設定を行う必要がある．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 が 29，ノード 4 が 31，合計 116 である．

KINK を利用する場合は IKE と異なり Kerberos との共通秘密鍵と自己の ID，Kerberos 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 ID と秘密鍵のペアは 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るため，ID と秘密鍵のペアが 2 つ必要である．そのため設定項目数は 5 である．セキュリティポリシは IKE と同様な設定が必要である．さらに各ノードと KINK を行うため，通信相手の ID を設定する必要がある．ゆえに KINK を利用する場合の管理負荷はノード 1〜3 が 18，ノード 4 が 21，Kerberos サーバにはノードの ID と共有鍵の設定が 15，合計 90 である．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荷が増大する．

### 4.2　性能評価

2 台の端末間のネゴシエーションによるオーバヘッドを測定した．その結果 GSCIP では，ネゴシエーションに 0.38ms，通信開始までの時間は 1.78ms であった．IKE，KINK ではネゴシエーションに 264.09ms，3.07ms，TCP 通信開始までの時間は両者とも約 3 秒となった．GSCIP では通信に使用する暗号鍵を事前に配送してあるためネゴシエーション時間が短い．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，大幅に遅くなる．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 に比べ速い．ただし IKE，KINK とも最初のパケットがロスするため，TCP の再送（3 秒）により通信が開始される．

## 5　まとめ

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 と IPsec それぞれを運用する場合の管理負荷について比較評価した．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．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 の分散化等検討を進め，有効性を確認していく．

