GSCIP と IPsec を併用したリモートアクセス方式の提案

今村　圭佑*，伊藤　将司，渡邊　晃（名城大学）

A Proposal of a Remote Access Method using GSCIP and IPsec

Keisuke Imamura, Masashi Ito, Akira Watanabe (Meijo University)

1.　はじめに

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 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，NAT を越えることが出来ないため，一般にはファイアウォールの外側で終端される．そのためバリアセグメント上のサーバへのアクセスは出来るが，社内ネットワークの重要なサーバへのアクセスは出来ない．そこで，柔軟なアクセス制御とセキュア通信を実現するために，我々が提案しているグループ通信方式 GSCIP[1]（Grouping for Secure Communication for IP）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 とは，グループ管理装置 MS（Management Server）から端末，サーバに内蔵された GE（GSCIP Element）へグループ鍵 GK（Group Key）を配送し，同一の GK を所持する端末が同一の通信グループを構成する．グループ間の通信は，GK により暗号化され，他のグループからのアクセスを拒否することができる．GSCIP におけるグルーピングの原理を図 1 に示す．

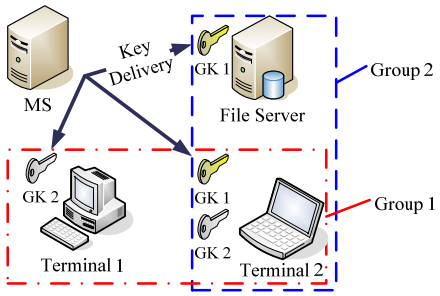


Fig 1. A principle of GSCIP

通信グループの定義は MS で行い，グループ鍵の生成と配送を行う．MS は，サーバや端末を確実に認証する．

GSCIP を構成するプロトコルとして DPRP[2]（Dynamic Process Resolution Protocol）が存在する．DPRP とは，通信に先立ち，通信経路上に存在する GE が互いに情報を交換し，GE 間の通信に必要な動作処理テーブル PIT（Process Information Table）を生成する．PIT により GE 間の通信パケットに対する処理（暗号化，平分通信，拒否）を決定する．

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 VPN 装置間は，IPsec を用いてトンネルを生成する．リモート端末の認証は，IKE-XAUTH（eXtended AUTHentication）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，VPN 装置内の DHCP サーバからプライベート IP アドレスをリモート端末に割り当てる．

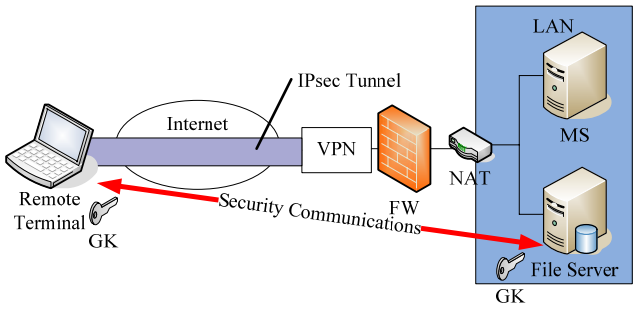


Fig 2. Remote access with GSCIP and IPsec

その後リモート端末は，社内 LAN 内に設置された MS に対して，グループ鍵の配送依頼をする．以後の動作は，GSCIP の動作と同様である．上記の手続きにより，リモート端末は，等価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，リモート拠点からの強靭なセキュリティ機能を介して，社内の重要なサーバへの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 の仕組み，第 26 回　CSEC 研究発表会

GSCIPとIPsecを併用したリモートアクセス方式の提案

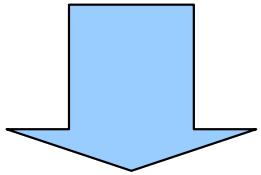
A Proposal of a Remote Access Method using GSCIP and IPsec

