4.XML署名事例調査報告
～ PKIでXML署名は使われている？ ～

XMLコンソーシアムWeek　2010年3月16日

セキュリティ部会

宮地　直人 (ラング・エッジ)

miyachi@langedge.jp

はじめに

- 事例調査の目的
  - PKI（公開鍵基盤）の世界でXML署名は使われているのか？
  - 事例をまとめてXMLを使ったPKIを広めて行きたい。
- セキュリティ部会2009年度第1回ミーティングで報告
  - 2009年6月4日のミーティングで資料にまとめて報告を行った。
- 本日の発表内容
  - 昨年の報告内容を簡単にまとめて発表。
  - 昨年の報告からほぼ1年が経過しているので新たな事例を追加。
  - 電子署名業界の最近の動向。

日本のPKI

- PKIとは証明書を発行する認証局を中心に秘密鍵と公開鍵（証明書）を管理して署名者の特定や保障をする仕組み。
  - GPKI（政府向け）/LGPKI（地方公共団体向け）
  - 特定認証局（税理士等の士業向け・一般向け）-GPKIと相互認証
  - 商業登記証明書（法人代表向け）-GPKIと相互認証
  - JPKI（一般向け）-「公的個人認証サービス」-GPKIと相互認証
  - HPKI（ヘルスケアPKI-保険医療福祉向け）
  - UPKI（全国大学共同電子認証基盤構築事業）
  - マイクロソフトトラストな認証局（Windows標準）
  - WebTrustな認証局（国際的な電子商取引保証規準）

PKIとXMLの関係

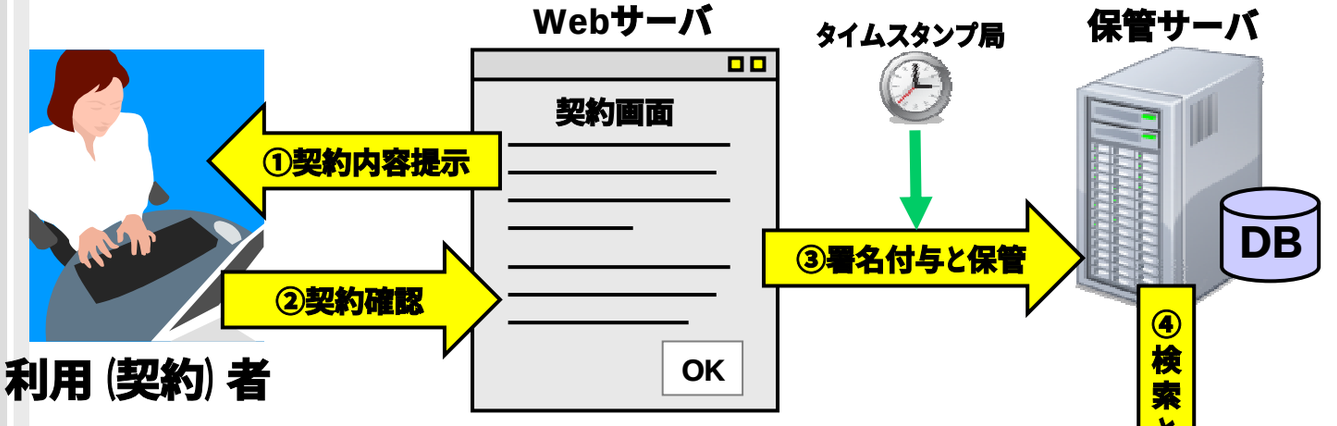
ASN.1は情報の構造を定義する抽象構文表記法

- PKIの世界ではASN.1のBER/DER形式が使われている
  - CMS署名データもX.509証明書もCRLも全てBER/DER形式。
  - BER/DERはバイナリ形式でありパーサが少なく可読性が低い。
- XML署名はCMS署名（バイナリ形式）とほぼ同等と言える
  - XMLパーサはDOM/SAX等標準化されているし可読性も高い。
  - 署名値や証明書はBER/DERバイナリをBase64化して利用。
- XML署名とCMS署名はどちらが使われている？
  - 海外ではXML署名の利用が広がっている。逆に日本はまだ少ない。
  - 署名対象がXMLデータならXML署名の方が使われるケースが多い。
  - 結局XML署名とCMS署名で出来る事は大差が無いとは言える。

