

米国における内部統制制度の最近のエンフォースメント ——内部会計統制と開示統制手続を中心に

萬 澤 陽 子

要 旨

本稿は、米国における内部統制に関する制度について、近時の SEC によるエンフォースメント事案を検討することにより、その法的意義を明らかにすることを目的とする。

米国では、1977年の海外不正支払防止法により、「内部会計統制」が導入され、2002年の SOX 法によって内部統制制度がさらに強化された。具体的に、SOX 法302条・404条に基づき制定された SEC のルールが、財務報告の信頼性に向けられた「財務報告に係る内部統制」と、開示すべき情報が適時に収集され経営陣に伝達されることを確保する「開示統制手続」を維持し、その有効性を評価することを発行会社に求めた。本稿では、近時のサイバー攻撃を受けた会社に対する SEC による執行事案において、これらの内部統制制度、特に「内部会計統制」と「開示統制手続」がどのように適用されているかを検討する。

「内部会計統制」について、SEC は、従来、会計・財務報告を中心に用いられてきた同規定を2024年の事案でサイバーセキュリティ統制にも適用しようとしたが、その後 SolarWinds 判決で、内部会計統制は財務会計に向けられたものであるとして、その適用範囲に限界が示された。

他方、「開示統制手続」については、虚偽記載の存在を前提とせず、財務報告に直接関係がなくても、会社内部の重要情報が開示判断を行う経営陣に適時に伝達されるための統制手続自体がなければ、そのことをもって責任を問う事案がみられた。また、2023年には重要なサイバーセキュリティ・インシデントについて新たな開示義務が設けられたところ、新しい開示義務を実効的に機能させるためには、インシデントに関する情報が開示判断権者に適時に伝わる必要があることから、新ルールの下で「開示統制手続」の重要性はさらに高まる。

以上のことから、米国の内部統制制度には、財務報告の信頼性に関して合理的保証をするための仕組みにとどまらず、投資者への適時・正確な情報開示のための情報のフローを確保する「開示統制手続」があり、SEC のエンフォースメントにおいて重要な役割を果たしているのである。

I. はじめに

わが国の金融商品取引法に内部統制報告制度が導入されてから15年以上が経過し、2023年には内部統制基準および実施基準が改訂された。同制度をめぐっては、それなりに機能しているという評価がなされる一方で、運用面で多くの問題点が指摘され、制度が形骸化しているという意見もある¹⁾。本稿では、わが国に同制度が導入された際に参考にされた米国において、内部統制およびその報告に関する制度がどのように運用されているのかについて、近時のSECによるエンフォースメント事案を検討することにより、その法的意義を明らかにすることを目的とする。

米国において最初に内部統制 (internal control) が導入されたのは、1977年の海外不正支払防止法 (Foreign Corrupt Practices Act (FCPA)) であった。その後、Sarbanes-Oxley 法 (SOX 法) によってさらに強化され、今日に至っている²⁾。そこで本稿では、まず、FCPA によって求められる内部統制を概観した後に、SOX 法制定以降、どのような内部統制が発行会社に求められ、それらが証券取引委員会 (SEC) によってどのように執行されているのかについて検討する。

II. Sarbanes-Oxley 法 (SOX 法) 成立前の内部統制 (internal control) の展開

1. 海外不正支払防止法 (FCPA) における内部統制

FCPA は、米国会社による海外での疑わしい支払いや違法な支払いが憂慮すべき水準に達していることを記載する1976年の証券取引委員会 (SEC) の報告書を受けて、1977年に連邦議会によって制定されたものである³⁾。同法は、一定の外国での支払いを違法とすること (反賄賂条項)、および、海外取引を正確に反映した記録を保存し、また内部会計統制の構築を義務付けること (会計条項) によって、外国公務員に対する会社の贈賄行為を根絶することを目指していた⁴⁾。会計条項は、贈賄行為の開示を強制することで、贈賄を抑止するという趣旨で設けられたものであり、この一環として導入されたのが内部統制 (internal con-

1) 兼田克幸「内部統制報告制度を巡る諸課題及び実効性確保のための対応策」法学新報130巻9, 10号71, 80-82頁 (2024)。

2) THOMAS LEE HAZEN, TREATISE ON THE LAW OF SECURITIES REGULATION 8th (2023) §9: 23.

3) William L. Larson, *Effective Enforcement of the Foreign Corrupt practices Act*, 32 STAN. L. REV. 561, 562 (1980).

4) *Id.*

trol) であった⁵⁾。

具体的に、会計条項とは、証券取引所法 (Securities Exchange Act (34年法)) 13条 (b) (2) (A) (B)⁶⁾である。すなわち、発行会社は、合理的な詳細さで正確かつ公正に取引および発行会社の資産の処分を反映する、会計帳簿、記録類および計算書を作成・保存することが求められ (13条 (b) (2) (A))、さらに、発行会社は、(i) 経営陣の一般的または個別的承認に従って取引が執行されること、(ii) 会計原則 GAAP または他の適用される基準に適合して財務諸表を作成するのに必要なように、かつ資産の説明責任を果たすのに必要なように、取引が記録されること、(iii) 資産へのアクセスは経営陣の一般的または個別的承認に従った時のみ許されること、(iv) 記録された資産明細が合理的な期間において現存資産と照合され、相違があるなら適切な措置が講じられることについて、それぞれ合理的保証 (reasonable assurance) をするのに十分な内部会計統制の制度の構築・維持をすることが求められている (同 (B))。

会計条項の解釈・運用について、議会と SEC の考え方には乖離があった。すなわち、「議会の意図としては…会計条項の適用も海外での賄賂禁止を定めた規定と結びついた形で適用すべきとされていた⁷⁾」のに対し、「SEC の関心はもともと海外での賄賂行為の防止のみにあるのではなく、そうした海外での賄賂行為にともなう簿外資産の存在を許している企業の歪んだ内部統制システムの是正それ自体にあった。…したがって、13条 (b) (2) は、SEC によれば単に適正な財務諸表の作成に貢献するものではなく、むしろ会社の経営責任の基礎たる適正な会社記録の維持、および内部統制維持義務を法的に課しており、ひいては34年法の開示制度の信頼性を支えるところにその目的がある⁸⁾」とされていたからである。

より具体的に、SEC は、34年法13条 (b) (2) (A) は、財務諸表の作成について信頼に値する基礎を提供するのみならず、とりわけ、簿外の裏金を実効的に防止する SEC の権限、および会社資金の使用について適切な会計処理が確実になされるようにする SEC の権限を確認する目的を有するとしていた⁹⁾。また、34年法13条 (b) (2) (B) は、制定法の目的が実現することを合理的に保証するのに十分な内部会計統制を構築・維持することを求めているところ、これら目的には、会計原則 (GAAP) に適合した財務諸表の作成に必要な取引の記録だけではなく、資産の説明責任を果たすために必要な取引の記録も含まれ (同 (ii) 参照)、さらに、会社の資産へのアクセスおよび会社の資産の取引が経営陣の一般的または

5) *Id.* 会計条項の執行は、もっぱら SEC によっている (at 562-563)。

6) 15 U.S.C. § 78m (b) (2) (A) (B)。これに対して、本稿では直接は扱わないが、反賄賂条項は34年法30A 条である。

7) 柿崎環『内部統制の法的研究』(日本評論社、2005) 37頁。

8) *Id.*

9) SEC, Promotion of the Reliability of Financial Information and Prevention of the Concealment of Questionable or Illegal Corporate Payments and Practices, Exchange Act Release No. 15570, 1979 SEC LEXIS 2141, at 18. (Feb. 15, 1979.)

個別的承認に従ってなされることを合理的に保証すること（同（i）（iii））の目的も明らかに含まれる¹⁰⁾と解釈していた。

このように、反賄賂条項と会計条項をセットのように考えていた議会の意図とは対照的に、SEC は、FCPA の目的を広く捉えた上で、そのために必要な権限を会計条項に基づいて（反賄賂条項からは独立した形で）行使していく旨表明していた。実際、SEC は、新しい13条（b）（2）が34年法で義務付けられる開示制度を支援する、登録会社内で行うべきことに関する要件を構築したのみならず、投資者に重要な点で虚偽または誤導的な情報を提供する事案に適用される条文の違反があろうがなかろうが、SEC によるエンフォースメントの独立した基礎を提供するかもしれないということまで、明示的に述べていたのである¹¹⁾。

もっとも、SOX 法以前においては、後にみるような、虚偽記載を伴わずに内部統制の不備それ自体を独立して問題とする SEC の執行は、少なくとも一般的なものではなかったと思われる。

Ⅲ. SOX 法で導入された内部統制—財務報告に係る内部統制 （internal control over financial reporting）および 開示統制手続（disclosure controls and procedures）、確認書—

内部統制は、FCPA で導入された当時には大きな論争となり、その範囲を狭める提案が複数回なされるほどであった¹²⁾。しかし、2002年に制定された SOX 法は、むしろ内部統制の中身を充実させ、改革の中核に据えたのである¹³⁾。

SOX 法で導入された内部統制は複雑であり、条文を見ただけではわかりにくい。なぜなら、SOX 法302条と404条はいずれも内部統制に関する規定であるものの、それぞれの規定で用いられる用語が統一されていないことが、その主たる理由の一つと思われる。この用語を統一したのは、SEC が同規定によって与えられた規則制定権限に基づいて制定したルールによってであり、それによって、内部統制は「財務報告に係る内部統制」および「開示統制手続（DCP）」という概念で再構成された。よって、以下では、まず両規定と SEC ルールとの関係を確認した上で、現在の内部統制制度を構成する「財務報告に係る内部統制」と「開示統制手続」について検討する。

10) Id. at 18–19.

11) Id. at 19.

12) Hazen, *supra* note 2, § 9.23.

13) Id.