### 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 pp. 2976–2991 (2006).

# 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

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

名城大学大学院理工学研究科

渡邊研究室

今村圭佑

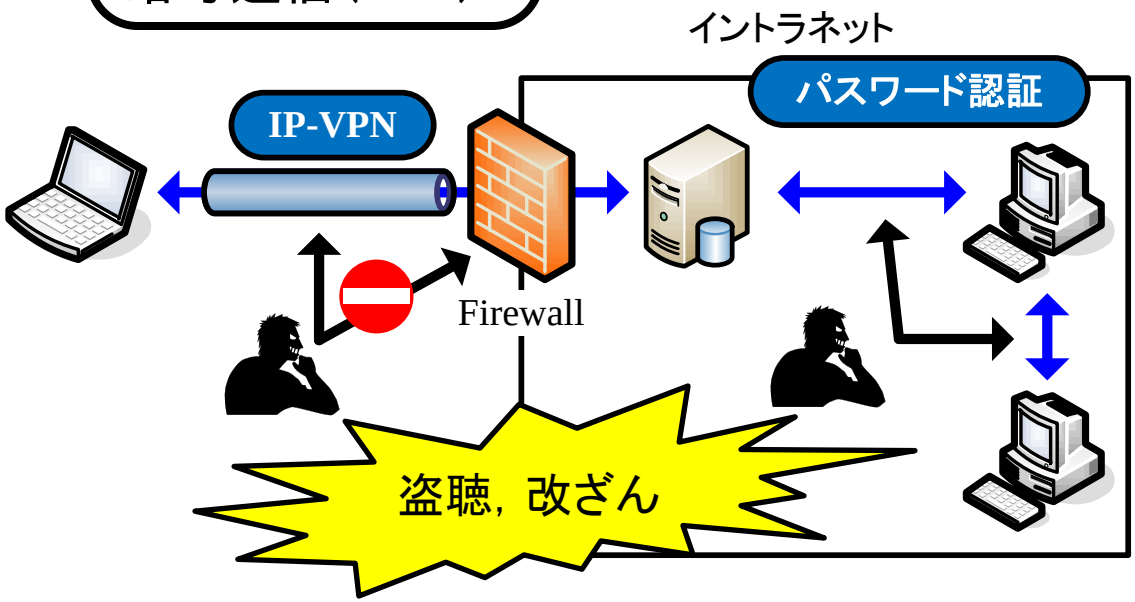
# 研究背景

- 企業ネットワークのセキュリティ対策は急務
  - 情報漏洩は社会的信頼の低下

**外部**
ファイアウォール
侵入検知
暗号通信（VPN）

**内部**
パスワード認証
平文通信

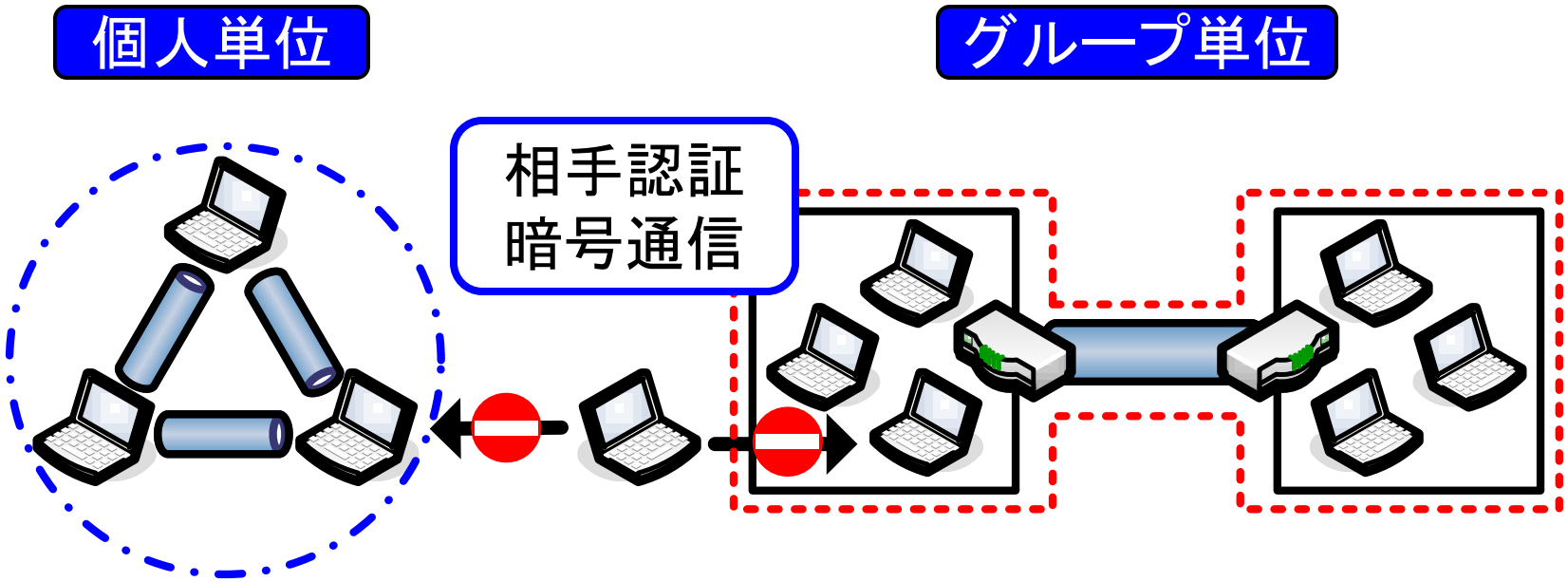
セキュリティの脅威は組織内部にも存在する




部門や業務に応じた通信グループを構築

通信グループ内の通信を暗号化

# 通信グループ構築方法



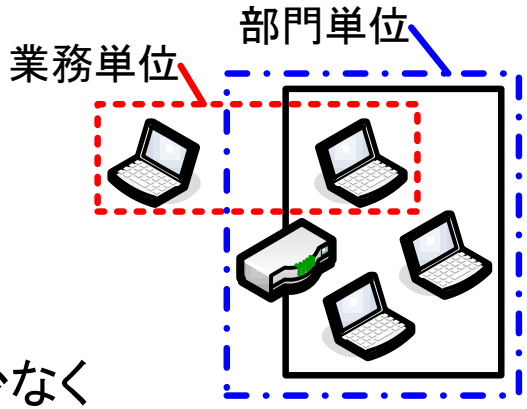

きめ細かいグルーピングが可能
個々に設定が必要：負荷大

大きな単位でグルーピングが可能
設定を集約できる：負荷小

両者の利点を活かした混在環境が有効

# 研究の目的

- 柔軟性・セキュリティ
  - 部門や業務内容による通信グループの構築
  - 通信グループ間の通信は暗号化
- 管理コスト
  - クライアントには最低限の設定
  - 複雑な通信グループ構成であっても設定コストは少なく



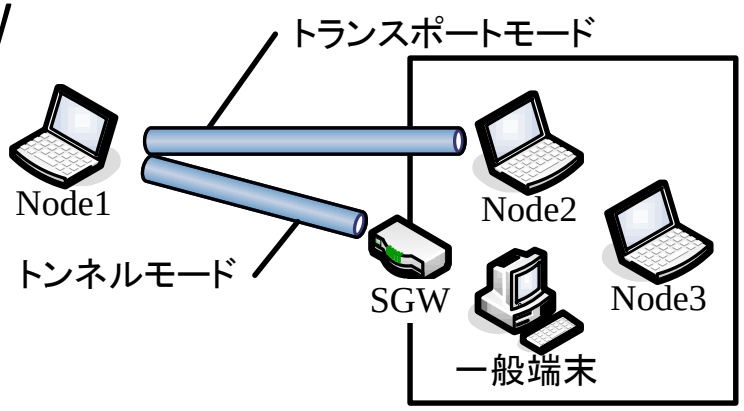

セキュリティを保ちつつ，管理コストを抑えた
GSCIP（Grouping for Secure Communication for IP）

- 混在環境を実現する場合の管理コストの比較評価
  - GSCIP
  - IPsec（IKE，KINK）

# 既存技術：IPsec

- TCP/IP上において汎用的に利用できる
  - トンネルモード：端末（SGW）ーSGW
  - トランスポートモード：端末ー端末

SA
- 送信元/宛先アドレス，プロトコル（ESP，AH）
- モード（トンネル，トランスポート）
- 通信に使用する暗号鍵



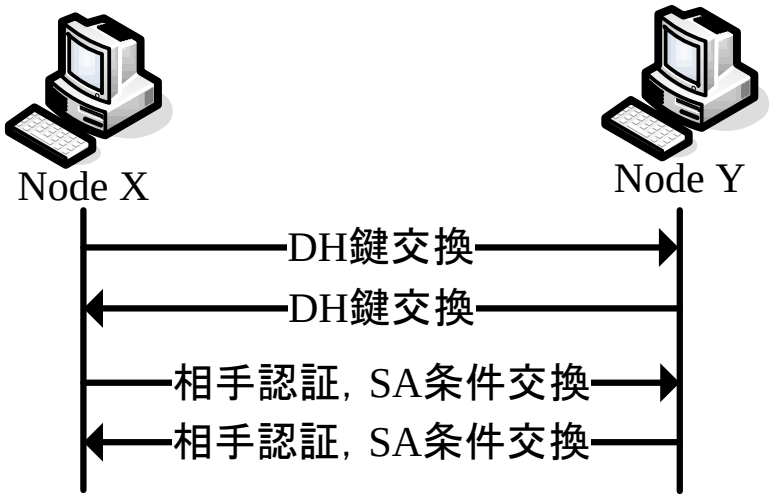

**互換性がないため別々に設定する必要がある**

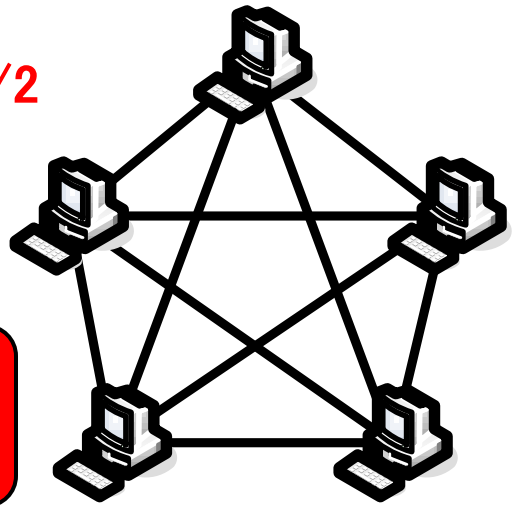
- SA共有のネゴシエーション技術
  - IKE（Internet Key Exchange）：RFC 4306
  - KINK（Kerberized Internet Negotiation of Keys）：RFC 4430

# IKE（Internet Key Exchange）

- ノード間SAパラメータの交換
- 通信に使用する暗号鍵の生成
  - DH鍵交換
- 相手認証
  - 事前共有鍵方式

  （事前に通信ピア間で鍵を共有する）
- 通信グループを導入する場合
  - 互いに事前共有鍵を設定する必要がある：n（n−1）/2
  - IKEではIPアドレスとペアで設定：2n（n−1）
  - IKEの設定に通信相手のアドレスを指定：n（n−1）



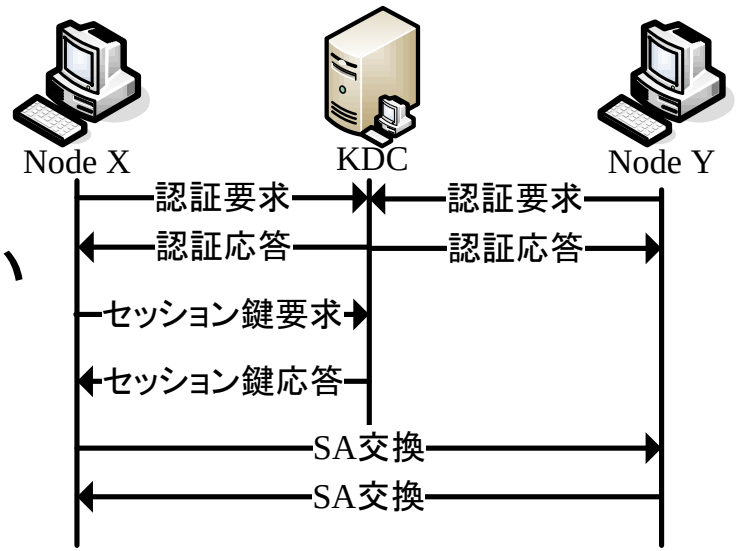
| | |
|---|---|
| x.x.x.x | KeyX |
| y.y.y.y | KeyY |
| z.z.z.z | KeyZ |

