金融資本市場における当局・金融機関による サイバーリスクへの対処

門倉　朋美、江夏　あかね

▌要　約▐

1. 金融機関は大量の機密情報や取引を取り扱うことから、サイバー攻撃の標的になることが多いと指摘されている。金融資本市場、特に証券市場は資金の効率的な配分や利用を促す機能を担っており、特定の市場や証券会社等の金融機関に対するサイバー攻撃の被害は甚大になり得ることが想定される。
2. 金融セクターの国際的な枠組みにおいては、金融安定理事会（FSB）や証券監督者国際機構（IOSCO）等が各国の金融当局や金融機関等を対象としたサイバー・レジリエンスの強化を図る施策を推進している。
3. 一方、各国金融当局は自国の金融機関に対してサイバーセキュリティの確保に資する取り組みを推進している。日米金融当局による近年の主な施策として、米国証券取引委員会（SEC）による証券市場関連組織に対する規制強化と日本の金融庁による金融機関に対するセルフアセスメントの促進が挙げられる。
4. 今後、日本の金融資本市場や金融機関がサイバーリスクの脅威に対応し、健全な発展を遂げるためには、（1）海外当局の動向の把握、（2）金融機関のサイバーセキュリティリスク評価の普及、が重要になると考えられる。

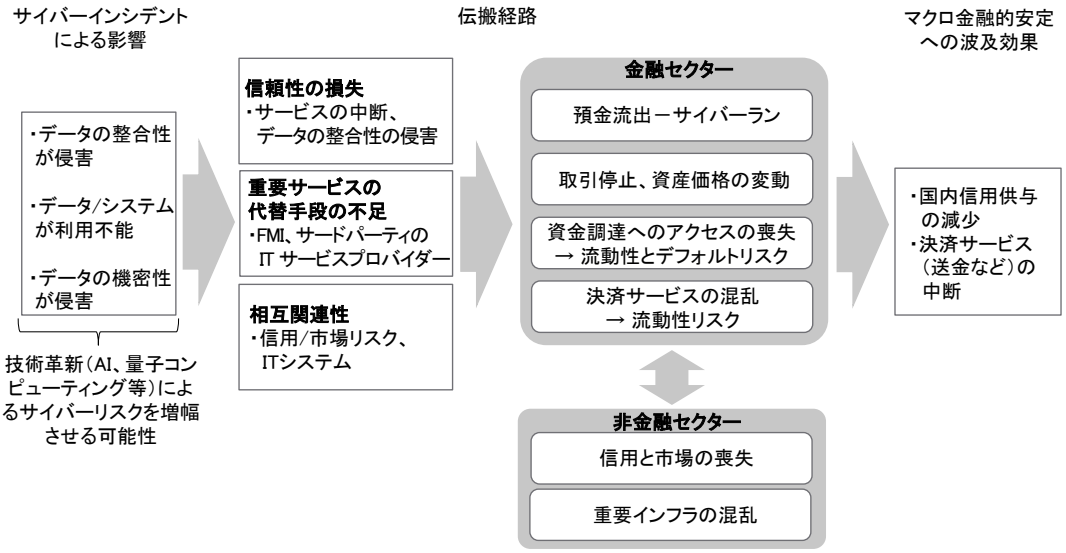
野村資本市場研究所　関連論文等

・門倉朋美・江夏あかね「金融機関に求められるサイバーセキュリティ対応－日米金融当局・国際機関の動向－」『野村サステナビリティクォータリー』2024年冬号。
・関根栄一・宋良也「中国証券業におけるサイバーセキュリティの強化に向けた動き」『野村サステナビリティクォータリー』2024年冬号。

