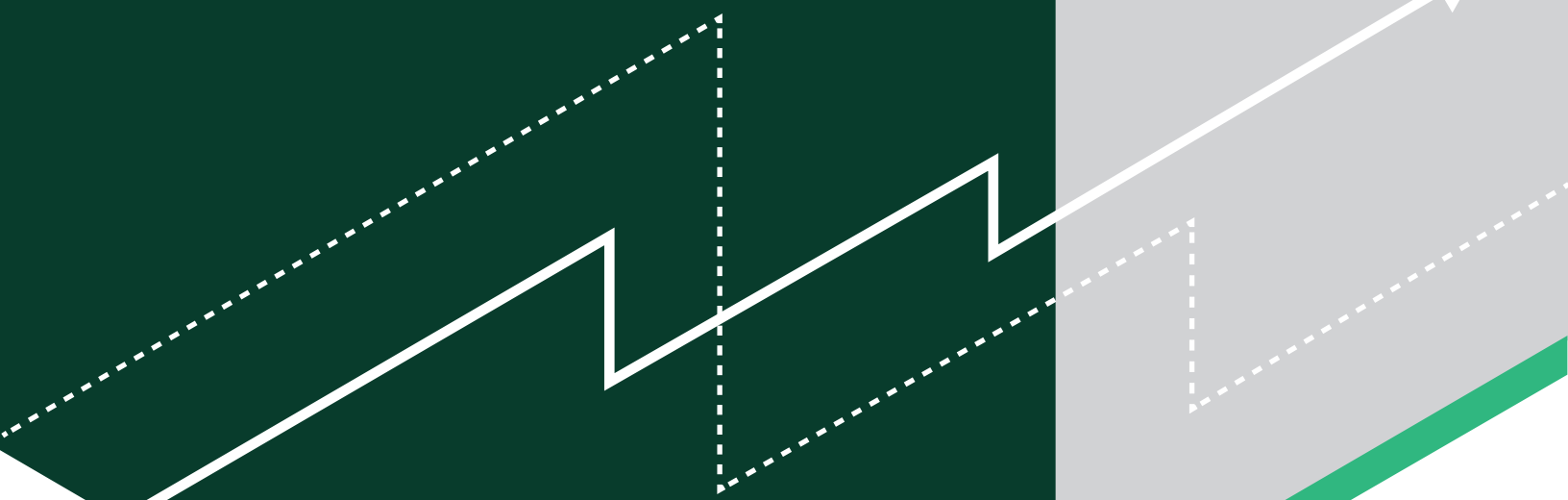
Forrester Consulting Thought
Leadership Paper
（HP社委託調査）

2021年6月

ゼロトラストによる エンドポイント保護と 生産性のバランス



FORRESTER®

目次

3 エグゼクティブサマリー

4 企業はゼロトラスト戦略の一環としてエンドポイントのセキュリティ強化が必須

6 ゼロトラストアプローチの採用を妨げる社内と技術面の課題

8 ゼロトラストは脅威の防御と検知を実現し、従業員の生産性を向上させる

12 主な推奨事項

13 付録

プロジェクト統括：
Madeline Harrell、マーケットインパクトコンサルタント

リサーチ貢献者：
Forrester社セキュリティ&リスク・リサーチ・グループ

FORRESTER CONSULTING について

Forrester Consulting は企業リーダーがその組織を成功に導けるよう、独立し客観的なリサーチベースのコンサルティングを提供しています。当社のサービスの内容は、短い戦略セッションからカスタムなプロジェクトに至るまで多岐にわたります。それらのサービスでは、調査アナリストが顧客に直接対応します。また、特定の事業における課題について専門家が知見を提供します。詳細については、forrester.com/consultingをご覧ください。

[E-51293]

FORRESTER®

エグゼクティブサマリー

企業のリモートワークフォースの増加に対応するため、セキュリティリーダーは、従来のセキュリティ境界の外で、企業の機密性の高いデータへアクセスするデバイスの、爆発的増加への対応に苦心しています。攻撃者はこのアタックサーフェスの拡大によって露呈した保護対策の間隙を利用し、企業のネットワークをラテラルムーブ（横展開）し、機密資産を侵害します。企業がこのリスクを抑えるには、エンドポイントデバイスに対するゼロトラスト（ZT）戦略の採用が必須です。ZTでは、エンドポイントのハードウェア、アプリ、データ、ネットワークリソース間における暗黙の信頼を排除し、アクセス制御の決定に対するリスクを継続的に評価します。

