情報処理学会研究報告
IPSJ SIG Technical Report

コンテンツ単位のグルーピングを実現するリモートアクセス方式の提案

三浦健吉[†1]　鈴木健太[†1]
鈴木秀和[†2]　渡邊晃[†1]

リモートアクセスで利用される既存技術として，IPsec-VPN，SSL-VPN，GSRA（Group-based Secure Remote Access）などがある．しかし，これらの技術はネットワークレベルの対策であり，アプリケーションの内容には干渉できない．そこで，本論文ではコンテンツ制御プロキシ（以下 CPROXY）を新たに導入し，GSRA と CPROXY が連携することで，コンテンツ単位のグルーピングを実現する．

A proposal of a Remote Access Method that Realizes Contentes-based Access Groups

Kenkichi Miura,[†1] Kenta Suzuki,[†1]
Hidekazu Suzuki[†2] and Akira Watanabe[†1]

IPsec-VPN, SSL-VPN and GSRA(Group-based Secure Remote Access) are conventional technologies for remote access methods. However, they can not participate the contents of applications because they are network level technologies. In this paper, we propose a combination of GSRA and the contents control proxy server, in oder to realize group communication based on the contents of applications.

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

1. はじめに

モバイル端末の高性能化やモバイルブロードバンドが普及し，移動中や出張先等の遠隔地から自宅や社内のサーバにアクセスできるリモートアクセス技術の需要が高まってきている．リモートアクセスを実現するに当り，サーバのコンテンツに対応したユーザのグルーピングができると有用である．例えば，大学内の Web サーバにアクセスする場合，学生が履修した科目のコンテンツに対してのみアクセスできるユーザグループを定義したいという要求がある．

リモートアクセスを実現する手法としては，インターネット上に VPN（Virtual Private Network）を構築するインターネット VPN が一般的である．インターネット VPN はインターネットを介する手法であるため，盗聴や改ざん，なりすましといったインターネット上の脅威に対抗する手段は必要不可欠である．そこで現在はセキュリティ技術に基づき VPN を構築する方式が主流となっている．インターネット VPN を構築する方式には，PPTP（Point-to-Point Tunnering Protocol）[1]，L2TP（Layer 2 Tunnering Protocol）[2]，IPsec（Security Architecture for Internet Protocol）[3]，SSL（Secure Socket Layer）[4] などがある．

我々は，GSRA（Group-based Secure Remote Access）[5][6] と呼ぶ，NAT 越え技術をベースとした新たなリモートアクセス技術を提案している．GSRA では，外部ノードと内部のサーバ間で通信グループを定義しておく．外部ノードと NAT 配下のサーバが通信を開始する際，NAT 機能を持つ GSRA ルータと外部ノードがネゴシエーションを実行し，GSRA ルータが外部ノードを認証したうえで，NAT マッピング処理を行う．外部ノードは，上記 NAT マッピングに一致するように，IP 層の中に通信パケットのアドレス/ポート変換テーブルを生成する．GSRA は，管理が容易でアプリケーションに制約がないという特長がある．さらに，ポート番号単位のグルーピングが可能であり，アプリケーションごとのアクセス制御が設定できる．しかし，GSRA はネットワークレベルの対策であり，アプリケーションのコンテンツには干渉できない．従って，GSRA だけではコンテンツの内容に対応したグルーピングを実現したいという要求を満たす．

そこで，本論文ではコンテンツ制御プロキシ（以下 CPROXY）を新たに導入し，コンテンツ単位のグルーピングを実現する．通信開始時に実行するネゴシエーションにより GSRA ルータは外部ノードを認証するとともに，認証情報を CPROXY に通知する．外部ノードが内部サーバにアクセスする際に，コンテンツ単位のグルーピングが必要な場合は，GSRA

ルータから必ず CPROXY を経由したアクセスとする．そこで，GSRA とプロキシサーバの技術を融合させることによりコンテンツ単位のリモートアクセスを実現する．

2. 既存技術

2.1 リモートアクセス技術

2.1.1 IPsec-VPN

IPsec-VPN は IPsec の仕組みを利用することで VPN を構築する．アクセス先に設置した IPsec-VPN 装置と外部ノード間で IKE（Internet Key Exchange）[7] による認証と暗号鍵の共有をし，IPsec ESP（Encapsulating Security Payload）[8] による暗号通信を行う．IPsec は IP 層におけるプロトコルであるため，アプリケーションを限定することなく，通信経路上で通信内容の盗聴や改ざんを防止することができる．しかし，セキュリティポリシの設定やネゴシエーションの設定等，端末毎に行わなければならない設定項目が多いため，管理負荷が大きいという課題がある．

また，ESP は，TCP/UDP ヘッダ部が暗号化範囲に含まれているため，NAT でアドレスが変換されるとエンド端末で偽装パケットと見なされ，破棄されてしまう問題がある．これを解決するため，パケットを UDP によりカプセル化して NAT 越えを実現する手法[9] があるが，ヘッダの追加に伴なうオーバヘッドの増加や，ヘッダ部のセキュリティが低下する等の課題が生じる．このように IPsec は NAT との相性が悪く，NAT をまたがった通信の暗号化には向いていない．

2.1.2 SSL-VPN

SSL-VPN は SSL[4] の仕組みを利用することにより VPN を構築し，リモートアクセスを実現する．SSL-VPN を利用する場合，DMZ（DeMilitarized Zone）上に設置した SSL-VPN サーバがプロキシサーバの役割を果たすことでリモートアクセスが実現される．

SSL-VPN によるリモートアクセス方式には以下の 2 種類の方法が存在する．

(1) クライアントが一般の WEB ブラウザを利用する場合

WEB ブラウザは標準で搭載されているため，ユーザによる特別な作業は不要である．また，携帯電話や PDA，ゲーム機等でも，ブラウザが SSL に対応していれば使用できる．しかし，利用できるアプリケーションが WEB 閲覧などに限定されるという課題がある．

(2) クライアントに専用ソフトをインストールする場合

クライアント側に専用ソフトを利用する技術として，OpenVPN[10] などがある．OpenVPN は，Ethernet フレームをカプセル化して通信を行うため，任意のアプリケーションが利用できるという利点がある．しかし，クライアントソフトの導入が必要であり，カプセル化するため通信速度が遅いという欠点がある．

2.1.3 PPTP

PPTP は，企業などで，インターネットを経由した拠点間の LAN 接続や，社員がインターネットを経由して社内 LAN に接続するために使われる．PPTP は，PPP（Point-to-Point Protocol）[11] のパケットを GRE（Generic Routing Encapsulation）[12] でカプセル化し，PPTP サーバーとの間で PPP 接続を確立する．GRE はレイヤ 4 のプロトコルであり，NAT によるポート番号の変換ができず，NAT を通過することができない．ただし，NAT が PPTP パススルーの機能を搭載している場合は，NAT を通過することができる．また，PPTP で利用している暗号方式 MPPE（Microsoft Point to Point Encryption）[13] は暗号化の強度が弱く，セキュリティ強度に課題があると言われている．

2.1.4 L2TP/IPsec

L2TP は PPTP と L2F[14] の仕様を統合したもので，PPTP と同様に IP 以外のプロコトルに対応している．しかし，L2TP は暗号化機能が無いため通信の暗号化には他の技術を併用する必要がある．一般的には，IPsec と組み合わせて利用する．このため，ヘッダの追加に伴ないオーバヘッドが増加するという課題がある．

2.1.5 GSRA

我々は，GSRA（Group-based Secure Remote Access）[5][6] と呼ぶ，NAT-f（NAT-free procotol）[15] をベースとした新たなリモートアクセス技術を提案している．NAT-f は独自の NAT 越え技術である．

外部ノードと NAT 配下のサーバが通信を開始する際，NAT 機能を持つ GSRA ルータと外部ノードがネゴシエーションを実行し，GSRA ルータが外部ノードを認証したうえで，NAT マッピング処理を行う．外部ノードは，上記 NAT マッピングに一致するように，IP 層の中に通信パケットのアドレス/ポート変換テーブルを生成する．GSRA ではトンネル通信は行わず，直接 TCP/UDP ヘッダの IP アドレス/ポート番号を変換する手法を取っているため，パケットのフォーマットが不変であり，オーバーヘッドが少なく高速な通信が実現できる．

また，GSRA は通信の暗号化に PCCOM（Practical Cipher Communication Protocol）[16] と呼ぶ独自の方式を利用している．PCCOM は暗号鍵とパケットの内容から生成した値を用いて独自の TCP/UDP チェックサム計算を行うことにより，本人性確認とパケットの完全性保証を実現できる．NAT を通過でき，ヘッダ部分の完全性も保証されるという特徴

がある．

GSRA は，NAT 越え技術にグループ単位での認証を追加したもので，管理が容易でアプリケーションに制約がない．さらに，サービス単位，すなわちポート番号単位のグルーピングを実現しており，アプリケーションごとのアクセス制御が設定できる．

2.2 アドレス管理についての考察

2.1.1 章から 2.1.4 章の方式では，通信を行う際に，仮想的な IP アドレスを利用しており，それらのアドレスを管理する必要がある．OpenVPN では，サーバ機器からクライアントに対して，DHCP により IP アドレスや DNS サーバなどのネットワーク設定情報を配布する必要がある．IPsec-VPN では，鍵交換プロトコル IKEv2[7] で定義されている IPsec CP（Configration Payload）により，ネットワーク設定情報を配布する．PPTP と L2TP/IPsec では，IPCP（Internet Protocol Control Protocol) によりネットワーク設定情報を配布する．いずれの手法も，クライアントが接続しているネットワークの設定情報と配布されたネットワーク設定情報が重複すると，正く通信が行われない．サーバ側がクライアント側の環境に合わせてネットワーク情報を配布する必要があり，管理が煩雑である．

