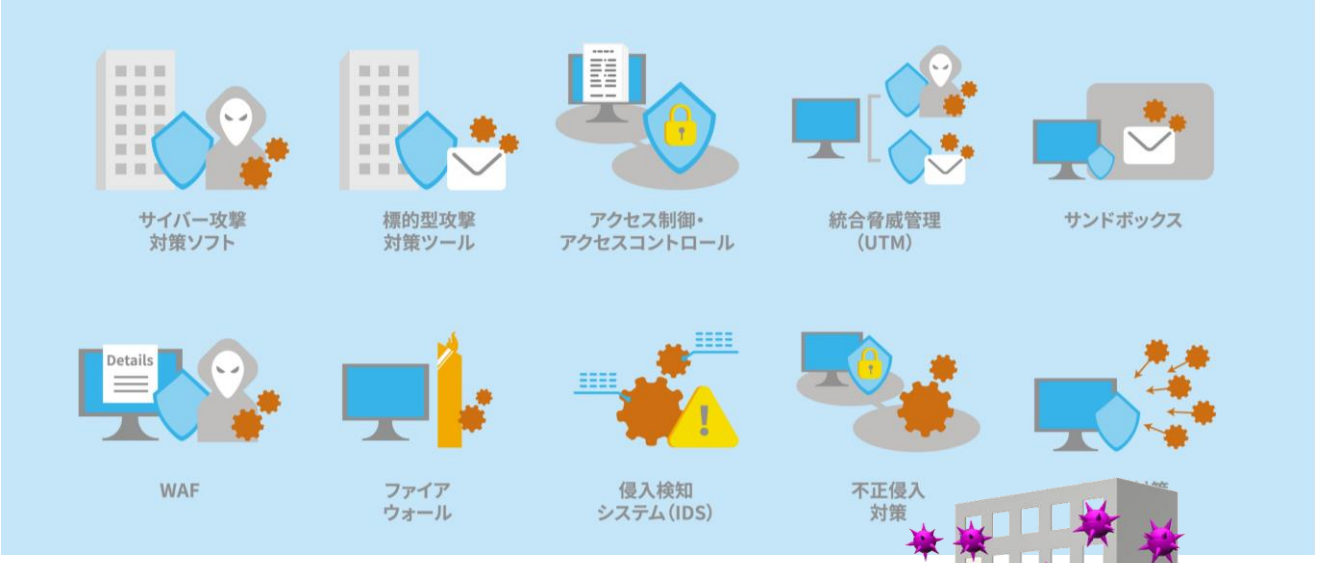
# Yamaichi Magazine

# Vol,22




## サプライチェーン攻撃とは？

### 中小企業におけるサプライチェーン攻撃へのセキュリティ対策

# ～ 目 次 ～

# はじめに

## サプライチェーン攻撃とは？
## 中小企業におけるサプライチェーン攻撃へのセキュリティ対策

「サプライチェーン攻撃」とは、中小企業への攻撃を足掛かりに、最終的にターゲットの大手企業に侵入しようとするサイバー攻撃の手口です。近年、大手企業の取引先や、サプライチェーン内の中小企業にとっても、重大な脅威として注目されています。

国内でも大手自動車メーカーや大規模病院において、サプライチェーン攻撃から操業停止や復旧に長期間かかったりと、ニュースにもなっていたのを覚えておられる方もいらっしゃると思います。

今回のYamaichi_Magazineでは、サプライチェーン攻撃のパターンや、中小企業としての不正アクセスを防ぐための対策、セキュリティ強化策をお伝えしてまいります。

