サイバーセキュリティに関わるSECの開示規則案
－広範囲に及ぶインシデントの懸念と情報開示－

板津　直孝

▌要　約▐

1. デジタル技術と電子通信を通じた国際的な経済活動においては、サイバーセキュリティ・インシデントが、企業の財務やインフラに継続的かつ拡大するリスクをもたらしている。
2. 米国のバイデン大統領は、2022年3月、「重要インフラに関するサイバーインシデント報告法（CIRCIA）」に署名し、サイバーセキュリティ・社会基盤安全保障庁（CISA）によって定められた米国の重要インフラ事業者に対して、重要なサイバーセキュリティ・インシデントが発生した場合は72時間以内に、ランサムウェア攻撃による身代金の支払を行った場合は24時間以内にCISAに報告することを義務付けた。
3. CISAの動向と並行して米国証券取引委員会（SEC）は、2022年3月、「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、及びインシデントの開示」の強化及び標準化のための規則案を公表した。同規則案では、サイバーセキュリティ・インシデントの財務的影響の範囲と大きさに関する情報が入手可能になった際に、その情報が適時に財務諸表に組み込まれる合理的な保証を提供できるように、企業が財務報告及びリスク管理システムを設計することを要請している。
4. 日本でも、海外からのサイバー攻撃が増加している。日本企業においても、サイバーセキュリティのリスクが企業の財務に及ぼす影響について、SECの開示規則案も参考にしつつ、非財務情報と財務情報の連動性を考慮して、有価証券報告書等において開示を検討することが重要であると言える。

野村資本市場研究所　関連論文等

・板津直孝「データローカライゼーション規制とデジタル経済の分断－強化される越境データの流通制限－」『野村資本市場クォータリー』2021年秋号。

Ⅰ　サイバーセキュリティ・インシデントとコストの現状

１．サイバーセキュリティの脅威とインシデント

デジタル技術と電子通信を通じた国際的な経済活動においては、サイバーセキュリティの脅威とインシデントが、企業や投資家及びその他の金融資本市場参加者に継続的かつ拡大するリスクをもたらしている。サイバーセキュリティのリスクは、新型コロナウイルス感染症（COVID-19）の蔓延を切っ掛けとしたリモートワークの普及、デジタル決済の拡大、クラウドサービスへの依存度の高まりなど、企業による業務のデジタル化を含むさまざまな要因で増加している。

コンピューターやその利用者に被害をもたらすことを目的とした、悪意のあるソフトウェアであるマルウェアは、個人情報や機密情報を侵害し、ネットワークで繋がっているデバイスなどに感染し拡大する。膨大な数のマルウェアが日々生成されており、代表的なものとしては、暗号化などによってファイルを利用不能な状態にし、元に戻すことと引き換えに金銭を要求するランサムウェアなどがある。

ランサムウェアなどによるサイバー攻撃の影響は、あらゆる規模の企業、重要なインフラ、医療など、広範囲に及んでいる（図表 1）。

サイバー攻撃を実行する犯罪者が高度な手法を使用するようになり、サイバーセキュリティ・インシデントが企業の財務に重要な影響を及ぼす可能性が高まっている。サイバーセキュリティ・インシデントとは、企業の情報システム又はその中に存在する情報の機密

図表 1　広範囲に及ぶサイバー攻撃の影響の事例

● 米国最大の燃料パイプライン運営会社は、2021 年 5 月、にランサムウェアによるサイバー攻撃を受け、米国東海岸の燃料供給のほぼ半分の供給源である同社のネットワーク全体を閉鎖した[1]。
● 米国の医療システムを標的としたランサムウェア攻撃が 2016 年から 2021 年にかけて 2 倍以上に増え、必要とされる医療の提供が妨害されるとともに、何百万人もの個人の医療情報が流出した[2]。
● ギリシャの国営郵便サービス企業は、2022 年 3 月、ランサムウェアによるサイバー攻撃を受け、郵便サービスや金融取引の処理などが全国的に停止した[3]。
● コスタリカは、数十件のサイバー攻撃の標的にされ、約 1,200 の病院と診療所が影響を受け、対外貿易と徴税業務の一部が凍結され、ロドリゴ・チャベス大統領は就任式の 2022 年 5 月に国家非常事態宣言をした[4]。
● インドの大手航空会社は、2022 年 5 月、ランサムウェアによるサイバー攻撃を受け、フライトの遅延や欠航が発生し、多くの乗客が影響を受けた[5]。

