2024 年 Duo
Trusted Access レポート

複雑な環境への対応

2024 年 Duo Trusted Access レポート

目次

Trusted Access レポートの凡例

- セクションの開始
- 関心のあるポイント
- セクションの続き
- 追加情報
- セクションの終了

MFA は優れたセキュリティ対策ですが、それだけでは不十分です。脅威の高度化に応じ、セキュリティを強化する必要があります。

はじめに

アクセス管理とアイデンティティ セキュリティの新領域

未来を模索するとき、私たちは多くの場合、未知のものを予測することに惹かれます。答えの探求に果てはなく、予測結果はデータに大きく左右されます。

今日、組織は危険なデジタル環境に囲まれています。金銭の要求、サイバースパイ活動、業務の中断、評判の低下、サイバー戦争など、攻撃者の攻撃手法は多岐にわたり、目的もまた同じくらい多様です。同時に、複雑な IT スタック、分散したハイブリッドワークフォース、システムやアプリケーションにアクセスする多種多様なデバイスなど、組織内で管理するものも複雑になっています。アドホックなテレワーク設定からハイブリッドワークモデルへと進化した結果、従来の企業の境界は、サイバー領域の果てまで拡張されることになりました。

数年前であれば、IT インフラストラクチャの保護の主な目的は、「明かりを灯し続ける (事業を継続する)」ということわざのように、システムをスムーズに稼働させることだったかもしれません。今ではその範囲は飛躍的に拡大しています。ランサムウェアから国家の支援を受けたハッキングに至るまで、外部からの多くのサイバー脅威に対して警戒を怠らないように防御する必要があります。脅威が拡大するにつれて攻撃の対象領域も拡大し、すべての従業員のアクセスやデバイスがエントリポイントとなる可能性があります。この変化により、IT 部門は、運用稼働時間を主に重視する部門から、高度で多岐にわたる外部の脅威から保護するための重要な監視部門へと変貌しました。

未来がどうなるかを正確に予測することはできませんが、過去のパターンを分析することで、将来の可能性に関する洞察が得られます。たとえば以前の Trusted Access レポートでは、企業が高度化するセキュリティ環境でリスクを軽減しようとしているため、多要素認証 (MFA) の導入が急増していることが指摘されています。

ますます巧妙化するサイバーセキュリティの脅威に組織が対処する中で、ここ数年、包括的なアクセス管理ソリューションに対する需要が顕在化しています。MFA は優れたセキュリティ対策ですが、それだけでは不十分です。脅威の高度化に応じ、セキュリティを強化する必要があります。

コンテキストを統合することで、アクセス管理ソリューションは、アクセスが要求されている状況を分析できます。たとえば通常のログイン時間、地理位置情報、デバイスなど、ユーザーの一般的なふるまいや環境に関する情報です。これにより、セキュリティが強化され、より包括的で動的な認証アプローチが実現します。

つまり、認証プロセスにコンテキストを追加することで、正当なユーザーと潜在的な脅威をシステムがより適切に区別できるようになり、優れたユーザーエクスペリエンスを維持しながらセキュリティを強化できます。つまり、コンテキストが MFA の新形態となるのです。

場所やデバイスの詳細（オペレーティングシステムなど）などのコンテキスト要因は、長年にわたって Trusted Access レポートで取り上げられています 。しかし、ハイブリッドワークがしっかりと根付いた現状では、コンテキスト要因の重要性はさらに大きくなっています。

関心が高まっているもう 1 つの分野は、アイデンティティの未来です。具体的には、サイバーセキュリティの観点からデジタルアイデンティティの急増に対処する方法のことです。

現代のワークプレイスでは、すべての従業員がさまざまなシステム、アプリケーション、プラットフォームで複数のデジタルアイデンティティを使用している場合があります。これは、電子メールアカウントから、内部システムへのアクセスログイン情報 、Slack などのコラボレーション プラットフォームのプロファイルにまで及びます。企業はクラウドサービス、Software as a Service プラットフォーム、リモート コラボレーション ツールを導入し続けています。これに伴い、こうしたデジタルアイデンティティの数も増加しています。デジタルアイデンティティの急増は、生産性とセキュリティの両方に大きく影響します。

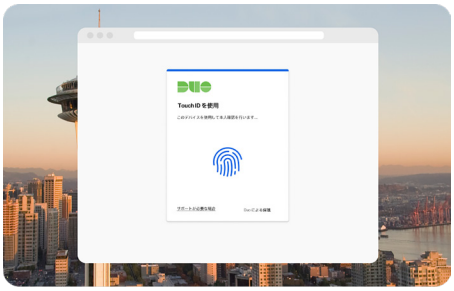
これらのアイデンティティにより、よりシームレスなコラボレーションと必要なリソースへのアクセスが可能になり、効率が向上します。その一方で、これらの多数のアイデンティティを管理し、それらを適切に保護するのは、手間のかかる作業になります。単一の包括的なインターフェイスで、組織のアイデンティティ エコシステム全体のリスクを可視化できることが必須になっています。

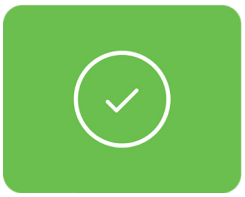
これは、アイデンティティ脅威の検出と対応(ITDR) 機能によって実現可能です。ITDR の進化はアイデンティティの未来に不可欠であり、日常生活でデジタルアイデンティティがますます普及していったとしても、デジタルアイデンティティの安全性を維持できます。

課題は明らかです。MFA の使用がグローバルに拡大し続けているため、攻撃者の手法も同様に拡大し続けるということです。侵害の可能性を最小限に抑えるには、ユーザーの典型的な行動や環境などのコンテキスト要因を利用するのはもちろん、単一の包括的なインターフェイスで組織のアイデンティティ エコシステム全体の可視化も行い、従来の MFA を強化する必要があります。

調査方法

このレポートでは、北米、中南米、ヨーロッパ、中東、アジア太平洋地域の約 5,800 万のエンドポイントと 2,100 万台の携帯電話上で動作する約 5,200 万のさまざまなブラウザを対象に、過去 1 年間に実行された 160 億件以上 (過去 4 年間で 440 億件以上) の認証を分析し、得られた洞察を紹介します。シスコでは、2022 年 6 月 1 日から 2023 年 5 月 31 日までを 2023 年度としています。





主な調査結果

01

認証方式の強化は増加傾向

Duo モバイルなどの認証アプリケーションは、セキュリティの強化と使いやすさの両方のニーズに対応しています。91.5% のアカウントで Duo Push が有効になっており、全認証の 21% に当たる 32 億回を超える認証で認証要素の 1 つとして使用されていました。なお、SMS と電話を認証要素として使用した認証は減少傾向にあり、4.9% (2022 年から 22% 減少) と過去最低水準にまで落ち込みました。

02

オフィス勤務の再開がハイブリッドワークの新たな現実に

リモート アクセス アプリケーションへのアクセスのための認証件数は 2020 年がピークで、昨年は認証の 25% 近くまで減少しました。従業員のオフィス勤務を再開する企業が増えたため、以来このカテゴリの認証件数は減少し続けています 。

03

グローバルに拡大を続ける MFA の使用

Duo を使用する MFA 認証の数は、この 1 年間で 41% 増加しました。認証件数が前年比で 52.3% 増加したドイツのような国々もあります。アジア太平洋地域では、日本、フィリピン、オーストラリアで昨年から引き続き増えており、それぞれ 28%、24.9%、16.9% の増加となっています。ブラジルは 3 番目に認証件数の増加率が高く、2022 年と比較して MFA の使用量が 26.3% 増加しています。

04

多様なデバイス環境にはベンダーに依存しないセキュリティが必要

オペレーティングシステム全体のランキングでは、アクセスデバイスの 38.2% を占める Windows が引き続き群を抜いて首位を占めていますが、2 番手の iOS が 33.4% と首位に迫る割合を占めており、注目されるところです。Apple は Duo ユーザーのモバイルカテゴリで常に最高の使用率を誇り、2 番手は Android ですが、使用率は 28.2% とはるかに低くなっています。ベンダーに依存しないセキュリティにより、潜在的なセキュリティギャップをなくすだけでなく、セキュリティシステムがデバイス環境の変化に容易に適応できるため、より優れた柔軟性と拡張性をも実現できます。

主な調査結果

05

組織は古いソフトウェアによるリスクを軽減するために制御を厳格化

古いデバイスに起因する障害の割合は、2023 年に 74.7% 増加しました。組織が認証を許可するオペレーティングシステム（OS）が多いほど、古い OS で認証が行われる可能性は高くなります。特に IT 環境を拡張している組織では、古いソフトウェアによってもたらされるリスクを軽減するために、制御の厳格化を進めています。

06

認証の失敗がユーザーのリスクを浮き彫りに

測定された全認証のうち、失敗していたのは 5% です。このデータを詳しく検証すると、失敗した認証の 28% は、ユーザーがシステムに登録されていないことが原因でした。未登録のユーザーが機密データや重要なシステムに不正アクセスし、データ漏洩につながる可能性があります。

07

セキュリティ負債を軽減する上位 3 つのポリシーグループ

セキュリティ負債を軽減するための最も効果的な戦略の 1 つは、リスクを包括的に管理することです。地理的制限、安全でないデバイス、ユーザー単位またはアプリケーション単位のきめ細かいアクセスに対応するポリシーにより、複雑さを軽減し、セキュリティの対応範囲を拡張できます。ただし、96.4% の組織では、場所に関連するポリシー（二要素認証の許可、拒否、必須）が設定されていません。

08

アイデンティティが新たな境界

適切な可視化、脅威検出、対応がなされなければ、アイデンティティ インフラストラクチャは攻撃者にとって重要なシステムに侵入する絶好の機会となります。Talos IR が確認したインシデント対応業務の 23% で、攻撃者は流出したログイン情報を悪用して有効なアカウントにアクセスしていました [1]。平均的な企業のアカウントの 40.26% は、MFA を使用していないか、脆弱な MFA をしています [2]。

高度なサイバー攻撃が常態化している環境では、アクセス管理ソリューションをアイデンティティの脅威検出と対応機能で強化し、単一の包括的なインターフェイスで組織のアイデンティティ エコシステム全体を可視化する必要があります。

注釈：

1.Talos IR の 2023 年版『一年の総括』の「テレメトリの動向」（6 ~ 7 ページ）を参照

2.『アイデンティティ セキュリティの状態』レポート（Oort 社）のセクション 2「多要素認証：フルカバレッジは今もなお困難」を参照

01 数十億件の認証

MFA によるパスワードの強化が続く

多要素認証は、従来のパスワードによるセキュリティに追加される形ながら、依然として高い効果を誇ります。Duo を使用した MFA 認証の数は、過去 1 年間で 41% 増加しました。

Push の利用が増加

最も使用されている認証方式は **Duo Push** で、全認証の 21% を占めています。

パスワードレスの導入は引き続き増加

セキュリティキーや TouchID などの生体認証技術を含む WebAuthn を活用した要素のアカウント導入率は、2022 年から 2023 年の 1 年だけで 53% 増加しました。