一方，GSRA では，IP アドレスをクライアント内で単独で生成しており，サーバ側から配布する必要はない．3 章で示すように，GSRA でも仮想アドレスという用語を用いるが，既存方式でいうところの仮想アドレスとは基本的に異なるものがある．これを区別するため，本文では内部仮想アドレスと呼ぶ．内部仮想アドレスは，実際に使用されるネットワークと異なるアドレス体系を選択すれば良く，サーバ側の管理負荷が発生しないという利点がある．

2.3 コンテンツ単位のアクセス制御技術

2.3.1 プロキシサーバによる方法

プロキシサーバを利用してコンテンツ単位のアクセス制御を一括して実現する方法がある．代表的な技術として，Squid[17] がある．プロキシサーバの主な機能として，通信内容を中継・キャッシュすることができる．ユーザは WEB ブラウザにてプロキシサーバを指定することにより，ネットワーク帯域を節約するとともに，目的のページに高速にアクセスすることができる．また，LAN 内でインターネット接続を共有する場合，プロキシサーバを利用することで，匿名性や安全性の向上などのメリットが得られる．上記基本機能の他に，ユーザ認証による利用者の制限や，通信の帯域制限，アクセス制御などの機能を有するものもある．

図 1 に Squid のコンテンツ単位のアクセス制御機能について述べる．WEB ブラウザが

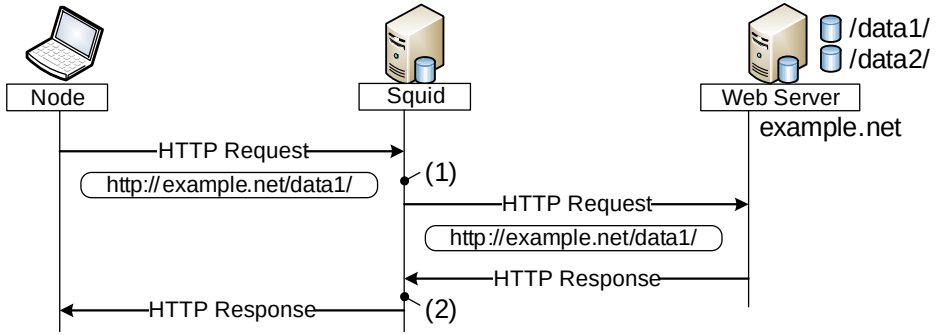


図 1 Squid によるアクセス制御
Fig. 1 Access control by Squid

プロキシサーバを経由して WEB サーバにアクセスする場合，1 往復の通信について往路/復路のそれぞれでアクセス制御を行うことができる．往路の通信では，(1) の時点において HTTP リクエストメッセージに記述された URL の情報に基づき，アクセス制御が可能である．アクセスを許可している場合は，HTTP リクエストメッセージは WEB サーバまで到達する．復路の通信では，(2) の時点において HTTP レスポンスメッセージに記述された WEB ページの内容に基づき，アクセス制御が可能である．ここでも，アクセスを許可している場合は，HTTP レスポンスメッセージはユーザノードまで到達する．往路/復路のいずれの通信でもアクセスを拒否していた場合は，アクセスが拒否されている旨を通知するメッセージを WEB ブラウザに対して通知する．

このように，コンテンツ単位のアクセス制御が可能であるが，リモートアクセスとの組み合わせは想定されておらず，両者は独立した技術である．また，ユーザとプロキシサーバ間の通信は暗号化に対応しておらず，セキュリティ上の課題がある．

2.3.2 コンテンツサーバ側で実現する方法

コンテンツサーバでアクセス制御を実現する技術として，Perl[18]，PHP[19]，JSP[20] などが存在する．これらの技術を利用することで，ログインユーザごとにアクセス制御を行うことができる．この手法では，コンテンツサーバごとに，アクセス制御を作りこめる利点がある．アプリケーションが Web に限定されている場合は，SSL-VPN と組み合わせて利用することにより，リモートアクセス時にログイン操作を 1 度行うだけで良い SSO（Single Sign-On）を実現できる．

しかし，サーバ側でアクセス制御を行う方法は，コンテンツサーバごとに設定が必要であり，コンテンツサーバの台数が多い場合には，管理が煩雑である．

3. GSRA

本章では，提案のベースとなる GSRA について概要を説明する．**図 2** に GSRA システムを用いてリモートアクセスを行うまでの通信シーケンスを示す．EN は外部ノード（External Node），IN は内部ノード（Internal Node）である．EN はホームルータ配下の一般家庭のネットワークに存在することを想定し，プライベートアドレスを保有している．GSRA ルータと IN1 は企業や大学等など組織のネットワークに存在し，GSRA ルータが外部からの入り口として動作する．GSRA ルータは，一般にはファイアウォールのバイアセグメント上に設置される．

ここで EN と GSRA ルータは通信グループに対応した共通のグループ鍵 GK（Group Key）を保持しているものとする．DDNS サーバには，IN のホスト名と GSRA ルータのグローバル IP アドレス G_{GR} との関係が登録されているものとする．以下に EN が IN1 と通信を開始するまでの手順を示す．

（1） 名前解決

EN は DDNS サーバに対して IN1 の名前解決を依頼し，G_{GR} を取得する．ここで EN はカーネル領域において，DNS 応答メッセージに記載されているアドレス G_{GR} を内部仮想 IP アドレス V_{IN1} に書き換える．これにより EN のアプリケーションは IN1 の IP アドレスを V_{IN1} と認識する．内部仮想 IP アドレスは，GSRA ルータ配下に複数の IN が存在するときに，これらを区別するために使用される．この時，IN のホスト名と GSRA ルータのグローバル IP アドレス，および内部仮想 IP アドレスの関係を NRT（Name Relation Table）に登録しておく．アプリケーションから送信される IN1 宛のパケットは宛先 IP アドレスが V_{IN1} となる．

（2） 通信開始

EN のアプリケーションから宛先が V_{IN1} のパケットが送信されると，EN は VAT（Virtual Address Translation）テーブルを検索する．初回は対応するエントリが存在しないため，上記のパケットをカーネル内に待避してから，(3) 以降の処理へと移る．(3) 以降の処理では，VAT テーブルおよびパケットの処理内容を記述した動作処理情報テーブル（PIT : Process Information Table）を生成する．PIT には，暗号化/復号，透過中継，廃棄の区別と暗号化/復号の場合は，使用する暗号鍵が記述される．

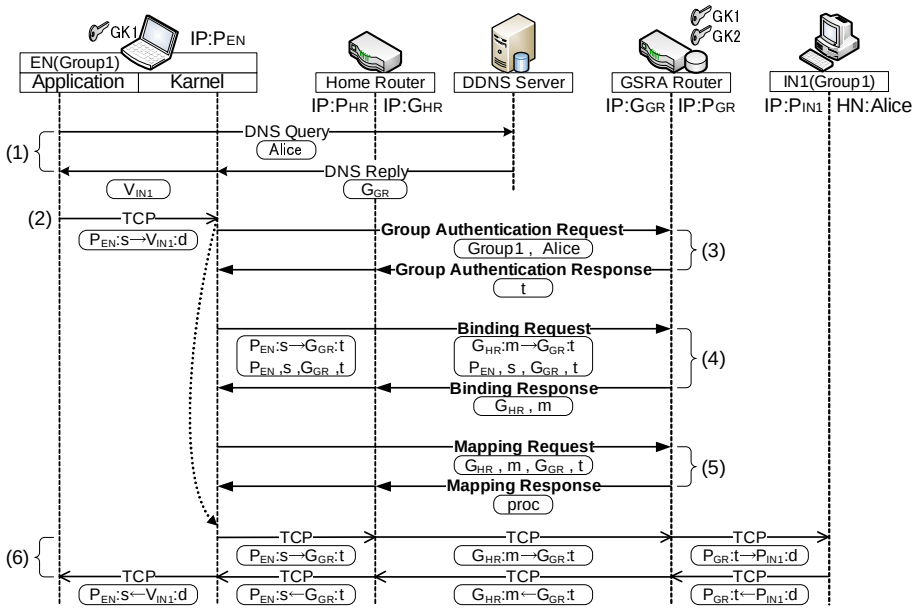


図 2 GSRA の動作シーケンス
Fig. 2 GSRA sequence

（3） グループ認証処理

EN は通信したい IN のホスト名“ Alice ”と自身のグループ番号“ Group1 ”を記載したグループ認証要求を GSRA ルータへ送信する．

GSRA ルータはこれを受信すると，EN と要求された IN が同一グループに属しているか GK を利用して認証を行う．認証が成功した場合，GSRA ルータのエフェメラルポート番号 t を予約し，EN へグループ認証応答を送信する．EN はグループ認証応答メッセージから t を取得して，VAT テーブルと PIT を仮生成する．

（4） バインディング処理

EN が家庭内のネットワークに存在する場合，EN から GSRA ルータに送信されるパケットの送信元アドレス/ポート番号はホームルータの G_{HR}:m となる．したがってメッセージに記載した送信元情報と実際に送信されるメッセージの送信元情報は異なるため，GSRA ルータはこのままでは正しいマッピング処理が行えない．そのため，EN にホームルータの

マッピングアドレスを通知する必要がある．このための処理をバインディング処理と呼ぶ．EN は自身の P_{EN}:s と宛先となる G_{GR}:t を記載したバインディング要求を GSRA ルータに送信する．GSRA ルータがバインディング要求を受信すると，受信メッセージの送信元アドレス/ポート番号 G_{HR}:m を取得し，取得した情報をバインディング応答に載せ EN へ送信する．この処理によって GSRA ルータはホームルータの情報を取得し，ホームルータ（NAT）によるアドレス変換に対応したマッピング処理を実行させることが可能となる．

