

Press Release

報道関係各位

SecurityScorecard株式会社

2024年1月10日

※本リリースは、米国時間2024年1月9日に米国SecurityScorecardより発表された[プレスリリース](#)の抄訳です。

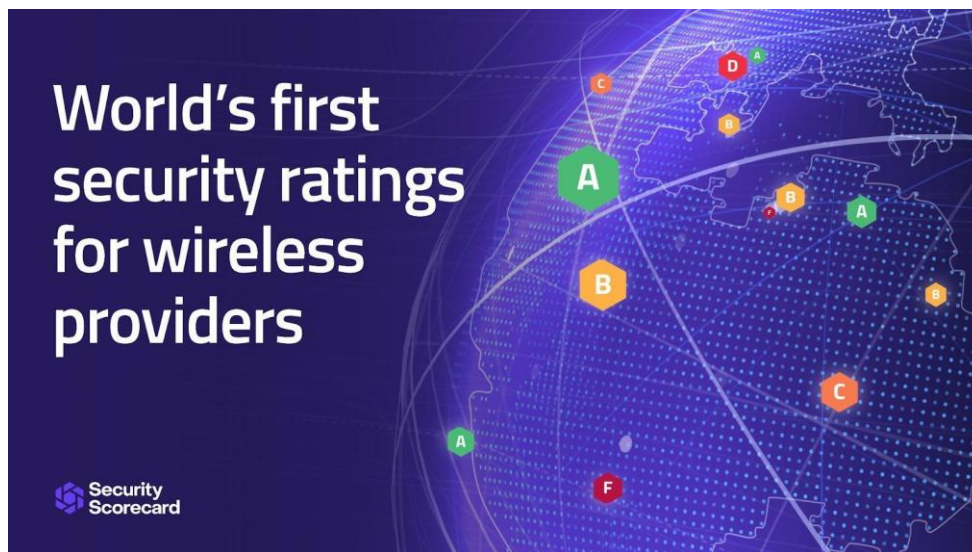
SecurityScorecard、業界大手企業と共同で 通信事業者、インターネットサービスプロバイダー、クラウドプロバイダー向けの 業種別セキュリティレーティングを提供

業界のフィードバックに基づく革新的スコアリング手法

[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、通信事業者、インターネットサービスプロバイダー、クラウドプロバイダー向けに開発した業界初の業種別セキュリティレーティングサービスを発表しました。このサービスは業界大手企業と緊密に連携し、実現されました。スコアリング手法は、通信業界全体でサイバーセキュリティの新しい基準を確立することが期待されています。

T-Mobile シニアバイスプレジデント兼最高セキュリティ責任者であるジェフ・サイモン氏は、次のように述べています。

「T-Mobileでは、お客様とその世界とのつながりを維持するという使命を果たす上で、当社のあらゆる業務活動にサイバーセキュリティを組み込むことが非常に重要であると考えています。セキュリティレーティングは、当社をはじめとするワイヤレスプロバイダーが、お客様やパートナー様のためにより安全なデジタルエコシステムを構築するために使用している重要なツールです。通信業界のセキュリティレーティング向上にむけたSecurityScorecardの積極的な取り組みは称賛に値するものです。今後は、T-MobileとSecurityScorecardが連携することで、サイバーセキュリティの新たな基準を設定できると考えています」



セキュリティレーティングの基準を設定

SecurityScorecardは標準化されたサイバーセキュリティ測定手法を通じて、サイバーセキュリティの透明性と信頼の回復に注力しています。今回開発した新たなスコアリングアルゴリズムは、業界のフィードバックに基づき、カスタマイズされたセキュリティレーティングのアプローチへの要求に対応しています。通信事業者、インターネットサービスプロバイダー、クラウドプロバイダー向けセキュリティレーティングの注目すべき強化機能は、次のとおりです。

- **業種別スコアリングの導入**：通信業界特有の複雑さを考慮した柔軟に適応可能な高度なスコアリングアルゴリズムを開発しました。このアルゴリズムは、通信業界特有の業務慣行（オープンDNSリゾルバ、他）を考慮に入れ、的確な評価を下します。
- **ネットワーク・パーティショニングによる正確性の向上**：ワイヤレスプロバイダーは、ネットワークが自社製品のため、非常に複雑なデジタルエコシステムに直面しています。従来、これらの企業は、IPやドメインなど、自社が所有するすべての資産（たとえ顧客がこれらの資産の大部分を管理していたとしても）を評価対象としていました。これを解決するため、SecurityScorecardでは、デジタル資産のスコア評価から顧客資産を除外しました。顧客資産は、自社のセキュリティポリシー、運用権限、管理の対象外であるため、これらの企業のリスクは限定的です。

- **AIが第三者へのリース資産を自動的に検出・分類**：SecurityScorecardは、独自のAIモデルによりサードパーティにリースされている資産を自動的に検出、分類します。組織はSecurityScorecardによって検出されたデジタルフットプリントを監査し、さまざまな資産が全体的なスコアにどのような影響を与えるかを把握することができます。SecurityScorecardは定期的に監査を行い、顧客資産の分類が正確であることを確認します。
- **ユーザーから提供されるデータの統合**：SecurityScorecardのスコアリング手法には、認証、ペネトレーションテスト、サイバーセキュリティトレーニングなどの成果を示す、ユーザーから提供されるデータが統合されるようになりました。SecurityScorecardは、SOC 2やISO 27001などの認証のための安全なリポジトリをエビデンスロッカーで提供しています。一旦文書が検証されると、組織はエビデンスに基づきスコアが改善されます。

