7R-1

ＳＡＭＬにおけるXML処理効率向上の提案

津田　斎志†　　辻　秀一‡

東海大学大学院工学研究科†　東海大学情報メディア学科‡

１．はじめに

IT 産業の活発化により Web サービスが進展するに従って、セキュリティに関するユーザ認証だけでなく属性やアクセス権限を一元管理する SSO(Single Sign On)を実現する SAML(Security Assertion Markup Language)が注目されてきている。現在 SAML は社会に適用されていないが、実験段階にまで来ており、今後のユビキタス社会に向け必要とされる技術となる。本研究では、具体例として SAML を利用したシステムを用い、その運営の際に生ずる XML での暗号処理負荷といった情報処理負荷問題の解決に向けて、処理効率化を図るため SAX と DOM を使用し互いに XML データ処理性能を比較検討し、社会での適用に向けての確かな方式策定と実験を行った。

２．背景

２．１SAMLモデル

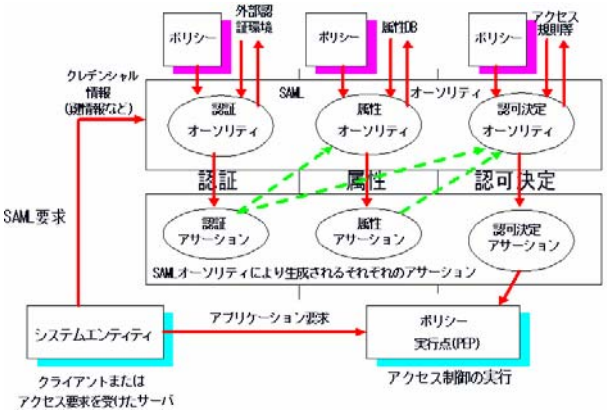

図１　SAML のモデル

SAML とはセキュリティ情報交換のための XML ベースのフレームワークであり、SAML は要求と応答のプロトコルと応答に含まれるアサーションの構文仕様を定めたものである。このセキュリティ情報は対象とする主体（人またはコンピュータ）のあるセキュリティドメインにおける認証情報や属性情報や認可情報をアサーション形式で表現する。SAML オーソリティには以下の項目がある。

・認証オーソリティは認証情報の再利用を可能にする認証アサーションを提供。

・認証オーソリティは認証情報の再利用を可能にする認証アサーションを提供。

・属性オーソリティはポリシーに定めた資格や役職などの属性アサーションを提供。

・認可決定オーソリティはポリシーで定めた規則に従った認可決定アサーションを提供。

リソースへのアクセスを要求するシステムエンティティはオーソリティからアサーションの要求を受け、ポリシーを実行するアプリケーション PEP に渡し要求を実行する。それは以下の３つである。

(1)本人性を認証し、指定した Web サイトにアクセスさせる。

(2)本人の資格属性によって特定のページにアクセスを許可する。

(3)本人の認可権限によって特定のリソースにアクセス(読み、書き、実行など)させる。

図に示した３つの SAML オーソリティは必ず必要では無い。SSO を実現するだけなら認証オーソリティのみで良い。だが、属性や認可権限を細かく制御するためには、認証オーソリティの認証アサーションを属性オーソリティやポリシー決定点に提示し認可決定のアサーションを受ける必要がある。この柔軟性が SAML 特有の長所である。

２．２ＸＭＬの情報処理負荷

SAML を利用する状況下において複数のサービスを次々に呼び出し、ビジネスプロセスを実行させる場合、メッセージ送受信ごとに大きな負荷が発生する。テキストデータである XML をアプリケーション間の共通データフォーマットに採用すると、送受信の際にアプリケーション側で XML を解析するオーバーヘッドが発生し、サーバ・アプリケーションの負荷を増大させる。また、XML のセキュリティには暗号化、電子署名と認証、XML スキーマ検証等が必要とされているため、メッセージの送受信時には、非常に負荷の大きいセキュリティ処理をしなければならないという問題がある。これらの問題の解決を図れば負荷によるパフォーマンスの低下を防ぐことが出来ると考えられる。

３．提案システム

SAML を用いた web サービスを実装する際、XML の処理の負荷を最小限に抑えたい。

外部ネットワークの送受信においてアプリケーション側で XML データを解析する際、または、セキュリティ処理の際、発生するオーバーヘッドによって生じたサーバ・アプリケーションの負荷の増加を防ぐため、新たに変換・セキュリティ処理専用サーバを作成する。なお、それはアプリケー

Propoasal of the XML processing efficiency improvement in SAMLformation

†MasashiTsuda

Graduate School of Engineering,Tokai University

‡Hidekazu Tsuji

School of Information Technology and Electronics,Tokai University

ション データから XML への変換処理が、データがアプリケーション境界を越える直前に実行するものとして設置する。この事により、オーバーヘッドの大きい XML の解析、セキュリティ処理、ルーティングやデータ変換などの処理を新設したサーバに負担させ、Web サービスを行ない複数のデータ処理を行なうアプリケーション側の負荷を減少させることが可能になる。また、今回処理効率化を図るため SAX と DOM を使用し互いに XML データ処理性能を比較検討した。