月間認証成功数（単位：10 億）

2019 年 5 月以降、Duo は 416 億件の認証成功を記録し、月間平均は 8 億 6,630 万件です。

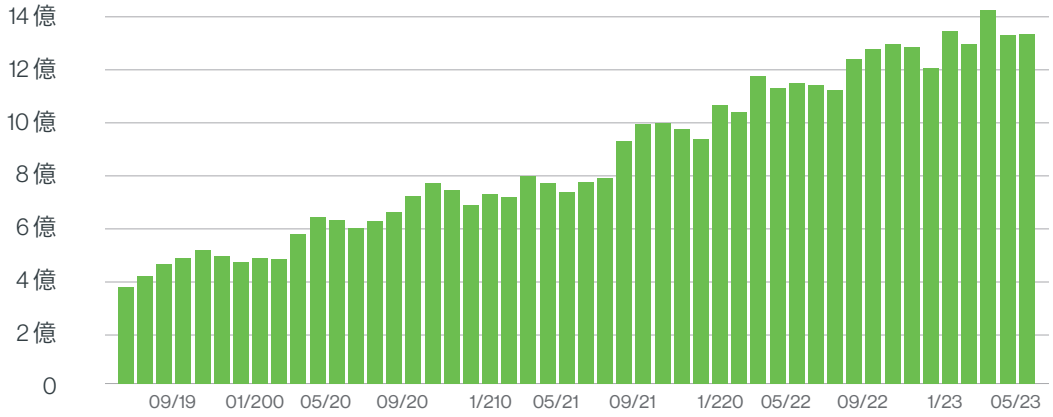
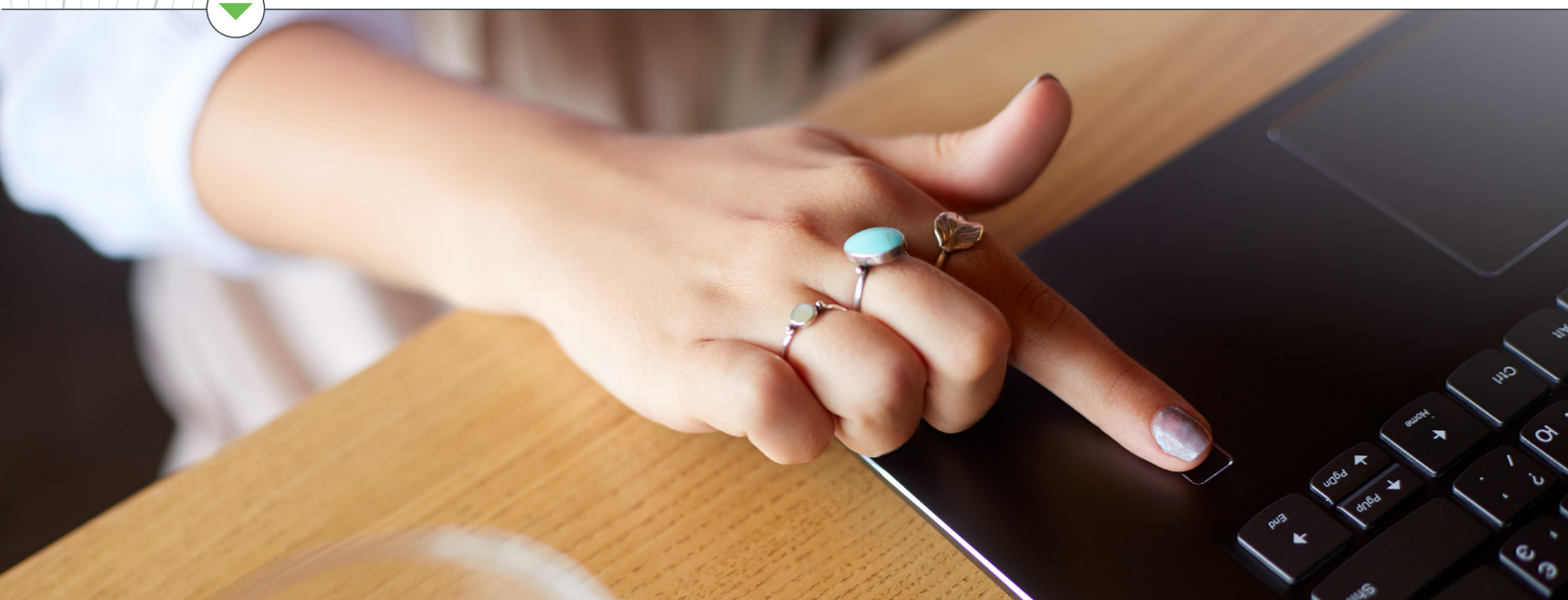


図 01 月別合計認証数



より強力な認証方式が増加傾向

認証方法としてのパスワードだけを使用することの脆弱性は、多くの文書で取り上げられています。パスワードは推測されたり、クラックされたり、フィッシングされたり、盗まれたりする可能性があります。そのうえユーザーが、複数のサービスでパスワードを再利用したり、簡単に解読できるシンプルなパスワードを作成したりすることで、脆弱性を悪化させることも珍しくありません。対照的に、多要素認証(MFA)は、潜在的な攻撃者に対して新たなハードルを導入することで、これらのリスクを軽減します。たとえパスワードが流出したとしても、攻撃者がユーザーの物理デバイスや生体情報を利用できる可能性はかなり低くなります。

しかし、最近注目を集めているサイバー攻撃を見ると、第二認証を有効にするだけでは、アカウントが侵入不可能になるわけではないことがわかっています。すべてのオーセンティケータがもともと同じ機能を有しているわけではなく、FIDO2 セキュリティキーや WebAuthn 対応の生体認証などの要素は、SMS テキストや電話などのアクセスしやすいものの脆弱な要素よりも、悪用されにくいことがわかっています。

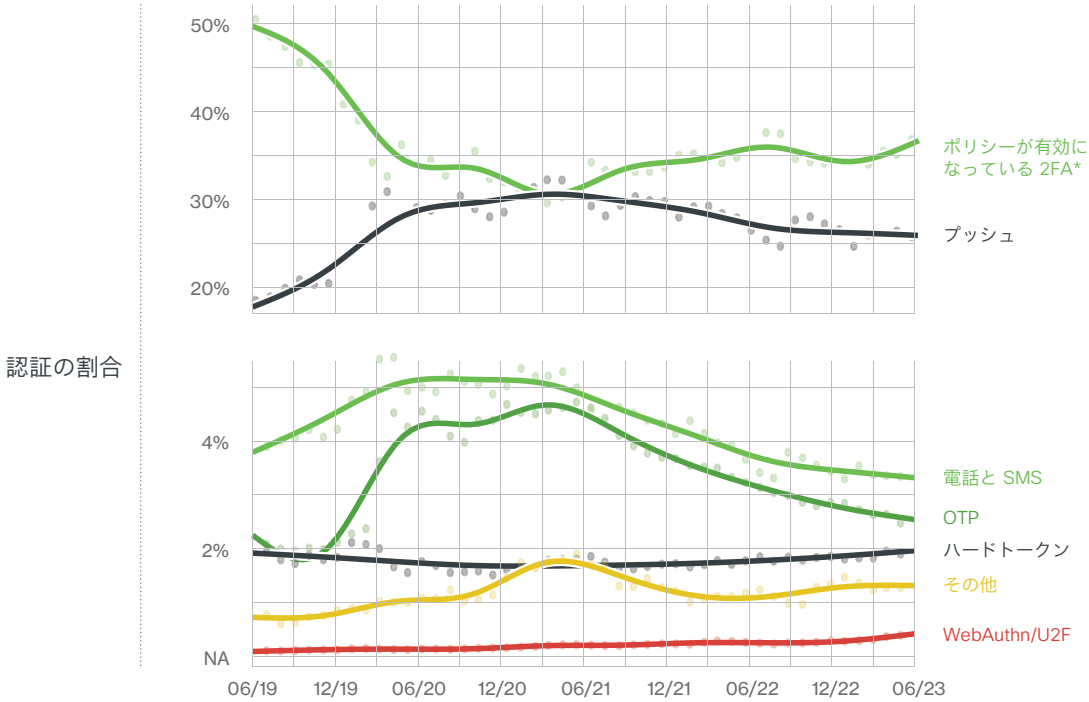


図 02 要素数ごとの認証率の推移

* このコンテキストでは、ポリシーが有効になっている 2FA には、アカウントで**バイパスステータス**が割り当てられたユーザーまたは Duo 記憶デバイスが有効になっているユーザーの認証が含まれます。これにより、シームレスで中断のないログインエクスペリエンスを維持しながら、ユーザーに強力な認証を提供します。Duo の**リスクベースの記憶済みデバイス機能**は、リスクの兆候に応じて記憶済みデバイスセッションの期間を調整することで、Duo の記憶済みデバイス機能のセキュリティを強化します。

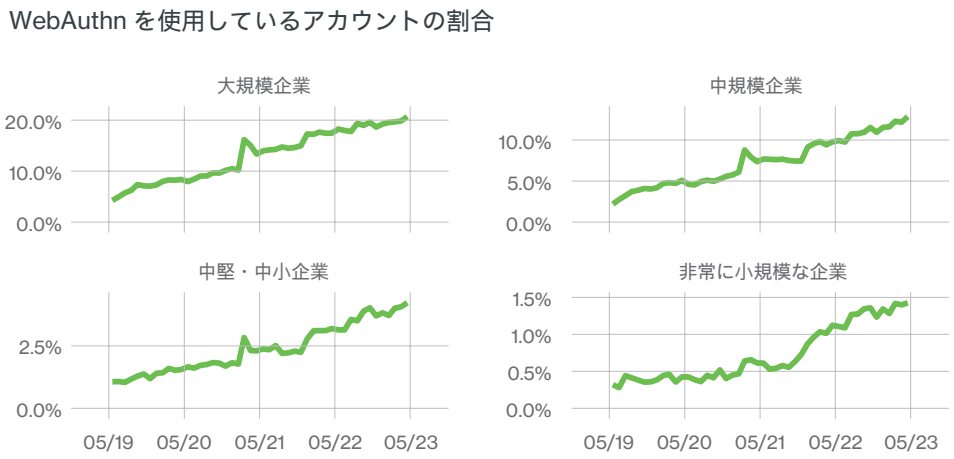


図 03 認証に WebAuthn を使用しているアカウントの割合

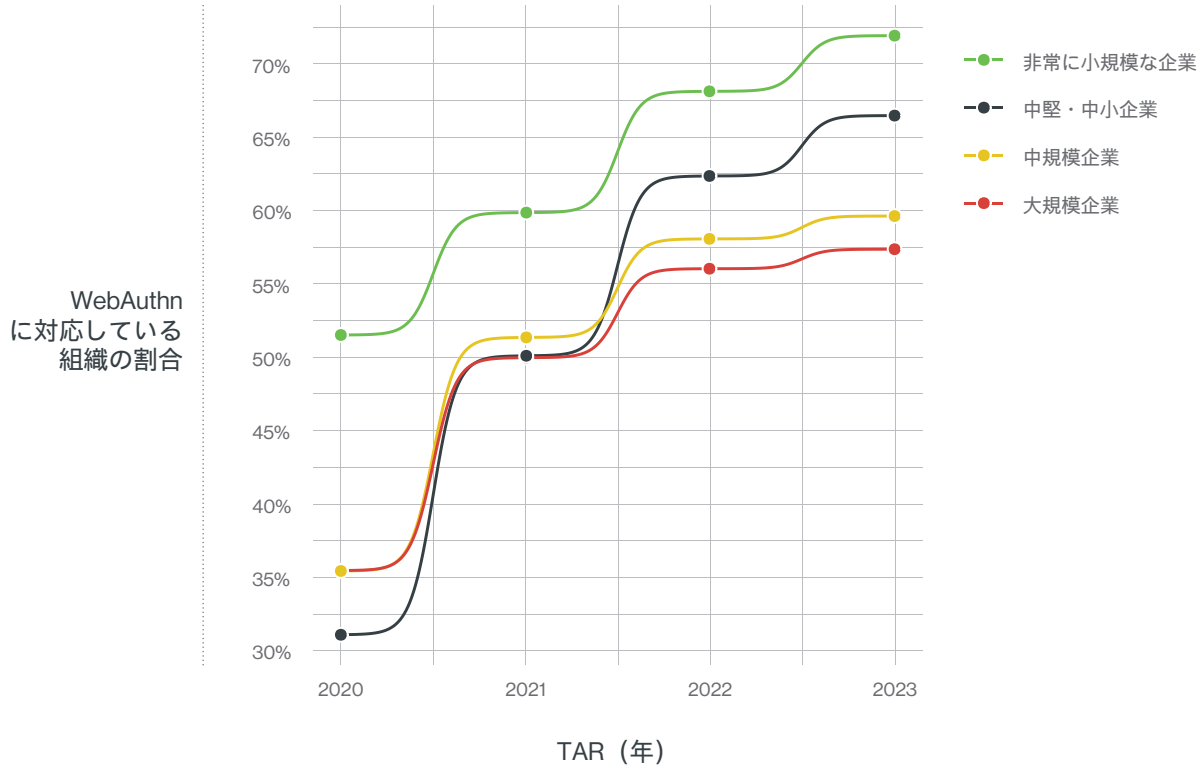


図 04 市場セグメント別の WebAuthn の導入状況

幸いなことに、**Duo Mobile** のような認証アプリケーションは、セキュリティの強化と使いやすさの両方のニーズに対応しています。91.5% のアカウントで Duo Push が有効になっています 。Duo Push は Duo Mobile アプリケーションで利用できるワンタップ認証で、全認証の 21% (32 億件以上）を占めています。また、SMS テキストと電話を認証要素として使用した認証は減少傾向にあり、4.9% (2022 年から 22% 減少）と過去最低水準にまで落ち込みました。それらに代わって WebAuthn やハードトークンなどのより安全な方法が導入されるようになっています。フィッシングに強い MFA とよりスマートなアクセスポリシーの利点が中小企業や大企業の間で注目されています。

