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

鈴木　秀和[†1]　竹内　元規[†2]　加藤　尚樹[†3]　増田　真也[†4]　渡邊　晃[†5]
名城大学大学院理工学研究科

A proposal of Secure Communication Architecture GSCIP realizing Flexible Private Network

Hidekazu Suzuki[†1]　Motoki Takeuchi[†2]　Naoki Kato[†3]　Shinya Masuda[†4]　Akira Watanabe[†5]
Graduate School of Science and Technology, Meijo University

1. はじめに

ネットワーク技術の進歩に伴い，あらゆる情報端末がネットワークに接続され，いつでもどこからでも様々なサービスを利用できるユビキタスネットワークの構築に向けて，様々な研究開発が行われている．ユビキタス社会では，あらゆるユーザが簡単にネットワークを利用でき，かつ安全な通信が保証されなければならない．また情報家電製品の普及や情報端末のさらなる高性能化に伴って，今後インターネットからホームネットワークに簡単にアクセスしたい，移動しながら通信をしたいという要求が高まると考えられる．

グローバルアドレス空間からプライベートアドレス空間にアクセスするには，VPN（Virtual Private Network）を構築して，リモートアクセスを行うことが企業業務を中心に広く利用されている．VPN を構築するために利用される IPsec [2]は，暗号化通信に先立ち，IKE（Internet Key Exchange）[3]によって暗号・認証に必要な情報を動的に生成して，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ことや，設定パラメータに通信相手を IP アドレスで指定する場合がある．そのため，端末が移動した際に設定項目を変更する必要が生じることや，専門知識を持たない一般ユーザが気軽に IPsec を利用することは難しい．またホームネットワーク内にアクセスするために NAT，ファイアウォール（以下 FW）を通過する必要がある．IPsec では NAT Traversal [6]により NAT/NAPT の通過を実現しているが，UDP ヘッダによる ESP のカプセル部分が完全性保証の範囲に含まれていない，ヘッダの追加によるオーバヘッドやフラグメントが発生するという課題が残されている．

移動しながら通信したいという要求に対して，移動透過通信を実現する代表的な技術として Mobile IP [4]がある．Mobile IP は移動ノードの位置を管理し，かつプロキシとして動作するホームエージェントを導入する．Mobile IP は完成された技術であるが，通信経路の冗長やヘッダの追加によるオーバヘッド，ホームエージェントという特殊な装置が必要であることや，ホームエージェントが複数設置できないことによる一点障害などの問題が指摘されている．

ユビキタスネットワークではホームネットワークへのアクセスと移動通信における要求が同時に満たされ，かつ様々な環境に対応できることが望まれる．IPsec と Mobile IP を併せるなどして，セキュアな移動通信を行う様々な研究が行われている[7][8]が，両者の要求を同時に満たすことや利用する環境に柔軟に対応することは難しい．さらにインターネットからホームネットワークにアクセスする場合，サブネット単位のセキュリティと個人単位のセキュリティを同時に守る必要もある．そこで我々は必要最低限のセキュリティを確保し，かつ端末があらゆる空間を自由に移動することが可能なネットワークを FPN（Flexible Private Network）[12]と呼んで実現に向けて研究を進めている．FPN を実現するための要素技術として，これまでに種々のプロトコルを定義してきた．その中には，動的に通信装置の動作情報を生成する動的処理解決プロトコル DPRP（Dynamic Process Resolution Protocol）[9]，通信中に IP アドレスが変わっても P2P で移動透過通信を実現することができる Mobile PPC（Mobile Peer-to-Peer Communication protocol）[10]，グローバルアドレス空間からプライベートアドレス空間への通信開始を可能とした NATF（NAT Free protocol）[11]などがある．

本稿ではこれらのプロトコルを全て統合したセキュア通信アーキテクチャ GSCIP（Grouping for Secure Communication for Internet Protocol；ジースキップ）を提案し，その実装方法について述べる．以降，2 章で FPN，3 章で GSCIP と GSCIP を構成する各プロトコルの概要，4 章で各プロトコルの統合と GSCIP の実装，5 章でまとめと今後の課題について述べる．

2. FPN

FPN と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グルーピング通信を行い，かつ移動透過性を実現することができるネットワークである．同一通信グループ内の端末間通信は暗号化され，異なる通信グループに属する端末からのアクセスを拒否することができる．ホストは複数の通信グループに帰属すること（多重帰属）が可能で，ホスト単位/サブネット単位というグループの違いを意識する必要はない．またサブネットが階層的に構築されている環境（縦列接続）にも対応することができる．FPN の条件として，自由な移動通信を実現することが重要である．ホストやサブネットは移動可能で，かつホストは特定のサブネットの内外を往復してもグルーピングの関係は常に維持される．このとき移動後にセキュアな通信を行うために必要な設定情報をユーザが変更する必要は無く，システムが自動的に学習して生成する．ユーザはいつ移動しても，これらの要求を満たしつつ，通信を開始したり，継続したりできることができる．FPN を構築することで，様々なシステム構成に柔軟に対応でき，ユーザの管理負荷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．

FPN の適用領域は大きく分けて，イントラネット内とインターネット上の 2 つが考えられる．図 1 に FPN の適用領域について示す．

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 [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，アクセス制御程度しか行われていないのが現状である．そこでイントラネット内に FPN を適用することで，多重帰属や縦列接続などイントラネットの特徴にも対応でき，安全性と柔軟性を両立し

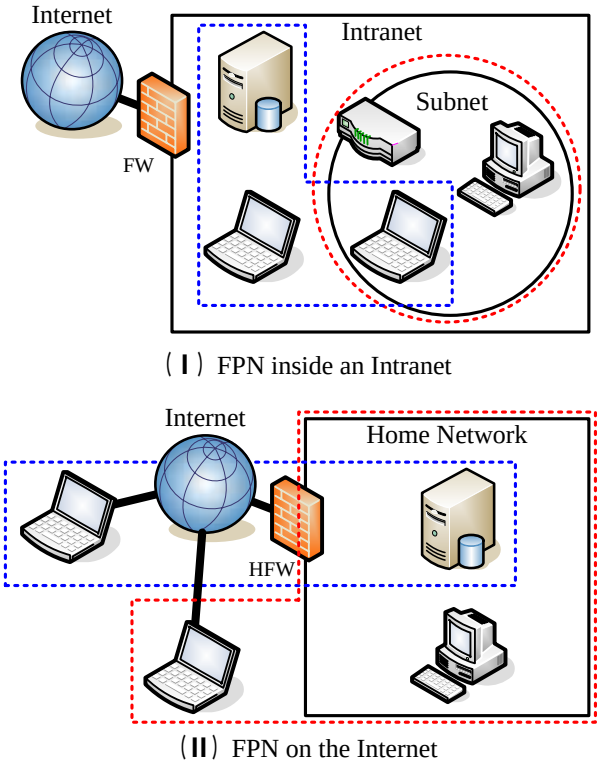


図 1　FPN の適用範囲
Fig 1. An application range of FPN

たシステムを構築することができる．しかし企業のイントラネットとインターネットの間には強固な FW が設置され，通信が大幅に制限されている．そのため，イントラネットとインターネットを跨った自由な通信は現実的ではない．よって FPN の 1 つの適用領域として，イントラネット内に限定した環境を想定する（図 1（Ⅰ））．

一方，ホームネットワークにも FW が設置されることになるが，企業ほど堅固ではなく，ユーザがホームネットワークにアクセスするために，ある程度の自由度を持たせた FW が適していると考えられる．本稿では企業の FW と区別するために，ホームネットワークに設置される FW を HFW（Home Firewall）と表記する．HFW は厳密に通信を遮断するものでなく，ホームネットワークはインターネットの延長に近いものと考えられる．すなわち，FPN はホームネットワークとインターネットを跨って適用することも可能であり（図 1（Ⅱ）），ユーザは家の中と外を移動しても，常に必要最低限の安全性を確保しつつ移動透過性を実現したい．このような環境では，グローバルアドレス/プライベートアドレスという異なったアドレス空間を跨る通信になるが，ユーザはこのような違いを意識する必要がないことが望まれる．

3.　GSCIP

GSCIP は FPN を実現するための有望な一方式としての位置づけにある．図 2 に GSCIP におけるグルーピングの原理を示す．GSCIP では各装置が所持する暗号鍵で FPN における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）と呼び，GK を所持する装置を GE（GSCIP Element）と呼ぶ．同一の通信グループの GE 間の通信は GK を用いて暗号化される．通信グループ情報と GK はグループ管理装置 MS（Management Server）から，各 GE の起動時

