調査レポート

2021

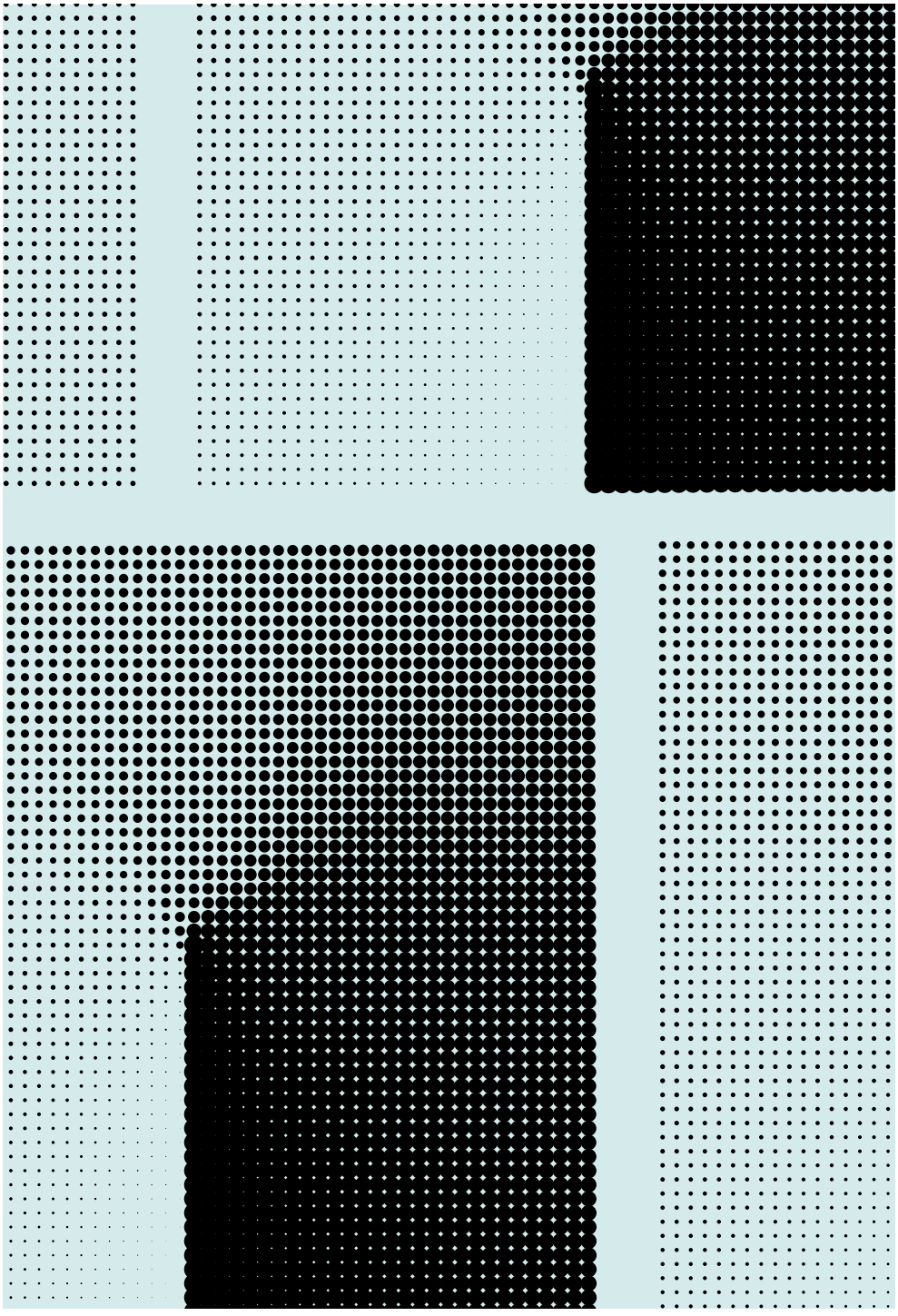
アイデンティティを中心としたゼロトラスト導入実態調査「The State of Zero Trust Security 2021」

グローバル組織におけるアイデンティとアクセス管理の成熟度

Okta Inc.

Okta.com

press@okta.com



okta

目次

はじめに

近年、「ゼロトラスト」はバズワードの域を脱し、現代の情報セキュリティの中で確固たる地位を築いています。いくつかの市場要因により、ゼロトラストセキュリティの取り組みがより注目されています。昨年、リモートワークの範囲、規模、認識がそれぞれ大きく変化しました。パンデミックが終わったとしても従業員が少なくとも一部の時間、リモートで働くことを許可したり、企業によってはフルタイムでの在宅勤務を恒久的に許可するところもあるでしょう。

その一方で、昨年はアイデンティティを起因とする攻撃が急増しました[1]。ウェブアプリケーションへの侵入の約90%は認証情報の不正使用が原因で、フィッシングはそれらの侵入の3分の1以上を占め、昨年の25%より増加しています。また、データ侵害の61%が認証情報データへのアクセスに関係しています[2]。

モバイルやクラウドの導入が急速に進む中、顧客や従業員、企業の安全性を高めるために、テクノロジーやセキュリティのリーダーたちの大半は、従来のセキュリティアプローチを改めました。「信頼できる」内部ネットワークと「信頼できない」外部ネットワークという境界線を作るのではなく、業界アナリストや政府機関が強く推奨（場合によっては義務化）しているゼロトラストフレームワークを採用しています。

現在のデジタル社会では、アイデンティティが新たな境界線となっています。今日のユーザーのアクセスと使い勝手に対する要求を満たし、データ漏洩やサプライチェーン攻撃の次の犠牲者にならないために、企業は「信頼せず、常に検証する」というゼロトラストの原則を中心とした、より強固で包括的なセキュリティ態勢に移行しつつあります。そのためには、ユーザーに負担をかけずにアクセス権限を継続的に評価する必要があります。

しかし、どのような組織でも、一夜にしてゼロトラストを実現することはできません。そのためには、場所、デバイス、ネットワークに関係なく、さまざまなタイプのユーザーを保護するためのアイデンティティ中心の考え方でゼロトラストに取り組んでいくことが、最も良い出発点となるでしょう。

これらの状況をふまえて、世界中の組織が現在どのようにゼロトラストに取り組んでいるのか、また今後18ヶ月の間にどこへ向かおうとしているのかを知るために、Oktaは、日本を含む700人のセキュリティ意思決定者（日本100人、APAC300人、EMEA100人、北米100人、グローバル2000企業100人）を対象に調査を実施しました。

[1] Federal Trade Commission, "**Consumer Sentinel Network Data Book**," February 2021
[2] Verizon, "**2021年データ漏洩/侵害調査報告書**," 2021年6月

ゼロトラストセキュリティに関する４つのポイント

1. パンデミックの影響で、ゼロトラストの優先順位が高まっています。

ゼロトラストの取り組みを実施しているか聞いたところ、すでに実施しているところを含めて今後18ヶ月の間で全世界の7割から9割以上がゼロトラストの取り組みを実施すると回答しています。また、新型コロナウイルスにともなうリモートワークの拡大によって、世界全体で約8割近くが、ゼロトラストの優先順位が高まったと回答しています。

2. アイデンティティが新たな境界線です。

ゼロトラストでの優先事項をランク付けするよう求めたところ、第1優先事項が「人」、次いで「デバイス」と「データ」となりました。先進的な企業は、従業員、顧客、パートナー、請負業者、サプライヤーのリソース全体で強力な認証を採用し、従来のネットワークベースから、よりユーザーベースやデバイスベースのアクセス制御に移行しています。

