デジタル・ドキュメント 25－3
（2000．9．22）

W3C と IETF における XML ドキュメントへのデジタル署名規格の現状

XML digital signature processing rules and syntax of IETF/W3C Working Group

白井 宣則
Yoshinori SHIRAI

shirai@dv4.nnes.nec.co.jp

ＮＥＣソフトウェア中国
〒732-0827 広島市南区稲荷町 4-1 住友生命広島ビル

Java コンソーシアム XML 部会

抄録：XML(eXtensible Markup Language:拡張可能なマーク付け言語)はプラットフォームを選ばないデータ交換フォーマットとして、1998 年 2 月の W3C 勧告以来、急速に注目を集めている。今後は、企業間電子取引(EC)およびコンテンツ管理の標準フォーマットとして、XML が標準になると思われる。そのような状況の中で、XML データの真正性(改竄されていないこと)をどのように確保するのかが、次のステップとして重要になってきている。IETF(Internet Engineering Task Force)と W3C(World Wide Web Consortium)では、1999 年 7 月に行われた 45th IETF Meeting; Oslo, Norway, から共同で、XML データへデジタル署名を行う場合の処理方法と構文を検討している。2000.年 8 月現在では最終版のドラフトが公開中(http://www.w3.org/TR/2000/WD-xmldsig-core-20000711/)でありコメントが寄せられている所である。本稿では、この XML デジタル署名の検討経緯と規格概要につてまとめてみたい。

Abstract: XML (eXtensible Markup Language) is a data format for structured document interchange on the Web. It is a text-based, non-binary format and uses syntax rather than binary markers to organize data; it can be used on just about any platform. It was accepted by the World Wide Web Consortium (W3C) as a recommendation on February 10, 1998, recently it is gathering attention. From now on, XML will be a standard data format as electric-commerce and management of the contents. Therefore maintaining data authentication (data is not altered) is next important point. After July 1999, 45th IETF; Oslo, Norway, IETF and W3C are joint reviewing about digital signature processing rules and syntax. On August 2000 now, this working draft is last call (http://www.w3.org/TR/2000/WD-xmldsig-core -20000711/), and gathering comments. In this document I will write about this XML digital signature processing rules and syntax.

1．はじめに

XMLは、定義可能なタグセットを用いる事によって、インターネット上を含め、プラットフォームに依存しないデータ交換を可能にしている技術である。この特性により、XMLは単なるタグ付け言語から、企業間アプリケーション開発プラットフォームの不可欠な要素へと変わりつつある。

日本においても、昨年(1999年)の夏頃から雑誌などにおいて、XMLの特集が目に付くようになり、今年(2000年)に入ってからは、入門書から雑誌・専門書に至るまで大量の書籍が出版され、専門の雑誌も創刊される状況にある。

このように基盤技術としてXMLが注目され、データ記述言語として重要な位置を占めるような状況にある中で、次のステップとして重要となるのがセキュリティである。

XMLで記述したデータによりデータ交換を行う課程で、改竄や発信者の否認、成りすましが簡単にできるようであれば、XMLを使用したデータ交換そのものが、信頼性のないものとなり、普及は難しくなる。

そこで、この問題に対処するために、IETFとW3CではXMLデータの真正性(改竄されていないこと)確保を目的として、XMLへのデジタル署名(XML-Signature Syntax and Processing)規格を策定中である。この規格は現在、勧告候補に至る直前のLast Call段階にある。

筆者は業務において認証局(CA：Certification Authority)の開発を行った経緯もあり、XMLへのデジタル署名について動向を注視している。IETF Meetingについては、実際に46th IETF Meeting-WASHINGTON,D.C.(November, 1999)、47th IETF Meeting-Adelaide, Australia (March, 2000)と参加した。

また、昨年のJavaコンソーシアムXML部会(当初はXML研究会。2000年7月よりXML部会に昇格)発足時より活動に参加し、その中でW3CでのXML関連の諸規格について情報交換を行ってきた。

そこで、本稿ではXMLデジタル署名の検討経緯と規格概要につてまとめてみたい。

2．W3C とIETFについて

(1) W3C(World Wide Web Consortium)

