

電子文書の長期原本性保証を実現する EVERSIGN

EVERSIGN: Long-Term Storage System for Signed Documents

宮崎 一哉*
(Kazuya Miyazaki)
山中 忠和*
(Tadakazu Yamanaka)
田中 学**
(Manabu Tanaka)

要 旨

e-文書法の施行や日本版 SOX 法（「証券取引法等の一部を改正する法律」及びその整備法）の成立により、文書の真実性や適正性が強く問われる状況となっている。電子的な文書の真実性や適正性を確保するためには、電子署名やタイムスタンプが利用される。これらはデジタル署名という公開鍵暗号基盤 PKI(Public Key Infrastructure)に基づく技術で構成されるが、この技術は公開鍵証明書が持つ有効期間や失効というしくみに起因する制約のため、長期間その有効性を維持することができない。

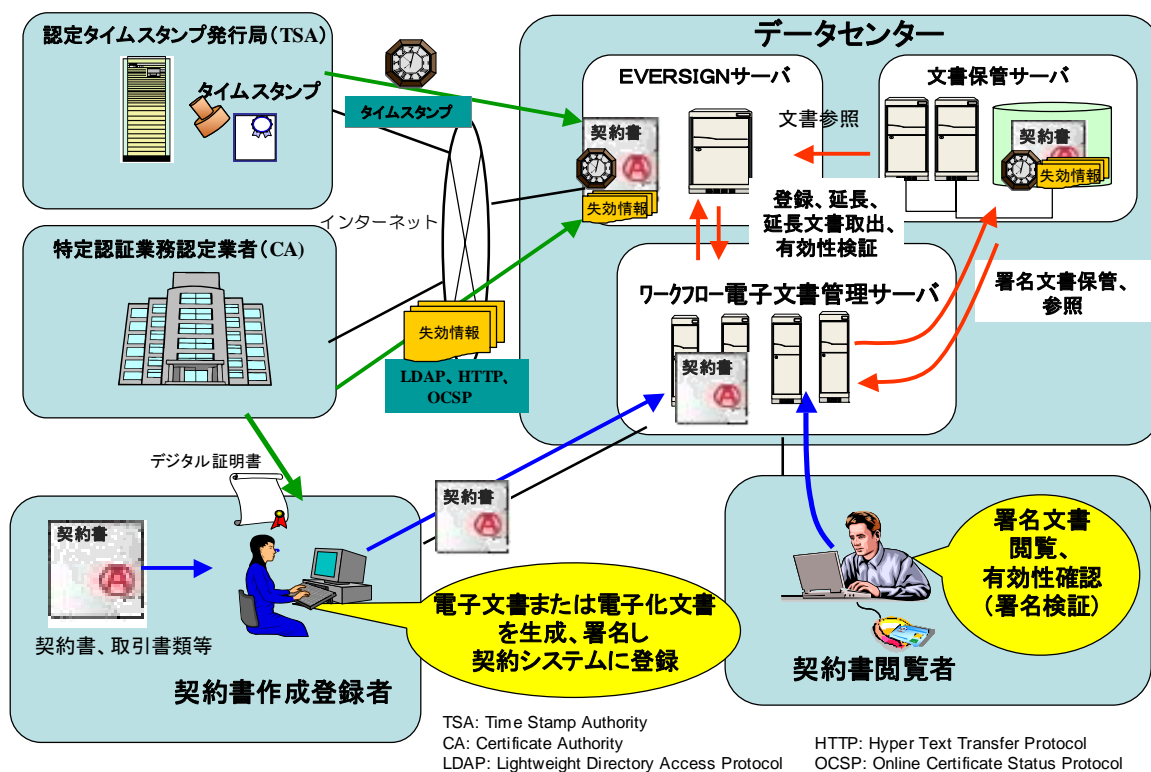
長期署名フォーマットは、デジタル署名の持つこのような制約を解消するための効果的な手段を提供するためのフォーマットである。長期署名フォーマットによるデジタル署名の有効性延長方式は、その構築や検証が複雑であるものの、誰でも有効性を検証できる極めてポータビリティが高い等の優れた特長を持つ。

