XML Consortium

～ 第6回 XMLコンソーシアムWeek ～

セキュリティ部会活動報告

オフィス文書と電子署名サービス

2007年5月21日

XMLコンソーシアム セキュリティ部会
山根利夫（株式会社日立製作所）

アジェンダ

- オフィス文書の標準化動向
  - OASIS/ISO　ODF
  - ECMA　Open XML
- MS　Office2007による実装
- オフィス文書の電子署名とDSS
  - DSSの概要
  - DSSによる署名処理の検討

(注) OASIS：Organization for the Advancement of Structured Information Standards
ISO：International Organization for Standardization
ECMA：European Computer Manufacturer Association
MS:　Microsoft

オフィス文書標準化の動向 (1)

- 2007年3月，総務省は「情報システムに係る政府調達の基本指針」を公表。
  2007年7月1日から適用。

- オープン化の促進
  競争の促進によるコスト低減や透明性の確保のため、調達仕様書を明確化しオープンな標準に基づく要求要件の記載を優先する。

- 経産省も、調達に当たり、標準技術としての妥当性を評価する「情報システムに係わる相互運用性フレームワーク」案を公表しパブリックレビュー中 (5月中)

オフィス文書標準化の動向 (2)

- *OASIS/ISO　ODF*
  (OASIS Open Document for Office Application)

経緯

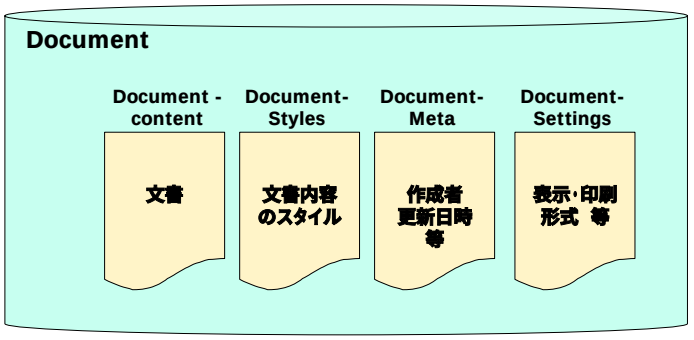
- *2002年11月　OASIS Open Office XML Format TC設置*
- *2005年　5月　OASISの標準仕様として認定*
- *2006年　3月　製品開発促進を目的として、OASIS内に*
  ODF Adoption Committeeを設置。
  (IBM, Sun Microsystems, Novell, Oracle 等)
  また、ODFの採用促進のためODF Allianceを設立
  ODF Adoption Committeeのメンバ他約250社が参加。
- *2006年5月　ISOの国際標準として認定*
- *ベルギー、デンマーク、フランス等で、ODFを政府標準形式に採用*
  米国でもマサチューセッツ州、ミネソタ州で同様の法案成立

出展：IPAニューヨーク便り　06年8月号

オフィス文書標準化の動向 (3)

- ODFフォーマット

  XML文書の集合をZIPファイルで提供。



オフィス文書標準化の動向 (4)

表1　主なアプリケーションでのODFサポート状況

アプリケーション名	ベンダ	ODFサポート状況	使用できるOS
KOffice	K Desktop Environment	採用	Linux,Unix
OpenOffice.org	OpenOffice.org	採用	Windows,Mac,Linux
StarOffice	SUN MICROSYSTEMS	採用	Windows,Linux
Workplace	IBM	進行中	Windows,Linux
NeoOffice	NeoOffice	進行中	Mac
One Special Edition	E-Press	進行中	Windows
Mobile Office	Odendahl SEPT-Solutions	進行中	Symbian
Microsoft Office	Microsoft	進行中	Windows,Mac

出展：IPAニューヨーク便り　06年8月号

オフィス文書標準化の動向 (5)

