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－

門倉　朋美、江夏　あかね

▌要　約▐

1. 金融機関等を標的としたサイバー攻撃は、国内外を問わず情報漏えいや金銭的被害をもたらしている。金融機関は情報技術（IT）を幅広く活用し、多くの個人情報や金融資産等を管理していることから、金融機関におけるサイバーセキュリティ確保は急務と言える。
2. 米国では、米国証券取引委員会（SEC）が、金融事業者等を対象としたサイバーセキュリティ強化に資する規則を提案した他、SEC 登録企業のサイバーインシデント開示を義務化する規則が制定された。日本では、金融庁が金融機関のサイバーセキュリティ強化に向けた取組指針の策定等に取り組む他、同庁及び総務省が、サイバーセキュリティ関連の情報開示に向けた支援策を展開している。
3. サイバー攻撃は国境を跨ぎ得ることから、その対処に向けて国際的な協調も重要となる。金融安定理事会（FSB）、証券監督者国際機構（IOSCO）、国際決済銀行（BIS）傘下の決済・市場インフラ委員会（CPMI）が、各国・地域の金融当局及び金融機関等におけるサイバーレジリエンス強化に取り組んでいる。
4. 日米の金融当局及び各国際機関の施策を踏まえると、今後、金融当局等が取り組むことが求められる点として、（1）金融機関におけるサイバー人材育成、（2）関連政策との連携、（3）リスクシェアリングの在り方の検討、が挙げられる。

野村資本市場研究所　関連論文等

・江夏あかね・門倉朋美「米国証券市場におけるサイバーセキュリティリスク対処に向けた SEC 規則案の公表」『野村サステナビリティクォータリー』2023 年春号。
・板津直孝「サイバーセキュリティに関わる SEC の開示規則案―広範囲に及ぶインシデントの懸念と情報開示―」『野村サステナビリティクォータリー』2023 年春号。
・富永健司「企業のサイバーセキュリティリスクとサイバー保険」『野村サステナビリティクォータリー』2023 年秋号。

Ⅰ 金融機関を取り巻くサイバー空間の脅威

社会におけるサイバー空間の拡大・浸透が進むなか、サイバー攻撃は社会・経済の発展や国民生活に対する深刻な脅威となっている。金融機関等を標的としたサイバー攻撃は、国内外を問わず情報漏えいや金銭的被害をもたらしている（参考資料 1～2 参照）。金融機関は情報技術（IT）を幅広く活用し、多くの個人情報や金融資産等を管理していることから、サイバー攻撃の標的になりやすい[1]。また、世界におけるデータ侵害による平均被害額を業種別にみても、金融はヘルスケアに次ぐ第2位の590万米ドルに達しており[2]、他の分野と比較してサイバー攻撃による影響が甚大であることが分かる。このように、金融機関におけるサイバーセキュリティ確保は急務となっている。

各国の施策として、例えば、米国では 2008 年頃から国家レベルでサイバーセキュリティ強化を図る動きが見られており、2010年代頃から米国証券取引委員会（SEC）が証券市場を中心としたサイバーセキュリティ関連の取り組みを推進している。日本でも、金融分野へのサイバー攻撃に対処すべく、2015 年頃から金融庁が中心となり取組方針の提示や金融業界横断的な演習の実施等に取り組んでいる。

また、サイバー攻撃は、その被害者、攻撃者の国籍、攻撃の発信源等が国境を跨ぎ得ることから、その対処に向けて各国の取り組みだけでなく、国際的な協調が重要となる。特に、金融安定理事会（FSB）、証券監督者国際機構（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、各国・地域の金融当局や金融機関等を対象としたサイバーセキュリティ関連の取り組みを推進している。

本稿では、日米の金融当局による証券市場のサイバーセキュリティ対応について、金融機関等のサイバーレジリエンス強化に向けた施策と、サイバーセキュリティ関連情報開示を促進する施策を中心に概観するとともに、上述の国際機関の動向を整理する。その上で、今後、金融当局等が取り組むことが求められる点を論考する。

Ⅱ 日米金融当局による証券市場を中心としたサイバー対応

日米の金融当局は 21 世紀に入り、サイバー攻撃に対する耐性力や回復力を指す、サイバーレジリエンスに関連した取り組みを重層的に展開している（図表 1～2 参照）。本章では、日米金融当局による主な施策として、金融機関等のサイバーレジリエンス強化、サイバーセキュリティ関連情報の開示促進に焦点を当てて概観する。

1 十川基「金融機関における戦略的なサイバーセキュリティ対策の計画立案・推進に関する考察」『FSA Institute Discussion Paper Series』DP2022-4、金融庁金融研究センター、2022 年 7 月。

2 IBM Security「データ侵害のコストに関する調査」2023 年。

図表 1　日本の主なサイバーセキュリティ関連の政策動向

暦年	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 2023 年 12 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

（出所）各種資料より野村資本市場研究所作成

図表 2　米国の主なサイバーセキュリティ関連の政策動向

暦年	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

（出所）各種資料より野村資本市場研究所作成

1．米国証券市場に関連するサイバーセキュリティ確保

米国では、ブッシュ政権終盤の 2008 年頃からサイバーセキュリティが米国政府の安全保障政策において重点分野の 1 つとなった[3]。近年では、2021 年 5 月にサイバーセキュリティ強化のための大統領令が発令され、2022 年 3 月に「重要インフラに関するサイバーインシデント報告法（CIRCIA）」[4]が成立するなど、国家レベルでサイバーセキュリティ強化を図る動きが活発化している。

金融セクターにおいては、SEC によって米国証券市場における金融事業者等の関連組織を対象としたサイバーセキュリティ確保に資する規則が提案された他、SEC 登録企業のサイバーインシデント開示を義務化する規則が制定された。

[3] 土屋大洋「米国におけるサイバーセキュリティ政策」日本国際問題研究所／編『米国内政と外交における新展開』2013 年 3 月。

[4] Cybersecurity & Infrastructure Security Agency, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),” March 2022.

１）金融機関等を対象としたサイバーセキュリティリスク対処

SECは、2023年3月に米国証券市場に関わる金融機関等を対象にサイバーセキュリティと消費者情報の保護に関する 3 つの規則案として、（1）規則 10 の制定、（2）レギュレーション SCI の改正、（3）レギュレーション S-P の改正、を公表した[5]（図表 3 参照）。

図表 3　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

（出所）各種資料より野村資本市場研究所作成

1点目の規則10は、証券取引法に基づく新たなサイバーセキュリティリスク管理規則である。同規則は、ブローカー・ディーラー、登録清算機関、主要証券ベーススワップ参加者等の事業体におけるサイバーセキュリティインシデントのリスクへの対処とその軽減を目的としている。主な要件には、サイバーセキュリティリスクに対処するために合理的に設計された方針と手順の採用、重大なサイバーインシデントが発生した場合の SEC への報告、重大なサイバーインシデントの概要等の一般への開示、が挙げられる。

2 点目のレギュレーション SCI は、登録証券取引所や登録清算機関等の証券売買のインフラとしての機能を担う組織に対して、システム障害の防止策の規定やシステム障害の発生時の SEC への報告等を義務付ける規則である。今回の改正では、対象組織の範囲拡大が図られた他、対象組織に課す要件として、レギュレーション SCI の遵守を意図した方針と手順の厳格化、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[6]。

3 点目のレギュレーション S-P は、SEC 登録のブローカー・ディーラー、投資会社、

[5] U.S. Securities and Exchange Commission, “SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets,” March 15, 2023; U.S. Securities and Exchange Commission, “SEC Proposes to Expand and Update Regulation SCI,” March 15, 2023; U.S. Securities and Exchange Commission, “SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information,” March 15, 2023. 各規則案の詳細については、江夏あかね・門倉朋美「米国証券市場におけるサイバーセキュリティリスク対処に向けた SEC 規則案の公表」『野村サステナビリティクォータリー』2023年春号を参照されたい。

