A Proposal of Risk-Communicator for Cost-effective Selection of Digital Forensic Investigation

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

デジタルフォレンジック調査選定に資するリスクコミュニケータの提案
A Proposal of Risk-Communicator for Cost-effective Selection of Digital Forensic Investigation

佐々木 葵* 村上 弘和† 天笠 智哉* 井坂 佑介*
奥村 紗名* 堀川 博史* 大木 哲史* 西垣 正勝*
Aoi Sasaki Tomoya Amagasa Yusuke Isaka Sana Okumura Hiroshi Horikawa
Hirokazu Murakami Tetsushi Ohki Masakatsu Nishigaki

あらまし セキュリティインシデントに的確に対処するためには，フォレンジック調査が必要となる．フォレンジック調査は多くの場合，専門の調査会社によって請け負われ，依頼者と調査会社の間でリスクコミュニケーションを通じて調査内容を検討する．しかし，依頼者と調査会社では有する知識やバックグラウンドが異なり，リスクコミュニケーションがうまくいかない現状がある．依頼者と調査会社には，共通の目標として「費用対効果が最良となる調査内容を選定する」ことがあるが，リスクコミュニケーションがうまくいかないことにより，目標が達成されないという問題がある．そこで，本稿では，フォレンジック調査選定を支援するリスクコミュニケータを提案する．本リスクコミュニケータは，依頼者と調査会社のやりとりを仲介・調停し，最も費用対効果が高い調査を自動的に選出するものである．また，リスクコミュニケータの実装に際して，フォレンジック調査選定を離散最適化問題として定式化する．そして，提案手法の利用可能性を机上検討により確認する．

キーワード フォレンジック，リスクコミュニケータ，離散最適化問題，インシデントレスポンス

1. はじめに

情報化社会の本格化に伴い，セキュリティインシデント（以下，インシデント）が多発している．組織では，平素からのセキュリティ確保が必須であり，かつ，万一の際には迅速かつ適切な対応が求められる．インシデントが発生した際，同様の原因によるインシデントの再発を防ぐには適切な対策を講じる必要があるが，その検討にはデジタルフォレンジック調査（以下，フォレンジック調査）に基づく詳細な原因究明が不可欠である．加えて，インシデントの対応には，行政機関等への報告義務や利用者への説明責任が発生する．情報漏洩を伴うインシデントでは，個人通知の義務や顧客への補償が生じる．これらを果たすためには，フォレンジック調査に基づく被害範囲や被害者の特定が不可欠となる．このように，インシデントの発生に対して適切な対策・対応が行えなければ，インシデントの再発リスクを抱え続けるだけでなく，社会的責任を問われる結果となり，それらがブランドイメージの低下，株価の下落，顧客の離反を招き，被害組織にとって大きな損失となる．したがって，インシデントの原因および被害範囲を究明するためのフォレンジック調査が担う役割は甚大である．

フォレンジック調査には，当然のことながら相応のコストが発生する．よって，調査内容の選定は，セキュリティ投資の考え方に従って費用対効果が最良となるようになされるべきである．多くの場合，フォレンジック調査は専門の調査会社によって請け負われるため，依頼者と調査会社の間でリスクコミュニケーションを通じて調査内容が決定されることとなる．リスクコミュニケーションとは，“リスクについて直接・間接に関係する人たちが意見を交換し，合意を形成する過程”である[7]．しかし，現実には，円滑なリスクコミュニケーションの実現は容易いものではない．なぜなら，依頼者と調査会社は，一般に専門家と非専門家の関係にあり，次の①②の障壁が生じるためである．

①依頼者はフォレンジック調査に関する知見に乏しく，調

* 静岡大学 〒432-8011 静岡県浜松市中区城北３丁目５－１. Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011, Japan.

† CyCraft Japan 〒100-0004. 東京都千代田区大手町１丁目９-２ 大手町フィナンシャルシティグランキューブ３階 Global Business Hub Tokyo. CyCraft Japan, 1-9-2 Otemachi, Chiyoda, 100-0004, Japan.

