2023年1月16日

SOMPOリスクマネジメント
安心・安全・健康のテーマパーク

損保ジャパンRMレポート | 236

サプライチェーンのサイバーリスク

髙宮　真之介　Shinnosuke Takamiya
サイバーセキュリティ事業本部 事業企画部
企画グループ 上級研究員

概要

市場のグローバル化やIT技術の発展に伴うサプライチェーンの拡大に合わせて、サイバー攻撃も高度化しつつある。サプライチェーンに起因するサイバーリスクは増大傾向にあり、企業・組織にとって重要な課題となっている。本レポートでは、サプライチェーンのサイバーリスクを概観するとともに、当該リスクを管理・低減するために必要な、組織的取り組みについて紹介する。

目次

1. 近年のサプライチェーン・サイバーリスクの増大

サプライチェーンに起因するサイバーリスクが近年特に懸念されている。独立行政法人情報処理推進機構（以下「情報処理推進機構」）は毎年、社会的に影響の大きいセキュリティ上の脅威をランク付けし公開している。2022 年に公開された「情報セキュリティ 10 大脅威 2022」[1]では、サプライチェーンの弱点を悪用したサイバー攻撃が、第 3 位にランクインした。2020 年、2021 年の第 4 位からランクアップしており、脅威の増大を示している。

本章では、社会・経済活動の変化に伴い増大した、サプライチェーン・サイバーリスクの傾向を紹介する。

1.1. サプライチェーンの功罪

現代の企業・組織は、グローバルにまたがる膨大なサプライチェーンを構築することが可能となった。市場のグローバル化や IT 技術の普及がその原動力である。商品・製品の原料調達から販売にいたるまでの各過程には、多くのサプライヤーや委託業者等が関与している。このような多数の組織体が連携し機能することで、事業フローを成立させている。

事業活動を支える IT 技術も、サプライチェーンを支える要素である。企業・組織が利用する設備やシステム、ソフトウェアは、インターネットや組織間ネットワークを通じて連接され、迅速な通信や処理を担っている。電子メールやテレビ会議といったコミュニケーション手段だけでなく、インターネットを利用したシステムや Web サイト、データ共有・連携の仕組み、サプライヤーとのネットワーク連接、クラウドサービスの利用も盛んである。このような IT 活用には、多くの通信・IT 事業者やシステム委託会社が関わっている。

さらに、次章で詳しく紹介するが、ビジネスにおいて用いられているソフトウェアもまた、機械や自動車製造と同じく、サプライチェーンを形成している。ソフトウェアは提供者や管理者の異なる多数のコンポーネント（ソフトウェアやハードウェアにおけるパーツ、構成部品のこと）によって成り立っており、この依存関係は、ソフトウェア・サプライチェーンと呼ばれる。

このように、サプライチェーンの最大の特長および強みは、個々の組織体を結びつけ、目的に向けた統合を可能にする相互依存性にある。物理的・システム的に密接に結合したサプライチェーンが力を発揮することで、現代の企業・組織はこれまでにない大規模かつ効率的な事業活動を推進できるようになった。

しかし、サプライチェーンの相互依存性が高まる一方で、サイバーリスクやインシデントを誘発する脆弱性もまた増大している。企業・組織の活動は、サプライチェーンを構成する多数のパートナーやサプライヤー、サードパーティによって成立している。たとえ自組織が強力なセキュリティ対策を講じていたとしても、守りの手薄なサプライヤーが攻撃を受ければ、被害や影響は自組織を含むサプライチェーン全体に波及する。さらに近年のサイバー攻撃者はその手口を高度化し、サプライチェーンの脆弱性を狙っている。

以下、特に増大しているサプライチェーン・サイバーリスクを、事例とともに紹介する。

1.2. 近年のサイバーリスク動向

欧州連合のサイバーセキュリティ当局である European Network and Information Security Agency（欧州ネットワーク情報セキュリティ機関、以下「ENISA」）は、2021 年の公表資料[2]において、サプライチェーン・

[1] 情報処理推進機構. 情報セキュリティ 10 大脅威 2022. https://www.ipa.go.jp/security/vuln/10threats2022.html, （アクセス日：2022-12-14）.

[2] ENISA. Threat Landscape for Supply Chain Attacks, ENISA (2021).https://digital-skills-jobs.europa.eu/en/inspiration/research/threat-landscape-supply-chain-attacks-enisa-2021.（アクセス日:2022-12-21）.

