PKI技術と私

東京電機大学未来科学部教授
佐々木良一

目次

1．印鑑と電子印鑑（電子署名）の歴史
2．PKI技術と私のかかわり
3．公開鍵暗号の危殆化とPKI
4．PKIの今後
5．さらに知りたい人のために

Information Security Laboratory

ISL

1．印鑑と電子印鑑（電子署名）の歴史

印鑑と電子印鑑（電子署名）の歴史

印鑑	年代	3000BC　2000BC　1000BC　紀元　1000AD　2000AD
	外国の出来事	△シュメール人が円筒印章使用（5300年前） （△シュメール人が古拙文字使用） △粘土版の契約書に捺印　△中国で印章使用 △印章から署名へ △中国で紙に朱泥捺印
	日本の出来事	△金印拝受△私印の普及 △官印の使用
電子印鑑	年代	1975年　1980年　1985年　1990年　1995年　2000年
	外国の出来事	△Hellmanら概念提案（1976年） △Rivestら具体的方式を提案（1978年） △ＰＧＰで利用 △SSL/SETでの利用
	日本の出来事	△双方向捺印実験 △GroupMaxで利用

世界最初の印鑑（はんこ）

○特定の財貨を入れた荷物を縄で縛り、その結び目を粘土隗で覆って、その上に円筒印章を押しつけた。　－＞　封印（鍵の代わり）

円筒印章

円筒印章を回転させながら粘土に押しつけたもの

メソポタミアの印章（レプリカ：佐々木良一所蔵）

外国における印章の歴史

○エジプトのスカラベ型印章：(4400年前)
○ヒッタイトのスタンプ型印章 (3500年前)
○古代ローマの指輪型印章 (2500年前)

エジプトのスカラベ型印章

○中国の印鑑の出現は比較的遅く周王朝後期の戦国時代 (約2500年前)
○紙は紀元１０５年に蔡倫が発明し、5世紀には広く使用
○6世紀はじめに朱泥を使い紙に印影を押すようになる。

日本における印章の歴史

○日本で記録に残っている最初のハンコは金印。

○奈良時代より官印として広く使われ始める。

○鎌倉時代から私印の習慣が広がり、武田信玄、上杉謙信ら戦国武将も印章を利用。江戸時代も同様。一般にも使われる様に成る

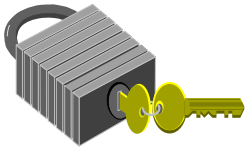
武田信玄の印章

印鑑と電子印鑑（デジタル署名）の歴史

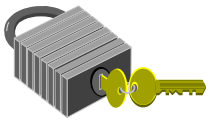
印鑑	年代	3000BC　2000BC　1000BC　紀元　1000AD　2000AD
	外国の出来事	△シュメール人が円筒印章使用（5300年前） （△シュメール人が古拙文字使用） △粘土版の契約書に捺印　△中国で印章使用 △印章から署名へ △中国で紙に朱泥捺印
	日本の出来事	△金印拝受△私印の普及 △官印の使用
電子印鑑	年代	1975年　1980年　1985年　1990年　1995年　2000年
	外国の出来事	△Hellmanら概念提案（1976年） △Rivestら具体的方式を提案（1978年） △ＰＧＰで利用△SSL/SETでの利用
	日本の出来事	△双方向捺印実験 △GroupMaxで利用

デジタル署名の歴史（1）

（1）公開鍵暗号と電子印鑑の概念を1976年、当時StanfordにいたDeffieeとＨｅｌｌｍａｎがＩＥＥＥ Tran. Information Theoryに発表（Invited Paper）。
（2）MerkleとHellmanが1978年にナップサック暗号方式を提案。ー＞1982年にShamirによってブレイク
（3）当時MITにいたR: Rivest、S: Shamir、A: Aleman １９７８年にＲＳＡ暗号を開発し発表（ACM）。
デジタル署名を重要な課題として意識。



電子印鑑の歴史（2）



（1）その後、公開鍵暗号方式として、ラビン暗号、エルガマル暗号、楕円曲線暗号などが開発され、電子印鑑に使用。

（2）電子印鑑専用の方式としてDSAやESIGNも開発された。

（3）捺印方式として、多重捺印、電子仮捺印、閾値捺印、ブラインド捺印、否認不可捺印などが提案された。

（4）1983年オランダのChaumによって提案されたブラインド捺印は電子投票や電子マネーにおいて匿名性の確保が可能になった。

2000年間で最大の発明

「この2000年間で最大の発明は何か？」

印刷機、コンピュータなどを上げる人が多いが

「それは**公開鍵暗号**である。」
チャールズサイモン (マイクロソフト)

出典：ジョン・ブロックマン編 (高橋健次訳)「2000年間で最大の発明は何か」草思社、2000

誰が公開鍵暗号の発明者か

(1) DiffieとHellman説
　　1976年。ただし具体的な方式未提案
(2) R: Rivest、S: Shamir、A: Adleman 説
　　1978年。広く使われている。
(3) 諜報機関事前開発説
　(a) 英国CESG#説
　　1970年　J.Ellisが概念を1973年にC.CocksがRSAに似た方式を開発していたと主張。
　(b) 米国NSA*説
　　1960年代に既に開発していたと主張。

⟶ いずれにしてもデジタル署名の発明者はDiffieとHellman

British Communications - Electronics Security Group
* National Security Agency

電子印鑑の長所

(1) 離れたところで印影付きの文書の作成が可能：ネットワークを経由して電子的な商取引が可能である。

(2) 捺印後の文書の改ざんが困難：ハッシュ値を用いることにより、文書の追加や改ざんが容易に検知できる。一方、紙の世界では、文字を追加しても気がつかない場合がある。

(3) 電子印鑑はデジタルデータなので物理的な表現形態を選ばない：いかなる表現形態の電子文書にも添付することができ、文書と印影のデータを紙に印字することもできる。

電子印鑑の短所（1）

（1）証拠能力の持続に関する信頼性：紙の世界では、50年以上にわたり、多くの印影付きの文書が保管され、証拠として有効に機能してきた。電子印鑑は、50年以内に秘密鍵を入れたICカードが壊れたり、公開鍵暗号が破られたりする可能性が否定できない。

（2）印影付き書類全体のコピーと再使用の可能性：紙の世界では、印影付き文書全体をコピーしたものは証拠とならなかった。電子印鑑では、印影と文書を丸ごとコピーするとそれらは、証拠として機能してしまう。したがって、電子マネーや電子小切手に、電子印鑑を適用する際はこの問題の解決が必要である。

電子印鑑の短所（2）

（3）印鑑が盗まれた場合の検知：紙の世界では印鑑が盗まれれば、実際に印鑑がなくなっているのですぐに分かり、紛失などの対応により対策を講じることができた。これに対し、電子印鑑では秘密鍵がコピーされ盗まれてもすぐに検知できるとは限らず、対策が遅れ、被害が大きくなる可能性がある。

（4）実感の欠如：紙の世界の捺印は、取引き文書が読めれば、どんな取引きかが分かり、捺印したことも、自分の印鑑に対応し、文書に朱肉がつくことによって確認が容易である。一方、電子印鑑における捺印機構は、本人の意思どうりに動いているかどうか確認するのが困難である。

ー＞ヒューマンクリプト

印鑑登録・証明の世界の歴史

○印鑑の登録と証明ならびに無効化については、今から３７００年ほど前のハムラビ王治下のバビロニアですでに行われていたという。印章をなくした場合には、悪用を防ぐため紛失の事実が公告されるような仕組みになっていた。