査会社の説明を適切に理解することが難しい.
②調査会社は依頼組織の経営方針に関する知見に乏しいため，依頼者側の状況を正確に聴取することが難しい. 互いの有する知識やバックグラウンドが異なるために, 意思疎通に困難が生じ,「費用対効果が最良となる調査内容を導く」というリスクコミュニケーションの目標達成が阻害されてしまう.

上述の問題に対して，本稿では，フォレンジック調査選定を支援するリスクコミュニケータ（以下，コミュニケータ）を提案する. 本コミュニケータは，依頼者と調査会社の間に位置し，両者のやりとりを仲介・調停するものである. 本コミュニケータの実現に際し，フォレンジック調査選定を離散最適化問題として定式化する. 具体的には，フォレンジック調査における「残存リスク」と「調査費」をモデル化し, その総和が最小となる調査内容を導くことによって, フォレンジック調査の費用対効果の最大化を図る. 本コミュニケータは, 入力として, 依頼者から「調査対象」,「資産価値」,「調査要件データ」の情報を，調査会社から「調査費単価」を得る. そして，これらの入力を基に離散最適化問題を解き, 出力として最も費用対効果が高いフォレンジック調査内容を選出する. 本コミュニケータを用いることで，依頼者と調査会社は，費用対効果が最良となる調査内容を自動的に求めることが可能となる. 本稿では，典型的な企業を想定して机上検討を行うことにより, 提案手法の利用可能性を確認する.

2. 課題設定

2.1 リスクコミュニケーションにおける問題

フォレンジック調査の選定には，安全性，コストなどの複数の指標が存在し，どの指標を重視するかは意思決定関与者の選好の問題となる. フォレンジック調査は多くの場合，専門の調査会社によって請け負われ，依頼者と調査会社の間でヒアリングを通して調査内容の選定が行われる. すなわち, フォレンジック調査における意思決定関与者は依頼者と調査会社であり, 両者の間でリスクコミュニケーションが試行される. リスクコミュニケーションが成立すれば, 意思決定関与者間で納得のいく形で調査内容が決定する. しかし，現状として，リスクコミュニケーションがうまくいかない場合が多い.

例えば, 調査会社の技術者が調査内容を技術的に説明しても，依頼者にうまく伝わらないことがある. 一般に，依頼者は経営陣であり, フォレンジック技術に精通していない場合がほとんどである. そのため，依頼者は技術的な説明を受けても理解につながらず,「どのくらいの出資でどういった効果が見込まれるのか」という経済的な評価へと帰結させることが難しい. その一方で，調査会社の技術者もまた一般に, 経営や経済には精通していない場合がほとんどであり, フォレンジック調査の効果を経済的な観点から説明することが難しい. 仮に技術者が経営や経営に対する素養を有していたとしても, 技術者は自身の所属先ではない依頼組織の経営方針を十分に理解しているわけではないため, 依頼者の望む塩梅の調査を見定めることは容易ではない. また，そもそもの問題として，現状ではフォレンジック調査の費用対効果を定量的に示す手立て自体が乏しい. このように，互いの有する知識やバックグラウンドが異なることにより, リスクコミュニケーションが円滑に進まないという現状がある（課題 1）. フォレンジック調査選定におけるリスクコミュニケーションが阻害された結果，安全性に劣後した合意形成（調査会社側が技術的観点から更なる調査を薦めているにも関わらず, 依頼者がその必要性を理解できずに追加調査に承服しなかった場合，必要な調査が未済となる），あるいは，経済性に劣後した合意形成（一通りの調査が終了したにも関わらず，依頼者側が経営的観点から更なる調査を求めた場合, 調査会社には依頼者がどのような情報を欲しているのか演繹できず, 末梢的な調査が追加されてしまう）に至ってしまう.

また，フォレンジック調査はその性質上，調査前に調査によって見込まれる成果を推測することが難しく, 調査にかけた工数に対して調査の効果が保証される訳ではないという現状がある（課題 2）. このようなフォレンジック調査の性質によって, 依頼者と調査会社の間のリスクコミュニケーションが阻害された結果，曖昧な合意形成（調査会社から依頼者に「決められた期間内に可能な限りの調査をする」という形で調査方針が提示されることになり，依頼者は調査の妥当性や費用対効果を評価できない）に至ってしまう.

