Vol.2019-IOT-47 No.7
Vol.2019-SPT-35 No.7
2019/9/19

中小金融機関における情報セキュリティ向上のためのリスク評価

菊池 大地[†1]　稲葉 緑[†1]

概要：金融機関でのサイバーセキュリティの確保は、金融システム全体の安定のための喫緊の課題となっている。特に中小金融機関における基礎的なサイバーセキュリティ管理態勢の整備により、業界全体の底上げを図ることが大きな課題である。しかし、官公庁が中小金融機関にセキュリティ対策の必要性を訴えているにもかかわらず、十分な対策はとられていない。その理由としては、経営資源の不足や経営層の無関心等の阻害要因が挙げられる。これらの阻害要因を踏まえると、中小金融機関が対応すべきリスクを明らかにするためにリスク評価を行ったうえで、適切な情報セキュリティ対策を行うことが重要である。本発表では、インタビューや国際規格のレビュー等を基に、中小金融機関におけるリスクを評価する。

キーワード：情報セキュリティ、金融機関、中小企業、リスク評価、

Risk assessment for improving information security in small and medium-sized financial institutions

DAICHI KIKUCHI[†1]　MIDORI INABA[†1]

Abstract: Securing cyber security in the financial institutions is an urgent issue for stabilizing the overall financial system. Particularly, the development of cyber security management in small and medium-sized financial institutions is required to increase the security in the financial sector as a whole. However, despite the fact that government have appealed to them the need for security measures, no adequate measures have been taken. Inhibitory factors have shown to be such as a lack of management resources and little concern about the security of the executives of the small and medium-sized institutions. According to these implications, we aim at proposing the measures that these institutions should focus on with limited resources as well as the way to raise the executive's' security awareness. For this purpose, we are assessing the security risks in the small and medium-sized financial institutions based on interviews and reviews of international standards.

Keywords: Information security, financial institutions, small and medium enterprises, risk assessment

1. はじめに

インターネットの普及拡大等に伴い、金融分野のサイバーセキュリティの確保は、金融システム全体の安定のための喫緊の課題となっている。このような状況を踏まえて、金融庁は､「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」を平成 27 年に公表した［1］。本取組方針では、金融分野へのサイバー攻撃の脅威に対抗すべく今後取り組むべき方針を明らかにし、金融機関、金融サービス利用者及び関係機関と問題意識を共有することを目的にしている。金融庁では、本取り組み方針に従い、金融分野のサイバーセキュリティ対策向上のため、以下の 5 項目に取り組んできた。

1) サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
2)金融機関同士の情報共有の枠組みの実効性向上
3)業界横断的演習の継続的実施
4)金融分野のサイバーセキュリティ強化に向けた人材育成
5)金融庁としての態勢構築

これまでの取り組みの結果、特に中小金融機関においては、基礎的なサイバーセキュリティ管理態勢の整備により業界全体の底上げを図ることが大きな課題であることが判明している[2]。本取組方針によると、サイバーセキュリティ対策が進んでいる金融機関は、サイバーセキュリティを重大なコーポレートリスクと捉え、サイバーセキュリティに着眼したリスク評価の実施、対応態勢の構築、コンティンジェンシープラン の整備等の取り組みを行っている。一方、サイバーセキュリティを単にシステム部門などの担当部署が対応すべきリスクと捉えている金融機関では依然として対応が不十分であるとしている。

