GSCIP と IPsec を併用したリモートアクセス方式の提案と評価

今 村 圭 佑[†]　鈴 木 秀 和[†]　渡 邊　晃[†]

社外から社内 LAN へ安全なアクセスを可能とするリモートアクセスの要求が高まっている．しかし既存のリモートアクセス方式では，十分高いセキュリティを確保できるが，イントラネット内のセキュリティ対策はぜい弱である．そこで，GSCIP と IPsec を併用することによりインターネットとイントラネットの両者を跨った End-to-End のセキュリティを可能とするリモートアクセス方式を検討した．

A Proposal and Evaluation for a Remote Access Method using GSCIP and IPsec

Keisuke Imamura,[†] Hidekazu Suzuki[†] and Akira Watanabe[†]

Demand for the system to make secure remote access from the Internet to enterprise networks has been increasing. However, the security of the existing remote access methods is vulnerable in Internets, although it is robust on the Internet. In order to solve this problem, we have studied a remote access method that uses GSCIP and IPsec in combination. This method can realize End-to-End secure communication not only for the Internet but also for Intranets.

1. はじめに

無線アクセスポイントの普及や，在宅勤務者の増加などの要因により，インターネット経由で社外から社内ネットワークへアクセスしたいという要求が高まっている．しかしインターネット空間には，盗聴，改ざん，成りすましといった脅威が存在する．それらの脅威から通信を保護するために，VPN（Virtual Private Network）を構築してリモートアクセスを行う方法がよく利用されている．リモートアクセス VPN を構築する手段として，PPTP（Point-to-Point Tunneling Protocol）[1]，L2TP（Layer 2 Tunneling Protocol）[2]，IPsec（Security Architecture for Internet Protocol）[3]，SSL（Secure Socket Layer）[4] などの方法がある．

PPTP，L2TP は，暗号化強度が低く企業ネットワークで使用する場合にはセキュリティ強度に問題がある．そのため，近年よく利用される VPN 構築手法として，IPsec や SSL がある．しかし IPsec は，設定項目が多く，ユーザが増加すると管理が煩雑になる．また，SSL はトランスポート層とセッション層の間に定義されていることから利用できるアプリケーションが限定されるといった課題が存在する．両方式ともインターネット上でのセキュリティは強いが，イントラネットでのセキュリティには考慮がなされていない．盗聴，改ざん，成りすましといった脅威はイントラネット内にも存在し，リモートアクセスにおいても End-to-End で暗号化するのが望ましい．End-to-End で暗号化を実現する方法として IPsec トランスポートモードが挙げられるが，NAT[5] を通過するには UDP カプセル化を行う必要があり，本来の IPsec が持つセキュリティ強度が得られない．

イントラネットのセキュリティ対策としては，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．イントラネットにも IPsec を適用する方法が考えられるが，管理が煩雑になるという課題がある．そこで我々は，セキュリティを確保しつつ，管理負荷の低減を可能とするネットワークアーキテクチャGSCIP（Grouping for Secure Communication for IP；ジースキップ）[6] を検討している．GSCIP では，通信グループと共通鍵を 1 対 1 に対応づけ，相手認証と暗号化通信を容易に実現することができる．本稿では，IPsec と GSCIP を組み合わせることにより，イントラネット内の重要サーバまで End-to-End でセキュア通信を可能にした

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

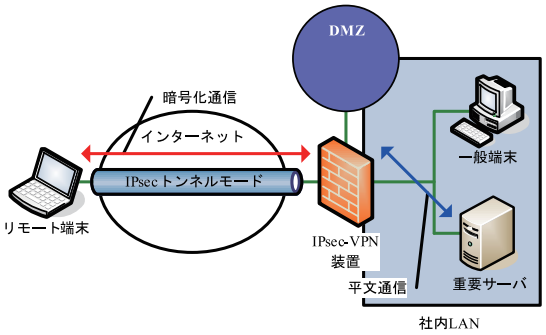


図 1 IPsec を用いたリモートアクセス

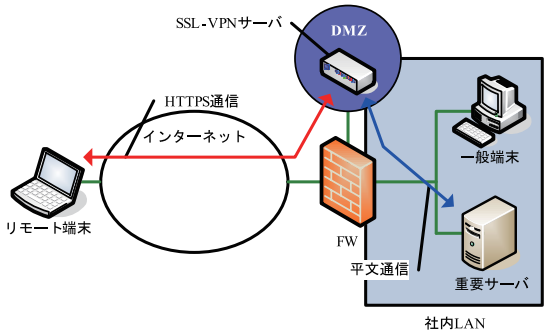


図 2 SSL を用いたリモートアクセス

リモートアクセス方式の提案を行う．

以降，2 章で既存のリモートアクセス VPN について述べる．3 章で GSCIP と IPsec を併用したリモートアクセス方式について説明し，4 章では提案方式の評価を行う．最後に 5 章でまとめる．

2. 既存技術とその課題

2.1 IPsec-VPN

IPsec は，TCP/IP 上において，汎用的に利用できるセキュリティ・プロトコルである．ネットワーク層に実装されており，IETF（Internet Engineering Task Force）で標準化されている．IPsec SA（Security Association）生成プロトコルとして，IKE[7] が存在する．IKE はアルゴリズムの種類や鍵などの情報をインターネット上で交換するプロトコルである．

図 1 に一般的な IPsec を利用したリモートアクセスの構成を示す．通常社内 LAN の入口に IPsec-VPN 装置を設置し，リモート端末は IPsec-VPN 装置に対し IKE を実行し，IPsec SA を構築する．以後，セキュリティポリシに従って IPsec SA 上のパケットは暗号化される．

IPsec を用いたリモートアクセス VPN の問題点として，End-to-End でセキュア通信を確保していない点と管理負荷が高いという 2 点がある．通常 IPsec を用いたリモートアクセスでは，VPN 装置に対し IPsec トンネルモードで接続するので，VPN 装置と社内 LAN の端末間は暗号化通信を行わない．End-to-End のセキュリティを確保する方法として，IPsec トランスポートモードを適応する方法があるが，この方法では，UDP カプセル化をして NAT を通過[8] させる必要がある．カプセル化のヘッダ部分は完全保障の対象外となるため，IPsec が持つ本来のセキュリティレベルを確保できない．

2.2 SSL-VPN

SSL はセッション層とトランスポート層の境界で動作し，HTTP や FTP などのアプリケーションで利用できるプロトコルである．SSL-VPN とは，暗号化に SSL を利用する VPN 技術である．多くの Web ブラウザでは標準で SSL に対応しており，比較的容易にリモートアクセスが可能である．

図 2 に SSL を利用したリモートアクセスの構成を示す．SSL を利用してリモートアクセスを実現する際は，DMZ（DeMilitarized Zone）上に SSL-VPN サーバを設置し，リモート端末は Web ブラウザを使用して SSL-VPN サーバにアクセスする．リモート端末と SSL-VPN サーバの間は HTTPS が用いられるため，セキュリティが確保される．ユーザ認証をパスすると，そのユーザが利用できるリソースへのリンクが表示される．ユーザがリンクを選択すると，SSL-VPN サーバは該当する内部サーバに対して，それぞれのアプリケーションプロトコルを使用してアクセスする．その後，サーバから得られた結果を HTTPS に変換してクライアントに転送する．この方式では，クライアントは Web ブラウザだけを準備すればよく，手軽に VPN を利用できるというメリットがある．しかし，SSL-VPN サーバ上でプロトコル変換機能が必要であるため，利用できるアプリケーションが限定される．特に，UDP を使用するアプリケーションや動的な TCP ポートを使用するアプリケーション，複数の TCP セッションを使用するアプリケーションが利用できない．在宅勤務などでは，通常の企業業務で使用しているアプリケーションをそのまま利用したいという要求があり，このような用途では利用できない可能性がある．

3. 提 案 方 式

3.1 提案方式の目的

既存のリモートアクセスでは，インターネット上のセキュリティは万全であるが，イントラネット内のセキュリティは考慮されていない．そもそもイントラネッ

トのセキュリティ対策としては，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．しかし，盗聴，改ざん，成りすましといった脅威はイントラネット内にも存在し，近年内部犯罪の増加が懸念されている．