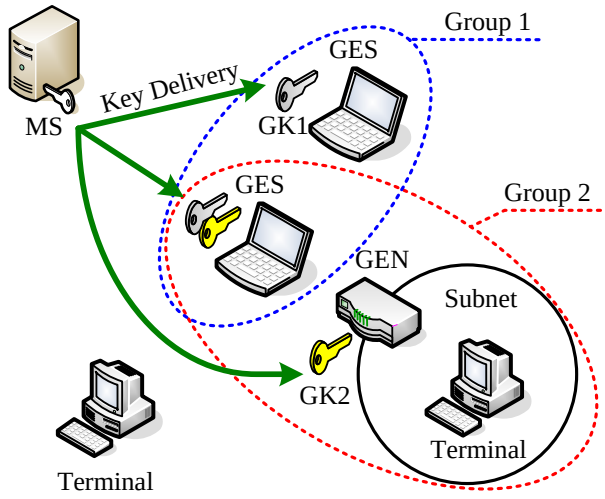


図 2　GSCIP におけるグルーピングの原理
Fig 2. The principle of the grouping in GSCIP

に配送される．GE にはサブネットを構成するルータタイプの GEN（GE for Network）と，各ホストにインストールされるソフトエアタイプ GES（GSCIP for Software）がある．GEN の配下に存在する一般端末は，GEN によって保護されているため，GEN と同一グループに所属していると見なすことができる．また GE には通信グループ外の端末との通信を一切禁止する閉域モード（CL；Closed Mode）と，通信グループ外の端末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 の所属グループと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柔軟に決定することができる．これを実現するために，端末間の通信に先立ち，通信経路上に存在するすべての GE 間で設定されている情報を相互に交換して，通信パケットの処理内容を決定，保存する．

また移動透過性を実現するために，GSCIP では通信開始時の IP アドレスの解決（初期 IP アドレスの解決）と，通信中に IP アドレスが変わった場合の処理（継続 IP アドレスの解決）を明確に分離する．GSCIP では初期 IP アドレスの解決には DDNS（Dynamic DNS）[5]を，継続 IP アドレスの解決には GSCIP の機能を適用する．なお DDNS は DNS 技術の延長であり，ホスト名と IP アドレスの関係を動的に管理できる．主に自宅サーバの構築・公開などで既に多く利用されており，導入が容易である．DDNS を用いることによって，動的な IP アドレスが割り当てられた移動端末を特定することができる．以下に GSCIP を構成する各プロトコルについて述べる．

（1）DPRP

DPRP は通信経路上の GE 間で必要な情報を交換し，認証処理後に動作処理情報テーブル PIT（Process Information Table）を自動生成する．通信開始時に GE は自らが保持する PIT を検索する．検索の結果，該当する動作処理情報が無い場合，通信パケットを一時的に退避させてから図 3 に示す DPRP ネゴシエーションを行う．このネゴシエーションは ICMP をベースとした DPRP 制御パケットを利用しており，通信パケットの送信元/宛先 IP アドレスとポート番号，プロトコル番号，グループ情報，動作モードなどの情報が GE 間で交換される．その後，交換した情報から動作処理情報を決定してから，通信経路上の全 GE に動作処理情報を通知して

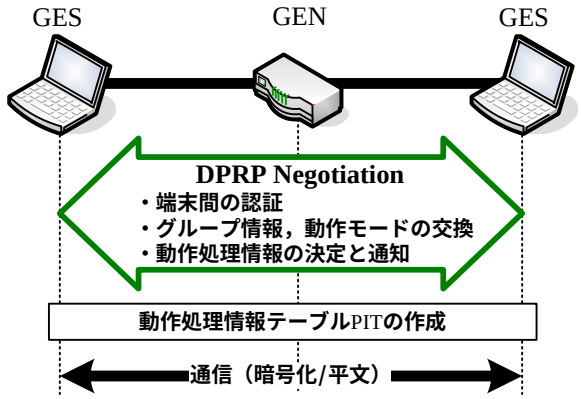


図 3　DPRP の概要

Fig 3. An outline of DPRP

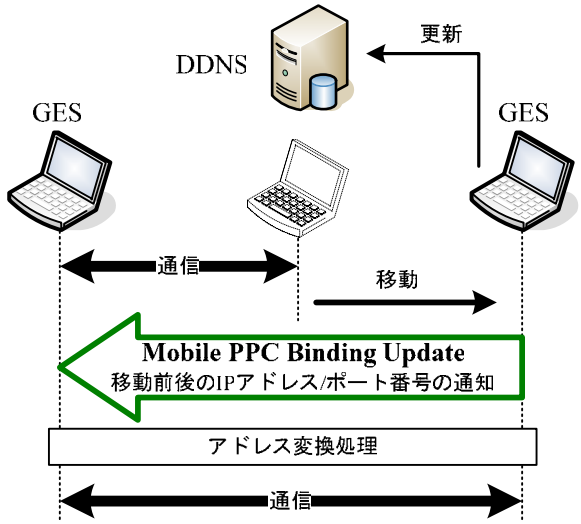


図 4　Mobile PPC の概要

Fig 4. An outline of Mobile PPC

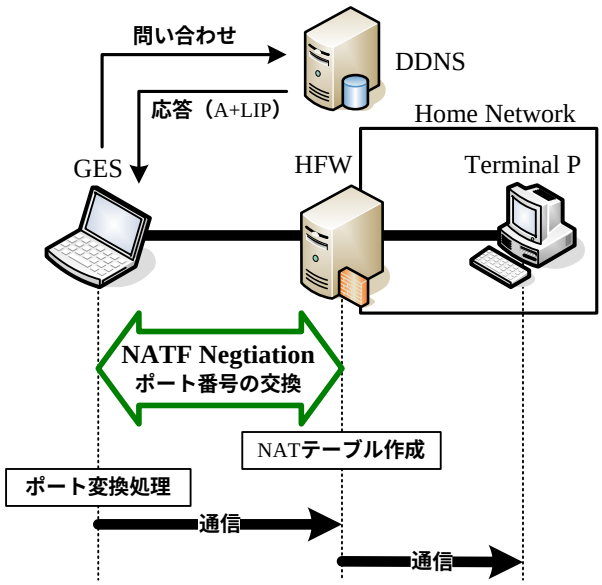


図 5　NATF の概要

Fig 5. An outline of NATF

PIT に登録する．このとき GK による確実な認証を行っているため，PIT を偽造されるなどの恐れはない．以後の通信は PIT の情報に基づいて，通信パケットの暗号化や破棄などの処理を IP 層で行う．

DPRP は通信に先立って実行される他に，ホストやサブネットが移動して IP アドレスが変化した場合にも実行される．従ってホストやサブネットはどこへ移動しても，その都度 GE 間で PIT を作成するため，IPsec/IKE のように暗号化通信に必要な設定パラメータをユーザが設定し直す必要はない．

（2）Mobile PPC

通信中に端末が移動すると IP アドレスが変化するため，一般には通信が継続できない．そこで移動透過性を実現するために，GSCIP では DDNS と Mobile PPC を使う．Mobile PPC は移動前後の IP アドレスの情報を交換して，IP 層でアドレス変換を行うことで通信を継続することができる．

図 4 に Mobile PPC の概要を示す．GE が通信中に別のネットワークに移動すると，GE は DHCP により新しく IP アドレスを取得する．ここで GE は移動前後の IP アドレスとポート番号を Binding Update として通信相手に通知する．これにより両 GE 間で移動前後の IP アドレス情報を共有でき，この情報に基づいて IP 層で新しい IP アドレスに変換するためのテーブルを生成する．そのため，IP 層以下では正しくルーティングされ，上位層ではアドレスの変化を隠蔽させてコネクションを維持することができる．

Mobile PPC は特定のアドレス管理装置が不要で、かつ P2P で移動透過性を実現するため，Mobile IP におけるような一点障害やカプセル化によるオーバヘッドなどの課題は発生しない．

（3）NATF

インターネット上のグローバル IP アドレスを持つ端末からホームネットワーク上のプライベート IP アドレスを持つ端末にアクセスを行うと，HFW に実装されている NAT のアドレス変換テーブルが生成できないため，一般には通信を開始することができない．NATF では GE，DDNS サーバおよび HFW が協調して，インターネットから NAT テーブルを動的に生成する．決定したポート番号の情報を端末と交換して，端末の IP 層でポート変換を行うことで，ホームネットワーク内の端末へのアクセスを開始することができる．

図 5 に NATF の概要を示す．NATF では，DDNS に予めホームネットワーク内の端末 P のプライベート IP アドレスを，LIP（Local IP address）と呼ぶ拡張レコードとして登録しておく．DDNS は GES から端末 P に対する IP アドレスの問い合わせを受けると，HFW のグローバル IP アドレスを A レコードとして，さらに LIP レコードを付加情報して応答する．A レコードと LIP レコードの組み合わせは唯一無二であるため，プライベートアドレスが重複するような場合でも相手を特定することが可能である．GES のアプリケーションは通信相手を HFW として認識する．GES は通信に先立って HFW とネゴシエーションを行う．GES は，送信元/宛先 IP アドレスとポート番号，プロトコル番号，LIP を HFW 宛に送信する．HFW はこれらの情報から NAT テーブルを強制的に生成した後，選択したポート番号を GES に通知する．GES はこのポート番号をもとに，IP 層でポート変換を行ってから HFW に送信する．HFW はこのパケットを上記生成済みの NAT テーブルに基づいて端末 P へ転送する．以上の動作によりグローバルアドレス空間からホームネットワークへの通信が開始可能となる．