署名対象フォーマットや最後は担当者の趣味で決まる？

事例1：電子契約データの保証と保管

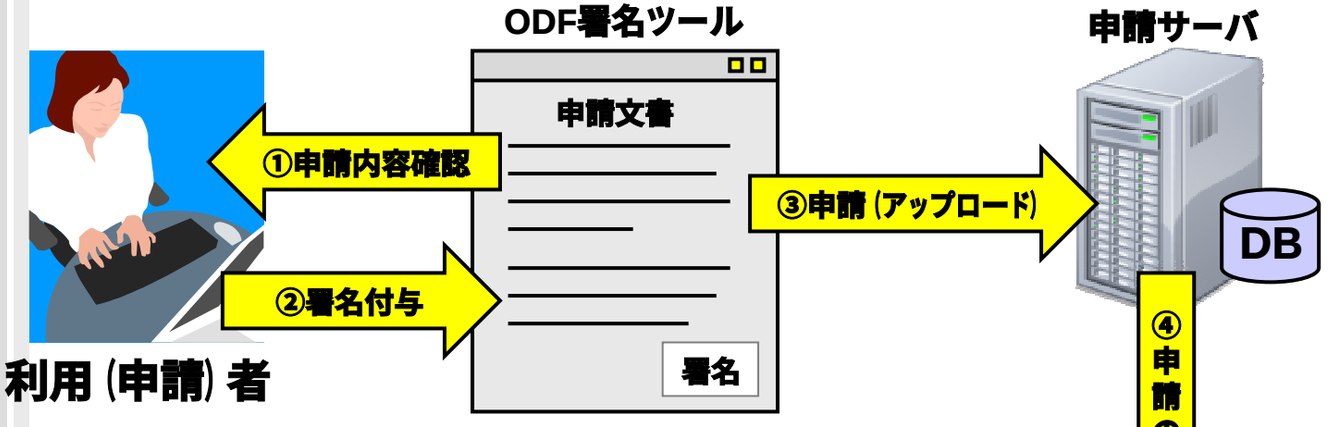
オンライン契約XMLデータにXML署名を付与して保証



署名は利用者が行うケースとサーバ側で行うケースがある。
保管時には長期署名（XAdES）を利用されるケースが多い。
タイムスタンプを併用して時間に関しても保証可能。
改竄と時間が保証されるのでコンプライアンス的に優れる。
電子契約書は印紙税の対象外となっている。
運用コストの低減と保管場所が少なくて済む。
電子署名法・J-SOX法・IT書面一括法等が関連法律。