イントラネットのセキュリティ対策として IPsec を適用する方法がある．個人単位の通信グループを構築する方法として IPsec トランスポートモードがある．この方法ではきめ細かい通信グループの定義が可能であるが，全ての端末に機能を実装する必要があり，規模が大きくなると管理負荷が大きくなる．サブネット単位で通信グループを構成する方法として IPsec トンネルモードがある．この方法ではルータのみにセキュリティ機能を実装すればよいが，個人単位のようなきめ細かい通信グループを定義することが難しい．イントラネットでは，個人単位，サブネット単位の通信グループが混在する環境になることが多い．IPsec はトランスポートモードとトンネルモードの間に互換性が無く，両者が混在した環境への適用には向いていない．IPsec では通信経路上に同一モードの IPsec 機能を持つ装置が対で存在することが前提となっており，混在環境を実現するにはエンド端末にトランスポートモードとトンネルモードの両方を設定しなければならないなど管理負荷が大きくなるという課題がある．このような課題を解決するため，我々は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 を提案している．

本稿では，IPsec と GSCIP と組み合わせることにより，インターネット空間からイントラネット内のエンド端末間まで End-to-End のセキュリティを確保したリモートアクセスの提案を行う．

3.2 GSCIP の原理

GSCIP とは柔軟性とセキュリティを兼ね備えたネットワークセキュリティアーキテクチャである．図 3 に GSCIP による通信グループの構築の原理を示す．

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

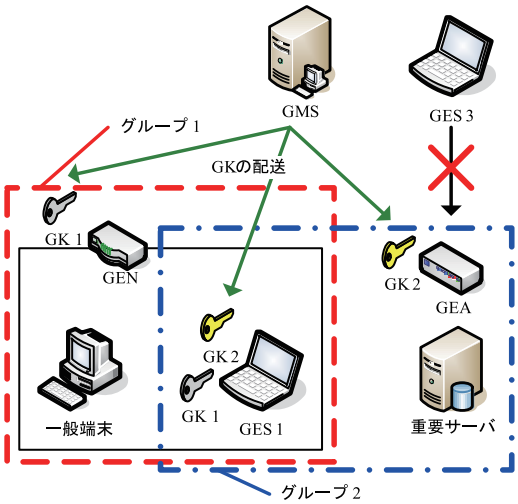


図 3 GSCIP による通信グループの構築原理

GK（Group Key）と呼ぶ．GK を通信グループと一対一に対応させることにより，IP アドレスに依存しない通信グループを構成することが可能となる．同一の通信グループ間の通信は， GK により暗号化される．

GE には動作モードが定義されており，同一通信グループに帰属しない端末との通信を一切禁止する閉域モード CL（Closed Mode）と，異なる通信グループの端末とは平文での通信が可能な開放モード OP（Open Mode）がある．一般に GEN，GEA およびサーバとして使用する GES には閉域モードが定義され，クライアントとして使用する GES には開放モードが定義される．図 3 では GEA はグループ 2 に所属しており，グループ外の GES3 からのアクセスを拒否することが可能となる．通信グループは，管理装置 GMS（Group Management Server）で定義し，GMS から各 GE へグループ情報とそれに対応する GK を配送する．この際，公開鍵を用いた確実な認証が行われる．GK は定期的に更新される．

3.3 DPRP の概要

DPRP（Dynamic Process Resolution Protocol）[9] は GSCIP を実現する一連のプロトコルの中の 1 つで，GE がネットワーク構成を学習することにより，自動的に自己の動作を決定することができる．各 GE は，自身が保持する動作処理テーブル PIT（Process Information Table）に従いパケットの処理を行う．PIT には送信元/宛先の IP アドレス，ポート番号，プロトコルタイプと，これらに一致するパケットの処理内容を規定した動作処理情報（暗号化/復号/透過中継/破棄），およびグループ鍵の識別情報が記述されている．PIT の検索には CID（Connection ID; 送信元/宛先

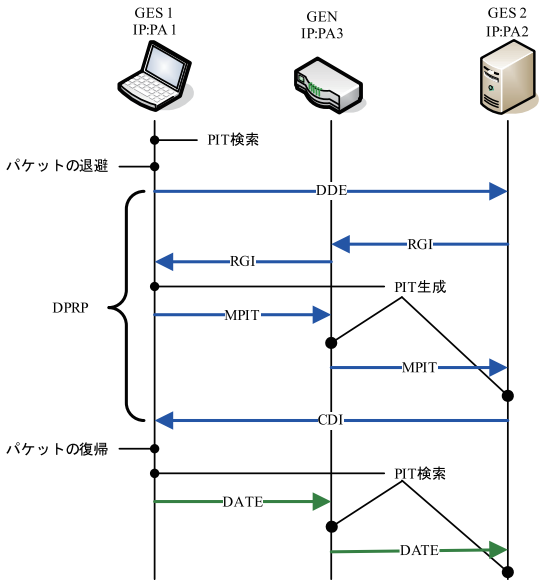


図 4 DPRP シーケンス

IP アドレス，ポート番号，プロトコルタイプ）を用いる．DPRP は, エンド端末間の通信に先立ちネゴシエーションを行う. パケット送信時に PIT を検索し，PIT の従ってパケットを処理する．該当する PIT が存在しない場合には，送信パケットを一時的に退避し，動作処理解決プロトコル DPRP を実行して PIT を動的に生成する．図 4 に DPRP のシーケンス図を示す.

DPRP には，ICMP をベースとした DDE（Detect Destination End GE），RGI（Report GE Information），MPIT（Make Process Information Table），CDN（Complete DPRP Negotiation）という 4 つの制御パケットを用いる．DDE には，DPRP のトリガーとなった通信パケットの CID がセットされ，通信パケットの宛先へ送信する．DDE を受信した GES2 が終点 GE となり，RGI を返送する．RGI には，GE のユーザ ID，動作モード，グループ鍵情報などの設定情報がセットされる．中間 GE は RGI を中継する際，自身の設定情報などをパケットに追加していく．RGI を受信した GES1 が始点 GE となり，収集した情報から各 GE の動作処理情報を決定する．GES1 は決定した動作処理情報を MPIT にセットして GES2 へ送信する．MPIT を受信した GEN，GES2 はパケットの内容から自身に関する動作処理情報を取り出し，PIT を生成する．GES2 は PIT 生成後，DPRP ネゴシエーションの完了を通知するために CDN を GES1 へ送信する．CDN を受信した GES1 は待避していた通信パケットを復帰させる．

パケットは PIT に記述されている動作処理情報に

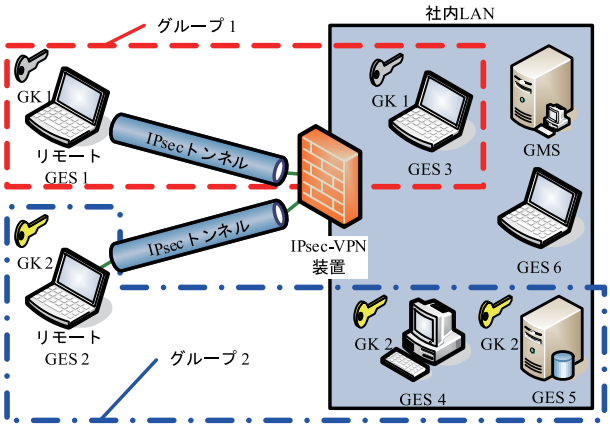


図 5 提案方式の構成

よって，暗号化/復号/透過中継/破棄を行う．暗号化通信には，PCCOM（Practical Cipher Communication Protocol）[10] を使用する．

3.4 提案方式によるリモートアクセス

図 5 に GSCIP と IPsec を併用したリモートアクセス方式の構成を示す．まずリモート GES は，IPsec-VPN 装置に対して IKE を実行し IPsec トンネルの構築を行う．その後リモート GES は鍵管理サーバ GMS に対してグループ鍵配送依頼を行う．GMS とリモート GES 間は公開鍵認証によって確実に認証され，該当するグループ情報とそれに対する GK が各リモート GES に配送される．グループ鍵が配送された後は，DPRP によって PIT が生成され，通信が開始される．

以上の手続きにより，リモート GES は社内 LAN に取り込まれ，GSCIP による End-to-End のセキュア通信が実現される．IPsec トンネル部分は，IPsec ESP[11),12)] と PCCOM による二重暗号となる．