[6] 従来の対象組織は、登録証券取引所、登録清算機関、金融業規制機構（FINRA）、米国地方債規則制定委員会（MSRB）等の自主規制機関（SRO）等が挙げられる。今回の改正案において、一定の要件を満たすブローカー・ディーラー、スワップデータデポジトリ、SECの登録免除清算機関が新たに加わった。

投資顧問業者に対して、顧客から収集した財務情報の保護を求める規則である。同規則では、顧客の記録と情報を保護するための書面による方針及び手順を採用すること（セーフガード規則）等を義務付けている。今回の改正では、顧客情報保護の強化を目的として、対象組織にトランスファー・エージェントを加える他、個人の財務データを危険にさらす可能性がある違反を顧客に通知すること等を義務付ける。

上記 3 つの規則案について、SEC の委員のうち、委員長を含む 3 名の委員が支持する姿勢を示す一方で、共和党の 2 名の委員は反対または懸念を示している。各規則案は、2024 年 4 月に最終化されるとみられている[7]。

2）SEC 登録企業を対象としたサイバーインシデント開示の義務化

SEC は、上場企業によるサイバーセキュリティのリスク管理、戦略、ガバナンス、インシデントに関する開示の強化と標準化を目的として、2023 年 7 月 26 日に 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した[8]。新規則の主な要件は、（1）年次報告書におけるサイバーセキュリティリスクの対応状況等の開示、（2）臨時報告書におけるサイバーセキュリティインシデントの開示、に大別される（図表 4 参照）。

図表 4　主な要件の概要

	対象	提出フォーム
年次開示	米国内の発行体	Form 10-K
	外国民間発行体	Form 20-F
重要インシデント開示	米国内の発行体	Form 8-K
	外国民間発行体	Form 6-K

（注）　1. 年次開示は 2023 年 12 月 15 日以降に終了する会計年度を対象とする年次報告書から適用。重要インシデント開示は、原則 2023 年 12 月 18 日以降に適用。
2. 流通株式総額が 2 億 5,000 万ドル未満等の要件を満たす SRC（smaller reporting companies、小規模報告企業）は、Form 8-K による開示に当たり 180 日の猶予が与えられるため、2024 年 6 月 15 日以降に適用。

（出所）各種資料より野村資本市場研究所作成

前者は、非財務情報の開示規制であるレギュレーション S-K に新たな項目（Item106）を設け、サイバーセキュリティに関するリスク管理、戦略、ガバナンスに関して、年次報告書（Form 10-K）を通じた開示を義務付ける。後者は、サイバーセキュリティインシデントが生じた際に、SEC 登録企業が当該インシデントを重大であると判断した場合に、臨時報告書（Form 8-K）を 4 営業日以内に提出することを義

[7] Davis Wright Tremaine LLP, “SEC Delays Proposed Cybersecurity Rules,” June 27, 2023; Office of Information and Regulatory Affairs, “Agency Rule List – Fall 2023: Securities and Exchange Commission.”

[8] Securities and Exchange Commission, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” July 26, 2023. SEC による規則案の詳細については、板津直孝「サイバーセキュリティに関わる SEC の開示規則案―広範囲に及ぶインシデントの懸念と情報開示―」『野村サステナビリティクォータリー』2023 年春号を参照されたい。

務付ける。外国民間発行体に対しては、いずれも上述の米国内の発行体と同等の開示が求められる。

なお、米国司法長官が、臨時報告書の開示が国家安全保障あるいは公共の安全に重大なリスクをもたらすと判断し、その旨を書面で SEC に通知した場合、Form 8-K による開示を遅らせる場合があるとされている。この点に関して、連邦捜査局（FBI）及び司法省（DOJ）は 2023 年 12 月に、重大なサイバーインシデント報告の遅延リクエストに関するガイダンスをそれぞれ公表している[9]。

当該規則に関しては、CIRCIA によるインシデント報告との重複を指摘する声もある[10]。CIRCIA では、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）が定める重要インフラ事業者に対して、サイバーインシデント発生後 72 時間以内に、ランサムウェア攻撃[11]に対する身代金を支払った場合は 24 時間以内に、CISA に報告することを義務付けている。

２．日本の金融分野における取り組みの現状

日本では、2014 年 11 月に成立したサイバーセキュリティ基本法に基づき、2015 年 1 月に、内閣には「サイバーセキュリティ戦略本部」[12]が、内閣官房には「内閣サイバーセキュリティセンター（NISC）」が設置された。金融は、サイバーセキュリティ戦略本部によって、国民生活及び社会経済活動が大きく依存する重要インフラに定められていることから[13]、金融機関には重要インフラサービスの継続的提供の観点から適切なサイバーセキュリティが求められると言えよう。金融庁は、金融機関のサイバーセキュリティ強化に向けた取組指針の策定や業界横断的な演習の実施等に取り組んでいる他、同庁及び総務省が、サイバーセキュリティ関連の情報開示に向けた支援策を展開している。

１）金融庁による金融機関のサイバーレジリエンス強化策

金融庁は、重要インフラ所管省庁として、重要インフラ防護の推進に向けて取り組んでおり、2015 年 7 月に「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

---

9 Federal Bureau of Investigation, “Policy Notice Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Notice 1297N,” December 6, 2023; Department of Justice, “DEPARTMENT OF JUSTICE MATERIAL CYBERSECURITY INCIDENT DELAY DETERMINATIONS,” December 12, 2023.

10 下院国土安全保障委員会サイバーセキュリティ・インフラ保護に関する小委員会のアンドリュー・ガルバリノ委員長は、重大なサイバーセキュリティインシデントの迅速な開示等の義務付けを阻止する法案を提出した（Jonathan Greig, “Chairman of House Cybersecurity Panel Wants to Overturn SEC Disclosure Rules,” *The Record*, November 15, 2023）。

11 ランサムウェア攻撃とは、情報システム上の無許可または悪意のあるコードの使用、使用の脅威、またはサービス妨害攻撃等の別のデジタルメカニズムの使用、または使用の脅威を含む、システムの運用を中断または混乱させるインシデント等を指す（Cybersecurity & Infrastructure Security Agency, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 [CIRCIA],” March 2022）。

12 サイバーセキュリティ戦略本部とは、2015 年 1 月に内閣に設置された、サイバーセキュリティ戦略の案の作成及び実施の推進等を所管する組織。

13 サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る行動計画」2022 年 6 月 17 日。

方針」を策定した。当該方針は、既述のサイバーセキュリティ基本法の制定等を踏まえ、金融分野へのサイバー攻撃の脅威の対応に向けた、取り組むべき方針を整理・明確化したものである。現在は、2022 年 2 月に更新された Ver. 3.0 に基づき、特に、（1）モニタリング・演習の高度化、（2）新たなリスクへの備え、（3）サイバーセキュリティ確保に向けた組織全体での取り組み、（4）関係機関との連携強化、（5）経済安全保障上の対応、に焦点を当てた対応を進めている（図表 5 参照）。2 点目の「新たなリスクへの備え」では、論点の一つに「サイバーレジリエンスの強化」を挙げている。サイバー攻撃の高度化・複雑化や外部委託の拡大等を鑑みて、インシデントの未然防止だけでなく、インシデント発生時におけるレジリエンスの重要性を示唆している。なお、金融庁は 2023 年 4 月に、各金融機関によるより良い実務の構築を目的として、オペレーショナル・レジリエンスの論点・課題を整理したディスカッション・ペーパーを公表している[14]。

上述の取組方針の他、金融庁は、金融業界全体のインシデント対応能力の更なる向上を図ることを目的とした「金融業界横断的なサイバーセキュリティ演習」を実施した。直近では、2023 年 10 月に 165 の金融機関を対象とした 8 回目の演習を実施し、各業態別の演習シナリオを通じて組織内外の連携の確認が行われた[15]。

