Information Security Laboratory
ISL

総務省公的個人認証サービス
における暗号移行検討会

資料3

2008年12月18日

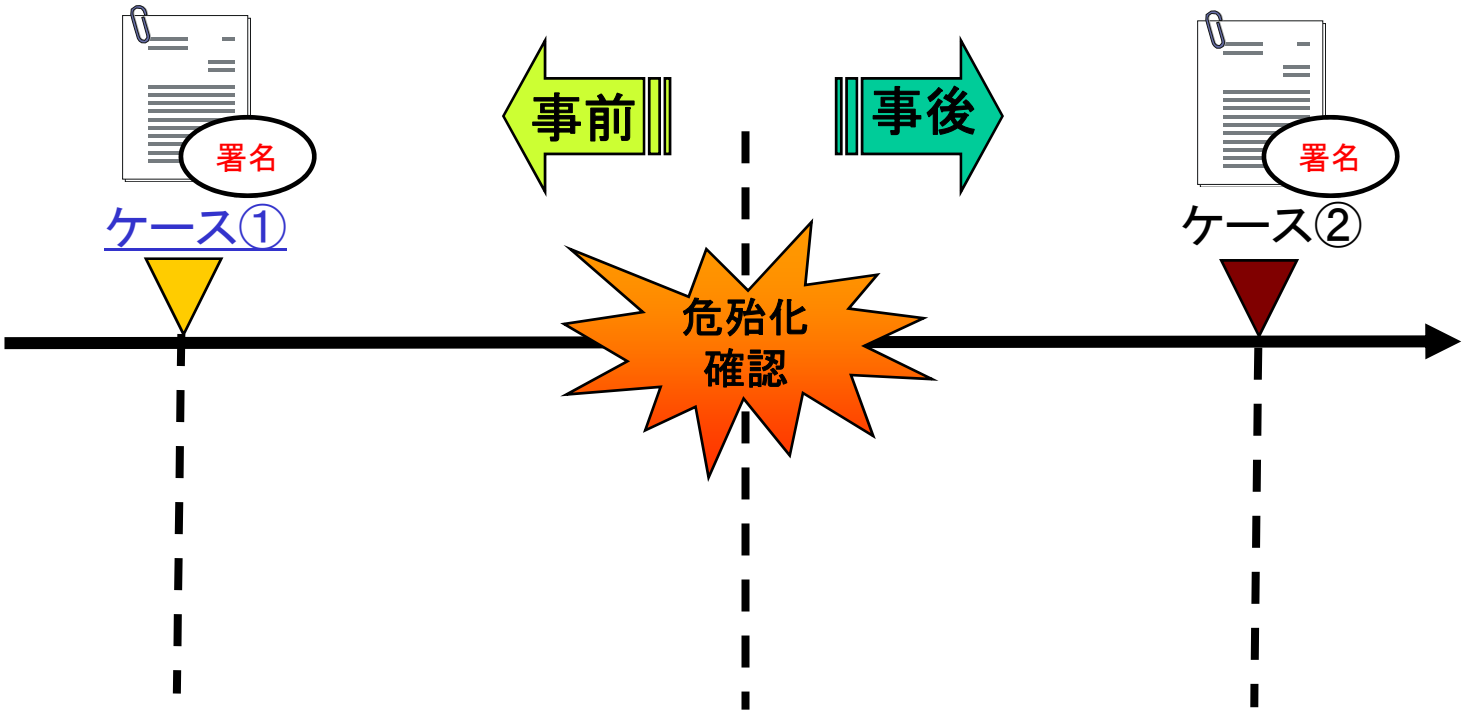
暗号移行のための
残された検討課題

東京電機大学教授
佐々木良一
sasaki@im.dendai.ac.jp

背景