（出所）各種資料より野村資本市場研究所作成

1 “Cyber-attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed,” *Reuters*, May 8, 2021.
2 University of Minnesota, “Ransomware attacks on America’s health care systems more than doubled from 2016 to 2021, exposing the personal health information of millions,” January 17, 2023.
3 “Greece’s national postal service restoring systems after ransomware attack,” *The Record*, March 24, 2022.
4 “Latest cyberattack in Costa Rica targets hospital system,” *Reuters*, June 1, 2022.
5 “SpiceJet: Passengers stranded as India airline hit by ransomware attack,” *BBC*, May 25, 2022.

性、完全性及び可用性を危険にさらす、当該情報システムへの、又は当該情報システムを通じて行われた、正当な権限を付与されていない事象の発生を言う。

２．インシデントに起因するコストと損害の現状

重要なサイバーセキュリティ・インシデントに起因するコストと損害は、広範囲に及ぶ。米国では、中小企業が特に深刻なサイバーセキュリティ攻撃の標的となっており、その結果、多くの中小企業が廃業に追い込まれている[6]。これらの直接的及び間接的なコストは、短期的及び長期的な株主価値や株価にも悪影響を及ぼす可能性がある。

サイバーセキュリティ・インシデントに関連するコストは上昇しており、その割合は増加している。サイバーセキュリティ・インシデントの結果として、企業が被る可能性のあるコストと悪影響には、以下が含まれる（図表 2）。

IBM セキュリティは、2022 年 7 月、「データ侵害のコストに関する報告書 2022 年」を公表した[7]。同報告書は、米国の調査組織であるポネモン・インスティテュート（Ponemon Institute）が、2021 年 3 月から 2022 年 3 月までに、17 の国と地域で発生したデータ侵害の影響を受けた 550 社を調査し、データ侵害の発生後に増加し続けるコストについて、IBM セキュリティがスポンサーとなり分析したものである（図表 3）。

同調査結果では、米国は 12 年連続でデータ侵害の平均コストが最も高額となっている。米国のサイバーセキュリティ・社会基盤安全保障庁（CISA）は、ランサムウェアを含むサイバー攻撃の増加は、米国が直面する最も深刻な経済的及び国家安全保障上の脅威のひとつであるとしている。

図表 2　企業が被る可能性のあるコストと悪影響

● 事業の中断、生産量の減少、製品の発売遅延によるコスト
● 恐喝に応じた支払い
● 情報漏洩の責任、システム損傷の修復、サイバー攻撃後に関係を維持するための顧客又はビジネスパートナーへのインセンティブなどの修復コスト
● 保険料の見直し、組織変更のコスト、追加人員と保護技術の展開、従業員のトレーニング、専門家やコンサルタントの関与などにより増加する、サイバーセキュリティ保護コスト
● 知的財産の侵害、機密情報の不正利用、サイバー攻撃後の顧客離れに起因する減収
● 当局による規制措置などによる訴訟及び法的リスク
● 従業員及び顧客への危害、プライバシー法の違反、及び顧客又は投資家の信頼に悪影響を及ぼす風評被害
● 企業の競争力、株価、及び長期的な株主価値への打撃