図表 5　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（抜粋）

1. モニタリング・演習の高度化
金融機関の規模・特性やサイバーセキュリティリスクに応じて、検査・モニタリングを実施し、サイバーセキュリティ管理態勢を検証する。共通の課題や好事例については業界団体を通じて傘下金融機関に還元し、金融業界全体のサイバーセキュリティの高度化を促す。特に
・ 3 メガバンクについては、サイバー攻撃の脅威動向の変化への対応や海外大手金融機関における先行事例を参考にしたサイバーセキュリティの高度化に着目しつつ、モニタリングを実施する
・ 地域金融機関については、サイバーセキュリティに関する自己評価ツールを整備し、各金融機関の自己評価結果を収集、分析、還元し、自律的なサイバーセキュリティの高度化を促す
・ サイバー演習については、引き続き、サイバー攻撃の脅威をめぐる動向や他国の演習等を踏まえて高度化を図る
2. 新たなリスクへの備え
・ キャッシュレス決済サービスの安全性を確保するため、リスクに見合った堅牢な認証方式の導入等を促す（セキュリティバイデザインの実践）
・ クラウドサービスの安全な利用に向けて、利用実態や安全対策の把握を進めるとともに、クラウドサービス事業者との対話も実践
3. サイバーセキュリティ確保に向けた組織全体での取組み
・ 経営層の積極的な関与の下、組織全体でサイバーセキュリティの実効性の向上を促す（セキュリティ人材の育成も含む）
4. 関係機関との連携強化
・ サイバー攻撃等の情報収集・分析、金融犯罪の未然防止と被害拡大防止への対応を強化するため関係機関（NISC、警察庁、公安調査庁、金融 ISAC[Information Sharing and Analysis Center]、海外当局等）との連携を強化
・ 経済安全保障上の対応
5. 政府全体の取組みの中で、機器・システムの利用や業務委託等を通じたリスクについて適切に対応を行う

（出所）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 月より野村資本市場研究所作成

[14] 金融庁「ディスカッション・ペーパー オペレーショナル・レジリエンス確保に向けた基本的な考え方」2023 年 4 月。

[15] 金融機関の参加数は暫定的（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 Ⅷ）』について」2023 年 10 月 18 日）。

２）サイバーセキュリティ関連情報の開示動向

日本においても、米国と同様に企業におけるサイバーセキュリティ関連の情報開示に向けた取り組みが展開されている。法律の観点からは、「企業内容等の開示に関する内閣府令」が2019年1月に改正され、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が求められた。本改正を受けて、金融庁は同年 3 月に「記述情報の開示の好事例集」を、総務省は同年 6 月に「サイバーセキュリティ対策情報開示の手引き」を、公表した。

前者は、有価証券報告書における開示例を中心に、個社の好事例を取りまとめたもので、投資家と企業との建設的な対話に資する充実した企業情報の開示の促進を目的としている。当該事例集は年次で改訂されており、2023 年 12 月に公表された「記述情報の開示の好事例集 2023」では、「個別テーマ」の開示例として、金融機関を含む複数社によるサイバー関連の開示例を紹介している。後者は、各企業が情報開示の在り方を検討する際の参考資料となることを目的として、主に社内の実務担当者を対象として、情報開示の手段、一般的なサイバーセキュリティ対策の内容、開示にあたっての要点や記載例を提示している。

Ⅲ 金融分野におけるサイバーセキュリティ関連の国際的な協調

サイバー攻撃は国境を跨ぎ得るため、その対処には各国のサイバーセキュリティ施策だけでなく、国際的な協調が重要となる。以下では、金融セクターのサイバーセキュリティ確保に向けて国際的な協調の促進を図る、FSB、IOSCO 及び CPMI の取り組みを概観する。

１．FSB によるサイバーレジリエンス強化に向けた取り組み

FSBは、25の国・地域の中央銀行、金融当局、基準設定主体等の代表が参加する国際機関[16]であり、「金融・世界経済に関する首脳会合（G20）」の下、国際的な金融安定の促進を図るために各国・地域の金融当局や基準設定主体による政策の策定において調整を行う。FSB は、サイバーレジリエンスの強化を金融安定の促進に向けた作業計画において重要な要素として位置付けており、各国・地域の金融当局や金融機関等を対象としたサイバーセキュリティ関連の施策を推進している[17]。

FSB による施策は、2017 年 3 月にドイツで開催された G20 財務大臣・中央銀行総裁会議声明[18]をきっかけに活発化した（図表 6 参照）。G20 は同声明において、情報通信技術

[16] 2023 年 12 月末時点（Financial Stability Board, “Members of the FSB”）。

[17] 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、迅速に回復することで、組織がその使命を遂行し続ける能力」と定義している（Financial Stability Board, “Cyber Lexicon Updated in 2023,” Aril 13, 2023）。

[18] G20, “Communiqué G20 Finance Ministers and Central Bank Governors Meeting Baden-Baden, Germany, 17-18 March 2017.”

（ICT）の悪意ある利用は金融サービスを混乱させ金融安定を脅かし得ると指摘し、FSBに対して、既存の関連規制や監督上の慣行、国際的なガイダンスに関する実績調査（stock-taking）を要請した。

当該実績調査の結果等を踏まえ、FSBは主に、（1）サイバー用語集の策定、（2）サイバーインシデントへの初動と回復（Cyber Incident Response and Recovery、CIRR）対応の効果的な実務の促進、（3）サイバーインシデント報告（Cyber Incident Reporting、CIR）共通化の促進、を推進した。以下では、これらの施策を図表6の時系列に沿って概観する。なお、3点目のCIR共通化の促進は、既述のとおりSECが米国証券市場の上場企業を対象としてインシデント報告を義務化する等、重要な論点と考えられるため、内容を詳述する。

図表6　FSBのサイバーセキュリティ関連の主な動向

時期	内容
2017年3月	ドイツで開催されたG20財務大臣・中央銀行総裁会議声明において、FSBに対して、G20加盟国・地域内において公表されている既存の関連する規制や監督上の慣行、国際的なガイダンスに関する実績調査（stock-taking）の実施を要請
2017年6月	「金融安定へのフィンテックからの含意：当局が注視する規制上及び監督上の諸問題」を公表。国際協力の優先事項として、「サードパーティーのサービスプロバイダーによる運用リスクの管理」や「サイバーリスクの軽減」に言及
2017年10月	「金融セクターのサイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク」の結果に関する概略報告書及び詳細分析を公表。G20の要請に基づくFSBの調査結果を示しており、FSBの全ての管轄区域において、金融分野におけるサイバーセキュリティに対処する規制やガイダンスが発出されていると指摘
2018年11月	「サイバー用語集」を公表。金融分野におけるサイバーセキュリティとサイバーレジリエンスに関連した主な用語として約50語の定義を提示
2019年2月	「2019年の作業計画」を公表。同年の重点分野「金融システムにおける新たな脆弱性への対処」に関する項目の一つとして、「サイバーレジリエンス」の強化に言及
2019年5月	G20財務大臣・中央銀行総裁会議に対する報告書として、「サイバーインシデントへの初動と回復に係る進捗報告書」を公表
2019年7月	「サイバーインシデントへの初動と回復：民間実務に関する調査」を開始。各国・地域の規制当局及び金融機関を対象にサイバー攻撃への初動と復旧に関するガイダンスの作成を目的とした調査
2019年12月	「金融におけるBigTech：市場動向と金融安定への潜在的な影響」及び「クラウドサービス利用における第三者サービスへの依存：金融安定への影響に関する考察」を公表
2020年10月	「サイバーインシデントの初動と回復対応の効果的な実務：最終報告書」を公表。サイバーインシデントの初動・回復対応を強化するための提言を示し、当局及び金融機関に対して本ツールキットの活用を推奨
2021年6月	「アウトソーシング・サードパーティーに関する規制・監督上の論点：市中協議に寄せられた意見の概要」を公表
2021年10月	「サイバーインシデント報告－既存のアプローチとより広い範囲での収斂に向けた今後のステップ」を公表。規制監督対応に関する各国・地域の違い、当局間で情報共有する際の課題、サイバー事象報告の調和に向けた今後の方向性を提示
2022年10月	「サイバーインシデント報告の更なる収斂の達成：市中協議文書」を公表。詳細な課題分析に基づく提案事項を取りまとめる他、サイバー用語集の改訂案を提示
2023年4月	「サイバーインシデント報告の更なる収斂に向けた提案：最終報告書」を公表。インシデント報告制度の更なる収斂に向けた提案、サイバー用語集の追加・改訂、共通データフォーマットを提示
2023年6月	「サードパーティーリスクの管理とオーバーサイトの向上：金融機関・金融当局のためのツールキット市中協議書」を公表。金融機関によるサードパーティーリスクの管理や金融当局による監督の向上に向けたツールキットを取りまとめ、広く意見を募集

