XMLと電子署名
XML and Digital Signatures

西澤　秀和　NISHIZAWA Hidekazu
才所　敏明　SAISHO Toshiaki

近年，インターネット上での情報交換のためのフォーマットとして，XML（eXtensible Markup Language）が注目を浴びている。一方，電子署名法の施行に代表されるように，ネット上での電子商取引（EC：Electronic Commerce）や電子申請における電子署名付与技術の重要性が高まっている。

ネット上で電子署名を実現するには，署名フォーマットの互換・拡張性や，Web技術との容易な結合が重要となる。そこで，XMLデータに対する署名付与フォーマットとして，W3C（World Wide Web Consortium）で標準化が進められているXML-Signatureの規格を導入し，更に，Webブラウザ上で利用可能とするため，ブラウザのプラグインとして機能するソフトウェアを開発した。

Extensible Markup Language (XML) and digital signatures are expected to become important technologies in the electronic commerce and government domains. Toshiba has developed an XML-Signature plug-in with the aim of realizing signing and verification of digital signatures via the Web browser. The signature format is based on the World Wide Web Consortium (W3C) XML-Signature specification. The plug-in implements the common functions of data exchange, and makes form-based document exchange possible without service-dependent application software on the client side.

1　まえがき

インターネット上でのECや電子申請などにおけるデータフォーマットとして，XMLが注目を浴びている。一方，電子署名法（「電子署名及び認証業務に関する法律」，2001年4月施行）に見られるように，ネット上で交換されるデータに対する電子署名付与技術が重要となっている。

しかし，従来の電子署名技術では，アプリケーションソフトウェア（以下，アプリケーションと略記）ごとに異なるフォーマットで署名を付与していたため，拡張性や互換性がなく，アプリケーションごとに独自に開発をしていた。また，あるサービスを受けようとした場合，サービスごとに異なるアプリケーションをインストールする必要があるなどの問題があった。

一方，ネット上でのサービスにおいては，Webブラウザのような，共通の機能を持ったアプリケーションを利用可能であることや，異なるサービス間でのデータ交換が柔軟に行えるなどの必要性があり，このため，標準に従ったフォーマットで，かつブラウザ上で容易に署名付与が可能な技術が必要となる（**図1**）。

このような要求の高まりに応じて，W3CにおいてXML-Signatureの標準化が進められている。XML-Signatureは，署名に関する情報をXMLの形で表現することで，HTML（HyperText Markup Language）文書やXML文書中にテキスト形式で署名情報を埋め込むことを可能にしており，共通のフォーマットで，相互運用性や拡張性の高い電子署名を記述することが可能となる。

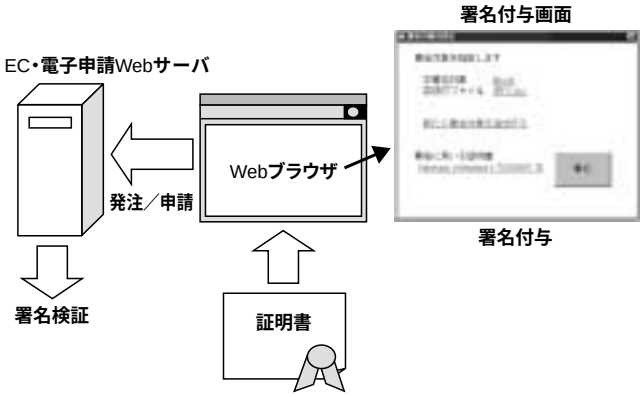


図1．ECなどにおける署名の利用　Webブラウザ上で署名付与画面が表示され，署名を行い，EC・電子申請Webサーバに送信する。
Model case of signature use

そこで，この論文では，W3C XML-SignatureをベースとしてWebブラウザ上での署名付与を容易に行える，プラグインによるXML署名付与ソフトウェアについて述べる。これにより，利用者にとってはサービスごとに異なるアプリケーションをインストールする必要がなく，また，ソフトウェア開発者にとってもアプリケーションの開発が容易になる，などのメリットが期待できる。

2 XML-Signatureの概要

XML-Signatureとは，電子署名のデータをXMLで表すためのW3Cの標準規格であり，署名対象，署名者などの情報をタグ付けし，XML文書で表すためのフォーマットを定めている。

