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

093430029　三浦 健吉
渡邊研究室

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．これを実現する場合，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技術の両方が必要である．

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セキュリティ技術を用いた VPN（Virtual Private Network）を構築する方法が一般的である．インターネット VPN を構築する方式には，PPTP（Point-to-Point Tunnering Protocol），L2TP（Layer 2 Tunnering Protocol），IPsec（Security Architecture for Internet Protocol），SSL（Secure Socket Layer）などがある．しかし，これらの技術は設定が面倒であったり，アドレス管理が必要になる等の課題がある．

コンテンツ単位のアクセス制御を実現する手法としては，プロキシサーバを利用する方法とコンテンツサーバ側で制御する方法がある．プロキシサーバを利用する方法では，コンテンツサーバへのアクセスを常にプロキシを経由するようことにより，アクセス制御を実現できる．しかし，既存の方式では，リモートアクセスとの連携が用意されていない．コンテンツサーバ側で制御する方法では，サーバごとにきめ細かい設定が可能であるが，管理が面倒であるという課題がある．

我々は，GSRA（Group-based Secure Remote Access）[1] [2] 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，GSRA 単独ではコンテンツ単位の制御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（CPROXY）を新たに導入し，GSRA と組み合わせる．これにより，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が可能となる．

2. GSRA

GSRA は NAT 越え技術 NAT-f（NAT-free procotol）[3] をベースとした独自のリモートアクセス方式である．

GSRA では，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，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．

GSRA は，NAT 越え技術にグループ単位での認証機能と通信暗号化機能を追加したもので，管理が容易でアプリケーションに制約がない．さらに，ポート番号単位のグルーピングを実現しており，アプリケーション種別ごとにアクセス制御が設定できる．しかし，アプリケーションの内容には干渉しないので，コンテンツ単位のグルーピングはできない．

3. 提案方式

提案システムの通信シーケンスを図 1 に示す．

EN は外部ノード（External Node），IN は内部ノード（Internal Node）である．EN は WEB ブラウザとし，IN は WEB ブラウザとする．EN が IN に対して HTTP 通信を開始する場合について述べる．コンテンツ制御プロキシ（以下 CPROXY）は一般的なプロキシサーバに独自機能を追加したものである．

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ものとし，プライベートアドレスを保有している．IN1 は企業や大学等など組織のネットワークに存在し，同様にプライベートアドレスを保有している GSRA ルータは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．

提案方式では，GSRA と CPROXY 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．

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，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．

(2) 通信開始　EN は，宛先が内部仮想アドレスのパケットを送信しようとする．ここで，EN はパケットをカーネル内に待避させておき，グループ認証を行う．

(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．認証成功の場合，EN はポート番号 t を予約する．

(4) バインディング処理，マッピング処理　EN はホームルータと GSRA ルータに対して IN と通信する際に必要なマッピングを行う．

(5) CPROXY ネゴシエーション処理

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，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．

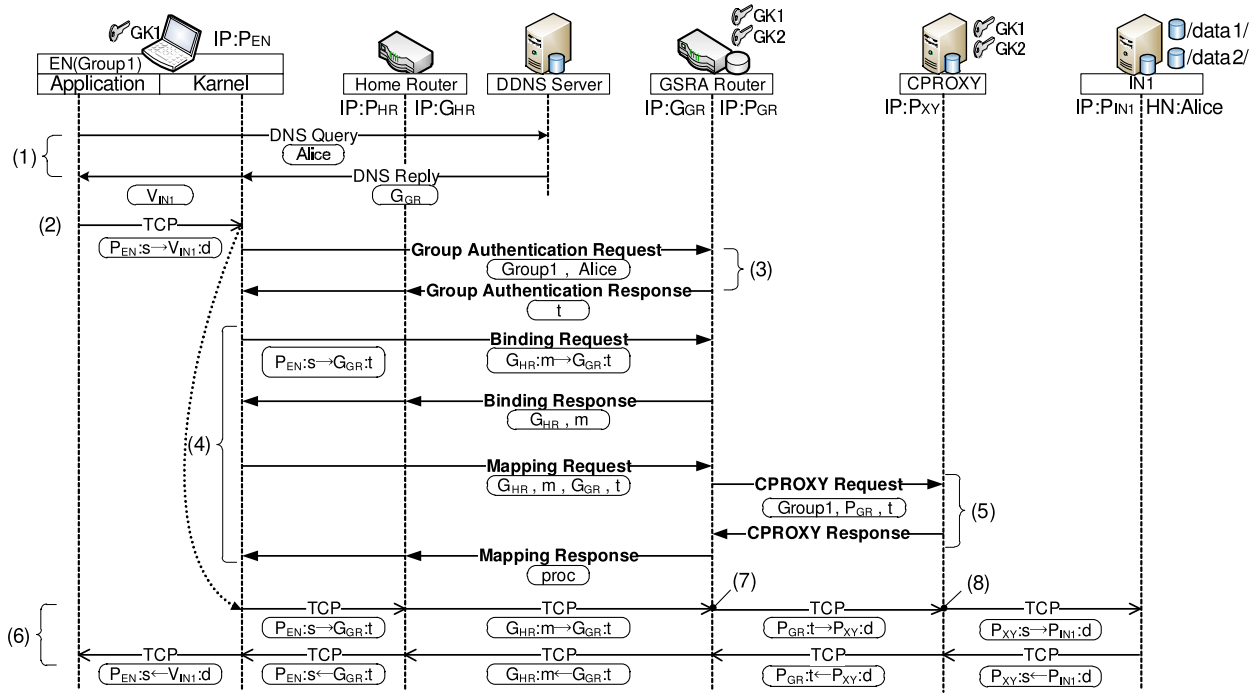


図 1: 提案方式の動作シーケンス

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　待避させていたパケットを復帰させ，宛先を GSRA ルータにマッピングしたポート番号に変換し，送信する．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 (7) においてパケットを復号後，マッピングテーブルに基づいて宛先の IP アドレスを PROXY に変換し，送信する．CPROXY では (8) において，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．

4. 動作確認と性能評価

プロトタイプシステムの実装を行い，EN が所属するグループ番号に対応するコンテンツにのみアクセスできることを確認した．

提案方式において，CPROXY を経由してコンテンツにアクセスする場合と，GSRA 単独で CPROXY を経由せずコンテンツにアクセスする場合の性能を比較評価した（表 1）．提案方式の機能を実装した結果，本来の GSRA に対する性能の劣化の度合いを測定した．CPROXY とのネゴシエーション通信には 0.19ms かかることが分かった．CPROXY 経由でコンテンツを取得した際に，HTTP 通信開始から終了までの時間を測定し，0.63ms の遅延があることが分かった．測定結果から，提案方式の実装による機能の劣化は非常に少ないものといえる．

また，スループットについても測定を行った（表 2）．EN と GSRA ルータ間に Dummynet（設定は表 3）を設置し，擬似的にインターネット接続の環境を構築した．性能評価の結果から，実際のインターネットを利用し，自宅などから大学のコンテンツサーバにアクセスする場合などにおいて，提案方式は十分に有用であると考えられる．

表 1: 動作時間

	GSRA	提案方式	遅延
ネゴシエーション時間	1.49ms	1.68ms	0.19ms
コンテンツ取得時間	3.61ms	4.24ms	0.63ms

表 2: スループット

	GSRA	提案方式
平文通信	32.2Mbps	31.1Mbps
暗号通信	29.6Mbps	24.6Mbps

表 3: Dummynet の設定

bandwidth	40Mbps
delay	20ms (片方向 10ms)
packet loss rate	0

参考文献

[1] 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).