名城大学理工学部

今村　圭佑　伊藤　将志　渡邊　晃

研究背景

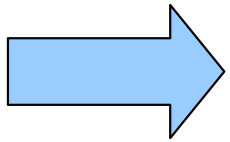
- 企業ネットワークにおけるセキュリティ脅威
  - インターネット経由による外部からの不正アクセス
    - FW，IDSなどで対策
  - イントラネット内のユーザによる内部犯罪
    - ユーザIDとパスワードだけに頼るなど脆弱



内部犯罪の増加

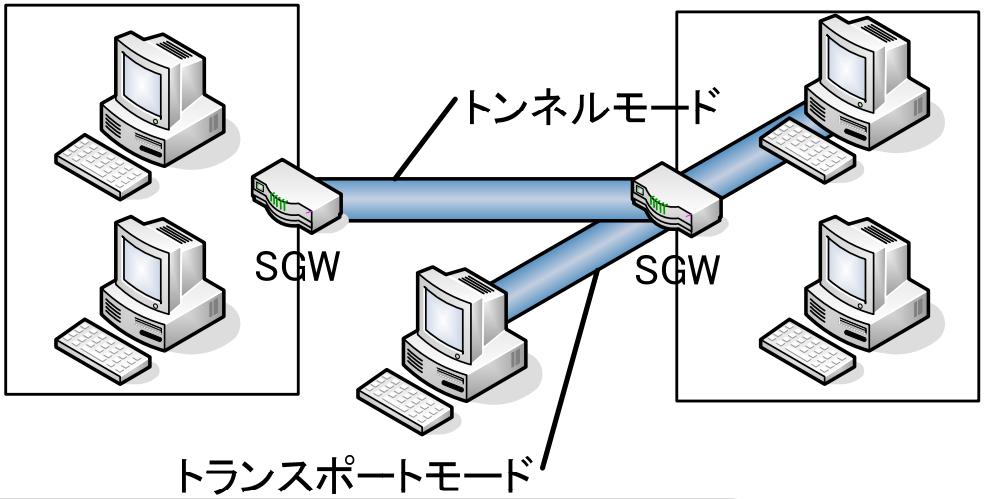
既存技術による対策

- ネットワークセキュリティ
  - 相手認証
  - 暗号化通信



IPsec

- イントラネットに適応させると
  - 設定項目が多く管理が煩雑
  - ネットワーク単位，個人単位が混在する構成は不向き

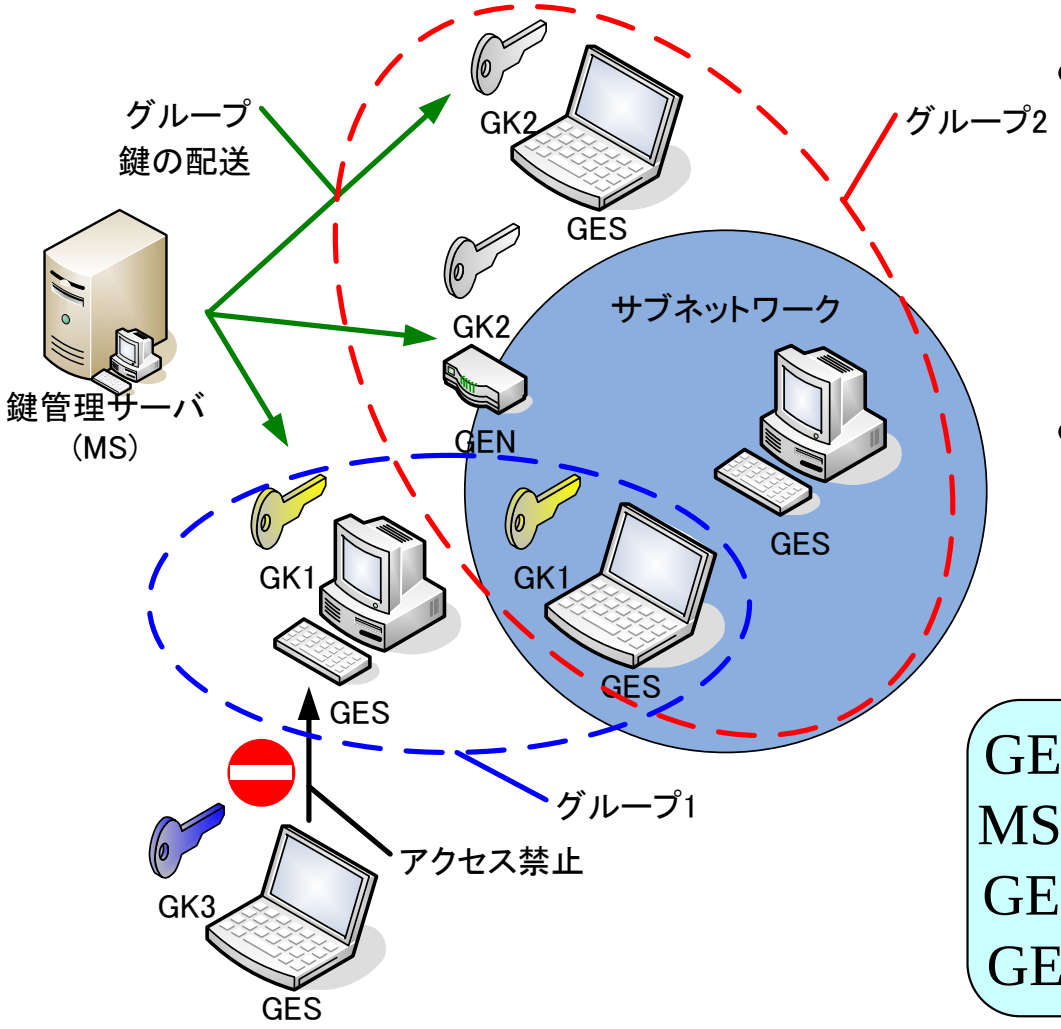


イントラネット内の管理には不向きであり，