1. 内部統制報告 (SOX 法404条)

(1) 404条 (a) の「財務報告に係る内部統制体制および手続」と SEC ルールの「財務報告に係る内部統制」

SOX 法404条 (「経営陣による内部統制評価 (Management assessment of internal controls)」)¹⁴⁾ は、発行会社に内部統制報告を求めている。より正確には、同条 (a) は、発行会社が提出する年次報告書に、(1) 十分な「財務報告に係る内部統制体制および手続 (internal control structure and procedures for financial reporting)」を構築し維持することについての経営陣の責任を記載し、および (2) 発行会社の直近の事業年度末時点における、当該発行会社の「財務報告に係る内部統制体制および手続」の有効性についての評価を含む内部統制報告書を含めることを義務付けるルールを SEC に定めることを求めている。

SEC は、同条 (a) に基づき多くのルールを制定・改正した¹⁵⁾。その際、SEC は、404条で使われている用語「財務報告に係る内部統制体制および手続」ではなく、404条では使われていない「財務報告に係る内部統制 (internal control over financial reporting)」という用語を統一的に用いた¹⁶⁾。よって、404条 (a) が年次報告書に含めることを義務付ける内容 (上記 (1) (2)) について、同条に基づき制定 (改正) された SEC ルールでは、「会社において、十分な『財務報告に係る内部統制』を構築・維持する経営陣の責任に関する表明を含まなければならない」「直近事業年度末時点における会社の『財務報告に係る内部統制』の有効性に関する経営陣の評価を含まなければならない」と規定されたのである¹⁷⁾。

なぜ、404条とは異なる用語が、同条に基づいて制定されたルールで用いられているのかについては、「財務報告に係る内部統制」という用語が、会社や監査人の間で広く使われており、投資者にとっても混乱が少ない上に、SOX 法の目的を最も包含することが挙げられている¹⁸⁾。

(2) 「財務報告に係る内部統制」の定義

このように、SEC ルールで採用された「財務報告に係る内部統制」は、13a-15 (f) で、「発行会社の最高経営責任者 (CEO) および最高財務責任者 (CFO)、または同様の職務を遂行する者の指示のもともしくは監督下で構築され、発行会社の取締役会、経営陣、その他の従

14) 15 U.S.C. § 7262.

15) SEC Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Release Nos. 33-8238; 34-47986; IC-26068 (June 5, 2003), available at <https://www.sec.gov/rule-release/33-8238> [hereinafter SEC Release 33-8238].

16) Id. "SUMMARY" 部分参照。

17) Id. 17 C.F.R. § 229.308 (Item 308) も参照。

18) Id. "II. Discussion of Amendments Implementing Section 404", "A. Definition of Internal Control", "3. Final Rules".

業員によって実施される、一般に公正妥当と認められる会計原則（GAAP）に準拠した外部向けの財務諸表の作成および財務報告の信頼性に関して、合理的保証をすることを目的としたプロセス」と定義される¹⁹⁾。SECは、この定義が34年法13条（b）（2）（B）の規定する内部会計統制の内容と一貫する、と述べている²⁰⁾。

2. 確認書（SOX 法302条）

（1） 302条の「内部統制」とSEC ルールの「開示統制手続」

SOX 法302条（「会社の財務報告責任（Corporate responsibility for financial reports）」²¹⁾は、1934年証券取引所法の規定に基づき提出される年次報告書および四半期報告書において、最高経営責任者および最高財務責任者（またはこれらに相当する者）に、多岐にわたる事項について確認（証明）することを義務付けるルールを制定するようSECに求めている²²⁾。具体的に、302条は、その対象が、同報告書に虚偽表示がないといったことのみならず、「内部統制（internal control）」の構築・維持の責任を負うこと、その設計、その有効性の評価およびその結論の開示、さらに「内部統制」の設計または運用における著しい不備等が見つかった場合の、取締役会の監査委員会等に対する開示にまで及ぶと規定する²³⁾。

302条も条文上は「内部統制」という用語が使われているが、これを受けて制定（改正）されたSECルール²⁴⁾は、その「内部統制」という用語を、「財務報告に係る内部統制」または「開示統制手続」に変更している。具体的に、「開示統制手続」および「財務報告に係る内部統制」の構築・維持の責任を負うこと、「開示統制手続」の設計、その有効性の評価およびその結論の開示、「財務報告に係る内部統制」の設計、直近の四半期において生じた「財務報告に係る内部統制」について変更があったならその開示、「財務報告に係る内部統制」

19) また、これには「（1）発行会社の資産の取引および処分を、合理的な詳細さで正確かつ公正に反映する記録の維持に関するもの。（2）一般に公正妥当と認められる会計原則に準拠した財務諸表の作成を可能にするために必要な取引が記録されていること、ならびに発行会社の収入および支出が、発行会社の経営陣および取締役の承認に準拠してのみ行われていることについて、合理的保証をするもの。（3）財務諸表に重要な影響を及ぼす可能性のある、発行会社の資産の無承認での取得、使用、または処分を防止する、あるいは適時に発見することについて、合理的保証をするもの。」に関する方針および手続が含まれると規定される（Id.）。

20) SEC Release 33-8238, *supra* note 15, “II. Discussion of Amendments Implementing Section 404”, “A. Definition of Internal Control”, “3. Final Rules”.

21) 15 U.S.C. § 7241.

22) 17 C.F.R. § 240.13a-14 (a).

23) SOX 法906条（18 U.S.C. § 1350）も、302条同様、開示書類に発行会社の最高経営責任者および最高財務責任者による確認（「確認書（certification）」）の提出を求める。しかし、906条の求める確認の対象は、302条とは異なって、当該開示書類が34年法13条（a）等の要件を完全に遵守していること、その記載情報は発行会社の財政状態・経営成績を重要な全ての点で適正に表示していることのみであり、内部統制は含まれていないことから本稿では扱わない。また、302条に基づく確認書はSECに対するものであるのに対し、906条に基づく確認書は連邦司法省に対するものである点で異なっており（Hazen, *supra* note 2, § 9.28），同違反に対して刑事責任が規定されている。

24) 17 C.F.R. § 229.601 (Item 601) (b) (31) (i).

の設計または運用における著しい不備等が見つかった場合の、取締役会の監査委員会等に対する開示について、実施したこと等の確認をすることを求めている。

(2) 「開示統制手続」の定義

「財務報告に係る内部統制」を定義する SEC ルール13a-15は、その (e) で、「開示統制手続 (disclosure controls and procedures)」について、「34年法のもと提出する書類に、発行会社による開示が求められる情報が、SEC のルールや様式に特定化された期間内に、記録され、記述され、要約され、報告されることを確保することが意図された、発行会社の統制とその他手続を意味する。それは、発行会社が34年法のもと提出する書類に開示が求められる情報が、発行会社の経営陣（最高経営責任者および最高財務責任者または同様の役割を担う者を含む）に集められ伝達されること、それによって、経営陣が求められる開示について適時の判断を可能にすることを確保することが意図された統制と手続を含むが、これに限るものではない。」と定義する。

「財務報告に係る内部統制」と「開示統制手続」の関係につき、「会社の開示統制手続と財務報告に係る内部統制との間には大きな重複が存在する一方で、開示統制手続の要素には財務報告に係る内部統制に包含されないものがあり、内部統制の要素にも開示統制手続の定義に包含されないものがある²⁵⁾」と述べて、両者を採用するに至った。具体的には、SEC は、開示統制手続について、「これらの手続は、発行会社の財務報告に関する (related to) 内部統制が対象とする情報よりも、広い範囲の情報を対象とすることを意図している。たとえば、これらの手続は、…Regulation S-K…に基づき開示の対象となり得る情報が、適時に収集され、評価されることを確保するものでなければならない。これらの手続は、発行会社の事業に関係するリスクおよび進展について、開示する必要があるかどうかを評価するうえで関連する情報を把握するものでなければならない²⁶⁾。」と述べている。

3. 13a-15の規定する「開示統制手続」および「財務報告に係る内部統制」に関する義務

SEC ルール13a-15 (a) は、「開示統制手続」および「財務報告に係る内部統制」について、発行会社にその維持を義務付けている。また、同 (b) は、「開示統制手続」の有効性の評

25) SEC Release 33-8238, *supra* note 15, “II. Discussion of Amendments Implementing Section 404”, “D. Differences Between Internal Control Over Financial Reporting and Disclosure Controls and Procedures”.

26) SEC Final Rule: Certification of Disclosure in Companies’ Quarterly and Annual Reports, Release Nos. 33-8124; 34-46427; IC-25722 (Aug. 29, 2002), available at <https://www.sec.gov/rule-release/33-8124> [hereinafter SEC Release 33-8124], “III. Disclosure Controls and Procedures” “B. Discussion of Disclosure Controls and Procedures”.

価を、同(c)は各事業年度末における「財務報告に係る内部統制」の有効性の評価、同(d)は各四半期に生じた「財務報告に係る内部統制」の変更の評価を、発行会社の経営陣にそれぞれ義務付けている。

すなわち、302条(そのもとのSECルール)の確認対象として、「開示統制手続」および「財務報告に係る内部統制」維持の責任を負うこと、「開示統制手続」の有効性の評価を実施したこと等が規定されているのは前述のとおりであるが、当該制度の維持・有効性の評価自体の義務付けは、302条ではなくSECルール13a-15によっているのである。

実際、SECは、同ルールを提案する際に、「新しいルールである13a-15…はSOX法302条の目的を全面的に補完するもので…ある。…新ルールは、発行会社が十分な開示統制手続を維持する責任も確実に負うようにしており、これにより、最高経営責任者および最高財務責任者がこれらの定期的な評価を監督・検証し、その結果を発行会社の34年法に基づく報告書を通じて証券保有者に報告できるようにしている²⁷⁾。」と述べている。すなわち、発行会社が13a-15(a)によって「開示統制手続」を維持することで、34年法のもと開示が求められる情報が、最高経営責任者および最高財務責任者に集められ伝達され、それによって、求められる開示について適時の判断が可能となり、最高経営責任者および最高財務責任者が、302条の求める、開示統制手続の有効性の評価を実施し、その結果を34年法で求められる開示書類を通じて公表できる、という意味で、13a-15が302条の目的を「全面的に補完する」、ということだと思われる²⁸⁾。

IV. 最近の内部統制に関する制度のエンフォースメント事案

以上のように、34年法13条(b)(2)(B)の定める内部会計統制に、SOX法の規定する内部統制制度が加わり、SECはこれらの内部統制に関する規定に基づいて、どのようにエ

27) Id.