GSCIP を利用することで, ユーザは難しい設定を行うことなく，多段構成や多重帰属に対応しながら，移動透過性を実現しつつ安全な P2P 通信を行うことが可能になる．また，ホームネットワーク内にあるプライベートアドレス端末へ接続できるため，これまで NAT が障害となり利用できなかったアプリケーションを使えるようになる．ホームネットワークにアクセスしてもよい端末はホームネットワークと同一の通信グループに所属している必要があるため，不特定多数のアクセスは拒否することができる．またホームネットワーク上の端末が複数あり, ある端末は友人のアクセスも許可したい，ある端末は家族しかアクセスを許可しないといった状況が想定できる．友人のアクセスを許可したい場合は，その友人とホスト単位の通信グループを構築し，ホームネットワークの通信グループと別にするなどの方法が考えられる．

4. GSCIP の実装

GSCIP は IP 層に実装される．OS には IP 層の情報が豊富な FreeBSD を選択した．図 6 に GSCIP の実装概要を示す．IP 層の入出力関数 ip_input( ), ip_output( )から GSCIP モジュールを呼び出し，処理されたパケットは IP 層の元の場所に戻されるため，既存の IP 層の処理に影響を与えない．

GSCIP に含まれる各プロトコルは IP 層で動作するため，プロトコル間の連携をとることが容易である．また DPRP, NATF のネゴシエーション，および Mobile PPC の Binding Update には，端末内の GSCIP 同士で情報を交換，共有するという共通の動作を含んでいることから，Mobile PPC と NATF を DPRP に統合した．図 7 に拡張した DPRP パケットフォーマットの概要を示す．DPRP 制御パケットにオプションフィールドを追加して，そこに Mobile PPC や NATF により交換される情報を格納する．制御パケットを受信した GE は，制御パケットヘッダからオプションの有無を検出し，その内容に応じて Mobile PPC，NATF モジュールに処理を渡す．

DPRP に統合したことにより，Mobile PPC や NATF の通信においても，相手端末の認証と通信の暗号化を同時に実現できる．特にインターネットからホームネットワークにアクセスする場合, 従来の NATF ではセキュリティに関する懸念があったが，DPRP に統合することにより，端末間で認証を行うことが可能になる．現在までに DPRP と Mobile PPC の統合と実装を完了して動作検証を終えている．

5. まとめ

本稿では DPRP，Mobile PPC，および NATF を統合したセキュア通信アーキテクチャ GSCIP を提案し，その実装方法について述べた．今後はホームネットワークとインターネットを跨った移動透過性の実現を目指している. また GSCIP を IPv6 に対応させることで，IPv4/IPv6 の混在ネットワーク上における FPN の構築方法についても検討する予定である．

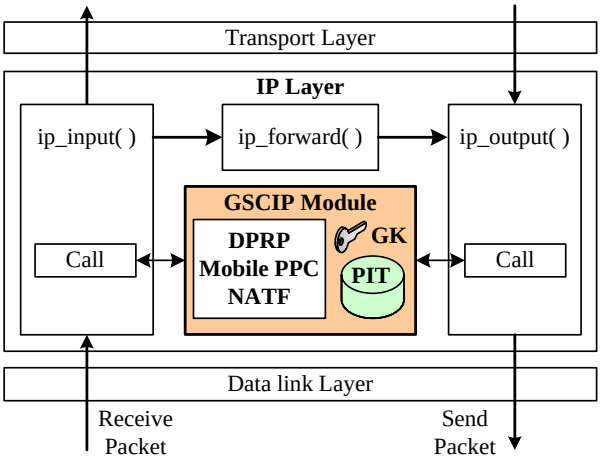


図 6　GSCIP の実装
Fig 6. Implementation of GSCIP

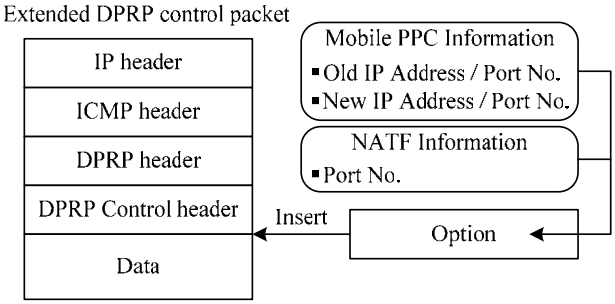


図 7　拡張 DPRP 制御パケットフォーマット
Fig 7. Extended format of DPRP control packet

参　考　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 (2004).
2) S. Kent and R. Atkinson: Security Architecture for the Internet Protocol, RFC2401 (1998).
3) D. Harkins and S. Carrel: The Internet Key Exchange (IKE), RFC2409 (1998).
4) C. Perkins: IP Mobility Support for IPv4, RFC3344 (2002).
5) P. Vixie, S. Thomson, Y. Rekhter, J. Bound: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC2136 (1997).
6) T. Kivinen, B. Swander, A. Huttunen and V. Volpe: Negotiation of NAT-Traversal in the IKE, RFC3947 (2005).
7) Sami Vaarala: Secure IPv4 Mobility for Enterprise Users, HUT T-110.551 Seminar on Internetworking (2004).
8) Chin-Fu Kuo, Yung-Feng Lu, Ai-Chun Pang and Tei-Wei Kuo: Implementations of the User Mobility Support over IPsec, WIA'05 (2005).
9) 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, 情報技報，2005-CSEC-28，pp.199-204 (2005).
10) 竹内元規，鈴木秀和，渡邊晃: モバイル端末の移動透過性を実現する Mobile PPC の実装，情報技報，2005-MBL-32，pp.29-35 (2005).
11) 加藤尚樹，柳沢信成，鈴木秀和，渡邊晃: アドレス空間の違いを意識しない通信方式 NATF の提案と実装, 情報技報，2005-DPS-122，pp.351-356 (2005).
12) Watanabe Lab.: Flexible Private Network, 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を実現するセキュア通信アーキテクチャGSCIPの提案

A proposal of Secure Communication Architecture GSCIP realizing Flexible Private Network

名城大学大学院　理工学研究科

鈴木秀和　竹内元規　加藤尚樹　増田真也　渡邊晃

はじめに

- ユビキタスネットワークの構築に向けた様々な研究開発
- ユビキタス社会では

あらゆるユーザが簡単にネットワークを利用できる

→ ✓ユーザが意識することなく通信の安全性を保証
✓様々な環境に対応できる

情報家電製品の普及
情報端末の高性能化

→ ✓移動しながら通信をしたい
✓インターネットからホームネットワークにアクセスしたい

既存技術と課題

- 通信の安全確保
  → **IPsec**
  - 利用するために専門知識と多くの設定が必要
  - 端末が移動する度に設定の変更が必要

- IPレベルでの移動通信
  → **Mobile IP**
  - 移動ノードの位置を管理する特殊な装置HAが必須
  - HAを多重化できない → 耐障害性の向上が必要

- ホームネットワークへのアクセス
  → **VPN**
  - 企業を中心に普及
  - インターネットとホームネットワークの境界にNATが存在

課題を解決するために

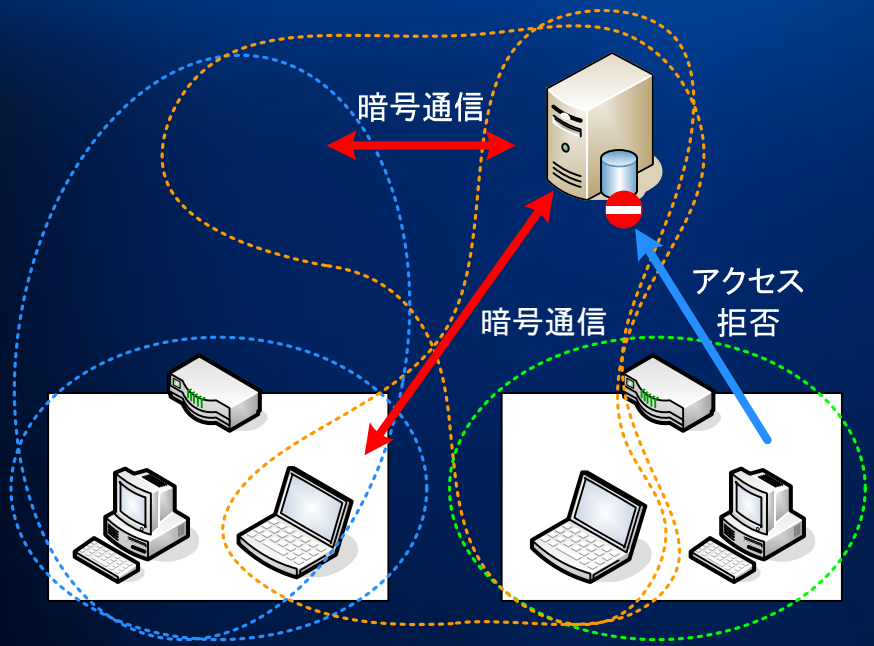
- これらの要求を様々な環境で同時に満たすことは困難
- サブネット単位のセキュリティと個人単位のセキュリティを同時に守る必要性

フレキシブルプライベートネットワーク
FPN (Flexible Private Network)

