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方式の提案

三浦 健吉[†1]　鈴木 秀和[†2]　渡邊 晃[†1]

リモートアクセスで主に利用される既存技術として，IPsec-VPN や SSL-VPN がある．しかし，IPsec-VPN は複雑な設定が必要で管理が面倒であり，NAT との相性が悪いなどの課題がある．また，SSL-VPN は手軽に利用できるが，使用するアプリケーションが限定されるという課題がある．そこで我々は，GSRA（Group-based Secure Remote Access）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．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 Access Groups by Contents

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

There are IPsec-VPN and SSL-VPN in the method chiefly used by a remote access. IPsec-VPN has problems such as complex setting is necessary and compatibility with NAT is bad. Though SSL-VPN can be easily used, there is a problem that the application used is limited. We have proposed remote access technology that is called GSRA based on the NAT traversal technology. However, GSRA is measures at the network level, and it is not possible to interfere in the content of the application. Then, the contents control proxy (henceforth CPROXY) is newly introduced, GSRA cooperates with CPROXY, and grouping of each contents is achieved in this thesis.

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，大学学内の Web サーバにアクセスする場合，特定のコンテンツに対して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．

リモートアクセスで主に利用される既存技術として，IPsec-VPN や SSL-VPN がある．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 EN 間で IKE（Internet Key Exchange）による認証と暗号鍵の共有をし，IPsecESP による暗号通信を行う．IPsec は IP 層においてデータの改ざん防止や秘匿機能を提供す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，またエンドエンドで暗号化されていないという課題がある．

SSL-VPN は SSL 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 は一般的なブラウザには標準で搭載されているため，ユーザによる設定は不要である．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，SSL-VPN は利用できるアプリケーションが Web 閲覧やメール送信などに限定されるという課題がある．また，IPsec-VPN と同様に，エンドエンドでの暗号化されないという課題がある．

そこで我々は，GSRA（Group-based Secure Remote Access）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

†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

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徴がある．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内容には干渉できない．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することはできない．

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，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 CPROXY を経由したアクセスとする．CPROXY としては，Squid を流用する．Squid は，コンテンツ対応のアクセス制御が可能であるが，リモートアクセスを想定した技術ではない．そこで，GSRA と Squid 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とする．

以降，2 章で要素技術となる GSRA と Squid について説明する．3 章で GSRA と Squid を組み合わせてコンテンツ単位のリモートアクセスを実現する手法について述べる．そして第 4 章でまとめる．

2. 要 素 技 術

2.1 GSRA

図 1 に EN が GSRA システムを用いて IN1 にリモートアクセスを行うまでの通信シーケンスを示す．左側の EN とホームルータは一般家庭のネットワークを想定している．EN はホームルータ配下に存在し，プライベートアドレスを保有している．右側の GSRA ルータと IN1 は企業や大学等など組織のネットワークである．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．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} となっているパケットが送信されると，EN は VAT 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，復号化，透過中継，廃棄の区別と暗号化/復号化の場合は，使用する暗号鍵が記述されている．

(3) グループ認証処理

EN は通信したい IN のホスト名 “ Alice ” と自身のグループ情報 “ 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 NAT 配下に存在する場合，EN から GSRA ルータに送信されるパケットの送信元情報はホームルータの 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，正しいマッピングが行えない．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しておく必要がある．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である 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．このバインディング処理によって GSRA ルータはホームルータの情報を取得し，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アドレス変換テーブルと 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 ルータのアドレス変換テーブルと EN の VAT テーブルの内容を**表 1** に示す．

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．

(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，アドレス変換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．GSRA は FreeBSD での実装を終え，動作を検証済みである．

表 1 GSRA ルータのアドレス変換テーブルと EN の VAT テーブル
Table 1 Address Transration Table in GSRA Router and VAT Table in EN

アドレス変換テーブル	:	$\{ G_{EN} : s \leftrightarrow G_{GR} : t \} \Leftrightarrow \{ P_{GR} : t \leftrightarrow P_{IN1} : d \}$
VAT テーブル	:	$\{ G_{EN} : s \leftrightarrow V_{IN1} : d \} \Leftrightarrow \{ G_{EN} : s \leftrightarrow G_{GR} : t \}$