３．１システム構成

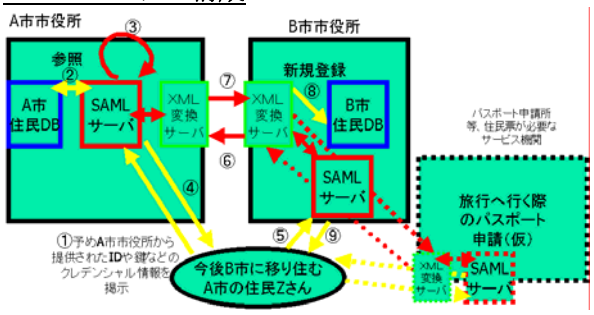

図２． SAML を使用した住民票移動の際の登録システム

図２では SAML を利用した住民票移動の際の登録を想定している。提案システムを下に手順を示す。①利用者は今まで住んでいた A 市役所（以下、市）に鍵などのクレデンシャル情報を掲示する。②A 市はあらかじめ登録された住民 DB で利用者の本人確認を行う。③確認後、認められたら認証アサーションを発行し保管する。④A 市はアーティファクト提供と共に利用者に移動先の市役所にアクセスするよう求める。⑤利用者は B 市へアクセスし B 市にアーティファクトを提示⑥B 市は A 市からそれを発行されたことを確認するため SAML 要求をする。⑦B 市が利用者のアーティファクトが本物と確認し、かつ A 市にあった利用者の認証情報を得れば⑧B 市は B 市住民 DB に新規で利用者の登録を済ませる。⑨B 市は利用者に住民登録が出来たという通知をする。なお、市役所同士のネットワークのみ XML 通信で行い、SAML サーバ間の通信暗号化やセキュリティ処理は必ず先に XML 変換用サーバを経由して行われるものとした。また、SAML の特性を生かし、必要があれば、両市役所の背後に PKI 機関の設置や住民票が必要なサービス機関なども契約を前提に自由に介入できる方式となっている。

３．２DOMとSAXの処理の比較

本研究では Java 開発環境として Sun MicroSystems 社の JDK を使用し、Java 言語を用い XML 言語の操作やタグ変換が出来る DOM や SAX を使用する。なお XML パーサとしては SourceForge 社の BENCHMARK を使用することで DOM と SAX 各々で一定の XML 文字列あたりの暗号変換に掛かる時間を計測し、比較検討を行なう。

４．評価

今回 Excel のグラフで結果を出力表示した。DOM では XML 文書全体を読み込んでからまとめて構造化するため、読み込み効率が悪くなり時間が掛かり、一方 SAX は逐次処理を行ない、DOM より早く処理を開始することができるが、DOM と比べ構造の操作性が劣るため、データ量が多い場合、文書の一部分の処理することがあれば、全体的に見れば DOM に比べ処理に時間がかかる事が確認できた。このことから、処理する XML データが多い場合は DOM を採用し、少ない場合は SAX を採用することで処理効率を上げることができる。

５．考察

本提案では SAML を Web サービスで利用する際、以下の利点が生じる。

(1)サービスを受ける側の利点として、住民票を登録する手続きの際、事前にただ一つの市役所に認証情報を登録しておくだけで済むので、次回の移動先に対する手続きの手間が省ける。

(2)サービス提供者側の利点として、B 市市役所無駄な属性情報を住民から取得する必要が無い。

(3)新たに XML 処理変換用サーバを設置する事で情報処理の際に生ずる負荷を減少させ、処理する XML データが長い場合は DOM を採用し、短い場合は SAX を採用することで SAML を利用したシステム全体の処理効率の向上させることが可能となる。

６.おわりに

本研究では、処理効率向上のための実験を行い、提案の有効性を検証した。処理する XML データが多い場合は DOM を採用し、少ない場合は SAX を採用するのであるが、今後の課題として、グラフで交差するポイントを境目に、DOM と SAX を切り替えることでさらに処理効率向上を図ることが可能になる事が明らかになった。

SAML を実際に運営させるためのシステム案がいまだ乏しく、電子政府や民間の電子商取引にどう適用させるかの検討が今後も必要である。XML ベースの SAML の課題としては、情報処理の負荷が問題となり、今現在、負荷はかかるがセキュリティを優先した標準技術を守るか、負荷処理解決のためのパフォーマンスを優先させるかのジレンマや運用管理の複雑化をどう解決していくかが課題になると考えられる。

７．参考文献

[1] 経済産業省調査,「ＳＡＭＬ利用検討報告書”電子商取引推進協議会」mar,2004

[2] 金子俊夫・蒲生良治,CQ 出版社:「Open Design No.36」feb,2000

[3]OASIS,http://www.oasis-open.org/specs/index.php#samlv2.0