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

鈴木　秀和[†]　　渡邊　晃[‡]

†‡名城大学大学院理工学研究科　〒468-8502　愛知県名古屋市天白区塩釜口 1-501

E-mail: † m0432022@ccmailg.meijo-u.ac.jp　‡ wtnbakr@ccmfs.meijo-u.ac.jp

あらまし　イントラネットではセキュリティ対策を講じることによって，ネットワークシステムの運用・管理が難しくなる傾向がある．そこで我々はセキュリティ対策と運用管理負荷の軽減を両立できるシステム FPN（Flexible Private Network）の構築を目指している．これまでに FPN 環境下において，端末間の認証および暗号通信に必要な動作処理情報テーブルを動的に生成する動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）を提案してきた．本稿では DPRP の有効性を確認するために実装を行い，通信開始時に発生するオーバーヘッドを測定したので報告する．

キーワード　セキュリティ，プロトコル，FPN，GSCIP，DPRP

Implementation of Dynamic Process Resolution Protocol in Flexible Private Network

Hidekazu SUZUKI [†]　　Akira WATANABE [‡]

†‡ Graduate School of Science and Technology, Meijo University

1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502 Japan

E-mail: † m0432022@ccmailg.meijo-u.ac.jp　‡ wtnbakr@ccmfs.meijo-u.ac.jp

Abstract　The management of network system tends to become difficult when we improve security in intranet. Therefore, we have been developing the concept of FPN (Flexible Private Network) which is compatible with security levels and simple management. Until now, we have been proposed DPRP (Dynamic Process Resolution Protocol) which create a process information table dynamically necessary for the authentication and cryptography between terminals under the FPN environment. In this paper, we report that implement DPRP to confirm the validity of it and measure an overhead which occurs when communication starts.

Keyword　Security, Protocol, FPN, GSCIP, DPRP

1.　はじめに

今日の企業ネットワークでは，不正進入，データの盗聴や漏洩・改竄などに対する様々なセキュリティ対策が重要な課題となっている．特に組織外部からのアクセスに対しては通信の暗号化やディジタル署名による認証など，セキュリティ強度の高い技術が利用されており，ファイアウォールや IDS などと共用して，第三者による悪意のあるアクセスなどの行為を防ぐ様々な工夫がなされている．しかし企業ネットワークのセキュリティ脅威はイントラネット内部にも存在し，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 [1]．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，アクセス制御しかされていないのが現状であり，有効な対策が今後必要になると考えられる．

ネットワークセキュリティの代表的な技術としては IPsec [2] があり，現在では VPN（Virtual Private Network）を構築する手段として広く利用されている．IPsec は暗号化通信に先立ち，IKE（Internet Key Exchange）[3] によって暗号・認証に必要なパラメータを動的に生成して安全に情報の交換を行う．しかし IKE は多くの設定が必要であるという課題があり，システム構成が頻繁に変わるような環境では管理負荷が大きい．また IPsec はホスト間で利用されるトランスポートモードと，異なるネットワーク間で利用されるトンネルモードに互換性がない．そのためイントラネットのように，セキュリティドメインが階層的に構築されていたり，個人単位のセキュリティが混在するような環境に対応することが難しい．さらに，IPsec による暗号化が強靭すぎて，管理者からはどんな通信をしているのかを把握することができない．このよ

うな点から，IPsec はイントラネットにおけるセキュリティ対策の手段としては普及が進んでいないのが現状である．他のネットワークセキュリティ技術として SOCKS[4] や SSL/TLS[5] などがあるが，いずれもイントラネットの特徴に対応しつつ，セキュリティと運用管理負荷の軽減を共に満たすことは難しい．

企業ネットワークではセキュリティ向上を図ることによって，ネットワークシステムの運用や管理が難しくなる傾向がある．そこでイントラネット内のセキュリティ対策と運用管理負荷の軽減を両立できるネットワークとして FPN（Flexible Private Network）を提唱している [11]．FPN とは柔軟性とセキュリティを兼ね備えたグルーピング通信を可能とするネットワークである．この FPN を実現する方式として GSCIP（Grouping for Secure Communication for IP；ジースキップ）[7][11] という独自のセキュア通信アーキテクチャを提案している．GSCIP では，同一の共通暗号鍵を持つサブネット / ホストを通信グループとして定義する．GSCIP を構築する装置 GE（GSCIP Element）は通信相手が同一のグループに帰属しているかを確認して，どの暗号鍵で通信を暗号化するかなどを示す動作処理情報を決定する．

著者らは，上記動作処理情報を通信に先立って自動的に生成するためのプロトコルとして，動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）を提案してきた [6][7]．DPRP は各端末に事前に設定されるグループ定義情報などを，通信経路上に存在する全ての GE が互いに情報交換することで，動的に動作処理情報を生成する．DPRP を使うことによって，システムの物理的構成に変化があっても，端末の保持する動作処理情報が動的に再生成されるため，管理者の作業負担が発生しなくなるという利点がある．

本稿では DPRP の実装報告とその性能評価について述べる．以降，2 章で FPN，GSCIP，DPRP の概要，3 章で GSCIP と DPRP の実装方式，4 章で評価，5 章でまとめと今後の課題について述べる．

2. ＦＰＮとその実現方法

2.1. ＦＰＮ

FPN はサブネット単位とホスト単位のセキュリティが混在する環境に対応できる．またサブネットとホストは移動が可能で，かつホストは特定のサブネットの内外を往復できる．さらにホストは特定のサブネット内にいながら個別に他の通信グループに帰属すること（重複帰属）も可能である．FPN をイントラネット内に構築することで，様々なシステム構成に柔軟に対応でき，管理負担の増加を抑えながらセキュリティの向上を図ることができる．

2.2. ＧＳＣＩＰ

GSCIP の基本は図 1 に示すように，CE（Communication Entity）が所持する暗号鍵で通信グループを構築する．この暗号鍵をグループ鍵 GK（Group Key）という．同一の GK を所持する CE の集合を通信グループとして定義する．同一の通信グループの CE 同士は，GK を用いて暗号化通信を行う．GK はグループ管理装置 MS（Management Server）から，グループ番号とシステム全体で共通に用いられる共通鍵 CK（Common Key）と共に各 CE に配送される．

CE は GE を必ず 1 台のみ保有する．GE にはサブネットを構成するルータタイプの GEN（GE for Network），各ホストにインストールされるソフトウェアタイプ GES（GE for Software），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 for Adapter）がある．GE には通信グループ外の CE との通信を一切禁止する閉域モード（CL；Closed Mode）と，通信グループ外の CE の場合は平文での通信が可能な開放モード（OP；Open Mode）という 2 つの動作モードがある．

GSCIP では GE が所属している通信グループと設定されている動作モードの組み合わせにより，通信の可否および暗号処理の有無を決定する．そのため通信に先立ち，通信経路上の GE 間で設定されている情報を相互に交換して，

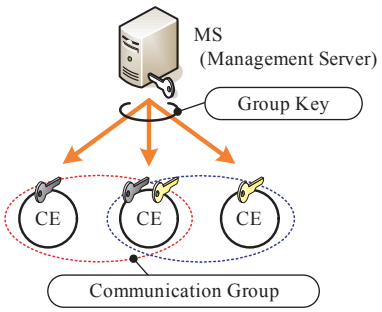


図 1　暗号鍵による通信グループの定義

通信パケットの処理内容を決定する．以後の通信は決定した情報に基づいて処理される．この情報は動作処理情報テーブル PIT（Process Information Table）として保存され，DPRP は上記 PIT を生成するために定義されたプロトコルである．