2.2 Squid

Squid はプロキシサーバソフトの一種で，フリーソフトとして入手可能である．プロキシサーバの主な機能として，通信を中継・キャッシュすることができる．ユーザは WEB ブラウザにて Squid を HTTP のプロキシサーバとして指定することで，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．LAN 内でインターネット接続を共有する場合，プロキシを利用することで，匿名性や安全性の向上などのメリットが得られる．Squid はその他に多くの機能を有しており，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．

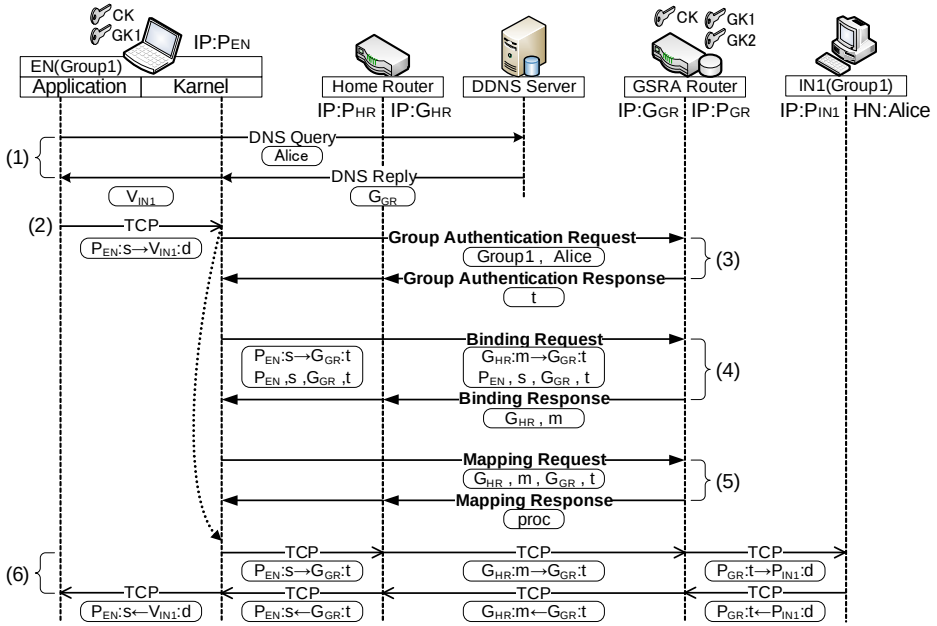


図 1 GSRA の動作シーケンス
Fig. 1 GSRA sequence

以下に Squid のアクセス制御機能について述べる．WEB ブラウザが Squid 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．**図 2** に Squid によるアクセス制御の例を示す．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 HTML 文書の内容に基づき，アクセス制御が可能である．ここでも，ア

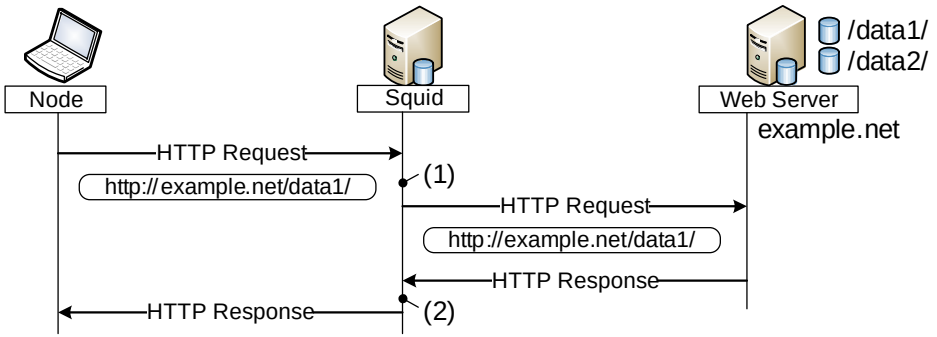


図 2 Squid によるアクセス制御
Fig. 2 Access control by Squid

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，Squid 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．

3. 提 案 方 式

図 3 に提案方式の通信シーケンスを示す．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目指す．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 3** に CCPROXY 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，グループ情報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，従来の 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．

