情報処理学会論文誌 Vol.53 No.3 958–968 (Mar. 2012)

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

藤村 喬寿[1] 西村 浩二[2,a)] 近堂 徹[2] 大東 俊博[2] 田島 浩一[2] 相原 玲二[2]

受付日 2011年6月28日, 採録日 2011年12月16日

概要：Web ブラウザをユーザインタフェースとする Web アプリケーションでは，セキュリティ上の理由から認証を要求するのが一般的であり，利用者はサービスを渡り歩くたびに繰り返し認証を行う必要がある．その一方で，ネットワークの利用者認証も普及しつつあることから，認証を行う機会は増加する一方である．その解決策としてシングルサインオンが注目されている．ネットワークの利用者認証にシングルサインオンを導入することで，Web アプリケーションとの認証連携が可能となり，結果として利便性の向上と管理の効率化が期待できる．しかし，ハードウェアリソースに厳しい制約がある認証スイッチを利用した認証ネットワークでの実装は存在しない．そこで本稿では，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方式を提案し，性能評価によりその有効性を示す．またベンダが異なる認証スイッチに対する性能評価を通して，提案方式の汎用性を示す．

キーワード：シングルサインオン，学認，認証スイッチ，キャンパスネットワーク

Implementation and Evaluation of Single Sign-On Function for Switch based Authentication Network

Takatoshi Fujimura[1] Kouji Nishimura[2,a)] Tohru Kondo[2]
Toshihiro Ohigashi[2] Koichi Tashima[2] Reiji Aibara[2]

Received: June 28, 2011, Accepted: December 16, 2011

Abstract: It is quite natural for Web applications to request the user authentication from security reasons. Then users are required to authenticate themselves repeatedly when they use from one service to the other. The network authentication increases the opportunity for user to make user authentication, too. For such problems, Single Sign-On will provide the convenience of managing user authentication information appropriately. However, the deployment of SSO to switch-based network authentication system has been discussed yet. In this paper, we propose the implementation of SSO to switch-based network authentication system and show the effectiveness by its performance evaluation. We also describe the applicability by applying our proposed method to the other authentication switch.

Keywords: Single Sign-On, GakuNin, authentication switch, campus network

1. はじめに

Web ブラウザをユーザインタフェースとするアプリケーション（Web アプリケーション）は，端末や OS への依存性が低いことから，業務作業の効率化や教育支援などの用途で広く普及した．その結果，利用者が複数の Web アプリケーションを渡り歩くようになった．Web アプリケーションでは，セキュリティ上の理由から認証を要求するのが一般的であり，複数の Web アプリケーションを利用する際には，利用者は繰り返し認証を行う必要がある．さらに，Web アプリケーションで使用するアカウントは管理主

[1] 西部電気工業株式会社
Seibu Electric Industry Co. Ltd., Fukuoka 812–8565, Japan
[2] 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University, Higashi-hiroshima, Hiroshima 739–8511, Japan
[a)] kouji@hiroshima-u.ac.jp

体ごとに発行されるため，利用者は複数のアカウントを適切に管理する必要がある．しかしこのアカウント管理の煩雑さから，セキュリティ意識の低い利用者はすべてのアカウントやパスワードを共通にしたり，安易なパスワードを設定したりする傾向があり，セキュリティレベル低下の要因の 1 つとなっている．

このような状況の解決策として，シングルサインオン（SSO：Single Sign-On）が注目されている．SSO は，利用者に対しては 1 回の認証手続きで利用権限のあるサービスの利用を可能とする利便性を提供する．一方，認証システムとサービス提供システムを分離し，サービス提供システムに必要以上の個人情報が提供されない仕組みとなっているため，利用者の匿名性を確保しつつ，サービス提供システム管理者に対しては利用者の一意性と追跡性を提供する認証情報交換基盤である．日本における SSO 利用の取り組みとしては，国立情報学研究所（NII）が主導する学術認証フェデレーション（学認）がある [1]．

広島大学では，2002 年度から全学統一 ID 基盤の運用が開始され，学内に存在する多くの Web アプリケーションで利用されてきた．また 2008 年度からは，ネットワーク利用に際して利用者認証を必要とするキャンパスネットワーク HINET2007 の運用を開始した [2], [3]．そのため，利用者はネットワークの利用，Web アプリケーションの利用に先立って毎日数回の利用者認証が必要となり，セキュリティ向上という本来の目的への理解はあるものの，認証手続きの煩雑さへの不満が生じていた．このようなネットワーク認証基盤に SSO 機能を導入することで，学内に存在する多くの Web アプリケーションとの認証連携が可能となり，利用者の利便性の向上と，それにともなう認証習慣の定着化が期待できる．さらに，認証連携を組織間に拡大することで，訪問者が自組織のアカウントでネットワークを利用できるゲストサービスも展開可能となる．

本稿では，スイッチベースの認証ネットワークへの SSO 機能の実装手法を提案し，性能評価によりその有効性を示す．ただし，ハードウェアリソースに厳しい制限がある認証スイッチに SSO 機能を実装することは容易ではないことから，本稿では認証スイッチに改変を加えることなく SSO 機能を追加する方式をとる．そのため，提案方式は既存のスイッチベースの認証ネットワークにも適用可能である．本稿では，ベンダが異なる認証スイッチに対する性能評価を通して，提案方式の汎用性を示す．本稿の構成は以下のとおりである．2 章では関連する研究を紹介し，スイッチベースの認証ネットワークでの実現の困難さを述べる．3 章では，提案する 2 方式の実装方法について説明し，続く 4 章で性能測定について述べる．5 章では，まとめと提案方式の運用状況のほか，今後の課題について述べる．

