THE DOCUMENT COMPANY
FUJI XEROX

PKI標準化最新動向

富士ゼロックス株式会社
サービス技術開発部
稲田 龍

THE DOCUMENT COMPANY
FUJI XEROX

はじめに

現状

THE DOCUMENT COMPANY
FUJI XEROX

- 証明書を使ったアプリケーション/プロトコルが増えている
  - SSL/TLSは当たり前
- ユーザ層の意識が変化
  - インターネットは「便利なもの」から「危ないもの」へ
  - さまざまなリスクを勘案して使うものへ

→このような状況において、PKIの提供する機能が注目されている

THE DOCUMENT COMPANY
FUJI XEROX

PKI標準化はどうなっているのか?

標準化の状況（概観）

THE DOCUMENT COMPANY
FUJI XEROX

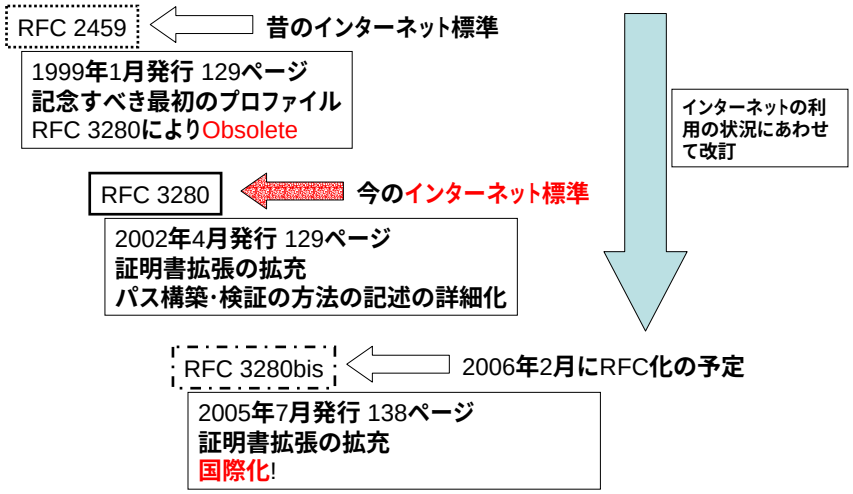
- **証明書自身のプロファイルはほぼ完成**
  - RFC 2459/RFC 3280/RFC 3280bis
- **証明書の検証の視点**
  - CRL(RFC 2459/RFC 3280/RFC 3280bis)
  - OCSP(RFC 2560/Light-weight OCSP)
  - SCVP(SCVP)
- **証明書の応用系**
  - **証明書自身を簡便に使うための視点**
    - CMP(RFC 2510/RFC 4210)
    - CRMF(RFC 2511/RFC 4211)
    - CP&CPS(RFC 2527/RFC 3647)
  - **プロトコルへの応用**
    - SSL/TLS/IPsec/Secure DNS(DNS extensions)
  - **アプリケーションへの応用**
    - **メールへの適用**(S/MIME)
    - SSH (Secure Shell)
    - **長期保存**(LTANS)
  - SPAM**対策への応用**
    - DKIM**など**

THE DOCUMENT COMPANY
FUJI XEROX

証明書プロファイル

証明書/CRLプロファイルの変遷

THE DOCUMENT COMPANY
FUJI XEROX



証明書プロファイル

THE DOCUMENT COMPANY
FUJI XEROX

- 大枠はRFC 3280bisで決まるであろう
  - 暗号アルゴリズム
    - 楕円暗号を用いた公開鍵アルゴリズムの追加
    - 各国の事情に合わせての追加
  - ハッシュアルゴリズム
    - SHA-1の対衝突性の低下により……
      - より長いビット数でのハッシュアルゴリズムの採用
      - 別のアルゴリズムの採用
  - 証明書の記載事項の信頼性の向上
    - 身分証明書としての利用
    - 法的な裏づけ
      - 日本でも2000年に電子署名法(特定認証局)
    - バイオメトリックス情報を入れる動き
      - Qualified Certificate
  - 個人情報対応?
    - 証明書の記載内容を守る?
      - 電子メールアドレスは個人情報
      - 公的個人認証サービスの証明書は4大基本情報全部いり

QC(特定証明書)とは何か?

THE DOCUMENT COMPANY
FUJI XEROX

- 通常の電子証明書に対して、より高位の「保証」をつける事を目論んでいる証明書
  - 欧州における公的個人認証の必要性から、
    - 自然人(個人)を対象
    - 法的に認められるための証明書として通用すること

- セキュリティポリシーとそれを反映した証明書フォーマット(プロファイル)の制定が必要
- 欧州の標準化団体により提唱された標準が、IETF で採用され RFC 3039 として規定されたものが「**クオリファイド証明書** (Qualified Certificate) (**特定証明書**)」
- 現在はRFC 3739 として改訂版が出ている。

QC(特定証明書)とは何か?

