長期署名フォーマットと ECOMにおける相互運用実証実験について

2006年6月7日

ＥＣＯＭ長期署名保存フォーマット普及SWGリーダ
宮崎　一哉
三菱電機株式会社　情報技術総合研究所

本日の報告事項

- ECOMでの活動概要
- 長期署名フォーマットとは
- 長期署名フォーマットプロファイルの策定
- 長期署名フォーマットの相互運用テスト実施
- 今後の予定

ECOMでの活動概要

- 2000年度　認証・公証WG
  - 「電子署名文書長期保存に関する中間報告」
- 2001年度　認証・公証WG
  - 「電子署名文書長期保存に関するガイドライン」
- 2002年度　認証・公証WG
  - 「タイムスタンプサービス調査報告書」
  - 「タイムスタンプサービスの利用ガイドライン」
  - 「タイムスタンプサービスの運用ガイドライン」
- 2003年度　認証・公証WG
  - 「署名ポリシー調査報告書」
  - 「電子署名文書長期保存に関する実用化動向調査報告書」
  - 「電子文書の長期保存と見読性に関する調査報告書」
- 2004年度　認証・公証WG
  - 「電子文書の長期保存と見読性に関するガイドライン」
- 2005年度　セキュリティWG
  - 「長期署名フォーマット相互運用性実験報告書」
- 2006年度　長期保存フォーマット普及WG
  - ハンドブック作成、標準化など

電子署名法公布 2000/5/31

電子署名法施行 2001/4/1

e-文書法公布 2004/12/1

ﾀｲﾑﾋﾞｼﾞﾈｽ信頼・安心認定制度創設 2005/2/1

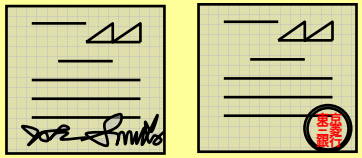
e-文書法施行 2005/4/1

電子署名法

「電子署名及び認証業務に関する法律」

●**電磁的記録の真正な成立の推定**と**特定認証業務の認定**及び国の役割、罰則

民事訴訟法第228条第4項



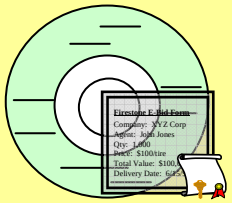
署名　　押印

「本人または代理人の署名又は押印がある時」

→ 「私文書は、真正に成立したものと推定」　　署名・押印自体に有効期限はない

＝　　≠

電子署名及び認証業務に関する法律第3条



電子署名

「本人による電子署名が行われている時」

→ 「電磁的記録に記録された情報は、真正に成立したものと推定」　　電子署名（デジタル署名）には有効期限がある

長期署名フォーマットとは

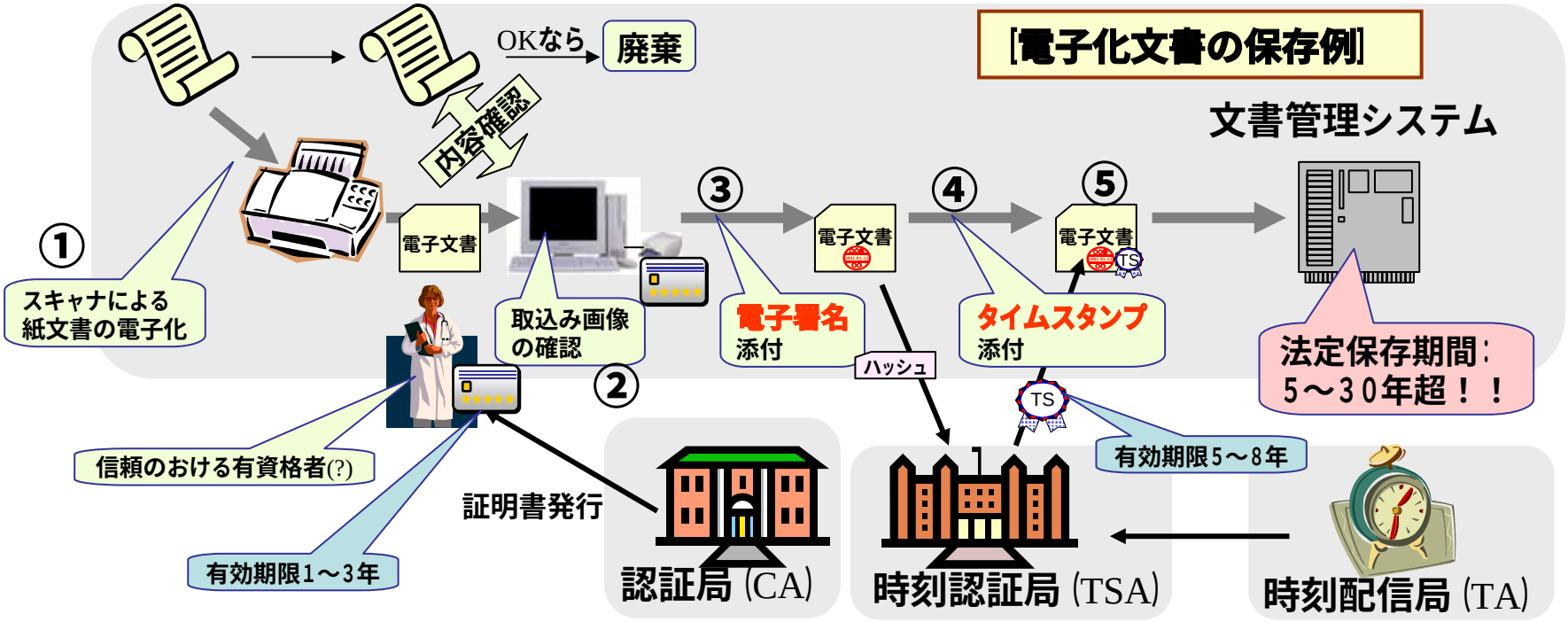
長期署名フォーマットの必要性

- 紙文書から電子文書へ ⇦ 効率化、省資源
- 紙文書と同様の信頼性 ⇨ 原本性、完全性、
  真正性、真実性
- 電子文書の信頼性確保の手段
  ⇨ 電子署名法で言うところの『電子署名』
  認定を受けた『タイムスタンプ』
  ↳ デジタル署名

e-文書法の成立

- 民間に対する紙による文書保存義務 ⇒ **原則全て電子保存を容認**
- **電子化文書**：紙文書をスキャンしたイメージデータ
  電子文書　：当初から電子文書であるデータ
  } ⇒ 両者の保存を含む
- 「通則法」と「整備法」
  - 通則法：電子保存容認に関する共通事項
  - 整備法：通則法のみでは手当てが完全でない場合の規定整備
- 具体的な保存方法については主務省令で定める
- 平成１７年４月１日施行

国税･地方税関連、厚生労働省関連では**真実性の確保**を要件に



文書保存期間

	行政機関の例	法人等の例
1年	請願書，届出書	
2年		健康保険関連書類
3年	予算要求説明資料	労働者名簿，調剤録
4年		雇用保険関連書類
5年	請求書，領収書	健康診断個人票，診療録
7年		売掛帳，買掛帳
10年	審議会答申，裁定書	商業帳簿
30年	決裁文書，判決書	特別管理物質関連の記録
永久		定款，株主総会議事録

⚠ 電子文書を長期にわたって保存することができるのか

長期署名フォーマットの必要性

- 紙文書から電子文書へ ⇦ 効率化、省資源
- 紙文書と同様の信頼性 ⇨ 原本性、完全性、真正性、真実性
- 電子文書の信頼性確保の手段
  ⇨ 電子署名法で言うところの『電子署名』
  認定を受けた『タイムスタンプ』
  ↳デジタル署名