28) SOX法制定後の内部統制をめぐる議論について、実務上の関心が「開示統制手続」よりも「財務報告に係る内部統制」に集中してきたことを指摘するものとして、Donald C. Langevoort, *Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care as Responsibility for Systems"*, 31 J. CORP. L. 949, 955 (2006) 参照。また、「開示統制手続」については、「財務報告に係る内部統制」と比較して研究の蓄積も限られていることが指摘されている。See Thomas R. Weirich & Lori Olsen, *An Analysis and Taxonomy of Disclosure Controls and Procedures Effectiveness*, 10 CURRENT ISSUES IN AUDITING A28, A29 (2016)。「開示統制手続」を対象とする主な研究として、このほか、Essam Elshafie, *The Information Content of Disclosure Controls and Procedures Deficiencies*, J. CONTEMP. BUS. ISSUES, SPECIAL NAAS ISSUE 2017 (2017); Andrew K. Jennings, *Disclosure Procedure*, 82 MD. L. REV. 920 (2023) 等参照。さらに、開示統制手続についての主な邦文研究として、柿崎、前掲注7) 280頁以下、梅村 悠「内部統制に関する情報開示制度の意義と正確性の確保」上智法学論集53巻3号101-140頁(2010)、脇黒丸新太郎「サイバーセキュリティ開示をめぐる日米比較考察－開示制度の実効性を確保するガバナンス体制の視点を踏まえて－」法学研究論集56号173-195頁(2022)、同「開示・統制手続違反に対するSECエンフォースメントの比較検討」大阪商業大学論集18巻3号51-66頁(2023) 等がある。

ンフォースメントを行なっているのだろうか。本稿では、近年増加しているサイバー攻撃を受けた会社の対応が問題となった事案を取り上げ、どのように責任が肯定されているのかを検討する。

まず最初に、2024年6月に出されたRRD社の事案を取り上げる。これは、SECが、34年法13条(b)(2)(B)を会社の会計処理および財務報告の正確性に直接的に影響を与えない事案に適用したものである。同規定は、開示書類に不実記載がなくとも、同規定の要件を満たせば、欺罔の意図(scienter)の立証なく²⁹⁾責任を肯定できるもので、SOX法制定後においても、SECにとって依然強力な武器である³⁰⁾。もっとも、同規定は内部会計統制を定めるもので、その対象は会計処理や財務報告との関連あるものに限られると理解されてきた³¹⁾。

RRD社の事案が出される前に、SECは、13条(b)(2)(B)の定める内部会計統制の範囲を広げ、同規定の対象に、法令を遵守しているかを審査することを確保するプロセスを含むように解釈し責任を肯定した事案³²⁾が存在していた³³⁾。これらに続き、13条(b)(2)(B)の適用範囲をサイバーセキュリティ統制に拡大しようとする試みがRRD社の事案であったと言える。

それでは、この事案でどのような議論が展開されたのか。以下、紹介する。

29) SEC v. World-Wide Coin Investments, Ltd., 567 F. Supp. 724, 751 (N.D. Ga. 1983).

30) なお、34年法13条(b)(2)の内部統制要件違反は私的訴権を認めていない。Hazen, *supra* note 2, § 9.23.

31) 13条(b)(2)(B)によって責任が認められた最近の事案として、例えば、*In re Portland General Electric Company*, Exchange Act Release No. 100917, 2024 SEC LEXIS 2165 (Sep. 4, 2024), *In re Circor International, Inc.*, Exchange Act Release No. 100934, 2024 SEC LEXIS 2174 (Sep. 5, 2024), *In re Quantum Corp.*, Exchange Act Release No. 87812, 2019 SEC LEXIS 5358 (Dec. 20, 2019), *In re National Energy Services Reunited Corp.*, Exchange Act Release No. 100845, 2024 SEC LEXIS 2091 (Aug. 28, 2024) 等が挙げられる。

32) *In re Andeavor LLC*. Exchange Act Release No. 90208, 2020 SEC LEXIS 4602 (Oct. 15, 2020) *In re Charter Communications, Inc.*, Exchange Act Release No. 98923, 2023 SEC LEXIS 3284 (Nov. 14, 2023) は、両者ともに、会社の行う株式買戻しが法令や社内のルールを遵守しているかにつき審査するための合理的なプロセスが設けられていなかったとして、13条(b)(2)(B)の「(i) 経営陣の一般的または個別的承認に従って取引が執行されること、… (iii) 資産へのアクセスは経営陣の一般的または個別的承認に従った時のみ許されること」について、合理的保証をするのに十分な内部会計統制の制度の構築・維持が求められるという規定に違反すると認定された。

33) Andeavor社およびCharter社の事案ともに、それぞれHester M. Peirce委員およびMark T. Uyeda委員による反対の意を表明する声明が出されている(Andeavor社につき<https://www.sec.gov/newsroom/speeches-statements/peirce-roisman-andeavor-2020-11-13>, Charter社につき,<https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-charter-communications-111423>)。同声明は、13条(b)(2)(B)が求めているのは一般的な「内部統制」ではなく「内部会計統制」を求めていること、SEC命令の解釈は、13条(b)(2)(B)の文言、立法史、および同規定の歴史的発展から大きく離れていること、会社の会計および財務諸表の正確性に直接影響を与えない事項について13条(b)(2)(B)の範囲に含めることはできないことが論じられている。

1. 34年法13条 (b) (2) (B) を基礎に責任が問えるかが問題となった事案

(1) *In re R.R. Donnelley & Sons Co.*³⁴⁾

(a) 事案の概要

RRD 社はビジネス・コミュニケーション・サービスとマーケティング・ソリューションを世界的に提供している業者で、業務の一部として顧客の大量の機密データの保存・転送サービスを行っていた。2009年8月から2016年8月まで NASDAQ で取引され、2016年8月から2022年2月まで NYSE に上場していた。

RRD 社内部にサイバー攻撃発見システムが設置されており、それから発せられる警告は、まず第三者によって運営されるセキュリティ・サービス・プロバイダ (MSSP) によって審査され、その後 RRD 社内部のサイバーセキュリティ担当部局に報告される仕組みになっており、承認されていないインシデントが特定された場合、その対応改善策は RRD 社内部の担当部局と MSSP によって行われることになっていた。

RRD 社は2021年11月29日から同年12月23日の間に生じたランサムウェア攻撃を受けた。その間、同社はサイバーセキュリティリスクとインシデントの開示に関する、34年法で定義される有効な開示統制手続を設計しておらず、また、同社の資産（取扱注意のビジネスおよび顧客情報を含む IT システムとネットワーク）へのアクセスが経営陣の承認のもとでのみ許されることを合理的に保証するのに十分なサイバーセキュリティ関連の内部会計統制システムを構築・維持していなかった。これらの内部会計統制に欠陥があった結果、上記ランサムウェア攻撃に速やかに対応することができなかった。

具体的には、RRD 社のサイバーセキュリティ警告の審査・インシデント対応の方針および手続は優先事項の枠組みを十分設定していなかった上に、インシデントに対応するための手続について内部および外部の担当者に対して明確なガイダンスを提供していなかった。さらに、RRD 社は MSSP の警告審査および報告を監督するための十分な内部統制を構築していなかった。上記ランサムウェア攻撃の間、RRD 社の資産へのアクセスが経営陣の承認のもとでのみ許されることを合理的に保証するのに十分な内部会計統制を構築・維持していなかったことがハッカーに利用されてしまった。

また、RRD 社にとってデータの完全性と機密性は重要なものであったにもかかわらず、RRD 社は適切な情報が経営陣に伝達され、潜在的に求められる開示について適時の判断を可能にすることを確保するための、サイバーセキュリティのインシデントについての有効な開示関連の統制手続を設計していなかった。例えば、RRD 社のサイバーセキュリティの手続および統制は警告やインシデントに関連するすべての適切な情報が RRD 社において開示

34) Exchange Act Release No. 100365, 2024 SEC LEXIS 1422 (June 18, 2024)

判断権限を有する者に速やかに報告されることを確保するよう設計されていなかった。また、そのような情報を経営陣に報告することに責任を負う者についてガイダンスを与えていなかった。その結果、RRD 社の発見システムや MSSP からランサムウェア攻撃に関する情報を有していたにもかかわらず、RRD 社は開示の観点からそれらを十分に評価できなかった。

上記ランサムウェア攻撃で、脅威アクター（攻撃者）は詐欺的なハッキング手法を用いて、RRD 社の一部のコンピュータに暗号化ソフトウェアをインストールし、70ギガバイトのデータを流出させたが、これには RRD 社の 2 万 2,000 社の顧客のうち 29 社のデータが含まれており、その一部には個人識別情報や財務情報が含まれていたことが判明したが、RRD 社の調査では、攻撃者が RRD 社の財務システムおよび会社の財務・会計データにアクセスしたという証拠は発見されなかった。

2021年12月27日、RRD 社はランサムウェア攻撃について公表した。

以上のことから、RRD 社は、会社の資産（取扱注意のビジネスおよび顧客情報を含む IT システムとネットワーク）へのアクセスが経営陣の一般的または個別的な承認にしたがう場合のみ許されることを合理的に保証するのに十分な内部会計統制の制度を構築・維持していなかったことから 34 年法 13 条 (b) (2) (B) に違反したことが認められる。また、RRD 社は、それが提出する書類に開示が求められる情報が SEC ルールや様式に記載された期間内に、記録され、記述され、要約されおよび報告されることを確保することが意図された開示統制手続を維持していなかったことから 13a-15 (a) にも違反したことが認められる。

これらのことから、34 年法 21C 条に基づき、同法 13 条 (b) (2) (B) および SEC ルール 13a-15 (a) 違反に関する排除（cease and desist）命令、および民事制裁金（civil penalty）212 万ドルの支払い命令が発せられる。

(b) 上記命令に対する声明（statement）

これに対して、34 年法 13 条 (b) (2) (B) に関する上記命令に反対の意を表明する声明が Hester M. Peirce 委員および Mark T. Uyeda 委員から出されている³⁵⁾³⁶⁾。

SEC の命令は、RRD 社が 13 条 (b) (2) (B) (iii) に違反すると結論づけるところ、この「資産」を「取扱注意のビジネスおよび顧客情報を含む IT システムとネットワーク」と

35) <https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-rr-donnelley-061824>

36) 反対の意を表明する声明は、冒頭で、SEC が 34 年法 13 条 (b) (2) (B) が定める「内部会計統制」の規定を「発行会社（上場会社）に対して SEC が賢明と考える方針や手続の導入を強制するための『万能ナイフ（スイスアーミー・スタチュート）』のように扱っている」と述べていた。その上で、本件で SEC が、この「多目的ツール」に「サイバーセキュリティ関連の内部会計統制システム」という新しい機能を追加したことについて厳しい批判を展開している。同声明は、34 年法 13 条 (b) (2) (B) の「内部会計統制」を「万能ナイフ」と呼ぶに至った事案として、前掲注 32)、33) で触れた、2020 年 11 月の Andeavor 社の事案、2023 年 11 月の Charter の事案を挙げている。

するが、この解釈は13条 (b) (2) (B) の内部会計統制条項でカバーされる種類の「資産」には当たらない。

13条 (b) (2) (B) は、米国公認会計士協会 (American Institute of Certified Public Accountants (“AICPA”)) の監査基準書 (Statement on Auditing Standards No.1 (“SAS”)) に由来する。SAS は内部会計統制の文脈で「資産の保全とは、取引を処理し関連資産を売買する際に、故意または故意でない誤りから生ずる損失から保護することのみを指す」とし、取引には資産またはサービスの交換を含み、取引や関連資産の流れに含まれるその主要な役割には、取引の承認、執行および記録とその結果生ずる資産の説明責任を含むと説明する。

監査基準書 (SAS) は、取引における資産の使用および処分のために、正確な会計記録の作成・維持を重視していることから、「資産へのアクセスは経営陣の…承認に従った時のみ [許される]」の、「資産」が、会社のあらゆる資産に関係しているのではなく、むしろ特定の性質を持つ資産、すなわち「会社取引の対象となる資産」に関係しているものということが明らかである。

