平成22年度　修士論文

邦文題目

# 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

英文題目

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

情報工学専攻

(学籍番号: 093430029)

三浦　健吉

提出日: 平成23年1月31日

名城大学大学院理工学研究科

# 内容要旨

近年，大学組織において講義資料の電子化やリモートアクセスシステムの導入が進んでいる．その中で，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．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コンテンツには干渉できない．そこで，本論文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ために，GSRA とプロキシの技術を組み合わせる方式を提案する．提案方式について，プロトタイプシステムの実装を行い，動作確認と性能評価を行った．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，提案方式は十分に有用であると考えられる．

# 目 次

**第 1 章　はじめに** **1**

**第 2 章　既存技術** **3**

2.1　リモートアクセス技術 . . . . . 3

2.2　コンテンツ単位のアクセス制御技術 . . . . . 5

**第 3 章　GSRA** **8**

**第 4 章　提案方式** **11**

**第 5 章　実装** **14**

5.1　GSRA ルータの改造 . . . . . 14

5.2　CPROXY のモジュール構成 . . . . . 14

**第 6 章　動作検証と性能評価** **16**

6.1　動作検証 . . . . . 17

6.2　性能評価 . . . . . 17

**第 7 章　まとめ** **19**

**謝辞** **21**

**参考文献** **22**

**研究業績** **24**

**付 録 A　記号の定義** **25**

# 第1章　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，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．このとき，サーバのコンテンツに対応してユーザをグルーピングし，アクセス制御を実現できると有用である．例えば，大学内の Web サーバに学生がアクセスする場合，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 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．PPTP は暗号化の強度が弱いことや利用できる OS が制限される課題がある．L2F [5] はトンネリングのためのプロトコルであり，暗号化機能を備えていないため，そのまま使用されることはない．L2TP は PPTP と L2F の仕様を統合したもので，マルチプロコトルに対応している．しかし，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り，ヘッダの追加に伴いオーバヘッドが増加する欠点がある．そのため，近年はセキュリティ技術の IPsec や SSL を利用したインターネット VPN がよく利用される．しかし，IPsec は導入に複雑な設定が必要であり，運用するには相応の知識が必要となる．SSL はクライアントに Web ブラウザを利用するものと専用ソフトウェアを利用するものが存在する．クライアントに Web ブラウザを利用するものは，一般のクライアントをそのまま使用することができるが，アプリケーションが Web に限定されるという課題がある．クライアントに専用ソフトウェアを利用するものは，任意のアプリケーションを利用することができるが，サーバからクライアントに対してネットワーク設定情報を配布する必要があり，管理が煩雑である．

我々は，GSRA（Group-based Secure Remote Access）[6] [7] 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 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．IP アドレス単位およびポート番号単位のグルーピングが可能であり，ホストごとおよび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，同じホストの同じサービスで提供されている異なるコンテンツを識別することはできない．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ことができない．

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設定する方法がある．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サーバを経由するように設定することで，コンテンツ単位のアクセス制御を実現する．しかし，既存のプロキシを利用する方式では，イントラネットでの利用を前提としたものがほとんどであり，セキュリティ的に課題がある．コンテンツサーバ側で設定する方法では，コンテンツを配布する際にユーザ認証を実施することで，コンテンツ単位のアクセス制御をきめ細かく実現できる．しかし，コンテンツサーバが既に稼働中の場合には，導入が煩雑である点が課題である．

そこで，本論文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ために，GSRA とプロキシの技術を組み合わせる．GSRA システムに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．

以降，2 章において既存の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について説明する．3 章においてリモートアクセス技術 GSRA について詳細に説明する．4 章において，GSRA と CPROXY 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．5 章において，今回試作したプロトタイプシステムの実装方法について述べる．6 章において，動作検証と性能評価の結果を示す．そして第 7 章でまとめる．

# 第2章　既存技術

本章では，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について述べる．リモートアクセス技術として，SSL-VPN，PPTP，L2TP/IPsec，GSRA の概要について述べる．GSRA については，以降の第 3 章でさらに詳細に述べる．

コンテンツ単位のアクセス制御技術として，コンテンツサーバで設定する方法とプロキシサーバを利用する方法について述べる．

## 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 IKEv2（Internet Key Exchange）[8]による認証と暗号鍵の共有を実施し，IPsec ESP（Encapsulating Security Payload）[9]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 [10] 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．