THE DOCUMENT COMPANY
FUJI XEROX

- 特定証明書の特徴
  - X.509 v3 証明書プロファイルに準拠
  - 基本領域、拡張領域への記載内容にルールを設定
  - 特定証明書に特化した拡張領域を保持
  - **「人」を対象とした証明書**
    - 必要となるポリシーを規定
- 記載内容に関するルールには、欧州電子署名指令案 (EU-directive) の指示のもと ETSI による標準化検討
  - 実際には欧州における法律制度・社会制度にのっとり内容についてさらに詳細な規定を加えて
- 特定証明書を定義したRFC 3739
  - 利用される国や団体の幅広い要件に対応できるように汎用的な内容

QCの標準化動向

THE DOCUMENT COMPANY
FUJI XEROX

- **欧州における電子署名の要件を満たすために検討が進められた**
  - **「電子署名についての欧州指令** (European Directive on Electronic Signature)」
    - Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- IETF**でインターネットでの適用の必要性を認め、**Standard Track**として標準化が進行中**
- 911**以降、米国内においてバイオメトリック認証の必要性が向上**
  - **米国政府内の標準的な認証用**ICカード**としてバイオメトリックス情報の利用が検討されている**

QCの主な規格

THE DOCUMENT COMPANY
FUJI XEROX

- ETSI TS 101 862 V1.3.2 (2004-06)
  - Title: Qualified Certificate profile
- ETSI TS 101 456 V1.2.1 (2002-04)
  - Title: Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 102 158 V1.1.1 (2003-10)
  - Title: Electronic Signatures and Infrastructures (ESI);Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
  - 2004/3**制定** RFC 3039**の改訂版**

THE DOCUMENT COMPANY
FUJI XEROX

証明書の検証

証明書の検証

THE DOCUMENT COMPANY
FUJI XEROX

- **発行された証明書が有効なものか**?
  - PKI**の特徴との対比**
    - **証明書の失効確認ができれば、認証サーバなどに接続せず、オフラインでの検証ができる**
      - CRL**が有利**?
  - **証明書の検証は大変**
  - **オレオレ証明書**
    - **自己署名証明書をどう扱うか**?
      - Trust Anchor (Trust Point) **をどう扱うか**?
        - » **予め別経路で配る**?
        - » CTL (Certificate Trust List)**を利用する**?

CRLと証明書の関係

THE DOCUMENT COMPANY
FUJI XEROX

- 証明書の失効情報を得るためには……
  - CRL (Certificate Revocation List)を参照するのが一般的
  - OCSPにより、証明書を指定して失効しているか否かを問い合わせる
- 具体的な手段
  - 証明書にはCRL Distribution Point (CRLDP)がある!
    - 証明書が失効されたら、CRLDPに指定されている場所にあるCRLに登録されることを示している
  - CRLには、発行した認証局の電子署名がある!
    - 電子署名の検証により発行した認証局がわかっていれば、署名の検証により正しいCRLであることがわかる。
      - Issuing Distribution Pointに発行した認証局の名前が入っていることもある
      - CRLに証明書同様にAIA (Authority Information Access: 発行認証局情報)を入れるドラフトも出ている(CRL-AIA)
  - これらの情報を組み合わせて、CRLと証明書の関係を解釈

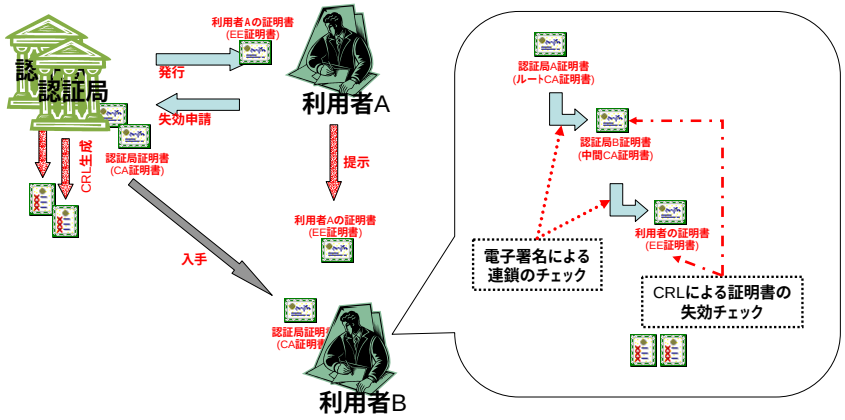
証明書の検証(続き)

THE DOCUMENT COMPANY
FUJI XEROX

- とまぁ、証明書の検証はかなり大変
  - Microsoft社のWindowsは、かなりがんばって検証可能であるが
    - 実際にプログラムを作るとなると大変
    - 種々のPKIモデルを理解するのは大変
    - CPUパワー、ネットワークのバンドワイズなどの資源が必要
- 一般のプログラマには無理?
  - とはいえ、証明書の検証は必要
    - いわゆるミドルウェアによるサポート
      - JAVAのPathBuilder/MicrosoftのCrypto APIなどのSecurity API
    - 難しいところはサーバサイドで解決
      - SCVPなどの新たなサービス