2.2 関連研究

情報セキュリティを確保するためのリスクマネジメントについて記述した規格等は, 国内外を問わず随時提唱され続けてきた. 現行の国際規格としては，ISO/IEC 27001 [1]およびISO/IEC 27005 [2]がある. ISO/IEC 27001 は, ISMS 認証のための要求事項を示す規格であり，ISO/IEC 27005 は, 情報セキュリティのリスクマネジメントに関するガイドラインである. しかし，このような規格やガイドラインがあるにもかかわらず，リスク基準の評価やセキュリティ対策の選定においては, 実施者の主観を排除できないという課題が存在する[3]. これは，評価や選定の結果が実施者に依存することを意味している.

この課題を解決する手法として，資産・脅威・対策案の関係をモデル化し, セキュリティ対策案選択問題を定式化することによってセキュリティ対策の最適な組み合わせを論理的に求める手法[4][5]が提案されている. また，文献[6]では，ISO/IEC 27001 の改定に伴い，資産，脅威の特定を前提としないセキュリティ対策選定手法が提案されている（文献[6]は，文献[4][5]の手法の簡易版と捉えることもできる）.

組織の目的に応じて, 何をもってセキュリティ対策の最適な組み合わせとするかが異なる. このため，複数の組織が関与する場合には，手法[4][5][6]などの手法を用いて

セキュリティ対策の最適な組み合わせを求める前に，組織間のリスクコミュニケーションによって「最適なセキュリティ対策」の定義を合意することから始める必要がある．情報セキュリティ分野においてリスクコミュニケーションを支援する手法としては，多重リスクコミュニケータ[7]がある．この手法は，目的が異なる複数の組織の合意形成を醸成しながら，すべての組織が納得する形で最適なセキュリティ対策を選定するものである．

上記のように，セキュリティ対策選定を支援する手法およびリスクコミュニケータは存在する．しかし，フォレンジック調査選定支援に焦点を当てた形での手法ならびにリスクコミュニケータを提案する研究は，筆者が調べた限り存在しない．そこで本稿では，フォレンジック調査の選定を支援するリスクコミュニケータを提案する．本コミュニケータにより，最も費用対効果が高い調査内容を導くことが可能となる．リスクコミュニケータの実現にあたり，フォレンジック調査選定をモデル化し，離散最適化問題として定式化する．

3. 問題解決のアプローチ

本稿では，フォレンジック調査選定を支援するリスクコミュニケータを提案する．本コミュニケータは，依頼者と調査会社のやりとりを仲介・調停し，最も費用対効果が高い調査内容を選定する．本コミュニケータの実現に際し，フォレンジック調査選定を離散最適化問題として定式化する．

2.1 節の課題 1 で述べたように，依頼者と調査会社の間には知識やバックグラウンドのギャップがあるため，フォレンジック調査の効果と対価を依頼者と調査会社の双方にとって明確な形で数値化する必要がある．そこで提案手法では，フォレンジック調査の効果を「残存リスク」という形で，フォレンジック調査の対価を「調査費」という形で，それぞれを金銭的にモデル化する．「金額」という共通の尺度で両者を表現することによって，「残存リスクと調査費の総和が最小となる調査内容を導く」ことによって，「費用対効果が最大となるフォレンジック調査を選出する」ことが達成される．

フォレンジック調査の対価を「調査費」としてモデル化するにあたっては，「調査費単価」と「調査工数」の積によって対価を数値化（金額化）する．

フォレンジック調査の効果を「残存リスク」としてモデル化するにあたっては，2.1 節の課題 2 で述べたフォレンジック調査の曖昧性が残存リスクの数値化（金額化）を困難にしている．そこで提案手法では，「資産価値」，「調査対象」，「調査材料」については調査に入る段階で確定しているという前提を置く．すなわち，フォレンジック調査の具体ケースを扱うというアプローチでフォレンジック調査の曖昧性の排除を試みる．また，「調査究明」については，その成果（究明率）は調査材料と調査工数に比例するという前提を置く．すなわち，フォレンジック調査の進捗を平滑化して捉えるというアプローチでフォレンジック調査の曖昧性の排除を試みる．これら 4 つの前提を以下に詳述する．

