2021 年 DUO

Trusted Access レポート

パスワードレスの未来への道

DUO

cisco SECURE

2021 年 DUO

Trusted Access レポート

パスワードレスの未来への道

作成
DAVE LEWIS

データサイエンス
ROSE PUTLER

編集
KATE BILLERBECK
CHRYSTA CHERRIE
J. WOLFGANG GOERLICH
TYRONE HARMON
WENDY NATHER
HELEN PATTON

設計および開発
CHELSEA LEWIS
SARAH OVRESAT
LAUREN FITZPATRICK
TRACY TOEPFER
HAFSAH MIJINYAWA
SUNNY BERRO
MARLA JONES
BEN ARMES
BEN COLMAN

導入
EMILY GORDY

バージョン 1.0

1.0

より安全な未来への合理的なプロセス

約 58 年もの長い間、私たちはセキュリティ制御としてパスワードを使用してきました。しかし、世界中のセキュリティ関係者は、パスワードによるセキュリティレベルが、家の鍵と同じようなものであることをよく知っています。パスワードはその目的を果たしてきましたが、企業がユーザー、資産、アプリケーションのセキュリティを確保するためには、パスワードよりも優れた方法に移行するときが来ています。

この 1 年半以上、全世界の企業は、さまざまな形式でテレワークを実現してきました。かつては、あれば便利だとしか思っていなかったものが、今や、ビジネスを遂行するための事実上の標準として、迅速に対応しなければならないものになっています。

その一例が Webex などの Web 会議テクノロジーです。ハイブリッドワークでは今や幅広く活用されています。さらに、古くからある Web カメラが再注目されました。しかもビデオ会議では衣装代を削減できるという副次的な効果もあります。さらに不幸中の幸いか、ワークライフバランスを改善する機会も得られました。

世界的なコロナ禍においてあらゆる業種の企業は、ハイブリッドワークのためのポリシーを調整し、適応しなければなりませんでした。しかし幸いなことに、この対応が従業員にとってはプラスに働いたのです。

ハイブリッドワーク環境が経済を維持するための戦略になり、多くの組織は短期間で大規模な移行を実現できました。今や企業は、アクセスを制御するための、より効果的な新しい方法に移行することを目指しています。その中では、従来の勤務環境の外でもユーザーを保護することで、セキュリティを損なうことなく、ハイブリッドワーカーが各自の業務に集中できる環境を整えられることが判明しつつあります。

多要素認証 (MFA) は、組織を保護するための優れた戦略を導入する、合理的なプロセスにおける次のステップであり、パスワードレス認証に移行するための準備段階と言えます。MFA では、パスワードを唯一のユーザー認証方式として使用するリスクを排除し、攻撃者がリモートから簡単に破れない 2 つ目の ID を検証することで、ログイン情報が窃取されるリスクを軽減できます。これにより、生体認証、セキュリティキー、モバイルデバイスなどの新たな認証方式の基盤が確立されます。その結果、日常的にパスワードを使用する必要がなくなり、最終的にセキュリティリーダーは、強力なセキュリティと使いやすさを両立させられるようになります。

「パスワードレスは、認証の強化とユーザーのメリットを両立させるものです。従業員は、ログインプロンプトや面倒な操作なしで、素早く認証を受けられることを求めています。一方、セキュリティチームは、認証における全体的な信頼性を強化しようとしています。

信頼できるパスワードレス認証は、デバイスの状態を含め、認証要求のコンテキストと状況を考慮して、ポリシーの決定および適用ポイントとしてログインプロセスを使用します。これらの制御を確立しているセキュリティチームは、多要素フィッシングや生体認証スプーフィングより先行しています。このように、パスワードレス化することで、従業員のエクスペリエンスをシンプルにしながら、サイバー犯罪者の侵入を防ぐことができます」

J. Wolfgang Goerlich
Duo Security CISO サポート

ユーザーエクスペリエンスの向上

現在、世界中の従業員が通常とは異なる方法で仕事しているため、セキュリティがユーザーに広く受け入れられるように、全体的な要件を考慮する必要があります。アプリケーションは、ユーザー、デバイス、アプリケーションのセキュリティを損なうことなく、ハイブリッドワーカーが主要な職務に集中できるようにサポートしなければなりません。ほんの数年前は、不正な第三者に侵害された場合にビジネスに大きな影響を与える、重要なシステムを保護する場合にだけ MFA を使用することが珍しくありませんでした。