図2はXML-Signatureの概念を表している。

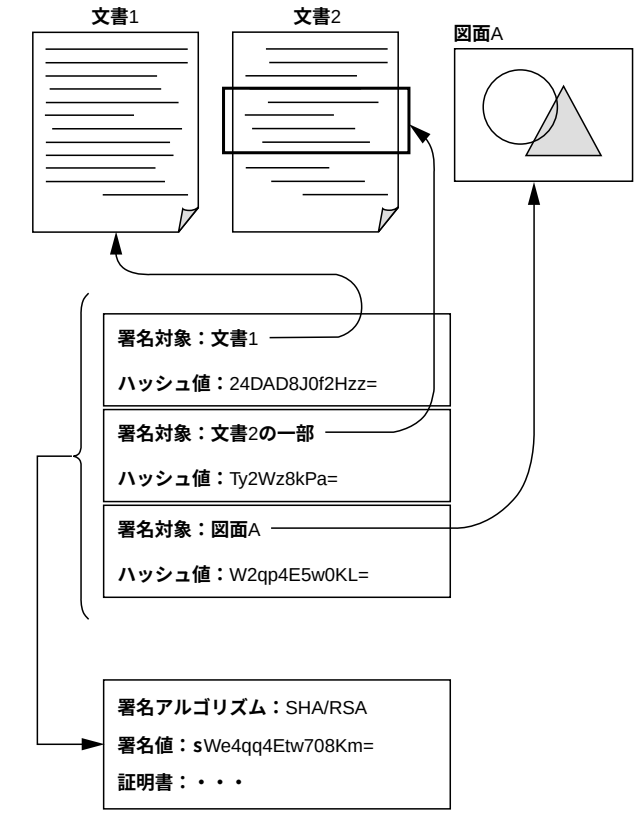


図2．XML-Signatureの概念　複数の署名対象に対するハッシュ値の全体に対して，更に署名をとることで署名値が得られる。
Concept of multiple signatures

署名対象としては，文書1の全体，文書2の特定部分及び図面Aであり，それぞれに対してハッシュ値を求め，所定のフォーマットでこれらの情報を記述する。更に，これらの情報を記述した部分に対して電子署名を求めることで，結果として複数の署名対象をまとめて署名することになる。この方法では，署名対象の一部だけが改ざんされた場合，どの部分かを容易に特定することができる。

XML-Signatureの一例を**図3**に示す。なお，ここでは説明を簡単にするため，一部を省略して記述している。Signatureタグは，署名対象の文書（XML）中に埋め込まれる場合もあるし，署名対象とは別ファイルとして，単体で存在する場合もありうる。

```
<Signature>
  <SignedInfo>
   <SignatureMethod Algorithm = "rsa-sha1"/>
   <Reference URI =" 文書1 ">
    <DigestMethod Algorithm="sha1"/>
    <DigestValue>j6lwx3rvEPbeu8nk=</DigestValue>
   </Reference>
  </SignedInfo>
  <SignatureValue>MC0CFFrVLt=</SignatureValue>
  <KeyInfo>
    ・・・
  </KeyInfo>
</Signature>
```

図3．XML署名の例　XML-Signatureのエレメントの一例を示す。
XML-Signature element

Referenceタグは，署名対象の指定とハッシュ値を記述する。例では一つのタグしかないが，図2の例の場合には，それぞれの署名対象に対してReferenceタグが存在する。署名対象の指定方法としては，対象のURL（Uniform Resource Location），又はXMLドキュメント内の特定のエレメントの場合には，ID（IDentification）などで示される参照先を指定することができる。

SignatureValueタグは，このXML-Signatureの署名値を記述しており，SignedInfoエレメント以下の電子署名の値が入る。また，署名に用いた鍵（かぎ）について，証明書情報をKeyInfoエレメント以下に入れることができる。

XML-Signatureを作成する場合のステップを以下にまとめて示す。

⑴　署名対象の指定
⑵　署名対象のハッシュ値の計算
⑶　SignedInfoの作成と署名値計算
⑷　Signatureエレメントの作成

また，XML-Signatureの検証は次の段階をとる。

⑴　KeyInfoエレメントの証明書情報の検証
⑵　SignatureValue及びSignedInfoエレメントから，SignedInfo以下が改ざんされていないことを検証
⑶　個々のReferenceエレメントについて，署名対象とハッシュ値の検証