1. 資産価値に関する前提：提案手法の適用対象は，資産価値が把握できている組織である．資産価値と脅威発生率の積により，リスクの大きさを数値化できる．
2. 調査対象に関する前提：提案手法の適用対象は，インシデントレスポンスの手順化がなされている組織である．インシデントが発生してしまった際には，手順に則った組織内の初動対応によって，インシデントの種別に見当を付けることができる．（インシデントに関する詳細な分析は組織内では実施できないため，調査会社に別途依頼する必要がある．）
3. 調査材料に関する前提：調査会社がインシデントの原因・被害範囲を詳細分析するにあたって必要となる調査材料（各種のログデータ等）は，インシデントの種別ごとに定まっている．
4. 調査究明に関する前提：十分な調査材料に対して十分な調査工数をかければ，インシデントの原因および被害範囲を 100%究明できる．究明率は，調査材料の充足率（分析に必要となる調査材料の内，どれくらいの調査材料を調査会社に提供できるか）と調査工数（調査会社に提供された調査材料をすべて分析するために必要となる工数に対し，実際にどれくらいの工数をかけて調査を行うか）の充足率の積に比例する．

なお，実際のインシデント対応においては，フォレンジック調査費の後に，調査結果応じた対策が取られることになる．また，1 つの調査を終えた後に，追加調査を行う場合もある．これらの対策費や追加調査費の多寡は，その組織の開発・契約状況や経営層の判断によって変動する．本稿では，提案手法にはそれらを含めず，初動対応直後の本調査にのみ焦点を当てている．

4. フォレンジック調査選定の定式化

4.1 表記

フォレンジック調査選定の定式化を行うにあたり，定式化に用いる表記について説明する．

- R（Residual Risk：残存リスク）：調査の実施後，なお残されるリスクの資産換算価値（円）．
- V（Asset Value：資産価値）：組織の保有する資産の価値（円）．
- R_T（Residual Threat Rate：脅威残存率）：調査の実施後，なお残される脅威の割合（%）．
- R_I（Investigation Progress Rate：究明率）：調査によって究明されるインシデントの原因（および被害範囲）の割合（%）．脅威除去率と等しい．
- R_D（Data Coverage Rate：調査材料充足率）：分析に必要な調査材料の内，実際にどれくらいのデー

タが揃っているかの割合（%）.

- D_R（Data Required：調査要件データ）：分析に必要となる調査材料.
- D_S（Data Supplied：提供可能データ）：依頼者から調査会社に提供される調査材料.
- R_L（Labor Sufficiency Rate：調査工数充足率）：調査に必要な作業工数の内，実際にどれくらいの工数をかけるかの割合（%）
- L_R（Labor Required：必要工数）：依頼者から提供された全データを分析するために必要となる調査工数（人日）
- L_S（Labor Supplied：発注工数）：依頼者から調査会社に発注される調査工数（人日）
- C（Investigation Cost：調査費）：調査にかかる総費用（円）
- U_C（Unit Investigation Cost：調査費単価）：調査にかかる 1 人日あたりの単価（円/人日）

表 1 データの種類と調査の対象との対応表

		調査に用いるデータの種類（調査要件データ）							
		イベントログ	タスクスケジュールログ	レジストリハイブファイル	メモリ	プリフェッチファイル	削除履歴	Webサーバログ	DBサーバログ
調査の対象	SQLインジェクション攻撃	-	-	-	-	-	-	○	○
	ディレクトリトラバーサル攻撃	○	-	-	-	-		○	-
	XSS攻撃	-	-	-	-	-		○	-
	認証情報の漏洩	○	-	-	-	-	-	○	-
	不正アクセス	○	-	-	-	-		△	○
	クレデンシャルダンプ	○	○	○	○	○	○	-	-
	RAT	○	○	○	○	○	○	-	-
	ランサムウェア	○	○	○	△	○	○	-	-
	脆弱性の利用	△	-	-	-	-	-	△	△