WWWで利用される技術の標準化をすすめる団体である。WWW技術に関わりの深い企業、大学・研究所、個人などが集まって、1994年10月に発足した。

W3Cの設立にはマサチューセッツ工科大学(MIT)や、WWWが開発された欧州合同素粒子原子核研究機構(CERN)などが大きな役割を果たしており、現在ではマサチューセッツ工科大学計算機科学研究所(MIT/LCS)、フランス国立情報処理自動化研究所(INRIA)、日本の慶應義塾大学SFC研究所(Keio-SFC)がホスト機関としてW3Cを共同運営している。

XMLに関する規格では、XML 1.0 をはじめ、XHTML ・ Xlink ・ XML Query ・ XML Schema ・ XML Signature ・ Xpointer ・ XSL
など殆どの規格が、W3Cで検討・勧告されている。

(2) IETF(Internet Engineering Task Force)

インターネット上で使われる各種プロトコルなどを標準化したRFC（request for comments）を発行する組織である。IAB（Internet Architecture Board）の下部組織として、1986に設立された。当初は，特定問題の解決を目指すワーキング・グループと呼ばれる委員会20余りで構成されていた。

しかしその後，出席者が急増するのに伴

い，IETF議長が一人でまとめることが困難になったため，中間組織としてIESG（Internet Engineering Steering Group）が構成され，エリアと呼ばれる分野ごとに責任者を置く形態に改組された。現在このエリアは８分野に分かれている。

----IETFでのエリア----
■APP - Applications
■INT - Internet Services
■IPNG - IP: Next Generation
■MGT - Network Management
■OPS - Operational Requirements
■RTG - Routing
■SEC - Security
■TSV - Transport
■USV - User Services

図 1　IETFでのエリア一覧

各エリアは，いくつものワーキング・グループで構成されている。各ワーキング・グループにはChair（s）と呼ばれる代表者が存在し、問題の切り分けや議論の方向性を調整している。ワーキング・グループ総数は、2000.8.25現在で１３３である。XMLへのデジタル署名の検討は、Securityエリアに属し、XML Digital Signatures (xmldsig)がワーキング・グループ名となっている。

その他、新しいワーキング・グループを立ち上げる前段階として、BOF(Birds Of a Feather)があり、IETF Meetingでは毎回、２０～３０のBOFが立ち上がりをみせている。BOFはCharterの承認などを経てワーキング・グループへ昇格できる。

IETFの特徴としては、
①正式なメンバシップは無い。
②メーリングリストでの検討が主な活動。
③"ラフコンセンサス"ベースの意志決定方式をとる。
④年３回のMeeting(3/7/11月　米国２回、他１回)を実施。
などがある。
このIETF Meetingには、世界中から毎回３０００名前後の技術者が集まり、１週間に渡って、各ワーキング・グループ毎に１回または２回のMeetignを実施する形態で行われている。日本からの参加者も、昨年11月に開かれた46th IETF Meeting-WASHINGTON,D.C.以来急激に増加している。具体的には、全参加者の約１割(３００名前後)が日本からの参加者になっており、国別では米国に次いで第二位の勢力となっている。

（３）W3CとIETFによるXML Digital Signaturesの共同検討について

IETFによるXML Digital Signaturesの検討は、1999年3月に行われた44th IETF Meeting; Minneapolis, Minnesota,USAでBOFとして登場する所から始まった。W3Cではその直後の1999年４月にW3C Signed XML Workshopが行われ、これが具体的な検討の開始となった。

それぞれの組織に於いて検討が開始された背景としては、IETF側としては、インターネット上でのセキュリティ的な方向からXMLに近づいてゆき、XML Digital dignaturesが検討範囲に入ってきたように個人的には思える。一方、W3C側としては、XMLの規格を拡張する上で、XML Digital dignaturesが検討範囲に入ってきたように思える。

このような状況の中で、1999年7月に行われた45th IETF Meeting; Oslo, Norway,でXML Digital dignaturesはBOFからワーキング・グループに昇格となり、同時にW3Cとの共同での検討を行う事が発表された。通常は１回のBOF Meetingでワーキング・グループに昇格になる事はあまりない。異例の早さであった。これは、XMLに関する注目が急速に高まり、標準化が急務となった事が背景にあると思われる。
IETFでのXML Digital Signaturesワーキング・グループでのChair(s)はJoseph Reagle Jr (W3C)とDonald Eastlake 3rd (IBM→現在はMotorola)の二名である。
XML Digital Signaturesワーキング・