3 プラグインの機能

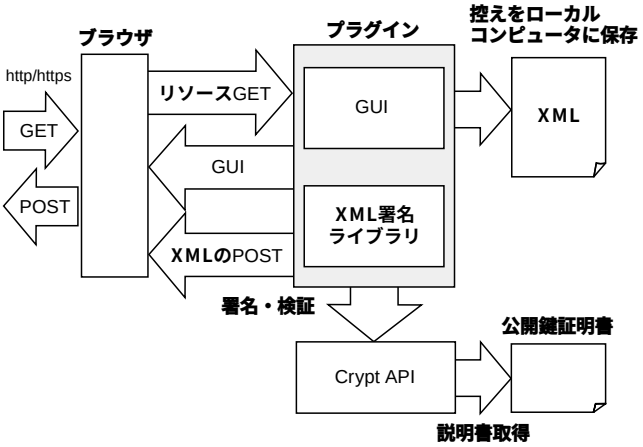
ここでは，XML-Signatureをブラウザのプラグインにより実現する場合に必要となる機能の検討を行う。プラグインは，Webブラウザに組み込むことで，特定のデータに対して独自の表示・処理を可能とするためのソフトウェアである。

ECや電子申請において，申込書や申請書に署名を付与

して送信する場合，クライアント側のアプリケーションでは，おおむね以下のプロセスを経ることになる。なお，ここで申込用紙や申請書はXMLで記述されるものとする。

⑴　入力された申請・取引情報を基にXML文書を生成
⑵　XML文書に署名を付与
⑶　場合によっては，控えとして保存
⑷　申請先に送信

これらプロセスの内，アプリケーションごとに特化した部分は⑴のXML文書作成だけで，他はおよそ同一のプロセスと言える。そこで，⑵～⑷の機能をプラグインの機能として備えるようにすれば，サービス提供側は，アプリケーションに特化した⑴の機能だけ開発すればよく，アプリケーションが非常にシンプルになる。特に，ローカルコンピュータのストレージへの保存や送信機能をプラグインが持つことで，JavaApplet(注1)などの特別なソフトウェアをロードしなくても，HTMLのフォーム機能やスクリプト言語によりアプリケーションが実現可能となる。プラグインの構成を図4に示す。



GET，POST：HTTPプロトコルにおいて，交換されるメッセージの一つ。
https　　：セキュリティ保護されたHTTPプロトコル

図4．プラグインの内部構造　　GUIとXML署名ライブラリから構成される。
Structure of plug-in

プラグインは，プラグインAPI（Application Programming Interface）を通じてブラウザと接続される。ブラウザは，署名を付与すべきXMLデータ（リソース）をHTTP（Hyper Text Transport Protocol）のGETメソッドにより受け取ると，署名プラグインを起動し，リソースを渡す。プラグインは，ブラウザ上にGUI（Graphical User Interface）を表示し，署名対象の指定，及び署名に用いる公開鍵証明書をユーザーに選択させる。これらの情報が選択され，署名ボタンが押されると，XML署名ライブラリにより署名の検証が行われる。

（注1）　Java及びその他のJavaを含む商標は，米国SunMicrosystems社の商標。

XML署名ライブラリは，指定された署名対象の情報に基づきSignatureエレメント以下を生成し，暗号ライブラリ（CryptAPI）により署名計算を行い，SignatureValueタグに値を入れる。これら処理が完了すると，プラグインはブラウザに署名完了画面を表示させる。

署名されたデータは，GUIの操作により，ローカルのコンピュータに控えとして保存することができる。また，ブラウザを通して，特定のURLに送信することができる。

4　テンプレート

プラグインのXML署名ライブラリにおいては，署名対象のXML文書中に埋め込まれたテンプレートを読み込めるようにしている。テンプレートには，署名対象として追加すべき文書又は図面などのURLがあらかじめ記述されており，プラグインがテンプレートを読み込むことで，自動で署名対象を指定できるようにしている。XML-Signatureの規格では，署名対象をURLで指定するようになっているが，この機能を用いることで，ユーザーはURLやXMLの構造などを知らなくても，簡単に署名を行うことができる。

