情報処理学会論文誌 Vol.62 No.12 1926–1936 (Dec. 2021)

情報セキュリティ対策停滞の心理的要因を考慮した中小金融機関向け対策促進策の検討

稲葉 緑[1,a)] 菊池 大地[1,2]

受付日 2021年3月7日, 採録日 2021年9月9日

概要：金融業界では，中小企業における情報セキュリティ対策進捗の遅れが目立つ．本研究は，このような企業に対策の実施を促す効果が高い，管轄官庁からの働きかけの方法を明らかにすることを目的とする．特に，対策実施を停滞させる一要因と推定された，企業の対策への投資回避欲求を考慮したナッジに焦点を当てる．はじめに，中小金融機関における情報セキュリティリスクの発生可能性と影響度を評価し，その結果から対応すべきリスクを選定した．次に，各リスクへの対策を導出し，対策のインシデント防止効果やコスト等を評価したうえで，効果もコストも高い対策を選定した．最後に，ナッジの枠組みを参照し，これらの対策の実施を企業に働きかける促進策を考案した．各促進策案について予測される効果等を管轄官庁関係者へのインタビュー調査によって評価した結果，企業の特性が類似した他社における対策の好事例情報を管轄官庁が提供する促進策の効果が最も高かった．最後に，促進策の実施にともなうコストの問題や，経営層の対策への関与促進についての影響等を議論した．

キーワード：情報セキュリティ，金融業界，中小企業，ナッジ

Nudge to Promote Implementation of Information Security Measures for Small and Medium-Sized Financial Institutions

Midori Inaba[1,a)] Daichi Kikuchi[1,2]

Received: March 7, 2021, Accepted: September 9, 2021

Abstract: The aim of this study is to identify the effective methods to encourage small and medium-sized financial institutions to implement information security measures. In particular, this study introduced the nudge approach into the encouragement methods executed by the competent authority. First, we selected the information security risks that each institution should address based on the assessment of the probability and impact of these risks. Next, we derived measures for each risk and evaluated their effectiveness in preventing incidents and their cost. The measures that were highly evaluated in both were selected. Finally, we devised methods to encourage the institutions to implement the selected measures with reference to nudges. For each method, the predicted promoting effect was evaluated by interviewing the officials of the competent authority. As a result, the method in which the competent authority shares the good practices for information security that were performed in other institutions with similar characteristics was evaluated to be the most effective. Finally, we discussed the issues involved in executing the encouragement methods such as the cost and impacts on top management.

Keywords: information security, financial industry, small and medium-sized company, nudge

1. はじめに

金融業界の情報セキュリティに関する課題の 1 つに，これらのリスク対策が十分ではない企業の存在がある [1]．金

[1] 情報セキュリティ大学院大学
Institution of Information Security, Yokohama, Kanagawa 221–0835, Japan
[2] 金融庁
Financial Services Agency, Chiyoda, Tokyo 100–8967, Japan
[a)] inaba@iisec.ac.jp

融機関は攻撃の標的になりやすいことから [2]，一般的に対策の進捗が進んでいる [3]．特に大規模な金融機関は，対策に多額を投資し [4]，有効なマネジメントに関心が高い [5]．一方，中小金融機関は，基礎的な対策にも遅れがみられる [6]．結果として，攻撃による損失はこれらの機関に集中している [7]．

金融の安全・安定を担う管轄官庁は，このような状況を改善させる課題に直面している．各企業の実態や事情を把握したうえで，特に進捗が遅れている企業には直接的に対策の導入を要請してきた [8]．それでもこれらの効果が十分にみられているとはいい難い．さらなる状況の改善に向けて，たとえば，対策の標準や基準等の策定といった手段も考えられる．しかし金融機関の業種等の多様性により，対策内容の標準化は難しい．また，標準化による弊害も考えられる．具体的には，大規模金融機関レベルの高度な対策実施を基準とすれば，経営体力の乏しい金融機関は情報セキュリティ対策によって経営難に陥る．中小金融機関の中には，地域の企業や市民を支える役割を果たすものがあり，地域経済の衰退を招き得る．一方，より低い基準とすれば，この基準をすでに満たす企業が対策の手を緩めかねない．管轄官庁の従来の厳しい経営指導によっては，監査項目を満たせばよいだろうと考える風潮が業界内に生まれたとの示唆がある [9]．この示唆に基づけば，対策への積極性を失い，現在よりも低水準の対策実施にとどまる企業が出現するおそれがある．

これまでにも企業に情報セキュリティ対策を奨励する方策として [10], [11]，各業界の状況や特徴によらない基本的なガイドラインが示されている．業界全体としては対策が進んでいる [3] 中で相対的に進捗が遅れている金融機関が，このようなガイドラインを参照するかは疑問である．本研究は，管轄官庁による中小金融機関への現在の奨励策の効果を補完することを目指し，従来とは異なるアプローチを導入した新たな促進策を提案する．特に中小金融機関での対策の進捗を阻む心理的要因に着目する．

2. 着目した要因と本研究の対象

情報セキュリティ対策が進んでいない金融機関については，経営層の当該リスクへの希薄な危機感や，対策への関与の欠如等が指摘されている [6]．これは金融業界に限らない中小企業の傾向とされる [12], [13]．しかし彼らは情報セキュリティリスクや，その対策の重要性をまったく認識していないわけではない [12], [13], [14]．それにもかかわらず対策に消極的である背景には，経営資源欠如とその資源配分における他活動との競合に起因した，対策への投資回避欲求があると推測される．Tawileh らは，中小企業における情報セキュリティの負のループを示した [14]．限られた資源によって運営される中小企業の経営層は，中核となる事業活動に資源投資を集中させる志向性が強い [13], [15]．それにともない，情報セキュリティ対策の優先度は押し下げられ，投資が絞られた結果，さらに優先度が低下する．専門知識を有する人材がこの低下を阻止する場合もあるが，中小企業においてそのような人材は不足している [16], [17]．こうした負のループによって縮小化された問題への投資，すなわち，コストを経営層は高額に感じやすく [18]，回避欲求が強まると考えられる．対策実施が遅れている金融機関の特徴や，中小企業の特徴に基づけば，中小金融機関の経営層もこのような心理状態にある可能性がある．

本研究では，経営層の情報セキュリティ対策への投資回避欲求を考慮した，管轄官庁から中小金融機関に向けた対策実施への促進策を示すことを目的とする．この目的に対し，我々はナッジの枠組みを参照する．ナッジとは，強制せずとも，人や組織が自主的に望ましい選択肢を選ぶように誘導することを目的とした，行動経済学分野から提案されている手法の 1 つである [19]．この手法の特徴は，人の心理・行動特性に関する様々な知見を基に，心理的障壁による影響の緩和に特化している点にある [20], [21]．対策への投資回避欲求は，確定的な損失を嫌う心理的障壁 [22] に相当し，促進策の検討にナッジを参照することは適当であると考えた．ナッジのほとんどは個人向け [21] で，情報セキュリティに関する個人向けナッジは研究されている [20]．管轄官庁から企業に向けたナッジについては，カナダの財務省から滞納している企業に納税を促すナッジの実証実験の例がある [23]．本研究は，情報セキュリティ対策の実施促進を目的として，管轄官庁から企業に向けたナッジを検討する研究としては初めての事例である．