Ⅰ サイバーリスクに晒される金融セクター

金融機関は大量の機密情報や取引を取り扱うことから、サイバー攻撃の標的になることが多いと指摘されている[1]。国際通貨基金（IMF）の「国際金融安定性報告書」によると、2004 年から 2023 年にかけて発生した世界のサイバーインシデントのうち、約 2 割が金融セクターに影響を及ぼした[2]。金融機関は金融資産の仲介、リスクの移転、決済等の機能を有し、金融資本市場を通じてあらゆるセクターの事業者及び個人と密接な関係にあることから、サイバー攻撃による影響は甚大なものになり得る。同報告書では、金融機関のサイバーインシデント発生からマクロ面での金融安定性に影響を及ぼすまでの伝搬経路を示している（図表 1 参照）。金融セクターでは、サイバーインシデントに伴う影響によって信頼性の損失、重要サービスの代替手段の不足、相互関連性の 3 つの要因によって預金流出や取引停止による資産価格の変動、決済サービスの混乱等に発展し得ると指摘された。さらに、その結果として信用供与の減少、決済サービスの中断等のマクロ面での金融安定性に影響を及ぼす可能性が指摘された。

図表 1　サイバーリスクがマクロ面での金融安定性に影響を及ぼす伝搬経路



（注）　AI は人工知能、FMI は金融市場インフラストラクチャー、IT は情報技術、サイバーランはサイバーインシデントに伴う預金引き出しや銀行への取り付け騒ぎを指す。

（出所）International Monetary Fund, “Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks,” April 2024 より野村資本市場研究所作成

1　International Monetary Fund, “Rising Cyber Threats Pose Serious Concerns for Financial Stability,” April 9, 2024.

2　International Monetary Fund, “Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks,” April 2024.

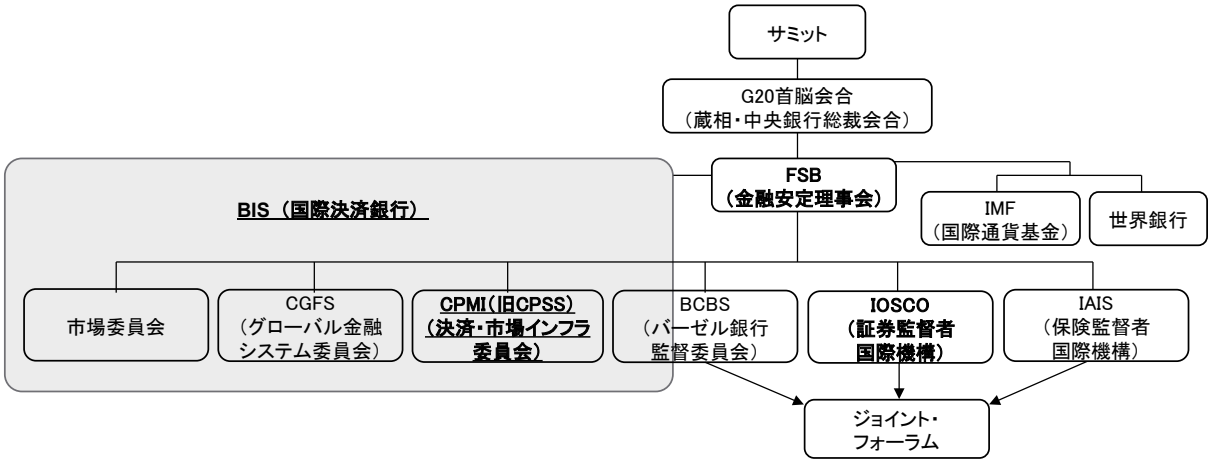
金融資本市場、特に証券市場は資金の効率的な配分や利用を促す機能を担っており、個人投資家から発行体までさまざまなステークホルダーが参加する。そのため、特定の市場や証券会社等の金融機関に対するサイバー攻撃の被害は甚大になり得ることが想定される。また、サイバー空間は必ずしも国境が明確でないことから、国を越えた連携がカギとなる。金融セクターの国際的な枠組みにおいては、加盟国の金融当局や金融機関に対してサイバー・レジリエンス強化に向けた施策等が示されている。一方、各国金融当局は自国の金融機関に対して、サイバーセキュリティの確保に資する規制強化やセルフアセスメントのツール等を提供している。

本稿では、金融安定理事会（FSB）や証券監督者国際機構（IOSCO）といった国際的な枠組みや、日米の金融規制当局によるサイバーリスクへの対応を概観した上で、日本の金融資本市場や金融機関がサイバーリスクの脅威に対応し、健全な発展を遂げるための論点を考察する[3]。