(5) マッピング処理

EN は (4) で通知されたホームルータのマッピングアドレス G_{HR}:m を送信元情報として，(2) で待避したパケットのセッション情報と，宛先情報 G_{GR}:t を記載したマッピング要求を GSRA ルータへ送信する．GSRA ルータはマッピング要求メッセージから取得した情報を用いてマッピングテーブルと PIT を生成し，マッピング応答を EN へ送信する．EN は受信したマッピング応答メッセージから動作処理情報（proc）を取得し，VAT テーブルと PIT を確定する．ここで確定した GSRA ルータのマッピングテーブルと EN の VAT テーブルの内容を**表 1** に示す．ここで，↔ は通信を，⇔ は変換を表す．以上で GSRA ネゴシエーションが完了し，(2) で待避させたパケットを復帰させて通信を再開する．

表 1 GSRA ルータのマッピングテーブルと EN の VAT テーブル
Table 1 Mapping Table in GSRA router and VAT Table in EN

GSRA マッピングテーブル	:	$\{ G_{EN} : s \leftrightarrow G_{GR} : t \} \Leftrightarrow \{ P_{GR} : t \leftrightarrow P_{IN1} : d \}$
VAT テーブル	:	$\{ G_{EN} : s \leftrightarrow V_{IN1} : d \} \Leftrightarrow \{ G_{EN} : s \leftrightarrow G_{GR} : t \}$

(6) アドレス変換処理

以後，EN から IN1 宛ての通信は，EN の VAT テーブルに従って宛先 IP アドレス/ポート番号が変換される．さらに PIT に従って暗号化されてから GSRA ルータへ送信される．途中のホームルータでは通常の NAT によるアドレス/ポート番号の変換が行われる．GSRA ルータではパケットを復号後，マッピングテーブルに基づいて宛先/送信元の IP アドレス/ポート番号を変換し，IN1 へと転送される．IN1 から EN への応答は上記と逆の順序でアドレス変換および暗号化処理が行われる．

以上の手順により，EN から IN1 へのリモートアクセスが実現される．

4. 提 案 方 式

提案方式では，GSRA と Squid を組み合わせることによりコンテンツ単位のグルーピングを可能とするリモートアクセスを実現する．**図 3** に提案方式の通信シーケンスを示す．EN は WEB ブラウザとし，EN が IN に対して HTTP 通信を行う場合について述べる．コンテンツ制御プロキシ（以下 CPROXY）は Squid に独自機能を追加したものである．**表 2** に CPROXY のアクセス制御テーブルの例を示す．Squid での定義情報に加え，グループ番号とグループごとにアクセス可能なコンテンツの URL の情報を保有するように改造を加える．なお，網掛け部分が追加した項目である．

コンテンツ単位のグルーピングが必要な場合，GSRA ルータは認証情報を CPROXY に通知する．GSRA ルータから IN への通信が CPROXY を通過することにより，コンテンツ単位のアクセス制御を実現する．また，アクセス制御は往路の通信で URL について行うものとする．

(1) 名前解決から (4) バインディング処理までは，既存の GSRA の場合と同様の処理であるため説明は省略する．以下に，マッピング処理とアドレス変換処理について詳細に説明する．

(5) マッピング処理

EN はホームルータのマッピングアドレス G_{HR}:m を送信元情報として，通信開始時に待避したパケットのセッション情報と，宛先情報 G_{GR}:t を記載したマッピング要求を GSRA ルータへ送信する．ここで，GSRA ルータは CPROXY に対して，EN のグループ番号“Group1”とその後の通信で使用する GSRA ルータ内側の IP アドレス/ポート番号 P_{GR}:t を通知する．これを受け取った CPROXY は，(A) の時点で，**表 3** に示すようにグループ番号とグループごとにアクセス可能なコンテンツの URL の情報に対して，GSRA ルータ内側の IP アドレス/ポート番号 P_{GR}:t を関連付けて記録する．そして，CPROXY は GSRA ルータに正常応答を返す．GSRA ルータはマッピング要求メッセージと CPROXY への通知メッセージをもとにマッピングテーブルを生成する．GSRA ルータはマッピング応答を EN へ送信する．EN は受信したマッピング応答メッセージから動作処理情報（proc）を取得し，VAT テーブルを確定する．ここで確定した GSRA ルータのマッピングテーブルと，EN の VAT テーブルの内容を**表 4** に示す．これにより，GSRA ルータから CPROXY に対してパケットが送信される．具体的には，表 1 と表 4 では，右端の IP アドレス/ポート番号の情報が IN1 宛 P_{IN1}:d から CPROXY 宛 P_{XY}:d となる点が異なる．

以上で GSRA ネゴシエーションが完了する．その後，(2) で待避させていたパケットを復帰させて通信を開始する．

(6) アドレス変換処理

EN から IN1 宛ての通信は，EN の VAT テーブルに従って宛先 IP アドレス/ポート番号が変換される．さらに PIT に従って暗号化されてから GSRA ルータへ送信される．ホームルータでは通常の NAT による変換が行われる．GSRA ルータではパケットを復号後，マッピングテーブルに基づいて宛先/送信元の IP アドレス/ポート番号を変換する．これにより，パケットは GSRA ルータから CPROXY へ送信される．CPROXY は図 3 の (C) の時点で，パケットから HTTP メッセージを復元し，HTTP メッセージの送信元 IP アドレス/ポート番号とメッセージ中の URL の情報を取得する． (5) で記録した情報と照らし合わせ，アクセスが許可されていれば，CPROXY は HTTP メッセージを IN1 へ転送する．IN1 から EN への応答は上記と逆の順序でアドレス変換および暗号化処理が行われる．以上の手順により，EN から IN1 へのコンテンツ単位のグルーピングを可能とするリモートアクセスが実現される．

表 2 CPROXY のアクセス制御テーブル
Table 2 Access Control Table in CPROXY

name	path	Group	status	source
alice	/data1/*	Group1,Group2	allow	N/A
alice	/data2/*	Group2	allow	N/A
	*	*	disallow	N/A

表 3 通信中における CPROXY のアクセス制御テーブル
Table 3 Access Control Table in CPROXY

name	path	Group	status	source
alice	/data1/*	Group1,Group2	allow	P_{GR}:t
alice	/data2/*	Group2	allow	N/A
	*	*	disallow	N/A

表 4 提案方式のマッピングテーブルと VAT テーブル
Table 4 GSRA Mapping Table and VAT Table

マッピングテーブル	:	$\{ G_{EN} : s \leftrightarrow G_{GR} : t \} \Leftrightarrow \{ P_{GR} : t \leftrightarrow P_{XY} : d \}$
VAT テーブル	:	$\{ G_{EN} : s \leftrightarrow V_{IN1} : d \} \Leftrightarrow \{ G_{EN} : s \leftrightarrow G_{GR} : t \}$

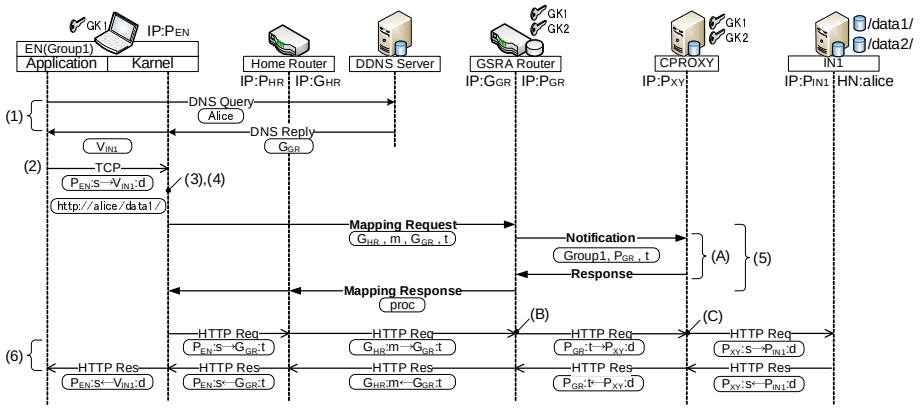


図 3 提案方式の動作シーケンス
Fig. 3 Sequence of the proposal method

5. 比較評価

表 5 に既存システムと提案システムの比較評価を示す．ここで，既存システムとは，一般的なリモートアクセス技術とコンテンツ単位のアクセス制御をサーバ側で実現したものの組み合わせである．提案システムとは，リモートアクセス技術 GSRA とコンテンツ制御プロキシ CPROXY の組み合わせである．一般的なリモートアクセスとプロキシサーバによる組み合わせは，両者が独立した技術であるため，実現が困難であり比較対象とはしない．

システムの導入負荷は，○は変更不要，△はアプリケーションの導入または設置が必要，×はカーネルの改造が必要な場合とした．IPsec-VPN と L2TP/IPsec については，家庭内のホームルータを通過できない場合がある．それに対して，パケットを UDP によりカプセル化して NAT 越えをする手法[9] があるが，ヘッダの追加に伴なうオーバヘッドの増加や，ヘッダ部のセキュリティが低下する等の課題が生じるなどの課題があるため△とした．

コンテンツサーバについては，既存システムでは，すべてのサーバに設定が必要である．提案システムではコンテンツサーバには手を加えなくてよい．逆に，提案システムでは，コンテンツ制御プロキシ CPROXY を導入する必要がある．

サービス単位のアクセス制御，すなわちポート番号単位のアクセス制御については，GSRA は対応している．他のリモートアクセス技術については，単独ではこの機能を実現すること

表 5 既存システムと提案システムの比較
Table 5 Comparison of the existing system and suggestion system

