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

東京電機大学
西本　敬志

目次

- 背景
- 関連研究
- 長期署名フォーマットについて
- 研究目的
- 評価方法
- 評価

「暗号の2010年問題」

- デファクトスタンダード暗号技術の大移行
  - 米国立標準技術研究所 (NIST) が2010年末までに米国政府標準暗号の内の80bit安全性の暗号技術の運用を終了し，112bit安全性以上の暗号技術へ移行させる方針を発表
  - 内閣官房情報セキュリティセンター (NISC) でも日本政府の情報システムを2013年までにより安全な暗号技術へ対応させるという指針を打ち出している

現在の利用されている暗号アルゴリズムの危殆化の危険性が見過ごせない

背景(1/2)

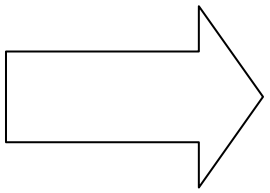
- デジタル署名はインターネット社会の基盤技術
  - 電子政府システム
    - 電子申請･届出
    - 電子決済
    - 情報公開

    etc...
  - 電子商取引システム
    - 電子契約
    - 電子帳票

    etc...

前提：公開鍵暗号やハッシュ関数が安全である

- CPU性能の向上
- 暗号アルゴリズムの欠陥
- 量子計算機の開発



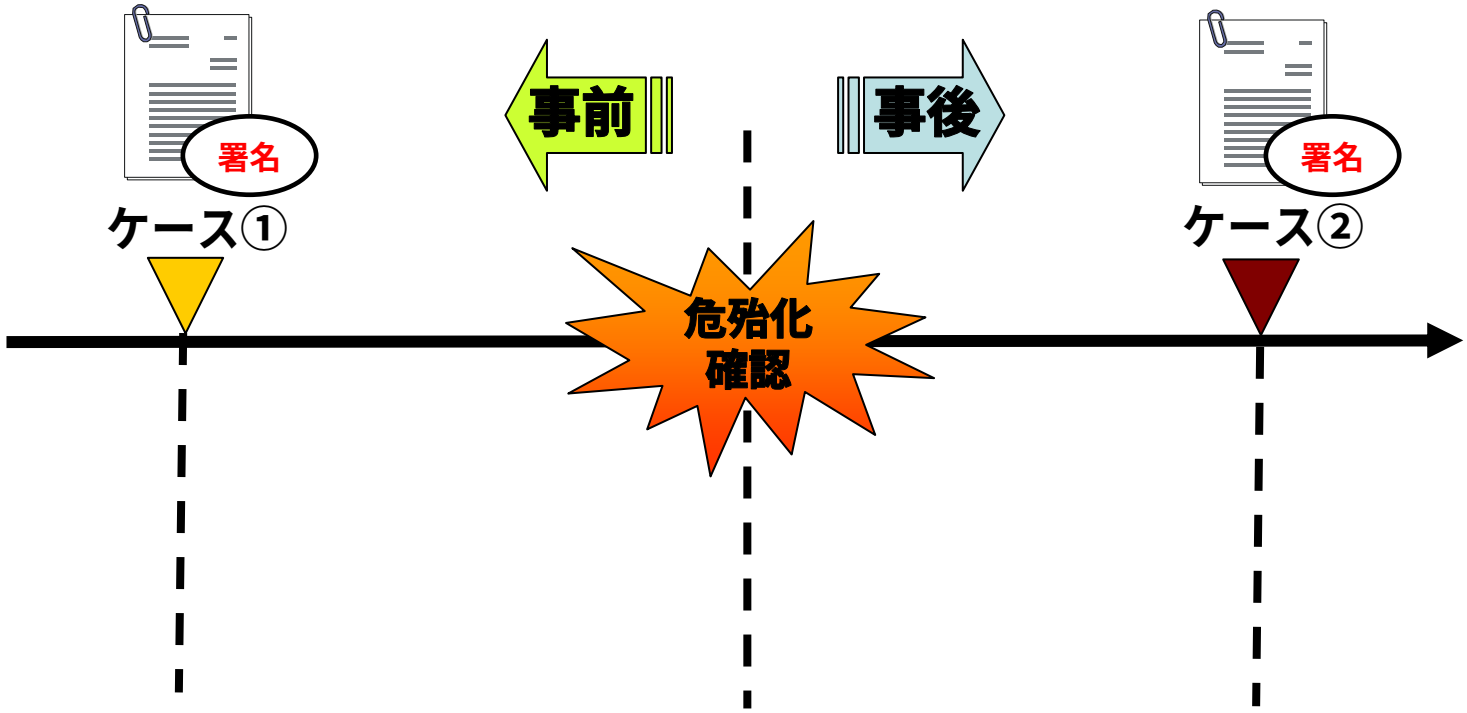
デジタル署名の
偽造･改ざん

公開鍵暗号･ハッシュ関数の危殆化

背景(2/2)

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た
デジタル署名付文書

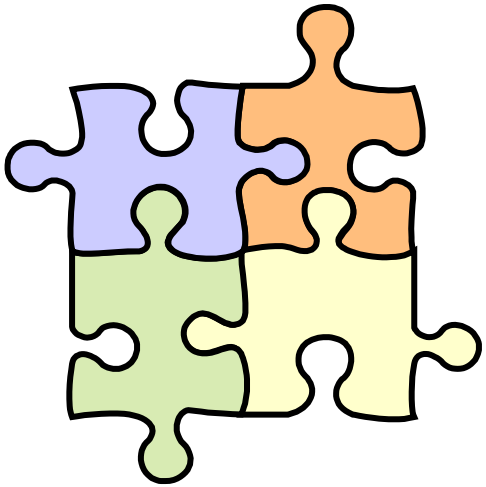


出典：藤本　肇「デジタル署名付き文書への公開鍵暗号危殆化対策の組合せ最適化法の提案と一適用」

- ケース②についての対策は色々検討されている
- ケース①についての対策の検討は不十分

関連研究

- 「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」　藤本　肇
  - 公開鍵暗号危殆化時の
    - 既存のデジタル署名付き文書のリスク分析
    - 最適な具体的対策案の組み合わせの算出



長期署名フォーマットについて(1/3)

- 暗号アルゴリズムを破られる危険性
- 公開鍵証明書の有効期限
- 公開鍵証明書の失効

デジタル署名の有効期限を長期間維持できない

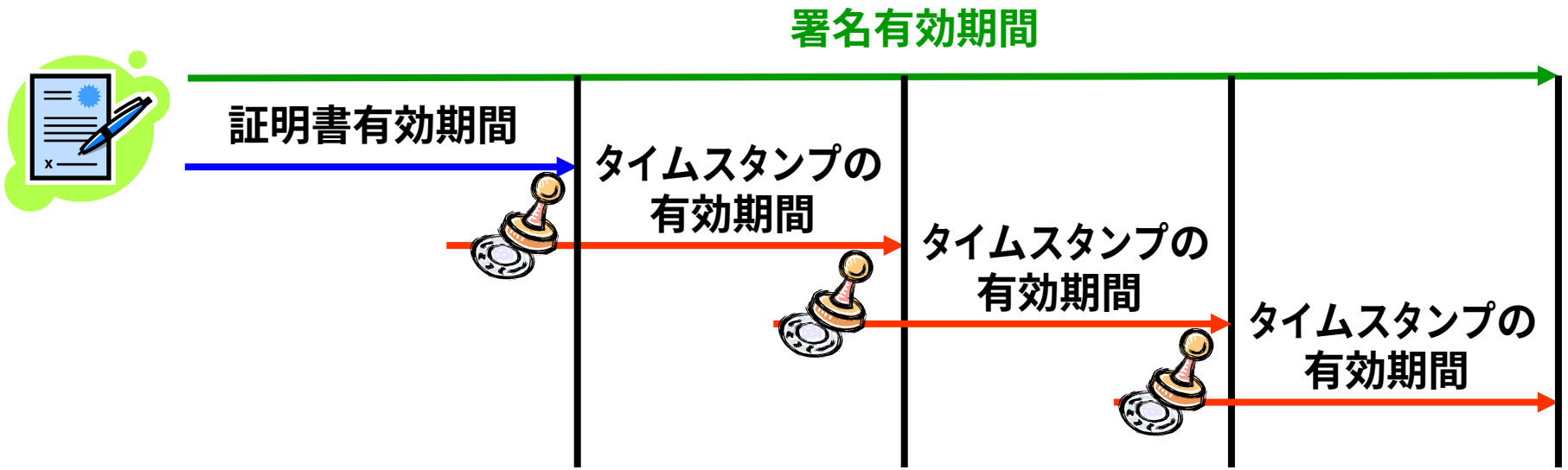
デジタル署名の長期保存技術

- **電子公証**
  - DVCS
  - LTA

  etc...
- **長期署名フォーマット**
  - CAdES
  - XAdES

長期署名フォーマットについて(2/3)