DPRP は通信に先立って実行される他に，通信中に IP アドレスが変化した場合にも実行されるが，本稿では通信に先立つ処理についてのみ記述する．

2.3. ＤＰＲＰ

図 2 に DPRP の動作を示す．図 2 はある役職 (Group2) のみが利用できるサーバ（GES2）に対して，ある部門（Group1）の役員（GES1）が通信する状況を想定している．GES2 は他のグループからの通信を拒否するために CL，GES1 は同一部門の一般端末とも通信するため OP，部門内の一般端末を保護するために GEN は CL がそれぞれ設定されている．サブネット / ホストが所属する通信グループと動作モードは予め設定されている．ここで GES1 が GES2 に通信をする場合について説明する．GES1 はデータを送信する際，自身が保持する PIT を検索する．検索の結果，GES1-GES2 間の動作処理情報がない場合，送信パケットを退避させてから DPRP ネゴシエーションを開始する．GES1-GES2 間の通信経路上に存在する GE において，ネゴシエーション開始 GE を始点 GE，始点 GE から最も離れた GE を終点 GE，両終端 GE に挟まれている GE を中間 GE と呼ぶ．

DPRP は ICMP Echo パケットをベースとした 4 種類の制御パケットを用いてネゴシエーションを行う．制御パケットは共通鍵 CK を使って暗号化される．

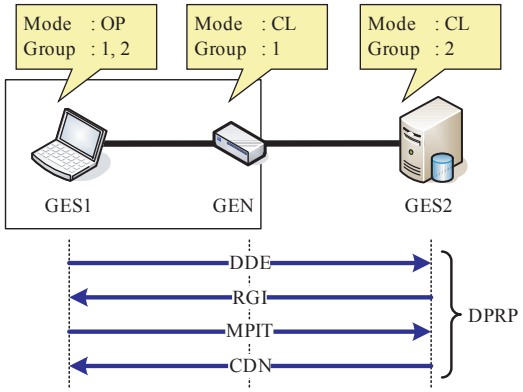


図 2　DPRP の動作

2.3.1. ＤＤＥ

始点 GE は終点 GE を決定するために DDE（Detect Destination End GE）を通信相手に向けてに送信する．DDE の宛先が一般端末の場合，受信したホストからの応答パケット ICMP ECHO REPLY を最初に受信した GE が終点 GE となる．DDE にはネゴシエーションのトリガーとなった通信パケットの送信元 / 宛先 IP アドレスとポート番号，プロトコルタイプの情報が設定される．

2.3.2. ＲＧＩ

DDE によって決定した終点 GE は GES1 に RGI（Report GE Information）を送信する．RGI には自端末に設定されている動作モード，通信グループ情報，認証情報 aID などの情報が設定される．ここで aID は乱数で，PIT に一時的に登録しておき，RGI 以降の DPRP 制御パケットを認証するために利用される．

中間 GE が RGI を受信すると，終点 GE と同様に自端末の設定情報などを RGI に追加する．始点 GE が RGI を受信すると，通信経路上の全 GE の情報を取得できる．始点 GE はこれらの情報を総合的に判断して，全ての GE の動作処理情報を決定する．

2.3.3. ＭＰＩＴ

始点 GE は通信経路上の各 GE に決定した動作処理情報を伝えるため，動作処理情報を PIT に登録してから MPIT（Make Process Information Table）を終点 GE に送信する．MPIT には決定した動作処理情報，RGI で受信した aID などの情報が設定される．各 GE が MPIT を受信すると，動作処理情報と aID を取得する．ここで取得した aID と PIT に登録しておいた aID を比較して認証を行い，正常なら動作処理情報を PIT に登録する．

2.3.4. ＣＤＮ

終点 GE は各 GE に PIT が生成され，DPRP ネゴシエーションが完了したことを通知するために，CDN（Complete DPRP Negotiation）始点 GE に送信する．始点 GE が CDN を受信することで，退避していた通信パケットを元に戻して通信が再開される．以後の通信は動作処理情報に基づいて処理される．

3. ＤＰＲＰの実装

DPRP は IP 層に実装される．GSCIP を実現

するモジュール群のことを GPACK と呼び，DPRP はその一部を構成する．OS には IP 層の情報が豊富な FreeBSD を選択した．GPACK の処理はカーネルレベルとアプリケーションレベルに分けられる．図 3 に GPACK の実装概要を示す．IP 層の入出力関数 ip_input( )，ip_output( ) から GPACK を呼び出して処理を行う．GPACK で処理された通信パケットは IP 層の元の場所に戻され，既存の IP 層の処理は GPACK の影響を一切受けない．図 4 に示すように，GPACK は受け取った通信パケットの種類を判別してから，適切なモジュールを実行する．

送信 / 受信パケットが TCP/UDP パケットの場合，まず PIT の検索を行う．動作処理情報が存在した場合，“暗号化 / 復号” なら暗号モジュールによりパケットを暗号処理する．“処理なし” ならそのまま IP 層へ戻す．“破棄” と “作成中” のフラグが設定されていたら IP 層で破棄する．一方，動作処理情報が存在しない場合，DPRP モジュールに処理が渡される．DPRP は DDE を作成して ip_output( ) に渡す．その後，ネゴシエーションのトリガーとなった UDP/TCP パケットを退避する．DHCP や RIP など一部の TCP/UDP パケットについては GPACK の処理を行わない．これは IP アドレスの割り当てや，ルーティングテーブル作成など，TCP/IP ネットワークにおける重要な機能に影響を与えないためである．

ICMP パケットの場合，さらに DPRP 制御パケットか否かを判別する．通常の ICMP パケットなら GPACK で処理を行わずに IP 層へ戻す．DPRP 制御パケットなら DPRP モジュールにより処理が行われる．

一方，アプリケーションレベルでは DPRP によって作成される PIT の管理を行う．一定時間参照されていない PIT レコードがあればホスト間の通信が行われていないと判断して，システムコールにより PIT レコードを削除する．削除対象となる時間は約 5 分とした．

4. 性能測定と評価

4.1. 性能測定

図 5 のようなテスト環境を用いて，GES1 が GES2 に FTP による接続を行う場合の DPRP の性能を測定した．ホストの性能を表 1 に示す．測定項目は (1)GPACK および DPRP モジュール

