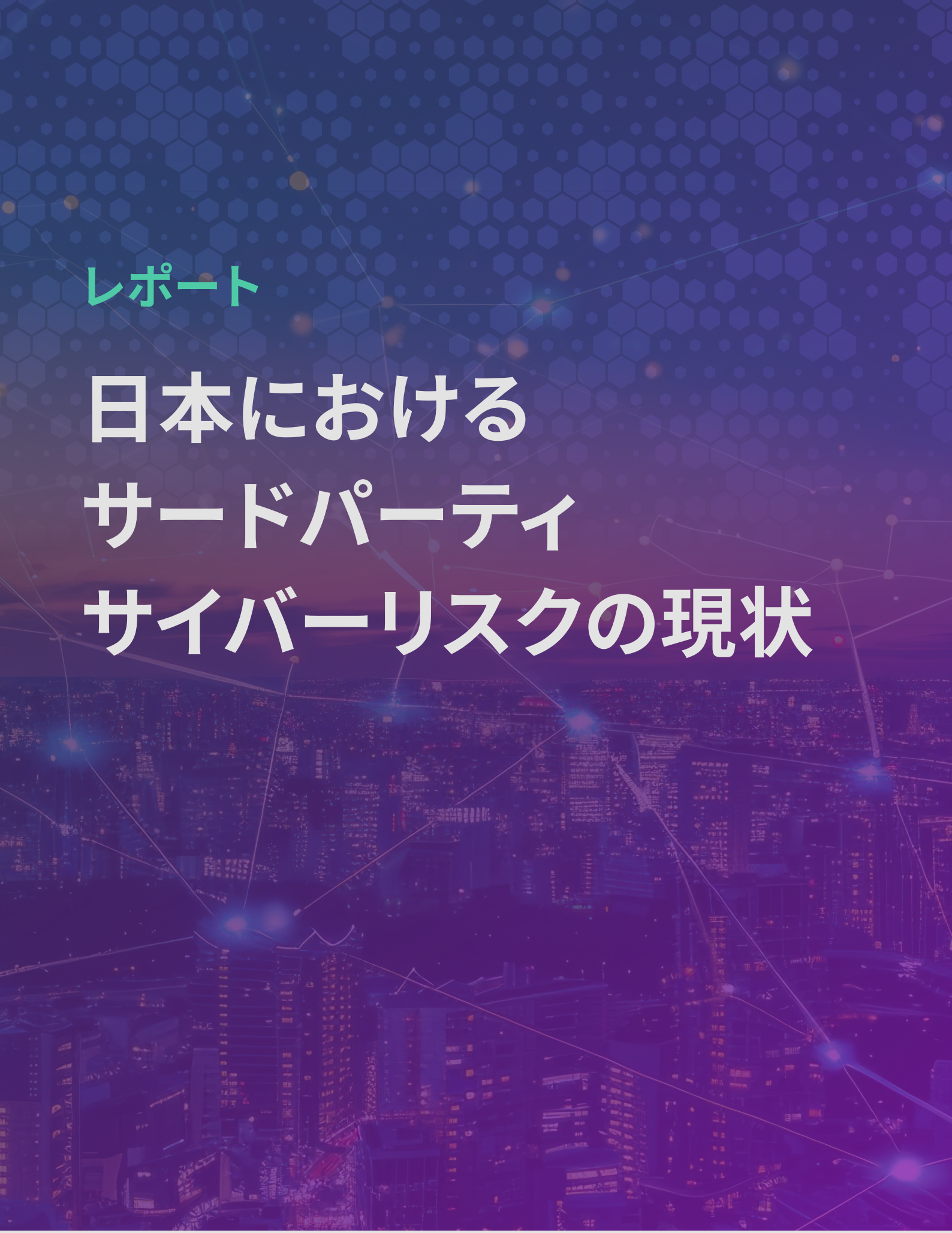
レポート

日本における サードパーティ サイバーリスクの現状



SecurityScorecard

なぜ日本に注目するのか？

このレポートでは、日本におけるサードパーティに起因するデータ侵害とサードパーティ サイバーリスクについて考察します。これは、2024 年春に公開された**SecurityScorecard の年次グローバルサードパーティ侵害レポート**の調査結果を追跡調査したものです。その当時の調査によると、日本におけるサードパーティ攻撃経路に起因する侵害の割合**(48%)**は、世界平均**(29%)**を大きく上回っています。

本レポートでは、日本がなぜこれほど高い割合になっているのかを調査するとともに、サードパーティのサイバーリスク全般についてより深い知見を探求します。本レポートの目的は、日本国内外のサードパーティリスクマネジメント(TPRM)チームが、ベンダーやその他のサードパーティを審査する際の優先事項を明確化するのに役立つ調査結果を提供することです。

また、セキュリティベンダーが公開しているサードパーティリスクのセキュリティ調査の多くが米国中心の視点によるものであり、日本に絞った調査をすることはとても有意義と言えます。日本は世界有数の経済大国であり、日本を拠点とする多国籍企業や有名な日本のブランドが、国境を越えてグローバルなビジネスを展開しているからです。

日本には、製造業、自動車、テクノロジー、金融といった主要産業の大手企業があります。したがって日本は、通常焦点が当てられる米国に代わる適切な選択肢であり、他のほとんどの先進国の経済圏よりも大きなサンプルプールと言えます。

主な調査結果

日本のサードパーティ侵害の割合は依然として高い（41%）。

この割合は、グローバルサードパーティ侵害レポートで日本について記載されている割合（**48%**）よりもやや低い値です。これはおそらく、サンプル数を増やしたことと、調査を実施した期間が異なることに起因されるものと考えられます（本レポートは 2023 年 9 月から 2024 年 9 月までの侵害を対象にしています）。それでも **41%** はかなり高い値です。

サードパーティ侵害が最も多くまたは頻繁に発生している日本の業界は ...