[2] 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).

[3] 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).

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
渡邊研究室
093430029 三浦 健吉

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

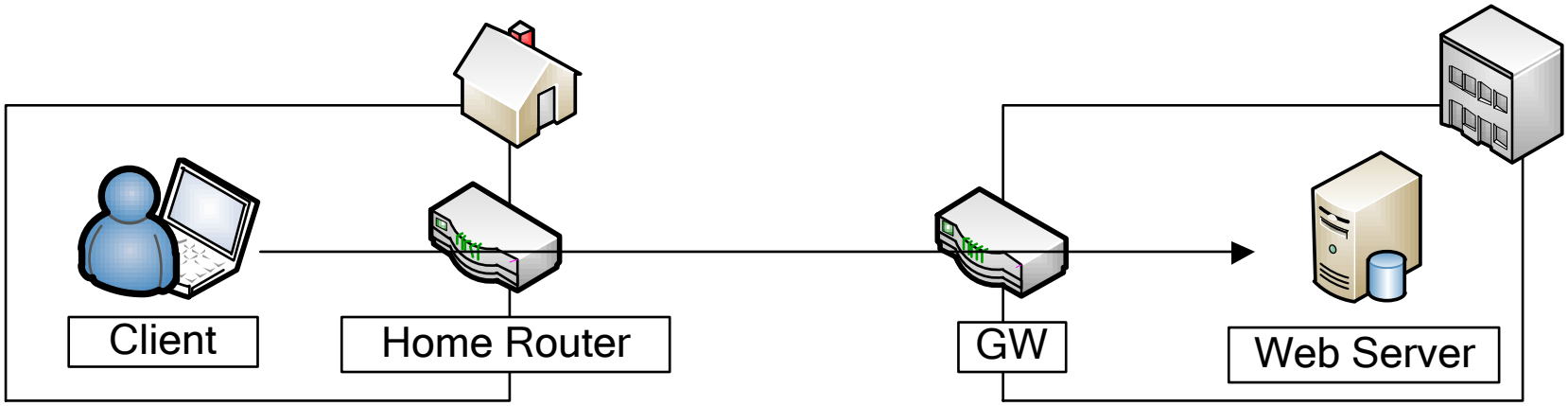
目的

- 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（科目履修者のみ教材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（学生）は自宅から教材コンテンツにアクセスする
  →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

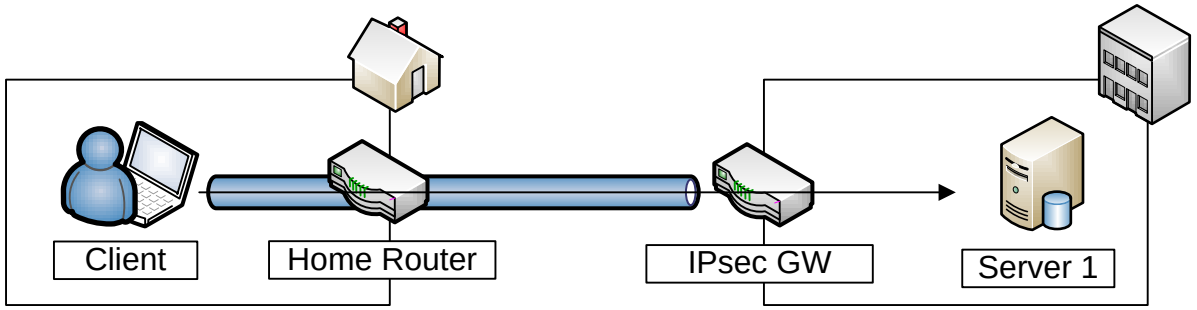
*鈴木秀和，渡邊晃：通信グループに基づくサービスの制御が可能なNAT 越えシステムの提案，情報処理学会論文誌，2010

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，DICOMO20010

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
  - 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

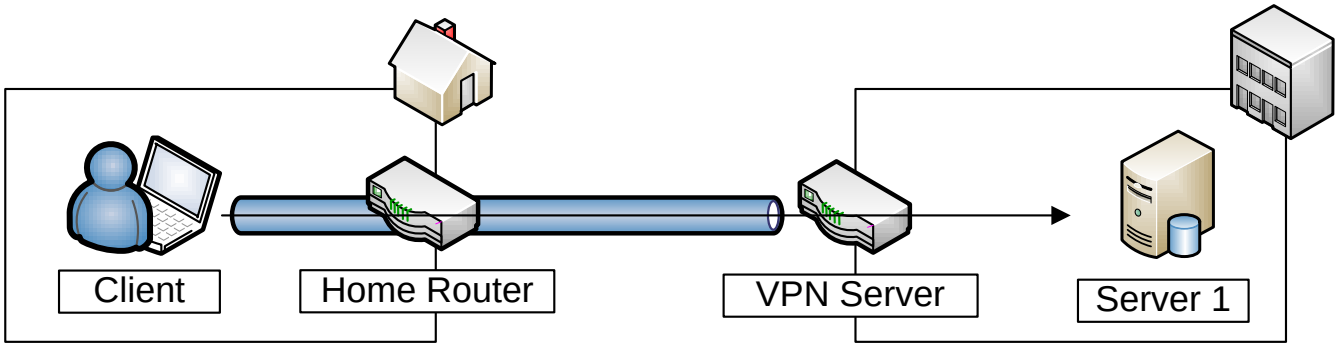
  →ホームNATと相性が悪い
- 端末ごとに設定が必要な項目が多く，管理負荷が高い



SSL-VPN

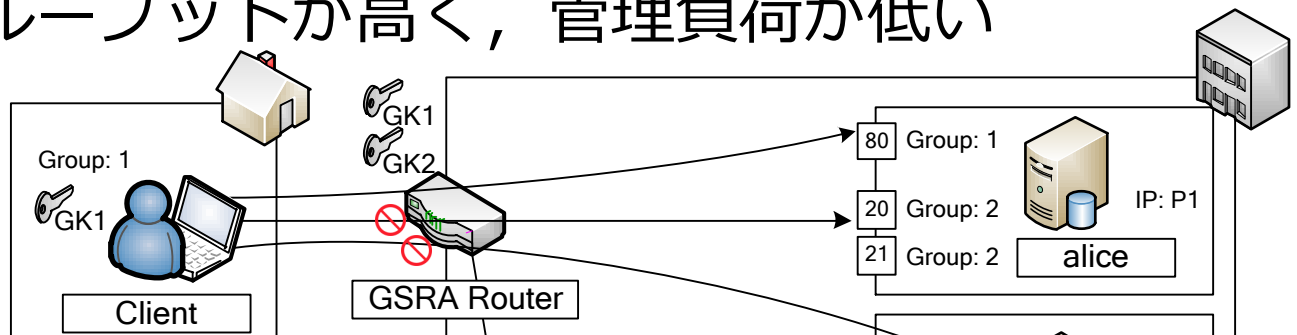
- クライアントがWebブラウザの場合
  - クライアントは一般的なWebブラウザだけで良い
  - アプリケーションの種類がWebに限定される

