米国 SEC による上場会社のサイバーセキュリティ関連の開示義務化について

金融ニューズレター　　2023 年 9 月 19 日号

執筆者:
濃川 耕平
k.koikawa@nishimura.com
横田 貴大
t.yokota@nishimura.com

1. はじめに

米国 Securities and Exchange Commission（SEC）は、2023 年 7 月 26 日付で新たにサイバーセキュリティに関する開示規制を採択しました [1]。本ニューズレターは、当該開示規制の概要 [2]を紹介するとともに、日本におけるサイバーセキュリティに関する開示規制の状況について論じるものです。なお、改正の内容について英文を日本語に翻訳している箇所がありますが、理解を容易にする観点から一部簡略化している箇所もあるため、正確な内容については原文である英文をご参照頂くようお願いいたします。

2. 改正の内容

(1) 概要

改正の内容は、大きく①Form 10-K や Form 20-F といった定期開示義務に基づく年次報告書におけるサイバーセキュリティへの対応状況及びセキュリティが侵害された場合の影響等の開示並びに②具体的にサイバーセキュリティに関するインシデントが生じた場合の Form 8-K や Form 6-K に基づく臨時開示義務の 2 つです。当該改正の内容については、①については 2023 年 12 月 15 日以降に終了する会計年度を対象とする年次報告書、②については原則として 2023 年 12 月 18 日以降に適用となります [3]。SEC は当該情報開示の必要性について、①上場会社の業務のデジタル化、リモートワークの増加、サイバーセキュリティのインシデントを収益化する犯罪者の能力、デジタルペイメントの利用及びクラウドコンピュータテクノロジーを含む情報技術サービスに対する第三者サービスプロバイダーへの依存の増大に伴って、サイバーセキュリティリスクが増加しており、サイバーセキュリティインシデントの発生による企業及びその投資家のコスト等も増加していること、並びに②2011 年及び 2018 年に SEC が発表した解釈ガイダンス [4]により一定の開示の向上は認められるものの、より規範的なアプローチが必要であると考えられたことを挙げています。以下では、まずは米国企業に適用される Form 10-K 及び Form 8-K の改正内容を説明します。

---

1 https://www.sec.gov/news/press-release/2023-139

2 より詳細な内容については、SEC の発表資料をご参照ください（https://www.sec.gov/files/rules/final/2023/33-11216.pdf）。

3 Smaller reporting companies（定義については Regulation S-K の Item 10(f)(1)をご参照）の場合は、2024 年 6 月 15 日以降となります。

4 https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
https://www.sec.gov/files/rules/interp/2018/33-10459.pdf

(2) 年次報告書におけるサイバーセキュリティへの対応状況等の開示

Form 10-K（日本における有価証券報告書に相当）においては、開示が必要な内容について Regulation S-K（SEC による非財務情報の開示規制）が引用されており、当該 Regulation S-K に Item 106 が新設される形で以下の内容の開示が必要となっています。

a. サイバーセキュリティに関するリスクマネジメント及びストラテジーの開示（Item 106(b)）

- サイバーセキュリティの脅威（cybersecurity threats[5]）による重大なリスクの評価、特定及び管理のためのプロセスがある場合は、当該プロセスについて、合理的な投資家が理解するために十分な程度に詳細な説明が必要となります。当該説明には以下の内容を含みます。
  - 当該プロセスが全体的なリスク管理システム又はプロセスに統合されているか否か及び統合の方法
  - 当該プロセスに関連して評価人、コンサルタント、監査人又はその他の第三者が関与しているか否か
  - 第三者が提供するプロバイダーの使用に関連したサイバーセキュリティの脅威による重大なリスクを監視及び特定するプロセスを有しているか否か
- 以前発生したサイバーセキュリティインシデントの結果を含めサイバーセキュリティの脅威に起因するリスクが、当該企業（当該企業のビジネス戦略、業績又は財政状態を含む）に重大な影響を及ぼしたか、又は重大な影響を与える可能性が合理的に高いか否か、該当する場合にはどのように該当するか、について説明が必要となります。

b. サイバーセキュリティに関するガバナンスの開示（Item 106(c)）

- サイバーセキュリティの脅威に関するリスクに対する取締役会による監視について説明が必要となります。加えて、監督を取締役会又は下位の委員会が担当している場合は、当該委員会を特定するとともに、当該委員会に対して当該リスクが通知されるプロセスの説明が必要となります。
- サイバーセキュリティの脅威による登録会社の重大なリスクに対する評価及び管理について、以下の内容についても適宜言及しながら、経営陣の役割を説明することが必要となります。
  - どのポジションの経営陣又は委員会が当該リスク評価及び管理する責任を負うか、並びに当該

[5] Cybersecurity threat については、"any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein"と定義されています（Item 106(a)）。

個人又は委員会メンバーが有する関連する専門知識（当該専門知識の性質を説明するために十分に詳細であること）

- サイバーセキュリティインシデントの防止、発見、軽減及び修復について、当該個人又は委員会へ通知されるプロセス及び当該個人又は委員会による監視プロセス
- 当該リスクに関する情報を当該個人又は委員会が、取締役会又は取締役会の委員会若しくは下位の委員会に報告するか否か

