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

今村圭佑† 鈴木秀和‡ 渡邊晃†
Keisuke Imamura† Hidekazu Suzuki‡ Akira Watanabe†

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

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，外出先等からも社内ネットワークへアクセスしたいという要望が高まっている．この用件を満たすため，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．また，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．GE 間の通信は，各 GE が保持する動作処理情報テーブル PIT（Process Information Table）に基づき，GK により暗号化されたり，他のグループからのアクセスを拒否したりすることが可能である．

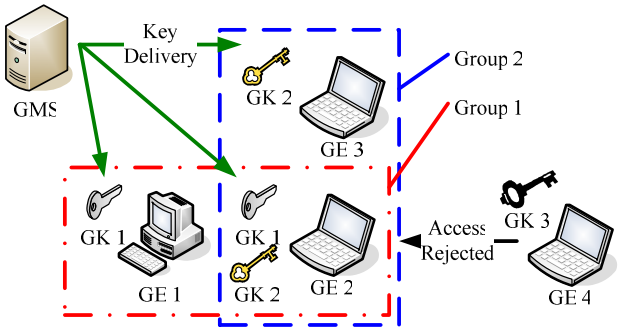


Fig 1. A principle of GSCIP

端末間の通信に先立ち，DPRP（Dynamic Process Resolution Protocol）[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 GE の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 PIT を動的に生成する．

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．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 アドレスをリモート端末に割り当てる．

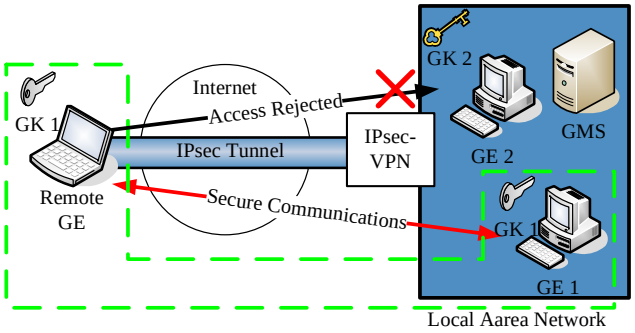


Fig 2. Remote access with GSCIP and IPsec

その後，リモート端末は社内 LAN 内に設置された 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．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．

このように，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．

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，情報処理学会　DICOMO2005 シンポジウム
[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

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

今村　圭佑，鈴木　秀和，渡邊　晃

研究背景

- 無線アクセスポイントの普及や在宅勤務者の増加
  - 社外から社内へアクセスが頻繁に行われている

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保護

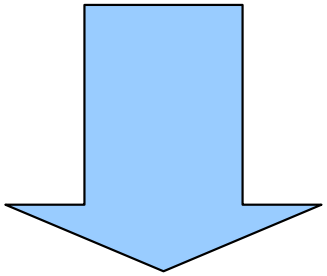
研究背景

- 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

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方式を提案

インターネット上のセキュリティ確保

- リモートアクセスVPN
  - IPsec（Security Architecture for Internet Protocol）
  - SSL（Secure Sockets Layer）
  - PPTP（Point to Point Tunneling Protocol）
  - L2TP（Layer 2 Tunneling Protocol）



