GSCIP と IPsec を併用したリモートアクセス方式の提案

030432017　今村圭佑
渡邊研究室

1. はじめに

ホットスポットの普及や在宅勤務の増加により，外出先等から社内ネットワークへアクセスするための VPN 構築が普及してきた．VPN 構築手法として様々な選択肢があるが，特に IPsec や SSL を利用したリモートアクセスが注目を浴びている．IPsec を利用したリモートアクセスは，IKE（Internet Key Exchange）を拡張することで提供される．しかし，IPsec はユーザが増加するとアクセス制御が煩雑になる．一方，SSL は Web アクセスを用いたアプリケーションでしか利用できないという問題が存在する．そこで，任意のアプリケーションが利用可能でかつ，End-to-End でセキュア通信を実現することを目的として，我々が提案しているグループ通信方式 GSCIP（Grouping for Secure Communication for IP）[1]と IPsec を併用したリモートアクセス方式を提案する．

2. GSCIP の概要

GSCIP におけるグルーピングの原理を図 1 に示す．グループ管理装置 GMS（Group Management Server）から，あらかじめ GSCIP を実装した装置 GE（GSCIP Element）へグループ鍵 GK（Group Key）を配送する．同一の GK を所持する GE の集合が，同一の通信グループを構成する．端末間の通信に先立ち，DPRP（Dynamic Process Resolution Protoco l）[2]によるネゴシエーションが行われる．DPRP は通信経路上に存在するすべての GE 間で設定されているグループ情報を相互に交換することで，各 GE 内に通信パケットの処理に必要となる動作処理情報テーブル PIT（Process Information Table）を動的に生成する．GE 間の通信は，DPRP により生成された PIT に基づき，GK により暗号化されたり，破棄されたりする．

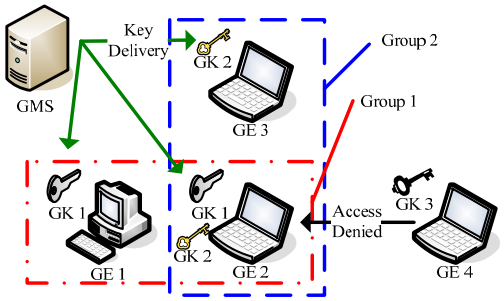


図 1.　GSCIP におけるグルーピングの原理

3. 提案方式

図 2 に GSCIP と IPsec を用いたリモートアクセスの構成例を示す．リモート端末と IPsec-VPN 装置間は，IPsec を用いてトンネルを構築する．リモート端末の認証は，IKE-XAUTH（eXtended AUTHentication）などを使用し，事前共有鍵，ユーザ名，パスワードで認証を行う．リモート端末の IP アドレスの割り当ては，IPsec-DHCP により行い，IPsec-VPN 装置からプライベート IP アドレスを割り当てる．上記の手続きにより，リモート端末は，透過的に社内ネットワークの一部に取り込まれる．

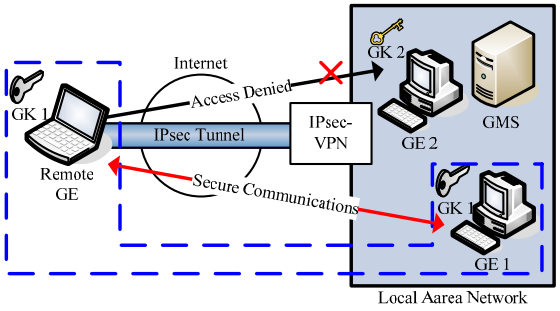


図 2.　提案方式の構成例

その後，リモート端末は社内 LAN に設置された GMS に対して，グループ鍵の配送を依頼する．以後の動作は，GSCIP の動作と同様に，同一の GK を所持する GE 同士でグループを構成する．動作処理テーブル PIT により，GK による暗号化，アクセス拒否を行うことが可能である．

表 1：提案方式と IPsec-VPN の比較

	提案方式	IPsec-VPN
管理負荷	○：GK により個人単位やサブネット単位での構成が容易	△：個人単位やサブネット単位の構成は，規模が大きくなると煩雑

表 1 に提案方式と IPsec トランスポートモードを使用した際の比較を示す．GSCIP と IPsec を利用することにより，リモート拠点から社内の重要なサーバまで End-to-End でセキュリティを確保しつつ，柔軟なアクセス制御を兼ね備えたリモートアクセスが可能となる．

4. まとめ

GSCIP と IPsec を併用したリモートアクセス方式の提案を行った．今後は，実装と評価を行う．

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を実現するセキュア通信アーキテクチャ GSCIP の提案，DICOMO2005 シンポジウム論文集，Vol.2005，No.6，pp.441-444，Jul.2005.
[2] 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，Nov.2006.

