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

著者	佐々木 葵, 天笠 智哉, 奥村 紗名, 井坂 佑介, 野崎 慎之介, 堀川 博, 村上 弘和, 大木 哲史, 西垣 正勝
雑誌名	コンピュータセキュリティシンポジウム2021論文集
ページ	492-498
発行年	2021-10-19
出版者	情報処理学会
権利	
注記	コンピュータセキュリティシンポジウム2021 開催期間 : 2021年10月26日(火) ～ 2021年10月29日(金) 会場 : オンライン(ZOOM Webinar) セッション番号 : 2C2-1
著者版フラグ	publisher
URL	http://hdl.handle.net/10297/00029060

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

佐々木 葵[1,*] 天笠 智哉[1] 奥村 紗名[1] 井坂 佑介[1] 野崎 慎之介[1] 堀川 博[1] 村上 弘和[2] 大木 哲史[1] 西垣 正勝[1]

概要：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．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が，一般に調査費は調査会社ごとに算定方法が異なり，積算根拠は開示されない．このため，依頼者は調査費の妥当性を判断することが難しい．そこで提案方式では，フォレンジック調査によるセキュリティインシデントの原因究明率と調査費を「フォレンジック調査の作業量」という尺度で数値化することにより，残存リスクと調査費の関係を離散最適化問題として定式化する．調査会社は，提案方式を用いて「費用対効果の高い作業量」を見積もることができ，調査費・期間に加え，その調査によって見込まれる原因究明率についても依頼者に提示することが可能となる．この結果，依頼者は，調査費・期間・原因究明率から調査の費用対効果を評価できるようになり，調査費の積算根拠が開示されなくとも最適な調査会社を選定することが可能となる．このように提案方式は，依頼者と調査会社の間における「客観性・透明性の保証されたリスクコミュニケータ」の実現に資する．本稿では，提案方式の可用性を机上検討により確認する．

キーワード：フォレンジック調査，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

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

Aoi Sasaki[1,*] Tomoya Amagasa[1] Sana Okumura[1] Yusuke Isaka[1] Shinnosuke Nozaki[1] Hiroshi Horikawa[1] Hirokazu Murakami[2] Tetsushi Ohki[1] Masakatsu Nishigaki[1]

Abstract: In forensic investigation, a risk-communication can be poor because the interaction is hold between experts and non-experts. This problem surfaces as the problem of not being able to show the appropriateness of the investigation contents and cost. In this paper, we propose a risk-communicator to be used between a forensic investigation company and its client. Also, we show that forensic investigation selection can be formulated as a discrete optimization problem, and that the most cost-effective investigation can be derived using the proposed equation. In our method, the relationship between the residual risk and the investigation cost is formulated as a discrete optimization problem by quantifying the investigation rate of the cause and the investigation cost by measure of investigation workloads.

Keywords: Forensic Investigation, Risk-Communicator, Discrete Optimization Problem, Incident Response

1. はじめに

近年，情報化社会の本格化に伴い，セキュリティ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．セキュリティインシデントが発生した際，同様の原因によるセキュリティ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，加えて，セキュリティインシデントの対応には，総務省庁への報告義務や利用者への説明責任が発生する．情報漏洩を伴うセキュリティインシデントでは，さらに個人通知の義務や顧客への補償が生じる．これらの社会的責任を果たすためには，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．セキュリティ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，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，セキュリティ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．

当然，フォレンジック調査には相応のコストが発生する．このため，セキュリティ投資の概念に従って，費用対効果が最大となるように調査内容（レベル・範囲・期間など）の選定がなされるべきである．多くの場合，フォレンジッ

1 静岡大学
Shizuoka University
2 株式会社 CyCraft Japan
CyCraft Japan

* nisigaki@inf.shizuoka.ac.jp

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．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，一般に非専門家と専門家であり，知識量やバックグラウンドが異なるために，コミュニケーションに困難が生じるためである．

