ivanti

2020
ゼロトラストに関する導入進捗報告書

Cybersecurity Insiders

はじめに

昨今、データ侵害が増加しており、これはサイバー攻撃から免れる組織は存在しないということを示しています。原因のひとつは、働き方のモビリティ化とクラウドコンピューティングの活用により、企業ネットワークと従来の防御境界域を超えてアクセスされているためです。ゼロトラストセキュリティモデルの企業での導入は、サイバーリスクを軽減するための重要な対策の一環として拡大しています。最低限の特権による条件付きアクセスを付与する前に、ユーザー、デバイス、インフラストラクチャ検証の原則に基づいて実施するため、ゼロトラストは大幅に強化された操作性、データ保護、ガバナンスを可能にします。この2020ゼロトラスト導入に関する進捗報告書では、企業がゼロトラストセキュリティをどのように実装しているかを明らかにし、導入に関する主要な要因、状況、技術、投資とメリットを解説します。

この2020年のゼロトラスト調査は、400人以上の複数の業界の様々な組織に在籍する技術系の役員からITセキュリティの実務者に至るまでのサイバーセキュリティ意思決定者を対象に実施したものです。72% の企業や組織が、増大するサイバー リスクを軽減するために、2020 年にゼロ トラストを評価または実装する予定で、ほぼ半数 (47%)のサイバーセキュリティの専門家の中には、ゼロトラストモデルを自社のセキュアアクセス環境に適用する自信がないと回答しています。

主な調査結果:

- セキュアアクセス環境にゼロトラストモデルを適用することに対する自信の有無はほぼ同等です(53%は自信を持ち、47%は自信がありません)。
- 53%がゼロトラストの機能をハイブリッドなIT環境に移行しようと計画しています。
- 60%以上が、ゼロトラストは継続的な認証と承認、人、モノなどすべての検証によって得られる信頼できるデータ保護施策であると認識しています。
- 40%以上が、特権管理や安全とは言えないパートナーアクセス、サイバー攻撃、シャドーIT のリスク、脆弱性の高いモバイルやデバイスへのアクセスが、アプリケーションやリソースへのアクセスを保護するための最も困難な課題と認識しています。
- 45%が、パブリッククラウドアプリケーションのアクセスセキュリティに、43%が、BYODによるアクセスセキュリティに関心を持っています。
- 70% の企業や組織が、アイデンティティ/アクセス管理機能の向上を計画しています。
- 30% の企業や組織が、ユーザー体験の向上や管理とプロビジョニングの最適化など、セキュリティで保護されたアクセスの提供を簡素化することを目指しています。
- 41%が、セキュアなアクセスインフラを再評価し、ソフトウェア定義の境界(SDP)を検討しようとしています - ハイブリッドITの展開が必要な大多数と、SaaSを採用している1/4にのぼります。

ゼロトラストの原則

ゼロトラストのどのような原則が企業や組織に最も有用なのでしょうか? 継続的な認証/承認が、ゼロトラストの一番の価値であると67%が回答しています。そして、ユーザー、デバイスなどのエンティティの検証による信頼(65%)、インフラストラクチャ コンポーネントとデータ保護 (例: 安全な接続) (63%)と続きます。

ゼロトラストのどの原則が貴社や組織にとって最も有用だと思われますか?

67%
継続的な認証と承認

65%
検証によって得られた信頼 (ユーザー、デバイス、インフラストラクチャなど)

63%
データ保護 (安全な接続など)

56%
エンドtoエンドなアクセスの可視化と監査

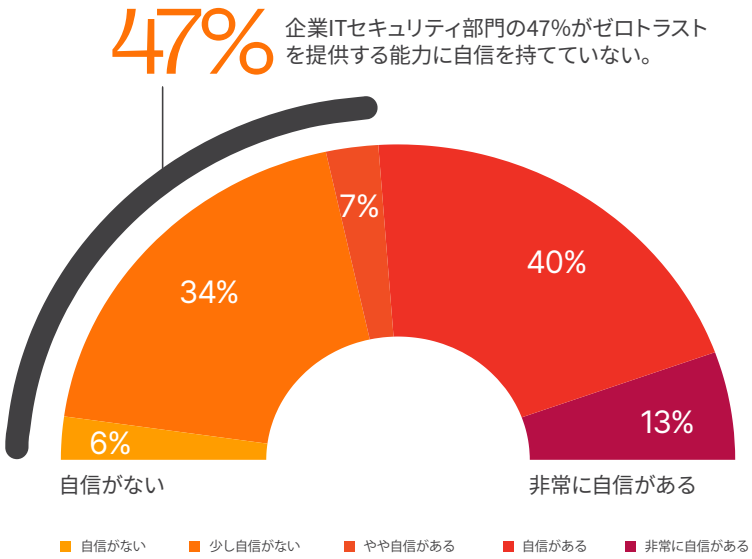
54%
最低限の特権アクセスを付与

46%
一元化されたきめ細かいアクセスポリシー

ゼロトラスト 実装への自信

53% の企業や組織が、セキュリティで保護されたアクセス アーキテクチャにゼロトラストを実装することに自信を持っていますが、企業の IT セキュリティ部門の 40% 以上が、ゼロ トラスト実装に自信がないと回答しています。

貴社のセキュリティインフラにゼロトラスト モデルを実装する自信はどれくらいありますか?



