KPMG Newsletter

KPMG Insight

Topic ⑤

サプライチェーン攻撃への対応の要点

Vol. 62

September 2023

Topic　リスクコンサルティング

サプライチェーン攻撃への対応の要点

KPMG FAS
Forensic
遠藤 正樹／パートナー

近年、サイバーセキュリティ対策に力を入れる企業が多くなったことで、きちんと対策を実施している企業に対するサイバー攻撃は容易ではなくなりつつあります。そこで、サイバー攻撃者は、標的である企業を直接攻撃するのではなく、「サプライチェーン攻撃」と呼ばれる攻撃手法を採用するケースが増加しています。サプライチェーン上にある関連会社や取引先企業のなかでセキュリティ対策が脆弱な箇所を狙うことで、最終的に標的企業へ侵入したり、標的企業に損害を与えたりするというわけです。このような攻撃を防ぐためには、セキュリティ対策は自社のみだけでなく、サプライチェーン全体の問題として捉える必要があります。本稿では、サプライチェーン攻撃の概要とその対応について解説します。
なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします。

☑ POINT 1
近年のサイバー攻撃は、自社を直接狙うのではなく、サプライチェーン上のセキュリティ対策が脆弱な箇所を標的として攻撃を仕掛けるケースが増加している。

☑ POINT 2
自社のサイバーセキュリティ対策のみでなく、サプライチェーン上の関連会社や取引先、利用しているサービス／ソフトウエアなどに関しても、セキュリティ対策が適切に施されているかを確認する必要がある。

☑ POINT 3
従来の手法であるセキュリティアセスメントやセキュリティ監査に加え、セキュリティレーティングの活用やサイバーインテリジェンスを利用したリスクの把握も有効である。

遠藤 正樹
Masaki Endo

Ⅰ サプライチェーン攻撃とは

1. サプライチェーン攻撃の概要

サイバー攻撃に関するニュースが日常的に流れている昨今では、多くの企業がサイバーセキュリティ関連のリスクを重要視するようになり、さまざまなセキュリティ対策が施されるようになりました。それに伴い、以前と比べてセキュリティレベルが高い企業が増え、そのような企業への攻撃は難しくなりました。そのため、近年ではいわゆる「サプライチェーン攻撃」と呼ばれる攻撃が増加しています。

情報処理推進機構（IPA）が2023年1月に公開した「情報セキュリティ10大脅威2023」では、組織向け脅威ランキングにおいて、「サプライチェーンの弱点を悪用した攻撃」が2位となりました（前年の3位からランクアップ、図表1参照）。

「サプライチェーン攻撃」では、攻撃者は標的企業のビジネスのサプライチェーン上で、セキュリティ対策が脆弱な企業を探し出し、その企業を利用／経由した攻撃を実行します。攻撃の端緒が自社ではないため、標的となっている企業自身がいくらセキュリティ対策を強化しても、サプライチェーン上に脆弱な企業が1社でも存在している限り、攻撃を受けるリスクが残ります。

2. 主なサプライチェーン攻撃の種類

サプライチェーン攻撃には明確な定義はありませんが、標的とする企業を直接的には攻撃しない、標的企業のサプライチェーン上にある企業やビジネス上の関係がある企業（特に当該企業のネットワークやシステムにアクセス可能な企業）を攻撃するという点は共通しています。以下に、代表的なサプライチェーン攻撃の種類を説明します。

（1）サプライチェーンそのものに対する攻撃

企業のサプライチェーン上にある、セキュリティ対策が脆弱な工場などを攻撃し、業務の停止を余儀なくさせることにより、サプライチェーンそのものが機能しなくなることを狙う攻撃です。日本でも大手メーカーの系列企業が攻撃を受けて操業が停止したことにより、製品の生産が止まってしまった事件は記憶に新しいかと思います。

数年前まではサプライチェーン攻撃と言えば、サプライチェーン上の重要なポイントである工場やインフラなどのOT（Operational Technology）環境を狙った攻撃のことを指していました。この攻撃を防ぐためには、攻撃対象となりやすい拠点に通常のオフィス環境のIT（Information Technology）環境とは異なるセキュリティ対策を施す必要があるとされています。

