# 諸外国の金融分野のサイバーセキュリティへの取組みに関する調査研究

# 【報告書】

2020 年 3 月 31 日

株式会社 NTTデータ 経営研究所

# 目次

# 序論

金融機関は従来から情報システムを利用してサービスを提供している。今般では、金融機関がコストや柔軟性の観点からクラウドサービスを利活用する等、デジタライゼーションが進んでいるところである。

一方、国内外においてサイバーセキュリティの脅威が増している。2017 年には世界的なランサムウェア感染、2019 年には認証情報を窃取するマルウェアの流行等、大規模なサイバー攻撃の事案が確認されている。国内金融機関においても、ホームページの改ざん、暗号資産の不正流出、不正アクセスによる顧客情報の漏洩、DDoS 攻撃等、複数のサイバー攻撃が確認されており、攻撃対象も預金取扱金融機関にとどまらず、複数の業態にまで拡大するなど増加傾向にある。

また我が国においては、東京 2020 オリンピック・パラリンピック競技大会等、国際的な大規模イベントの開催を予定しており、金融機関を含む重要インフラ事業者はサイバー攻撃のターゲットとなる蓋然性が高まっている。

こうした金融分野のサイバーセキュリティに関する状況が変化する中、金融庁では「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」をアップデート（平成 30 年 10 月）し、官民が一体となって金融分野のサイバーセキュリティ強化に取り組んでいる。金融機関においてもサイバーセキュリティ強化に向けて、ガバナンス強化、リスク管理、インシデント対応手順の整備等をはじめとする、対応態勢の構築・高度化を進めてきた。

本調査の目的は、金融分野におけるサイバーセキュリティを更に強化していくにあたり、参考となる諸外国のサイバーセキュリティに関する取組みを確認することである。また、中小金融機関のサイバーセキュリティ強化に資するために諸外国における金融機関の取組みを調査し、その結果を基に示唆を整理した。

## 1. 本調査研究のアプローチ

本調査研究においては、諸外国のサイバーセキュリティの取組みを確認することを目的に、各国の規制・ガイドラインに関する文献の調査、インタビューおよびアンケートを実施した。

### (1) 調査対象国・地域

以下の 3 つの国・地域について、前回調査[1]以降、過去 5 年間の規制・ガイドラインの更新を調査した。

① 米国
② EU
③ 英国

加えて、近年サイバーセキュリティに関する取組みを強化している

④ シンガポール

を、新たに調査対象としている（以下、上記①～④を合わせて「調査対象国」という）。

### (2) 調査期間

2020 年（令和 2 年）1 月 7 日から 2020 年（令和 2 年）3 月 31 日

### (3) 調査方法

調査対象国の監督当局および関連団体が公表している資料を確認した他、金融機関等に対し、インタビュー（電話）もしくはアンケートを実施した。

[1] 諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書（2015 年 3 月 31 日）
https://www.fsa.go.jp/common/about/research/20150706-4/01.pdf

(4) 調査内容

① 調査対象国別の調査

調査対象国における、サイバーセキュリティの取組みを把握することを目的に、各国のサイバーセキュリティに関する規制・ガイドラインを調査した。

**表 1 対象国の調査項目**

| 項目 | | 調査内容 |
|---|---|---|
| サイバーセキュリティ関係当局 | | 調査対象国のサイバーセキュリティに関係する当局の役割等。 |
| 調査対象概要 | | 今回対象とした規制・ガイドラインの概要。なお、個別のガイドライン・規制の概要・特徴は各規制・ガイドラインに記載。 |
| 各規制・ガイドライ | 目的・経緯 | 各規制・ガイドラインの作成された目的および経緯に加え、各規制・ガイドラインの利用方法。 |
| | 概要 | 各規制・ガイドラインの要請事項の概要。 |
| | 特徴 | 各規制・ガイドラインについて特徴のある内容。<br>なお、特筆すべき事項がない規制またはガイドラインについては、本項目を記載していない。 |
| インタビューまたはアンケート | | 調査対象国における金融機関のサイバーセキュリティ担当者または金融機関の実務に詳しい有識者を対象に、金融機関のサイバーセキュリティのガバナンス、リスク管理の状況について、インタビューまたはアンケートを実施し、その結果をまとめた。 |

② 調査対象国のまとめ

「①調査対象国別の調査」における結果を踏まえ、調査対象国ごとのアウトソーシングに関するガイドラインの内容を基に、金融機関がアウトソーシングする際に求められている事項を比較した。

③ 共助・演習の取組みの調査

調査対象国における共助の取組みを確認するため、情報共有機関が提供する機能を調査した。加えて、実施されている演習を調査した。

**表 2 対象国の調査項目**

| 項目 | 調査内容 |
|---|---|
| 共助に関する取組み | 調査対象国における情報共有機関が提供する共助に関する取組み。 |
| 演習 | 調査対象国における当局が関係する演習およびその他の演習。 |

## 2. 米国におけるサイバーセキュリティ

### (1) 米国のサイバーセキュリティ関係当局

米国における金融監督は、当該金融機関の業態に応じて、FRB（Federal Reserve System・連邦準備制度理事会）、OCC（Office of the Comptroller of the Currency・通貨監督庁）、FDIC（Federal Deposit Insurance Corporation・連邦預金保険公社）等により実施されており、それぞれがサイバーセキュリティも含めて監督を行っている

また、金融機関の監督の統一化を促進するため、これらの当局の連邦審査における原則、基準、報告書様式は、FFIEC（Federal Financial Institutions Examination・連邦金融機関検査評議会）が統一して定めている。

### (2) 米国の調査対象概要

今回、米国における調査は、米国のサイバーセキュリティ対策の基礎となっている NIST の「Cybersecurity Framework」に加え、FFIEC が提供する「IT Handbook Information Security」及び、「IT Handbook　Outsourcing Technology Services」、「Cybersecurity Assessment Tool」を調査対象とした。

IT Handbook は、FFIEC によって作成された、検査官が金融機関を検査する観点や基準をまとめたガイドラインである。情報システムにおけるセキュリティレベルの評価を行うために必要となる要素や、アウトソーシングを行う際のリスク管理手法等が記載されている。

「Cybersecurity Assessment Tool」は、金融機関が自組織におけるサイバーリスクの識別と、サイバーセキュリティの成熟度レベルの評価を実施するために公表されたものである。

また、上記の文献に加えて、補足として、サイバーセキュリティに関する民間団体が提供する「Cybersecurity Profile」、「Cybersecurity Capacity-building Tool Box for Financial Organizations」を調査の対象とした。いずれの文献も、中小規模の金融機関が利用することを想定し、質問数を限定する等の考慮がされている点が特徴として挙げられる。

**表　3　米国の調査対象文献一覧**

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 1 | NIST（National Institute of Standards and Technology・米国国立標準技術研究所） | Cybersecurity Framework[2] | 重要インフラ事業者等が自主的にサイバーセキュリティリスクを管理するためのフレームワーク |

[2] Cybersecurity Framework: https://www.nist.gov/cyberframework

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 2 | FFIEC（Federal Financial Institutions Examination Council・米国連邦金融機関検査協議会） | IT Handbook Information Security[3] | 金融機関の情報システムに対するセキュリティリスクを評価するためのガイドライン |
| 3 | | IT Handbook Outsourcing Technology Services[4] | 金融機関がサードパーティへの委託を実施する際の、リスク管理プロセスを確立し、当該プロセスを評価するための手順を示すガイドライン |
| 4 | | Cybersecurity Assessment Tool[5] | 金融機関が自組織におけるリスクの識別とサイバーセキュリティの成熟度レベルを評価するためのツール<br>成熟度レベルの一部の定義には「IT Handbook Information Security」を満たす水準が設定されている |
| 5【補足①】 | FSSCC（Financial Services Sector Coordinating Council・米国金融サービスセクター連携協議会） | Cybersecurity Profile[6] | 金融機関が自社システムやサードパーティにおけるサイバーリスクを評価するためのフレームワーク「Cybersecurity Framework」等の既存のガイドラインやツールをベースとして作成されている |
| 6【補足②】 | Carnegie Endowment for International Peace（カーネギー国際平和基金） | Cybersecurity Capacity-building Tool Box for Financial Organizations[7] | 特に中小規模のようなサイバーセキュリティに関する成熟度の低い金融機関が使うことを想定し公表されたチェックリスト |

[3] IT Handbook Information Security: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

[4] IT Handbook Outsourcing Technology Services: https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

[5] Cybersecurity Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm

[6] Cybersecurity Profile: https://fssc.org/Financial-Sector-Cybersecurity-Profile

[7] Cybersecurity Capacity-building Tool Box for Financial Organizations: https://carnegieendowment.org/specialprojects/fincyber/guides

① NIST 「Cybersecurity Framework」

(ア) 目的・経緯

2014 年に施行された「Cybersecurity Enhancement Act[8]」を受けて、NIST により策定されたサイバーリスクに関するフレームワークであり、重要インフラ事業者等が自主的にサイバーリスクを管理するために策定されたガイドラインである。2014 年に第 1 版が発行され、2018 年に利用者のフィードバックやワークショップのコメント等を反映した第 1.1 版が発行されている。

(イ) 概要[9]

NIST の「Cybersecurity Framework」は、フレームワークコア、フレームワークインプリメンテーションティア、フレームワークプロファイルの 3 つの要素から構成されている。フレームワークコアで概要を理解し、フレームワークインプリメンテーションティアで自組織の現状把握を行い、フレームワークプロファイルによって自組織がサイバーセキュリティで目指す目標の状態を定義する。

本フレームワークを利用することで、自組織のフレームワークコアごとの状況（本フレームワークでは「ティア」と表現される）を把握し、あるべき姿に到達するためには何が足りないのかを特定することが可能となる。

（ｉ）フレームワークコア

全ての重要インフラ分野に共通するサイバーセキュリティ対策、期待される成果、適用可能な参考情報をまとめたものである。フレームワークコアは「識別」「防御」「検知」「対応」「復旧」の 5 つの機能で構成されている。

またフレームワークコアの各要素は機能、カテゴリー、サブカテゴリー、参考情報で構成されている。


**図 1 フレームワークコアの構造**

[8] Cybersecurity Enhancement Act: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[9] 情報処理推進機構 セキュリティ関連 NIST 文書「Cybersecurity Framework」より抜粋（https://www.ipa.go.jp/files/000071204.pdf）

（ⅱ）フレームワークインプリメンテーションティア

組織がサイバーリスクをどのように捉えているか、またそのリスクを管理するためにどのようなプロセスが存在しているかを示す。ティアは組織のプラクティスがティア１（部分的である）からティア４（適応している）までのいずれの段階にあるかを示す。

**表 4 フレームワークインプリメンテーションティアの段階**

| 段階 | 概要 |
|---|---|
| ティア１<br>（部分的である） | 組織のサイバーリスクマネジメントプラクティスが定められておらず、リスクは場当たり的に、場合によっては事後に対処される。 |
| ティア２<br>（リスク情報を活用している） | リスクマネジメントプラクティスは経営層によって承認されているが、組織全体にわたるポリシーとして定められていない場合がある。 |
| ティア３<br>（繰り返し適用可能である） | 自組織のリスクマネジメントプラクティスは正式に承認され、ポリシーとして述べられている。組織のサイバーセキュリティプラクティスは、ビジネス・ミッション上の要求事項の変化と、脅威およびテクノロジー状況の変化へのリスクマネジメントプロセスの適用に基づいて、定期的に更新されている。 |
| ティア４<br>（適応している） | 自組織は過去と現在のサイバーセキュリティプラクティスを基に、サイバーセキュリティ対策を調整する。自組織は最新のサイバーセキュリティ技術およびプラクティスを組み入れた継続的な改善のためのプロセスを介して、変化するサイバーセキュリティの技術と実践に進んで順応し、進化・高度化する脅威にタイムリーかつ効果的に対応している。 |

（ⅲ）フレームワークプロファイル

フレームワークプロファイルは、自組織のビジネス上の要求事項、リスク許容度、割当可能なリソースに基づいて調整された機能、カテゴリー、サブカテゴリーをまとめたものである。

プロファイルは、規制上の要求事項と業界のプラクティスを考慮して作成され、リスクマネジメントの優先事項を反映し、組織の目標のみならず、業界の目標を踏まえた、サイバーリスクを低減するためのロードマップの確立を可能にする。

② FFIEC「IT Handbook – Information Security」

(ア) 目的・経緯

「IT Handbook」は、FFIEC によって作成された、検査官が金融機関を検査する観点や基準をまとめた情報システム全般の管理についての文書である。その中において「IT Handbook Information Security」は、金融機関の情報システムに対するセキュリティリスクのレベルを評価するために必要とされる要素を解説することを目的として発行されている。

(イ) 概要

本ガイドラインは金融機関が遵守すべき事項を以下の 4 章に分けて記載している。

（ｉ）情報セキュリティプログラムのガバナンス

経営層に求められる効果的な情報セキュリティのガバナンスについて解説されている。社内における情報セキュリティカルチャーの確立や、情報セキュリティにおける責任の所在の定義等について記載されている。

A) セキュリティカルチャー

金融機関におけるセキュリティカルチャーは、セキュリティの有効性に大きく貢献する。経営層は情報セキュリティを深く理解し、金融機関内に対して適切な情報発信を通じてセキュリティカルチャーの醸成に貢献する。

B) 責任

金融機関における情報セキュリティに関する責任は、経営層により指定された委員会等に帰属する。責任を有する委員会等は、経営層に対し少なくとも年 1 回の情報セキュリティに関する報告を実施する。

C) リソース配分

経営層は、情報セキュリティプログラムの開発、実装、維持のための適切な資金を提供し、責任を有する委員会等によって監視を受ける。また、資金を提供するだけでなく、リスクプロファイルに見合ったスキルを有する人材を配置する。

（ii）情報セキュリティプログラム管理

情報セキュリティプログラムの開発、及び実装方法について解説されている。リスクの特定、リスク特定後の対応や継続的な監視について記載されている。

A) リスクの特定

リスクを特定するためのプロセスの開発、実装について記載されている。金融機関が抱えるリスクと脆弱性を継続的に特定するためのプロセスを文書化する。

B) リスクの評価

金融機関固有のリスクを評価するためのプロセスを構築する。

C) リスクへの対応

金融機関に影響を与える可能性のあるリスクと脆弱性に関する様々な情報を取得し、分析する。分析した結果に基づき適切な計画を策定し、実行する。

D） リスクの監視と報告

日々変化するリスクに対して情報の追跡を行う。併せて、リスクを許容されるレベルで維持するため、金融機関内での経営層に対する適切な報告方法について定めておく。

（ⅲ）セキュリティ運用

セキュリティソフトウェアやデバイス管理、脆弱性の特定等を運用するにあたって対処すべき事項について解説されている。サードパーティとの連携についても説明されており、より詳細な解説は「IT Handbook　Outsourcing Technology Services」を参照するよう記載されている。

A） リスクの識別と評価

経営層はリスクに対する適切な知識を有し、リスクへの対応手順を策定する。そのためには、日ごろから脆弱性やセキュリティインシデントに関する情報を入手し、自組織への影響度を正確に評価する。

B） リスクの監視

経営層は、リスクの監視に使用するツールとその使用条件を確認及び承認する。また、経営層の指示の下、脆弱性、外部攻撃、セキュリティポリシーの遵守状況に関する監視プロセスを確立し、文書化する。

C） インシデントの特定と評価

インシデントが発生した際には、そのインシデントが金融機関にもたらす影響範囲を適切に特定する。特定した影響範囲に応じて、経営層への報告や、場合によっては外部への報告も必要である。

D） インシデント対応

インシデントに適切に対応するために、経営層は事前にプログラムを用意し、従業員に対する適切な教育を実施する。金融機関の中に CSIRT(Computer Security Incident Response Team)を設置することや、サードパーティとの連携による対応も行う。

（ⅳ）情報セキュリティプログラムの有効性検証

情報セキュリティプログラムの有効性の継続的な改善を行うために必要とされる、ペネトレーションテストや、脆弱性診断等を通じ、IT システムの設計の正しさだけでなく、サイバーセキュリティに対する人員が適切に配置されているかを確認する。

③　FFIEC「IT Handbook　－　Outsourcing Technology Services」

(ア) 目的・経緯

「IT Handbook」は、FFIEC によって作成された、検査官が金融機関を検査する観点や基準をまとめた情報システム全般の管理についての文書である。その中において「IT Handbook　Outsourcing Technology Services」は、金融機関におけるアウトソーシングの活用の増加に伴い、法律や、FRB、OCC、FDIC、NCUA（National Credit Union Administration・全米協同組織金融機関監督庁）等の規制・ガイダンスの内容を基に、金融機関がアウトソーシングを実施する際のリスク管理プロセスを確立し、当該プロセスを評価するための手順を示すものである。

(イ) 概要

本ガイドラインは金融機関が遵守すべき事項を「取締役会および経営層における責任」、「リスク管理」の 2 章と、それらに加え補足事項として「付録」が記載されている。

（ｉ）取締役会および経営層における責任

金融機関の取締役会および経営層は、アウトソーシングにおけるリスク管理手法を確立し、アウトソーシング先のサードパーティの規模や関係性によって、適切なリスク管理を実施する。

（ii）リスク管理

経営層はすべてのアウトソーシングにおけるリスクを管理する責任があり、そのためにサードパーティの業務内容を監督するための効果的なリスク管理プロセスを確立する。

A) リスク評価

経営層はアウトソーシングにおけるリスク評価にあたり、リスクベースによる評価基準を文書化する。その上で、文書化された評価基準に基づき、サードパーティを管理する。

B) アウトソーシング先の選定

経営層はアウトソーシングにあたって、自組織のニーズと委託する業務の内容が合致しているかを確認するだけでなく、規制当局によって発行されている規制やガイダンスへの準拠状況を確認する。

C) 契約管理

経営層はサードパーティとの契約にあたり、契約範囲、サービスレベルアグリーメント（以下、SLA）、価格等の情報を確認する。

D) 継続的な監視

経営層はサードパーティとの契約期間中、サードパーティのパフォーマンスや財務状況、自組織のニーズの変化に伴う契約への影響を監視する。

（ⅲ）付録

A) 検査手順

IT システムや IT サービスのアウトソーシングに関連する、リスクマネジメント手法の有効性を確認する。

B) 法律、規制、ガイダンス

アウトソーシングに関連する法律、規制、ガイダンスを一覧形式で記載する。

C) 外国に拠点を置くサードパーティ

外国を拠点とするサードパーティの利用を検討する際には、サードパーティとの契約から発生する可能性のあるリスクと、それらのリスクを管理する際に考慮するべき手順を定める。

D) セキュリティ管理機能のアウトソーシング

セキュリティ管理機能の一部、または全ての機能をアウトソーシングする金融機関が増えてきている実態を踏まえ、セキュリティ管理機能をアウトソーシングする際に意識すべきリスクを提示する。金融機関はここに提示されるリスクを正しく理解したうえで、対応策を検討する。

(ウ) 特徴

本ガイドラインでは、アウトソーシングに伴い発生するリスクの量を考慮する必要があると述べられている。

例えば特定のアウトソーシング先の企業への極度の依存によって、当該アウトソーシング先の企業にインシデントが発生した際に、自組織のリスク量への影響が大きくなることを指摘している。

④ FFIEC「Cybersecurity Assessment Tool」[10]

(ア) 目的・経緯

FFIEC「Cybersecurity Assessment Tool」は、サイバー攻撃の脅威が拡大と高度化の一途を辿っている現状を受け、金融機関が自組織におけるサイバーセキュリティが適切な状態であるかを判断できるように 2015 年 6 月に公表されたものである。

FFIEC「IT Handbook」や、NIST「Cybersecurity Framework」等の内容とも整合している。

(イ) 概要

「Cybersecurity Assessment Tool」は、固有リスクプロファイルの識別とサイバーセキュリティ成熟度の評価の 2 部構成になっており、金融機関の固有リスクと、成熟度を照らし合

[10] FFIEC「Cybersecurity Assessment Tool」に関する詳細は、「『FFIEC Cybersecurity Assessment Tool に関する調査研究』調査報告書（2016 年 3 月 31 日）」を参照。
https://www.fsa.go.jp/common/about/research/20160815-1.html

わせることにより、金融機関のサイバーセキュリティが適切な状態であるかを判断することが可能となる。

（ｉ）固有リスクプロファイルの識別

固有リスクを業務、サービス、商品のカテゴリーに体系化した上で識別する。

固有リスクには、各組織の業種や事業の規模、利用しているテクノロジー等の複雑性やその組織に対する脅威といった要素がある。

（ii）サイバーセキュリティ成熟度の評価

サイバーセキュリティ成熟度の評価では、5 つの領域における金融機関の対応状況を評価する。領域別に評価要素が複数あり、評価要素は更に個別の評価項目により構成されている。各評価項目について金融機関の対応状況を 5 段階の成熟度レベルで評価する。

(ウ) 特徴

「Cybersecurity Assessment Tool」は、全金融機関に対して一律の基準を提示するのではなく、金融機関の固有リスクに応じたサイバーセキュリティへの成熟度を特定し、自組織がサイバーセキュリティリスクに対して適切な状態であるかを判断することが可能である点が特徴として挙げられ、米国金融機関で広く利用されている。