» 簡単にセキュリティを向上できる
» 端末があらゆる空間を自由に移動できる

Flexible Private Network

- 柔軟性とセキュリティを兼ね備えたグルーピング通信
- 移動透過性を実現

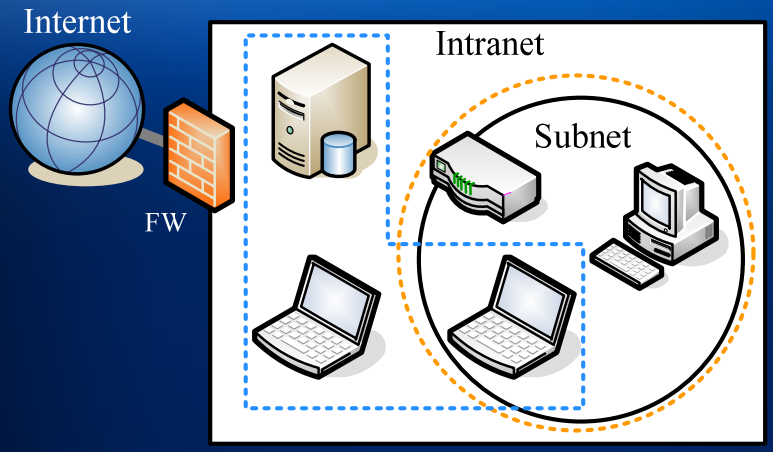


- 端末は特定のサブネットにいながら他のグループに帰属可能（多重帰属）
- 同一グループ内の通信は暗号化
- 他のグループからのアクセスを拒否することが可能
- サブネットの階層化に対応（縦列接続）
- 端末/サブネットは自由に移動可能
- 移動しても定義されたグループは不変
- 必要な設定はシステムが学習して生成

様々なシステム構成に柔軟に対応でき，ユーザの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

FPNの適用範囲

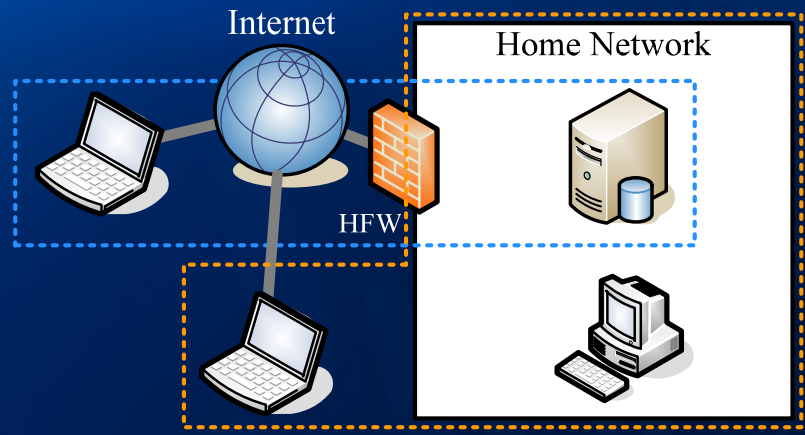
イントラネット内のFPN



強固なFW→通信を大幅に制限

- 多重帰属や縦列接続など
  イントラネットの特徴に対応
- 安全性と柔軟性を両立した
  システムの構築が可能

インターネット上のFPN

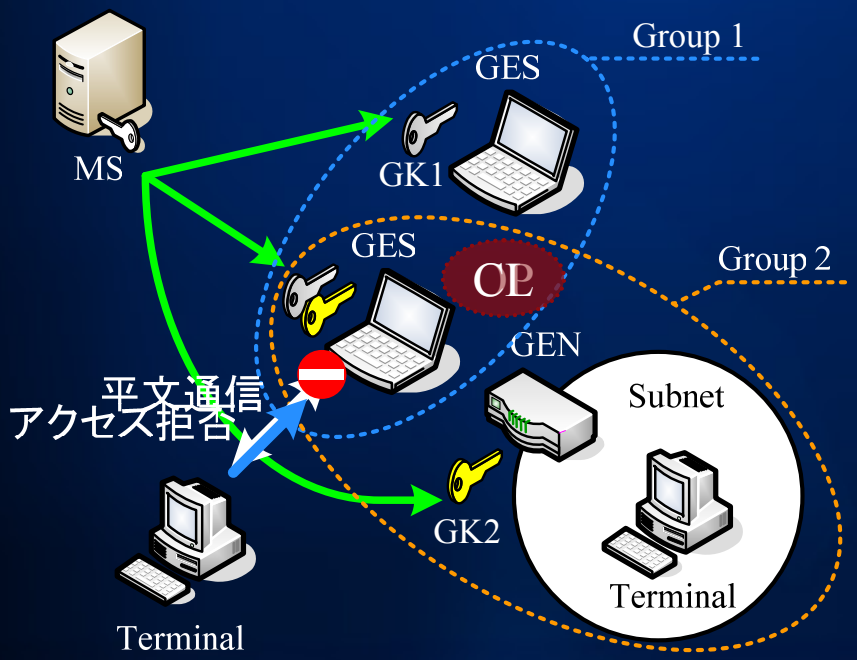


HFW→ある程度の自由度あり

- 家の内外で常にセキュリティを確保
- アドレス体系の違いに影響されない
- 簡単かつ安全にホームネットワーク
  にアクセス可能

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
  - 同じ暗号鍵を持つサブネット/端末を同一の通信グループとして定義（暗号鍵＝グループ鍵GK）
  - グループ管理装置MSは予め設定されたグループ番号とGKを配送
    - MS-GE間で確実な認証　→　保持しているGKが信用できる



GE（GSCIP Element）

- GES（Software型）：クライアントに実装
- GEN（Network型）：ルータに実装

動作モード（他の通信グループとの通信）

- 開放モード（OP）：平文通信が可能
- 閉域モード（CL）：一切禁止

GSCIPを構成する技術

- *DPRP (Dynamic Process Resolution Protocol)*
  - 端末間の情報交換と認証処理
  - 動作処理情報の決定とPIT（Process Information Table）の生成

- *Mobile PPC (Mobile Peer-to-Peer Communication protocol)*
  - 継続IPアドレスの解決（IPアドレス変化時）
  - IP層でアドレス変換を行い，P2Pで通信を継続

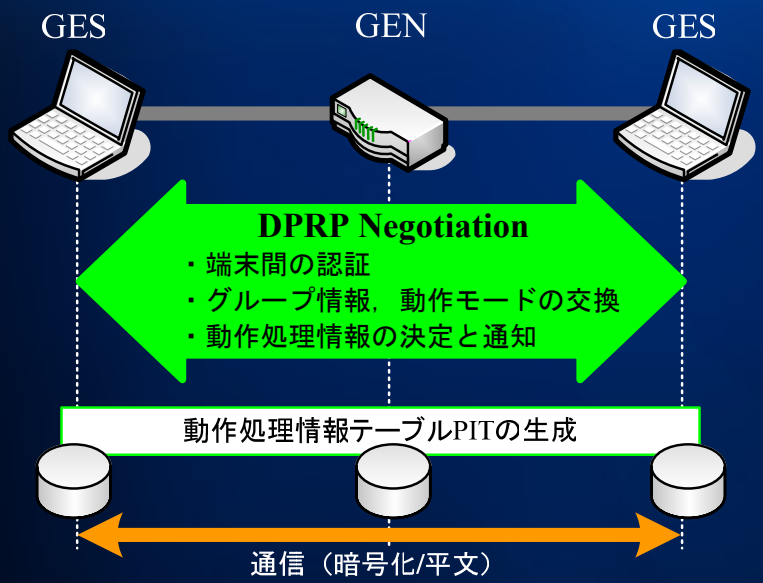
    ※初期IPアドレスの解決（通信開始時）

    → *DDNS (Dynamic DNS)*を利用

- *NATF (NAT Free protocol)*
  - インターネット側からNATテーブルを動的に生成
  - 端末側でポート変換処理を行い，NATを通過

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
  - 通信開始時
  - サブネット/端末が移動してIPアドレスが変化した時



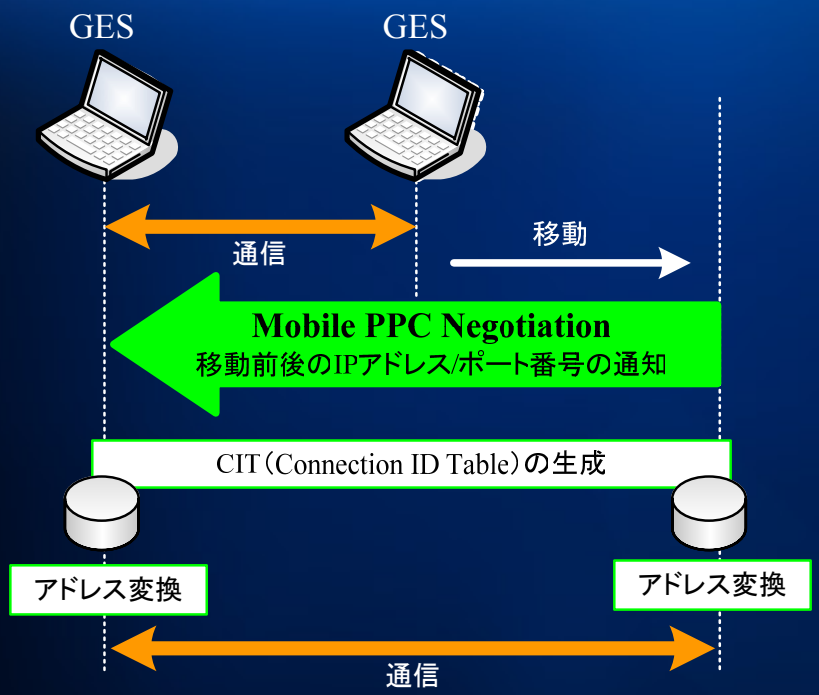
PIT検索→情報がなければDPRP開始
- 通信経路上の全GEの情報を取得
- 動作処理情報を決定
- 決定した情報を通信経路上の全GEに通知
- GKにて認証処理後，PIT生成