リスクおよびサプライチェーンを狙ったサイバー攻撃が増加傾向にあると述べている。 同じく国際的な IT ガバナンス団体である Information Systems Audit and Control Association（情報システムコントロール協会、以下「ISACA」）は、2022 年の脅威レポート[3]において、サプライチェーンが原因のサイバー被害が増大した点を指摘している。また、カナダの IT 企業 BlackBerry 社が毎年刊行している情報漏洩調査レポート[4]によれば、2021 年に世界で発生したセキュリティインシデントの 63%が、被害組織の属するサプライチェーンによって引き起こされたものだという。

現在最も流行している攻撃手法の 1 つがランサムウェアである。ランサムウェアは、感染したコンピュータ内のファイルを暗号化し、身代金（ランサム）を要求するマルウェア[5]の一種である。ランサムウェアに感染すると、システムが利用不能となり、事業活動に大きなダメージを与える。ランサムウェア攻撃の多発もまた、サプライチェーン・サイバーリスクを増大させる一因となっている。

2021 年に発生した、サプライチェーンに起因する主要なインシデントを表 1 に示す。

表 1　2021 年のサプライチェーンに起因するインシデント[6]

年	国	概要	被害影響
2021	米国	石油パイプライン大手がランサムウェアに感染、石油供給ラインが全停止[7]	米国東海岸一帯のガソリンスタンドが停止
2021	スイス	航空輸送用 IT サービスを手掛ける SITA 社のシステムに不正アクセスが発生、同システムを利用する Air India や国内航空会社の顧客情報が流出[8]	各国の航空会社利用客 200 万名超の情報が流出
2021	米国	Kaseya Limited 社の IT 管理製品がランサムウェアに感染し、同製品を利用する MSP を通じ感染が拡大[9]	世界各国 1,000 社以上がランサムウェア被害
2021	ブラジル	食肉加工大手 JBS USA Holdings, Inc 社がランサムウェアに感染、米国所在の食肉処理施設が運用停止[10]	米国、カナダ、オーストラリアの食肉供給中断
2021	日本	政府機関が利用するクラウド情報共有ツールに不正アクセスがあり、機密情報が流出	各省庁の業務データや職員情報流出
2021	日本	カード決済代行業者のシステムに不正アクセス発生、同システムを導入していた企業組織の顧客情報が流出	46 万件のクレジットカード情報、加盟店情報流出

[3] ISACA. Supply Chain Security Gaps: A 2022 Global Research Report. https://www.isaca.org/resources/reports/supply-chain-security-gaps-a-2022-gloworbal-research-report. （アクセス日:2022-12-21）.
[4] BlackBerry. 2022 Threat Report. https://www.blackberry.com/us/en/forms/enterprise/report-bb-2022-threat-report-pi.（アクセス日:2022-12-21）.
[5] マルウェアは、コンピュータに対し悪意ある動作を引き起こすプログラム。コンピュータウイルスとも呼ばれる.
[6] 当社作成
[7] U.S.Energy Department. Colonial Pipeline Cyber Incident. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident. （アクセス日:2022-12-21）.
[8] BleepingComputer. SITA data breach affects millions of travelers from major airlines. https://www.bleepingcomputer.com/news/security/sita-data-breach-affects-millions-of-travelers-from-major-airlines/.（アクセス日:2022-12-21）.
[9] CISA. Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers. https://www.cisa.gov/uscert/kaseya-ransomware-attack.（アクセス日:2022-12-21）.
[10] Reuters. Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack. https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/.（アクセス日:2022-12-21）.

1.3. 2022 年もインシデントが続発

2022 年の統計資料はまだ少ないが、サプライチェーンに起因するインシデントは依然増加傾向にある[11]。

国内では、大手メーカーにパーツを供給するサプライヤーがランサムウェアの被害を受けた。その結果、当該メーカーの全生産ラインが停止に追い込まれ、マスメディアでも大きく報じられた。2022 年 7 月には、企業 Web サイト向け SaaS[12]を提供する事業者がサイバー攻撃を受けた。事業者のプログラムが改ざんされたことで、サービスを利用する複数の企業が、顧客の個人情報を漏洩させる結果となった。直近では、地方自治体が運営する医療機関がランサムウェアに感染、院内の電子カルテシステムが利用不能となり、医療機関は患者の受け入れを停止した。攻撃者は、医療機関そのものではなく、医療機関とネットワーク上で接続された給食業者のサーバーから侵入した可能性が高いと報じられている。

海外でもサプライチェーンに起因するインシデントは後を絶たない。11 月には、広告配信システムを運営する米国企業に対し、不正アクセスが発生した。配信システムに不正なプログラムが挿入された結果、同システムを利用する 250 超のニュースサイトが、マルウェア攻撃を行う悪性 Web サイトに変化した[13]。また本レポート執筆中の 12 月、ダークウェブフォーラム[14]上に、7 万 7 千件超の Uber Technologies, Inc.の従業員データが公開される事案が起きている[15]。まだ進行中のインシデントではあるが、この情報漏洩のきっかけが、Uber 本社ではなく、IT 機器管理を委託する企業に対するサイバー攻撃であることが判明している。

米国の仮想通貨取引所 Gemini Trust Company, LLC（以下「Gemini」）が、同じく 12 月、サードパーティ企業経由で不正アクセスを受け、約 600 万件の顧客メールアドレスおよび電話番号が流出したことを公表した。Gemini 利用者は現在、犯罪者から多数のフィッシング攻撃[16]を受けているという[17]。

事例が示すように、サプライチェーン・サイバーリスクの影響度は非常に大きく、また発生可能性も高いため、企業・組織にとって無視できない懸念事項である。次章では、サプライチェーン・サイバーリスクがどのようなものかを、性質に基づいて分類・整理することにより、当該リスクの全体像を提示したい。

