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[†1] 上田祐輔[†2] 佐々木良一[†1,†3]

デジタル署名の利用が増加する傾向にある．デジタル署名の安全性は公開鍵暗号に依存している．したがって，デジタル署名の長期利用を考慮すると，危殆化を確認した際の影響を考慮せざるをえない．特に，公開暗号危殆化時の署名付き文書への影響の分析とその対策については，検討が不可欠である．そこで，本論文では，公開鍵暗号の危殆化が近く生じることが明確になった場合に，既存の署名付き文書の証拠性を確保するために必要な対策の最適な組合せを費用とリスク低減効果のバランスを考慮して求める方法を提案する．さらに提案した方式に，ある想定した状況におけるパラメータ値を設定し，リスクの影響と対策費用のバランスを考慮した最適な対策案の組合せを求めたので，その適用結果を報告する．

Proposal on Combinatorial Optimization Method for Countermeasures to Digitally Signed Document against Public Key Cipher Compromise and Its Application

Hajime Fujimoto,[†1] Yusuke Ueda[†2] and Ryoichi Sasaki[†1,†3]

The popularization of the Internet increases the usage of a digital signature. The safety of a digital signature depends on the strength of a public key cipher. Therefore, it is necessary to examine the influence on compromise of public key cipher, because digital signature is sometimes used for long time. Especially, the impact analysis on compromise of public key cipher to the digitally signed documents is essential to obtain the solution for countermeasure. We propose the method to obtain the optimal combination of countermeasures considering the cost and the effects to decrease the risk, when it is discovered that the compromise of public key cipher occurs in near future. In addition, we report the obtained optimal combination of measures after setting the parameters to the proposed method on cost and risk.

1. はじめに

インターネットの発展にともない，行政と国民・事業者との間をオンライン接続し住民サービスを行う電子政府や，ネットワークを利用して企業間の契約や決済などを行う電子商取引などが普及しつつある．これらを安全かつ安心して利用するための基盤技術としてデジタル署名がある．デジタル署名は公開鍵暗号[14]の安全性に強く依存しており，公開鍵暗号が安全であれば署名者以外は，署名用秘密鍵を知りえないという前提の下に利用されている．

†1 東京電機大学
Tokyo Denki University
†2 アマノ株式会社
AMANO
†3 JST 社会技術研究開発センター研究員
JST The Research Institute of Science and Technology for Society Researcher

しかし，コンピュータの演算能力の向上や新しい攻撃手法の発見などにより，公開鍵暗号が安全であるという前提が崩壊してしまう危険性を無視することはできず，署名用秘密鍵が知られてしまう可能性がある．署名用秘密鍵が知られてしまえば，だれもが，その人に成りすまし，署名付き文書を偽造することができるようになる．

公開鍵暗号の安全性が喪失してしまうことを，「公開鍵暗号の危殆化」と呼ぶ[2]．さらに，SHA-1 などのハッシュ関数が衝突する可能性も指摘されており，そちらについても無視できない状況になってきている[6]．もし，ハッシュ関数が危殆化してしまったとすると，不正者の都合のいいようにデジタル署名付き文書を改竄されてしまう恐れがある．これを「ハッシュ関数の危殆化」と呼ぶ．

公開鍵暗号やハッシュ関数の危殆化を確認した際に，安全性の高い公開鍵暗号（たとえば，鍵長 2048 ビット

の RSA 暗号）やハッシュ関数（たとえば，SHA-256）を用い新しくデジタル署名付き文書を作成できるようにする対策はいろいろ検討され始めている（文献 8) など）．しかし，すでに存在しているデジタル署名付き文書に対する対策の検討については，非常に限定されており，それも定性的分析にとどまっている[1),4),8)]．さらに既存のデジタル署名付き文書に対する対策において対策コストと対策効果のバランスを考慮し，分析する手法はなく，対策のスムーズな導入が困難である．公開鍵暗号の危殆化やハッシュ関数の危殆化が近く生じる可能性がある場合に，何も対策をとらなければ，危殆化が実現した際に，次の 2 つの不正行為が発生しうる．

(1) 偽のデジタル署名付き文書を本物だと主張する
たとえば，「A さんに 1 億円を貸している，借用証書がここにある」と主張する場合が考えられる．

(2) 本物のデジタル署名付き文書なのに，偽者だと主張する
たとえば，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」と主張する場合が考えられる．

このような状況では本物か偽者か分からない契約文書が多数存在することとなり，大きな社会問題になってしまうと考えられる．なお，公開鍵暗号の危殆化もハッシュ関数の危殆化もその後の現象は類似であるので，以下では公開鍵暗号の危殆化を対象として説明を行う．

本論文では，公開鍵暗号の危殆化が近く生じることが明確になった場合に，既存の署名付き文書の証拠性を確保するために必要な対策の最適な組合せを費用とリスク低減効果のバランスを考慮して求める方法を提案する．あわせて，1 つのケースにおける最適な対策案を示し，今後，社会にとって必要な対応に関し考察を行う．

ここでは，最適な組合せを求める際に必要となるリスク分析手法として原子力工学の分野で実績のあるイベントツリー分析[12)] を利用し，さらに，最適化手法として，離散型最適化手法（組合せ最適化法などともいう）を用いている．

ここで，イベントツリー分析は原子力工学などで広く利用されているが，コンピュータ関連の分析に用いられた例は著者らが調査した範囲では見当たらない．また，イベントツリー分析と最適化手法を組み合わせた方式は従来なかったと考えている．イベントツリー分析は，フォルトツリー分析と異なり，時系列的な推移がある問題の分析に適しており，ここで扱う問題は，まさしくそのような問題であると考え採用した．また，危殆化に限らずセキュリティ対策を実施しようとする場合，必ず対策コストと各種の対策効果の間に対立する要素があり，対策案を 0-1 変数で表す離散型最適化手法を用いることにより，対策コストなどの制約の下に目的関数を最適化する対策案の組合せを容易に求めることが可能となる．

2. 最適な対策案を求める手順

公開鍵暗号の危殆化が発生した際，デジタル署名付き文書へのリスクを軽減させるような最適な対策案を求める手順を以下に示す（**図 1** 参照）．

(1) 対象の決定と予備的検討

ここでは，危殆化における定義を明確化し，分析の対象，分析の前提，関与者の抽出，脅威・脆弱性の抽出，対策の抽出を行う．

(2) イベントツリー分析によるリスク分析

(1) で決定した分析の対象，分析の前提，脅威・脆弱性の抽出，対策方法から，イベントツリーを作成する．イベントツリーについては，後ほど説明する．

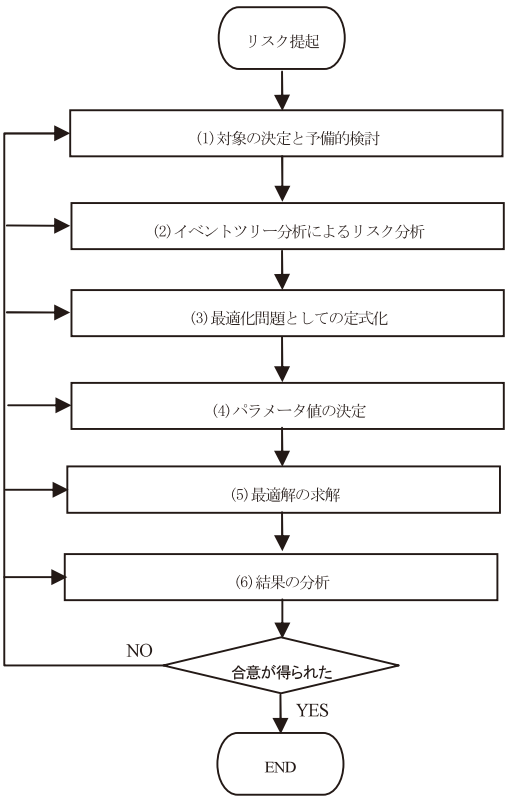


図 1 最適な対策案を求める手順のフローチャート
Fig. 1 Flow chart for procedure to obtain the optimized measures.

