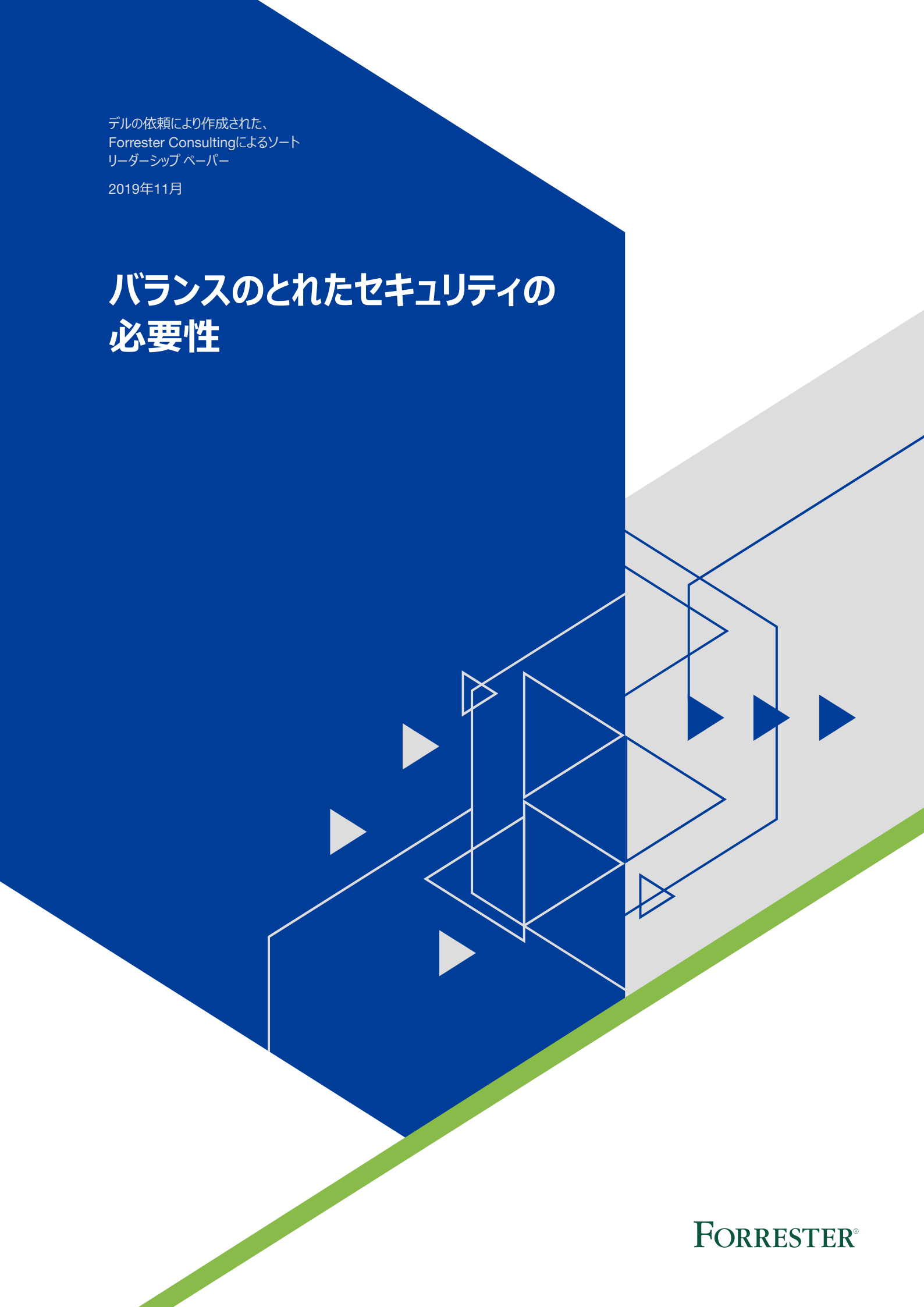
デルの依頼により作成された、
Forrester Consultingによるソート
リーダーシップ ペーパー

2019年11月

バランスのとれたセキュリティの必要性



FORRESTER®

目次

プロジェクト ディレクター：
Tarun Avasthy、
マーケット インパクト コンサルタント

調査協力：
Forresterインフラストラクチャ&
オペレーションズ リサーチ グループ

FORRESTER CONSULTINGについて

Forrester Consultingは、ビジネス リーダーが組織で成功するのをサポートするために、独立した客観的な調査に基づくコンサルティング サービスを提供しています。簡単な戦略セッションからカスタム プロジェクトまでの広範にわたるForresterのコンサルティング サービスでは、専門家ならではの洞察力を生かしてお客様固有のビジネス課題に取り組むリサーチ アナリストに直接ご相談いただけます。詳細については、forrester.com/consultingをご覧ください。

FORRESTER®

概要

バランスのとれたセキュリティを実現するために、企業は、コンプライアンス要件としてのプライバシーとデータ セキュリティに対処するのではなく、プライバシー保護を推進し、その優れたテクノロジーを活用してブランドを差別化していく必要があります。ITインフラストラクチャにおける失敗や変更によってさらに複雑になる可能性があるため、バランスのとれたセキュリティ戦略を構築することが非常に重要です。バランスのとれたセキュリティ戦略では、テクノロジーの変化の速さと、業界の混乱や法令遵守の進化に遅れないようにすることで複雑さが排除されます。

2019年3月、デルは、従業員を保護し、その可能性を引き出すために必要な新たなセキュリティの動向とテクノロジーの評価をForrester Consultingに依頼しました。デルの調査により、セキュリティ プロトコルに従いながら従業員の自由度を高めることで、従業員の生産性が向上することが分かりました。Forresterは、887人の経営幹部とIT導入決定者を対象にオンライン調査を実施し、このトピックを調査しました。

