XML セキュリティツール/製品調査報告書

2010 年 03 月 03 日
XML コンソーシアム
セキュリティ部会

目次

＜利用条件＞

本書は、本書に記載した要件･技術･方式に関する内容が変更されないこと、および出典を明示いただくことを前提に、無償でその全部または一部を複製、翻案、翻訳、転記、引用、公衆送信等して利用できます。なお、全体を複製、翻案、翻訳された場合は、本書にある著作権表示および利用条件を明示してください。

本書の著作権者は、本書の記載内容に関して、その正確性、商品性、利用目的への適合性等に関して保証するものではなく、特許権、著作権、その他の権利を侵害していないことを保証するものでもありません。本書の利用により生じた損害について、本書の著作権者は、法律上のいかなる責任も負いません。

1. 概要

XML コンソーシアム セキュリティ部会では、XML のセキュリティに関連するツール/製品の調査を行った。

調査メンバー (氏名五十音順):

- 大沼啓希 (日本アイ・ビー・エム株式会社)
- 中山弘二郎 (株式会社日立製作所)
- 林正樹 (富士通株式会社)
- 松永豊 (東京エレクトロン デバイス株式会社)
- 宮地直人 (有限会社ラング・エッジ)

1.1. 調査の目的と用途

当調査は、これから XML をベースにしたシステム開発を検討されるエンドユーザーおよび開発者に、XML セキュリティ技術実装のための基本的技術情報の一環として供することを目的としている。

1.2. 調査活動期間と経過

活動期間: 2008 年 10 月～2009 年 12 月

2008 年 10 月 セキュリティ部会で調査活動の検討開始

2008 年 11 月 13 日 運営委員会にて活動承認

2008 年 11 月 19 日～2009 年 12 月 19 日 セキュリティ部会で情報募集の具体案作成

2008 年 12 月 22 日～2009 年 04 月 01 日 情報募集について理事会審議

2009 年 04 月 01 日～2009 年 04 月 24 日 情報募集

2009 年 05 月 07 日 理事会より情報募集の期間と方法変更指示

2009 年 05 月 13 日～2009 年 06 月 30 日 再度情報募集

2009 年 11 月 報告書草稿を作成し、情報提供各社に内容確認

2009 年 12 月 情報提供各社からの指摘事項を反映し、報告書を完成

本報告書の内容は、基本的に 2009 年 04 月 01 日から 2009 年 06 月 30 日の情報募集において提供された情報をもとに作成している。 ただし、2009 年 11 月に情報提供各社に内容確認を依頼した際に指摘された点を加筆している。 従って、情報提供時期が異なる内容が含まれている。 また、調査後に製品の機能強化などが行われている場合もある。 最新の提供内容については、情報提供各社に確認されたい。

1.3. 調査対象製品分野

以下の各機能を提供するツールと製品で、日本で利用可能なもの。

- XML 暗号、XML 電子署名、WS-Security
- XML ベースの長期署名
- XML/SOAP ファイアウォール

1.4. 調査方法

- 公開情報の収集 – 仕様や無償提供されているツールについて、主にインターネットでの公開情報を収集した。
- 情報募集による情報収集 – 商用の製品について、開発元あるいは提供元からの情報提供を呼びかけ、情報を収集した。

1.5. 情報収集製品リスト

1.5.1. XML 暗号、XML 電子署名、WS-Security

1.5.1.1 アプリケーション・サーバー型およびライブラリ型

- IBM WebSphere Application Server
- 日本オラクル株式会社 Oracle Security Developer Tools 10g Release 3 (10.1.3)
- 日本オラクル株式会社 Oracle WebLogic Server
- 日本電気株式会社 SecureWare/電子署名開発キット
- 株式会社日立製作所 uCosminexus Application Server
- 富士通株式会社 Interstage Application Server

1.5.1.2 ゲートウェイ型

- IBM WebSphere DataPower SOA アプライアンス XML セキュリティーゲートウェイ
- 日本オラクル株式会社 Oracle Web Services Manager
- 日本セーフネット株式会社 Luna XML

1.5.2. XML ベースの長期署名

- セイコーインスツル株式会社 長期署名システム「NiXAdES」
- 日本電気株式会社 PKI サーバ/Carassuit 原本保管サーバ
- 有限会社ラング･エッジ XML 長期署名 Le-XAdES Library

1.5.3. XML/SOAP ファイアウォール

- IBM WebSphere DataPower SOA アプライアンス XML セキュリティーゲートウェイ
- Imperva Inc. SecureSphere Web Application Firewall

2. 調査対象分野の解説

本章では、調査対象とした製品分野がそれぞれどういうものか、解説を行っている。 本章の内容は、公開されている情報と調査メンバーの知見をもとに執筆した。

2.1. XML 暗号、XML 電子署名、WS-Security

2.1.1. XML 暗号

XML 暗号（XML Encryption Syntax and Processing）は、W3C の XML Encryption WG によって策定された仕様であり、2002 年に W3C 勧告となっている[1]。
XML 暗号では、既存の暗号技術を利用し、暗号化に関する情報（暗号化した結果のデータや復号に必要となる鍵の情報など、以下「暗号情報」と書く）を XML 形式で記述する方法を規定している。XML 暗号では、任意の形式のデータに対する暗号化をサポートしているが、XML データに対する暗号化の際に利用されることが多い。XML データに対する暗号化に XML 暗号を利用する場合、次のような利点がある。

- XMLデータの一部分に対する暗号化（部分暗号）が可能である。部分暗号を利用することで、例えば、XMLデータ内のうち秘匿性が求められる部分だけを暗号化するといった、高度な暗号処理が実現できる。
- 暗号対象のデータや暗号情報が全てXML形式であるため、処理が行いやすい。例えば、暗号化されたデータと復号に必要となる鍵情報とを1つのXMLデータ内に格納するといったことが容易である

2.1.2. XML 電子署名

XML 署名（XML Signature Syntax and Processing）は、W3C と IETF の合同ワーキンググループである XML Signature WG によって策定された仕様である。XML 署名は 2002 年に W3C 勧告および RFC3275 となり、2008 年には XML 署名(Second Edition) が W3C 勧告となっている[2]。
XML 署名では、既存の署名技術を利用し、署名に関する情報（署名した結果である署名値や署名検証に必要となる鍵の情報など、以下「署名情報」と書く）を XML 形式で記述する方法を規定している。XML 署名は、任意の形式のデータに対する署名をサポートしているが、XML データに対する署名の際に用いられることが多い。XML データに対する署名に XML 署名を利用する場合、次のような利点がある。

- XML データの一部分に対する署名（部分署名）が可能である。部分署名を利用することで、例えば、XML データ内のうち、変更される可能性のある部分は署名対象から外し、変更しない（してはいけない）部分にのみ署名を行うといった、高度な署名処理が実現できる。

- 署名対象のデータと署名情報のデータが共に XML 形式であるため、処理が行いやすい。例えば、署名対象の XML データと署名情報とを 1 つの XML データ内に格納するといったことが容易である。

しかしながら、XML データを署名する場合には、考慮するべき点もある。
それは、XML データのタグ情報に空白文字(<xxx >)が入ったり、空要素が省略(<xxx/>)されたりなど、XML 文書としては同一であっても、署名情報が変わってしまう点である。この問題を解決するために、XML データの署名をする前に、XML の正規化を行う必要があり、2001 年に W3C で勧告(Canonical XML)されている。