リスクコミュニケーションの障害は，フォレンジック調査選定において，次のような問題となって表面化する．調査会社は，依頼者側の状況を依頼者から正確に聴取することができず，調査内容を見積もって依頼者にとって最良となるプランを依頼者に示すことが難しい（問題１）．このため，調査会社が依頼者に提示できるのは，調査方針と調査費のみとなる（問題２）．調査によって見込まれる成果が調査会社から示されないため，依頼者は調査内容の妥当性を判断することができない（問題３）．調査内容の妥当性が不明である以上，依頼者は調査費の妥当性（調査の費用対効果）を判断することもできない（問題４）．

上述の問題に対して，本稿では，「原因究明率」と「残存リスク」の２つの尺度を用いて，フォレンジック調査選定問題を離散最適化問題として定式化する．原因究明率は，フォレンジック調査の完遂度を見積もるための尺度であり，今回は，調査要件データ充足率（インシデントの原因究明のために必要なデータがどの程度揃っているか）と調査工数充足率（調査対象となる全データの調査に必要となる作業工数の内，どの程度の工数が調査費によって賄われるか）の積によってこれを見積もる．残存リスクは，フォレンジック調査の効果を見積もるための尺度であり，今回は，風評被害額（インシデントによって被ることになった風評被害）と再発被害額（インシデントの再発リスク）の和によってこれを見積もる．風評被害額および再発被害額が原因究明率の関数として数値化されることによって，残存リスクと調査費の関係性が定式化され，調査費の費用対効果を評価することが可能となる．

調査会社は，（１）提案方式を用いて「費用対効果の高い作業量」を見積もることができ，（２）調査費・期間に加え，その調査によって見込まれる原因究明率についても依頼者に提示することが可能となる．この結果，依頼者は，（３）調査費・期間・原因究明率から調査の費用対効果を評価できるようになり，また，（４）積算根拠が開示されなくとも最適な調査会社を選定することが可能となる．

このように提案方式は，依頼者と調査会社の間における「客観性・透明性の保証されたリスクコミュニケータ」の実現に資する．典型的な企業を想定して机上検討を行うことにより，提案方式の可用性を確認する．

2. 課題設定

2.1 フォレンジック調査におけるセキュリティ投資

フォレンジック調査の対象・期間の選定には，安全性，コストなどの複数の指標が存在する．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]．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調査が選定できる．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ということがある．一般に，依頼者は経営陣であるため，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されても評価しづらく，「どれくらいの出資でどういった効果が見込まれるのか」という経済的な説明の方が有用である．しかし，説明を行う技術者は，フォレンジック調査の経済的な説明を行うことが難しい．このように，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成立しないという問題がある．

リスクコミュニケーションがうまくいかないことは，結果として，次の１～４の問題となって表面化する．フォレンジック調査は，未確定の事象に対する調査であるため，「調査前に調査の結果を予測することは不可能である」という性質がある．そのため，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．よって，調査会社は，調査の費用対効果を定量的に示すことが難しい．したがって，「決められた期間内に可能な限りの調査をする」という方法を採らざるを得ない（問題１）．そのため，調査会社が依頼者に提示できるのは，大まかな調査内容と調査費，期間のみであり，調査内容の妥当性や調査費の積算根拠を依頼者に提示することができない（問題２）．調査によって見込まれる成果が提示されないことで，依頼者は調査の費用対効果を評価したり，調査の対象・期間の妥当性を判断したりすることができない（問題３）．また，調査費の積算根拠が開示されないことにより，調査費の妥当性を判断することが難しい（問題４）．

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る. 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．すなわち，評価や選定の結果は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・対策案の関係のモデル化し，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対策の最適な組み合わせを求める手法[3]がある．これらは，組織における対策選定を論理的に求める実用的な手法である. その後, ISO/IEC 27001が改訂し，資産，脅威，脆弱性の特定および評価の要求項目が削除され，資産，脅威の特定を前提としない対策選定手法が求められると予想される．これを受けて，リスク対応に伴う意思決定を支援する手法[4][5][6]が提案された．

また，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，多重リスクコミュニケータ[7]がある．

このように，対策選定を支援する手法は複数存在する．しかし，フォレンジック調査に関して，リスクコミュニケーションの問題を解決する手法や選定問題としての考え方を導入した研究は，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離散最適化問題として定式化し，最も費用対効果の高い調査を選定する方式を提案する．また，定式化を通して，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を実現するリスクコミュニケータを提案する．