Ⅱ　国際的枠組みにおける金融安定への取り組み

金融セクターの国際的な協調を図る枠組みとして、G20の下に設置されたFSBや基準策定主体（SSB）等が挙げられる（図表2参照）。以下では、FSBと、証券分野のSSBであるIOSCOの取り組みを概観する。

図表2　金融規制を策定する主な国際会議



（出所）宮内惇至「講演 国際的な金融規制改革を見直す動き：プロシクリカリティ対策を踏まえて」『リスクと保険』第14号、日本保険・年金リスク学会、2018年3月より野村資本市場研究所作成

[3] FSBはサイバーリスクを「サイバーインシデントの発生確率及びその影響の組み合わせ」と定義する（Financial Stability Board, “Cyber Lexicon Updated in 2023,” April 13, 2023）。

１．FSB：サイバーインシデント報告の共通化

FSBは、25の国・地域の中央銀行、金融監督局、SSB等が参加する国際機関であり、国際的な金融安定の促進を図ることを目的として、各組織による政策の策定において調整を行う。サイバー攻撃はオペレーショナル・レジリエンスの混乱を招き得る要因の一つであることから、FSB は 2017 年頃より各国の金融当局や金融機関等を対象としたサイバー・レジリエンスの強化を図る施策を推進している[4]。本節では、近年の取り組みとしてサイバーインシデント報告の共通化に向けた施策を取り上げる。

FSBは2023年4月、サイバーインシデント報告（Cyber Incident Reporting、CIR）の共通化を促進する一連の施策を公表した。サイバーインシデントの適時かつ正確な情報がサイバーインシデントの初動と回復（Cyber Incident Response and Recovery、CIRR）及び金融安定の向上において重要であることを踏まえたG20によるFSBへの要請に対応したもので、一連の施策は主に3つのパートに大別される[5]。特に、2022年10月の市中協議を経て公表された最終報告書「サイバーインシデント報告の更なる収斂に向けた提案」は、金融機関にサイバー攻撃があった場合の対応を迅速化し、金融システムへの影響を抑制することを目的として、サイバーインシデント報告のベストプラクティスを示すものである[6]。FSBは、サイバーインシデント情報を収集・利用する上での金融当局・金融機関が直面する課題を指摘し、当該課題に対処するための 16 項目の提案が各課題に対してどの程度の効果をたらすかを照らし合わせたマッピングを提示している（図表 3 参照）。FSB は画一的なアプローチは望ましくないと認識しつつも、各国の金融当局及び金融機関が自国の法規制上の枠組みに沿って、適切かつ関連性のある場合に各提案を採用できるように整備している。

なお、FSBが2023年12月に公表した「サードパーティリスク管理とオーバーサイトの強化：金融機関及び金融当局向けのツールキット」では、上述のサイバーインシデント報告のさらなる強化の必要性を示唆している[7]。当該ツールキットは必ずしもサイバーリスクに焦点を据えていないものの、金融当局に対するインシデント報告について、「インシデントが金融の安定性に潜在的なリスクをもたらす可能性がある場合にサービス・プロバイダーによる報告を含めるよう、既存のサイバー報告フレームワークを強化する可能性を含む」としている。

