Vol.2014-IOT-27 No.5
Vol.2014-SPT-11 No.5
2014/10/9

岡山大学事務情報システムにおけるShibbolethとの連携を考慮した多要素認証の導入

河野 圭太[1,a)]　藤原 崇起[1]　稗田 隆[1]

概要：岡山大学では，2014 年 7 月に，事務情報システムを更新した．新システムでは，多要素認証システムが導入されており，仮想デスクトップの利用時には，IC カードと PIN コードによる認証が行われる．各種アプリケーションへのシングルサインオンも多要素認証システムで管理されており，重要なアプリケーションの利用時には，IC カードによる再認証が求められる．本報告では，新システムにおける多要素認証の導入について述べると共に，多要素認証システムと Shibboleth を連携させる際に発生した問題とその対策について述べる．

キーワード：多要素認証，Shibboleth，シングルサインオン，事務情報システム

Introduction of Multi-Factor Authentication Considering Cooperation with Shibboleth in Okayama University Administrative Information System

Keita Kawano[1,a)]　Takaoki Fujiwara[1]　Takashi Hieda[1]

Abstract: In Okayama University, we replaced our administrative information system in July 2014. The new system introduces a multi-factor authentication system. Users are to be authenticated with their IC card and PIN code when they use their virtual desktop. Single sign-on for some applications is also controlled using the multi-factor authentication system. Users are to be re-authenticated with their IC card when they use some important applications. This report describes an introduction of multi-factor authentication in the new system. A problem of the multi-factor authentication system emerging when it cooperates with Shibboleth and its countermeasure are also described.

Keywords: multi-factor authentication, Shibboleth, single sign-on, administrative information system

1. はじめに

岡山大学では，2014 年 7 月に，事務情報システムを更新した．新システムでは，約 800 台のシンクライアント端末が導入されており，作業端末に依存しない仮想デスクトップの提供による利便性の向上と，業務データの集中管理による安全性の強化が図られている．

また，新システムでは，DDS 社の多要素認証統合プラットフォームである EVE MA（および ID マネージャ）が導入されており，仮想デスクトップや業務アプリケーションの利用時に，要求される認証の強度に応じて，方式を組み合わせた認証が提供される [1]．仮想デスクトップの利用時には，IC カードと PIN コードによる認証が行われ，重要なアプリケーションの利用時には，IC カードによる再認証が求められる．これらの設定はサーバで集中的に管理されており，容易に変更できる．

EVE MA では，業務アプリケーションの認証画面を検知し，要求された組み合わせの認証を実施後，業務アプリケーションに対する通常の認証操作をエミュレートすることにより，業務アプリケーションを改変することなく，多

[1] 岡山大学
Okayama University, Okayama 700–8530, Japan
[a)] keita@okayama-u.ac.jp

要素での認証を実現する．そのため，既に他システムでシングルサインオンが実現されている場合，個別の業務アプリケーションに対する認証方式の組み合わせを制御できない．岡山大学でも，既に Shibboleth によるシングルサインオンが提供されているため，この問題への対処が求められた [2]．

本報告では，岡山大学事務情報システムにおける多要素認証の導入事例について紹介すると共に，Shibboleth を用いて認証連携している個々の業務アプリケーションで多要素認証を実現するために実施中の対策について述べる．

2. 事務情報システムの更新

本章では，まず，2.1 節において，更新後の事務情報システムの概要を述べる．また，2.2 節において，新システムにおける多要素認証の導入について述べた後，2.3 節において，多要素認証の導入に伴う問題について述べる．

2.1 概要

新システムは，約 800 台のシンクライアント端末と，学内外のクラウドサーバから構成されている．BCP を考慮し，一部の仮想サーバを学外のデータセンターで運用すると共に，各種サーバやデータのバックアップを別のデータセンターに保管している．

シンクライアント端末としては，HP 社の t510 が採用されており，VMware 社の Horizon View による仮想デスクトップが提供されている [3], [4]．利用者は，シンクライアント端末から各自の仮想デスクトップに接続し，業務を遂行する．利用者と仮想デスクトップとの紐付けはサーバで管理されており，利用者は訪問先の作業端末で自身の仮想デスクトップを呼び出せる．

ファイルサーバでは，初期値として，1 人 10GB の個人領域に加えて，1 人につき 10GB の部署共有領域を配分しており，シンプロビジョニングの活用状況に応じて，更なる配分量の増加を計画している．加えて，学内外関係者とのファイル交換には大容量ファイル受け渡しシステムを利用でき，USB メモリの交換やメールへの添付に頼らない安全な情報の共有を行える．