2.1.3. SOAP への適用 (WS-Security)

XML データのセキュリティ保護のために、2.1.1, 2.1.2 で述べた XML 暗号、XML 電子署名が仕様として策定されているが、これらの仕様を、SOAP (Simple Object Access Protocol)で使用する方法として定義したものが、WS-Security (Web Services Security)である。

WS-Security は、OASIS の WSS TC (Web Services Security Technical Committee)によって策定され、v1.0 が 2004 年に、v1.1 が 2006 年に OASIS 標準となっている[3]。
WS-Security では、SOAP メッセージのセキュリティを確保するため、主に次の 3 つの機能を提供している。

- XML 暗号を利用した SOAP メッセージの秘匿性の確保
- XML 署名を利用した SOAP メッセージの完全性の確保
- SOAP メッセージへのセキュリティ・トークン(認証情報などのセキュリティに関する情報)の付与

2.1.4. 標準化の最新動向

暗号化と電子署名については、W3C の XML Security Working Group が改善提案を行っている。 2009 年 7 月 31 日に、6 種類の文書が発表された[4]。

- XML Signature Best Practices - XML 電子署名における推奨慣行を記述する文書の草稿。セキュリティ面や名前空間に関する推奨事項など。
- XML Signature Syntax and Processing Version 1.1 - XML 電子署名の標準規格を変更する新バージョンの草稿。主な変更点は暗号とハッシュのアルゴリズム拡充。また、この文書の中で、より大きな変更を行うバージョン 2 を開発中と記されている。
- XML Signature Transform Simplification: Requirements and Design - XML Signature Transform の仕組みを単純化し、セキュリティや性能を改善するための仕様の草稿。
- W3C XML Encryption Syntax and Processing Version 1.1 - XML 暗号の標準規格を変更する新バージョンの草稿。主な変更点は暗号アルゴリズムの拡充。
- XML Security Generic Hybrid Ciphers - ハイブリッド暗号の規格を規定する新しい文書の草稿。

- XML Security Algorithm Cross-Reference - 暗号アルゴリズムのリファレンス。

電子署名についてはさらにその後 2009 年 10 月 22 日に、Version 2.0 の草稿が発表された[5]。 この新バージョンでは、Transform が見直され、あいまいさやセキュリティ面の課題に対処することを狙いとしている。

2.1.5. アプリケーション・サーバー型

XML データに対する暗号処理は、アプリケーション･サーバーのソフトウェアに組み込まれることが多くある。 暗号化や電子署名の個別の機能として提供される場合と、WS-Security など、より大きな機能の一部として組み込まれている場合がある。
この形態で暗号処理を利用する利点として、次のことが挙げられる。

- Web サービスの実行環境だけで暗号処理機能を提供できる。
- 多くの場合コーディング無しで対応できる。

ただし、サーバーおよびアプリケーションごとに、該当機能の指定、設定が必要になる。

2.1.6. ゲートウェイ型

ゲートウェイ型とは、XML の暗号化／復号、電子署名の署名／署名検証、及びそれに伴う鍵管理など、アプリケーション･サーバーが本来実施する処理の一部分をオフロードして、その処理に特化した専用装置である。ハードウェアとソフトウェアが一体となったアプライアンス製品と、ソフトウェアとして提供される製品があり、セキュリティに重点をおいた製品から、スキーマ検証、ＸＳＬ変換など、XML 処理のオフロードやその他の管理機能も提供する製品まで、様々なタイプがある。

ゲートウェイ型製品を利用する利点として、以下の点が挙げらる。

- アプリケーション･サーバーの負荷軽減
- 処理のハードウェア化対応等により、高速化を実現
- 特定機能に特化することで、設計、構築、運用の効率化、導入までのスケジュールの短縮化

2.1.7. ライブラリ型

XML の暗号化、電子署名についてはライブラリとして提供される製品もある。 また、インターネットで公開されているツールはライブラリ型のものが多い。

- Apache XML Security - Apache による Java と C++のライブラリ。
  http://santuario.apache.org/index.html

- JSR-106 - Java の XML Digital Encryption API 仕様。IBM SDK 6 で提供されている。
- JSR-105 – Java の XML Digital Signature API 仕様。Java 6 で提供されている[6]。
- .Net Framework - Microsoft による実装。

こうしたツールを利用したセキュリティ機能の実装については、XML コンソーシアム セキュリティ部会において、実際の XML インスタンスを使った複数の暗号化パターンによる暗号化･復号の検証、複数の暗号化ツールにおける暗号化･復号の検証、複数のツール間での復号互換性の確認を実施し,2009 年 5 月 12 日の XML コンソーシアム Week にて検証結果の概要を報告した[7]。
詳細は別途セキュリティ部会より報告書を公開予定。
WS-Security についてもインターネットで公開されているツールが存在する。

- Apache WSS4J http://ws.apache.org/wss4j/
- WSIT https://wsit.dev.java.net/

2.2. XML ベースの長期署名

XML 電子署名について2.1.2節で紹介したが、この他に長期保存に対応するための長期署名仕様も存在する。 XAdES は XML 署名に長期保存や他の高度な電子署名用の機能を加えた規格で、ヨーロッパの ETSI （ www.etsi.org ）により、V1.3.2 が 2006 年 3 月に標準化されており、V1.3.2 をベースに JIS 化され JIS X 5093:2008 としてプロファイル化されている。ETSI では最新の V1.4.1 が 2009 年 6 月に公開されているが、2009 年 10 月時点では JIS への反映はされていない。

2.2.1. サーバー型

長期署名の利用方法としては長期保管をサーバーにて行う文書サーバーが一般的となっている。同じサーバー型としても異なる利用方法としては、サーバーに与えられた文書に長期署名を付与して返すサービス提供型のサーバーもある。

2.2.2. ライブラリ型

サーバーでの利用およびクライアントでも利用できるライブラリ型の製品もある。利用インターフェイスとしては.NET Framework や Java 等が多い。

2.2.3. 現実世界と電子世界の比較

電子署名は現実世界において印鑑を使った場合と同等のことができると言われている。図 2.2.3.1 において印鑑のシステムと電子署名のシステムを比較した。現実世界での印

鑑に相当するものが証明書と秘密鍵のペアとなる。正確には秘密鍵が印鑑そのものと同等と言えるが、通常ペアで利用される。現実世界の印影に相当するものが電子署名の署名値と言える。印影が有効かどうかを確認する為に現実世界では印鑑証明書等を利用するがこれに相当するものが失効情報（CRL 等）の検証情報となる。なお長期署名とは検証情報を含んだ電子署名の拡張と言える。

現実世界	 印鑑（ハンコ）	 紙に押印した印影	 印鑑証明書や住民票等
電子世界	証明書と秘密鍵	電子署名（XML 署名）	検証情報（失効情報等）

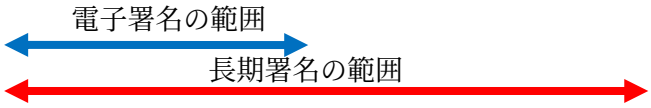

図 2.2.3.1 現実世界と電子世界の比較

2.2.4. 現実世界と電子世界の差異

現実世界と電子世界の電子署名では、ほぼ同じと言えど以下に上げた差異も存在する。電子署名は有効期限がある点で不利だが、タイムスタンプ技術により時間の確認ができる点では有利であり、一長一短がある。

