タイムスタンプ技術解説

最新動向と将来展望

IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

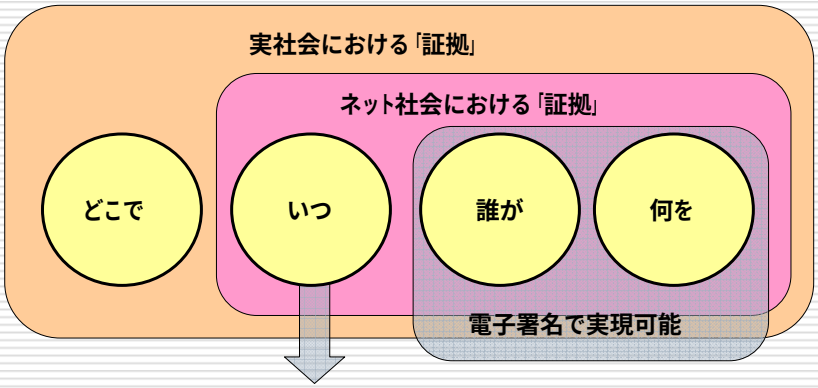
1

解説内容

- タイムスタンプとは？
  - 要素技術（RFC 3161）
  - 否認防止・電子署名・長期署名とタイムスタンプ
- タイムビジネスの分類とケーススタディ
  - 国立印刷局、アマノ、セイコー(SII)、米国郵政局
- 行政におけるユースケースの検討
  - 公開情報、電子申告・申請
- まとめ

2

タイムスタンプとは？



これを実現するのがデジタルタイムスタンプ
電子文書の時刻を証明

3

タイムスタンプとは？（つづき）

- タイムスタンプが証明すること
  - ある時刻にその文書が存在していた　（存在）
  - その文書は改ざんされていない　　（完全性）
- 利用シーン
  - 公開文書　　（約款，技術報告書，IR情報）
  - 知的財産　　（実験データ，設計図，写真）
  - 業務文書　　（契約書，議事録）
  - 記録　　（作業・検査報告，監査記録）
- ビジネス領域
  - 食品，保険，金融，警備，文書保管サービス…

電子ビジネス・社会基盤を支える技術として注目

4

関連するニュース

資料提供：アマノ（株）他

- **奈良県K市**
  - 補助金交付申請書と口座振替申出書の日付に改ざん跡
  - 市民オンブズマンによる住民監査請求（H14.11）
- **食品会社**
  - 雪印食品：国産牛買い取り時期に合わせバックデート（H14.1）
  - 愛知県Y社：ヨーグルトの品質保持期限を偽造（H15.1）
  - 京都府S組合：半年前に採卵した卵約5万個を出荷（H16.1）
- **その他**
  - 投資信託の米セキュリティー・トラスト社が取引時刻を不正操作し，ヘッジファンド等の特定顧客に利益をあげさせた(H15.11)
  - タイの入国審査官が査証の日付を間違い，邦人が不法滞在として罰せられた(H16.2)

リアルワールドでは多くの事件・事故がある

5

歴史

- 1990年代初め
  - 米Surety社
    - 商用タイムスタンプ・サービスの登場
    - 階層型のリンキング・プロトコル
- 1990年代中ごろ
  - 米国・英国での商用タイムスタンプ・サービス
- 2000年代
  - 標準化が行われる
    - IETF, ISO/IECでのタイムスタンプ標準整備
    - 欧州を中心にタイムスタンプの法的な要件が検討
  - 世界各所でタイムスタンプ・サービスが開始
  - 日本国内でも関連製品やサービス展開が始まる
  - テストサイトの活性化