製造、自動車、建設業、テクノロジー、メディア、通信、小売およびホスピタリティ産業です。製造、自動車、建設業は日本経済の大きな部分を占める業界であり、テクノロジー、メディア、通信 、小売およびホスピタリティ産業は特にサードパーティ侵害が多い業界です。

社内で使用している他社製のテクノロジー製品およびサービスが、日本のサードパーティ侵害の原因のトップを占めている（58%）。

この結果は世界的な傾向と一致していますが、日本のサードパーティ侵害のうち、サードパーティのテクノロジーに起因する侵害の割合はやや低めになっています。

日本におけるサードパーティ侵害のもう一つの主な原因は、日本国外の子会社と買収先である（33%）。

このリスク要因は日本に限られたことではありませんが、日本においてサードパーティ侵害の割合が高いことの一因であるようです。

日本におけるサードパーティ侵害の主な脅威には、ランサムウェアや中国・北朝鮮の国家的な支援を受けた攻撃者グループによる攻撃などがあり、特に後者は、全般的な侵害に比べて割合が多くなっています。

サードパーティの攻撃経路は、国家的な支援を受けた攻撃者グループが狙う難易度の高いターゲットに対して、セキュリティレベルの低いサプライチェーンの脆弱性を見つけることで攻撃を可能にしています。

スコアリング手法

SecurityScorecard は、データ漏洩やその他のサイバーセキュリティ事象に関するオープンソースレポートを収集するための独自の機能を運用しています。これは、主要ニュースメディア、セキュリティ専門ニュース刊行物、プレスリリース、企業の情報開示、政府文書および法的文書、ソーシャルメディアへの投稿、ダークウェブでのコミュニケーションなど、さまざまなオンラインソースから関連データポイントを収集します。その主な目的は、弊社のスコアリングアルゴリズムを可能にする侵害の相関関係を確立すること、また組織のスコアに影響する侵害を文書化することです。また 、本レポートや**年次グローバルサードパーティ侵害レポート**のように、他の専門的な調査目的にもこの侵害データを使用しています。

本レポートは、2023 年 9 月下旬から 2024 年 9 月下旬までに収集されたデータを反映しています。調査対象になった侵害の中には、この期間より前に発生していたものが含まれている可能性もあります。これは発見や開示の遅れ、あるいはその他の要因によって、後にオープンソースレポートで初めて表面化したことに起因します。また、日本を拠点とする多国籍企業の海外支店や子会社に影響した侵害も、その資本構造や侵害そのものが日本の親会社へ水平展開する可能性を考慮し、調査対象としています。

これらの情報源のほとんどは日本語で報告されていたものです。弊社の収集プラットフォームの統計によれば、当社の保有データのうち、日本語は英語、スペイン語、中国語に次いで 4 番目によく利用されている言語です。対象範囲を他の言語へ拡大することは、英語中心の視点では見逃す可能性があるデータポイントを収集する上で極めて重要です。ただし、日本語の情報源では得られない詳細な情報がある場合は、一部の日本語情報源を英語による報告で補足しています。

サードパーティの侵害とサードパーティのタイプ

日本における侵害 **160 件のうち 66 件**には、サードパーティ攻撃経路が関与していました（約 **41%**）。この割合は、**グローバルサードパーティ侵害レポート**の **48%** を下回っていますが、大きなサンプルサイズにおいてはある程度の希釈が想定されます。このレポートは対象期間が長いため、使用する侵害のサンプル数も多くなります。このサンプルには日本における侵害のサブセットが含まれていますが、このサブセットも、前述の高い数値を出したサブセットよりも大きいものです。サンプルが多いほど、サードパーティ侵害の割合は低くなります。ただし **41%** は、依然として世界平均の **29%** よりも高い割合です。

