2021 Global Digital Trust Insights－日本企業への示唆

PwCコンサルティング合同会社

はじめに

サイバーセキュリティはこれまで、テクノロジー利用の拡大と共に発展し、脅威との攻防をとおして知見や経験を蓄え、成熟してきました。しかし近年、状況は大きく変わろうとしています。デジタルを前提とした社会やビジネスへの変革が益々加速し、それに伴う脅威の変化・拡大は留まるところを知りません。サイバーセキュリティを重要な経営課題と捉え、全社一丸となって主体的に施策を推進する――。こうした考えのもと、時代の変革に応じて抜本的な改革へと舵を切る企業が出始めています。サイバーセキュリティはいわば、新時代への転換点に差し掛かっているのです。

このような状況下、PwCは全世界3,249名の経営者・テクノロジー担当責任者を対象にGlobal Digital Trust Insights 2021（以下、Global DTI 2021）調査を実施し、サイバーセキュリティのさらなるレベルアップを図るために実施すべき5つの行動を提言しました。本レポートでは、同調査における日本企業（約100名　）の回答に焦点を当て、日本固有の状況や背景を考察しながら、日本企業が新時代のサイバーセキュリティを実現するために何をすべきかを提言します。

Global DTI 2021調査から浮かび上がる日本企業とグローバルの違い

私たちは、Global DTI 2021調査で得られた回答を、日本企業とグローバル全体とで比較することを試みました。その結果、特に2つの大きな違いが浮かび上がってきました。

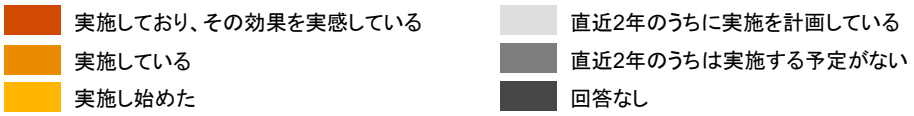
1. 日本企業はセキュリティ施策の効果の実感度合いが薄い

各セキュリティ施策の取り組みの状況を問う質問a～hに対し、「実施している」または「実施しており、その効果を実感している」と回答した日本企業の割合は、全てにおいてグローバルを下回りました。「直近2年のうちは各施策を実施する予定がない」と回答した企業の割合は日本とグローバルで大きな差はないことから、日本企業の多くはグローバルに比べて、各施策に取り組むタイミングまたは取り組みの成果を検証する段階で、セキュリティの重要性の理解や明確なゴール設定がなされていないことが読み取れます。

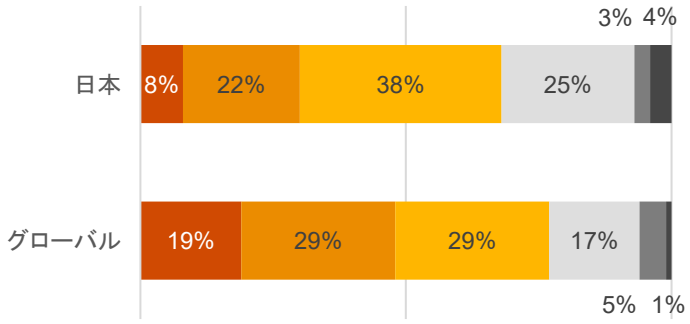
このような状況の背景には、日本企業の「横並び意識」の強さがあると私たちは考えています。日本企業においては、セキュリティ施策を検討する場合、ベストプラクティスや他社事例が重んじられるケースが多く見受けられます。あるいは、顧客やサプライチェーンからの要求や法規制などの外的圧力が高まることで、特定業界に所属する企業が足並みを揃えて対策に着手するという例も珍しくありません。もちろん、限られたリソースの中で不必要な投資・コストを避けるために十分に必要性を見極める慎重な姿勢は、否定されるものではありません。しかし、ビジネスの変革も脅威の増大も益々加速する中で、後手に回ることなくセキュリティ施策を展開するためには、各社が先を見据えて目的とゴールを設定し、主体的に施策を進めていくことが肝要です。