主な調査結果

- **絶えず進化を続けている脅威により、中堅企業は事後対応ではなく、プロアクティブな対応を迫られている。**注目度の高い多くのセキュリティ侵害やサイバー攻撃がニュースで定期的に報告されている中で、中堅企業はより先進的な考えでセキュリティに取り組む必要があります。
- **セキュリティのみに力を入れるのは、特効薬とは言えない。**中堅企業は、イネーブルメントの文化、従業員の継続的なスキル開発、そして最も重要と思われる、健全で堅牢なセキュリティ インフラストラクチャを宣言する必要があります。
- **堅苦しいITポリシーでは、従業員が業務を遂行するために、ITセキュリティのベスト プラクティスを回避することになる。**ルールを曲げることは職場では珍しくありませんが、業務を遂行するためにITポリシーを完全に回避するのはリスクになります。

FORRESTER®

EXおよび運用効率を向上させるために組織に必要なバランスのとれたセキュリティ

多様なテクノロジー ランドスケープと変化する従業員のワークスタイルによって、組織の全体的なセキュリティ態勢と組織の評判を脅かすさまざまなリスクへの扉が開かれました。堅牢でバランスのとれたセキュリティ インフラストラクチャにより、ビジネス パフォーマンスを最大限に高め、保護することができます。一方、摩擦を減らし、従業員が最も重要な作業を効率的に行えるように、従業員体験戦略の開発に関心を持つ企業が増えている状況を受けて、ビジネス イニシアティブとしての従業員体験（EX）が重要視されるようになってきています。

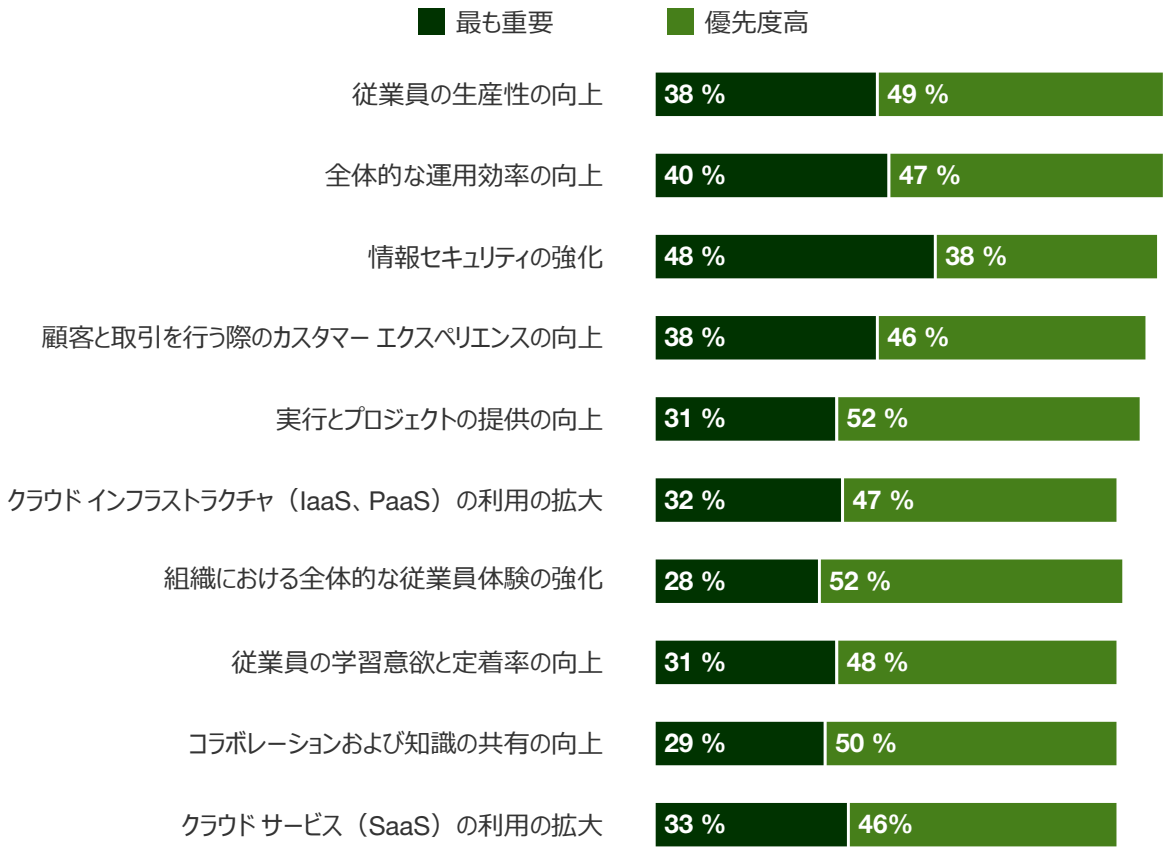
テクノロジーだけにコストをかけても、従業員体験を向上させることはできません。組織、特に中堅企業は、リスクを管理すると同時にビジネス パフォーマンスもサポートするには、従業員イネーブルメントの文化の構築、継続的なスキル開発、堅牢なセキュリティに投資する必要もあります。優れたEXを実現するために、企業は次の3つの主要分野においてバランスのとれたセキュリティへの取り組みが求められます（図1を参照）。