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

6 National Cybersecurity Institute, “Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks,” April 22, 2015.

7 IBM Security, “Cost of a Data Breach Report 2022,” July 2022.

図表 3　データ侵害のコストに関する報告書の概要

435 万ドル（データ侵害の平均総コスト）
2022 年のデータ侵害によって発生した平均コストは 435 万ドルで、2020 年の 386 万ドルから 12.7%上昇し、過去最高額に達した。
83%（データ侵害の件数が 2 件以上の組織の割合）
調査対象組織の 83%で 2 件以上のデータ侵害が発生し、調査対象組織の 60%でデータ侵害が原因でサービスや製品の値上げを実施した。
482 万ドル（重要インフラ組織のデータ侵害の平均コスト）
調査した重要インフラ組織のデータ侵害の平均コストは、その他の業界の平均コストよりも 100 万ドル多い、482 万ドルであった。
305 万ドル（セキュリティに AI と自動化を全面的に導入している組織のコストの節減額）
セキュリティに AI と自動化を全面的に導入している組織のデータ侵害の平均コスト（315 万ドル）は、未導入の組織の平均コスト（620 万ドル）よりも、305 万ドル少ない金額になった。
454 万ドル（身代金を除いたランサムウェア攻撃の平均コスト）
本調査ではデータ侵害の 11%がランサムウェア攻撃によるもので、データ侵害の全般的な平均総コストの 435 万ドルよりも若干高い。
45%（クラウドで発生したデータ侵害の割合）
本調査において、データ侵害の 45%はクラウド内で発生した。
12 年（医療業界が平均データ侵害コストの最高額を記録し続けている年数）
医療業界は 12 年連続で最もデータ侵害コストが高額な業界であり、そのコストは、2020 年比で 41.6%増加している。金融の平均コストは 597 万ドルで医療の次に高額で、これに製薬の 501 万ドル、テクノロジーの 497 万ドル、エネルギーの 472 万ドルが続く。
944 万ドル（世界で最も高額な米国の平均データ侵害コスト）
データ侵害の平均コストが高額な上位 5 つの国と地域は、米国（944 万ドル）、中東（746 万ドル）、カナダ（564 万ドル）、英国（505 万ドル）、ドイツ（485 万ドル）であった。

（注）　重要インフラ組織：金融サービス、製造、テクノロジー、エネルギー、運輸、通信、医療、教育等の業界に属する組織。

（出所）IBM Security, “Cost of a Data Breach Report 2022,” July 2022 より野村資本市場研究所作成

バイデン大統領は、2022 年 3 月、「重要インフラに関するサイバーインシデント報告法（CIRCIA）」[8]に署名し、CISA の規則によって定められた米国の重要インフラ事業者に対して、重要なサイバーセキュリティ・インシデントが発生した場合は 72 時間以内に、ランサムウェア攻撃による身代金の支払を行った場合は 24 時間以内に、CISA に報告することを義務付けた。これらの報告により、CISA はリソースを迅速に展開してサイバー攻撃を受けた被害者を支援し、新たな脅威と傾向を特定しネットワーク防御者と情報を共有

[8] CISA, “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), FACT SHEET,” March 15, 2022.

して保護措置を講じ、他の潜在的な被害者に警告を発することができるようになる。

CISA の動向と並行して米国証券取引委員会（SEC）は、2022 年 3 月、「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、及びインシデントの開示」の強化及び標準化するための規則案を公表した[9]。サイバーセキュリティのリスクとインシデントは、企業の財務に重要な影響を与える可能性がある。同規則案は、SEC 登録企業のサイバーセキュリティに関するリスク管理、戦略、ガバナンスについて投資家により良い情報を提供し、重要なサイバーセキュリティ・インシデントをタイムリーに報告することを目的としている。

Ⅱ 重要性のあるインシデントの適時及び定期開示

SEC の規則案では、重要性のあるサイバーセキュリティ・インシデントについて、SEC 登録企業に適時及び定期的な報告を要請している。

1．重要なインシデントが発生した場合の適時開示

SEC 登録企業のうち米国内の発行体は、サイバーセキュリティ・インシデントが発生し、当該インシデントが重要であると判断した場合、当該判断を行った日から 4 営業日以内に、国内公開企業向けの臨時報告書（Form 8-K）を提出することが求められる。

具体的には、米国内の発行体は、重要なサイバーセキュリティ・インシデントに関する以下の情報を臨時報告書で開示する（図表 4）。

臨時報告書は、投資家やその他の市場参加者にタイムリーかつ関連性のある情報を提供し、長期的及び短期的な財務への影響など、重要なサイバーセキュリティ・インシデントが企業に及ぼす可能性のある影響を評価する上で有用である。

臨時報告書での開示を、インシデントの発生日ではなく、インシデントが重要であると判断した日から 4 営業日以内と定めていることにより、企業の重要性の判断日がインシデ

図表 4　米国内の発行体における臨時報告の概要

● インシデントが発生した時期及び現在進行中か。
● インシデントの性質及び範囲に関する簡単な説明。
● データが盗難、改ざん、アクセス、又はその他の不正な目的で使用されたか否か。
● インシデントが SEC 登録企業の業務に及ぼす影響。
● SEC 登録企業がインシデントを修復したか、又は現在修復中か。

