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

江夏　あかね、門倉　朋美

▌要　約▐

1. 米国証券取引委員会（SEC）は2023年3月15日、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つの規則案を公表した。具体的には、（1）市場関連組織をサイバー脅威から保護することを目的とした「規則10」（Rule 10）の制定、（2）主要な市場インフラの強度と回復力強化を目的とした「レギュレーションSCI」の改正、（3）データのプライバシーと顧客情報の保護を目的とした「レギュレーションS-P」の改正、を通じてサイバーセキュリティ関連要件を提案している。
2. 世界的なサイバー攻撃の脅威の増大やG7、G20・金融安定理事会（FSB）等での国際的な議論も鑑みると、米国を含めて当局によるサイバーセキュリティリスクに対する規制・監督が厳格化する方向が近い将来に大きく変わることはないと想定される。
3. 日本でも金融機関に対するサイバー攻撃・犯罪が近年増加しており、2014年11月に制定されたサイバーセキュリティ基本法も受け、金融庁が金融分野におけるサイバーセキュリティ取組方針の策定等、様々な対応を行っている。
4. 日本の証券業界については、米国でビジネスを行っている証券会社のみならず、それ以外の証券会社あるいはインフラ運営者についても、顧客基盤や企業価値保全の観点からサイバーセキュリティ対策を強化することが喫緊の課題となろう。一方で、サイバー攻撃の複雑性や甚大な経済的インパクトを考慮すると、民間事業者が実行可能な対策や負担できるコストには限界があり、官民一体で検討を進めることが重要と言える。

野村資本市場研究所　関連論文等

・江夏あかね「機関投資家から見たサイバーセキュリティーサステナブルな情報化社会実現に向けた論点整理ー」『野村サステナビリティクォータリー』第3巻第4号（2022年秋号）。
・淵田康之「サイバーリスクと金融規制」『野村資本市場クォータリー』第23巻第2号（2019年秋号）。

Ⅰ　米国証券市場関連組織に焦点を当てた規則案

米国証券取引委員会（SEC）は 2023 年 3 月 15 日、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べく、3 つの規則案を公表した[1]。

情報化社会が急速に発展し、サイバーセキュリティリスクへの脅威が世界的に高まる中、SEC では 2010 年代に入る頃から、企業、ブローカー・ディーラー、投資アドバイザー、ファンド等に対して、リスク管理や情報開示を促すべく様々な取り組みを続けてきた[2]。SEC が今般公表した規則案は、米国のブローカー・ディーラーや証券取引所といった市場インフラ運営者と市場参加者に焦点を当てたものである。具体的には、（1）市場関連組織をサイバー脅威から保護することを目的とした「規則 10」（Rule 10）の制定、（2）主要な市場インフラの強度と回復力強化を目的とした「レギュレーション SCI」の改正、（3）データのプライバシーと顧客情報の保護を目的とした「レギュレーション S-P」の改正、という形で、サイバーセキュリティ関連要件を提案している[3]。

Ⅱ　証券市場が直面するサイバー関連の脅威（規則案の背景）

米国の証券市場は 100 兆ドルを超える規模を有し、日々1 兆ドル以上の取引が行われている[4]。サイバーセキュリティー・インフラセキュリティー庁（CISA）は、2013 年 2 月に発令された大統領令等[5]に基づき、証券市場を含めた金融サービスセクターを 16 の重要インフラセクターの 1 つと位置付けている[6]。

一方で、サイバー犯罪や攻撃が複雑化・巧妙化する中、SEC は 2010 年代半ば頃から証券市場や市場関連組織にも焦点を当てて、（1）規則の制定・改正、（2）監査の充実化、

---

1 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.

2 SEC による企業に対する適切なサイバーセキュリティ関連情報開示を促すための取り組みの詳細は、江夏あかね「機関投資家から見たサイバーセキュリティ―サステナブルな情報化社会実現に向けた論点整理―」『野村サステナビリティクォータリー』第 3 巻第 4 号（2022 年秋号）、を参照されたい。

3 U.S. Securities and Exchange Commission, “Statement on Amendments to Regulation S-P, Cybersecurity Risk Management, and Amendments to Regulation SCI - Commissioner Caroline A. Crenshaw,” March 15, 2023.

4 U.S. Securities and Exchange Commission, “17 CFR Parts 232, 240, 242 and 249 [Release No. 34-97142; File No. S7-06-23] RIN 3235-AN15: Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents,” March 15, 2023.

5 大統領令第 13636 号「重要インフラのサイバーセキュリティ強化に関する大統領令」、大統領令政策指令第 21 号「重要インフラセキュリティと強靭化に関する大統領政策指令」（2013 年 2 月 12 日発令）

6 重要インフラセクターとは、その資産、システム、ネットワークが物理的か仮想的かを問わず、米国にとって極めて重要と考えられており、その無力化または破壊は、安全保障、国家経済の保障、国家の公衆衛生または安全、またはこれらのあらゆる組み合わせに弱体化をもたらす可能性のあるセクターを指す。（Cybersecurity & Infrastructure Security Agency, “Critical Infrastructure Sectors”）

