サイバーセキュリティのインシデントの情報開示規制に関する米国の動向

東京大学 名誉教授
神田　秀樹

▌要　約▐

1. 米国連邦証券取引委員会（US Securities and Exchange Commission、SEC）は、2023 年 10 月 30 日に、サイバーセキュリティのインシデントへの対応等に関し、SolarWinds 社と同社の最高情報セキュリティ責任者（CISO）に対し、連邦証券法及び連邦証券取引所法に違反したとして、違反の是正や民事制裁金の賦課等を求める訴訟を連邦地方裁判所に提起した。この事案はサイバーセキュリティ関連の対応が証券詐害（securities fraud）に該当すると SEC が主張して提訴した初めての事案であり、また、内部統制の不備を理由として会社の CISO を提訴した初めての事案である。実務界での反発も強かったが、2024 年 7 月 18 日に裁判所は SEC の請求の一部だけを認める判決を言い渡した。
2. 上記のインシデントが 2020 年に発生したことを重視して、SEC は、2023 年に開示規制の改正を行った。その主な内容は、米国の上場会社等に対し、（ア）サイバーセキュリティのインシデントがあった場合には、会社は遅滞なくそれが重要な（material）ものか否かを判断しなければならず、重要なものと判断した場合には、一定の例外的な場合を除き、重要と判断した日から 4 営業日以内に臨時報告書においてそのインシデントの内容と対応、会社の事業への影響などを開示しなければならないとすることと、（イ）年次報告書においてサイバーセキュリティに関するリスク管理等とガバナンス体制整備とに関する情報開示を求めることである。
3. SEC は、2024 年に、SEC が監督権限を有する証券業者に対し顧客情報の保護等に関する規則の改正を行った。その内容は、対象となる証券業者は顧客情報への不正なアクセスや使用等のインシデントを評価し、統制し、影響を及ぼしうる顧客に通知することを含んだインシデント対応プログラムを策定して実施しなければならない等である。
4. 上記の米国の動向に鑑みると、サイバーセキュリティに関し、日本でもガバナンスの観点からの対応の強化が今後の課題となるように思われる。

Ⅰ はじめに

本稿は、サイバーセキュリティに関する米国の最近の動向について、米国連邦証券取引委員会（US Securities and Exchange Commission、SEC）によるサイバーセキュリティのインシデントに関する連邦証券諸法に基づく情報開示規制を中心として、概観することを目的とする。以下、2023 年 10 月末に SEC が提訴した事案や 2023 年 12 月 18 日から施行されている臨時報告書による情報開示規制の改正等について、概観する。

Ⅱ SEC による提訴事案

１．概要

後述する SEC の情報開示規制改正の最終版が 2023 年 8 月 4 日に公布された後、改正後の規制が施行された同年 12 月 18 日よりも前に、SEC は、SolarWinds 社と同社の最高情報セキュリティ責任者（CISO）に対し、1933 年連邦証券法及び 1934 年連邦証券取引所法に違反したとして、違反の是正や民事制裁金の賦課等を求める訴訟を連邦地方裁判所に提起した[1]。

SolarWinds 社は情報管理等の業務管理ソフトを開発・販売するテキサス州の会社であり、その開発したソフトは全米で広く利用されていたが、2020 年に同ソフトにサイバーセキュリティ上の欠陥があり外部者により攻撃を受けたことが判明した。これに対する同社の対応、とくに情報開示面での対応において、不実開示等があり（当時の）連邦証券諸法に違反したとして、2023 年 10 月 30 日に、SEC は同社と同社の CISO を提訴した[2]。なお、この事案は後述する SEC による 2023 年の規則改正につながった重要な事案である。

この事案の特徴は、次の 2 点にあると言われている[3]。第 1 に、本事案は、単なる臨時報告書や年次報告書における開示義務の違反だけでなく、より重大な「詐害（fraud）」（1934 年連邦証券取引所法 10 条(b)項に基づく SEC の規則 10b-5 の違反）に該当するとして SEC が提訴した初めての事案である。第 2 に、本件はサイバーセキュリティのインシデントに関連して内部統制の不備を理由として会社の CISO を提訴した初めての事案である。本件での CISO には積極的な不正な行為があったわけではないものの、インシデントの取締役会等への報告や対応において不備があったと SEC は主張した。これらの点をみると、それまでの提訴事案と異なり、SEC がサイバーセキュリティを重視し、規則違反に強い対