(3) 最適化問題としての定式化

最適解を算出するのに必要である目的関数・制約条件の定式化を行う．各対策案を採択するか，しないかを 0-1 変数で表し，組合せ最適化問題として定式化することを前提とする．

(4) パラメータ値の決定

(3) の定式化の際に，係数として与えられている対策コスト，確率，影響といったパラメータの値を決定する．あわせて制約条件の値を設定する．

(5) 最適解の求解

設定された制約条件の下で，最適な対策案の組合せを算出する．今回は総当たり法を用い求解した．1 つの制約条件値の下ではなく制約条件値を変化させるなどして，様々な状況での最適解を算出する．

(6) 結果の分析

(5) で行った種々の条件下での最適解の求解．具体的には，公開鍵暗号が危殆化した際にデジタル署名付き文書にどのような影響があり，どうしても行うべき対策としてどのようなものがあるのか検討する．パラメータの値については，どうしても主観性がともなうが，その中で確実に提言できることを検討する．

少数の解析者により，上記の (1)–(6) が一応の結果が得られたら，その結果をいろいろな専門家に見せつつ，合意が得られるまで一緒にこの過程を繰り返す．

3. 組合せ最適化のための方式

3.1 対象の決定と予備検討

3.1.1 危殆化における対策の種類

危殆化における対策は**図 2** に示すように，大きく 2 つの対策に分類することができる．まずケース ① は，危殆化は徐々に進行するという前提の下，すでに存在するデジタル署名付き文書に対して対策を施すものである．ケース ② は，危殆化における前提は同じなのだが，危殆化を発見した後，新たに生成するデジタル署名に対する対策である．ここでは従来ほとんど検討が行われていなかった ① を対象とする．

3.1.2 分析の前提と危殆化確認後既存署名付き文書に対する対策方法

分析の前提を以下に記す．

① 分析の前提として，**図 3** に示すように公開鍵暗号の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段階で危殆化を発見するものとし，かつ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公開鍵暗号が存在するものとする．具体的に，十分に対策をとれる段階と対策をとりにくい段階の境界線はどこなのかといった議論もあるが，今回はその部分については考慮せず，あくまで十分に対策がとれる段階（半年から 1 年）で危殆化を発見するということを前提とする．

② 署名に利用する公開鍵暗号は RSA の 1,024 bit 鍵長のものを利用し，公開鍵証明書に使用するものは RSA の 2,048 bit 鍵長のものを利用する．ハッシュ関数は SHA-1 を利用するものとする．

③ 5 年以内に危殆化する確率を与える．後述する具体例では 0.01 とした．

④ 適用モデルとしては，電子借用書を利用したとき，返済完了前に危殆化してしまうような場合についてリスク分析を行う．

⑤ デジタル署名付き電子借用書の普及率を与える．後述する具体例では 0.01 とした．現時点では，これほど普及しているわけではないが，将来的なことを考慮に入れ，この数値を設定した．

⑥ デジタル署名付き文書は，法的に正しく運用されているものとする．

分析の前提でも記述したが，適用モデルとしては，電子借用書を利用したとき，返済の途中で危殆化してしまうような場合についてリスク分析を行う．電子借用書を適用モデルとして採用した理由としては，比較的利用期間が長く，損害を，直接，損害コストとして

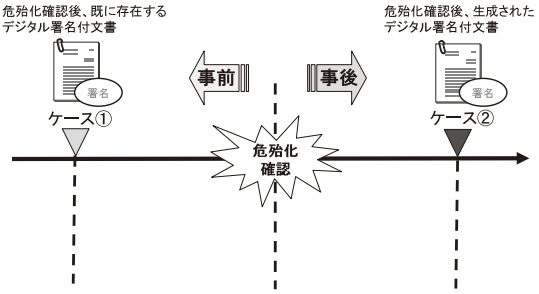


図 2 危殆化時のデジタル署名における対策の種類
Fig. 2 Kind of measures when digital signature is compromised.

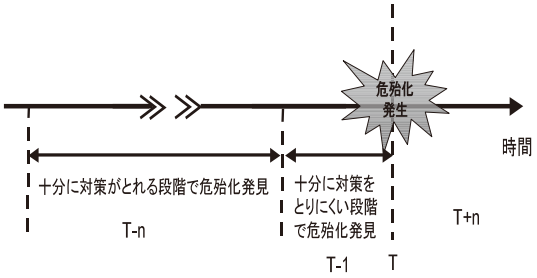


図 3 危殆化発見パターン
Fig. 3 Discovery patterns against compromise.

算出できるためである．危殆化の影響を最も受けるパターンとしては，ローンなどを利用して長期的に借金を返すような場合が考えられる．電子借用書は，まだ，ほとんど実際に存在しないが，5 年後の社会状況を予想し，少しずつ使われ始めているものと想定した．

ここでは，社会全体として，危殆化時対応ポリシを前もって決めておき，危殆化の発生が具体的に予期された場合には危殆化時対応ポリシに基づき，署名者，検証者（署名付き文書を持っている人）が決められた対応を必ず実施するようになっていなければならない．このポリシの検討がなされてないのが現状である．

このポリシに基づく対応としては，次のようなものが考えられる．

(1) 文書への再署名：危殆化の発生が具体的に予期された場合には，署名者と署名付き文書を持っている人の 2 者間で，その時点で安全であるとされている強い公開鍵暗号を用いて，対象とする文書に再署名をする．

(2) 第三者機関による追加署名：危殆化の発生が具体的に予期された場合には，既存の署名付き文書に対して安全性を確保するためにその時点で安全であるとされている強い公開鍵暗号を用い第三者機関が追加署名生成処理を行う．

3.1.3 想定環境

関与者

リスク分析を行ううえでの想定環境は，次に示すようなエンティティから構成されるものとする（**図 4**，**図 5** 参照）．各エンティティの役割・機能を以下に記述する．

(1) 政府：危殆化情報を確認する機関を設置する．現在，CRYPTREC がこの役割を担っている[13]．CRYPTREC とは Cryptography Research and Evaluation Committees の略であり，電子政府推奨暗号の安全性を評価・監視し，暗号モジュール評価基準などの策定を検討するプロジェクトである．総務省および経済産業省が共同で開催する暗号技術検討会と，独立行政法人情報通信研究機構（NICT）および独立行政法人情報処理推進機構（IPA）が共同で開催する暗号技術監視委員会および暗号モジュール委員会で構成される．政府は CRYPTREC を資金面などで支援するとともに，公開鍵危殆化の時期が近いことの警告を受けると，企業と国民に公開鍵暗号の危殆化が近いことや，署名付き文書に対する対策を指示する．国民には，テレビ・新聞・WEB などのメディアを利用して伝達する必要がある．

(2) CRYPTREC：CRYPTREC は政府の支援を受け，学会の動向などの調査を行い，公開鍵暗号の危殆化の時期が近づいてないか監視する．危殆化が近く起こることが確認されたら政府に対し，対策を行うよう警告を行う．

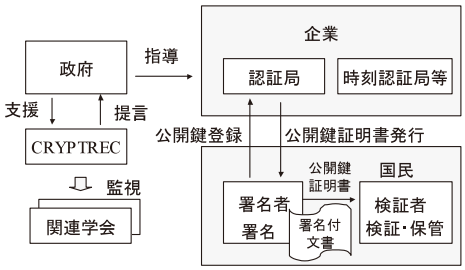


図 4 関与者間の関係（危殆化確認前）
Fig. 4 Relationship between entities (Before finding compromise).

