サイバーセキュリティの概念と世界及び日本の現状

江夏　あかね

▌要　約▐

1. 世界では、2010 年代後半頃から、デジタル・トランスフォーメーション（DX）の推進、人工知能（AI）の発展、サイバー攻撃者の多様化も背景に、サイバー攻撃が複雑化、巧妙化、甚大化し、直接的な攻撃対象である企業等に被害が及ぶのみならず、社会経済全体に及ぼす影響が懸念されている。日本でもサイバー攻撃が年々増加しており、特に 2022 年 4 月に施行された改正個人情報保護法により、被害者本人への通知が必要となり、公表されるケースが増加しているようだ。
2. 金融資本市場の観点からは、（1）2019 年 3 月にサイバー攻撃を受けたものの、情報開示も背景に対応が好意的に受け止められたノルウェーのノルスクハイドロ、（2）2020 年 12 月にサイバー攻撃を受けたことを公表し、その後 2023 年 11 月に米国証券取引委員会（SEC）により提訴されたほか、SBOM（Software Bill of Materials）という概念の広がりのきっかけとなった、米国のソーラーウィンズ、の事例が注目される。
3. 今後も世界的にサイバー攻撃に伴うリスクの拡大傾向が続くと想定されるが、その勢いや内容を見据える場合、主に、（1）AI の進展に伴うサイバーリスクとセキュリティへの影響、（2）地政学リスクの状況、（3）人材確保・育成、が注目点になり得ると言える。特に、サイバーセキュリティに関する人材の観点からは、外部人材の採用が難しい現状を踏まえると、当面においては、企業内部での育成強化のみならず、企業間連携、政府や業界団体等による支援等も、企業のサイバーリスク軽減の観点からカギになると考えられる。

野村資本市場研究所　関連論文等

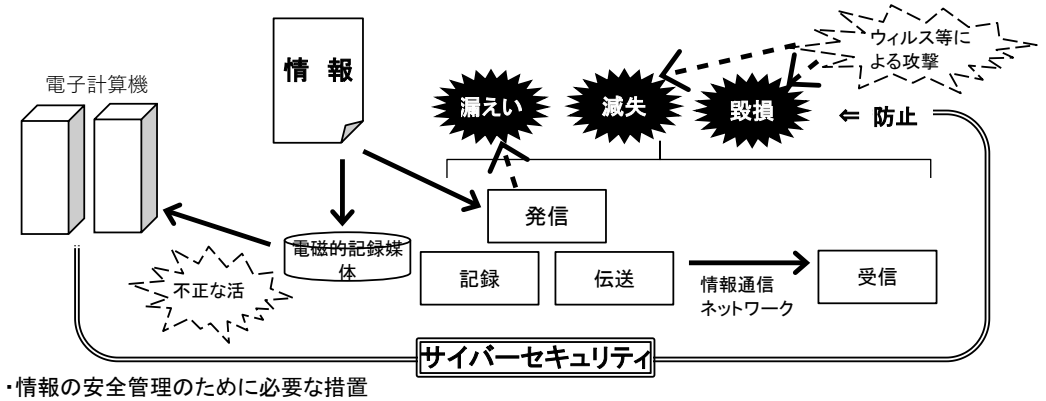
・江夏あかね「機関投資家から見たサイバーセキュリティーサステナブルな情報化社会実現に向けた論点整理ー」『野村サステナビリティクォータリー』第 3 巻第 4 号（2022 年秋号）。
・江夏あかね「サイバーセキュリティと企業価値ー投資家による評価と効果的な情報開示ー」『野村サステナビリティクォータリー』第 5 巻第 2 号（2024 年春号）。

Ⅰ 情報化社会の進展で重要性が増すサイバーセキュリティ

世界では、情報通信技術やサービスが 1990 年代終盤頃から急速に発展し、情報化社会、すなわち、情報の生産・収集・伝達・処理を中心として社会経済が発展していく社会[1]へと変貌を遂げている。その一方で、2010 年代後半頃から、デジタル・トランスフォーメーション（DX）[2]の推進、人工知能（AI）[3]の発展、サイバー攻撃者の多様化も背景に、サイバー攻撃が複雑化、巧妙化、甚大化し、直接的な攻撃対象である企業等に被害が及ぶのみならず、社会経済全体に及ぼす影響が懸念されている[4]。そのような中、情報化社会の安全性、持続可能性を維持すべく、サイバーセキュリティの重要性がますます高まっている（図表 1 参照）。

本稿では、サイバーセキュリティの概念を整理した上で世界及び日本のサイバー攻撃[5]の現状についてサイバー攻撃を受けた企業事例も含めて概観し、今後の注目点を考察する。

図表 1　サイバーセキュリティ（イメージ）



・情報の安全管理のために必要な措置
・情報システム及び情報通信ネットワークの安全性及び信頼性確保のために必要な措置
（電磁的記録媒体を通じた電子計算機に対する不正な活動による被害防止のために必要な措置を含む）
・適切な維持管理

（出所）羽室英太郎『サイバーセキュリティ入門－図解×Q&A』慶應義塾大学出版会、2018 年

1 情報化社会には、様々な定義があるが、例えば、デジタル大辞泉では、「物や資本などにかわって知識や情報に価値が置かれ、情報の生産・収集・伝達・処理を中心として社会・経済が発展していく社会。情報社会」と定義している（小学館『デジタル大辞泉』）。

2 経済産業省は、DX を「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」と定義付けている（経済産業省「デジタルガバナンス・コード 2.0」2022 年 9 月 13 日）。

3 総務省及び経済産業省は、AI を「AI システム（活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム）自体又は機械学習をするソフトウェア若しくはプログラムを含む抽象的な概念」と定義付けている（総務省・経済産業省「AI 事業者ガイドライン〔第 1.0 版〕」2024 年 4 月 19 日）。

4 例えば、世界経済フォーラム（WEF）が 2024 年 1 月に公表した専門家メンバーに対するアンケート調査結果では、発生の可能性が高いグローバルリスクの順位において、今後 2 年間では 4 位、今後 10 年間では 8 位に、サイバー犯罪やサイバーセキュリティ対策の低下が挙がっている（World Economic Forum, “The Global Risks Report 2024 19th Edition,” 2024）。

5 サイバー攻撃は、コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと（経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 3.0」2023 年 3 月 24 日）。

Ⅱ　サイバーセキュリティの概念

本章では、サイバーセキュリティの定義及び特徴を確認した上で、主なサイバー攻撃者やインシデントの種類を整理する。

１．サイバーセキュリティの定義及び特徴

サイバーセキュリティに関しては、様々な定義が存在するが、日本のサイバーセキュリティ基本法第 2 条に基づくと、データ、情報システム、情報通信ネットワークを安全に保つための対策を講じて、それを維持することを意味している[6]（図表 2 参照）。

図表 2　サイバーセキュリティに関する主な定義

定義主体	内容
サイバーセキュリティ基本法	電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体〔以下「電磁的記録媒体」という。〕を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう（第 2 条）
経済産業省・IPA	電子データの漏えい・改ざん等や、期待されていた情報技術（IT）システムや制御システム等の機能が果たされないといった不具合が生じないようにすること
総務省	私たちがインターネットやコンピューターを安心して使い続けられるように、大切な情報が外部に漏れたり、ウイルスに感染してデータが壊されたり、普段使っているサービスが急に使えなくなったりしないように、必要な対策をすること（サイバーセキュリティ対策）
	情報に関して（1）機密性（ある情報へのアクセスを認められた人だけがその情報にアクセスできる状態）、（2）完全性（情報が破壊、改竄または消去されていない状態）、（3）可用性（情報へのアクセスを認められた人が、必要時に中断することなく、情報にアクセスできる状態）、を確保すること
ISO/IEC TS27100：2020（サイバーセキュリティの概要を提供する規格）	サイバーセキュリティ：サイバーリスクから人々、社会、組織及び国々を守ること ・ サイバーリスク：サイバー空間内のエンティティの目的に対する不確かさの影響 ・ サイバー空間：ネットワーク、サービス、システム、人々、プロセス及び組織が相互接続されたデジタル環境にあって、デジタル環境上に存在するか、またはその中を横断するもの