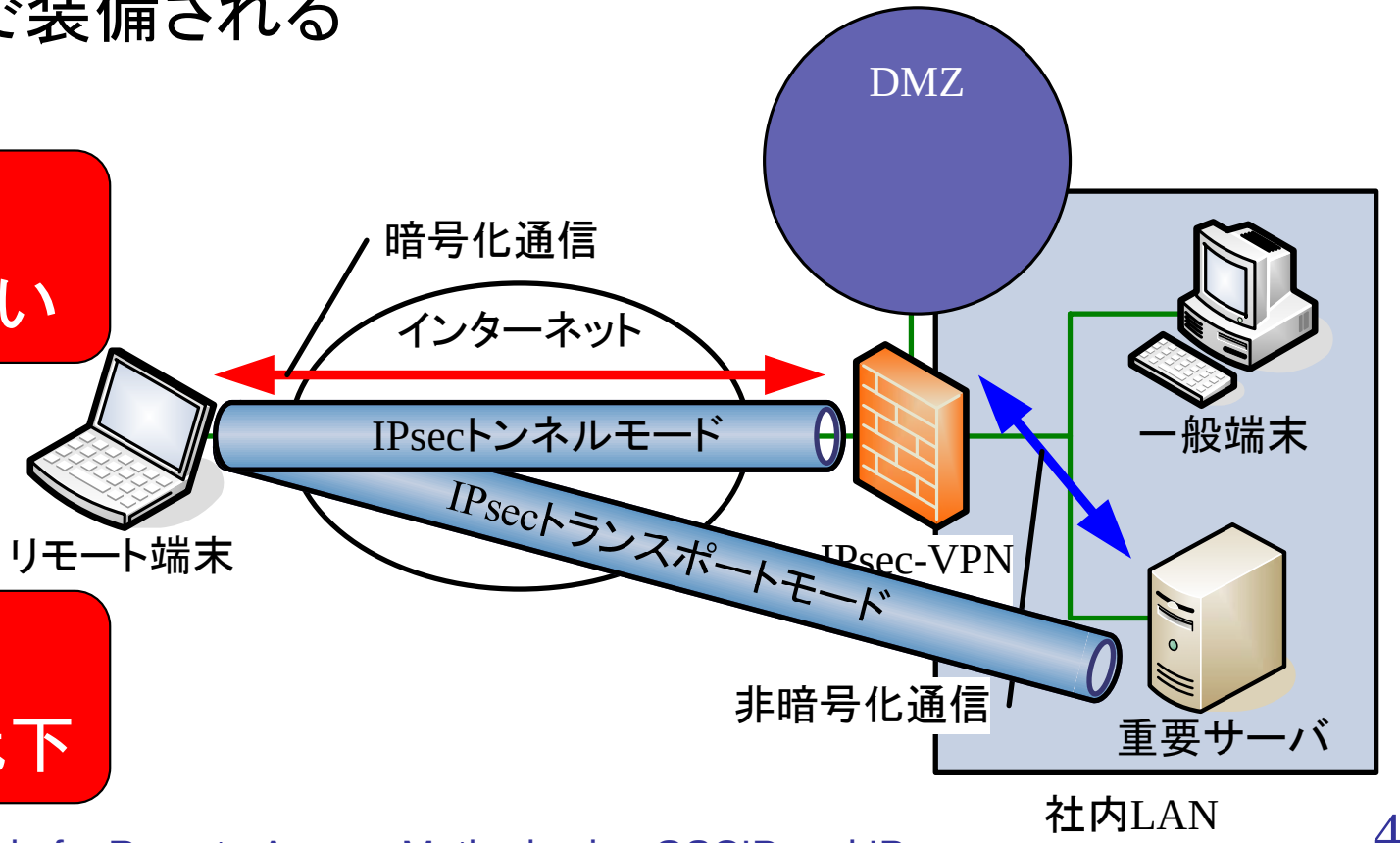
リモートアクセスVPNとしてIPsec，SSLが
良く利用されている

IPsecの概要と問題点

- データの改ざん防止や秘匿機能を提供するプロトコル
- 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