ゼロトラスト戦略を採用すれば、セキュリティ＆リスク（S&R）の専門家は、リモートワーカーとそのデバイスが企業の機密資産へアクセスすることに付随するリスクを、より効果的に管理し、限定化できるようになります。そのためにはネイティブOSのセキュリティやハードウェアのセキュリティ対策など、エンドポイントの脅威に対する異なった防御や検知のテクノロジー連携が必要となります。最終的にこの連携により、S&R専門家は、従業員体験（EX）とセキュリティのバランスを保ちながら、以前より良い環境で新たな脅威や既存の脅威に対処することができます。

HPは、Forrester Consultingに、エンドポイントセキュリティに対するゼロトラストアプローチの潜在的なベネフィットと課題についての評価を委託しました。Forresterは、これらの動向を把握するために、ネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人を対象に、オンラインアンケート調査を実施しました。

主な調査結果

- **企業は、就業場所に関係なく、データやデバイス、ネットワークを保護する重要性の高まりを認識している。**インシデント対応は依然として高優先事項ですが、調査参加者の79%は脅威検知について重要ないし高優先と回答しており、企業ではモバイルセキュリティ体制の一貫として脅威防止および積極的なデータ保護を通してエンドポイントセキュリティに対する、よりプロアクティブなアプローチがとられています。
- **ゼロトラストは、悪意あるアクターによるラテラルムーブや、それに伴う企業や従業員データの侵害に対抗するのに有効と考えられる。**過去1年間に、ラテラルムーブまたは在宅ワーカーのデバイス、全体的なセキュリティインシデントの増加による企業データの侵害を経験したと回答した調査参加者は3分の 1 を超えます（34%）。
- **ゼロトラストアプローチではデータ侵害の防止・検知のみならず、ビジネス側面とEX側面の恩恵も得られる。**調査参加者の3分の 1 近くが、ゼロトラスト戦略の採用なくしては職場のセキュリティ文化が脆弱となると回答しています。ZTの採用によって全体的なリスクが低減されるだけでなく、従業員の生産性も向上します。

FORRESTER®

企業はゼロトラスト戦略の一環としてエンドポイントのセキュリティ強化が必須

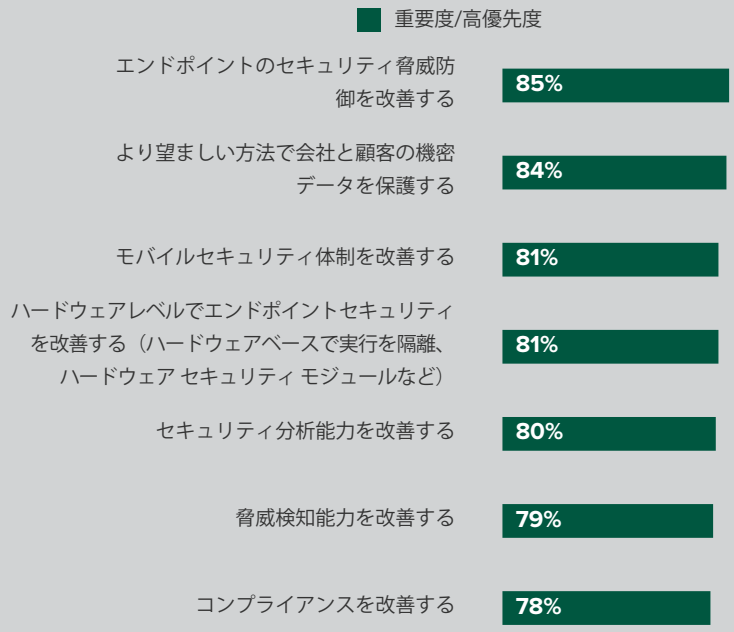
悪意あるアクターによるラテラルムーブにさらされたエンドポイントの数と種類が増加すれば、その分リスクも増加します。

- **企業では、ハードウェアレベルまで、ますますエンドポイントセキュリティに注力している。**企業と顧客のデータ保護に重点が置かれており、エンドポイントはそのインフラとデータのすべてに対しアクセスを可能にするスポークとなっています。調査参加者の85%は、今後12か月間で、エンドポイントのセキュリティ脅威防御の改善が重要で優先度が高いと回答しており、続いて企業と顧客の機密データ保護の強化が挙げられていました。これには従業員の会社提供デバイス、従業員所有デバイス、リモート従業員が就業するホームネットワークに接続されているあらゆるデバイス（IoTデバイス、プリンターなど）が含まれます。また、ハードウェアレベルでのエンドポイントセキュリティの向上も主な優先事項（81%）となっており、ITやセキュリティチームの最優先事項がエンドポイントセキュリティとハードウェアの安全性確保であることが表れています（図1参照）。