（出所）経済産業省・独立行政法人情報処理推進機構（IPA）「サイバーセキュリティ経営ガイドライン Ver 3.0」2023 年 3 月 24 日、総務省国民のためのサイバーセキュリティサイト「サイバーセキュリティって何？」、永宮直史 編著・特定非営利活動法人日本セキュリティ監査協会 著『ISO/IEC 27001・27002 拡張によるサイバーセキュリティ対策―ISO/IEC TS 27100 : 2020 の解説と ISMS 活用術―』日本規格協会、2022 年、より野村資本市場研究所作成

サイバーセキュリティ基本法に基づくと、サイバーセキュリティの主な特徴として、（1）保護客体としての情報は、電磁的方式によりやり取りされるサーバーや端末、記録媒体に保存されたデータに限定、（2）外部からのサイバー攻撃への対策のみならず、企業の従業員による機密性の高い情報の不正持ち出し、不正送金、天災や何らかの人為ミスによって企業の情報システムに障害が発生した場合にそれを迅速復旧するための措置等も

6　増島雅和・蔦大輔『事例に学ぶサイバーセキュリティ』経団連出版、2020 年。

含む、（3）サイバー攻撃はインターネットを通じたもののみならず、例えば USB メモリ等の外部記録媒体を用いた物理的攻撃も含む、が挙げられる[7]。

他方、サイバーセキュリティの概要を提供する規格である「ISO/IEC TS27100：2020[8]」では、国や組織などの安定性と継続性の確保、財産の保全、人々の生命や健康の維持のために許容される水準以下にサイバーリスクを抑えることを目的として掲げている[9]。なお、同規格では、サイバーセキュリティと関連する概念である情報セキュリティとの関係も整理している。具体的には、情報セキュリティは情報そのものを対象としているのに対し、サイバーセキュリティは組織自身の財産等に係るリスクのみでなく、関連する組織や社会、人々を対象としていると示している。

２．サイバー攻撃者の種類

サイバー攻撃者（脅威主体、サイバー脅威アクター）は、一般的に「デジタル・デバイスまたはシステムに意図的に損害を与える個人またはグループ[10]」のことを指す。サイバー攻撃者は、多様な主体が存在し、属性、動機、スキル・レベル、戦術が異なる。本稿では、公安調査庁と IBM による説明に基づき整理する[11]（図表 3 参照）。

公安調査庁は、深刻な脅威として懸念される攻撃者として、国家等が関与・支援する高度なサイバー攻撃集団を挙げている。そして、一般的な特徴として、（1）重要インフラの破壊、情報操作、諜報活動など、政治的・軍事的な国家目標を達成するため、軍や情報機関のオペレーションとして攻撃を実行、（2）任務達成のため、コスト度外視で執拗な攻撃を継続、（3）犯罪者や民間のハッカーを外部の協力者・代理人として使う場合もある、と説明している。また、サイバー攻撃はその特性上、匿名性・秘匿性が高く、攻撃源は自明ではなく、国家の関与・支援の下で行われた攻撃であっても、加害国が否認しやすいことから、伝統的な軍事的脅威に比べて抑止が難しい状況にあると言及している。

---

7 前掲脚注 6 を参照。

8 国際標準化機構（ISO）は、各国の代表的標準化機関から成る国際標準化機関で、電気・通信及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）に関する国際規格を作成している。国際電気標準会議（IEC）は、各国の代表的標準化機関から成る国際標準化機関であり、電気及び電子技術分野の国際規格を作成している。技術仕様書（TS）は、将来的に国際規格（IS）として合意される可能性がある文書と位置付けられるものである。「ISO/IEC TS27100：2020」は、ISO と IEC が共同で策定したもので、「情報技術−サイバーセキュリティ―概要と概念」を提供する規格として、2020 年 12 月に発行された（日本産業標準調査会「ISO/IEC」、同「IEC 規格の制定手順」、一般財団法人 日本情報経済社会推進協会「ISO/IEC27000 ファミリー規格について」2022 年 7 月 22 日）。

9 永宮直史 編著・特定非営利活動法人日本セキュリティ監査協会 著『ISO/IEC 27001・27002 拡張によるサイバーセキュリティ対策―ISO/IEC TS 27100：2020 の解説と ISMS 活用術―』日本規格協会、2022 年。

10 サイバー脅威アクターに関する定義（IBM「脅威アクターとは何か」）。

11 公安調査庁「サイバー空間における脅威の概況 2022」2022 年、同「サイバー空間における脅威の概況 2023」2023 年、IBM「脅威アクターとは何か」。

図表 3　主なサイバー攻撃者の種類

種類	概要
サイバー犯罪者	主に金銭的利益を目的としてサイバー犯罪を犯す。サイバー犯罪者による一般的な犯罪には、ランサムウェア攻撃や、人を騙して金銭の授受をさせたり、クレジットカード情報やログイン資格情報、知的財産、その他の個人情報や機密情報を漏らすフィッシング詐欺などがある
国家アクター	国家や政府は、機密データの窃盗、機密情報の収集、または他の政府の重要なインフラの妨害を目的として、脅威アクターに資金を提供することがしばしばある。これらの悪意のある活動にはスパイ行為やサイバー戦争が含まれることが多く、多額の資金が投入される傾向があるため、脅威は複雑で検出が困難になる
ハクティビスト	社会的・政治的主張を目的としてサイバー攻撃を行う個人・組織。「不正にコンピュータシステム等に侵入すること」を意味する「ハック」と、「活動家」を意味する「アクティビスト」を組み合わせた造語。ハッキング技術を使用して、言論の自由を広めたり、人権侵害を明らかにしたりするなど、政治的または社会的な話題を喚起する。ハクティビストは、自分たちが社会に前向きな変化をもたらしていると信じており、秘密やその他の機密情報を暴露するために個人、組織、政府機関を標的にすることは正当化されていると感じている
スリルを求める人	主に楽しみのためにコンピューターや情報システムを攻撃する。スリルを求める人は常に危害を加えようとするわけではないが、ネットワークのサイバーセキュリティを妨害し、将来のサイバー攻撃への扉を開くことで、意図しない損害を引き起こす可能性がある
内部脅威	他のほとんどの攻撃者タイプとは異なり、内部関係者の脅威アクターは必ずしも悪意を持っているわけではない。中には、知らないうちにマルウェアをインストールしたり、会社支給のデバイスを紛失してサイバー犯罪者にネットワークへのアクセスに使用されたりするなど、ヒューマン・エラーによって企業に損害を与える場合もある。ただし、悪意のあるインサイダーも存在する
サイバーテロリスト	政治的またはイデオロギー的な動機に基づいてサイバー攻撃を開始し、最終的に脅しや暴力に訴える。サイバーテロリストの中には国家アクターである者もいれば、単独で、または非政府グループを代表して行動する人もいる

（出所）IBM「脅威アクターとは何か」、公安調査庁「サイバー空間における脅威の概況 2022」2022 年、より野村資本市場研究所作成

3．インシデントの種類

インシデントには、「サイバーセキュリティ分野において、サイバーセキュリティリスク[12]が発現・現実化した事象[13]」等の定義がある。主なインシデントの種類を、IPA の「情報セキュリティ白書 2023」に基づき、図表 4 にまとめた。

一方、サイバー攻撃が起こる可能性を指すサイバー脅威[14]に関しては、IPA が毎年、「情報セキュリティ 10 大脅威」として公表しているものが参考になる（図表 5 参照）。これらの脅威は単独ではなく複数が組み合わされる場合があると指摘されている[15]。具体

