

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

今 村 圭 佑^{†1} 鈴 木 秀 和^{†1}
後 藤 裕 司^{†1} 渡 邊 晃^{†1}

イントラネット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。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概念として FPN (Flexible Private Network) と呼ぶシステムを提唱してきた。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、更新などを行う。本稿ではイントラネットにおいて GSCIP と IPsec をそれぞれ運用する場合に発生する管理負荷を定量的に求め、有効性を確認する。

Implementation and Operation Evaluation of Group Management Server which realize secure communication architecture GSCIP

KEISUKE IMAMURA,^{†1} HIDEKAZU SUZUKI,^{†1} YUJI GOTO^{†1}
and AKIRA WATANABE^{†1}

Network crimes in intranet by insiders are often reported. However, in intranets, a very simple authentication method using a user name and a password is widely used. The communication group according to business is built in a enterprise network, and encryption communication is beneficial. Thus, we have been proposing the concept of Flexible Private Network (FPN) that provides both flexibility and security. We have been proposing a new network architecture called "GSCIP" (Grouping for Secure Communication for IP) for realizing FPN. In GSCIP, allowance of communication and a encryption key are decided dynamically from location of terminals, group numbers, and operation modes. GSCIP is managed by the group management server GMS (Group Management Server). In GMS, the definition of communication groups and operation mode are defined by a network manager. In this paper, management loads in GMS are calculated, and it is compared with the case of IPsec.

1. はじめに

企業ネットワークでは、不正侵入、データの盗聴、改竄などに対するセキュリティ対策が重要な課題となっている。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、セキュリティ強度の高い技術を駆使したり、ファイアウォールや IDS (Intrusion Detection System) などと併用したりするなど、様々な対策がなされている。しかし企業ネットワークのセキュリティ

の脅威は組織内部にも存在し、社員や関係者の不正による犯罪が多く報告されている。企業ネットワーク内部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。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。この方法によりネットワークインフラ環境をそのまま利用しながら、同一グループのメンバー間通信の安全性を確保することができる。

エンド端末同士でセキュリティを確保する既存の方法として IPsec¹⁾ トランスポートモードがある。この

^{†1} 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University

本稿では適当なネットワークモデルを想定し、GMSを用いて GSCIP を運用する場合と IPsec を用いた場合の管理負荷を、初期設定時、ネットワークの構成変化時、および通信グループのメンバ構成変化時に分けて評価した。

以下にクライアント X と Y が KINK を利用して SA 情報を交換し、SA を設定する手順を説明する。図 1 に KINK の動作概要を示す。Kerberos の鍵発行局を KDC (Key Distribution Center) と呼び、KDC は一般的に AS (Authentication Server) と TGS (Ticket Granting Server) で構成される。KDC はクライアント X、および Y と事前に共通鍵を共有している必要がある。ここで AS は、Kerberos を利用するクライア



ントの認証と TGT (Ticket Granting Ticket) の配送を行う。TGS (Ticket Granting Server) は、クライアントが提出した TGT を調べ KINK を実行するために必要な情報とセッション鍵を配送する。

- (1) クライアント X は AS に対して任意のチケットを発行するためのチケット TGT を要求する。
- (2) AS は、Kerberos の識別子に応じてチケット TGT と TGS と通信するためのセッション鍵 S_x を返信する。
- (3) クライアント X は Y と SA を交換するために必要なチケット $T_{x:y}$ を TGS に要求する。チケットの要求には事前に取得した TGT を提示する必要がある。
- (4) TGS はクライアント X と Y が SA を交換するために必要な $T_{x:y}$ とセッション鍵 $S_{x:y}$ を返信する。
- (5) クライアント X は乱数関数 prf_x とセッション鍵 $S_{x:y}$ を使用して SA に利用する鍵を生成し、自らの inbound として設定する。設定した情報をクライアント Y に送信する。
- (6) クライアント Y は乱数関数 prf_y とセッション鍵 $S_{x:y}$ を使用して SA に利用する鍵を生成し、自らの inbound として設定する。また X の inbound の情報を自らの outbound として設定する。その後設定した inbound の情報をクライアント X に送信する。
- (7) クライアント Y から受信した inbound の情報を X の outbound として設定し SA が共有される。

KINK ではクライアントに KDC との共通鍵と Kerberos の識別子を設定すればよく、設定による管理負荷は大きくない。しかし KINK ではホストベースの通信のみサポートしており、IPsec 通信を実現するにはエンド端末すべてに IPsec の実装が必要である。また通信ペアごとに SA を構築するため管理するセッション鍵が増加する。

3. GSCIP

3.1 通信グループ構築方法

我々が目指している FPN とは、ネットワークのあるべき姿を示したものである。ドメイン単位と個人単位が混在したネットワーク環境であっても容易にグループを定義できる。またユーザはセキュリティを確保したまま自由に移動できる。さらにユーザは、IPv4 グローバルアドレス空間、IPv4 プライベートアドレス空間、IPv6 アドレス空間の違いを意識する必要がな

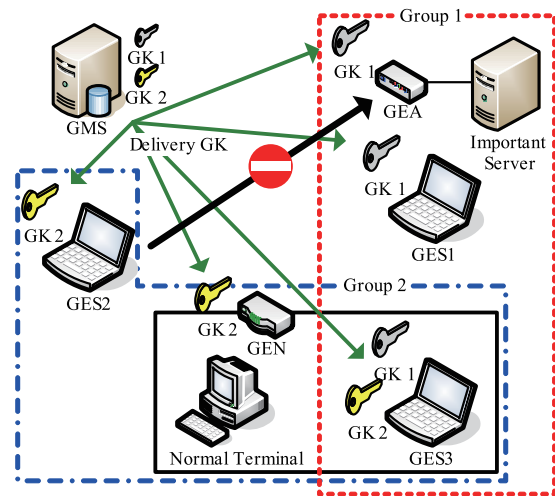


図2 通信グループの構築方法

い。GSCIP とは FPN を具体的に実現するためのネットワーク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 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 による相互認証と暗号通信が実行される。

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所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2では GEA はグループ1に所属しており、グループ外の GES2 からのアクセスを拒否することが可能となる。

GE に必要な情報はグループ管理サーバ GMS で定

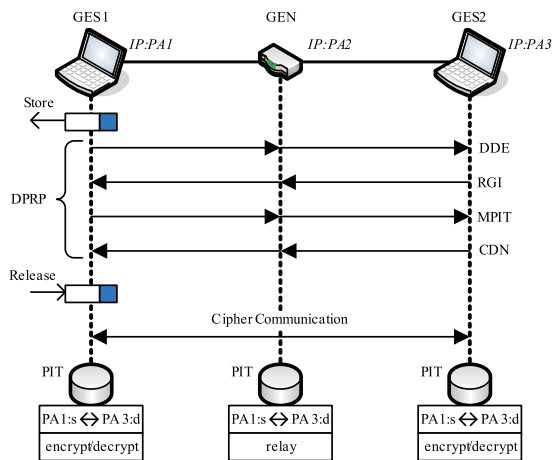


図 3 DPRP のシーケンス

義される。この情報を GE 情報と呼び、ユーザ ID と動作モード、および通信グループ番号から構成される。通信グループ番号は IP アドレスに依存することなく定義でき、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。サブネット内に存在する個人に対して、そのサブネットとは別の通信グループを定義することもできる。GMS では通信グループの定義のほかに、グループ鍵 GK の生成、更新などを行う。グループ鍵 GK は定義された通信グループに対応して生成され、定期的に更新される。

3.2 DPRP の概要

DPRP (Dynamic Process Resolution Protocol)⁶⁾ は GSCIP を実現する一連のプロトコルの 1 つで、GE がネットワーク構成を学習することにより、自己の動作を決定する動作処理テーブル PIT (Process Information Table) を自律的に生成する。各 GE は自己の PIT 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バージョン番号が記述されている。DPRP はエンド端末間の通信に先立ち実行するネゴシエーションプロトコルである。端末はパケット送信時に PIT を検索し、PIT に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カーネル内に退避し、DPRP を実行して PIT を動的に生成する。図 3 に DPRP のシーケンスを示す。図 3 はエンド端末 GES1、GES2 の間にルータ GEN が存在する場合を示している。

