# サードパーティ リスク マネジメント プログラム 構築完全ガイド

SecurityScorecard

# はじめに

セキュリティの専門家は、企業のデジタル資産を保護するという問題を熟知しています。企業経営者たちも、2020年1月から4月にかけてはクラウドサービスに対する攻撃が630%増加したという統計[1]を目の当たりにしつつ、前線に立って広範囲に及ぶ攻撃対象領域を管理しています。

デジタルトランスフォーメーションが加速し、在宅勤務が一般化していることを背景として、サードパーティのネットワークは複雑化しているため、限られたリソースで運営されているセキュリティオペレーション（SecOps）チームの負荷が増大しています。情報セキュリティ最高責任者（CISO）とその部署のメンバーの仕事量が限界に達していても、いまだにサードパーティ評価をExcelシートに展開して追跡管理しています。この時間のかかる手作業から得られるものは、一時的なセキュリティデータに限られ、拡張性もなく、サードパーティの全面的な協力とデータ開示に左右されます。

ゼロデイ攻撃が日々発生する世界で一時的な評価に依存する企業は、可視化されていない部分で被害を受けてしまいます。IBMによると、これにより平均386万ドルものコストが発生する可能性があります[2]。最近注目を浴びている情報漏洩事件以降、取締役会や経営陣に対してデータ、ブランド、顧客のプライバシーが確実に保護されているかどうか、厳格な監視が求めてられています。KPMGの調査によると、CEOが認識している成長リスクのトップ5のうち3つはサイバーセキュリティリスク、規制リスク、サプライチェーンリスクでした[3]。

[1] McAfee.(2020).Cloud Adoption and Risk Report.

[2] IBM.(2020).Cost of a Data Breach Report.

[3] KPMG.(2021).CEO Outlook Pulse Survey.

プログラムの成果を実証し、規制遵守を証明するためには、取引先の新規登録やM&Aデューデリジェンスなどのビジネスプロセスを妨げないタイムラインで、ビジネスの目標、戦略、リスク許容度に関連するリスクを説明したセキュリティレポートを作成できなければなりません。では、セキュリティチーム
はどうしたら予算や人員を増やすことなく、必要な可視性を確保し、セキュリティ上の脅威が生じている環境で対応能力を最大化できるのでしょうか。

Gartnerは、自動化された統合型サイバーセキュリティプラットフォームを活用するチームは、リスクを管理し、大きな成果を上げることができると説明しています。サードパーティリスクマネジメント（TPRM）プログラムの成熟度を高めるためには、適切なテクノロジーを選定することが重要です。また、貴重な資産が相互に接続されたクラウド環境に置かれていて、管理されていないデジタルデバイス、不正なWebアプリケーション、先進技術を駆使するハッカーなどのセキュリティの脅威が多数存在するダイナミックな環境では、状況の可視化が最優先事項となります。

次世代のセキュリティレイティングプラットフォームでは、セキュリティの堅牢性に関する外部データ、インテリジェンス、自動化されたベンダーアンケートを突合させることで、企業のセキュリティ体制を統一的、客観的、包括的に表示することができます。

[4] Gartner.(2021).2021 Planning Guide for Security and Risk Management.

# 1,200万以上の組織のセキュリティ評価を行ってきた経験に基づき、堅牢なTPRMプログラムを推進するための主要な機能をいくつか紹介します。

外部クラウドのスキャニング、サードパーティソース、調査を通じて、セキュリティシグナルやインテリジェンスに関して360度のビューを提供する統合型の統一されたプラットフォーム

アンケートデータおよび規制遵守のエビデンスを自動的に送信して管理

多数の企業を監視できるエンタープライズ規模の機能により人員を増やさずに対応可能

ゼロデイ攻撃やCVEをリアルタイムで特定し、ハッカーに悪用される前に脆弱性に対処

機械学習とグローバルIPスペースの継続的なスキャンを活用して、一貫性のある正確で透明性の高いセキュリティ評価をオンデマンドで提供

NIST、ISO、GDPRといった主要なセキュリティガイドラインや法令について、データ共有と自己診断を実施

GRCやSIEMソリューションなどのセキュリティスタックワークフローとの統合

Excelシートなど手作業による追跡管理のメカニズムをすべて排除

# このeBookでは、TPRMプログラムの成熟度を高め、現在のリスク環境に正面から取り組むための戦略とテクノロジーについて学びます。





## 第1部

サードパーティのリスク評価について、またリスク マネジメントの観点でそれを最大限に有効活用する方法をご紹介します。まず、組織にとって最も重要なリスク要因を特定し、サードパーティとそれらの要因の対応関係を明らかにすることから始めます。これは、企業に関わるリスクを理解するために必要な基本的なステップです。第1部の残りの部分では、その情報を利用して評価を適切に委託する方法をご紹介します。これにより、サードパーティをやみくもに評価するのではなく、リスクに基づいて評価の優先順位を決定できます。

## 第2部

多くのサイバーセキュリティ基準や規制基準（ガイドライン）で義務付けられているように、サードパーティのリスクを継続的に管理するために、サードパーティに対する継続的なモニタリングプロセスを確立する方法を学びます。まず、TPRMの成熟度を高めるために必要なステップとなる、専任のTPRMチームの設立から始めます。その後、コミュニケーション、サードパーティのモニタリング、レポーティングをどのように確立するかご説明します。