GSCIPとIPsecを併用したリモートアクセス方式の提案

A Proposal of a Remote Access Method using GSCIP and IPsec

名城大学理工学部情報科学科

渡邊研究室

030432017　今村　圭佑

研究背景

- ホットスポットの普及や在宅勤務者の増加
  - 社外から社内にアクセスしたいという需要が高まる

盗聴，改ざん，成りすまし

- リモートアクセスVPNが注目を浴びている
  - 社外から社内までセキュリティを確保

暗号化
ユーザ認証

インターネット空間での脅威から通信を守る

研究背景

- 企業ネットワークにおけるセキュリティ脅威
  - IDとパスワードだけに頼るなど脆弱
  - イントラネット内のユーザによる内部犯罪の増加

情報漏えいの
80%以上は内部から

インターネット，イントラネット共にセキュリティを確保
セキュアなリモートアクセスを提案

既存リモートアクセスVPN

- リモートアクセスVPNを構築するシステム
  - IPsec（Security Architecture for Internet Protocol）
  - SSL（Secure Sockets Layer）
  - PPTP（Point to Point Tunneling Protocol）
  - L2TP（Layer 2 Tunneling Protocol）
  - SOCKS

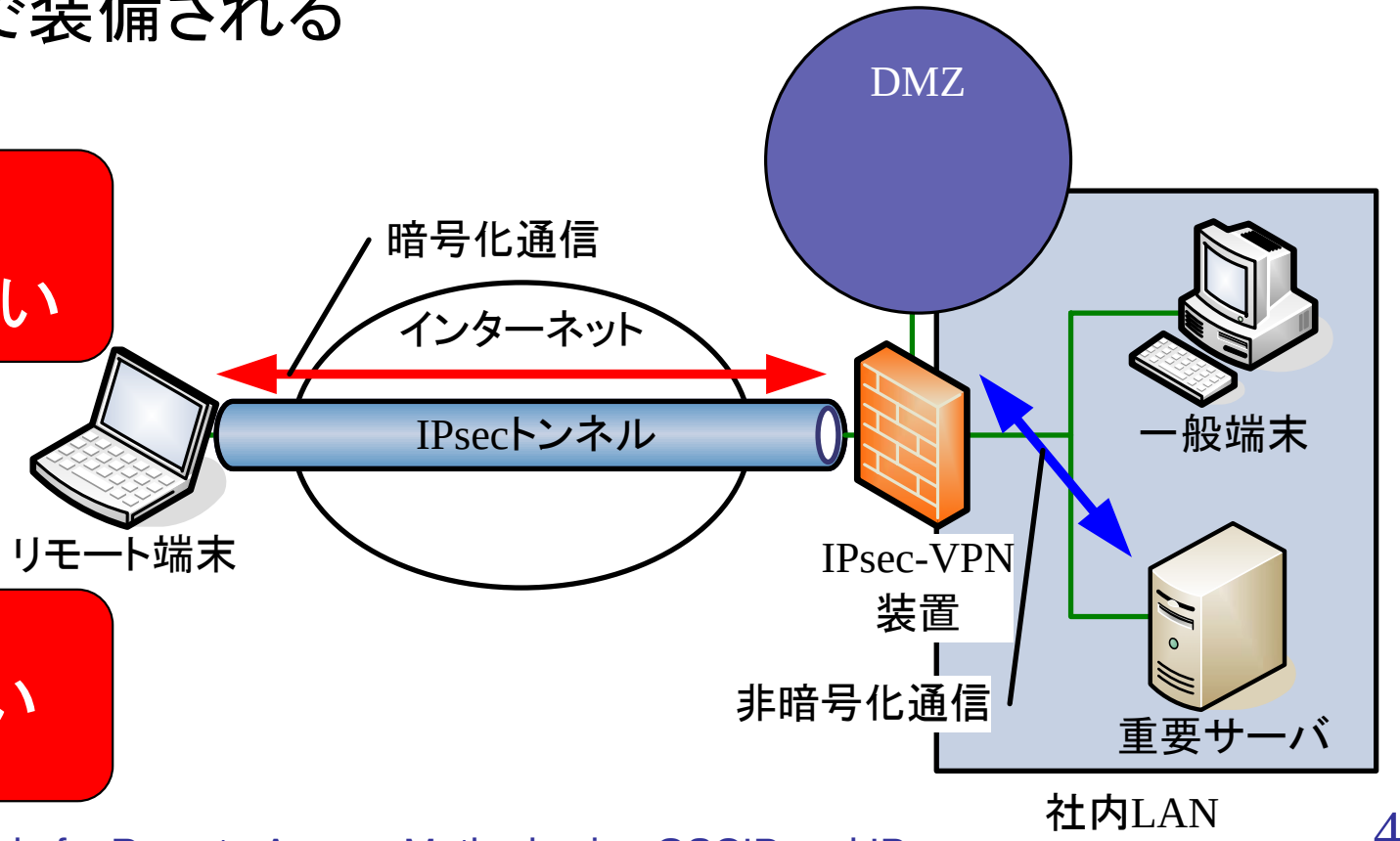
リモートアクセスVPNとしてIPsec，SSLが
良く利用されている

IPsecの概要と問題点

- インターネットで暗号通信を行なうための規格
- ネットワーク層に実装されており，TCPやUDP，SMTP，POP3などアプリケーションは意識せずに利用できる
- IPv6では標準で装備される