オフィス勤務の再開がハイブリッドワークの新たな現実に

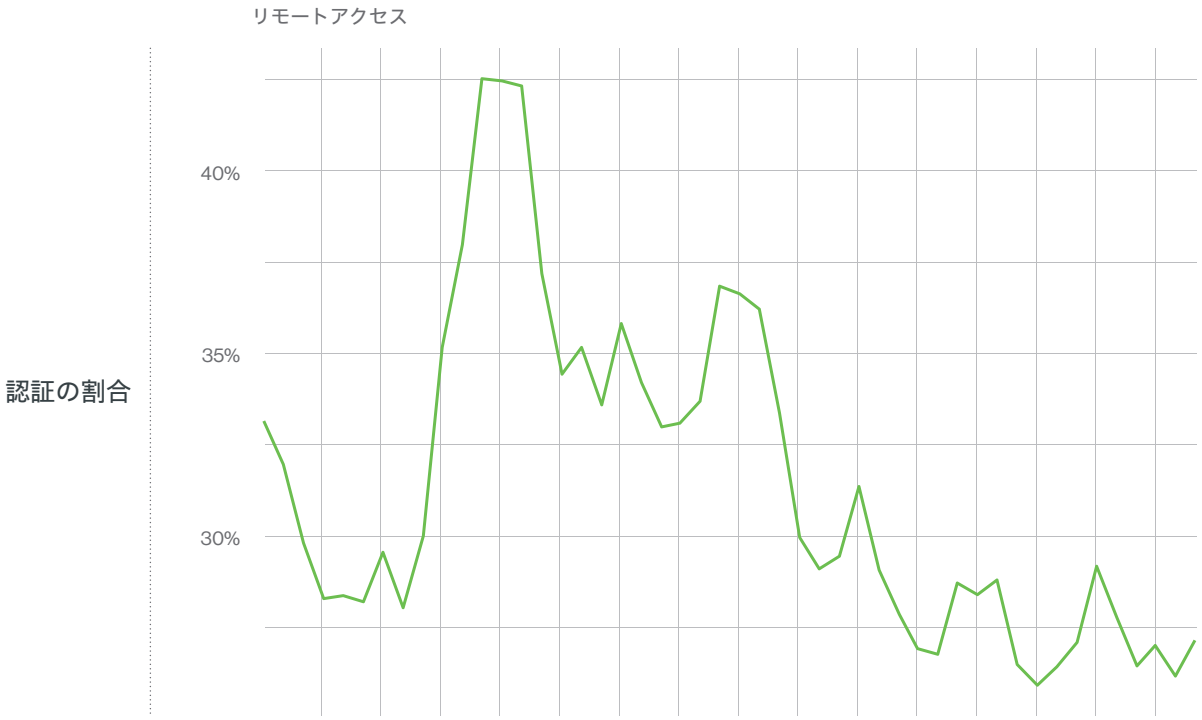


図 05 リモート アクセス アプリケーションの認証

リモート アクセス アプリケーションとは、ユーザーがインターネットまたはローカルネットワーク接続を介して別のコンピュータまたはネットワークにリモートからアクセスして制御できるようにするソフトウェアアプリケーションです。これらのアプリケーションは、トラブルシューティング、ファイル転送、リモート管理、またはオフィスのコンピュータ上のファイルやソフトウェアへのリモートロケーションからのアクセスなど、さまざまな目的で使用されます。

昨年、リモート アクセス アプリケーションの認証数は約 25% でした。2020 年がピークで、その後はパンデミック前のレベルを下回っています。従業員のオフィス勤務を再開する企業が増えたため、以来このカテゴリの認証件数は減少し続けています 。12 月から 1 月にかけての休暇期間中は、全体的に認証件数が減少しましたが、教育、小売、医療などのいくつかの業界では第 1 四半期に認証件数が急増しました。

状況の考察

出張が再開されたり、オフィス内でのポリシーが指定されたり、あるいはインフルエンザの季節が到来したりすると、予測可能な認証リクエストの増減の波が変動し始めます。従業員が休暇を取得したり、テレワークをしたり、さまざまなスケジュールで業務を行ったりすると、リズムが変わります。こうした変化に伴い、リモートアクセス要求が急増する可能性があります。従業員は、通常の作業用端末だけでなく、さまざまな場所やデバイスから企業ネットワークにアクセスするようになります。その結果、IT システムは、VPN やその他のリモート アクセス テクノロジーへの依存度を高め、オンプレミスとオフサイトが混在するログイン試行の急増に対応する必要があります。

さらに、季節性の変動により、企業が規模の拡大に伴う需要に対応するために、臨時職員が増加する可能性もあります。この急増により、追加の一時的なログイン情報を作成して管理する必要が生じるため、認証システムへの新しいエントリの波が発生します。季節が終わると、これらの季節限定のログイン情報は取り消されるため、それに対応する流出が発生します。

この違いは、認証の量だけでなく、その性質も変化させます。こうした時期にサイバー脅威のリスクが急増することが多いため、堅牢なセキュリティ対策の必要性が高まります。そのため、階層化されたセキュリティアプローチがさらに重要になります。MFA は最低必要条件です。

これらのピーク時に、IT 環境の認証プロトコルは、システムの完全性を維持しながら、負荷の増加や変化に対応できるように拡張し、柔軟かつ安全である必要があります。IT スタッフは、侵害の試みを示唆する異常なアクティビティがないか常に警戒しています。

将来を見据えた攻撃対策

アイデンティティの脅威は急速に進化しており、信頼できるアイデンティティ プロバイダーが攻撃にさらされています。CISA によると、攻撃者は重要なアプリケーションにアクセスするためにアイデンティティポリシーのギャップを積極的に悪用しようとしています。リスクが高まっているにもかかわらず、『シスコ セキュリティ成熟度指標』[3] の調査によると、85% の組織は、最新の攻撃を防ぐ準備が整っていないと感じています。

仕掛けられるさまざまな攻撃に対処するには、アイデンティティ インフラストラクチャ全体の可視化が不可欠です。Duo による MFA 認証は大幅に増加していますが、別の調査によると、市場全体には依然としてセキュリティギャップが存在しています。平均的な企業のアカウントの 40% が、MFA を使用していないか、脆弱な MFA をしています[4]。特に変動が発生する時期には、強力なアクセス管理とアイデンティティの可視性が重要になります。一時的にはバランスがとれても、新たに脅威が出現したり、ユーザーの行動が変化したり、IT 環境が複雑であったりすれば、結局はバランスが崩れてしまいます。

そのため、セキュリティについての最新の取り込みでは、アイデンティティ、重要なアプリケーション、人事情報システム (HRIS) 全体の継続的なモニタリングが必要となっています。セキュリティ環境の進化に伴い、多くの企業は、最新の攻撃対象領域を減少させるために、ゼロトラスト アクセス ポリシー戦略を採用しています。成熟したゼロトラストを導入している組織は、ゼロトラスト戦略を導入していない組織よりもセキュリティレジリエンスが 30% 高くなっています[5]。

2023 年は、プッシュベースの認証と受け身なユーザーを利用して MFA を狙う、次の 2 種類の攻撃が急増しました。

01

プッシュハラスメント

プッシュ通知を複数回続けて、不正なログイン試行のプッシュ通知をユーザーに受け入れさせます。

02

プッシュ疲れ

常に MFA を使用しているうちに、ユーザーがログインの詳細に注意を払わなくなり、無意識にプッシュログイン要求を受け入れてしまうようになります。

Duo は、MFA ベースの攻撃に対して最も強力な保護を提供する WebAuthn FIDO2 オーセンティケータをすでにサポートしています。しかし、組織全体にパスワードレスを導入するのは大変な作業になることでしょう。このレポートのデータ収集期間中に、すべての Duo ユーザーがより柔軟なステップアップ認証である Duo Verified Push の一般利用が始まりました。5,600 を超えるアカウントで有効化されていることは、心強いニュースです。

攻撃の手口が高度化するにつれて、多層防御システムが不可欠になっています。

ユーザーを信頼することは重要ですが、それで十分とは言えなくなっています。外部ベンダーや請負業者が加わることで、エンドポイントのみのクローズドな管理型アクセスポリシーは複雑になります。**Duo Trusted Endpoints** は、Duo のすべてのエディションで利用できます。組織がデバイスを直接管理できない場合でも、セキュリティを強化できます。管理者は、管理対象かどうか、会社支給、請負業者所有、個人所有のいずれかにかかわらず、すべてのエンドポイントに対して信頼ポリシーを定義できます。MFA がバイパスされた場合でも、攻撃者が使用する不明なデバイスを阻止できます。

負担の増加は、多くの場合、ユーザーの利用に伴う課題として認識されます。セキュリティと生産性のバランスを図る取り組みの一環として、リスクの変化に対応できるように **Duo の記憶済みデバイス機能**を拡張しました。ユーザーが使用しているデバイスを認識すると、信頼が維持されている限り、安全に生成されたデバイストークンを使用して認証が行われます。

アクセスセキュリティはリスクのレベルに合わせて調整する必要がありますが、ログインのたびに手間がかかることについて、組織が賛同を得るのは、なかなか難しいことです。Duo の**リスクベースの認証**ソリューションは、この課題に対処します。環境のリスクシグナルが、ロケーションの異常や既知の攻撃パターンなどの潜在的な脅威の存在を示している場合にのみ、より安全な方法に移行します。セキュリティチームが**検証済み Duo Push** をすべてのユーザーに対して有効にするか、リスクベースのアプローチで有効にするかに関係なく、組織はリスク選好と組織のニーズに基づいてアクセスセキュリティを決定できます。

IT チームは、アイデンティティ セキュリティ プログラムが、強力な MFA による認証やインテリジェント ステップアップなどの適切なツールを備えた強力な基盤の上に構築されていることを確認する必要があります。これらのツールとポリシーを導入すると、**アイデンティティ脅威の検出と対応** (ITDR) により、IT セキュリティ プロフェッショナルはプロアクティブな機能とリアクティブな機能の両方を備えたツールを利用できるようになるため、組織のアイデンティティ セキュリティ態勢を強化できます。

ITDR は、ポリシーの設定不備、アイデンティティ プロバイダーと HRIS の不一致、過剰な権限の付与をプロアクティブに検出するのに役立ちます。また、休眠アカウントや非アクティブなアカウント、MFA が無効になっているアカウントなどのリスクの高いシナリオも検出できます。この傾向は、Cisco Talos の 2023 年版『一年の総括』レポート [6] で指摘されています。またリアクティブな機能として、IT チームはこのツールを使用して、新しい MFA デバイスの登録、リスクの高い SSO セッション、スーパーマン (非現実的な移動) によるログイン、新しいデバイスやロケーションからのアクセスなどの不審なアクティビティに対応できます。

注釈：

3.『**シスコ サイバーセキュリティ成熟度指標**』を参照。この指標では、5 つの重要な柱に対する企業の準備体制と、その中の 19 のセキュリティソリューションの導入状況に基づいて、企業の成熟度を「初歩 (Beginner)」、「形成 (Formative)」、「進展 (Progressive)」、「成熟 (Mature)」の 4 段階に分類

4.『**アイデンティティ セキュリティの状態』レポート** (Oort 社) のセクション 2「多要素認証：フルカバレッジは今もなお困難」を参照

5. シスコによって公開された**セキュリティ成果レポート Vol 3** (Renner 社) の調査結果の詳細を参照

6.**Cisco Talos『一年の総括』**の全文を参照

攻撃対象領域の拡大

02

MFA の使用が世界的に引き続き増加

Duo の多要素認証セキュリティによって保護されている世界中のカスタマーベースが拡大し続けていることをデータが示しています。Duo を使用する MFA 認証の数は、この 1 年間で 41% 増加しました。認証件数が前年比で 52.3% 増加したドイツのような国々もあります。アジア太平洋地域では、日本、フィリピン、オーストラリアで昨年から引き続き増えており、それぞれ 28%、24.9%、16.9% の増加となっています。測定が開始された最初の 1 年で、ブラジルは認証件数の増加率第 3 位を記録しました。2022 年と比較して MFA の使用量が 26.3% 増加しています。

このことから、セキュリティ対策の強化の重要性が認識される傾向が高まっていることがわかります。主にサイバー脅威の増加への対応と考えられますが、GDPR、C5、AgID、HIPAA などの国際的なコンプライアンス要件が反映された結果でもあります。

