Web Services Security:
X.509 Certificate Token Profile
OASIS Standard 200401, March 2004

日本語訳 2006 年 7 月

日本語訳作成 (Japanese Translation):

XML コンソーシアム セキュリティ部会 (XML Consortium Security SIG)

日本語訳編集 (Editors):

松永 豊	MATSUNAGA, Yutaka	東京エレクトロン株式会社
西村 利浩	NISHIMURA, Toshihiro	富士通株式会社

日本語訳貢献者 (Contributors):

秋本 論史	AKIMOTO, Satoshi	大日本印刷株式会社
岡村 和英	OKAMURA, Kazuhide	株式会社ネット・タイム
中山 弘二郎	NAKAYAMA, Kojiro	株式会社日立製作所
山根 利夫	YAMANE, Toshio	株式会社日立製作所

免責事項 (disclaimer notice):

This translated document is provided by <YOUR NAME/ORGANIZATION> as an informational service to the global community. This is an unofficial, non-normative translation of the official document, Web Services Security X.509 Certificate Token Profile, located at http://docs.oasis-open.org/wss/2004/01/ oasis-200401-wss-x509-token-profile-1.0.pdf, © copyright OASIS 2002-2004. This translation is published with acknowledgement of and in agreement with terms specified in the OASIS Translation Policy. Neither OASIS nor <YOUR NAME/ORGANIZATION> assume responsibility for any errors contained herein.

本翻訳文書はグローバルなコミュニティへの情報のサービスとして XML コンソーシアムによって提供される。これは http://docs.oasis-open.org/wss/2004/01/ oasis-200401-wss-x509-token-profile-1.0.pdf にある公式文書 Web Services Security X.509 Certificate Token Profile, © copyright OASIS 2002-2004 の非公式の、参考的な翻訳である。本翻訳は OASIS Translation Policy に明記されている条項を承知し同意のもとで公表されている。OASIS も XML コンソーシアムもここに含まれるいかなる誤りに対しても責任をもたない。

BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THIS DOCUMENT.

XML コンソーシアムは、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、XML コンソーシアムは、法律上のいかなる責任も負いません。

Web Services Security

X.509 Certificate Token Profile

OASIS Standard 200401, March 2004

Document identifier:
{*WSS: SOAP Message Security* }-{X509 Profile }-{1.0} (Word) (PDF)

Location:
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0

Errata Location:
http://www.oasis-open.org/committees/wss

Editor:

Phillip	Hallam-Baker	VeriSign
Chris	Kaler	Microsoft
Ronald	Monzillo	Sun
Anthony	Nadalin	IBM

Contributors:

Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Lab
Merlin	Hughes	Baltimore Technologies
Irving	Reid	Baltimore Technologies
Peter	Dapkus	BEA
Hal	Lockhart	BEA
Symon	Chang	CommerceOne
Srinivas	Davanum	Computer Associates
Thomas	DeMartini	ContentGuard
Guillermo	Lao	ContentGuard
TJ	Pannu	ContentGuard
Shawn	Sharp	Cyclone Commerce
Ganesh	Vaideeswaran	Documentum
Sam	Wei	Documentum
John	Hughes	Entegrity
Tim	Moses	Entrust
Toshihiro	Nishimura	Fujitsu
Tom	Rutt	Fujitsu
Jason	Rouault	HP
Yutaka	Kudo	Hitachi
Paula	Austel	IBM
Maryann	Hondo	IBM
Michael	McIntosh	IBM

Kelvin	Lawrence	IBM (co-Chair)
Anthony	Nadalin	IBM
Nataraj	Nagaratnam	IBM
Don	Flinn	Individual
Bob	Morgan	Individual
Paul	Cotton	Microsoft
Vijay	Gajjala	Microsoft
Chris	Kaler	Microsoft (co-Chair)
Chris	Kurt	Microsoft
John	Shewchuk	Microsoft
Johannes	Klein	Microsoft
Prateek	Mishra	Netegrity
Frederick	Hirsch	Nokia
Senthil	Sengodan	Nokia
Lloyd	Burch	Novell
Ed	Reed	Novell
Charles	Knouse	Oblix
Steve	Anderson	OpenNetwork (Sec)
Vipin	Samar	Oracle
Jerry	Schwarz	Oracle
Eric	Gravengaard	Reactivity
Stuart	King	Reed Elsevier
Andrew	Nash	RSA Security
Rob	Philpott	RSA Security
Peter	Rostin	RSA Security
Martijn	de Boer	SAP
Blake	Dournaee	Sarvega
Pete	Wenzel	SeeBeyond
Jonathan	Tourzan	Sony
Yassir	Elley	Sun Microsystems
Jeff	Hodges	Sun Microsystems
Ronald	Monzillo	Sun Microsystems
Jan	Alexander	Systinet
Michael	Nguyen	The IDA of Singapore
Don	Adams	TIBCO
John	Weiland	US Navy
Phillip	Hallam-Baker	VeriSign
Morten	Jorgensen	Vordel