ラテラルムーブメントまたは在宅ワーカーのデバイスからの企業データの侵害、もしくはセキュリティインシデントの全体的な増加を経験したと回答した調査参加者は3分の1を超えます（34%）。

図1

「貴社のIT組織では、今後12か月間における以下の情報／ITセキュリティ目標および取り組みの優先度はどの程度になりますか？」



対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
注：回答13件中の上位7件を表示
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

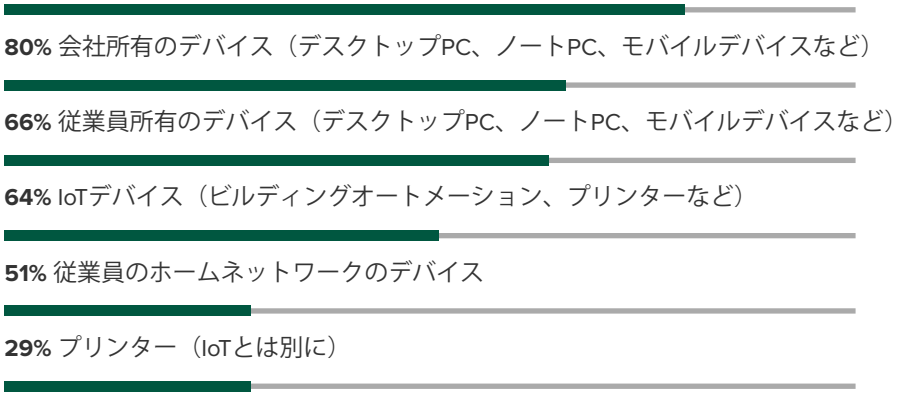
FORRESTER®

› **在宅ワーカーを介した脅威は、企業のリスクを高めている。**リモートワークフォースとハイブリッドワークフォースの急激な増加により、ほとんどの企業ではアタックサーフェスが拡大され、IoTデバイスやプリンターなどホームインターネットを含めた、企業のネットワークにアクセスする全エンドポイントの安全性確保の必要性が高まっています。80%が会社所有のデバイスの保護を行っており、66%が従業員所有のデバイスを保護していますが、IoTデバイス（プリンター含む）を保護しているのは64%にとどまっています（図2参照）。実際には、攻撃と侵害の絶え間ない増加に鑑みれば、これらの数字はすべて100%近くになるべきです。企業は従業員とIoTデバイスの保護をこれ以上は先送りできません。従業員とIoTデバイスは、リモートワークの増加のためにアタックサーフェスの一部となってしまっています。

› **企業がリモートワーカーの増加に対応している間にも、悪意あるアクターは時間を無駄にせず、エンドポイントセキュリティの弱い企業を狙っている。**過去1年間では、3分の1を超える企業（34%）がラテラルムーブまたは在宅ワーカーのデバイスから企業データの侵害、あるいはセキュリティインシデントの全体的な増加を経験しています。32%は、従業員所有のデバイスからの企業データの侵害を経験しています。ゼロトラストは、悪意あるアクターの企業環境内の移動と、それに続く企業や従業員のデータ侵害を防御するうえで必要不可欠です。

図 2

「貴社のエンドポイントセキュリティ戦略の一環として、どのエンドポイントが保護対象に含まれていますか？」



対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

ゼロトラストアプローチの採用を妨げる社内と技術面の課題

ITチームは、エンドポイントセキュリティへのゼロトラストアプローチ採用に価値を見出していますが、採用の大きな一歩を踏み出そうとして、社内と技術面での困難に直面しています。企業は現在のセキュリティソフトウェアによるエンドポイントの保護に苦労していることを認めています。企業の47%が現在のエンドポイントのセキュリティソフトウェアの有効性について、今日の脅威に対抗するには不十分であると回答しています（図3参照）。さらに、攻撃者によるエンドポイント、サーバーあるいはアプリケーション間のラテラルムーブを阻止する十分なバリアも存在しません。ZTアプローチの採用は有効と考えられますが、経営幹部の参画を得るのは、依然として困難です。