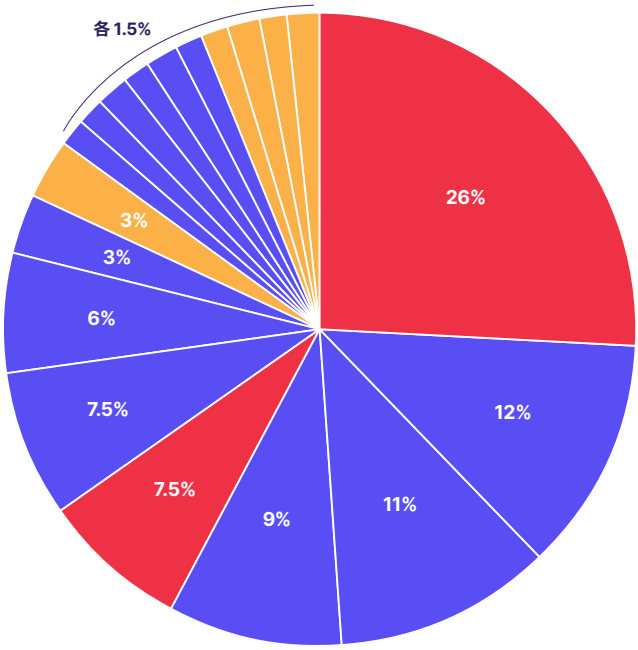
この調査結果には注意すべき点があります。情報源または報告でサードパーティの関わりが特定されている攻撃のみをサードパーティ侵害として認定しています。情報源や報告でさまざまな理由から言及されなかったサードパーティ攻撃経路が、他の侵害に関与している場合、サードパーティ侵害の実際の割合はこれよりも高くなる可能性があります。情報源がサードパーティ攻撃経路を省略する理由としては、以下のことが考えられます。

- 被害者自身またはセキュリティ専門家が、サードパーティ攻撃経路を認識していなかった
- 被害者が、侵害の技術的な詳細を公開しなかった
- ジャーナリストがビジネス上の理由から、それらの経路を含めないことにした
- 編集上の理由としての技術的な詳細を省いた

この注意事項を念頭に置くと、日本のサードパーティ侵害の **41%** という割合は、控え目な推定値である可能性があります。同様に、日本のサードパーティによる侵害の割合が他国と比べて高く見えるのは、多くの日本語で記述された報告書が詳細な技術情報を含めており、他国の報告では触れられないサードパーティ攻撃経路が明確に記載されているためかもしれません。どのようなケースであれ、この特定可能なサードパーティ侵害の充実したサブセットから、日本のみならず世界中の TPRM チームにとって有益なサードパーティリスクに関する知見を得ることができます。

まず最初に、「日本でのサードパーティ侵害の原因となるサードパーティとの関係は、どのようなものか」という問いについて考えます。全 66 件のサードパーティ侵害におけるサードパーティを次のように分類しました。

日本での侵害の原因となったサードパーティとの関係



- **海外子会社、支店または買収先:** 17 件/26%
- **IT サービス全般:** 8 件/12%
- **ペイメントカードデータ E コマース Web サイトでの侵害** 注:本レポートでのペイメントカードとは、クレジットカードやデビットカードなど支払い機能を持つカード全般を示します。 7 件 /11%
- **ソーシャルメディアおよびプロフェッショナル ネットワーキング サービス:** 6 件 /9%
- **国内子会社:** 5 件 /7.5%
- **クラウドサービスプロバイダー:** 5 件 /7.5%
- **ファイル転送ソフトウェア:** 4 件 /6%
- **教育アプリおよびインフラ:** 2 件 /3%
- **マーケティングおよび顧客関係管理 (CRM):** 2 件 /3%
- **VPN:** 1 件 /1.5%
- **メッシュ Wi-fi サービスプロバイダー:** 1 件 /1.5%
- **ソフトウェアリポジトリ:** 1 件 /1.5%
- **Web ベースの自動車保険保険料計算機能:** 1 件 /1.5%
- **電子料金収受 (ETC) システム:** 1 件 /1.5%
- **サイバーセキュリティ組織:** 1 件 /1.5%
- **印刷サービス:** 1 件 /1.5%
- **自動車サプライチェーンの顧客:** 1 件 /1.5%
- **人材派遣会社:** 1 件 /1.5%
- **会計事務所:** 1 件 /1.5%

これらのサードパーティとの関係は、次の3つのカテゴリーに分類されます。1 番目のカテゴリーは、日本企業の子会社、支店、または買収先です。その場所は主に海外ですが、日本国内のこともあります。このカテゴリーは円グラフで赤色で示されており、22 件の侵害の原因となっています。これは、サードパーティ侵害サブセットの 3 分の 1 (約 33%) に相当します。

2 番目のカテゴリーはテクノロジー製品とサービスのプロバイダーです。円グラフでは青色で示されています。このカテゴリーは、このサブセット内の 38 件の侵害 (約 58 %) の原因となっています。3 番目のカテゴリーは、他の 2 つのカテゴリーのどちらにも該当しない関係です。黄色で示されているこのカテゴリーは、サードパーティ侵害のサブセットの残り 9% の原因となるものです。

テクノロジー製品とサービス

サードパーティリスクの原因としてサードパーティのテクノロジー製品とサービスが占める割合が全体的に高いことは、世界的な傾向と一致していますが、日本ではそれほど顕著ではありません。**グローバルサードパーティ侵害レポート**によると、世界全体のサードパーティ侵害の 75% には、サードパーティのテクノロジー製品およびサービスが関与しています。弊社のサードパーティリスクに関する業界別のケーススタディ（**エネルギー**、**航空**など）と、**トップテクノロジーベンダーの分析**でも、サードパーティのテクノロジー製品およびサービスがサードパーティリスク発生源の上位を占めており、多くの場合その他の発生源と大きな差があります。