技術名称	リモートアクセス技術	SSL-VPN		IPsec-VPN	L2TP/IPsec	PPTP	提案方式 (GSRA)
		Webベース	App制限なし OpenVPN				
	コンテンツ単位のアクセス制御箇所	コンテンツサーバ	コンテンツサーバ	コンテンツサーバ	コンテンツサーバ	コンテンツサーバ	CPROXY
暗号方式		SSL	SSL	IPsec	IPsec	MPPE	PCCOM
トンネル通信		使用	使用	使用	使用	使用	非使用
導入負荷	EN	○	△	△	△	△	×
	家庭内のホームルータ	○	○	△	△	×	○
	コンテンツサーバ	×	×	×	×	×	○
	コンテンツ制御機器	○	○	○	○	○	×
サーバからのアドレス配布方法		不要	DHCP	IPsec CP	IPCP	IPCP	不要
利用可能なアプリケーション	WEB	○	○	○	○	○	○
	IP	×	○	○	○	○	○
	IP以外のプロトコル	×	○	×	○	○	×
サービス単位のアクセス制御		×	×	×	×	×	○
コンテンツサーバ台数増加時の管理負荷		×	×	×	×	×	○
コンテンツ単位のアクセス制御の柔軟さ		○	○	○	○	○	△
ログイン操作の回数	学外から	1	2	2	2	2	1
	学内から	1	1	1	1	1	1

は不可能であり，別途 Firewall 等を導入する必要がある．

コンテンツサーバ台数増加時の管理負荷については，既存システムでは，個別対応が必要である．提案システムでは，CPROXY に設定追加を行うだけで良い．

コンテンツ単位のアクセス制御の柔軟さについては，既存システムでは，アクセス制御部分をいくらでも作りこむことができるが，提案システムでは，URL を基準とした一定レベルのアクセス制御のみが可能である．

ログイン操作の回数については，既存システムのうち，Web ベースの SSL-VPN については，SSO を実現すればログイン回数は 1 回で済む．それ以外の既存システムについては，リモートアクセス技術を利用する際のログイン操作と，コンテンツサーバにログインする際の操作と 2 回必要である．提案システムでは，GSRA ルータと CPROXY 間で認証情報を共有しているため，ログイン回数は 1 回で良い．

大学組織では，コンテンツサーバが学科ごとに存在し，さらに学科ごとに管理者が異なる場合が多い．そのような環境において，コンテンツ単位のアクセス制御を行いたい場合，コンテンツサーバの設定を変更することは困難を極めることが予想される．しかし，提案システムでは，各コンテンツサーバの設定に手を加える必要はなく，CPROXY を設置するだけで良い．また，大学組織のコンテンツサーバは科目コンテンツがディレクトリごとに分けられて設置されている場合が多く，提案システムの URL を基準とした一定レベルのアクセス制御方式で十分に対応できるものと考えられる．また，コンテンツサーバが既に稼働中の場合でも，切り替えが容易である．提案システムは，本研究のモチベーションとなった大学組織への導入に適していると考える．

6. ま と め

本論文では，GSRA と Squid を組み合わせることにより，コンテンツ単位のアクセス制御を可能とするリモートアクセス方式を提案した．GSRA はネットワークレベルのプロトコルであり，アプリケーションの内容には干渉できないため，アプリケーションの内容を制御する部分は Squid に任せる方式を取った．提案システムは，コンテンツサーバの台数が多い場合に効果がある．

今後は，提案システムの実装と性能評価を行う予定である．

参 考 文 献

1) K.Hamzeh, G.Pall, W.Verthein, J.Taarud, W.Little and G.Zorn: Point-to-Point Tunneling Protocol (PPTP), RFC 2637, IETF (1999).
2) W.Townsley, A.Valencia, A.Rubens, G.Pall, G.Zorn and B.Palter: Layer Two Tunneling Protocol "L2TP", RFC 2661, IETF (1999).
3) S.Kent and K.Seo: Security Architecture for the Internet Protocol, RFC 4301, IETF (2005).
4) T.Dierks and E.Rescorla: The Transport Layer Security (TLS) Protocol, RFC 5246, IETF (2008).
5) 鈴木秀和，　渡邊晃：通信グループに基づくサービスの制御が可能な NAT 越えシステムの提案，情報処理学会論文誌，Vol.51, No.9, pp.1–11 (2010).
6) 鈴木健太，鈴木秀和，渡邊　晃：NAT 越え技術を応用したリモートアクセス方式の提案と設計，マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム論文集，Vol.2010, No.1, pp.288–294 (2010).
7) C.Kaufman, P.Hoffman, Y.Nir and P.Eronen: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, IETF (2010).
8) S.Kent: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).
9) A.Huttunen, B.Swander, V.Volpe, L.DiBurro and M.Stenberg: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).

10) OpenVPN: http://openvpn.net/.
11) W.Simpson: The Point-to-Point Protocol (PPP), RFC 1661, IETF (1994).
12) D.Farinacci, T.Li, S.Hanks, D.Meyer and P.Traina: Generic Routing Encapsulation (GRE), RFC 2784, IETF (2000).
13) G.Pall and G.Zorn: Microsoft Point-To-Point Encryption (MPPE) Protocol, RFC 3078, IETF (2001).
14) A.Valencia, M.Littlewood and T.Kola: Cisco Layer Two Forwarding (Protocol) "L2F", RFC 2341, IETF (1998).
15) 鈴木秀和，宇佐見庄吾，　渡邊晃：外部動的マッピングにより NAT 越えを実現する 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).
16) 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).
17) Squid: http://www.squid-cache.org/
18) Perl: http://www.perl.org/
19) PHP（PHP:Hypertext Preprocessor）: http://www.php.net/
20) JSP（JavaServer Pages）: http://java.sun.com/products/jsp/

コンテンツ単位のグルーピングを実現するリモートアクセス方式の提案

名城大学大学院理工学研究科
三浦 健吉, 鈴木 健太, 鈴木 秀和, 渡邊 晃

Watanabe Lab.

研究背景

- 大学の講義資料の電子化が進んでいる
  - 教材利用時の利便性が向上している
  - 一方で，著作権への配慮等から，科目履修者に対してのみ教材を配布したい
- 大学でリモートアクセスシステムの導入が進んでいる
  - 自宅からでも教材配布サーバやe-learningシステムにアクセスできる

⇒リモートアクセス時においても，科目履修者のみに教材を配布したい

研究背景・目的

- 自宅からリモートアクセス技術を利用して教材コンテンツにアクセスする

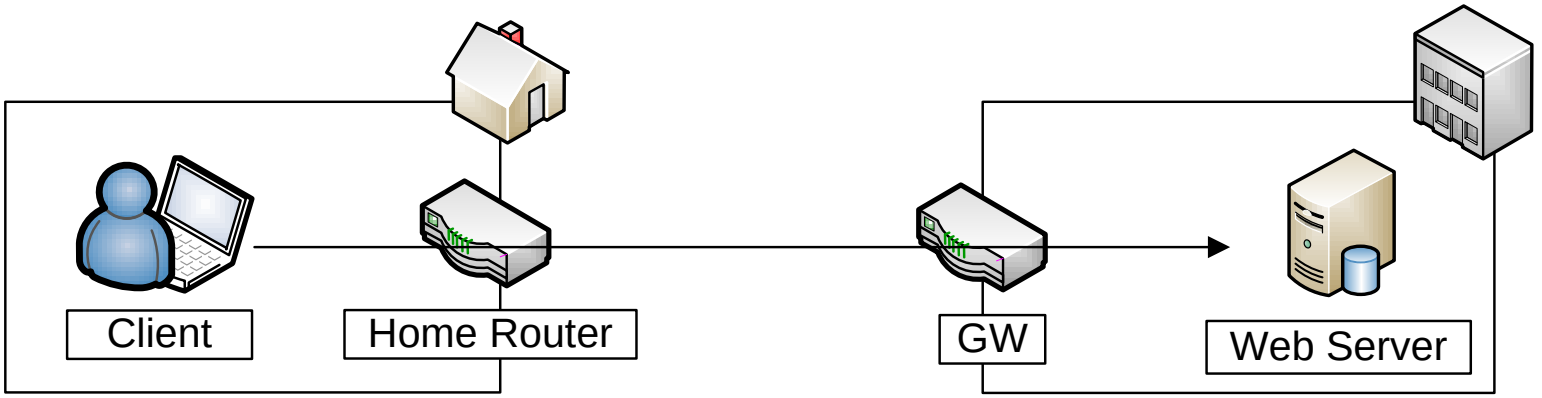
- ユーザをグループ単位で扱い，コンテンツごとにアクセス制御を実現する
  - あるユーザグループはあるコンテンツにアクセスできるようにする

要求仕様

- ユーザ数が多い（学生全員）ため，管理が容易でなければならない
- コンテンツサーバは一般的なWebサーバを想定
- コンテンツサーバには手を加えない
  - 学科ごとにコンテンツサーバを保有
  - 学科ごとに管理者が異なる

  →コンテンツサーバを改造するのは難しい
- ユーザは自宅から教材にアクセス

  →ホームNAT配下から通信を開始



既存技術

- リモートアクセス技術
  - IPsec-VPN
  - SSL-VPN
  - GSRA*（Group-based Secure Remote Access）
- コンテンツ単位のアクセス制御技術
  - コンテンツサーバ側で実現する方法
  - プロキシサーバによる方法

→上記2種類の技術を組み合わせる

*鈴木秀和，渡邊晃：通信グループに基づくサービスの制御が可能なNAT 越えシステムの提案，情報処理学会論文誌，2010

鈴木健太，鈴木秀和，渡邊晃：NAT越え技術を応用したリモートアクセス方式の提案と設計，DICOMO20010

既存技術

- リモートアクセス技術
  - IPsec-VPN
  - SSL-VPN
  - GSRA*（Group-based Secure Remote Access）
- コンテンツ単位のアクセス制御技術
  - コンテンツサーバ側で実現する方法
  - プロキシサーバによる方法