DPRP には、ICMP をベースとした DDE (Detect

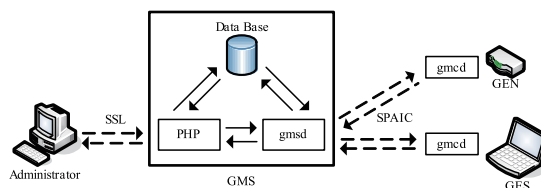


図 4 GSCIP における管理システムの構成

Destination End GE), RGI (Report GE Information), MPIT (Make Process Information Table), CDN (Complete DPRP Negotiation) という 4 つの制御パケットからなる。DDE は終点 GE を探索するもので、DPRP のトリガーとなった通信パケットの CID (Connection ID; 送信元/宛先 IP アドレス、ポート番号、プロトコルタイプ) がセットされ、通信パケットの宛先へ送信される。図 3 では GES2 が終点 GE となり、RGI を返送する。RGI は始点 GE を探索し、かつ各 GE の設定情報を収集するためのものである。中間 GE は RGI を中継する際、自身の設定情報をパケットに追加していく。図 3 では 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 を仮生成する。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 を受信した各 GE は PIT を確定させる。GES1 は待避していた通信パケットを復帰させる。以後の通信は各 GE において、PIT に従った処理が実行される。

パケットは PIT に記述されている動作処理情報によって、暗号化/復号、透過中継、破棄を行う。暗号化通信には、どのような方式を適用することも可能であるが、GSCIP と親和性の高い PCCOM (Practical Cipher Communication Protocol)⁷⁾ を使用すれば、高スループットの通信が可能である。

4. グループ管理サーバの実現

4.1 管理システムの構成

図 4 に GSCIP におけるシステムの構成を示す。GMS は GE 情報やグループ鍵を格納するデータベース、クライアントに情報を配送するサーバデーモン gmsd、および管理者からのユーザ登録等を受け付ける Web アプリケーション PHP から構成されている。管理者は管理用端末から SSL により GMS にアクセスし、操作を行うことができる。各 GE は起動時に GMS に対し設定情報を要求する。GMS は GE の確実な認証

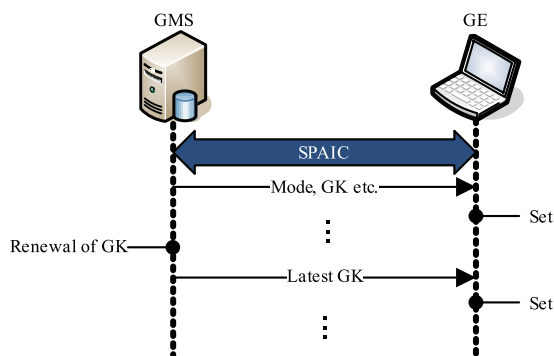


図 5 GMS から GE への配送

を行った後、設定情報を暗号化して配送する。認証の方法については既存の方式を適用することも可能であるが、ここでは GSCIP と親和性の高い SPAIC（Secure Protocol for Authentication with IC card）⁸⁾ を使用することを想定する。SPAIC は非接触 IC カードの利用が可能な公開鍵認証システムで、GMS と GE 間で共通鍵を生成し、その共通鍵で設定情報やグループ鍵を安全に配送することができる。

4.2 配送情報

GMS から GE へ配送する情報を表 1 に示す。GE 情報として通信モード、所属通信グループ番号、グループ鍵情報としてグループ鍵 GK、鍵バージョンを配送する。

図 5 に GMS から GE への配送を示す。GE は電源投入時に SPAIC による認証を行い、GMS から GE 毎に定義されている情報を取得する。この情報には GE 情報、グループ鍵情報が含まれる。GE は通信開始時にここで配送された情報を用いて DPRP を実行し、GE 間の認証と PIT の生成を行う。グループ鍵情報は GMS で定期的に更新され、最新のグループ鍵が GE に配送される。

5. 管理負荷の評価

5.1 評価項目

GSCIP をイントラネットでも運用した場合の管理負荷について評価する。評価項目は 1. 初期管理負荷、2. ネットワークの構成変化時に発生する管理負荷、および 3. 通信グループのメンバ構成変化時に発生する管理負荷とする。ここで構成変化とは引越、人事異動や出張などオフラインでの移動による変化であり、通信

表 1 配送情報

GE 情報	通信モード、所属通信グループ番号
グループ鍵情報	グループ鍵 GK、鍵バージョン

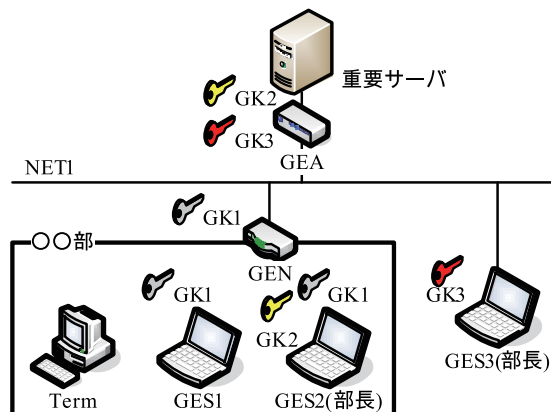


図 6 想定するネットワーク構成

中の移動は含まない。通信中の移動については GSCIP の枠組みの中で Mobile PPC（Mobile Peer to Peer Communication）⁹⁾ を適用すべく別途検討中である。

図 6 に想定するネットワーク構成を示す。〇〇部に所属する一般端末 Term、GEN、GES1、GES2（部長）と GES3（部長）、および部長のみアクセスが可能な重要サーバの直前に配置されている GEA で構成される。各 GE が所持するグループ鍵を表 2 に示す。〇〇部はグループ鍵 GK1 を使用しグループを構成している。〇〇部に所属する部長（GES2）は〇〇部のグループ鍵 GK1 と重要サーバへアクセスするための GK2 を所持している。同様に部長（GES3）は重要サーバにアクセスするための GK3 を所持している。ここで GEA、GEN は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、GES1、GES2、GES3 は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で設定されているものとする。〇〇部間の通信は GK1 で暗号化される。重要サーバへのアクセスは部長のみが許されており、それぞれ GK2、GK3 で暗号化される。

5.2 初期管理負荷

GSCIP と IPsec の管理負荷を評価するため管理装置における設定項目数を評価指標としてとりあげる。GSCIP と IPsec をそれぞれ運用するために必要な

表 2 各 GE が所持する GK

	所持するグループ鍵
GEA	GK2, GK3
Term（一般端末）	—
GES1	GK1
GES2（部長）	GK1, GK2
GES3（部長）	GK3
GEN	GK1

表 3 設定項目数

GSCIP/DPRP			
	グループ鍵情報	動作処理情報	GE 情報
設定内容	グループ番号 グループ鍵 GK GK バージョン		ユーザ ID 動作モード 所属通信グループ番号
項目数	3	0	3

IPsec/IKE			
	事前共有鍵情報	セキュリティポリシー	IKE
設定内容	通信相手識別子 事前共有鍵	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) ポリシーレベル etc.	通信相手識別子 交換モード (main/aggressive) 暗号アルゴリズム ハッシュアルゴリズム DH グループ etc.
項目数	2	Discard/None:8 IPsec,Transport:14 IPsec,Tunnel:16	12

表 4 各端末の設定項目数

GSCIP/DPRP				
	グループ鍵情報	動作処理情報	GE 情報	合計
GES1	3		3	6
GES2	6		4	10
GES3	3		3	6
GEN	3		3	6
GEA	6		4	10
合計	21	0	17	38

IPsec/IKE				
	事前共有鍵情報	セキュリティポリシー	IKE	合計
ST1	2	IPsec,Transport:14	12	28
ST2	4	IPsec,Transport:14 × 2	12	44
ST3	2	IPsec,Transport:14	12	28
SGW	2	None:8, Discard:8	12	30
Server	4	IPsec,Transport:14 × 2	12	44
合計	14	100	60	174

る設定内容と各設定 1 つあたりに必要な項目数を表 3 に示す。GE 情報にはユーザ ID、動作モード、および GE が所属する通信グループ番号の 3 項目が必要である。グループ鍵情報には通信グループ番号とグループ鍵、グループ鍵のバージョン番号の 3 項目必要となる。一方、IPsec では事前にエンド端末で共有する秘密鍵、どの通信パケットに対してどのような処理を行うかを定めたセキュリティポリシー、および IKE の設定が必要である。セキュリティポリシーは双方向定義する必要があり、処理内容やモードにより項目数が異なる。IPsec における設定項目数はそれぞれ 2, (8, 14, 16), 12 である。

図 6 における想定環境の GE の数は 5 台である。各 GE の所属する通信グループ数は GES1, GES3, GEN1 が 1 グループ、GEA, GES2 が 2 グループである。ゆえに GE 情報として必要な設定項目数は、ユー

ザ ID と動作モードで 10、所属グループの合計が 7、合計 17 である。また通信グループ数は 3 であり、グループ鍵情報の設定項目として 21 必要となる。よって初期管理負荷の合計は 38 となる。