- 長期署名フォーマットの基本的な仕組み
  - 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



長期署名フォーマットについて(3/3)

- **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

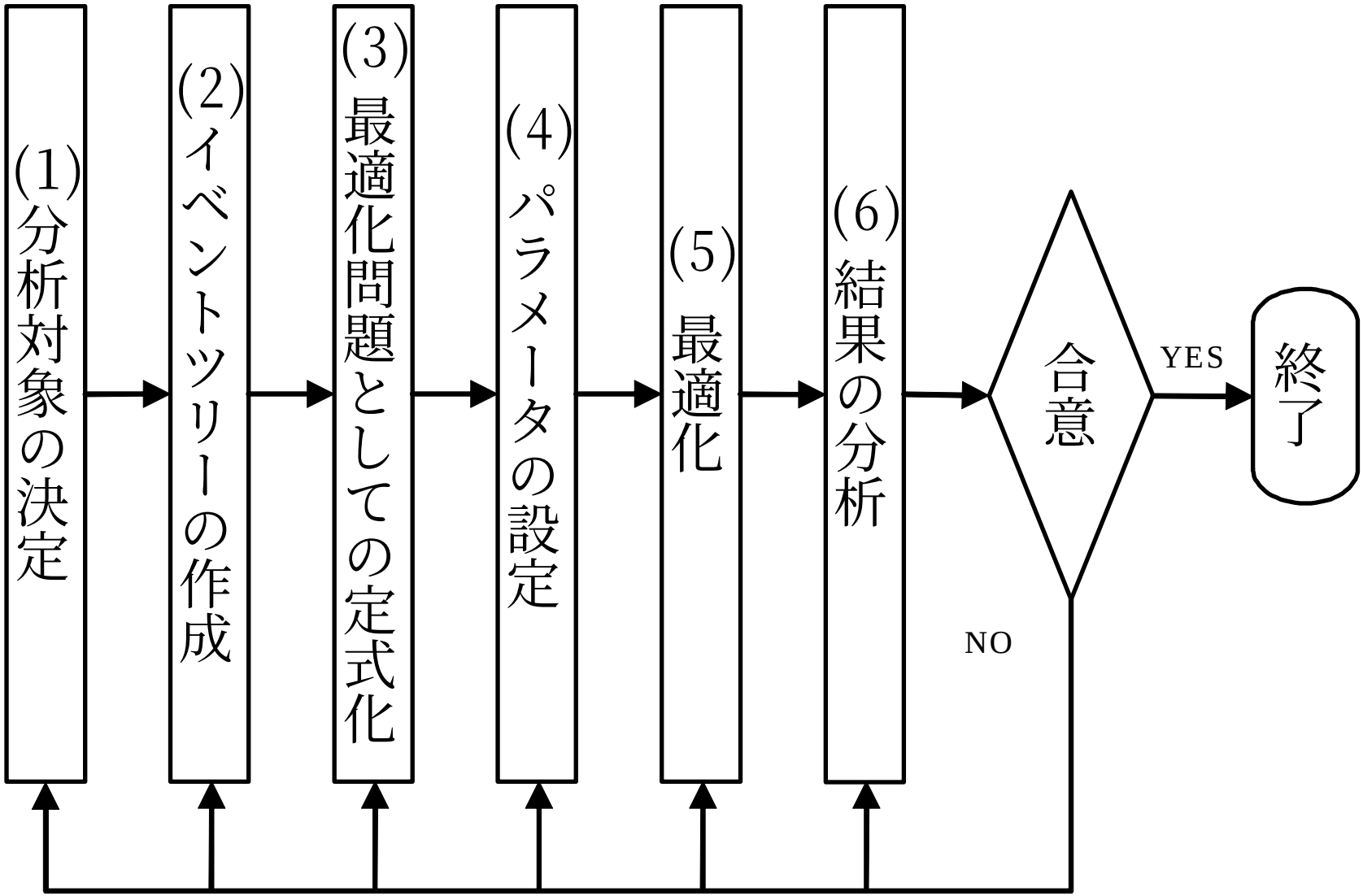
  などで標準化

- **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**)