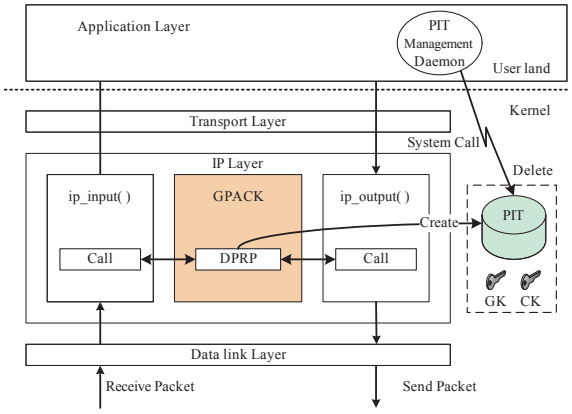


図 3　GPACK の実装概要

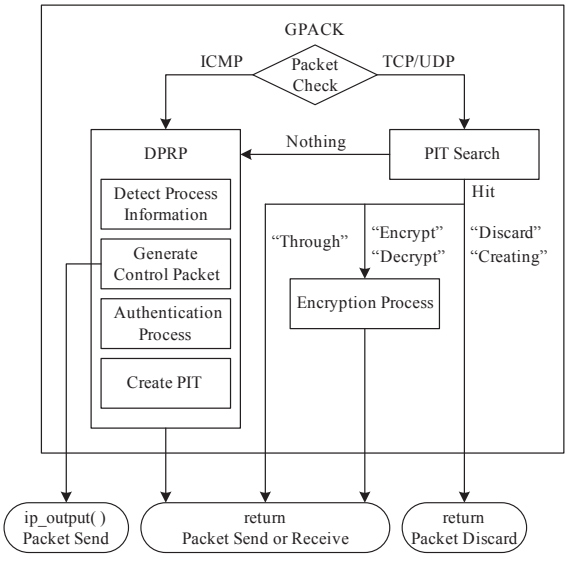


図 4　GPACK の処理フロー

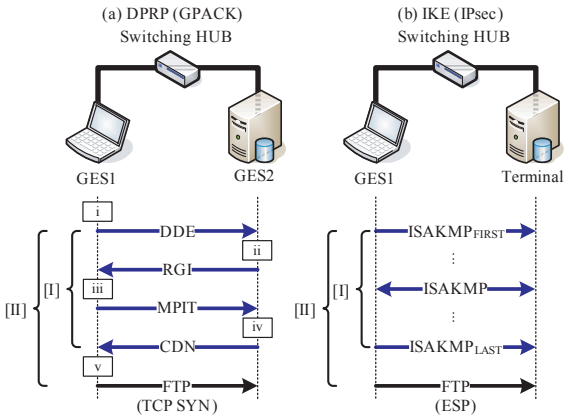


図 5　測定ポイント

の内部処理時間，(2)DPRP ネゴシエーションのオーバーヘッドである．各 GE が保持する GK は設定済みとする．

参考のために，同一条件下における IKE の処理時間も計測した．IPsec は FreeBSD に実装されている KAME および IKE デーモンの

表 1　実験端末スペック

	GES1 / GES2 (Terminal)
CPU	Pentium4 2.4GHz
RAM	512MB
NIC	100BASE-TX
OS	FreeBSD 5.2.1-RELEASE

表 2　IKE 設定パラメータ

Phase1 Exchange	Main mode
Authentication Method	Pre-Shared Key
Encryption Algorithm	3DES-CBC
Hash Algorithm	SHA-1
Diffie-Hellman Group No.	1 (MODP 768bit)

racoon を使用し，ESP トランスポートモードで通信させた．IKE で使用したパラメータの設定を表 2 に示す．

4.1.1　モジュールの内部処理時間

内部処理時間の測定には Pentium Time Stamp Counter を用いた．図 5(a) に示した [i] ～ [v] における GPACK，DPRP 各モジュールの処理時間と DPRP モジュール内における暗号処理時間を表 3 に示す．

4.2.1　ネゴシエーションのオーバーヘッド

ネゴシエーションによるオーバーヘッドを測定するために，Ethereal でパケットの送受信時間を測定した．測定対象は DPRP では図 5(a) に示す DDE ～ CDN 間 [I] と，DDE ～ TCP SYN 間 [II] である．一方，IKE では図 5(b) に示す $ISAKMP_{FIRST}$ ～ $ISAKMP_{LAST}$ 間 [I] と，$ISAKMP_{FIRST}$ ～ ESP 間 [II] である．それぞれの測定結果を図 6 に示す．

表 3　GES1-GES2 間における内部処理時間

		GPACK	DPRP	Encryption
GES1	[i]	11.77	50.99	14.54
	[iii]	9.58	37.45	5.18
	[v]	21.96	14.54	1.88
GES2	[ii]	9.92	51.24	15.85
	[iv]	7.27	26.90	4.69

単位：[usec]

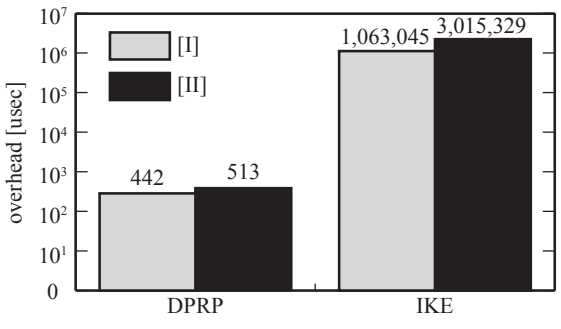


図 6　DPRP と IKE のオーバーヘッド

4.2　評価

表 3 より GES1-GES2 間のネゴシエーション全体の内部処理時間は 241.62[usec] となり，処理を高速に行うことが確認できた．また DPRP 制御パケットの暗号 / 復号処理は，DPRP モジュール処理時間の 25% 程度で行えた．DPRP ネゴシエーションは高速かつ安全に行うことができたといえる．図 6 よりネゴシエーションが完了してから 71[usec] 後に通信を開始していた．これはネゴシエーションのトリガーとなった TCP パケットを退避しておき，ネゴシエーション完了後に退避パケットを送信したためである．よって TCP の再送処理は発生せず，通常の通信は GPACK 未実装時とほとんど変わらない速度を実現できた．

参考のため計測した IKE は，ネゴシエーション時に通信を暗号化するための共有暗号鍵を Diffie-Hellman アルゴリズムにより生成する．鍵生成時に公開鍵演算の処理が含まれるため，ネゴシエーションに約 1 秒ほどかかった．また IPsec/IKE ではネゴシエーションのトリガーとなったパケットを破棄するため，RTT の初期値である約 3 秒後に暗号通信が始まる．

IPsec/IKE が主に使われている VPN（リモートアクセス）のように，インターネット上にいる多数のリモートホストとセキュリティゲートウェイ間で共有秘密鍵を一括して変更することは現実的でない．そのため，インターネットではネゴシエーション時に共有秘密鍵を生成する IKE が有効である．イントラネットでは管理者が全てのホストを管理しているため，GSCIP のように共有秘密鍵に対応する GK を MS で定期的に更新して，該当する GE に一括して配布することが可能である．GE と MS 間の認証は PKI の仕組みをそのまま利用し，GSCIP に含まれるプロトコル SPAIC（Secure Authentication with IC card protocol）[8] により安全に GK が配送される．

DPRP および IKE ネゴシエーションを行うために必要な設定項目を表 4 に示す．IKE は様々なアルゴリズムを組み合わせることで，安全性と汎用性を実現しているため，多くの設定が必要になる．一方, DPRP では動作モードやグループ番号など簡単な設定だけでよいため，イント

表 4　DPRP と IKE に必要な設定項目

DPRP	IKE	
・User ID	・Traffic Information	・Exchange Mode (Main / Aggressive)
・GE Mode (OP/CL)	・Protocol (ESP or/and AH)	・Authentication Algorithm (HMAC-MD5/SHA-1, ...)
・Group No.	・IPComp (on / off)	・Encryption Algorithm (3DES, Towfish, AES, ...)
・GK	・Mode (Transport / Tunnel)	・Compression Algorithm (DEFLATE)
	・Pre-Shared Key	・Hash Algorithm (MD5, SHA-1)
	・Life Time	・Diffie-Hellman Group No. (1, 2, 5)　etc...