4. 評　　価

表 1 に既存技術と提案方式の比較を示す.「IPsec トンネルモード」は，リモート端末と VPN 装置間を IPsec トンネルモードで接続する方法である．この方法では，社内 LAN での通信は平文となり，End-to-End で暗号化は行われていない.「IPsec トランスポートモード」は，社内 LAN 内の端末にも IPsec を実装し，リモート端末との間で End-to-End の暗号化を行う方法である．この方法では，NAT を越えるために IPsec パケットを UDP カプセル化する必要があり，本来 IPsec が持つセキュリティを確保できない．また，規模が大きくなると管理負荷が大きくなる．

「SSL-VPN」は，DMZ に設置された SSL-VPN サーバが代理となって社内のサーバにアクセスする

表 1 既存技術と提案方式の比較

	IPsec トンネルモード	IPsec トランスポートモード	SSL-VPN	提案方式
方式	リモート端末と VPN 装置間を IPsec トンネルモードで接続	リモート端末と社内サーバ間を IPsec トランスポートモードで接続	リモート端末と SSL-VPN 装置間を SSL で接続	リモート端末と VPN 装置間を IPsec トンネルモードで，リモート端末と社内サーバ間を GSCIP で接続
セキュリティ	× End-to-End で暗号化を行っていない	△ UDP カプセル化によるセキュリティ強度低下	× End-to-End で暗号化を行っていない	○
管理負荷	○	× システムの規模が大きくなると管理負荷が増大	× システムの規模が大きくなると管理負荷が増大	△ GSCIP の管理負荷は小さい
アプリケーション	○	○	× UDP や動的な TCP ポートを使用するアプリケーションが利用できない	○

方法である．SSL-VPN サーバとリモート端末間は HTTPS 通信を行い，セキュリティを確保できるが，任意のアプリケーションが利用できないという課題がある．

「提案方式」は，IPsec トンネルモードと GSCIP を併用する方法である．インターネット空間のセキュリティとイントラネット内の両者のセキュリティを確保することができる．GSCIP では動的に動作処理情報を生成するので，IPsec トンネルモードに比べて，管理負荷の増加はそれほど大きくならない．また任意のアプリケーションが利用可能である．

5. ま と め

これまでのリモートアクセス VPN は，インターネット側のセキュリティは考慮されていたが，イントラネット側では，パスワードによる認証のみでありセキュリティが脆弱であった．そこで GSCIP と IPsec を組み合わせることにより End-to-End でセキュリティを確保する方法を提案した．管理負荷の増加はわずかで，任意のアプリケーションが利用可能である．今後は提案方式の実装を行い，性能測定と実運用を試みる．

参 考 文 献

1) K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W.Little, and G.Zorn. Point-to-point tunneling protocol (pptp). RFC 2637, July 1999.
2) W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter. Layer two tunneling protocol “l2tp”. RFC 2661, August 1999.
3) S. Kent and K. Seo. Security architecture for the internet protocol. RFC 4301, December 2005.
4) T. Dierks and C. Allen. The tls protocol version 1.0. RFC 2246, January 1999.
5) P. Srisuresh and K. Egevang. Traditional ip network address translator (traditional nat). RFC 3022, January 2001.
6) 鈴木 秀和, 竹内 元規, 加藤 尚樹, 増田 真也, and 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. In **マルチメディア，分散，協調とモバイル（*DICOMO2005*）シンポジウム論文集**, volume 2005, pages 441–444, July 2005.
7) P. Hoffman. Algorithms for internet key exchange version 1 (ikev1). RFC 4109, May 2005.
8) A.Huttunen, B.Swander, V.Volpe, L.DiBurro, and M. Stenberg. Udp encapsulation of ipsec esp packets. RFC 3948, January 2005.
9) 鈴木 秀和 and 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**, 47(11):2976–2991, November 2006.
10) 増田 真也, 鈴木 秀和, 岡崎 直宣, and 渡邊 晃. Nat やファイアウォールと共存できる暗号通信方式 pccom の提案と実装. **情報処理学会論文誌**, 47(7):2258–2266, July 2006.
11) S. Kent. Ip encapsulating security payload (esp). RFC 4303, December 2005.
12) V. Manral. Cryptographic algorithm implementation requirements for encapsulating security payload (esp) and authentication header (ah). RFC 4835, April 2007.

GSCIPとIPsecを併用したリモートアクセス方式の提案と評価

A Proposal and Evaluation for a Remote Access Method using GSCIP and IPsec

名城大学大学院 理工学研究科

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

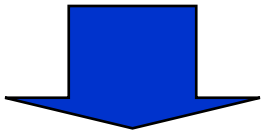
研究背景

- 企業ネットワークにおけるセキュリティ脅威
  - ユーザ名とパスワードに頼る簡単な相手認証・アクセス制御
  - 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

- インターネットVPN
  - IPsec（Security Architecture for Internet Protocol）
  - SSL（Secure Sockets Layer）
  - PPTP（Point to Point Tunneling Protocol）
  - L2TP（Layer 2 Tunneling Protocol）



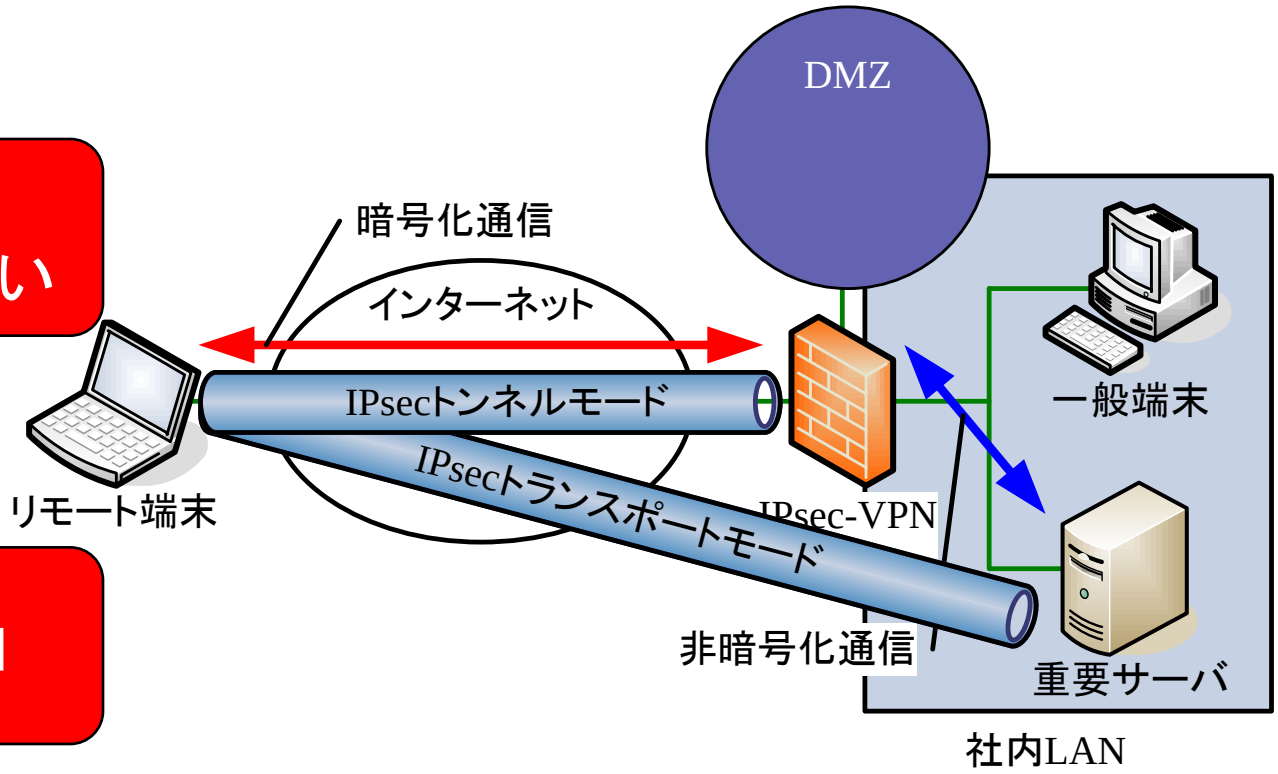
リモートアクセスVPNとしてIPsec，SSLが
良く利用されている

IPsec-VPN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，アプリケーションは意識せずに利用できる