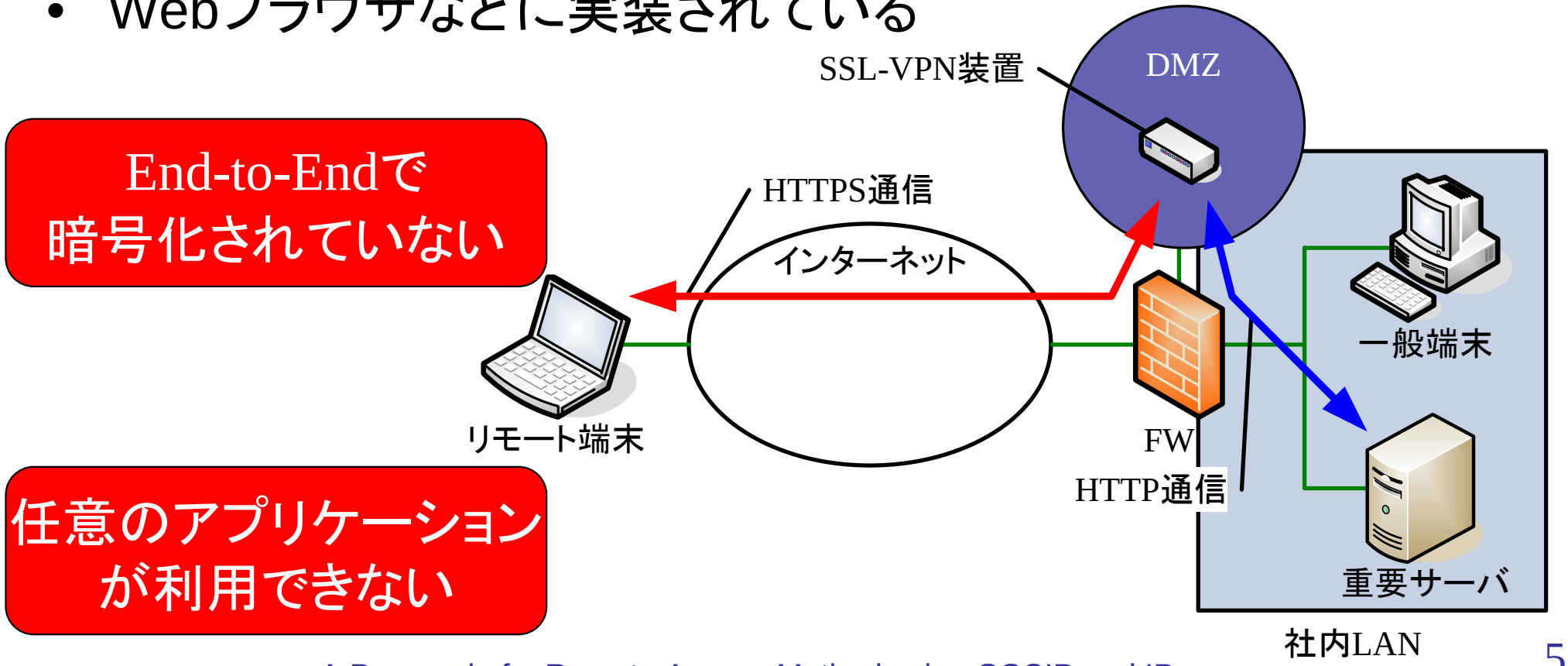
End-to-Endで
暗号化されていない

管理負荷が大きい



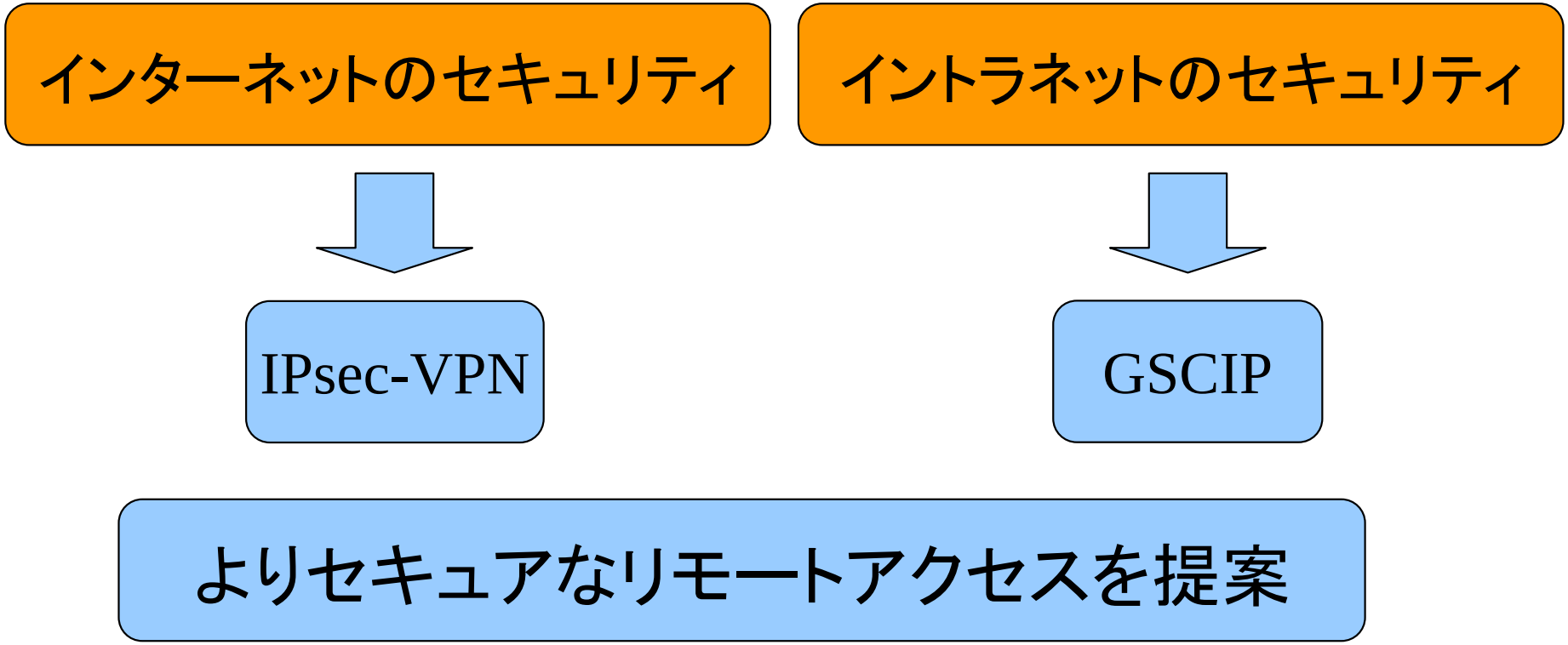
SSLの概要と問題点

- インターネット上で情報を暗号化して送受信するプロトコル
- レイヤ5とレイヤ4の間に実装されており，HTTPやFTPなど上位プロトコルを利用するアプリケーションが使用できる
- Webブラウザなどに実装されている