現在では、個人と組織のリスクを軽減するだけでなく、セキュリティ運用を効率化するために、すべてのアクセスを MFA に移行する取り組みが行われています。

これまでのセキュリティワークフローは、サポート期間が過ぎて効果がなくなったセキュリティ制御機能を使用することで、成果をあげられていませんでした。物理的なオフィスの場所に縛られることなくグローバルに分散したワークフォースに対応しようと、セキュリティはさらに効率化が進んでいます。

ユーザーエクスペリエンスが重要

現在は、ユーザーエクスペリエンスがセキュリティ制御そのものだと言っていいほど、非常に重要になっています。セキュリティ制御に非常に手間がかかる場合や、エンジニアがユーザーのことを考えずに開発したようなひどい状況の場合、平均的な従業員がセキュリティ制御機能を効率的に利用できるとは思えません。映画「フィールド・オブ・ドリームス」でケビン・コスナーが言った有名なセリフがあります。「まず (球場を) 作れば、観客は来るだろう (If you build it, they will come.)」。ただし今のユーザーは、使いやすく効果的なツールでなければ利用してくれません。

非常に小規模な企業から大規模な企業に至るまで、リモートアクセス認証の増加率は驚くべきものです。Duo は、多くの企業において、実際にハイブリッドワーカーがオフィスと同じ生産性を維持できることを何度も確認してきました。企業は、Web 会議、MFA、VPN、RDP テクノロジーを活用することでビジネスを継続し、ログインを保護できます。

優れたユーザーエクスペリエンスは、企業のセキュリティと成功において基本的な役割を担うものです。セキュリティが組織の進歩を妨げる障害だと考えた従業員は、セキュリティ制御を回避する方法を見つけようとする可能性があり、セキュリティ全体に悪影響が及びます。

実際には、ユーザーにとって使いやすい認証方法もありますが、20 文字以上もの長いパスワードを何百も覚えるのは困難です。パスワード マネージャ アプリケーションを利用すればそのプロセスもシンプルになりますが、MFA や生体認証によるセキュリティはさらに効果的です。また、Webauthn などの方式を使用するパスワードレス認証により、ユーザーは、昔のように大量のパスワードを覚えておかなくても自分のタスクを完了できます。

ユーザーがより使いやすい認証方式を活用することで、セキュリティが強化されます。パスワードレス認証が使いやすく、従来のセキュリティ制御を上回るメリットがある場合、パスワードレス化は成功します。セキュリティ制御機能を利用するのが困難だったり面倒だったりする場合、従業員は正しく使用する気がなくなります。優れたデザインは、セキュリティの強化に大いに役立ちます。

シングルサインオン (SSO) などのテクノロジーの利用が拡大することで、従業員は、自分にとって最も重要な作業に注力できるようになります。たとえば、SSO を使用した認証件数は着実に増加しています。2020 年には、すべての認証の 20.6% が SSO アプリケーションで行われ、2021 年には 24.8% にまで増加しました。

世界中でのセキュリティ範囲の拡大

2020 年以降世界を席巻しているコロナ禍は、ハイブリッドワークの急速な拡大を招き、企業に新たなセキュリティ上の課題をもたらしました。これは特定の地域に限ったことではありませんでした。企業やさまざまな組織は、ワークフローに大きな悪影響を与えることなく、ビジネスを遂行するために必要なアプリケーションやリソースに従業員が安全にアクセスできるようにする必要がありました。その一方で、組織のリスクを軽減することにも真剣に取り組む必要があります。そのため、データ、アプリケーション、知的財産に悪影響を与えないようにしながら、明確な目的を持って対応を続けなければなりませんでした。

企業の焦点は、一夜にして、グローバルレベルで従業員の働き方をシフトすることに移ったかのようでした。時間が経つにつれて、さまざまなレベルの成功事例が聞こえてきています。円滑に移行できた企業もあれば、オンプレミスからの移行に必要なリソースを確保できずに止まってしまった企業もありました。しかし、世界全体として、物事は企業にとってプラスの方向に進んでいる傾向にあります。従業員がこの新しいグローバル環境で仕事ができるようにサポートするため、組織はシステムをオーケストレーションして活用する必要がありました。

