TANIUM

サプライチェーン攻撃の脅威

加害者にならないために必要なセキュリティ対策

はじめに

「サプライチェーン攻撃」という新たなサイバー攻撃の手口が話題になっています。大企業のサプライチェーンの一部である中小企業を攻撃し、そこから本命の大企業を狙うという手法です。

大企業やグローバル企業はセキュリティ対策が充実しているので、狙いにくくなっています。そこで攻撃者は、より攻撃しやすいサプライチェーンの企業を狙うことが増えてきているのです。
しかし、いったんサプライチェーン攻撃の対象となれば、自社が被害者になるだけではありません。サプライチェーン全体にとっては加害者にもなってしまいます。攻撃対象となった企業としては、損害が発生するだけでなく企業の存続に関わる問題です。

そこでこの資料では、サプライチェーン攻撃の対象とならないためには、つまり被害者にも加害者にもならないためにはどうしたらいいのかを紹介します。

Index

サプライチェーン攻撃が話題になっている

最近は、サイバー攻撃のなかでも「サプライチェーン攻撃」が話題になっています。実際にサプライチェーン攻撃により、誰もが知っている大企業も被害にあっているからです。
サプライチェーン攻撃とはどんなものでしょうか。

サプライチェーン攻撃とはなにか

サプライチェーン（Supply Chain）とは、商品を作成するための原材料調達→生産加工→流通・販売、在庫管理など、商品の開発から販売までの一連の流れを指します。自社だけでなく、原材料メーカーや工場、販売会社や小売店、配送業者もサプライチェーンの一部となります。
サプライチェーン攻撃とは、大企業のサプライチェーンの一部にサイバー攻撃を行い、そこを足がかりにして大企業にまで被害を及ぼすサイバー攻撃です。サプライチェーンとして狙われるのは、多くは比較的規模の小さい企業で、子会社の子会社ということもあります。

サプライチェーン攻撃の実態

実際に、サプライチェーン攻撃による大企業の情報漏えい、サーバー停止、稼働停止などの被害も何件も発生しており、企業も危機感を募らせています。
IPAの「情報セキュリティ10大脅威2022」では「サプライチェーンの弱点を悪用した攻撃」が組織の脅威の第3位でした。
また大阪商工会議所が調査したところ、大企業・中堅企業118社のうち、取引先がサイバー攻撃被害を受け、影響が自社に及んだ経験があるという企業が30社（25%）ありました。

参考：サプライチェーンセキュリティの重要性について | 経済産業省

経済産業省でも対策

サプライチェーン攻撃は、大企業だけでなく政府でも問題にされています。経済産業省では「サプライチェーンセキュリティの重要性について」という報告を発表しました。
また、サプライチェーン攻撃では対象の多くが中小企業であることから「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）」を実施しています。これは、中小企業に向けてサイバー攻撃発生後の初動対応を支援するものです。
さらに、経済産業省ではサプライチェーン・サイバーセキュリティ・コンソーシアムを立ち上げています。これは大企業と中小企業がともにサイバーセキュリティ対策を推進し、サプライチェーン全体のサイバーセキュリティを強化するためのものです。

サプライチェーン攻撃はなぜ大きな問題になるのか（1）

中小企業向けの攻撃であるサプライチェーン攻撃が、なぜ国をも巻き込んだ大きな問題になるのでしょうか。
サプライチェーン攻撃の流れから説明します。

1　対象を探す

攻撃者がサプライチェーン攻撃の対象を探します。
対象となるのは、目的である大企業のサプライチェーンのなかにあり、相対的にセキュリティの弱い企業、多くは中小企業です。

2　中小企業への攻撃

攻撃者が、対象に選んだ中小企業へ標的型攻撃を行います。

ランサムウェアの配布

フィッシングメール内のリンクや添付ファイル、フィッシングサイトからのマルウェア配布などの方法で
ランサムウェアに感染させることが多いです。同時に端末やサーバーの情報を詐取し、認証情報を抜き取ることもあります。