→上記2種類の技術を組み合わせる

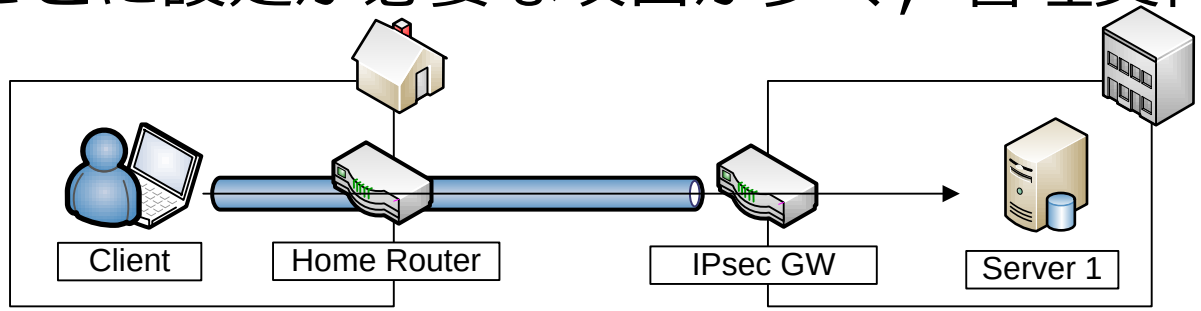
*鈴木秀和，渡邊晃：通信グループに基づくサービスの制御が可能なNAT 越えシステムの提案，情報処理学会論文誌，2010

鈴木健太，鈴木秀和，渡邊晃：NAT越え技術を応用したリモートアクセス方式の提案と設計，DICOMO2010

IPsec-VPN

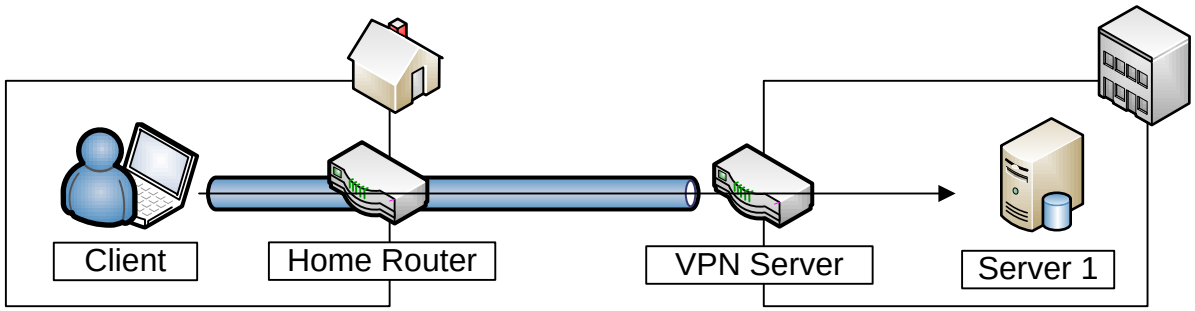
- IPsecのトンネルモードを利用
- 任意のアプリケーションが利用できるメリットがある
- TCP/UDPヘッダが暗号化範囲に含まれているため，ホームNATでアドレス変換されると，偽装パケットとみなされ破棄される
  - パケットをUDPによりカプセル化してNAT 越えを実現する手法が存在するが，ヘッダの追加に伴なうオーバヘッドの増加や，ヘッダ部のセキュリティが低下する等の課題が生じる

  →ホームNATと相性が悪い
- 端末ごとに設定が必要な項目が多く，管理負荷が高い



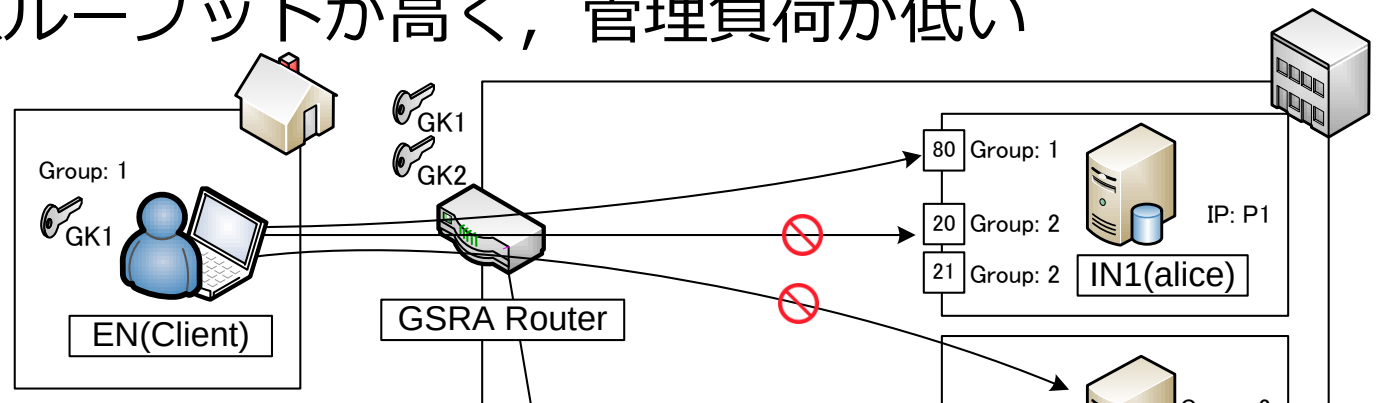
SSL-VPN

- クライアントがWebブラウザの場合
  - クライアントは一般的なWebブラウザだけで良い
  - アプリケーションの種類がWebに限定される
- クライアントが専用ソフトの場合（OpenVPN等）
  - 任意のアプリケーションが利用できる
  - 専用クライアントの導入が必要
  - スループットが低い



GSRA（Group-based Secure Remote Access）

- 通信グループを定義し，グループごとでアクセス制御
- 通信グループは，ACT（Access Control Table）に記述
  - ホスト単位（IPアドレス単位）
  - サービス単位（ポート番号単位）
- ネットワークレベルで実装されているため，任意のアプリケーションが利用できる
- スループットが高く，管理負荷が低い



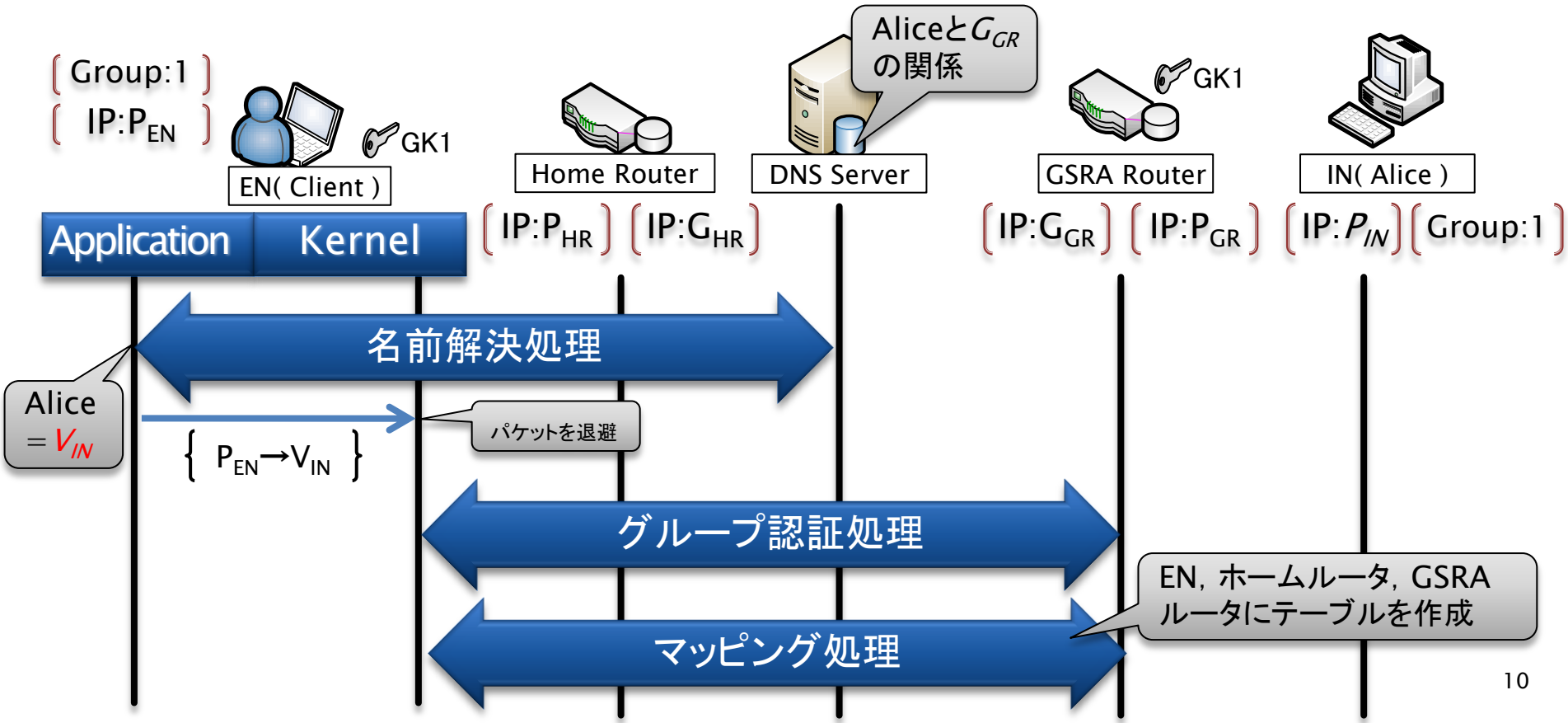
ACT

Hostname	IP	Service	Permit	Group
alice	P1	80	allow	1
alice	P1	20, 21	allow	2
bob	P2	*	allow	2