- 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

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

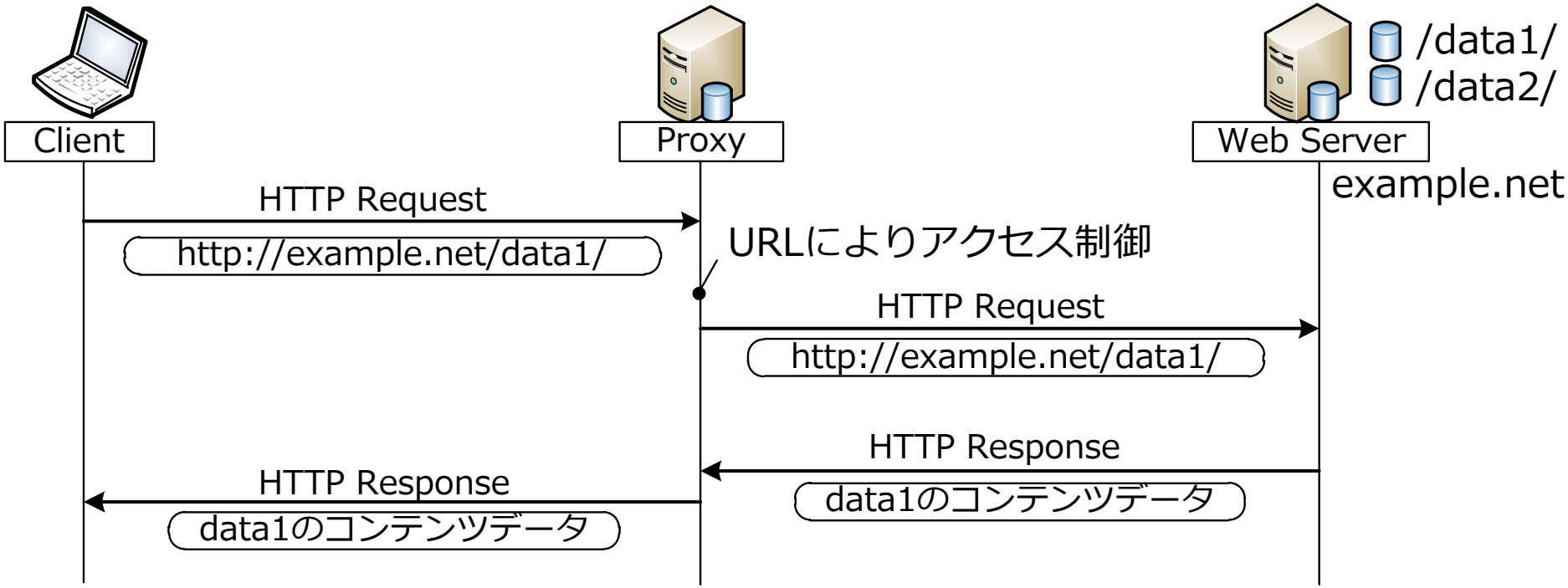
鈴木健太，鈴木秀和，渡邊晃：NAT越え技術を応用したリモートアクセス方式の提案と設計，DICOMO20010

コンテンツサーバ側で実現する方法

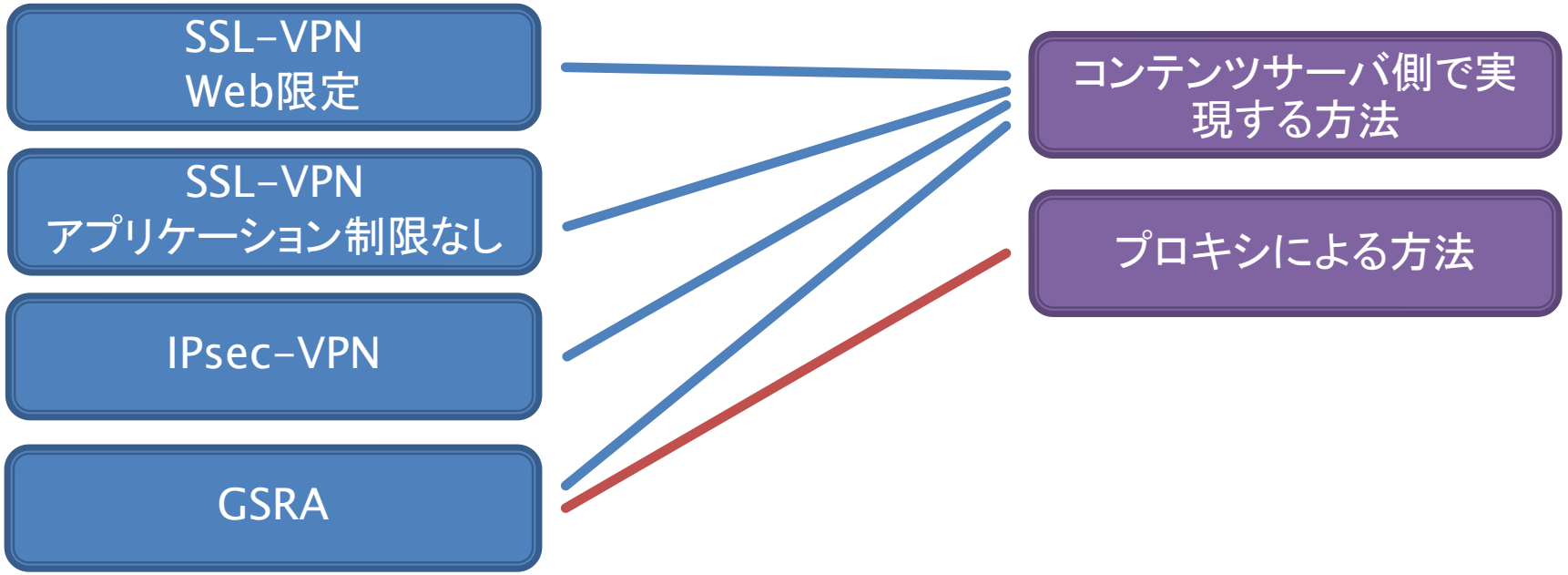
- 動的なページを生成する技術を使用する
- コンテンツサーバにPerl/PHP/JSPなどで記述されたプログラムを導入する
- ログインしたユーザごとに，異なるコンテンツを提示できるようにする

Webプロキシサーバ

- 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



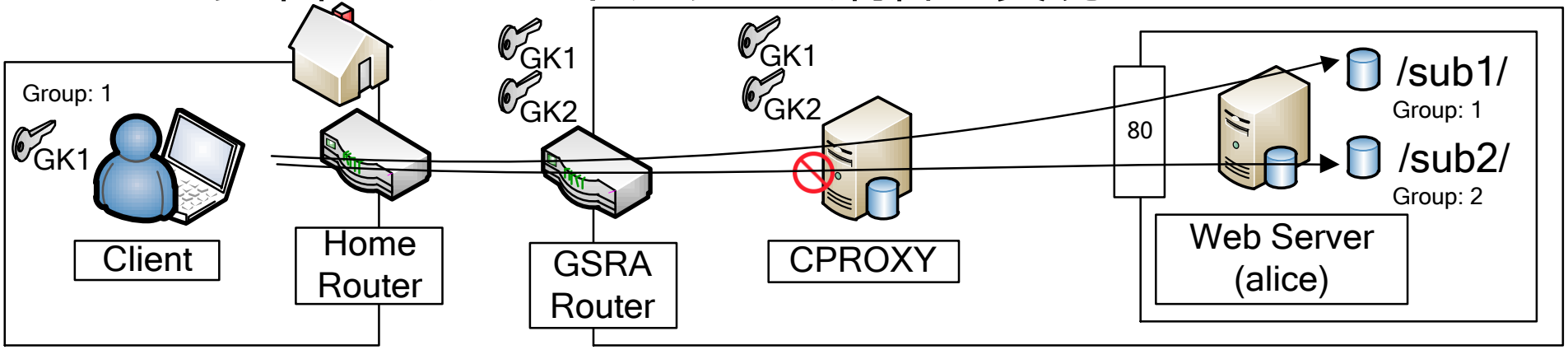
既存技術の組み合わせ



- 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
- 一般的なリモートアクセス技術は，プロキシと独立した技術であるため，組み合わせることは難しい
- 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