一般的な IT ベンダーとの関係という漠然とした説明を超えて、E コマース Web サイトにおけるペイメントカードの侵害は、このサブセットで最も多いテクノロジー関係の種類です。情報漏洩したペイメントカードは、犯罪者が大規模に利用するコアデータセットであり、その犠牲となるのは、カードを発行し、不正取引による損失を被る銀行です。従来、物理的な小売店舗/ホスピタリティ施設における POS（Point-of-Sale）端末のマルウェア感染がペイメントカードの不正使用の主な原因でしたが、犯罪市場はその後、消費者と同様に E コマース Web サイトへ移行しています。

犯罪者は通常、（多くの場合悪意のあるスクリプトの形で）デジタルペイメントカードスキマーを使って、脆弱な E コマース Web サイトからカードデータを収集します。これは、過去に犯罪者が ATM、ガソリンスタンド、その他の POS 端末に仕組んでいた旧式のハードウェアカードスキマーに相当する現代のソフトウェアです。侵害されたサードパーティのテクノロジー製品やサービスがこのような Web サイトで使用されていることが原因で、サードパーティ攻撃経路として機能するスキマーが知らず知らずのうちにインストールされる可能性があります。したがって、このような E コマース Web サイトのカード侵害の一部は、フォースパーティ侵害と見なされることがあります。これは、テクノロジーベンダーが侵害を受けたことで、犯罪者が顧客の E コマース Web サイトにスキマーをインストールでき、これにより銀行のカード情報が漏洩するためです。

ファイル転送ソフトウェアがサードパーティリスクの原因として注目されるようになったのは、Progress Software のファイル転送製品 MOVEit のゼロデイ脆弱性（CVE-2023-34362）を悪用した犯罪集団 Cl0p による 2023 年半ばの大規模な攻撃でした。**日本の組織**はまた、これよりも規模が小さい **CVE-2023-45727** の悪用による独自の**侵害**を受けました。これは、NorthGrid の日本語ファイル転送ソフトウェア Proself のゼロデイ脆弱性で、2023 年 10 月に公開されました。CVE-2023-45727 は、日本語情報源に繰り返し出現する、名前付きで特定された唯一の脆弱性です。TPRM チームは、ファイル転送ソフトウェアの脆弱性の悪用をサードパーティ攻撃経路として監視し、2023 年に発生した大規模な攻撃が例外的なものであるのか、それともこの手のソフトウェアを悪用する大きな傾向の始まりなのかを判断する必要があります。

子会社、海外支店、買収先

このサブセットでは技術的な関係が多数を占めていますが、侵害の原因となる最も大きな1つのサードパーティ関係タイプは、日本企業の海外子会社、海外支店、海外買収先でした。これらの関係は、その他の関係に比べて2倍以上のサードパーティ侵害の原因となっていました。それだけで、サードパーティ侵害のサブセットのほぼ26%（4分の1以上）を占めています。

日本国内の子会社と合わせると、このカテゴリーはサードパーティ侵害サブセットの33%を占めています。このような関係は、他国を対象とした調査でもリスク要因として現れますが、通常、この日本のケースほど顕著ではありません。日本の多くのグローバルな大企業やブランド、特に海外に事業を展開する大企業の複雑な構造が、日本でのサードパーティ侵害の発生率がこれほど高いことの大きな理由であると推測しています。他のセキュリティ調査でも日本におけるこの傾向が指摘されています。そのような調査の中で、**この日本のサイバー脅威インテリジェンスの現状に関する報告では、一般的な日本のサードパーティリスクの高さが指摘されています。**

このような海外子会社を経由した侵害の一例として、製造業を主力とするフジクラグループの子会社の例があります。**同グループのタイ子会社で発生した侵害**により、攻撃者はグループの日本のインフラに水平展開できました。さらに大規模な例として、**中国のサイバー攻撃集団 BlackTech** が親会社である日本企業に水平展開するために海外子会社へ侵入していると報じられています（2023年9月現在）。BlackTechは、ルーターのファームウェアを改ざんし、海外子会社のルーターの信頼できるアクセスを利用して親会社へのアクセスを乗っ取ります。

もう1つの例として、2023年11月に東アジアのメッセージングアプリLINEで発生し、約51万人のLINEユーザーに影響した侵害の原因は、LINE（日本のLINEヤフーとソフトバンクが共同所有）とNaver（韓国の企業で、この企業の日本の子会社がLINEを開発）の間での **Active Directoryの共有**が原因であったと日本の政府関係者が結論付けた事例があります。米国に匹敵する東アジアの巨大テクノロジー企業の誕生を目指した一連の合併買収が、より悪用しやすいアタックサーフェスを生み出したのです。日本の政府関係者は、LINEがNaverの技術に依存しすぎていたことと、Naverに与えられていたLINEへのネットワークアクセス権が必要以上に高かったことを主張しています。

セキュリティ研究者は、海外子会社、海外支店、海外買収先が、日本のサードパーティリスクの現状において顕著な特徴となった理由と思われる 2 つの要因を特定しました。その要因の一つは、言葉の壁です。もう一つの要因は、ビジネス文化と環境です。