ラネットにおける導入の容易さや，FPN の重要な目的である運用管理負荷の軽減を達成するのに適しているといえる．

これらのことから，インターネットではセキュリティが強靭な IPsec/IKE を，イントラネットでは管理負荷が少ない GSCIP を適用するのが有効であると考えられる．

5.　まとめ

本稿では動的処理解決プロトコル DPRP の実装を行い，評価を行った．その結果，DPRP は高速かつ安全に通信相手を認証することが可能で，暗号通信に必要な動作処理情報を動的に生成できたことを確認できた．

DPRP を応用してホスト間で必要な情報を DPRP 制御パケットに含めることで，様々な処理を行うことが可能になる．この一例として GSCIP に含まれる Mobile PPC（Mobile Peer-to-Peer Communication protocol）[9] や NATF（NAT Free Protocol）[10] がある．Mobile PPC は移動前後の IP アドレスなどの情報を交換して，IP 層でアドレス変換することで移動した場合もコネクションを維持するプロトコルであり，現在実装している．NATF はグローバルアドレス環境から動的に NAPT テーブルを生成し，プライベートアドレス環境に対して自由に通信が行えるプロトコルである．今後はこれらのプロトコルや装置を実装して，FPN の実現を目指す．さらに FPN（GSCIP）と VPN（IPsec）の連携について検討する予定である．

謝辞

本研究は，栢森情報科学振興財団の助成により行われた．

文献

[1] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, “2004 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute, Jun. 2004.

[2] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC2401, Nov. 1998.

[3] D. Harkins and S. Carrel, “The Internet Key Exchange (IKE)”, RFC2409, Nov. 1998.

[4] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas and L. Jones, “SOCKS Protocol Version 5”, RFC1928, Mar. 1996.

[5] T. Dierks and C. Allen, “The TLS Protocol, Version 1.0”, RFC2246, Jan. 1999.

[6] 渡邊晃，井手口哲夫，笹瀬巌，“イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理解決プロトコルの提案”，信学論（D-I），vol. J84-D-I，No. 3，pp. 269-284，Mar. 2001.

[7] 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”，情処研報，2004-CSEC-26，pp. 259-266，Jul. 2004.

[8] 保母雅敏，前羽理克，渡邊晃，“非接触 IC カードを利用した重要情報の配送手段に関する提案”，CSS2004，vol. II，pp. 373-378，Oct. 2004.

[9] 竹内元規，渡邊晃，“モバイル端末の移動透過性を実現する Mobile PPC の提案”，情処技報，2004-MBL-030，pp. 17-24，Sep. 2004.

[10] 加藤尚樹，渡邊晃，“アドレス空間の違いを意識しない通信方式 NATF の提案”，WiNF2004，pp. 222-225，Sep. 2004.

[11] Flexible Private Network, Watanabe Lab. , Department of Information Engineering, Meijo Univ. , http://www-is.meijo-u.ac.jp/~watanabe/research/fpn1.html.