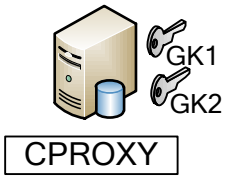
提案システムの概要

- GSRAとプロキシを組み合わせる
- グループの定義方法
  - 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）
  - コンテンツ単位（URL単位）
- 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

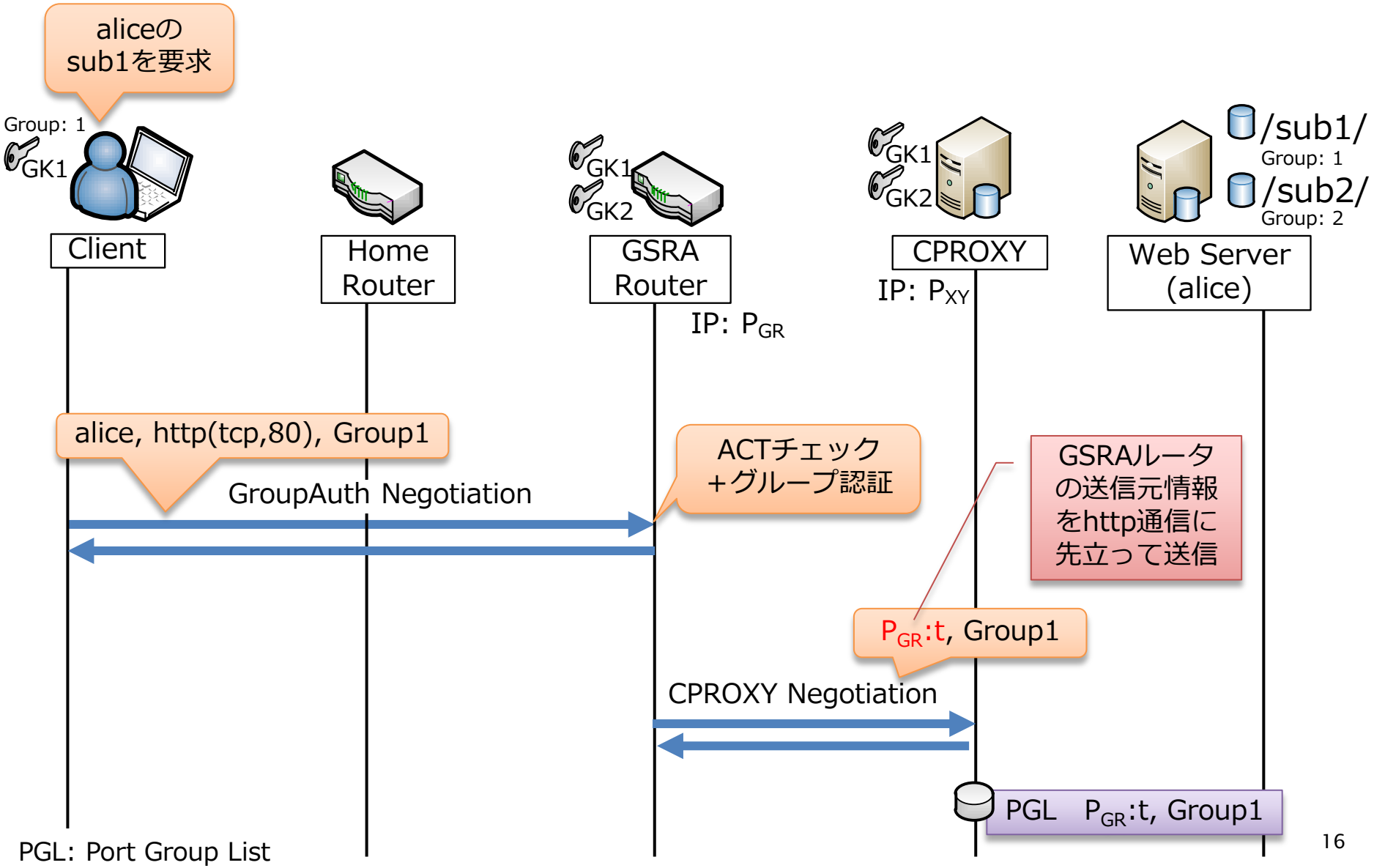
- CPROXYはACL（AccessList）を保有
  - URLとアクセス許可グループを関連付ける
- CPROXYはグループ認証用の鍵を保有