また，IPsec-VPN はリモートアクセスに利用する場合，鍵交換プロトコル IKEv2 で定義されている IPsec CP（Configration Payload）により，内部ネットワークの設定情報を配布する．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．

### 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

サーバが中継サーバの役割を果たすことでリモートアクセスを実現する．

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 [11]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．また，サーバ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り，配布されたネットワーク設定情報と実際のネットワーク構成が重複すると，正しく通信が行われないという課題がある．

### 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）[12]のパケットを GRE（Generic Routing Encapsulation）[13]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）[14]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 [5]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場合が多い．このため，ヘッダの追加に伴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）[6] [7]と呼ぶリモートアクセス技術を提案している．GSRA は，NAT-f（NAT-free procotol）[15]を NAT 越え技術ベースとした技術である．

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．

また，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という特徴がある．しかし，GSRA はネットワークレベルで実装されており，アプリケーションの内容に干渉しないため，コンテンツ単位のアクセス制御はできない．

第 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，他の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．

## 2.2 コンテンツ単位のアクセス制御技術

### 2.2.1 コンテンツサーバ側で実現する方法

コンテンツサーバ側で動的 Web ページを構成するための技術を利用することで，コンテンツ単位のアクセス制御が可能である．動的 Web ページを構成するプログラミング言語として，Perl [17]，PHP [18]，JSP [19]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．アプリケーションが Web に限

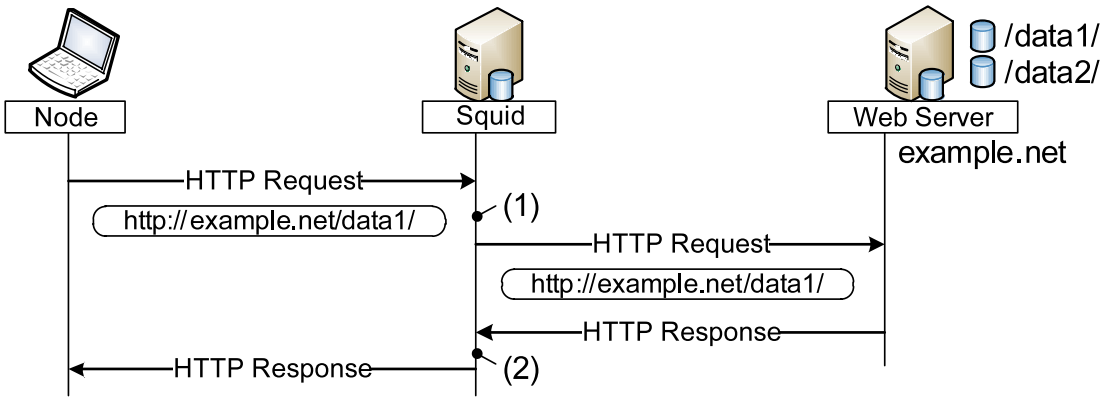


**図 2.1　Squid によるアクセス制御**

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おいても SSO（Single Sign-On）を実現できる．

しかし，この手法は，コンテンツサーバごとに設定が必要であり，サーバ台数が多くなると，管理が煩雑である．

### 2.2.2　プロキシサーバによる方法

プロキシサーバを利用することによりコンテンツ単位のアクセス制御を一括して実現することが可能である．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．代表的なプロキシサーバのソフトウェアとして，Squid [20]などがある．

図 2.1 を用いて 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．

プロキシサーバによる方法は，一般に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．

# 第3章　GSRA

本章では，提案のベースとなる GSRA について説明する．なお，本論文で使用する記号は付録 A に示す．

図 3.1 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．ホームルータは改造が不要で，そのまま利用できる．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，IN1 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．