現在はVPN以外で普及していない

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



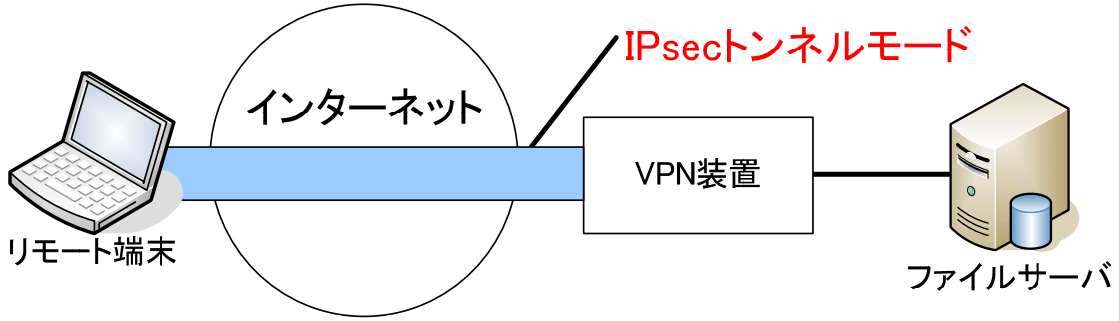
- 鍵管理サーバ(MS)は，GEに設定されている情報を元にグループ鍵(GK)を配送
- 同じグループ鍵を持つもの同士で通信グループを構成

GE(GSCIP Element)
MS(Management Server):鍵管理サーバ
GES(Software型):クライアントに実装
GEN(Network型):ルータに実装

柔軟なアクセス制御とセキュア通信を実現

既存のリモートアクセスシステム

- IPsecを用いたリモートアクセス
  - トンネルモード
    - End-to-Endで暗号化されていない
  - トランスポートモード
    - アクセス先毎にトンネルを確立しなければならない