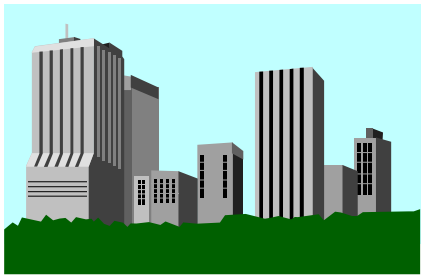
認証機関の歴史

○認証機関の機能については1980年ごろからMITなどで研究

○実際に広く使われ始めたのは商用インターネットが普及した1990年代中盤から

○日本で認証機関のサービスが開始されたのは1996年からで、日本ベリサイン(株)によるものが最初

(注) 認証機関：CA (Certification Authority)や認証局とも呼ばれる。



PKIとは

(1) 狭義のPKI：公開鍵暗号を利用した証明書の作成、管理、格納、配布、破棄のために必要なハードウエア、ソフトウエア、人，ポリシー、プロトコルによって提供される基盤のことである。(IETFでの定義)

(2) 広義のPKI：公開鍵暗号を利用した電子署名や電子認証のために必要なハードウエア、ソフトウエア、人，ポリシー、プロトコルによって提供される基盤のことである。

PKI：Public Key Infrastructure

電子認証基盤一覧

認証基盤	認証主体		認証対象		主な利用分野
政府認証基盤 GPKI	公的組織	府省庁	官職	府省庁の官職	政府文書の認証など
地方自治体認証基盤LGPKI		地方公共団体		地方公共団体の官職	自治体文書の認証など
公的個人認証		地方公共団体	民間	地方公共団体の住民	電子申請･届出など
商業登記認証基盤		法務局		会社･法人の代表者	電子申請･届出 電子商取引
民間特定認証業務	民間組織	民間企業		個人	電子申請･届出 電子商取引
民間一般認証業務		民間企業		個人･法人	電子商取引

佐藤純通氏CSM誌２００２年6月号記事を参考に作成

公的個人認証システム

地方公共団体がその住民の公開鍵の登録を証明するもの

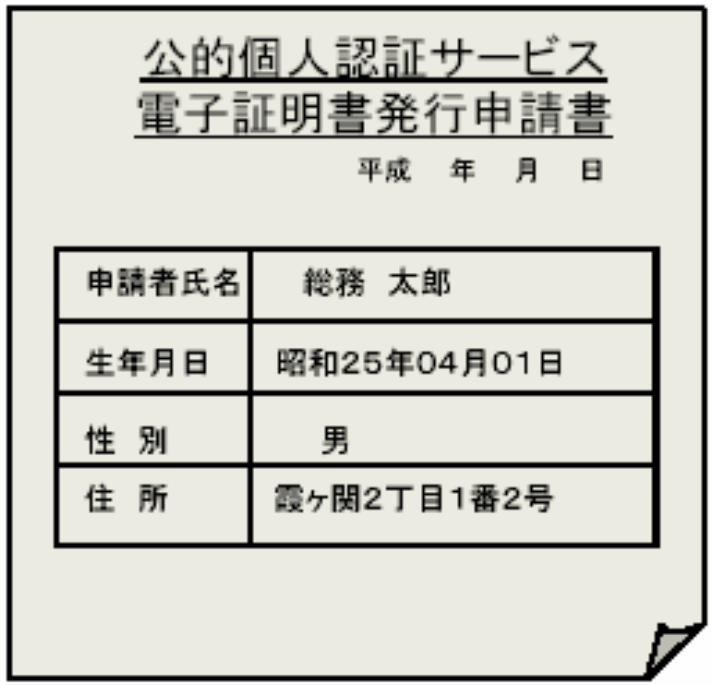
⇨ **印鑑登録証明に類似**

「電子署名に係る地方公共団体の認証業務に関する法律(公的個人認証法)」　－平成１４年１２月１３日　公布

岐阜県において公的個人認証の全国実証試験を実施(平成15年年12月まで)

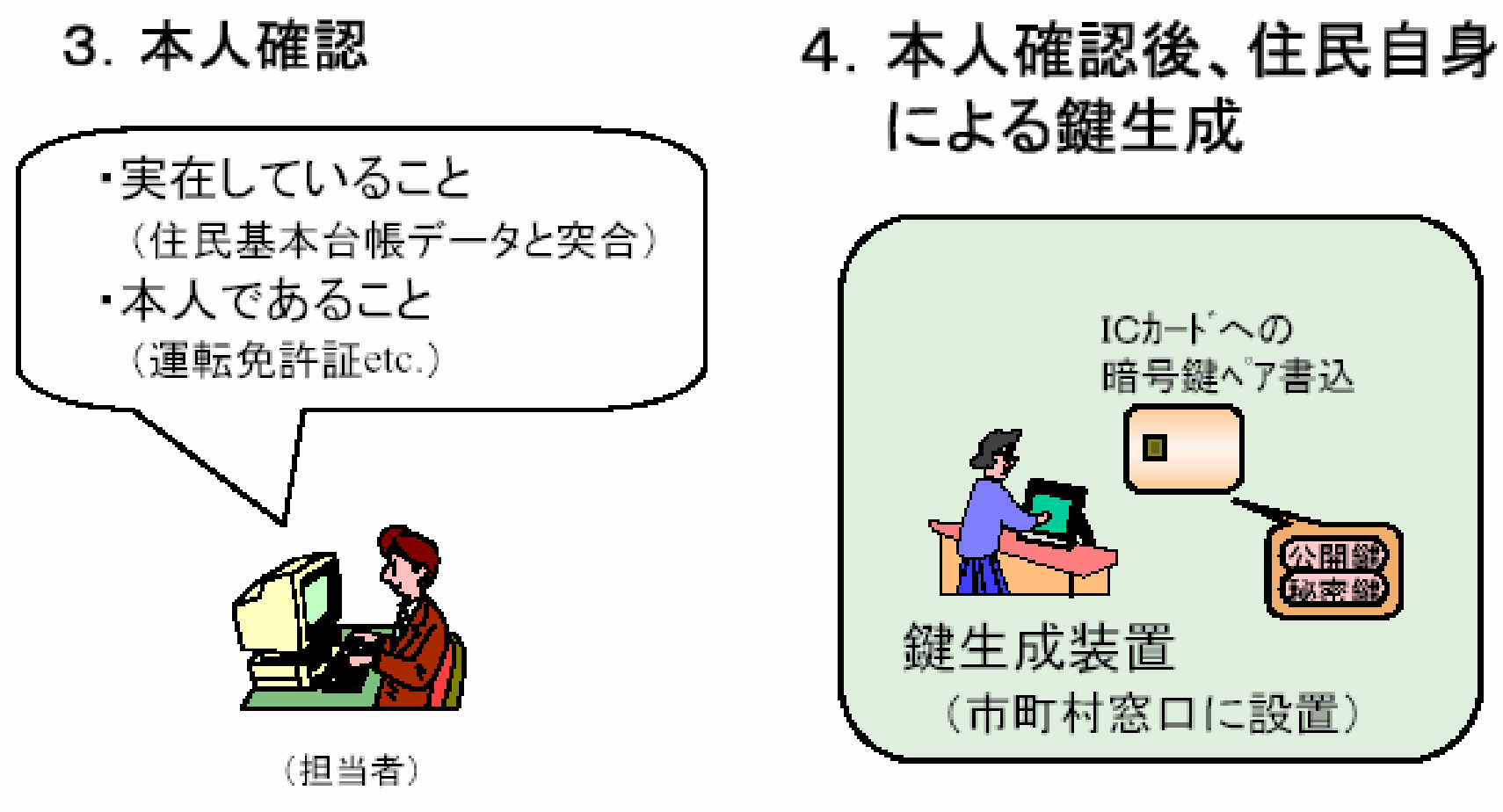
平成１６年２月２日より実運用：名古屋国税局管内（岐阜県、静岡県、愛知県及び三重県）の納税者の方を対象に、所得税及び個人事業者の消費税の申告について運用を開始