# 第3部

サードパーティのサードパーティ、つまりフォースパーティのセキュリティについて学びます。サードパーティにリスクがあるならば、当然ながらサードパーティのサードパーティにもリスクがあります。重要なことは、あらゆるリスクから組織を安全に守ることです。第3部では、サードパーティとの関係性を築くところから始め、協力関係が深まるにつれて必要となる高度なTPRMプログラムの導入について見ていきます。サードパーティと強固な関係性を築いたら、フォースパーティの追跡管理を開始していきます。ここで最も重要な点は、契約をツールとして活用することで、リスクに対するエクスポージャーを確実に軽減しておくことです。

このeBookは各セクションとそれに
関連するステップで構成されていますが、
TPRMプログラムの一部はすでに導入
されていたり、特定の部分を他よりも
優先すべき場合があるかもしれません。
このeBookを最大限にご活用
いただけるよう、組織にとって最も
重要なステップにジャンプ
していただいても構いません。
各セクションの要点を以下
にまとめています。


# 正しいセキュリティ評価に基づいてサードパーティリスクマネジメント リソースを投入する

# ほとんどの企業では、サードパーティリスク マネジメントのための包括的なプロセスが導入されていません。

KPMG の調査によると、サードパーティリスク マネジメント担当役員の4分の3が、サードパーティ リスク マネジメントを企業全体でより一貫性のあるものにすることが急務であると回答しており、企業の評判はサードパーティのセキュリティに依存していると述べています[5]。サードパーティ リスクを軽減し、サードパーティを通じて未知のリスクにさらされることのないようにするためには、簡単に拡張できる効率的なプロセスを持つことが不可欠です。

サードパーティリスク マネジメントの大きな課題は、サードパーティ評価を導入する際に、サードパーティの様々なリスクレベルを分類することです。リスク要因を特定することで、オンサイト評価や侵入テストなどのサードパーティ監査の優先順位を正確に設定できます。

[5] KPMG.(2020).Third Party Risk Management Outlook 2020.

## ステップ1

# 具体的なリスク要因を特定して分析する

デロイトの報告によると、多くの企業では重大なリスクを生じさせるサードパーティの分類体系が明確ではない、という課題を抱えていることが明らかになっています[6]。

## すべてのリスクが企業にとって重大とは限りません。

業界によって異なりますが、まず企業に特有の潜在的なリスクを洗い出し、低リスク、中リスク、重大リスクの3グループに分類する必要があります。この作業により、極めて重要なセキュリティリスクを優先し、組織にとって最も重要な基準に基づいてサードパーティを確実に評価できます。

[6] Deloitte.(2019).Extended enterprise risk management survey 2019.

# 組織のリスクを確認するために以下の質問に答えてみてください。

## サードパーティでデータ漏洩が発生した場合、どの情報の漏洩により最も大きな損害を受けますか？

- 機密情報
- 顧客の財務情報
- 従業員の個人情報
- 他のサードパーティのデータ
- 経理および戦略に関連する情報

### サイバー攻撃による事業の中断

Allianzの調査によると、サイバーインシデントによる事業中断は、中堅企業のビジネスリスクの上位に浮上しています[7]。これは、大規模なサプライチェーンを持つ企業にとって特に問題であり、サイバーインシデントによる操業停止は大きな損失につながります

[7] Allianz.(2021).Allianz Risk Barometer.

これらのリスク要因は
サードパーティとの依存関係や
取引関係の種類に応じて
特定する必要があります。

これらのリスクを適切に分類
するため、組織に起こりうる
影響を考えてみましょう。

## サードパーティのデータ漏洩の影響：

**ブランド
価値の毀損**

**罰金および
コスト**

**規制当局による
制裁**

**訴訟の
可能性**

**株主の
否定的な反応**

このリスクの把握と分析により、企業のリスク要因を包括的に把握できます。
その後、サードパーティについて検討します。

ステップ2

# サードパーティのリスク要因をランク付けする

自社に固有のリスクを定義したのと同じように、サードパーティサービスのリスクも、自社と当該サードパーティの関係の種類に応じて定義する必要があります。

- 対象のサードパーティは自社の従業員や顧客のデータにアクセスしていますか？
- 対象のサードパーティは自社ネットワーク内にシステムを導入しますか？
- 対象のサードパーティのサードパーティ（フォースパーティ）や委託業者が情報を扱うことがありますか？
- それらのアクセスはコンプライアンス基準の対象に該当しますか？

## セキュリティ関連の重大インシデントの原因のトップはサードパーティによるものであることをご存知でしたか？

Ponemon Instituteが実施し、Security Boulevardが発表した最近の調査によると、53%の組織がサードパーティが原因のデータ漏洩を一度以上経験し、修正作業に平均750万ドルのコストがかかっていることが明らかになりました[8]。TPRMプログラムの成熟度を高めることで、セキュリティインシデントが発生した時に迅速に対応できるよう、サードパーティが適切な管理体制を整えていることを確認することができます。

[8] Security Boulevard.(2020).Automation In Compliance:Why It's a Business Imperative and Where to Start

サードパーティのサービスリスクを
定義したら、そのリスクを重要度で
ランク付けします。私たちは低、中、重大
の3段階でサードパーティリスクを評価す
ることをお勧めしています。

これにより既存のサードパーティや
新たに取引を始めるサードパーティを
評価するための標準的な手法を確立
できます。重大なリスクを持つサード
パーティへの評価と改善要求を優先する
ことで、監査予算を効果的に活用できま
す。