多台数間の設定は負担がかかる
複数のグループの定義は煩雑

# KINK（Kerberized Internet Negotiation of Keys）

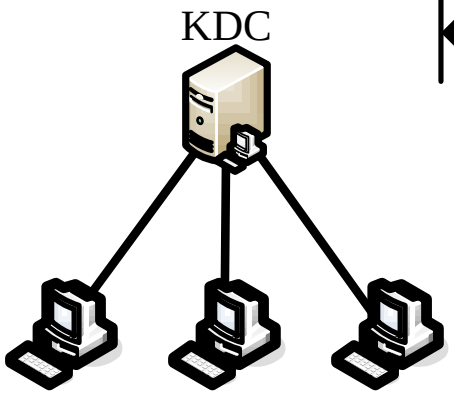
- Kerberosの共通鍵認証機構を利用したSA交換方法
  - ノードは事前にKerberosサーバ（KDC）と秘密鍵を共有
  - Kerberos IDと秘密鍵のペアをKDCが管理

KDCが提供するセッション鍵を用いSAの交換



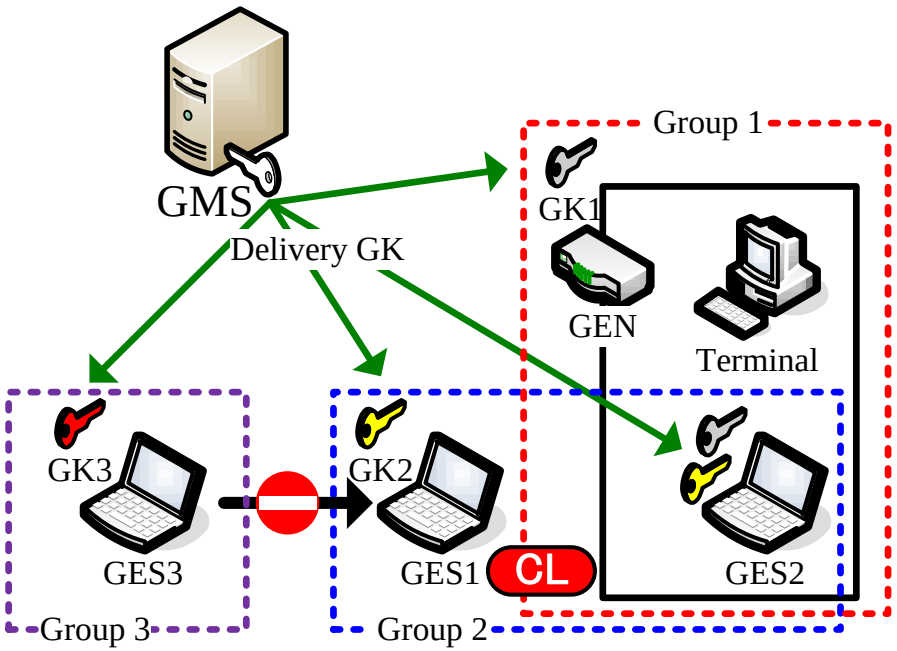

- 通信ピア間で鍵を共有する必要がない
- 通信相手のKerberos IDのみ設定
  - KDC－ノードの共有鍵：n
  - 通信相手のID：n（n−1）

IKEに比べ少ない



# GSCIPの概要

- 同じ暗号鍵を持つノードを同一の通信グループと定義
  - 暗号鍵＝グループ鍵GK
- グループ管理サーバ(GMS)おいて通信グループを定義
  - GMS－GE間で認証→GKの配送

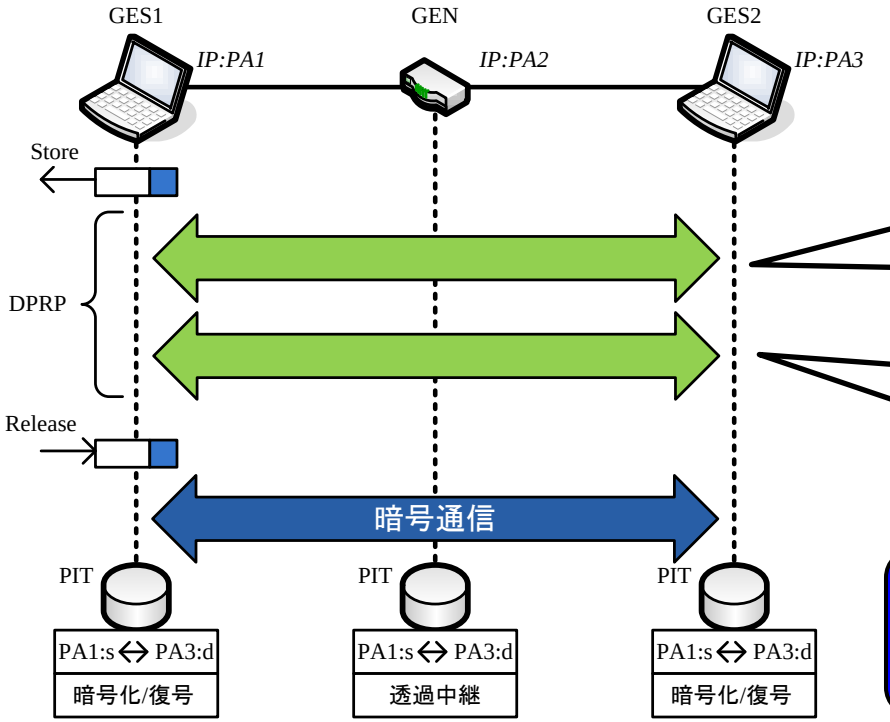



- GE：GSCIPに対応した装置
  - GES（Software型）：ホストタイプ
  - GEN（Network型）：ルータタイプ
- GMS（Group Management Server）
  グループ管理サーバ
  - GMS-GE間で鍵を共有
  - GEに対応するGKを配送
- 動作モード：他グループとの通信を定義
  - 開放モードOP：平文通信可
  - 閉域モードCL：一切禁止