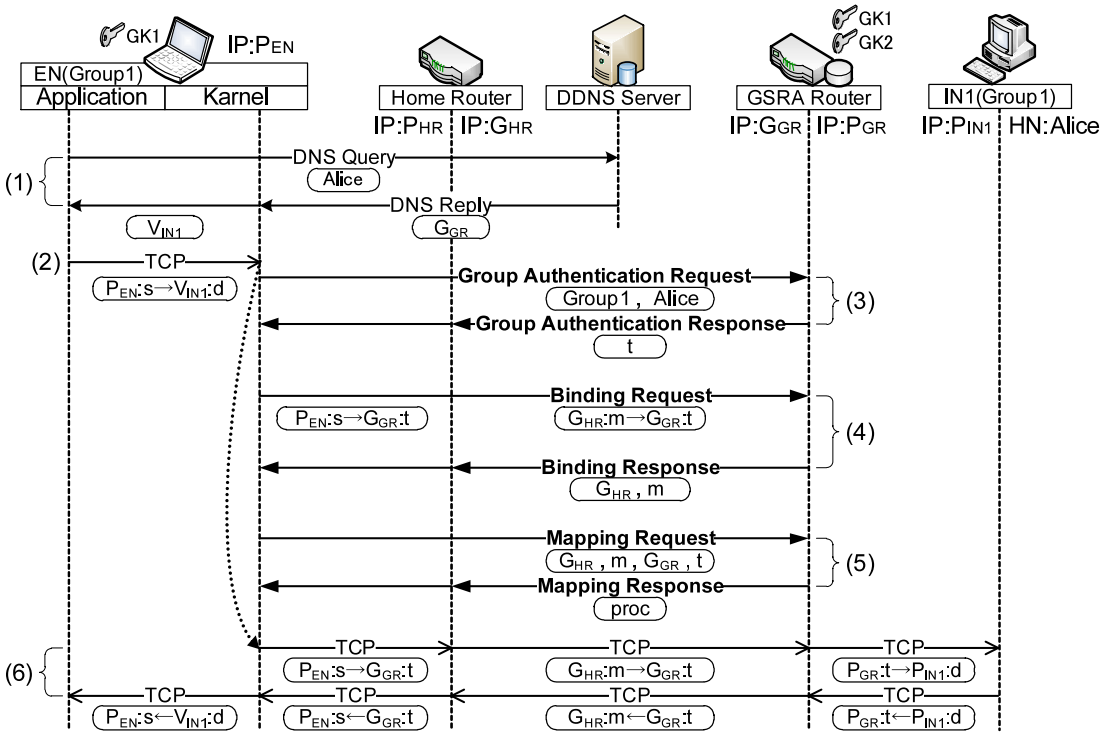


**図 3.1　GSRA の動作シーケンス**

**(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．VAT テーブルは内部仮想 IP アドレスと GSRA ルータに割り当てられたマッピングアドレスの情報を関連付けるために使用する．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．

**(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 3.1 に示す．ここで，$\leftrightarrow$ は通信を，$\Leftrightarrow$ 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 3.1　GSRA ルータのマッピングテーブルと EN の VAT テーブル**

| | | |
|---|---|---|
| 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．

# 第4章　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 4.1 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 4.1 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．

通信シーケンスにおける名前解決から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，提案方式の動作について説明する．

**表 4.1　CPROXY のアクセス制御テーブル**

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

**表 4.2　通信中における CPROXY のアクセス制御テーブル**

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

**(1) CPROXY への認証情報の通知**

GSRA ルータは EN からのマッピング要求受け取ると 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/

