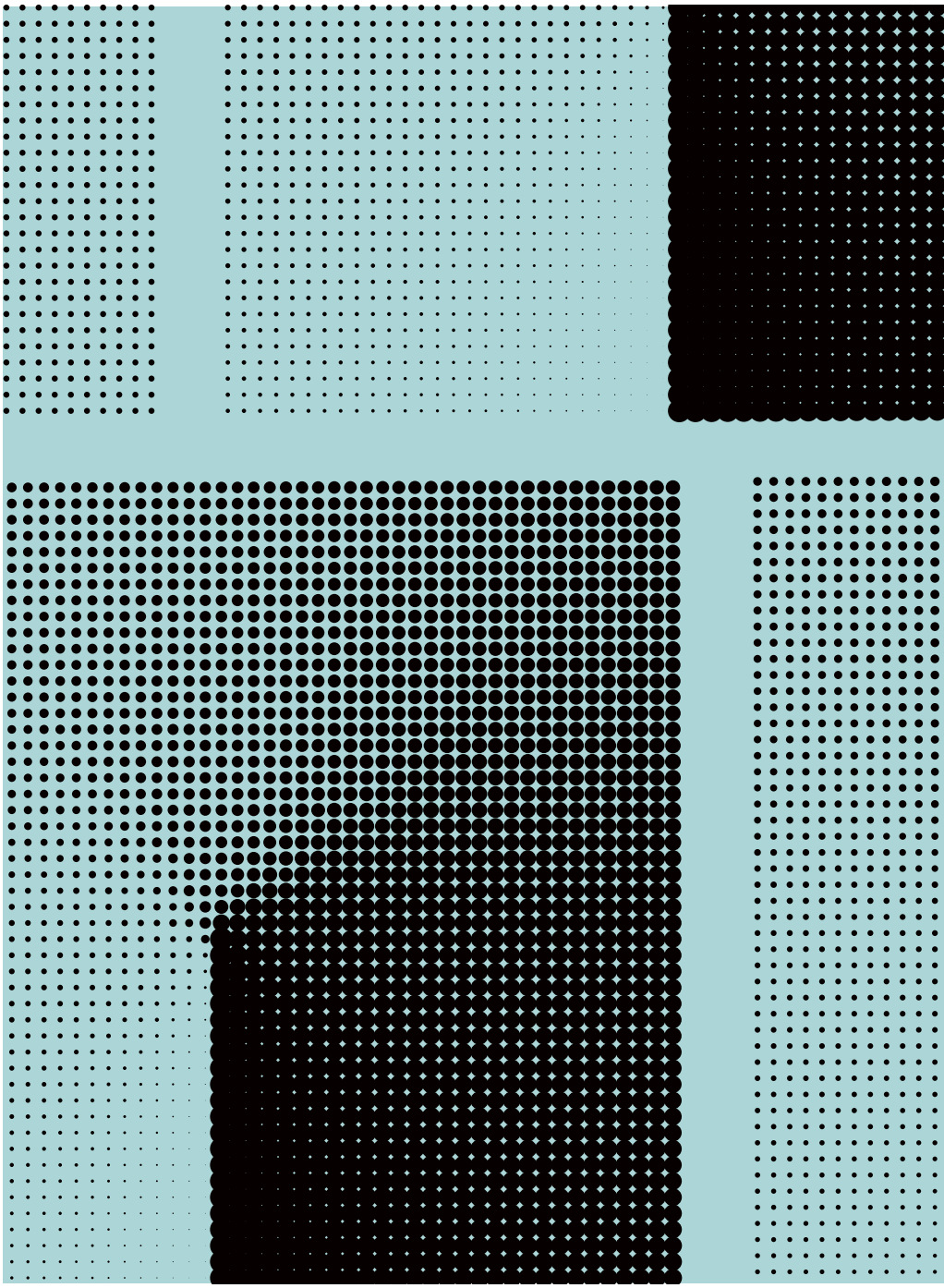
ホワイトペーパー
アジア太平洋地域
2022年8月

ゼロトラストセキュリティの現状 2022

日本語版

アジア太平洋地域における
アイデンティティ&アクセス管理の成熟度

Okta Inc.
okta.com
info_apac@okta.com



okta

ホワイトペーパー
アジア太平洋地域
2022年8月

目次

3 なぜ今、ゼロトラストが必要なのか

アジア太平洋地域のセキュリティ戦略における「3つのポイント」

› ゼロトラストはもはや単なる流行語ではない

› 企業セキュリティに特効薬はない

› ゼロトラスト実現の鍵は「アイデンティティ」

5 アジア太平洋地域でアイデンティティ主導のセキュリティが本格化

6 アイデンティティ：ゼロトラストソリューションの中核とは

8 ゼロトラストの成熟度における5つのフェーズ

› 第1フェーズ：初期

› 第2フェーズ：発展期

› 第3フェーズ：成熟期

› 第4フェーズ：高度化

› 第5フェーズ：進化

11 業種別にみるゼロトラスト導入状況

› ヘルスケア

› 金融サービス

› ソフトウェア

› 政府機関

13 アイデンティティファーストのキュリティエコシステムとは

14 ゼロトラストの課題と未来像

15 調査方法

なぜ今、ゼロトラストが必要なのか

ネットワークやデバイスにおいて、「すべてを信頼せず、常に検証する」というゼロトラストセキュリティの考え方が、人々の心を捉えていることが調査で明らかになりました。クラウドを中心とした世界では、防御すべき境界はありません。組織やネットワークを境界とする基本的なセキュリティの概念を超えて、侵入者が常にネットワーク上に存在するということを受け入れるまでには、数十年の歳月がかかりました。

