In brief

SECがサイバーセキュリティに関する新たな開示要求事項を提案

No. US2022-04
March 17, 2022

要点

米国証券取引委員会（SEC）が、すべての公開企業および外国登録企業（FPI）のサイバーセキュリティに関連する新たな開示を提案しました。この提案に対するコメント募集期限は5月です。

最新の動向

2022年3月9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図るための修正を提案しました。このSEC規則案「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、およびインシデントの開示」の主要な規定は以下のとおりです。

重要性のあるインシデントの適時開示

SEC登録企業は、発生したサイバーセキュリティインシデントに重要性があるとの判断を下してから4営業日以内に、Form 8-Kを用いて当該インシデントについての報告を行うことを要求されます。インシデントに重要性があるかどうかの判定は、米国証券法で使用される重要性の定義に基づきます。

開示には以下が含まれます。

- いつインシデントを発見したか、インシデントは現在進行中か
- インシデントの性質および範囲の簡単な説明
- データは盗難、改変、アクセス、または他の許可されていない目的のために使用されたかどうか
- インシデントがSEC登録企業の事業に与える影響
- SEC登録企業はすでにインシデントを修復したか、あるいは現在修復中か

また、SEC登録企業は、当初にインシデントの報告を行ったForm 8-Kにおいて開示した情報の重要な変更、追加、更新があればForm 10-KやForm 10-Qでも開示することが必要になります。さらに、これまで報告していなかった個別には重要性の低い一連のインシデントが、合算して重要性が生じた場合、Form 10-KおよびForm 10-Qで開示することが必要になります。

リスク管理および戦略の年次開示

Regulation S-Kへの追加が提案されているItem 106は、SEC登録企業に対し、サイバーセキュリティに関するリスク管理と戦略について、首尾一貫し、より有用な開示の提供を要求しています。開示には、サイバーセキュリティリスクの評価ならびに管理、関連する方針、手続および戦略の実施における経営者の役割と関連する専門知識が含まれます。また、同案では、サイバーセキュリティリスクの特定と管理に関する方針および手続（ある場合）ならびにSEC登録企業のサイバーセキュリティ・ガバナンスに関する情報についての開示の拡充を要求しています。

経営者の役割と専門知識

経営者の役割と専門知識の開示には、以下が含まれます。

- 特定の管理職または委員会がサイバーセキュリティリスクの測定および管理の責任を負っているかどうか、ならびにそれらの者の有する関連する専門知識についての説明
- 指名された最高情報セキュリティ責任者、または同等の者がいるかどうか、その者が組織内の誰に対して報告を行うか、およびその者の有する関連する専門知識についての説明

- サイバーセキュリティインシデントについて情報セキュリティ責任者または委員会に伝達する報告プロセス、およびサイバーセキュリティインシデントの防止、軽減、発見、修復の監視プロセス
- 情報セキュリティ責任者または委員会が、取締役会またはサイバーセキュリティリスクに関する取締役会内の委員会に報告を行うかどうか、およびその頻度

サイバーセキュリティリスクの特定および管理に関する方針と手続

方針および手続の開示には、SEC登録企業のサイバーセキュリティリスク評価プログラム（ある場合）、コンティンジェンシープランまたはリカバリープラン、および第三者の利用についての説明が含まれます。さらに、SEC登録企業は、企業の事業戦略、財務計画、資本配分の一環としてサイバーセキュリティリスクを考慮しているかどうか、そしてそれをどのように考慮しているかを開示するとともに、過去に発生したサイバーセキュリティインシデントが企業のガバナンス構造をどのように変えたかを説明することも要求されています。

最後に、SEC登録企業は、サイバーセキュリティリスクおよびサイバーセキュリティインシデントが企業の業績または財務状況に影響を与えたか、または影響を与える可能性が合理的に高いかどうか、影響を与える場合にはどのような影響かを示す必要があります。

取締役会のガバナンス

SEC登録企業は、取締役会によるサイバーセキュリティリスクの監視およびサイバーセキュリティに関する専門知識がある場合、その詳細を開示することが要求されます。取締役会の監視に関連する開示には、以下が含まれます。

