NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松 法律事務所

NO&T Compliance Legal Update
危機管理・コンプライアンス ニュースレター

2025 年 8 月　No.108

サプライチェーンにおけるサイバーセキュリティリスク対応の近時の動向（1）

弁護士　工藤　靖

はじめに

近時、サイバー攻撃がビジネスのサプライチェーンに影響を及ぼす事案が、業種・業界を問わず報道されています。独立行政法人情報処理推進機構が 2025 年 1 月 30 日に公表した「情報セキュリティ 10 大脅威」では、「サプライチェーンや委託先を狙った攻撃」が組織向け脅威として 2 位に挙げられており、この 10 大脅威としての取扱いは 7 年連続 7 回目と紹介されています。

サプライチェーンにおけるサイバーセキュリティリスクは、DX 化や IoT 化の進展に伴うシステム連携の増加、及びサイバー攻撃の高度化・巧妙化により、企業や社会における安定供給、品質、安全確保に甚大な影響を及ぼす可能性のある重要な脅威として認識されています。本ニュースレターでは、このような脅威状況とそれに対する対応の近時の動向をテーマとして解説します。

1　サプライチェーンにおけるサイバーセキュリティリスクのリスクシナリオについて

そもそもサプライチェーンにおけるサイバーセキュリティリスクには、大きく二つの文脈があります。

一つ目は、自社が調達し、運用しているシステム・ソフトウェアに予め又はファームウェアのアップデート時などに、供給者側のセキュリティ上の脆弱性を利用して攻撃者が組み込んだマルウェア等により生じる事業リスクが挙げられます。海外の事例ですが、あるシステムにマルウェアによるバックドアが仕掛けられていた結果、このシステムが納入・利用されていた多数の政府機関が、このバックドアの実行により情報を奪われたといったケースがあります。

二つ目は、取引先等のシステム・セキュリティ上の脆弱性が攻撃者に悪用され、何らかのネットワークによってつながれた自社システム上のセキュリティに影響を及ぼすことや、サイバー攻撃に起因して発生した取引先等における事業停止等により生じるリスクが挙げられます。

例えば、近時の報道事例として記憶に新しい病院に対するランサムウェア攻撃の事例では、攻撃者が、まず入院患者の食事を納入する給食委託事業者のシステムへ、同システム構築事業者がリモート保守のために設置した VPN 機器の脆弱性を利用して侵入し、次に窃取した病院のサーバ認証情報によりリモートデスクトップ通信を用いて、病院サーバに侵入し、同病院の電子カルテシステムに障害を生じさせました。その結果、被害に遭った病院は、緊急以外の手術や外来診療を停止せざるを得ないなど、通常診療が行えない状況に至っています。また、情報処理サービスとそれに伴う印刷・発送業務の受託等を主な業務とする株式会社に対するランサムウェア攻撃により、最終的に流出が確認された個人情報が約 307 万人分に上り、その影響は当該株式会社の顧客である金融機関、政府機関、地方自治体等を含む約 100 団体に及び、委託関係によるサプライチェーンへの大規模な被害が生じています。このケースでは、ランサムウェア攻撃を受けた被害者から一転して加害者にもなった会社は、ISO 認証等を停止され、影響を受けた地方公共団体は当該株式会社に対し損害賠償請求を行う予定である旨を公表しています。

このようなサプライチェーンにおけるサイバーセキュリティリスクに対する近時の動向について、以下解説します。

2 SBOM（Software Bill of Materials）の活用に関する議論動向について

外部から調達し、運用しているシステム・ソフトウェアにセキュリティ上の脆弱性があり、これを利用して攻撃者が組み込んだマルウェア等により生じる事業リスクへの対応については、調達/運用時において SBOM（Software Bill of Materials）を入手し、その脆弱性について随時確認することが提唱されています。SBOM とは、ソフトウェアの部品構成表を意味し、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す。ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が進む中で、ソフトウェアにおける脆弱性管理等の重要性から、SBOM を利用した管理手法が挙げられており、近時は、国内外でこの SBOM の取り扱いに関する規制が強化されています。

1. 関連するガイドライン等の策定状況

(1) 政府調達における SBOM の取扱いについて

まず、日本政府による調達においてサイバーセキュリティの確保を図るために策定されている政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）4.3.1(1)-4 においては、ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とする場合、SBOM の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定めることとしています。