2021 年 Duo Trusted Access レポートでは、企業が現在どのようにハイブリッドワーク環境を保護しているかに焦点を当て、強固でセキュアなリモートアクセス戦略を実現するために何が必要かについてまとめています。Duo のデータによると、現在すべての業種で従業員の在宅勤務に対応する組織が増加していて、その期間は延長される見込みです。また、それらの組織は、アプリケーションに安全にアクセスするための適切な制御機能を導入しようとしています。

ユーザーがより使いやすい認証方式を活用することで、セキュリティが強化されます。

調査方法

ゼロトラストセキュリティ戦略には、ユーザー、デバイス、アプリケーションという 3 つの柱があります。そのため、以下の質問が重要になります。

ユーザー

企業の情報へのアクセス権限を持っているのは誰ですか？

デバイス数

アプリケーションへのアクセスにはどのデバイスが使用されていますか？

アプリケーション

ユーザーはどのアプリケーションにアクセスしていますか？

このレポートを作成するために、Duo のデータサイエンティストは、北米、中南米、ヨーロッパ、中東、アジア太平洋地域のお客様の 3,600 万台を超えるデバイス、40 万種類を超えるアプリケーション、および月間約 8 億件の認証に関するデータを分析しました。Duo では、2020 年 6 月 1 日から 2021 年 5 月 31 日までを 2021 年度とし、その期間に実施された認証を調査しました。認証以外のデータについては、2021 年 5 月 31 日にメトリクスを測定しました。

8 億以上

1 ヵ月あたりの認証件数

3,600 万台以上

デバイス数

40 万種類以上

アプリケーション数

主な傾向のサマリー

パスワードレス化の拡大

ユーザーは使いやすい二要素認証に移行しています。**Webauthn** の利用は、2019 年 4 月から 5 倍に増加しています。

ブロックされた場所

デバイスベースのポリシーを導入している組織の約 74% が、中国とロシアからのアクセスを制限しています。

生体認証の拡大

71% を超えるスマートフォンで生体認証が有効になっていて、スマートフォン全体で 12% 増加しています。

Push の利用が増加

Duo Push が最も使用されている認証方式で、全認証の 30% を占め、前年の 23% から増加しています。

頻繁に更新される iOS

iOS では、セキュリティアップデートまたはパッチの公開日から 30 日以内に更新されるデバイスが、Android デバイスより 40% 多くなっています。

古いソフトウェアを搭載したデバイスの認証拒否

古いソフトウェアを搭載したデバイスの認証が拒否される件数は、2020 年から 2021 年の間に 33% 増加しました。

MFA でパスワードの強化が継続

多要素認証は強力さを保ちながら、従来のパスワードのみのセキュリティを強化し続けています。Duo の MFA の利用は、この 1 年で 39% 増加しました。

ハイブリッドアプローチを採用している企業が増加

リモート アクセス アプリケーションを使用している企業の割合は、2020 年 3 月から 8 月にかけてピークをわずかに下回っていますが、その後の 9 ヵ月間で、平均月間認証数ベースで 15% 高い状態が続いています。

クラウドでの利用が増加

クラウドアプリケーションに対する認証は、認証全体の 13% から 15% に増加しました。

ポリシーの使用状況

セキュリティソリューションに関して重要なのは、人的要素を考慮することです。導入されたシステムと、結局導入されなかったシステムとの間には根本的な違いがあります。後者は、攻撃者との最初の接触に対応する計画がないのです。ユーザーが組織の目標とミッションを達成する上で必要なシステムとアプリケーションを統合するためには、ポリシーを適用する必要があります。Duo を利用すれば、企業はアクセス制御を適用できるため、全体的なリスクを軽減できます。Duo ではユーザーグループごとにアプリケーション単位でポリシーをきめ細かく定義できるため、セキュリティチームは、ユーザーの業務に影響を与えることなくセキュリティを強化できます。