**グループ鍵と通信グループを1対1で対応させる**

# DPRP（Dynamic Process Resolution Protocol）の概要

- 通信開始時にネゴシエーション
  - 端末間の認証処理：グループ鍵による認証
  - 動作処理情報の決定：所属通信グループ，動作モード




通信経路上の各GEの設定情報を取得し動作処理情報を決定

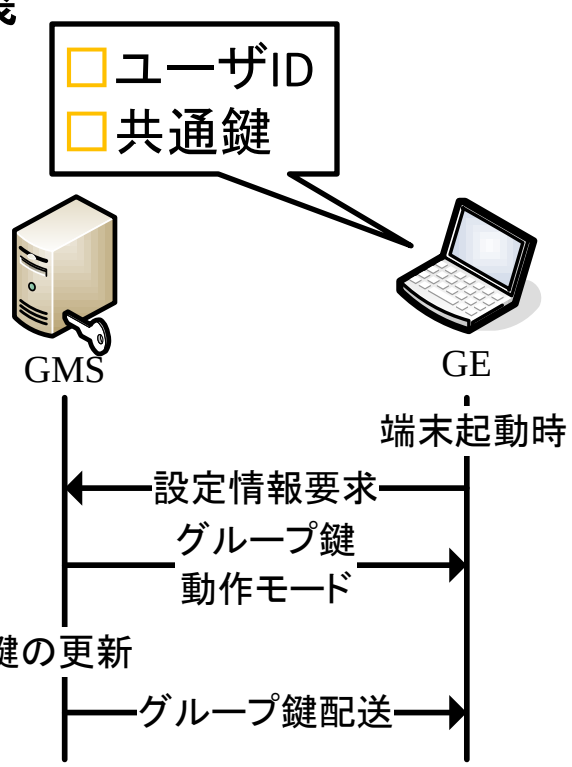
動作処理情報の生成と通知

パケットは動作処理情報に従って処理される

# グループ管理サーバGMS

- GSCIPのユーザや通信グループを管理する
  - グループ鍵の管理と通信グループの定義

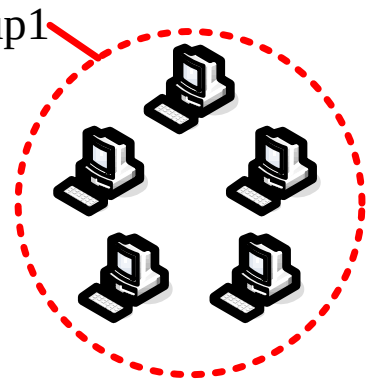
□GE情報
≫ユーザID，動作モード，共通鍵（GMS-各GE間）
□グループ鍵情報
≫通信グループ番号，グループ鍵GK，鍵バージョン
□所属通信グループ
≫ユーザID，通信グループ番号

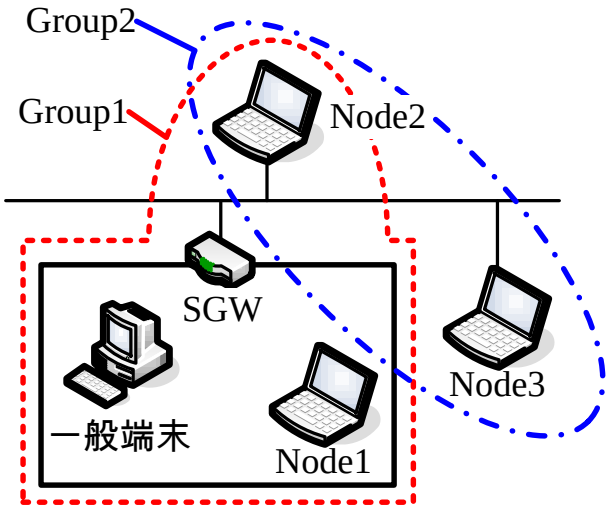



- 端末起動時に要求
  - 所属する通信グループの鍵情報を応答
- 通信開始時にDPRPネゴシエーションを実行
  - 端末間の動作処理情報の決定

# 本システムの有効性の評価

- 各方式の比較評価
  - IPsec/IKE
  - IPsec/Kerberos+KINK
  - GSCIP/GMS+DPRP



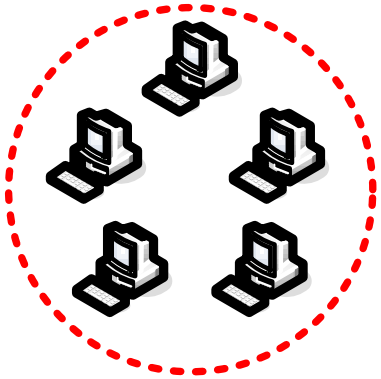




- 評価項目
  - ノード数に応じた設定コスト
  - 実環境を想定した設定コスト

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，管理コストの比較を行う

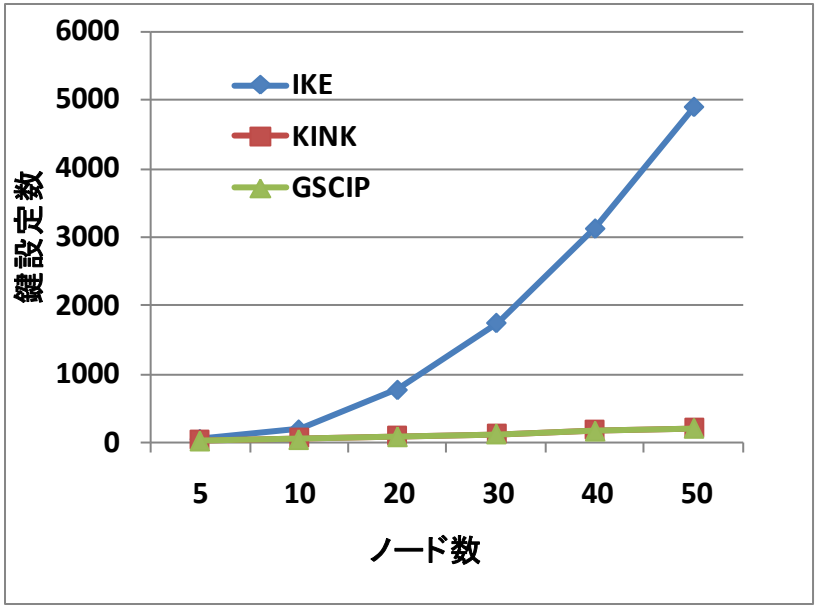
# ノード数に応じた鍵管理コスト

- IKEは全ピア間で鍵を共有するため設定コストは高い
  - IPアドレス，鍵のペアを互いに共有
- KINK，GSCIPはサーバ，ノード間の共有鍵
  - 自己のID，サーバとの共通鍵