3. アイデンティティ中心のゼロトラスト導入が急速に進んでいます。

今年、企業はアイデンティティとアクセス管理（Identity and Access Management = IAM）の成熟に向けた取り組みを加速させ、来年末までに飛躍的な進歩を遂げることを計画しています。Oktaが推奨するアイデンティティの成熟度曲線（ステージ0〜3）[3]における全てのゼロトラストプロジェクトの採用率は、2023年までに少なくとも日本では10%、その他の国では25%になるでしょう。この数値は、フォーブスのグローバル2000企業では40%近くに跳ね上がります。

4. 企業はIAMの成熟度が高いステージのプロジェクトを強化しています。

IT部門とセキュリティ部門のリーダーたちは、即効性のあるプロジェクトだけではなく、今後18ヶ月の間に優先的に取り組むべきゼロトラストプロジェクトとして、IAMの成熟度が高いステージのプロジェクトを挙げる企業が最も多くなっています。例えば、コンテキストベースのアクセスポリシー、従業員のプロビジョニングとデプロビジョニングの自動化、パスワードレスアクセスの導入を優先しています。

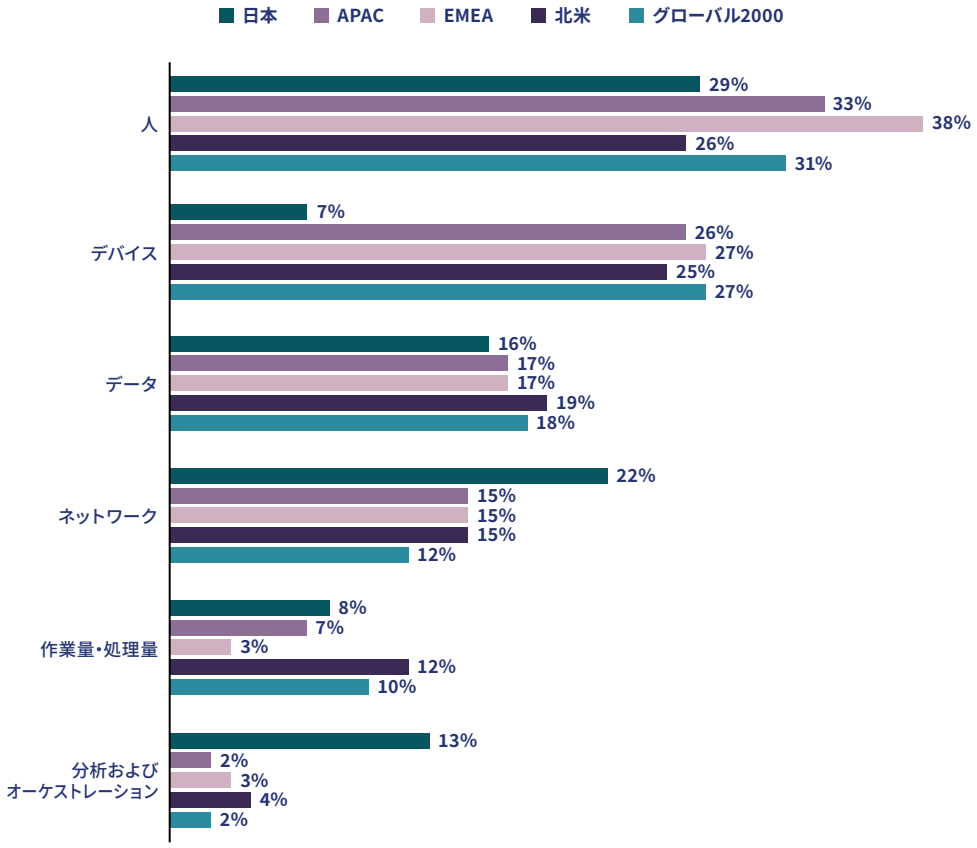
[3] アイデンティティ管理とゼロトラスト：**アセスメントツール**

アイデンティティ：ゼロトラストの基盤

アイデンティティが企業の新たな境界線となることで、IAMは、ユーザー、デバイス、データ、ネットワークの中央の管理ポイントとなります。実際、ガートナー社は最近、「アイデンティティ・ファーストのセキュリティ」を、今年のセキュリティとリスクのトップ・トレンドの1つとして挙げています[4] 。アイデンティティ・ファーストは、どのユーザーがどのリソースにアクセスできるかを可視化および制御し、認証情報の漏洩や誤ったプロビジョニング、認証などのリスクを最小限に抑えることができます。

ゼロトラストを実施する上で重要な要素のランキングについて尋ねたところ、最も重視しているのが「人」、次いで「デバイス」と「データ」でした。従業員、顧客、パートナー、請負業者、サプライヤーなどの人を重視し、従来のネットワークベースから、人やデバイス、データを重視する方向に移行しています。日本では、「ネットワーク」を重視する割合が他国より高い一方で、「デバイス」を重視する割合が極めて低い結果でした。

あなたの組織において、ゼロトラストを実施する上で求められる重要な要素は何だと思いますか？

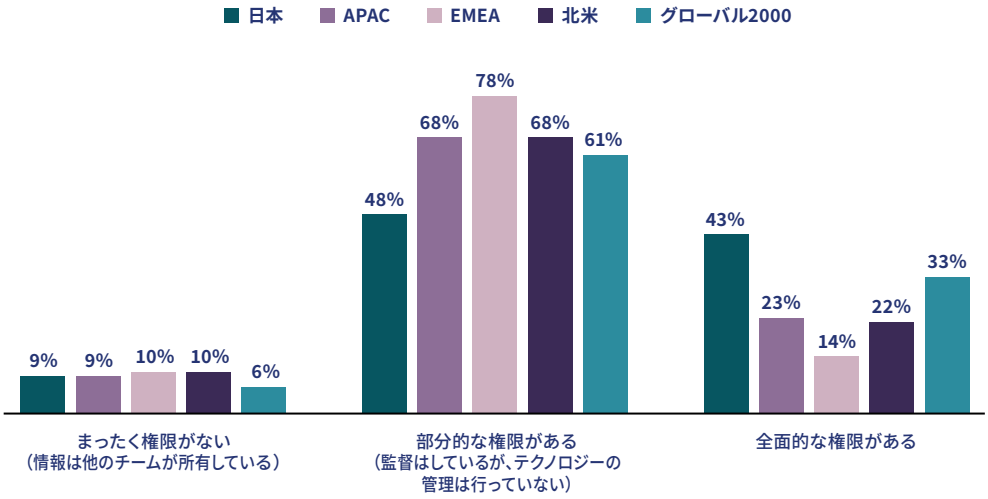


[4] Gartner, "**2021年のセキュリティとリスクのトップ・トレンド**" 2021年6月11日

アイデンティティを中心としたセキュリティへの変遷

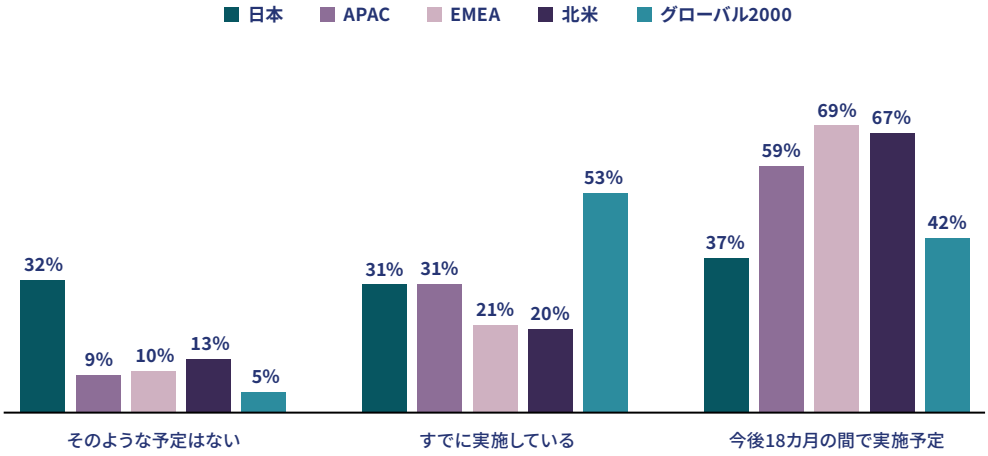
アイデンティティとセキュリティがいかに密接に関係しているかを考えると、ゼロトラスト戦略では、IAMに関してITチームとセキュリティチームが緊密に連携することが効果的です。今回の調査によると、セキュリティチームが部分的にIAMを監督している割合が5割から8割を占め、セキュリティチームが全面的にIAMを所有している割合が最も高いのは日本（43%）、次いでグローバル2000企業（33%）でした。

