情報処理学会論文誌 Vol.54 No.3 1099–1108 (Mar. 2013)

高度な利用者認証が利用可能なネットワークを対象とした柔軟なアクセス制御の一実装

佐藤 聡[1,a)] 櫻井 孝一[2] 吉田 健一[3] 新城 靖[4]

受付日 2012年6月29日, 採録日 2012年12月7日

概要：現在では，認証方法は，ますます高度になってきている．ネットワークに対するアクセス制御でも，Shibboleth や OAuth といったように分散的に管理されている認証情報を利用したいという要望がある．その目的は，認証情報に基づいて分けられたグループごとに異なるアクセス権を与えることである．本論文では，高度な信頼できる利用者認証が利用可能なネットワークを対象とした柔軟なアクセス制御の一実装について述べる．この実装では，外部の認証サーバにより認証を受けた持ち込み PC のパケットに対してアクセス権に対応する QoS のマーキングを行い，上位のルータがそのマーキング値によりアクセス制御を行う点に特徴がある．これにより，ネットワーク構成に対する制約がないシステム構成とすることが可能である．アクセス制御を行うための設定は持ち込み PC の接続前に設定したものを利用し続けるという特徴もある．本論文では高度な利用者認証の例として，Facebook の利用者認証を用いる方法を示す．Facebook 上の特定のグループに所属している人，単に Facebook アカウントを有する人とに分けて，ネットワーク接続環境を提供するための Facebook アプリケーションを作成する．これにより，本論文で述べる実装の有用性を示す．

キーワード：利用者認証，ネットワーク，アクセス制限

An Implementation of Flexible Access Control for Networks with Advanced User Authentication

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

Received: June 29, 2012, Accepted: December 7, 2012

Abstract: Today, user authentication methods have become increasingly advanced. In access control for networks, there is a need to use user authentication information which is managed in a distributed manner such as Shibboleth and OAuth. Its purpose is to give different access rights for each group was divided based on user authentication information. In this paper, we describe an implementation of flexible access control for networks with advanced and trusted user authentication. A characteristic of this implementation is to make a network switch to mark the QoS value which is associated to an access right on an IP packet and to make routers to enforce an access right using the QoS value on an IP packet. In this implementation, there are no constraints on the network system configuration and setting to enforce an access right is static. In this paper, we describe an example of using advanced user authentication on Facebook. This example is a Facebook application, and divides people which into several groups based on Facebook user information. Each group has its access right for the network. We clarify the effectiveness of this implementation by this example.

Keywords: user authentication, network, access control

1. はじめに

大学や公共機関では，利用者が持ち込む PC をそれらが管理するネットワークに接続させたいという要望がある．

[1] 筑波大学学術情報メディアセンター
Academic Computing and Communications Center, University of Tsukuba, Tsukuba, Ibaraki 305–8577, Japan
[2] 筑波大学大学院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, Tsukuba, Ibaraki 305–8573, Japan
[3] 筑波大学ビジネスサイエンス系
Faculty of Business Sciences, University of Tsukuba, Bunkyo, Tokyo 112–0012, Japan
[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, Tsukuba, Ibaraki 305–8573, Japan
[a)] akira@cc.tsukuba.ac.jp

持ち込み PC にネットワークを使わせるときには認証は必須となっている．現在では，認証方法は，ますます高度になってきており，Shibboleth や OAuth といったように分散的に管理されている認証情報をネットワークに対するアクセス制御でも利用したいという要望がある．その目的は，認証情報に基づいてグループ分けを行い，それぞれのグループごとに異なるアクセス権を与えることである．たとえば，まったく認証を受けていない人は，組織の情報提供 Web サイトのみアクセスでき，認証された人は外部の Web サイトへアクセスでき，特別な構成員であれば，SSH サーバへのアクセスを許すという要望である．

このようにグループごとに異なるアクセス権を与える方法として，いくつかの方法が提案されている．しかしながら，これらの方法には，以下に示すような管理上の問題がある．詳しくは 2 章で述べる．

- 認証の前後に持ち込み PC に割り当てられる IP アドレスが変化することがある．このため，利用者としては，持ち込み PC の OS やブラウザに制限を受けたり，認証前に起動したアプリケーションを認証後に再起動する必要があったりする等の不便さが生じる．また，管理者としてもインシデントの発生時に利用者を特定する際に必要となる情報が複雑になる．
- ネットワーク構成に制約が発生するため，情報提供サーバや外部の認証サーバを柔軟に利用することが困難となる．
- 持ち込み PC が接続されるたびに多くの機器でアクセス制御の設定を変更する必要がある．

