サプライチェーンセキュリティ調査

2025年3月17日

一般社団法人　情報通信ネットワーク産業協会

通信ネットワーク機器セキュリティ委員会

内容

１．はじめに

１．１ 背景

毎年 IPA が発表している「情報セキュリティ 10 大脅威」の「組織」の 10 大脅威に「サプライチェーンの弱点を悪用した攻撃」が６年連続で取り扱われるなど、近年サプライチェーンを利用した攻撃が多くなっており大きな問題となっている。

サプライチェーンを利用した攻撃は、サプライチェーンの様々な部分で行われる可能性があるため、全体像が把握しづらく、誰がいつどのように対策を行うのかが分かりづらいという課題がある。

本書では、サプライチェーンセキュリティの入門としてサプライチェーンセキュリティの概要を把握できるように作成したものである。

１．２ 目的

本書では、サプライチェーンセキュリティとはどのようなものなのかの概要を把握できるようにするとともに、サプライチェーンに対する攻撃事例から、攻撃のタイプを分類し攻撃タイプ毎に企業の担当者がどのようなことに注意する必要があるのかの概要を理解できるようになることを目的とする。

１．３ 対象読者

本書の対象読者としては、企業でサプライチェーンセキュリティに関係する部門(調達部門、情報システム部門、開発部門、セキュリティ部門 等)の担当者を対象とする。

２．サプライチェーンセキュリティ概要

２．１ サプライチェーンセキュリティとは

製品の原材料や部品の調達から販売に至るまでの一連の流れやその一連の流れに関わるシステムや組織群をサプライチェーンと呼ぶ。

サプライチェーンセキュリティとは、上記にあるサプライチェーン(製品やサービスの供給連鎖)におけるサイバー攻撃に対策を施すことである。サプライチェーン攻撃は、原材料や部品の調達、製造、管理、配送、販売、消費などの過程で、ソフトウェアやハードウェアに不正なコードや機器を仕込んだり、あるいは情報を盗むものである。

「情報セキュリティ10 大脅威 2024」には、ソフトウェア開発の ライフサイクルに関与する全てのモノ（ライブラリ、各種ツール等）や人の繋がりをソフトウェアサプライチェーン と呼び、このような「ソフトウェアの繋がり」を悪用した攻撃もまた脅威であり、対策が必要である。と記載されている。

「情報セキュリティ 10 大脅威」では、年度毎に発生した社会的に影響が大きかったと考えられる情報セキュリティに置ける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などからなる「10 大脅威選考会」が脅威候補に対して審議、投票を行い、「個人」「組織」の 2 つに分けたセキュリティの脅威を順位づけし、まとめた資料である。

本資料に記載されている「サプライチェーンセキュリティ」に関する脅威は 2019 年から「組織」の 10 大脅威に「サプライチェーンの弱点を悪用した攻撃」が記載されている。さらに 6 年連続で 10 大脅威として取り扱われており、表 2-1 にあるように「情報セキュリティ 10 大脅威 2024」(2023 年に発生した情報セキュリティに関する脅威)では「組織」項目の第 2 位の脅威として扱われている。

取引先や委託先、提供先など多岐にわたるサプライチェーンによる脆弱な部分を攻撃、または経由して標的組織を狙う動きが多いため、外部に対してセキュリティを強固に保つためだけでなく、内部的にもセキュリティ対策を行わなければならないため、組織全体として注意が必要である。

表 2-1 情報セキュリティ 10 大脅威 2024 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
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	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

引用元：情報セキュリティ 10 大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

サプライチェーンに対する攻撃の事例一つとし、ビジネスサプライチェーン攻撃の約 8 割でシステム停止が発生した件がある。

集計期間(2023 年 1 月～2023 年 10 月 31 日)において、日本国内で発生したセキュリティインシデントは 316 件中 14 件(4.4%)がサプライチェーン攻撃によるものであった。いずれも取引先や関係先を踏み台にネットワークや共有システムを介して被害組織に侵入するビジネスサプライチェーン攻撃である。以下、国内で公表されたビジネスサプライチェーン攻撃の被害事例を表 2-2 に示す。表 2-2 の攻撃に使われた手口は海外拠点へのサイバー攻撃を発端に、本社やグループ会社、関連会社にランサムウェアの感染被害が拡散した事例になる。

このように上記表 2-1 の脅威第 2 位である「サプライチェーンの弱点を悪用した攻撃」に脅威第 1 位の「ランサムウェアによる被害」が入ってきているため、上記の順位ごとに注意するだけでなく、全体を見てセキュリティを強化していく必要がある。

表 2-2 国内で公表されたビジネスサプライチェーン攻撃の被害事例

発覚/ 公表年	業種・業界/被害件数	被害内容	発覚原因	攻撃の手口
2023 年	運輸・交通・インフラ/ 1 件	情報漏洩	未公表	ネットワーク共有サーバーへ障害
2023 年	建設・不動産/ 7 件	障害発生(システム停止)、 データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア(Lockbit)
2023 年	水産・農林・鉱業/ 2 件	障害発生(システム停止)、 データ改ざん/破壊、情報漏洩	攻撃者による通知	ランサムウェア(Lockbit)
2023 年	製造/ 3 件	障害発生(システム停止)、 データ改ざん/破壊、情報漏洩	攻撃者による通知/ 自己調査	ランサムウェア(Lockbit)/ ファイルサーバー侵害/ なりすまし
2023 年	医療/ 1 件	情報漏洩	未公表	海外アカウント経由のクラウド プラットフォームへの侵害

引用元：2023 年、サプライチェーンにおけるセキュリティリスク動向～被害事例にみる企業が直面するリスクとは？ | トレンドマイクロ | トレンドマイクロ (JP) (trendmicro.com)

また近年では、「OSINT(オシント)」を活用したサイバー攻撃が増加している。
「OSINT」とは「オープン・ソース・インテリジェンス」の略で、一般公開されているあらゆる情報を収集・分析し、独自の情報を得る手法で、近年サイバー攻撃に対する防衛力の判定にも活用されている。

例えば、OSINT で意図せずに公開されてしまっている内部データや個人情報を収集し、ターゲットとなる企業に属している方のメールアドレスに対して、悪意のあるメールを標的企業に送り付ける（＝標的型メール攻撃）という流れである。これも一部のサプライチェーンの弱点を悪用した攻撃といえるであろう。

ここでは注目すべきポイントとして、攻撃者は闇雲に攻撃しているのではなく、OSINT ツール等で十分に偵察、分析してから攻撃を仕掛けていると説明されている。

この点から自社に関わるサプライチェーンを定期的に監視し、自社で気づけていないセキュリティの盲点を見つけだし、対応することが非常に重要となる。

表 2-3 サプライチェーン統制で重視すべきセキュリティの盲点

引用元：[サプライチェーンのセキュリティ統制入門｜最新動向と調査結果から考える持続可能な取り組み｜ブログ｜NRI セキュア（nri-secure.co.jp）]