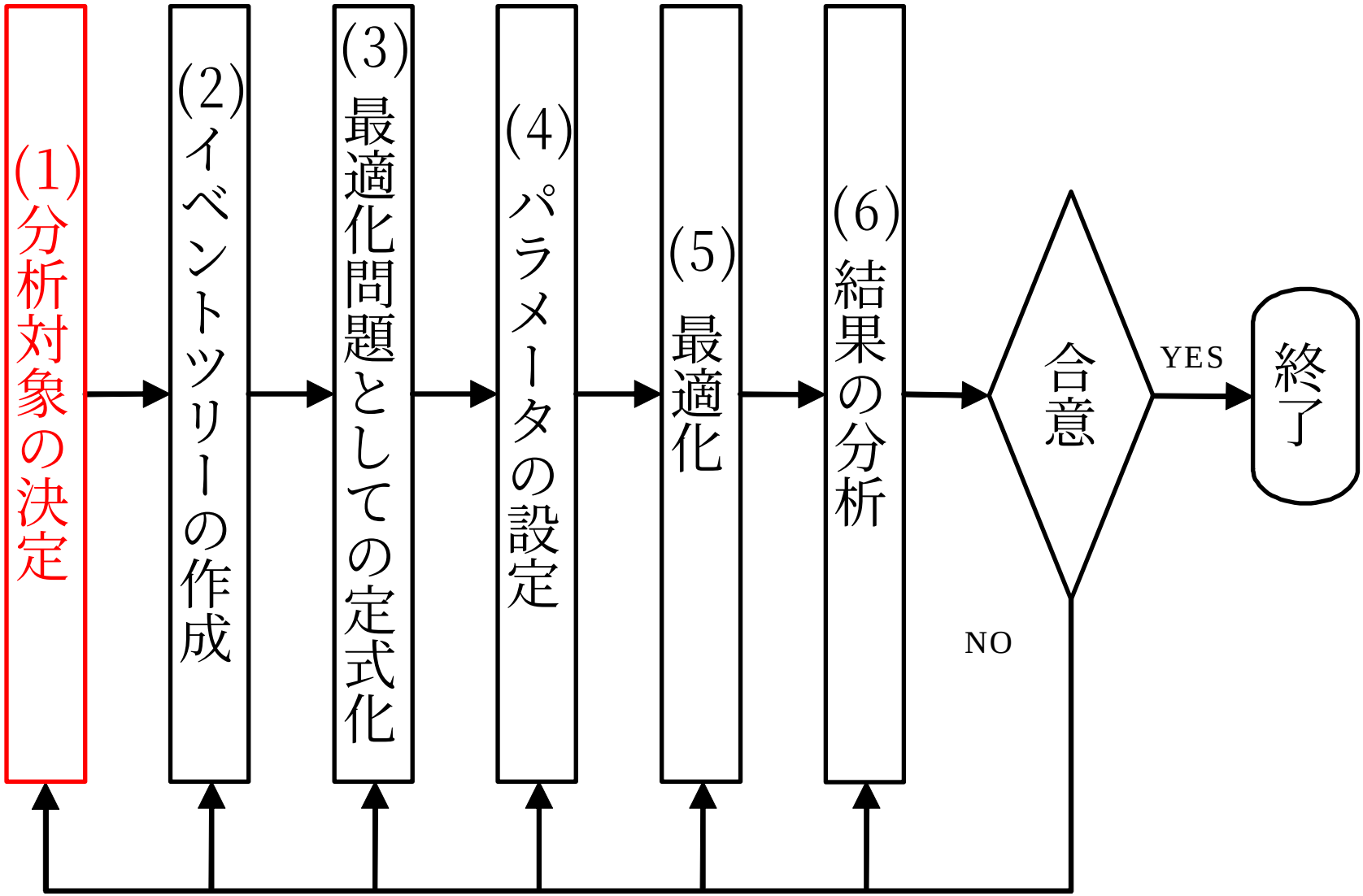
研究目的

- 暗号危殆化時のデジタル署名と長期署名フォーマットのリスク分析を行い，それぞれの結果を比較することでその安全性を評価する

評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
終了
NO

評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
NO
終了

分析モデル

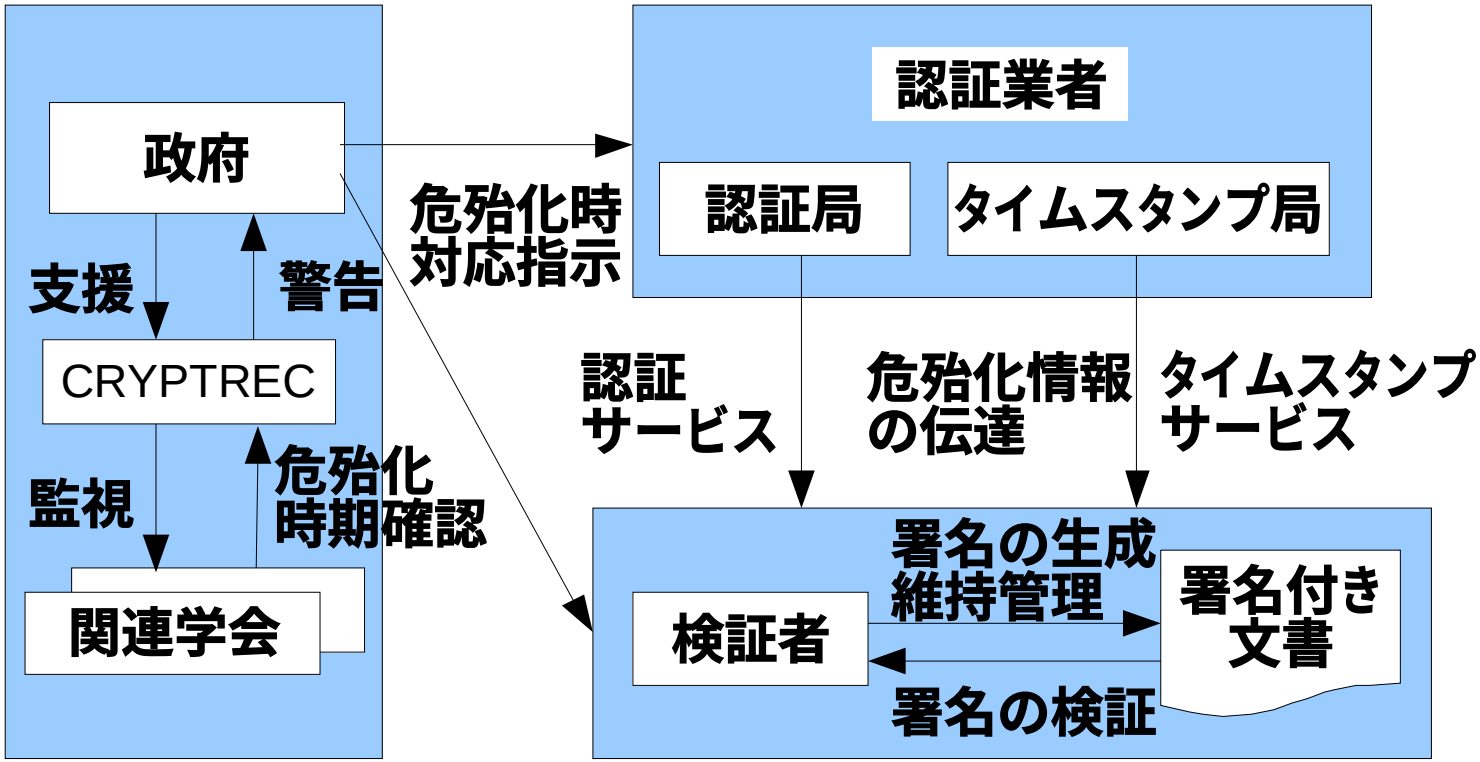
- 企業において電子保存された税務関連書類が保存の義務づけられた期間中に危殆化する

前提条件

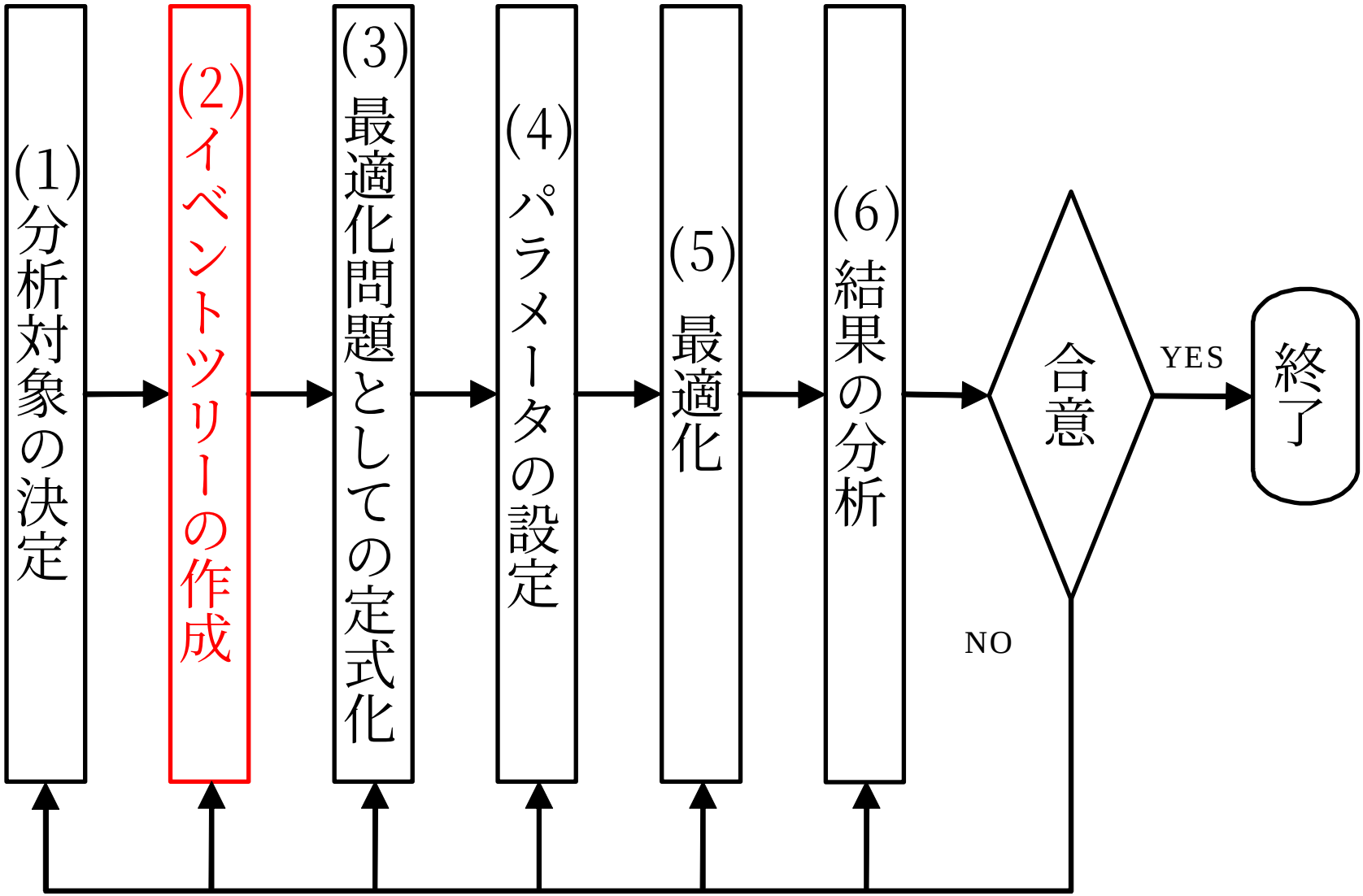
- 危殆化確認後，既に存在するデジタル署名が対象
- 十分に対策が取れる段階(半年～1 年)で危殆化を発見
- 危殆化が発生しても十分に既存の署名の証拠性を確保できる代替暗号が存在
- デジタル署名では以下の暗号アルゴリズムを使用
  - 公開鍵暗号：RSA1024bit
  - 公開鍵証明書：RSA2048bit
  - ハッシュ関数：SHA-1
- タイムスタンプでは以下の暗号アルゴリズムを使用
  - 公開鍵暗号：RSA2048bit
  - ハッシュ関数：SHA-2
- デジタル署名付き文書は法的に正しく運用される