（3）エンフォースメント（課徴金等）の実施、（4）SEC自身の組織体制の拡充、などの対応を進めてきた（図表1参照）。

図表1　米国におけるサイバーセキュリティリスク関連の主なインシデントとSECの対応

時期	詳細
2000年11月	レギュレーションS-P施行
2011年10月	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あり方に関するガイダンスを公表
2014年4月	登録ブローカー・ディーラーや投資アドバイザーに対してSEC内のコンプライアンス検査局（OCIE）によるサイバーセキュリティ保護の対応状況の監査を実施する旨を公表
2014年11月	レギュレーションSCI採択
2015年2月	OCIE、サイバーセキュリティ保護の監査において発見された見解事項をまとめたリスク警告文書を公表
2017年9月	SEC、前年に、適時開示情報システム「エドガー」への不正アクセスがあったことを公表
2017年9月	SEC、サイバーベースの脅威に対して個人投資家を保護することを目的に、サイバー関連を対象とするサイバー部門と、個人投資家に直接影響を与えるイニシアティブを実施するリテール戦略タスクフォースの創設を公表
2018年2月	SEC、上場企業のサイバーセキュリティ関連情報開示に関する声明及び解釈ガイダンスを採択
2018年4月	SEC、アルタバ（前・ヤフー!）が数億件に及ぶユーザーアカウントのデータ流出事件を公表せずに投資家を欺いたとして、3,500万ドルの課徴金を支払うことに合意した旨を公表
2018年9月	SEC、ブローカー・ディーラー及び投資アドバイザーであるボヤ・フィナンシャル・アドバイザーズが、数千人の顧客の個人情報を危険に晒すサイバー犯罪者による侵入をめぐり、サイバーセキュリティのポリシーの不備及び不適切な手順に関して、100万ドルを支払うことに合意した旨を公表
2018年10月	SEC、サイバー詐欺の被害に伴い数百万ドルの損失を出した9つの上場企業の調査に基づく報告書を公表。上場企業が内部会計管理を実施する際にサイバーの脅威を考慮すべきと警告
2019年2月	SEC、データ管理及びサイバーセキュリティの観点から、投資登録会社が作成する投資ポートフォリオ投資レポート（N-PORT）の提出期限を変更すると発表。従来の毎月末から30日以内より、新たに四半期末から60日以内に変更
2020年1月	OCIE、サイバーセキュリティと回復力対策に関する検査所見を公表
2021年6月	SEC、不動産決済サービス会社のファースト・アメリカン・ファイナンシャル・コーポレーションを、機密性の高い顧客情報を公開したことに伴う開示統制違反などで提訴し、同社が487,616ドルの課徴金を支払うことで和解
2021年8月	SEC、英国の教育出版企業のピアソンが2018年に数百万人の学生の個人情報の窃盗を含むサイバー侵入について投資家を欺き、開示統制や手順が不十分であったとして、100万ドルを支払うことで和解した旨を公表
2022年2月	SEC、登録投資アドバイザーとファンドのサイバーセキュリティリスク管理規則と修正案を提案
2022年2月	SEC、上場企業によるサイバーセキュリティリスク管理、戦略、ガバナンス、インシデント開示に関する規則案を公表
2022年3月	SECの投資家諮問委員会、人工知能（AI）とサイバーセキュリティに関して協議。同委員会は、調査結果と勧告をSECに提出する権限を有する
2022年5月	SEC、暗号資産市場の投資家をサイバー関連の脅威から保護する責任を負う、法執行局の暗号資産及びサイバーユニットの人員を20名増員する旨を公表
2023年3月	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べく、3つの規則案を公表
2023年3月	SEC、2022年2月に公表したサイバーセキュリティリスク管理規則案と登録投資アドバイザーとファンドの修正案のコメント期間を再開。当初のコメント期間は2022年4月11日に終了したが、新たな期間は連邦官報に再掲載された日から60日後で設定

（出所）米国証券取引委員会（SEC）のプレスリリースのヘッドラインでサイバーと記されているものを中心に抽出。
（出所）U.S. Securities and Exchange Commissionのウェブページ、より野村資本市場研究所作成

SEC による対応経緯を見ると、2010 年代半ば頃までは、各種規則を制定しつつ、ブローカー・ディーラーや投資アドバイザー等の市場インフラ運営者・参加者におけるサイバーセキュリティリスク保護状況の監査を実施し、市場インフラ運営者・参加者自身の規律強化を促すスタンスを採っていたが、その後はエンフォースメントも実施するようになった。2020 年代に入って、上記の対応に加えて SEC の組織体制の強化や、従来の規制・監督の範疇となっていない部分を補完すべく、今般の新たな規則案の制定・改正に至ったと解釈される。

今回の規則案の背景としては、（1）情報システムへの依存度の高まり、（2）情報システムの相互接続性の広がり、（3）証券ビジネス・取引慣行の変化によって、証券市場への脅威が変容し高まっていること、が考えられる。

１．情報システムへの依存度の高まり

証券市場インフラ運営者・参加者は従来、様々な機能を情報システム（電子情報、通信、コンピューターのシステム）に依存してきた。近年は、フィンテックの導入やアプリの開発等を通じて、ユーザーの利便性向上が図られる一方で、市場関連組織側では業務効率化やコスト削減を進める動きが加速しており、非対面コミュニケーションの重要性が高まると同時に、注文処理・決済などにおける情報システムの依存度が高まっている。加えて、2020 年から世界的大流行となった新型コロナウイルス感染症問題も、デジタル化やリモートワーク対応などを通じて情報システムへの依存度増大を促したと言える。

このような状況下、サイバーインシデントの多様化と増加が進んでいる。証券業界の事業者が顧客情報保護を不適切に管理したこともあり、サイバー攻撃により、多数の顧客情報が流出する事案が散見されている（図表 2 参照）。

仮に、流失した顧客情報が不正利用された場合、（1）顧客にとっては各種資産の毀損、（2）攻撃を受けた事業者にとっては風評リスク、情報を盗まれた個人による訴訟関連費用、当局による課徴金といったネガティブな影響、（3）証券市場全体の信頼失墜や機能不全といった負の連鎖が起きかねない。その意味で、SEC による早急な対応が求められる局面にあったと考えられる。

図表2　米国証券業界における顧客情報保護の不適切な管理に関する主な事例

事業者	内容
モルガンスタンレー・スミスバーニー	顧客データを保護するために合理的に設計された書面による方針と手順を採用せず、2011年から2014年にかけて、当時の従業員が約73万件のアカウントに関するデータに許可なくアクセスし、個人のサーバーに転送し、最終的に第三者にハッキングされた。同社とSECは2016年6月、100万ドルの課徴金を支払うことで合意
ケンブリッジ・インベストメント・リサーチ、ケンブリッジ・インベストメント・リサーチ・アドバイザーズ	顧客データを保護するために合理的に設計された書面による方針と手順を採用せず、2018年1月から2021年7月1日にかけて、121人以上のケンブリッジの証券営業員のメールアカウントが第三者によって乗っ取られた。少なくとも2,177人の個人識別情報が漏洩し、それとは別にさらに3,800人の個人識別情報が漏洩する可能性が生じた。当該2社とSECは2021年8月、25万ドルの課徴金を支払うことで合意
セテラ・アドバイザー・ネットワークス、セテラ・インベストメント・サービス、他3社	顧客データを保護するために合理的に設計された書面による方針と手順を採用せず、2017年11月から2020年6月にかけて、従業員60人以上のメールアカウントが第三者によって乗っ取られ、個人識別情報4,388件以上が漏洩した。当該5社とSECは2021年8月、30万ドルの課徴金を支払うことで合意
KMSファイナンシャルサービス	顧客データを保護するために合理的に設計された書面による方針と手順を採用せず、2018年9月から2019年12月にかけて、同社のファイナンシャルアドバイザー15人のメールアカウントが第三者によってアクセスされ、約4,900人の顧客データが漏洩した。同社とSECは2021年8月、20万ドルの課徴金を支払うことで合意