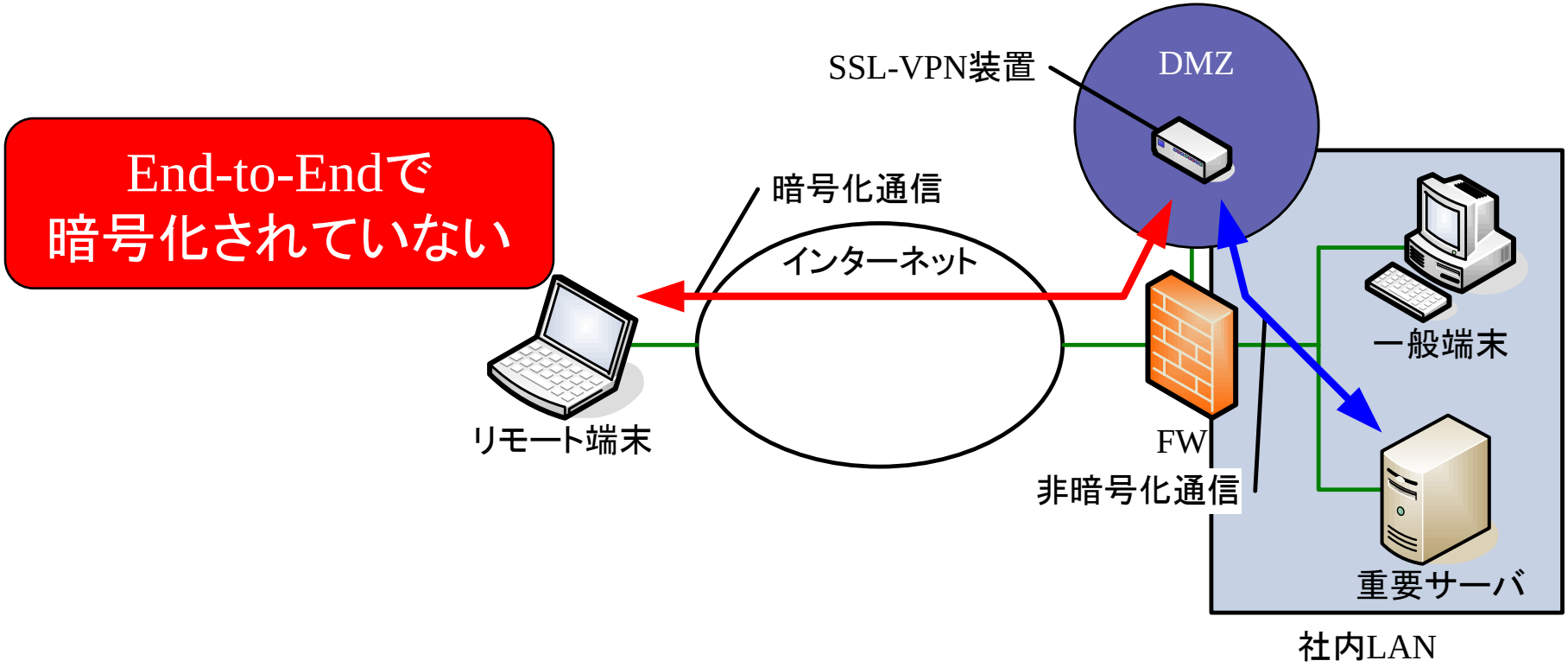
End-to-Endで
暗号化されていない

管理負荷の増加



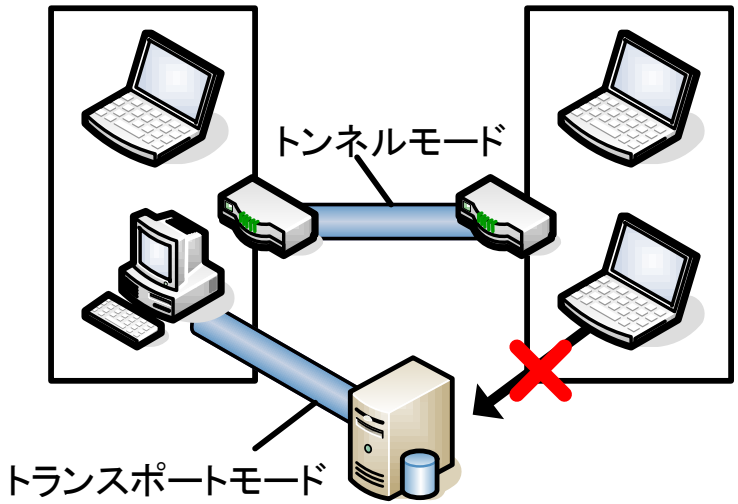
SSL-VPNの概要と問題点

- 暗号化にSSLを利用するVPN技術
- 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

- イントラネットにIPsecを適応させると
  - 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

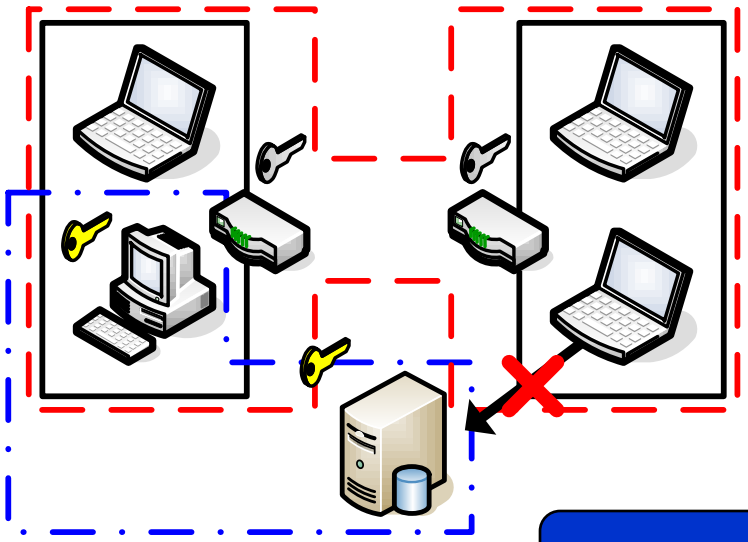


イントラネットの
セキュリティ対策
普及していない

GSCIP（Grouping for Secure Communication for IP）

GSCIPの概要

- 柔軟性とセキュリティを兼ね備えたグループ通信
  - 端末は通信グループに所属（多重帰属）
  - 同一グループ内の通信は暗号化
  - 必要な設定はシステムが学習して生成



