通信グループに基づくサービスの制御が可能なNAT越えシステム

鈴木 秀和[†1,†2] 渡邊 晃[†1]

外出先からホームネットワーク内の通信機器に対してアクセスする場合，NAT 越え問題を解決する必要がある．筆者らは，外部ノードとホームゲートウェイが連携することにより NAT 越え問題を解決する NAT-f（NAT-free protocol）を提案している．しかし従来の NAT-f は，誰でもホームネットワーク内の内部ノードにアクセスできてしまう課題があった．本稿では従来方式に通信グループの概念を導入した新たな NAT 越えシステムを提案する．これにより外部ノードからのアクセス制御と，内部ノードが提供するサービスの制御を同時に実現することが可能となる．

NAT Traversal System with Communication Group-based Service Control

HIDEKAZU SUZUKI[†1,†2] and AKIRA WATANABE[†1]

A NAT traversal problem has to be solved if you access communication devices in a home network from the outside. To solve the problem, we have proposed NAT-free protocol (NAT-f) that an external node and a home gateway cooperate with each other. However, the existing NAT-f system has security issues that anyone can access internal nodes in a home network. This paper presents a new NAT traversal system that combines the existing method and the concept of a communication group. With this method, it is possible to provide the access control of external nodes and the service control of internal nods simultaneously.

†1 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†2 日本学術振興会特別研究員 PD
Research Fellow of the Japan Society for the Promotion of Science

1. はじめに

現在のホームネットワークは IPv4 プライベート IP アドレスを適用するのが一般であり，インターネットの接点には NAT（Network Address Translator）[1),2)] を設置する必要がある．しかし，NAT によりエンドツーエンド接続性が失われ，NAT の外部から内部のネットワークへ通信を開始できない，いわゆる NAT 越え問題が表面化してきた．近年では携帯デバイスの高性能化，小型化やブロードバンドの普及に伴い，IP 電話やマルティメディア通信など個人間の通信が増加している．このような利用形態では，インターネット側からホームネットワーク内の PC や情報家電機器に向けて通信を開始することも想定される．そのため NAT 越え技術の必要性が高まっており，様々な NAT 越え方式が提案されている[3)–7)]．

筆者らは，宅外の外部ノード（以下 EN; External Node）と NAT が実装されたホームゲートウェイ（以下 HGW）に機能を追加することにより，NAT 越え問題を解決する NAT-f（NAT-free protocol）[8)] を提案している．NAT-f では仮想 IP アドレスを導入することにより，EN がプライベートネットワーク上の内部ノード（以下 IN; Internal Node）を仮想的に認識する．仮想的に認識した IN へ通信を開始する際，EN は HGW に対して NAT-f によるネゴシエーションを実行し，IN と通信するために必要な NAT マッピング情報を生成する．以後，EN が送信するパケットの宛先を仮想 IP アドレスから，マッピングされた HGW の外部 IP アドレス・ポート番号に変換することにより，HGW を通過して IN へアクセスすることを可能としている．しかし，従来の NAT-f は要求があれば無条件で NAT マッピング情報を生成してしまうため，外部からの接続を許可された IN に対して誰でもアクセスできるという課題があった．

そこで，本稿では既存の NAT-f に通信グループの仕組みを適用し，EN のアクセス制御と IN のサービス制御を実現する NAT 越えシステムを提案する．EN と IN を特定の属性に基づいてグルーピングし，そのグループで利用可能なサービスを定義する．通信開始時に実行する NAT-f ネゴシエーションに EN が帰属する通信グループの情報を付加する．HGW はこの情報により，EN と IN が同一通信グループのメンバであるかを確認してから NAT マッピング情報を生成する．また，同一通信グループの End-to-End 間，または End-to-GW 間の通信は暗号化され，その安全性は保証される．

以下，2 章で NAT-f の基本的仕組みと，提案方式に係わる要素技術について説明する．3 章で提案方式の詳細について述べ，4 章で提案方式のセキュリティおよび利用シーンについて考察する．最後に 5 章にてまとめる．

2. 要 素 技 術

2.1 NAT 越 え

NAT-f は，EN と HGW が連携することによりホームネットワーク内の IN に対して通信を開始できる NAT 越え技術である．**図 1** に NAT-f の概要を示す．EN は通信開始時にホームネットワーク内に存在する IN の名前解決処理を行う．この過程において，EN は HGW のグローバル IP アドレスを取得するが，IP 層より上位ソフトウェアに対しては IN の FQDN をもとに生成した仮想 IP アドレスを通知する．

上位ソフトウェアは仮想 IP アドレス宛に TCP/UDP パケットを送信することになるが，このとき EN は HGW に対してマッピングネゴシエーションを行う．このマッピング処理により，HGW は EN と IN が通信するために必要な NAT マッピングを生成する．EN は仮想 IP アドレスと HGW で割り当てられたマッピングアドレスの対応関係を示した仮想アドレス変換テーブル（VAT Table）を IP 層内に生成する．

EN は VAT テーブルに基づいて，TCP/UDP パケットの宛先を仮想 IP アドレスから HGW のマッピングアドレスに書き換えて送信する．HGW には既に NAT マッピングが生成されているため，通常の NAT によるアドレス変換処理を実行し，EN からのパケットを IN へ転送する．

このような処理により，インターネット側からホームネットワーク内の機器への通信開始を実現できる．IN には NAT 越えに係わる機能を一切実装しないため，一般の PC はもちろん，情報家電機器などをそのまま利用することができる．しかし，マッピングネゴシエーションには認証機能がないため，誰でも IN にアクセスできてしまう課題がある．そのため，プライベートなコンテンツを特定のユーザに限定して公開することができない．

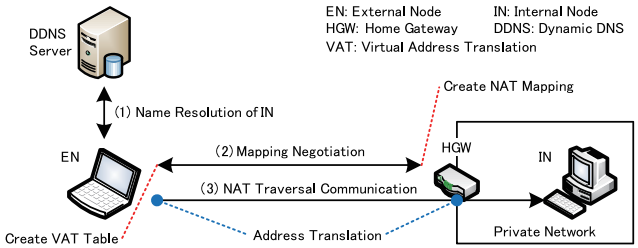


図 1 NAT-f による通信シーケンス
Fig. 1 Communication sequence with NAT-f.

2.2 通信グループの構築

特定の属性に基づくユーザあるいはノードを集合させて通信グループを構築する技術は，通信の安全性を確保する上で有用である．これにより，通信グループ内のメンバ間の通信は暗号化され，第三者による盗聴や改ざんから保護される．

通信グループの構築方法として，例えば GSCIP（Grouping for Secure Communication for IP）[9] が採用しているエリア定義方式[10] がある．この方式では通信グループとグループ鍵と呼ぶ暗号鍵を 1 対 1 に対応付けているため，ユーザが複数のグループ鍵を所持することにより，容易に複数の通信グループに多重帰属することができる．また通信グループの定義が容易であり，IP のサブネットワークに依存しないグループの定義が可能である．

通信開始時に，通信相手とグループ情報を交換して同一グループに属しているか確認し，暗号化通信に必要な動作処理情報を生成する．

2.3 暗号化通信

アプリケーションを意識することなく通信パケットを暗号化する技術は，様々なアプリケーションの利用が想定される NAT 越えシステムにも有効である．IP レベルの暗号化通信を実現する技術として，IPsec ESP[11] や PCCOM（Practical Cipher Communication Protocol）[12] がある．

IPsec は強靭なセキュリティ機能を提供する一方，TCP/UDP ヘッダのポート番号とチェックサムフィールドが暗号化範囲および完全性保証の範囲に含まれているため，NAT を通過すると偽造パケットと見なされ，エンドノードで破棄されてしまう．ESP パケットを UDP によりカプセル化して NAT 越えする方法[13] もあるが，ヘッダ追加に伴うオーバヘッドの増加やフラグメントの発生，またヘッダ部のセキュリティが低下するなどの課題が生じる．従って，IPsec は NAT やファイアウォールとの相性が悪いといえる．

PCCOM は IPsec の課題を解決できる暗号通信方式である．PCCOM は本人性確認とパケット全体の完全性保証を，暗号鍵とパケットの内容から生成した疑似データと呼ぶ値を用いて，独自の TCP/UDP チェックサム計算を行うことにより実現する．暗号化範囲は TCP/UDP ペイロード部であるため，NAT を通過することができ，かつファイアウォールによるトラヒック制御か可能である．パケットヘッダの 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されるため，改ざんを防止することができる．この方式によると，NAT やファイアウォールと共存することが可能で，かつパケットフォーマットを変えないため，ヘッダオーバヘッドやフラグメントが発生せず，高スループットを実現できる．

3. 提 案 方 式

3.1 概　　要

本稿で提案する NAT 越えシステムは，従来の NAT-f に通信グループの概念と暗号化通信を導入し，以下の機能を新たに追加する．

- HGW における通信グループに基づくアクセス制御を実現する．
- グルーピングの概念をノード単位からサービス単位に拡張し，柔軟なサービス制御を実現する．
- EN と HGW 間，または EN と暗号化通信機能を有する IN 間の通信を暗号化する．

通信グループの構築は 2.2 節で示したグループ鍵による方法を採用する．EN は HGW に自身が所属する通信グループを通知するために，NAT-f 制御メッセージを拡張する．これにより，NAT マッピングおよび VAT テーブルに加えて，新たにパケットの暗号化に必要な動作処理情報テーブル PIT（Process Information Table）を生成する．暗号化通信には PCCOM を採用し，拡張した NAT-f により生成された PIT に基づいて TCP/UDP パケットを暗号化する．なお，以後本稿で用いる記号は付録に示す．

3.2 グルーピングに関する概念の拡張

図 2 に拡張した ACT（Access Control Table）とサービスのグルーピングイメージを示す．ACT とは NAT-f を実装した HGW が保持する情報で，IN のプライベートホスト名（PHN）[⋆1]とプライベート IP アドレス，および外部からのアクセス可否を示すフラグから構成される．提案方式では新たに Encryption，Service，Group の 3 つの項目を追加する．Encryption には該当する IN が暗号化機能（PCCOM）をサポートするか否かを設定する．Service には該当する IN が外部に公開するサービスが設定され，対応するポート番号を指定する．Group には該当するサービスにアクセス可能な通信グループを指定する．HGW は上記情報に基づいて，外部からのアクセス制御および IN のサービス制御を行う．

図 2 では，alice のサービス *d* と bob のサービス *f* がグループ *g*1 にグルーピングされている．このサービスは，グループ *g*1 に対応付けられたグループ鍵 *GK*1 を所持する EN だけが利用することができる．一方，carol のサービス *d* は ACT によるとグループ “*any*” と設定されている．これは，例えば公開 Web サーバのように誰でもアクセス可能であるノードであることを示しており，どの通信グループにも設定されない．

⋆1 PHN はホームネットワーク内で自由に設定可能であり，外部の DNS に登録する必要はない．

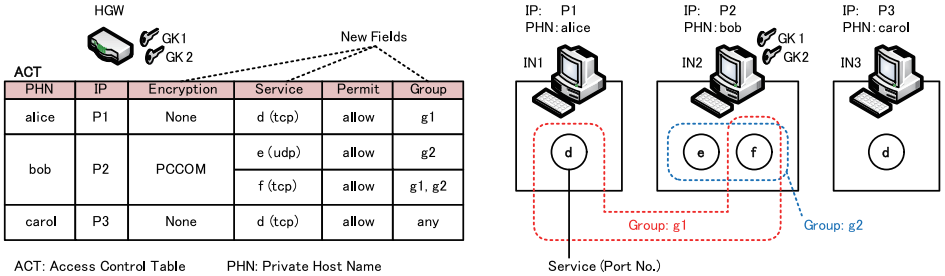


図 2　拡張した ACT とサービスのグルーピング
Fig. 2　Extended Access Control Table and service grouping.

表 1　ノード間の通信可否と暗号化範囲
Table 1　Availability of communication between ENs and INs and its encryption range.