- **従業員の生産性の向上。**現在のあわただしい職場では、従業員は認識力を強く求められます。そのため、従業員が各自の業務を管理できるようにサポートすることが、優れたEXの本来の特性です。しかし、多くのセキュリティ対策ではその逆の取り組みが行われ、生産性のレベルを低下させています。このため、中堅企業は今後12か月間に従業員の生産性を向上させたいと考えています（88%）。テクノロジーが進化を続ける中で、回答者は、従業員の定着率と学習意欲の向上を図ることで（79%）、人材のギャップを可能な限り埋めていくと回答しています。
- **情報セキュリティの強化。**従業員が作業をスムーズに進めるには、作業している場所や、作業に使用するデバイスに関係なく、作業を行うために必要な情報に自由にアクセスできることも必要です。しかし、企業は、ビジネスの運用を妨げ、顧客や従業員の個人情報または企業の機密情報といった機密データを侵害する可能性のある、さまざまなタイプのサイバー攻撃や出来事にさらされています。さらに、サード パーティのリスクやサプライ チェーンのセキュリティなどの問題について、組織はビジネスに対するリスクの考え方を自社の環境を越えて拡大する必要があります。86%の企業が、情報セキュリティを優先していくと回答していることは驚きではありません。
- **運用効率の向上。**ビジネスの運用を支えるセキュリティ チームは、チームの運営方法についてより一貫したプロセスを確立し、セキュリティへのアプローチにおいて事後対策型の対応ではなく、プロアクティブな対応をとることが必要です。中堅企業は、標準のチェックボックス アプローチを越えて、主にコンプライアンス要件に基づいたセキュリティへの取り組みを行い、より戦略的でリスクに基づいたセキュリティ アプローチに転換しなければなりません。これを実現するには、リスク インテリジェンス、脅威の特定と対応、リスク アセスメント、およびプロジェクトの実行と提供（83%）という約束を守るためのビジネスの耐久性をサポートするプロセスが必要です。

中堅企業は、従業員のイネーブルメント文化の構築、継続的なスキル開発、強固なセキュリティ インフラストラクチャへの取り組みに投資する必要があります。

図1

「今後12か月間であなたの所属部門で最優先事項となるテクノロジー関連のイニシアティブは次のうちどれですか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年9月に実施した調査

進化する脅威とITの複雑さが継続的な課題

競合する優先事項、新たなテクノロジー、新しい規制条件に直面しているセキュリティ管理者は、継続的な防御と、攻撃者の成功を防ぐという任務を担っています。しかし、調査の回答者に対してセキュリティの最重要課題は何かを尋ねたところ、次のことが分かりました（図2を参照）。

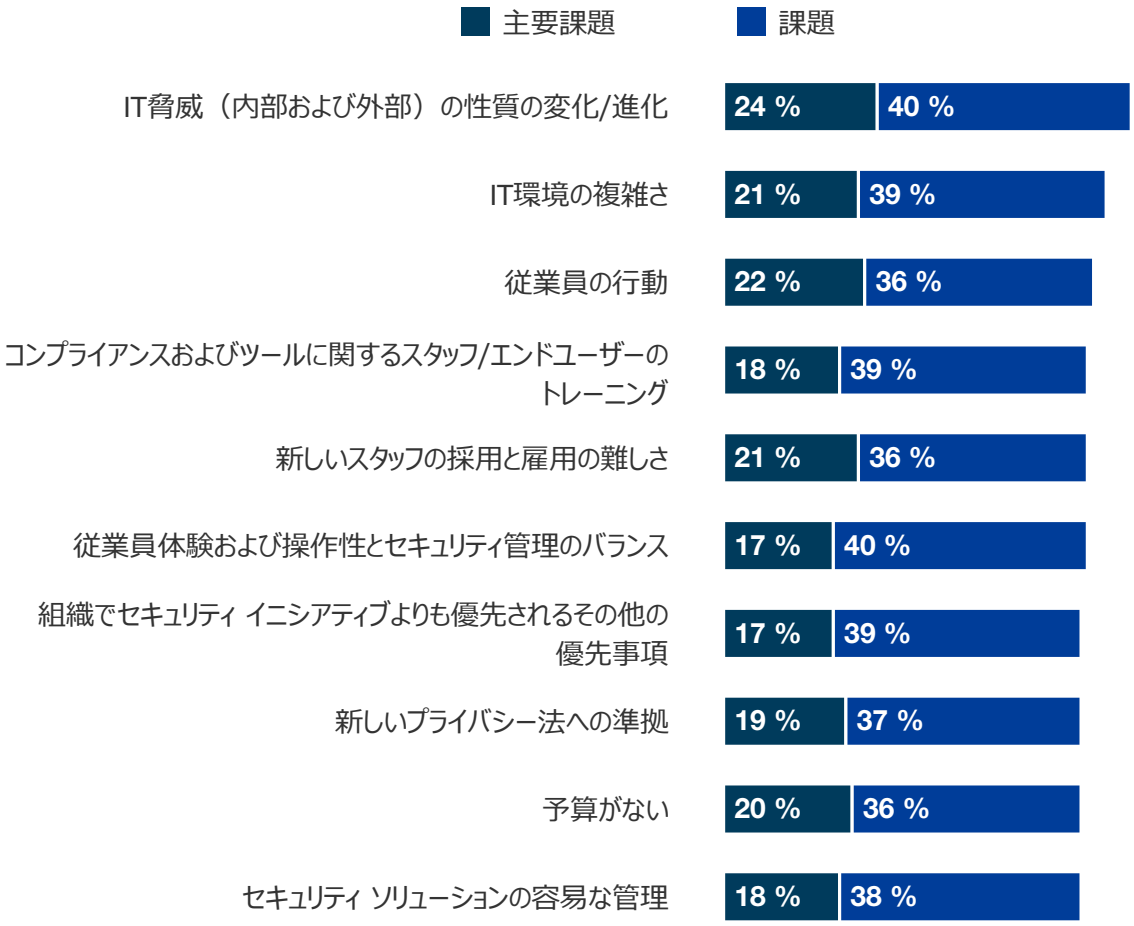
› **脅威の性質の進化により、中堅企業は常に警戒態勢で躍起になっている。** 攻撃者に対抗するために、IT部門には堅牢で適応性に優れた戦略が必要です。現在、65%の組織が、セキュリティ攻撃の性質の変化による問題に直面しています。組織のリーダーが、ニュースで最新のサイバー攻撃や出来事を知り、社内でそのような攻撃が発生する可能性があるかどうか尋ねてきた場合、発生する理由と方法（または環境と管理に基づいて、発生しない理由）を評価し、伝えると役に立ちます。ただし、このような事後対応型のアプローチで全体的なセキュリティ戦略を推進しないでください。