---

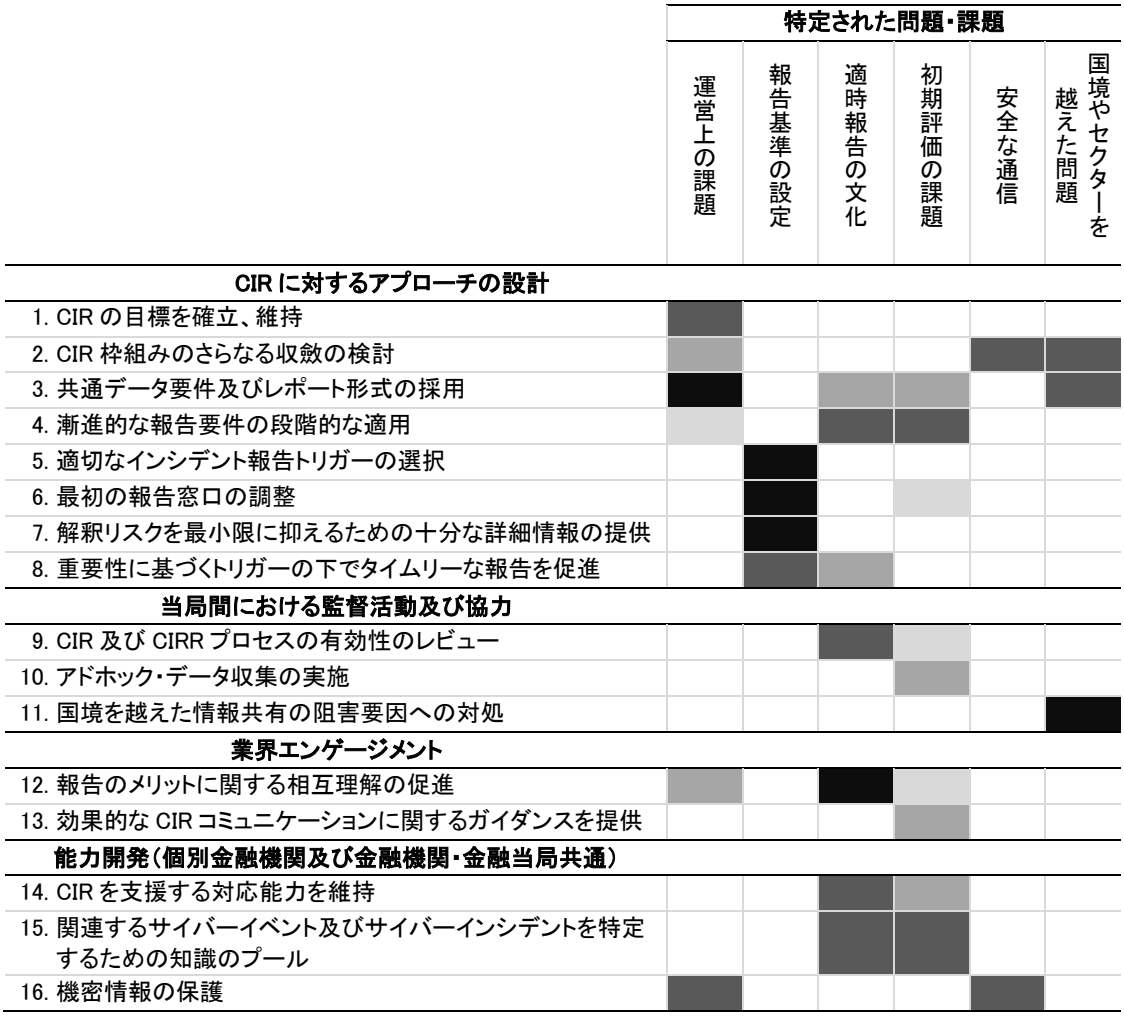
4 FSBはサイバー・レジリエンスを「サイバー脅威やその他の関連する環境の変化を予測して適応し、サイバーインシデントに耐え、封じ込め、迅速な回復により、組織がミッションを遂行し続ける能力」と定義する（Financial Stability Board, “Cyber Lexicon Updated in 2023, ” April 13, 2023）。

5 主な施策としては、①サイバーインシデント報告の更なる収斂に向けた提案に関する報告書の公表、②金融セクターにおけるサイバー関連用語の定義を示す「サイバー用語集」の 2023 年改訂版の公表、③インシデント報告交換フォーマット（FIRE）の今後の方針を示す報告書の公表、が挙げられる。

6 Financial Stability Board, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report,” April 13, 2023.

7 Financial Stability Board, “Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities,” December 4, 2023.

図表 3　FSB による提案の一覧と各課題に対する効果



（注）　なし　軽度　中度　重度　最重度

（出所）Financial Stability Board, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report,” April 13, 2023 より野村資本市場研究所作成