宛先		送信元ノード（所属グループ）		
ノード	サービス	EN1 (*g*1)	EN2 (*g*2)	EN3 (nothing)
IN1	*d*	*E*1 [EN1-HGW]	×	×
IN2	*e*	×	*E*2 [EN2-IN2]	×
IN2	*f*	*E*1 [EN1-IN2]	*E*2 [EN2-IN2]	×
IN3	*d*	*E*1 [EN1-HGW]	*E*2 [EN2-HGW]	*C*

Ex: グループ鍵 *GKx* で暗号化 [始点-終点]　*C*: 平文通信　×: 通信不可

従来の NAT-f システムでは，IN を特別な機能を有さない一般ノードと想定していたため，このような IN にグループ鍵を保持させることができない．そこで提案方式では HGW に全てのグループ鍵を保持させ，かつ ACT に登録された情報を利用することにより，IN を通信グループに所属しているかのように扱う．ただしこの場合，HGW と IN 間の通信は暗号化されず，平文となる．EN から IN までのエンドエンド間を全て暗号化する場合は，IN に提案方式を実装してグループ鍵を保持させることになる．例えば図 2 の設定がされたホームネットワークに対して，グループ *g*1 に属する EN1，グループ *g*2 に属する EN2，および一切のグループ鍵を保持しない EN3 が通信を開始する場合の通信可否は**表 1** のようになる．

3.3 通信シーケンス

前提条件として，EN1，EN2，HGW および IN2 は 1 つのホームネットワークで共通の暗号鍵 *CK* と，各通信グループに対応したグループ鍵 *GK* を保持しているものとし，通信グループの関係は図 2 と表 1 に示したものと仮定する．事前設定として，HGW には図 2 に示した ACT が，また DDNS（Dynamic DNS）サーバには HGW の FQDN “*home.example.net*”

とグローバル IP アドレス $G4$ の対応関係が，ワイルドカード A レコード[14] として登録されているものとする．

3.3.1 IN が PCCOM をサポートしない場合

図 3 に IN が PCCOM をサポートしない場合の通信シーケンスを示す．これは，グループ $g1$ に所属し，グローバル IP アドレス $G1$ が割り当てられた EN1 が IN1 のサービス d にアクセスを開始する場合を想定している．提案方式は以下の 3 フェーズから構成される．

(1) DNS 名前解決

EN1 は HGW の FQDN の先頭に IN1 の PHN を付加した “*alice.home.example.net*” を IN1 の FQDN として，DDNS サーバに対して名前解決を行う．DDNS サーバは IN1 の FQDN に対して，HGW のグローバル IP アドレス $G4$ を回答する．ここで，EN1 の IP 層において，受信した DNS 応答を一時待避してから HGW 宛に Support Check Request を送信する．これは HGW が NAT-f に対応しているかを確認するためのメッセージであり，ノンス値 N_{EN} が記載される．

$$\mathit{Support\ Check\ Request} := N_{EN1} \tag{1}$$

HGW が NAT-f に対応している場合は，Support Check Response を応答する．このメッセージは受信したノンス値 N_{EN1} のハッシュ値と別のノンス値 N_{HGW} を CK で暗号化したものが記載される．

$$\mathit{Support\ Check\ Response} := E(CK, h(N_{EN1}) \mid N_{HGW}) \tag{2}$$

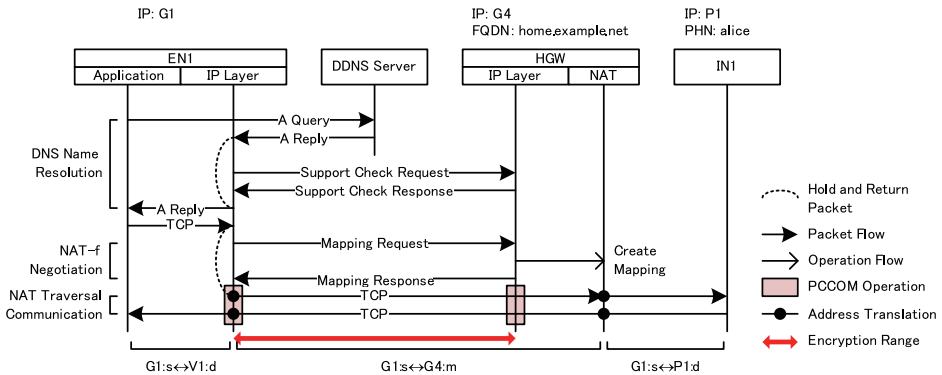


図 3 IN が PCCOM をサポートしない場合の通信シーケンス
Fig. 3 Communication sequence in the case IN does not support PCCOM.

上記メッセージを受信した EN1 は復号後，受信したハッシュ値と自身で計算したハッシュ値 $h(N_{EN1})'$ を比較して，CK の共有を確認する．さらに，待避していた DNS 応答に記載された HGW の IP アドレスを，$G4$ から仮想 IP アドレス $V1$ へ書き換えて上位層へ渡す．このとき，PHN と HGW のグローバル IP アドレス，および仮想 IP アドレスの関係を NRT（Name Relation Table）に記録しておく．これにより，IN1 宛のパケットは宛先を仮想 IP アドレス $V1$ となる．

HGW が NAT-f に対応していない場合は，正しい Support Check Response が応答されないため[⋆1]，EN1 は待避していた DNS 応答をそのまま上位層へ渡す．この場合，以下のフェーズは実行されないため，NAT-f による NAT 越えは行われない．

(2) マッピングネゴシエーション

アプリケーションが IN1 のサービス d 宛に通信を開始すると，IP 層には送信元 “$G1 : s$”，宛先 “$V1 : d$” の TCP パケットが渡される．ここで宛先が仮想 IP アドレスの場合，VAT（Virtual Address Translation）テーブルを検索する．最初は該当エントリが存在しないため，送信パケットを一時待避させてから Mapping Request を HGW へ送信する．これは HGW に対して IN1 との通信に必要な NAT マッピングの生成を要求するメッセージであり，提案方式では既存の NAT-f の Mapping Request の情報に加え，EN1 のグループ情報を付与して通知する．

$$\mathit{Mapping\ Request} := E(CK, G1 \mid s \mid V1 \mid d \mid tcp \mid alice \mid g1 \mid E(GK1, h(N_{HGW}))) \tag{3}$$

Mapping Request を受信した HGW は，受信した PHN をキーとして ACT をチェックする．該当エントリの Permit が “*allow*” で，かつ Service と Group が一致したら，グループ鍵 $GK1$ で復号して取得したハッシュ値と自身で計算した $h(N_{HGW})'$ を比較して，$GK1$ の共有を確認する．次に，取得した通信識別子と IN1 のプライベート IP アドレスを用いて，NAT マッピングを生成する．

$$\mathit{NAT}: \quad G1 : s \leftrightarrow \{G4 : m \Leftrightarrow P1 : d\} \quad [tcp] \tag{4}$$

これは IN1 のポート番号 d と HGW のポート番号 m がマッピングされたことを示しており，“$G4 : m$” をマッピングアドレスと呼ぶ．さらに提案方式では，EN1 からマッピングアドレス宛のパケットを $GK1$ で復号するような PIT を生成する．HGW は上記マッピングアドレスと一致した通信グループ番号を Mapping Response により応答する．

$$\mathit{Mapping\ Response} := E(CK, G1 \mid s \mid V1 \mid d \mid tcp \mid g1 \mid E(GK1, G4 \mid m)) \tag{5}$$

⋆1 NAT-f 制御メッセージは ICMP Echo をベースに定義されている．従って NAT-f 非対応ノードが本メッセージを受信したら，Request と同じ内容の ICMP Echo Reply を応答する．

EN1 は受信した Mapping Response を復号後，記載されている情報から VAT テーブルを生成する．

$$VAT: \quad G1:s \leftrightarrow \{V1:d \Leftrightarrow G4:m\} \quad [tcp] \tag{6}$$

これは仮想的に認識した IN1 のトランスポートアドレス “$V1:d$” 宛の通信を HGW のマッピングアドレス “$G4:m$” にマッピングすることを示している．さらに提案方式では，EN1 からマッピングアドレス宛のパケットを $GK1$ で暗号化するような PIT を生成する．以上で NAT-f によるネゴシエーションを完了し，先ほど待避していた送信パケットを復帰する．

(3) 仮想アドレス変換

以後，EN1 から IN1 のサービス d 宛の TCP パケットは，EN1 において VAT テーブルに基づくアドレス変換処理により，宛先が “$V1:d$” から “$G4:m$” に変換される．このパケットは PIT に基づいて $GK1$ で暗号化されてから，HGW へ送信される．HGW では上記パケットを復号後，NAT により宛先を “$G4:m$” から “$P1:d$” に変換してから IN1 へ転送する．

以上の手順により，EN1 から IN1 へのアクセスを実現できる．IN1 から EN1 への応答は上記と逆の順序により，アドレス変換処理および暗号化処理が行われる．

3.3.2 IN が PCCOM をサポートする場合

図 4 に IN が PCCOM をサポートする場合の通信シーケンスを示す．これは，グループ $g2$ に所属し，グローバル IP アドレス $G2$ が割り当てられた EN2 が IN2 のサービス e にアクセスを開始する場合を想定している．

EN2 は 3.3.1 項と同様に，“$bob.home.example.net$” により IN2 の名前解決を行い，アプリケーションには仮想 IP アドレス $V2$ を通知する．その後，送信元 “$G2:t$”，宛先 “$V2:e$” の UDP パケット送信をトリガに，HGW に Mapping Request を送信する．

HGW も前述した通り，ACT をチェックする．ここで，該当する IN が暗号化機能をサポートしているため，新たに定義した PIT Request を IN2 へ送信する．これは IN2 に対して EN2 との暗号化通信に必要な PIT の生成を要求するメッセージであり，Mapping Request に記載されていた EN2 のグループ情報などが記載される．

$$PIT\ Request := E(CK, G2 \mid t \mid P2 \mid e \mid udp \mid N_{HGW} \mid g2 \mid E(GK2, h(N_{HGW}))) \tag{7}$$

上記メッセージを受信した IN2 は CK により復号後，グループ鍵 $GK2$ で復号して取得したハッシュ値と自身で計算した $h(N_{HGW})'$ を比較して，$GK2$ の共有を確認する．グループ鍵の共有を確認したら，IN2 は EN2 からサービス e 宛のパケットを $GK2$ で復号することを示す PIT を生成して，PIT Response を応答する．

$$PIT\ Response := E(CK, G2 \mid t \mid P2 \mid e \mid udp \mid g2 \mid E(GK2, h(N_{HGW}) \mid proc)) \tag{8}$$

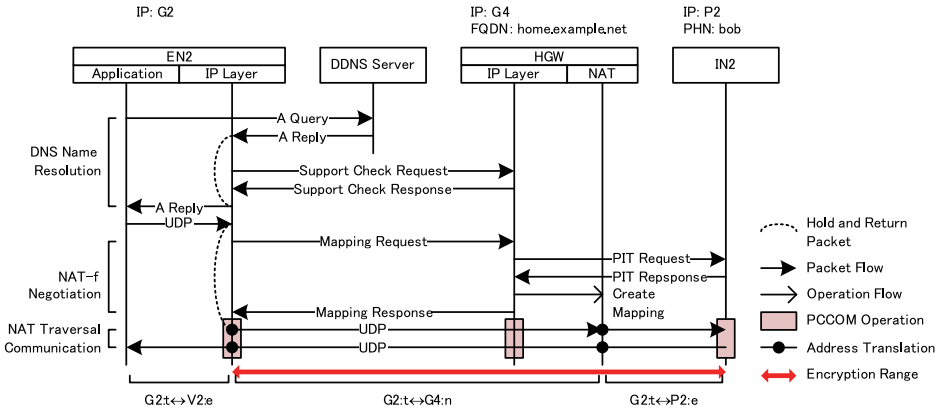


図 4 IN が PCCOM をサポートする場合の通信シーケンス
Fig. 4 Communication sequence in the case IN supports PCCOM.

ここで，$proc$ には HGW における動作処理情報が記載されるが，ここでは「何も処理ない」ことが設定される．

PIT Response を受信した HGW は，ハッシュ値の比較により $GK2$ の共有を確認してから，記載されている情報から NAT マッピングを生成する．

$$NAT: \quad G2:t \leftrightarrow \{G4:n \Leftrightarrow P2:e\} \quad [udp] \tag{9}$$

さらに通知された $proc$ に示された通り，EN2 からマッピングアドレス “$G4:n$” 宛の UDP パケットを何も処理しないことを示す PIT を生成してから，Mapping Response を応答する．

EN2 は HGW からの応答に基づいて，VAT テーブルを生成する．

$$VAT: \quad G2:t \leftrightarrow \{V2:e \Leftrightarrow G4:n\} \quad [udp] \tag{10}$$

その後，マッピングアドレス宛の UDP パケットを $GK2$ で暗号化するような PIT を生成する．

以後，EN2 から IN2 のサービス e 宛の UDP パケットは，EN2 において VAT テーブルに基づくアドレス変換処理により，宛先が “$V2:e$” から “$G4:n$” に変換される．このパケットは PIT に基づいて $GK2$ で暗号化されてから，HGW へ送信される．HGW では上記パケットを暗号化されたまま，NAT により宛先を “$G4:n$” から “$P2:e$” に変換してから IN2 へ転送する．IN2 は PIT に基づいて，受信パケットを $GK2$ により復号する．

以上の手順により，EN2 から IN2 へのアクセス開始と，NAT を挟んだエンドエンドの暗号化通信を実現できる．

4. 考　　察

4.1 セキュリティ

提案方式では，本機能を実装している機器はグループ鍵に加えて共通暗号鍵 *CK* を保持している．NAT-f 制御メッセージは Support Check Request 以外は全て暗号化されるため，EN と HGW 間および HGW と暗号機能を実装した IN 間で交換される情報の安全性は保証される．*CK* は 1 つのホームネットワークで共通な暗号鍵であるため，一般にホームネットワーク内のユーザのみが保持することになる．例えば，友人など家族とは異なる第三者に対して，自宅の通信グループに所属させて IN のサービスを提供する場合は，第三者にも *CK* を配布する必要がある．ただし，この場合は第三者により制御メッセージの情報を盗聴される危険性がある．

