Web Services Security: UsernameToken Profile 1.0

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):

山根 利夫	YAMANE, Toshio	株式会社日立製作所
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

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: Username Token Profile 1.0, located at http://docs.oasis-open.org/wss/2004/01/ oasis-200401-wss-username-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 XML Consortium 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-username-token-profile-1.0.pdf にある公式文書 Web Services Security UsernameToken Profile 1.0, © 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上で公表されている。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。

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

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

Translated by XML Consortium.

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。

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

Translated by XML Consortium.

Web Services Security UsernameToken Profile 1.0

OASIS Standard 200401, March 2004

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

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

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

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

Translated by XML Consortium.

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

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

Translated by XML Consortium.

Abstract:

本文書では、WSS: SOAP Message Security specification [WSS] 仕様で ユーザ名トークンを利用する方法を記述する。.

Status:

これは OASIS Web Services Security (WSS)技術委員会により考慮のために提出された技術委員会文書である。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。

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

Translated by XML Consortium.

63 # Table of Contents

77

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

Translated by XML Consortium.

78 # 1はじめに

79 本文書では、WSS: SOAP Message Security specification [WSS] 仕様で ユーザ名トークンを
80 利用する方法を記述する。もっと具体的に言うと、web サービス消費者が web サービス作成
81 者へ身元を認証するために、"ユーザ名" およびオプションとしてパスワード (または、共有秘
82 密、またはパスワードと同等のもの) により要求者を識別する方法としてどのように ユーザ名
83 トークンを提供することができるかを記述する。

84 本節は参考である。

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

Translated by XML Consortium.

2記法と用語

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 [RFC2119] 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 により使用される記法を利用する。特に、抽象プロパティ名は常に角括弧内に現れる(例えば、[some property])。

具体的な XML スキーマ [XML-Schema] を説明するとき、本規定では WSS: SOAP Message Security の記法を利用する。とくに、要素の [children] または [attributes] プロパティの各メンバーは XPath [XPath] と同様の記法で説明される (例えば、/x:MyHeader/x:SomeProperty/@value1)。 {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。

一般に使われるセキュリティ用語は Internet Security Glossary [SECGLO] で定義される。読者はこの用語集中の用語と同様に、Web Services Security 規定中の定義に精通していることを想定している。

2.2 名前空間

(一般形式 "some-URI" の) 名前空間 URI は、RFC 2396 [URI] で定義されるように、アプリケーション依存または文脈依存の URI を表現する。本規定は、一般的な SOAP [SOAP11, SOAP12] メッセージ構造と処理モデルで動作するよう設計されており、SOAP の任意の版に適用できる必要がある。ここでは現在の SOAP 1.1 名前空間 URI が詳細の例を提供するために利用されているが、本規定の適用を SOAP の単一の版に限定する意図はない。

本文書で利用する名前空間を次の表に示す (簡単のために、例では以下にリストされた接頭辞を利用するが、URI を含まない - 以下にリストされたものが仮定される)。

Prefix	Namespace
S11	http://schemas.xmlsoap.org/soap/envelope/
S12	http://www.w3.org/2003/05/soap-envelope
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

wsse と wsu 名前空間に対して提供される URL は、スキーマ・ファイルを取得するために利用することができる。

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

Translated by XML Consortium.

2.3 頭文字と省略形

次の (参考の) 表は、本文書のための頭文字と省略形を定義する。

Term	Definition
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
URI	Uniform Resource Identifier
UCS	Universal Character Set
UTF8	UCS Transformation Format, 8-bit form
XML	Extensible Markup Language

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

Translated by XML Consortium.