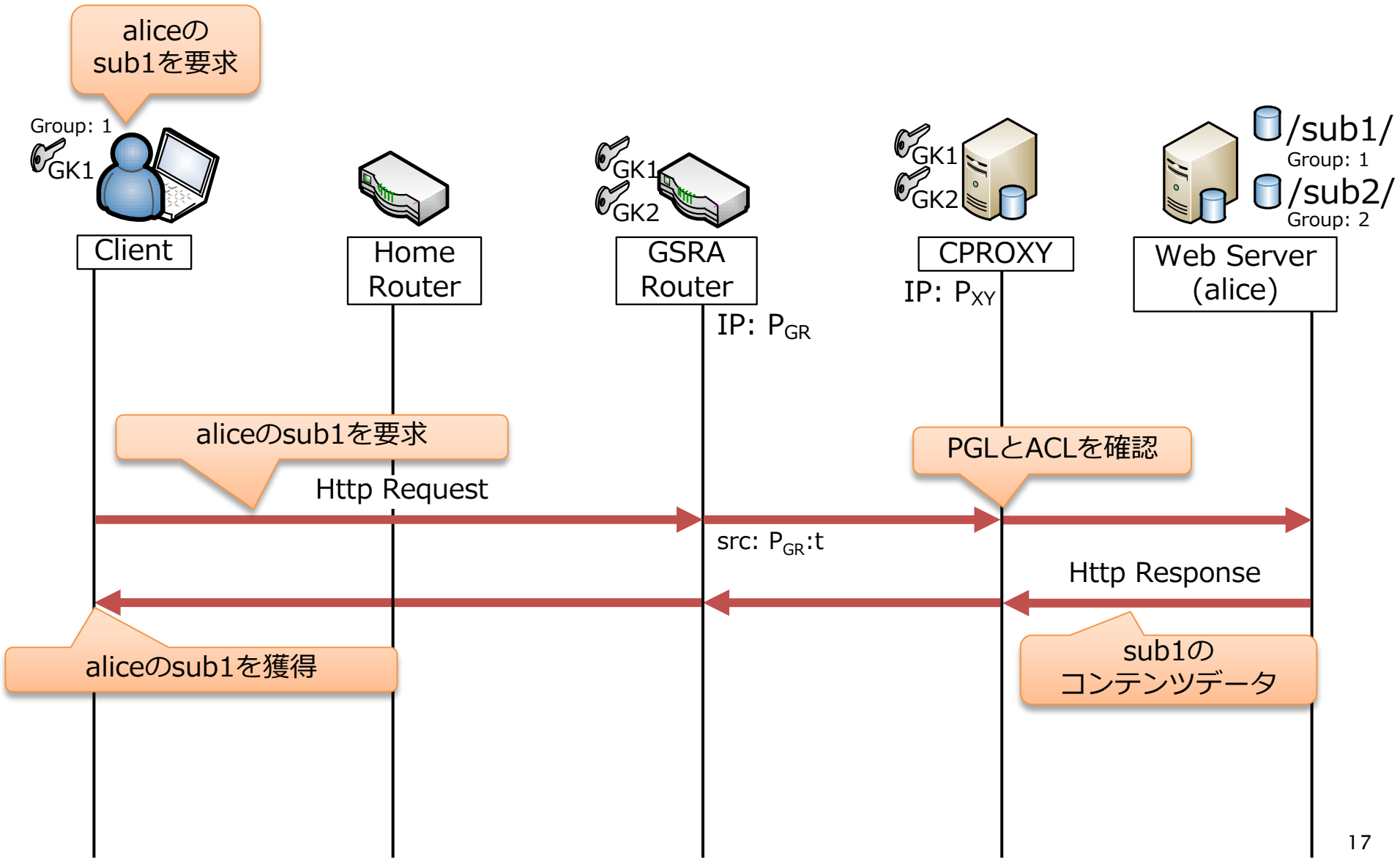
ACL

Hostname	Path	Permit	Group
alice	/sub1/*	allow	Group1
	/sub2/*	allow	Group2

提案システムの概略シーケンス（1/2）



提案システムの概略シーケンス（2/2）

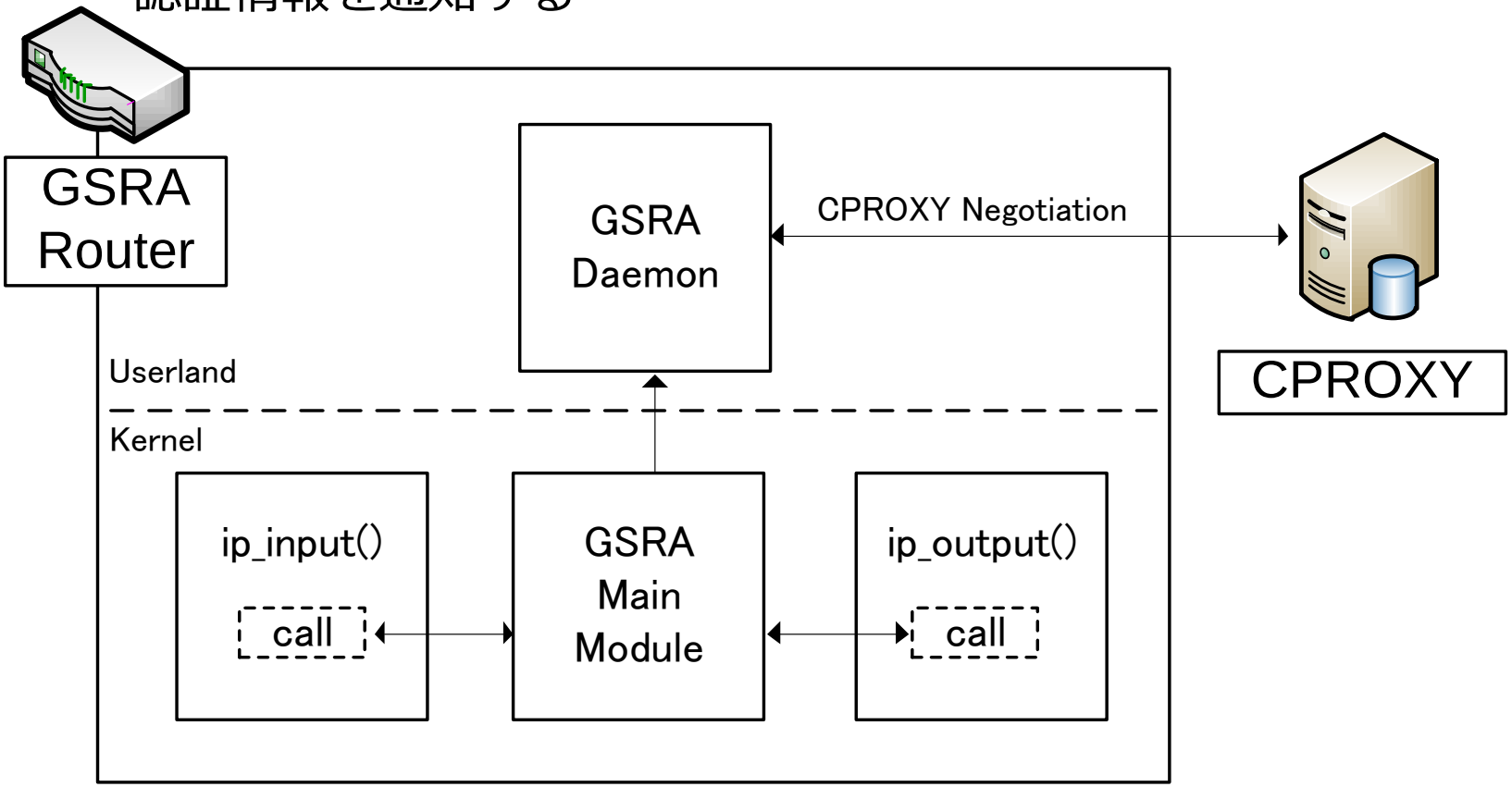


実装と動作確認

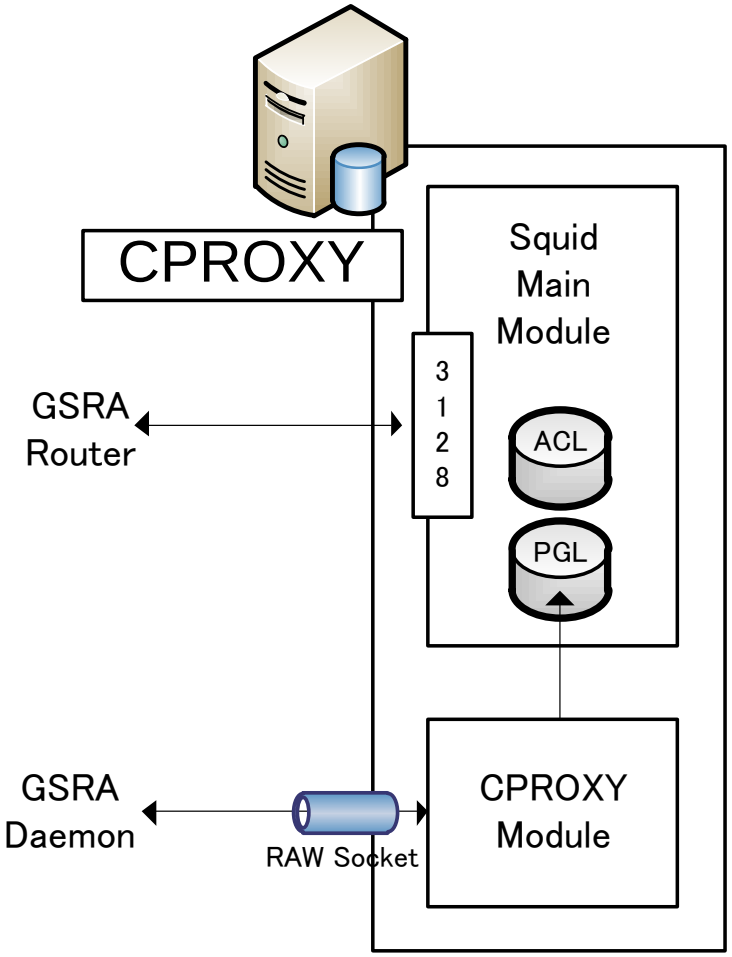
- プロトタイプシステムの実装を完了し，提案システムの動作について確認を行った.