ステップ3

# サードパーティの評価タイプをマッピングする

まず、評価方式について、評価を実施するために必要なリソースの量に基づいて分類します。考慮すべき最も重要なリソースは3つです。

**経済的なコスト**

**消費する時間**

**必要なスタッフ**

オンサイト評価のように大量のリソースを必要とする方式では、コストがかかり、複数のスタッフを現場に派遣しなければならず、結果が出るまでに時間がかかります。この方式は、リスクの高いサードパーティについてのみ実施します。その他のサードパーティに対しては、アンケートや自己評価など、リソースをあまり必要としない評価を委託できます。

# サードパーティをランク付けして、リスクの重要度を分類したら、評価のマッピングを開始できます。

これにより、最も適切なサードパーティ、つまりデータ漏洩が発生した場合に最も被害が大きくなると考えられるサードパーティにリソースを集中させることができます。この柔軟で拡張可能なフレームワークは、既存および新規のサードパーティのすべてに適用できます。

## SecurityScorecardのメリット

リスクの分類が完了していないサードパーティが多数ある場合、評価に優先順位を付けることは困難です。SecurityScorecardのプラットフォームを活用すると、評価の優先順位を付けるのに役立つことをご存知ですか？SecurityScorecardでは、オンデマンドであらゆる企業を評価できるため、セキュリティ体制の脆弱なサードパーティを最初に評価することができます。

# 新しい評価方式を継続的に適用する

## ご存知ですか？

EYのグローバルサードパーティリスク管理調査（2019-20年版）によると、サードパーティクラウドベンダーのサイバーセキュリティ体制を継続的にモニタリングしていない組織が35%に上ることが明らかになっています[9]。

ここまでで包括的なリスク優先の観点から、サードパーティを評価できるようになっているはずです。ただし、これは強力なサードパーティリスク マネジメント プログラムを確立するための最初のステップに過ぎません。

従来のTPRMプログラムでは、サードパーティの1年ごとの評価、またはすぐに古くなってしまうポイントインタイム、つまり一時点での情報しか得られていませんでした。サードパーティのエコシステムでは、日々新たな脆弱性や脅威が発生していますが、継続的な洞察がなければ、セキュリティの問題にリアルタイムで対応することはできません。

[9] Ernst & Young LLP.(2021).Data breaches and cybersecurity: managing third-party risk.

### 金融機関におけるセキュリティ評価

米国銀行協会が最近発行した報告書では、効果的なTPRMプログラムの一環として、セキュリティレイティングとリスクスコアの使用を推奨しています。金融機関でサイバーリスクを効果的に把握する目的で、セキュリティレイティング プロバイダーは組織のサイバーセキュリティの健康状態を簡単に測定する手段を提供できます。

2

# 一時的なサードパーティ リスク マネジメントから 継続的モニタリングへ

継続的なモニタリングプロセスを導入する前に、まず第1部で説明したように、企業にとって重要なサードパーティのリスクを特定し、ランク付けすることが重要です。これにより、評価方法を最適化し、サードパーティのリスクを適切に管理できます。次に、サードパーティを継続的に評価する方法について、ご説明します。これにより企業はポイントインタイム、つまり一時的な評価ではなく継続的にリスクを評価して管理できるようになります。

一時的な評価で収集した情報は往々にして古くなり、前回の評価から次の評価が実施されるまでの間、サードパーティのセキュリティ体制の変更は考慮されません。最悪のケースのシナリオが実際に起こり、サードパーティのデータ漏洩が発覚した場合、サードパーティから通知が来るか、次の評価が実施されるまで気付かないかもしれません。その時には、すでにハッカーがネットワークに侵入している可能性があります。

## サードパーティリスクを低減するリモートワーク

リモートワークをサポートするコネクテッドデバイスの爆発的な増加により、リスク管理の強化および機密データを保護するテクノロジーの導入が求められています。適切なポリシーに基づくセキュリティ運用をしていないサードパーティが1社でもあれば、ハッカーはそのサードパーティのデバイスに侵入し、アップストリームまたはダウンストリームで重要なデータにアクセスしてしまうかもしれません。

脆弱性の悪用が急速に進むダイナミックな環境において、サードパーティのセキュリティ体制を継続的に把握することにより、潜在的な問題に対応し、リスクを軽減するための情報と機会が得られます。EYによると、外部ソースからのデータを対象とする継続的モニタリングは、サードパーティの最大のリスクが企業のエコシステムのどこに存在するかを把握するために重要です[10]。

[10] Ernst & Young LLP.(2021).Data breaches and cybersecurity: managing third-party risk.

前述のEYのレポートでは、テクノロジーによってTPRM管理のワークフローは手動から自動に移行するという将来のトレンドが予測されています。ただし、サードパーティセキュリティの長期的な追跡管理については、企業側に大きな課題があります。EYが実施した調査では、サードパーティクラウドベンダーのサイバーセキュリティ体制を継続的にモニタリングしていると回答した企業は、わずか35%にとどまっています[11]。

こうした数字は、現在のサードパーティリスク マネジメントの体制が企業を不必要なリスクにさらし、それによって後々高いコストが発生する可能性があることを示しています。

本eBookの第2部では、サードパーティ リスク マネジメント プログラムの一環として、継続的なサードパーティモニタリングを導入する方法をご紹介します。この方法では、専任のTPRMチームを設立することにより、モニタリングの制御方法とプロセスを定義し、サードパーティと協力して追跡管理、レポート作成、および修正プロセスを実施します。

[11] Ernst & Young LLP.(2021).Data breaches and cybersecurity: managing third-party risk.