提案方式の目的

- 任意のアプリケーションが利用可能
- End-to-Endのセキュリティを確保
- 管理負荷の低減

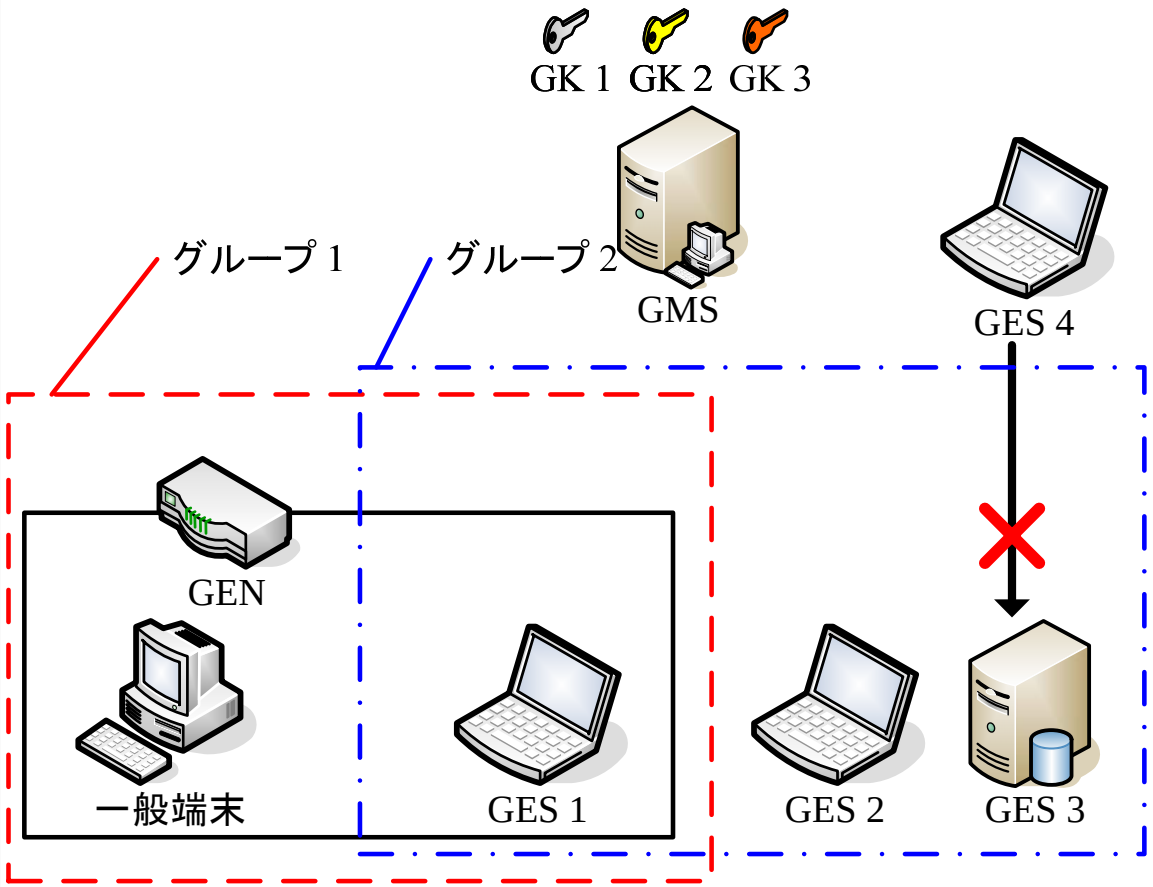


GSCIPの概要

- GSCIP (Grouping for Secure Communication for IP)
  - 同一の暗号鍵を持つもの同士が同一の通信グループを形成
  - グループ鍵（GK）と通信グループは1対1に対応
  - ネットワーク単位，個人単位が混在した環境でも簡単にグルーピングが可能
  - グループ間通信は，グループ鍵により暗号化
  - IPレベルでの暗号化

