Gartner

- News Release -

参考資料
【海外発プレスリリース】
本資料は、ガートナーが発信したプレスリリースを一部編集して、和訳したものです。
本資料の原文を含めガートナーの発信したリリースはすべて以下でご覧いただけます。
http://www.gartner.com/newsroom/

2018年7月18日

報 道 関 係 各 位

ガートナー ジャパン株式会社
広報室

ガートナー、サイバーセキュリティの専門家を有する企業はわずか65%とのサーベイ結果を発表

『ガートナー セキュリティ&リスク・マネジメント サミット 2018』(7月24～26日、八芳園) において、サイバーセキュリティに対する見解を発表

豪州シドニー発 － 2018年7月17日 － CIOの95%が今後3年間にサイバー攻撃による脅威が増加すると考えているにもかかわらず、現在社内にサイバーセキュリティの専門家がいると回答したCIOは65%にすぎない —— ガートナーは本日、サーベイの結果を発表しました。このサーベイでは、デジタル化を進めている企業にとってスキルの確保が引き続き課題であり、デジタル・セキュリティの人材不足がイノベーション (革新) にとって最大の阻害要因になっていることも明らかになりました。

2018年のガートナーCIOアジェンダ・サーベイでは、世界98カ国の主要業種に属する3,160人のCIOから回答を得ました。回答したCIOが所属する企業・機関の売上高／公的機関の予算の総額はおよそ13兆米ドル、IT支出総額は2,770億米ドルに達します。

サーベイでは、サイバーセキュリティが引き続き企業にとって深刻な懸念事項の1つであることが明らかになっています。企業が攻撃を未然に防ごうと躍起になっても、多くのサイバー犯罪者はさまざまな手段を講じるだけでなく、変化する環境への適応力も備えるようになっていると、ガートナーのリサーチ ディレクターであるロブ・マクミラン (Rob McMillan) は述べています。

マクミランは次のように説明しています。「うがった見方をすれば、サイバー犯罪者はデジタルのパイオニアであり、ビッグ・データやWebスケールのさまざまなテクニックを活用して攻撃を仕掛け、データを盗み出す算段を立てています。CIOは、すべての攻撃から自社を守れるわけではありません。このため、CIOは自社を保護するニーズとビジネスを運営するニーズのバランスを取り、持続可能な管理・統制基盤を確立しなければなりません」

今回のサーベイでは、35%のCIOが、既に何らかの形でデジタル・セキュリティに投資している、または展開していると回答しており、さらに36%のCIOは積極的に実験しているか近いうちに導入する予定であると答えています。ガートナーは、2020年までにセキュリティ予算の60%は検知と対応の能力の支援に使われると予測しています。

マクミランは次のように述べています。「サイバーセキュリティの準備についてターゲットとするレベルを設定するには、リスク・ベースのアプローチが不可欠です。サイバーセキュリティ予算

を増やすだけでリスク態勢を強化することはできません。セキュリティへの投資はビジネスの成果に基づいて優先順位付けを行い、適切な対象に適切な額を支出しなければなりません」

ビジネスの成長による新たな攻撃ベクトルの登場

今回のサーベイでは、多くのCIOが2018年のビジネスの優先事項として、成長と市場シェアをトップに挙げています。成長には、より多様なサプライヤー・ネットワーク、異なる働き方や投資モデル、テクノロジ投資のパターン、また異なる製品やサービス、サポートするチャネルなども含まれます。

マクミランは次のように述べています。「残念ながら、サイバーセキュリティの脅威は、より多くの企業に、より多様な方法で影響を及ぼすようになります。企業がこれらを予想することは難しいでしょう。これまで以上に危険な環境でビジネスを行うことになるという予測は、十分な情報に接しているCIOにとって目新しいニュースではないと思いますが、これらの要因によって、新たな攻撃ベクトルと新たなリスクが出現し、CIOは対応に苦慮するでしょう」

人材層の強化を継続

今回のサーベイでは、トップ・レベルのパフォーマンスを実現している企業のCIOの93%が、デジタル・ビジネスは、IT組織において変化への対応能力を高め、よりオープンなマインドセットを生み出したと回答しています。多くのセキュリティ・プラクティスのメリットとして、このようなオープンな組織文化によって、新しい採用や研修の手段に対する組織の考え方の幅が広がります。

マクミランは次のように述べています。「サイバーセキュリティの分野では、スキルを持った人材が不足しています。このような人材の不足はさまざまな調査報告で裏付けられており、イノベーション (革新) にとって最も大きな阻害要因の1つであると考えられます。企業におけるサイバーセキュリティの責務を負うことができる、有能で高い意識を持った人材を見つけることは困難であり、終わりのない仕事です」

ガートナーでは、ほとんどの企業はサイバーセキュリティの専門知識に特化した専任の役割を設けており、そのニーズを十分に理解していますが、一方でサイバーセキュリティのスキルを備えた人材不足は続くとの見解を示しています。ガートナーは、セキュリティ・チームの能力開発に革新的なアプローチを採り、引き続き人材層の強化を進めることを、CISO (最高情報セキュリティ責任者) に推奨しています。

今回のサーベイの結果を踏まえ、ガートナー リサーチ＆アドバイザリ部門リサーチ ディレクターの礒田 優一は、日本の状況について次のようにコメントしています。「国内においては、サイバーセキュリティの専門家を有する組織は、グローバルのサーベイよりもさらに少なく、同サーベイに参加した日本のCIOの回答でも51%という結果になっています。サイバーセキュリティの専門家を有する組織は、日本ではそれほど一般的ではありませんが、人材不足は国内においても同様の課題であり、世界共通であるといえます。また、テクニカルな分野における専門家のみではなく、経営者やビジネス・リーダーと対等にわたり合うことのできる、真のセキュリティ・リーダーの存在が不可欠になってきています」

ガートナーのサービスをご利用のお客様は、ガートナー・レポート「The 2018 CIO Agenda: Security and Risk Management Insights on Becoming a Digital CISO」で詳細をご覧いただけます。

ガートナーでは『ガートナー セキュリティ&リスク・マネジメント サミット2018』を、東京、サンパウロ、シドニー、ムンバイ (インド)、ロンドン、ドバイで開催し、ITセキュリティのトレンドに関する詳細な分析を提供していきます。

日本では7月24～26日、『ガートナー セキュリティ&リスク・マネジメント サミット 2018』を開催します。本サミットでは、前出のマクミランや礒田、ならびに国内外のアナリストおよびコンサルタントが、リーダーシップ能力を研鑽し、世界的に高まっているセキュリティ・リスクの問題に対してセキュアなデジタル・ビジネスを実現するにはどうすればよいのかについて、幅広いトピックにわたる最新のトレンドや最先端の知見・洞察を提供いたします。

本サミットの詳細については下記Webサイトをご覧ください。
http://www.gartner.co.jp/event/srm/

本サミットに関するニュースと最新情報は、ガートナーのTwitter (https://twitter.com/Gartner_jp) でもご覧いただけます (#GartnerSEC)。