[1] U.S. Securities and Exchange Commission, “SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures,” October 30, 2023、を参照。

[2] 訴状は、SEC v. Solar Winds Corp. and Timothy G. Brown (US District Court New York Southern District, Civil Action No. 23-cv-9518, October 30, 2023)。

[3] Sullivan & Cromwell LLP, “SEC Charges SolarWinds and Its CISO with Fraud and Internal Control Failures,” November 6, 2023、による。

応をしようとする姿勢がうかがわれる[4]。

この訴訟については実務家からの反発も強かったが[5]、この提訴事案が実務に与えた影響はそれなりに大きいと見受けられる[6]。

２．SEC の主張と裁判所の判決

１）SEC の主張

（ア）証券詐害（securities fraud）

SolarWinds 社のウェブサイト上のサイバーセキュリティ対策等に関する説明、同社のプレスリリース等における説明、発行開示書類および継続開示書類におけるリスクファクターに関する開示、臨時報告書における開示のいずれにおいても、虚偽ないし誤解を招く開示があったと SEC は主張し、1933 年連邦証券法 17 条(a)項（発行開示）、1934 年連邦証券取引所法 10 条(b)項と規則 10b-5（詐害）、同法 13 条(a)項（継続開示）に違反すると主張している。

（イ）財務内部統制

SEC は、SolarWinds 社は上記に関して財務内部統制（internal accounting controls）の運用を怠ったとして、1934 年連邦証券取引所法 13 条(b)(2)(B)に違反したと主張し、同社の CISO はその違反に関与した（aided and abetted）と主張している。

（ウ）情報開示統制

SEC は、適切な情報が経営陣に報告されず、それが上記の開示規制違反を招いたとして情報開示統制（disclosure controls and procedures）の不備を理由に 1934 年連邦証券取引所法の規則 13a-15(a)に違反したと主張し、同社の CISO はその違反に関与したと主張している[7]。

---

[4] 過去の SEC のエンフォースメント事例の一覧は、U.S. Securities and Exchange Commission, ”Crypto Assets and Cyber Enforcement Actions”（https://www.sec.gov/securities-topics/crypto-assets、2024 年 7 月 2 日閲覧）に掲載されている。なお、サイバーセキュリティに関する米国の全般的な歴史を概観するには、たとえば、Lawrence J. Trautman , Scott Shackelford, Brian Elzweig and Peter Ormerod, “Understanding Cyber Risk: Unpacking and Responding to Cyber Threats Facing the Public and Private Sectors,” *University of Miami Law Review*, Vol. 78, No. 3, 2024 を参照。

[5] たとえば、Motion of Chief Information Security Officers and Cybersecurity Organizations for Leave to File Brief as Amicus Curiae Support of Defendants Motion to Dismiss the Amended Complaint (submitted to the US District Court New York Southern District, March 29, 2024).

[6] たとえば、Karen Painter Randall, Joshua P. Previl, and Adam J. Salzer, “Mitigating Cybersecurity Risks in Mergers and Acquisitions: The Importance of Due Diligence and Regulatory Compliance,” *New Jersey Lawyer*, April 2024; Vinson & Elkins, “Double-Edged Disclosure: Navigating 10-K Season with the SEC’s New Cybersecurity Disclosure Rules Insight,” March 4, 2024.