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

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

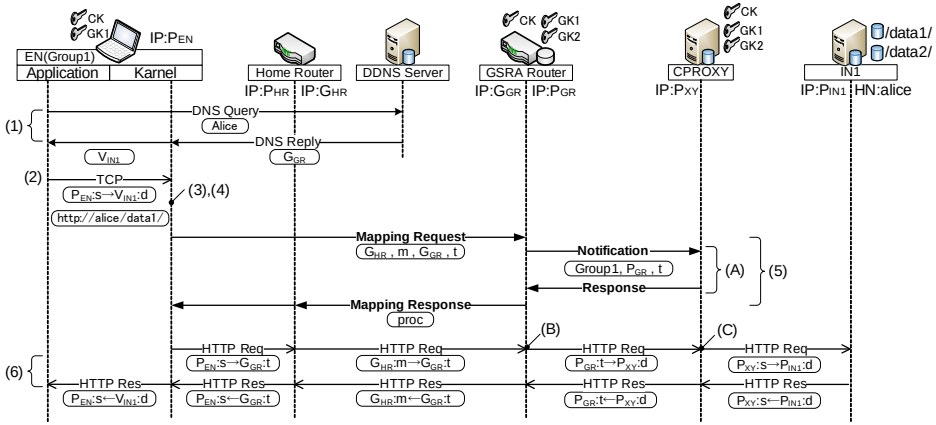


図 3 提案方式の動作シーケンス
Fig. 3 Sequence of the proposal method

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

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

(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 のグループ情報“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

表 4 提案方式のアドレス変換テーブルと VAT テーブル
Table 4 Address Transration Table and VAT Table

アドレス変換テーブル	:	$\{ G_{EN} : s \leftrightarrow G_{GR} : t \} \Leftrightarrow \{ P_{GR} : t \leftrightarrow P_{XY} : d \}$
VAT テーブル	:	$\{ G_{EN} : s \leftrightarrow V_{IN1} : d \} \Leftrightarrow \{ G_{EN} : s \leftrightarrow G_{GR} : t \}$

る．これを受け取った CPROXY は，(A) の地点で，**表 3** に示すようにグループ情報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アドレス変換テーブルと PIT 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 テーブルと PIT を確定する．ここで確定した GSRA ルータのアドレス変換テーブルと，EN の VAT テーブルの内容を**表 4** に示す．GSRA ルータから Squid に対してパケットを送信するため，アドレス変換テーブルは，表 1 と表 4 では，右端の IP アドレス/ポート番号の情報が異なっている．

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，アドレス変換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，内容が一致しており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．

4. ま と め

本論文では，GSRA と Squid を組み合わせることにより，コンテンツ単位のグルーピング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．今後は，実装と性能評価を行う．

参 考 文 献

1) 鈴木健太，鈴木秀和，渡邊晃：NAT-f を応用したリモートアクセス方式 GSRA の提案と実装，情報処理学会第 72 回全国大会講演論文集， Vol.3, pp.377–378 (2010).
2) 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).
3) 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).
4) 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).
5) S.Kent and K.Seo: Security Architecture for the Internet Protocol, *RFC 4301* (2005).
6) T.Dierks and E.Rescorla: The Transport Layer Security (TLS) Protocol, *RFC 5246* (2008).