新しい標準化技術 ・ 法整備は欧州中心

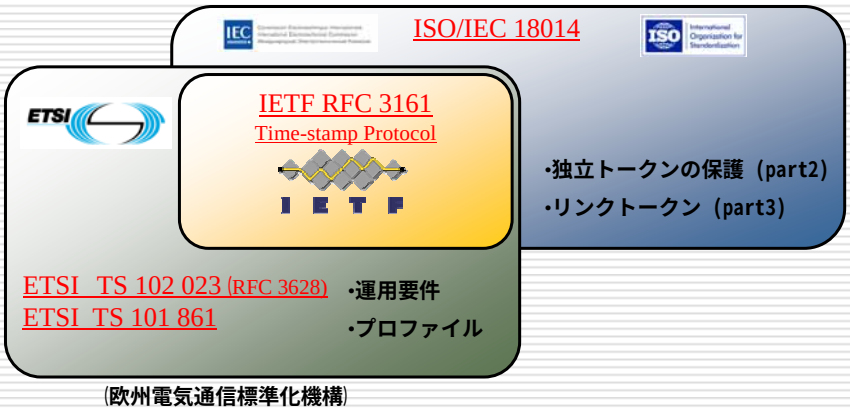
6

要素技術マップ

ベースとなる技術	タイムスタンプ技術	関係する標準
デジタル署名	デジタル署名	RFC 3161 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，RFC3161ベース）
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
分散TSA	デジタル署名方式 リンキング方式	複数のTSAによってハッシュ値を関連させる

7

標準化動向

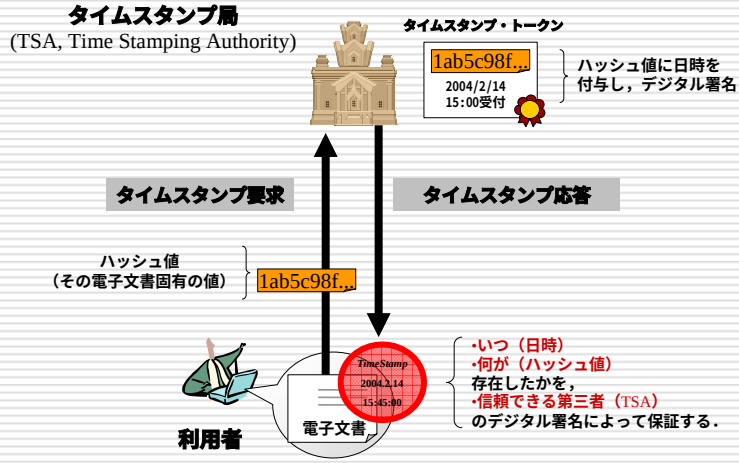


（欧州電気通信標準化機構）

8

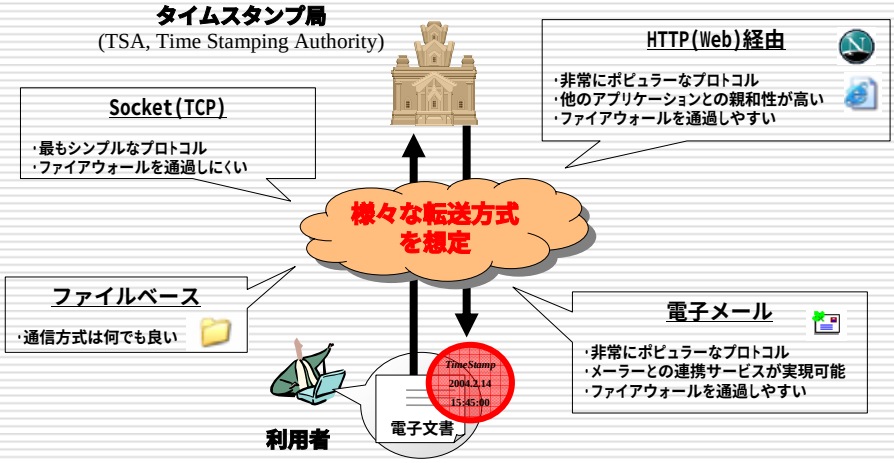
RFC 3161: Time-Stamp Protocol

最も基本的なタイムスタンプ技術



RFC 3161: Time-Stamp Protocol

TSAと利用者間の転送方式



RFC 3161: Time-Stamp Protocol

応答･要求プロファイル

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

非常にシンプルなプロファイル
（実装しやすい）

11

参考：ETSI TS 101 861

（欧州電気通信標準化機構）

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

12

RFC 3161: Time-Stamp Protocol

ーまとめー

- **関連技術**
  - 公開鍵証明書（X.509）
  - デジタル署名（CMS Signed Data）
- **様々な転送方式を想定**
  - 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）
- **多くの対応機器・多くのサービス事例**
  - Entrust, nCipher, Symmetricom…
  - 米国郵政公社(USPS)，日本電子公証（株），SII，アマノ…