[12] サイバーセキュリティリスクは、サイバーセキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと（経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 3.0」2023 年 3 月 24 日）。

[13] 経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 3.0」2023 年 3 月 24 日。

[14] サイバー脅威とサイバー攻撃の主な違いは、前者はサイバー攻撃が起こる可能性を指すのに対し、後者は実際に起こる攻撃のことを示す（Keeper Security「サイバー攻撃とサイバー脅威のデータベース」）。

[15] 独立行政法人情報処理推進機構（IPA）「情報セキュリティ白書 2023」2023 年 7 月。

例として、（1）フィッシング[16]によって詐取された認証情報でスマートフォン決済の不正利用やインターネット上のサービスへの不正ログインが行われる、（2）自組織のサプライチェーンに含まれる取引先等の関連組織がランサムウェアの被害に遭い、最終的に自組織も被害を受ける、が挙げられている。

図表 4　主なインシデントの種類

種類	概要
ランサムウェア攻撃	ランサムウェアは、パソコンやサーバー等のシステムをロックすることや、システムに保存されているファイルを暗号化することにより使用不能にするウイルスの総称。ランサムウェアによって使用不能にしたシステムやファイルを復旧できるようにすることと引き換えに身代金を要求するサイバー攻撃をランサムウェア攻撃と呼ぶ
標的型攻撃	ある特定の企業・組織や業界等を狙って行われるサイバー攻撃の一種。特定の企業・組織や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的をもって行われる
ビジネスメール詐欺（BEC）	巧妙な騙しの手口を駆使した偽のメールを企業・組織に送り付け、職員を騙して送金取引に関わる資金を詐取する等の金銭被害をもたらすサイバー攻撃
分散型サービス妨害（DDoS）攻撃	DDoS（Distributed Denial of Service）攻撃とは、Web サーバー等の攻撃対象に対して複数の送信元から同時に大量のパケットを送信することで、攻撃対象のリソースに負荷をかけ、サービス運用を妨害する攻撃
ソフトウェア（VPN 製品等）の脆弱性を悪用した攻撃	VPN は、専用のネットワーク回線を仮想的に構築することで、物理的に離れている拠点のネットワーク間を、あたかも同一のネットワークであるかのように接続する技術。VPN は、拠点のネットワークと離れた場所にあるパソコン等を安全に接続するために使用される。VPN 製品に加え、多くの利用者がいる Microsoft 製品、影響範囲の広い開発フレームワークに関する脆弱性を狙った攻撃が散見される
ばらまき型メールによる攻撃	ばらまき型メールは、特定の組織や個人ではなく、不特定多数の一般利用者を狙った、ウイルス感染を目的としたメール。ばらまき型メールでウイルスに感染させる手口としては、添付ファイルを用いる手法等がある
個人を狙う SMS・SNS・メールを悪用した手口	実在のサービスや企業を語り、偽サイト（フィッシングサイト）へ誘導し、IDやパスワードなどの情報を盗んだり、マルウェア（不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称）に感染させたりする手口。メールに加え、SMS（携帯電話のショートメッセージサービス）や SNS（ソーシャル・ネットワーキング・サービス）を悪用したものも増えている
個人を狙う様々な脅しと悪用の手口	Web ブラウザーを悪用した手口、遠隔操作アプリを悪用した副業詐欺、偽 EC サイト（インターネット上で商品やサービスを販売するウェブサイト）など
情報漏えいによる被害	外部からの不正アクセス、操作ミス等の過失、内部者の故意による持ち出し等の内部不正、不適切な情報の取り扱いなど

（出所）独立行政法人情報処理推進機構（IPA）「情報セキュリティ白書 2023」2023 年 7 月、警察庁「フィッシング対策」、より野村資本市場研究所作成

[16] フィッシングとは、実在する組織を騙って、ユーザネーム、パスワード、アカウント ID、銀行等の現金自動預け入れ払い出し機（ATM）の暗証番号、クレジットカード番号といった個人情報を詐取すること。電子メールのリンクから偽サイト（フィッシングサイト）に誘導し、そこで個人情報を入力させる手口が一般的に使われている（フィッシング対策協議会「フィッシングとは」）。

図表 5　情報セキュリティ 10 大脅威 2024 における「個人」・「組織」向け脅威の概要

「個人」向け脅威（五十音順）
概要
インターネット上のサービスからの個人情報の窃取
インターネット上のサービスへの不正ログイン
偽警告によるインターネット詐欺
クレジットカード情報の不正利用
スマホ決済の不正利用
ネット上の誹謗・中傷・デマ
フィッシングによる個人情報等の詐取
不正アプリによるスマートフォン利用者への被害
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求
ワンクリック請求等の不当請求による金銭被害

「組織」向け脅威	
順位	概要
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

（出所）独立行政法人情報処理推進機構（IPA）「情報セキュリティ 10 大脅威」2024 年 2 月、より野村資本市場研究所作成

Ⅲ 世界及び日本におけるサイバー攻撃の現状

本章では、世界と日本におけるサイバー攻撃の状況を概観した上で、金融資本市場の観点から示唆があると考えられるサイバー攻撃に関する 2 つの事例（ノルスクハイドロ及びソーラーウィンズ）を紹介する。

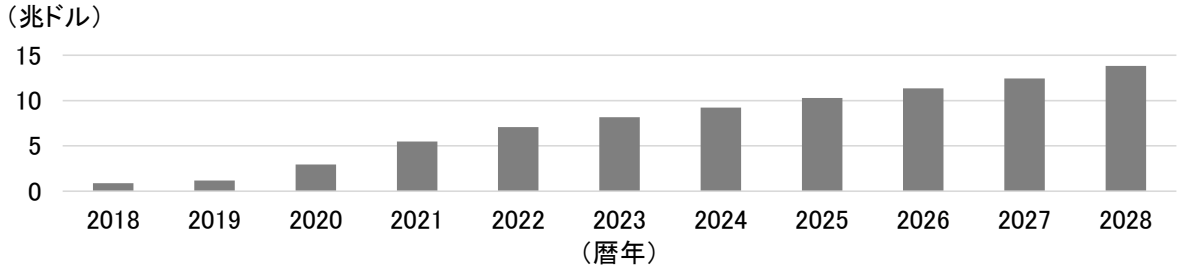
１．世界におけるサイバー攻撃の状況

１）サイバー攻撃による経済的損失に関する試算

サイバー攻撃は近年、新型コロナウイルスの感染拡大を背景としたデジタル化の進展や地政学的緊張も背景に、多様化、高度化、巧妙化している。攻撃対象は個別企業・組織のみならず、重要インフラ、政府等と広範に渡るとともに、被害は直接的な攻撃対象のみならず、連鎖的に広がり、経済社会全体に及ぼす影響が甚大となり得る可能性が示唆されている。

例えば、総務省の「情報通信白書」では、サイバーセキュリティに関する問題が引き起こす経済的損失をめぐる複数の試算を紹介している[17]。同白書で取り上げられた米国のサイバーセキュリティ調査研究企業のサイバーセキュリティ・ベンチャーズでは、世界のサイバー犯罪による損害額は、2024 年に 9.5 兆ドル、2025 年に 10.5 兆ドルに達するとの見込みを公表している[18]。同時に、サイバー犯罪のうち、警察等に報告されているのは 2024 年時点で 4 分の 1 未満との推計を明らかにしている。一方、ドイツの統計調査データプラットフォーム提供企業のスタティスタは、2024 年に 9.22 兆ドル、2025 年に 10.29 兆ドル、2028 年に 13.82 兆ドルに達するとの見込みを示している（図表 6 参照）。