経済産業省のサイバーセキュリティガイドライン[3]においても、サイバーセキュリティは経営問題であることが強調されている。同ガイドラインにおいては、

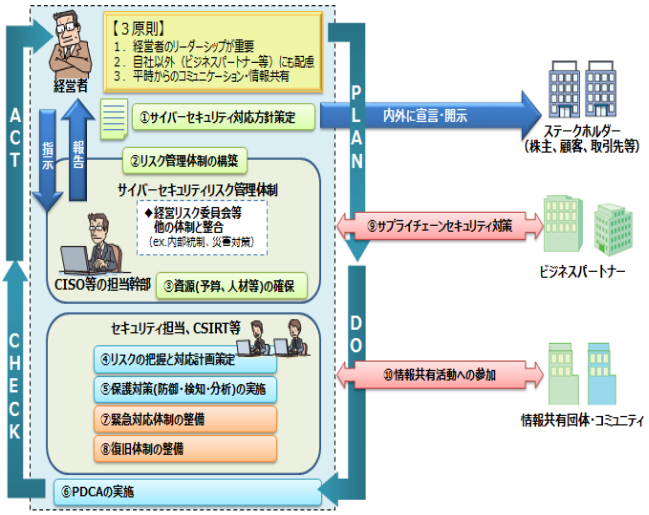
・企業の IT の利活用は、業務の効率化による企業の収益性向上だけでなく、グローバルな競争をする上で根幹をなす企業として必須の条件となっていること
・サイバー攻撃は年々高度化、巧妙化してきており、サ

†1 情報セキュリティ大学院大学
Graduate School of Information Security INSTITUTE of Information Security

Vol.2019-IOT-47 No.7
Vol.2019-SPT-35 No.7
2019/9/19

イバー攻撃によって純利益 の半分以上を失う企業が出るなど、深刻な影響を引き起こす事件が発生していることなどの背景を踏まえると、サイバーセキュリティ対策の実施は将来の事業活動・成長に必須なものと位置づけて経営者が関与することが責務であると指摘している。

また、同ガイドラインでは、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」がまとめられている（図表 1）。

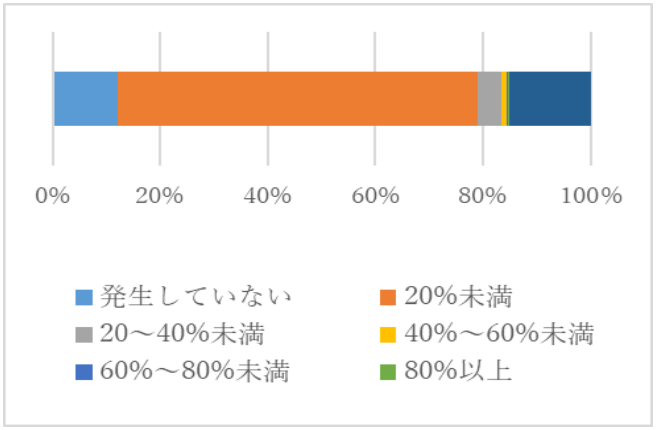


図表 1 サイバーセキュリティ経営ガイドライン概要図[3]
Figure 1 Outline of cyber security management guidelines [3]

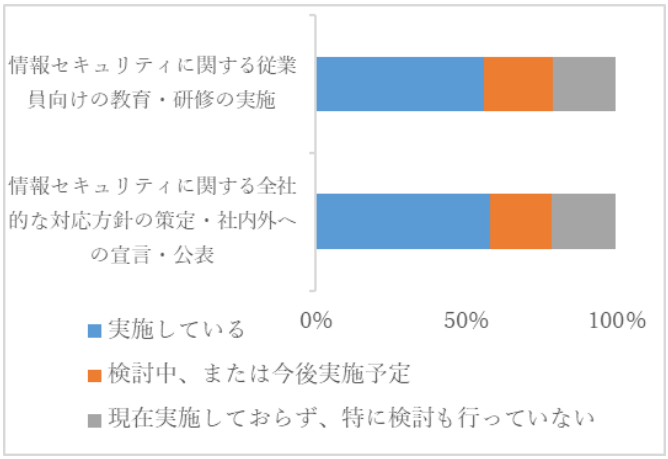
こうした訴えかけがなされているにも関わらず、中小企業において十分に対策はとられていない。このことは、経済産業省が行った情報処理実態調査[4]においても、明らかである。同調査における、企業の「情報セキュリティ対策費用の対 IT 関係支出総額比」では、「20%未満」の企業が67.1%と最も多く、情報セキュリティ費用が発生していない企業も 12.0%存在した（図表 2）。

また、「情報セキュリティ対策の実施状況」をみると、「情報セキュリティに関する全社的な対応方針の策定・社内外への宣言・公表」「情報セキュリティに関する従業員向けの教育・研修の実施」といった比較的コストのかからない対策でも、およそ半数の企業が実施していなかった。