柔軟なアクセス制御と
End-to-Endで暗号化

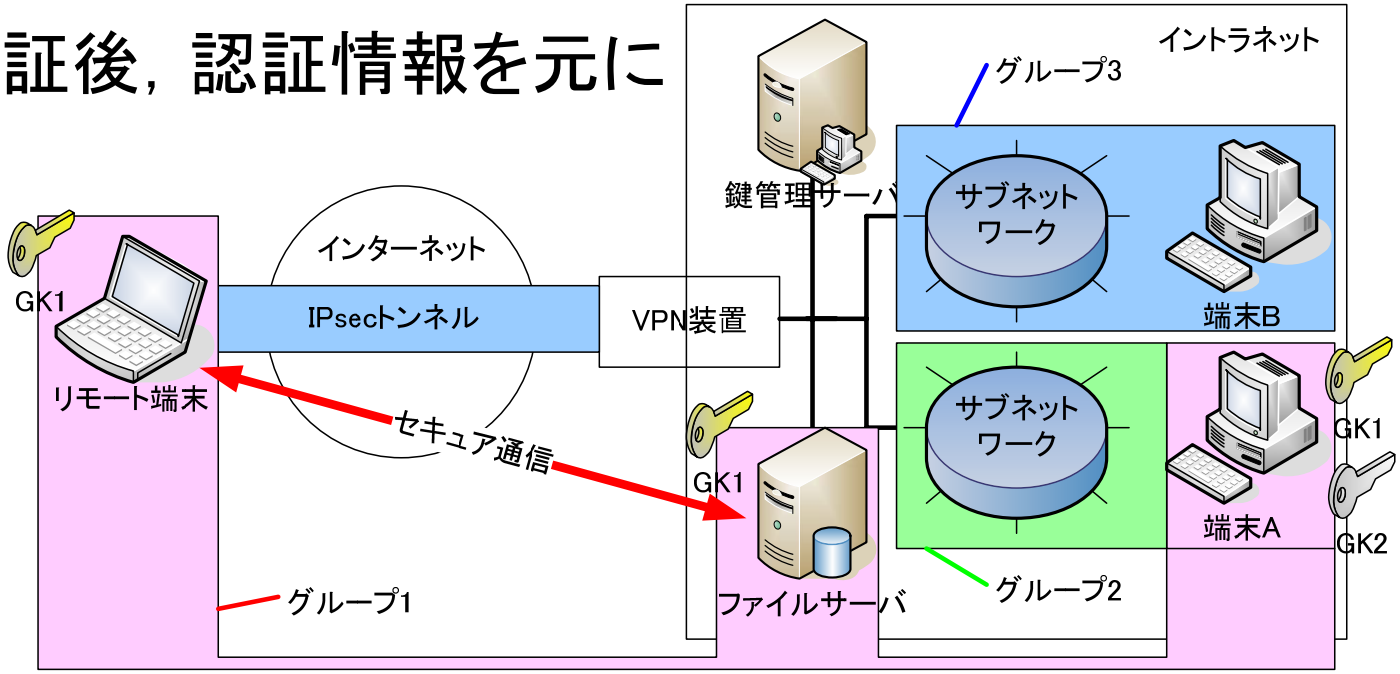
提案方式の実現手段

- 既存のVPN装置を利用
  - IPsecトンネルモードでリモート端末とVPN装置間をトンネリング
  - IPsec-DHCPによりリモート端末にプライベートIPアドレスの割当
  - XAUTH（eXtended AUTHentication）などを使用し，リモート端末の認証
- GSCIPをリモート端末にも適用
  - グループ鍵をリモート端末に配送
  - イントラネットのグループ構成の中に取り込まれる