2.0

ユーザーが受け入れやすいセキュリティ

従業員が安心 / 安全に仕事をするための機能を強化する必要性が高まっています。企業のセキュリティは、よりシンプルで自動化されたものでなければなりません。ゼロトラスト戦略は、単なるアクセス制御ではなく、より包括的なものと考える必要があります。企業が、オンプレミスシステムからエッジ、クラウドに至るまでのワークロードを保護し、複雑な分散環境と仮想化に対応できるようにする必要があることは明らかです。

「誰もが自分のリソースとデータへのアクセスを制御する権利と機能を持っているべきです。信頼できるアクセスとは、セキュリティ、コンプライアンス、プライバシーに関する要件をすべて満たしながら、ユーザーが使いやすいものでなければなりません。信頼できるアクセスを進化させることは、デジタル化された未来にとって最も重要なことです」

Wendy Nather
Duo Security CISO サポート責任者

認証は、企業の従業員が業務に必要なシステムにアクセスするための最初のポイントです。多要素認証は、ゼロトラスト戦略への移行プロセスがどのように進み始めるかを示す好例です。

効率化

セキュリティの強化は、昨年、さまざまな業種で行われた大きな変化です。「シスコ **セキュリティ成果調査**」で示されているように、2020 年 3 月以降、世界中の多くの場所で企業の従業員がテレワークを始めたため、組織は運用を効率化し、チームの生産性を高めるために最適な方法を検討してきました。

企業は、セキュリティの俊敏性を強化し、急速に変化する IT 環境に適応するためにレジリエンスを高めています。また、Continuous Trusted Access とゼロトラストのセキュリティ戦略を活用して、ユーザーやデバイスのアクティビティの可視化機能、アプリケーション検出機能、リスク管理機能を強化しています。

ポリシーを一貫して適用することで、さらなる効率化も進んでいます。セキュアエッジを含む拡張された企業全体で、ネットワークゾーンのセグメンテーション機能とアクセス管理機能をさらに活用することでセキュリティを強化し、リスクを軽減しました。

また、自動検出機能や自動対応メカニズムを利用して、セキュリティ運用も効率化しています。企業は、デバイスとアプリケーションからより多くのインテリジェンスを収集し、セキュリティ制御をオーケストレーションする機能と自動化機能を活用して既存の従業員をサポートすることでセキュリティを強化し、安心 / 安全な方法でワークフォース、ワークプレイス、ワークロードを効率的かつ効果的に運用しようとしています。

企業内でセキュリティの問題に確実に対応できるようになると、従業員が組織の最も重要なプロジェクトに集中する時間が取れるようになります。多くの組織は、長年にわたってプロジェクトのためにさまざまなシステムを導入してきましたが、それらのシステムでは、ビジネス目標を達成することしか考えられていませんでした。そのため、システムを長期間にわたって利用するには、継続的にメンテナンスすることが必要だという認識が欠けていたのです。

その結果、適切に設定されて最新のパッチが適用されているかどうかがわからない、推奨されないシステムが増えています。古いシステムに細心の注意が払われないことによって、気付かない間に企業に脆弱性が発生してしまう可能性があります。

企業のネットワークアーキテクチャを効率化することで、セキュリティ担当者と IT 担当者は、組織のリスクを軽減できます。ここで、Continuous Trusted Access の概念が重要になります。組織のセキュリティを強化するための一貫した戦略を策定することで、IT システムがビジネスを最適にサポートできるように変革できます。

昨年は、ハイブリッドワークモデルをサポートするために、企業でクラウドアプリケーションを利用する機会が大幅に増加しました。Duo のデータによると、2020 年 6 月~ 2021 年 5 月における 1 日あたりのクラウドアプリケーションに対する平均認証数が、1 年前の同じ期間の平均より 65% 増加しています。

Duo は、クラウドベース アプリケーションの認証に関するデータを分析し、北米、ヨーロッパ、中東、アジア太平洋、中南米の企業におけるハイブリッドワーカーの認証処理方法の変化について確認しました。その結果、2020 年から 2021 年にかけて、すべての地域でクラウドアプリケーションに対する認証の割合が増加していることがわかりました。ヨーロッパと中東が最も多く、190% の急増を示し、アジア太平洋、中南米、北米では、それぞれ 38%、18%、13% と、比較的穏やかな増加でした。