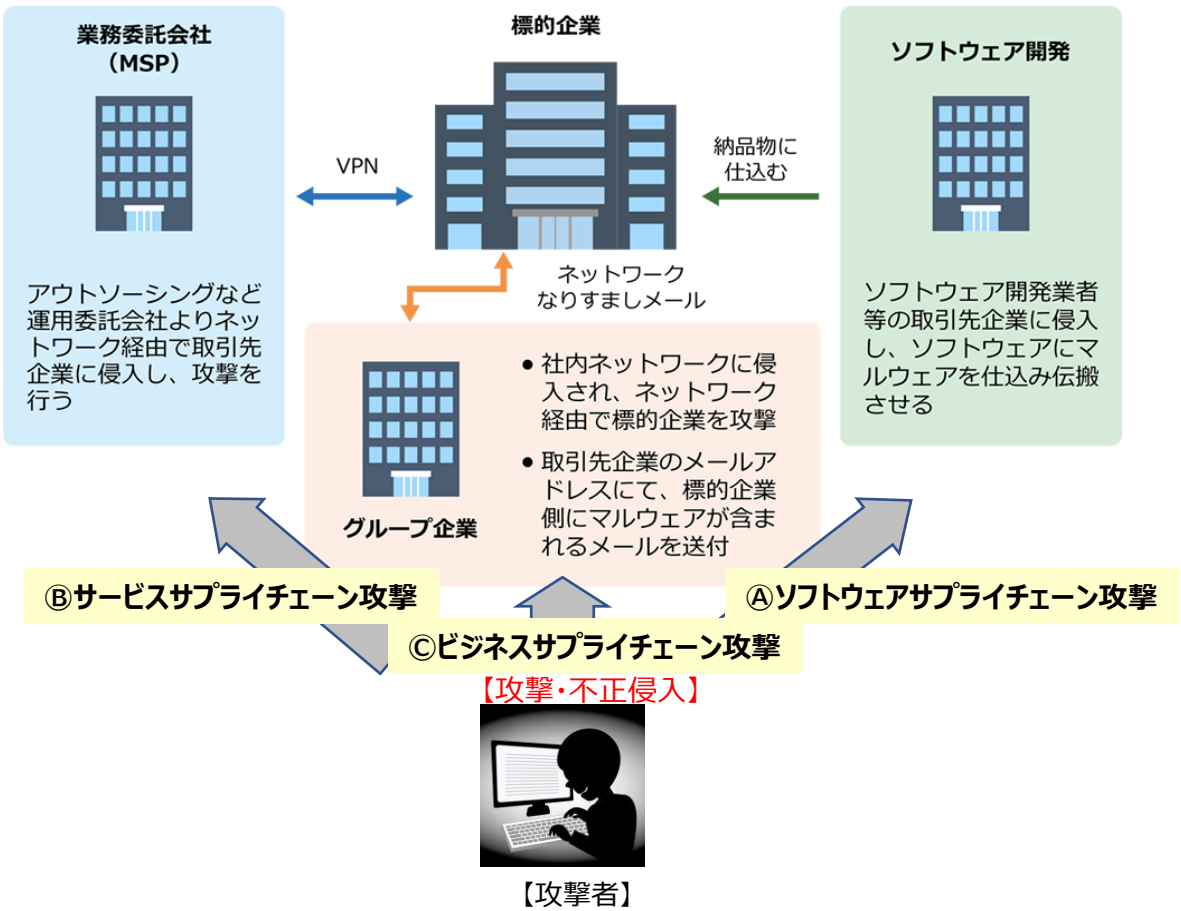
# 1、サプライチェーン攻撃とは？

「サプライチェーン」とは、原材料や部品調達から、製造、在庫、物流、販売のプロセスのつながりと、そこに関わる会社などの組織のことを指します。一般的には、製造業のことを思い浮かべる方が多いと思いますが、サプライチェーン攻撃においては、製造業だけでなく、ビジネスで取引関係を持つ複数の企業の連鎖として広くとらえる必要があります。つまり、ほぼ全ての企業は、何らかのサプライチェーンに属しているという事です。

サプライチェーン攻撃では、セキュリティ対策が遅れがちな中小企業を経由して、セキュリティが強固で直接的な攻撃が難しい大手企業への侵入を狙う手口です。大手企業としては、自社内のセキュリティレベル向上だけでは防げない脅威として、注意喚起される一方、サプライチェーン内の調達や物流に携わる中小企業にとっても対処しなければならない重大な問題として認識しなければなりません。