また，統合認証システムとの連携が行われ，ID・パスワードおよび利用者情報管理の共通化が図られている．仮想デスクトップには，クライアントエージェント型のシングルサインオンシステムが導入されており，各種 Web アプリケーションやクライアント・サーバ型のアプリケーションへのシングルサインオンを提供している．このシステムは業務アプリケーションの認証画面を検知し，通常の認証操作をエミュレートすることにより，シングルサインオンを提供する．エミュレート時に利用する認証情報が事前に登録されていない場合には，利用者によるオンサイトでの登録も可能である．

さらに，グループウェアとして，アイアット OEC 社の WaWaOffice が導入されており，メール利用や施設予約，スケジュール共有などに活用されている [5]．WaWaOffice をはじめとした幾つかの Web アプリケーションは，Shibboleth によるシングルサインオンで利用できる．

2.2 多要素認証の導入

シンクライアント端末へのログインや各種業務アプリケーションへのシングルサインオンは，DDS 社の多要素認証統合プラットフォームである EVE MA（および ID マネージャ）により管理されている [1]．EVE MA はクライアントエージェント型のシステムであり，業務アプリケーションを改変することなく，要求される認証の強度に応じて，方式を組み合わせた認証を提供できる．

EVE MA では，プラグインアーキテクチャの採用により，様々な方式を組み合わせた認証を提供できるが，岡山大学では，現在，統合 ID（岡大 ID）とパスワードによる認証，IC カードによる認証，PIN コードによる認証の 3 つを組み合わせて利用している．

シンクライアント端末へのログインや画面ロックからの復帰には，安全性を高めるため，IC カードによる認証と PIN コードによる認証の組み合わせを利用している．ただし，IC カードとして利用できる職員証の配布が着任から 2，3 週間遅れて実施されることを考慮し，岡大 ID とパスワードによる認証と PIN コードによる認証の組み合わせもオプションとして利用できるようにしている．このように，PIN コードがシステムの安全性を大きく左右するため，PIN コードによる認証には，定期的な変更の強制と，一定回数の試行失敗に対するロック制御が導入されている．

また，新システムでは，クライアントエージェント型のシングルサインオンシステムにより，各種業務システムへのシングルサインオンが実現されている．シングルサインオンの実現により利用者の利便性は向上するが，離籍時の画面ロックなどが徹底されていなければ，安全性の低下につながる可能性がある．そこで，シングルサインオンの際にも多要素認証との連携を実施し，重要な業務アプリケーションの利用時には，IC カードによる再認証を求めるようにしている．

2.3 多要素認証に伴う問題

多要素認証（シングルサインオン）の導入に伴い，幾つかの問題が発生している．

まず，対応するブラウザに関する問題がある．EVE MA（ID マネージャ）では，現在，IE 以外のブラウザをサポートしておらず，Firefox や Chrome 等のブラウザを用いて Web アプリケーションを利用する場合に，多要素による認証を実施できない．これらのブラウザを利用した場合，シングルサインオンも機能しないため，シングルサインオン

の安全性を高める現在の用途への影響は少ないが，業務アプリケーションに対してより強固な安全性を提供するためには，EVE MA のエミュレートによる認証操作のみを受け付けるよう，Web アプリケーション側も含めた改変が必要になると考えられる．

次に，利用者による複数 ID の利用に関する問題がある．利用者によっては，1 つの業務アプリケーションに対して，複数の ID を保有している場合がある．システム導入の際に，この点に対する考慮が不足しており，一部の業務アプリケーションにおいて，問題が露呈した．現在，対象の業務アプリケーションに対するシングルサインオンを無効化することにより，暫定的な対応をしているが，この問題は共有 ID の利用に関する問題とも深く関わるため，恒久的な対応が必要となっている．

また，システムの可用性に関する問題がある．EVE MA では，何らかの障害によりクライアントエージェントと EVE MA サーバの接続ができない場合に備えて，認証情報をクライアントエージェントに一時的にキャッシュする機能を有している．しかしながら，シンクライアント端末では，ポリシーにより，環境復元の機能が働いており，キャッシュされた認証情報も含めて加えられた変更が削除されるため，実質的に，EVE MA サーバとの接続ができない場合に，認証を実施できない．シンクライアント端末に導入している環境復元ソフトの設定で，認証情報をキャッシュする領域を保護の対象から外すことも考えられたが，安全性を優先し，シンクライアント端末の利用時には認証情報のキャッシュを行わないことにした．

