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―

永　野　秀　雄

要旨

近年、サイバー攻撃の多発により、企業が被害を被る事態が多発するようになった。上場企業は、投資家への適切な情報開示の一部として、このような被害を有価証券報告書に記載すべきであるが、これをどのような基準で開示すべきかについては、具体的な指針が存在しなかった。米国では、2011年にそのような指針として、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」が策定された。

本稿では、有価証券報告書における情報開示のあり方を規制する連邦証券諸法の枠組みの中で、本指針の内容や効果等を明らかにした。また、今後、わが国で、この問題にどのように対応すべきかについても提案を行った。

キーワード

公開企業、サイバー・インシデント、サイバー攻撃、サイバーセキュリティ、
サイバーセキュリティ・リスク、財務諸表、証券法、情報開示、連邦証券取引委員会、有価証券報告書

１．はじめに

株式投資家が、証券市場で投資を行う場合、公開されている情報が判断の根拠となる。この判断が適切になされるためには、公開企業（上場企業）に、適切な情報開示を行わせる制度的な担保が必要となる。米国では、連邦証券取引委員会（Securities and Exchange Commission: SEC）が、証券取引諸法に基づいて、公開企業による財務情報の開示要件を設定するとともに、その実施を監視してきた。

当初、このような情報開示は、伝統的な財務情報に限られていたものの、米国では、公開企業による土壌汚染等に対する巨額の債務負担が顕在化したことで、一定の環境情報の開示が求められるようになった[1]。近年、新たに情報開示の必要性が検討されるようになったのが、サイバーセキュリティ・リスクである。ある公開企業がサイバー攻撃を受け、顧客の個人情報や営業秘密等が漏洩した場合には、大きな損害が予想されるからである。

たとえば、2015年１月29日、米国で２番目に大きい健康保険会社であるAnthem, Inc.は、数週間に渡ってサイバー攻撃を受け、7,880万人の顧客と被用者の社会保険番号、誕生日、住所や収入といった個人情報を含むデータベースへの不正アクセスがあったことを公表した[2]。報道によれば、この不正アクセスに関する損害等は、同社が加入していたサイバーリスク保険の保険金をはるかに上回るものになるとされている[3]。

連邦証券取引委員会は、2011年に多発した情報漏洩事案をきっかけに、連邦議会から対応を迫られた。そして、同委員会は、2011年10月13日に、サイバーセキュリティに関するリスクの情報開示につい

ての指針を公表した。それが、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」（以下、「本指針」という。）である[4]。本稿では、この本指針に関して十分に分析した邦語論文がないことから[5]、その内容や効果を検討する[6]。わが国における情報開示のあり方の参考になれば、幸いである[7]。

以下では、①連邦証券諸法における情報開示に関する法的枠組みを説明したのち、②本指針について、その制定の背景、効力、問題点並びに内容を明らかにし、③本指針制定後の評価と提案について触れることにする。そして、④最後に、本指針を踏まえて、わが国におけるサイバーセキュリティ・リスクの開示の方向性を示したい。

２．連邦証券諸法における情報開示に関する法的枠組み

2.1 連邦証券諸法における情報開示

米国の1933年証券法[8]と1934年証券取引法[9]は、株式を公開している企業に対して、一定の情報開示義務を課している。その内容をおおまかに言えば、1933年証券法は、公募されている株式の登録および売買について規制し、1934年証券取引法は、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。

連邦議会がこれらの立法を制定した目的は、投資家が十分な情報に基づいた投資決定を行えることができるように、重要な財務情報を企業に開示させることにあったと言える[10]。

2.2　証券取引委員会規則における情報開示規定

ある公開企業がどのような情報開示を行うべきかについては、主として、証券取引委員会規則S-K[11]と同S-X[12]とに定められている。

前者の規則S-Kでは、連邦証券取引委員会（SEC）へ申請を行うときに提出する登録届出書による開示方法と、株主への定期的な報告書などによる継続的な開示方法とが定められている。この規則の下では、必要な情報を文章により記述すること（narrative statements）が求められている。これに対して、後者の規則S-Xは、企業の財務諸表において記載されなければならない情報を定めている。

本稿で検討するサイバーセキュリティ・リスク等については、規則S-Kの規定に従うことになるので、以下では、関係する規定の概要を説明したい。

2.3　証券取引委員会規則S-K

規則S-Kは、連邦証券取引委員会へ証券の発行を申請する場合に提出する登録届出書における情報開示と、株主への定期的な報告書などの継続開示について定めた規定である。具体的には、同規則の101項[13]、103項[14]、303項[15]及び503(c)項[16]が、連邦証券取引委員会への申請、目論見書（prospectuses）、登録届出書（registration statements）及び株主に対する定期的な報告書において、どのようにサイバーセキュリティ・リスクに伴う情報を開示するかに関係してくる。