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

名城大学大学院　理工学研究科
鈴木　秀和　　渡邊　晃

名城大学

発表の概要

大要

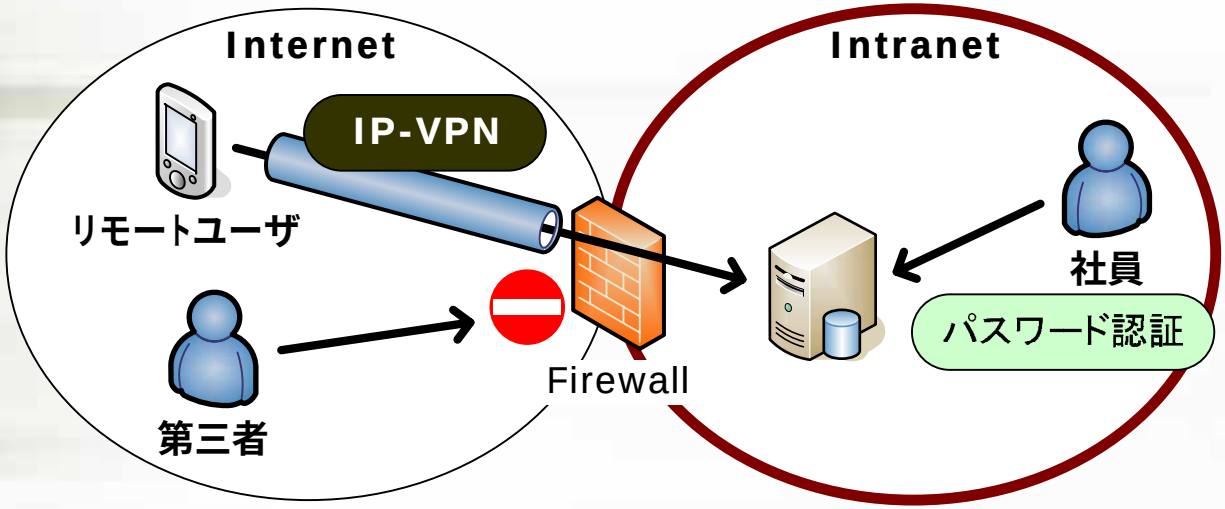
» イントラネットのセキュリティ対策の一方式

発表の流れ

1. フレキシブルプライベートネットワークの研究背景
2. 動的処理解決プロトコルDPRPの概要と実装について
3. 性能の測定結果と評価
4. まとめ

研究背景

企業ネットワークのセキュリティ対策は重要な課題



外部

- 暗号通信
- ディジタル署名による認証
- ファイアウォール
- IDS

内部

- パスワード認証
- ファイルのパーミッション

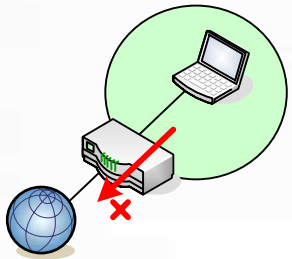
研究背景

内部セキュリティは外部と比べて十分でない

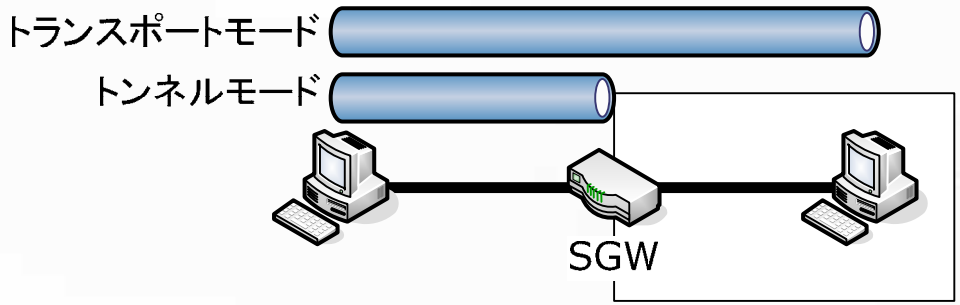
» 情報漏洩など内部犯罪が増加

➔ネットワークセキュリティ（IPsec）を導入すると

設定項目が
多くて難しい



NAPTとの
相性問題



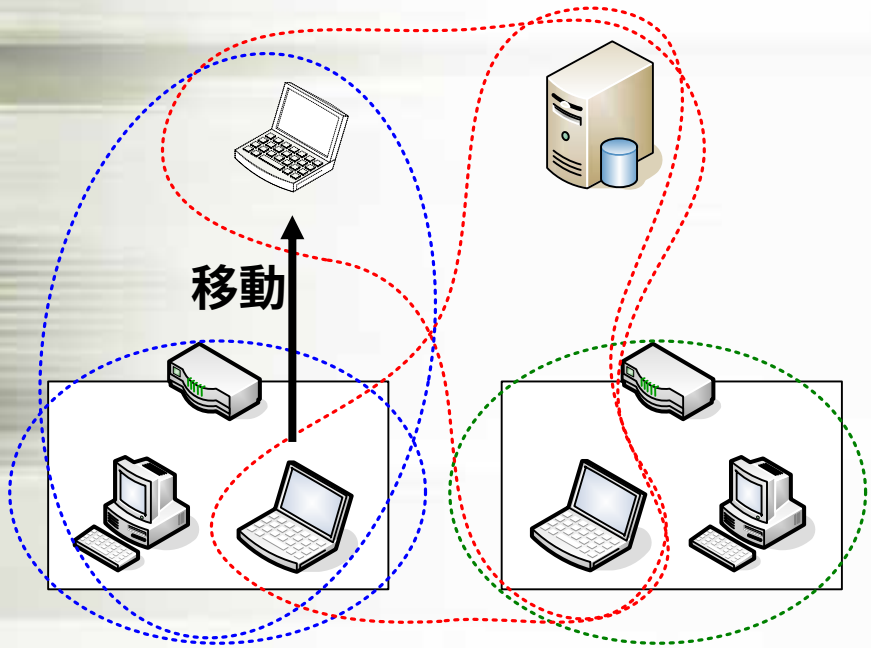
部門（サブネット）単位や個人（ホスト）
単位のセキュリティが混在する環境
に対応するのが難しい

イントラネットのセキュリティ技術として利用するのは難しく，普及していないのが現状

FPN (Flexible Private Network)

フレキシブルプライベートネットワーク

» 柔軟性とセキュリティを兼ね備えたグルーピング通信



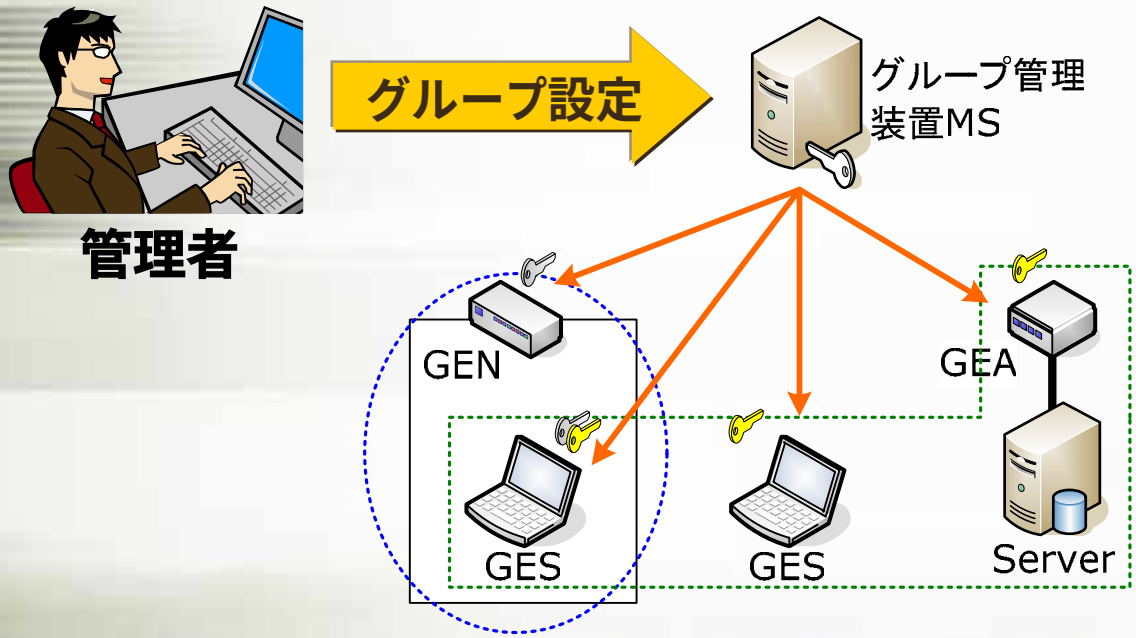
- ホストは特定のサブネットにいながら個別に他のグループに帰属可能
- 同一グループ内の通信は暗号化
- 動作モードの設定により違うグループからのアクセスを拒否することも可能
- サブネット/ホストは自由に移動可能
- 移動しても定義されたグループは不変

様々なシステム構成に柔軟に対応でき，管理負荷の増加を抑えながらセキュリティの向上が可能

GSCIP (Grouping for Secure Communication for IP)

FPNを実現するためのセキュア通信アーキテクチャ

- 同じ共通暗号鍵を持つサブネット/ホストを同一の通信グループとして定義　(共通鍵＝グループ鍵GK)
- MSに予めグループ番号とグループ鍵を設定
  - GE-MS間は公開鍵認証を行って各情報を配送



GE (GSCIP Element)

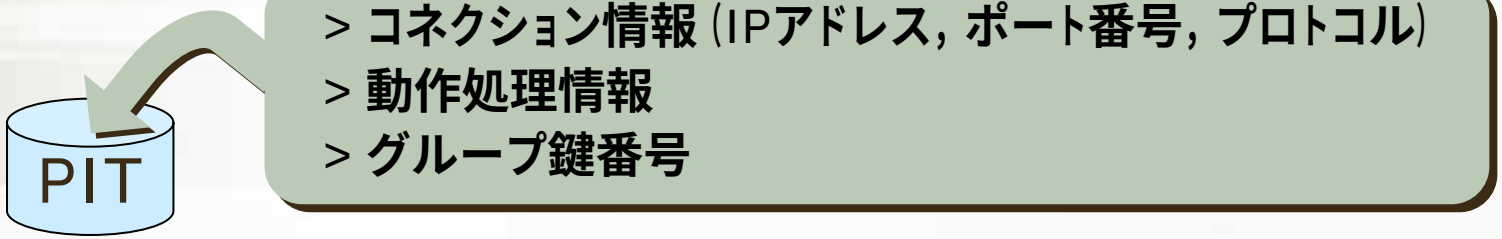
- **GES** (Software型)
  - > クライアントに実装
- **GEN** (Network型)
  - > ルータとして動作
- **GEA** (Adapter型)
  - > ブリッジとして動作

DPRP (Dynamic Process Resolution Protocol)