以後の通信はPITを参照して行う
- PITは[src/dst{IP,Port},protocol]により検索

どの環境に移動しても常にその場に応じた設定を生成することが可能
➔ FPNにおけるグルーピング通信を実現

Mobile PPCの動作概要

- 通信中のGE間で動的にネゴシエーション
  - サブネット/端末が移動してIPアドレスが変化した時



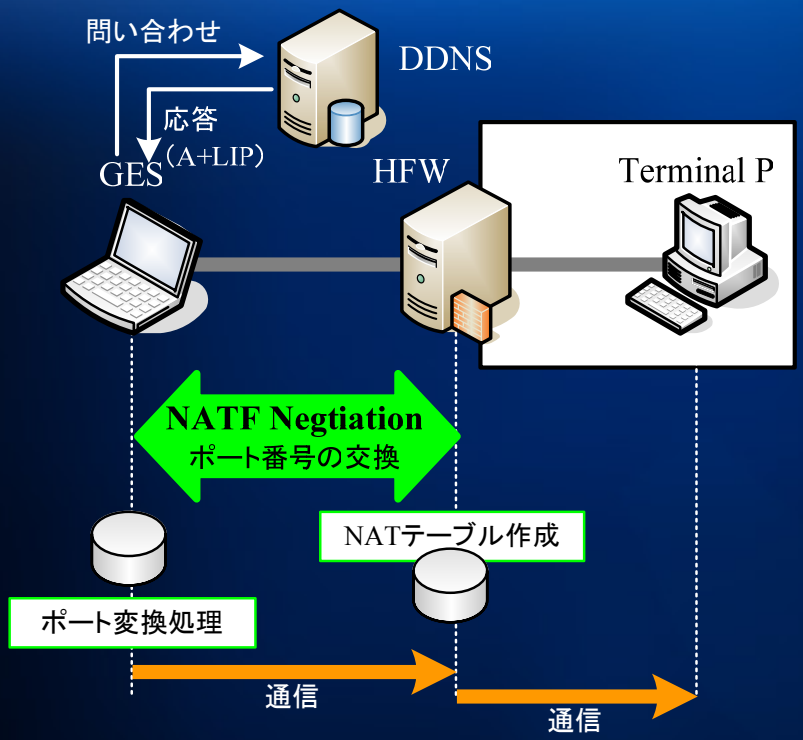
移動→新しいアドレスを取得したら開始
- 通信中の端末に移動前後のIPアドレス，ポート番号を通知
- 取得した情報からCIT（Connection ID Table）を生成

以後CITを参照してIP層にてアドレス変換
- IP層以下では新IPで正しくルーティング
- IP層以上では旧IPでコネクション維持

通信中に移動してもP2Pでコネクションを維持することが可能
➔ FPNにおける移動透過性を実現

NATFの動作概要

- インターネット上の端末とHFW間で動的にネゴシエーション
  - ホームネットワーク上の端末との通信開始時



DNS応答にLIP（Local IP）が付いてれば開始

- 送信元IP，ポート番号，宛先ポート番号，LIP（端末Pのプライベートアドレス）を通知
- 取得した情報からNATテーブルを生成（端末Pからの応答パケットに見せかける）
- NATが選択したポート番号を通知

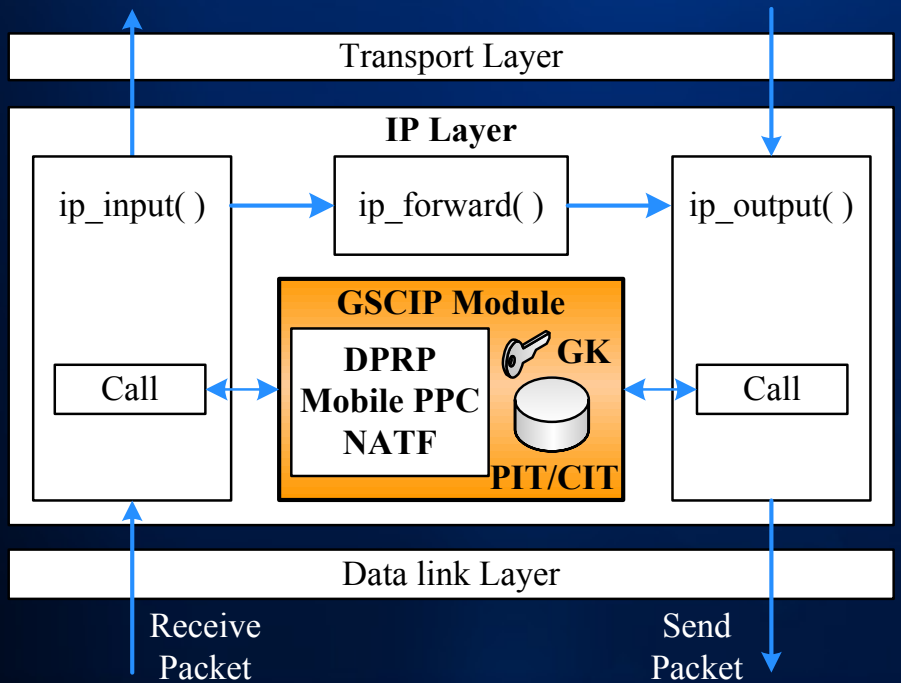
以後端末はIP層にてポート番号変換

- HFWのNATテーブルに一致

グローバル空間とプライベート空間の通信制約を解除することが可能
➔ FPNにおけるホームネットワークへのアクセスを実現

GSCIPの実装

- IP層に実装
  - 各プロトコルはIP層で動作し，連携が容易
  - 各プロトコルに共通動作あり
    - 端末間で情報交換，テーブル生成と検索，パケット処理
  - ➔ Mobile PPC，NATFをDPRPに統合（DPRPのオプション機能として）