1. 電子署名（証明書）は**有効期限**がある （現実より劣っている）
2. 「**誰が**」だけで無く「**いつ**」もタイムスタンプ技術で保証可能 （現実より優れている）

1. の有効期限に関しては、暗号方式の脆弱化の恐れ等から通常は数年から5年程度で無効になる。暗号方式が脆弱化することで改竄が可能となってしまう。例えば現在最も使われている SHA-1 ハッシュ方式に関しても近い将来に脆弱化の恐れがある為に、内閣官房情報セキュリティセンターより 2008 年 4 月に「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」により、公的利用としては 2013 年度に SHA-2 への適合が求められている。なお長期署名は期限切れの前に更新する仕組み（仕様）で期限延長が可能となっている。

2. のタイムスタンプは、正しい時刻を保証する電子署名の一種でタイムスタンプ局が運営する。長期署名の仕様により電子署名＋タイムスタンプを実現している。

2.2.5. XML 電子署名と長期署名の比較

XML 電子署名は W3C 勧告の XmlDsig として標準化が行われている。その XML 電子署名をベースとして、長期署名 XAdES が ETSI TS 101 903 として標準化されている。更に日本においては国内の相互運用性を確保する為に長期署名 XAdES のプロファイルが JIS として定義されている。

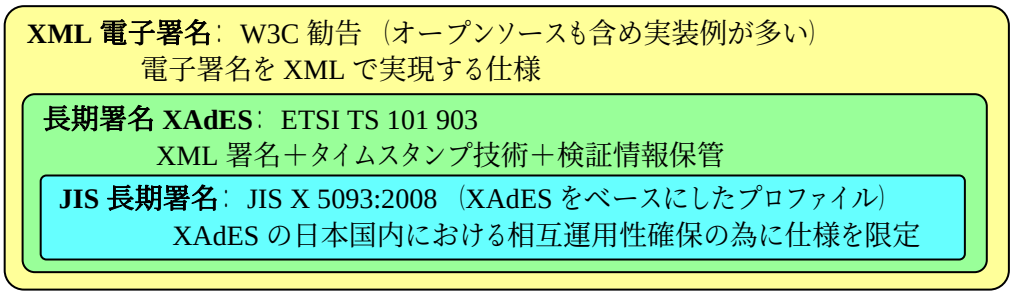

図 2.2.5.1 各種電子署名標準規格の関係

短期的に改竄や否認を防止する目的であれば XML 署名で良い。電子署名により「**誰が**」「**何を**」を保証できる。正確な存在時刻を保証するなら長期署名 XAdES（XAdES-T）が必要。電子署名と署名タイムスタンプにより「**誰が**」「**何を**」「**いつ**」を保証できる。有効期限をこえて長期間保管するなら長期署名 XAdES（XAdES-A）が必要。保管タイムスタンプにより**有効期限後**の保証ができる。

2.3. XML/SOAP ファイアウォール

ここでは、XML/SOAP ファイアウォールとは、通信中の XML データあるいは SOAP アクションを検査し、事前に定義されたポリシーに抵触するものがあれば遮断を行えるファイアウォール機能と定義する。

XML 向けのファイアウォール機能を提供する製品は、XML を使った Web サービスが話題になった 2001～2002 年頃から登場し、最近では単独の製品というよりは、他の機能を主とする製品の一部機能として提供する形態に変化している。

2.3.1. 製品分野の動向

需要としては、当初 SOAP プロトコルを利用する Web サービス、特に B2B での通信保護での利用を目的に製品提供がなされた。 最近では Web 2.0 といわれるアプリケーション構造の変化に伴い、動的ユーザーインターフェースを実現する AJAX が XML でデータをアクセスしたり、サイト間の認証連携で XML が使われるようになってきて、通信中 XML データのセキュリティが改めて重要視されている。

2009 年 7 月に調査会社 Gartner が発表した基盤保護製品のトレンドを示した報告書[8]において、XML Firewall が Slope of Enlightenment (啓蒙活動期)に入り、2 年以内にメインストリームになると報告しており、XML ファイアウォールの重要性を指摘している。

2.3.2. ツールや製品の提供形態

製品機能としては、XML データの妥当性検査が中核となり、スキーマ検証機能を提供するものもある。

大きく分けて、ファイアウォールあるいは Web アプリケーション･ファイアウォール(WAF)の一部として提供される場合と、XML 処理ツールの一部として主にゲートウェイの形態で提供される場合がある。

フリーのツールとしては、Apache のプラグインとして WAF 機能を提供する ModSecurity[9]が、2006 年にリリースされたバージョン 2.0 で XML データ検査の機能を提供開始した。

製品形態としては、アプライアンスとソフトウェアがあり、Web サーバーの前段にゲートウェイとしてネットワーク接続するか、サーバー上にインストールする。

3. 商用製品調査結果

情報提供のあった商用製品について概要を紹介した後、提供のあった情報（調査票）を掲載する。

3.1 節では、提供のあった情報の概要をまとめている。

3.2 節から 3.4 節までは、情報提供された各社から報告いただいた内容を体裁の変更を除いてそのまま記載してある。 記載順は、製品分野ごと、企業名の五十音順としている。

3.1. 調査結果概要

3.1.1. XML 暗号、XML 電子署名、WS-Security

アプリケーション・サーバー型が 4 製品、ライブラリ型（XML 署名関連のライブラリ）が 2 製品、ゲートウェイ型として 3 製品の情報提供があった。

アプリケーション・サーバー型では、XML 暗号機能、電子署名機能、WS-Security 機能を共通的にサポートしていた。

ゲートウェイ型の 3 製品は、XML 暗号に特化した製品と、WS-Security 機能まで提供している製品で、形態が異なっていた。

3.1.2. XML ベースの長期署名

サーバー型に 2 製品、ライブラリ型に 1 製品の情報提供があった。サーバー型 2 製品も文書サーバーと長期署名付与サーバーであり、提供する機能が異なるものだった。

3.1.3. XML/SOAP ファイアウォール

2 製品の情報提供があった。

ゲートウェイ型と Web アプリケーション・ファイアウォール(WAF)の付属機能という、異なる形態のものだった。

3.2. XML 暗号、XML 電子署名、WS-Security

3.2.1. アプリケーション・サーバー型およびライブラリ型

3.2.1.1 IBM WebSphere Application Server

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。 :IBM
2－2. 製品の正式名称をご回答下さい。 :WebSphere Application Server
2－3. 製品の最新バージョンと出荷日をご回答下さい。:7.0 出荷日:2008 年 9 月 27 日(ダウンロード)
2－4. 製品を説明している Web 頁の URL をご回答下さい。 :
http://www.ibm.com/jp/software/websphere/
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。:お問合せ窓口
http://www-06.ibm.com/jp/software/contactus/index.html
2－6. 製品価格をご回答下さい。 :製品発表レター
http://www.ibm.com/jp/press/2008/09/1701.html
製品価格は改定され、発表時とは異なることがありますので、弊社営業担当にお問合せ下さい。

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号･復号機能
■XML 電子署名付与･検証機能
■WS-Security(Web Services Security)機能

3－2. 製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
□ライブラリー(API)として提供
■アプリケーション･サーバー機能として提供
□ゲートウェイ機能として提供