また、先述の質問に対し「実施しており、その効果を実感している」と回答した日本企業の割合を見ても、いずれの施策でもグローバルの4-6割程度の水準に留まっています。さまざまなセキュリティ施策を実施していたとしても、期待する効果を定義していないというケースは少なくありません。効果を実感するためには、セキュリティアセスメントの結果や法規制などの外的要因から生まれる動機付けのみならず、セキュリティを統括する部門がビジネスにどのように貢献するか、企業としてどのような効果を得たいのかといった、明確な目的・目標を定めることが必要です。

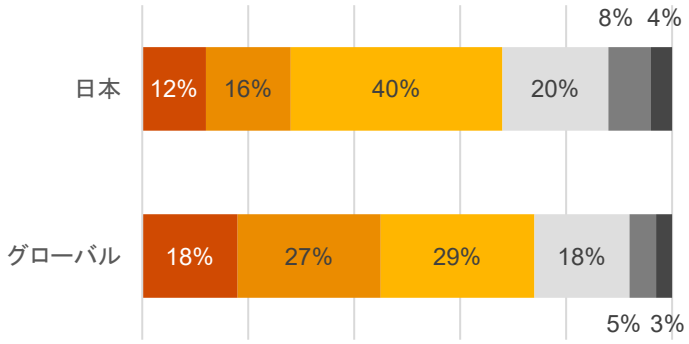
Q. 以下のセキュリティ施策を実施していますか。または実施する予定がありますか。