長期署名フォーマットは国際的な標準仕様として定義されている。ポータビリティ確認のために 2005 年度末には次世代商取引推進協議会（ECOM）で、標準プロファイルに基づく相互運用性実験が実施された。

“三菱署名有効性延長システム MistyGuard^(注1) <EVERSIGN^(注2)>” は、標準の長期署名フォーマットの自動構築や検証機能を提供するサーバシステムであり、上記相互運用性実験において、標準プロファイルへの適合性が確認されている。e-文書法や日本版 SOX 法に適合するシステムを構成するコンポーネント製品として、既にいくつかの電子文書・記録管理システムで採用されており、今後、ますます同分野での貢献が期待される。

(注1) MistyGuard は、三菱電機（株）の登録商標である。

(注2) EVERSIGN は、三菱電機インフォメーションシステムズ（株）の登録商標である。



EVERSIGN を応用した長期保存機能付き電子契約書管理サービス例

電子契約書の真実性確保のためには、電子契約書にデジタル署名を付与した上で送受を行う。最終的に電子契約書を保存する場合、法律で定められた保存期間（例えば 7 年、10 年等）にわたってデジタル署名の有効性を維持する必要がある。EVERSIGN を導入することにより、通常は 1～3 年で切れる有効性を永続的に維持することが可能となる。

1. まえがき

2005年4月1日に施行されたe-文書法（「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」及びその整備法）により、原則的に全ての保存義務のある文書を電子的に保存することが許された。これは主に紙文書の保管コストの削減ニーズに端を発するものであったが、電子的文書の活用による業務の効率化や紙文書の削減による資源保護といった積極的な目的にもかなう動きである。

一方、米国におけるエンロンやワールドコムによる会計不祥事を契機に、2002年7月に企業改革法（サービンス・オクスリー法：SOX法、「Public Company Accounting Reform and Investor Protection Act of 2002：上場企業会計改革及び投資家保護法」）が米国で承認され、日本でも日本版SOX法（「証券取引法等の一部を改正する法律」及びその整備法）が2006年6月に成立・公布された。

e-文書法では、税務関連文書や医療関連文書等の重要な文書については、電子的保存の要件として“真実性の確保”が挙げられており、真実性の確保のためにデジタル署名及びタイムスタンプを利用することが要求されている。

また、日本版SOX法においては、記録の適正性及び適切に記録及び保存されることが要件として挙げられているものの、“記録”が電子的なものであるとは限らないこともあり、具体的にそれらの技術の利用が要求されているわけではない。しかし、日本版SOX法においては、ITが組織に浸透した現状に即して“ITへの対応”が謳われており、電子的な記録の適正性確保と保存が要求されることが考えられる。

本稿で紹介する“三菱署名有効性延長システムMistyGuard<EVERSIGN>”は、標準の長期署名フォーマットに基づいて、電子的な文書や記録の真実性あるいは適正性を長期にわたって保証することにより、e-文書法や日本版SOX法に適合するシステムを構成するコンポーネント製品である。次章以降、署名有効性延長の仕組み、ECOMで実施した長期署名フォーマット相互運用性実験への参加結果、そして適用事例について述べる。

2. 署名有効性延長の仕組み

電子的な文書や記録の真実性確保には、デジタル署名を用いる。デジタル署名とは、公開鍵暗号基盤PKI(Public Key Infrastructure)における電子署名のことであり、認証局の発行する公開鍵証明書に信頼の基点を置く。公開鍵証明書には、有効期間や失効という仕組みが存在し、デジタル署名の有効性は公開鍵証明書の有効期間や失効に依存する(図1)。つまり、公開鍵証明書が有効期間を超過しあるいは失効してしまうと、デジタル署名の有効性も失われる。