しかし今日、多くの企業の経営者は、ゼロトラストセキュリティの枠組みを受け入れています。ゼロトラストは、変わった流行語という位置づけから、戦略的な差別化要因やビジネス上の必要条件へと変化を遂げています。

Forrester社の2022年の定義によると、「ゼロトラストは、アプリケーションやデータへのアクセスをデフォルトで拒否する情報セキュリティ・モデルである」とされています。そして、ゼロトラストは次の3つの基本原則を提唱しています。

1. **すべてのエンティティはデフォルトで信頼しない**
2. **最小の特権アクセスが強制される**
3. **包括的なセキュリティ監視が実施される**

ゼロトラストはもはや机上の空論ではありません。ゼロトラストは、デジタル・フットプリントを持つほぼすべての企業にとって、積極的な取り組みとして位置づけています。しかし、多くの企業や組織が先進的なゼロトラストセキュリティの成果を実感するには、まだ長い道のりが必要です。

例えば、4年前の調査では、ゼロトラストへの取り組みを実施している、または今後1年〜1年半以内に実施すると答えた企業は、わずか16%でした。現在では、その数は97%に達しています。

昨年、Oktaによる「2021年ゼロトラストセキュリティの現状」レポート発表以来、すでにゼロトラストへの取り組みを行っているアジア太平洋地域企業の割合は31%から50%に増加しました。また、アジア太平洋地域の調査回答者の96%が、2022年に向けてゼロトラストセキュリティの取り組みを実施中または計画中であると回答しています。

> すでにゼロトラストへの取り組みを行っているアジア太平洋地域の企業の割合は、2021年の31%から2022年には50%に増加

第4回のレポート「ゼロトラストの現状」では、Oktaは、アジア太平洋地域の200人を含む世界各国のセキュリティリーダー700人を対象に、ゼロトラストセキュリティ態勢の確立に向けた取り組み状況を調査しています。

そこでは、セキュリティリーダーがすでに行っている具体的な取り組みや、短期的・長期的な観点で、どのように優先順位をつけていくのかをたずねています。

Oktaでは、Forrester社とCISA社が普及させたゼロトラストフレームワークを用いて、ゼロトラストへの取り組みにおいて、重要な優先事項を探りました。「データ」「ネットワーク」「デバイス」は、調査対象組織で最も優先度の高い項目としてランクインしていることは驚くことではありません。しかし、この優先順位は、時間の経過とともに変化し、ネットワークからユーザに重きを置くセキュリティ対策に、「人」という項目が徐々に重要度を増していくと考えられます。そこで、アイデンティティは、ゼロトラストセキュリティの取り組みにおいて、強力な推進力となります。

アイデンティティの考え方は今や一般的になりつつあります。調査対象であるアジア太平洋地域のほぼすべての企業や組織が、すでにゼロトラストへの取り組みを始めている、あるいは今後数カ月のうちに取り組みを始める明確な計画を持っていることがわかっています。

アジア太平洋地域のセキュリティ戦略における「3つのポイント」

1. ゼロトラストはもはや単なる流行語ではない

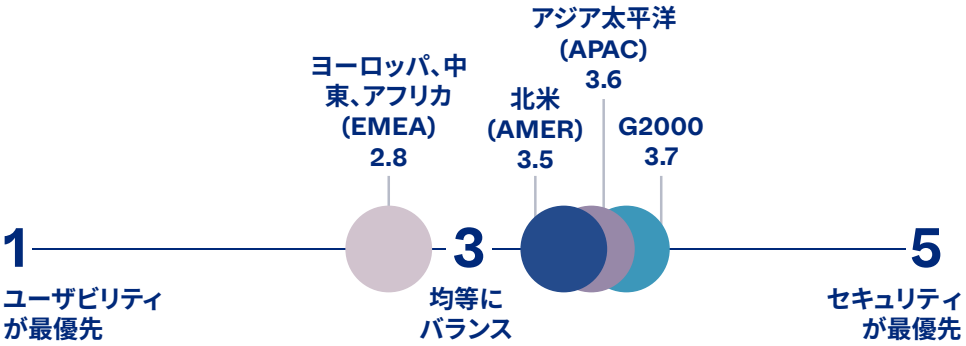
ゼロトラストの考え方は、世界中の企業や組織にとってセキュリティの捉え方として一般的になっています。これらの企業や組織の多くは、すでに取り組みを始めており、ゼロトラストをさらに加速させるための具体的なソリューションを積極的に探し求めています。

ゼロトラストの採用は単なる計画ではありません。大半の企業や組織が驚くべき早さで、ゼロトラストを実行に移しています。2021年には、アジア太平洋地域の組織の31%がゼロトラストへの取り組みをすでに実行している述べましたが、今年はその数が増え、ほぼ50%に達しています。