## ◇「サプライチェーン攻撃」の手口

サプライチェーン攻撃の手口は、主に次の3つのパターンに分類できます。



A) **ソフトウェアサプライチェーン攻撃**
ＩＴ機器やソフトウェアの開発元を狙う攻撃です。開発元に対して不正アクセスを行い、ソフトウェアやサービスにウィルスやマルウェアを仕掛けたりする事でソフトウェアやサービスの利用開始時や、バージョンアップ時にシステムに侵入し、ウィルスに感染させます。

B) **サービスサプライチェーン攻撃**
ウェブサービスを提供する事業者を経由して、ターゲット企業の情報を狙う方法です。ＩＴシステムの保守を担う事業者や、クラウドサービスを提供する会社を経由して、ターゲット企業のシステムに侵入します。そのサービスを利用する複数の顧客など、被害が広範囲に及ぶケースもあります。

C) **ビジネスサプライチェーン攻撃**
ターゲットを含むサプライチェーンの関連企業や、取引先、子会社などのシステムに侵入して標的を狙う手口です。セキュリティ対策が不十分な関連会社に対して、マルウェアを仕掛けたメールを送信したり、委託先を経由して標的のシステムに不正アクセスしたり、ランサムウェアを仕掛けたりします。

## ◇「サプライチェーン攻撃」の被害事例

【ソフトウェアサプライチェーン攻撃の事例】

ウイルス対策のソフトウェアメーカー
2017年、ウイルス対策を展開しているソフトウェアメーカーのシステムクリーナーツールにマルウェアが仕込まれ、利用している多くの企業に影響が出ました。導入している企業には大手IT企業も多く、大量のPCが被害にあっています。

【サービスサプライチェーン攻撃の事例】

アメリカのアクセス管理会社
2023年、アメリカに本社を構えるクラウド型ID管理・統合認証サービスを展開する企業のセキュリティツールのサポートシステムが攻撃され、顧客データが窃取されました。この攻撃により、ほとんどのユーザー企業の情報が漏洩したとされています。

【ビジネスサプライチェーン攻撃の事例】

大手自動車メーカー
2022年、大手自動車会社に部品を提供しているメーカーがサイバー攻撃を受け、マルウェアに感染しました。そこからサプライチェーンを経由し、中核企業およびグループ企業の工場まで停止しています。その結果、グループ全体に大きな損害が発生しました。

# 2、サプライチェーン攻撃から身を守る方法

サプライチェーン攻撃から身を守り、自社と取引先の情報漏えいを防ぐためにどのような対応が必要でしょうか。
サプライチェーン攻撃とはいっても、最初に攻撃される企業にとっては、通常のサイバー攻撃と何ら変わりありません。

主なセキュリティ対策、考え方については、以下のとおりです。

## 1：迷惑メール対策

『迷惑メール対策』では、危険なメールからサイバー攻撃を受けないための対策です。迷惑メールを受信しない、怪しい添付ファイルやURLを無効化して受信する、といった対策があります。

- **迷惑メールを受信しない仕組みを導入する**
  ウイルス対策ソフト、UTM、迷惑メールフィルターなど複数の対策を組み合わせることが重要です。

- **受信した怪しいファイルやURLを無効化する**
  受信したメールを検査し、怪しい添付ファイルを削除する、URLを安全なものに変更もしくは削除する、といったサービスがあります。

- **迷惑メールについて社員教育を行う**
  怪しいメールは、「開かない」「クリックしない」「情報を入力しない」ことが大切です。社員へのセキュリティ教育を行うことでリスクを減らす対策は「人的防御」と呼ばれ、非常に重要です。


## 2：多層防御（たそうぼうぎょ）

**『多層防御』とは、「複数のセキュリティ防御策」のことです。**

一つの対策が破られても次の対策で防御する、あるいは速やかに検知するといった、多層防御は、情報セキュリティ対策の基本です。

| | | |
|---|---|---|
| 1層：「ネットワーク入口」 | … | 外部から不正な通信が入り込むことを防ぐ対策 |
| 2層：「ネットワーク内部」 | … | 入口対策をすり抜けた不正な通信に対する対策 |
| 3層：「ネットワーク出口」 | … | 外部との不正な通信や情報持ち出しを防ぐ対策 |
| 4層：「データ」 | … | 重要なデータが破壊・改竄されても復旧できるようにバックアップする対策 |