実装：GSRAルータ側

- GSRAはFreeBSD7.2のカーネルに実装・動作検証済み
- GSRAデーモンを新たに作成
- カーネル内のGSRAモジュールから通知を受け取ると，CPROXYに認証情報を通知する



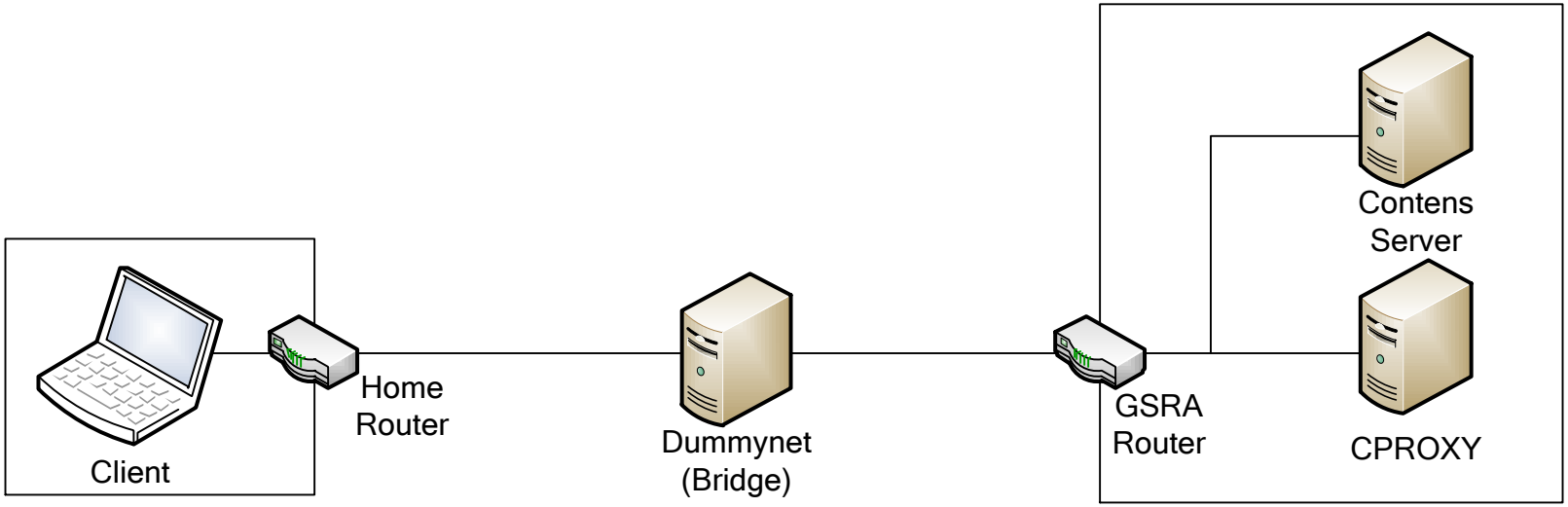
実装：CPROXY側



- Squid 3.1.4を改造し，CPROXYを作成
- ACL（Access List）
  - URLとアクセスの可否を管理するリスト
  - リストにグループ番号を追加実装
- PGL（Port Group List）
  - ポート番号とグループ番号を対応付けて管理
- CPROXYモジュールは，GSRAデーモンからCPROXYリクエストを受け取ると，PGLに情報を追加

性能測定環境

- Dummynetによる擬似的なインターネット環境を構築
  - 遅延：20ms，帯域幅：40Mbps，パケットロス：無し



Name	OS / Product	CPU	Memory	NIC
Client	FreeBSD 7.2	Pentium4 3.4GHz	1024MB	1000Base-TX
Home Router	Baffalo WZR-G144NH			
Dummynet	FreeBSD 8.1	Pentium4 2.8GHz	512MB	100Base-TX
GSRA Router	FreeBSD 7.2	Pentium4 3.4GHz	2048MB	100Base-TX
CPROXY	Debian GNU/Linux 5.0	Core 2 Duo E6600 2.4GHz	4096MB	100Base-TX
ContensServer	FreeBSD 7.2	Pentium4 2.8GHz	1024MB	100Base-TX

性能評価（動作時間）

- ネゴシエーション時間（Dummynet無効時）
  - HTTP通信以前のネゴシエーション時間
- コンテンツ取得時間（Dummynet無効時）
  - 0Byteのコンテンツを取得したときに，HTTP通信開始から終了まで
- 10回試行し平均値を求めた

測定箇所	GSRA	提案方式	遅延
ネゴシエーション時間	1.49ms	1.68ms	0.19ms
コンテンツ取得時間	3.61ms	4.24ms	0.63ms

- CPROXYネゴシエーションの通信時間は0.19ms
- CPROXY経由のため，0.63msの遅延が発生

性能評価（スループット）

- HTTPクライアント：wget 1.11.4
- HTTPサーバ：Apache 2.2.11
- CPROXYのHDDにキャッシュが保存されないように設定
  - 5回試行し平均値を求めた

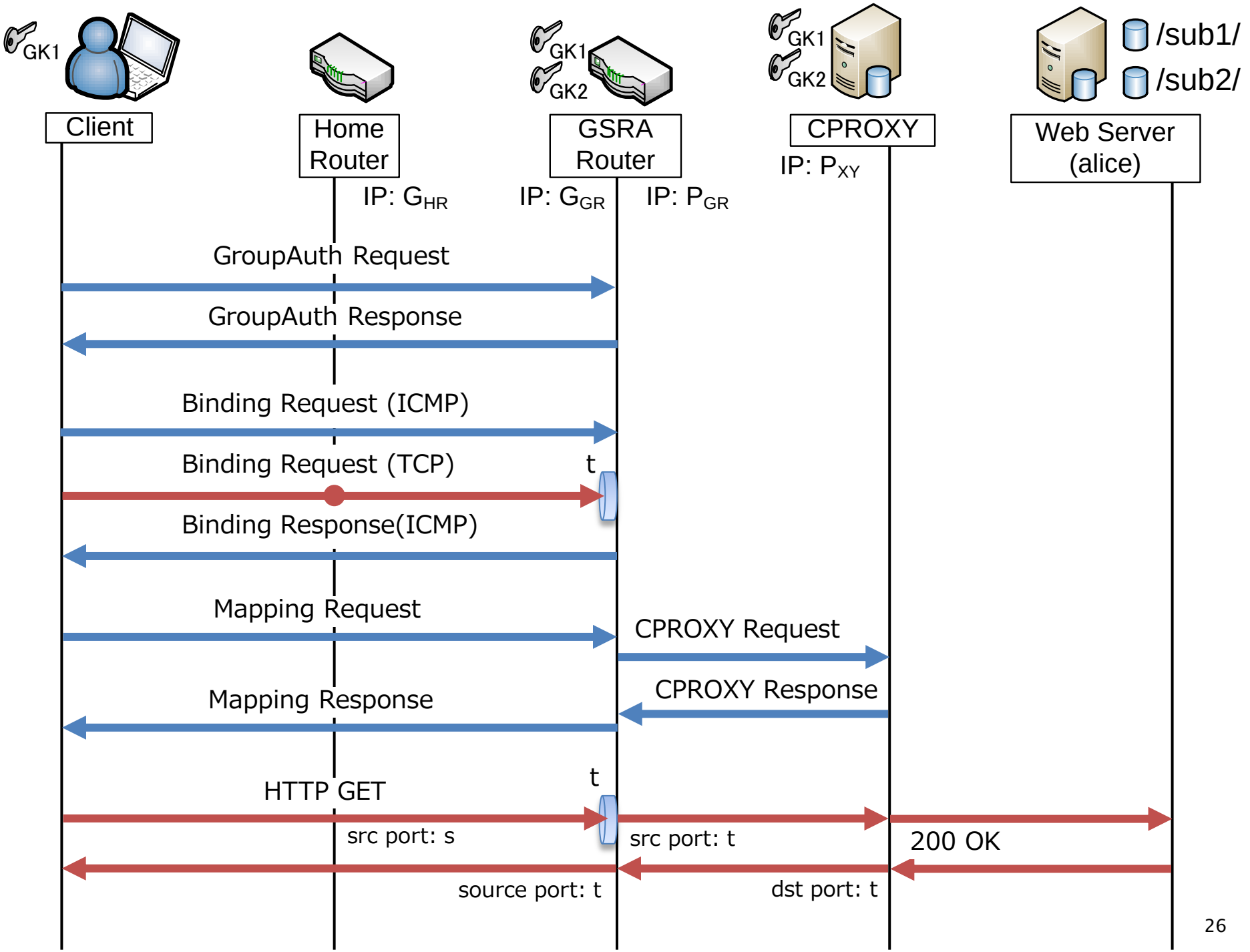
	GSRA	提案方式	性能劣化
Dummynet無効時	68.3Mbps	33.2Mbps	53%劣化
Dummynet有効時	29.8Mbps	24.6Mbps	14%劣化