不正ログイン

OSやVPNの脆弱性を利用して不正アクセスを継続的に行い、本命の大企業を攻撃するための足がかりを固めます。
さらに、攻撃対象のネットワークにランサムウェアをはじめとするマルウェアを配布することも多いです。

3　サプライチェーン内の大企業への攻撃

サプライチェーン内での不正なログインに成功したら、そこからネットワークにつながっている本命の大企業に向かって、不正なアクセスに挑戦します。
大企業のネットワークに侵入したら、情報を詐取したり、ランサムウェアでファイルを暗号化したり、他のマルウェアを配布したりします。

4　大企業でも被害が発生

この攻撃が成功したら、大企業でも大きな被害が発生します。
ランサムウェアを配布した場合は、この段階で脅迫文を送付することも多いです。

このように、サプライチェーン攻撃の対象となると、被害者になるだけでなく、加害者にもなるという問題があります。

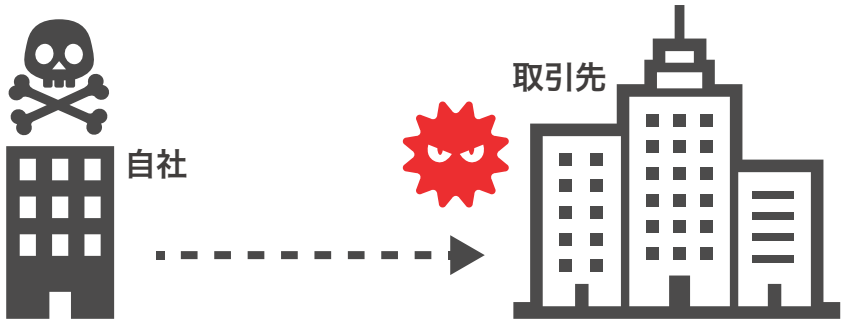
サプライチェーン攻撃はなぜ大きな問題になるのか（2）

サプライチェーン攻撃対象となった企業は被害者になる

サプライチェーン攻撃の対象となった中小企業では、次のような被害が発生します。それだけでも大きな被害となるでしょう。

- 自社内の情報漏えい
- マルウェアやランサムウェアへの感染
- 保存しているデータや公式 Web の改ざん
- サーバーや端末、ネットワークの停止

場合によっては自社の業務が停止し、自社のみならず取引先にも大きな損害が発生します。



サプライチェーン攻撃対象となった企業は加害者にもなる

サプライチェーン攻撃の対象となった中小企業は、次のような他社の被害のきっかけになります。これは、サプライチェーン内の他の企業にとっては加害者になるということです。

自社になりすまして
他社のネットワークに不正なアクセスを行う

→ **他社でもマルウェア配布や情報漏えいなどの被害が発生します**

自社の事業停止により、
サプライチェーン全体の事業が停止する

→ **事業に大きな損失が発生します**

攻撃対象となった企業にとっては、自社が「加害者になる」ことも大きな問題です。それによってサプライチェーン内の企業、および社会的な信頼をなくし、取引停止を引き起こしてしまいます。結果的に、攻撃対象となった企業は事業の存続も危うくなる可能性もあるからです。

なぜサプライチェーン内の中小企業が狙われるのか

サプライチェーン攻撃で狙われるのは、多くの場合比較的規模の小さい企業です。なぜ有名な大企業ではなく、中小企業が狙われるのでしょうか？

中小企業が狙われる理由

中小企業が主に狙われるのには、次のような理由があります。

狙われているという意識が低い

多くの中小企業では「狙われるのは有名な大企業であり、うちのような中小企業は攻撃者の目にもとまらないだろう」と考えています。しかしこれは大きな間違いです。
大企業のサプライチェーン内にあれば、攻撃の足がかりとして狙われるリスクは大きいでしょう。

セキュリティが甘い

中小企業では、情報システム部門やセキュリティに割くリソース（予算や人材など）が少なく、セキュリティ対策がしっかりしていないところも多いものです。その分攻撃しやすいといえます。
逆に、大企業の多くはリソースが潤沢にあり、セキュリティ対策もしっかりしているので攻撃しにくいのです。