規則S-Kの101項は、公開企業として登録する企業に対して、自社の事業活動を記述する義務を課すとともに[17]、その財務内容の情報開示を求めている[18]。

規則S-Kの103項は、公開企業に対し、同社が現在直面している訴訟等の法的手続（これには、司法機関における訴訟のみならず行政手続も含まれ、また、係争中のもののみならず、これから始まる訴訟等で、現に同社に通知されたものも含まれる）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いる[19]。

規則S-Kの303項は、「財務状況と営業活動に関する経営者による検討と分析（Management's Discussion and Analysis of Financial Condition and Results of Operation）（以下、「MD&A」と表記する場合もある）をいかに記述するかを規定した条項である[20]。

最後に、規則S-Kの503(c)項「リスク要因（Risk Factors）」は、公開企業に対して、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、これについて記述することを求めている。そして、この開示にあたっては、決まり文句やどの企業にも該当するような一般的なリスクを記述するのではなく、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が求められている[21]。

2.4 情報開示が求められる「実質的な」情報について

現在の連邦証券諸法の下では、公開企業に対してサイバーセキュリティ・リスクとインシデントを開示する義務を明白に定めた規定は存在していない[22]。現在、サイバーセキュリティ・リスクとインシデントにつき情報開示を行う必要がある情報は、「実質的な（material）」情報と言われるものである[23]。以下、この点につき、説明していきたい。

連邦証券諸法の下では、ある情報が実質的なものとみなされるのは、「合理的な投資家からみた場合、もしも開示されなかった事実が開示されていたならば、利用可能な情報の全体像（total mix）が著しく変わってしまう蓋然性が高い」[24]場合を意味する。たとえば、ある会社から他の会社にある権利を譲渡した結果として、経営権に変更が生じる場合は、実質的な情報と考えられる[25]。

公開企業は、情報開示にあたり、この「実質性（Materiality）」を満たすことが重要になる。その理由は、この実質性が、投資家が情報の不開示に伴う訴訟を提起する場合における当事者適格を満たすための主要な要素のひとつとなっているためである[26]。

連邦証券諸法に関する判例では、投資家が、①1934年証券取引法規則10b-5条違反に対して黙示的な救済を求める場合[27]と、②1934年証券取引法規則14a-9条における委任状開示要件[28]については、黙示的権利に基づく訴訟提起が認められてきた[29]。ここでは、まず、これらが何を意味するかについて、説明しておきたい。

上記①の同規則10b-5条は、証券の購入又は売却に伴って、詐欺と禁止されている詐欺的行為があった場合についての救済を定めている[30]。本条の下で損害賠償請求が認められるためには、原告は、他の要件に加え[31]、当該公開企業による虚偽の記載（misstatement）又は情報の不開示（omission）が実質的なものであったことを証明する必要がある[32]。また、②の規則14a-9条は、委任状の勧誘に関連する実質的な虚偽記載と情報の不開示を禁じていることから、原告は、同様に実質性を立証する必要がある[33]。

これらのいずれの訴訟類型においても、実質性の判断基準は同一である。それは、その虚偽記載又は情報の不開示が実質的なものであること、すなわち上述したように、「合理的な投資家からみた場合、もしも開示されなかった事実が開示されていたならば、利用可能な情報の全体像が著しく変わってしまう蓋然性が高い」[34]ことを証明することが求められるのである。逆に言うと、公開企業は、そのような実質的な情報を開示していない場合、上記の類型の訴訟において敗訴する可能性が生じるのである。

サイバー攻撃による被害の潜在的な重大性からすると、この問題が実質的なものとみなされる可能性がある。また、投資家による将来の訴訟においては、実質性の立証が不可欠なものとなる。さらには、公開企業はそのコンプライアンスを確実にする必要から、その実質的な情報開示を行ないたいと考えるであろう。

連邦証券取引委員会の企業財務局による本指針は、連邦証券諸法との関連において、公開企業に対して、サイバーセキュリティ・リスクとインシデントに関する事実とリスク等について、その実質的な情報を開示するための指針を示す役割を果たすものとなっているのである[35]。

3．本指針について

ここでは、本指針について、①本指針が制定された背景、②本指針の効力と問題点、③本指針の内容の順に説明する。なお、③本指針の内容については、原文を尊重しつつも、日本語として意味が成立しうるための改変を加えた仮訳を示した。

3.1 本指針制定の背景

本指針が公表される主たる原因となったのは、2011年前半に大きく報道された公開企業からの情報漏洩事案である[36]。もちろん、これ以前にもサイバー攻撃により情報漏洩事案は存在していたものの、ソニーやRSAといった著名企業による事案が

起きたことから注目が集った[37]。

これらの事案を受けて、ジョン・D・ロックフェラー４世らの上院議員が、何らかの対処が必要であると考えるに至った。そして、連邦証券取引委員会の委員長に対して、サイバーセキュリティ・リスクに関する情報開示要件を明確化する何らかの指針を公表するように求めたことから[38]、本指針が発せられることになった。