3－3．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等)をご回答下さい。:システム稼動要件 http://www.ibm.com/support/docview.wss?rs=180&uid=swg27012284
AIXR
HP-UX on PA-RISC
HP-UX on Itanium
IBM i?
LinuxR on x86
Linux on x86-64
Linux on POWER
Linux on System z9 and zSeriesR
Solaris SPARC
Solaris x64
WindowsR

3－4．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例:仕様拡張、処理性能、運用機能等)
特徴
:WSS V1.1 をフルサポート(WAS V7.0 から)
WAS6.1 でも Feature Pack for WebServices と呼ばれるアドオンを適用して頂くと WSS V1.1 がご利用になれます。
:WAS6.1 以降は以下の url にあるように鍵管理マネージャーikeyman と同等の機能を備えています。
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_sslcertmanadmin.html
また、鍵ストアとしては kdb 以外にも JCEKS、JKS、および PKCS12 のフォーマットをサポートしています。

3－5．準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
□OASIS Web Services Security (WS-Security 2004) v1.0
■OASIS Web Services Security (WS-Security 2004) v1.1

3－6．使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。

XML 暗号

■Triple DES　■AES 128 ビット　■AES 256 ビット

■その他：AES 192 ビット

XML 電子署名

(ダイジェストのアルゴリズム)

■SHA-1 □SHA-256

□その他：_____

(署名アルゴリズム)

■DSA-SHA1　□RSA-SHA1　□RSA-SHA256　□ECDSA-SHA256

□その他：_____

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。：

SecurityToken(Username,X509(3Types),LTPA,Custom token)

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。

□XML 暗号・復号機能　：_____

□XML 電子署名付与・検証機能　：_____

□WS-Security(Web Services Security)機能　：_____

導入実績　件数共に大量にありますので、以下の URL をご参照下さい。

http://www-06.ibm.com/jp/software/casestudies/websphere/

以下のように 2001 年から事例があり、現在迄各種事例で利用されています。

：電子署名技術採用事例　オリックス様　日経産業新聞、日本工業新聞　掲載　2001 年 4 月 1 日運用開始

：WS 及び電子署名事例　東京三菱銀行様「輸出信用状明細案内サービス」2003 年 1 月 21 日

3.2.1.2　日本オラクル株式会社 Oracle Security Developer Tools 10g Release 3 (10.1.3)

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。 ：日本オラクル株式会社
2－2. 製品の正式名称をご回答下さい。 ：Oracle Security Developer Tools 10g Release 3 (10.1.3)
2－3. 製品の最新バージョンと出荷日をご回答下さい。 ：
2－4. 製品を説明している Web 頁の URL をご回答下さい。 ：
http://www.oracle.com/technology/global/jp/products/id_mgmt/osdt/
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：Oracle Direct 0120-155-096
2－6. 製品価格をご回答下さい。 ：Oracle Security Developer Tools は Oracle Internet Application Server に含まて提供されます。
Oracle Internet Application Server Standard Edition は￥25,000/ユーザー～、¥1,250,000/プロセッサ～

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号･復号機能
■XML 電子署名付与･検証機能
■WS-Security(Web Services Security)機能

3－2. 製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
■ライブラリー(API)として提供
□アプリケーション･サーバー機能として提供
□ゲートウェイ機能として提供

3－3. 稼動するプラットフォーム(OS,バージョン,稼動条件,言語等) をご回答下さい。：
Java ライブラリとして提供。Windows、Linux、Solaris、HP-UX などの主要 OS に対応。

3－4. 製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例：仕様拡張、処

理性能、運用機能等)
Oracle Security Developer Tools は、XML/Web サービス･セキュリティに関連する
標準仕様を実装した Java ライブラリです。

3－5. 準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
■OASIS Web Services Security (WS-Security 2004) v1.0
□OASIS Web Services Security (WS-Security 2004) v1.1

3－6. 使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号
■Triple DES　■AES 128 ビット　■AES 256 ビット
■その他：AES 192 ビット

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 □SHA-256
□その他：_____

(署名アルゴリズム)
■DSA-SHA1　■RSA-SHA1　□RSA-SHA256　□ECDSA-SHA256
□その他：_____

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしている
セキュリティ･トークンの種類をご回答下さい。：X.509 Certificate Token

- Web Services Security の下記 Profile をサポートしています。

- Username Token Profile 1.0
- X.509 Token Profile 1.0
- SAML Token Profile 1.0

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていれ

ばその URL をご回答下さい。
□XML 暗号･復号機能　　：_____
□XML 電子署名付与･検証機能　　：_____
□WS-Security(Web Services Security)機能　：_____

本製品に特化した事例調査は実施してはおりません。

3.2.1.3　日本オラクル株式会社 Oracle WebLogic Server

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。　　：日本オラクル株式会社
2－2. 製品の正式名称をご回答下さい。　　：Oracle WebLogic Server
2－3. 製品の最新バージョンと出荷日をご回答下さい。　：10g Release 3 (10.3) : 2008 年 11 月
2－4. 製品を説明している Web 頁の URL をご回答下さい。　：
http://www.oracle.com/lang/jp/appserver/index.html
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：Oracle Direct 0120-155-096
2－6. 製品価格をご回答下さい。　　：￥21,700/ユーザー～、¥1,087,000/プロセッサ～

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号･復号機能
■XML 電子署名付与･検証機能
■WS-Security(Web Services Security)機能

3－2. 製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。

□ライブラリー(API)として提供
■アプリケーション・サーバー機能として提供
□ゲートウェイ機能として提供

3－3．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等）をご回答下さい。：
Windows、Linux、Solaris、HP-UX などの主要 OS に対応。

3－4．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。（例：仕様拡張、処理性能、運用機能等）
Oracle WebLogic Server はエンタープライズ・アプリケーションの開発、デプロイおよび統合のための、業界でもっとも包括的な Java アプリケーションサーバです。
ミッションクリティカルな多くの大規模システムでの実績に裏付けられた、業界屈指の信頼性と高パフォーマンス、そして運用管理性を提供します。

3－5．準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
■OASIS Web Services Security (WS-Security 2004) v1.0
■OASIS Web Services Security (WS-Security 2004) v1.1

他に XML/Web サービスセキュリティに関連する標準仕様として、
下記のものをサポートしています。

- Web Services Security Policy (WS-SecurityPolicy) 1.2
- Web Services Trust Language (WS-Trust) 1.3
- Web Services Secure Conversation Language (WS-SecureConversation) 1.3
- SAML (Security Assertion Markup Language) 2.0/1.1

Oracle WebLogic Server 10.3 の Web サービス機能でサポートしている標準は、
下記 URL にて公開されています。
http://otndnld.oracle.co.jp/document/products/wls/docs103/webserv_intro/standards.html

3－6．使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号

■Triple DES　■AES 128 ビット　□AES 256 ビット
□その他:_____

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 □SHA-256
□その他:_____

(署名アルゴリズム)
■DSA-SHA1　■RSA-SHA1　□RSA-SHA256　□ECDSA-SHA256
□その他:_____

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。:X.509 Certificate Token

- Web Services Security の下記 Profile をサポートしています。

- Username Token Profile 1.0/1.1
- X.509 Token Profile 1.0/1.1
- SAML Token Profile 1.0/1.1

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号・復号機能　:_____
□XML 電子署名付与・検証機能　:_____
□WS-Security(Web Services Security)機能　:_____