41%

この 1 年間における Duo を使用した MFA 認証の増加

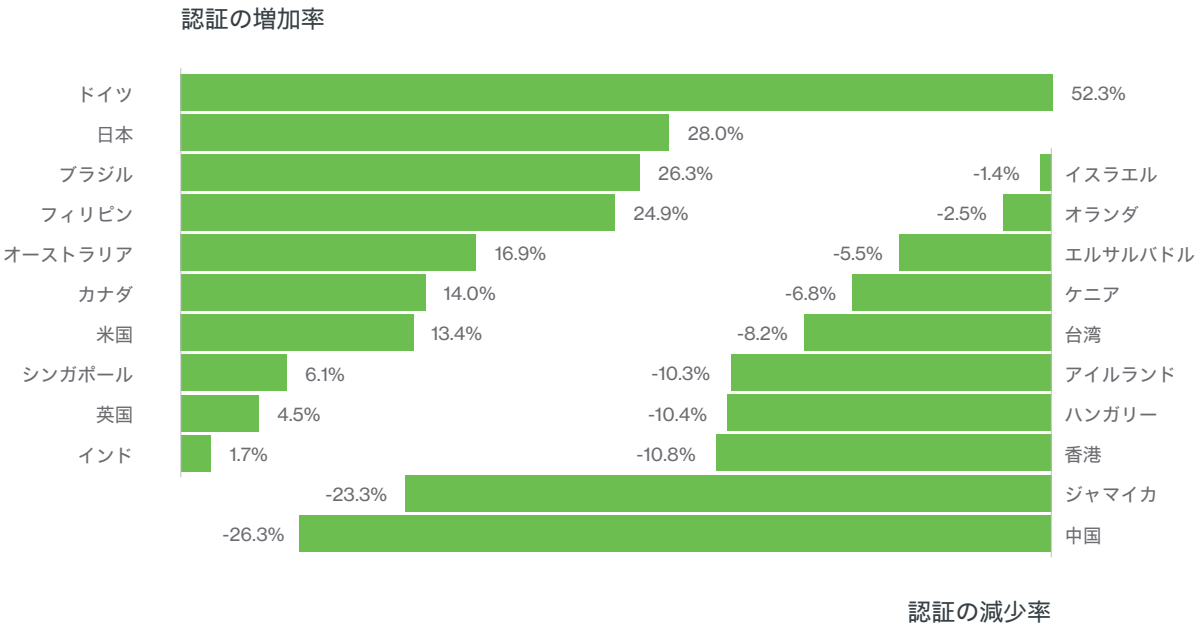


図 06 アクセスデバイスの IP アドレスに基づいて認証件数が増減した上位 10 か国

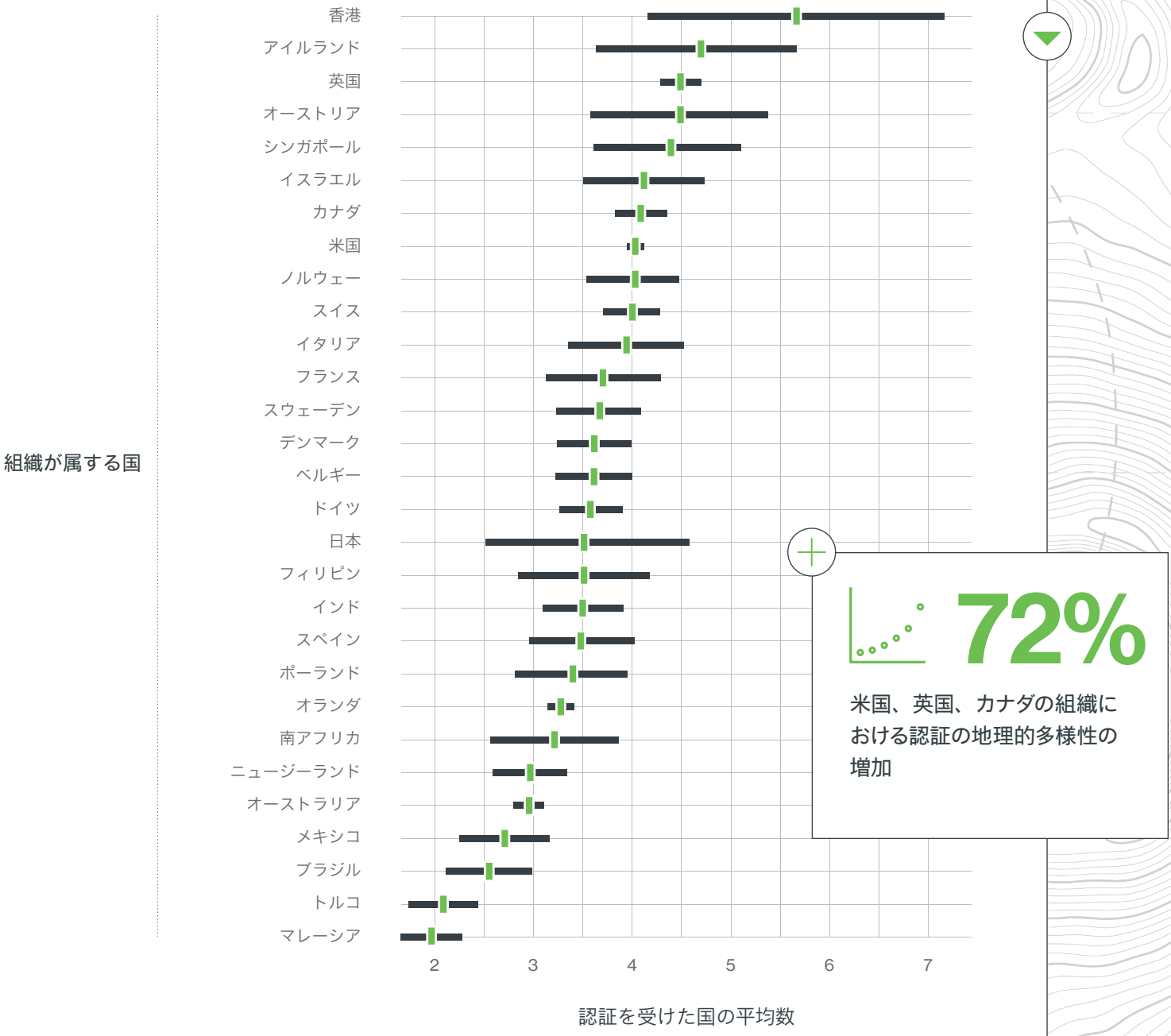


図 7 特定の国の組織によってアクセスされたさまざまな国の平均数

図 7 では、昨年確認した統計情報を再掲しています。これは、組織が活動する地理的な多様性を示しています。特に、ユーザーが認証を行っている国の平均数に注目します。例として、香港にある組織に注目してみましょう。香港ではビジネスの多様化と分散が続いているため、認証の分散状況は平均して 5.6 か国と最も高くなりました。米国、カナダ、英国の組織では、平均 4 か国から認証が行われています。これは、昨年の平均 1.5 ~ 1.75 か国から 72% 増加しています。

従業員が国際的に分散するということは、より多くの従業員、請負業者、クライアント、および第三者が、さまざまな場所から組織のデジタル インフラストラクチャにアクセスする可能性があるということです。多くの場合、デバイス、ネットワーク、オペレーティングシステムが異なるため、脆弱性が増す可能性があります。データとリソースにも、より大規模なネットワークとエンドポイントからアクセスされる可能性があります。これは、「アイデンティティは新たな境界」であり、「コンテキストは新たな MFA」という概念の裏付けになるでしょう。アイデンティティ セキュリティは永遠に進化し続ける問題であり、ユーザー ジャーニーにおいて生じるすべての問題に対応することは組織にとって容易ではありません。

さらに、国際的な存在感により、テクノロジースタックの多様性が高まるだけでなく、地理的に多様なユーザーベースが抱える物理的な課題もさらに広範にわたる可能性があります。また、IT システムは、さまざまなテクノロジースタックや、さまざまなデータ保護法やプライバシー法に対応する必要があります。これにより、IT チームが対処しなければならない複雑さがさらに高まっています。

組織の規模と同様に、グローバル化によって、複数のアイデンティティ プロバイダーが存在する可能性が高まります。さらに、大規模な組織が他社を買収したところ、利用していたアイデンティティ プロバイダーがそれぞれ異なるという場合もあるでしょう。1 つのアイデンティティ プロバイダーにすべてを統合すると複雑で混乱を招く可能性があるため、組織によっては複数のアイデンティティ プロバイダーを維持することを選択する場合もあります。

複数のアイデンティティ プロバイダー (IdP) をサポートする可能性が高くなるため、アイデンティティの管理はますます複雑になります。適切なセキュリティ対策が講じられていないと、セキュリティギャップや脆弱性が発生し、ログイン情報の侵害などのアイデンティティベースの攻撃に悪用される可能性があります。

グローバルなビジネスプラクティスでは、攻撃の検出、対応、レポートを支援する、ベンダーに依存しない広範なアクセス管理が必要です。

アイデンティティは新たな境界

アイデンティティ セキュリティは、アクセス管理の重要な要素です。アイデンティティとアクセスの管理 (IAM) システムでアイデンティティを保護して検証することで、リソースへのアクセスを効果的かつ安全に管理できます。よって、このレポートをまとめる際に明らかになったアイデンティティ セキュリティのトレンドについて、ここで説明しておく必要があるでしょう。

アイデンティティ セキュリティにギャップが生じる理由はいくつかあります。一部の企業では、クラウドへの移行がきっかけとなっています。企業が成長して運用をクラウドに移行するのに伴い、新しい IAM システムの導入が必要になることがよくありますが、古い IAM システムを完全に廃止することはできません。オンプレミスのディレクトリからクラウドベースのディレクトリに移行する企業もありますが、両方を維持する企業もあります。また、1 社以上の企業を買収したため、多数のアイデンティティ プラットフォームをサポートしている企業もあります。

もう 1 つの要因は、運用上の課題です。アイデンティティ セキュリティは多くの場合 IT 機能に分類されるため、効果的に運用するために必要な注意やリソースが不足する可能性があります。IAM システムの管理と継続的なモニタリング、規制へのコンプライアンスの確保、セキュリティインシデントへの対応を行うには、テクノロジーと人材への投資が必要です。

クラウドへの移行や組織の拡張には、新しい IAM システムの導入が必要な場合もあります。合併や買収、運用のグローバル化、地理的に多様なユーザーベースにより、アイデンティティ認証の追跡はさらに複雑になっています。

デジタル トランスフォーメーションに際しては、アイデンティティ セキュリティは、通常セキュリティ機能ではなく IT 機能に分類されるため、リソース不足や優先順位の低さのせいで苦しい状況に陥る可能性があります。適切な可視性と脅威検出がなければ、アイデンティティ インフラストラクチャは攻撃者にとって重要なシステムに侵入する絶好の機会となります。アイデンティティは従来、組織の IT チームによって管理されてきました。アイデンティティは最大の攻撃ベクトルであるため、アイデンティティチームとセキュリティ オペレーション センター (SOC) を連携させて ITDR を活用し、全員が同じ情報を共有できるようにすることが重要です。-

適切な可視性と脅威検出がなければ、アイデンティティ インフラストラクチャは攻撃者にとって重要なシステムに侵入する絶好の機会となります

Talos の視点

サイバー攻撃者は俊敏であり、多くの場合、国家による支援など潤沢なリソースに支えられています。その結果、アイデンティティを標的にして機密情報にアクセスする APT (Advanced Persistent Threat) 攻撃が増加しています。

しかし、これは目新しいことではありません。攻撃者は長年にわたってアイデンティティを標的とした攻撃を展開しています。たとえば、追加の保護機能がないオンプレミスのアイデンティティ ディレクトリや VPN は、さまざまな攻撃の標的になってきました。管理するアイデンティティの範囲が広がっていることは、攻撃対象領域が広がっていることの表れでもあります。Talos インシデント対応チーム (Talos IR) は、攻撃者がベンダーや請負業者のアカウント (VCA) を標的にするのを繰り返し目にしてきました。VCA の権限とアクセスは、通常拡大されています。サードパーティへの信頼ゆえに、VCA はアカウントの監査で見落とされることが多く、攻撃者にとって格好の標的となっています。

Talos の 2023 年版『一年の総括』レポートによると、有効なアカウントのログイン情報の侵害が初期アクセスベクトルの 23% を占めており、有効なアカウントの使用は MITRE ATT&CK 手法の中で 2 番目に多くなっています[7]。重大な脆弱性の 1 つは、MFA が不適切に導入されているか、または導入が不十分であることですが、対応事例の中には、MFA 疲れやプッシュボム攻撃によって MFA を回避していたものもありました。ITDR を使用すると、有効なアカウント攻撃に関連するリスクを明らかにし、HRIS から取得した情報をアイデンティティ プロバイダーや重要なアプリケーションに関連付けることができます。これにより、盗まれやすい状態のログイン情報を狙った攻撃を軽減できます。

23%

侵害された有効なアカウントログイン情報が最初のアクセスベクトルとなった割合

アイデンティティスプロール

組織は、同期されていない複数のシステムで管理されているアカウントとアイデンティティをユーザーが大量に持ってしまう「アイデンティティスプロール」に苦慮しています。これは、多くのセキュリティチームと IT チームにとって、継続的なセキュリティリスクと運用上の課題となっています。

アイデンティティスプロールはますます大きな課題となっています。Talos IR による調査では、ログイン情報が従業員の個人デバイスなど会社の目が届かないデバイスから入手されたとなると、ログイン情報が侵害された方法を突き止めるのは容易ではないと指摘しています。あるレポートによると、企業は平均 340.5 の個人アカウント (Gmail、Yahoo、Hotmail、iCloud など) を所有しており、それらのアカウントから企業データにアクセスしています[8]。BYOD や境界のない働き方の文化により、従業員のアイデンティティがチェックされない、または管理されないままになっているケースが増えています。

340.5

企業データにアクセスする個人アカウントの平均

注釈：

7.Talos IR の 2023 年版『一年の総括』の「テレメトリの動向」(6 ~ 7 ページ) を参照

8.『アイデンティティ セキュリティの状態』レポート (Oort 社) のセクション 3「アイデンティティとアクセス管理 : 不十分な対策が攻撃者に狙われる」を参照

03 デバイスの信頼性の確立

無数のデバイスを可視化して保護することは、特に高等教育機関のようにエンドポイントの多様性が非常に大きい組織や業界において、今もなお継続的に行われている取り組みです。強力な認証メカニズムは、セキュリティプロトコルの中核であり、ネットワークにアクセスするユーザーのアイデンティティを確認するための重要な防御線です。ただし、堅牢な認証は、サイバーセキュリティ対策の一角にすぎません。

ユーザーが信頼できるデバイスとネットワークを使用して企業データにアクセスするようにすると、複雑さがさらに増します。サプライチェーンの運用が複雑で、サードパーティとのパートナーシップがあり、請負業者のデバイスがある IT 環境では、管理されていない外部デバイスや不明なエンドポイントのリスクが発生します。このようにさまざまな状況に対応しなければならないため、専用のセキュリティレイヤを構築せずに可視性と信頼性を保証することは、不可能ではないにしても決して容易なことではありません。強力なエンドユーザー認証があっても、ネットワークとデバイスのセキュリティが管理されていないという不確実な状況は、依然として脆弱なままです。

このような状況において、アイデンティティ中心のセキュリティは、動的で多面的な取り組みです。これには、高度な認証、ネットワーク セキュリティ ソリューション、エンドポイント保護、継続的なモニタリングを統合した、包括的で適応性のある戦略に加え、情報に通じ誠実に働くワークフォースが必要です。

多様なデバイス環境

デバイスの信頼確立の第一歩は、デバイス自体 (オペレーティングシステム、使用しているブラウザ、パッチレベル、企業のセキュリティポリシーへのコンプライアンス) を包括的に理解することです。デバイスのセキュリティ態勢は、OS とブラウザの最新性と整合性に大きく影響されるため、この理解が重要となります。古いソフトウェアはパッチが適用されていない脆弱性だらけのため、エクスプロイトの格好の的となり、何の変哲もないデバイスがネットワーク内でトロイの木馬に変わってしまう可能性があります。