（出所）Financial Stability Board、各種資料より野村資本市場研究所作成

１）サイバー用語集の策定

FSB は 2018 年 11 月、金融当局と民間セクター間における効率的なコミュニケーションの強化を念頭に、金融セクターにおけるサイバーセキュリティ及びサイバーレジリエンスに関連した約 50 語の定義を示す「サイバー用語集」[19]を公表した。当該用語集は、FSB、基準設定主体、金融当局、民間部門におけるサイバーレジリエンス向上に関する取り組みの支援を目的に策定されたものである。従って、対象範囲となる用語は、金融セクターにおける官民の取り組みに有用とされる用語に限定し、他組織による既存の用語集等への準拠[20]、包括的な定義、平易な言葉、を基準に各定義が策定された。

その後、FSB は後述する 3 点目の CIR 共通化の促進に関する一連の施策として、2023 年 4 月に当該用語集を改定した。進化するサイバー情勢や情報技術の発展が考慮された対応であり、既存の用語の定義が一部改訂された他、新たな用語が追加された[21]。

２）CIRR 対応の効果的な実務の促進

FSB は 2018 年 10 月の FSB 本会合において、金融セクターの相互関連性を考慮し、関連する金融安定リスクを制限するための対応として、CIRR に関する効果的な慣行（ツールキット）の整備に合意した。FSB は重大なサイバーインシデントが適切に抑制されない場合、金融システムへの深刻な混乱に伴う金融安定への影響等を懸念し、サイバーインシデントへの効率的かつ効果的な初動と回復の重要性を訴えた。

2020 年 4 月より実施した市中協議を経て、FSB は 2020 年 10 月に「サイバーインシデントの初動と回復対応の効果的な実務：最終報告書」[22]を公表した。本報告書は、主に金融機関を対象として CIRR 活動を強化する要素として機能する一連の効果的な実務方法を示すものである。具体的には、CIRR の構成要素（ガバナンス、計画・準備、分析、影響緩和、復旧・回復、調整・コミュニケーション、改善）を時系列（発生前・発生中・発生後）に整理した上で、計 49 項目の具体的な実務が盛り込まれている。例えば、インシデント発生中に分類される「影響緩和」は、組織が緩和策を発動することにより状況の悪化を防ぎ、サイバーインシデントのタイムリーな根絶により、事業運営やサービスへの影響を軽減することを指している。その具体的な項目には、各インシデントに応じた封じ込め措置の適用や事業継続対策等が挙げられた。

FSB は、金融システムの強さはその最も弱い部分に準じることから、CIRR は金融エコシステム内の全ての組織に関係すると指摘した。

---

[19] Financial Stability Board, “Cyber Lexicon,” November 12, 2018.

[20] BIS 決済・市場インフラ委員会と証券監督者国際機構（CPMI-IOSCO）による金融市場インフラのサイバーレジリエンスに関するガイダンス、G7 サイバー専門家グループ、米国国立標準技術研究所（NIST）による重要な情報セキュリティ関連用語の用語集、国際標準化機構（ISO）等の他組織による取り組み、に基づき構築され、FSB の目的に準じて抽出、修正を加えている。

[21] 新たなに追加された用語は、サイバー攻撃、インサイダー脅威、フィッシング、ランサムウェア、ゼロデイ脆弱性（情報システム内の未知の脆弱性）、セキュリティオペレーションセンター。

[22] Financial Stability Board, “Effective Practices for Cyber Incident Response and Recovery: Final Report,” October 19, 2020.

３）CIR 共通化の促進

G20 は、サイバーインシデントに関する適時で正確な情報が、効果的な CIRR、ひいては金融安定の促進にとって極めて重要であると指摘し、FSB に対して CIR の調和向上に関する報告書の提出を要請した。FSB は、当該要請に対応する過程で公表した報告書において、CIR の収斂を達成するための方法として、ベストプラクティスの開発、共通する一般的な情報の種類の特定、CIR のための共通用語の作成、を定めた[23]。

FSB は 2023 年 4 月、これに対応した施策の一つとして、主に各国・地域の金融当局や金融機関を対象とした、「サイバーインシデント報告の更なる収斂に向けた提案：最終報告書」を公表した[24]。本報告書は、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いる。まず、2022 年に実施した FSB 加盟国・地域への調査[25]に基づき、CIR のフレームワークを集約する上で、金融機関からのサイバーインシデント情報の収集、規制当局間の情報共有に関する実務上の課題が特定された（図表 7 参照）。

図表 7　CIR フレームワークの実務上の課題

- **複数の当局への報告プロセスから生じる運用上の課題**
- **報告のための適切かつ一貫性のある定性的・定量的基準／閾値の設定**
- **インシデントを適時に報告するための適切な文化の確立**
- **サイバーセキュリティに関連する定義及び分類法の一貫性の欠如**
- **サイバーインシデントに関する安全な連絡メカニズムの確立**
- **国境やセクターを越えて当局と情報共有する際の法的または秘密保持上の制約**

（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

これらの課題に対処する提案として、CIR フレームワークの集約の促進に資する計 16 項目が示された（図表 8 参照）。なお、付属文書には各項目がそれぞれの課題に対してどの程度の好影響を与えるかを予測したマッピングが盛り込まれている。FSB は、CIR に対する画一的なアプローチは実現が難しく、必ずしも望ましいわけではないといった考えを示しており、あくまでも規制当局や金融機関は自国の法的・規制的枠組みとの整合性、適切性、関連性を踏まえて当該提案の採用を選択するよう推奨している。

---

[23] Financial Stability Board, “Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence,” October 19, 2021.

[24] Financial Stability Board, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting; Final Report,” April 13, 2023. なお、CIR の収斂の促進に向けた取り組みの一環として、本報告書の他に、既述のサイバー用語集の改訂、「インシデント報告交換フォーマット（FIRE）：今後の展望」の公表が行われている。後者は、金融機関が規制当局に提出する CIR のための共通データフォーマットの開発に向けた今後の進め方等を示す報告書である。

[25] 同調査を通じて、CIR のフレームワークは、国・地域やセクターを越えて、その報告目的やインシデントに関して収集されるデータ種類、金融機関の報告義務のトリガーとなる基準や重要性の閾値の使用に関して共通点が多くあると指摘された。