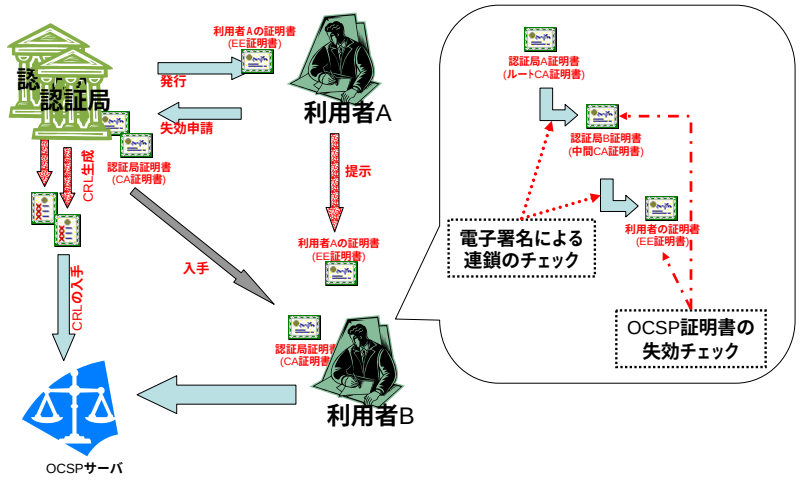
証明書の検証 – CRL利用の場合

THE DOCUMENT COMPANY FUJI XEROX



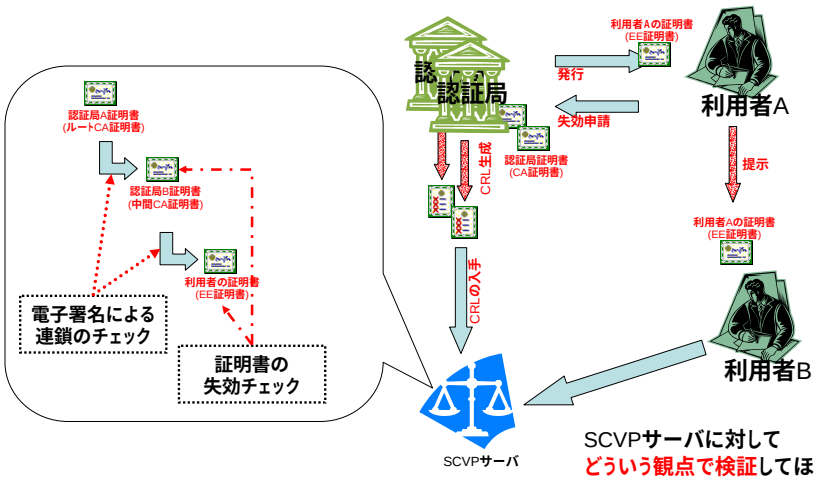
証明書の検証 – OCSP利用の場合

THE DOCUMENT COMPANY FUJI XEROX



証明書の検証 – SCVP利用の場合

THE DOCUMENT COMPANY
FUJI XEROX



SCVPサーバに対して
どういう観点で検証してほしいか
指定

THE DOCUMENT COMPANY
FUJI XEROX

証明書の応用系

証明書の応用系

THE DOCUMENT COMPANY
FUJI XEROX

- SSL/TLS
- S/MIME
- **長期保存**
- IPsec

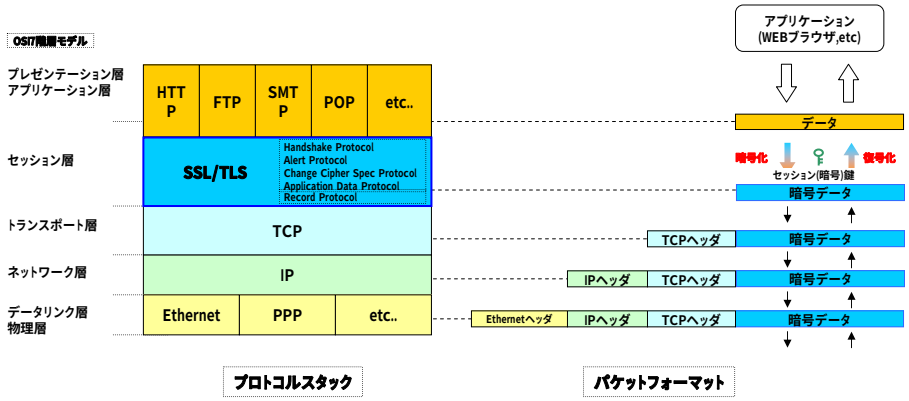
SSL/TLS

THE DOCUMENT COMPANY
FUJI XEROX

- **新たなハッシュアルゴリズムの適用を検討中**
  - 11/5**の第**64**回**IETF**で議題に**
    - 2-3**年後に標準化か**?
- **いくつかの拡張が考慮されている模様**
  - HTTP 1.1**でのホストベースバーチャルホストへの対応**
    - Server Name Indication

SSL/TLS – プロトコルスタック

THE DOCUMENT COMPANY
FUJI XEROX



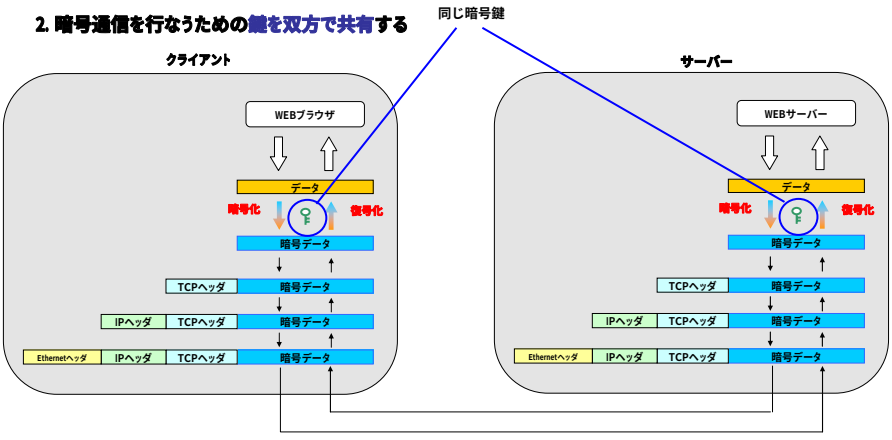
SSL/TLSはアプリーケーションとトランスポートの中間に位置するため、
利用するアプリケーションに依存せずにセキュアな通信が行なうことができる。

