KPMG Newsletter

KPMG Insight

Digital Transformation

日本型サプライチェーンの
サイバーセキュリティリスク

Vol.68

September 2024

Digital Transformation

日本型サプライチェーンのサイバーセキュリティリスク

KPMG FAS
フォレンジック
遠藤 正樹／パートナー

近年、取引先を経由したサイバー攻撃が増加しており、特に日本ではサイバー攻撃による被害の約半数が、子会社や取引先が原因だったとの調査結果があります（グローバル全体では約29%）。その要因として考えられる日本型サプライチェーンの特徴と課題、およびそれに適した対応策について解説します。
なお、本文中の意見に関する部分は筆者の私見であることをあらかじめ申し添えます。

遠藤 正樹
Masaki Endo

POINT 1

サードパーティ経由のサイバー攻撃の増加

サイバー攻撃による侵害のうち、サードパーティが原因となったのは約29%であり、サプライチェーン攻撃であるとの調査結果がある。

POINT 2

日本では約半数がサードパーティ経由の攻撃

調査結果を国別に分析したところ、日本では約48%がサードパーティ経由の攻撃であることが判明しており、グローバル全体の平均から突出して多い傾向にある。

POINT 3

日本型サプライチェーンに適した対応が必要

サプライチェーン上のサードパーティのセキュリティレベルを向上するためには、日本型サプライチェーンに適した対応を検討する必要がある。

I

サードパーティ経由のサイバー攻撃

企業等へのサイバー攻撃のニュースが後を絶ちませんが、近年では自社ではなく取引先や外部委託先等のいわゆる「サードパーティ」が原因となった、サプライチェーン攻撃の割合が増加しています。

情報処理推進機構（IPA）が2024年1月に公開（6月に更新）した「情報セキュリティ10大脅威2024」[1]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2023年に引き続き2位となり、2019年以来6年連続で10大脅威として挙げられています（図表1参照）。

1. サプライチェーン攻撃のリスク

「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「サードパーティ」を探し出し、そこを利用／経由した攻撃を実行します。

サードパーティが攻撃された場合に発生すると想定されるリスクの例としては、以下が挙げられます：

- 業務委託先
  - 業務委託先へ預けていた情報が流出してしまう
- システム連携先
  - 連携先システムから自社システムへ侵入されてしまう
- サービス提供元
  - 業務で利用していたクラウドサービスが停止し、業務が遂行できなくなる
- 調達元
  - 部品が調達できないため、自社製品の製造が止まってしまう
  - 調達したアプリケーションにマルウェアが仕込まれており、攻撃に利用される
- システム開発委託先
  - 開発したシステムに不正なプログラムが組み込まれて攻撃に利用される

2. サードパーティ経由の攻撃の割合

サイバーセキュリティリスク評価ツールを手掛けるセキュリティ・スコアカード社（SSC）が実施した調査[2]によると、一般公開されている2023年のサイバーセキュリティ侵害事案のうち、約29%がサードパーティ経由での攻撃に起因しているものでした。ただし、調査上で原因が特定されていないインシデントに関しても、サードパーティに起因していたものが含まれている可能性があるため、実際の割合はもっと高くなると考えられます。

サイバーセキュリティ侵害を発生地域別に分析したところ、やはり北米が最も多くなります（図表2-1参照）。これをサードパーティ経由での侵害と特定されたものだけで見ても、ほぼ同様の分布となりますが、アジア太平洋地域の割合が若干大きくなっています（図表2-2参照）。

さらにサイバーセキュリティ侵害の件数が多い上位国に関して、サイバーセキュリティ侵害全体に対するサードパーティ経由の侵害の割合を見てみると、日本については48%とグローバル全体の平均となる約29%と比較して突出して多くなっていることが分かります（図表2-3参照）。日本におけるサイバーセキュリティ侵害の約半数がサードパーティ経由での攻撃という事実は、日本におけるサードパーティの管理が進んでいない実態をあらわしていると考えられます。

日本で対策が進んでいない原因としては、欧米と比べてサプライチェーン上のサードパーティへの統制が効かせづらい日本型サプライチェーンの特徴があると考えられます。

II

日本型サプライチェーンの特徴と課題

1. 日本型サプライチェーン（主に製造業）の変遷

製造業のアーキテクチャは、モジュラー（組み合わせ）型とインテグラル（すり合わせ）型があります。モジュラー型は共通部品の寄せ集めで設計し、人財の入れ替えが効きやすい製品で、欧米や中国が得意としています。一方、インテグラル型は専用部品で最適化し、多能工化するために人財固定が必要である製品で、日本が得意とするとされています。代表的な製品の