図表 6　世界のサイバー攻撃に伴う推計損害額の推移



（注）　2023 年 9 月時点のデータに基づき、Statista が推計。
（出所）Statista, “Cybercrime Expected to Skyrocket in Coming Years,” February 22, 2024、より野村資本市場研究所作成

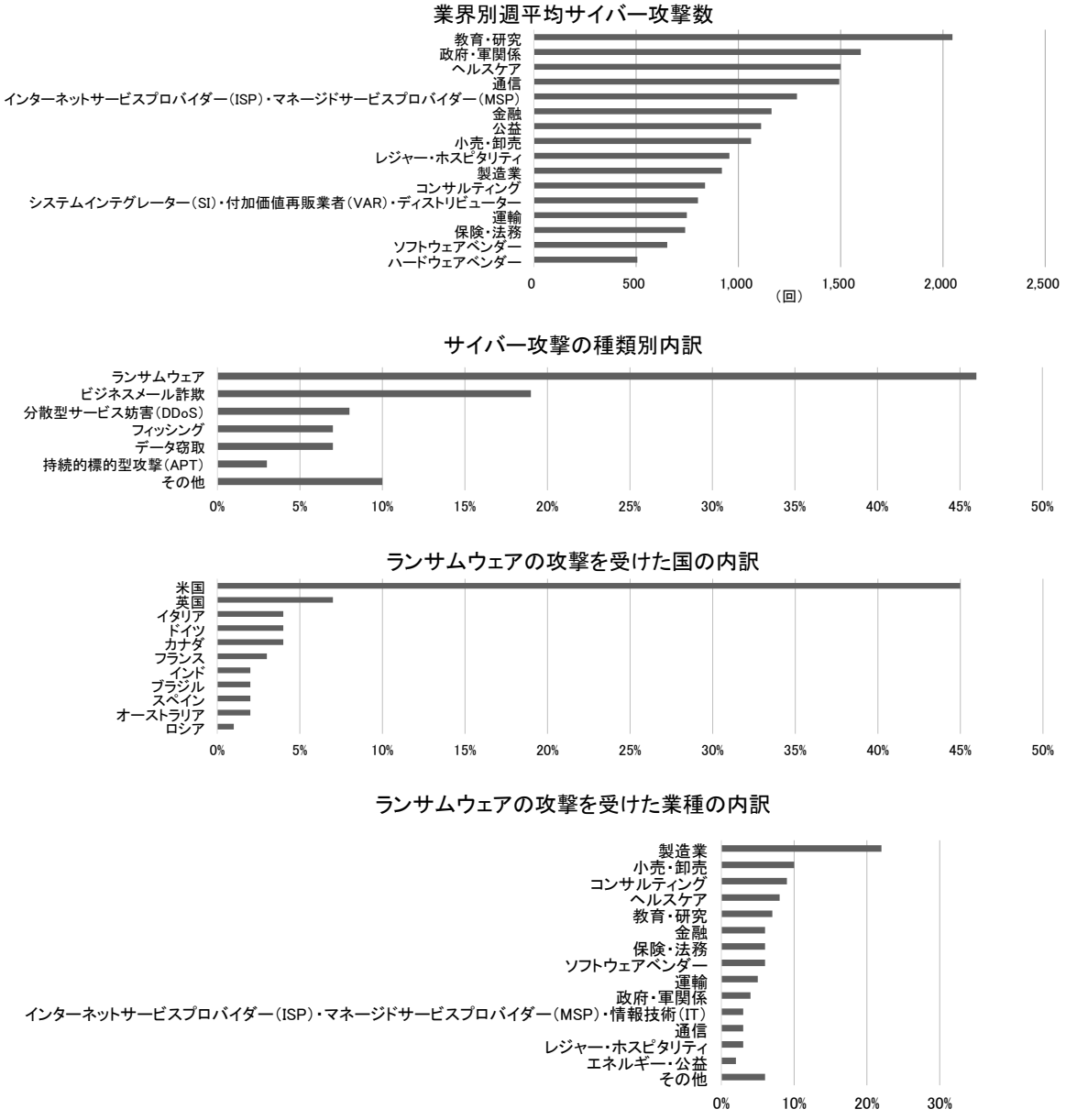
２）サイバー攻撃に関する傾向

サイバーセキュリティソリューションを手掛けるイスラエル系企業のチェック・ポイント・ソフトウェア・テクノロジーズ（チェックポイント）による世界のサイバー攻撃に関する調査分析結果に基づくと、（1）業界別の攻撃ターゲットとしては、教育・研究、政府・軍関係、ヘルスケア等が多い、（2）サイバー攻撃の種類としてはランサムウェアが最も多い、（3）ランサムウェアの攻撃を受けた国では米国が突出している、（4）ランサムウェアの攻撃を受けた業種では、製造業、小売・卸売等が多い、といった傾向が見られる（図表 7 参照）。業種別内訳における順位がサイバー攻撃全体とランサムウェアで異なる背景としては、教育や政府関係機関は身代金を支払う確率が他業種より低く、サイバー攻撃の目的としては恐喝というよりは個人情報等のデータの搾取が主な目的であるためと説明されている。

なお、チェックポイントによる調査結果では、ランサムウェアの攻撃を受けた国の内訳において日本に関する言及はなかった。ただし、英国の法人向けコンピュータセキュリティベンダーであるソフォスの調査結果では、日本の組織も多くの国と同様にランサムウェアの攻撃を受けている傾向が明らかにされている（図表 8 参照）。

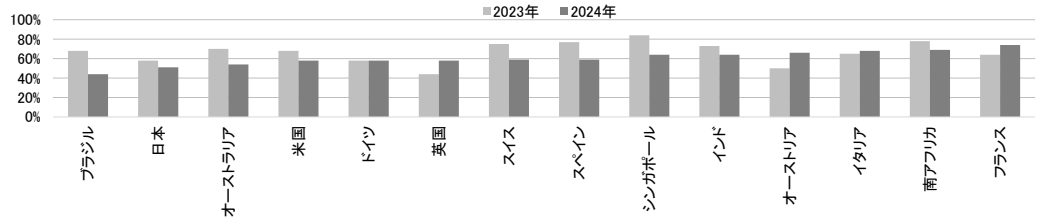
[17] 総務省「令和 6 年版情報通信白書」2024 年 7 月。
[18] “2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics,” *Cybercrime Magazine*, June 24, 2024.

図表 7　世界のサイバー攻撃に関する調査研究結果



（出所）Check Point Software, “Security Report 2024,” 2024、より野村資本市場研究所作成

図表 8　ランサムウェア攻撃を受けた組織の割合（国別）



（注）　14 ヵ国の IT／サイバーセキュリティリーダー5,000 人を対象に 2024 年 1 月から 2 月に独立した調査会社が実施した調査から得られた結果に基づく。

（出所）Sophos「ランサムウェアの現状 2024 年版」2024 年 4 月、より野村資本市場研究所作成

２．日本におけるサイバー攻撃の状況

１）サイバー攻撃による被害額に関する試算

日本の組織に対するサイバー攻撃に伴う被害額については、セキュリティ関連製品の開発・販売を行うトレンドマイクロが複数回にわたって調査を行っている（図表 9 参照）。被害額の範囲をどのように捉えるかは調査によって異なっているが、例えば、上述のソフォスの調査において世界でランサムウェア攻撃を受けた場合の復旧コストの平均は273万ドルと示されており、日本の被害額が突出した水準ではないことがわかる[19]。