あなたの組織では、セキュリティ部門がどの程度まで
アイデンティティ情報を所有し、アクセスすることができますか？



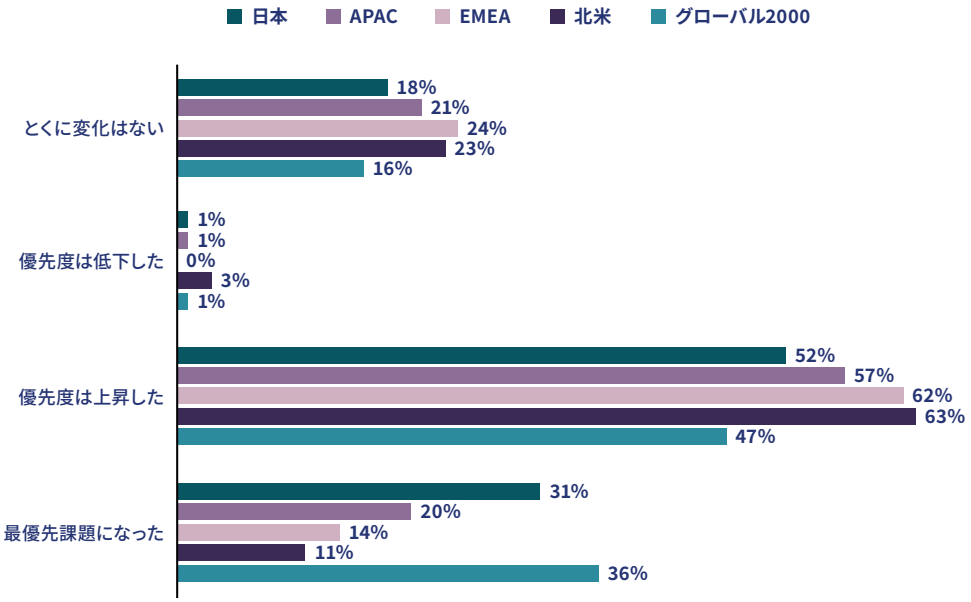
ゼロトラストに基づくセキュリティの取り組みを実施しているかを尋ねたところ、グローバル2000企業は、強固なセキュリティ体制の構築をリードしており、回答者の53%がすでにゼロトラストセキュリティの取り組みを導入しており、さらに42%が今後18ヶ月の間に導入を計画しています。ただ、日本企業の回答を見ると、ゼロトラストの取り組みの予定がないと回答した割合が他国より高い結果でした。

あなたの組織では現在、ゼロトラストに基づくセキュリティの取り組みが実施されていますか？
そうした取り組みを今後18カ月の間に実施する予定はありますか？



パンデミックが組織のゼロトラストへの動きを加速させ、ゼロトラストに向けてより多くの予算が割り当てられたことが明らかになりました。世界全体では、ゼロトラストに取り組んでいる組織のうち、約80%の企業が、新型コロナウイルスにともなうリモートワークの拡大によって、組織におけるゼロトラストの優先度が高くなった、もしくは最優先事項になったと回答しています。日本ではゼロトラストが最優先課題になったと回答した割合が他国より高くなっています。

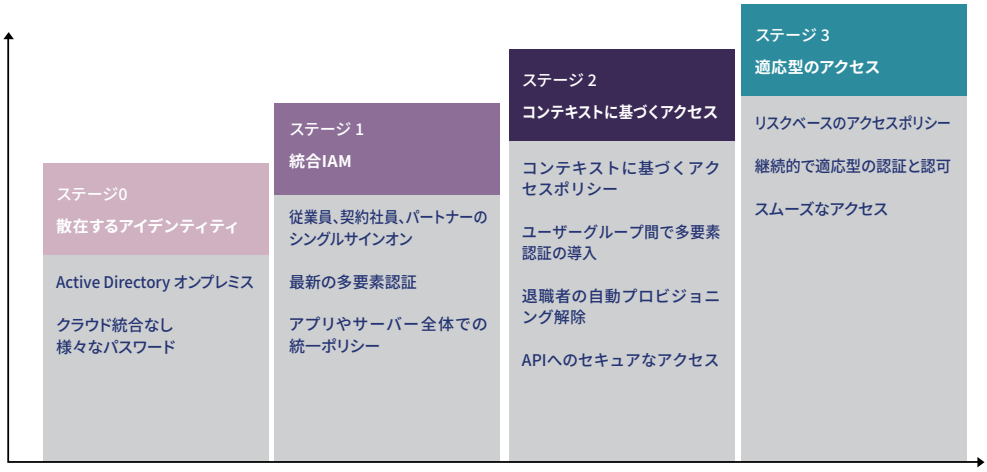
新型コロナウイルスにともなうリモートワークの拡大によって、
組織におけるゼロトラストの優先度は高まりましたか？



ゼロトラスト成熟度の進化：2021年

これまで企業がゼロトラストについてマクロレベルでどのように考えているかを確認してきました。ここから、Oktaが推奨するIAM成熟度曲線を通して、企業が実際に進めている具体的なゼロトラストプロジェクトの状況をいくつか探ります。組織がアイデンティティ中心のセキュリティ対策に基づくゼロトラストアーキテクチャの導入に取り組む際には、大まかに4つの主要な成熟度の段階をたどることが分かっています。なお、Oktaでは各企業のゼロトラスト成熟度を評価するためのアセスメントツールを公開[5] しています。

アイデンティティとアクセスの成熟度



ゼロトラストプロジェクトは、組織が管理するリソースの種類から、ユーザーのプロビジョニングとデプロビジョニングの方法、どの認証方法を導入するかなど、あらゆるものに及びます。アイデンティティに対するアプローチが断片的な企業は、まだゼロトラストへの取り組みを歩み始めているとは言えません。ステージ0の段階では、クラウド技術を採用し始めているかもしれませんが、それらのソリューションをIAMプラットフォームやオンプレミスのリソースと統合するまでには至っていません。

ステージ1では、統合されたIAMエコシステムを導入し、従業員が重要なリソースにアクセスする際のシングルサインオン（SSO）や多要素認証（MFA）を実装することで、安全でないパスワードに依存した状態を改善します。

ステージ2に移行すると、企業はアクセス制御をAPIなどの他のリソースにまで拡大したり、や多様な要素を用いて認証の判断をより適切に行うなど、さらなるセキュリティのベストプラクティスを採用します。