3.2　本指針の効力と問題点

ここでは、本指針の内容に入る前に、本指針の効力と問題点について簡単に触れておきたい。

まず、本指針の効力についてであるが、本指針は証券取引委員会企業財務局の見解を表したものであって、証券取引委員会により正式に承認されたものではない[39]。このため、本指針は、企業財務局による提案という地位にとどまっており、証券取引委員会規則等に認められる法的拘束力はなく[40]、執行力も認められないものとなっている[41]。このような形になったのは、正式に規則等で定めた場合、株主からの訴訟が多発することを懸念したものと思われる。

次に、本指針の問題点を指摘しておきたい。まず、上述のように、本指針には法的拘束力がないことから、公開企業に対して、どこまで情報開示に関する効力をもつのかがはっきりしない点を挙げることができる。第２に、これはサイバーセキュリティに特有の問題であるが、あまりに詳細な情報開示を行うと、その情報がサイバー攻撃を行う者に利することになるという問題が生じることである。自社のサイバーセキュリティを脅かすような効果をもつ情報開示を行えば、結果的に、そのことで投資家から訴えられるという潜在的な訴訟リスクにさらされてしまうことが指摘できよう[42]。

3.3　本指針の内容

（仮訳）

連邦証券取引委員会企業財務局

企業財務局・情報開示指針（Disclosure Guidance）第２号

サイバーセキュリティ

日付：2011年10月13日

要約：本指針は、サイバーセキュリティに関するリスク及びサイバー・インシデントに関する情報開示義務についての企業財務局の見解を示すものである。

補足情報：本指針における見解は、企業財務局の意見を示したものである。なお、本指針は、規則（rule）、規制（regulation）又は連邦証券取引委員会の見解（statement）を示すものではない。また、連邦証券取引委員会は、本指針の内容を承認も否認もしていない。

はじめに

長年にわたり、登録会社（registrants）は、その業務の遂行にあたりデジタル技術への依存度を増してきた。そして、デジタル技術への依存度が増すにつれ、登録会社にはサイバーセキュリティ[43]に伴うリスクが増大し、その結果としてより多くの重大なサイバー・インシデントが発生している。近年、登録会社と法律及び会計の専門家の間で、連邦証券諸法おいて課されている情報開示義務の枠組みにおいて、登録会社の事業遂行におけるこれらのリスクと、これによってもたらされる影響をどのように記述すべきかについて注目が高まってきた。このため、企業財務局は、登録会社が、サイバーセキュリティ関連の事項につき、同社の個別具体的な事情の下で、どのように評価し、情報開示すべきかにつき支援する目的で指針を提供することが有益であると決定するに至った。

企業財務局は、ビジネスリスクに伴う関連する情報開示についての判断と矛盾することがないように、本指針を策定した。本局は、あまりに詳細な情報開示が、サイバーセキュリティの強化を損ねかねないことに留意している。たとえば、詳細な情報開示は、登録会社のネットワークに不正アクセスを試みようとする者に「ロードマップ」を提供する効果をもつ懸念がある。したがって、そのような性格をもつ情報開示が連邦証券諸法の下で求められているわけではないことを強調しておきたい。

一般的に、サイバー・インシデントは、意図的な攻撃又は意図的ではない出来事により引き起こされる。本局は、財産若しくは機微な情報の不正取得、データの破壊又は営業の混乱を引き起こすことを目的として、デジタル・システムに不正アクセスを行う等のサイバー攻撃について、注目度が上がっていることを認識している。なお、サイバー攻撃は、不正アクセスを用いない手法によっても実行されうる。たとえば、ウェッブサイトへのサービス妨害攻撃（DoS攻撃）によっても引き起こされる。また、サイバー攻撃は、第三者又はインサイダーにより、電子技術を用いてネットワーク・セキュリティを回避したり、ウェブサイトを機能させないようにしたりといった高度に洗練された方法から、アクセス権を取得するのに必要な情報を得るために、古くから用いられてきたインテリジェンスの収集やソーシャル・エンジニアリングといった手法を用いて行われることがある。

サイバー攻撃の目的には様々なものがあるものの、登録会社、その顧客若しくは取引先に帰属する金融資産、知的財産又はその他の機微な情報の窃盗などの目的が含まれている。成功裏に終わったサイバー攻撃の被害者となった登録会社は、かなりの費用負担やその他のマイナスの影響を被ることになる。これらの被害には、以下のもの等が含まれる。

- 盗まれた財産又は情報に対する損害賠償や、システム損害が起きた場合の修復費用などの復旧費用（Remediation costs）。また、この費用には、攻撃を受けた後にも顧客やその他の取引先との取引関係を維持するために提供されるインセンティブも含まれる場合がある。
- サイバーセキュリティに必要な保護費用として増加するものとしては、組織変更、追加人員の配備や防止技術の採用、従業員への教育訓練、外部の専門家やコンサルタントとの契約費用等が含まれる。
- 独占的に利用が認められていた情報の不正使用や、攻撃後に顧客を失い又は獲得できなくなったことによる減収。
- 訴訟。
- 顧客や投資家の信頼に負の影響をもたらす風評被害。