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

本研究の目的

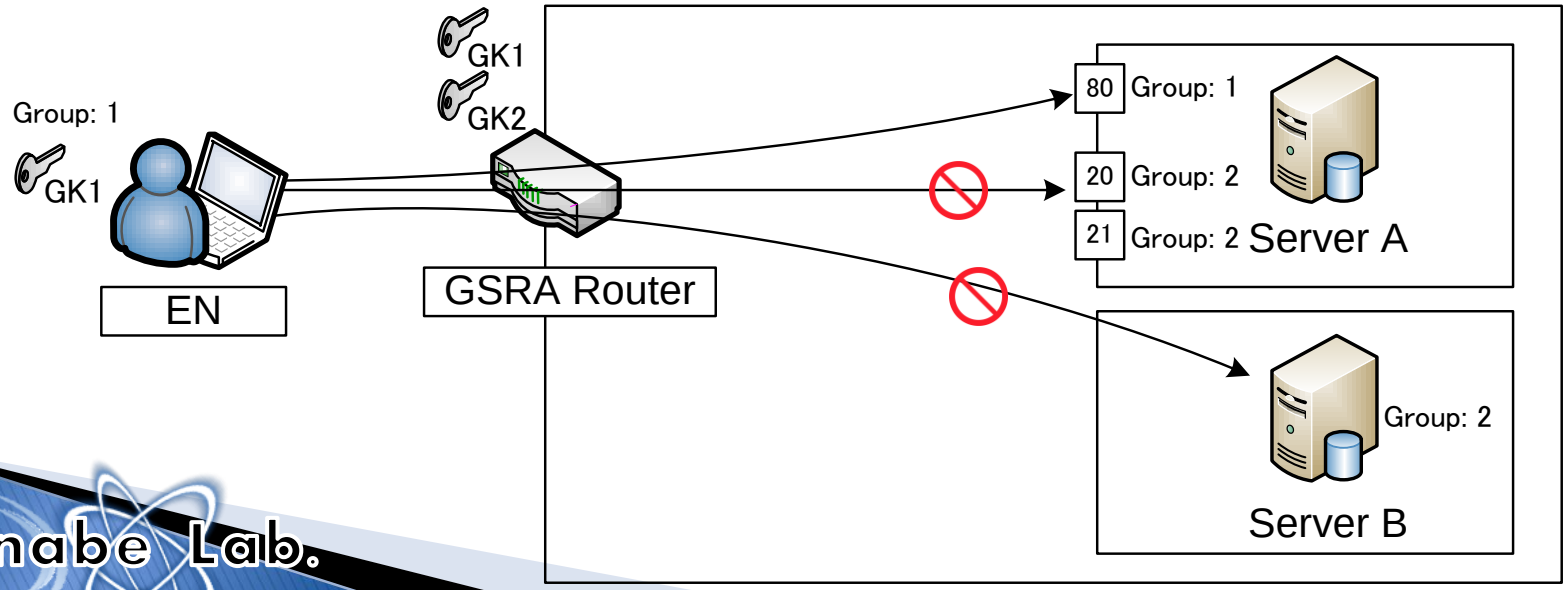
- 遠隔地から教材コンテンツへアクセスする
  - ユーザをグループ単位で扱い，コンテンツごとのアクセス制御を実現する
    - あるユーザグループはあるコンテンツにアクセスできる
  - 学内のコンテンツサーバには，一切手を加えない