3. 問題解決のアプローチ

3.1 解決に向けてのアイディア

上述した問題を解決するために，本稿では，デジタル・フォレンジック調査におけるリスクコミュニケーションを実現するためのリスクコミュニケータを提案する．リスクコミュニケータは，フォレンジック調査の依頼者と受託者を仲介する形で位置し，依頼者と調査会社は，リスクコミュニケータを通して調査選定を行う．提案方式では，最も費用対効果の高い調査の対象・期間を導くために，調査費と原因究明率を「フォレンジック調査の作業量」という尺度で数値化することにより，残存リスクと調査費の関係を離散最適化問題として定式化する．調査に必要な情報を依頼者がリスクコミュニケータに入力すると，提案方式で定式化する式に基づいて，最も費用対効果の高い調査対象・工数および原因究明率が判明する．

具体的には，まず依頼者が保有するデータの種類から，調査に必要なデータが揃っている度合い（データ充足率）を算出する．そして，データ充足率と調査にかける工数から，調査によって見込まれる原因究明率を算出する．これにより，調査会社は依頼者に原因究明率を提示することが可能となる（問題２の解決）．また，離散最適化問題を解くことにより，調査会社は，最も費用対効果の高い調査の対象・工数を見定めることが可能となる（問題１の解決）．この結果，依頼者は，調査費・工数・原因究明率から調査の費用対効果を評価できるようになる（問題３の解決）. また，積算根拠が開示されなくとも最適な調査会社を選定することが可能となる（問題４の解決）.

3.2 フォレンジック調査選定問題の定式化

本節では，フォレンジック調査選定問題の定式化を行う. フォレンジック調査の選定基準は,「セキュリティインシデントによる損害をいかに小さく抑えることができるか」および「いかに費用対効果が高いか」である．よって，セキュリティインシデントにより予想される損害額（円）と調査費（円）の合計が最も小さくなるような調査の対象・工数の組み合わせを求める．したがって，計算式は次のような構造となる．

$$\min(\text{残存リスク} + \text{調査費}) \qquad (1)$$

ここで，計算式に用いる用語および記号について説明する．

- V_a（All Asset Value：全資産価値）：組織の保有する全資産の価値（円）
- V_r（Related Asset Value：再発被害を受ける可能性のある資産の価値）：発生したセキュリティインシデントと同様の原因により被害を受ける可能性のある資産の価値（円）
- γ（原因究明率）: 調査によって見込まれる原因の究明率（%）
- a（最大顧客離反値）: 原因を全く究明しなかった際の割合
- b（最小顧客離反値）: 原因を完全に究明した際の割合
- D（Data Fill Rate：調査要件データ充足率）: 調査に必要なログが満足されている割合（%）
- M（Man-hours Fill Rate：調査工数充足率）: 調査に必要な工数が充足される割合（%）
- C（Cost：調査費）: 調査にかかる費用（円）

3.3 原因究明率

提案方式では, 原因究明の度合いを「原因究明率:γ(%)」として表す．原因究明率は，調査に用いるデータの状態や調査の対象・工数，調査するデータの量に依存する．調査に用いるデータの状態によっては，実施可能な調査の幅が狭まることがある．データの種類や記録日数が十分である

表 1　データの種類と調査の対象との対応表

Table 1　Correspondence between the data and the subject of investigation

			調査に用いるデータの種類							
			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	Web サイトへの攻撃	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	－	－	－	－	－		○	－
	不正ログイン	パスワードリスト攻撃など	○	－	－	－	－		○	－
	マルウェア	クレデンシャルダンプ系	○	○	○	○	○	○	－	－
		RAT	○	○	○	○	○	○	－	－
		ランサムウェア	○	○	○	△	○	○	－	－

