In brief

SEC がサイバーセキュリティ開示規則を採択

No. US2023-05
July 26, 2023
(revised December 14, 2023)

サイバーセキュリティのリスクやインシデントの発生は現代生活においてますます避けがたいものとなっています。重要性のあるインシデントが発生した場合、財務、業務、法務、レピュテーションなど、幅広い影響をもたらす可能性があります。

SEC 議長 ゲンスラー氏
2023 年 7 月 26 日

要点

米国証券取引委員会（SEC）は、公開企業（外国登録企業（FPI）を含む）によるサイバーセキュリティに関連する開示の拡充と標準化を要求する修正を採択しました。

本資料は、SEC スタッフにより最近公表された解釈指針ならびに米国司法省（DOJ）および米国連邦捜査局（FBI）により公表されたインシデント報告の遅延要請に関するガイダンスを追加するため、2023 年 12 月 14 日にアップデートされました。

最新の動向

2023 年 7 月 26 日、SEC は、サイバーセキュリティに関連する開示の拡充と標準化を目的とする修正を採択しました。本修正は、重要性のあるサイバーセキュリティインシデントの適時開示と、サイバーセキュリティのリスク管理、戦略、ガバナンスに関する年次開示を要求しています。最終規則は 1934 年証券取引所法に基づく報告を行う、全ての登録企業に適用されます。また、最終規則は、2022 年に公表された規則案に記載されていたいくつかの規定の変更を反映しています。これには、開示の簡素化および個別には重要性の低いサイバーセキュリティインシデントの集約と報告についての明確化が含まれています。

本新規則は、SEC 登録企業の年次開示を大幅に拡充し、投資家およびその他の利害関係者に、登録企業のサイバーセキュリティのリスク管理、戦略、ガバナンスに関するより標準化された情報を提供します。重要性のあるサイバーセキュリティインシデントの開示では、より具体的かつ詳細さが要求されるため、登録企業は、過去に行ったそのような事象に関する報告よりも迅速に対応する必要があります。これにはシステム、プロセスおよび統制の変更が必要となります。

重要性のあるインシデントの適時開示

米国の SEC 登録企業または米国書式でファイリングを行う FPI は、登録企業がサイバーセキュリティインシデントに重要性があると判断してから 4 営業日以内に、Form 8-K の新項目である Item 1.05 において当該インシデントの報告が要求されます。

SEC は、サイバーセキュリティインシデントを「登録企業の情報システムまたは情報システムに存在する情報の機密性、完全性、または利用可能性を脅かす、登録企業の情報システム上または情報システムを介した不正の発生または一連の関連する不正の発生」と定義しています。インシデントに重要性があるかどうかの判断は、連邦証券法で用いられている重要性の定義に基づきます。登録企業は、発見後、不合理に遅延することなくインシデントの重要性を判断しなければなりません。

インシデントの定義には、一連の関連する事象が含まれています。例えば、同一の悪意ある主体または同一の脆弱性の悪用が関係している場合、それらの事象は関連がある可能性があります。一連の関連する不正の発生により、企業が重要性のある影響を受けていると結論付けられた場合、個々の発生事象には重要性がないと判断した場合であっても、Form 8-K による開示要求事項が適用されます。

Form 8-K には、インシデントの性質、範囲、時期の重要性のある側面および、財政状態や経営成績など、登録企業に関する重要性のある影響または重要性があると合理的に考え得る影響の記載が要求されます。登録企業は、インシデントやシステムへの対応計画における具体的な情報または技術的な情報を、インシデントへの対応や是正を妨げるほど詳細に開示する必要はありません。

Form 8-K で開示を要求される情報が、ファイリング書類の提出時までに確定しないまたは入手できない場合、登録企業は、提出書類にその旨を記載しなければなりません。この情報が確定または入手可能になった場合には、登録企業は 4 営業日以内に修正した Form 8-K を提出しなければなりません。

本規則は、即時開示が国家安全保障または公共の安全に相当のリスクをもたらす可能性があることを、米国司法長官が書面により SEC に通知した場合について、一連の延長を規定しています。2023 年 12 月、DOJ および FBI の両方から、SEC 登録企業がサイバーセキュリティインシデントの開示がこの規準を満たすと考える場合の支援となるガイダンスを公表しました。さらに、SEC スタッフは関連する考慮事項に対応する法令遵守および開示に関する解釈指針（C&DI）を公表しました。

FPI Forms を提出する FPI は、Form 6-K の指示書に概説されているその他の要件を満たしていることを前提として、Form 6-K による重要性のあるサイバーセキュリティインシデントに関する情報の提供が要求されます。

リスク管理、戦略、ガバナンスの年次開示

Regulation S-K の新項目である Item106 は、SEC 登録企業に対し、Form 10-K または Form 20-F の年次報告書において、企業のサイバーセキュリティに関するリスク管理、戦略およびガバナンスに関する情報の提供を要求しています。

リスク管理と戦略

SEC 登録企業は、サイバーセキュリティの脅威から生じる重要性のあるリスクの評価、特定、管理についてのプロセスがある場合には、投資者がそれらのプロセスを理解するのに十分な詳細さで記載することが要求されます。要求される開示には、以下（に限らない）の事項が含まれます:

- プロセスは、登録企業の全体的なリスク管理システムまたはプロセスに統合されているか、またどのように統合されているか
- 登録企業は、当該プロセスに関連して、評価者、コンサルタント、監査人またはその他の第三者を従事させているかどうか
- 登録企業が、第三者サービスプロバイダの利用に関連するサイバーセキュリティの脅威から生じるリスクを監視および特定するプロセスを有しているかどうか

また、登録企業は、過去のサイバーセキュリティ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から生じるリスクが、登録企業の事業戦略、業績、財務状況を含め、登録企業に対し、重要性のある影響を与えたか、または、重要性のある影響を与える可能性が合理的に高いかどうか、そしてどのように影響を与えた（または、与える可能性が合理的に高いか）を説明しなければなりません。

ガバナンス

経営者および取締役会によるサイバーセキュリティリスクの監督について、以下の開示が要求されます。

- サイバーセキュリティの脅威から生じるリスクに対する取締役会の監督の記述
  - サイバーセキュリティの脅威から生じるリスクの監督に責任を負う、取締役委員会または小委員会の特定
  - そのようなリスクについて取締役会または委員会が情報提供を受けるプロセス
- 以下の開示事項（ただし、これらに限定されない）など、サイバーセキュリティの脅威から生じる登録企業の重要性のあるリスクの評価および管理における経営者の役割の記述

- 経営委員会または役職がそのようなリスクの評価や管理の責任を負うかどうか、責任を負う場合にはどの経営委員会又は役職が負うのか、そのような担当者や委員が有する関連する専門知識
- 上述の担当者または委員会がサイバーセキュリティインシデントの防止、検出、軽減、是正についての情報を提供され、監視を行うプロセス
- 上述の担当者または委員会は、当該リスクに関する情報を取締役会または取締役会内の委員会や小委員会に報告するか

次のステップ

SEC 登録企業は、Form 8-K または Form 6-K に定義される重要性のあるサイバーセキュリティインシデントの報告要求の遵守を 2023 年 12 月 18 日に開始しなければなりません。小規模報告企業は 2024 年 6 月 15 日から適用になります。

全ての登録企業は、2023 年 12 月 15 日以後に終了する事業年度の年次報告書より年次開示要求の遵守が要求されます。