**Press Release**
報道関係各位

SecurityScorecard株式会社
2024年12月2日

# SecurityScorecard
# 2025年サイバーセキュリティに関する予測を発表

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、2025年におけるサイバーセキュリティに関する予測を発表しました。「サードパーティ由来の侵害による供給網全体へのインパクト」、「AI主導の採用詐欺の進化」、「CISOへの圧力の高まり」、「グローバル規制調和の必要性」など、2025年のサイバーセキュリティに関する予測をしています。

## 2025年サイバーセキュリティに関する予測

### 共同設立者兼CEO:アレクサンドル・ヤンポルスキー博士

**セキュリティに関する規制強化、ソフトウェアに対する禁止措置が現実のものに**
世界各国においてセキュリティに関する規制が一層厳格化し、組織やそのサプライヤーに対して高度な安全基準の順守を求める動きが加速すると予測されます。特に、セキュリティ上の既知の欠陥が存在するオープンソースを含む一部のソフトウェアは、全面的な使用禁止となる可能性があります。このような規制強化により、企業は使用するソフトウェアやサプライヤーとの提携について、徹底したリスク評価の責任を負うことになります。同時に、政府は重要インフラを守るための対策を強化し、システムの脆弱性を軽減するための取り組みを強化していきます。

**米国インフラに潜む国家によるスパイ活動**
トランプ政権の国家安全保障を最優先とする政策が、中国のサイバー活動に対する直接的な対抗措置に繋がる可能性があります。中国は脆弱なルーターや潜在的なネットワークデバイスを通じて、さらに多くの米国のインフラシステムを狙ってくると予測されます。これらの潜在的なエントリーポイントは、即時的な攻撃を目的とするものではなく、長期的な戦略資産として機能するでしょう。密かに確立されたネットワークアクセスは、国際的な緊張が臨界点に達した際に利用される可能性があるため、インフラの脆弱性に対する継続的な監視と迅速な対策がさらに重要になります。

**サードパーティ由来の侵害、供給網全体を揺るがす規模に拡大**
攻撃者がサプライチェーンの最も脆弱な部分を標的とする中、サードパーティを起点とした侵害が過去最高水準に達する勢いで増加しています。特に、高度なサイバー攻撃への防御が不十分な小規模なパートナー企業が、大規模な組織への侵入の足がかりとして悪用されています。この傾向は、企業に対してリスク管理戦略の抜本的な見直しを求める一方で、供給網全体のセキュリティ強化が急務であ

ることを明らかにしています。また、日本におけるサードパーティを介したサイバー攻撃の割合は、世界平均を大幅に上回っています。詳細については、「日本におけるサードパーティサイバーリスクの現状」レポートを参照ください。

**サプライヤーネットワークの継続的な監視が必須に**
従来の年次でのセキュリティレビューだけでは不十分となり、組織はサプライヤーネットワークを継続的に監視する必要性が高まっています。リアルタイムでリスクを検出・対処するアプローチは必須です。従来のセキュリティ手法に依存し続ける企業は、業務中断に伴う巨額のコストや、企業ブランドの長期的な毀損という深刻なリスクに直面する可能性があります。さらに、相互に接続されたシステム環境では、サプライヤーのセキュリティ施策に生じたわずかな隙が、ビジネスネットワーク全体に攻撃を拡散させる引き金となりかねません。

## 最高情報セキュリティ責任者（CISO）スティーブ・コブ

**CISOへの圧力が増大し、離職するCISOが後を絶たず**
セキュリティリーダーであるCISO（Chief Information Security Officer）に対するプレッシャーがさらに増し、侵害発生時の責任を、企業がCISO個人に押し付け、スケープゴートとして利用することが予測されます。このような状況は、経験豊富なセキュリティ担当者のCISO職への関心を大幅に低下させる結果を招きます。

さらに深刻なのは、サイバー侵害が増加して社会の目が厳しくなる一方、多くのCISOが管理職や取締役会への直接的なアクセスを制限されていることです。このような状況下でのサポートやコミュニケーションの欠如は、CISOが変革を推進する能力を著しく制約します。企業がCISOに十分な権限とリソースを与え、戦略的な役割を果たせる環境を整備しない限り、優れたセキュリティリーダーを確保することが困難になり、結果として重大なサイバー脅威に対してますます脆弱になります。