（○：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）

ほど，より十分な調査が可能であるため，原因究明率は大きくなる．本方式では，調査に必要なデータが揃っている度合いを「データ満足率：D（%）」として算出する．また，調査に日数・人数をかけるほど，より詳細な調査が可能であるため，原因究明率は大きくなる．このような調査にどの程度のリソースを割くかを「工数充足率：M（%）」として算出する．これより，原因究明率を求める式は，次のようになる．

$$\gamma = DM \qquad (7)$$

表 1 に示すように，調査にはその内容に応じてそれぞれ必要なデータがいくつか存在し，それらが揃っているほど効率的な調査が可能となる．本稿では，調査に必要なデータを「調査要件データ」と呼ぶ．そして，データが揃っている度合いを調査要件データ充足率：D（%）として示す．調査要件データ充足率は，調査要件データの種類（個数）に対する，組織が提供可能な調査要件データの種類（個数）で算出する． 例えば，提供可能なデータが Web サーバログのみである場合，SQL インジェクション攻撃の調査の調査要件データ充足率は，$\frac{1}{2} = 50\%$である．調査要件データ充足率は，

$$\frac{\text{提供可能な調査要件データの種類（個）}}{\text{調査要件データの種類（個）}} \qquad (8)$$

で表される．調査の対象と調査に必要なデータの種類の対応については，4 章で述べる．

調査するデータの量によって，調査に必要な工数（人日）が決定する．本方式では，調査に必要な工数は，専門家の知見の基，100MB あたり 1 人日とする．例えば，調査するデータの量が 500MB だった場合，調査に必要な工数は 5 人日となる．工数充足率は，上述のように，調査に必要な工数（人日）に対して，実際に調査にかける工数（人日）で表す．よって，工数充足率は，

$$\frac{\text{発注工数（人日）}}{\text{必要工数（人日）}} \qquad (9)$$

で表される．ここで，M の最大値は 100（%）とする．計算の際，必要工数を超えて工数をかけるとする場合も，M の値は 100（%）とする．

3.4 残存リスク

提案方式では，残存リスクを「風評被害額（円）」と「再発被害額（円）」の和として定義する．

風評被害を小さくするためには，セキュリティインシデントが発生した原因を詳らかにし，説明やお詫びなどの社会的責任を果たす必要がある．風評被害は，組織に求められる社会的責任の達成度合いによって，その大きさが変化する．かつ，社会的責任の達成には原因究明が必要であり，原因究明度合いによって果たせる社会的責任の範囲が左右される．よって，風評被害は原因究明率により変化する．また，風評の対象となるのは，セキュリティインシデントに直接関係する部署だけでなく，被害組織全体である．よって，風評被害の影響を受けるのは，組織が保有する全資産である．これより，風評被害額は，

$$V_a(1-\gamma) \qquad (3)$$

で表される．

加えて，風評被害の実質的な影響は，顧客が離反するこ

とによる利益の減少である．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]．よって，離反する顧客の割合は，何の究明もしない場合は 64%となる．この値を最大顧客離反係数（a）とする（a=0.64）．また，最大限の調査を行った場合の顧客離反率は，0.0%と仮定する．この値を最小顧客離反係数（b）とする（b=0）．顧客の離反度合いは，セキュリティインシデントの原因究明率に比例する．これより，式 3 はさらに，

$$V_a\{(1-\gamma)(a-b)+b\} \qquad (4)$$

と表せる．

再発被害を小さくするためには，セキュリティインシデントが発生した原因を詳らかにし，適切な対策を講じる必要がある．再発被害に関連するのは，発生したセキュリティインシデントに係る資産全体である．よって，再発被害として損失し得るのは，発生したセキュリティインシデントに係る総資産額である．これより，再発被害額は，

$$V_r(1-\gamma) \qquad (5)$$

で表される．

式(1)～式(5)より，次式が得られる．

$$\min[V_a\{(1-\gamma)(a-b)+b\}+V_r(1-\gamma)+C] \qquad (6)$$

式(6)を満たす値が，依頼者が支払う損害額と調査費の合計であり，この値が最小となる調査の対象・工数が依頼者によって最適な解である．

4. リスクコミュニケータ

本章では，図 1，2 に示すようなリスクコミュニケータを基に，提案するリスクコミュニケータの利用方法を述べる．依頼者と調査会社は，次に示すような手順でリスクコミュニケータを利用する．

① 依頼者による情報入力
依頼者は，図 1 の①のフォームに，提供可能な調査要件データの情報を入力する．調査要件データを提出可能な場合は，該当する調査要件データの欄にチェックマークを付し，そのデータ量を入力する．提供不可能な場合は，チェック欄は空欄とし，リスクコミュニケータにより当該部分に「無し」と表示される．