FORRESTER®

› **ITの複雑さは、リスクとIT管理の課題の増加につながる。**ITインフラストラクチャにおける失敗や変更によってさらに複雑になる可能性があるため、堅牢なセキュリティ戦略を構築することが非常に重要です。テクノロジーの変化、業界の分裂、進化する法令遵守に遅れずに対応できるセキュリティ戦略は、好ましい変化のきっかけとなります。セキュリティを最初から構築できる戦略の方が、事後に追加する戦略よりも推奨されます。環境内の多くのセキュリティ製品の統合について精査して、容易なIT管理をサポートできるためです。現在、調査回答者の60%が、IT環境の複雑さを組織に対する脅威と考えています。

図2

「貴社のITセキュリティの課題は次のうちどれですか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年9月に実施した調査

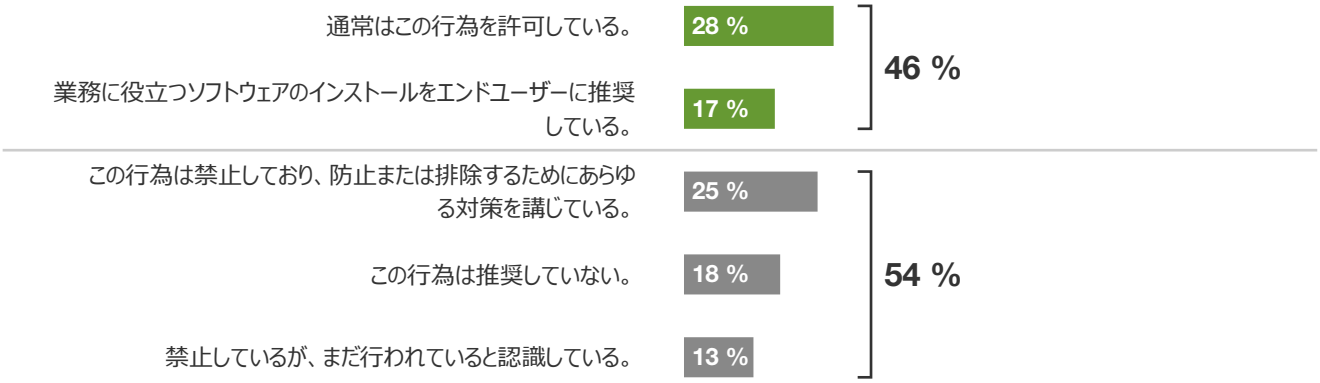
従業員は権限が与えられていると感じないと、ITポリシーを回避する

従業員は、作業を遂行するために最も容易な方法を選びます。従業員が作業を遂行するために自分のソフトウェアやアプリケーションをインストールしたいと考えている場合、中堅企業の回答者の54%が、従業員のそのような行為を防止、阻止、禁止していると回答していますが、それでもそのような行為は続くと考えています。従業員はビジネスによって支えらていると感じる必要があります（図3を参照）。

従業員は、生産性の妨げとならないような方法で作業を行い、セキュリティ担当者はビジネスが確実に保護されるようにする必要があります。回答者の58%が、従業員が作業を遂行するためにITポリシーを回避することがあり、それによってビジネスがリスクにさらされると回答しています。このため、EXおよび操作性とセキュリティ管理のバランスをとることが重要ですが、57%の回答者はこの点はいまだに課題であると述べています。さらに、組織がセキュリティ プログラムの有効性を測定できない場合（52%）、ゴール（バランスのとれたセキュリティ戦略という黄金のアーチ道）が常に次の丘を越えたところにある、終わりのないレースを走り続けることになります。

図3

「貴社の一般的な情報関連の社員に対して、社員が所有するソフトウェアの使用またはインストールに関する貴社のIT組織としてのポリシーはどのようなものですか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年9月に実施した調査

時代に合わせた進化が必要なセキュリティ インフラストラクチャ

企業の境界という考えは今では古くなり、時代遅れになってきています。従業員はさまざまな場所で作業を行うため、どこからでも情報にアクセスできることが必要です。消費者市場は、企業環境における従業員の働き方や使用するデバイスに影響を与えています。デジタル ビジネスには境界がありません。現在、組織はクラウドに手を広げ、モバイル ワーカーをサポートし、センサーやその他のインターネット接続デバイスを接続して物理環境をデジタル化することができます。従業員が機密データを漏洩する場合も、攻撃者が環境とデータを侵害する場合も、その方法は増えてきています。現在の職場および脅威環境では、セキュリティ戦略とアーキテクチャはデータ中心型の、セキュリティに対するゼロ トラスト アプローチに根ざしたものになるように進化する必要があります。

