機器間認証における SAML の適用と実装[1]

馬場　昭宏　　大沼　聡久　　近藤　誠一
三菱電機株式会社　情報技術総合研究所

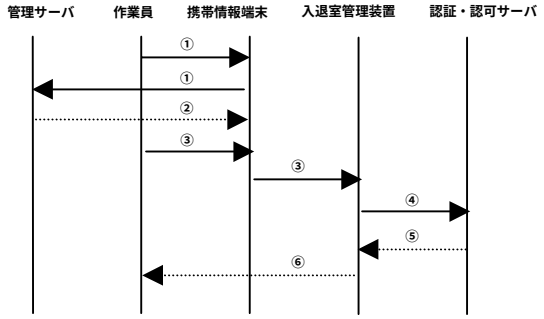
1　はじめに

IC カードや携帯端末を利用して認証を行い，サービスを提供するシステムが整備されてきている．たとえばビルなどの入退室管理装置や電子チケットを発行してコンサート等の入場に利用するようなサービス等である．しかしこれらの装置／サービスの互換性の欠如，紛失時の第三者によるなりすましが可能という課題がある．
一方，情報ネットワークシステムにおいては，認証・認可情報交換のプロトコルである SAML（ Security Assertion Markup Language ）[1][2]が標準化団体である OASIS で標準として批准されている．SAML では認証，属性，認可決定の 3 種類の情報を表明するアサーションと，アサーションを要求／回答するフォーマットを XML で規定している．また，このフォーマットを使用して SOAP によって通信するための方法，異なる認証システム間でアサーションを交換することでシングル・サインオンを実現する方法（Browser/artifact および Browser/POST プロファイル）を規定している．
SAML は一般に情報ネットワークシステム間でシングル・サインオンを実現するために使用されるが，我々は SAML の携帯情報端末，IC カード物理セキュリティ等機器間認証への適用に関して考察した． 本論文では，SAML を機器間認証に適用するメリット，適用例，実装するための技術課題および，実装方式について述べる．

2　SAML の機器間認証への適用

SAML を機器間認証に適用することで以下のようなメリットが得られる．①SAML は標準であるため，対応した機器間であれば様々な用途の認証に利用できる．②SAML のアサーションは短期間，一時的な認証・認可情報を対象としたものであるため，携帯情報端末等の機器を持ち運ぶ際に紛失しても第三者による不正利用（なりすまし）の被害を減少できる．③SAML のアサーションは認証情報に加え認可情報を持つことができるため，認可のロジックをアサーション発行側のみに実装し，受入側の構成を簡略化し得る．

SAML を機器間認証に適用する例として，ビル管理会社の作業員が複数のビルを訪問してメンテナンスを行うというシナリオを考える．訪問先のビルの入り口には入退室管理装置があり，ビル管理会社が発行したアサーションを提示することで訪問先のビルに入れるものとする．また，ビル管理会社では各作業員の作業予定を管理サーバで管理する．作業員が入室するまでのシーケンスを図 1 に示す．



①作業員は自社で携帯情報端末等の機器を使用して管理サーバにログイン.
②管理サーバはその日作業する予定があるすべての訪問先のビルに入るためのアサーションを作業員の携帯情報端末等の機器に送信.
③作業員は携帯情報端末等の機器を訪問先に持ち運び，入退室管理装置に Bluetooth 等の手段でアサーションを提示.
④入退室管理装置は認証・認可サーバにアサーションを送信.
⑤認証・認可サーバはアサーションを検証し，入退室管理装置に対して作業員の入室を許可.
⑥入退室管理装置は作業員を入室させる.

図 1　作業員が入室するまでのシーケンス

3　実装にあたっての課題

3.1　課題 1：記憶容量

情報ネットワークシステムではネットワーク経由でアサーションを交換するのに対し，機器間では携帯情報端末等の機器を経由して交換する．1 つのアサーションのサイズはアサーションの種類，署名の有無，署名の方法などにより異なるが，数キロバイト程度である．訪問先ごとのすべてのアサーションをあらかじめ携帯情報端末等の機器に記憶する方法とした場合，訪問先が多くなると記憶しておかなければならないアサーションの量が増える．このことは使用する機器が IC カード等記憶容量が小さいものである場

[1] Implementation of SAML for Machine Authentication
Akihiro Baba, Akihisa Onuma and Seiichi Kondo, Information Technology R&D Center, Mitsubishi Electric Corporation