（出所）U.S. Securities and Exchange Commission, “Statement on Amendments to Regulation S-P, Cybersecurity Risk Management, and Amendments to Regulation SCI - Commissioner Caroline A. Crenshaw,” March 15, 2023、各種資料、より野村資本市場研究所作成

２．情報システムの相互接続性の広がり

米国連邦準備制度理事会（FRB）は、金融システムの相互接続性を「ドミノ効果」と呼び、ある金融機関でサイバーインシデントが発生すると、その金融機関の送金能力が中断され、他の金融機関の流動性や業務に連鎖的な影響を及ぼすといった例を挙げて問題視している[7]。国際決済銀行（BIS）及び証券監督者国際機構（IOSCO）も、金融市場インフラ（FMI）にとってサイバー攻撃を受ける可能性のある侵入点は、FMI自身のみならず、相互接続性により、接続された別のFMI、サービス提供者、ベンダー、ベンダーの製品等、幅広い範囲になると指摘している[8]。そして、例えば、FMIがマルウェア[9]に感染した場合、FMI自体が相互接続された組織へのマルウェアの配布を通じて、サイバー攻撃をさらに伝播するチャンネルになるとも述べている。

このような情報システムの相互接続性に伴う問題は、国境を越えて米国金融市場にも影響を及ぼしている。例えば、英国のソフトウェア会社IONトレーディングUKに対するランサムウェア（身代金要求型のウイルス）による攻撃の事案は、記憶に新しい[10]。2023年

[7] FRBは、ドミノ効果を1つまたは複数の企業での事象が他の企業に波及する可能性と説明している。（Board of Governors of the Federal Reserve System, “Implications of Cyber Risk for Financial Stability,” May 12, 2022）

[8] Bank for International Settlements and International Organization of Securities Commissions, “Guidance on Cyber Resilience for Financial Market Infrastructures,” June 2016.

[9] マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコード。（総務省「令和2年版 情報通信白書」2020年8月）

[10] 「ION へのサイバー攻撃、金融システミックリスクとならず－米財務省」『ブルームバーグ』2023年2月2日、「米CFTCの建玉データ公表延期、データ会社IONにランサム攻撃」『ロイター』2023年2月2日。

1 月、株式や債券、商品市場でデリバティブ取引を完了するために使用されている同社のソフトウェアが停止した。同社の顧客企業は、売買を手作業で処理せざるを得なくなり、追加証拠金請求（マージンコール）の計算や大口ポジションに関する規制当局への報告等で不可欠な作業が困難となった結果、取引所や規制当局のデリバティブ取引活動に関する週次レポートが期日通りに作成できなくなった。同社の顧客企業には、英国のみならず欧米の複数の銀行や証券会社も含まれていたことから、米国商品先物取引委員会（CFTC）が週次の建玉明細データの公表を延期せざるを得なくなるなど、米国金融市場にも大きな混乱が発生した[11]。

情報システムの相互接続が広がる中、従来の規制監督では想定されなかったサイバーセキュリティリスクが広範囲で顕在化する状況となり、SEC 内部でも危機感が強まっていたとみられる。

３．証券ビジネスや取引慣行の変化

米国証券市場のビジネスや取引慣行も、技術の進歩とともに変化している。証券ビジネスについては、例えば、ブローカー・ディーラーが近年、アルゴリズム取引[12]を用いた収益性の確保、電子的な手法も用いた顧客関係管理に取り組むようになった[13]。

取引慣行をめぐって、米国の債券市場では、株式市場に比して自動化と電子取引への依存度が低く、手動（電話等）でディーラー間やディーラーと顧客の交渉が行われていることが多いものの、近年は電子的に行われる場面が増える傾向にある[14]。また、米国には店頭取引の一形態として、証券会社等が運営する電子取引システムを通じて取引所のように有価証券の取引ができる仕組みである代替的取引システム（ATS）が存在するが、地方債市場では ATS による取引数が 2015 年から 2021 年にかけて 3 倍以上に増加し、日次平均取引量も大幅に拡大している[15]。そのため、後述の「レギュレーション SCI」の制定当初、社債や地方債を取引する ATS は適用対象外だったが、現在の取引慣行に必ずしも適した状態にはなっていないと考えられている[16]。

このように、米国証券市場では近年、システムの電子化や高速化により、取引量が増加

[11] Commodity Futures Trading Commission, “CFTC Statement on ION and the Impact to the Derivatives Markets,” February 2, 2023; Commodity Futures Trading Commission, “CFTC Issues Statement on the Ongoing Impact to Reporting,” February 10, 2023.

[12] アルゴリズム取引は、コンピューターシステムが株価や出来高等に応じて、自動的に株式売買注文のタイミングや数量を決めて注文を繰り返す取引のこと。

[13] Greenwich Associates, “All-to-All Trading Takes Hold in Corporate Bonds: Q2 2021,” 2021.

[14] 前掲脚注 13 を参照。

[15] Municipal Securities Rulemaking Board, “Customer Trading with Alternative Trading Systems,” August 2022.

[16] 前掲脚注 3 を参照。

する傾向が見られており、過去にあったような市場のクラッシュや混乱[17]を起こさないように、市場インフラの強度や回復力をさらに強化する必要があったとみられる。

SECは、情報システムへの依存度の高まりや相互接続性の広がり、証券ビジネス・取引慣行の変化等を背景に顕在化していた米国証券市場のサイバーセキュリティリスクへの脆弱性に対処すべく、今般のサイバーセキュリティリスクへの対処に関する規則案の制定・改正に取り組んだと解釈される。

Ⅲ 3つの規則案の対象範囲と狙い

SECが公表した米国証券市場の特定の関連組織を対象とした一連の規則案は、（1）サイバーセキュリティリスク管理に関する「規則10」（Rule 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、で構成されている。いずれもサイバーインシデントに対する組織の備えと対応を改善するために策定された提案という意味で共通しているが[18]、対象組織については新たに制定された「規則10」が最も広範囲になっている（図表3参照）。また、「レギュレーションSCI」の改正については市場インフラ、「レギュレーションS-P」の改正については顧客情報を取り扱うブローカー・ディーラー等に焦点を当てた内容が示されている。