- **ZTがエンドポイントセキュリティの問題を解決することは明らかでも、ITチームは組織面の障害に直面している。** IT部門の意思決定者は、エンドポイントセキュリティに対するアプローチになると、ITチームとセキュリティチーム間で過剰な摩擦が生じると回答しています（43%）。IT部門の意思決定者の45%が、ZTの実装に踏み切るうえで経営陣の同意が得られないと回答しています。経営陣はZTの採用で何が失われると考えているのでしょうか？経営陣が懸念しているのは、ゼロトラストの採用で従業員ワークフローに混乱が生じること、実装のパートナーに支払う予算がないこと、それに対応できるプロセスが社内にないということです。
- **ZTの採用には、技術的な課題がないわけではない。**組織面の課題から視線を外しても、採用に踏み出す際に企業は何から着手すべきか現在も不確実なままです。ITチームがZTを容易に採用できない主な技術的課題には、IDアクセス管理機能を強化する必要性があること、また、社内におけるコンプライアンスに関する専門知識の欠如が挙げられます。42%が採用について、どこから着手してよいのか、あるいは中止すべきなのかわからないと回答しています。組み込みでユーザーフレンドリーな導入体験を提供する新テクノロジーの採用や、サードパーティのサービス経由でノウハウを得ることは、ITチームがZTへのロードマップを得られるというメリットがあります。ZTを推進する方法をゼロから考案する必要はないのです。
- **ゼロトラストがないと、従業員体験が損なわれ、ビジネスも同様に損なわれる。** 経営幹部が従業員ワークフローの混乱を懸念する一方で、調査参加者の過半数（57%）がZTの採用前にはセキュリティ関連タスクに従業員の時間が過剰に費やされていたと回答しています。VPNのログインに無駄に時間を費やしたり、2要素認証で所定のフィールドに適切なコードを入力したり、従業員はセキュリティに時間を費やしすぎています。また、企業はアタックサーフェスの拡大に伴って厳重なセキュリティ対策を講じているため、従業員は就業する場所の選択（37%）や個人所有デバイスの利用可否（56%）に関して自主性を失う状況に陥っています。企業がオフィス勤務への回帰、またはオフィス勤務と在宅勤務のハイブリッドモデルに移行している中で、従業員がどこで、どのように働くか、柔軟かつ自律的な選択を提供できることの価値は高まるばかりです。

図3

「現在エンドポイントセキュリティに対して行われている貴社のアプローチの最大の課題とは何ですか？」

47% 会社で使用されているエンドポイントセキュリティ用ソフトウェアが昨今の脅威に対抗するには不十分である

43% 攻撃者によるエンドポイントおよび／またはアプリケーション間のラテラルムーブを防御する十分なバリアが存在しない

43% ITチームとセキュリティチーム間の摩擦が大きすぎる

37% 会社のセキュリティのテクノロジーとポリシーが、進化し続けるワークフォースに生じるリスクに対応するには静的すぎる

「ゼロトラストアプローチ採用前に直面していた従業員体験に関する課題にはどのようなものがありましたか？」

57% 従業員がセキュリティ関連タスク（VPN、2FAなど）に費やさねばならない時間が長すぎる

56% BYOD（個人所有デバイスを業務に使用すること）にまつわる柔軟性の欠如

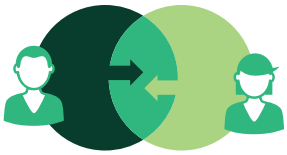
37% 従業員に就業場所を選択する自由が与えられていない

35% 従業員満足度が低い

対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
注：上位4件を表示
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