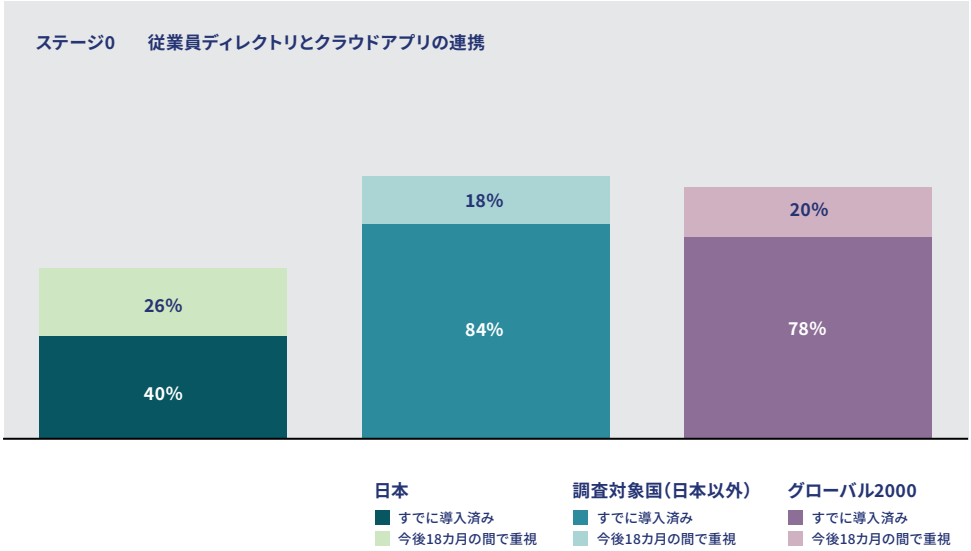
ステージ3に到達した企業は、パスワードレスソリューションや継続的なアクセスソリューションなど、ゼロトラストに向けた完全なリスクベースの認証アプローチを採用することに成功したことになります。

[5] アイデンティティ管理とゼロトラスト：**アセスメントツール**

ステージ0：散在するアイデンティティ

従業員ディレクトリ（従業員情報）とクラウドアプリの連携の導入状況について質問したところ、すでに連携していると回答した割合が、日本で40%であるのに対して、それ以外の国では約80%がすでに連携済みと回答しており、日本での取り組みが大分遅れています。

現時点であなたの組織で導入済みの取り組みはありますか？
今後18カ月の間でどの取り組みを重視しますか？



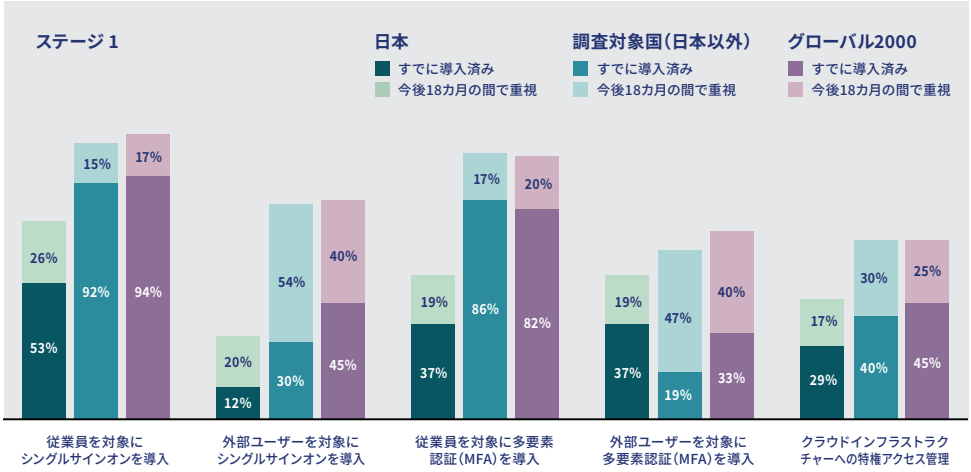
ステージ1：統合IAM

統合IAMの進捗状況を評価するために、従業員や外部ユーザーにSSOを導入しているか、MFAを導入しているか、クラウドインフラストラクチャへの特権的なアクセスを管理しているかを尋ねました。ステージ 1 の企業は、認証メカニズムに複数のセキュリティレイヤーを追加することで、適切な人が適切なリソースに最小限の負担でアクセスできるようにする効果的な方法を見つけています。

現在、ステージ1の5つのプロジェクトの1つである「従業員を対象にしたシングルサインオンの導入」状況において、すでに導入済みと回答したのが日本で53%であるのに対し、日本以外の調査対象国やグローバル2000企業では90%以上がすでに導入済みと回答しています。また、「従業員を対象にしたMFAの導入」においても、すでに導入していると回答した割合が日本で37%であるのに対し、日本以外の国やグローバル2000企業では80%以上で導入が完了しており、日本での取り組みが遅れていることが顕著になりました。

その他、パートナー、請負業者、サプライヤーなどの外部ユーザーを対象にした3つのプロジェクトにおいても、現在を含めて今後18カ月の間に導入される割合を見ると日本での取り組みが遅れていることが明らかになりました。「外部ユーザーを対象にしたシングルサインオンの導入」が日本で32%であるのに対し、日本以外の調査対象国で84%、グローバル2000企業で85%、「外部ユーザーを対象にしたMFAの導入」が日本で56%、日本以外の調査対象国で66%、グローバル2000企業で73%、「クラウドインフラストラクチャーへの特権アクセス管理の導入」においては日本で46%、日本以外の調査対象国で70%、グローバル2000企業で70%でした。

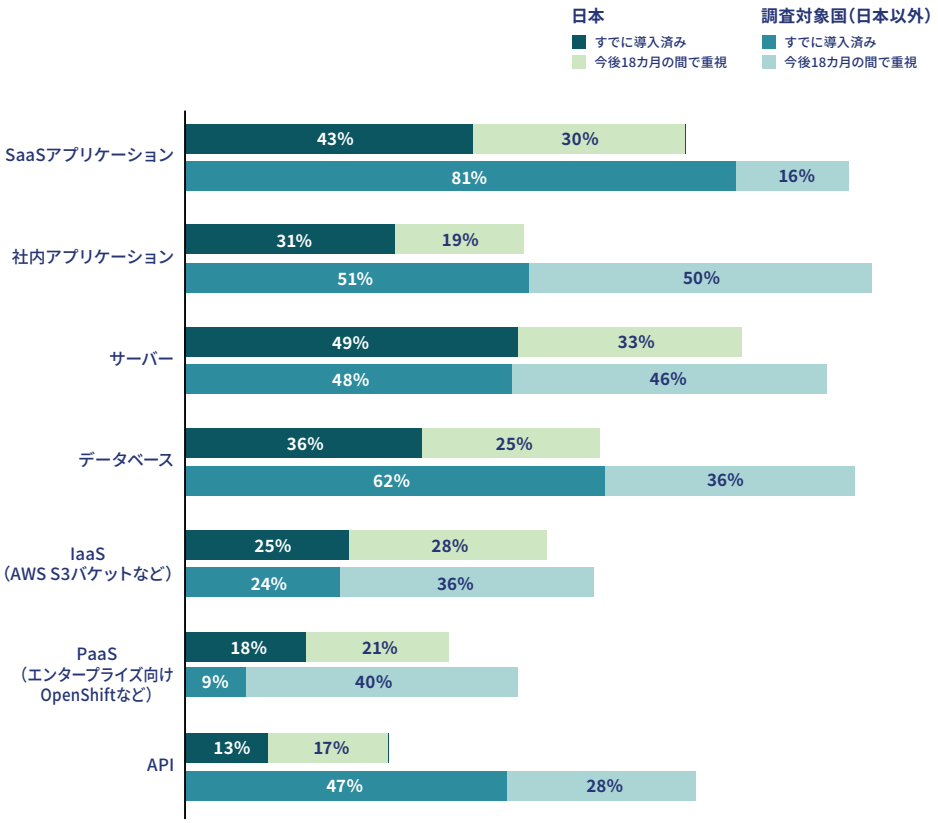
現時点であなたの組織で導入済みの取り組みはありますか？
今後18カ月の間でどの取り組みを重視しますか？