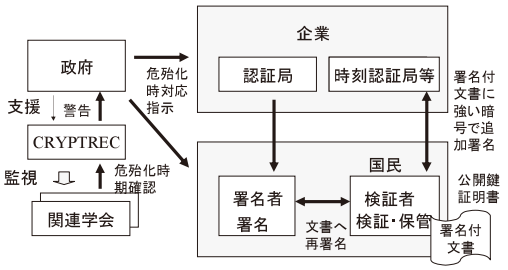


図 5 関与者間の関係（危殆化確認後）
Fig. 5 Relationship between entities (After finding compromise).

(3) 企業：

(a) 認証局：公開鍵証明書の生成と発行，証明書失効リスト（CRL）の生成，掲示を行う．さらに，危殆化時には公開鍵証明書を発行した署名者に対して危殆化の伝達を行う．本当にこの情報が必要な検証者（金を貸している人）には，認証局はだれが検証者か分からないので，この情報を流せないことを知っておく必要がある．

(b) 時刻認証局などの第三者機関：危殆化が影響する既存の署名付き文書に対して，署名付き文書の持ち主などの依頼により，安全性を確保するためにその時点で安全であるとされている強い公開鍵暗号を用い追加署名生成処理を行う．この機能は時刻認証局が担当してもよい．また，上記（a）の認証局がこの第三者機関と同じでもよい．

(4) 国民：

(a) 署名者：借金をする人であり，認証局から証明書の発行を受け，署名付き文書を生成する．危殆化時には，危殆化時対応ポリシの内容によっては，署名者と署名付き文書を持っている人の 2 者間で，その時点でも安全であるとされている公開鍵暗号を用いて対象

とする文書に再署名をする場合もある．署名者が法人であってもよいが，ここでは個人とした．

（b）検証者：署名付き文書（借用書）を入手し，デジタル署名の検証を行い署名付き文書と証明書を保管しておく．危殆化時対応ポリシに基づき，署名者との間で再署名をしたり，第三者機関に追加署名をしたりしてもらう．検証者が法人であってもよいがここでは個人とした．

これらのエンティティに対して対策を施すことにより，（1）偽のデジタル署名付き文書を本物だと主張したり，（2）本物のデジタル署名付き文書であるのに，偽者だと主張したりするというリスクを軽減させる．

脅威・脆弱性

公開鍵暗号の秘密鍵が外部に漏れ出る要因については，大きく分けて以下のものがあげられる[8]．

暗号アルゴリズムの危殆化による脅威
- 計算機能力の向上
- 計算機モデルの変化
- 攻撃手法の進歩

暗号モジュールの危殆化による脅威
- モジュール実装上の問題の発見
- 計測能力の向上
- 攻撃手法の進歩
- モジュールの変形を起こす手段の改良

暗号利用システムの危殆化による脅威
- システムデザインの問題
- 管理運用の問題

本論文では，社会に及ぼす影響が最も大きい暗号アルゴリズムの危殆化を対象とする．個別の秘密鍵が管理運用のミスなどによって，漏洩してしまった場合はその秘密鍵で作成した署名付き文書にしか影響が及ばないのに対し，公開鍵暗号アルゴリズム（単に公開鍵暗号ともいう）が安全であるという前提が崩壊してしまう場合には，その公開鍵暗号を利用したすべての文書に影響が及ぶ．また，管理のミスなどによって，漏洩してしまった場合の対策は，認証局で鍵無効化リストを公開するなどの方法が確立しているのに対し，後者の場合は従来，対策の検討がほとんど行われてこなかった．

3.2 ETA を用いたリスク分析

3.2.1 ETA の一般的手順

本研究では，イベントツリー分析（ETA）[12] を用いて既存の署名付き文書に対してリスク分析を行う．一般的な ETA の手順は以下のとおりである．

（1）イベントツリー分析は，事故の引き金になる可能性のある異常事象を初期事象と呼び，これをリストアップする．ここでは，建物の火災の発生を初期事象として考えてみることにしよう（**図 6** 参照）．

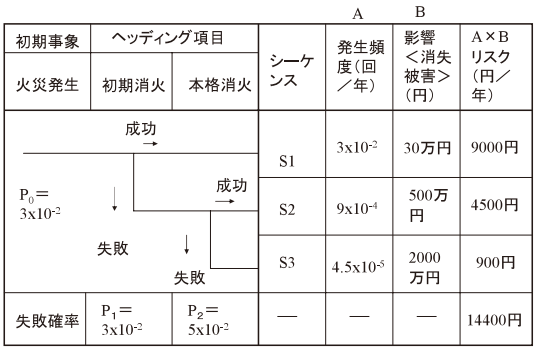


図 6 イベントツリーの一例
Fig. 6 Example of event tree.

（2）初期事象が決定すると，次に，イベントツリーの構造を決定する．ETA では，初期事象が発生したとき，それを保証する各種の安全対策（ここでは，初期消火と本格消火）をヘディング項目として図 6 に示すように記述する．

（3）次にヘディング項目に示された各種の安全対策の成否の組合せをシーケンスとして表現する．図 6 の例では，安全対策として初期消火対策と，本格消火対策とがあり，それぞれの対策の成功，失敗に応じて分岐を行い，全体で 3 つのシーケンスを得ることができる．ここで，初期消火に成功すれば，本格消火は必要ないので本格消火の部分での分岐はないようになっている．

（4）統計データやフォルトツリーなどを用い，初期事象の発生頻度（図 6 では P_0）や各種安全対策が機能しない確率（図 6 では P_1，P_2 など）を計算する．続いてこれらの値を用い，シーケンス別の発生頻度を計算する．

（5）イベントツリーのシーケンスごとに影響の推定を行う．影響としては死亡者数や平均余命の短縮年や，対策費用などが目的に応じて使い分けられる．図 6 では，火災が広がることによる損害額を用いている．

（6）次に（4），（5）の結果より，シーケンス別に両者の積をとりリスクを計算する．そして，各シーケンスのリスクを合計することにより，全体のリスクを推定している．

（7）この全体のリスクが，目標に比べ小さければ安全であるとして処理を終了し，そうでなければ対策を追加して同じ処理を続ける．

3.2.2 ETA の対象問題への適用方法

今回の暗号の危殆化の問題への ETA の適用方法も，

基本的には上記の方法と同じである．違いは，いろいろな対策案を組み込み，後でその対策案の最適な組合せを計算できるようにしている点である．以下にその方法を説明する．

既存の署名に対して十分対策がとれる段階で危殆化を発見するという前提をおいているので，公開鍵暗号が危殆化するという初期事象を設定している．ここでは危殆化は起こると仮定したので，初期事象の確率を 0.01 とした．ヘディング項目に対応する対策方法は，(a) 危殆化情報の確認，(b) 暗号危殆化情報の伝達（署名者に伝達），(c) 暗号危殆化情報の伝達（検証者に伝達），(d) 署名付き文書の再処理の試み，(e) 既存の署名付き文書に対する再処理の実施という 5 つを設定した．このような順番で，対策方法を設定した理由について説明する．