3ユーザ名トークン 拡張

3.1 ユーザ名 と パスワード

<wsse:UsernameToken> 要素は、ユーザ名を提供する方法として WSS: SOAP Message Security 文書で導入された。

<wsse:UsernameToken> 要素の中に、<wsse:Password> 要素を指定してもよい。 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されないが、それが一般的である。導出されたパスワードや S/KEY (一度だけのパスワード) のような、パスワードと同等のものは何でも利用することができる。 wsse:PasswordText 型に対する wsse:PasswordDigest 型についても、パスワードに保たれている情報が、情報の "ダイジェスト" を保持しているのではなく、単なる"平文" として扱われることを意味する。

例えば、サーバが平文のパスワードを持たず、そのハッシュを持っている場合、ハッシュはパスワードと同等とみなされ、本規定でパスワード(password)と示されている箇所では、何処でも使用することが出来る。本規定は、全ての実装に平文のパスワードによる接続を、求めてはいない。

wsse:PasswordText 型および wsse:PasswordDigest 型のパスワードは UTF8 符号化されたパスワード (または同等のもの) の SHA-1 ハッシュ値を Base64 [XML-Schema] 符号化したものとして定義される。しかしながら、このダイジェストされたパスワードが安全な伝達経路で送られるかトークンが暗号化されているのでなければ、ダイジェストの利用は 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セキュリティを提供するわけではない。

<wsse:Nonce> と <wsu:Created> の 2 つのオプションの要素が、再送攻撃への対抗策を提供するために <wsse:UsernameToken> に導入される。nonce は、送信者が送信する各 ユーザ名トークンに含めるために作る乱数値である。nonce を利用することは再送攻撃に対して効果的な対抗策ではあるが、利用された nonce をサーバがキャッシュすることが必要とされ、サーバの資源を消費する。nonce に作成時のタイムスタンプを組み合わせることによって、nonce のキャッシュに "新鮮さ" の期限設定を可能にするという利点をもち、資源要求に上限を確立する。 <wsse:Nonce> と <wsu:Created> の片方または両方が存在するなら、次のようにダイジェスト値に含まれなければ**ならない (MUST)**。

Password_Digest = Base64 (SHA-1 (nonce + created + password))

すなわち、nonce、生成タイムスタンプ(created)、およびパスワード (または共有秘密またはパスワード同等のもの) を結び付け、SHA-1 ハッシュ・アルゴリズムを利用してその連結のダイジェストを取り、それからその結果の Base64 符号化したものをパスワード (ダイジェスト) として含める。これはパスワードを不明瞭にすることを助け、再送攻撃を防ぐための基礎を提供する。 web サービスの提供者が再送攻撃を防ぐためには、3 つの対策が**推奨される (RECOMMENDED)**:

1. web サービス作成者は nonce と生成タイムスタンプの両方を利用していない ユーザ名トークンはどれも拒否することが**推奨される (RECOMMENDED)**。
2. web サービス作成者はタイムスタンプの "新鮮さ" の期限を提供し、"新鮮でない" タイムスタンプをもつ ユーザ名トークン はどれも拒絶することが**推奨される**

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

Translated by XML Consortium.

(RECOMMENDED)。ガイドラインとして、5 分という値を、再送を検知し、そして拒絶するための最小値として使用することができる。

3. 使用された nonce は少なくともタイムスタンプ新鮮さの期限まではキャッシュされ、すでに利用された (そしてキャッシュ中にある) nonce をもつ ユーザ名トークン は拒否することが**推奨される (RECOMMENDED)**。

nonce は復号された値のオクテット列を利用してハッシュされるのに対して、タイムスタンプは要素の内容に指定される UTF8 符号化のオクテット列を利用してハッシュされることに注意。

wsse:PasswordDigest は、平文パスワード (またはパスワードと同等のもの) が要求者と受信者の両方で利用可能である場合にのみ利用されることができることに注意。

秘密が入力の最初ではなく最後に置かれることに注意。これは、SHA-1 の出力が、入力ストリームの処理の最後での関数の完了状態であるためである。入力ストリームがハッシュ関数のブロック長にきれいに適合した場合、攻撃者は入力を追加のブロックで拡張し、元々のストリームに対するハッシュ出力だけを知って新しい固有のハッシュ値を生成することができる。秘密がストリームの最後にあれば、攻撃者がそれを勝手に拡張することを妨ぐことができる -- 彼らが知らないパスワードで入力ストリームを終えなければならないためである。同様に、nonce/created が最後に置かれると、攻撃者は nonce を nonce+created になるよう更新し、新しいハッシュを生成するために新しい created 時刻を追加できる。