SSL/TLS – 鍵共有

THE DOCUMENT COMPANY
FUJI XEROX

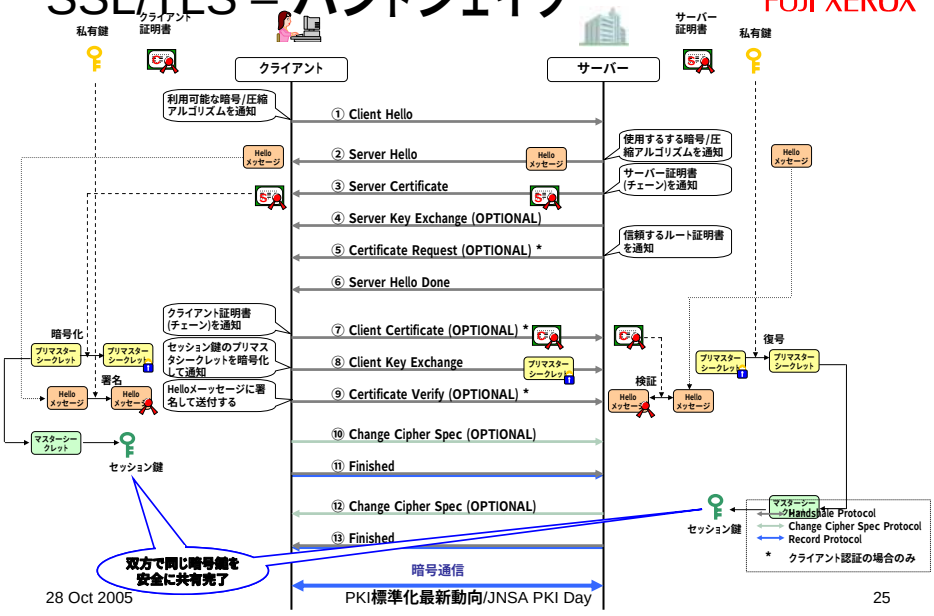
暗号通信を行なうためには…

1. **通信相手が正しい通信相手なのか認証する**
2. **暗号通信を行なうための鍵を双方で共有する**



SSL/TLS – ハンドシェイク

THE DOCUMENT COMPANY
FUJI XEROX



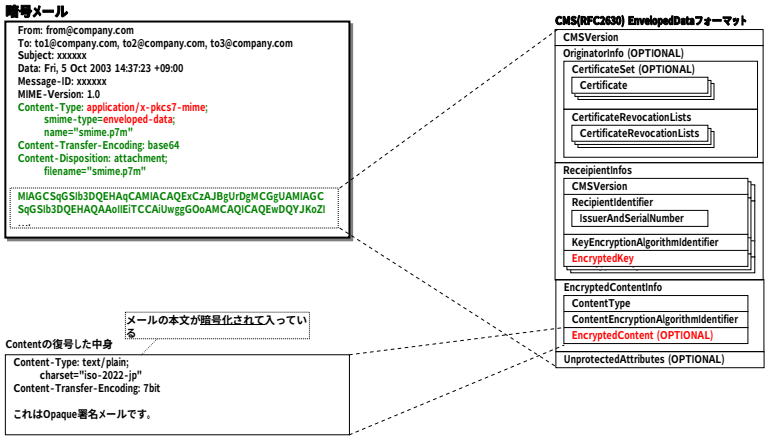
S/MIME

THE DOCUMENT COMPANY
FUJI XEROX

- Ver.3.1
  - RFC 3850/RFC 3851/RFC 3852
- **暗号アルゴリズムの追加**
  - **楕円暗号の追加**
  - AES**の追加**
  - **各国の事情での追加**
    - **韓国、ロシア、日本など**
- **その他**
  - S/MIME Capability**を証明書に入れる**

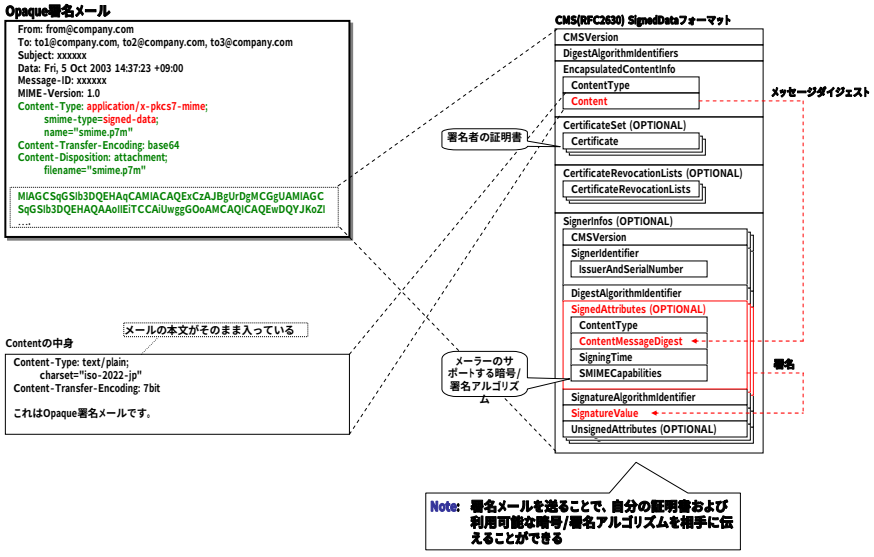
S/MIMEメッセージ内部構造 (暗号)