(1) まず，公開鍵暗号の危殆化を確認しなくては，次の対策方法に進むことは難しいと考え，最初の対策方法に，「暗号危殆化情報の確認機能」を設定した．これは，前述したように現状では CRYPTREC が実施する．

(2) CRYPTREC が暗号危殆化情報を確認したら，次は，確認した暗号危殆化情報を署名者・検証者に伝達する必要があるので，暗号危殆化情報の「伝達機能」を設置した．この伝達は図 5 に示すように CRYPTREC から政府に警告し，政府から企業と国民に伝達し，危殆化時対応指示を行う．また，認証局は，署名者に連絡を行う．ここで，前にも書いたように署名者は通常借金をしている人で，検証者は署名付き文書を持つ金を貸している人になる．

(3) 次に伝達を受けても，既存のデジタル署名付き文書に再処理を試みる場合と試みない場合があると考え，再処理を試みるという項目を設定した．

(4) そして最後に，実際に既存の署名付き文書に対して，再処理を実施する必要があるので，それを対策方法として設定した．

次に，ETA の分岐について説明する．

(1) 最初の対策方法である暗号危殆化情報の確認機能が失敗してしまった場合，「暗号危殆化情報の伝達」は実施できないので，以降の分岐は存在しない．

(2) 暗号危殆化情報の伝達（署名者に伝達）に失敗しても，暗号危殆化情報の伝達（検証者に伝達）に成功すれば，「再処理を試みる」を実施し，以降の対策に成功すれば，デジタル署名付き文書の安全性確保に成功する場合も考えられるので，分岐が存在する．

(3) 暗号危殆化情報の伝達（検証者に伝達）に失敗した場合，「暗号危殆化情報伝達」（署名者に伝達）が成功しても，再署名などを実施したいのは検証者なので「再処理を試みる」ことなく，デジタル署名付き文書の安全性確保に失敗してしまう．したがって以降の分岐は存在しない．

(4) 既存の署名付き文書に対する再処理の実施を試みなければ，再処理の実施はないので以降の分岐は存在しない．

以上のような考えから分岐を行い，**図 7** に示すような ETA を作成した．

危殆化確率は，対策方法ごとに設定した確率の積をとることにより算出される．損害コストは危殆化確率と影響の積をとることにより算出される．危殆化情報の確認に失敗してしまうと対策を施すことができないので，初期事象の確率と危殆化情報の確認が失敗した確率の積で表される．シーケンスごとのデジタル署名付き文書の状態は，ヘディング項目を構成する対策方法の成否の関係から定性的に分析した結果である．

3.2.3 対策案とリスクの計算方法

3.1.2 項で設定した対策方法に具体的対策案を設定するのだが，その前に，具体的対策案をどのようにしてイベントツリーに反映させるのかについて述べる．図 7 のように 3.1.2 項で示したイベントツリー分析のヘディング項目に，対策方法を対応付け，その対策方法に**表 1** に示すような具体的対策案を複数個用意する．R_l は，式 (1) に示すように，シーケンスごとのリスクであり，ここでは危殆化確率 P_l と影響 M_l の積で表している．

$$R_l = P_l \cdot M_l \tag{1}$$

l は l 番目のシーケンスを表す

$$P_l = P_0 \cdot \prod_{i=1}^{H} P_i \tag{2}$$

i は i 番目の ヘディング項目を表す

H はヘディング項目数

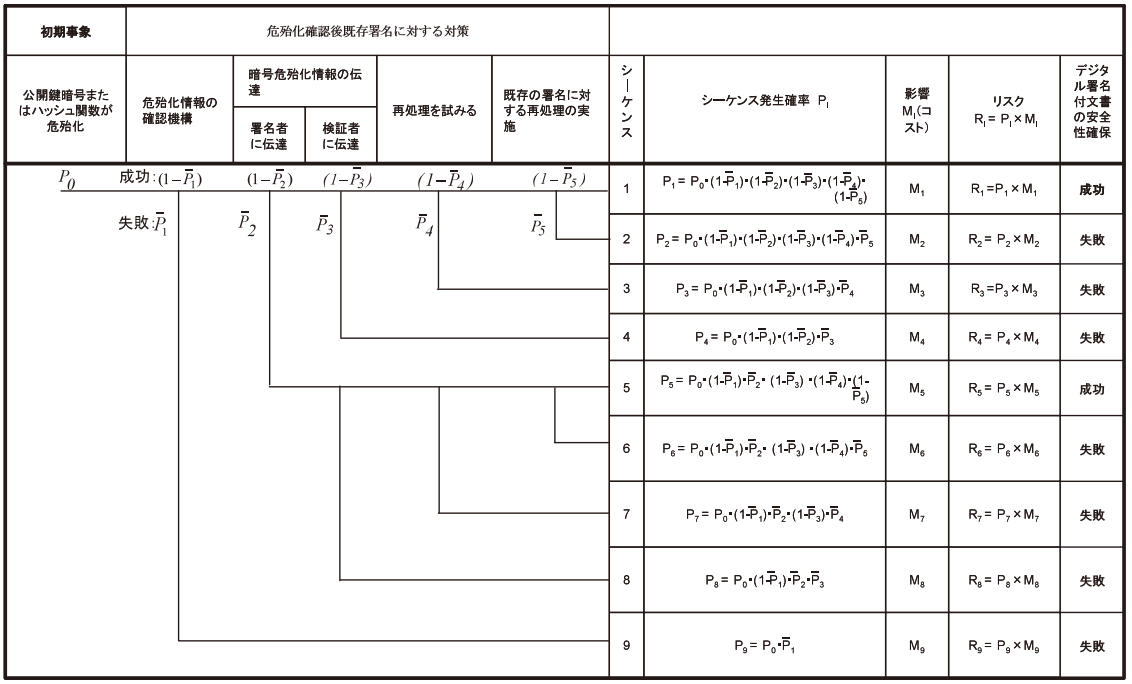
P_i は i 番目のヘディング項目の分岐確率

$$P_i = ((1 - \bar{P}_i)(1 - y_i) + \bar{P}_i \cdot y_i) \tag{3}$$

$$y_i = \begin{Bmatrix} 1：\text{ヘディング項目が下に展開} \\ 0：\text{ヘディング項目が横に展開} \end{Bmatrix}$$

P_l は，式 (2) に示すように，初期事象 P_0 と各ヘディング項目の発生確率の積で表すことができる．

たとえば，シーケンス 1 の場合だと $P_1 = P_0 \cdot (1 - \bar{P}_1) \cdot (1 - \bar{P}_2) \cdot (1 - \bar{P}_3) \cdot (1 - \bar{P}_4) \cdot (1 - \bar{P}_5)$ と表すことができる．式 (3) に示すとおり，P_i は，各ヘディング項目が，下に展開する場合と横に展開する場合を式で表したものである．M_l は，不正が生じない場合