図表1 「情報セキュリティ 10 大脅威 2024」（組織）

順位	「組織」向け脅威	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	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	6年連続6回目
3	内部不正による情報漏えい等の被害	9年連続9回目
4	標的型攻撃による機密情報の窃取	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）	3年連続3回目
6	不注意による情報漏えい等の被害	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	4年連続7回目
8	ビジネスメール詐欺による金銭被害	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	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）	2年連続4回目

出典：IPA「情報セキュリティ10大脅威2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

例としては、モジュラー型はパソコン、自転車、レゴ等、インテグラル型は自動車、オートバイ、小型電池等が挙げられます。

日本の製造業がインテグラル型が得意になった背景は戦後に遡ります。第二次世界大戦の敗戦を機に、日本は航空機開発を禁止され、ハイレベルの技術者は自動車やオートバイ、鉄道等へと職を変えましたが、働き手が足りない状況でもあったことから、多能工化が急速に進みました。日本の終身雇用もこの頃から傾向として現れましたが、その背景には、多能工化した技術者が転職すると事業が立ち行かなくなることがありました。他方で、米国は移民、中国は人口ボーナスという背景から、そもそも多能工化が必要とされなかったことから、急速にモジュラー型の製造が進みました。

その後、製造過程におけるすり合わせが優位性を発揮する自動車、オートバイ、鉄道等の産業が発達し、多能工化を促進する社会的仕組みが構築されました。

なかでも重要なパートを担ったのが系列メーカーの存在です。彼らは、必ずしも資本関係になくても、メーカーのサプライチェーンの一部を担うことで、メーカーからの大きなサポートを受けることができ、他方、メーカーとしては、サポートし続けることで一定のガバナンス体制を維持していました。このようにして、インテグラル型アーキテクチャを得意とする国が誕生しました。

2. 日本型サプライチェーンの特徴

日本のサプライチェーンにおける重要なサプライヤーの多くは、忠誠を誓わせるかたちでのガバナンス設計に組み込まれています。

日本企業の多くは、通常規格以上の品質水準を求めているため、ISO等の規格を軽視する文化が生まれました。

そのため、ガバナンスを利かせるために必要なルールは、統一的なものがあるわけでなく（それはむしろ有効でないため）、個別のすり合わせにより構築されてきました。

その結果、日本企業においては、サードパーティリスク管理（TPRM：Third Party Risk Management）は、統一的な方法を適用することが難しく、相当程度、個別のカスタマイズが必要とされる現状があります。

サイバーセキュリティの予防体制強化においても、統一的なフレームワーク、方法論をすべてのサードパーティに適用するのではなく、個別・個社対応がフィットする傾向があります。

TPRMの一環としてのサイバーセキュリティのレベル確認も「すり合わせ」の文化で行われるため、ペネトレーションテスト等の疑似的診断もほぼ実施されていない状況です。

モジュラー型の欧米企業は、統一的なルールや手続きを採用することで、高度なサイバーセキュリティのレベルを横断的に更新し続けることが比較的容易です。一方で、インテグラル型の日本企業は、各サードパーティに対して個別対応が必要とされるため、全てのサードパーティについて、サイバーセキュリティのレベルを確保・維持することが困難な状況です。

III 日本型サプライチェーンに適した対応

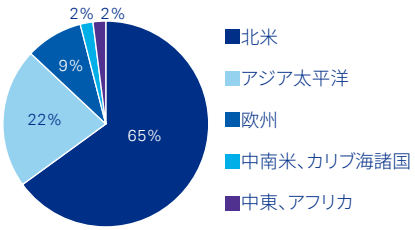
前述の通り、個別の「すり合わせ」文化の強い日本企業のTPRMに関しては、統一的なフレームワークを適用することは困難です。ただ、すべてのサードパーティに対して個別の対応を実施していくことは多くの時間とリソースを必要とするため、まずはリスクの高そうなサードパーティを特定し、そこから優先的に対応を実施していくという方法が現実的と考えれられます。