このようなリスクも回避するためには，*CK* をホームネットワークごとに対応させるのではなく，EN，HGW および IN の各装置間に個別の共通鍵を割り当てる方法や，通信開始時に Diffie-Hellman 鍵交換[15] を行って個別のセッション鍵を共有する方法などが考えられる．ただし，前者は鍵の管理が煩雑になってしまう課題が，後者は中間者攻撃に対して脆弱性が生じるなどの課題が残る．

提案方式は通信グループの認証機能を有しているが，これは NAT マッピングの生成時点だけ行われる．従って，正規の手順により生成された NAT マッピングを利用して，通信グループ外の第三者が IN のサービスを利用することも考えられる．このようなリスクを回避するためには，HGW が採用する NAT の種類を限定する方法やファイアウォールと連携する方法などが考えられる．

NAT にはマッピングの管理や生成方法の違いにより 4 つのタイプ[⋆1]が存在するが，このうち Full Cone NAT のときのみ第三者からの通信を無条件で内部へ転送してしまう．従って，Full Cone NAT 以外の NAT を選択すれば上記のような問題は発生しない．なお，NAT-f は全てのタイプの NAT に対応することが可能である．

一般に NAT とファイアウォールは連動して処理が行われる．そこで，Mapping ネゴシエーションを正しく完了した EN からのアクセスだけを通過させるようなフィルタリングを動的に設定することにより対処可能である．

⋆1 Full Cone NAT，Restricted Cone NAT，Port Restricted Cone NAT，Symmetric NAT がある．前者から後者に向かって NAT 越えの難易度が高くなる．

4.2 利用シーン

提案方式はホームネットワーク内の様々なシステムに応用することが可能である．近年，DLNA（Digital Living Network Alliance）[16] に対応した情報家電機器が充実しつつあり，外出先からこれらの機器に保存されたコンテンツを利用する様々な方式が提案されている[17),18)]．筆者らも文献 19) において NAT-f をベースとした遠隔 DLNA 通信方式を提案しており，本提案方式と組み合わせることにより**図 5** のようにホームネットワーク内のマルチメディアコンテンツを，特定の外部ノードに限定して利用させることができる．

また情報家電機器の増加に伴い，ユーザの機器管理負荷が増加することが想定される．そこで，機器ベンダーがインターネットを介してユーザが購入した機器を遠隔でメンテナンスするサービスがある．このようなサービスをグルーピングすることにより，ユーザは安全かつ容易に機器のメンテナンスを委託することも可能と考えられる．

提案方式はホームネットワークに限らず，企業や大学ネットワークに対しても利用可能である．例えば IPsec や SSH を利用した VPN では，リモートユーザの管理や外部からアクセス可能なサービスをコントロールすることが難しいが，提案方式ではユーザが所属する部門や役職に応じてサービスをグルーピングすることにより，柔軟なリモートアクセス環境を構築することにも応用できる．

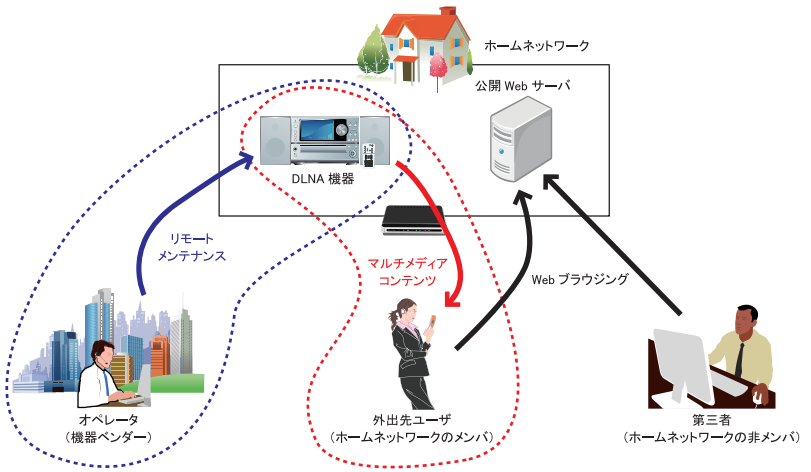


図 5　ホームネットワークにおける利用シーンの一例
Fig. 5　Example usage for home networks.

5. ま と め

本稿では，従来の NAT-f に通信グループの概念と暗号化通信を導入した新しい NAT 越えシステムを提案した．サービス単位でグルーピングすることにより，外部からのアクセス制御と内部のサービス制御を同時に実現できることを示した．

今後は提案方式の実装と評価を行い，有効性を確認するとともに，実運用に向けた準備を行う予定である．

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) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
2) Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, IETF (1999).
3) Srisuresh, P., Ford, B. and Kegel, D.: State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs), RFC 5128, IETF (2008).
4) Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
5) Rosenberg, J., Mahy, R. and Matthews, P.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), Internet-draft, IETF (2009). http://tools.ietf.org/id/draft-ietf-behave-turn-14.txt
6) Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, Internet-draft, IETF (2007). http://www.ietf.org/internet-drafts/draft-ietf-mmusic-ice-19.txt
7) UPnP Forum: *Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp
8) 鈴木秀和，宇佐見庄五，渡邊 晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌，Vol.48, No.12, pp.3949–3961 (2007).
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 の実装と評価，情報処理学会論文誌，Vol.47, No.11, pp.2976–2991 (2006).
10) 渡邊 晃，厚井裕司，井手口哲夫，横山幸雄，妹尾尚一郎：暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌，Vol.38, No.4, pp.904–914 (1997).
11) Kent, S.: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).
12) 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).
13) Huttunen, A., Swander, B., Volpe, V., DiBurro, L. and Stenberg, M.: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).
14) Lewis, E.: The Role of Wildcards in the Domain Name System, RFC 4592, IETF (2006).
15) Diffie, W. and Hellman, M.: New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.644–654 (1976).
16) Digital Living Network Alliance: *DLNA Networked Device Interoperability Guidelines Expanded* (2006). http://www.dlna.org/
17) 武藤大悟，吉永 努：ルールベースアクセス制御機能を持つ DLNA 情報家電の遠隔共有支援機構，情報処理学会論文誌，Vol.49, No.12, pp.3985–3996 (2008).
18) Oh, Y.J., Lee, H.K., Kim, J.T., Paik, E.H. and Park, K.R.: Design of an Extended Architecture for Sharing DLNA Compliant Home Media from Outside the Home, *IEEE Transactions on Consumer Electronics*, Vol.53, No.2, pp.542–547 (2007).
19) 鈴木秀和，渡邊 晃：NAT-f を用いたホームネットワーク間相互接続方式の検討，マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム論文集，Vol.2008, No.1, pp.1675–1682 (2008).

付 録

A.1 記号の定義

- Gi; グローバル IP アドレス
- Pi; プライベート IP アドレス
- Vi; 仮想 IP アドレス
- $A:p$; トランスポートアドレス（IP アドレス A とポート番号 p の組）
- gx; 通信グループ番号 x
- GKx; 通信グループ gx に対応するグループ鍵
- CK; 1 つのホームネットワークにおける共通鍵
- Nn; ノード n が生成したノンス値
- $x \mid y$; データ x と y の連結
- $h(x)$; データ x のハッシュ値
- $E(k,m)$; 暗号鍵 k でメッセージ m を暗号化
- $S \leftrightarrow D$; S と D 間の通信
- $\{S \Leftrightarrow D\}$; S から D，または D から S へのアドレス変換

Watanabe Lab.
Department of Information Engineering, Meijo University
Information Networks Laboratory

通信グループに基づく サービスの制御が可能なNAT越えシステム

鈴木　秀和†‡　　渡邊　晃†

†名城大学大学院理工学研究科

‡日本学術振興会特別研究員PD

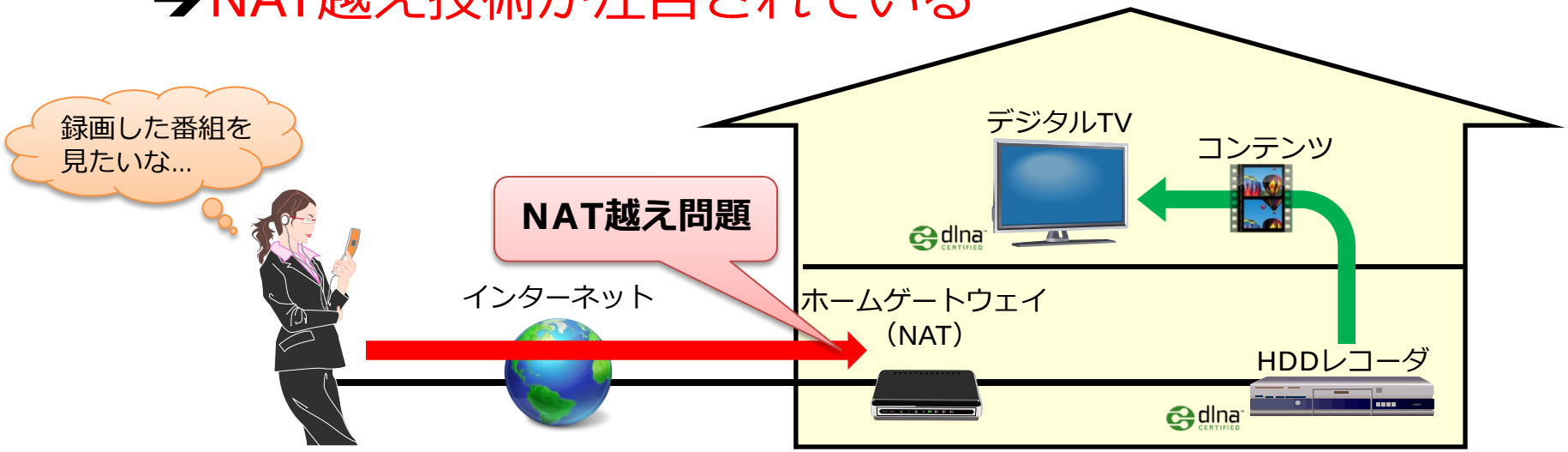
研究背景

- **ホームネットワークの充実**
  - 家庭内におけるデジタルコンテンツの共有

  ➔外出先からでもシームレスに利用したい要求が高まる

- **IPv4ネットワークにおける課題**
  - NATが存在するため外から中に通信を開始できない

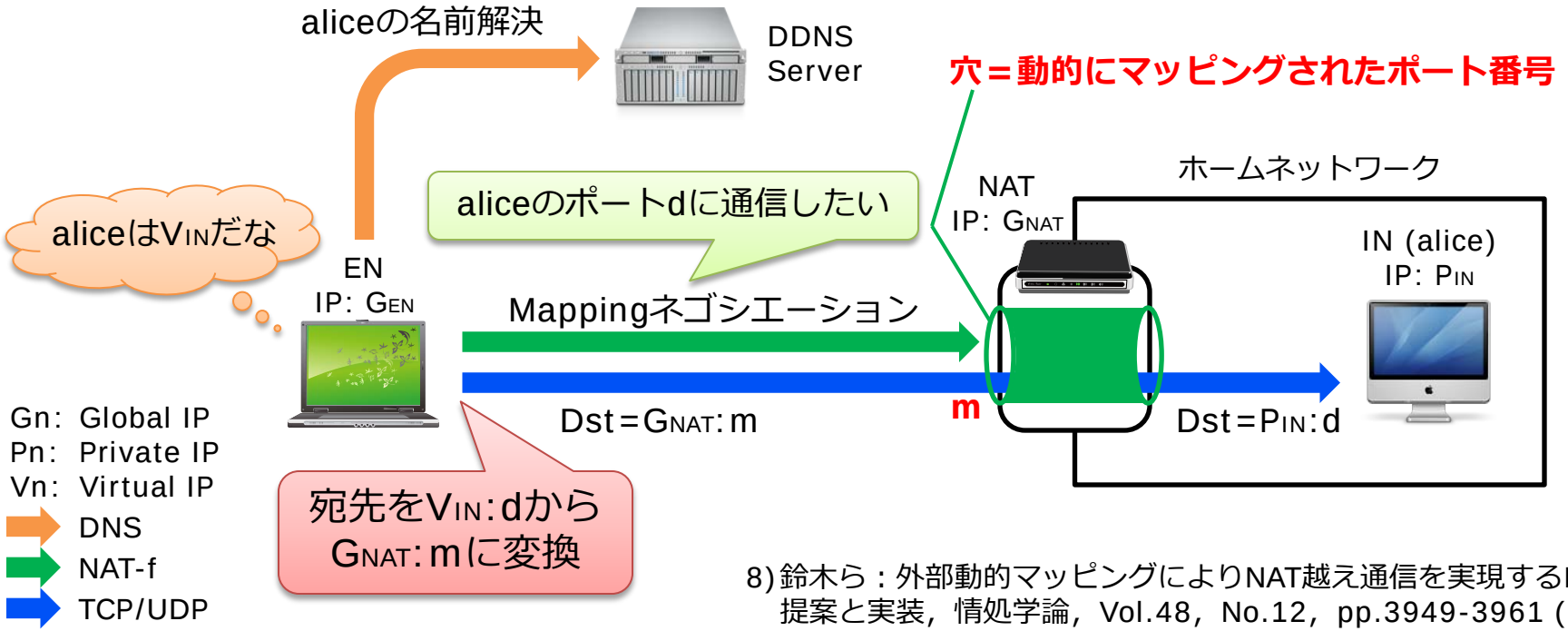
  ➔NAT越え技術が注目されている



NAT-f（NAT-free protocol）

DDNS: Dynamic DNS

- **ネットワークレベルのNAT越え技術**
  - INを仮想的に認識
  - オンデマンドに外からNATに穴を開ける（マッピング作成）
  - ENは仮想的な宛先を開けた穴の情報に変換