SSOとMFAをアプリケーションやサーバに対して統合されたアクセスポリシーを作成するという点では、リソースの種類によって導入状況が異なります。日本を除く世界の調査対象国の81%の企業がSSOとMFAをSaaSアプリケーションに適用していることから、その他のリソース、つまり社内のアプリケーション、サーバ、データベース、APIにもこれらの保護機能を追加し始めています。

また、IaaSとPaaSは現在の焦点ではありませんが、今後18カ月の間に、この2つのリソースタイプを優先的に使用することを計画している企業が増えています。

シングルサインオン（SSO）や多要素認証（MFA）を導入済みのリソースはありますか？
今後18ヶ月の間でそれらの導入を検討しているリソースはありますか？



ステージ 2: コンテキストベースのアクセス

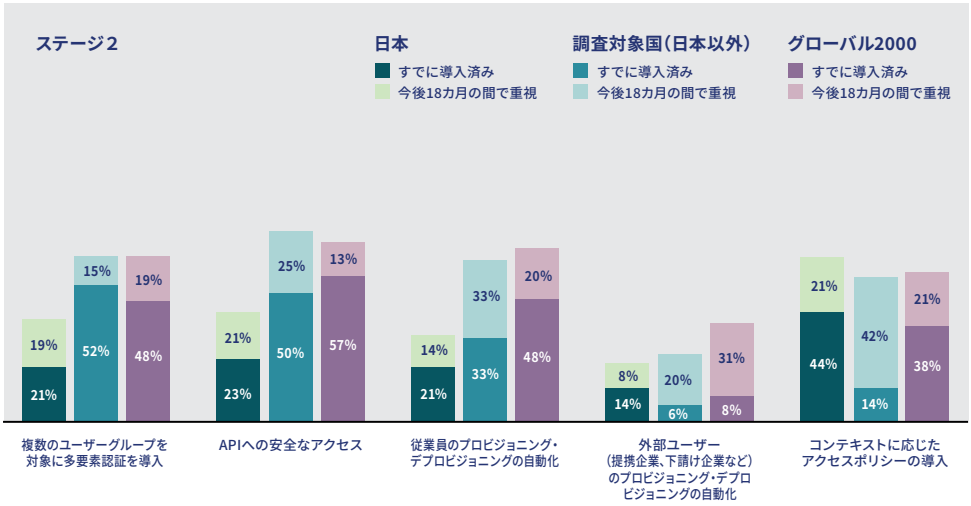
ステージ2を評価するために、回答者には、ユーザーグループ間での多要素認証、APIへのセキュアなアクセス、従業員や外部ユーザーに対するアカウントの自動プロビジョニングとデプロビジョニング、コンテキストベースのアクセスポリシーなどを導入しているかどうかを尋ねました。

世界各国の企業は、今後18カ月の間にステージ2の各プロジェクトを進めていく予定で、18ヶ月後の導入率は22%～75%となります。これらの5つのプロジェクトのうち4つが18ヶ月後に半数以上の企業に導入される予定です。これらのプロジェクトのうち、「APIへの安全なアクセス」と「従業員のプロビジョニング・デプロビジョニングの自動化」の導入率が、日本以外の調査対象国で70%を超えると予想されます。

APIへの安全なアクセスを導入する企業が増加しています。デジタルビジネスモデルの進化に伴い、企業は外部のサプライチェーン、新たなデータソース、サードパーティのテクノロジーシステムとのシームレスな接続を必要としているため、APIの安全なアクセスに注目が集まるのは当然のことです。このようなデジタルでつながった環境では、APIのセキュリティは必須のものとなります。

外部ユーザーに対するプロビジョニング・デプロビジョニングの自動化が最も取り組みが遅れている分野です。外部ユーザーのプロビジョニング・デプロビジョニングによってセキュリティ態勢を改善する機会を認識している企業はまだ少なく、パートナーや契約社員が会社を辞めた後も重要なリソースへのアクセスを許可してしまうリスクを抑えることができます。

現時点であなたの組織で導入済みの取り組みはありますか？
今後18カ月の間でどの取り組みを重視しますか？



セキュリティ要素

ユーザーグループごとに多要素認証をすでに導入していると回答したのが日本で21%、日本以外の調査対象国で52%、グローバル2000企業で48%であることから、組織が最も使用しているセキュリティ要素を調べました。

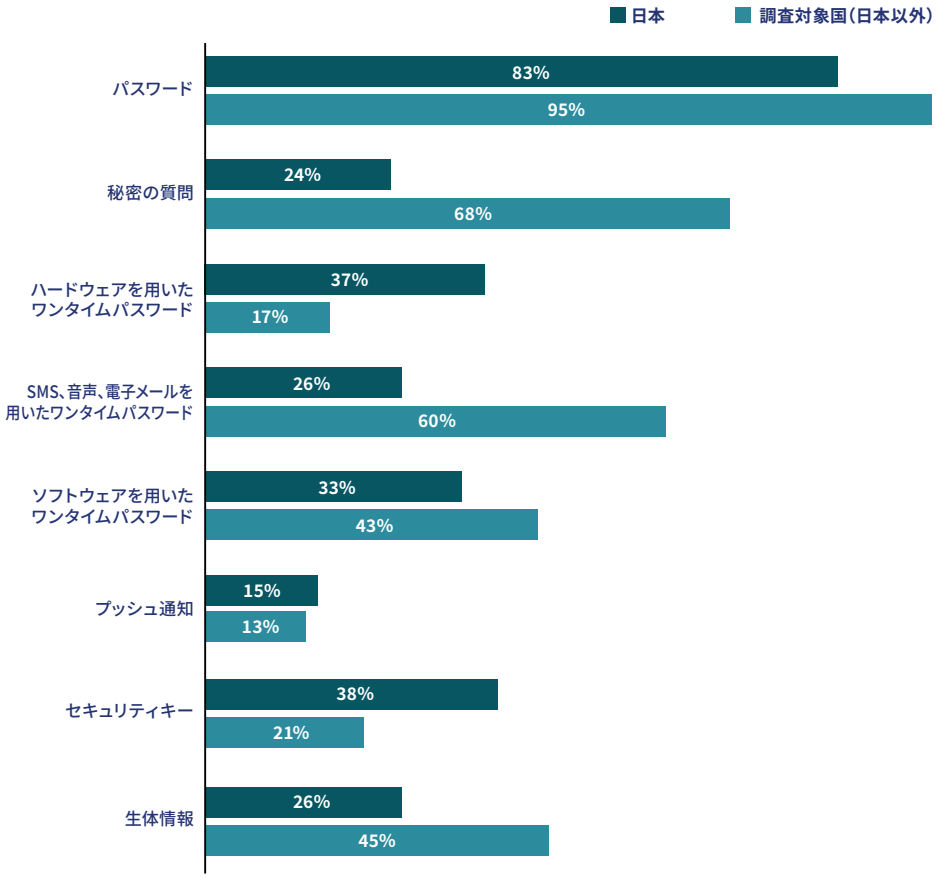
印象的だったのは、日本では主にパスワードの要素が最も多いですが、その他の調査対象国では、パスワード、秘密の質問、生体認証、SMS・音声・電子メールを用いたワンタイムパスワードの要素の割合が多いことです。

高いレベルの安全性を求める組織は、米国国立標準技術研究所（National Institute of Standards and Technology）のデジタル・アイデンティティ・ガイドライン（Digital Identity Guidelines） [6] を参考にすべきです。