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	$P_1 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot (1-\bar{P}_5)$	M_1	$R_1 = P_1 \times M_1$	成功
2	$P_2 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot \bar{P}_5$	M_2	$R_2 = P_2 \times M_2$	失敗
3	$P_3 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot (1-\bar{P}_3) \cdot \bar{P}_4$	M_3	$R_3 = P_3 \times M_3$	失敗
4	$P_4 = P_0 \cdot (1-\bar{P}_1) \cdot (1-\bar{P}_2) \cdot \bar{P}_3$	M_4	$R_4 = P_4 \times M_4$	失敗
5	$P_5 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot (1-\bar{P}_5)$	M_5	$R_5 = P_5 \times M_5$	成功
6	$P_6 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot (1-\bar{P}_3) \cdot (1-\bar{P}_4) \cdot \bar{P}_5$	M_6	$R_6 = P_6 \times M_6$	失敗
7	$P_7 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot (1-\bar{P}_3) \cdot \bar{P}_4$	M_7	$R_7 = P_7 \times M_7$	失敗
8	$P_8 = P_0 \cdot (1-\bar{P}_1) \cdot \bar{P}_2 \cdot \bar{P}_3$	M_8	$R_8 = P_8 \times M_8$	失敗
9	$P_9 = P_0 \cdot \bar{P}_1$	M_9	$R_9 = P_9 \times M_9$	失敗

図 7 危殆化リスクのイベントツリー
Fig. 7 Event tree for risk analysis on compromise.

$M_l = 0$ をとり，改竄ありの場合の M_l の値は，改ざんによって生じる損失額推定値を用いることとした．

下記の式 (4) は対策案ごとの対処失敗確率を p_{ij}（i は各対策方法を示し，j はその j 番目の対策案を示す）としたときの，ETA の対処失敗確率 $\bar{P}_i$ との関係を表現するものである．

$$\bar{P}_i = \sum_{j=1}^{J_i} p_{ij} \cdot X_{ij} \tag{4}$$

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

ここで，X_{ij} は，対策方法 i の j 番目の具体的対策案を表す 0-1 変数である．J_i は，対策方法 i における具体的対策案の数を表している．また，$\sum_{j=1}^{J_i} X_{ij} = 1$ は，対策方法 i において採用しうる具体的対策案は必ず 1 つであることを表している．

このように定式化した後，パラメータを設定し，後述するように危殆化対策の最適組合せを求める．具体的対策案やパラメータの値は，4.1 節の表 1 に示すとおりである．

3.3 組合せ最適化問題としての定式化

本論文では，様々な具体的対策案の組合せが存在する中で，各種の対策コストを制約条件においたとき，トータルコストに関する目的関数を最小にする最適解を導き出す．

対策方法の採用方法としては前節で述べたように 0-1 変数を用いて表現する．対策方法を採用するときには変数 X に 1 を代入し，採用しないときには，X に 0 を代入する．目的関数は，シーケンスごとの損害コストの和と各関与者の対策コストを加算したものをトータルコストとし，トータルコストが最小になるものを目的関数とする．それを定式化したものが式 (5) となる．

制約条件を政府の対策コスト，企業の対策コスト，署名者の対策コスト，検証者の対策コストとし，それら定式化したものが式 (6)，(7)，(8)，(9) である．

Minimize:

$$\sum_{l=1}^{L} R_l + \sum_{i=1}^{I} \sum_{j=1}^{J_i} C_{gij} \cdot X_{ij} + \sum_{i=1}^{I} \sum_{j=1}^{J_i} C_{cij} \cdot X_{ij} + \sum_{i=1}^{I} \sum_{j=1}^{J_i} C_{sij} \cdot X_{ij} + \sum_{i=1}^{I} \sum_{j=1}^{J_i} C_{vij} \cdot X_{ij} \tag{5}$$

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

Subject to:

表 1 具体的対策案とパラメータの設定
Table 1 Measures and parameters.

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	企業	署名者	検証者	危殆化確率
(1-1)監視機関なし（X11）	Cg11=0 円	Cc11=0 円	Cs11=0 円	Cv11=0 円	p11 = 0.5
(1-2)CRYPTREC による監視(X12)	Cg12=2000 万円	Cc12=0 円	Cs12=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	Cs13=0 円	Cv13=0 円	p13 = 0.005
2．暗号危殆化情報の伝達(署名者)					
(2-1)伝達手段なし（X21）	Cg21=0 円	Cc21=0 円	Cs21=0 円	Cv21=0 円	p21 = 0.9
(2-2)認証局による伝達（X22）	Cg22=0 円	Cc22=47 万 2200 円	Cs22=47 万 2200 円	Cv22=0 円	p22 = 0.01
(2-3)伝達機関による伝達（X23）	Cg23=4 億円	Cc23=0 円	Cs23=0 円	Cv23=0 円	p23 = 0.1
(2-4)認証局と伝達機関による伝達（X24）	Cg24=4 億円	Cc24=47 万 2200 円	Cs24=47 万 2200 円	Cv24=0 円	p24 = 0.001
3．暗号危殆化情報の伝達(検証者)					
(3-1)伝達手段なし（X31）	Cg31=0 円	Cc31=0 円	Cs31=0 円	Cv31=0 円	p31 = 0.9
(3-2)認証局による伝達（X32）	Cg32=0 円	Cc32=47 万 2200 円	Cs32=47 万 2200 円	Cv32=0 円	p32 = 1.0
(3-3)伝達機関による伝達（X33）	Cg33=4 億円	Cc33=0 円	Cs33=0 円	Cv33=0 円	p33 = 0.1
(3-4)認証局と伝達機関による伝達（X34）	Cg34=4 億円	Cc34=47 万 2200 円	Cs34=47 万 2200 円	Cv34=0 円	P34 = 0.1
4．署名付き文書の再処理を試みる					
（4-1）危殆化時対応ポリシーなし(X31)	Cg41=0 円	Cc41=0 円	Cs41=0 円	Cv41=0 円	p41 = 0.8
（4-2）危殆化時対応ポリシーあり(X32)	Cg42=1 億円	Cc42=0 万円	Cs42=472 万 2000 円	Cv42=0 円	p41 = 0.1
5．既存の署名付き文書に対する再処理					
(5-1)対策なし(X41)	Cg51=0 円	Cc51=0 円	Cs51=0 円	Cv51=0 円	p51 = 0.9
(5-2)文書に対する再署名(X42)	Cg52=0 円	Cc52=0 円	Cs52=354 万 1500 円	Cv52=354 万 1500 円	p52 = 0.2
(5-3)第三者機関による追加署名(X43)	Cg53=0 円	Cc53=0 円	Cs53=236 万 1000 円	Cv53=236 万 1000 円	p53 = 0.1

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{gij}\cdot X_{ij} \le C_g \quad (6)$$

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{cij}\cdot X_{ij} \le C_c \quad (7)$$

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{sij}\cdot X_{ij} \le C_s \quad (8)$$

$$\sum_{i=1}^{I}\sum_{j=1}^{J_i} C_{vij}\cdot X_{ij} \le C_v \quad (9)$$

ここで,
X_{ij}：対策方法を採用するかどうかを決定する変数
対策案 *i-j* を採用するなら $X_{ij}=1$，採用しないなら $X_{ij}=0$.
C_{gij}：対策方法 *i-j* を採用した場合の政府の対策コスト，ここでは，CRYPTREC の対策コストも政府の対策コストに含むことにした.
C_{cij}：対策方法 *i-j* を採用した場合の企業の対策コスト，これは，認証局と時刻認証局などの第三者機関のコストである.
C_{sij}：対策方法 *i-j* を採用した場合の署名者の対策コスト.
C_{vij}：対策方法 *i-j* を採用した場合の企業の対策コスト.
C_g：政府の対策コストにおける制約値.
C_c：企業の対策コストにおける制約値.
C_s：署名者の対策コストにおける制約値.
C_v：検証者の対策コストにおける制約値.
M_l：シーケンス l の影響の大きさ（損害額など）.
R_l：前節で述べた式 (1)–(4) によって導出されるものであり，各種の対策方法 X_{ij} の値のすべての組合せに対応したシーケンス l（エル）のリスクの値.
L：イベントツリー分析におけるシーケンスの数.
I：対策方法の数.
J_i：対策方法 i における具体的対策案の数.