**AI主導の採用詐欺がLinkedInからZoomへ、脅威が一層大胆に**

2024年には、LinkedInでのAIのなりすましが驚くべき展開を見せ、攻撃者が採用担当者を装って開発者やエンジニアリングの人材をターゲットにしていました。攻撃者は、AIで生成されたペルソナを使用して接触を試み、採用試験を装って被害者に悪意あるファイルをダウンロードさせました。かつては詐欺メールだったものが、完全に没入型の採用詐欺へと変化し、攻撃者がAIを習熟するベースを加速し、使いこなし始めていることを浮き彫りにしました。

2025年には、LinkedInでの詐欺を超えて、AIによって生成されたソーシャルエンジニアリング攻撃がさらに進化するでしょう。攻撃者がより洗練されたAIを活用することで、AIが生成したよりリアルなZoom会議が登場し、ターゲットを欺き搾取する手法が予想されます。これらの没入型攻撃は従来のセキュリティ対策を回避し、信頼をベースにした新たな侵害の戦術となるでしょう。時代遅れの防御に依存する企業は、AIがよりインタラクティブな形式に発展する中で前例のない規模で人々を陥れる状況に、不意を突かれることになるでしょう。

## グローバル政府関係および公共政策担当副社長 ジェフ・リー

### 新政権下で国家による執拗なサイバー脅威が米国防衛を試す

次期米国大統領政権は、中国、イラン、ロシア、北朝鮮からのサイバー攻撃の急増に直面すると予測されます。台湾問題を巡る緊張が高まる中、中国は米国における重要インフラへの攻撃を強化する可能性があります。一方、ロシアは西側の分断を利用してNATO同盟地域を不安定にさせるため、情報操作やDDoS攻撃を仕掛けるでしょう。北朝鮮はランサムウェアや暗号通貨の窃盗を活用し、体制維持を図ると予想されます。

AIを活用した情報操作や洗練された戦術を採用する敵対国に対峙するため、米国の防衛システムは迅速な適応が求められます。攻撃的なサイバー戦術への転換や国際協力の縮小は、最も必要な時に情報共有ネットワークに負荷を掛けるさせる可能性があります。政権は、重要資産を保護し、安定を維持しながら、研究と経済の優位性を守るために、積極的な抑止と強力な官民連携のバランスを取る必要があります。

### 州レベルのAI法が国家レベルのAI規制強化をけん引、米国のAIリーダーシップを試す

カリフォルニア州とテキサス州は、AI規制の変革時代を主導し、ランサムウェア、LLMの安全性と監視、倫理的AIの使用など、緊急課題に取り組む法案を策定して他州のモデルとなるでしょう。しかし、州固有の規則は連邦政策との齟齬を生み、州境を越えて事業を展開する企業にとって、コスト増加やコンプライアンスの複雑化、運用上の障害を引き起こす可能性があります。

過去における州のプライバシー法と連邦の不作為からの教訓は、類似した経験を示唆しています。それぞれの州法が施行されていく中、連邦政府への圧力が高まるでしょう。一貫したアプローチは、経済的影響を最小化し、イノベーションを妨げないようにするために重要です。中国政府とのAI競争で優位に立つために、共和党が主導する新たな議会がトランプ政権と連携して「ルール」を優先できるかが鍵となります。中国におけるAI進展への懸念が超党派協力を促し、予想外の同盟を形成する可能性はありますが、バイデン政権が制定したAIに関する大統領令が撤回される可能性が高まる中、どれだけ議会が迅速にAI法制化を進めるかがが課題となるでしょう。この規制がコンプライアンスの課題を生む一方で、安全で倫理的なAI環境を育成し、中国のイノベーションに対する遅れを懸念する声を払拭できれば、新たな機会を提供する可能性もあります。

### 政府、グローバル規制調和の新時代へ

2025年、各国政府はサイバースペースの規制の複雑さに対処するため、グローバルでのガバナンスにおける転換期を迎えると予想されます。現在、国ごとに異なるサイバーセキュリティやデータプライバシー法が存在し、国境を越えて事業を展開する企業にとって、コンプライアンスの大きな負担となっています。
こうした課題の緊急性が高まる中、規制調和を目指す動きが2025年に本格化する見込みです。政府、国際機関、業界団体が連携し、米国、カナダ、オーストラリ

ア、英国、アジア諸国などで採用可能な共通基準やフレームワークの策定に向けた取り組みが進むと考えられます。一方、EUとの規制調整については、政治的・経済的な要因から進展が遅れる可能性があり、結果は依然として不透明です。それでも、より安全で信頼性の高いグローバルなデジタルエコシステムを実現するため、規制要件の簡素化と国際的な調和は、企業が効率的に運営し、リスクを軽減するための重要なステップとなります。

**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。https://jp.securityscorecard.com/

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