48

Contributors of input documents (if not already listed above) :

Bob	Blakley	IBM
Joel	Farrell	IBM
Satoshi	Hada	IBM
Hiroshi	Maruyama	IBM
David	Melgar	IBM
Bob	Atkinson	Microsoft
Allen	Brown	Microsoft
Giovanni	Della-Libera	Microsoft
Johannes	Klein	Microsoft
Scott	Konersmann	Microsoft
Brian	LaMacchia	Microsoft
Paul	Leach	Microsoft
John	Manferdelli	Microsoft
Dan	Simon	Microsoft
Hervey	Wilson	Microsoft
Hemma	Prafullchandra	VeriSign

Abstract:

本文書では、Web Services Security: SOAP Message Security specification [WS-Security]仕様で X.509 証明書を利用する方法を記述する。

Status:

これは暫定的な草稿である。

部会のメンバーはこの仕様に対するコメントを wss@lists.oasis-open.org リストに送付されたい。その他の方は wss-comment@lists.oasis-open.org リストを購読し、そこにコメントを送付されたい。購読するには、http://lists.oasis-open.org/ob/adm.pl へアクセスすること。

本規定の実装に本質的かもしれない特許開示情報とライセンス条項の提供については、http://www.oasis-open.org/committees/wss/ipr.php にある OASIS Web Services Security Technical Committee (WSS TC)の Intellectual Property Rights の部分を参照のこと。

Table of Contents

1はじめに (参考)

本規定では、Web Services Security: SOAP Message Security 規定 [WS-Security] における X.509 認証フレームワークの利用について説明する。

X.509 証明書は、公開鍵と属性の集合との間の結合を定める。属性には、(少なくとも) 主体の名前、発行者の名前、通し番号、および有効期間が含まれる。この結合は、CRL の発行、OCSP トークン、または XKMS のような X.509 フレームワークの外にある仕組みを含む仕組みにより公表される、事後の失効による影響を受けるかもしれない。

X.509 証明書は SOAP メッセージを認証するために利用されるかもしれない公開鍵の正当性確認のために利用されてもよいし、または、暗号化された SOAP メッセージに付随する公開鍵を識別するために利用されてもよい。

2記法と用語 (標準)

本節では、本規定で利用される記法、名前空間および用語を指定する。

2.1 記法

本文書に出てくるキーワード「しなければならない(MUST)」、「してはならない(MUST NOT)」、「要求されている(REQUIRED)」、「することになる(SHALL)」、「することはない(SHALL NOT)」、「する必要がある(SHOULD)」、「しないほうがよい(SHOULD NOT)」、「推奨される(RECOMMENDED)、「してもよい(MAY)」および「選択できる(OPTIONAL)」は RFC 2119 で説明されるように解釈される。

抽象データ・モデルを説明するとき、本規定では XML Infoset により利用される記法を利用する。とくに、抽象プロパティ名はつねに角括弧に現れる (例えば、[some property])。

具体的な XML スキーマを説明するとき、本規定では、要素の [children] または [attributes] プロパティの各メンバーは XPath ライクな記法で説明される (例えば、/x:MyHeader/x:SomeProperty/@value1) 記法を利用する。 {any} の利用は、要素ワイルドカード (<xs:any/>) の存在を示す。 @{any} の利用は属性ワイルドカード (<xs:anyAttribute/>) の存在を示す。

2.2 名前空間

本規定の実装により利用されなければ**ならない (MUST)** XML 名前空間 [XML-ns] URI は次の通りとする (本規定で利用される要素は、これらの名前空間のどちらかで定義されることに注意すること):

```
http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
```