ゼロトラストの採用の伸びは目覚ましいものがあります。しかし、アジア太平洋地域のゼロトラスト採用率は、世界平均（55%）に及ばず、世界平均（前年比31%増）やEMEAや北米などの他の地域と比べても採用率が低いことを示しています（アジア太平洋地域の前年比は18%増）。

セキュリティへの懸念は、ゼロトラストへの強い動機付けとなっています。企業や組織は、長い間セキュリティとユーザビリティでバランスをとるのに苦労してきました。近年はユーザビリティに対する懸念が優先されていましたが、今年はその傾向が反転し、調査対象の企業や組織では、セキュリティプロジェクトの優先度が平均してやや高くなっています。

地域別比較：あなたの組織では、セキュリティの重要性とユーザビリティの重要性のバランスをどのように取っていますか？



グローバルな傾向とは対照的に、アジア太平洋地域の回答者はユーザビリティ（25%）よりもセキュリティ（75%）を優先するという点は、興味深いところです。

さらに注目すべき点は、アジア太平洋地域の組織はゼロトラストの採用で著しい伸びを示していることです。しかしグローバルな企業や組織にはまだ遅れをとっています。

2. 企業セキュリティに特効薬はない

ゼロトラストは、実現には複雑な要素が絡み合い、深く統合された複数のベスト・オブ・ブリードのソリューションがシームレスに連携することが必要です。個々の企業や組織によって、開始時の状況やリソース、優先順位は異なり、最終的なゼロトラストセキュリティにおける同じ目標に到達するための経緯は、それぞれ異なるものになります。

3. ゼロトラスト実現の鍵は「アイデンティティ」

世界中の企業や組織が、ゼロトラスト戦略を成功させるためには、アイデンティティが重要です。企業は、ゼロトラストの取り組みの一環として、新たな領域であるアイデンティティのセキュリティ確保に向けて、日々取り組んでいます。そして、各企業がこれらの取り組みを支えるために進めている具体的な「IAM戦略」は、5つの異なるフェーズで表すことができます。アジア太平洋地域の調査回答者の多くは、ゼロトラストセキュリティ戦略全体においてアイデンティティが重要であると回答しています。

アジア太平洋地域でアイデンティティ主導のセキュリティが本格化

ゼロトラストセキュリティというテーマについて回る「アイデンティティ主導のセキュリティ」は、新型コロナウイルス感染拡大の影響によるリモートワークへの働き方の変化を背景に、アジア太平洋地域のほぼすべての企業や組織において優先度が高くなっています。

昨年のレポートでは、アジア太平洋地域の調査回答者の約76%が、ゼロトラストに関する予算を「中程度に増やす」または「大幅に増やす」と回答しています。今年のレポートでは、回答がほぼその通りになっていることが示されています。過去1年間でゼロトラストの予算がどのように変化したかをたずねたところ、82%が予算支出に中程度の変化があったと回答しています。また、アジア太平洋地域においてゼロトラストセキュリティの取り組みの課題のうち、上位3つは、「人材とスキルの不足（31%）」、「関係者の賛同が得られないこと（18%）」、「ソリューションに対する認識不足（18%）」となっています。

一目でわかる：日本における回答者の主なポイント

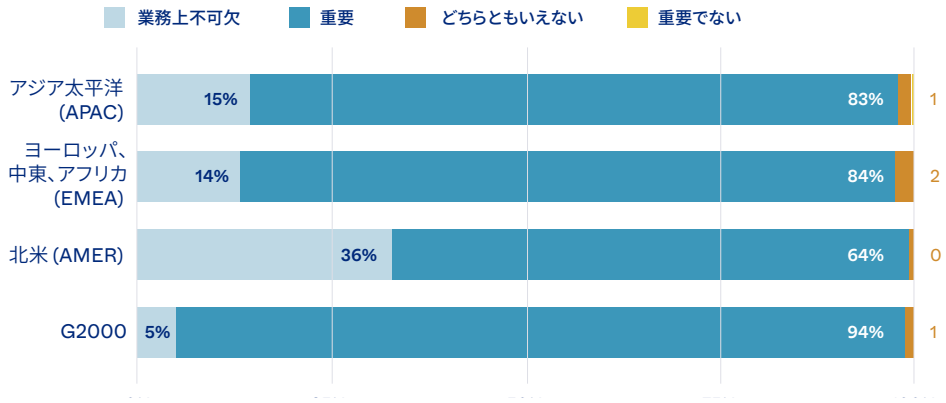
- 2021年時点で、日本の68%の組織が、ゼロトラストセキュリティ戦略をすでに実施しているか、今後1年以内に実施する予定であると回答、2022年には85%まで増加しています
- クラウドインフラへの特権アクセス管理およびAPIへのアクセス保護は、日本の企業や組織にとって最優先事項であり、回答者の半数がこれらの取り組みは、今後1年～1年半の最優先事項であると回答しています
- 日本の企業や組織の62%は、ユーザビリティよりも「セキュリティ」を優先しています
- ゼロトラストセキュリティ戦略全体において、日本ではアイデンティティがビジネスに必要不可欠であると考える組織は、わずか10%でした
- 日本の企業や組織がゼロトラスト戦略を実施する際の上位3つの課題は、「1.コスト面での懸念」、「2.人材・スキル不足」、「3.ソリューションへの認識不足」です