## SecurityScorecardのメリット

SecurityScorecardでは、基本理念のひとつとして、世界をより安全にし、リスクを継続的に見通すことのできる360度ビューの提供を掲げています。そのためにグローバルなIP空間を毎日スキャンし、信頼できるパートナーからのシグナルを統合しているので、脆弱性やゼロデイ攻撃をリアルタイムで特定し、実用的なサイバーリスクインテリジェンスを活用していただけます。

# ステップ4

# 専任のTPRMチームを設立する

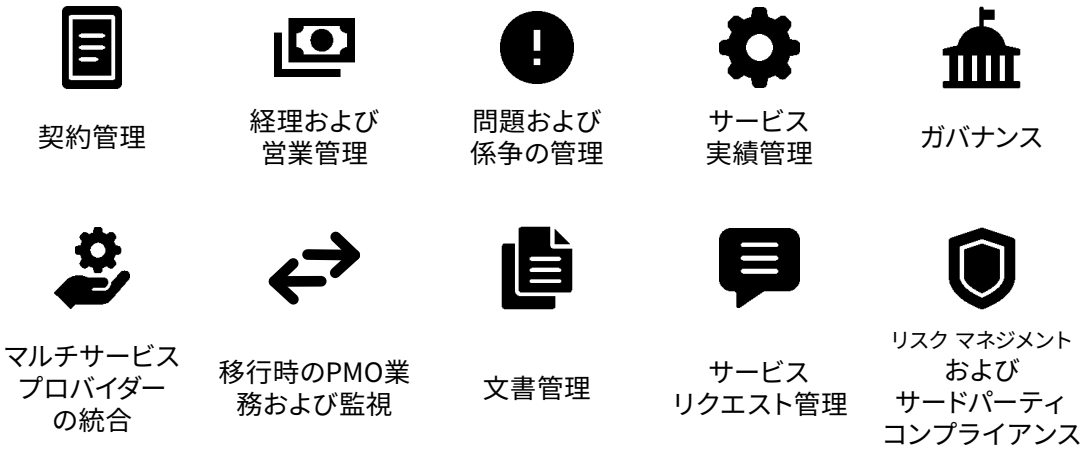
デロイトの調査では、
回答者の半数は
サードパーティリスクの
管理に十分に投資
していないと報告
されています[12]。

TPRMプログラムを成熟させるためには、十分な資金を費やして、セキュリティに強い経営者や専任スタッフを採用する必要があるという考えが多くの企業の共通認識になっています。
サードパーティの継続的モニタリングの基盤を確立するためには、専門のTPRMチームの設立が不可欠です。また、TPRMチームは、サードパーティリスクのすべての側面を担当する現場部門としても機能します。

専任のTPRMチームを設立することで、部門横断チームであれ、特定の部署であれ、サードパーティとのコミュニケーションを担当し、標準的な業務プロセスを確立し、追跡管理してレポートを作成し、オーナーシップを取って責任を担い、サードパーティと取引している他の部署の責任者に対する窓口を一元化できます。
専任のTPRMチームは、重要な決定を下し、ただちに部署の責任者に連絡し、重大な問題が生じたときには優先順位を上げます。

[12] Deloitte.(2020).Extended enterprise risk management survey 2020.

TPRMチームの設立は、TPRMチームメンバーの新規採用、既存従業員のTPRMチームへの異動、または現在の情報セキュリティ関係者にTPRM担当としての役割を与えることから始まります。TPRMチームとは、企業全体の情報セキュリティを支援する高度な専門化された部署のことです。




## 専門部署を設立したら、モニタリング対象を定義します。

# ステップ5

# サードパーティのモニタリングの制御方法とプロセスを定義し、レポーティング方法を確立する

PwCの調査では、経営者およびテクノロジー/セキュリティ担当役員のうち、最も重大なリスクに対応するためにセキュリティ関連の投資をしていると自信をもって回答したのは半数を下回りました[13]。

継続的モニタリングには、他のTPRMプロセスより多くのリソースを必要とするため、関係するリソースの最適化が極めて重要となります。さまざまな基準に基づいてサードパーティのどの部分をモニタリングするかを定義する必要があります（データ、アセット、プロセス、コントロールなど）。以下の基準が含まれます。

## 重大なリスク

このeBookのステップ1を実施していれば、すでに自社のリスク要因を定義、特定できているはずです。自社にとって何のリスクが最も重大かを定義することで、何をモニタリングすべきかがわかります。サードパーティで機密情報を処理または保存している場合、サードパーティのネットワークやエンドポイントを保護するためのセキュリティ管理やシステムの監視をする必要があります。

[13] PwC.(2021).Rethink your cyber budget to get more out of it.

