W3C XML 暗号の実装とその評価

阿部　玲子　　北山　泰英　　砂田　英之　　茂木　強
三菱電機株式会社　情報技術総合研究所

1　はじめに

現在、W3C や OASIS といった標準化団体で、XML(eXtensible Markup Language)セキュリティの標準化策定が進められており、すでに W3C にて W3C XML 暗号仕様[1、2]と W3C XML 署名仕様[3]が勧告になっている。弊社ではセキュアな XML ベースの文書交換の実現を目的とし、W3C XML 暗号仕様に準拠した XML 文書の部分暗号化を可能とする Java クラスライブラリを開発した。本稿では、上記開発での仕様検討及び実装評価の観点から、W3C XML 暗号仕様の実用性の評価を述べる。

2　W3C XML 暗号

（1）W3C XML 暗号の特徴

・XML 文書の一部及び文書全体（XML 以外の文書を含む）の暗号化が可能である。暗号化単位は要素または要素のコンテンツである。

・暗号結果は XML 文書形式である。

（2）XML 暗号の例と解説

図１に AES 鍵でデータを暗号化し、使用した AES 鍵を公開鍵 RSA で暗号化した例を示す。

```
<EncryptedData Id='ED' xmlns='http://www.w3.org/2001/04/xmlenc#>
 <EncryptionMethod Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc'/>
 <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
  <ds:RetrievalMethod URI='#EK'
        Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
  <ds:KeyName>Sally Doe</ds:KeyName>
 </ds:KeyInfo>
 <CipherData><CipherValue>DEADBEEF</CipherValue></CipherData>
</EncryptedData>

<EncryptedKey Id='EK' xmlns='http://www.w3.org/2001/04/xmlenc#>
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
 <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
  <ds:KeyName>John Smith</ds:KeyName>
 </ds:KeyInfo>
 <CipherData><CipherValue>xyzabc</CipherValue></CipherData>
 <ReferenceList>
  <DataReference URI='#ED'/>
 </ReferenceList>
 <CarriedKeyName>Sally Doe</CarriedKeyName>
</EncryptedKey>
```

①暗号化されたデータに関する情報

暗号化したデータそのもの

②暗号化された鍵に関する情報

暗号化に用いた鍵を暗号化したもの

図１．W3C XML 暗号の例

“Implementation and evaluation of W3C XML Encryption Syntax and Processing “
Reiko ABE, Yasuhide KITAYAMA, Hideyuki SUNADA and Tsuyoshi MOTEGI, Information Technology R&D Center, Mitsubishi Electric Corporation

暗号化データは、下記の２種類に分類できる。（図１内の番号に対応）

①暗号化されたデータに関する情報
EncryptedData 要素の子要素である CipherData 要素には暗号化されたデータそのものが格納される。

②暗号化された鍵に関する情報
EncryptedKey 要素は本例のようにデータの暗号化に使用した鍵を暗号化する場合に存在する。子要素である CipherData 要素には暗号化に用いた鍵の暗号化結果が格納される。また、EncryptedKey 要素は再帰的に使用できる。

本例と異なる鍵の種類や配送方式を用いる場合は鍵情報の格納先が変る。例えば、要素暗号化に使用する鍵が DH(Diffie-Hellman)鍵共有[5]にて共有される場合、暗号鍵生成に必要な DH 共有鍵情報は KeyInfo 要素の子要素として AgreementMethod という要素内に格納される。なお、あらかじめ暗号に使用する鍵を取り決めた上で暗号データの交換を行う場合、鍵交換のロジック及び鍵情報格納要素が不要となる。

3　Java による W3C 準拠の XML 暗号実装

実装概要として、暗号化機能を提供する W3C XML 暗号パッケージについて説明する。図２に W3C XML 暗号パッケージの構成図を示す。

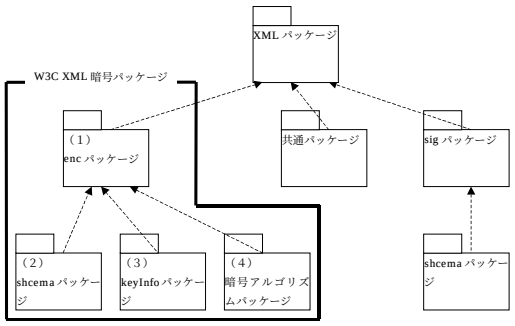

図２．W3C XML 暗号パッケージ構成図

W3C XML 暗号パッケージ自体は図２の太枠内で示されるが、構成図としては図２の様になる。理由は、W3C XML 暗号仕様では W3C XML 署名仕様内で制定されている要素の一部を利用しており、W3C XML 暗号パッケージが署名機能の一部である sig パッケージの機能を利用するからである。そのため、これらを統括する XML パッケージ及び、XPath 変換、正規化機能などを持つ共通パッケー