デジタル署名の弱点⇨有効性が長時間持続しない

電子文書の信頼性を長時間維持できない！！

長期署名フォーマット（署名延長）

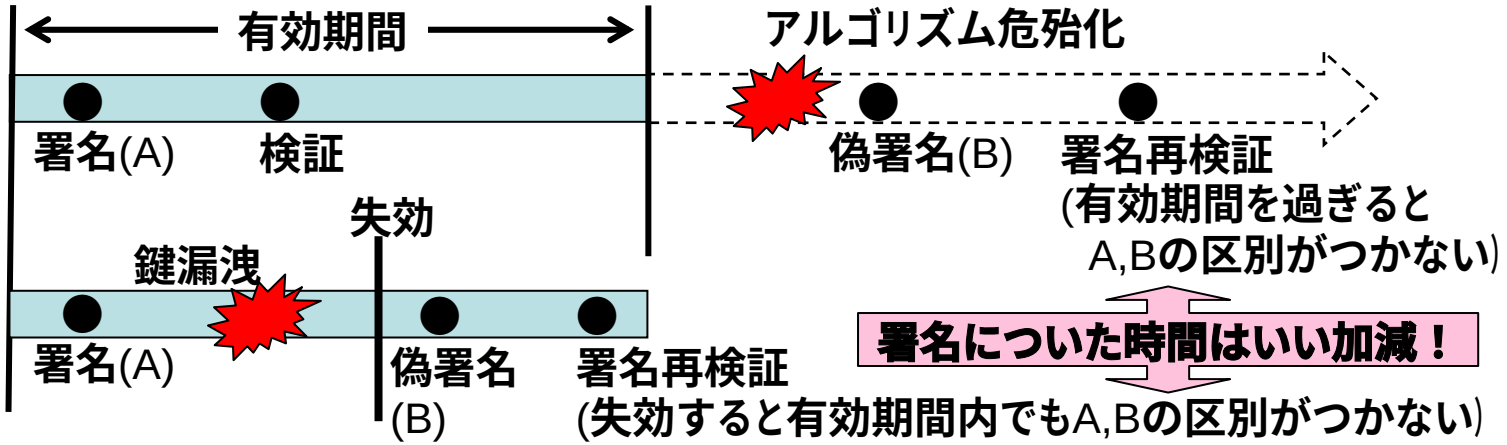
デジタル署名の限界

- 署名鍵は、盗難にあったり偽造されると真偽の区別が付かない。
  - 盗難/失格対策 → 失効の仕組みを導入
  - 偽造対策 → 有効期限を設定

} PKIで実現

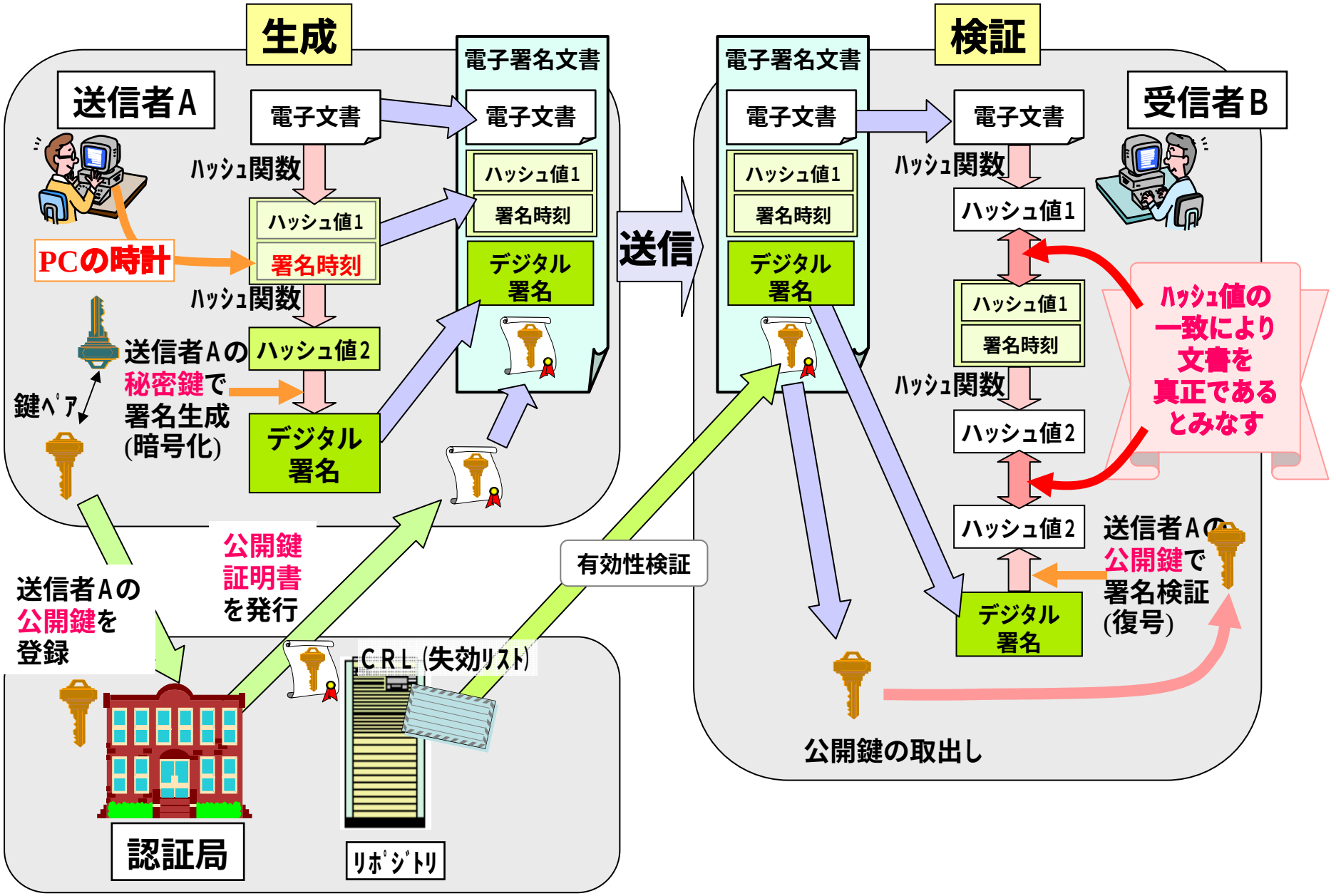
しかしながら。。

署名の真偽が確認できるのは、有効期間内かつ失効がないときのみ
(それ以外は真偽の区別がつかない)

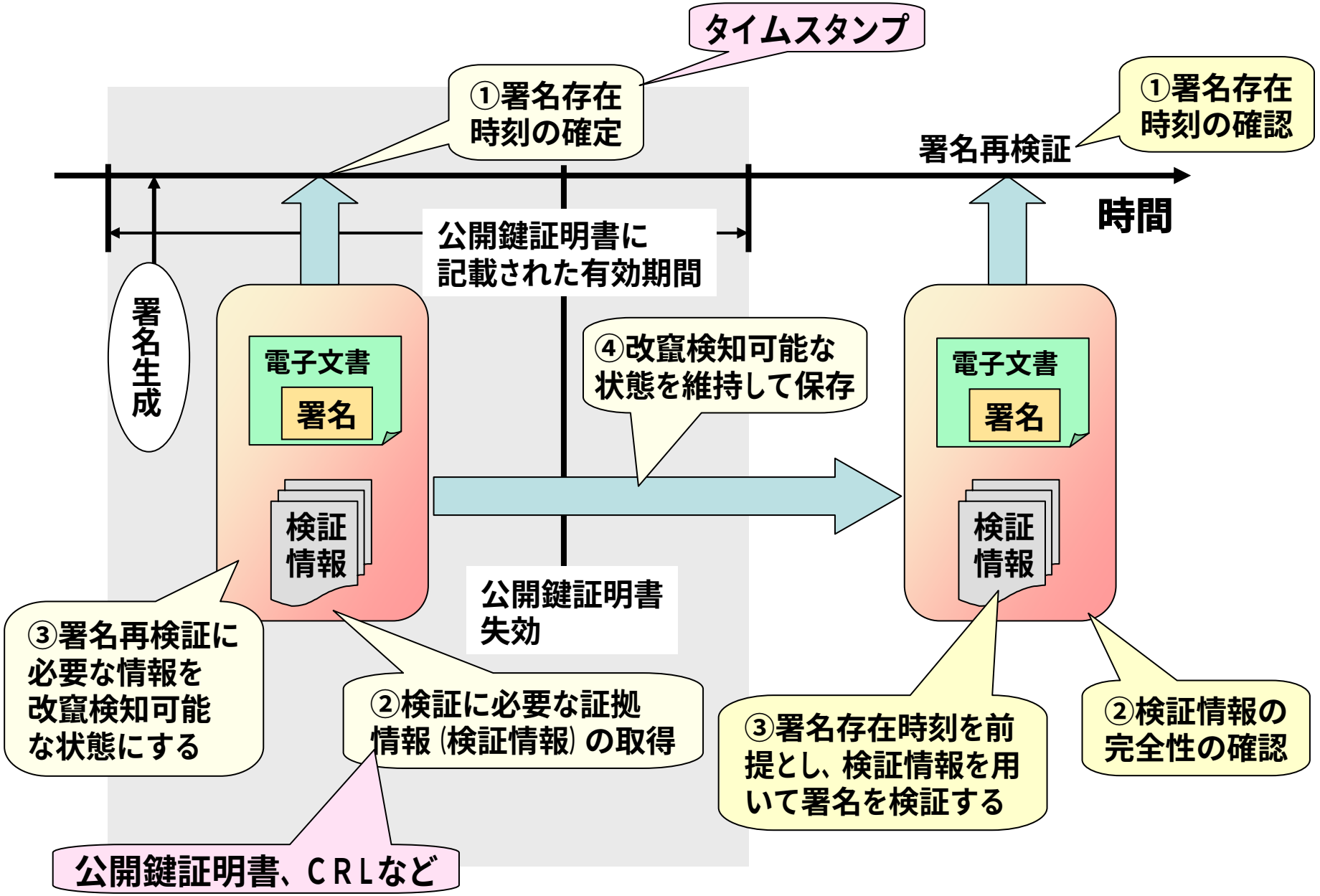


⚠ 失効が発生しても有効期間が過ぎても、署名がかって有効であったことを検証(署名再検証)できないか？

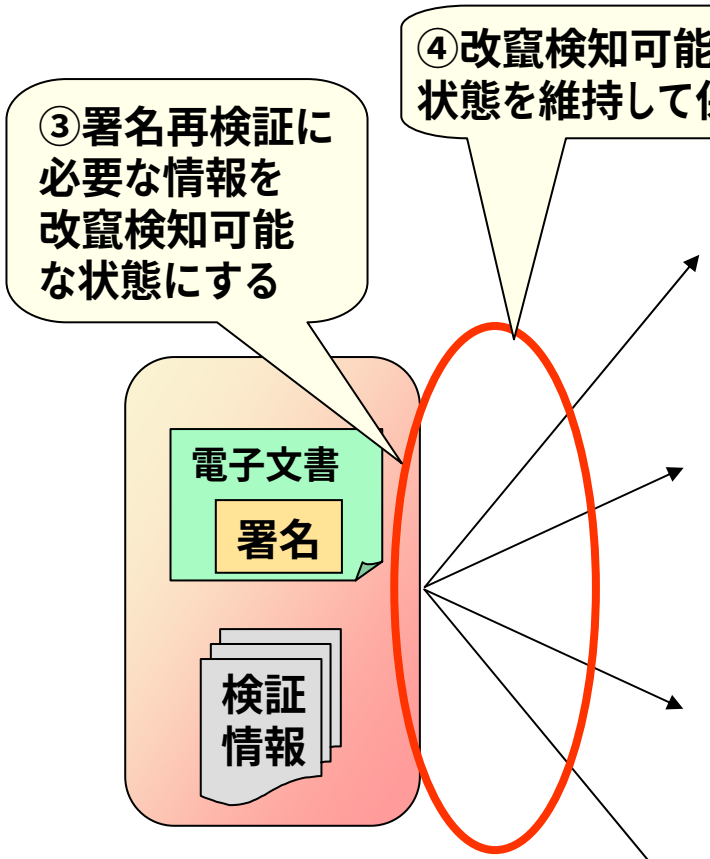
デジタル署名の生成と検証



署名再検証の要件


タイムスタンプ
①署名存在
時刻の確定
①署名存在
時刻の確認
署名再検証
時間
公開鍵証明書に
記載された有効期間
署名生成
電子文書
署名
検証
情報
④改竄検知可能な
状態を維持して保存
電子文書
署名
検証
情報
公開鍵証明書
失効
③署名再検証に
必要な情報を
改竄検知可能
な状態にする
②検証に必要な証拠
情報（検証情報）の取得
③署名存在時刻を前
提とし、検証情報を用
いて署名を検証する
②検証情報の
完全性の確認
公開鍵証明書、ＣＲＬなど

