
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

免責事項 (disclaimer notice):

This translated document is provided by XML Consortium as an informational service to the global community. This is an unofficial, non-normative translation of the official document, Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) Errata 1.0, located at <http://www.oasis-open.org/committees/download.php/16792/oasis-200512-wss-soap-message-security-1.0-errata-005.pdf>, © copyright OASIS 2002-2005. This translation is published with acknowledgement of and in agreement with terms specified in the OASIS Translation Policy. Neither OASIS nor XML Consortium assume responsibility for any errors contained herein.

本翻訳文書は、XML コンソーシアムによって世界中の地域社会に提供される情報サービスです。これは、<http://www.oasis-open.org/committees/download.php/16792/oasis-200512-wss-soap-message-security-1.0-errata-005.pdf> に掲載された公文書 Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) Errata 1.0、copyright OASIS 2002-2005 の非公式かつ非規範的な翻訳です。本翻訳は OASIS 翻訳方針に規定された条件を認知し、かつこれに同意の上で公表されます。OASIS および XML コンソーシアムでは、ここに含まれるいかなる誤りについてもその責任は負いません。

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT

28 LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT,
29 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL
30 XML CONSORTIUM, BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT,
31 INDIRECT, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING,
32 WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS
33 INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS)
34 ARISING OUT OF THIS DOCUMENT.

35 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
36 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
37 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
38 律上のいかなる責任も負いません。

39 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
40 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
41 ています。



42

43

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

44

45

Errata 1.0

46

47

Committee Draft 200512, December 2005

48

Document identifier:

49

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

50

Document Location:

51

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

52

Errata Location:

53

<http://www.oasis-open.org/committees/wss>

54

Editor:

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

55

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	Entegritty
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

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

59 **Status:**
60 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
61 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-](mailto:wss@lists.oasis-open.org)
62 [open.org](mailto: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
63 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。
64 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-](mailto:wss-comment-request@lists.oasis-open.org)
65 [request@lists.oasis-open.org](mailto: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
66 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-](http://www.oasis-open.org/committees/wss/ipr.php)
67 [open.org/committees/wss/ipr.php](http://www.oasis-open.org/committees/wss/ipr.php) にある OASIS Web Services Security Technical Committee
68 (WSS TC)の Intellectual Property Rights の部分を参照のこと。一般的な OASIS IPR 情報は
69 <http://www.oasis-open.org/who/intellectualproperty.shtml> に見つけることができる。

70 **Table of Contents**

71	1	解決された問題点	7
72	2	誤字	8
73	2.1	「7.1 SecurityTokenReference 要素」	8
74	3	規定に関する誤り	9
75	3.1	「2.2 名前空間」	9
76	3.2	「4.2 Id スキーマ」	9
77	3.3	「5 Security ヘッダ」	9
78	3.4	「7.1 SecurityTokenReference 要素」	9
79	3.5	「7.2 鍵識別子」	9
80	3.6	「7.3 鍵識別子」	10
81	3.7	「7.4 埋め込まれた参照」	10
82	3.8	「8.1 アルゴリズム」	10
83	3.9	「8.3 トークンへの署名」	10
84	4	規定外の誤り	12
85	4.1	「3.4 例」	12
86	4.2	「6.2.1 利用者名」	12
87	4.3	「6.3.2 バイナリ・セキュリティ・トークンの符号化」	12
88	4.4	「7.3 鍵識別子」	12
89	4.5	「8.3 トークンへの署名」	13
90	4.6	「11 拡張例」	13
91	5	明確化	14
92	5.1	「8.3 トークンへの署名」	14
93		Appendix A. 改版履歴	15
94		Appendix B. Notices	16

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

97

2 誤字

98

2.1 「7.1 SecurityTokenReference 要素」

99

次の行 (655) を削除する:

100

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

101

そして次の行に置き換える:

102

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。

103

使用

104

105 3 規定に関する誤り

106 3.1 「2.2 名前空間」

107 行 221-224 を削除する:

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

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

110 そして、次に置き換える:

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

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

113 3.2 「4.2 Id スキーマ」

114 行 436 を削除する:

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

116 そして次に置き換える:

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

118 3.3 「5 Security ヘッダ」

119 行 509 を削除する:

120 らば、フォルトを生成しなければならない。

121 そして次に置き換える:

122 らば、フォルトを生成しなければならない (MUST)。

123 3.4 「7.1 SecurityTokenReference 要素」

124 行 639 を削除する:

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

126 そして次に置き換える:

127 <wsse:SecurityTokenReference> 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

128 れる場合、応答

129 3.5 「7.2 鍵識別子」

130 (訳注: 「7.3 鍵識別子」の誤りと思われる)

131 行 735 の後に次を加える:

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

133 **3.6 「7.3 鍵識別子」**

134 行 759 の表を削除する:

135

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

136 そして次に置き換える:

137

URI	説明
#Base64Binary	XML Schema base 64 符号化

138

139 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.
140 SecurityTokenReference モデル」の内容と思われる)