IKE：全ピア間で鍵を共有：n×（n−1）×2
KINK：KDCとノード間のID，共通鍵：2n×2
GSCIP：GMSとノード間のID，共通鍵：2n×2

**多台数間の設定は
大幅にコストが増加**



# ノード数に応じた設定コスト

- IPsecではSAに通信相手のIPアドレスを送受信ペアで設定
  - ノード数に大きく影響する

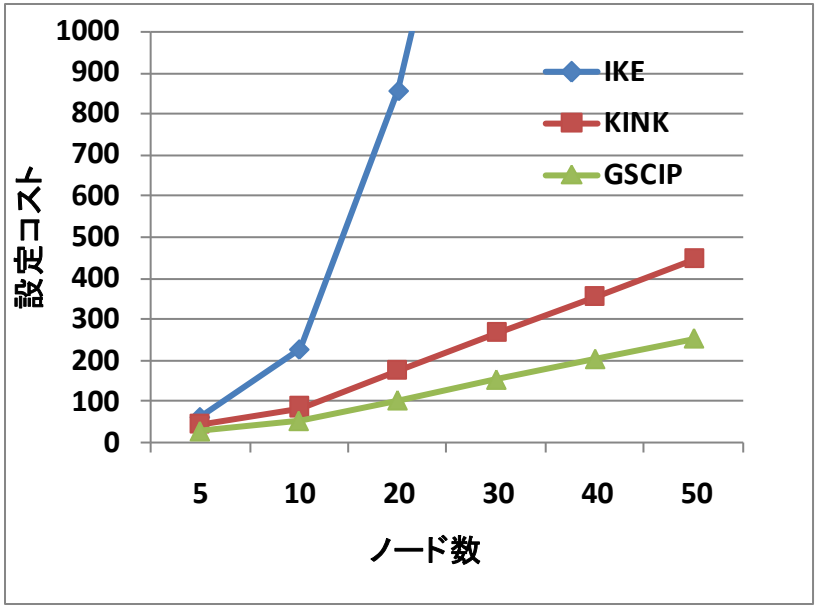
IKE：SAに全ノードのアドレスのペア：2(n-1)×2
KINK：SAに全ノードのアドレスのペア：2(n-1)×2
GSCIP：所属通信グループの定義：n

ノードA

送信：IP_A→IP_B
受信：IP_B→IP_A

IKE，KINKはネゴシエーションに
IPアドレスの設定要素を含む

GSCIPはグループ鍵で管理している
IPアドレスに依存しない

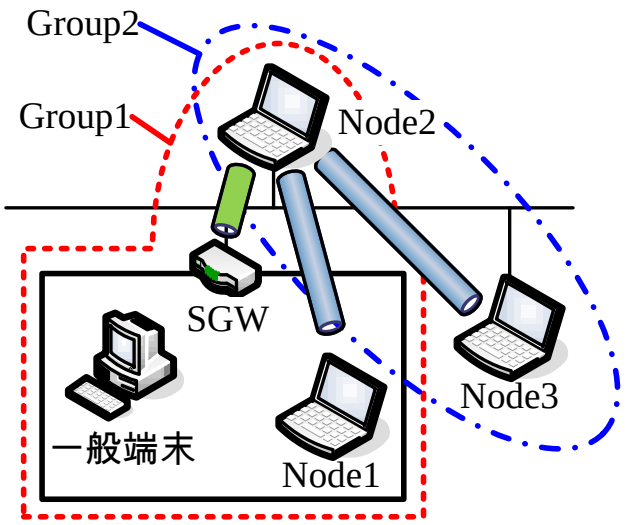


# 初期管理負荷：IPsec/IKE

| | 事前共有鍵情報 | セキュリティポリシ | IKE | 合計 |
|---|---|---|---|---|
| ノード1 | 2：ノード1→ノード2 | IPsec Transport:14 | 11 | 27 |
| ノード2 | 6：ノード2→1，3，SGW | IPsec Transport:14+2<br>IPsec Tunnel:16 | 13 | 51 |
| ノード3 | 2：ノード3→ノード2 | IPsec Transport:14 | 11 | 27 |
| SGW | 2：SGW→ノード2 | None:8, Discard:8 | 11 | 29 |
| 合計 | 12 | 76 | 46 | **134** |

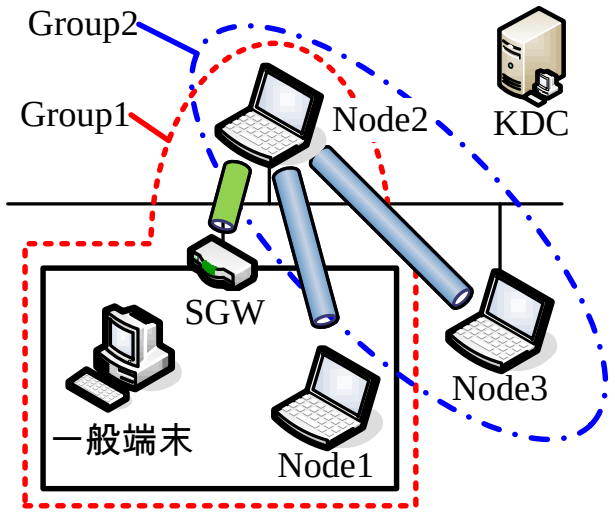
トンネル，トランスポートモードに互換がなく
別々に定義する必要がある

通信ペアが増加すると事前共有鍵の
設定が増加する



# 初期管理負荷：IPsec/Kerberos+KINK

| | KDC | セキュリティポリシ | KINK | 合計 |
|---|---|---|---|---|
| ノード1 | 3 | IPsec Transport:14 | 1 | 18 |
| ノード2 | 3＋2 | IPsec Transport:14+2<br>IPsec Tunnel:16 | 3 | 39 |
| ノード3 | 3 | IPsec Transport:14 | 1 | 18 |
| SGW | 3 | None:8, Discard:8 | 1 | 20 |
| 合計 | 14 | 76 | 6 | 96 |




**KDC：15 + 96 ＝ 111**

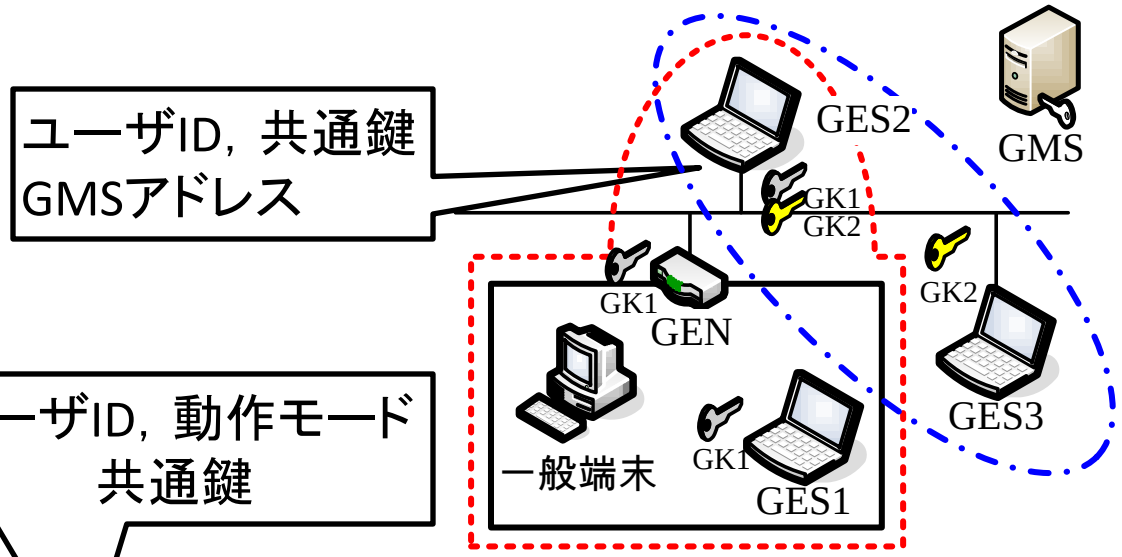
**ノード**：ID，共通鍵，KDC
**KDC**：ID，共通鍵，通信グループ