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

9 SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022.

図表 5　外国民間発行体における臨時報告の概要

● 本国の法令に基づいて開示した、又は開示することが要請される情報
● 証券取引所の規則に基づいて開示した、又は開示することが要請される情報
● 証券保有者に対して配布した情報

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

ントの発生日と重なる場合もあれば、発生日より後に重要性判定が行われる場合もある。開示義務を回避するために、一部の企業が判断を遅らせる可能性があることから、企業はインシデントに関する重要性の判断を、インシデントの発生後合理的に実行可能な限り速やかに行わなければならないとしている。

インシデントの適時開示における重要性については、投資の意思決定を下す際に合理的な株主が重要であると考える可能性が相当に高い場合、又は利用可能な情報の全体を大幅に変更する可能性がある場合、情報は重要であるとしている。

外国民間発行体に対しては、上記と同様の臨時報告義務はないが、以下の全てのサイバーセキュリティ・インシデントに関わる情報のコピーを、外国公開企業向けの臨時報告書（Form 6-K）で提出することが求められる（図表 5）。

２．定期報告によるインシデントの開示

企業は、サイバーセキュリティ・インシデントが重要であると判断した時点では、完全な情報を得ていない可能性があることから、臨時報告書による適時開示に加えて、定期報告によるインシデントの開示が求められる。

SEC 登録企業のうち米国内の発行体は、四半期報告書（Form 10-Q）又は年次報告書（Form 10-K）において、以前に提出した臨時報告書の情報更新と、全体で重要となったインシデントの開示が要請される（図表 6）。

全体で重要となったインシデントは、概念的にはさまざまな形態をとる可能性があるが、一例として、悪意のある同一人物が、同じ企業に対して、時間的にも形態的にも関連する多数の小規模ではあるが継続的なサイバー攻撃を行うケースがある。個別では重要性の低いインシデントであるが、全体として量的にも質的にも重要であるか、又はその両方であ

図表 6　米国内の発行体における定期報告の概要

● 以前に提出した臨時報告書の情報の重要な変更、追加、又は更新を、重要な変更、追加、又は更新が発生した期間における四半期又は年次報告書で開示する。
● 個別に開示されていなかった重要性の低いインシデントが、全体として重要になった場合、臨時報告書と同様の開示要件を四半期又は年次報告書で開示する。

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

図表 7　外国民間発行体における定期報告の概要

● 以前に提出した臨時報告書の情報の重要な変更、追加、又は更新を、重要な変更、追加、又は更新が発生した期間における年次報告書で開示する。
● 報告期間中に発生した非公開の重要なサイバーセキュリティ・インシデントに関する情報を、年次報告書で開示する。

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

る場合がある。このようなインシデントは、企業が全体として重要であると判断した期間の定期報告で開示されることになる。

SEC 登録企業のうち外国民間発行体は、年次報告書（Form 20-F）において、以前に提出した臨時報告書の情報更新と、報告期間中に発生した非公開の重要なサイバーセキュリティ・インシデントに関する情報開示が要請される（図表 7）。

外国民間発行体に臨時報告書で開示が求められるインシデントは限られているため、報告期間中に発生した非公開の重要なインシデントに関する情報開示が求められている。

Ⅲ リスク管理、戦略及びガバナンスの年次報告書での開示

SECの規則案では、より一貫性のある情報開示をSEC登録企業に求めるために、レギュレーション S-K（非財務情報）において新たな開示項目を定め、サイバーセキュリティのリスク管理と戦略の開示、ガバナンスの開示、及びサイバーセキュリティの専門性を有する取締役の有無に関する開示を要請している。

１．リスク管理と戦略の開示

企業は、リスクを特定し、評価し、管理するための方針と手順を含むリスク管理システムを開発することによって、自社の事業に対する重大なリスクに対処する。

SECの規則案は、サイバーセキュリティのリスクが事業戦略に与える影響を含め、知的財産の盗難、詐欺、恐喝、従業員又は顧客への危害、プライバシー法の違反、その他の訴訟及び法的リスクなどの、サイバーセキュリティのリスクを特定し管理するための方針と手順について、年次報告書での情報開示を要請している。