デバイスを信頼できるものと見なせるかどうかを判断するために、IT チームとセキュリティチームは、いくつかの重要な質問に答える必要があります。

- 不正なアプリケーションやソフトウェアが存在しますか？
- デバイスは暗号化されていますか？また、企業の規格に従ってセキュリティ設定が構成されていますか？
- デバイスで実行されている OS は何ですか？
- この OS は現在もサポートされており、セキュリティアップデートを適用できますか？
- インストールされているブラウザのバージョンは何ですか？また、自動更新されるように設定されていますか？

まず、Duo のお客様が使用しているブラウザと OS を見てみましょう。

モバイルおよび非従来型のオペレーティング システム プラットフォームは着実に導入されており、測定された認証の 61.8% を占めています。Windows は依然として上位を占めていますが、混在 IT 環境では、プラットフォームに依存しないセキュリティの検討が必要になる可能性があります。

利用頻度上位の OS		モバイル OS の利用状況	
Windows :	38.2%	**iOS :**	71.7%
iOS :	33.4%	**Android :**	28.2%
Mac OS X :	13.7%	**Windows :**	0.0%
Android :	13.1%		
Chrome OS :	1.1%		
Linux :	0.45%		

Windows が引き続き群を抜いて首位を占めていますが、2 番手の iOS が 33.4% と首位に迫る割合を占めており、注目されるところです。Apple はモバイルカテゴリで常に最高の使用率を誇り、2 番手は Android ですが、使用率は 28.2% とはるかに低くなっています。

Chrome が支配を継続

Google Chrome が引き続き企業で最も多く利用されているブラウザとして優勢な状況を維持しています。これに迫るブラウザさえありません。

利用頻度上位のブラウザ

Chrome :	41.7%	**Chrome Mobile :**	7.7%	**Firefox :**	3.3%
Mobile Safari :	13%	**Mobile Safari Webview :**	4.7%	**Chrome Mobile iOS :**	2.9%
Edge Chromium :	12.6%	**Safari :**	4.6%	**Edge :**	0.1%

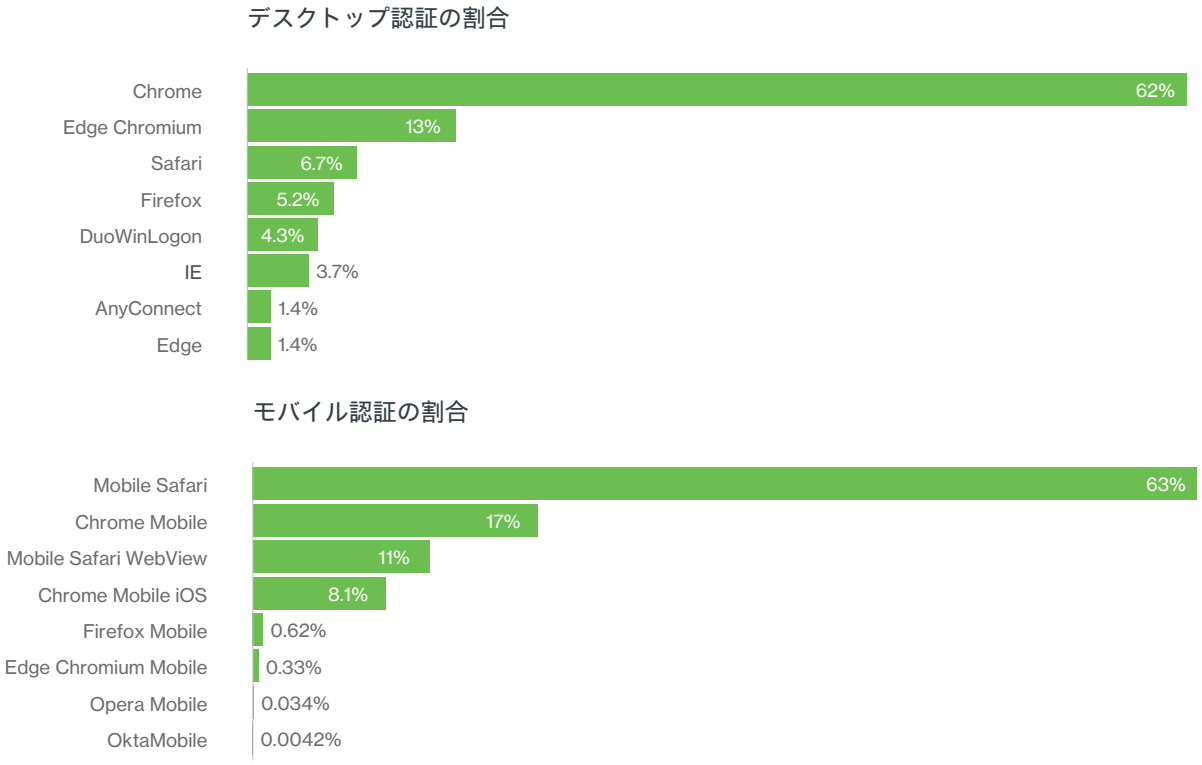


図 8 認証に使用されるさまざまなブラウザ

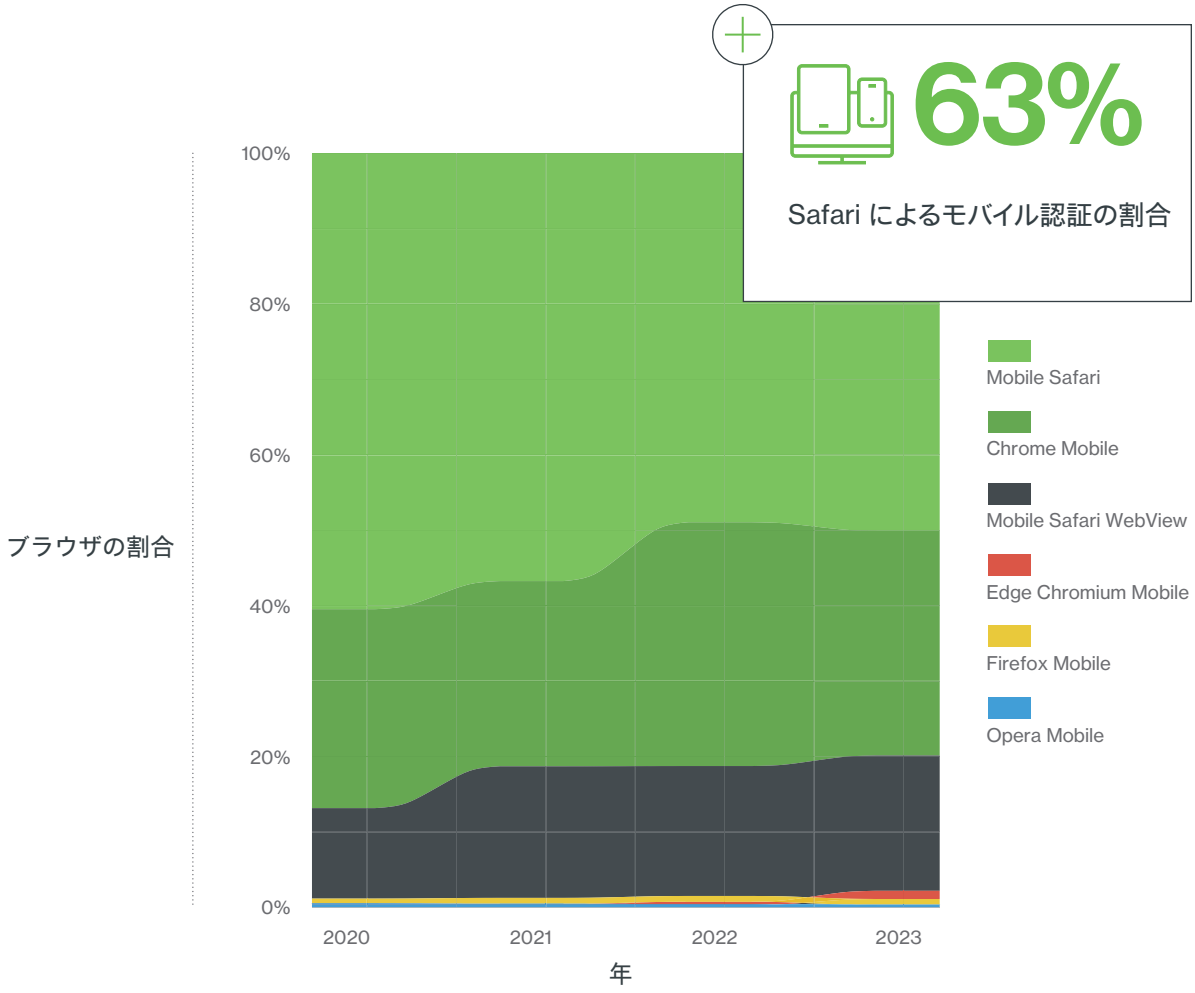


図 9 使用されているモバイルブラウザの割合

多様なシステムとブラウザを使用する IT 環境では、より厳格なデバイスベースのポリシーを導入することが急務となっています。

デバイスの可視性：見えないものを保護

デバイスの信頼性を維持することは継続的なプロセスであり、定期的な評価と更新が必要です。これには、アクセスを許可する前に、デバイスが設定されたパラメータ内で動作しているかどうかを検証する自動コンプライアンスチェックが含まれる場合があります。サポートが終了したバージョンの OS を実行しているなど、デバイスに問題がある場合は、レビューのためにフラグを設定したり、機密リソースへのアクセスをブロックしたり、アクセスを制限および制御して潜在的なリスクを軽減したりできます。

こうした対応は、Google Chrome などのアプリケーションやブラウザがパッチを適用する頻度を増やし、パフォーマンスとセキュリティのバグ修正を毎週行うようになっている状況で重要なことと言えます。では、どのくらいの頻度でアプリケーションは再起動および更新されているのでしょうか。測定された 160 億件の認証のうち、モバイル以外の認証の 62% は Chrome ブラウザを利用して行われています。アクセスデバイスのパッチレベルを確認し、古いデバイスを自己修復するようユーザーに促す機能は、ますます重要になっています。

可視性は、さまざまなツールとプラクティスによって実現できます。たとえば、エンドポイント管理システムには、ネットワークに接続されているすべてのデバイスのステータスに関するリアルタイムのインサイトを提供するダッシュボードがあります。自動インベントリツールにより、使用中のデバイス、ソフトウェアバージョン、パッチ履歴を追跡できます。このモニタリングは、継続的な管理だけでなく、潜在的なセキュリティインシデントに迅速かつ正確に対応するためにも不可欠です。

古いソフトウェアによる認証

古いソフトウェアを搭載したデバイスによる認証失敗

古いソフトウェアを搭載したデバイスによる認証失敗の割合は、2023 年に 74.7% 増加しました。古いソフトウェアを搭載したデバイスを管理するポリシーを導入している組織の割合が 6.9% 減少しているにもかかわらず、このような結果になっています。アジア太平洋地域が最も高く、認証の 3.8% が古いブラウザで行われています。

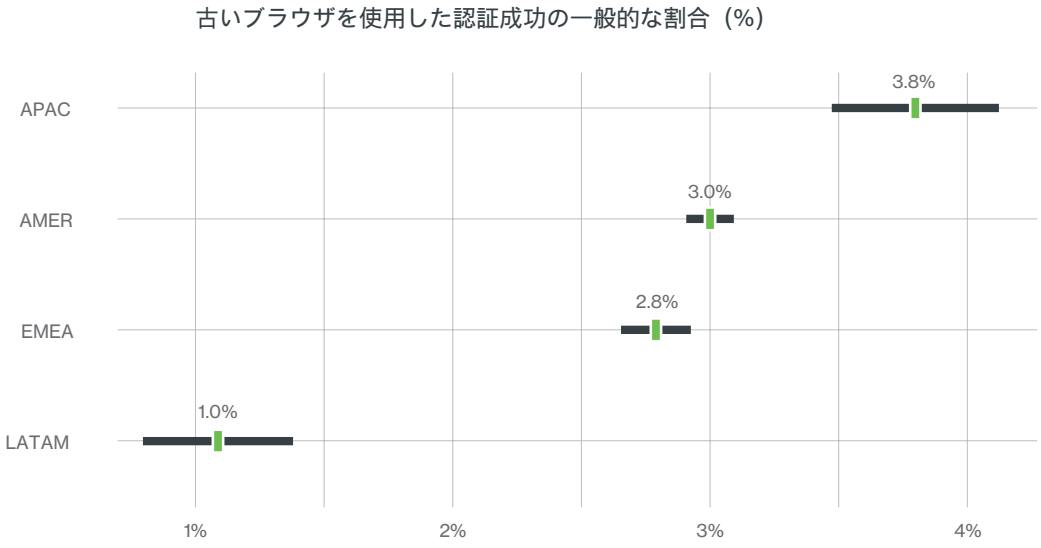


図 10 古いブラウザを使用した認証成功の一般的な（幾何平均）割合

デバイスの信頼性の中核を成すのは、企業のアプリケーションやデータへのアクセスを要求しているデバイスの完全な可視化です。地理的にもデジタル脅威が拡大し続ける中で、古いソフトウェアに依存した IT 環境内で認証を行うことは、古い地図を持って船を航行するようなものです。