図表3　SECによる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、主要証券派生スワップ参加者、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情報開示を要請等	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	連邦政府レベルで顧客情報保護を強化等

（出所）各種資料、より野村資本市場研究所作成

[17] 例えば、SECのキャロライン・クレンショー委員は、米国証券市場における過去のクラッシュや混乱の事例として、（1）2010年5月のフラッシュクラッシュ（ダウ工業株30種平均が2010年5月6日に数分間で約9%下落し、取引時間中に過去最大の下げ幅を記録）、（2）2012年5月のフェイスブック（現・メタ）のNASDAQ市場への新規株式公開（IPO）時のシステム不具合による取引遅延や障害に伴う混乱、（3）2012年10月の大型ハリケーン・サンディの米国東海岸への上陸によるニューヨーク証券取引所の2日間の閉鎖及び取引停止、を挙げている。（U.S. Securities and Exchange Commission, “Statement on Amendments to Regulation S-P, Cybersecurity Risk Management, and Amendments to Regulation SCI - Commissioner Caroline A. Crenshaw,” March 15, 2023）

[18] Chapman and Cutler LLP, “SEC Proposes Enhanced Cybersecurity Regulations for Financial Industry,” March 22, 2023.

１．サイバーセキュリティリスク管理に関する「規則 10」の制定

「規則 10」は、1934 年証券取引所法[19]に基づき新たに提案されたもので、投資家と市場を保護するためにサイバーセキュリティリスク管理を強化することを目的としている[20]。

同規則の対象組織は、前述のとおり、ブローカー・ディーラー、清算機関、証券取引所、金融業規制機構（FINRA）等、「レギュレーション SCI」や「レギュレーション S-P」に比して広範囲となっている。対象組織に課される主な要件は、（1）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、（2）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、（3）組織に重大な影響を与える可能性のあるサイバーセキュリティリスクの概要と該当年及び前年の重大なサイバーインシデントの概要の一般への開示、である[21]（図表 4 参照）。

SEC のゲイリー・ゲンスラー委員長は、SEC が「規則 10」を制定した意図について、市場関連組織におけるサイバーセキュリティ慣行の基準として、投資家保護と市場の秩序を維持するという SEC の使命を果たすためと述べた[22]。加えて、同規則の主な狙いとしては、（1）サイバーセキュリティリスクの高まりの中で投資家、発行体、市場参加者がデジタル時代に適した保護が行われていることを認識できるため、米国証券市場の信認の確保につながる、（2）情報開示の拡充を通じて、投資家が自身の資金管理、データ及び個人情報をどの企業に委託するかを検討、選択する際に必要な情報を得ることができる、等が挙げられた。

---

[19] 1934 年証券取引所法は、米国における証券の流通市場を規制すべく、1934 年 6 月に制定された連邦制定法。同法に基づき設立された SEC に証券業界に関する幅広い権限が与えられている。具体的には、証券会社、証券代行業者、清算機関及び国内の証券自主規制機関（SRO）の登録、規制及び監督する権限や、上場証券を保有する企業による定期的な情報報告を要求する権限等が含まれる。（U.S. Securities and Exchange Commission, “The Laws That Govern the Securities Industry”）

[20] 前掲脚注 3 を参照。

[21] U.S. Securities and Exchange Commission, “Statement on Enhanced Cyber Security for Market Entities - Chair Gary Gensler,” March 15, 2023.

[22] U.S. Securities and Exchange Commission, “SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets,” March 15, 2023.

図表4　「規則10」の概要

項目	詳細
目的	サイバーセキュリティインシデントの有害な影響から、市場事業体と投資家を保護する措置を要求し、サイバーセキュリティインシデントのリスクに対処し、軽減させること
対象組織（市場事業体）	ブローカー・ディーラー、地方債規則制定委員会（MSRB）、清算機関、主要証券派生スワップ参加者、金融業規制機構（FINRA）、登録証券取引所、証券派生スワップデータデポジトリ、証券派生スワップディーラー、トランスファー・エージェント
要件	全ての市場事業体に対する要件 ・ サイバーセキュリティリスク(注1)に対処するために、合理的に設計された書面による方針と手順の確立、維持、実施の義務付け ・ 少なくとも年1回、当該方針及び手順の設計・有効性の見直しと評価の義務付け（対象期間中のサイバーセキュリティリスクの変化を反映しているかを含めて） ・ 重大なサイバーセキュリティインシデントが発生した、または発生していると結論付ける合理的な根拠がある場合、SECに対して直ちに書面による電子通知の提出が必要 対象事業体(注2)に対する追加要件 1. サイバーセキュリティリスクに対処するための方針と手順の採用について、下記の事項を含む ・ 対象事業体の情報システムに関連するサイバーセキュリティリスクの定期的な評価及びリスク評価の文書化 ・ ユーザー関連のリスクを最小化し、対象事業体の情報システムへの不正アクセスを防止するために構築された統制 ・ 対象事業体の情報システムを監視し、不正なアクセスまたは使用から情報を保護するための対策と、情報を受領、保持、処理するサービスプロバイダー、または対象事業体の情報システムへのアクセスを許可されているサービスプロバイダーの監督 ・ 対象事業体の情報システムに関するサイバーセキュリティの脅威及び脆弱性を検出、軽減、修復するための措置 ・ サイバーセキュリティインシデントの検出、対応、復旧のための対策とサイバーセキュリティインシデントの対応、復旧のための文書作成手順 2. 対象事業体は、重大なサイバーセキュリティインシデントの書面による電子通知を直ちに提出した後、新たに提案されたフォームSCIR(注3)のパートIの提出を通じて、SECに報告し、重大なサイバーセキュリティインシデントに関する情報の更新が必要となる 3. 対象事業体は、フォームSCIRのパートⅡにおいて、サイバーセキュリティリスクと、当年または前年の暦年に経験した重大なサイバーセキュリティインシデントの概要説明を公に開示する必要がある。対象事業体は、フォームSCIRのパートⅡをSECに提出し、ウェブサイトに掲載する必要がある。また、ブローカー・ディーラーを採用または紹介する対象事業体は、口座開設時、フォームの更新時と毎年、顧客にフォームSCIRのパートⅡを提供する必要がある
今後の予定	規則案は連邦官報に公示。パブリックコメントは公示日から60日間受け付け