動的処理解決プロトコル

» 通信に先立ち通信経路上の全てのGEが連携して
ネゴシエーションを実行

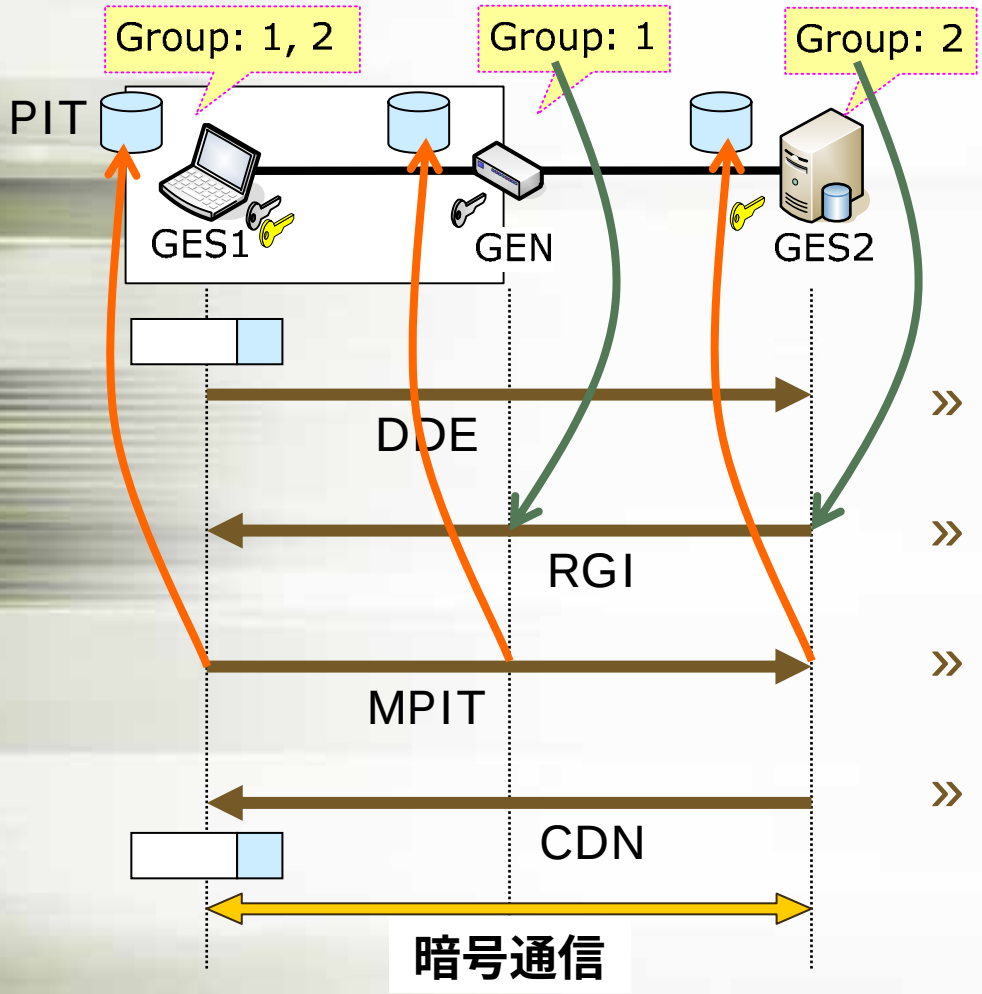
- グループ番号，動作モードなどの情報を交換
→動作処理情報の決定
  - > 「暗号」「復号」「処理なし」「破棄」
- 決定した情報を格納する動作処理情報テーブル
PIT (Process Information Table) **の生成**



» ICMPをベースとした4種類の制御パケットで実行

- 制御パケットはシステム共通鍵CKで暗号化

DPRP (Dynamic Process Resolution Protocol)



1. PIT検索 ➔あり→4.へ
   ➔なし→2.へ
2. パケットを退避してDPRP開始
3. 退避していたパケットを戻す
4. PITの情報に基づいて通信

» **DDE** (Detect Destination End GE)
- 終点GEの決定

» **RGI** (Report GE Information)
- 始点GEの決定, 各GEの情報伝達

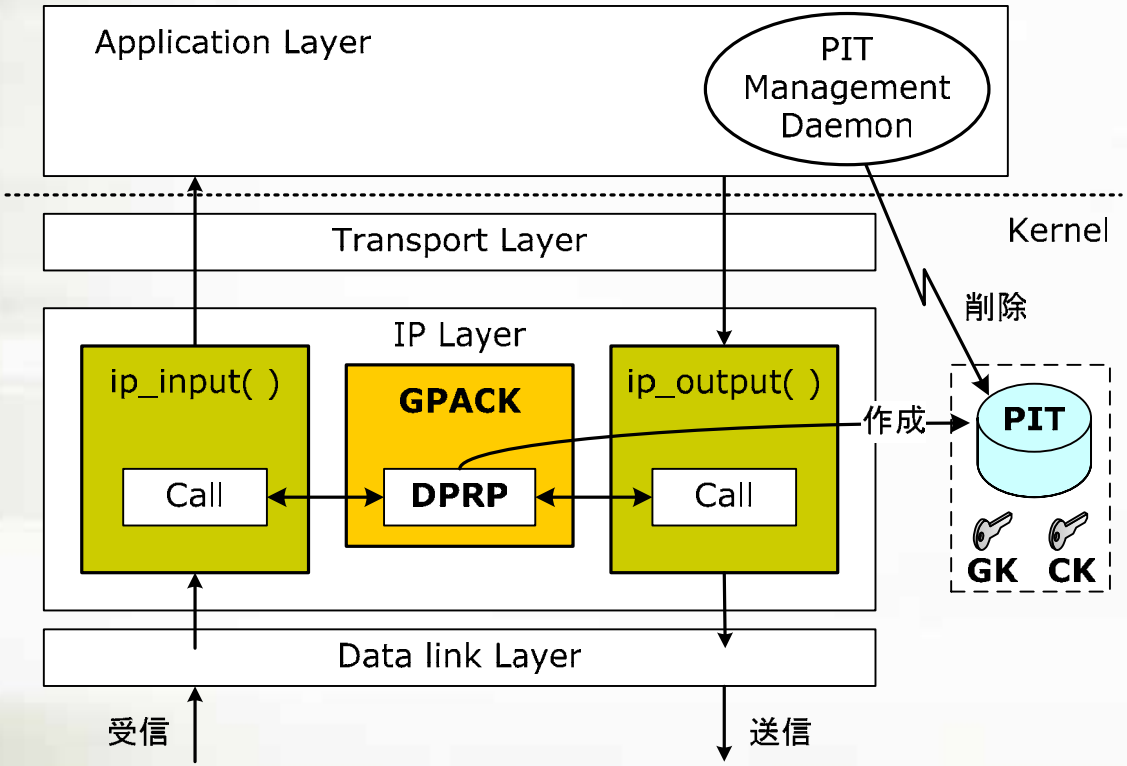
» **MPIT** (Make Process Information Table)
- 動作処理情報の伝達, PITの作成