ゼロトラストは脅威の防御と検知を実現し、従業員の生産性を向上させる

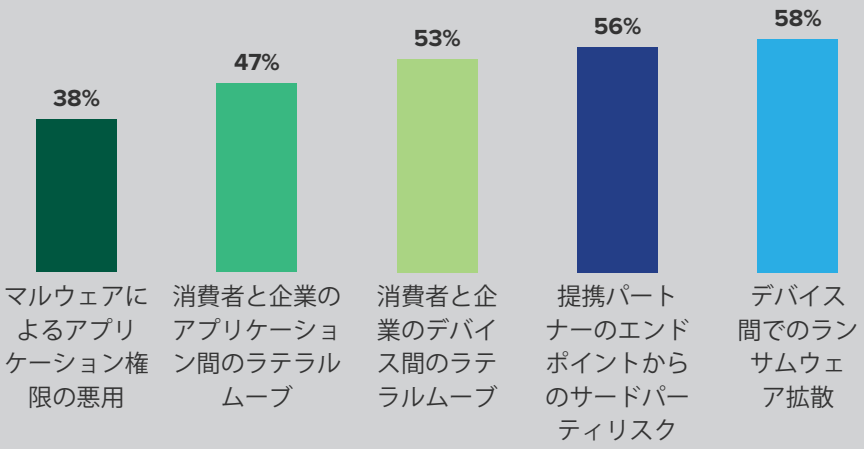
ITチームがゼロトラストの無視できないメリットについて経営陣の説得に奮闘する傍ら、増え続けるリモートまたはハイブリッドのワークフォースを実現させるために準備を進めている間にも、他社に先行してゼロトラストを採用した、あるいは現在採用している企業はすでに大きな恩恵を享受しています。エンドポイントセキュリティに対するゼロトラストアプローチは、現在の脅威を解決に導くだけでなく、チームが侵害の発生前に積極的に予防行動を取ることを可能にします。保護を必要とする潜在的な脅威が多くないのであれば、ITチームやセキュリティチームは、本質的ではないセキュリティ関連の業務に時間を費やすことなく、生産的な業務に時間を活用できるようになります。このように生産性を向上させる自由度が加わることで、ゼロトラストは従業員が切望する自律性と柔軟性を高め、企業の従業員満足度を上昇させます。



- **ZTアプローチは、悪意あるアクターのラテラルムーブを防ぐなど、技術面での主要な懸念に対応できる。**ZTをエンドポイントに対して採用した後で、企業はデータ侵害の検知だけでなく防御能力の改善についても既に実現済みか、今後実現すると予想しています。実際、調査参加者の過半数がエンドポイントのZTアプローチは、とくにデバイス間のランサムウェア拡散、そしてパートナー企業のエンドポイント由来のサードパーティリスクに対応してくれると回答しています（それぞれ56%、58%）。また、消費者と企業のアプリケーションおよびデバイス間でのラテラルムーブメントに関しても、ゼロトラストはアイランドホッピング攻撃（サプライチェーン攻撃）の阻止に役立ちます（それぞれ53%、47%）（図4参照）。

図4

「貴社のエンドポイントに対するゼロトラストアプローチでは、具体的にどのような脅威に対抗することが可能ですか？」



50%超がサードパーティパートナーのエンドポイントとランサムウェアからのラテラルムーブのリスクにZTで対抗できると確信している。

「ゼロトラストセキュリティのフレームワーク採用によって実現が予測される、または実際に実現したテクノロジーのベネフィットにはどのようなものがありますか？」

43% セキュリティ侵害の防御能力の向上

37% セキュリティ侵害の検知能力の向上

35% 認証情報の漏洩低減能力の向上

33% マルウェアの伝播阻止能力の向上

30% データ管理プロセスの効率性の向上

対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
注：上位5件を表示
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

FORRESTER®

- **ZTによって従業員の自律性と満足感が高まる。**ZTではエンドポイントのすべてをより堅牢に保護することが可能になるため、企業が従業員に配慮する余裕が生まれます。デバイスとセキュリティ対策をした従業員所有デバイス間のラテラルムーブを減少させる技術面のベネフィットにより、従業員は場所を選ばずに就業できる自由が得られ、望んでいた自律性の向上を享受できるようになります（54%）。動作の重いVPNへのログインや認証などの、セキュリティ関連のタスクに従業員が費やす時間が短縮されると、より創造的な業務に時間を使うことができるようになります。全体としては、企業の57%でゼロトラストアプローチの採用後に従業員満足度の全体的な向上を予想しているか、すでに向上を実現したことが示されています（図5参照）。
- **ZTはリスク全体を低減しながら従業員の生産性を高め、ビジネスに有効である。**ゼロトラストは最初の段階でラテラルムーブを阻止するので、企業は悪意あるアクターからの攻撃の防御と検知を行う自社の能力を案じる必要がなくなります。その結果、従業員には生産性向上とそれぞれの役割に満足するために必要な時間と自由が与えられます。しかし、一般的な意味合いにおいて、ZTが組織にもたらすのはセキュリティ文化の変容です。51%がZTのセキュリティフレームワークの採用によって会社でセキュリティが優先されるようになったと回答しています。続いて僅差で生産性の向上（48%）ならびにリスク全体の低減（47%）が挙げられていました。ZTアプローチでは典型的な管理のためのセキュリティタスクに費やされる時間を短縮できるため、優先度の高い侵入者の防止と検知に集中する時間が生まれます。40%近くの回答者はまた、利害関係者の賛同数の増加をはじめ、コンプライアンス関連の取り組みのコスト削減や、全社規模のアジリティの向上にも貢献したとコメントしています。ゼロトラストフレームワークを採用することにより、企業は顧客と企業のデータを守る、より効果的な新戦略を手に入れ、従業員の満足度と生産性の向上と、セキュリティ機能全体の成熟を優先できるだけの余裕も手に入れることができたのです。