本文書では次の名前空間接頭辞が利用される:

Prefix	Namespace
S11	http://schemas.xmlsoap.org/soap/envelope/
S12	http://www.w3.org/2003/05/soap-envelope
ds	http://www.w3.org/2000/09/xmldsig#
xenc	http://www.w3.org/2001/04/xmlenc#
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

表 1 Namespace prefixes

2.3 用語

本規定では Web Services Security: SOAP Message Security 規定 [WS-Security] で定義された用語を採用する。読者は Internet Security Glossary [Glossary] の用語定義に精通していることを前提とする。

3利用方法 (標準)

本規定では、Web Services Security: SOAP Message Security 規定 [WS-Security] において X.509 認証フレームワークを利用するための構文と処理規則について説明する。

3.1 トークンの型

本プロファイルでは、表 2 で指定される QName 値を利用したバイナリ・セキュリティ・トークンの 3 つの型の構文と処理規則を定義する (URI フラグメントは本規定の URI に相対的なものであることに注意)。

Token	ValueType URI	Description
単一の証明書	#X509v3	X.509 v3 署名検証証明書
証明書パス	#X509PKIPathv1	PKIPath にパッケージされた X.509 証明書の順序付きリスト
証明書と CRL の集合	#PKCS7	PKCS#7 ラッパにパッケージされた X.509 証明書と (オプションの) CRL のリスト

表 2 Token types

3.1.1 X509v3 トークン型

この方法を利用した証明書によって認証されるエンド・エンティティの型は、ポリシーの問題であり本規定の範囲外である。

3.1.2 X509PKIPathv1 トークン型

#X509PKIPathv1 トークン型は証明書パスを表現するために利用されても**よい (MAY)**。

3.1.3 PKCS7 トークン型

#PKCS7 トークン型は証明書パスを表現するために利用されても**よい (MAY)**。アプリケーションはこの目的のためには代わりに PKIPath オブジェクトを利用することが**推奨される (RECOMMENDED)**。

PKCS#7 データ構造中の証明書の順序は意味がない。順序付き証明書パスが PKCS#7 符号化バイトに変換されそれから元に戻された場合、証明書の順序は保たれないかもしれない。処理装置はデータ構造中の証明書の順序に有意を仮定**してはいけない (SHALL NOT)**。詳細情報については [PKCS7] を参照のこと。

3.2 トークン参照

WSS: SOAP Message Security でサポートされたすべてのトークン型にわたり首尾一貫した処理モデルを保証するために、本プロファイルに準拠した署名または暗号要素の中で X.509 トークン型へのすべての参照を指定するために <wsse:SecurityTokenReference> 要素が利用される**ことになる (SHALL)**。

<wsse:SecurityTokenReference> 要素は、次の方法の 1 つによって X.509 トークン型を参照してもよい (MAY)。

サブジェクト鍵識別子への参照

<wsse:SecurityTokenReference> 要素は、X.509 SubjectKeyIdentifier 参照を利用してトークンデータを指定する wsse:KeyIdentifier 要素を含む。

バイナリ・セキュリティ・トークンへの参照

<wsse:SecurityTokenReference> 要素は、ローカルの <wsse:BinarySecurityToken> 要素またはトークン・データそのものを含むリモートのデータ・ソースを参照する <wsse:Reference> 要素を含む。

発行者と続き番号への参照

<wsse:SecurityTokenReference> 要素は X.509 Issuer と Serial Number によりエンド・エンティティの証明書をユニークに識別する <ds:X509IssuerSerial> 要素を含む <ds:X509Data> 要素を含む。

3.2.1 Subject Key Identifier への参照

<wsse:KeyIdentifier 要素が、X.509 SubjectKeyIdentifier 属性への参照によって X.509 証明書への参照を指定するために利用される。本プロファイルは表 3 で指定される URI 値 (URI フラグメントは本規定の URI に対して相対的なものであることに注意) を用いて Subject Key Identifier を参照するための構文および処理規則を定義する。

Subject Key Identifier	ValueType URI	Description
Certificate Key Identifier	#X509SubjectKeyIdentifier	証明書の X.509 SubjectKeyIdentifier の値

