2004－CSEC－25　(1)
2004／5／21

サーバによる電子文書の長期署名フォーマット生成方式

島　成佳　　小松　文子
日本電気株式会社　システム基盤ソフトウェア開発本部
〒108-8557 東京都港区芝浦 2-11-5
E-mail: shima@ap.jp.nec.com, a-komatsu@ay.jp.nec.com

概要：　電子署名が施された電子文書は，証明書の有効性が失われると同時に信頼性を失う．電子署名を長期に保証するためには，署名者または検証者が電子署名の有効時の検証情報を収集し，それらの情報を存在証明したものを長期署名フォーマットに格納する．本論文では，長期署名フォーマットをサーバにおいて安全に生成する方式と，その効果について述べる．

Building Method of Long Term Electronic Signature Formats for Digital Documents on the Server

Shigeyoshi SHIMA, Ayako KOMATSU
NEC Corporation,
System Platform Software Development Division
2-11-5 Shibaura, Minato-ku, Tokyo, 108-8557, Japan
Email: shima@ap.jp.nec.com, a-komatsu@ay.jp.nec.com

Abstract：　When a public key certificate is not valid, Digital documents with electronic signature are not valid. If a digital signature is held on the long term of validity, a signer or a verifier will collect some validation data of electronic signature and build a long term electronic signature. In this paper, we propose building method of long term electronic signatures by the server.

１．　はじめに

近年，インターネット上での電子商取引が広がりをみせており，電子取引において文書の電子化が進んでいる．文書の電子化に関しては，電子署名法や IT 一括書面法の 2001 年 4 月の施行や，e-Japan 戦略 II 加速化パッケージの e 文書法の制度化に向けた活動などがあり，電子文書が法的に紙と同等の効力を持つような環境整備が行われている．現在法的に有効な電子文書には，公開鍵基盤(PKI)を使用した作成者の電子署名が施されている必要がある．電子署名は，電子文書の作成者と非改ざん性を保証しており，認証局から発行された証明書によって検証可能である．証明書には有効期間が存在しており，有効期間が切れると

電子署名の信頼性が失われてしまう．そのため電子文書を長期に保証するためには，電子署名の信頼性を長期に保証する必要がある．電子署名の長期保証では，電子署名が有効であるうちに電子署名の検証情報を収集し，電子署名と検証情報が有効時点においての存在したことを証明する必要がある．検証情報は認証局証明書，署名者証明書，CRL(Certificate Revocation List)などである．また存在証明には，タイムスタンプ[1]や，耐タンパーな装置などを使用する方式がある．本論文では存在証明にタイムスタンプを用いている．電子署名や検証情報，タイムスタンプの格納に関しては，ETSI[1]や IETF[2]，OASIS[3]においてフォーマットが標準化されている．フォーマットの表記としては，ASN.1 形式の Electronic Signature Formats for long term electronic signatures[2]と，XML 形式の XAdES (XML Advanced Electronic Signatures)[3]の 2 つがある．本論文では電子署名や検証情報，タイムスタンプを格納するフォーマットを以降長期署名フォーマットと呼んで説明する．

2． 長期署名フォーマット

本節では長期署名フォーマットと作成手順の概要を述べる．

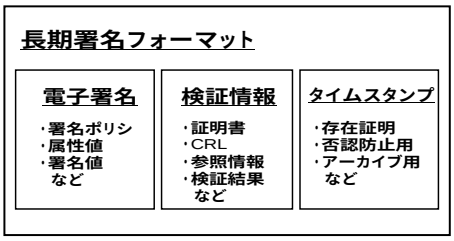

図1：長期署名フォーマット

[1] The European Telecommunications Standards Institute
[2] The Internet Task Engineering Task Force
[3] Organization for the Advancement of Structured Information Standards

長期署名フォーマットには，図 1 に示すような情報が格納されており，電子署名を論理的に保証する．本論文では，電子文書の作成者が過去に電子文書が存在したことを証明するために用いている．作成者は次のような手順によって長期証明フォーマットを作成する．

① 電子文書や，属性情報，署名ポリシなどのハッシュ値から署名値を生成し，電子署名を生成する．そして電子署名フォーマットを生成する．
② 電子署名の検証情報を収集して，電子署名の検証を行い長期署名フォーマットに追加する．
③ ①，②の情報に対して，タイムスタンプ局からタイムスタンプを取得して，長期署名フォーマットに追加する．

このあと 4 節において，①の署名値生成処理部分のみをクライアント行い，それ以外の処理をサーバで行う方式について述べる．

3．システム構築における課題

本論文では，システム要件として，クライアントが電子文書管理システムから電子文書をダウンロードし，サーバに電子文書の長期保管要求を行うものとする．サーバは組織外部とのネットワークと通信することが可能であり，外部のタイムスタンプ局と通信し，利用者制限や課金管理などを行うものとする．また CRL のサイズが数 MB と比較的大きい環境を想定している．電子文書は一般的に 1MB 未満であり，数 MB の CRL を含む長期署名フォーマットを共に格納すると電子文書の数倍の記録容量を必要とするという問題がある．また各クライアントが長期署名フォーマット作成のために数 MB の CRL をダウンロードことで，ネットワークに負荷がかかるという問題もある．そのため長期署名フォーマットをサーバ側