公開会社による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情報開示

連邦証券諸法では、合理的な投資家が、その投資決定に重要であると判断するリスクや事実に関する情報について、適宜、包括的かつ正確な情報開示を行うように求めている[44]。既存の情報開示要件の下では、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ものはないものの、多くの開示要件が、登録会社に、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。さらに、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ために、その開示が必要となる場合がある[45]。したがって、登録会社は、他の事業及び財務上のリスクと同様に、継続的にサイバーセキュリティ・リスクやサイバー・インシデントに関する情報開示が適切か否かについて検討すべきである。

以下では、サイバーセキュリティ・リスクやサイバー・インシデントについての検討が必要となる特定の情報開示義務に関する概説を行う。

リスク要因

登録会社は、サイバー・インシデントに関するリスクが、同社への投資を投機的又はリスクを伴うものにする最も実質的な要因のひとつにあたる場合には、当該リスクを開示すべきである[46]。このリスク開示の要否を決めるときには、登録会社は、自社のサイバーセキュリティ・リスクを評価し、以前のサイバー・インシデントやその重大性や頻度等の全ての利用可能な関連情報を考慮することが期待される。そして、この評価の一部として、登録会社は、サイバー・インシデントが将来に起きる蓋然性、及び、資産又は秘密情報の不正目的使用、データの破損又は事業の中断に伴う潜在的な費用やその他の結果等のリスクについての定量的かつ定性的な重大性

を考慮すべきである。また、リスク要因が開示されるべきか否かを評価するにあたっては、登録会社は、自らが属する業界において発生すると考えられているサイバーセキュリティ・リスクと、既知の直面しうる攻撃等のセキュリティに対するリスクとを低減させるための予防措置が適切であるか否かを考慮すべきである。

一般的に、リスク要因に関する情報開示は、証券取引委員会規則S-Kの503項(C)の要件に基づいて行われているが、サイバーセキュリティ・リスクの開示にあたっては、その実質的なリスクの性質を適切に記述し、かつ、個々のリスクが当該登録会社にどのように影響するのかを特定しなければならない。登録会社は、どのような発行者又は募集にも当てはまるようなリスクを記述するべきではないし、かつ、一般的なリスク要因にすぎない情報開示も避けるべきである[47]。登録会社に特有の事実関係や状況、及び、そのリスクがどの程度実質的なものかによるが、適切な情報開示には以下の事項が含まれうる。

- 実質的なサイバーセキュリティ・リスクと、同リスクが顕在化したときの潜在的な費用と結果により、登録会社の事業や運営にもたらされる事象に関する検討。
- 登録会社が外部に委託している機能のうち、実質的なサイバーセキュリティ・リスクを伴うものに関する記述と、同社がこれらのリスクにどのように対応するのかに関する記述。
- 登録会社が個別的に又は総体的に経験した実質的なサイバー・インシデントに関する記述。なお、この記述には、これに伴う費用やその他に生じた結果等の記述も含まれる。
- 長期間にわたり発見されないサイバー・インシデントに関するリスク。
- これらのリスクに関連する保険の担保範囲。

登録会社は、既知の又は脅威となるサイバー・インシデントと、これに関するサイバーセキュリティ・リスクに関する検討について、情報開示をする必要があるかもしれない。たとえば、登録会社が、そのシステムにマルウエアが組み込まれていたことにより、顧客データが漏出したという実質的なサイバー攻撃を経験した場合には、当該登録会社は、そのような攻撃が起こりうるというリスクについて開示するだけでは不十分である。そうではなく、マルウエア、又は、特定のリスクを引き起こす同様な攻撃に関する広範な検討の一部として、登録会社は、特定の攻撃の発生、及び、これに伴う既知の又は潜在的な費用及びその他の帰結につき論じる必要があるかもしれない。

登録会社は、自社の特定の状況に合わせて情報開示を行うべきであり、一般的な「決まり文句」を用いた情報開示を避けるべきである。その一方で、連邦証券諸法は、その情報開示により登録会社のサイバーセキュリティそのものを脅かすような情報開示を求めているのではないことを、もう一度指摘しておきたい。そうではなく、登録会社は、投資家が、特定の登録会社が直面しうるリスクの性質を適切に評価しうるに足る情報開示を行うべきである。

経営者による財政状態及び経営成績の討議及び分析（MD&A）

もしも、登録会社の１つ若しくは複数の既存のインシデント又は潜在的なインシデントのリスクに伴う費用又はその他の帰結が、登録企業の運営、流動性若しくは財務状態に重大な影響をもたらすと合理的に考えられうる重大な事案、傾向若しくは不確実性に相当する場合、又は、将来的な事業の帰結又は財務状態を必然的に示唆するものではないものの報告すべき財務情報を引き起こしうる重大な事案、傾向若しくは不確実性に相当する場合には、同社は、自らのMD&Aにおいて、サイバーセキュリティ・リスクとサイバー・インシデントに言及すべきである[48]。たとえば、もしもサイバー攻撃により重要な知的財産が盗まれた場合、かつ、この窃盗事案の影響が合理的に重大であると考えられる場合には、当該登録会社は、その盗まれた財産に関する記述、その結果としての事業、流動性又は財務状況への影響、及び、その攻撃により、将来における事業の帰結又は財務状態を示唆するものではないものの、報告すべき財務情報が生じるか否かにつき記述しなければならない。もしも、当該攻撃により、収益が減