THE DOCUMENT COMPANY
FUJI XEROX



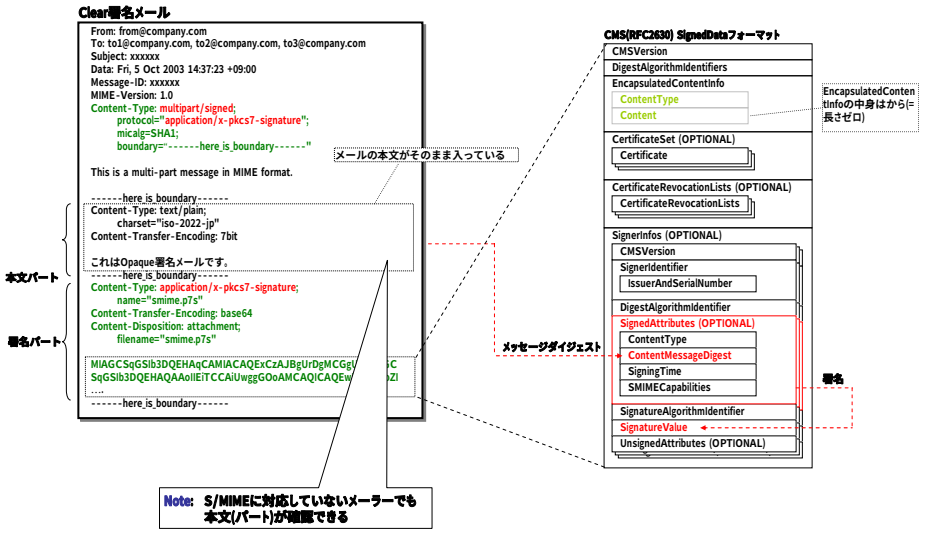
メッセージ内部構造 (Opaque署名)

THE DOCUMENT COMPANY
FUJI XEROX



メッセージ内部構造 (Clear署名)

THE DOCUMENT COMPANY
FUJI XEROX



長期保存

THE DOCUMENT COMPANY
FUJI XEROX

- 電子署名の限界
  - 証明書の有効期限が切れると署名検証ができない!
- いわゆるe文書法で必要とされている技術要件
  - 可読性 (紙と同等の表現力の確保)
    - 一定値以上のスキャン性能
      - 300dpi以上
      - 256階調(1677万色)
    - ファイル形式と圧縮
      - TIFF、PDF、……
      - 品質に影響のないデータ圧縮
    - 検索性の確保
      - OCRによる索引の入力
      - 重要項目による検索機能の確保
        - » 年月日、金額など
  - 真正性
    - 入力操作者の認証と電子署名
      - 権限を有する者によって申請に電子化された旨を証明
      - 特定認証局の証明書であることが前提
    - タイムスタンプの付与
      - 基準や認定について関連団体と協議

この部分の保障のためにPKIを利用

PKIの文書への適用の流れ

THE DOCUMENT COMPANY FUJI XEROX

電子文書
閲覧性/検索性の向上

⇩ 電子署名の付加

改竄の有無の検出(否認防止)

連絡書、社内文書など

⇩ 時刻認証の付加

改竄の有無の検出(否認防止)
作成(受領)時刻の保証

→ 契約文書、特許届け、入札書など時刻の保障が必要な文書への適用

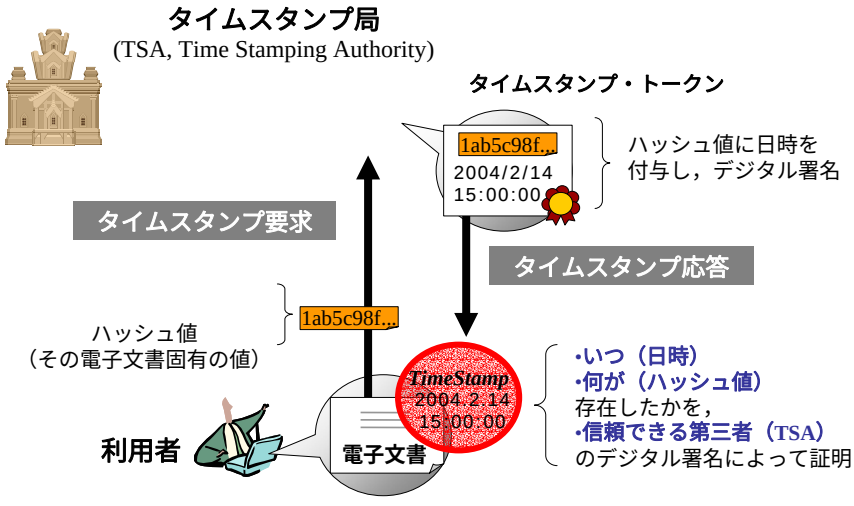
⇩ 長期署名の付加

改竄の有無の検出(否認防止)
作成(受領)時刻の保証
長期間(3-10年程度)の電子署名の検証

→ 長期にわたる文書の保存に対応。訴訟対応、保証対応

RFC 3161 – 最も一般的なタイムスタンプ

THE DOCUMENT COMPANY FUJI XEROX



関連標準マップ－技術･運用標準－

THE DOCUMENT COMPANY FUJI XEROX

ベース技術	タイムスタンプ技術	関係する標準
デジタル署名	**シンプルプロトコル**	**RFC3161** ETSI TS 101 861 ISO/IEC18014-2
	デジタル署名による独立トークン	ISO/IEC18014-2
	MACによる独立トークン	ISO/IEC18014-2
	アーカイブトークン	ISO/IEC18014-2
	XMLタイムスタンプ	OASIS DSSで策定中（旧TIML）
ハッシュ関数	リニア･リンキング	ISO/IEC18014-3
	階層型リンキング	ISO/IEC18014-3
	集約にRSAを用いる方式	ISO/IEC18014-3

