調査・分析レポート

連邦証券取引委員会によるサイバーセキュリティに関する情報開示の最終規則、司法省ガイドライン、臨時報告書における記載例、関連訴訟等について

法政大学　人間環境学部　教授　**永野　秀雄**

I　はじめに

連邦証券取引委員会（Securities and Exchange Commission: SEC）は、2023年7月26日に、サイバーセキュリティに関する情報開示の最終規則「サイバーセキュリティに関するリスク管理、戦略、ガバナンス及びインシデントの情報開示（Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure）」[1]について、3対2の僅差でこれを採用することに決定した[2]。その内容は、2022年3月9日に公表された規則案とは、かなり異なる部分がある。また、この最終規則に定められている内容の手続を具体化するため、司法省ガイドライン等が公表されている。

本最終規則に対しては、登録企業（日本で言えば上場企業等）に対しても負担が大きい等に理由により、連邦議会上下院の共和党議員により最終規則に対する反対決議が提出された。この決議は、同規則を廃止することを目的としたものであるが、後述するように、成立する可能性はほぼないと言ってよい。

本最終規則は、2023年9月5日に発効し、既に登録企業による臨時報告書において「重大なサイバーセキュリティインシデント」に関する情報開示が始まっている。

本稿では、この最終規則について、①本最終規則の背景、②本最終規則の概要、③国家安全保障等を理由とした情報開示の延長に関するFBI指針及び司法省ガイドライン、④SECの最終規則に関連した2つの動き、⑤最終規則に基づいて登録企業が臨時報告書で開示した「重大なサイバーセキュリティインシデント」の記載例、⑥SECによるサイバーセキュリティリスクに関する不適切な情報開示等に対

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed.Reg. 51896 (Aug. 4, 2023).
[2] Heather M. Ducat, James Koenig, David I. Meyers, Sadia Mirza, Kim Phan, Betty Linkenauger Segaar, Karla Ballesteros, Jason L. Langford & Connor Nechodom, *SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on their Security and Disclosure Plans*, Troutman Pepper Hamilton Sanders LLP (July 31, 2023).

する訴訟、⑦我が国において今後期待される対応の順に説明していくことにする[3]。

なお、本稿の内容は、CISTEC Journal 2022年7月号259頁以下に掲載して頂いた拙稿「連邦証券取引委員会によるサイバーセキュリティに関する情報開示規則案の概要及び関連する行政執行・訴訟について」（以下、永野・規則案論文）と一部重複する部分があるとともに、同論文を参照して頂く場合があることをお断りしておきたい。

II　本最終規則の背景

A　関連法令

米国の1933年証券法（Securities Act of 1933）[4]と1934年証券取引所法（Securities Exchange Act of 1934）[5]は、株式を公開している企業（登録企業）に対して、一定の情報開示義務を課している。大まかに言えば、1933年証券法は公募されている株式の登録及び売買について規制し、1934年証券取引所法は株式を公開している全ての企業の年次報告要件及び定期報告要件を規定している。

また、登録企業に対する具体的な情報開示規制は、連邦証券取引委員会規則第S-X号[6]が財務諸表において記載しなければならない情報を定め、同規則第S-K号[7]が主に非財務情報の情報開示を規定している。このうち、後者の規則第S-K号は、SECへ申請を行うときに提出する登録届出書における情報開示方法や、株主への定期的な報告書などにおける継続的な開示方法等を定めている。このため、サイバーセキュリティに関する情報開示の多くは、規則第S-K号に基づくものである。

この規則第S-K号においてサイバーセキュリティに関する情報開示に関係する主な規定は、①第101項[8]が、登録企業に対して、その事業活動を記述する義務と、その財務内容の情報開示を求めており、②第103項[9]が、登録企業に対し、現在直面している訴訟等の重要な法的手続（係争中のもの、行政手続等を含む）の状況について、当該企業の業務に日常的に付随する訴訟を除き、簡潔に記述する義務を課しており、③第105項「リスク要因（Risk Factors）」[10]は、登録企業に対して、同社の証券への投資が、投機的又はリスクを負うことになる最も重大な諸要因を開示し、これについてどのような特定のリスクが影響するのかにつき明確に記述することを求めており、④第303項[11]が、「財務状態と経営成績に関する経営者による議論と分析（Management's Discussion and Analysis of Financial Condition and Results of Operation: MD&A）」において、登録企業の経営者が、過去又は将来における「既知の傾向又は不確実性」を認識し、これが当該企業の財務状況や事業結果に重大な影響をもたらすと合理的に予測される場合（サイバーインシデント等の発生による影響に関係する）に、その情報開示を求めており、⑤第307項[12]が、登録企業の最高経営責任者や最高財務責任者等に対して、情報開示に関する管理と手続についての

