M-072

Web サービスのセキュリティの研究 —WS-Security/SAML/XACML 適用の基礎実験—

Study on Web service security - Basic experiments on applying WS-Security, SAML and XACML -

武藤 裕介† 野口 健一郎‡
Yusuke Muto Kenichiro Noguchi

1．まえがき

これまで Web サービスのセキュリティ確保のために、SAML を利用した認証の実験[1]および XACML を利用したアクセス制御の実験[2]を行ってきた。さらに、WS-Security に準拠した暗号化機能を追加し、暗号化、認証、アクセス制御というセキュリティ要件を首尾一貫して持った Web サービスシステムを実装した。また、Web サービスのメッセージ通信を実現するためのツールである JAXM に対して、暗号化や署名というセキュリティ機能のための API を追加する拡張を行った。

2．背景

Web サービスのセキュリティの要件を図 1 に示す。

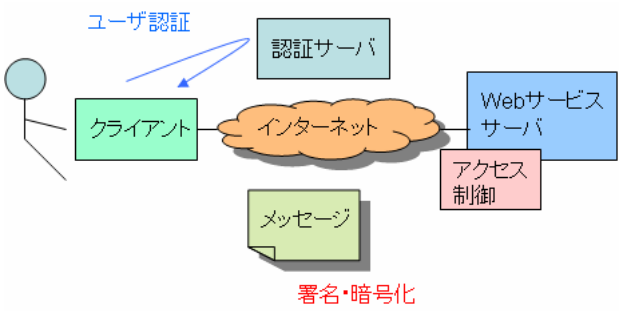

図 1. Web サービスのセキュリティの要件

セキュリティの要件に対応して次の規格がある。
①ユーザ認証のための認証情報の表現形式を定めた SAML(Security Assertion Markup Language)
②ユーザの実行可能操作の制限のためのアクセス制御に関わる情報の表現形式を定めた XACML (eXtensible Access Control Markup Language)
③メッセージの盗聴・改ざん防止のため、SOAP メッセージの暗号化・署名方式を定めた WS-Security [3]

3．研究課題

(1) Web サービスのセキュリティ要件を首尾一貫して持ったシステムの実装
(2) WS-Security に準拠した暗号化・復号化機能の実装
(3) SOAP 通信実装用ツールの拡張

† 神奈川大学理学部情報科学科（現在　日立エスケイソーシャルシステム株式会社）
‡ 神奈川大学理学部情報科学科

4．実装実験

4.1　システム構成と全体の流れ

本実験で実装したシステムの構成を図 2 に示す。
Web サービス技術を情報家電へ適用した。ただし、家電機器はコンピュータ上でシミュレートした。

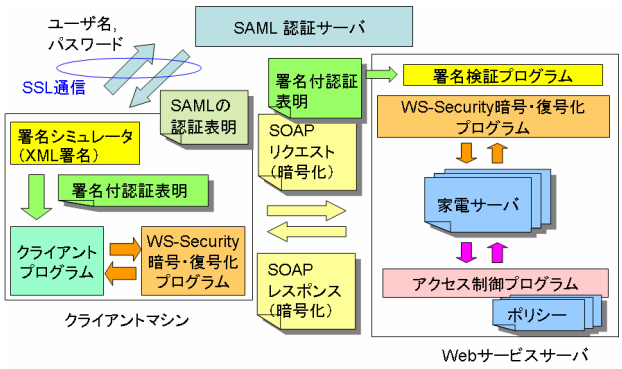

図 2. 本実験で実装したシステムの構成

システムの処理の流れを次に示す。
①ユーザはユーザ名、パスワードを入力し、認証サーバから認証表明を取得する。
②クライアント上の署名シミュレータが認証表明に認証サーバの個人鍵で署名する。（詳細後述）
③ユーザは署名付き認証表明を持って情報家電サービスにアクセスする。
④Web サービスサーバが認証表明の署名を検証する。認証が失敗ならばユーザにその旨が通知される。
⑤情報家電サービスはユーザ情報と要求操作に基づきアクセス権評価を行い、許可時は要求された操作が実行され、不許可時はユーザにその旨が通知される。
⑥ユーザは署名付き認証表明を使って別の情報家電サービスにアクセスできる（シングル・サインオン）。