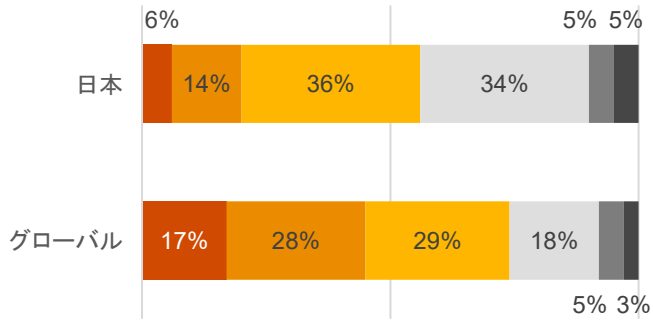
a. サイバーセキュリティに係るスキルセットの向上



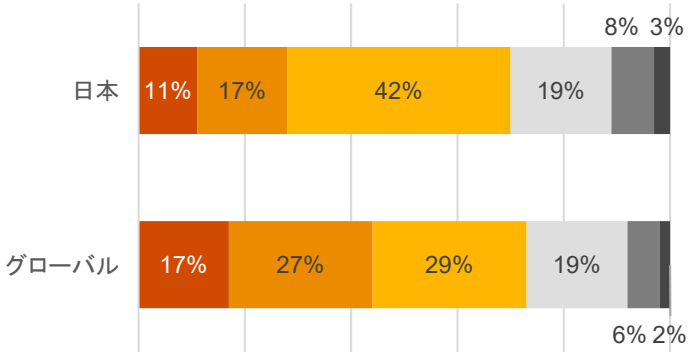
b. サイバーセキュリティ管理部門とビジネス部門との協力



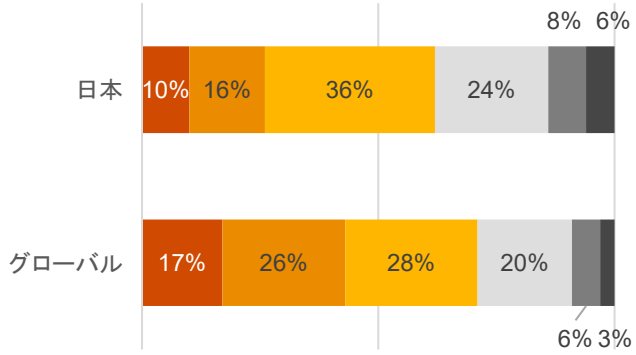
c. サイバーセキュリティリスクの定量化



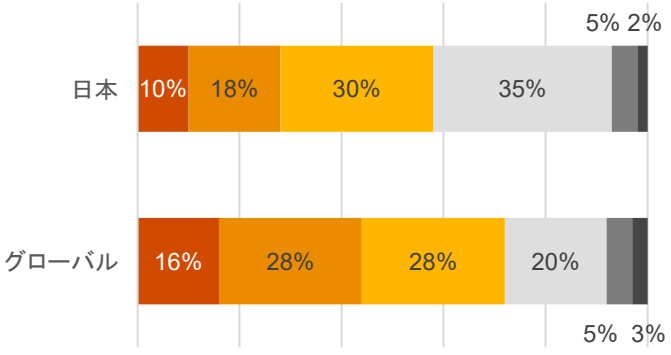
d. 全社的なサイバーセキュリティに係る報告



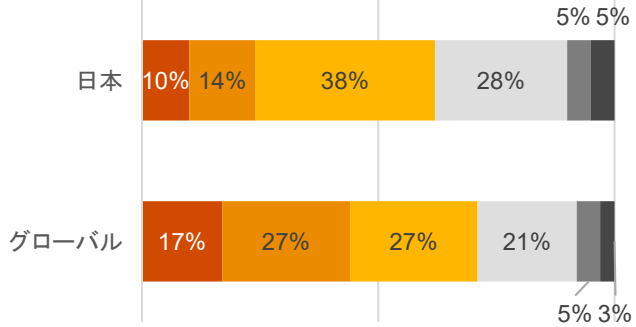
e. サイバーセキュリティに係る投資価値の明確化



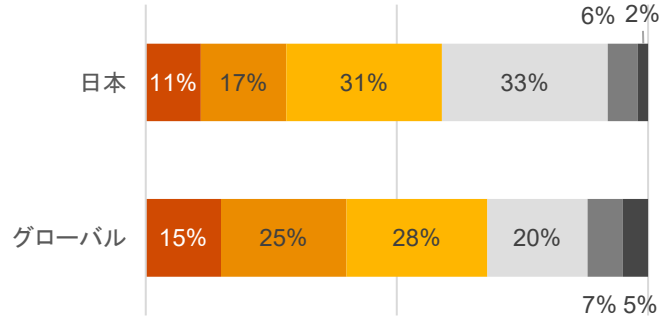
f. リアルタイムな資産・リスク管理



g. サイバーセキュリティ向上のための最新技術導入



h. サイバーセキュリティオペレーションの自動化や効率化



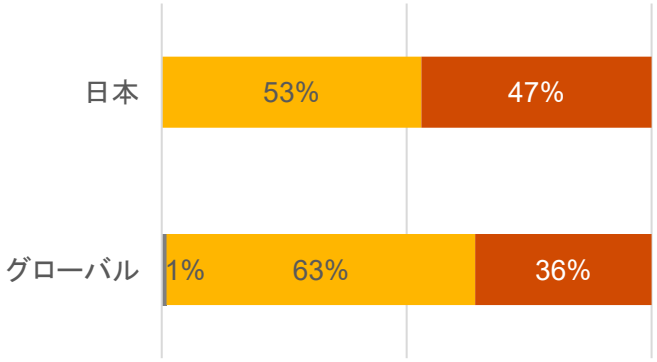
2. 日本企業はセキュリティ施策の効果の実感度合いが薄い

私たちは、ビジネス部門に所属する回答者　に対して行ったテクノロジー・セキュリティ領域に係る学習時間の質問iの回答の比較も試みました。その結果、「週に7時間以上」と回答した企業の割合は、日本がグローバルを20%以上下回りました。一方で、IT部門に所属する回答者の場合（j）、「週に7時間以上」と回答した企業の割合は、日本がグローバルを11%上回りました。このことから、日本企業においては、IT部門とビジネス部門の間にテクノロジーやセキュリティに対する当事者意識の差が存在することが推察されます。

