

米国証券取引委員会 (SEC) の サイバーセキュリティ開示最終規則

取締役会の視点

最終規則が課す重要な開示要件 — 取締役会による厳格な監視強化が急務に。

最終規則の概要

サイバーセキュリティインシデントに重要性がある場合、 Form 8-Kでの報告が必須

上場企業は今後、「サイバーセキュリティインシデント」を発見した際、インシデントの発見時点からではなく、重大であると企業が判断してから4営業日以内に報告することが義務づけられます。さらに、重要性の判断も、インシデントの発見後、「不合理な遅滞なしに」おこなわなければなりません。開示すべき情報として、インシデントの性質や影響範囲、発生時期に関する要点のほか、財務状況や事業結果を含め、自社に対する重要な影響（または合理的にみて生じる可能性が高い重要な影響）に関する記述が含まれます。重要性の判断に関する上記の期限の遵守においては、経営陣の能力が試されることになるかもしれません。事実が次々と明らかになり、サイバーインシデントへの対応に依然として追われる状況においては、経営陣にとってかなりの難題となりえます。適時に重要性の判断をおこなうには、内部統制や開示統制の新たな構築または改定に加え、サイバーチーム、証券を専門とする弁護士、サイバーチームを支援する弁護士、経営層による開示チームで、連携することが必要になります。

企業側は、法執行機関が延期を要請した場合や、国家安全保障にかかわる場合には開示することについて、懸念を示していましたが、最終規則では例外は極めて限定的となっています。米国司法長官が速やかな開示が国家安全保障または公共安全に重大なリスクをもたらすと判断し、SECに書面で通告した場合、(特段の事情がない限り)開示を最長60日遅らせることができます。ただし、実際問題として、米国司法長官からそのような迅速な決定を得るのは困難と考えられます。また、現行の米国証券取引所法に基づくSEC規則0-6を受け、国家防衛または対外政策に係る権益を保護するために米国連邦政府の省庁局が機密指定している情報の開示も、不要とされます。以前に開示した重要性のあるインシデントについて当初のForm 8-Kの提出時点で入手できなかった情報や未確定だった情報を新たに入手した場合、Form 8-Kにおけるインシデントの開示を最新の内容に修正することが求められます。

サイバーセキュリティリスクの管理、戦略、ガバナンスに 関する開示

企業は、サイバーセキュリティ脅威からの重要なリスクを評価・特定・管理するプロセス、および、現在の脅威や過去のサイバーセキュリティインシデントによるリスクの重大な影響や合理的に予測される影響について、Form 10-Kで開示することが義務づけられます。企業は、取締役会レベルが有するサイバーセキュリティの専門知識については開示が求められない一方、サイバーセキュリティ脅威によるリスクを取締役会がどのように監視するか、サイバーセキュリティの脅威のリスクを評価・管理するための経営陣の役割と専門知識については記述が必要になります。

発効日

サイバーインシデント開示のForm 8-Kは、米国連邦官報の公告日の90日後か2023年12月18日のいずれか遅い方の日から義務づけられます。小規模報告会社の場合、Form 8-Kにおける開示義務の開始までさらに180日の猶予が与えられます。全ての上場企業は、2023年12月15日以後に終了する会計年度の年次報告書から毎年Form 10-Kで開示をおこなうことが一律に要求されます。

Form S-3の使用資格、セーフハーバー

重大なサイバーインシデントの報告が遅れてForm 8-Kを提出しても、Form S-3申請書の略式版を使用できなくなることはありません。また、新規則は、経営陣が迅速に重要性の判断をおこなわなければならないため、米国証券法上の責任からの限定的なセーフハーバーが提供されています。




コンプライアンス遵守に向けた 経営陣のモニタリング

最終規則は企業のサイバーセキュリティに関する開示義務を大幅に拡大しています。以前から準備を進めてきた企業が多いとはいえ、最終規則の遵守に向けた準備は経営者にとって果たすべき重大な課題であるため、取締役会による監視が不可欠です。以下、取締役会の注目のべき点を取り上げます。

サイバーセキュリティガバナンスの開示

最終規則で要求されるのは、Form 10-Kで、「サイバーセキュリティの脅威によるリスクの取締役会による監視について記述すること。取締役会に委員会または小委員会を設置している場合、サイバーセキュリティの脅威によるリスクを監視する責任を負う委員会または小委員会を特定し、取締役会または委員会が当該リスクについて報告を受けるプロセスを記述すること」です。この開示に向けて準備するなかで、取締役会がサイバーセキュリティリスクの監督責任を(委員会構成を通じて)どのように割り当て、調整するか再評価する必要があります。サイバーセキュリティリスクの監視については、取締役会によってアプローチはさまざまですが、監査委員会に監視機能を委ねるケースが大半です。サイバーセキュリティの監視が取締役会全体またはテクノロジー委員会などの別の委員会に委ねられている場合でも、監査委員会がサイバーセキュリティ関連の内部統制や開示統制、手続の有効性を引き続き監視することが必要になります。複数の委員会が関与する場合、委員会間や取締役会全体との情報共有やコミュニケーション、連携が肝要です。取締役会は、必要なプロセスを確立するために協力することが重要です。




ガバナンスの開示にも、サイバーセキュリティ脅威による重大なリスクの評価・管理にする経営陣の役割を記述しなければなりません。最終規則では、開示の際に、適宜、以下の項目にも言及することが求められています。