» **CDN** (Complete DPRP Negotiation)
- ネゴシエーション完了通知

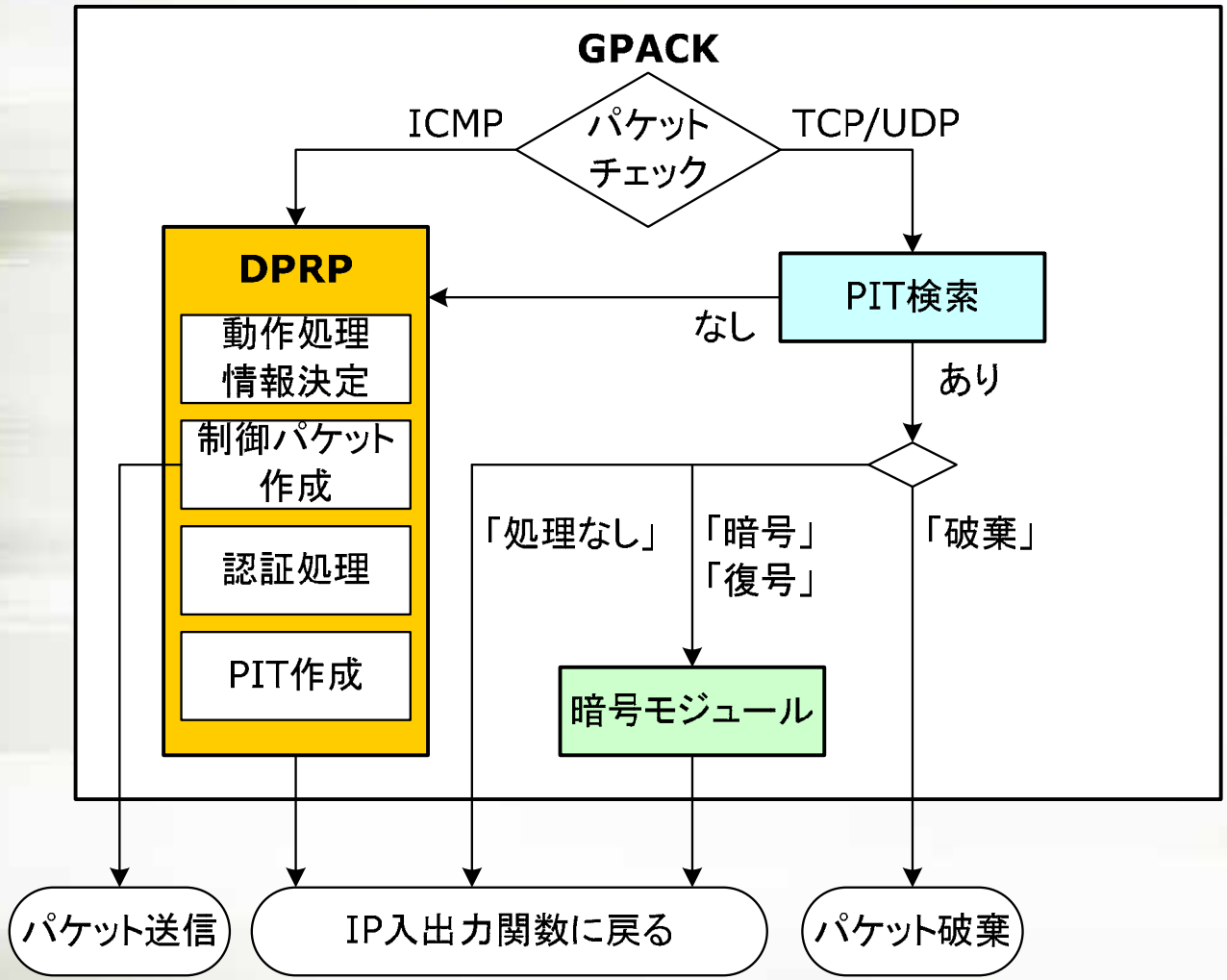
DPRPの実装

GPACK (GSCIP Package)

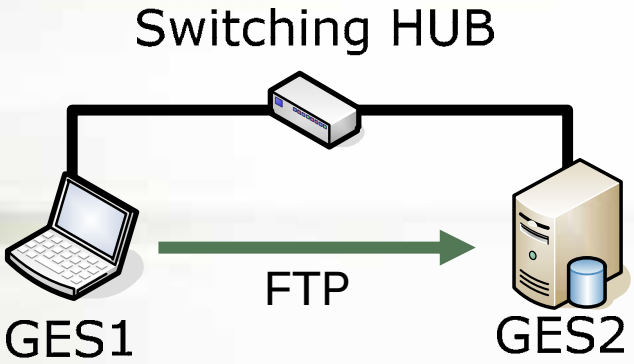
- » GSCIPを実現するモジュール群 (DPRPを含む)
- » FreeBSDのIP層に実装



GPACKの処理フロー



性能測定



CPU	Pentium4 2.4GHz
RAM	512MB
NIC	100BASE-TX
OS	FreeBSD 5.2.1-R

実験概要

» GES1がGES2にFTP接続する

測定項目

(1) GPACKとDPRPモジュールの内部処理時間

(2) DPRPネゴシエーションのオーバーヘッド

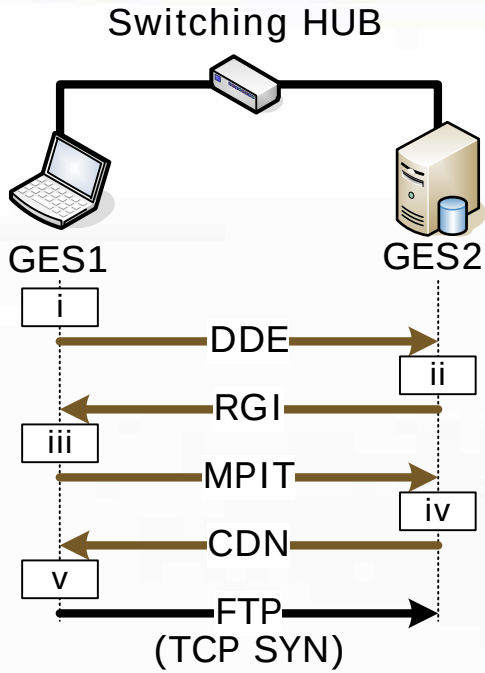
条件

» 両端末は既に同一のグループ鍵，システム共通鍵を保持

測定結果 (1) 内部処理時間

		DPRP(+GPACK)	暗号処理
GES1	[i]	62.76	14.54
	[iii]	47.03	5.18
	[v]	36.50	1.88
GES3	[ii]	61.16	15.85
	[iv]	34.17	4.69