2. サプライチェーン・サイバーリスクの概観

本章では、サプライチェーンに起因するサイバーリスクを、(1) サプライヤーに起因するリスク、(2) ソフトウェア・サプライチェーンに起因するリスク、(3) サプライチェーン攻撃、の 3 つに分けて説明する。

2.1. サプライヤーに起因するリスク

サプライチェーン、すなわち事業活動をめぐる企業間の相互依存は多様化しており、サプライヤーとの関係も様々である。

---

[11] ISACA. Supply Chain Risk Management: Where Do We Start?. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/supply-chain-risk-where-do-we-start.（アクセス日:2022-12-21）.

[12] SaaS（System as a Service）とは、クラウド上のソフトウェアを顧客に提供するサービス.

[13] BleepingComputer. Hundreds of U.S. news sites push malware in supply-chain attack. https://www.bleepingcomputer.com/news/security/hundreds-of-us-news-sites-push-malware-in-supply-chain-attack/.（アクセス日:2022-12-21）.

[14] ダークウェブフォーラムとは、ハッカーやサイバー犯罪者が利用する、匿名インターネットフォーラムのこと.

[15] BleepingComputer. Uber suffers new data breach after attack on vendor, info leaked online. https://www.bleepingcomputer.com/news/security/uber-suffers-new-data-breach-after-attack-on-vendor-info-leaked-online/.（アクセス日:2022-12-21）.

[16] フィッシング攻撃とは、なりすましメールや電話を通じて、ターゲットから金銭や情報を窃取する詐欺行為のこと.

[17] BleepingComputer. Hackers leak personal info allegedly stolen from 5.7M Gemini users. https://www.bleepingcomputer.com/news/security/hackers-leak-personal-info-allegedly-stolen-from-57m-gemini-users/.（アクセス日:2022-12-21）.

まずは製造業に代表される、原料調達から開発、生産、販売に至る伝統的なサプライチェーンが存在する。この事業フローは、各構成企業が連携することで力を発揮する。しかし、チェーンを構成するサプライヤーが十分なセキュリティ対策を講じておらず、サイバー攻撃を受けた場合、サプライチェーン全体が被害を受ける。具体的には、生産ライン全体の停止や、委託していた機密情報・個人情報の流出といった事態をもたらす。

企業の多くは、人事、総務、財務、法務といった管理業務も、外部に委託しているケースが多い。こうした委託先企業がサイバー攻撃を受けた場合にも、同様の被害拡大が生じる。

企業・組織の情報システム構築・保守には、システムインテグレータ[18]と、そこから業務を請け負う多数の IT 企業が関わっている。情報システムは、コミュニケーションや情報共有といった業務の円滑な実施を担うのみならず、事業に係る重要情報や個人情報を取り扱っている。よって、情報システムに携わる関係企業がインシデントを起こしたときのインパクトは甚大である。IT 技術の高度化と、サイバーセキュリティ対策の専門化・高コスト化に伴い、近年は組織の IT 環境管理・セキュリティ業務を、MSP[19]や MSSP[20]と呼ばれる事業者に外部委託することも多い。MSP や MSSP は、受注企業の IT・セキュリティ業務を一任されるため、大きなサイバーリスクを抱えているといえる。前章表 1 の米国の Kaseya 社事例が示すように、IT 運用管理を代行する MSP がランサムウェア攻撃を受けた結果、多数の企業が業務停止に陥っている。

クラウドサービスの普及も、サプライチェーンとそのリスクを拡大する要素の 1 つである。企業・組織の Web サービスやシステムの大半が、クラウドサービスを基盤としている。SaaS の利用や、外部 Web アプリケーションの利用、API[21]を通じた他社・外部サービスとの連携が進み、サードパーティとの関係はこれまで以上に複雑化している。

以下は、サプライヤーに起因するインシデントの想定シナリオをいくつか例示したものである。すべて実際に発生している事象であり、当該リスクの範囲の広さを示すものである。

サプライヤーに起因するインシデントシナリオ例

- 部品製造を担当するサプライヤーがサイバー攻撃を受け、サプライチェーン全体が停止する。
- 人事情報を取り扱う委託業者がサイバー攻撃を受け、従業員情報が流出する。
- 情報システム開発を委託していたシステムインテグレータの下請会社において、開発者がソースコードや機密情報を、アクセス制限を施すことなくインターネット上に保管していた。
- オンラインショッピングサイト運営に利用していた、他社が提供する Web 決済サービスが改ざんされ、自社の顧客情報・クレジットカード情報が流出する。
- 委託先の MSP がランサムウェア攻撃を受け、自社のシステムが暗号化され、かつ犯罪者から身代金を要求される。

2.2. ソフトウェア・サプライチェーンに起因するリスク

事業活動上のサプライチェーンとは別に、ソフトウェアにも独自のサプライチェーンが存在する。IT に携

[18] システムインテグレータとは、企業の情報システム構築を請け負う IT サービス業者のこと.
[19] MSP とは、Managed Service Provider（マネージドサービスプロバイダ）の略語.
[20] MSSP とは、Managed Security Service Provider（マネージドセキュリティサービスプロバイダ）の略語.
[21] API とは、Application Programming Interface の略語であり、アプリケーション同士を連携させる仕組みのこと.