本論文では，これらの問題を解決するようなネットワークに対するアクセス制御の実装について述べる．この実装の特徴は，ネットワーク構成に制限がないため，Facebook 等の外部の認証サーバや，すでに存在する組織の情報提供を行う Web サーバを利用できる点にある．また，認証の前後で持ち込み PC に割り当てられる IP アドレスが変更されることがないため，利用者の環境が制限を受けることがない．また，管理側もネットワーク構成を簡素化し，管理コストを低減させることが可能である．本論文で述べる実装は，持ち込み PC からの IP パケットに対して末端のスイッチが有する QoS 機能を活用してマーキングを行い，分散して配置されたルータでマーキングに基づいてアクセス制御を行う．アクセス制御の設定は，分散して配置されたルータに静的に保存することができる．アクセス制御を行う箇所はネットワーク上のどこでも可能となり，ネットワーク構成に関する制限がないといえる．

本論文では高度な利用者認証の例として，Facebook の利用者認証を用いる方法を示す．Facebook 上の特定のグループに所属している人，単に Facebook アカウントを有する人とに分けて，ネットワーク接続環境を提供するための Facebook アプリケーションを作成する．これにより，本論文で述べる実装に有用性があることを示す．

2. 既存のネットワーク認証システムの問題点

大学や公共機関のネットワーク環境へのアクセスサービスを提供する際には，持ち込まれた PC の利用者を特定し，その利用者に許可されたネットワークを利用させるために利用者認証が必要となる．特に，管理している組織の構成員以外の利用者にもサービス提供する際には，ネットワーク管理者の負担を軽減するために，分散的に管理されている認証情報を利用する試みがなされている．

現在，日本の大学と国立情報学研究所が連携し，認証連携を実現するために「学術認証フェデレーション（学認）」の運用を行っている．これは Shibboleth を用いて実現されている．この方法では，各大学等が認証情報を分散的に管理している．

一方，ソーシャルネットワークシステム（以後，SNS と記す）の普及により，SNS の利用者は増加している．それぞれの SNS が，利用者情報を適切に管理している．また，SNS ではグループ管理が行えるものもある．これら SNS で管理されている利用者認証情報や，グループ情報を外部のシステムで利用するための枠組みとして OAuth がある．Facebook や Twitter 等は，OAuth に対応しており，これらの認証情報を使った Web アプリケーションも多数存在している．

分散的に管理されている認証情報を使ってネットワーク利用者を認証しているシステムとして，Eduroam がある [1]．これは大学等の教育機関間の無線 LAN の相互利用を行うための仕組みである．このシステムでは，認証情報の相互利用のために Radius ツリーを構築し，IEEE 802.1x 認証を用いて利用者認証を行っている．IEEE 802.1x 認証はネットワーク利用の前に行われるため，認証を受けることができない利用者は，ネットワーク環境をいっさい利用できない．

広島大学では，2008 年度から運用している HINET2007 において，ネットワークを対象とした利用者認証を行っている [2]．利用者認証のための Web フォームによる認証を Shibboleth の SP として実装することにより，学認との認証連携を実現している [3]．持ち込み PC からの通信の制御には，ネットワークスイッチが持っている Mac アドレスをもとにした制御を利用している．具体的な手順としては SP での認証が終了すると，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作成し，持ち込み PC からそのアカウントを用いてネットワークスイッチに対する認証処理を行っている．

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 Opengate を開発し運用を行っている [4]．ゲートウェイにおける利用者認証のため

の Web によるフォーム認証を Shibboleth の SP として実装することにより，学認との認証連携を実現している [5]．持ち込み PC からの通信の制御は，ファイアウォールの IP アドレスをもとにしたアクセス制限の機能を用いている．

ヘルシンキ大学でも，佐賀大学と同様のシステムが開発されている [6]．このシステムでは持ち込み PC が接続されるネットワークとインターネットとの境界点に設置される Web サーバ機能を持つソフトウェアルータとして実装されている．Web サーバ機能が Shibboleth の SP となっている．持ち込み PC からの通信の制御は，iptables による IP アドレスをもとにしたアクセス制限の機能を用いている．

そのほかにも，持ち込み PC からの通信の制御の実現方法はいくつか存在する．それらは，持ち込み PC からの通信の制御の方法の観点に着目すると，Mac アドレスをもとにしてグループ化する方法と IP アドレスをもとにしてグループ化する方法の 2 種類に分類することができる．

Mac アドレスをもとにグループ分けする方法の利点は，グループごとに異なる仮想的なネットワークスイッチに接続されるため，認証された持ち込み PC を複数のグループに分けることができる点である．しかしながら，認証前後で持ち込み PC の IP アドレスの変更が必要となるため，持ち込み PC で用いることができるアプリケーションに制限があったり，認証後にアプリケーションを再起動する必要があったりする等利用者にとっての不便さがある点や，インシデントの発生時に利用者を特定する際の情報が複雑となり，管理者が迅速に利用者を特定することが難しくなるといった欠点がある．また，ネットワーク構成に制限が発生するため，既存の情報提供サーバや，外部の認証サーバが利用しにくくなるといった欠点がある[*1]．