日本語は、話者数が同程度以上の他の言語と比べると、日本国外での話者数が比較的少ない言語です。その他のすべての条件が同じであるとすると、一般的な脅威アクターや犯罪者は、自分が知っている、あるいは自分にとって馴染みのある言語を話す標的を狙う傾向があります。言葉の壁がないため、ソーシャルエンジニアリング、偵察、データ搾取が容易になります。脅威アクターは、機械翻訳や、最近では AI を使って言葉の壁を克服できますが、そのようなツールを使用することで労力が増え、作業が複雑化し、またこのようなツールを使ってもエラーを避けることはできません。日本の多国籍企業を標的にする外国の脅威アクターは、英語やその他の馴染みのある言語を話す海外の支店や子会社を経由すれば、最初のアクセスを容易に乗っ取ることができることに気付いている可能性があります。

大規模な多国籍企業の監視には、そのアタックサーフェスのセキュリティも含め、多くの課題があります。マネジャーと従業員が異なる言語を話し、異なるタイムゾーンで働いている可能性があります。ビジネス文化で期待されるパフォーマンスやコミュニケーションスタイルが国によって異なる可能性もあります。他の国では法律や規制環境が異なることがあります。同じ国内であっても、買収される側の規模が小さい企業の職場文化が、買収した側の大企業のそれとはまったく異なる可能性があります。多くの多国籍大企業の規模はもちろんのこと、このようなさまざまな複雑さが原因で、セキュリティの問題が簡単に見過ごされる可能性があり、これによって脅威アクターが悪用できる機会がもたらされます。あるいは、企業の合併や買収の前にすでに侵害が発生している場合もあります。そのような場合には、合併や買収の一環として既存の侵害が「継承」されることになります。

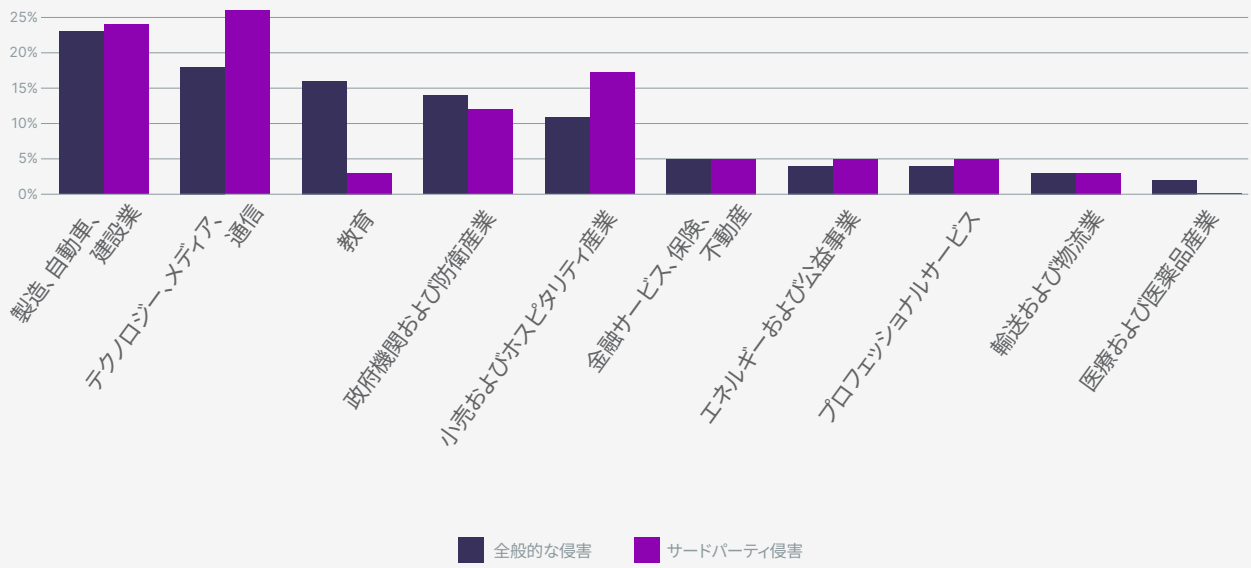
その他

その他のサードパーティ関係という最後のカテゴリーは、わずか 9% と比較的低く、その他の関係タイプごとの数も比較的少ないものです。グローバルサードパーティリスクレポートでの同カテゴリーは、侵害の原因となったサードパーティ関係全体の 25% を占めていましたが、これと比較するとこの「その他」カテゴリーの割合はかなり低いものです。このカテゴリーの規模が比較的小さく、また細分化されていることから、日本の TPRM チームは、サードパーティーリスクの発生源として最初の 2 つのカテゴリーに優先して対応すべきです。

業種別の違い

次に、「日本における業種別のサードパーティ侵害の発生頻度の違いはどのようなものか?」という問いについて考察します。データセット全体における業種別の侵害の分布と、サードパーティ侵害のサブセットにおける業種別の侵害の分布を比較しました。

業界別にみる侵害の分布:
全般的な侵害とサードパーティ侵害



2 つの異なる分布を比較することで、特定の業種が浮き彫りになります。たとえば、製造、自動車、建設業はサンプル全体の 23% と最大の割合を占めています。これは、日本経済におけるこれらの業界の重要性を踏まえれば容易に想定できます。サードパーティ侵害のサブセットに占める割合は 24% とほぼ同じであり、増加分は四捨五入の誤差範囲内です。製造、自動車、建設業は日本経済において多くの比重を占め、かつサイバーリスクにおいても大きな割合を占めていることから、サードパーティ侵害においても大部分を占めるものと結論付けることができます。