ゼロトラスト 推進の要因

企業や組織がゼロトラストの取り組みを開始し、導入する要因は何なのでしょうか。データセキュリティが85%で第一の要因であり、次いで侵害の防止(70%)、エンドポイントに対する脅威の削減(56%)と回答されています。業界や法規制、社内コンプライアンス以外にも、企業の1/3近くがハイブリッドITのセキュリティの問題に取り組んでいます。

貴社で アイデンティティアクセス管理やゼロトラストを推進する主な要因は何でしょうか?

85%

セキュリティ/
データ保護

70%

セキュリティ
侵害の防止

56%

エンドポイント、
IoTセキュリティ脅
威の低減

内部脅威の低下

業界/法規制の順守
(HIPAA, GDRP, PCI DSSなど)

内部コンプライアンス

セキュアなアクセス の課題

セキュアなアクセスの実現に、企業や組織が直面している主な課題は何でしょうか。特権を持つ従業員(62%)、機密性の高いリソースへのパートナーからのアクセス(55%)、脆弱なモバイルや危険なデバイスのアクセス(49%)などの課題を企業や組織は経験していると回答しています。

アプリケーションやリソースへのセキュアなアクセスを確保するうえで、貴社が直面している 課題は何でしょうか?

62%

特権を持つ従業員
のアクセス

55%

アプリやリソースへの
安全でないパートナー
からのアクセス

49%

脆弱なモバイルや危
険に晒されているデ
バイスへのアクセス
(不明、未認可、非準拠、無効
なエンドポイントなど)

サイバー攻撃
(DoS攻撃、クロスサイトスクリプティング
攻撃、中間者攻撃、フィッシングなど)

シャドウ IT

セキュリティの 優先度

調査では、企業や組織の 71% が アイデンティティアクセス管理の向上を最優先にしているという結果になりました。そして、データ損失の防止 (59%)、クラウド サービス プロバイダーが提供するクラウド アプリへの安全なアクセス (45%)が続きます。

貴社のセキュリティに関する現在の優先度が最も高いのは何でしょうか?

71%
アイデンティティとアクセス管理の向上 (IAM)

59%
データ損失の防止 (DLP)

45%
クラウドサービスプロバイダがホストするアプリケーションへのセキュアなアクセスの確保(Microsoft, Amazon, Googleなど)

43%
エンドポイントモバイル管理の有効化(EMM) / BYOD (ユーザー、デバイスなど)

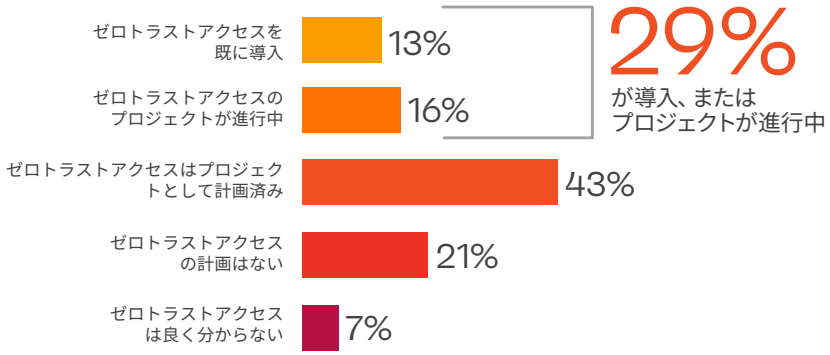
35%
詳細な SSL 検証の実施 (セキュアなセッション、マルウェアスキャンとウェブ/メールフィルタリングのための復号化など)

30%
セキュアなアクセスの展開を簡素化 (ユーザー体験、管理など)

ゼロトラスト の導入

ゼロトラストアクセスを導入する計画について尋ねたところ、29%近くがゼロトラストアクセスを既に導入しているか、プロジェクトが進行中で、43%は計画段階にあると回答がありました。驚くべきことに、ほぼ1/3は計画を持っていないか、ゼロトラストに精通していないという事実が明らかになりました。

貴社では、ゼロトラストアクセスを導入する計画をお持ちでしょうか?