[7] 以上の詳細は、前掲脚注 2 の訴状を参照。

２）裁判所の判決

2024 年 7 月 18 日に、裁判所は、事実認定手続前の判断として、SEC の請求の一部だけを認め、その多くを棄却する判決を言い渡した[8]。裁判所が SEC の請求を認めたのは、ウェブサイトにおける security statement（セキュリティに関する取扱方針）に関連する不備であり、この点については証券詐害に該当する可能性もあるとされた。もっとも、この security statement は法定の情報開示ではなく任意のものであって、法定の開示書類における虚偽等に関する上記の SEC の請求は棄却された。また、上記の 1934 年連邦証券取引所法 13 条(b)(2)(B)について、裁判所は、この規定は財務会計の統制（financial accounting control）にだけ適用される規定であって、より広く内部統制一般に適用されるものではないとして、この点に関する SEC の請求を棄却した。今回の判決の以上の判示内容については、今後さまざまな観点からの議論を呼ぶものと推測される[9]。

Ⅲ SEC の開示規制の 2023 年改正

１．2023 年の開示規則改正

SEC は、2023 年にサイバーセキュリティに関する開示規則を改訂している[10]。改訂の最終版は 2023 年 7 月 26 日に公表され、同年 8 月 4 日に Federal Register（日本の官報にほぼ相当する）において公布されている[11]。その内容は、米国の上場会社等の登録会社（日本での有価証券報告書提出会社に相当する）に対し、（ア）サイバーセキュリティのインシデントがあった場合には、会社は遅滞なく（without unreasonable delay）それが重要な（material）ものか否かを判断しなければならず、重要なものと判断した場合には、一定の例外的な場合を除き、重要と判断した日から 4 営業日以内に書式 8-K 報告書（臨時報告書、日本での臨時報告書に相当する）の項目 1.05（Item 1.05）においてそのインシデントの内容と対応、会社の事業への影響などを開示しなければならないとする点と、（イ）書式 10-K 報告書（年次報告書、日本での有価証券報告書に相当する）においてサイバーセキュリティに関するリスク管理等とガバナンス体制整備とに関する情報開示を求める点に、主な特徴がある[12]。

---

[8] 判決は、SEC v. Solar Winds Corp. and Timothy G. Brown (US District Court New York Southern District, Civil Action No. 23-cv-9518-PAE, July 18, 2024)。

[9] たとえば、Sullivan & Cromwell LLP, “Court Dismisses Most of SEC’s Claims Against SolarWinds and Its CISO,” July 19, 2024。

[10] U.S. Securities and Exchange Commission, “SEC Adopts Rules on Public Company Cybersecurity Disclosures,” July 26, 2023; Sullivan & Cromwell LLP, “SEC Adopts New Cybersecurity Disclosure Rules for Public Companies, July 28, 2023.

[11] U.S. Securities and Exchange Commission, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 88 FR 51896,” August 4, 2023.

[12] Erik Gerding, U.S. Securities and Exchange Commission, “Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents, May 21, 2023; Erik Gerding, U.S. Securities and Exchange Commission, “Cybersecurity Disclosure,” December 14, 2023、林浩美・湯川昌紀「米国 SEC のサイバーセキュリティに関する開示規則」『森・濱田松本法律事務所・データ・セキュリティ NEWSLETTER』Vol.18、2023 年 11 月 1 日、参照。

少し敷衍すると、上記の（ア）については、重要か否かの判断は、定量的な面だけでなく定性的な面での判断も含む。この臨時報告書による開示に関する規則改正の施行日は2023年12月18日である。

また、（イ）の年次報告書における開示については、第1に、リスク管理等については、会社はサイバーセキュリティの脅威に関する重要なリスクを評価・特定・管理するプロセスを年次報告書に記載することが求められるが、その際、そのプロセスが会社全体のリスク管理プロセスに統合されているか否か、そのプロセスに監査人等の第三者が関与しているかどうか、外部のサービスプロバイダーの利用に伴うサイバーセキュリティの脅威を監視・特定するプロセスを有しているかどうかの記載が含まれなければならない。また、過去のサイバーセキュリティのインシデントの結果を含むサイバーセキュリティの脅威のリスクが事業戦略・経営成績・財政状態を含めて会社に重要な影響を与えたかどうか、与える可能性が合理的にあるか、ある場合はどう影響を与えるかについても記載することが求められる。

第2に、ガバナンス体制の整備については、取締役会によるサイバーセキュリティの脅威のリスクの監視についての記載が求められ、この監視に責任をもつ取締役会の委員会や下部組織を置く場合には、それを特定し、そこから取締役会や委員会がリスクに関する情報の伝達を受けるプロセスを特定することが求められる。これには、責任をもつ者や委員会メンバーの専門性やその者ないし委員会によるモニタリングのプロセス、取締役会ないし委員会への報告体制が含まれなければならない。この年次報告書による開示に関する規則改正は、2023年12月15日以降に終了する事業年度に係る年次報告書から適用される[13]。

