Vol.2013-IOT-22 No.10
2013/8/1

SAML連携を行うPAMに基づくSSO認証対応Webメールシステムの開発

大谷 誠[1,a)]　江藤 博文[1]　松原 義継[1]　只木 進一[1]

概要：
佐賀大学では，Shibboleth による SAML 認証を用いて，Web 型システムの統合基盤の構築を行ってきた．しかし，メールシステムが IMAPS プロトコルを利用しているため，Web インタフェースのシステムであっても，個別認証が必要であった．この問題を解決し利便性を向上させるため，SAML に対応可能な PAM モジュールを導入することで IMAPS 認証を SSO 対応とした．これにより，Web メールシステムを Shibboleth 認証に対応させることが可能となった．本稿では，この認証方法を解説するとともに，Web メールシステムへの実装を報告する．

キーワード：SSO 認証, Shibboleth, SAML, Web サービス, メール

Web-based mail system with SSO authentication through SAML supporting PAM

Makoto Otani[1,a)]　Hirofumi Eto[1]　Yoshitsugu Matsubara[1]　Shin-ichi Tadaki[1]

Abstract:
We, in Saga University, have been constructing a unified foundation of Web-based systems using SAML-based authentication mechanisms with Shibboleth. Web-based interfaces for e-mail accesses, however, have never been unified into the foundation, because the e-mail system has used the IMAPS protocol. For overcoming this problem and improving the usability of e-mail services, we introduced a PAM module compatible with SAML for IMAPS authentication, and we developed a Web-based interface for the e-mail system, which the users can use under Shibboleth authentication. We will report the method for SAML-based authentication and its implementation.

Keywords: Single Sign-On Authentication, Shibboleth, SAML, Web Service, Mail

1. はじめに

大学など組織内の情報サービスの提供を目的とした多種多様なシステムが，Web を用いる形で提供されることが多くなってきた．このような Web システムは用途ごとに構築される場合が多く，利用者が目的に応じてそれぞれの情報システムを利用することとなる．その際に，システム毎に利用認証が求められると不便である．よって，このような環境においては，一度の認証で多くの Web システムが利用できるシングルサインオン (SSO) 認証が導入されていることが望ましい．

佐賀大学では，Shibboleth を用いた SAML による認証連携により，学内の Web システムの SSO 認証対応を進めている．ネットワークの利用者認証システム (Opengate) を始めとし，教育関連の教務システムや e ラーニングシステム，図書システムや教職員が利用するグループウェアなど，多くの Web システムが Shibboleth を用いた SSO 認証に対応している．たとえば佐賀大学においては，ネットワークを利用する際に，まず始めに Opengate によってネット

[1] 佐賀大学総合情報基盤センター
Computer and Network Center, Saga University
[a)] otani@cc.saga-u.ac.jp

ワークの利用認証を行えば，学内の Web システムの多くを再認証なしにスムーズに利用することができる．また，佐賀大学は，国立情報学研究所が運営する学術認証フェデレーション (学認) [1] に参加しているため，学認に対応している電子ジャーナルや，他大学の提供する学認対応サービスなどを再認証なしで利用することができる．

この様に Web システムを Shibboleth による SSO 認証に対応させることでシステムの利便性の向上を図っているが，学内のすべての Web システムが SSO 認証に対応できている訳ではない．その理由には，コスト面によるものもあるが，その他の理由としてシステムの構成に起因しているものがある．例えば Web を用いてメールの読み書きを行う Web メールシステムなどである．

佐賀大学で利用している Shibboleth を用いた SAML 認証では，認証を必要とする際に IdP(Identity Provider) と呼ばれる認証サーバにおいて，Web による認証が行われる．この認証に成功すると Web システム (SP:ServiceProvider) へ利用者の属性情報 (サービス提供に必要となるユーザ情報) が提供される．この際，パスワード情報は IdP のみで一元管理され，セキュリティの観点からもその情報は Web システムには提供されない．このため，例えば佐賀大学のように Web メールシステムにおいて MRA(Mail Retrieval Agent) に IMAPS サーバを利用している場合，IMAPS 認証を行う際に別途パスワード情報が必要となってしまう．つまり，最も基本的なネットワークサービスであるメールへの Web インタフェースに SSO 認証でログインできないことになる．この問題を解決し利便性を向上させるために，MRA が稼働しているホストの認証機構に機能追加を行うことを検討した．つまり，PAM(Pluggable Authentication Module) に SAML 対応機能を導入することで IMAPS 認証を SSO 対応とした．この機構を用いることで Web システム及びメールサービスをほとんど変更することなく，SSO 対応の Web メールサービスを可能とすることができた．本稿ではこの機構の概要を述べるとともに，実装方法について報告する．