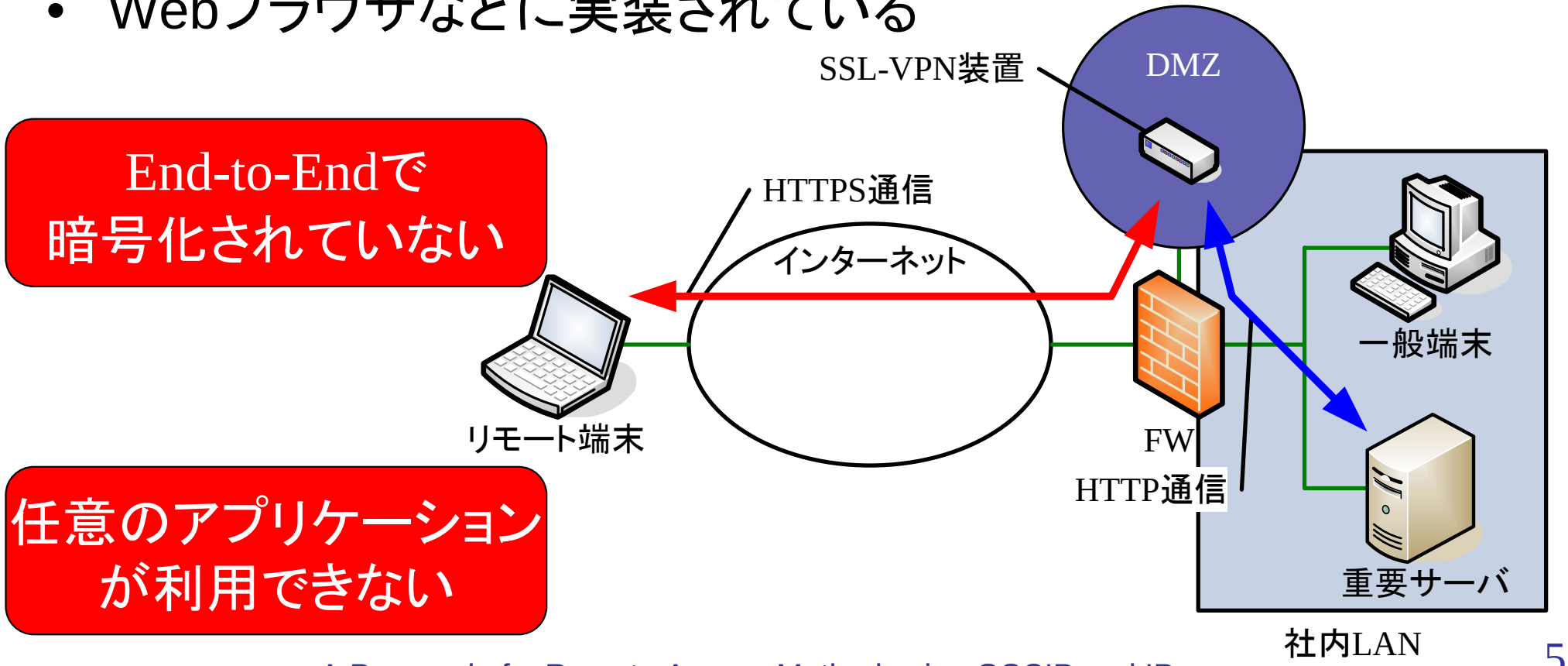
End-to-Endで
暗号化されていない

UDPカプセル化
セキュリティ強度低下



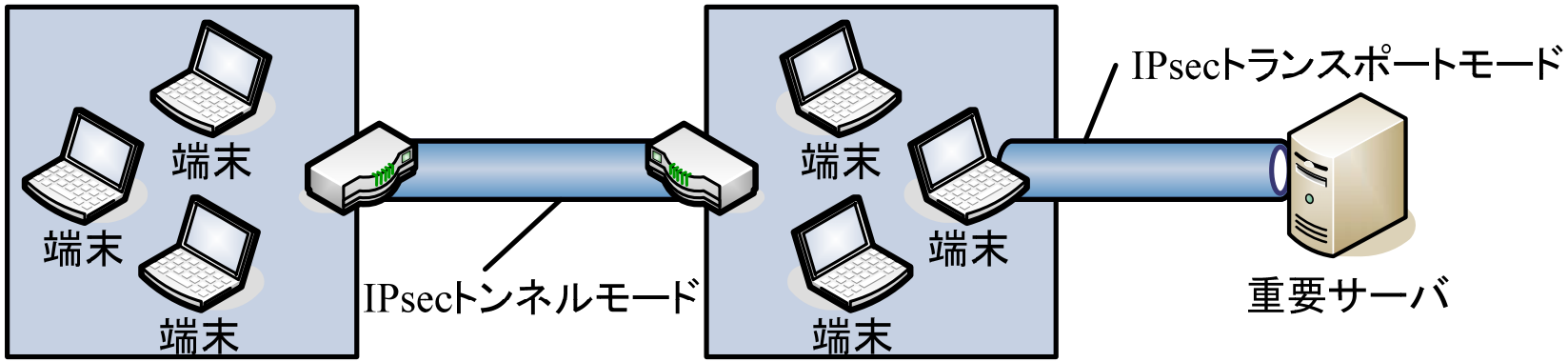
SSLの概要と問題点

- データ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



イントラネット内のセキュリティ対策

- イントラネットをIPsecで構築
  - トンネルモード，トランスポートモードに互換性がない
  - 通信系路上すべてに設定が必要になり管理負荷が増大