で作成することで，サーバのみが CRL を取得することを考えた．また長期署名フォーマットに CRL でなく CRL の参照情報を使用することで，長期署名フォーマットのサイズを小さくすることができる．これらを実現するために，次の 2 つの課題を解決する必要がある．

- クライアントとサーバで，長期署名フォーマットを安全に生成すること
- 長期署名フォーマットに CRL を含まなくても後に問題なく検証できること

４．長期署名フォーマットの分離生成方式

本節では，署名値を除く長期署名フォーマットの生成をサーバで行い，署名値の生成をクライアントで行うための安全な方式について述べる．本方式のクライアントとサーバ間の処理について図２に沿って説明する．

- h_x：x のハッシュ値
  (doc は電子文書，sig は署名対象)
- Pub_x(y)：x の公開鍵で y を暗号化した値
- Sig_x(y)：x の署名鍵で y を署名した値
- Cert_x：x の証明書

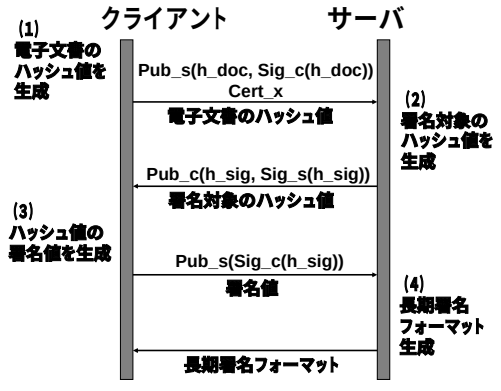

図２：署名部分分離方式処理

図２の(1)から(4)までの処理を説明する．

はじめにクライアントの(1)の処理について電子文書のハッシュ値の生成から送信までを説明する．

(1.1) クライアントは，電子文書のハッシュ値 h_doc を生成する．

(1.2) ハッシュ値 h_doc をクライアントの秘密鍵で署名値 Sig_c(h_doc)を生成する．

(1.3) サーバの公開鍵で h_doc と sig_c(h_doc)暗号化して Pub_s(h_doc, Sig_c(h_doc))を生成する．

(1.4) サーバに Pub_s(h_doc, Sig_c(h_doc))とクライアント証明書 Cert_c を送信する．

ここではハッシュ値の完全性保証のために署名値を生成している．またハッシュ値の漏洩防止のため暗号化を行っている．

次にサーバの(2)の処理について，電子文書のハッシュ値の受信から電子署名の署名値生成要求を送信までを説明する．

(2.1) サーバの秘密鍵で，Pub_s(h_doc, Sig_c(h_doc))を復号して h_doc と Sig_c(h_doc)を取り出す．

(2.2) クライアント証明書の公開鍵で Sig_c(h_doc)の署名値を検証する．このとき信頼する認証局までの証明書検証を含む．

(2.3) ハッシュ値 h_doc とクライアント証明書，署名ポリシなどの情報を元に署名対象データを生成する．

(2.4) 署名対象データのハッシュ値 h_sig を生成する．

(2.5) ハッシュ値 h_sig にサーバの秘密鍵で署名値 Sig_s(h_sig)を生成する．

(2.6) クライアントの公開鍵で h_sig,と Sig_s(h_sig)を暗号化して Pub_c(Sig_s(h_sig)を生成する．

(2.7) クライアントに Pub_c(h_sig, Sig_s(h_sig))を送信する。

ここでは(1)と同様の理由でハッシュ値に署名，暗号

化を行っている.

次にクライアントの(3)の処理について, 署名対象データのハッシュ値の受信から署名値の送信までを説明する.

(3.1) クライアントの秘密鍵で Pub_c(h_sig, Sig_s(h_sig))を復号して h_sig と Sig_s(h_sig)を取り出す.

(3.2) サーバの証明書の公開鍵で Sig_s(h_sig)を検証する. このとき信頼する認証局までの証明書検証を含む.

(3.3.) クライアントの秘密鍵で h_sig の署名値 Sig_c(h_sig)を生成する.

(3.4) サーバの証明書の公開鍵で Sig_c(h_sig)を暗号化して Pub_s(Sig_c(h_sig))を生成する.

(3.5) サーバに Pub_s(Sig_c(h_sig))を送信する.

次にサーバの(4)の処理について, 署名値に受信から長期署名フォーマット生成までの処理を説明する.

(4.1) サーバの秘密鍵で Pub_s(Sig_c(h_sig))を復号して Sig_c(h_sig)を取り出す.