グループでのデジタル署名の構文の検討は、Had Brown氏のSyntax Proposalが1999年８月に出されたことから具体的に始まった。当初は、2000年１月にSignature SyntaxとProcessing documentをIESGにProposed Standardとてして登録予定のスケジュールであった。その後、2000.6頃にずれ込み、2000.8.25時点では、まだこの直前の状態である。2000.8.25現在の最新ドラフトは

- http://www.w3.org/TR/2000/WD-xmldsig-core-2000711/
- http://www.ietf.org/internet-drafts/draft-ietf-xmldsig-core-08.txt [W3C-mirror] で公開されている。

実際のIETF Meetingに参加して感じた事であるが、W3Cサイドの人たちはxmldsigに拡張性・利便性を持たせることを重要視しており、IETFサイドの人たちは、セキュリティの専門家が多いこともあり、信頼性や堅牢性を重視している傾向があるように思える。

３．XML デジタル署名の基本的考え方

（１）署名の概念について

デジタル署名は、公開鍵暗号方式を使用している。公開鍵暗号方式では鍵の利用者(この場合は署名者)本人だけが持つ「秘密鍵」と公に公開する「公開鍵」の二つの鍵がある。デジタル署名は、対象となるドキュメントに署名者の「秘密鍵」で署名を行う事で、真正性を保証する考え方が基本となっている。

（２）正規化処理とトランスフォーム

XML 文書は、データを記述しているのみのため、表現のされ方が違っても、内容的(意味的に)に同じであれば、同一文書と見なさなければならない。XML デジタル署名では、まず対象となるドキュメントの正規化を行い、署名対象データを成形する。この規格も IETF で標準化されており、canonical XML[XML-C14N]

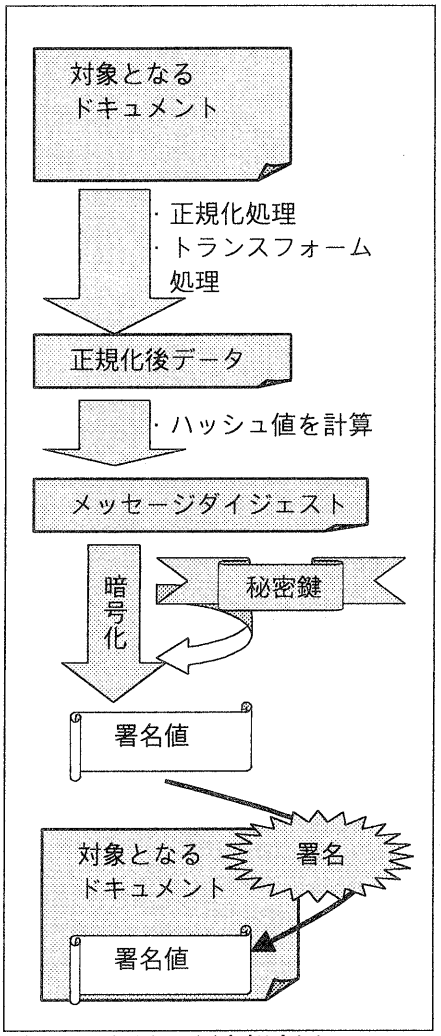

図 2 デジタル署名概念図

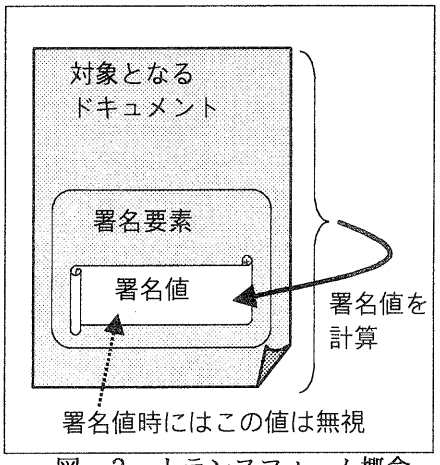

図 3 トランスフォーム概念

と呼ばれている。

ドラフトは以下のURLで参照できる。
http://www.w3.org/TR/2000/WD-xml-c14n-20000710
現在のステータスは、勧告候補直前のLastCallである。

トランスフォーム処理は、署名対象文書に対して、署名値を計算する前に、ユーザが指定する部分を無視する機能である。これは、署名対象自体に署名が含まれる場合、その署名値を無視する必要があるため、XML文書の部分抽出を行う設定された処理である。