## 情報/状況変化の可能性

重大なリスクをはらむサードパーティのサービスやシステムを分類する頻度は時間とともに変化します。サードパーティが急速に従業員数を増やしている場合、それはエンドポイントの数が増えていて、エンドポイントのセキュリティにより注意を払うべきことを意味しています。ただし、ホスティングやCMSプロバイダーなど、長期間にわたって変更される可能性のないシステムについては、年1回のレビューで十分だと判断することもできます。

## コンプライアンス体制

サードパーティをコンプライアンス体制の延長線上に捉える場合、今日は問題なくても、明日には問題が発生するかもしれません。規制当局は、効果的なリスク マネジメント プログラムの実施を証明できない企業に対してますます強力な措置を講じるようになっています。セキュリティ上の脅威が進化する環境において、変化する規制への持続的なコンプライアンスを確保するため、企業やパートナーのセキュリティ体制を継続的にモニタリングすることが求められます。企業はサードパーティアンケートのプロセスを自動化するプラットフォームを活用して、特定の規制の枠組みに関連する問題を継続的に追跡管理することにより、コンプライアンス違反による罰則や、公的データの漏洩に起因するイメージ悪化のリスクを軽減できます。

### 評価プロセスを自動化する

成熟したTPRMプログラムは、リスクの特定を支援するテクノロジーを組み込んでいます。セキュリティレイティングプラットフォームを活用することで、規制基準（ガイドライン）に対応するサードパーティアンケートを自動的に配信して追跡管理できるようになります。そして、その結果は外部の客観的なデータで検証し、リソースを追加することなく多数のサードパーティのモニタリングを実施できるようになります。

ステップ6

# コミュニケーション、追跡管理、報告のプロセスをサードパーティと協力して設定する

サードパーティモニタリングを成功させるには、サードパーティの協力とコミュニケーションが重要になります。TPRMチームは、関係者全員のセキュリティ体制を改善するために、何をモニタリングして、何を追跡管理しているかサードパーティに明確に伝える必要があります。

もしかしたら、自動化ツールやソリューション、その他のプロセスを活用してすでに企業のセキュリティ体制の継続的モニタリングが行われているかもしれません。サードパーティが所有する統合システムのモニタリングに同じツールとプロセスを使用することもできます。なお、サードパーティにアラート通知しないツールを使用しているとしても、問題が発生した場合にはサードパーティに連絡して修正作業の開始を促す必要があることを覚えておいてください。

Ponemon Instituteの調査によると、回答者の59%がサードパーティのデータ漏洩の被害にあっており、サードパーティのリスクを効果的に軽減していると回答しているのはわずか16%に過ぎないことが明らかになっています[14]。
このサードパーティのデータ漏洩を経験している59%に当てはまる場合、TPRMプログラムの有効性と一貫性を高めるために、以下の要素を運用プロセスに組み込んでください。

### 指標

モニタリングと追跡管理では、長期的なデータの変化でセキュリティ環境の状態を示す重要業績評価指標（KPI）を策定する必要があります。セキュリティパッチがリリースされてから適用するまでの平均日数の短縮や、オープンポートのスキャン頻度を増やすなどの目標を設定します。具体的な目標を設定することにより、基準を満たしていないサードパーティを特定できます。

### 追跡管理とモニタリング

TPRMチームでは、導入済みのテクノロジーやツールを使ってサードパーティのモニタリングと追跡管理を行う一方で、それらのテクノロジーに加えて新しいツールまたはテクノロジーを活用することも検討します。統合された、APIにより統合されたプラットフォームを活用することで、サードパーティとのセキュリティ問題に関わるコミュニケーションを一元化して、ワークフローを最適化し、サードパーティとの協力を促進し、リスクの軽減を加速させることができます。

[14] Business Wire.(2018).Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study:59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third- Party Risks.

## レポート

専任のTPRMチームは、サードパーティのレポート方法を定めて、それを各部署の責任者に共有する必要があります。TPRMオフィスは、サードパーティと各部署の責任者の双方に対し、発生し得るすべての重大な問題についてレポートで警告する責任を担います。

## 修正作業の実施

これまでのステップで行った基礎的な作業は、TPRMチームが問題や異常を明確に特定するのに役立ちます。サードパーティの側でセキュリティに関する問題が発生した場合、TPRMチームは各部署の責任者やサードパーティと連携して問題を修正します。

サードパーティの継続的なモニタリングは、多少の労力が必要になるとはいえ、サードパーティのリスク マネジメントができるだけでなく、自社のセキュリティ体制も改善でき、複合的な成果を上げることができます。

## SecurityScorecardのメリット

SecurityScorecardは、GRC、SIEM、その他のセキュリティスタックのワークフローと統合可能なセキュリティ評価プラットフォームを提供することで、TPRM活動の集中化と効率化を支援します。業界をリードするSecurityScorecardのマーケットプレイスによって、信頼できるパートナーのソリューションや事前に構築された統合機能を見つけて導入し、TPRMプログラムから最大限の価値を実現できるワンストップショップとしてご活用いただけます。

# フォースパーティについての情報を収集する

サードパーティがビジネスに重大なリスクをもたらすことを考えた場合、サードパーティのサードパーティ（フォースパーティ）についても考慮する必要があります。これは、最初にサードパーティを評価する際にそのサードパーティのセキュリティをについて把握するために重要です。また、継続的モニタリングを実施する際は、以前にリスクがあると判断した企業とサードパーティが最近取引を開始していないかどうか確認することが重要です。

# サードパーティおよびフォースパーティのリスクを管理する

サードパーティの評価に優先順位をつけ、集中的なサードパーティのリスク管理プログラムを確立し、このeBookの最初の2つのパートで説明したような継続的モニタリングを行っていれば、強力なリスク軽減策を講じることができていると言えます。ただし、サードパーティが業務を委託するサードパーティ（フォースパーティ）という、大きなリスク要因が見過ごされているかもしれません。