最後に，既存のシングルサインオンシステムとの連携に関する問題がある．岡山大学では，Shibboleth を利用したシングルサインオンが既に確立されており，新システムで導入した業務アプリケーションの一部でも，Shibboleth を用いた認証連携を実施している．新システムで新たに導入したクライアントエージェント型のシングルサインオンシステムは多要素認証システムとの連携が密になされており，業務アプリケーションごとに多要素認証を設定することができるが，Shibboleth を用いて認証連携している業務アプリケーションに対しては，個別に多要素認証を設定することができない．この問題とその対策については，次章で詳しく述べる．

3. 多要素認証システムと Shibboleth の連携

本章では，まず，3.1 節において，Shibboleth を用いたシングルサインオンの概要について述べる．次に，3.2 節において，多要素認証システムと Shibboleth を連携させる際に発生する問題について述べる．最後に，3.3 節において，認証要求の内容を部分的に書き換えることにより，その問題を解決する対策について述べる．

3.1 Shibboleth によるシングルサインオン

Shibboleth は，OASIS で策定された SAML 標準に基づき，組織間のシングルサインオンを実現するための，オープンソースソフトウェアである [6], [7].

図 1 に，Shibboleth の動作原理を示す [*1][9]．図 1 は，利用者が，ある情報サービス（Service Provider：SP）（SP1）を利用するために，自組織の認証サーバ（Identity Provider：IdP）で認証を受けた後に，別の SP（SP2）を利用する様子を示している．

まず，(1) 利用者が SP1 のリソースにアクセスしようとすると，(2) 利用者からの認証要求は，利用者のブラウザを介して IdP へリダイレクトされる [*2]．(3) IdP では認証画面が表示され，利用者認証が行われる．IdP での認証に成功すると，(4) 認証応答が利用者のブラウザを介して SP1 にリダイレクトされ，(5) 利用者が SP1 のリソースにアクセスできるようになる．

引き続き，(6) 利用者が SP2 のリソースにアクセスしようとすると，(7) 利用者からの認証要求は，再び，利用者のブラウザを介して IdP へリダイレクトされる．利用者は既に IdP で認証済みであるため，認証画面は表示されず，(8) 認証応答が利用者のブラウザを介して SP2 にリダイレクトされる．その結果，(9) 利用者が SP2 のリソースにアクセスできるようになる．

3.2 多要素認証システムと Shibboleth の連携に伴う問題

岡山大学で導入した EVE MA では，業務アプリケーションの認証画面を検知し，通常の認証操作をエミュレートすることにより，多要素認証を提供する．前節で示したように，Shibboleth によるシングルサインオンが実現されている場合，認証画面が表示されるのは最初の SP 利用時のみ

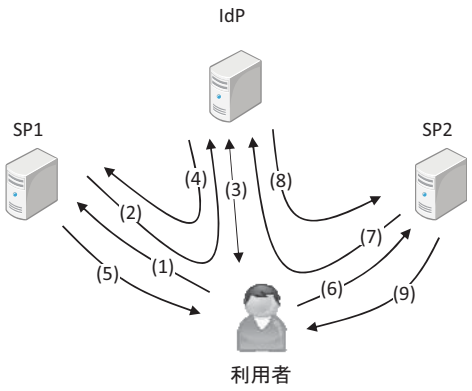

図 1 Shibboleth の動作原理.
Fig. 1 Operating principle of Shibboleth.

[*1] 本稿では，SAML V2.0 の Web Browser SSO Profile を前提とする [8].
[*2] 自組織の IdP を発見する手順が含まれる場合もある．

であるため，2 つ目以降の SP に対して，多要素認証を設定できない．Shibboleth によりシングルサインオンが実現されている全ての業務アプリケーションに対して，同一の設定をする際には問題はないが，個別の設定をする場合には，何らかの対策が必要となる．

SAML 標準では，認証要求に ForceAuthn という属性を含めることで再認証を要求できるが，これを活用した場合，事務情報システムの仮想デスクトップ以外から対象の業務アプリケーションを利用する場合にも再認証が発生してしまう [10]. また，EVE MA では認証セッションが管理されておらず，認証画面が表示される度に多要素認証が要求される．同一の組み合わせを利用する業務アプリケーションを連続して使う場合に，利便性の低下が問題となる．

また，SAML 標準では，認証要求の中で，利用する認証方式を指定できる [11]．事前に複数の認証方式（ログインハンドラ）を用意しておき，認証要求による指定を使い分けることで，個別の業務アプリケーションに対して，認証セッションを考慮した多要素認証を設定できる．しかしながら，単純にこれを適用した場合，先ほどと同様に，事務情報システムの仮想デスクトップ以外から対象の業務アプリケーションを利用する場合に問題が発生してしまう．

そこで，文献 [11] の方法を応用し，特定サブネットからの認証要求でのみ，認証方式の指定を書き換えることにした．

3.3 認証要求の書き換えによる対策

SAML 標準では，3.1 節における図 1 の手順（2）で生成される認証要求に，SP が許容できる認証方式（認証コンテキスト）のリストを含めることができる [11]．これらは，認証要求に含まれる RequestedAuthnContext として指定される [10].