公的個人認証の証明書の発行のイメージ（1）



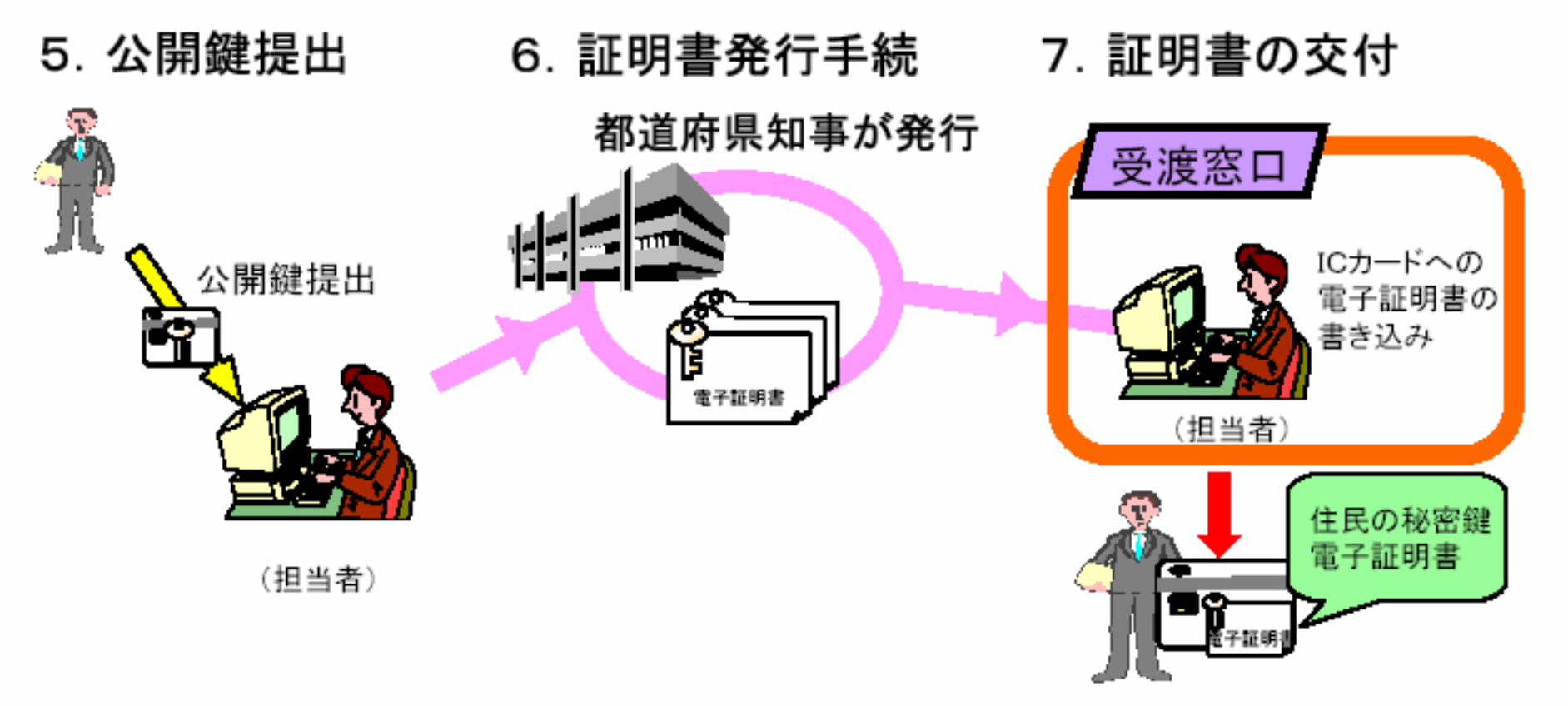
http://www.soumu.go.jp/c-gyousei/daityo/pdf/juki_yakuwari_02.pdf

公的個人認証の証明書の発行のイメージ（2）



http://www.soumu.go.jp/c-gyousei/daityo/pdf/juki_yakuwari_02.pdf

公的個人認証の証明書の発行のイメージ（3）



http://www.soumu.go.jp/c-gyousei/daityo/pdf/juki_yakuwari_02.pdf

e-Taxの運用スケジュール

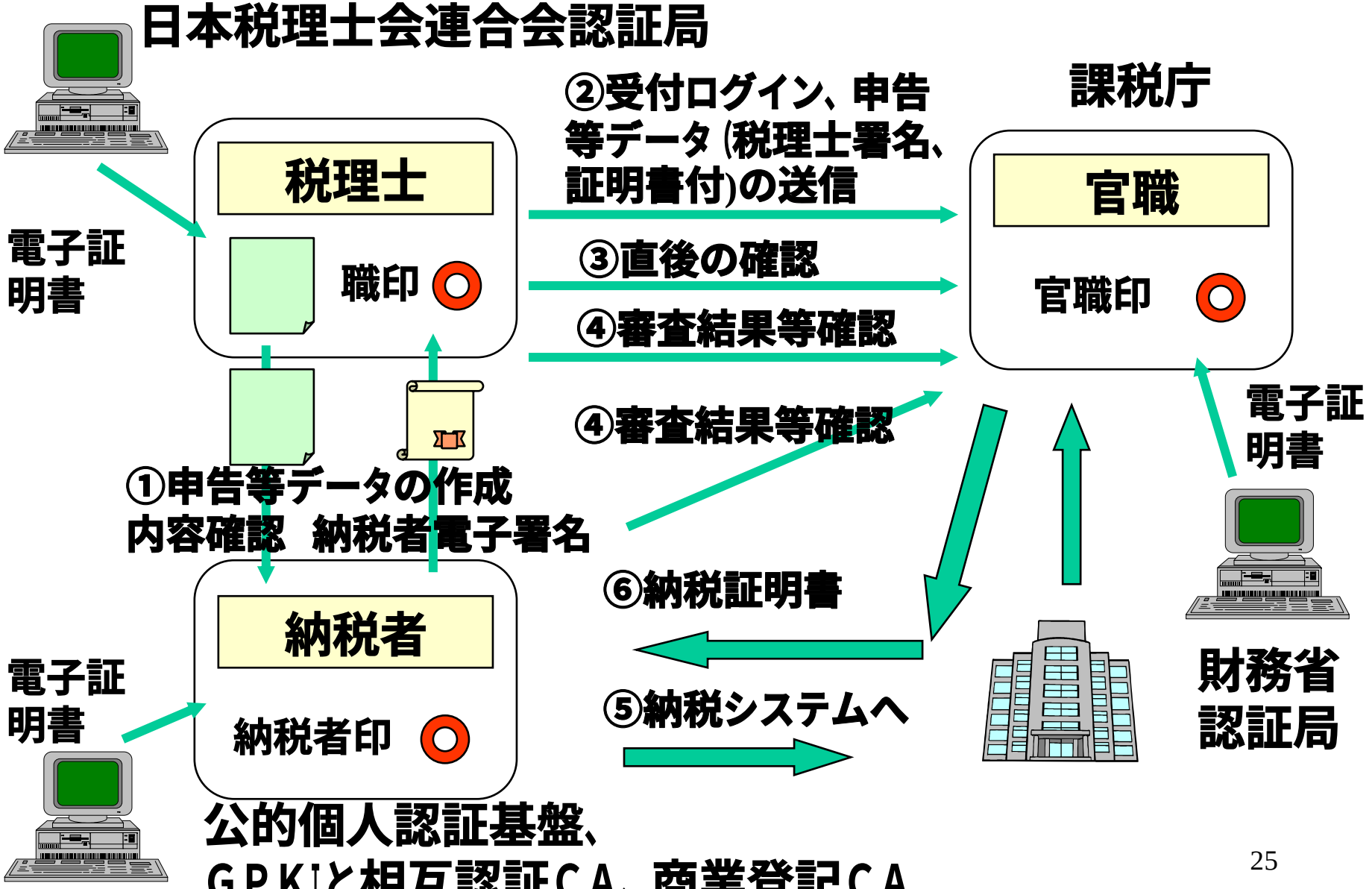
イ　平成16年2月2日
名古屋国税局管内（岐阜県、静岡県、愛知県及び三重県）の納税者の方を対象に、所得税及び個人事業者の消費税の申告について運用を開始