これは、公開鍵証明書が有効期間を超えてしまうと、署名用の鍵の漏洩やアルゴリズムの脆弱化により署名が偽造される可能性を否定できなくなるためであり、また失効の場合も同様で、漏洩した鍵により署名が偽造される可能性を否定できなくなるためである。

デジタル署名には時刻情報を含めることが可能であるが、それは通常、デジタル署名を生成するパソコンのシステム時計の時刻が用いられる。この時刻はパソコンの管理者が自由に変更できるため、一般に信頼できる時刻とは考えられない。そのため、署名の再検証を行う際

に、署名が有効期間内に作成された本物なのか、その後作成された偽物なのかの区別がつかない。失効が生じた場合にも、同様に失効前の署名なのか失効後の署名なのかを区別することができない。更に有効期間後は失効情報さえ発行されないため、失効の有無をも確認できなくなる。

従って、通常は1～3年程度でデジタル署名の有効性は失われてしまうため、診療録では5年、税務関連文書では7年、その他30年から永年にわたって保存義務のある文書を、真実性を保ったまま保存することができないことになる。

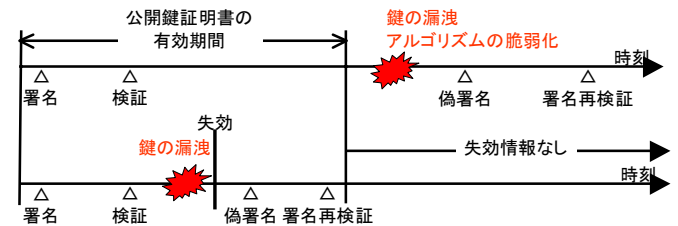


図1 デジタル署名の限界

署名有効性延長とは、公開鍵証明書の有効期間や失効、更にはデジタル署名で利用している暗号技術の脆弱化を克服し、長期にわたってデジタル署名の有効性を維持する技術である。署名有効性延長の要件①を次に示す(図2)。

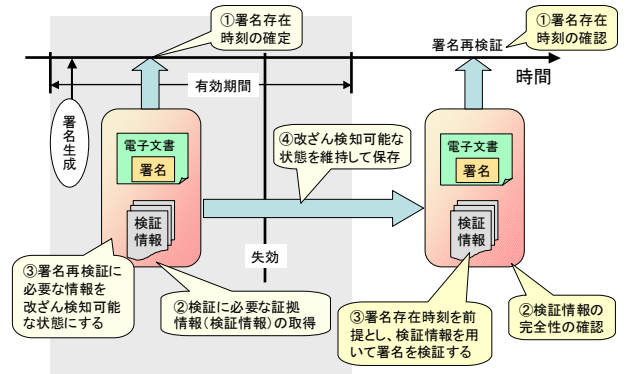


図2. 署名有効性延長の要件

要件① デジタル署名の存在時刻を確定する:デジタル署名に信頼のできる時刻を与え、有効期限や失効との前後関係を確認可能とする。

要件② デジタル署名の検証に必要な証拠情報(検証情報)を取得する:署名者の公開鍵証明書からルート認証局までの公開鍵証明書のセット、それらの公開鍵証明書に対するCRL(Certificate Revocation List)やOCSP(Online Certificate Status Protocol)レスポンス等の失効情報を収集する。

要件③ デジタル署名の再検証に必要な情報を改ざん検知可能な状態にする:元々の署名付電子文書や検証情報を改ざん検知可能な状態とする。

要件④ ③の改ざん検知可能な状態を維持して保存する:③の状態を必要な保存期間にわたって維持する。

要件①から④を満足すれば、次の確認①～③を行うことにより、元々の署名の真偽を区別することが可能となる。

確認① 署名存在時刻を確認する。

確認② 署名付電子文書や検証情報が改ざんされていないことを確認する。

確認③ 署名存在時刻を想定した検証を、検証情報を利用して実施する。

3. 長期署名フォーマット

前章の要件を満たす方法として長期署名フォーマット（図3）を利用する方法がある。長期署名フォーマットは RFC3126^④等として世界的な標準となっている。この方法では、各要件に次のように対応する。