141 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

142 そして次に置き換える:

143 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

144

145

146 **3.7 「7.4 埋め込まれた参照」**

147 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
148 れる必要がある。

149

150 行 766 の後に次を加える:

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

152 **3.8 「8.1 アルゴリズム」**

153 表の中の URI を削除する (行 855):

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

155 そして次に置き換える:

156 <http://www.w3.org/TR/soap12-n11n/>

157 **3.9 「8.3 トークンへの署名」**

158 (訳注: 「10 セキュリティ・タイムスタンプ」の誤りと思われる)

159 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**)。

165

4 規定外の誤り

166

4.1 「3.4 例」

167 行 330-333 を削除する:

```
168 (005) <xxx:CustomToken wsu:Id="MyID"  
169                                xmlns:xxx="http://fabrikaml23/token">  
170 (006)     FHUIORv...  
171 (007) </xxx:CustomToken>
```

172 そして次に置き換える:

```
173 (005) <wsse:BinarySecurityToken ValueType="  
174 http://fabrikaml23#CustomToken "  
175     EncodingType="...#Base64Binary » wsu:Id=" MyID ">  
176 (006)     FHUIORv...  
177 (007) </wsse:BinarySecurityToken>
```

178

4.2 「6.2.1 利用者名」

179 行 544 を削除する:

180 このセキュリティ・トークンのための文字列ラベル。

181 そして次に置き換える:

182 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。

183

4.3 「6.3.2 バイナリ・セキュリティ・トークンの符号化」

184 行 611-617 を削除する:

185 <wsse:BinarySecurityToken> が署名に含められるとき - すなわち、<ds:Signature> 要素から参
186 照されるとき - カノニカルゼーション・アルゴリズム (例えば、Exclusive XML
187 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
188 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
189 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
190 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**
191 **(RECOMMENDED)**。

192

193 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。

194

4.4 「7.3 鍵識別子」

195 行 755-758 を削除する:

196 /wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType

197 オプションの EncodingType 属性は、URI を利用して、KeyIdentifier の符号化形式(#
198 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
199 ラグメントは本文書の URI に相対的であることに注意):

200 そして次に置き換える:

201 /wsse:SecurityTokenReference/wsse:KeyIdentifier/@EncodingType

202 オプションの EncodingType 属性は、URI を利用して、KeyIdentifier の符号化形式(#
203 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
204 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
205 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
206 EncodingType 属性を含まなければならない (MUST)。

207 4.5 「8.3 トークンへの署名」

208 次の行 (1021-1022) を削除する:

209 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
210 ライズのために利用される。

211 そして次に置き換える:

212 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
213 ライズのために利用される。

214 4.6 「11 拡張例」

215 行 1375-1380 を削除する:

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

222 そして次に置き換える:

```
223 (015) <ds:KeyInfo>  
224 <wsse:SecurityTokenReference>  
225 (016) <wsse:KeyIdentifier  
226 EncodingType="...#Base64Binary"  
227 ValueType="...#X509v3">MIGfMa0GCSq...  
228 (017) </wsse:KeyIdentifier>  
229 </wsse:SecurityTokenReference>  
230 (018) </ds:KeyInfo>
```

231

5 明確化

232

5.1 「8.3 トークンへの署名」

233 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
234 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
235 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
236 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
237 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
238 い。

239

240 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

241

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	09/19/04	Updated per comments on list
4	10/01/04	Updated per comments on list
5	12/07/05	Issue 444

242

243 本節は参考とする。

Appendix B. Notices

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

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

257 Copyright © OASIS Open 2002-2004. *All Rights Reserved.*

258 This document and translations of it may be copied and furnished to others, and derivative
259 works that comment on or otherwise explain it or assist in its implementation may be prepared,
260 copied, published and distributed, in whole or in part, without restriction of any kind, provided
261 that the above copyright notice and this paragraph are included on all such copies and
262 derivative works. However, this document itself does not be modified in any way, such as by
263 removing the copyright notice or references to OASIS, except as needed for the purpose of
264 developing OASIS specifications, in which case the procedures for copyrights defined in the
265 OASIS Intellectual Property Rights document must be followed, or as required to translate it
266 into languages other than English.

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

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

274 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
275 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
276 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
277 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
278 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
279 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
280 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
281 から取得することができる。

282 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
283 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おう願
284 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。

285 Copyright © OASIS Open 2002-2004. *All Rights Reserved.*

286 上記著作権表示とこの段落が全ての複製と派生物に含められるなれば、本文書とその翻訳は複製
287 され他者へ提供されてもよく、それを解説したり説明したり、その実装を援助する派生的作業は、

288 全てであれ一部であれ何の制限もなく、準備され、公表され、配布されてもよい。しかしながら、
289 OASIS 仕様を開発するという目的のために必要とされる場合（この場合、OASIS Intellectual
290 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
291 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
292 OASIS への参照を削除するなどのような方法でも改変できない。
293 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
294 によって取り消されることはない。

295 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
296 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
297 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。

298

299 本節は参考である。

300