文献 [11] では，Shibboleth IdP の実装において，これらが認証処理の状態を保持するための LoginContext に保存され，利用される点に着目し，適切なタイミングで LoginContext の内容（requestedAuthenticationMethods および authenticationMethodInformation）を書き換えることにより，実用的な運用レベルで Level of Assurance（LoA）を考慮した認証連携を実現する機能を開発した．本研究では，これを応用し，事務情報システムのサブネットからの認証要求に対して，IC カードによる再認証を必要とする場合に LoginContext の書き換えを実行し，新たな認証画面が表示されるようにした．

まず，既存のログインハンドラに加えて，**図 2**，**図 3** のような設定を追記することにより，IC カードによる再認証のためのログインハンドラ（サーブレット）を定義した．これにより，LoginContext 内の要求認証方式に関する情報（requestedAuthenticationMethods）を PasswordProtectedTransport2 に変更することで，既存の ID・パスワード認証によるログインハンドラと同等の認証画面が表示されるようになり，EVE MA による多要素認証を追加できる．

```
<!--  Username/password login handler -->
<ph:LoginHandler xsi:type="ph:UsernamePassword"
                jaasConfigurationLocation="file:/
//opt/shibboleth-idp/conf/login.config" authent
icationServletURL="/Authn/UserPassword2">
    <ph:AuthenticationMethod>PasswordProtectedT
ransport2</ph:AuthenticationMethod>
</ph:LoginHandler>
```

図 2 handler.xml の設定例.
Fig. 2 A configuration example of handler.xml.

```
<!-- Servlet for doing Username/Password authen
tication -->
<servlet>
    <servlet-name>UsernamePasswordAuthHandler2<
/servlet-name>
    <servlet-class>edu.internet2.middleware.shi
bboleth.idp.authn.provider.UsernamePasswordLogi
nServlet</servlet-class>
    <init-param> <param-name>authnMethod</param
-name> <param-value>PasswordProtectedTransport2
</param-value> </init-param>
    <load-on-startup>3</load-on-startup>
</servlet>

<servlet-mapping>
    <servlet-name>UsernamePasswordAuthHandler2<
/servlet-name>
    <url-pattern>/Authn/UserPassword2</url-patt
ern>
</servlet-mapping>
```

図 3 web.xml の設定例.
Fig. 3 A configuration example of web.xml.

Shibboleth IdP の実装では，このように複数のログインハンドラを定義することにより，それぞれに認証セッションが管理されたシングルサインオンが実現される．そのため，IC カードによる再認証を求める SP を短時間に連続して使う場合に，再認証の処理を省略できる．また，requestedAuthenticationMethods に含まれる他のログインハンドラによる認証結果を再利用し，認証処理を省略できるため，最初に再認証を求める SP を利用するために認証後，再認証を求めない SP を利用する場合にも，EVE MA による認証操作のエミュレートを省略できる．

なお，relying-party.xml の defaultAuthenticationMethod を PasswordProtectedTransport と定義しておくことで，事務情報システムの仮想デスクトップ以外からの認証要求

に RequestAuthnContext が含まれていない場合に，追加したログインハンドラが選択されないようにしている [*3]．

次に，LoginContext の書き換えにより，認証要求の変換，認証応答の逆変換を実施するためのフィルタを作成した．

変換処理のフローチャートを**図 4** に示す．変換処理は，事務情報システムのサブネットから IC カードによる再認証を求める SP への認証要求が発生した場合に実行される．具体的には，requestedAuthenticationMethods に PasswordProtectedTransport が含まれる場合に，その値を PasswordProtectedTransport2 に書き換える．また，requestedAuthenticationMethods が空の場合にも，PasswordProtectedTransport2 を追加する．

逆変換処理は，事務情報システムのサブネットへの認証応答が発生した場合に実行される．具体的には，PasswordProtectedTransport2 が使用され，認証要求時の requestedAuthenticationMethods が空，もしくは，requestedAuthenticationMethods に PasswordProtectedTransport2 が含まれず，PasswordProtectedTransport が含まれる場合に，LoginContext 内の使用認証方式に関する情報（authenticationMethodInformation）を書き換える．