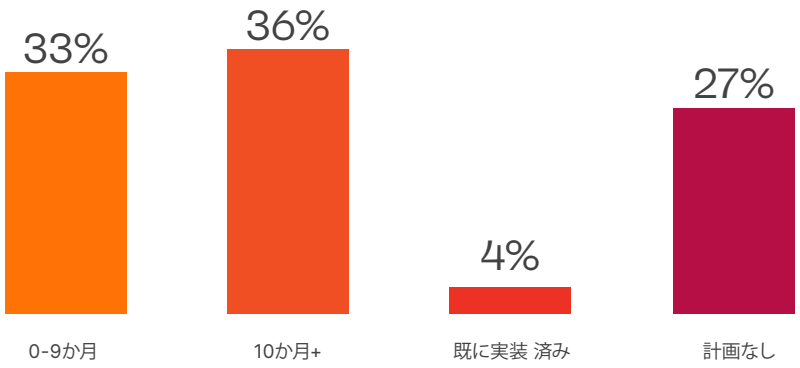


導入のスピード

ゼロトラストへの関心は、初期の導入展開に移っています。実際に企業の33%が9か月以内にゼロトラストを導入する予定です。しかし、ほぼ1/3は、価値や成果に関する誤解から導入計画を持っていないと回答しています。

貴社ではどのような時間枠でゼロトラスト セキュリティを導入する可能性が最も高いでしょうか?

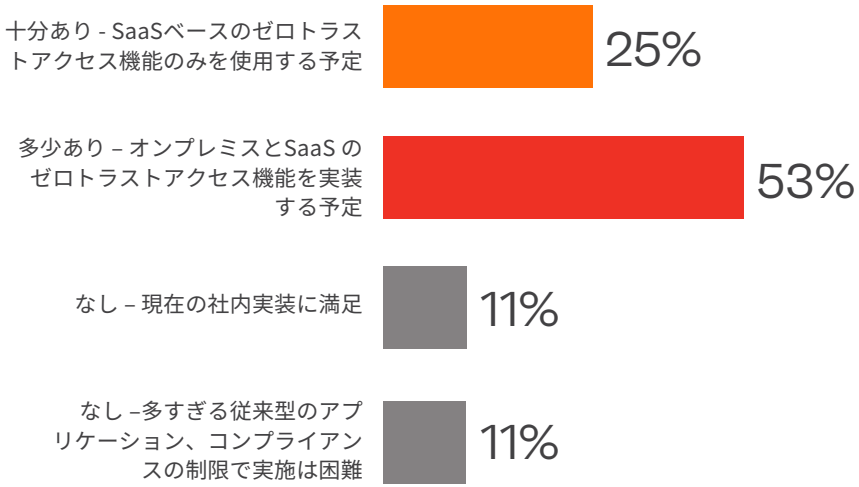
33% の企業が9か月以内にゼロトラストを導入する予定です。



ゼロトラスト SaaS

企業や組織の半数以上がゼロトラストアクセスをハイブリッドIT(オンプレミス/SaaS)環境に移行する予定があると回答しました。1/4が、SaaSベースのゼロトラストソリューションのみを移行する予定であり、22% が、従来のアプリケーションやコンプライアンスの制限、または現在実装されているアクセス保護に満足しており、SaaS ベースのゼロトラストを展開する計画を持っていないという結果になりました。

今後 18 か月間で貴社は、どの程度の範囲でゼロトラストアクセスの機能を SaaS に移行する予定でしょうか?



ゼロトラスト アクセス 投資の優先度

ゼロトラストアクセスへの投 の大半は、多 素 証(59%)、アイデンティティ管理とガバナンス(48%)、シングルサインオン(44%)に向けられています。そして、ネットワーク アクセス制御と Web アプリケーションのファイアウォール (43%)、特権アクセス管理とマイクロセグメンテーション (41%)、さらに仮想プライベート ネットワーク (35%)へと続く結果となりました。

次の アイデンティティアクセス/ゼロトラストの 素のうち、社が今後 12 か月以内の投 で最も い優先 位を付けるものはどれでしょうか?[6]

59%

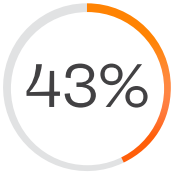
Multi-Factor Authentication (MFA)

48%

Identity management and governance

44%

Single Sign-On (SSO)



Network Access Control (NAC), Web Application Firewall (WAF)