わる者以外にはまだ馴染みの薄い概念と思われるが、今日、各国政府や IT 業界が最も懸念し、対策を急いでいる領域が、ソフトウェア・サプライチェーンとそのリスクと考えられる。

ソフトウェア、すなわちコンピュータ・プログラムは、製造業と同じく、設計、構築、試験、リリース、提供、運用、監視といった一連のライフサイクルに基づいて開発される。このプロセスには、開発環境、OS（オペレーティング・システム）、ハードウェア、クラウドサービス、コードベース（ソースコード[22]の集まり）、オープンソース・プロジェクト[23]、リポジトリ[24]等が関わっている[25]。開発サイクルに用いられるこのようなコンポーネント等をまとめて、ソフトウェア・サプライチェーンと称する（表 2）。例えば、私たちが日常的に業務で活用している電子メールサーバーや、社内ネットワーク等を維持するためのソフトウェアも、多くのライブラリ（特定の処理を行うためにまとめられたパッケージのまとまり）やオープンソース・プロジェクトを組み合わせて作られたものである。

開発者は、プログラミング言語を用いてソースコードを書くことでソフトウェアを作成する。しかし、IT ビジネスの規模が巨大化し、開発からリリースまでが高速化した現代では、プログラマーがゼロからソースコードを書くというケースは稀である。ソフトウェアを形作るソースコードは、多数のオープンソース・ライブラリや、商用ライブラリの組み合わせによって成り立っている。さらに、こうした個々のライブラリも、さらに別のライブラリを組み合わせてできている。このため、ソフトウェア・サプライチェーンは複雑な相互依存関係に基づいた入れ子構造を形成する。近年は、このソフトウェア・サプライチェーンが、攻撃者に付け入る隙を与えるアタックサーフェス[26]となっている。

表 2　ソフトウェア・サプライチェーンの構成要素[27]

段階	設計	構築	リリース	保守
要素	・オープンソース ・ライブラリ ・パッケージ	・開発環境 ・ハードウェア ・リポジトリ	・デジタル署名[28] ・クラウドサービス	・アップデート環境 ・保守環境

開発やリリースのために用いられる環境も含めると、1 つのソフトウェアが保有するサプライチェーンは膨大なものとなる。企業・組織がこうした依存関係を正確に把握することは困難であるため、セキュリティ上の弱点を生む原因となっている。

ソフトウェア・サプライチェーンに起因するサイバーリスクは、現実に生起しており、実際に経験した企業・組織も多いと思われる。2021 年、プログラミング言語 Java で広く利用されているログ記録用のコンポーネント「Apache　Log4j」に深刻な脆弱性[29]が発見された[30]。Log4j は多くのソフトウェアや製品に用いられて

[22] ソースコードとは、プログラミング言語で書かれた、コンピュータ・プログラムを表現するテキストのこと.
[23] オープンソース・プロジェクトとは、無償で利用・再配布可能なプログラムおよびソースコードのこと.
[24] リポジトリとは、ソースコード等のバージョン管理を行う仕組み。Git 等が有名.
[25] RedHat. ソフトウェア・サプライチェーンのセキュリティとは. https://www.redhat.com/ja/topics/security/what-is-software-supply-chain-security. （アクセス日:2022-12-21）.
[26] アタックサーフェス（Attack Surface）とは、攻撃者が攻撃にとりかかれるシステム、人、環境などの境界面.
[27] NCSC. Software Supply Chain Attack. https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf.（アクセス日:2022-12-21）. を元に当社作成.
[28] デジタル署名とは、ソフトウェアが真正であり、改ざんされていないことを証明するプロセスのこと.
[29] ソフトウェアが持つ欠陥・バグであり、予期せぬ動作や、攻撃者による悪用を引き起こす弱点のこと.
[30] IPA. 「Log4shell」は何故これだけ騒がれたのか. https://www.ipa.go.jp/security/sc3/activities/kougekiWG/co

おり、悪用が容易であった。このためインターネット上からの攻撃が多数発生し、多くの組織が対応に追われた。ソフトウェア・サプライチェーン管理の重大性を知らしめた事例である。

国外では、2020 年のロシア政府による米国連邦政府ハッキング事案が有名である[31]。米国連邦政府機関が導入していた、SolarWinds Corporation 社の IT 運用管理製品がハッカーによって攻撃され、大量の情報を窃取された事件である。この事例では、製品のアップデートファイルにマルウェアが埋め込まれ、被害が波及している。

ソフトウェア開発に有用なオープンソースのパッケージ（複数のソースコードを集めたもの）を集めた Web サイトには、多数の悪性パッケージが混在している。ある大手パッケージサイトでは、2022 年だけで 1,500 件を超える悪性パッケージが検知されている。攻撃者は正当な開発元になりすまし、悪性パッケージを開発者に利用させることで攻撃を行うことができる[32]。