⑤ 【補足①】FSSCC 「Cybersecurity Profile」

(ア) 目的・経緯

FSSCC が提供する、NIST「Cybersecurity Framework」等の既存のガイドラインやツールをベースとした、システムやサードパーティにおけるサイバーリスクを評価するためのフレームワークである。

アセスメントに用いられる質問は、回答者が回答しやすいよう包括的に作成されており、FFIEC「Cybersecurity Assessment Tool」と比較した場合、３割から５割程度の質問に回答することでリスクの評価を行うことが可能となっている。そのため、中小規模の金融機関にも利用しやすいものとなっている。

(イ) 概要

本フレームワークを用いた評価方法は、大きく４つのステップで構成されている。

(i) 質問に回答し、自社の階層（Tier）を特定する

特定される階層は以下のとおりである。

| | |
|---|---|
| Tier1 | 北米、もしくは世界経済の安定性に影響を与える可能性のある組織 |
| Tier2 | 米国の金融サービスセクターに全国的な影響を与える可能性のある組織 |
| Tier3 | 米国の金融サービスセクターに地域的な影響を与える可能性のある組織 |
| Tier4 | 地域的な存在であり、百万人未満の顧客を有する組織 |

階層の特定にあたっての質問事項は以下のとおりである。

・自社が金融システムにおける重要な機関（G-SIB や G-SIFI 等）に指定されているか
・自社を介して行われる取引は、重要な市場(国債、外為等)における取引額の 5%以上を占めているか
・自社が他の業界の企業、金融サービス業界の他の機関に商品やサービスを提供しており、その商品やサービスの提供ができなくなった場合に、決済システムにおける信頼性の損失等を発生させる可能性があるか
・自社は外国の会社に全部、もしくは一部を所有されているか
・自社は 500 万人以上の個人データを保有しているか
・自社は金融機関に対して顧客データを保持するサービスを提供しているか

(ii) 上記(ｉ)で確定した階層ごとの質問に回答し、セルフアセスメントを実施する

評価軸は以下のとおりである。

(ア) ガバナンス

- 戦略とフレームワーク
  取締役会によって確認され承認された、組織のリスク許容度と社会基盤としての重要度に応じたサイバーリスクの管理フレームワークを有しているか
- リスク管理
  組織における優先順位、制約、リスク許容度、前提条件を設定し、オペレーショナルリスクを評価しているか
- ポリシー
  組織のサイバーリスクフレームワークを支えるためのセキュリティポリシーを設立しているか
- 役割と責任
  組織はサイバーセキュリティに関する適切な役割と責任を設定しているか

- 独立したリスク管理機能
  組織は独立したリスク管理機能を設定しているか
- 監査
  組織はサイバーセキュリティに関する適切な監視を行うための独立した監査機能を有しているか
- テクノロジー
  組織は新たな技術の開発、設計、導入、採用にあたりサイバーリスクへの配慮を行っているか

(イ) 識別

- 資産管理
  組織が事業目標を達成するために必要な、データ、人員、システム、設備を、組織のリスク戦略に対する重要度に応じて管理しているか
- リスク評価
  組織は、組織の運営、資産、所属する個人におけるサイバーリスクを理解しているか

(ウ) 防御

- アクセス権限の特定
  物理的、論理的資産及び関連設備へのアクセスは、許可されたユーザー、プロセス、及びデバイスに限定しているか
- 訓練サイバーセキュリティに関する教育が組織の人員に提供され、関連する方針、手順に沿った対応を行うため適切な訓練を行っているか
- データ管理機密性、完全性、可用性を保護するために、組織のリスク戦略に則り、記録したデータを管理しているか
- 維持規定された方針と手順に則り、情報システムを維持しているか
- 保護技術
  セキュリティソリューションはシステムと資産を保護するために管理され、関連する手順、及び契約に準拠しているか

(エ) 検知

- 異常検知
  インシデントをタイムリーに検知し、異常事象の潜在的な影響を特定しているか
- 検知プロセス異常事象をタイムリーかつ適切に検知するために検知プロセスを維持し、テストしているか

(オ) 対応

- 対応計画
  検知されたサイバーセキュリティインシデントへのタイムリーな対応を行うため、手順を整備し、維持しているか

- コミュニケーション
  必要に応じて、当局含む、外部及び内部の関係者と調整を行っているか
- 緩和
  インシデントの拡大を防止しているか
- 改善現在及び過去の検知、対応から得られる教訓を取り入れ、組織的な対応を改善しているか

(カ) 復旧

- 復旧計画サイバーセキュリティインシデントの影響を受けたシステム、または資産の復旧を確実に実行するために、復旧手順を整備し、維持しているか
- 改善学んだ教訓を今後の対応に反映することで復旧手順を改善しているか
- コミュニケーション
  復旧対応では、インターネットサービスプロバイダ、攻撃を受けたシステムの所有者、CSIRT やベンダー等の社内外の関係者と調整を行っているか

(キ) サプライチェーン

- 内部連携
  組織は、組織内部の連携によるリスクを管理しているか
- 外部連携
  組織は、組織外部との連携によるリスクを管理しているか
- レジリエンス
  組織は、サイバー攻撃を受けた際にも業務を継続できるか
- 事業環境
  組織の使命、目的、利害関係者が理解され優先順位がつけられていることにより、サイバーセキュリティの役割や責任を決定することができているか

(iii) 上記( ⅱ )で実施したセルフアセスメントを基に、不足している点やギャップを特定する

(iv) 上記（ iii ）で特定した不足している点やギャップを埋めるための計画を立て実行する

(ウ) 特徴

「Cybersecurity Profile」は、( ⅰ )で示した通り、自組織の規模・業態に応じた評価観点で成熟度を評価する仕組みとなっている。

⑥ 【補足②】Carnegie Endowment for International Peace
「Cybersecurity Capacity-building Tool Box for Financial Organizations」

(ア) 目的・経緯

金融機関のサイバーレジリエンスを強化するために、Carnegie Endowment for International Peace が、国際通貨基金や SWIFT、スポンサーである FS-ISAC[11]、

[11] 『7. 共助・演習の取組みの調査 (1)共助に向けた取組み』を参照

Standard Chartered、Cyber Readiness Institute の協力を受け、作成したチェックリストである。特に中小規模の金融機関や、サイバーセキュリティに関する成熟度の低い組織が使うことを想定し公表されている。

(イ) 概要

金融機関のサイバーセキュリティに関して、取締役会（Board）、最高経営責任者（CEO）および最高情報セキュリティ責任者（CISO）の階層別のチェックリストを提示している。

(i) 取締役会向けサイバーセキュリティリーダーシップ

A) 監視

取締役会は、サイバーリスクを管理するための最終的な説明責任を負うことから、以下の対応が求められている

- 一人の執行役員（corporate officer）に役職を割り当て、サイバーレジリエンスに関連する機能と、各機能の実装状況を報告する責任を負う
- 組織におけるリスク許容度を定義し、企業戦略とリスクアペタイトのバランスを確保する
- サイバーレジリエンスに関する計画、実装、テスト、継続的な改善を監督し、CISO もしくは他の責任ある役員から定期的に報告を受ける

B) 最新情報の入手

取締役会が効果的にサイバーリスクの監視を行うために、サイバーリスクへの知識と、最新情報の取得に努める

- 取締役会の全員が、サイバーセキュリティに関する適切かつ最新のスキルと知識を有する
- サイバーリスクを定量化し、その評価を実施することを、取締役会の常設の議題として取り扱う

C) セキュリティに関するトーンの設定

取締役会は、組織のコアバリュー、リスクカルチャー、サイバーレジリエンスに関する期待値を設定し、組織内に提示する

- 組織のサイバーレジリエンスを確保するうえで、全ての従業員が、自身の職務がサイバーセキュリティに及ぼす影響を適切に認識する文化を醸成する
- 全ての従業員が誠実に行動し、コンプライアンス違反があった場合には組織内外に対して迅速に報告することが期待されることを明示する

（ii）CEO 向けサイバーセキュリティリーダーシップ

A) ガバナンス

CEO は取締役会とともにセキュリティリスクを理解し、組織のサイバーセキュリティにおける活動と要員に対する最終的な説明責任を負う

- CISO 職を設ける
- CISO や技術担当者と協力し、国内外の金融業界のガイドラインを使用することで、組織のサイバーリスクに合わせたサイバーセキュリティ戦略とフレームワークを確立し、維持する
- 組織のサイバーセキュリティの実装および管理する担当者の役割と責任を明示する

B) リスク評価とリスクマネジメント

強固なサイバーセキュリティを構築するためには、リスクベースアプローチによる継続的なサイバーリスクの分析が求められる

- CISO や技術担当者と協力し、リスク評価を実施するための計画を立案する
- サイバーセキュリティの状況を監視し、改善が必要とされる場合の措置について検討を行う

C) 組織カルチャー

組織内における継続的なサイバーセキュリティ対応を実現するために、CEO は以下の対応を行う

- サイバーリスクの管理に責任を持つ担当者と定期的にコミュニケーションをとる
- 全ての新規従業員を対象としたサイバーセキュリティに関する研修を実施し、全ての従業員が最新のサイバーセキュリティポリシーを遵守することに同意したことを証明する署名を収集する
- 一年ごとに組織内のサイバーセキュリティポリシーの見直しを実施する
- サイバーインシデント等に関する情報の、組織内の自主的な共有を奨励する

（ⅲ）CISO 向けガイドライン

（ⅲ-a）自組織の保護

A) マルウェアによる被害の防止

- ファイアウォールをアクティブにし、ネットワークとインターネットの間に DMZ(DeMilitarized Zone)を作成し、特定の IP アドレスまたはサービスをブラックリストに登録するのではなく、ホワイトリストによりアクセス制御することが推奨される
- 全てのコンピュータに対してウイルス対策およびスパイウェア対策を実施する
- 新たなプログラムのインストールを、管理者権限を持つ従業員のみに制限する
- ペネトレーションテストサービスを利用した、資産とシステムのセキュリティ評価の実施を検討する

B) 従業員の訓練

- 新規従業員及び、業務に従事中の従業員全員に対して、定期的、少なくとも年一回のサイバーセキュリティトレーニングを実施する
- 訓練用のアカウントからフィッシングメールの送信を行う等、従業員の意識を定期的にテストする

C) データの保護

- 重要なデータを定期的にバックアップし、復元できるかどうかのテストを実施する。必要に応じてクラウド環境へのバックアップを検討する
- 全てのコンピュータと重要なネットワークデバイスが無停電装置に接続されていることを確認する

（iii-b）顧客保護

A) アカウントの管理

- 顧客がサービスにログインするために使用するユーザーID とパスワードは他のサービスと同じものを使わないようアドバイスする
- ユーザーID とパスワードだけではなく、多要素認証を活用し顧客を認証する

B) 顧客データの保護

- 金融機関がサービスを提供するために収集する必要がある顧客データを特定し、それを超える顧客データの収集は行わない
- 不要になった顧客データは破棄する
- 保存する顧客データは暗号化する

C) WEB アプリケーションの保護

- 金融機関の公開する WEB アプリケーションに HTTPS を実装する
- ペネトレーションテストサービスを利用し、少なくとも年 1 度は WEB アプリケーションに関するセキュリティ評価を実施する

D) 顧客への通知

- 金融機関が、顧客データへの不正アクセス等のインシデントを検知した場合、該当する顧客に可能な限り早く通知する

（iii-c）サードパーティの対応

A) サードパーティを利用することによるリスクの特定

- 全てのサードパーティとの関係と、それぞれに提供しているデータのリストを、常に最新化し保持する
- サードパーティにおけるセキュリティインシデントが金融機関に与える影響度に基づき、サードパーティのランク付けを実施する

- 高ランクに位置付けられたサードパーティから順に、サイバーセキュリティレベルの評価を行う

B) サードパーティのセキュリティ管理

- サードパーティとの契約において、ビジネスの継続性、インシデント対応、SLA について明記し、サイバーインシデント発生時の責任について定義する
- サードパーティのサイバーセキュリティ基準への対応状況について監視する
- サードパーティとの契約を毎年評価し、データセキュリティに関する規制要件への準拠を確認する

C) 情報の共有

- 金融機関とサードパーティにおいて、セキュリティの問題について連絡を取るためのコミュニケーションチャネルを確立する
- サイバーセキュリティに関する情報を、社内及び社外の利害関係者と随時共有する
- 脆弱性や他組織におけるインシデント等の最新情報を取得する

（vi）金融機関におけるインシデント対応

A) 準備

- 金融機関は、サイバーリスク評価で特定された最も差し迫ったリスクについて、インシデント対応及び、業務継続計画を策定する

B) 演習の実施

- 金融機関の幹部、広報、法務等のコンプライアンスチームを含む全てのレベルの従業員の代表者による机上演習を実施する
- 演習から得られた教訓が、金融機関のサイバーセキュリティ戦略に組み込まれるためのプロセスを確立する

C) 対応

- 影響を受ける、もしくは不正アクセスを受けたシステムを特定し、損害を評価する
- 影響を受ける資産を特定、分離し、インシデントに関連する証拠となるログ等の保持に努める
- 内部関係者、及び当局に通知し、必要に応じて支援を要請する
- 法律、規制、ガイダンスに沿った顧客への通知を行う
- FS-ISAC 等の情報共有プラットフォームを通じて、インシデントについて業界内に周知する
- インシデント対応中に行われた手順を文書化し、後日、対応手順について確認する

D) インシデント発生後の対応

・ インシデント発生後、インシデントの原因となった脆弱性を特定し、低減するための計画を作成する
・ 同様の、または類似のインシデントを検出するための行動計画を策定する

(ウ) 特徴

本資料では、意思決定の役割を担う、取締役会および CEO が担うべき、サイバーセキュリティにおける役割が、チェック項目として提示されている。

（i）取締役会が担うべきサイバーセキュリティリーダーシップ

・ 取締役会はサイバーリスクを管理するための最終的な説明責任を要する
・ 取締役会に参加するすべての個人が、サイバーリスクに関する適切かつ最新のスキルと知識を有する
・ 取締役会は組織に存在するリスクと、そのリスクが及ぼす影響範囲を提示する

（ii）CEO が担うべきサイバーセキュリティリーダーシップ

・ 組織の中におけるサイバーセキュリティに関する担当者と役割・責任を明確化する
・ 監督を行う取締役会のために、CEO はリスク評価の分析結果の説明責任を負う
・ すべての従業員に対して、サイバーセキュリティに関するトレーニングを実施する

(3) インタビュー結果

米国の中小金融機関 3 社に、金融機関におけるサイバーセキュリティの取組み状況を把握する目的から、以下の項目をヒアリングした。

✓ サイバーセキュリティにおけるガバナンスの構築に関する取組み
✓ サイバーリスク管理に関する取組み

① サイバーセキュリティにおけるガバナンスの構築に関する取組み

ヒアリングを行った 3 社の中小金融機関でも、「第一線：業務執行部門」、「第二線：サイバーリスク管理部門」、「第三線：内部監査部門」の三つの防衛線を意識したサイバーセキュリティ体制を構築し、牽制機能を確保していた。また、サイバーセキュリティに関する最終意思決定は、経営層が関与することが可能なよう、理事会または取締役会にて承認する仕組みが構築されていた。

一方で、第二、第三線の人材の不足等の、体制を構築するうえでの以下の悩みが挙げられた。

・ 第二線の機能を「第一線：業務執行部門」の CIO が自ら実施しており、職務分掌ができていない
・ 第三線における内部監査を担う人材が不足していることから、外部のコンサルタントや IT ベンダーの有識者に委託しており、社内への知識移転が必要

② サイバーリスク管理に関する取組み

サイバーリスク管理に関する取組みについては、リスクの特定、リスクの評価、リスクの低減、リスクの見直しの 3 つの観点でヒアリングを実施した。

(ア) リスクの特定

基本的に、ガイドラインとして紹介した FFIEC「Cybersecurity Assessment Tool」におけるサイバーセキュリティ成熟度評価の「サイバーリスクの管理と監督」領域の設問を利用している。

(イ) リスクの評価

「Cybersecurity Assessment Tool」を利用して自社の固有リスクを識別している。

(ウ) リスクの低減

サイバーセキュリティリスク低減のための予算獲得は困難であるという実態があるものの、「セキュリティインシデントによる損失を防止する」という観点で経営層への説明を行うことで、予算の獲得を行っていた。

リスク低減への対策について、技術的対策、非技術的対策の 2 つの観点で整理すると、技術的対策（ツール）を導入または実装する際には、限りある予算を有効活用するため、RFP 等の要件の詳細化を行い、複数の IT ベンダーから提案を受けることで、最小限の予算で対応していた。

非技術的対策としては、IT ベンダーへ依存せざるを得ない状況から、委託前における IT ベンダーのセキュリティ状況のチェック（セキュリティに関するドキュメント確認、開発現場の確認等）を重点的に実施していた。

具体的な対策としては、脆弱性診断及びペネトレーションテストの定期的な実施によるシステムの脆弱性のチェックに加え、経営層を含む机上演習、IT ベンダーを含めたインシデント対応演習等によるインシデント対応手順の見直しを実施していた。

また、FS-ISAC に加え、情報共有のための任意団体の活用等を通じて情報収集を行っており、他の金融機関のセキュリティポリシーの内容、ペネトレーションテストの実施方法、利用するセキュリティソフトウェア等の、多岐に渡るサイバーセキュリティに関する情報交換が行われていた。

## 3. EU におけるサイバーセキュリティ

### (1) EU のサイバーセキュリティ関係当局

まず、EU の政策決定機関として、金融業態に限らず、EU 全体のサイバーセキュリティに関する政策を決定する European Commission（欧州議会）（以下、EC）が存在する。また、本報告書は、EU 金融機関の監督当局である European Central Bank（欧州中央銀行）（以下、ECB）と European Banking Authority（欧州銀行監督局）（以下、EBA）を調査対象とした。EBA は EU の機関の 1 つであり、欧州の銀行部門全体の監督に責任を有している。なお、この 2 つ以外にも、保険会社や証券会社の監督当局として、それぞれ、European Insurance and Occupational Pensions Authority（欧州保険・年金監督局）（以下、EIOPA）、European Securities and Markets Authority（欧州証券市場監督局）（以下、ESMA）が存在している。

### (2) EU の調査対象概要

EU における、サイバーセキュリティ対策についての基本的な規制として、EC が発行した「NIS Directive（The Directive on security of network and information systems）」がある。また、EU 加盟国のネットワークセキュリティや情報セキュリティの向上のために、各加盟国に対してアドバイスや提言を行う European Network and Information Security Agency（欧州ネットワーク情報セキュリティ機関）（以下、ENISA）の権限や役割を定めた、「The EU Cybersecurity ACT」がある。上記に加え、ECB が公表した Threat-Led Penetration Test（脅威ベースのペネトレーションテスト）（以下、TLPT）のフレームワークである「TIBER-EU」、EBA の金融機関に対するガイドラインである「Guidelines on ICT and security risk management」と「Guidelines on outsourcing arrangements」を本報告書で調査対象とした。EBA のガイドラインのうち前者は、金融機関の Information and Communication Technology（情報通信技術）（以下、ICT）とセキュリティにおけるリスク管理に関するガイドラインであり、後者は、金融機関の業務のアウトソーシングに関するガイドラインである。EU における調査対象の法規制・ガイドラインの一覧を以下に記載する。

**表 5 EU の調査対象一覧**

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 1 | European Commission | NIS Directive[12]（The Directive on security of network and information systems） | 金融機関を含む重要サービスの運営者に対するセキュリティ義務を定めている。 |
| 2 | | The EU Cybersecurity Act[13] | EU のサイバーセキュリティ機関である ENISA（European Network and Information Security Agency・欧州ネットワーク情報セキュリティ機関）の権限や役割を定めている。<br>ENISA には、NIS Directive によって設立された加盟国の CSIRT を支援する義務がある[14]。 |
| 3 | European Central Bank | TIBER-EU[15]（The Framework for Threat Intelligence-based Ethical Red Teaming） | EU 加盟国の監督当局が、金融機関が脅威ベースのペネトレーションテストを行うために定めた、EU 共通的なフレームワークである。 |
| 4 | European Banking Authority | Guidelines on ICT and security risk management[16] | 金融機関に対して、ガバナンス・戦略、ICT とセキュリティ管理フレームワーク、情報セキュリティ、ICT の運用管理等の要件を定めている。 |

[12] NIS Directive : https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[13] Cybersecurity Act : https://eur-lex.europa.eu/eli/reg/2019/881/oj

[14] Cybersecurity Act : https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

[15] TIBER-EU : https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

[16] Guidelines on ICT and security risk management : https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 5 | | Guidelines on outsourcing arrangements[17] | 金融機関や決済機関及び電子マネー事業者が、特に重要な業務をアウトソーシングする際に、実施すべき健全なリスクマネジメントを含めた、内部ガバナンス体制を定めている。 |

① EC「NIS Directive」

(ア) 目的・経緯

「NIS Directive」（以下、本指令）は、2016 年 7 月に成立し、同年 8 月に施行された。EC は、サイバーセキュリティに関するインシデントやリスクへの対応能力が低い加盟国の存在のために、EU 全体のネットワークと情報システムが脆弱化していることを問題として指摘していた[18]。そこで、EU のネットワークと情報システムの全体的な安全性を向上させることを目指し、本指令が制定された。