8) 鈴木ら：外部動的マッピングによりNAT越え通信を実現するNAT-fの提案と実装，情処学論，Vol.48，No.12，pp.3949-3961 (2007)

NAT-fの課題

- **NATを越えるための手段を提供**
  - セキュリティに関しては十分な検討が行われていない
- **無条件でNATマッピングの生成が可能**
- **生成したNATマッピングは誰でも利用可能**
  - **誰でも外部からINと通信できてしまう**
    - 安全性，プライバシー，著作権等の観点からも好ましくない

既存のNAT-fシステムにセキュリティ技術を適用することにより，上記課題を解決する

提案方式の概要

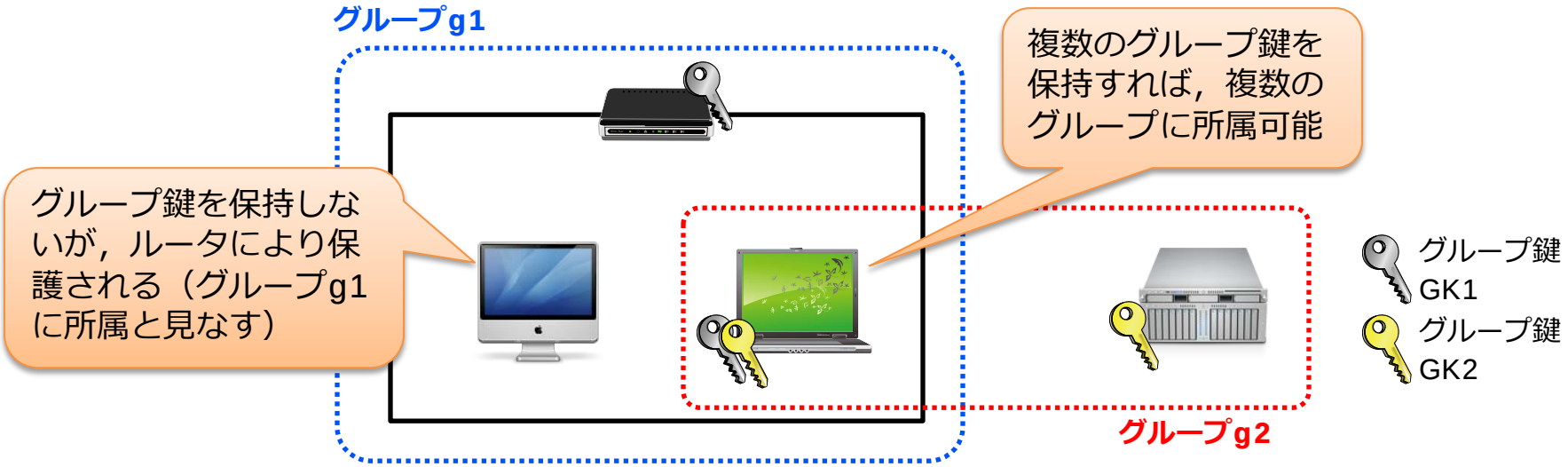
HGW: Home Gateway

- **通信グループの導入**
  - HGWにおけるアクセス制御
  - 外部に公開するサービスの柔軟な制御
  - ENとHGW間（またはENとIN間）の暗号化通信

- **通信グループの概念を拡張**
- **NAT-fシーケンスを拡張**
  - グループ認証に必要な情報を交換メッセージに追加
  - 暗号化通信に必要な動作処理情報の生成機能を追加

通信グループの構築方法

- **エリア定義方式**
  - 特定の属性に基づいてユーザやネットワークをグループ化
  - 通信グループと暗号鍵（グループ鍵）を1対1に対応
  - 同一通信グループ内のメンバ間は暗号化通信



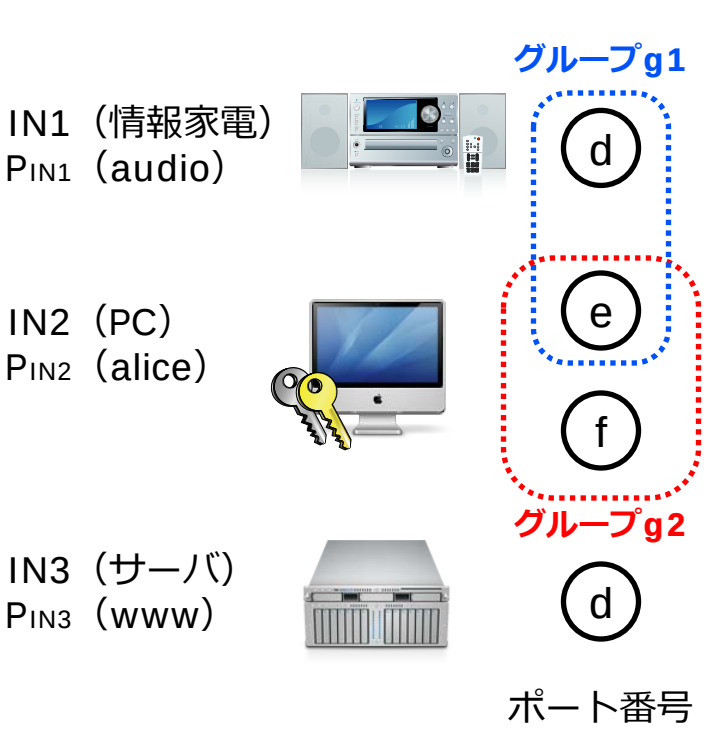
10)渡邊ら：暗号技術を用いたセキュア通信グループの構築方法とその実現，情処学論，Vol.38，No.4，pp.904-914 (1997)

グルーピング概念の拡張

ACT: Access Control Table
PHN: Private Host Name
PCCOM: Practical Cipher Communication

サービス単位のグルーピング

- HGWのアクセス制御テーブル**ACT**に情報を追加
  - 暗号化機能の有無，サービス（ポート番号），グループ番号



HGW

ACT

追加部分

PHN	IP	暗号化機能	サービス	グループ
audio	PIN1	None	d (tcp)	g1
alice	PIN2	PCCOM	e (udp)	g1,g2
			f (tcp)	g2
www	PIN3	None	d (tcp)	any

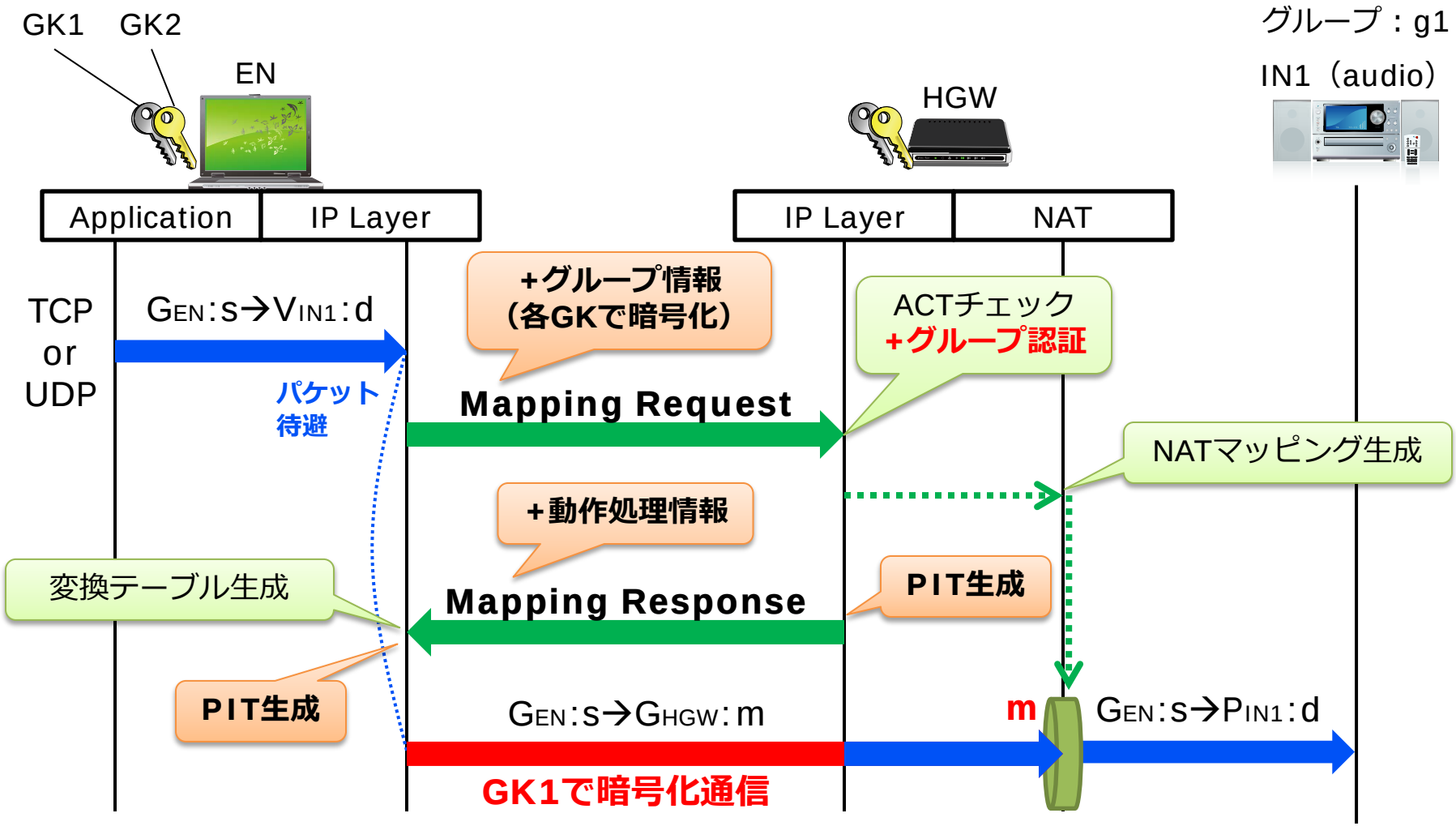
誰でもアクセス可能にする場合に設定

12)増田ら：NATやファイアウォールと共存できる暗号化通信方式PCCOMの提案と実装，情処学論，Vol.47，No.7，pp.2258-2266 (2006)

提案システムのシーケンス概略

- **INが暗号化機能をサポートしない場合**

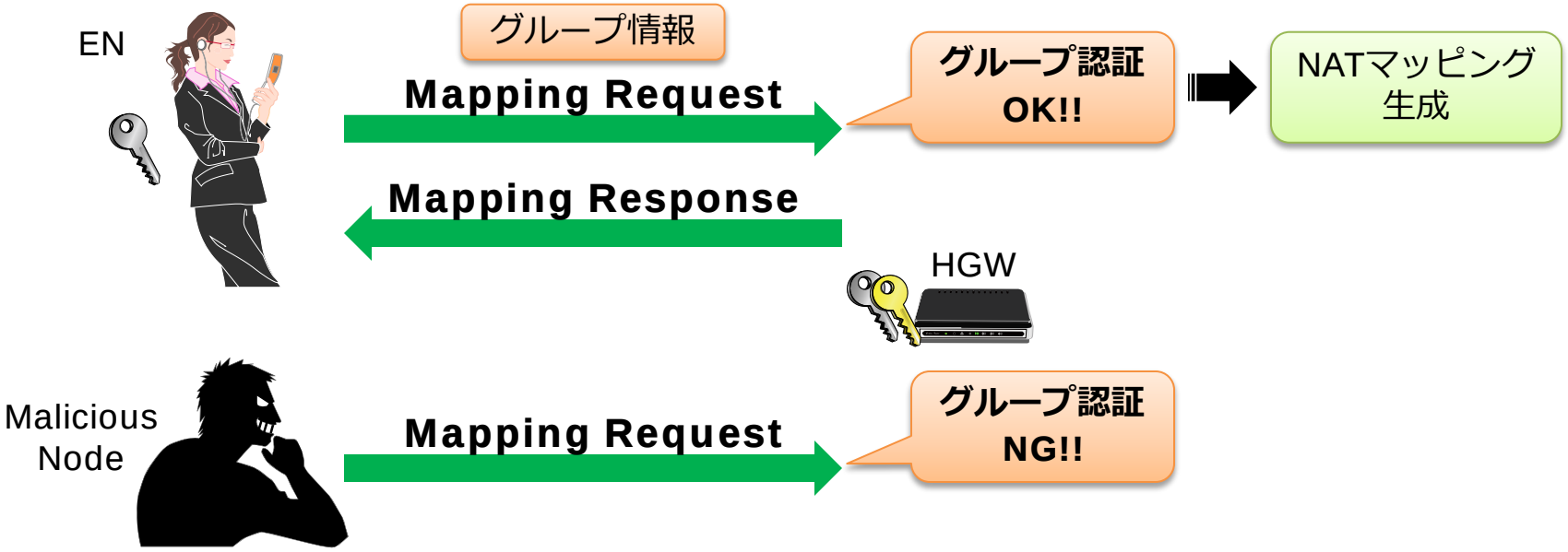
PIT: Process Information Table



セキュリティに関する考察 (1)