IPsec を利用して図 6 と同様な想定環境を実現する場合の設定項目数を表 4 に示す。ここで ST1, ST2, ST3, SGW, Server はそれぞれ GES1, GES2, GES3, GEN, GEA に対である。ST1 と ST2 は互いにトランスポートモードのセキュリティポリシーの設定が必要である。ST2 と ST3 は Server に対するトランスポートモードの設定が必要である。同様に Server は ST2 と ST3 に対してトランスポートモードの設定が必要である。ゆえに IPsec を利用する場合の初期設定の項目数は、ST1, ST3 に 28, ST2, Server に 44, SGW に 30、合計 174 になる。

5.3 ネットワーク構成変化時に発生する管理負荷

図6においてGES2(部長)がGEN配下からNET1へ移動した際に必要な設定項目を評価する。GSCIPでは端末が移動しても、そのつどDPRPにより動作処理情報を新しく生成するため、ユーザや管理者が行う作業はいっさい発生しない。

一方IPsecで同様の変更を実現しようとする、ST2は移動によりIPアドレスが変化するため、通信を識別するための識別子を変更する必要がある。そのための管理負荷は4である。さらに〇〇部に所属する一般端末と通信するために、SGWに対してトンネルモードの設定を追加する必要がある。その管理負荷は16となり、ST2の移動による管理負荷は合計20となる。

5.4 通信グループのメンバ構成変化時に発生する管理負荷

図6においてグループ1に所属し、重要サーバにアクセス可能なユーザGES4を新たにNET1上に配置する場合の管理負荷を評価する。GSCIPでは管理者がGMSにてGES4のGE情報を追加定義する。その情報はGES4のユーザID、動作モードおよび所属通信グループ番号のみである。また重要サーバへのアクセスのために、新しい通信グループを追加定義する必要があり、グループ鍵情報として、通信グループ番号、グループ鍵および鍵バージョンを定義する。GES4は電源投入時に定義されたGE情報とグループ鍵をGMSから取得し、自動に設定される。通信を行う際にはDPRPにより動作処理情報を動的に決定する。よって新しく端末を追加した場合の管理負荷は合計10である。

一方IPsecでは、ST4に事前共有鍵情報、セキュリティポリシー、およびIKEの設定をST2, Serverに行う必要がある、合計44である。さらにST2, ServerはST4に対するセキュリティポリシーを追加する設定する必要がある(合計28)。実際の環境では、1つの部門や業務グループに多くのメンバがいることが想定されるため、さらに設定追加による管理負荷が増加する。

これらのことから、GSCIPは初期導入時や端末の移動、メンバの追加にともなう管理負荷が発生しないため、FPNを実現する有効な方法であるといえる。

6. む す び

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。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を運用する場合の管理負荷について評価した。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検討を進め、有効性を確認していく。

謝辞 本研究の一部は、日本学術振興会科学研究費補助金(特別研究員奨励費20・1069)の助成を受けたものである。

参 考 文 献

- 1) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301 (2005).
- 2) 鈴木秀和, 竹内元規, 加藤尚樹, 増田真也, 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, 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, Vol.2005, No.6, pp.441-444 (2005).
- 3) Hoffman, P.: Algorithms for Internet Key Exchange version 1 (IKEv1), RFC 4109 (2005).
- 4) Neuman, C., Yu, T., Hartman, S. and Raeburn, K.: The Kerberos Network Authentication Service (V5), RFC 4120 (2005).
- 5) Sakane, S., Kamada, K., Thomas, M. and Vilhuber, J.: Kerberized Internet Negotiation of Keys (KINK), RFC 4430 (2006).
- 6) 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 (2006).
- 7) 増田真也, 鈴木秀和, 岡崎直宣, 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, Vol.47, No.7, pp.2258-2266 (2006).
- 8) 束 長俊, 鈴木秀和, 渡邊 晃: 非接触型ICカードを用いた認証方式SPAICの提案, マルチメディア, 分散, 協調とモバイル(DICOMO2007)シンポジウム論文集, Vol.2007, No.1, pp.1332-1337 (2007).
- 9) 竹内元規, 鈴木秀和, 渡邊 晃: エンドエンドで移動透過性を実現するMobile PPCの提案と実装, 情報処理学会論文誌, Vol.47, No.12, pp.3244-3257 (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 Operation Evaluation of Group Management Server
which realize secure communication architecture GSCIP

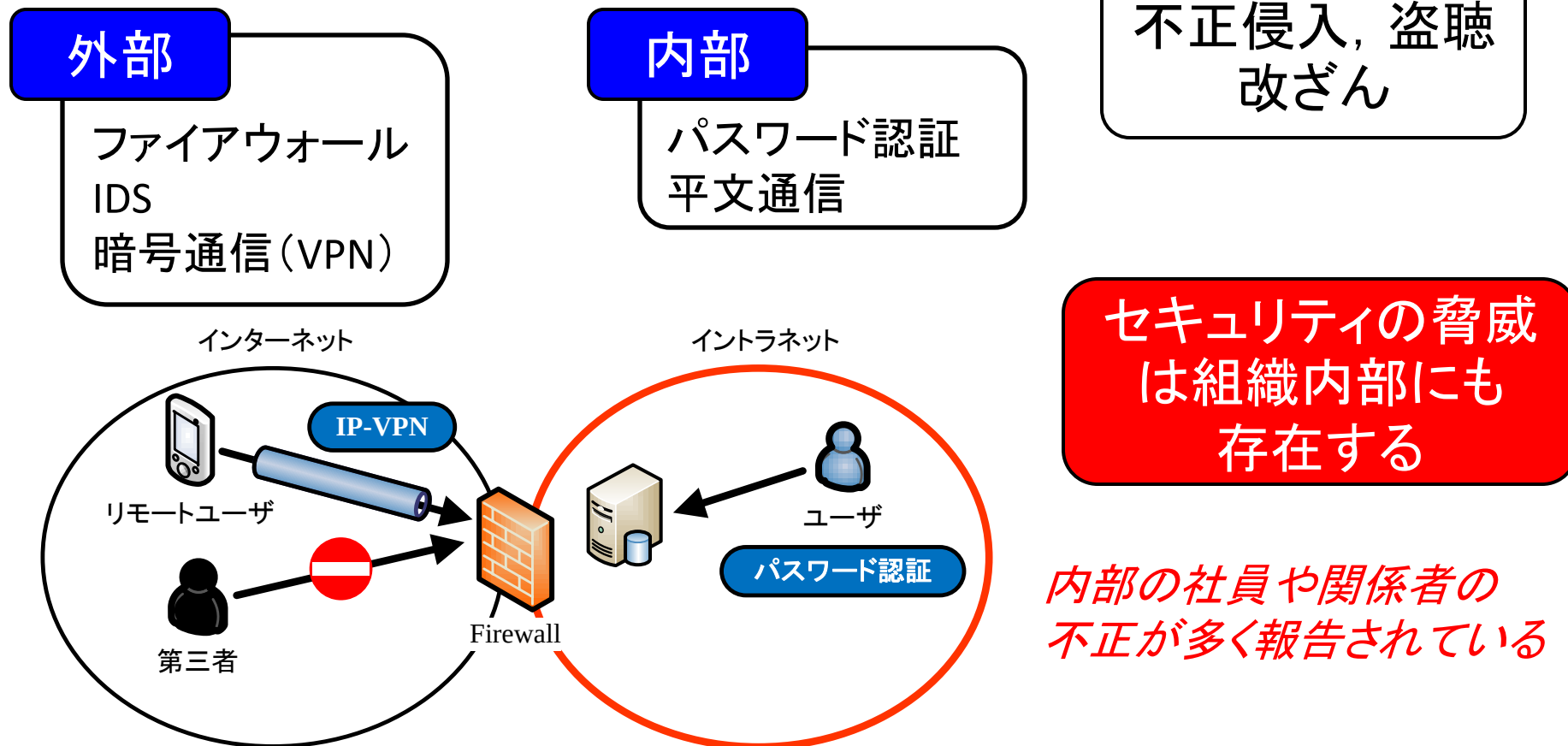
名城大学大学院理工学研究科

今村圭佑, 鈴木秀和, 後藤裕司, 渡邊晃

研究背景1

■ 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



研究背景2

■ 企業ネットワーク

- ◆ 部門やプロジェクト単位
- ◆ 役職単位(部長, 課長)