今回は中小金融機関のうち，信用金庫と信用組合（以降，「信金・信組」と呼ぶ）を例に検討する．預金を取り扱う金融機関は，小規模でも多くの金融資産を有する傾向がある．しかし，業界全体としての対策の遅れや [8]，経営層の関与についての問題が指摘されている [24]．加えて，地方銀行の半数以上が赤字で [25]，厳しい経営状況にある企業が多いことが窺える．ここから，信金・信組業界は経営層の対策投資回避欲求が喚起されやすい状況にあり，今回の促進策の実施対象として相応であると考えた．

はじめに，中小の信金・信組が優先的に対応すべき情報セキュリティリスクを選定した．金融機関でインシデントが発生した場合はその影響が広範囲に及ぶため，機関は多数かつ多様なリスク対策に取り組む必要がある．その中でも，金融機関にまず求められるのは，インシデントやそれによる直接的な被害発生の防止である．本研究ではこれに関するリスクに限定した．また，各信金・信組が対応しなければならないリスクを選んだ．システムに関しては，行内の事務処理やオンラインバンキングのウェブサイト管理等に関するシステムのリスクに限定される．会計勘定処理を行う勘定システムの利用にあたっては，管理を大手ベンダーが請け負う共同機構に，多くの信金・信組が加盟して

いるためである．次に，選定されたリスクへの対策を評価し，財務的・人的コストが高い対策を促進策の対象として選んだ．コストが高い対策の導入ほど経営層の判断が介在する可能性が高まるためナッジが経営層に届きやすくなるとともに，経営層の投資回避欲求が刺激されやすいためである．最後に各対策の促進策を評価した．この評価は，管轄官庁の関係者による予測である．たとえば促進策の実証実験を行っても，その協力のためだけに各企業が予算や人員計画を変更するとは考えにくい．したがって，管轄官庁が今後，施策として促進策を本実施するために必要な，その効果等の予測までを本研究の範囲とする．

3. 対応すべきリスクの選定

3.1 概要

信金・信組が対応すべき情報セキュリティリスクを選定する．第1に，深刻なインシデントに寄与し，かつ，組織やシステムの特性に左右されにくい一般的・概略的なリスクを網羅的に抽出した．ただし，対応資源が限られた企業にとって，抽出されたリスクすべてに一律的に対応することは難しい．そこで第2に，各リスクの発生可能性および影響度を評価した．この結果をリスク対応方針概念図 [26] と照らし合わせ，優先的に対応すべきリスクの選定を試みた．

3.2 方法

(1) リスク分析

はじめに，リスク分析のトップ事象とするインシデントを選定した．選定には，金融機関向けの情報セキュリティの教育資料にあげられていた事象例およびその解説 [27] を利用した．この教育資料の中では事象 45 個があげられており，各事象の資産への影響とブランドへの影響が数値で示されている．この2つの影響の数値を合計し，45 個のなかでも特に影響が甚大である事象を8個選んだ．このなかから評判低下等インシデントの波及的影響に関する事象2個，顧客の端末に対するパッチ未適用等原因が金融機関にはない事象1個を除外した結果，5事象に収束した．また，この5事象がインシデントによって発生した影響を含む場合は，教育資料の解説に基づき，インシデントに焦点を当てることとした．最終的に，「ATM からの不正出金」，「情報漏えい」，「自社の Web サイト改ざん」，「業務システムの停止・自社サービス応答不能」，「自社を装った不審メール拡散」の5事象をトップ事象とした．次に，様々な業界や企業での情報セキュリティ対策の実務経験者4人を含む6人によって，事業被害ベースのリスク分析 [28] を行った．上述のトップ事象の下に攻撃ステップを最大第2層まで明らかにした．顧客の端末に対するパッチ未適用等，原因が金融機関にはないリスクは除外した．結果，合計 66 個のリスクが得られた．また，次のリスク評価における調査協力者の負担軽減を目的とし，内容の類似性に基づいて 24 個のリスクに集約した．

(2) リスク評価および追加的リスク分析

抽出したリスクを評価するとともに，分析の網羅性を高めるための調査を実施した．調査においては，企業で情報セキュリティ対策を計画・実施した経験を持つ協力者を募集した．この募集時に，協力者には調査用 Google Form にアクセスし，表示された質問に回答するように依頼した．これらの回答は，ここから個人および対策実施企業が特定される可能性を排除するため，個人が特定できない形で収集した．協力者のうち，金融機関および中小企業で情報セキュリティ対策の実施経験を持つと回答した5人のデータを本研究では使用した．5人の内訳は2人が金融中小機関，2人が金融の大企業，1人が金融機関ではない中小企業での業務経験者であった．また，このうち1人（金融・大企業）が ATM 端末へのセキュリティ対策実施経験者であった．

各リスク評価では，金融機関および中小企業での情報セキュリティ業務経験を想起して回答するよう求めた．5つのトップ事象と各リスクを1組ずつ表示し，トップ事象に対する各リスクの関与の有無を回答してもらった．また，各リスクの発生可能性と影響度の評価を依頼した．評価基準は既存例 [29] に従い，5段階（発生可能性5「非常に多い」〜1「非常に少ない」；影響度5「重大」〜1「軽微」）とした．なお，トップ事象「ATM からの不正出金」は，ATM へのセキュリティ対策実施経験者1人のみに表示した．この調査では業務経験を想起したリスク評価を依頼したため，当該対策実施の経験を持たない協力者には表示しなかった．トップ事象「自社を装った不審メールの拡散」に関し，各企業への直接的な攻撃によらないリスク（**表 1** の 23–25 参照）は，その評価が困難であるとして評価対象からは除外した．ただし，次章での対策の対象には含めた．

また，各トップ事象について自由記述欄を設置し，表示したリスク以外に関与するリスクを想起した場合には入力を依頼した．ここで入力されたリスクは，ほとんどが 24 個のリスクに集約されたが，取引先・契約先による故意の情報流出（表 1 の 16）は集約されず，対応すべきリスクに追加した．先の調査への協力者を特定できないため，このリスクの評価者を新たに募集した．結果，情報セキュリティ対策の計画・実施経験者5人（金融大企業2人，金融機関ではない中小企業3人）から協力を得，このリスクの発生可能性と影響度を上述した評価基準で評価してもらった．

(3) 対応方針の判定

(2) で得られた発生可能性と影響度の評価値を使い，リスク対応方針概念図 [26] を参照として，各リスクを4種類の対応方針に分類した．上述の概念図では具体的な閾値の数値が示されておらず，分析者に設定が任されている．そこで著者は概念図からおおよその数値を読み取り，次のように閾値を設定した：① 保有（発生可能性および影響度が 2.5 以下），② 回避（発生可能性および影響度が 3.5 以上），

表 1 リスクの発生可能性・影響度評価平均および対応方針
Table 1 Mean scores of probability and impact assessment of risks with corresponding actions.