また、2022 年に顕著となった傾向として、特定のソフトウェア・コンポーネントの提供者が、政治的主張から自身が提供するソースコードにマルウェアや悪性の動作を潜ませる「プロテストウェア（Protestware）」という攻撃がある。2022 年 3 月には、あるライブラリの作成者が、ロシアによるウクライナ侵攻への抗議を目的として、ロシア国内のコンピュータで利用したときのみ動作する攻撃コードを密かに追加した。

ソフトウェア・サプライチェーンのリスクは、今後もさらに増大していくと考えられる。米国のリサーチ・コンサルティング企業 Gartner 社が公表したセキュリティトレンド予測は、2025 年には、全世界の企業のうち 45%が、ソフトウェア・サプライチェーンに対する攻撃を受けると予測している[33]。

各国も、この新たなリスクに対処すべく様々な法規制が進行中である。米国のバイデン政権は、ソフトウェア・サプライチェーンのセキュリティを確保するための大統領令[34]を発簡した。また、米国の National Security Agency（国家安全保障局、「NSA」）および Cybersecurity Infrastructure Security Agency（サイバーセキュリティ・インフラストラクチャセキュリティ庁、「CISA」）は、ソフトウェア・サプライチェーンに関するセキュリティガイダンスを合同で発行している[35]。大統領令を受けて、Google はソフトウェア・サプライチェーン脆弱性を管理するためのサービスを開始した。[36]

欧州では、ソフトウェア・サプライチェーンを欧州全体で強化するための Cyber Resilience Ac（サイバーレジリエンス法案）が審議中である[37]。当該法案は、EU 域内で流通するすべてのソフトウェア、ハードウェア、IoT デバイス等に、SBOM の導入を義務付けるものである。SBOM（Software Bill of Materials）とは、ソフトウェアを構成するコンポーネントに関する詳細や依存関係を記載したリストであり、いわばソフトウ

---

ntent/column/col-vol02.html. （アクセス日:2022-12-21）.

[31] TechTarget. SolarWinds supply chain attack explained: Need-to-know info. https://www.techtarget.com/searchsecurity/ehandbook/SolarWinds-supply-chain-attack-explained-Need-to-know-info. （アクセス日:2022-12-21）.

[32] DarkReading. Malicious Python Trojan Impersonates SentinelOne Security Client. https://www.darkreading.com/vulnerabilities-threats/malicious-python-trojan-impersonates-sentinelone-security-client. （アクセス日:2022-12-21）.

[33] Gartner. 7 Top Trends in Cybersecurity for 2022. https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022. （アクセス日:2022-12-21）.

[34] NIST. EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity. （アクセス日:2022-12-21）.

[35] NSA. NSA, CISA, ODNI Release Software Supply Chain Guidance for Developers. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3146465/nsa-cisa-odni-release-software-supply-chain-guidance-for-developers/. （アクセス日:2022-12-21）.

[36] Google. A distributed vulnerability database for Open Source. https://osv.dev/ （アクセス日:2022-12-21）.

[37] European Commission. Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. （アクセス日:2022-12-21）.

ェアの「部品表」である。ソフトウェア・サプライチェーンを明確化し、リスク管理を行うことが、EU 域内で活動する IT 企業・製造業にとって必須となる見通しであり、日本にも影響を与えると想定される。

2.3. サプライチェーン攻撃

最後に、「サプライチェーン攻撃」について紹介したい。サプライチェーン攻撃と、サプライチェーンに起因するセキュリティインシデントとは混同される傾向にある。しかし ENISA の定義を引用すると、サプライチェーン攻撃とは、攻撃者がサプライヤーとそのカスタマー（元請企業）との関係を「明確に悪用する」手法のことである[38]。よって、攻撃者の最終目的はサプライヤーを抱えるカスタマーであり、サプライチェーン攻撃には、サプライヤーとカスタマー双方に対する攻撃が伴う。

例えば、米国政府機関からのデータ窃取を目的とした SolarWinds Corporation 社への攻撃は、典型的なサプライチェーン攻撃である。他には、セキュリティ研究者をハッキングすることでソフトウェアの脆弱性情報を盗み出し、これを悪用し別のターゲットを攻撃するという、より高度な方法も確認されている[39]。1 章で紹介した地方自治体医療機関に対するランサムウェア攻撃も、給食業者のネットワークを経由して、身代金恐喝の効果が見込める大規模病院を攻撃するという手口である。

サプライチェーン攻撃は従来、軍や情報機関のハッカー部隊等、国家主体が利用してきた攻撃法である。ところが、サプライチェーンの相互依存の深化や、攻撃技術・防御技術の高度化に伴い、金銭目的のサイバー犯罪者もサプライチェーン攻撃を用いる傾向が強まっている。サイバー犯罪組織の中には、例えばランサムウェア運用者のように、企業等の非国家主体に対する攻撃を通じて、国際紛争に加担する者もいる[40]。民間企業にとっても、サプライチェーン攻撃は対岸の火事ではない。