具体的には、該当する場合、リスク管理と戦略の開示が求められる（図表 8）。

図表 8　リスク管理と戦略の開示の概要

● サイバーセキュリティのリスク評価プログラムの有無、及び該当する場合はその内容
● サイバーセキュリティのリスク評価プログラムに関与する、外部の評価者、コンサルタント、監査人又はその他の第三者の有無
● 外部のサービスプロバイダー（顧客及び従業員のデータにアクセスできるプロバイダーなどを含む）の利用に伴うサイバーセキュリティのリスクの監督及び識別の方針及び手順の有無、プロバイダーの選択と監視、プロバイダーに関連するサイバーセキュリティのリスクを軽減するための契約やその他のメカニズムがサイバーセキュリティの考慮事項に与える影響の有無、及び該当する場合はその内容
● サイバーセキュリティ・インシデントを防止し、検出し、影響を最小化するための活動の有無
● サイバーセキュリティ・インシデントに対する事業継続計画（BCP）の有無
● 過去のサイバーセキュリティ・インシデントにより生じた、ガバナンス、方針、手順又は技術に関する変更の有無
● 経営成績又は財政状態に影響を与えた、又は与える合理的可能性があるサイバーセキュリティ関連のリスク及びインシデントの有無、及び該当する場合はその内容
● 事業戦略、財務計画及び資本配分の一部として考慮されたサイバーセキュリティのリスクの有無、及び該当する場合はその内容

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

2．ガバナンスの開示

SEC の規則案では、サイバーセキュリティのリスクに関するガバナンスの情報開示として、SEC 登録企業に対して、取締役会によるサイバーセキュリティのリスクの監視、及びサイバーセキュリティのリスクの評価と管理に関する経営陣の役割について、年次報告書での開示を要請している。

具体的には、取締役会によるサイバーセキュリティのリスクの監視について、以下の開示が求められる（図表 9）。

図表 9　取締役会によるサイバーセキュリティのリスクの監視

● 取締役会全体、特定の取締役又は委員会のいずれが、サイバーセキュリティのリスクの監視に責任を負っているか否か。
● サイバーセキュリティのリスクについて取締役会に報告されるプロセス、及び審議の頻度。
● 取締役会又は委員会が、サイバーセキュリティのリスクを事業戦略、リスク管理、及び予算管理の一部として考慮しているか否か、及びその方法。

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

図表 10　サイバーセキュリティのリスクの評価と管理に関する経営陣の役割

● 特定の管理職又は委員会が、サイバーセキュリティのリスクの測定と管理、特にサイバーセキュリティ・インシデントの予防、軽減、検出、修復に責任を負っているか否か、及び当該立場の者又は構成員の関連する専門知識。
● 指定された最高情報セキュリティ責任者（CISO）又は同等の地位にある者を有しているか否か、該当する場合は組織図の中で当該立場の者が誰に報告しているか、及び当該立場の者の関連する専門知識。
● 当該立場の者又は委員会が、サイバーセキュリティ・インシデントの予防、軽減、検出、修復について通知され、監視するプロセス。
● 当該立場の者又は委員会が、サイバーセキュリティのリスクについて取締役会又は取締役で構成される委員会に報告しているか否か、及びその頻度。

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

サイバーセキュリティのリスクの監視に関する取締役会の役割を開示することで、サイバーセキュリティの問題について取締役会がどのように経営陣に関与し、リスク監視の責任を果たしているかを、投資家が理解することができるようになる。

サイバーセキュリティのリスクに対する経営陣の役割については、サイバーセキュリティのリスクの評価と管理、サイバーセキュリティの方針、手順、戦略の実施における経営陣の役割を具体的に開示することが求められる（図表 10）。

３．専門性を有する取締役の有無に関する開示

サイバーセキュリティのリスクやインシデントは、企業にとって脅威であることから、サイバーセキュリティはすでに多くの取締役会の最優先事項のひとつとなっている。したがって投資家にとっては、企業への投資及び取締役の選出に関する議決権行使を検討する際に、取締役会の構成員がサイバーセキュリティの専門性を有しているか否かの情報が重要となっている。サイバーセキュリティの専門性は、さまざまな経験、スキル、及びタスクをカバーする可能性がある。