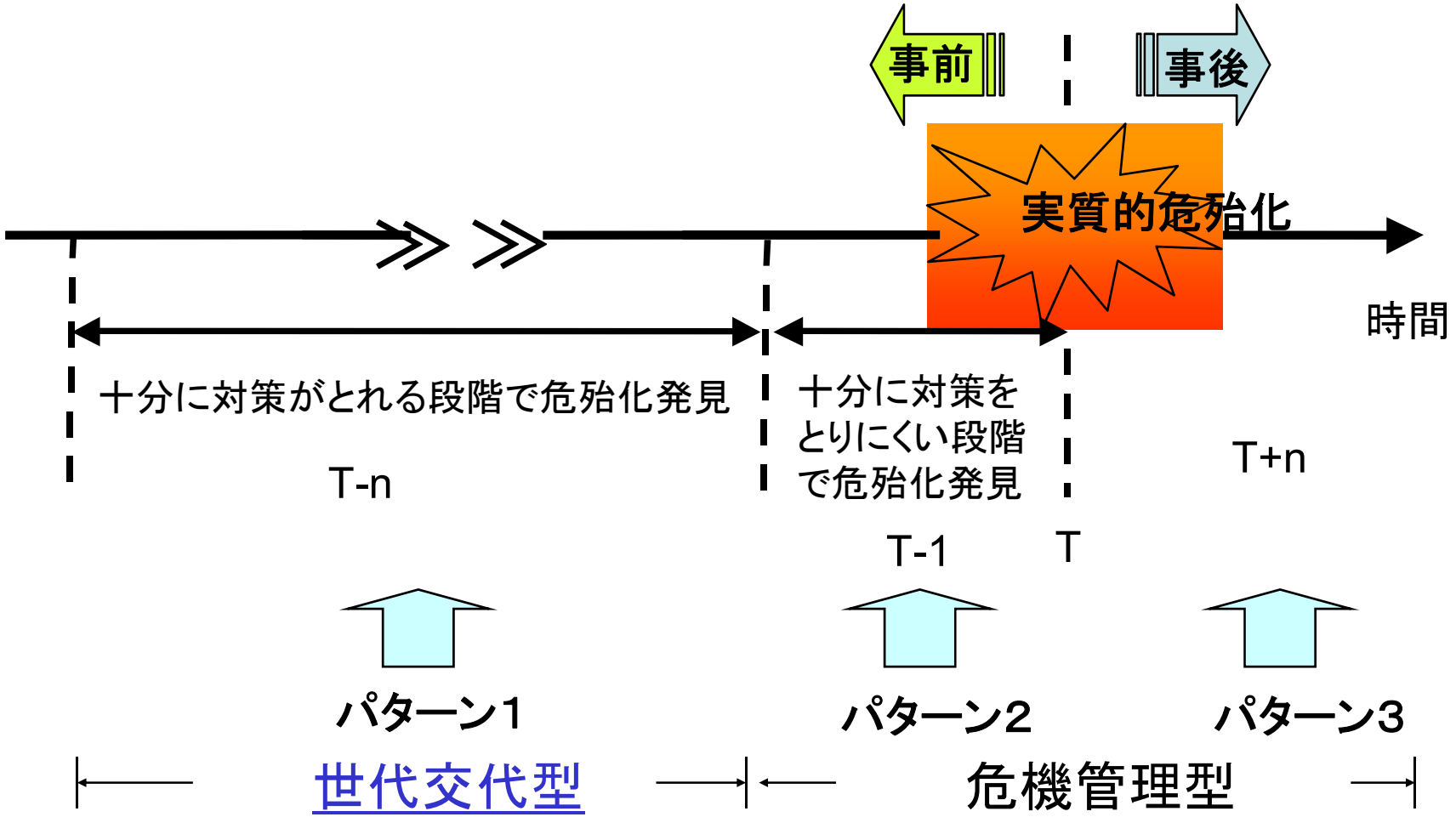
危殆化確認前から既に存在する
デジタル署名付文書

危殆化確認後に新しく生成される
デジタル署名付文書



- ケース②が本研究会の主要対象。
- ケース①についても検討必要。

危殆化発見パターン



ここでは、代替公開鍵暗号があり、危殆化を確認した際に、十分に既存の署名に対して対策がとれるパターン1で危殆化を発見するものとする.