ゼロトラストソリューションの中核とは

各企業や組織のゼロトラスト実現への過程はそれぞれ異なりますが、グローバルな組織の考え方の中では、ゼロトラストに対するアイデンティティ・ファーストのアプローチが最重要であるだけでなく、必要不可欠であるという認識が高まっています。

これにより、企業や組織はアイデンティティ＆アクセス管理（IAM）を他の重要なセキュリティソリューションと統合することで、ユーザ、デバイス、データ、ネットワーク間のアクセスをインテリジェントに管理する強力な中央管理プラットフォームとしてフル活用することができるようになります。

地域別比較：ゼロトラストセキュリティ戦略全体において、アイデンティティはどの程度重要ですか？



調査によると、グローバル企業の80%が、ゼロトラストセキュリティ戦略全体にとってアイデンティティが重要であると回答し、さらに19%がアイデンティティがビジネスにとって重要であると回答しています。すなわち、合わせて99%の組織がゼロトラスト戦略における主要な要素としてアイデンティティを挙げていることになります。特にCISOやその他の経営層においては、（重要であると答えた98%のうち）26%が、アイデンティティをビジネスに必要不可欠とみなしています。Gartner社が最近、2022年のセキュリティの7大トレンドの1つとして「IDシステム防御」を取り上げたのは不思議ではありません。

アジア太平洋地域の回答者は、ゼロトラストセキュリティ戦略全体におけるアイデンティティの重要性を83%と評価しています。さらに14%が、自社のビジネスにとって必要不可欠であると回答しています。

> アジア太平洋地域 (アジア太平洋地域) の回答者の83%が、ゼロトラストセキュリティ戦略においてアイデンティティが重要であると回答しています

また今年の調査では、中小企業よりもForbes社の「Forbes Global 2000企業」のほうが、セキュリティプロジェクトにおいてセキュリティチームがIAM技術を完全に把握している傾向にあることがわかりました。しかし世界的には、IAMを少なくとも部分的に統率するセキュリティチームが増えています。ただし、アジア太平洋地域と北米では、その数はほぼ横ばいとなっています。

さらに、セキュリティへのシフトはアジア太平洋地域と北米でより顕著なものとなっており、EMEA地域では両者の優先順位がより均衡していると報告されています。ではなぜ、セキュリティにシフトしているのでしょうか。リモートワークやハイブリッドワークを定着させた企業は、すでに新型コロナウイルスの影響下の中で、ユーザビリティへの投資を活用し、セキュリティの負債を取り戻しつつあるのかもしれません。

ゼロトラストの取り組みのためのアイデンティティ導入モデル

ゼロトラストの成熟度 5つのフェーズ

企業は、ゼロトラストへの取り組みを加速させています。ほとんどの企業や組織は、少なくとも重要なアイデンティティに関する取り組みから、ゼロトラストセキュリティ実現への道を歩み始めています。

今回の調査では、全世界で70%以上の回答者がすでに第1フェーズ（初期）を実現していることが明らかになりました。また、95%の回答者が、今後1年～1年半の間に第1段階のプロジェクトを完了する予定であり、成熟曲線に沿ってプロジェクトに着実に取り組んでいることがわかります。第2フェーズ（発展期）の取り組みについては、ほとんどの回答者（約80%）が従業員のシングルサインオン（SSO）を導入していますが、外部ユーザ向けにMFA（多要素認証）を導入し、権限を与えられた契約社員、サプライヤー、ビジネスパートナーに重要なデータへの安全なアクセスを保証していると答えた回答者は、わずか38%でした。ゼロトラストへの取り組み状況は、以下に述べるように第2フェーズ以降に分かれますが、全世界の全回答者の約50%が、複数のアイデンティティプロジェクトを完了しており、残りの回答者の多くは、今後数カ月間にこれらの追加プロジェクトに取り組む予定であると述べています。

Forbesの「Global 2000」企業グループに目を向けると、これらの回答者のほぼ100%が、今後1年半以内にすべての第1フェーズのアイデンティティプロジェクトを完了する予定であることがわかります（まだ完了していない場合）。また、これらの企業の回答者の少なくとも半数は、同じ期間内に第1フェーズ～第4フェーズすべてのプロジェクトを実質的に完了し、第5段階のプロジェクトに着手する予定であると述べています。

第1フェーズ：初期

調査では、ゼロトラストの初期フェーズにおいて、企業や組織は、連携していないディレクトリ、リスクの拡大、および無限に発生するアイデンティティベースの攻撃といった基本的なアイデンティティに関する課題に直面していることがわかっています。この段階で、成熟度曲線の進捗を測定するために、企業や組織に対して、従業員のディレクトリが自社のクラウドアプリに接続されているか、従業員に多要素認証（MFA）を導入しているかをたずねました。研究者は、第1フェーズにおいても、企業や組織は認証プロセスに何重ものセキュリティを追加することによって、適切な人材に適切なデータへのアクセスを与える効果的な方法を見い出していることを発見しました。

このレポートによると、今後1年半以内に、世界中の企業や「Global 2000」企業の回答者のほぼすべてが、第1フェーズのアイデンティティプロジェクトを完了させる予定であることが示されています。また、従業員へのMFAの導入は、今後1年半以内に全地域の回答者が、従業員向けMFAを全体的なアイデンティティ戦略の一環として位置づけるとしています。

