
1 **Web Services Security:**
2 **UsernameToken Profile 1.0**
3 **Errata 1.0**
4 **Committee Draft 200401, September 2004**
5 **日本語訳 2006 年 7 月**

6 **日本語訳作成 (Japanese Translation):**
7 XML コンソーシアム セキュリティ部会 (XML Consortium Security SIG)

8 **日本語訳編集 (Editors):**

山根 利夫	YAMANE, Toshio	株式会社日立製作所
-------	----------------	-----------

9 **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
西村 利浩	NISHIMURA, Toshihiro	富士通株式会社

10 **免責事項 (disclaimer notice):**

11 This translated document is provided by XML Consortium as an informational service
12 to the global community. This is an unofficial, non-normative translation of the official
13 document, Web Services Security: Username Token Profile 1.0 Errata 1.0, located at
14 <http://www.oasis-open.org/committees/download.php/11143/oasis-200401-wss-username-token-profile-1.0-errata-004.pdf>, © copyright OASIS 2002-2004. This
15 translation is published with acknowledgement of and in agreement with terms
16 specified in the OASIS Translation Policy. Neither OASIS nor XML Consortium
17 assume responsibility for any errors contained herein.
18

19 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
20 ービスです。これは、[http://www.oasis-](http://www.oasis-open.org/committees/download.php/11143/oasis-200401-wss-username-token-profile-1.0-errata-004.pdf)
21 [open.org/committees/download.php/11143/oasis-200401-wss-username-token-profile-](http://www.oasis-open.org/committees/download.php/11143/oasis-200401-wss-username-token-profile-1.0-errata-004.pdf)
22 [1.0-errata-004.pdf](http://www.oasis-open.org/committees/download.php/11143/oasis-200401-wss-username-token-profile-1.0-errata-004.pdf) に掲載された公文書 Web Services Security: UsernameToken
23 Profile 1.0 Errata 1.0、copyright OASIS 2002-2004 の非公式かつ参照的な翻訳です。
24 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

25 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
26 いてもその責任は負いません。

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

37 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
38 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
39 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
40 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。

41 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、
42 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
43 意図する内容を表しています。



44

45

Web Services Security:

46

UsernameToken Profile 1.0

47

Errata 1.0

48

Committee Draft 200401, September 2004

49

50

Document identifier:

51

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

52

Document Location:

53

[http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0-](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0-errata-003)

54

[errata-003](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0-errata-003)

55

Errata Location:

56

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

57

Editor:

Anthony	Nadalín	IBM
Phil	Griffin	Individual
Chris	Kaler	Microsoft
Phillip	Hallam-Baker	VeriSign
Ronald	Monzillo	Sun

58

Contributors:

Gene	Thurston	AmberPoint
Frank	Siebenlist	Argonne National Lab
Merlin	Hughes	Baltimore Technologies
Irving	Reid	Baltimore Technologies
Peter	Dapkus	BEA

WSS: UsernameToken Profile1.0 Errata1.0 September 2004

Copyright © OASIS Open 2002-2006. All Rights Reserved.

Translated by XML Consortium.

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

59 **Abstract:**
60 本文書は WSS Technical Committee により承認された WSS Username Token Profile
61 1.0 に対する正誤リストを含んでいる。

62 **Status:**
63 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
64 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
65 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。
66 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
67 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
68 "subscribe"という言葉を入れて wss-comment-request@lists.oasis-open.org へ email メ
69 ッ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
70 条項の提供については、<http://www.oasis-open.org/committees/wss/ipr.php> にある
71 OASIS Web Services Security Technical Committee (WSS TC)の Intellectual Property
72 Rights の部分を参照のこと。一般的な OASIS IPR 情報は [http://www.oasis-](http://www.oasis-open.org/who/intellectualproperty.shtml)
73 [open.org/who/intellectualproperty.shtml](http://www.oasis-open.org/who/intellectualproperty.shtml) に見つけることができる。

WSS: UsernameToken Profile1.0 Errata1.0 September 2004

Copyright © OASIS Open 2002-2006. All Rights Reserved.

Page 6 of 18

Translated by XML Consortium.