想定環境

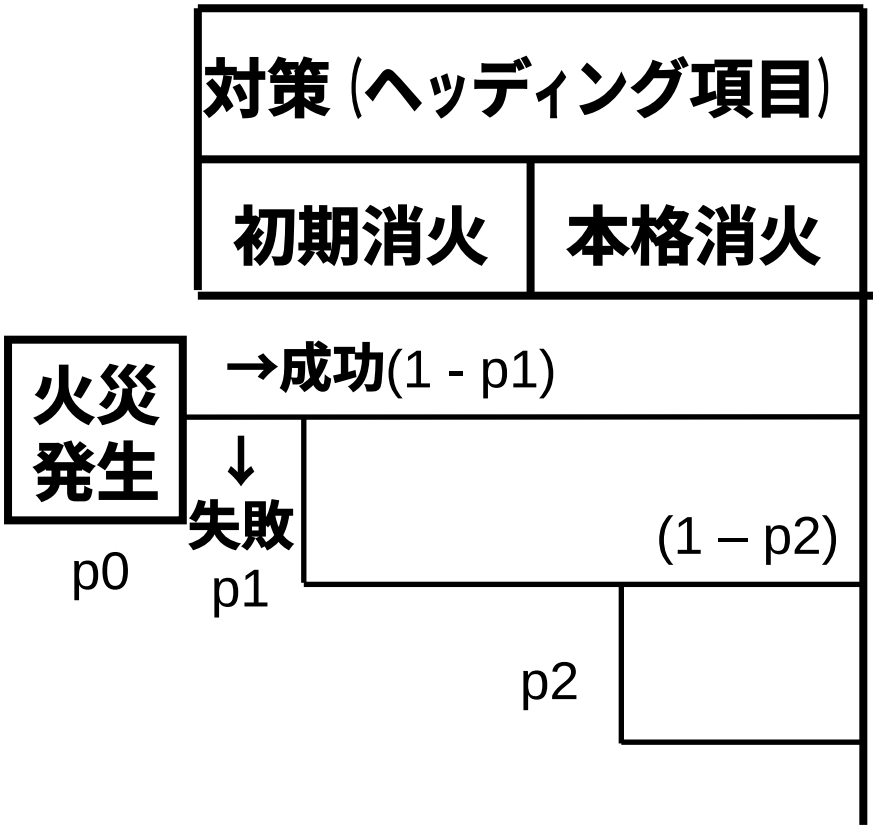
- 政府：危殆化情報確認機関
- 認証業者：認証局，タイムスタンプ局
- 検証者：企業



評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
終了
NO

イベントツリー分析とは



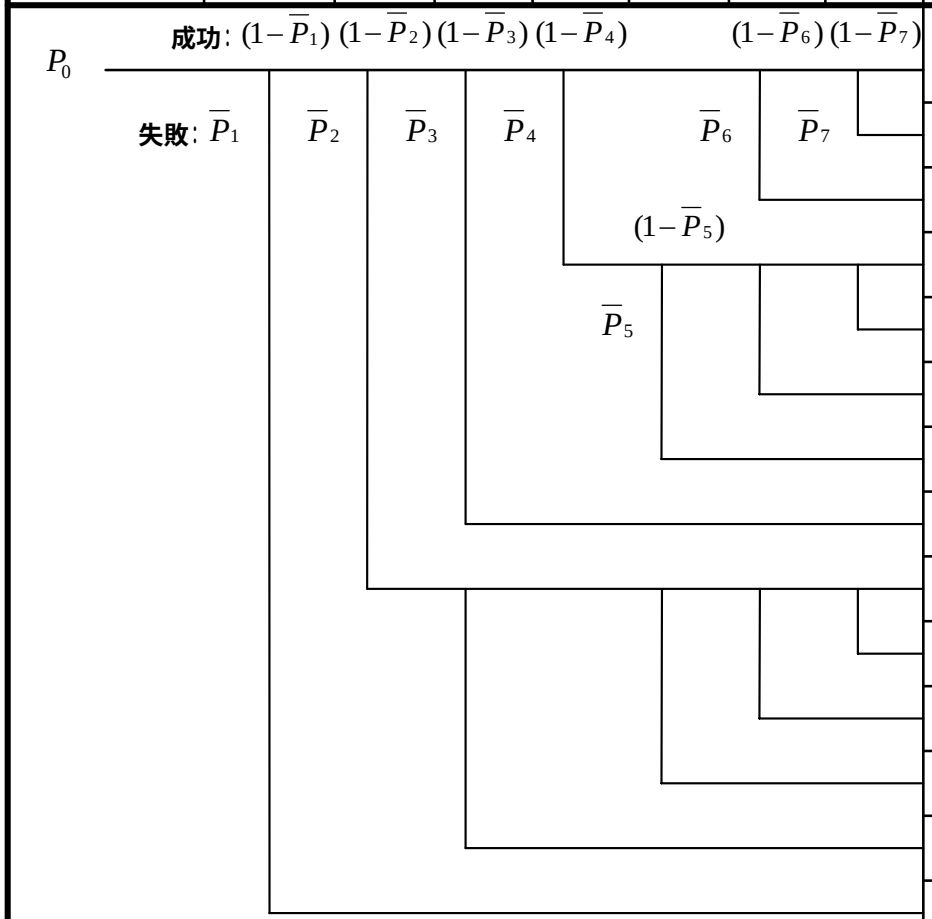
発生確率	影響	リスク
$P_1=p0\cdot(1-p1)$	M_1	$R_1=P_1\cdot M_1$
$P_2=p0\cdot p1\cdot(1-p2)$	M_2	$R_2=P_2\cdot M_2$
$P_3=p0\cdot p1\cdot p2$	M_3	$R_3=P_3\cdot M_3$

$$ETAのリスク=\sum_{i=1}^{3}R_i$$

基本的な対策の流れ

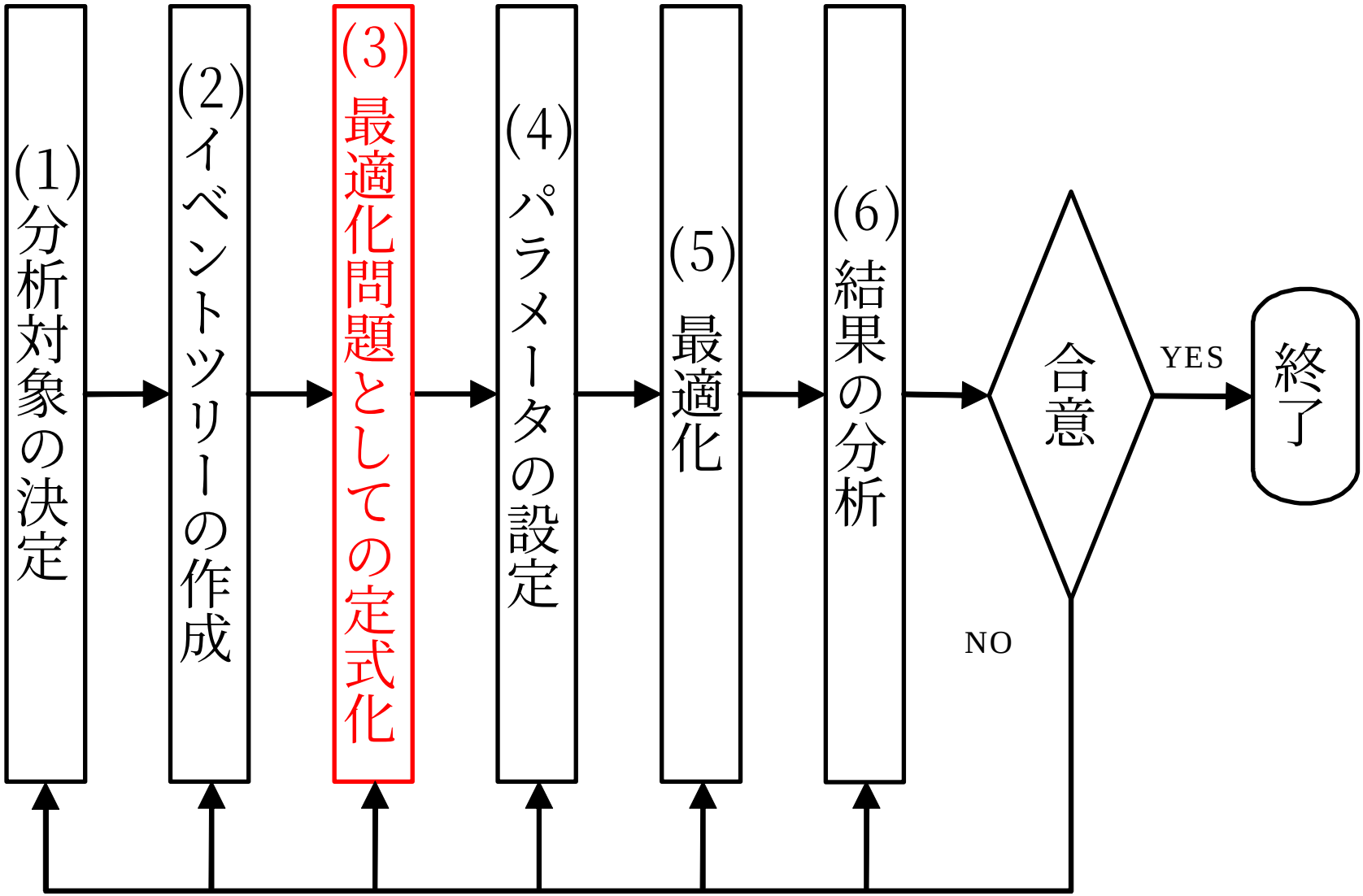
1. 暗号危殆化の発生
2. 暗号危殆化の確認
   - CRYPTRECによる監視
3. 暗号危殆化を認証業者へ伝達
   - 暗号危殆化の発表
4. 暗号危殆化に対する認証業者の対策
   - 暗号アルゴリズムの変更
5. 暗号危殆化を検証者へ伝達
   - メディアや認証業者による伝達
6. 暗号危殆化に対する検証者の対策
   - タイムスタンプの更新