Okta の顧客の間では、プッシュ通知のような安全性の高い要素が、安全性の低い二要素認証に比べて増加していることがわかっています。昨年、Okta のお客様は、SMS やセキュリティ質問への依存度を下げ、より安全性の高い要素に依存するようになりました。パンデミック前の6ヶ月間では、Oktaの多要素認証スマホアプリ「Okta Verify」の利用は28%増加し、2020年2月から10月までででは184%も急増しました。

[6] NIST, “**Digital Identity Guidelines**” March 2, 2020

あなたの組織で使用しているセキュリティ要素は？

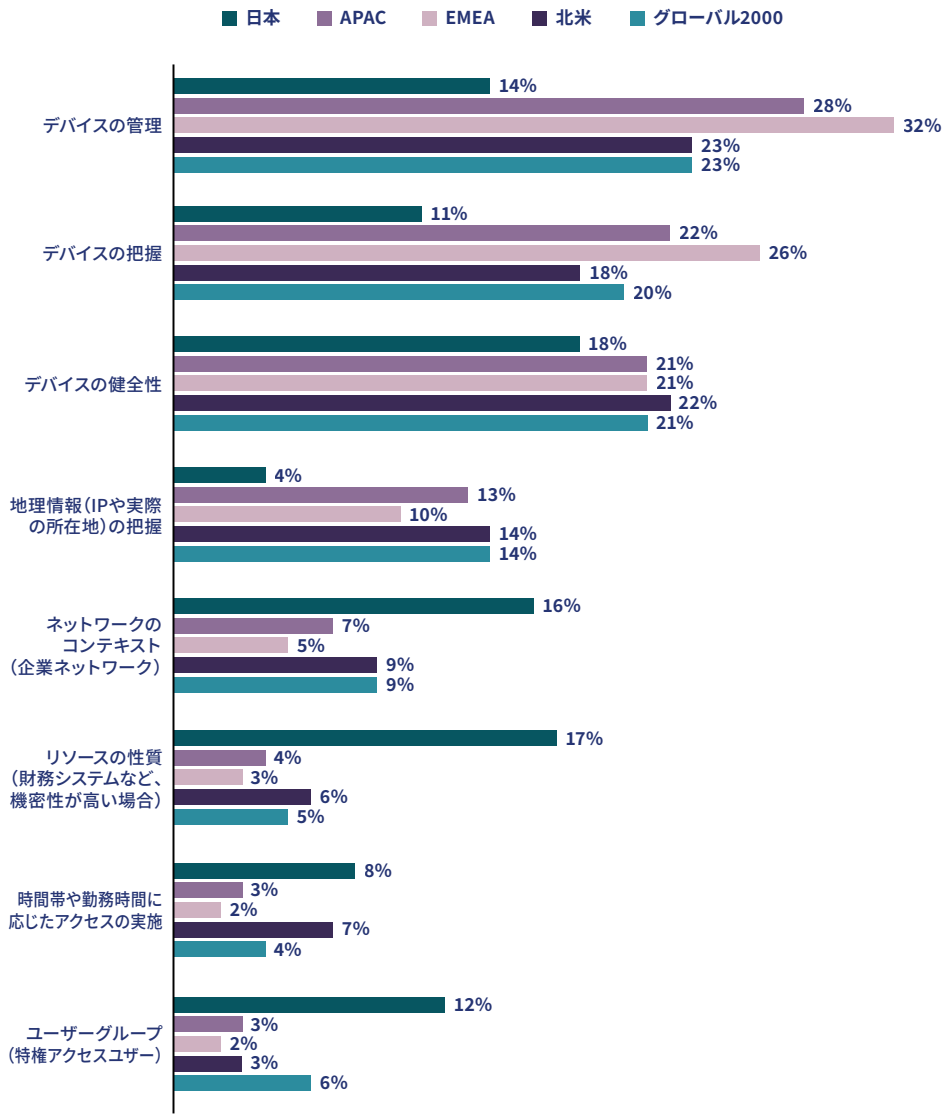


アクセスポリシー

ゼロトラスト戦略のもう一つの鍵は、人々が適切なコンテキストで適切なレベルのアクセスを得られるようにすることです。これには、ユーザーのデバイス、ネットワーク、場所、またはアクセスしようとしているアプリケーションをより適切に評価できるアクセスポリシーの設定が含まれます。日本ですでに導入している割合が44%で世界で最も高い割合でした。他国でも今後18ヶ月で重視すると回答した割合が42%であり、回答者が明らかに注力している分野の1つです。

また、回答者は、ゼロトラストのベストプラクティスに沿って、アクセスの承認で使用するより重要な要素は、ユーザーのデバイスが管理されているか、識別されているか、健全であることが確認されているかなど、デバイスの状態に関連するものであると述べています。社内リソースへのアクセスを承認する際に最も重要な要素は、ユーザーのデバイスが管理されているかどうかを確認することです。日本では、デバイスの管理や把握を重視する割合が低く、ネットワークのコンテキストやリソースの性質を重視しています。

組織の内部リソースへのアクセスを管理・承認するにあたり、最も重要だと思う要素は？



パンデミックが発生する前には、このような状況に依存していたと思われますが、2020年のロックダウン開始時には、多くのITスタッフが、利用可能なデバイスを使って従業員を有効にすることを急がなければなりませんでした。このような状況では、多くの企業が次善の策として「デバイスがわかっている」ということを選択したと考えられます。現在では、これらの既知のデバイスが検証され、健全であるかどうかに注目している企業が増えています。これは、ゼロトラストを実現するための2つの重要な要素です。

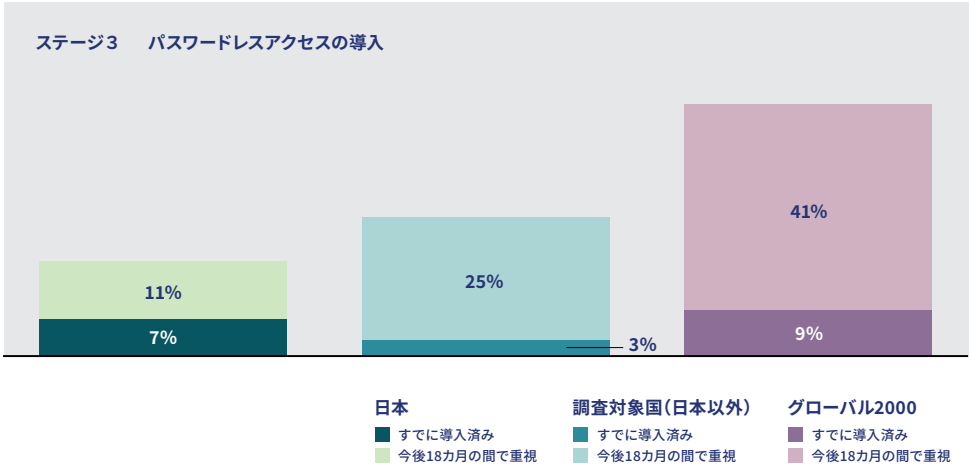
ステージ3：適応型のアクセス

ステージ 0〜2で説明した中核的なゼロトラストプロジェクトに加えて、組織が柔軟性を高める方法の1つとして、安全性の高い要素を使用したパスワードレスのアクセスがあります。パスワード使用において、重複したパスワードを使用する割合が多いことから 、クレデンシャルハーベスティングが今日の攻撃者にとって最も有益な戦術となる傾向があります。データ漏洩の 60%以上は、盗まれた、または脆弱な認証情報に起因するものであり[7] 、ユーザ情報の漏洩を防ぐ最善の方法は、継続的な安全確認によって認証を確保することです。

パスワードだけに頼っていると、組織はパスワードスプレー攻撃やクレデンシャルスタッフィング攻撃に対して脆弱になります。WebAuthnやU2Fセキュリティキーによる生体認証ベースのログインなど、安全性の高い要素や複数の要素の組み合わせを使用することで、これらのリスクを軽減することができ、パスワードが必要ないシナリオでは、パスワードレス認証に柔軟に対応することができます。これは、アカウントの乗っ取りを防ぐ上で大きな助けとなるため、パスワードレスの導入が活発化することは期待できます。