EN: External Node
IN: Internal Node

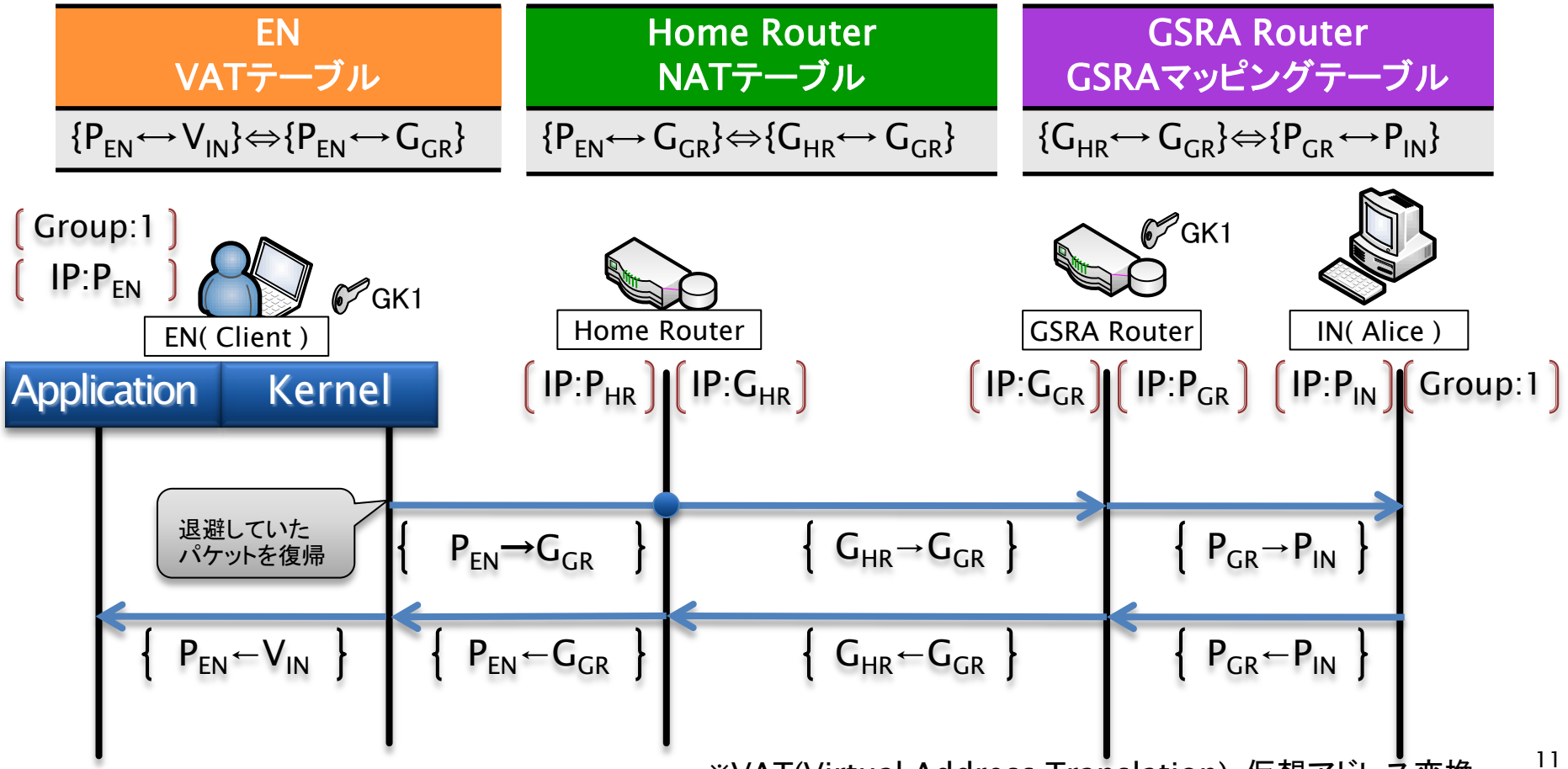
GSRA通信シーケンス（1/2）

- 名前解決処理：DNS応答内容(G_{GR})を仮想IPアドレス(V_{IN})に書き換え
  内部ノードを仮想アドレスで認識する
- グループ認証処理：アクセスが許可されているかGK1を利用して判断
- マッピング処理：EN，ホームルータ，GSRAルータにテーブルを作成



GSRA通信シーケンス（2/2）

- マッピング処理：EN，ホームルータ，GSRAルータにテーブルを作成
- アドレス変換処理：テーブルに従いアドレスを順次変換していく
- 以上により，リモートアクセスを実現



※VAT(Virtual Address Translation)：仮想アドレス変換

既存技術

- リモートアクセス技術
  - IPsec-VPN
  - SSL-VPN
  - GSRA*（Group-based Secure Remote Access）
- コンテンツ単位のアクセス制御技術
  - コンテンツサーバ側で実現する方法
  - プロキシサーバによる方法