ジも存在し、W3C XML 暗号パッケージと関連する。また、実装上の特長として、ユーザの XML 暗号データ生成処理を簡易化するために、暗号データを格納するテンプレートと DOM 操作を軽減する schema パッケージを用意した。

W3C XML 暗号パッケージを構成する各パッケージ概要を以下に示す。（図２内の番号に対応）

（１） enc パッケージ

W3C XML 暗号仕様の記述にあわせて暗号化と復号の機能を提供するクラスを定義した。

（２）schema パッケージ

操作の統一と、DOM の上位 API の提供によるユーザの操作簡便化を目的とし、XML Encryption Syntax and Processing にて定義されている XML 要素及び XML Signature Syntax and Processing にて定義され XML 暗号でも使われる XML 要素ごとに要素の操作用クラス定義をした。また、操作性を考慮し XML 要素に対応する全てのクラスを基底となる１つのクラスから継承させた。

（３）keyInfo パッケージ

暗号に用いる鍵の種類や格納場所に依存せず共通のインタフェースを提供する。

（４）暗号アルゴリズムパッケージ

暗号化及び復号処理を行う機能を持つ。JCE（Java Cryptography Extension）で提供される機能を用いて、暗号アルゴリズムに依存しない共通 API を提供する。

４　W3C XML 暗号の実用面と実装面での評価

４．１　実用面の評価

W3C XML 暗号は部分暗号が可能であり、一つの文書中に暗号化すべき部分とそうでない部分が混在する文書のやり取りを行うシステムへの適用が可能である。例えば、図３の様な電子申請システムにおける入札フローへの適用が挙げられる。

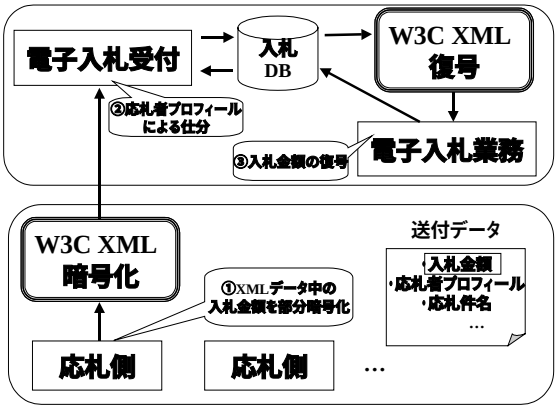

図３．電子申請入札データフロー適用イメージ

W3C XML 暗号は、このように従来暗号化を使用し難いと考えられていた文書システムに対して暗号化を適用することができる点が優れている。

４．２　実装面の評価

実装面のポイントは二点ある。第一に W3C XML 暗号仕様そのままでは操作時にユーザの負荷が高いという問題点がある。暗号化データを仕様通りに組み立てる操作や、煩雑な DOM 操作をユーザが行なう必要が生じるためである。そこで本開発では、テンプレートの提供で暗号化データの組み立てを軽減し、スキーマパッケージの提供で暗号化の際の DOM 操作を不要とした。これらのユーザ負荷の軽減は、暗号化データ作成ミスによる復号失敗などの危険性を減らすことに繋がると考えている。

第二に、アルゴリズムのサポートに関しては、W3C XML 暗号は JCE 上で動作するものであるのだが、Sun の提供している JRE（Java Runtime Environment）では、全てのアルゴリズムがサポートされているわけではない。よって、サポート外のアルゴリズムを使用するためには、別途暗号アルゴリズムを用意する必要がある。

５　おわりに

本稿では、W3C XML 暗号の概要紹介及び弊社で行った W3C XML 暗号に準拠した Java の API 開発について記述した。また、開発報告として W3C XML 暗号仕様の実装面、実用面での評価を報告した。

また、W3C XML 暗号は部分暗号化が可能であり、XML 文書以外の情報をも扱うことができるという優れた点を有する。今後 XML 文書の普及と共に、従来暗号化を使用し難いと考えられていた文書システムを含め、幅広いシステムへの応用が期待される。

謝辞

平成 13 年度情報処理振興事業協会（IPA）セキュリティ対策研究開発等事業として情報処理相互運用技術協会（INTAP）の XML 暗号仕様策定 WG にて検討し開発した「ＸＭＬセキュリティ関連標準のリファレンス実装」の研究成果を含む。

参考文献

1）XML Encryption Syntax and Processing
<http://www.w3.org/TR/xmlenc-core/>
2) XML Encryption Requirements
<http://www.w3.org/TR/xml-encryption-req>
3) XML-Signature Syntax and Processing
<http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/>
4) IPA ISEC [PKI 関連技術解説 公開鍵暗号方式]
<http://www.ipa.go.jp/security/pki/022.html>
5) RFC 2631: Diffie-Hellman Key Agreement Method
<http://www.ietf.org/rfc/rfc2631.txt>