署名再検証を可能とする各種方式



タイムスタンプを重ねて利用する

電子署名文書長期保存フォーマット

耐タンパなH/Wに格納する

原本管理装置？

厳密な運用により安全に保管する

セキュア電子文書保管ASP ？

電子公証人に預ける

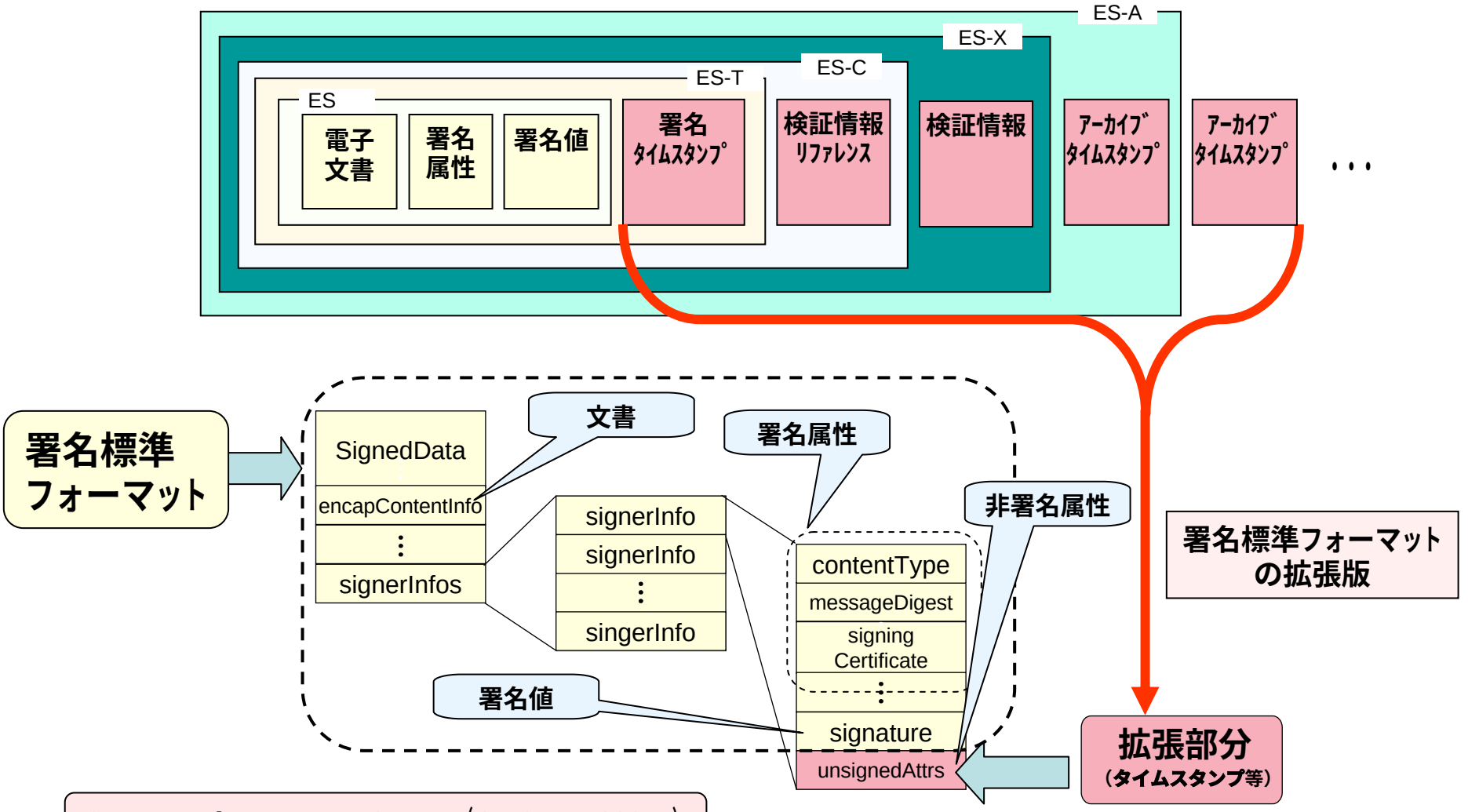
電子公証制度による電子公証サービス

CMS版標準フォーマット

Electronic Signature Formats(ETSI TS 101 733)

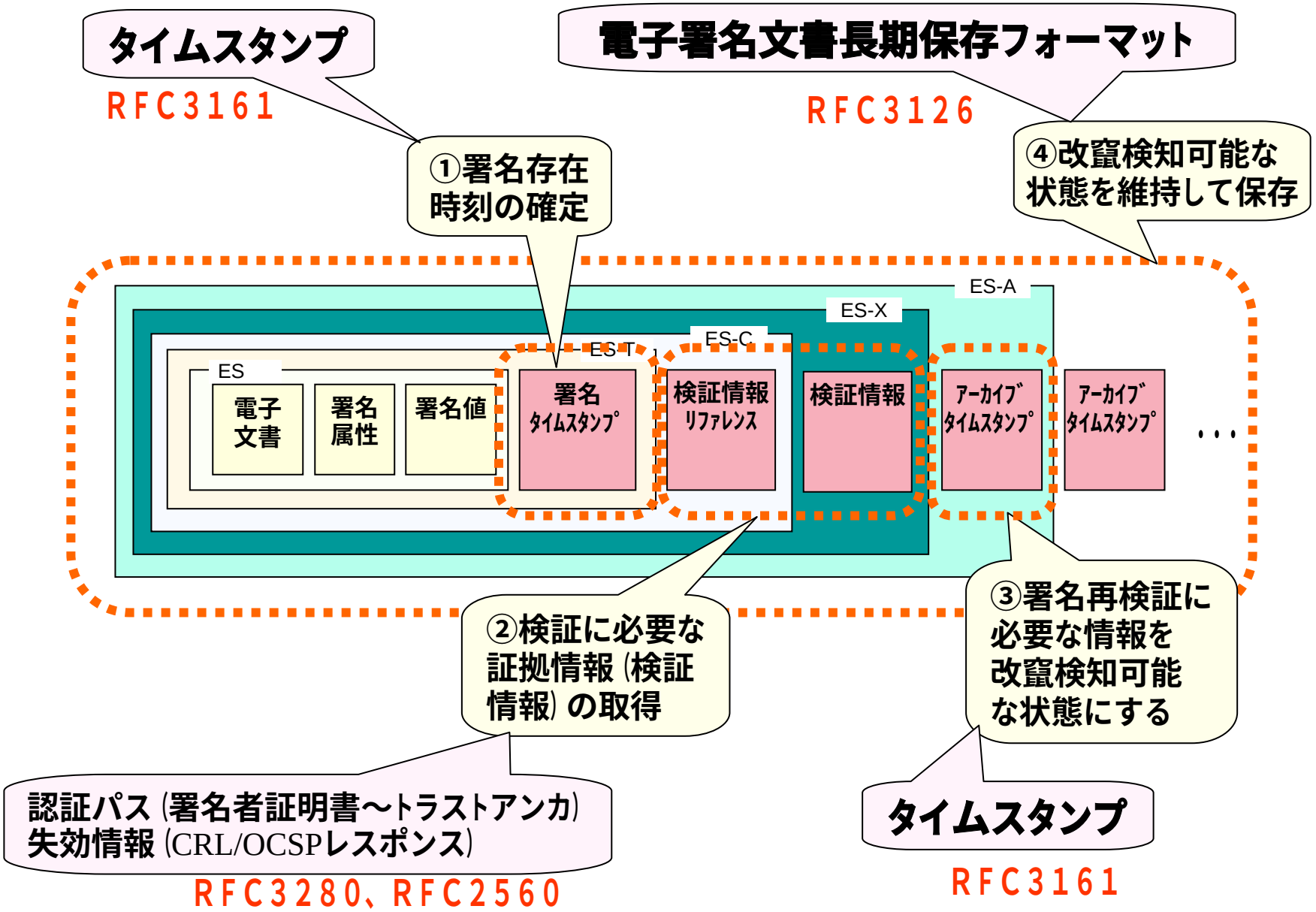
Electronic Signature Formats for long term electric signature（RFC3126)

＋ ECOMプロファイル



Cryptographic Message Syntax（CMS : RFC3852)