インシデントと関連リスク項目	発生可能性	影響度	対応方針
ATMからの不正出金			
1.スキミング被害	5.0	3.0	④
2.ATMマルウェア感染	5.0	5.0	②
3.ATMの物理的被害(破壊・損失等)	5.0	2.0	④
情報漏えい			
4.従業員のミス(メール誤送信、書類・USB紛失等)	3.4	3.4	④
5.従業員のモバイルデバイス・書類等の盗難	2.9	3.1	④
6.悪意のある従業員による故意の情報流出	3.4	4.2	④
7.取引先・契約先のミス(書類紛失・メール誤送信等)	3.0	3.2	④
8.標的型攻撃	3.9	3.5	②④
9.暗号鍵の解読	1.9	3.5	③④
10.情報及びアプリケーション(個人情報、webアプリケーション等)への不正ログイン	2.8	3.4	④
11.ネットワークのマルウェア感染	2.4	3.0	④
12.特権アクセス権の詐取	2.6	3.8	④
13.ユーティリティプログラムの不正利用	2.0	3.0	④
14.脆弱性攻撃	2.6	2.8	④
15.ゼロデイ攻撃	2.6	2.7	④
16.取引先・契約先による故意の情報流出	2.0	2.6	④
自社のwebサイト改ざん			
[情報漏えい 10〜15 のリスク]			
業務システム停止・自社サービス応答不能			
17.物理的侵入による装置破壊	2.4	2.4	①④
18.火災・自然災害による装置破損	2.8	3.2	④
19.サポートユーティリティの破損	2.0	2.4	①④
20.環境(開発, 試験, 運用)の差による不具合	2.8	2.8	④
21.システム統合・リプレイス切り替えによる不具合	3.0	2.8	④
22.サービス妨害(DoS)攻撃	3.2	3.6	④
[情報漏えい 4–7, 10–15のリスク]			
自社を装った不審メール拡散			
23.フィッシングサイトでの情報盗難	評価値無(企業への直接的攻撃ではない)		
24.偽装アプリ蔓延			
25.なりすまし攻撃			
[情報漏えい 8のリスク]			

③ 移転（発生可能性が 2.5 以下および影響度が 3.5 以上），④ 低減（発生可能性および影響度が 1.5〜4.5，ならびに，① から ③ までに該当しない）．

このうち，当面の間は対応しない ① 保有を検討しうると分類されたリスクについては，その対応方針と，促進策の対象とするかについて改めて検討することとした．② から ④ のリスクは優先的に対応すべきリスクと判定した．

3.3 結果・考察

各リスクの発生可能性と影響度の評価の平均，および，これらから判定された対応方針を表 1 に示す．(3) で ① 保有を検討しうると判定されたリスクは，物理的侵入による装置破壊（17）とサポートユーティリティの破損（19）であった．これらの攻撃は成功すれば甚大な被害を発生しうることから ① 保有するリスクとは考えにくく，④ 低減するリスクとして対策を検討する．ただし，今回，発生可能性も影響度も低く評価された理由として，両リスクへの対策を実施済みの金融機関が多いことが考えられた．本研究では，既存の機関への対策導入の促進に重点を置き，2 つのリスクに特化した対策は促進策の対象から除くこととした．

また，③ 移転を検討しうるリスク（暗号鍵の解読（9））が確認されたことから，この対策を含む包括的な外部委託サービスの利用の可否を，次章で評価することとした．一方，リスク自体を排除する ② 回避検討に相当するリスクは，考察の結果，④ 低減を目指す対策が妥当と推測した．このリスクには，評価者が 1 人で慎重な解釈が必要であるが脆弱性が指摘される ATM 端末のリスク [30]（ATM マルウェア感染 (2)）や，金融機関が標的となりやすい従業員に関するリスク [31]（標的型攻撃（8））が該当する．しかし，オンラインバンキングに不慣れな高齢の顧客を考慮すると，すべての ATM をすぐに撤去することは難しい．また，標的型攻撃のリスク要因である従業員やメールシステム利用をなくすといった対策の実現可能性は低いと考えた．

4. 促進策の対象とするリスク対策の選定

4.1 概要

中小金融機関が対応すべきリスク 25 個への対策のインシデント防止効果および財務的・人的コスト等を評価する．ここでは対策のコストだけでなくインシデント防止効果にも着目した．2 章で述べたとおり，情報セキュリティ対策の実施が不十分な企業には，まずはインシデントやそれによる直接的な被害の発生防止が求められると推察する．インシデント防止効果が高い対策を優先的に導入することで，これを効率的に実現できると考えた．

最終的には，各対策への評価結果からインシデント防止効果が高く，かつ，コストが高い対策を選定し，次章の管轄官庁による促進策の対象とする．

4.2 方法

(1) リスク対策の考案

各リスクについて，組織やシステムの特性に依存しない一般的な対策を 3 つの観点から列挙した．第 1 に，ISO/IEC27002 における情報セキュリティ対策群 [32] から関連する対策を選定した．第 2 に，金融 ISAC や管轄官庁が主催する企業向けワークショップおよび演習等で示された対策から，適用しうるものを抽出した．第 3 に，ヒューマンエラーについては，信頼性工学的手法 [33] を使って対策を考案した．前章で判定された対応方針と一致しない対策を導出した際には，それも対策に含めた．結果，合計 109 個の対策を列挙し，内容が重複するもの等を取りまとめ，43 個の対策に集約した．

(2) リスク対策の評価

中小金融機関の情報セキュリティ対策の実施状況等に詳しい管轄官庁の職員 6 人にインタビュー調査を実施し，中

表 2 リスク対策のインシデント防止効果およびコスト評価平均
Table 2 Mean scores of evaluated effectiveness and costs of risk measures.