ロ　平成16年3月22日
名古屋国税局管内の納税者の方を対象に、上記のほか、法人税、法人の消費税の申告、全税目の納税及び申請・届出等の一部について運用を拡大

ハ　平成16年6月1日
全国（名古屋国税局管内以外の地域）の納税者の方を対象に、名古屋国税局管内で開始したすべての手続について運用を拡大

http://www.e-tax.nta.go.jp/gaiyou/gaiyou2.html

税理士と電子申告


日本税理士会連合会認証局
課税庁
税理士
職印
官職
官職印
電子証明書
②受付ログイン、申告等データ(税理士署名、証明書付)の送信
③直後の確認
④審査結果等確認
④審査結果等確認
電子証明書
①申告等データの作成
内容確認　納税者電子署名
⑥納税証明書
納税者
納税者印
電子証明書
⑤納税システムへ
財務省認証局
公的個人認証基盤、
ＧＰＫＩと相互認証ＣＡ、商業登記ＣＡ

納税も電子化時代　ｅ－Ｔａｘ利用１４倍

2007年5月29日8時0分配信 産経新聞

　平成１８年分の確定申告で、インターネットの「国税電子申告・納税システム（ｅ－Ｔａｘ）」を利用した所得税の申告件数が前年に比べ１４倍増えたことが、国税庁のまとめで分かった。

　全申告数に対する利用率は２・１％と依然低水準だが、同庁は「オンライン利用計画の目標をクリアした」として、さらに普及を図りたい考え。２２年分の申告で５０％の利用率を目指している。

　まとめによると、ｅ－Ｔａｘを利用した所得税の申告件数は約４９万件で、前年（3万５０００件）から約１４倍となった。個人事業者の消費税申告も約１０万件あり、対前年比で１０・５倍増。

http://headlines.yahoo.co.jp/hl?a=20070529-00000010-san-soci

Information Security Laboratory

ISL

2．PKI技術と私のかかわり

PKI関連技術と私（その1）

（1）1985年日立の宝木、佐々木らは2者間で安全な取引を可能とする電子仮捺印を利用した双方向電子捺印のプロトシステムを開発し、実験を実施。

（2）その際、RSAの高速化のため専用装置の開発も行い、５１２ビット鍵長の印影作成に０．１３秒を実現（当時PCでは5分以上かかっていた）。

PKI関連技術と私（その2）

1．1997年ドイツで行われたVIS’ 97（Reliable Information System Conference）で“Security Requirements and Countermeasures in Japan in the Electronic Commerce Era”, と題し、第二招待講演者として講演を行った。そのときの第一招待講演者がPGP開発者のTimmerman 。

2．1999-2000年に日本で最初の公的認証機関の開発に関与。

3．2001年ごろより暗号危殆化の署名つき文書への影響と対策の研究を実施。

（その他、インターネットマークス、ヒステリシス署名や墨塗り署名の研究も実施）

PKI関連技術と私（その2）

1．1997年ドイツで行われたVIS’ 97（Reliable Information System Conference）で“Security Requirements and Countermeasures in Japan in the Electronic Commerce Era”, と題し、第二招待講演者として講演を行った。そのときの第一招待講演者がPGP開発者のZimmermann 。

2．1999-2000年に日本で最初の公的認証機関の開発に関与。

3．2001年ごろより暗号危殆化の署名つき文書への影響と対策の研究を実施。

（その他、インターネットマークス、ヒステリシス署名や墨塗り署名の研究も実施）

インターネットマークの基本アイディア

基本アイデア：
　デジタル署名と電子透かしの融合

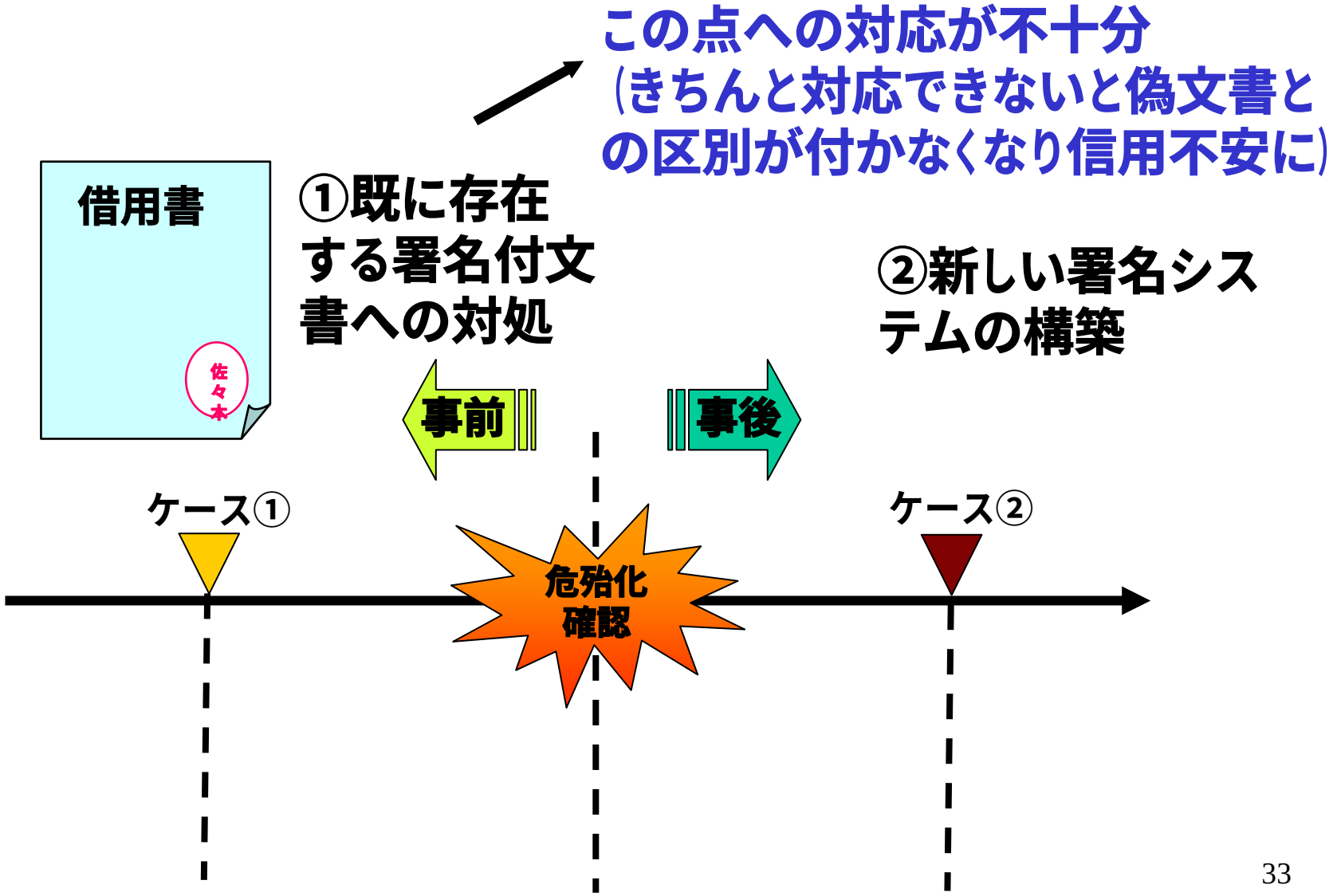
効果：以下の改ざん検知
　(1) ホームページの内容、
　(2) ウエブサイト（URL）、
　(3) マークそのもの
＜ブランド管理機能＞