3. サプライチェーン・サイバーリスクの低減に向けて

サプライチェーン・サイバーリスクは企業・組織の根幹に関わる課題である。そのリスク管理対象は、サプライヤーやサードパーティ、ソフトウェア・ベンダー、ソフトウェア・コンポーネント供給者等多岐にわたる。サプライチェーン・サイバーリスクは範囲が非常に広いため、実際にインシデントが発生したときの損失も大きなものとなる。本章ではまず、当該リスクが組織に与えるインパクトについて触れた後、このリスクを低減・管理する方策について紹介したい。

なお、本レポートはセキュリティ実務者向けの技術的対策（ウイルス対策ソフトの導入等）ではなく、リスク管理のための組織的な方針・施策に焦点をあてる。なぜなら技術的対策は、リスク管理の組織的土台が成立して初めて有効となるからである。

3.1. インシデントがもたらす損失は莫大

セキュリティベンダーの調査では、年間約 6 割の企業が何らかのセキュリティインシデント被害を経験している。そして、インシデントがもたらす年間平均被害額は約 3 億 2850 万円に上るという[41]。また、特定非

[38] 前掲脚注 2
[39] ENISA. Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.（アクセス日:2022-12-21）.
[40] Australian Financial Review. World's most prolific hacking gang threatens Ukrainian allies. https://www.afr.com/politics/federal/world-s-most-prolific-hacking-gang-threatens-ukrainian-allies-20220227-p5a00o.（アクセス日:2022-12-21）.
[41] TrendMicro. 法人組織のセキュリティ成熟度調査を発表. https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20221207-01.html.（アクセス日:2022-12-21）.

営利法人日本ネットワークセキュリティ協会が 2021 年に発行したレポートでは、インシデント対応に係るコストを、ケースにより大きく変わるとしながらも、数百万円から 6 億円と見積もっている[42]。

インシデントの被害は金銭的損失に留まらない。サイバー攻撃被害を受けて機密情報や重要情報、個人情報を窃取された場合、社会的な信用の損失や、競争力の低下を招くことになる。特に個人情報が流出した場合、顧客からの信頼を失うとともに、当局からの制裁を受ける場合がある。個人情報に係る厳格な罰則を導入している欧州では、サイバー攻撃の約 6 割が顧客の個人情報をターゲットにしているとの調査結果も出ている[43]。2022 年 11 月には、国内企業の欧州子会社が General Data Protection Regulation （EU 一般データ保護規則、「GDPR」）[44]に違反したとして罰金を科されている[45]。

サプライチェーン・サイバーリスクがもたらす損失やインパクトは組織活動を揺るがすものである。こうした事実を踏まえ、次節からは、いかにしてこのリスクを取り扱うかを検討する。

3.2. 全社的リスクマネジメントへの統合

サプライチェーン・サイバーリスクマネジメントは、自社を取り巻くサプライチェーンおよびソフトウェア・サプライチェーンを特定し、各構成主体に潜むリスクを把握し、対策を講じ、継続的にモニタリングしていく活動である。一組織を対象としたセキュリティ対策とは異なり、ステークホルダーや関連部門が多いため、情報システム部門やセキュリティ担当者だけに任せる問題ではない。経済産業省および情報処理推進機構が現在制定を進めている「サイバーセキュリティ経営ガイドライン Ver. 3.0」においても、サプライチェーン対策は、経営者が認識すべき 3 原則の 1 つであることが明記されている[46]。

このようなスケールの大きな課題に取り組むにあたって最も重要なことは、全社的枠組みの形成である。

3.2.1. リスクマネジメントの組織化

National Institute of Standards and Technology（米国国立標準技術研究所、以下「NIST」）が公開するサイバー・サプライチェーンリスクマネジメントに関するガイダンスでは、リスク管理のために実施する事項として、題にも掲げた「全社的リスクマネジメントへの統合」を挙げている[47]。サプライチェーン全体のサイバーリスクを管理するためには、これまでに存在しなかった新たなガバナンス体系や枠組みを創設する必要がある。すなわち、組織全体での領域・部門横断的なアプローチを実践し、組織の文化を変えていかなければならない。この枠組みには、各部門、各事業プロセス、サプライヤー、サードパーティが参画することになる。組織を構成する各部門が統一のチームを形成し活動できる環境の整備が必要である。

NIST ガイダンスでは、経営層レベル、事業レベル、運用レベルの各層において、職責に応じたサプライチェーン・サイバーリスク管理活動に取り組むことを推奨している（表 3）。併せて、サプライチェーン・サイバーリスクに特化した専門のプロジェクト・マネジメント・オフィス設置も有効であるとしている。

---

[42] 特定非営利法人日本ネットワークセキュリティ協会. インシデント損害額調査レポート　2021 年版. https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20210910.pdf. （アクセス日:2022-12-21）.
[43] 前掲脚注 2
[44] GDPR は、EU における個人情報保護を定めた法令であり、違反には罰則を伴う.
[45] NIKKEI Asia. NTT Data unit fined for violating EU data protection law. https://asia.nikkei.com/Business/Companies/NTT-Data-unit-fined-for-violating-EU-data-protection-law. （アクセス日:2022-12-21）.
[46] SecurityNext. 「サイバーセキュリティ経営ガイドライン Ver3.0」の意見募集が開始に. https://www.security-next.com/140973. （アクセス日:2022-12-21）.
[47] NIST. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final. （アクセス日:2022-12-21）.