本指令の目的は、「域内市場の機能を向上させるために、EU 域内におけるネットワークと情報システムの安全性に関する高度で共通的なレベルを達成するための措置を定めること」[19]とされている。

(イ) 概要

本指令では、EU 加盟国に対して、EU 域内のネットワーク・情報システムの安全性向上を目的として、主に以下の規定が定められている。このうち、特に（ⅳ）は、金融機関を含む重要サービス運営者に関係する規定である。

（ⅰ）ネットワークと情報システムの安全に関する国家戦略の策定

（ⅱ）国内のネットワーク・情報システムを管轄する官庁と CSIRT の創設

（ⅲ）EU 加盟国間の協力および情報共有

（ⅳ）重要サービス運営者およびデジタルサードパーティへのセキュリティ要件およびインシデントの通知義務

---

[17] Guidelines on outsourcing arrangements : https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.pdf/38c80601-f5d7-4855-8ba3-702423665479

[18] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013.2.7 P3 : http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_directive_en.pdf

[19] NIS Directive 第 1 条第 1 項 : https://eur-lex.europa.eu/eli/dir/2016/1148/oj

本指令では、金融機関（銀行、金融市場インフラ（証券取引所等））は、重要サービス運営者と定義されており、以下の義務が定められている[20]。

（ｉ）防護措置義務

重要サービス運営者は、自らの業務遂行のために必要なネットワーク・情報システムの安全性に対するリスクに対処するため、適切な技術的及び組織上の措置を講じなければならない。当該措置は、最新技術を考慮して、リスクに適切に対応し、ネットワーク・情報システムの安全水準を確保するものでなければならない。

また、重要サービス運営者は、自らの業務継続のために必要なネットワーク・情報システムへ影響するインシデントの発生を防ぐとともに、その影響を最小化するための措置を講じなければならない。

（ii）通知義務

重要サービス運営者は、提供する業務の継続性に重大な影響を及ぼすインシデントが発生した場合、不当に遅滞することなく、所属する国の監督官庁又は CSIRT に通知しなければならない。当該通知の内容には、監督官庁又は CSIRT が、当該インシデントが及ぼす国境を越える影響を判断するための情報を含めなければならない。

また、インシデントの影響の重大性を判断するために、特に以下の情報を含めなければならない。

A) 重要サービスの中断により影響を受ける利用者の数
B) インシデントの継続時間
C) インシデントにより影響を受ける地域の地理的範囲

② EC「The EU Cybersecurity Act」

(ア) 目的・経緯

「The EU Cybersecurity Act」（以下、本規則）は、2019 年 3 月に成立し、同年 6 月に施行された。罰則は、2021 年 6 月 28 日より適用される。EU 域内におけるネットワークおよび情報システムの普及に伴い、Internet of Things（以下、IoT）等のネットワークに接続するデジタル機器の増加が予測されている中で、デジタル機器の安全性やレジリエンスが不十分なことにより、サイバーセキュリティが侵害されていることが指摘されている[21]。そこで、EU 域内の高水準なサイバーセキュリティ、サイバーレジリエンス、信頼の達成を目指し、本規則が制定された。

本規則の目的は、「European Network and Information Security Agency（欧州ネットワーク情報セキュリティ機関）（以下、ENISA）の権限の強化」と「EU 域内

[20] NIS Directive 第 14 条：https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[21] Cybersecurity Act 前文(4)：https://eur-lex.europa.eu/eli/dir/2016/1148/oj

における ICT 製品、ICT サービス及び ICT プロセスの十分なレベルのサイバーセキュリティを確保するための、欧州サイバーセキュリティ認証制度の枠組みの整備」とされている[22]。

(イ) 概要

本規則は、ENISA の組織としての任務や目的、業務内容、予算等や、サイバーセキュリティ認証制度[23]の枠組みを定めている。

ENISA の主な業務内容[24]について以下に記載する。金融機関には、(ⅲ)-D)「技術分野におけるセキュリティ要件について、助言やガイドラインの提供」や(ⅳ)-C)「ネットワークおよび情報システムのセキュリティに関する、助言やガイドライン、ベストプラクティスの提供」が関係する。

（ⅰ）EU の政策、法律の策定及び実装の補助・支援

A) サイバーセキュリティの分野における EU の政策及び法律の策定及び見直し、ENISA の独立的な意見や分析の提供

B) NIS Directive と一貫性を持った、リスク管理やインシデント通知等に関する助言及びベストプラクティスの提供

（ⅱ）EU 加盟国の能力開発支援

A) サイバーセキュリティの向上やインシデントの防止・検知能力の向上のための、情報や専門知識の加盟国への提供

B) 加盟国の国内 CSIRT の構築の補助

C) 加盟国のネットワーク・情報システムの安全性に関する国内戦略の策定の補助

D) 加盟国 CSIRT との最新技術に関する対話や情報交換

E) 少なくとも 2 年に 1 度の EU レベルのサイバーセキュリティ演習の立案・実施

（ⅲ）サイバーセキュリティ認証の標準化

A) ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ認証に関する EU の政策の策定及び実装の支援・促進

B) サイバーセキュリティ認証機関及び産業界と協力し、ICT 製品、ICT サービス及び ICT プロセスのサイバーセキュリティ上の要求事項に関する、ガイドラインの取りまとめ及び公表

C) 加盟国の要請に応じて支援を提供することによって、認証プロセスに関連する加盟国の能力開発への貢献

---

[22] Cybersecurity Act 第 1 条：https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[23] サイバーセキュリティ認証制度：個々の ICT 製品、ICT サービスまたは ICT プロセスに対して、定められたセキュリティ上の要求事項を遵守した場合に、認証を与える制度

[24] Cybersecurity Act 第Ⅱ章：https://eur-lex.europa.eu/eli/dir/2016/1148/oj

D) 加盟国および産業界と共働して、重要サービス運営者及びデジタルサービス運営者の技術分野におけるセキュリティ要件に対する、助言やガイドラインの作成

E) EU 内のサイバーセキュリティ市場を育成する観点から、サイバーセキュリティ市場の主要動向の継続的な分析

（ⅳ）知識と情報収集

A) 先端技術の分析を実施するとともに、サイバーセキュリティの技術革新による社会的・法的・経済的影響の評価

B) 先端技術やサイバーセキュリティの最新の傾向を把握し、インシデントを防ぐための、戦略的な分析

C) 重要サービス運営者及びデジタルサービス運営者が使用する、ネットワークおよび情報システムのセキュリティに関する、助言やガイドライン、ベストプラクティスの提供

D) 重大なインシデントに関する情報を収集及び分析し、EU 全域の市民や組織、企業に対してガイドラインを提供するための報告書のとりまとめ

③ ECB「TIBER-EU」

(ア) 目的・経緯

「TIBER-EU（The Framework for Threat Intelligence-based Ethical Red Teaming）」は、英国の CBEST[25]やオランダの TIBER-NL 等の取組みから得られた知見を基に、ECB と加盟国の中央銀行と共同で開発され、2018 年に公表された[26]。TIBER-EU 制定の背景として、まず、ECB 理事会が 2016 年に公表した「Guidance on cyber resilience for FMIs（金融市場インフラのためのサイバーレジリエンスに関するガイダンス）」を踏まえ、2017 年 3 月に EU の金融システムのサイバーレジリエンスの強化を目的とした「Eurosystem's cyber resilience strategy（ユーロシステムにおけるサイバーレジリエンス戦略）」（以下、同戦略）が公表されたことが挙げられる[27]。同戦略は、「金融市場インフラのサイバーレジリエンス能力の向上」を目標として掲げており、これを実現するためのツールとして、TIBER-EU が策定された。

TIBER-EU を、EU 各国が国内の基準等に基づいて独自にカスタマイズしたものが、TIBER-XX（XX には、各国の国名の略称二文字が入る）である。本報告書作成時点で、9 か国（オランダ、ベルギー、デンマーク、ルーマニア、ドイツ、アイルランド、スウェーデン、フ

25 諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書：https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf

26 TIBER-EU：https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

27 What is the Eurosystem's cyber resilience strategy?：https://www.ecb.europa.eu/paym/intro/events/shared/pdf/fs07/ecb_focus_session_20180917_cyber.pdf

ィンランド）が TIBER-XX を策定していることが確認できた。また、現在ノルウェーでも策定が検討されている。

**表 6 TIBER-EU に関する各国の対応状況[28]**

| 国名 | 状況 | TIBER-XX | 策定時期 |
|---|---|---|---|
| オランダ[29] | TIBER 策定済み。策定した TIBER に基づいてテスト実施。 | TIBER-NL | 2017 年 11 月 |
| ベルギー[30] | TIBER 策定済み。 | TIBER-BE | 2018 年 11 月 |
| デンマーク[31] | TIBER 策定済み。策定した TIBER に基づいてテスト実施。 | TIBER-DK | 2018 年 12 月 |
| ルーマニア[32] | TIBER 策定済み。 | —（確認できず） | 2018 年 6 月～2019 年 3 月（詳細確認できず） |
| ドイツ[33] | TIBER 策定済み。 | TIBER-DE | 2019 年 9 月 |
| アイルランド[34] | TIBER 策定済み。 | TIBER-IE | 2019 年 12 月 |
| スウェーデン[35] | TIBER 策定済み。テストは、2020 年～2022 年に実施予定。 | TIBER-SE | 2019 年 12 月 |

[28] ECB のプレスリリース（https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html）および、各国中央銀行の HP を基に、NTT データ経営研究所にて作成

[29] TIBER-NL：https://www.dnb.nl/en/news/nieuwsbrief-betalingsverkeer/Juni2018/index.jsp

[30] TIBER-BE：https://www.nbb.be/en/payments-and-securities/tiber-be-framework

[31] TIBER-DK： http://www.nationalbanken.dk/en/financialstability/Operational/Pages/TIBER-DK-and-implementation-guide.aspx

[32] National Bank of Romania：https://www.bnr.ro/DocumentInformation.aspx?idDocument=32161&directLink=1

[33] TIBER-DE：https://www.bundesbank.de/en/tasks/payment-systems/services/tiber-de/tiber-de-817014

[34] TIBER-IE：https://centralbank.ie/financial-system/tiber-ie

[35] TIBER-SE：https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2019/the-riksbank-coordinates-cybersecurity-tests/

| 国名 | 状況 | TIBER-XX | 策定時期 |
|---|---|---|---|
| イタリア[36] | TIBER 策定済み。 | TIBER-IT | 2020 年 1 月 |
| フィンランド[37] | TIBER 策定済み。 | TIBER-FI | 2020 年 4 月 |
| ノルウェー[38] | TIBER を策定する方針を 2020 年 4 月に公表。 | TIBER-NO | 未策定 |

(イ) 概要

TIBER-EU は、金融機関の重要な情報システムに対してレッドチームテストを行うための、EU 共通的なフレームワークである。レッドチームテストとは、現実のサイバー攻撃者の戦術や技術、手順を模倣し、組織のサイバーレジリエンスをテストするものである。TIBER-EU を参照すべき主体は以下のとおり[39]。

（ｉ）国家および EU レベルで TIBER-EU の採用や実施の権限を有する当局
（ii）金融機関の監督機関
（iii）TIBER-EU に基づく、サイバー脅威インテリジェンスサービス提供事業者
（iv）TIBER-EU に基づく、レッドチームテストサービス提供事業者
（v）金融セクター

TIBER-EU で定められている、金融機関によるテストの実施のためのプロセスを以下に記載する[40]。なお、プロセスは、(ｉ) 一般的な脅威把握のフェーズ、(ii)準備フェーズ、(iii)テストフェーズ、(iv)クロージングフェーズの 4 段階に分けられている。

（ｉ）監督当局による一般的な脅威把握のフェーズ

各国の監督当局は、一般的な金融セクターの脅威の状況の評価を行い、金融機関（銀行や取引所等）の具体的な役割を確認し、サイバー攻撃者や金融機関を対象とした、サイバー攻撃の戦術や技術、手順を特定する。なお、このフェーズは任意のフェーズである。

---

36 TIBER-IT：https://www.bancaditalia.it/media/comunicati/documenti/2020-01/cS_BIConsob_20200116_ENG.pdf?language_id=1
37 TIBER-FI：https://www.suomenpankki.fi/en/money-and-payments/tiber-fi-implementation-guideline/
38 TIBER-NO：https://www.norges-bank.no/en/news-events/news-publications/Press-releases/2020/2020-05-14-tiber/
39 TIBER-EU FRAMEWORK P7：
https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
40 TIBER-EU FRAMEWORK P20-21：
https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

（ⅱ）準備フェーズ

本フェーズで実施される主な取組みは、体制確立とテスト範囲の決定、プロバイダの調達の2点である。以下に、本フェーズで実施される取組みを記載する。なお、本フェーズは、TIBER-EU のフレームワーク上では必須のフェーズである。

A) テストの実施・管理に責任を有するチームの設立
B) テスト範囲の決定
C) 取締役会によるテスト実施の承認
D) 当局による検証
E) テスト実施のための Threat Intelligence（脅威インテリジェンス）（以下、TI）および Red Team（レッドチーム）（以下、RT）プロバイダの調達

（ⅲ）テストフェーズ

本フェーズでは、調達した TI プロバイダが、テストのための脅威シナリオと金融機関に対する有益な情報を記述した、Targeted Threat Intelligence レポート（金融機関等の当該組織に焦点を絞った脅威情報レポート）（以下、TTI レポート）を用意する。

TI プロバイダは RT プロバイダと密接に連携し、TTI レポートは、RT プロバイダが金融機関の重要な機能を支える本番システムや、従業員、業務に対する、レッドチームテストの攻撃シナリオを開発し実行するために活用される。なお、本フェーズは、TIBER-EU のフレームワーク上では必須のフェーズである。

（ⅳ）クロージングフェーズ

本フェーズでは、RT プロバイダがレッドチーム報告書を作成する。報告書には、テスト実施時のアプローチ（方針や手順）や、得られた知見、技術・方針・教育等の観点から改善すべき点についての助言が記載される。本報告書を基に、関係者は、実施されたシナリオを振り返りながら、テスト中に発見された問題点について議論を行う。

また、金融機関は、テストの結果を踏まえ、監督機関と緊密な協議・承認のもと、改善計画を構築する。改善計画の構築後は、テスト終了の承認を関連当局から取得しなければならない。なお、本フェーズは、TIBER-EU のフレームワーク上では必須のフェーズである。

④ EBA「Guidelines on ICT and security risk management」

(ア) 目的・経緯

「Guidelines on ICT and security risk management」（以下、本ガイドライン）は、2017 年 5 月に策定され、2019 年 11 月に内容が改定された。改定されたガイドラインは、2020 年 6 月 30 日から運用される予定である。

本ガイドライン策定の背景として、ICT リスクが金融機関の健全性に重大な影響をもたらし、存続を脅かす可能性があることが挙げられている。各金融機関が戦略的・組織的な目

標を達成するためには、ICT とセキュリティのリスク管理が重要であることを踏まえ、本ガイドラインが策定された[41]。

本ガイドラインの目的は、決済サービス提供事業者、信用機関、投資会社（以下、金融機関）の ICT リスクの低減・管理に関する要件を定め、単一市場全体で一貫性のある強固なアプローチを確保することである[42]。

(イ) 概要

本ガイドラインでは、金融機関に対して、ガバナンス・戦略、ICT とセキュリティ管理フレームワーク、情報セキュリティ、ICT の運用管理等の要件を定めている。具体的な内容を以下に記す。

（ｉ）ガバナンス・戦略

本章は、ICT とセキュリティリスクの管理・低減を目的に、金融機関に対して、健全な内部ガバナンスの確立と、経営層を含めたすべての従業員に対する明確な責任を定めた内部統制の枠組みの構築を求めている。

また、金融機関がアウトソーシングやサードパーティを利用する際は、金融機関自身のリスク管理フレームワークで定義されたリスク低減策の有効性を確認することも求めている。

（ii）ICT およびセキュリティリスク管理フレームワーク

本章は、金融機関に対して、自身の業務機能、情報資産等の台帳を常に最新化するとともに、データの機密性等の観点で、その台帳を分類することを求めている。この取組みに基づいて、金融機関は、ICT とセキュリティリスクに関連するオペレーショナルリスクを評価するとともに、そのリスクを低減するために必要な対策を判断する。

（iii）情報セキュリティ

本章は、効果的な情報セキュリティ対策を実施するための要件を定義している。具体的には、情報セキュリティポリシーの策定、情報セキュリティ対策の確立・実施・テスト及び全従業員や委託先等のためのトレーニングプログラムの確立を金融機関に求めている。

（iv）ICT の運用管理

本章は、金融機関の ICT 運用・管理における原則を規定している。具体的には、ICT 業務の効率化や、重要な ICT 業務のログの取得（記録）及びモニタリングの実施、

---

41 Guidelines on ICT and security risk management P6：https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

42 Guidelines on ICT and security risk management：https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

ICT 資産台帳の最新状態の維持、ICT 資産のライフサイクルのモニタリング及び管理、バックアップ計画とリカバリ手続きの整備が求められている。

（ｖ）ICT プロジェクト管理と変更管理

本章は、ICT システムやサービスの取得・開発・保守に関する、ICT プロジェクト管理および変更管理に関する要件を定めている。金融機関は、実運用システムへの変更が評価・テストされ、変更の実施が承認された後に、管理された方法で変更されることを保証する。ICT プロジェクトを適切なガバナンスと監督下においた上で、アプリケーションの開発についてテスト段階から実運用の段階まで慎重に監視しなければならない。

（vi）業務継続管理

金融機関は、事業を継続する能力を最大化し、業務中断中の深刻な損失を抑制するために、健全な業務継続管理プロセスを確立する。そのために、事業インパクト分析や、業務継続計画の策定、対応・復旧計画の策定、業務継続計画の検証、危機対応への備えを実施する。

（vii）決済サービス利用者リレーションシップ管理

決済サービス提供事業者に対して、決済サービス利用者による特定の決済機能の無効化の許可や、決済取引の開始または失敗に関するアラートの受信、決済サービス利用者へのサポート（問い合わせ対応）を含めた、顧客との関係構築が求められている。EBA は、決済サービス提供事業者が決済サービス利用者に対して透明性を確保することの重要性を強調している。

(ウ) 特徴

本ガイドラインでは、金融機関のリスクアペタイト[43]に応じて、ICT およびセキュリティに対するリスクアペタイトを決定することが必要と記載されている。

⑤ EBA「Guidelines on outsourcing arrangements」

(ア) 目的・経緯

「Guidelines on outsourcing arrangements」（以下、本ガイドライン）は、2006 年に CEBS（Committee of European Banking Supervisors・欧州銀行監督委員会）が発行した、アウトソーシングに関するガイドラインを更新する形で、2019 年 2 月に EBA によって策定され、2019 年 9 月 30 日から適用された。本ガイドライン策定の背景として、近年、金融機関は、コスト削減や効率化の観点から、業務のアウトソーシングや、IT と FinTech 等の最新技術の導入を進めている一方、金融機関におけるガバナンスフレームワー

43 リスクアペタイト：組織の目的や事業計画を達成するために、組織として受け入れることができるリスクの種類や量を明示したもの

クにセキュリティの問題が発生していることが挙げられている。また、クラウドサービス提供事業者へのアウトソーシングの重要性が高まってきており、その特殊性に対応することも目的としている[44]。

(イ) 概要

本ガイドラインは、金融機関、決済機関及び電子マネー事業者（以下、金融機関）が、特に重要な業務をアウトソーシングする際に、実施すべき健全なリスクマネジメントを含めた、内部ガバナンス体制を規定している。具体的な内容を以下に抜粋する。

（本ガイドラインの対象となるアウトソーシング契約の評価）

A) アウトソーシング

金融機関は、サードパーティとの協定が本ガイドラインのアウトソーシングの定義に該当するかを評価する。一般的に、本ガイドラインの適用対象外となる金融機関の業務やサービスを以下に記載する。

- サードパーティによって実施されることが法的に要求されている法定監査等の機能
- 市場情報サービス（Bloomberg 等）
- グローバルなネットワーク基盤（VISA や MasterCard 等）
- クリアリングおよび決済に関する協定
- グローバルな金融メッセージインフラ
- コルレス銀行業務
- 法律で定められている金融機関が実施できないサービス

B) 重要な機能

以下の条件に当てはまる場合、金融機関にとって、重要な機能とみなされ、より厳格な要件が求められる。

- その機能がなくなることによって、金融機関の財務状況や、銀行業務および決済サービスの健全性・継続性が著しく損なわれる場合
- 内部統制機能の運用業務をアウトソーシングする場合
- 監督機関等の権限を有する機関による許可を必要とする範囲における機能をアウトソーシングする場合