そこで、中小金融機関が情報セキュリティ対策を行わない阻害要因について文献調査を実施する。文献調査で明らかになった阻害要因を踏まえた上で、効果的な情報セキュリティ対策を明らかにすることを目指し、リスクを評価する。



図表 2 企業の情報セキュリティ対策の対 IT 関係支出総額比[4]より編集
Figure 2 Edited from the Comparison of total IT-related spending on corporate information security measures [4]



図表 3 情報セキュリティ対策の実施状況[4]より編集
Figure 3 Edited from the implementation status of information security measures [4]

2. 関連研究

2.1 Sean らの研究[5]

中小企業の経営層がこのような情報セキュリティ対策を行わない要因について、Sean らは［5］、中小企業における、情報セキュリティリスクマネジメント能力向上を目的に、シンガポールをはじめとした中小企業の CTO やマネジャーに対してインタビューによる調査を実施した。結果、インタビュー対象の企業においては、情報セキュリティの改善に対する投資については重要性を認識していたものの、自組織内でのリスクの洗い出しを行っている企業はなかった。中小企業が情報セキュリティ行動を起こさない動機付けについて、インタビュー結果より以下の 3 つに分類されることが判明した。まずは、①外的要因である。これは、消費者が購買決定をする際の企業のイメージや評判をセキュリティインシデントによって損ないたくないときにのみ情報セキュリティ対策を講じている現状が明らかになった。

また、同業態・同規模の他企業の情報セキュリティ水準に合わせようとする動きも頻繁にみられていた。次に②意識の欠如である。企業規模が小さいから自社は狙われないだろう、内部からの脅威はないだろうといった情報セキュリティリスク分析を実施する個人の認識による誤解が存在し、組織の意思決定に悪影響が現れる。最後に③組織の意思決定である。中核となるビジネス活動に集中して投資を行い情報セキュリティへの投資の優先順位を低減しており、重大なインシデントが発生しない限り見直しを行っていない。また、情報セキュリティ対策を実施しているにもかかわらず、十分なレベルまで行っていない企業も多くみられた(バックアップを保存していたが、バックアップファイルの可用性を確認していない等)。今後の情報セキュリティ対策においては、以上の 3 点を踏まえた比較的低コストかつ専門知識を必要としないリスクアセスメント方法論が必要であると主張している。

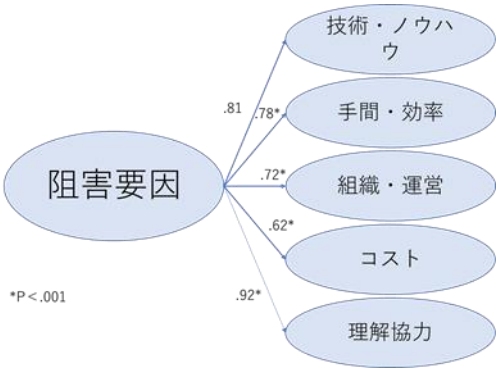
2.2 菅野らの研究[6]

菅野ら[6]は、中小企業の情報セキュリティ対策に資するため、企業の情報セキュリティ対策の実施を妨げる阻害要因に着目した。そこで、企業の情報セキュリティ担当者を対象に、情報セキュリティ対策の実施に影響を及ぼす阻害要因に関するアンケート調査を行った。そして、探索的因子分析と構造式モデリング（SEM） を行い、情報セキュリティ対策に関する阻害要因の構造モデルを作成した。探索的因子分析の結果、企業における情報セキュリティ対策の阻害要因は「技術・ノウハウ因子」、「組織運営因子」、「手間・効率因子」、「理解・協力因子」、「コスト因子」の五つに分類された 。これらの五因子が、企業における情報セキュリティの阻害要因という高次の因子を形成していると仮定して、SEM を用いた二次因子モデルを形成し、妥当性を検証した（図表 4）。