- **誰でもNATマッピングを生成できる？**

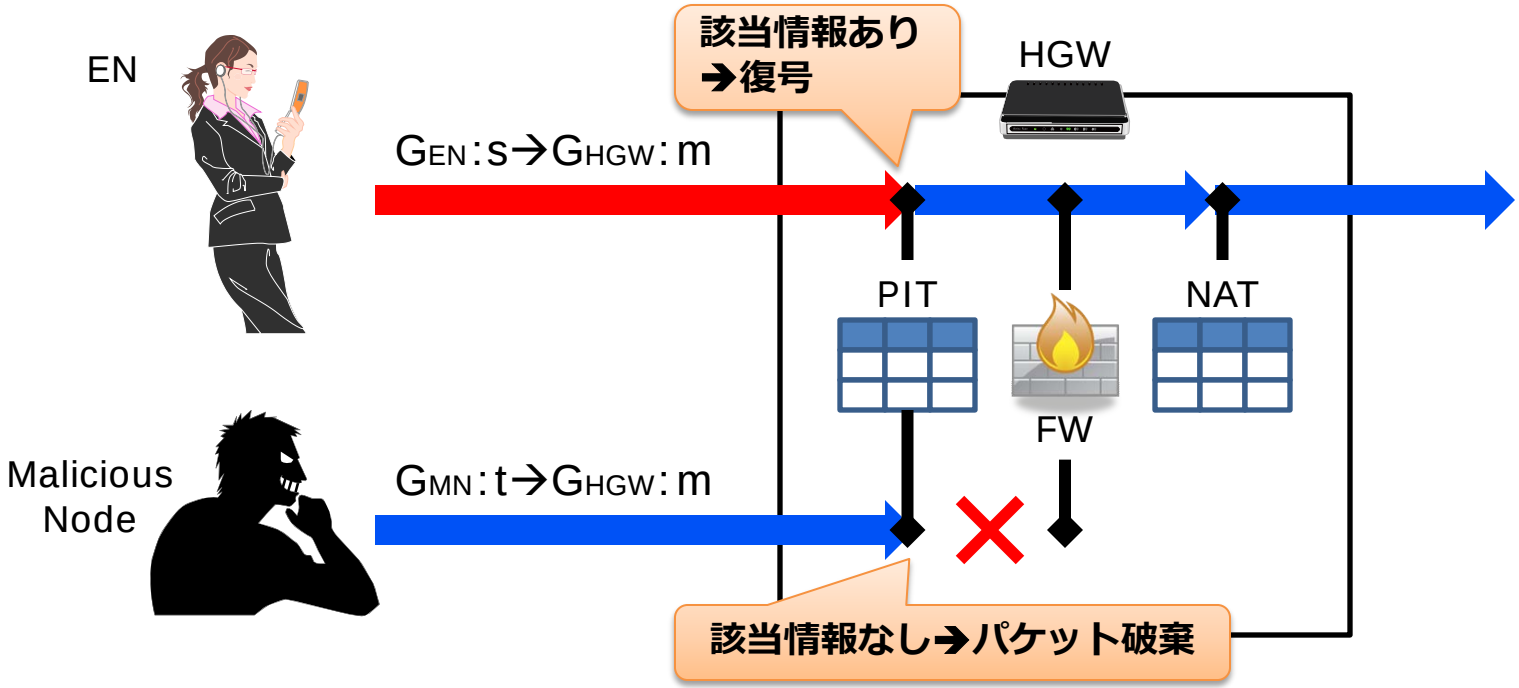
  ➔HGWと同一の暗号鍵を持つユーザしか生成できない
  （不特定多数に公開するノードが対象の場合は除く）



Mapping Requestに追加したグループ情報にはノンス値を含む
➔正規のメッセージを盗聴して再送しても認証は成功しない

セキュリティに関する考察 (2)

- **生成されたNATマッピングは誰でも利用可能？**
  ➔NATマッピングを作成したユーザのみ利用可能

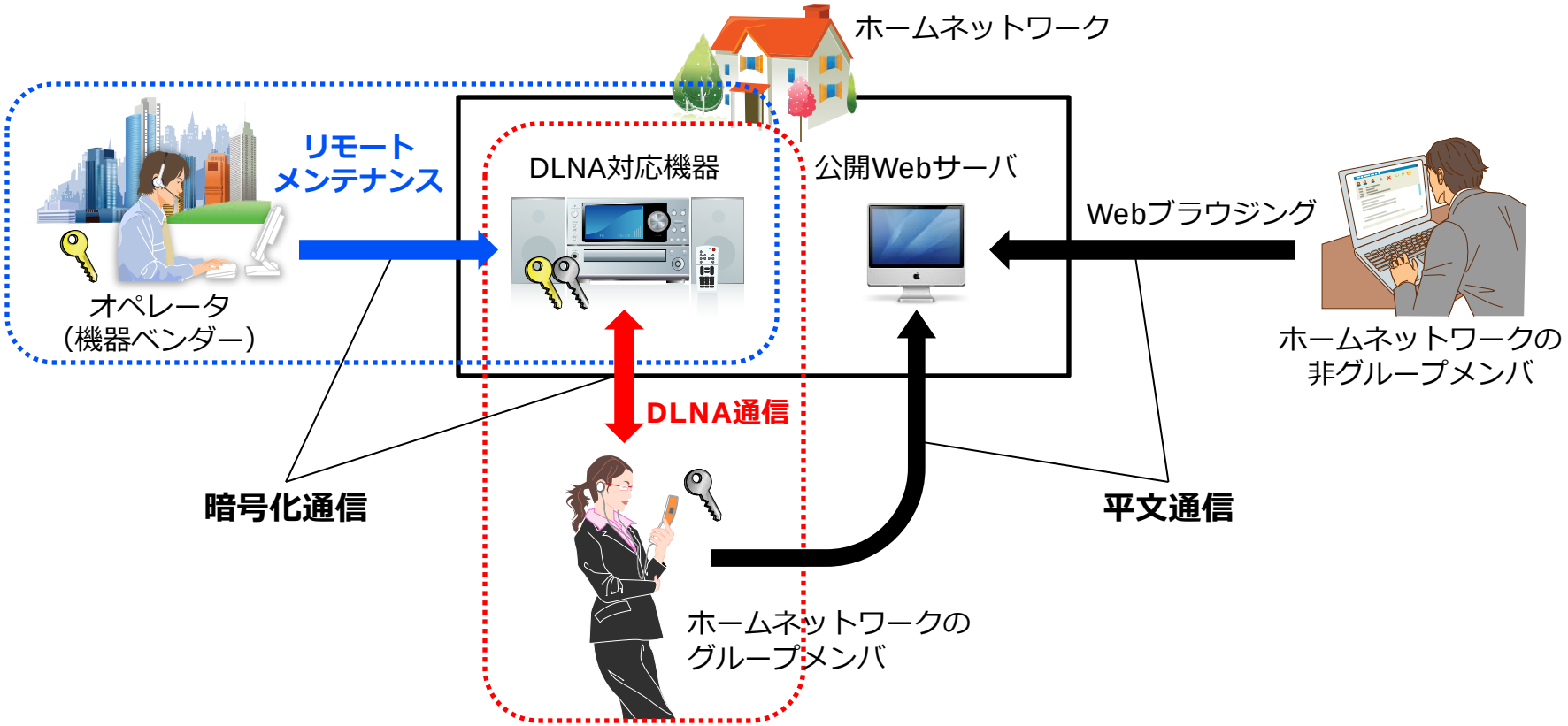


送信元IPアドレス・ポート番号を偽装
➔Ingress Filteringで悪意あるノード側のネットワークで破棄
➔暗号化機能におけるパケットの検証過程で異常の発見が可能

利用シーン

DLNA: Digital Living Network Alliance

- 遠隔DLNA通信
- 機器ベンダーによる遠隔メンテナンスサービス
- 企業や大学ネットワークへのリモートアクセス



まとめ

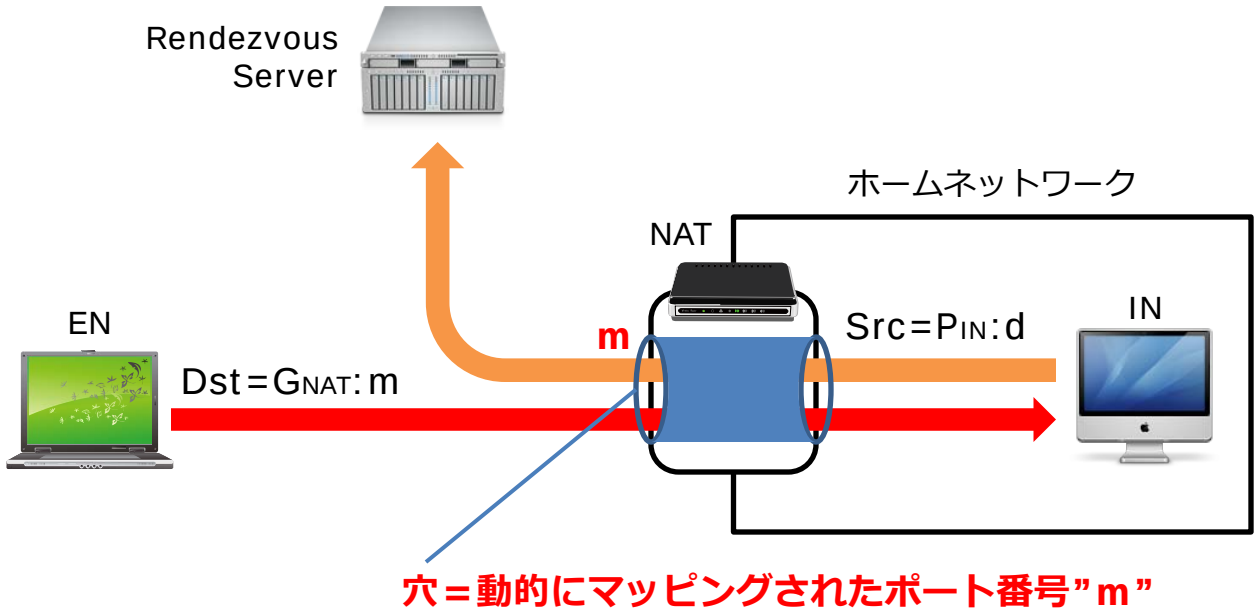
- **NAT-fを拡張したNAT越えシステムを提案**
  - 通信グループの導入とグルーピング単位の拡張
    - 強力なアクセス制御
    - 柔軟なサービス制御
    - 暗号化通信
- **今後の予定**
  - 実装システムの評価と有効性の確認
  - 実運用に向けた準備

付録

NAT越え技術

EN: External Node
IN: Internal Node

- **POINT**
  - 通信開始前にNATに穴を開ける（マッピング作成）
  - ENは開けられた穴の情報を取得
  - ENは穴に向けてパケットを送信すればINと通信可能



- NAT越え技術
  - STUN
  - TURN
  - UPnP
  - ICE

  etc...

NAT-fの事前準備

- Dynamic DNSサーバ
  - RR (Resource Record)
    - HGWのホスト名とグローバルIPアドレスの関係をワイルドカードで登録

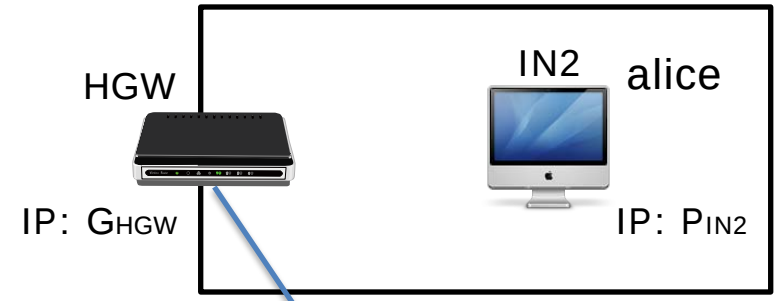
DDNS
(example.net)