２．２ サプライチェーンセキュリティ想定モデル

- ビジネスのサプライチェーン

サプライチェーンは、自社を中心に考えた場合、顧客、委託先、調達先、サービス事業者等の外部の組織や、情報や物をやり取りするための配送業者、通信事業者等との直接の関連があり、また、顧客を中心に考えた場合は、自社が委託先となり、他にも顧客から見た調達先や、委託先、サービス事業者、配送業者、通信事業者と直接の関連がある。それらが連鎖的につながっていくことで全体のサプライチェーンとなっている。顧客、委託先、調達先、サービス事業者、配送業者、伝送業者等も様々なタイプ(委託先であれば、ソフトウェア開発委託、部品の製造委託)があり、それらの特性に応じて生じるリスクも異なる。

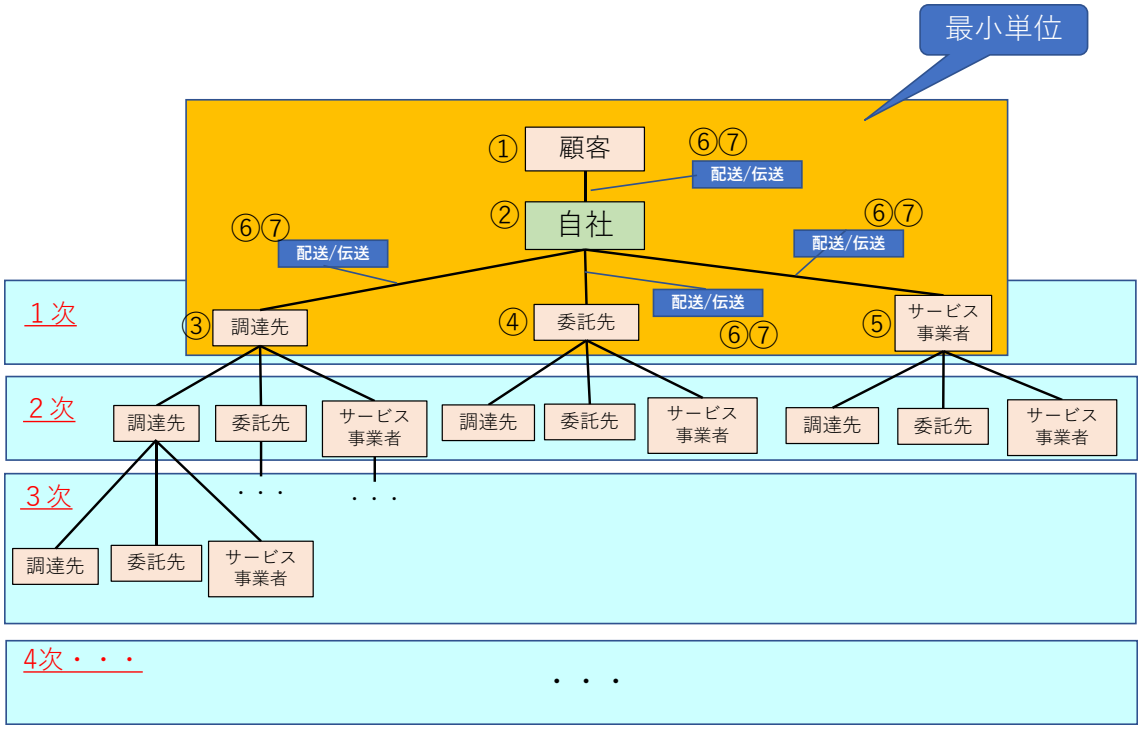

図 2-1 ビジネスのサプライチェーン

最小単位としては①顧客・②自社・③調達先・④委託先・⑤サービス事業者・⑥配送業者・⑦通信事業者の７つからなると考えられる。

番号	アクター	説明
①	顧客	製品やサービスの納入先
②	自社	他社の製品やサービスを自社で利用 他社の製品やサービスを部品として製品を製造し顧客に納入
③	調達先	既製品を販売している事業者(パッケージソフト、HW、部品など)

④	委託先	自社からの委託で製品等を製造する事業者(ソフトウェア開発委託、ハードウェア開発委託)、自社からの委託でサービスを提供する業者
⑤	サービス事業者	既製のサービスを提供する自業者（IaaS、PaaS、SaaS サービス等）
⑥	配送業者	物理的に物を配送する業者
⑦	通信事業者	電子データを伝送するための回線を提供する業者

自社を中心とした最小単位の範囲でセキュリティを確保し、それらを下位に連鎖的に適用させることで、全体のセキュリティの確保につながると考えられる。

- 自社内のサプライチェーン

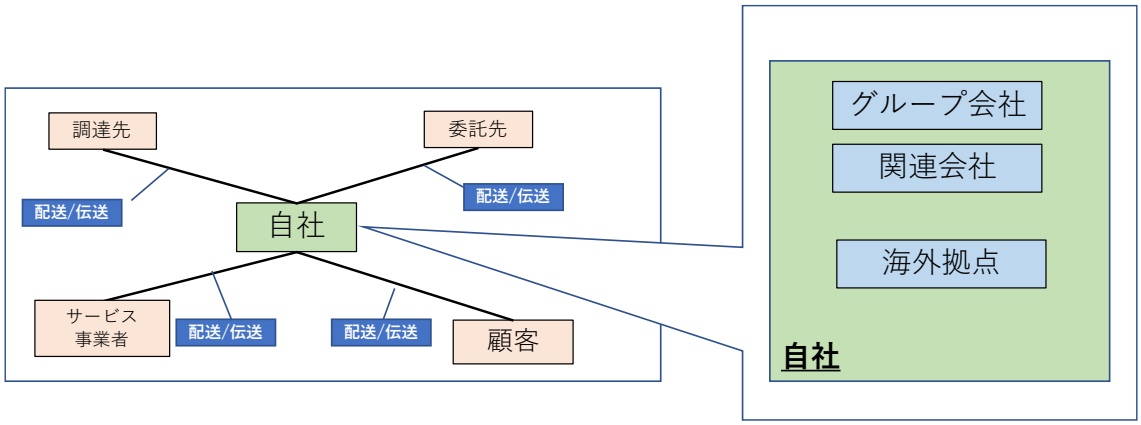

図 2-1 自社のサプライチェーン

自社の中でも、グループ会社、関連会社、海外拠点等とのつながりがあり、それらとのサプライチェーンについても考慮する必要がある。(本社に比べてセキュリティの弱い海外拠点等が狙われ、そこから本社の情報を盗まれるといった事例が発生している)

サプライチェーンのセキュリティ対策ではガバナンスをどこまで効かせられるかが重要になる。自社内であれば直接管理可能であるが、顧客・調達先・サービス事業者・配送業者・通信事業者は直接管理することはできない。また自社内でも、グループ会社、関連会社、海外現地法人等では、本社の関与できる範囲が異なる。ガバナンスをどこまで効かせられるかによってとるべきセキュリティ対策のレベルが異なってくる。

３．サプライチェーン攻撃事例

サプライチェーンに関する攻撃事例について、世界的なニュースになった事例を下記に紹介する。

３．１ 事例① 米国 S 社(ネットワーク管理ソフト開発)