Java アプリケーションサーバ製品はエンタープライズアプリケーションの開発・実行基盤であり、XML 暗号/電子署名機能に特化した事例調査は実施してはおりません。

3.2.1.4　日本電気株式会社 SecureWare/電子署名開発キット

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。　：日本電気株式会社
2－2. 製品の正式名称をご回答下さい。　：SecureWare/電子署名開発キット
2－3. 製品の最新バージョンと出荷日をご回答下さい。　：Ver1.2　(2007 年 11 月 23 日)
2－4. 製品を説明している Web 頁の URL をご回答下さい。　：
http://www.nec.co.jp/cced/SecureWare/dsdk/index.html
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：

NEC IT プラットフォームマーケティング本部
(ソフトウェアお問い合わせ)
TEL:03-3798-7177
受付時間：午前9：00~午後12：00　午後1：00~5：00
(土・日・祝日・NEC所定の休日を除く)
E-mail:contact@soft.jp.nec.com

2－6. 製品価格をご回答下さい。　：¥1,200,000～

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
□XML 暗号・復号機能
■XML 電子署名付与・検証機能
□WS-Security(Web Services Security)機能

3－2. 製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
■ライブラリー(API)として提供
□アプリケーション・サーバー機能として提供
□ゲートウェイ機能として提供

3－3．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等) をご回答下さい。:

OS: Windows、Solaris、Linux
詳細は以下を参照
http://www.nec.co.jp/cced/SecureWare/dsdk/requirement.html

3－4．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例:仕様拡張、処理性能、運用機能等)
･XML 署名の作成･検証に必要な基本機能を提供(XML 署名ライブラリ)。
･Web クライアントでの IC カードなどのローカル資源へのアクセスといった、
XML 署名で頻繁に要求される機能をフレームワークとして提供(XML 署名フレームワーク)
･ XML 分離署名用の、再利用可能な実装を提供(テンプレート)
･W3C/IETF 勧告に準拠した XML 署名の作成･検証を行うシステムを容易に構築。

3－5．準拠している標準仕様をご回答下さい。
□W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
□OASIS Web Services Security (WS-Security 2004) v1.0
□OASIS Web Services Security (WS-Security 2004) v1.1

3－6．使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号
□Triple DES □AES 128 ビット □AES 256 ビット
□その他:

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 □SHA-256
□その他:

(署名アルゴリズム)
■DSA-SHA1 ■RSA-SHA1 □RSA-SHA256 □ECDSA-SHA256

■その他：HMAC-SHA1

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。：_____

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号・復号機能　　：_____
□XML 電子署名付与・検証機能　　：_____
□WS-Security(Web Services Security)機能　：_____

3.2.1.5　日立製作所 uCosminexus Application Server

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。　　：日立製作所
2－2. 製品の正式名称をご回答下さい。　　：uCosminexus Application Server
2－3. 製品の最新バージョンと出荷日をご回答下さい。　：08-00, 2008/11 リリース
2－4. 製品を説明している Web 頁の URL をご回答下さい。　：
http://www.hitachi.co.jp/Prod/comp/soft1/cosminexus/index.html
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：0120-55-0504 (日立オープンミドルウェア問い合わせセンター)
2－6. 製品価格をご回答下さい。　　：1,260,000 円～ (税抜:1,200,000 円～)

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号・復号機能
■XML 電子署名付与・検証機能
■WS-Security(Web Services Security)機能

3－2．製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
□ライブラリー(API)として提供
■アプリケーション・サーバー機能として提供
□ゲートウェイ機能として提供

3－3．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等）をご回答下さい。
：OS=Windows, Linux, HP, AIX, Solaris
言語=Java
詳細は下記 URL 参照。

http://www.hitachi.co.jp/Prod/comp/soft1/apserver/products/platform/index.html

3－4．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。（例：仕様拡張、処理性能、運用機能等）
：高性能、高信頼

3－5．準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
□OASIS Web Services Security (WS-Security 2004) v1.0
■OASIS Web Services Security (WS-Security 2004) v1.1

3－6．使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号
■Triple DES ■AES 128 ビット □AES 256 ビット
□その他：_____

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 □SHA-256
□その他：_____

(署名アルゴリズム)

■DSA-SHA1 ■RSA-SHA1 □RSA-SHA256 □ECDSA-SHA256
□その他:_____

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの
種類をご回答下さい。
:UsernameToken : PasswordText, PasswordDigest, Nonce, Created
BinarySecurityToken: X.509v3

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号・復号機能 :_____
□XML 電子署名付与・検証機能 :_____
□WS-Security(Web Services Security)機能 :_____
非公開

3.2.1.6 富士通株式会社 Interstage Application Server

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。 :富士通株式会社
2－2. 製品の正式名称をご回答下さい。 :Interstage Application Server
2－3. 製品の最新バージョンと出荷日をご回答下さい。 :V9.2、2009/08 販売開始
2－4. 製品を説明している Web 頁の URL をご回答下さい。 :

http://interstage.fujitsu.com/jp/apserver/
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。:
http://interstage.fujitsu.com/jp/contact/をご参照ください
2－6. 製品価格をご回答下さい。 :55 万円より (Standard-J Edition)
(http://interstage.fujitsu.com/jp/apserver/price/をご

参照ください)

3．機能仕様に関して

3－1．以下の機能の中で、製品が提供しているものにチェックして下さい。

□XML 暗号･復号機能

□XML 電子署名付与･検証機能

■WS-Security(Web Services Security)機能　(コメント:これは上記 2 つの機能を包含)

3－2．製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。

□ライブラリー(API)として提供

■アプリケーション･サーバー機能として提供

□ゲートウェイ機能として提供

3－3．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等)をご回答下さい。:

Windows、Solaris、Linux

(詳細について http://interstage.fujitsu.com/jp/apserver/environment/をご参照ください)

3－4．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例:仕様拡張、処理性能、運用機能等)

業務安定稼働、業務運用の効率化、資産の長期利用、安全なシステム構築

3－5．準拠している標準仕様をご回答下さい。

□W3C XML Encryption Syntax and Processing

□W3C XML-Signature Syntax and Processing

■OASIS Web Services Security (WS-Security 2004) v1.0

■OASIS Web Services Security (WS-Security 2004) v1.1

3－6．使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。

XML 暗号

■Triple DES　■AES 128 ビット　■AES 256 ビット

■その他:_上記のビット違い_

XML 電子署名

(ダイジェストのアルゴリズム)
■SHA-1 ■SHA-256
■その他:_上記のビット違い_

(署名アルゴリズム)
■DSA-SHA1 ■RSA-SHA1 ■RSA-SHA256 □ECDSA-SHA256
■その他:_上記のビット違い、RSA- RIPEMD160_

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。:
Username, X.509

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号・復号機能 :_____
□XML 電子署名付与・検証機能 :_____
□WS-Security(Web Services Security)機能 :_____

製品に WS-Security 機能は取り込んでおりますが、下記の理由によりとくに積極的な公開はしておりません。

WS-Security は、自由度が高く極めて広範な利用形態が実現可能である一方、
その裏返しとして以下のような注意点があります。
・WS-Securiry を生かした適切なシステム設計・運用には、高度な内容の理解が必要
・内容理解が不十分なままシステムを構築すると、お客様システムにセキュリティの不備が生じる恐れがある
そのため、お問い合わせを頂いてコンサルティング込みでのご提供が望ましいと判断しております。