RR

Name	IP Address
*.home	G_{HGW}

- HGW
  - **ACT (Access Control Table)**
    - INのホスト名とプライベートIPアドレスの関係を保持

home.example.net



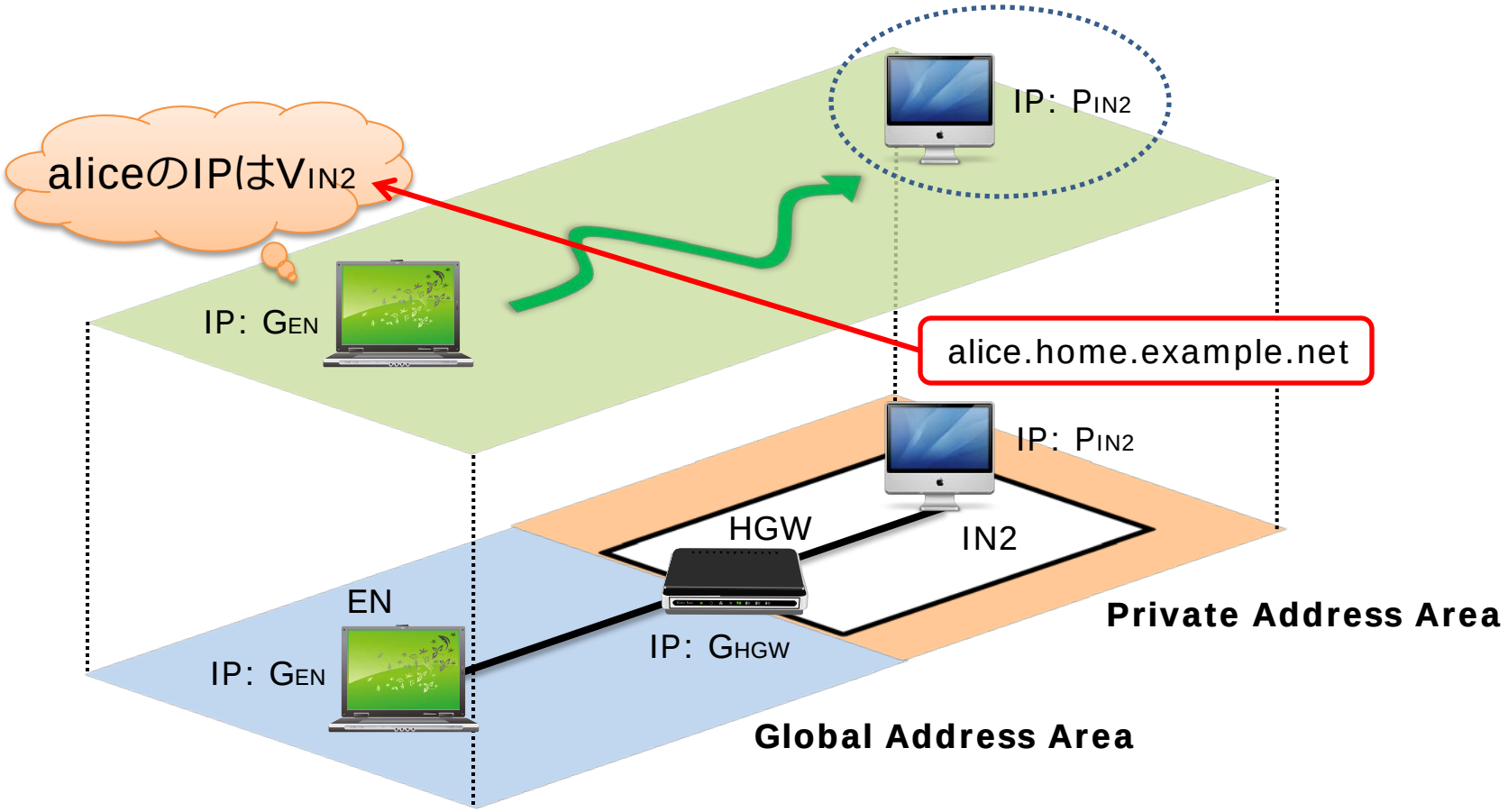
ACT

Name	IP Address
alice	P_{IN2}

INの認識方法

FQDN: Fully Qualified Domain Name

- 仮想的に認識
  - INのFQDNから動的に**仮想IPアドレス**を生成



仮想アドレスの生成方法

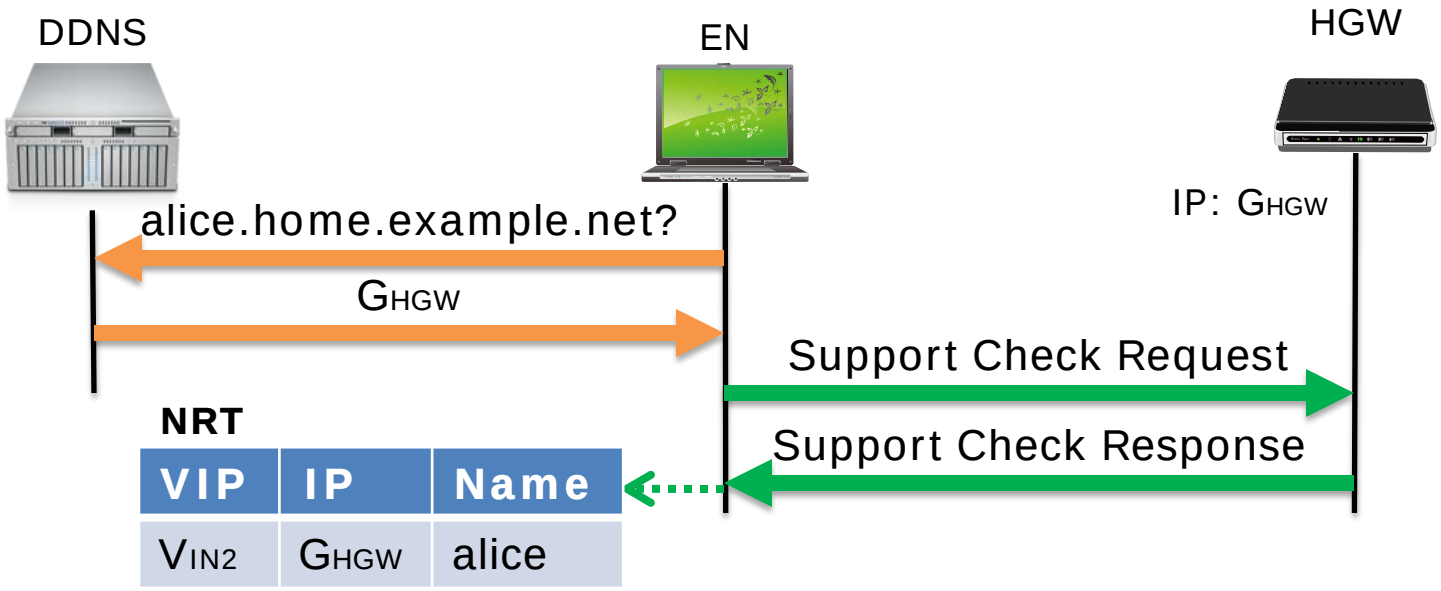
- 通信相手のFQDNから生成

仮想アドレス＝A.B.C.D

- A＝仮想アドレスと識別するための値
  - ENにとってリーチャビリティがなければなんでもよい
  - トライアルシステムでは，「10」or「240」を利用
- B＝初期値はゼロ
  - アドレスの衝突が発生したら変化させる
- C＝ドメイン名のハッシュ値（home.example.net）
- D=ホスト名のハッシュ値（audio）

NAT-f (Ph.1): DNS名前解決

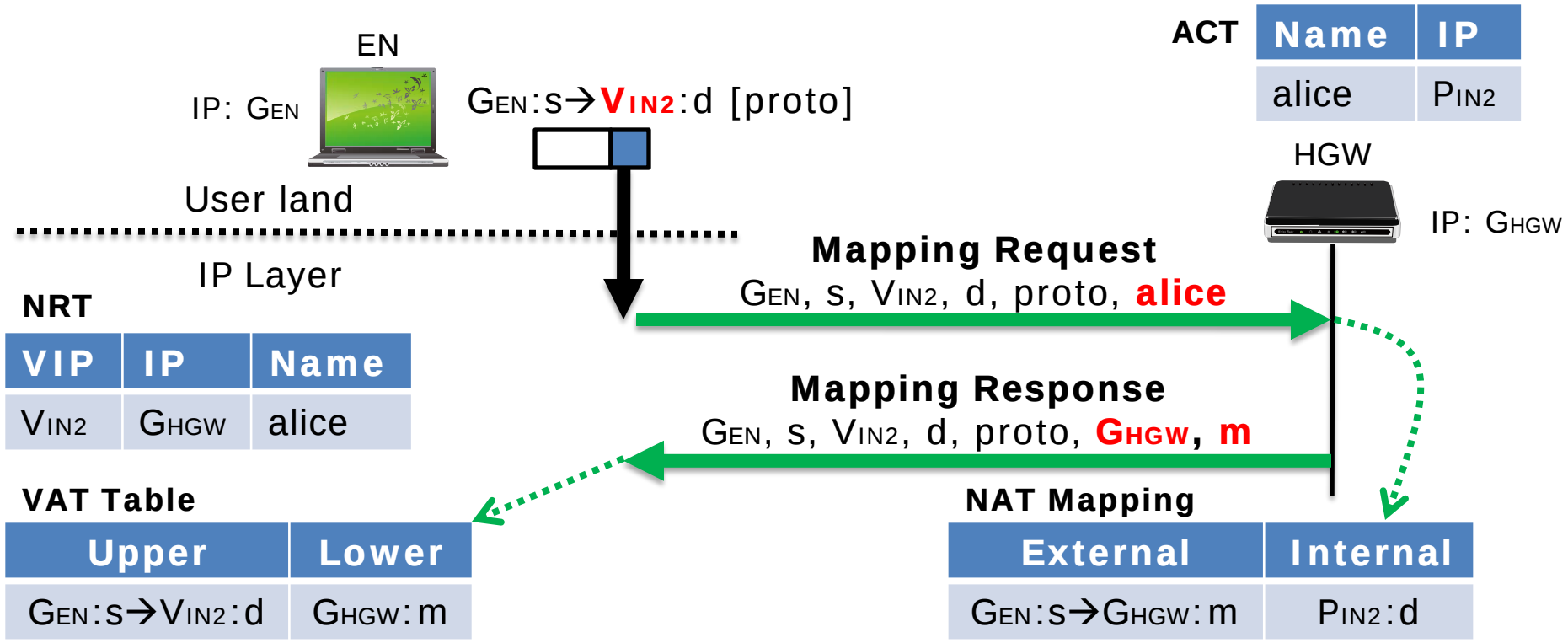
- DDNSサーバに問い合わせ
- Support Checkメッセージを送信
  - HGWがNAT-fに対応しているか確認
    - HGWの場合➔**仮想IPアドレスに書き換え**
      - **NRT (Name Relation Table)**にキャッシュ



