Press Release

報道関係各位

SecurityScorecard株式会社
2024年5月８日

※本リリースは、米国時間2024年2月28日に米国SecurityScorecardより発表されたプレスリリースを基に、日本向けに内容を編集しています。

SecurityScorecard、
世界のサードパーティサイバーセキュリティ侵害に関するレポートを発表
- 日本における全侵害の48%がサードパーティ由来の攻撃を起点に -

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**世界のサードパーティサイバーセキュリティ侵害に関するレポート**を発表しました。

本調査では、リスクと脅威に関する世界最大のSecurityScorecard独自のデータセットを基に、SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement（STRIKE）の脅威分析官が、サードパーティリスク管理（TPRM）の対象となるサードパーティ侵害に焦点を当て、脅威全体においてサードパーティ侵害がどのくらいの頻度で起こっているかを調査し、業界や地域ごとにその頻度の変動を特定し、サードパーティ侵害の頻度が高い外部関係を明らかにしています。そして、この分野で特に活動が目立つ攻撃者グループと、最も頻繁に悪用されているソフトウェアの脆弱性が判明しました。

重要な調査結果（日本）

- **侵害の48%がサードパーティ由来の攻撃を起点にしています。**
  世界全体の割合（29%）を大きく上回っており、日本ではすべてのインシデントのほぼ半数を占めています。上位国の侵害件数総数に占めるサードパーティ侵害の割合を見てみると、明らかに突出しています。

日本のサードパーティ侵害は、従来の系列内の提携から頻繁に発生しているのか、比較的新しいベンダーとのより「匿名的な」アウトソーシング契約から発生しているのか、あるいは、その両方から発生しているのか、という疑問が生じます。弊社サンプル内で、日本において侵害の被害を受けたサードパーティとの関係を精査しましたが、明確な答えは得られませんでした。しかしながら、さらなる調査により明らかになる可能性はあります。

重要な調査結果（世界全体）

1. **侵害の 29% 以上が、サードパーティ由来の攻撃に起因しています。**
2. 犯罪脅威グループ **Cl0p**（FIN11、TA505、Graceful Spider、Gold Tahoe、SectorJ04、Hive0065、G0092 とも呼ばれます）**は、他と比べて圧倒的に発覚件数が多く、最も活発に活動している攻撃者グループです。特にサードパーティ侵害で、その傾向がより顕著にみられます。**
3. Cl0p が暗躍している大きな理由は、MOVEit ファイル転送ソフトウェアの**ゼロデイ脆弱性を大規模に悪用しているという点です。これは、最も多く悪用された脆弱性でもありました。**
4. **サードパーティ侵害が最も多く発生したのは、医療および金融サービス業界です。**これら 2 つの業界におけるサードパーティ侵害は、弊社サンプル内のサードパーティ侵害に占める割合が最大（医療）および 2 番目（金融サービス）でした。
5. **テクノロジーおよび電気通信業界におけるサードパーティ侵害は、**弊社サンプル内のサードパーティ侵害全体に対する割合としては小さいものでした。それにも関わらず、**この業界では内数としてのサードパーティ侵害の発生率が最も高い割合（43%）でした。**
6. **サードパーティ侵害を引き起こした外部関係の 75% には、ソフトウェアまたはその他のテクノロジー製品およびサービスが関わっていました。**サードパーティ侵害の残りの 25% には、技術的でない製品またはサービスが関係していました。
7. サードパーティ侵害の頻度は、国や地域によって大きな差はないようですが、**日本での傾向は異なるようです。**
8. **医療におけるエコシステムはサードパーティとの関係が複雑で、**多数の高度な専門ベンダーがケア サイクルの各種段階に係わっています。**これが、医療業界全体が、特にサードパーティ侵害の被害者になりやすい理由の 1 つであるといえます。サードパーティの数が増えると、サードパーティリスクも増加します。**サプライチェーンが従来の垂直統合の形態から多様化している日本でも、同様の要因がはたらいている可能性があります。
9. ソフトウェアやその他のテクノロジー製品やサービスがサードパーティによって侵害されると、多くの場合、攻撃者は最小限の労力で攻撃範囲を拡大できるようになります。**つまりその攻撃者は、他の攻撃者より活発になります。**

