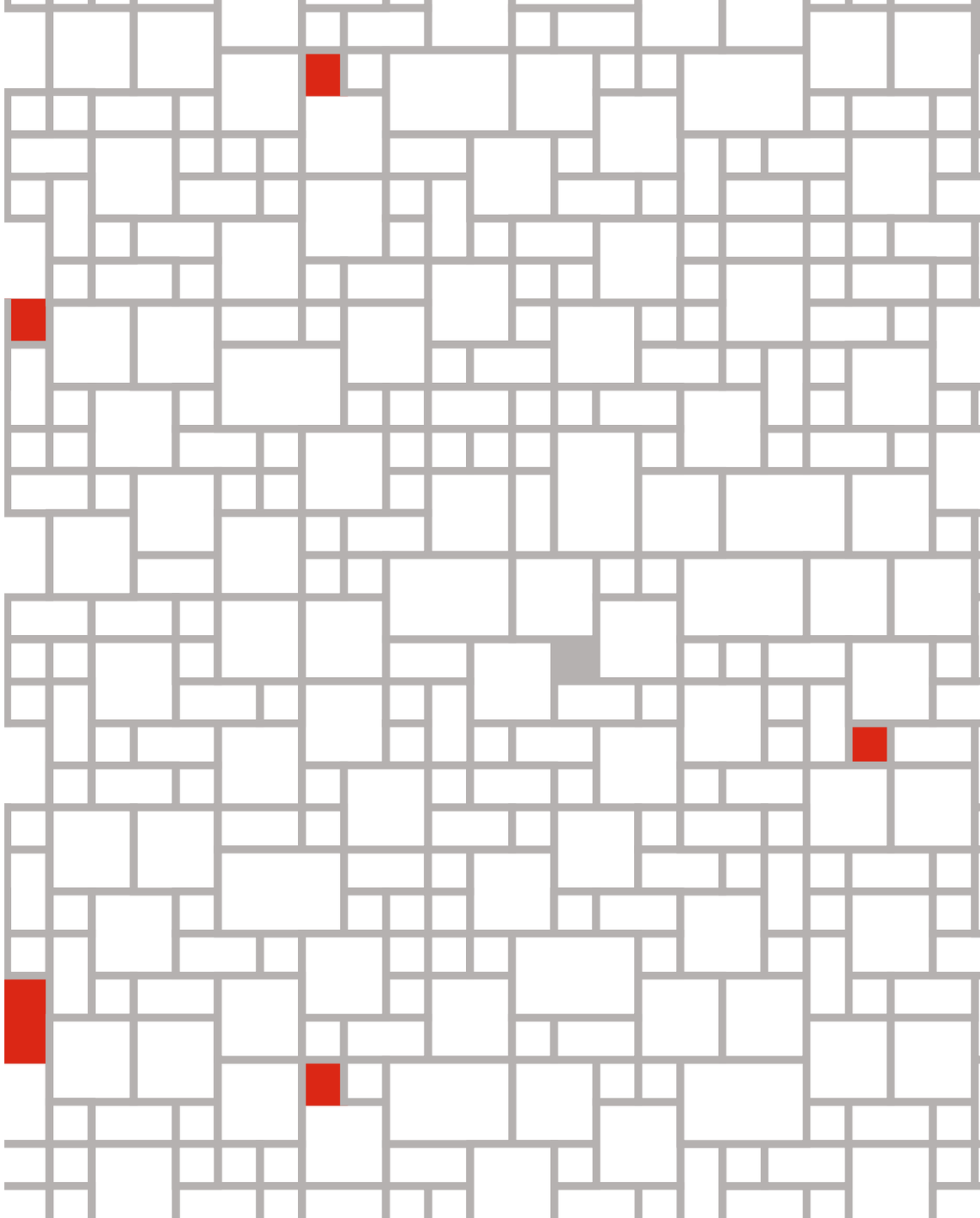
サイバーセキュリティの先進的企業は、新たな枠組みで事業の成長を推進

Digital Trust Insights

pwc

www.pwc.com/jp



日本企業の皆様へ

IoTや5Gといった技術革新によって、ビジネスにおけるデジタルトランスフォーメーションへの取り組みは、さまざまな産業分野で始まっています。デジタルトランスフォーメーションは、創造的な取り組みを通じて、自社における業務効率化から顧客や社会全体に対する新たな価値創造に至るまで、大きな効果が期待されています。その一方で、従来から存在するサイバーリスクに加えて、これまでにない新たなリスクも顕在化し始めています。