事例2：電子申請1

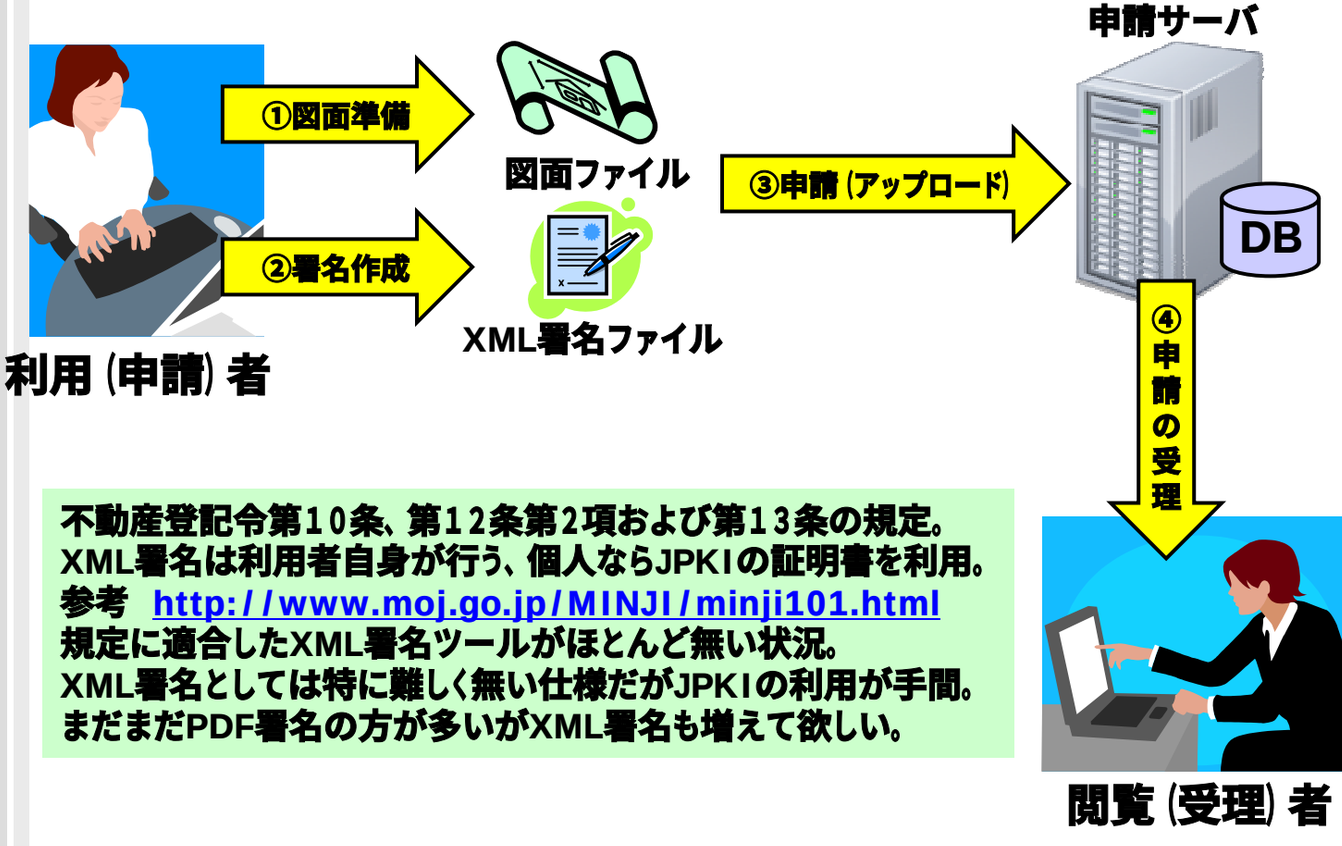
オンライン申請時に署名を付与したODFファイルを利用



署名は利用者自身が行う。
ODF文書の署名は内部フォーマットとしてXML署名を利用。
実際に特定認証局の証明書更新申請にて利用されている。
郵送だった業務がオンライン化でコストと時間が削減された。
電子署名法等が関連法律。