※その他のタイムスタンプ関連標準
TSAの運用要件：　ETSI TS 102 023(RFC 3628)
長期署名：　ETSI TS 101 733 (RFC 3126),XAdES,DVCS,TAPなど

RFC 3161 応答･要求プロファイル

THE DOCUMENT COMPANY FUJI XEROX

要求（TSQ, Time-stamp Request）

TimestampReq		
version	構文バージョン番号	
messageimprint	TSAが時刻を結合する対象のハッシュ値（アルゴリズムも含める）	
reqPolicy	タイムスタンプ･トークン発行TSAに要求されるサービスポリシー、OIDで指定	OPTIONAL
nonce	特定の要求を識別するための値（リプレイアタックを防ぐ）	OPTIONAL
certReq	TSAに証明書情報の提供を要求	OPTIONAL
extensions	タイムスタンプ操作に適切な要求を与える拡張	OPTIONAL

応答（TSR, Time-stamp Responce）

TimestampResp		
status	CMPで定めたPKIstatusInfo	
timestampToken	タイムスタンプ･トークン	OPTIONAL
contentType	Contentのタイプ、OIDで指定	
content	Contentの内容	

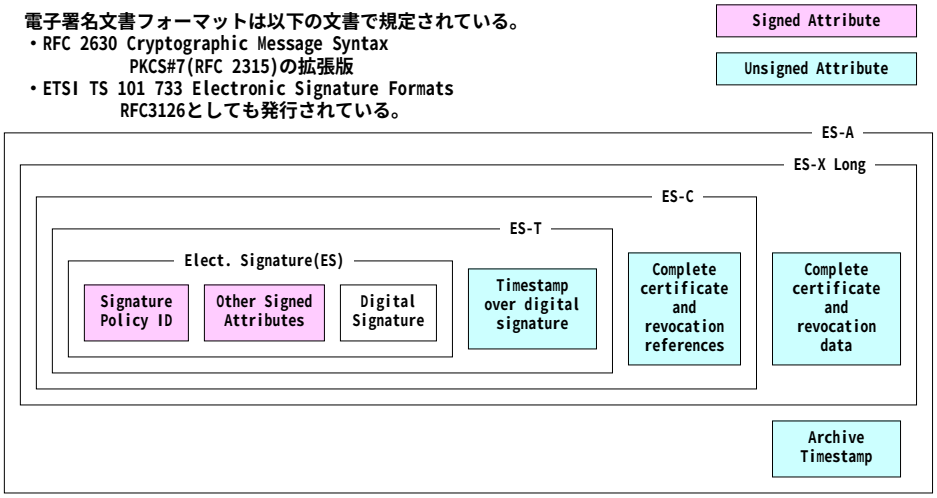
TSTInfo（タイムスタンプ･トークン情報）		
version	構文バージョン番号	
policy	TSAがサポートするポリシー	
messageimprint	TSAが時刻を結合する対象のハッシュ値（TSRの内容をそのまま入れる）	
serialNumber	トークンのシリアル番号	
genTime	トークンを生成した時刻、UTCで記述	
accuracy	精度	OPTIONAL
ordaring	順序（トークン同士の時間的前後関係）	OPTIONAL
nonce	特定の要求を識別するための値	OPTIONAL
tsa	TSAに証明書情報の提供を要求	OPTIONAL
extensions	拡張	OPTIONAL

転送プロトコルは自由：
- HTTP　（最も現実的）
- FILE　（ファイルを元にやりとりする）
- SMTP　（電子メールを利用する）
- Socket　（TCPで通信する）

電子署名文書フォーマット

THE DOCUMENT COMPANY
FUJI XEROX

電子署名文書フォーマットは以下の文書で規定されている。
- RFC 2630 Cryptographic Message Syntax
  PKCS#7(RFC 2315)の拡張版
- ETSI TS 101 733 Electronic Signature Formats
  RFC3126としても発行されている。