デジタルトランスフォーメーションの時代において、重要なアプリケーションの配信はSaaS（Software-as-a-Service）やその他のクラウドベースのサービスに依存しています。ご存知のようにフォースパーティがサードパーティ企業のサービスに影響を与えることがあります。2021年6月にはコンテンツ配信ネットワークのFastlyが障害を起こし、Amazon、Twitch、Reddit、New York Timesなど数十のサイトがダウンしました。そのため、フォースパーティのリスクをモニタリングするTPRMプログラムを備えておくことが、戦略の重要ポイントになります。

米国通貨監督庁（OCC）のBulletin on Third-Party Relationships（第三者委託関係に関する公示）では、再委託先の評価の可視化に重点を置いた数々のガイドラインと基準が提供されています。これには、重要なサードパーティサービスプロバイダーが利用可能な最善のものであることを保証するためにリスクに基づいた意思決定を行うことなどの項目が含まれます[15]。

[15] Office of the Comptroller of the Currency.(2020.)Third-Party Relationships:Frequently Asked Questionsto Supplement OCC Bulletin 2013-29.

# さらに、KPMGのアウトソーシングとサードパーティリスク マネジメント レポートには、フォースパーティと下請業者に関する重要な検討事項が記載されています[16]。

そこには、以下の項目が含まれます。

サードパーティリスクの評価と制御が、フォースパーティが提供するサービスや処理データに見合ったものであることを確認する。

リスクの集中、つまり地理的に近い複数のサードパーティや、共通のフォースパーティとの取引が管理されていること。

デューデリジェンスプロセスにより外部委託の取り決めが文書化され、サードパーティによるフォースパーティのガバナンスが検証されていること。

以降のステップでは、フォースパーティのモニタリングとレポーティングを強化する方法についていくつかの方向性を説明しています。

[16] KPMG.(2021).Outsourcing and third-party risk management.

## ステップ7

# サードパーティとの関係性を築いて フォースパーティのリスクを管理する

フォースパーティのモニタリングは、サードパーティとの協力の上で成り立っています。フォースパーティのセキュリティ体制に関するデータを収集するためにはサードパーティとの強固な関係性が求められます。サードパーティと協力してフォースパーティのモニタリングを促進して、実施することで、自社のサイバーセキュリティの健全性を改善できるだけでなく、パートナー企業のTPRMプロセスの改善にも貢献できます。パートナー企業とセキュリティの話題が挙がった際にこの点を強調しておくことで、サードパーティとフォースパーティのセキュリティ問題に対応する際に、同意をうまく取り付けることができます。

フォースパーティのモニタリングでは集中的な努力が求められるため、それを全体に適用することはお勧めできません。サードパーティに関してはすべてモニタリングすべきですが、必ずしもフォースパーティのすべてをモニタリングする必要はありません。

まず、このeBookのステップ1で推奨しているように、リスクの重大性が最も高いサードパーティを特定してください。重大なリスクをはらむサードパーティを特定した後は、サードパーティと協力してサプライヤーをリストアップし、フォースパーティが提供するサービスを定義した対応表を作成します。

# フォースパーティについて把握しておくべきこと

フォレスター/RSAの調査によれば、回答者の82%が、サードパーティのインベントリー作成、評価、管理にいまだにスプレッドシートを利用しています[17]。

どんなサービスをどのように提供していますか？

企業の機密データにアクセスしていますか？

サードパーティの機密データにアクセスしていますか？

セキュリティが侵害され、データが漏洩するとしたら、攻撃経路どのようなものになりますか？

あなたの組織とフォースパーティの間の接続を阻止する目的で、何らかの分断または意図的なネットワークのセグメンテーションが存在しますか？

フォースパーティの拠点はどこにありますか？

[17] RSA.(2020).82 Percent of Organizations Still Use Spreadsheets to Manage Third Parties.

サードパーティとその提供サービスのリストを作成した後、そのサードパーティのモニタリング機能について把握しなければなりません。成熟したTPRMプログラムを導入していますか？継続的なサードパーティ（あなたにとってのフォースパーティ）リスクのモニタリングを実施していますか？パートナー企業がデータ漏洩を起こした場合に、どのようなインシデント対応計画が立てられていますか？

フォースパーティのセキュリティ体制を把握することは、成熟したサードパーティリスク マネジメントの重要な要素であり、サードパーティにTPRMのベストプラクティスを導入してもらう動機づけにもなります。

### SecurityScorecardのメリット

主要なビジネス機能が、多数の企業にサービスを提供するサードパーティのSaaSプラットフォームによって支えられている環境では、1台のサーバーダウンでエコシステム全体のサービスが停止させられてしまう可能性があります。サードパーティとサードパーティにサービスを提供するフォースパーティを追跡管理することにより、有害事象の発生時に自社のビジネスへのリスクをはらむ相互依存関係を特定できます。SecurityScorecardでは、APIコール、セキュリティレイティングデータ、自動化されたアンケートのやり取りと検証により、企業がフォースパーティのセキュリティデータを監視できるようにしています。

ステップ8

# 高リスクのサードパーティ/フォースパーティに対する保険として契約を活用する

契約の活用は、最も重要なサービスが外部に委託されないことを保証する良い手段となります。契約書を作成する際、または既存の契約書を修正する際には、外注や下請けに出すことができないサービスを明記するようにしてください。これは、重大なリスクをはらむサードパーティに対して今すぐ実施でき、新しいサードパーティがエコシステムに参入してきたときにも役立ちます。