さらにこの SEM に基づいて、大企業のグループと中小企業の情報セキュリティ阻害要因の共通性と相違点を検討した。結果、因子構造については同様の構造であることが証明された。一次因子の比較をした結果、大企業と中小企業を比較した場合、技術・ノウハウとコストについて、中小企業においては、大企業より困難に感じている度合いが大きかった。一方で、情報セキュリティ対策の必要性を認識していたとしても、技術・ノウハウがない、組織体制が整っておらずリソースの割り当てがない等の理由で、対策の実施に困難を感じている状況は、企業規模によらず同様だった。

2.3 是永らの研究[7]

是永[7]は、大企業と比較して、予算や人材が限られている中小企業における情報セキュリティ管理者について、考察を行った。是永によると、中小企業における情報セキュリティを阻害する要因として、①手間・コストがかかる②対策をどこまでやればいいか不明③知識ノウハウがない④専門家がいないという 4 点を指摘している。特に、知識・



図表 4　阻害要因の二次因子モデル[5]より編集
Figure 4 Edited from the Inhibitory factor secondary model [5]

ノウハウの欠如・専門家の不在の 2 点が特に課題であるとし、情報セキュリティ管理者が必要であると述べている。情報セキュリティ管理者の役割･求められる技能としては、情報システムの利用部門にあって、情報セキュリティリーダーとして部門の業務遂行に必要な情報セキュリティ対策や組織の定めた情報セキュリティ諸規定の目的・内容を適切に理解し、情報システムを安全に活用するため、情報セキュリティが確保された状況を実現し、維持改善する者であるとしている。一方で中小企業においては人材育成に十分な時間が取れないため、こうした人材を育成することが難しい。したがって、中小企業においては、情報セキュリティ管理者を選定するにあたり、最低限以下 3 点を抑えるべきであるとしている。

① 守るべきものの把握・守る方法の決定を行う
情報資産の管理台帳を作成する。それぞれのリスクについて評価し、セキュリティポリシーを作成する。
② 一般社員に対する教育を行う
IPA の教材等を用いて SNS の利用やトラブルを予防する
③ 定期チェックを行う
ログの分析・システム監査を実施する。あるいは外部に委託する。

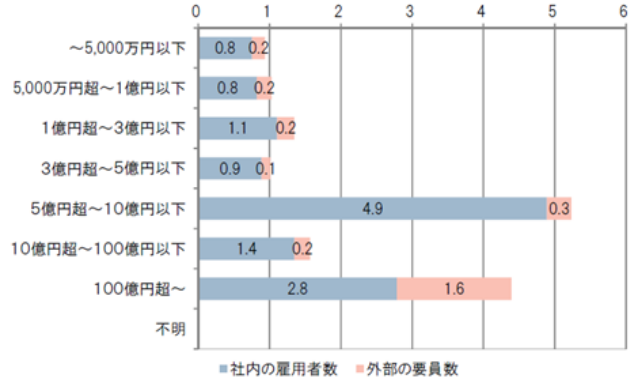
2.4 先行研究のまとめ

上記の研究より、中小企業においては技術やノウハウの欠如、対策を行う手間やコスト、企業の投資戦略といった組織運営上の問題等によって情報セキュリティ対策が阻害されていることが分かった。特に技術・ノウハウの欠如、専門家や情報セキュリティ管理者等の人材の欠如が深刻であった。

中小企業における人材の欠如は､経済産業省が平成 29 年度に行った情報処理実態調査[4]においても、明らかになっ

Vol.2019-IOT-47 No.7
Vol.2019-SPT-35 No.7
2019/9/19

ている。情報セキュリティに関する一社平均専任要員数は 1,8 人（社内の雇用者数 1,4 人、外部の要因 0,4 人）であったが、資本金規模別にみると、資本金が 1 億円以下の企業においては、情報セキュリティに関する一社平均専任要員数は 1,0 人と平均を下回っており、中小企業においては、情報セキュリティに従事する人員が不足していることが分かる（図表 5）。



図表 5 情報セキュリティに関する一社平均専任要員数[4]
Figure 5 One company's average full-time staff for information security [4]