NTT 最高情報セキュリティ責任者である横浜 信一氏は、次のように述べています。

「SecurityScorecardは、NTTグループにとって欠くことのできないパートナーです。通信業界が直面している特有の課題を理解するために、SecurityScorecardが行っている取り組みは、当社のサイバーセキュリティ戦略に大きく貢献するでしょう。SecurityScorecardとの協力体制により、セキュリティ対策を強化し、サイバーセキュリティに対する共同責任意識を育んでいくことでしょう」

デジタルの世界で信頼と透明性を促進

SecurityScorecardが実施した新しい調査によると、変革的なアプローチが急務であることが指摘されています。米国、英国、フランス、イタリア、デンマーク、ドイツの大手通信事業者のうち、サードパーティ由来のデータ侵害を受けた組織の割合は、過去12ヶ月で実に85%に達しています。この目を見張るような調査結果は、サプライチェーン全体でサイバーセキュリティを確保する上で指標ベースのアプローチの必要性が極めて高いことを示しています。

セキュリティレーティングは、サイバーセキュリティに対する社会の信頼を取り戻す力を持っています。1,200万を超える組織を注視しているSecurityScorecardの影響力は単なる理論上のものではなく、経験によって立証されています。広範囲にわたる調査では、「A」と評価された組織が侵害を受ける可能性は7.7倍低いことが判明しています。

SecurityScorecard 最高テクノロジー責任者であるクリストス・カランツィスは、次のように述べています。

「SecurityScorecardはアルゴリズムを継続的に改善し、組織のサイバーセキュリティを正確に反映したレーティングを行うことで、組織がその制御外のファクターによる不利益を被らなくて済むようにしています。サイバーセキュリティは日々変化し続けていますが、SecurityScorecardが誤検知率を1%未満に抑えていることを誇りに思います。弊社は、組織と協力することにより、セキュリティレーティングの精度を継続的に高め、関係者全員に利益をもたらすことができると考えています」

主な調査結果

- **大手通信事業者の85%がサードパーティによるデータ侵害を経験**：米国、英国、フランス、イタリア、デンマーク、ドイツの大手通信事業者のうち、過去1年間で85%の組織がサードパーティが原因のデータ侵害を経験していることが判明しました。
- **サードパーティによるデータ侵害を国ごとに分析**：
 - 米国 - 大手通信会社の90%がサードパーティによるデータ侵害を受け、さらに60%は自社ビジネスでもデータ侵害を経験
 - 英国 - 90%がサードパーティによるデータ侵害を経験
 - フランス - 78%がサードパーティによるデータ侵害を経験
 - デンマーク - 大手通信会社の67%がサードパーティによるデータ侵害を経験
 - イタリア - 大手通信会社の78%がサードパーティによるデータ侵害を経験
 - ドイツ - 100%がサードパーティによるデータ侵害を経験
- **サプライチェーンリスクが急速に増大**：注目すべきことに、調査対象となったサードパーティベンダーのうち、侵害を受けたのはわずか4%にとどまっており、サプライチェーンに脆弱性が1つあるだけでも、その波及的影響が大きいことを示しています。

SecurityScorecardは通信業界が直面する特有の課題に対し、あらゆる組織がデジタル資産を保護できるよう支援することに取り組んでいます。サードパーティによるデータ侵害を防ぐため、サプライチェーンのリスクは継続的に分析され、自動的に検出されます。

動的脅威識別では、顧客の広範なサードパーティおよびフォースパーティエコシステムをスキャンするなどして、ハッカーの視点でリスクを把握することができます。こうした包括的なアプローチにより、インシデントが発生するリスクを大幅に低減することが可能です。さらに、SecurityScorecardは、ベンダーが脆弱性やその他のセキュリティ上の問題に迅速に対処できるようにするための検証サービスも提供しています。

すべての組織に無料のセキュリティ評価を提供

SecurityScorecardは、セキュリティレーティングが社会と経済を守るために必要な基本的権利であると確信しています。10年以上前の設立以来、SecurityScorecardは、透明性、公平性、包括性という理念を堅持してきました。このコミットメントは、SecurityScorecardのプラットフォームに6万を超える組織の積極的な参加によって証明されています。

信頼と透明性は、組織が無料アカウントに登録した時点から、SecurityScorecardのすべての製品とサービスにより提供されます。SecurityScorecardは、サイバーセキュリティは連帯責任であり、セキュリティレーティングの正確性を確保するために誰もが発言権を持つべきだと考えています。

サイバーセキュリティの信頼と透明性に対するSecurityScorecardのコミットメントについては、<https://securityscorecard.com/trust/> をご覧ください。

公開時期

強化されたスコアリング アルゴリズムは、業界大手企業によるテストを経て、現在世界中で利用可能です。

ホワイトペーパーの詳細については、[こちら](#)をご覧ください。

SecurityScorecardについて

SecurityScorecard Inc.は、アメリカのニューヨーク州に本社を置く、2013年に設立されたサイバーセキュリティレーティングの世界的リーディングカンパニーです。1,000万以上の組織を継続的に評価し

ている特許取得済みのレーティング技術は16,000以上の組織で、自社のリスクマネジメント、サプライチェーン リスク マネジメント、経営陣向けのレポート、サイバー デュー デリジェンス、またサイバー保険の料率算定などに活用されています。自社グループ・取引先のセキュリティ リスクを定量的に可視化し、サイバー攻撃による侵害発生の可能性を低減するための具体的なアクションを促すことにより、世界をより安全な場所にすることを目標にしています。

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)、富安 (070-2161-6963)

Email: securityscorecard@prap.co.jp