古いソフトウェアには、多くの場合、パッチが適用されていない脆弱性が含まれています。これらは、サイバー攻撃者にしてみると、裏でバックドアが開いているようなものです。これらの脆弱性は詳細に文書化されており、パブリックドメインで公開され続けるため簡単に悪用でき、攻撃者が不正アクセスを行うための宝の地図となります。こうしたシナリオでは、各認証イベントはいわばギャンブルのようなものになってしまい、セキュリティ上の欠陥を利用してログイン情報が流出する可能性が高くなります。

さらに、サポート期間が終了したソフトウェアは、開発者から更新プログラムを入手することはできなくなります。つまり、新しい脅威が出現しても、認証メカニズムは変化しないままであるため、現代のサイバー攻撃者が使用する高度な手法に対する効果がますます失われていくということです。これでは、動的な攻撃に対して静的な防御をしているようなものです。

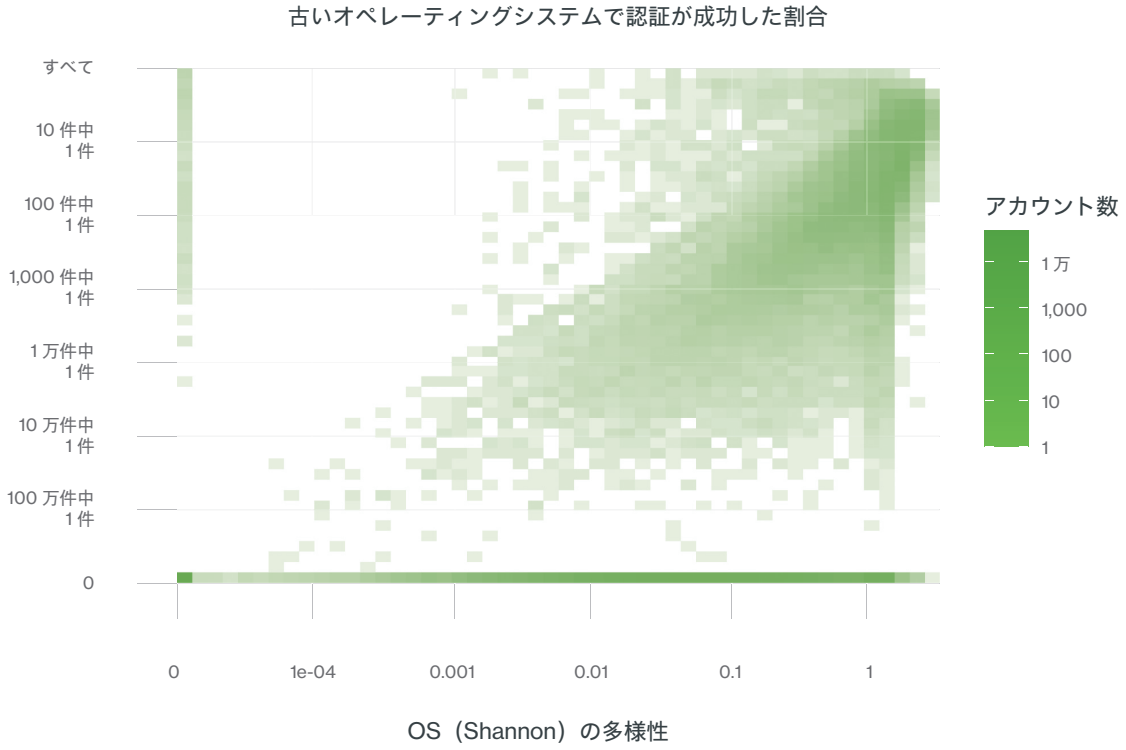


図 11 OS の多様性と、古いオペレーティングシステムを使用した認証の割合

横軸は、さまざまな OS が組織内の認証でどれほど「多様」（生態学的な意味）に使用されているかを示しています。数値が大きいほど、同じ割合の認証を共有する OS の種類が多いことを意味します。縦軸は、古い OS を使用して行われた認証の割合です。下部の横線は、OS を最新の状態にする組織を示し、左側の縦線は、単一の OS のみを使用する組織を示しています。

図 11 のデータに基づく相関関係から、認証を許可するオペレーティングシステムが多いほど、古い OS で認証が行われる可能性が高くなることがわかります。これは、IT 環境を拡大している企業にとって、急速に現実味を帯びてきました

古い認証ソフトウェアに依存することは、セーフティネットなしで綱渡りをするようなものです。セキュリティ侵害やデータ窃取の原因となり、それに続いてさまざまな被害を招く可能性があります。IT 環境の安全性と効果を維持するには、デジタル脅威の状況に合わせて進化し、可視性を提供し、修復を可能にする、最新の堅牢なデバイスの信頼方法に投資することが不可欠です。これは単なるベストプラクティスではありません。デジタル時代における責任ある IT 管理の基本的な考え方です。

69%

暗号化の使用率の増加

暗号化とファイアウォールについて

ハイブリッドワークモデルでは、仮想プライベートネットワーク（VPN）の使用、厳格なファイアウォールポリシーの適用、データ暗号化の適用、ホームネットワークの安全なセットアップも検討する必要があります。Duo Endpoint Health について、特に組織が導入中のさまざまな保護策を一般に増やしているか減らしているかを把握すべく調査しました。組織ごとに見ると、暗号化の使用率が平均で 69% 増加したことがわかります。

デバイスの健全性は、一度設定すれば後は何もしなくてもよいというわけではなく、企業にとって進化し続ける継続要件です。この責任は、デバイスの廃棄プロセスにも及びます。すべてのデータを安全にワイプし、セキュリティ上の脅威とならない方法でデバイスを廃棄しなければなりません。同様に、ユーザーのアクセスレベルを調整して、不要な権限や過剰な権限は減らす必要があります。定期的な監査とコンプライアンスチェックにより、デバイスとアイデンティティの健全性対策が実施されているだけでなく、効果的に適用および更新されていることを確認します。

オペレーティングシステムやブラウザなど、デバイスの属性を熱心に管理および監視することで、組織は強力なセキュリティ体制を実施し、信頼がやみくもに与えられるのではなく、検証可能でコンプライアンスに準拠したデバイスの動作に基づいていることを確認することができます。

強力なポリシー制御

04

前のセクションでは、セキュリティ負債という重大な課題に焦点を当てました。組織が対処しなければならない未対処のリスクと脆弱性の蓄積です。セキュリティ負債は、古いソフトウェア、レガシーシステム、技術的なショートカット、セキュリティパッチの適用の遅れなど、さまざまな原因で発生する可能性があります。この負債を減らすことは、堅牢なセキュリティ態勢を維持し、組織が潜在的な侵害を受けるリスクを最小限に抑えるために不可欠です。

セキュリティ負債を軽減するための最も効果的な戦略の 1 つは、リスクを包括的に管理することです。これには、組織の IT インフラストラクチャ内の脆弱性の特定、評価、および優先順位付けが含まれます。最大のリスクがどこにあるのかを理解することで、最も差し迫ったセキュリティ上の懸念に真っ先に対処できるようリソースと労力をより効果的に割り当てることができ、全体的なセキュリティ負債を削減できます。

認証が失敗したタイミングから学習する

ポリシーに関するデータを確認したところ、いくつかの注目すべきことがわかりました。より強力な認証方法への移行として、Duo Push ベースの認証は、すべてのグローバルポリシーの 99.3% で使用されていました。モバイルのワンタイムパスコードは、定義されたポリシーの 91.4% に含まれていました。興味深い結果の 1 つは、WebAuthn がグローバルポリシーの 69.2% に含まれていたことです。

失敗した認証を測定することは、それと同じくらい重要です。測定されたすべての認証のうち、5% が失敗しています。このデータを詳しく検証すると、失敗した認証の 28% は、ユーザーがシステムに登録されていないことが原因でした。

69.2%

WebAuthn など、より強力な認証方式への移行が有望視されているグローバルポリシーの割合

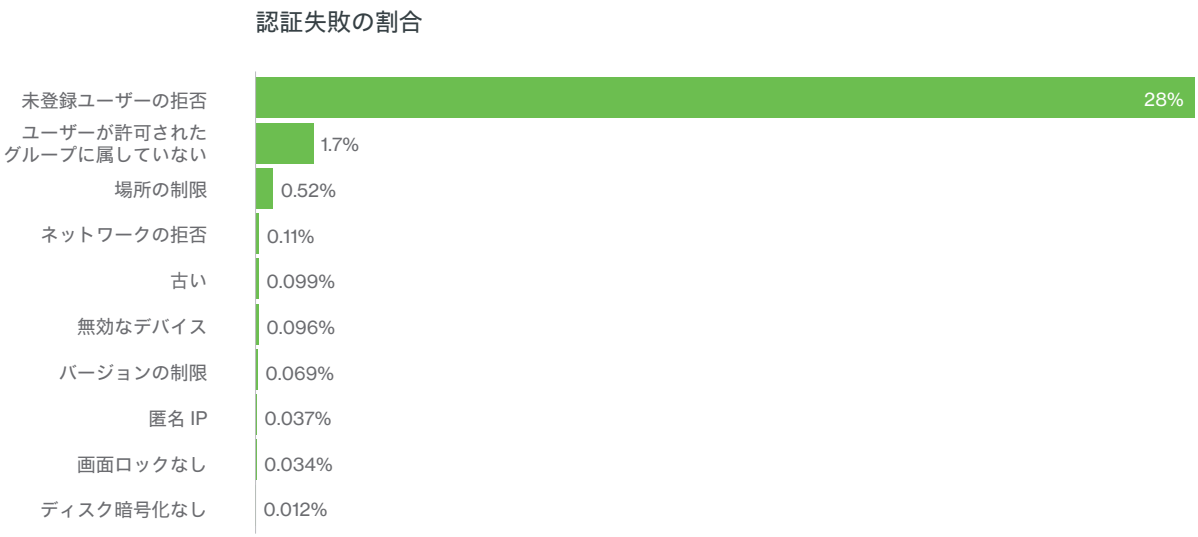
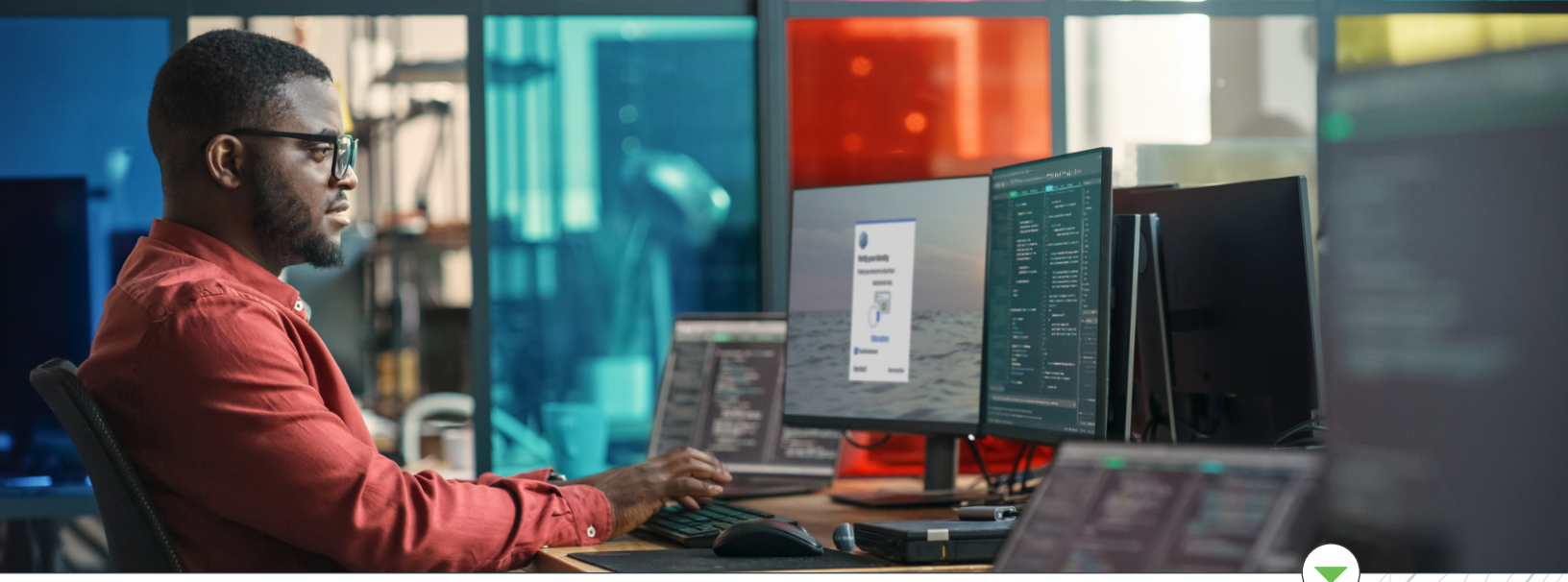