図表 9　サイバー攻撃に伴う被害額に関する調査結果

調査名称	概要
法人組織のセキュリティ成熟度調査	・国内の従業員規模 1,000 名以上の法人組織に所属する情報セキュリティに中心的・主体的に関わる立場の 253 名を対象に 2022 年 9 月に調査を実施 ・回答者の約 6 割がセキュリティインシデントによる被害を経験。年間平均被害額は約 3 億 2,850 万円 ・被害額は、システムの復旧、システム停止中の業務効率低下、売上機会の損失などの直接被害に対応した費用のみならず、再発防止策構築のための費用や、イメージ損傷、信頼度下落、株価下落、法的補償など二次的な被害に対応した費用も含む合計の金額を指す
サイバー攻撃よる法人組織被害状況調査	・国内の法人組織（従業員 500 名以上）に勤めるセキュリティやリスクマネジメントの責任者（部長職以上）305 名を対象に 2023 年 6 月に調査を実施 ・過去 3 年間のサイバー攻撃の累計被害額は平均 1 億 2,528 万円、ランサムウェア被害を経験した法人組織の累計被害額は平均 1 億 7,689 万円 ・対応コストとしては、(1)直接コスト（例：不正送金、身代金支払い、業務停止期間の売上、コンサル料、補償金）、(2)復旧エスト（例：被害範囲の特定、データやシステムの復旧人件費）、(3)再発防止コスト（例：セキュリティ対策強化、追加投資）

（出所）トレンドマイクロ「法人組織のセキュリティ成熟度調査を発表―インシデント平均被害額は約 3 億 2,850 万円、復旧に着目した見直しを―」2022 年 12 月 7 日、トレンドマイクロ「過去 3 年間で 56.8%がサイバー攻撃の被害を経験、3 年間の累計被害額は平均 1.3 億円、ランサムウェア被害経験企業では平均 1.8 億円―サイバー攻撃による法人組織の被害状況調査―」2023 年 11 月 1 日、より野村資本市場研究所作成

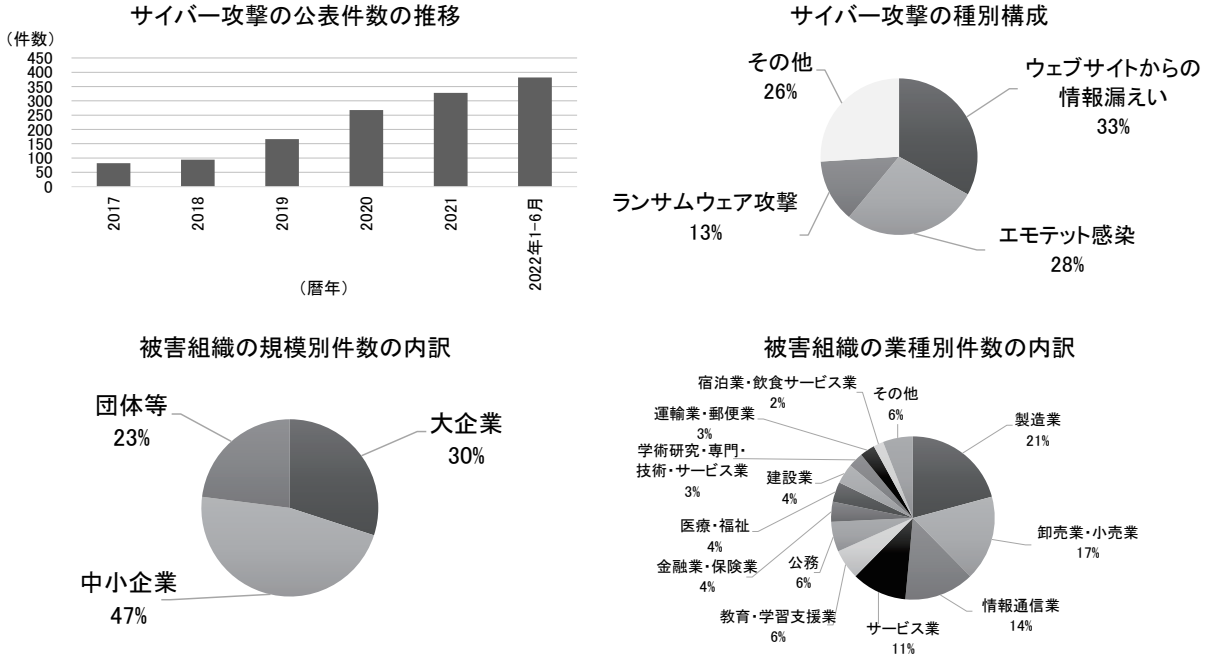
２）サイバー攻撃に関する傾向

日本ネットワークセキュリティ協会（JNSA）が 2017 年 1 月から 2022 年 6 月までの 5 年半のサイバー攻撃の国内被害組織（約 1,300 組織）を対象として 2023 年 9 月に実施した実態調査結果に基づくと、（1）サイバー攻撃の公表件数は年々増加傾向、（2）サイバー攻撃の種類としてはウェブサイトからの情報漏えい、エモテット[20]感染が各々約 3 割ずつを占めている、（3）被害組織の規模は中小企業、大企業、団体等と続いている、（4）被害組織の業種別件数では、製造業、卸売業・小売業等が多い、といった傾向が見られる（図表 10 参照）。サイバー攻撃の公表件数の増加について、サイバー攻撃の増加に加え、2022 年 4 月に施行された改正個人情報保護法により、被害者本人への通知が必要となり、公表されるケースが増加している可能性があると説明されている。

[19] 復旧コストは、ダウンタイム、人件費、デバイスのコスト、ネットワークコスト、逸失利益等（Sophos「ランサムウェアの現状 2024 年版」2024 年 4 月）。

[20] エモテット（Emotet）は、2020 年秋、2022 年春に国内で多くの被害が発生しているマルウェア。攻撃者からのなりすましメールに端を発し、添付ファイルを開封する等により感染、メールアドレス等を窃取する（日本ネットワークセキュリティ協会〔JNSA〕「インシデント損害額調査レポート　別紙『被害組織調査』」2024 年 2 月 9 日）。

図表 10　日本のサイバー攻撃に関する調査研究結果



（出所）日本ネットワークセキュリティ協会（JNSA）「インシデント損害額調査レポート　別紙『被害組織調査』」2024 年 2 月 9 日、より野村資本市場研究所作成

３．サイバー攻撃に関する事例

本節では、サイバー攻撃を受けた企業の事例のうち、金融資本市場にとって示唆があると考えられる主なものを時系列で、（1）ノルスクハイドロ、（2）ソーラーウィンズ、の順に紹介する。

１）ノルスクハイドロ：情報開示も背景に対応が好意的に受け止められた事例

ノルウェーのアルミニウム製造・エネルギー大手のノルスクハイドロは 2019 年 3 月 19 日、ランサムウェア「LockerGoga」の被害を受けたことが明らかになった[21]。40 ヵ国 160 の拠点で 23,000 台のコンピューターのうち 11,000 台が感染するなどした結果、メール、発注や顧客情報管理のコンピューターのみならず製造用のコンピューターも被害を受け、長期間に渡り手作業による製造を強いられた。同社の 2019 年の年次報告書に基づくと、売上高（約 1,497 億ノルウェークローネ〔NOK〕）に対して、サイバー攻撃関連の損失の推計は 6.5～7.5 億 NOK、サイバー保険による補償は 2.16 億 NOK だった旨を公表した[22]。

サイバー攻撃による被害を受けたノルスクハイドロではあるが、金融資本市場では、同社の株価がサイバー攻撃直後に約 5%下落したものの、1 ヵ月後には約 6%上昇した。これは、同社のサイバーセキュリティ対策と事後対応（攻撃直後の手動操作への

[21] Norsk Hydro, “2019: Cyber-Attack on Hydro,” June 11, 2021.
[22] Norsk Hydro, “Annual Report 2019,” 2020.