---

[3] 本稿では、直接に脚注で引用している文献以外に、以下の文献を参照した。なお、本稿では、紙幅の関係から、サイテーションによりネット上で下記の文献を特定できる場合には、URLの表示を省略している。*See* Alan Dye, Richard Parrino, John Beckman, Kevin Greenslade, Ann Kim, Paul Otto, Peter Marta, Allison Holt Ryan, Nathan Salminen & Nicholas Hoover, *Agencies issue guidance on delayed SEC reporting of material cybersecurity incidents*, Hogan Lovells International LLP (Jan. 9, 2024); Cydney Posner, *Corp Fin Issues New CDIs On Delaying Form 8-Ks For Material Cybersecurity Incidents*, Mondaq Business Briefing (Dec. 21, 2023); Gicel Tomimbang, Julia Jacobson & Alan Friel, *FBI and DOJ Issue Guidance on SEC Incident Reporting Delay Requests*, Squire Patton Boggs LLP (Jan. 16, 2024); Evan D. Wolff, Daniel L. Zelenko, Matthew B. Welling, Jennie Wang VonCannon, William J. Bruno, Alexander Urbelis, Anand Sithian, Garylene (Gage) Javier & Neda M. Shaheen, *FBI Offers Pathway to Request Delay of SEC Cybersecurity Incident Disclosures*, Crowell & Moring LLP (Dec. 19, 2023).

[4] Securities Act of 1933, ch. 38, 48 Stat. 74 (codified as amended at 15 U.S.C. § § 77a-77aa (2018)).

[5] Securities Exchange Act of 1934, ch. 404, 48 Stat. 881 (codified as amended at 15 U.S.C. § § 78a-78qq (2018)).

[6] 17 C.F.R. Part 210 (2020).

[7] 17 C.F.R. Part 229 (2020).

[8] 17 C.F.R. § 229.101(2020).

[9] *Id*. § 229.103.

[10] *Id*. § 229.105.

[11] *Id*. § 229.303.

[12] *Id*. § 229.307.

情報開示を求めており、⑥第 407 項[13]が、企業統治（Corporate Governance）に関して、監査委員会に財務の専門家がいるのか否かに関する情報開示を求めている（特定組織において専門知を持った者の必要性の有無に関係する規定であり、サイバーセキュリティの専門家の必要性で関係する）。

B　本最終規則が制定されるまでの経緯

１　２つの解釈指針

連邦証券取引委員会（SEC）は、これまで、サイバーセキュリティリスクに関する２つの解釈指針を出している。

まず、SEC の企業財務局は、2011 年 10 月 13 日にサイバーセキュリティに関するリスク情報の開示に関する指針[14]（以下、「2011 年指針」という。）を公表した。そこでは、「明示的にサイバーセキュリティリスクやサイバーインシデントに言及した開示要件はないものの、多くの開示要件が、登録企業（registrants）に、このようなリスクやインシデントを開示する義務を課すことになる場合がある。」と述べるとともに、「サイバーセキュリティリスクやサイバーインシデントに関する実質的な情報は、それが生じた状況につき誤解を生じさせないようにするという観点から、他の情報開示要件を満たすことになる場合、その開示が必要となる場合がある。」としている。ただし、この 2011 年指針には法的拘束力はなかった[15]。

次に、SEC は、2018 年２月 16 日に、2011 年指針を強化した解釈指針[16]（以下、「2018 年指針」という。）を公表した。この 2018 年指針では、サイバーセキュリティに関する包括的な指針と手続の重要性が強調されるとともに、重大なサイバーセキュリティインシデントやリスクを知りながら、これを「重要な未公表情報（material non-public information）」として非開示にしておくと、インサイダー取引規制に抵触する事態が生じる可能性があること等が指摘されている。なお、この 2018 年指針にも、法的拘束力はなかった。

２　本規則案の公表

その後、SEC は、2022 年３月９日に「サイバーセキュリティに関するリスク管理、戦略、ガバナンス及びインシデントの情報開示を行う義務を新たに課す規則案」[17]（以下、「本規則案」という）を公表している。この本規則案は、上記の 2011 年指針及び 2018 年指針が出された後に、①経済活動の多くが急速に電子システムに依存するようになり、これがサイバー攻撃に直面して停止した場合、登録企業に重大な影響をもたらしうる可能性が生じたこと、②ランサムウエア攻撃等の様々な要因により、サイバーインシデントが急増したこと、及び、③企業がサイバーセキュリティインシデントにより被る被害（業務の停止に伴う損失、ランサムウエアに関する支払い、修復費用、第三者への損害賠償、サイバーセキュリティに必要な費用、訴訟リスク、企業イメージの悪化等）が増大したことから、投資家等により登録企業のサイバーセキュリティに関連するタイムリーで信頼できる情報が求められるようになったとして策定されたものである。

３　本規則案公表後の重要な立法

また、本規則案が公表されてから、２つの大きな法的な進展が見られた。

その第１は、2022 年３月 15 日に 2022 年包括歳出法（Consolidated Appropriations Act of 2022）の一部として成立した「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（Cyber Incident Reporting for Critical Infrastructure Act of 2022）」（以下、「CIRCIA」という。）である。同法では、サイバーセ

---

[13] *Id.* § 229.407.
[14] SEC, Div. of Corp. Fin., CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).
[15] 2011 年指針については、ネット上で読める拙稿「米国の公開企業とサイバーセキュリティ・リスクの開示 ―連邦証券取引委員会企業財務局『連邦証券取引委員会企業財務局情報開示指針第２号　サイバーセキュリティ』の検討」公共政策志林５巻 17 ページ以下（2017 年）を参照のこと。
[16] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release No. 33-10459, 83 Fed. Reg. 8166 (Feb. 26, 2018).
[17] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed.Reg.16590 (Mar. 9, 2022).