対照的に以下の 2 つの業種では、サードパーティ侵害における順位と割合が、サンプル全体に比べて大きく上昇しています。テクノロジー、メディア、通信は、サンプル全体では 2 位（18%）でしたが、サードパーティ侵害のサブセットでは 1 位（26%）となり、製造、自動車、建設業を抜いてトップとなりました。実際、製造、自動車、建設業 とテクノロジー、メディア、通信 だけでこのサブセットのちょうど半分を占めています。小売およびホスピタリティ産業は、サンプル全体では 5 位（11%）でしたが、サードパーティ侵害のサブセットでは 3 位（17%）と大きく上昇しました。この上位 3 つの業種だけで、サードパーティ侵害のサブセットの 3 分の 2 以上（67%）を占めています。

サードパーティ侵害のサブセットの中で、特にこの 2 つの業種が目立つことは、驚くべきことではありません。**SecurityScorecard の以前の調査でも明らかにされているように**、特にテクノロジー企業は、他の業種の組織への**サードパーティ攻撃を知らないうちに可能にしており**、また自社ベンダーからの**サードパーティリスクの「受け手」**になっていることから、サードパーティリスクのレベルが高くなっています。テクノロジー企業のアタックサーフェスは通常大きく、より複雑であることから、脅威アクターは侵害の機会をより多く得ることになり、ネットワーク防御担当者がセキュリティの問題を見過ごす可能性が高まります。

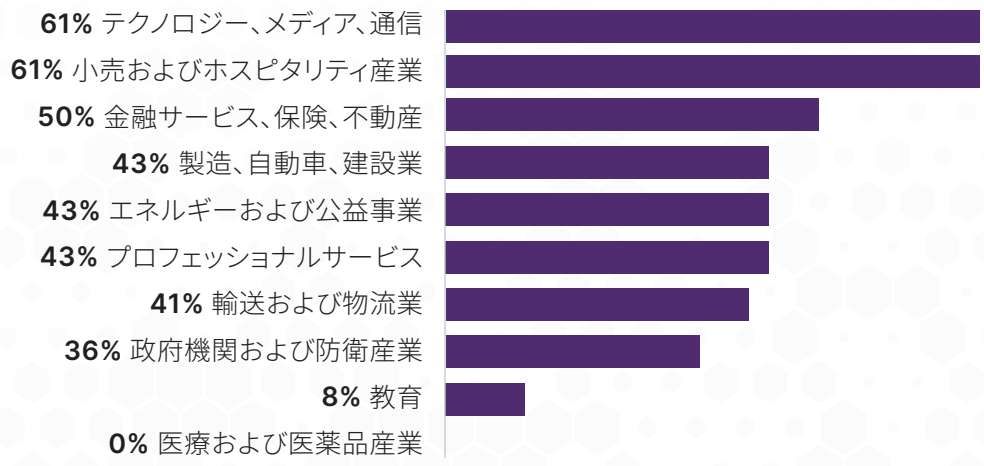
小売およびホスピタリティ産業の企業はこれまで、不正取引のためにペイメントカード情報を盗み出す先として、よく狙われる標的でした。小売およびホスピタリティ産業の企業でのペイメントカードのデータ漏洩は、その結果として銀行が発行する決済手段のデータが流出する限り、サードパーティ侵害であり、不正取引による損失は通常、銀行が被ります。ただし弊社のサンプルの多くのケースでは、標的となっていたのは E コマースの Web サイトでした。犯罪者は、このような Web サイトで使用されている侵害されたサードパーティのテクノロジー製品とサービスを介して、デジタルカードスキマーや悪意のあるスクリプトをインストールします。これらの侵害は、実際にはフォースパーティ侵害といいます。

各業種における侵害のうち、サードパーティ侵害として特定できるものの割合は、上記の説明の一部を裏付けます。テクノロジー、メディア、通信と小売およびホスピタリティ産業では、サードパーティ侵害の割合はどちらも 61% と最も高く、また他の業界よりも大幅に高い数値です。次にこの割合が高かったのは、金融サービス、保険、不動産で 50% でした。日本の金融機関の侵害に関する報告件数は比較的少なく、これは恐らくこの業界における厳格なセキュリティ文化によるものと考えられます。この比較的少ない件数のちょうど半分をサードパーティ侵害が占めていますが、これはサードパーティ攻撃経路により攻撃者が銀行のより強力な防御を迂回できたことによるものと考えられます。

製造、自動車、建設業での割合は 43% であり、これはサンプル全体の全業界での割合である 41% に近い数値ですが、これはおそらく、製造、自動車、建設業がこのサンプルと日本の実体経済における大きな割合を占めているためと考えられます。エネルギーおよび公益事業とプロフェッショナルサービスでの割合も 43% であり、これは金融サービス、保険、不動産業同様に、全般的な侵害の数が比較的少ないが、サードパーティ侵害の発生率が特に高いことに起因しています。運輸および物流産業は、全業界の 41% に一致しています。