- 取締役会の全員、特定の取締役、あるいは委員会が、サイバーセキュリティリスクの監督の責任を負っているかどうか
- 取締役会がサイバーセキュリティリスクについての情報提供を受けるプロセス、およびこのトピックに関する議論が行われる頻度
- 取締役会または取締役会内の委員会が、企業の事業戦略、リスク管理および財務計画の一環としてサイバーセキュリティリスクを考慮しているかどうか、そしてそれをどのように考慮しているか

SEC登録企業は、取締役のうちの誰かがサイバーセキュリティに関する専門知識を有しているかどうか、専門知識を有している場合には、当該取締役の氏名および専門知識の性質を開示することが要求されます。この規則案では「サイバーセキュリティの専門知識」を定義していませんが、取締役がサイバーセキュリティに関する過去の業務経験や知識を有しているか、サイバーセキュリティに関する資格や学位を有しているかどうかなど、その判定において考慮すべき事項が記載されています。

その他の新たなサイバー関連規則および提案

法整備

2022年3月15日、米国サイバーセキュリティ強化法（法律）が法制化されました。同法の規定は、非常に重要なインフラストラクチャーの所有者および運営者に対し、「実質的な」サイバーインシデントについては72時間以内、ランサムウェア（訳注：身代金要求型不正プログラム）への支払については24時間以内に米サイバーセキュリティ・インフラセキュリティ庁（CISA）に報告することを要求しています。また、CISAの長官に24か月以内に規則を策定する権限を付与しました。詳細については、PwC米国の「Cyber breach reporting to be required by law for better cyber defense」（英語のみ）をご参照ください。

SEC登録済投資アドバイザーおよびファンドに関するSEC規則案

SECは、2022年2月、SEC登録投資アドバイザー、SEC登録投資会社、および事業開発企業に対し、サイバーセキュリティリスクに対処するため、明文化されたサイバーセキュリティ方針および手続の導入と実施を要求する規則を提案しました。また本規則案は、投資アドバイザーに対し、投資アドバイザーやその顧客であるファンドまたはプライベート・ファンドに影響を及ぼす重大なサイバーセキュリティインシデントをSECに秘密裏に報告することを要求しています。詳細については、In brief US2022-02「SECがプライベート・ファンドおよびアドバイザーに影響を及ぼす規則を提案」（英語のみ）をご参照ください。

SECの既存のサイバーガイダンス

サイバーセキュリティの開示に関する、SECによる現行の解釈指針は2011年版および2018年版の開示ガイダンスに記載されています。現行の解釈指針ではリスク要因、事業の説明、経営者による説明と分析（MD&A）、法的手続、開示に関する統制および手続、または財務諸表においてサイバーセキュリティリスク、方針および手続、ならびに重要性のあるインシデントを開示することを要求していますが、詳細さのレベルについての規範的な要求事項はありません。

なぜ重要なのか

2022年3月9日公表の本規則案は、外国登録企業（FPI）を含むすべての公開企業に適用されます。現在の開示要求は米国企業か外国登録企業かで異なっていますが、本規則案はFPIに関する要求事項を修正し、すべてのSEC登録企業に首尾一貫したサイバーセキュリティ開示の提供を求めます。

SECのリリースによると、本規則案は、SEC登録企業のサイバーセキュリティリスク管理、戦略、ガバナンスおよびサイバーセキュリティインシデントに対するエクスポージャーについてのより良い情報を投資家に提供することを目的としています。

この規則が提案通りに最終化された場合、サイバーセキュリティインシデントの定義の適用方法やインシデントの重要性の判定方法など、いくつかの条項の適用は解釈と判断が伴うことになるでしょう。

次のステップ

コメント募集期限は、連邦官報掲載後30日間または5月9日のいずれか遅い方の日となります。SECは寄せられたフィードバックを検討し、今年度末までに最終規則を公表する見込みです。それまでの期間において、企業は、規則が現在の提案通りに最終化された場合、その遵守のために自社のプロセス、コントロール、ガバナンス構造、開示の強化が必要かどうかを検討しなければなりません。

PwC米国では、3月後半にこの提案の概要を説明するポッドキャストを公表する予定です。Viewpoint.pwc.com またはポッドキャストでご視聴ください。