-  どの経営陣または委員会がサイバーセキュリティリスクの評価・管理の責任を負うか、また、責任を負う者または委員会が有するサイバーセキュリティ関連の専門知識の内容、性質を詳細に記述すること
-  上記の者または委員会がサイバーセキュリティインシデントについて報告を受け、ならびに防止、検知、緩和および是正を監視するためのプロセス
-  上記の者または委員会がリスク情報を取締役会または取締役会の委員会もしくは小委員会に報告しているかどうか

これらのガバナンスに関する開示の準備には時間と注意力を要し、取締役会や経営陣による現行のサイバーセキュリティガバナンスのプロセスのほか、既存のガバナンス開示についても、再評価する必要があります。今後経営陣がForm 10-Kにおける開示に向けて準備をおこなううえで、取締役会は今から積極的に経営陣と協力することが望まれます。

サイバーセキュリティリスクの管理および戦略に関する開示

最終規則では、サイバーセキュリティ脅威による重大なリスクを評価・特定・管理するプロセスを整備している場合、これを合理的な投資家が理解できるよう十分詳細にForm 10-Kに記述するよう企業に求めています。開示の際には、以下の開示項目(項目を限定するものではありません)に適宜、対処する必要があると書かれています。

-  上記のプロセスが会社全体の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否か、統合されている場合、どのように統合されているか
-  上記のプロセスに関して評価者、コンサルタント、監査人などの第三者を関与させているか否か
-  第三者である業務提供者の利用に伴うサイバーセキュリティ脅威によるリスクを監視・特定するプロセスを整備しているか否か

加えて、過去のサイバーセキュリティインシデントによるものも含め、サイバーセキュリティ脅威によるリスクが事業戦略や経営成績、財務状況に重大な影響を与えたか、あるいは重大な影響を及ぼす可能性が合理的にみて高いか否か、についても記述するよう企業に求めています。

これらのリスク管理や戦略の開示に向けた準備には、既存のリスク管理プロセスや関連する開示の再評価、および修正が必要になると予想されます。繰り返しになりますが、経営陣が今後Form 10-Kにおける開示に向けて準備するにあたり、取締役会は今から経営陣と協力することが重要です。

経営者のサイバーインシデント対応計画

経営陣のサイバーインシデントに関する対応方針や手順は開示統制や手続も含め、経営陣による是正や調査の取り組みと並行して、重要性を適切に考慮し迅速に対応するために、内容の見直しと最新化することが必要不可欠です。これには、経営層によるサイバーセキュリティおよびリスク管理チームや開示委員会、法務部門の責任の明確化、重要性の判断をする際のエスカレーション手順、開示の準備・レビューに関する手順の策定が含まれます。エスカレーション手順に盛り込むべきものとして、取締役会が報告を受けるタイミングのほか、社内外コミュニケーションの取り扱いも挙げられます。経営陣と取締役会は机上演習を実施し、インシデントの文書化や重要性の評価方法、Form 8-Kの開示ドラフト作成の手順を含め、経営陣の対応計画や手続を検証し、反省点を反映させて改善を図ることが望まれます。さらに、インシデント対応計画については、変化するサイバーリスクの状況を考慮し、定期的に更新していくことも必要です。

「重要性」の検討

最終規則では、「インシデントの発見後、不合理な遅滞なしに」重要性の判断をおこなうよう企業に求めています。重要性の定義に変更はないものの、その基準をサイバーセキュリティインシデントの状況に応じて適用するのは簡単ではありません。SECは最終公表版で、インシデントの重要な影響を評価する際に、定性的要因を検討するべきであると述べており、重要な影響に該当する可能性のある例として、企業の評判、顧客やベンダーとの関係、競争力毀損、訴訟または規制当局による調査もしくは処分の可能性を挙げています。監査委員会と取締役会は、経営陣が重要性の判断をおこなうための方針と手続を整備していることや、エスカレーションすべき重要なサイバーインシデントを特定し、経営陣による開示委員会や法務チームと協議する手順があり、重要性判断を文書化していることを確認する必要があります。

詳細は、下記リンクより英語全文をダウンロードしてください。

<https://boardleadership.kpmg.us/relevant-topics/articles/2023/sec-final-cybersecurity-rules-a-board-lens.html>

Contact us

John H. Rodi
Leader, KPMG Board
Leadership Center, KPMG US
T: 312-203-3732
E: jrodi@kpmg.com

Claudia H. Allen
Senior Advisor, KPMG Board
Leadership Center, KPMG US
T: 312-659-7407
E: claudiaallen@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia



経営陣による開示委員会の役割と構成

サイバーセキュリティに関する開示義務が拡大することを考えると、経営陣の開示委員会の人選、サイバーセキュリティ関連の開示統制・内部統制や手続を構築・維持する委員会の役割と責任について、再検討が必要になるかもしれません。サイバーインシデントが発生した場合に重要性を適時に判断するために委員会が必要とするのは、どんなリソースやプロセスでしょうか？

CEOとCFOが四半期ごとに開示統制 (内部統制を含む) や手続の整備・運用状況の有効性に関する宣誓している内容を裏付ける、補完的な宣誓プロセスの拡大

経営陣による開示委員会は、米国企業改革法 (SOX法) 第302条により要求されている内部統制・開示統制や手続の有効性と整備状況に関するCEO (最高経営責任者)とCFO (最高財務責任者)による四半期ごとの宣誓の裏付けをおこないます。開示委員会は通例、従業員からの内部統制に関する補完的な宣誓プロセスを維持し、CEOとCFOによる宣誓の裏付けに使用されています。企業に求められるサイバーセキュリティに関する開示の範囲が拡大し、詳細さも増すことを考えると、サイバーセキュリティ関連の補完的な宣誓を新たに得るうえで、補完的な宣誓プロセスを必要に応じて拡大することが求められます。

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS004907-1A