Press Release

報道関係各位

SecurityScorecard株式会社
2024年8月28日

※本リリースは、米国時間2024年7月31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
2024年 世界の航空業界に関するサイバーセキュリティレポートを発表

国家に支援を受けている攻撃とサプライチェーンに対するサイバーリスクが
今後の大きな混乱を示唆

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、民間旅客航空会社上位100社を含む世界の主な航空会社250社に関する最新のサイバーセキュリティレポートを発表しました。「世界の航空業界におけるサイバーリスク2024年版」（英語版のみ）と題する本レポートでは、セキュリティリサーチャーが航空業界とそのさまざまなサプライチェーンにおけるサイバーセキュリティの脆弱性を明らかにしています。

航空業界のサイバーセキュリティに関する新たな洞察
本レポートは、世界中の規制機関が航空業界に対するサイバーセキュリティ要件を強化する中で発表されました。米国運輸保安局は2023年3月に新たな規制を導入し、欧州委員会（EU）の規則2023/203が2026年に発効され、航空情報セキュリティリスク管理の新たな基準を確立します。

航空業界は従来、物理的なセキュリティ脅威に焦点を当ててきましたが、ボーイング社のサプライチェーンのリスクに関して最近明らかになった事実により、サプライチェーンのリスクを評価し、対策することが求められています。SecurityScorecardの最新調査は、特にサプライチェーンのサイバーリスクに関する意識を高めることを目的としており、航空業界全体の包括的なサイバーセキュリティ監視の必要性とベストプラクティスを強調しています。

主な調査結果

- 航空業界におけるサイバーセキュリティ評価は「**B**」：航空業界の平均評価は「B」でした。これは落第点ではないものの、サイバー攻撃の被害を受ける可能性が低いことにはなりません。評価「B」の企業は、評価「A」の企業よりも2.9倍もデータ侵害の被害に遭う可能性が高いことが明らかになっています。
- **IT**ベンダーと航空会社の脆弱性：特筆すべきは、航空業界に特化したソフトウェアおよびITベンダーのスコアが最も低いことで、平均スコアは83点で、航空会社にとってはサードパーティリスクとなります。同様に、航空会社もベンダーに対して第三者リスクをも

たらす可能性があります。例えば、この調査では、最近航空会社で発生した3件の情報漏えいにおいて、航空関連ベンダーの情報が流出した事例を紹介しています。

- サードパーティーによる情報漏えいの影響：調査対象企業の7%が、過去1年間に情報漏洩があったことを公表しており、17%が過去1年間に少なくとも1台のシステムが侵害されていたことが明らかになりました。さらに、航空会社では、低スコアのベンダーの脆弱性がサードパーティーリスクを高め、業界ベンチマークよりも4%多く侵害が発生しています。
- サイバーと地政学的脅威における世界的格差：西欧やオーストラリアのような先進国は、新興国よりもサイバーセキュリティが堅牢で、スコアは新興国を大きく上回っています。中国などの国家が支援する攻撃は、今後大きな混乱を予示しています。
- ランサムウェアが最大の脅威：ランサムウェアは、この業界において最大の脅威となっています。航空業界を積極的に標的とするランサムウェア攻撃グループには、BlackCat、LockBit、BianLian、Dunghill Leakなどが存在します。
- 業績との相関：業界および消費者基準で業績上位の航空会社のセキュリティスコアは平均を上回っており、業務運営における卓越性、そして特にサイバーセキュリティとの関連性を示しています。

航空業界に対するサイバーセキュリティに関する提言

本レポートの分析に基づき、SecurityScorecard の脅威リサーチャーは、航空業界のサイバーセキュリティ強化のための実用的なインサイトを提供しています。

- ソフトウェアおよび**IT**ベンダーの優先順位付け：サードパーティリスクが最も高いソフトウェアベンダーと IT ベンダーによるリスクの軽減に注力しましょう。
- サードパーティのリスク管理を強化：潜在的な脅威全般をカバーするため、サードパーティのリスク管理プログラムにパートナーやお客様など関連するすべての組織を含めましょう。
- 重要データの保護を強化：航空産業の知的財産や旅客データは、サイバー犯罪者や国家の支援を受ける攻撃者にとって価値の高いターゲットであるため、強固な防御策を導入しましょう。
- 身代金の支払いを控える：身代金の支払いを控えることで、攻撃を助長することを防ぎ、法的規制に遵守できます。

SecurityScorecard 脅威調査・情報担当上級副社長 ライアン・シェルトビトフ氏は、次のように述べています。
「航空業界のパートナーシップは複雑に入り組んでいるため業界内のセキュリティは脆弱なものとなっています。当社の調査では、航空会社はサードパーティのリスクに対して無防備であることが明らかになっています。乱気流が大惨事に発展する前に、航空業界全体で意識を合わせ、エコシステム全体で強固なセキュリティ対策の整備を優先すべき時です」

調査方法

SecurityScorecardは、上位の民間旅客航空会社100社、航空機およびその部品のトップメーカー50社、航空サービスのトッププロバイダー50社、航空に特化したソフトウェアおよびIT製品・サービスのトッププロバイダー50社を含む250の組織からサンプルを抽出しました。対象企業

は、業界ランキングや業界誌、消費者向け出版物から抽出し、定量的な指標と業績指標、戦略的な重要性を組み合わせています。

その他のリソース

- 「世界の航空業界に関するにおけるサイバーリスク2024年版」（英語版のみ）のダウンロードはこちら
- 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)、冨安(070-2161-6963)
Email: securityscorecard@prap.co.jp