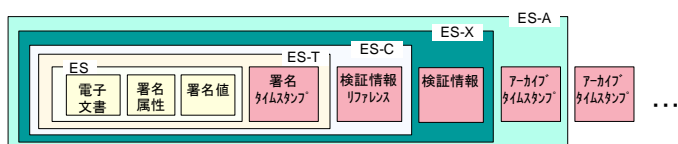


図3 長期署名フォーマット

要件① 署名値に対して標準のタイムスタンプを付与する（ES-Tの署名タイムスタンプ）

要件② 公開鍵証明書のセットと CRL や OCSP レスポンス等の失効情報を格納する（ES-C、ES-Xの検証情報リファレンスと検証情報）

要件③ 署名付文書（ES）、署名タイムスタンプ、検証情報リファレンス、検証情報全体にタイムスタンプを付与する（ES-Aのアーカイブタイムスタンプ）

要件④ 長期にわたって非改ざん性を維持するために、更に全体に対してタイムスタンプを重ねる（外側のアーカイブタイムスタンプ）

タイムスタンプによって要件③④を達成する長期署名フォーマットを利用する方法は、システムや運用の安全性を仮定することによって同様の効果を得ようとする方法（電子原本管理システム等）と比較して、次のような優れた特長を持つ。

- (1) 標準的な PKI 技術を用いることで誰でも有効性を検証できる。
- (2) 長期署名の構築や延長処理を誰でも実施でき、更に途中から他者に処理を引継ぐこともできる。
- (3) 信頼の対象を標準の PKI における信頼点に置けばよく、現状では一般的に確認が困難なシステムや運用の安全性に置く必要がない。
- (4) タイムスタンプは常にその時点で安全性が確認されている暗号技術を用いてサービスされるため、技術の陳腐化を気にする必要はない。

4. 署名有効性延長システム MistyGuard<EVERSIGN>

長期署名フォーマットを構築するためには、署名タイムスタンプの取得、失効情報を含む検証情報の取得、アーカイブタイムスタンプの

取得をそれぞれ適切なタイミングで実施し、長期署名フォーマット内に適切に格納する必要がある。タイミングの管理はさきわめて複雑であり、一般にその作業を個々の利用者に任せることは難しい。

また、構築された長期署名を検証する際も、元々の署名、署名タイムスタンプ、検証情報、アーカイブタイムスタンプ等をそれぞれ定められた時刻（各タイムスタンプが示す時刻等）を想定した上で実施し、更にタイムスタンプの示す時刻と有効期間や失効時刻との整合性を確認した上で真偽の判定をしなければならない。

三菱署名有効性延長システム MistyGuard <EVERSIGN>は、サーバタイプのシステムであり、決められたプロトコルに従って署名付文書を登録するだけで、長期署名フォーマットを自動的に構築する。EVERSIGN サーバが内部にスケジューラをもち、各種タイミングやタイムスタンプサービス等の各種データ取得先に関する設定に基づき、処理を自動実行することによってこのような動作が実現される。構築された長期署名データは、やはり決められたプロトコルに従って利用者が取得することができる。

また、長期署名の検証についても、検証プロトコルを用いて EVERSIGN サーバにリクエストを発行することにより、検証結果のレポートを得ることができる。

EVERSIGN サーバとのリクエスト/レスポンスのやり取りは、EVERSIGN クライアントライブラリを用いることにより、さまざまなアプリケーションに組み込むことができる。通常、EVERSIGN を単独で用いるのではなく、各種文書管理システムや記録管理システムと連携させることにより長期保存機能を拡張するような形態をとる。

5. 長期署名フォーマット相互運用性実験

2005年10月から12月にかけて、ECOMで長期署名フォーマット相互運用性実験を実施した^④。この実験は、ECOMで策定した“長期署名プロファイル”への準拠性と各社製品間の相互運用性を確認することを目的としたものである。同プロファイルは、標準の長期署名フォーマットが持つ冗長性とあいまい性を極力排除するために策定したものである。このプロファイルに従った実装を行うことで、長期保存を目的とした長期署名の構築や検証が可能となる。