切り替えによる操業継続、政府機関の協力の下での迅速なインシデント対応、損害額の一部がサイバー保険により補填される見込み等）を、社会や株主が好意的に捉えたことが背景との分析がある[23]。

このような好意的な受け止めは、ノルスクハイドロが透明性（Transparency）と公開性（Openness）を柱に、情報開示を行ったことも下支えしているようだ[24]（図表 11 参照）。専門家によると、サイバー攻撃の被害企業であるノルスクハイドロによるステークホルダーに向けた情報開示は、参考になり得る 5 つのポイントがあると指摘している（図表 12 参照）。

図表 11　ノルスクハイドロがサイバー攻撃に関して行った社内外の広報戦略（2019 年 3～6 月）

日時	社内でのグローバル・タウンホールミーティング	プレスリリース	記者会見（＋ウェブストリーミング）
3 月 19 日	ー	08:31CET（サイバー攻撃の第一報。証券取引所での発表） 14:41CET（サイバー攻撃についての情報更新。証券取引所での発表）	15:00CET
3 月 20 日	09:00CET	08:39CET（サイバー攻撃の最新情報。証券取引所での発表）	14:00CET
3 月 21 日	09:00CET	14:15CET	ー
3 月 22 日	09:00CET	15:53CET	ー
3 月 25 日	09:00CET	13:20CET	ー
3 月 26 日	09:00CET	13:13CET	14:30CET
3 月 27 日	09:00CET	14:01CET	ー
3 月 28 日	09:00CET	14:38CET	ー
4 月 1 日	09:00CET	18:30CET	ー
4 月 5 日	09:00CET	14:57CET	ー
4 月 9 日	09:00CET	ー	ー
4 月 12 日	09:00CET	17:03CET（第 1 四半期決算発表を当初の 4 月 30 日から 6 月 5 日へ変更。証券取引所での発表） 17:05CET	ー
4 月 23 日	09:00CET	ー	ー
4 月 26 日	-	16:07CET	ー
4 月 30 日	-	07:04CET	ー
6 月 5 日	09:00CET	07:00CET（第 1 四半期決算を発表。証券取引所での発表）	遅れた第 1 四半期の決算発表

（注）　1. 本社では毎朝、全社員参加のミーティング（タウンホールミーティング）を行い、それをビデオカメラで録画し、その動画を同社の世界拠点に配信した。それに加えて、社員が Android や iPhone などのデバイスにダウンロードできる社内用アプリもコミュニケーションツールとして駆使した。
2. CET は中央ヨーロッパ時間。

（出所）「その時何が起きたのか?大手アルミ製造「Norsk Hydro」に聞く！―ランサムウェアに感染し操業停止！―」『インプレス』2021 年 4 月 11 日、より野村資本市場研究所作成

[23] 鈴木乾也「運命を変える―サイバー攻撃と企業の命運―」『週刊 経団連タイムス』第 3466 号、一般社団法人日本経済団体連合会、2020 年 9 月 3 日。

[24] ノルスクハイドロは、「Norwegian Communication Association's Transparency Award」を受賞した（独立行政法人情報処理推進機構〔IPA〕「制御システム関連のサイバーインシデント事例 5－2019 年 ランサムウェアによる操業停止－」2020 年 3 月）。

図表 12　ノルスクハイドロの情報公開において参考になり得るポイント

項目	概要
迅速に被害を発表	・被害を受けた翌日に発表
SNS を使って情報発信	・自社のシステムより早く、社外のサービスを活用して被害を受けた旨を情報発信（自社のシステムでリリースを出す前に、フェイスブックを使って感染が明らかになった当日〔2019 年 3 月 19 日〕に情報発信） ・企業や組織で SNS の公式アカウントを用意しておけば、仮に、サイバー攻撃の被害を受けて自社のシステムが使用不能になっても、素早く情報発信が可能に ・SNS であれば、ステークホルダーとのコミュニケーションツールとして使用することも可能。ウェブサイトでは情報通信が一方通行になるため、SNS を使った情報発信も意義がある
透明性を確保する姿勢	・記者会見をウェブで動画中継。上述のフェイスブックへの投稿でノルウェーのウェブキャスティングサービス「HegnarTV」を使って、感染が明らかとなった当日に動画中継を行うことを公表 ・中継は記者からの質問時間も全て対象として配信 ・動画中継は、感染が明らかになった当日のみならず、翌日、1 週間後にも実施
頻繁に情報発信	・感染が明らかになってから約 1 ヵ月後に当たる 2019 年 4 月 12 日までに 10 件以上のリリースを発出。特に、同年 3 月 19 日から 27 日までは、土日を除いて毎日リリースを出した（複数のリリースを出した日もあった） ・リリースでは、部門ごとの運用状況を頻繁に更新。YouTube を利用して、現場の状況がわかるような動画も配信 ・各部門の最新状況、報道機関や投資家の連絡先などを一目で確認できるようなポータルサイトも作成。同ポータルサイトでは、取引先に対して、フィッシングや BEC に関する注意喚起も実施
リーダーシップの可視化	・経営幹部が積極的にコメントを発信。サイバー攻撃の被害企業から出されるリリースは、情報の発信源が情報システム部門の現場担当者になりがちだが、同社の場合、2019 年 3 月 21 日以降、最高財務責任者（CFO）や情報システム部門のトップなどが積極的にコメントを掲載するように ・2019 年 3 月 21 日の CFO のコメントでは、最初の対応でウイルスの封じ込めに成功したこと、徐々に回復に向かっていることなどを明らかに。責任ある立場の人間がコメントすることで、全社を挙げて復旧に努めている姿勢が外部に伝わりやすくなることも

（出所）辻伸弘「辻伸弘の裏読みセキュリティ事件簿－第 52 回－ウイルス被害企業の情報公開　参考になる 5 つのポイント」『日経 NETWORK』2019 年 7 月、より野村資本市場研究所作成

ノルスクハイドロの事例は、サイバー攻撃により被害を受けたものの、上述の透明性と公開性を軸にした情報開示も含めて適切な事後対応を行ったこともあり、投資家も含めたステークホルダーに評価されたと解釈され、他の企業にとっても参考になり得ると言える。

2）ソーラーウィンズ：SEC による提訴とソフトウェアセキュリティへの着目

米国のサイバーセキュリティ企業ソーラーウィンズは 2020 年 12 月 13 日、同社のネットワーク監視ソフトウェア「Orion Platform」に、正規のアップデートを通じてマルウェア「Sunburst」が仕込まれたことを公表した[25]。サイバー攻撃は 2019 年 9 月には始まっていたとみられ、2020 年 3～6 月のアップデートファイルの侵害を通じて、米政府機関等を含む最大約 1 万 8,000 組織が影響を受けたとされている[26]。トレンドマイクロによると、「Sunburst」が検出された事例は米国が中心だったが、複数の

[25] Solarwinds, “SolarWinds Security Advisory RE: CERT Emergency Directive,” April 6, 2021.
[26] 経済産業省「サイバーセキュリティに関連する海外の動き」2021 年 3 月。

国・地域も含まれており、少数ながら日本のものもあった[27]。加えて、米国のサイバーセキュリティ企業アイアンネットによると、ソーラーウィンズのサイバー攻撃の影響を受けた企業は、平均して年間収益額の約 11%の損害を被った[28]。

本攻撃による被害が甚大かつ時間をかけて広まっていったのは、（1）ソーラーウィンズは製品をプログラムする部門が政府系ハッカーに侵入され、気が付かないまま製品に不正なコードを埋め込まれ、その製品がアップデート等で顧客に配布、（2）その製品が顧客のシステムにダウンロードされると、しばらく何もしない期間（最大 14 日間）を経て、バックドア（第三者が侵入できる裏口）を不正に設置し、攻撃者にその旨を通知、（3）攻撃者がシステムに外部より勝手に入れるようになり、欲しい内部情報を探して窃取、といった手法が背景の 1 つとされている[29]。

ソーラーウィンズに対するサイバー攻撃は、金融資本市場の観点から、（1）米国証券取引委員会（SEC）による提訴、（2）ソフトウェアのセキュリティ確保に向けた「SBOM」（後述参照）という考え方の広がり、といった点が注目に値する。