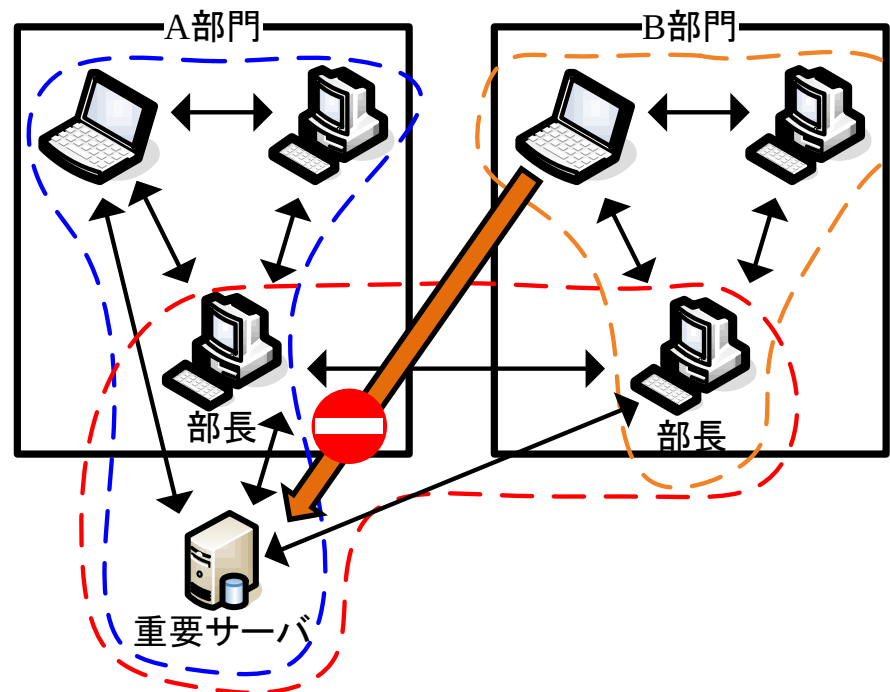
部署毎にデータを扱っている

部門や業務, 役職に応じた通信グループを構築

- 部門や業務によってアクセス可・不可
- 役職によってアクセス可・不可

認証・暗号通信

有効なセキュリティ対策となる



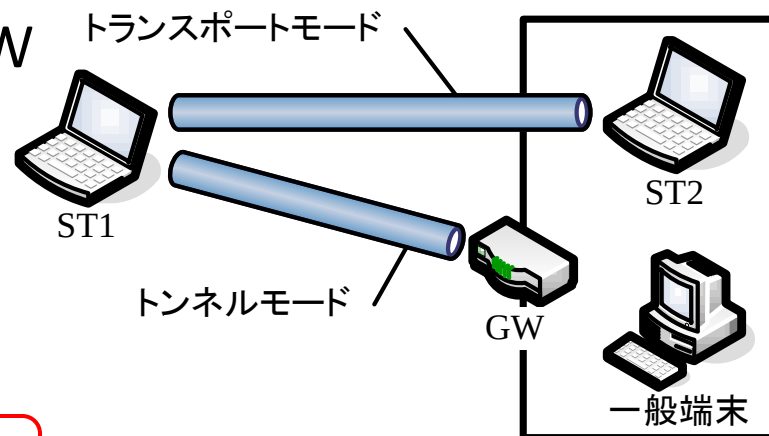
既存技術: IPsec

■ 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) – SGW

◆トランスポートモード: 端末 – 端末

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), 鍵, SAの有効期間



IPsec SAを共有することで通信を行う

SA生成に必要な鍵やパラメータの交換方式として...

IKEv1 (Internet Key Exchange)

RFC 4109

KINK (Kerberized Internet Negotiation of Keys)

RFC 4430

IKE (Internet Key Exchange)

■ 最も普及している鍵交換プロトコル

◆ 動作モード, 認証パラメータ, 認証方式, 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...

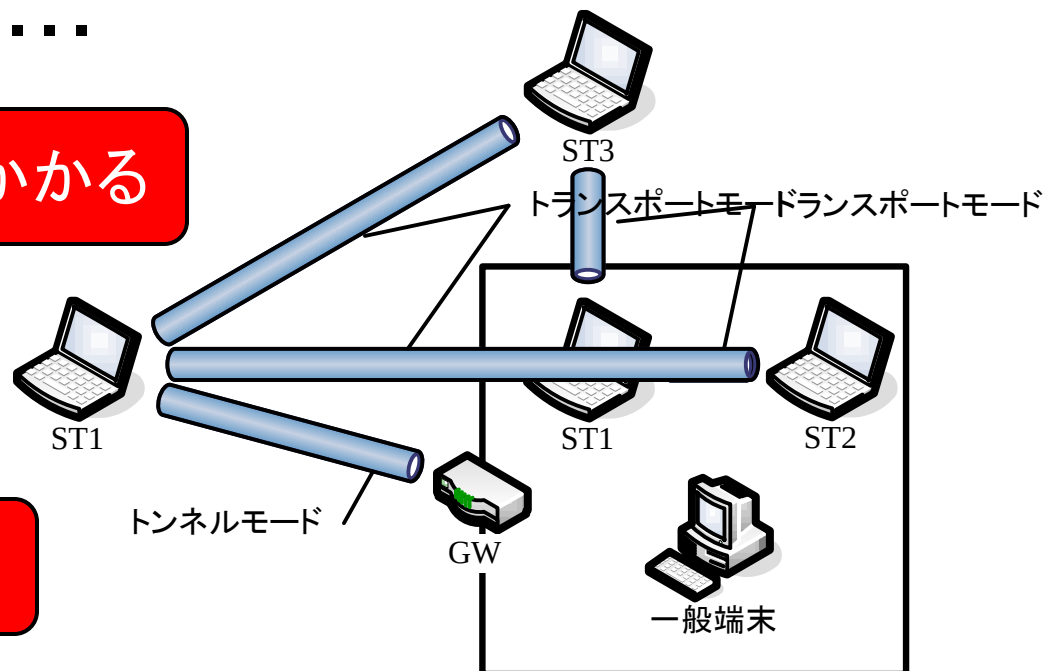
◆ 高度な専門知識が必要

任意の2点間なら良いが...

多台数間の設定は負担がかかる

端末が移動してIPアドレスが
変化すると...

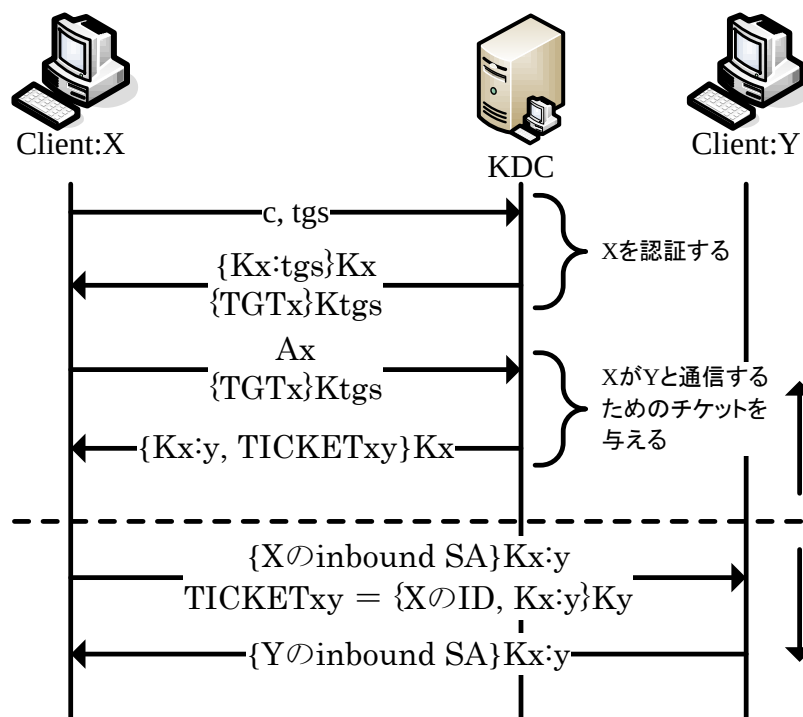
設定の変更が必要になる



KINK (Kerberized Internet Negotiation of Keys)

■ Kerberosの認証機構を利用したSA交換方法

- ◆ KINKサービスチケットを利用して相互認証を行う
- ◆ サービスチケットに含まれるパラメータをSAに利用



ノードとKDCは事前に鍵を共有

1. TGTxを取得
2. Yと通信するためのTICKETxyを取得
3. 取得したTICKETxyに提示してSAを設定する

Kerberosの範囲

KINKの範囲

チケットを所持している端末で
SAを構築

KINK (Kerberized Internet Negotiation of Keys)

■ KINKでグループ通信を導入すると...