なお、WS-Security には、信頼できない第三者を経由した通信を安全に出来るという、
SSL/TLS では不可能なセキュリティ機能をお客様システムにもたらすことが出来ます。
しかし、そのような要件をお持ちのお客様システムは、実際には極めて例外的です。

3.2.2. ゲートウェイ型

3.2.2.1 IBM WebSphere DataPower SOA アプライアンス XML セキュリティーゲートウェイ

調査票 1-2 XML 暗号/電子署名機能提供ゲートウェイ製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。 ：IBM
2－2. 製品の正式名称をご回答下さい。 ：WebSphere DataPower SOA アプライアンス XML セキュリティーゲートウェイ
2－3. 製品の最新バージョンと出荷日をご回答下さい。 ： Firmware 3.8 2009 年 11 月
2－4. 製品を説明している Web 頁の URL をご回答下さい。 ：http://www-06.ibm.com/jp/software/websphere/bi/datapower/xs40/index.html
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：_http://www-06.ibm.com/software/jp/contactus/ _____
2－6. 製品価格をご回答下さい。 ：¥10,296,000～

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号･復号機能
■XML 電子署名付与･検証機能
■WS-Security(Web Services Security)機能

3－2. 稼動するアプライアンス製品の稼動条件等あればご回答下さい。
：温度：0～40 度、相対湿度 0～90（結露なしの場合）

3－3. 製品の機能仕様に関して、特筆すべき特徴をご回答下さい。（例：仕様拡張、処理性能、運用機能等）
XML 処理テクノロジーを搭載し、セキュリティーを考慮して開発されたため、XML および Web サービスのトランザクションのセキュリティー実装ポイントとなり、包括的な XML セキュリティー、および実際のアプリケーションに必要なワイヤースピードのパフォーマンスを提供します。

暗号、署名機能など、ユーザーが簡単に定義できる GUI が提供されており、アプリケーションに手を加えることなく容易に WS-Security を実装できます。
http://www-06.ibm.com/software/jp/websphere/integration/datapower/xs40/features.html

3－4. 準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
■OASIS Web Services Security (WS-Security 2004) v1.0
■OASIS Web Services Security (WS-Security 2004) v1.1

3－5. 使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号
■Triple DES ■AES 128 ビット ■AES 256 ビット
■その他：AES 192 ビット

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 ■SHA-256
■その他：md5,ripemd160,sha224,sha384,sha512

(署名アルゴリズム)
■DSA-SHA1 ■RSA-SHA1 ■RSA-SHA256 □ECDSA-SHA256
■その他：rsa-md5,rsa-ripemd160,rsa-sha384,rsa-sha512

3－6. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。：X.509,Username Token,SAML,Kerberos,HTTP Authentication Header,HTTP Authentication Header,WS-Trust Base or Supporting Token,LPTA

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号・復号機能 ：_____
□XML 電子署名付与・検証機能 ：_____
□WS-Security(Web Services Security)機能 ：_____

3.2.2.2　日本オラクル株式会社 Oracle Web Services Manager

調査票 1-1 XML 暗号/電子署名機能提供ソフトウェア製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。　：日本オラクル株式会社
2－2. 製品の正式名称をご回答下さい。　：Oracle Web Services Manager
2－3. 製品の最新バージョンと出荷日をご回答下さい。　：10g Release 3: 2006 年 11 月
2－4. 製品を説明している Web 頁の URL をご回答下さい。　：
http://www.oracle.com/technology/global/jp/products/webservices_manager/index.html
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：Oracle Direct 0120-155-096
2－6. 製品価格をご回答下さい。　：￥100,000/ユーザー～、¥5,000,000/プロセッサ～

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号･復号機能
■XML 電子署名付与･検証機能
■WS-Security(Web Services Security)機能

3－2. 製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
□ライブラリー(API)として提供
□アプリケーション･サーバー機能として提供
■ゲートウェイ機能として提供

3－3. 稼動するプラットフォーム(OS,バージョン,稼動条件,言語等) をご回答下さい。：
Windows、Linux、Solaris、HP-UX などの主要 OS に対応。

3－4. 製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例：仕様拡張、処理性能、運用機能等)

Oracle Web Services Manager (WSM)は、あらゆる既存の Web サービスや新しい Web サービスに
ポリシー・ドリブンのセキュリティ機能と管理機能を提供します。WSM では、ポリシー(アクセス・ポリシー、ログ・ポリシーなど)を一元的に定義でき、サービスを変更せずにこれらのポリシーを Web サービスに組み込むことができます。

3－5. 準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
■OASIS Web Services Security (WS-Security 2004) v1.0
□OASIS Web Services Security (WS-Security 2004) v1.1

3－6. 使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号
■Triple DES　■AES 128 ビット　■AES 256 ビット
□その他:_____

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 □SHA-256
□その他:_____

(署名アルゴリズム)
■DSA-SHA1　■RSA-SHA1　□RSA-SHA256　□ECDSA-SHA256
□その他:_____

3－7. WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。:X.509 Certificate Token

- Web Services Security の下記 Profile をサポートしています。

- Username Token Profile 1.0
- X.509 Token Profile 1.0
- SAML Token Profile 1.0

4．以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号･復号機能　　：＿＿＿＿＿＿＿＿＿＿
□XML 電子署名付与･検証機能　　：＿＿＿＿＿＿＿＿＿＿
□WS-Security(Web Services Security)機能　：＿＿＿＿＿＿＿＿＿＿

本製品に特化した事例調査は実施してはおりません。

3.2.2.3　日本セーフネット株式会社 Luna XML

調査票 1-2 XML 暗号/電子署名機能提供ゲートウェイ製品調査票

1．ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2．製品に関して
2－1．ベンダーの会社名をご回答下さい。　　：日本セーフネット株式会社
2－2．製品の正式名称をご回答下さい。　　：Luna XML
2－3．製品の最新バージョンと出荷日をご回答下さい。　：Luna XML 1.0.22009/02/26
2－4．製品を説明している Web 頁の URL をご回答下さい。　：http://jp.safenet-inc.com/products/pki/luna_XML.asp
2－5．製品に関する連絡先(TEL、メールなど)をご回答下さい。：03-5776-2751
2－6．製品価格をご回答下さい。　　：468 万円～

3．機能仕様に関して
3－1．以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML 暗号･復号機能
■XML 電子署名付与･検証機能
□WS-Security(Web Services Security)機能

3－2．稼動するアプライアンス製品の稼動条件等あればご回答下さい。
厳密にはゲートウェイというよりは、リクエストを受けて処理を実行して応答するアプライアンス形態。

クライアント側にライブラリ必要なし(WSDL)。

3－3. 製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例:仕様拡張、処理性能、運用機能等)

SafeNet Luna XML は、ハードウェア・セキュリティ・モジュール(HSM)を利用したアプリケーションのセキュリティ構築を非常に簡単に行えるソリューションです。
他の HSM 製品では、複雑なセキュリティ用 API を利用し、アプリケーションへの組込み作業が必要となり、数ヶ月の期間を要する場合もありますが、Luna XML では XML ベースのインターフェースとなっているため、特別なセキュリティ用 API の知識がなくともアプリケーションへの組込みが容易に行えます。
また、Luna XML はホスト・アプリケーション・サーバに対するフット・プリントはゼロで、システムへの統合、運用面でも素早い、柔軟性のある、拡張性の高い展開を進めることができます。