- CPROXY経由の通信のためスループットは低下
- 実際のインターネットを想定した環境では，十分なスループットが得られた

むすび

- GSRA とCPROXY 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.
- 性能評価の結果から，実際に自宅などから大学のコンテンツサーバにアクセスする場合などにおいて提案方式の有用性を確認した
- 今後はセッション数を増やした場合のサーバ負荷について性能測定を行う

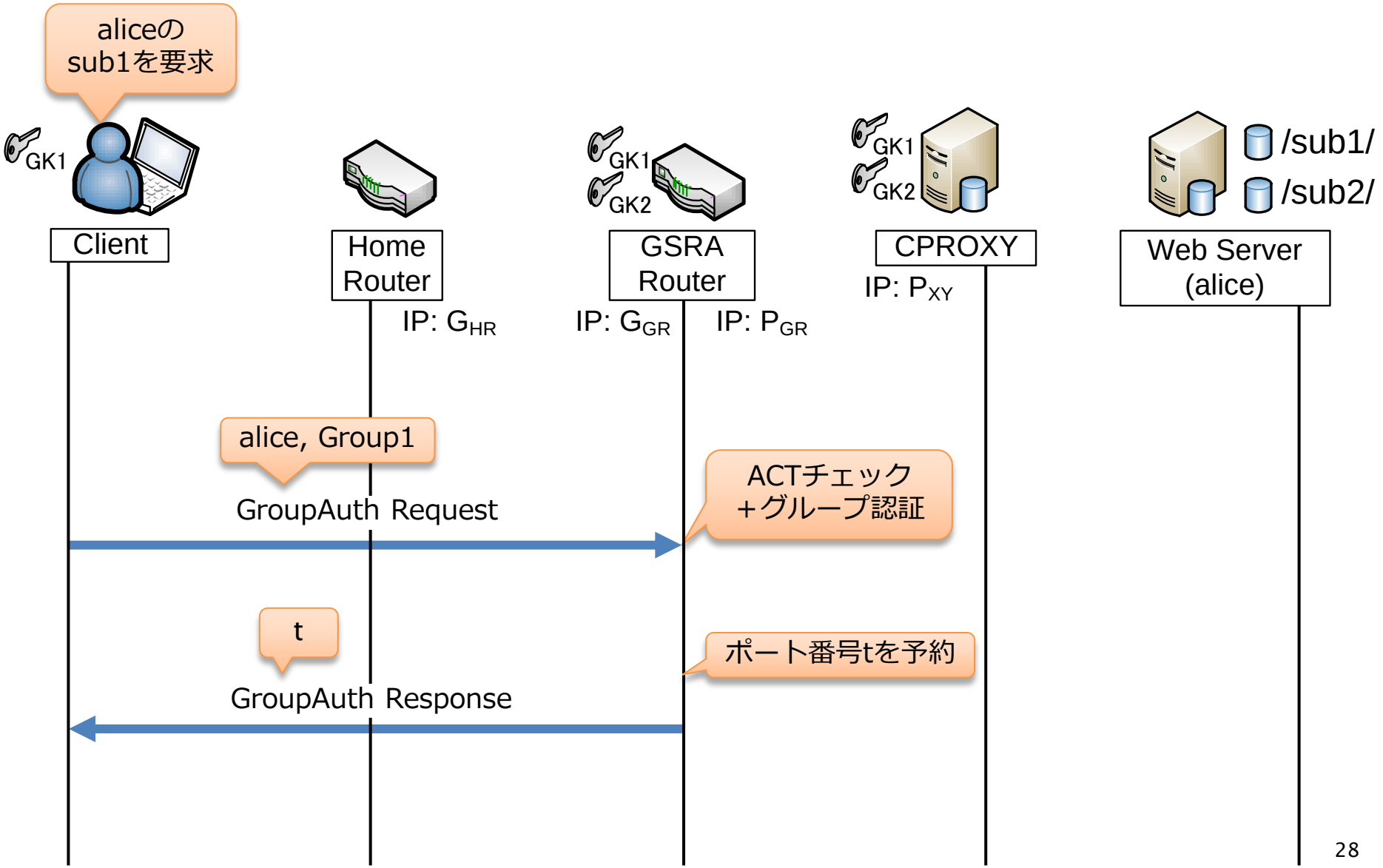
補足資料


GK1
Client
Home Router
IP: G_{HR}
GK1
GK2
GSRA Router
IP: G_{GR}
IP: P_{GR}
GK1
GK2
CPROXY
IP: P_{XY}
/sub1/
/sub2/
Web Server (alice)
GroupAuth Request
GroupAuth Response
Binding Request (ICMP)
Binding Request (TCP)
t
Binding Response(ICMP)
Mapping Request
CPROXY Request
CPROXY Response
Mapping Response
HTTP GET
t
src port: s
src port: t
200 OK
source port: t
dst port: t