署名再検証の要件との関係



長期署名方式の特長

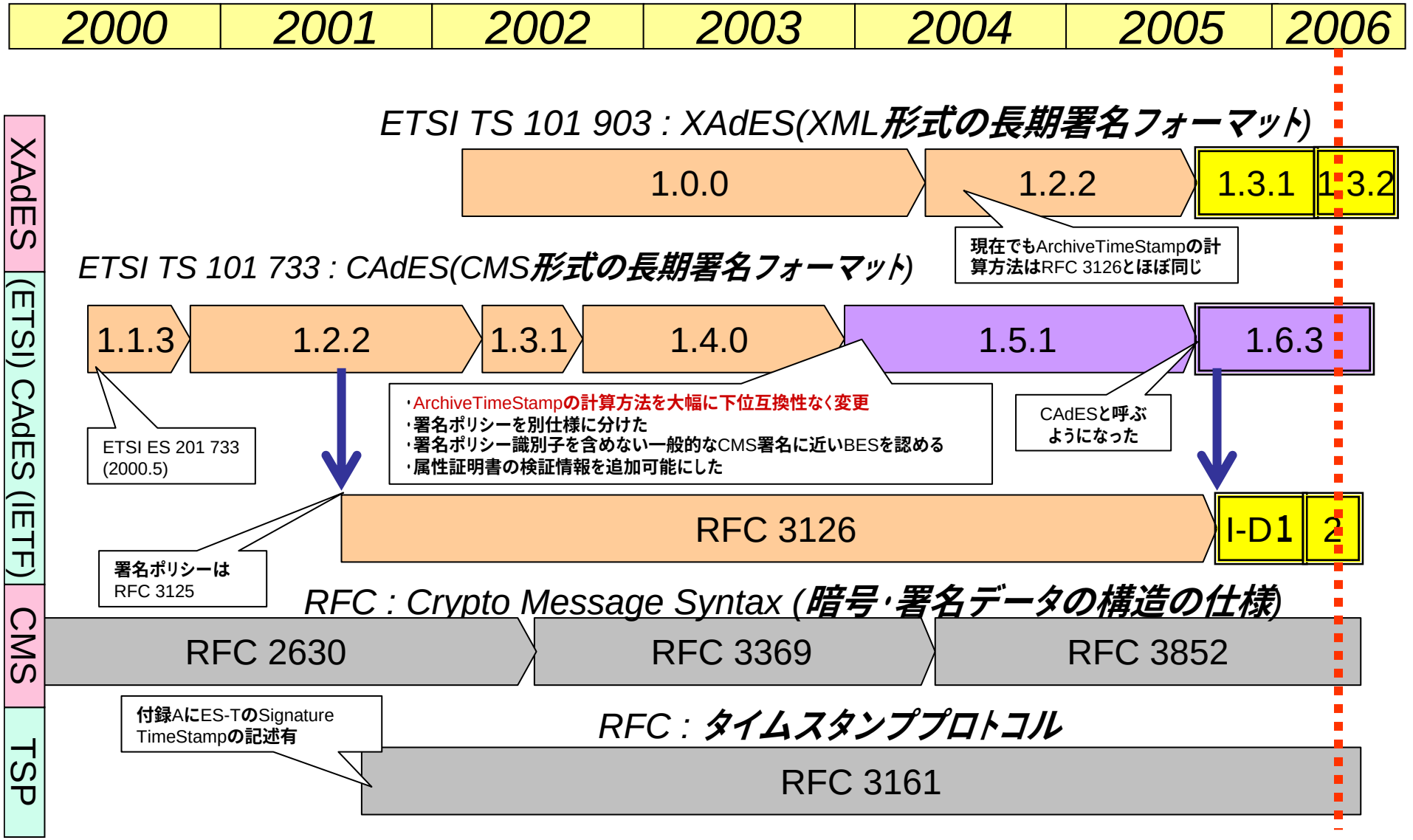
- **第三者が検証可能**
  - •署名及び証明書の検証
  - •信頼点の照合
  - •各種時刻間の整合性の検証
- **第三者が延長処理を引き継ぐことが可能**
- **最新の署名技術によるカプセル化**
  - ポータビリティ
  - 技術の陳腐化を気にする必要なし
- TTPはCAとTSAのみ
  - 『電子公証局』のような新奇な信頼点を想定する必要なし
- **複数のタイムスタンプの取得による安全性強化が可能**
  - タイムスタンプをいくつでも自由に付与できる

他の方式との比較

- **ポータビリティ、正当であることの客観性の点で有利。**

長期署名フォーマット
プロファイルの策定

長期署名関連の標準の系譜



ECOMプロファイルの要点

- CAdES版(CMS)とXAdES版(XML)がある
- 最新の仕様に合わせている
  - CAdES(ETSI v1.6.3), XAdES(1.3.1)

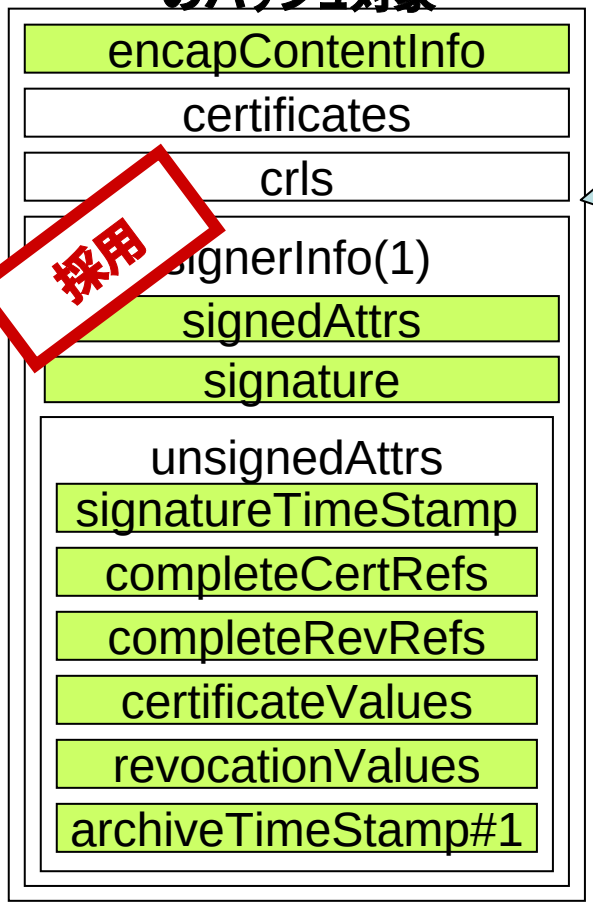
- 以下の部分のみ制限
  - ES-Aがあれば冗長となるものは除いた
    - ES, ES-T, ES-C, ES-X Long, ES-Aのみ
    - ES-X (type1/2, long type1/2は除外)
  - CAdESのアーカイブタイムスタンプの計算方法はRFC3126の方法を採用
  - 証明書の検証情報の格納方法を明示
  - CMS ver3を必須としない
    - SignerInfoのSignerIdentifierはIssuerAndSerialも可
      (SigningCertificateのcertHashが必須のため)
  - CRLとOCSPレスポンス以外(DVC等)の失効情報は除く(実証実験はCRLのみ)

主なパブリックコメントと処置(8/10意見募集、9/9締切、9/27確定)

直列署名の規程を明確化すべき
→独自仕様は避け，今後の課題とする
アーカイブタイムスタンプの処理は，ETSI TS 101 733の最新版の規程を推奨すべき
→正規化方法が未定義。今後の詳細化を待ち，現時点ではRFC3126準拠とする
XAdESについて、SignningCertificate要素を必須とすべき
→XML署名で他の代替手段(ds:KeyInfoに証明書パスを含み署名の対象とする)が既に利用されているため，変更しない

ArchiveTimeStamp計算方法

RFC 3126および
ETSI TS 101 733 v1.4.0以前
のハッシュ対象



・ハッシュ対象は必要最小限で明確
・正規化方法も一部記述(タグや長さバイトを含まない等)

・正規化に関する記述が全く無い
1) DER/BERの正規化
2) ContextSpecificタグ
3) タグ、長さバイトを含むか
・何世代かArchive Time Stampを追加している途中で他のCMS非署名属性が加えられた場合にハッシュ値が合わず検証できなくなる
・下位互換性がない

ETSI TS 101 733 v1.5.1以降
のハッシュ対象

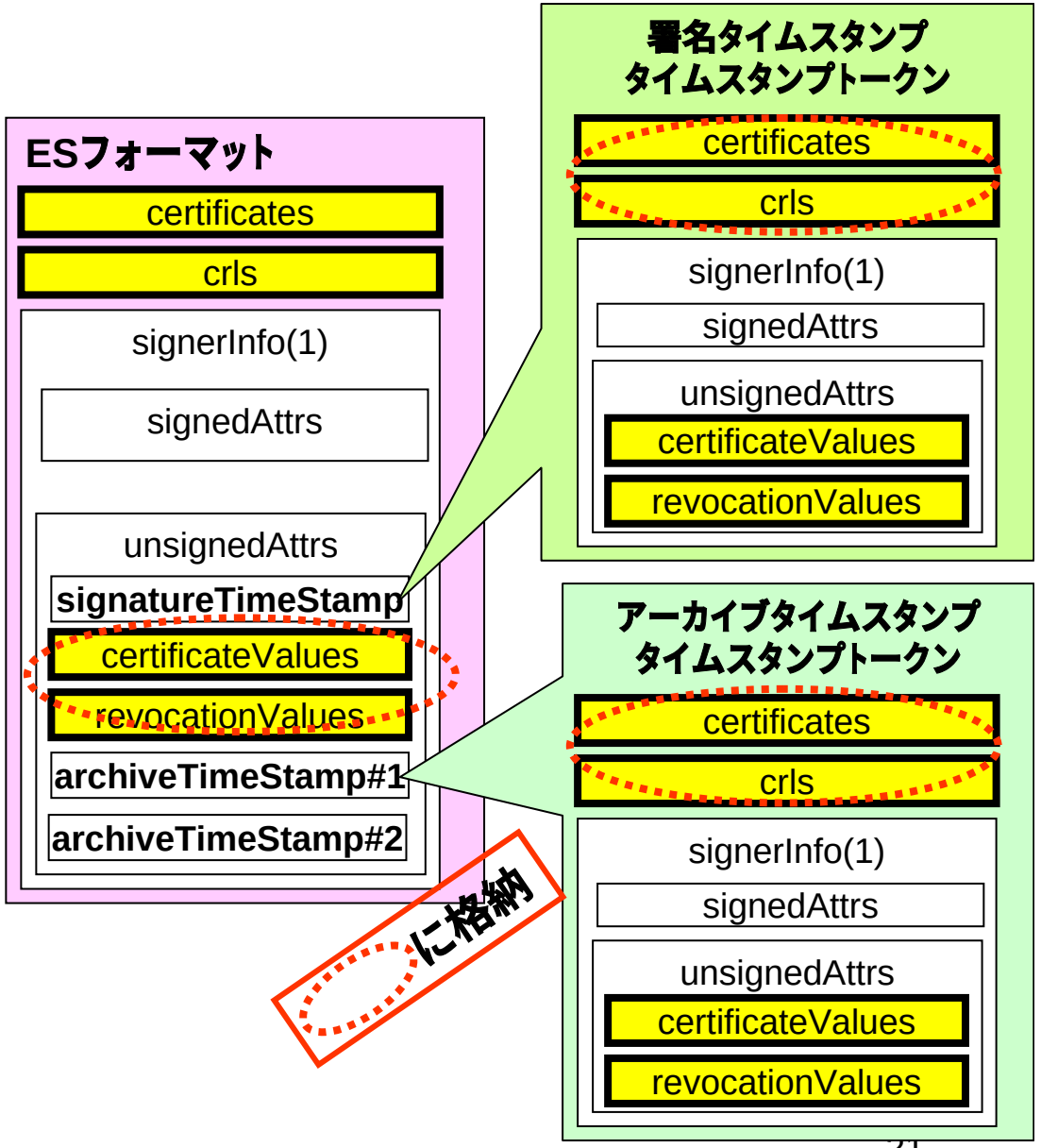
証明書検証情報の格納方法

以下の証明書の検証情報(CA→EE証明書、CRL)を格納する必要がある

1) **署名者の証明書**
2) **署名タイムスタンプのTSA証明書**
3) **最新を除くアーカイブタイムスタンプのTSA証明書(最新はリアルタイム検証)**