既存署名付文書への対応（ケース①）

検討対象

① 一般の認証サービスを利用したシステムへの対応
（a）署名付文書は短期間のみ利用（電子申請など）
（b）署名付文書を長期間利用（電子借用書への署名などのように署名付文書を検証者が保管）
（c）署名付文書を長期間利用（長期保存文書への署名などのように署名付文書を署名者が保管）

② 公的個人認証サービスを利用したシステムへの対応

対策手法

（1）通常のデジタル署名

（2）長期署名フォーマット

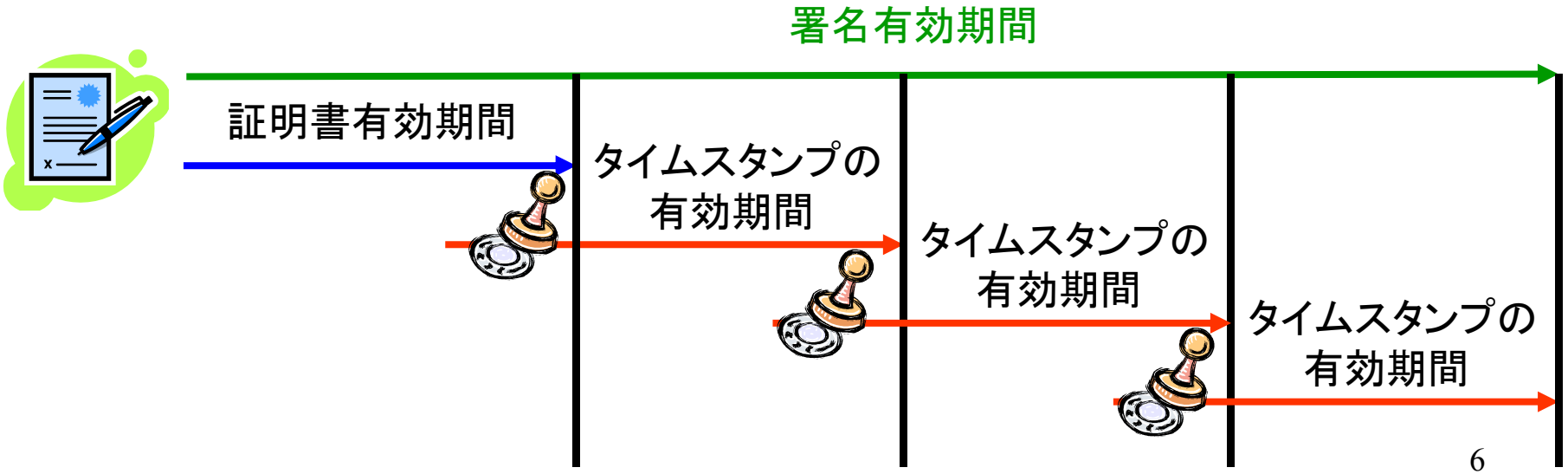
- 欧州電気通信標準化協会(ETSI)によって提案
  - ETSI TS 101 733
  - ETSI TS 101 903
  - RFC3126