概要	開発時にネットワーク管理ソフトウェアにマルウェアを埋め込み、アップデートを通じて、ソフトウェア利用者を攻撃
攻撃ポイント	開発時点のシステム
攻撃タイプ	ソフトウェアサプライチェーン攻撃
攻撃対象	同社製品導入企業(米国政府、軍も含む) 18,000 団体
攻撃者	Cozy Bear（APT29）：軍事、政府、エネルギー、外交、通信分野をターゲットとするロシア系ハッカーグループ
攻撃者の目的	不明
被害	マルウェア組み込み、サーバーへの不正アクセス
発生時期・頻度	２０２０年１２月
詳細	ハッキングにより、同社のソフトウェアを改ざん、トロイの木馬化し、アップデートを行った利用者に対して、サプライチェーン攻撃を実施。同ソフトウェアを利用する複数の政府機関や民間企業に広範な侵害が発生、多くの顧客が影響を受けた。 一般的な更新システムの悪用は、正規の Web サイトを改ざんすることにより偽のアップデートサイトへ製品ユーザーを誘導し、偽のアップデータを取り込ませることによりウイルスに感染させるが、当事例の場合、ソフトウェアの開発時点からマルウェアを仕込み、正規のサイトからダウンロードさせることで、不正なアップデートであることを発覚しにくくした。

３．２ 事例② 米国 E 社 (消費者信用情報会社)

概要	オープンソースソフトの既知脆弱性を利用し、個人情報を搾取
攻撃ポイント	システムで使用されたオープンソース(製品 A)の既知脆弱性
攻撃タイプ	アイランドホッピング攻撃、ソフトウェアサプライチェーン攻撃
攻撃対象	1 億 4700 万人の顧客情報漏洩
攻撃者	人民解放軍所属のハッカー（※4 人が起訴されたが追加証拠が出ておらず詳細は不明）
攻撃者の目的	不明
発生時期・頻度	2017 年 7 月発生 ・頻度不明
被害	顧客情報流出：1 億 4700 万人分 罰金・和解金：連邦政府、複数の州政府に対して最大 7 億ドルの支払い
詳細	同社 Web サイトのソフトウェア（サーバーソフトウェア A）の脆弱性を悪用され、顧客の生年月日、住所、運転免許証番号などの個人情報にアクセス、少なくとも 20 万 9,000 人のクレジットカード認証情報が盗まれた。 同社のシステムにおいて数多くのソフトウェアが正しくパッチがあてられていなかった(更新されていなかった)ことで侵入され、従業員のクレデンシャル情報の窃取から、重要な顧客個人情報野漏えいに繋がった。

３．３ 事例③ 英国 C 社

概要	英国のソフトウェア開発（C 社）のシステム最適化ツール製品 C に、ユーザーデータを収集するための不正なコード(マルウェア)が仕込まれ 2,300 万台の PC に感染した
攻撃ポイント	(企業買収後の)クリーナーツール
攻撃タイプ	ソフトウェアサプライチェーン攻撃
攻撃対象	製品 C の利用者(大手企業多数)
攻撃者	不明（Axiom との説あり）
攻撃者の目的	不明
発生時期・頻度	２０１７年９月
被害	2300 万台の PC が感染。改ざんされたバージョンを利用した場合、外部から不正に制御できる状態となり、PC 名、IP アドレス、インストールされているソフトのリスト等の情報が外部のサーバーに送られた。
詳細	リモート接続用ソフトを使って同社のネットワークに接続された開発用のワークステーションにアクセスし、そこを足掛かりに他のコンピュータに侵入、悪意ある製品 C のソフトウェア（バックドアを仕掛けたソフトウェア）を用意し、利用者に配布。悪意あるバージョンのソフトのユーザーから情報を窃取したものと思われる。 企業買収の際のデューデリジェンスにおいては財務や法務面のみならず、サイバーセキュリティにも重点を置く必要があるとアンチウイルスソフト開発会社の Avast 社は述べている。

３．４ 事例④ 米国/中国 A 社製品 X

概要	開発ツール X を改ざんした X ゴーストを配布、それを利用して開発されたアプリケーションにマルウェアが混入し、A 社のサイトで配布された
攻撃ポイント	アプリケーションソフトウェア開発ツール(A 社製品 X)
攻撃タイプ	ソフトウェアサプライチェーン攻撃(開発ツール)
攻撃対象	直接的には中国のアプリケーション開発者、間接的には開発されたアプリケーションの全利用者
攻撃者	プログラマー（自首）
攻撃者の目的	単なる趣味
発生時期・頻度	2015 年 9 月発生
被害	X ゴーストによって開発されたアプリがマルウェア化、最終的には 1000 を超えるアプリが感染した。インストールしたユーザーの個人情報を抜き出すことが可能だった
詳細	中国では A 社製品および A 社サイトでのアプリの販売、配布サービスは行われているが、ネットワーク環境により通信速度が非常に遅く、数ギガバイトある製品 X をダウンロードするにはかなりの時間が必要となる。そのため製品 X やその他のアプリを大量にアップロードしたサーバーが存在し、正規の製品 X に改ざんが加えられた X ゴーストもそうしたサーバーにアップロートされていた。 X ゴーストを使用して開発されたアプリはマルウェアに感染した状態で正式な A 社のストア上で配布され、アプリ W（メッセージングアプリ）など多数のユーザーを持つアプリも被害を受けた。これらのアプリをインストールした利用者の端末から、情報を窃取することが可能だった他、特定の URL を開くハイジャックも可能であった。

3．5 事例⑤ ロシア/ウクライナ N 社（製品 M）

概要	ウクライナ N 社の会計ソフト M にマルウェアが仕込まれ、アップデートを通じてウクライナ、ロシア、その他の国へ広められた。
攻撃ポイント	企業やインフラを制御する端末（世界中に拡散）
攻撃タイプ	ソフトウェアサプライチェーン攻撃
攻撃対象	会計ソフトを利用している企業(ウクライナ国内の企業や変電所、空港、決済システムなどの重要インフラ)
攻撃者	Fancy Bear（APT28）：東ヨーロッパの政府、軍、治安機関をターゲットとするロシア系ハッカーグループ
攻撃者の目的	重要インフラの破壊
発生時期・頻度	2017 年 6 月
被害	推定ではランサムウェア感染による売上被害等、被害総額は 100 億ドル以上とされている。
詳細	通常、ランサムウェア攻撃（身代金要求型攻撃）は金銭を目的とし、ターゲットのシステムを停止させたりファイルを破壊してしまうものだが、ロシアが使用したとされるランサムウェア N は金銭目的ではなく、無条件にシステム停止やファイル破壊をおこなうものだったため、重要インフラに大きな影響を与えた。

3．6 事例⑥ 台湾 T 社

概要	IT ハードウェアサプライヤーの 1 社
攻撃ポイント	サプライヤーのソフトウェア(ソフトウェアップデートシステムへのマルウェア)
攻撃タイプ	ソフトウェアサプライチェーン攻撃
攻撃対象	T 社(世界最大級の半導体メーカー)の生産設備
攻撃者	不明
攻撃者の目的	不明
発生日時・頻度	2018 年 8 月
被害	約 250 万ドル(2018 年第三四半期の収益の約 3%相当)、株価 1%下落
詳細	T 社のハードウェアサプライヤーK 社が新しいソフトウェアツールをインストールしていたところマルウェア（ランサムウェア：WannaCry の亜種とされる）に感染、T 社内のネットワークに接続されていたため被害が拡大し、パッチが適用されていなかった 1 万台以上の Windows7 マシンが被害に遭い、台南、新竹、台中の 3 拠点の生産施設で影響が生じた。