(4.2) クライアント証明書の公開鍵で Sig_c(h_sig)を検証する. このとき信頼する認証局までの証明書検証と, (2)で送信したハッシュ値 h_sig と同じであるかの確認を含む.

(4.3) (4.2)で署名値を検証した証明書, CRL などから検証情報を作成.

(4.4) 署名対象データと, Sig_c(h_sig)から電子署名を生成.

(4.5) 電子署名と検証データから長期署名フォーマットを生成. このときタイムスタンプ部分は含まれていない.

(4.6) 長期署名フォーマットのハッシュ値に対してタイムスタンプを取得し, タイムスタンプを長期署名フォーマットに追加する.

(4.7) クライアントに長期署名フォーマットを送信する.

5. CRL 参照情報の格納方式

本方式では CRL のサイズが比較的大きな環境において, 長期署名フォーマットのサイズが小さくなるように CRL そのものを格納せず, CRL の参照情報を格納するものである. 参照情報には, CRL のハッシュ値と, 発行者, 発行番号を用いた. 参照情報には検証局が証明書を検証した結果情報を使用できるが, 電子署名の再検証の際に証明が複雑になるため使用しなかった. CRL は一般的に数時間から数日程度間隔で発行されており, 認証局において過去のものが保管されていない. また CRL の電子署名の有効期間切れてしまうと, CRL が存在したこと自体証明することが困難になる. そのため CRL の参照情報を用いる際には, CRL の存在証明を行い保管しておく必要がある. 本方式では, 図3のようにサーバにおいて, CRL と CRL のタイムスタンプを保管と管理を行う.

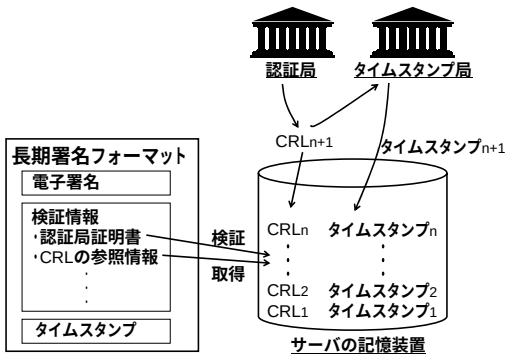

図3：CRL の保管と管理

電子文書の検証者は, 長期署名フォーマットを検証する際に, 検証情報の CRL の参照情報を元にサーバから CRL を取得する. また本方式では, 取得した CRL を検証情報の認証局証明書により検証が可能であるため, タイムスタンプの対象を CRL のみとしている.

6．本方式の考察

長期署名フォーマットの分離生成方式には次のような特徴がある.

- クライアントはサーバに電子文書の電子文書のハッシュ値のみを送信しているため，サーバに電子文書の内容を知られることがない.
- ハッシュ値は，通信相手の証明書の公開鍵によって暗号化されているため，第三者による通信路上の盗聴が困難である.
- ハッシュ値の送信時に共にハッシュ値の署名値を送信しているため，ハッシュ値と作成者と関連性の確認可能であり，クライアントやサーバのなりすましを防止している.
- クライアントはサーバから受信した電子署名フォーマットを検証することで，サーバで不正が行われたどうか確認することが可能である.

長期署名フォーマットにおいて, CRL の参照情報を用いた効果について述べる．例えば CRL サイズが 2MB 程度の環境において，サーバが CRL を保管することで，保管文書と共に格納する長期署名フォーマットのサイズを 2MB 程度小さくすることが可能である．一般的に PDF 文書のサイズが 1MB 未満であることから，CRL が 2MB の環境において必要な記憶装置の容量が 3 分の 1 以下になる．つぎに実際の運用例を元に考察する．電子文書の長期保管の申請量が月間 1 万件あり，そのドキュメントを 10 年間保管すると想定する．また電子文書の平均サイズは 1MB , CRL の発行間隔は 1 日でサイズが 2MB，長期署名フォーマットは 10KB 未満と考え誤差の範囲とする．このときサーバで CRL を保管しない場合は，3.4TB の記憶容量が必要となる．一方サーバで CRL を保管する方式では，サーバ内の CRL のための記憶容量が 7.3G で，電子文書の記録容量が 1.2TB となり，2.4TB 程度記憶容量が小さくて済む.

7．おわりに

本論文では，長期署名フォーマットをクライアントとサーバで分離して生成する安全な方式と，CRL のサイズが比較的大きな環境においての効果について述べた．今後も電子文書の長期保管に関する課題を検討して，解決していきたいと考えている.

参考文献

[1] C. Adams, C. Cain, D. Pinkas, R. Zuccherato, “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”, RFC3161, August 2001.

[2] D. Pinkas, J.Ross, N. Pope, “Electronic Signature Formats for long-term electronic signatures”, RFC3126, September 2001.

[3] ETSI, “XML Advanced Electronic Signatures (XAdES): ETSI TS 101 903 V1.1.1”, February 2002.