（注）　1. サイバーセキュリティインシデント、サイバーセキュリティ脅威、サイバーセキュリティ脆弱性に起因し得る財務、運営、法律、評判に関する、またその他の悪影響と定義付けられている。
2.「対象組織」（市場事業体）から特定の種類の小規模ブローカー・ディーラーを除く。
3. サイバーセキュリティリスクに関する情報を適切に開示するための、規則10の関連フォーム。パートIとIIに分かれており、それぞれSECへの提出やウェブサイトへの掲載等が義務付けられている。

（出所）U.S. Securities and Exchange Commission, “Factsheet- Addressing Cybersecurity Risks to the U.S. Securities Markets,” March 15, 2023、より野村資本市場研究所作成

2．「レギュレーションSCI」の改正

「レギュレーションSCI」は、証券取引所、清算機関等を対象にシステム障害の発生の抑制、問題発生時の回復力の向上、証券市場技術インフラに対するSECの監督と執行の強化を柱として、2014年11月に採択された規制である[23]。SCIは、システム・コンプライアンス（法令順守）・アンド・インテグリティ（整合性）の頭文字であり、対象組織に対して、

[23] U.S. Securities and Exchange Commission, “Spotlight on Regulation SCI.”

システム障害を防止するための対策の構築を義務付けているほか、万一障害が起きた場合の対応策を明確にするとともに、SEC や市場参加者への迅速な報告も要請するものである。同レギュレーションの存在は、取引量の急激な増加や市場のボラティリティの高まりによるクラッシュや混乱を回避し、機能を回復するのに一定程度寄与してきたとの見方もある[24]。

その一方で、レギュレーション SCI が制定されて以降、テクノロジーが急速に進化し、市場のデジタル化、クラウドやオープン API[25]の活用が劇的に増加している。加えて、市場における相互接続性が高まっており、特定の市場関連組織をレギュレーション SCI の対象から排除することが難しくなってきた。そのため、レギュレーション SCI の対象組織の範囲として、従来から含まれていた証券取引所や清算機関に加え、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・リポジトリ（SDR）[26]及び SEC の登録免除清算機関[27]を含める形で改正が提案された（図表 5 参照）。特に、ゲンスラー委員長は、今回追加される範囲の中心を構成するブローカー・ディーラーについて、仮に（サイバー攻撃等の）技術的イベントに伴う影響を受けた場合、市場の秩序の維持が困難となると共に効率的な運営を妨げる可能性があるため、回復力を強化することが重要と指摘した[28]。

上記の対象組織に課される主な要件は、（1）「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、（2）システム侵入被害を遅滞なく、SEC に報告、（3）事業継続・災害復旧（BC/DR）計画に主要なサードパーティ・プロバイダーを含める、等である。

すなわち、同規則改正案は、「レギュレーション SCI」制定後の技術進化や取引慣行の変化、相互接続性の高まりを踏まえて、米国証券市場のインフラを担う組織や情報システムの能力及び回復力を確保することを目指し、規則の対象範囲を拡充するとともに、対象組織の情報システム管理体制を厳格化することを意図したと考えられる。

---

[24] U.S. Securities and Exchange Commission, “Statement on Amendments to Regulation S-P, Cybersecurity Risk Management, and Amendments to Regulation SCI - Commissioner Caroline A. Crenshaw,” March 15, 2023; Financial Industry Regulatory Authority, “Market Structure & COVID-19: Handling Increased Volatility and Volumes,” April 28, 2020.

[25] アプリケーション・プログラミング・インターフェース（API）は、あるアプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様・仕組みを指す。それを他の企業等に公開することを「オープン API」と呼ぶ。金融機関によるオープン API は、金融機関と外部の事業者との間の安全なデータ連携を可能にする取り組みである。金融機関がシステムへの接続仕様を外部の事業者に公開し、あらかじめ契約を結んだ外部事業者のアクセスを認めることで、金融機関以外の事業者が金融機関と連携して、相互に知恵を絞り、利便性の高い高度な金融サービスを展開しやすくなる。（全国銀行協会「オープン API って何？」）

[26] スワップデータリポジトリ（SDR）は、ドッド・フランク法によって作成された新しい組織であり、スワップデータの報告と記録管理のための中心的な機能を提供する。同法の下で、全てのスワップ取引は清算されたか否かに関わらず、登録された SDR に報告する必要がある。（Commodity Futures Trading Commission, “Data Repositories”）

[27] 1934 年証券取引所法は、事業体が清算機関（Clearing Agency）の機能を実行する前に、SEC に登録するか、登録の免除を受けることを要求している。登録に当たっては、SEC による許可が必要である。登録清算機関は、セントラルカウンターパーティ（CCP）及び中央証券保管機関（CSD）の機能を担う。SEC から登録が免除されている清算機関は、クリアストリームバンク、DTCC ITP マッチング、ブルームバーグ STP、SS&C テクノロジーズ、ユーロクリアバンクである。（U.S. Securities and Exchange Commission, “Clearing Agencies”）

[28] U.S. Securities and Exchange Commission, “Statement on Amendments to Regulation SCI - Chair Gary Gensler,” March 15, 2023.