表 3 Subject Key Identifier

参照が作られる <wsse:SecurityTokenReference> 要素は <wsse:KeyIdentifier> 要素を含む。<wsse:KeyIdentifier> 要素は <wsse:X509SubjectKeyIdentifier>という値の ValueType 属性をもたなければならず (MUST)、その内容は証明書の X.509 SubjectKeyIdentifier 拡張の値が、<wsse:KeyIdentifier> 要素の EncodingType 属性により符号化されたものでなければならない (MUST)。本規定の目的においては、SubjectKeyIdentifier 拡張の値は KeyIdentifier オクテット列の内容で、オクテット列接頭辞の符号化を除いたものである。

3.2.2 セキュリティ・トークンへの参照

<wsse:Reference> 要素は URI 参照によって X.509 セキュリティ・トークン値を参照するために利用される。

URI 参照は内部的でもよく (MAY) 、この場合 URI 参照は、バイナリの X.509 セキュリティ・トークン・データを含む先行するメッセージ・ヘッダに含まれる <wsse:BinarySecurityToken> 要素への無装飾名の XPointer 参照である必要がある (SHOULD)。

3.2.3 Issuer と Serial Number への参照

<ds:X509IssuerSerial> 要素は、証明書の発行者の名前と通し番号によって X.509 セキュリティ・トークンへの参照を指定するために利用される。

<ds:IssuerSerial> 要素は、<ds:X509Data> 要素の直接の子で、それは参照が作られる <wsse:SecurityTokenReference> 要素の直接の子である。

3.3 署名

署名されたデータは、本規定で定義される X.509 セキュリティ・トークン型と参照のどれかを利用して、署名と関連付けられた証明書を指定してもよい **(MAY)**。

X.509 証明書は、公開鍵と属性の集合との間の結合を定める。属性には、(少なくとも) 対象の名前、発行者の名前、通し番号、および有効期間が含まれる。他の属性が、証明書の利用に制約を指定したり、その証明書に依存するパーティへ与えられているかもしれない遡及権に影響を与えてもよい。与えられた公開鍵は 1 つ以上の X.509 証明書中で指定されてもよい。すなわち、与えられた公開鍵は 2 つ以上の別個の属性集合に結び付けられてもよい。

したがって、X.509 証明書トークンの下で作成された署名は、ユニークにまた明確に署名が作成された証明書を必ず指定することが必要である。

実装は、続く節で説明されるように証明書を参照するために利用される方法にしたがって証明書そのものまたは署名の範囲内の証明書への不変で明白な参照を含めることによって、証明書置き換え攻撃に対して防御する**必要がある (SHOULD)**。

3.3.1 Key Identifier

<wsse:KeyIdentifier> 要素は参照される証明書への不変であいまいでない参照を保証しない。したがって、署名の中で参照のこの型を利用する実装は、参照される証明書が署名されており、単にあいまいな参照ではないことを保証するために、署名鍵情報への参照の中で STR Dereferencing Transform を採用する**必要がある (SHOULD)**。参照の形式は XPointer 規定 [XPointer] で定義されているように無装飾名参照である。

次の例が Key Identifier によって参照される証明書を示す。署名の範囲は <ds:SignedInfo> 要素であり、それはメッセージ本体 (#body) と署名に使われる証明書 (#keyinfo) の両方を含む。証明書は、直接参照している <ds:KeyInfo> 要素への参照で示されている。 <ds:KeyInfo> 要素は、証明書自身ではなく証明書への変わりやすい参照を含むだけであるので、証明書への参照を証明書で置き換える変換が指定される。 <ds:KeyInfo> 要素は、署名証明書の X.509 主体鍵識別子を指定する <wsse:KeyIdentifier> 要素を含む <wsse:SecurityTokenReference> 要素によって、署名鍵を指定する。

```
<S11:Envelope xmlns:S11="...">
   <S11:Header>
      <wsse:Security
           xmlns:wsse="..."
           xmlns:wsu="...">
         <ds:Signature
              xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>…
               <ds:Reference URI="#body">…</ds:Reference>
               <ds:Reference URI="#keyinfo">
                  <ds:Transforms>
                     <ds:Transform Algorithm="...#STR-Transform">
                        <wsse:TransformationParameters>
                          <ds:CanonicalizationMethod Algorithm="…"/>
                        </wsse:TransformationParameters>
                     </ds:Transform>
                  </ds:Transforms>…
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>HFLP…</ds:SignatureValue>
            <ds:KeyInfo Id="keyinfo">
               <wsse:SecurityTokenReference>
                  <wsse:KeyIdentifier EncodingType="...#Base64Binary"
                       ValueType="...#X509SubjectKeyIdentifier">
```

```
                    MIGfMa0GCSq…
                  </wsse:KeyIdentifier>
               </wsse:SecurityTokenReference>
            </ds:KeyInfo>
         </ds:Signature>
      </wsse:Security>
   </S11:Header>
   <S11:Body wsu:Id="body"
        xmlns:wsu=".../">
      …
   </S11:Body>
</S11:Envelope>
```