実験には合計13社の製品あるいは試作品が持ち込まれたが、当社関連では、三菱電機（株）情報技術総合研究所の試作品と三菱電機インフォメーションシステムズ（株）の製品、EVERSIGNが参加した。

実験は、次の二通り実施した。

- (1) オフライン検証実験：予め用意した ES フォーマットのデータ（ES-T、ES-X Long、ES-A）、検証情報、設定情報のセットをテスト対象として、各社の実装でオフラインにより有効性を検証する。
- (2) オンラインマトリックス生成・検証実験：各社の実装により生成された長期署名テストデータを、他社の実装がエラーなく読み込み、正しく検証できるかどうかを確認する。

当社関連の2つの実装を含み、各社の実装がテストに合格し、ECOMで定めた長期署名プロファイルに準拠することが確認された。

6. 適用事例

EVERSIGN は、2006 年 5 月より某社会インフラ系企業等の電子文書管理システムに組み込まれた形で稼働中である。このシステムは、システム導入企業とその企業との取引企業間で、電子契約を行うためワークフローと電子文書・電子化文書の保存管理機能を提供するサービスであり、EVERSIGN はシステム中核の文書保管サーバから、取引会社間で電子署名された契約書その他の取引書類に対して、長期署名フォーマットの生成、有効性の延長及び有効性検証機能を提供している。このシステムでは、e-文書法の改正電子帳簿保存法に対応するため、特定認証業務の認定を受けた証明書と、日本データ通信協会から認定された(株)PFU のタイムスタンプサービスを利用している(要旨イメージ図のシステム構成参照)。2006 年 6 月現在の実績では、運用開始直後であることと、初期の利用企業数を限定したこともあって、登録文書ベースで 3000 件/月程度の利用にとどまっているが、今後利用企業を増やしていく予定であり、利用規模が大きく拡大する見込みである。

また 2006 年の秋には、某金融機関が提供する全国規模の電子契約文書保管サービスでの利用も予定されている。このシステムでは、利用企業数、取り扱い文書数ともに現在稼働中のシステムを上回る見込みである。このシステムの基本的な構成は、本章で紹介した稼働中のシステムとほぼ同じであるが、複数の企業間で利用可能な ASP (Application Service Provider) サービスとして提供される予定である。また公開鍵証明書検証の仕組みとして、OCSP による失効検証方式が使用される予定である。

7. むすび

標準の長期署名フォーマットに基づき、電子的な文書や記録の真実性や適正性を長期間にわたって維持できる技術について紹介した。ここで述べた方法は、ある特定のシステムに縛られることなく、いつでも、誰でも、有効性の確認や、延長処理の引継ぎができるという利点を持つ。このようなポータビリティは、特に“長期”を考える上では、きわめて重要な意味をもつ。ある特定のシステムやサービスに依存するという事は、そのシステムやサービスを提供するある特定の企業や組織に依存するという事であり、ここでいうポータビリティを具備することにより、その企業あるいは組織の事業継続性に左右されてしまうことがなくなるからである。

ただし、このポータビリティという特長が活かされる前提として、相互運用性が実際に確保されていることが必須であるが、ECOM の相互運用性実験により、当社の実装がこの前提を満たしていることが確認されている。

今後予定されている日本版 SOX 法の施行により、文書や記録の真実性や適正性の確保とその保存が、今後ますます重視されることになる中、当社の技術や製品がそれらに大いに貢献していくことを期待する。

参考文献

- (1) 宮崎一哉, 他: 電子文書保存の仕組みと実務, 中央経済社 (2005)
- (2) RFC2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP (1999)
- (3) RFC3126: Electronic Signature Formats for long term electronic signatures (2001)
- (4) 次世代電子商取引推進協議会: 長期署名フォーマット相互運用性実験報告書 (2006)