	情報セキュリティ対策	インシデント防止効果					コスト		外部委託	促進策対象
		ATMからの不正出金	情報漏えい	自社のwebサイト改ざん	業務システム停止・自社サービス応答不能	自組織を装った不審メール拡散	財務的	人的		
1	キャッシュカードのセキュリティ向上	4	—	—	—	—	1	1	可	○
2	ATM利用者への呼びかけ（例 適切なパスワード設定）	4	—	—	—	—	4	3	可	
3	ATM端末へのアクセス制御・Webポートの防止	4	—	—	—	—	2	3	可	
4	ATMシステムに関するホワイトリスト型製品の導入	4	—	—	—	—	2	2	可	
5	ATM端末の監視（例 監視カメラ・警備員配置）	3	—	—	—	—	4	2	可	
6	情報セキュリティに関わる規則の整備・点検	4	4	4	4	—	3	4	可	
7	情報セキュリティに対する経営者の関与	4	4	4	4	4	4	4	不可	
8	資産管理（例 情報資産の把握、アクセス権指定）	3	3	2	3	—	2	4	可	
9	情報資産の把握・格付け区分・点検	3	3	3	3	—	4	4	不可	
10	情報資産の物理的な保護（例 施設の施錠、入退管理）	3	4	2	2	—	4	1	可	
11	情報機器及び記録媒体の資産管理・物理的保護	3	4	2	2	—	3	4	不可	
12	情報システムのログ・証跡の記録・保存・点検	4	4	4	4	—	3	4	可	
13	内部不正を防ぐ環境つくり（例 コンプライアンスの徹底）	3	4	2	3	—	4	4	不可	
14	内部不正発生時の事後対応・再発防止策の検討	2	2	2	2	—	4	4	不可	
15	内部不正の通報・監査制度の導入	2	2	2	2	—	4	4	不可	
16	社員教育の継続的な実施	4	4	4	4	—	3	4	可	
17	個人用端末へのアンチマルウェアソフトの導入・更新	3	4	4	4	—	3	3	可	
18	業務用サーバへのアンチマルウェアソフトの導入・更新	4	4	4	4	—	3	2	可	
19	社外への情報誤送信対策（例 社外向けメール送信の厳密化）	—	4	2	2	—	3	3	可	
20	社員の端末におけるログインパスワードの管理徹底	2	4	2	2	—	2	4	不可	
21	社員端末ログイン時の高セキュリティ手順（例 二段階/生体認証）	2	4	2	2	—	2	3	可	
22	ISACや信金信組間等での情報共有	3	3	3	3	4	3	3	不可	
23	特権アクセス権の適切な管理	3	4	4	4	—	2	4	可	
24	ユーティリティプログラムの適切な管理	3	3	3	3	—	3	3	不可	
25	OSINT等の情報収集	4	4	4	4	—	2	4	可	
26	ペネトレーションテストの実施	4	4	4	4	—	2	1	可	○
27	脆弱性診断の実施	4	4	4	4	—	2	3	可	
28	ファイアウォール・サンドボックス等の入口対策	4	4	4	4	—	2	2	可	○
29	ホワイトリスト型の製品の導入	4	4	4	4	—	2	2	可	○
30	外部への送信データをチェックする等の出口対策	4	4	4	4	—	2	3	可	
31	暗号鍵管理システムの導入	4	4	2	2	—	3	2	可	
32	CSIRTの整備・招集訓練	4	4	4	4	3	1	4	不可	
33	ISAC等の演習・訓練への参加	4	4	4	4	3	1	3	不可	
34	火災・自然災害対策	—	2	—	4	—	4	2	可	
35	クラウドの利用	—	—	—	3	—	1	3	可	
36	定期的なシステム検査・試験	3	3	3	4	—	2	2	可	
37	バックアップの確保	3	4	4	4	—	3	4	可	
38	システム更新時の可用性確保（例 開発・試験環境の分離）	—	3	2	4	—	2	3	可	
39	取引先・契約先とのセキュリティ情報共有	4	4	4	4	—	3	4	不可	
40	報道発表（フィッシングサイトからの情報流出などについて）	4	4	4	4	4	4	4	不可	
41	顧客への注意喚起（対偽装アプリ/フィッシングサイト）	4	4	4	4	4	4	4	不可	
42	関係機関への連絡（対偽装アプリ/フィッシングサイト）	4	4	4	4	4	4	4	不可	
43	SPFレコードの設定	—	—	—	—	4	3	4	可	

「—」：トップ事象との関与が評価されなかったリスクの対策については，そのトップ事象を防止する効果を評価していない．

小金融機関を想定したうえで，対策 43 個について 3 項目の評価を依頼した．各評価基準は 4 段階で，中小金融機関における対策についての管轄官庁職員の意見を基に，評価しやすさ等も考慮して設定した．第 1 の評価項目はインシデントを防止する効果（4「十全な効果が期待できる」，3「効果が期待できる」，2「一部効果が期待できる」，1「全く効果がない」）である．3 章でトップ事象との関与が評価されたリスクの対策について，そのトップ事象を防止する効果の評価を依頼した．第 2 に財務コスト（4「0〜数万円程度」，3「数十万円程度あるいは月数万円程度の運用コ

スト」，2「数百万円程度あるいは月数十万程度の運用コスト」，1「1 千万円以上あるいは月数百万円程度の運用コスト」)，第 3 に人的コスト（4「対策に必要な知識は必要ない」，3「情報セキュリティに関する知識がある程度必要」，2「高度な知識が必要」，1「高度な知識を有した人材が複数必要」）であった．また，各対策の外部委託の可否についても尋ねた．

(3) 促進策の対象とするリスク対策の選定

インシデント防止効果の評価値が 4 で，財務的・人的コスト両方の評価値が 2 以下の対策を選定した．3.2 節 (3) で①保有を検討しうると判定されたリスクに特化した対策は除外した．

4.3 結果・考察

中小金融機関が対応すべきリスクへの対策として導出された 43 個の対策と評価されたインシデント防止効果，コスト，ならびに外部委託の可否を**表 2** に示す．特に「キャッシュカードのセキュリティ向上」と「ペネトレーションテスト」のコストが高かった．前者は ATM 端末を含むシステムの全面的な交換や顧客のキャッシュカード交換・周知等，莫大なコストがかかる．後者は 1 回で数千万円程度の費用を要し，専門人材が必要である．このほか，「ファイアウォール・サンドボックス等の入口対策」と「ホワイトリスト型の製品の導入」が選定基準を満たした．以上 4 つの対策を次章で検討する促進策の対象とした．

なお，対策の 1 つとしてあげた「情報セキュリティに対する経営者の関与」は促進策検討の対象外となった．いずれの効果も非常に高いものの，物理的対策への投資や専門知識を有する人材を要しないことで，コストが低いと評価されたためである．しかし前述のとおり，これは奨励されているにもかかわらず，信金・信組において進展が思わしくない対策である．この対策自体は低コストでも，これを引き金として様々な対策への多大なコストに直面すると予期させることが，経営層の対策投資回避欲求を刺激している可能性がある．そこで，次章の結果を参考としつつ，総合考察においてこの対策の促進策を考察する．

最後に，外部委託については，ほとんどの技術的対策について利用可能との回答を得た．一方，「情報資産の把握」，「CSIRT の整備・招集訓練」等の対策は，外部委託が不可能と評価された．企業全体の資産を把握したり，社内の横断的な協力を得たりする等，経営層の支援が必須な対策ほど外部委託が難しいことが示唆された．

5. 促進策の評価

5.1 概要

前章で選定された，インシデント防止効果が高いものの，コストも高いと評価された 4 つの対策について，これらの対策実施を中小の信金・信組に働きかける促進策を考案する．本研究では経営層の心理的障壁を考慮した促進策を考えるにあたり，ナッジを参照する．また，考案した促進策が企業における各対策の実施を促進する効果を評価する．さらに，定期的・継続的な実施にあたって考慮する必要がある，促進策実施にまつわるコストを評価する．

表 3 促進策案考案に使用したナッジ分類

Table 3 Nudge classification to consider encouragement methods.