3. 目的

このように、中小金融機関において、経営資源やセキュリティ人材等のリソースが限られており、経営層も知識が不足している状況が判明した。金融庁が 2019 年 6 月に公表した「金融分野のサイバーセキュリティレポート」[8]においても、信用金庫・信用組合については、業界全体としての遅れが指摘されている。遅れている要因としてサイバーリスクに対する経営陣の危機感が希薄であることに加え、専門の担当者もいない中で地域銀行のような共助態勢もないことが挙げられている。しかし、これまでの研究では、技術・ノウハウが不足している中小企業に対して、比較的低コストかつ専門知識を必要としないリスクアセスメント方法が必要であると述べつつも、その具体的な対策案については明らかにされていない。さらに、中小企業一般に対する調査に比べて、中小金融機関に対する調査は不足している。

そこで、中小金融機関におけるリスクを評価することを本研究の目的とする。

なお、一概に金融機関といえども、保険業や証券業・預金取扱業務など、それぞれの業務内容は幅広く、保有するリスクも異なる。

本研究では中小金融機関の中でも、中小規模の預金取扱金融機関、具体的には信用金庫及び信用組合といった金融機関を対象とする。信用金庫及び信用組合に着目した理由としては、「金融分野のサイバーセキュリティレポート」[8]でも特に業界全体としての遅れが指摘されていること、業務上、不正出金などのサイバー攻撃による被害がより甚大になりやすいこと、が挙げられる。

4. 方法

技術・ノウハウが不足している中小金融機関における有効な具体的対策として、情報セキュリティリスク分析を行うことが必要だと考えた。何故なら全ての情報セキュリティ脅威に対して、適切な判断をし、対策を行うことは難しい。そこで、中小金融機関においては、考えられる情報セキュリティ対策を全て行うのではなく、組織規模等を踏まえ、どの程度の情報セキュリティ対策まで行うべきか、整理を行うことが重要であると考えた。リスク評価にあたり、下記の手順で進めていく。

4.1 具体的リスクの特定

まず、中小金融機関に起こり得る、具体的な情報セキュリティ上のリスクの特定を行う。

中小金融機関に起こり得る、具体的な情報セキュリティ上のリスクの特定については、トレンドマイクロが提供している、金融業界向け「インシデント対応ボードゲーム」を参考にした。同ボードゲームにおいては、金融機関に起こり得る情報セキュリティ上のイベントが 45 項目例示されているが、その中で自組織の資産及び自組織のブランドイメージの 2 つに影響が生じるイベントとして、1.ATM からの不正出金、2.自組織の web サイトの改ざん、3.自組織のサービスが応答不能 4.自組織を装った不審メールが拡散、5.情報漏洩の発生が挙げられる。そこで、これらを金融機関の情報セキュリティ上の脅威と定義した。

4.2 フォルトツリー解析

このような脅威が発生する原因として考えられる事象を引き起こす要因についてフォルトツリー解析を行っている（図表 6 参照）。本研究では、技術的な要因よりもマネジメントに関する要因に焦点を当てる。

4.3 脅威の要因に対するリスク評価

フォルトツリー解析で明らかにした脅威の要因について、リスクマネジメントの観点から、発生可能性・影響度評価を行い研究会当日に報告する予定である。（図表 6 参照）。