アンケートを実施する際に、サードパーティが提供するサービスを外部に委託しているかどうかを確認することで、フォースパーティに関する情報をサードパーティリスクマネジメントのプロセスに組み込むことができます。

2020年の世界のデータ漏洩被害のトップは前年に引き続き米国で 被害額の平均は864万ドル、中東の被害額の652万ドルがこれに続いています。世界のデータ漏洩1回あたりの平均被害額は386万ドルです[18]。

契約書を作成する際、「サードパーティが新規の下請け業者に委託する場合、例え既に契約の最終段階であったとしても通知を求める」という文言を盛り込むことができます。

医療や金融など、規制の厳しい業界では、契約書の活用の重要性はさらに高まります。こうした業界の組織は厳しい監視下に置かれているため、サードパーティを管理する際には、あなたの組織が規制当局のように振る舞う必要があります。

フォースパーティの情報を体系的に収集することにより、規制対象の企業は、積極策を講じ、TPRMを重視したガイドラインと規制を遵守できます。

[18] IBM.(2020.)Cost of a Data Breach Report 2020.

# 成功へのロードマップ

SecurityScorecardでは、何百万もの組織のセキュリティ体制を評価してきた経験から、企業が適切な戦略とテクノロジーを採用することで、ペースの変化に対応し、同業他社に差をつけることができると考えています。今こそ、企業のセキュリティ対策を資産とし、持続可能な戦略的パートナーとなるべきときです。

このeBookで紹介されているプラクティスやツールを導入することで、定型的な手作業のプロセスに費やす時間を削減し、チームの能力を高めて組織全体に価値をもたらすことができます。クラス最高のTPRMソリューションを選択するプロセス、また評価基準として役立つ以下のチェックリストをご確認ください。

## 全般：

**データ精度。**セキュリティの観点で外部から見たとき、非常に精度が高く、信頼できること。新たなセキュリティの問題が検出された場合、スコアは自動で作成され、更新される必要があります。

**データ漏洩の可能性と相関するスコア。**スコアリングのアルゴリズムがデータ漏洩の可能性と直接的な相関性があること。スコアリングの方法は透明性があり、反論が可能で、第三者によって検証できるものであるべきです。

**統合アンケート管理。**自動化された統合アンケート管理ソリューションを提供してサードパーティリスク評価のアンケートを実施して追跡管理できること。

## スピードと拡張性：

**企業スコアの新規登録。**評価されていない企業が見つかった場合、人手に頼ることなく、必要に応じて新しいスコアカードを作成できること。

**拡張性。**グローバルなサプライチェーン全体を評価できること。レイティングプラットフォームが効果を発揮し、価値を実現するには小企業やスタートアップ企業も登録する必要があります。

## スコアカードの詳細：

**スコアの改善および修正プラン。**企業のセキュリティ体制を改善するためのスコア改善計画を作成できること。スコア改善計画では、特定の問題を改善したときにスコアがどの程度変化するかを明確に示す必要があります。

**データの透明性。**判明した望ましくない状態の詳細とリスクを軽減するための推奨事項を提供できること。レイティングプロバイダーは、リスクが確認されたIPアドレスの一覧と、問題が最後に観測された時点のタイムスタンプを開示する必要があります。

**デジタルフットプリント。**組織に属するすべてのIPをセグメント化し、検出の根拠と併せて完全なIPの詳細を開示し、IPの属性が正しくない場合は、デジタルフットプリントを自己修正できること。レイティングプラットフォーム上でIPの追加や削除を依頼し、自社のデジタルフットプリントを自己修正できるようになっている必要があります。

**カスタムスコアカードの作成。**大規模な組織のカスタムのスコアカードを、IPアドレスのレンジ（範囲）、ドメイン、サブドメイン、地理的な位置といったフィルターを使用して作成できること。

**コンプライアンスのマッピング。**コンプライアンスマッピングにより、CMMC、NIST、ISOといった一般的によく使われるフレームワークのギャップ分析を実施できること。

### 継続的モニタリングとアラート：

**継続的モニタリングと毎日のスコアのアップデート。** スコアは毎日更新され、検出された新しいセキュリティの問題がプラットフォームで可視化されること。

**アラートと通知。** スコアの変化、リスク要因の変化、新たに検出された問題やデータ漏洩に基づいて、個人やチームに対してアラートや通知を設定できること。

### 修正と誤検出：

**修正のワークフロー。** 修正された問題を送信してレビューできるインタフェースを提供するとともに、プロセスを追跡管理するメカニズムが存在し、SLAが文書化されていること。

**修正後のスコア変更。** スコアが修正作業から72時間以内に更新されること。

**誤検出。** 検出されたセキュリティ問題のうち、誤検出と思われるものに反論するためのインタフェースを提供できること。反論が認められた場合、送信後72時間以内にスコアに反映されること。

### 報告：

**レポート機能。** 企業のセキュリティ体制に関するさまざまなレポートを提供できること。サマリーレポート（簡易表示）や詳細レポート（検出されたすべてのセキュリティ問題とIPの詳細）が含まれます。

**並べて比較する機能。** 競合のベンチマーキングのために、様々な組織を横並びで比較することができること。

**取締役会向けレポート。** 事業目標、戦略、リスク許容度に関連するリスクを説明した、取締役会に適したレポートを提供できること。

### サードパーティコラボレーション：

**サードパーティ招待機能。** サードパーティに対して永続アクセスを無償で提供し、パートナー企業が自分のレイティングを確認できるようにすること。

**サードパーティダッシュボード機能。** 招待されたサードパーティの修正アクティビティを追跡するためのダッシュボードを提供できること。

### 統合：

**インテグレーションとAPIライブラリー。** SIEM、チケット発行システム、GRCソリューションと統合するための広範なAPIライブラリーを提供できること。APIは、PyhonやJavascriptなど、複数の言語でカスタム統合に対応している必要があります。