(2) 重要インフラにおける SBOM の取扱いについて

また、一般的に重要インフラとされる分野においても、監督官庁からのガイドラインにおいて、SBOM の作成、利用について言及されています。例えば、2024 年 10 月 4 日に策定された金融分野におけるサイバーセキュリティに関するガイドラインにおいては、情報資産管理としてのハードウェア・ソフトウェア等の管理において「対応が望ましい事項」として、自社開発のソフトウェア、利用しているサービス（当該サービス事業者が SBOM を提供している場合）について SBOM を整備することが挙げられています。同じく重要インフラの一つとされ、近時ランサムウェアによる不正アクセス被害に関し複数の調査報告が公表されている医療分野においても、医療機器が具備すべき品質や安全性等に関する基本的な要件基準が定められており[1]、同基準 12 条 3 項は、プログラムを用いた医療機器のサイバーセキュリティ確保のための要件[2]を規定しています。この要件の適合性に関しては、JIS T81001-5-1[3]等の規格への適合性が求められています[4]。そして、JIS T81001-5-1 への適合性を確認するに際して、その箇条 8 のソフトウェア構成管理プロセスについての追加確認事項として、医療機器の SBOM を適切に作成することによって確認することが求められています[5]。

(3) IoT 製品のセキュリティ機能の評価・可視化と SBOM の取扱いについて

そして、近年、IoT 製品の脆弱性を狙ったサイバー攻撃の脅威が高まり、EU におけるサイバーレジリエンス法

[1] 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準参照。

[2] ①製品の全ライフサイクルにわたって医療機器サイバーセキュリティを確保する計画を備えること、②サイバーリスクを低減する設計及び製造を行うこと、③適切な動作環境に必要となるハードウェア、ネットワーク及び IT セキュリティ対策の最低限の要件を設定することが要件とされています。

[3] ヘルスソフトウェア及びヘルス IT システムの安全，有効性及びセキュリティ―第 5 – 1 部：セキュリティ―製品ライフサイクルにおけるアクティビティ

[4] 2023 年 3 月 31 日付け薬生機審発 0331 第 8 号　厚生労働省医薬・生活衛生局医療機器審査管理課長による「医療機器の基本要件基準第 12 条第 3 項の適用について」参照。

[5] 2023 年 5 月 23 日付け薬生機審発 0523 第 1 号　厚生労働省医薬・生活衛生局医療機器審査管理課長による「医療機器の基本要件基準第 12 条第 3 項の適合性の確認について」参照。

など、海外においても IoT 製品のセキュリティ対策に関する適合制度の検討が進められていることを受け、日本においても共通的な物差しで IoT 製品のセキュリティ機能を評価・可視化し、適切なセキュリティ対策を講じることを求める制度の構築・運用が進められています。この IoT 製品に関するセキュリティ要件適合評価及びラベリング制度（JC-STAR）は、任意の制度として、経済産業省の主導のもと、独立行政法人情報処理推進機構（IPA）により運用開始に向けた取り組みが進められています。この制度の対象となる「IoT 製品」は、供給者による販売又は利用者による購入の単位となるものであって、意図した目的を達成するための単独の IoT 機器、又は IoT 機器と必須付随サービスとで構成される一式とされており、考慮要素として、①ラベルの対象となる機器が含まれていること、②インターネットプロトコル（IP）を使用したデータの送受信機能を持つこと、③直接・間接を問わず、インターネットにつながる可能性を否定できないこと、④購入時に具備されているセキュリティ機能を利用し、調達者・利用者が自らの意志により事後的にセキュリティ機能を追加することができない又は困難であること、が挙げられています。そして、製品類型毎の特性に応じて、求められるセキュリティ要件、適合基準、評価手順や評価方式がレベル分けして設定されています。このレベル分けの中で、レベル☆3 以上については、政府機関や重要インフラ事業者、大企業の重要なシステムでの利用を想定した IoT 製品類型毎の汎用的な適合基準を定め、それを満たすことを独立した第三者が評価し認証するものとされており、このレベルにおいては SBOM の活用により脆弱性情報を適切に共有し、迅速なパッチ適用を目指す方針が示されています（2024 年 8 月経済産業省商務情報政策局サイバーセキュリティ課「IoT 製品に対するセキュリティ適合性評価制度構築方針」4.5 参照）。

