Vol.2012-CSEC-57 No.9
Vol.2012-IOT17 No.9
2012/5/10

認証をアウトソースするネットワークスイッチの機能設計

櫻井 孝一[1]　佐藤 聡[2]　吉田 健一[3]　新城 靖[4]

概要：パブリックスペースでは、持ち込み PC の利用者を認証し、利用者に許可されているネットワークに接続させることが一般的となっている。この利用者認証は多くの場合、ネットワークスイッチが行っており、802.1X 認証や、Web のフォーム認証などが用いられている。最近では、利用者の利便性の向上や、セキュリティレベルの向上のために、ざまざまな新しい利用者認証の仕組みが提案されている。本研究では、ネットワークスイッチがこれらの新しい仕組みに柔軟に対応できるようにするために、利用者認証の仕組みを外部サーバにアウトソース可能となるための機能設計を提案する。

キーワード：利用者認証、ネットワークスイッチ、アウトソース

The design of network switches that outsource user authentication

Koichi Sakurai[1]　Akira Sato[2]　Kenichi Yoshida[3]　Yasushi Shinjo[4]

Abstract: In a public space, network switches authenticate guest users, and control the connection between PCs of the guest users and the allowed network segments. Such a switch often perform user authentication based on are used 802.1x and Web forms. Today, in order to improve user convenience and security level, many new methods of user authentication are developed. In this paper, we propose a functional design of network switches which allows network switchis to outsource user authentication to external servers to new mechanisms.

Keywords: User authentication, Network swiches, outsourcing

1. はじめに

近年、パブリックスペースを持つ大学等の組織においては、そのスペースの利用者自身が持ち込んだ PC のためのネットワーク環境を整備するのが一般的になっている。このようなスペースでのネットワーク利用では、利用資格がないものが無許可に接続できない様にするため、また、インシデント発生時にネットワークの利用者を特定するために、持ちこまれる PC に対して利用者を認証し、利用者に許可されているネットワークに対する接続の制御を行うことが一般的になっている。利用者認証およびネットワーク接続制御の処理は、多くの場合、それら持ち込み PC が接続されるネットワークスイッチや無線 LAN ルータが行っている。

利用者認証については、現在、802.1X 認証 [1] や Web のフォームによる認証などが用いられている。これらの認証の仕組みについては、ネットワークスイッチにあらかじめハードウェアの一部として実装されている。従って、その柔軟性は高いとは言えない。

近年は、セキュリティ保護の観点から、必要以上にパスワードの入力をさせない為に、Web アプリケーションにおいてはシングルサインオンが採用されている。また、国内の大学等の組織では、「学術認証フェデレーション」により、認証連携の実現が行われている。一般においても、OAuth といったオープンに認可情報を委譲できる仕様が策

[1] 筑波大学 システム情報工学研究科コンピュータサイエンス専攻
Master's Program in Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba
[2] 筑波大学 学術情報メディアセンター
Academic Computing and Communications Center, University of Tsukuba
[3] 筑波大学 ビジネスサイエンス系
Faculty of Business Sciences, University of Tsukuba
[4] 筑波大学 システム情報系情報工学域
Division of Information Engineering, Faculty of Engineering, Information and Systems, University of Tsukuba

ⓒ2012 Information Processing Society of Japan

定されている。新しい認証や認可の仕組みを利用して、利用者にとってより利便性の高い方式や、よりセキュリティレベルが高い方式による利用者認証を行う研究も盛んに行われている。しかし、ネットワークスイッチでは利用者認証をハードウェアとして実装しているため、新しい仕組みに柔軟に対応していくことは難しい。

本研究では、持ち込み PC の利用者の認証の仕組みを外部にアウトソースできるようにするためのネットワークスイッチの機能設計を提案する。

2. 関連研究

2.1 HINET2007

広島大学では、2008 年度から運用している HINET2007 において全学的規模でネットワークの利用者認証を行っている [2]。これはネットワークスイッチが有する Web によるフォーム認証により実装を行っている。広島大学では、訪問者の利用者認証に Shibboleth 認証 [3] を利用する方法について研究を行っている [4]。各組織の IdP(Identity Provider) による認証が利用するためには、利用者認証を行うネットワークスイッチ内に実装されている Web サーバが SP(Service Provider) となればよい。しかし、ネットワークスイッチ内の Web サーバは改修することが難しいため、外部の SP にてネットワークスイッチが参照している LDAP サーバに一時的なアカウントを発行し、RADIUS 経由でそのデータを参照することにより、訪問者の利用者認証を実現している。従って、文献 [4] による研究は、本研究と同様に新たな認証の仕組みへ対応と考えることができる。本研究では、様々な認証の仕組みへの対応可能となるようにスイッチに対して API を定義している点で異なっている。