監査基準書 (SAS) は統制 (controls) の定義について、2つのはっきりと異なる分類をした。それは管理統制 (administrative controls) と会計統制 (accounting controls) である。管理統制は会計統制に先行するものであり、組織の計画、ならびに経営陣による取引の承認に至る判断プロセスに関係する手続および記録を含む。これとは対照的に、会計統制は取引それ自体に焦点を当て、資産の保全や財務記録の信頼性に関係する。

本件で、資産とされる RRD 社のコンピュータシステムは、その本質的な特徴を備えていない。それは、会社の所有物という意味においては資産を構成するものの、会社取引の対象にはならない。それは、せいぜい、会社資産の取引を処理するに過ぎず、内部会計統制が関心を持っているのは、会社資産そのものの使用および処分である。会社資産の取引を処理するための手段に関連する統制は、取引承認「前」の、経営陣の判断に関係する「管理統制」としてより適切に分類される。

SEC の命令は13条 (b) (2) (B) (iii) の「資産」を構成するものについて広く解釈し、新しい境地を開こうとするもので誤っている。命令は内部会計統制とより広い管理統制との間の区別を無視している。この区別は13条 (b) (2) (B) の適切な適用範囲を理解し維持するために大変重要である。

(c) 検討

本件は、サイバー攻撃を受けた RRD 社が、「開示統制手続を設計しておらず」、また「サイバーセキュリティに関連した内部会計統制の制度を構築・維持していなかった」ことから、「ランサムウェア攻撃に速やかに対応することができなかった」として、SEC ルール 13a-15 (a) および34年法13条 (b) (2) (B) に違反するとされた。後者につき、13条 (b)

(2) (B) は、その (iii) で「資産へのアクセスは経営陣の一般的または個別的承認に従った時のみ許されること」を合理的に保証するのに十分な内部会計統制の制度の構築・維持をすることを求めているところ、本件では、「取扱注意のビジネスおよび顧客情報を含む IT システムとネットワーク」という同社の資産へのアクセスがそのように合理的に保証されるのに十分な「サイバーセキュリティ関連の内部会計統制システム」の構築・維持がなされていなかったとして違反が認められた。

これに対して、反対の意を表明する声明は、SEC の命令における「資産」の解釈は、13 条 (b) (2) (B) における内部会計統制の定義が採用される元となった SAS における「資産」の解釈（会社取引の対象になるという特徴を備えるもの）とは矛盾しており、RRD 社のコンピュータシステムは「資産」には該当せず、「管理統制」としてより適切に分類されるものであると論じた。すなわち、SEC 命令の述べるような「サイバーセキュリティ関連の内部会計統制システム」は認められないとした。

このように、13 条 (b) (2) (B) (iii) の「資産」について、SEC 命令が広く解して責任を認めたのに対し、反対する声明はそのような「資産」は従来の解釈と相容れず、採り得ないとして否定した。

RRD 社に対する手続のちょうど 1 ヶ月後の 2024 年 7 月 18 日、ニューヨーク州南部地区連邦地方裁判所から、まさにこの、13 条 (b) (2) (B) における内部会計統制の（「資産」も含めた）解釈を示した判決が出された。SolarWinds 社判決である。以下紹介する。

(2) SEC v. SolarWinds Corp.³⁷⁾

(a) 事実

SEC は、最上位の安全とされるソフトウェアを政府機関や民間企業に販売している S 社と、同社の最高情報セキュリティ責任者（CISO）である B に対して、(1) S 社が、33 年法・34 年法で提出が義務付けられる情報開示書類や同社のウェブサイト等において、同社の製品や業務のサイバーセキュリティが脆弱であるという事実を隠し、同社の主力商品サイバー攻撃に対する脆弱性が最小限であると投資者に誤解させた、(2) 同社が、数ヶ月にわたって SUNBURST として知られる大規模なサイバー攻撃を受けていたことについて投資者に誤解させたとして、34 年法 10 条 (b)、SEC ルール 10b-5 (b)、13 条 (a)、33 年法 17 条 (a)、34 年法 13 条 (b) (2) (B)、SEC ルール 13a-15 (a) に基づき、訴えを提起した。

(b) 判旨（ここでは、34 年法 13 条 (b) (2) (B) に関する議論のみ取り上げる。）

SEC は、S 社のサイバーセキュリティの欠陥は、13 条 (b) (2) (B) (iii) に基づき責任

37) 741 F. Supp. 3d 37 (S.D.N.Y. 2024).

を追及できると主張する。その理由として、(1) 同社のソースコード、データベース、および製品は同社の最も重要な資産であったが、(2) 同社の不十分なアクセス管理、脆弱な内部パスワードポリシー、および VPN セキュリティギャップの結果、同社はこれら資産へのアクセスを「経営陣の一般的または個別的承認に従った時のみ」に制限できず、外部の攻撃者によるアクセスを可能にしてしまったからである。S 社は、13条 (b) (2) (B) は、SEC に発行会社の「内部会計統制のシステム」を規制する権限を与えているが、この文言から、パスワードや VPN プロトコルといった会社のサイバーセキュリティ統制 (cybersecurity controls) をカバーすると合理的に解釈することはできないと反論している。S 社の反論は明らかに正しい。

さまざまな点から、制定法の文言は、「内部会計統制のシステム」が会社の財務会計を指していることを強く裏付けている。「会計 (accounting)」という用語は、「事業および財務の取引を記録および要約し、その結果を分析、検証、報告するシステム」と広く定義される。また、13条 (b) (2) (B) で連邦議会が用いた文言——特に “transactions,” “preparation of financial statements,” “generally accepted accounting principles,” and “books and records” ——は、共通して財務会計と一貫している。このように、同規定をサイバーセキュリティ統制に適用しようとする SEC の主張は退けられることになる。また、議会が「内部会計統制のシステム」をサイバーセキュリティ統制への適用を含むように意図していたという他のいかなる証拠もない。(もっとも、この法令が制定されたのは1977年であり、サイバーセキュリティがビジネスや社会に関連する概念となるずっと前のことであるから当然である。)

13条 (b) (2) (B) (iii) の「内部会計統制」という文言を解釈した数少ない裁判所は、一貫してそれを財務会計に向けられたものと解してきた。例えば、SEC v. World-Wide Coin Investments, Ltd., 567 F. Supp. 724 (N.D. Ga. 1983) は、「内部会計統制」を「資産を保護し、財務記録の信頼性を保証する統制であり、その主な仕事の1つは、会社の会計システムで発生するエラーや不正を防止・検出することである」と定義した。また、内部会計統制は、財務諸表、財務諸表が作成される会計システムおよび記録の信頼性を示す基本的な指標とも述べた。McConville v. SEC, 465 F. 3d 780 (7th Cir, 2006) は、内部会計統制の例として、記録の完全性、正確性、真正性をチェックするための手動または自動によるレビュー、取引を完全かつ正確に記録する方法、誤りを発見するための会計入力との照合などを挙げている。

以上を踏まえると、発行会社が「内部会計統制のシステムを構築・維持する」という要件は、発行会社が財務に関係する取引や出来事を正確に報告、記録および照合することを要求していると適切に読み取ることができる。サイバーセキュリティの欠陥（例えば、パスワードの選択ミスといったもの）を発見できないことは会計上の問題とは合理的には解されず、

サイバーセキュリティ統制は同規定の文言に適合しないと見るのが自然である。サイバーセキュリティ統制は極めて重要であり、その機能不全はシステム全体に損害を及ぼす可能性がある。しかし、これらの統制 (controls) は、「会社の会計システムで発生するエラーや不正を防止・検出する」ために置かれているとは言えない。

SEC は、「資産へのアクセスは経営陣の一般的または個別的承認に従った時のみ許されることの合理的保証をする」(13条 (b) (2) (B) (iii)) ために必要であることを理由に、同条はサイバーセキュリティ統制を規制する権限を必要としていると主張する。SEC はサイバーセキュリティ統制の欠陥は、会社の中核的資産を損害や破壊にさらし、その価値を低下させる可能性があるとして指摘する。しかし、この議論は、同条の適用範囲を限定する重要な文言、すなわち「内部会計統制」の制度であることに触れていない。その文言により、13条 (b) (2) (B) は、上場会社がその資産への不正アクセスを防止するために使用するすべての内部システムをカバーするものではなく、内部会計の統制として適格なもののみをカバーしているのである。

(c) 検討

SEC は、RRD 社に対する手続の時と同様、13条 (b) (2) (B) (iii) の「資産」を広く解して、同社のソースコード、データベース、および製品がそれに当たるとし、S 社はこれら資産へのアクセスを「経営陣の一般的または個別的承認に従った時のみ」に制限できなかったとして、同条違反を主張した。

しかし、連邦地裁は、13条 (b) (2) (B) の規定する「内部会計統制」は、制定法の文言およびこれまでの判例における解釈から、会社の財務会計に向けられたものと解釈すべきとした上で、SEC の「資産」の解釈はこれとは整合しないと、否定した。

本判決後³⁸⁾、サイバー攻撃を受けた会社の対応について、SEC は13条 (b) (2) (B) の規定する「内部会計統制」違反は使わず、開示義務違反 (33年法17条 (a) (2) および (3)、34年法13条 (a) 違反) で責任追及をしている。4 社に対する手続が同一日に出されており、

38) SolarWinds 社および CISO に対する訴訟について、SEC は2025年11月20日、再提訴不可能な形で取り下げる (dismiss, with prejudice) 旨の共同合意書を提出した。Joint Stipulation to Dismiss, and Releases, SEC v. SolarWinds Corp., 1 : 23-cv-09518-PAE, Litigation Release No. 26423, 2025 SEC LEXIS 2904 (S.D.N.Y. Nov. 20, 2025) 参照。この訴えの取下げは、SEC が2025年2月に公表した、サイバー・新興技術部門 (CETU) を設置し、CETUの重点分野としてさまざまな詐欺行為や詐欺の開示を挙げていたりリリース (“SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors”, Press Release 2025-42 (Feb. 20, 2025)) とあわせて、SEC 自身が開示の瑕疵に関するより微妙で複雑な主張に基づく執行から、投資者に損害をもたらす重大な虚偽表示に重点を置く、原点に立ち返る (“back to basics”) アプローチへの方針転換を示すものとして捉えられるとの評価もみられる。Andrew Tannenbaum and Anna Rudawski, *SolarWinds Dismissed: What the SEC’s U-turn Signals for Cyber Enforcement*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Dec. 7, 2025), <https://corpgov.law.harvard.edu/2025/12/07/solarwinds-dismissed-what-the-secs-u-turn-signals-for-cyber-enforcement/>.

