PRESS RELEASE

2020 年 8 月 6 日

Tenable Network Security Japan K.K

99%の日本企業が過去 12 か月間に少なくとも 1 回、ビジネスに悪影響を及ぼすサイバー攻撃を受けていることが新調査で明らかに

「会社のセキュリティとリスク度は大丈夫？」と問いかけられて自信を持って答えられるセキュリティ責任者は 10 人中 4 人のみ

※本リリースは米国で同時に発表されるプレスリリースの日本語版になります。

Cyber Exposure カンパニーと銘打つ Tenable®, Inc.が発表した世界のセキュリティ業界の調査結果によれば、「日本企業の大多数（99%）が過去 12 か月間にビジネスに悪影響を及ぼすサイバー攻撃を経験している」と、事業責任者とセキュリティ責任者が回答しています。このデータは、Tenable がフォレスターコンサルティング（Forrester Consulting）に委託して実施した調査の結果報告書「The Rise of the Business-Aligned Security Executive（ビジネス志向のセキュリティ担当エグゼクティブの台頭）」から得たもので、世界の 800 人以上の事業およびセキュリティ責任者を対象とし、日本国内の回答者は 51 人含まれています。

ネット犯罪者によって執拗な攻撃が繰り返される現在、国内の回答者の 81%が、ここ 2 年間にビジネスに悪影響のあるサイバーアタックが劇的に増加していると実感しています。残念ながらこのような攻撃は、調査の結果から株価の下落（46%）、なりすまし詐欺（44%）、機密データの侵害（42%）などのダメージを伴っていることがわかりました。また、オペレーショナルテクノロジー（OT）にも影響が波及していることが、国内のセキュリティ責任者のおよそ 68%の回答からわかります。

事業責任者は、事業戦略の策定と実施にあたって、自社のリスク度とその変容を明確に捉えることを望んでいます。しかし、ビジネスに被害をもたらすサイバー攻撃が頻繁に発生しているにも関わらず、「会社のセキュリティとリスク度は大丈夫？」という基本的な質問に自信を持って答えられる国内のセキュリティ責任者は 10 人中 4 人しかいません。

世界に拡がる回答結果のデータを見ても、「サイバーセキュリティの脅威を特定のビジネスリスクのコンテキストの枠組みで捉えている」と回答したセキュリティ責任者は全体の 50%未満。例えば、回答者の 96%は新型コロナウィルスの感染拡大に対応した戦略を展開しているのに、ビジネス面とセキュリティ面での戦略の整合は「少し」しかしていない、と 75%が認めています。

サイバーセキュリティをビジネスの戦略的リスクとして位置づけ、双方の責任者が整合して測定と管理を行っている企業は、その結果がデータに顕著に表れています。セキュリティのみを思考するサイロ思考型の責任者と比べて、ビジネスへ整合的な態度と思考を取るセキュリティ責任者は、

●8 倍、自社のセキュリティのレベルとリスク度をまとめて報告できる自信があることが推測できます。

○90%は、完全にまたは極めて確信を持って、サイバーセキュリティ投資が事業のビジネスパフォーマンスにポジティブに貢献していることを実証できると回答しています。サイロ思考型の責任者の場合、この値は 55%です。

○85%は、サイバーセキュリティの ROI を追跡するメトリクスがあると回答しています。サイロ思考型の責任者の場合、この値は 25%です。

●また、ビジネス整合的なサイバーセキュリティ責任者が在任している企業について、データから次のことが推測できます。

○3 倍、サイバーセキュリティの目標とビジネスの優先項目の歩調を合わせています。

○3 倍、企業のアタックサーフェス全体を総体的に把握しています。

○3 倍、資産の重大度と脆弱性を組み合わせた方法を使って修正作業の優先順位を設定しています。

「将来の CISO は、2 つのタイプ - ビジネスと直接整合を取るタイプとそうでないタイプ - に分かれるでしょう。このデジタルトランスフォーメーションの時代で成功する唯一の方法は、必ずサイバーをビジネスの課題、決定、投資の一部として考えることです。この調査結果は、進歩的な企業はサイバーセキュリティなしでは改革が不可能であると認識していること、そしてセキュリティとビジネスが密接に連携すれば結果が大きく変わることを示していると思います」と Tenable の共同設立者で最高技術責任者を務めるルノー・デライゾン（Renaud Deraison）は語っています。

メディア用情報：

●フォレスターコンサルティングは、世界 10 か国のセキュリティ責任者 416 人と事業責任者 425 人を対象にオンライン調査、また同責任者 5 人と電話インタビューを実施し、その結果から中～大規模の企業のサイバーセキュリティ戦略と実践の状況を分析しました。対象国は、日本、オーストラリア、ブラジル、フランス、ドイツ、インド、メキシコ、サウジアラビア、英国、米国。調査は 2020 年 4 月に実施されました。

●「ビジネスに悪影響を及ぼす」とはサイバーアタックまたはセキュリティの侵害によって顧客、従業員、その他の機密データが損失する、事業の運営に支障が出る、ランサムウェアに対する支払、財務上の損失または窃盗、知的財産の窃盗や損失などが生じることを指します。

調査結果はこちら

https://jp.tenable.com/analyst-research/forrester-cyber-risk-report-2020

■Tenable について

Tenable®, Inc.は Cyber Exposure カンパニーです。世界中の 3 万以上の企業と組織が Tenable のサービスを利用して、サイバーセキュリティリスクを把握して削減しています。Nessus®の開発者である Tenable は、脆弱性に対する専門性をさらに広げ、あらゆるコンピューティングプラットフォーム上のあらゆるデジタル資産を管理、保護できる世界初のプラットフォームを展開しています。Tenable は、Fortune 500 の半数以上、およびグローバル 2000 の 30%以上の企業や、大規模の政府機関などで採用されています。詳しくは、www.tenable.com をご覧ください。