# 今、企業に求められるサプライチェーンリスク管理
# ー効果的/効率的なサードパーティリスクマネジメントの実践ー

SecurityScorecard 株式会社 代表取締役社長　藤本大

## はじめに

今、サイバーセキュリティに関わるサプライチェーンリスク管理への注目度が高まっている。

まず、日本においてサプライチェーンリスク管理への注目度が高まっている背景を述べ、その後、多くの企業における対応状況の現状と課題に触れ、その課題への1つの解決策となる「セキュリティ リスク レーティング」というサービスの概要と期待できる効果について述べる。

なお、本稿においては、「サプライチェーンリスク管理」という言葉に代えて、海外でより一般的に利用されている「サードパーティリスクマネジメント（Third Party Risk Management)」（以降、TPRM）という言葉を用いる。

## TPRMに注目が集まっている背景

サイバー侵害に関連する記事が各メディアにかなりの頻度で取り上げられているが、その多くで、狙われた企業自身ではなく、国内外のグループ企業や取引先が攻撃先として狙われていることにお気づきの方も多いと思う。

独立行政法人情報処理推進機構（IPA）が2024年1月に公表した「情報セキュリティ10大脅威2024」でも、「サプライチェーンの弱点を悪用した攻撃」が前年同様2位にランクインしている。

また、経済産業省がIPAとともに2015年に策定、2023年3月に最新版であるVer3.0を公開した「サイバーセキュリティ経営ガイドライン」においても、「サイバーセキュリティ対策は経営者のリーダーシップのもとで推進すべきことである」と示されるとともに、「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」と強調されていることからも、日本の企業がTPRMに取り組むことが求められていることは明らかである。

本稿ではSecurityScorecardが2024年3月に発表した、「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」における、関連データを紹介したい。このレポートは、2023年の世界の主なサイバー侵害の状況について、サードパーティ（取引先）に焦点を当てて調査したものである。

サードパーティ起因のサイバー侵害が全体に占める割合は、世界が29%であったのに対し、日本は49%とほぼ半数がサードパーティ起因であった。日本の割合は、米国（29%)、英国（9%)、インド（22%)、オーストラリア（40%）等に比して圧倒的に高く、日本でTPRMに注目が集まっていることを裏付ける結果となっている。

## TPRMの現状

これまで述べた背景からも、多くの企業においてTPRMの重要性は理解されている。

ただし、対策としては多くの企業において、下記のような必ずしも十分な効果が期待できない内容にとどまっている。

(1) 自社／グループ会社／取引先が準拠すべきセキュリティガイドラインを策定
(2) 準拠状況を年に1度程度のアンケート調査で確認

上記対応は、必要なものであるし、一定の効果は期待できるものであるが、実施されている企業自身も下記のような課題が認識されていることが多い。

- グループ企業／取引先に聞かないと、彼らのセキュリティ態勢を把握できない。
- 限られた頻度（1年に1回や多くても四半期ごと）でのアンケートでは管理すべき対象のセキュリティ態勢をリアルタイムに把握できない。

・そもそも、アンケートで回答される内容が、実態通りの内容であるか確証が持てない。

すなわち、リアルタイムに、継続的に、実態に即した内容で、立場の異なるステークホルダー間でコミュニケーションを取るための「共通言語」がないことが、多くの企業が抱えている課題である。

## セキュリティ リスク レーティング

SecurityScorecardが提供するセキュリティ リスク レーティングは、サイバーキルチェーン[1]の「偵察（情報収集）」フェーズにフォーカスしている。具体的には、IPv4[2]空間全体をスキャン、攻撃者視点でリスク要素を非侵入／非破壊的な手法で大量に収集し、評価したい対象のドメインを入力するだけで、A～D／F及び100点満点で、『サイバー攻撃による侵害の可能性との相関』を持つスコアを提供するものである。

F評価の組織は、A評価の組織と比較して、将来的にサイバー侵害を受ける可能性が13.8倍高い状況にある。

セキュリティ リスク レーティングは、グレードを示すだけではなく、外部から確認できる状況にある脆弱なポイントを、エビデンスとともに示す。その内容を確認し適正に対処することが、グレードを向上し、結果将来的にサイバー侵害を受ける可能性を低減することにつながる。

この評価を得るために必要な情報はドメイン情報のみであるため、自組織のみならず状況を把握したいグループ企業や取引先についても、それらに依頼することなく現状を客観的／俯瞰的に把握することができる。セキュリティ リスク レーティングは継続的に評価し続けているので、利用者は一度ドメインを登録してしまえば新たな脆弱性などによる急激なスコアダウン（＝高リスクの状況）にも気づくことができる。

海外では、グループ企業や取引先に対して、一定基準以上のグレードを取引条件として求めることもあるが、現状日本では、客観的な情報に基づいてグループ企業や取引先とサイバーセキュリティに関する具体的な情報共有を行い、サプライチェーンリスク対策レベルの底上げを行うためのコミュニケーションツール／共通言語として活用されているケースが多い。

## おわりに

日本でも既に数百の大企業及び中堅企業がセキュリティ リスク レーティングを活用して、自社のみならずTPRMにも取り組んでいる。

それに加え、サイバー格付け調査においても、その調査手法の一つとして活用されている。一例として、一般社団法人 日本IT団体連盟が2023年12月に発表した「サイバーインデックス企業調査2023」がある。

自組織のTPRMという観点に加え、「セキュリティ リスク レーティングの評価結果が低い状況にあることで取引先として対象から除外されるというビジネスリスクを回避したい」という利用目的も含め、セキュリティ リスク レーティングを活用している企業が増えている。

セキュリティ リスク レーティングが、より一般的に様々な企業／サプライチェーンで活用されることで、管理する側／管理される側のいずれの組織にとっても、効果的／効率的なTPRMの実現に寄与できるものであると確信している。

---

1　サイバーキルチェーンとは、2009年にアメリカの宇宙船・航空機製造会社「ロッキード・マーチン社」が作成した、サイバー攻撃の行動段階を構造化して整理したものである。

2　Internet Protocol version 4の略で、インターネット上でデバイス同士を識別・通信するためのアドレス方式。