NAT-f (Ph.2): マッピング

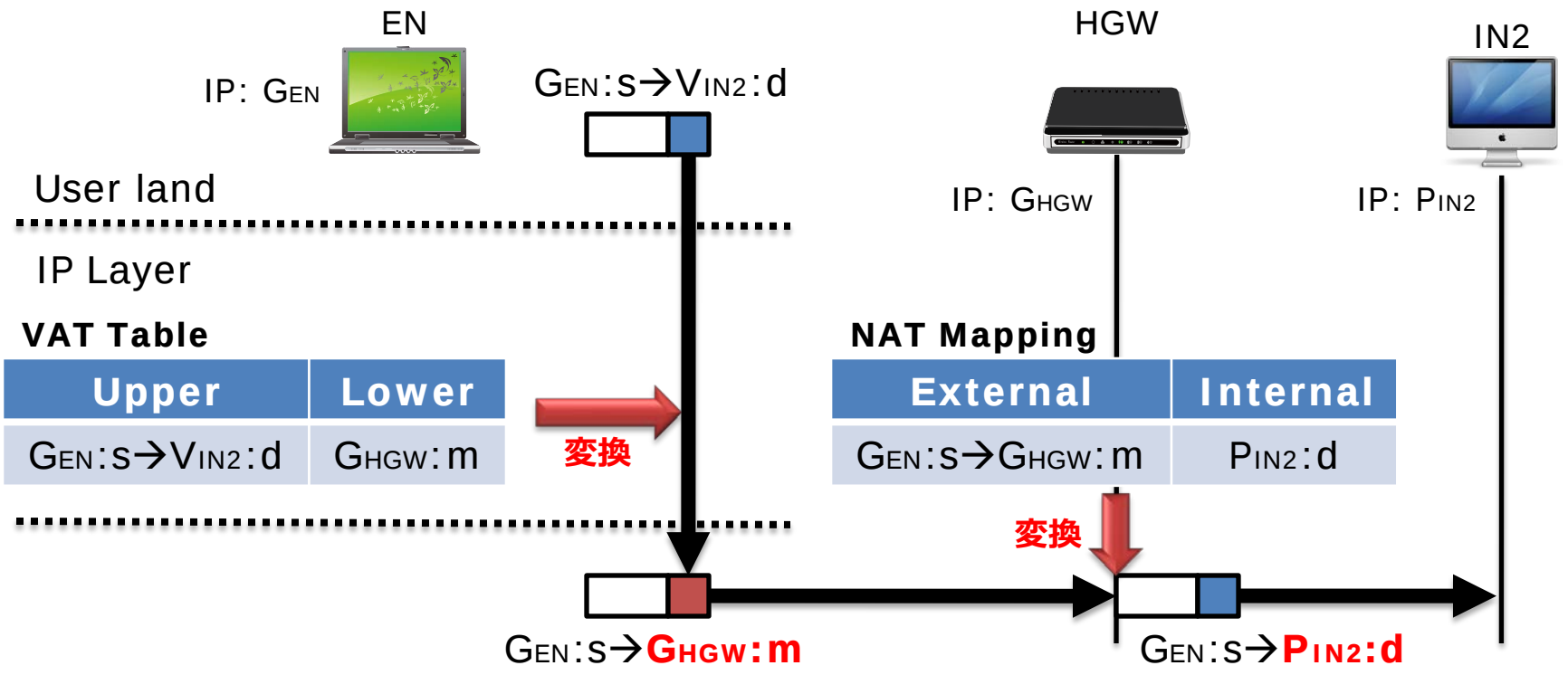
VAT: Virtual Address Translation

- HGWはマッピング情報生成（G_{HGW}:m）
- ENはVATテーブルを生成
  - 仮想IPアドレスとマッピングアドレスの変換関係



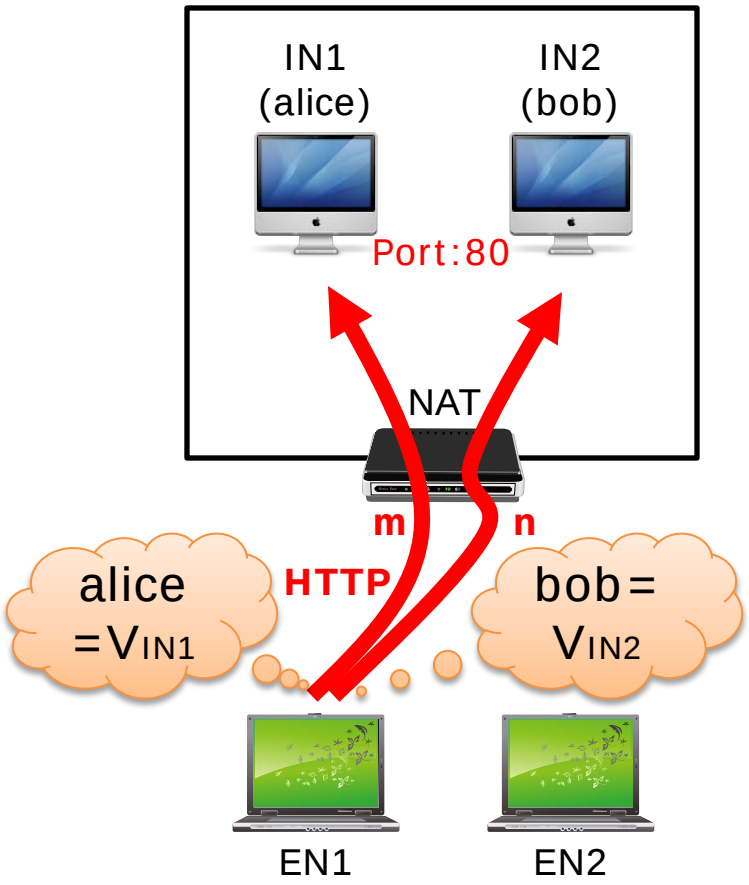
NAT-f (Ph.3): 仮想アドレス変換

- 2回のアドレス変換
  - VAT処理@EN，NAT処理@HGW
- INからの応答は逆の変換を実施

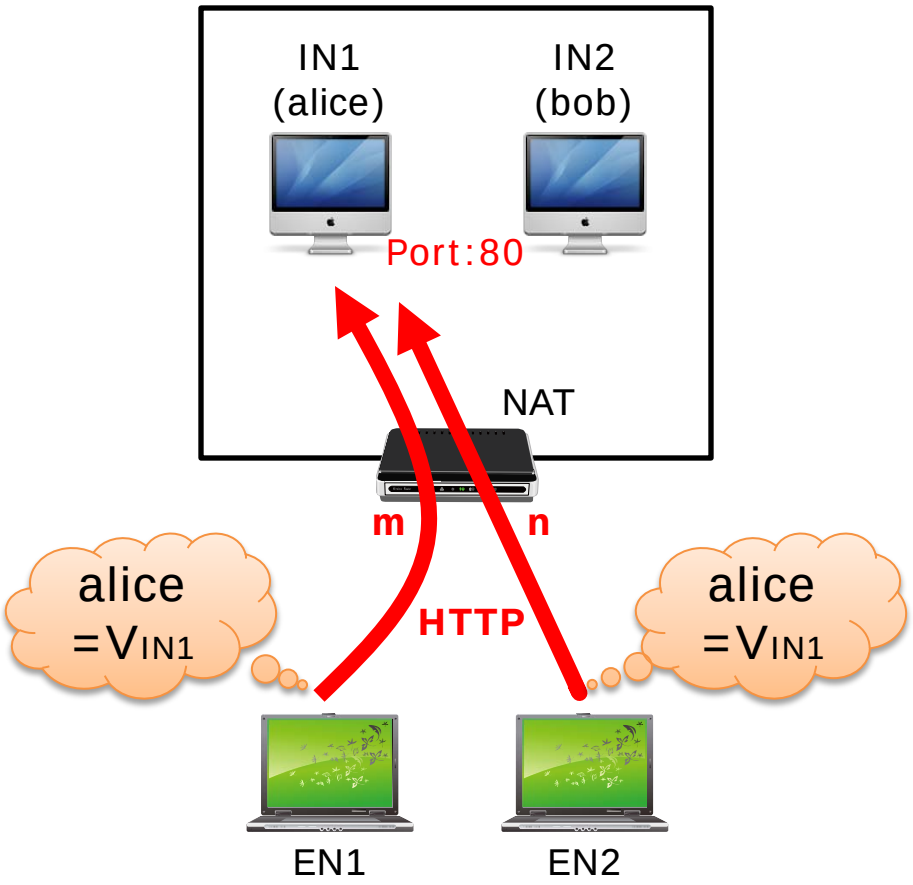


同時通信

- 複数のINに対して同一ポートの通信が可能

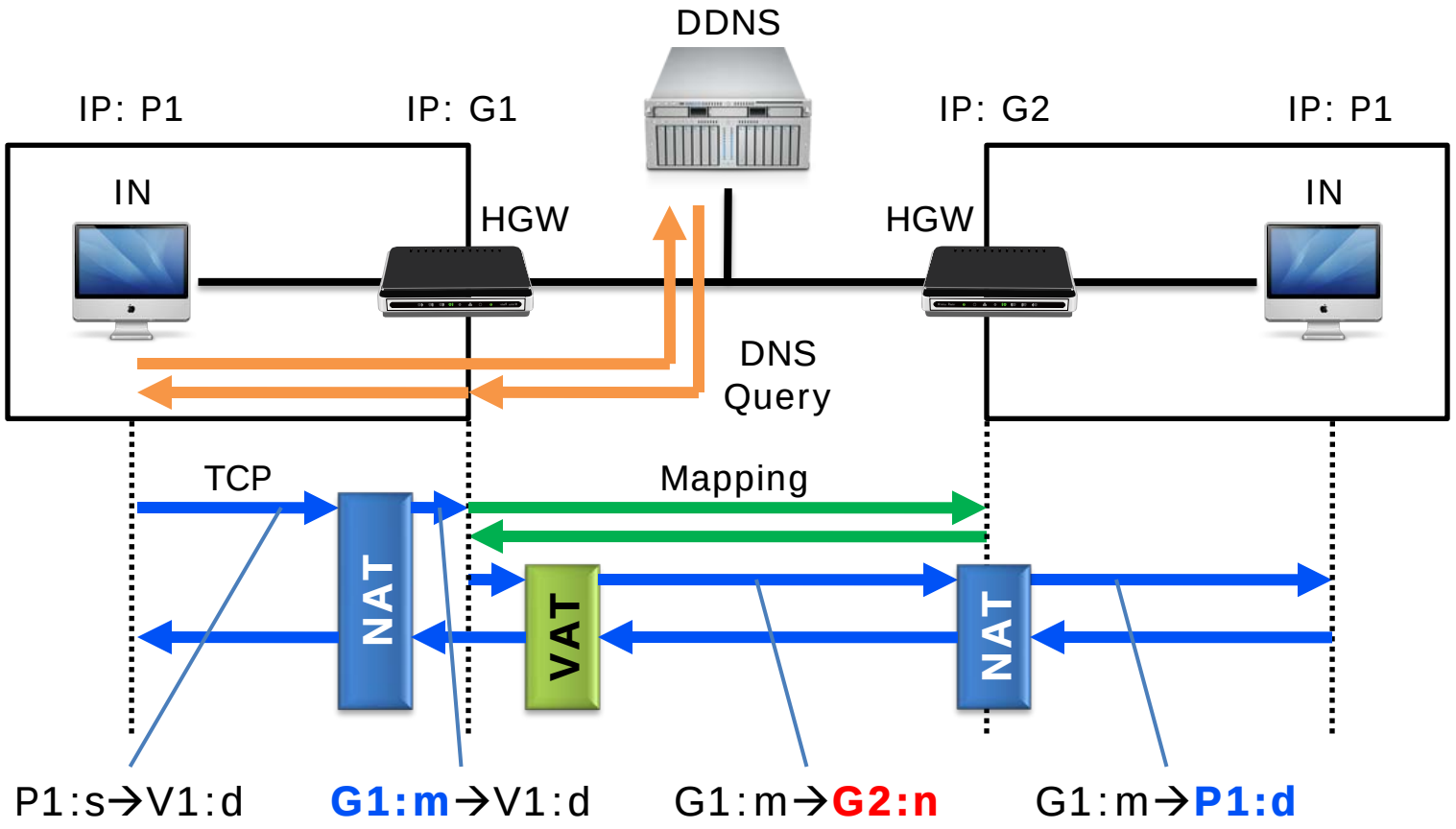


- 複数のENから同一のINに対して同時通信が可能



Home-to-Home

- 通信開始側HGWにNAT-f機能を実装
  - HGW間でネゴシエーション



NAT-fシーケンスの拡張

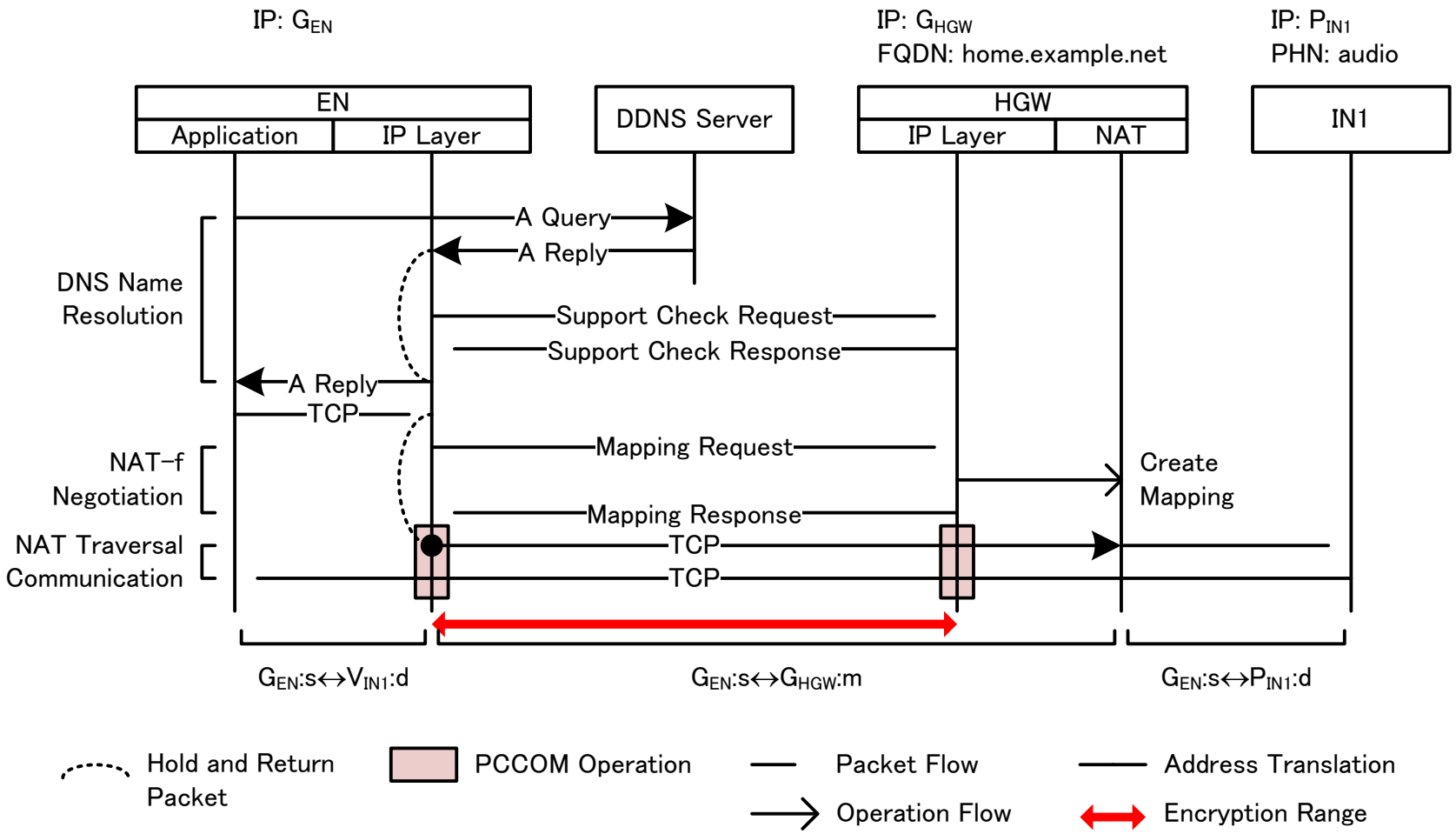
- メッセージを暗号化
- グループ情報を追加（Request）
- マッピングアドレスを決定したグループ鍵で暗号化（Response）