ナッジツールの分類	促進策との関連
記憶想起関連（例 自己奉仕バイアスに関する情報提供）	(c)
インセンティブ（報酬を設定する）	(d)
損失回避（損失回避欲求を刺激する）	
感情ヒューリスティック（回避すべき事象に否定感情を抱かせる）	
代表性ヒューリスティック（例 代表的事例を示す）	
利用可能性ヒューリスティック（例 選んで欲しい選択肢を目立たせる）	
アンカリングヒューリスティック（例 情報提示の順序調整）	
フレーミング効果（促すべき／回避すべき事象ごとに表現を変える）	
メンタル・アカウンティング（例 トピックごとの情報提供）	
参照点依存（例 即時の判断回避）	
デフォルト（例 初期設定, サンクコスト効果を利用する情報提供）	(e)
他者の存在（他者を意識させる）	(a)(b)
社会的影響（例 規範の意識づけ）	(b)
情報の発信者（情報の伝達者を工夫する）	(b)

山崎[21]による分類に他の知見[20, 34]を追加・編集して表を作成

5.2 方法

(1) 促進策の考案

先行研究 [20], [21], [34] にあげられているナッジの分類を**表 3** のようにまとめ，これらのナッジを利用した促進策案を検討した．また，管轄官庁の協力者に実施可能性等について意見を聞きながら，企業に向けた管轄官庁主導の促進策を考案した．内容が類似したものをまとめた結果，次の 5 種類に集約された．

(a) 様々な特性の企業による情報セキュリティ対策の好事例を信金・信組の連携の場において配信する．

ほとんどの信金・信組が参加する連携の場において，様々な地域や規模の企業における対策の好事例の情報が配信されるよう，管轄官庁が手配する．ナッジの枠組みのうち，情報提供等によって他者の存在やその判断を意識させる「他者の存在」[21], [35], [36] を導入した手段である．類似した企業の対策実施状況を意識させ，それらの企業と同様の対策をとることへの同調意識を刺激する．

(b) 企業の特性に応じた情報セキュリティ対策の好事例を管轄官庁が信金・信組に配信する．

管轄官庁が各企業の対策の進捗状況を把握し，その情報

を企業の特性ごとに整理したうえで，好事例の情報を管轄官庁から配信する．促進策案 (a) と同じ「他者の存在」に，管轄官庁から送る「情報の発信者の変化」[34] を追加した．これは，情報を肯定的に認識させたり，信用度を高めたりするために情報の伝達者を工夫するナッジである．管轄官庁から提供される情報の信用度を企業は高く評価すると考えられる．また，管轄官庁が発信者となることにより，好事例を企業が手本例と認識することによる「規範」の効果も期待された．規範は，表 3 の「社会的影響」に含まれ，規範的メッセージ等を提供することで，それに沿った行動をとろうとする心理を刺激する [20], [21]．一般的に，企業には社会規範に則った企業活動が求められる．企業が好事例を社会規範として受け取れば，これと同様の対策を実施しようとする可能性がある．

(c) 管轄官庁の企業向け講演等で，踏み台攻撃の事例を紹介する．

対策を実施しない企業が踏み台となり，他の信金・信組が攻撃されるリスクを説明する．「記憶想起関連」（表 3）のナッジの 1 つとされる自己奉仕バイアスを刺激する情報提供では [21]，相補性の高いチームワークにおいて成果を高める可能性を示す．具体的には，連携する他者に迷惑をかけたくないと思う心理を刺激するナッジの検証例がある [20]．本研究ではこれを他社に読み替えて利用した．

(d) 情報セキュリティ対策に積極的な金融機関を定期的に，あるいは，管轄官庁主催の講演等で表彰する．

ナッジの「インセンティブ」[20], [21], [34] を参照した促進策案である．この促進策案では，対策実施に対する非金銭的なインセンティブによって，管轄官庁から高い評価を得たい，および，他の信金・信組から承認されたい心理を刺激する．なお，金銭的なインセンティブについても検討した．たとえば，「情報セキュリティ対策の実施によって保険の優遇を受けられる」といった促進策案である．しかしこれについては管轄官庁の協力者から，保険会社の管轄機関でもある同庁が，特定の金融分野を優遇していると疑われかねない対応を推し進めることは不適切であるとの意見を得た．したがって，この案は本研究では評価対象として採用しなかった．

(e) 初期投資を小さくし，徐々に新しいシステムの導入を進める取り組みを紹介する．

促進策案 (e) は，今回の調査では対策「キャッシュカードのセキュリティ向上」のみに適用する促進策である．これは，「デフォルト」との類似性から同じ分類に位置づけられた「サンクコスト効果」に関する情報提供 [21] である．1 度始めたことをやめたら，それまでに費やしたコストがもったいないと思う心理を利用し，徐々に進捗させることで，後に戻りづらくさせることを目指す．促進策案 (e) では，一度にすべてのキャッシュカードを IC カードに変える必要はないとし，コストが低いことを強調する．途中も IC カードと磁気カードの併用期間の設定を許容する．最初の目標を小さく設定し，徐々に対策実施を進めると，その取り組みを中止したり停滞させたりすることを企業が躊躇するようになると考えた．

表 4 促進策案の効果およびコスト評価平均
Table 4 Mean scores of evaluated effectiveness and cost of encouragement methods.