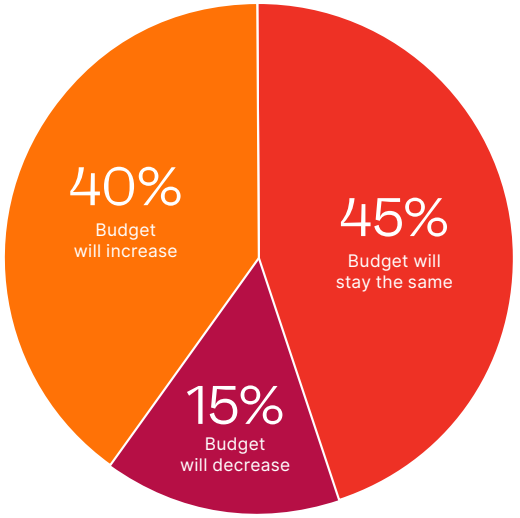
Privileged Access Management (PAM), Micro-segmentation

Virtual Private Networks (VPN)

ゼロトラスト アクセスの予算

40%の企業や組織 は、今後 18 か月間にアクセス管理関連の予算が増加すると予想しています。減少とみているのは15%だけです。

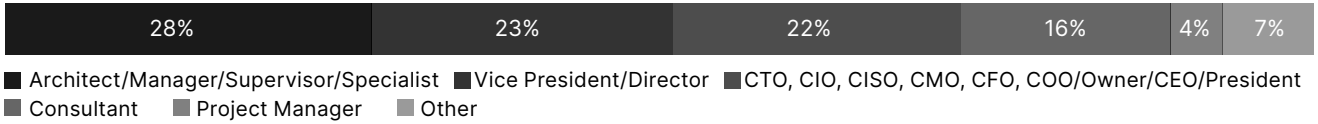
今後 18 か月間で、貴社のアクセス管理関連の予算はどう変化すると予想されますか?



調査方法と回答者の属性

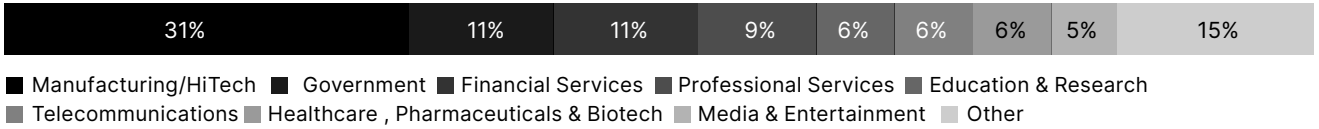
この調査報告書は、米国の413人のITとサイバーセキュリティの専門家を対象としたオンラインアンケートの結果をまとめたものです。ゼロトラストセキュリティに関する最新の企業での導入動向、課題、ギャップ、解決策の特定を目的として2020年1月に実施されました。回答者は技術部門の重役からITセキュリティの実務者まで多岐にわたり、多様な業界のあらゆる規模の企業・組織に在籍しています。

Career Level



Company Size

Industry



ivanti

ivanti.co.jp
03-5226-5960
contact@ivanti.co.jp

Ivanti は、ユーザー、デバイス、モノ、サービス間の可視化と簡単で安全に保護された接続であるソフトウェア型セキュア・アクセス・ソリューションを提供するベンダーです。当社は、ハイブリッドなIT向けのクラウドやモバイル・アプリケーションとネットワークアクセス制御を統合したスイート製品を提供しています。あらゆる業界の23,000社以上の企業とサービスプロバイダーがIvantiを活用しており、モバイルワーカーにビジネスのコンプライアンスを確保しながらデータセンターやクラウドのアプリケーションや情報への安全なアクセスを提供しています。詳細については ivanti.co.jp をご ください。

1 リソースの分離 44% |内部ネットワークと外部ネットワークの信頼関係なし 39% |その他 2%

2 監査やセキュリティインシデントへの対応 37% |業務効率 33% |ハイブリッド IT セキュリティの問題への対処 31% |その他 4%

3 手動プロセスは複雑で、迅速に対応できない 37% |その他 2%

4 SD-WANセキュリティ機 の強化 28% | 完するエンドポイントの検出/応答 (EDR) 27% |既存のリモート アクセス ツール (VDI、VPN、RDP など) の 強、 せ替え 24% |その他 5% |なし 2%

5 SSL 検証 40% | セキュアなSD-WAN 27% | 簡素化 26% | 既存のリモートアクセスセキュリティ技術の載せ替え (VPNなど) 25% | EDR 20% | なし 2% | その他 8%

6 Aクラウドアクセスセキュリティブローカー (CASB) 33% | エンタープライズモバイル管理 (MDM) 31% | ソフトウェア定義の境界 (SDP) 28% | アイデンティティ分析 24% | エンタープライズディレクトリサービス 17% | その他 2%