パスワードレスアクセスが増加した業種

このレポートでは、主な業種を調査し、面倒な二要素認証から、より効率化された認証方法にどのように進化しているかを分析しました。新しい認証方法としては、生体認証などの手間のかからないパスワードレス認証があります。Duo は、最新の認証方式への対応方法の変化に関して、先行している上位 5 つの業種を調査しました。対象の 1 つである金融サービス業では、生体認証を 2 つ目の要素として利用し始めた企業が最も多く、11 倍増加しています。一方、テクノロジー業界の増加率が最も少なく、2020 年からの増加率は 11% でした。

2021 年において生体認証の利用率が上位の業種の傾向

金融サービス：

↑ 1100%

85,000 件に増加

教育：

↑ 770%

180 万件に増加

医療：

↑ 580%

13,000 件に増加

IT/ 通信：

↑ 160%

20 万件に増加

テクノロジー：

↑ 11%

170 万件に増加

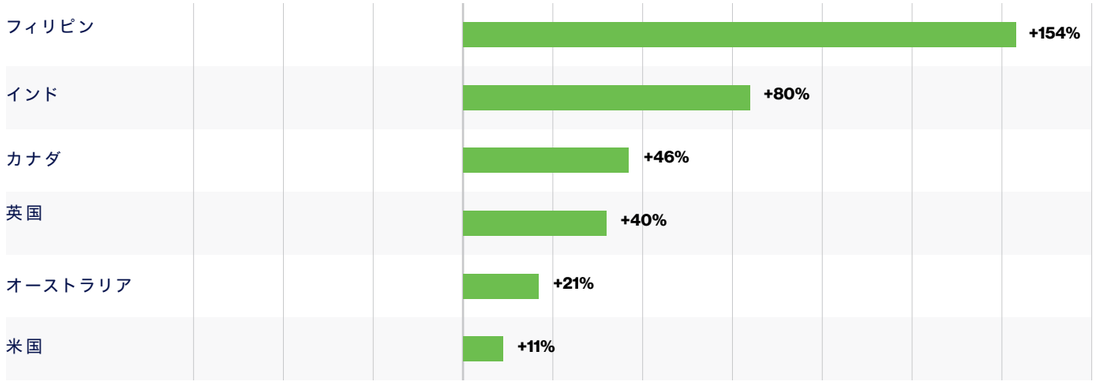
MFA の世界的な増加

Duo では、MFA テクノロジーの利用が最も増加している地域がどこかも調査しました。たとえば北米では、MFA テクノロジーを利用した 1 日あたりの平均認証件数が全体的に増加していました。米国では 11% の増加でしたが、カナダでは 46% 増加しています。

