**Press Release**

報道関係各位

SecurityScorecard株式会社
2024年11月5日

※本リリースは、米国時間2024年10月23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、
# 米国エネルギー業界のサイバーセキュリティリスク調査レポートを発表
## サイバー侵害の67%がソフトウェアおよびITベンダーに起因
## エネルギー業界のベンダーへの依存の高まりに伴い、サプライチェーンリスクが急増

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）とKPMG LLPは2024年10月23日、米国大手エネルギー企業250社を対象に実施した共同サイバーセキュリティ調査レポート「米国のエネルギーサプライチェーンにおけるサイバーリスクの定量分析 (英語のみ）」を発表しました。本レポートは、エネルギー業界とそのサプライチェーン全体にわたるサイバーセキュリティの脆弱性について、セキュリティリサーチャーと業界の専門家による詳細な分析を提供しています。

**エネルギー業界サイバーセキュリティに関する新たなインサイト**
本レポートは、世界中の規制機関が米国のエネルギー業界に対し、サイバーセキュリティ要件とその取り組みを強化している極めて重要な時期に発表されました。2024年6月のG7サミットで討議された、増大するサイバー脅威に対する防衛強化の姿勢を反映しており、世界的にエネルギーのサプライチェーンにおけるサイバーセキュリティの強化が進んでいます。米国政府も「国際ランサムウェア対策イニシアチブ（CRI）」の第4回会議を開催し、参加68か国が共同声明「ランサムウェアに対する集団的な強靭性の構築」を発表しています。さらに、米国エネルギー省はエネルギー業界のリーダーと連携し、サプライチェーンにおけるサイバーセキュリティ原則を推進しています。

本調査レポートによると、エネルギー業界が頻繁に被害を被る脅威として、従来のITシステムに対するランサムウェア攻撃などエネルギー業界全般にわたり広範な混乱を引き起こすことが指摘されています。特に、産業用制御システム （ICS） とオペレーショナルテクノロジー（OT） への潜在的な攻撃に注目が集まっています。これらは引き続きリスク軽減の焦点となります。しかし、よりクリーンなエネルギーへの移行が加速する中、ソフトウエアへの依存が増加し、エネルギー業界の脆弱性も増大する可能性があります。

**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・シェルストビトフ氏は、次のように述べています。**
「エネルギー業界のサードパーティベンダーへの依存度が高まっていることは、重大な脆弱性を示しています。私たちの調査によると、この依存度の高まりが大きなリスクをもたらすと予想されます。国家的な侵害という緊急事態に発展する前に、業界は断固たる行動を取り、サイバーセキュリティ対策を強化する時です」

**主な調査結果**

- **エネルギー業界における高いサードパーティリスク:**エネルギー業界の侵害のほぼ半数 (45%) はサードパーティリスクに起因しており、世界全体の 29% を大幅に上回っています。複数の侵害を受けた企業の 90% は、サードパーティ ベンダー起因の被害を受けています。
- **米国エネルギー業界のサイバーセキュリティ評価は「B」:**SecurityScorecard の評価方法に基づくと、米国エネルギー業界は平均して「B」評価を受けており、81% の企業 が 「A」または「B」評価である一方、残りの 19%の企業は低評価となっており、 サプライ チェーン全体に重大なリスクをもたらしかねません。
- **サードパーティに起因した侵害はソフトウェアおよび IT ベンダーが起源:**サードパーティに起因した侵害の主な起源はエネルギー業界外のソフトウェアおよび IT ベンダーです。サードパーティに起因した侵害の 67% はソフトウェアおよび IT ベンダーが起源となっており、他のエネルギー企業が関与していた侵害はわずか 4 件でした。
- **再生可能エネルギー企業はサイバーセキュリティ体制に遅れ:**石油・天然ガス企業は平均を大きく上回る「A」評価である一方、再生可能エネルギー企業は「B」評価とサイバーセキュリティ対策の体制整備において遅れをとっています。
- **脆弱性は特定のリスクに集中:**92% の企業は、10 のリスク要因のうち 3 つ（アプリケーションセキュリティ40%、ネットワークセキュリティ23%、DNS健康度29%）で最も低い評価となっています。

**エネルギー業界向けサイバーセキュリティに関する推奨事項**

この分析に基き、SecurityScorecard STRIKE チームは、エネルギー業界のサイバーセキュリティ向上に向けた実行可能なインサイトを提示しています。

- **ソフトウェアおよび IT ベンダーを優先:**サードパーティ リスクをもたらす可能性が最も高いソフトウェアおよび IT ベンダーから、リスク軽減に注力
- **新テクノロジーによるセキュリティ重視:** CISA の「 セキュア・バイ・デザイン」や米国エネルギー省のサプライチェーン サイバーセキュリティ原則を採用して、新技術によるセキュリティを整備
- **再生可能エネルギー源のセキュリティを優先:**特に国家からの潜在的なサプライチェーンに対するリスクや地政学的脅威から保護するため、再生可能エネルギー向けのセキュリティプログラムを強化
- **混乱に備え、他のリスクとのバランスを:**データ侵害やその他の一般的なサイバーリスクへの備えを整備
- **海外のサイバー攻撃から学ぶ:** 海外のランサムウェア攻撃を研究し、強靭性とサイバーセキュリティ防御を強化

**KPMG 米国サイバーセキュリティ部門リーダーであるプラサナ・ゴビンダンクッティは、次のように述べています。**

「エネルギー業界は、安定したサプライチェーンに大きく依存する、世代交代を遂げつつある複雑ナシステムです。地政学的および技術的に脅威が増大する中、この複雑なシステムは国民と企業の両方に被害をもたらす可能性があります。また、同様に世代交代のリス

クにさらされています。これらのリスクを定量化し、対策を講じることができる組織は、エネルギー移行の行程で成功の可能性を高めるでしょう」

**方法論**
SecurityScorecard のリサーチャーは、米国トップ250のエネルギー企業を時価総額および各社が代表するさまざまな業界セクターに基づいて選定しました。対象には、従来の石油およびガスのサプライ チェーンの各段階や、サプライ チェーン全体をカバーする垂直統合型石油およびガス企業、一部のエネルギーを提供する公共事業、再生可能エネルギーに特化する企業が含まれます。

**その他のリソース**
- 「米国エネルギーサプライチェーンにおけるサイバーリスクの定量分析」をダウンロード（英語ページへ）
- SecurityScorecard の脅威インテリジェンスの詳細については、当社の Web サイトをご覧ください （英語ページへ）

**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。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