ビジネスにおけるデジタル環境とサイバーリスクが変化する中で、サイバーセキュリティ領域における人材不足、スキル不足に関する問題は、世界的にも、また日本国内においても一層深刻な問題となっています。一方で、デジタル施策においてもサイバーセキュリティにおいても、先進的な取り組みを通じて他社よりも優れた実績を残している企業も存在します。本レポートは、そのような先進的企業の特徴、その他の企業との違いについて解説しています。

本レポートが日本企業の皆様のお役に立てますと幸いです。

サイバーセキュリティ専門家に対する需要が急増

サイバーセキュリティ専門人材の需要が急速に高まっている。ある調査では、サイバーセキュリティ専門家の不足は2022年には世界中で180万人に達すると予測されている。しかし単純に人を増やすことだけが、これから新たに発生するさまざまなリスクに対して、企業が取り組むデジタル施策の推進を安定させるための解決策にはならない。

企業はデジタルトランスフォーメーションに投資して組織を近代化し、新しい能力を社内に構築することで業務をより速く、より高度に進めようとしている。企業はデジタルトランスフォーメーションに事業成長の加速とカスタマーエクスペリエンス（顧客の体験）の向上を期待している。デジタルに対応するためのさまざまな取り組みから生まれる最大のリスクは何だろうか。企業幹部の答えは、どの調査を見ても「サイバーセキュリティリスク」である。企業にとってサイバーセキュリティの専門家を増やすだけでは対策として不十分であり、専門家が何をどのように行うのかを再定義する必要がある。

求められているのはビジネスドリブン型、すなわち経営視点から発想したサイバーセキュリティだ。自社の戦略目標達成に貢献することこそ、サイバーセキュリティの責務を担う社内組織の使命だという方向に発想を変えることである。では、どの程度の企業が、このような発想の転換を始めているのか。発想を転換した企業は業績が向上しているのか。そのような企業において、サイバーセキュリティ専門家の業務は他の企業と比較して何が異なるのか。

PwCのDigital Trust Insights調査によって、先進的企業、すなわち回答者の上位25%は、デジタル施策およびセキュリティ全般で他より優れた実績を上げていることが明らかになった。多くの企業がこの先進的企業の事例から学ぶべきである。Digital Trust Insights調査は、世界中の企業幹部とITプロフェッショナル3,000人以上を対象に調査を行い、その結果をもとにロードマップを作成した。

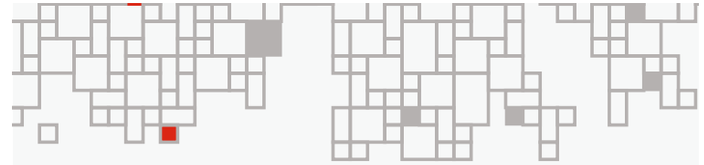
先進的企業の特徴は?

Digital Trust Insights調査において、先進的企業は期待値以上の成果を達成していると報告する傾向にある。「デジタルトランスフォーメーションに求める第一の価値は増収である」と答えた回答者のうち9割近くが、期待値どおりもしくは期待値を上回る成果を上げていると述べている（増収以外を挙げた回答者では、3分の2が同様の回答をしている）。

先進的企業は自社を評して、他社よりも先を見越していち早く行動し、問題への対応も迅速であり、サイバー脅威が業務に及ぼす影響を最小限に抑えていると述べている。先進的企業10社のうち8社以上が、デジタル関連施策における新たなサイバーリスクを予測し、取引先や顧客に影響が及ぶ前にそのリスクに対処したと回答している（先進的企業以外の場合は、10社のうち6社）。