2. 関連する技術とシステム

2.1 Shibboleth

Shibboleth [4] は，Internet2 によって開発された SAML [5] をベースとする，認証のための属性交換を行うミドルウェアである．Shibboleth は**図 1** に示すように，サービスの利用認証を行う IdP（Identity Provider），IdP から提供される権限情報に基づいて Web サービスを提供する SP（Service Provider），SP が複数の IdP と連携する場合に IdP のリストを提供する DS（Discovery Service）で構成されている．自組織の IdP が SP と認証連携をすることで，利用者は自組織の IdP での認証により SP が利用できるようになる．また 1 度認証を行うと認証チケットが発行されるため，Web ブラウザを閉じるまでの間の SP 利用の際の認証は認証チケットの提示によって行われる．

2.2 SSO-Opengate

認証ネットワークの SSO 化の試みとして，佐賀大学のキャンパスネットワークで運用されている SSO-Opengate [6] がある．SSO-Opengate は，認証ポイントとなるゲートウェイに Shibboleth を実装し，認証機能と連携させることで SSO を実現している．SSO-Opengate では，ネットワーク認証状態の維持を Web ブラウザ上の JavaApplet（または Ajax）によって行っている．そのため，Web ブラウザを閉じるとネットワーク認証と SSO の両方が終了する．SSO-Opengate は PC 上にゲートウェイを実装することで，Shibboleth による SSO 認証の実装や，仮想マシン上にゲートウェイを実装 [7] が可能であるなど拡張性に優れている．しかし，ゲートウェイ方式ではトラフィックや認証が集中するため，大規模なネットワークでは，高負荷時のデータ転送においてワイヤレートが出ないなどの問題がある．

2.3 HINET2007

広島大学では，2008 年度から HINET2007 の運用を開始した [2], [3]．HINET2007 では，セキュアでスケーラブルなネットワークを構築するため約 460 台の認証スイッチによるスイッチベースの認証ネットワークを採用している．

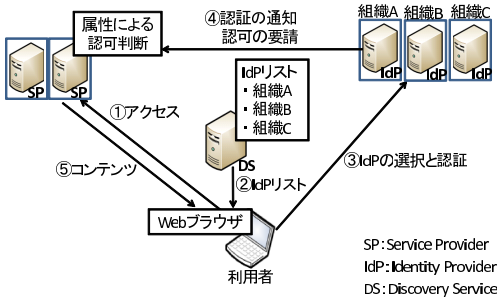

図 1 Shibboleth の認証手順
Fig. 1 Shibboleth authentication.

約2万人の構成員が利用する大規模ネットワークにおいて，ネットワークの入り口で認証を要求する水際対策と各認証スイッチでの分散処理によって，セキュリティとスケーラビリティに対する要件を満たしている[*1]．

本稿では，認証スイッチにより構成される HINET2007 に，SSO 機能を追加する方法について述べる．しかし，認証スイッチにはメモリなどの資源に強い制約があるため，認証スイッチ上に Shibboleth を実装することは困難である．Shibboleth 対応が難しい場合への対策として，アプリケーションの認証を代理で行うログインプロキシを設置する方法[*2]があるが，認証スイッチは端末情報（MAC アドレスや IP アドレス）とアカウント情報で認証状態を管理する．そのため，ログインプロキシ経由では認証を行うことができない．

このようにスイッチベースの認証ネットワークにはゲートウェイのような拡張性はないが，セキュリティとスケーラビリティ，そしてハードウェア処理による高スループットというメリットがある．そのため，今後はスイッチベースの認証ネットワークへの SSO 機能追加の要求が高まることが予想される．

3. スイッチベースの認証ネットワークでの SSO 認証の実現

前章で述べたように，スイッチベースの認証ネットワークでの SSO 機能の実現には，認証スイッチに対する機能拡張を前提にできないという条件がある．この条件に加え，利用者の利便性を向上させることを主たる目的として，次の3つを満たすべき機能要件とした．

（1）SSO 機能を利用する場合，当該機能を選択する以外の操作を必要としない[*3]．
（2）認証中は利用者に無用な画面遷移を見せない．
（3）一時的なアカウント（以下，一時アカウントと呼ぶ）を使用する場合でも，利用者はそれを覚えたり入力したりする必要がない．

以下では，これらの条件を満たす2方式を提案する [8]．

[*1] 無線 LAN に対しては，ローミングによる意図しない切断を防ぐため，認証ポイントをエッジスイッチではなく，ゲートウェイ付近に配置している．
[*2] https://upki-portal.nii.ac.jp/docs/fed/technical/sp/WebApp/
[*3] HINET2007 ではネットワーク認証状態の維持を定期的な ARP 応答により行うため，Web ブラウザを起動し続ける必要はない．そのため Web ブラウザを閉じることで SSO の認証状態のみを解除することができる．しかし，SSO 化により利用する予定のない Web アプリケーションも認証状態となってしまうことを防ぐため，本稿では必要に応じて利用者に SSO 認証を選択させることとした．一方，SSO の認証状態を維持したままネットワーク認証が解除される場合がある．静的アカウント方式の場合は再度認証情報を入力し直す必要があるが，動的アカウント方式の場合は SSO によりネットワークの認証状態を復旧させることができる．

表 1 静的アカウント・動的アカウント方式の比較
Table 1 Comparison of static account method and dynamic account method.