この4つの観点から、UTM、ウイルス対策ソフト、メールフィルタ-、バックアップシステム、ログ管理システム等、複数の対応策を組み合わせる事でセキュリティレベルを上げることができます。

## 3：脱PPAP

**『脱PPAP』とは、暗号化した圧縮ファイルをメールに添付し、別のメールでパスワードを送る手法を取りやめる動きです。**

P：PasswordつきZIP暗号化ファイルを送ります
P：Passwordを送ります
A：A（暗号化）
P：Protocol（プロトコル）

「電子メールでファイルを送受信する際に、ファイルを暗号化し、暗号化したファイルとその解除用パスワードを、別々のメールで送る手法」ですが、近年、PPAPには多くのセキュリティリスクがあるとの認識から「脱PPAP」が進んでいます。

- 暗号化されたファイルは、ウイルスチェックをすり抜けてしまう
- 暗号化形式の脆弱性
- 送信ミスなどによる情報漏えいのリスク

以上のようなリスクから暗号化ファイルをメールで送信することを禁止する動きが、近年広がっており、クラウドストレージの利用が、一般的な対応策として広まりつつあります。ウイルスチェックといったセキュリティ対策や、アクセス制限、ダウンロード回数の制限、ダウンロード通知機能等、セキュリティに対応したクラウドストレージサービスが活用されています。

---

## 4：ログ管理

『ログ管理』とは、いつ、誰が、どこで、どの端末で、何をしたか、といった履歴をデータで残し、それによって外部からの攻撃の早期発見や、内部からの情報漏えいの抑止などを図る対策です。また、実際に被害に遭った場合も、ログは調査に欠かせない情報です。

対象となるログは様々で、何を対象とし、どのようなデータを記録し、そして管理・運用するかは、業種・業態・目的などよって異なります。自社で重視している点を整理しながら、導入ツール、サービスを検討し、運用方法・体制についても検討が必要です。

ツールとしては、ログ管理もできる高機能なIT資産管理ツールから、クラウド版ツール、Microsoft 365「監査ログ」の活用まで、自社の状況に合わせたツールを選ぶことが必要です。

## 5：ゼロトラスト

『ゼロトラスト』とは、「境界型防御内のネットワークは安全で、境界外部のネットワークは危険だ」という従来の考え方に対して、「たとえ境界内部であっても無条件に信用せず、全てにおいて確認し認証・認可を行う」という概念です。

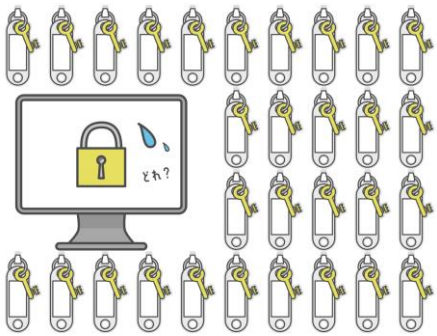
出典:「ゼロトラスト移行のすゝめ」（IPA、P5　第1章：はじめに　1.1.ゼロトラストとは）

従来のセキュリティ対策の考え方は「境界型防御」とも呼ばれ、侵入されないように守る対策です。一方、ゼロトラストは、社内のデータなどにアクセスするもの（人、端末、アクセス元など）をすべて信用せず、毎回その安全性を検証することで、被害を防ぎます。近年、テレワークの普及やクラウドサービス利用の急増などにより、社外で仕事をする、社外（クラウド上）でデータ運用を行うといったことが一般的になってきました。このような背景もあり、ゼロトラストセキュリティの考え方をもって対策していく事が広まってきました。

- **「誰も信用せず、全部確認する」**
- **3つの原則　　：①明示的に検証する　②最小限の特権アクセス　③侵害を想定する**
- **6つの基本的な柱：①ID　②ﾃﾞﾊﾞｲｽ　③ｱﾌﾟﾘｹｰｼｮﾝ　④データ　⑤インフラ　⑥ﾈｯﾄﾜｰｸ**