4. 適 用 例

4.1 パラメータの設定

ここでは，具体的対策案を設定し，それらに対策コ

ストと対処失敗確率を設定した．以下に，対策コストと対処失敗確率の設定根拠を述べる．以下に記述する設定根拠は，暗号や，保険，法律の専門家を交えた議論から決定したものである．したがって，これらの値はかなりの合理性を持つと考えられるが，一適用例であり，評価者が必要に応じ，自分の判断で，これらのパラメータの値をいろいろに変えて演算することも可能である．

4.1.1 具体的対策案と対策コストにおけるパラメータの根拠

表 1 に示すように，具体的対策案に対策コストを設定した．対策コストのパラメータの設定根拠を以下に記述する．

① 危殆化情報の確認機構

危殆化情報の確認機構については，正式な監視機関なし，CRYPTREC による監視，CRYPTREC による監視の強化の 3 つの確認手段が考えられる．

正式な監視機関がなしの場合は，すべての関与者にコストは発生しないので，表 1 に示すように C_{g11}，C_{c11}，C_{s11}，C_{v11} とも 0 円を設定した．

現在の CRYPTREC における予算は提案内容/規模を固めるうえでの目安として，2,000 万円前後となっている[7]．このことから，政府に 2,000 万円の対策コストを設定した．企業・署名者・検証者に対しては，コストは発生しないので 0 円を設定した．CRYPTREC による監視の強化における対策コストは，現行における CRYPTREC における予算の 3 倍の値を設定してみた．この対策も政府にのみ対策コストが発生するという考え方から，企業・署名者・検証者に対しては，コストは発生しないので 0 円を設定した．

② 暗号危殆化情報の伝達機構

危殆情報の伝達としては，正式な伝達手段なし，認証機関による伝達，伝達機関による伝達，認証局と伝達機関による伝達の 4 つの伝達手段が考えられる．

正式な伝達手段がない場合というのは，口コミ，個人間のメールなどにより危殆化情報が伝達するという状況を想定している．この場合，すべての関与者にコストが発生しないので 0 円を設定した．

認証局による伝達は，認証局が危殆化情報を署名者に対して伝達する伝法である．政府は，認証局業務をやっていないものと仮定し 0 円を設定した．企業と署名者に対しては，4,722 万世帯×普及率×単価 = 4,722 万世帯 × 0.01 × 1 円 = 47 万 2,200 円を設定した．検証者にはコストがかからないので 0 円を設定した．

伝達機関による伝達は，テレビ・新聞・WEB などの媒体を利用し，伝達する方法である．政府は危殆化情報を伝達するために，テレビ・新聞・WEB を利用することによりコストがかかる．テレビ + 新聞 + WEB = 2 億円 + 1 億円 + 1 億円 = 4 億円を設定した．

メディアを利用して危殆化情報を伝達するのは政府だけなので，企業・署名者・検証者にはコストがかからないので 0 円を設定した．

認証局と伝達機関による伝達は，(2-2)，(2-3) を足し合わせたものから算出し，4 億 47 万 2,200 円とした．

③ 再処理を試みる

再処理を試みるにおいては，危殆化時対応ポリシなしと危殆化時対応ポリシありの場合が考えられる．

危殆化時対応ポリシを所持する場合は，あらかじめ公開鍵証明書内に危殆化時対応ポリシを埋め込んでおき，危殆化発生時に危殆化時対応ポリシを実施する方法が考えられる．ポリシの内容としては，文書を再作成しデジタル署名で再署名する場合と第三者機関による追加署名が考えられる．

危殆化時対応ポリシがない場合は，すべての関与者にコストがかからないので 0 円を設定した．危殆化時対応ポリシありの場合は，政府はポリシ策定にコストがかかるので 1 億円を設定した．企業・署名者に対しては，4,722 万世帯 × 普及率 × ポリシ単価からコスト = 4,722 万世帯 × 0.01 × 10 円 = 472 万 2,000 円を設定した．ただし，企業は署名者からそれに対し収入を得るので 0 円を設定した．検証者は，コストがかからないので 0 円を設定した．

④ 既存の署名に対する再処理

既存の署名に対する再処理については，対策なし，デジタル署名による再処理，第三者機関による再処理の 3 つの対策方法が考えられる．

対策なしの場合は，すべての関与者にコストがかからないので 0 円を設定した．

デジタル署名による再処理は，デジタル署名ユーザ自身が，再度，代替暗号を用いて署名することにより署名の安全性を確保する対策である．対策コストは，以下のように設定した．

デジタル署名による再処理の場合は，政府にかかるコストは 0 円を設定した．企業にかかるコストは，4,722 万世帯×普及率×デジタル署名の単価（15 円：タイムスタンプの単価が 10 円なので，それより少し上乗せした値段を設定）のコストがかかるが，署名者と検証者から利益を得るものと考えられるので 0 円を設定した．署名者と検証者は，4,722 万世帯 × 普及率 × デジタル署名の単価 ÷ 2 = 4,722 万世帯×0.01 × 15 ÷ 2 = 354 万 1,500 円をコストとして設定した．

第三者機関による再処理は，信頼できる第三者にデジタル署名を施してもらうことにより，署名の安全性を確保する対策である．対策コストは，以下のように設定した．

第三者機関による再処理の場合は，政府にかかるコストは 0 円を設定した．企業にかかるコストは，強い公開鍵暗号の準備や，依頼に基づき追加署名するのに必要なものがある．これらは，現状の時刻認証局の運用費用程度だとすると，4,722 万世帯 × 普及率 × タイムスタンプの単価（タイムスタンプの単価が 10 円程度）程度のコストがかかる．しかし，このコストは，署名者と検証者から収入として得られるものと考えられるので 0 円を設定した．署名者と検証者は，4,722 万世帯 × 普及率 × タイムスタンプの単価 ÷ 2 = 4,722 万世帯 × 0.01 × 10 ÷ 2 = 236 万 1,000 円よりコストを設定した．