一方，IP アドレスをもとにグループ分けする方法の利点は，持ち込み PC の利用開始から利用終了まで同じ IP アドレスが用いられるため，外部の認証サーバや既存の情報提供サーバの利用を柔軟に行うことが可能となる等の，管理運用のコストを小さくすることができるという点にある．しかし，既存のシステムでは，持ち込み PC にアクセス権を与える際に IP アドレスをもとにしてアクセス制御を行うため，持ち込み PC がネットワークに接続されるたびに，保護されるべきネットワークとの境界にある複数のルータ等に対してアクセス制御のための設定変更が必要となる．この問題を解決するために，ルータを 1 つだけに限定する方法が考えられる．その場合，ネットワーク構成の変更が必要になることがあり，ネットワークの自由度が低くなる．

Yap らは，OAuth や OpenID を用いて，無線によるネットワーク利用時の利用者認証に Facebook や Google+を用いる方法の提案を行っている [7]．この方法では，認証を受けた持ち込み PC と受けていない PC とのグループ分けを行っている．アクセス制限の実装には，OpenFlow の技術を用いている．そのため，この方法ではすべてのネットワーク機器が OpenFlow に対応する必要がある．また，持ち込み PC が接続されるたびに，OpenFlow のコントローラからの命令により複数のスイッチが FlowTable の変更を行わなければならず，ネットワーク機器数が多くなるにつれ変更数が多くなる．

3. ネットワークを対象としたアクセス制御の実装

本研究で想定している利用者認証によるネットワークを対象としたアクセス制御を行うシステムに求められる要求要件を以下に示す．

(1) OAuth や Shibboleth 等，外部の高度な信頼できる（trusted）認証サーバが利用できること．認証サーバが提供する利用者の属性を用いて，認証された利用者を複数のグループに分けて管理できること．
(2) ルータにおいて利用者のグループを用いてアクセス制御の設定を記述できること．この設定は，静的に設定できること．持ち込み PC が接続されるたびに変更されることがないこと．
(3) 既存のルータの構成を，アクセス制御のために変更する必要がないこと．
(4) 持ち込み PC の IP アドレスが利用開始から終了まで変化しないこと．

本論文で述べる実装では，ネットワーク管理者は分散的に管理されている信頼できる認証サーバを利用することができる．たとえば，Facebook 等の SNS では，特定の管理者がグループのメンバを管理することが可能なグループ機能が存在する．そのグループの管理者が信頼できる場合，あるいは，自らがグループ管理を行う場合，そのようなグループに対して，ネットワーク管理者がアクセス権を与える．

他にも，国立情報学研究所が進めている学認のフェデレーションに参加する Shibboleth SP として本論文で述べる実装を用いる場合には，自組織以外の IdP を信頼できる認証サーバとして利用して，特定の組織に所属し，特定の属性値を持つ利用者群をグループとして取り扱うことも可能である．

認証ゲートウェイでは，認証サーバから受け取る情報でグループ分けを行うため，グループに所属する利用者の追加変更があっても，認証ゲートウェイをはじめ，ネットワーク機器設定を変更する必要はない．また，新たにグループが作成された場合に，ネットワーク管理者がそのグループ管理者からの申請を承認するならば，グループに対するア

[*1] Mac アドレスをもとにグループ分けする方法に対して，IP アドレスを変更させない仕組みを導入することが考えられる．しかし，この仕組みを導入することによりネットワーク構成はさらに複雑になり制限も発生する．したがって，この方法については本論文における議論の対象としない．

クセス権を与えるためにグループとアクセス権の関係を認証ゲートウェイ上で設定し，アクセス権制御をルータに設定する．

本研究の目的はこれらすべての要求要件を満たすシステムの実現にある．

本論文で述べる実装は，IP アドレスをもとにグループ分けする方法に QoS（Quality of Service）技術を応用することにより，上記の要求要件を満たす．

本論文で述べる実装は，持ち込み PC の利用者が所属するグループに応じて，その PC からの IP パケットに対してグループに対応した値を QoS の技術を用いてマーキングする．そして，あらかじめルータに設定されているルールにより，そのマーキング値に対応したアクセス権の制御を実施する．これにより，持ち込み PC が接続されるたびに発生する各種設定の変更は，持ち込み PC が接続されるネットワークスイッチのマーキング設定だけとなり，アクセス制御の設定は変更しない．また，アクセス制御は分散配置されたルータで行うことが可能である．また，既存のネットワーク構成を柔軟に使えるため，外部の認証サーバや既存の情報提供サーバを柔軟に活用することが可能となる．なお，持ち込み PC の IP アドレスは，DHCP 機能による割当てを用い，利用開始から終了まで同じである．