セキュリティの強度は、最も脆弱な部分によって決まる

業界別の侵害におけるサードパーティ侵害の割合

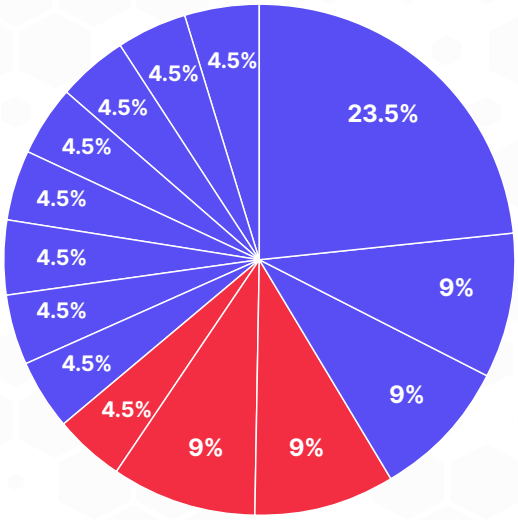


脅威集団

3 つ目の問いは「特定の脅威アクター集団による侵害は、日本の全体的な脅威の状況と比較して、サードパーティ侵害における割合が高いか低いか？」というものです。

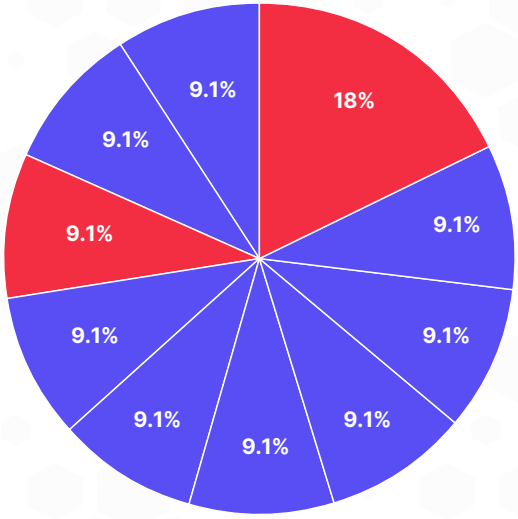
侵害の帰属分類：全般的な侵害とサードパーティ侵害

全般的な侵害



- **8Base**：23.5%
- **BlackCat**：9%
- **RansomHub**：9%
- **中華人民共和国**：9%
- **Lazarus Group（北朝鮮）**：9%
- **Kimsuky（北朝鮮）**：4.5%
- **Akira**：4.5%
- **BlackSuit**：4.5%
- **ClOp**：4.5%
- **Enmity**：4.5%
- **Everest**：4.5%
- **Hunters International**：4.5%
- **INC Ransom**：4.5%
- **Medusa**：4.5%

サードパーティ侵害



- **中華人民共和国**：18%
- **8Base**：9.1%
- **Akira**：9.1%
- **BlackCat**：9.1%
- **BlackSuit** 9.1%
- **ClOp**：9.1%
- **INC Ransom**：9.1%
- **Lazarus Group（北朝鮮）**：9.1%
- **Medusa**：9.1%
- **RansomHub**：9.1%

いずれの場合も、犯罪的なランサムウェア集団（青色）による攻撃が大半を占め、国家による支援を受けた北朝鮮や中国の集団（赤色）による攻撃は少数でした。国家の支援を受けた北朝鮮と中国の集団の場合、サードパーティ侵害における攻撃の割合が全般的侵害の割合よりも高くなっていたことが特徴的です（27% と 22.5%）。

このように、サードパーティ侵害において国家の支援を受けたアクターの攻撃の割合が高いことは当然の結果といえます。特に、APT10 のような国家的な支援を受けている中国のアクターは、これまでサードパーティ攻撃経路を利用してきた長い経歴があります。国家的な支援を受けたアクターは、政府機関や防衛関連企業など、より強固なセキュリティを導入している標的を頻繁に狙います。サードパーティ攻撃経路により、アクターはサプライチェーンの脆弱な部分を悪用することで強力なセキュリティを迂回して、このような強固な標的を狙います。

結論と推奨対策

サードパーティリスク管理での優先順位の設定

弊社の分析から、TPRM チームが優先的に対処すべき 2 つの重要なリスク発生源が明らかになりました。サードパーティのテクノロジー製品とサービスは、日本をはじめ世界各国のすべての業界で、最大のサードパーティリスク発生源となっています。日本の企業にとってもう 1 つの重大なリスク発生源は、子会社、海外支店、買収先（特に海外の買収先）との関係です。このサードパーティリスク発生源から、多国籍企業、あるいは他国に拠点を置く複雑な構造/コングロマリット構造を持つ企業について考慮する必要があります。

このような多国籍企業や、複雑な構造/コングロマリット構造を持つ企業のセキュリティ責任者は、企業「ファミリー」全体のセキュリティ連携を保ち、ある子会社から別のグループ企業や親会社への水平展開のリスクを最小限に抑えるための措置を講じる必要があります。親会社は、子会社、新規買収先、海外支店の基準を設定して適用する必要があります。このような企業内のさまざまな構成要素や事業体間でネットワークセグメンテーションを行うことで、ある事業体での侵害が他の事業体に水平展開するリスクを低減できます。攻撃者が事業体間を水平展開できる機会を減らすために、企業のさまざまな構成要素間のネットワークアクセスと接続を必要最小限に抑える必要があります。合併または買収の広範なデューデリジェンスプロセスの一環として厳密なセキュリティ審査を実施し、その後合併先または買収先のテクノロジー資産に潜在的な侵害がないかどうかを調べる必要があります。