	NAT-f（Original）	拡張NAT-f（提案方式）
Mapping Request	CID | alice	E(CK, CID | alice | g1 | E(GK1, h(N_{HGW})) | g2 | E(GK2, h(N_{HGW})))
Mapping Response	CID | G_{HGW} | m	E(CK, CID | g1 | E(GK1, G_{HGW} | m | proc))

CID: Connection ID = G_{EN} | s | V_{IN2} | d | proto　　proto: Protocol (TCP/UDP)
CK: Common Key　　N_{HGW}: Nonce of HGW
proc: Process Information (Encrypt/Decrypt/Transparency/Discard)

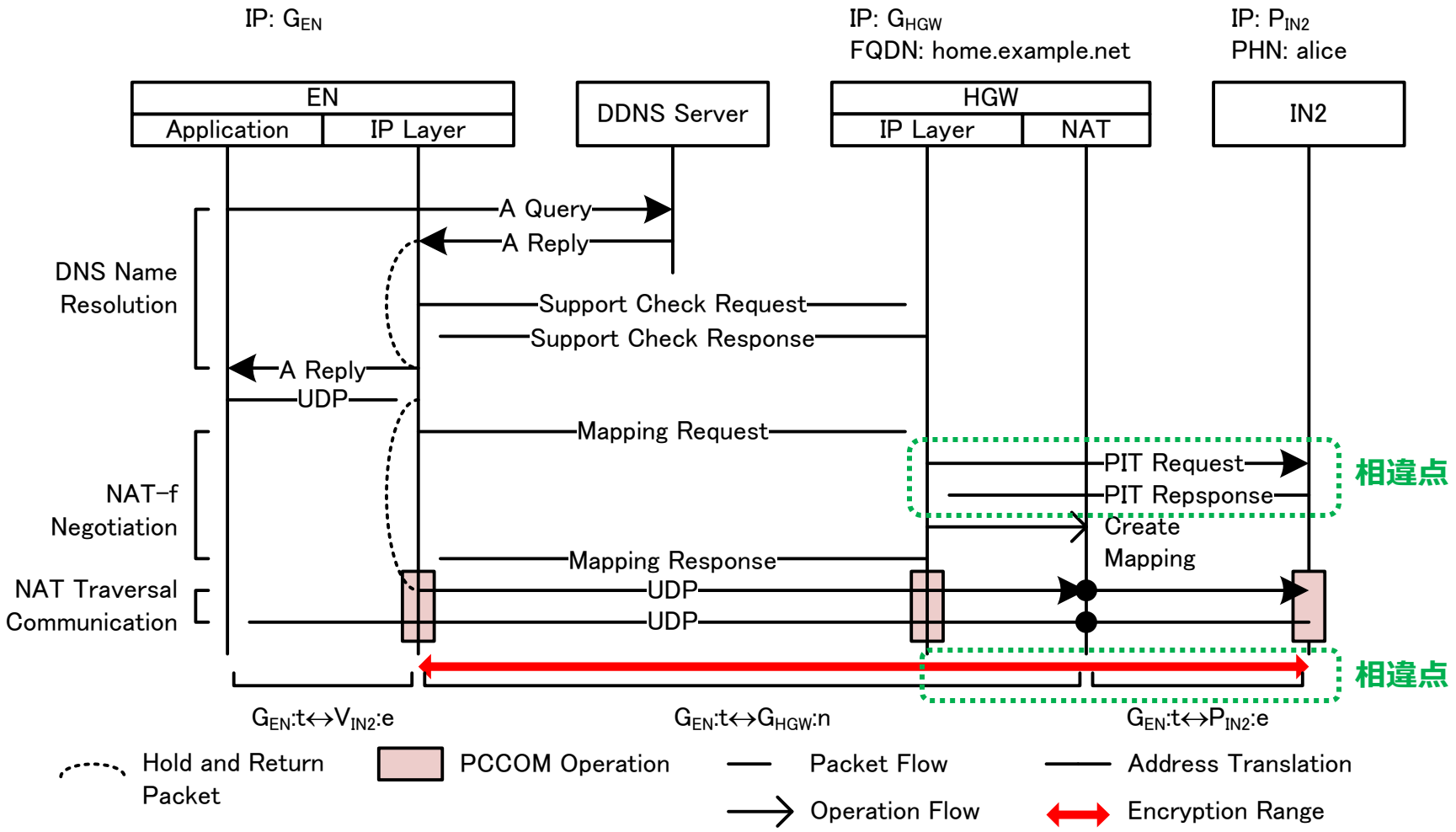
提案システムのシーケンス（1）

- INが暗号化機能をサポートしない場合



提案システムのシーケンス（2）

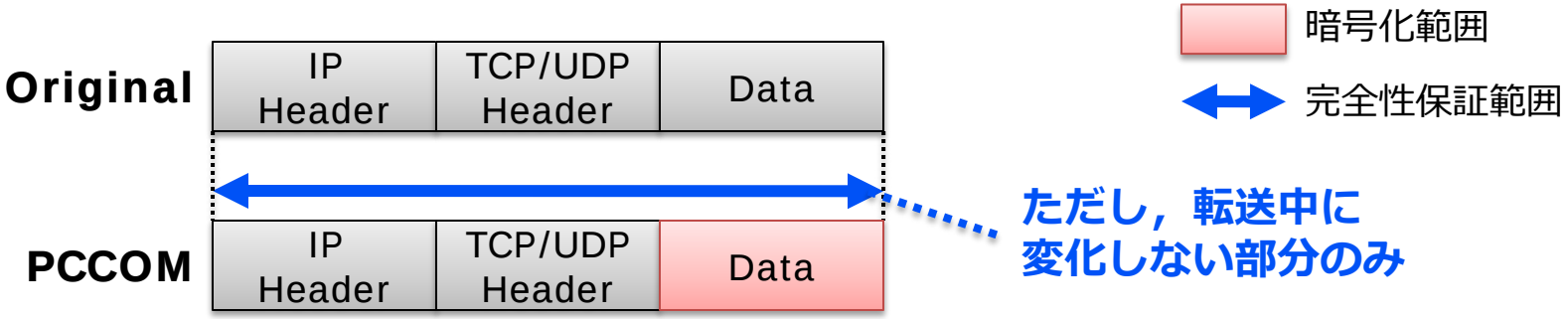
- INが暗号化機能をサポートする場合



PCCOM

PCCOM: Practical Cipher Communication

- パケットフォーマットが不変

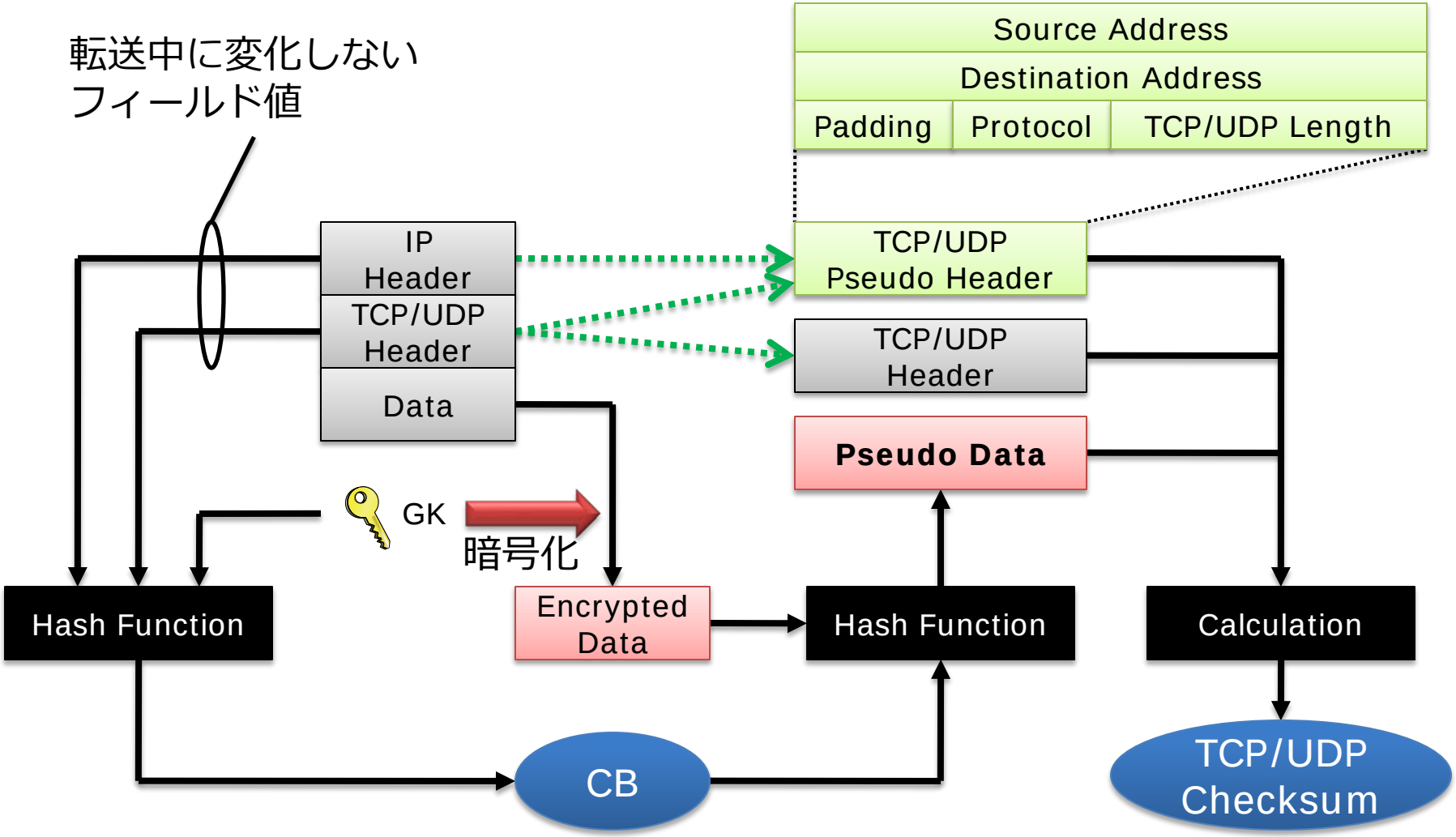


- 独自のTCP/UDPチェックサム計算
  - 本人性確認とパケットの完全性保証を実現
  - **CB (Checksum Base)値**を元とした**疑似データ**を利用

➔転送中に変化しないフィールドとデータ部を保証

12)増田ら：NATやファイアウォールと共存できる暗号化通信方式PCCOMの提案と実装，情処学論，Vol.47，No.7，pp.2258-2266 (2006)

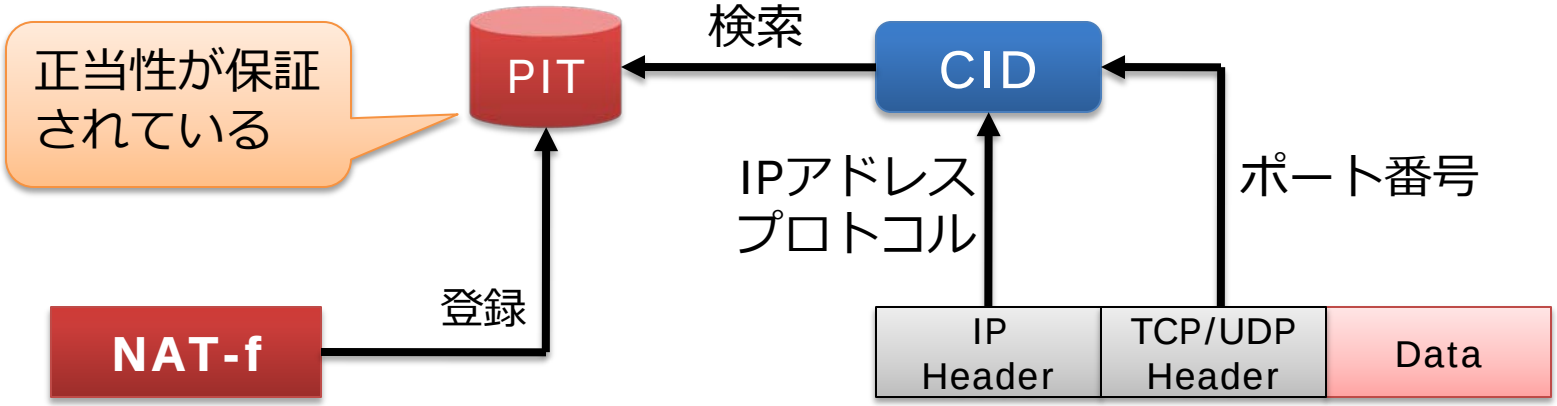
PCCOMのチェックサム計算方法



完全性保証の補完

CID: Connection ID

- IPアドレスとポート番号の完全性
  - 生成されたPITの検索過程で保証



- NATにおけるチェックサム計算
  - 変換部分の差分計算（IPアドレス・ポート番号）

∴PCCOMによる完全性保証プロセスに影響なし

スループット測定結果（PCCOM論文より）