74 **Table of Contents**

75	1	解決された問題点	8
76	2	誤字	9
77	3	規定に関する誤り	10
78	3.1	「2.2 名前空間」	10
79	3.2	「3.1 ユーザ名とパスワード」	10
80	3.3	「3.2 トークン参照」	11
81	3.4	「3.4 キー導出」	11
82	3.5	「4 セキュリティ考察」	12
83	4	規定外の誤り	14
84	5	明確化	15
85		Appendix A. 改版履歴	16
86		Appendix B. Notices	17

87

1 解決された問題点

88

次の問題点が本文書で解決される

問題点	説明
259	V1 レビュー以降の UserName Profile に対する、編集上のコメント

89

2誤字

90

なし

91 3 規定に関する誤り

92 3.1 「2.2 名前空間」

93 行 113 の後に以下を追加する:

94 WSS:Username Token Profile 1.0 で規定する URI フラグメントは、以下の URI に相対
95 的である

96 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0>

97 3.2 「3.1 ユーザ名とパスワード」

98 行(121)を削除する:

99 wsse:PasswordText 型 と wsse:PasswordDigest 型 のパスワードは実際のパスワードに
100 限定は

101 そして次に置き換える:

102 PasswordText 型 と PasswordDigest 型 のパスワードは実際のパスワードに限定は

103

104 行(123-124)を削除する

105 wsse:PasswordText 型 に対する wsse:PasswordDigest 型 についても

106 そして次に置き換える

107 wsse:PasswordText 型 を持つ、ということは

108

109 行(130)を削除する

110 wsse:PasswordText 型 および wsse:PasswordDigest 型 のパスワードは UTF8 符号化さ
111 れた

112 そして次に置き換える

113 PasswordDigest 型 のパスワードは UTF8 符号化された

114

115 行(134)を削除する

116 wsse:PasswordText および wsse:PasswordDigest を利用することに比べて実際の付加
117 的な

118 そして次に置き換える

119 PasswordText を利用することに比べて実際の付加的な

120

121 行(164)を削除する
122 wsse:PasswordDigest は、平文パスワード (またはパスワード同等のもの) が要求者と
123 受信
124 そして次に置き換える
125 PasswordDigest は、平文パスワード (またはパスワード同等のもの) が要求者と受信
126
127
128 (訳注 : 以下 3.2 章修正の誤り)
129 行(262)を削除する
130 属性は必要とされない。もし指定されるなら、<wsse:UsernameToken> の値が指定さ
131 れなけ
132 そして次に置き換える
133 属性は必要とされない。もし指定されるなら、#UsernameToken の値が指定されなけ

134 **3.3 「3.2 トークン参照」**

135 行(262)を削除する
136 属性は必要とされない。もし指定されるなら、<wsse:UsernameToken> の値が指定さ
137 れなけ
138 そして次に置き換える
139 属性は必要とされない。もし指定されるなら、#UsernameToken の値が指定されなけ

140 **3.4 「3.4 キー導出」**

141 以下を新しい節として行(283)の後に追加する。
142 ユーザ名に伴うパスワードは、メッセージの内容を保護し、完全性や、機密性を保持す
143 るための共通秘密キーを導出するために使用してもよい。本節では、そのようなキーを
144 導出するための拡張スキーマ及び手続きを定義する。この手続きは、相互運用性を確保
145 するため、パスワードからキーを導出する場合には適用しなければ**ならない (MUST)**。
146 但し、パスワードは各種攻撃の対象であり、それが導出されたキーの漏洩に繋がること
147 を考慮しなければならない。キー導出手順は、出来る限り攻撃のリスクを最小限とする
148 よう意図しているが、人間が記憶して、標準キーボードから入力するという、パスワー
149 ドの危うさによる限界が有る。この問題に関する詳細は、次章「セキュリティの考慮事
150 項」に述べる。
151 パスワードからのキー導出を可能とするため、更に2つの要素が必要であり、それらは
152 <wsse:Salt>と<wsse:Iteration>である。これ等の値は秘密ではなく、キー導出を使用す
153 る場合はユーザ名トークンに含めて送られなければならない。また、キー導出を使用す
154 る場合は、ユーザ名トークンにパスワードを含めては**ならない(MUST)**。

155 受信者は、自分が知っているパスワードを基に、送信者と同じキーを導出する。

156 以下に<wsse:Salt>と<wsse:Iteration>の文法を示す。

```
157 <wsse:UsernameToken wsse:Id="...">  
158 <wsse:Username>...</wsse:Username>  
159 <wsse:Salt>...</wsse:Salt>  
160 <wsse:Iteration>...</wsse:Iteration>  
161 </wsse:UsernameToken>
```