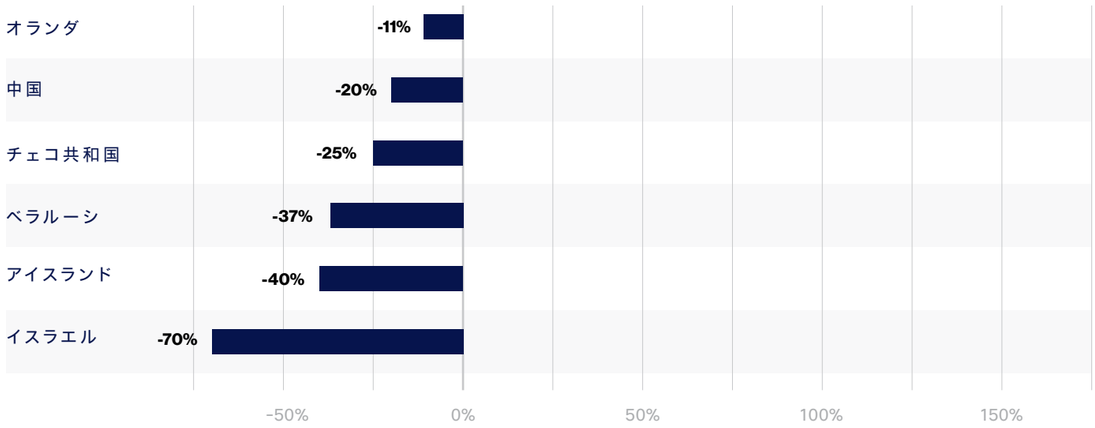
一方、英国では、同時期に 40% 増加しています。

アジア太平洋地域では、オーストラリアは 21% 増、インドはそれより多い 80% 増、フィリピンはさらに多い 154% 増など、増加傾向が見られました。

認証件数が増加した上位の国



認証数が減少した上位の国



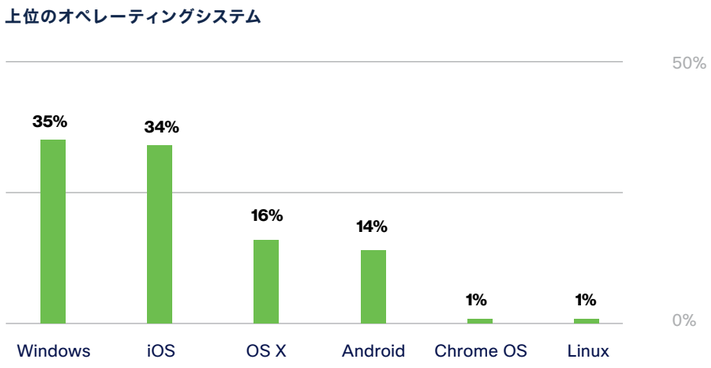
2021 年の認証件数 (アクセスデバイスの IP アドレスベース)

デバイスの可視性

デバイスの信頼性を確立するには、アプリケーションやデータにアクセスするデバイスを可視化する必要があります。中でも、デバイスで実行されているオペレーティングシステムとブラウザを把握すること、およびそれらの OS とブラウザが最新のものであるかどうかを把握することで、信頼できるデバイスかどうかを判断できます。まず、ブラウザと OS について見てみましょう。

主要な OS は引き続き Windows

オペレーティングシステムに関しては、Windows が引き続き最も多く利用されています。Duo のデータによると、上位のオペレーティングシステムは次のとおりです。



パスワードレスの未来に向けて

企業は、グローバルで変化する課題に組織を適応させる方法を改善するために、システムの効率化を進めています。生体認証の利用が増加していることは、ユーザーが従来とは異なる認証方式に慣れてきていることを示しています。つまり、ユーザーは、パスワードレス認証などの方式を利用することに抵抗がなくなっているということです。企業はパスワードからの移行を進めています。これにより、大多数のユーザーのログインエクスペリエンスが大幅に向上します。

パスワードは、セキュリティ制御として推奨されない概念です。個人がパスワードを再利用することで、実際にリスクに直面し続けています。それは、パスワードは簡単に解読できるからというだけでなく、複数のサイトやアプリケーションで同じパスワードを使用したり、長さや複雑さが足りないパスワードを作成したりする人が多いからです。

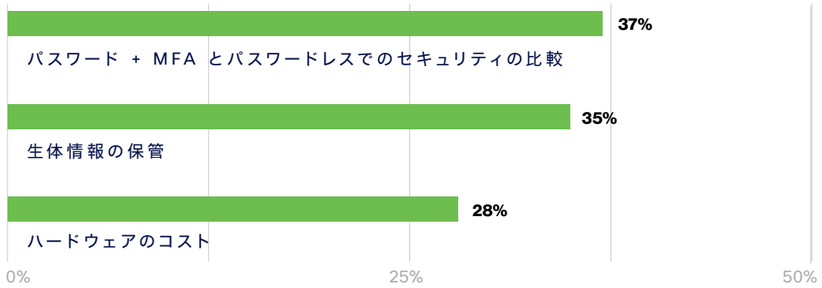
パスワードレス認証に移行することで、組織のパスワードへの依存度が徐々に低下し、パスワードによるリスクを軽減できます。パスワードレスの未来への道のりは、パスワードによる時代遅れのセキュリティ制御への依存度を減らし、強力な認証方式を利用するところから始まります。

では、OS は、パスワードレス化とどのような関係があるでしょうか。最近、シスコは、世界中の企業を対象に、自社の環境におけるパスワードレスの概念をどのように認識しているかを調査しました。調査対象となったすべての国の回答者の中で、製品がパスワードレスであると認定するための最も重要な条件は、テクノロジー自体に、生体認証、PIN、セキュリティキー、スマートカードなど、何らかの方式の「パスワードレス」技術が組み込まれていることでした。回答者の 36% 以上が、これが最も重要な条件であると考えていて、中でもインドでは、最も多くの回答者がそのように考えていました (49%)。