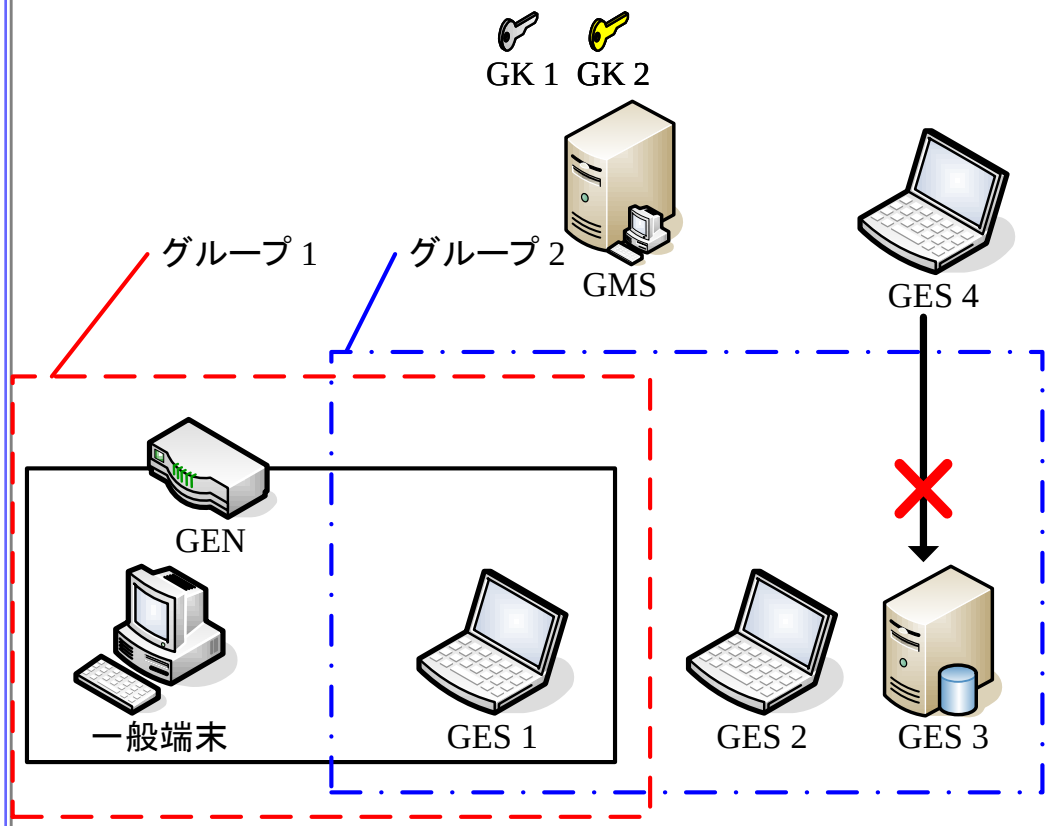
通信に先立ち
ネゴシエーションを実行

□端末間の認証
□動作処理情報の決定

DPRP（Dynamic Process Resolution Protocol）

GSCIPの動作概要

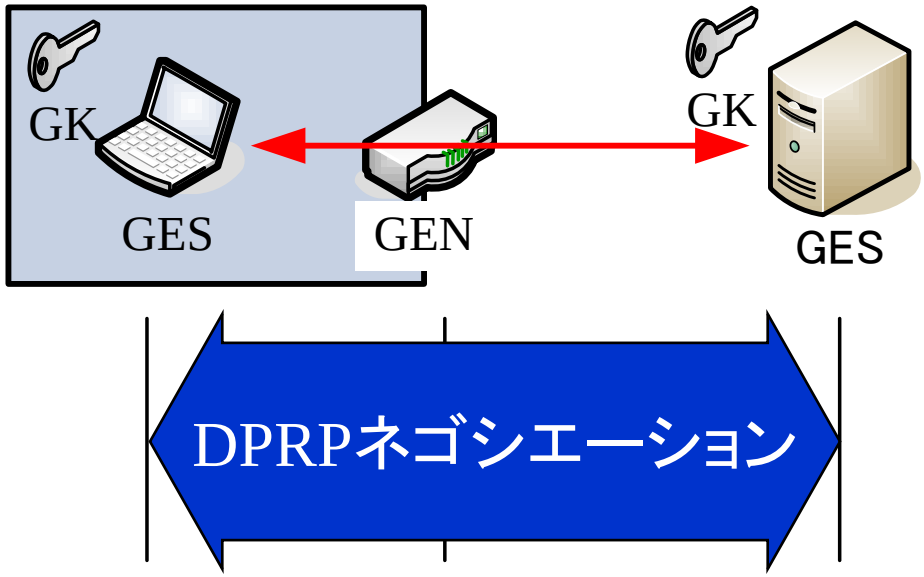
- GSCIPの構成



- 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は各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
- 動作モード
  - 開放モード（OP）
  - 閉域モード（CL）