2.　SBOM の活用による効果

このように、外部から調達し、運用しているシステム・ソフトウェアにセキュリティ上の脆弱性があり、これを利用して攻撃者が組み込んだマルウェア等により生じる事業リスクへの対応については、SBOM の作成・提供を通じて、システム・ソフトウェアに対する脆弱性を速やかに把握して、適切に対応することが求められつつあるものと考えられます。2025 年 3 月 13 日付けで警察庁が公表した「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」によれば、脆弱性を有する VPN 機器がランサムウェア被害企業における感染経路の 6 割弱を占めており、こうした脆弱性への適時の対応としても有益なものと考えられます。

そして、このような対応を進めることは、昨今のランサムウェアによる不正アクセスといったサイバー攻撃が企業にとって「通常想定されるリスク」となっている状況においては、サイバーセキュリティリスクに関する法令等遵守体制・損失危険管理体制・情報保存管理体制の構築・運用を求める取締役の善管注意義務としての内部統制システムの整備義務（会社法 362 条 4 項 6 号・同 5 項）[6]を適切に果たすことにもつながっていくものと考えられます。

3　最後に

以上、今回のニュースレターでは、サプライチェーンにおけるサイバーセキュリティリスク管理の近時の動向として、SBOM の作成・利用を通じたシステム・ソフトウェアにおける脆弱性への対応について解説しました。

次回以降のニュースレターでは、取引先等のシステム・セキュリティ上の脆弱性が攻撃者に悪用され、ネットワークによって繋がれた自社システム上で生じるセキュリティリスクやサイバー攻撃に起因して発生した取引先等における事業停止等により生じる自社の事業リスクへの対応について解説します。

[6] 「重要インフラのサイバーセキュリティに係る行動計画」（2024 年 3 月 8 日サイバーセキュリティ戦略本部改定）10-11 頁参照。

[執筆者]

工藤 靖（弁護士・パートナー）
yasushi_kudo@noandt.com, 03-6889-7396（直通）

2007 年に長島・大野・常松法律事務所へ入所後、2014 年から 2018 年にかけて、金融庁検査局及び証券取引等監視委員会事務局へ出向し、金融機関のガバナンス・コンプライアンスの検査や上場企業による開示規制違反の調査等、幅広く法執行に携わる。復帰後は、業種を問わず、行政・刑事事件対応を含む危機管理・不祥事対応、コンプライアンス、金融・証券規制を含む各種レギュレーションに関するアドバイス、サイバーセキュリティ・データプライバシー、コーポレートガバナンスその他一般企業法務を幅広く取り扱う。近時は、サイバーセキュリティにおけるサプライチェーンリスクマネジメントなどの法務リスク・コンプライアンス管理体制の構築・運用についても注力している。2004 年東京大学法学部卒。2006 年東京大学法科大学院、2013 年 The University of Chicago Law School 卒業（LL.M.）。

コンプライアンス・アセスメントのご案内

当事務所の危機管理・コンプライアンスチームでは、事業環境を踏まえ企業のコンプライアンスリスクを分析した上、社内規程その他のコンプライアンス体制の改善に向けたアドバイスを提供するコンプライアンス・アセスメントをご提供しています。対象とする分野を限定した初期的なアセスメントを実施することも可能です。

役員研修、コンプライアンス研修等のご案内

当事務所の豊富な実務経験を活かした実践的な研修プログラムを各種実施しています。最近の不祥事事件からの教訓や、コーポレートガバナンスコード対応を含む最新の法令動向を踏まえ、各社のニーズに沿った内容とさせて頂いています。

ご興味をお持ちの場合や、さらに詳しい情報を知りたい場合は、遠慮なく下記編集者までお問い合わせください。

[編集者]

垰 尚義　パートナー
takayoshi_tao@noandt.com

眞武 慶彦　パートナー
yoshihiko_matake@noandt.com

工藤 靖　パートナー
yasushi_kudo@noandt.com

福原 あゆみ　パートナー
ayumi_fukuhara@noandt.com

深水 大輔　パートナー
daisuke_fukamizu@noandt.com

辺 誠祐　パートナー
tomohiro_hen@noandt.com

渡辺 翼　パートナー
tsubasa_watanabe@noandt.com

長島･大野･常松 法律事務所　www.noandt.com

〒100-7036　東京都千代田区丸の内二丁目７番２号　ＪＰタワー
Tel: 03-6889-7000（代表）　Fax: 03-6889-8000（代表）　Email: info@noandt.com

長島・大野・常松法律事務所は、600 名以上の弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。
（*提携事務所）