３．７ 事例⑦ 日本 P 社

概要	P 社のインド子会社にランサムウェアに感染させサーバーを経由して日本のファイルサーバーにアクセスし個人情報への不正アクセス
攻撃ポイント	海外拠点のサーバー
攻撃対象	日本の本社のファイルサーバー
攻撃タイプ	ビジネスサプライチェーン攻撃(アイランドホッピング攻撃)
攻撃者	不明
攻撃者の目的	不明
発生日時・頻度	2021 年 11 月
被害	不正アクセスを受けたサーバーに保存されていた採用応募者、インターンシップ参加者、及び取引先役員の個人情報流出
詳細	不正にアクセスした海外子会社のサーバーを経由して本社のサーバーにアクセスした例。正常アクセスとみなされたため発見に時間がかかった。発表当時、実際に情報が流出したと確証を得る事実は確認されていなかったものの、同社では流出の可能性を想定し謝罪。その後のアナウンスで一部の情報が実際に流出したことを認め、対象者には順次連絡をしていることを明らかにした。

３．８ 事例⑧ インド W 社

概要	インドの IT サービスプロバイダーW 社のネットワークにハッカーが、アクセスし顧客の機密データを盗み出した。攻撃者は同社のシステムを使用して少なくとも十数社の顧客に対しフィッシング攻撃をおこなった。
攻撃ポイント	サプライヤーである W 社の IT システム
攻撃対象	W 社の顧客
攻撃タイプ	サービスサプライチェーン攻撃
攻撃者	ハッカー(国家レベルのものとされる)
攻撃者の目的	顧客の機密情報
発生日時・頻度	2020 年
被害	W 社の顧客少なくとも 12 社へのフィッシング攻撃
詳細	W 社の従業員を狙ったフィッシング詐欺が入口となり、詐欺にあった従業員のアカウントがギフトカード詐欺の踏み台として使用された。W 社の顧客の多くは標的になりやすい業界、石油・ガス・自動車・航空宇宙・防衛・銀行・医療機関など特に国家の支援を受ける業界に属している。

３．９ 事例⑨ 米国 製品 C

攻撃ポイント	開発ツール（コードカバレッジツール）
攻撃タイプ	ソフトウェアサプライチェーン攻撃
攻撃対象	製品 C を使用して開発されたシステムの利用者
攻撃者	ハッカー(不明)
被害	調査中。世界的企業をはじめ全世界で 29,000 以上の組織が製品 C を利用。
概要	製品 C の開発インフラに不正にアクセスした第三者がスクリプトを改ざんし、利用者の個人情報を盗み出すもの。国内企業が被害にあい、約 17,000 件の銀行口座情報を含む顧客情報、約 8,000 件の加盟店情報が流出した。

３．１０ 事例⑩ 米国/欧州 Dragonfly 2.0 attack

概要	ロシアハッカー集団による、米国、トルコ、スイスなどの送電施設に対する、ソフトウェアの既知脆弱性を利用した攻撃
攻撃ポイント	ソフトウェアの既知脆弱性
攻撃タイプ	ソフトウェアサプライチェーン攻撃
攻撃対象	直接の対象は送電施設、間接的には市民や社会全体が対象
攻撃者	ロシアハッカー集団(Dragonfly 2.0)
攻撃者の目的	情報の窃取
被害	国、トルコ、スイス等の送電施設
発生日時・頻度	２０１４年
詳細	米国政府機関、重要インフラ分野を狙ったサイバー攻撃キャンペーンで、様々な手段を使い、不正侵入し、情報の窃取や攻撃の準備を行っていたものと思われる。 電力等重要インフラへの攻撃は直ちに大きな混乱を引き起こすため、国家にとって大きな脅威である。2016 年ウクライナのキーウではロシアのハッカー攻撃により首都が 1 時間にわたって停電した。インフラのシステムは規模が大きくアップグレードには時間もコストもかかるため、脆弱な状態であることも多いとされる。米国では 2021 年、バイデン大統領がサイバーセキュリティを強化する大統領令に署名し、2023 年には国家サイバーセキュリティ戦略を公表した。

３．１１ 事例⑪ 日本 利用しているサービスの改ざん

概要	サービス提供会社が提供するサービスを改ざんされ、利用していた取引先の複数のサービスから顧客の個人情報が漏洩した
攻撃ポイント	対象サービスに不正アクセスされ、ソースコードを改ざん
攻撃タイプ	サービスサプライチェーン攻撃
攻撃対象	対象サービスのソースコード
攻撃者	不明
攻撃者の目的	対象サービスの利用者が入力した情報
被害	サービス提供会社が提供するサービスを利用していた取引先のサービスで扱われた顧客情報の流出
原因	対象サービスの一部の脆弱性をついたことによる第三者の不正アクセス によりソースコードが改ざんされたことによる
発生時期・頻度	2022 年 10 月

３．１２ 事例⑫ 日本 業務委託先業者からの顧客情報漏えい

概要	複数の保険会社が業務委託先から 顧客の個人情報の流出を公表
攻撃ポイント	業務委託先のサーバー
攻撃タイプ	ビジネスサプライチェーン攻撃(アイランドホッピング攻撃) （ネットワーク上の脆弱な部分を起点とする攻撃）
攻撃対象	サーバー内の個人情報
攻撃者	不明
攻撃者の目的	不明
被害	流出した個人情報が海外の Web サイトに掲載 多いところで約 130 万人分
原因	業務委託先の適切なセキュリティ対策がされていない サーバーへの不正アクセス
発生時期・頻度	2023 年 1 月発生 ・頻度不明

３．１３ 事例⑬ 日本 委託先のシステムを介した顧客情報漏えい

概要	委託先のシステムを介して不正アクセスされ、 顧客情報が漏えい
攻撃ポイント	企業サーバー （但し 関連会社の従業員のウイルス感染が発端）
攻撃タイプ	ビジネスサプライチェーン攻撃(アイランドホッピング攻撃)
攻撃対象	サーバー内の個人情報
攻撃者	不明
攻撃者の目的	不明
被害	ユーザーに関する情報が約 30 万件、取引先等に 関する情報が約 9 万件、従業員等に関する情報が 約 5 万件が漏えい
原因	第三者による社内システムへの不正アクセス 委託先企業である韓国 IT 大手会社のさらに委託先の企業で従業員の PC がウイルス感染したことが発端
発生時期・頻度	2023 年 11 月発生 ・頻度不明

３．１４ 事例⑭ 日本 提携先企業の不正アクセスによる、顧客情報漏えい

概要	通信事業者の提携先企業に不正アクセス、顧客情報漏えい
攻撃ポイント	提携先企業に不正アクセス
攻撃タイプ	ビジネスサプライチェーン攻撃(アイランドホッピング攻撃) （提携先のサーバーに不正アクセス）
攻撃対象	サーバーの個人情報等
攻撃者	不明
攻撃者の目的	不明
被害	当社がメッシュ Wi-Fi（高機能 Wi-Fi 含む：以下メッシュ Wi-Fi）を提供するお客さま、および当社がメッシュWi-Fiを提供するケーブルテレビ事業者様の約 23 万件の顧客の氏名と約 5,000 件の顧客のメールアドレスが漏えい
原因	通信事業者の提供するメッシュ Wi-Fi の提供元の米国 Plume Design 社の提携先のモバイルアプリのアクセスログサーバーが 不正アクセスされたことが原因
発生時期・頻度	2023 年 11 月発生 ・頻度不明