イベントツリー (デジタル署名)



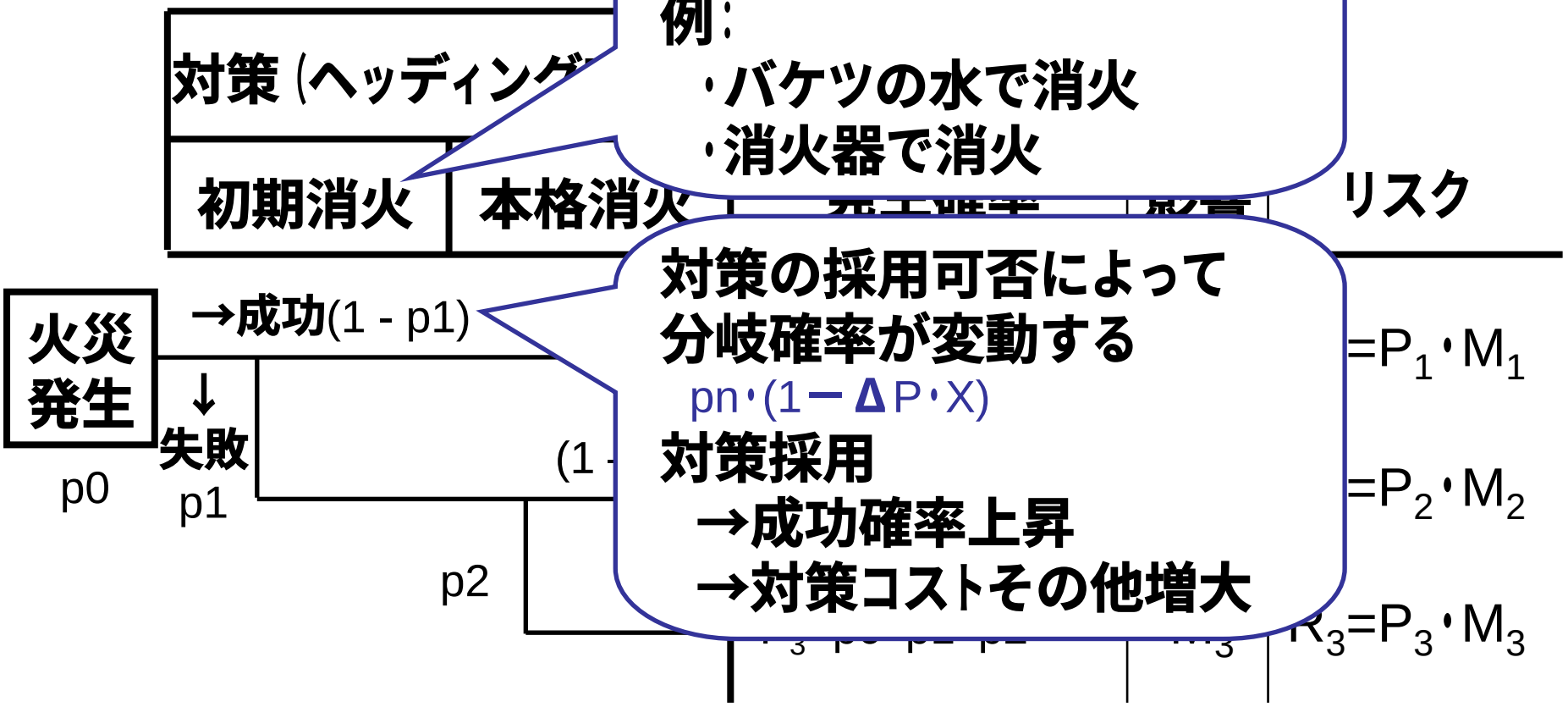
シーケンス	シーケンス発生確率 P_i	影響 M_i (コスト)	リスク $R_i = P_i \times M_i$	デジタル署名付文書の安全性確保
1	$P_1 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot (1-\overline{P}_6) \cdot (1-\overline{P}_7)$	M_1	$R_1 = P_1 \times M_1$	成功
2	$P_2 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot (1-\overline{P}_6) \cdot \overline{P}_7$	M_2	$R_2 = P_2 \times M_2$	失敗
3	$P_3 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot \overline{P}_6$	M_3	$R_3 = P_3 \times M_3$	失敗
4	$P_4 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot (1-\overline{P}_5) \cdot (1-\overline{P}_6) \cdot (1-\overline{P}_7)$	M_4	$R_4 = P_4 \times M_4$	成功
5	$P_5 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot (1-\overline{P}_5) \cdot (1-\overline{P}_6) \cdot \overline{P}_7$	M_5	$R_5 = P_5 \times M_5$	失敗
6	$P_6 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot (1-\overline{P}_5) \cdot \overline{P}_6$	M_6	$R_6 = P_6 \times M_6$	失敗
7	$P_7 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_4) \cdot \overline{P}_5$	M_7	$R_7 = P_7 \times M_7$	失敗
8	$P_8 = P_0 \cdot (1-\overline{P}_1) \cdot (1-\overline{P}_2) \cdot \overline{P}_3$	M_8	$R_8 = P_8 \times M_8$	失敗
9	$P_9 = P_0 \cdot (1-\overline{P}_1) \cdot \overline{P}_2 \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_5) \cdot (1-\overline{P}_6) \cdot (1-\overline{P}_7)$	M_9	$R_9 = P_9 \times M_9$	成功
10	$P_{10} = P_0 \cdot (1-\overline{P}_1) \cdot \overline{P}_2 \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_5) \cdot (1-\overline{P}_6) \cdot \overline{P}_7$	M_{10}	$R_{10} = P_{10} \times M_{10}$	失敗
11	$P_{11} = P_0 \cdot (1-\overline{P}_1) \cdot \overline{P}_2 \cdot (1-\overline{P}_3) \cdot (1-\overline{P}_5) \cdot \overline{P}_6$	M_{11}	$R_{11} = P_{11} \times M_{11}$	失敗
12	$P_{12} = P_0 \cdot (1-\overline{P}_1) \cdot \overline{P}_2 \cdot (1-\overline{P}_3) \cdot \overline{P}_5$	M_{12}	$R_{12} = P_{12} \times M_{12}$	失敗
13	$P_{13} = P_0 \cdot (1-\overline{P}_1) \cdot \overline{P}_2 \cdot \overline{P}_3$	M_{13}	$R_{13} = P_{13} \times M_{13}$	失敗
14	$P_{14} = P_0 \cdot \overline{P}_1$	M_{14}	$R_{14} = P_{14} \times M_{14}$	失敗