2. 佐賀大学における Web メールシステム

佐賀大学では，総合情報基盤センターが教職員や学生に対してメールアドレスを割り当てるとともに，メールサービスの運用を行っている．通常のメールクライアントソフトを用いた SMTP-AUTH, POP3S, IMAPS によるメールの送受信の他に，2000 年頃より，大学で独自に開発した Web メールシステム [2], [3], [4] を用いたサービスも提供している．この Web メールシステムは多言語対応・Java Servlet による高速動作など 2000 年当時としては高機能な Web メールシステムであった．現在は，この Web メールシステムをベースとした PHP による Web メールシステムを学内で運用している．

運用中の Web メールシステムは，MRA として IMAPS サーバを用いている．このサーバのソフトウェアは Dovecot[5] である．IMAPS によるメールの取得の際には，PAM を経由し佐賀大学で運用している統合認証システムの LDAP を使って認証が行われる．Web メールシステムにログインする際も，IMAPS 認証を用いている．IMAPS サーバに対する実際のアクセスは，PHP の IMAP 関数を使用する．

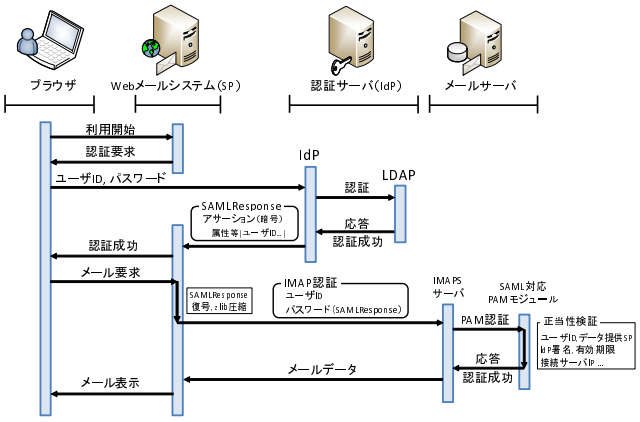

図 1　認証の流れ
Fig. 1　Authentication flow.

IMAPS 認証には通常，ユーザ ID とパスワードを必要とする．しかし，Web メールシステムに対するログインを SAML を用いた SSO 認証で行ったとしても，先に述べたように利用者のパスワード情報は IdP より取得できず，IMAPS 経由でメールを読むことはできない．よって，IMAP に対する認証の仕組みを変更する必要がある．そこで，SAML に対応した PAM 認証モジュールを導入し，IMAPS 認証においてこのモジュールを用いることで，Web メールシステムを SAML を用いた SSO 認証に対応させた．

3. SAML 対応 PAM モジュール

メールクライアントからの IMAPS を用いたアクセスでは，IMAPS は PAM を通じてローカル認証や LDAP 認証を行っている．PAM を SAML に対応させることができれば，Web メールシステムの SSO 対応が可能となる．そこで，SAML 対応 PAM モジュール crudesaml[6] を用いることとした．この crudesaml には，SAML アサーション (SAML の認証に関する情報) を検証する機能を備えた PAM モジュールと cyrus SASL[7] プラグインが含まれている．本システムにおいては，PAM モジュールの機能を利用した．

crudesaml では通常のパスワードの代わりに，IdP から SP(Web メールシステム) に認証成功後に渡される SAMLResponse を用いる．この SAMLResponse 内の SAML アサーションを検証することで認証の代わりとする．**図 1** に SAML 対応 PAM モジュールを使用した際の認証の流れを示す．

crudesaml を利用する場合，PAM の設定においては，crudesaml を利用する設定に変更を行うとともに，SAML ア

サーションの検証等に必要となる以下の情報も設定する必要がある．

- SAMLResponse を発行した IdP のメタデータ (idp)
- SP(Web メールシステム) の entityID(trusted_sp)
- ユーザ ID として使用する属性名 (userid)
- 接続を許可するクライアント IP アドレス (only_from)

これらの情報を基に，SAML アサーションが正当なものであるかを検証し，認証の判断を行う．この際には，信頼する IdP が発行した SAMLResponse であるかの署名検証，信頼する SP の受け取った SAMLResponse であるのチェックなどが行われる．その他にも，SAML アサーション内に含まれるユーザ ID の属性情報と IMAPS 認証のユーザ ID として渡された情報が同一であるといったことや，SAML アサーションが有効時間 (佐賀大学の例では 4 時間に設定) 内であるかといったことも含まれる．よって，IMAPS によって認証を行う際には，ユーザ ID としては別途属性情報として取得したユーザ ID を，パスワードとしては SAML アサーションとしてユーザ ID 情報を内部に含む有効期限内の SAMLResponse を渡す必要がある．