３．１５ 事例⑮ 日本 海外拠点を経由した不正アクセス

概要	大手電機メーカーが約 8,000 台の PC に不正アクセスを受けた
攻撃ポイント	中国に拠点を置く関連会社へ侵入
攻撃タイプ	ビジネスサプライチェーン攻撃(アイランドホッピング攻撃) （セキュリティが脆弱な海外関連会社を起点とする攻撃）
攻撃対象	国内本社の PC 約 120 台、サーバー約 40 台に不正アクセスを実施
攻撃者	不明
攻撃者の目的	不明
被害	個人情報・企業機密の外部漏洩　２ケ月間業務停止 防衛省や内閣府・原子力規制委員会など 10 を超える政府機関や、電力会社・JR など主要民間企業のデータ漏洩が疑われる被害
原因	本国の本社と比較して、海外関連会社のセキュリティが脆弱だった
発生時期・頻度	2019 年 6 月発生　・頻度不明

３．１６ 事例⑯ 日本 外部の委託先を経由した攻撃

概要	総合病院がサプライチェーン攻撃により２ヶ月業務停止となった
攻撃ポイント	医療センターに給食を提供していた事業者を踏み台に、同病院へと侵入しランサムウェア攻撃
攻撃タイプ	ビジネスサプライチェーン攻撃(アイランドホッピング攻撃) （ネットワーク上の脆弱な部分を起点とする攻撃）
攻撃対象	医療センターの約 2,300 台の機器のうち、バックアップを含む基幹サーバー、電子カルテシステム関連のサーバー、パソコン等約 1,300 台
攻撃者	不明
攻撃者の目的	身代金の要求
被害	医療センターの約 2,300 台の機器のうち、バックアップを含む基幹サーバー、電子カルテシステム関連のサーバー、パソコン等約 1,300 台において、ファイルが暗号化される被害が発生
原因	給食提供事業者が VPN 機器のアップデートを行っておらず、ネットワーク上の脆弱性が放置されていた
発生時期・頻度	2022 年 10 月発生 ・頻度不明

３．１７ 事例⑰ 日本 協力会社のシステム停止による、工場の停止

概要	自動車メーカーが協力会社のシステム障害により国内全工場を停止した。
攻撃ポイント	協力会社の子会社の外部企業とのリモート接続機器の脆弱部分
攻撃タイプ	ビジネスサプライチェーン攻撃(物理サプライチェーン攻撃)
攻撃対象	子会社の社内ネットワーク
攻撃者	不明
攻撃者の目的	システム障害を発生させることによる操業停止
被害	協力会社は、ネットワークに侵入されランサムウェア攻撃を受け、 社内の PC やサーバーが暗号化され操業できなくなった。 自動車メーカーが協力会社のシステム障害により国内全工場を停止
原因	協力会社の子会社と外部とのリモート接続機器が脆弱であり そこから侵入されランサムウェア攻撃を受けたことによる
発生時期・頻度	2022 年

４．サプライチェーン攻撃分類

昨今、世界中でサプライチェーン攻撃による被害が発生しています。サプライチェーン攻撃とは、組織間の業務上の繋がりを悪用して次なる攻撃の踏み台とするサイバー攻撃手法全般を指します。
サプライチェーン攻撃の特徴は、本来侵入が難しいセキュリティレベルの高いターゲット組織でも、比較的セキュリティレベルの低い取引先や子会社などを経由することで、ターゲット組織への侵入を可能にすることです。最終的な標的となる組織は、普段の業務上のやりとりを介して侵入されているため、侵入段階で気づくことは非常に困難であり、気づかない間に攻撃を受けていたという状況になりかねません。

サプライチェーン攻撃は、攻撃の起点の違いから 3 種類に分類できます。ソフトウェアサプライチェーン攻撃、サービスサプライチェーン攻撃、ビジネスサプライチェーン攻撃の 3 種類です。

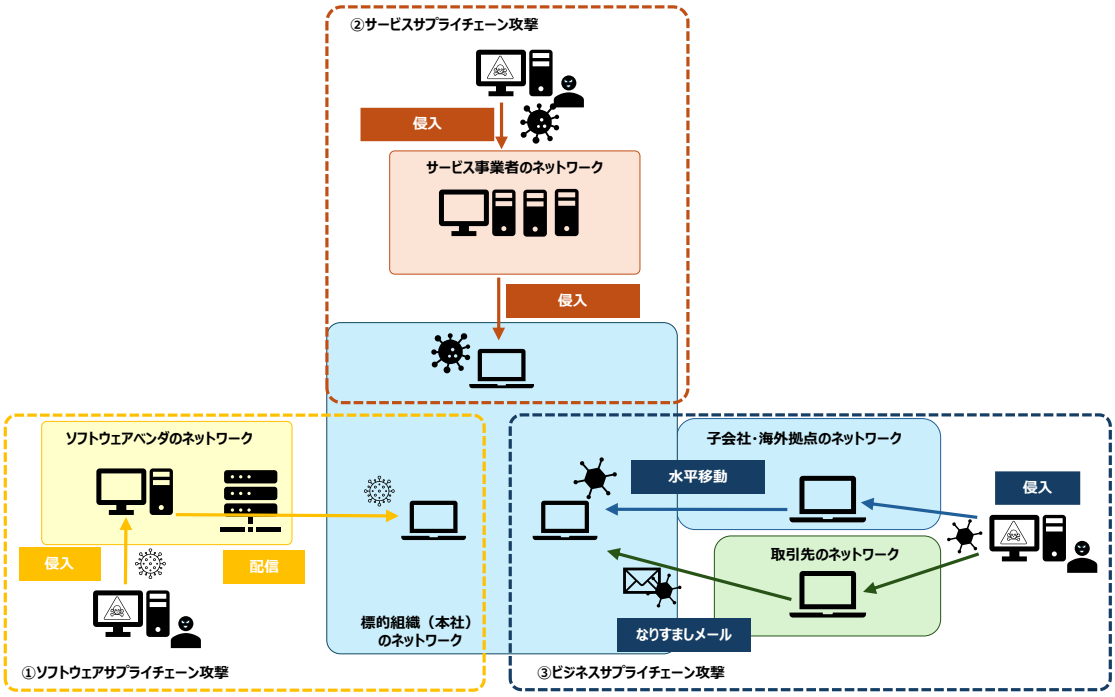

図　4-1 サプライチェーン攻撃の分類

４．１ ソフトウェアサプライチェーン攻撃

ソフトウェアサプライチェーン攻撃とは、ソフトウェアの製造や提供の工程を侵害し、ソフトウェアそのものやアップデートプログラムなどに不正コードを混入し、標的組織に侵入する攻撃です。主な攻撃経路として、オープンソースコード、システム管理ツール、利用するアプリケーションなどが挙げられます。まず、これらのソフトウェアを開発する企業のシステムやソフトウェアのダウンロード元に侵入した後、アップデートサーバーなどを経由して不正なプログラムを含めた「正規のソフトウェア」をターゲット組織に配布（アップデートなど）する手法です。