以下に，実装の詳細について述べる．

3.1 利用するネットワーク機器

本論文において述べる実装では，以下に述べるネットワークスイッチ，ルータが利用可能であるものとする（**図 1**）．

3.1.1 ネットワークスイッチ

本論文で述べる実装では，ネットワークスイッチに持ち込み PC が接続される．本論文で述べる実装においてネットワークスイッチは複数台から構成される．ネットワークスイッチには，QoS のマーキング機能が備わっているものとする．

QoS 技術とは，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等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 [8] を用いる．ネットワークスイッチでは，到着した IP パケットに対して，指定された条件に従って，パケットの IP ヘッダに DSCP（Differentiated Services Code Point）値を書き込むことができる．本論文では，この機能のことをマーキング機能と呼ぶ．

本研究において，ネットワークスイッチとして Alaxala 社製 AX1240S を対象に実装を行った．

3.1.2 ルータ

ルータはネットワークスイッチ，他のルータとインターネット環境等の上位のネットワークとの中継をする．ルータには以下の機能が備わっているものとする．

- DSCP 値に基づいてパケットを制御する機能
- DHCP サーバ機能

いずれかのルータは持ち込み PC への IP アドレスの払い出しを行う DHCP サーバとして機能させる．

また，ルータは，持ち込み PC から送信される IP パケットにマーキングされた DSCP 値に基づいてパケットを制御することにより，グループごとに与えられたアクセス制御を行う．

本研究において，ルータとして Alaxala 社製 AX620R-2105 を対象に実装を行った．

3.2 認証ゲートウェイ

認証ゲートウェイは，利用者認証において，持ち込み PC と外部の認証サーバとの間に置かれ，外部の認証サーバの認証情報を用いて，利用者が所属するグループと利用者が使っている持ち込み PC の IP アドレスとを関連付ける．これにおいてアクセスされた持ち込み PC とその利用者のグループとの関連付けが行われると，持ち込み PC の IP アドレスが送信元アドレスとなっている IP パケットに対して，そのグループに対応する DSCP 値をマーキングする命令を，ネットワークスイッチに対して投入する．

認証ゲートウェイは Java Servlet として実装した．ネットワークスイッチに対して命令を投入する部分を Java のライブラリとした．

3.3 持ち込み PC の接続前に行われる作業

本論文で述べる実装では，ネットワークスイッチにおいて，持ち込み PC から送信される IP パケットに，持ち込み PC の利用者が所属するグループごとに同じ DSCP 値をマーキングする．本論文で述べる実装においては，IP パケットの DSCP 値に基づいて IP パケットの転送を許可するか拒否するかといったルールにより，グループごとに与えるアクセス権を表現する．たとえば，あるグループにおいて組織内のメールサーバへの通信を許可するというアクセス権は，そのグループに割り当てられた DSCP 値がマーキングされた IP パケットに対して，その送信先 IP アドレスがそのメールサーバの IP アドレスである場合には転送を許可するルールとして表現する．

持ち込み PC が認証を受ける前に所属するグループに対して，認証ゲートウェイ，外部の認証サーバおよび既存の情報提供サーバへのアクセスを許可する．

これらのルールは，持ち込み PC が接続される前にルータに設定される．したがって，本論文で述べる実装においては，持ち込み PC が接続されるたびにアクセス権に関する設定の変更は発生しない．また，これらのルールはシステムを構成するすべてのルータで設定可能である．このことは，本論文で述べる実装ではネットワーク構成に制限がないことを意味する．