(3) インシデントが生じた場合の臨時開示

a. 開示のタイミング

サイバーセキュリティインシデント（cybersecurity incident[6]）が重大であると登録会社が判断した場合、4 営業日以内に 8-K（日本における臨時報告書に相当）を提出しなければなりません（Form 8-K Item 1.05(a)）。登録会社は、当該インシデント発見後、重要性に関する決定を「不当な遅延なしに（without unreasonable delay）」行わなければならないとされています（Instructions to Item 1.05(1)）。但し、米国司法長官（United States Attorney General）が当該サイバーセキュリティインシデントの臨時開示が「国家安全保障又は公共の安全に重大なリスク」をもたらすと判断し、そのような決定を書面で SEC に通知した場合、原則として、当該 Form 8-K の提出を最大 30 日間遅らせることができるとされています（Form 8-K Item 1.05(c)）。

b. 開示の内容

Form 8-K で要求されているセキュリティインシデントの開示内容は以下の通りです。

- インシデントの性質、範囲及びタイミングの重要部分
- 登録会社において生じる又は生じる可能性のある重大な影響（財政状態及び経営成績を含みます。）

但し、Form 8-K の提出の時点で、当該情報が未確定又は利用できない場合、当該情報が確定又は利用可能となったのち、不当な遅延なしに（without unreasonable delay）、4 営業日以内に訂正報告書（amendment to its Form 8-K filing）を提出する旨の開示を行うことが認められています（Instructions to Item 1.05(2)）。また、当該インシデント若しくはサイバーセキュリティシステム、関連するネットワークとデバイス、又は潜在的なシステムの脆弱性に対する対応策に関して、特定の又は技術的な情報について、登録会社の対応又はインシデントの修復を妨げるほど詳細な開示は必要ないとされています

---

6 Cybersecurity incident については、"an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein"と定義されています（Regulation S-K Item 106(a)）。

（Instructions to Item 1.05(4)）。

3. Foreign Private Issuer への適用

日本企業その他の外国民間発行体が、Foreign Private Issuer（FPI）[7]として米国での開示義務を負っている場合、上記 2 と同等の開示が Form 20-F（日本における有価証券報告書に相当）又は Form 6-K（日本における臨時報告書に相当）で要求されることになります。

具体的には、Form 20-F においては、新たに Item 16K という開示項目が設けられ、定期開示義務に基づき 20-F を提出する場合[8]には、上記 Regulation S-K の Item 106 と同様の内容の開示が必要となります。

また、Form 6-K においては、General Instruction B に"material cybersecurity incidents"の文言が追記されました。"material cybersecurity incidents"に関する情報が以下のいずれかに該当して開示される場合には、米国においても開示が必要となります。

(i) 設立準拠法域の法令に従い、開示する場合又は開示することが求められる場合

(ii) 登録会社の証券が取引されている取引所に対して提出する場合又は提出することが求められる場合で、それが取引所によって開示された場合

(iii) 登録会社の証券の保有者に対して配布する場合又は配布することが求められる場合

4. 日本におけるサイバーセキュリティ開示規制

(1) 有価証券報告書における開示について

日本におけるサイバーセキュリティに関する有価証券報告書上の開示義務については、金融商品取引法上、直接的な開示項目として定められたものはないものの、上場会社の個々の開示項目への該当性判断を通じて、有価証券報告書の「経営方針、経営環境及び対処すべき課題等」[9]、「事業等のリスク」[10]、「コーポレート・ガバナンスの概要」[11]等において記載されることがありました。

---

7 FPI の該当性要件については Exchange Act of 1934 に基づく Rule 3b-4 をご参照ください。

8 "Instruction to Item 16K. Item 16K applies only to annual reports, and does not apply to registration statements on Form 20-F."

9 企業内容等の開示に関する内閣府令（以下「開示府令」といいます。） 第三号様式記載上の注意(10)、第二号様式記載上の注意(30)

10 開示府令 第三号様式記載上の注意(11)、第二号様式記載上の注意(31)

金融庁 2023 年 3 月 24 日付「記述情報の開示の好事例集 2022」（https://www.fsa.go.jp/news/r4/singi/20230131/01.pdf）では、オムロン株式会社、ヤマハ株式会社の例が記載されている。

11 開示府令 第三号様式記載上の注意(35)、第二号様式記載上の注意(54)

もっとも、総務省による 2019 年 6 月付「サイバーセキュリティ対策情報開示の手引き[12]」p.14 によれば、「現状、サイバーセキュリティ対策に係る記載の量は、任意開示の書類（CSR 報告書、サステナビリティ報告書）が比較的多い傾向にあり、制度開示（有価証券報告書、コーポレート・ガバナンス報告書）の書類では比較的少ない傾向にある」とされています。