以下、まとめて紹介する。

2. 開示義務違反・開示統制手続を基礎に責任が問えるかが問題となった事案

(1) *In re Avaya Holdings Corp.*³⁹⁾, *In re Check Point Software Technologies Ltd.*⁴⁰⁾,
*In re Mimecast Limited*⁴¹⁾, *In re Unisys Corp.*⁴²⁾

(a) 事案の概要

これらはいずれも、SolarWinds 社の Orion software による、機密情報を含めたデータや電子メール、ソースコード等への不正アクセス等のシステム侵害が生じたことに関する事案である。

① Avaya 社

同社は、四半期報告書（フォーム10-Q）を提出したが、その中で、自社の調査の過程において、「限られた数の当社電子メールメッセージへのアクセスの証拠」を特定したものの、「当社の他の内部システムへの不正アクセスの現時点での証拠はない」と記載し、また、「当社は、このインシデントが当社のビジネスまたは業務に重大な悪影響を及ぼした、あるいは及ぼすであろうとは考えていない」とも記載していた。しかし、これは重大な誤解を招く記述を含んでいた。なぜなら、上記の開示書類は、その提出時点で同社が把握していた重大な情報である、サイバー攻撃が国家レベルの攻撃者によるものである可能性が高いこと、同社のシステム内に攻撃者が長期間にわたり監視されない状態で存在していたこと、機密情報が含まれる少なくとも145の共有ファイルへのアクセスがあったこと、攻撃者がサイバーセキュリティ担当部署の一人のメールボックスにアクセスしていたことを記載していなかったからである。以上のことから33年法17条（a）（2）および（3）⁴³⁾、34年法13条（a）違反等が認められ、違反行為の排除命令、および民事制裁金100万ドルの支払い命令が発せられる。

39) Securities Act Release No. 11320, Exchange Act Release No. 101398, 2024 SEC LEXIS 2840 (Oct. 22, 2024).

40) Securities Act Release No. 11321, Exchange Act Release No. 101399, 2024 SEC LEXIS 2839 (Oct. 22, 2024).

41) Securities Act Release No. 11322, Exchange Act Release No. 101400, 2024 SEC LEXIS 2836 (Oct. 22, 2024).

42) Securities Act Release No. 11323, Exchange Act Release No. 101401, 2024 SEC LEXIS 2844 (Oct. 22, 2024).

43) 33年法17条（a）は、33年法に規定された詐欺禁止条項（34年法の10b-5に相当）である。33年法の規定は、通常は発行市場のみに向けられているが、17条（a）はその例外で、流通市場での売買にも適用されることが、*United States v. Naftalin*, 441 U.S. 768 (1979) で明らかにされている（17条（a）は、「新規の募集・売出しの過程であるか、あるいは通常の市場取引の過程であるかを問わず、証券の売付けまたはオファーにおけるあらゆる詐欺的な仕組みを対象とすることを意図していた」（at 777-778）と述べている）。また、17条（a）（2）および（3）は、同（1）とは異なって、欺罔の意図（scienter）の立証が不要であることが、*Aaron v. SEC*, 446 U.S. 680 (1980) で明らかにされている。

② Check Point 社

同社が提出した年次報告書（フォーム20-F（外国会社向け））は、サイバーセキュリティ・リスクについて、「当社は、インターネット経由での不正アクセスや、当社の情報技術（IT）システムへの悪意あるソフトウェアの導入を試みる第三者からの攻撃に日常的に直面している」、「さらに、悪意あるハッカーが不正アクセスを試みる可能性がある……」、「当社は時折、当社の製品およびネットワークへの侵入や不正アクセスの試みに遭遇する」といった一般的な表現で記載するにすぎず、攻撃者による同社ネットワークへの侵入という事実を踏まえた、サイバーセキュリティ・リスクに関する重大な変化を反映した開示の更新を行わなかった。同社の開示は、その前年度（サイバー攻撃を受ける前）のサイバーセキュリティ・リスク要因に関する開示と同一であり、一般的かつ同社「固有のサイバーセキュリティ・リスクおよびインシデント」に即したものではなかったため、インシデント発生後に同社が直面し認識していたサイバーセキュリティ・リスクについて、重大な誤解を招くような印象を与えるものとなっていた。以上のことから、33年法17条（a）（2）および（3）、34年法13条（a）違反等が認められ、違反行為の排除命令、および民事制裁金99万5,000ドルの支払い命令が発せられる。

③ Mimecast 社

同社が提出した臨時報告書（フォーム8-K）には、「証拠によれば、当該証明書は少数の顧客を標的とするためにのみ使用された」と記載されているが、同社は、攻撃者が、（同社の顧客の大多数を占める）約31,000社の顧客の暗号化された認証情報を含むデータベース、および約17,000社の顧客のサーバー・構成情報を含むデータベースにアクセスしたという事実を公表しなかった。

また、同臨時報告書には、「調査の結果、攻撃者が当社のソースコードリポジトリの一部（限定された数）にアクセスし、これをダウンロードしたことが判明した。…当社は、攻撃者がダウンロードしたソースコードは不完全であり、当社のサービスのいかなる部分の構築や実行にも不十分であると考えている。」と記載したが、攻撃者が同社の「exgestion（データ取り込み・処理）」ソースコードの58%、「M365認証」ソースコードの50%、「M365相互運用性」ソースコードの76%を外部に流出させ、これらの3つの領域におけるソースコードの大部分を占めていたという事実を記載しなかった。これらが、国家の支援を受けているとされる攻撃者に流出したという事実は、同社の投資者にとって重要である。以上のことから、33年法17条（a）（2）および（3）、34年法13条（a）違反等が認められ、違反行為の排除命令、および民事制裁金99万ドルの支払い命令が発せられる。

④ Unisys 社

（i）開示義務違反

同社は、2020年度、2021年度の年次報告書（フォーム10-K）に、重大な誤解を招き、か

つ同社固有のリスクやインシデントに十分に適合（個別化）させていないサイバーセキュリティ・リスク開示をしていた。すなわち、同社は、複数回の侵入が実際に発生しており、かつ実際に機密情報の不正アクセスおよび流出を伴っていたことを把握していたにもかかわらず、侵入の成功という事実の存在や、データおよび情報への不正アクセスのリスクについて、仮定的な表現で、不正確に記載していた。よって、33年法17条（a）（2）および（3）⁴⁴⁾と34年法13条（a）違反等が認められる。

（ii） 開示統制手続の維持義務違反

また、同社のサイバーセキュリティ担当部門は、攻撃を受けていることに気づいてから1年が経過するまで、開示の判断権者に対してそれを報告せず、また恐喝インシデントについては、ハッカーらによる公開声明がなされるまで、報告しなかった。これは、当時、同社において、重大なサイバーセキュリティ・インシデントを巡る情報が、とりわけ開示に責任を持つ経営陣に報告され、それによって投資者に対して適時に報告されることを確実にするよう設計された、開示統制手続がなかったことによる。すなわち、同社においては、重大な可能性のあるインシデントを経営陣および開示の判断権者にエスカレーション（報告）することを義務付ける、実効的な統制を維持しておらず、また、同社の開示の判断権者が、インシデントに関するどの情報がSECへの提出書類において開示を求められる可能性があるかを判断するために、同社が保有するサイバーセキュリティ・インシデントに関する情報を確実に確認できるよう設計された、統制および手続を備えていなかったのである。このことは、年次報告書に重大な誤解を招くリスク要因の開示をもたらす原因となった。よって、13a-15（a）違反が認められる。

以上のことから、違反行為の排除命令、および民事制裁金400万ドルの支払い命令が発せられる。

（b） 上記命令に対する声明

上記命令に反対の意を表明する声明がHester M. Peirce 委員およびMark T. Uyeda 委員から出されている⁴⁵⁾。

Avaya 社と Mimecast 社は、サイバー攻撃に関する情報を開示したが、SEC は、その開示に一定の重要な情報を含めていないと判断した。Check Point 社と Unisys 社は、サイバー攻撃に対応して既存のリスク要因情報を更新しなかったため、重大な誤解を招くものになったと判断した。

これらを通じて、SEC は、会社の開示が投資者に対して重要な情報を提供するか否かを

44) 15 U.S.C. § 77q (a).

45) <https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224>

考慮しているというより、責任を認めるために、開示されていない、重要ではない細部の情報を挙げて、後知恵的に会社の開示内容を批判していることから、私たちは反対する。

① Avaya 社

Avaya 社について、SEC は、開示されていない重要な情報の例として「[サイバー攻撃]が国家レベルの攻撃者によるものである可能性が高いこと」を強調している。しかし、2023年のサイバーセキュリティ・インシデント開示に関するルール⁴⁶⁾(2023年ルール)制定の際、投資者も SEC も、攻撃者の身元が重要な情報であるとの見解はとっていなかった。2023年ルールを制定する際、SEC は、サイバーセキュリティ・インシデントの開示について、「インシデントそのものに関する詳細」よりも「インシデントの……影響」に「主として……焦点を当てる」べきであると述べていた。攻撃者の身元は明らかに「インシデントそのものに関する詳細」である。それにもかかわらず、SEC は、当該情報が重要であるとの見解を示すことにより、法執行を通じた規制 (regulates by enforcement) を行なっている。

また、Avaya 社が2021年2月にサイバー攻撃に関する情報を開示した時までに、既にロシアが攻撃者である可能性が高いという広範なメディア報道や政府機関による共同声明が出されていた。Avaya 社の開示では、同社のインシデントが SolarWinds 社へのサイバー攻撃と関連付けられていなかったものの、サイバー攻撃に関する既存の公表された情報を考慮すると、合理的な投資者にとって、インシデントがロシアによるものと開示されても、Avaya 社に関する「情報のトータルミックスを大きく変える (“significantly altered the ‘total mix’ of information”)」とは考えにくい。

また、SEC が Avaya 社によって開示されなかった重大な情報として他に指摘したものも、「インシデントの『影響』」ではなく「インシデントそのものに関する詳細」であり、SEC 自身が開示を要しないとしていた事項に該当する。

② Mimecast 社

SolarWinds 社判決は、フォーム 8-K が重大な誤解を招くものであるかどうかを評価するには「大局的な見地と文脈が極めて重要⁴⁷⁾」であり、また「開示が全体として読まれた場合に全体像を捉えている⁴⁸⁾」のであれば、その提出書類は誤解を招くものではないと述べた。

SEC が Mimecast 社に対する責任を問うにあたって、インシデントの影響という、より大きな全体像とは対照的に、攻撃者が顧客の認証情報を含むデータベースにアクセスしたという「詳細な事実」に焦点を当てている。認証情報へのアクセスそれ自体は、脅威アクターが

46) SEC Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023), available at <https://www.sec.gov/rules-regulations/2023/07/s7-09-22#33-11216> [hereinafter SEC Release 33-11216].

47) *SolarWinds Corp.*, 741 F. Supp. 3d, at 100.

48) *Id.*, at 102.

