Web Services Security:
SOAP Message Security 1.0
(WS-Security 2004)
Errata 1.0

Committee Draft 200512, December 2005
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):

西村 利浩	NISHIMURA, Toshihiro	富士通株式会社

日本語訳貢献者 (Contributors):

秋本 諭史	AKIMOTO, Satoshi	大日本印刷株式会社
松永 豊	MATSUNAGA, Yutaka	東京エレクトロン株式会社
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

LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL XML CONSORTIUM, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, 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。

この翻訳の元となった文書 (英文) は英文仕様書の行番号と記述を引用していますが、この翻訳では英文仕様書の日本語訳の行番号と記述に置き換えることにより、英文の意図する内容を表しています。

Web Services Security:
SOAP Message Security 1.0
(WS-Security 2004)
Errata 1.0
Committee Draft 200512, December 2005

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

Document Location:
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0-errata-004

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

Editor:

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

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
Yutaka	Kudo	Hitachi
Jason	Rouault	HP
Paula	Austel	IBM
Bob	Blakley	IBM
Joel	Farrell	IBM
Satoshi	Hada	IBM
Maryann	Hondo	IBM
Michael	McIntosh	IBM
Hiroshi	Maruyama	IBM
David	Melgar	IBM
Anthony	Nadalin	IBM
Nataraj	Nagaratnam	IBM
Wayne	Vicknair	IBM
Kelvin	Lawrence	IBM (co-Chair)
Don	Flinn	Individual
Bob	Morgan	Individual
Bob	Atkinson	Microsoft
Keith	Ballinger	Microsoft
Allen	Brown	Microsoft
Paul	Cotton	Microsoft
Giovanni	Della-Libera	Microsoft
Vijay	Gajjala	Microsoft
Johannes	Klein	Microsoft
Scott	Konersmann	Microsoft
Chris	Kurt	Microsoft
Brian	LaMacchia	Microsoft
Paul	Leach	Microsoft
John	Manferdelli	Microsoft
John	Shewchuk	Microsoft
Dan	Simon	Microsoft
Hervey	Wilson	Microsoft
Chris	Kaler	Microsoft (co-Chair)
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
Mark	Hays	Verisign
Hemma	Prafullchandra	VeriSign

Abstract:
本文書は WSS Technical Committee により承認された WSS OASIS Standard Version 1.0 に対する正誤リストを含んでいる。

Status:
正誤表の本版は委員会の作業ドラフトである。したがって、将来の OASIS Standard への統合の前に変更となるかもしれない。コメントは編集者へ送付されたい。もし wss@lists.oasis-open.org リストに含まれているならば、コメントはそこに送付されたい。そのリストに含まれていないなら、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、メッセージの本体として"subscribe"という言葉を入れて wss-comment-request@lists.oasis-open.org へ email メッセージを送付のこと。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。一般的な OASIS IPR 情報は http://www.oasis-open.org/who/intellectualproperty.shtml に見つけることができる。

Table of Contents

95 # 1解決された問題点

96 次の問題点が本文書で解決されている

問題点	説明
327	TimestampのValueTypeを明確にする必要がある
328	STR変換の誤り
256	STR属性が保護されていない
264	レビュー期間後のコメント: WSSコアとusername/x.509プロファイルの例の間違い
290	コアとSAMLの間で、KeyIdentifier符号化型のデフォルト値に矛盾がある
444	WSSページからWS-Security 1.0 errataを削除するか、修正するよう要望

2誤字

2.1 「7.1 SecurityTokenReference 要素」

次の行 (655) を削除する:

このオプションの属性は <wsse:SecurityToken> の使用法の分類のために利用される。使用

そして次の行に置き換える:

このオプションの属性は <wsse:SecurityTokenReference> の使用法の分類のために利用される。使用

3規定に関する誤り

3.1 「2.2 名前空間」

行 221-224 を削除する:

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

そして、次に置き換える:

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

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

3.2 「4.2 Id スキーマ」

行 436 を削除する:

"`http://www.w3.org/2001/XMLSchema`" で {name} が "Id" である [type definition] をその

そして次に置き換える:

"`http://www.w3.org/2001/XMLSchema`" で {name} が "ID" である [type definition] をその

3.3 「5 Security ヘッダ」

行 509 を削除する:

らば、フォルトを生成しなければならない。

そして次に置き換える:

らば、フォルトを生成しなければ**ならない (MUST)**。

3.4 「7.1 SecurityTokenReference 要素」

行 639 を削除する:

<wsse:SecurityTokenRefeference> が <wsse:Security> ヘッダ部の外で利用される場合、応答

そして次に置き換える:

<wsse:SecurityTokenRefeference> がセキュリティ・ヘッダを処理している部分の外で利用される場合、応答

3.5 「7.2 鍵識別子」

(訳注：「7.3 鍵識別子」の誤りと思われる)

行 735 の後に次を加える:

<wsse:KeyIdentifier>要素は<wsse:SecurityTokenReference>要素の内部でのみ許される。

3.6 「7.3 鍵識別子」

行 759 の表を削除する:

URI	説明
#Base64Binary	XML Schema base 64 符号化(デフォルト)

そして次に置き換える:

URI	説明
#Base64Binary	XML Schema base 64 符号化

次の行を削除する:(訳注：以下は英文での 1834 行目、訳では 1794 行目で「Appendix B. SecurityTokenReference モデル」の内容と思われる)

号化されているかを指定する。例えば、ハッシュ値が base 64 符号化 (デフォルト) を利用し

そして次に置き換える:

号化されているかを指定する。例えば、ハッシュ値が base 64 符号化を利用し

3.7 「7.4 埋め込まれた参照」

スキーマでは ValueType 属性があるが wsu:Id 属性がない。ValueType が wsu:Id に置き換えられる必要がある。

行 766 の後に次を加える:

<wsse:Embedded>要素は<wsse:SecurityTokenReference>要素の内部でのみ許される。

3.8 「8.1 アルゴリズム」

表の中の URI を削除する (行 855):

http://www.w3.org/TR/2003/NOTE-soap12-n11n-20030328/

そして次に置き換える:

http://www.w3.org/TR/soap12-n11n/

3.9 「8.3 トークンへの署名」

(訳注：「10 セキュリティ・タイムスタンプ」の誤りと思われる)

行 1277-1279 を削除する:

160 成**してはならない (MUST NOT)**。しかしながら、もし他の時刻型が利用されるなら、(以下で
161 説明される) ValueType 属性が時刻形式のデータ型を示すために指定されなければ**ならない**
162 **(MUST)**。

163 そして次に置き換える:

164 成**してはならない (MUST NOT)**。

4規定外の誤り

4.1 「3.4 例」

行 330-333 を削除する:

```
(005)         <xxx:CustomToken wsu:Id="MyID"
                              xmlns:xxx="http://fabrikam123/token">
(006)             FHUIORv...
(007)         </xxx:CustomToken>
```

そして次に置き換える:

```
(005)         <wsse:BinarySecurityToken ValueType=”
http://fabrikam123#CustomToken “
      EncodingType=”...#Base64Binary » wsu:Id=” MyID “>
(006)             FHUIORv...
(007)         </wsse:BinarySecurityToken>
```

4.2 「6.2.1 利用者名」

行 544 を削除する:

このセキュリティ・トークンのための文字列ラベル。

そして次に置き換える:

このセキュリティ・トークンのための文字列ラベル。wsu:Id はオープンな属性モデルを許す。

4.3 「6.3.2 バイナリ・セキュリティ・トークンの符号化」

行 611-617 を削除する:

<wsse:BinarySecurityToken> が署名に含められるとき - すなわち、<ds:Signature> 要素から参照されるとき - カノニカリゼーション・アルゴリズム (例えば、Exclusive XML Canonicalization [EXC-C14N]) が属性または要素値の中で利用されている QName の名前空間接頭辞の認可されない置換を許さないように注意すべきである。特に、もしトークンが検証用の鍵を運ばない(そして、その結果それは暗号的に署名に結びつけられない)ならばこれらの名前空間接頭辞は <wsse:BinarySecurityToken> 要素の中で宣言しておくことが**推奨される (RECOMMENDED)**。

置き換えのテキストは必要ない。QName は URI に置き換えられた。

4.4 「7.3 鍵識別子」

行 755-758 を削除する:

/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType

オプションの EncodingType 属性は、URI を利用して、KeyIdentifier の符号化形式(＃Base64Binary)を示すために利用される。本規定により定義される基本の値が利用される (URI フラグメントは本文書の URI に相対的であることに注意):

そして次に置き換える:

/wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType

オプションの EncodingType 属性は、URI を利用して、KeyIdentifier の符号化形式(＃Base64Binary)を示すために利用される。本規定では、次の表にある EncodingType URI 値を定義する。トークン固有のプロファイルが追加のトークン固有の EncodingType URI 値を定義してもよい **(MAY)**。ValueType が符号化型を識別するのに十分でない場合、KeyIdentifier は EncodingType 属性を含まなければならない **(MUST)**。

4.5 「8.3 トークンへの署名」

次の行 (1021-1022) を削除する:

変換は単一の必須のパラメタ <ds:CanonicalizationMethod> をもち、入力ノード集合のシリアライズのために利用される。

そして次に置き換える:

変換は単一の必須のパラメタ <ds:CanonicalizationMethod> をもち、出力ノード集合のシリアライズのために利用される。

4.6 「11 拡張例」

行 1375-1380 を削除する:

```
(015)             <ds:KeyInfo>
(016)                <wsse:KeyIdentifier
                         EncodingType="...#Base64Binary"
                  ValueType="...#X509v3">MIGfMa0GCSq...
(017)                </wsse:KeyIdentifier>
(018)             </ds:KeyInfo>
```

そして次に置き換える:

```
(015)             <ds:KeyInfo>
                       <wsse:SecurityTokenReference>
(016)                        <wsse:KeyIdentifier
                                    EncodingType="...#Base64Binary"
                             ValueType="...#X509v3">MIGfMa0GCSq...
(017)                        </wsse:KeyIdentifier>
                       </wsse:SecurityTokenReference>
(018)             </ds:KeyInfo>
```

5明確化

5.1 「8.3 トークンへの署名」

SecurityTokenReference (STR)への署名は認証と完全性保護を STR に対してのみ提供し、参照されたセキュリティ・トークン (ST)に対しては提供しない。ST に署名することを意図するならば、ダイジェスト計算のために STR を ST で置き換え、STR ではなく ST を効果的に保護する STR Dereference Transform (STRDT)が利用されてもよい。ST と STR の両方の保護を望むなら、STR を二度、一度は STRDT を利用し一度は STRDT を利用しないで、署名してもよい。

次の表に仕様で参照される各 URI フラグメントに対する完全 URI を列挙する。

URI フラグメント	完全 URI
#Base64Binary	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary
#STR-Transform	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#STR-Transform
#X509	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509

Appendix A. 改版履歴

Rev	Date	What
1	06/25/04	First Draft of Errata
2	07/06/04	Updated per comments on list
3	0919/04	Updated per comments on list
4	10/01/04	Updated per comments on list
5	12/07/05	Issue 444

本節は参考とする。

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.

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。

本節は参考である。