2.2 Opengate

佐賀大学では、キャンパス全域にある情報コンセントに接続される多数の端末に対して適用可能な利用者認証のためのゲートウェイシステムとして Opengete を開発し運用を行っている [5]。このシステムはソフトウェアとして実装されている。また、佐賀大学では、利用者認証の共通化を行っており、大学ポータルの認証とネットワーク認証を統合できるように、Opengate の拡張を行っている [6]。佐賀大学で大学ポータルの認証は、他の情報システムとのシングルサインオンを実現するために、Shibboleth 認証 [3] を利用している。従って、文献 [6] による研究は、本研究と同様に新たな認証の仕組みへの対応と考えることができる。本研究では、様々な認証の仕組みへの対応可能となるように API を定義している点で異なっている。

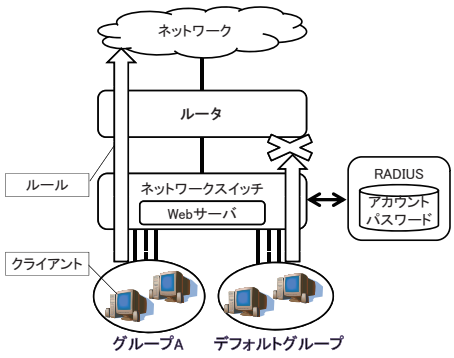

図 1 ネットワークスイッチにおける利用者認証
Fig. 1 user authentication of newtwork swiches

2.3 ケーパビリティを用いた外向きネットワークアクセス制御

我々は、ケーパビリティを利用したネットワークアクセス制御システムとして CaNector[7] を開発した。通常外部からの訪問者は訪問先のネットワークを利用するためのアカウントを管理者から発行してもらう。この発行には多くの手続きや時間が掛かる。この手法はネットワークアクセスに関する権限を持っている利用者が管理者の変わりにネットワーク利用の権利を訪問者に与えるという方法であり、ケーパビリティを利用する。ケーパビリティに基づくアクセス制御方法は、利用者認証とは異なる方式である。しかし、API を持たないため、他の方式に適用できず拡張性がない。

3. ネットワークスイッチにおける利用者認証とその問題点

既存のネットワークスイッチにおける利用者認証とは、そのスイッチに接続してきたネットワーク機器の利用者を認証し、そのネットワーク機器を利用者に対して利用が認められているネットワークへ接続させることをいう。本論文では、接続されるネットワーク機器のことをクライアントと呼ぶことにする。また、所属させるネットワークのことをグループと呼び、グループの中でも特に利用者認証が行われていないクライアントが所属するグループのことをデフォルトグループと呼ぶことにする。それぞれのグループにはネットワークに関するアクセスのルールが設定されている。これらの概念を図にしたものを**図 1** に示す。

既存のネットワークスイッチは、(1) クライアントの利用者を認証し、どのグループに所属させるかを決定すること、(2) 入力パケットごとにどのグループのパケットであるかを識別し、そのグループのルールを適用すること、の 2 つの作業を全て行っている。

例えば、ネットワークスイッチが 802.1X 認証を支援している場合を考える。デフォルトグループでは EAPOL パ

ⓒ2012 Information Processing Society of Japan

ケットや EAP パケットしか受け取らないようなルールが設定されており、利用者認証が成功した際に所属するグループでは任意のパケットを受け取るようなルールが設定されているととらえることができる。また、利用者ごとにクライアントが所属する VLAN を切り替えることは、クライアントが所属するグループを利用者ごとに切り替えているととらえることができる。

また、ネットワークスイッチが Web によるフォーム認証を支援している場合を考える。デフォルトグループではスイッチ上に設置されている Web サーバへのパケットのみを受け取るようなルールが設定が設定されており、利用者認証が成功した際に所属するグループでは、どのようなパケットでも受け取るルールが設定されているととらえることができる。