製造過程や提供元に不正コードが仕掛けられるため、アプリケーションやソフトウェアが幅広い層に使われるほど、被害が大規模になりやすいという特徴があります。

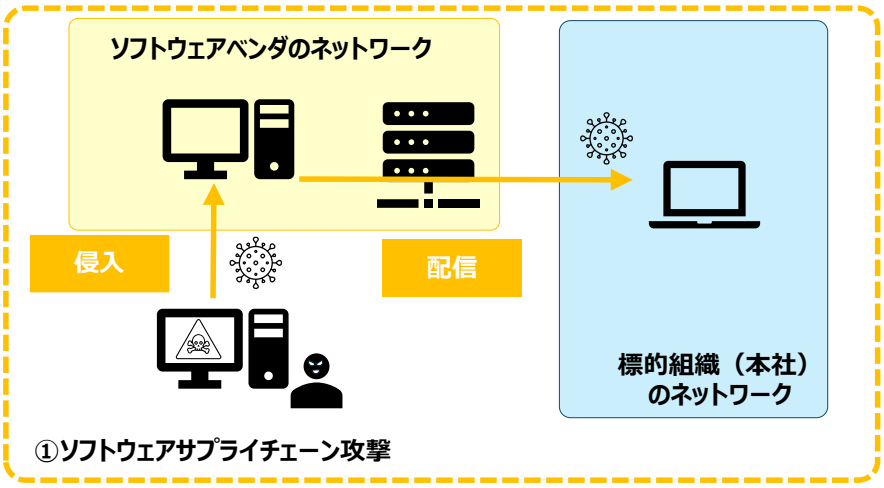

図 4-2 ソフトウェアサプライチェーン攻撃

４． ２ サービスサプライチェーン攻撃

サービスサプライチェーン攻撃とは、MSP（マネージドサービスプロバイダ）などのサービス事業者を侵害し、サービスを通じて顧客に被害を及ぼす攻撃です。MSP サービス事業者自身や、その MSP の顧客である多数の企業などに対するランサムウェア攻撃がサービスサプライチェーン攻撃に当てはまります。MSP 事業者は企業から委託を受けてネットワークの管理や運用を行っているため、攻撃者は MSP 経由で、ランサムウェアを拡散させることが可能となります。

サービスを通じて侵入されれば、サーバーなどが乗っ取られ、各種データにアクセスされることによる情報漏洩、ネットワークの停止といった大きな影響が出る可能性があります。

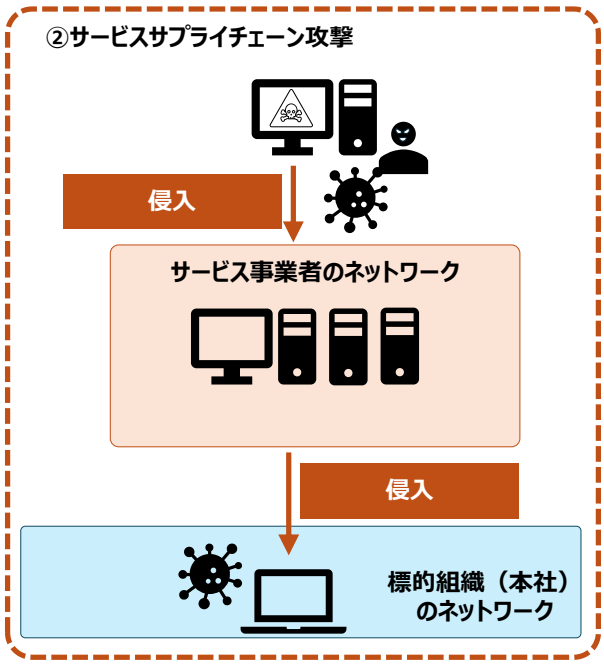

図 4-3 サービスサプライチェーン攻撃

４．３ ビジネスサプライチェーン攻撃（又は、グループサプライチェーン攻撃）

ビジネスサプライチェーン攻撃は、標的組織の関連組織や子会社、取引先などを侵害し、業務上の繋がりを利用して標的組織へ攻撃します。この攻撃は、組織への侵入を行うためにすでに常套手段化されていると言ってもよい段階に入っています。

常習的にやりとりをしている組織を経由した攻撃のため、攻撃に気づくまでに時間がかかり、被害が拡大しやすいといった特徴もあります。

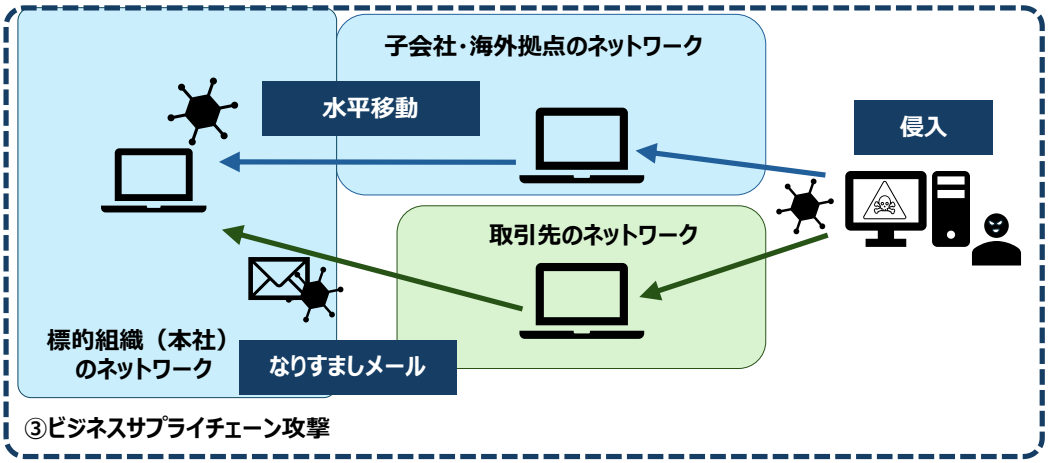

図 4-4 ビジネスサプライチェーン攻撃

- アイランドホッピング攻撃

ビジネスサプライチェーン攻撃の一種として、アイランドホッピング攻撃があります。アイランドホッピング攻撃とは、観光船の島巡りツアーが島から島へと渡っていくように、サプライチェーン内を移動しながら攻撃を進めていく、という手法です。サプライチェーンの中で脆弱性を放置している最も弱い取引先を起点にし、徐々に影響範囲を拡大していくことで、最終的にターゲットへ到達することを目指します。

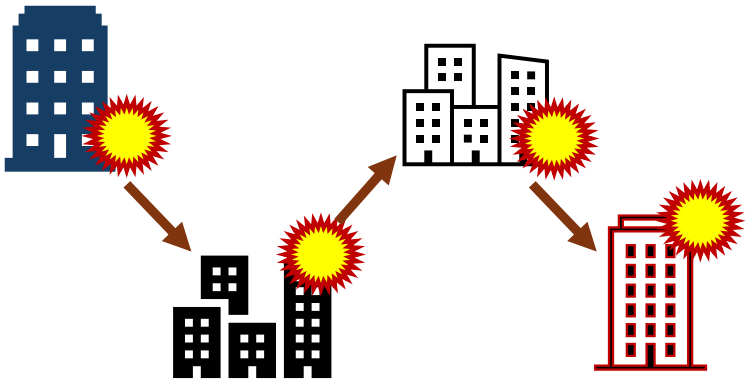

図 4-5 アイランドホッピング攻撃

- 物理サプライチェーン攻撃

また、ビジネスサプライチェーン攻撃の一種として、物理サプライチェーン攻撃があります。物理サプライチェーン攻撃とは、取引先が攻撃されることで、部品供給が滞る物理的な被害が発生します。