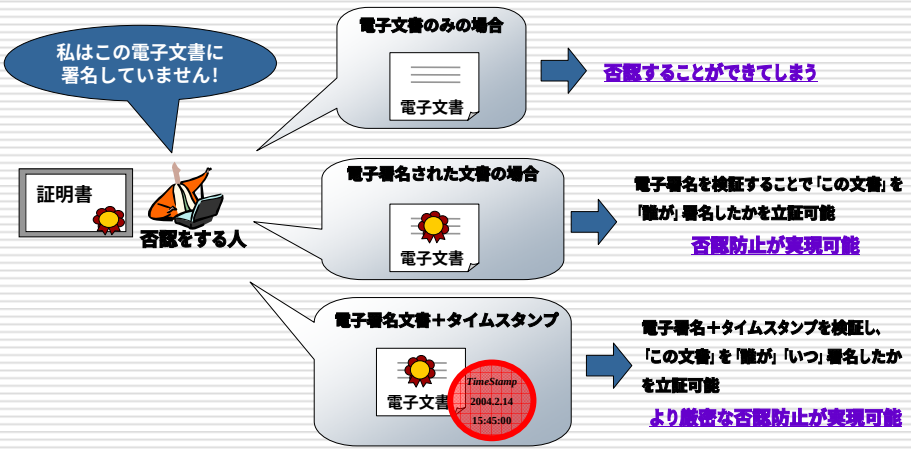
汎用的な標準で，多くの利用事例がある

13

否認防止とタイムスタンプ

（事実を否定すること）

※関連：ISO/IEC 13888 Part1,2 and 3

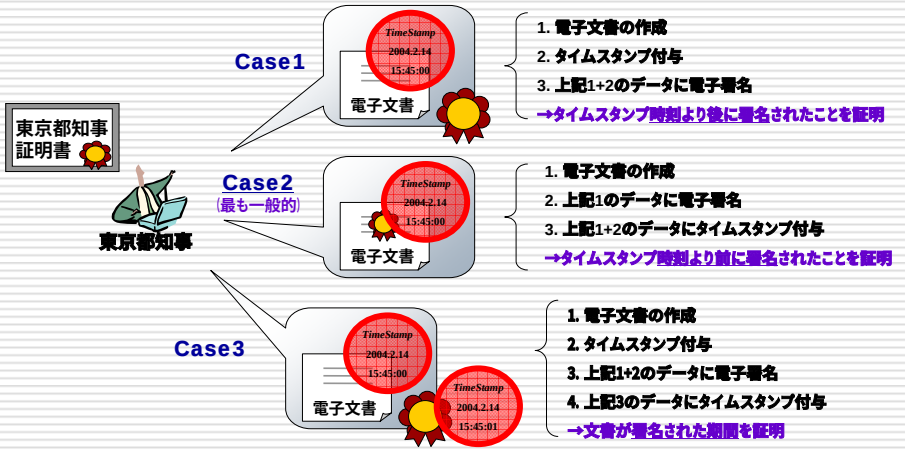


14

※ISO/IEC 18014 Part1より

電子署名とタイムスタンプ

－署名時刻を特定するための3つの利用法－



署名文書（誰が・何を）の時刻（いつ）を、いずれかの方法で特定

15

タイムスタンプとは？

－まとめ－

- **タイムスタンプは**
  - 「完全性」の確保と「存在証明」を行う
  - 電子文書の時刻を確定
    - 電子署名付き/無し
    - 自然人/機械がつくったもの
    - 文書/画像/音声/ログ
  - 否認防止を強力にサポート可能