（2）ビジネス上の関係を利用した攻撃

標的企業とビジネス上のやり取りのある関連企業や取引先企業を攻撃し、侵入することにより、それらの企業を経由して標的企業へ侵入することなどを目的とした攻撃です。

攻撃者は、第1段階として標的企業と関連のある企業について調査をし、セキュリティレベルが低い企業を特定します。セキュリティ対策が十分実施されていない企業を発見した後は、その企業への侵入を試みます。この時点では侵入した企業は標的ではないため、損害を与えるような攻撃は実施しません。

その後、攻撃者は侵入した企業内ネットワークに潜伏しつつ調査を実施し、標的企業への侵入経路を探します。日常のビジネスでシステムを共同利用していたり、ネットワークを介してデータのやり取りが発生している場合、そこに紛れて侵入をすることが可能なケースがあるからです。多くの企業は外部からの侵入を警戒しており、監視や検知の仕組みを導入していますが、関係企業からの侵入は通常のビジネス上のやり取りと区別がつきにくいため、検知することが難しくなります。

また、標的企業への侵入経路が見つからず、侵入ができないような場合でも、侵入を許した関連企業内で保管している標的企業の情報が盗み出されることで、被害を被る可能性もあります。特に、個人情報の取扱いを委託している企業から情報が窃取された場合は、委託先の監督義務が生じているため、自社からの情報漏え

図表1 「情報セキュリティ10大脅威2023」（組織）

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

出典：IPA「情報セキュリティ10大脅威2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html

いではないにもかかわらず、当局対応や顧客対応が必要となるケースが発生します。

(3) ソフトウエアサプライチェーンを利用した攻撃

ソフトウエアを開発している企業を攻撃することで、ソフトウエアの開発ライフサイクルを侵害し、ソフトウエア自体にマルウェアやバックドアを組み込む手口です。侵害されたソフトウエアが広く利用されているものであれば、攻撃対象となる企業の数は膨大となります。最近ではネットワーク管理ソフトウェアを開発する米国のITベンダーへの攻撃により、同社の製品が侵害され、それを導入していた多くの企業や政府機関が攻撃の被害に遭ったことが報告されました。

また、ソフトウエアが開発された時点ではマルウェアなどは仕込まれていなくても、アップデートプログラムなどを適用することで、悪意のあるコードが追加されるというケースもあります。ソフトウエア導入時だけでなく、その後の保守運用の管理体制についても注意をする必要があります。

自社でソフトウエアを利用する際には、このような視点も考慮して、信頼のできるベンダーが開発／保守運用しているソフトウエアを選定する必要があります。

(4) 利用サービスを経由した攻撃

企業が利用するクラウドサービスやMSP（マネージドサービスプロバイダー）を攻撃することで、そのサービスを利用している企業を攻撃する手法です。

クラウドサービスが侵害された場合、そのサービス上で稼働しているシステムや保管しているデータが攻撃を受ける可能性があります。システムやネットワークの運用管理を委託しているMSPが侵害された場合、管理対象となっている顧客企業は容易に攻撃を受けてしまいます。

最近でも大手企業が運営しているクラウドサービスへのサイバー攻撃から、そのサービスを利用していた企業や政府機関のデータが外部へ漏えいするという事件がありました。クラウドサービスの利用が一般的となってきている現在では、このような攻撃の影響範囲は広く、クラウドサービス運営企業の責任はきわめて重大です。

また、クラウドサービスの利用者側もセキュリティ設定などをきちんと確認していないケースが見受けられます。クラウド上で稼働しているシステムだからといって、無条件にセキュリティレベルが担保される訳ではありません。適切なセキュリティ設定が施されているかを定期的に確認することが重要です。

Ⅱ サプライチェーン攻撃への対応強化

前章で見てきたサプライチェーン攻撃に対応するためには、どのような手法があるのでしょうか。ここからは、サプライチェーン攻撃に備えるためのより包括的なガバナンス手法について解説します。

1. 企業間の連携強化

サプライチェーン攻撃に対応するためには、企業単体ではなく、サプライチェーンに関わる企業全体の連携が必要となります。

サプライチェーン攻撃の被害の拡大を踏まえて、経済産業省は2023年3月に「サイバーセキュリティ経営ガイドライン」を改訂しています。ポイントは次の2つです。

- 「経営者が認識すべき3原則」（図表2参照）について、(2) 国内外のサプライチェーンでつながる関係者全体へのセキュリティ対策への目配り、(3) 社内関係者との積極的なコミュニケーションの必要性を追加・修正
- 「サイバーセキュリティ経営の重要10項目」の「指示9: ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策」について、サプライチェーンリスクへの対応に関しての役割・責任の明確化、対策導入支援などサプライチェーン全体での方策の実行性を高めることについての追記・修正