    などで標準化

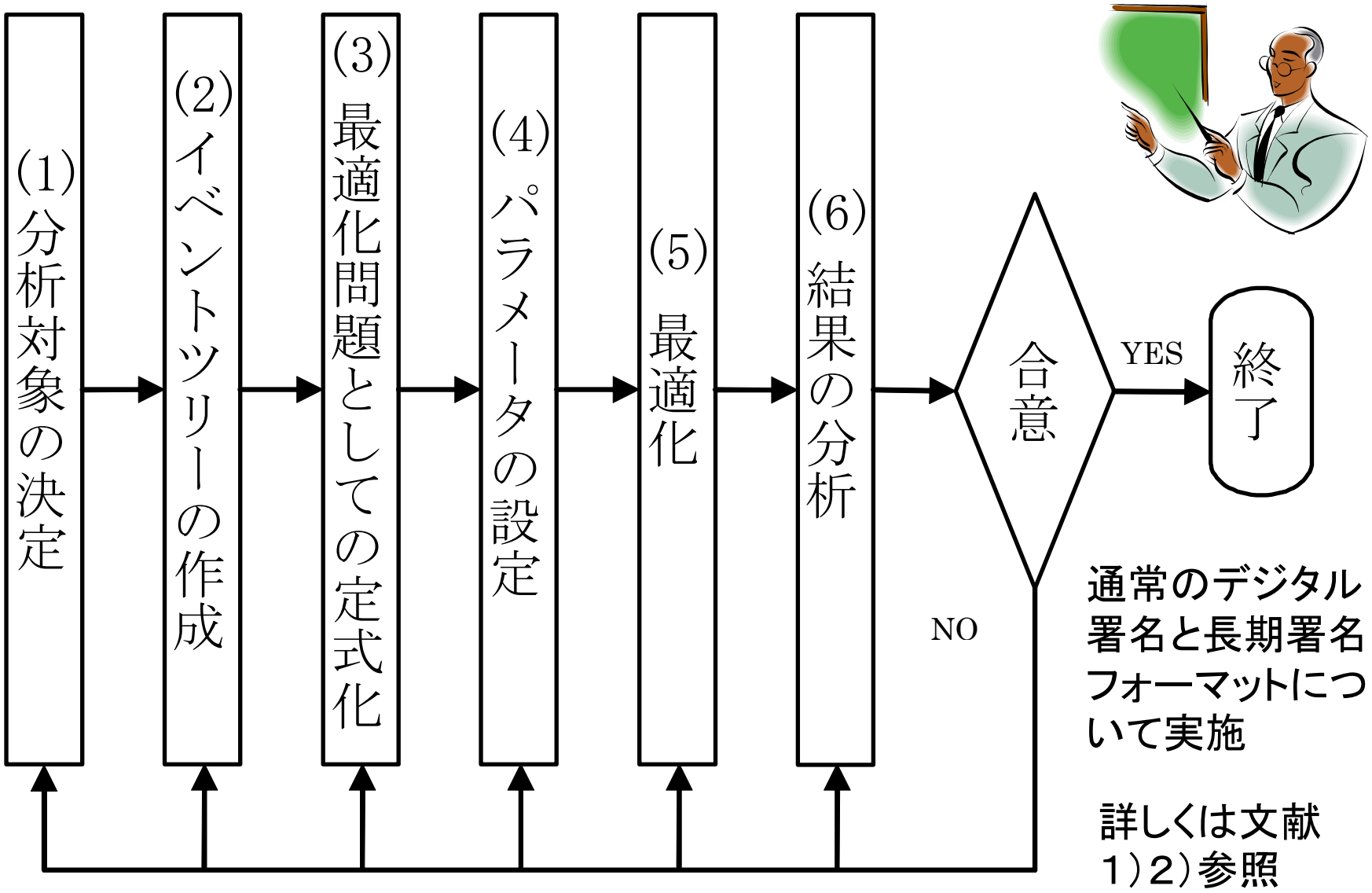
- 日本では次世代電子商取引推進協議会(ECOM)が普及を図る
  - 長期署名プロファイルがJIS化（2008年3月）

長期署名フォーマットについて

- 長期署名フォーマット（ES-A）の基本的な仕組み
  - タイムスタンプを重ねがけすることにより、署名の有効期間を延長していく
    - 検証情報(CAの証明書や失効情報など)の保管
    - 定期的なタイムスタンプの更新