② 調査要件データ充足率の出力
手順①の入力内容に応じて，提供可能な要件データの有無が図 1 の②に反映される．また，調査要件データ充足率が算出され，③に出力される．

図 1　リスクコミュニケータの例①

Figure 1　Example of the Risk-Communicator 1

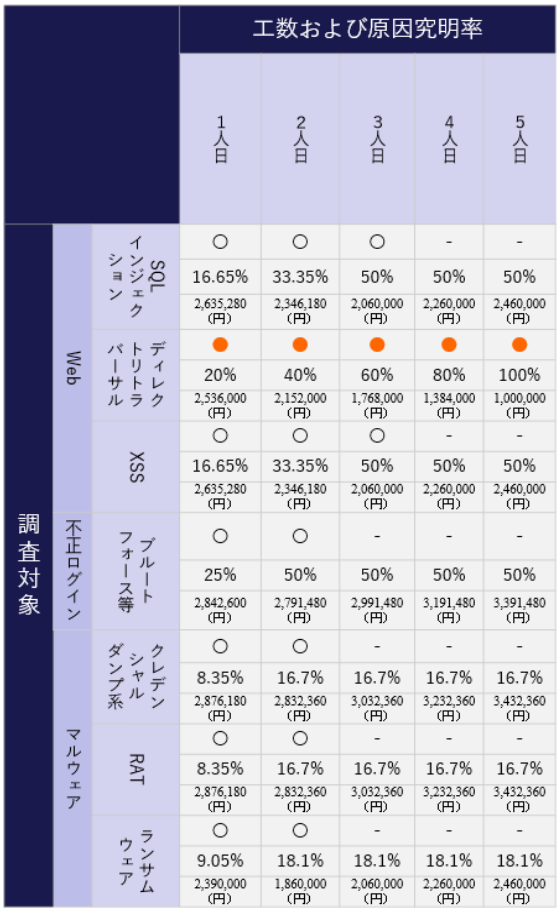

図 2　リスクコミュニケータの例②

Figure 2　Example of the Risk-communicator 2

③　調査選択

図 2 のように，リスクコミュニケータにより，調査対象・工数に応じた原因究明率および式 6 の値が算出される．依頼者はこれを受けて，依頼したい調査対象・工数を選択する．

④　調査費の算出

リスクコミュニケータを通して，調査会社が手順③で選択された依頼の調査対象・工数を確認する．問題が無ければ，依頼された調査対象・工数で調査を受注する．

5.　評価

5.1　想定するケース

提案方式の可用性を評価するために，典型的なセキュリティインシデントを想定して机上検討を行う．まず，想定するケースについて説明する．依頼者となる組織（企業 A）は，EC サイトを運営しており，ISMS 認証を取得している中小企業とする．そして，企業 A が標的型攻撃によってマルウェア感染し，顧客情報を漏洩したケースを想定する．企業 A の保有する資産は，図 2 の通りである．

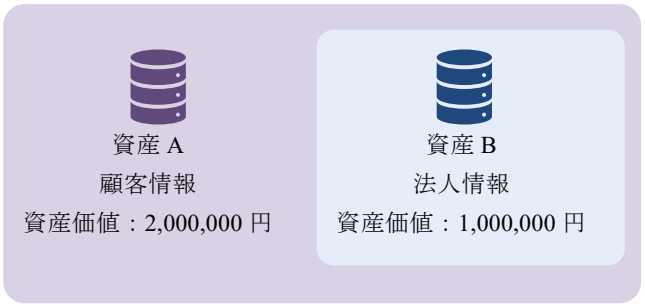

図 3　企業 A の保有する資産

Figure 3　Assets of Company A

資産 A と資産 B は異なるネットワーク内に保管されており，漏洩した情報は資産 A の顧客情報である．すなわち，再発被害に係る資産は，資産 A であり，V_r =2,000,000（円）となる．また，風評被害に係る資産は保有する全資産であり，V_a =3,000,000（円）である ．調査費は 1 人日あたり 200,000（円）とする．また，企業 A の提供可能な調査要件データは，次の通りである．