図表 5　「レギュレーション SCI」の改正案の概要

項目	詳細
目的	レギュレーション SCI の導入以降の技術と取引の進化を考慮し、米国証券市場の技術インフラのキャパシティ、インテグリティ、回復力、可用性、安全性を引き続き確保すること
対象組織	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）、全米市場システム（NMS）の株式及び非 NMS 株式のうち出来高基準を満たす代替的取引システム（ATS）、一定の統合された市場データの独占提供者、一定の基準を満たした統合市場データ提供者、登録免除清算機関
要件	対象組織の範囲拡大 ・ SEC に登録されたブローカー・ディーラーで、NMS 株式、上場オプション、米国財務省証券またはエージェンシー証券に係る総資産閾値または取引アクティビティの閾値を超える組織 ・ 登録されたセキュリティベースのスワップ・データ・リポジトリ（SDR） ・ 登録免除清算機関 レギュレーション SCI の強化・拡充 ・ SCI 対象組織における下記の点に関する必要な方針と手順の特定 ➢ SCI システム(注 1)と間接 SCI システム(注 2)の在庫、分類、ライフサイクル管理プログラム ➢ SCI または間接 SCI システムを提供またはサポートする、クラウドサービスプロバイダーを含むサードパーティ・プロバイダーを管理及び監督するプログラム ➢ 重要な SCI システムに重大な影響を与えるサードパーティ・プロバイダーが利用できない場合に対処する事業継続・災害復旧（BC/DR）計画 ➢ SCI システム及びその情報への不正アクセスを防止するプログラム ➢ 対象組織の方針と手順について、現行の SCI 業界標準と整合性があるか確認 ・ 「システム侵入」の定義を、特定の分散型サービス拒否攻撃等のサイバーセキュリティイベントを捕捉することを目的とした、追加の種類のサイバーイベント及び脅威を含むように修正。システム侵入被害を遅滞なく、SEC に通知することを要求 ・ 対象システムのリスク、内部統制の設計と運用の有効性及びサードパーティ・プロバイダーの管理リスクとコントロールを客観的主体が評価し、少なくとも年 1 回のペネトレーションテスト（ネットワークに接続されたシステムの安全性を検証するテスト）が必要であることを明記すべく、SCI レビュー(注 3)を更新 ・ SCI 対象組織が BC/DR の年次テストに主要なサードパーティ・プロバイダーを含めることを明記 ・ レギュレーション SCI の記録保持規定及びフォーム SCI をこれらの改訂に合わせて更新
今後の予定	規則案は連邦官報に公示。パブリックコメントは公示日から 60 日間受け付け

（注）　1. SCI システムとは、証券に係る取引、清算及び決済、注文ルーティング、市場データ、市場規制または市場監視を直接支援する SCI 対象組織等により運営される全てのコンピューター、ネットワーク、電子的・技術的なシステム等を指す。
2. 間接 SCI システムとは、ハッカー等にシステムが侵害された場合に、SCI システムにセキュリティ上の脅威をもたらす可能性が合理的に高い、SCI 対象組織のシステム等を指す。
3. SCI レビューとは、確立された手順と基準に従って、SCI システムと間接 SCI システムのレビューを実施するための適切な経験を持つ客観的な担当者によって行われるレビューを指す。

（出所）U.S. Securities and Exchange Commission, “Factsheet- Regulation SCI: Proposed Expansion and Updates,” March 15, 2023、より野村資本市場研究所作成

３．「レギュレーション S-P」の改正

「レギュレーション S-P」は、個人の顧客情報の取り扱いと保護に対処すべく、グラム・リーチ・ブライリー法[29]に基づき、2000 年 11 月に施行された規則である[30]。同規則は、（1）ブローカー・ディーラー、投資信託及び登録投資顧問業者に対して、顧客の記録及び情報の保護に関する方針及び手順を書面で採択することを求める（セーフガード規則）、（2）顧客レポートに掲載される情報の適切な廃棄を求める（廃棄規則）、が柱となっている。

本規制が制定された頃から、データ侵害の性質、規模、影響は大きく変化し、図表 2 におけるモルガンスタンレー・スミスバーニー事案のように、個人情報の流出が大幅に増加している[31]。そのため、顧客情報保護を強化すべく、レギュレーション S-P を、主に 4 つの側面から改正することが提案された（図表 6 参照）。

1 点目として、対象組織に対して、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を義務付ける。現行の規則では、対象企業は個人の財務データの使用方法について顧客に通知する必要があるが、違反について顧客に通知することは義務付けられていない。

2 点目として、対象企業は、データ等の侵害が発生した際に適切に識別できるようにするために、機密性の高い顧客データがアクセスされたか否かを監視して検出する必要があるとともに、そのような違反に対応すべく適切な措置を講じることが義務付けられる。

3 点目として、対象企業が顧客情報を処分するために適切な措置を講じることを明確化している。そして、4 点目として、レギュレーション S-P の対象に、これまでのブローカー・ディーラー、投資会社、登録投資顧問業者に加え、トランスファー・エージェント[32]を含める。

すなわち、「レギュレーション S-P」改正案に基づくと、上記の対象組織に課される主な要件は、（1）インシデント対応プログラムの採用、（2）機密性の高い個人情報が許可なくアクセス・使用された場合（可能性が高い場合も含む）、顧客への通知を要求、等である。

これらの改正案は、総じて顧客情報保護の強化を意図したものであるが、狙いとして

---

[29] グラム・リーチ・ブライリー法は、1999 年 11 月に制定された連邦法で、金融機関（ローン、金融または投資のアドバイス、保険等の消費者金融商品・サービスを提供する企業）に、情報共有慣行を顧客に説明し、機密データを保護することを義務付けている。（Federal Trade Commission, “Gramm-Leach-Bliley Act”）

[30] U.S. Securities and Exchange Commission, “Regulation S-P”

[31] 米国連邦捜査局（FBI）のインターネット犯罪苦情センターには、2021 年に個人データ侵害や個人情報の盗難に関する 84 万 7,376 件（2017 年比 181%増）の苦情が寄せられた。（Federal Bureau of Investigation, “Internet Crime Report 2021,” 2022; U.S. Securities and Exchange Commission, “Statement on Amendments to Regulation S-P - Chair Gary Gensler,” March 15, 2023）

[32] トランスファー・エージェントは、証券の所有権変更の記録、証券所有者の記録の維持、証書発行・取り消し、配当の分配等を行う。トランスファー・エージェントは、発行体と証券保有者の間に位置するため、流通市場での取引を成功させるために重要な役割を担っている。（U.S. Securities and Exchange Commission, “Transfer Agent.”）

SECのキャロライン・クレンショー委員は、「多くの州では通知等に関して特定の顧客保護が既に実施されているが、本改正案は連邦政府レベルの基準を設けることを通じて、全ての州の顧客に、重大な危害や不便をもたらす可能性のある機密情報の侵害について確実に通知されることになる」と述べている[33]。

