Web Services Security: UsernameToken Profile 1.0 Errata 1.0

Committee Draft 200401, September 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):

山根 利夫	YAMANE, Toshio	株式会社日立製作所

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

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 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: UsernameToken Profile 1.0 Errata 1.0

Committee Draft 200401, September 2004

Document identifier:
{WSS: SOAP Message Security }-{UsernameToken Profile}-{1.0} (Word) (PDF)
Document Location:
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0-errata-003
Errata Location:
http://www.oasis-open.org/committees/wss

Editor:

Anthony	Nadalin	IBM
Phil	Griffin	Individual
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 Username Token Profile 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

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

3規定に関する誤り

3.1 「2.2 名前空間」

行 113 の後に以下を追加する:

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

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

3.2 「3.1 ユーザ名とパスワード」

行(121)を削除する:

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

そして次に置き換える:

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

行(123-124)を削除する

wsse:PasswordText 型に対する wsse:PasswordDigest 型についても

そして次に置き換える

wsse:PasswordText 型を持つ、ということは

行(130)を削除する

wsse:PasswordText 型および wsse:PasswordDigest 型のパスワードは UTF8 符号化された

そして次に置き換える

PasswordDigest 型のパスワードは UTF8 符号化された

行(134)を削除する

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

そして次に置き換える

PasswordText を利用することに比べて実際の付加的な

行(164)を削除する

wsse:PasswordDigest は、平文パスワード (またはパスワード同等のもの) が要求者と受信

そして次に置き換える

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

（訳注：以下 3.2 章修正の誤り）

行(262)を削除する

属性は必要とされない。もし指定されるなら、<wsse:UsernameToken> の値が指定されなけ

そして次に置き換える

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

3.3 「3.2 トークン参照」

行(262)を削除する

属性は必要とされない。もし指定されるなら、<wsse:UsernameToken> の値が指定されなけ

そして次に置き換える

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

3.4 「3.4 キー導出」

以下を新しい節として行(283)の後に追加する。

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。**

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項」に述べる。

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 <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)。**

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。

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

```
            <wsse:UernameToken wsse:Id="...">
                <wsse:Username>...</wsse:Username>
                <wsse:Salt>...</wsse:Salt>
                <wsse:Iteration>...</wsse:Iteration>
            </wsse:UsernameToken>
```

これらの要素の説明は以下の通り。

/wsse:UsernameToken/wsse:Salt

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。

/wsse:UsernameToken/wsse:Iteration

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 進数で指定し、指定の無い場合 1000 が仮定される。

パスワードから導出されたキーは、Message Authentification Code(MAC)の計算や、暗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を使用**してはならない（MUST NOT)。**

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。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 32 ビットは捨てられる。

<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 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 数に等しくなるまで繰り返される。言い換えると:

K1=SHA1(passward+Salt)

K2=SHA1(K1)

Kn=SHA1(Kn-1)

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 機能に使用されるか、適当な長さに縮めて、暗号化に使用される。

3.5 「4 セキュリティの考慮事項」

以下を行(308)の後ろに追加する。

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当り攻撃があるため、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。

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、安全性を高めずに処理だけを増加させる。

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 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れないため、PBKDF2 に代えて使用されている。

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。

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）とする必要がある。

204 # 4規定外の誤り

205 なし

206

5 明確化

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

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

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.

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

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を対
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。

274

275 本節は参考である。

276