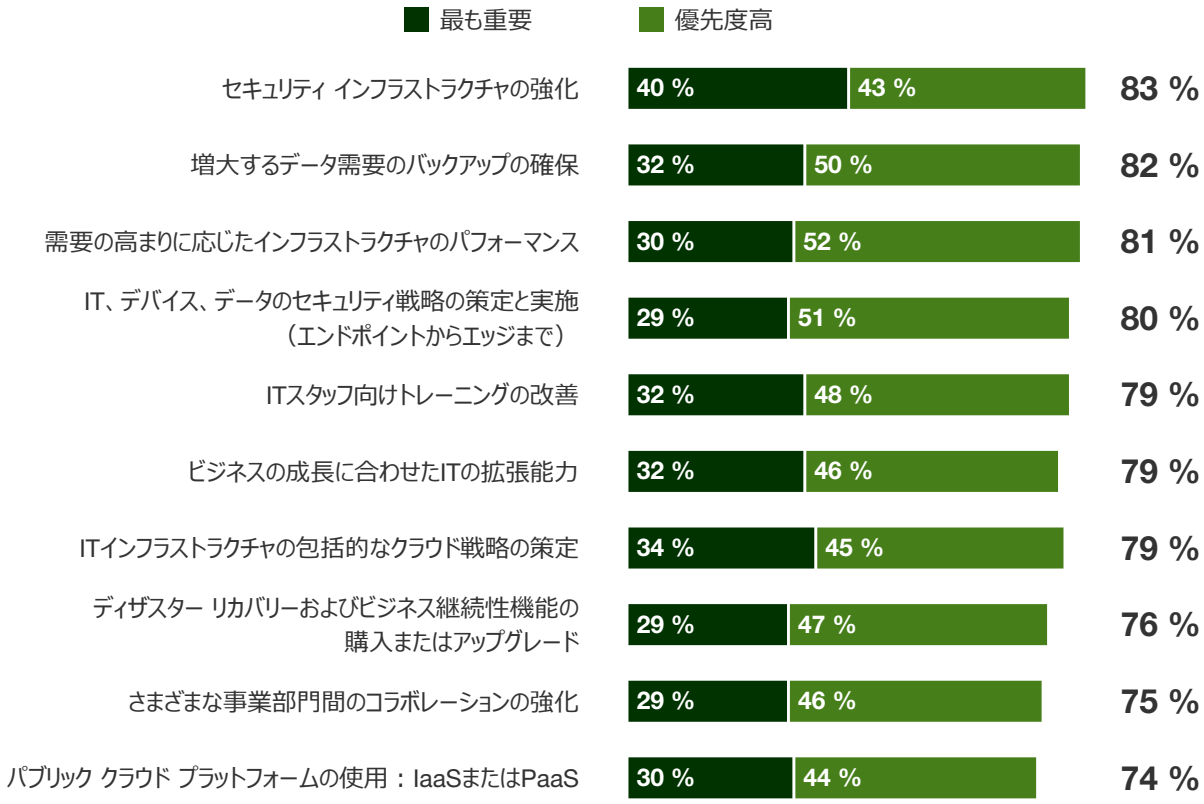
ゼロ トラストとは、セキュリティ チームがネットワークを安全なマイクロ境界に再設計し、難読化によってデータ セキュリティを強化したり、過剰なユーザー権限に伴うリスクを抑えたり、分析と自動化を使用してセキュリティの検出と対応を大幅に改善する方法を示す概念およびアーキテクチャ モデルです。このアプローチにより、データ セキュリティを大幅に向上させることができます。現在、多くの組織がすでにゼロ トラスト アプローチを採用しています。調査の回答者は次のようなインフラストラクチャを優先事項として挙げており、ゼロ トラストへの準備が整っていることを示しています（図4参照）。

- **エンドユーザーにトレーニングを実施して、安全なデータ処理方法を改善する。**攻撃者は、知的財産にアクセスするために、従業員と契約業者を標的にします。職場では、従業員は、企業所有のシステム/ネットワーク上のクラウドサービスを利用する接続されているデバイスを使用していますが、外出先、自宅、空港や喫茶店などの公共の場所からも、従業員は、企業が所有するデバイスほど十分に保護されていない個人所有のデバイスから機密情報やデータにアクセスする必要があります。従業員が安全な実践方法などによりデータを責任を持って処理する必要性は、必ずしも理解されず、効果的なコミュニケーションとは言えません。
- **リスクを軽減するためには、ITスタッフを対象にトレーニングを実施する。**ITスタッフのスキルの継続的な開発は、テクノロジーおよびセキュリティ インフラストラクチャを担当する個人が現在のベスト プラクティスを常に把握するために重要です。ITチームを成功に導くためには、変化するテクノロジー オプションと進化するリスクおよび脅威のランドスケープを理解することが必要です。そのため、79%の回答者が、ITスタッフのトレーニングを改善すると回答しています。これには2つの良い面があります。1つはITスタッフが最新のスキルとアプローチを身につけることができること、もう1つは人材の需要が高い時期に人材維持の取り組みをサポートできることです。

› **セキュリティ戦略を見直す。**組織は、コンプライアンス要件を満たすことと、強固なセキュリティを構築することが同じではないという認識を高めつつあります。サード パーティのビジネス パートナーは、連携の条件として、強固なセキュリティとリスク管理対策の証拠を求めてきます。将来を見据えた戦略は、強固なセキュリティ プログラムを構築するのに加え、ビジネスの優先事項に基づいて、懸案事項に対処するためのスキルの改善や新たなスキルの導入が必要な分野を予測する組織の取り組みをサポートします。回答者の80%が、IT、デバイス、データのセキュリティ戦略を策定し、実施する必要性を優先事項としていました。

図4

「貴社のITインフラストラクチャで今後12か月間に最優先事項となることが見込まれるイニシアティブは次のうちどれですか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年9月に実施した調査