少し、関連する訴訟費用も含めたサイバーセキュリティ保護費用が増加することが合理的に予期できる場合には、登録会社は、それが実質的なものである場合には、予想される費用の合計と期間を含めて、これらの起こりうる結果につき検討するべきである。あるいは、そのサイバー攻撃により知的財産は失わなかったものの、サイバーセキュリティ保護に必要な支出が実質的に増加した場合に、登録会社は、その増加費用を記すべきである。

事業に関する記述

もしも、単一の又は複数のサイバー・インシデントが、登録会社の製品、サービス、顧客若しくは供給事業者との関係又は競争条件に実質的に影響をもたらすものである場合には、当該登録会社は、その「事業に関する記述（Description of Business）」において情報を開示するべきである[49]。情報を開示すべきか否かを決定するにあたっては、登録会社は、個々の報告セグメントに対する事案の影響を考慮すべきである。たとえば、登録会社には開発中の新製品があるものの、サイバー・インシデントの発生により、同製品の将来性が実質的に損なわれうる場合、当該登録会社は、それが実質的である限りにおいて、このインシデントとその潜在的影響を検討するべきである。

法的手続

もしも、登録企業又はその子会社がサイバー・インシデントの当事者となり、それが実質的な係争中の法的手続に発展した場合には、当該登録会社は、「法的手続（Legal Proceedings）」を開示する箇所において、その訴訟に関する情報を開示する必要があるかもしれない。たとえば、相当な数の顧客情報が盗まれ、それが訴訟に発展した場合には、登録企業は、訴訟を管轄する裁判所の名称、訴訟が提起された日、訴訟の主たる当事者、訴訟で主張されている事実関係及び請求されている救済の内容を開示すべきである[50]。

財務諸表の開示

サイバーセキュリティ・リスクとサイバー・インシデントは、その具体的事案又は潜在的事案の性質や重大さにより、登録企業の財務諸表に広範な影響を及ぼす可能性がある。

サイバー・インシデント以前

登録会社は、サイバー・インシデントを防ぐためにかなりの費用を負担している場合がある。これらの費用を資産計上（capitalization）する場合の会計処理は、米国会計基準集サブトピック350-40「自社利用ソフトウエア」（Accounting Standards Codification（ASC）350-40, Internal-Use Software）に規定されており、そのような費用が会社内部で用いられるソフトウエアである限り資産として扱うことができる。

サイバー・インシデントの最中及びそれ以後

登録会社は、サイバー・インシデントを被った後、顧客との取引関係を維持しようとしてインセンティブを提供することにより、損害を軽減しようとするかもしれない。登録会社は、米国会計基準集サブトピック605-50「収益認識－顧客への支払い及びインセンティブ」（ASC 605-50, Customer Payments and Incentives）を参照して、このようなインセンティブにつき、適切な認識、算定及び分類を確実に行うべきである。

サイバー・インシデントは、既に請求された又は今後請求されるクレームによる損失を起こすかもしれない。これらのクレームには、保証、契約違反、製品のリコールや交換、取引先企業が改善のために行った努力に伴う損失などが含まれる。登録会社は、これらの損失が発生するかなりの可能性があり、かつ、これを合理的に見積もることができる場合には、これをいつ計上すべきかを決める際に、米国会計基準集サブトピック450-20「偶発損失」（ASC 450-20, Loss Contingencies）を参照すべきである。さらに、登録会社は、少なくとも合理的な可能性のある損失については、一定の情報開示を行わなければならない。

サイバー・インシデントは、キャッシュ・フローを減少させる結果を招くかもしれない。このため、営業権、顧客関連の無形資産、商標、特許、資産計上したソフトウエア、ハードウエア又はソフトウエアに関連した固定資産及び在庫等の一定の資産の減損を検討する必要があるかもしれない。登録会社は、サイバー・インシデントによる影響をすぐには把握できずに、会計処理を必要とする様々な財務上の影響の見積もりを進展させていく必要があるかもしれない。このため、登録会社は、財務諸表を準備するときに用いた見積もりの根拠となった推測を事後的に再評価すべきである。登録会社は、短期の見積りにおける合理的な可能性のある増減のうち、財務諸表に重要な影響を及ぼすリスク又は不確実性について説明しなければならない[51]。サイバー・インシデントにより影響がある見積もりの事例を挙げると、製品保証、返品の引当金、資産計上したソフトウエアの費用、在庫、訴訟及び繰延収益に関する見積もりなどがある。