---

44 Guidelines on outsourcing arrangements：
https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

また、アウトソーシング契約が『重要な機能』[45]に当てはまるか否かを評価するために、金融機関が考慮すべき事項を以下に記載する。

- 当該アウトソーシング契約が、銀行業務の提供に直接関連しているか
- アウトソーシングした機能の停止や、アウトソーシング先による不十分なレベルでのサービス提供による潜在的な影響（利益、ビジネス継続性、オペレーショナルリスク、風評リスク等）
- アウトソーシング契約が、リスク管理や規制遵守等に与える潜在的な影響
- 顧客に対するサービスへの潜在的な影響
- アウトソーシング契約の影響を受ける事業領域の規模と複雑さ
- 合意済みのアウトソーシング契約が、基本契約の変更や修正なしに延長される可能性
- 他のサードバーティへ、アウトソーシング契約を移転できる権利の有無
- アウトソーシングした機能を、必要に応じて再統合する権利の有無
- データの保護と、機密性の違反がもたらす潜在的な影響

（ガバナンスフレームワーク）

A) 健全なガバナンス体制とサードパーティリスク

全体的な内部統制として、金融機関は、すべての事業部門や内部ユニットに跨るリスク管理の枠組みを持つ。この枠組みの下で、金融機関は、サードパーティとの協定に起因するすべてのリスクを特定し、管理すべきである。また、リスク管理の枠組みは、金融機関のリスクテイクに関する十分な情報に基づいた意思決定と、サイバーセキュリティリスクを含めたリスク管理措置が適切に実施されていることを保証するものでなければならない。

B) 健全なガバナンス体制とアウトソーシング

金融機関は、『重要な機能』のアウトソーシングを監督する能力を含め、規制上のすべての義務の遵守に対して、引き続きすべての責任と説明責任を負う。したがって、金融機関は、本ガイドラインの対象となるアウトソーシング契約の適切な管理及び監督を行うために、十分な能力と熟練したリソースを有する。アウトソーシングについて、金融機関に求められている要件を以下に記載する。

- 本ガイドラインの対象となるアウトソーシング契約の文書化や管理、責任の明確化
- 本ガイドラインを含め、すべての法律および規制の要件を確実に遵守するための十分な資源の確保

[45]『重要な機能』：一般的な意味の重要な機能ではなく、「Guidelines on outsourcing arrangements」が示す重要な機能の条件に当てはまるものを『重要な機能』（『』つき）で表す

・ アウトソーシングについて、社内の取締役会等の管理機関に対する説明責任を担う担当者の指名

上記に加え、アウトソーシングの際に、金融機関が確認すべき項目を以下に記す。

・ アウトソーシングされた業務を含め、自らの事業活動の重要な業務に関する意思決定を行うこと
・ 銀行業務及び決済業務の秩序を保つこと
・ アウトソーシング契約に関するリスクを適切に特定・評価・管理・低減すること（IT や FinTech のリスクも含む）
・ データ及びその他の情報について、適切な秘密保持契約がなされていること
・ サードパーティとの情報の流れが適切に整備されていること
・ 『重要な機能』のアウトソーシングについて、サードパーティへの移転や、自組織への再統合、依存する業務の停止が可能であること
・ General Data Protection Regulation（一般データ保護規則）（以下、GDPR）に従って個人データが処理されていること

C）アウトソーシングポリシー

アウトソーシング契約を締結しているもしくは、契約する計画がある金融機関は、アウトソーシングポリシーを承認し、定期的なレビューや更新を行う。このポリシーでは、アウトソーシングのライフサイクルと原則及び責任、プロセスを定義する。アウトソーシングポリシーに記載すべき項目を以下に記す。

・ 『重要な機能』のアウトソーシングに関する意思決定への適切な関与を含む、取締役会等の管理機関の責任
・ 「社内横断的に関連する部門（業務部門、顧客対応部門 等）」や内部統制部門等の関与
・ 計画
・ 実施、監視及び管理（サードパーティのパフォーマンス評価等）
・ 出口戦略と終了プロセス

D）利益相反

金融機関は、アウトソーシング契約に関する利益相反を特定・評価・管理する。アウトソーシング契約が、重大な利益相反を生じさせる場合、金融機関はこの利益相反に対する適切な措置を講じる。

E）業務継続計画

金融機関は、アウトソーシングした『重要な機能』に関して、適切な業務継続計画を策定・管理し、定期的に検証する。業務継続計画では、アウトソーシ

ングした『重要な機能』の質の許容できないレベルまでの低下や、アウトソーシング先の倒産等の想定できる最悪のケースを考慮に入れて策定する。

F）内部監査機能

内部監査部門は、リスクベースアプローチに則り、アウトソーシングした機能に対して、独立した監査を行う。

G）ドキュメント要件

リスク管理フレームワークの一部として、金融機関は、すべてのアウトソーシング契約に関する情報が記載された台帳を整備するとともに、現在のすべてのアウトソーシング契約を、『重要な機能』のアウトソーシングとその他のアウトソーシングとを区別したうえで、文書化する。また、国内法を考慮し、金融機関は終了したアウトソーシング契約の文書を前述の台帳内に適切な期間保管する。すべてのアウトソーシング契約について、前述の台帳に保管すべき情報を以下に記す。

- アウトソーシング契約の参照番号
- アウトソーシングの開始日、次回の契約行使日、終了日
- アウトソーシングした機能やデータの概要説明
- アウトソーシング先の企業名、法人登録番号、登録住所、連絡先
- サービスが提供される国、地域
- 『重要な機能』かどうかの判断
- クラウドサービス提供事業者のアウトソーシング契約の場合、当該クラウドサービスの名前と導入モデル（パブリック、プライベート、ハイブリッド等）、保管されるデータの性質と保管場所
- アウトソーシングした機能の重要性の最新の評価日

また、金融機関は、監督当局等からの要請があった場合、アウトソーシング契約に関するすべての情報を開示しなければならない。

（アウトソーシングプロセス）

A） 事前分析

金融機関は、アウトソーシング契約の締結前に、アウトソーシング先の監督当局からの認可や登録の有無の確認や、リスクの特定・評価、適切なデューデリジェンスを実施する。

- アウトソーシング先の認可・登録（銀行業務や決済業務をアウトソーシングする際）

  金融機関は、銀行業務や決済業務をアウトソーシングする際、アウトソーシング先が金融機関の監督当局から認可または登録されていること、または、国内法で銀行業務または決済サービス業務を認可されていることを確認する。

・ リスクの特定・評価

金融機関は、アウトソーシング契約が及ぼす、オペレーショナルリスクへの影響やステップインリスク[46]、複数の機能をアウトソーシングした際の全体のリスクを特定・評価する。

・ デューデリジェンス

アウトソーシング契約の締結及び関連するオペレーショナルリスクの検討の前に、金融機関は、アウトソーシング先が適切であることを確認する。デューデリジェンスを実施する際には、アウトソーシング先の、ビジネスモデルや事業規模、適切なデータの取扱い、行動規範の観点で、アウトソーシング先を評価する。

B) 契約

金融機関及びアウトソーシング先の権利及び義務は、明確に割り当てた上で、書面上の合意を得る。アウトソーシング契約に記載すべき主な項目として、アウトソーシング機能に関する明確な記述や、契約開始日・終了日、契約の準拠法のほか、『重要な機能』の再委託、データとシステムのセキュリティ、アクセス権や監査権、解除権があげられている。

・ 『重要な機能』の再委託

アウトソーシング契約書には、『重要な機能』の再委託を認めるか否かを明記する。再委託を許可する場合、アウトソーシング契約書に、再委託の対象外となる活動や、再委託する場合の遵守事項、再委託先の監督義務等を明記する。

・ データとシステムのセキュリティ

金融機関は、アウトソーシング先が適切な IT セキュリティ基準を遵守していることを確認する。さらに、アウトソーシング契約内で、データおよびシステムのセキュリティ要件を定義し、遵守状況を継続的に監視する。また、クラウドサービス提供事業者へのアウトソーシングや、個人・機密データの取扱い及び転送を伴うアウトソーシングの場合、データのストレージや処理の場所の選定に、リスクベースアプローチを採用する。

・ アクセス権・監査権

金融機関は、アウトソーシングした機能をリスクベースアプローチで評価するために、アウトソーシングした機能に関するすべての情報等へのアクセス権や、アウトソーシング契約に対する検査及び監査の権利を確認する。

・ 解除権

---

[46] ステップインリスク：金融ストレス時に銀行が、契約相手先の事業体に対して契約上の義務を超えた財政上の支援を行わざるを得ないリスクのこと

金融機関がアウトソーシング契約を解除できる権利や、アウトソーシング先の変更、アウトソーシングした機能の自組織への再統合を行う権利を確保する。

C) アウトソーシング業務の監視

金融機関は、リスクベースアプローチで、データの可用性、完全性、安全性が確保されていることを含め、契約に基づいて、『重要な機能』のアウトソーシング先のパフォーマンスを継続的に監視する。また、定期的にリスク評価を更新するとともに、『重要な機能』のアウトソーシングに関して特定されたリスクを社内の取締役会等の管理機関に報告する。

D) 出口戦略

金融機関は、『重要な機能』のアウトソーシングの終了に向けた出口戦略を文書化する。その際、アウトソーシング先の倒産や、アウトソーシングした業務の質の低下や中断等を考慮すべきである。また、金融機関は、事業活動の過度な中断や、顧客へのサービス提供の継続性や質を損なうことなく、アウトソーシング契約を終了できることを確認する。

(ウ) 特徴

本ガイドラインでは、複数の業務を同一企業にアウトソーシングする集中リスクとして、以下の 2 点が定義されている。

- 他社に容易に代替できない、支配的なサードパーティにアウトソーシングすること
- 同一のサードパーティ、もしくは、密接な関係同士のサードパーティに、複数の業務をアウトソーシングすること

(3) インタビュー結果

EU 域内に拠点を持つ金融機関 2 社（銀行、決済サービス事業者）へのヒアリングを実施した。なお、ヒアリング内容は米国と同様とした。

① サイバーセキュリティにおけるガバナンスの構築に関する取組み

EBA「Guidelines on ICT and security risk management」に沿って、組織を構築していた。また人材育成においては、情報システムコントロール協会（ISACA）の資格取得を若手人材に義務付ける等の工夫がみられた。

② サイバーセキュリティリスク管理に関する取組み

リスクの特定では、EBA「Guidelines on ICT and security risk management」を利用する形や、外部の機関が作成したフレームワーク（NIST「Cybersecurity Framework」、ISO27001 等を融合した独自のフレームワーク）を活用することで、自社のリスク管理フレームワークを構築していた。

リスクの評価では、NIST「Cybersecurity Framework」、外部の機関が作成したアセスメントツールを利用するといった意見が聞かれた。また EBA「Guidelines on outsourcing arrangements」を活用してアウトソーシング先の評価を実施していた。

リスクの低減では、金融機関が一般的に利用する情報共有機関は確認できなかったものの、他の業態も利用する情報共有機関を活用して、業界のベンチマークについて、他の業態と情報交換等を行うといった工夫も聞かれた。また、定期的な脆弱性診断およびペネトレーションテストに加え、第三者のホワイトハッカー等に新たなセキュリティ上のバグがないかを確認してもらう、報奨金プログラムを実施していた。

## 4. 英国におけるサイバーセキュリティ

### (1) 英国のサイバーセキュリティ関係当局[47]

英国金融機関のサイバーセキュリティに関係する当局は、4 つ存在する。1 つは金融機関に限らず、英国全体のサイバーセキュリティを所掌する National Cyber Security Centre（国立サイバーセキュリティセンター）である。

さらに 3 つの金融当局が存在する。1 つはイングランド銀行であり、英国の中央銀行としてサイバーセキュリティに関与している。

次に Prudential Regulation Authority（健全性規制機構）（以下、PRA）である。イングランド銀行の 1 機関として、金融安定を目的とした規制を行う機関であり、金融インフラ全体のサイバーセキュリティを監督する役割を担っている。

最後に Financial Conduct Authority（金融行為監督機構）（以下、FCA）である。消費者や投資家保護を目的とした規制を行う機関であり、サイバーセキュリティの分野では主に金融機関個々のサイバーセキュリティ対応を監督する役割を担っている。

### (2) 英国の調査対象概要

今回、英国における調査対象とした文献は以下の 5 つである。英国では FCA が発行する金融機関が遵守するルールが記載される「FCA Handbook」において、チーフオペレーショナルオフィサーがサイバーセキュリティを所掌することが原則として記載されている[48]。詳細なサイバーセキュリティに係る要件は、個々のガイドラインやフレームワークに記載されている。

また直近では、オペレーショナルレジリエンスのガイドラインの素案が提示されている。ここでは、サイバー攻撃によるものを含む、業務の中断がもたらす重要な業務やサービスへの影響の許容度（Impact tolerances）を評価・テストするための枠組みも検討している。

---

47 EU との関係においては 2020 年 12 月 31 日をもって、EU からの離脱移行期間が満了となる予定であるが、調査時点においては EU の離脱以降の対応についての記載は確認できなかった。

48 FCA と同様に英国の規制当局である PRA より発行される、PRA Rulebook については、内容にサイバーセキュリティに関する個別の記載は見られなかったため、本調査対象からは割愛する。

**表 7 英国の調査対象一覧**

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 1 | FCA | FCA Handbook[49] | FCA の認可を受けた金融機関に対する規制。<br>サイバーセキュリティを含むシステムの管理、システム等を統括するチーフオペレーショナルオフィサーの役割について、プリンシプルベースで記載されている。 |
| 2 | イングランド銀行 | CBEST[50] | 脅威ベースのペネトレーションテストに関するフレームワーク。 |
| 3 | PRA/FCA 共同発行 | Cyber Resilience Questionnaire[51] | 金融機関が自社のサイバーレジリエンスを理解するためのセルフアセスメントシート。<br>全 6 つの分野、48 項目の設問に回答する。 |
| 4 | | Building operational resilience:Impact tolerances for important business services[52] | オペレーショナルレジリエンスを確保することを目的に金融機関の重要なサービスの影響許容度（Impact tolerances）を評価・テストするためのガイドラインの素案で、現在パブリックコメントの募集中である。 |
| 5 | PRA | Outsourcing and third party risk management[53] | 金融機関がサードパーティに業務を委託する場合のガイドラインの素案であり、現在パブリックコメントの募集中である。 |

[49] FCA Handbook：https://www.handbook.fca.org.uk/handbook

[50] CBEST：https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf

[51] Cyber Resilience Questionnaire：https://www.fca.org.uk/firms/cyber-resilience

[52] Building operational resilience:Impact tolerances for important business services：https://www.bankofengland.co.uk/news/2019/december/building-operational-resilience-impact-tolerances-for-import-business-services

[53] Outsourcing and third party risk management ：https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management

① FCA「FCA Handbook」

(ア) 目的・経緯

FCA は消費者の保護、市場の完全性の保護、競争の促進の 3 つを目的としており、本規制は、FCA の認可を受けた金融機関に対する規制である。

(イ) 概要

本規制は 7 つの章、2 つのガイドブックにより構成されている。本調査においては、特にサイバーセキュリティに限った箇所について記載する。

（ｉ）該当箇所：スタンダード－SYSC（Senior Management Arrangements, Systems and Controls・上級管理職の手配、システムおよびコントロール）[54]

（SYSC 3.1.1 システムおよびコントロール）

A) 企業は事業に適したシステムとコントロールを確立し、維持するために合理的な注意を払わなければならない

（SYSC 3.2.6 コンプライアンス、金融犯罪、マネーローンダリングに関連するシステムとコントロール）

B) 企業は規制の下で適用される要件や基準を遵守し、金融犯罪に利用されるリスクに対抗するための効果的なシステムと管理を確立し、維持するために合理的な注意を払わなければならない

（ii）該当箇所：規制プロセス－SUP（Supervision・監督）[55]

（SUP10C.6B.2 チーフオペレーショナルオフィサーの機能）（抜粋）

C) チーフオペレーショナルオフィサーは、企業または企業の一部の内部業務、技術の全部または実質的に全部を統括的に管理する責任を有する。

（SUP10C.6B.4 チーフオペレーショナルオフィサーの機能）

D) チーフオペレーショナルオフィサーが所管する業務には以下のような分野が含まれているが、必ずしもこれに限定されるものではない。

1. 業務継続
2. サイバーセキュリティ
3. IT
4. 内部業務
5. 業務の継続性、レジリエンスおよび戦略
6. アウトソーシング、調達およびベンダー管理

54 FCA Handbook High Level Standards の章：
https://www.handbook.fca.org.uk/handbook/SYSC/3/?view=chapter

55 FCA Handbook Regulatory Processes の章：
https://www.handbook.fca.org.uk/handbook/SUP/10C/?view=chapter

② イングランド銀行「CBEST」

(ア) 目的・経緯

イングランド銀行は、金融機関のサイバー攻撃への耐性を確保することを目的に本フレームワークを導入した。脅威ベースのペネトレーションテストに関して、世界に先駆けて策定されたフレームワークである。2014 年に第 1 版が、2016 年に、より利用しやすいよう改定された第 2 版が発行されている。

(イ) 概要

本フレームワークでは、脅威情報を基としたペネトレーションテストのプロセスは、4 つのフェーズにより構成されている[56]。

（ｉ）開始フェーズ

開始フェーズは、主にスコープの決定、脅威インテリジェンスプロバイダー（Threat Intelligence Provider、以下　TI）、ペネトレーションテストプロバイダー（Penetration Test Provider、以下　PT）の調達を行う。

（ii）脅威インテリジェンスフェーズ

脅威インテリジェンスフェーズでは、TI 主導の下で現実的な脅威シナリオを作成する上でベースとなる情報収集を行う。TI は、金融機関または金融市場インフラ（FMI（Financial Market Infrastructure））　からスコープの説明を受け、脅威情報の収集、分析、発信、レビューを行う。 並行して、PT は　TI の支援の下、ペネトレーションテスト計画書の作成に向けて、脅威シナリオを作成する。脅威インテリジェンスフェーズの成果物（脅威情報の収集結果およびペネトレーションテスト計画書）は、全てのステークホルダーが参加するレビューを経て最終化され、TI から PT へ引継がれる。

（iii）ペネトレーションテストフェーズ

ペネトレーションテストフェーズでは、PT がペネトレーションテスト計画書に基づき、テストを実施するとともに、PT が金融機関または金融市場インフラ（FMI）の検知、対応能力を評価し、ペネトレーションテスト報告書に取りまとめる。また、ペネトレーションテスト報告書を金融機関または金融市場インフラ（FMI）、監督当局がレビューする。

（iv）完了フェーズ

完了フェーズでは、TI が作成した脅威インテリジェンスおよび PT が作成した検知・対応能力の評価を基に、イングランド銀行が脅威インテリジェンス・検知・対応に関する報

[56] 詳細は「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」を参照。
https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf

告書を作成し、監督当局がレビューする。改善が必要である場合、金融機関または金融市場インフラ（FMI）は改善計画書を作成し、監督当局は改善計画書に基づきモニタリングする。

③　PRA/FCA 共同「Cyber Resilience Questionnaire」

(ア) 目的・経緯

金融機関が自社のサイバーレジリエンスの対応レベルを理解できるように、PRA および FCA が作成したセルフアセスメントシートである。

(イ) 概要

評価項目は全 6 分野 48 項目あり、A、B、C、D の 4 段階で自社のレベルを評価する。詳細な評価項目の内容は別紙「B)Cyber Resilience Questionnaire の点検項目」に記載する。

**表 8　Cyber Resilience Questionnaire の概要**

| 分野 | 概要 |
|---|---|
| ガバナンスとリーダーシップ | サイバーセキュリティ戦略およびフレームワークの策定等、金融機関としてのガバナンスの構築状況に加え、サイバーセキュリティを担当する上級管理職の知識、スキルレベル、役割等のリーダーシップに関する項目 |
| 識別 | 情報資産管理台帳の整備、システムの利用状況、ビジネス上の重要性を考慮したリスク評価の対応状況に加え、サードパーティの管理、ハードウェア・ソフトウェアの保守期限の管理等に関する項目 |
| 防御 | データセキュリティに関する技術的対策、オペレーションシステム、データベース、アプリケーション、デバイス等システムに関する技術的対策の実施状況に加え、採用や教育等のスタッフの管理に関する項目 |
| 検知 | 外部からの異常な活動やイベントの監視、検知機能等、システムおよびネットワークの監視状況に加え、情報共有・分析プロセスの整備状況に関する項目 |
| 対応 | 内外連携、セキュリティイベントの調査等、インシデント対応計画の策定状況に関する項目 |
| 復旧 | データ、サービスの復旧プロセスの整備状況に関する項目 |

(ウ) 特徴

本セルフアセスメントシートでは、上級管理職を定めることに加え、CISO 等を含む、サイバーセキュリティに関する上級管理職に求められる知識・スキルの充分性を評価項目としている。

【チェック項目】

・サイバーセキュリティフレームワークの提供について、責任を負う上級管理職の任命状況

・上級管理職の知識、スキルの充分性

・上級管理職による「金融機関全体のサイバーセキュリティ戦略における役割、アカウンタビリティ、責任」の定義状況

④ PRA/FCA 共同「Building operational resilience: Impact tolerances for important business services」

(ア) 目的・経緯

金融機関および金融市場インフラ(FMI)のオペレーショナルレジリエンスを促進するためのより強固な枠組みを整備することを目的に、PRA および FCA はオペレーションレジリエンスの構築に関するガイドラインを策定した。本報告書作成段階では、素案に対するパブリックコメントを募集しているところである。