また、KPMGがグローバルで実施した調査「KPMGサイバートラストインサイト2022」によると、「サイバーセキュリティ強化のためにパートナー企業との協力／情報交換を行っている」という回答がグローバル全体では42%であり（図表3参照）、まだ半数以上の企業が連携を取れていない状況であることが分かりました。なお、日本企業では同回答は30%となり、グローバル全体を10%ほど下回る結果でした。

企業間の連携が重要となっているなかで、今後、その連携を強化する取組みとして、以下のようなものが考えられます。

図表2 サイバーセキュリティ経営ガイドライン「経営者が認識すべき3原則」

経営者が認識すべき3原則	
(1)	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
(2)	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
(3)	平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

出典：経済産業省「サイバーセキュリティ経営ガイドライン Ver 3.0」
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

（1）企業間で情報共有の仕組みを構築

脅威情報や脆弱性情報をタイムリーに共有する仕組みがあれば、セキュリティレベルを同程度に保つ手助けになります。また、最新のサイバー攻撃の動向や事例などを共有することで、今後の攻撃に備えることができます。

（2）企業間の連絡体制や役割分担の明確化

実際に攻撃を受けた際に混乱を招かないために、各社の連絡窓口や連絡手段、対応の際の役割分担などを定義して、各社で合意を取っておきます。各社それぞれでインシデント対応フローを整備しておくことはもちろんですが、企業間での連携におけるインシデントに関するルールを定義しておくことを推奨します。

（3）インシデント発生時に備えて合同トレーニング／予行演習の実施

上記で定義されたインシデント対応フローどおりに動けるように、定期的に企業合同でのトレーニング／予行演習を実施しておけば、インシデント発生時の対応がスムーズになることが期待できます。

同一グループ企業であれば、上記のような対応も比較的容易に実施可能だと思われますが、グループ外の企業との連携は個別に交渉が必要となるため、ハードルが高くなります。特に、日本企業は欧米企業のように契約で縛るという文化が馴染みにくいため、先述のKPMGの調査でもグローバルと比較して低い数字となっていると考えられます。

2. アセスメント／デューデリジェンスの強化

サプライチェーン上の企業に一定のセキュリティレベルを求める場合、取引開始前のベンダー選定段階でのアセスメント／デューデリジェンスが重要となります。

取引先の選定時にセキュリティ管理体制に関する確認を実施する企業が増えてきましたが、現状ではセキュリティに関する調査票に回答してもらうことや、保有している情報セキュリティ認証を確認することなどで済ませているケースが多いようです。

より厳格に取引先のセキュリティレベルを確認している例としては、サウジアラビアのサウジアラムコ社の取組みが挙げられます。サウジアラムコ社では、取引先に対してNISTサイバーセキュリティフレームワークをベースとしたサイバーセキュリティ監査の実施を義務付けています。取引先はサウジアラムコ社が認定する監査法人によるセキュリティ監査を受けたうえで、サイバーセキュリティコンプライアンス認証を取得することが求められます。

このような手続きは取引先に多くの負担を強いるものであるため、多くの企業ではここまでの取組みを実施することは難しいと推察されます。

とはいえ、調査票への回答のような自己申告に依拠してセキュリティレベルを判断することにはリスクがあります。そのため、客観的な判断材料を得るために、サイバーインテリジェンスを活用したデューデリジェンスを実施するケースもあります。