合に問題となる．

3.2 課題 2：アサーション授受のインタフェース

認証システム間でシングル・サインオンを行う方法として SAML の仕様で規定されている 2 種類のプロファイルはいずれもアサーションを必要とするたびに発行し，2 サイト間の通信にネットワークを使用する．我々の方式では複数の対象に対して発行し別々のタイミングで使用するアサーションを携帯情報端末に入れて物理的に持ち運ぶため既存のプロファイルをそのままでは使用できない．そのためアサーションを携帯情報端末等の機器に保持し，使用するタイミングで必要なアサーションを選択して提示するための独自のインタフェースを規定する必要がある．

4 実装方式

4.1 構成

実装は図 2 のような構成とする．

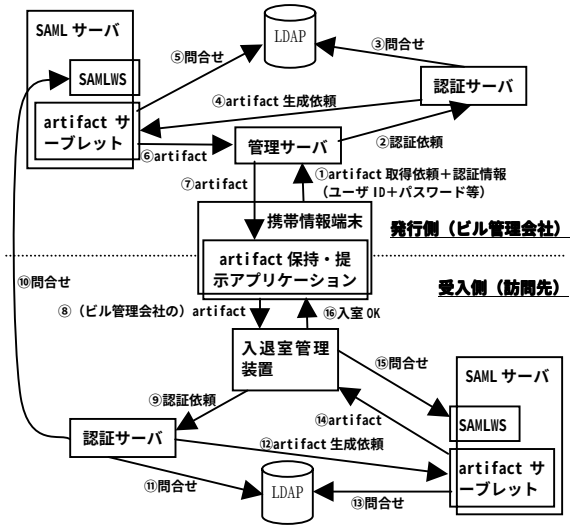


図 2 システム構成

ビル管理会社の管理サーバ，訪問先の入退室管理装置を認証システム（SAML サーバおよび認証サーバ）を利用するシステムと捉えるとビル管理会社，訪問先双方とも同一の構成である．認証サーバはユーザによって入力された認証情報（ユーザ ID＋パスワード等）に基づき認証を行う．SAML サーバは要求に応じてアサーションを含むレスポンスを返す．

4.2 課題 1 の解決方法

SAML サーバの artifact サーブレットは Browser/artifact プロファイルを実現するためのものである．Browser/artifact プロファイルではアサーションそのものを返さず，アサーションに 1:1 で対応する artifact と呼ばれるサイズの小さな情報を返し，artifact を受け取ったサーバが artifact を発行したサーバに対して受け取った artifact に対応するアサーションを要求する．artifact は本来は WEB ブラウザの URL サイズの制限を回避するためのものであるが，我々は課題 1 を解決するためにこれを使用する．
artifact の種類は 2 種類が規定されているが，サイズが固定されている（42 バイト＝TypeCode2 バイト＋SourceID20 バイト＋AssertionHandle20 バイト）ために保持可能な artifact の数を計算可能な type1 を採用する．
artifact を使用する場合，発行元への対応するアサーションの要求（図 2 の⑩の部分）が必須であるため，ネットワークで接続されている必要が生じる．これを避けるため，記憶容量が問題にならない場合はアサーションを直接携帯情報端末に保持することも選択可能とする．

4.3 課題 2 の解決方法

artifact を artifact サーブレットから受け取った管理サーバは，自身で artifact（に対応するアサーション）を消費せず，受け取った artifact と，その artifact を使用する訪問先の ID（以降 DestID と記述する）の対を携帯情報端末に送る．DestID は artifact の SourceID 同様の方法で生成し，サイズも同様に 20 バイトとする．携帯情報端末上の artifact 保持・提示アプリケーションがこの対を受け取り，保持する．
各訪問先に移動後，このアプリケーションが入退室管理装置から DestID を受け取り，DestID に対応した artifact を選択して提示する．以降のシーケンスは通常の Browser/artifact プロファイルに準ずる．

5 まとめ

本論文では SAML を機器間認証に適用するための技術課題および，実装方式について述べた．実際に携帯情報端末等の機器に実装し，評価を行うことが今後の課題である．

参考文献

[1] E. Maler et al. *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1*. OASIS, July 2003.
[2] E. Maler et al. *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1*. OASIS, July 2003.