（○：必要なデータ，△：必ずしも必要ではないデータ，-：不要なデータ）

4.2 定式化

提案手法では，フォレンジック調査の効果と対価を，それぞれ，「残存リスクR（円）」，「調査費C（円）」という形でモデル化する．残存リスクRと調査費Cの和が最も小さくなるような調査内容が，最も費用対効果が高いフォレンジック調査である．

$$\min(R + C) \quad (1)$$

残存リスクとは，調査を実施した後になお残るリスクであり，そのリスクによって組織が被り得る損害（期待値）の資産換算価値Rとして数値化（金額化）する．残存リスクの大きさは，一般に，当該リスクが引き起こされる確度と当該リスクが影響を及ぼす資産の大きさに比例する．前者は，脅威がどれだけ残っているかに依存し，これを「脅威残存率R_T（%）」と表す．後者は，組織が保有する総資産であり，これを「資産価値V（円）」と表す．すなわち，残存リスクRは資産価値Vと脅威残存率R_Tの積により求められる．ここで，3 章で置いた前提 1 より，依頼者は自組織の資産価値Vを把握している．

$$R = VR_T \quad (2)$$

フォレンジック調査によってインシデントの原因が判明したならば，適切な対策が講じられてその脅威が除去される．調査が不十分であった場合には，原因が特定されず，脅威が残存する．よって，「フォレンジック調査によりインシデントの原因がどの程度究明されたのか」という割合を用いて，「フォレンジック調査によって脅威がどの程度除去されたのか」という割合を示すことができる．前者を「究明率R_I（%）」，後者を「脅威除去率」として表す．「脅威の残存」は「脅威の除去」の排反事象であるため，脅威残存率R_Tは究明率R_Iを用いて次式で表現できる．

$$R_T = 1 - R_I \quad (3)$$

3 章で置いた前提 4 より，究明率は，調査材料の充足率（分析に必要となる調査材料の内，どれくらいの調査材料を調査会社に提供できるか）と調査工数（調査会社に提供された調査材料をすべて分析するために必要となる工数に対し，実際にどれくらいの工数をかけて調査を行うか）の充足率の積としてモデル化できる．前者を「調査材料充足率R_D（%）」，後者を「調査工数充足率R_L（%）」と表すと，究明率R_Iは次式となる．

$$R_I = R_D R_W \quad (4)$$

3 章で置いた前提 2 より，発生したインシデントの種別については依頼者側で特定ができており，かつ，3 章で置いた前提 3 より，調査会社がインシデントの原因・被害範囲を詳細分析するにあたって必要となる調査材料（各種のログデータ等）はインシデントの種別ごとに定まっている．

このため提案手法においては, 依頼者が調査会社に詳細分析を依頼する時点で,「分析に必要となる調査材料」が判明している. その一方で, 依頼者がどの種類のログを残しているのか, 攻撃がログ自体にまで及んでいるか否か等によって,「依頼者から調査会社に提供できる調査材料」は異なってくる. 前者を「調査要件データD_R」, 後者を「提供可能データD_S」と表すと, 調査材料充足率R_Dは次式となる.

$$R_D = \frac{D_S}{D_R} \quad (5)$$

調査要件データD_Rならびに提供可能データD_Sは, それぞれ, 種別とサイズによってモデル化される. しかし, 提案手法においては簡便性に鑑み, 調査材料充足率R_Dの算出についてはデータ種別のみを用いることとした. 例えば, SQL インジェクション攻撃の調査には, 一般的に, Web サーバログと DB サーバログの 2 種類が必要であるが, 依頼者が提供可能な調査材料が Web サーバログの 1 種類のみであった場合, D_R=2, D_S=1, R_D=1/2 となる. なお, 3 章の前提 3（調査要件データはインシデントの種別ごとに定まっている）に関しては, 専門家の知見の下, 調査要件データと攻撃種別の体系化を行った. その結果を表 1 に示す. 提案手法では, 表 1 の情報を基に, 調査要件データと提供可能データの種類数をそれぞれ計数し, 調査材料充足率を算出する.