統合によるメリット

- Mobile PPCとNATFの通信のセキュリティレベル向上
  - 相手端末の認証
  - 通信の暗号化

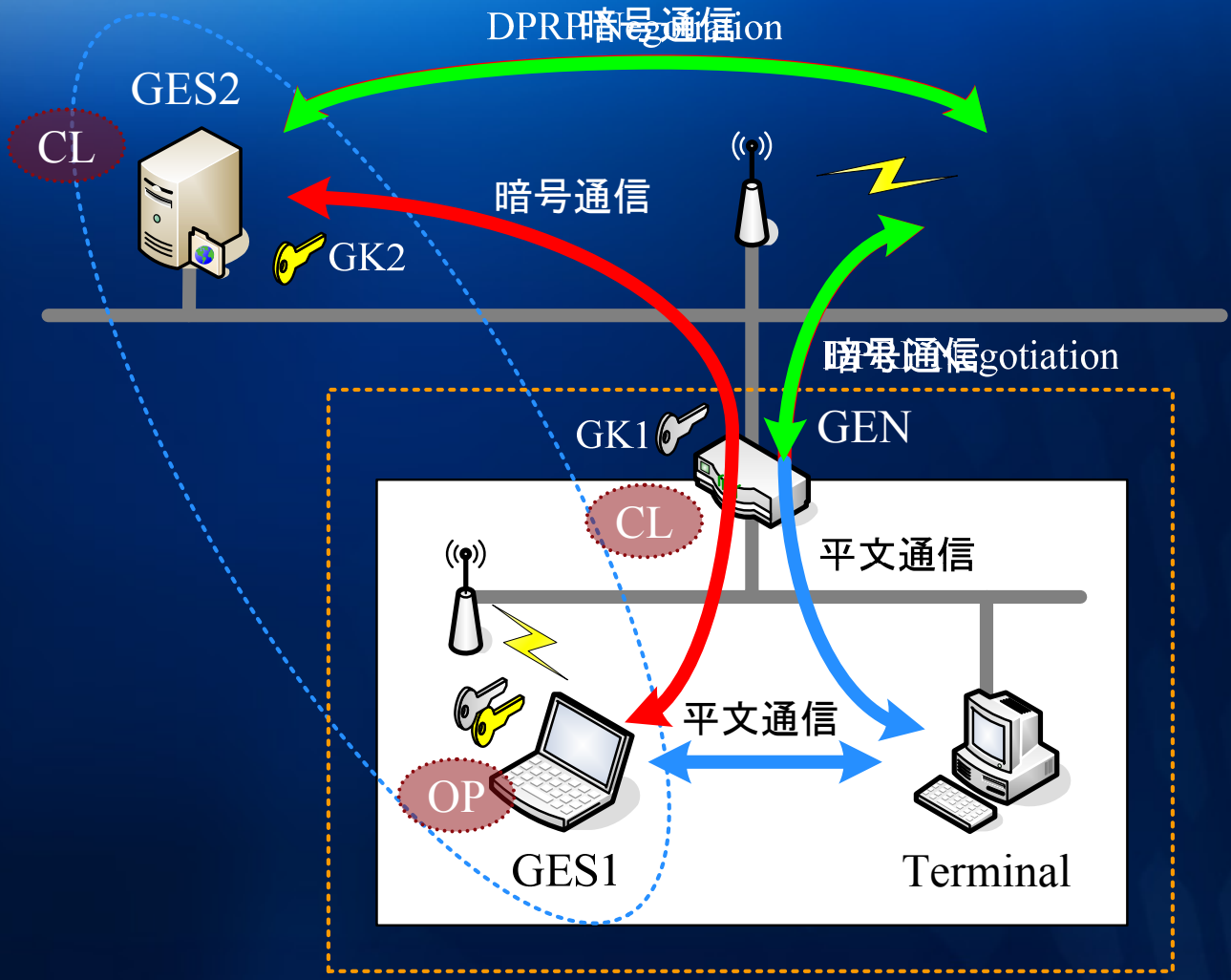
実装状況

- DPRP，Mobile PPC：実装・統合完了
- NATF：実装中

GSCIPでできること

- ユーザは難しい設定を必要としない
  - 通信の安全性を高めることが可能
  - 移動透過通信が可能
  - どこに移動してもシステムが動的に学習して処理してくれる
- インターネットからホームネットワークへアクセスできる
  - NATが障害で利用できなかったアプリケーションが使用可能
- ホームネットワークにアクセスするためには
  - HFWと同一通信グループに所属している必要あり
  - 不特定多数のアクセスを拒否できる
  - 複数のグループを定義することで柔軟なアクセスを許可できる

GSCIPの現状


DPRP暗号通信
GES2
CL
暗号通信
GK2
暗号通信
GK1
GEN
CL
平文通信
平文通信
OP
GES1
Terminal

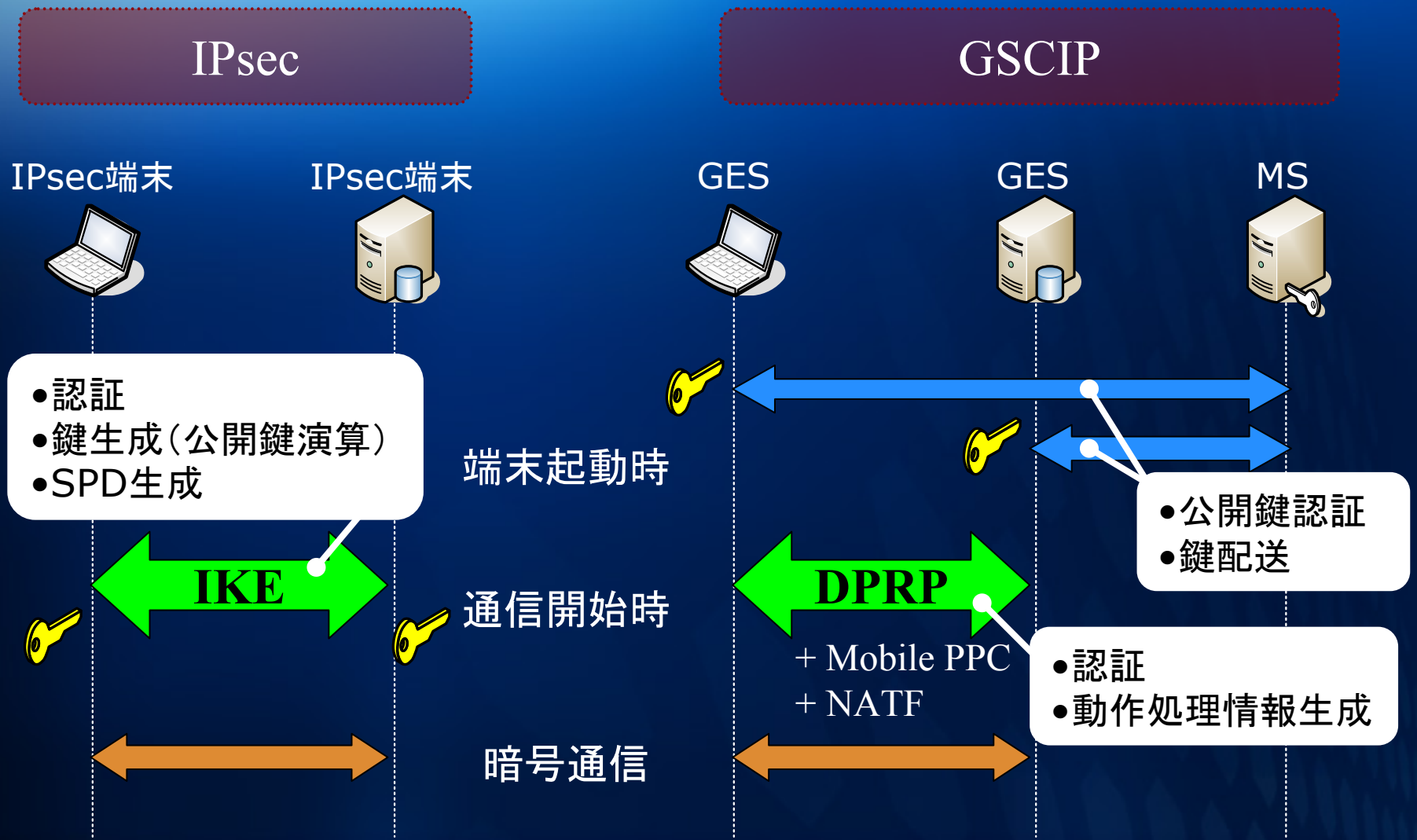
まとめ

- セキュア通信アーキテクチャGSCIPの提案
  - FPNを実現するための有望な一方式
  - DPRP，Mobile PPC，NATFを統合することで実現
- 今後の課題
  - NATFの実装と統合
  - ホームネットワークとインターネットを跨った移動通信の実現
  - GSCIPのIPv6化
    - IPv4/v6混在ネットワークにおけるFPNの構築方法の検討

A proposal of Secure Communication Architecture GSCIP realizing Flexible Private Network

Thank you

GSCIPとIPsecのアーキテクチャの違い



GSCIPにおける3つの機能役割

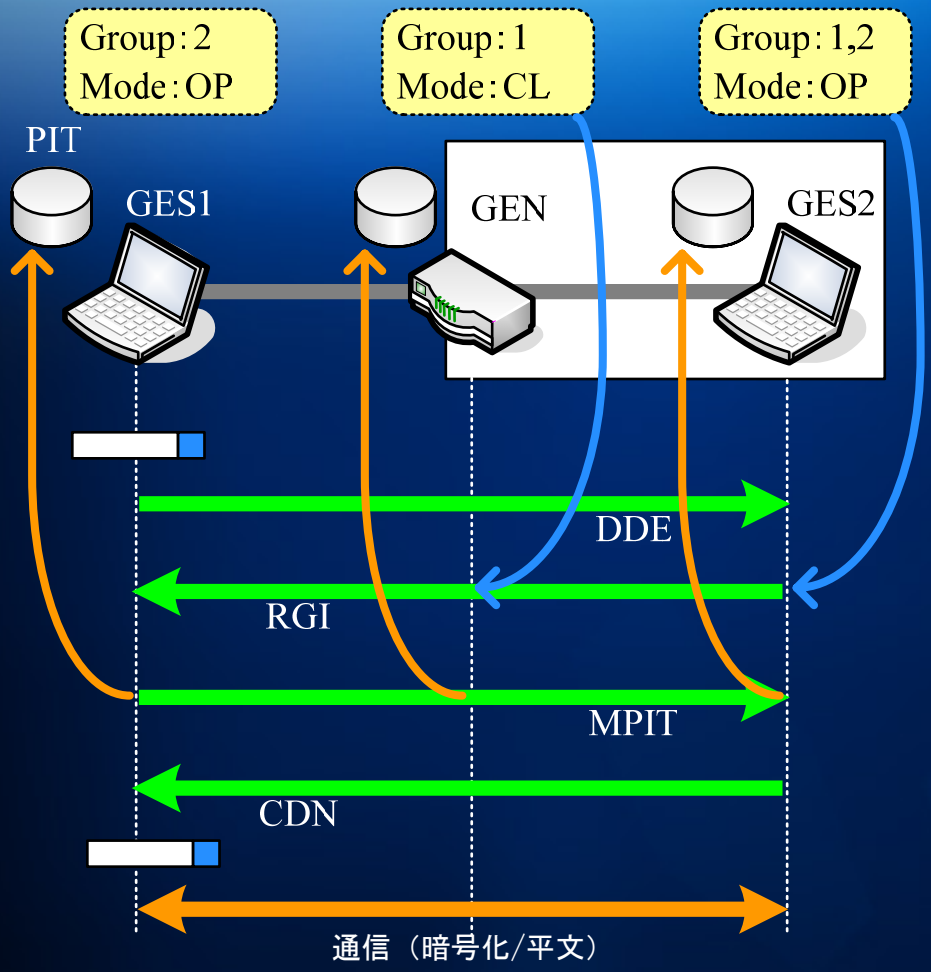
次の3つの機能は独立して動作

1. GEへの情報配送
   - » ユーザはGEにログイン後，予め設定されている情報をMSから取得

2. GE間の認証および各種テーブルの生成
   - » DPRPにより通信経路上の各GEの情報を取得してPIT生成
   - » Mobile PPCによりGE移動時にCUを行ってCIT生成
   - » NATFにより決定したポート番号を取得して変換テーブル生成