事例3：電子申請2（不動産登記）

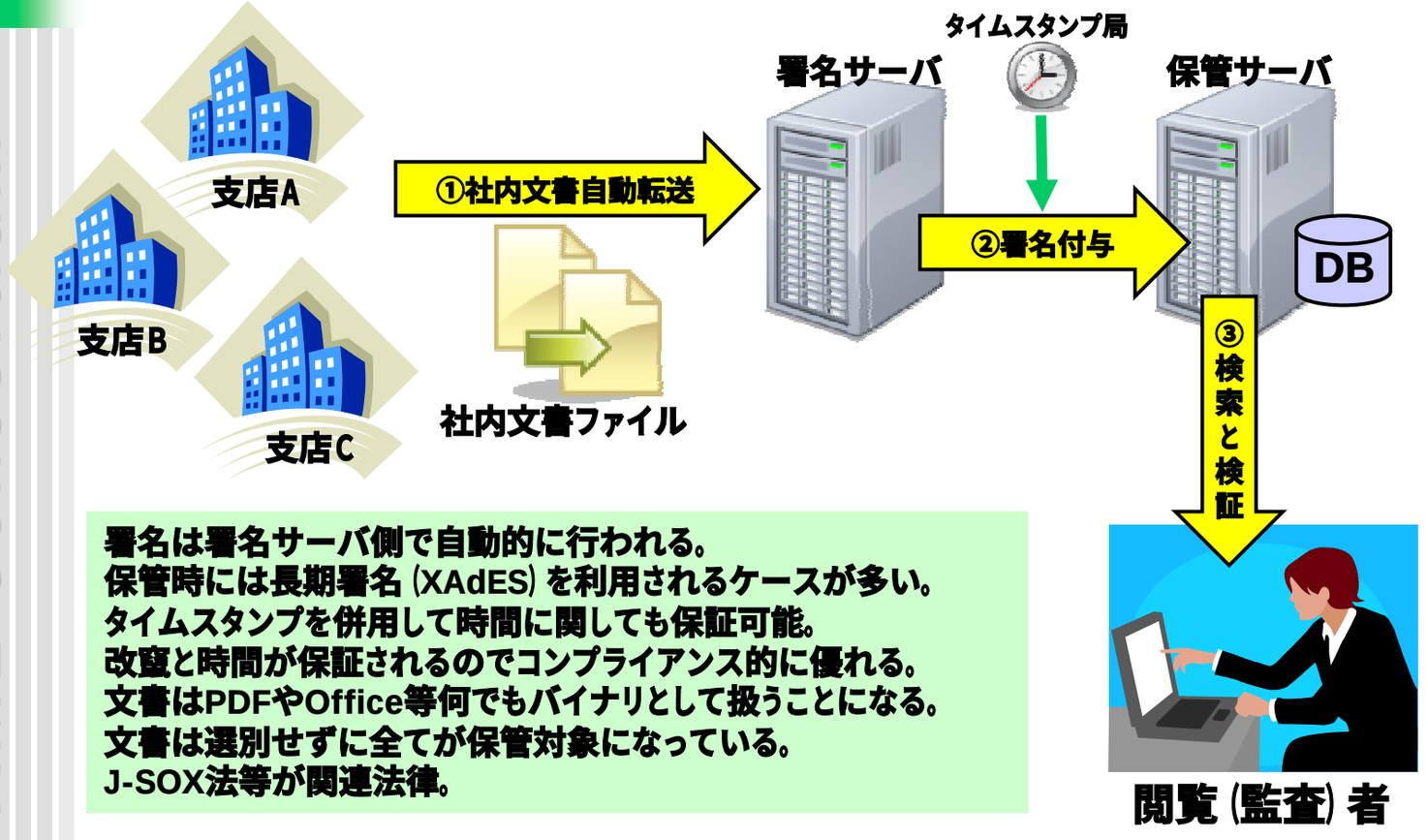
図面ファイルの申請時にXML署名ファイルを添付して提出



不動産登記令第１０条、第１２条第２項および第１３条の規定。
XML署名は利用者自身が行う、個人ならJPKIの証明書を利用。
参考　http://www.moj.go.jp/MINJI/minji101.html
規定に適合したXML署名ツールがほとんど無い状況。
XML署名としては特に難しく無い仕様だがJPKIの利用が手間。
まだまだPDF署名の方が多いがXML署名も増えて欲しい。

事例4：社内文書保管

株式公開企業の社内文書に対するコンプライアンスの遵守対応



署名は署名サーバ側で自動的に行われる。
保管時には長期署名（XAdES）を利用されるケースが多い。
タイムスタンプを併用して時間に関しても保証可能。
改竄と時間が保証されるのでコンプライアンス的に優れる。
文書はPDFやOffice等何でもバイナリとして扱うことになる。
文書は選別せずに全てが保管対象になっている。
J-SOX法等が関連法律。