これにより，SP から明示的な指定があった場合を除いて，既存の ID・パスワード認証を使用したように認証応答を返すことができる．最初に再認証を求める SP を利用するために認証後，再認証を求めない SP を利用する場合も想定し，この処理は，再認証を求めない SP への認証応答が発生した場合にも実行する．

なお，認証要求時に PasswordProtectedTransport も PasswordProtectedTransport2 も指定されていないにも関わらず，PasswordProtectedTransport2 が使用された場合（requestedAuthenticationMethods が空の場合は除く）には，認証要求とは異なる方式で認証されたことになるため，認証エラーとしている．

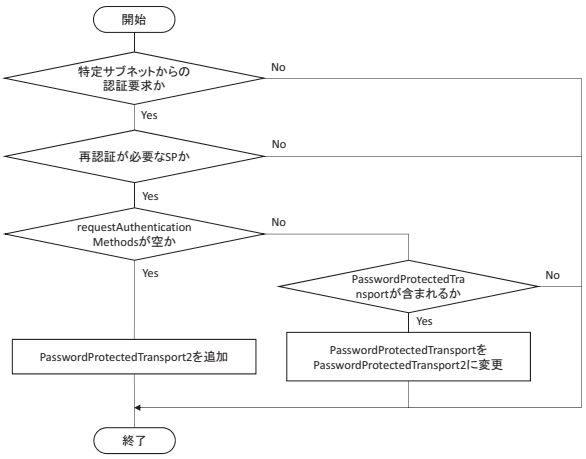

図 4 変換処理のフローチャート．
Fig. 4 A flowchart of conversion process.

[*3] 実際には，urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport のような形式で定義している．

これらの機能を有するフィルタを，web.xml に記載する url-pattern を/AuthnEngine および/profile/SAML2/-Redirect/SSO として，稼働中の IdP に組み込んだ．これにより，シングルサインオン時に IC カードによる再認証を求める SP を利用する際に，新たな認証画面が表示されることが確認できた．時間の都合上，最終的な確認はできていないが，この認証画面に対して EVE MA の設定を加えることにより，目的の動作が達成される予定である．

4. おわりに

本報告では，2014 年 7 月に更新した岡山大学事務情報システムにおける多要素認証の導入とそれに伴う問題について述べた．特に，既に他システムでシングルサインオンが実現されている場合に発生する問題を明らかにし，Shibboleth IdP に新たなフィルタを導入することにより，この問題を解決する対策について述べた．

今後は，新規フィルタを導入した Shibboleth IdP と EVE MA の連携に関する最終確認を含め，残された課題の検討を進める予定である．

謝辞 本研究の一部は JSPS 科研費 26330158 の助成を受けたものである．

参考文献

[1] DDS：EVE MA | DDS 製品情報サイト (online)，入手先 ⟨http://www.dds.co.jp/product/eve-ma/⟩ (2014.08.11).
[2] Shibboleth Consortium: Shibboleth (online), available from ⟨https://shibboleth.net/⟩ (2014.08.11).
[3] HP：HP シンクライアント ソリューション | 日本 HP (online)，入手先 ⟨http://www8.hp.com/jp/ja/thin-clients/t620.html⟩ (2014.08.11).
[4] VMware：VMware Horizon（with View）：仮想デスクトップとアプリケーションの配信 | VMware 日本 (online)，入手先 ⟨http://www.vmware.com/jp/products/horizon-view/⟩ (2014.08.11).
[5] アイアット OEC：情報共有にはまず機能をチェック|WaWaOffice (online)，入手先 ⟨http://www.wawaoffice.jp/product/groupware/⟩ (2014.08.11).
[6] Shibboleth Consortium: Shibboleth Consortium - What's Shibboleth (online), available from ⟨https://shibboleth.net/about/⟩ (2014.08.11).
[7] OASIS: OASIS Security Services (SAML) TC | OASIS (online), available from ⟨https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security⟩ (2014.08.11).
[8] Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R. and Maler, E.: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, saml-profiles-2.0-os (2005).
[9] Shibboleth Consortium: Shibboleth Consortium - How Shibboleth Works (online), available from ⟨https://shibboleth.net/about/basic.html⟩ (2014.08.11).
[10] Cantor, S., Kemp, J., Philpott, R. and Maler, E.: As-

sertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, saml-core-2.0-os (2005).
[11] 河野圭太，中村素典：Shibboleth IdP における LoA を考慮した認証方式グループ化機能の開発，情報処理学会研究報告，Vol.2014-IOT-26，No.2 (2014).