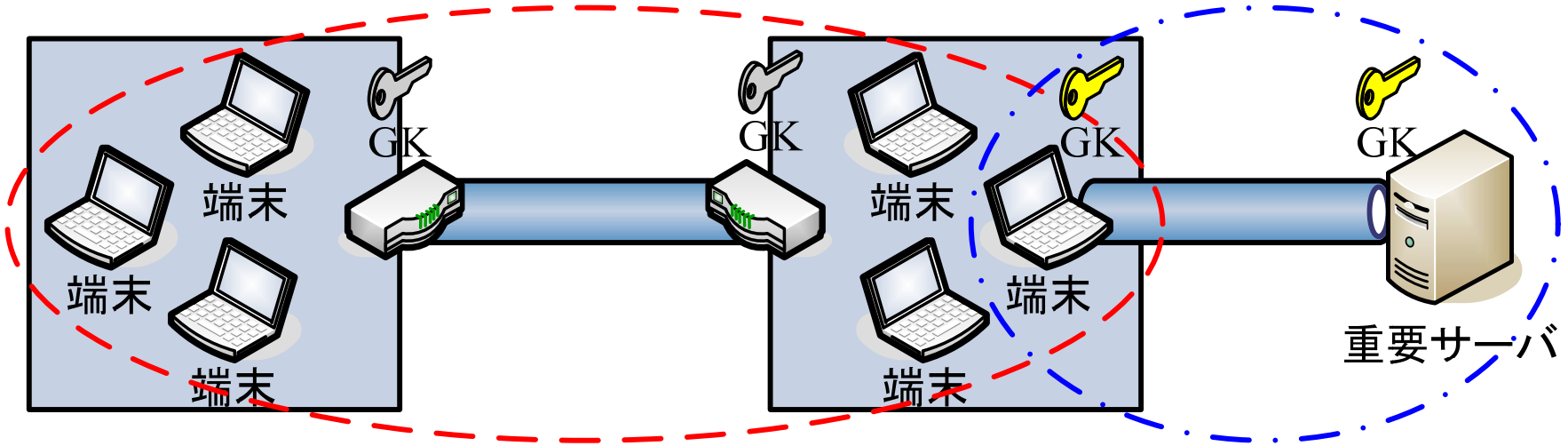


イントラネットのセキュリティ対策

GSCIP（Grouping for Secure Communication for IP）

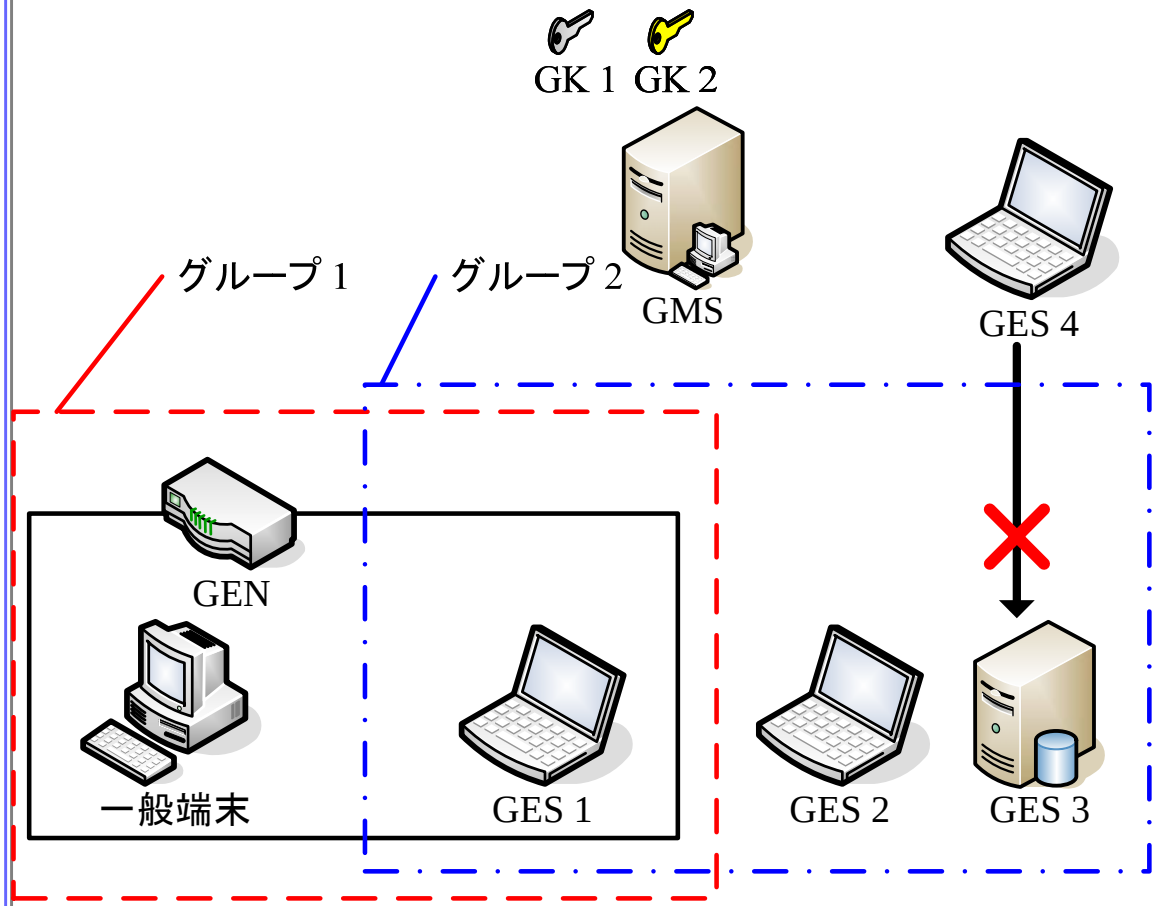
GSCIPの概要

- 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
- ドメイン単位，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
- 通信開始時に動的に設定情報を設定