→上記2種類の技術を組み合わせる

*鈴木秀和，渡邊晃：通信グループに基づくサービスの制御が可能なNAT 越えシステムの提案，情報処理学会論文誌，2010

鈴木健太，鈴木秀和，渡邊晃：NAT越え技術を応用したリモートアクセス方式の提案と設計，DICOMO2010

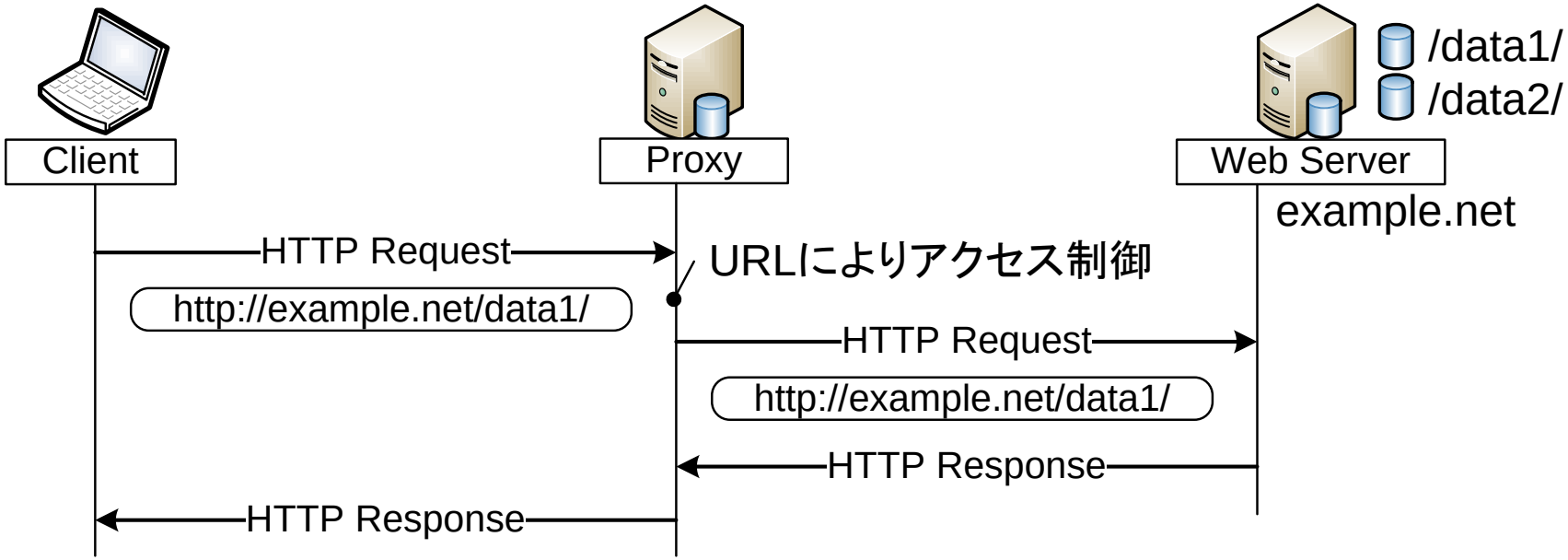
コンテンツサーバ側で実現する方法

- コンテンツサーバにPerl/PHP/JSPなどで記述されたプログラムを導入する
- ログインしたユーザごとに，異なるコンテンツを提示できるようにする

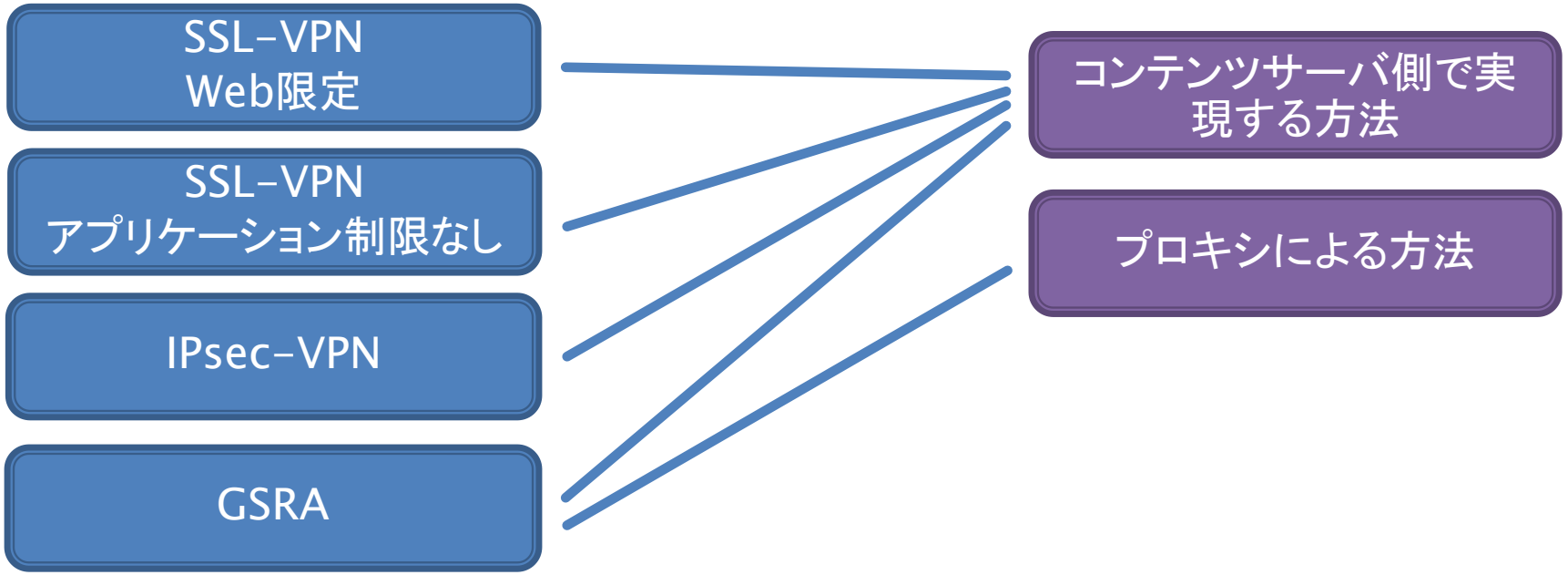
- 例
  - ログインユーザA → 履修科目である科目A, 科目Bにのみアクセスできる
  - ログインユーザB → 履修科目である科目A, 科目Cにのみにアクセスできる

プロキシサーバによる方法

- プロキシサーバはHTTP通信を中継できる
- コンテンツの場所を示すURLの情報によりアクセス制御を行う



既存技術の組み合わせ

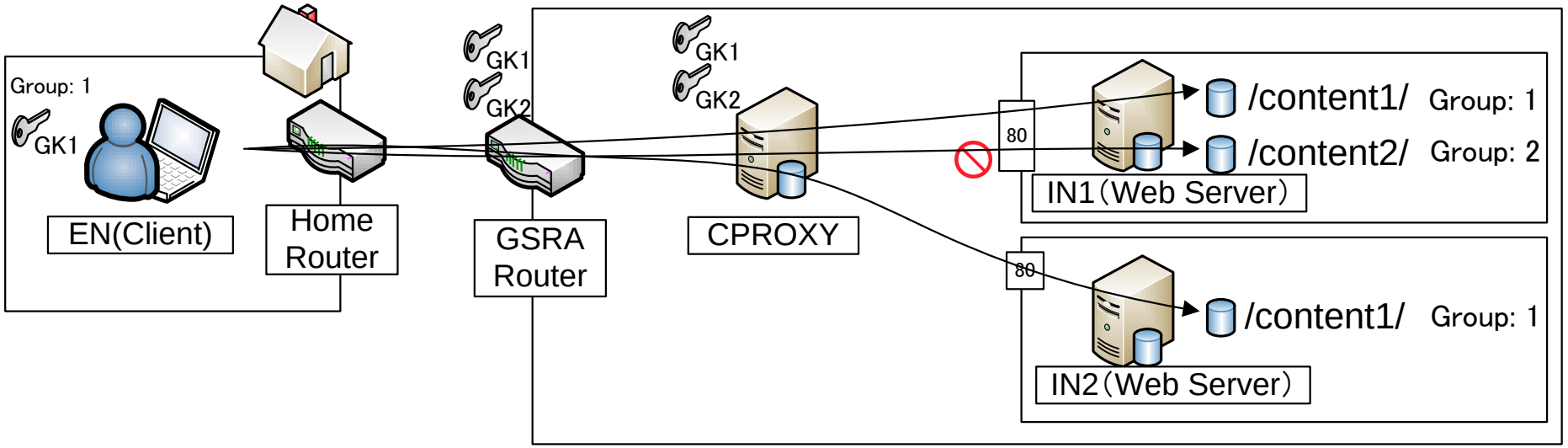


- 提案システムでは，GSRA+プロキシの組み合わせ
- 要求定義としてコンテンツサーバには手を加えないため，プロキシによる方法を選択
- GSRAは独自に開発した技術であるため，プロキシと組み合わせるように改造が可能

提案システムの概要

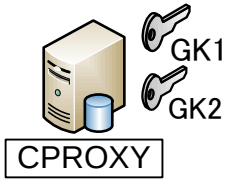
- GSRA＋プロキシの組み合わせ

- コンテンツ制御プロキシ（CPROXY）を導入する
- GSRAルータとCPROXYが連携することにより，コンテンツ単位のリモートアクセス制御を実現



提案システム：事前設定

- CPROXYはアクセス制御テーブルを保有
  - URLとコンテンツの対応関係とアクセス許可グループを関連付け
- CPROXYはグループ認証用の鍵を保有

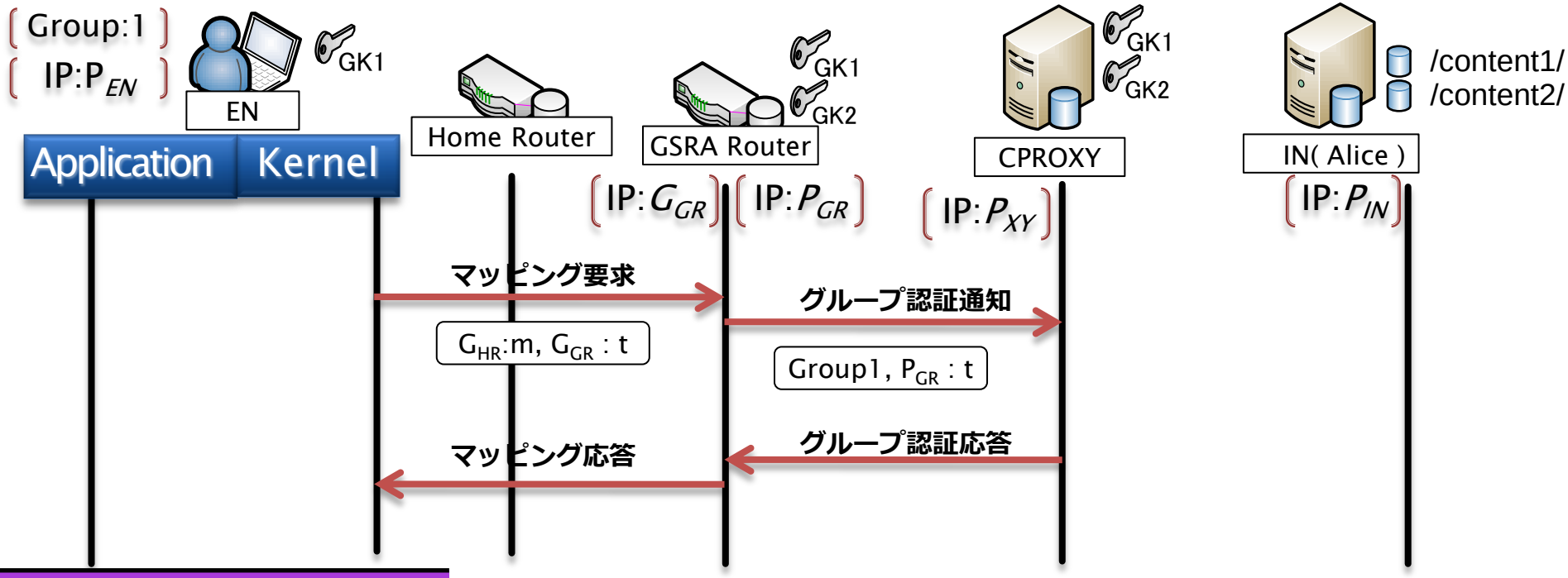


アクセス制御テーブル

Hostname	Path	Permit	Group	Source
alice	/content1/*	allow	Group1	*none*
	/content2/*	allow	Group2	*none*

動作シーケンス(1/2)