(イ) 概要

本ガイドラインには、主に、重要なビジネスサービスの特定、重要なビジネスサービスが中断した場合に生じる影響の許容度（Impact tolerances）を定義すること、重要なビジネスサービスのオペレーショナルレジリエンスをテストすること、の 3 点が記載されている。

（ｉ）重要なビジネスサービス

A) ビジネスサービス

ビジネスサービスを「金融機関または金融市場インフラ（FMI）が顧客に提供する製品およびサービス」と定義しており、金融機関が外部の顧客等、エンドユーザーまたは市場参加者に提供するサービスを指している。

ビジネスサービスのバリューチェーンを紐解き、どの部分がサービス提供において重要かを決定する。

B) 重要なビジネスサービス

重要なビジネスサービスとは、提供が中断されることで、消費者や市場参加者に許容できない損害を与えるおそれがあるビジネスサービスをいう。

消費者や市場参加者に許容できない損害とは、市場の健全性が損なわれること、保険契約者の保護が脅かされること、金融機関の安全性・健全性が脅かされること等を指している。

金融機関および金融市場インフラ（FMI）は自ら重要なビジネスサービスを特定する責任を負っており、特定した重要なビジネスサービスについて、取締役会および上級管理職に承認を得る。また、当該ビジネスサービスのレジリエンスを他のビジネスサービスよりも優先して確保する。

また重要なビジネスサービスの特定に際しては、「（ⅲ）オペレーショナルレジリエンスの提供」に記載されるシナリオテストを実施可能なよう、十分に細分化されるべきである。

（ii）影響許容度（Impact tolerances）

A) 影響許容度の定義

影響許容度を「特定のビジネスサービスの中断が発生することを前提とした、中断の許容度」と定義している。影響許容度を設定する目的は、経営者が重要なビジネスサービスのために構築する必要がある回復力のレベルを把握できるように、明確な測定基準を提供することである。

B) 影響許容度の設定

金融機関および金融市場インフラ（FMI）は、最大許容停止レベルに関する具体的な指標を特定すべきである。指標には、ビジネスサービスの重要度を考慮して、最大許容停止時間を含める必要がある。ただし、時間のみに基づく指標では影響が十分に把握できない場合が考えられる。例えば、最大許容停止業務量、処理できない取引数、または影響を受ける顧客数を含むことによって、中断の程度を測定することができる。

なお、影響許容度とリスクアペタイトの考えは異なるものである。リスクアペタイトは金融機関が戦略を実現するにあたり、自ら引き受けるリスクの量であるのに対し、影響許容度はリスクが集約されたものであり、自社のリスクアペタイトを超過し、深刻なオペレーションへの影響をもたらした場合も、ビジネスサービスの継続が可能かについて焦点を当てている点で異なる。

C) 二重規制の企業の対応

PRA と FCA の両方に規制されている金融機関は、消費者の被害、市場の健全性に係る影響許容度と、企業の財務の安定性、安全性、健全性に係る影響許容度の 2 つを持つことが可能である。

（iii）オペレーショナルレジリエンスの提供

A) オペレーショナルレジリエンスの構築に向けた行動

金融機関および金融市場インフラ（FMI）は影響許容度を用いて、厳しいが妥当なシナリオにおいて中断の影響を影響許容度以下に収めることができることを保証すべきである。そのため、厳しいが妥当なシナリオ、シナリオテストおよびマッピングを行い、中断の影響を影響許容度以下に収めることができるかを検証する。

B) 厳しいが妥当なシナリオ

金融機関や市場インフラ（FMI）が影響許容度以下で重要なビジネスサービスの提供を再開することができるシナリオとそうでないシナリオを特定することで、適切な業務回復力を確保できるとしている。影響許容度を超えてしまうシナリオを特定した後、取締役会および上級管理職は影響許容度以下に収まらないシナリオが許容されるかどうかを判断する。

C) シナリオテスト

シナリオテストとは、蓋然性が高い重大な業務中断が発生した場合に金融機関または金融市場インフラ（FMI）が重要なビジネスサービスの中断が及ぼす影響を影響許容度以下に収める能力をテストすることである。金融機関は、事業およびリスクプロファイルに関する性質、深刻度、継続期間の異なる様々な不利な状況を想定し、そのような状況下において重要なビジネスサービスの提供に対するリスクを想定する。

D) 影響のマッピング（テスト結果の検証）

マッピングとは、重要なビジネスサービスの提供に必要な人員、プロセス、テクノロジー、設備、情報等のリソースを特定し、文書化することである。

マッピングによって金融機関は重要なビジネスサービスがどのように提供され、どのように混乱を招く可能性があるかを理解できる。具体的には以下の順序で対応を行う。

- 高複雑性、単一障害点、単一の資源への依存等、重要なビジネスサービスの提供における脆弱性を特定する
- 脆弱性対策を適宜実施する
- シナリオに耐えられるかをテストする

(ウ) 特徴

本ガイドラインでは、金融機関および金融市場インフラ（FMI）が自社の重要業務が中断した場合の、影響許容度を評価し、テストすることを求めている。具体的には、「最大中断期間」、「中断時に影響する業務量」、「データの整合性を確保可能かどうか」、「影響を受ける顧客数」等を測定基準として、業務停止時の影響を評価することで、影響許容度を設定する。

業務継続の観点から、経営者自らが重要業務の影響許容度を認識し、どの程度のオペレーショナルレジリエンスを有する必要があるかを判断していくことが求められている。

⑤ PRA「Outsourcing and third party risk management」

(ア) 目的・経緯

本ガイドラインは金融機関によるアウトソーシングに適用される法的要件を含んでおり、金融機関は本ガイドラインを遵守することで法的要件を満たせる。EBA「Guidelines on outsourcing arrangements」を受けて、修正が加えられている。

なお、本ガイドラインの大部分は信用組合（credit unions）、Non Directive Firms（NDFs）[57]には適用されない。

[57] 総保険料収入が 500 万ユーロ未満かつ技術的準備金が 2,500 万ユーロ未満の保険会社を指す。

(イ) 概要

本ガイドラインは、アウトソーシングに係るガバナンスに加え、プロセスおよび留意事項を、7点記載している。

（ｉ）ガバナンスおよび記録管理

A) アウトソーシングに関する取締役会の関与

取締役会および上級管理機能を遂行する個人は、自社のアウトソーシング全般に責任を負う。アウトソーシング契約を締結した金融機関は全ての規制を遵守する責任を負っている。金融機関の取締役会はアウトソーシングに関して以下を行う。

- アウトソーシングリスクを含む全社的な管理環境を構築する
- 金融機関が晒されている全てのリスクを効果的に管理する責任を負う

B) アウトソーシングと上級管理職の責任

金融機関は上級管理職に対し、アウトソーシングに関する規制上の義務を果たす責任を割り当てる。

責任は、アウトソーシングに関する全社的なフレームワーク、ポリシー、仕組みおよびコントロールを包含しているものと解釈する。ただし個々のアウトソーシング契約の責任は、個々の業務ラインにある。

C) アウトソーシングポリシー

EBA「Guidelines on outsourcing arrangements」では、取締役会が書面によるアウトソーシングポリシーを承認し、定期的に見直すことが定められている。金融機関はこのアウトソーシングポリシーまたはその一部をサードパーティとの契約に適用することを選択できる。アウトソーシングポリシーは金融機関の戦略やポリシーと整合的であるべきである。本項目は EBA「Guidelines on outsourcing arrangements」を準用している。

D) 記録管理

EBA「Guidelines on outsourcing arrangements」は、2019 年 9 月 30 日から新たなアウトソーシング契約を締結した場合には、契約したアウトソーシングの情報登録を行い、2021 年 12 月 31 日以降全てのアウトソーシング契約について、重要なものと重要でないものを区別した最新のアウトソーシングの情報登録を求めている。本項目は EBA「Guidelines on outsourcing arrangements」を準用している。

（ii）アウトソーシング前のフェーズ

A) アウトソーシング契約の重要性の評価

金融機関はアウトソーシング契約の重要性を評価する責任を負う。重要性は契約の段階等によって変化する可能性があるため、以下のタイミングで実施すること。

- 契約締結前
- 契約後の定期的なレビュー
- 金融機関がサービスの利用やサービスプロバイダへの依存を拡大することを計画している場合
- 所有権や財務状態の変更等、サービスプロバイダまたは再委託先で組織変更が発生した場合

重要性を評価するために金融機関は一定の評価基準を定めることが望ましい。
金融機関はアウトソーシング契約を、金融機関のパフォーマンスの欠陥または失敗が重大な損害を与える可能性のある要素と考える必要がある。
アウトソーシング契約を締結または大幅に変更する場合、PRA に通知する。なおアウトソーシング契約を締結する前に通知を提出することが望ましい。
また、金融機関の計画するアウトソーシング契約の重要性に応じて、金融機関からサードパーティへの追加情報の提供、適宜のフォローアップ措置を実施することが望ましい。

B) 全てのサービスプロバイダに対して適切なデューデリジェンスを実施
金融機関は外部委託契約の締結前に、代替またはバックアップ機能の提供者を含めた、サービスプロバイダのデューデリジェンスを実施することが望ましい。

C) アウトソーシング契約のリスクの評価の時期と頻度
金融機関は定期的にアウトソーシング契約のリスク評価を実施する。
また重大な契約違反、またはリスクの顕在化により、アウトソーシング契約のリスクに重大な変化が生じた可能性がある場合にも、リスク評価を実施すべきである。
リスク評価に際してはサードパーティへの依存度、金融機関やグループにおける集中リスク、ベンダーロックインを管理する。

（iii）アウトソーシングの契約
全てのアウトソーシング契約は書面によるものとする。
金融機関が特定のサービスを追加または削除できる基本サービス契約がある場合、個々のサービスが適切に文書化されていることが望ましいが、必ずしも個別の契約に含まれている必要はない。
重要な機能におけるアウトソーシング契約には以下を含める。
- データセキュリティ（ivに記載）
- アクセス権、監査権、情報に関する権限（ｖに記載）
- 再委託（viに記載）
- 業務継続計画およびアウトソーシング終了計画（viiに記載） 等

（ⅳ）データセキュリティ

この章でいうデータには、機密データ、企業データ、トランザクションデータ、データの処理・転送・保存等に使用されるシステムを含む。

重要なアウトソーシング契約にデータの転送が含まれる場合、金融機関がデータに関する自社およびアウトソーシング先それぞれの責任を理解のうえ、定義、文書化し、適切な保護措置を講じることが望ましい。

A) データの分類

データの分類では、重要なビジネスサービスに対する影響許容度（Impact Tolerance）を考慮して、システム停止が発生した場合に優先的にアクセスし、移行する必要のあるデータを特定する。

また、金融機関がデータをクラウドサービス提供事業者に外部委託する場合、クラウドに移行する自社のデータおよびアプリケーションのクラウド対応可否を評価する必要がある。

B) データの場所

金融機関は使用中でないデータ、使用中のデータおよび転送中のデータを考慮し、データの格納場所をリスクベースアプローチで選定する。具体的には、以下二つのバランスを勘案する。

- GDPR の下での法的リスク、相反する法的または規制上の要件、英国外の特定の地域のデータにアクセスする際の課題
- アウトソーシングされたデータが複数の場所に保存されることによる運用面でのレジリエンスのメリット

C) データセキュリティ

金融機関は転送中のデータ、メモリ内のデータおよび保存中のデータに対する堅牢なコントロールを実装することが望ましい。

（ⅴ）アクセス権、監査権、情報に関する権限

重要な機能におけるアウトソーシング契約とそれ以外のアウトソーシング契約に分けて、各々に求められるアクセス権、監査権、情報に関する権限について言及している。

A) 重要な機能におけるアウトソーシング契約

重要な機能におけるアウトソーシング契約のアクセス権、監査権、情報に関する権限には以下を含めるべきである。

- 外部委託されたサービスの提供やパフォーマンスの監視に使用されるデータ、デバイス、システムおよびネットワークにアクセスできること。また必要に応じてサイバーおよび内部の IT セキュリティ対策とプロセスの有効性を評価するため、自社のアプリケーション、データおよびシステムに対するペネトレーションテストを実施すること

・ サービスプロバイダの会社情報、財務情報を取得できること
・ サービスプロバイダの外部監査人、担当者および施設に関する情報を取得できること

また、金融機関はアウトソーシング契約に関するアクセス権、監査権および情報に関する権限について以下を行使することが望ましい。
・ サービスプロバイダが提供する証明書、その他の独立した報告書等によるオフサイト監査
・ 個別監査または他の金融機関とのオンサイト監査（共同監査）

B) 重要な機能以外のアウトソーシング契約

重要な機能以外のアウトソーシング契約に関しては、金融機関がアクセス権、監査権、情報に関する権限を保持するか否かについて、リスクベースアプローチを採用することを期待する。ただし、これらの権限を取り決めない場合においても、将来重要な機能になる可能性を考慮すべきである。

（vi）再委託

再委託とは、「アウトソーシング契約下においてサービスプロバイダが、アウトソースされた業務の一部を他のサービスプロバイダにさらに移転する状況」と定義されている。

重要な機能におけるアウトソーシング契約が再委託を伴う場合、再委託先のデューデリジェンスを行う目的から、金融機関は再委託先の最新のリストを維持することが望ましい。

特に重要なビジネスサービスの提供に関与している再委託先は監視する必要がある。

また、重要な機能におけるアウトソーシング契約には再委託の可否等を契約事項に盛り込むべきである。

（vii）業務継続計画およびアウトソーシング終了計画

重要な機能におけるアウトソーシング契約に伴い、業務継続計画およびアウトソーシング終了計画をドキュメント化し、維持、テストすることが望ましい。

A) 業務継続計画

金融機関はサービスプロバイダに、事業の中断を予測したうえで、回復するための業務継続計画を策定、実行することを要求すべきである。

特にデータ復旧に関してはデータ破壊を意図したサイバー攻撃の影響を考慮することが望ましい。

またクラウドを利用した重要な機能におけるアウトソーシング契約においては、金融機関がアウトソーシングするサービスとデータのレジリエンス要件を評価のうえ、リスクベースアプローチを利用して、1 つまたは複数のクラウドのレジリエンスオプション[58]を検討すべきである。

B) アウトソーシング終了計画

金融機関のアウトソーシング終了計画は、可能な限り適切に文書化し、テストするべきである。

アウトソーシング終了計画策定の目的は、サービスプロバイダの倒産、清算等により、他の業務継続手段では管理できない混乱が生じた場合を想定し、最終手段としてリスク低減を図ることにある。そのためアウトソーシング契約そのものの終了プロセスを整理するのではなく、サービスプロバイダが関連する重要なビジネスサービスを継続するための以下のような対応を検討すべきである。

- データ、機能またはサービスの内製化
- 代替またはバックアップからのデータ、機能またはサービスの転送
- 他の実行可能な方法の検討

C) 業務継続計画とアウトソーシング終了計画のガバナンス

計画されているアウトソーシング契約が重要であると判断した場合には、契約前に業務継続計画とアウトソーシング終了計画を策定すべきである。

(ウ) 特徴

本ガイドラインでは、アウトソーシングのリスク評価において、サードパーティへの依存度、金融機関やグループにおける集中リスク、ベンダーロックインを管理し、合理的な措置を講じるよう記載されている。

(3) インタビュー結果

英国の金融機関 2 社（銀行、チャレンジャーバンク）へのヒアリングを実施した。またヒアリング内容は米国・欧州と同様とした。

① サイバーセキュリティにおけるガバナンスの構築に関する取組み

英国のコーポレートガバナンスコードに従って設置した、リスクに関する委員会がアジェンダの一つとしてサイバーセキュリティを取り扱っていた。

また英国の会社法によって、取締役が合理的なスキル、注意、勤勉さを発揮し、その役割を果たすことと定められていることを踏まえ、最高情報セキュリティ責任者（CISO）を取締役に

58 クラウド使用時における耐障害性を目的としたサービスのオプション。ガイドラインには、地理的に分散した複数のデータセンターの活用、異なるアベイラビリティゾーンにある複数のデータセンターの活用、データセンターダウン時の再ルーティング機能の活用、ハイブリッドクラウドの活用等を検討することが例示されている。

据え、法的責任を伴う形で業務を遂行させている金融機関もあった。これにより最高情報セキュリティ責任者のアカウンタビリティを明確にするといった効果を期待していた。

さらに金融機関における CISO のレポーティングラインを直接取締役会（CEO を介さない）とすることで、事業とは独立する形でサイバーセキュリティを経営課題として議論できるようにしているといった工夫も聞かれた。

② サイバーリスク管理に関する取組み

リスクの特定では、ISO27000 シリーズ[59]を網羅する形で、リスク管理フレームワークを構築しているといった意見が聞かれた。

リスクの評価では、ISO27004[60]を活用したといった意見や、情報システムコントロール協会（ISACA）の CRISC[61]の資格保有者を活用したリスクマネジメントを行っているといった話も聞かれた。

リスクの低減では、外部のベンダーの活用等により、脆弱性診断・ペネトレーションテストを定期的に実施し、発見された脆弱性へ対応していた。ペネトレーションテストでは外部からの攻撃に加え、内部からの攻撃の視点でもテストを実施していた。

59 国際標準化機構（ISO）が策定する情報セキュリティに係る規格

60 ISO27000 シリーズのうち、導入された ISMS および管理策（群）の有効性を評価するための測定に関するガイダンス（出所：https://isms.jp/chumon.html）

61 情報システムコントロール協会（ISACA）が提供する資格である。CRISC は Certified in Risk and Information Systems Control の略。

## 5. シンガポールにおけるサイバーセキュリティ

### (1) シンガポールのサイバーセキュリティ関係当局

シンガポール金融機関のサイバーセキュリティに関係する当局は、2 つ存在する。1 つは金融機関に限らず、シンガポール全体のサイバーセキュリティ戦略を監督する Cyber Security Agency of Singapore（サイバーセキュリティ庁）（以下、CSA）である。CSA はシンガポールの首相府の直下組織であり、サイバーセキュリティに関する専門機関として、2015 年 4 月に設立された。もう 1 つはシンガポールの中央銀行でもある Monetary Authority of Singapore（金融管理局）（以下、MAS）である。MAS は 1971 年 1 月に設立され、通貨・金融政策から金融機関の規制監督に至るまで、広範囲の業務を担当している。

### (2) シンガポールの調査対象概要

今回、シンガポールにおける調査対象とした文献は以下の 5 つである。シンガポールでは、他国と比較し、法令・ガイドラインにおいて詳細な要件が定められているものが多い。

「CYBERSECURY ACT[62]」は金融業に限らず、全ての重要インフラ保護のため制定された法律であり、シンガポール政府により発行された。この法律に則り、「Notice on Technology Risk Management[63]」、「Notice on Cyber Hygiene[64]」等の通知が発出・改定されている。なかでも「Notice on Technology Risk Management」については、さらに詳細な内容を定めた「Technology Risk Management Guidelines[65]」が策定されており、金融機関のシステムリスク管理の詳細を定義している。なお、現在パブリックコメント中である「Technology Risk Management Guidelines」の改定案「Consultation Paper Technology Risk Management Guideline[66]」の内容についても、参考として確認した。

**表 9 シンガポールの調査対象文献一覧**

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 1 | シンガポール政府 | CYBERSECURITY ACT | シンガポールの重要インフラ保護に向け、サイバーセキュリティの監視と維持のための法的枠組みを明確化した法律 |

62 CYBERSECURITY ACT：https://sso.agc.gov.sg/Acts-Supp/9-2018/

63 Notice on Technology Risk Management：https://www.mas.gov.sg/regulation/notices/notice-cmg-n02

64 Notice on Cyber Hygiene：https://www.mas.gov.sg/regulation/notices/notice-655

65 Technology Risk Management Guidelines：https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

66 Consultation Paper Technology Risk Management Guideline：https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-proposed-revisions-to-technology-risk-management-guidelines

| # | 発行機関 | 規制・ガイドライン名 | 概要 |
|---|---|---|---|
| 2 | MAS | Notice on Technology Risk Management | 「CYBERSECURITY ACT」制定を受けて策定された、金融機関の重要システムのリスク管理手法を定めた規制要件 |
| 3 | MAS | Notice on Cyber Hygiene | 金融機関のサイバー衛生維持のため、平時に実施すべきサイバーセキュリティ対策を定めた規制要件 |
| 4 | MAS | Technology Risk Management Guidelines | 「Notice on Technology Risk Management」に沿って策定された金融機関のシステムリスク管理のガイドライン（2020 年 3 月現在改定中） |
| 5 | MAS | Guidelines on Outsourcing[67] | 金融機関におけるアウトソーシングについて、金融サービス提供の安定化、セキュリティの確保等を目的に策定されたガイドライン |

① シンガポール政府「CYBERSECURITY ACT」

(ア) 目的・経緯

2016 年 10 月に発表された「サイバーセキュリティ戦略」に基づき、シンガポール政府が自国の金融業を含む重要インフラの強靭性を高めることを目的に 2018 年に制定した。