  →ビジネス・生活のあらゆる分野と関係がある
    - 電子商取引，知的財産保護，業務文書管理
    - 電子申告，電子申請

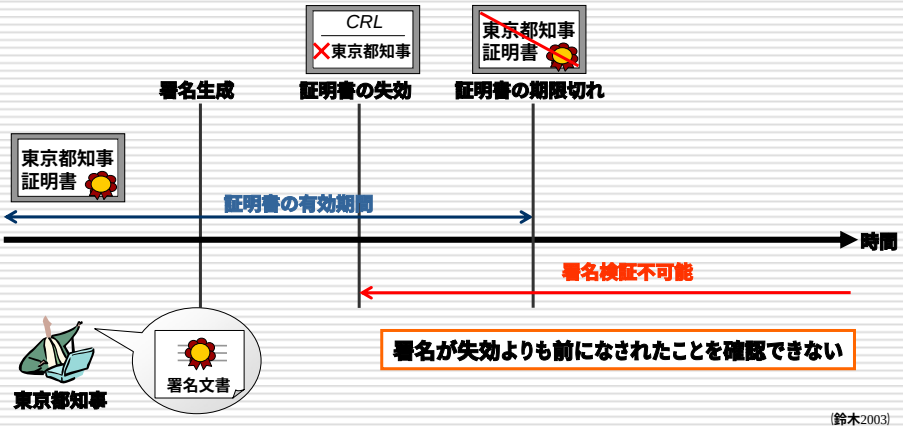
- **プロトコルとデータフォーマット**
  - 仕様は十分に整備されている
    - IETF RFC，ISO/IEC，ETSI
  - 歴史は浅いが多くの利用事例がある

  →技術的には成熟している

社会基盤としての必要条件は満たしている

16

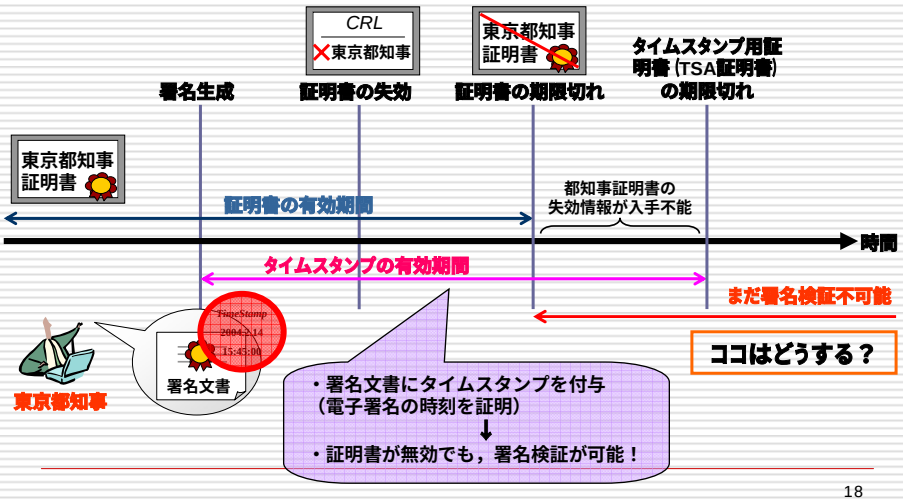
長期署名とタイムスタンプ
－タイムスタンプが無い場合－



(鈴木2003)

17

長期署名とタイムスタンプ
－タイムスタンプが有る場合－



18

電子署名の長期保存

- 証明書の期限切れ後
- 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)

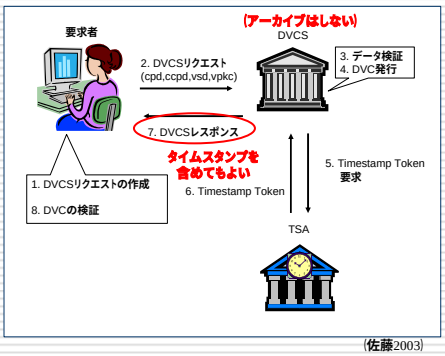
19

DVCS

(Data Validation & Certification Protocol)

- **データ所有の認証**
  - cpd: Certification of Possesion of Data
  - 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

→いずれか１つの機能を有すれば良い



(佐藤2003)

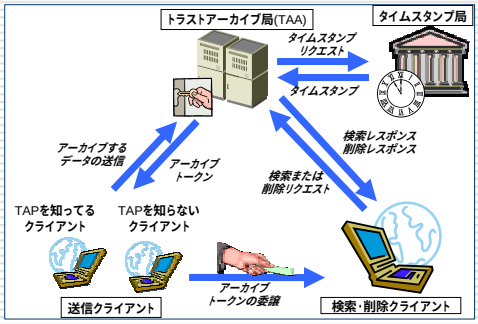
・タイムスタンプだけを目的としたサービスではない
・アーカイブは想定していない

20

TAP

(Trusted Archival Protocol)