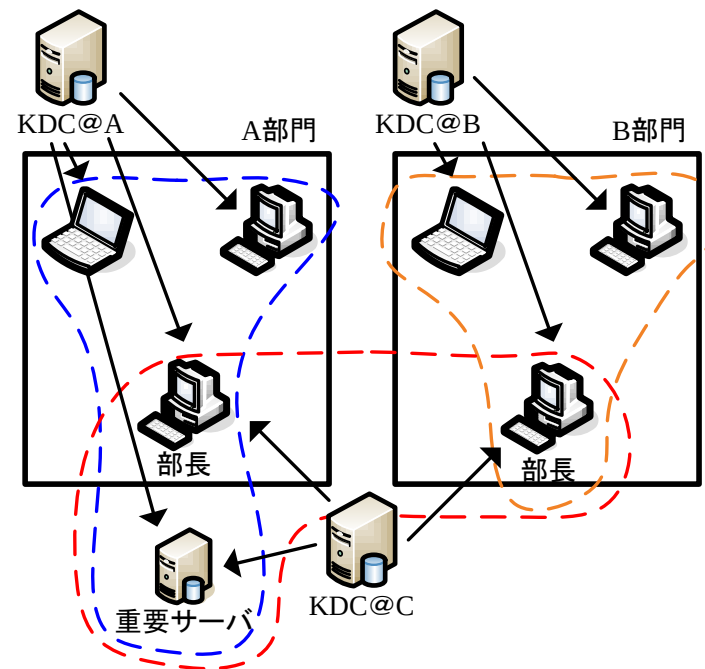
◆ KDCサーバをグループ毎に導入しなければならない

■ 少数のユーザでサーバを設置するのは現実的ではない

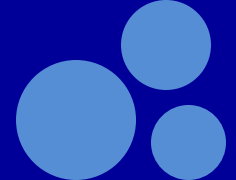
◆ 所属グループ数に応じてKerberos ID, 共通鍵が必要になる

■ 複数のID, 共通鍵の所持になる

一般的に制御ネットワーク, センサネットワークに用いられている



提案方式の目的



■ 柔軟性

- ◆ 部門や業務内容，役職単位で構成が可能
- ◆ 場所を移動しても設定の変更・追加はなし

■ セキュリティ

- ◆ 端末間，端末－SGW間で認証と暗号通信

■ 管理コスト

- ◆ 必要な情報は自動生成
- ◆ 複雑な構成であっても設定コストは少なく

柔軟性とセキュリティを兼ね備えたグループ通信
GSCIP (Grouping for Secure Communication for IP)

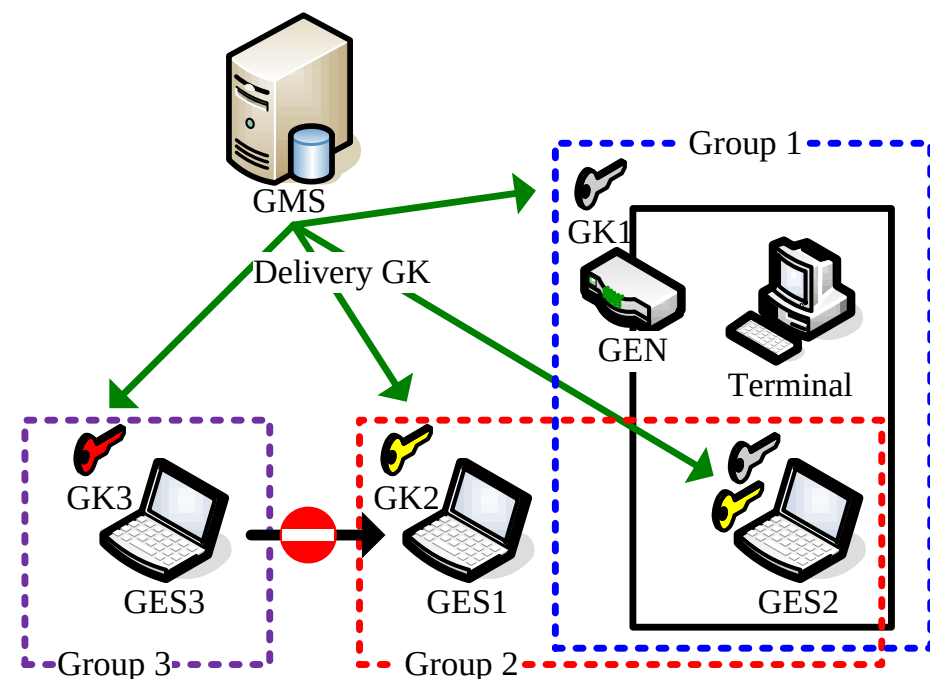
GSCIPの概要

- 同じ暗号鍵を持つ端末/サブネットを同一の通信グループと定義
 - ◆ 暗号鍵＝グループ鍵
- グループ管理サーバに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間で確実な認証
 - ≫ GEに対応するGKを配送

グループ鍵と通信グループを
1対1で対応させる

IPアドレスに依存しない
通信グループの構成



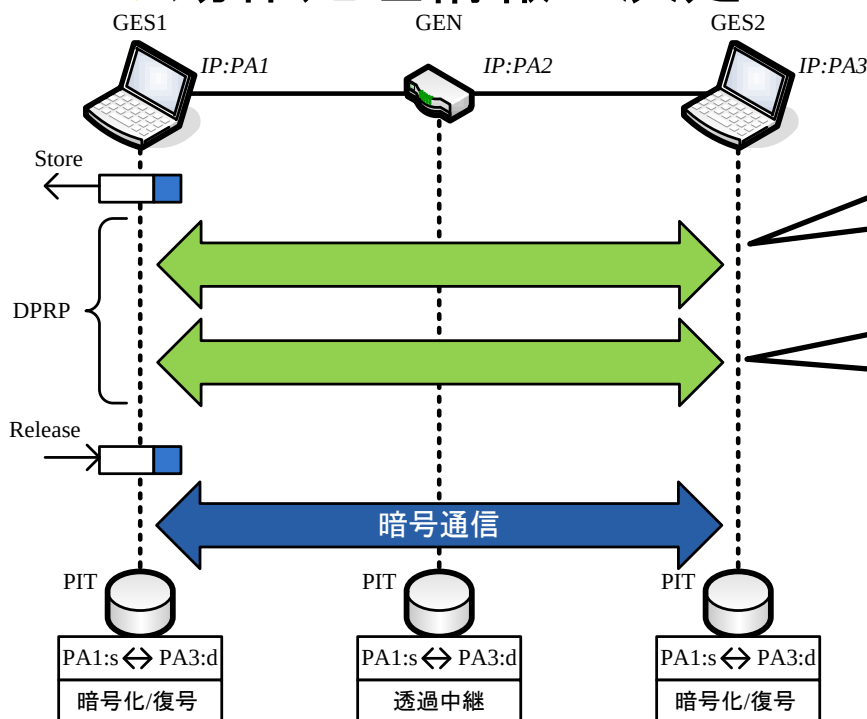
DPRP (Dynamic Process Resolution Protocol) の概要