提案方式の動作概要

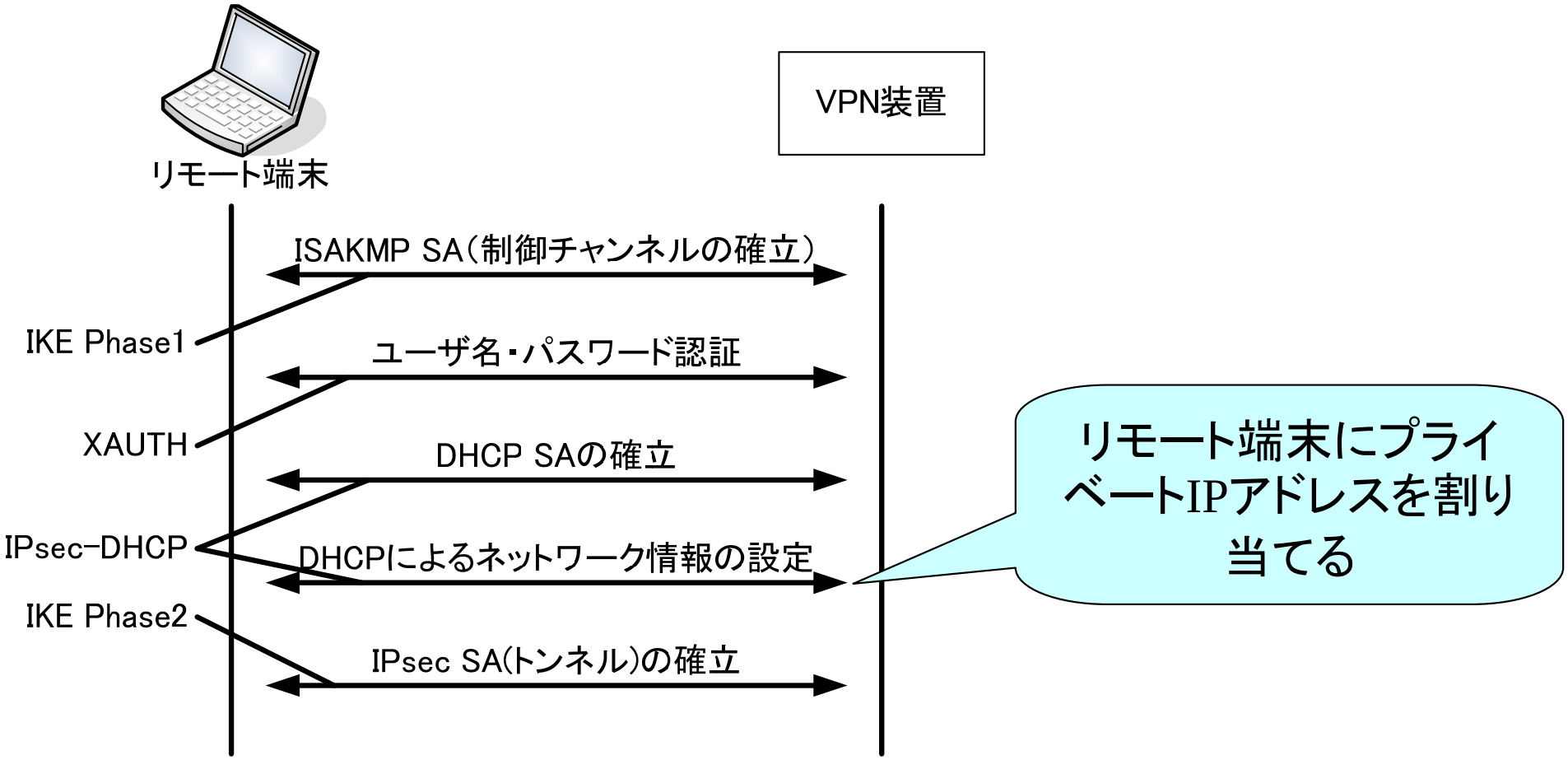
- VPN装置に対しIPsecトンネルを構築
- リモート端末の認証，プライベートIPアドレスの割当
- 鍵管理サーバに対しグループ鍵の配送依頼
- 公開鍵による認証後，認証情報を元にグループ鍵を配送