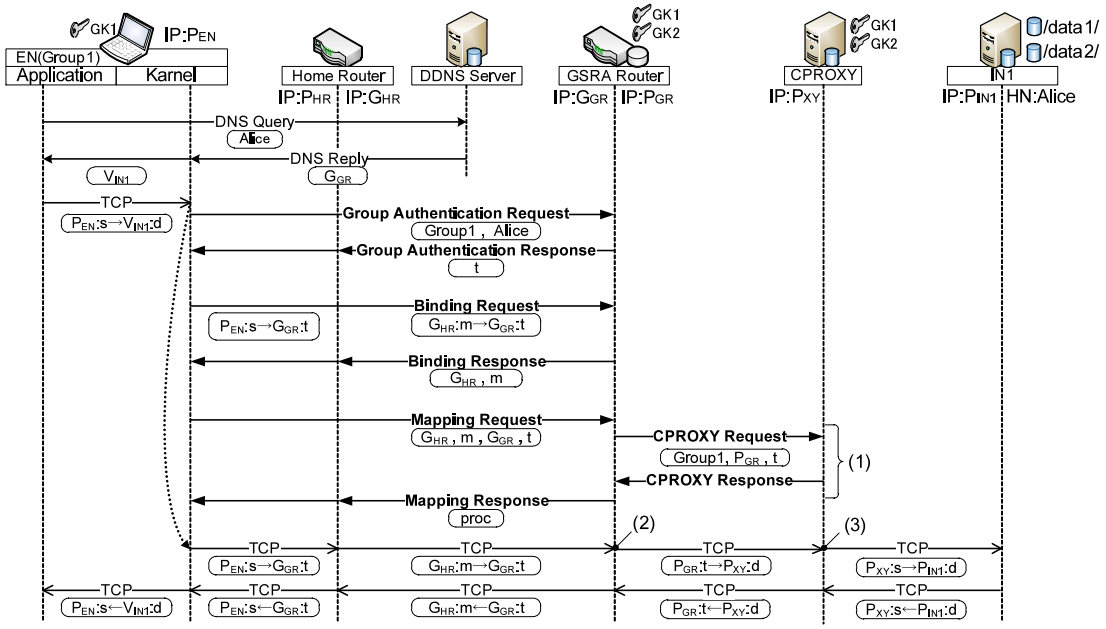


**図 4.1　提案方式の動作シーケンス**

ポート番号 $P_{GR}$:t を通知する．これを受け取った CPROXY は，表 4.2 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 4.3 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 3.1 と表 4.3 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，通信開始時に待避させていたパケットを復帰させて通信を開始する．

**表 4.3　提案方式のマッピングテーブルと VAT テーブル**

| | | |
|---|---|---|
| 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 | ： | $\{ G_{EN} : s \leftrightarrow V_{IN1} : d \} \Leftrightarrow \{ G_{EN} : s \leftrightarrow G_{GR} : t \}$ |

### (2) 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，表 4.3 の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．

**(3) コンテンツ単位のアクセス制御処理**

CPROXY は GSRA ルータから送信されたパケットを受け取ると，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． (1) 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る送信元ポートであれば，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．

# 第5章　実装

提案方式の動作確認と性能評価を行うために，プロトタイプシステムの試作を行った．

GSRA は，参考資料 [6] [7]にて，実装と性能評価を既に終えている．GSRA は，FreeBSD のカーネル内の IP 層に実装されている．提案方式を実行させるため，CPROXY に対する認証情報を通知するための専用のデーモン（以下 GSRA デーモン）を実装した．

CPROXY は, Squid に対して機能を追加した．CPROXY は, Linux 系のディストリビューションである Debian GNU/Linux において実装を行った．アクセス制御を実行する部分に対して GSRA で定義したグループ単位で認証を行う機能と，GSRA デーモンと通信を行うための機能を追加した．

## 5.1　GSRA ルータの改造

図 5.1 に GSRA ルータのモジュール構成を示す．GSRA モジュールは IP 層に実装された GSRA ルータの機能を実現するモジュールである．GSRA デーモンは CPROXY に対する認証情報を通知するためのデーモンである．今回，GSRA モジュールの一部を改造し，GSRA デーモンを新たに開発した．

GSRA には，Divert ソケットをベースにして作成した GSRA ソケットというソケットが存在し，ユーザランドとカーネルの間でメッセージの送受信を行うことが可能である．提案方式の実装にあたり，GSRA ソケットを利用し，EN からの通信に割り当てられる予定の送信元ポート番号の情報や，EN が所属するグループの情報をカーネルからユーザランドへ通知できるようにした．GSRA デーモンは，Divert ソケットを利用し，CPROXY に対する CPROXY リクエストを送信する機能を実装した．CPROXY リクエストは ICMP パケットをベースとした独自パケットである．

## 5.2　CPROXY のモジュール構成

図 5.2 に CPROXY の実装を示す．CPROXY には，Squid の本来の機能が実装されている Squid メインモジュールと，GSRA デーモンとの通信機能を実装した CPROXY モジュールで構成されている．

Squid メインモジュールは，TCP の任意（ここでは 3128 番）のポートでリッスンを行い，HTTP パケットの到着を待機する．Squid には，アクセス制御の機能を実現するために，ACL（Access List）と呼ばれるテーブルが存在し，アクセス先 URL とアクセスの可