SEC は、サイバーセキュリティの専門性を有している取締役の選任を義務付けてはいないが、取締役会の構成員が専門性を有している場合、SEC 登録企業に対して、当該取締役の氏名及び専門性の詳細を情報開示することを求めている。米国内の発行体は、委任状又は情報説明書[10]、及び年次報告書において、外国民間発行体は、年次報告書において、当該情報を開示することが求められる。

SEC の規則案では、サイバーセキュリティの専門性を構成する定義を定めていないが、取締役がサイバーセキュリティの専門性を有しているか否かを判断する際に、企業が考慮すべき包括的な基準を示している（図表 11）。

[10] 議決権の代理行使の勧誘を行う委任状勧誘を行わない場合に、勧誘が行われた場合送付することが必要とされている情報に実質的に等しい情報を提供する書類（1934 年証券取引所法第 14 条(c)）。

図表 11　サイバーセキュリティの専門性に関する包括的な基準

● 取締役は、情報セキュリティ責任者、セキュリティポリシーアナリスト、セキュリティ監査人、セキュリティアーキテクト又はエンジニア、セキュリティオペレーション又はインシデント対応マネージャー、BCP 立案者としての経験を含む、サイバーセキュリティの実務経験を有しているか。
● 取締役は、サイバーセキュリティに関する資格又は学位を取得しているか。
● 取締役は、セキュリティポリシー及びガバナンス、リスク管理、セキュリティ評価、統制評価、セキュリティアーキテクチャ及びエンジニアリング、セキュリティ運用、インシデント対応、BCP の分野を含む、サイバーセキュリティに関する知識、スキル、又はその他のバックグラウンドを有しているか。

（出所）SEC, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,” March 9, 2022 より野村資本市場研究所作成

サイバーセキュリティの専門性を有していると判断された取締役は、1933 年証券法第 11 条「登録届出書の虚偽記載に関する民事責任」に関するセーフハーバーが定められている。これにより、取締役会の構成員として課されるよりも大きな職務、義務及び責任を、当該取締役に課さないことを明確にしている。なお、サイバーセキュリティの専門性を有する取締役を選任することで、他の取締役会の構成員の職務、義務及び責任が軽減されることもない。

Ⅳ サプライチェーン攻撃に対するリスクと日本への示唆

近年、企業の事業におけるサプライチェーンの繋がりを利用したサイバー攻撃による被害が、国際的に増加している。一般に、セキュリティレベルの高い標的企業に対しては侵入が難しい。そこで比較的セキュリティレベルの低い標的企業の子会社や取引先などを侵害し経由することで、業務上の繋がりを利用して標的企業への攻撃を可能にするのが、ビジネス環境を悪用するサプライチェーン攻撃である。最終的に標的となる企業は、グループ会社などを足掛かりに侵入され、サプライチェーンを介して攻撃されるため、当初の侵入段階で感知することが非常に困難となっている。

サプライチェーン攻撃により、必要な部品や材料がすぐに調達できなくなり、製造工程に遅延や停止が発生する可能性がある。また、サプライチェーン内部でサイバー攻撃の被害が発生すると、生産が停止する可能性がある。

ひとつの事例を挙げると、日本の大手自動車企業の主要サプライヤーの 1 社であるプレス企業は、2022 年 3 月、マルウェアによるサイバー攻撃の被害を公表した。サプライチェーンを支える 1 社へのサイバー攻撃により、同自動車企業の 14 カ所の工場の 28 ラインが止まり、約 1 万 3,000 台の自動車の生産が見送られ、グループの自動車会社 2 社においても、一部の生産を見合わせることとなった[11]。同事案は、サプライチェーン攻撃のリ