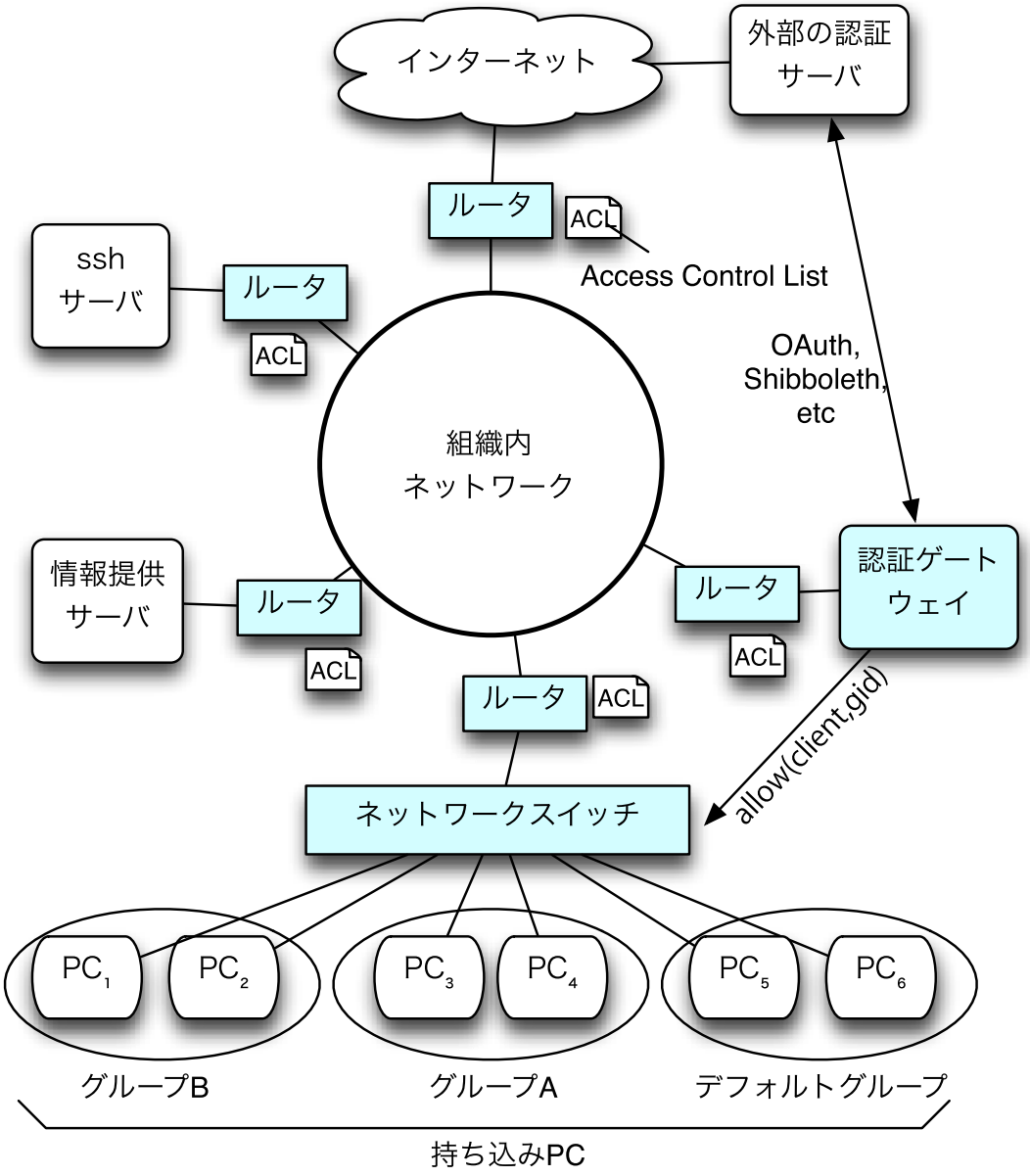

図 1 ネットワークを対象とした柔軟なアクセス制御の実装の概要
Fig. 1 Overview of an implementation of flexible access control for networks.

また，ネットワークスイッチにおいて，持ち込み PC から受け取る IP パケットには，原則として，認証を受けていないグループを表す DCSP 値をマーキングするように設定する．

3.4 持ち込み PC が接続されたときの処理

前節で述べた設定が行われた状態において，持ち込み PC が接続されて利用を開始したときの処理を以下に示す（図 2）．

(1) 持ち込み PC がネットワークに接続され，持ち込み PC から，DHCP に基づいて，IP アドレスの要求が送られる．その結果として，ルータから IP アドレス等に関する応答が送られる．
(2) 利用者は，持ち込み PC で Web ブラウザを実行し，能動的に認証ゲートウェイにアクセスする．
(3) 認証サーバは以下の手順により属性情報によりグループ情報を取得し，持ち込み PC の IP アドレスと利用

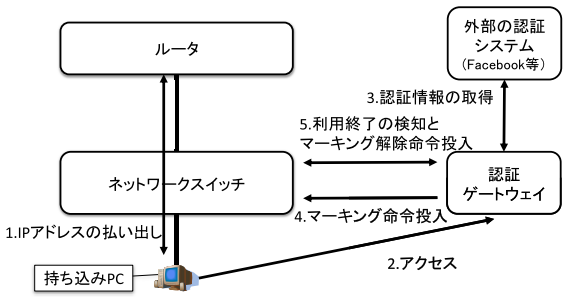

図 2 接続時の処理
Fig. 2 Processes on connect.

者の所属するグループとの関連付けを行う．

(a) 認証ゲートウェイは，利用者がまだ認証サーバで認証を受けていないと判断すると，自動的に外部の認証サーバへリダイレクトする．これは，Facebook アプリケーションや Shibboleth SP にある機能である．

(b) 利用者は，外部の認証サーバで認証を受ける．認証が成功すると，利用者の Web ブラウザは自動的に元の認証ゲートウェイにリダイレクトされる．これは，Facebook アプリケーションや Shibboleth SP にある機能である．

(c) 認証ゲートウェイは，認証サーバから利用者に関するグループ情報を取得する．たとえば，Facebook であればユーザが所属するグループの一覧情報を取得し，ネットワーク管理者が指定するグループがその中に含まれるかを調べることによりグループ情報を取得する．Shibboleth であれば，グループ分けに用いたい属性をあらかじめ IdP に設定することにより取得可能となり，その属性値を取得し，その値がネットワーク管理者が指定する値と一緒かどうかを調べることによりグループ情報を取得する．