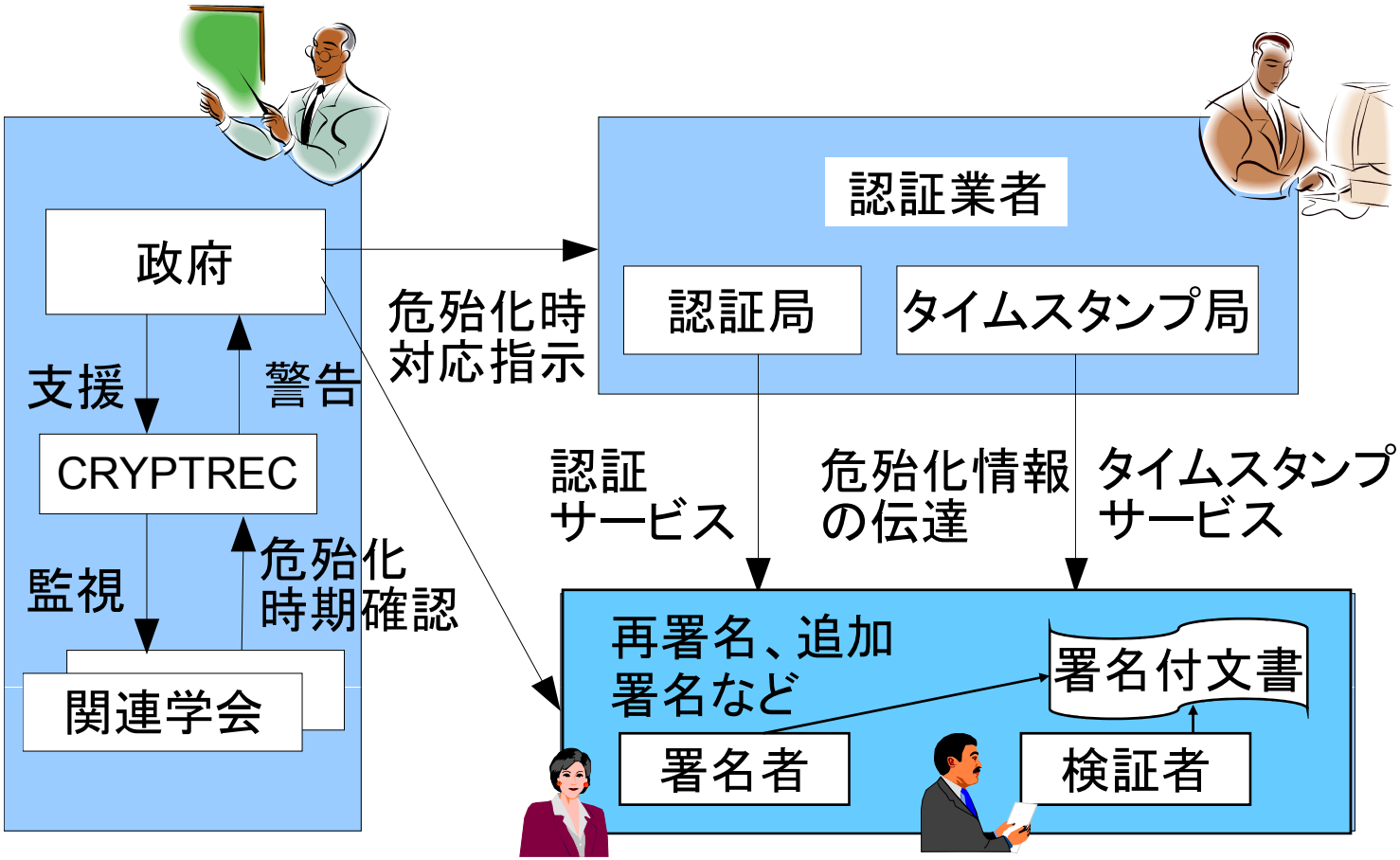
評価方法



通常のデジタル署名と長期署名フォーマットについて実施

詳しくは文献1）2）参照

危殆化発見時の対応


政府
支援
警告
CRYPTREC
監視
危殆化
時期確認
関連学会
危殆化時
対応指示
認証業者
認証局
タイムスタンプ局
認証
サービス
危殆化情報
の伝達
タイムスタンプ
サービス
再署名、追加
署名など
署名付文書
署名者
検証者