表 2　企業 A の提供可能な調査要件データ

Table 2　Data of Company A

イベントログ	200MB
Web サーバログ	300MB

5.2　可用性の検討

6.1 節で想定したケースについて，提案手法の可用性を検討する．企業 A が提供可能な調査要件データは表 2 の通りであるから，調査要件データ充足率および必要工数は，表 3 のようになる．

表 3　調査要件データ充足率と必要工数

Table 3　Data Fill Rate and Required Man-hours

調査対象	調査要件データ充足率	必要工数
SQL インジェクション攻撃	50%	3 人日
ディレクトリトラバーサル攻撃	100%	5 人日
XSS 攻撃	50%	3 人日
パスワードリスト攻撃など	50%	2 人日
クレデンシャルダンプ	16.7%	2 人日
RAT	16.7%	2 人日
ランサムウェア	18.1%	2 人日

ここで，調査 A を SQL インジェクション攻撃の調査，調査 B をディレクトリトラバーサル攻撃の調査，調査 C を RAT の調査とすると，調査工数充足率による原因究明率はそれぞれ次のようになる．

表 4　調査工数充足率と原因究明率

Table 4　Man-hours Fill Rate and Investigation Rate

		1 人日	2 人日	3 人日	4 人日	5 人日
調査 A	工数充足率	33.3%	66.7%	100%	100%	100 %
	原因究明率	16.65 %	33.35 %	50%	50%	50%
		1 人日	2 人日	3 人日	4 人日	5 人日
調査 B	工数充足率	20%	40%	60%	80%	100 %
	原因究明率	20%	40%	60%	80%	100 %
		1 人日	2 人日	3 人日	4 人日	5 人日
調査 C	工数充足率	50%	100%	100%	100%	100 %
	原因究明率	8.35%	16.7%	16.7%	16.7%	16.7 %

これより，式 6 の値，すなわちセキュリティインシデントによる損害額と調査費の合計は，それぞれ次の通りとな

る.

表 5　式 6 の値

Table 5　Value of eq.6

	１人日	２人日	３人日	４人日	５人日
調査 A	2,635,280（円）	2,346,180（円）	2,060,000（円）	2,260,000（円）	2,460,000（円）
調査 B	2,536,000（円）	2,152,000（円）	1,768,000（円）	1,384,000（円）	1,000,000（円）
調査 C	2,876,180（円）	2,832,360（円）	3,032,360（円）	3,232,360（円）	3,432,360（円）

表 5 の計算結果より, 式 6 の値が最も小さくなるのは, 調査 B に５人日かけた場合であると導かれた.

以上のように，提案手法を用いて，最も費用対効果の高い調査の対象・工数を導くことができた.

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離散最適化問題として定式化し, 調査の費用対効果を算出する方法を示した. また，フォレンジック調査選定におけるリスクコミュニケータを提案した.

本稿では，調査費と原因究明率を「フォレンジック調査の作業量」という尺度で数値化することにより，残存リスクと調査費の関係を離散最適化問題として定式化した．本稿で用いた「原因究明率」には，セキュリティインシデントの原因の究明率という意味合いに加え，個人情報漏洩の際の被害ユーザの特定率という意味合いがあった．セキュリティインシデントの原因を究明するための調査と被害ユーザを特定するための調査は, 厳密には異なる場合がある. より精度の高い式を立式するためには，これらを別々に定義し，計算する必要があると考える.

参考文献

[1] “ISO/IEC 27001:2013”. https://www.iso.org/standard/54534.html (参照 2021-08-23).

[2] “ISO/IEC 27005:2018”. https://www.iso.org/standard/75281.html (参照 2021-08-23).

[3] 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.

[4] Kawasaki (Aiba) R. and Hiromatsu T.. Proposal of a Model Supporting Decision-Making on Information Security Risk Treatment. WASET (World Academy of Science, Engineering and Technology) International Journal of Economics and Management Engineering. 2014, vol. 8, no. 4, pp. 583-589.

[5] Kawasaki (Aiba) R. and Hiromatsu T.. Proposal of a Model Supporting Decision-Making Based On Multi-Objective Optimization Analysis on Information Security Risk Treatment. WASET (World Academy of Science, Engineering and Technology) International Journal of Economics and Management Engineering. 2014, vol.8, no. 5, pp. 827-833.

[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-