優先順位をつけるために、まずはリスクの高そうなサードパーティをいかに特定するかという視点で、個別リスク診断の実施を試みることが重要です。

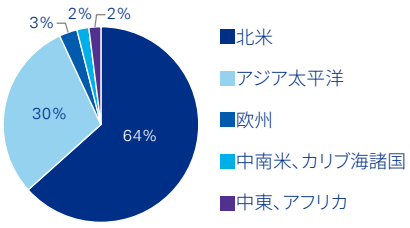
リスクの高いサードパーティを特定するためには、発見的統制の方法論が必要とされています。従来の様な対象企業とのすり合わせが必要となる手法（質問票等での確認の実施）ではなく、たとえばサイバーインテリジェンスを活用した診断ツールを利用した簡易診断（個社ごとにすり

図表2 「サイバーセキュリティ侵害の発生地域別分析」

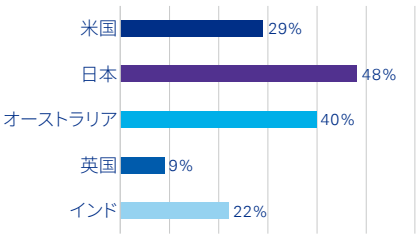
1.サイバーセキュリティ侵害全体



2.サードパーティ侵害のみ



3.サードパーティ侵害の割合



出典：SSC「世界のサードパーティサイバーセキュリティ侵害に関するレポート」

合わせしなくても実施可能な手法）等が有効と考えられます。

ツールでの簡易診断の結果、スクリーニングされたサードパーティ（なんらかのサイバーセキュリティリスクが検出されたサードパーティ）に関しては、個別の対応を実施することが可能です。セキュリティ体制やセキュリティツールの設定等の見直しや、場合によってはサイバーフォレンジック等の深堀調査を実施して、セキュリティリスクの原因を特定し、改善策を検討していきます。

さらに、サイバーセキュリティレベルを維持していくために、定期的なモニタリングやテストを実施できるような体制を構築することも重要となります（たとえば、ツールでの簡易診断を定期的に実施する等）。

また、サプライチェーン上の企業間でサイバーセキュリティに関連する情報交換のための仕組みを構築することも検討すべきです（日本企業は欧米企業と比べて特に遅れているため）。

IV
事業の成長リスクとしてのサプライチェーンとサイバーセキュリティ

企業のサプライチェーンの複雑化に伴い、関連するリスク領域も広範囲となってきております。また、各企業の事業のデジタル化が進むなかでサイバー攻撃の対象領域も拡大してきています。

ランサムウェア等のサイバー攻撃により、サプライチェーン上のサードパーティのシステムが停止したり、重大な情報漏洩等が発生した場合、原因が自社ではなくサードパーティだとしても、企業の存続を脅かす事態に発展する可能性があります。

昨年実施された「KPMGグローバルCEO調査2023」[3]でも、今後3年間の成長リスクとして、「サプライチェーン」と「サイバーセキュリティ」が挙げられています（図表3参照）。

このようにサプライチェーン上のサイバーセキュリティは、今後の企業の成長のための重要な要素として認識されており、サプライチェーンにおけるサイバーセキュリティの高度化に関する課題を解決するために、さまざまな手法・ツール・サービス等が開発されてきています。それらを有効活用することで、効率的にサイバーセキュリティレベルを上げていくことを推奨します。

図表3　今後3年間の成長リスク2023

1	地政学的不確実性
2	オペレーショナルリスク
3	最先端技術／破壊的技術
4	サプライチェーン
5	規制リスク
6	環境／気候変動
7	金利
8	サイバーセキュリティ
9	レピュテーショナルリスク
10	人材

出所：KPMG　「KPMGグローバルCEO調査2023」
https://kpmg.com/jp/ja/home/insights/2023/12/ceo-outlook-2023.html

1 情報セキュリティ10大脅威 2024（情報処理推進機構（IPA）発行）
https://www.ipa.go.jp/security/10threats/10threats2024.html

2 SecurityScorecard Third-Party Breach Report Reveals Software Supply Chain as Top Target for Ransomware Groups（SecurityScorecard）
https://securityscorecard.com/company/press/global-third-party-risk-report/

3 KPMGグローバルCEO調査2023（KPMG発行）
https://kpmg.com/jp/ja/home/insights/2023/12/ceo-outlook-2023.html

サードパーティリスク管理関連サービス

ウェブサイトでは、サードパーティにおけるサイバーリスク簡易診断等を紹介しています。

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