	SSO 認証	ネットワーク認証	学内者	学外者
静的アカウント方式	IdP の認証情報	IdP と同じ認証情報	○	×
動的アカウント方式	IdP の認証情報	一時アカウント	○	○

静的アカウント方式
SSO 認証に使用する認証情報（アカウントとパスワード）をネットワーク認証でも利用する方式である．次に述べる動的アカウント方式に対して一時アカウントの生成を必要としないことから，静的アカウント方式と呼ぶ．SSO 認証とネットワーク認証で同じ認証情報を利用していることが前提となるため，学内者向けの利用に限られる．

動的アカウント方式
SSO 認証の結果に基づいてネットワーク認証用の一時アカウントを動的に生成してネットワーク認証を行う方式である．SSO 認証では所属組織で使用しているアカウントを，ネットワーク認証では動的に生成された一時アカウントを使用する．一時アカウントの登録や削除などの処理が必要となる一方，SSO 認証とネットワーク認証の認証情報が異なってもよいため，SSO 連携する他組織の構成員にネットワーク利用を提供することができる．

両方式の比較を**表 1** に示す．

3.1 静的アカウント方式の認証手順

静的アカウント方式での認証手順を**図 2** に示す．各ステップの概要は以下のとおりである．

（a1）任意の URL へのアクセス
任意の URL へアクセスすると，ネットワーク認証ページにリダイレクトされる．ここで認証情報を入力すると，従来のネットワーク認証を行うことができる．

（a2）SSO 認証の選択
ネットワーク認証ページ内の SSO 認証へのリンクを選択する（機能要件（1））と，SP にリダイレクトされ，続いてあらかじめ指定された IdP にリダイレクトされる．IdP からは Javascript を含む SSO 認証ページが返される．

（a3）認証情報入力ページの表示
（a2）で返された SSO 認証ページを表示したまま，再度ネットワーク認証ページにリダイレクトされ，SSO 認証，ネットワーク認証ともに認証情報の入力待ちとなる．

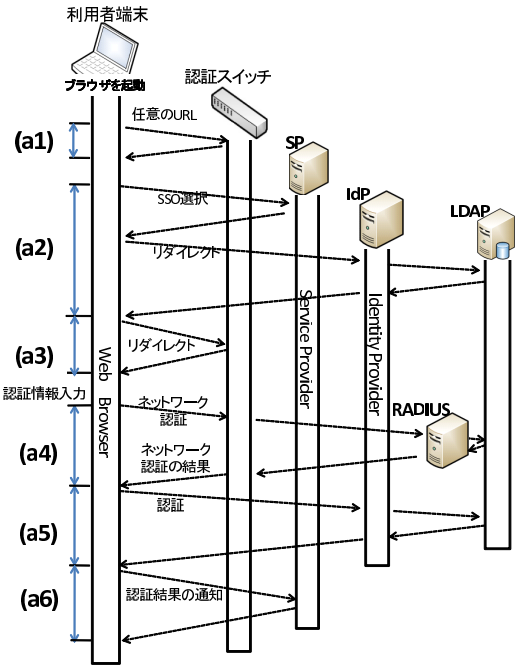

図 2 静的アカウント方式の認証手順
Fig. 2 Authentication flow of static account method.

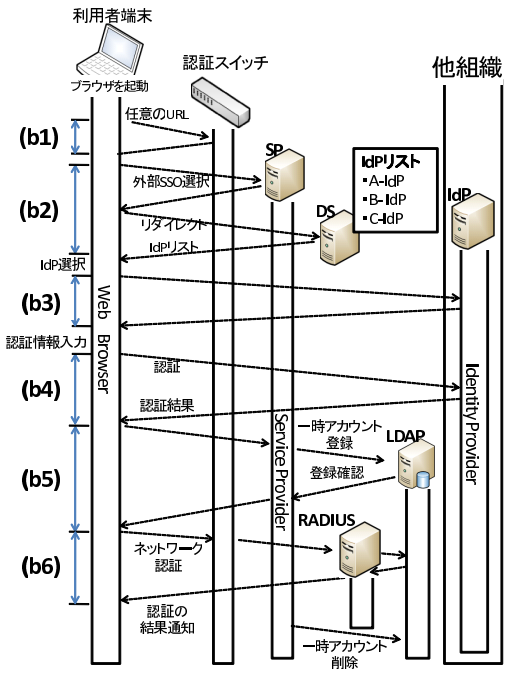

図 3 動的アカウント方式の認証手順
Fig. 3 Authentication flow of dynamic account method.

（a4）認証スイッチへの認証情報の送信
画面遷移をともなわない状態で，入力された認証情報が認証スイッチへ送信（HTTPS で POST）される．

（a5）IdP への認証情報の送信
認証スイッチでのネットワーク認証が成功するとネットワークが利用可能となり，続いて同じ認証情報が IdP に送信される．IdP での SSO 認証が成功すると，SP にリダイレクトされる．

（a6）SP への認証結果の通知
SP による利用権限の確認後，認証完了を通知するページが返される．

IdP はクライアント上の Web ブラウザに認証チケットを発行するため，クライアントから SP を経由したアクセスが必要であり，一方認証スイッチはクライアントの MAC アドレスと IP アドレスを取得するため，クライアントから直接アクセスされる必要がある．静的アカウント方式では，これらの技術的要件と（a3）～（a5）の処理で画面遷移を発生させない機能要件（2）を両立させるため，（a2）で返される SSO 認証ページにおいて Ajax の非同期通信技術を利用している．

3.2 動的アカウント方式の認証手順

動的アカウント方式の認証手順を図 **3** に示す．各ステップの概要は以下のとおりである．

（b1）任意の URL へのアクセス
任意の URL へアクセスすると，ネットワーク認証ページにリダイレクトされる．ここで認証情報を入力すると，従来のネットワーク認証を行うことができる．

（b2）SSO 認証の選択
ネットワーク認証ページ内の SSO 認証へのリンクを選択する（機能要件（1））と，DS へリダイレクトされる．

（b3）自組織の IdP の選択
DS で自組織の IdP を選択するとリダイレクトされ，IdP から SSO 認証ページが返されて，認証情報の入力待ちとなる．

（b4）IdP への認証情報の送信
入力された認証情報が IdP に送信される．IdP での認証が成功すると，SP にリダイレクトされる．

（b5）SP への認証結果の通知と一時アカウント登録
SP による利用権限の確認後，一時アカウントおよびパスワードが生成・登録され，その認証情報を認証スイッチにリダイレクトするページが返される．