リモートアクセス技術GSRA*を利用して実現

＊ 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

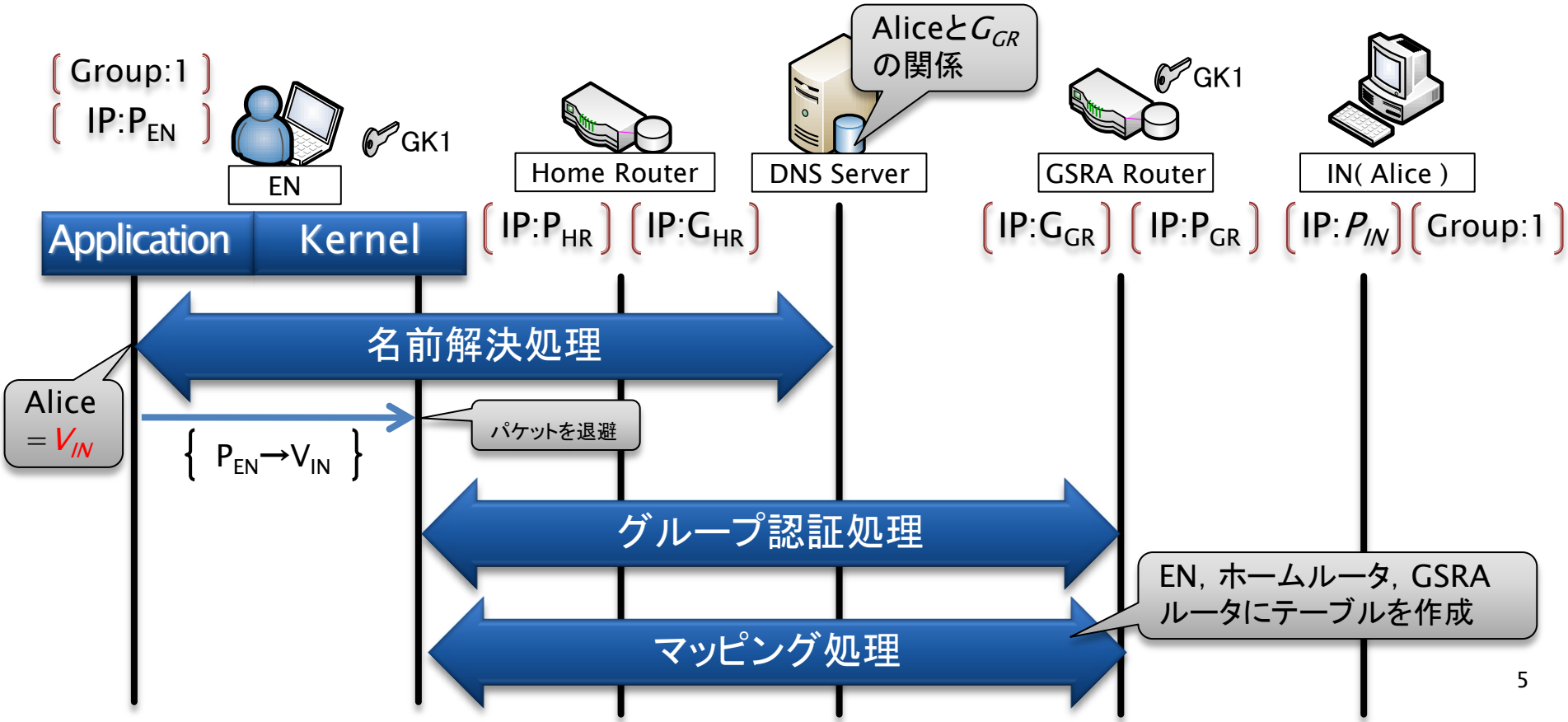
GSRA（Group-based Secure Remote Access）の特徴

- 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，詳細に設定可能
  - 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。