２．規則改正後の臨時報告書による開示の実務

2024年2月22日付のある論稿[14]によれば、2023年12月18日の規則改正施行以後、14の会社がサイバーセキュリティのインシデントについて臨時報告書の項目 1.05 における開示を行っている。なお、臨時報告書は提出した後に改訂ないし修正したものが提出されることが少なくないことに留意する必要がある（この点は、日本でも制度上は同様である）。この改訂ないし修正は会社が自発的に行う場合が多いが、SECのコメントを受けて行われる場合もあり、その例として、ある会社が2023年12月15日に提出した臨時報告書についてSECが2024年1月5日にコメントを公表し、同社は18日に修正臨時報告書を提出している（ただし、この例では重要性ありとの修正がされたわけではない）。

[13] 以上は、前掲脚注12所掲のものによっている。

[14] Paul Rodel, Charu Chandrasekhar and Erez Liebermann , “What Cos. Are Reporting Under New SEC Cybersecurity Rule,” *Law360*, April 22, 2024. 以下の記述はこれに負う。

（ア）日数

インシデントの発覚日から開示までの平均日数は 5.43 営業日となっている。10 社は、インシデントの発覚日から 4 営業日以内に臨時報告書による開示をしている。最短の例は 1 日、最長の例は 25 日となっている。

（イ）開示内容

（ⅰ）重要性

上記の 14 社のうち、3 社が重要なインパクトを明示的に特定している。2 社は業務上の障害発生（operational disruption）を当初の臨時報告書において開示しており、1 社は当初の臨時報告書の 3 週間後の改訂において業務への重要なインパクトがあったと開示している。残りの 11 社は重要なインパクトに言及していない。業務上の障害発生はなかったと明記する例もあるが、その他、会社の財務状態や業務に影響を及ぼす可能性は低いと述べる例が典型的である。

（ⅱ）財務への影響

1 社は当該四半期の財務への影響があると開示しているが、5 社はそうした影響はないであろうと開示している。残りの 8 社は財務への影響はわからないと開示している。これに対して、業務上の障害発生は特定しやすいので、上記の 1 社はこれがその会社の事業にとって重要であると開示している。

（ⅲ）顧客情報の漏洩

8 社が顧客情報の漏洩があったことを開示している。このうち 5 社は当初の臨時報告書において、2 社は臨時報告書の改訂においてこれを開示している。もっとも、その実態や影響の解明にはさらに時間を要することに留意する必要がある。

（ⅳ）攻撃者の特定

5 社が何らかの形で攻撃者を特定している。3 社は当初の臨時報告書では国としていたが、そのうちの 1 社は臨時報告書を改訂しサイバー犯罪グループと修正している。残りの 2 社はサイバー犯罪グループの可能性があるとだけ開示している。

３．2024 年 6 月 24 日の SEC の Q&A 改訂

上記の臨時報告書の項目 1.05 における開示について、2024 年 6 月 24 日に、SEC はガイダンス文書における Q&A を改訂している[15]。

（ア）Q&A 104B.05　ランサムウェアによる攻撃への対応が終了したとしても、そのインシデントが重要なものでなかったことにはならない。

（イ）Q&A 104B.06　インシデントへの対応が完了したとしても臨時報告書での開示をしなくてよいことにはならない。

[15] U.S. Securities and Exchange Commission, “Exchange Act Form 8-K, June 24, 2024.