162 これらの要素の説明は以下の通り。

163 /wsse:UsernameToken/wsse:Salt

164 この要素は下記のように、パスワードと結合され、128 ビットの 16 進数で示される。

165 /wsse:UsernameToken/wsse:Iteration

166 この要素は、キーを導出するため、何回ハッシング操作を繰り返すかを示す。10 進数
167 で指定し、指定の無い場合 1000 が仮定される。

168 パスワードから導出されたキーは、Message Authentication Code(MAC)の計算や、暗
169 号化のための対称キーとして使用される。MACで使用する場合、キー長は常に 160 ビ
170 ットである。暗号化に使用する場合、160 ビット以上のキー長を必要とするアルゴリズム
171 を使用してはならない (MUST NOT)。

172 キーの上位ビットの必要な長さが暗号化に使用され、不要な下位ビットは捨てられる。
173 例えば AES-128 の場合、導出された 160 ビットの、上位 128 ビットが使用され、下位
174 32 ビットは捨てられる。

175 <wsse:Salt>要素は以下のように構成される。Salt の上位 8 ビットは、MAC で使用され
176 る場合は 01 であり、暗号化で使用される場合は 02 である。Salt の残りの下位 120 ビッ
177 トは乱数とする **必要がある(SHOULD)**。キーは以下のように導出される。パスワードと
178 Salt は、この順番で結合される。パスワードの実際のオクテットが使用され、0 等で埋
179 め字されることは無い。この値は SHA1 アルゴリズムによりハッシュされる。その結果
180 はまた SHA1 を使ってハッシュされる。この手順が、ハッシュ処理回数が Iteration 数に
181 等しくなるまで繰り返される。言い換えると:

182 $K1 = \text{SHA1}(\text{password} + \text{Salt})$

183 $K2 = \text{SHA1}(K1)$

184 $Kn = \text{SHA1}(Kn-1)$

185 ここで、+ は結合を表し、n は Iteration 数を表す。結果の 160 ビットは MAC 機能に使
186 用されるか、適当な長さに縮めて、暗号化に使用される。

187 3.5 「4 セキュリティの考慮事項」

188 以下を行(308)の後ろに追加する。

189 パスワードから導出されたキーによる安全性は、パスワード自体に対する推測攻撃や総
190 当たり攻撃があるため、限界がある。人間が記憶できる長さ、容易にキー入力できるオク
191 テット数の限界から、典型的なパスワードは、最大 50 ビット相当の情報量に相当する。

192 このためキー長は最大 160 ビットとなっている。これ以上のキー長は、安全性を高めず
193 に処理だけを増加させる。

194 本書に示したキー導出のアルゴリズムは、RFC2898 に述べられている。その中では
195 PBKDF1 として参照されている。これはより単純で、160 ビットを超えるキーを要求さ
196 れないため、PBKDF2 に代えて使用されている。

197 Salt の目的は、知られてしまったパスワードに対し、大量の計算によりキー値をテスト
198 される事を防ぐ事である。Salt の値は、MAC や暗号化のキーが、同じパスワードから
199 導出されたとしても異なる値を持つことを保証する。これが暗号解析攻撃を防ぐ。

200 Iteration 数は、キー導出のコストを余り増やさずに、推測攻撃や、総当り攻撃での作業
201 量を増やすことを目的としている。Iteration 数は、少なくとも 1000(デフォルト)とす
202 る必要がある。

203

204	4 規定外の誤り
205	なし
206	

207

5 明確化

208

下記の表は、本書で参照する URI フラグメントの、完全 URI を示す。

URI フラグメント	完全 URI
#PasswordDigest	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordDigest
#PasswordText	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText
#UsernameToken	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#UsernameToken

209

210 **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

211

212 本節は参考とする。

213 Appendix B. Notices

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

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

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

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

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

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

246 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
247 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
248 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
249 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
250 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
251 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
252 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

253 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
254 る。
255 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に対
256 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
257 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
258 絡してほしい。

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

260 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
261 訳は複製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
262 する派生的作業は、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
263 されてもよい。しかしながら、OASIS 仕様を開発するという目的のために必要とされ
264 る場合（この場合、OASIS Intellectual Property Rights 文書中で定義される著作権のた
265 めの手続きにしたがわなければならない）や英語以外の言語へ翻訳するために必要とさ
266 れる場合を除いて、本文書自身は著作権表示または OASIS への参照を削除するなど
267 のような方法でも改変できない。

268 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
269 は任命者によって取り消されることはない。

270 **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**
271 **どのよ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**
272 **暗黙の保証を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**
273 **OASIS は行なわない。**

274

275 本節は参考である。

276