顧客情報を不正に流出させるためにその認証情報を使用しない限り、重大ではない可能性がある。Mimecast 社の開示は、全体として読めば、認証情報への不正アクセスと、不正流用された情報の欠如に関する完全なストーリーを伝えている。Avaya 社のケースと同様に、SEC が指摘する開示されなかった情報は、開示する必要のない「インシデント自体に関する詳細な事実」である。

これらに加え、2023年ルールの一部として制定されたフォーム 8-K の Item 1.05に基づく開示が、SEC の本事案における判断によって影響を受けてしまうことについても懸念している。Item 1.05は、会社に対し、重大なサイバーセキュリティ・インシデントの性質、範囲、および時期に関する重要な要素を開示することを求めているところ、会社は、SEC による後知恵的な批判を避けるため、Item 1.05の開示としてインシデントに関する重要でない細目的情報を記載したり、さらに悪いことに、重要でないインシデントに関する開示を行う可能性もあるからである。

③ Check Point 社

SolarWinds 社判決において、SEC は、同社のリスク開示について、「自社のセキュリティシステムに不備があるとの社内認識」があったにもかかわらず、その記載が「容認できないほど定型かつ一般的」であったと主張した⁴⁹⁾。しかし裁判所は、SolarWinds 社のリスク開示内容を詳細に検討した結果、その開示は、同社が直面していたサイバーセキュリティ・リスクの種類や性質、およびそれらが同社の財務の健全性や将来にもたらし得る重大な結果について、投資者に注意を喚起するのに十分なものであったと結論付け、SEC の主張を退けた。よって、Check Point 社の責任を認める根拠となる主張も慎重な検討が必要となる。SolarWinds 社判決の論じた内容に照らせば、SEC の主張に再考すべき余地があると考えられるからである。

④ Unisys 社

ある事象が実際に発生し、会社に重大な影響を及ぼした場合には、一般的に、当該事象は開示書類の別の箇所（事業の概況、経営陣による財政状態および経営成績の分析（MD&A）、あるいは財務諸表およびその注記など）において開示することが求められる。ある仮定上のリスクが現実化したことを受けてリスク開示を更新すべきかどうかという判断は容易ではなく、SEC はこれに関して法的措置を講じることに慎重であるべきである。リスク要因は本質的に仮定上の事象を開示するものであるから、もし SEC が抑制的な姿勢をとらなければ、あらゆる会社のリスク開示において違反が認定されかねず、発行会社は重要性の低い事象の発生までリスク開示に盛り込む事態を招くおそれがあるからである。

49) SEC は、SolarWinds 社が2018年に提出したフォーム S-1で開示されたサイバーセキュリティのリスク要因情報が、すでに具体化していたにもかかわらず、その後の情報開示で更新されないままであったことは、同社が直面していたリスクを重大な程度に低く述べていたと主張した。

(c) 検討

SolarWinds 社判決の後に出了されたこれらの事案では、内部会計統制違反ではなく、全ての事案で開示義務違反によって責任が肯定された。手続の中で SEC は、発行会社が何か積極的な虚偽記載をしたのではなく、開示すべき情報を開示していないと主張していた。具体的に、Avaya 社、Mimecast 社で、SEC は、サイバーセキュリティ・インシデントについて一応開示したものの、重要な事実がそれに含まれていなかったと主張し、Check Point 社、Unisys 社では、リスク・ファクター開示が一般的（仮定的）な表現でなされており、同社固有のリスクに即したように更新されていなかったと主張した。

これに対して、反対の意を表明する声明は、Avaya 社、Mimecast 社については、投資者の判断に重要ではない、詳細な事実を開示していないとして責任を課すことは、SolarWinds 社判決で述べられたこと（開示全体から全体像を捉えられることが重要）と矛盾する上に、SEC 自身が2023年ルールを制定する際にとっていた立場（「インシデントそのものに関する詳細」よりも「インシデントの……影響」を重視）とも相容れないとして、批判した。Check Point 社、Unisys 社については、SolarWinds 判決における、SEC によるリスク開示が「容認できないほど定型かつ一般的」との主張が否定されたこと、リスク開示の更新の判断は容易ではないことから、SEC はこれらに基づいて責任を認めることに慎重であるべきと、論じた。

上記声明のうち、Check Point 社に関して言及された SolarWinds 社判決において、連邦地裁は、複数の判例を引用しながら「リスク開示が、訴訟提起の対象となり得ると判断されるのは、その開示が『すでに発生している（現実化している）リスクについて警告していた』ということが十分に主張・立証されているという、限定的な状況に限られている⁵⁰⁾」と述べていた⁵¹⁾。すなわち、法定開示書類に開示が求められる事柄（重要な情報）についてリスクを警告しているということは、（すでにリスクが現実化しているにもかかわらず）合理的な

50) *SolarWinds Corp.*, 741 F. Supp. 3d, at 90.

51) なお、SolarWinds 社判決では、リスク開示に不備があったことも争われたが、その一方で、開示書類における虚偽記載も認められている。それは、ウェブサイトに掲載されていた「セキュリティに関する声明（Security Statement）」（S 社が顧客にセキュリティのインフラと実践に関するより詳細な情報を提供することを目的としたもの）に記載されていた、5つのサイバーセキュリティ慣行のうち少なくとも2つ「強力なパスワード保護を備えていたこと」および「適切なアクセス制御を維持していたこと」に関する部分である。具体的には、アクセス権制御について、「セキュリティに関する声明」では、「従業員は、それぞれの職務に基づき、特定の追加リソースへのアクセスを許可されている」、「当社は機密データへのアクセスを『必要最小限の権限』に基づいて提供している」と記載され、公に向けた表示がなされていたが、実際は同社において従業員に広範囲に管理権限を付与していた。従業員への管理者権限の付与がほぼ無差別に行われていることは、セキュリティに関する声明と明らかに矛盾していたことから、虚偽記載とされたのである。これに対して、SEC が S 社によるプレスリリース、ブログ投稿、ポッドキャストで同社の強力なサイバーセキュリティ対策について述べていたことについては、いずれも法的責任を生じさせない会社の誇大広告とみなされ、合理的な投資者がそれを信頼するにはあまりに一般的として否定された。

投資者に「まだリスクは発生していない」という誤った印象を重要な点で与えることから責任は認められる、ということだと思われる⁵²⁾。

SEC 自身も、この立場で（「すでに発生している（現実化している）リスクについて警告していた」として）虚偽記載を認めた事案が存在する。以下紹介する。

（2） *In re Blackbaud, Inc.*⁵³⁾

（a） 事案の概要

さまざまな非営利組織にドナーに関する情報を管理するためのソフトウェアを提供している会社である B 社は、会社のシステムへの不正アクセスを発見し、当該インシデントについて、会社のウェブサイト公表し、影響のあった顧客に通知した。その公表・通知において、B 社は当該サイバー犯罪者による銀行口座情報や社会保障番号へのアクセスはなかった旨述べた。しかしこの数日後、B 社の従業員はさらに調査・分析をしたところ、攻撃者による寄付者の銀行口座情報や社会保障番号への不正アクセスおよび外部流出の事実を確認した。それにもかかわらず、同社の開示担当の経営陣にこの事実を伝達しなかった（同社にはそれを確実にを行うための組織的な方針・手続がなかった）。

B 社は、四半期報告書（フォーム10-Q）において、このインシデントの範囲について説明し、「サイバー犯罪者がデータの一部のコピーを持ち出した」とのみ記載しており、一定数の顧客について、暗号化されていない銀行口座情報および社会保障番号が外部に流出されたという重要な事実を開示していなかった。さらに、同社はフォーム10-Qにおけるサイバーセキュリティ・リスク開示の中で、「当社のデータ・セキュリティが侵害され、その結果、顧客または寄付者の個人データもしくは支払カード・データが権限のない者によって取得された場合には（could）、顧客その他の者からの当社の評判、ならびに当社の事業活動、経営成績、財政状態および流動性に悪影響を及ぼす可能性があ…る」と記載していた。顧客または寄付者の個人データが実際に攻撃者によって外部に持ち出されたという重要な事実を前提にすると、このような攻撃が同社の事業にもたらすリスクは、もはや仮定上のものではなかった。

52) もっとも、判例においても、リスク要因についての開示義務違反の判断は難しく、解釈が分かれることも多い。2024年、連邦最高裁は、実際に発生していたことを開示せずに、そのリスクを仮定上のものとして説明したことが誤導的と言えるかについて問題となった *Amalgamated Bank v. Facebook, Inc. (In re Facebook, Inc. Sec. Litig.)*, 87 F.4th 934 (9th Cir. 2023) [第9巡回区連邦控訴裁判所は誤導的であると認めた] についてサーシオレイライ（裁量上訴）を受理したが、最終的にサーシオレイライを十分な熟慮なく認めたとして却下している（dismissed as improvidently granted）(604 U.S. 4)。リスク要因の開示に関する損害賠償責任について検討・分析したものとして、荒達也「アメリカにおける事業等のリスクに関する情報の開示」岩原紳作＝山下友信＝神田秀樹古稀『商法学の再構築』505-533頁（有斐閣、2023）等参照。

53) Securities Act Release No.11165, Exchange Act Release No.97098, 2023 SEC LEXIS 602 (Mar. 9, 2023).

B 社が上記の重要な事実を記載しなかったことにより、本件インシデントについての同社の記載は誤解を招くものとなった。なぜなら、このような重要な事実の開示によって、同社がそれ以前に行ったウェブサイトへの掲載および顧客への通知によって生じていた、本件インシデントによって、攻撃者が機密性の極めて高い寄付者データにアクセスするには至らなかったという誤った印象が、そのまま継続されたからである。

よって、33年法17条 (a) (2) および (3) 違反が認められる。また、これら取扱注意のドナー情報の流出を含むサイバーセキュリティ・リスクを（開示担当の）経営陣に伝達させるための開示統制手続を備えていなかったことから13a-15 (a) 違反も認められる。

これらのことから、違反行為の排除命令、および民事制裁金300万ドルの支払い命令が発せられる。

(b) 検討

本件では、主に2つのことが問題とされている。一つは、同社の従業員が攻撃者による寄付者の銀行口座情報や社会保障番号への不正アクセスおよび外部流出の事実を知っていたにもかかわらず、フォーム10-Qにはその事実を開示せず「当社のデータ・セキュリティが侵害され、その結果、顧客または寄付者の個人データもしくは支払カード・データが権限のない者によって取得された場合には」という仮定上の表現を使っていたこと、もう一つは、それを同従業員が開示担当の経営陣に確実に伝えるための手続がなかったことである。

前者について、本件は、SolarWinds 社判決で述べられた、「すでに発生している（現実化している）リスクについて警告していた」事案に該当すると言える。なぜなら、寄付者の機密性の高いデータへの不正アクセスおよび外部流出の事実を確認しながら、仮定的に「データが…取得された場合には」と記載しているからである。すでにリスクが現実化していたのであるから、仮定的な表現による記載では、重要な点で合理的な投資者の有していた誤った印象を正すことができず、誤導的な記載と解釈されたと思われる。