アジア太平洋地域では、従業員向けMFA（76%）が最も採用されているアイデンティティプロジェクトで、今後1年半以内に、すべての地域の回答者の全員が、このアイデンティティプロジェクトを全体的なアイデンティティの一部として採用するとしています。アジア太平洋地域では、自社のディレクトリがクラウドアプリケーションに接続されていると回答した企業は少なかったですが（68%）、今後1年半以内にこのアイデンティティプロジェクトの完了に向けて推進していく予定です。

アジア太平洋地域で、従業員へのMFA導入（76%）が、最も採用されているアイデンティティプロジェクト

第2フェーズ：発展期

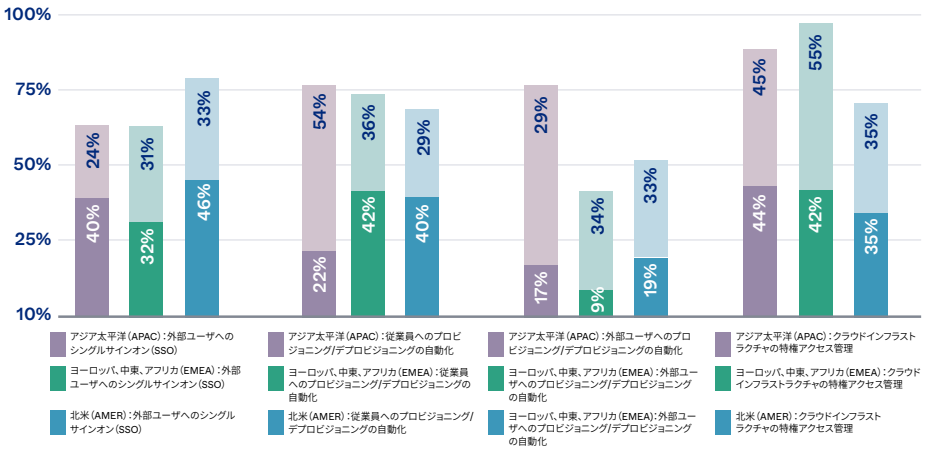
発展段階においては、企業や組織は通常、クラウドアプリケーションの導入の増加やM＆Aなどの変化によって、異なるシステムを連携しようとしており、それに伴ってユーザアクセスを簡素化する必要性が高まっています。

第2フェーズの進捗を評価するため、回答者に対して、ビジネスパートナーや契約業者などを含む外部ユーザにMFAを導入しているか、また従業員にシングルサインオンを導入しているかどうかをたずねました。アジア太平洋地域では、39%の組織がすでに外部ユーザに対してMFAを導入しており、さらに27%が今後1年～1年半の間に導入する予定であるという結果が得られました。また興味深いのは、70%の企業がすでに従業員にシングルサインオンを導入しており、さらに30%が今後1年～1年半の間に導入する予定であることです。

企業は、遠隔地にいる従業員だけでなく、契約社員、ボランティア、サプライヤーや非正規雇用・その他のパートナーに依存する傾向にあります。これらの人員は、組織にとって増大するセキュリティ上の脅威でもあり、これらの外部ユーザへのMFAの拡張は、すべての地域にとって、データへのアクセスと安全を確保するための主な焦点となっています。

第3段階：成熟期

フェーズ3地域別比較：あなたの組織では、今日現在、どのプロジェクトをすでに実施し、今後1年～1年半の間にどのプロジェクトを優先的に実施する予定ですか？



調査によると、成熟した組織は、コンプライアンスや規制要件の増加、ハイブリッドインフラ、大規模で多忙である、動的である、一部または大部分がリモートワーカーをサポートする法的な必要性があるなど、複雑な課題を抱えていることがわかりました。このような課題を解決するためには、従業員やレガシーネットワークを超えたIAMの取り組みを展開することや、増加する外部ユーザや拡大するクラウド、マルチクラウドインフラに対応させることが必要があります。アジア太平洋地域地域の企業の回答者は、今後1年半の間に、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、およびクラウドインフラの特権アクセスへの取り組みを重視すると述べており、それぞれの導入率は22%から76%、43.5%から88%（2倍以上）になるとのことです。

第4フェーズ：高度化

成熟度曲線に沿った組織は、アイデンティティをベースとしたゼロトラストの基本を実現し、これまで以上に複雑なアイデンティティの課題に取り組むためのツールやプロセスを備えています。

調査対象となった「Global 2000」企業のすべてが、今後1年～1年半の間に、ユーザグループ間でのMFAの導入（アジア太平洋地域では44%が導入済み）やAPIへのアクセスのセキュア化（アジア太平洋地域では46%が導入済み）などのアイデンティティプロジェクトを完了させる予定です。