（ウ）Q&A 104B.07　ランサムウェアによる被害について保険でカバーされたとしても、そのインシデントが重要なものでなかったことにはならない。

（エ）Q&A 104B.08　ランサムウェアによる被害の金額は、その大小がインシデントの重要性判断を左右するものではなく、その判断に際しての一要素にすぎない。

（オ）Q&A 104B.09　一連の複数のインシデントが発生した場合には、全体をもって重要性判断をしなければならない。

Ⅳ SECが監督権限を有する業者に関する規制（規則S-P）の改正

以上に紹介したところは、日本でいう有価証券報告書提出会社の情報開示に関する規制であるが、いうまでもなく、SECは証券業者の監督当局でもある。

SECは、2000年に、証券業者に対し、顧客情報の保護等に関する規則S-Pを制定しているが、2024年5月16日にその改正が行われている[16]。同改正は、2024年6月3日に連邦官報に公布され、2024年8月2日から施行されている[17]。

この規則は、一定規模以上の証券業者（ブローカー・ディーラー、投資会社、投資助言業者など）に対し、顧客情報の取扱いや情報提供に関する規制を設けるものであるが、今回の改正の概要は次のとおりである[18]。

（ア）適用範囲の拡大

規則の適用範囲として、顧客情報には他の金融機関等から得た顧客情報も含まれる。また、名義書換代理人（Transfer Agent、TA。日本での株主名簿管理人に相当する）もこの規則の対象となる。

（イ）インシデント対応

対象となる証券業者は、顧客情報への不正なアクセスや使用等のインシデントを評価し、統制し、影響を及ぼしうる顧客に通知することを含んだインシデント対応プログラムを策定して実施しなければならない。

（ウ）顧客への通知

対象となる証券業者は、顧客のセンシティブ情報への不正なアクセスや使用等のインシデントがあった場合には、インシデントの認識後原則として30日以内に顧客に通知しなければならない。ただし、顧客への被害の可能性がない場合、通知は免除さ

[16] U.S. Securities and Exchange Commission, “Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information,” June 21, 2024.

[17] U.S. Securities and Exchange Commission, “Regulation S‐P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 89 FR 47688,” June 3, 2024. 89 FR 53487 (June 27, 2024) により一部訂正。

[18] U.S. Securities and Exchange Commission, “Exchange Act Form 8-K,” June 24, 2024. 以下は、Debevois & Plimpton, The SEC Adopts Significant Cybersecurity Amendments to Reg S-P, May 17, 2024 に負う。

れる。影響を受ける顧客が特定できない場合は、すべての顧客に通知しなければならない。

（エ）サービスプロバイダーの監督

対象となる証券業者は、サービスプロバイダーが適切なインシデント対応体制を有しているか等を含めてサービスプロバイダーの監督に関するプログラムを策定して実施しなければならない。必要な事項はサービスプロバイダーとの間の契約等で定められなければならない。

（オ）記録保持

対象となる証券業者は、上記のインシデント対応プログラム等は書面で策定し、インシデントの調査や顧客への通知等についての記録も書面にて保持しなければならない。

（カ）年次でのプライバシー情報の管理に関する顧客への通知

この点については、一定の場合に消費者金融保護局（Consumer Financial Protection Bureau、CFPB）の規則 P[19]と同じ例外が認められる。

V むすびに代えて

上記で概観した米国の動向は、次の点を示唆する。第 1 に、サイバーセキュリティのインシデントについて、その迅速な情報開示と適切な対応が求められるということである。そして第 2 に、そのためには体制の整備、すなわち適切なリスク管理とガバナンス体制の構築が求められ、それには取締役会が責任をもつということである。

日本では、これまで、インシデント発生の防止と発生した場合の対応という実質を重視し、とくに予防面でのサイバーセキュリティ対策の重要性が説かれてきている[20]。ただ、ガバナンス体制については、一般的なルールとしては、2021 年改訂後の「コーポレートガバナンス・コード」において言及はなく、2021 年改訂後の「投資家と企業の対話ガイドライン」の「1-3」[21]に言及がある程度である。今後、日本でもガバナンスの観点からの対応の強化が課題となるように思われる[22]。

---

[19] Consumer Financial Protection Bureau, “Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P),” August 10, 2018.

[20] 内閣サイバーセキュリティセンター（NISC）による各種の注意喚起や金融庁「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 月など。

[21] 金融庁「投資家と企業の対話ガイドライン」（2018 年 6 月 1 日策定、2021 年 6 月 11 日改訂）の「1-3」。

[22] なお、法制度一般の課題については、蔦大輔「サイバーセキュリティ法制の概観と課題」『ジュリスト』第 1599 号、2024 年 7 月、を参照。