トンネル，トランスポートモードに互換がなく
別々に定義する必要がある

所属する通信グループが増加すると
IDとサーバとの共通鍵が増加する

# 初期管理負荷：GSCIP/GMS+DPRP

- GMSに所属する通信グループを定義するのみ




グループ番号
鍵バージョン，GK

ユーザID，動作モード
共通鍵

| 所属通信グループ情報 | |
|---|---|
| GES1 | グループ1 |
| **GES2** | **グループ1** |
| **GES2** | **グループ2** |
| GES3 | グループ2 |
| GEN | グループ1 |

| | 設定数×台数 | 合計 |
|---|---|---|
| GE情報 | 3×4 | 12 |
| グループ鍵情報 | 3×2 | 6 |
| 所属通信グループ情報 | 2×5 | 10 |

**GE：12＋28 ＝ 40**

# 各方式の比較

| | GSCIP/GMS+ DPRP | IPsec/IKE | IPsec/Kerberos +KINK |
|---|---|---|---|
| ノード数に応じた鍵管理コスト | サーバ，クライアント間のみ | 全ピア間で鍵を共有<br>n×（n−1）×2 | サーバ，クライアント間のみ |
| ノード増加による管理コスト | 通信グループの定義のみ | IPアドレスに依存し増加する | IPアドレスに依存し増加する |
| イニシャル管理コスト（想定した環境の設定数） | グループ鍵と通信グループを一対一で対応付け：40 | 事前共有鍵が大幅に増加<br>134 | ID，共通鍵のペアがグループに応じて増加：111 |

IPsecは複雑なネットワーク構成になると大幅にコストが増加する

柔軟性とセキュリティを兼ね備えたグループ通信が可能である

# まとめ

- 柔軟性とセキュリティを兼ね備えた通信アーキテクチャGSCIP
  - 通信グループとグループ鍵を1対1で対応させることで，IPアドレス，物理的配置に依存しないグルーピングが可能
  - グループ管理サーバの実装を行い，実運用にて有効性を確認

**管理負荷を抑えつつ運用が可能であり**
**セキュリティ対策として有効な方法である**

- 今後
  - 負荷分散のためGMSの分散化とその連携
  - GSCIPをインターネット空間へ適用
    - GMSの運用方法の検討

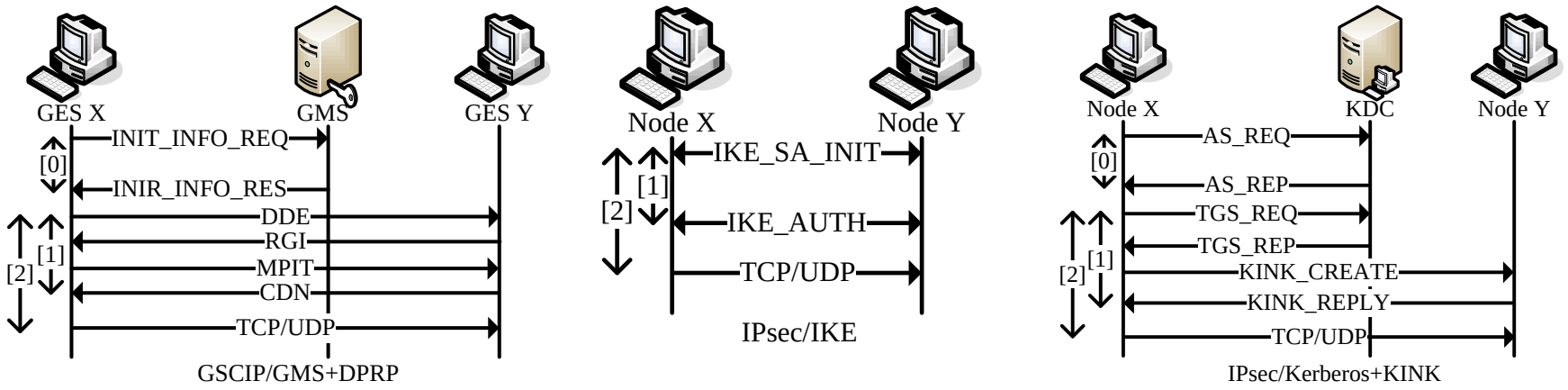
# 付録

# 通信性能測定環境

- [1]ネゴシエーション時間
- [2]通信開始までの時間
- [0]情報配送時間

OS : FreeBSD6.1
CPU : Pentium4 3.0GHz
MEMORY : 1GB
Ethernet : 1000BASE-TX

試行回数 : 10回
IKE，KINKにはracoon2を使用
KerberosサーバにはHeimdalを使用



# 測定結果

- ネゴシエーション
  - GSCIP：起動時にグループ鍵を取得
  - IKE：ネゴシエーション時に共通鍵を生成（DH）
  - KINK：KDCがセッション鍵を生成し配送

- 通信開始までの時間
  - GSCIPではトリガーとなったパケットをカーネル内に待避
  - IPsecではTCPの再送処理に頼っている

TCP再送処理

| | DPRP | IKE | KINK |
|---|---|---|---|
| [0]情報配送 | 6.11 | — | 0.89 |
| [1]ネゴシエーション | 0.38 | 264.09 | 3.07 |
| [2]通信開始までの時間（TCP） | 1.78 | 2862.15 | 3037.98 |
| [2]通信開始までの時間（UDP） | 1.89 | 429.92 | 16.03 |

単位：ミリ秒

# 暗号化処理モジュールについて

- PCCOM（Practical Cipher COMmunication）
  - パケットフォーマットを変更せずに
    - 本人性確認，パケット全体の完全性保証を実現
  - NATやFWを通過可能（イントラネットでは有効）