利用者認証に用いられるアカウント名とパスワードの組は、ネットワークスイッチ自身が記憶しているものを使ったり、外部にある情報を使うことも可能である。外部にある情報にアクセスするには、一般的には RADIUS プロトコルが使われている。アカウント名とパスワードの組の記憶方法にはさまざまな方法があり、LDAP を用いて管理する方法や、リレーショナルデータベースにより管理する方法がある。RADIUS プロトコルを解釈するゲートウェイのようなものを経由することにより、様々な記憶方法を採用することが可能となっている。この点においては、ネットワークスイッチは柔軟な対応が可能であるといえる。

しかしながら、認証の仕組みの実装はネットワークスイッチのハードウェアとして実装されているため、新たな認証の仕組みには柔軟には対応できない。例えば、組織において認証情報が統一化されている現状では、複数のサイトに統一化されたアカウントやパスワードを入力するようになってしまうと、セキュリティレベルが下がってしまうため、Web アプリケーションではシングルサインオンを行うことが一般的になってきている。ネットワークスイッチの Web フォームによる認証も、一種の Web アプリケーションであるため、シングルサインオン化するべきであるが、その対応を行うことは難しい。

4. 認証をアウトソースすることによる解決方法

本論文では、新たな認証の仕組みに対してネットワークスイッチが柔軟に対応するために、ネットワークスイッチから認証をアウトソースすることによる解決方法を提案する。提案手法の概要を**図 2** に示す。

ネットワークスイッチにおける利用者認証において、既存のネットワークスイッチが行っていた (1) クライアントの利用者を認証しどのグループに所属させるかを決定することを、外部サーバが行うようにする。ネットワークスイッチは、外部サーバでの結果の情報を受けて (2) 入力パケットごとにどのグループのパケットであるかを識別し、そのグループのルールを適用することだけを行う。

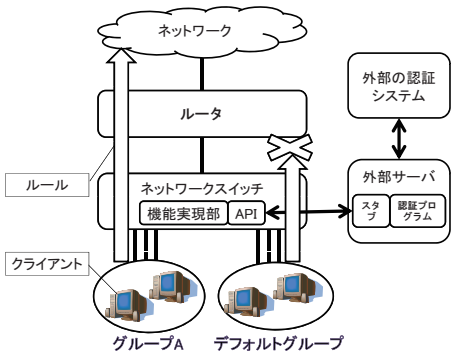

図 2 提案する方式の概要
Fig. 2 overview of our proposed method

(1) の部分を外部サーバが行うため、新たな認証の仕組みは外部サーバ上で動作する認証プログラムとして動作させることが可能である。従って柔軟に対応することができる。

本論文では、利用者認証をアウトソースするためにネットワークスイッチに求められる機能の提案を行う。また、それらの機能を使うための API についての提案を行う。

従って subsection ネットワークスイッチに求められる機能認証をアウトソースするためにネットワークスイッチに求められる要件は以下の通りである。

(1) 参加通知機能
外部サーバがネットワークスイッチに対して、認証されたクライアント情報、および、そのクライアントが所属するグループ情報の組の通知が行える必要がある。

(2) 離脱通知機能
外部サーバがネットワークスイッチに対して、利用を終了したクライアント情報の通知が行える必要がある。

(3) 離脱監視機能
離脱処理を行わなずに、離脱したクライアントの情報を保持し続けることは、セキュリティの観点から好ましくない。このような離脱処理をし忘れたクライアントについてネットワークスイッチ自身による検知が行える必要がある。検知できたクライアントの情報については、機能 (2) を満たす機能を用いて削除することが可能である。従って、この機能を呼び出して、離脱処理のし忘れが検知されたクライアントを削除する機能を呼び出すといったことを定期的に実行する機能が必要となる。

(4) 一覧取得機能
管理者がネットワークスイッチが管理しているグループ毎に現在利用しているクライアントの一覧が取得できる機能が必要となる。現在利用ているクライアント

ⓒ2012 Information Processing Society of Japan

の一覧はネットワークスイッチ自身が管理する。

(5) デフォルトグループの設定機能
クライアントがネットワークスイッチに初めて接続されたときには、利用者認証が行われていない。このように利用者認証が行われていないクライアントや、認証処理に失敗したクライアントを所属させるグループをどのグループに所属させるかを管理者が設定する機能が必要となる。