本命の大企業とネットワークでつながっている

セキュリティがしっかりした大企業に外部から不正アクセスを行うのは非常に難しいものです。しかしサプライチェーン内にある中小企業は大企業とネットワークでつながっており、社内ネットワークほどではありませんが、かなり容易にアクセスできます。

これらの理由から、大企業を攻撃するときは、直接大企業を狙うよりもサプライチェーン内の中小企業を狙ったほうが楽で、かつ効果的なのです。
つまり、中小企業でも狙われる可能性は高いという意識を持たなくてはなりません。

サプライチェーン攻撃の事例

電機メーカー

2020年1月、大手電機メーカーのネットワークで120台以上のパソコンや40台以上のサーバーに不正なアクセスを受け、情報漏えいの可能性があると報じられました。中国の関係会社をきっかけとしたサプライチェーン攻撃と見られています。
同社だけでなく、防衛省や内閣府、多くの民間企業の情報が流出した可能性があるとのことです。

自動車関連メーカー

2022年3月、自動車メーカーに部品を供給しているメーカーが、子会社を経由してランサムウェアに感染しました。これによって、多くのグループ会社の工場が稼働を停止しています。
同部品メーカーの子会社から親会社へ、さらに得意先である自動車メーカーへという2段階のサプライチェーン攻撃です。

委託先における内部不正

金融機関の現金自動預払機（ATM）の保守管理業務を委託している企業の社員が、顧客情報を詐取し、そこから偽装キャッシュカードを作成して現金を引き出しました。
このように、グループ企業や業務委託先の社員による被害もサプライチェーン攻撃にあたります。

サプライチェーン攻撃から自社を守るためには

セキュリティに割くリソースが少ない中小企業で、サプライチェーン攻撃の対象となることを防ぐためには、次の２つを併用するのが効果的です。

- **セキュリティツールによる防御**
- **サイバー・ハイジーンによる日常的な対策**

セキュリティツールでできること

セキュリティツールでは、エンドポイントやそこに保存されている端末を、不正なアクセスやマルウェア感染などのサイバー攻撃から守ります。また、仮にサイバー攻撃を受けたとしても、被害を最小限に抑えて速やかに原状復帰させることが可能です。

セキュリティツールにはさまざまな種類があります。それぞれに異なった機能があり、防御する方法も対象とするサイバー攻撃も異なるのです。そのため、セキュリティツールで強固なセキュリティを実現するためには、いくつかのツールを組み合わせる必要があります。

サイバー・ハイジーンでできること

サイバー・ハイジーンを行うことで、日々の端末管理やセキュリティパッチの適用を適切に行い、脆弱性をなくしていくことが可能です。それによって、仮にサイバー攻撃を受けても被害を発生しにくい状態を維持することができます。

端末やシステムに脆弱性が残っていれば、いくらセキュリティツールを導入しても意味がありません。サイバー・ハイジーンによって脆弱性をなくすことは、セキュリティツールの導入にかかわらず必要です。