以後の動作は，GSCIPと同様



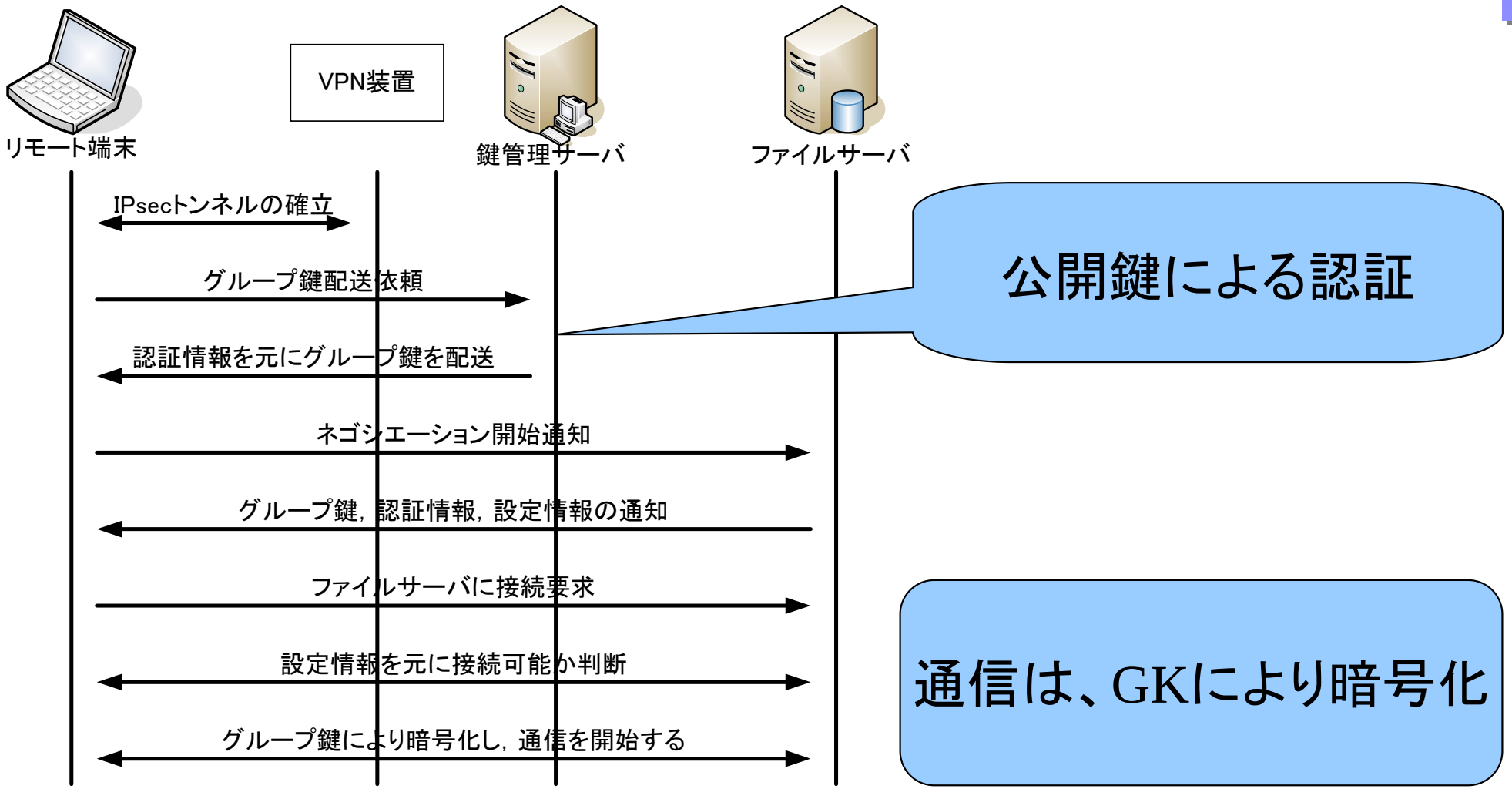
柔軟なアクセス制御とEnd-to-Endで暗号化通信が可能なリモートアクセスを実現