- *ECMA Open XML Format*

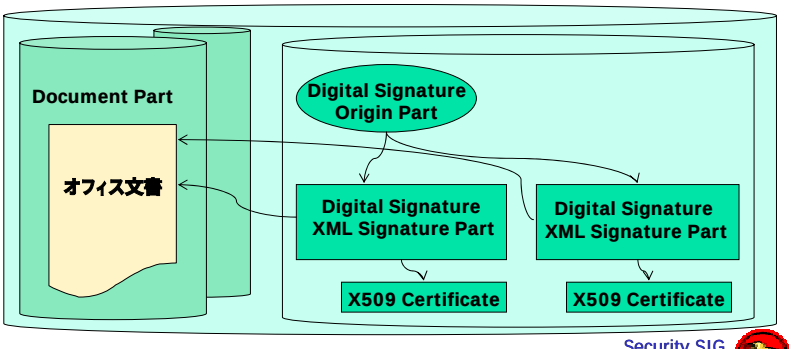
  MS社がODFに対抗して推進するXML標準

経緯

- *2001年 5月 MS OfficeXP でXML出力をサポート*
- *2005年11月 ECMAへ仕様書案を提出*
  (MS, Intel, 東芝 等9社の提案)
- *2006年12月 ECMA標準仕様として認定*
- *2007年 1月 ISOの早期承認プロセス開始を申請*
- *2007年 1月 MS Office2007を出荷*
- *2007年 4月 ISOで、5ヶ月間の検証、承認投票プロセス開始*

オフィス文書標準化の動向 (6)

- OPC(Open Packaging Conventions)
  - 個々のコンポーネントにセグメント化され、各コンポーネントはZIP技術により圧縮され、1つのファイルに格納される。



オフィス文書標準化の動向 (7)

項 目	ODF	Open XML
国際規格認定	2005年5月OASIS規格、2006年5月ISO規格に認定	2006年12月ECMA標準に認定。 12月にはISOにもFirst Track提案し、4月から9月2日迄の検証・投票ﾌﾟﾛｾｽに入った。
支持企業・団体	ODF AllianceにはIBM、Sun、Novell、Oracle、Google等300以上の企業・団体が参加	MS,Apple,東芝等10社が提案
仕様書	オープンソフトOpenOfficeベース、約700ページの仕様書	MS Officeベースの1,900ページに及ぶ仕様書
相互互換性	従来のOfficeとの互換性を持たせている。	MS社はODFもサポートするとしてアドインを開発
オフィス機能	表計算の式等はバージョン1.2	拡張機能等で実装が複雑
電子署名	各社の個別実装	仕様として規定
署名欄・印影	各社の個別実装	MSの独自実装

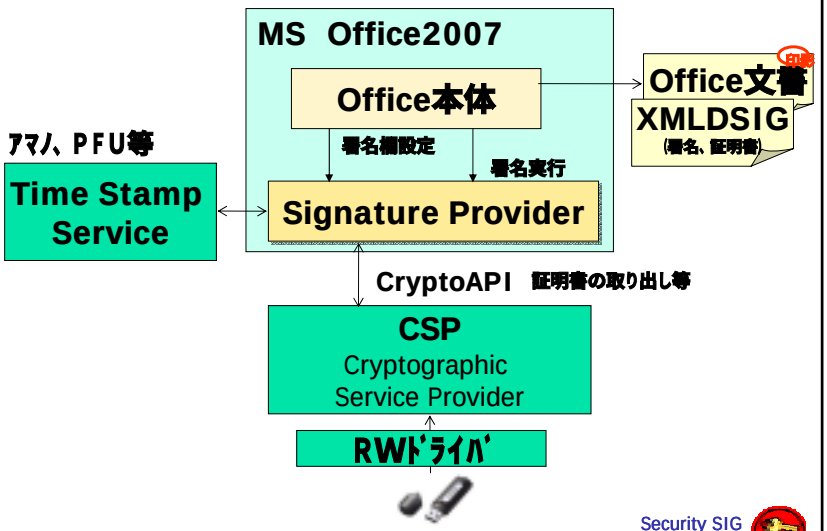
MS Office2007による実装(1)