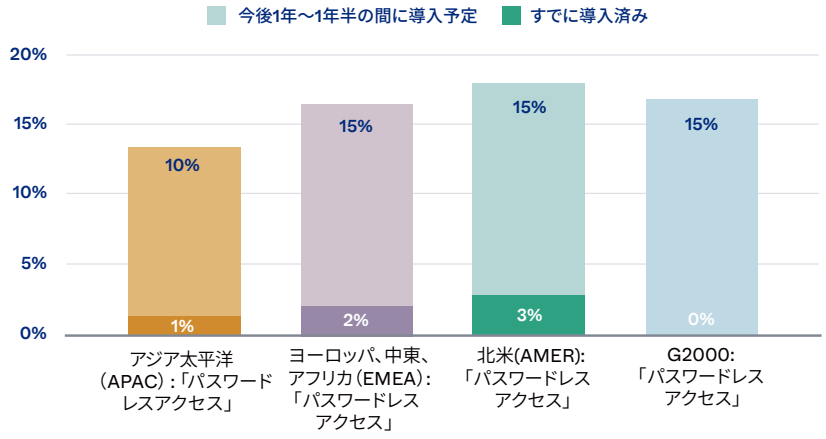
これらの企業の少なくとも半数は、上の期間内に第4フェーズすべてのアイデンティティプロジェクトを完了させる予定です。その際、ユーザがアクセスを試みた時点のデバイスの信頼度、アクセスを試みた場所、ユーザや データリソースそのもの、その他の重要な入力などのコンテキストベースのアクセスポリシーに重点を置いています。

第5フェーズ：進化

進化の段階にある企業や組織は、すでにAWS（Amazon Web Services）、GCP（Google Cloud Platform）、Microsoft Azureなどのクラウドベースのプラットフォームに業務を移行しており、自動化とエッジセキュリティの導入に重点を置いていることが明らかになりました。

ここでは、これまでのフェーズで強調されたゼロトラストの中核プロジェクトの実施から、ユーザライフサイクル管理の最適化、サーバへのセキュリティアクセス制御の適用、高保証度要素（ファクターシーケンス、WebAuthnによる生体認証ベースのログイン、U2Fセキュリティキーなど）を用いたパスワードレスアクセスの実装に焦点が移行します。

地域別比較:「パスワードレスアクセスオプション」をすでに導入していますか、それとも今後1年〜1年半の間に導入する予定ですか?



また、調査では、すべての地域の回答者がパスワードレスアクセスの採用を拡大する予定であることがわかっています。今日のデータ漏えいの半数以上が脆弱な認証情報や盗まれた認証情報に関連しており、ランサムウェアやその他のアイデンティティベースの攻撃増加の多くが認証情報の悪用が原因であることを考えると、これは特に好ましい結果であるといえます。

アジア太平洋地域では、世界的にパスワードレスアクセスの採用が最も低く、わずか0.5%がすでに導入済みで、今後1年半以内に採用を予定しているのはわずか10%です

業種別にみるゼロトラストの導入状況

各業界や企業、組織によって、慣行や優先順位、業務で求められる内容がそれぞれ異なっています。それに伴って、ゼロトラスト実現への過程もそれぞれ少し異なる傾向があります。今年の調査では、ヘルスケア、金融サービス、ソフトウェア、そして今回初めて政府機関という4つの主要な業種に深く踏み込み、これらの業種における企業や組織特有のニーズがゼロトラストソリューションの採用にどのように影響するかをより明確化しようと試みました。Oktaは、「セキュリティ」と「ユーザビリティ」という、相反しがちな要素の間のバランスのとり方を解明したいと考えています。

もちろん、企業や組織はこれら両方の要件を満たす方法を見い出しています。興味深いことに、今年のグローバル調査の回答者は、平均してユーザビリティよりもセキュリティをやや高く優先順位をつけており、ユーザビリティがセキュリティをやや上回っていた2021年のデータから変化が見られます。セキュリティへの関心が高まっている例として、ヘルスケア業界では、クレデンシャルベースの攻撃に対して非常に脆弱な、パスワードのような要素への依存を減らしています。対象となるすべての業種において、ゼロトラストセキュリティ戦略を導入する際の課題上位4つは、驚くほど一貫していました。今年の最大の課題は「人材・スキル不足」であり、次いで「ステークホルダーからの賛同が得られないこと」、「コストへの懸念」「ゼロトラストを

サポートするセキュリティソリューションの認知度」となっています。

主要な業種：ヘルスケア

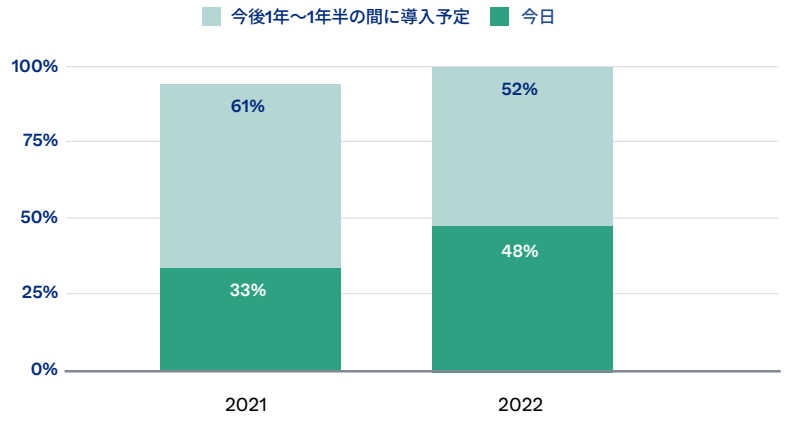
ヘルスケア分野で課題となるのは、ゼロトラストの導入計画の策定です。ゼロ・トラストへの取り組みを実施中、あるいは今後1年～1年半で開始する予定であると回答したヘルスケアの回答者の割合は、2021年の91%から2022年には96%に上昇しました。ヘルスケア分野の回答者の58%がすでにゼロトラスト実現のための取り組みを開始しており、昨年のレポート時点での開始していた割合の37%から20%の増加となっています。