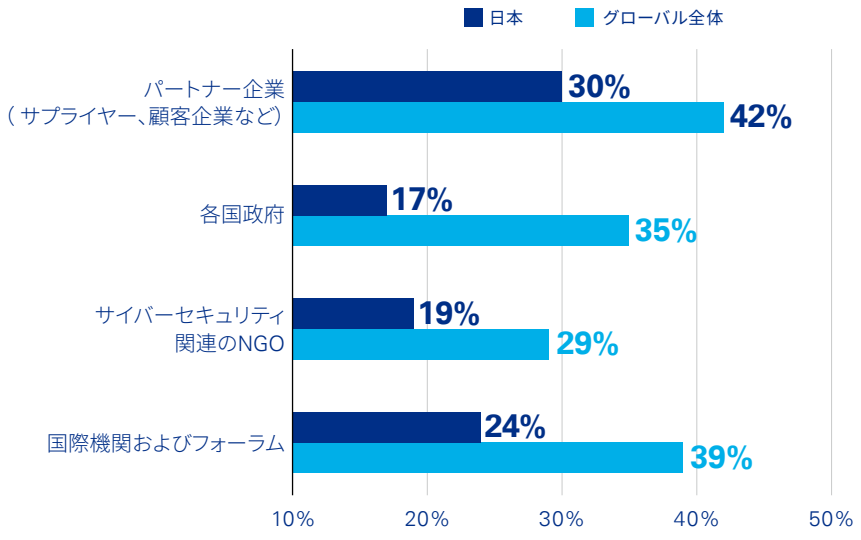
サイバーインテリジェンスでは、ダークウェブを含むさまざまな情報ソースから対象企業のサイバーセキュリティに関連するデータを収集し、分析／評価することにより、企業自身も認識していない潜在的なサイバーリスクを発見することができます。

3. モニタリングの強化

日本企業では業務委託先などに対して、年次のセキュリティ監査の実施やセキュリティアセスメント（調査票への回答など）に留まっているケースが多いように見受けられます。それに対して、グローバルではセキュリティレーティングを活用することでモニタリングの頻度を高め、リスクを早期に検知する仕組みを構築しているケースが増えてきています。

セキュリティレーティングとは、各企業のセキュリティリスクを外部の目線から調査し、評価を可視化する手法のことです。もともとはサイバー保険の適用において、対象企業のリスクを査定するために

図表3　サイバーセキュリティ強化のために、次のうちどの組織と協力／情報交換をしていますか



出所：KPMG作成

用いられることが多かったのですが、近年ではサードパーティリスクマネジメント（TPRM）の手法の1つとして注目されています。いくつかの企業がセキュリティレーティングをサービスとして提供しており、主にサイバー攻撃者の目線から各企業のサイバーリスクの有無やその度合いを評価しています。調査は外部から収集可能な情報に基づき実施されるものであるため、対象企業に調査票への回答や資料提供などの協力を依頼することは不要で、幅広い企業を対象にすることが可能です。

ただし、評価結果はあくまでも外部からの情報によって導き出されるものなので、必ずしも実態を正確に捉えているとは限らないことに留意する必要があります。外からはリスクがあるように見えても、内部ではしっかり対策が取られているケースもあるためです。とはいえ、評価は一定の目安としては有効であり、多くの企業を横並びで比較することも可能なため、有効活用できる場面は多いと考えられます。

Ⅲ 自社のサプライチェーンを守るために

ここまで解説してきたように、サプライチェーン攻撃には、自社のセキュリティレベルを高めるだけでは対応することはできません。攻撃者はサプライチェーンのなかでセキュリティが脆弱な企業を探し出し、狙ってきます。そのような攻撃ポイントを無くすには、企業間の連携を強化して、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しかありません。ただし、連携を強化するためには、関係企業間の調整などが必要となり、なかなか対策を進めることが難しいケースも想定されます。そのような場合には、専門家を活用することを推奨します。利害関係の無い第三者としての視点からの提言や、他社での先進事例などを踏まえた対策などにより、スムーズな対応が期待できます。

関連情報

サイバーインシデントレスポンス

https://kpmg.com/jp/ja/home/services/advisory/risk-consulting/investigation-prevention-fraud/cyber-response.html

サードパーティリスク管理

https://kpmg.com/jp/ja/home/services/advisory/risk-consulting/investigation-prevention-fraud/third-parties-risk-management.html

KPMGサイバートラストインサイト2022

https://kpmg.com/jp/ja/home/insights/2023/04/cyber-trust-2022.html

本稿に関するご質問等は、
以下の担当者までお願いいたします。

株式会社 KPMG FAS
遠藤 正樹／パートナー
masaki.endo@jp.kpmg.com

KPMGジャパン
home.kpmg/jp

home.kpmg/jp/socialmedia