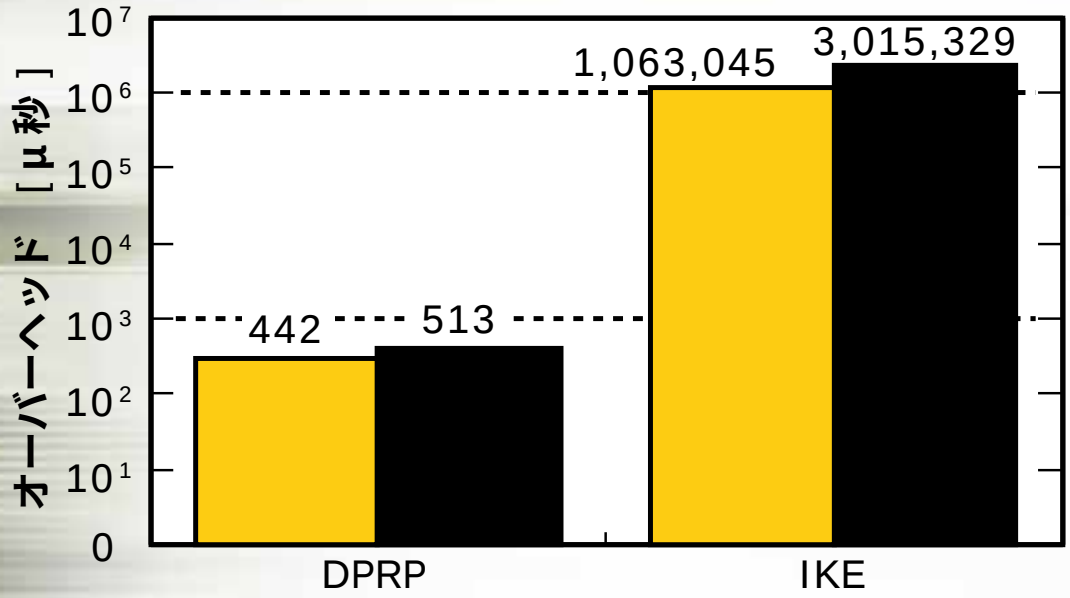
単位：μ秒



- ネゴシエーション全体の内部処理時間＝241.62μ秒
- 暗号処理時間＝DPRPモジュール処理の約25％

一般の通信に影響を与えずに，認証とPIT生成が行える

測定結果 (2) オーバーヘッド



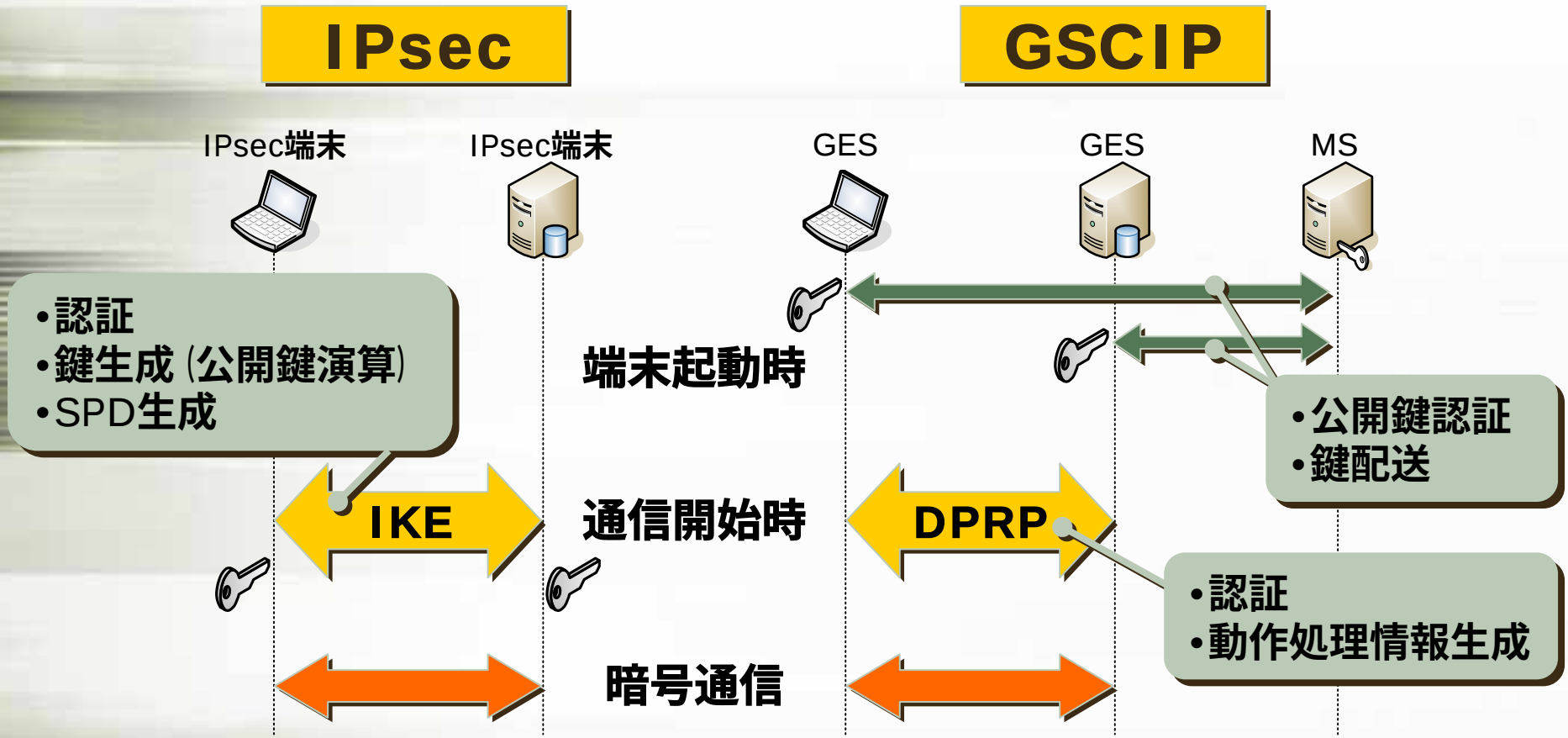
[I] ネゴシエーションにかかった時間

[II] ネゴシエーション開始から実際の通信が開始するまでにかかった時間

- DPRPではTCPの再送処理は発生しない
  - トリガーパケットを破棄せず退避したため
- IKEではネゴシエーションに約1秒
  - RTTの初期値 (=3秒後) に暗号通信を開始

評価 ～GSCIPとIPsecの比較～

アーキテクチャの違い



評価　～設定項目～

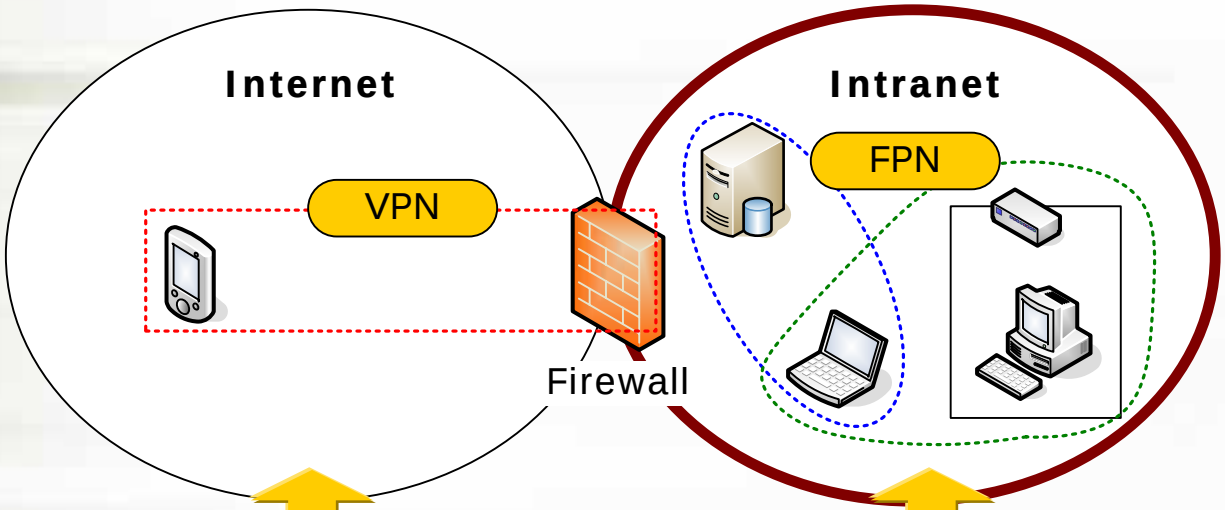
GSCIP/DPRP	IPsec/IKE	
➢ユーザID	➢トラフィック情報	➢鍵交換モード
➢動作モード	➢適用プロトコル	➢認証アルゴリズム
➢グループ番号	➢IPペイロード圧縮	➢暗号アルゴリズム
➢グループ鍵GK	➢動作モード	➢圧縮アルゴリズム
	➢事前共有秘密鍵	➢ハッシュアルゴリズム
	➢有効時間	➢DHグループ　etc...

» IKEは様々なアルゴリズムに対応➔安全性と汎用性
» DPRPは簡単な設定➔ユーザがわかりやすい

FPNの重要な目的である運用管理負荷の軽減を実現でき，導入・利用も比較的容易

評価　～総括～

IPsecとGSCIPの適用範囲のすみわけが可能



IPsec

- セキュリティが強靭
- 高い汎用性を実現

GSCIP

- イントラネットの特徴に対応
- 管理負荷軽減を実現

まとめ

動的処理解決プロトコルDPRPの実装と評価

- DPRPは高速かつ安全に
  - 通信相手の認証
  - 動作処理情報の動的生成
- イントラネットにおけるセキュリティ対策として有効

今後の課題

- DPRPの拡張→FPNの実現へ
- GSCIPとIPsecの連携について