3. 通信パケットの処理
   - » PITに基づき，暗号処理/透過送受信/破棄
   - » CITに基づき，IPアドレス変換
   - » 変換テーブルに基づき，ポート番号変換

DPRPの詳細動作



DPRP制御パケット（ICMPベース）

- DDE（Detect Destination End GE）
- RGI（Report GE Information）
- MPIT（Make Process Information Table）
- CDN（Complete DPRP Negotiation）

1. PIT検索 → あり→9.へ
   → なし→2.へ
2. パケットを待避してDPRP開始
3. DDEで終点GEを決定
4. RGIにより各GEの設定情報を通知
5. 動作処理情報を決定
6. MPITにより決定した情報を通知，PIT生成
7. CDNによりネゴシエーション完了通知
8. 待避していたパケットを戻す
9. PITの情報に基づいて通信再開

DPRP性能測定

内部処理時間

単位：usec

GES1	GEN	GES2	合計
96.59	44.32	62.43	203.34

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
最初の通信開始	1,040	2,994,033

IKEネゴシエーション

- 通信を暗号化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

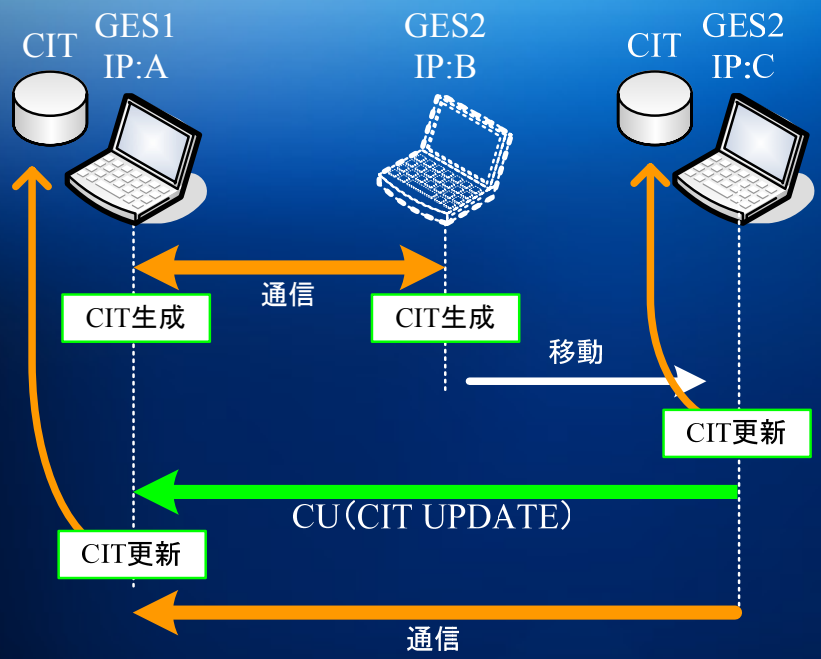
IPsec/IKE（参考測定）

- 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

Mobile PPCの詳細動作

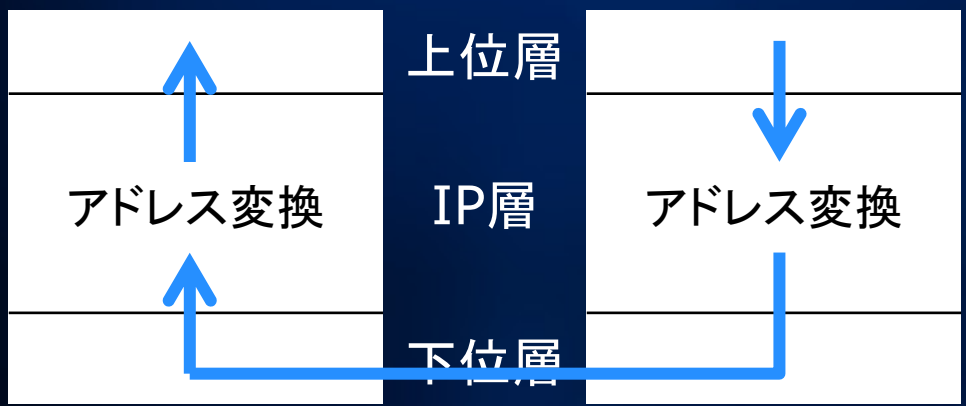


GES1のCIT

移動前	移動後
A:x→B:y	A:x→C:y
B:y→A:x	Cy:→A:x

GES2のCIT

移動前	移動後
B:y→A:x	C:y→A:x
A:x→B:y	A:x→C:y

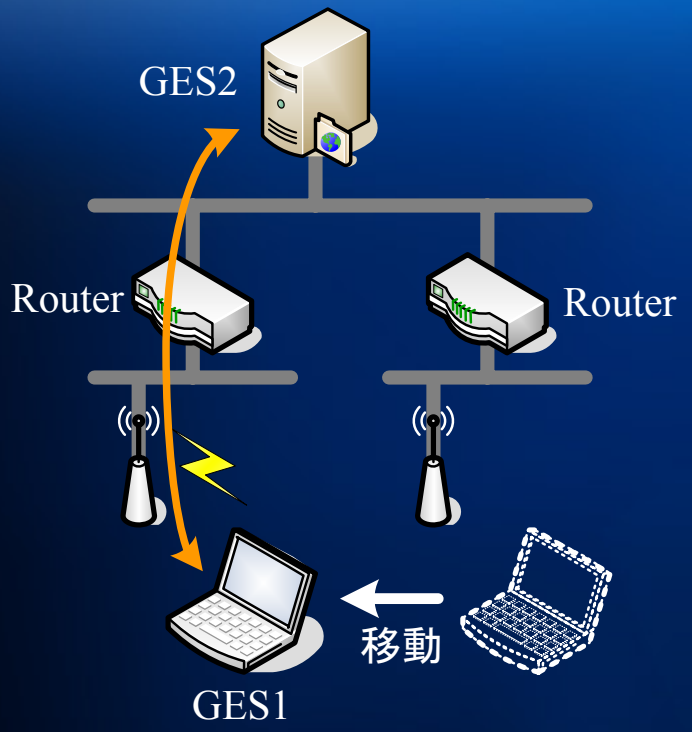


＝ A:x ⇔ B:y　古いアドレス

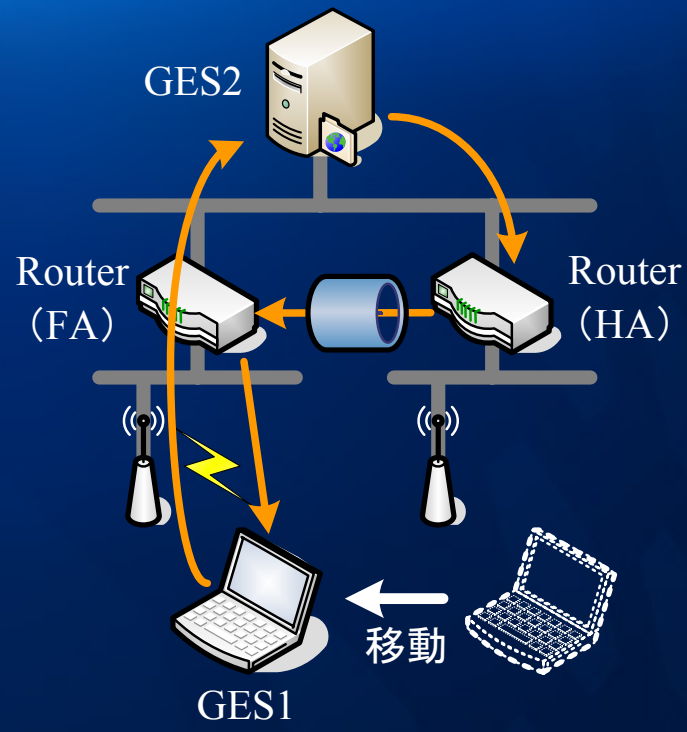
＝ A:x ⇔ C:y　新しいアドレス

Mobile PPC性能測定　実験環境

Mobile PPC



Mobile IP



Mobile PPC実装端末

» GES1，GES2

Mobile IP実装端末