(イ) 概要

本法律では、主に以下の内容が定められている。

（ｉ）『重要な情報システム』の指定・取消

以下の条件を満たす際、対象のシステムの所有者に書面で通知することにより、本法案の対象である『重要な情報システム』であると指定することができる

- 社会維持に必要不可欠なサービスを継続的に提供するために必要であり、かつ、損失又は危殆化がサービスの利用に影響を及ぼすものであること
- 全部又は一部がシンガポールにあること

（ii）『重要な情報システム』に関する情報の CSA への提出義務

- 『重要な情報システム』については、CSA に求められた情報（設計・構成・セキュリティに関する情報等）を提出することが義務付けられている
- 違反とみなされた場合、10 万シンガポールドル以下の罰金、または 2 年以下の懲役、またはその両方が科される

67 Guidelines on Outsourcing ：https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

（iii）重要インフラ事業者[68]が受けたサイバーセキュリティインシデントの CSA への報告義務

- サイバーセキュリティインシデントが発生した場合、CSA 長官への報告が義務付けられている
- 違反とみなされた場合、10 万シンガポールドル以下の罰金、または 2 年以下の懲役、またはその両方が科される

（iv）重要インフラ事業者のサイバーセキュリティ監査とリスク評価

- 2 年に 1 度、CSA に承認または任命された監査人による監査の実施が義務付けられている
- 年次でのサイバーリスク評価の実施が義務付けられている
- 違反とみなされた場合、2 万 5 千シンガポールドル以下の罰金、または 12 ヶ月以下の懲役、またはその両方が科される

（v）サイバーセキュリティ演習への参加の義務化

- CSA から指示された場合、サイバーセキュリティ演習への参加が義務付けられている
- 違反とみなされた場合、10 万シンガポールドル以下の罰金が科される

（vi）CSA によるサイバーセキュリティインシデント調査における権限

- CSA がサイバーセキュリティインシデント調査のために要求した場合、いかなる人物でも、面談の実施、記録・文書等の提出が義務付けられている
- 違反とみなされた場合、2 万 5 千シンガポールドル以下の罰金、または 2 年以下の懲役、またはその両方が科される

（vii）サイバーセキュリティサービスプロバイダの免許制

- サイバーセキュリティサービスプロバイダとして事業を行うために、免許の取得が義務付けられている
- 免許は 5 年ごとの更新制
- 免許を持たないで事業を行った場合、制裁金や懲役が科される（違反内容によって制裁金の金額や懲役の期間は異なる）

(ウ) 特徴

本法律は金融機関に留まらず、重要インフラ全てを対象とした適用範囲の広い法律であるが、法律内で CSA に対する情報の提出・報告の義務や、監査の頻度、サイバーセキュリティ演習への参加義務等が明確に定められていることが特徴である。

68 重要インフラ事業者：社会維持に必要不可欠なサービスを継続的に提供する事業者。金融機関についても対象となるものと考えられる。

② MAS「Notice on Technology Risk Management」

(ア) 目的・経緯

2013 年 6 月に公示された、MAS が定義したシステムリスク管理の規制要件。同月に発表された「Technology Risk Management Guidelines」はこの要件に沿って策定されている。2018 年、「CYBERSECURITY ACT」制定を受け、内容が改定された。なお、本規制は大手金融機関、中小金融機関、また業態を問わず、全ての金融機関が対象となっている。

(イ) 概要

本規制では、金融機関における重要システムについて、以下の内容が定められている。

（ⅰ）金融機関における重要システムの定義

（ⅱ）金融機関における重要システム維持に関する態勢整備

- 金融機関は重要システムを特定するための体制とプロセスを整備する
- 金融機関は重要システムの可用性を維持する取り組みを行う。なお、重要システムのダウンタイムは 12 ヶ月のうち合計 4 時間を超えないようにすること
- 金融機関は重要システムの復旧目標時間（RTO）を 4 時間以内としなければならない。また、システム復旧テストを最低でも 12 ヶ月に 1 度は実施し、どのように復旧目標時間（RTO）内での復旧実現が検証されたかを文書化しなければならない

（ⅲ）金融機関における重要システムがサイバーインシデントを受けた場合の報告義務

- 金融機関はインシデント発見から 1 時間以内に MAS へ報告することが義務付けられている
- 金融機関はインシデント発見から（原則）14 日以内で、根本原因及び影響分析を記した報告書を MAS へ提出することが義務付けられている
- 金融機関は不正アクセス等から顧客情報を保護するための IT 管理を実施する

(ウ) 特徴

本規制では、重要システムのダウンタイムの制限、また復旧目標時間等が数値として明確に定められている。さらに金融機関の MAS へのサイバーインシデントの報告についても、発見から報告までの期間が詳細に規定されている。

③　MAS「Notice on Cyber Hygiene」

(ア) 目的・経緯

MAS は、サイバー脅威の深刻化を考慮し、金融機関のサイバーレジリエンス能力の向上を目的に、金融機関のサイバー衛生[69]についての規制を発出した。「Notice on Technology Risk Management」と同様に、本規制についても全ての金融機関が対象となっている。なお、本規制の適用は 2020 年 8 月 6 日からと定められている。

(イ) 概要

金融機関のサイバー衛生維持に向けて、以下の 6 つを義務付けている。

（ｉ）アカウント管理

システムに無制限にアクセス可能な特権アカウントを保護する。対象のシステムは、オペレーティングシステム、データベース、アプリケーション、セキュリティ製品、ネットワーク機器とする。

（ii）セキュリティパッチの適用

金融機関が保有する全てのシステムに対し、最新のセキュリティパッチを適用し、脆弱性に対処する。

セキュリティパッチを適用できないシステムがある場合、脆弱性についてのリスクを低減するために、管理体制を確立する。

（iii）セキュリティスタンダードの策定

金融機関はシステムのセキュリティスタンダードを策定する。

セキュリティスタンダードには、金融機関が保有するシステムのセキュリティの保護および改善を目的に一連のプロセスを規定する。

策定したセキュリティスタンダードに準拠できないシステムが存在する場合、そのシステムが保有するリスクを低減するために、管理体制を確立する。

（iv）ネットワーク境界の防御

不正なネットワークトラフィックが発生する可能性のある全てのネットワークの境界に対して、ネットワークの制御機能を実装する。

（ｖ）マルウェアからの保護

全てのシステムに対しマルウェアのリスクを低減するため、マルウェアからの保護対策を導入する。

（vi）多要素認証

以下の対象に対して、多要素認証を導入する。多要素認証とは、パスワード等のアカウント所有者のみが知りうるもの、身分証明書等のアカウント所有者が持つもの、生

69 サイバー衛生：平時において、社内の IT 環境や個人のコンピュータやその他デバイスの健全性を維持し、オンラインセキュリティを向上させるために行う取組み

体情報等のアカウント所有者に紐づくもののうち、2 つ以上の要素を使用してアカウント所有者を認証することを指す。

- オペレーティングシステム、データベース、アプリケーション、セキュリティ製品、ネットワーク機器にアクセスする全ての管理アカウント
- インターネットを介してアクセスする顧客サービスの全てのアカウント

(ウ) 特徴

本規制では、平時のサイバーセキュリティ対応として、「アカウント管理」、「セキュリティパッチの適用」、「セキュリティスタンダードの策定」、「ネットワーク境界の防御」、「マルウェアからの保護」、「多要素認証」の 6 つの項目への対応が具体的に示されており、規模・業態を問わず、全ての金融機関を対象に義務付けられている。

④ MAS「Technology Risk Management Guidelines」

(ア) 目的・経緯

金融機関のシステムリスクのコントロールを目的に、2013 年 6 月、MAS は「Technology Risk Management Guidelines」を策定した。本ガイドラインは、これまでの「Internet Banking and Technology Risk Management Guidelines[70]」では金融サービス業の変化に対応しきれなくなっていたことを受け、策定されたものである。対象は MAS が認可・承認・規制する全ての金融機関となっており、同月に公示された「Notice on Technology Risk Management」に沿って、さらに詳細な内容が明記されている。なお、「Notice on Technology Risk Management」には罰則が規定されているが、本ガイドラインには法的拘束力がなく、罰則は規定されていない。本ガイドラインは 2014 年 7 月より施行され、本ガイドラインに基づく MAS の検査は 2015 年より開始されている。なお、本ガイドラインは現在改定中である。（参考 1「Consultation Paper Technology Risk Management Guideline[71]」参照）

(イ) 概要

本ガイドラインでは、主に以下の内容が記載されている。また、MAS よりこの 12 項目に沿ったチェックリストが公開されており、上級管理職が毎年チェックを行うこと、またさらにその上位者が確認を行うことが求められている。チェックリストにおいて完全準拠ができていないと判断された項目は、その理由と、いつまでにどのようにして是正措置を講じるのかについて、上級管理職が上位者に対して説明する必要がある。

---

70 Internet Banking and Technology Risk Management Guidelines ： https://www.mas.gov.sg/news/media-releases/2008/mas-updates-guidelines-on-internet-banking-and-technology-risk-management

71 Consultation Paper Technology Risk Management Guideline ： https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-proposed-revisions-to-technology-risk-management-guidelines

（ｉ）システムリスクガバナンス

- 取締役会及び上級管理職は、システムリスク管理を行い、テクノロジーに関する重要な意思決定を行う
- 取締役会及び上級管理職は、システムリスクに関する内部統制、リスク管理手法の実施に対し、責任を負う
- IT セキュリティ意識向上のための訓練プログラムを策定し、年 1 回実施・更新を行う

（ii）システムリスク管理フレームワーク

A) システムリスク管理のフレームワークを、以下の要件を含めて確立する
   - システムリスクの管理における役割と責任
   - 情報システム資産の特定と優先順位付け
   - 現在および将来の脅威、リスク、脆弱性の影響と可能性の特定と評価
   - リスクを低減するための適切な措置と統制の実施
   - リスク分析に影響を与えるシステム、環境または運用状況の変更を踏まえたリスク評価の定期的な更新とモニタリング

B) 情報システム資産の保護に関する明確な方針の策定、及び情報システム資産の重要度を把握する

C) IT 環境に対するリスクを特定・評価し、リスクの種類ごとに対応策を検討する

D) リスクのモニタリング及び報告を容易にするために、リスク管理簿を作成のうえ、定期的に更新を行う

（iii）アウトソーシングリスクの管理

- 取締役会及び上級管理職は、IT アウトソーシング[72]に関連するリスクを十分に理解し、サービスプロバイダを指定する前に、デューデリジェンスを実施する
- サービスプロバイダに対しては、自社業務と同水準の厳格なセキュリティポリシー、手順、及び管理を要求する
- サービスプロバイダのセキュリティポリシー、手順、及び管理について、定期的に監視し、見直す
- サービスプロバイダに対し、災害復旧のためのコンティンジェンシープランの策定を要求する
- サービスプロバイダを含むすべての関係者は、コンティンジェンシープランの実行に関する定期的な訓練を受ける
- 現在のサービスプロバイダが業務を継続できない場合に備え、金融機関側でもサービスの中断に関する最悪のシナリオに基づいたコンティンジェンシープランを

[72] IT アウトソーシング：本ガイドラインでは、システム開発・保守、データセンターの運用、ネットワーク管理等、単一もしくは複数の外部事業者による IT 機能及び設備の提供を指す。

策定する。またコンティンジェンシープランには、他の場所で IT を利用したビジネスを再開するための実行可能な代替案を盛り込む

- クラウドサービス事業者へのデューデリジェンスを実施する場合、クラウドサービス固有の属性及びリスクを認識する
- クラウドサービス事業者が、規定された復旧時間（RTO）内にシステム及びサービスを復旧する能力があることを確認する

（ⅳ）情報システムの取得・開発

システム導入の際には、運営委員会を設置し、プロジェクトの進捗状況の監視・監督を行うべきである

（ⅴ）IT サービス管理

IT サービス管理フレームワークは、変更管理、リリース管理、インシデント管理、問題管理、キャパシティ管理のプロセス及び手順で構成する

（ⅵ）システムの信頼性・可用性・復元性

システムの復旧及び業務再開の優先順位を明確にし、業務中断を最小限に抑えるために緊急時対応手順をテストし、実践する

（ⅶ）運用インフラのセキュリティ管理

サイバー攻撃に適切に対処し、封じ込めるためには、データ、アプリケーション、データベース、オペレーティングシステム、ネットワークの各層において、セキュリティ対策を実施することが不可欠である

（ⅷ）データセンターの保護と管理

金融機関の重要なシステムやデータがデータセンターに集中し、維持されていることから、データセンターにおける内部及び外部の脅威からの回復力と物理的な安全性を確保することが重要である

（ⅸ）アクセス制御

システムを保護するための最も基本的な内部セキュリティ原則は、次の 3 つである

- 一人で実行しない - 機密性及び重要性が高い特定のシステム機能及び手順は、複数の者によって同時に実行されるか、一人の者によって実行されたとしても、他の者によってチェックされなければならない
- 職務分掌 - 職務の分掌は、内部統制の重要な要素である。金融機関は、システム運用、システム設計・開発、アプリケーション保守、アクセス制御管理、データセキュリティ、データ管理、バックアップデータファイル保管の 7 つの業務について、異なる従業員によって行われるようにする必要がある。また、セキュリティ管理部門（内）のジョブローテーションやクロストレーニングを実施することが望ましい。金融機関は、不正行為、あるいは取引内容を隠蔽することができないように、取引プロセスを設計しなければならない
- アクセス管理 - アクセス権及びシステム権限の付与は、職務上の責任と職務遂行上の必要性に基づいて行うものである。また、職位や地位に応じて、機密

データ等への不要なアクセス権を有する者がいないことを確認する。金融機関は、正当な目的のためにのみ機密情報にアクセスし、システムリソースを使用するための適切な権限をスタッフに許可しなければならない。

（ｘ）オンライン金融サービス

金融機関は、サービスプロバイダから提供されるサービスの種類に応じたリスクを明確に特定しなければならない。また金融機関は、すべてのインターネット業務について、リスクのレベルに見合ったセキュリティ対策をシステムの可用性及び復旧能力を踏まえて策定しなければならない

（xi）ペイメントカード（キャッシュカード、クレジットカード、デビットカード、その他チャージ及び支払が可能なカード）におけるセキュリティ

- ペイメントカード詐欺の種類には、偽造、紛失／盗難、カード未受領およびカード未提示詐欺がある
- ペイメントカードサービスを提供する金融機関は、ペイメントカードデータを保護するために、適切な保護措置を実施するものとする。またペイメントカードデータが暗号化されており、保存及び伝送中のデータの機密性及び完全性が確保され、機微情報又は機密情報の処理が安全な環境で行われていることを確認する
- ペイメントカードサービスを提供する金融機関は、ペイメントカードシステム及びネットワークにおいて、セキュリティ管理が実施されていることを確認する

（xii）IT 監査

- IT 監査は、IT リスクを管理するために適用されている統制の有効性について、独立した客観的な評価を取締役会及び経営層に提供する
- IT 監査機能の独立性と客観性を維持するために、IT 監査のための組織構造と報告ラインを確立しなければならない

参考1　　MAS「Consultation Paper Technology Risk Management Guideline」

(ア) 目的・経緯

昨今のサイバーリスクの顕在化を受けて、現在 MAS では「Technology Risk Management Guidelines」を改定中である。改定案では、従来のガイドラインの内容を最新化するとともに、サイバーセキュリティに関する項目が新たに追加されている。

(イ) 概要

現状のコンサルテーションペーパー（ガイドライン改定案）では、以下の主要分野に重点を置いた更新を行うことが記載されている。

（ｉ）テクノロジーリスクガバナンスと監視

金融機関の取締役会及び経営層は、テクノロジーリスクの監視及び管理において重要な役割を果たしている。提案されている改定案では、金融機関の取締役会と上級

管理職の両方に、テクノロジーリスクに関する必要なスキルと理解を持つメンバーが必要であることが明確に示されている。また、取締役会及び上級管理職の責任には、強固なリスク文化及び健全で強固なテクノロジーリスク管理の枠組みを確立することも含まれている。

（ii）ソフトウェアの開発及び管理

多くの金融機関は、迅速なソフトウェアの提供を促進するために、アジャイル開発手法と DevOps [73]プラクティスを採用している。提案されている改定案では、アジャイル開発手法を使用する際のセキュアなコーディングやコードレビュー、主要な DevOps プラクティスにおける職務分掌の実施など、セキュアなソフトウェア開発のベストプラクティスの採用を提唱している。

（iii）新技術

金融機関は、サービス提供や効率性を向上させるために、API、スマート電子デバイス、仮想化などのテクノロジーへの投資を増やしている。しかし、これらの技術が適切に実装され、管理されていない場合、サイバー攻撃の対象となる可能性がある。提案されている改定案には、このような技術から生じるリスクを管理するため、リスク管理フレームワーク、研修、監査等において、新たなリスクを意識する必要性が記載されている。

（iv）サイバーレジリエンス

金融サービスの信頼を維持するためには、強力なサイバーレジリエンスが不可欠である。本ガイドラインは、サイバーレジリエンスを強化するための緻密な防衛策をサポートするものである。今回の改定案には、サイバー監視、サイバーセキュリティ評価・テスト、サイバーインシデント管理に関する指針が含まれている。金融機関は、サイバーインシデントの識別・防御・検知・対応・復旧のためのプロセスとコントロールを確立し、継続的に強化することが重要である。

なお、現状のコンサルテーションペーパーでは、目次は以下の通りとなっている。（下線部は改定案で追加となった項目）

（i）テクノロジーリスクガバナンス
（ii）テクノロジーリスク管理フレームワーク
（iii）IT プロジェクト管理およびセキュアデザイン
（iv）ソフトウェアの開発・管理
（v）IT サービス管理
（vi）IT レジリエンス
（vii）アクセス制御

[73] DevOps：「Development（開発）」と「Operations（運用）」を掛け合わせた造語。開発チームと運用チームが協力することで、柔軟かつ迅速にシステム開発を進めること

（viii）暗号技術
（viii）運用インフラのセキュリティ
（ix）サイバー監視とセキュリティ運用
（x）サイバーセキュリティ評価
（xi）オンライン金融サービス
（xii）IT 監査

改定案で追加となった３項目では、以下のような内容が記載されている。

（viii）暗号技術

- 暗号技術の主な用途はデータの機密性の保護及びデータの完全性・真正性の維持である。金融機関は確立された国際標準規格の暗号アルゴリズムを採用しなければならない。また、使用される全ての暗号アルゴリズムが、セキュリティの目的及び要求事項を満たすために、厳格なテスト又は審査を受けていることを確認する
- 金融機関は暗号鍵が安全に生成され、保護されていることを確認する。また、データの機密性及び保護すべきシステムの重要性に基づき、各暗号鍵の有効期間を設定する

（ix）サイバー監視とセキュリティ運用

- 金融機関は、サイバー関連情報の収集・処理・分析のプロセスを確立し、金融機関のビジネス及び IT 環境への関連性及び潜在的な影響を分析する。サイバー関連情報には、サイバー攻撃事案、サイバー脅威情報、システムの脆弱性に関する情報が含まれる
- 金融機関は、不審または悪意のあるシステムの動向を確実に監視する体制を構築する。重要システムへのサイバー攻撃をリアルタイムで監視し、異常を迅速に発見することができるようにする
- 金融機関は、サイバーインシデントを迅速に切り分け、攻撃を無力化し、影響を受けたサービスを可能な限り早期に再開するために、サイバーインシデントへの対応と管理計画を策定する。計画には、サイバー攻撃のシナリオに対応するための手順を記述する。また計画は少なくとも年 1 回、見直し・更新・テストを行う。サイバーインシデントから得られた教訓は、既存の管理体制の強化やサイバーインシデント管理計画の改善に活用されるべきである

（x）サイバーセキュリティ評価

- 金融機関は、セキュリティ上の脆弱性を特定し、その脆弱性に起因するリスクに適時に対処するために、システムの脆弱性診断を定期的に実施するプロセスを確立する。脆弱性診断の頻度は、システムの重要性及びそれにさらされるセキュリティリスクに見合ったものでなければならない

・ 金融機関は、サイバーセキュリティ防御態勢の詳細な評価を得るために、ペネトレーションテストを実施する。オンライン金融サービスについては、ブラックボックステスト（評価者がテスト環境の事前情報が一切ない状態で行うテスト）とグレーボックステスト（評価者が通常の顧客と同様の認証情報を使用して行うテスト）を組み合わせて実施すべきである。金融機関は IT インフラのセキュリティをテストするため、バグ報奨金プログラムの実施を検討しても良い

・ 金融機関は、サイバーインシデントへの対応・復旧及びコミュニケーション計画の検証・見直しのため、 シナリオベースのサイバー演習を定期的に実施する。これらの演習には、ソーシャルエンジニアリング演習（フィッシング・なりすまし等を用い、パスワード等の機密情報を漏らすよう仕向ける演習）、机上演習、サイバーレンジ演習（模擬的なシステム環境を用意し、サイバー攻撃への対応を身に着ける実践的な演習）が含まれる。

(ウ) 特徴

改定案において、新たに追加された「サイバーセキュリティ評価」の項目では、バグ報奨プログラム[74]の活用について記載されており、バグ報奨プログラムを、ペネトレーションテストを補完するためのツールとして利用しても良いと記載されている。