業界別の知見

製造、自動車、建設業は、日本におけるその規模の大きさのために統計上突出していました。製造、自動車、建設業は日本の国家経済の中心的な存在であり、またグローバルリーダーでもあります。製造、自動車、建設業 特有のリスクとして、サードパーティ侵害自体だけでなく、製造業のサプライチェーン全体を混乱させる製造、自動車、建設業の サプライチェーン関係者の侵害に留意する必要があります。一例として、**2022 年に発生したトヨタの自動車部品サプライヤー、小島プレス工業に対する攻撃が原因で、**部品不足のためにトヨタの製造業務が中断された事例があります。小島プレス工業への攻撃のような日本の製造、自動車、建設業での事例から学んだ教訓は、他の国々での製造、自動車、建設業の企業に適用できる可能性があります。製造、自動車、建設業のビジネスリーダーは、サプライチェーンのサイバーリスクの軽減に特化したセキュリティチームに加え、このようなオンラインでのサプライチェーンの混乱に備えた緊急時対応計画を策定する必要があります。

弊社の統計におけるテクノロジー、メディア、通信業界の重要性は、弊社のグローバル調査や他国の調査とも一致しています。テクノロジー企業は、サードパーティ攻撃経路の格好の標的であること、またテクノロジー企業の侵害によって（日本では少ないが）世界全体のサードパーティ侵害の大半が可能になることを認識する必要があります。テクノロジー企業は、このリスクを念頭に置いて防御策を策定する必要があります。

脅威アクターは企業自体への関心はそれほどなく、企業をその顧客に対するサードパーティ攻撃経路として利用することに関心があります。テクノロジー企業はまた、業界内外を問わず、自社ベンダーからのサードパーティリスクの「受け手」になる可能性もあります。

小売およびホスピタリティ産業の企業におけるサードパーティ侵害は、サードパーティリスクの発生源としてのテクノロジー企業の特徴を浮き彫りにします。E コマース Web サイトの運用をサポートするサードパーティのテクノロジー製品とサービスが、脅威アクターがこれらの Web サイトをペイメントカードデータを盗み出す先として侵害するために利用する攻撃経路となることがあります。オンラインでペイメントカードに対応している企業は、ペイメントカードに対応している Web サイトのサポートを行うベンダー、特にショッピングカートや決済フォームなどに関連するサードパーティ製品またはサービスの審査の実施を優先する必要があります。

国家的な支援を受けている脅威とサードパーティのリスク

ベンダーのセキュリティがそれほど厳格ではない可能性があるため、脅威アクターはサードパーティ攻撃経路を利用してサプライチェーンの脆弱な部分を突くことによって、より厳重にセキュリティ保護されている標的のセキュリティを迂回することができます。サードパーティ攻撃経路を使用するこの理由から、日本のサードパーティ侵害において、国家的な支援を受けているアクターによる侵害の割合が高かったことが説明できます。このようなアクターの標的は多くの場合、防衛産業など、セキュリティがより厳格な企業です。同じ理由は、セキュリティが厳重なその他の標的に対する犯罪攻撃にも当てはまります。日本のサンプルにおける金融サービスへの攻撃の半数がサードパーティ侵害であったのは、この理由によるものである可能性があります。

理想的には、自社に適用するセキュリティ標準をベンダーにも適用すべきです。自社のセキュリティの強度は、その最も脆弱な部分（サプライチェーンにおけるサードパーティを含む）によって決まります。自社のネットワークや資産を保護しようと取り組んでも、1 社のベンダーへの侵害から攻撃者がそのベンダーにアクセスできてしまえば、その取り組みが無駄に終わる可能性があります。

中国のサイバースパイによる脅威は、隣国であり、政治的、軍事的、経済的な競争相手でもある日本に大きく迫っています。また、他の多くの国の組織にとってもこれは最大の脅威です。自社内に中国のサイバースパイの存在が疑われる場合には、中国のサイバースパイ集団がこれまでに使用していたサードパーティ攻撃経路（ATP10 による MSP を狙った攻撃、BlackTech の侵害されたルーターの利用など）を理解してください。

詳細や無料アカウントの作成については、jp.security-scorecard.comをご覧ください。

SecurityScorecardについて

アメリカのニューヨーク州に本社を置く SecurityScorecard は、サイバーセキュリティレーティング、レスポンス、レジリエンスの世界的リーディングカンパニーです。

セキュリティとリスクの専門家、アレクサンドル・ヤンポルスキー（Aleksandr Yampolskiy）博士とサム・カシューメ（Sam Kassoumeh）が 2013 年に設立した SecurityScorecard の特許取得済みの評価テクノロジーは、企業のリスク管理、サードパーティリスク管理、経営者向けレポート、デューデリジェンス、サイバー保険の査定のため、25,000 以上の組織で活用されています。

SecurityScorecard は、組織がサイバーセキュリティのリスクを理解し、改善を図り、経営者、従業員、ベンダーとのコミュニケーションを変革することで、世界をより安全な場所にすることを目指しています。

SecurityScorecard

jp.securityscorecard.com
sales-jp@securityscorecard.io

©2024 SecurityScorecard Inc. All Rights Reserved.