図 5

「ゼロトラストアプローチの採用によって実現した、または実現が予測されていた従業員体験のベネフィットにはどのようなものがありますか？」

57% 全体的な従業員満足度の増加

54% 場所を選ばずに仕事ができる能力／従業員の高い自律性の向上

53% セキュリティ関連タスク（VPN、2FAなど）に費やされる従業員の時間の短縮

48% BYODに関する柔軟性の向上

41% 会社のセキュリティ文化の向上

31% 良好なUX（ユーザー体験）のテクノロジーを用いた従業員エンゲージメントの向上

「ゼロトラストセキュリティのフレームワーク採用によって実現が予測される、または実際に実現したビジネスのベネフィットにはどのようなものがありますか？」

51% セキュリティの優先度上昇

48% 組織全体の生産性向上

47% 全体的なリスクの低減

39% 利害関係者の賛同数の増加

39% コンプライアンスの取り組みに対するコストの削減

39% 組織全体のアジリティの向上

38% セキュリティの設備投資および／または運用コストの削減

対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

主な推奨事項

Forresterのセキュリティ&リスクの意思決定層を対象にしたエンドポイントセキュリティに関する詳細なアンケート調査により、以下のような重要な推奨事項が導き出されました。

セキュリティの複雑性を削減する防御重視のアプローチを取る。アタックサーフェスの縮小を主体とする脅威防御ツールを採用します。それによりセキュリティの複雑性が低下し、エンドポイントセキュリティのレジリエンスが全体的に改善されます。具体的には、ハードウェアセキュリティ、エクスプロイト対策テクノロジー、アプリケーションセキュリティ、データセキュリティ、セキュリティ構成管理が含まれます。これらはいずれも、インシデント対応チームの余計な仕事を増やす、攻撃者による従業員のエンドポイントへの侵入の可能性を低減します。

従業員のエンドポイント全体に渡って重要なデータとアプリケーションを特定し、セグメント化する。エンドポイントセキュリティのポリシーと基準はゼロトラスト戦略をサポートし、データとアプリケーションのセグメント化が定義するリスクのレベルと整合性が取られていなければなりません。これはエンドポイントのハードウェア層とソフトウェア層での可視性と制御を必要とします。

脅威分析には、エンドポイントの複数の層から収集されたイベントデータを相関させる必要がある。悪意ある活動を特定しブロックするためには、エンドポイントの保護層は、全てのハードウェア、ソフトウェア、ユーザーア クティビティをカバーして、外部の脅威インテリジェンスと相関させる必要があります。ふるまい分析をOSとハードウェア層から得られるセキュリティテレメトリを用いて強化すれば、全体的な精度が向上し、サードパーティ製品との統合に有用です。

ゼロトラストの採用で基軸にすべきなのは、強力な従業員体験の提供である。ゼロトラストとは、従業員のトラスト（信頼）を排除することではありません。実際のところ、ゼロトラストを適切に活用すれば、柔軟性が皆無の厳格で包括的な方針に比べて、従業員が制限の少ない望み通りの方法での勤務をより自由に選べるようになります。これには、検知されたリスクの程度に応じて柔軟に制御できる機能と、ユーザー、デバイス、アプリケーション、データに関するリスクをリアルタイムできめ細やかに把握することが必要です。そしてそれらのバランスを取り、適切な場合にのみ従業員を制限し、それによって、機密性の高いワークリソースにより迅速で安全なアクセスを可能にします。