２．IOSCO：FMI のサイバー・レジリエンス強化

SSB は各金融セクターにおいて、規制対象の金融機関に対してサイバー・レジリエンス強化に向けた施策を推進している。近年は、特定の金融市場インフラ（FMI）がシステム障害を起こす事案が発生しており、サイバー攻撃に起因するものに限らないが、金融機関の中でも決済システムや清算機関等の FMI に対するサイバー・レジリエンスの強化は金融システムの安定を確保する上でも重要となっている。SSB の中で、FMI が遵守すべき原則の「金融市場インフラのための原則（FMI 原則）」を定めているものとしては、IOSCO 及び国際決済銀行（BIS）傘下の決済・市場インフラ委員会（CPMI）が挙げられる[8]。両者は 2016 年 6 月、「金融市場インフラのためのサイバー・レジリエンスに係るガイダンス

[8] IOSCO は、各国・地域の証券監督当局や証券取引所等が加盟する、証券分野の国際的な基準設定主体である。CPMI は、各中央銀行の支払決済システム等を担当する幹部により構成される基準設定主体である。

（サイバーガイダンス）」を公表した[9]。同ガイダンスは FMI 原則におけるサイバーセキュリティ関連の原則の明確化を図ることを目的としており、サイバー・レジリエンス強化に向けて FMI が考慮すべき要素を明示している（図表 4 参照）。

図表 4　サイバーガイダンスにおけるサイバー・レジリエンス強化に向けた要素

主要なリスク管理要素		概要
	ガバナンス	経営陣の役割明確化等を通じた適切な枠組みの策定
	特定	保護すべきデータ･機能の種類の洗い出し
	防御	組織的なセキュリティ態勢の構築
	検知	包括的･継続的なモニタリングによる攻撃の予兆等の早期発見
	対応と復旧	危機対応計画（コンティンジェンシー･プラン）の策定等による対応態勢の構築
リスク管理を効果的に機能させるための要素		概要
	テスト	ストレステストや点検プログラムによる対策の十分性点検
	状況認識	潜在的なサイバー攻撃にかかる情報収集、理解深耕
	学習と進化	内外の事象や最新のリスク管理手法のモニタリング、自身のシステムへの適用

（出所）日本銀行「決済システムレポート」2019 年 3 月より野村資本市場研究所作成

なお、IOSCO による直近の動きとしては、2024 年 6 月に「株式市場の機能停止に関する最終報告書」を公表したことが挙げられる[10]。同報告書は、市場のレジリエンスと投資家の信頼確保に向けて、当局や証券取引所、市場参加者における市場の機能停止への備え、管理、レジリエンスの向上に役立つグッド・プラクティスを共有するものである。同報告書においては、2018 年から 2022 年にかけて発生した市場の機能停止は、サイバー攻撃が要因ではなかったものの、近年の情勢を踏まえると、サイバー攻撃が起きた場合、市場が長期停止し兼ねないといった可能性を指摘した。

Ⅲ　日米金融当局によるサイバーリスクへの対応

日米の金融当局は近年、金融機関のサイバーセキュリティ関連の取り組みを重層的に展開している（図表 5 参照）。本章では、日米金融当局による近年の主な施策として、米国証券取引委員会（SEC）による証券市場関連組織に対する規制強化と日本の金融庁による金融機関に対するセルフアセスメントの促進を概論する。

[9] Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, “Guidance on Cyber Resilience for Financial Market Infrastructures,” June 2016.

[10] Board of the International Organization of Securities Commissions, “Market Outage Final Report,” June 2024.