Information Security Laboratory

ISL

3．公開鍵暗号の危殆化とPKI

対策の種類


この点への対応が不十分
（きちんと対応できないと偽文書との区別が付かなくなり信用不安に）
借用書
佐々木
①既に存在する署名付文書への対処
②新しい署名システムの構築
事前
事後
ケース①
危殆化確認
ケース②

想定される不正行為

(1) 偽のデジタル署名付き文書を本物だと主張

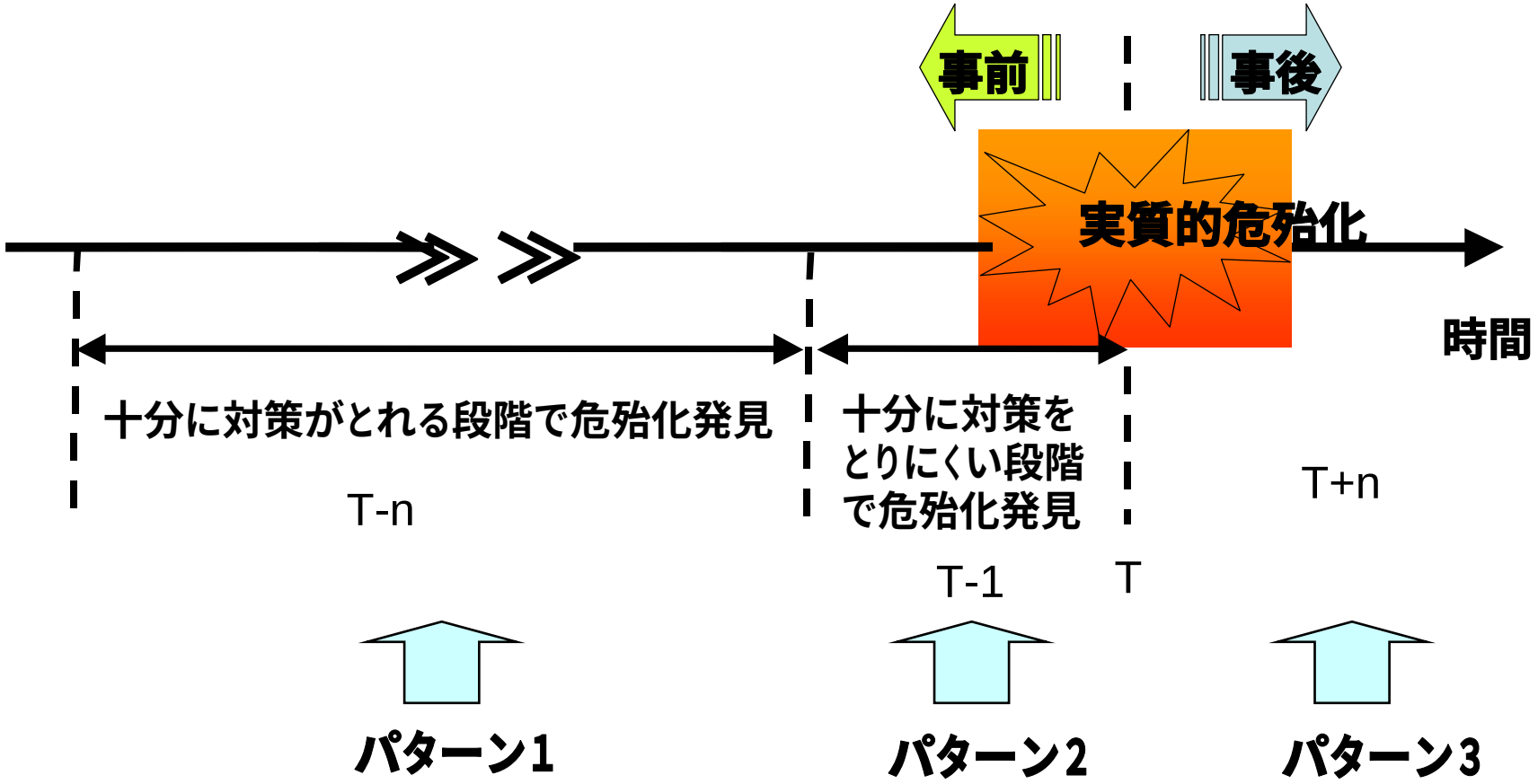
(2) 本物のデジタル署名付き文書であるのに、偽者だと主張

具体例

(1)「Aさんに1億円を貸している，借用証書がここにある」と主張する場合

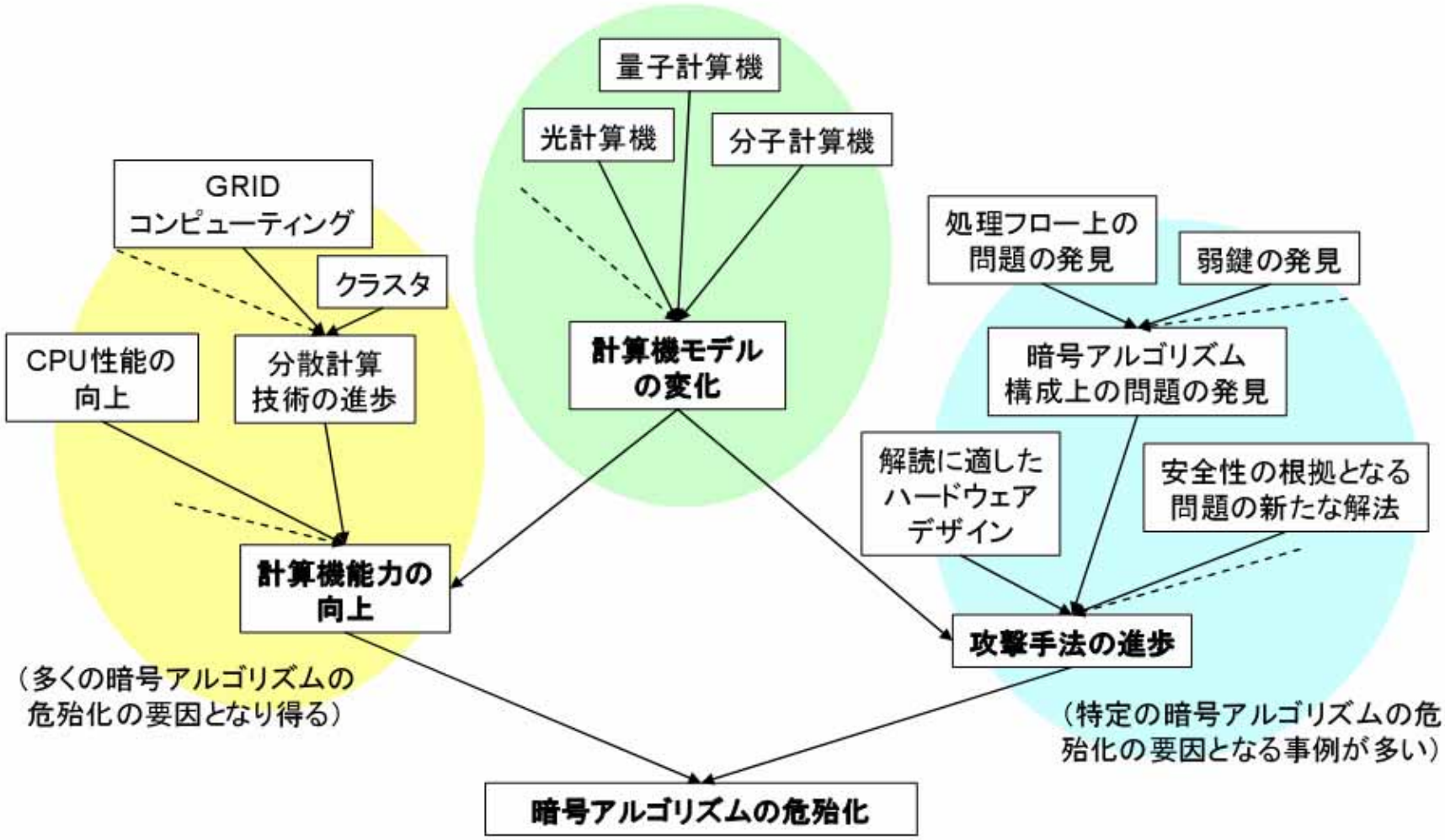
(2) 5億円借りたという借用書があるのに「それは偽者で，私は金を借りていない」と主張

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.