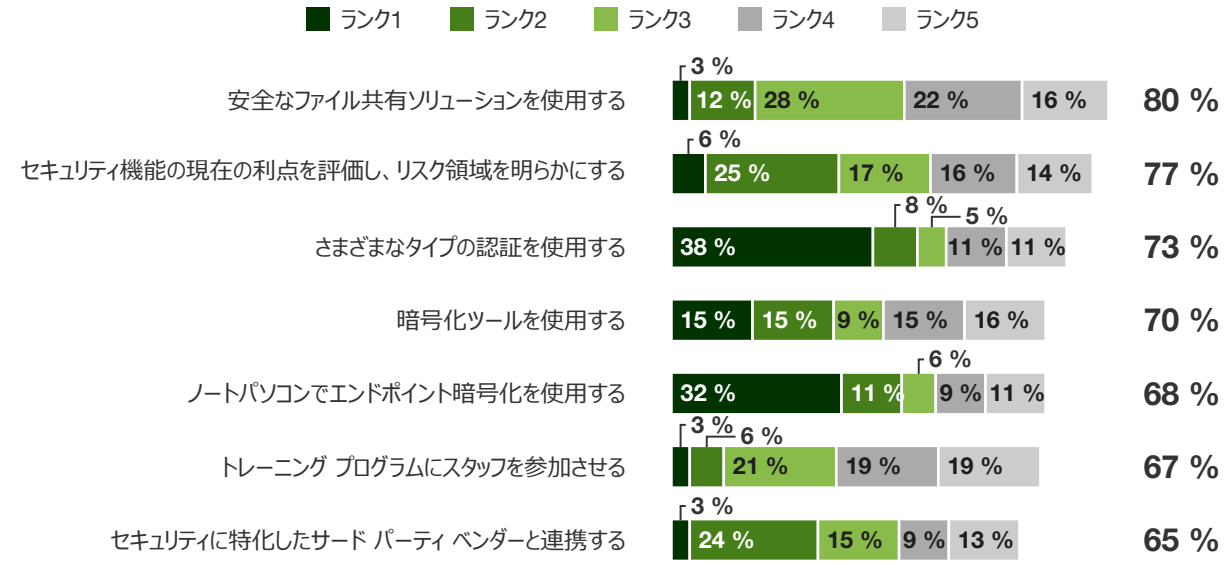
セキュリティを強化する方法

デジタル時代においてサイバー脅威はあらゆる場所にあります。そのため、侵害が毎日のようにトップニュースになり、企業の評判、資本、将来の成長と拡大を奪っています。つまり、組織の収益のセキュリティは、デジタル ビジネスの基本通貨とも言えるデータの保護のためのテクノロジーに左右されます。データ侵害は、避けがたい事実です。グローバル ネットワーク セキュリティの導入決定者の50%は、企業が過去1年間に少なくとも1回は侵害を受けたことを認識しており、この値は大企業になると55%に上昇します。この点を踏まえて、組織が改善したいと考えているセキュリティの要素が明らかになりました（図5を参照）。

- **ファイル共有を保護して従業員のコラボレーションをサポートする。**テクノロジーと従業員はどちらも、組織のコラボレーションを可能にして長期的な経済価値を創出する上で重要な役割を担います。80%の回答者が、セキュリティ機能を強化するために安全なファイル共有ソリューションを使用すると回答しています。ただし、ファイル共有ではオフィス内だけでなく、在宅型社員や、出張先の社員も必要に応じてファイルにアクセスし、共有できるようにする必要があります。
- **従業員がデータに安全にアクセスするための認証。**最もシンプルなフォームの認証ソリューションは、攻撃者を追い出し、承認されたユーザーを許可します。世界中で多くのデータ侵害が発生しているため、制御を適用する重要性は最重要課題となってきています。回答者の73%が、さまざまなタイプの認証を使用すると回答しています。また、回答者の38%が、セキュリティを向上させるための一番の戦略的取り組みとして認証を挙げています。ただし、これらのプロセスによって従業員の生産性が妨げられたり、仕事に支障をきたさないようにする必要があります。ユーザーの認証体験の円滑さが大きな差を生みます。
- **データを管理し、コンプライアンス要件を満たすための暗号化。**73%の回答者が暗号化ツールを使用すると回答していましたが、68%は特に従業員のノートパソコンのエンドポイント暗号化（フルディスク暗号化）が、セキュリティの向上にとって重要だと考えています。従業員がデバイスを紛失したり、盗難に遭う確率が高い環境では、この方法が最適です。静止データの暗号化にも、さまざまな種類があり（フルディスク、ファイル レベル、アプリ/フィールド レベル、透過的/データベース暗号化など）、組織はニーズに応じて選択できます。
- **現在のセキュリティ成熟度を把握するためのセキュリティ評価。**ほとんどのセキュリティ チームは、ビジネスの安全性を維持するためにさまざまな管理および標準を実装していますが、多くの場合、セキュリティ ギャップがある場所を客観的に特定することはできません。また、すべての主要な問題が解決しているかどうか、ベスト プラクティスの中で取り組んでいない箇所があるかどうかを判断するのに苦心しています。回答者の77%はこの点を認識しており、すべての要素が目的の役割を確実に果たせるように、詳細な改善計画を策定することで、セキュリティを向上させたいと考えています。

図5

「セキュリティを強化するためにどの方法を実行したいですか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年9月に実施した調査

バランスのとれたセキュリティが従業員とビジネスにもたらすメリット

セキュリティの取り組みは、ビジネスの安全性を高めるためのものです。収益増加の追求における障害を生み出して、ビジネスの成長を不鮮明にするためのものではありません。ビジネスの障壁をなくすために、導入決定者は、人間中心型のリスクベース アプローチでセキュリティ体験を設計する必要があります。優れた従業員体験と強力なセキュリティのバランスをとると、次のことを実現する上で役に立ちます（図6を参照）。