図表 5　米日の主なサイバーセキュリティ関連施策の動向

暦年	米国の概要
2008	サイバーセキュリティ戦略の枠組みである「包括的全米サイバーセキュリティ・イニシアティブ（CNCI）」発出
2011	SEC の企業財務局、サイバーセキュリティリスク及びサイバーインシデントに関する開示の在り方に関するガイダンスを公表
2018	SEC、2011 年に公表した開示の在り方に関するガイダンスの解釈指針を公表
	「2018 年サイバーセキュリティ・社会基盤安全保障庁設置法（CISA 法）」成立
2021	サイバーセキュリティ強化のための大統領令、発令
2022	「2022 年重要インフラに関するサイバーインシデント報告法（CIRCIA）」成立
2023	SEC、米国証券市場における特定関連組織に対してサイバーセキュリティリスクに対処することを義務付ける 3 つの規則案を公表
	SEC、SEC 登録企業を対象にサイバーセキュリティ関連の開示を義務付ける新たな規則を採択
2024	SEC、金融機関におけるデータプライバシーと顧客情報保護を目的として、レギュレーション S-P の規則案を採択
暦年	日本の概要
2014	サイバーセキュリティ基本法、成立
2015	内閣に「サイバーセキュリティ戦略本部」、内閣官房に「内閣サイバーセキュリティセンター（NISC）」が設置
	金融庁、「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 1.0）」を公表（2018 年 10 月に Ver. 2.0、2022 年 2 月に Ver. 3.0 を公表）
2016	金融庁、金融業界横断的なサイバーセキュリティ演習（Delta Wall）の初回を実施（2023 年 10 月に 8 回目を実施）
2019	「企業内容等の開示に関する内閣府令」改正（有価証券報告書における「事業等のリスク」に関する情報の充実を求める）
	金融庁、「記述情報の開示に関する原則」、「記述情報の開示の好事例集」を公表（同事例集の最新版は 2024 年 3 月公表）
	総務省、「サイバーセキュリティ対策情報開示の手引き」を公表
2023	日本銀行と金融庁、自己評価ツールを整備し、地域金融機関を対象にサイバーセキュリティセルフアセスメントの実施を求め、その集計結果を還元（2024 年 4 月に地域金融機関、保険会社及び証券会社の集計結果を公表）

（出所）各種資料より野村資本市場研究所作成

1．SEC：米国証券市場関連組織のサイバーセキュリティ確保

米国では、2023 年 3 月に米国証券市場における特定関連組織を対象に、サイバーセキュリティリスクに対処することを義務付ける 3 つの規則案（規則 10 の制定、レギュレーション SCI の改正、レギュレーション S-P の改正）を公表した（図表 6 参照）[11]。

1 点目の規則 10 は、証券取引法に基づき、ブローカー・ディーラーや登録清算機関等の対象組織にサイバーセキュリティリスク関連の開示等を求める新たな規則である。2 点目のレギュレーション SCI は、証券売買のインフラを担う組織を対象にシステム障害の防止策や SEC への報告等を義務付ける規則であり、改正案では対象組織の範囲拡大や方針・手順の厳格化、システム侵入被害を遅滞なく SEC に報告すること等が盛り込まれた。いずれの規則案も 2024 年 4 月に最終化される予定との見方であったが、2024 年 5 月末時点で最終化には至っていない。

[11] 経済産業省及び独立行政法人情報処理推進機構（IPA）はサイバーセキュリティリスクを「サイバーセキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと」と定義する（経済産業省、IPA「サイバーセキュリティ経営ガイドライン Ver 3.0」2023 年 3 月 24 日）。

3 点目のレギュレーション S-P は、ブローカー・ディーラー、投資顧問業者（RIA）等に対して顧客情報の保護を義務付ける規則であり、主にセーフガード規則と廃棄規則が柱となっている[12]。改正案では対象組織の範囲拡大や個人の財務データを危険にさらす可能性のある違反を顧客に通知すること等が盛り込まれ、2024 年 5 月 16 日にパブリックコメントを踏えた修正を経て、採択された。規則案の最終化に伴い、対象組織には機微情報が無許可でアクセス又は使用された顧客に対して、遅くとも 30 日以内に通知すること等が義務付けられた。また、当初、一部では規則案による対象組織への過度な負担が懸念されていたが、最終化にあたり、「重大な損害または不便（substantial harm or inconvenience）」の定義の削除等の修正を受けて、対象組織における負担が一定程度軽減された[13]。

図表 6　SEC による各規則案の概要

規則案	「規則 10」（Rule 10）の制定	「レギュレーション SCI」の改正	「レギュレーション S-P」の改正
主目的	市場関連組織を サイバー脅威から保護	主要な市場インフラの 強度と回復力強化	データのプライバシーと 顧客情報の保護
主な対象組織	ブローカー・ディーラー、地方債規則制定委員会（MSRB）、登録清算機関、主要証券ベーススワップ参加者、金融業規制機構（FINRA）、登録証券取引所等	登録証券取引所、登録清算機関、FINRA、自主規制機関（SRO）、一定の要件を満たす代替取引システム（ATS）等	ブローカー・ディーラー、投資信託、登録投資顧問業者及びトランスファー・エージェント
主な内容	サイバーセキュリティリスク関連開示の要請等	対象組織やサイバーイベントの適用範囲の拡大や方針・手順の追加等	連邦政府レベルにおける顧客情報保護の強化等