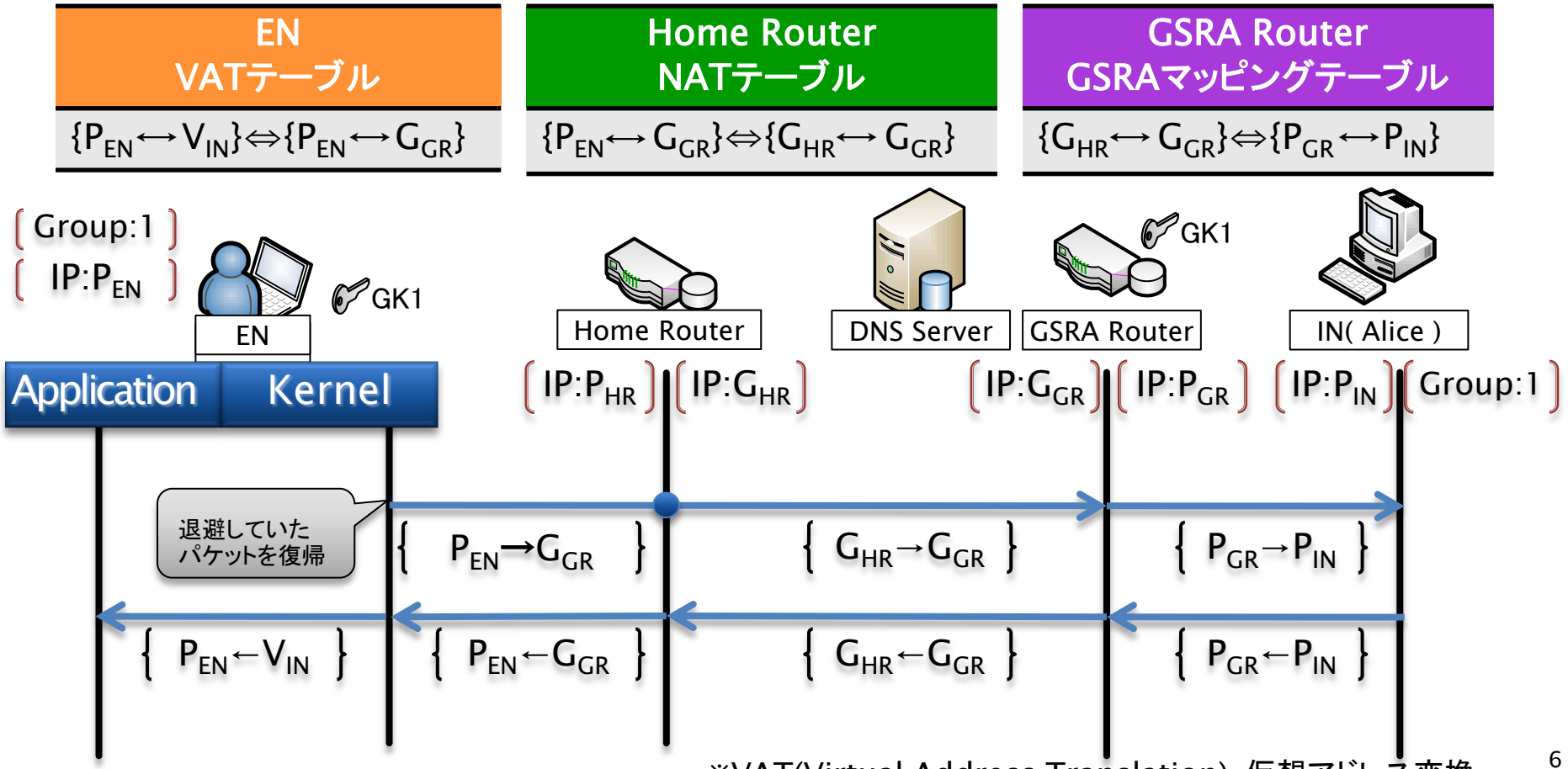
GSRA通信シーケンス

- 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

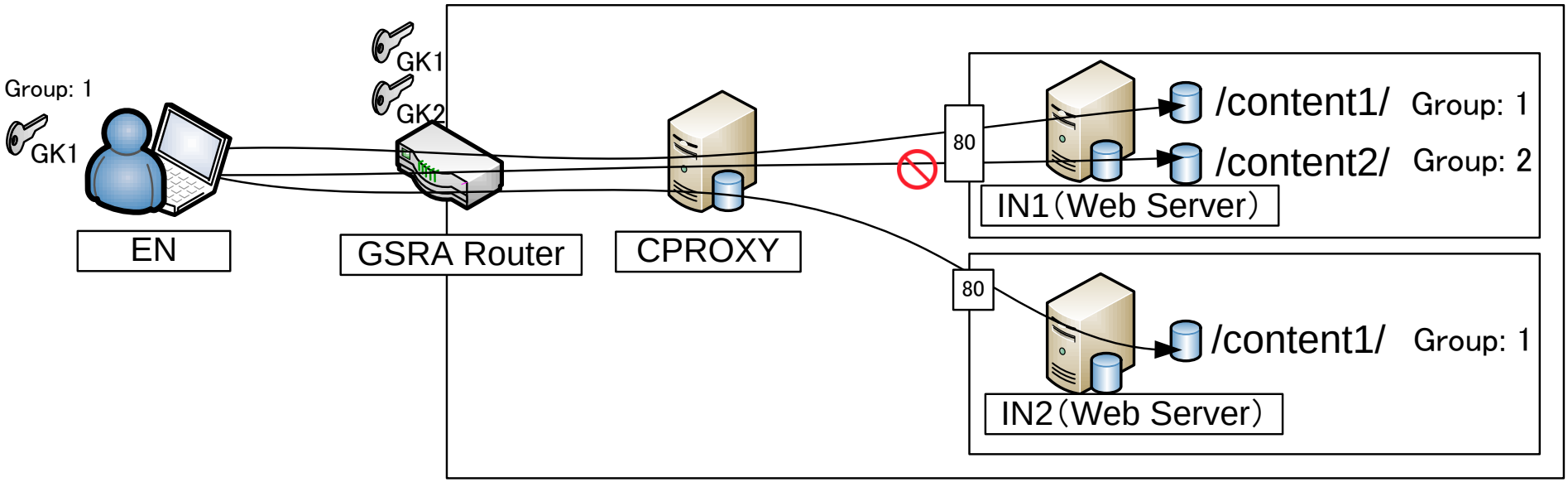
- マッピング処理：EN，ホームルータ，GSRAルータにテーブルを作成
- アドレス変換処理：テーブルに従いアドレスを順次変換していく
- 以上により，リモートアクセスを実現