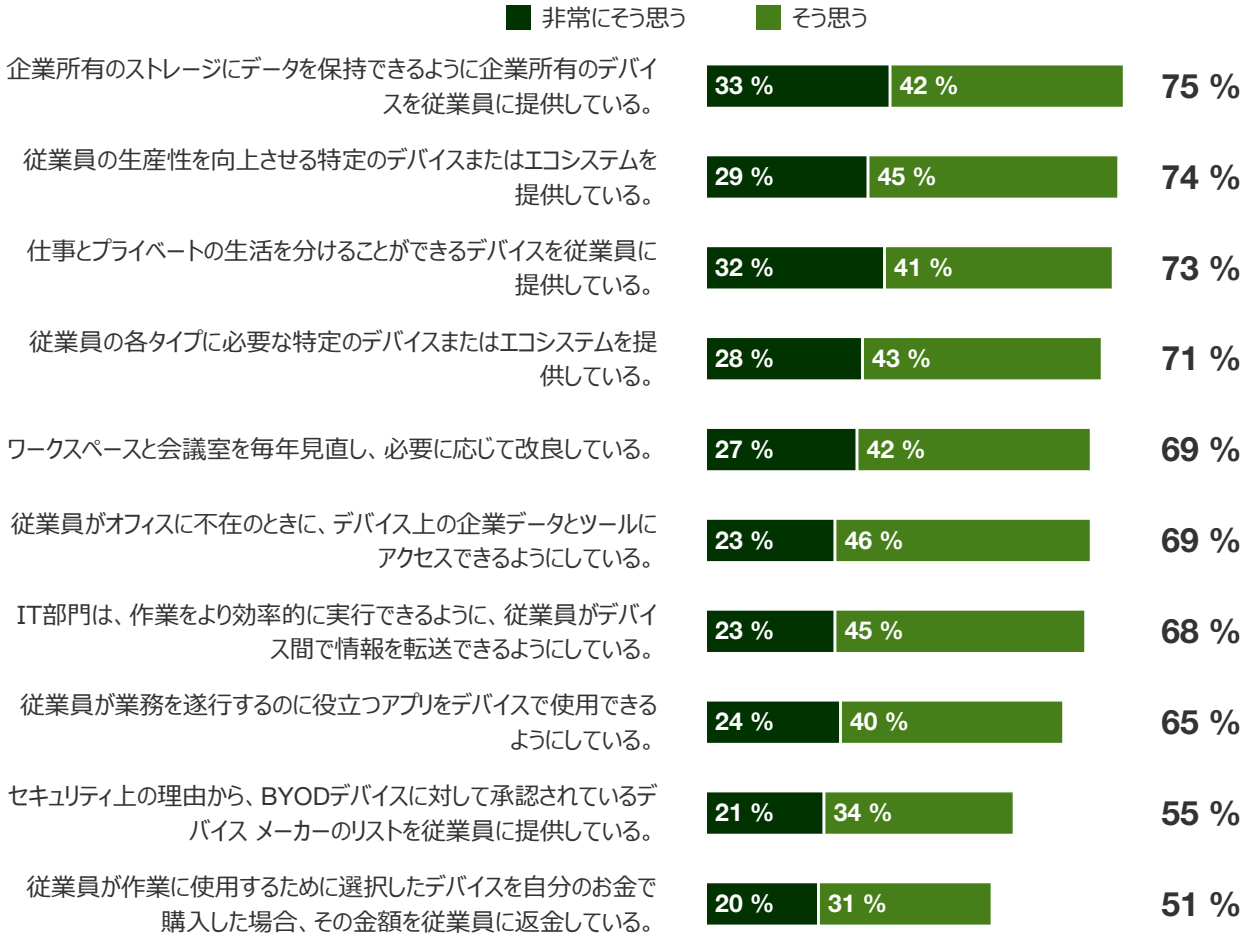
- **リモート ワークにより生産性と競争力を高める。**リモート ワークのサポートは、人材の雇用と維持における競争上の優位性です。これには、従業員がワークライフ バランスのサポートの改善を求めているかどうかや、通勤のために近場に居住しているかどうかに関係なく、仕事に最適な人材を組織が雇用しているかどうかなどが含まれます。テクノロジーによりリモート ワークが可能になり、セキュリティは企業がリモート ワークを安全に行うための重要な基盤です。回答者の69%が、従業員が社外で仕事をする際にデバイス上の企業データにアクセスできるようにしていると回答しました。
- **コラボレーションによりイノベーションを促進する。**従業員は体験の共有を望んでおり、最終的には、ファイルやアイデアを同僚と共有したいと考えています。人間同士のつながりとそのつながりを促進するツールは、特に、オフィス内で常に同僚と向き合って仕事をするわけではない各地に分散されている従業員にとって、イノベーションの環境、つまり文化をキュレートするための前提条件です。今のところ、回答者の49%が、従業員がデータを簡単かつ安全に共有できるように取り組んでいると回答しています。メリットを得るためには、改善の余地があります。

FORRESTER®

› **カスタマー エクスペリエンスを向上させ、従業員の離職率を下げる。**EXの改善によって従業員の満足度を向上させることで、顧客はより優れたサポートを受け、従業員とスムーズにやりとりできるようになります。満足度の高い従業員は、顧客とって適切な選択を行う可能性が高くなります。[1]ある調査によると、従業員の満足度が高い組織では、顧客満足度が81%向上し、従業員の離職率が半分になっています。[2]

図6

「リモート ワークまたは柔軟な働き方を実現するために、貴社はどのような対策を行っていますか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年9月に実施した調査

主な提言

セキュリティ インフラストラクチャと管理に投資することは、セキュリティ プログラムの重要な要素です。しかし、テクノロジーへの投資だけでは不十分です。組織固有のニーズとリスク許容度に基づいて、組織に最適なバランスのとれたセキュリティ レベルを判断します。

組織でセキュリティと従業員体験の適切なバランスを実現する、次の4つのステップを今すぐ実行しましょう。

現在のセキュリティの成熟度を評価する。評価を実施するプロセスそのもので、原則的な知識である手順やプロセスも可視化される場合があります。これらの手順/プロセスの中には文書化されていないものあるため、文書化を進めることが、主要なチーム メンバーが組織を退職または離職した場合に詳細を明らかにする上で重要です。評価によって、組織の既存のセキュリティ管理、プロセス、監視が可視化されて、潜在的なギャップがある領域や、対策が必要な領域を判断できるようになります。この評価は、注目する必要がある箇所や理由を把握するためのガイダンスとして役に立ちます。

機密データと、その理由および保存場所を特定する。これには、コンプライアンス要件によって規制されているデータと、組織全体におけるデータの価値を理解することが含まれます。セキュリティ管理と適切なデータ処理に関する考慮事項とは別に、データを理解することによって、個人データのプライバシーと倫理的な使用をサポートするための基盤も構築されます。データを明確に把握し、理解することによって、データの保護とその適切な利用に必要な対策を判断できるようになります。