評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
終了
NO

最適化について

各ヘッディング項目に対して
複数の対策候補を設定する
例:
・バケツの水で消火
・消火器で消火



対策の採用可否によって
分岐確率が変動する
pn・(1－ΔP・X)
対策採用
→成功確率上昇
→対策コストその他増大

リスクや対策コストと言った要素を考慮して
最適な対策案の組み合わせを求める

目的関数と制約条件の設定

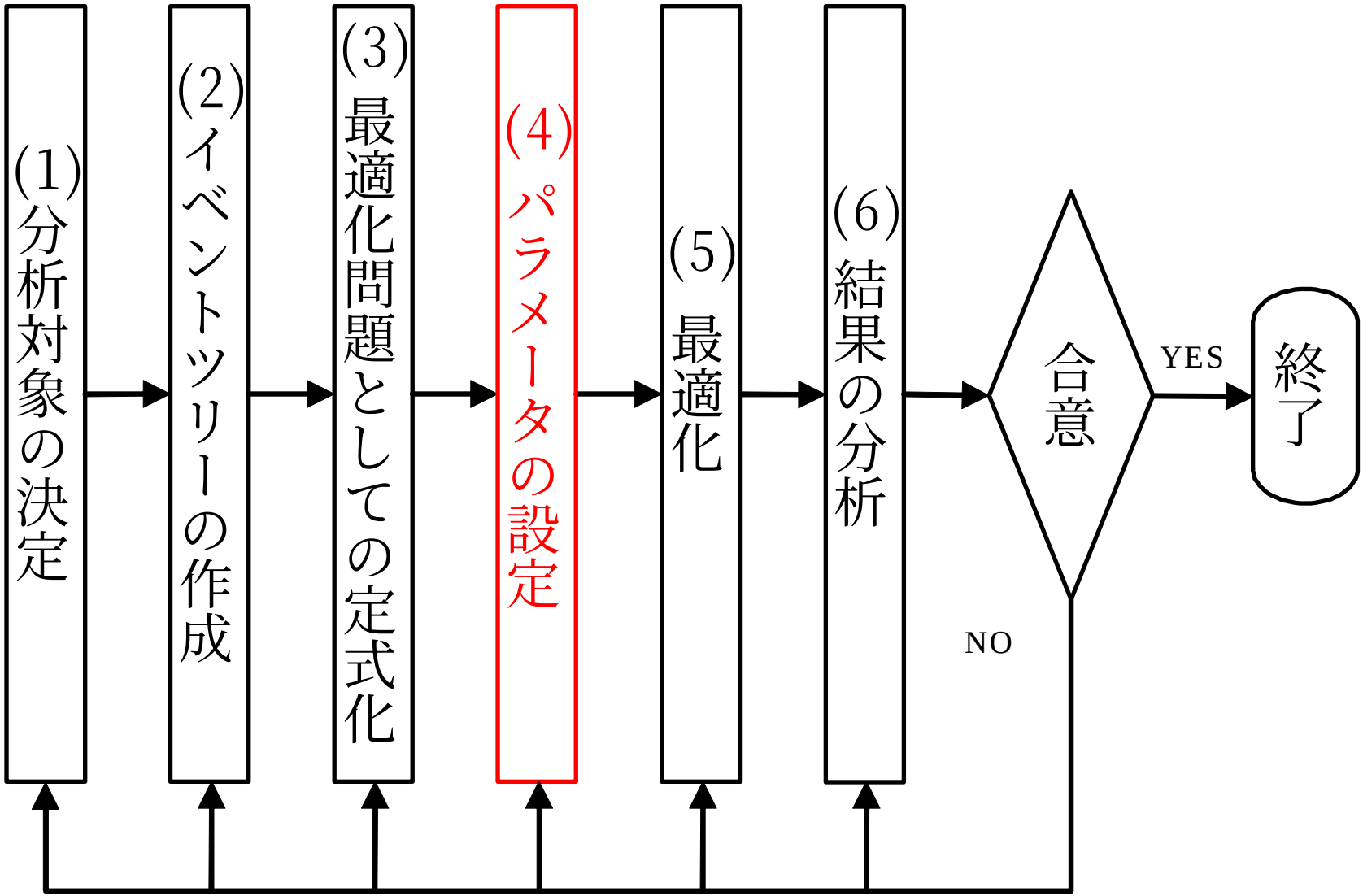
- **目的関数**

$$Min\left[ETAリスク+各対策コスト+運用コスト\right]$$

$$Min\left[\sum_{l=1}^{L} R_l + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{gij}\cdot X_{ij} + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{cij}\cdot X_{ij} + \sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{vij}\cdot X_{ij} + OC\right]$$

- **制約条件**
  - **政府の対策コスト** ⇨ $\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{gij}\cdot X_{ij} \le C_g$
  - **認証業者の対策コスト** ⇨ $\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{cij}\cdot X_{ij} \le C_c$
  - **検証者の対策コスト** ⇨ $\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{vij}\cdot X_{ij} \le C_v$

評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
終了
NO

パラメータの設定 (1/2)

- 暗号危殆化による影響
  - 経済界全体での税務関連書類の保存コスト = 3000億円
    - 日本経済団体連合会，「税務書類の電子保存に関する報告書」
  - 書類1枚あたりの保存コストを2円とする
  - 電子保存された税務関連書類数の割合を10%とする
  - 書類1枚あたりの危殆化による影響を変数Xとする

電子保存された税務関連書類数N

N ＝(3000億円÷2円)×7年×0.1 ＝ 1050億枚

税務関連書類の危殆化による影響 M

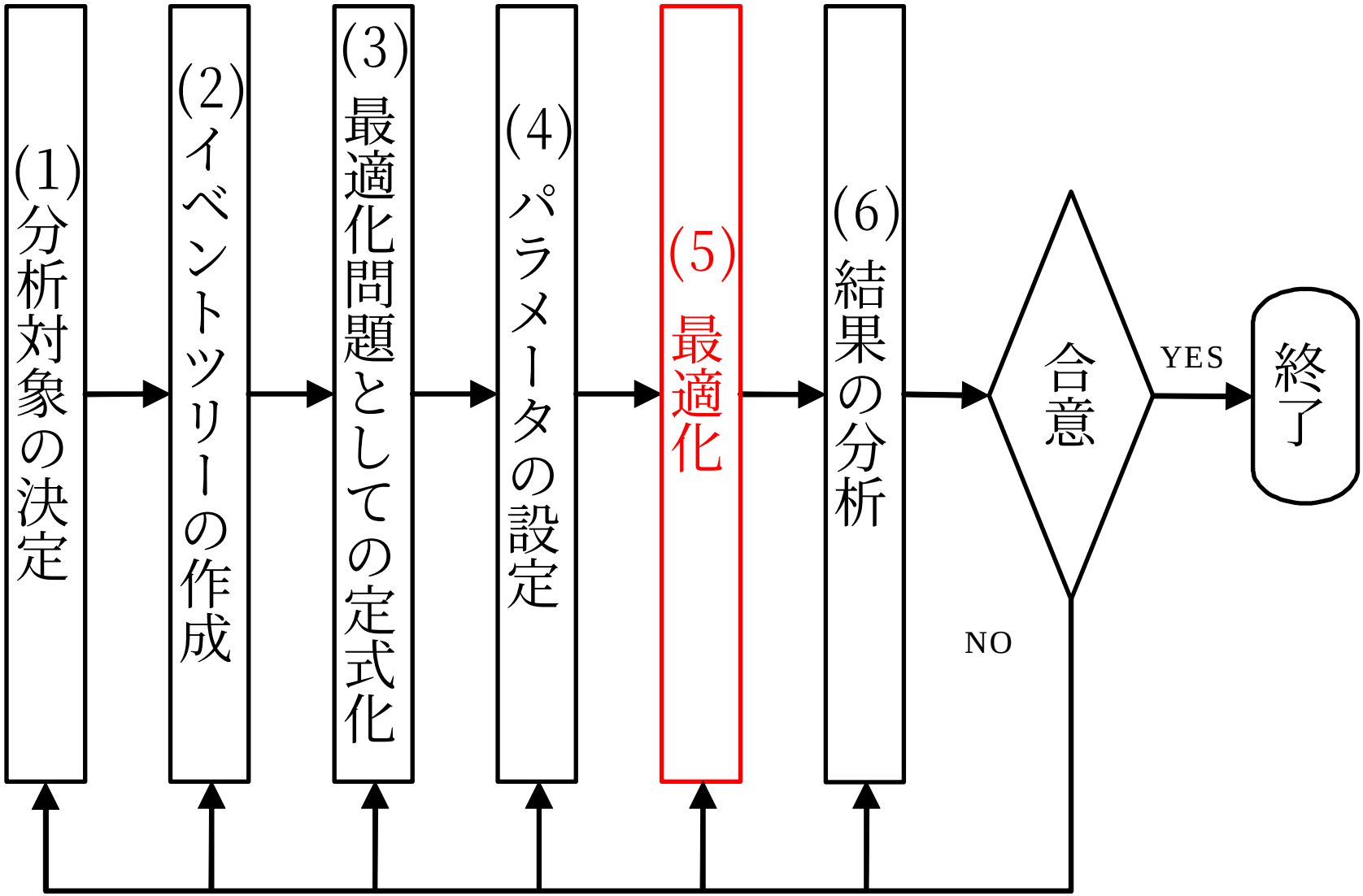
M = N×X円 = 1050億×X円

パラメータの設定 (2/2)