（b6）一時アカウントによるネットワーク認証
一時アカウントとパスワードが認証スイッチに送信（HTTPS で POST）され，認証完了を通知するページが返される．

動的アカウント方式では，（b2）～（b4）で SSO 認証が行われた後，（b5）で一時アカウントの登録，（b6）で一時アカウントによるネットワーク認証が行われる．このとき，（b5）～（b6）の処理において利用者に画面遷移を見せず（機能要件（2）），利用者が一時アカウントの認証情報を覚えたり，入力したりする必要をなくす（機能要件（3））ため，（b5）で返されるページに（b6）を自動的に行うための Javascript を埋め込んでいる．

なお（b2），（b3）はネットワーク認証前のアクセスとな

るため，DS と IdP に対しては事前に HTTPS 通信を許可しておく必要がある．これについては，学認から提供されるメタデータから定期的に DS と IdP を抽出し，認証スイッチに設定を行っている．

不正利用などのインシデントが発生した場合は，一時アカウントの情報から SP のログを調査し，SP に提供された情報から利用者の所属組織の IdP のログでの調査を依頼することで，不正利用者の追跡が可能となる．また，DS と IdP に対する認証前の通信許可設定には慎重な対応が必要であるが，DS と IdP への HTTPS 通信のみに限定されており，インシデント発生時には MAC アドレスや IP アドレスなどから原因の特定と対応が可能であることから，セキュリティ上の大きな問題はないと考えている．

3.3 一時アカウントの登録と削除

一時アカウントの登録にあたって，まず，アカウント名やパスワードの生成に利用する，アクセスごとにユニークな値（アクセス ID）を生成する．アクセス ID は [サーバ ID-利用カウンタ] の形式であり，サーバ ID を加えることで，複数の SP を構築して運用した場合でもユニークになるようにしている．

パスワードは，ハッシュ関数（HMAC-SHA256 [9], [10]）に秘密鍵とアクセス ID を入力して得られたハッシュ値を Base64 でエンコードし，その上位 32 文字とした[*4]．

アカウント名には，運営組織の事情に応じた形式が選択できる．先に述べたように，SSO の利用目的の 1 つはサービス提供システムに必要以上の個人情報を提示しないことにある．そのため，ネットワーク認証の管理者と IdP の管理者が異なる場合はアクセス ID を（case1），同一の場合は IdP から得られる ePPN（eduPersonPrincipalName）を（case2），アカウント名として利用することで，それぞれの管理者に対して利用者の匿名性と一意性（追跡性）を両立させた形で利用者情報を提供することができる．アクセス ID とアカウント名，パスワードの組合せ例を以下に示す．

アクセス ID が 01-8713000000000 の場合
[case1：アクセス ID をアカウント名に利用]
アカウント名：01-8713000000000
パスワード：s1cVuz0IfjD45qJEva4hMky51knBhkcj
[case2：ePPN をアカウント名に利用]
アカウント名：testuid@hiroshima-u.ac.jp
パスワード：s1cVuz0IfjD45qJEva4hMky51knBhkcj

一時アカウントは，1 回だけ認証に利用できるよう制限を設けている．しかし，使用済みアカウントや未使用状態のアカウントが長くシステムに存在することは，検索負荷の増大やセキュリティ上のトラブルの原因となりうる．そこで，一時アカウントに有効期限を設け，登録後一定時間が経過した一時アカウントは，削除プロセスにより自動的に削除を行う．なお今回の実装では，有効期限を 120 秒とした．

[*4] HINET2007 で利用されている認証スイッチの仕様から，アカウント名とパスワードの最大長はそれぞれ 32 文字となっている．

4. 性能評価

HINET2007 設計時に行われた利用状況に関する事前調査（平成 22 年 7 月 20 日実施）では，事務部門の始業時間帯にあたる 8 時 20 分～35 分の間（15 分間）に約 700 台からの認証要求が集中することが分かっている [11]．HINET2007 のネットワーク認証機能の仕様は，この結果に基づいて決定された[*5]．このように，実運用に耐えるネットワーク認証を実現するには，認証要求の集中に対する耐性の検証は不可欠である．そこで本章では，HINET2007 の性能要件を満たすことを条件としたうえで，各方式において認証要求が集中した際の各ステップの処理時間を測定して，SSO 機能の追加によって増加する処理時間が全体の処理時間に与える影響を評価する．

性能測定に使用した機器の仕様を**表 2** に，ネットワーク構成を**図 4** に示す．測定はクライアント上で Jmeter[*6] を起動し，各方式の認証手順に基づいたシナリオファイルを実行して，HTTP リクエストの送信から HTTP レスポンスの受信までの時間を測ることで行った．測定は 1 から 256 クライアントまで各 10 回行い，その平均を測定値とした．HTTP レスポンスのタイムアウトを 120 秒に設定し，タイムアウトしたクライアントは認証が成立しなかったものとして，測定値の計算対象から除外した．以下，特に断わりがない場合は，タイムアウトは発生していない．5 クライアント未満の測定は実機で，それ以上は Jmeter の擬似セッション生成機能を使用し，4 台のクライアント上で 8，16，32，64，128，256 台の擬似クライアントをシミュレートした．Jmeter の同期実行には dsh[*7] を使用し，操作 PC から各クライアントに制御コマンドを送信して実行した．

4.1 静的アカウント方式の処理性能

測定結果を**図 5** に示す．縦軸は HTTP レスポンスが戻るまでの時間を対数で，横軸は処理の番号を示している．測定の結果，256 クライアントの場合に（a1）で 19%のタイムアウトが発生したが，その他の箇所ではタイムアウトや処理の失敗は観測されなかった．図 5 から，認証スイッチでの処理である（a1），（a3），（a4）の処理時間が支配的であり，SSO 機能のための処理である（a2），（a5），（a6）の処理時間はクライアント数によらずほぼ一定であることが確認できる．また（a1）で発生したタイムアウトは，

[*5] 100 台からの同時の認証要求に対してすべての認証が成立し，かつ認証処理（図 2（a4）および図 3（b6））が 30 秒以内に完了することを性能要件とした．
[*6] http://jakarta.apache.org/jmeter/
[*7] http://www.netfort.gr.jp/ dancer/software/dsh.html

表 2 性能測定に使用した機器の仕様
Table 2 Specifications used for performance evaluation.