そして、セキュリティツールとサイバー・ハイジーンを併用することで相互補完することができます。
サイバー攻撃に強い、より強固なセキュリティを実現できるのです。

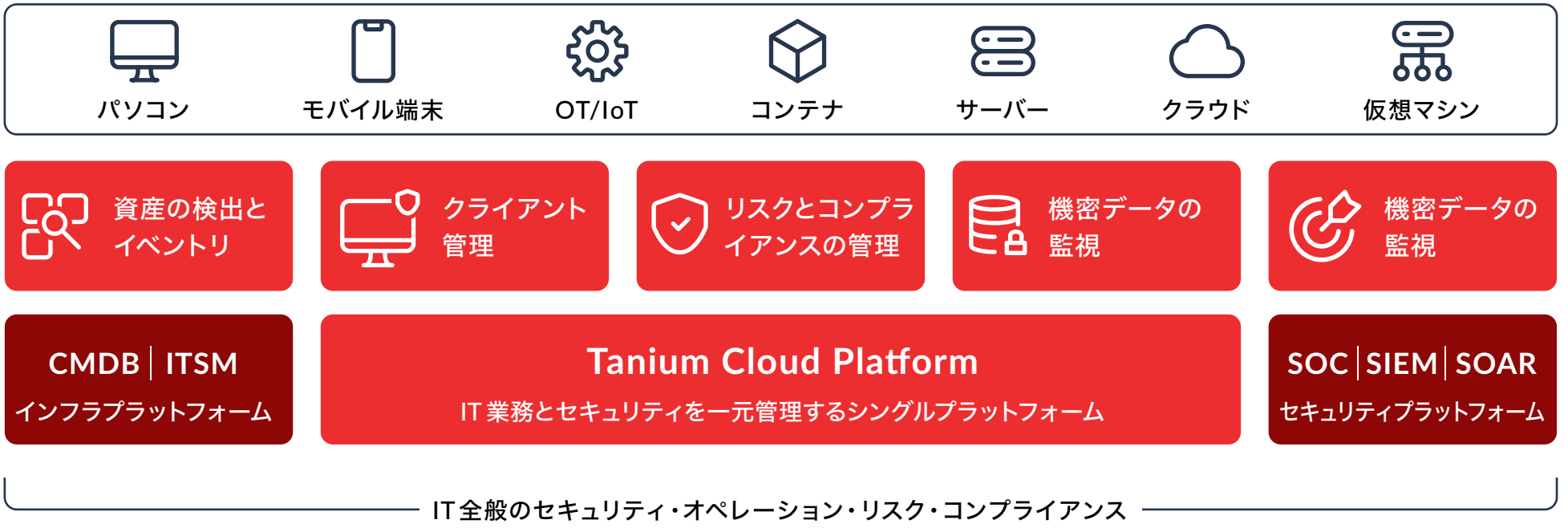
セキュリティツールとサイバー・ハイジーンを併用するためのツール

セキュリティツールとサイバー・ハイジーンをうまく組み合わせれば、より効果的なセキュリティを実現できます。しかし、中小企業でそれを実現するのは容易ではありません。情報システム部門の予算や人員が少ない企業が多いからです。
そこで、セキュリティツールとサイバー・ハイジーンの両方をトータルで管理できるプラットフォームをおすすめします。ツールを使えば、必要なセキュリティを効率的に実現し、中小企業の情報システム部門でもセキュリティを強化することが可能です。

たとえば、Tanium Cloud Platformならセキュリティツールとサイバー・ハイジーンを一元的に管理することができます。このようなプラットフォームを使えば、情報システム部門のリソース不足を補いながら強固なセキュリティを実現することも可能です。
さらに、Tanium Cloud Platformはクラウドサービスとして提供されているため、クラウドサービス利用やテレワークでも導入しやすいのです。

現代のIT課題に対処する最新アーキテクチャ

サービスページ
Tanium Cloud Platform はこちら ▶



まとめ

サイバー攻撃は、有名な大企業だけを標的にしたものではありません。サプライチェーン攻撃により、企業の規模、地域などに関わらず、どんな企業においても、サイバー攻撃を受ける可能性はあります。サイバー攻撃の被害を防ぐ、もしくは被害を最小限に抑えるためには、2つの対策が必要になります。1つはセキュリティツールの導入、もう1つはサイバー・ハイジーンの実現です。
しかし、サプライチェーン攻撃の攻撃対象とされるような企業では、この2つの対策を十分に行うことができない場合もあります。大企業とは違い、情報システム部門の予算や人員、ノウハウが足りないためです。

そこで、Tanium Cloud Platformのような、サイバー・ハイジーンとセキュリティツールを一元的に管理できるプラットフォームの導入をおすすめします。そうすれば、情報システム部門のリソース（人員）が少なくても2つの対策を実現し、セキュリティを強化・維持することが可能です。セキュリティを強化すれば、サプライチェーン攻撃の対象となることを防ぐことにもつながります。