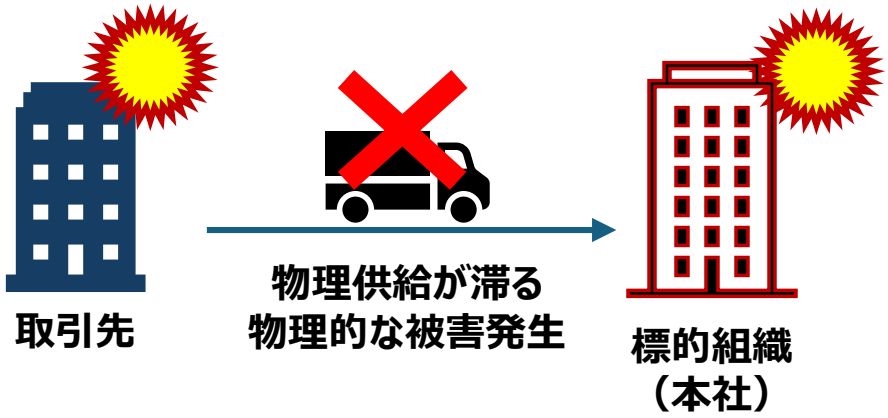

図 4-6 物理サプライチェーン攻撃

４．４ サプライチェーン攻撃分類と事例の対応

３章の攻撃事例が、４章の攻撃分類のどれに対応するかを示す。

表 4-1 攻撃分類と事例の対応

攻撃分類	事例
ソフトウェアサプライチェーン攻撃	事例①、事例②、事例③、事例④、事例⑤ 事例⑥、事例⑨、事例⑩
サービスサプライチェーン攻撃	事例⑧、事例⑪
ビジネスサプライチェーン攻撃	事例②(アイランドホッピング) 事例⑦(アイランドホッピング) 事例⑫(アイランドホッピング) 事例⑬(アイランドホッピング) 事例⑭(アイランドホッピング) 事例⑮(アイランドホッピング) 事例⑯(アイランドホッピング) 事例⑰(物理サプライチェーン)

５．サプライチェーン攻撃対策

５．１ ソフトウェアサプライチェーン攻撃対策

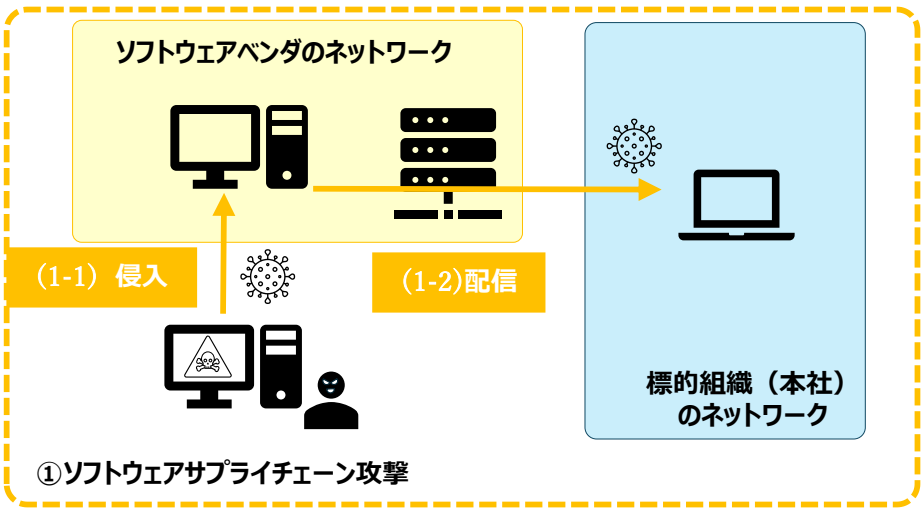

図 5-1 ソフトウェアサプライチェーン攻撃ポイント

ソフトウェアの製造や提供の工程を侵害し、ソフトウェアそのものやアップデートプログラムなどに不正コードを混入し、標的組織に侵入する攻撃です。

本攻撃を防ぐための対策を、ソフトを導入する組織の視点で記載する。

対応 フェーズ	攻撃 ポイント	対策の 主担当部門	対策内容
調達時	1-1	調達部門 情報システム部門	調達先のセキュリティ実施状況の確認 ・外部からの侵入へのセキュリティ対策が適切に実施されているか ・システムの脆弱性対応が適切に実施されているか ・出荷ソフトウェアのマルウェア検査が適切に実施されているか 等
導入時	1-1	情報システム部門	導入時のソフトウェアのマルウェアチェック
運用時	1-2	情報システム部門 利用部門	インストール PC での定期的なマルウェアチェック

5．2 サービスサプライチェーン攻撃対策

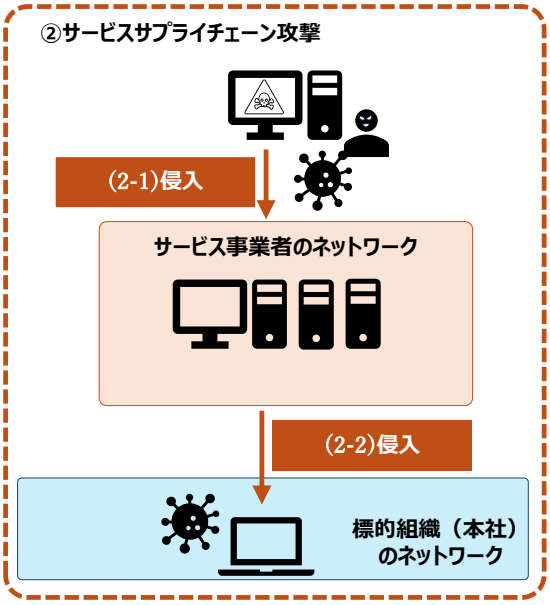

図 5-2 サービスサプライチェーン攻撃ポイント

サービスサプライチェーン攻撃とは、MSP（マネージドサービスプロバイダ）などのサービス事業者を侵害し、サービスを通じて顧客に被害を及ぼす攻撃です。

本攻撃を防ぐための対策を、自社組織の視点で記載する。

対応 フェーズ	攻撃 ポイント	対策の 主担当部門	対策内容
調達時	(2-1)	調達部門 情報システム部門	調達先のセキュリティ実施状況の確認 ・外部からの侵入へのセキュリティ対策が適切に実施されているか ・システムの脆弱性対応が適切に実施されているか ・サービスの定期的なマルウェア対策が適切に実施されているか 等
導入時	(2-2)	情報システム部門	導入時のソフトウェアのマルウェアチェック
運用時	(2-2)	情報システム部門 利用部門	インストール PC での定期的なマルウェアチェック