図 12 認証失敗の理由の割合



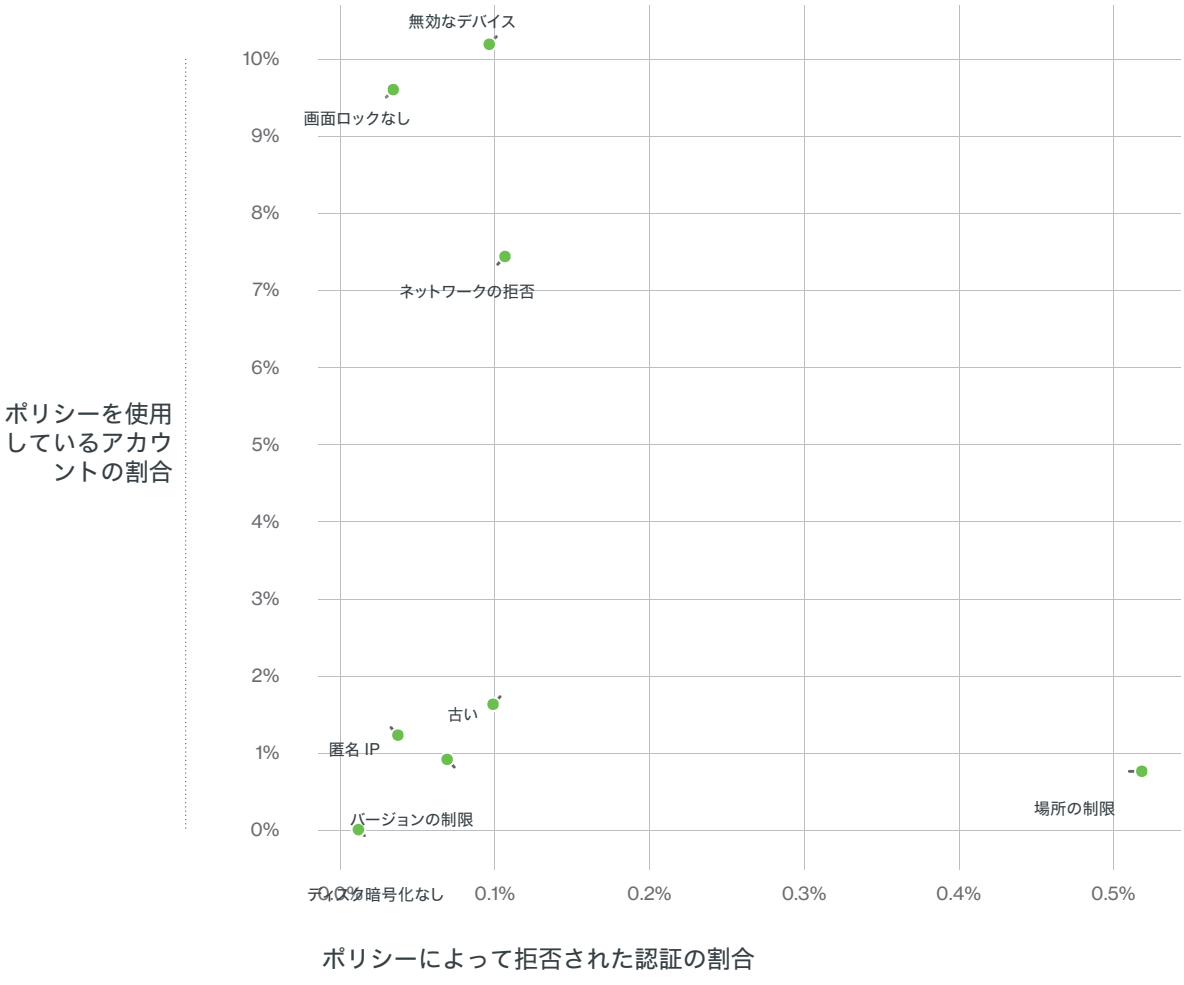


図 13 認証失敗の理由の割合

場所に関連するポリシーを使用している組織は 1% 足らずであるにもかかわらず、このポリシーが認証失敗の大きな割合を占めていることがわかります。ユーザー登録が原因で失敗した認証を除外することで、ポリシー設定の影響を受けやすい認証の失敗に焦点を当てることができます。

強力なデバイスベースポリシーの利点

このリスク軽減戦略の基盤となるのは、環境内のすべてのアセットに、統一されたセキュリティポリシーを実装することです。デバイスベースのポリシーは特に重要です。場所やユーザーに関係なく、組織内のすべてのデバイスに適用される一貫したセキュリティフレームワークを提供できるからです。これらのポリシーでは、強力な認証手段の適用、定期的なパッチと更新の適用、ファイアウォールとウイルス対策ソフトウェアの設定、ユーザー権限の管理など、デバイスセキュリティのさまざまな側面を制御できます。

統一されたデバイスベースのポリシーには、次のようないくつかの利点があります。

一貫性：すべてのデバイスが同じセキュリティ標準に準拠するようにし、攻撃者が悪用する可能性のあるセキュリティチェーンの脆弱なリンクを切断できます。

拡張性：組織の成長に合わせて、確立されたポリシーを自動的に適用して新しいデバイスを導入できるため、大規模なセキュリティ管理が容易になります。

コンプライアンス：デバイスベースのポリシーによって、すべてのデバイスが業界標準と法律に準拠していることが保証されるため、組織は法的規制を満たし、罰金やその他の罰則のリスクを軽減できます。

自動化：これらのポリシーは多くの場合、自動的に適用できるため、手動による介入の必要性とそれに伴うヒューマンエラーが削減されます。

可視性と制御：統一されたポリシーを実装すると、デバイスセキュリティのモニタリングと制御を行いやすくなり、ポリシー違反を検出して修復しやすくなります。

セキュリティ負債を削減する上位 3 つのポリシーグループ

セキュリティ負債の削減は複雑で多面的な取り組みですが、この取り組みの基盤となるのは、包括的なデバイスベースのポリシーを一貫して適用することです。このようなアプローチにより、セキュリティ負債を根本から解消し、リスクを軽減し、より安全で復元力の高い組織環境を促進できます。

アクセスデバイスとセキュリティポリシーの相互作用は、組織のサイバーセキュリティ フレームワークの重要な側面です。企業リソースにアクセスしようとするデバイスがネットワークへの侵入を許可される前に、一定のセキュリティ基準を満たすように、厳格なセキュリティポリシーが設定されています。デバイスがこれらの所定の基準を満たしていない場合、組織のデジタルアセットを保護することを目的とした一連の自動応答がトリガーされます。

Duo のデータによると、デバイスベースのポリシーを導入している企業の多くは、安全でないと思われる場所や、アクセス元として望ましくない場所からのアクセスをブロックしています。また、無効なデバイス、ソフトウェアが古いデバイス、画面ロック機能やディスク暗号化機能を使用していないデバイスをブロックするポリシーも設定されるようになりつつあります。これらのシンプルなセキュリティ手順によって、デバイスやデバイスが送信するデータが他者に見られないように保護できるからです。

ここでは、複雑さを軽減し、セキュリティカバレッジを拡大するのに役立つ 3 種類のポリシーを紹介します。

01

まず、一般的なセキュリティ対策である**地理的制限**が挙げられます。データの所在地と主権を規定する法的または企業ポリシーによって機密データが規制されている場合は特によく講じられます。ユーザーがホワイトリストに登録されていない場所からシステムにアクセスしようとすると、セキュリティプロトコルが即座に介入し、認証は失敗します。この地理的な制限は、国際的なサイバー犯罪者による不正アクセスなど、さまざまな脅威に対する効果的な抑止力となっています。

シスコの調査によると、多くの組織は、地理情報に基づいたポリシーを導入するために必要な措置を講じていません。実際、昨年レポートしたように、特定の地理的な場所を拒否する何らかのポリシーを使用する組織の割合は、2020 年以降 20% 減少しています。2023 年には、96.4% の組織では、場所に関連するポリシー (二要素認証の許可、拒否、必須) が設定されていませんでした。ただし、地理的な場所を拒否している企業の 91% がロシアか中国のいずれかをブロックし、さらにこれらの組織の 63% は両方の国をブロックしています。

96.4%

場所に関連するポリシーが設定されていない組織の割合

国ごとの拒否の推移

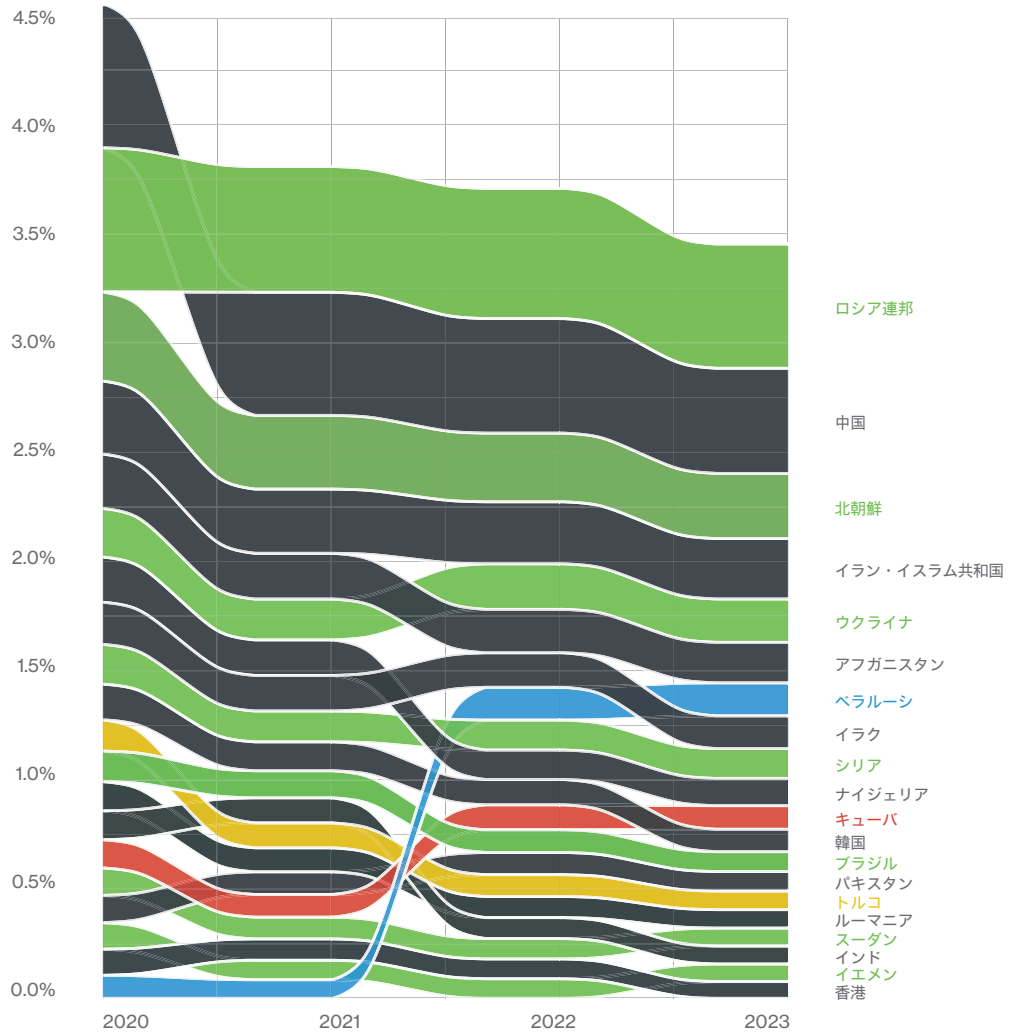


図 14 特定の国に焦点を当てた拒否ポリシーを適用しているアカウントの割合

02

第 2 に、**無効なデバイスやソフトウェアが古いデバイス**の使用は大きなリスクをもたらします。サポートが終了したデバイスや、最新のセキュリティパッチが適用されていないデバイスには、サイバー攻撃者にエクスプロイトされる可能性のある脆弱性が多く存在します。セキュリティポリシーは、セキュリティ態勢（オペレーティングシステムのバージョン、インストールされているセキュリティパッチ、その他の重要なセキュリティ設定など）に基づいてデバイスを検出するように設計されています。これらの分野のいずれかを満たしていないデバイスが見つかった場合、ユーザーはログインできなくなるか、または現在のセキュリティ標準に準拠するようにデバイスの更新を求められます。

たとえば、認証成功した際に使用されている可能性が最も高いのは Mobile Safari ですが、最新でないかサポートが終了している可能性も最も高くなります。図 16 が示しているように、ほとんどのアカウントで「最新」のアップデートが適用された状態で動作しているのは 20 ~ 40% のブラウザだけです。