GSCIPの動作概要

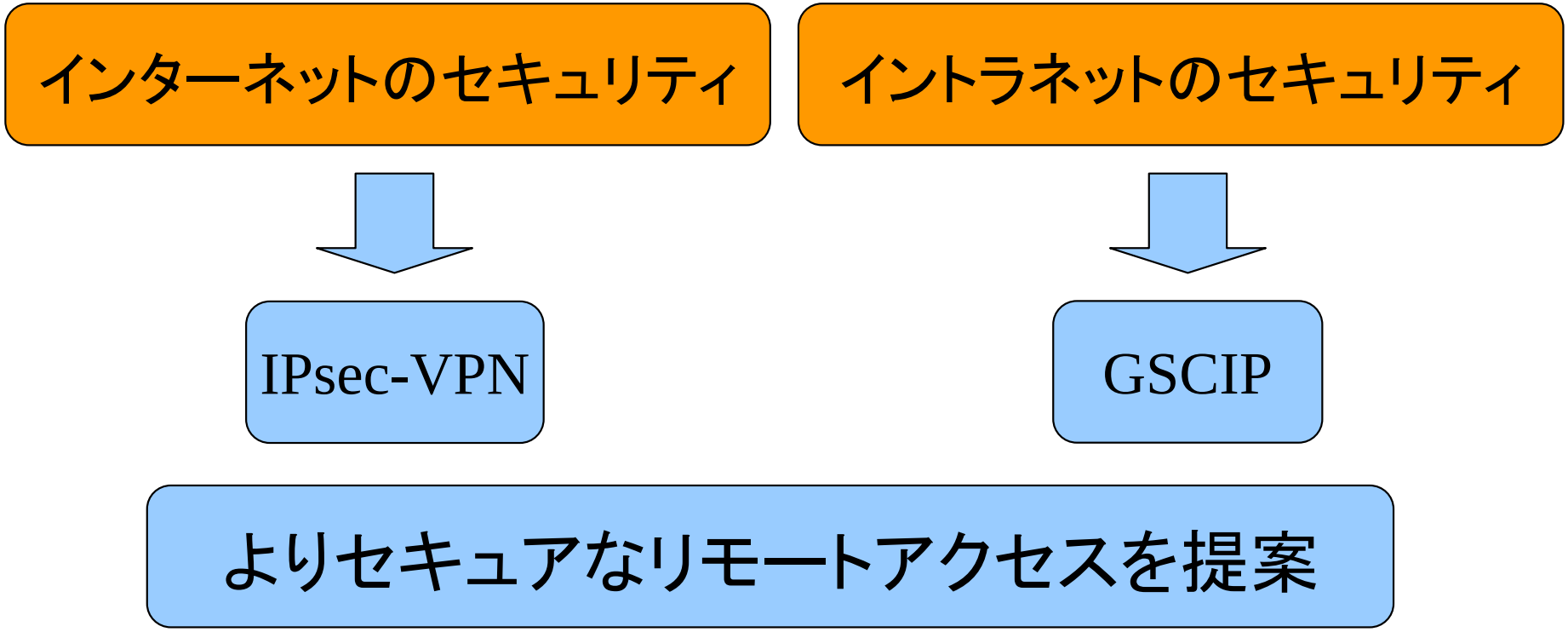
- GSCIPの構成



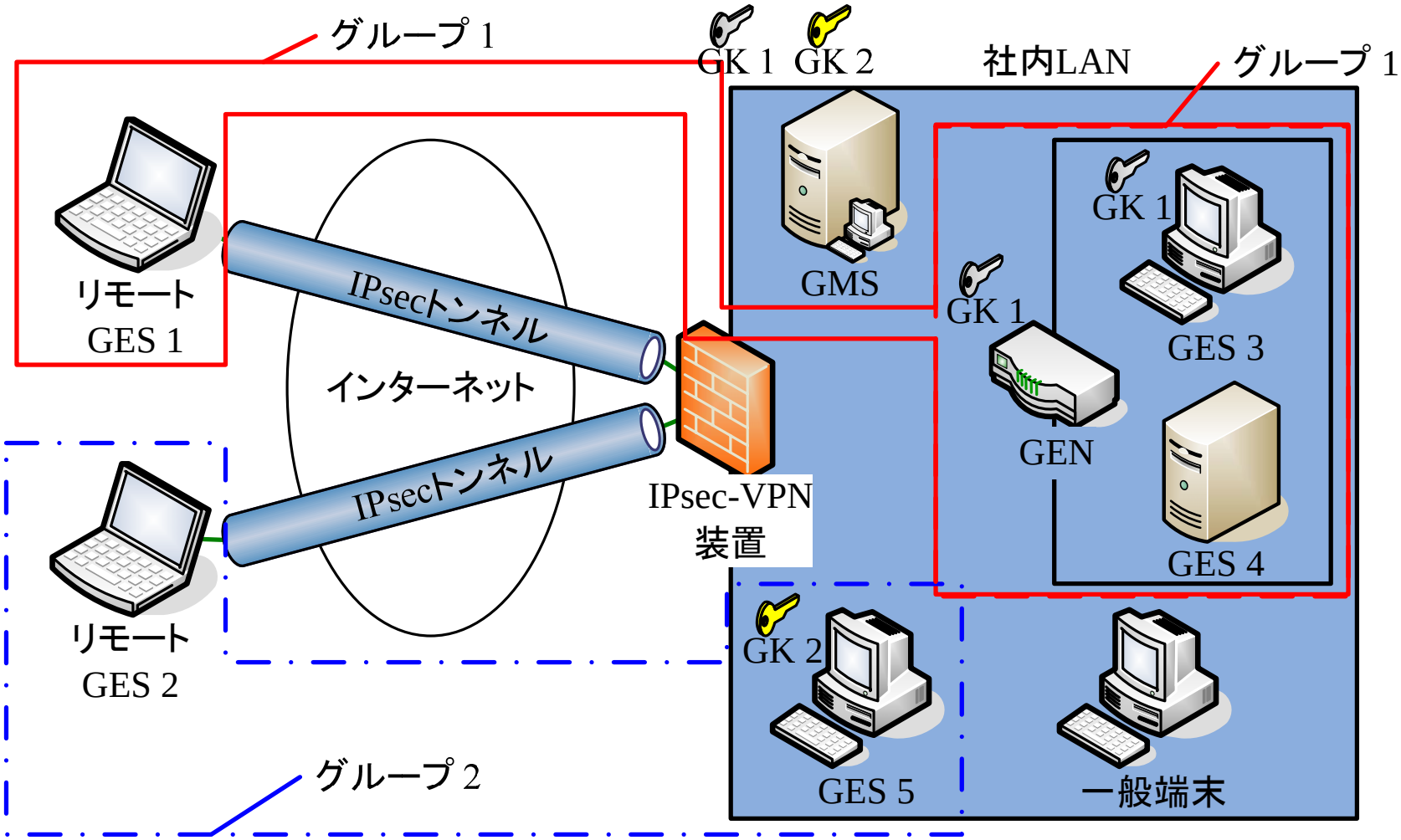
- ◆ 構成要素
  - □GE（GSCIP構成装置）
    - ≫GES（ソフトウェア型）
    - ≫GEN（ネットワーク型）
  - □GMS（グループ管理装置）
- ◆ GMSから各GEに定義情報の配送
  - □GMS-GE間で公開鍵認証
  - □GKを配送
- ◆ 通信グループの定義
  - □同一のGKを持つGE同士で構成
  - □GKとグループは一対一に対応（IPアドレスに依存しない構成）