DPRPの動作概要

- 通信経路上のGE間で動的にネゴシエーション
  - 端末間の認証
  - グループ情報，動作モードの交換
  - 動作処理情報の決定と通知

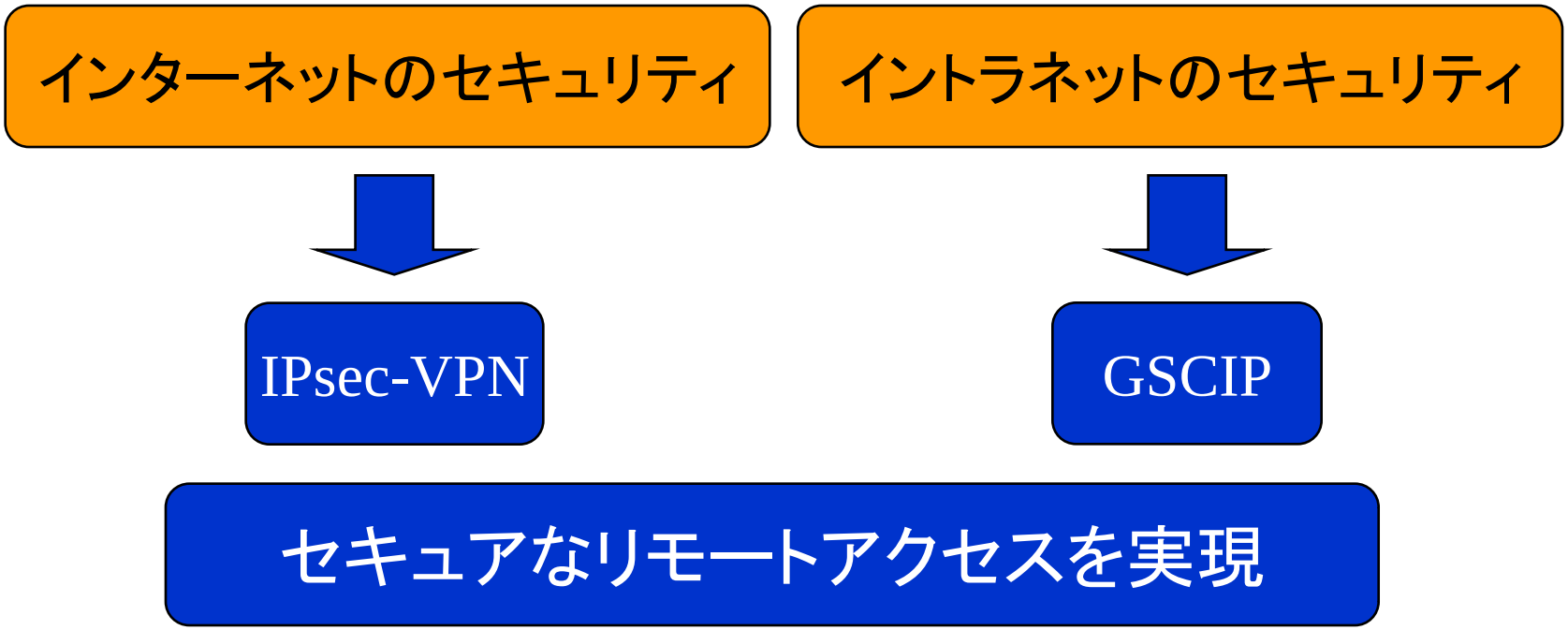


- グループ鍵による認証
- パケットの処理に必要な動作処理情報を生成
- 通信経路上のGEに通知

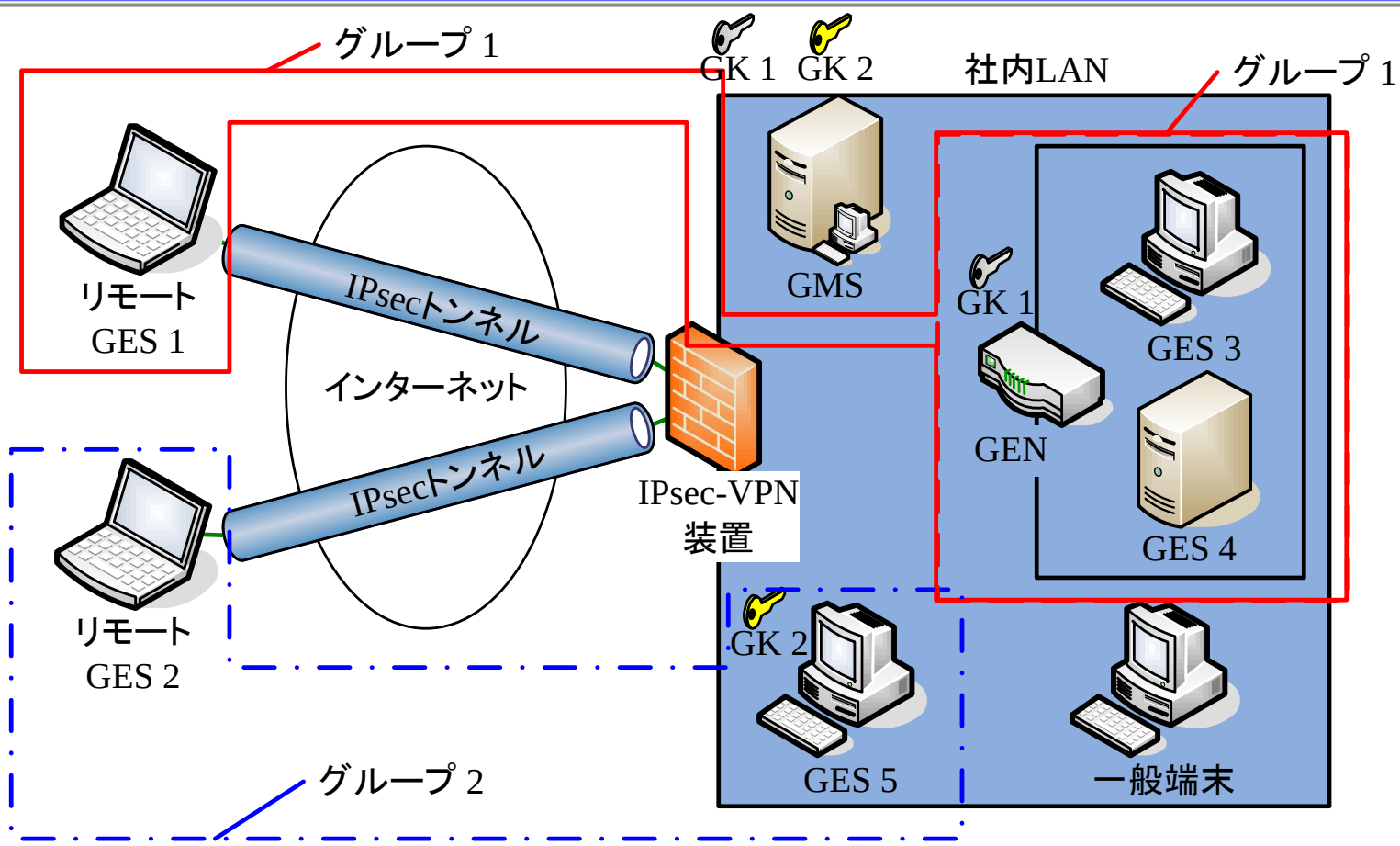
自動で設定することで管理負荷を抑える

提案方式の目的

- End-to-Endのセキュリティを確保
- 管理負荷の増加を抑える



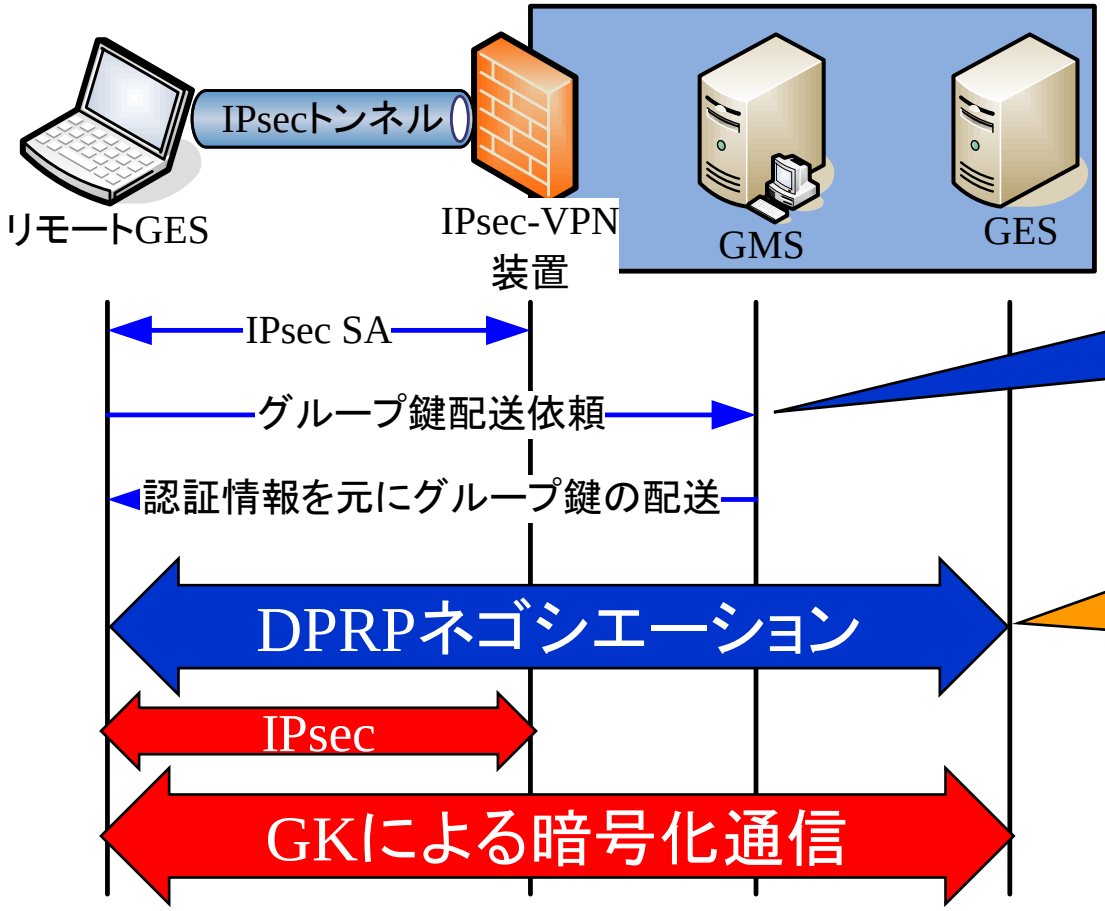
GSCIPとIPsecを併用したシステム構成



イントラネット：GSCIP

GSCIPをリモート端末まで適用

提案方式におけるGSCIPの動作



公開鍵認証を行い
GKの配送

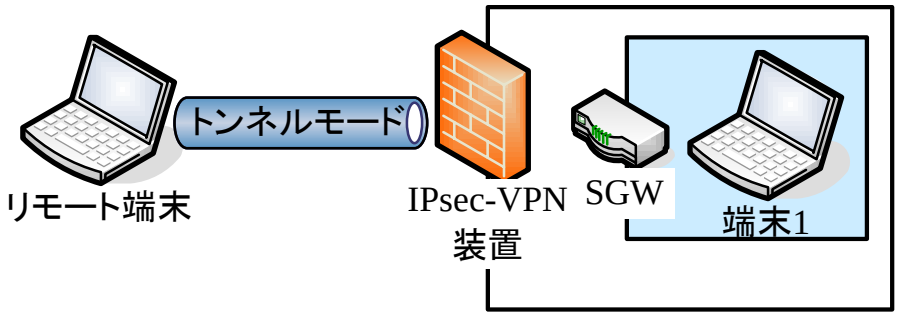
GE間の認証と
動作処理情報の
設定

End-to-Endのセキュア通信が可能になる

評価　～設定項目～

IPsecトンネルモード

	共有秘密鍵	セキュリティポリシ	IKE
設定項目	通信相手識別子 鍵データ	通信ペア識別子（送信元，宛先） 処理内容（IPsec/Discard/None） プロトコル（ESP/AH） モード（Transport/Tunnel） ポリシ適用レベル etc.	通信相手識別子 交換モード 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　etc.
項目数	2	16	12

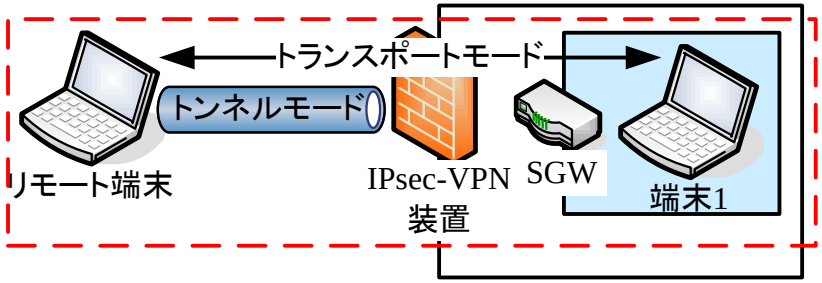


30項目の設定が必要

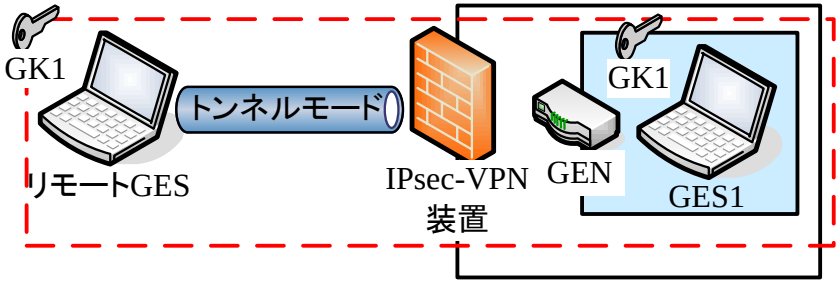
評価　～設定項目～

	トンネル/トランスポートモードの併用	トンネルモードとGSCIPの併用
設定項目	■トンネルモードの設定 □共有秘密鍵：2項目 □セキュリティポリシ：14項目 □IKE：12項目	■トンネルモードの設定 *□通信グループ番号* *□バージョン番号* *□鍵データ(GK)* □動作モード □通信グループ番号
項目数	トンネルモードの設定＋28項目	トンネルモードの設定＋5項目