その他事例（XML署名に限定しない）

PKIって使われているの？法的な対応は証拠性は？

- e-文書法：国税関連書類の保管
- PL法対応と先使用権保護による知財保護
- 会社法：取締役会議議事録等の電子化
- 医療分野：電子カルテや紹介状や外部保存での利用
  - 医療分野のデータにはXMLデータも多い
- 学術分野：論文やプレプリント情報の公開時の保護

：

電子認証局会議作成「電子署名活用ガイド」が参考になる。

http://www.c-a-c.jp/about/download.html

電子署名業界の最近の動向

- 長期保管の為に長期署名（XAdES/CAdES）が普及
  - JIS化され法的対応（長期保管）のニーズも増えて来ている。
- PDF長期署名（PAdES）がISO32000-2として検討中
  - まもなくCD（規格原案）を経てDIS（ドラフト）になる予定。
  - PAdESのXFA（XML Forms Architecture）はXAdESを利用。
  - PAdES原案はAdobeから提出されたのでサポートが期待される。
- 韓国ではPKIが既に普及しており新しい動きも
  - 政府のバックアップもあり電子証明書はビジネスマンなら必携。
  - 銀行口座を開くと電子署名が提供される。認証局も黒字。
  - 公認電子文書保管所にて一般向けの文書保管サービスも普及。

参考：韓国「公認電子文書保管所」

日本の認証局のように公的に認められた文書保管サービスを提供

サービス名		内容
基本サービス	保管サービス	様々なデジタルコンテンツ（電子文書）を安全に保管するサービス
	閲覧サービス	保管された文書の検索／閲覧サービス
	発行サービス	保管された文書の出力版（原本に替わる）発行サービス
	流通サービス	保管された文書を電子的に第三者に配送するサービス
付加サービス	スキャンサービス	スキャンニング作業による紙文書の電子化サービス
	SIサービス	利用者企業の内部システムと保管所の連携の為のソリューション及びSIサービス
保管所ベースの応用サービス	保管所独自の応用サービス	保管所事業者が独自に構築・提供する新規のサービス
	パートナー提供の応用サービス	外部のサービスプロバイダが保管所インフラと連携して提供する新規のサービス

※自分でサーバ運用できない規模の企業や個人だとこのようなサービスが必要になる。クラウドにあると便利？

電子署名業界の最近の動向2

- 「電子記録マネジメントコンソーシアム（ERMC）」の設立
  - ARMA/ECOM/JIIMA/JIPDEC/TBF が発起団体の予定。
  - 電子署名を実際に運用/利用する為に必要な課題を検討整理。
  - 各団体の情報を共有して電子文書マネジメント標準化を目指す。
  - http://www.ecom.jp/press/2010_001.pdf
- 「電子記録応用基盤フォーラム」の設立
  - ECOM（次世代電子商取引推進協議会）電子署名普及WGの後継団体。
  - 長期署名や電子認証等の標準化やビジネス化の活動を予定。
  - ERMCでは基盤となる電子署名/電子認証の技術面を担当。
  - http://www.ecom.jp/Publication/forum4-application.pdf

おわりに

- XMLとPKI（電子署名）の組み合わせは日本では少ない
  - 日本は保守的なのかXML署名の採用率が低いように感じる。
    - 欧州では逆にXML署名のベンダーの方が多いくらいなのだが…
- PKI普及にはXMLにこだわるべきでは無いのかもしれない
  - 署名対象がXMLかどうかはエンドユーザには関係が無い。
  - 必要なのは設計者やプログラマがXML署名を使いやすくする環境。
  - XML署名他の技術に関する情報がもっと必要なのかもしれない。
    - その意味ではツール検証の調査のような情報がもっと必要。
- 実世界のハンコのように電子署名が使われる日を夢見て。

「セキュリティ部会＆Webサービス実証部会の皆様色々ありがとうございました。」