# SecurityScorecardによる サードパーティリスク マネジメント

前述のとおり、セキュリティレイティングプロバイダーは複雑化するサードパーティのエコシステムとデジタルフットプリントの管理を支援できます。SecurityScorecardの自動化ツールや機能を既存のワークフローに統合すれば、日常業務を簡素化し、投資の価値を高めることができます。

- SecurityScorecard **Sentinel**により、グローバルIPスペースを毎日スキャンすることで、次のことが可能になります。
  - 自社とサードパーティのセキュリティ対策を継続的にモニタリングする。
  - ハッカーの動向に合わせて、自社のエコシステムでCVEを検索し、ゼロデイエクスプロイトの影響を受けたかどうかを判断する。
- **FastScore**はオンデマンドで企業を評価し、迅速なデューデリジェンスとサードパーティオンボーディングを可能にします。
- **Digital Footprint**は、すべてのエンドポイント、アプリケーション、Webドメインを含むITアセットの全体像を提供し、シャドーITがセキュリティ上の脅威となることを防ぎます。
- **Integrate 360° Marketplace**は、ワークフローの統合と自動化を可能にする最大手セキュリティレイティングマーケットプレイスで、**CybelAngel**、**HackerOne**、**DarkOwl**などの信頼できるインテリジェンスパートナーのシグナルを活用できます。これらのシグナルで脅威の現状把握が強化されますが、スコアに影響が及ぶことはありません。
- **Rule Builder**を使用すると、**Slack**、**Jira**、**ServiceNow**、**Zapier** などでアラート通知を受信することが可能になり、サードパーティのデータ侵害やサードパーティセキュリティ対策の変更があった場合の連絡や修復を効率化できます。
- **Atlas**では、サードパーティのサイバーセキュリティに関するアンケートの回答をSecurityScorecardのデータに自動的にマッピングでき、サードパーティの評価サイクルを83%削減できます。Atlasでアンケートを作成・編集する際に、**Custom Issue Mapping**を使用すると、各質問を検証するセキュリティ レイティングのデータポイントを選択できます。これにより、サイバーセキュリティ評価プロセスのカスタマイズ性と透明性が高まり、リスクの360度ビューが真の意味で実現します。

- SecurityScorecardの強力な**API**により、企業は実用的なデータに直接アクセスして、ワークフローを強化し、時間を節約し、テクノロジースタックでからより多くの価値を得ることができるようになります。どの企業も**SecurityScorecard Ratings API**を活用し、カスタムソリューションを開発することも、既存のサービスをSecurityScorecardのプラットフォームと統合することもできます。さらに、SecurityScorecardでは、業界最先端のSIEMやTPMRMなど20種類以上のソリューションとの統合機能が提供されているため、ユーザーは日常業務にただちに活用できます。

- **Score Planner**では、特定の問題がスコアにどう影響しているかが完全に透明化されており、目標とする成績に到達するための修正プランが自動的に作成されます。推奨事項が自社のセキュリティ優先事項と完全に一致していない場合は、SecurityScorecardのシンプルなユーザーインタフェースで簡単にプランをカスタマイズできます。

- アンケート交換および検証プラットフォームの**Atlas**を活用すると、サードパーティのリスク評価を自動化して加速することができます。**Evidence Locker**は、TPRMドキュメントのシングルソースとして機能し、チームは**Atlas**と**Ratings**の間でこの情報を交換することで、保存されたデータをサードパーティやコンプライアンスのアンケートに自動的に入力できます。

- **Custom Scorecard**ではサードパーティ組織を個別に階層化して表示することで、関連性の最も高い子会社、地域、ドメインのセキュリティ体制を格付けできます。

- SecurityScorecardの**Board Trends Reports**では、コンプライアンスや戦略的なTPRMパフォーマンスを管理するエグゼクティブレベルの洞察がリアルタイムに提供されるため、事業への影響を時系列で把握できます。

# SecurityScorecardについて

SecurityScorecardはサイバーセキュリティレイティングのグローバルリーダーで、1,200万社を超える企業が継続的に評価を受ける唯一のサービスです。SecurityScorecardの特許取得済みのレイティングテクノロジーは、1,700以上の組織でセルフモニタリング、サードパーティリスク マネジメント、取締役会レポート、サイバー保険の引受に活用されており、外部から確認できるデジタルフットプリント全体のサイバーセキュリティリスクの発見と修正を容易にすることで、すべての組織の回復力を高めています。SecurityScorecardは、サードパーティのサイバーセキュリティに関するアンケート回答を自動的にマッピングしてリスクを瞬時に評価し、真の意味で360度ビューを提供する唯一のプロバイダーです。

## さらに詳しくは
## デモをご依頼ください。

SecurityScorecard

SecurityScorecard 株式会社
〒100-0005
東京都千代田区丸の内一丁目 1 番 3 号
日本生命丸の内ガーデンタワー 3 階
marketing-jp@securityscorecard.io
www.securityscorecard.io/jp