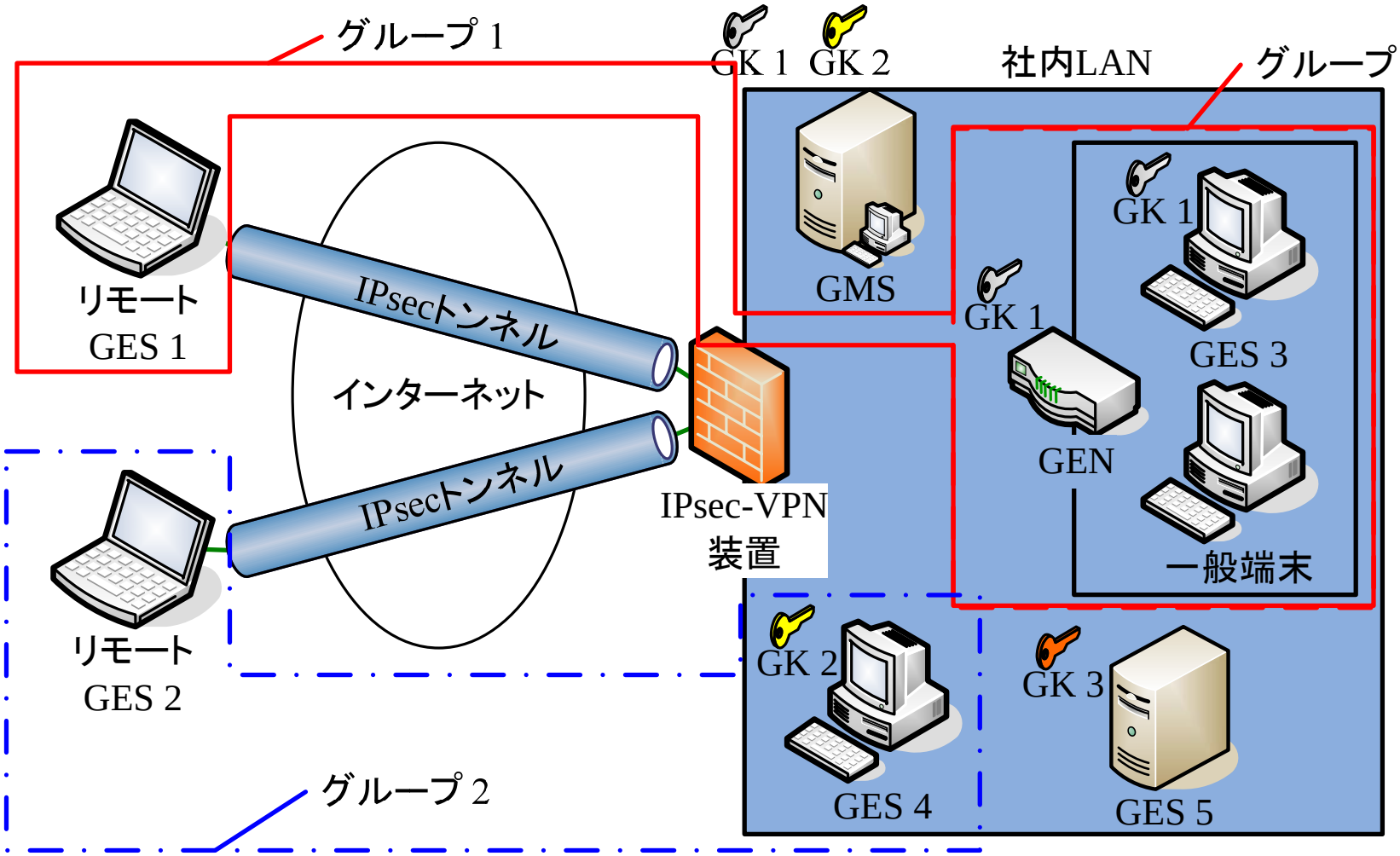
GSCIPの動作概要

- GSCIPの構成



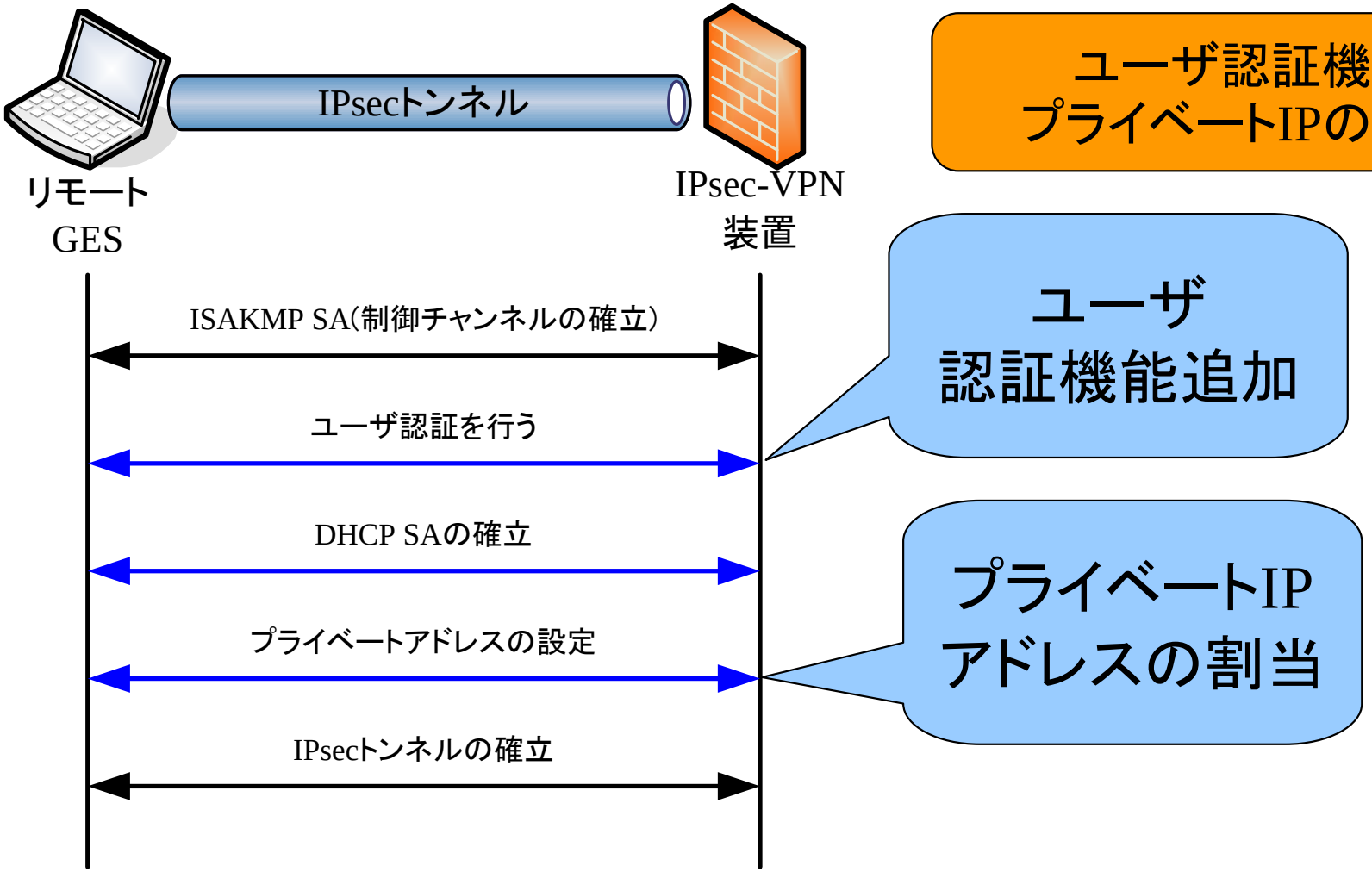
- ◆ 構成要素
  - □GE（GSCIP構成装置）
    - ≫GES（ソフトウェア型）
    - ≫GEN（ネットワーク型）
  - □GMS（グループ管理装置）
- ◆ GMSから各GEに定義情報の配送
  - □ GMS-GE間は公開鍵認証
  - □グループ情報，GKを配送
- ◆ 通信グループの定義
  - □同一のGKを持つGE同士で構成
  - □GKとグループは一対一に対応