促進策案および促進対象の対策	効果	コスト
(a) 各企業における情報セキュリティ対策の好事例を信金・信組の連携の場において配信する		
ペネトレーションテスト	2	3
キャッシュカードのセキュリティ向上	2	
ファイアウォール・サンドボックス等の入口対策	4	
ホワイトリスト型製品の導入	4	
(b) 企業の特性に応じた情報セキュリティ対策の好事例を管轄官庁が信金・信組に配信する		
ペネトレーションテスト	3	2
キャッシュカードのセキュリティ向上	4	
ファイアウォール・サンドボックス等の入口対策	4	
ホワイトリスト型製品の導入	4	
(c) 管轄官庁が実施する企業向けの講演等で、踏み台攻撃の事例を紹介する		
ペネトレーションテスト	2	3
ファイアウォール・サンドボックス等の入口対策	3	
ホワイトリスト型製品の導入	3	
(d) 情報セキュリティ対策に積極的な金融機関を定期的に、あるいは、管轄官庁主催の講演等で表彰する		
ペネトレーションテスト	2	3
キャッシュカードのセキュリティ向上	2	
ファイアウォール・サンドボックス等の入口対策	2	
ホワイトリスト型製品の導入	2	
(e) 初期投資を小さくし、徐々に新しいシステムを増やす取り組みを紹介する		
キャッシュカードのセキュリティ向上	3	3

(2) 促進策案の評価

前章での対策評価の協力者に，改めて 5 種類の促進策案について次の 2 項目の予測を依頼した．第 1 に，効果である．促進策案に従った働きかけによって，中小の信金・信組が各リスク対策を実施する可能性の高さを指す．4 段階（4「十全な効果が期待できる」〜1「期待できない」）での評価を依頼した．第 2 に，管轄官庁が促進策案を実施する際に要するコスト（時間や労力，予算等）である．こちらも評価基準は 4 段階（4「ほとんどコストがかからない」〜1「多大な予算や時間がかかる」）とした．

5.3 結果・考察

評価結果を**表 4** に示す．促進策案 (b) の促進効果が最も高く評価された．促進策の対象である対策 4 つのうち，各促進策案による効果が最も確認されにくかった「ペネトレーションテスト」についても，促進策案 (b) は一定の効

果が予測された．高評価の要因の 1 つは「他者の存在」であると考えられる．インタビューの協力者より，信金・信組業界には横のつながりが強い風土があるとのコメントが聞かれた．他社との関係が強いほど，自社も同様の振る舞いをしようとすることが推測される．ただし，他社とのつながりは，促進策案 (a)，促進策案 (c) の効果にも寄与したと考えられる．これらに増して促進策案 (b) の評価が高かったのには，管轄官庁が「情報の発信者」となったことで，好事例が「規範」の意味合いを帯びたことによる可能性がある．企業が好事例を企業特性ごとの暗黙の基準と見なせば，同様の対策を実施することへのプレッシャを感じると予測される．

また，管轄官庁との良好な関係維持によるベネフィットが，対策へのコスト節約よりも価値が大きいと企業は考えるだろうとの協力者の意見も聞かれた．ここから促進策案 (b) は，「インセンティブ」の心理も喚起する可能性がある．それでも，管轄官庁が対策の進捗を働きかけてきたにもかかわらず応じない企業がある現状をふまえると，この促進策案の効果が高いと評価された背景には，「インセンティブ」だけでなく，上述した「他者の存在」や「規範」が信金・信組に対して機能するとの予測があると考えられる．

しかし，この促進策案 (b) はコストも高いと評価された．各企業の対策の実施状況を詳細に把握し，特性によって適切に金融機関をグルーピングすることの難しさ等が影響したと推測される．

一方，促進策案 (d) は，他の促進策案よりも効果が低いと評価された．前述した管轄官庁との関係悪化を回避することに比べ，さらに良好なものにすることへの動機付けは強くは働かないと予測された可能性がある．

6. 総合考察

本研究は，企業における情報セキュリティ対策への消極的な取り組みの背景にある心理的要因に着目し，これを考慮した管轄官庁による対策実施への促進策を検討した．対策の進捗が十分ではない金融機関，特に中小の信金・信組を対象とした．まず，各信金・信組が遭遇しうるリスクを抽出し，それらへの対策を導出した．このなかから，インシデント防止効果は高いがコストも高いために実施が見送られやすい対策を選定した．そのうえで，これらの対策実施を働きかける 5 種類の促進策案を評価した．最も効果が高かった促進策案は，促進策案 (b) であった．ただし，促進策の実施者である管轄官庁に求められるコストも最も高く評価された．コストを下げるためには実施頻度を下げること等が考えられるが，一方で効果も低下しうる．これに対し，たとえば，効果は相対的に低いがコストも低い，促進策案 (a) を並列的に行い，効果を補充することがあげられる．2 種類の促進策案を実施する場合，開始準備のためのコストのみに目を向ければ，1 種類を実施する場合よりもコストが高くなる．しかし，促進策案 (a) における管轄官庁の役割は手配や調整であり，実施 1 回あたりのコストは相対的に低いと評価された．ここから，促進策案 (b) の実施頻度を減らし，連携の場を利用する促進策案 (a) との 2 種類を並列的に実施することで，前者の促進策案 1 種類を毎回実施するよりも，長期的にはコストを抑えることができると考えられる．

また，連携の場を利用する促進策案 (a) を並列的に実施することには副次的効果も期待できる．管轄官庁によって紹介された好事例（促進策案 (b)）が各企業に規範と認識されることは，働きかけの促進効果を高める一方，好事例の対策のみを実施すれば十分だと考える，従来の金融機関の受動的な姿勢 [9] をも助長するおそれがある．これに対し，企業間の連携体制に組み込まれた促進策案 (a) は，企業に連携の一員としての社会的責任を感じさせる可能性がある．社会的責任は，企業の情報セキュリティに関する 1 つのモチベーションであることが示唆されている [37]．これによって企業の自律的な姿勢が向上すれば，管轄官庁の直接的な促進策による受動的姿勢の問題が緩和されると期待できる．

ここで本研究の評価結果や考察に基づき，経営層の情報セキュリティへの関与について論じる．経営層の関与は組織の対策進捗の鍵として広く認識されているが [5], [10], [38], [39]，本研究でもこれを支持する示唆が得られた．たとえば，我々は中小金融機関の経営状態の厳しさに鑑み，優先的に対応すべきリスクを限定することによるコスト低減を試みた．しかし，対応済みのリスクを除き，このようなコスト削減は困難であるとの結果が得られた．この結果は，経営状態が厳しい企業ほど難易度の高い経営資源の配分が求められることを意味する．情報セキュリティは，経営層の関与なしに担当部署が判断する問題ではないことを示すものと解釈できる．このような経営層の関与の必要性は，外部委託が不可能である対策の特徴からも浮き彫りになった．

本研究が検討した各対策への促進策案の実施によっては，経営層の関与の問題をも改善することが期待されるが，さらに直接的な促進策案について推察する．ナッジの枠組みにおける「他者の存在」を導入した促進策案の効果がおおむね高評価であった結果から，情報セキュリティへの関与について信金・信組の経営層どうしが意見を交換する機会を設置することが考えられる．ただし，意見交換において中小金融機関が，経営層の関与という企業の特性によらない対策を実施済みの大企業と自社とを比較する余地を残せば，経営資源の差等を理由に，対策未実施を正当化する可能性が生じる [40]．これに対し，意見を交換する機会に特性が類似した企業を集めることが有効であると考えられる．また，地域ごとの企業への働きかけでは効果が不十分な例があったとの管轄官庁による報告 [8] がある．ここか