表 3　サプライチェーン・サイバーリスク管理のステークホルダー[48]

レベル	名称	ステークホルダー	活動内容
1	経営層レベル	CEO、CIO、COO、CFO、CISO、CRO 等	• リスク管理戦略の策定 • ガバナンス組織と運用モデルの形成 • 全社リスク把握とリスクアペタイト方針策定 • プロジェクト・マネジメント・オフィス設置
2	事業レベル	各部門管理者（事業、研究・開発、エンジニアリング、調達、購買、安全、会計、品質管理等）	• 事業ごとの戦略策定 • 脆弱性対策およびポリシー、手順、規制の策定 • 事業システム、人員、組織フローに対するリスクアセスメント • リスク管理計画策定と適用 • プロジェクト・マネジメント・オフィスとの連携 • 経営層レベル・運用レベルとの連携
3	運用レベル	企画者、開発者、システムオーナー、品質保証・品質管理担当者、契約担当者、システム管理者	• リスク管理計画の策定とポリシー・要求の実行 • 上位レベルが定めた規制の遵守 • 個別のシステムやソフトウェア開発へのリスク管理策適用 • 事業レベルへの報告

全社的リスクマネジメントへの参加部門としては、情報システム・セキュリティ、調達、リスク管理、生産、ソフトウェア開発、法務、人事などが考えられる。

組織全体でのリスク管理は、いわゆる一次請けに該当する組織・企業だけでなく、チェーンを形成するサプライヤー等の各組織にも要求される。一般的に、組織のセキュリティ部門が持つ権限は非常に限られたものである。取引先やサードパーティに対して特定のセキュリティ対策を要請する場合、そのカウンターパートがセキュリティ担当者だけでは、予算増額や取引価格調整、契約の変更作業、事業部門への適用といったタスクに対処できない等の問題が生起する。

3.2.2. 活動の継続と改善

一般的なリスクマネジメントと同様、サプライチェーン・サイバーリスクマネジメントにおいても、継続的な活動サイクルの確立が重要である。リスクの特定、調査、対策、モニタリングといった基本的なプロセスの繰り返しに加え、各フェーズを精緻化させ、製品開発などの各事業プロセスに、リスク管理活動を組み込んでいくことが効果的である。成熟したリスク管理体制を確立することで、活動を自動化・計量化することも可能となる。

3.3. サプライチェーン統制の指針

本節では、英国の National Cyber Security Centre（英国サイバーセキュリティセンター、「NCSC」）が公開しているガイダンス[49]を参考に、サプライチェーンの統制におけるいくつかの指針を紹介したい。

[48] NIST ガイダンスを元に当社作成.
[49] NCSC. Supply chain security guidance. https://www.ncsc.gov.uk/collection/supply-chain-security. （アクセ

3.3.1. サプライヤーの正確な把握

サプライヤーの特定と把握は、リスクマネジメント活動の開始点であると同時に、最も難しい作業の 1 つでもある。組織が把握すべきサプライヤーは、直接契約関係にあるサードパーティだけでない。その先に存在する孫請け等のフォースパーティもまた統制の対象である。また、自組織やサプライヤーが導入する IT システムのソフトウェア・サプライチェーンも、把握に努める必要がある。

サプライチェーン上の各企業・組織に対しては、ビジネス上の重要性や共有するデータに応じて、影響度や優先順位を付与することが推奨される。ISACA は、各サプライヤーの依存関係・影響度に応じて必要なセキュリティ対策基準を適用することを実践すべきとしている[50]。自組織の顧客個人情報を共有する委託企業と、印刷用紙の納入企業とでは、サプライチェーン・サイバーリスク上の影響度は全く異なる。それぞれの企業に対して要求するべきセキュリティ対策レベルも自ずと変わる。

3.3.2. 基準の提供

サプライチェーンを構成する各組織に対して、一定のセキュリティ対策基準およびインシデント対処指針を提供することを推奨する。セキュリティ対策基準は、前述したとおり、各サプライヤーが持つ影響度に応じたものであることが望ましい。

サプライチェーンにおいてインシデントが発生した場合は、組織・企業間の連携が対処の鍵となる。よって、明確な指針を示すとともに、普段から対処要領等の確認・訓練を行い、事態発生時の混乱や錯綜を最小限に抑えることが有効である。

なお、セキュリティ対策をサプライヤーに対して要請する場合は、法規の遵守も考慮すべき点である。公正取引委員会は、取引先に対するサイバーセキュリティ対策の要請に関して、独占禁止法や下請法を踏まえた指針を公開している[51]。具体的には、下請法に該当する事業者がサイバーセキュリティ対策を講じることで上昇したコストを適切に考慮することや、不明確な根拠に基づいて対策費を負担させたり、セキュリティ製品を購入させたりといった行為を行わないことが示されている。