提供可能データが調査会社に渡され, 調査会社の技術者によって詳細分析が進められていく. すなわち, 分析に要する調査工数は, 分析の対象である提供可能データD_Sのデータサイズによって定まる. 提供可能データの総量を技術者の分析速度で除すことによって,「提供可能データのすべてを分析するために必要となる調査工数」が得られる. その一方で, 依頼者がどの種類のログを残しているのか, 攻撃がログ自体にまで及んでいるか否か等によって,「依頼者から調査会社に提供できる調査材料」は異なってくる. 前者を「調査要件データD_R」, 後者を「提供可能データD_S」と表すと, 調査材料充足率R_Dは次式となる. 提案手法では, 専門家の知見の下, 技術者の平均的な分析速度を 20 MB/人日と設定した.

$$R_L = \frac{L_S}{L_R} \quad (6)$$

調査費Cは,「調査費単価D_R（円/人日）」と「発注工数L_S（人日）の積により求めることができる.

$$C = D_R L_S \quad (7)$$

以上をまとめると, 式 1 は次の通りとなる.

$$\min\left\{V\left(1 - \frac{D_S}{D_R} \cdot \frac{L_S}{L_R}\right) + D_R L_S\right\} \quad (8)$$

依頼者の組織に複数の資産があり, 当該インシデントに関する残存リスクが複数の資産に跨る場合は, 資産の数だけ式 8 を積算する形になる. 式 8 を構成する各変数に対し, 添字 iを付記することによって資産の種別を表記すると, n個の資産を考慮した場合のフォレンジック調査選定問題は, 次式によって定式化できる. 式 9 を解くことによって, 最も費用対効果が高い調査内容が求められる.

$$\min\left\{\sum_i V_i\left(1 - \frac{D_{Si}}{D_{Ri}} \cdot \frac{L_{Si}}{L_{Ri}}\right) + \sum_i D_{Ri} L_{Si}\right\} \quad (9)$$

なお, 式 3 においては, 脅威残存率R_Tの定義域を$0 \leq R_T \leq 1$（$0\% \leq R_T \leq 100\%$）として定式化を行った. しかし, 現実には, インシデントの原因（や被害範囲）が 100%究明できたとしても, 脅威残存率がゼロにならない場合がある. 例えば, 風評被害は, 脅威残存率R_Tの定義域が$0 \leq R_T \leq 1$とならない. Gemalto 社の調査によると, 情報漏洩の被害企業に対して, 64%の消費者がその企業との取引に対して不安を抱き, 代替となるサービス利用を検討すると言う[8]. すなわち, 裏を返せば, 企業が情報漏洩事故を発生させてしまったとしても, 36%の消費者は当該企業から離反しないということを意味する. また, 逆に, インシデントを発生させてしまった企業が再発防止策を徹底したとしても, ある割合の消費者は離反する可能性が残るであろう. 上記に鑑み, 脅威残存率R_Tの定義域を$a \leq R_T \leq b$とした場合, 式 9 は次のように改められる.

$$\min\left[\sum_i V_i\left\{b_i - (b_i - a_i)\left(1 - \frac{D_{Si}}{D_{Ri}} \cdot \frac{L_{Si}}{L_{Ri}}\right)\right\} + \sum_i D_{Ri} L_{Si}\right] \quad (10)$$

5. 提案手法の評価

5.1 ユースケース

本章では, 提案手法の利用可能性の評価を行う. 今回の評価にあたり, 次のユースケースを設定する.

- 想定する組織は, EC サイトを運営する中小企業で, 3 章の前提 1 および 2 に沿う組織である.
- 当該組織で, 何らかのインシデントにより顧客情報が漏洩した可能性が浮上した.
- 組織内で初動対応を行ったところ, インシデントの種別は SQL インジェクション攻撃である可能性が高いとの結論を得た. これを受けて, 詳細な調査をフォレンジック調査会社に依頼した.
- 依頼組織の保有する資産（表 2）は, 1,000 人分の顧客情報である. 依頼組織は, JNSA の個人情報漏洩における想定損害賠償額の算出モデル[9]を参考にし, 顧客情報の資産価値を 300,000 円と算出している.
- 依頼組織が提供可能な調査要件データは表 3 の通りであった.

