Press Release
報道関係各位

SecurityScorecard株式会社
2025年7月9日

※本リリースは、米国時間2025年6月25日に米国SecurityScorecardより発表されたプレスリリースの抄訳です。

SecurityScorecard
2025年サプライチェーンサイバーセキュリティトレンド調査を発表
- 6社中5社がサプライチェーンに対するセキュリティの未熟さでリスクにさらされていることが明らかに -

SecurityScorecard株式会社（本社：米国、ニューヨーク州、CEO：アレクサンドル・ヤンポルスキー、以下SecurityScorecard、日本法人代表取締役社長　藤本 大）は、「2025年サプライチェーンサイバーセキュリティトレンド調査」（英語）を発表しました。本調査では、サイバーセキュリティ責任者の88%がサプライチェーンに対するサイバーリスクに懸念を抱いていることが明らかになりました。世界各国の約550名のCISOおよびセキュリティ専門家から得られたインサイトに基づいており、多くの組織におけるサプライチェーンに対するサイバーリスクの管理が、拡大する脅威に対応しきれていない実態が浮き彫りになりました。

Verizonの2025年度データ漏洩/侵害調査報告書によると、サードパーティに起因する情報漏洩は15%から約30%に倍増しています。現在、少数のサードパーティプロバイダーが世界のテクノロジーとインフラの多くを支えており、それによって極端にリスクが集中する構造が生まれています。たった一社のプロバイダーが侵害されるだけで、数千の組織が同時に影響を受ける可能性があります。攻撃者はこの構造を理解しており、サプライチェーンは格好の侵入口となっています。各ベンダーとの関係が、新たな攻撃対象面（アタックサーフェス）を広げることになるのです。守る側はすべての接続やネットワーク階層（サードパーティからn次パーティまで）を守る必要がある一方、攻撃者はたった一つの脆弱性を突けばよいという、非対称性が浮き彫りとなっています。

SecurityScorecard最高脅威インテリジェンス責任者であるライアン・シャーストビトフ氏は、次のように述べています。
「サプライチェーンを狙ったサイバー攻撃は、もはや一過性の出来事ではなく、日常的な脅威となっています。しかし、多くの組織では、サードパーティに対するリスク管理が依然として受動的であり、特定時点での評価やコンプライアンスチェックリストに重点が置かれているため、侵害が後を絶ちません。この時代遅れの静的なアプローチでは、動的に進化する脅威には対応することが難しくなっています。今こそ必要なのは、能動的な防御体制への転換です。具体的には、サードパーティのリスク管理チームとセキュリティオペレーションセンターを連携させ、継続的な監視と脅威インテリジェンスをリアルタイムの対応に連動させることが不可欠です」

主な調査結果：

- 70%以上の組織が、過去 1 年間にサードパーティに起因した重大なサイバーインシデントを少なくとも 1 件経験し、5% の組織は10 件以上のインシデントを経験
- 50%未満の組織しか、自社のn次サプライチェーンのうち半分以上のサイバーセキュリティ状況を把握していない
- 79%の組織では、n次サプライチェーン全体の半分以下しかサイバーセキュリティプログラムの対象になっていない
- 26%の組織のみが、サプライチェーンのサイバーセキュリティプログラムにインシデント対応を組み込んでいる
- 88%の回答者が、サプライチェーンに関するサイバーリスクについて懸念している
- 40%近くの回答者が、情報過多と脅威の優先順位付けの困難さを最大の課題として挙げている

推奨事項
本調査に基づき、SecurityScorecardは以下の重点的な対策を推奨しています：

- **脅威インテリジェンスの統合**：サプライチェーン全体を網羅する脅威インテリジェンスフィードを、ベンダーリスク管理ワークフローへ統合、ランサムウェアやゼロデイ攻撃の兆候をリアルタイムで検知
- **専用のインシデント対応体制を確立**：サプライチェーンに関するリスクを速やかに解決するため、組織内で役割と責任を明確化、対応プロセスの継続的な検証と改善を実施
- **ベンダー階層化（ティアリング）の導入とリスク優先順位付け**：サプライチェーンマップを作成し、リスクの高い依存関係や障害点を特定し、重要度に応じたリソース配分と重点的な対策を実行
- **レジリエンスの文化と部門連携の推進**：調達、法務、オペレーション、経営層を含めた部門間の連携のもと、サイバーセキュリティを意思決定プロセスに組み込み、共通指標に基づく評価と教育を実施

調査方法
本レポートは、サイバーセキュリティ業務に従事するITディレクター以上の役職者546名を対象としたアンケート調査をもとに、定量的に分析を行ったものです。回答者は、世界各国の多様な業種の大企業に所属しており、年間売上高は2億ドル未満から50億ドル超までの企業規模です。

その他のリソース

- 2025年サプライチェーンサイバーセキュリティトレンド調査「2025年サプライチェーンに対するサイバーセキュリティのトレンド：可視性が次の競争優位性となる理由」（英語）

SecurityScorecardについて
Evolution Equity Partners、Silver Lake Partners、Sequoia Capital、GV、Riverwood Capitalなど、世界トップクラスの投資家から出資を受けたSecurityScorecardは、サイバーセキュリティ レーティングにおけるグローバルリーダーであり、Supply Chain Detection

and Response（SCDR・サプライチェーンにおける検知・対応）ソリューションのパイオニアです。
セキュリティとリスクの専門家であるアレクサンドル・ヤンポルスキー博士とサム・カッスーメによって2013年に設立されたSecurityScorecardの特許取得済みセキュリティレーティングテクノロジーは、企業のリスク管理、サードパーティリスク管理、取締役会報告、デューデリジェンス、サイバー保険の引き受け、規制当局の監視のために25,000以上の組織で使用されています。
SecurityScorecardは、企業におけるサイバーセキュリティ・リスクの理解、改善を促進し、取締役会、従業員、ベンダーに伝える方法を変革することで、世界をより安全にすることを目指します。https://jp.securityscorecard.com/

日本法人社名 ：　SecurityScorecard株式会社（セキュリティスコアカード）
本社所在地 ：　東京都千代田区丸の内一丁目 1 番 3 号
代表取締役社長 ：　藤本 大

【本件に関する連絡先】
SecurityScorecard
広報代理店 株式会社プラップジャパン
担当　菊池(070-2161-7123)、牟田(090-4845-9689)、冨安(070-2161-6963)
Email: securityscorecard@prap.co.jp