分析結果

対象 ＼ 対応方式		デジタル署名	長期署名フォーマット
署名付文書は短期間のみ利用（電子申請など）		①問題なし	②問題なし
署名付文書を長期間利用	署名付文書を検証者が保管（電子借用書への署名など）	③詳細説明1参照	④詳細説明2参照（問題なし）
	署名付文書を署名者が保管（長期保存文書への署名など）	⑤（この使い方は通常存在しない）	⑥問題なし

詳細説明１

(a)　暗号危殆化の情報を検証者に広く確実に伝達するしくみが必要（署名者に連絡する手段はすでにあるが検証者にはない）

(b)　暗号危殆化時には、署名者が既存文書に再署名をしない可能性があるので、再署名確実にするよう強制するか（再署名ポリシーの事前締結など）、しなくてもよい仕組み（時刻認証局で既存文書に自動追加署名する方式など）が不可欠

(c)　CRYPTRECのような暗号監視機関の活動は重要であり、この活動を強化することが望ましい。

藤本肇，上田祐輔，佐々木良一「デジタル署名付き文書への公開鍵暗号危殆化対策の組合せ最適化法の提案と一適用」 情報処理学会論文誌、第49巻第3号、pp1105-1118 （平成20年）参照

詳細説明2

詳細説明1で述べたデジタル署名を長期利用に用いる際の次の2つの問題は長期署名フォーマットを用いることで以下のようになる。

(a) 暗号危殆化の情報を検証者に広く確実に伝達するしくみが必要＝＞署名つき文書を検証者が持つ場合は時刻認証局より検証者に連絡できる仕組みがあるので問題ない。

(b) 暗号危殆化時には、署名者が既存文書に再署名をしない可能性があるので、再署名を確実にするよう強制するか、しなくてもよい仕組みが不可欠＝＞ 時刻認証局で既存文書に追加署名を自動的に行うようにすれば対応可能。

既存署名付文書への対応（ケース①）

検討対象

① 一般の認証サービスを利用したシステムへの対応

（a）署名付文書は短期間のみ利用（電子申請など）

（b）署名付文書を長期間利用（電子借用書への署名などのように署名付文書を検証者が保管）

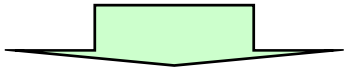
（c）署名付文書を長期間利用（長期保存文書への署名などのように署名付文書を署名者が保管）