FTPダウンロード時間

単位：sec

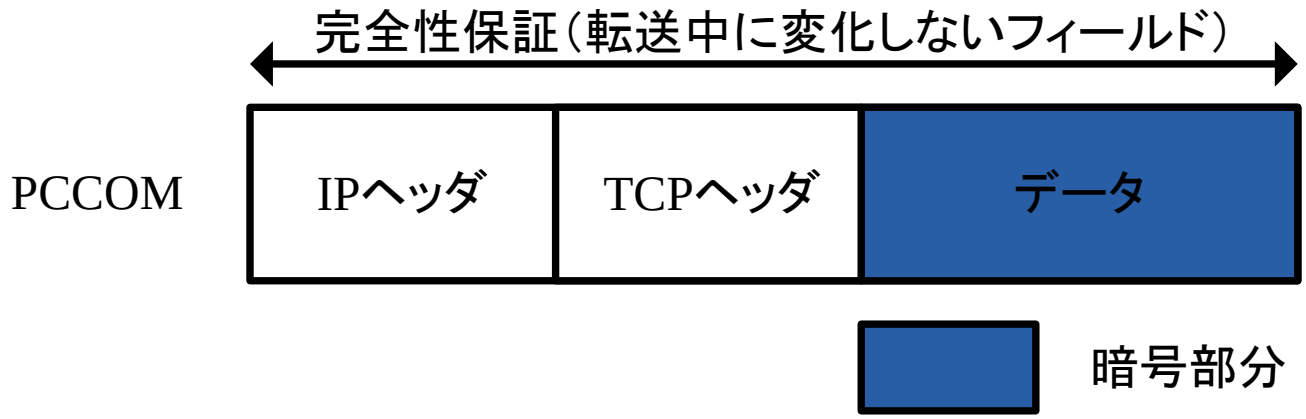
| Normal | PCCOM | IPsec ESP |
|---|---|---|
| 13.94 | 20.22 | 43.43 |

500MBのファイルをダウンロード

スループットの低下は少ない

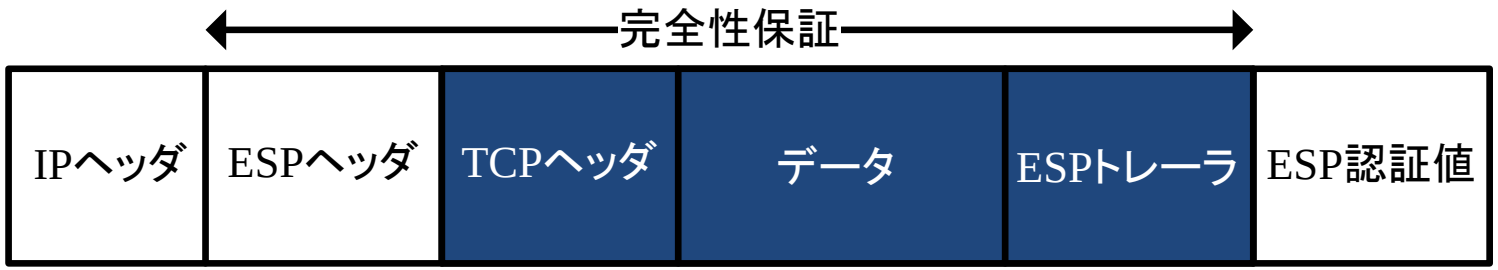
# PCCOM詳細

- 完全性保証・本人性確認
  - 疑似データを用いたTCP/UDPチェックサムの独自計算により実現
  - IPアドレスとポート番号の完全性は動作処理情報の検索過程で保証
    - NATと共存可能
- ユーザデータのみを暗号化
  - 従来どおりパケットフィルタリング可能で，ファイアウォールと共存可能



# IPsec ESP詳細

- TCPヘッダを含め暗号化
  - TCPヘッダにポート番号を含む
  - NATを通過させるにはUDPでカプセル化



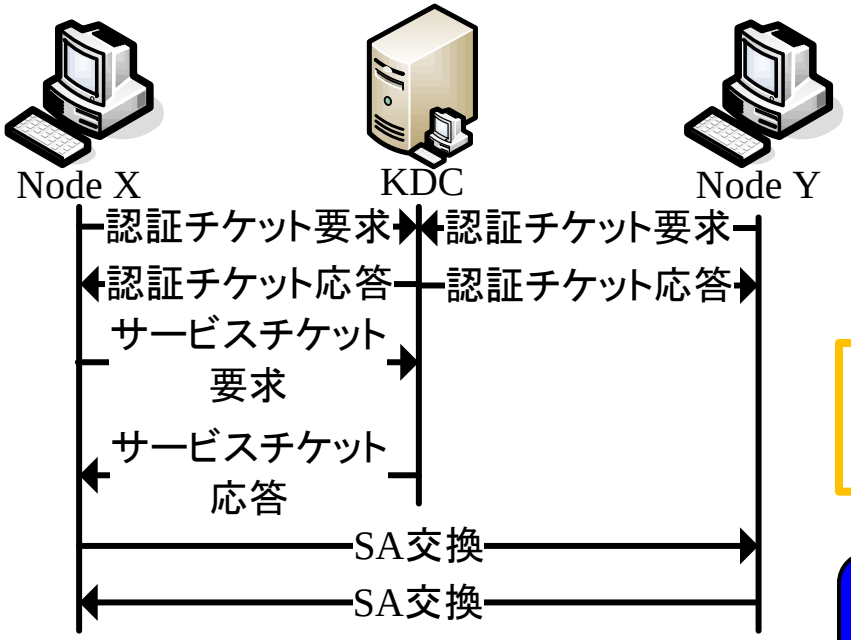
# IPsec ESPとPCCOM

- IPsecは強靭なセキュリティ
  - インターネット空間への適用
- PCCOMはイントラネットの環境に特化
  - NATやFWと共存できるためイントラネットへの適用

| | IPsec ESP | PCCOM |
|---|---|---|
| 機密性 | ◎ | ○ |
| 本人性確認 | ◎ | ○ |
| 完全性保証 | ◎ | ○ |
| NAT | △ | ○ |
| ファイアウォール | △ | ○ |
| フラグメント | △ | ○ |
| トラフィック解析 | ○ | △ |