図表 8　FSB による提案の一覧

CIR に対するアプローチの設計
1. **CIR の目標を確立、維持** 金融当局は、インシデント報告の目的を明確に定義し、金融機関と当局の双方に対して、当該目的を効率的に達成できる方法を定期的に評価、実証すべき
2. **CIR 枠組みのさらなる収斂の検討** 金融当局は、潜在的な断片化を最小限に抑え、相互運用性を向上させるために、国境や分野を越えて、CIR 制度を他の関連当局と連携する方法を引き続き模索すべき
3. **共通データ要件及びレポート形式の採用** 金融当局は、共通のデータ要件を個別または共同で特定し、必要に応じて、インシデント報告情報を交換するための標準化された形式を開発または採用すべき
4. **漸進的な報告要件の段階的な適用** 金融当局は、インシデント直後はタイムリーな最小限の報告、事態の鎮静化に伴い包括的な報告を求める要件を導入するべき
5. **適切なインシデント報告トリガー** 金融当局は、CIR 制度の設計の一環として、さまざまな報告トリガーの選択肢における利点及び影響を調査すべき
6. **最初の報告窓口の調整** 金融当局は、最初の報告に使用される窓口の設計または調整に関連する潜在的な結果を考慮すべき
7. **解釈リスクを最小限に抑えるための十分な詳細情報の提供** 金融当局は、報告基準値の設定において適切なレベルの詳細情報を提供し、共通の用語を使用し、CIR ガイダンスを事例で補足することにより、一貫した理解を促進し、解釈リスクを最小化すべき
8. **重要性に基づくトリガーの下でタイムリーな報告を促進** 重要性の閾値（materiality thresholds）を使用する金融当局は、重要なインシデントについて金融機関による迅速な報告を促すために、閾値の文言を微調整すること、または他の適切なアプローチを検討すべき
当局間における監督活動及び協力
9. **CIR 及びサイバーインシデント対応・復旧（CIRR）プロセスの有効性のレビュー** 金融当局は、既存の監督または規制エンゲージメントの一環として、金融機関の CIR 及び CIRR のプロセス及び手順の有効性をレビューする方法を検討すべき
10. **アドホック・データ収集の実施** 金融当局は、必要に応じて CIR の枠組みを監督措置で補完し、実際のインシデント中あるいはそれ以外の双方でサイバーインシデントに対して金融機関に関与させる方法を模索すべき
11. **国境を越えた情報共有の阻害要因への対処** 金融当局は、国境を越えた CIR 情報の交換に関連する法的または守秘義務上の課題に共同して対処する方法を模索すべき
業界エンゲージメント
12. **報告のメリットに関する相互理解の促進** 金融当局は、インシデント報告の価値及び重要性についての認識を高めるために金融機関と定期的に連携し、金融機関が直面する可能性のある課題を理解し、正当な場合は、それらを克服するためのアプローチを特定すべき
13. **効果的な CIR コミュニケーションに関するガイダンスを提供** 金融機関は、サイバーインシデント報告における効果的なコミュニケーションの実践を促進するため、ツールキットやガイドラインを開発あるいは、開発を促進する方法を検討すべき
能力開発（個別金融機関及び金融機関・金融当局共通）
14. **CIR を支援する対応能力を維持** 金融機関は、継続的なインシデント検知、評価及び訓練を含む、CIR を直接支援するサイバーインシデント対応能力におけるあらゆるギャップを特定し、対処すべき
15. **関連するサイバーイベント及びサイバーインシデントを特定するための知識のプール** 金融当局及び金融機関は、状況の不確実性に対処し、金融分野の集団的防衛のために知識を蓄積するために、金融分野の参加者間でイベント、脆弱性及びインシデント情報をプロアクティブに共有するメカニズムを特定、実施するために協力するべき
16. **機密情報の保護** 金融当局は、常に機密情報の保護を確保するために、安全な形式のインシデント情報処理を実装すべき

（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 と CPMI

IOSCO と CPMI は、金融市場インフラ（FMI）が遵守すべき原則を示した「金融市場インフラのための原則（FMI 原則）」[26]を定めており、各国・地域のメンバーは自らの法域において FMI 原則を適用している[27]。両者は FMI のサイバーレジリエンス強化の観点から、FMI 原則を補完するガイダンスを公表した。以下では、当該ガイダンスを概観するとともに、2022 年に両者が各国・地域における現状を調査した報告書を概説する。

１）FMI に焦点を当てたサイバーガイダンスの公表

IOSCO と CPMI は、2012 年 4 月に公表した FMI 原則において、FMI 向けの原則と FMI の関係当局向けの責務を定めている。なかでも、前者の原則のうち、原則 17 のオペレーショナルリスクに関する項目では、その要因の一つにサイバー攻撃について言及している。当該原則の重要な考慮事項（Key Considerations、以下 KC）6 では、不可欠な情報システムにおける事務処理の停止から 2 時間以内の再開を確保する設計等が推奨されており、金融市場インフラの業務継続体制の観点においてサイバーレジリエンスの重要性が示唆されている。

そうしたなか、IOSCO と CPMI はサイバーレジリエンスに関連する原則[28]を補完する観点から、2016 年 6 月に「金融市場インフラのためのサイバー攻撃耐性に係るガイダンス（サイバーガイダンス）」[29]を公表した。サイバーレジリエンスが FMI のオペレーショナル・レジリエンスに影響し、ひいては金融システム及び広範な経済全体のレジリエンスの決定的な要因となり得ることを踏まえて、FMI のサイバーレジリエンスの強化を目的とするものである。

サイバーガイダンスでは、FMI のサイバーレジリエンス体制において取り組むべき 5 つの主要なリスク管理要素と 3 つの包括的な構成要素を解説している（図表 9 参照）。FMI に対して、サイバーレジリエンスを向上するためにステークホルダーと連携して直ちに必要な措置を講じることの他、本ガイダンスの発行から 12 カ月以内に 2 時間以内の業務再開の達成のための具体的な計画の策定を求めた。

---

[26] Bank for International Settlements, International Organization of Securities Commissions, “Principles for financial market infrastructures,” April 12, 2012.

[27] IOSCO とは、世界各国・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機関であり、証券監督に関する原則・指針等の国際ルールの策定等を行う。CPMI とは、各国・地域の中央銀行が加盟する BIS の傘下に位置する、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。支払・清算・決済等の安全性と効率性を促進、監視し、提言を策定する他、政策や運営事項等の中央銀行間の連携において意見交換の場を提供する。金融市場インフラ（financial market infrastructures）とは、資金決済システム、証券集中振替機関、証券決済システム、清算機関、取引情報蓄積機関を指す。日本の場合、日本証券クリアリング機構、証券保管振替機構等が該当する。

[28] FMI 原則のうち、主にガバナンス（原則 2）、包括的リスク管理体制（原則 3）、決済のファイナリティ（原則 8）、オペレーショナルリスク（原則 17）、FMI 間リンク（原則 20）、を補完するもの。

[29] The Committee on Payments and Market Infrastructures and The International Organization of Securities Commissions, “Guidance on Cyber Resilience for Financial Market Infrastructures,” June 29, 2016.

図表 9　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（抜粋）

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体制の構築
	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

2）FMI におけるサイバーレジリエンスの現状

IOSCO 及び CPMI は、既述の FMI 原則に関する実施状況を定期的に評価している。2022 年 11 月に「『金融市場インフラのための原則』の実施状況に関するモニタリング（金融市場インフラのサイバーレジリエンスに関するレベル 3 評価）」を公表した[30]。2020 年から 2022 年にかけて参加のあった 29 の国・地域の 37 の FMI におけるサイバーレジリエンスの状況（2021 年 2 月時点）の現状評価や、サイバーガイダンスの利用状況を示すもので、全ての FMI が対象となった[31]。

評価の結果、サイバーガイダンスの採用率はある程度高く（reasonably high）、大多数が部分的に採用または参考にしていることが示された。ただし、深刻な懸念事項が 1 点と、懸念事項が 4 点、示された（図表 10 参照）。明確な課題として最優先で取り組むべき「深刻な懸念事項」には、少数の FMI が 2 時間の復旧時間目標（2hRTO）に対して十分な水準に達しておらず、確実な業務再開を可能とするような設計がなされていないと指摘した。

IOSCO 及び CPMI は、これらの結果は FMI のサイバーレジリエンスに明確な課題を提起しているとして、関連する FMI とその監督機関に対して最優先でこれらの問題に取り組むよう促している。

[30] レベル 3 評価とは、特定の分野について個別の FMI における FMI 原則の実施状況の評価。なお、レベル 1 評価は、FMI 原則の国内実施のための枠組み、関連法、規制、方針の整備状況の確認。レベル 2 評価は、各国・地域の枠組みの内容と FMI 原則との整合性の検証（The Committee on Payments and Market Infrastructures, the International Organization of Securities Commissions, “Implementation monitoring of the PMFI: Level 3 assessment on Financial Market Infrastructures’ Cyber Resilience,” November 2022）。