(6) グループごとのルール設定機能
管理者がグループごとのアクセスに関するルールを設定する機能が必要となる。一般的には、前述のデフォルトグループでは、外部サーバへのアクセスのみが許可され、その他は拒否されるような設定が行われる。また、その他のグループでは、それ以外のサーバ等へのアクセスも許可されるような設定が行わ

4.1 API の提案

前述の機能を利用するための API を提案する。API は外部サーバから利用される API と管理者が使う API から構成される。

外部サーバ用の API は外部サーバから利用されるために、RPC(Remote Procedure Call) により呼び出される。管理者用 API は管理者が利用するため、その実装についてはコマンドラインインタフェースによる実装等が考えられる。

なお、機能 (3) については、ネットワークスイッチ自身により実行される機能であるため、API は持たない。

4.1.1 外部サーバ用 API

4.1.1.1 allow(client,gid)

認証に成功したクライアントの情報とそのクライアントが所属するグループの情報を外部サーバからネットワークスイッチに通知する際に利用する。この API は機能 (1) を呼び出すための API である。引数は、認証に成功したクライアント情報 `client` と、そのクライアントが所属するグループ情報 `gid` である。

ネットワークスイッチは、`client` にて指定されたクライアントに関して送受信されるパケットに対して、この API が呼び出された以後は、`gid` にて指定されたグループに設定されたアクセスに関するルールを適用する。

4.1.1.2 release(client)

利用を中止したクライアントの情報を、外部のサーバからネットワークスイッチに通知する際に利用する。この API は機能 (2) を呼び出すための API である。引数は、利用を中止したクライアント情報 `client` である。

ネットワークスイッチは、`client` にて指定されたクライアントに関して送受信されるパケットに対して、この API が呼び出されてた以後は、デフォルトグループに設定されたアクセスに関するルールを適用する。

4.1.2 管理者用 API

4.1.2.1 list(client)

管理者がグループ毎に現在利用しているクライアントの一覧を取得する際に利用する。この API は機能 (4) を呼び出す API である。引数は、利用を中止したクライアント情報 `client` である。

ネットワークスイッチは、`client` にて指定されたグループに現在所属しているクライアントの一覧を返す。

4.1.2.2 set default group(gid)

管理者が認証処理を行っていないクライアントが所属すべきグループを指定する際に利用する。この API は機能 (5) を呼び出す API である。引数は、デフォルトグループ情報 `gid` である。

4.1.3 set group rule(gid,rules)

管理者がグループごとのアクセス制限を設定する際に利用する。この API は機能 (6) を呼び出す API である。引数は、デフォルトグループ情報 `gid` と、アクセスに関するルール群 `rules` である。

5. 実装方式

提案する機能が有効であることを確かめるために、機能の実装を行った。ネットワークスイッチのハードウエアを実装することはコストがかかるため、以下に示す方針に従って実装を行った。

(1) 外部サーバ用の API は RPC にて利用されることに着目し、そのスタブとなる部分のプログラムを拡張する。
(2) スタブは既存のネットワークスイッチに Telnet で接続しその機能を利用する。

クライアントの特定には、IP アドレスを用いた。また、本実装方式では、クライアントのグループへの所属と、グループごとのルールの適用を別々のネットワークスイッチを用いて実装する方式を取った。この方式では、ネットワーク構築で一般的に用いられる 3 層構造に適用しやすい方法である。アクセス層にてグループ所属処理を行わせ、ディストリビューション層にてルール適用処理を行わせる。

アクセス層のスイッチとて、Alaxala 社製 AX1240S を、ディストリビューション層のスイッチとして、Alaxala 社製　AX620R-2105 を対象として実装を行った。

既存のネットワークスイッチの機能として、QoS 技術と DHCP snooping の技術を用いた。QoS 技術はクライアントをグループに振り分ける処理に適用し、DHCP snooping 技術はクライアントの離脱監視に用いた。

持ち込み PC の IP アドレスの管理には DHCP を用いることが一般的であるため、利用者認証を行うネットワークスイッチでは、この DHCP snooping の機能を活用していることが一般的であり [8]、この機能を実装に応用しやすい。