■ 通信開始時にネゴシエーション

2往復のネゴシエーション

- ◆ 端末間の認証処理
- ◆ 通信グループ, 動作モードの情報交換
- ◆ 動作処理情報の決定

GKにより通信相手が同一グループであるかどうかを確認

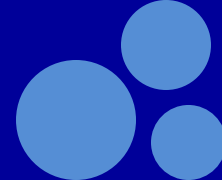


通信経路上の各GEの設定情報を取得し動作処理情報を決定

動作処理情報の通知と動作処理情報テーブルPIT (Process Information Table) の生成

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



■ 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, 通信グループ番号, 共通鍵

□ 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

□ ユーザID

□ 共通鍵



端末起動時

設定情報要求

グループ鍵, 動作モード

DPRP

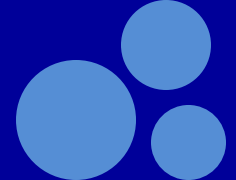
■ 端末起動時に要求

◆ 所属する通信グループの鍵情報を応答する

■ 通信開始時にDPRPネゴシエーションを実行する

◆ 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



■ 評価項目

◆ 初期管理負荷

■ 導入時

◆ ネットワーク構成変化時に発生する管理負荷

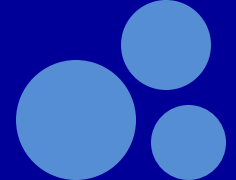
■ 端末が場所を移動した場合

◆ 通信グループのメンバ構成変化時に発生する管理負荷

■ 新しいメンバを追加した場合

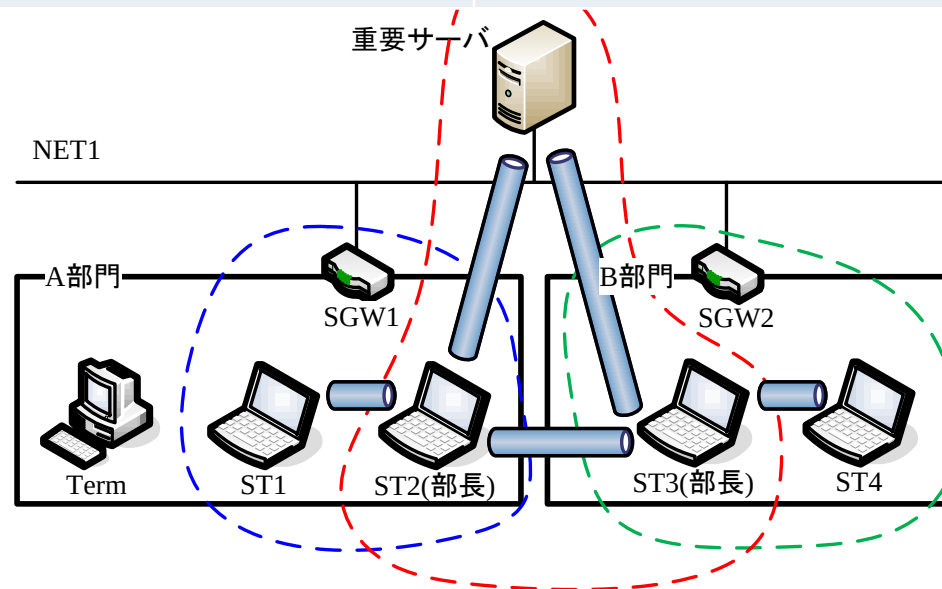
定量的評価により有効性を確認

初期管理負荷: IPsec/IKE

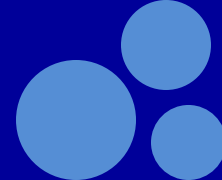


		事前共有鍵情報	セキュリティポリシー	IKE	合計
ST1, ST4		2	IPsec, Transport:14	12	28×2
ST2, ST3(部長)		6	IPsec, Transport:14 $\times$ 3	12	60×2
SGW1, STW2		2	None:8, Discard:8	12	30×2
Server		2	IPsec, Transport:14 $\times$ 2	12	44
合計					280
項目数	2	16(トンネルモードは14)		12	

構成が複雑になると
設定コストがかかる



初期管理負荷: IPsec/KINK



■ 部門, 役職毎にKDCを設置

◆ チケットを所持している端末のみSAを共有→通信

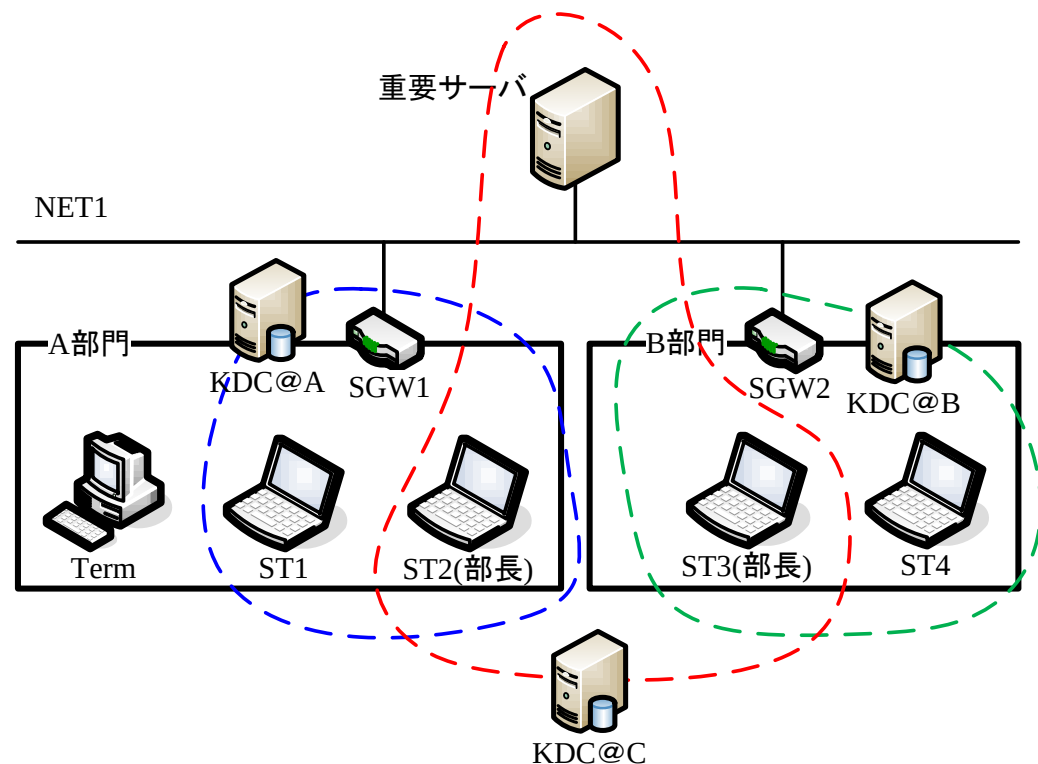
KDC@A	A部門
KDC@B	B部門
KDC@C	部長

クライアントにはIDと共通鍵だけ

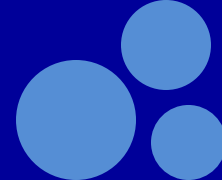
部門, 役職毎にKDCを
導入

導入によるコストは多くないが...

大・小の通信グループを
複数作る場合は
コストがかかる



初期管理負荷: GSCIP/DPRP

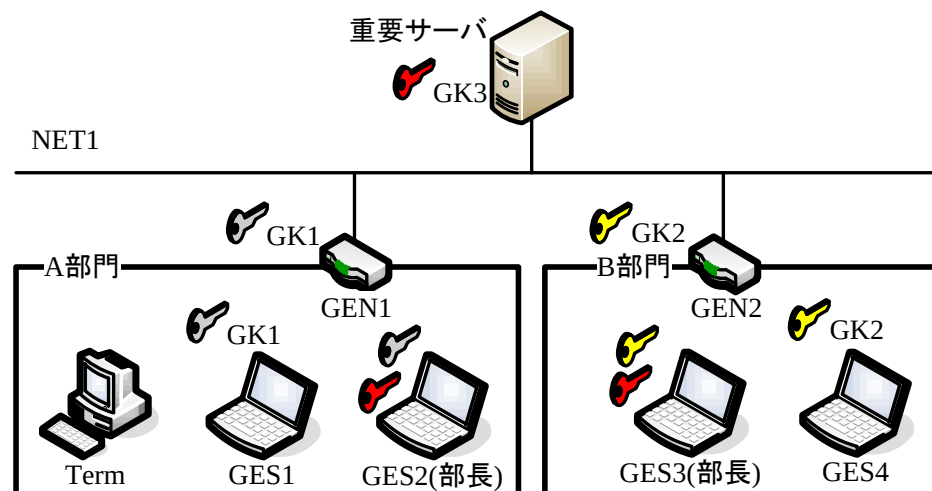


■ GMSに所属する通信グループを設定するのみ

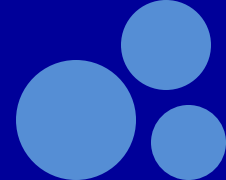
GK1	A部門
GK2	B部門
GK3	部長

	所持するGK
GES1	GK1
GES2(部長)	GK1, GK3
GES3(部長)	GK2, GK3
GES4	GK2
重要サーバ	GK3
GEN1	GK1
GEN2	GK1

	グループ鍵情報	動作処理情報	GE情報	合計
GES1, GES4	3	0	4	7
GES2, GES3	6	0	5	11
GEN1, GEN2	3	0	4	7
Server	3	0	4	7

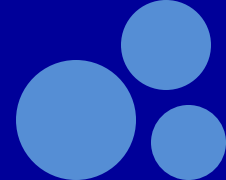


各方式の比較



	GSCIP/DPRP	IPsec/IKE	IPsec/KINK
柔軟性 (通信グループ構築の簡単さ) (端末移動)	きめ細かい通信グループの構築が行える 移動しても設定の変更は必要なし	個々に設定が必要になり多台数間の通信は難しい 場所を移動すると設定が必要になる	きめ細かい通信グループの構築は難しい 移動しても設定の変更は必要なし
管理コスト (初期管理負荷) (新しいグループ追加)	グループ鍵の定義と設定だけ	設定が多くなる	通信グループ追加毎にKDCが必要

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



■ 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

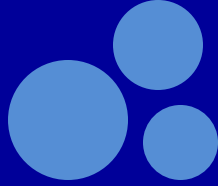
- ◆ 通信グループとグループ鍵を1対1で対応させることで、IPアドレス、構成に依存しないグルーピングが可能
- ◆ 通信に必要な情報は動的に生成し、設定による管理負荷は少ない