暗号危殆化の原因



（株式会社　三菱総合研究所作成）

対策のために必要な事項

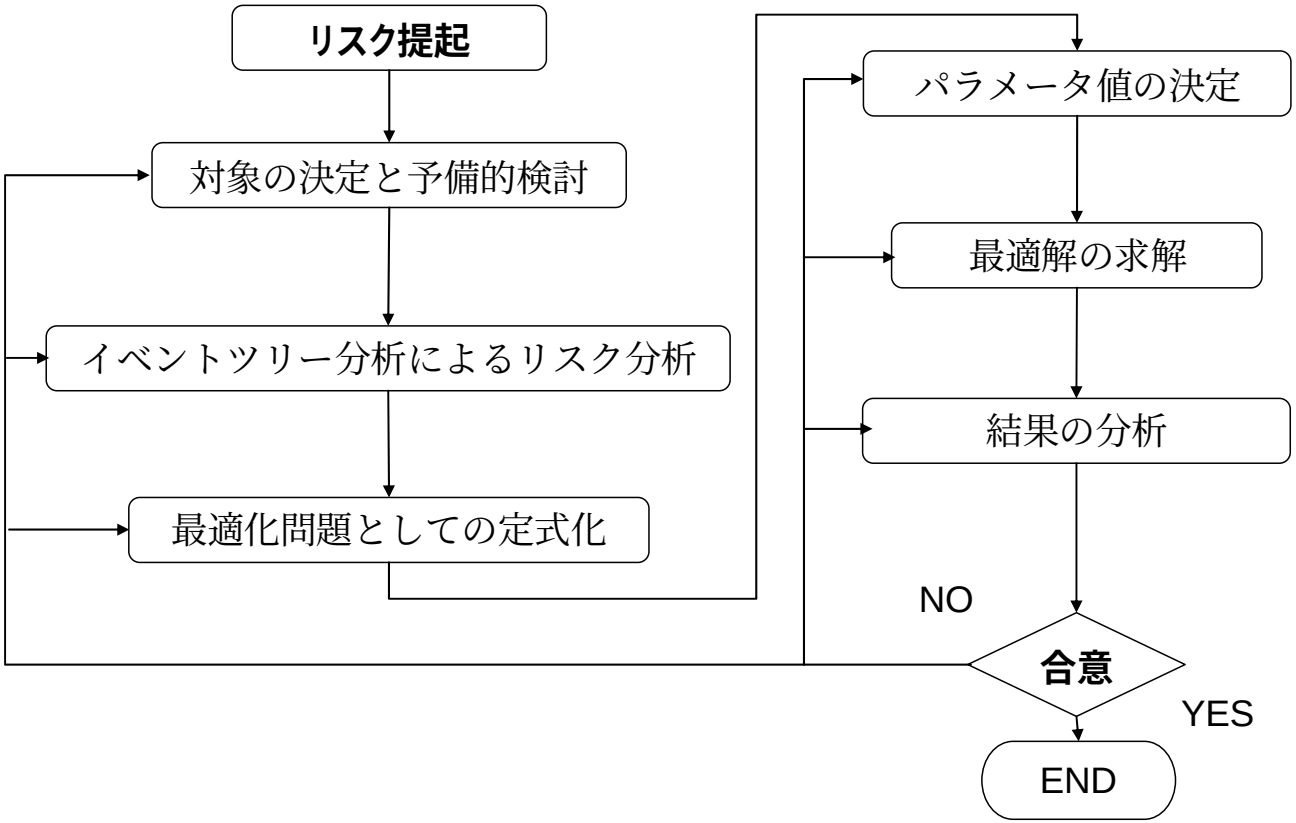
①暗号危殆化情報の確認

②暗号危殆化情報の伝達

③危殆化時対応ポリシー設定

④署名付文書への処置
　(1) 署名付文書の再作成
　(2) 署名付文書へのより強い暗号での第三者署名など

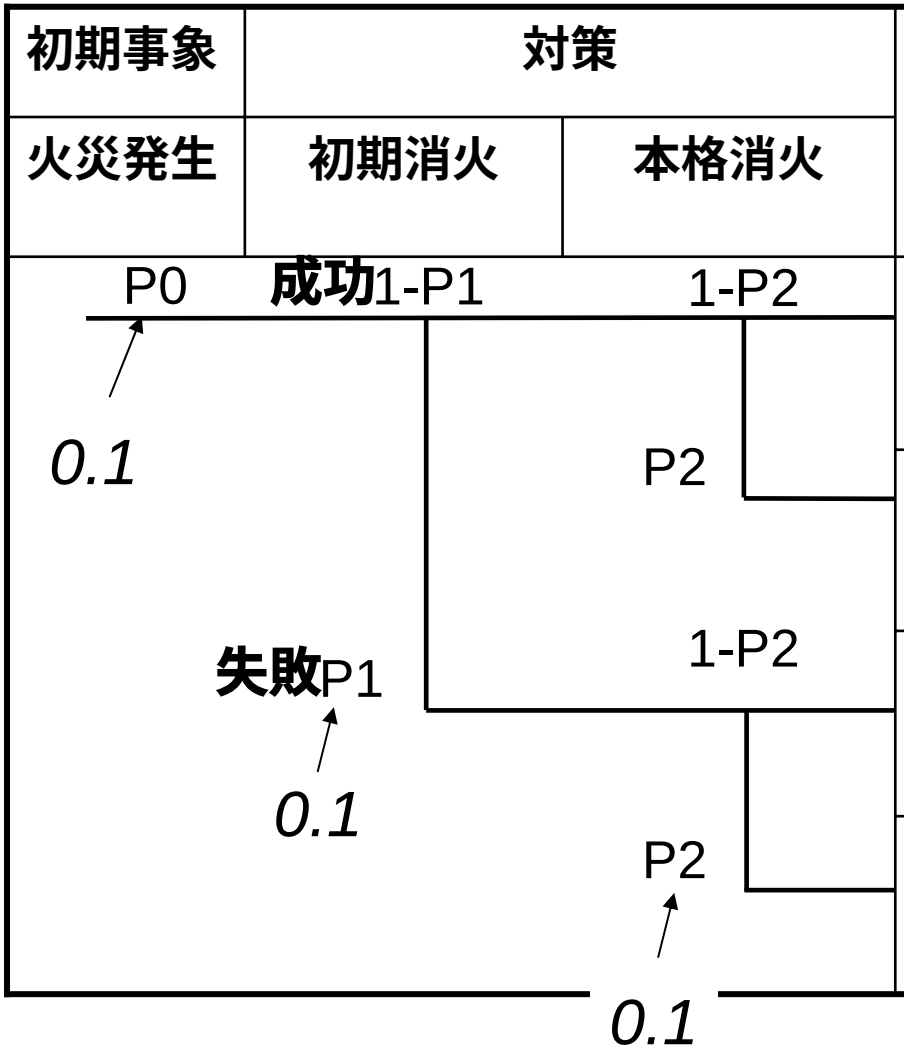
アプローチ方法


リスク提起
対象の決定と予備的検討
イベントツリー分析によるリスク分析
最適化問題としての定式化
パラメータ値の決定
最適解の求解
結果の分析
NO
合意
YES
END