トンネル/トランスポートモードの併用



トンネルモードとGSCIPの併用



設定項目が多く通信相手が増加すると
管理負荷が増大する

提案方式との比較

	IPsecトンネルモード	IPsecトンネルモードとトランスポートモードの併用	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をIPsecで暗号化	○ GKによるEnd-to-Endの暗号化
管理負荷 （リモート端末）	○ IPsecトンネルモードのみの設定	× アクセス先が増加すると管理負荷が増大	△ グループの管理のみであり動作処理情報は自動設定
	30項目	トンネルモードの設定（30項目）＋ 端末数×28項目	トンネルモードの設定（30項目）＋ 通信先×5項目

むすび

- まとめ
  - GSCIPとIPsecを併用したリモートアクセス方式の提案と評価
    - GSCIPとIPsecを併用
      - グループ鍵による暗号化でEnd-to-Endのセキュア通信
      - IPsecに比べ管理負荷を抑えた
- 今後の展開
  - 実装・性能測定を行う

付録

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

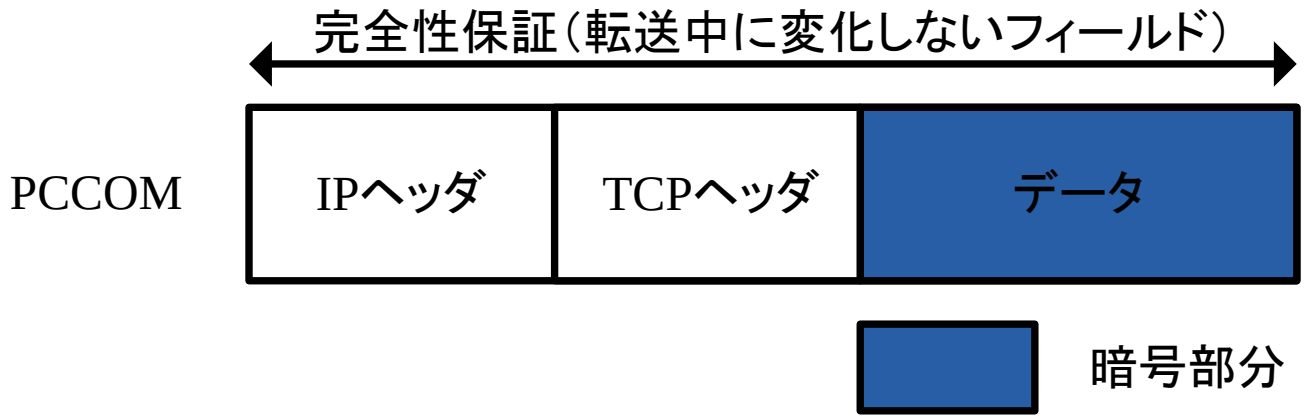
Normal	PCCOM	IPsec ESP
13.94	20.22	43.43

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

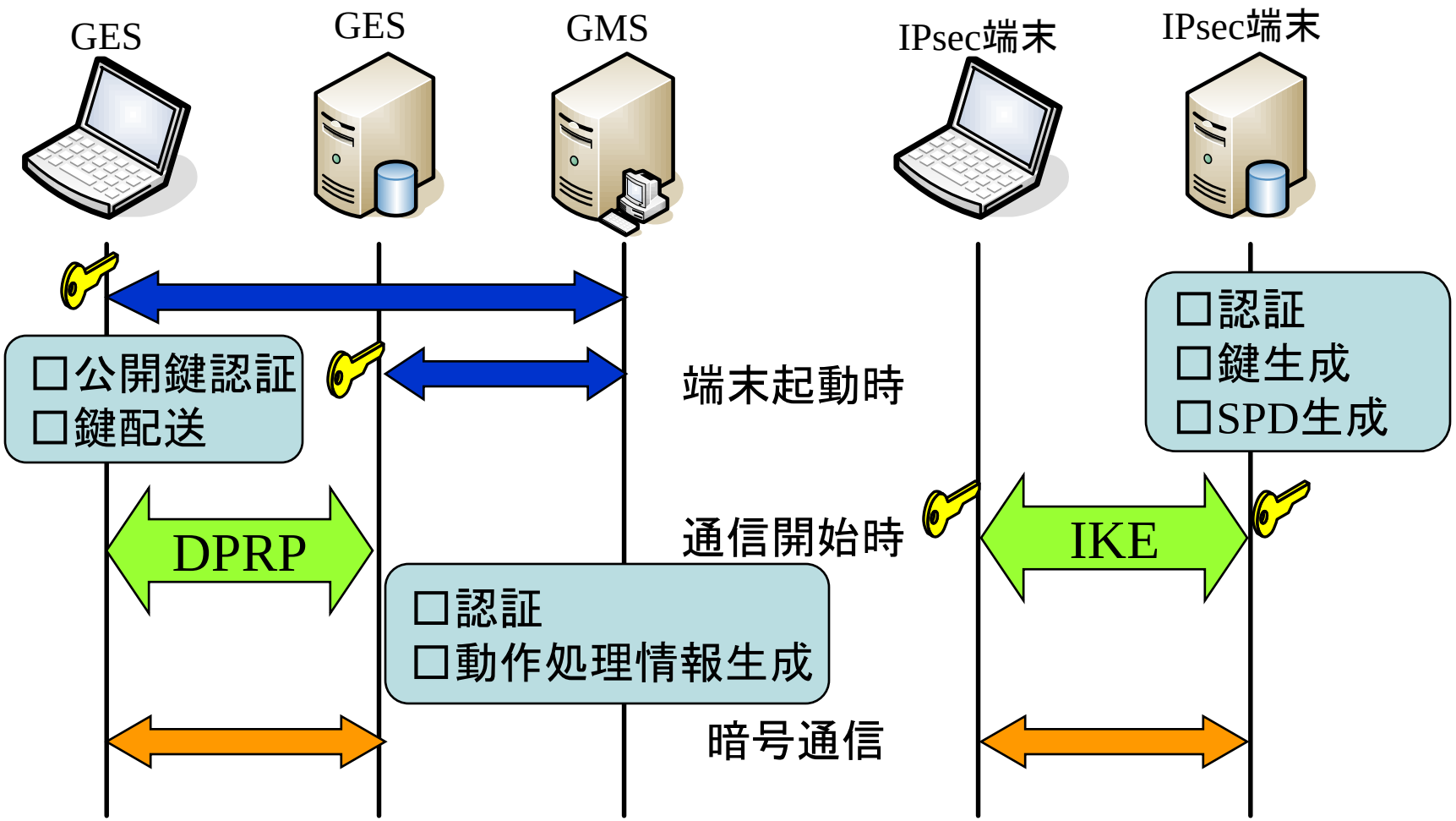


IPsec ESPとPCCOM

- 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	○	△

GSCIPとIPsecのアーキテクチャの違い



設定項目の詳細

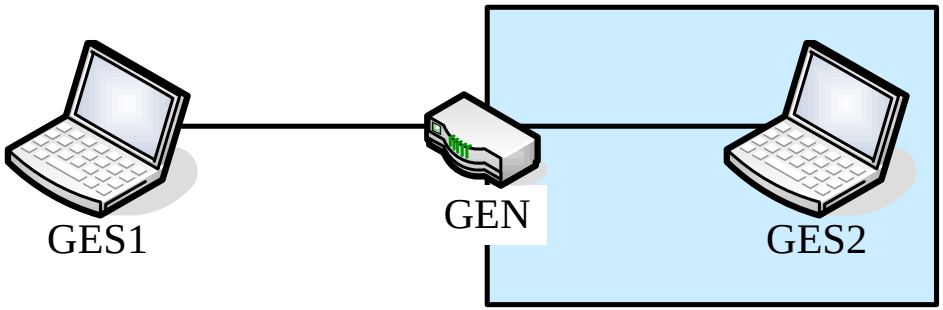
IPsec/IKE

	共有秘密鍵	セキュリティポリシ	IKE
設定項目	通信相手識別子 鍵データ	通信ペア識別子（送信元，宛先） 適用する上位プロトコル 処理内容（IPsec/Discard/None） プロトコル（ESP/AH） モード（Transport/Tunnel） SAの両端のアドレス ポリシ適用レベル（require/use）	交換モード 通信相手識別子 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
項目数	2	16	12