⑤ MAS「Guidelines on Outsourcing」

(ア) 目的・経緯

本ガイドラインは、金融機関におけるアウトソーシングに関して、サービス提供の安定化、セキュリティの確保等を目的に MAS が定めたものである。2016 年 7 月に発表され、2018 年 10 月に改定が行われている。

(イ) 概要

本ガイドラインでは、主に以下のような内容が記載されている。

（ｉ）MAS がアウトソーシング契約に関して求める内容

A) 本ガイドラインの遵守、及び年次もしくは要請に応じたアウトソーシング業務登録書[75]の提出

金融機関はアウトソーシング先の本ガイドラインへの遵守状況を年一回、また適宜 MAS の要請に応じて、本ガイドラインに付属されたアウトソーシング業務登録書に基づいて示す必要がある。アウトソーシング業務登録書では、アウトソーシングするサービス・業務の内容、アウトソーシング先、アウトソーシング先の重要な顧客情報保有有無、アウトソーシング先の監査の状況・頻度、アウトソ

74 バグ報奨プログラム：自社システムの脆弱性有無について、ホワイトハッカーを活用して確認する方法で、実際にシステムへ侵入を試みてもらい、システムの脆弱性を発見した場合に報奨を提供する仕組み

75 アウトソーシング業務登録書：https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

ーシング先の業務継続計画訓練における結果等、全 26 項目の入力が求められている。

B) MAS のガイドライン遵守状況への指摘
MAS は金融機関がガイドラインを遵守していないと判断した場合、不備に対処するための追加的な措置を要求することができる。その際、金融機関の本国の規制当局やアウトソーシング先と連絡を取り合い、金融機関におけるアウトソーシングリスクの監督に協力を要請することがある

C) MAS のアウトソーシング契約に対する権限
MAS は金融機関のアウトソーシング契約内容が不十分であると判断した場合、アウトソーシング・サービスの変更や代替案の作成等を要求することができる

D) アウトソーシング契約に起因する問題に関する MAS への通知
アウトソーシング契約に起因する問題が発生した場合、可能な限り速やかに MAS に通知を行う必要がある

（ii）リスクマネジメントの実践

A) 取締役会および上級管理職の責任
金融機関の取締役会と上級管理職は、金融機関のアウトソーシングによるリスク度合を包括的に把握するための適切なプロセスがあることを確認し、そのようなリスクの評価と低減を組織のアウトソーシングリスク管理の枠組みに組み込むべきである

B) リスクの評価
金融機関の取締役会と上級管理職は、アウトソーシングによって生じるリスクを十分に認識し、理解しておく必要がある。金融機関は、以下のステップを含めたリスク評価のフレームワークを確立しなければならない。

- 組織の全体的な事業戦略と目的におけるアウトソーシングの役割を特定する
- アウトソーシングの性質、範囲、複雑性について包括的なデューデリジェンスを行い、主要なリスクを特定し、低減する
- アウトソーシング先に対し、高水準のサービス提供能力、求められる規制基準への適合について、自社と同様の水準で評価を行う
- アウトソーシングが金融機関の既存のリスクに与える影響を分析したうえで、特定されたリスクを低減するための適切な専門知識とリソースがあるかどうかを確認する
- アウトソーシングの集中リスクを管理するため、金融機関及び金融機関のグループ全体のアウトソーシング契約の総量を分析する
- サービスの一時的な中断による影響から、セキュリティや守秘義務違反、予期せぬ契約終了に至るまで、発生する可能性のあるリスクとアウトソー

シングの利点を勘案し、戦略的・内部統制上の理由から、アウトソーシング契約を締結すべきかどうかを検討する

C) サービスプロバイダの評価

アウトソーシング契約を検討・再交渉・更新する際には、適切なデューデリジェンスを実施し、 アウトソーシング契約に関連するリスクを評価しなければならない

D) アウトソーシング契約

アウトソーシング契約における契約当事者の関係、義務、責任、権利、期待を規定する契約条件は、文書化された契約書に慎重かつ適切に定義されなければならない。また、契約条件は、その合法性と執行可能性について、権限のある者（例：金融機関の顧問弁護士）によって検証されなければならない

E) 機密性とセキュリティ

金融機関は、アウトソーシング先のセキュリティに関するポリシー・手順・コントロール方法が、顧客情報の機密性と安全性を保護できていることを自ら確認する必要がある

F) 事業継続マネジメント

「Notice on Technology Risk Management」に規定されている通り、特に重要システムについては、その運用をアウトソーシングすることによって事業継続性が損なわれないようにしなければならない。また、効果的な事業継続マネジメント（BCM）を実現するためには、MAS が発行した BCM ガイドライン[76]に記載されている施策と基準を採用しなければならない

G) アウトソーシングの監視と管理

金融機関は、アウトソーシングを管理・統制するための体制を構築しなければならない。また、パフォーマンス、運用、内部統制、リスク管理の基準が守られているかどうかを確認するために、アウトソーシング先との関係をより密にする必要がある。（例：頻繁にミーティングを行う）さらに、サービスプロバイダとのアウトソーシング契約には、契約の監視・管理に関する条項が含まれていることを確認すべきである

H) 監査・検査

重要なアウトソーシング契約については、以下の条項を盛り込まなければならない。

- アウトソーシング先及びその再委託先に対して、内部監査人、外部監査人、または金融機関が任命した代理人による監査を実施し、アウトソーシング先及びその下請業者の内部監査人、外部監査人、 または金融機

[76] Guidelines on Business Continuity Management：
https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management

関が任命した代理人が作成した、アウトソーシング先及びその再委託先に対する報告書及び所見の写しを取得することを認めること

・ 必要に応じて、MAS 又は MAS が指名した代理人が金融機関の契約上の権利を行使できるようにすること

（iii）クラウドサービス

A) クラウドサービスの定義

クラウドサービスとは、アプリケーション、サーバー、ストレージ、ネットワークセキュリティなどのリソースの共有プールへのオンデマンドアクセスを可能にするビジネスと配信モデルの組み合わせである

B) クラウド技術の活用状況

多くの金融機関がクラウドサービスを採用しており、社内運用の場合もあれば、サーピスプロバイダによって運用される場合もある。また金融機関がプライベートクラウドとパブリッククラウドを組み合わせたハイブリッドクラウドを構築する傾向が強まっており、運用面とセキュリティ面のどちらを重要視するかによって、選択するクラウドモデルは異なる。多くのクラウドサービスプロバイダは、金融機関の要求に合わせ、強固な認証、アクセス制御、トークン化技術、データの暗号化を導入し、セキュリティを強化している

C) クラウドサービスと他の形態のアウトソーシングの同一性

MAS は、サービスプロバイダが運営するクラウドサービスをアウトソーシングの一形態と捉えており、金融機関はクラウドサービスを活用して業務とサービスの効率性を向上させることができると認識している。また金融機関が直面するクラウドサービスのリスクの種類は、他の形態のアウトソーシングとは異なるものではない。金融機関は、クラウドサービス を利用する際には、必要なデューデリジェンスを実施し、本ガイドラインに明記されている健全なガバナンスとリスク管理の実践を行うべきである

D) クラウドサービスの特徴とそれに応じた管理の必要性

金融機関は、マルチテナント、データの混在、複数の場所で処理が行われる傾向が高いなど、クラウドサービスの典型的な特徴を認識したうえで、リスクに対処するため、積極的な措置を講じるべきである。特にサービスプロバイダが、強力な物理的または論理的管理措置を用いて、顧客データを明確に識別し、分離する能力を有していることを保証しなければならない。サービスプロバイダは、顧客情報を保護するために強固なアクセス管理を実施しなければならない

E) クラウドサービスの活用における金融機関の責任

金融機関は、他の形態のアウトソーシングと同様に、クラウドサービスの監視を維持し、クラウドサービスの採用に伴うリスクを管理するための最終的な責任と説明責任を負う。金融機関は、監督と管理のレベルがクラウドサービスがもたら

すリスクの重要性に見合ったものであることを保証するために、 リスクベースアプローチをとるべきである

(ウ) 特徴

本ガイドラインでは、全体を通し、アウトソーシングリスクの管理方法が詳細に示されていることが特徴である。また序論において、同一の外部事業者に複数の機能を委託する場合、集中リスクにさらされる可能性があるとの記載があり、集中リスクについての認識が明確に示されている。さらに、リスク評価のフレームワークには、「集中リスクを管理するため、金融機関及び金融機関のグループ全体のアウトソーシング契約の総量を分析する」ステップを含める必要があると述べられており、アウトソーシング契約の総量分析について、指示されている。

(3) アンケート結果

シンガポールの金融機関の取組みについて、シンガポール国内のサイバーセキュリティ有識者へアンケートを実施した。なお、アンケート内容は他国と同様とした。

① サイバーセキュリティにおけるガバナンスの構築に関する取組み

一般的にチーフセキュリティオフィサーまたは同等レベルの役職を担う方がセキュリティの責任者としてサイバーセキュリティに対応している。また、サイバーセキュリティの予算は IT 総予算に組み込まれており、セキュリティ対策を単独で予算化している例は少ない。

② サイバーリスク管理に関する取組み

MAS が発出した「Technology Risk Management Guideline」に基づき、サイバーセキュリティを含む IT リスクを評価・管理している。実際には当ガイドラインを参考にしつつ、金融機関で評価軸を設定の上、評価している。

リスクの低減では、脆弱性診断およびペネトレーションテストに加え、CREST[77]が認定したベンダーが提供する TLPT の実施、セキュリティ監査の定期的な実施と多くの取組みを実施していることが伺えた。

77 CREST : https://www.crest-approved.org/index.html

## 6. 調査対象国のまとめ

### (1) 各国におけるアウトソーシングに関する比較

今回調査対象の 4 か国・地域では、アウトソーシングに関するガイドラインを発出していることから、外部委託における点検事項について、外部委託のプロセスである外部委託前、外部委託契約時、外部委託中、その他の 4 つの観点で要請事項を比較した。

調査国は共通して、金融機関にアウトソーシングポリシーなどアウトソーシングに関するリスク管理の PDCA サイクルの枠組み構築を求めている。また、構築したリスク管理の枠組みに基づき、リスク評価、契約、契約後の点検を求めている点についても共通している。

加えて、サービスプロバイダには、契約時、および契約後の定期的なデューデリジェンスのほか、SLA 等を用いた金融機関自らの監視、外部監査人等による監査等、複数の方法によりサービス提供状況を管理することが求められていた。

#### ① 外部委託前

外部委託前では各国ともアウトソーシングに関するリスク管理の枠組みの構築と、これを受けたアウトソーシングポリシー、プロセス（手順を含む）等の文書作成が求められている。

また、アウトソーシングによって発生するリスク評価の結果を受けた業務継続計画の策定や、アウトソーシングした業務の中断、停止を想定して対応を事前に検討することが求められている。

#### ② 外部委託契約時

各国共通してサービスプロバイダのデューデリジェンスを行うことが求められている。また、EU、英国、シンガポールではアウトソーシングの一覧の提出や届出が要求されている。さらに英国、シンガポールではクラウドサービスを利用する場合の、クラウドサービス固有のリスク対応やレジリエンスオプションの使用を検討すること等が求められている。

#### ③ 外部委託中

各国共通して対象の業務におけるサービスプロバイダのリスク評価を定期的に点検することとなっている。アウトソーシングに関するリスクの管理状況を把握することを目的に、サービスプロバイダのリスク評価、内部統制・セキュリティ統制等の監査の実施を求めている。

#### ④ 当局への報告要件

今回調査した文献においては、EU、英国、シンガポールでアウトソーシングに関する情報を定期もしくは要請のあった際等、都度当局に報告するよう求めている。報告を求める国では、金融機関より報告を受けたアウトソーシングに関して、当局が複数の金融機関の依存関係を確認する等を目的に取得していた。

## 7. 共助・演習の取組みの調査

### (1) 共助に向けた取組み

調査対象国において、金融機関が専門機関を通じて相互に情報共有を行う「共助」の取組みを調査した。

#### ① 主な情報共有機関と利用状況

(ア) FS-ISAC（米国）

米国を本拠とする情報共有機関であり、米国大統領令に対応して 1999 年に発足した。銀行、証券、信用組合、保険会社、投資会社等 7,000 以上の団体が参加している。また米国に加え、ロンドンおよびシンガポールに拠点を設置しており、70 以上の国・地域の金融機関にもサービスを提供している。

提供している機能は以下のとおり。

**表 10 FS-ISAC が提供する機能とその概要**

| 機能 | 提供機能の概要 |
|---|---|
| サイバー攻撃の脅威情報の共有 | 参加金融機関に脅威情報レポートを発信し、インシデント情報、脆弱性情報を提供するとともに、参加金融機関からインシデント情報を収集する。 |
| サイバーセキュリティ演習の提供 | 参加金融機関に対して、複数の種類のサイバーセキュリティ演習を提供。当局が主催する演習にも関与。 |
| サイバーセキュリティ対策に係る情報の共有 | 専門家の紹介、年次セミナーの実施、ウェブセミナーの開催等により、他社のサイバーセキュリティ対策の紹介、サイバーセキュリティ対策について対応。 |

(イ) Financial Data Exchange（FDX）（米国）

FS-ISAC の子会社として設立され、消費者のデータ保護を目的に金融機関、フィンテック企業等のアグリゲーター（データ仲介を行う事業者）との間に入り、消費者の意思に基づきデータの提供を行うプラットフォームを提供。

銀行、業界団体、金融市場インフラ、フィンテック企業等、97 の団体が参加している。

**表 11 Financial Data Exchange（FDX）が提供する機能とその概要**

| 機能 | 提供機能の概要 |
|---|---|
| サイバーセキュリティ対策の提供 | 金融機関、フィンテック企業等のアグリゲーターとの間で消費者の情報をシームレスにやり取りする API を提供。消費者は自ら提供するデータを選択できる。 |

(ウ) FSARC（米国）

米国の金融セクターを支える重要な機能の回復力を向上させ、それらを保護・防御するためのインテリジェンスを開発することを目的として設立された。

米国国土安全保障省が重要インフラの運営者として認定した主要な金融決済インフラ事業者加え、8 つの金融機関（Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, Wells Fargo）がメンバー企業として参加。

**表 12　FSARC が提供する機能とその概要**

| 機能 | 提供機能の概要 |
|---|---|
| サイバー攻撃の脅威情報の共有 | 参加する金融機関や市場の公益事業者、米国政府、その他の主要なセクターのパートナーとの間で、重要な金融セクターのシステムの分析を行い、それらのシステムに対する脅威を共同で監視し、警告する。 |

(エ) Sheltered Harbor（米国）

FS-ISAC の子会社であり、官民共同のサイバーセキュリティ演習「Hamilton Series」の結果から、情報保護に関する共通的な枠組みが必要との示唆から設立された。

サイバー攻撃により、金融機関の重要システム（バックアップを含む）に大規模な障害が発生した場合に、顧客、金融機関、そして金融システムに対する国民の信頼を守ることを目的としている。

「Deposit Accounts（預金口座）」の 72%、「Retail Brokerage Client Assets（個人向け証券口座）」の 71%がデータ保管されている[78]。

**表 13　Sheltered Harbor が提供する機能とその概要**

| 機能 | 提供機能の概要 |
|---|---|
| サイバーセキュリティ対策の提供 | 重要な顧客口座データを Sheltered Harbor の標準フォーマットでバックアップし、復旧可能なデータとして利用できるよう保管する。 |

(オ) Cross Market Operational Resilience Group(英国)

イングランド銀行、UK Finance[79] 等が共同で、「Cross Market Operational Resilience Group[80]」を構築し、官民間の情報共有を進めている。

---

78 Sheltered Harbor のシェア：https://shelteredharbor.org/images/ShelteredHarbor/Documents/ShelteredHarborAtAGlance.pdf

79 英国における金融機関の協会（https://www.ukfinance.org.uk/）

80 現時点で活動の内容、参加金融機関等は開示されていない。

**表 14　Cross Market Operational Resilience Group の機能とその概要**

| 機能 | 提供機能の概要 |
|---|---|
| サイバー攻撃の脅威情報の共有 | オペレーショナルレジリエンスを目的とした官民間の情報共有。 |

② 情報共有機関が提供している機能

調査対象国の情報共有機関の調査結果から、情報共有機関が提供する機能を分類して整理した。

(ア) サイバー攻撃の脅威情報の共有

参加金融機関や外部から収集したサイバー攻撃に関するインシデントの情報や、脆弱性に関する情報を基に作成したレポートを参加金融機関に送付している。

(イ) サイバーセキュリティ演習の提供

FS-ISAC を中心に、参加金融機関に向けた演習を提供している他、特定業界向けの演習、特定地域向けの演習、当局と連携した演習等が存在している。（詳細については「７．共助・演習の取組みの調査（２）②」を参照）

(ウ) サイバーセキュリティ対策に係る情報の共有

サイバーセキュリティ対策に係る情報を、参加金融機関に共有している。なお、有償で参加金融機関にサービス提供する形式や、有識者を参加金融機関に紹介する形式についてもこちらに含んでいる。

また、サイバーセキュリティ対策の導入や、サイバーセキュリティリスク管理に関する助言等、提供する情報はサイバーセキュリティ対策全般を含んでいる。

(エ) サイバーセキュリティ対策の提供

サイバー攻撃によるシステムの破壊や情報漏洩といったリスクを低減することを目的に金融機関等へサイバーセキュリティ対策を共同利用の方式で提供している。

本調査では、サイバー攻撃によるシステムの破壊等によるデータ消失からデータを守るため、金融機関から情報を預かり保護する対策の提供、消費者から預金等の情報を預かり保護する対策の提供が確認できた。

(2) 業界横断的な演習

我が国においても金融庁が主催する金融業界横断的なサイバーセキュリティ演習（Delta Wall）等当局が主導する演習、金融 ISAC が主催する会員合同演習（Fire）等、民間が主導する演習といった、金融機関の個々のサイバーインシデント対応を確認する演習が存在する。

調査対象国における演習の取組みを確認することを目的に、当局が主催する演習、情報共有機関が主催するその他の演習について調査した。

① 当局が主催する演習

(ア) Hamilton Series（米国）

米国財務省の主催により、FS-ISAC、FSSCC 等が共同開発した演習である。ニューヨークでは金融システムにおける重要な機関（G-SIB や G-SIFI 等）等の大規模な金融機関が参加、地域では中小金融機関が参加している。

**表 15　Hamilton Series 概要**

| 実施年 | 実施概要 | |
|---|---|---|
| 2014 年<br>～<br>2016 年 | 演習シナリオ | シナリオや実施方法は非開示 |
| | 参加金融機関 | 金融システムにおける重要な機関（G-SIB や G-SIFI 等）等の大規模な金融機関に加え、中小金融機関が参加 |
| | 実施日数 | 全 13 回各回 1 日間 |

(イ) BoE Sector Resilience Exercise（英国）

イングランド銀行は、業界横断的な演習「BoE Sector Resilience Exercise」を実施した。金融システムにおける重要な機関（G-SIB や G-SIFI 等）を対象とした、金融インフラのレジリエンスを確認することを目的とした演習である。

**表 16　BoE Sector Resilience Exercise の概要**

| 実施年 | 実施概要 | |
|---|---|---|
| 2018 年 | 演習シナリオ | 金融システムにおける重要な銀行（G-SIB）の業務停止が長引くことに起因する、参加企業と幅広いセクターへの課題と影響を確認するシナリオ<br>（想定するサイバー攻撃の内容は不明） |
| | 参加金融機関 | 金融システムにおける重要な機関（G-SIB や G-SIFI 等）、金融市場インフラ、金融当局（イングランド銀行、PRA、FCA および財務省）等の 29 の機関 |
| | 実施日数 | 1 日間 |

(ウ) Exercise Raffles（シンガポール）

MAS では、金融機関の業務継続性を確認することを目的とした、業界横断的な演習（通称 Exercise Raffles）を 2 年または 3 年に一度実施している。直近 3 回はサイバー攻撃を含むシナリオで演習を実施しており、サイバーインシデントに対するレジリエンス能力を確認する内容となっている。

**表 17 Exercise Raffles の実施概要**

| 実施年 | 実施概要 | |
|---|---|---|
| 2019 年 | 演習シナリオ | 銀行および決済サービスの混乱、取引障害、データ窃取、ソーシャルメディアでの噂や虚偽の情報拡散を含むシナリオ |
| | 参加金融機関 | 銀行、金融会社、保険会社、資産管理会社、金融ユーティリティプロバイダー、業界団体、シンガポール取引所、MAS など、140 以上の組織 |
| | 実施日数 | 2 日間 |
| 2017 年 | 演習シナリオ | テロとサイバー攻撃が同時に起こるシナリオ |
| | 参加金融機関 | 銀行、金融会社、保険会社、資産管理会社、証券会社、金融市場インフラ、業界団体、シンガポール取引所、MAS を含む 139 の機関 |
| | 実施日数 | 1 日間 |
| 2014 年 | 演習シナリオ | 金融機関のシステムの停止および取引所の注文システムのサイバー攻撃による取引停止、ATM の中断、ウェブサイトの改ざんを含むシナリオ |
| | 参加金融機関 | 銀行、金融会社、保険会社、資産運用会社、証券会社、ブローカー、シンガポール取引所、金融市場インフラ、MAS 等の 141 の機関 |
| | 実施日数 | 1 日間 |