4.2　WS-Security 暗号化・復号化機能の実装

WS-Security に従って SOAP メッセージを暗号化、および復号化する機能を実装した。暗号化された SOAP リクエストの例を図 3 に示す。
・暗号化対象は SOAP メッセージの Body 要素とした。クライアントおよび Web サービスサーバが送信したいデータは全て Body 要素の中に含めた。
・Body 要素の暗号化に処理時間が短い共通鍵暗号を用いることとし、TripleDES を用いた。

・共通鍵をクライアントと Web サービスサーバの間で安全に交換するために共通鍵を公開鍵暗号で暗号化した。

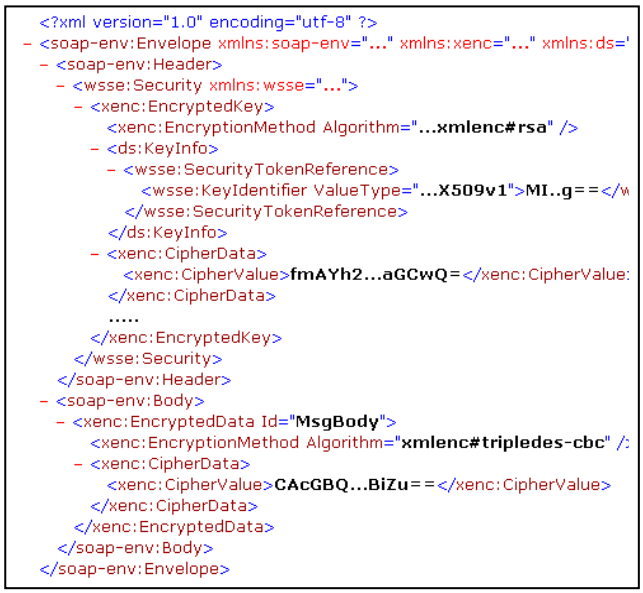

図 3. 暗号化された SOAP リクエストの例

4.3 Web サービスサーバによる認証情報の確認

認証情報が正当であるかどうかを Web サービスサーバが確認するために、認証表明に認証サーバの個人鍵で署名を付ける機能を実装した。

・署名文書の形式は、署名対象の Assertion 要素と XML 署名規格（署名情報を XML で記述するための規格）で規定される Signature 要素を、SignedAssertion 要素の中に含めるようにした。

図 4. 署名された認証表明の例

・Web サービスサーバ上に、認証サーバの公開鍵で認証表明の署名を検証する機能を実装した。

・認証サーバには既存のツールを用いたため、それへの署名付加機能の実装が困難なので、クライアント上に実装しシミュレーションした。

署名された認証表明の例を図 4 に示す。

4.4 XACML によるアクセス制御機能の実装

アクセス制御機能は Sun Microsystems が提供する XACML 実装用 API である Sunxacml-1.2 を用いて Web サービスサーバ上に実装した。主体に Role 属性を持たせ、きめ細かいアクセス制御を実現した。なお、ポリシーは Web サービスサーバ上に配置した。

4.5 SOAP 通信実装用ツール(JAXM)の拡張

JAXM では SOAP メッセージを SOAPMessage クラスとして表現する。SOAPMessage オブジェクトを操作して暗号化・復号化を行う際に必要な API を新たに実装した。

①要素の内容を文字列として取り出すメソッド

入力要素の下位の階層を再帰的に探索し、子要素の内容を文字列として順に追加していく。

②要素の任意の子孫を取得するメソッド

①と同様に下位の階層を再帰的に探索し、目的のタグ名を持つ要素を見つけたら、それを返す。

5. 評価

(1) 暗号化、認証、アクセス制御というセキュリティ要件を首尾一貫して持った Web サービスシステムを実装できた。

(2) SOAP 通信実装用ツール(JAXM)の拡張により、SOAP メッセージの暗号化と署名処理の実装が容易になった。

6. 今後の課題

(1) 署名付加プログラムを認証サーバ上に設置

(2) 実行可能な操作をユーザに通知する機能を追加

(3) XACML のポリシー作成・編集機能の追加

(4) 公開鍵の妥当性を保証する認証局の設置

参考文献

[1] 中尾 一、野口 健一郎、門脇 吉彦：SAML を利用した Web サービスの認証方式の検討、FIT（情報科学技術フォーラム）2004.

[2] 江川貴彦、野口 健一郎：Web サービスのセキュリティの研究－XACML を用いたアクセス制御の基礎実験、FIT (情報科学技術フォーラム) 2005.

[3] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification, 2006.

[4] 丸山宏：「XML と Web サービスのセキュリティ―XML デジタル署名と暗号化」共立出版、2004.