- **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**

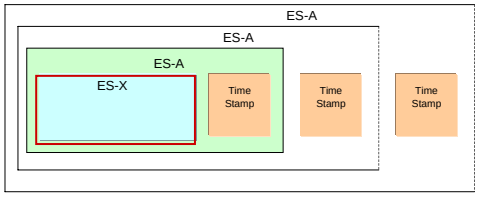


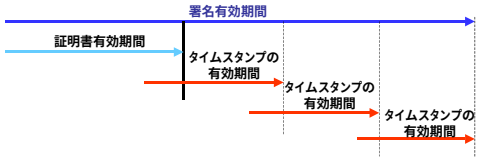
(磐城2003)

・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 ※ETSI TS 101 733 とほぼ同様

(Electronic Signature Formats for long term electronic signatures)





＋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

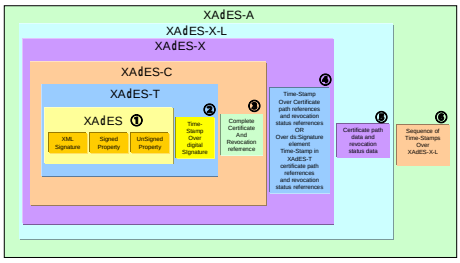
繰り返し付与することで有効性を延長する

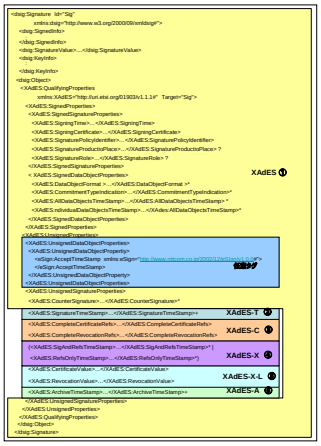
(鈴木2003)

XAdES

(ETSI TS 101 903 XML Advanced Electronic Signatures)

RFC3126のXML版





(鈴木2003)

長期署名とタイムスタンプ
ーまとめー

- **長期署名に対応した製品**
  - 三菱電機 MistyGuard署名延長システム (RFC 3126)
  - 日本ボルチモアテクノロジーズ SignusDVCS (DVCS)
- **アーカイブ・タイムスタンプの課題**
  - データの肥大化
  - 検証環境の複雑化
  - TSA運営上の制約 (鍵が危殆化することを前提)
- **長期署名発展のシナリオ**
  - 長期署名が必要となる重要ドキュメントの電子化 (昨今1～2年)
  - サービス運営母体の設立
  - アーカイブタイムスタンプの技術的な議論

タイムビジネス
ー分類とケーススタディー

※参考：タイムビジネス研究会報告書（H14.6）

- **標準時配信サービス**
  - 正確な時間を提供
- **時刻認証・流通型サービス**
  - いわゆる「TSAサービス」
  - 電子文書にタイムスタンプを付与
  - アーカイブは行わない
- **時刻認証・保存型サービス**
  - いわゆる「電子公証」サービス
  - タイムスタンプや元本を長期間保存
- **検証サービス**
  - タイムスタンプの有効性を検証

まだ未発達

- **関連ビジネス**
  - タイムスタンプ関連製品のビジネス
  - 専用クライアントやプラグインの販売・配布

米国郵政公社(USPS)

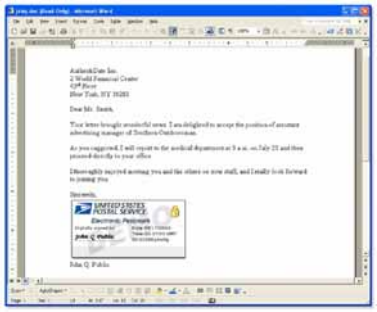
電子消印サービス(EPM)

http://www.usps.com/electronicpostmark/welcome.htm

（時刻認証・流通型サービス）

- **利用者拡大の戦略**
  - MicrosoftOfficeの専用プラグインを無料配布
  - 誰でも利用できる
  - 1スタンプ$0.1～$0.8※
- **官民連携ビジネス**
  - 米国郵政公社（USPS）
  - 米Authentidate社（サービス・技術の提
  - マイクロソフト

アジアへの進出も計画（鼻息が荒い）



※
25EPMを購入する場合：1EPM当たり0.8米ドル
1,000,000EPMを購入する場合：1EPM当たり0.1米ドル

独立行政法人・国立印刷局

官報情報サービス

http://kanpou.npb.go.jp/search/introduce.html

(時刻認証・流通型サービス)