このようにリスク開示が誤導的であると認められる事案⁵⁴⁾もあるものの、そのように明確に判断できる事案ばかりではない。実際、前出の Avaya 社、Mimecast 社のように詳細な事実を開示していなかった場合や、Check Point 社、Unisys 社のように一般的なリスク開示

54) 他には、*In re Altaba Inc., f/d/b/a YAHOO! Inc., Securities Act Release No. 10485, Exchange Act Release No. 83096, 2018 SEC LEXIS 964 (Apr. 24, 2018)* [Y 社において情報セキュリティチームは、数億にも上る利用者の氏名、生年月日、電話番号といったデータが不正アクセスされ、流出したことを発見し、同社の経営陣および法務チームに伝えたが、経営陣・同チームスタッフはデータ侵害がどの開示書類でどのように開示すべきなのか等について適切に評価できず、同社は約2年もの間当該データ侵害を情報開示書類で開示しなかった。その間の年次報告書、四半期報告書におけるリスクファクター開示には、すでに大規模なデータ侵害が起きていることを開示せずに、将来起きるかもしれないリスクとして記述されており、重要な点において誤導的であり、33年法17条 (a) (2) および (3) 違反が認められた。] がある。

を更新していなかった場合には、誤導的な開示とは解釈されない可能性も十分ある。

そこで、そういった場合にも責任の基礎として有効に機能し得るのが、後者の開示統制手続の維持義務違反である。開示統制手続は、前述のとおり、34年法の法定開示書類において「開示の対象となり得る情報が、適時に収集され、評価されることを確保するものでなければなら[ず] …、発行会社の事業に係するリスクおよび進展について、開示する必要があるかどうかを評価するうえで関連する情報を把握するものでなければならない⁵⁵⁾。」と広く捉えられており、会社としてこれを維持していなければ13a-15 (a) 違反が認められるものである⁵⁶⁾。

実際にこれを認めた事案を2つ紹介し、開示統制手続の意義を検討する。First American 社と Activision Blizzard 社に対する手続である。

(3) *In re First American Financial Corp.*⁵⁷⁾

(a) 事案の概要

不動産取引サービス業者のFA社は、2019年5月24日の朝、サイバーセキュリティのジャーナリストから、同社の画像共有のソフトウェアアプリケーション（EaglePro）によって、2003年以降の不動産取引に関する8億を超える画像—ソーシャルセキュリティナンバー及び銀行口座、運転免許証等といった個人情報を含む画像も含む—が晒されていることを知らされた。これは、個人情報を含む画像は“SEC”（secure）というタグをつけパスワードで保護されるが、そのタグ付けはFA社の従業員が手作業で行うところ、誤って個人情報を含む何千もの画像が“SEC”とタグが付けられなかったことによるものであった。その結果、利用者は個人情報を含む画像をパスワードなしに閲覧でき、第三者と共有もできる状況になってしまった。2019年5月24日の数ヶ月前に、同社の情報セキュリティ担当者はこのアプリケーションの脆弱性について認識し、その旨報告書（以下、2019年1月報告書）に記載していたが、同社のポリシーに従って改善するに至らなかった。

FA社は、2019年5月24日の午後、アプリケーションに設計上の欠陥があり、顧客のデータに権限なくアクセスできる状況にあったことを確認したこと、顧客の情報保護は最優先で取り組むものとして、この状況に対処し、同アプリケーションへの外部からのアクセスを遮

55) SEC Release 33-8124, *supra* note 26, “III. Disclosure Controls and Procedures” “B. Discussion of Disclosure Controls and Procedures”. See also SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459, 34-82746 (Feb. 21, 2018), available at <https://www.sec.gov/rules-regulations/2018/02/commission-statement-guidance-public-company-cybersecurity-disclosures>, “II. Commission Guidance”, “B. Policies and Procedures”, “1. Disclosure Controls and Procedures”.

56) また、前掲注31)で掲げた、34年法13条 (b) (2) (B) を基礎に責任が認められている事案の中でも Portland 社の事案、National Energy 社の事案で13a-15違反が認められている。

57) Exchange Act Release No. 92176, 2021 SEC LEXIS 1630 (June 14, 2021).

断するための対策を速やかにとったことを示すメッセージを、メディアに流した。その翌営業日である同月28日、FA社はフォーム8-Kを提出し、追加的なプレスリリースも添付した。そのリリースには、「現時点では、顧客情報への大規模な権限のないアクセスは確認されていない」と記載されていた。フォーム8-Kが提出された後、FA社は調査によって2014年から脆弱性があったことを確認した。

FA社の最高情報セキュリティ責任者（CISO）及び最高情報責任者（CIO）はフォーム8-Kが提出される直前まで2019年1月報告書の内容を知らなかった。5月24日の朝、CISOは2019年1月報告書の内容を初めて知り、CIOは25日に知ったが、いずれも速やかに改善するよう取り組まなかった。開示担当のシニアエグゼクティブも、5月24日または同月28日より前にこれらの事実に気づくことはなかった。このように、開示担当のシニアエグゼクティブは、会社の情報開示を承認するときに、会社のサイバーセキュリティ対応及びEagle Proの脆弱性から生ずるリスクの重大性について十分評価するための情報を欠いていた。

以上のことから、FA社は、開示統制手続を維持することを発行会社に求める13a-15(a)違反が認められ、違反行為の排除命令、および民事制裁金48万7,616ドルの支払い命令が発せられる。

(4) *In re Activision Blizzard, Inc.*⁵⁸⁾

(a) 事案の概要

ビデオゲーム開発および出版業を営むAB社は、2018年から2021年に提出した年次報告書（フォーム10-K）および四半期報告書（フォーム10-Q）において、優秀な人材を確保することが事業にとって特に重要であることを認めていた。

これらの情報開示の対象期間、同社は職場でのハラスメントに関する従業員の苦情についての情報がAB社の開示担当者に伝達され、適切な時期にその開示の評価ができるようにすることを確保することが意図されたコントロールおよび手続を欠いていた。

以上のことから、AB社に34年法ルール13a-15(a)違反が認められ、違反行為の排除命令、および民事制裁金3,500万ドルの支払い命令が発せられる（他に内部告発者保護規定である34年法ルール21F-17(a)違反も認められているがここでは省略する）。

(b) 上記命令に対する声明

上記命令に反対する声明がHester M. Peirce委員から出されている⁵⁹⁾。

13a-15(a)の開示統制手続は、13a-15(e)で定義されている通り、「発行会社が34年法

58) Exchange Act Release No. 96796, 2023 SEC LEXIS 258 (Feb. 3, 2023).

59) <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-activision-blizzard-020323>

のもと提出する書類に発行会社によって開示が求められる情報」が、「発行会社の経営陣…に集められ伝達されること、それによって、経営陣が求められる開示について適時の判断を可能にすることを確保する」と規定されている。

これを素直に読めば、開示統制手続は開示が求められる情報のみを対象としているように思われるが、SEC の命令は発行会社の事業に関連する進展およびリスクを開示する必要性についての評価に関係する情報を対象とすべきとしている。換言すれば、求められる開示統制手続の対象は、開示情報のみならず、追加的で曖昧に定義される、リスクが開示の求められる基準に達したか否かを判断するのに「関係する」情報としているのである。

数年間、AB 社は同社への投資にリスクをもたらす重要な要素の一つとして、AB 社の業界は従業員の転職率が高いという特徴があり、優秀な人材を確保することが困難になるかもしれない、その確保のために相当なコストを払うかもしれないと開示していた。SEC の命令はこの開示が誤導的であったということについてはどこにも述べていない。そうではなく、SEC 命令は、AB 社は開示の視点からこれらのリスク要因に関する情報を入手し評価することを確保することが意図された統制および手続を欠いていることの責任を問うている。具体的には、職場でのハラスメントに関する従業員からの苦情についての情報が AB 社の開示担当者に伝達されるように意図された統制および手続を欠き、その開示についての評価を適切な時期にすることができなかったと指摘する。AB 社は職場のハラスメントについての従業員の苦情の量および内容を理解するための情報を十分に得ていなかったから、AB 社の事業に関するリスクを経営陣が評価することができなかったと結論づけている。

経営陣が入手できなかった情報が本ルールの対象となるものならば、それを入手できないと関連する開示の正確性や質に影響を及ぼすと考えるのが合理的であろう。しかし SEC 命令は、AB 社の経営陣が開示書類を作成するときに適切な情報にアクセスできなかったとしながらも、リスク開示について誤導的または不完全であるということは全く主張していない。この点を整合的に理解することは困難である。

(c) 検討

以上見てきたように、FA 社、AB 社の事案では、両者ともに、開示書類に虚偽記載があったことは認定されず（SEC が主張すらしていない）、開示統制手続の維持義務違反のみ認められている。反対の意を表明する声明も述べるように、SEC 命令は、AB 社の「リスク開示について誤導的または不完全であるということは全く主張し…ない」で、「経営陣が開示書類を作成するときに適切な情報にアクセスできなかった」ことをもって責任を肯定しているのである。

このことは、開示統制手続が、34年法上要求される情報開示の正確性を確保するための単なる「手段」ととどまらず、開示判断に必要な情報が適切な権限を有する者に伝達されるた

めの情報フローを確保することそれ自体を、独立してエンフォースし得る義務として機能していることを示唆する。

また、両者において開示担当者に伝達されていなかった情報は、財務報告に直接関係のあるものではなかった⁶⁰⁾。さらに、13条 (b) (2) (B) および財務報告に係る内部統制は、内部統制が「合理的保証 (reasonable assurance) をする」ものと位置付けられているのに対し、開示統制手続は、「確保する (ensure)」ものと規定されており、開示統制手続違反か否かの判断がより容易になされ得る。このような意味で、開示統制手続は内部会計統制や財務報告に係る内部統制よりも広範囲で適用できると思われる。

もっとも、AB 社の事案で反対の意を表明する声明は、開示統制手続の対象となる情報の範囲について、開示情報より広く、発行会社の事業に関連する進展およびリスクを開示する必要性についての評価に関係する情報 (リスクが開示の求められる基準に達したか否かを判断するのに「関係する」情報) としていることを批判している。しかし SEC 自身当初から述べている通り、開示統制手続は、「最高経営責任者や最高財務責任者が、求められる確認 (certification) を行う責任を果たすこと、および証券保有者に対して正確かつ完全な情報を提供する責任を果たすことについて支援するために、会社が社内コミュニケーションやその他の手続を機能させることを確保することが必要であり、それにより、重要な情報が適時に適切な…開示担当者へと伝達されるようになる⁶¹⁾」として導入されたものであるから、その対象となる情報は「発行会社の財務報告に関する内部統制が対象とする情報よりも、広 [く] …発行会社の事業に係るリスクおよび進展について、開示する必要があるかどうかを評価するうえで関連する情報を把握するもの⁶²⁾」である必要があるという見解⁶³⁾は、理にかなっていると思われる。開示する必要があるか否か (重要性があるかどうか) を判断させるためには、発行会社の事業に関連する進展およびリスクを開示する必要性についての評価に「関係する」情報を対象とせざるを得ないと解される⁶⁴⁾。

3. 2023年ルールによる影響

前述の通り、2023年7月に制定されたサイバーセキュリティ・インシデント開示に関する

60) 他にも、例えば、本稿で取り上げてきた RRD 社、Unisys 社の事案においても、財務報告に関係のない情報について開示統制手続が問題となった。

61) SEC Release 33-8124, *supra* note 26, “III. Disclosure Controls and Procedures” “A. Rule Requirements”.