近時、2023 年 1 月 31 日付「企業内容等の開示に関する内閣府令」等の改正により「サステナビリティに関する考え方及び取組[13]」が有価証券報告書において求められることになりました。ここでいう「サステナビリティ情報」には、「国際的な議論を踏まえると、例えば、環境、社会、従業員、人権の尊重、腐敗防止、贈収賄防止、ガバナンス、サイバーセキュリティ、データセキュリティなどに関する事項が含まれ得ると考えられる[14]」とされています。当該開示項目においては、サステナビリティに関する考え方及び取組の状況について、①ガバナンス及びリスク管理、②戦略並びに指標及び目標のうち重要なもの、③人的資本に関する戦略並びに指標及び目標について記載すべきとされています。

この点に照らすと、今後有価証券報告書においてもサイバーセキュリティに関連する詳細な開示がなされる例が増える可能性はあるものの、「開示が求められるサステナビリティ情報については、開示原則において示された全ての項目を記載する必要はなく、各企業において、自社の業態や経営環境、企業価値への影響等を踏まえ、サステナビリティ情報の重要性を判断することが求められて[15]」いるとの金融庁の回答によれば、現状においても引き続き開示の要否及びその内容は、基本的に各社の開示項目への該当性判断に委ねられたままの状況であると考えられます。

(2) 適時開示及び臨時報告書における開示について

a. 概要

重大なセキュリティインシデントが発生し、当該インシデントが、東京証券取引所の適時開示事由[16]や臨時報告書の提出要件[17]に該当する場合には、適時開示及び臨時報告書による開示を行うことが必要となります。特にその発生の内容、影響、被害の状況等によっては、投資者の投資判断に影響を及ぼすものとして、適時開示及び臨時報告書のいわゆる「バスケット条項[18]」に該当する可能性があります。

---

12 https://www.soumu.go.jp/main_content/000630516.pdf

13 開示府令 第三号様式記載上の注意(10-2)、第二号様式記載上の注意(30-2)

14 記述情報の開示に関する原則（別添）―サステナビリティ情報の開示について―（https://www.fsa.go.jp/news/r4/sonota/20230131/07.pdf）

15 金融庁（2023 年 1 月 31 日）「『企業内容等の開示に関する内閣府令の一部を改正する内閣府令（案）』に対するパブリックコメントの概要及びコメントに対する金融庁の考え方」106、107 番（https://www.fsa.go.jp/news/r4/sonota/20230131/01.pdf）

16 東京証券取引所有価証券上場規程（以下「上場規程」といいます。）第 402 条第 1、2 号ご参照

17 開示府令第 19 条第 2 項ご参照

18 上場規程第 402 条第 1 号 ar、同条第 2 号 x、開示府令第 19 条第 2 項第 12、19 号

b.　開示のタイミング

インシデントの発生がバスケット条項に該当する場合は、適時開示については「直ちに [19]」開示すること、臨時報告書については「遅滞なく [20]」提出を行うこととされており、Form 8-K と異なり具体的な日数等は定められていません。いずれにおいても、重要な事象が発生していることを投資者に対してできる限り早く開示することが望ましい点に照らすと、損害や詳細等が未確定の場合であってもインシデントの概要を一旦開示し、詳細は改めて開示を行うなどの対応が考えられます [21]。

c.　開示の内容

インシデントの発生がバスケット条項に該当する場合は、適時開示においては「ａ．事実の概要　ｂ．発生の経緯　ｃ．今後の見通し [22]　ｄ．その他投資者が会社情報を適切に理解・判断するために必要な事項」、臨時報告書においては「イ 当該事象の発生年月日　ロ 当該事象の内容　ハ 当該事象の連結損益に与える影響額」を記載することが必要とされており、上記の SEC が 8-K で要求している開示内容と類似した内容の開示が行われる可能性が高いと思われます。

5. まとめ

コロナ禍において、日本社会においてもリモートワーク、業務のデジタル化などが急速に広がっており、米国と同様にサイバーセキュリティを巡る社会的な状況の変化が生じていると考えられます。また、日本の金商法上の開示規制は、SEC の開示規制を参考にしている部分も多いため、今後日本における法令改正等に影響を与える可能性もあります。一方で、「強制開示は、企業の負担が大きいという問題がある（罰則等を恐れて、過度に保守的な開示や体制構築へと向かうおそれ）」との指摘もあり [23]、今後の議論が待たれます。

19　上場規程第 402 条柱書

20　金融商品取引法第 24 条の 5 第 4 項

21　宝印刷株式会社/株式会社ディスクロージャー&IR 総合研究所・編「適時開示の実務 Q&A〔第 2 版〕」（商事法務、2018）25 頁、宝印刷株式会社/株式会社ディスクロージャー&IR 総合研究所・編「臨時報告書作成の実務 Q&A」（商事法務、2015）12 頁

22　①当期以降の業績に与える影響の見込み及び②今後の方針等がある場合はその内容も記載する。

23　総務省サイバーセキュリティタスクフォース・情報開示分科会「資料 1-5　会社法・金商法上のリスク情報の開示の現状と課題」[大杉謙一]（2017 年 12 月 13 日）（https://www.soumu.go.jp/main_content/000528737.pdf）

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。
また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所・外国法共同事業 広報室 newsletter@nishimura.com