調査対象国でパスワードレスアクセスを現在導入している割合は少ないですが、今後18ヶ月後には18%から50%が導入すると回答しています。グローバル2000企業のうち、現在パスワードレスアクセスを導入している企業は9%、今後18ヶ月で導入を予定している企業は41%です。日本では、それぞれ7%と11%になると回答しています。

現時点であなたの組織で導入済みの取り組みはありますか？
今後18カ月の間でどの取り組みを重視しますか？



[7] Verizon, "**2021年データ漏洩/侵害調査報告書**," 2021年6月

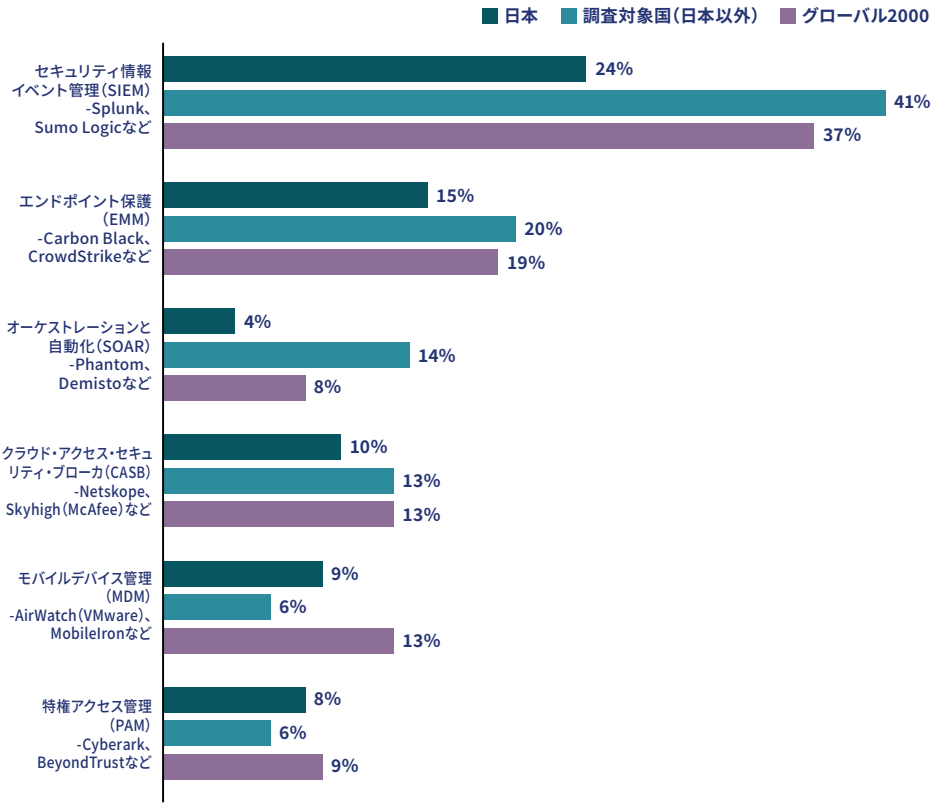
ベストインクラスのゼロトラストエコシステム

ForresterやNISTなどが推進しているゼロトラストの推奨事項をすべて自動化するソリューションはありません。どの業界においても、重要なベストプラクティスは、セキュリティスタック全体の基盤技術としてアイデンティティを活用することです。

セキュリティ情報イベント管理（SIEM）、セキュリティオーケストレーションオートメーションと応答（SOAR）、エンドポイントプロテクション（EMM）、モバイルデバイス管理（MDM）、クラウドアクセスセキュリティブローカー（CASB）、特権アクセス管理（PAM）など、セキュリティアーキテクチャ全体をIAMソリューションで統合することで、ゼロトラスト防衛のための全体的かつ詳細なアプローチを確立することができます。

これを踏まえて、セキュリティ担当者に、ゼロトラストのセキュリティ運用を行うために、どのツールをIAMシステムと統合することが最も重要だと思うかを尋ねたところ、大多数の企業が、SIEMと回答し、次に重視しているのがEMMとの回答でした。

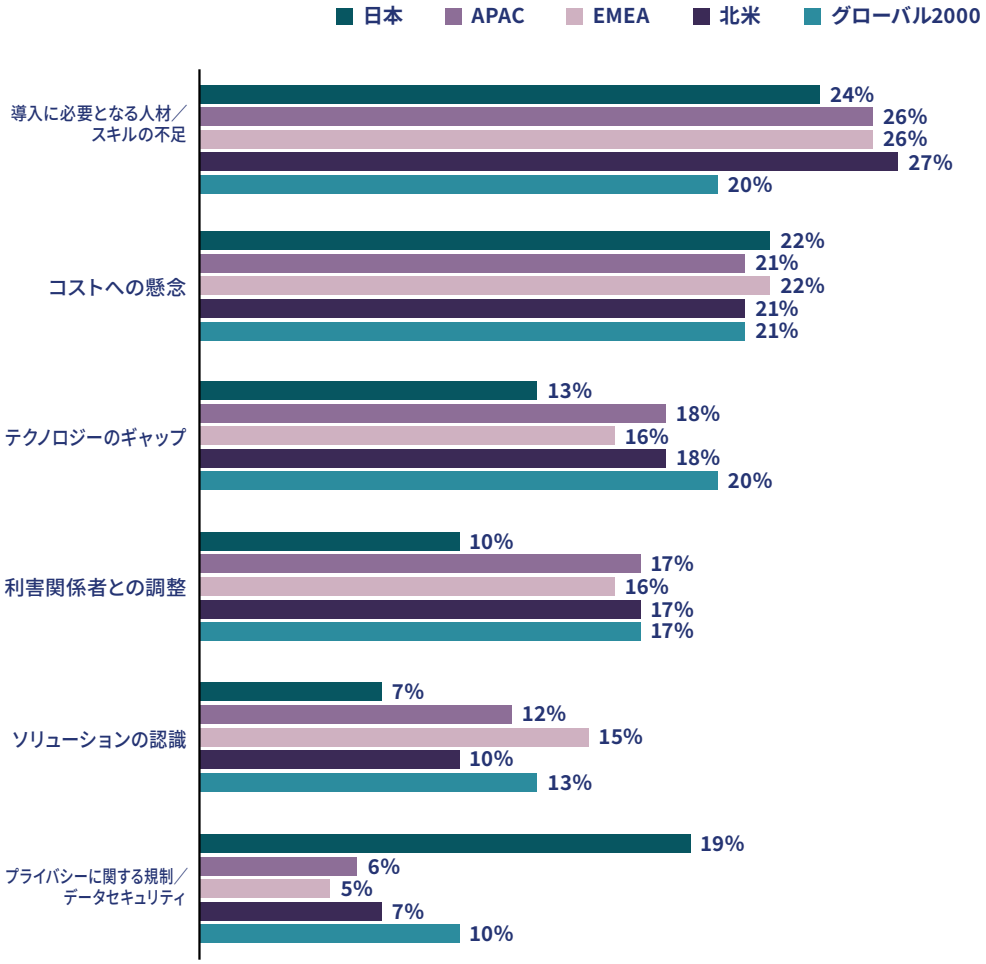
ゼロトラストのセキュリティ運用を行うためには、
どれをIAMソリューションと統合することが最も重要だと思いますか。



ゼロトラストの次のステップ

昨年来、世界中の企業がゼロトラスト戦略を大きく進展させていますが、今後も多くの機会と課題が待ち受けています。ゼロトラストモデルを導入するのにあたって、世界各国で導入に必要となる人材/スキルの不足が課題となっています。日本で顕著なのは、プライバシーに関する規制やデータセキュリティを課題と考える回答者が他国よりも多いことです。

ゼロトラストモデルを導入するにあたって、
あなたの組織ではどのような課題に直面していますか?



