Legal Wire

pillsbury

Japan Practice

Vol. 45 / March 2018

米国証券取引委員会（SEC）、サイバーセキュリティの開示に関するガイダンスを再び発表

デビッド・M・ファーブッシュ、ブライアン・M・ウォン、デビッド・S・バクスター、エイリーン・モナハン

- 会社は、重要なサイバーセキュリティインシデントを正確かつ適時に開示する手続きを確立し、維持する必要があります。
- 会社は、サイバーセキュリティに関する未公表情報の誤用や一部のみの開示を防止する必要があります。

米国証券取引委員会（SEC）は 2018 年 2 月 21 日、SEC スタッフが 2011 年に発行したガイダンスをベースとして、サイバーセキュリティインシデントとリスクの開示義務に関する解釈を発表しました。

Securities Act や Exchange Act といった証券取引法に基づく開示要求条項は、いずれもサイバーセキュリティについて明示的に言及していませんが、上場会社が直面するサイバーセキュリティの脅威やリスクの性質からすると、様々な情報開示が今後必要となり得ます。サイバーセキュリティインシデントやリスクの重大性は、リスクの性質、程度、発生可能性、およびインシデントが引き起こす可能性がある損害の範囲（評判、財務実績、顧客やベンダーとの関係、訴訟や規制捜査の可能性を含む）によって左右されると SEC は述べています。サイバー攻撃には様々な形態があるため、サイバーセキュリティリスクについて以下の点を会社は考慮する必要があります。

- 修復・改善
- セキュリティや防止策
- 逸失利益
- 訴訟および規制リスク
- 顧客やビジネスパートナーとの関係維持
- 保険
- 評判に関するリスク
- 競争力

会社は、定型文や一般的な言葉を使わずに、開示手続きの策定を進めなければなりません。リスクを十分に記載したと言えるためには、サイバーセキュリティインシデントが発生する可能性があると述べるだけでなく、以前に発生したサイバーセキュリティインシデントの発生についても開示する必要があるかもしれません。しかし、SEC のガイダンスでは、システムの脆弱性をさらけ出すような

具体的な情報や技術的な情報を開示することまでは求めていません。さらに、SEC は、サイバー攻撃の性質上、「サイバーセキュリティインシデントの影響を把握するために時間を要することもある」ことを認識していますが、インシデントについて調査を進めていることは、インシデントの不開示や開示の遅れの理由にはならないとしています。また、開示内容が不正確なものとならないよう、サイバーセキュリティインシデントの調査の進展に伴い、会社は開示情報を更新する必要もあるかもしれません。

会社は、「有価証券の売却に先立ち、十分に前もって」「正確かつ適時な」開示を行うことが期待されています。そのため、会社は、有価証券の売買に際して、投資判断に必要な範囲でサイバーセキュリティインシデントに関する情報が十分開示されていることに留意する必要があります。SEC の指針に照らし、上場予定の会社は、引受人が行うサイバーセキュリティリスクに関するデューディリジェンスがより厳格になること、引受契約により広範な表明保証条項が求められる可能性があるなど、より注意を払う必要があります。

SEC は、会社が定期的な報告書の中でサイバーセキュリティインシデントおよびリスクに関してどのような情報を開示しなければならないかを明示することによって、2011 年に SEC スタッフが発行したガイダンスを再確認しました。

該当項目	根拠条項	報告するべき事項（主要な場合）
Form 8-K	Items 1.0.1, 7.01 and 8.01 of Form 8-K	サイバーセキュリティインシデントの発生とその影響の即時報告
Risk Factors	Item 503(c) of Regulation S-K	会社は、リスクファクターとして、過去または進行中のインシデントを開示しなければならない場合がある。
MD&A	Item 303 of Regulation S-K	対策費用、防止に向けた取組み、インシデントが生じた際に要するコスト（対応努力、資産の喪失および修復を含む。）の傾向
Description of Business	Item 101 of Regulation S-K	会社の製品、サービス、顧客またはサプライヤーとの関係、または競争条件に対する重大な影響
Legal Proceedings	Item 103 of Regulation S-K	サイバーインシデントに関する係属中の法的手続きのうち重大なもの（例えば、顧客の個人情報の喪失に関するもの。）
Financial Statements	Item 301 of Regulation S-K	会社の財務諸表への影響（サイバーインシデントへの対応費用、顧客維持努力、補償、追加資金調達費用、収益悪化を含む。）
Board Risk Oversight	Item 407 (h) of Regulation S-K and Item 7 of Schedule 14A	取締役会のリスク監理の役割（サイバーセキュリティリスク管理プログラムを含む。）