4.1.2 危殆化確率におけるパラメータの根拠

表 1 に示すように各具体的対策案に危殆化確率を設定した．危殆化確率の設定根拠を以下に記述する．

署名者の署名コストが第 3 者機関によるデジタル署名の 1.5 倍になっているのは，単純にデジタル署名の単価よりタイムスタンプの単価のほうが高いためである．

1．暗号危殆化情報の確認方法

1-1．正式な監視機関なし

正式な監視機関が存在しない場合でも，学会や研究会が開かれているので，暗号危殆化情報の確認失敗確率を 0.5 に設定した．

1-2．CRYPTREC による監視

CRYPTREC が危殆化を監視しているので，0.01 を設定した．

1-3．CRYPTREC による監視の強化

CRYPTREC の監視能力をより強化した対策方法なので，0.005 を設定した．

2．暗号危殆化情報の伝達（署名者）

2-1．正式な伝達手段なし

伝達手段なしというのは，口コミ，個人間のメールなどを意味する．まったく伝達しないというわけではないので，暗号危殆化情報の伝達失敗確率を 0.9 に設定した．

2-2．認証局による伝達

認証局には，署名者の情報が登録されているので，伝達可能なことから，伝達失敗確率を 0.01 と設定した．

2-3．伝達機関（政府）による伝達

テレビや Web などを媒体とした伝達での伝達では，効果が薄いと思われることから，0.1 を設定した．

2-4．認証局と伝達機関による伝達

認証局と伝達機関による伝達の伝達失敗確率は両方が失敗するので，2-2，2-3 の積から確率を算出し，0.001 を設定した．

3．暗号危殆化情報の伝達（検証者）

3-1．正式な伝達手段なし

伝達手段なしというのは，口コミ，個人間のメールなどを意味する．まったく伝達しないというわけではないので，暗号危殆化情報の伝達失敗確率を 0.9 に設定した．

3-2．認証局による伝達

認証局には，検証者の情報は登録されていないので，伝達するのが困難であることから，1.0 を設定した．

3-3．伝達機関による伝達

テレビや Web などを媒体とした伝達での伝達では，認証局などから直接連絡する場合に比べ効果が薄いと思われることから，0.1 を設定した．

3-4．認証局と伝達機関による伝達

3-2，3-3 の積から確率を算出し，伝達失敗確率を 0.1 に設定した．

4．署名付き文書に対し再処理を試みる

4-1．危殆化時対応ポリシなし

対応ポリシがあらなじめ設定されてなければ，ユーザの自由意志により再処理を試みるのか試みないのかが決定されるため，再処理を試みない確率が高いことから再処理非実行確率 0.8 に設定した．

4-2．危殆化時対応ポリシあり

こういうことがあれば再処理をするということに承認していることになり，再処理を試みる確率が向上すると考えられるので，0.1 を設定した．

5．既存の署名付き文書に対する再処理

5-1．対策なし

危殆化が発生した際にも，両者の合意などにより契約が成立する場合も考えられる．全体の 1 割は，署名の効力が失われても契約が成立すると仮定し，再処理失敗確率を 0.9 に設定した．

5-2．文書への再署名

ほとんどの再署名が成功すると思われる．ただ，利用者が 1 度に認証局を利用し負荷が集中した場合を考慮し，0.02 を設定した．

5-3．第三者機関による追加署名

利用者の要求に対して，第三者が再処理を行う場合，利用者が 1 度に認証局を利用し，再署名が間に合わない確率より，第三者機関の処理が間に合わない確率のほうが低いと考えられるので，0.01 を設定した．

デジタル署名付き文書が改竄されたときの影響 M_l

表 2 普及率を変化させた場合の最適化結果
Table 2 Optimization result of when diffusion rate has been changed.

対策方法	具体的対策案	0.00001	0.0001	0.001	0.01	0.1	0.3	0.5
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(X21')	○	○					
	(3-2)認証局による伝達(X22)'							
	(3-3)伝達機関による伝達(X23)'			○	○	○	○	○
	(3-4)認証局と伝達機関による伝達(X24)'							
4. 署名付き文書に再処理を試みる	(4-1)危殆化時対応ポリシーなし(X31)	○	○					
	(4-2)危殆化時対応ポリシーあり(X32)			○	○	○	○	○
5. 既存の署名付き文書に対する再処理	(5-1)対策なし(X41)							
	(5-2)文書への再署名(X42)							
	(5-3)第三者機関による追加署名(X43)	○	○	○	○	○	○	○
トータルコスト		24,525,312 円	245,253,124 円	1,804,774,226 円	13,347,616,090 円	128,436,160,904 円	384,188,482,712 円	639,940,804,520 円
損害コスト		24,520,590 円	245,205,904 円	1,283,829,826 円	12,778,172,090 円	127,781,720,904 円	383,345,162,712 円	638,908,604,520 円

のパラメータを設定する．3.2 節で示した影響 M_l は，総世帯数と電子借用書の普及率と一世帯あたりの負債現在高の積から算出した[10]．デジタル署名付き文書が改竄されたときの影響 M_l とする．

デジタル署名付き文書の影響 M_l

M_l = 4,722 万件 × 524 万円 × 0.01 = 2 兆 4,743 億 2,800 万円

ここで設定した電子借用書の普及率 0.01 は基準値であり，このパラメータを振ることにより，電子借用書が世の中に多く普及している場合としていない場合の影響を考察する．これについては，次節で述べる．

4.2 最適解の求解

前節までで行ったパラメータ設定と定式より本手法を適用し，総当たり法により，対策案の最適組合せの求解を行った．この結果，次のような解が求められた．

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としては，

(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あり，
(5-3) 第三者機関による追加署名，

が採用され，以下のような結果が算出された．

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

4.3 結果の分析

普及率を変化させた場合の最適化結果をまとめたものを，**表 2** に示す．表 2 より普及率が 0.0001 を超えたあたりから，様々な対策が必要になることが分かる．すべての普及率において (5-3) の対策が選ばれている．これは，(5-3) の対策は (5-2) の対策に比べて対策コストも安く，対策効果が大きいためこのような結果になった．一見すると (5-2) の対策案は不要のように思えるが，対策案をリストアップした時点ではこれが分からなかったので対策案として残っているものである．

制約条件を設定した場合の最適化結果

基準値として設定した電子借用書の普及率 0.01 の場合に，制約条件を設定した最適化結果を**表 3** に示す．

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

表 3 制約条件値を変化させた場合の最適化結果
Table 3 Optimization result of when constrained condition value is changed.

対策方法	具体的対策案	基本ケース	ケース①	ケース②
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(X21')		○	○
	(3-2)認証局による伝達(X22)'			
	(3-3)伝達機関による伝達(X23)'	○		
	(3-4)認証局と伝達機関による伝達(X24)'			
4. 署名付き文書に再処理を試みる	(4-1)危殆化時対応ポリシーなし(X31)			
	(4-2)危殆化時対応ポリシーあり(X32)	○	○	○
5. 既存の署名付き文書に対する再処理	(5-1)対策なし(X41)			
	(5-2)文書への再署名(X42)			
	(5-3)第三者機関による追加署名(X43)	○	○	○
トータルコスト		1,804,774,226 円	22,888,560,376 円	23,850,621,160 円
損害コスト		1,283,829,826 円	22,759,116,376 円	23,741,177,160 円

ケース ①

各関与者の制約条件を政府：4 億円，企業：2,000 万円，署名者：500 万円，検証者 200 万円と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

ケース ②

各関与者の制約条件を政府：1 億円，企業：1,000 万円，署名者：100 万円，検証者：100 万円と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

普及率を変化させた場合の最適化結果を見てみると，普及率を 0.00001〜0.0001 においては，(5-3) 以外の対策は採用されていないことが分かる．普及率をあげていくと，普及率 0.001 から変化が生じる．(5-3) の対策だけではなく，新たに (1-2)，(3-3)，(4-2) が採用される．さらに，普及率をあげていき，普及率を 0.3 とした場合を見てみると，(1-3)，(2-1)，(3-3)，(4-2)，(5-3) といった対策案が採用される．