(4) 認証ゲートウェイは，持ち込み PC が接続されているネットワークスイッチに対して，持ち込み PC から送信される IP パケットにグループに対応した DSCP 値をマーキングする命令を投入する．投入が成功すると，持ち込み PC が能動的に利用終了を宣言する際に利用する終了のボタンが含まれるページを持ち込み PC に返す．

3.5 持ち込み PC が利用終了したときの処理

本論文で示す実装において，持ち込み PC の利用終了とは，持ち込み PC がネットワークへの接続がなくなったときである．本論文で示す実装では，認証ゲートウェイでの処理が終了すると，終了ボタンが表示される．利用者はこのボタンを押すことにより，持ち込み PC の終了を能動的に宣言することができる．また，このボタンを押さずに，持ち込み PC がネットワークへ接続できなくなった場合には，ネットワークスイッチにおいて持ち込み PC からのパケットが一定時間以上到達しないときに利用が終了したと判断し，利用終了時の処理を行う．この利用終了の判断方法については，文献 [2], [3] と同様である．

3.6 ライブラリ

前節で述べたメッセージの流れにおいて，認証ゲートウェイとネットワークスイッチ間の送受信を行うためのライブラリを作成した．このライブラリは，文献 [9] で実装されている方法と同様に，telnet を用いてネットワークスイッチに接続し，コマンドラインインタフェースを介して命令を投入する．本実装では，telnet 接続を維持するようにし，ライブラリ呼び出しの部分で直列化する方法を用いた．この方法では 1 回のライブラリ呼び出しに要する時間は平均 15.5 msec であった．また，本実装では，ネットワークスイッチごとに異なる領域が割り出されるように DHCP の設定を行っているため，持ち込み PC の IP アドレスがどのネットワークスイッチの下流に接続されているかが判断可能となっている．ライブラリは，以下に述べる手続きを含む．

3.6.1 allow(client, gid)

認証ゲートウェイ上で，持ち込み PC の利用者と，その利用者が所属するグループとの関連付けがなされたとき，持ち込み PC の IP アドレスと所属すべきグループに対応した DSCP 値を引数として受け取り，ネットワークスイッチに対してその IP アドレスからの IP パケットに対して，その DSCP 値をマーキングするための命令を投入するための手続きである．

3.6.2 release(client)

持ち込み PC の利用者自身が利用終了を宣言するために，終了ボタンを押した際に，その持ち込み PC の IP アドレスからの IP パケットに対して，マーキングを解除する命令を投入する手続きである．

3.7 DSCP 値を用いたアクセス制御の設定例

ルータでは，DSCP 値に基づいたアクセス制御が行われる．たとえば，DSCP 値が 11 であり，送信先 IP アドレスが 192.0.2.1 となる IP パケットの転送を許可するルールの例を以下に示す．なお紙面の都合で 2 行となっているが本来では 1 行である．

```
ip access-list filter1 permit
src any dest 192.0.2.1 dscp 11
```

4. Facebook を用いたネットワーク認証システムの実装

この章では高度な利用者認証の例として，Facebook の利用者認証を用いる方法を示す．

Facebook では，グループを構成した利用者が，そのグループの管理者となってグループの構成員を管理することが可能となっている．持ち込み PC の利用者をこの Facebook 上で適切に管理されているグループの情報を用いてグループ分けに利用することにより，ネットワーク管理者は，利用者管理のコストを軽減することが可能となる．

Facebook では第三者が開発した Facebook のアプリケーション（以下，Facebook AP と呼ぶ）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 [10]．Facebook AP において 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，編集等を行う権限を利用者か

```
1  public class fbserv extends HttpServlet {
2
3  .....
4
5    public void doGet (HttpServletRequest  req,
6                       HttpServletResponse res)
7    throws ServletException, IOException{
8      String auth ="....." ;
9       /*access token address*/
10
11     req.getSession().setAttribute("code",
12                       req.getParameter("code"));
13     String at = getAccesstoken(auth);
14     int GID
15     try
16       if(getAccesstoken(auth) == null){
17         if(inGroup(at,LOGINSOFTLAB) == true )/*グループ確認Facebook*/
18           GID = 11
19         else
20           GID = 12
21         if(NetworkSwitch(HOST).allow(
22                 req.getRemoteAddr(),GID)== 0){
23           req.getSession().setAttribute(
24                 "access_token", at);
25           res.sendRedirect("/auth/fbcomplete.jsp");
26          }else{
27           res.sendRedirect("/auth/error.jsp");
28          }
29       }else{
30          res.sendRedirect("/auth/error.jsp");
31       }
32     } catch (InterruptedException e) {
33       e.printStackTrace();
34     }
35 }
```

図 3 実装した Facebook AP のプログラム（抜粋）
Fig. 3 A part of implemented Facebook application program.