この新しい発表は、特に下記の 2 つの分野において、2011 年のガイダンスの解釈を拡大しています。第一に、サイバーセキュリティの開示コントロールと手続きの重要性を強調しています。第二に、

サイバー脅威やインシデントに関する重要な未公表情報の使用がインサイダー取引にあたる可能性があることを繰り返し強調しています。会社は、いずれの分野においても、SEC 執行部門による厳重な監視を受けると考えておくべきでしょう。

開示手続き

Exchange Act Rules 13a-15 および 15d-15 は、会社に対して、公開する必要のある情報を取得・記録するだけでなく、かかる情報を適時に経営陣に伝達する仕組みを維持することを求めています。会社は、サイバーセキュリティインシデントとリスクを特定し、ビジネスへの影響やその重要性を評価・分析し、技術専門家や開示アドバイザーとオープンなコミュニケーションを行ったうえで、インシデントやリスクについて適時開示を行える必要があります。これは、インシデントやリスクを適時に評価して経営陣に報告できるよう、インシデントの評価をリアルタイムで行う新しいプロセスを開発することも意味するのかもしれません。

こうしたプロセスには、サイバーセキュリティのインシデントとリスクを特定し、その影響を評価し、適切かつタイムリーな方法でかかる問題を開示し、さらには必要に応じて、これまでの開示を修正またはアップデートすることも組み込まれていることとなります。

インサイダー取引

新しいガイダンスでは、インサイダー取引に関連する SEC のサイバーセキュリティへの関心も強調されています。SEC は、「会社のサイバーセキュリティインシデントとリスクに関する情報は、重大な未公表情報となる可能性があり、取締役、役員およびその他の会社関係者が未公表情報を保有する間に信任義務や守秘義務に反して会社の証券を取引した場合、不正行為防止規定に違反する。」と明確に述べています。ガイダンスでは、会社に対して、社内倫理規定を見直し、会社関係者が非公表のサイバーセキュリティ問題を認識する場合には取引の禁止も考慮すると明記することを推奨しています。新しいガイダンスは、同様に、サイバー関連問題に伴って不適切な取引が発生しないような対策を検討することも会社に推奨しています。

取締役会のリスク監視

新しいガイダンスは、「取締役会がどのように監視機能を果たすのか、その監視機能が取締役会のリーダシップにおいてどのような効果があるかなど、取締役会のリスク監視の役割の範囲を開示することを会社に求める。」と規定しています。さらに、ガイダンスには「会社のサイバーセキュリティリスク管理プログラムやサイバーセキュリティ問題に関する取締役会の経営陣との取組みを開示することによって、取締役会がそのリスク監視責任をどのように果たしているのかについて、投資家がこれを評価する機会となる」という SEC の見解が記載されています。

本稿の原文（英文）につきましては、Déjà Vu All Over Again: SEC Provides Cybersecurity Guidance をご参照ください。また関連する右記の投稿についてもご参照ください。SEC Guidance Affirms Need for Board Oversight of Cybersecurity Risks

サイバーセキュリティに関するその他の情報については、Pillsbury の Cybersecurity and the Law のウェブサイト（英文）をご覧ください。

本稿の内容に関する連絡先

木本泰介（日本語版監修）
725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
213.488.7113
taisuke.kimoto@pillsburylaw.com

Brian M. Wong
Four Embarcadero Center, 22nd Floor
San Francisco, CA 94111-5998
415.983.6372
brian.wong@pillsburylaw.com

今井　千鶴（日本語版作成協力）

David S. Baxter
1540 Broadway
New York, NY 10036-4039
212.858.1222
david.baxter@pillsburylaw.com

David M. Furbush
2550 Hanover Street
Palo Alto, CA 94304-1115
650.233.4623
david.furbush@pillsburylaw.com

Eileen Monahan
1540 Broadway
New York, NY 10036-4039
212.858.1232
eileen.monahan@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com