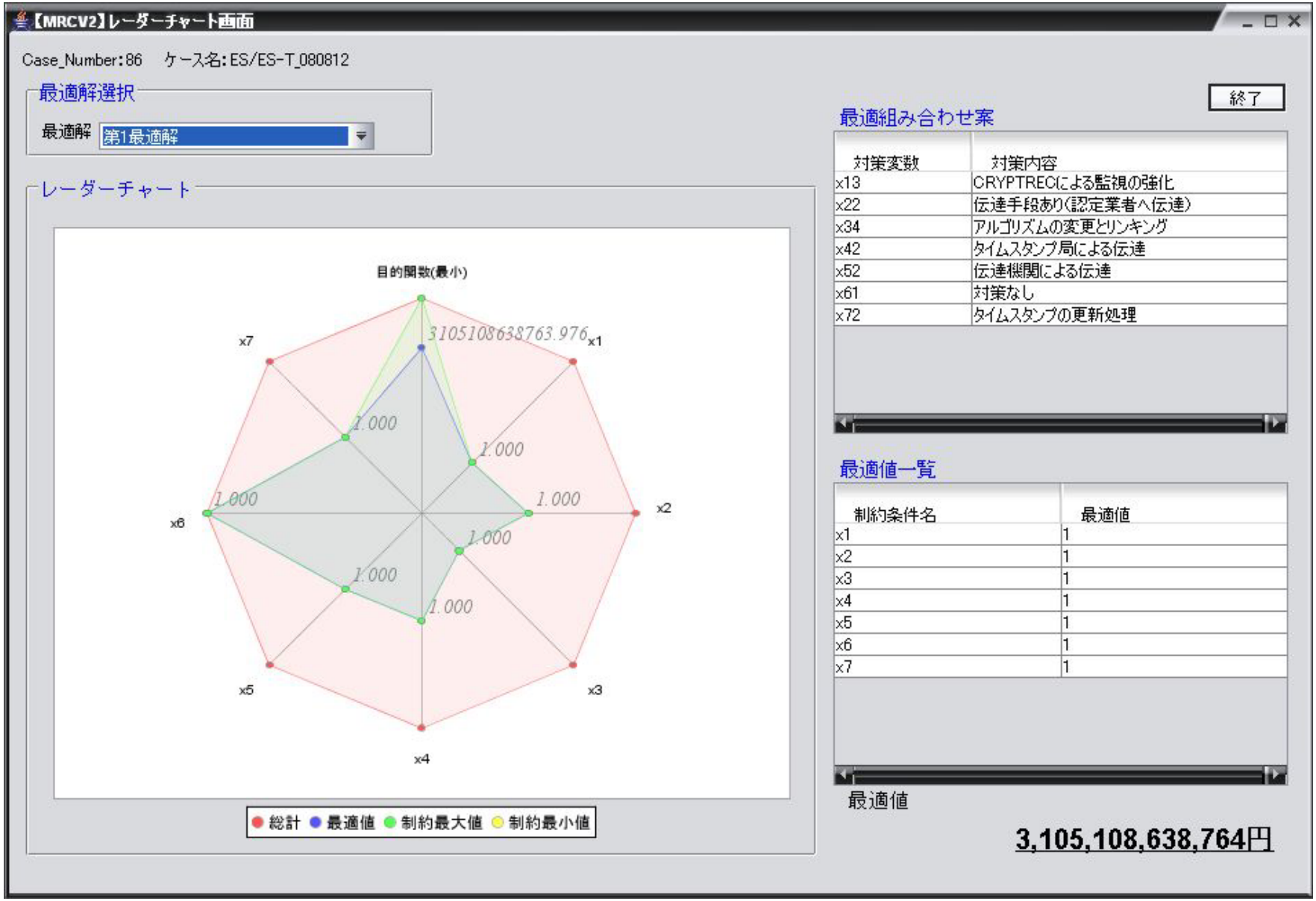
対策案	パラメータの設定			
1．暗号危殆化情報の確認機構	政府	認証業者	検証者	危殆化確率
(1-1)監視機関なし（X11）	Cg11=0 円	Cc11=0 円	Cv11=0 円	p11 = 0.5
(1-2)CRYPTREC による監視(X12)	Cg12=2000 万円	Cc12=0 円	Cv12=0 円	p12 = 0.01
(1-3)CRYPTREC による監視の強化(X13)	Cg13=6000 万円	Cc13=0 円	Cv13=0 円	p13 = 0.005
2．認証業者への伝達				
(2-1)伝達手段なし（危殆化の発表のみ）（X21)	Cg21=0 円	Cc21=0 円	Cv21=0 円	p21 = 0.01
(2-2)伝達手段あり（認定業者へ伝達）（X22)	Cg22=100 万円	Cc22=0 円	Cv22=0 円	p22 = 0.005
3．認証業者の対策（通常時）				
(3-1)対策なし（X31)	Cg31=0 円	Cc31=0 円	Cv31=0 円	p31 = 1.0
(3-2)ハッシュのリンキングと公知化（X32)	Cg32=0 円	Cc32=8 億円	Cv32=0 円	p32 = 0.05
4．認証業者の対策（危殆化時）				
(4-1)対策なし（X41)	Cg41=0 円	Cc41=0 円	Cv41=0 円	p41 = 1.0
(4-2)代替暗号アルゴリズムへの変更（X42)	Cg42=0 円	Cc42=6 億円	Cv42=0 円	p42 = 0.01
5．認証業者による伝達				
(5-1)伝達手段なし（X51)	Cg51=0 円	Cc51=0 円	Cv51=0 円	p51 = 1.0
(5-2)タイムスタンプ局による伝達（X52)	Cg52=0 円	Cc52=297 万 7 千円	Cv52=297 万 7 千円	p52 = 0.01
6．伝達機関による伝達				
(6-1)伝達手段なし（X61）	Cg61=0 円	Cc61=0 円	Cv61=0 円	p61 = 0.9
(6-2)伝達機関による伝達（X62）	Cg62=4 億円	Cc62=0 円	Cv62=0 円	p62 = 0.1
7．対策を試みる（通常時）				
(7-1)対策なし(X71)	Cg71=0 円	Cc71=0 円	Cv71=0 円	p71 = 0.9
8．対策を試みる（危殆化時）				
(8-1)対策なし(X81)	Cg81=0 円	Cc81=0 円	Cv81=0 円	p81 = 0.1
9．検証者の対策（通常時の対策）				
(9-1)対策なし(X91)	Cg91=0 円	Cc91=0 円	Cv91=0 円	p91 = 1.0
(9-2)タイムスタンプの更新処理(X92)	Cg92=0 円	Cc92=0 円	Cv92=1050 億円	p92 = 0.01
10．検証者の対策（危殆化時の対策）				
(10-1)対策なし(X101)	Cg101=0 円	Cc101=0 円	Cv101=0 円	p101 = 1.0
(10-2)タイムスタンプの更新処理(X102)	Cg102=0 円	Cc102=0 円	Cv102=10500 億円	p102 = 0.01

atory

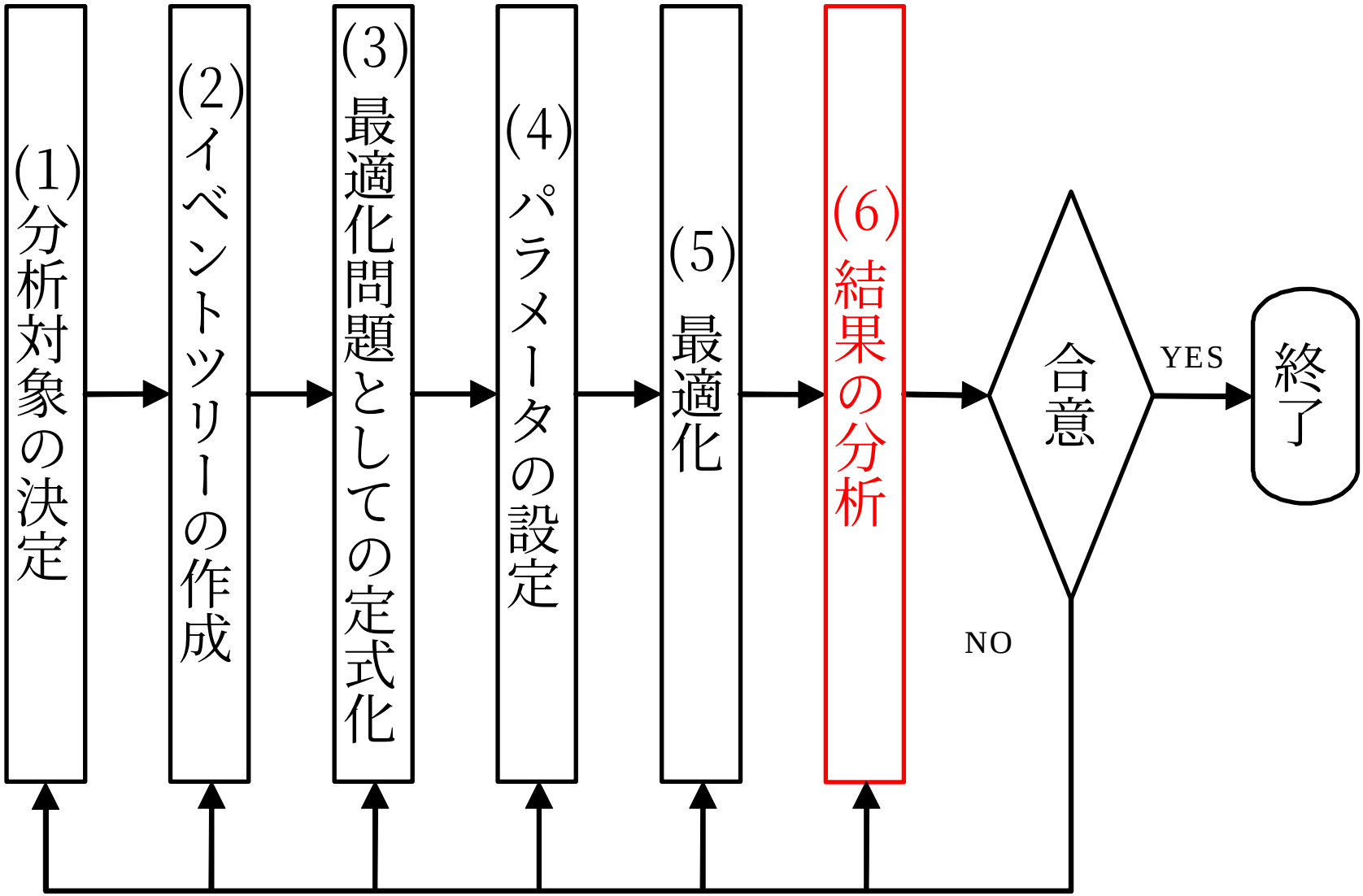
評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
NO
終了