ら得る必要がある．そのため，利用者が Facebook AP を初めて利用する場合に Facebook は利用者に Facebook AP 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 AP を利用することはできない．

Facebook AP 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（**図 4**）．Facebook で認証処理が完了すると Facebook AP のページにリダイレクトされる（**図 5**）．実装したアプリケーションでは，確認のために，利用者の氏名や，トークン，グループ等の情報を表示させている．実行結果より，アプリケーションで認証情報やグループ情報が取得できることが分かる．

この仕組みを利用して，Facebook AP 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 アドレスを持ち込み PC の IP アドレスとし，Facebook 上で特定のグループに所属しているか否かでグループ分けを行い，それぞれのグループに対して DSCP 値をマーキングする命令をネットワークスイッチに投入するようにした．

今回作成した Facebook AP の主要部分を**図 3** に示す．このプログラムでは，利用者が特定のグループのメンバであれば DSCP 値を 11 に設定し，メンバではない場合には 12 に設定した．このプログラムにより，本論文で述べる実装では，Facebook で認証をしていないグループ，Facebook により認証されたグループ，そして Facebook 上の特定のグループに所属しているグループの 3 つのグループに分けて，それぞれにアクセス権を与えることができることを確認した．このプログラムを応用することで，Facebook から提供される認証情報やグループ情報を用いて柔軟なグルー

図 4 Facebook による利用者認証
Fig. 4 User authentication on Facebook.

図 5 実装した Facebook AP のページ
Fig. 5 Page of implemented Facebook application.

プ管理が可能となる．

5. 評価

3 章では，本論文で実装したネットワークを対象としたアクセス制御の要件について述べた．3 章の要件 (1) から (4) に対して考察を行う．

要件 (1) は，認証ゲートウェイにより実現した．本研究では，認証ゲートウェイを，OAuth を用いる Facebook AP として実装した．Facebook AP では，Facebook 内に定義したグループの情報を用いることもできる．

本論文では，Facebook を対象にした認証ゲートウェイの実装を示したが，認証ゲートウェイを Shibboleth の SP として実装することもできる．そのとき，Shibboleth IdP から提供される属性情報を組み合わせることにより同様のグループ分けが可能である．

要件 (2) について，この方法により，SSH サーバへのアクセス権を制御できる．利用者認証を用いない伝統的な SMTP サーバ等へのアクセス権を，サーバの設定変更をすることなく，実現できる．また，本来であれば，構成員しかアクセスさせないイントラネットサーバに対してのアクセス制御も可能となる．さらに，大学の図書館のように公共性の高い場所でのネットワーク利用において，Facebook 等にアカウントがある来場者のアカウントをアクセス権を与えるグループに追加することにより，一時的にネットワークアクセスを提供するといったことが可能となる．

要件 (2) から要件 (4) は，持ち込み PC から受け取る IP パケットをスイッチにおいて DSCP 値をマーキングし，分散配置されたルータで DSCP 値を参照してアクセス制御を行うことにより満たすことができた．ルータでは，3.6 節で示したように，DSCP 値を用いてアクセス制御の設定を記述することができる．この設定は，静的に行うことが可能であり，持ち込み PC が接続されるたびに変更されることがない．また，持ち込み PC の IP アドレスは変化しない．

本実装は，文献 [1] の方法とは異なり，認証を受けていない利用者に対しても一部のネットワークを利用させることができる．文献 [2], [3] の方法とは異なり，本実装では利用者認証は 1 度で済む．これらの方法は，認証前後で IP アドレスが変化するが，本実装では変化しない．これらの方法はネットワークスイッチが持つ送信元 Mac アドレスによる VLAN への振り分け機能に依存している．一方，本実装では，QoS という広く普及した機能を利用している．本研究では，IP パケットに DSCP 値をマーキングする機能と DSCP 値を用いてアクセス制御の設定を行う機能を利用した．このような機能は，組織内ネットワークの基幹部分を構成するルータがネットワークスイッチでは一般的に利用可能になっている．

文献 [5] や文献 [6] の方法とは異なり，本実装では分散したルータにアクセス制御の設定を記述することができる．

本論文で述べた実装における制約事項を以下に示す．

- ユーザが QoS を使えない．QoS を使うアプリケーションとは競合してしまう．また，DSCP 値は 12 種類しか使えないため，この実装で取り扱えるグループ数の上限は 12 となる．本実装では，持ち込み PC からの DSCP 値による偽装を防ぐために，ネットワークスイッチが持ち込み PC からのパケットを受け取ると，そのパケットにすでに付けられている DSCP 値は無条件に設定に従って上書きするように設定している．したがって，持ち込み PC からのパケットを優先制御するために DSCP 値を使うことはできない．
- IP アドレスの偽装に対して弱い．ネットワークスイッチと持ち込み PC の間に NAT（Network Address Translation）機能を有する装置を設置することができない．NAT 機能を有する装置の下流に接続された持ち込み PC がアクセス権を得ると，その装置の下流に接続されている他のすべての持ち込み PC がアクセス権を得てしまう．この制約は IP アドレスをもとにしている他のシステム [5], [6] でも同じである．
- 外部の認証サーバを使うときには，認証サーバだけをアクセス可能にして，それ以外へのアクセスを拒否する設定をルータに行う必要がある．ルータにおいてこの制限を行うことができない（たとえば，IP アドレスによるアクセス制御ができない）場合には，本論文で