ら，「他者の存在」に同調する姿勢を喚起し，「規範」を企業に強く感じさせるためには，経営層が対策に関与する企業を意見を交換する機会に集まる企業のうちの多数にする等の工夫が必要であると予測される [41]．さらに，各企業がすでに参加・加盟し，メリットを享受している枠組みを利用すれば，「インセンティブ」の側面を強化できる．たとえば，勘定システムの機構を情報セキュリティに取り組む連携の場として発展させる案が考えられる．経営層の対策への関与と，これを満たさない企業が機構からの脱退を求められる可能性とを経営層に比較させることができれば，低コストという理由から前者が選択される可能性が高い．

最後に，本研究の留意点を 3 点述べる．第 1 に，本研究で着目した経営層の投資回避欲求による対策進捗の遅れは，ナッジを参照とした促進策によってすべて改善されるわけではないと考える．たとえば，対策投資回避欲求を高める経営資金不足等の根本的な要因は，心理的障壁による問題の解消を目的としたナッジの対象ではない．したがって，本研究の促進策は単独で現状の問題を解消させるものではなく，管轄官庁による企業への様々な奨励策の 1 つとしての位置づけにある．第 2 に，中小金融機関における情報セキュリティリスクの評価には，大規模金融機関および金融ではない中小企業での対策実施経験者による評価を統合した．十分な数の中小金融機関での経験者の協力を受けた場合とは，リスクへの評価結果や，導出される対策が異なる可能性がある．第 3 に，本研究で検討した促進策案は，信金・信組業界での実施を想定したうえで，管轄官庁関係者の協力を得て考案し，評価した．同様の促進策の他の業界における有効性予測は，今後の課題としたい．

7. 総括

情報セキュリティ対策実施が進むとされる金融業界では，実際には，その進捗の差が企業間で大きい．特に中小企業において遅れが目立つ．このような遅れを管轄官庁が強制的に改善させることの難しさを背景に，情報セキュリティ対策の実施を中小金融機関に促す効果が高い働きかけの方法を明らかにすることを本研究の目的とした．具体的には，既存の知見より，対策進捗を阻害する一要因として経営層の対策投資回避欲求を推定し，これを考慮したナッジを検討した．はじめに，中小の信金・信組を例に，情報セキュリティリスクを抽出した．また，各リスクに対して発生可能性と影響度を評価した．この評価結果に基づき，信金・信組が優先的に対処すべき 25 個のリスクを選定した．次に，各リスクへの対策のインシデント防止効果と財務および人的コスト等を評価した．ここから，効果が高いために実施が望まれるものの，コストも高いために実施が見送られる可能性が高い対策を 4 つ選定した．最後に，ナッジの枠組みを参照し，4 つの対策の実施を信金・信組に働きかける促進策を 5 種類考案した．促進策案について予測される効果，および，実施のコストを管轄官庁関係者へのインタビューによって評価した結果，企業特性ごとの対策の好事例を管轄官庁が信金・信組に配信する促進策案が最も効果的であると評価された．総合考察では，促進策を実施するうえでのコストの課題について議論を展開した．また，経営層の対策関与の促進に対する示唆を提供した．

謝辞 対策および促進策案の評価等にご協力いただいた管轄官庁の関係者の皆様，リスク分析・評価にご協力いただいた皆様に，謹んで感謝の意を表する．

参考文献

[1] Healey, J., Mosser, P., Rosen, K. and Tache, A.: The Future of Financial Stability and Cyber Risk, The Brookings Institution (online), available from ⟨https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf⟩ (accessed 2021-02-13).

[2] Johnson, K.N.: Cyber Risks: Emerging Risk Management Concerns for Financial Institutions, *Georgia Law Review*, Vol.50, No.1, pp.131–142 (2015).

[3] Mijnhardt, F., Baars, T. and Spruit, M.: Organizational Characteristics Influencing SME Information Security Maturity, *Journal of Computer Information Systems*, Vol.56, No.2, pp.106–115 (2016).

[4] Camillo, M.: Cybersecurity: Risks and Management of Risks for Global Banks and Financial Institutions, *Journal of Risk Management in Financial Institutions*, Vol.10, No.2, pp.196–200 (2017).

[5] Soomro, Z.A., Shah, M.H. and Ahmed, J.: Information Security Management Needs More Holistic Approach: A Literature Review, *International Journal of Information Management*, Vol.36, pp.215–225 (2016).

[6] 金融庁：「金融分野におけるサイバーセキュリティ強化に向けた取組方針」のアップデートについて，金融庁（オンライン），入手先 ⟨https://www.fsa.go.jp/news/30/20181019-cyber.html⟩（参照 2021-02-13）．

[7] Bouveret, A.: Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, *IMF Working Paper*, Vol.2018, No.143, pp.1–28 (2018).

[8] 金融庁：金融分野のサイバーセキュリティレポート，金融庁（オンライン），入手先 ⟨https://www.fsa.go.jp/news/30/20190621_cyber/cyber_report.pdf⟩（参照 2021-02-13）．

[9] 日本経済新聞：処分庁から育成庁へ，金融行政を刷新　有識者会議が報告書，日本経済新聞（オンライン），入手先 ⟨https://www.nikkei.com/article/DGXLASDC17H2Z_X10C17A3EA4000/⟩（参照 2021-02-13）．

[10] 経済産業省：サイバーセキュリティ経営ガイドライン Ver 2.0，経済産業省（オンライン），入手先 ⟨http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf⟩（参照 2021-02-13）．

[11] 情報処理推進機構：中小企業の情報セキュリティ対策ガイドライン第 3 版，情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000055520.pdf⟩（参照 2021-02-13）．

[12] 情報処理推進機構：「2016 年度　中小企業における情報セキュリティ対策に関する実態調査」報告書，情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000058502.pdf⟩（参照 2021-02-13）．