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

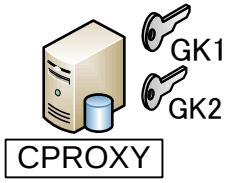
提案システムの概要

- 新たにコンテンツ制御プロキシCPROXYを導入する
- WEBコンテンツ（TCP80番）を対象にする
- 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



提案方式：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

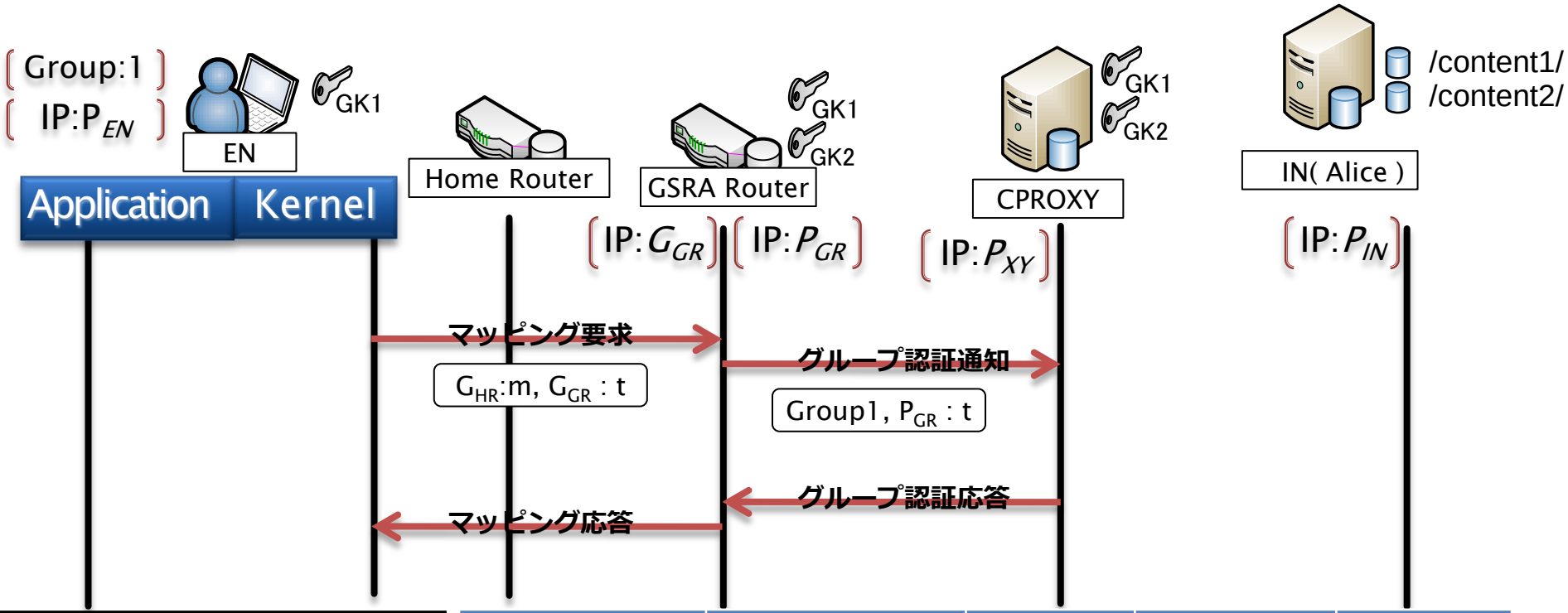


アクセス制御テーブル

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

提案方式：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



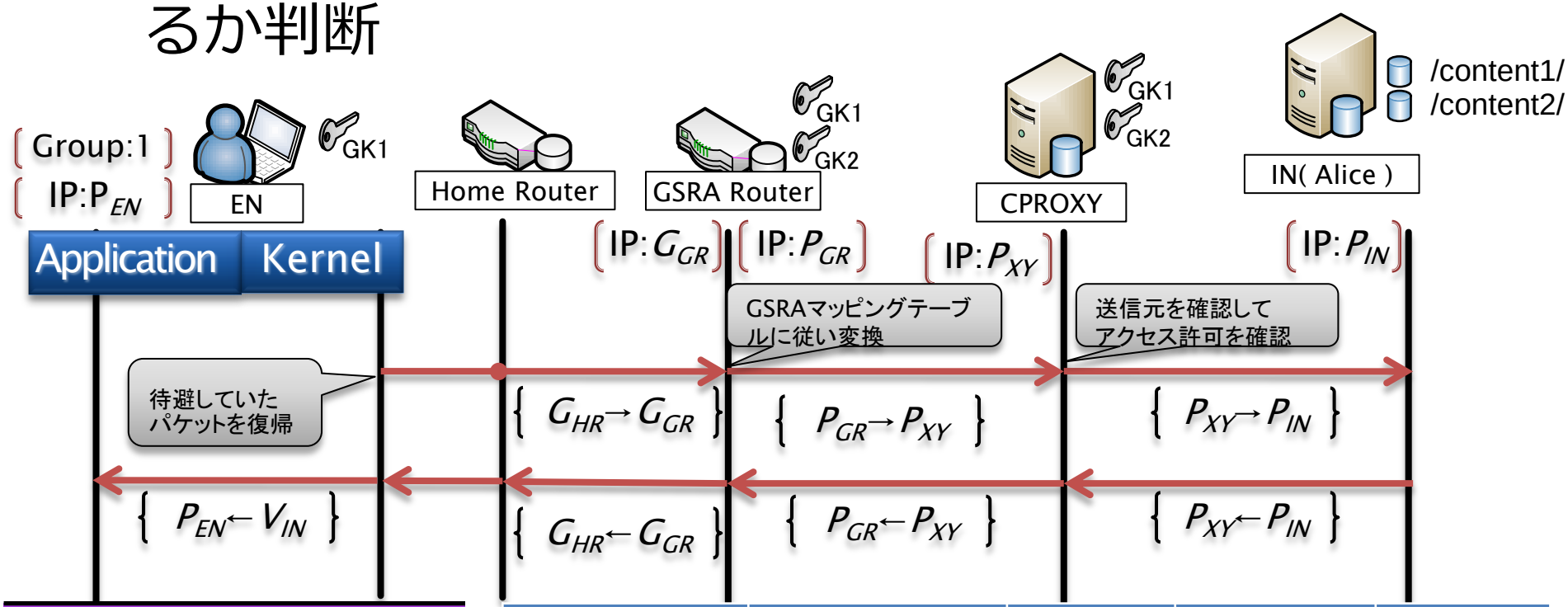
GSRA Router
GSRAマッピングテーブル

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

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

提案方式：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*

実装方法について

- 通常のリモートアクセス
  - ENとGSRAルータは実装を完了しており，動作確認・性能評価ともに完了
- 提案方式のリモートアクセス
  - CPROXYは，WEBプロキシSquidを改造する
  - Squidはユーザ認証機能，ユーザごとにアクセスできるコンテンツをURLにより制御する機能があるため，それを活用する
  - GSRAルータとCPROXY間で認証情報を共有するために，メッセージの送受信モジュールを実装する

比較評価

	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。 CPROXYの導入が必要。
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
学内からの利用	○	△	[既存] コンテンツサーバ接続時にユーザ認証を行う必要がある [提案] 通信がCPROXYを経由するように設定変更が必要

まとめ

- 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，コンテンツサーバーに手を加えずに，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