Science Journal of Kanagawa University **16**：81-82 (2005)

■報告書■　2004 年度神奈川大学総合理学研究所助成共同研究

ウェブサービスのセキュリティの研究

野口健一郎 [1,3]　門脇吉彦 [2]

Study on Web Service Security

Kenichiro Noguchi[1] and Yoshihiko Kadowaki[2]

[1] Department of Computer and Information Science, Faculty of Science, Kanagawa University, Hiratsuka-City, Kanagawa 259-1293, Japan
[2] eSEC, Yamato-City, Kanagawa 242-0002, Japan
[3] To whom correspondence should be addressed. Email: noguchi@info.kanagawa-u.ac.jp

Abstract: We studied the newly standardized security technologies for Web Services, SAML (Security Assertion Markup Language), which is for authentication, and XACML (XML Access Control Markup Language), which is for access control. We applied these technologies in an experimental system and confirmed that these technologies, combined together, can realize secure Web Services.
Keywords:　security, web services, SAML, XACML

序論

SAML とは、XML で記述された認証情報をやり取りするための仕様である。Web サービスにおいては SOAP メッセージ等に、SAML で記述された認証情報が挿入され、利用される。また XACML とは、XML 文書に対してアクセス権を設定するための仕様である。

まず、情報家電を Web サービス技術を用いて遠隔操作する実験システムに、SAML による認証機能を追加する実験を行った[1)]。図 1 に示す構成を取ることで、SAML によるユーザ認証がうまく行くことを確かめた。

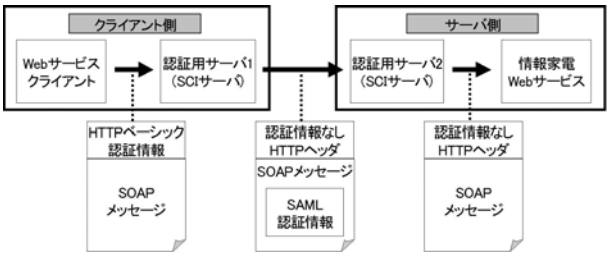

図 1.　SAML を利用した認証の概要.

実際の運用では、認証対象のユーザの管理が必要になる。そこで、Web サービス技術と SAML を利用して、認証対象のユーザの管理を遠隔地から行う方式を開発した。その概要を図 2 に示す。

次に、認証後のユーザに対して、アクセス制御を

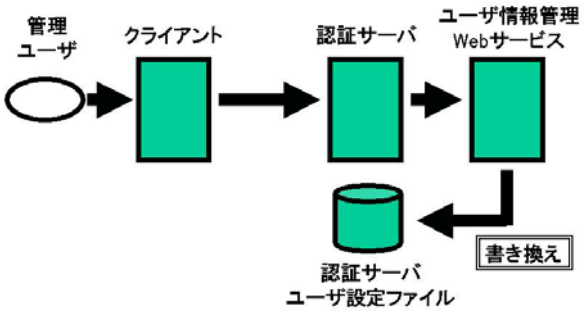

図 2.　認証対象ユーザの管理方式の概要.

行う実験を行った。図 3 にシステムの概要を示す。クライアントから①,②,③の順で、Web サービスサーバにアクセスする。

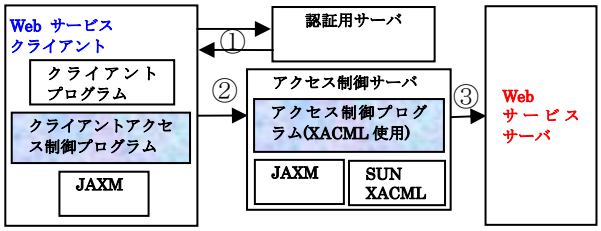

図 3.　XACML を用いたアクセス制御の概要.

サーバのアクセス制御プログラムの構成を図 4 に示す。XACML を用いてアクセス制御を実現し、実

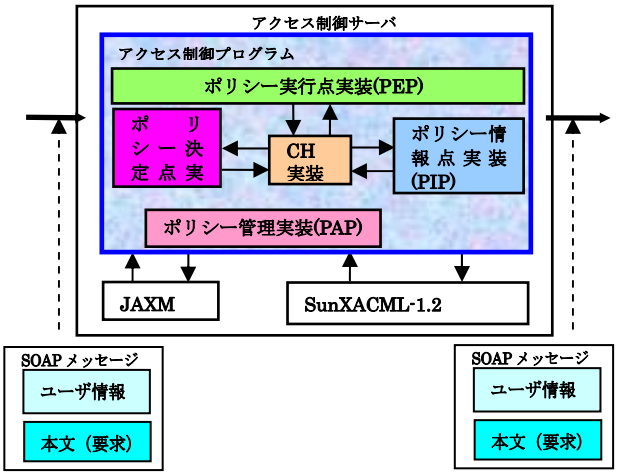

図 4. アクセス制御プログラムの構成.

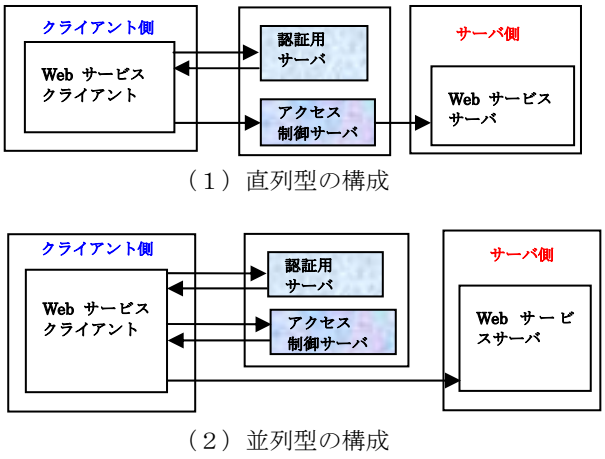

図 5. 認証とアクセス制御を組み合せた構成.

際にアクセス制御が行えることを確かめた。

以上の二つの実験をベースにこれらを組み合わせた構成での実験を行った。構成を図 5 に示す。（1）は Web サービスのクライアントとサーバ間にアクセス制御サーバを直列に配置する構成である。（2）はアクセス制御サーバによるチェックを行った後に、クライアントからサーバにアクセスする方式である。実験結果からは、後者のほうが、より融通が利き、安全性を確保しやすい方式だと考える。

今後の課題としては、図 6（2）の構成において、Web サービスサーバがアクセス制御情報のチェックを行うためにアクセス制御サーバとの間にインタフェースを持たせることなどがある。

なお、本実験において、認証用サーバには米国 Quadrasis 社の SOAP Content Inspector (SCI)を利用した。また XACML による制御を実現するために Sun Microsystems 社が提供しているパッケージである SunXACML-1.2 を利用した。

文献

1) 中尾 一, 野口 健一郎, 門脇 吉彦 (2004) 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.* pp.267-268.