4. Web サーバの SAML 対応

先にも述べたが，SAML による SSO 認証に対応した Web メールシステム (SP) では，通常の IMAPS 認証と異なり，ユーザ ID には SAML アサーションの属性情報から取得したユーザ ID，パスワードには IdP より受け取った SAMLResponse を PAM に渡す必要がある．佐賀大学における SAML による SSO 認証においては，IdP, SP ともにこれまでミドルウェアとして Shibboleth を利用してきた．Shibboleth では，IdP での認証後に，SP に対しては SAML アサーション内に含まれている属性情報が，Apache の環境変数として提供される．Web サービスはこの環境変数を用いてサービスの認可判断を行うことができる．

SAML に対応した PAM モジュールを用いて認証を行う際は，SAMLResponse 自体が必要となる．しかし，通常の Shibboleth 環境では，この SAMLResponse を取得することができない．そこで，Apache モジュールである mod_mellon[8] を用いることとした．

mod_mellon は，Shibboleth と同様に環境変数より利用者の属性情報が取得できるとともに，PAM がパスワードとして代用する SAMLResponse も環境変数 (MELLON_SAML_RESPONSE) から取得できる．ユーザ ID も環境変数 (REMOTE_USER) より取得できる．この二つの情報を用いて IMAPS 認証を行う．

ただし，環境変数より取得した SAMLResponse 内に記述されている SAML アサーションの一部は，SP の公開鍵によって暗号化されている．そのため，このままではこの SAMLResponse を受け取った SP しか中身を検証することができない．一方，Web メールシステムにおいては IMAPS サーバの PAM モジュールで SAML アサーションを検証する必要がある．Web メールシステムである SP において秘密鍵を用いて暗号化部分を復号化し利用することとした．この動作は，IdP からの SAML アサーションを暗号化しない設定によっても回避できると考えられる．

mod_mellon の主な設定項目は以下の通りである．

- 環境変数 REMOTE_USER として利用する属性名 (IMAPS の場合はユーザ ID)
- SAMLResponse 利用 (環境変数として) の有無
- SP の秘密鍵と公開鍵
- SP メタデータ
- IdP の公開鍵
- IdP メタデータ

また，環境変数から受け取った SAMLResponse は，BASE64 によるエンコードが行われている．そこで SAML アサーションの復号化を行うために，BASE64 によるデコードを行う必要がある．そして SAML アサーションを復号化した後，IMAPS サーバにパスワードとして SAMLResponse を利用する際は，BASE64 によるエンコードの必要がある．また，この SAMLResponse は IMAPS のパスワードとして利用するには非常に長いため，BASE64 にエンコードするよりも前に zlib による圧縮を行う．SAML に対応した PAM のモジュールである crudesaml では，この zlib によって圧縮された SAMLResponse に対応している．

5. SSO 認証対応 Web メールシステム

5.1 システムの動作

以下に SAML による SSO 認証に対応した Web メールシステムの動作について述べる．

(1) メール利用者が Web メールシステムにアクセスする．
(2) 認証を行うために IdP にリダイレクトさせる．
(3) 利用者が IdP の認証ページ (**図 2**) にてユーザ ID とパスワードを入力する (すでに認証を行っていた場合は次の動作に進む)．
(4) 認証に成功した場合，IdP は SP である Web メールシステムにサービスに必要となる属性情報 (ユーザ ID 等) を提供する．これら属性情報や SAMLResponse 自体は，Web サーバの環境変数より取得される．
(5) SAMLResponse 内のアサーション情報の一部は暗号化されているため SP の秘密鍵を使って復号化したのち，SAMLResponse を再構築する．
(6) Web メールシステムは，属性情報から取得したユーザ ID と再構築した SAMLResponse をそれぞれ IMAPS 認証のユーザ ID とパスワードとし認証を行う．
(7) IMAPS サーバは，受け取ったユーザ ID とパスワード (SAMLResponse) を PAM の SAML 認証モジュールに渡し，そこで SAML アサーションの正当性の検証を行う．

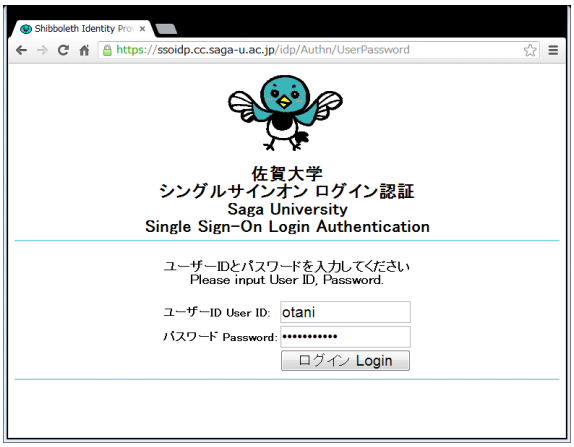

図 2　IdP 認証ページ
Fig. 2　IdP authentication page.