※ **タイムスタンプトークンもCMS構造である**

※ **追加格納できるのはCMS署名属性以外である必要があることに注意する**



CAdES版プロファイル

		CAdES BES	CAdES EPES	CAdES ES-T	CAdES ES-C	CAdES ES-X Long	CAdES ES-A
SignedAttributes		○	○	○	○	○	○
	ContentType	○	○	○	○	○	○
	MessageDigest	○	○	○	○	○	○
	SigningTime	△	△	△	△	△	△
	SigningCertificate	○	○	○	○	○	○
	SignaturePolicyIdentifier	×	○	△	△	△	△
	ContentReference	△	△	△	△	△	△
	ContentIdentifier	△	△	△	△	△	△
	ContentHints	△	△	△	△	△	△
	CommitmentTypeIndication	△	△	△	△	△	△
	SignerLocation	△	△	△	△	△	△
	SignerAttribute	△	△	△	△	△	△
	ContentTimeStamp	△	△	△	△	△	△
UnsignedAttribute		△	△	○	○	○	○
	CounterSignature	△	△	△	△	△	△
	SignatureTimeStamp	×	×	○	○	○	○
	CompleteCertificateRefs	×	×	×	○	○	○
	CompleteRevocationRefs	×	×	×	○	○	○
	AttributeCertificateRefs	×	×	×	△	△	△
	AttributeRevocationRefs	×	×	×	△	△	△
	CertificateValues	×	×	×	×	○	○
	RevocationValues	×	×	×	×	○	○
	ES-C TimeStamp	×	×	×	×	×	×
	TimeStampedCertsAndCrls	×	×	×	×	×	×
	ArchiveTimeStamp	×	×	×	×	×	○

○ 必須， △ オプション， × 不要（あってはならない），　ベース標準にそのまま従うもの

XAdES版プロファイル

	XAdES-BES	XAdES-EPES	XAdES-T	XAdES-A	備考
QualifyingProperties	○	○	○	○	
SignedProperties	○	○	○	○	
SignedSignatureProperties	○	○	○	○	
SigningTime	△	△	△	△	XAdES(V1.1.1)では必須
SigningCertificate	△	△	△	△	XAdES(V1.1.1)では必須
SignaturePolicyIdentifier	×	○	△	△	XAdES(V1.1.1)では必須
SignatureProductionPlace	△	△	△	△	
SignerRole	△	△	△	△	
SignedDataObjectProperties	△	△	△	△	
DataObjectFormat	△	△	△	△	
CommitmentTypeIndication	△	△	△	△	
AllDataObjectsTimeStamp	△	△	△	△	
IndividualDataObjectsTimeStamp	△	△	△	△	
UnSignedProperties	△	△	○	○	
UnSignedSignatureProperties	△	△	○	○	
CounterSignature	△	△	△	△	
SignatureTimeStamp	×	×	○	○	
CompleteCertificateRefs	×	×	×	△	
CompleteRevocationRefs	×	×	×	△	
AttributeCertificateRefs	×	×	×	△	XAdES(V1.1.1)では未定義
AttributeRevocationRefs	×	×	×	△	XAdES(V1.1.1)では未定義
SigAndRefsTimeStamp	×	×	×	△	
RefsOnlyTimeStamp	×	×	×	△	
CertificateValues	×	×	×	○	
RevocationValues	×	×	×	○	
ArchiveTimeStamp	×	×	×	○	

○ 必須，△ オプション，× 不要（あってはならない），ベース標準にそのまま従うもの

長期署名フォーマットの
相互運用テスト

相互運用テスト

目的:

・ECOM**長期署名フォーマットプロファイルへの準拠性の確認**

・**各組織の製品が生成するデータの相互運用性の確認**

期間: 2005**年**10**月**～12**月**

参加組織:

CAdES**フォーマットテスト参加企業**(10**社**)

RSA**セキュリティ、エヌ・ティ・ティ・データ、セコム、日本電子公証機構、日本電信電話(情報流通プラットフォーム研究所)、ハイパーギア**、PFU、**日立製作所(システム開発研究所)、三菱電機**(**情報技術総合研究所**)**、三菱電機インフォメーションシステムズ**

XAdES**フォーマットテスト参加企業**(3**社**)

関電システムソリューションズ、日本電気、富士ゼロックス

実験協力(1**社**)

エントラストジャパン

テスト内容:

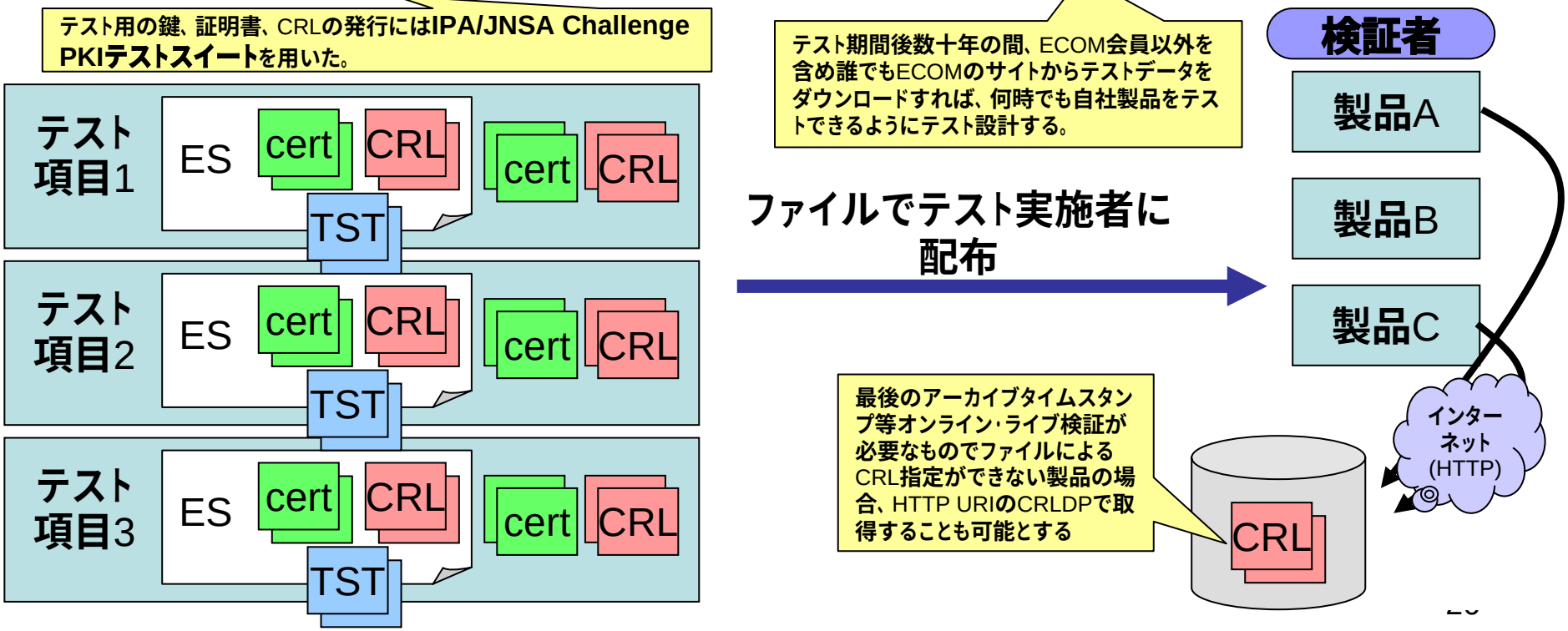
・**オフライン共通データ検証テスト**

・**製品マトリックス相互生成・検証テスト**

結果公表: 2005**年**12**月**

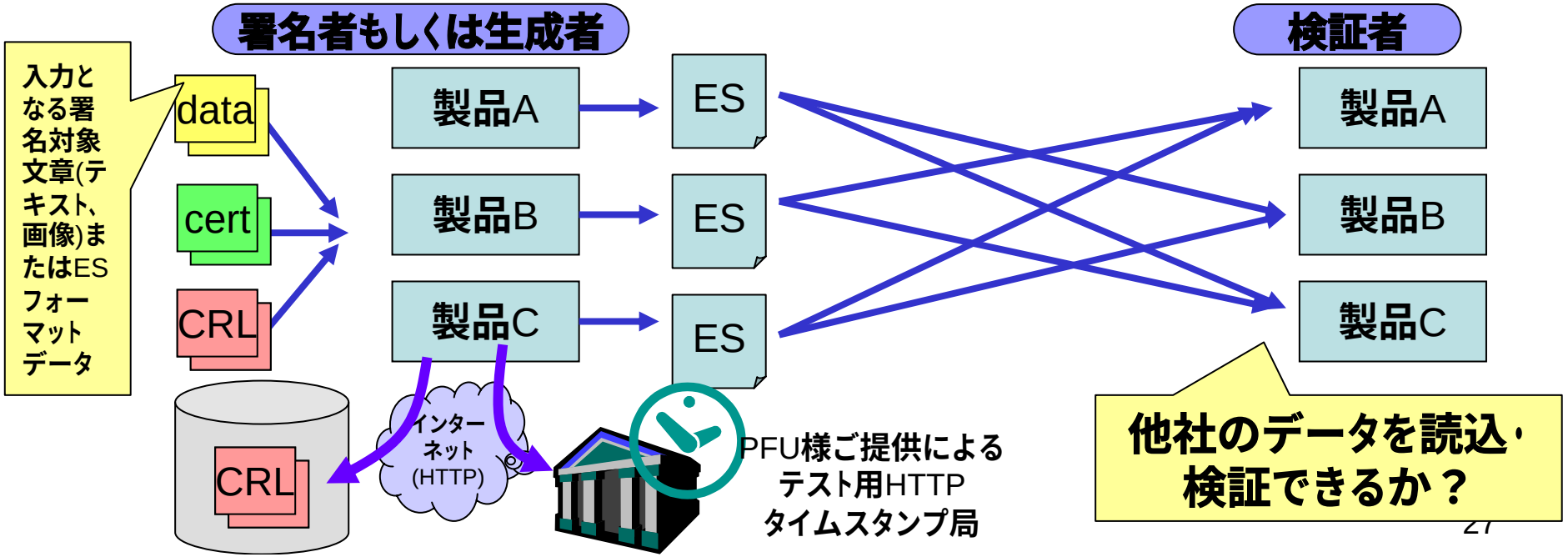
テスト1：オフライン共通データ検証テスト

目的	・ECOMプロファイルへの準拠性の確認 ・実装されている長期署名フォーマットの検証機能の確認
内容	予め用意したESフォーマットのデータ(ES-T, ES-X Long, ES-A)、検証情報のセットをテスト対象として、各社製品でオフラインにより有効性を検証する。結果は有効、無効の2種類のみ。無効の理由は問わないこととする。



テスト2：オンラインマトリックス生成・相互検証テスト

目的	・他社製品が生成した有効なESフォーマットのデータが相互に読込み、検証できることを確認
内容	指定した証明書、CRL、タイムスタンプサービスを利用し、各製品により有効であるようなESフォーマット(ES-T, ES-X Long, ES-A)を生成する。各製品において相互に読込み、他社の生成したデータが有効である事を検証する。CRL、TSAはオンライン、それ以外はオフラインとする。



オフライン共通データ検証テストケース抜粋

(全22ケース)

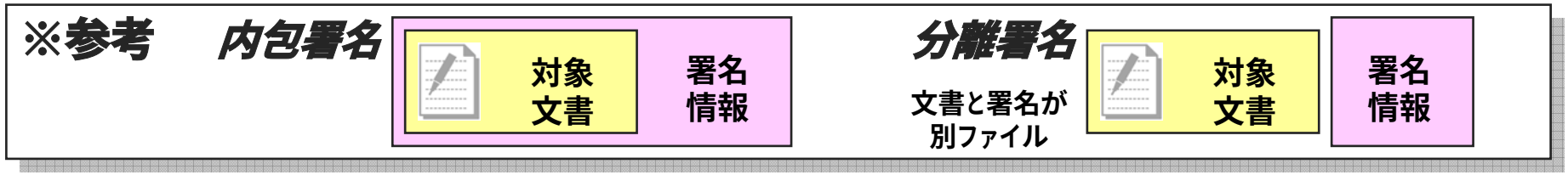
ES	ケース名	説明
T	OFF-T-1	一般的な内包署名のES-Tフォーマットを読み込むことができる
	OFF-T-4	ES-Tフォーマットの署名者証明書の認証パス検証を正しく行える
	OFF-T-5	ES-Tフォーマットでサイニングタイムに関係なく署名タイムスタンプの時刻により署名者証明書の失効検証ができる
	OFF-T-9	ES-Tフォーマットの署名タイムスタンプのタイムスタンプトークンのMessageDigestのハッシュ値の改竄を検知できる
	OFF-T-OP-1	OtherSigningCeritificate属性においてSHA-256であるES-Tフォーマットを扱える
	OFF-T-OP-3	署名タイムスタンプのタイムスタンプトークンのハッシュや署名にSHA-512アルゴリズムが使われているES-Tフォーマットを扱える
C	OFF-C-OP-1	一般的な内包署名のES-Cフォーマットを読み込むことができる
XL	OFF-X-2	分離署名のES-X Longフォーマットを扱える
A	OFF-A-1	ECOMプロファイルに基づく内包署名の第一世代のES-Aフォーマットを扱うことができる
	OFF-A-OP-2	ETSI TS 101 733 v1.5.1以降のハッシュ計算法に基づく分離署名の第一世代のES-Aフォーマットを扱うことができる

必須機能を確認する標準テストとオプショナルテストがある

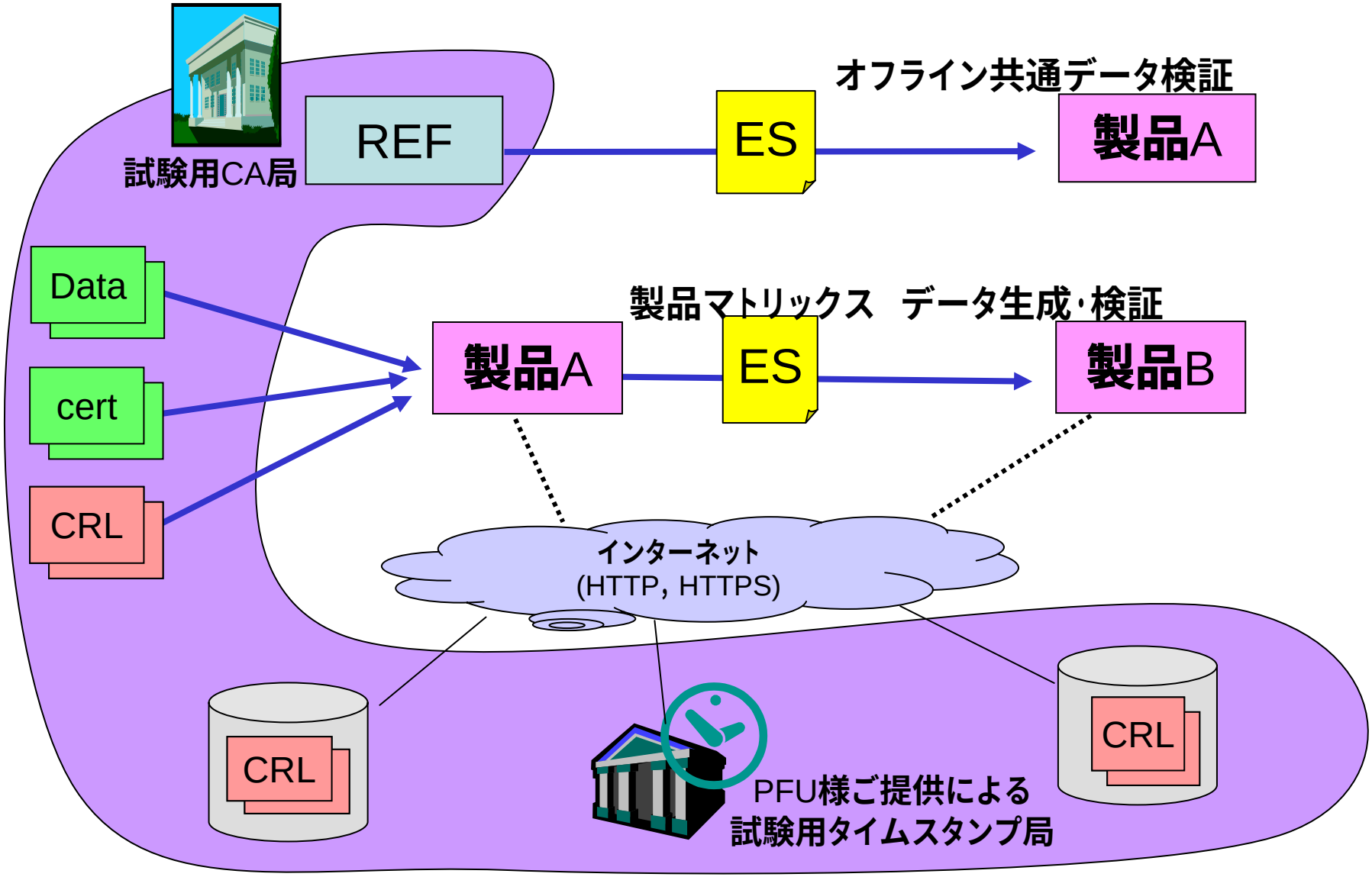
オンラインマトリックス生成･相互検証テストケース

(全10ケース)

フォーマット	ケース名	説明
ES-T	ON-T-1	**内包署名**ES-T**データの生成･相互検証**
	ON-T-2	**分離署名**ES-T**データの生成･相互検証**
ES-XL	ON-X-1	**内包署名**ES-X Long**データの生成･相互検証**
	ON-X-2	**分離署名**ES-X Long**データの生成･相互検証**
ES-A	ON-A1-1	**内包署名第**1**世代**ES-A**データの生成･相互検証**
	ON-A1-2	**分離署名第**1**世代**ES-A**データの生成･相互検証**
	ON-A1-3	V1.5.1**に基く第**1**世代**ES-A**データの生成･相互検証(オプション)**
	ON-A2-1	**内包署名第**2**世代**ES-A**データの生成･相互検証**
	ON-A2-2	**分離署名第**2**世代**ES-A**データの生成･相互検証**
	ON-A2-3	V1.5.1**に基く第**2**世代**ES-A**データの生成･相互検証(オプション)**



相互運用性テスト環境


試験用CA局
REF
ES
オフライン共通データ検証
製品A
Data
cert
CRL
製品マトリックス　データ生成･検証
製品A
ES
製品B
インターネット
(HTTP, HTTPS)
CRL
CRL
PFU様ご提供による
試験用タイムスタンプ局