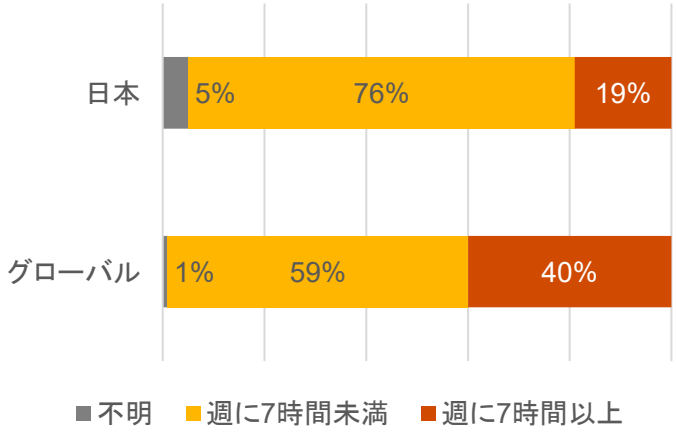
この背景には、日本企業の特徴として語られがちな「縦割り構造」があると私たちは考えています。社内インフラの構築や運用、新たなテクノロジーの導入はIT部門のミッション、戦略立案はビジネス部門のミッションといったように、役割を部門ごとに区切り、結果として全社的なテクノロジー導入やセキュリティへのリテラシー浸透に苦心する企業は少なくありません。デジタルトランスフォーメーション（DX）推進の必要性が声高に叫ばれる昨今、テクノロジーを駆使したビジネス変革はもはや避けられません。ビジネスとテクノロジーの親和性を高め、それに伴うセキュリティを担保することは、全社一丸となって取り組むべき重要な経営課題となりつつあります。「DX推進部」といった組織横断型の部門の設置をはじめ、ビジネスとテクノロジー・セキュリティを一体として捉えることが、環境変化に適応する上で重要なのではないでしょうか。

Q.業務を改善するテクノロジー分野に関する新たな知識を学ぶのに、個人的にどれくらいの時間を割いていますか。

i. ビジネス部門のテクノロジー・セキュリティ学習時間



j. IT部門のテクノロジー・セキュリティ学習時間



日本企業への提言

Global DTI 2021調査をとおして、日本企業にはグローバルと比較して、次のような違いがあることが見えてきました。

1. セキュリティ施策の効果の実感度合いが薄い

2. ビジネス部門のセキュリティリテラシーが劣る

その背景には、日本企業の特徴として語られがちな「横並び意識」の強さや、組織の「縦割り構造」があると考えられます。ここからは上記を踏まえ、新時代のサイバーセキュリティへと歩みを進めるために、日本企業が取り組むべきと考える施策を2つ提言します。

1. ビジネスゴールから逆算したセキュリティ戦略の検討

1つ目は、ビジネスの目標・ゴールから逆算したセキュリティ戦略を検討・立案することです。前述のとおり、アセスメント結果による是正対応、サプライチェーンからの要望や法規制対応など、半ば義務的な動機に基づくセキュリティ施策のみを検討・実施するのみの状態では、効果の検証や改善施策の検討にまで話が及ばず、結果的に成果を実感するに至らないケースが少なくありません。効果を実感できなければ、セキュリティ施策に対するモチベーションの低下やセキュリティ予算確保の難化などが引き起こされる可能性もあるでしょう。