1 点目について、SEC は 2023 年 10 月 30 日、ソーラーウィンズと最高情報セキュリティ責任者（CISO）を、既知のサイバーセキュリティリスクと脆弱性[30]に関する詐欺行為と内部統制の不備で提訴した旨を公表した[31]。ニューヨーク州南部地区連邦地方裁判所に提出された訴状では、少なくとも 2018 年 10 月の新規株式公開（IPO）から、2020 年 12 月のサイバー攻撃に関する公表まで、同社と CISO が同社のサイバーセキュリティ対策を誇張し、既知のリスクを過小に開示して投資家を欺いたと指摘された。具体的には、ソーラーウィンズは 2020 年 12 月 14 日に提出した臨時報告書（Form 8-K）の中で「Sunburst」による攻撃に関する不完全な開示を行い、その後、株価が 2 日間で約 25%、同月末までに約 35%下落したと説明されている。SEC の訴状では、ソーラーウィンズと CISO が 1933 年連邦証券法及び 1934 年連邦証券取引法の不正防止条項に違反したと主張し、違反の是正や民事制裁金の賦課等が求められた。

本件について連邦地方裁判所は 2024 年 7 月 18 日、SEC の提訴のうち、ソーラーウィンズのセキュリティ対策に関する誇張が証券詐害（securities fraud）に該当する可能性があるとしたものの、SEC の申し立ての大部分を棄却する判決を下した[32]。ただし、本件は、サイバー攻撃の被害に遭った企業を対象とした初めての訴訟とみられ

---

27 トレンドマイクロ「SolarWinds 社製品を悪用、米政府などを狙う大規模サプライチェーン攻撃」2020 年 12 月 16 日。

28 IronNet, “2021 Cybersecurity Impact Report,” June 2021.

29 「大手企業が次々と被害に　ソーラーウィンズから連鎖した『サプライチェーン攻撃』の脅威」『ITmedia』2020 年 12 月 24 日。

30 脆弱性とは、1 つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと（経済産業省「ソフトウェア管理に向けた SBOM〔Software Bill of Materials〕の導入に関する手引 ver 1.0」2023 年 7 月 28 日）。

31 U.S. Securities and Exchange Commission, “SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures,” October 30, 2023; United States District Court Southern District of New York, “Securities and Exchange Commission, Plaintiff, -v- Solar Winds Corp. and Timothy G. Brown, Defendants: Jury Trial Demanded,” October 30, 2023.

32 United States District Court Southern District of New York, “Securities and Exchange Commission, Plaintiff, -v- Solar Winds Corp. & Timothy G. Brown, Defendants: Opinion & Order,” July 18, 2024.

る[33]ことからも、金融資本市場から注目を集めたようだ。

2点目のSBOM（Software Bill of Materials、エスボム）とは、ソフトウェアの部品構成表のことを指し、ソフトウェアを構成する各部品（コンポーネント）を誰が作り、何が含まれ、どのような構成となっているか等を示すものである[34]。

ソフトウェア業界でも部品を組み合わせてアプリケーションを構築することが一般的になっており、オープンソースソフトウェア[35]（OSS）に代表されるソフトウェア部品を供給・利用するサプライチェーンが形成されている[36]。ソフトウェア部品の利用は、高度な機能を有するアプリケーションを効率良く開発できるといったメリットがある一方、上流で発生した事象がサプライチェーンの下流全体に影響を及ぼすといった構造的な課題があり、ソフトウェアのサプライチェーンの弱点を悪用した攻撃が増加傾向にある。

SBOMが注目を集めるようになった背景の1つには、米国大統領令の存在が挙げられる。ジョー・バイデン大統領は2021年5月、ソーラーウィンズ等の国家レベルのサイバー攻撃の激化を受けて、大統領令（EO）14028「国家のサイバーセキュリティの改善に関する大統領令」に署名した[37]。同大統領令の中で、ソフトウェアの構成要素に関する詳細の開示手段としてSBOMが言及されている。

日本においても、経済産業省がSBOMの企業による活用を推進すべく、2023年7月にSBOMを導入するメリットや実際に導入するにあたって実施すべきポイントをまとめた手引書[38]を公表している。同省では、SBOMの導入により、脆弱性対応に関するコストや対応期間を縮減すること等が期待されるほか、脆弱性リスクの低減を通じた製品価値や企業価値の向上も間接的なメリットとして考えられると説明している[39]。

Ⅳ 今後の注目点

本稿では、世界及び日本におけるサイバー攻撃が近年、複雑化、巧妙化、甚大化しており、攻撃対象への直接的な被害のみならず、経済社会全体に及ぼす影響が懸念される旨をデータも踏まえて概観した。そして、サイバー攻撃を受けた企業のうち、（1）情報開示も背景に対応が好意的に受け止められた事例として、ノルウェーのノルスクハイドロ、

33 “SolarWinds Beats Most of US SEC Lawsuit over Russia-Linked Cyberattack,” *Reuters*, July 19, 2024.
34 経済産業省「『ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0（案）』の概要及び意見募集について」2024年4月26日。
35 オープンソースソフトウェア（OSS）とはソフトウェアのソースコードが公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェア（経済産業省「OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」2022年8月1日）。
36 PwC「SBOM普及の本格化－ソフトウェアサプライチェーンの構造的な課題と解決策－」2022年4月8日。
37 The White House, “Executive Order on Improving the Nation’s Cybersecurity,” May 12, 2021.
38 経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 1.0」2023年7月28日。
39 経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0（案）」2024年4月26日。

（2）SEC により提訴されたほか、SBOM という概念の広がりのきっかけとなった事例として、米国のソーラーウィンズ、を取り上げた。

今後も世界的にサイバー攻撃に伴うリスクの拡大傾向が続くと想定されるが、その勢いや内容を見据える場合、主に3つの要素（AIの進展に伴うサイバーリスクとセキュリティへの影響、地政学リスクの状況、人材確保・育成）が注目点になり得ると言える。

1点目は、AIの進展に伴うサイバーリスクとセキュリティへの影響である。AIは近年、画像・音声認識、ビッグデータ解析、車の自動運転、医療診断をはじめとして幅広い分野で導入、開発、活用が進んでおり、経済社会の発展を後押ししている。その一方で AI 技術を悪用したサイバー攻撃が現実化している。例えば、英国の国家サイバーセキュリティセンター（NCSC）が 2024 年 1 月に公表した「サイバー脅威に対する AI の短期的影響」と題したレポートでは、AIが今後2年間でサイバー攻撃を増加させ、影響が高まることはほぼ確実との予想を示した上で、（1）AI が偵察とソーシャル・エンジニアリング[40]の能力を向上させる、（2）サイバー犯罪初心者が効果的なアクセスや情報収集実行のための障壁を低くするため、ランサムウェアの脅威を後押しする可能性がある、等の分析結果を示している[41]。

AI は、ディープフェイクを始めとしたサイバー攻撃をもたらす一方、ログの監視・解析等のサイバーセキュリティ対策での活用も進められている（図表 13～14 参照）。AI の進展に伴い、サイバーリスクやサイバーセキュリティへどのような影響が及ぶのかは注視するポイントの1つと考えられる。