4.4 セキュリティ対処法の分類

4.3 の評価に基づき、どのようにリスク対処するか整理する。

発生可能性・影響度評価とリスクの対処法との関係性については、IPA 等でも用いられている[9]以下の考え方で整理する。（図表 7）

① 発生可能性及び影響度が低い場合

そのリスクの持つ影響力が小さいため、特にリスクを低減するためのセキュリティ対策を行わず、許容範囲内として受容する（リスク保有）。

原因として考えられる事象	原因の原因			発生可能性評価	影響度評価
偽装カードが作成された	マルウェア設置				
	自組織に対するハッキング	パスワードの流失			
		トランザクションの改竄			
		情報及びアプリケーションへの第三者による不正アクセス			
		不正ログオン			
	暗号鍵が解読	暗号鍵の管理体制の不備			
	顧客に対するハッキング	ソーシャルエンジニアリングによるパスワード流出			
	スキミング	（カード作成後のパスワード等については推測またはソーシャルエンジニアリング等）			
顧客のキャッシュカードが盗まれた	盗難（物理セキュリティ）				
顧客のスマホ、PCが乗っ取られた	SIMハイジャックによる不正操作				
	顧客のスマホ紛失による悪意者からの不正操作				
	マルウェア感染				
ATMがマルウェアに感染	マルウェア設置	ATM保守会社PCからの感染（サプライチェーンセキュリティの不備）			
オンラインバンクのID・認証情報の窃取					
ATMにおける物理的被害	鍵のこじ開け				
	ATMごと運搬				
システムに対して、第三者が不正アクセス	特権アクセス権の詐取				
	ユーティリティプログラム不正利用				
	自サイトが踏み台になる				
サイト更新者がマルウェア感染していた	更新端末の管理不足				
物理的破損	物理的侵入				
	火災				
	自然災害				
	装置の破損				
	サポートユーティリティの破損				
	通信ケーブル、電源ケーブルの破損・妨害				
システムインシデント	開発環境と試験環境及び運用環境の差によるインシデント				
	脆弱性を突いた攻撃				
	運用ソフトウエアのインシデント				
	ゼロデイ攻撃				
	セキュリティアップデートによる不具合				
	システム統合、リプレイス切替による不具合				
	サービス妨害攻撃（DoS）				
	マルウェア感染（特にランサムウェア）				
外的要因によるサービス影響	国内金融基盤の停止				
	国際金融基盤の停止				
	他銀の停止				
フィッシングサイトによる情報流出	アドウェアによる誘導				
	ソーシャルエンジニアリングによる誘導				
偽装アプリの蔓延	アドウェアによる誘導				
	ソーシャルエンジニアリングによる誘導				
標的型メール	関連会社への攻撃				
なりすまし	メール盗聴によるなりすまし				
	愉快犯・効率狙いのなりすまし（楽天銀行の例のように）				
自組織内からの流失	善意の従業員の失敗	モバイルデバイスの紛失			
		テレワーキング中の通信の傍受			
		公衆ネットワーク使用時の情報漏洩			
		電子メールの誤送信			
		資産の返却忘れ			
		PC等の媒体からの情報流失	取り外し可能媒体による情報流失		
			媒体の廃棄ミスによる情報流失		
			媒体の輸送ミスによる情報流失		
		外部サービス（パブリッククラウド等）の不適切な公開設定・権限設定			
		機器・書類等の盗難			
	悪意の従業員による故意の流失	雇用前の従業員による情報流失			
		雇用中の従業員による情報流失	特権を用いた情報抽出・持出		
			特権を用いた機器の設定変更		
			脆弱性をついた攻撃		
		雇用終了後の従業員による情報流失			
		アクセス権の管理違反			
	取引先・契約先の失敗	秘密保持契約違反			
		供給者のインシデント			
		機器・書類等の盗難			
外部からの攻撃による流失	マルウェア設置				
	脆弱性を突いた攻撃	サーバ等機器に対する攻撃			
		Webサイト等に対する攻撃			