アジア太平洋地域におけるヘルスケア分野の回答者のうち88%が、過去1年間にゼロトラストの予算が中程度増加したことを記録しており、同じ回答者の63%がユーザビリティよりもセキュリティを優先していることが印象的でした。

この回答者では、すでにゼロトラストへの取り組みを現時点で実施しているか、今後6カ月～1年以内に実施する意向であり、短期間での実現に向けた勢いが続いています。これは、悪意のある攻撃に対して、ヘルスケア業界の脆弱性の認識の強さを反映しています。

主要な業種：金融サービス

金融サービスの前年度比：あなたの組織では、現在、ゼロトラストセキュリティの取り組みを明確に定義していますか、または今後1年～1年半の間に実施する予定はありますか？



当然のことながら、金融サービス企業はゼロトラストに関心を寄せています。世界の金融サービスの回答者のほぼすべてが、今後1年から1年半以内にゼロトラストへの取り組みを開始する予定です。実際、回答者の約半数（48%）は、このような取り組みをすでに実施しており、昨年のわずか1/3から増加しており、増加率は15%と堅調です。

アジア太平洋地域の金融サービス企業の94%は、ユーザビリティよりもセキュリティを優先しており、同じ回答者の88%以上が、過去1年間にゼロトラストの予算がやや増加したと述べています。

金融サービス企業において、ゼロトラストの取り組みを実現するためのガイドライン策定作業の大半は、すでに始まっています。金融サービス企業は現在、他のセクターと比較してゼロトラ

ストの成熟度がやや遅れているかもしれませんが、近いうちに追いつくために大きな前進を遂げる、積極的で具体的な計画を立てています。

主要な業種：ソフトウェア

昨年の調査では、ソフトウェア業界は他の調査対象業種に比べ、大きく遅れをとっていました。しかし、このレポートでは、ソフトウェア企業の回答者は、今後1年～1年半の間にゼロトラストセキュリティの取り組みを大きく前進させることを約束しています。2021年、調査対象となったソフトウェア企業のうち、ゼロトラストへの取り組みをすでに策定している企業はわずか9%でしたが、さらに79%がゼロトラストへの取り組みを開始する予定であると回答しています。

そして、ソフトウェア業界の回答者は約束を果たしています。今年、アジア太平洋地域のソフトウェア企業のうち、取り組みを実施している企業は50%に急上昇し、さらに45%が今後1年半に取り組みの定義を行う予定であることから、合わせて95%のアジア太平洋地域のソフトウェア企業が少なくともその取り組みを開始したことになります。ゼロトラストの採用も同じように加速しています。ソフトウェア企業は迅速に行動に移しており、ゼロトラスト戦略を定義するスピードも上がり、今後半年～1年以内にゼロトラストの取り組みを実施する見込みです。

主要な業種：政府機関

世界的にみると政府機関では、ゼロトラストの取り組みが他業種組織に先行しているように見えますが、アジア太平洋地域ではあてはまらず、同地域の政府機関でゼロトラストセキュリティの取り組みを行っている回答者は半数未満でした。

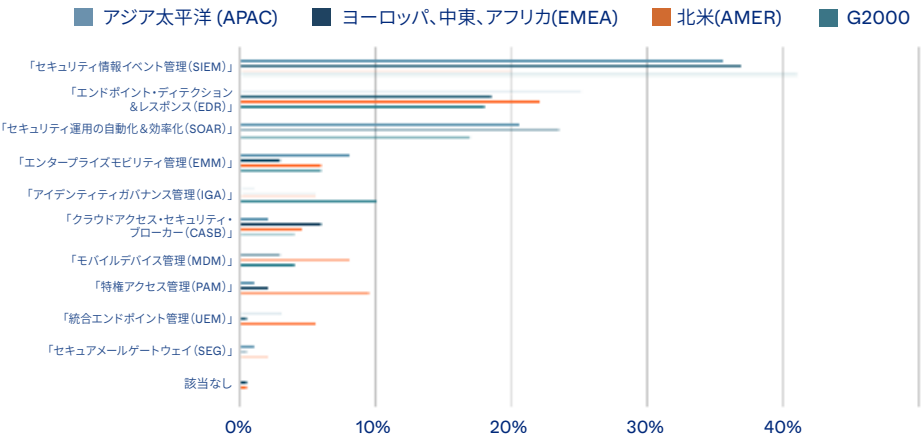
世界の政府機関の回答者における共通点としては、成熟曲線全体で大きな前進させる計画であることがわかります。とりわけ、12のアイデンティティ・プロジェクトのうち6つについて、進捗をほぼ倍増させ、従業員やユーザグループへのMFA導入などの取り組みを優先させるとしています。