[13] Ng, Z.X., Ahmad, A. and Maynard, S.B.: Information Security Management: Factors that Influence Se-

curity Investments in SMES, *Proc. 11th Australian Information Security Management Conference*, pp.60–74 (2013).
[14] Pohlmann, N., Reimer, H. and Schneider, W. (Eds.): ISSE/SECURE 2007 Securing Electronic Business Processes, Tawileh, A., Hilton, J. and McIntosh, S.: Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach, pp.331–339, Springer (2007).
[15] Moncayo, D. and Montenegro, C.: Information Security Risk in SMEs: A Hybrid Model Compatible with IFRS: Evaluation in Two Ecuadorian SMEs of Automotive Sector, *Proc. 6th International Conference on Information Communication and Management*, pp.1–6 (2016).
[16] 菅野泰子，島田裕次：情報セキュリティ対策における阻害要因の構造に関する企業規模別比較研究，日本情報経営学会誌，Vol.30, No.3, pp.109–121 (2009).
[17] 総務省：我が国のサイバーセキュリティ人材の現状について，総務省（オンライン），入手先 ⟨https://www.soumu.go.jp/main_content/000591470.pdf⟩（参照 2021-06-10）.
[18] Labuschagne, L. and Eloff, J.H.P.: Electronic Commerce: The Information-Security Challenge, *Information Management & Computer Security*, Vol.8, No.3, pp.154–157 (2000).
[19] Thaler, R.H. and Sunstein, C.R.: Nudge: Improving Decisions About Health, Wealth, and Happiness, Penguin Books (2009).
[20] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S.: Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online, *ACM Computing Surveys*, Vol.50, No.3, article 44, pp.1–44 (2017).
[21] 山崎由香里：アノマリーを活かしたナッジングのためのフレームワーク：ナッジツールのレビューと整理，成蹊大学経済学部論集，Vol.49, No.1, pp.51–81 (2018).
[22] Kahneman, D. and Tversky, A.: Prospect Theory: An Analysis of Decision under Risk, *Econometrica*, Vol.47, No.2, pp.263–292 (1979).
[23] Robitaille, N., House, J. and Mazar, N.: Effectiveness of Planning Prompts on Organizations' Likelihood to File Their Overdue Taxes: A Multi-Wave Field Experiment, *Management Science*, Articles in Advance, pp.1–14 (online), DOI: 10.1287/mnsc.2020.3744 (2020).
[24] 金融庁：業界団体との意見交換会において金融庁が提起した主な論点　全国信用金庫協会, 金融庁（オンライン）, 入手先 ⟨https://www.fsa.go.jp/common/ronten/201801/04.pdf⟩（参照 2021-02-13）.
[25] 全国信用金庫協会：2020 年度全信協事業計画，全国信用金庫協会（オンライン），入手先 ⟨https://www.shinkin.org/about/disclosure/pdf/05.pdf⟩（参照 2021-02-13）.
[26] 情報処理推進機構：情報セキュリティマネジメントと PDCA サイクル，情報処理推進機構（オンライン），入手先 ⟨https://warp.da.ndl.go.jp/info:ndljp/pid/11561275/www.ipa.go.jp/security/manager/protect/pdca/risk.html⟩（参照 2021-02-13）.
[27] トレンドマイクロ：インシデント対応ボードゲーム金融版，トレンドマイクロ（オンライン），入手先 ⟨https://resources.trendmicro.com/jp-docdownload-form-m059-web-incidentboardgamesfinance.html⟩（参照 2021-02-13）.
[28] 情報処理推進機構：制御システムのセキュリティリスク分析ガイド第 2 版，情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000069436.pdf⟩（参照 2021-02-13）.
[29] 内閣サイバーセキュリティセンター：重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版），内閣サイバーセキュリティセンター（オンライン），入手先 ⟨https://www.nisc.go.jp/active/infra/files/tebikisho.zip⟩（参照 2021-02-13）.
[30] 重要生活機器連携セキュリティ協議会：製品分野別セキュリティガイドライン　金融端末（ATM）編　セキュリティ対策検討実践ガイド—犯罪事例の分析と対策立案—Ver. 2.0”，重要生活機器連携セキュリティ協議会（オンライン），入手先 ⟨https://www.ccds.or.jp/public/document/other/guidelines/[CCDS]ATM 編別冊_セキュリティ対策検討実践ガイド (概要)_Ver2.0.pdf⟩（参照 2021-02-13）.
[31] PwC Japan グループ：経済犯罪実態調査 2014 金融業界分析版　金融業界にとっての脅威, PwC Japan グループ（オンライン），入手先 ⟨https://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/economic-crime-survey-industry2014financial.pdf⟩（参照 2021-02-13）.
[32] 中尾康二（編）, 北原幸彦, 竹田栄作, 中野初美, 原田要之助, 山下　真（著）：ISO/IEC27002:2013 情報セキュリティ管理策の実践のための規範　解説と活用ガイド，日本規格協会 (2015).
[33] 中條武志：人間信頼性工学：エラー防止への工学的アプローチ，静岡県放射線技師会，Vol.22, No.21, pp.29–33 (2012).
[34] Dolan, P., Hallsworth, M., David, H., Dominic, K. and Ivo, V.: MINDSPACE: Influencing Behaviour through Public Policy, The Institute for Government (online), available from ⟨https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf⟩ (accessed 2021-02-13).
[35] Acquisti, A., John, L.K. and Loewenstein, G.: The Impact of Relative Standards on the Propensity to Disclose, *Journal of Marketing Research*, Vol.49, No.2, pp.160–174 (2012).
[36] Brandon, A., List, J.A., Metcalfe, R.D., Price, M.K. and Rundhammer, F.: Testing for Crowd Out in Social Nudges: Evidence from a Natural Field Experiment in the Market for Electricity, *Proc. National Academy of Sciences of the United States of America*, Vol.116, No.12, pp.5293–5298 (2019).
[37] 内閣サイバーセキュリティセンター：平成 28 年度企業のサイバーセキュリティ対策に関する調査報告書，内閣サイバーセキュリティセンター（オンライン），入手先 ⟨https://www.nisc.go.jp/inquiry/pdf/kigyoutaisaku_honbun.pdf⟩（参照 2021-02-13）.
[38] Kwon, J., Ulmer, J.R. and Wang, T.: The Association between Top Management Involvement and Compensation and Information Security Breaches, *Journal of Information Systems*, Vol.27, No.1, pp.219–236 (2013).
[39] Singh, A.N., Gupta, M.P. and Ojha, A.: Identifying Factors of “Organizational Information Security Management,” *Journal of Enterprise Information Management*, Vol.27, No.5, pp.633–667 (2014).
[40] Jost, J.T. and Hunyady, O.: The Psychology of System Justification and the Palliative Function of Ideology, *European Review of Social Psychology*, Vol.13, pp.111–153, Taylor & Francis (2002).
[41] Levine, J.M.: Solomon Asch's Legacy for Group Research, *Personality and Social Psychology Review*, Vol.3, No.4, pp.358–364 (1999).

稲葉 緑 （正会員）

2005 年名古屋大学大学院環境学研究科修了．（独）交通安全環境研究所自動車安全研究領域，電気通信大学大学院情報システム学研究科，JR 東日本研究開発センター安全研究所を経て，現在，情報セキュリティ大学院大学准教授．情報セキュリティ等の人・マネジメントの側面に関する研究に従事．情報処理学会論文誌編集委員等．博士（心理学）．

菊池 大地

2020 年情報セキュリティ大学院大学情報セキュリティ研究科修了．現在，金融庁総合政策局秘書課情報課統括室内閣府事務官．金融庁内の情報セキュリティ水準の維持等を図るため，庁内システム運営，職員教育，庁内セキュリティポリシー改定等の職務に従事．