

Press Release

報道関係各位
SecurityScorecard株式会社
2024年9月2日

※本リリースは、米国時間2024年8月5日に米国SecurityScorecardより発表された[プレスリリース](#)の抄訳です。

Forbes Global 2000企業の99%がサプライチェーンの侵害に直接関与

[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）と[Cyentia Institute](#)の最新調査「[Global 2000: 業界の巨人がサプライチェーンのサイバーリスクという脅威と闘う](#)（英語のみ）」によると、[Global 2000 企業の 99%](#)が、最近侵害を経験したベンダーと直接関係していることが明らかになりました。本レポートでは、SEC（米国証券取引委員会）が新たなサイバーセキュリティ要件に基づき、開示を求める第三者による侵害に対する透明性により、マルチパーティ サプライ チェーン攻撃のリスクが高まっていることを強調しています。

現代のビジネスは互いに密接に関連しているため、サプライ チェーンの一部に脆弱性が存在すると、その影響は広範囲に及び、エコシステム全体に波及する可能性があります。Change Healthcare、MOVEit、SolarWinds などの大規模なサードパーティに起因したインシデントは、サプライチェーンにおける堅牢なサイバーセキュリティが極めて重要であることを強調しています。

主な調査結果:

- Forbes Global 2000 企業の 99% が、サプライ チェーン of 侵害に直接関係しています。
- これらの大企業の20% は、1,000 種類以上の製品を使用しています。
- サプライ チェーンに起因したインシデントの修復と管理には、自社での侵害対応と比較して17 倍のコストがかかります。
- Forbes Global 2000 の侵害による推定総損失額は、15ヶ月間で 200 億ドルから 800 億ドルに及びます。
- Forbes Global 2000 企業は相互依存性が高く、90% が互いにベンダーとして機能しているため、重大なリスクの集中に直面しています。
- 最も広範囲で導入されている上位 8 社のベンダー製品/サービスは、Forbes Global 2000 企業の少なくとも 80% で使用されており、しかも、上位 5 社のうち 4 社の製品/サービスを使用している企業では最近侵害が発生したと報告されています。

Cyentia Instituteのパートナー兼共同設立者であるウェイド・ベイカー氏は、次のように述べています。

「Forbes Global 2000は51.7兆ドルの収益を誇る一方で、その高い相互接続性が深刻なサイバーリスクを引き起こしています。99%の企業が侵害を経験したベンダーや数百億ドル規模のインシデントに直接関係しています」

サプライチェーンを把握する

悪意ある DDoS 攻撃、またはパッチ適応の遅れであれ、サプライチェーンにおけるインシデントの最終結果は同じで、ユーザーは重要なシステムへのアクセスを拒否されます。

サプライチェーンの把握は、サイバーレジリエンスの重要な要素になりつつあります。組織内およびベンダー間の依存関係を理解することは、効果的にインシデントに対応する上で不可欠です。最も信頼できるベンダーやパートナーであっても、問題が発生する可能性があります。

サプライチェーンにおけるセキュリティを確保するための主な手順は、次のとおりです。

1. 外部の攻撃対象領域を継続的に監視: 継続的な自動スキャンにより IT エコシステムを保護し、ベンダー、代理店、パートナーの IT インフラストラクチャ全体とサイバーセキュリティのリスクを特定し、軽減します。
2. 単一脆弱点を特定: 重要なビジネス プロセスとテクノロジーをマッピングし、単一脆弱点を特定します。これにより、ベンダー関連の警戒リストを作成します。
3. 新しいベンダーを自動的に検出: ベンダーの IT 環境を監視し、隠れたサプライチェーンのリスクを特定して解決します。

脅威調査およびインテリジェンス担当上級副社長のライアン・シェルストビトフ氏は、次のように述べています。

「世界は、リスクの集中によって引き起こされる混乱の可能性を理解し始めたばかりです。サプライチェーンを理解し、適切に管理することは事業継続性を維持するために不可欠です。それは単に混乱を防ぐだけでなく、相互に関連する経済基盤そのものを保護することでもあります」

方法論

Forbes Global 2000 は、売上高、利益、資産、時価総額の 4 つの指標を使用して世界最大の企業をランク付けしています。2024 年のリストでは、収益が 51.7 兆ドル、利益が 4.5 兆ドル、資産が 238 兆ドル、時価総額が 88 兆ドルに達しています。分析によると、Forbes Global 2000 のセキュリティ体制と侵害経験、およびこれらの企業を取り巻くサードパーティ ベンダーのエコシステムに直接焦点を当て、サプライチェーン全体にわたるサイバーリスクの性質を明らかにしました。

サードパーティに関するデータは、SecurityScorecard の自動ベンダー検出機能から取得されます。自動ベンダー検出は、現代の組織のデジタル サプライチェーンを構成するベンダーと製品を識別します。

SecurityScorecard は、インターネットを継続的にスキャンし、脆弱なデジタル資産や構成ミスのあるデジタル資産を特定します。さらに、SecurityScorecard は、北米、南米、アジア、ヨーロッパにまたがるグローバル センサーネットワークを活用し、インターネット全体を監視しています。同社は、世界最大級のシンクホールおよびハニーポット ネットワークを運営し、悪意ある信号を捕捉することで、商用およびオープンソースのインテリジェンス ソースを活用してデータセットを強化しています。

その他のリソース

- [「Global 2000: 業界の巨人がサプライチェーンのサイバー リスクという脅威と戦う」レポート](#) (英語のみ)
- [SecurityScorecard、Forrester Waveのサイバーセキュリティリスク評価においてリーダーに選出](#) (英語のみ)

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が出資するSecurityScorecardは、サイバーセキュリティの格付け、対応、回復力におけるグローバルリーダーであり、1200万社以上の企業が継続的に格付けを受けています。

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。SecurityScorecardは、Federal Risk and Authorization Management Program (FedRAMP) Readyの指定を受け、顧客情報を保護するための同社の強固なセキュリティ基準を強調し、[米国のCybersecurity & Infrastructure Security Agency \(CISA\)によって無料のサイバーツール](#)およびサービスとして登録されています。すべての組織は、信頼性と透明性の高いInstant SecurityScorecardの評価を受ける普遍的な権利を有しています。

www.securityscorecard.com/jp/

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)、富安(070-2161-6963)

Email: securityscorecard@prap.co.jp