

## Press Release

報道関係各位

SecurityScorecard株式会社

2024年12月17日

※本リリースは、米国時間2024年12月12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 サイバーセキュリティ侵害に関するレポートを発表 -米国主要銀行の97%がサードパーティ由来のデータ侵害を経験-

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、「サイバーセキュリティ侵害に関するレポート 2024」を発表しました。本レポートでは、米国の時価総額上位銀行100行の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、銀行業におけるサプライチェーンに重大な脆弱性が存在することを明らかにしています。

銀行が業務の中核をサードパーティベンダーに依存する割合が増加するにつれ、サプライチェーンに関連したリスクも増大しています。SecurityScorecardの専門家は、業界最大規模の独自のリスクおよび脅威インテリジェンスに関するデータセットを活用し、サードパーティ由来のデータ侵害が金融業界に及ぼす影響を分析しました。サードパーティ由来の侵害が深刻なリスクをもたらす中、サードパーティベンダーへの依存構造を包括的に把握することが、リスクの軽減とレジリエンスの確保に不可欠となっています。

## SecurityScorecard 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・シャーストビトフは、次のように述べています。

「米国の大手銀行の大多数がサードパーティ由来の侵害を経験していることから、相互接続されたデジタルエコシステム全体に深刻な脆弱性が存在していることが明らかになりました。最近のクラウドストライクのインシデントは、エコシステム上の脆弱性の存在を浮き彫りにし、侵害が発生しなくとも、たった1社のベンダーに起因する問題が広範囲に影響を及ぼすリスクを生み出す可能性があることを示しました。銀行にとって、サードパーティにおける脆弱性は、その脆弱性を保有するサードパーティベンダー1社が侵害されるだけで、金融システム全体を不安定に陥れる可能性があることを示唆しています」

## 主な調査結果

- 米国主要銀行の**97%**がサードパーティ由来のデータ侵害を報告している一方、侵害の被害を受けたベンダーはわずか**6%**となっており、サードパーティ由来のインシデントの影響が広範囲に
- 米国主要銀行の大多数（**97%**）が、わずか**2%**のフォースパーティベンダーに由来するデータ侵害を経験

- 米国主要銀行の**上位10行**すべてがサードパーティ由来のデータ侵害を経験しており業界全体のリスクを浮き彫りに

### 金融業界向けのサイバーセキュリティに関する推奨事項

この分析に基づき、SecurityScorecard STRIKE チームは、銀行業界のサイバーセキュリティを強化するための実用的な洞察を提起しています。

- **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
- **単一障害点を特定**：重要な業務プロセスやテクノロジーを把握し、単一の障害点を特定します。また、ベンダーをリスト化し、重点的に監視
- **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、隠れたサプライチェーンリスクを特定して解決

### 調査方法

SecurityScorecard の研究者は、米国の時価総額上位100 行を分析し、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 9,000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。

### その他のリソース

- SecurityScorecardの脅威インテリジェンスの詳細については、[当社のウェブサイト](#)（英文のみ）をご覧ください。

### 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](mailto:securityscorecard@prap.co.jp)