GSCIPとIPsecを併用したシステム構成



GSCIPをリモート端末にも適用し，
End-to-Endのセキュリティを確保

リモートアクセスにおけるIPsecの動作



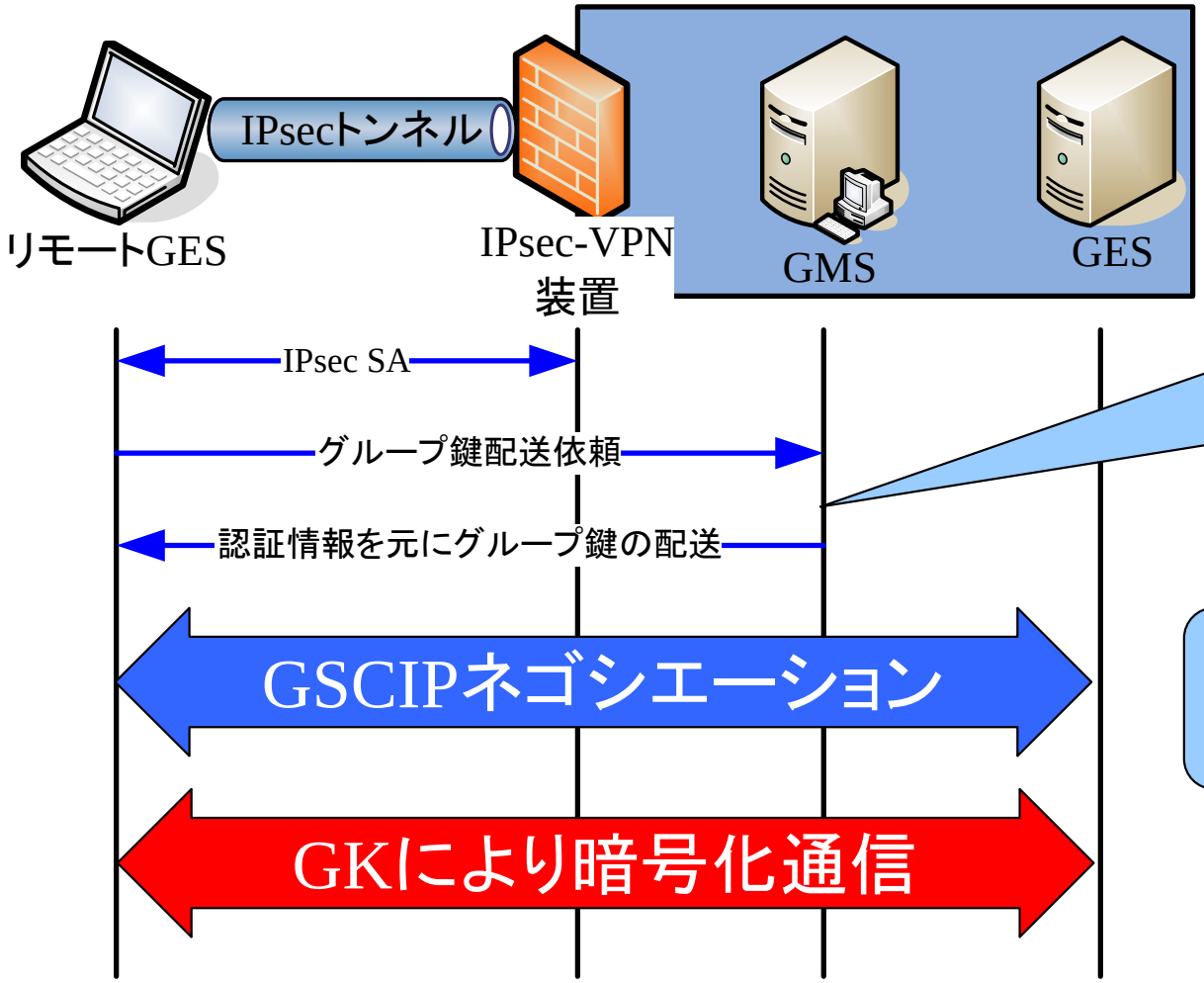
ユーザ認証機能
プライベートIPの割当

ユーザ
認証機能追加

プライベートIP
アドレスの割当

既存のIPsec-VPNの動作
IKEを拡張して提供

提案方式におけるGSCIPの動作



公開鍵認証を行い
GKの配送

GSCIPの動作

従来のIPsecに比べよりセキュアな通信が可能

提案方式との比較

	IPsecトンネルモード	IPsecトランスポートモード	提案方式
End-to-Endの暗号化	×	○	○
利用可能なアプリケーション	○ 任意のアプリケーション	○ 任意のアプリケーション	○ 任意のアプリケーション
管理負荷	○ IPsecの設定のみ	× セキュリティポリシの設定が多くなり管理負荷が高い	△ 個人単位，ネットワーク単位の混在環境をGKで簡単に構築