図表 13　AIによる主なサイバー攻撃の種類

項目	概要
ディープフェイク	ディープフェイクとは、人物の動画や音声を AI 処理によって人工的に合成する技術のこと。ディープフェイクにより生成された偽の映像や音声は、人々を欺くために使用されることがある
DDoS 攻撃	AIを駆使したDDoS攻撃は、対象となるウェブサイトやオンラインサービスを高効率で無力化させる
AIファジング	ファジングは、ソフトウェアテストの手法の 1 つ。AI を用いたファジングは、ソフトウェア内の脆弱性を効率的に発見するために利用されるが、悪意のある攻撃者によって使われると、未知の脆弱性を突く新たな攻撃に繋がる恐れがある
フィッシングメール	AI を活用したフィッシングメールは、受信者の行動や好みを細かく分析し、メッセージに説得力を加える。これにより、従来の手法に比べて受信者が騙されやすくなるほか、自動化技術によって大量のフィッシングメールが作成可能になる
機械学習ポイズニング	機械学習ポイズニングは、AI の自動学習機能を悪用した攻撃手法。AI モデルの学習データに意図的に誤情報を混入させることで、信頼できるモデルの判断を歪める可能性がある
回避攻撃	回避攻撃は、敵対的サンプルを利用してAIの誤認識を発生させる攻撃手法。推論用の認証・識別データにノイズを発生させることで、AIの誤分類を意図的に誘発させ、既存の防御メカニズムを無効化する

（出所）GMOインターネットグループ「AI時代に求められるセキュリティ対策｜サイバーセキュリティとAIの関係性」2024年4月22日、より野村資本市場研究所作成

[40] ソーシャル・エンジニアリングとは、人々を操り、共有すべきでない情報を共有させたり、ダウンロードすべきでないソフトウェアをダウンロードさせたり、訪問すべきでないウェブサイトを訪問させたり、犯罪者に送金させたり、個人または組織のセキュリティを危険にさらすその他のミスを犯させたりする。ソーシャル・エンジニアリングの種類には、フィッシング攻撃等がある（IBM「ソーシャル・エンジニアリングとは何か？」）。

[41] National Cyber Security Centre, “The Near-Term Impact of AI on the Cyber Threat,” January 24, 2024.

図表 14　AIによる主なサイバーセキュリティ対策の種類

項目	概要
ログの監視・解析	ログデータの監視と解析に AI を活用することで、異常な挙動を即座に検出し、未知の脅威を特定することが可能に。AI による解析は、複雑なデータパターンの中からも異常を見つけ出し、セキュリティチームが脅威に対して迅速に対応できるようサポートする
マルウェアの検出	機械学習を利用した AI は、未知のマルウェアや変異型の検出に優れている。近年はディープラーニング（深層学習、多数の層から成るニュートラルネットワーク〔人間の脳の仕組みをコンピューター上で真似た仕組み〕を使って行う機械学習）を用いた技術の活用により、従来の方法では検出できない新型のマルウェアに対しても、高い検出率を実現する
トラフィックの監視・解析	ネットワークトラフィックのリアルタイム分析を通じて、AI は異常な通信パターンを迅速に検出する。これにより、内部からの脅威やデータ漏洩の試みを早期に発見し、適切な対策を講じることが可能にする
脆弱性診断	脆弱性診断とは、システムの不具合を洗い出すセキュリティ診断のこと。AI 技術を用いることで、システムの脆弱性を自動で診断し、潜在的なセキュリティリスクを事前に特定する
ペネトレーションテスト	ペネトレーションテストとは、攻撃者の視点で脆弱性から侵入を試みたときに、目的達成できるか否かを検証する侵入テストのこと。AI を活用した自動化ペネトレーションテストにより、システムのセキュリティ弱点を効率的に発見する

（出所）GMO インターネットグループ「AI 時代に求められるセキュリティ対策｜サイバーセキュリティと AI の関係性」2024 年 4 月 22 日、総務省「人工知能（AI：エーアイ）のしくみ」、より野村資本市場研究所作成

2 点目は、地政学リスクの状況である。サイバー空間には国境がないものの、通信インフラ等の施設が設置されている場所の地理的・政治的特性は地政学的リスクの影響を受ける[42]。また、前述のとおり、国によっては政府がサイバー空間において様々な活動を展開しているケースもあり、国際政治情勢の悪化がサイバー空間のリスクを高めることに繋がり得る。企業にとっても自身を取り巻く地政学的環境を把握・分析した上でサイバーセキュリティ対策に取り組むことが、価値保全に向けて不可欠と言える[43]。

3 点目は、人材確保・育成である。人材サービス業等を営むリクルートによると、2023 年のサービスセキュリティ関連求人数は 2014 年比で 24.3 倍に増加している一方、転職者数の伸びは 2014 年比で 3.62 倍にとどまっている[44]。同社によると、近年の求人数の急速な増加は、（1）東京 2020 オリンピック・パラリンピック競技大会の開催を背景とした重要インフラを狙ったサイバーテロへの懸念の高まり、（2）新型コロナウイルス感染症の流行によるテレワークの浸透により、バーチャル・プライベート・ネットワーク（VPN）機器の脆弱性を突いたサイバー攻撃の多発、等がきっかけとなっており、人材のニーズに転職者数が追い付いていない状況となっている。

42 菊池朋之「日本企業が直面する『サイバー空間の地政学的リスク』、脅威の傾向と防衛策とは」『ダイヤモンド・オンライン』2022 年 5 月 17 日。

43 専門家は、サイバー空間における地政学的リスクへの対応として、サイバー脅威分析（世界的なサイバー空間上のトレンド〔攻撃手法、攻撃主体、対象セクター等〕を収集し、サイバー空間における一般的なリスク環境を適切に把握した上で、地政学的リスク環境を踏まえてその企業や組織にとってのサイバー空間上のリスク環境を分析）すること等が重要と指摘している（菊池朋之「日本企業が直面する『サイバー空間の地政学的リスク』、脅威の傾向と防衛策とは」『ダイヤモンド・オンライン』2022 年 5 月 17 日）。

44 リクルート「サイバーセキュリティー関連求人、2014 年比で 24.3 倍に増加　生成 AI を悪用するサイバー攻撃への対応でさらに加速　即戦力人材の採用は『レッドオーシャン』。転職時の年収は上昇傾向」2024 年 3 月 15 日。

加えて、サイバーセキュリティ関連で求められる人材像にも変化があるとの指摘もある[45]。具体的には、従来のサイバーセキュリティ関連の求人は、ニッチな専門人材が主な対象で、例えばデジタル的なセキュリティに関するスキルに特化した人材が求められ、個人情報保護方針の対応は他部門で行われているケースが多い傾向にあった。しかし、近年、経済産業省が企業の DX に関する自主的な取り組みを促すべく、「デジタルガバナンス・コード[46]」を公表していることもあり、「デジタルガバナンス[47]」の概念が日本でも注目を集めている。デジタルガバナンスの概念を踏まえると、サイバーセキュリティそのもののみならず、ガバナンス、さらには関係企業やグローバル部門、支社、子会社との関係折衝まで網羅的に担えるサイバーセキュリティ人材が求められるところであるが、転職市場にそのような人材が実在するかは不明とされている。

サイバーセキュリティに関する外部人材の採用が難しい現状を踏まえると、当面においては、企業内部での育成強化のみならず、企業間連携、政府や業界団体等による支援等も、企業のサイバーリスク軽減の観点からカギになると言える。

[45] 中川貴史「セキュリティー人材に必須となるデジタルガバナンスの新潮流」『金融財政事情』第 75 巻第 27 号、2024 年 7 月 16 日。

[46] デジタルガバナンス・コードは、企業の DX に関する自主的取組を促すため、デジタル技術による社会変革を踏まえた経営ビジョンの策定・公表といった経営者に求められる対応をまとめたもの。2020 年 11 月 9 日に策定され、2022 年 9 月 13 日に改訂された（経済産業省「デジタルガバナンス・コード 2.0」2022 年 9 月 13 日）。

[47] デジタルガバナンスとは、企業が内外環境の変化やステークホルダーとの対話による価値共創を踏まえ、デジタルテクノロジーを活用するにあたり、経営によるリーダーシップのもと、事業戦略の実現のために機動性と健全性を兼ね備えたデジタル推進・管理態勢を確保するための機能を意味する（PwC「デジタルガバナンス整備支援」）。