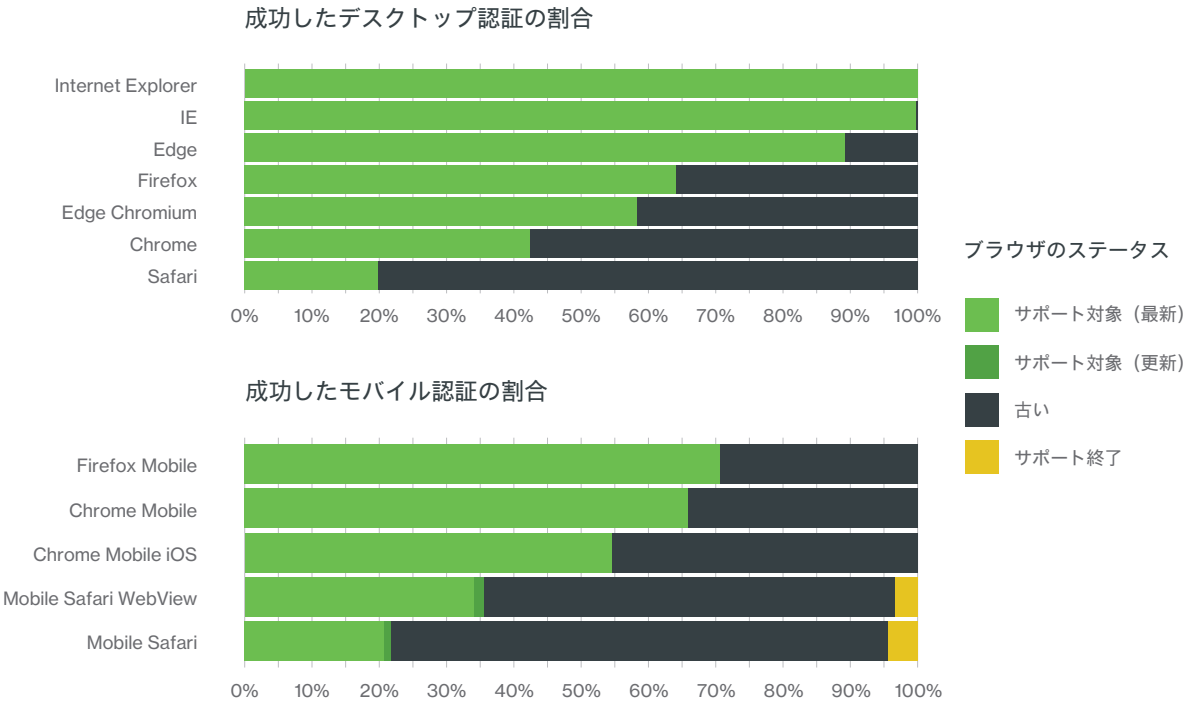


図 15 ブラウザとブラウザの更新ステータス別の認証の割合

Mobile Safari は、モバイル認証の最大の割合を占めていますが、モバイルブラウザが最新である可能性が最も低い

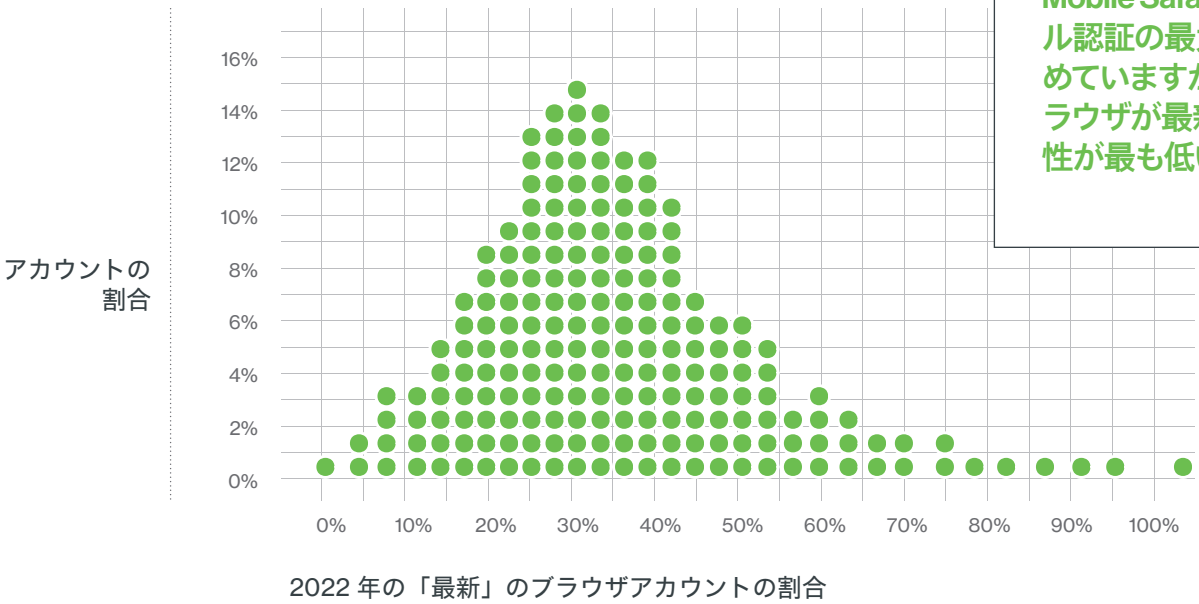


図 16 アカウント内で最新のブラウザを使用している割合

03

第 3 に、ユーザーグループ単位またはアプリケーション単位できめ細かいアクセスポリシーを設定することで、**最小限の特権アクセス**の基盤を構築します。今日の組織は、重要なビジネス機能を補完してサポートするために、サードパーティのエコシステムに依存しています。規制要件に加えて、不明なゲストアカウント、休眠アカウント、孤立アカウントがあると、管理オーバーヘッドが増加し、機密リソースへの不正アクセスのベクトルになる可能性があります。組織は、アカウントを管理し、アクセス可能なものを制限するためのポリシーと手順を実装する必要があります。これには、強力な多要素認証の適用、ゲストアカウントの定期的なレビューと監査、不要になったゲストアカウントの無効化などが含まれます。

2023 年版『アイデンティティ セキュリティの状態』レポートによると、平均的な組織には多くの非アクティブなアカウントがあり、アイデンティティ全体の 24% を占めています。これらのアカウントは、毎月 500 件以上の攻撃を受けています。ユーザーベースをさらに複雑にしているのが、全アイデンティティの 3.24% 以上がゲストアカウントであることです。

平均的な組織では非アクティブなアカウントに対する攻撃が毎年 500 件以上発生しています

これらのポリシーを効果的に実施するには、従業員の教育と意識向上にも投資する必要があります。結局のところ、どんなに洗練されたポリシーでもヒューマンエラーによって損なわれる可能性があります。ゲストアカウントに関連する潜在的なリスクと、信頼できる外部ユーザーにのみアクセスを許可することの重要性について、ユーザーを教育する必要があります。定期的なトレーニングセッション、シミュレーション、セキュリティ演習を実施することで、ベストプラクティスを定着させ、セキュリティの脅威をプロアクティブに特定して対応できる、警戒を怠らないワークフォースを育成できます。

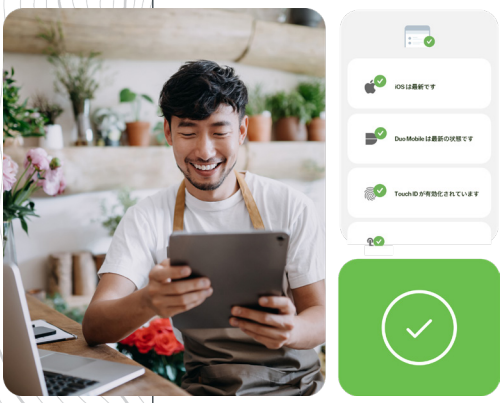
このような厳格なアクセス制御は、ユーザーにとっては不便なこともありますが、サイバー攻撃が巧妙化し続ける時代には必要な防御です。コンプライアンスに準拠したデバイス、ひいてはそのユーザーだけが組織のシステムと通信できるようにすることで、企業のデータとサービスの完全性、機密性、可用性が保たれます。

おわりに

アイデンティティ セキュリティの未来

アイデンティティスプロールによって脆弱性が助長されます。ただし、従来のアイデンティティ インフラストラクチャは、セキュリティではなく IT 運用を念頭に置いて構築されていました。アイデンティティとセキュリティの統合は進んでいますが、多くの大企業では、セキュリティチームはいまだに IAM チームから独立して機能しています。人材不足が組織の保護をさらに困難なものにしています。中小規模の組織の場合、IT 部門は多くの役割を担う少数の人々で構成されているかもしれません。セキュリティチームがまだ設立されていない可能性もあります。アイデンティティによる脅威の検出や対応などの新しいセキュリティテクノロジーは、アイデンティティとセキュリティチームとの間のギャップを埋めるのに役立ちます。

組織は、運用上の課題に加えて、人的資本の制約、つまりアイデンティティの管理を人に依存するという課題にも直面しています。アイデンティティ セキュリティは複雑であり、次のような複数の要素を監視する必要があります。



ユーザーアイデンティティ。特定のユーザーを表し、通常は認証用の一意のログイン情報に関連付けられます。

デバイスアイデンティティ。一意に識別でき、ユーザーに関連付けることができます。デバイスのステータスと信頼性は、特定のリソースへのユーザーのアクセスに影響を与える可能性があり ます。

アイデンティティの**属性**またはプロパティ (ユーザーのロール、場所、部門など)。属性を使用してアクセスポリシーを決定し、適用できます。

アイデンティティに付与される**権限**とアクセス権。これにより、アイデンティティがアクセスできるリソースと実行できるアクションが決まります。

IAM の健全性が低いと、アイデンティティの攻撃対象領域が拡大し、攻撃者にとって新たなチャンスとなります。デバイス、属性、アイデンティティ、権限の間に作成される関係が増えるにつれて、どのアイデンティティが何を行っているかを確認して追跡することがますます困難になります。

複数のソースからアイデンティティ関連のデータを収集するソリューションや、コンテキスト化されたポスチャ情報を IT から SOC に渡すソリューションがなければ、インシデントの調査も困難です。従業員、請負業者、サービスアカウントを含め、誤って設定されたアカウントや未使用のアカウントを可視化することも不可欠です。

アイデンティティの脅威を検出して対応する機能をアクセス管理と一体化させることが必要になっています。これらの機能を連携させることで、アイデンティティに基づく攻撃が成功する可能性を最小限に抑えながら、アイデンティティとアプリケーション全体を包括的にカバーできます。

アイデンティティベースの攻撃に効果的に対処するには、IAM 分析機能をこうしたソリューションに組み込む必要があります。このように、IT 管理者は、お客様のエンタープライズスタック全体で脆弱な認証環境から、強力でフィッシング耐性のある多要素パスワードレスの環境に移行することで、セキュリティギャップに迅速に対処できます。

コンテキストは新しい MFA

データが最も重要ながら鍵はコンテキストが握る世界では、強力なアクセス管理は企業のセキュリティを強化するだけでなく、それを再構築します。パスワードに依存するシステム特有の弱点に対処し、進化し続ける脅威に対してより堅牢で動的な防御を確立します。

雑多なデータについて理解するには、詳細なロギングとアラートのメカニズムが不可欠です。MFA による認証の試みでは、2 番目または 3 番目の要素が失敗した場合にアラートがトリガーされるため、リアルタイムの脅威検出と迅速な対応が可能になります。これにより、侵害が発生してから検出されるまでの間隔である「滞留時間」を大幅に短縮できます。これは、セキュリティインシデントによる被害を軽減する上で非常に重要です。

未知の複雑さを克服する際に必要な手順について理解するのは簡単ですが、実装するのは難しい場合があります。サイバー脅威がますます複雑化し、巧妙になるにつれ、IAM のベストプラクティスを採用することは、セキュリティプロトコルの進化に必要であり、現代の組織の資産、評判、将来を守るために不可欠です。

推奨事項

- **強力な MFA** を組織全体で採用し、特権アカウントには FIDO2 セキュリティキーなどフィッシング耐性のある MFA のみを要求するように移行します。
- **検証済み Duo Push** を有効にします。これにより、プッシュハラスメントやプッシュ疲れといった攻撃を防止し、組織を**パスワードレス化**に向けて前進させることができます。
- 管理対象か管理対象外かにかかわらず、**信頼できるデバイス**のみに企業リソースへのアクセスを許可します。
- 組織のリスクレベルと重点項目を考慮したデータに基づくユーザー**認証ポリシー**を設定し、ユーザーの生産性を妨げないインテリジェントな認証ステップアップを実現します。
- 最新の**シングルサインオン** ソリューションをポリシー適用ツールとして活用し、各アプリケーションにゼロトラストと最小限の特権アクセスの原則を適用します。
- **Duo リスクベース認証**など、ユーザーとデバイスのテレメトリを評価して、既知の脅威パターンと異常を特定するソリューションを活用します。ログイン試行のコンテキストとリスクを評価します。
- ITDR を使用して環境内の IAM の複雑さを特定し、可視性の程度に基づいて弱点を評価します。**アイデンティティ脅威の検出と対応**機能を活用して、単一の包括的なインターフェイスでアイデンティティエコシステム全体を可視化します。

クレジット

データサイエンス

Cyentia Institute

Elizabeth Gilbert

Kevin Pelaez, PhD

Rose Putler, M.S.

ライター

Katherine Yang

Michael Parker

Slavka Bila

運用

Yolina Nenov

Taylor Stewart

設計および開発

Amanda Cash

Chris Canote

Clayton Chu

Mary Jane Duty

Tony Ly

参考資料

- 『2023 年版アイデンティティ セキュリティの状態 : ワークフォースの保護』
  Oort 社、2023 年
- 『サイバーレジリエンスの達成 : セキュリティ成果レポート Vol. 3 の調査結果』
  シスコ、2023 年 1 月 10 日
- 『シスコ サイバーセキュリティ成熟度指標』
  シスコ、2023 年 3 月
- Cisco Talos の 2023 年版『一年の総括』
  Cisco Talos、2023 年 12 月 5 日
- 『インシデント対応の動向（2023 年第 2 四半期）: データ窃盗による恐喝が増加、最も狙われた業種は今四半期も医療』
  Cisco Talos、2023 年 7 月 26 日

duo.com から 30 日間の無料トライアルをご利用ください。 すべてのユーザー、 デバイス、 アプリケーションの保護にすぐにお役立ていただけます