2005年度のテストスケジュール

- 8/10　**プロファイル案に対する意見募集開始**
- 9/9　**意見募集締め切り**
- 9/21　**プロファイル確定**
  相互運用テスト参加企業募集開始
  http://www.ecom.or.jp/press/2005_006.html
- 10/5　**相互運用テスト説明会**
  テスト用証明書配付申し込み開始
- 10/11　**テスト用証明書配付開始**
- 10/20　**相互運用テスト開始**
- 10/25　**参加申し込み締め切り**
- 12/16　**テスト結果報告（広報）**

実験参加製品（または試作品）

	企業名(略称)	種別	製品名	Ver	リリース予定
CAdES	RSAセキュリティ	既存製品	RSA BSAFE e文書法対応ライブラリ	V1.1(β1)	‘06.02
	NTTデータ	試作品	長期署名対応プラットフォーム(プロトタイプ)	0.1	‘05.12
	セコム	既存製品	セコム長期署名ライブラリ	1.3	‘06.01
	日本電子公証機構	既存製品	JN++ 電子署名タイムスタンプSDKキット	2.0	2006
	NTT	試作品	CYNOS-L(プロトタイプ)	1	ー
	ハイパーギア	既存製品	HG/PscanServ Pro	4.0	‘06.02
	PFU	試作品	PFU長期署名ライブラリ(プロトタイプ)	0.1	ー
	日立製作所	試作品	長期署名フォーマットライブラリ(プロトタイプ)	0.1	ー
	三菱電機	試作品	ー	ー	ー
	MDIS	既存製品	三菱署名有効性延長システムMistyGuard<EVERSIGN>	2.0	‘06春
XAdES	関電システム	新規製品	XAdES長期署名ライブラリ for .NET	1.3	‘06.01
	NEC	試作品	PKIサーバ/Carassuite原本保管サーバ	3.0プロトタイプ	ー
	富士ゼロックス	新規製品	ArcSuite	ー	ー

オンライン生成･相互検証テスト結果

	データ生成企業名(略称)	種別	ES-T	ES-XL	ES-A	備考
CAdES	RSAセキュリティ	既存製品	○	○	○	
	NTTデータ	試作品	○	○	○	
	セコム	既存製品	○	○	○	
	日本電子公証機構	既存製品	○	○	○	
	NTT	試作品	○	○	○	
	ハイパーギア	既存製品	○	○	○	
	PFU	試作品	○	○	○	
	日立製作所	試作品	○	○	○	
	三菱電機	試作品	○	○	○	
	MDIS	既存製品	○	ー	○	
XAdES	関電システム	新規製品	○	ー	○	
	NEC	試作品	○	ー	○	
	富士ゼロックス	新規製品	○	ー	○	

凡例：
○：サポート(合格)
×：不合格
ー：製品非サポート

オフライン共通データ検証テスト結果

	データ生成企業名(略称)	種別	ES-T	ES-XL	ES-A	備考
CAdES	RSAセキュリティ	既存製品	○	○	○	
	NTTデータ	試作品	○	○	○	
	セコム	既存製品	○	○	○	
	日本電子公証機構	既存製品	○	○	○	
	NTT	試作品	○	○	○	
	ハイパーギア	既存製品	○	○	○	
	PFU	試作品	ー	ー	ー	
	日立製作所	試作品	○	○	○	
	三菱電機	試作品	○	○	○	
	MDIS	既存製品	○	ー	○	
XAdES	関電システム	新規製品	○	ー	○	
	NEC	試作品	○	ー	○	
	富士ゼロックス	新規製品	○	ー	○	

凡例：
○：サポート(合格)
×：不合格
ー：製品非サポート

相互運用実証実験で判明した懸案事項

- **共通の懸案事項**
  1. **各証明書の有効性確認の基準日時の定義**
  2. **失効情報取得までの猶予期間**(Grace Period)**の設定**

- CAdES**フォーマットの実証実験上の懸案事項**
  3. **アーカイブタイムスタンプのハッシュ対象となるデータの**BER→DER **正規化方法**
  4. ETSI**および**RFC**の新方式のハッシュ計算方法**

- XAdES**フォーマットの実証実験上の懸案事項**
  5. SigningCertificate**要素が存在する場合の**keyInfo**要素の扱い**
  6. V1.2.2**ベース、**V1.3.1**ベースといったバージョン間の差異吸収**
  7. **検証情報の持ち方（タイムスタンプトークンに埋め込むか否か）**

懸案1：証明書の検証日時

- ESフォーマットで使われる証明書に関し、実験メンバ間で合意がとれていないことで議論となった
  - 署名者証明書
  - 署名タイムスタンプ中のTSA証明書
  - アーカイブタイムスタンプ中のTSA証明書

- 各証明書が「何時の時点で有効であったか」を定める必要がある
- ES-T,C,XLとES-Aを検証する時とで検証日時を変える必要がある
- 仕様・プロファイルからは理解が難しい

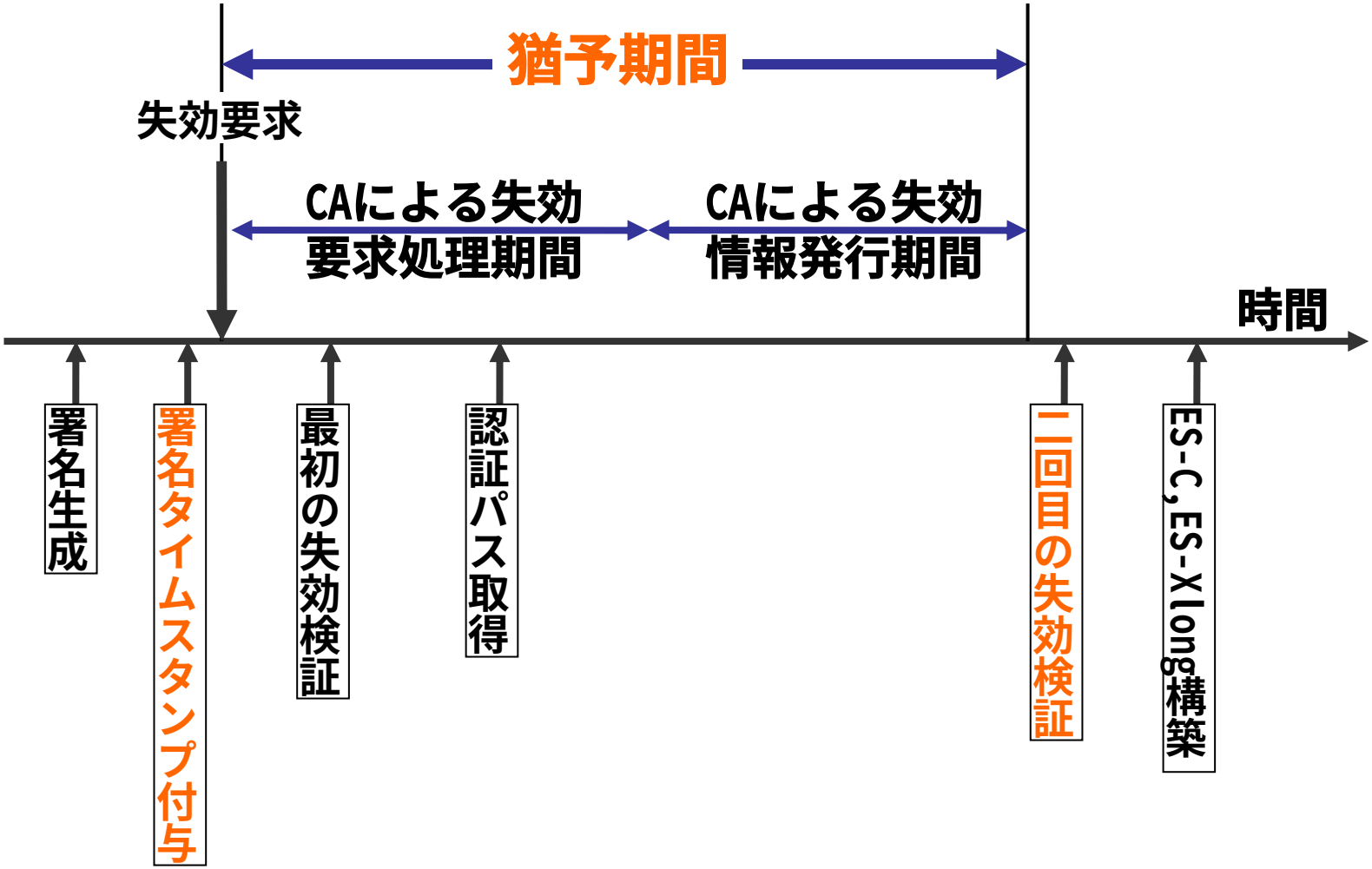
証明書の検証日時に関する合意事項

フォーマット	証明書の種類	有効性を確認すべき日時
ES-T	署名者証明書	署名タイムスタンプ属性のトークンの時刻
	署名タイムスタンプTSA証明書	現在時刻
ES-C ES-XL	署名者証明書	署名タイムスタンプ属性のトークンの時刻
	署名タイムスタンプTSA証明書	現在時刻またはセキュアアーカイブされた時刻
ES-A	署名者証明書	署名タイムスタンプ属性のトークンの時刻
	署名タイムスタンプTSA証明書	第1世代アーカイブタイムスタンプのトークンの時刻
	第1世代アーカイブタイムスタンプTSA証明書	第2世代アーカイブタイムスタンプのトークンの時刻
	第2世代アーカイブタイムスタンプTSA証明書	第3世代アーカイブタイムスタンプのトークンの時刻
	:	:
	第n-1世代アーカイブタイムスタンプTSA証明書	第n世代アーカイブタイムスタンプのトークンの時刻
	第n世代アーカイブタイムスタンプTSA証明書	現在時刻

解決済み

懸案2：猶予期間(grace period)