ⓒ2012 Information Processing Society of Japan

5.1 QoS 技術の適用

QoS 技術はアプリケーションが提供しているサービスのタイプによってパケットの送信順序やパケットの送信ポートなどを設定することができる技術である。この QoS 技術には Diffserv と Intserv と呼ばれる方式が存在する。本研究では Diffserv 方式 [9] を用いる。Diffserv 方式ではスイッチにパケットが到達するとパケットの IP ヘッダの DSCP(Differentiated Services Code Point) 値を確認してスイッチに定められているルールに従ってパケットを処理する。本研究ではクライアントから送られてくるパケットの DSCP 値をグループ情報として用いる。

従って、`allow` は、引数 `client` にて指定された IP アドレスからのパケットに対して、引数 `gid` にて指定されて DSCP 値を設定するような設定をネットワークスイッチに投入する処理として実装する。

また、`set default group` は、この実装では、DSCP 値のデフォルト値となるように実装した。さらに、`release` は、引数 `client` にて指定された IP アドレスを対象とした DSCP 値の設定をやめるような設定をネットワークスイッチに投入する処理として実装する。また、`list` は、引数 `gid` にて指定された DSCP 値を設定する IP アドレスのリストを返す処理として実装する。`set group rule` は、ディストリビューション層におけるネットワークスイッチにおいて、DSCP 値をみてパケットの宛先を変更する、PBR(Policy Based Routing) の機能を用いて実装する。

5.2 DHCP Snooping 技術の適用

DHCP Snooping は DHCP[10] サーバがネットワーク上の機器に IP アドレスを配布するやりとりを監視するネットワークスイッチの機能である。ネットワークスイッチにて DHCP Snooping を有効にするとネットワークスイッチ内にバインディングデータベースが作成される。作成されたバインディングデータベースには DHCP Snooping により取得した情報を格納する。

DHCP サーバは配布する IP アドレスにリース期限を設定する。リース期限を越えた IP アドレスは利用できなくなる。ネットワークスイッチはバインディンデータベースに IP アドレスとリース期限の組を登録している。リース期限を越えた IP アドレスを見つけると、ネットワークスイッチはバインディングデータベースからその IP アドレスの情報を消去する。クライアントがネットワーク利用を続けている場合は、リース期限を越えた時に再度利用要求をだす。このため、バインディングデータベースに情報が残り続けることとなる。

本実装では、利用されなくなったクライアントの検知に、この機能を応用する。`list` により取得したクライアントの一覧と、バインディングデータベースの一覧との比較を行い、クライアント一覧にあってバインディングデータベースにない IP アドレスは利用されなくなったものとして、`release` を用いてクライアント情報を削除する。この機能は、ネットワークスイッチ内に実装されるべきであるが、ネットワークスイッチ内で定期的に呼び出されるようなプログラムを組み込むことは難しいため、本実装では、外部サーバにてプログラムとして実装する。

6. 機能の評価実験

ここでは、認証方式を自由に選択できることを確認するために Facebook アプリケーション [11] を用いた認証が実装できるかを確認した。

Facebook では第三者が開発した Facebook のアプリケーション (以下 Facebook APPS) に対して Facebook が管理している利用者の情報を提供している。Facebook APPS では Facebook 利用者の情報を利用したい場合、利用する項目に対しての閲覧、編集などを行う権限を利用者から得る必要がある。そのため、利用者が Facebook APPS を初めて利用する場合に Facebook は利用者に Facebook APPS が取得希望する権限を与えるか否かを質問する。権限を与えない場合には Facebook APPS を利用することはできない。

Facebook APPS は Facebook にログインしないと利用できない。そのため、ログインしていない場合は Facebook が認証を要求するページに移動する。Facebook にて認証処理が完了すると Facebook APPS のページにリダイレクトされる。

この仕組みを利用して、Facebook APPS のページに利用者がアクセスしたときに、そのアクセス元の IP アドレスをクライアントの情報の引数に使い参加通知機能を呼び出す API である `allow` を呼び出すことにより利用者認証を実現する。

この実験では、グループは一つだけとした。デフォルトグループでは、Facebook サイトと、Facebook APPS のページのサイトのみアクセスが可能となるルールを設定した。また、認証後に所属させるグループでは、上記以外のサイトにもアクセスできるようなルールを設定した。