3－4. 準拠している標準仕様をご回答下さい。
■W3C XML Encryption Syntax and Processing
■W3C XML-Signature Syntax and Processing
□OASIS Web Services Security (WS-Security 2004) v1.0
□OASIS Web Services Security (WS-Security 2004) v1.1

3－5. 使用可能な XML 暗号、XML 電子署名の暗号アルゴリズムと鍵長についてご回答下さい。
XML 暗号
■Triple DES ■AES 128 ビット ■AES 256 ビット
■その他:RSA1024,2048,3072,4096、ECDSA、AES128,192,256、TDES

XML 電子署名
(ダイジェストのアルゴリズム)
■SHA-1 ■SHA-256
■その他:RSA with SHA1,256,384,512、ECDSA with SHA1,256,384、DSA with SHA1

(署名アルゴリズム)
■DSA-SHA1 ■RSA-SHA1 ■RSA-SHA256 ■ECDSA-SHA256

■その他：RSA with SHA1,256,384,512、ECDSA with SHA1,256,384、DSA with SHA1

3－6．WS-Security(Web Services Security)機能を提供している場合、サポートしているセキュリティ・トークンの種類をご回答下さい。：_____

4．以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。
□XML 暗号・復号機能　　：ございません
□XML 電子署名付与・検証機能　　：ございません
□WS-Security(Web Services Security)機能　：ございません

3.3. XML ベースの長期署名

3.3.1. セイコーインスツル株式会社 長期署名システム「NiXAdES」

調査票 2 XML 長期署名(XAdES)製品調査票

1．ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2．製品に関して
2－1．ベンダーの会社名をご回答下さい。　　：セイコーインスツル株式会社
2－2．製品の正式名称をご回答下さい。　　：長期署名システム「NiXAdES」
2－3．製品の最新バージョンと出荷日をご回答下さい。　：version1.0　2008 年 12 月
2－4．製品を説明している Web 頁の URL をご回答下さい。　：http://www.sii.co.jp/ni/
2－5．製品に関する連絡先(TEL、メールなど)をご回答下さい。：043-211-7479
2－6．製品価格をご回答下さい。　　：オープン

3．機能仕様に関して
3－1．製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
□ライブラリー(API)として提供
■サーバー機能/製品として提供
□クライアント機能/製品として提供
□サービス(ASP/SaaS 等)として提供

3－2．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等)をご回答下さい。
･OS Windows Server2003 以上
･稼動条件 Microsoft .NET Framework 2.0 以上, CAPICOM 2.0 以上

3－3．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例:仕様拡張、処理性能、運用機能等)
･JIS X5093:2008 プロファイルに対応
･電子データを指定フォルダに格納すると自動的に長期署名データを生成します。
･ファイル渡しのインタフェースなので、文書管理アプリケーション等との連携が容易です。

3－4．使用可能な暗号アルゴリズムと鍵長についてご回答下さい。
(ダイジェストのアルゴリズム)
■SHA-1 ■SHA-2(SHA-256/SHA-384/SHA-512)
□その他:_____

(署名アルゴリズム)
□DSA-SHA1 ■RSA-SHA1 □RSA-SHA2 □ECDSA-SHA2
□その他:_____

3－5．付与可能なタイムスタンプの種類をご回答下さい。
■標準タイムスタンププロトコル(RFC3161)
■商用タイムスタンプサービス対応 :PFU タイムスタンプサービス他

4．可能なら日本国内での事例件数、事例名称、Web で公開されていればその URL をご回答下さい。
:医療文書の完全性証明、知的財産の完全性証明を目的として採用されています。

3.3.2. 日本電気株式会社 PKI サーバ/Carassuit 原本保管サーバ

調査票 2 XML 長期署名(XAdES)製品調査票

1．ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2．製品に関して

2－1．ベンダーの会社名をご回答下さい。　　：日本電気株式会社
2－2．製品の正式名称をご回答下さい。　　：PKI サーバ/Carassuit 原本保管サーバ
2－3．製品の最新バージョンと出荷日をご回答下さい。　：Ver1.0
2－4．製品を説明している Web 頁の URL をご回答下さい。　：
http://www.nec.co.jp/cced/pki/caras-esd/index.html
2－5．製品に関する連絡先(TEL、メールなど)をご回答下さい。：

NEC IT プラットフォームマーケティング本部
（ソフトウェアお問い合わせ）
TEL:03-3798-7177
受付時間：午前9：00~午後12：00　午後1：00~5：00
（土・日・祝日・NEC所定の休日を除く）
E-mail:contact@soft.jp.nec.com

2－6．製品価格をご回答下さい。　　：¥7,000,000～

3．機能仕様に関して
3－1．製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
□ライブラリー(API)として提供
■サーバー機能/製品として提供
□クライアント機能/製品として提供
□サービス(ASP/SaaS 等)として提供

3－2．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等）をご回答下さい。
：Solaris
詳細は以下を参照
http://www.nec.co.jp/cced/pki/caras-esd/requirement.html

3－3．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。（例：仕様拡張、処理性能、運用機能等）
：
・電子文章をデータベースに格納し，「機密性」，「完全性」，「見読性」を担保した状態で保管
・署名時の時刻証明情報の保持や保管期間の延長により電子文書の長期保存機能を

提供
・Java 言語で操作 API を提供

3－4．使用可能な暗号アルゴリズムと鍵長についてご回答下さい。
(ダイジェストのアルゴリズム)
■SHA-1 □SHA-2(SHA-256/SHA-384/SHA-512)
■その他：MD5

(署名アルゴリズム)
■DSA-SHA1　■RSA-SHA1　□RSA-SHA2　□ECDSA-SHA2
□その他：

3－5．付与可能なタイムスタンプの種類をご回答下さい。
■標準タイムスタンププロトコル（RFC3161）
□商用タイムスタンプサービス対応　：_____

※商用のタイムスタンプサービスを利用する場合は、要相談

4．可能なら日本国内での事例件数、事例名称、Web で公開されていればその URL をご回答下さい。
：_____

3.3.3. 有限会社ラング・エッジ XML 長期署名 Le-XAdES Library

調査票 2 XML 長期署名(XAdES)製品調査票

1．ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2．製品に関して
2－1．ベンダーの会社名をご回答下さい。　：有限会社ラング・エッジ
2－2．製品の正式名称をご回答下さい。　：XML 長期署名 Le-XAdES Library
2－3．製品の最新バージョンと出荷日をご回答下さい。　：Ver1.20R3　2008 年 3 月 18

日

2－4．製品を説明している Web 頁の URL をご回答下さい。 ：

http://www.langedge.jp/pub/LeXAdES/

2－5．製品に関する連絡先(TEL、メールなど)をご回答下さい。：03-3862-2268 / contact@langedge.jp

2－6．製品価格をご回答下さい。 ：商用基本ライセンス 100 万円～

（詳細はお問合せ下さい）

3．機能仕様に関して

3－1．製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。

■ライブラリー(API)として提供

□サーバー機能/製品として提供

□クライアント機能/製品として提供

□サービス(ASP/SaaS 等)として提供

3－2．稼動するプラットフォーム(OS,バージョン,稼動条件,言語等）をご回答下さい。

･OS Windows/XP SP2 以上

･稼動条件 Microsoft .NET Framework 2.0 以上, CAPICOM 2.0 以上

･Microsoft Visual Studio 2005 - C++ 以上

3－3．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。（例：仕様拡張、処理性能、運用機能等）

･JIS X5093:2008 プロファイルに対応

･ECOM 相互運用性テスト合格

･既に日本国内での豊富な実績あり

･ソースを公開しているのでメンテナンス性に優れる

･独自開発の ASN.1/BER/DER と XML の相互変換用ライブラリも同梱

3－4．使用可能な暗号アルゴリズムと鍵長についてご回答下さい。

(ダイジェストのアルゴリズム)