アイデンティティファーストのセキュリティエコシステムとは

Forrester社やNISTなどが推進するゼロトラストの推奨事項に対応する単一のソリューションは存在しないことが、調査から判明しています。しかし、アイデンティティはセキュリティスタック全体の基本技術として登場し、アイデンティティを後から付け加えるのではなく、セキュリティ計画の中心に据える必要があることが明確になってきています。

調査では、セキュリティ情報およびイベント管理（SIEM）、セキュリティオーケストレーション、自動化および応答（SOAR）、エンドポイント保護のためのエンタープライズモビリティ管理（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でIAMソリューションを統合できれば、企業や組織が構築するゼロトラストによる防御はより有効で効果的になると述べられています。IAMとSIEMを連携させることで、潜在的なセキュリティイベントをインテリジェントにトリアージすることができます。例えば、IAMとSOARを統合することで、より良い情報に基づいた自動セキュリティ対応が可能になり、IAMとEDRを統合することでアイデンティティを使い、攻撃が進行中であることを示している独立したデータポイントを集中的に相関させることができます。

地域別比較:ゼロトラストセキュリティをサポートするために、どのツールをIAMソリューションと統合することが最も重要でしょうか?



セキュリティリーダーは、「ゼロトラストセキュリティを確立するため、IAMソリューションと統合する際に最も重要であると考えるツールは何か」とたずねました。SIEMは、調査対象の「Global 2000」企業の40%を含む、ほぼすべての地域でSIEMが統合に最も不可欠な要素であると考えられています。最も必要不可欠な要素としてSIEMを挙げなかったのは北米だけで、EDRがわずかに上回りました。現在IAMと統合されているのは、SIEM、EDR、CASBが最も多く、この3つは 調査対象企業の5社中3社以上ですでに運用されています。

ゼロトラストの課題と未来像

最新のレポートによると、多くのグローバル企業が昨年からゼロトラストへの取り組みを加速させています。一方で、チームが新しいテクノロジーを導入するための多額の投資など、依然としていくつかの深刻な課題に直面していることがわかりました。

セキュリティリーダーに、具体的にゼロトラストへの取り組みを進めるうえでの最大の課題について質問したところ、アジア太平洋地域の企業では「人材/スキル不足」がトップとなり、この点はテクノロジーとのギャップとして重要視されています。

ゼロトラストの先にあるものとは?

世界中が人材不足やスキル不足に直面している中、企業や組織は、予算や人員、トレーニングリソースを増やさずに、ゼロトラストを実現するためのソリューションを見つける必要があります。そして、これらのソリューションは、より簡単かつ迅速に展開でき、組織の成長とゼロトラスト戦略の進展に合わせて拡張できるものでなければなりません。ステークホルダーの賛同が得られないのは、セキュリティ部門がIAMソリューションや、その他のセキュリティ関連ソリューションにおいて、完全なオーナーシップを持っていないことが理由と考えられます。ゼロトラストへの取り組みに対して、あまり熱心でない他の部門は、そのような取り組みにリソースを割くことにためらいを感じるかもしれません。

しかし、こうした課題の中にも、調査にあるようにチャンスも隠れています。企業や組織は、協働する部門を教育して合意を形成し、ゼロトラストへの取り組みを推進する必要性を確立する必要があります。そのためには、他の企業の仲間に目を向けて、組織的なアプローチを指揮す

るためのインスピレーションを見つける必要があります。

そして、最も重要なことは、組織は適切なパートナーと協力して、どの過程においても活用できるゼロトラストソリューションを導入し、既存のセキュリティインフラと統合できる具体的なソリューションを見つけ、存在する課題を克服することです。

調査方法

Pulse Q&Aは、Oktaの委託を受け、さまざまな業種のグローバル企業で、セキュリティ部門の役職に就くリーダー700名を対象に調査を実施しました。セキュリティリーダーとは、テクノロジーの購買決定を行う責任者と定義され、調査パートナーのPulse社が2022年初頭にこれらの方から回答を収集しました。

業界データは、ヘルスケア、金融サービス、ソフトウェア、政府機関の4つの業界と、3つの地域、ならびに「Forbes Global 2000」に選ばれた企業に焦点を当てました。日本を含むアジア太平洋地域は、回答者の29%を占めています。調査対象のセキュリティリーダーは、バイスプレジデント、ディレクター、またはCレベルの企業幹部で、レポート作成者は各セグメント内のパーセンテージを使用して正規化しています。アジア太平洋地域に特化したデータでは、8%が政府関係者、26%がCレベルの回答者で構成されています。

回答者は、少なくとも500人以上の従業員を雇用する組織に所属しています。昨年と同様に、回答者の約40%が1万人以上の規模の企業に勤務しています。

Oktaについて

Oktaは、業界をリードするアイデンティティ管理の独立系プロバイダーです。Okta IdentityCloudは、あらゆる人があらゆるテクノロジーを 安全に使うことができる世界を実現します。Oktaは、7,000以上のアプリケーションやインフラプロバイダーとの統合機能を備え、世界中の人々や組織にシンプルで安全なアクセスを提供し、最大限の可能性を発揮できるよう支援します。JetBlue、Nordstrom、Siemens、Slack、Takeda、Teach for America、Twilioなど15,800以上の組織が、Oktaを利用して従業員や顧客のアイデンティティを保護しています。詳しくは、https://www.okta.com/jp/をご覧ください。