# KINK（Kerberized Internet Negotiation of Keys）

- Kerberosの共通鍵認証機構を利用したSA交換方法
  - ノードは事前にKDCと秘密鍵を共有
  - ノードIDと秘密鍵をKDCが管理



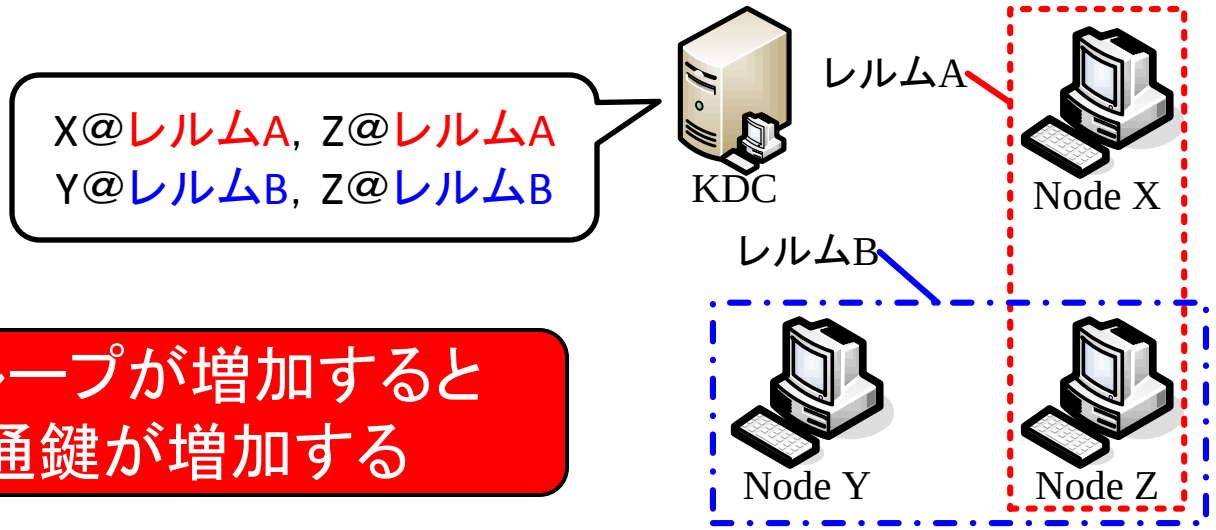

ノードとKDCは事前に鍵を共有
ノードはレルムに所属

サービスチケット
鍵x{セッション鍵，鍵y{セッション鍵，IDx}}

KDCが提供するセッション鍵を用い
SAの交換

# KINK（Kerberized Internet Negotiation of Keys）

- KINKでグループ通信を導入すると・・・
  - 通信グループの定義をKDCに集約
  - クライアントには通信相手のKerberos IDだけでよい：n
  - 所属グループに応じてKerberos ID，共通鍵が必要である
    - 複数のID，共通鍵を所持する



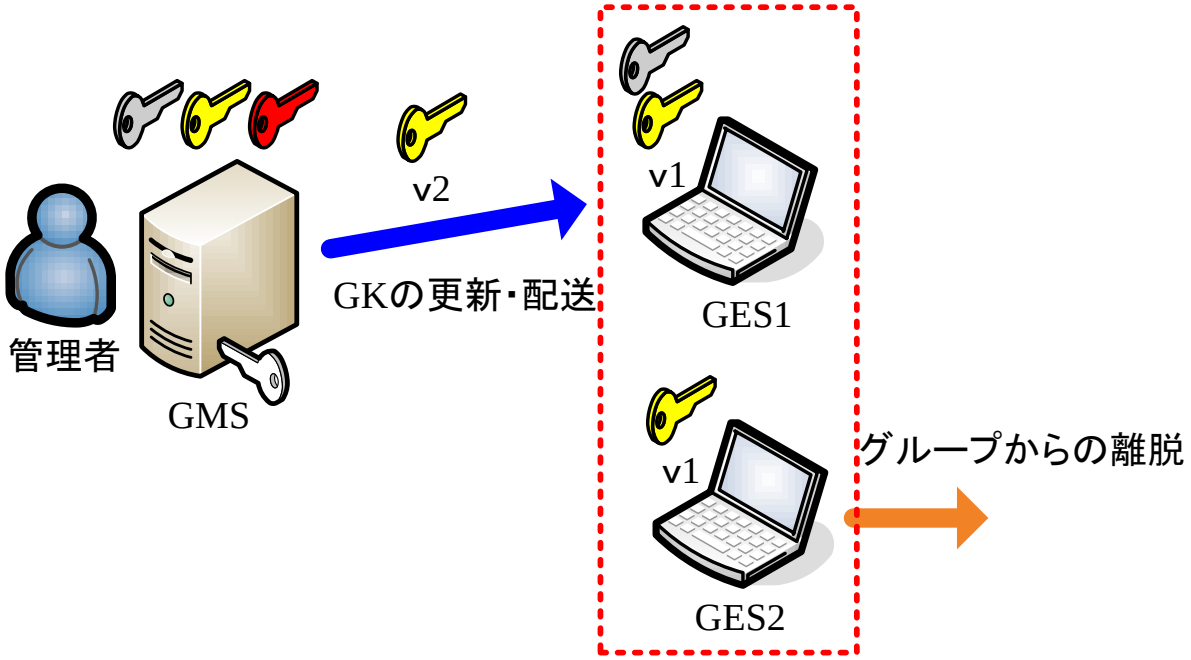

所属する通信グループが増加すると
IDとKDCとの共通鍵が増加する

# SSL（TSL）

- 特徴
  - ペイロードを暗号化したTCP
- 長所
  - NATとの併用が可能
  - Webアプリケーションのセキュリティ確保は，事実上標準
- 短所
  - WWWサービス以外ではあまり普及していない
  - Socket APIとは別のAPI を利用するため，非SSLアプリケーションをSSL対応させるには，アプリケーションの修正が必要

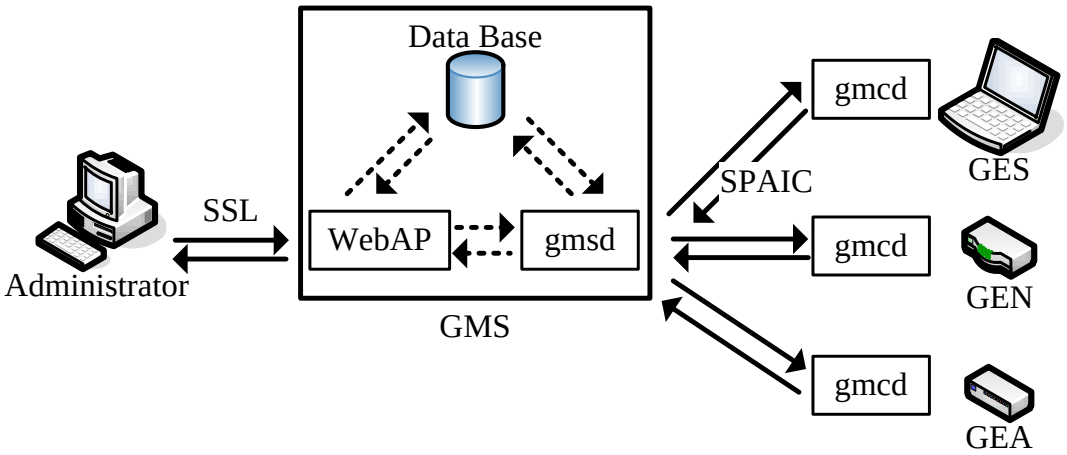
# グループ鍵の更新

- 通信グループから離脱
- 一日毎に更新(3時)



# グループ管理サーバの実装

- Fedora6（Linux）に実装
  - サーバデーモン：gmsd
  - データベース：MySQL
  - Webアプリケーション：Apache
- GE：FreeBSD6.1
  - クライアントデーモン：gmcd



# IKEの相手認証方式

- 事前共有鍵方式
  - スケーラビリティに欠ける
- デジタル署名方式
- 公開鍵方式
  - キック（通信グループの定義方法？）

事前共有鍵方式以外
は実装が必須ではない