サイバー・インシデントが、決算日の後で財務諸表の発表日より前に発見された場合には、登録会社は、認識された又はされていない後発事象の情報開示が必要であるか否かを検討するべきである。もしも当該事案が、重大な未認識の後発事象に該当する場合には、財務諸表において、当該事案の性質、財務上の影響に関する見積り、又は、そのような見積もりを行うことはできないとする表明を開示すべきである[52]。

開示統制と手続

登録企業は、開示統制とその手続の有効性に関する結論の開示を求められる。登録企業は、サイバー・インシデントにより、連邦証券取引委員会への提出書類において情報開示が求められている情報を記録、処理、要約及び報告する能力にリスクがもたらされた場合、経営陣は、その開示統制及び手続に不備が生じ、それにより開示統制と手続が無効となるか否かにつき、検討するべきである[53]。たとえば、サイバー・インシデントによる登録企業の情報システムに影響が及んだことで、適切に情報の記録ができない合理的な可能性がある場合には、登録企業は、その開示統制と手続が無効であると結論づけることになるかもしれない。

４．本指針制定後の評価・提案

4.1　連邦議会における反応

本指針が公布されてからおよそ２年後、連邦議会は、再び本指針について感心を示した[54]。2013年４月、本指針の策定に重要な役割を果たした上院議員のジョン・Ｄ・ロックフェラー４世は、連邦証券取引委員会のマリー・Ｊ・ホワイト委員長に対して、本指針の効果を賞賛するとともに、本指針を委員会レベルのものに引き上げるように求める手紙を送付している[55]。

これに対して、ホワイト委員長は、さらなる措置の必要性を見極めるため、情報開示の現状と本指針に関する全体的なコンプライアンスを見直すと回答している[56]。ただし、現在まで、具体的な変更はなされていない。

4.2　2014年のサイバーセキュリティに関する討論会

2014年３月26日に、連邦証券取引委員会は、サイバーセキュリティに関する討論会を開催した[57]。この討論会で議論された４つのテーマの中には、公開企業による情報開示の枠組みも含まれていた[58]。

この討論会での議論は有益ではあったものの、近年中に指針の強化等を求めるといった提案はなされなかった[59]。また、同委員会も、本指針の範囲を明確化するといったことも行わなかった[60]。

4.3　学説における本指針への提案

本指針に関しては、いくつかの論文で様々な提案がなされている。たとえば、ある著者は、①本指針を連邦証券取引委員会の正式な規則として制定するとともに、②情報開示を行う義務課す場合には、一定以上の被害額又は当該企業の資産の一定割合を超える被害を受けた場合に限定するとともに、③サイバー攻撃により受けた被害が実質的なものかどうかがグレーゾーンに入り判断が難しい場合には、秘密裏に連邦証券取引委員会にのみ報告する制度を構築

することで、事後的な訴訟等のリスクを回避するという提案を行っている[61]。

また、別の著者は、①投資家のリスク評価のために、公開企業は、その自主的な判断により情報セキュリティ監査人による格付け評価を公表する方法を採用することや、②これを連邦証券取引委員会による義務的な制度とすること、などを提案している[62]。

5．最後に

米国では、これまで紹介してきたように、2011年に本指針が発せられ、公開企業の年次報告と定期報告において、サイバーセキュリティ・リスクやインシデントを開示することが期待されるようになった。なお、本指針は、法的拘束力をもたないものの、これらのリスクやインシデントが従来の連邦証券諸法において「実質的な（material）」情報に該当する場合には、開示義務を負うことになる。

わが国でも、米国のこのような動向を受け、サイバーセキュリティに関するリスクを自主的に情報発進する方法のひとつとして有価証券報告書の活用が挙げられるようになった。しかしながら、どのような項目につき、どのような基準で開示すべきかを定めた指針は存在しておらず、企業の自主的な取り組みが推奨されるにとどまっている[63]。また、有価証券報告書の「事業等のリスク」の中で抽象的な記述がなされる場合が多く見受けられる[64]。

今後は、米国の例等を参考にしながら、有価証券取引法の下で、投資家の判断に十分に資する形での指針等の策定に取り組むべきであると考える。

注

1　米国において公開企業が負う環境関連情報の開示については、以下の２つの拙稿を参照のこと。永野秀雄「企業による環境関連情報のディスクロージャー　－米国証券取引法の下での偶発債務の開示とわが国への示唆－」人間環境論集６巻１号１頁以下（2005年）、永野秀雄「米国の公開企業と気候変動リスク－米国連邦証券取引委員会『気候変動に関する情報開示指針』の検討」人間環境論集12巻１号１頁以下（2011年）。

2　*How to Access & Sign Up for Identity Theft Repair & Credit Monitoring Services, Anthem Facts, available at* https://www.anthemfacts.com.

3　Bob Herman, *Details of Anthem's massive cyberattack remain in the dark a year later*, Modern Healthcare (Mar. 30, 2016), *available at* http://www.modernhealthcare.com/article/20160330/NEWS/160339997.