3.3.2 バイナリ・セキュリティ・トークンへの参照

署名されたデータは、参照されるセキュリティ・トークンを含む <wsse:BinarySecurityToken> 要素へのコア無装飾名参照 (XPointer 規定 [XPointer] で定義されたように)、または、セキュリティ・トークンを含んでいる外部のデータ・ソースへのコア参照を含む**必要がある (SHOULD)**。

次の例が、<wsse:BinarySecurityToken> 要素内に埋め込まれ、署名内部から URI により参照された証明書を示す。証明書は識別子として binarytoken をもつ <wsse:BinarySecurityToken> 要素として <wsse:Security> ヘッダ中に含まれている。 <ds:SignedInfo> 要素中の <ds:Reference> 要素で定義される署名の範囲は、URI 無装飾名ポインタ #binarytoken によって参照される署名用証明書を含む。 <ds:KeyInfo> 要素は、URI 無装飾名ポインタ #binarytoken によって証明書を参照する <wsse:Reference> 要素を含む <wsse:SecurityTokenReference> 要素によって署名鍵を指定する。

```
<S11:Envelope xmlns:S11="...">
   <S11:Header>
      <wsse:Security
           xmlns:wsse="..."
           xmlns:wsu="...">
         <wsse:BinarySecurityToken
              wsu:Id="binarytoken"
              ValueType="wsse:X509v3"
              EncodingType="wsse:Base64Binary">
            MIIEZzCCA9CgAwIBAgIQEmtJZc0…
         </wsse:BinarySecurityToken>
         <ds:Signature
              xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>…
               <ds:Reference URI="#body">…</ds:Reference>
               <ds:Reference URI="#binarytoken">…</ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>HFLP…</ds:SignatureValue>
            <ds:KeyInfo>
               <wsse:SecurityTokenReference>
                  <wsse:Reference URI="#binarytoken" />
               </wsse:SecurityTokenReference>
            </ds:KeyInfo>
         </ds:Signature>
      </wsse:Security>
   </S11:Header>
   <S11:Body wsu:Id="body"
        xmlns:wsu="...">
      …
   </S11:Body>
</S11:Envelope>
```

3.3.3 発行者および通し番号への参照

署名されたデータは、セキュリティ・トークン参照を含む <ds:KeyInfo> 要素へのコア無装飾名参照 (XPointer 規定 [XPointer] で定義されたように) を含む**必要がある (SHOULD)**。

次の例は、発行者名と通し番号によって参照される証明書を示す。この例では、メッセージに証明書が含まれていない。 <ds:SignedInfo> 要素により定義される署名の範囲は、メッセージ本体 (#body) および鍵情報要素 (#KeyInfo) の両方を含む。 <ds:KeyInfo> 要素は、<ds:X509IssuerSerial> 要素によって、指定された証明書の発行者と通し番号を指定する <wsse:SecurityTokenReference> を含む。

```
<S11:Envelope xmlns:S11="...">
   <S11:Header>
      <wsse:Security
           xmlns:wsse="..."
           xmlns:wsu="...">
         <ds:Signature
                xmlns:ds="...">
            <ds:SignedInfo>…
               <ds:Reference URI="#body"></ds:Reference>
               <ds:Reference URI="#keyinfo"></ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>HFLP…</ds:SignatureValue>
            <ds:KeyInfo Id="keyinfo">
               <wsse:SecurityTokenReference>
                  <ds:X509Data>
                     <ds:X509IssuerSerial>
                       <ds:X509IssuerName>
                          DC=ACMECorp, DC=com
                       </ds:X509IssuerName>
                       <ds:X509SerialNumber>12345678</X509SerialNumber>
                     </ds:X509IssuerSerial>
                  </ds:X509Data>
               </wsse:SecurityTokenReference>
            </ds:KeyInfo>
         </ds:Signature>
      </wsse:Security>
   </S11:Header>
   <S11:Body wsu:Id="body"
        xmlns:wsu="...">
      …
   </S11:Body>
</S11:Envelope>
```