2023年のセキュリティ侵害に関するこのレポートは、SecurityScorecardの新しいBreachDetails脅威インテリジェンス・ソリューションを使用し、初めてまとめられました。BreachDetailsにより、SecurityScorecardはAIを駆使し、ニュース記事、ランサムウェア通知、国際的な情報源を分析することで、他の侵害通知プロバイダと比較して侵害データのカバー範囲を50%向上させました。

脅威リサーチ・インテリジェンス担当上級副社長のライアン・シェルストビトフは、次のように述べています。
「サプライヤーのエコシステムは、ランサムウェアグループにとって恰好のターゲットとなっています。サードパーティ由来の侵害の被害者は、ランサムウェアの攻撃通知を受けとるまでインシデントに気づかないことが多く、攻撃者が検出されることなく何百もの企業に侵入する時間的余裕ができてしまいます」

サードパーティ由来のサイバーリスクはビジネスリスク
米国証券取引委員会（SEC）の新しいサイバーセキュリティ事件開示要件に引用されているように、SecurityScorecardは、組織の98%が侵害されたサードパーティとの関係を持っていることを明らかにしました。Gartner® Researchは、次のように見解を表しています。「サードパーティ由来のサイバー侵害の復旧に掛かるコストは、通常、社内のサ

イバーセキュリティ侵害を修復するコストよりも40%高くなります」データ侵害の平均復旧コストは2023年には445万ドルに達し、企業はビジネスリスクを軽減するためにサプライチェーンのサイバーリスク管理を積極的に取り入れる必要があります。

SecurityScorecardのCEO兼共同設立者であるアレクサンドル・ヤンポルスキー博士は、次のように述べています。
「デジタル時代においては、信頼はサイバーセキュリティと同じように重要な意味を持ちます。企業は、デジタルおよびサードパーティのエコシステム全体にわたって、継続的で、測定可能な、ビジネスに沿ったサイバーリスク管理を実施することによって、回復力を向上させなければいけません」

詳細な分析とレポートのダウンロードこちら
https://securityscorecard.com/reports/third-party-cyber-risk/

注記
1 Forrester, "The State Of Third-Party Risk Management, 2022," Alla Valente, October 20, 20222
2 ガートナー、「CISOが採用すべき4つのサードパーティリスク原則」、ルーク・エラリー、サム・オリヤイ、2022年6月21日。GARTNERは、米国およびその他の国におけるGartner, Inc.および/またはその関連会社の登録商標およびサービスマークであり、許可を得て使用しています。無断複写・転載を禁じます。

スコアリング手法
本レポートのサンプルは、侵害に関する一般公開済みのレポートを収集する、社内開発した新しいフィードから得たものです。調査期間は、フィードが運用された最初の四半期である 2023 年第 4 四半期に収集したレポートに限定しました。報告された事件の多くは、去年前半に発生したものであることにご留意ください。侵害が世間に知られるまで、数か月以上かかることがあります。被害者が侵害を発見するまで数週間または数か月かかる可能性があり、（たとえ発覚したとしても）その後数週間または数か月は公開のレポートに掲載されないことがあります。全く公開されないこともあるのです。そのため、侵害レポートで起こりがちなこの時差/遅延を考慮に入れ、有用なデータポイントが除外されることを避けるために、今年の初めに発生したインシデントを含めることにしました。つまり、弊社のサンプルは、第 4 四半期に重点を置いた、2023 年全体の侵害のスナップショットとなっています。

SecurityScorecard STRIKEについて
STRIKEの脅威インテリジェンスチームは、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。STRIKEはSecurityScorecardのテクノロジーを活用し、世界中のCISOの戦略的アドバイザーとなっています。STRIKEの脅威リサーチにより、企業はサプライチェーンのサイバーリスクと攻撃者の特性を理解することができます。

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: 八代(070-2161-7123)、牟田(090-4845-9689)、冨安（070-2161-6963）
Email: securityscorecard@prap.co.jp