上の対抗手段は、トークンが異なる受信者へ再送されるようなケースをカバーしない。この脅威に対抗するいくつかの (参考の) 可能なアプローチがあり、単独で、または組み合わせて利用することができる。それらの利用には、相互運用性を提供するために通信する組織間で事前の協定を必要とする (おそらく、新しいパスワード型を導入するような、別に公開されたプロファイルの形で)：

- 複数のユーザアカウントが同一のパスワードを持つような場合に対抗するために、ハッシュにユーザ名を含める (例えば、会社名を基にしたパスワード)
- 同じユーザ名/パスワードが複数のシステムで利用されている場合に対抗するために、ハッシュにドメイン名を含める
- 受信するシステムが nonce キャッシュを共有しない場合に対抗するために、ハッシュに意図した受信者の何らかの印を含める (例えば、2 つの別のアプリケーション・クラスタが同じセキュリティ・ドメインにある場合)

次にこの要素の XML 構文を例示する。

```
<wsse:UsernameToken wsu:Id="Example-1">
    <wsse:Username> ... </wsse:Username>
    <wsse:Password Type="..."> ... </wsse:Password>
    <wsse:Nonce EncodingType="..."> ... </wsse:Nonce>
    <wsu:Created> ... </wsu:Created>
</wsse:UsernameToken>
```

次に、上の例でリストされた属性と要素を説明する。

/wsse:UsernameToken/wsse:Password

このオプションの要素はパスワード情報 (またはハッシュのような同等なもの) を提供する。この要素は安全なトランスポート (例えば HTTP/S) が利用されている場合やトークン自体が暗号化されている場合のみに渡されることが**推奨される (RECOMMENDED)**。

/wsse:UsernameToken/wsse:Password/@Type

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

Translated by XML Consortium.

このオプションの URI 属性は提供されるパスワードの型を指定する。下の表に既定義の型を示す (URI フラグメントは本規定の URI に相対的であることに注意せよ)。

URI	説明
#PasswordText (default)	ユーザ名に対する実際のパスワード、パスワードのハッシュ、または導出されたパスワードまたは S/KEY。この型は nonce または生成時刻によらないハッシュされたパスワード同等物が利用されている、または SHA1 以外のダイジェスト・アルゴリズムが利用されている場合に利用されるべきである。
#PasswordDigest	ユーザ名に対するパスワード (およびオプションで nonce と/または生成タイムスタンプ) の、上で示したアルゴリズムを利用したダイジェスト。

/wsse:UsernameToken/wsse:Password/@{any}

これはスキーマに基づき、要素に付加されるべき付加的な属性を許すための拡張機構である。

/wsse:UsernameToken/wsse:Nonce

このオプションの要素は暗号的にランダムな nonce を指定する。 <wsse:Nonce> 要素を含む各メッセージは web サービス作成者が再送攻撃を検知できるように新しい nonce 値を利用しなければ**ならない (MUST)**。

/wsse:UsernameToken/wsse:Nonce/@EncodingType

このオプションの属性 URI は nonce の符号化型を指定する (有効な値については <wsse:BinarySecurityToken> の定義を参照)。この属性が指定されないなら、デフォルトの Base64 符号化が利用される。

/wsse:UsernameToken/wsu:Created

このオプションの <wsu:Created> 要素は生成時刻を示すために用いられるタイムスタンプを指定する。 <wsu:Timestamp> の定義の一部として定義される。

すべての準拠した実装は <wsse:UsernameToken> 要素を処理できなければならない。規定が、要素が「処理される」べきであることを要求するところでは、それは要素がサポートされないなら適切なエラーが返されるという点で要素型が認識されなければ**ならない (MUST)** ことを意味する。

WSS: SOAP Message Security 規定で説明される <wsse:KeyIdentifier> と <ds:KeyName> 要素は本プロファイルではサポートされないことに注意。

次の例はこの要素の利用を示す。この例では、パスワードが平文で送られ、そのためこのメッセージは秘密の伝達経路で送られるべきである。

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="...">
   <S11:Header>
      ...
      <wsse:Security>
         <wsse:UsernameToken>
            <wsse:Username>Zoe</wsse:Username>
            <wsse:Password>IloveDogs</wsse:Password>
         </wsse:UsernameToken>
```


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

Translated by XML Consortium.