ETSI TS 101 861

THE DOCUMENT COMPANY
FUJI XEROX

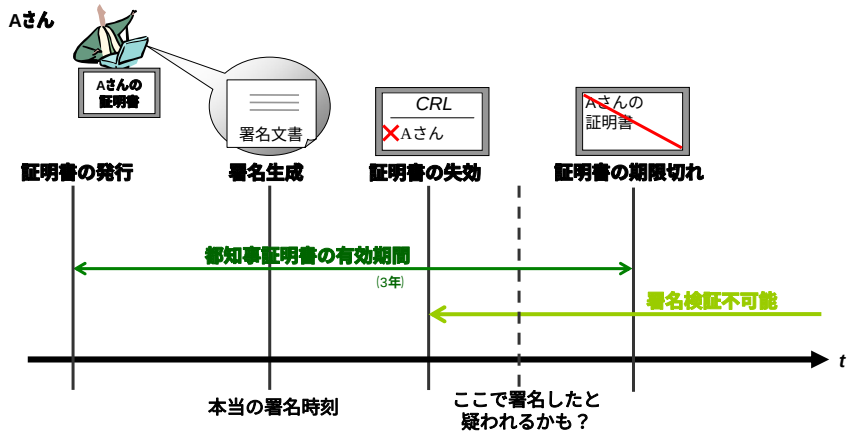
RFC 3161を元に，以下のプロファイルを追加

- **TSPクライアント要件**
  - **拡張領域は含めない** (SHALL NOT)
  - **ハッシュ関数アルゴリズム**
    - SHA-1あるいはRIPEMD-160を推奨
    - MD5は使っても良い (MAY)
  - **以下のTSP応答を処理する**
    - accuracy,nonceのサポート(MUST)
    - ordaringはなし、またはFALSE
    - 署名アルゴリズムのサポート
      - SHA-1withRSA(MUST)
      - RSAの鍵長1024bits (MUST)、2048bits (SHOULD)
      - DSAの素数pまたはqが1024bits以上(SHALL)
  - **転送プロトコルとしてHTTPをサポート**
- **TSPサーバ要件**
  - **時刻関連の要件**
    - nonceのサポート(MUST)
    - accuracyは1秒以下
    - orderingは存在しないか、FALSEをセット
    - genTimeは1秒単位
  - **拡張領域は含めなくてよい、含めた場合全てnon-critical (SHALL)**
  - **ハッシュアルゴリズムのサポート(MUST)**
    - SHA1、MD5およびRIPEMD160
  - **署名アルゴリズムのサポート**
    - SHA-1withRSA(MUST)
    - RSAの鍵長1024bits (MUST)、2048bits (SHOULD)
  - **TSAの名前**
    - X.520のName属性 (C、ST、O、CNで記述)、ただしSTはオプション
  - **転送プロトコルとしてHTTPをサポート**

実装面・運用面での実用性を重視

長期署名とタイムスタンプ
－タイムスタンプが無い場合－

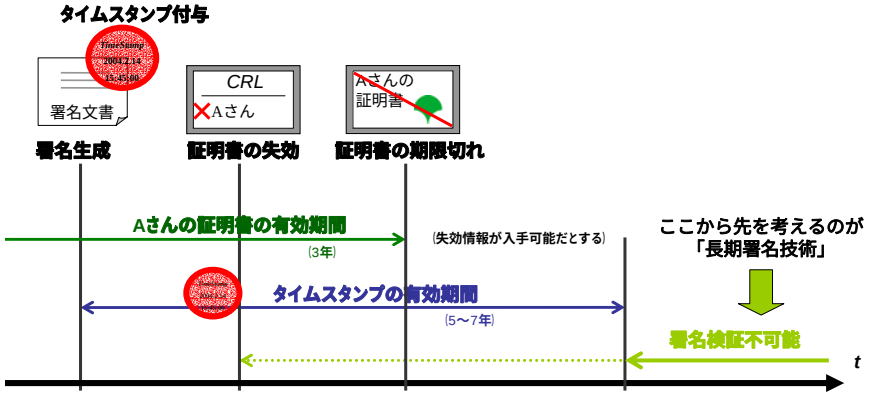
THE DOCUMENT COMPANY
FUJI XEROX



署名時刻を特定できない限り、証明書失効後は署名検証ができない

長期署名とタイムスタンプ
－タイムスタンプが有る場合－

THE DOCUMENT COMPANY
FUJI XEROX



タイムスタンプによって署名の有効性を延長できる

※参考：Microsoftコード署名 (CodeSigning, 別名Authenticodeサービス)における署名の有効期間延長モデル
http://www.verisign.co.jp/codesign/authcodeWP.html

技術動向

THE DOCUMENT COMPANY
FUJI XEROX

- **証明書の期限切れ後**
- **電子署名の正当性を長期にわたって確保**

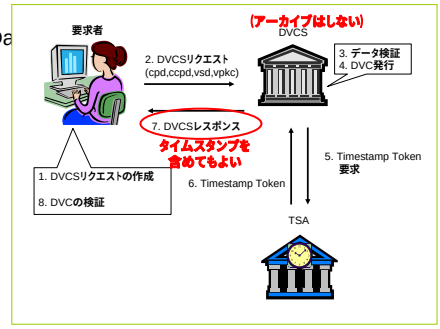
- **電子公証(TTP)を用いる方式**
  - DVCS (Data Validation & Certification Protocol, RFC 3029)
  - TAP (Trusted Archival Protocol, IETFドラフト)

- **電子署名を元に実現する方式**
  - RFC 3126 Electronic Signature Formats for long term electronic signatures
  - ETSI TS 101 733 ESI Electronic Signature Formats
  - ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)

DVCS (Data Validation & Certification Protocol)

THE DOCUMENT COMPANY
FUJI XEROX

- **データ所有の認証**
  - cpd: Certification of Possession of Da
  - **データそのものを送信**
- **データ所有の主張の認証**
  - ccpd: Certification of Claim of Possession of Data
  - **データのハッシュ値を送信**
- **署名文書の検証**
  - vsd: Validation of Digitally Signed Document
- **公開鍵証明書の検証**
  - vpkc: Validation of Public Key Certificates