（注）　2024 年 5 月末時点で最終化された規則案はレギュレーション S-P のみである。
（出所）各種資料より野村資本市場研究所作成

２．金融庁：金融機関によるセルフアセスメントの実施要請

金融庁は 2015 年 7 月に公表した「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」を起点に、金融機関のサイバー・レジリエンスの強化に向けた支援策に取り組んでいる。同指針は、金融庁が金融分野へのサイバー攻撃の脅威への対応に向けて、取り組むべき方針を整理、明確化したものであり、2018 年 10 月に Ver. 2.0 を、2022 年 2 月に Ver. 3.0 を公表した。

金融庁は Ver. 3.0 において、新たに焦点を当てる項目に「モニタリング・演習の高度化」を掲げ、金融機関のサイバーセキュリティ管理態勢の強化を促すことを目的として、金融機関によるサイバーセキュリティに関する自己評価の促進を図る旨を示した[14]。同指針を

[12] セーフガード規則とは、顧客の記録や情報を保護するための管理的、技術的、物理的なセーフガードに対処する書面化された方針と手順の採用を求める規則である。廃棄規則とは、顧客情報の盗難等の消費者詐欺や関連被害のリスク対応のために顧客情報報告書に記載される情報の適切な廃棄を求める規則である。

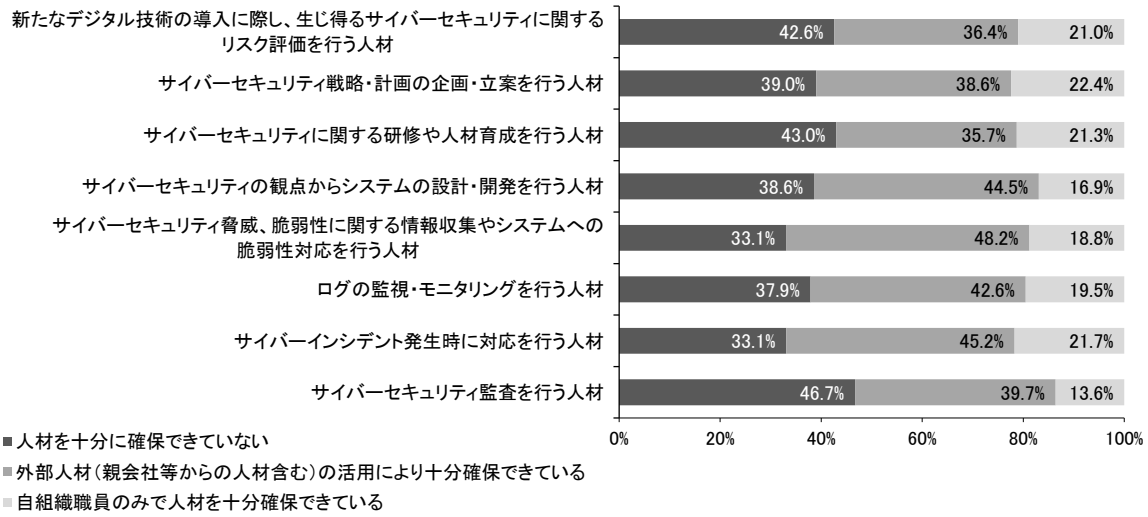
[13] 規則案では、顧客に「重大な損害または不便」をもたらす可能性のある顧客情報への無許可のアクセス又は使用から保護することを義務付けており、新たに提案された「重大な損害または不便」の定義は必ずしも重大ではない状況も範囲となり得た（Securities and Exchange Commission, “Statement on the Amendments to Regulation S-P: Privacy of consumer Financial Information and safeguarding Customer Information,” May 16, 2024）。

[14] 金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）」2022 年 2 月。

基に、金融庁は 2022 事務年度から日本銀行と共同でサイバーセキュリティ管理態勢の自己評価ツール（点検票）を整備し、金融機関を対象に実施を要請し、その集計結果を還元している[15]。同ツールによって、金融機関は「他の金融機関対比での自組織の立ち位置や課題となる領域」を特定することが可能とされている。2022 事務年度には地域金融機関（地域銀行、信用金庫、信用組合）を対象に、2023 事務年度には地域金融機関に加えて保険会社及び証券会社を対象とした。