（3）ハッシュ処理

ドキュメントの完全性保証のため、メッセージダイジェストをハッシュ処理により作成する。ハッシュ(Hash)とは、任意の長さの文章から、短いランダムな固定長のメッセージダイジェストを作る方法である。MD5やSHAなどの方法があり、元のメッセージから作られたメッセージダイジェストは、1対1の対応関係を持ち、衝突(異なる文章から同一のメッセージダイジェストになる)の確率が極めて小さい事から、完全性保証に使われている。

また、MD5やSHAは、作られたハッシュから元のデータを再現する事ができない、またはその計算が困難である関数(1方向ハッシュ関数)となっているので、メッセージダイジェストから元の文章を復元(推測)することは困難である。

これは、元の文章が1文字でも変更された場合は、ハッシュ計算後のメッセージダイジェストの値が変わることを表している。そのため、データ交換時の完全性検証を行う場合は、データとして文章とそのメッセージダイジェストを送ってもらい、検証時に文章のメッセージダイジェストを受信側で再計算し、送られてきたメッセージダイジェストと比較して一致すれば、文章の改竄が途中の経路で行われていなかった事が保証されることになる。

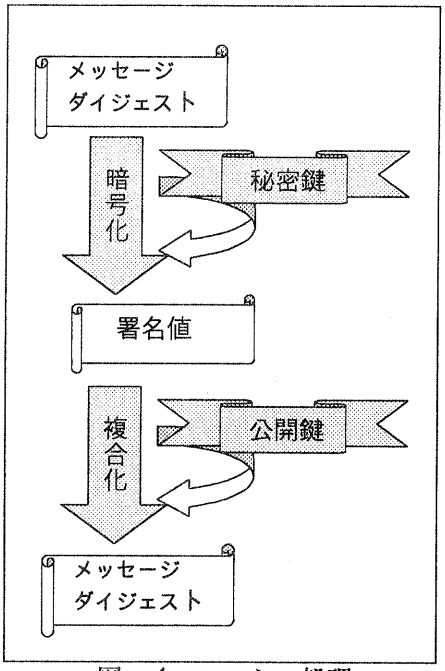

図　4　ハッシュ処理

（4）署名処理

署名処理では、署名者の「秘密鍵」で先程のメッセージダイジェストを暗号化し、署名値を算出する。「秘密鍵」で暗号化された署名値は、署名者の「公開鍵」でのみ複合化できる。この複合化したメッセージダイジェストを、文章から再計算されたメッセージダイジェストと比較して同一であれば、署名者が確実にこの文章を署名したことと、文章が改竄されていない事が同時に確認できる。

署名処理は、多重署名(署名に対してさらに署名を施すこと)も可能である。これは稟議諸のように、承認が階層的になる場合などに対応できる。

多重署名になるか否かは、対象となる文書の領域指定範囲に依存するため、処理内容自体は変わらない。
また、Xlink機能を使用すれば、署名

済みデジタル文書に変更を加える事なく署名後に情報を後付することも可能である。

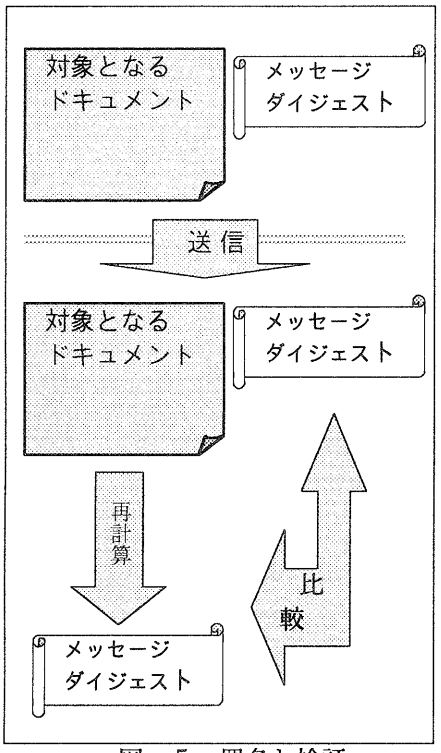

図　5　署名と検証

4．現状の XML デジタル署名規格

（1）XML デジタル署名文書の構成

この節では、2000.年 8 月現在では最新版のドラフトである http://www.w3.org/TR/2000/WD -xmldsig- core-20000711/ に従い、XML デジタル署名文書の構成についてまとめてみたい。