[11] 「トヨタの工場を止めたサイバー攻撃　サプライチェーン攻撃のリスクが露呈」『日経クロステック』2022 年 3 月 14 日。

スクと影響の大きさを、日本社会に知らしめたと言える。

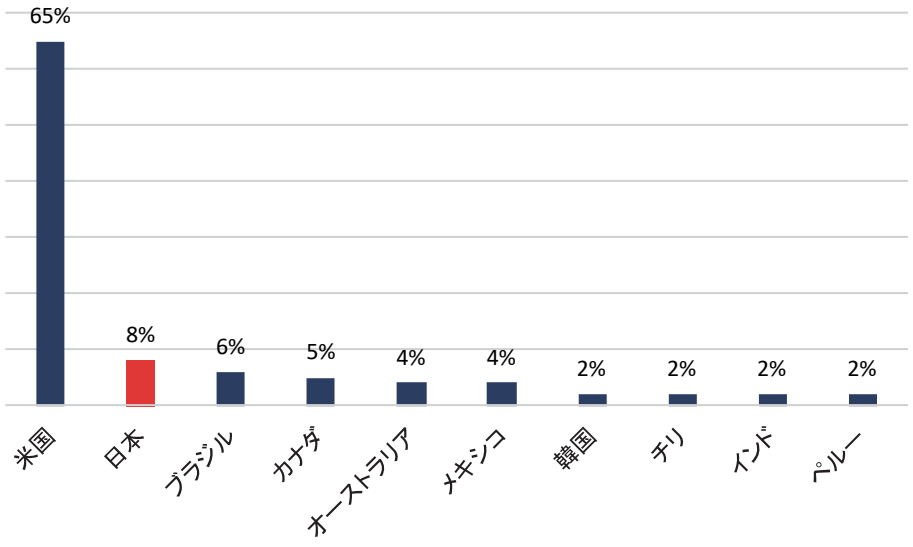
日本では、海外からのサイバー攻撃が増加している。ブラックベリーが、2023 年 1 月に公表した「グローバル脅威インテリジェンスレポート」[12]によれば、日本が米国に次いでサイバー攻撃の対象になっている（図表 12）。

日本においても、企業グループにおけるサイバーセキュリティに対する取り組みについて、「サイバーセキュリティ報告書」として透明性のある開示が行われ始めている。サプライチェーン攻撃のリスクが増大している事業環境においては、ステークホルダーからの信頼性を高めるため、そのような開示が有用な可能性がある。

経済産業省の「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティのリスクに対しては、「経営者が認識すべき 3 原則」のひとつとして、自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきであるとしている[13]。そして、サイバーセキュリティ対策の状況について、サイバーセキュリティのリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや有価証券報告書等への記載を通じて開示を検討することが重要であるとしている。

総務省では、サイバーセキュリティ・タスクフォースの下に「情報開示分科会」を開催し、同分科会において、企業のセキュリティ対策の情報開示に関する課題を整理し、企業におけるサイバーセキュリティ対策の情報開示を促進するために必要な方策等について検討を行った。総務省は、同検討結果を踏まえ、企業にとって参考となり得る情報開示の実

図表 12　サイバー攻撃の多い上位 10 か国の攻撃数の割合



（注）　サイバー攻撃の割合は、2022 年 9 月から 11 月の間に、Cylance Endpoint Security Solutions が未然に防御したサイバー攻撃の数が最も多かった 10 か国を示したもの。
（出所）BlackBerry, “Global Threat Intelligence Report,” January 2023 より野村資本市場研究所作成

[12] BlackBerry, “Global Threat Intelligence Report,” January 2023.
[13] 経済産業省「サイバーセキュリティ経営ガイドライン Ver 2.0」2017 年 11 月 16 日。

例等をまとめた「サイバーセキュリティ対策情報開示の手引き」を公表した[14]。同手引きでは、企業において実施されることが望まれるサイバーセキュリティ対策のひとつとして、監査の実施や対策状況の把握を含むサイバーセキュリティ対策の取り組みについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用を実施し、システム管理等の委託について、自社組織で対応する部分と外部に委託する部分で適切な切り分けをすることを推奨している。

米国のサイバーセキュリティに関わる SEC の開示規則案では、サイバーセキュリティ・インシデントの財務的影響の範囲と大きさに関する情報が入手可能になったときに、その情報が適時に財務諸表に組み込まれる合理的な保証を提供できるように、企業が財務報告及びリスク管理システムを設計することを要請している。日本企業においても、サイバーセキュリティのリスクが企業の財務に及ぼす影響について、SEC の開示規則案も参考にしつつ、非財務情報と財務情報の連動性を考慮して、有価証券報告書等において開示を検討することが重要であると言える。企業が、サイバーセキュリティのリスク管理、戦略及びガバナンスを整備し情報開示することにより、重要なインシデントが発生した場合の適時開示が速やかに行われ、企業の取り組みが顧客や投資家などのステークホルダーから適正に評価される。

[14] 総務省「サイバーセキュリティ対策情報開示の手引き」2019 年 6 月。