② 情報共有機関が主催するその他の演習

(ア) Cyber-Attack Against Insurance Systems (CAIS) : FS-ISAC

保険業界向けに特化した机上演習として、二日間にわたって実施される。参加者は現在のリスク低減手順を評価、潜在的な問題点を特定し、リスク低減手順の再考を行う。

本演習は参加者の拠点で実施される。

(イ) Cyber-Attack Against Payment Systems (CAPS) : FS-ISAC

決済業界向けに特化した机上演習として、二日間にわたって実施される。決済システムに対して攻撃があったと想定し、攻撃の特定、最適な対応に関する経験を積むことができる。

本演習は各参加者の拠点で実施される。

(ウ) Cyber-Range Exercises[81] : FS-ISAC

ランサムウェアや e-mail への不正アクセス等の複数のタイプの攻撃を観察し、チームごとにそれに対する対応策の検討を行う。それぞれの対応策をチーム間でレビューし、今後の改善案について議論を行った後に同じ攻撃を受けた場合に結果が改善されるか確認する。

[81] 『5. シンガポールにおけるサイバーセキュリティ 参考 1 MAS「Consultation Paper Technology Risk Management Guideline」』に記載のサイバーレンジ演習と同様の形式の演習を指している。

本演習は 20～30 人が集合し開催されるが、遠隔地からの参加も可能である。また、本演習は世界的に行われており、様々な場所で開催されている。

(エ) Playbook Drills：FS-ISAC

FS-ISAC が作成した「Financial Sector Crisis Response Framework」を基に、特定の地域に限定し、地域内での情報共有および危機対応を構築することを目的としている。

本演習は様々な場所で開催される。

(オ) Regional Exercises and Workshops：FS-ISAC

地域、規模、組織のセグメント等に応じた特有のリスクを対象とし、参加者の優先事項に応じて組み立てられる演習。

③ 業界横断的な演習の特徴

当局に加え、情報共有機関においても、対象とする金融機関の規模・数、目的や演習のシナリオが異なるさまざまな演習を実施している。

これらの演習について、シナリオの観点からみると、金融機関個々のシステムを対象としたシナリオに加え、金融インフラまたは特定の業界を対象としたシナリオを実施していることが確認できた。金融機関個々のシステムを対象とした場合、個別金融機関が策定しているコンティンジェンシープランおよび業務継続計画の見直しに寄与できるものと考えられる。例えば、FS-ISAC が提供する演習では、個別金融機関のサイバーレジリエンスを確認することが目的となっている演習が多い。

金融インフラまたは特定の業界を対象とした場合、個別金融機関のコンティンジェンシープランおよび業務継続計画の見直しにとどまらず、業界全体のサイバーレジリエンス能力の確認、ひいては国全体の金融安定への影響の確認が期待できるものと考えられる。例えば、当局が主催する演習では、金融インフラ事業者、G-SIBs 等が参加しており、金融セクター全体のサイバーレジリエンスの確認にフォーカスされていることが伺える。

## 8. 本調査を踏まえた考察

### (1) 調査対象国における取組みからの示唆

今回の調査においては、調査対象国ごとの規制・ガイドラインの特徴を確認した。米国においては、アセスメントツールである、「Cybersecurity Framework」及び「Cybersecurity Assessment Tool」が存在し、これらは米国金融機関のみならず国際的に活動する金融機関のサイバーセキュリティの基礎となっている。金融機関における情報システムの利用状況に応じて、対応すべきセキュリティレベルに即した対策ができているかを網羅的に評価し、金融機関が課題を把握するのに効果的であると考えられる。このように米国においては、アセスメントツールを活用しつつ、金融機関自ら課題を見出してサイバーセキュリティ対策を進めていることに特徴がある。我が国金融機関にとっても、サイバーセキュリティ対策の更なる高度化を図る観点から、こうした評価ツールを活用しつつ、取組みを進めることが考えられる[82]。

また、脆弱性診断、ペネトレーションテスト、TLPT についても、サイバーセキュリティ対策の実効性を確保するために重要な取組みであり、各国の規制・ガイドラインにおいて記載されている[83]。我が国においても、金融機関が継続的にサイバーセキュリティの実効性を確保し高度化を進めるにあたって、脆弱性診断、ペネトレーションテスト、TLPT の活用を継続的に進めていくことが重要である。

さらに、最近の動向として、英国においてオペレーショナルレジリエンスに関するガイドラインが策定・公表されるなど、国際的にオペレーショナルレジリエンスの議論が高まりを見せている。サイバー攻撃は日々巧妙化、高度化されておりインシデントの発生を完全に防ぐことは難しい。業務継続の観点から、金融機関がオペレーショナルレジリエンスを確保し、サイバー攻撃の影響を緩和し、的確に対応できるような取組みが進むことが望ましい。

### (2) サードパーティリスクへの対応

サードパーティリスクについては、国際的にもさまざまな場において議論がなされており、調査対象国においてもガイドラインにより、金融機関のアウトソーシングに関する枠組みやルールを定め、集中リスクを含めたリスク評価等が求められていた。

アウトソーシング先のリスク評価では、契約時におけるデューデリジェンスに加え、契約後の定期的なデューデリジェンス、SLA の遵守状況等のサービス提供状況の監視、外部監査人等を活用した監査等、複数のタイミング及び視点による評価が求められていた。

我が国金融機関においても、クラウドサービスや Fintech 事業者等、外部のサービスの活用が進んでいるため、アウトソーシング先のリスクを適切に評価・管理していくことが重要である。

---

82 すでに大手金融機関の一部では、「Cybersecurity Assessment Tool」を活用した取組みが進められている。

83 例えば、EU および英国では TLPT のフレームワークが導入されている。また、シンガポールにおいては、脆弱性診断、ペネトレーションテストの実施が求められている。

(3) 共助に関する取組みの進展

共助に関する取組みを調査した結果、単に脅威情報の共有にとどまらず、演習の実施、サイバーセキュリティ対策に関する情報提供、サイバーセキュリティ対策の提供等、複数の組織において、さまざまな共助の取組みが進展していた。

我が国においては脅威情報の共有に加え、演習の実施、サイバーセキュリティ対策に関する情報、知見共有等の共助の取組みが金融 ISAC を中心に進められてきている。サイバーセキュリティ対策の提供についても、業界団体を含めた関係者による今後の検討が期待される。

(4) 業界横断的なサイバーセキュリティ演習の活用

演習の調査結果からは、金融機関の個々への攻撃を想定した演習に限らず、特定の業態・地域、決済サービス等の金融インフラ全体への攻撃を想定した演習も実施されていた。

我が国においても、金融庁が主催する金融業界横断的なサイバーセキュリティ演習をはじめ、複数のサイバーセキュリティ演習が行われている。金融機関においては、目的に応じた演習への参加を通じて、サイバーインシデントへの対応能力を高めることが重要である。現時点では個々の金融機関のインシデント対応を確認する演習が中心であるが、今後は、金融分野全体への影響を想定した演習、特定の業態内への影響を想定した演習等、業界におけるサイバーレジリエンスを確認する演習も有効となろう。

A) 参考文献

| 脚注番号 | 文書 | 出所 |
|---|---|---|
| 1 | 諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書（2015年3月31日） | https://www.fsa.go.jp/common/about/research/20150706-4/01.pdf |
| 2 | Cybersecurity Framework | https://www.nist.gov/cyberframework |
| 3 | IT Handbook Information Security | https://ithandbook.ffiec.gov/it-booklets/information-security.aspx |
| 4 | IT Handbook Outsourcing Technology Services | https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx |
| 5 | Cybersecurity Assessment Tool | https://www.ffiec.gov/cyberassessmenttool.htm |
| 6 | Cybersecurity Profile | https://fsscc.org/Financial-Sector-Cybersecurity-Profile |
| 7 | Cybersecurity Capacity-building Tool Box for Financial Organizations | https://carnegieendowment.org/specialprojects/fincyber/guides |
| 8 | Cybersecurity Enhancement Act | https://www.congress.gov/bill/113th-congress/senate-bill/1353/text |
| 9 | 情報処理推進機構 セキュリティ関連NIST文書「Cybersecurity Framework」 | https://www.ipa.go.jp/files/000071204.pdf |
| 10 | 『FFIEC Cybersecurity Assessment Toolに関する調査研究』調査報告書（2016年3月31日） | https://www.fsa.go.jp/common/about/research/20160815-1.html |
| 11 | FS-ISAC | - |
| 12 | NIS Directive | https://eur-lex.europa.eu/eli/dir/2016/1148/oj |
| 13 | Cybersecurity Act | https://eur-lex.europa.eu/eli/reg/2019/881/oj |
| 14 | Cybersecurity Act | https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act |
| 15 | TIBER-EU | https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf |
| 16 | Guidelines on ICT and security risk management | https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20IC |

| 脚注番号 | 文書 | 出所 |
|---|---|---|
| | | T%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf |
| 17 | Guidelines on outsourcing arrangements | https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.pdf/38c80601-f5d7-4855-8ba3-702423665479 |
| 18 | Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013.2.7 P3 | http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_directive_en.pdf |
| 19 | NIS Directive 第 1 条第 1 項 | https://eur-lex.europa.eu/eli/dir/2016/1148/oj |
| 20 | NIS Directive 第 14 条 | https://eur-lex.europa.eu/eli/dir/2016/1148/oj |
| 21 | Cybersecurity Act 前文(4) | https://eur-lex.europa.eu/eli/dir/2016/1148/oj |
| 22 | Cybersecurity Act 第 1 条 | https://eur-lex.europa.eu/eli/dir/2016/1148/oj |
| 23 | サイバーセキュリティ認証制度 | - |
| 24 | Cybersecurity Act 第Ⅱ章 | https://eur-lex.europa.eu/eli/dir/2016/1148/oj |
| 25 | 諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書 | https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf |
| 26 | TIBER-EU | https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html |
| 27 | What is the Eurosystem's cyber resilience strategy? | https://www.ecb.europa.eu/paym/intro/events/shared/pdf/fs07/ecb_focus_session_20180917_cyber.pdf |
| 28 | ECB のプレスリリース | https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html |

| 脚注番号 | 文書 | 出所 |
|---|---|---|
| 29 | TIBER-NL | https://www.dnb.nl/en/news/nieuwsbrief-betalingsverkeer/Juni2018/index.jsp |
| 30 | TIBER-BE | https://www.nbb.be/en/payments-and-securities/tiber-be-framework |
| 31 | TIBER-DK | http://www.nationalbanken.dk/en/financialstability/Operational/Pages/TIBER-DK-and-implementation-guide.aspx |
| 32 | Nationnal Bank of Romania | https://www.bnr.ro/DocumentInformation.aspx?idDocument=32161&directLink=1 |
| 33 | TIBER-DE | https://www.bundesbank.de/en/tasks/payment-systems/services/tiber-de/tiber-de-817014 |
| 34 | TIBER-IE | https://centralbank.ie/financial-system/tiber-ie |
| 35 | TIBER-SE | https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2019/the-riksbank-coordinates-cybersecurity-tests/ |
| 36 | TIBER-IT | https://www.bancaditalia.it/media/comunicati/documenti/2020-01/cS_BIConsob_20200116_ENG.pdf?language_id=1 |
| 37 | TIBER-FI | https://www.suomenpankki.fi/en/money-and-payments/tiber-fi-implementation-guideline/ |
| 38 | TIBER-NO | https://www.norges-bank.no/en/news-events/news-publications/Press-releases/2020/2020-05-14-tiber/ |
| 39 | TIBER-EU FRAMEWORK P7 | https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf |
| 40 | TIBER-EU FRAMEWORK P20-21 | https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf |
| 41 | Guidelines on ICT and security risk management P6 | https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guid |

| 脚注番号 | 文書 | 出所 |
|---|---|---|
| | | elines%20on%20ICT%20and%20security%20risk%20management.pdf |
| 42 | Guidelines on ICT and security risk management | https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management |
| 43 | リスクアペタイト | - |
| 44 | Guidelines on outsourcing arrangements | https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf |
| 45 | 『重要な機能』 | - |
| 46 | ステップインリスク | - |
| 47 | 英国のサイバーセキュリティ関係当局に関する補足 | - |
| 48 | PRA Rulebook に関する補足 | - |
| 49 | FCA Handbook | https://www.handbook.fca.org.uk/handbook |
| 50 | CBEST | https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf |
| 51 | Cyber Resillience Questionnare | https://www.fca.org.uk/firms/cyber-resilience |
| 52 | Building operational resilience:Impact tolerances for important business services | https://www.bankofengland.co.uk/news/2019/december/building-operational-resilience-impact-tolerances-for-import-business-services |
| 53 | Outsourcing and third party risk management | https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management |
| 54 | FCA Handbook High Level Standards の章 | https://www.handbook.fca.org.uk/handbook/SYSC/3/?view=chapter |
| 55 | FCA Handbook Regulatory Processes の章 | https://www.handbook.fca.org.uk/handbook/SUP/10C/?view=chapter |

| 脚注番号 | 文書 | 出所 |
|---|---|---|
| 56 | 諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書 | https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf |
| 57 | Non Directive Firms（NDFs） | - |
| 58 | クラウドのレジリエンスオプション | - |
| 59 | ISO27000 シリーズ | - |
| 60 | ISO27004 | https://isms.jp/chumon.html |
| 61 | CRISC | - |
| 62 | CYBERSECURITY ACT | https://sso.agc.gov.sg/Acts-Supp/9-2018/ |
| 63 | Notice on Technology Risk Management | https://www.mas.gov.sg/regulation/notices/notice-cmg-n02 |
| 64 | Notice on Cyber Hygiene | https://www.mas.gov.sg/regulation/notices/notice-655 |
| 65 | Technology Risk Management Guidelines | https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines |
| 66 | Consultation Paper Technology Risk Management Guideline | https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-proposed-revisions-to-technology-risk-management-guidelines |
| 67 | Guidelines on Outsourcing | https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing |
| 68 | 重要インフラ事業者 | - |
| 69 | サイバー衛生 | - |
| 70 | Internet Banking and Technology Risk Management Guidelines | https://www.mas.gov.sg/news/media-releases/2008/mas-updates-guidelines-on-internet-banking-and-technology-risk-management |
| 71 | Consultation Paper Technology Risk Management Guideline | https://www.mas.gov.sg/publications/consultations/2019/consultation-paper-on-proposed-revisions-to-technology-risk-management-guidelines |
| 72 | IT アウトソーシング | - |
| 73 | DevOps | - |
| 74 | バグ報奨プログラム | - |
| 75 | アウトソーシング業務登録書 | https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing |

| 脚注番号 | 文書 | 出所 |
|---|---|---|
| 76 | Guidelines on Business Continuity Management | https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management |
| 77 | CREST | https://www.crest-approved.org/index.html |
| 78 | Sheltered Harbor のシェア | https://shelteredharbor.org/images/ShelteredHarbor/Documents/ShelteredHarborAtAGlance.pdf |
| 79 | UK Finance | https://www.ukfinance.org.uk/ |
| 80 | Cross Market Operational Resilience Group | - |
| 81 | Cyber-Range Exercises | - |
| 82 | アセスメントツールの活用状況 | - |
| 83 | 脆弱性診断、ペネトレーションテスト、TLPT の利用状況 | - |
| 84 | National Cyber Security Centre（国家サイバーセキュリティセンター） | - |

B) Cyber Resilience Questionnaire の点検項目

| 分野 | 項目 |
|---|---|
| ガバナンスとリーダーシップ | 1.サイバーセキュリティ戦略の策定とその承認者に関する要件 |
| | 2.サイバーセキュリティ戦略を実現するための文書化されたフレームワーク（ポリシー、標準、マニュアルを含む）の策定状況 |
| | 3.サイバーセキュリティフレームワークの提供について、責任を負う上級管理職（Senior Management）の任命状況 |
| | 4.サイバーセキュリティリスク管理の位置づけ（全社のリスクとして管理されているか） |
| | 5.サイバーコントロール（技術的対策）の有効性についての評価実施状況（誰が実施するか、実施の頻度） |
| | 6.上級管理職の知識、スキルレベル |
| | 7.上級管理職による「金融機関全体のサイバーセキュリティ戦略における役割、アカウンタビリティ、責任」の定義状況 |
| | 8.意思決定を行うための定期的な議論における、リスクに関する KPI を含む管理情報の活用状況 |
| | 9.インシデント対応能力の検証による、サイバーセキュリティフレームワークを改善する仕組みの有無 |
| 識別 | 10.ビジネスの重要性とシステムの利用状況を踏まえた、システムの優先順位の定期的なレビュー状況およびリスク評価の見直し状況 |
| | 11.情報資産管理台帳の整備状況、および情報資産管理台帳へのリスク評価結果の反映状況 |
| | 12.サードパーティとサードパーティの提供サービスとの紐づけの管理、管理プロセスの整備状況 |
| | 13.ハードウェア、ソフトウェアの脆弱性の把握状況、脆弱性検出プロセスの整備状況 |
| | 14.ハードウェア、ソフトウェアの保守期限を管理し、保守期限前までに対象のハードウェア、ソフトウェアを特定可能な管理プロセスの整備状況 |
| | 15.外部インタフェース一覧（利用する通信の、接続先、接続要件、プロトコル等を一覧化したもの）の整理および文書化の状況 |
| 保護 | 16.社内ネットワークへのリモートアクセスにおける強力な認証の仕組みの採用有無 |
| | 17.データへのアクセスの許可方針（データ所有者の許可） |
| | 18.データへのアクセス許可状況の管理（許可された運用でのアクセス状況） |
| | 19.特権 ID の一元的な管理、文書化の状況（特権 ID の作成、移動、削除の管理） |

| 分野 | 項目 |
| --- | --- |
| 保護 | 20.ポリシーに従った情報資産とドキュメントに対する情報種別の付与状況 |
| | 21.機密データの外部流出を防止するツールの導入および機密データの管理プロセスの整備状況 |
| | 22.バックアップおよび暗号化の実施状況 |
| | 23.サードパーティのセキュリティ機能、サイバーセキュリティを評価するためのプロセス（マニュアル）の整備状況 |
| | 24.サードパーティのインフラストラクチャーおよび情報へのアクセス権の管理状況。サービスプロバイダへの定期的なデューデリジェンスの実施有無 |
| | 25.ビジネスおよびシステムの変更時におけるサイバーセキュリティの遵守状況 |
| | 26.オペレーションシステム、データベース、アプリケーション、デバイス等において、ベースラインとなるシステムセキュリティ構成の標準化・手順の整理状況 |
| | 27.ネットワークトラフィック監視の導入状況 |
| | 28.外部ネットワークからの侵入に対する多層化防御実施状況 |
| | 29.スタッフの教育状況 |
| | 30.高リスクのスタッフの特定、高リスクスタッフ向けのトレーニングの提供有無<br>※高リスクのスタッフとは、特権 ID を管理する従業員を指す。 |
| | 31.採用時のスクリーニング、バックグラウンドチェックの実施有無 |
| | 32.物理的なアクセス制御の実施、定期的なレビューの実施<br>※物理的なアクセス制御とは、データセンター、サーバー、端末等の物理的な情報資産の保護のことを指している |
| 検出 | 33.異常な活動やイベントの監視、検出機能の導入状況 |
| | 34.リモートアクセスで行われる悪意のあるアクティビティの検知、アラート機能の導入状況 |
| | 35.企業内ネットワーク上の不正な接続、デバイスの検知機能の導入状況、および、監視担当者への通知機能の有無 |
| | 36.既知の脆弱性に対する対応プロセスの整備状況 |
| | 37.ペネトレーションテストの実施状況 |
| | 38.監視システムとインシデント対応プロセスとの紐づけ |
| | 39.サイバー脅威に関する情報収集、分析、共有プロセスの整備状況 |
| | 40.サイバーセキュリティインテリジェンス情報の活用による、サイバーセキュリティ戦略、フレームワークの改善状況 |
| 応答 | 41.インシデント対応計画への外部連携（顧客、サードパーティ、当局、報道機関等）の有無 |
| | 42.当局、ステークホルダーへの報告を含むインシデント対応手順の有無 |

| 分野 | 項目 |
| --- | --- |
| 応答 | 43.CiSP 等へのインシデント情報、攻撃予告の共有状況<br>※CiSP：サイバーセキュリティ情報共有パートナーシップ（NCSC[84]が中心となる情報共有の枠組み） |
| | 44.セキュリティイベント、インシデントが発生した際の対応を判断する、しきい値の設定有無 |
| | 45.セキュリティイベント、インシデント発生後の調査プロセスの整備状況 |
| 回復 | 46.インシデント後のシステムへのデータ復旧プロセスの有無 |
| | 47.サイバーセキュリティインシデント後の改善を実施するプロセスの有無 |
| | 48.重要なサービスプロバイダと連携した復旧計画の有無<br>※システムを内製化している海外金融機関の場合は、厳密にサービスプロバイダと自社との役割分担を明確にしたうえで、検証（テスト）を実施する必要あり |

以 上

[84] National Cyber Security Centre（国家サイバーセキュリティセンター）