まず、署名対象となる Object は以下の 3 種類である。

①署名の中
②同じドキュメントの署名の外
③全く別のドキュメント

従って、署名となるのは XML データだけではなく、TEXT や Word 文書など様々な形式の電子文書が対象となり得る。

署名手順としては、まずこれらの署名対象文書から、ハッシュ値を求める。次にこのハッシュ値と、関連情報としてハッシュのアルゴリズムや対象文書の URI などの情報を合わせて、署名者の秘密鍵で暗号化し、署名値を求める。

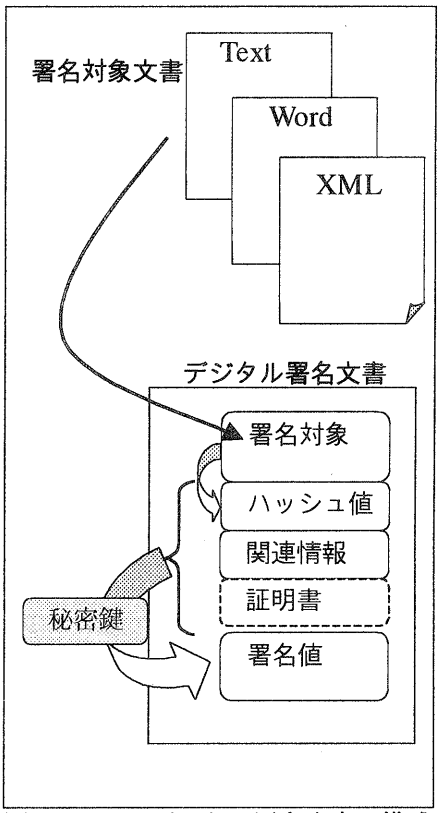

図　6　XML デジタル署名文書の構成

（2）中心構文

中心構文の主な要素は、次のようになる。

① SignedInfo：署名の情報
- **正規化の方法**
- 署名の方法
  (ハッシュ アルゴリズム等)
- 署名対象文書の情報

②SignatureValuie：署名値

② keyInfo：証明書情報

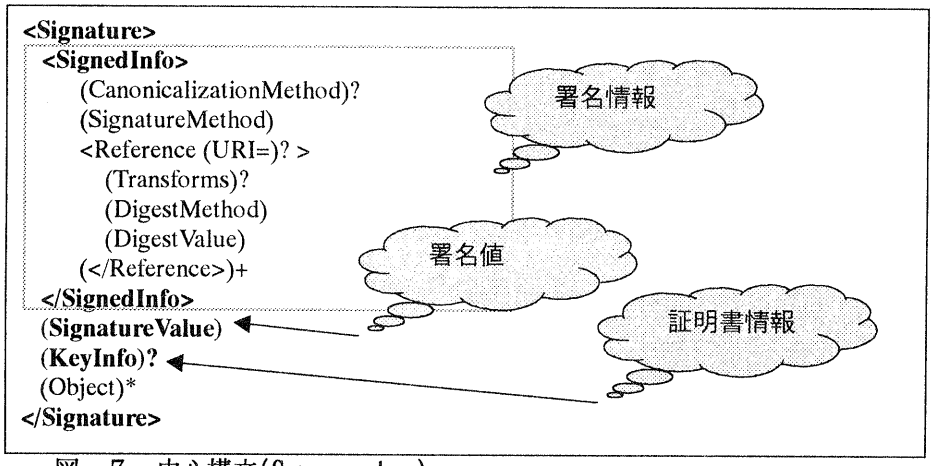

図　7　中心構文(Core syntax)

（3）XML デジタル署名文書例

この節では、SampleExample を使用し、具体的に XML デジタル署名文書を説明したい。

SignedInfo では正規化の方法として、c14n を使用し、署名の方法としては、dsa-sha1 を使用することが書かれている。

The following example is a detached signature of the content of the HTML4 in XML specification.

```
[s01] <Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/07/xmldsig#">
[s02]   <SignedInfo>
[s03]   <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-
          20000710"/>
[s04]   <SignatureMethod Algorithm="http://www.w3.org/2000/07/xmldsig#dsa-sha1"/>
[s05]   <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
[s06]     <Transforms>
[s07]       <Transform Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710"/>
[s08]     </Transforms>
[s09]     <DigestMethod Algorithm="http://www.w3.org/2000/07/xmldsig#sha1"/>
[s10]     <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
[s11]   </Reference>
[s12] </SignedInfo>
[s13]   <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
[s14]   <KeyInfo>
[s15a]    <KeyValue>
[s15b]      <DSAKeyValue>
[s15c]        <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
[s15d]      </DSAKeyValue>
[s15e]    </KeyValue>
[s16]   </KeyInfo>
[s17] </Signature>
```