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



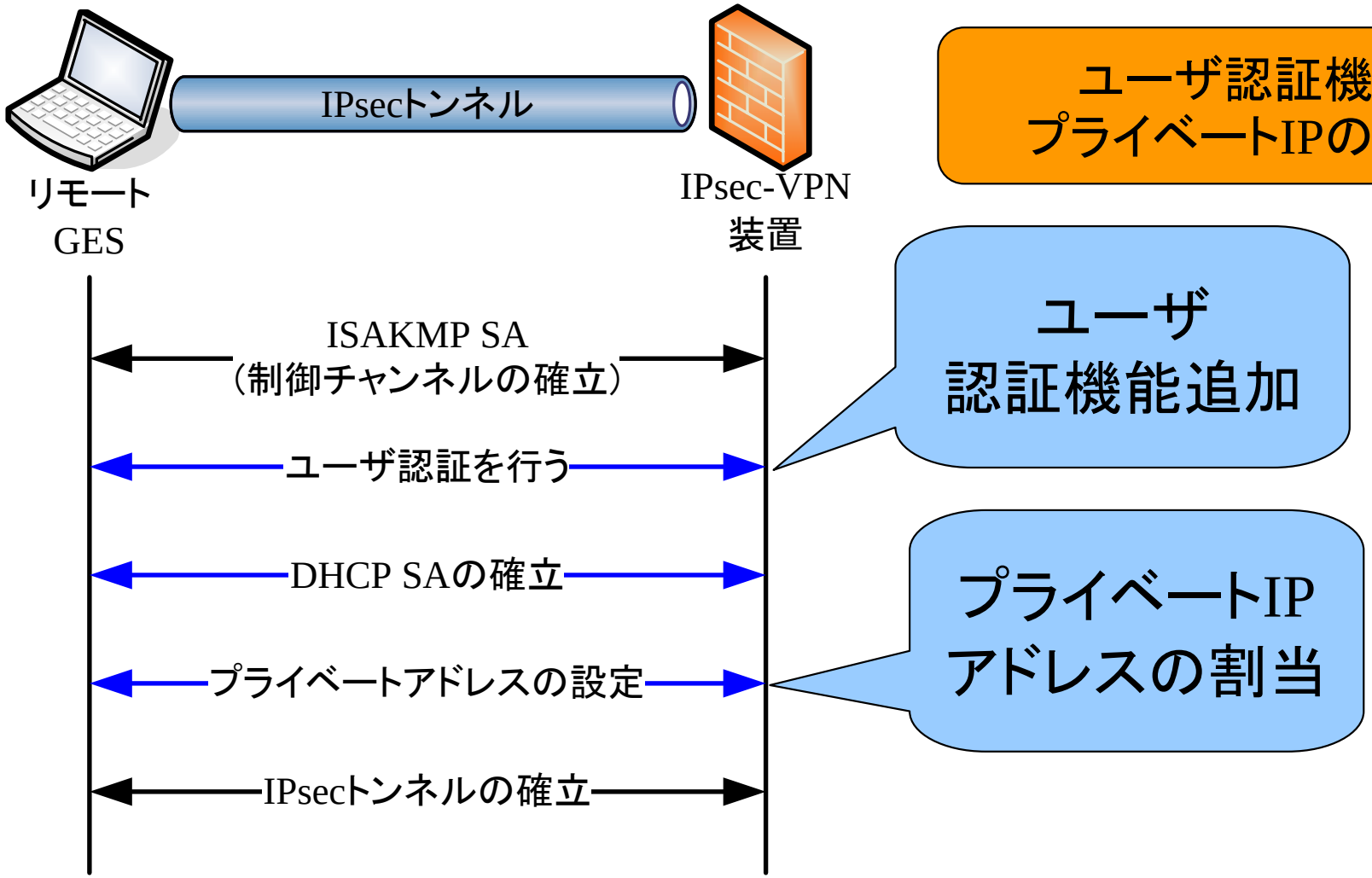
GSCIPとIPsecを併用したシステム構成



インターネット空間：IPsec
イントラネット：GSCIP

GSCIPをリモート端末まで適用

リモートアクセスにおけるIPsecの動作



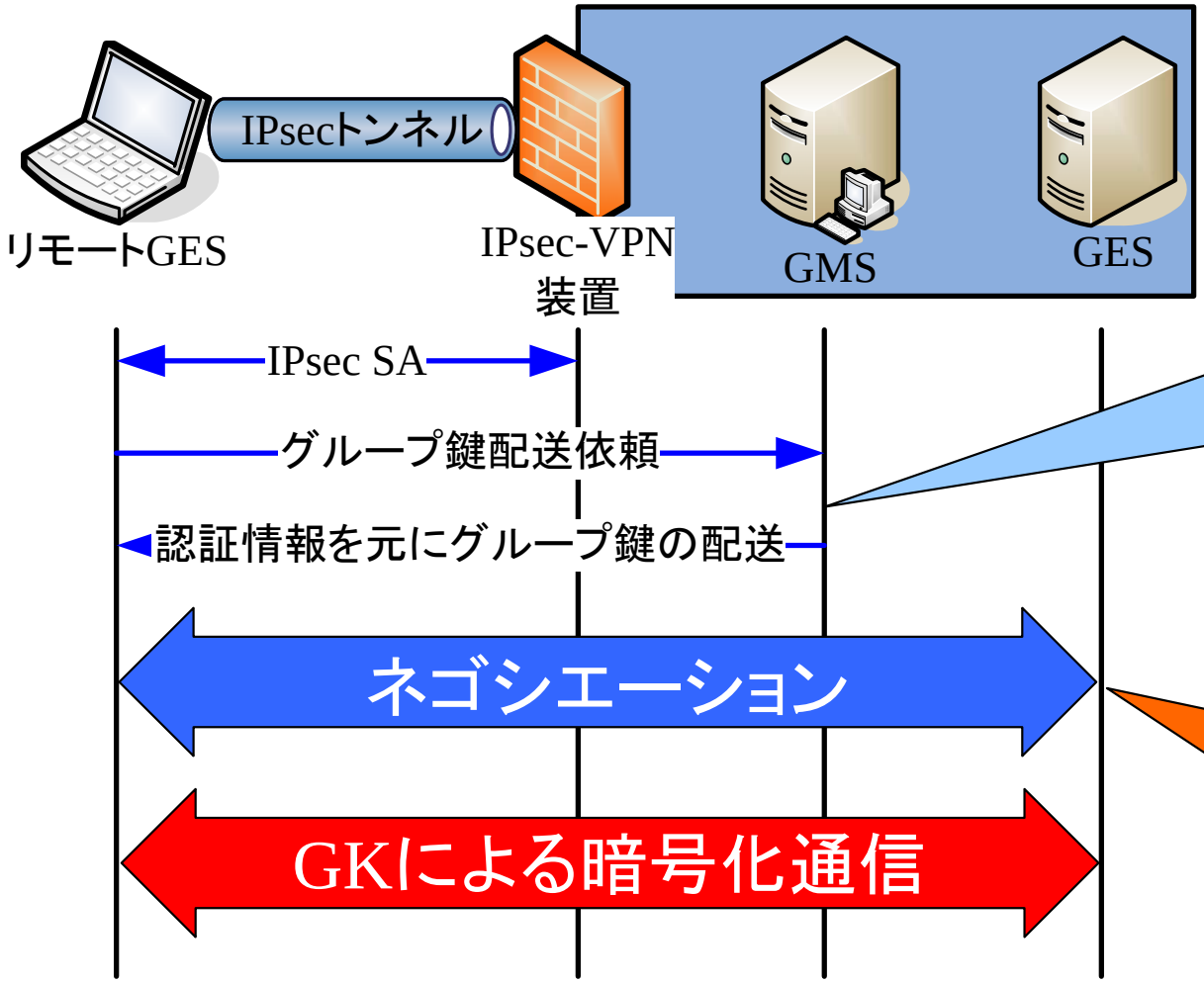
ユーザ認証機能
プライベートIPの割当

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

所持するGKに
よって処理内容を
動的に決定

End-to-Endのセキュア通信が可能になる

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
セキュリティ強度	× End-to-Endで暗号化を行っていない	△ UDPカプセル化によりセキュリティ強度低下	○ GKによる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	× 設定項目が多く，アクセス先が増加すると管理負荷が増大	△ GKの配送後，動的にポリシーの設定を行う