GSCIP/DPRP

	グループ鍵		GE情報
設定項目	通信グループ番号 バージョン番号 鍵データ		動作モード（OP/CL） 通信グループ番号
項目数	3		2

オーバーヘッド



スペック（GES1,GES2,GEN）
>> Pentium4 2.4GHz
>> 512MB
>> 100BASE-TX

単位：usec

	DPRP	IKE
ネゴシエーション	1,012	1,105,954
通信開始時間	1,040	2,994,033

IKEネゴシエーション
□通信を暗号化を利用するための鍵を生成
>> 公開鍵技術を利用しているため遅い
IPsec通信
□SAが無くIKEを開始するとパケットを破棄
>> TCPの再送処理に頼っている

IPsec/IKE (参考測定)
>> GES→IPsecクライアント
>> GEN→SGW

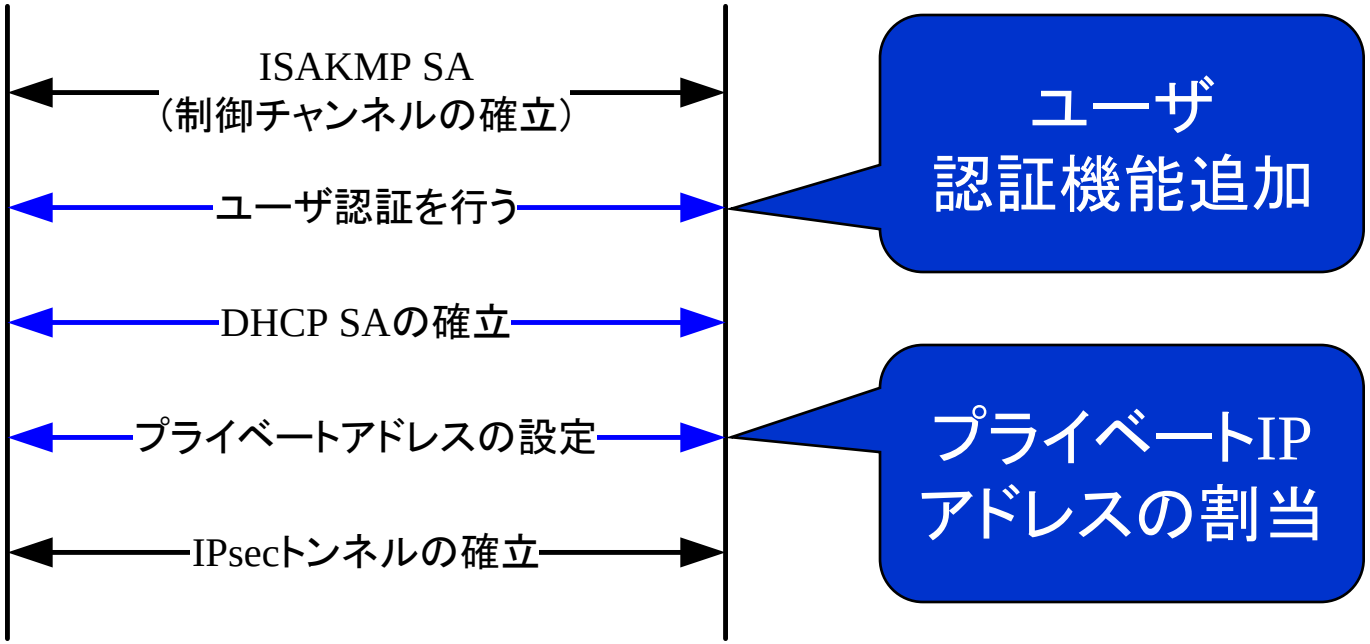
IKE (racoon)
>> 事前共有鍵方式
>> ESPトランスポートモード
・GES1-GES2:ipsec
・GES1-GEN:none
・XXX-GEN:discard

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
管理負荷	○ IPsecトンネルモードのみの設定	△ 詳細なアクセス制御が可能であるが管理負荷増大	△ グループの管理のみであり動作処理情報は自動設定

リモートアクセスにおけるIPsecの動作

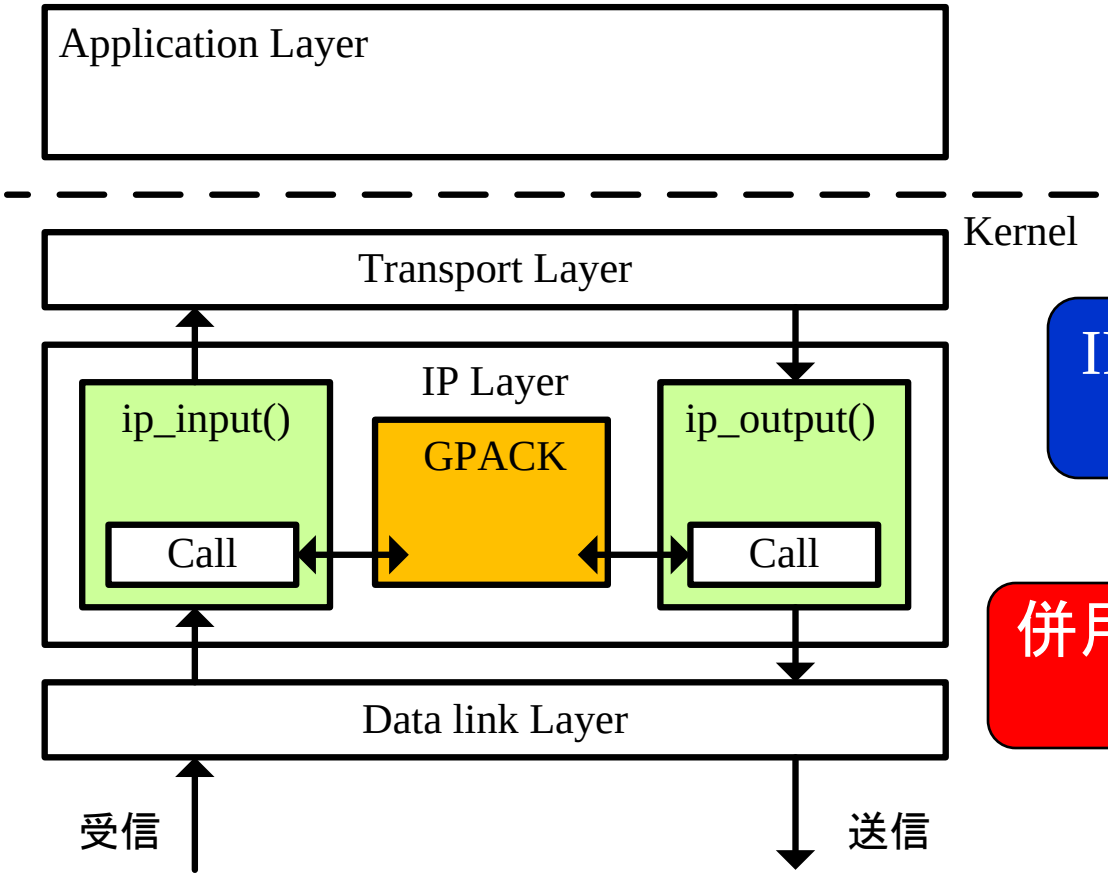
ユーザ認証機能
プライベートIPの割当



既存のIPsec-VPNの動作
IKEを拡張して提供

実装

- GSCIPはIP層に実装



IPsecはIP層全体に実装されている

併用するにはGSCIPの処理手順を考慮