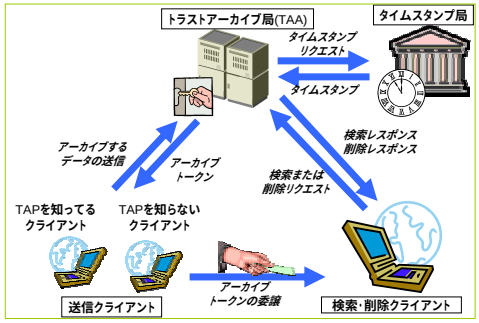
→いづれか1つの機能を有すれば良い

- タイムスタンプだけを目的としたサービスではない
- アーカイブは想定していない

TAP (Trusted Archival Protocol)

THE DOCUMENT COMPANY FUJI XEROX

- **完全性を持つデータを永久に保存**
  - アーカイブのタイムスタンプを適宜更新
  - 関連する暗号データも保存
  - データの編集が可能 (検索・削除)
- **任意のデータを保存可能**
  - データのフォーマットや有効性は無関係
  - 暗号化の有無とは関係ない
  - データの有効・無効とも関係ない
- **サーバー側のオプション処理の追加**
  - データ検証(データ検証の証拠)
  - パス構築・パス検証(有効であった証拠)
- **TAP未対応の送信クライアントもサポート**

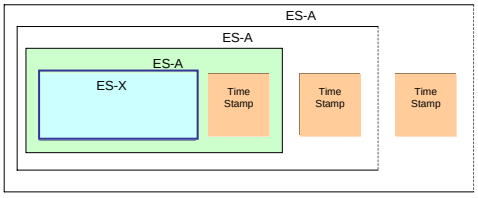


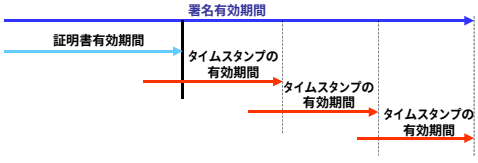
•タイムスタンプを応用した公証サービス（証拠保全・否認防止）
•長期間のアーカイブを想定

RFC 3126

(Electronic Signature Formats for long term electronic signatures)

THE DOCUMENT COMPANY FUJI XEROX





＋認証パス上の全証明書
＋全ての失効情報 (CRL/OCSP応答)
＋アーカイブタイムスタンプ

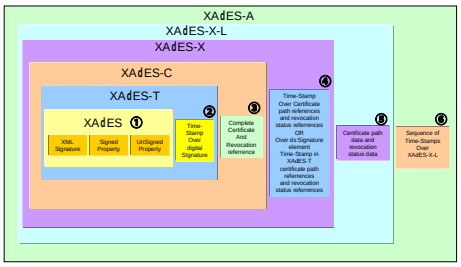
タイムスタンプを繰り返し付与することで、署名の有効性を延長

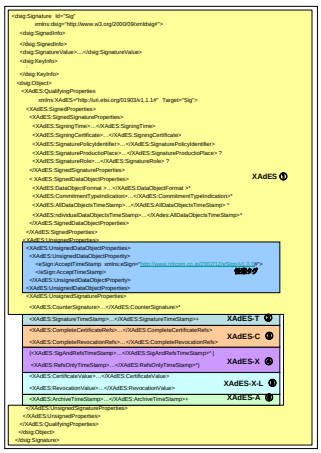
XAdES

(ETSI TS 101 903 XML Advanced Electronic Signatures)

THE DOCUMENT COMPANY
FUJI XEROX

RFC3126のXML版





長期署名とタイムスタンプ

THE DOCUMENT COMPANY
FUJI XEROX

- 技術的課題
  - アーカイブデータの肥大化
  - 検証環境･アルゴリズムの複雑化
  - マルチベンダ間の相互運用性
  - TSA運営上の制約（鍵が危殆化することを前提）
- 周辺課題
  - 永く保存する必要のある重要文書の電子化
    - 法廷保存文書の電子化
    - 長期署名を前提とした法律の整備
  - データの長期保存(long-term archive) の問題※
    - メディアとフォーマットの陳腐化対策
      - マイグレーション（移行手段）
      - アクセス維持（エミュレーション等）

※参考： 国立国会図書館: 電子情報保存に係る調査研究報告書(2003) http://www.ndl.go.jp/jp/aboutus/preservation_02_01.html
CCSDSによるOAIS参照モデル（電子データ保存の技術標準） http://ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf

長期保存

THE DOCUMENT COMPANY
FUJI XEROX

- **欧州のETSIが活発に活動**
- IETFでもLTANS-WGで議論されている
  - Adobeが積極的?

IPsecへの応用

THE DOCUMENT COMPANY
FUJI XEROX

- IKEv1/ISAKMP、IKEv2にて証明書の利用がIETF pki4ipsec WGで検討中
  - 国際化対応
  - 失効検証が話題になっている

Secure DNSへの応用

THE DOCUMENT COMPANY
FUJI XEROX

- DNSサーバ自身の認証
- DHCPなどによるDynamic Updateに対する対応
- SPAMへの対応も検討中

登録商標等について

THE DOCUMENT COMPANY
FUJI XEROX

- Microsoft、MS、Windows、Windows 2000、Windows NT、Windows XP、Windowsロゴ、Internet Explorer、Outlook、Outlook Expressなどは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標である。
- Sun Microsystems、Sunロゴ、Java コーヒーカップロゴ、Solaris、Java、JDKなどは、米国Sun Microsystemsの米国およびその他の国における登録商標または商標である。
- その他、本文小児記載されている会社名、商品名、製品名などは、一般に各社の商標または登録商標である。
- 本書では、™、©、®などを記載しない

THE DOCUMENT COMPANY
FUJI XEROX

ご清聴ありがとうございました