図 3　Web メールシステム
Fig. 3　Web mail system.

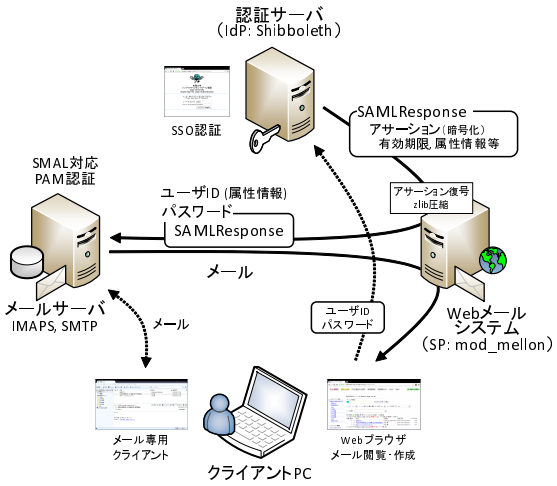

図 4　システム構成
Fig. 4　System architecture.

(8) 検証に成功した場合，認証の成功と判断し，ユーザの所有するメールスプールへのアクセスを許可する．

(9) Web メールシステム (**図 3**) は，受信しているメール内容の提示や，新規メール作成等の環境を提供する．

システム構成を**図 4** に示す．利用者から見た Web メールシステムの動作は，ユーザ ID とパスワードを IdP の認証画面で入力 (最初の認証の場合) する以外は，従来のシステムと同様である．よって利用者は，システムの変更を意識せずに Web メールシステムを利用できるとともに，SSO 認証の利便性を享受することができる．また，SAMLResponse 等が環境変数より取得できない場合は，従来通りにユーザ名とパスワードを Web インタフェースから送ることで，IMAPS が LDAP またはローカル認証を行うことができる．つまり，同じインタフェースで SSO 認証と従来の認証を併存させることができる．

表 1　IdP 環境
Table 1　IdP environment.

Web サーバ	Apache 2.2.14
SAML 対応	Shibboleth IdP 2.3.8
	apache-tomcat 6.0.36

表 2　SP 環境
Table 2　SP environment.

Web サーバ	Apache 2.2.5
SAML 対応	mod_mellon 0.6.1
	xmlseclibs 1.3.0 (アサーション復号化用)
PHP 関連	PHP 5.3.3
	c-client 2007f(PHP IMAP 関数)

表 3　メールサーバ環境
Table 3　Mail server environment.

IMAPS サーバ	IMAP Dovecot 2.1.5
SAML 対応	crudesaml 1.4

5.2　動作環境

表 1, **2**, **3** にそれぞれ SSO 認証に対応した Web メールシステムのソフトウェア構成を示す．以下に述べるように，従来のシステムに若干の変更を加えることで構成している．

IdP は，佐賀大学の SSO 認証対応の Web サービスで実運用に利用しているものであり，Web メールシステムである SP に新たに属性情報を提供するように設定追加したのみである．SP である Web メールシステムには，SAML 対応として Shibboleth ではなく mod_mellon，およびアサーション復号用に xmlseclibs と呼ばれるライブラリを使用したが，それ以外は従来の Web メールシステムと同じ環境である．メールサーバ環境については，SAML 対応の PAM モジュールを追加したのみであり，それぞれのシステムを大きく変更することなく SAML 対応が実現できた．

現在，上記の環境で，学生向けの Web メールシステムとして試験運用を行っているが安定して動作しており，Shibboleth によって構築されている他の SSO 対応の Web サービスとの連携も問題無く動作した．

6. 考察

6.1 Web メールシステムの SAML 対応

システムの基本的な認証動作としては，IdP から受け取った SAMLResponse を，Web メールシステムである SP が受け取り，SAML アサーションを復号化した後に，IMAPS サーバにパスワードとして渡すことにより，SAML 対応の PAM モジュールによって認証処理が行われる．よって，SAMLResponse を環境変数として受け取れる SP 環境と，SAML に対応した PAM のモジュールの導入を行った．それに加えて手を加えた部分がある．それは IMAPS サーバと，IMAPS サーバのクライアントとなる PHP(IMAP 関数) のパスワードのバッファサイズの調整である．