- **特徴**
  - 国の威信に関わる重要文書
  - 大量のトランザクション(300件/日)
    (特開2003-244139)
  - Acrobatの検証プラグインを無料配布
  - B2Cで1:*n*の流通を想定
    - 高性能なタイムスタンプ発行環境
    - 負担の少ない検証環境

システム構築:アマノ(株)

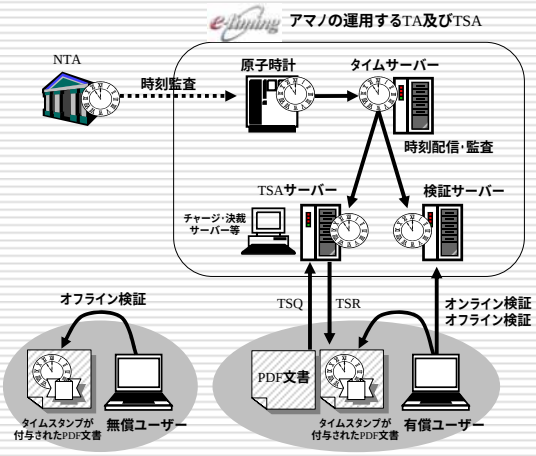
27

アマノ株式会社

TSAサービスモデル

http://www.e-timing.ne.jp/

(時刻認証・流通型サービス)



28

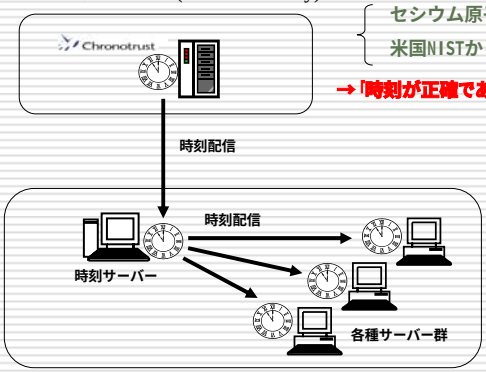
セイコーインスツルメンツ株式会社

Chronotrust 時刻配信サービス

http://www.sii.co.jp/ni/tss/

(標準時配信サービス)

SIIの運用するTA (Time Authority)



- セシウム原子時計
- 米国NISTからの時刻配信

→「時刻が正確であることを証明」するプロバイダ

TOKYO STAR BANK 東京スター銀行

ユーザー企業

ログイット株式会社

音声公証サービス

http://www.logit.co.jp/products/onseikosyo/

(時刻認証・保存型サービス)

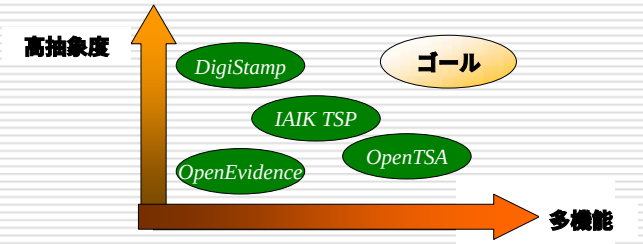
- **通話録音データにタイムスタンプを付与**
  - **電話取引**
    - 金融など
  - **コールセンター**
  - **オペレーションセンター**
    - レスキュー
    - 警備会社

- ログイット株式会社
- 日本電子公証株式会社
- セイコーインスツルメンツ株式会社

タイムビジネス

－開発ツールキット－

	言語	ソース提供	ライブラリドキュメント
OpenTSA	C	○	×
IAIK TSP	Java	×	○
Open Evidence	C	○	△(作成中)
DigiStamp	C, C++, Java	×	○

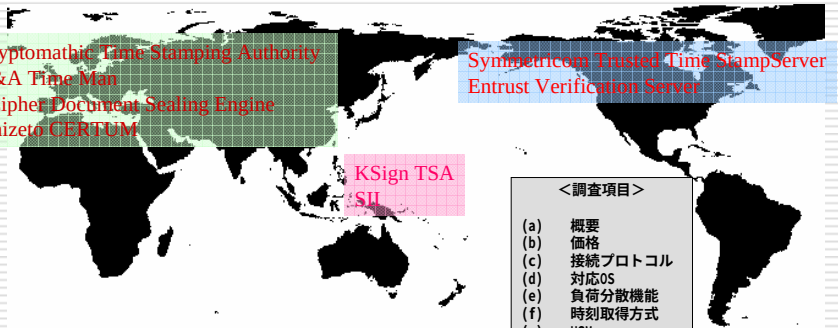


(伊藤2003)