ダイジェスト計算
Reference要素のURI属性で指定される署名対象部分のダイジェスト値を指定されたダイジェスト計算法により計算し、DigestValueを得る

署名計算
指定された正規化方式を用いて正規化を行った後に、指定のアルゴリズムで署名値を求める

XML-Signature Syntax and Processing　W3C Working Draft 11-July-2000
http://www.w3.org/TR/2000/WD-xmldsig-core-20000711/
より引用

図　8　XML デジタル署名文書例

次に、Reference 要素の URI 属性で指定されている、../REC-xhtml1-20000126 が署名対象文書だと分かる。

この署名対象部分を、指定されたダイジェスト計算方法(sha1)により算出した値がダイジェスト値（DigestValue)として格納されている。

これらの SignedInfo の内容を、指定された正規化方法(c14n)を用いて正規化を行った後に、指定のアルゴリズム(dsa-sha1)で処理し求めた値が署名値(SignatureValue)として格納されている。

5．今後の課題と展望

当初は 2000 年 1 月の W3C 勧告を目標に規格を検討してきた XML デジタル署名であるが、現時点で半年以上勧告が遅れている。これは、mobility の向上と、セキュリティ上の堅牢性のバランスをどのように取るかが、予想以上に難しかったためではないかと個人的には思っている。XML の長所を取り入れるためには mobility は必要　　だが、Syntax が複雑となり、セキュリティ上はどうしても弱点が発生する可能性が高まるからである。

正規化の問題も、予想以上に大きかったのではないかと思う。Minimal C14n 規格などは、その一意性が問題となり、規格は提案されたが、実装ではほとんどの技術者が対応しない姿勢であった。実際に、現在の各パーサでの正規化も、非互換性は存在し XML 署名値をマルチベンダ環境で検証するのは難しい現実がある。正規化が標準化されて、初めてメッセージダイジェストの互換性→署名値の互換性が実現するので、今後は各パーサ間での標準化が望まれる。

証明書そのものについても、今後は XML 化の方向にあるのではないかと思う。今までの検討では、証明書は既存のものを使用する前提で曖昧に定義されていたが、47 th IETF Meeting などでは、SPKI のワーキング・グループから、<cert>タグなどを定義し、XML で証明書を定義できるような提案もあった。これが実現すれば、現在は証明書の作成および検証に使用している ASN.1 の DER エンコードなどが不要になり、シンプルな形で PKI を構築できる可能性が出てくる。この提案が行われた背景としては、証明書の暗号化フォーマットが複雑になりすぎている問題があると思える。この証明書の署名を XML で行う XML 署名案によれば、XML エンコードされた証明書を作成するためには

- Crypto library
- XML processor
- XML-Signature processor　のみで

implement できる事になり、開発環境が今までよりもシンプルになると思われる。

その他、ASN1(Abstract Syntax Notation 1)/XML トランスレータもこれから注目されると思われる(実際に IBM は開発中との発表が既にあり)。ASN1 は SNMP,LDAP,X.509, PKCS で広く使われている。ASN1/XML トランスレータは、この ASN1 データを Web に適したモノにできるので、将来的にはこれら全てのフォーマットが XML で記述される日が来る可能性があるのでは…と個人的には期待している。

参考文献

[1] XML-Signature Syntax and Processing W3C Working Draft 11-July-2000XML http://www.w3.org/TR/2000/WD-xmldsig-core-20000711/

[2] http://www.ietf.org/

[3] セキュリティ関連用語 http://www.w3.tokyoweb.or.jp/isl/dokuhon/p10.htm

[4] XML　PRESS Vol 1 (2000.8)　Pp2 - 10

[5] SHA-1 FIPS PUB 180-1. Secure Hash Standard. U.S. Department of Commerce/National Institute of Standards and Technology. http://csrc.nist.gov/fips/fip180-1.pdf

[6] XML Extensible Markup Language (XML) 1.0 Recommendation. T. Bray, J. Paoli, C. M. Sperberg-McQueen. February 1998. http://www.w3.org/TR/1998/REC-xml-19980210

[7] ML-C14N Canonical XML. Working Draft. J. Boyer. July 2000. http://www.w3.org/TR/2000/WD-xml-c14n-20000710.html