SP/LDAP	
CPU	Intel® Pentium® 4 CPU 1.90 GHz
Memory	1 GB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	Shibboleth-SP 2.3.1, Tomcat 6.0.26, Apache 2.2.3, OpenLDAP 2.3.43（一時アカウント用）
IdP/LDAP	
CPU	Intel® Pentium® 4 CPU 1.60 GHz
Memory	640 MB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	Shibboleth-IdP 2.2.0, Tomcat 6.0.26, Apache 2.2.3, OpenLDAP 2.3.43（認証アカウント用）
DS	
CPU	Intel® Pentium® 4 CPU 1.60 GHz
Memory	640 MB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	Shibboleth-DS 1.0.0, Tomcat 6.0.26, Apache 2.2.3
RADIUS	
CPU	Intel® Pentium® 4 CPU 2.80 GHz
Memory	512 MB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	FreeRADIUS 2.1.10
クライアント× 4	
CPU	Intel® Core™i7 CPU 920 @ 2.67 GHz
Memory	6 GB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	Jmeter 2.4
操作 PC	
CPU	Intel® Atom™ CPU N270 @ 1.60 GHz
Memory	1 GB
OS	Ubuntu 9.10（2.6.31-22-generic）
Package	dsh 0.22.0
認証 SW	
Product	Alaxala AX2400S
CPU	PowerPC® 533 MHz
Memory	256 MB

（a1）を通過したリクエストが（a3），（a4）で繰り返し認証スイッチに接続を要求したことで，認証スイッチの接続待ちキューが枯渇したことが原因であると考えられる．以上から，静的アカウント方式は前述の性能要件を満たしており，SSO 機能の追加による全体の処理時間への影響はほとんどないことが確認された．

4.2 動的アカウント方式の処理性能の測定

測定の結果を**図 6** に示す．縦軸・横軸は図 5 と同様である．処理が完了した否かは，HTTP レスポンスより判断した．測定の結果，すべての箇所でタイムアウトや処理の失敗は観測されなかった．図 6 から，認証スイッチでの処理である（b1），（b6）の処理時間が支配的であり，SSO 機能のための処理である（b2）～（b5）の処理時間はクライアント数によらずほぼ一定であることが確認できる．本方式では，認証スイッチによる処理のボトルネックが（b1）と（b6）の 2 カ所のみであったため，静的アカウント方式のようなタイムアウトが発生しなかったと考えられる．以上

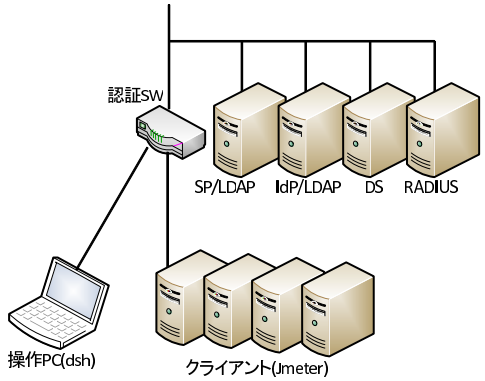

図 4 性能測定のネットワーク構成
Fig. 4 Network topology for performance evaluation.

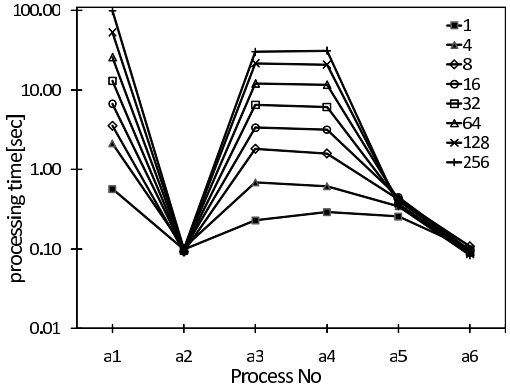

図 5 静的アカウント方式の性能測定
Fig. 5 Evaluation results of static account method.

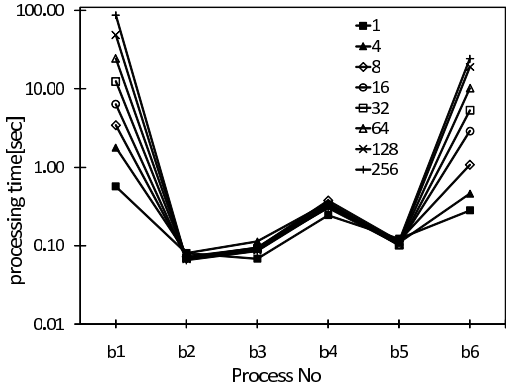

図 6 動的アカウント方式の性能測定
Fig. 6 Evaluation results of dynamic account method.