このことから，デジタル署名が普及していない現時点では，対策を講じる意味は薄いかもしれないが，徐々にデジタル署名が普及したときに，危殆化が発生した場合は，社会に多大な影響を及ぼす可能性が高い．

次に，制約条件を設定した場合の最適化結果について検討する．まず，基本ケースとケース ① を比較する．採用されている対策案を比較すると，基本ケースでは，CRYPTREC による監視の強化が採用されているが，ケース ① では，CRYPTREC による監視が採用されている．さらに，基本ケースでは，(3-3) 伝達機関による伝達が採用されているが，ケース ① では，(3-1) 伝達手段なしが採用されている．基本ケースとケース ① のトータルコストを比較してみると暗号危殆化情報の確認機能と暗号危殆化情報の伝達機能の重要性が分かる．

さらに，ケース ② を見てみると，(1-1) 正式な監視機関なしが採用されており，ケース ② とケース ① のトータルコストと比較してみると，10 億円近く差があることが分かる．

コストを抑える方向であるにもかかわらず，トータルコストが大きくなるのは，各エンティティのコストを抑えた分，対策コストはかかるが対策効果の高い対策は採用されなくなり，損害コストが大きくなるためである．したがって，対策コストを絞りすぎない方が，社会全体としては望ましいことが分かる．

基本ケースのように，十分対策費用がある場合には，

暗号の危殆化を確実に伝達する暗号危殆化情報の伝達機能と，危殆化を確認した後の対応を記した危殆化時対応ポリシと，既存の署名付き文書に対する再処理について充実させる必要があるといえる．特に危殆化時対応ポリシについては，対策コストをかけても行う必要がある．また，CRYPTREC もより対策コストをかけ，監視をさらに強化していくことが望ましいといえる．

5. まとめと今後の展開

本論文では，公開鍵暗号の危殆化が近く生じることが明確になった場合に，既存の署名付き文書の証拠性を確保するために必要な対策案の最適な組合せを求める方法を提案した．あわせて，1 つのケースにおける最適な対策案を示し，デジタル署名が普及した場合に，社会にどのような影響があり，どのような対策を講じる必要があるかを論じた．

2 章でも述べたとおり，専門家と議論を行いパラメータの値を適切なものにするよう努力したが，パラメータの値については，どうしても主観をともなう．しかし，感度解析などを行うことにより，パラメータの値が少々変わっても必要な対策などについては明確な点があり，少なくとも次のようなことはいえると考える．

(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) 署名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) 署名付き文書の再処理方法について今から検討しておく必要がある．

危殆化時対応ポリシは，最適化結果から特に重要であることが分かった．このような指摘，特に危殆化時対応ポリシの必要性については，従来提案されていなかったものである．

今後は，専門家の意見だけでなく，政府機関，企業，署名者，検証者などの関与者の意見もフィードバックする必要があると考えられることから，これらを実現するために，著者らが開発している多重リスクコミュニケータ（MRC）[11] の適用も行っていく予定である．

また，電子公証サービスに対しても本提案方式を適用する予定である．

謝辞 最後に，パラメータの設定などにご助言をいただいた赤井健一郎氏，猪俣敦夫氏，岡本栄司氏，長嶋潔氏，藤村明子氏（あいうえお順）に感謝申し上げる．なお，本研究は一部，科学技術振興機構社会技術開発センター「情報と社会」計画型研究開発「高度情報社会の脆弱性の解明と解決」の研究として行われたものである．

参 考 文 献

1) 佐々木良一，吉浦 裕，洲崎誠一，宮崎邦彦：デジタル署名付文書の長期的安全性に関する考察，情報処理学会 Computer Security Symposium2003 (CSS2003) (2003-5).
2) 伊藤信治，宮崎邦彦，本多義則，谷川嘉伸：電子署名の長期保証に関する一考察，*The 2004 Symposium Cryptography and Information Security* (*SCIS2004*), pp.527–532 (2004-1).
3) 電子署名文書長期保存に関するガイドライン，電子商取引推進協議会 (2002-3). http://www2.ecom.jp/report/pdf/H13/h13_cert3.pdf
4) 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，技術と社会倫理研究会（SITE）(2004-1).
5) 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金融研究，Vol.22, No. 別冊第 1 (2003-6). http://www.imes.boj.or.jp/japanese/kinyu/2003/yoyaku/kk22-b1-2.html
6) Wang, X., Yin, Y. and Yu, H.: Collision Search Attacks on SHA1 (Feb. 13, 2005). http://www.infosec.sdu.edu.cn/sha-1/shanote.pdf
7) 暗号技術関連の調査に関する公募 Q&A. http://www.ipa.go.jp/security/enc/CRYPTREC/fy13/cryptrec20010921_koboqa.html
8) 株式会社三菱総合研究所：暗号危殆化に関する調査報告 (2005-4). http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/documents/crypt_compromize.pdf
9) 田村裕子，宇根正志，岩下直行，松本 勉，松浦幹太，佐々木良一：デジタル署名の長期利用について. http://www.imes.boj.or.jp/japanese/kinyu/2005/kk24-b1-3.pdf
10) 総務省統計局：家計調査報告（二人以上の世帯）平成 16 年平均結果の概況（貯蓄・負債編結果）. http://www.stat.go.jp/data/sav/2004np/pdf/gk21.pdf
11) 佐々木良一，石井真之，日高 悠，矢島敬士，吉浦裕，村山優子：多重リスクコミュニケータの開発構想と試適用，情報処理学会論文誌，Vol.46, No.8, pp.2120–2129 (2005).
12) 独立行政法人原子力安全基盤機構：高速増殖炉の確率論的安全評価（レベル 1 PSA）に関する報告書. http://www4.jnes.go.jp/katsudou/seika/2003/04_kaibu_0052/04_kaibu_0052.htm

13) CRYPTREC（Cryptography Research and Evaluation Committees）.
http://www.cryptrec.jp
14) 佐々木良一，吉浦　裕，手塚　悟，三島久典：インターネット時代の情報セキュリティ，p.66, 共立出版 (2000).

(平成 19 年 6 月 11 日受付)
(平成 19 年 12 月 4 日採録)

藤本　　肇（正会員）

2005 年東京電機大学工学部情報通信工学科卒業，同年同大大学院情報メディア学修士課程入学．情報セキュリティの研究に従事．2007 年同大学院修了．同年ニッセイ情報テクノロジー株式会社に入社．

上田　祐輔

2003 年東京電機大学工学部第一部情報通信工学科卒業．2005 年同大学大学院工学研究科情報通信工学専攻修士課程修了．この間情報セキュリティの研究に従事．現在，アマノタイムビジネス（株）にて時刻認証サービス等の企画開発に従事．情報処理学会情報規格調査会 SC27/WG2 小委員会委員．

佐々木良一（フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より東京電機大学工学部教授，2007 年 4 月より未来科学部教授．工学博士（東京大学）．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．2007 年総務大臣表彰．2007 年度『情報セキュリティの日』功労者表彰等．著書に，『インターネットセキュリティ入門』（岩波新書，1999 年）等．情報処理学会フェロー．情報処理学会コンピュータセキュリティ研究会顧問．日本セキュリティ・マネジメント学会常任理事，情報ネットワーク法学会理事長，日本学術会議連携会員，日本ネットワークセキュリティ協会会長．