4　SEC, Div. of Corp. Fin., CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011) [hereinafter *Topic No. 2*], *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

5　本指針を扱った文献としては、ニュートン・コンサルティング株式会社『企業の情報セキュリティリスク開示に関する調査―調査報告書（平成26年度内閣サイバーセキュリティセンター委託調査）』（2015（平成27）年３月）がある。たしかに同報告書では本指針が取り上げられているものの（28-32頁）、簡単な概要が示されているにとどまっており、この内容から本指針の内容、効力、問題点等を把握することはできない。このため、本稿での本指針に関する分析には意義があると考える。

6　本論文の執筆にあたっては、邦語文献としては前注で挙げた『企業の情報セキュリティリスク開示に関する調査―調査報告書（平成26年度内閣サイバーセキュリティセンター委託調査）』に加え、三澤伴暁「サイバー・セキュリティ・リスクの開示に関する動向」PwC's View ３号（2016年７月）15頁を参照した。また、英語文献は、直接に引用したものを除き、以下の論文を参照した。*See* Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 Washburn L.J. 193 (2014); Joel Bronstein, *The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporation Finance's Recent Guidelines on Cybersecurity Disclosure Requirements*, 13 N.C. J.L. & Tech. On. 257 (2012); Matthew F. Ferraro, "*Groundbreaking*" *or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, its Effectivenss and Implications*, 77 Alb. L. Rev. 297 (2013 / 2014); Rick E. Hansen, *Climate Change Disclosure by SEC Registrants: Revisiting the SEC's 2010 Interpretive Release*, 6 Brook. J. Corp. Fin. & Com. L. 487 (2012); Matthew B. Hilowitz, *Developments in Banking and Financial Law: 2015: I. SEC Enforcement Efforts with Insider Trading and Cybersecurity*, 35 Rev. Banking & Fin. L. 120 (2015); Howard M. Privette, D. Scott Carlton & Sarah Kelly-Kilgore, *The SEC Guidance on Cybersecurity Measures for Public Companies*, 37 Los Angeles Lawyer 14 (2014).

7　なお、本稿では扱わないものの、連邦証券取引委員会は、公開企業に対して、サイバーセキュリティに関するコンプライアンスについての追加情報を求めている指針も出している。SEC, Off. of Compliance Inspections & Examinations, Nat'l Examination Program, Risk Alert: OCIE Cybersecurity Initiative (Apr. 15, 2014), *available at* https://www.sec.gov/

ocie/announcement/ Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

8 15 U. S. C. 77a-77aa (2012).

9 *Id.* at 78a-78ll.

10 *Id.* at 77a-77aa, 78a-78ll.

11 17 C. F. R. § 229 (2016).

12 *Id.* § 210.

13 *Id.* § 229. 101.

14 *Id.* § 229. 103.

15 *Id.* § 229. 303.

16 *Id.* § 229. 503 (c).

17 *Id.* § 229. 101 (a).

18 *Id.* § 229. 101 (b).

19 *Id.* § 229. 103.

20 *Id.* § 229. 303.

21 *Id.* § 229. 503 (c).

22 *Topic No. 2, supra* note 4.

23 *Id.*

24 TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).

25 *See generally id.*

26 Thomas Lee Hazen, Principles of Securities Regulation 259 (3d ed. 2009).

27 17 C. F. R. § 240. 10b-5 (2016).

28 *Id.* § 240. 14a-9.

29 Hazen, *supra* note 26, at 259.

30 *Id.*

31 原告は、当該証券の購入又は売却に関する詐欺（fraud or deceit）を立証しなければならない。*Id.* at 262.さらに、同規則10b-5条では、原告が立証すべき詐欺の構成要件として、コモンロー上の詐欺の要素である実質性（materiality）、これに対する信頼、因果関係及び損害を立証することを求めている。*Id.*

32 *Id.* at 263.

33 *Id.* at 211-12.

34 TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).

35 *Topic No.* 2, *supra* note 4.

36 Arnold & Porter, LLP, *SEC Cybersecury Disclosure for Public Traded Companies, Including Government Contractors* 1 (2011), *available at* http://files.arnoldporter.com/advisory-sec_cybersecurity_disclosure_%20fo_%20publicly-traded_companies.pdf.

37 Ellen Messmer, *2011's biggest security snafus: From Anonymous to the SCADA attack that wasn't; was this the year of the advanced persistent threat?*, Network World (Dec. 1, 2011), *available at* http://www.networkworld.com/article/2183666/security/2011-s-biggest-security-snafus.html.

38 Letter from John D. Rockefeller IV, Commerce Chairman, U.S. Senate to Mary Schapiro, Chairman, Sec. & Exch. Comm'n 1 (May 11, 2011), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.

39 *Topic No. 2, supra* note 4.