から，動的アカウント方式は前述の性能要件を満たしており，SSO 機能の追加による全体の処理時間への影響はほどんどないことが確認された．

動的アカウント方式では，静的アカウント方式と異なり，一時アカウントの登録処理が必要となる．一時アカウントの登録処理による処理時間の増加が懸念されるのと同時に，今後認証スイッチの処理性能が向上すると，この処理にリクエストが集中する可能性がある．そこで，一時アカウントの登録処理を行う CGI に複数のクライアントから同時アクセスさせた場合の処理時間を測定した．測定の結果を**図 7** に示す．縦軸は HTTP レスポンスが戻るまでの時間，横軸は同時アクセス数を示している．測定の結果，128 クライアントからのアクセスを 5 秒以内で処理できることが分かった．したがって，一時アカウントの登録処理にリクエストが集中する状況でも実用的な時間で処理できることが確認できた．

4.3 各方式の比較

静的アカウント方式は，一時アカウントの登録・削除にともなう処理時間が発生しないため，すでに学内にアカウントを持つ利用者を対象とする処理負荷の小さい SSO サービスとして設計した．しかし，測定の結果，動的アカウント方式の方が処理時間が小さいことが分かった．静的アカウント方式では（a3）の処理が必要であるため，認証スイッチへのアクセス回数が多く，それにより負荷が高くなることが影響していると考えられる．一方，当初懸念された（b5）の一時アカウント登録処理はほぼ一定の時間で処理可能であり，認証スイッチの処理時間の増加と比較して十分に小さい値であった．結果，SSO 機能を利用しないネットワーク認証と同程度の時間で処理可能あることが分かった．

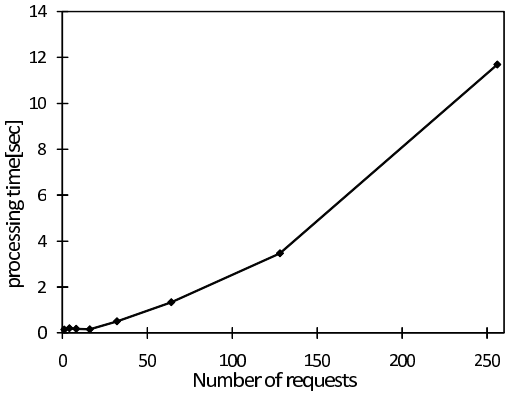

図 7 一時アカウント登録処理（b5）の性能測定
Fig. 7 Evaluation results of registering temporary account (b5).

以上の考察により，より一般性のある動的アカウント方式のみを採用すればよいことが判明した．ただし，学内利用者に対しては IdP を選択させる必要がないため，サービス提供の際には，DS から IdP を選択する「学外者用」と，IdP をあらかじめ指定した「学内者用」の 2 つのリンクを用意することで，学内利用者への便宜を図ることとした．

4.4 認証スイッチの違いによる処理性能への影響

本稿の提案方式は，ネットワークスイッチへの機能拡張を必要としないため，Web 認証機能を有する認証スイッチに対して汎用的な拡張方式となりうる．しかし，4.1 節，4.2 節で明らかになったように，認証スイッチでの処理が支配的であることから，認証スイッチの性能の違いが，全体の処理性能に及ぼす影響を明らかにすることは，汎用性を確認するうえで重要である．そこで，ベンダが異なる 2 種類の認証スイッチに対して動的アカウント方式を適用し，提案方式の汎用性の確認と性能評価を行う．

測定に使用した機器の仕様を**表 3** に，ネットワーク構成を**図 8** に示す．クライアントと操作 PC の仕様は表 2 と同じである．また測定方法も，試行回数が 5 回であるほかは 4 章と同様である．次に本測定で使用する認証手順は 4.2 節を基本とするが，2 つの認証スイッチの測定条件を揃えるため，運用上の理由から複雑化していた部分および認証手順の簡素化を行った．前者は，運用状況を表示させるためフレーム化していた認証ページをフレームなしの簡素

表 3 認証スイッチ別性能測定で使用した機器の仕様
Table 3 Specifications used for performance evaluation of authentication switch.

ESXi サーバ	
CPU	Intel® Core™2 Quad CPU Q6600 @2.40 GHz
Memory	3 GB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
SP/LDAP[仮想サーバ]	
CPU	1 vCPU
Memory	1 GB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	Shibboleth-SP 2.3.1, Tomcat 6.0.26, Apache 2.2.3, OpenLDAP 2.3.43（一時アカウント用）
IdP[仮想サーバ]	
CPU	1 vCPU
Memory	640 MB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	Shibboleth-IdP 2.2.0, Tomcat 6.0.26, Apache 2.2.3
RADIUS/LDAP[仮想サーバ]	
CPU	1 vCPU
Memory	640 MB
OS	CentOS 5.4（2.6.18-164.11.1.el5）
Package	FreeRADIUS 2.1.10, OpenLDAP 2.3.43（認証アカウント用）
認証 SW-A	
Product	Alaxala AX2400S
CPU	PowerPC® 533 MHz
Memory	256 MB
認証 SW-B	
Product	Apresia 13000-48X
CPU	非公開
Memory	512 MB

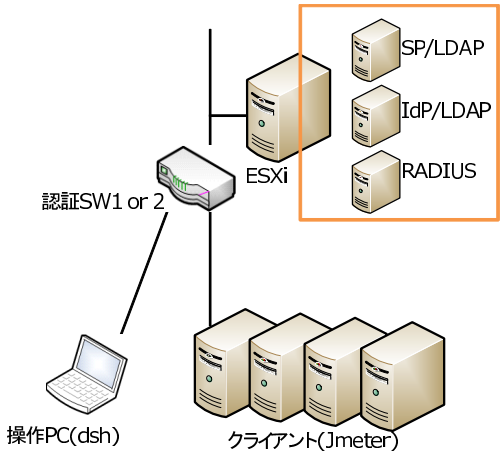

図 8 認証スイッチ別性能測定のネットワーク構成
Fig. 8 Network topology for performance evaluation of authentication switch.