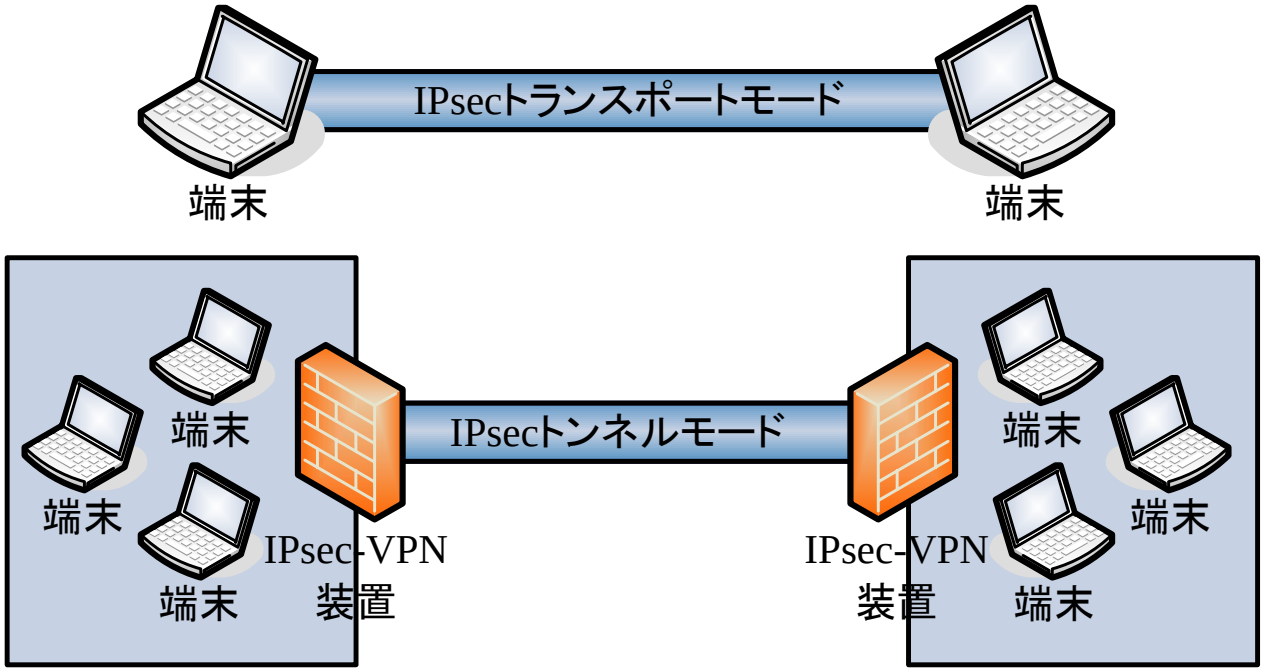
むすび

- まとめ
  - GSCIPとIPsecを併用したリモートアクセス方式提案
    - IPsecのみでは行えなかった柔軟なグルーピング
    - グループ鍵による暗号化でEnd-to-Endのセキュア通信
    - IPsecトランスポートモードに比べ管理負荷の低減
- 今後の展開
  - 実装・評価を行う

付録

トンネルモードとトランスポートモード

- IPsecには2種類の構成方法が存在
  - ネットワーク単位を結ぶIPsecトンネルモード
  - エンド端末同士を結ぶIPsecトランスポートモード



トンネルモードと
トランスポートモードに
互換性がない

混在環境の
構築が困難

提案方式との比較

	IPsecトンネルモード	SSL-VPN	提案方式
End-to-Endの暗号化	× End-to-GW	△ End-to-GW	○ End-to-End
利用可能なアプリケーション	○ 任意のアプリケーション	△ レイヤ5以上のアプリケーション	○ 任意のアプリケーション
管理負荷	○ 提案方式とほぼ同程度	△ 詳細なアクセス制御が可能であるが管理負荷増大	△ 個人単位，ネットワーク単位の混在環境をGKで簡単に構築

実装状況

- FreeBSD5.3に実装
  - GSCIPとIPsecを併用
    - 通信開始時にIPsec構築後，GSCIPが動くように処理
    - IPsecのプログラムにGSCIP呼び出しを追加
- 実装状況
  - FreeBSD5.3でIPsec構築完了
- 今後は
  - GSCIPをリモート端末にインストールし併用出来るようにIPsecプログラムの変更