3.4 暗号

暗号化された鍵またはデータは、ここで規定される X.509 セキュリティ・トークン型または参照のいずれかの方法を用いて暗号のために利用された対応する鍵を識別することによって、復号に必要とされる鍵を識別しても**よい (MAY)**。

唯一の目的は復号鍵を識別することであるため、信頼パスまたは証明書自身の特定の内容を指定する必要はない。

実装は、X509v3 証明書セキュリティ・トークンの Issuer と Serial Number への参照によって暗号鍵を指定することが**推奨される (RECOMMENDED)**。

次の例が、関連付けられた証明書の発行者名と通し番号によって参照された復号鍵を示す。この例では、メッセージに証明書が含まれていない。 <ds:KeyInfo> 要素が、<ds:X509IssuerSerial>

344 要素によって指定された証明書の発行者と通し番号を指定する <wsse:SecurityTokenReference>
345 要素を含む。

```
346 <S11:Envelope
347     xmlns:S11="..."
348     xmlns:ds="..."
349     xmlns:wsse="..."
350     xmlns:xenc="...">
351    <S11:Header>
352       <wsse:Security>
353          <xenc:EncryptedKey>
354             <xenc:EncryptionMethod Algorithm="…"/>
355             <ds:KeyInfo>
356                <wsse:SecurityTokenReference>
357                   <ds:X509IssuerSerial>
358                      <ds:X509IssuerName>
359                         DC=ACMECorp, DC=com
360                      </ds:X509IssuerName>
361                      <ds:X509SerialNumber>12345678</X509SerialNumber>
362                   </ds:X509IssuerSerial>
363                </wsse:SecurityTokenReference>
364             </ds:KeyInfo>
365             <xenc:CipherData>
366                <xenc:CipherValue>…</xenc:CipherValue>
367             </xenc:CipherData>
368             <xenc:ReferenceList>
369                <xenc:DataReference URI="#encrypted"/>
370             </xenc:ReferenceList>
371          </xenc:EncryptedKey>
372       </wsse:Security>
373    </S11:Header>
374    <S11:Body>
375       <xenc:EncryptedData Id="encrypted" Type="…">
376          <xenc:CipherData>
377             <xenc:CipherValue>…</xenc:CipherValue>
378          </xenc:CipherData>
379       </xenc:EncryptedData>
380    </S11:Body>
381 </S11:Envelope>
```

382 3.5 エラー・コード

383 X.509 証明書を利用するとき、WSS: SOAP Message Security 規定 [WS-Security] で定義された
384 エラー・コードが利用されなければ**ならない (MUST)**。

385 実装がカスタム・エラーを利用することを必要とするならば、Web Services Security: SOAP
386 Message Security 規定 [WS-Security] で定義されたコードの 1 つの拡張としてサブコードが定義
387 されることを推奨する。

4脅威モデルと対応策 (参考)

WS-Security での X.509 証明書の利用は、WSS: SOAP Message Security 規定 [WS-Security] で確認されたものを越える新しい脅威は導入しない。

メッセージ改変と盗聴に対しては、SOAP Message Security で説明される完全性と秘匿性の機構を利用することによって対応することができる。再送攻撃は、メッセージのタイムスタンプとキャッシュ、および他のアプリケーション固有の追跡機構を利用することにより対応することができる。 X.509 証明書に対しては、アイデンティティは鍵の利用によって認証されるので、中間者攻撃は通常回避できる。

重要な意味があり変更してはいけないメッセージ・データはすべて署名されることが強く**推奨される (RECOMMENDED)**。

SSL または TLS [RFC2246] のようなトランスポート・レベルでのセキュリティ・プロトコルが、WSS: SOAP Message Security specification [WS-Security] の代替としてまたは併せてメッセージとセキュリティ・トークンを防御するために利用されても**よい (MAY)** ことに注意されるべきである。

5参考文献

[Glossary] Informational RFC 2828, *Internet Security Glossary*, May 2000. http://www.ietf.org/rfc/rfc2828.txt

[KEYWORDS] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, RFC 2119, Harvard University, March 1997, http://www.ietf.org/rfc/rfc2119.txt.