なページに変更した．これは，認証 SW-B の仕様上の制限により，複雑な認証ページを保持できないという理由によるものである．後者は，よりリクエストが集中する状況を作るため，学内者向けサービスを想定し，DS による IdP 選択の手順を省略したものである．これらを反映させた認証手順を図 9 に示す．なお，2 つの認証スイッチ間で本質

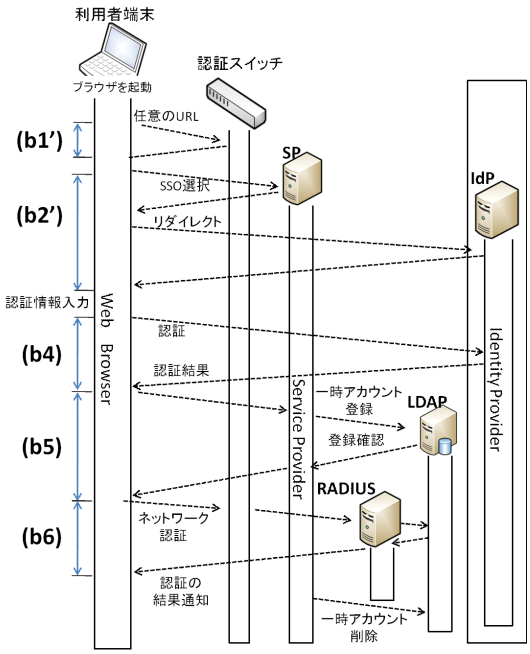

図 9 動的アカウント方式の認証手順（変更後）
Fig. 9 Authentication flow of dynamic account method (modified).

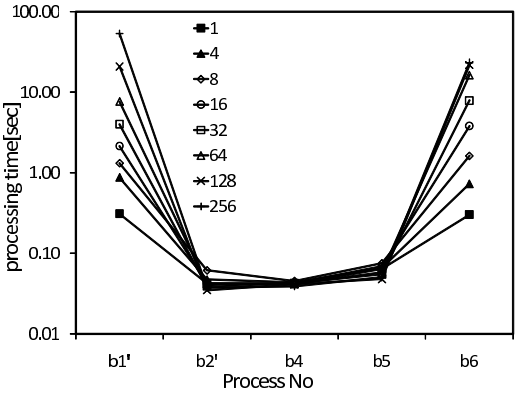

図 10 認証 SW-A の測定
Fig. 10 Evaluation results of authentication switch A.

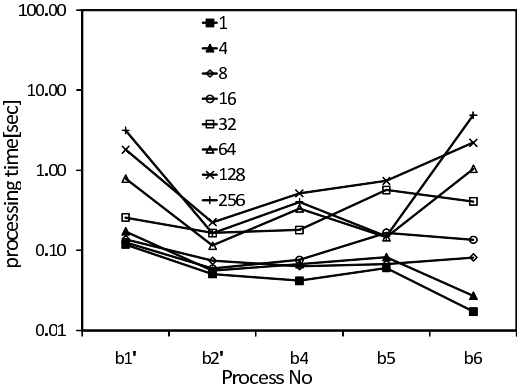

図 11 認証 SW-B の測定
Fig. 11 Evaluation results of authentication switch B.

的に異なるのは，HTTPS で POST する URL（ホスト名と引数として渡す認証情報のフォーマット）のみであり，提案方式は他の認証スイッチにも容易に対応できるようになっている．

認証 SW-A，認証 SW-B の測定結果をそれぞれ**図 10**，**図 11** に示す．縦軸は HTTP レスポンスが戻るまでの時間を対数で，横軸は処理の番号を示している．測定の結果，認証 SW-B を用いた 256 クライアントの場合に（b6）で 21%のタイムアウトが発生したほかは，タイムアウトや処理の失敗は観測されなかった．

測定の結果，認証 SW-A に比較して認証 SW-B の SSO 機能のための処理である（b2’），（b4），（b5）の処理時間が増加した．認証 SW-B は認証 SW-A より処理性能が高いことから（b1’）の処理時間が短くなり，（b2’）以降の処理にボトルネックが移動したと考えられる．しかしながら，（b2’），（b4），（b5）の平均処理時間はどのクライアント数においても 1 秒以内であったため，（b6）にリクエストが集中したと考えられる．その結果，256 クライアントの場合には認証スイッチの接続待ちキューが溢れ，タイムアウトが観測されたと考えられる．また，**表 4** に図 10，図 11 の各クライアント数における処理時間の最悪値 [sec] を示す．128 クライアントを例にとると，全体の処理時間は

表 4 認証スイッチ別性能測定の各クライアントにおける最悪値
Table 4 Worst-case value of performance evaluation of authentication switch.

クライアント数 [台]	認証 SW-A [sec]	認証 SW-B [sec]
1	0.9	0.3
4	2.0	0.6
8	4.0	0.8
16	7.7	1.4
32	15.5	2.3
64	49.0	3.0
128	71.0	7.6
256	140.0	12.1*

* タイムアウトを除く．

71.0 [sec] から 7.6 [sec] に短縮されており，認証スイッチの処理性能向上が全体の処理性能向上に貢献することが確認された．ただし，認証スイッチによっては接続待ちキューが溢れることによるタイムアウトが観測されるなど，仕様に現れない条件が存在する場合がある．そのため，実運用に際しては十分なテストを行い，リクエストが集中するポイントを見極めて対応する必要がある．

5. おわりに

本稿では，HINET2007 に代表されるスイッチベースの認証ネットワークへ SSO 機能を追加する，静的アカウント方式，動的アカウント方式の 2 方式について性能評価を行った．その結果，一時アカウントの生成・削除を必要とする動的アカウント方式の方が処理性能に優れており，また一般性もあることから，スイッチベースの認証ネットワークに適した方式であることが分かった．また異なるベンダの認証スイッチに動的アカウント方式を適用した場合の性能評価を行い，本方式の汎用性の高さを示した．本稿の結果は，既存のスイッチベースの認証ネットワークに SSO 機能を追加する際の指標となるだけでなく，今後認証スイッチの処理性能が向上した際に，認証スイッチ上に SSO 機能を実装するか否かの判断材料となる．