■SHA-1 ■SHA-2(SHA-256/SHA-384/SHA-512)

□その他：_____

(署名アルゴリズム)

□DSA-SHA1 ■RSA-SHA1 ■RSA-SHA2 □ECDSA-SHA2

□その他:_____

3－5. 付与可能なタイムスタンプの種類をご回答下さい。
■標準タイムスタンププロトコル(RFC3161)
■商用タイムスタンプサービス対応　:PFU 他個別対応可能

4. 可能なら日本国内での事例件数、事例名称、Web で公開されていればその URL をご回答下さい。
・出荷件数:2009 年 3 月現在で9ライセンス出荷済み
・事例1:認証局(日本認証サービス様)の証明書電子更新サービスでの利用
・事例2:1部上場企業の社内文書や契約データの保管サーバへの組み込み(複数実績あり)
・事例3:官公庁におけるデータの保管時に利用
・事例4:長期文書保管サーバ製品への組み込み採用
・事例5:長期署名研究における利用

3.4. XML/SOAP ファイアウォール

3.4.1. IBM WebSphere DataPower SOA アプライアンス XML セキュリティーゲートウェイ

調査票 3 XML/SOAP ファイアウォール製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。　:IBM
2－2. 製品の正式名称をご回答下さい。　:WebSphere DataPower SOA アプライアンス XML セキュリティーゲートウェイ
2－3. 製品の最新バージョンと出荷日をご回答下さい。 : Firmware 3.8　2009 年 11 月
2－4. 製品を説明している Web 頁の URL をご回答下さい。 :http://www-06.ibm.com/jp/software/websphere/bi/datapower/xs40/index.html
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。:http://www-06.ibm.com/software/jp/contactus/
2－6. 製品価格をご回答下さい。　:¥10,296,000～

3．機能仕様に関して

3－1．以下の機能の中で、製品が提供しているものにチェックして下さい。

■XML を利用する不正アクセス検知機能(シグネチャやパターンによる)

■XML の値や属性の妥当性検証機能

■SOAP アクションの妥当性検証機能

■スキーマ検証機能

3－2．製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。

□ソフトウェアとして提供 (稼動条件:_____)

■ゲートウェイ機能(アプライアンス)として提供

□その他 _____

3－3．製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例:処理性能、ポリシー作成機能、セキュリティ機能、運用機能等)

XML 処理テクノロジーを搭載し、セキュリティーを考慮して開発されたため、XML および Web サービスのトランザクションのセキュリティー実装ポイントとなり、包括的な XML セキュリティー、および実際のアプリケーションに必要なワイヤースピードのパフォーマンスを提供します。

XML プロキシー機能を提供し、XML の製形式妥当性検証、バッファー・オーバーラン検査、XML スキーマ妥当性検査、XML フィルタリング、および XDoS 攻撃からの保護を実行することにより、XML 脆弱性に対する保護を行います。また、アクセス制御(AAA)、XML 暗号化とデジタル署名、WS-Security、およびコンテンツ・ベースのルーティングなど、XML ファイアウォールのセキュリティー機能以上に多くの重要なセキュリティー機能が含まれています。

http://www-06.ibm.com/software/jp/websphere/integration/datapower/xs40/features.html

4．以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。

■XML/SOAP ファイアウォール機能　　:数件ございます。事例の詳細については直接お問い合わせください。

3.4.2. Imperva Inc. SecureSphere Web Application Firewall

調査票 3 XML/SOAP ファイアウォール製品調査票

1. ご回答者に関してご記入下さい。
(この項目は非公開です。
XML コンソーシアムから追加のお問い合わせをすることがあります。)

2. 製品に関して
2－1. ベンダーの会社名をご回答下さい。 ：Imperva Inc.
2－2. 製品の正式名称をご回答下さい。 ：SecureSphere Web Application Firewall
2－3. 製品の最新バージョンと出荷日をご回答下さい。 ： Ver.7.0 2009 年 8 月 2 日
2－4. 製品を説明している Web 頁の URL をご回答下さい。 ：
http://www.imperva.com/japanese/products.asp
2－5. 製品に関する連絡先(TEL、メールなど)をご回答下さい。：03-4360-5721
2－6. 製品価格をご回答下さい。 ：298 万円より

3. 機能仕様に関して
3－1. 以下の機能の中で、製品が提供しているものにチェックして下さい。
■XML を利用する不正アクセス検知機能(シグネチャやパターンによる)
■XML の値や属性の妥当性検証機能
■SOAP アクションの妥当性検証機能
□スキーマ検証機能

3－2. 製品の提供は以下のどの形態でしょうか。チェックにてご回答下さい。
□ソフトウェアとして提供 (稼動条件：_____)
■ゲートウェイ機能(アプライアンス)として提供
□その他 _____

3－3. 製品の機能仕様に関して、特筆すべき特徴をご回答下さい。(例：処理性能、ポリシー作成機能、セキュリティ機能、運用機能等)
1) 高性能：最大で 2Gbps、44,000 http/秒
2) 既存環境を変えずに導入可能：透過型ブリッジでの導入に対応しており、ネットワークやアプリケーションへの変更無く導入が可能。
そのほか、ミラーポートへの接続による導入、Proxy での導入にも対応。
3) ポリシー自動作成・調整機能あり：URL やパラメーター、XML の値範囲を学習して異常な通信を検知するポリシーを自動生成。SOAP および REST に対応。

4. 以下の機能の日本国内での事例件数、可能なら事例名称、Web で公開されていればその URL をご回答下さい。

□XML/SOAP ファイアウォール機能　　：公表可能な事例なし

参考資料

1 W3C, “XML Encryption Syntax and Processing”, W3C Recommendation, 10 December 2002, http://www.w3.org/TR/xmlenc-core/

2 W3C, “XML Signature Syntax and Processing (Second Edition)”, W3C Recommendation, 10 June 2008, http://www.w3.org/TR/xmldsig-core/

3 XML コンソーシアム セキュリティ部会, “Web Services Security 1.0 日本語訳”, 2005 年 03 月 31 日, http://www.xmlconsortium.org/wg/sec/wss.html

4 Six XML Security Documents Published http://www.w3.org/News/2009#item136

5 XML Signature Syntax and Processing Version 2.0, 22 October 2009, http://www.w3.org/TR/xmldsig-core2/

6 JavaTM XML Digital Signature API Specification (JSR 105) http://java.sun.com/javase/6/docs/technotes/guides/security/xmldsig/overview.html

7 第 8 回 XML コンソーシアム Week - テーマ：XML が支えるエンタープライズシステム新潮流 2009 年 5 月 12 日 http://www.xmlconsortium.org/seminar09/090512-13+19-20/090512-prog.html

8 Hype Cycle for Infrastructure Protection,2009, http://www.gartner.com/DisplayDocument?doc_cd=169194

9 ModSecurity http://www.modsecurity.org/