実際に取り扱う SAMLResponse は zlib によって圧縮が行われているが，それでも通常用いられるパスワード長 (数文字から十数文字程度) に比べ非常に長い．組織情報 (Organization) など直接認証に用いていない属性情報も含まれているが，試験運用を行った環境おいて，zlib で圧縮した状態での SAMLResponse のサイズは約 3.4KB であった．

IMAPS のサーバとして用いた Dovecot と PHP の IMAP 関数 (c-client) におけるパスワードのバッファサイズはともに 1KB(1024 文字) となっていた．パスワード長がバッファサイズを超えており，そのままではうまく認証できなかった．そこで，それぞれバッファサイズを 4KB となるようにソースコードを変更することで対応した．

このように，利用するサービスのサーバとクライアントによっては，ソフトウェアが設定するパスワードのバッファサイズが問題となり場合あり，別途その対応が必要となる場合がある．

6.2 SAML フォーマット

システムに用いた IdP(Shibboleth) と，PAM の SAML 対応モジュール (crudesaml) はアサーションの有効期限に関する時刻フォーマットに違いがあった．IdP から発行されるアサーションの有効期限はミリ秒まで記載されているのに対し，PAM の SAML 対応モジュールでは秒までしか想定されていなかった．このフォーマットの違いによって，アサーションの検証に失敗するため，crudesaml のソースコードの変更を行った．以下が Shibboleth の IdP より発行されたアサーションの時刻フォーマット例である．

- アサーションの有効期限の例 (Shibboleth IdP)

```
<saml2:Conditions
NotBefore="2013-06-30T06:23:45.413Z"
NotOnOrAfter="2013-06-30T10:23:45.413Z">
```

SAML 対応の実装によって，このように SAML のフォーマットに違いが発生する場合があるため，SAML 対応の際には，SAML のフォーマットや SAML のバージョン自体に対する注意が必要である．

6.3 他のシステムへの応用

今回利用した方式は，Web メールシステムの SSO 認証対応だけでなく，認証に PAM を用いるサービスと，Web インタフェースとの連携に広く用いることができると思われる．基本的に，PAM に SAML 対応モジュールを追加することで動作するため，サービス側のソフトウェアに大きな変更が発生しない．よって Web による SSO 認証と容易に連携することが可能となる．例えば，Web インタフェースを用いた SSH によるサーバのターミナルサービスや，サーバのリモート制御や設定変更, リモートデスクトップなどにも応用できると考えられる．ただし，第 6.1 節で示したように，利用するソフトウェアによっては，パスワードのバッファサイズの制限が SAMLResponse のサイズを想定していない場合があるので注意が必要である．

7. まとめ

近年，大学などで運用される情報サービスの多くは Web を用いて行われる様になってきたが，利用するサービス毎に利用認証が求められると不便である．佐賀大学では，Shibboleth を用いた SAML による認証連携により，学内の Web システムの SSO 認証対応を進めており，非常に多くの Web サービスを再認証なしにスムーズに利用できる環境が整いつつあった．しかし，佐賀大学で運用を行っていた Web メールシステムは，メールの取得に IMAPS サーバを利用しており，このサーバとの IMAPS 認証にユーザ ID とパスワードが必要であったため，SSO 認証対応できていなかった．

そこで，IMAPS 認証と連携可能な PAM に SAML 対応のモジュールを追加し，このモジュールが Shibboleth IdP と SAML 連携することで，Web メールシステムやメールサーバ自体に大きな変更を行うことなく，Web メールシステムの SSO 認証対応が可能となった．

参考文献

[1] 学術認証フェデレーション (学認), https://www.gakunin.jp/
[2] IMAP4 に対応した Web ベース電子メールクライアント WebMailer の開発: 渡辺健次, 竹田暁彦, 只木進一, 学術情報処理研究, Vol.4, pp.35-43 (2000)
[3] レスポンスに優れ多言語に対応した Web ベースメールシステムの開発: 渡辺 健次, 竹田 暁彦, 情報処理学会研究報告, 2002-DSM-26, pp.7-12 (2002)
[4] LDAP による情報管理機能を有するウェブメールソフトウェアの開発: 松原義継, 只木進一, 情報処理学会 学術情報処理研究, No.8, ISSN 1343-2915, pp.83-88 (2004)
[5] DOVECOT Secure IMAP server, http://www.dovecot.org/
[6] crudesaml, http://ftp.espci.fr/pub/crudesaml/
[7] Project Cyrus, http://cyrusimap.web.cmu.edu/
[8] mod_mellon - a SAML 2.0 Apache module https://code.google.com/p/modmellon/