図表6　「レギュレーションS-P」の改正案の概要

項目	詳細
目的	レギュレーションS-Pの導入以降、企業は個人情報を取得、共有、保持することが容易になり、顧客情報への不正アクセスや使用リスクが悪化しているほか、州毎に対象機関の顧客に与えられる保護が実質的に異なる場合があるため、対象機関が影響を受けた個人にデータ侵害の通知を提供するための連邦レベルでの最低基準を確立すること
対象組織	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
要件	<u>インシデント対応プログラム</u> ・ 顧客情報が関わるセキュリティインシデント発生による被害を食い止めるべく、対象組織に対して、セーフガード規則に基づく書面による方針と手順の一部として、インシデント対応プログラムを採用することを要求。インシデント対応プログラムは、顧客情報への不正なアクセス・使用を検出、対応、及び回復するように合理的に設計すること等が求められる <u>顧客への通知要件</u> ・ 対象組織に対し、機密性の高い顧客情報が許可なくアクセスまたは使用された、またはその可能性が合理的に高い個人に通知することを要求。対象組織に対し、実行可能な限り速やかに、ただし、顧客情報への不正アクセス・使用が発生したこと、または発生する可能性が合理的に高いことを対象組織が認識してから30日以内に、通知することを要求 <u>その他の強化策</u> ・ セーフガード規則と廃棄規則における顧客情報の定義を拡大。対象機関が自社の顧客について収集する非公開個人情報と、第三者金融機関から受け取った当該金融機関の顧客に関する非公開個人情報の両方に、両方の規則が適用されることになる ・ 対象機関に対し、セーフガード規則及び廃棄規則の要件の遵守を文書化した記録の作成及び維持を要求 ・ 一定の条件が満たされた場合、対象機関は年次プライバシー通知を配信する必要がないことを規定（2015年のFAST法〔Fixing America's Surface Transportation Act〕の例外条項に準拠） ・ セーフガード規則の対象範囲にSEC若しくは他の当局に登録されたトランスファー・エージェントを追加
今後の予定	規則案は連邦官報に公示。パブリックコメントは公示日から60日間受け付け

（出所）U.S. Securities and Exchange Commission, "Factsheet- Proposed Enhancements to Regulation S-P," March 15, 2023、より野村資本市場研究所作成

[33] 前掲脚注3を参照。

Ⅳ 今後の注目点

SEC は 2010 年代以降、様々な分野へのサイバーセキュリティ関連施策を講じてきたが、今回示された米国証券市場の特定関連組織を対象とした 3 つの規則案では、サイバーセキュリティリスクを徹底的に管理・軽減すべく包括的な対処策が示された。「規則 10」では対象組織に対してサイバーセキュリティリスク関連情報の開示等を求めている。「レギュレーション SCI」の改正では、適用範囲の拡大を通じてサイバー攻撃等の技術的なイベントを受けても市場の秩序や効率的な運営を行うべく回復力を強化すること等が焦点となっている。「レギュレーション S-P」の改正では、連邦政府レベルで顧客情報保護を強化することが主眼となっている。

3 つの規則案に対しては、SEC の委員のうち、委員長を含め 3 名が支持、2 名が懸念を示している。マーク・ウエダ委員は、（1）3 つの規則案の全てがサイバーセキュリティに重点を置いているものの、その相互作用や最も効率的にサイバーセキュリティリスクを軽減する方法が SEC により十分に検討されていない、（2）「規則 10」における SEC への通知や報告の規範的な期限が、対象事業体の経営層が他の対応に追われる中で注意を要求するため、利益よりも害を及ぼす可能性がある、（3）「規則 10」について、SEC には、情報漏洩を封印し、技術支援を即座に提供できるサイバー対応チームが存在しない、等の指摘を行った[34]。ヘスター・パース委員は、「レギュレーション S-P」について、多くの州では既に顧客通知規定が存在しており、一部の州では改正規則案との矛盾が生じる等の懸念を示した[35]。

一方、実務家の反応を見ると、3 つの規則案に対して評価する意見と懸念を示すものが混在している（図表 7 参照）。サイバーリスクコンサルタント会社の専門家からは概ね評価する声が多いようだが、中小規模のブローカー・ディーラー等で今般の規則案の適用に伴い新たに発生するコンプライアンス関連コスト負担の大きさを心配する声もある[36]。法律事務所の弁護士からは、規則案に対して多くの懸念を示しており、（1）SEC による様々な規則が混在しているため、統合的なものとして機能しない限り、組織の実務・コスト負担が大きくなりかねない、（2）重大なサイバーインシデントの SEC への即時報告を満たすのは困難、等の意見がある。

---

[34] U.S. Securities and Exchange Commission, “Statement on the Proposed Amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information - Commissioner Mark T. Uyeda,” March 15, 2023; U.S. Securities and Exchange Commission, “Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities - Commissioner Mark T. Uyeda,” March 15, 2023.

[35] U.S. Securities and Exchange Commission, “Statement on Regulation SP: Privacy of Consumer Financial Information and Safeguarding Customer Information - Commissioner Hester M. Peirce,” March 15, 2023.

[36] 「規則 10」を適用した場合、対象事業体 1 社あたりに新たに発生し得る想定年間費用（3 年間で年率換算した初期負担の見積もりを含む）として、（1）コンプライアンスに係る分が 1 万 4,631.54 ドル、（2）新たな方針と手順の導入及び年次レビューに係る分が 3,472 ドル、との SEC による試算が示されている。（U.S. Securities and Exchange Commission, “17 CFR Parts 232, 240, 242 and 249 [Release No. 34-97142; File No. S7-06-23] RIN 3235-AN15: Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents,” March 15, 2023）

図表7　SECによる規則案に対する実務家による主な反応

業態	意見の概要
法律事務所	・規則が適用された場合、統合的なものとして規則が機能しない限り、組織の実務負担は大きくなる可能性がある ・SECが正しい方向への一歩を踏み出しているとはいえ、実際には様々な提案をさらに明確化する必要がある。さもなければ、提案に一貫性がなく、煩雑なため、組織が実装するに当たってコストを要することが明るみになる可能性がある ・「規則10」では、インシデント発生後48時間以内に関連情報をSECに報告する義務があるが、この時間軸はかなり野心的 ・重大なサイバーインシデントのSECへの即時報告を満たすのは困難。攻撃を特定するには、関連する事実の収集に基づく分析が必要であり、時間を要する ・(「規則10」の)「合理的な根拠」という文言は、対象組織の柔軟性を確保すべく盛り込まれたものの、要件が明確でなく、コンプライアンスの不確実性をもたらす可能性がある ・規則案では(サイバーセキュリティリスク管理戦略の一環として、サードパーティ・サービスプロバイダーやベンダーを評価することを求めているが)、サービスプロバイダーをどのように定義するかなど、詳細を詰めるべき部分が残されている ・提案された規則案を踏まえても、SECが外注先のサービスプロバイダーを直接監督する法的権限がない ・提案の複雑さを考えれば、規則制定プロセスが長引いても驚かない
サイバーリスクコンサルタント会社	・SECの提案は、従来の規制の状況を改善するものだが、中小規模の組織にとっては多大なコンプライアンスコストがかかり、必要な管理や手続きの実施に苦労する可能性がある ・SECが規則の遵守を効果的に監視し、強制する十分なリソースを有しているか疑問 ・SECの提案は、具体的な要件を定義する際に規範的で明確ではなかった以前のガイダンスを改善している ・規則案は、重要な外注機能を提供するベンダーのセキュリティ体制を理解するものとなる ・規則案には、21世紀にあらゆる組織が取るべき不可欠なステップが含まれている ・規則案を踏まえると、組織はサービスプロバイダーのサイバーセキュリティプラクティスを評価し、ハードウェアとソフトウェアの脆弱性に対する適時のパッチ適用に注力する必要がある ・既存のリスクフレームワークには欠けている要素として正確で意味のあるサイバーリスク測定があり、SECの提案が既存の状況を変える可能性がある
金融機関	・SECによるサイバーセキュリティをめぐる関与は、(IONトレーディングUKの件もあり)適切なタイミングだが、誤った規則と言える