IPsecの動作



既存のVPN装置動作

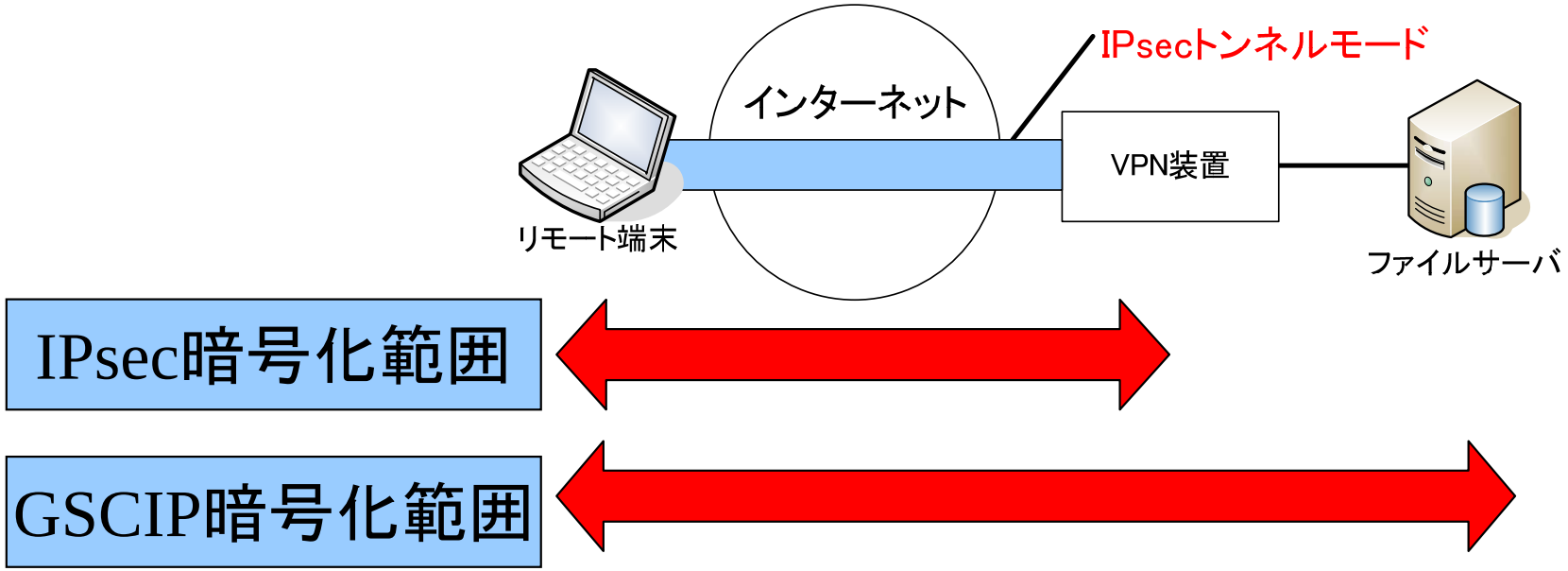
提案方式の動作



End-to-Endで通信を保護

提案方式の利点

- リモート端末からアクセスしたいサーバまでEnd-to-Endでセキュア通信が可能



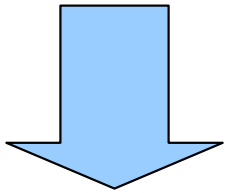
むすび

- 柔軟なアクセス制御とセキュア通信を可能とするリモートアクセス方式
  - グループ鍵による通信グループの形成
    - 柔軟なアクセス制御
  - グループ鍵による暗号化
    - End-to-Endでセキュリティを確保
- 今後の展開
  - 実装と評価を行う