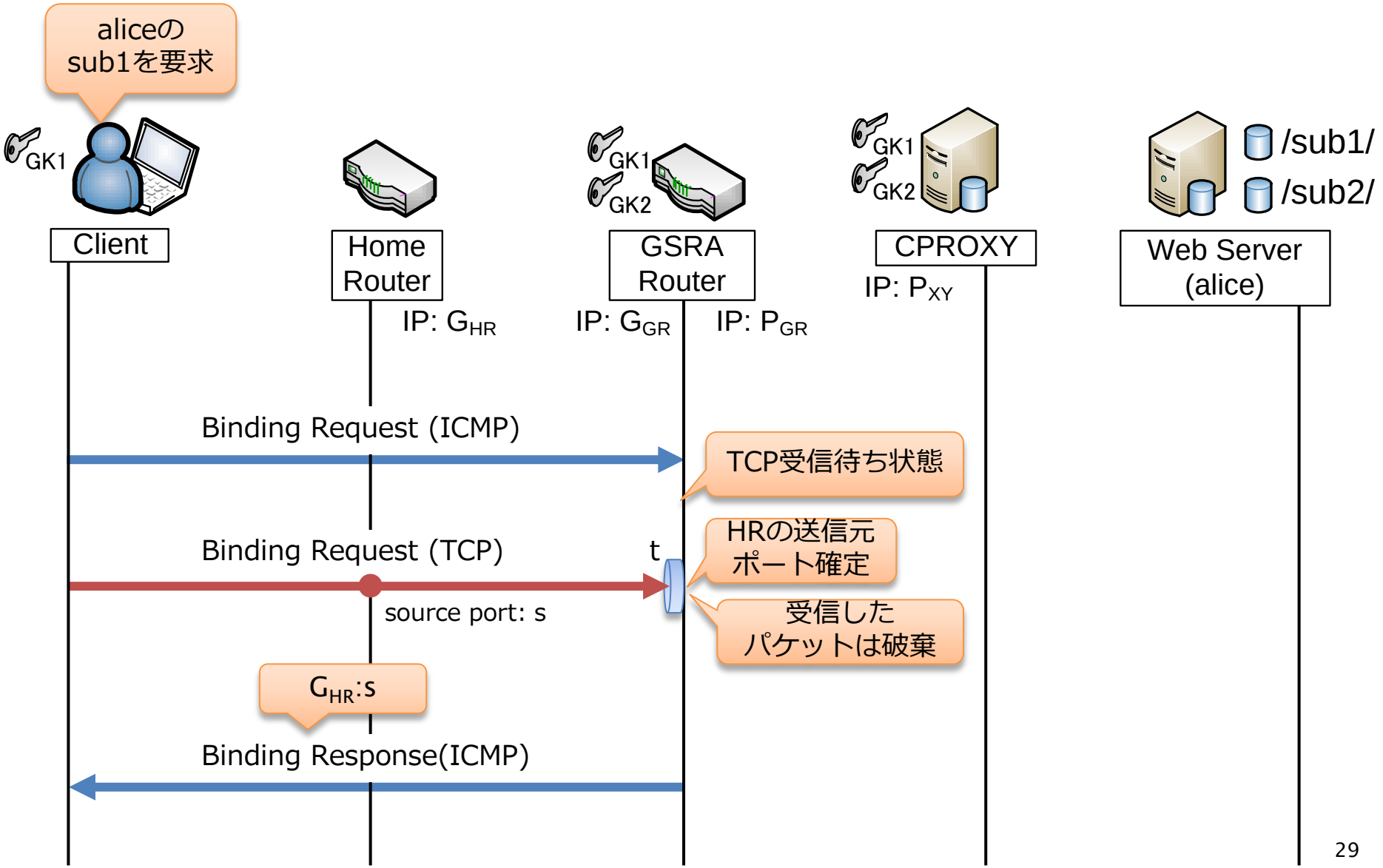
IPsec-VPN：NATとの相性

- 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をIPsecパススルーに対応したNATに交換すれば，NAT越えは可能

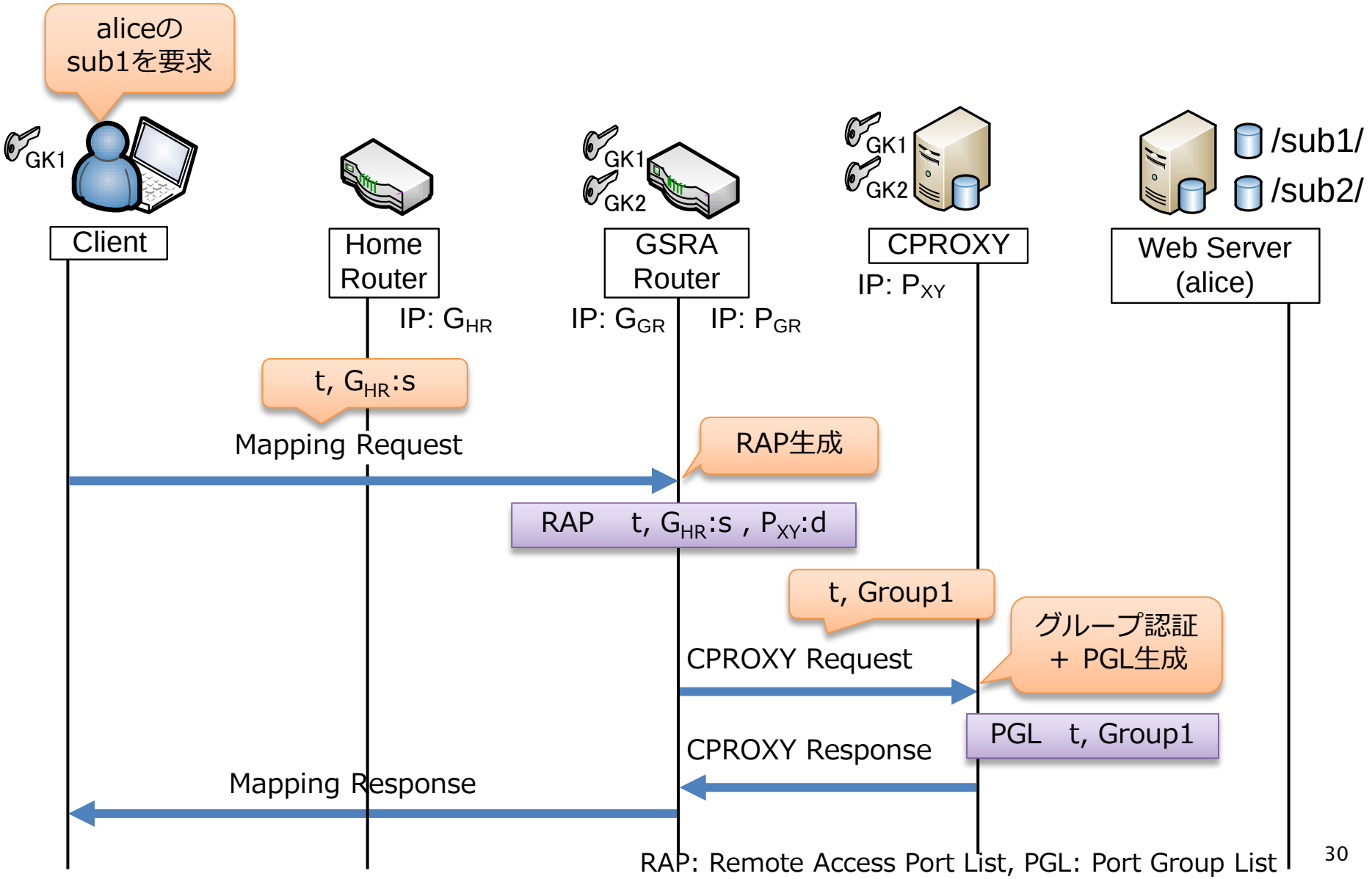
提案システムの詳細シーケンス（1/4）



提案システムの詳細シーケンス（2/4）



提案システムの詳細シーケンス（3/4）



RAP: Remote Access Port List, PGL: Port Group List

提案システムの詳細シーケンス（4/4）