組織のリスク許容度のレベルを把握する。規制によって特定のアクションやアクティビティが義務付けられる場合がありますが、組織が実装する管理のタイプやレベルは、リスク許容度のレベルによって決まります。データと組織に対するリスクを把握し、セキュリティ管理に対するリスクベースの判断を行い、従業員のニーズと生産性のバランスをとるようにします。

従業員の働き方と作業方法を評価する。セキュリティ管理が従業員の作業体験に影響を及ぼす領域と、就業日や生産性に与える影響度のレベルを調査します。従業員の役割から、従業員が作業を実行するためにアクセスするデータまで、従業員のさまざまなプロファイルも、テクノロジーのニーズ、従業員が直面する可能性のあるリスク、それらのリスクを軽減するために実装する必要のあるセキュリティ管理のタイプに影響します。不必要な摩擦の原因となるものではなく、必要なセキュリティ制御を実装します。

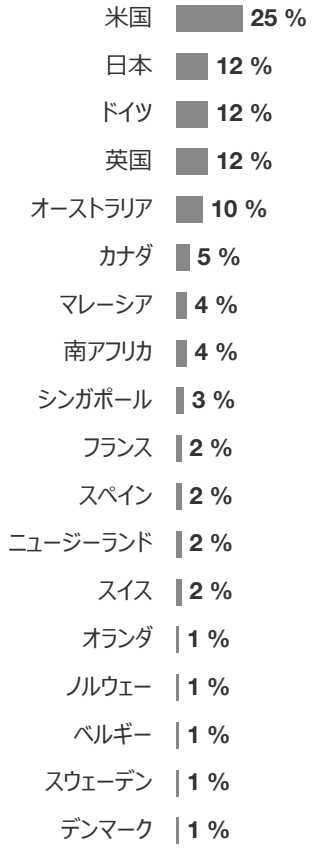
FORRESTER®

付録A：手法

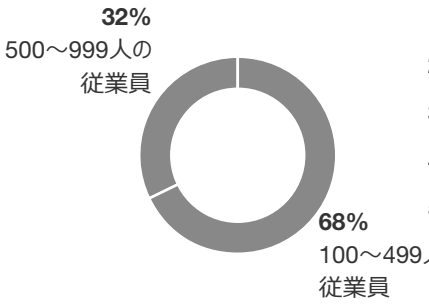
この調査で、Forresterは、市場のさまざまな業界における887人のビジネス リーダーとITリーダーを対象にオンライン調査を実施しました。参加者に対する質問では、セキュリティにかけるコストの変化、セキュリティ戦略、コンプライアンス、規制に関する課題に影響を与える要素、組織におけるセキュリティの将来像について尋ねました。この調査は2019年3月に始まり、ソート リーダーシップ ペーパーは2019年8月に完成しました。

付録B：人口統計

「お住まいの国はどちらですか。」

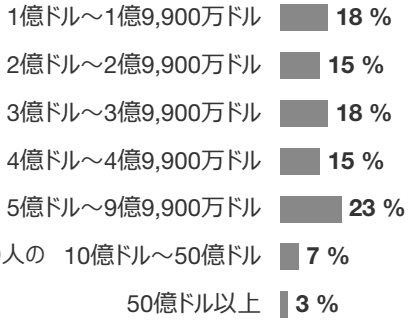


「最も正確に見積もって、貴社の従業員数は世界中でどのくらいですか。」

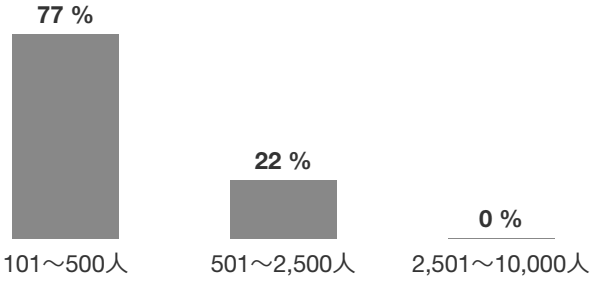


「最も正確に見積もって、貴社の年間収益（米ドル）はどのくらいですか。」

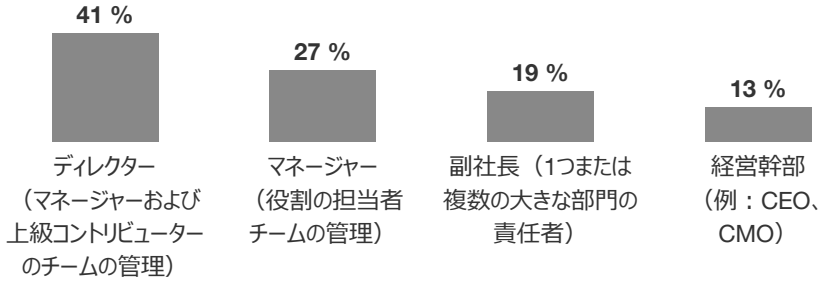
（N = 861）



「あなたが最も影響力を持っているテクノロジーおよびサービスの購入に関する決定について、直接影響を受ける従業員または組織のメンバーの数はどのくらいですか。」



「貴社におけるあなたの役職を最も的確に表している説明はどれですか。」



対象者：ノートパソコン、PC、その他のデバイスの導入決定に関わる887名のビジネスおよびIT導入決定者
原典：デルにより委託され、Forrester Consultingが2019年3月に実施した調査

FORRESTER®

付録C

巻末注

[1] 出典：『Transform The Employee Experience To Drive Business Performance』Forrester Research, Inc.、2018年2月12日。

[2] 出典：James K. Harter、Frank L. Schmidt、Theodore L. Hayes『Business-Unit-Level Relationship Between Employee Satisfaction, Employee Engagement, and Business Outcomes: A Meta-Analysis』Journal of Applied Psychology、2002年4月（http://www.factorhappiness.at/downloads/quellen/s17_harter.pdf）。