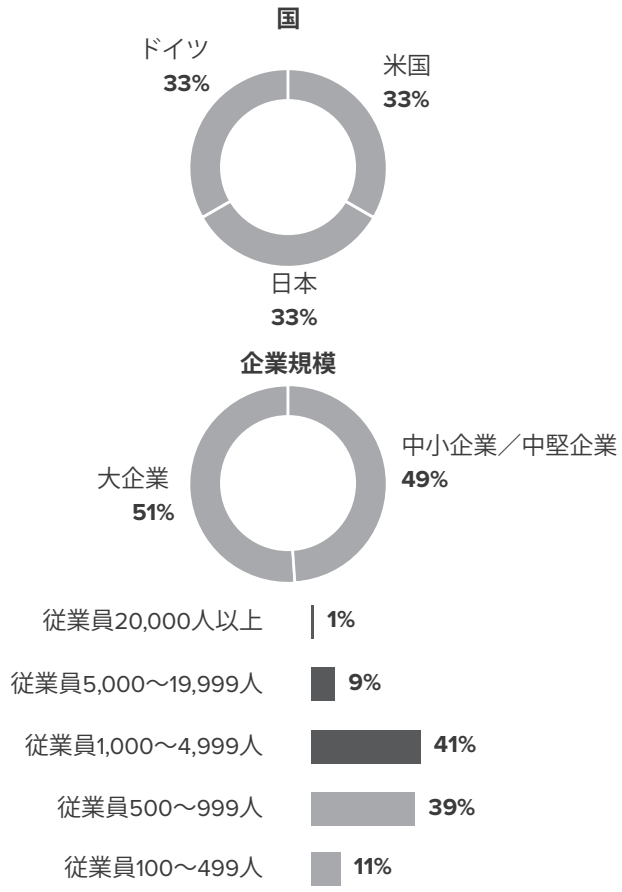
3〜5年間を見据えた戦略的なエンドポイントセキュリティのロードマップを構築する。少なくとも1年に1回は、エンドユーザーのデバイスの保護と管理に携わるセキュリティとITの運営チームの主要な利害関係者を集め、エンドポイントセキュリティのテクノロジーへの現在の投資を評価します。そして、サードパーティおよび有償のセキュリティツールの重複している部分を確認します。その際、現状において問題となっている機能の成熟度およびコモディティ化の程度を元に、現在重複している部分と将来潜在的に重複する部分を確認します。たとえば、完全なディスクの暗号化、アンチウイルス、アプリケーションホワイトリストなどの機能は、企業レベルで利用可能で、様々なサードパーティテクノロジーに現在置き換えが可能なものです。一方で、ホスト型ファイアウォール、実行隔離、セキュリティ構成管理などの機能は、将来の置き換え候補と言えるかもしれません。

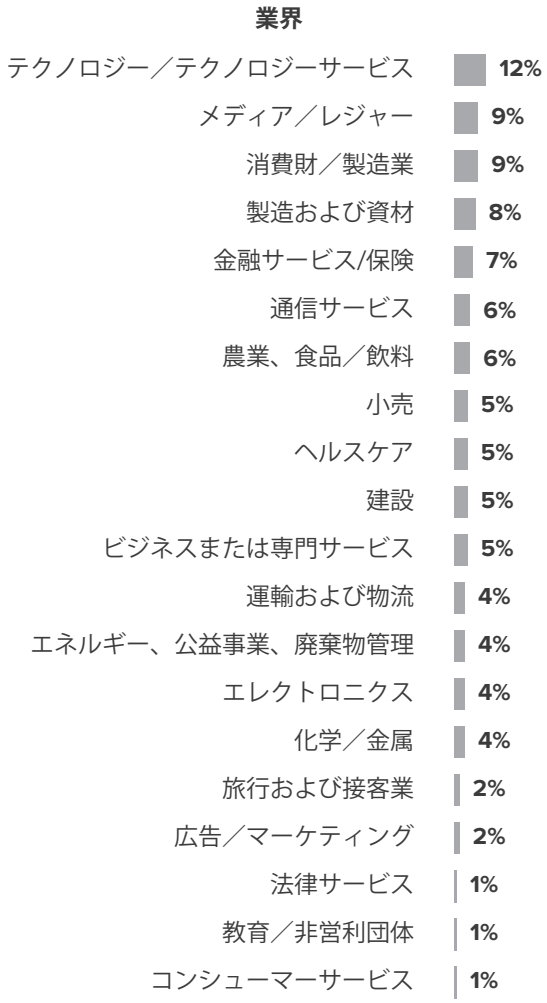
FORRESTER®

付録A：調査方法

この調査では、Forresterは、企業でのエンドポイントセキュリティに対するゼロトラストアプローチの採用について評価するため、NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人にオンラインアンケート調査を実施しました。調査参加者に出された設問では、エンドポイントセキュリティの現在の状態や、エンドポイントセキュリティに関し直面している課題、ゼロトラストを採用することによるメリットについて質問しました。調査は2021年3月に開始され、2021年4月に終了しました。

