

Press Release

報道関係各位

SecurityScorecard株式会社

2024年11月28日

※本リリースは、米国時間2024年11月20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

「小売業界における脅威インテリジェンスレポート」を発表

米国大手小売業者の97%がサードパーティ由来の侵害を経験
年間最大の繁忙期を迎えるショッピングシーズンに向けて、小売業界における脆弱性を指摘

[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、2024年11月20日に「小売業界における脅威インテリジェンスレポート」を発表しました。このレポートでは、米国の小売業者上位100社の97%が過去1年間にサードパーティ由来のデータ侵害を経験しており、年間最大の繁忙期となるショッピングシーズンを迎える中、重大な脆弱性が存在していることを明らかにしています。

機密性の高い支払い情報や個人識別情報 (PII) を含む膨大な量の顧客データを保有している小売業者は、サードパーティ由来の侵害に対して特に脆弱です。非常に価値の高い顧客データは、サイバー犯罪者にとって「宝の山」であり、個人情報盗難、金融詐欺、その他の悪意ある目的に悪用されています。

SecurityScorecard 脅威リサーチおよびインテリジェンス担当上級副社長のライアン・シャーストビト氏は、次のように述べています。

「ホリデーセールを迎える中、小売業者は決して警戒を緩めてはいけません。サイバー犯罪者は隙を突こうと狙っています。たった1度のデータ漏洩が、企業の収益を壊滅させ、消費者の信頼を取り返しのつかないほどに損う可能性があります。小売業者に注目が集まる中、小売業者は足を止めている余裕はありません。自社だけでなく、取引先を含めたセキュリティ対策を最優先にすることが不可欠です」

主な調査結果

- 米国大手小売業者の**97%**がサードパーティ由来の情報漏洩を経験しています。侵害を受けたサードパーティベンダーは全体の**4%にすぎず**、サードパーティの脆弱性による影響が広範囲に及んでいることが明らかになりました。自社が要因での漏洩を経験した小売業者は **12社**のみでした。
- **97%**の企業がフォースパーティベンダー由来の侵害を経験しており、その原因はフォースパーティベンダー全社のわずか**2%**のみに起因しています。
- **米国の小売業者上位20社**はいずれも、サードパーティ由来の情報漏洩を経験しています。
- 小売業者の**22%**がセキュリティ評価「A」を獲得している一方、評価「B」の小売業者は、データ漏洩のリスクが**2.9倍**高くなっています。

小売業界向けのサイバーセキュリティに関する推奨事項

この分析に基づいて、SecurityScorecard STRIKE チームは、小売業界のサイバーセキュリティを強化するための具体的なインサイトを提供しています。

- **外部攻撃対象の継続的な監視**：自動スキャンを導入し、ベンダーおよびパートナー環境における IT インフラとサイバーセキュリティリスクを検出します。
- **単一の障害点を特定**：重要な業務プロセスやテクノロジーをマッピングし、単一の障害点を特定します。これらのベンダーをリスト化し、重点的に監視します。
- **新規ベンダーを自動検出**：ベンダーの IT 環境を受動的に監視し、潜在的なサプライチェーンにおけるリスクを特定して解決します。
- **eコマースサイトをサポートする外部テクノロジーを精査**：サードパーティ製品やサービスは、攻撃者がeコマースサイトに侵入し、クレジットカード情報を収集する手段となっているため注意が必要です。

調査方法

SecurityScorecard の研究者は、2023 年の世界の小売売上高を基に米国トップ100 社の小売業者を分析し、サードパーティおよびフォースパーティのベンダーを含む 14,000以上のドメインを評価しました。

SecurityScorecard は、世界中の企業のサイバーセキュリティパフォーマンスに関する大量の非侵襲的データを収集しています。このデータを基に、SecurityScorecard はセキュリティ侵害の予測に有効な 10 の要因を用いて「A」から「F」までの企業の総合スコアを算出しています。

SecurityScorecard のThreat Research, Intelligence, Knowledge, and Engagement(STRIKE) チームについて

独自の脅威インテリジェンス、インシデント対応の経験、サプライチェーンのサイバーリスクに関する専門知識を兼ね備えています。SecurityScorecardのテクノロジーに支えられた STRIKEチームは、世界中のCISOの戦略的アドバイザーとなり、STRIKE チームによる脅威調査を基に、組織にサプライチェーンのサイバー リスクと攻撃者の特性に関してアドバイスをを行っています。

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)、富安(070-2161-6963)

Email: securityscorecard@prap.co.jp