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

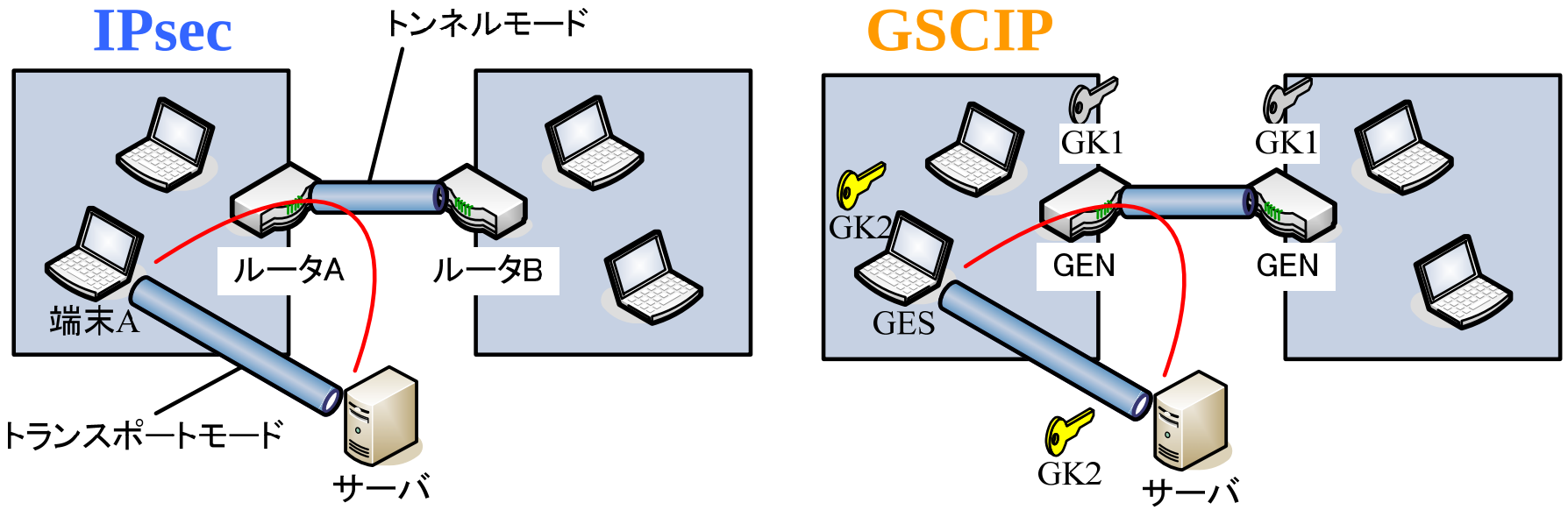
GSCIPとIPsecの違い

- ルータAとBにトンネルモード
- 端末Aとサーバにトランスポートモード
- ルータAに端末Aと重要サーバをトランスポートモードでつなぐ設定

- GENにGK1を配送
- GESとサーバにGK2を配送
- GENはDPRPにより動的に設定

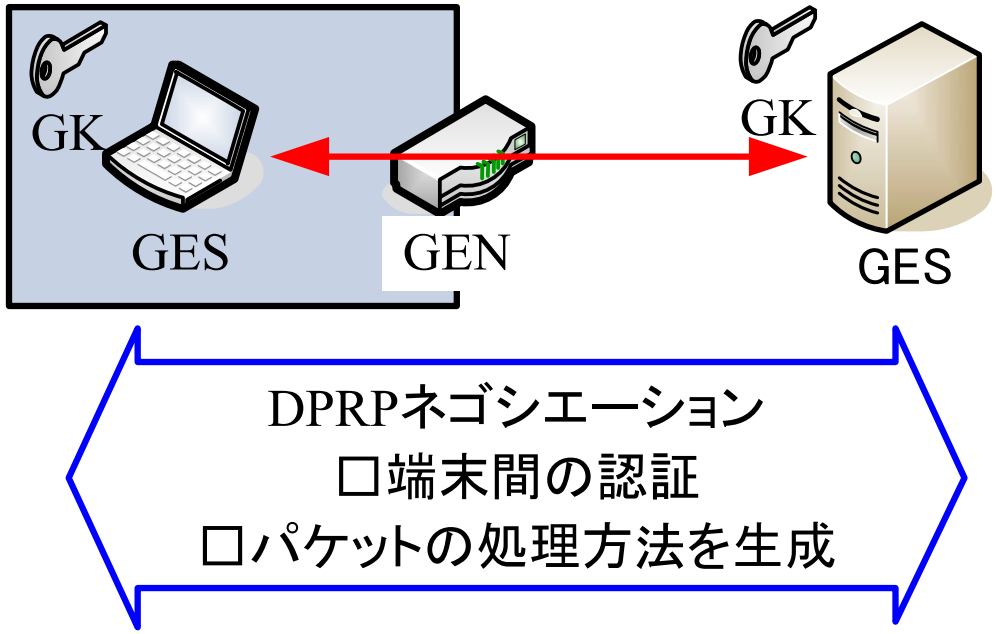
設定項目が多く管理負荷が高い

GKを管理するのみ



動的処理解決プロトコルDPRP

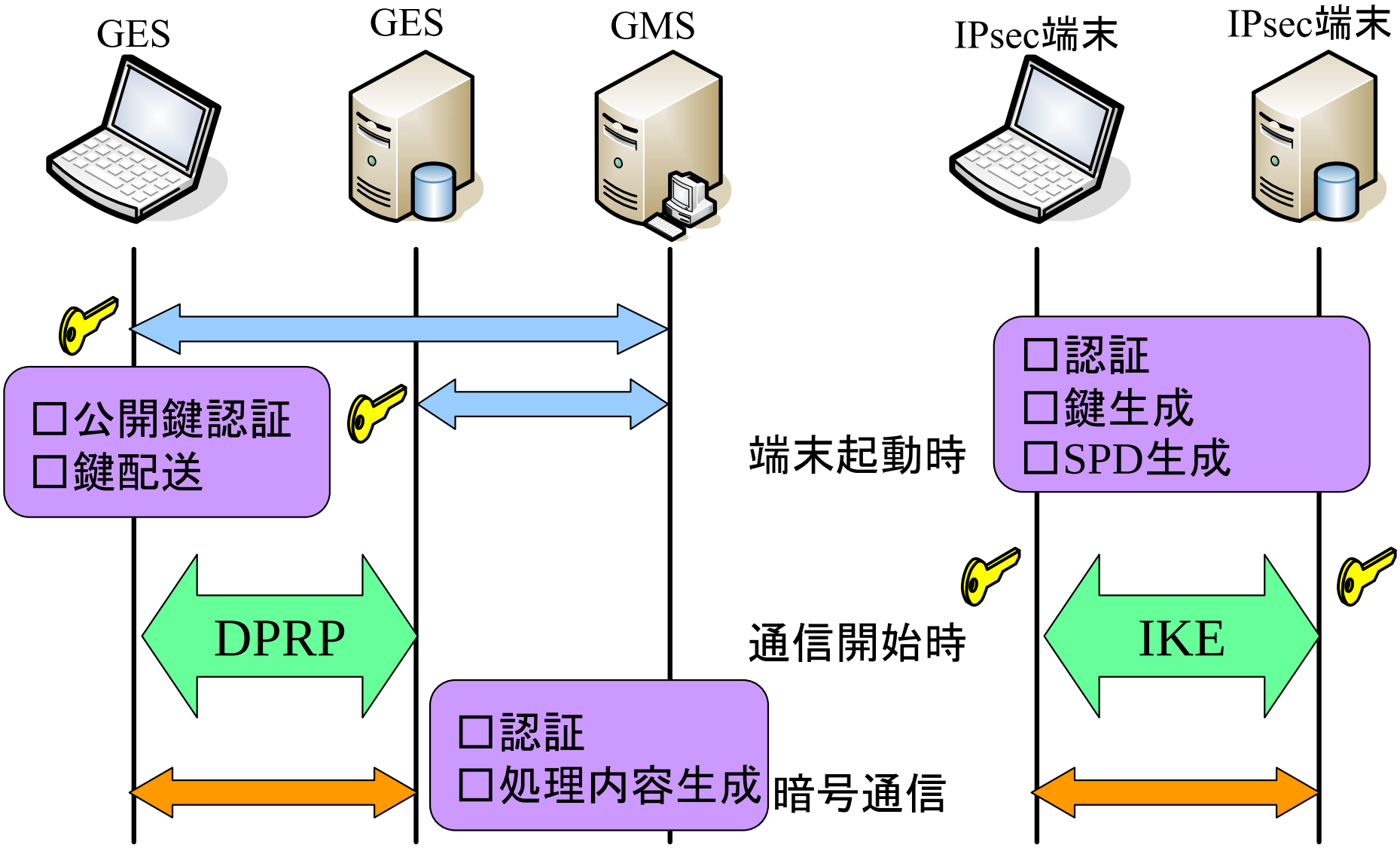
- DPRP（Dynamic Process Resolution Protocol）
  - GSCIPの一部を構成するプロトコル
  - 通信に先立ち，通信系路上に存在するGEに通信に必要な情報を設定する



□IPsecのように事前に設定する必要がない

□GKによる管理でIPアドレスが変化しても設定し直す必要がない

GSCIPとIPsecのアーキテクチャの違い



提案方式との比較

	IPsecトンネルモード	SSL-VPN	提案方式
セキュリティ強度	× End-to-Endで暗号化を行っていない	× End-to-Endで暗号化を行っていない	○ GKによる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	× 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	○ IPsecの設定のみ	△ 詳細なアクセス制御が可能であるが管理負荷増大	△ GKの配送後，動的にポリシーの設定を行う