まずは、セキュリティ施策の効果に対する定義付けが必要です。セキュリティがビジネス上の利益に結び付いているか、という視点だけでは、セキュリティは多くの経費をねん出することからネガティブなイメージを持たれがちです。日々安全に業務に従事できること自体が、セキュリティが担保されているがゆえの効果であることを、経営層からの発信や部門間協議などを通じて、まずは全社に認識してもらう必要があるでしょう。その上で、ビジネスの目標・ゴールから逆算するアプローチでセキュリティ戦略を考えることが重要です。全社にセキュリティの重要性を理解してもらった上で、さらにセキュリティ施策を通じてどのような効果を得たいのかを明確にするのです。

セキュリティがビジネスに貢献していることを経営層や現場を問わずあらゆる従業員が認識し、自社のあるべき姿を実現するために必要なセキュリティ施策を考え、効果を検証する――。こうしたサイクルを築くことが、セキュリティ対策の成果を最大化できる組織作りの第一歩になるのではないでしょうか。

2. ビジネス部門とIT部門のミッション・役割の再定義

2つ目は、ビジネス部門とIT部門のミッション・役割を再定義することです。経営のあらゆるフェーズにデジタルが入り込む現代においては、ビジネス部門とIT部門が一体となり、全社でビジネスを推進していくことが求められるでしょう。そのためには、ビジネス部門とIT部門のミッション・役割を再定義し、かつお互いの業務に積極的に関与していくべきとの意識を醸成していくことが重要です。特にIT部門は、社内インフラの構築や運用に留まることなく、新たなビジネスに係るシステム構築・運用およびそのセキュリティ強化など、従来はビジネス部門が主導していた分野にも積極的に関与していくべきです。

直近では、IT部門のビジネス部門への積極関与によるITガバナンスの強化が最も現実的な目標となるでしょう。相互理解の暁には、両部門が協働し、切磋琢磨する体制が構築され、新たなテクノロジーやインフラを導入するにあたって新たなスキルを身に付け合うようなことも期待されます。ただし、こうした状態を築くにはそれなりに時間がかかることが見込まれます。デジタル化のさらなる推進に向けて全社的なスキルアップを図るには、長期的な視点で取り組むことが肝要です。

総括

本レポートでは、Global DTI 2021調査の中でも日本企業の回答に焦点を当て、日本固有の状況やその背景の考察をとおして、日本企業が新時代のサイバーセキュリティを実現するために何をすべきかを提言しました。デジタル化の進展によりビジネス環境が大きく変化する昨今、セキュリティ戦略のアプローチはもちろん、組織の在り方も併せて変革していくことが必要となってくるでしょう。従来のやり方や、これまで培ってきたものを大きく作り変えることは簡単ではありません。経済的ならびに心理的なハードルの高さから、変革に後ろ向きになりがちなのは十分に理解できます。

確かに、現在のやり方を続けることで事業が突然機能しなくなるということは考えづらいでしょう。そのため、既存の方法やスタイルを継続して様子を見ようという心理は、理に適っているように感じられます。しかしながら、そうしている間にもビジネス環境は刻一刻と変化しています。企業の今をよりよい状態にするため、未来をさらに花開かせるため、この瞬間から変革を検討し、行動に移してみてはいかがでしょうか。本レポートが、日本企業の皆様にとって、新時代のサイバーセキュリティを実現するための一助となれば幸いです。

PwCコンサルティング合同会社のご紹介

PwCコンサルティング合同会社は、経営戦略の策定から実行まで総合的なコンサルティングサービスを提供しています。PwCグローバルネットワークと連携しながら、クライアントが直面する複雑で困難な経営課題の解決に取り組み、グローバル市場で競争力を高めることを支援します。

PwC Japanグループ

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCコンサルティング合同会社を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。

お問い合わせ

PwCコンサルティング合同会社

〒100-0004東京都千代田区大手町1-2-1 Otemachi One タワー
TEL：03-6257-0700（代表）
https://www.pwc.com/jp/ja/about-us/member/consulting.html

丸山　満彦
PwCコンサルティング合同会社
パートナー

綾部　泰二
PwCあらた有限責任監査法人
パートナー