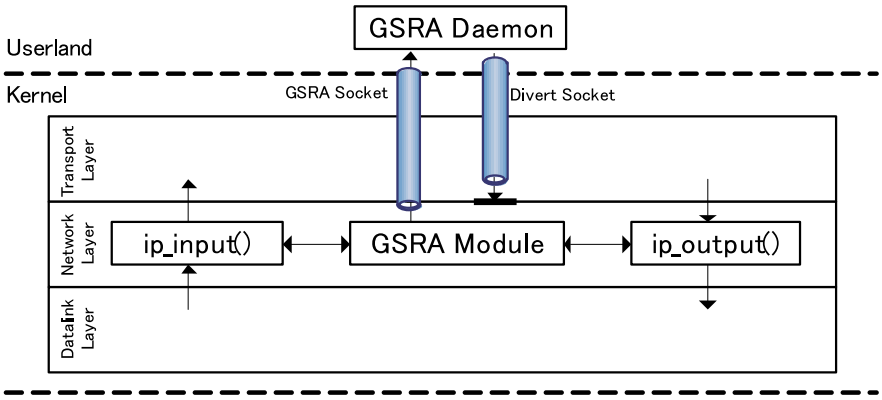


**図 5.1　GSRA ルータのモジュール構成**

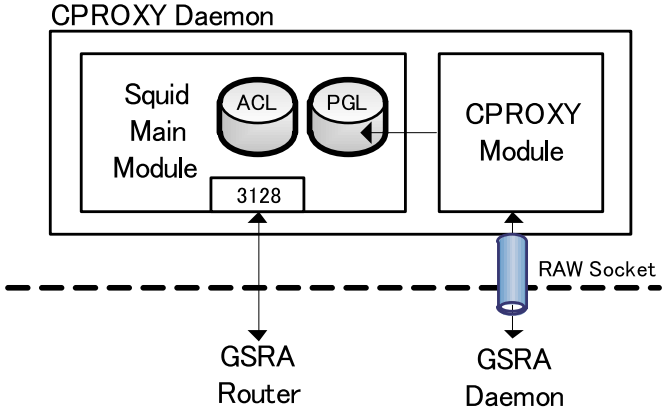


**図 5.2　CPROXY のモジュール構成**

否の情報を管理している．CPROXY を実装するにあたり，ACL に対して URL とグループ番号を対応付けて管理できるように改造を施した．また，送信元ポート番号とグループ番号を対応付けて管理するために，Squid メインモジュールに，PGL（Port Group List）と呼ぶテーブルを実装した．

CPROXY モジュールは，GSRA デーモンからのパケットを受信するため，RAW ソケットにより，CPROXY リクエストを受信できるように実装を行った．また，受信した送信元ポート番号やグループ番号の情報を Squid メインモジュール中の PGL に通知する機能を実装した．

# 第6章　動作検証と性能評価

図 6.1 の環境において，動作検証と性能測定を行った．ここで，Dummynet はネットワークに遅延や帯域制限，パケットロスなどを発生させるためのソフトウェアである．今回の測定では，スループット測定時に，ローカル環境での測定と，Dummynet による擬似的なインターネット環境での測定を行った．表 6.1 に性能評価に利用した各装置の仕様を示す．表 6.2 に Dummynet の設定を示す．帯域幅は 40Mbps に設定した．遅延は，両方向の通信についてそれぞれ 10ms ずつ設定した．パケットロス率は 0 に設定した．

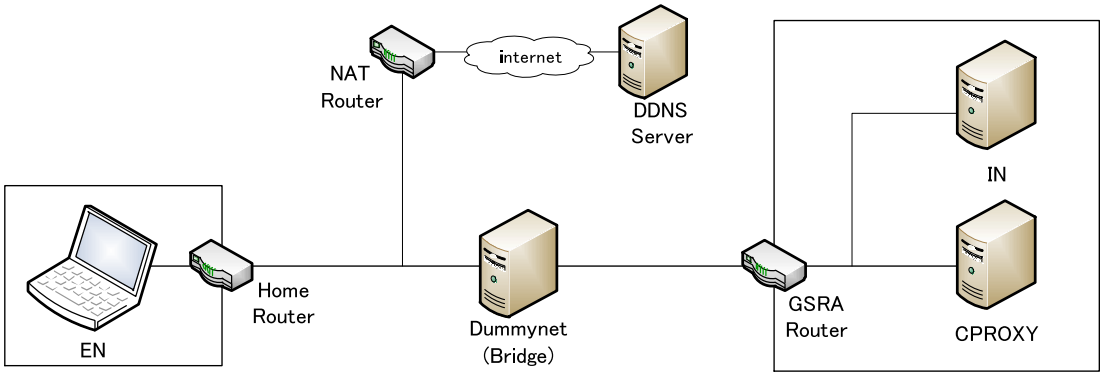


**図 6.1　性能測定環境**

**表 6.1　性能測定環境における各装置の仕様**

| Name | OS / Product | CPU | Memory | NIC |
|---|---|---|---|---|
| EN | 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 |
| IN | FreeBSD 7.2 | Pentium4 2.8GHz | 1024MB | 100Base-TX |

