【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足がかりとして攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりを足掛かりとする(ソフトウェアサプライチェーン)攻撃も存在する
- 取引先や業務を委託している外部組織から情報漏えいする

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

IPA

- **攻撃手口**

・サプライチェーンの中でセキュリティが脆弱な組織を狙う

- **標的組織の取引先や委託先を攻撃し、それらが保有する標的組織の機密情報を狙う**
- **ソフトウェア開発元やMSP(企業システムの運用・監視等を請け負う事業者)等を攻撃し、標的を攻撃するための足掛かりとする**
  - ソフトウェアのアップデートにウイルスを仕込み、アップデートを適用した利用者にウイルスを感染させる等

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **2023年の事例/傾向①**
  - **業務委託先業者からの顧客情報漏えい**
    - 2023年1月、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した
    - 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が原因であった
    - 流出した個人情報が海外のWebサイトに掲載されていた
    - 流出の規模は、多いところで約130万人分であり、調査や対処に追われた

【出典】 個人情報流出に関するお詫びとお知らせ(アフラック生命保険株式会社)
https://www.aflac.co.jp/news_pdf/2023011001.pdf
個人情報漏えいに関するお詫びとご報告(チューリッヒ保険会社)
https://www.zurich.co.jp/customerdata/
個人情報流出に関する再発防止策について(アフラック生命保険株式会社)
https://www.aflac.co.jp/news_pdf/20230710.pdf
個人情報漏えいに関する追加のお知らせ(チューリッヒ保険会社)
https://www.zurich.co.jp/aboutus/news/news/2023/0117/

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **2023年の事例/傾向②**
  - **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**
    - 2023年11月、LINEヤフーは同社の保有する顧客情報が漏えいしたことを公表
    - 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
    - 第三者による社内システムへの不正アクセスが原因
    - 委託先企業であるNAVER Cloud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

【出典】 不正アクセスによる、情報漏えいに関するお知らせとお詫び(LINEヤフー株式会社)
https://www.lycorp.co.jp/ja/news/announcements/001002/

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **2023年の事例/傾向③**
  - **提携先企業に不正アクセス、顧客情報漏えい**
    - 2023年11月、JCOMが顧客情報を漏えいしたことを公表
    - JCOM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
    - 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

【出典】 お客さまの個人情報漏えいに関するお知らせとお詫び(JCOM 株式会社)
https://newsreleases.jcom.co.jp/news/20231122_9239.html

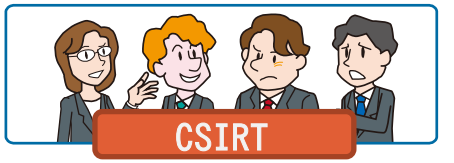
【2位】サプライチェーンの弱点を悪用した攻撃

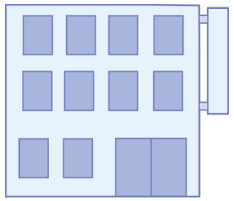
～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(経営者層)**

【被害の予防】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする





【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織で実施)**

【被害の予防】

- 情報管理規則の徹底
- セキュリティ評価サービス(SRS)を用いた自組織のセキュリティ対策状況の把握
- 信頼できる委託先、取引先、サービスの選定
- 契約内容の確認
- 委託先組織の管理
- 納品物の検証(ソフトウェアの把握や管理※1 、脆弱性対策の実施等)

【出典】 ※1 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」を策定しました(経済産業省)
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織で実施)**

【被害を受けた後の対応】

- インシデント対応体制を整備し、対応する
- 被害への補償

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

【被害の予防】

- 取引先や委託先との連絡プロセスの確立
- 取引先や委託先の情報セキュリティ対応の確認、監査
- 情報セキュリティの認証取得
- 公的機関等が公開している資料※1の活用

【出典】 ※1 サイバーセキュリティ経営ガイドラインと支援ツール(経済産業省)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書(内閣サイバーセキュリティセンター)
https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
自動車産業サイバーセキュリティガイドライン(一般社団法人日本自動車工業会)
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

【2位】サプライチェーンの弱点を悪用した攻撃

～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等