[31] 参加のあった国・地域名、FMI の個別名は非公表となっている。

図表 10　IOSCO・CPMI による FMI 原則に関する実施評価の主な結果

深刻な懸念事項（Serious issue of concern）
1.　2 時間の復旧時間目標（2hRTO）を満たす、確立された対応・復旧計画の欠如 少数の FMI は、原則 17 の重要な考慮事項（KC）6 に沿って 2hRTO を達成するためのサイバーへの初動・復旧計画が未策定。この少数の FMI の中には、シナリオに対処する計画がない FMI もあり、その結果、復旧時間の目標が未達成。この発見は、該当する FMI のサイバーレジリエンス及び準備の水準に疑問を投げかけるもので、最優先で取り組むべき深刻な懸念事項
懸念事項（Issues of concern）
1.　極端なサイバー攻撃シナリオの下で 2hRTO を満たす、確立された対応・復旧計画の欠点 深刻な懸念事項が関連する少数の FMI に加えて、2hRTO を満たすサイバー対応・復旧計画を策定していた別の少数の FMI は、極度のサイバー攻撃のシナリオ下では計画が 2hRTO を満たすことができないことを認識。これは原則 17KC6 に関連する FMI の実施結果における乖離または欠点であり、対処が必要
2.　大規模なシステム変更後のサイバーレジリエンステスト（バックアップデータの完全性、脆弱性評価、侵入テストなど）の欠如 多くの FMI は、システムに大幅な変更が加えられた後、サイバーレジリエンスのテストが未実施。例えば、FMI の大多数はバックアップデータの整合性をテストせず、一部の FMI は脆弱性評価を実行しておらず、ほとんどの FMI は重大な変更が発生した後の侵入テストが未実施。これは原則 17 の KC2 に関連する FMI の実施結果における乖離または欠点であり、対処が必要
3.　包括的なシナリオベースのテストの欠如 複数の FMI が包括的なシナリオベースのテストを実施していない可能性があり、これらの FMI がサイバー攻撃による障害の発生後に復旧して業務を再開する能力を適切に検証しているかどうかが懐疑的。例えば、一部の FMI は、シナリオベースのテスト演習でガバナンス上の取決めをテストしていないと表明。これは、原則 17 の KC6 と比較した FMI の実施結果における乖離または欠点であり、対処が必要
4.　対応策のテストにおけるステークホルダー（FMI 参加者、重要なサービスプロバイダー等）の不十分な関与 一部の FMI には、FMI 参加者が含まれておらず、ほとんどの FMI はサイバーインシデントに関する対応、再開、復旧計画とプロセスのテストに重要なサービスプロバイダーや関連する FMI を含まない。外部関係者からのリスクの特定、監視、管理に関して原則 17 の KC7 を満たす FMI の能力は懐疑的。また、これは原則 17 の KC6 で予見されているように、FMI がサイバーインシデント後に復旧して業務を再開する能力を実証できるかどうかにも影響する可能性があり、いずれも対処すべき懸念事項

（出所）Bank for International Settlements and International Organization of Securities Commissions, “Implementation Monitoring of the PFMI: Level 3 Assessment on Financial Market Infrastructures’ Cyber Resilience,” November 2022、各種資料より野村資本市場研究所作成

Ⅳ　今後の論点

本稿では、金融セクターに対するサイバー攻撃が国内外を問わず頻発するなかで、各国の金融当局や国際機関が金融機関のサイバーレジリエンス強化に取り組む施策を概観した。

日米の金融当局のサイバーレジリエンス及び情報開示強化に関する施策を踏まえると、米国は規制対応が中心だが、日本は金融機関の取り組みを支援することに焦点を当てる傾向にあり、金融機関への関与のスタンスが異なる点が見受けられた。ただし、いずれの金融当局も、各金融機関等を対象とした規制、指針の提示や演習等の実務に即した取り組みを通じて、各金融機関等の業務運営に直接的に影響し得る施策を展開している。

他方、国際機関は、各国・地域の現状分析やそれを踏まえた提言の発信等、国際的なベースラインの底上げを目指す施策が中心である。ただし、国際通貨基金（IMF）が 2023 年 3 月に公表した調査結果によると、新興市場国・発展途上国における中央銀行または監督当局の 56%は、金融セクターを対象とした国家サイバー戦略を確立していないこと等が指摘されており、国際的なベースラインの向上にはさらなる取り組みが求めら

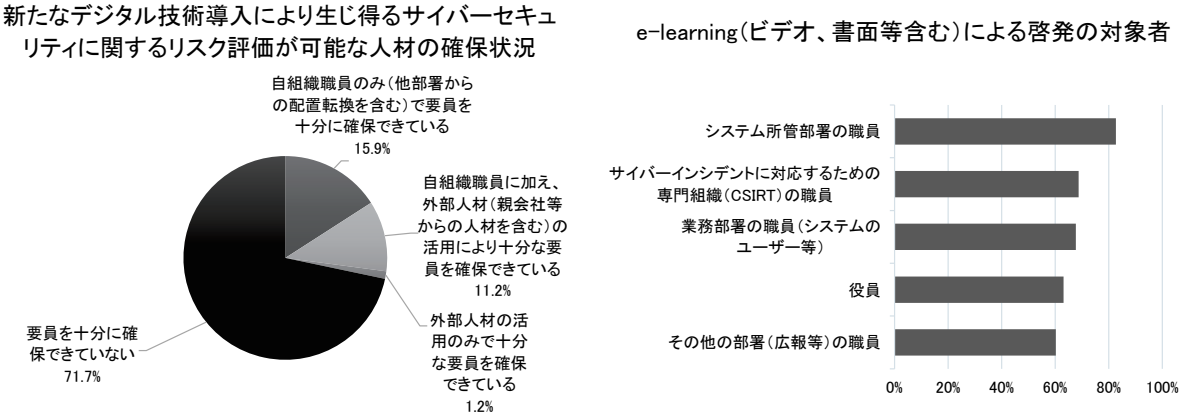
れるとも言える[32]。

既述の日米の金融当局及び各国際機関の施策を踏まえると、今後の金融当局等が取り組むことが求められる点としては、（1）金融機関におけるサイバー人材育成、（2）関連政策との連携、（3）リスクシェアリングの在り方の検討、が挙げられる。

１．金融機関におけるサイバー人材育成

日本では、金融機関におけるサイバー人材育成が、喫緊の課題となっている。例えば、日本銀行及び金融庁が 2023 年 4 月に公表した「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）」では、サイバーリスク評価ができる人材について、7 割強の地域金融機関が十分に確保できていないほか、サイバーセキュリティ人材の育成・強化策である e-learning の対象者もシステム所管部署の職員が相対的に高く、役員やその他の職員については全体の 6～7 割にとどまっていること等が示されている（図表 11 参照）。

図表 11　地域金融機関におけるサイバーセキュリティ人材の確保の態勢



（注）　調査対象は、498 の地域金融機関で、自己評価期間は 2022 年 7～8 月。
（出所）日本銀行金融機構局・金融庁総合政策局「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 月より野村資本市場研究所作成

日本では 2022 年 12 月に閣議決定された「デジタル田園都市国家構想総合戦略」において、サイバーセキュリティ人材を含むデジタル推進人材が量・質ともに不足していることから、2022～2026 年度末までに 230 万人の育成を目指すこととされている。これを受けて、各省庁がサイバーセキュリティ人材育成に向けて様々な取り組みを実施している（図表 12 参照）。金融庁においても、金融分野の人材育成の強化を図るべく、各種取り組みを行っている（図表 13 参照）。

[32] International Monetary Fund, “Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards,” March 2, 2023.