**表 6.2　Dummynet の設定**

| | |
|---|---|
| bandwidth | 40Mbps |
| delay | 20ms (10ms+10ms) |
| packet loss rate | 0 |

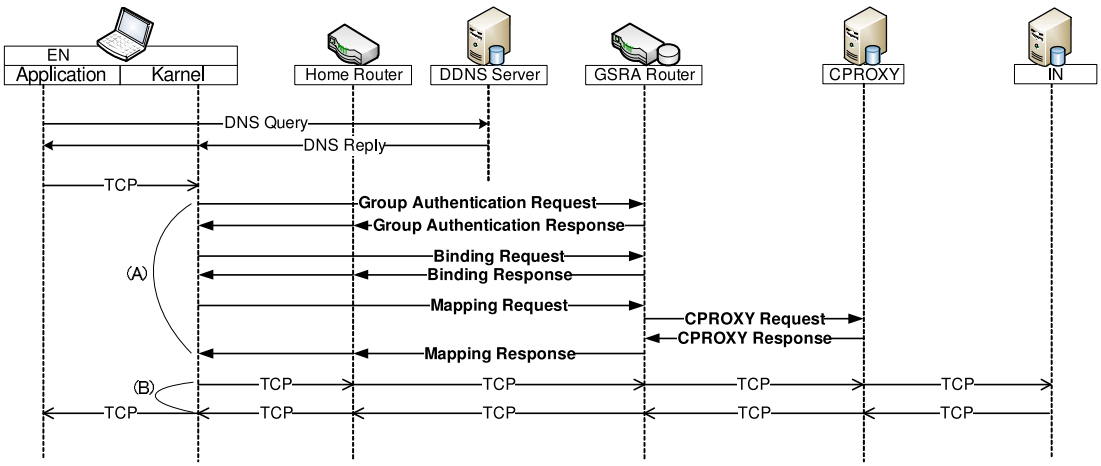


**図 6.2　性能測定箇所**

## 6.1　動作検証

EN から IN に対して HTTP 通信を行った結果，GSRA ルータと CPROXY を経由してアクセスが行われていることを確認した．また，EN が所属するグループの情報を変更し，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．また，EN が所属するグループを複数設定した場合においても，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．また，提案方式の動作と GSRA 単独の動作を併用できることを確認した．以上の結果，正しく実装が行われていることが確認できた．

## 6.2　性能評価

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 において，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．すなわち，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．

通信時間の測定はネットワークアナライザ Wireshark を用いて測定した．HTTP クライアントには，wget 1.11.4 を使用した．HTTP サーバには，Apache 2.2.11 を使用した．CPROXY には，Squid 3.1.4 を改造したものを使用した．なお，CPROXY には HDD にキャッシュが保存されないように設定を施すことで，毎回の測定の際に CPROXY が IN にアクセスするようにした．通信時間の測定は 10 回ずつ実施し，平均を求めた．スループットは 5 回ずつ測定し，平均を求めた．

### 6.2.1　通信時間

測定時のシーケンスを図 6.2 に示す．なお，取得対象のコンテンツは 0Byte のファイルである．また，Dummynet の設定は無効にし，通常のブリッジとして動作するように設

表 6.3　通信時間

| | 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 6.4　スループット（Dummynet 無効）

| | GSRA | 提案方式 |
|---|---|---|
| 平文通信 | 71.3Mbps | 35.8Mbps |
| 暗号通信 | 68.3Mbps | 33.2Mbps |

表 6.5　スループット（Dummynet による制限あり）

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

定した．また，EN と GSRA ルータ間で暗号通信を行う場合について性能測定を行った．

測定結果を表 6.3 に示す．ネゴシエーション時間として，グループ認証要求からマッピング応答までの時間（図 6.2 の括弧 A の部分）を測定した．コンテンツ取得時間として，HTTP 通信の開始から終了までの時間（図 6.2 の括弧 B の部分）を測定した．ネゴシエーションについて，GSRA に対する提案方式の遅延差分を求めたところ，CPROXY ネゴシエーションは 0.19ms の通信時間であることが分かった．HTTP 通信が CPROXY を経由することで，0.63ms の遅延があることが分かった．