» GES1，Router（HA，FA）

スペック（GES1）

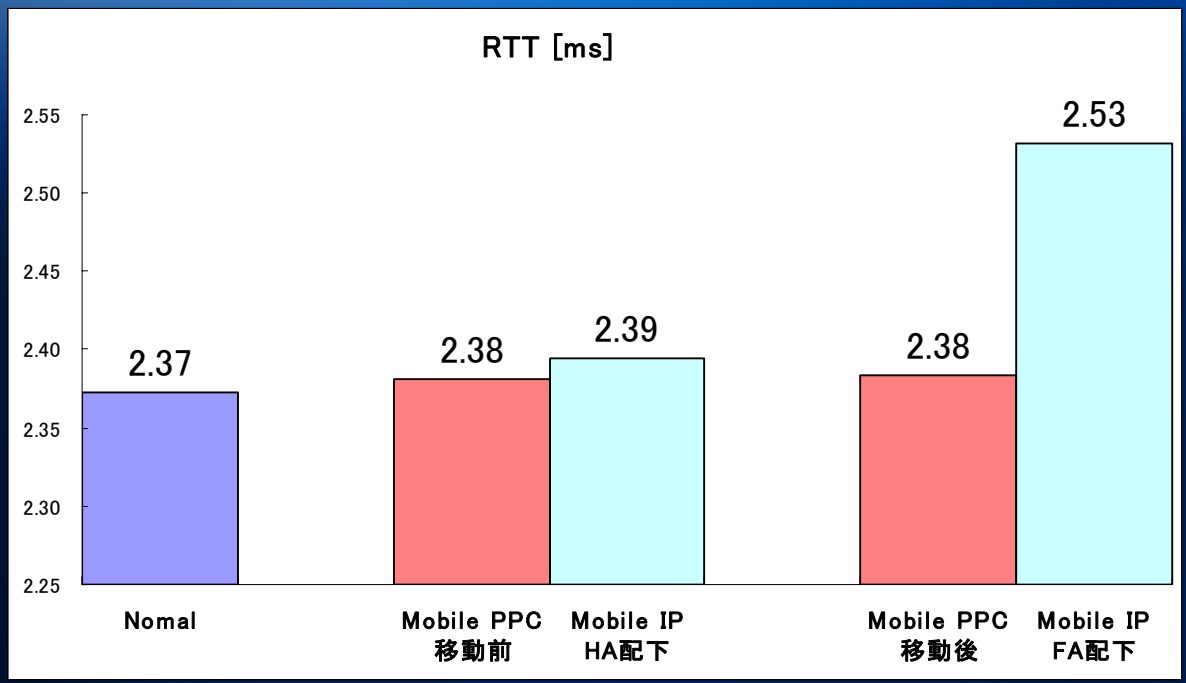
» Celeron 2.0GHz
» 256MB
» IEEE802.11b

GES2，Router

» Pentium4 2.4GHz
» 512MB
» 100BASE-TX

Mobile PPC性能測定

GES1-GES2間のRTT

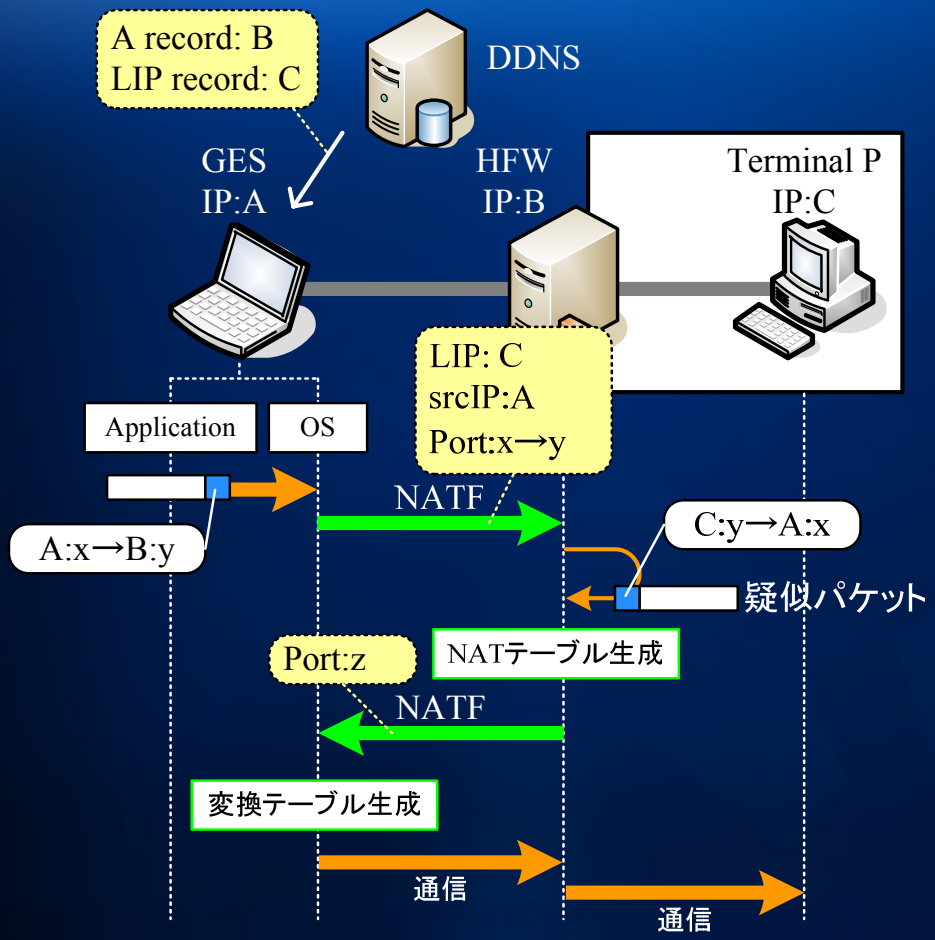


実験

- GES1-GES2間でUDP通信
- 1000パケットの平均

- Mobile PPCは移動前後で変化なし
- Mobile IPは，FA配下になると経路の冗長やトンネリングなどによるオーバヘッドの影響が出ている
- Mobile PPCの処理が通信に与える影響は，Mobile IPに比べて小さいことが実証できた

NATFの詳細動作



GESの変換テーブル

変換前	変換後
A:x→B:y	A:x→B:**z**
B:**z**→A:x	By:→A:x

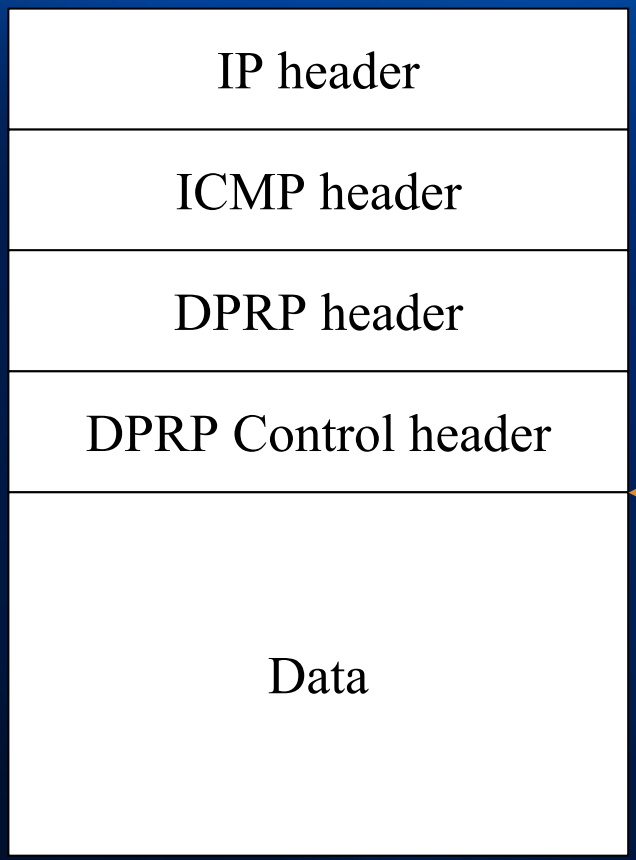
HFWのNATテーブル

受信	送信
C:y→A:x	B:**z**→A:x
A:x→B:**z**	A:x→C:y

- 疑似パケットによりNATテーブルを生成
- GESはIP層でポート変換
  ➔NATテーブルに一致する

DPRP拡張フォーマット

従来のDPRPフォーマット



Mobile PPC

- Old IP address / Port number
- New IP address / Port number

NATF

- LIP
- Port number

Option

暗号処理モジュールについて

- PCCOM（Practical Cipher COMmunication）
  - NAPT/FWを通過可能
  - 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
  - 多様な利用形態への対応が求められる一般端末での利用を想定

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

結果

- PCCOM → Normalの約1.5倍
- ESP → Normalの約3倍

スペック

- Pentium 4 2.4GHz
- 256MB
- 1000BASE

詳細はこちら

- 7/8　10：20～ 8A1
- IPv4/IPv6の混在環境における暗号通信方式の考察
  - 増田真也，渡邊晃