```
      </wsse:Security>
      ...
   </S11:Header>
   ...
</S11:Envelope>
```

次の例はパスワードのダイジェストを nonce および生成タイムスタンプと一緒に利用する。

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu= "...">
   <S11:Header>
      ...
      <wsse:Security>
         <wsse:UsernameToken>
            <wsse:Username>NNK</wsse:Username>
            <wsse:Password Type="...#PasswordDigest">
               weYI3nXd8LjMNVksCKFV8t3rgHh3Rw==
            </wsse:Password>
            <wsse:Nonce>WScqanjCEAC4mQoBE07sAQ==</wsse:Nonce>
            <wsu:Created>2003-07-16T01:24:32Z</wsu:Created>
         </wsse:UsernameToken>
      </wsse:Security>
      ...
   </S11:Header>
   ...
</S11:Envelope>
```

3.2 トークン参照

UsernameToken が <wsse:SecurityTokenReference> を利用して参照されるとき、ValueType 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れば**ならない (MUST)**。

次の符号化形式が定義済みである (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せよ)。

URI	説明
#UsernameToken	UsernameToken

UsernameToken が<ds:KeyInfo>要素から参照されるとき、それはパスワードを利用して、メッセージ認証アルゴリズムのための鍵を導出するために利用することができる。本プロファイルでは鍵導出のための特定の機構は範囲外だと考える。実装は相互運用性のために鍵導出アルゴリズムに関して合意が必要である。

UsernameToken に対する KeyIdentifier の定義はない。したがって、KeyIdentifier 参照は UsernameToken を参照するときは利用しては**ならない (MUST NOT)**。

同様に UsernameToken に対する KeyName の定義はない。したがって、KeyName 参照は UsernameToken を参照するときは利用しては**ならない (MUST NOT)**。

すべての参照はトークンのための wsu:Id を参照する。

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

Translated by XML Consortium.

3.3 エラー・コード

実装は、必要なら私用の名前空間に定義されたカスタム・エラー・コードを利用してもよい。しかし、相互運用を改善するために、署名、復号、符号化とトークン・ヘッダのエラーに対しては WSS: SOAP Message Security 仕様で定義されたエラー処理コードを利用することが**推奨される (RECOMMENDED)**。

カスタム・エラー・コードを利用するときは、実装は返されるエラー・コードで攻撃者を助けるかもしれないセキュリティ脆弱性を導入しないように注意すべきである。

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

Translated by XML Consortium.

4セキュリティの考慮事項

ユーザ名トークン の利用は、セキュリティ・トークンの他の型に対して既に確認されたものを越える追加の脅威は導入しない。再送攻撃には、他のアプリケーション固有の追跡機構と同様に、メッセージのタイムスタンプ、nonce、およびキャッシュを利用することにより対応することができる。トークンの所有権は鍵の利用により検証され、中間者攻撃を一般的に回避できる。トランスポート・レベルでのセキュリティを、ユーザ名トークン と全メッセージ本体の両方の秘匿性と完全性を提供するために利用してもよい。

<UsernameToken> 中のパスワード (またはパスワードと同等のもの) が認証のために利用されるとき、パスワードは適切に保護される必要がある。下位のトランスポートが盗聴に対して、十分な防御を提供しないなら、パスワードは本書で説明するようにダイジェスト化されるべきである。そうしたとしても、パスワードは、単純なパスワード推測攻撃が捕獲されたメッセージから秘密を暴露しないように十分強くなければならない。