### 6.2.2　スループット

提案方式と GSRA のスループットをそれぞれ測定した．Dummynet を有効にして疑似的なインターネットを想定した場合と Dummynet を無効にした場合を測定した．測定結果を表 6.4 と表 6.5 に示す．提案方式では，CPROXY を経由する通信となるため，GSRA に比べてスループットが低下することが分かる．しかし，実際のインターネット環境を想定した場合，GSRA と提案方式ではそれほどの差は見られない．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，提案方式は殆ど性能劣化を感じることはない．

# 第7章　まとめ

本論文では，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．そこで，アプリケーションの内容を制御する部分は CPROXY に任せる方式を取った．

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．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，提案方式は十分に有用であることが分かった．

# 謝辞

本研究を遂行するにあたり，多大なるご指導，ご鞭撻を賜りました，名城大学大学院理工学研究科 渡邊晃教授に心より厚く御礼申し上げます．また，本論文をまとめるにあたり，有益な御助言をして頂きました，名城大学大学院理工学研究科 柳田康幸教授，宇佐見庄五准教授に心より厚く御礼申し上げます．そして日々の研究活動に対して様々な御指導を頂きました名城大学理工学部情報工学科の鈴木秀和助教に心より感謝致します．

本研究を遂行するにあたり，有益なご助言，適切なご検討をいただいた，渡邊研究室の皆様に心より感謝いたします．

## 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] A.Valencia, M.Littlewood and T.Kola: Cisco Layer Two Forwarding (Protocol) ”L2F”, RFC 2341, IETF (1998).

[6] 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).

[7] 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).

[8] C.Kaufman, P.Hoffman, Y.Nir and P.Eronen: Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, IETF (2010).

[9] S.Kent: IP Encapsulating Security Payload (ESP), RFC 4303, IETF (2005).

[10] A.Huttunen, B.Swander, V.Volpe, L.DiBurro and M.Stenberg: UDP Encapsulation of IPsec ESP Packets, RFC 3948, IETF (2005).

[11] OpenVPN: http://openvpn.net/.

[12] W.Simpson: The Point-to-Point Protocol (PPP), RFC 1661, IETF (1994).

[13] D.Farinacci, T.Li, S.Hanks, D.Meyer and P.Traina: Generic Routing Encapsulation (GRE), RFC 2784, IETF (2000).

[14] G.Pall and G.Zorn: Microsoft Point-To-Point Encryption (MPPE) Protocol, RFC 3078, IETF (2001).

[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] Perl: http://www.perl.org/.

[18] PHP（PHP: HypertextPreprocessor）：http://www.php.net/.

[19] JSP（JavaServerPages）：http://java.sun.com/products/jsp/.

[20] Squid: http://www.squid-cache.org/.

# 研究業績

## 学術論文

なし

## 研究会・大会等

1. 三浦健吉, 鈴木健太, 鈴木秀和, 渡邊晃 “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,” 情報処理学会研究報告，2010-DPS-145，pp.1–8，Nov.2010.

2. 三浦健吉, 鈴木秀和, 渡邊晃 “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,” 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.1678–1682，Jul.2010.

3. 三浦健吉, 鈴木秀和, 渡邊晃 “NAT-f を利用した SIP の NAT 越え通信方式の提案,” マルチメディア，分散，協調とモバイル（DICOMO2009）シンポジウム論文集，Vol.2009，No.1，pp.1572-1577，Jul.2009.

## 国内会議

1. 三浦健吉, 鈴木秀和, 渡邊晃 “NAT-f を利用した SIP の NAT 越え通信の提案,” 情報処理学会第 71 回全国大会講演論文集，Mar.2009.

2. 三浦健吉, 鈴木秀和, 渡邊晃 “NAT-f を利用した SIP の NAT 越え通信の検討,” 平成 20 年度電気関係学会東海支部連合大会論文集，Sep.2008.

# 付 録A　記号の定義

- $G_i$　グローバル IP アドレス
- $P_i$　プライベート IP アドレス
- $V_i$　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）
- Group*x*　通信グループ番号
- GK*x*　通信グループ Group*x* に対応するグループ鍵
- 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