例えば、クラウドサービスを利用する際のワンタイムパスワード、多要素認証といったものはID統制であり、ユーザーの認証を強化する仕組みです。また、ログの収集や監視・分析も有効な対策の一つです。社内・社外問わず、ログを管理することで、サイバー攻撃の検知や情報漏えい対策に役立てられます。

大企業を中心にこのゼロトラストへの移行が進んでいますが、中小企業には難易度が高いセキュリティ対策と言えます。中小企業のお客さまにおいては、まず境界型防御を整備し、さらに自社に必要なサービスを検討されることが現実的な対策になると思われます。



# 3、サプライチェーン全体で実施するセキュリティ対策

サプライチェーン攻撃を防ぐには、自社のセキュリティ対策だけでは不十分です。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ためには、サプライチェーン全体で連携して対策に取り組む必要があります。

**サプライチェーン全体のリスク評価の実施**
サプライチェーン攻撃の被害を防ぐため、業務委託や情報管理における規則の徹底が非常に大切です。日頃から取引先や委託先、利用しているサービス提供会社の情報セキュリティ対応状況の確認や監査を行います。

**サプライチェーン全体のセキュリティ管理体制や監視体制の構築**
サプライチェーン全体にわたるセキュリティ管理体制を構築し、セキュリティ管理責任者を明確にしましょう。また、取引先や関係会社との契約書に、セキュリティ管理に関する規定を明確にすることも重要です。報告体制や問題発生時の対応計画の整備を行うとともに、適宜見直しましょう。さらに、情報漏えいが発生した場合に備えて、どの情報がどれだけ漏えいしたか等を後から調査できるように、パソコンの操作ログ等を収集する仕組みの導入も必要です。

① 委託契約時の重要情報の明確化と取り扱いを規定
契約時に重要な情報を明確にして、どのように取り扱うかを決めることが大切です。また、攻撃を受けた場合の発覚後の報告など、事後の対策を事前に準備しておくことも重要です。

② 該当情報を管理するドメインを明確にして運用する
重要情報は、定められたドメイン内に留め、扱う場所・人・ＩＴ情報機器等を明確にして運用管理し、情報漏えいリスクを回避しなければなりません。個人利用の持ち込み端末やＵＳＢ等、脆弱性のあるＩＴ機器は、この重要情報のドメインに持ち込まないようにするべきです。

製造業においての注意点
製造業等においては、納品物の検証や出荷検査を徹底し、模造品や脆弱なソフトウェアが紛れ込む、または出荷しないように注意します。さらに、原料や部品の調達先を複数用意しておくことで、サプライチェーン寸断による生産停止や出荷遅延等のリスク低減につながります。

# 4、まとめ

サプライチェーン攻撃は、セキュリティ対策が手薄な中小企業を攻撃し、その中小企業を経由してセキュリティ対策が強固な大企業などへ侵入・攻撃するサイバー攻撃の手法です。
知らないうちに自社が侵入経路となってしまうと、ビジネスにも大きな影響を与えてしまいます。セキュリティの脆弱性を放置して攻撃されてしまった場合、甚大な被害に加え、社会的な信頼も失いかねません。
まず、基本的なセキュリティ対策を確実に進めましょう。

ヤマイチテクノでは、お客様に合わせた最適なセキュリティ対策をご提案いたします。是非一度、ご相談ください。

# Yamaichi magazine Vol,22

## サプライチェーン攻撃とは？

### 中小企業におけるサプライチェーン攻撃へのセキュリティ対策


| | |
|---|---|
| 発行日 | 2025年 2月26日 |
| 発行者 | 株式会社ヤマイチテクノ |
| HP | ← 株式会社ヤマイチテクノ公式HP<br>← yamaichi magazine バックナンバー |




【参考資料】


独立行政法人 情報処理推進機構(IPA)：ホームページより

「実務者のためのサプライチェーンセキティハンドブック」
「実務者のためのサプライチェーンセキュリティ手引書」
「中小企業の情報セキュリティ対策ガイドライン第3版」