パスワードが暗号化されるとき、暗号化に対する通常の脅威に加えて、2 つのパスワード固有の脅威が考慮されなければならない: 再送と推測。攻撃者が、暗号化されたまたはハッシュされたパスワードを再送することによって利用者のふりをすることができるなら、実際のパスワードを知ることは必要ではない。再送を防ぐ 1 つの方法は、前に説明した nonce を利用することである。一般的に、保存されなければならない以前の nonce の数に上限を設けるために、タイムスタンプもまた利用する必要がある。しかしながら、効果的であるためには、nonce とタイムスタンプが署名されなければならない。署名が暗号化の前にパスワード自身にも被さるなら、パスワードに対するオフラインの推測攻撃を遂行するために署名を利用することは簡単なことである。この脅威は次を含むいくつかの方法で防御されることができる: パスワードを署名の下に含めない (パスワードは後で検証されるだろう) または暗号化されたパスワードに署名する。

脅威と可能な対抗手段についての追加の議論については、読者は、WSS: SOAP Message Security 文書の 13 章もまた吟味すべきである。

本節は参照である。

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

Translated by XML Consortium.

5参考文献

以下は規範的な参考文献である。

[SECGLO]	*Informational RFC 2828, "Internet Security Glossary," May 2000.*
[RFC2119]	*S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997*
[WSS]	*OASIS standard, "WSS: SOAP Message Security," TBD.*
[SOAP11]	*W3C Note, "SOAP: Simple Object Access Protocol 1.1," 08 May 2000.*
[SOAP12]	*W3C Working Draft**, "**SOAP Version 1.2 Part 1: Messaging Framework", 26 June 2002.*
[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.*
[XML-Schema]	*W3C Recommendation, "XML Schema Part 1: Structures,"2 May 2001.* *W3C Recommendation, "XML Schema Part 2: Datatypes," 2 May 2001.*
[XPath]	*W3C Recommendation, "XML Path Language", 16 November 1999*

次のものは、背景や、関連する資料としての参考的なものである。

[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-C14N]	*W3C Recommendation, "Canonical XML Version 1.0," 15 March 2001*
[EXC-C14N]	*W3C Recommendation, "Exclusive XML Canonicalization Version 1.0," 8 July 2002.*
[XML-Encrypt]	*W3C Working Draft, "XML Encryption Syntax and Processing," 04 March 2002* *W3C Recommendation, "Decryption Transform for XML Signature", 10 December 2002.*
[XML-ns]	*W3C Recommendation, "Namespaces in XML," 14 January 1999.*
[XML Signature]	*W3C Recommendation, "XML Signature Syntax and Processing," 12 February 2002.*
[XPointer]	*"XML Pointer Language (XPointer) Version 1.0, Candidate Recommendation", DeRose, Maler, Daniel, 11 September 2001.*

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

Translated by XML Consortium.

Appendix A. 改版履歷

Rev	Date	By Whom	What
Wd-1.0	2002-12-16	Phil Griffin	Initial version cloned from the WSS core specification
Wd-1.1	2003-01-26	Anthony Nadalin	Bring in line with WSS-Core Update
Wd-1.2	2003-02-23	Anthony Nadalin	Editorial Updates
Wd-1.3	2003-06-30	Anthony Nadalin	Editorial Updates
Wd-1.4	2003-08-11	Anthony Nadalin	Editorial Updates
Cd-1.5	2003-12-09	Anthony Nadalin, Chris Kaler	Editorial Updates based on Issue List #30
Cd-1.5	2003-12-15	Anthony Nadalin, Chris Kaler	Editorial Updates based on Editorial feedback
Cd-1.6	2003-12-22	Anthony Nadalin	Editorial Updates based on Editorial feedback
Cd-1.7 & 1.8	2003-12-29	Anthony Nadalin, Chris Kaler	Editorial Updates based on Editorial feedback
Cd-1.8	2004-01-19	Anthony Nadalin, Chris Kaler	Editorial corrections for name space and document name
Cd-1.9	2004-02-17	Anthony Nadalin	Editorial corrections per Karl Best

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

Translated by XML Consortium.

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.

Copyright © The Organization for the Advancement of Structured Information Standards [OASIS] 2002-2004. All Rights Reserved.

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

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。

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

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、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、

391 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
392 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
393 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
394 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。
395 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
396 によって取り消されることはない。
397 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**
398 **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**
399 **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。**
400 本節は参考である。

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

Translated by XML Consortium.