本研究におけるリスク分析手法

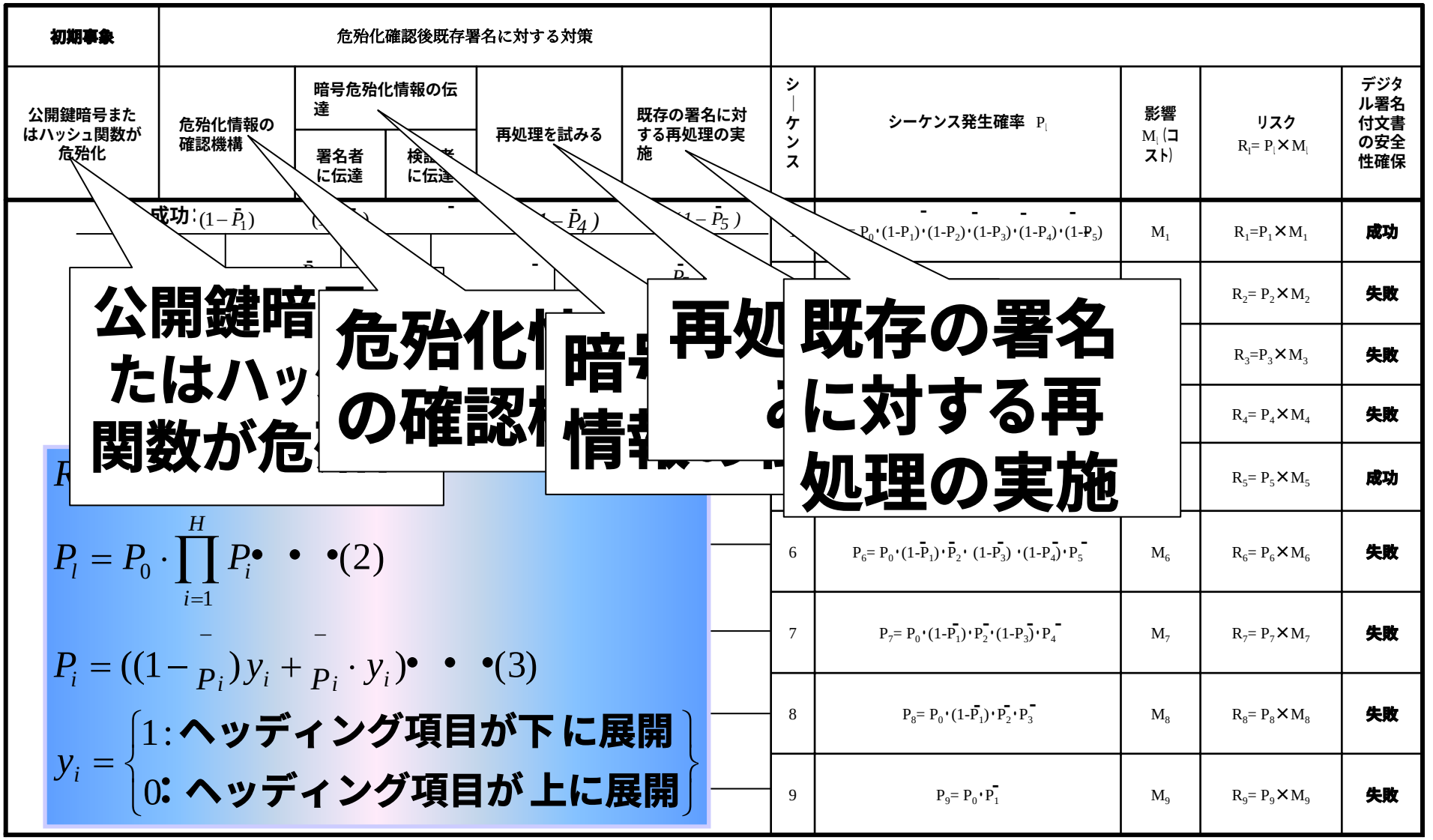
- **イベントツリー分析**（ETA）とは
  - 発端となる初期の事象からスタートして、これが最終的な事象に発展していく過程を、ツリー状 に展開して解析するもの

イベントツリー分析の例



発生確率 Pi	影響 Mi	リスク Rs	火災の被害規模
0.081	*500**万円***	*40**万** 5000**円***	**小**
0.009	*1500**万円***	*13**万** 5000**円***	**中**
0.009	*1500**万円***	*13**万** 5000**円***	**中**
0.001	*3000**万円***	*3**万円***	**大**

危殆化におけるイベントツリー



なぜETAなのか？

本リスク分析にETAを利用する理由

- ケース毎にどのような被害が起こるかが分かりやすい
- 対策方法の影響範囲が分かりやすい
- 各ケースの発生確率が算出可能

ETに適用する具体的対策案

対策案

1. 暗号危殆化情報の確認機構
(1-1)監視機関なし(X_{11})
(1-2)CRYPTRECによる監視(X_{12})
(1-3)CRYPTRECによる監視の強化(X_{13})

2. 暗号危殆化情報の伝達(署名者)
(2-1)伝達手段なし(X_{21})
(2-2)認証局による伝達(X_{22})
(2-3)伝達機関による伝達(X_{23})
(2-4)認証局と伝達機関による伝達(X_{24})

3. 暗号危殆化情報の伝達(検証者)
(3-1)伝達手段なし（X_{31}）
(3-2)認証局による伝達（X_{32}）
(3-3)伝達機関による伝達（X_{33}）
(3-4)認証局と伝達機関による伝達（X_{34}）

4. 再処理を試みる
(4-1)危殆化時対応ポリシーなし(X_{41})
(4-2)危殆化時対応ポリシーあり(X_{42})

5. 既存の署名に対する再処理
(5-1)対策なし(X_{51})
(5-2)デジタル署名による再処理(X_{52})
(5-3)第三者機関によるデジタル署名(X_{53})

1. 暗号危殆化情報の確認機構
(1-1)監視機関なし(X_{11})
(1-2)CRYPTRECによる監視(X_{12})

2. 暗号危殆化情報の伝達(署名者)
(2-1)伝達手段なし(X21)

3. 暗号危殆化情報の伝達(検証者)
(3-1)伝達手段なし(X31)

4. 再処理を試みる
(4-1)危殆化時対応ポリシーなし(X41)
(4-2)危殆化時対応ポリシーあり(X42)

5. 既存の署名に対する再処理
(5-1)対策なし(X51)
(5-2)デジタル署名による再処理(X52)
(5-3)第三者機関によるデジタル署名(X53)