- ENはHTTP通信により，aliceの/contents1/を要求
- CPROXYはGSRAルータ内側のポート番号を記録



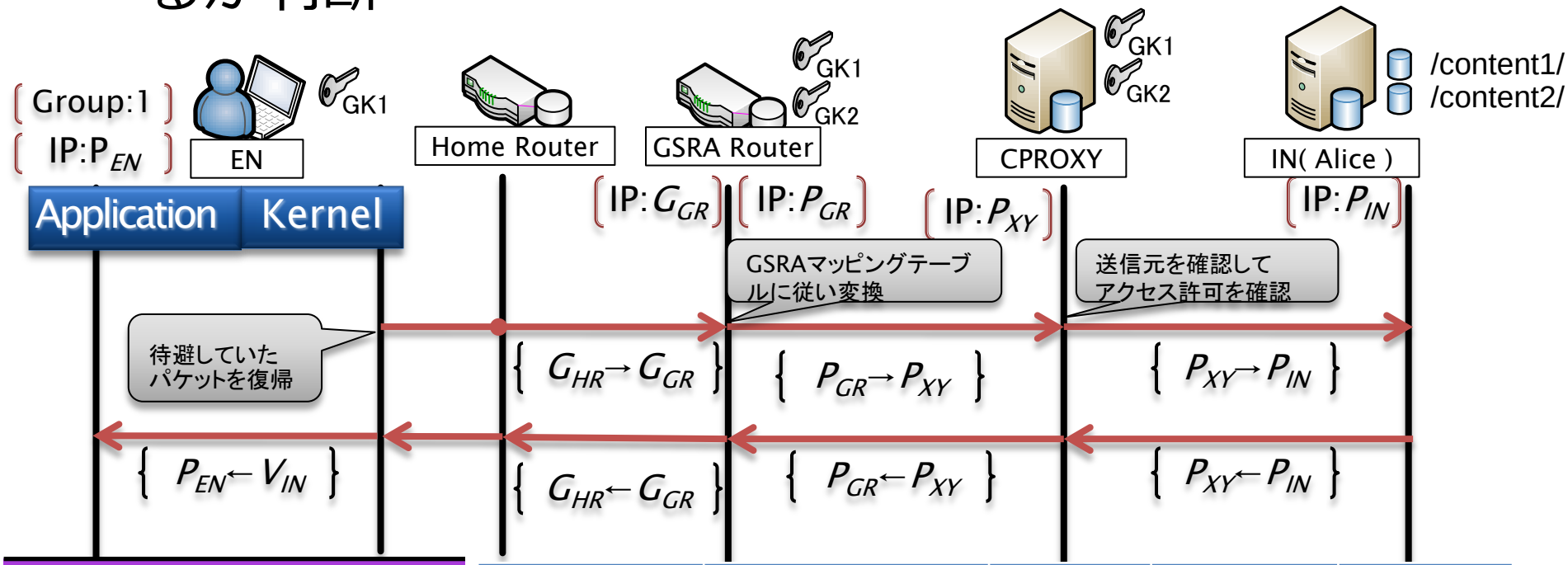
GSRA Router
GSRAマッピングテーブル

$\{G_{HR} \leftrightarrow G_{GR}\} \Leftrightarrow \{P_{GR} \leftrightarrow P_{XY}\}$

Hostname	Path	Permit	Group	Source
alice	/content1/*	allow	Group1	P_{GR}:t
	/content2/*	allow	Group2	*none*

動作シーケンス(2/2)

- CPROXYは送信元を確認して，アクセスを許可するか判断



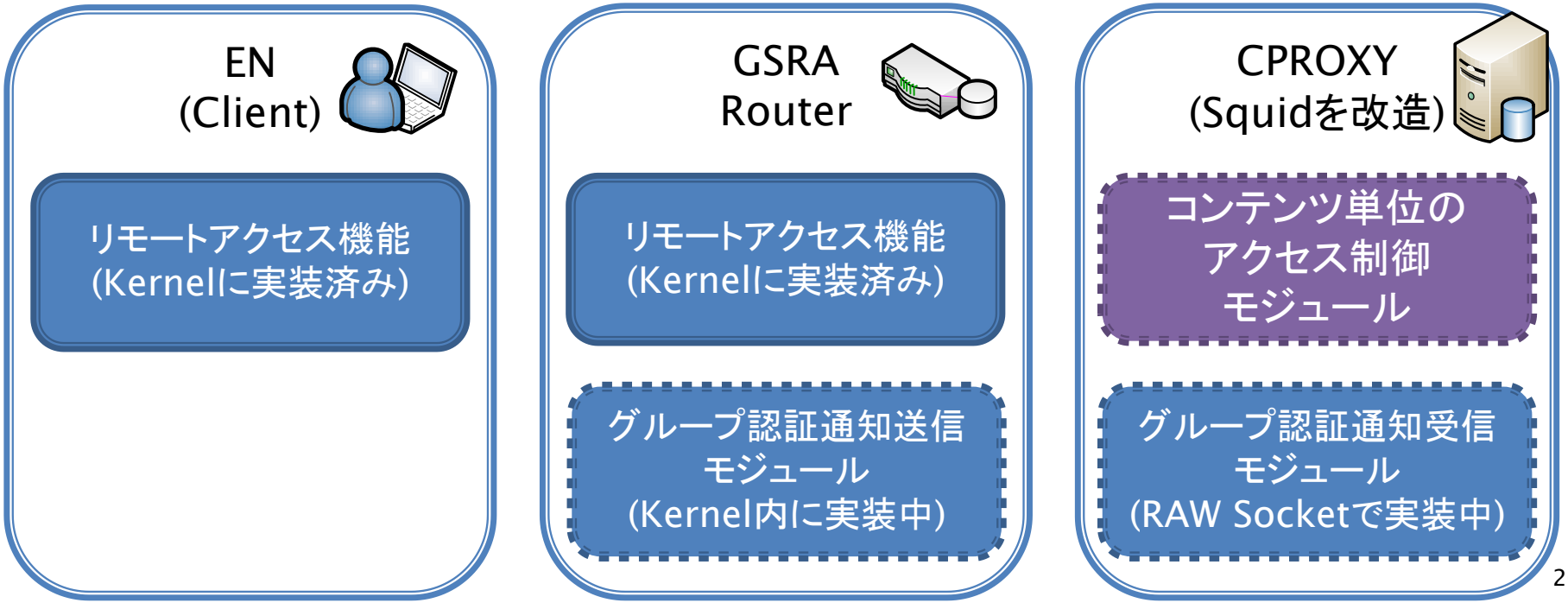
GSRA Router
GSRAマッピングテーブル

$\{G_{HR} \leftrightarrow G_{GR}\} \Leftrightarrow \{P_{GR} \leftrightarrow P_{XY}\}$

Hostname	Path	Permit	Group	Source
alice	/content1/*	allow	Group1	P_{GR}:t
	/content2/*	allow	Group2	*none*

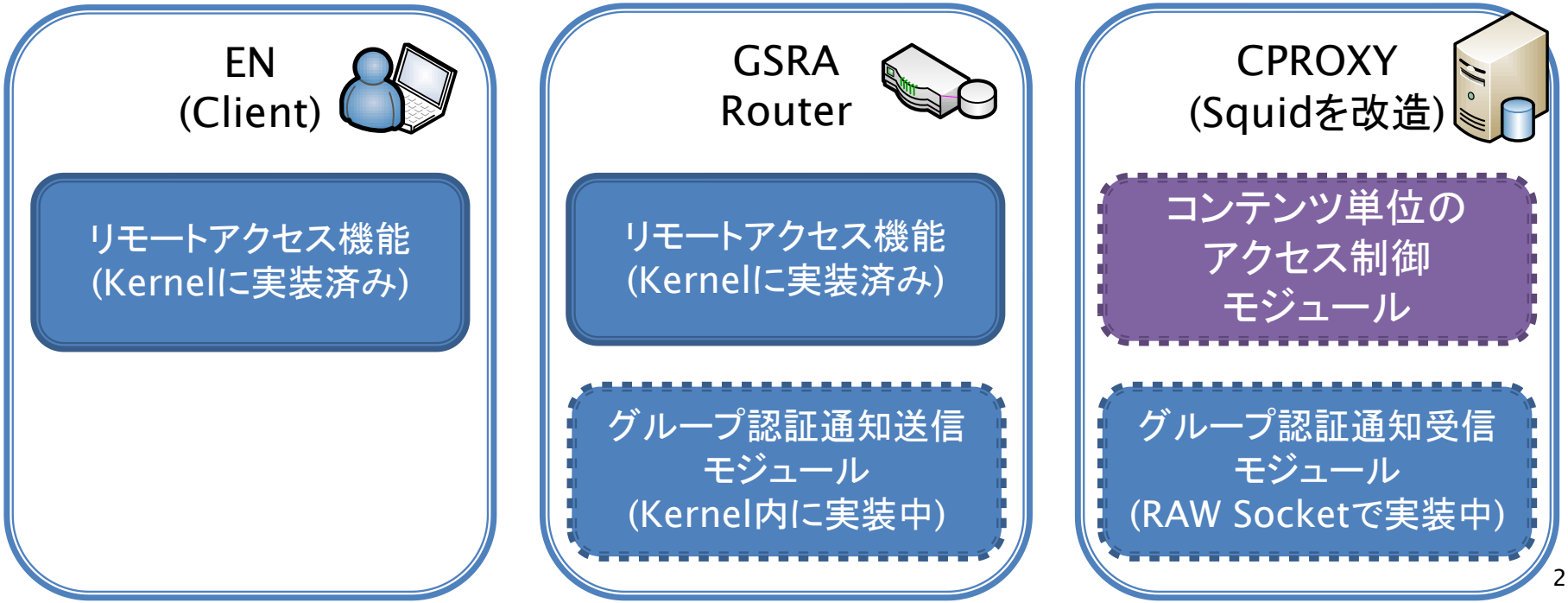
実装について（1/2）

- 通常のリモートアクセス機能
  - ENとGSRAルータについては，FreeBSDのカーネル部分に実装済みであり，動作確認・性能評価についても完了している



実装について（2/2）

- 提案システムを構成する部分について
  - CPROXYはSquidを改造する
  - グループ認証通知はICMPパケットを使用する
  - コンテンツ単位のアクセス制御モジュールはSquidのモジュールを活用



比較評価

- 提案システム：GSRA＋CPROXY
- 既存システム：一般的なリモートアクセス技術＋コンテンツサーバ側で実現する方法

	既存	提案	
導入コスト	△	○	[既存] 学内のコンテンツサーバを入れ替える必要あり [提案] 学内のコンテンツサーバはそのまま利用できる
管理コスト	△	○	[既存] GWと学内の各コンテンツサーバで個別にユーザを管理する必要がある [提案] GWとCPROXYは一元的にユーザ管理が可能
アクセス制御の柔軟さ	○	△*	[既存] 個別のコンテンツサーバでアクセス制御を作り込める [提案] CPROXYで一定レベルのアクセス制御が可能

*科目コンテンツがディレクトリごとに分けられて設置されている場合は，URLによる一定レベルのアクセス制御で十分対応可能

むすび

- 学内のコンテンツサーバに対するリモートアクセス時に，コンテンツサーバに手を加えずに，一定レベルのアクセス制御を行う手法を提案した
- GSRAルータとCPROXYが認証情報を共有することにより，コンテンツ単位のアクセス制御を実現する
- 今後の作業
  - 提案方式の実装の完了