31

タイムビジネス

－関連製品－



Cryptomathic Time Stamping Authority
C&A Time Man
nCipher Document Sealing Engine
Unizeto CERTUM

Symmetricom Trusted Time StampServer
Entrust Verification Server

KSign TSA
SII

＜調査項目＞

(a) 概要
(b) 価格
(c) 接続プロトコル
(d) 対応OS
(e) 負荷分散機能
(f) 時刻取得方式
(g) HSM
(h) データベース
(i) その他

32

タイムビジネス
ーまとめー

- **ビジネスフィールドは着実に広がりつつある**
  - 時刻配信サービス
    - 官民連携プロジェクト（CRL）
  - 時刻認証サービス
    - 流通型（SII，アマノなど）
    - 保存型（NTTData SecureSeal）

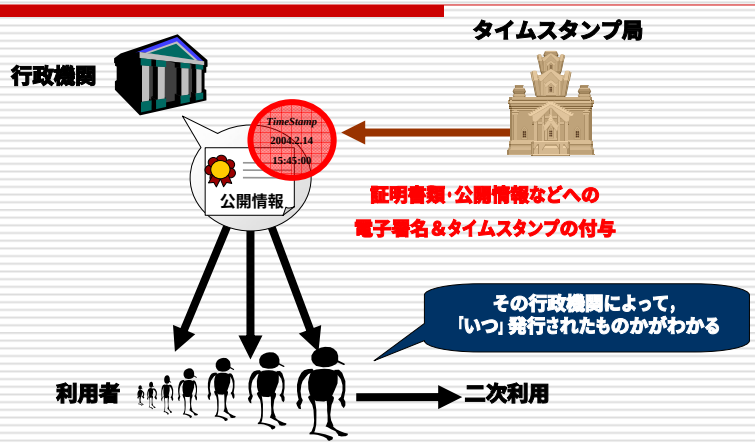
  →企業内・B2Bでは法的な裏付けが不要（カジュアルに利用可能）

- **国・地方自治体における利用シーンは未知数**
  - G/LGが発信する文書へのタイムスタンプ付与 (1:*n*)
  - 電子申請･申告などのレシート (1:1)
    - 作成基準と到達基準
    - 誰が時刻認証を行うのか？
  - 電子文書の組織内での長期保存