(出所) "SEC Cyber Rules Risk Creating Web of Confusion and Costs," *Risk.net*, March 28, 2023、より野村資本市場研究所作成

規則案に対しては上記のように様々な意見はあるものの、世界的に金融機関等に対するサイバー攻撃の脅威が増し、金融システムの安定等にも影響を与えかねないことを踏まえて、G7、G20・金融安定理事会（FSB）等の国際的な場でもサイバーセキュリティに関する議論が繰り広げられている。そうした現状も踏まえると、米国を含めて各国当局によるサイバーセキュリティリスクに対する規制・監督が厳格化する方向が近い将来に大きく変わることはないと想定される[37]。

一方、証券会社にとっても、サイバーセキュリティリスクは財務面・非財務面を通じて

[37] 例えば、FSBは2023年4月13日、各法域の金融機関によるサイバーインシデントの報告枠組みの収斂に向けた報告書を公表している。同報告書では、金融機関においてサイバーインシデントがあった場合の対応を迅速化して金融システムへの影響を抑止することを目的に、(1) 各規制当局がサイバー事案報告に関して明確に目標を定義し、その目標が効率的に達成されているか評価すること、(2) 各規制当局が金融機関に課す報告様式の共通化等の合計16項目を推奨している。(Financial Stability Board, "FSB Sets Out a Comprehensive Approach to Achieve Greater Convergence in Cyber Incident Reporting," April 13, 2023; Financial Stability Board, "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting," April 13, 2023)

企業価値へ影響を及ぼしかねない[38]。特に、今回公表された 3 つの規則案のうち、「規則 10」では対象組織のサイバーセキュリティリスク関連情報の開示を求めている。顧客が証券会社を選択する際に、サイバーセキュリティを重要な経営課題として捉え、適切なガバナンス体制の下、適切に対応しているかといった点の開示も判断材料として活用する可能性がある。

なお、日本でも近年、金融機関に対するサイバー攻撃・犯罪が増加している（図表 8 参照）。証券会社においても顧客情報漏洩、不正出金、オンライン取引停止等のサイバーセキュリティリスクが顕在化している。

図表 8　近年の国内金融分野のサイバー脅威の動向

年月	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4,000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3,000件
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 ・ 地方公共団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	ホームページ改ざん	・ サイバー攻撃によりホームページの閲覧とホームページ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

[38] 例えば、SEC が 2011 年 10 月に米国上場企業を対象に公表したサイバーリスク開示の在り方に関するガイダンスにて、サイバー攻撃に伴う企業価値への影響として、復旧・修復コスト、サイバーセキュリティ対策コストの増加、売上減少、訴訟対応、風評被害を例示している。（U.S. Securities and Exchange Commission, “CF Disclosure Guidance: Topic No.2 Cybersecurity,” October 13, 2011）

このような状況下、金融庁でも様々な取り組みを進めている[39]。2014 年 11 月に制定されたサイバーセキュリティ基本法を受け、2015 年 7 月に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）を策定し、その後 2018 年 10 月に同方針を Ver2.0 に、2022 年 2 月には Ver 3.0 に更新した。Ver 3.0 では新たな取組方針として、5 項目（モニタリング・演習の高度化、新たなリスクへの備え、サイバーセキュリティ確保に向けた組織全体の取り組み、関係機関との連携強化、経済安全保障上の対応）が掲げられている[40]。特に、関係機関との連携強化の観点からは、FSB による金融分野のサードパーティリスクの規制監督に関する国際的な議論に積極的に参画している[41]。その他、同庁では、「金融分野のサイバーセキュリティレポート」の取りまとめ、金融業界横断的なサイバーセキュリティ演習（Delta Wall）の実施等に取り組んでいる[42]。

日本の証券業界においても、米国でビジネスを行っている証券会社のみならず、それ以外の証券会社あるいはインフラ運営者についても、顧客基盤や企業価値の保全の観点からサイバーセキュリティ対策の強化が求められる状況となろう。ただし、海外における動きをそのまま追随するのではなく、日本の現状も踏まえた適切な対応を目指すことが重要である。その際に論点となり得るのは、（1）海外の動きのうち日本にとって導入の意義がある分野やすぐに取り組める分野はあるか、（2）外部委託に係るリスク等の開示を義務化することが脆弱性を示唆し新たな攻撃を招くことにつながらないか、（3）大規模なサイバーインシデントの発生時に官民が連携して対応するような仕組みの構築は可能か、などが挙げられる。また、サイバーセキュリティリスクの甚大化に鑑みると、民間事業者が実行可能な対策やコストには限界があり、官民一体で検討を進めることがカギになると言える。

---

39 金融庁「金融分野におけるサイバーセキュリティ対策について」。

40 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方針（Ver 3.0）」2022 年 2 月、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。

41 Financial Stability Board, “Third-party Dependencies in Cloud Services: Considerations on Financial Stability Implications,” December 9, 2019; Financial Stability Board, “Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion Paper,” November 9, 2020; Financial Stability Board, “Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships,” June 14, 2021.

42 Delta Wall は、サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の 3 つの視点（Delta）と防御（Wall）を指す。（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）』について」2016 年 10 月 20 日）