図表 12　サイバーセキュリティの人材確保、育成、活躍推進に関する横断的施策（2023 年度）

1.「DX with Cybersecurity」に必要な人材に係る環境整備
・ 経済産業省 ➢ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）と連携し、「プラス・セキュリティ」の普及における必要な取り組みの調査・検討と、企業・教育機関での先行試行と検証を通じて推進を行う ➢ サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直し ➢ 各人材類型に対応する人材育成プログラムについて「マナビ DX」等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行う ➢ サイバーセキュリティを含む専門的・実践的な教育訓練講座の認定を引き続き実施 ・ 内閣官房 ➢ 引き続き、普及啓発・人材育成施策ポータルサイトへ掲載する人材育成プログラムの募集、プログラムの更なる普及促進策を検討
2. 巧妙化・複雑化する脅威への対処
・ 総務省 ➢ 情報通信研究機構（NICT）のサイバーセキュリティネクサス（CYNEX）を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供し、社会全体でサイバーセキュリティ人材を育成するための基盤の本格運用を開始 ・ 経済産業省 ➢ 引き続き、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む ➢ 若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的として、「セキュリティ・キャンプ」を開催 ・ 文部科学省 ➢ サイバーセキュリティ人材などを含むデジタル人材の育成に寄与する ・ 厚生労働省 ➢ 2022 年 12 月に閣議決定された「デジタル田園都市国家構想総合戦略」を踏まえ、サイバーセキュリティを含むデジタル推進人材を育成するため、都道府県、民間教育訓練機関等において、サイバーセキュリティに関する公共職業訓練を実施する
3. 政府機関における取り組み
・ 内閣官房及びデジタル庁 ➢ 「デジタル社会の実現に向けた重点計画」に基づき、研修等の見直しを行う

（出所）サイバーセキュリティ戦略本部「サイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画）」2023 年 7 月 4 日より野村資本市場研究所作成

図表 13　金融庁における金融分野の人材育成の強化の取り組み（抜粋）

金融庁は、経営層、実務担当者層など、幅広い階層における人材育成を促進するため、財務（支）局、金融 ISAC、金融情報システムセンター（FISC）、その他の業界団体等が主催するセミナーに講師を派遣し、サイバーセキュリティの強化に関する講演を行った。また、振り込め詐欺やインターネットバンキング不正送金などの金融犯罪撲滅に向けた取組みとして、都道府県警察、財務（支）局、地域金融機関及び業界団体と連携して会議を実施し、最新の犯罪手口や防犯への取組事例等について知見の共有を図った

（出所）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 月より野村資本市場研究所作成

今後もサイバーリスクの脅威が高まり続けかねないことを踏まえると、政府による取り組みの継続もさることながら、産業界、学術界等との連携もカギになると考えられる。例えば、米国のホワイトハウスが 2023 年 7 月に公表した「国家サイバー人材教育戦略」[33]では、産官学の様々な団体がコミットメントを表明しており、連携等も通じて人材育成効果がどのように高まるかが注目される。

２．関連政策との連携

サイバーセキュリティは、複数の政策分野と直接的・間接的に関係し得る。公的部門の限られたリソースを踏まえると、関連政策分野と連携し、相乗効果を模索することも重要と言える。

例えば、サイバーセキュリティと同様に、情報化社会が進展する中で論点となっている人工知能（AI）をめぐって、IMF は、AI の導入が、サイバー脅威の範囲を拡大し、新たな特有のサイバーリスクをもたらすと指摘している[34]。一方、英国政府は、AI のパターン認識と再帰的学習機能は、悪意のある者に対する積極的なサイバー防御においてますます重要な役割を果たす可能性が高いとして、AI によるサイバーセキュリティ能力の強化に言及している[35]。

日本では、政府の AI 戦略会議が 2023 年 5 月に取りまとめた「AI に関する暫定的な論点整理」において、（1）「AI がサイバー攻撃に使われる事例の類型等について情報を収集し、必要に応じ周知するなどの対策を検討すべきではないか」、（2）「AI を用いてセキュリティ対策を向上させることも必要ではないか」、等の論点を提起している[36]。

サイバーセキュリティと AI は両方とも今後もますます技術の発展や普及が進むことが想定される分野であり、新しい論点が近い将来に浮き彫りになる可能性もある。本稿では、サイバーセキュリティに関連する分野として AI を取り上げたが、関連政策分野とも連携をし、双方の課題の解決に寄与し、相乗効果の創出を模索することが大切と言える。

---

[33] コミットメントを表明したのは、全米科学財団（NSF）、国家安全保障局（NSA）、国家サイバー局長室（ONCD）、国立標準技術研究所（NIST）、労働省（DOL）、人事管理局（OPM）、退役軍人省（VA）、サイバーセキュリティ・インフラセキュリティ庁（CISA）、住宅都市開発省（HUD）、クレイグ・ニューマーク・フィランソロピー、ウーマン・イン・サイバーセキュリティ（WiCyS）、サイバーセーフ財団、SANS 協会、サイバー準備機構（CRI）とサイバー技術革新センター（CCTI）、ガール・セキュリティ、トレリックス、人的資源管理協会（SHRM）、オミダイヤー・ネットワーク、NPower、タスクフォース・ムーブメント（TFM）、チェック・ポイント・ソフトウェア・テクノロジーズ、ブラック・テック・ストリート、マスベイ・コミュニティ・カレッジ、アクセンチュアとイマーシブ・ラボ、全米サイバーセキュリティ・アライアンス（NCA）、アスペン研究所のサイバーセキュリティ・プログラム、ダコタ州立大学（DSU）、情報技術シニア・マネジメント・フォーラム（ITSMF）、マスターカード、iKeepSafe、ライトキャスト、グーグル、クラウドストライク、マイクロソフト、SAP、コンソル USA、アメリカン大学（The White House, “Factsheet: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America’s Cyber Talent,” July 31, 2023）。

[34] International Monetary Fund, “Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance,” October 22, 2021.

[35] Secretary of State for Science, Innovation and Technology by Command by His Majesty, “Policy Paper: A Pro-innovation Approach to AI Regulation,” Marc 29, 2023.

[36] AI 戦略会議「AI に関する暫定的な論点整理」2023 年 5 月 26 日。

３．リスクシェアリングの在り方の検討

世界のサイバー犯罪による損害額は、2024 年に 9.5 兆ドル、2025 年には 10.5 兆ドルに達するとの試算がある[37]。サイバーセキュリティリスクに起因して発生する様々な損害に対応するための金融商品として、サイバー保険[38]があるが、保険監督者国際機構（IAIS）によると、世界の同保険の元受収入保険料は 2021 年時点で約 137 億ドル（19 ヵ国・地域による報告）に過ぎない[39]。もちろん、企業等は、サイバー保険のさらなる活用を通じて経営に対する影響を軽減することが可能とも考えられるが、サイバーリスクが高まる中、民間の保険会社によるサイバー保険の引受能力にも限界がある。近年は、損害保険会社によるサイバー保険料の引き上げやサイバーCAT ボンドの発行[40]といった動きが見られている。加えて、英国ロイズ保険組合は 2022 年 8 月、ロイズ保険組合は 2023 年 3 月末から損害保険会社の約款に国家の関与によるサイバー攻撃に対する免責条項を明記するよう要請している[41]。

仮に、民間セクターで吸収できない規模の甚大なサイバー被害が顕在化し、国民生活及び社会経済活動に深刻な影響を及ぼしかねないような事態となった場合、官民におけるリスクシェアリングが論点になり得る。例えば、地震保険の場合、地震保険に関する法律に基づいて、政府と民間の損害保険会社が共同で運営を行っており、地震災害による被災者の生活の安定に寄与すべく、一定以上の支払保険金が生じた場合、保険金の一部を政府が負担（政府再保険）する仕組みがある[42]（図表 14 参照）。

IT システムの相互接続性が高まる社会において、金融市場に対するサイバー攻撃が経済社会に甚大な被害をもたらす可能性が否めないことから、その被害への補償を官民で分担する仕組みを構築するといったファイナンスの枠組みの検討も今後、重要になる可能性があると言える。