- 証明書の失効申請をしてから署名検証者がその反映を利用できるようになるまでの期間を「猶予期間」という
  - ETSI TS 101 733 v1.5.1以降詳しく述べられるようになった



懸案2：猶予期間(grace period)

- 証明書の失効申請をしてから署名検証者がその反映を利用できるようになるまでの期間を「猶予期間」という
  - ETSI TS 101 733 v1.5.1以降詳しく述べられるようになった
- 猶予期間を厳密に実装している製品が幾つかあり、テストデータの対応させたり、また製品側で調整が必要な場合もあった

- 猶予期間後にES-C, ES-X Long, ES-Aを作成しないと署名者の失効状態が反映されていない可能性がある。
- 猶予期間は認証サービスのCP/CPSによる。長期署名フォーマットでは署名ポリシーにこれを記すことも可能。

懸案3：BER→DER正規化

BER→DER正規化方法が製品によって異なりハッシュ値が合わない

BER不定長表現のDER正規化

A0 80 型は[0] で長さ不定長’0x80’

04 02 61 61 OCTETSTRING ‘aa’

00 00 終端記号 ‘0x00,0x00’

固定長 ‘0x04’にDER正規化

A0 04 04 02 61 61

SET OF構造のDER正規化

31 0B SET OF SEQUENCE

30 04 04 02 1F 1F

30 03 04 01 1F

31 0B

ソート

30 03 04 01 1F

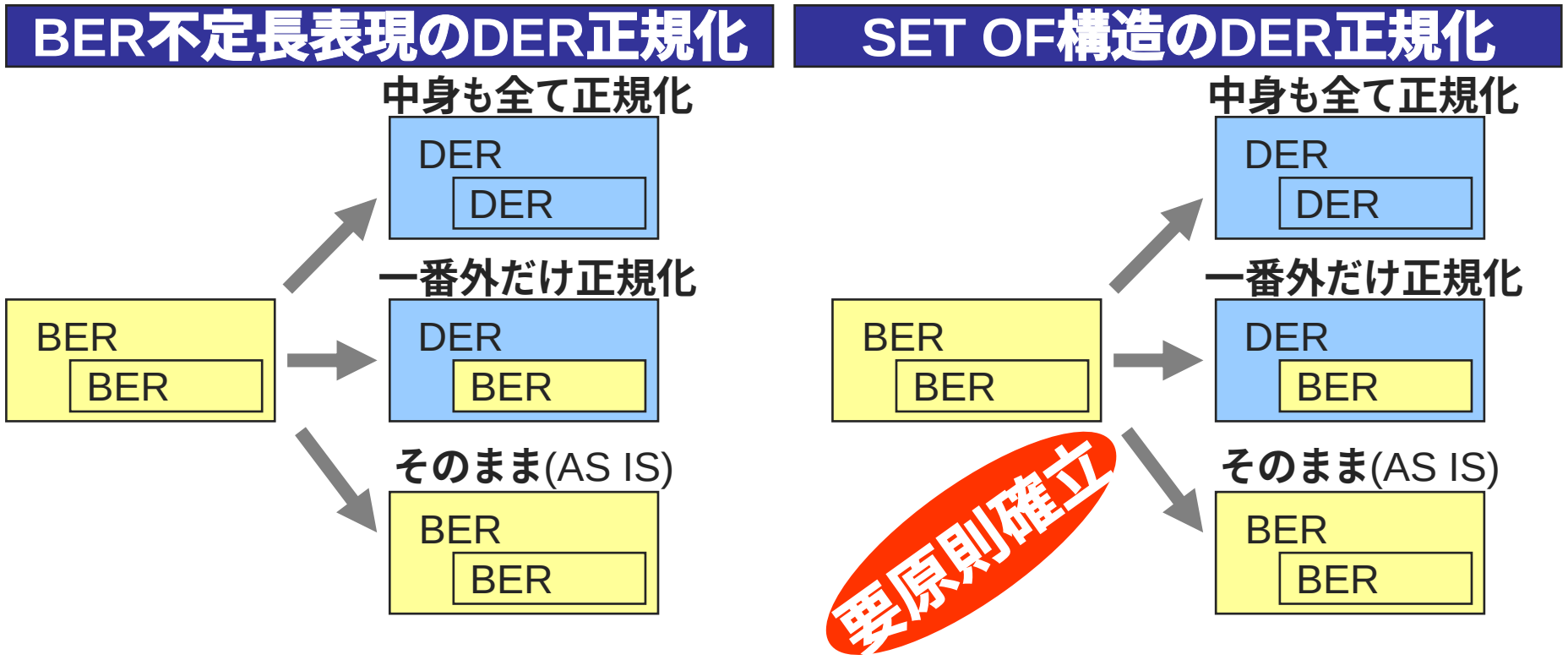
30 04 04 02 1F 1F

ESの元であるCMSはBERで表現される
のであらゆる所で使われる可能性がある

CMSのcertificates, crls, signedAttrs,
unsignedAttrsなどで使われる

懸案3：BER→DER正規化

- **正規化するといってもどの範囲まで正規化するのか？**
- **例えばCMS属性のタイムスタンプトークンの中身まで正規化する必要があるか？**
- **・signedAttrやencapContentInfoなど正規化対象は様々→場所によって異なるのは困る**

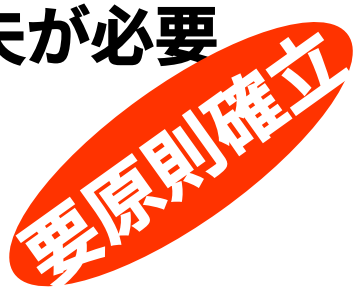


懸案4：CAdES v1.5.1アーカイブハッシュ

オフライン検証のオプショナルテストとしてETSI v1.5.1以降、またRFC 3126の後継(id-cades)となるアーカイブハッシュ方式のテストケースを提供し有志がテストを行った。
仕様には正規化の説明、ASN.1 TLV構造のVのみをとるといった記述は全くないため、テスト用に数多くのレギュレーションを設ける必要があった。

- **各IMPLICITタグはそのままハッシュ対象とする**
- DER**正規化する(内部構造までではなく表層の部分のみの正規化)**
- **分離署名の**encapContentInfo**はDERでコンテンツを含むよう再構築**

- **標準かプロファイルで規定しないと相互運用は困難**
- **新旧両バージョンの共存を可能とする工夫が必要**
- ETSI**との協調作業が必要**



懸案5：KeyInfo要素の扱い

- XAdESではKeyInfo要素について煩雑な制約があり、SigningCertificate要素が存在したときにkeyInfo要素をどう扱うかが議論となった。
  - SigningCertificate要素がなくても以下の条件を満たすKeyInfoがあれば、SigningCertificateの替わりとなる。
    - ① ds:KeyInfoは、署名者証明書を含むds:X509Data要素を含まなければならない
    - ② ds:KeyInfoは、信頼点までの証明書チェーンを構成する証明書も含む場合がある。
    - ③ ds:SignedInfo要素のds:Reference要素でds:KeyInfoを参照することにより、署名の計算対象として署名値の計算に含まれなければならない。
  - ArchiveTimeStampの計算時のkeyinfo関係の規定として以下がある。
    - 上記③で参照されている場合は、アーカイブタイムスタンプ対象とする。ds:SignedInfo要素内のds:Reference毎にInclude要素を生成する。
    - 上記とは別にds:KeyInfo をアーカイブタイムスタンプの対象とする必要がある

- 案1　状況によってkeyinfoを署名対象とするかどうかの判断が煩雑なので、keyinfoは必ず署名対象とする。
- 案2　CMSではcertificatesフィールドに署名者証明書が入っているが署名対象ではない、仕様を厳密に読めば、SigningCertificate要素があるときSignedInfoからKeyInfoへのRefernece がなくてもの問題ないなどの理由から、keyInfoを署名対象とするかどうか署名文書生成者が自由に決められるべき。
- 結論　プロファイルとしては、案2 (標準準拠) を採用する

懸案6：XAdESのバージョン差異の吸収

- **バージョンの互換性の問題**
  - ECOMプロファイル→当時未リリースのETSI TS 101 903 v1.3.1をベースにしている
  - 実験メンバによってはETSI TS 101 903 v1.2.2をベースにしているものがあり、バージョンによって互換性が問題となった。
- **実験参加製品では複数のバージョンを検証できるように機能追加し問題を解決した。**

- **プロファイルで複数バージョンの検証を義務付けるか否か**

懸案7：検証情報の持ち方

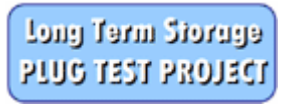
- XAdESにおいて、タイムスタンプトークンへの検証情報の埋め込みは製品ごとにまちまちであり、特に複数世代を持つES-Aフォーマットの場合には、相互運用性に課題があることがわかった
- 実験は、タイムスタンプトークンに検証情報を埋め込む方式で実施

- プロファイルを分けるべきか否か

今後の予定

- **成果の展開**
  - **実証実験報告書の作成(エグゼクティブサマリは英語版も作成)・公開**
  - **成果の国際的(ETSI、韓国、中国等)な広報**
- **実験結果を受けたECOMプロファイルの改定**
- ECOM**プロファイル、テストケース設計書、テストデータ (準備中) の公開**

  ECOM**サイト** (http://www.ecom.or.jp/) **よりWebで一般公開**

  - **テストデータとテストケースを入手すれば誰でも製品を検証可能**
  - **一部のテストは環境整備が必要**
    - **オンライン生成テスト (テスト用タイムスタンプ局の終了、検証は可)**
    - **HTTPリポジトリを使った失効検証 (HTTPリポジトリ終了)**
- **有志によるオフラインオプショナルテストケースの追加実験**
- ECOM**プロファイルの**JIS**化** (2006/5/23**プレスリリース**)

  「長期署名フォーマットプロファイルの標準化に向けた活動を開始」
  － ETSI/ESI**と協調し**JIS**原案作成に着手 －**
- **長期署名を含むデジタル署名ハンドブック作成**
- ETSI**との連携**
- **まだまだ不十分なインフラの整備へ**

END