付録

リモートアクセスVPN

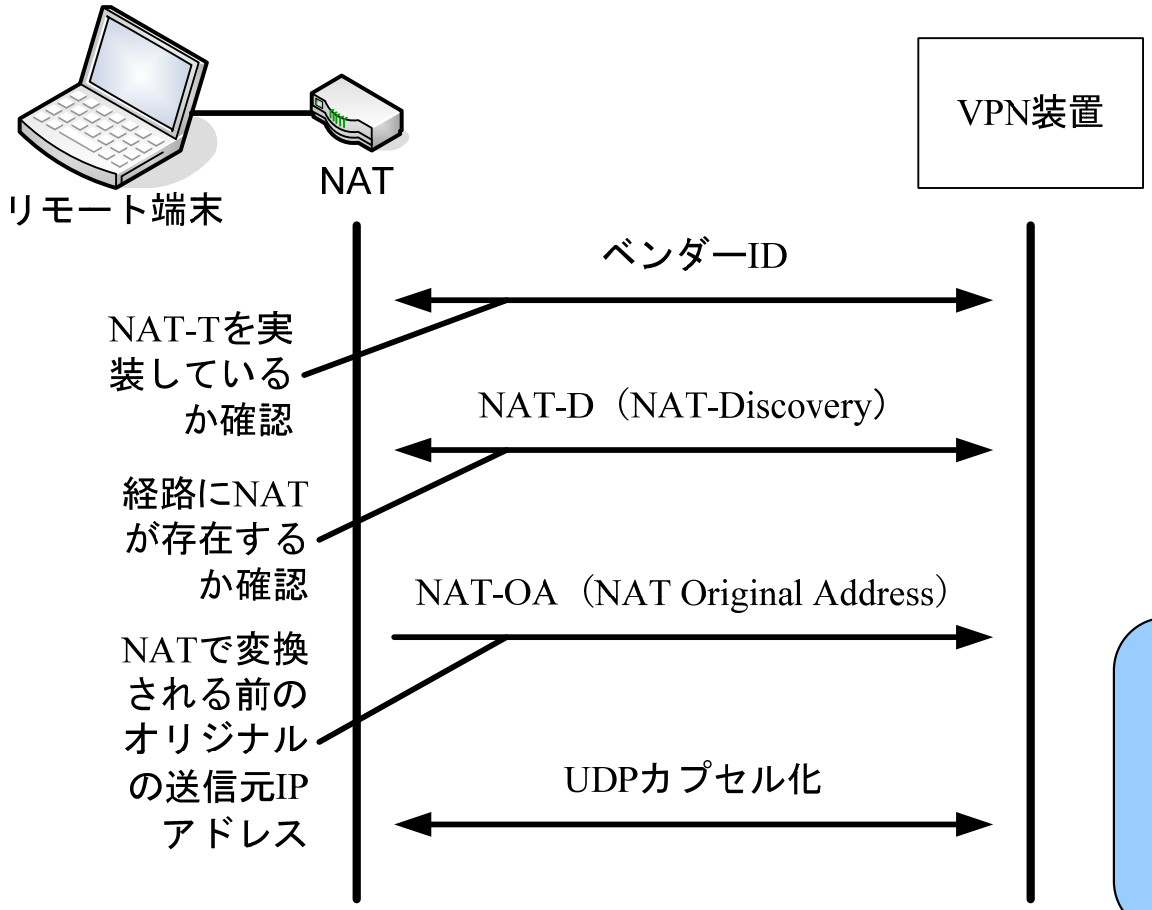
- IPsec-VPN
  - IPレベルでセキュリティが確保されるため，様々なアプリケーションで利用可能
- SSL-VPN
  - SSL対応のアプリケーションがあれば利用可能
  - UDPや動的なTCPを使用するアプリケーションが利用できない



アプリケーションが限定されるSSL-VPNは不便

NAT越え技術（NAT-Traversal）

- リモート端末がNATの配下に存在する場合IPsecパケットが通過できない



在宅勤務など自宅のネットワーク環境でも利用可能