② 公的個人認証サービスを利用したシステムへの対応

公的個人認証サービスを利用したシステムへの対応

1．公的個人認証サービスでは、長期利用文書に対する署名はほとんど無いようである。（要検討）

2．公的個人認証サービスでは、検証者は通常、公的機関なので、危殆化情報の連絡ルートは確保されている。



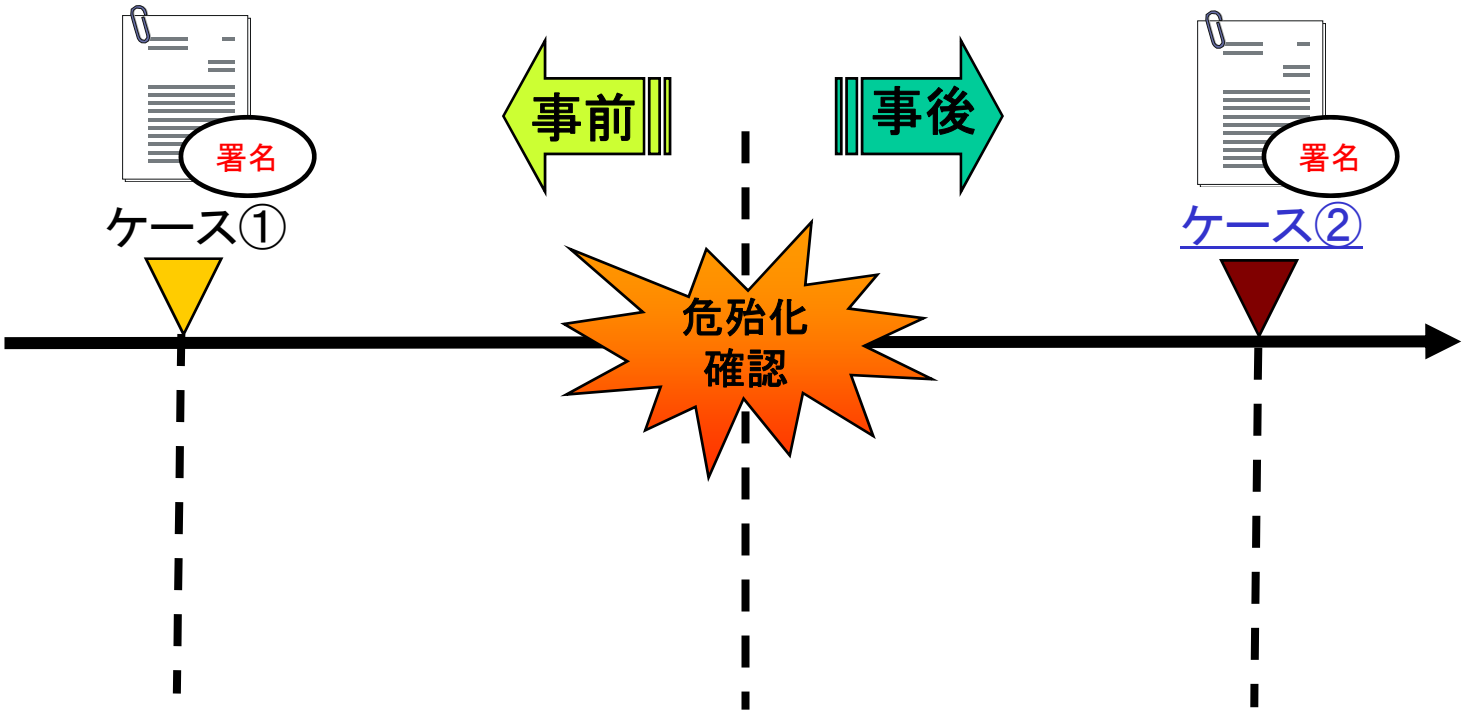
したがって、現在の使用法では既存署名付文書への対応はあまり考える必要がない。

長期利用文書への署名に利用する場合は、危殆化時にどう対応するかの合意（たとえば時刻認証局による追加署名の実施など）を利用者との間でとっておく必要がある。

背景

危殆化確認前から既に存在する
デジタル署名付文書

危殆化確認後に新しく生成される
デジタル署名付文書



- ケース②が本研究会の主要対象。
- ケース①についても検討必要。

新しく生成されるデジタル署名付文書への対応（ケース②：１）

１．移行後の暗号の最終決定。将来の変更を少なくするためRSA1024からRSA2048に行くのではなく、直接RSA3072にいくのも考えられる（次PPT参照）。しかし、ICカードなどの実装が追いつかない可能性もあり、RSA2048が現実的か。

2.　公的個人認証に関連して利用する自作の署名利用システムへの移行に関する現実的問題の解決。応用プログラムの変更に要するマンパワーは予想以上に多い可能性がある。2000年問題対応時のように変更必要部発見や半自動変更用のツールを共通で開発することも検討すべきではないか。