5．3 ビジネスサプライチェーン攻撃対策

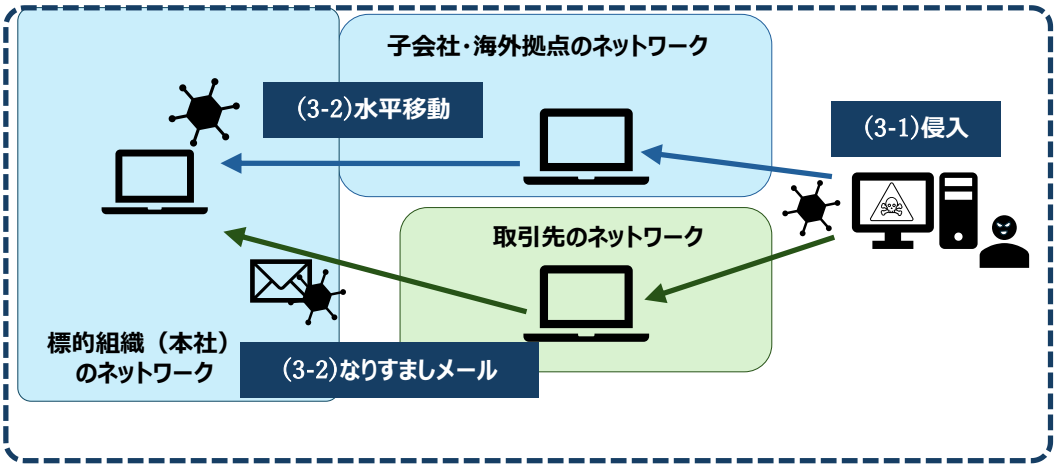

図 5-3 ビジネスサプライチェーン攻撃ポイント

ビジネスサプライチェーン攻撃は、標的組織の関連組織や子会社、取引先などを侵害し、業務上の繋がりを利用して標的組織へ攻撃します。

本攻撃を防ぐための対策を、自社組織の視点で記載する。

対応 フェーズ	攻撃 ポイント	対策の 主担当部門	対策内容
調達時	(3-1) 取引先	調達部門 情報システム部門	調達先・取引先のセキュリティ実施状況の確認 ・外部からの侵入へのセキュリティ対策が適切に実施されているか ・システムの脆弱性対応が適切に実施されているか ・サービスの定期的なマルウェア対策が適切に実施されているか 等
インフラ 構築時	(3-1) 子会社 海外拠点	情報システム部門	子会社・海外拠点のセキュリティ実施状況の確認 ・国内拠点と同等のセキュリティ対応策が実施されているか
運用時	(3-2)	情報システム部門	調達先からの通信については、マルウェア対策等を実施する。
運用時	(3-2)	情報システム部門	子会社・海外拠点からの通信について、それぞれの子会社・海外拠点のセキュリティレベルにあわせて、本社側でもセキュリティチェックを行う

- アイランドホッピング攻撃対策

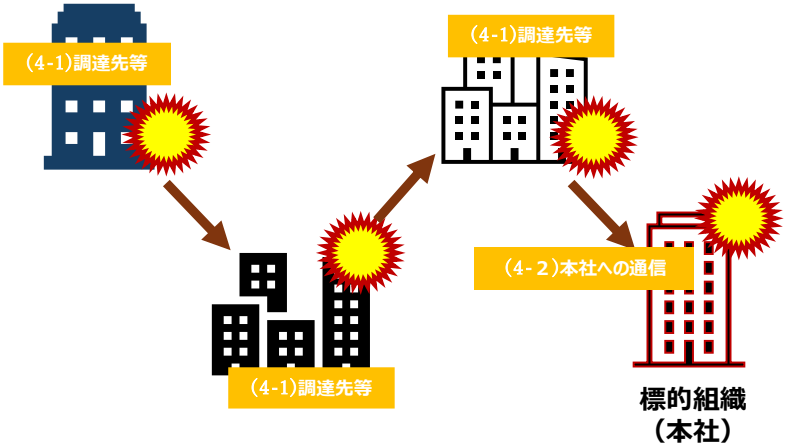

図 5-4 アイランドホッピング攻撃ポイント

アイランドホッピング攻撃とは、サプライチェーン内を移動しながら攻撃を進めていく、という手法です。

本攻撃を防ぐための対策を、自社組織の視点で記載する。

対応 フェーズ	攻撃 ポイント	対策の 主担当部門	対策内容
調達時	(4-1)	調達部門 情報システム部門	調達先・取引先のセキュリティ実施状況の確認 ・外部からの侵入へのセキュリティ対策が適切に実施されているか ・システムの脆弱性対応が適切に実施されているか ・サービスの定期的なマルウェア対策が適切に実施されているか 等 ・調達先・取引先の子会社・海外拠点のセキュリティ状況の確認を行っているか ・調達先・取引先の調達先・取引先のセキュリティ状況の確認を行っているか ・調達先・取引先からの通信については、マルウェア対策等の適切なセキュリティ対応を行っているか
運用時	(4-2)	情報システム部門	調達先からの通信については、マルウェア対策等の適切なセキュリティ対応を実施する

運用時	(4-2)	情報システム部門	子会社・海外拠点からの通信について、それぞれの子会社・海外拠点のセキュリティレベルにあわせて、本社側でもセキュリティチェックを行う

- 物理被害サプライチェーン攻撃対策

図 5-5 物理サプライチェーン攻撃ポイント

物理被害サプライチェーン攻撃とは、取引先が攻撃されることで、部品供給が滞る物理的な被害が発生します。

本攻撃を防ぐための対策を、自社組織の視点で記載する。

対応 フェーズ	攻撃 ポイント	対策の 主担当部門	対策内容
調達時	(5-1)	調達部門 情報システム部門	調達先・取引先のセキュリティ実施状況の確認 ・外部からの侵入へのセキュリティ対策が適切に実施されているか ・システムの脆弱性対応が適切に実施されているか ・サービスの定期的なマルウェア対策が適切に実施されているか 等 ・調達先・取引先の子会社・海外拠点のセキュリティ状況の確認を行っているか ・調達先・取引先の調達先・取引先のセキュリティ状況の確認を行っているか ・調達先・取引先の調達先・取引先からの通信については、マルウェア対策等の適切なセキュリティ対応を行っているか

６．最新動向

６．１ SBOM

サプライチェーンを利用した攻撃として、４．１節で説明したようなソフトウェアサプライチェーン攻撃がある。ソフトウェアサプライチェーン攻撃は、外部から導入したソフトウェアに脆弱性があり、その脆弱性を利用して攻撃を行う攻撃方法である。

これらの攻撃を防ぐためには、自社で利用しているソフトウェアの情報を把握し、それらの脆弱性が見つかった場合には開発元が提供している脆弱性パッチを速やかに適用するなどの、脆弱性対応が必要となる。しかし、オープンソースソフトウェアの利用が一般化していることなどから、外部から導入したソフトウェアについて内部でどのようなソフトウェアを利用しているのかを正確に把握するのが難しいという問題がある。

そこで、ソフトウェアの開発元が SBOM(Software Bill of Materials)と呼ばれるソフトウェアの部品表を作成することでこの問題を解決する取り組みが行われています。

日本では、経済産業省が「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」を発行しており、その中で SBOM に関する基本的な考え方や、SBOM を活用することによるソフトウェア脆弱性管理のメリット等が説明されています。

７．参考文献

- 「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)」（経済産業省）
- 「情報セキュリティ 10 大脅威 2024」
  （独立行政法人 情報処理推進機構）

サプライチェーンセキュリティ調査

一般社団法人　情報通信ネットワーク産業協会
〒103-0026　東京都中央区日本橋兜町 21－7
HF 日本橋兜町ビルディング 6 階
電　話　03-5962-3450
ＦＡＸ　03-5962-3455