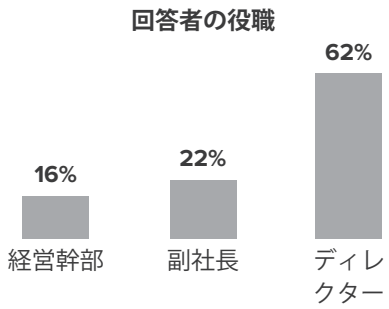
付録B：統計／データ

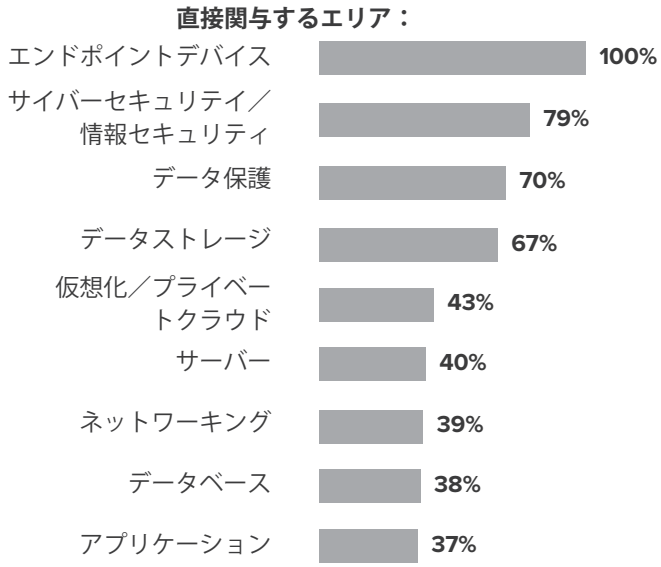


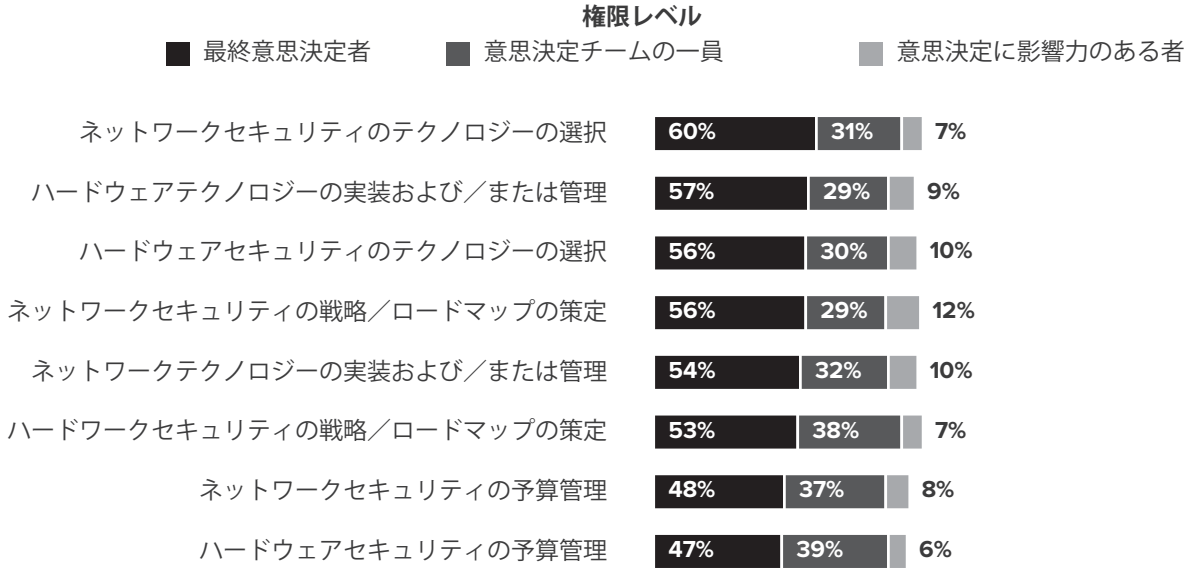


対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

FORRESTER®







対象：NA、EMEA、APACの中小企業／中堅企業および大企業のネットワークセキュリティ／ハードウェアセキュリティの責任者であるディレクター以上のITセキュリティ専門家607人
出典：2021年4月にHP社からの委託によりForrester Consultingが実施した調査

FORRESTER®