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

各システムは実装済み

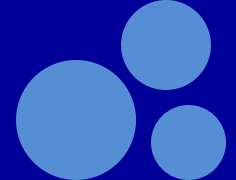
■ 今後

- ◆ 実運用による性能評価
- ◆ GMSの分散化



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)

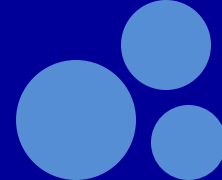
FTPダウンロード時間

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



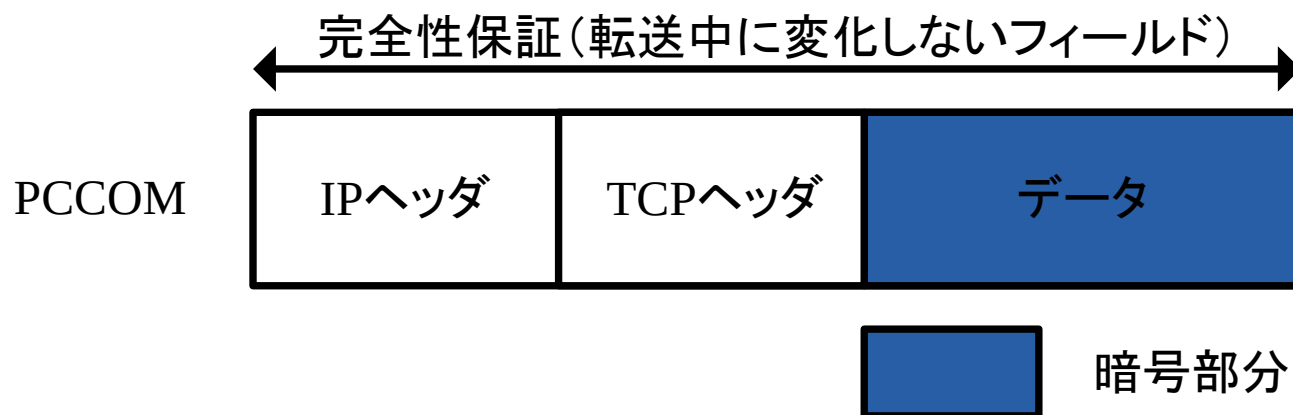
■ 完全性保証・本人性確認

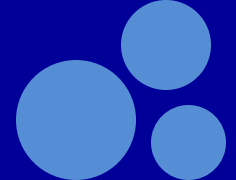
- ◆ 疑似データを用いたTCP/UDPチェックサムの独自計算により実現
- ◆ IPアドレスとポート番号の完全性は動作処理情報の検索過程で保証

■ 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

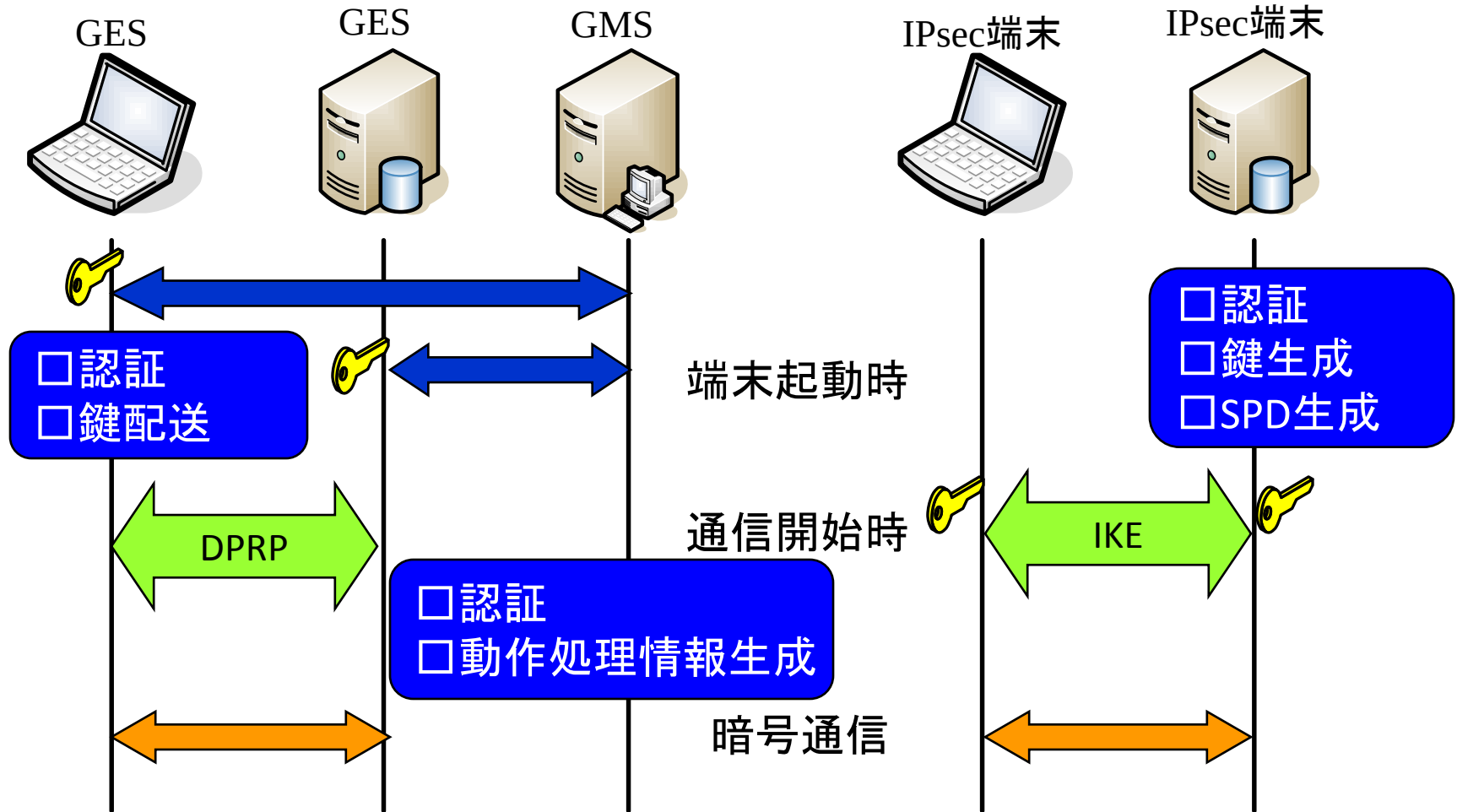
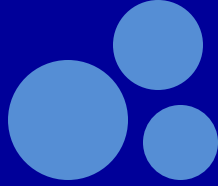




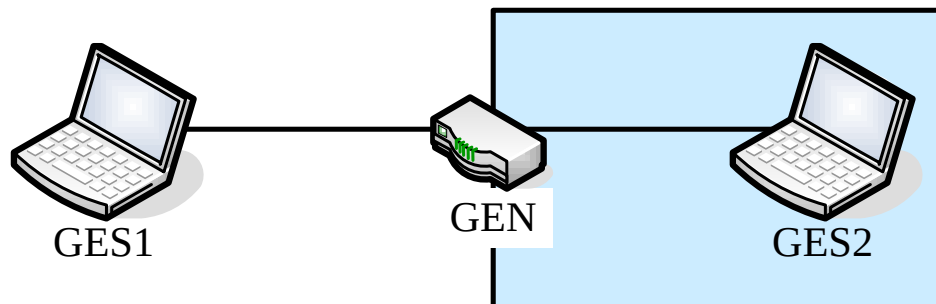
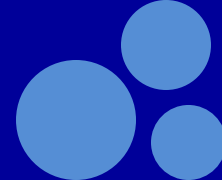
- IPsecは強靱なセキュリティ
 - ◆ インターネット空間への適用
- PCCOMはイントラネットの環境に特化
 - ◆ NATやFWと共存できるためイントラネットへの適用

	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



オーバーヘッド



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

スペック (GES1, GES2, GEN)

>> Pentium4 2.4GHz

>> 512MB

>> 100BASE-TX

IPsec/IKE (参考測定)

>> GES→IPsecクライアント

>> GEN→SGW

IKE (racoon)

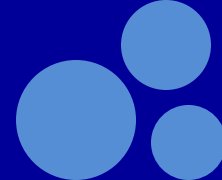
>> 事前共有鍵方式

>> ESPトランスポートモード

▪ GES1-GES2:ipsec

▪ GES1-GEN:none

▪ XXX-GEN:discard



■ 特徴

- ◆ ペイロードを暗号化したTCP

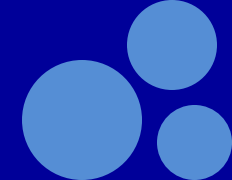
■ 長所

- ◆ 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

設定項目の詳細



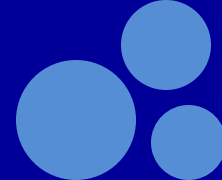
IPsec/IKE

	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		ユーザID 動作モード(OP/CL) 所属通信グループ番号
項目数	3		3