先進的企業のサイバーセキュリティ部門は、他社に比べてはるかに高い割合で、大きな付加価値を生み出しているという評価を得ている。先進的企業の86%が、サイバーセキュリティ部門は自社の価値を大幅に高めていると考え（先進的企業以外では50%）、58%が自社のサイバーセキュリティ部門はデジタルトランスフォーメーションから発生する重大なリスクを極めて効果的に管理していると考えている（同21%）。

また重要なことだが、先進的企業は、売上高と利益率の見通しについても非常にポジティブである。今後3年間に売上高が平均5%以上増加すると予測している企業は57%（先進的企業以外では31%）、利益率が5%以上上昇すると予測している企業は53%（同28%）だった。



57%

の先進的企業が、今後3年間に売上が平均5%以上増加すると予測

先進的企業以外の場合には 31%

出典：PwC「Digital Trust Insights survey, May 2019」
集計ベース：全回答者数3,145名

先進的企業とその他の企業の違いは何か?

先進的企業では、サイバーセキュリティ部門を事業に組み込むことで戦略目標を支援している傾向が強い。サイバーセキュリティ部門が資産の保護だけを使命とする部門ではなく、戦略パートナーとして組織を支えることを使命とする部門として再構築されているのである。

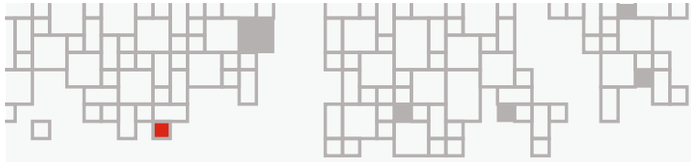
また、さまざまな役職者とサイバーセキュリティ部門のつながりも強い。戦略策定を行う最高経営責任者（CEO）やデジタル施策を実施する幹部［最高デジタル責任者（CDO）、最高イノベーション責任者（CIO）、最高マーケティング責任者（CMO）、最高技術責任者（CTO）］、そしてリスクを管理する最高リスク責任者や事業活動を監視する取締役会とも密接に連携している。

先進的企業は次の3分野において、サイバーセキュリティと事業との関係が際立って強い。

戦略におけるつながり　先進的企業のサイバーセキュリティ部門は、事業戦略をよく理解している。例えば製品開発の場面では、サイバーセキュリティの専門家が積極的にかかわり、設計上の安全性を高める支援をしている。65%の先進的企業が自社のサイバーセキュリティ部門について、事業の中に組み込まれ、会社の事業戦略を熟知し、事業における必達事項を支えるサイバーセキュリティ戦略を備えているかという問いに「非常にそう思う」と答えた。先進的企業以外で同様の回答をしたのは15%だった。

リスクベースアプローチにおけるつながり　先進的企業の大半が、デジタルトランスフォーメーションのリスク管理にサイバーセキュリティ部門が常に関与していると答えている。自社で業務改革やデジタル施策を実施する際、それに伴うリスクの管理にサイバーセキュリティ部門が常に関与していると答えた先進的企業は89%だった（先進的企業以外では41%）。

統一性のある事業運営　先進的企業では、自社のリスク選好度に関する話し合いに、サイバーセキュリティ部門が常に参加している。それによってリスク軽減策や脅威への対抗策が会社全体で協調的に実施できている。サイバーセキュリティ部門が経営幹部と十分に意思疎通を行い、中核事業における自社のリスク選好度を把握できているかという質問に対し、先進的企業の77%が「非常にそう思う」と答えている（それ以外では22%）。



65%

の先進的企業が、自社のサイバーセキュリティ部門が事業の中に組み込まれているかという問いに「非常にそう思う」と回答

先進的企業以外では15%

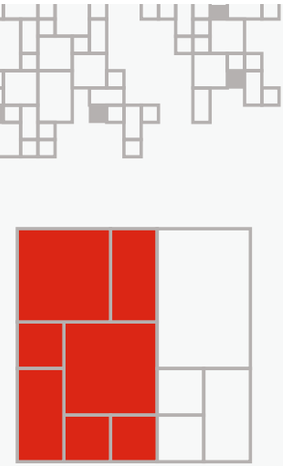
出典：PwC「Digital Trust Insights survey, May 2019」
集計ベース：全回答者数3,145名

先進的企業に該当する企業とは?