最適化


【MRCV2】レーダーチャート画面
Case_Number:86　ケース名:ES/ES-T_080812
最適解選択
最適解
第1最適解
終了
レーダーチャート
目的関数(最小)
3105108638763.976
x1
x2
x3
x4
x5
x6
x7
1.000
総計
最適値
制約最大値
制約最小値
最適組み合わせ案
対策変数
対策内容
x13 CRYPTRECによる監視の強化
x22 伝達手段あり(認定業者へ伝達)
x34 アルゴリズムの変更とリンキング
x42 タイムスタンプ局による伝達
x52 伝達機関による伝達
x61 対策なし
x72 タイムスタンプの更新処理
最適値一覧
制約条件名
最適値
x1 1
x2 1
x3 1
x4 1
x5 1
x6 1
x7 1
最適値
3,105,108,638,764円

評価方法


(1)分析対象の決定
(2)イベントツリーの作成
(3)最適化問題としての定式化
(4)パラメータの設定
(5)最適化
(6)結果の分析
合意
YES
NO
終了

最適化結果

- デジタル署名と長期署名フォーマットにおいて最適な対策案の組み合わせを求める
  - 各関与者の制約条件を上限値まで設定
  - 書類1枚あたりの危殆化による影響は5000 円

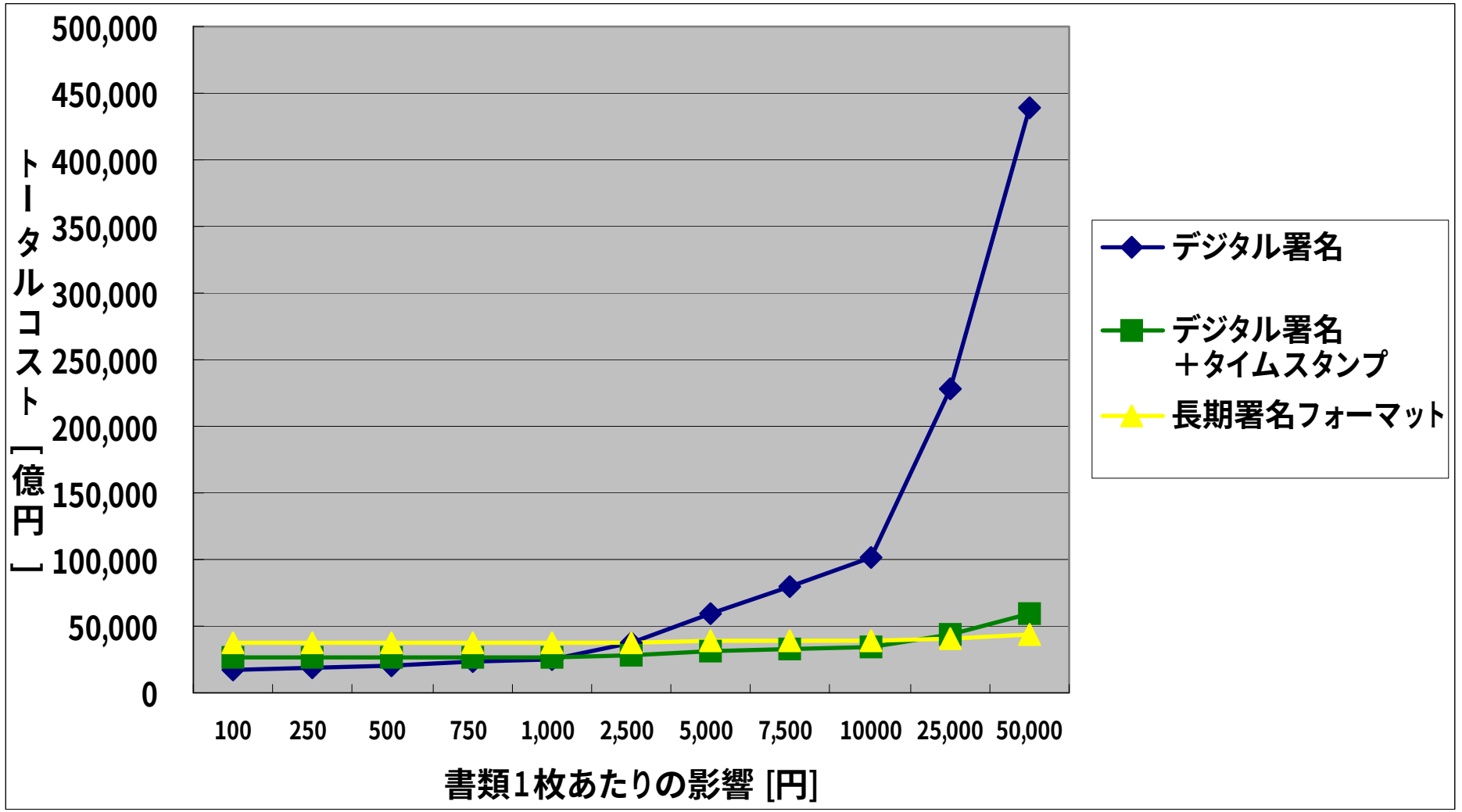
最適化結果の比較

対策案番号	デジタル署名	長期署名フォーマット
x1	CRYPTRECによる監視の強化	CRYPTRECによる監視の強化
x2	認証業者への伝達	危殆化の発表
x3		対策なし
x4	アルゴリズムの変更とハッシュのリンキング	代替暗号アルゴリズムへの変更
x5	認証業者による伝達	認証業者による伝達
x6	伝達機関による伝達	伝達機関による伝達
x7		対策なし
x8	対策なし	対策なし
x9		対策なし
x10	タイムスタンプの更新処理	タイムスタンプの更新処理
トータルコスト	5,899,627,114,346	3,842,012,220,835

安全性の評価

- 以下の3方式で分析結果を比較
  1. デジタル署名
  2. デジタル署名＋タイムスタンプ
  3. 長期署名フォーマット

各方式の比較


500,000
450,000
400,000
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
トータルコスト［億円］
100
250
500
750
1,000
2,500
5,000
7,500
10000
25,000
50,000
書類1枚あたりの影響 [円]
デジタル署名
デジタル署名
＋タイムスタンプ
長期署名フォーマット

まとめ

- 長期署名フォーマットでは認証業者の対策などは現状で十分であるが，CRYPTREC による監視の強化や検証者への情報の伝達手段の確保が重要である
- 暗号の危殆化という面から考えると書類の重要度に合わせた以下のような方式の使い分けが有効である
  - あまり重要ではない書類
    ⇨ デジタル署名
  - 税務関係書類などの重要な書類
    ⇨ デジタル署名＋タイムスタンプ
  - 非常に重要な書類
    ⇨ 長期署名フォーマット

今後の課題

- ヒステリシス署名や電子公証などその他の長期保存方式についても分析
- 暗号危殆化に対する効果的な対策手法についての検討

ご清聴ありがとうございました