表 2　依頼組織の情報

顧客数	1,000 人
資産種別	顧客情報
資産価値	300,000 円

表 3　提供可能な調査要件データ

Web サーバログ	40MB
DB サーバログ	100MB

5.2　適用結果

実装したコミュニケータにユースケースの数値を入力したところ，費用対効果が最高となる調査内容について，表 4 の出力が得られた．なお，今回のユースケースでは，調査費単価を 20 万円/人日として計算している．発注工数を変化させた場合の費用対効果は図 4 の通りであった．

表 4　費用対効果が最高となる調査内容

発注工数	7 人日
調査費	140,000 円
残存リスク	0 円

上記の結果では，調査費を 20 万円/人日として計算している．その他，調査工数ごとの費用対効果は次の通りであった．

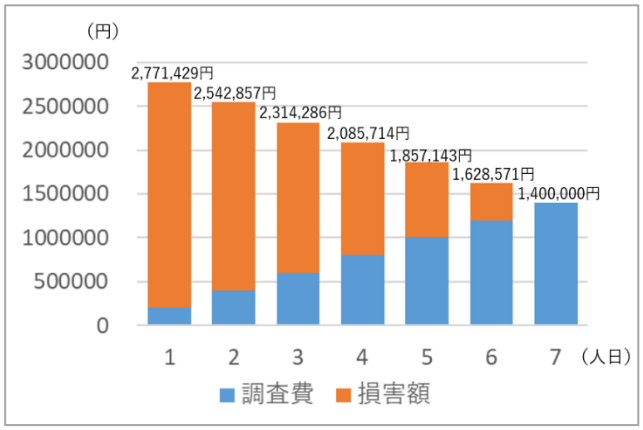

図 1　発注工数に対する費用対効果の変化

6.　まとめと今後の課題

本稿では，フォレンジック調査選定を支援するリスクコミュニケータを提案した．また，フォレンジック調査の選定が離散最適化問題として定式化できることを示した．

今後は，実用化に向けた有用性の向上と有効性の評価を行う必要がある．本稿での定式化にあたっては，4 つの前提を置いているが，実際のフォレンジック調査は前提に当てはまらない場合がある．よって，実用化に向けてはこれらの前提を緩和する必要がある．また，本稿で行った評価は提案手法の利用可能性を確認するものであるため，今後は有効性の評価も行いたい．

参考文献

[1] “ISO/IEC 27001:2013”. https://www.iso.org/standard/54534.html（参照 2022-01-04).
[2] “ISO/IEC 27005:2018”. https://www.iso.org/standard/75281.html（参照 2022-01-04).
[3] NIST, “リスクアセスメントの実施の手引き,” NIST SP 800-30 rev.1, 2012.
[4] 中村逸一, 兵藤敏之, 曽我正和, 水野忠則, 西垣正勝, “セキュリティ対策選定の実用的な一手法の提案とその評価,” 情報処理学会論文誌, 2004, vol. 45, no. 8, pp. 2022-2033.
[5] 堀川博史, “情報セキュリティインシデントデータベースに基づく全社的情報セキュリティマネジメントの強化手法の提案と評価,” 静岡大学博士論文, 2017.
[6] 川崎律子, “組織の情報セキュリティリスク対応を支援するモデルの提案とその適用可能性の検討—ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 適合モデルとその運用手法について—,” 情報セキュリティ大学院大学博士論文, 2015.
[7] 佐々木 良一, 日高 悠, 守谷 隆史, 谷山 充洋, 矢島 敬士, 八重樫 清美, 川島 泰正, 吉浦 裕, “多重リスクコミュニケータの開発と適用,” 情報処理学会論文誌, 2008, vol. 49, no. 9, pp. 3180-3190.
[8] 大元隆志, “情報漏洩を行った企業に対して，64%の消費者は取引意欲が低下する”. https://news.yahoo.co.jp/byline/ohmototakashi/20171112-00078036（参照 2022-01-04).
[9] JNSA, “情報セキュリティインシデントに関する調査報告書【速報版】”. https://www.jnsa.org/result/incident/data/2018incident_survey_sokuhou.pdf（参照 2022-01-04).