今回作成した Facebook アプリケーションのプログラムの抜粋を**図 3** に示す。このプログラムにおいて認証として利用するため追加した部分は 13 行目のコードだけであった。これにより簡単に Facebook アプリケーションをネットワーク認証として利用できることが確認できた。

7. おわりに

本論文では新しい認証の仕組みに柔軟に対応可能とするために、利用者認証をアウトソースするためにネットワークスイッチに求められる機能設計を行い、その機能を利用するための API を提案した。また、提案した機能の有用性を示すために、API を利用する際に用いるスタブのプログ

ⓒ2012 Information Processing Society of Japan

```
1  public class fbserv extends HttpServlet {
2
3  .....
4
5    public void doGet (HttpServletRequest req,HttpServletResponse res)
6    throws ServletException, IOException{
7      String auth ="....." ; /*access token address*/
8
9      req.getSession().setAttribute("code",req.getParameter("code"));
10     String at = getAccesstoken(auth);
11     try
12       if(getAccesstoken(auth) == null){
13         if(NetworkSwitch(HOST).allow(req.getRemoteAddr(),GID)== 0){
14           req.getSession().setAttribute("access_token", at);
15           res.sendRedirect("/auth/fbcomplete.jsp");
16         }else{
17           res.sendRedirect("/auth/error.jsp");
18         }
19       }else{
20         res.sendRedirect("/auth/error.jsp");
21       }
22     }catch (InterruptedException e) {
23       e.printStackTrace();
24     }
25   }
26 }
```

図 3 実装した Facebook アプリケーションのプログラム（抜粋）
Fig. 3 a part of implemented Facebook application program

ラムを拡張し、現在ネットワークスイッチが有している機能を用いて、提案する機能の実装を行った。さらに、それらの API を使って、Facebook アプリケーションとして外部サーバを構築し、利用者認証のアウトソースが実現できることを示した。

本研究の今後の課題としてはネットワーク認証のアウトソースの性能実験や MAC アドレスを利用した場合のネットワーク認証のアウトソースについて考える。

参考文献

[1] IEEE Standard 802.1X-2004: *Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control*, IEEE Computer Society (2004-12-13).
[2] 大東俊博，近堂　徹，岸場清悟，田島浩一，岩田則和，西村浩二，相原玲二：広島大学における新キャンパスネットワークへの移行手法，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol. 2008, No. 87, pp. 31–36 (2008-09-12).
[3] Marlena Erdos and Scott Cantor: Shibboleth Architecture v4, `http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v04.pdf` (Accessed 2010 Apr 10) (2001-11-21).
[4] 藤村喬寿，田島浩一，大東俊博，西村浩二，相原玲二：学術認証フェデレーションに基づくキャンパスネットワークの認証機構，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol. 2010, No. 37, pp. 1–6 (2010-02-22).
[5] 渡辺義明，渡辺健次，江藤博文，只木進一：利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発 (<特集>次世代のインターネット/分散システムの構築・運用技術)，情報処理学会論文誌， Vol. 42, No. 12, pp. 2802–2809 (2001-12-15).
[6] 大谷　誠，江藤博文，渡辺健次，只木進一，渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発，情報処理学会論文誌， Vol. 51, No. 3, pp. 1031–1039 (2010-03-15).
[7] 馬渕充啓，高田真吾，小沢健史，豊岡　拓，松井慧悟，佐藤　聡，新城　靖，加藤和彦：利用者間で接続権限を受け渡し可能なネットワーク制御機構の実現，情報処理学会論文誌， Vol. 51, No. 3, pp. 974–988 (2010-03-15).
[8] 柘植宗俊，中村　亮，坂本健一，加沢　徹，芦　賢浩：光アクセスシステム向けレイヤ 2 アクセスセキュリティ機能の一検討 (Ethernet 関連技術, エミュレーション技術, 一般)，電子情報通信学会技術研究報告. CS, 通信方式, Vol. 105, No. 512, pp. 7–12 (2006-01-09).
[9] Nichols, K., Blake, S., Baker, F. and Black, D.: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, RFC 2474 (Proposed Standard) (1998).
[10] Droms, R.: Dynamic Host Configuration Protocol, RFC 2131 (Draft Standard) (1997).
[11] facebook developers: Authentication, `https://developers.facebook.com/docs/authentication/ (Accessed 2011 Nov 23)`,.

ⓒ2012 Information Processing Society of Japan