62) Id., “III. Disclosure Controls and Procedures” “B. Discussion of Disclosure Controls and Procedures”.

63) さらに、SEC は、別のリリースで「重要なこととして、関連情報の『重大性 (重要性) に関する疑念』が生じるのは『よくあること』であり、そのような場合は『法が保護しようとしている対象』、すなわち投資者に有利なように判断されるべきである」とも述べている。SEC Release 33-11216, *supra* note 46, “II. Discussion of Final Amendments” “3. Final Amendments”.

64) なお、SEC は、この主張を前出の SolarWinds 社判決においても行ったが、連邦地裁はそれについて判断しなかった。741 F. Supp. 3d, at 109-110.

新しいルールが制定された⁶⁵⁾。これは、発行会社が、サイバーセキュリティ・インシデントが重要であると判断した場合、その判断から4営業日以内に、当該インシデントの性質、範囲、および時期に関する重要な点、ならびに会社（その財政状態および営業成績を含む）に対して与える（与えることが合理的に予想される）重要な影響について記載し提出することを求めるものである。このルール制定により、本稿で取り上げてきた事案も含め、開示義務違反の主張にどのような影響を及ぼすのか、若干の検討を試みたい。

まず、サイバーセキュリティ・インシデントを重要と判断したにもかかわらず、4営業日以内に開示しなかった場合には、開示が要求されているにもかかわらず開示していないことから、それ自体で開示義務違反が認められよう。同ルール制定前は、開示しなかったことによって開示内容が誤導的になったと主張する必要があったが、より直接的に責任を主張できるようになる。

これに対して、前出の Avaya 社、Mimecast 社のように詳細な事実を開示していなかった場合や、Check Point 社、Unisys 社のように一般的なリスク開示が更新されていなかった場合はどうか⁶⁶⁾。これは、同事案について反対の意を表明する声明が述べていた通り、2023年ルール制定の際に SEC 自身が「私たちは [ルールの] …合理化（簡素化）を図り、インシデントそのものに関する詳細についてではなく、主に重要なサイバーセキュリティ・インシデントがもたらす影響についての開示に焦点を当てる⁶⁷⁾」と明確に述べており、「重要な」インシデントがもたらす「重要な」影響がその対象となっていることに鑑みると、「重要」かどうか（開示が要求されるか）の判断の問題は依然として残ることになる。「重要」であればそれを開示しないことは開示義務違反になるが、その判断は依然困難な場合も多いであろう。

もっとも、2023年ルールは、発行会社に、サイバーセキュリティの脅威による重要なリスクを評価、特定、および管理するためのプロセス（ある場合）、およびサイバーセキュリティの脅威によるリスクが、自社の経営戦略、営業業績、または財務状態に重要な影響を与えたか（その合理的可能性があるか）について、年次報告書（フォーム10-K）で説明することを求めており⁶⁸⁾、Check Point 社、Unisys 社のような事案で、このような「重要な影響」がある場合には、情報開示する（更新する）ことが求められるように思われる。ただし、ここ

65) SEC Release 33-11216, *supra* note 46. 2023年のサイバーセキュリティ開示ルールについて、特にサイバーセキュリティ上の脅威およびインシデントの重要性判断およびその開示義務を検討する近時の研究として、Deborah Slattery-Pereira, *Reporting Materiality Under the SEC Cybersecurity Disclosure Rules: How Corporate Boards Balance Duty and Risk for Cyber Threats and Incidents*, 15 AM. U. BUS. L. REV. 303 (2026); Clayton Anderson, *Uncertainty in Cybersecurity Disclosures: A Reasonably Likely Approach*, 73 U. KAN. L. REV. 721 (2025) 等参照。

66) Avaya 社、Mimecast 社、Check Point 社、Unisys 社、それぞれの事案は2020年から2022年の開示が問題となったことから、2023年ルールは適用されていない。

67) SEC Release 33-11216, *supra* note 46, “II. Discussion of Final Amendments” “3. Final Amendments”.

68) Regulation S-K Item 106 (17 C.F.R. 229.106) (b).

でも「重要」かどうかの判断の問題が残る。

2023年ルールは「重要な」サイバーセキュリティ・インシデントについての開示義務を明示的に課した点で大きな意義がある一方で、すべての開示義務違反の主張が認められやすくなったわけではなく、開示が求められる「重要」な情報とは何か、という解釈の困難性は解決されていないのである。

V. おわりに

以上、サイバー攻撃を受けた会社の対応に問題がある場合に、SEC がどのように責任を問うてきたのかについて、最近の事例をいくつか取り上げて検討してきた。

まず、34年法13条 (b) (2) (B) の規定する内部会計統制に基づいて ((i) 経営陣の一般的または個別的承認に従って取引が執行されること, (iii) 資産へのアクセスは経営陣の一般的または個別的承認に従った時のみ許されること, の部分について, 合理的保証をするのに十分な内部会計統制の制度の構築・維持をすることが求められている, として) 法令遵守を確保するために設計された統制やサイバーセキュリティ統制を欠いていることの責任を問うた事案 (Andeavor 社, Charter 社, RRD 社) があるが, いずれも, 会計や財務諸表の正確性に直接影響を与えず, 「内部会計統制」に含まれるものではない, との反対の意を表明する声明 (Hester M. Peirce 委員および Mark T. Uyeda 委員によるもの) が出された。

また, SolarWinds 社判決で, RRD 社で述べられた13条 (b) (2) (B) (iii) の「資産」の解釈は否定され, 「内部会計統制」は財務会計に向けられたものであることからサイバーセキュリティ統制には及ばないことを明確にした。SolarWinds 判決の解釈を踏まえば⁶⁹⁾, 34年法13条 (b) (2) (B) の内部会計統制を広く解釈し, 積極的に執行を行うことが継続するかは不透明である。

そこで, SEC が開示義務違反 (33年法17条 (a) (2) および (3), 34年法13条 (a) 等) で責任を問うことはどうか。もし「すでに発生している (現実化している) リスクについて警告していた」ような事案 (Blackbaud 社, Altaba 社) であるなら, リスク開示が誤導的として開示義務違反が認められる。しかし, 例えば, 詳細な事実を開示していなかった事案 (Avaya 社, Mimecast 社), 開示が同社固有のリスクおよびインシデントに十分に適合 (個別化) していなかった事案 (Check Point 社, Unisys 社) のように誤導的な開示があったか

69) なお, SEC は, 2025年11月, SolarWinds 社および同社 CISO に対する残存請求について訴えを取り下げしており, このことを, サイバーセキュリティに関する SEC の執行方針の転換を示すものとする評価もある (前掲注39) 参照)。また, 2026年8月現在, RRD 社等の事案における内部会計統制規定の拡張的な適用に反対の意を表明していた Hester M. Peirce 委員および Mark T. Uyeda 委員は, 引き続き SEC の委員を務めており, 2025年に就任した Paul S. Atkins 委員長とともに, 現在の SEC を構成している。このような近時の動向および委員構成の下で, 同規定について今後どのような執行方針が採られるかが注目される。

否かについて容易には判断できない場合も多い。

2023年ルールは、サイバーセキュリティ・インシデントについての情報開示を明示的に要求したものの、「重要」な事項がその対象であることから、開示すべき「重要」な情報の範囲をめぐる問題は依然として残されている。

これに対して、開示統制手続は、これまで見てきた通り（RRD 社、Unisys 社、Blackbaud 社、First American Financial 社、Activision Blizzard 社等）、会計や財務報告に関係がなくても、虚偽記載が認められなくても、SEC ルール13a-15（e）の要件を満たす統制手続が会社に存在しなければ責任を問うことができ、その結果、他の違反と同様に排除命令と民事制裁金の支払いを命じられる点で、SEC にとって有力な手段となる。

このような開示統制手続の意義は、2023年ルールが制定されても変わらない。前述の通り、2023年ルールを導入しても、開示が求められる「重要」の解釈の問題は残るのであるから、その判断を可能にするためにも、インシデントに関する情報を開示判断権者に適時に伝えることを確保する統制手続の必要性は極めて高い。SEC 自身も、2023年ルール制定時に（一部コメントで同ルールのセーフハーバーの提案があり、それは不要であることの理由として）「通常の社内実務、および開示統制手続を遵守することによって、誠実な法令遵守を証明するには十分である⁷⁰⁾」と述べており、開示統制手続の重要性を強調している⁷¹⁾。

わが国では、内部統制制度のうち、米国の開示統制手続に直接対応する制度は設けられてこなかった。米国においては、本稿で見てきたように、開示統制手続について、開示書類に虚偽記載が認められない場合や、問題となった情報が財務報告に直接関係しない場合であっても、必要な統制手続が維持されていないこと自体を理由として、13a-15（a）違反が認められ得る。このような意味で、開示統制手続は、虚偽記載の存在や財務報告との直接的な関連を必ずしも前提とせず、開示判断に必要な情報が会社内部で適切に収集され、開示判断権者に伝達されるための情報フローそれ自体を SEC による執行の対象とすることを可能にする点で、米国の内部統制制度において重要な意義を有するものと思われる。

（筑波大学准教授）

70) SEC Release 33-11216, *supra* note 46, “II. Discussion of Final Amendments” “3. Final Amendments”.

71) さらに、2023年ルールは、Regulation S-K Item 106 (17 C.F.R. 229.106) (c) で、発行会社に、サイバーセキュリティの脅威による重要なリスクを評価および管理する上での経営陣の役割、リスクの評価・管理責任を負う経営陣がサイバーセキュリティ・インシデントの予防、検知、是正等に関する情報の報告を受けこれらを監視するプロセス、取締役会がサイバーセキュリティの脅威によるリスクに関する情報の報告を受けるプロセス、サイソのようなリスクに対する取締役会の監督体制等について説明することを求めている。すなわち、開示統制手続によって経営陣に情報が集められることが求められているところ、実際、会社内で、どのように経営陣にサイバーセキュリティ・インシデント情報が集められ、取締役会に報告されるのか、さらに取締役会がどのようにリスクを監督するのかといったガバナンスの情報についても開示が求められているのである。