---

37 サイバーセキュリティ・ベンチャーズによる試算（eSentire, “Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024,” 2023）。

38 サイバー保険に関する詳細については、富永健司「企業のサイバーセキュリティリスクとサイバー保険」『野村サステナビリティクォータリー』2023 年秋号を参照されたい。

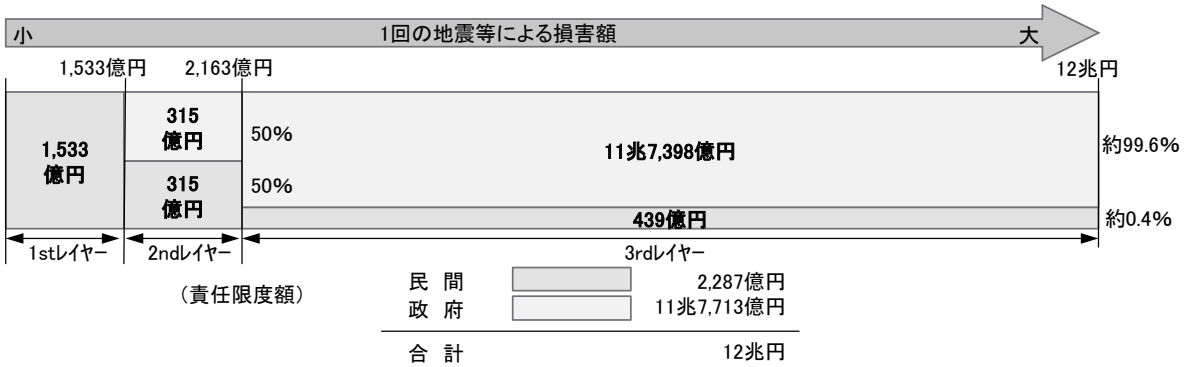
39 International Association of Insurance Supervisors, “Global Insurance Market Report Topic Edition Cyber,” April 2023.

40 英国の損害保険大手ビーズリーは 2023 年 1 月、世界初となるサイバーCAT ボンド（4,500 万ドル）を発行した。3 億ドルを超える大災害が発生した際に、機関投資家の投資資金を保険の支払いに利用できる仕組みである（Beazley, “Beazley Launches Market’s First Cyber Catastrophe Bond,” January 9, 2023）。

41 Lloyds of London, “Market Bulletin: State Backed Cyber-Attack Exclusions,” August 16, 2022.

42 地震保険では、地震・噴火・津波を直接または間接の原因とする火災・損壊・埋没・流出による損害を補償するものである（内閣府「地震保険の概要」第 1 回被災者に対する国の支援のあり方に関する検討会参考資料、2011 年 2 月 3 日）。

図表 14　地震保険再保険スキーム



（注）　1 回の地震等により支払われる保険金の額が 1,533 億円に達するまで（1st レイヤー）は民間が負担。1,533 億円を超え 2,163 億円に達するまで（2nd レイヤー）政府・民間が 50%ずつ負担。2,163 億円を超える部分（3rd レイヤー）については政府がその大半（約 99.6%）を負担。

（出所）日本地震再保険「地震保険再保険スキーム」より野村資本市場研究所作成

【参考資料】

参考資料 1　諸外国における金融関連のサイバーインシデント（2022 年）

業態	社名	発生国	被害内容
銀行	OP Financial Group	フィンランド	サイバー攻撃を受け、サービスが中断
銀行等	ウクライナ政府・国営銀行	ウクライナ	ウクライナ国防省のウェブポータルと複数の大手国営金融機関の銀行・端末サービスが同国を襲った DDoS 攻撃によりダウン
	モスクワ証券取引所／Sberbank	ロシア	DDoS 攻撃を受け、Web サイトがオフライン化
保険	Aon	米国	ランサムウェア攻撃により、多くのサービスに限定的な混乱が発生
貸金	CashMama	インド	データ漏洩を報告し、不正に収集・保存された顧客データが流出
暗号資産	Crypto.com	—	サイバー攻撃を受け、3,500 万ドル相当のビットコインとイーサが不正に引き出され、少なくとも 483 のユーザーアカウントに影響
	Multichain	—	ハッカーがブロックチェーンサービスの脆弱性を悪用し、約 140 万ドルを損失
	Qubit Finance	英国	情報漏洩に見舞われ、脅威アクターは 8,000 万ドル相当の暗号通貨を窃取
	Wormhole	スイス	脅威アクターがプラットフォームのスマートコントラクトの脆弱性を悪用し、推定 3 億 2,200 万ドル相当のイーサ通貨を窃取
	IRA Financial Trust	米国	未知の脅威アクターが IRA 顧客の自己管理型個人退職金口座からビットコインで 2,100 万ドル、イーサリアム 1,500 万ドルを流出させ、暗号通貨 3,600 万ドルを損失
	Ronin	カナダ	過去 2 番目に大きな暗号通貨の強盗となる、6 億 1,500 万ドルのイーサと USD コイントークンを損失
	Beanstalk	米国	暗号通貨の強盗により 1 億 8,000 万ドルを損失
信用調査	TransUnion SA	南アフリカ	サイバー攻撃を受け、約 300 万人の顧客データが犯罪者である第三者によって窃取

（注）　カーネギー国際平和基金が示すサイバーインシデントのうち、2022年に発生した主なインシデントを抽出したものであり、同年に発生した全てのインシデントを網羅するものではない。

（出所）Carnegie Endowment of International Peace, “Timeline of Cyber Incidents Involving Financial Institutions.”、各種資料より野村資本市場研究所作成

参考資料 2　日本の金融機関等を標的としたサイバーインシデント

時期	業態	概要	
2020 年 7 月	証券会社	顧客情報の漏洩（氏名・生年月日・住所等）	・顧客情報管理システムへの不正アクセス ・個人情報 4 千名分が漏洩 ※運転免許証、個人番号カード等の画像データも一部流出
2020 年 8 月	商品先物業者	顧客情報の漏洩（氏名・住所・銀行口座情報、パスワード等）	・Web サイトへの不正アクセス ・オンライントレード口座開設時の入力情報約 3 千件が漏洩
2020 年 9 月	証券会社	不正出金	・何らかの方法で取得したログイン情報を利用してアクセス ・偽装本人確認書類で作成した銀行口座を出金先に変更し、不正に出金 ・被害総額は約 1 億円
2020 年 9 月	資金移動業者	不正出金	・キャッシュレス決済サービスにおける本人認証設計の不備によって不正に預貯金が引き出される ・被害総額は約 3 千万円
2020 年 10 月	保険代理店	顧客情報の漏洩（氏名・生年月日・住所等）	・データ管理システムへの不正アクセス ・攻撃を受けた個人データの総数は 9 万件
2020 年 11 月	暗号資産交換業者	顧客情報の漏洩（電子メールアドレス、氏名、暗号化されたパスワード等）	・ドメイン登録サービスに登録した情報が不正に変更されたことによる、システム・インフラへの不正アクセス ・約 17 万件の情報が漏洩。（他に身分証明書等の本人確認書類約 3 万件も漏洩した可能性あり）
2020年12月～	資金移動業者 銀行等	顧客情報の漏洩（氏名・住所・電話番号等）	・クラウドサービスの設定不備による不正アクセス ・地方自治体及び一般事業者でも発生
2021 年 4 月	証券会社	オンライン取引停止	・オンライントレードシステムへの不正アクセス ・データを暗号化され、現行システムの復旧を断念
2021 年 11 月	信用金庫・信用組合	ウェブサイト	・サイバー攻撃によりウェブサイトの閲覧とウェブサイト経由のオンラインバンキングが利用不可
2021年11月～	保険会社	個人情報の漏洩・不正出金	・フィッシングサイトへ誘導する不審メールが複数の保険会社で発見 ・偽装口座を使用した不正出金被害も発生

（出所）金融庁「金融分野のサイバーセキュリティ強化に向けた取組みについて」2022 年 5 月 11 日より野村資本市場研究所作成