具体的対策案の適用例

初期事象	危殆化確認後既存署名に対する対策								
公開鍵暗号またはハッシュ関数が危殆化	危殆化情報の確認機構	暗号危殆化情報の伝達		再処理を試みる	既存の署名に対する再処理の実施	シーケンス	シーケンス発生確率 P_i	影響 M_i (コスト)	リスク $R_i = P_i \times M_i$	デジタル署名付文書の安全性確保
		署名者に伝達	検証者に伝達							
P_0	成功:$(1-\bar{P}_1)$	$(1-\bar{P}_2)$	$(1-\bar{P}_3)$	$(1-\bar{P}_4)$	$(1-\bar{P}_5)$	1	$P_1 = P_0 \cdot (1-P_1) \cdot (1-P_2) \cdot (1-P_3) \cdot (1-P_4) \cdot (1-P_5)$	M_1	$R_1 = P_1 \times M_1$	成功
	失敗:$\bar{P}_1$	$\bar{P}_2$	$\bar{P}_3$	$\bar{P}_4$	$\bar{P}_5$	2	$P_2 = P_0 \cdot (1-P_1) \cdot (1-P_2) \cdot (1-P_3) \cdot (1-P_4) \cdot P_5$	M_2	$R_2 = P_2 \times M_2$	失敗
	p_{12}					3	$P_3 = P_0 \cdot (1-P_1) \cdot (1-P_2) \cdot (1-P_3) \cdot P_4$	M_3	$R_3 = P_3 \times M_3$	失敗
										失敗
										成功
										失敗
						7	$P_7 = P_0 \cdot (1-P_1) \cdot P_2 \cdot (1-P_3) \cdot P_4$	M_7	$R_7 = P_7 \times M_7$	失敗
						8	$P_8 = P_0 \cdot (1-P_1) \cdot P_2 \cdot P_3$	M_8	$R_8 = P_8 \times M_8$	失敗
						9	$P_9 = P_0 \cdot P_1$	M_9	$R_9 = P_9 \times M_9$	失敗

1. 暗号危殆化情報の確認機構

(1-1)監視機関なし (X11)

(1-2) CRYPTRECによる監視(X12)

(1-3)CRYPTRECによる監視の強化(X13)

$$\bar{P}_1 = p_{11} \cdot X_{11} + p_{12} \cdot X_{12} + p_{13} \cdot X_{13}$$

$$\bar{P}_1 = p_{11} \cdot 0 + p_{12} \cdot 1 + p_{13} \cdot 0$$

$$\bar{P}_1 = p_{12}$$

$$\bar{P}_i = \sum_{j=1}^{J_i} p_{ij} \cdot X_{ij} \quad \cdots (4)$$

$$\left(X_{ij} = 0,1 \quad \sum_{j=1}^{J_i} X_{ij} = 1 \quad (i = 1,2,\ldots,n) \right)$$

普及率を変化させた場合の最適化結果

対策方法	具体的対策案	0.001%	0.01%	0.1%	1%	10%	30%	50%
1.暗号危殆化情報の確認	(1-1)監視機関なし(X11)	○	○					
	(1-2)CRYPTRECによる監視(X12)			○				
	(1-3)CRYPTRECによる監視の強化(X13)				○	○	○	○
2.暗号危殆化情報の伝達(署名者)	(2-1)伝達手段なし(X21)	○	○	○	○	○	○	○
	(2-2)認証局による伝達(X22)							
	(2-3)伝達機関による伝達(X23)							
	(2-4)認証局と伝達機関による伝達(X24)							
3.暗号危殆化情報の伝達(検証者)	(3-1)伝達手段なし(X31)	○	○					
	(3-2)認証局による伝達(X32)							
	(3-3)伝達機関による伝達(X33)			○	○	○	○	○
	(3-4)認証局と伝達機関による伝達(X34)							
4.再処理を試みる	(4-1)危殆化時対応ポリシーなし(X41)	○	○					
	(4-2)危殆化時対応ポリシーあり(X42)			○	○	○	○	○
5.既存の署名に対する再処理	(5-1)対策なし(X51)							
	(5-2)デジタル署名による再処理(X52)							
	(5-3)第三者機関によるデジタル署名(X53)	○	○	○	○	○	○	○
トータルコスト		24525312.480000004円	245253124.8円	1804774226.0800002円	13347616090.400002円	12843616090.400002円	384188482712円	639940804520円
損害コスト		24520590.480000004円	245205904.8円	1283829826.0800002円	12778172090.400002円	12778172090.400002円	383345162712円	638908604520円

最適解の求解 (基本ケース)

各関与者の制約条件を上限値まで設定したときのトータルコストが最小となるような対策案の組合せ

(1-3) CRYPTRECによる監視の強化
(2-1) 署名者に対する特別な伝達手段なし
(3-3)　検証者に対する伝達機関による伝達
(4-2) 危殆化時対応ポリシーあり
(5-3) 第三者機関による再処理

トータルコスト:13,347,616,090円
損害コスト:12,778,172,090円

必要な対策

(1) CRYPTRECを今後，より強化することが望ましい．

(2) 危殆化時対応ポリシーを早急に策定し，それに沿って対応することを強制できるよう制度化する必要がある．

(3) 危殆化情報を，証明付き文書を扱う人たちに，危殆化に関する情報を，認証局経由ではなく，広く確実に伝達する仕組みが必要である．

(4) デジタル署名の再処理については、文書再作成形よりも、既存文書への第三者署名が望ましいが、この仕組みを今から検討しておく必要がある．

Information Security Laboratory

ISL

4．PKIの今後

デジタル署名はどうなるか

ネットワークを経由してやり取りする文書に対し、本人性と非改ざん性 (完全性)を確認する機能を持つのは公開鍵暗号をベースとするデジタル署名だけ

本人性や非改ざん性を強く要求されるなら生き残るのはデジタル署名しかない!!

セキュリティやプライバシーに関する要求が下がることはない

時代は動くべき方向に動く

デジタル署名やPKIは社会基盤として今後ますます重要になる

参考文献(1)

1) 土居範久監修、佐々木良一代表編者「情報セキュリティ事典」共立出版、2003

2) 佐々木良一、宝木一夫「印鑑と電子印鑑の歴史と類似性の分析」情報処理学会論文誌第42巻8号、2001年8月

3)塚田孝則「企業システムのためのPKI」日経BP、2001年

4)Carlisle Adams, Steve Lloyd “ Understanding Public Key Infrastructure Concepts, Standards, and Deployment Considerations “, Macmillan Technical Publishing, 1999

参考文献(2)

1) 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月 (http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/)

2) 松本勉、岩下直行、「デジタル署名の長期的利用とその安全性について」日本銀行金融研究所、Discussion Paper No.2003-J-4、2003年3月31日

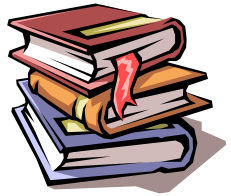
3) 宇根正志「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」日本銀行金融研究所、Discussion Paper No.2002-J-32、2002年

4) 松本勉、岩村充、佐々木良一、松木武、「暗号ブレイク対応電子署名アリバイ実現機構(その1)ーコンセプトと概要」情報処理学会研究報告 2000-CSEC-8、情報処理学会、2000年3月、pp13ー17

5) 米倉早織「電子署名文書長期保存の要件」ビジネスショウ2002 2002年5月22日、http://www.ecom.or.jp/ecit/tenji/bs2001/yonekura.pdf

6) 宇根 正志、田村 裕子、岩下 直行、松本 勉、松浦 幹太、佐々木良一「公開鍵証明書・失効情報欠損時におけるETSI TS 101 733に基づく署名の検証可能性」CSS2004

参考文献(3)



7) 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

8) 宮崎邦彦、吉浦裕、岩村充、松本勉、佐々木良一「連鎖構造を用いた電子署名技術における信頼性評価方法の提案」電子情報通信学会技術報告、Vol. 102, No. 212, 電子情報通信学会、2002年7月、pp109－115

9) 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

10) 佐々木良一、宝木一夫「印鑑と電子印鑑の歴史と類似性の分析」情報処理学会論文誌第42巻8号、2001年8月

11)藤本肇, 上田祐輔, 佐々木良一「公開鍵暗号危殆化のデジタル署名付き文書への影響分析と対策案の提案」CSS2006，2006.11