

---

---

## XML コンソーシアム、 暗号化 XML データの利用技術の検討を開始

---

---

XML コンソーシアム（会長：鶴保証城 独立行政法人 情報処理推進機構ソフトウェアエンジニアリングセンター所長）は、本日、XML データのビジネス利用で必要となる XML 暗号化の利用技術を検討する活動を開始しました。本活動では、従来困難とされてきた「暗号化 XML データの妥当性検証」をスムーズに行う技術を確立するために必要な技術の検討と参考実装の開発および検証を行い、現実の業務への適用を提案していきます。この活動の結果として、XML データ交換、特に Web サービスにおいてデータ秘匿性を確保する手法を確立し、機密性を必要とする商取引のインターネット化推進に寄与することを目標としています。

本活動は、XML コンソーシアムの Web サービス実証部会とセキュリティ部会が共同で実施します。

### 【背景】

XML で記述されたデータの秘匿性を実現するためには標準化団体 W3C が暗号化の規格 XML Encryption<sup>(注1)</sup>を定めており、商用およびオープンソースのソフトウェアにおいて利用可能となっています。Web サービスのセキュリティを定義する WS-Security 2004 (OASIS 標準<sup>(注2)</sup>)でも XML Encryption の利用が前提となっています。一方、XML データ処理に際しては確実な処理と不正データ排除のために XML Schema<sup>(注3)</sup>を用いた妥当性検証(スキーマ検証)が必要になりますが、XML Encryption で暗号化した場合にはこのスキーマ検証が実施できなくなる問題が存在しています。XML コンソーシアムで 2004 年に実施した「TravelXML 利用 Web サービス実証実験」<sup>(注4)</sup>でも商取引における SOAP プロトコル<sup>(注5)</sup>を使った交換データを暗号化した際の問題点を指摘しました<sup>(注6)</sup>。

### 【活動予定】

本活動では上記問題点を解決するために、SOAP プロトコルで XML データを交換するビジネス・アプリケーションを前提に、XML を暗号化した際のスキーマ検証方法を検討・開発・提案します。

具体的には、W3C の文書<sup>(注7)</sup>で提案されている、以下の 3 つの方法について、Web サー

ビスへの具体的な適用手段を検討し、その成果を公表、広く利用してもらうことを目的とします。

暗号化前と暗号化後の両方を許すスキーマを用意する  
暗号化前のスキーマと暗号化後のスキーマを両方用意する  
復号してから妥当性検証を行う

なお、第一次の成果報告は、2006年6月を予定しております。

---

注1 XML Encryption の仕様 <http://www.w3.org/TR/xmlenc-core/>

注2 WS-Security 2004 仕様の日本語訳 <http://www.xmlconsortium.org/wg/sec/wss.html>

注3 XML Schema 技術解説 <http://www.xmlconsortium.org/websv/kaisetsu/C4/main.html>

注4 プレスリリース [http://www.xmlconsortium.org/release/pdf/20040520TravelXML\\_Final.pdf](http://www.xmlconsortium.org/release/pdf/20040520TravelXML_Final.pdf)

注5 SOAP:主にインターネット経由でプログラム間通信を行うためのプロトコル。技術解説  
<http://www.xmlconsortium.org/websv/kaisetsu/C1/main.html>

注6 公開資料 [http://www.xmlconsortium.org/koukai/travelxml-p/6\\_soukatsu.pdf](http://www.xmlconsortium.org/koukai/travelxml-p/6_soukatsu.pdf)

注7 XML Encryption Requirements W3C Note 04 March 2002 <http://www.w3.org/TR/xml-encryption-req#sec-Processing>

#### 【関連する既存技術について】

XML暗号化およびスキーマ検証に関しては既に多くの開発、製品化がなされており、本活動で検討予定の暗号化XMLデータの妥当性検証についても既に技術開発などが行われている可能性があります。XMLコンソーシアムではこうした既存技術、特許権等を尊重し、一般に利用可能な手法の提案・確立を目指しています。このため、関連する技術を既に検討・開発されている会員の方々があれば情報提供いただけるよう、お願いしています。

なお、XMLコンソーシアムの知的財産権に関するポリシーは会員規約第44条を参照ください。  
(<http://www.xmlconsortium.org/nyuukai/kiyaku.html>)

#### XML コンソーシアムについて

XML コンソーシアムは、XML 技術のビジネスにおける実用化推進を行う国内唯一の団体です。セミナー・イベント、部会活動、情報発信、標準化推進、各業界団体との連携などの具体的な活動を通じて、さまざまなコンピュータシステムにおける XML 技術の適用に貢献してまいります。

(<http://www.xmlconsortium.org/>)

### 参加企業一覧(50音順)

- アドソル日進(株)
- (株)内田洋行
- キヤノン(株)
- (株)J I E C
- 東京エレクトロン(株)
- 日本電気(株)
- (株)ネット・タイム
- (株)ノムラシステムコーポレーション
- (株)日立製作所
- PFU アクティブラボ(株)
- 富士ゼロックス(株)
- 富士通(株)

### <お問い合わせ先>

XMLコンソーシアム事務局

<http://www.xmlconsortium.org/>

E-mail: [xmlcons@fsi.co.jp](mailto:xmlcons@fsi.co.jp)

電話：03-5600-6205

担当：野田（富士ソフト ABC 内）

以上