- 2007年1月 Office2007出荷開始
- 署名欄 (記名方式と印鑑方式) をサポート
  (MSの独自仕様)

.docxファイル

MS Office2007による実装(2)

標準外の署名欄ファイル仕様は、アドイン・インタフェースの公開で対応



Office文書の電子署名とDSS

- 実業務運用上の課題
  - 社外でも有効な第三者発行の証明書を各人に与えるのではコストが膨大となり、また証明書更新の手間も膨大となる。
- 解決方式案
  - 個々人には社内で有効な証明書を発行
  - 社外送付時に、リモートで社内書名の有効性を確認し、社外用署名を付与

⇨ DSSプロトコルの検討

DSS(Digital Signature Service)概要

- OASIS DSS TCのBallotにより、2007年4月にOASIS標準として承認された。
- 電子署名／署名検証サービスのためのインターフェースを規定
  - XMLを用いた要求／応答メッセージ
  - XML-SignatureまたはCMS（RFC3369）による署名形式に対応
  - X.509 PKI TSP(RFC3161)を模した、XML形式のタイムスタンプ
  - PGPなどの他の署名形式、タイムスタンプ形式にも拡張可能
  - 様々な用途に応じたプロファイルの提供

DSSの用途

- 企業での署名サーバとしての利用
  - 社外への正式文書や、配布プログラムに対する署名の付与。
    - 個々の社員ではなく、組織としての署名の付与
    - 個々の社員には、社内用証明書を配布し、組織署名使用の権限を管理。
  - 署名リクエストの中央管理、監査、アーカイブ。
    - 何時、誰の要求で、どのメッセージに署名を行ったかを記録

仕様書構成

- 概要
  - Digital Signature Service Overview
- コア仕様
  - Digital Signature Serivce Core Protocols, Elements, and Bindings
    - メッセージ形式の定義
      - 署名プロトコル (SignRequest / SignResponse)
      - 検証プロトコル (VerifyRequest / VerifyResponse)
      - XMLタイムスタンプ (TimeStamp)
    - メッセージ送受信方法の定義
      - HTTP POST Transport Binding
      - SOAP 1.2 Transport Binding
      - TLS Security Binding
- プロファイル
  - 利用目的に応じて、バインディング方式、拡張仕様、制限事項、処理手続き等を規定

プロファイル概略 (1)

- XML Timestamping Profile
  - RFC3161 Timestampの生成と検証。
  - HTTP POST ＋ TLS X.509 Server AuthN
  - SignRequest
    - OptionalInputs
      - RenewTimestamp　既存のタイムスタンプの有効期限を延長する。
- Asynchronous Processing Abstract Profile
  - 非同期通信による署名／検証サービスの為のメカニズムを提供。
- Abstract Code-Signing Profile
  - ソフトウェアプログラムに対する署名を行うための抽象プロファイル。
- J2ME Code-Signing Profile
  - MIDP 2.0アプリケーションに対する署名の付与。

プロファイル概略 (2)

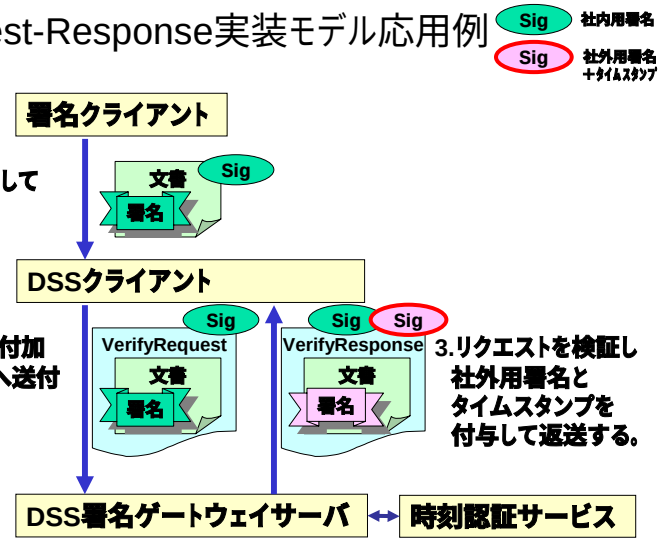
- Entity Seal Profile
  - 指定された電子データが所定の時間に存在していたことを示す「シール」の生成と検証。
- Electronic PostMark (EPM) Profile
  - UPU (万国郵便連合) の支持に基づく、電子消印
- German Signature Law Profile
  - 独デジタル署名法 (SigG／SigV) に準ずる、電子署名の生成と検証。
- Advanced Electronic Signature (AdES) Profiles
  - XAdESおよびETSI TS 101 733(Electronic signature formats and Signature Policies)に定義される、高度な電子署名の生成と検証。