テンプレートで指定可能なXML文書は，テンプレートを含むXML文書中の任意のエレメントと，外部の文書（添付文書など）である。XML文書中のエレメントに対しては，IDなどの参照により指定する。外部の添付文書については，文書のファイル名だけを指定し，プラグインのGUI上で，ユーザーが同一ファイル名のデータをファイルダイアログで指定することができる。なお，テンプレートに記述されている署名対象以外のデータでも，GUI上で指定することで追加が可能である。

テンプレートを埋め込んだXML文書の一例を図5に示す。

```
<purchaseOrder>
  <order id =“ 注文書 ”>
    <name>○○○</name>
    <address>東京都府中市△△△△</address>
    <item>□□□バッグ<item>
    <price>12000¥<price>
  </order>
  <SignatureTemplate>
    <SignedInfoTemplate>
      <ReferenceTemplate URI =“ #注文書 ”/>
    </SignedInfoTemplate>
  </SignatureTemplate>
</purchaseOrder>
```

図5．テンプレートの例　　テンプレートを埋め込んだ注文書の一例を示す。
Example of signature template element

前述の例では，署名対象としてorderエレメント以下を指定している。テンプレートはSignatureTemplateエレメント以下であり，ReferenceTemplateタグで署名対象のorderエレメントを指定している。プラグインでは，このようなXMLデータを読み込んだ場合，SignatureTemplateエレメント部分と入れ替えてSignatureエレメントを生成する。

5 署名の利用方法

XML署名適用の一例として，ネット上で商品の購買を行うサービスの例を考える。初めに利用者は，ネットショップのサービスを提供しているWeb上のホームページを，Webブラウザ上で閲覧する。ホームページ上で購入商品を決定し，氏名・住所などの顧客情報，決済方法とともに入力を行う。

入力内容はWebサーバに送信され，入力内容を基に購買申込書をXML形式で作成する。ここで，XML文書には署名対象を記述したテンプレートを挿入しておく。申込書は顧客に送られ，ブラウザに表示される。顧客は購入申込内容を確認したうえで“ 署名付与 ”ボタンを押すと，プラグインの画面が表示される。

画面上では，テンプレートに記述されていた署名対象がリストアップされる。また，公開鍵証明書を選択するボタンがあり，顧客はボタンを押して証明書選択画面を表示し，リストから証明書を選ぶ。

プラグインのGUI画面において，証明書が選択された時点での表示画面を図6に示す。図は，ネット上のショップでバッグの購入をしようとしている画面である。画面上で署名ボタンを押すことで，署名が付与されたXML文書が作成され，署名完了画面が表示される。

完了画面上では送信ボタンが表示され，署名が付与されたXML文書をWebサーバに送ることができる。Webサーバ側では受け取ったデータを検証し，問題がなければ，顧客のブラウザに“ お買い上げありがとうございました ”などのメッセージが送信される。

図6．ネット上の商店における署名の利用例　商品購買要求の確認画面でプラグインが起動し，署名を促す。
Example of signature use in online shopping

6 あとがき

WebベースのECや電子申請において，Webブラウザ上でXML署名の付与・検証を可能とするプラグインを開発した。

この開発では，W3Cで標準化が進められているXML-Signatureを採用し，アプリケーションに依存しない署名付与・検証環境の構築を目指した。

また，開発したプラグインは，アプリケーション共通の機能として，署名付与・検証機能に加え，署名したファイルのローカルコンピュータへの保存，及びWebサーバへの送信機能を持つことで，Formベースやスクリプトでの簡単なアプリケーション開発を容易に行えるようにした。

文　献

(1) Mark, B. "XML-Signature Syntax and Processing". W3C Candidate Recommendation. http://www.w3.org/signature/

西澤　秀和　NISHIZAWA Hidekazu, D. Eng.
e-ソリューション社 SI技術開発センター SI技術担当，工博。XML及び情報・ネットワークセキュリティの研究・開発に従事。
Systems Integration Technology Center

才所　敏明　SAISHO Toshiaki
e-ソリューション社 SI技術開発センター 戦略企画担当参事。暗号・情報セキュリティの研究・開発に従事。情報処理学会，CSI，ACM，IEEE会員。
Systems Integration Technology Center