[RFC2246] T. Dierks, C. Allen., *The TLS Protocol Version, 1.0.* IETF RFC 2246 January 1999. http://www.ietf.org/rfc/rfc2246.txt

[SOAP11] W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.

[SOAP12] W3C Recomendation**, "**http://www.w3.org/TR/2003/REC-soap12-part1-20030624/", 24 June 2003

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396, MIT/LCS, U.C. Irvine, Xerox Corporation, August 1998. http://www.ietf.org/rfc/rfc2396.txt

[WS-Security] OASIS,"Web Services Security: SOAP Message Security" 19 January 2004, http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0

[XML-ns] T. Bray, D. Hollander, A. Layman. *Namespaces in XML. W3C Recommendation.* January 1999. http://www.w3.org/TR/1999/REC-xml-names-19990114

[XML Signature] D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. *XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002. http://www.w3.org/TR/xmldsig-core/

[PKCS7] *PKCS #7: Cryptographic Message Syntax Standard* RSA Laboratories, November 1, 1993. http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html

[X509] ITU-T Recommendation X.509 (1997 E): Information Technology - *Open Systems Interconnection - The Directory: Authentication Framework*, June 1997.

[XPointer] Paul Grosso, Eve Maler, Jonathan Marsh, Norman Walsh, *XML Pointer Language (XPointer)*, W3C Recommendation 25 March 2003 http://www.w3.org/TR/xptr-framework/

Appendix A. 改版履歴

Rev	Date	What
01	18-Sep-02	Initial draft based on input documents and editorial review
03	30-Jan-03	Changes in title
04	19-May-03	Added by reference and pkipath modes of cert identification. Added section 1 introduction, changes to formatting etc.
05	6 June 2003	
06	20 June 2003	Included examples showing how tokens must be referenced from signatures and cipher values. Defined how key-agreement keys are to be conveyed in a Security header.
07	4 August 2003	Modifications to KeyIdentifier handling and use of SecurityTokenReference. Changes to the acknowledgements section.
08	6 August 2003	Reorganization of major sections to simplify flow
09	14 August 2003	Editorial corrections raised in off list emails.
10	19 August 2003	Editorial corrections raised in profile teleconference.
11	09 January 2004	Editorial corrections raised in forum
12	15 January 2004	Editorial correction, amend X509IssuerSerial usage
13	19 January 2004	Editorial corrections for name space and document name
14	17 Febuary 2004	Editorial corrections per Karl Best

Appendix B. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS は、本文書で記述された技術の実装や利用に関して主張される可能性がある知的財産や他の権利の正当性や範囲についてや、そのような権利のライセンスが利用可能または不可能かもしれないことについて、何の立場もとらないし、そのような権利を確認するために努力してきたとも主張しない。OASIS 仕様の権利に関する OASIS の手続き情報は OASIS ウェブサイトで見ることができる。公表のために利用可能となっている権利の主張の写しと利用可能となるであろうライセンスの保証、または、本仕様の実装者または利用者がそのような財産権を利用するための一般的なライセンスまたは許可を取得しようとした試みの結果は、OASIS Executive Director から取得することができる。
OASIS は、関心のあるものは誰でも、本仕様を実装するために必要とされる技術を対象とする著作権、特許または特許申請、または、他の財産権についての注意をうながしてもらうようお願いする。このような情報については、OASIS Executive Director に連絡してほしい。

484 Property Rights 文書中で定義される著作権のための手続きにしたがわなければならない) や英語
485 以外の言語へ翻訳するために必要とされる場合を除いて、本文書自身は著作権表示または
486 OASIS への参照を削除するなどどのような方法でも改変できない。
487 上で付与した制限付きの許可は永続的なものであり、OASIS もしくはその後継者または任命者
488 によって取り消されることはない。
489 本文書およびここに含まれる情報は「現状有姿」のままで提供され、**この情報の利用がどのよ**
490 **うな権利も侵害しないという保証や、商品性や特定の目的への適応性についての暗黙の保証を**
491 **含むがこれらに限らず、明示的または暗示的を問わず、一切の保証を OASIS は行なわない。**
492 本節は参考である。