図表 6 リスク評価表

Figure 6 risk assessment table

② 発生可能性及び影響度が高い場合

脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去る（リスク回避）。

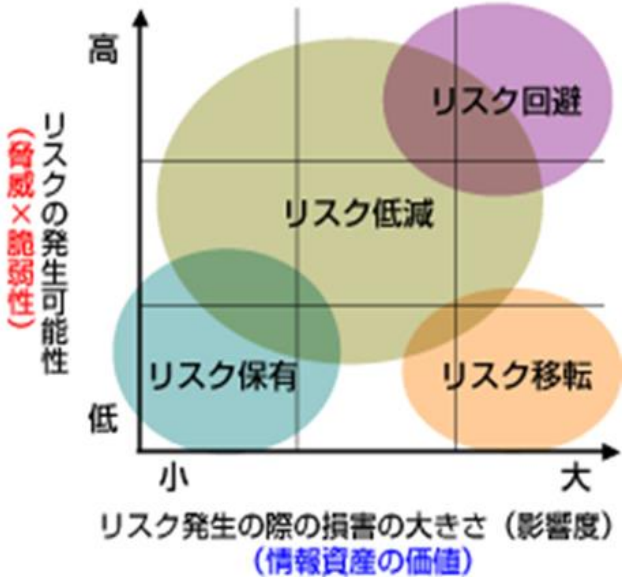
③ 発生可能性が低く、影響度が高い場合

リスクが顕在化したときに備え、社内の情報システムの運用を他社に委託するなど、リスクを他社へ移転する（リスク移転）。

④　上記①～③に当てはまらない場合

脆弱性に対して情報セキュリティ対策を講じることにより、脅威発生の可能性を下げる（リスク低減）。

上記のリスク対処方法のうち、リスク保有をとるべきリスクであれば、脅威を受容する。リスク回避をとるべきリスクであれば、脅威の発生原因となるシステム等を中小金融機関内で採用しない。リスク移転をとるべきリスクであれば、外部にアウトソースすることで被害の発生を最小限にできる、と考える。したがって経営資源が限られる中小金融機関において、率先して対策を行うべき情報セキュリティリスクはリスク低減であると考えられる。そこで、情報セキュリティリスクを分類した表を作成することを通じて、中小金融機関として率先して取り組むべき情報セキュリティリスクを明らかにすることが可能になるのではないかと考える。



図表 7　リスクへの対応概念図[9]

Figure 7 Conceptual diagram for dealing with risks [9]

4.5 今後の研究

今後の研究としては、現在行っているフォルトツリー解析について､インタビューやアンケートを活用することで、網羅性を確保していく。

また、リスク分析で洗い出した情報セキュリティ上のリスクに対して、具体的な対策を考察していく。具体的な方法としては、

①既存の枠組みの活用、②インタビュー形式による確認、③ISO/IEC27002 等を用いた管理策の妥当性評価、④新規の対策の考察等の方法が挙げられる。

① 既存の枠組みの活用については、リスク分析で明らかになったリスクについて、金融 ISAC での情報共有や FISC のサイバーセキュリティワークショップ、金融庁のサイバーセキュリティ演習等の対応策と、情報セキュリティ上のリスクとの関係を確認する。

② インタビュー形式による確認については、中小企業の実態について、実際に中小企業の情報セキュリティ業務に従事する人を対象にしたインタビューを行い、企業の実態を踏まえた対策を確認する。

③ 情報セキュリティ上のリスクに対して、ISO/IEC27002 における情報セキュリティ対策群から、対策方法を選定する。なお、ISO/IEC27002 における情報セキュリティ対策群においては、重要な対策が記載されているものの、そのすべてを中小企業に適応することは、予算や難易度等の制約があり、困難である。そこで、情報セキュリティ対策群について、管理策を実行したときのコスト、管理策を実行に移す際の難易度等について評価することによって、ISO/IEC27002 に記載のある、情報セキュリティ対策群の中で、中小企業における優先度を選定する。

④ 上記の①から③で対策しきれない脅威について新たな対策を考える。例えば心理的アプローチの観点から、ナッジを利用する、動機や規範をコントロールして情報セキュリティ対策を取らせるなどを用いた具体的な対策を考える。

今後の研究では、①から④で洗い出したリスク及びそれらの対策案について、インタビュー等を通じて評価データを集め、その妥当性について検証する。

その後、中小企業における対策の妥当性が証明されたうえで、中小金融機関向けの事情を鑑みて、金融機関にも適用可能か確認する。

参考文献

[1] 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」の公表について
https://www.fsa.go.jp/news/27/20150702-1.html
[2] 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
https://www.fsa.go.jp/news/30/20181019-cyber.html
[3] 経済産業省　サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
[4] 経済産業省　情報処理実態調査　報告書
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H29_report.pdf
[5] Sean B. Maynard, Atif Ahmad, Zhi Xian Ng, Information Security Management_Factors that Influence Security Investments in SMES 2013.
[6] 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 30 巻 3 号　2009.
[7] 是永逸郎, 中小企業における情報セキュリティ管理者の必要性とその役割に関する考察 Global Management (5), 4-11, 2016-03
[8] 金融庁 「金融分野のサイバーセキュリティレポート」の公表について https://www.fsa.go.jp/news/30/20190621-cyber.html
[9] IPA 情報セキュリティマネジメントと PDCA サイクル
https://www.ipa.go.jp/security/manager/protect/pdca/risk.html