推奨暗号アルゴリズムと使用推奨期間

nビット 安全性	ブロック暗号	ハッシュ 関数	公開鍵暗号 （RSA）	使用推 奨期間
80ビット	2-Key TDES	SHA-1	RSA1024	-2010年
112ビット	3-Key TDES	SHA-224	RSA2048	-2030年
128ビット	AES-128	SHA-256	RSA3072	-2030 超年

山岸篤弘「暗号の世代交代」IPA Forum2008　p21より作成[6]

新しく生成されるデジタル署名付文書への対応（ケース②：2）

３．上記2に接続されたPC内市販ソフトや、関連サーバへの対応

（１）新しいものに対応できるようソフトの開発会社やサーバ運用者に働きかけが必要。

（２）これらの新しいものへの対応が遅れる場合でどうしても使わざるを得ないシステムなら、複数のアルゴリズムに同時に対応できるような機能を自作の署名利用システムに入れる必要がある。この場合にもセキュリティホールの作りこみに注意する必要がある。

新しく生成されるデジタル署名付文書への対応（ケース②：３）

４．暗号アルゴリズムの危殆化に備えた体制整備
　特に、省庁横断組織と事後対応を行う各システムの対応チームの編成法の検討。
５．個別のシステムやトータルシステムとしてのテストの実施。
６．暗号の危殆化時の民間での対応方法に関するガイドの作成。
７．暗号の危殆化に際して訴訟になった場合に備えての法的問題点の検討。

さらに将来的な課題

1．危殆化の検知から対応まで時間がない場合や、危殆化発生後に危殆化を検知するなど危機管理型対応が必要な暗号危殆化発見パターンへの対策

　過去の検討結果を次pptに示す。
　当時はハッシュ関数の危殆化をあまり考えていないのでさらに検討が必要

2．暗号の危殆化に伴う種々のコンテンジェンシー対策、BCP対策の立案　（検討委託が必要ではないか）

暗号危殆化をめぐる国内外の状況[5)]
～研究開発の状況～ ＜三菱総研作成＞

大分類	分類	詳細	技術名称等
安全性確保型	計算能力対応型	計算機能力が向上しても、安全性を確保可能な暗号技術を構成する。	Unconditional Secure署名 量子公開鍵暗号
	脆弱性補完型	解読技術等に対応するために、既知の攻撃への耐性を持たせるような暗号技術を構成する。	暗号設計技術 解読技術
証拠性確保型	偽造判定型	電子署名等のデータに何らかの情報を織り込んでおいて、偽造等を判別可能とする方法。暗号が危殆化しても、偽造された署名であるか等判定可能であるので、ある一定の証拠性を確保できる。	タイムスタンプ(ETSI TS 101 155） Forward Secure署名 Key Insulated 署名 Intrusion Resilient 署名 電子署名アリバイ実現機構[4)] ハードウェア確認タグ付署名 Fail Stop 署名
	データ保管型	暗号が危殆化したときのために、電子文書データ等を安全に保管しておく技術。危殆化後に保管されているデータを証拠として利用する。	セキュア・アーカイバ 電子公証

参考文献

1)藤本肇，上田祐輔，佐々木良一「デジタル署名付き文書への公開鍵暗号危殆化対策の組合せ最適化法の提案と一適用」 情報処理学会論文誌、第49巻第3号、pp1105-1118 （平成20年）

2）西本敬志、佐々木良一「暗号危殆化に対する長期署名フォーマットの安全性評価」情報処理学会、CSS2008

3）佐々木良一、上田　祐輔「デジタル署名付文書の長期的利用を可能にする方式の提案」電子情報通信学会、SITE研究会2004年1月

4）上田　祐輔、佐々木良一、吉浦　　裕、洲崎　誠一、宮崎　邦彦「データ喪失を想定したヒストリシス署名方式評価手法の提案」情報処理学会論文誌第45第8号、pp1966-1976

5）三菱総合研究所「暗号の危殆化に関する調査」情報処理振興機構、2005年4（http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/index.html）