40 Joseph Menn, *SEC issues guidelines on hacking*, The Fin. Times (Oct. 14, 2011).

41 Connor R. Raso, *Strategic or Sincere? Analyzing Agency Use of Guidance Documents*, 119 Yale L. J. 782, 803 (2010).

42 *See* Roland L. Trope & Sarah Jane Hughes, *The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-thieves More?*, A. B. A. (Dec. 19, 2011), *available at* http://apps.americanbar.org/buslaw/blt/content/2011/12/article-3-trope-hughes.shtml.

43 サイバーセキュリティとは、ネットワーク、システム、コンピュータ、プログラム及びデータを、攻撃、損害又は不正アクセスから保護することを目的とした技術、プロセス及び実務の総体を意味する。Whatis?com, *available at* http://whatis.techtarget.com/definition/cybersecurity.html. *See also* Merriam-Webster.com *available at* http://www.merriam-webster.com/dictionary/cybersecurity.

44 本指針における情報は、1933年証券法の下で届出登録書（registration statements）に求められている情報開示、及び、1934年証券取引法の下での定期報告要件について、登録会社が情報開示を行うのを支援することを意図している。なお、登録会社は、発行届出書（shelf registration statements）における情報の正確性と完全性を確保するために、さらに、実質的なサイバー・インシデントにより生じた費用やその他の結果を開示するために、臨時報告書（Form 6-K）又は財務状況等に関する特別報告書（Form 8-K）を提出する必要があるか否かを検討しなければならない。*See* Item 5(a) of Form F-3 and Item 11(a) of Form S-3.

45 この点については、連邦証券取引法規則408条（Securities Act Rule 408）、連邦証券取引所法規則12b-20条（Exchange Act Rule 12b-20）及び同規則14a-9条（Exchange Act Rule 14a-9）を参照のこと。ある情報が、合理的な投資家にとってその投資決定に重要であると判断される相当の蓋然性がある場合、又は、当該情報が利用可能な情報の総体を実質的に変更する恐れがある場合に、当該情報は、実質的な（material）ものであると判断される。*See* Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976). さらに、登録会社は、連邦証券取引委員会への届出等における記載又は不記載に対して適用される連邦証券諸法上の詐欺防止条項についても考慮すべきである。*See* Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.

46 *See* Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

47 これは、証券取引委員会規則S-Kの503項(C)が、登

録会社に対して、どのような発行者又は募集にも当てはまりうるリスクを記述すべきではなく、かつ、当該登録会社に対してどのようにリスクが影響するのかを説明することを求めているためである。Item 503(c) of Regulation S-K.

48 *See* Item 303 of Regulation S-K; and Form 20-F, Item 5. 過去の多くの委員会通達では、これらの情報開示要件についての一般的な解釈指針が示されている。 *See, e.g.*, Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056] ; Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746]; Management's Discussion and Analysis of Financial Condition and Results of Operations; and Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427].

49 *See* Item 101 of Regulation S-K; and Form 20-F, Item 4.B.

50 *See* Item 103 of Regulation S-K.

51 *See* FASB ASC 275-10, Risks and Uncertainties.

52 *See* ASC 855-10, Subsequent Events.

53 *See* Item 307 of Regulation S-K; and Form 20-F, Item 15(a).

54 *See* Letter from John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci., & Transp., to Mary Jo White, Chairman, Sec. & Exch. Comm'n (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51.

55 *See id.*

56 *See* Letter from Mary Jo White, Chairman, Sec. & Exch. Comm'n, to John D. Rockefeller IV, Chairman, U.S. Senate Comm. on Commerce, Sci. & Transp. (May 1, 2013), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-97qfyd.

57 Cybersecurity Roundtable, March 26, 2014, *arailableat* http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.

58 *See* sifma.org, Mar 26 - SEC Holds Roundtable on Cybersecurity, *available at* http://www.sifma.org/members/hearings.aspx?id=8589948185 (last visited Oct. 25, 2014).

59 *See* Susan D. Resley et al., SEC Hosts Roundtable on Cybersecurity Issues and Challenges, Morgan Lewis, *available at* http://www.morganlewis.com/pubs/Securities_LF_SECRoundtableonCybersecurityIssues_31march14.

60 *Id.*

61 *See* Sam Young, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 Iowa J. Corp. L. 659, 676-678 (2013).

62 *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC Be Sticking Its Nose Under This Tent?*, 2016 U. Ill. J.L. Tech. & Pol'y 35, 61 (2016).

63 内閣官房・内閣サイバーセキュリティセンター「企業経営のためのサイバーセキュリティの考え方」(2016（平成28）年８月２日）４頁。

64 内閣官房・内閣サイバーセキュリティセンター「民間企業のサイバーセキュリティリスクの開示に係る動向等について」(2015（平成27）年３月）によれば、上場企業225社（日経225）の2009年から2013年の５年間における有価証券報告書において、「事業等のリスク」にサイバーセキュリティリスクの開示項目があった企業は136社（全体の60％）である。このうち、記載内容が５年間にわたり同一の企業は65社あり、その内容は包括的なもので具体性に欠けるものが多かったという。