ネットワーク構成変化時



■ 端末が場所を移動した場合

GSCIP

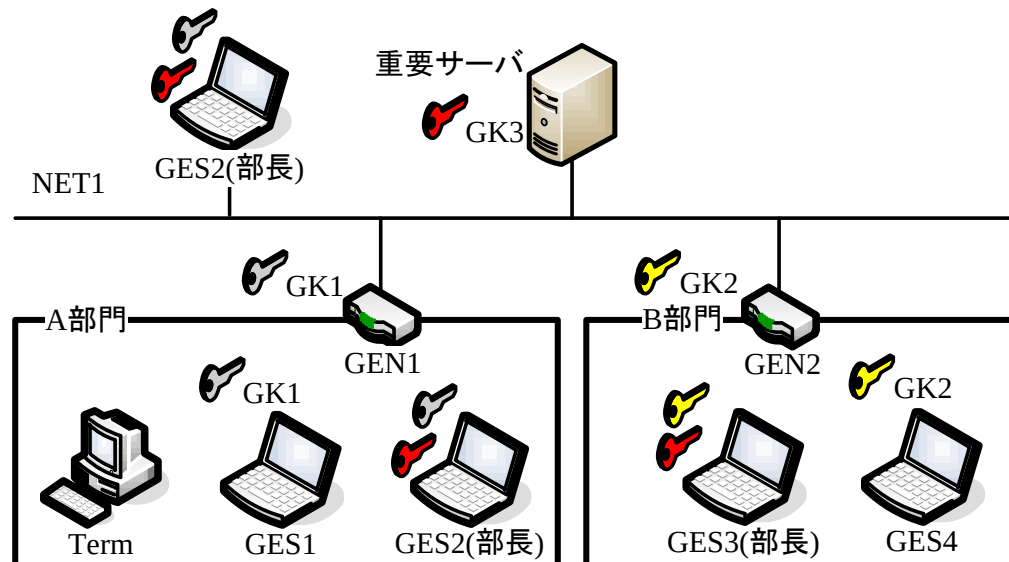
端末が移動しても、そのつどDPRPにより認証・動作処理情報を生成するため、設定作業は発生しない

IPsec/IKE

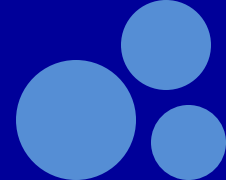
IPアドレスが変化するため、セキュリティポリシーの識別子を変更する必要がある
SGWに対してトンネルモードの設定の追加が必要

IPsec/KINK

チケットを使用してKINKを実行するため移動による設定の変更はない



通信グループのメンバ構成変化時



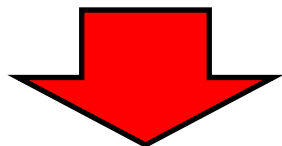
■ 新しいメンバを追加した場合

- ◆ 新規通信グループの追加
- ◆ GES5にGK2, GK4の設定
- ◆ 重要サーバにGK4の追加

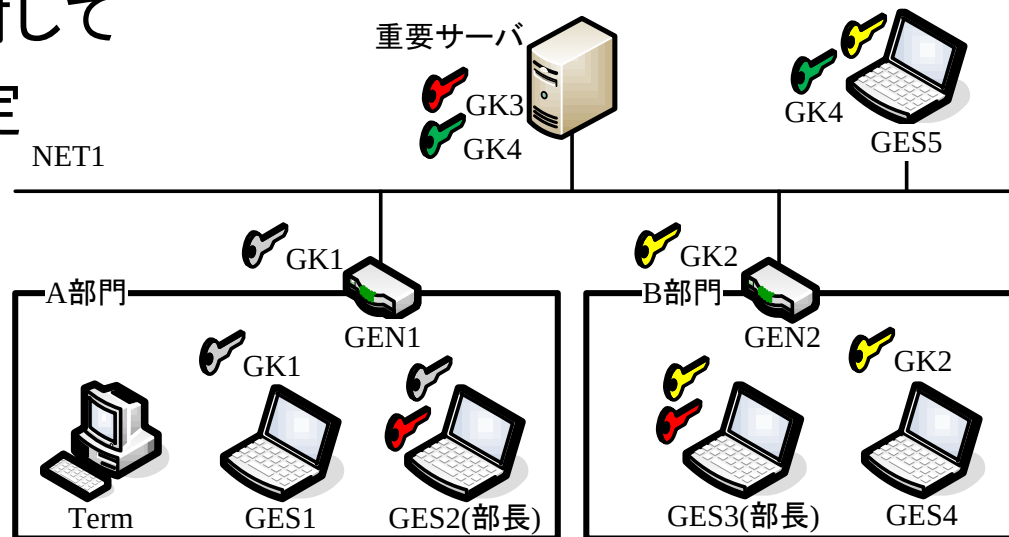
GK1	A部門
GK2	B部門
GK3	部長
GK4	特権ユーザ

■ IPsec/IKEでは・・・

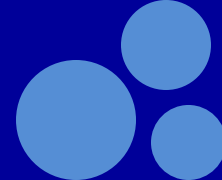
- ◆ B部門と重要サーバに対して
トランスポートモードの設定



設定が多いためコスト増



通信グループのメンバ構成変化時



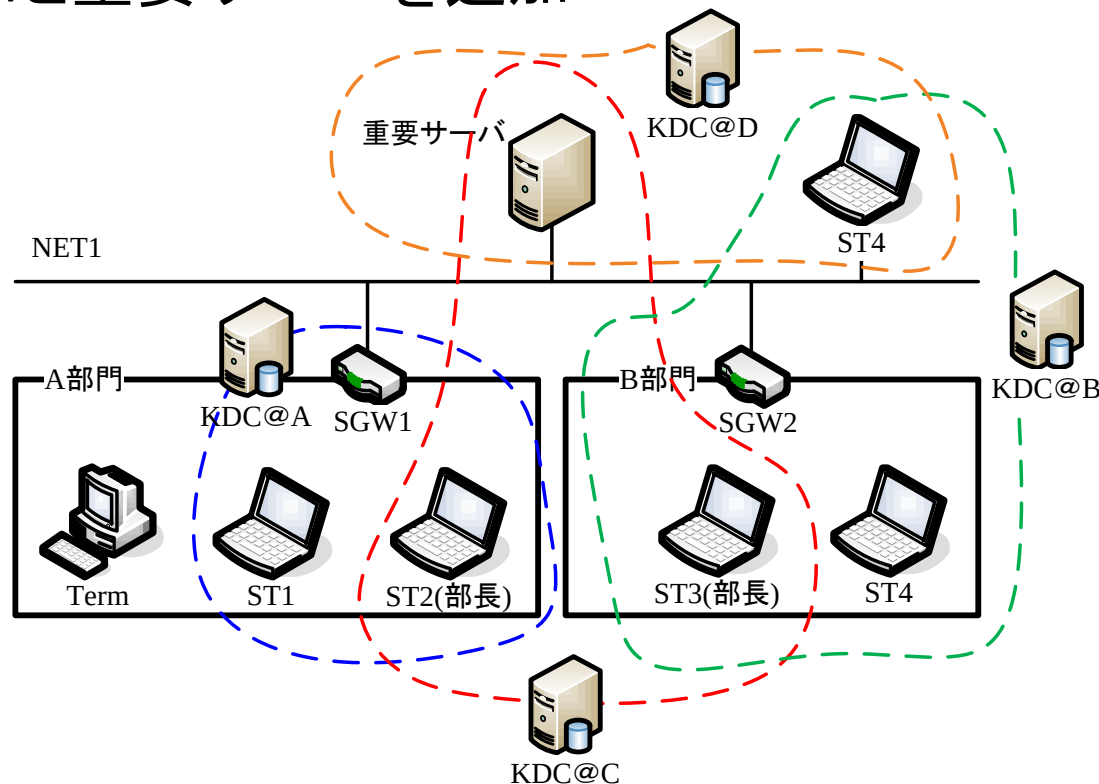
■ B部門のST4を追加

◆ KDC@BにST4を追加

◆ KDC@Dを設置し, ST4と重要サーバを追加

KDC@A	A部門
KDC@B	B部門
KDC@C	部長
KDC@D	特権ユーザ

新規グループ追加時に
コスト増



グループ鍵の更新

- 通信グループから離脱
- 一日毎に更新

