プレスリリース

報道関係各位

SecurityScorecard株式会社

2026年3月17日

※本抄訳リリースは、米国時間2026年3月6日に米国SecurityScorecardより発表されたブログをもとに編集しています。

SecurityScorecard、
中東紛争における「サイバーリスクの波及」に関する最新調査を発表
-重要インフラとサプライチェーンを脅かす被害の連鎖に警鐘-

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、同社の脅威インテリジェンスチーム「STRIKE」による分析を基に、中東紛争における「サイバーリスクの波及」に関する最新調査を公開しました。本レポートでは、サイバー攻撃がもはや単なる軍事支援ではなく、戦場を構成する重要な領域になっている現状を指摘しています。また、中東地域のみならず、世界の重要インフラやサプライチェーンにまで影響を及ぼし、サイバー攻撃が引き起こす「波及リスク」に対して強い警鐘を鳴らしています。

■ 主な調査結果

中東における地政学的な緊張とサイバー攻撃の連動について、以下の事実が明らかになりました。

- サイバー攻撃の活用: 国家の支援を受けるハッカー集団やプロキシ（代理）組織は、サイバー攻撃を関与を否認できる形で、段階的な報復を可能にする手段として積極的に活用しています。
- 紛争と連動した組織的攻撃キャンペーン（**2025**年の事例）: 2025年に発生した12日間の武力衝突において、国家の支援を受ける攻撃者やイデオロギーに共鳴するハクティビストらが、敵対勢力に対して組織的なサイバー攻撃（偵察、データ窃取、DDoS攻撃、マルウェア配信など）を展開したことが確認されています。また、「Imperial Kitten」として知られるハッカー集団は、

地政学的な紛争の火種に同期した攻撃計画やタスク実行の運用サイクルを確率したことが判明しています。

- 日常生活への直接的な波及（伝達メカニズム）: 2026年現在、サイバー攻撃は地政学的な紛争と日常生活を繋ぐ「伝達メカニズム」となっており、国家間の戦略的な対立が、重要インフラ、商業、医療に影響を及ぼし市民生活への直接的な被害に結びついています。

■ 警戒すべき**4**つの波及領域

局地的な紛争が激化するにつれ、サイバー攻撃の影響は企業や民間人にも予期せぬ被害をもたらします。特に以下の4つの領域で深刻な影響が懸念されます。

- エネルギーおよび湾岸インフラ: 製油所やパイプラインの物流は象徴的かつ経済的価値が高く、限定的な機能停止でも市場に不安定な状況を引き起こします。
- 政府機関と公共サービス: 州や自治体のネットワーク、医療システム、緊急事態管理プラットフォームは、国防システムに比べて脆弱であり、破壊活動の標的になりやすい傾向があります。
- 交通と航空: 空港、海事物流システム、国境を越えた貨物プラットフォームの予約・管理システムの中断は、経済的な連鎖反応を引き起こします。
- サードパーティおよびサプライチェーンのリスク: 最も重大な間接的リスクです。マネージドサービスプロバイダー、SaaSプラットフォーム、リモートITツールなど、単一のベンダーが侵害されることで、数十の組織に被害が同時波及する恐れがあります。

今日、戦場は、物理的な領土だけに留まることはありません。組織のレジリエンスは、リスクをどれだけ早く可視化し、攻撃者が動く前にアタックサーフェス（攻撃対象領域）を縮小できるかにかかっています。

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行っています。

SecurityScorecardについて

SecurityScorecardは、サプライチェーン攻撃という最も急成長している脅威に対抗するため、Supply Chain Detection and Response（SCDR）領域を立ち上げました。業界をリードするセキュリティレーティングを基盤に、サードパーティリスクを継続的にモニタリングし、要因ベースのレーティング、自動アセスメント、独自の脅威インテリジェンスを用いて脅威を防御します。また、MAXを通じてサービスパートナーと連携し、サプライチェーン全体を保護し、運用におけるレジリエンス強化、第三者リスク管理の強化、単一の脆弱性からのエコシステム全体に及ぶリスクの低減を支援します。

SecurityScorecardは、Fortune 100の3分の2を含む3,000以上の組織に信頼され、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）からも信頼できるリソースとして認められています。

Evolution Equity Partners、Silver Lake Partners、Sequoia Capital、GV、NGP、Intel Capital、Riverwood Capitalなどを投資家に持ち、エンドツーエンドのサプライチェーンセキュリティを提供します。

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】

セキュリティスコアカード

広報代理店 株式会社プラップジャパン

担当 中田(070-7523-6980)、牟田(090-4845-9689)、冨安(070-2161-6963)

Eメール:securityscorecard@prap.co.jp