述べた実装は使えない．また，外部の認証サーバの IP アドレスが変化した場合には，その IP アドレスに関連するルータのアクセス制御の設定を変更する必要がある．そのための維持管理が必要になる．たとえば，本論文で述べる実装を国立情報学研究所が進めているプロジェクトである学認の SP とする場合には，自組織以外の IdP へのアクセスが必要となるが，これについてはフェデレーションのメタデータから自組織以外の IdP のホワイトリストを自動的に作成することにより対応可能であると考えられる．

6. おわりに

本論文では，高度な利用者認証が利用可能なネットワークを対象とした柔軟なアクセス制御の一実装について述べた．

この実装では，認証を受けた持ち込み PC のパケットに対してアクセス権に対応する QoS のマーキングを行い，上位のルータがそのマーキング値によりアクセス制御を行う点に特徴がある．これにより，ネットワーク構成に対する制約がないシステム構成とすることが可能である．上位のルータのアクセス制御設定を，信頼できる認証サーバのグループ管理者からの申請に基づいてネットワーク管理者が決めておくことにより，ネットワーク構成に対する制約がないシステム構成とすることが可能である．

今後は，このシステムを IPv6 に応用することや，複数の認証サーバに対応させたうえで複数のグループに所属する利用者に対して適切なアクセス権を与える手法に関する研究を行いたい．

参考文献

[1] Florio, L. and Wierenga, K.: Eduroam, providing mobility for roaming users, *Proc. EUNIS 2005 Conference* (2005).

[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（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110006967167/⟩（参照 2008-09-12）．

[3] 藤村喬寿，西村浩二，近堂　徹，大東俊博，田島浩一，相原玲二：スイッチベースの認証ネットワークへのシングルサインオン機能の実装と評価，情報処理学会論文誌，Vol.53, No.3, pp.958–968（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110008802651/⟩（参照 2012-03-15）．

[4] 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（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110002726084/⟩（参照 2001-12-15）．

[5] 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（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110007970705/⟩（参照 2010-03-15）．

[6] Linden, M. and Viitanen, V.: Roaming Network Access Using Shibboleth, *The 20th Trans European Research and Education Networking Conference* (2004).

[7] Yap, K.-K., Yiakoumis, Y., Kobayashi, M., Katti, S., Parulkar, G. and McKeown, N.: Separating Authentication, Access and Accounting: A Case Study with OpenWiFi, OpenFlow Technical Report 2011-1 (2011).

[8] 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).

[9] 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（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110007970700/⟩（参照 2010-03-15）．

[10] facebook developers: Authentication, Facebook, Inc. (online), available from ⟨https://developers.facebook.com/docs/authentication/⟩ (accessed 2011-11-23).

佐藤 聡 （正会員）

1996 年筑波大学大学院工学研究科単位取得退学．同年広島市立大学情報科学部助手．2001 年筑波大学大学院システム情報工学研究科講師．現在，同大学学術情報メディアセンター勤務．博士（工学）．キャンパスネットワークの企画管理運用，ネットワークデータベース，言語処理等の研究に従事．電子情報通信学会，ACM-SIGMOD-JAPN 各会員．

櫻井 孝一 （学生会員）

2012 年筑波大学情報学群情報科学類卒業．現在，同大学大学院システム情報工学研究科コンピュータサイエンス専攻博士前期課程在学中．ネットワーク認証やネットワークルータの研究に従事．

吉田 健一 （正会員）

1980 年東京工業大学理学部情報科学科卒業，同年日立製作所入社．1992 年 9 月博士（工学，大阪大学）．2002 年より筑波大学大学院ビジネス科学研究科教授．インターネット上の各種データを，機械学習の手法を使って解析する研究に従事．電子情報通信学会，人工知能学会各会員．

新城 靖 （正会員）

1993 年筑波大学大学院工学研究科電子・情報工学専攻博士課程修了．同年琉球大学工学部情報工学科助手．1995 年筑波大学電子･情報工学系講師, 2003 年同助教授，2004 年同大学院システム情報工学研究科助教授．2007 年同准教授．オペレーティング・システム，分散システム，仮想システム，並行システム，情報セキュリティの研究に従事．博士（工学）．ACM，IEEE，USENIX，日本ソフトウェア科学会各会員．