プロファイル概略 (3)

- Signature Gateway Profile
  - 署名検証プロトコルのみを取り扱う。
    - SignatureRequestおよびSignatureResponseは扱わない。
  - ユースケース。
    1. 署名者が署名用の証明書を使って署名を生成する。
    2. 署名を直接受領者に送付する代わりに、署名ゲートウェイへ送付する。
       - 受領者が署名者の署名を 1) 理解できない / 2) 信頼しない かもしれないので。
       - 署名ゲートウェイは署名者と受領者の双方から信頼されている。
    3. 署名ゲートウェイが受領者の検証可能な新しい署名を生成。
       - 現在の署名を検証し、新しい署名を生成する。
  - 2つの実装モデル (Deployment Model) を定義。
    - Request-Response実装モデル
    - In-Line実装モデル

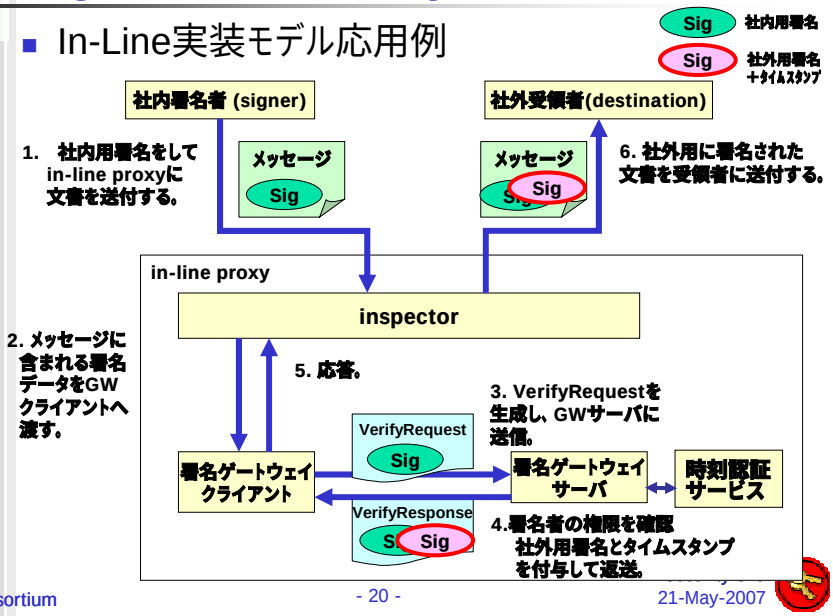
Signature Gateway Profile

- Request-Response実装モデル応用例



Signature Gateway Profile

- In-Line実装モデル応用例



まとめ

- DSSを利用した電子署名の運用
  - オフィス文書の標準化により、電子署名処理を業務システム化することが容易となり、ペーパーレス化、業務効率化を促進することが出来る。
  - DSSにより、電子署名処理をWebサービス化しての集中管理、監査対応が容易となる。
  - 個人の社内用署名と社外用署名を使い分け、費用的負担の大きい社外用証明書の利用を最小限とすることが出来る。
  - 署名欄、印影の扱いは標準化されておらず、社内運用にはアドインによる作り込み等が必要。

END