ゼロトラストセキュリティプロジェクトへの予算の増加、より洗練されたセキュリティ対策に向けた業界の機運、さらには最近の政府による義務化などが、組織がゼロトラスト導入を進めていく上での支えとなっています。

主な教訓

ゼロトラストの導入には、特効薬はありません。このタスクに最大のリソースを投入できる企業でも、一夜にして完全な成熟を達成することはできません。しかし、今日の経済のデジタル化は、セキュリティへの脅威がますます強まることを意味しており、どの企業も立ち止まっているわけにはいきません。ゼロトラスト戦略を加速させるためには、アイデンティティ中心のセキュリティを導入する方法がいくつかあります。

ゼロトラストセキュリティ体制を成熟させるための重要なステップ

- 人が新たな境界線であることを認識し、オンプレミス、クラウド、モバイル、そして従業員、顧客、パートナー、請負業者、サプライヤーなどが、あらゆる場所で利用するあらゆるサービスに強力な認証を導入する。

- 企業全体のアイデンティティとアクセス制御を一元化することで、リスク管理をより容易にする。

- IAMの成熟度曲線を確認し、自社がどの程度のレベルにあるのかを判断し、ゼロトラストに向けたアイデンティティ・ファーストのアプローチにより、自社の地位を迅速に向上させるための即効性のある方法を見つけることで、リスクを低減する。

- 主要なツールをIAMソリューションと統合することで、セキュリティエコシステムを拡張し、組織全体のセキュリティの可視化とコラボレーションが可能にする。

- パスワードレス認証やコンテキストベースのアクセスポリシーの採用、従業員アカウントの保護からパートナーアカウントのアクセス保護への移行など、時間をかけてセキュリティをさらに向上させていく、より高度なプロジェクトを計画する。

組織がセキュリティ向上のためのステップを進めていく際に、この作業を同業他社と比較することは非常に有益です。Oktaが公開しているアイデンティティ管理とゼロトラストのアセスメントツール [8] では、ゼロトラストのアイデンティティとアクセス制御を導入するためのロードマップを確認することができます。上記のIAM成熟度曲線に基づき、自社がどこまで達成しているのか、今後どのような対策が必要なのかについて知ることができます。さらに、他の組織が実装のプロセスを通じて得たノウハウや、どのようなエコシステムと連携することでゼロトラストをさらに強化できるかについての提言も得ることができます。

[8] アイデンティティ管理とゼロトラスト：**アセスメントツール**

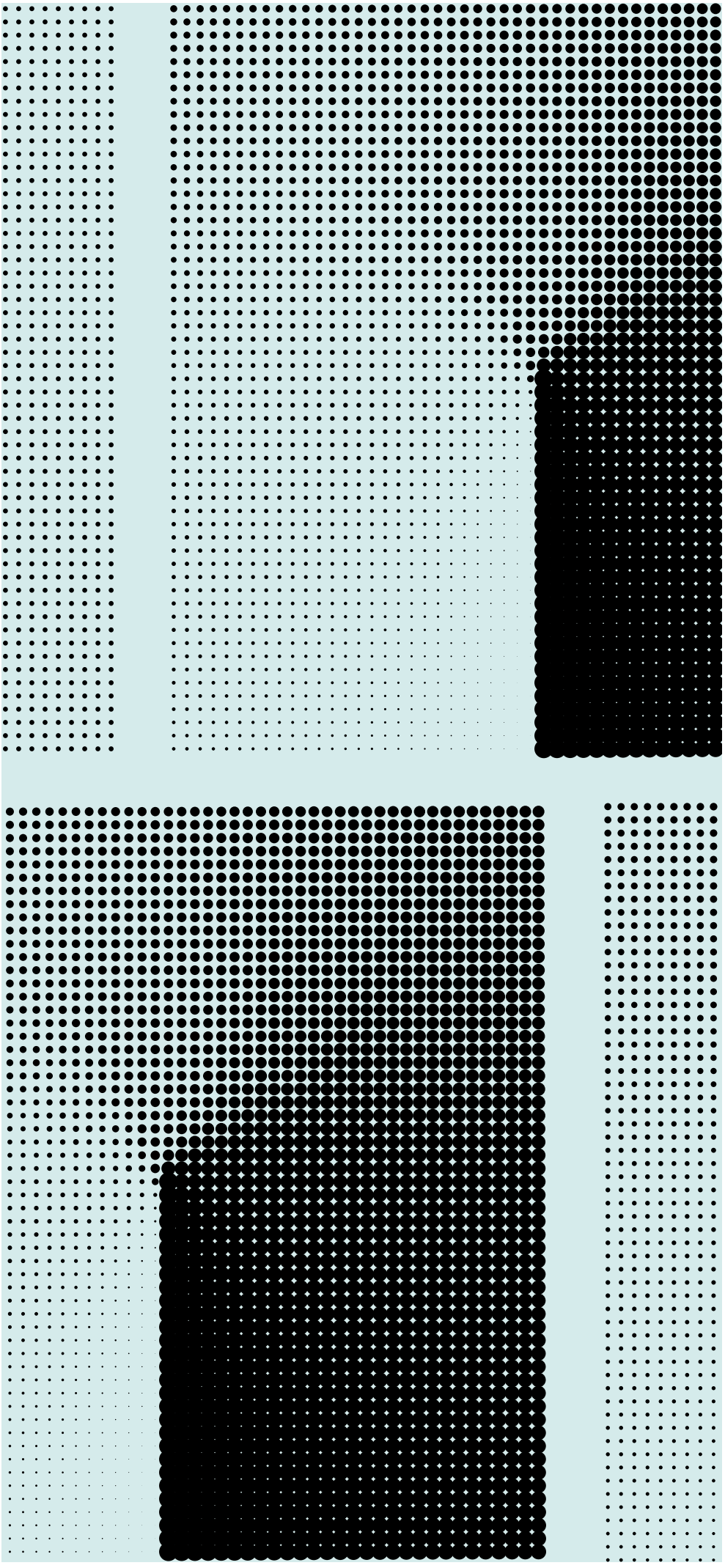
調査方法について

本調査は、OktaがPulse Q&Aと楽天インサイトに委託をして、700人のセキュリティ意思決定者を対象にオンラインで実施しました。Pulse Q&Aが日本以外のグローバル企業のセキュリティ意思決定者600人を対象に実施し、楽天インサイトが日本国内のセキュリティ意思決定者100人を対象に調査を実施しました。700人の回答者の内訳は、日本100人、APAC300人、EMEA100人、北米100人、グローバル2000企業100人となります。調査実施期間は、2021年の3月から5月。

Oktaについて

Oktaは、すべての人のアイデンティティとアクセスを安全に管理するベンダーニュートラルなサービスプロバイダーです。Oktaが提供するプラットフォーム「Okta Identity Cloud」により、クラウド、オンプレミスを問わず、適切な人に適切なテクノロジーを適切なタイミングで安全に利用できるようにします。7,100以上のアプリケーションとの事前連携が完了している「Okta Integration Network」を活用して、あらゆる人や組織にシンプルかつ安全なアクセスを提供し、お客様の潜在能力を最大限発揮できるように支援します。JetBlue、Nordstrom、Siemens、Slack、T-Mobile、Takeda、Teach for America、Twilioを含む10,000以上のお客様がOktaを活用して、職場や顧客のアイデンティティを保護しています。

https://www.okta.com/jp/



okta