証券会社の集計結果では、多くの事業者がサイバーセキュリティの確保を経営上の重要課題と捉え、サイバーセキュリティ対策の実効性向上に向けた取り組みを進めているとの評価を示した[16]。一方で、改善の余地がある点として重要なサードパーティのリスク管理、人材確保・育成、コンティンジェンシープランの整備が指摘された。特に、多くの領域や機能に渡り、サイバーセキュリティの人材が十分に確保されていないことが明らかとなり、人材育成の必要性も示唆された（図表 7 参照）。

図表 7　証券会社における機能別にみたサイバーセキュリティ人材の確保状況



（出所）金融庁「【概要】証券会社におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」2024 年 4 月より野村資本市場研究所作成

[15] 日本銀行、金融庁「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2022 年度）」2023 年 4 月。

[16] 金融庁「【概要】証券会社におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」2024 年 4 月。

Ⅳ 今後の論点

本稿では、FSB や IOSCO・CPMI といった国際機関や日米金融当局等による、各地域・法域の FMI や証券会社等の金融機関を対象としたガイダンスの提供、規制強化、セルフアセスメントの支援等の取り組みを概観した。そして、国際機関はサイバー・レジリエンス強化における国際的なベンチマークを示す役割を担い、日米金融当局等は各金融機関等に自社のサイバーセキュリティリスクに対する実態把握の促進を図っていることが推察される。

今後、日本の金融資本市場や金融機関がサイバーリスクの脅威に対応し、健全な発展を遂げるためには、（1）海外当局の動向の把握、（2）金融機関のサイバーセキュリティリスク評価の普及、が重要になると考えられる。

1 点目について、既述のとおり、米国では SEC が証券市場関連組織に対して、サイバーセキュリティの確保に向けた重層的な規則の制定・改正を進めている。こうした規制強化に向けた取り組みは、投資家の信認を得る上で、日本の金融資本市場においても注目に値し得ると言える。また、海外当局や関係機関との連携強化を通じた情報収集は、ボーダーレスかつ最新のサイバー攻撃の実態把握に繋がり得るため、日本の金融資本市場のサイバーセキュリティ強化を図る上で要となる。金融庁の「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（Ver. 3.0）」では、新たに焦点を当てる項目として「関係機関との連携強化」が盛り込まれており、国際連携の深化を図る方針が示された[17]。国際的なサイバー攻撃への対策を講じる観点からも、各国の規制当局の動向の把握に加えて、海外当局とのさらなる連携が期待される。

2 点目について、金融庁がセルフアセスメントの要請を行っているとおり、金融機関が自らのサイバーセキュリティ管理態勢の実態を把握しておくことが金融当局に求められている。米国においても SEC が規則 10 にサイバーセキュリティリスクに対処する方針・手順を盛り込むなど、ブローカー・ディーラーを始めとする金融機関に対して定期的なリスク評価を義務付ける動きが見受けられる。米国では、連邦金融機関検査協議会（Federal Financial Institutions Examination Council、FFIEC）やサイバーリスク研究所（The Cyber Risk Institute、CRI）が金融機関を対象にサイバーセキュリティを評価する枠組みを公表しており、金融機関による取り組みの成熟度を測ることが可能である[18]。この様なサイバーセキュリティリスク評価の枠組みの活用は、自組織のサイバーセキュリティ強化の促進につながり得る[19]。日本の金融資本市場や金融機関のサイバーリスクへの対処の面からも不可欠である。

---

17 脚注 14 を参照。

18 Federal Financial Institutions Examination Council, “Cybersecurity Assessment Tool,”; Cyber Risk Institute, “Our Cyber Profile for the financial sector is a global standard for cyber risk assessment.”

19 金融庁及び日本銀行が開発したセルフアセスメントツール（点検票）は、CRI が公開する CRI Profile 等を参考に作成された（日本銀行、金融庁「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2022 年度）」2023 年 4 月）。