事業戦略とサイバーセキュリティ戦略の一貫性、リスクベースアプローチ、リスク管理と監視を行う社内組織の調整に優れている先進的企業は、どの業種、どの地域に多いのだろうか？

調査対象の中でも売上高10億米ドル以上の企業の約40%が先進的企業に該当した。金融サービスの3分の1、テクノロジー・メディア・テレコムの30%がその中に含まれている。その他、製造業、小売・消費財、ヘルスケア、医薬・ライフサイエンス、エネルギー・資源・鉱業などでは、調査対象の約4分の１が先進的企業だった。地域別ではEMEA（欧州・中東・アフリカ）が少なく、先進的企業と評価されたのはわずか21%だった。

金融サービス、テクノロジー・メディア・テレコム業界の企業の場合、先進的企業である確率が他業界に比べて高い



出典：PwC「Digital Trust Insights survey, May 2019」
集計ベース：全回答者数3,145名

先進的企業に近づくための方法は?

先進的企業の仲間入りを目指すならば、先進的企業の特徴である下記の3つのポイントについて改善していくことが不可欠である。また、PwCのDigital Trust Insightsではロードマップも提供しているので、サイバーセキュリティのギャップへの対応に際して、注目していただきたい。このロードマップは、米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワークのさまざまなカテゴリーに基づき、各社のITプロフェッショナルに自社の状況を評価していただき、その結果をもとに作成したものである。カテゴリーは、フレームワークの5つの機能（識別、防御、検知、対応、復旧）の下位項目である。評価では、CMMI（能力成熟度モデル統合）の成熟度レベルを使い、各社の状況をレベル分けしてもらった。

1. **識別**は、防御が必要な資産やプロセスを正確に特定することである。全てのITプロフェッショナルの間で、この機能は最も成熟度が低いという評価だった。その一方で、先進的企業は、先見性をより高める余地があるものの、この機能において明確な強みを持っていた。自社内の物理資産やソフトウェア資産を管理できるように識別する活動について、成熟度が非常に高いとした回答者は比較的少数だった。企業は、事業上の優先課題の情報をサイバーリスク管理にいかに生かすべきかを、もっと理解する必要がある。

2. **復旧**は、全てのITプロフェッショナルが最も成熟度が高いと評価した機能であり、先進的企業が最も優位性を持つ機能でもある。この機能については、教訓やコミュニケーションを復旧計画に活用することが、先進的企業とのギャップを縮めるのに有効ではないかと考えられる。

3. データセキュリティ（**防御**）、検知プロセス（**検知**）、対応計画（**対応**）、改善（**対応**）なども先進的企業の強さが際立っている。

ビジネス全体においてサイバーセキュリティを組み込んでいる企業は、デジタルトランスフォーメーションのメリットを実現しやすいと言える。また関連リスクの管理やデジタルトラストの構築においても有利である。そうした企業および現在の先進的企業は、徐々に競争優位を形成する中でやがて市場の注目を集めることになるだろう。

お問い合わせ先

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
pwjppr@pwc.com

外村 慶
パートナー
kei.tonomura@pwc.com

林 和洋
パートナー
kazuhiro.hayashi@pwc.com

Brendan Dougher
Principal, PwC US
brendan.p.dougher@pwc.com

Joseph Nocera
Principal, Cybersecurity and Privacy, PwC US
joseph.nocera@pwc.com

Joseph Greene
Principal, PwC US
joe.greene@pwc.com

Grant Waterfall
EMEA Cybersecurity and Privacy Leader, PwC United Kingdom
grant.r.waterfall@pwc.com

Paul O’ Rourke
Asia Pacific Cybersecurity and Privacy Leader, PwC US
paul.orourke@pwc.com

T.R. Kane
Principal, PwC US
t.kane@pwc.com

www.pwc.com/jp

日本語版発刊年月：2019 年 8 月　　管理番号：I201906-6