Press Release

報道関係各位

SecurityScorecard 株式会社
2024 年 4 月 26 日

※本リリースは、米国時間 2024 年 4 月 3 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、CISO 向けにサイバー脅威の傾向を解説した「2024 S&P 500 サイバー脅威レポート」を発表
-S&P 500 企業の 21%が 2023 年に情報漏えいの被害に-

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、S&P 500 企業を対象とした脅威調査を実施し、最高情報セキュリティ責任者（CISO）向けにサイバー脅威の傾向を解説した「S&P 500 サイバー脅威レポート」（英文のみ）を発表しました。本調査結果において、S&P 500 企業の 21%が 2023 年に情報漏洩の被害に遭った経験があることが判明しました。

2023 年秋、米国証券取引委員会（SEC）は新たなサイバーセキュリティ開示規則を採択し、米国の上場企業に対してサイバーセキュリティ インシデントが発生した際、そのインシデントを重要だと判断してから 4 営業日以内に詳細を開示することを義務付けました。採択以前は、インシデントの報告義務が「無い」に等しかったため、政府当局者、政策立案者、投資家はサイバーセキュリティインシデントに関する重要な関連情報を取得できずにいました。

SecurityScorecard 共同設立者兼 CEO であるアレクサンドル・ヤンポルスキーは、次のように述べています。
「規制の厳格化が進み、企業は明確な指標を備えたサイバーセキュリティ履行義務に向けた統一された定義を必要としています。金融業界のクレジットスコアリング標準化のように、企業にはサイバーセキュリティのリスクを測定し、重要性を定義するための統一フレームワークが必要です」

このような規制の厳格化を背景に、SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) チームは、米国経済の主要プレーヤーである上場企業のセキュリティを向上させる方法を見つけるために、S&P 500 企業のセキュリティ評価を分析しました。

主な調査結果

- **S&P 500 企業の 21%が 2023 年に情報漏洩を報告**
  攻撃者は金銭を狙っています。ランサムウェアを使った攻撃者は、株式時価総額に基づき、S&P 500 企業に対して高額の身代金を要求できると算段し、特に価値があるターゲットとみなしています。攻撃者は、より株式時価総額が高い企業が高額な身代金を支払えることを知っています。

- **上記侵害の 25%は、金融サービスおよび保険会社が被害に**
  金融機関は巨額の資金と資産を保有しているため、最も強固なセキュリティプログラムを実施しています。この調査は、金融業界が相互に関連しているという特徴から、一機関や普及している製品が侵害されることで、業界全体に広範な影響が及ぶ可能性があることを示しています。

- **52%の企業が個人情報を流出**
  攻撃者はソーシャルエンジニアリング攻撃を活用して、従業員情報へのアクセスに成功しています。熟練した攻撃者は、さまざまな情報源を組み合わせることにより、ソーシャルエンジニアリング攻撃をカスタマイズし、最大限の損害を与えたり、従業員になりすましたりします。

- **S&P 500 企業のソーシャルエンジニアリングリスクの平均は "F"評価**
  健全なリスクプロファイルと強固なセキュリティ体制を持つ企業であっても、ソーシャルエンジニアリングは、重大なリスクをもたらします。攻撃者が、ユーザーを操り、セキュリティソリューションを回避するために、ソーシャルエンジニアリングを攻撃手法の一つとして使用しています。

- **ランサムウェアによる攻撃では数百万ドルを要求**
  S&P 500 企業の被害者に対するランサムウェアの要求額は、現在では 8 桁台（ドルベース、日本円で数千万円程度）に上ることが多くなっています。ランサムウェアを使った攻撃では、従業員数や金銭的価値（株式時価総額や年間売上高など）といった企業規模に基づいて身代金要求が行なわれています。

- **サプライチェーン攻撃は重大な影響を及ぼす**
  攻撃者は、ターゲット企業に直接アクセスできない場合、その企業のベンダーやパートナー経由で狙ってきます。SEC 要件で引用されているように、SecurityScorecard の調査によると、98%の企業が侵害経験のあるサードパーティとの関係を有しています。よって、公開企業、非公開企業にかかわらず、サードパーティ企業も、新たな規制について十分理解する必要があります。

SecurityScorecard 脅威リサーチインテリジェンス担当シニアバイスプレジデントのライアン・シェルストビトフは、次のように述べています。
「サプライチェーンを狙った大規模なサイバー攻撃が数千の企業に影響を与え、数百万人の顧客データを流出したことを受け、企業はベンダー監視を優先するようになっています。企業におけるサイバーセキュリティの強化は、関連企業内の小規模ベンダーのセキュリティ対策も含まれます。」

最新の「2024 S&P 500 サイバー脅威レポート（英語のみ）」については、以下よりご覧ください。
https://securityscorecard.com/research/a-quantitative-analysis-of-the-security-ratings-of-the-sp-500/

SecurityScorecard 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 は、世界中の CISO の戦略的アドバイザーとなり、STRIKE 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 Inc.について
米国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。1,200 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 25,000 超の組織で、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)、冨安（070-2161-6963）
Email: securityscorecard@prap.co.jp