サプライヤーとの契約に際しては、セキュリティ条項に関するフォーマットの作成や、セキュリティに関する第三者認証の活用による購買・調達プロセスの効率化を図ることを推奨する。

3.3.3. コミュニケーション

サプライチェーン統制を実現するには、各サプライヤーの積極的な関与が大きく影響する。リスク管理プログラムを始めるにあたっては、サプライチェーン全体のセキュリティレベルを向上させるという目的の共有、ならびにセキュリティレベル向上が生み出す利益に関する認識の共有を図ることを推奨する。セキュリティ対策は労力およびコストを伴うものであり、目的・利益の共有なしに各組織と連携を図ることは困難だろう。

併せて、サプライヤー、サードパーティ、さらに CSIRT[52]や ISAC[53]といった関連団体を通じた日常的な情報

ス日:2022-12-21）.

[50] 前掲脚注 11

[51] 公正取引委員会. サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて. https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html. （アクセス日:2022-12-21）.

[52] CSIRT（Computer Security Insident Response Team）とは、コンピュータセキュリティにかかるインシデントに対処するための組織の総称のこと.

[53] ISAC（Information Sharing and Analysis Center)とは、米国から始まった民間業界ごとの情報共有コミュニティ.

共有も、サイバーリスク低減を推進する力となる。攻撃者は、セキュリティ対策の未熟な、攻撃しやすい組織をターゲットにする。同業他社や関連団体との情報共有を通じて、自社やサプライヤーの相対的なセキュリティレベルを認識することは、攻撃を未然に回避する上で非常に役に立つ。

3.3.4. ソフトウェア・サプライチェーン対策は始まったばかり

ソフトウェア・サプライチェーンの管理は、米国の例で示したように、各国・各業界が現在進行形で対策を急いでいる領域である。ソフトウェア・サプライチェーンに起因するサイバーリスクの低減策は、組織の IT 管理部門やソフトウェア開発部門が中心に取り組むことになる。その場合も、全社的なリスク管理枠組みと、サプライヤー、サードパーティとのコミュニケーションが成功の鍵になるだろう。

4. おわりに

本レポートでは、サプライチェーンに起因するサイバーリスクを概観し、そのリスクを管理・低減するための取り組みを紹介した。事業活動におけるサプライチェーンおよびソフトウェア・サプライチェーンはどちらも拡大傾向にあり、我々の経済・社会活動における相互依存性は今後もますます高まっていくと考える。

2022 年に成立した経済安全保障推進法[54]において、重要インフラストラクチャーのサプライチェーン管理に関する対策が規定された。また防衛省では、防衛産業に対するサイバーセキュリティ体制強化のため、下請企業に対する税制優遇措置を計画中である[55]。このように、サプライチェーン・サイバーリスク対策が日本でも進められている。

サプライチェーンに起因するリスクや、サプライチェーン攻撃に対し適切に対策を立てることは、組織の事業のみならず、顧客や経済・社会基盤を守ることにもつながる。この意味で、サプライチェーン・サイバーリスク管理は、組織・企業に課された社会的責任を果たす活動であるともいえる。

今回紹介した取り組みが、サプライチェーンのセキュリティ統制、そして事業発展・拡大の一助となれば幸いである。

[54] 内閣府. 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）. https://www.cao.go.jp/keizai_anzen_hosho/index.html. （アクセス日:2022-12-21）.
[55] 財務省. 令和５年度税制改正要望「防衛産業のサイバーセキュリティ体制の強化のための税制上の所要の措置」. https://www.mof.go.jp/tax_policy/tax_reform/outline/fy2023/request/mod/05y_mod_k_01.pdf （アクセス日:2022-12-21）.

参考文献

NIST. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final. （アクセス日:2022-12-21）.

NIST. Cybersecurity Framework. https://www.nist.gov/cyberframework. （アクセス日:2022-12-21）.

NCSC. Supply chain security guidance. https://www.ncsc.gov.uk/collection/supply-chain-security. （アクセス日:2022-12-21）.

Verizon. 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/. （アクセス日:2022-12-21）.

Richard A. Clarke. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press (July 16, 2019).

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. https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf. （アクセス日:2022-12-21）.

執筆者紹介

髙宮 真之介　Shinnosuke Takamiya
サイバーセキュリティ事業本部事業企画部
企画グループ
上級研究員
専門はサイバーセキュリティ

ＳＯＭＰＯリスクマネジメントについて

ＳＯＭＰＯリスクマネジメント株式会社は、損害保険ジャパン株式会社を中核とするＳＯＭＰＯホールディングスのグループ会社です。「リスクマネジメント事業」「サイバーセキュリティ事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、サイバー攻撃対策等のソリューション・サービスを提供しています。

本レポートに関するお問い合わせ先

ＳＯＭＰＯリスクマネジメント株式会社
営業企画部　広報担当
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-3500