HINET2007 では，2010（平成 23）年 11 月 22 日より動的アカウント方式による SSO 機能の運用を開始し，本学構成員は自らのアカウントで，学認参加組織の構成員は所属組織のアカウントで HINET2007 の利用が可能である．

今後の課題として，SSO 対応 Web サービスの充実があげられる．1 章で述べたように，広島大学でもさまざまな Web サービスが運用されており，HINET2007 への SSO 機能の追加によって，その利便性が飛躍的に向上することが期待できる．ただしその一方で，利用者教育の徹底も重要な課題である．SSO は認証情報の一元化を促進し，利用者はアカウント管理の煩雑さから開放される．しかし，1 つの認証情報が漏えいすることで，利用権限があるすべてのサービスでなりすましが可能になるという危険もあわせ

持っている．セキュリティレベルの異なるサービスではステップアップ認証を要求するなど，システム面での対策と同時に利用者のセキュリティに対する意識の向上も図る必要がある．

謝辞 本研究にあたってシステムの設計，実装の議論にご参加していただいた広島大学情報メディア教育研究センターの関係者に心から感謝いたします．本研究の一部は科研費（23500089）の助成を受けたものである．

参考文献

[1] 国立情報学研究所：GakuNin – Academic Access Management Federation in Japan, 入手先 ⟨http://www.gakunin.jp/⟩（参照 2011-12-26）.
[2] 相原玲二，西村浩二，岸場清悟，田島浩一，近堂 徹：利用者認証機能を持つ大規模キャンパスネットワークの構築，電子情報通信学会 2008 年総合大会，BS-8-7, pp.S-116–S-117 (2008).
[3] 西村浩二，相原玲二，近堂 徹，大東俊博，田島浩一，岸場清悟，岩田則和：日本最大規模のキャンパス認証ネットワーク—HINET2007 の構築と運用，サイエンティフィック・システム研究会 SS 研ニュースレター選集，Vol.9, pp.23–40 (2009).
[4] A Project of the Internet2 Middleware Initiative: Shibboleth, available from ⟨http://shibboleth.internet2.edu/⟩ (accessed 2011-12-26).
[5] Online community for the Security Assertion Markup Language (SAML) OASIS Standard: SAML XML.org, available from ⟨http://saml.xml.org/⟩ (accessed 2011-12-26).
[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).
[7] 大谷 誠，渡辺健次，只木進一：仮想システム上でのディスクレスブートによる Opengate の運用，情報処理学会第 3 回インターネットと運用技術シンポジウム（IOTS2010）論文集，Vol.2010, No.14, pp.105–110 (2010).
[8] 藤村喬寿，田島浩一，大東俊博，西村浩二，相原玲二：大規模キャンパスネットワーク HINET2007 へのシングルサインオン機能の実装および評価，情報処理学会第 3 回インターネットと運用技術シンポジウム（IOTS2010）論文集，Vol.2010, No.15, pp.111–118 (2010).
[9] Krawczyk, H., Bellare, M. and Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, RFC 2104 (online), available from ⟨http://datatracker.ietf.org/doc/rfc2104/⟩ (1997).
[10] Eastlake, D. and Hansen, T.: US Secure Hash Algorithms (SHA and HMAC-SHA), RFC 4634 (online), available from ⟨http://datatracker.ietf.org/doc/rfc4634/⟩ (2006).
[11] 近堂 徹，田島浩一，岸場清悟，大東俊博，岩田則和，西村浩二，相原玲二：利用者認証機能を備えた大規模キャンパスネットワークの性能評価，情報処理学会第 1 回インターネットと運用技術シンポジウム（IOTS2008）論文集，Vol.2008, No.13, pp.121–128 (2008).

藤村 喬寿

2009 年山口県立大学生活科学部生活環境学科卒業．2011 年広島大学大学院総合科学研究科博士課程前期修了．修士（学術）．現在，西部電気工業株式会社．コンピュータネットワーク，ネットワークセキュリティに関する業務に従事．

西村 浩二 （正会員）

1989 年広島大学工学部第二類（電気系）卒業．1991 年同大学大学院工学研究科博士課程前期修了．全日空システム企画株式会社，広島大学総合情報処理センター助手，同大学情報メディア教育研究センター准教授を経て，現在，同教授．博士（工学）．コンピュータネットワーク，情報セキュリティに関する研究に従事．電子情報通信学会会員．

近堂 徹 （正会員）

2001 年広島大学工学部第二類（電気系）卒業．2006 年同大学大学院工学研究科博士課程後期修了．現在，広島大学情報メディア教育研究センター准教授．博士（工学）．コンピュータネットワーク，リアルタイムマルチメディア通信，QoS 保証技術に関する研究に従事．電子情報通信学会会員．

大東 俊博 （正会員）

2002 年徳島大学工学部知能情報工学科卒業．2004 年同大学大学院工学研究科博士前期課程修了．2008 年神戸大学大学院自然科学研究科博士課程後期課程修了．現在，広島大学情報メディア教育研究センター助教．博士（工学）．暗号理論，ネットワークセキュリティ，認証プロトコルに関する研究に従事．電子情報通信学会 SCIS20 周年記念賞受賞．電子情報通信学会会員．

田島 浩一 （正会員）

1994 年宮崎大学工学部電子工学科卒業．2000 年同大学大学院工学研究科博士課程後期修了．現在，広島大学情報メディア教育研究センター助教．博士（工学）．コンピュータネットワークの管理に関する研究に従事．電気学会会員．

相原 玲二 （正会員）

1981 年広島大学工学部第二類（電気系）卒業．1986 年同大学大学院博士課程後期修了．同大学助手，同大学集積化システム研究センター助教授を経て，現在，同大学情報メディア教育研究センター教授．工学博士．コンピュータネットワークに関する研究に従事．電子情報通信学会，IEEE Computer Society，IEEE Communications Society 各会員．