  →厳密な法的根拠・官側での運用主体が必要となる

33

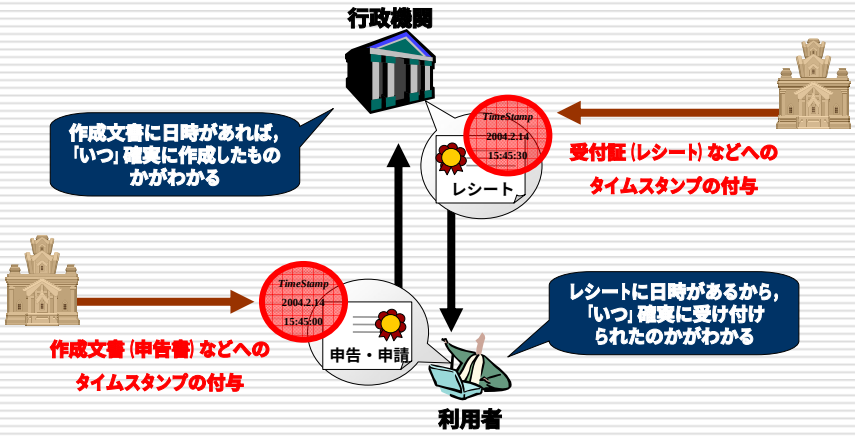
行政におけるユースケースの検討
ー各種証明書類･公開情報などー



不特定多数への発信情報の存在証明が可能

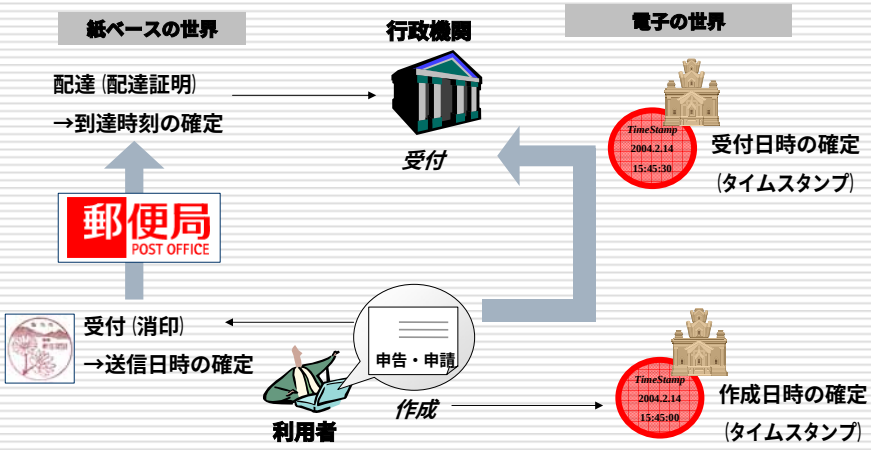
34

行政におけるユースケースの検討
－電子申請等－



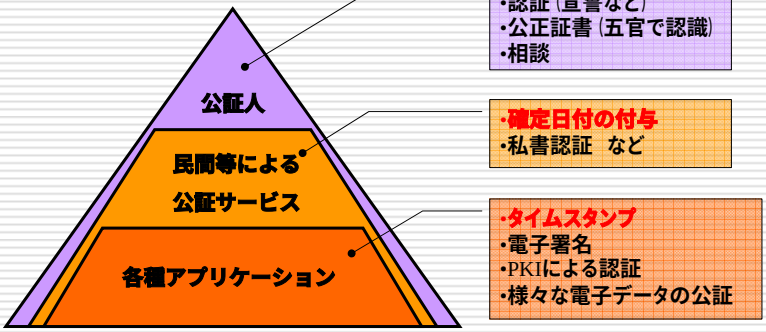
35

行政におけるユースケースの検討
－紙と電子の比較－



36

行政におけるユースケースの検討
－電子公証－



検討課題
- ・運用ポリシ
- ・利用約款
- ・認定監査基準
- ・証拠能力に関するガイドライン

※参考：ECOM電子公証システムガイドライン(H10)

37

まとめ

- **e-Japan 重点計画2003（2005年までの目標）**
  - タイムスタンプ・プラットフォーム技術
  - デジタル・アナログ・ハイブリッド保存技術等
  - 電子文書の長期保存

  →文書の電子化促進のためにはタイムスタンプが必要

- **電子社会における時刻の信頼性確保**
  - 要求
    - 大量の電子文書に消印・確定日付を付与
    - ROIを考慮した効率的なシステム投資
  - 解不在の現状
    - 電子公証制度（ほとんど使われていない）
    - 紙の仕組みをそのまま置きかえることはできない

38

参考
公証制度と知的財産

- **販売事実の立証**
  - 出願したけど成立しなかった場合でも，出願内容は公知となる
  - 他社が模倣した製品を出すのを防ぐ
  - 販売状況や商品の陳列履歴などに確定日付を得ておく
  - 「不正競争防止法：商品形態の模造」と関連
- **先使用権の確保**
  - 「特許出願の準備をしていた」ということを立証
  - 他人より前に出願準備をしてれば，一定の条件下で実施を確保可能
- **ノウハウの保護**
  - 共同開発などの場面を想定
  - ノウハウの内容やNDAの契約書
  - 不正競争防止法：営業機密と関連

参考：知的財産分野における公証制度の利用について，パテント2003

参考
公証制度と知的財産（つづき）

- **公知・公用事実立証**
  - パンフレット・技報などの「公知の事実」を，より確かなものとする
  - 公知の事実であれば，第三者は特許権を取得できない
- **証拠保全**
  - 物の生産方法に関する特許侵害の裁判を想定
  - 予め生産方法などを公証
  - 被告側が特許を侵害していないことを立証する義務をもつ場合がある
- **新規性喪失の例外規定適用**
  - Webサイトの掲載日時やURL，内容などを予め公証 ※英国Wolf社のサービスモデル
  - 平成11年の法改正によって「新規制遺失の例外」と見なされる
- **商標の使用・周知及び著名性の立証**
  - 既に商標を使用している情報に対し確定日付を取得
  - 「商標法：使用・周知事実の立証」と関連