このレポートでは、静的パスワードの処理に関して大きく不満を感じていることが確認されました。すべての国の回答者の約半数 (46%) が、ログイン情報の侵害に関連するセキュリティの問題が、自社の環境内でパスワードを処理する上で最も不満を感じている、または懸念している点であると回答しています。その数はインドの回答者が 57% と最も多く、ドイツでは平均より少なく 36% でした。この認識は、すべての国で共通していました。

任意のタイプのセキュリティアクティビティを個人的に実行した回答者に関しては、職務に関係なく、自社の環境内でパスワードを処理する上で最も不満を感じている、または懸念している点は、ログイン情報の侵害に関連する問題でした。中でも、セキュリティソフトウェアの選択にかかわっている人が最も多く懸念を示していました (53%)。

調査の回答者にパスワードレス認証方式に関する最大の懸念事項について尋ねたところ、最も懸念されていたのは次の 3 点でした。

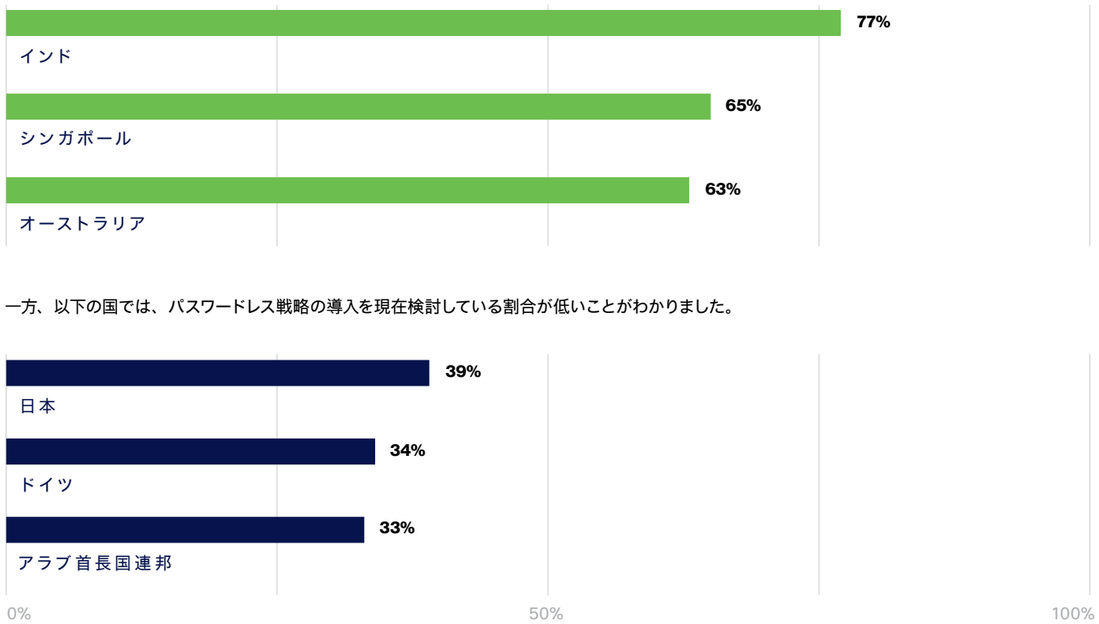


これらの懸念事項は、企業のセキュリティチームが懸念していることとまったく同じです。収益が 1 億ドルから 4 億 9,990 万ドルの企業で働く調査回答者の 45% 以上が、パスワードレス認証方式 (生体認証、PIN、セキュリティキーなど) を検討する際に、生体情報の保管が最大の懸念事項の 1 つであると述べています。一方、収益が 10 万ドル未満の企業では、同じ懸念を示しているのは、回答者の 23% です。

ただし、回答者のほぼ 11% が、パスワードレス認証方式について特に大きな懸念はないと回答しています。

大きな疑問は、企業は現在、組織にパスワードレス戦略を導入することを検討しているのか、ということです。興味深いことに、調査対象者の 52% が、パスワードレス戦略の導入を実際に計画しています。現在、パスワードレス戦略を検討していない回答者が、検討している回答者よりも多いのは日本のみです。その日本でも両者の割合はほぼ同じです (39% と 35%)。ただし、現時点ですでにパスワードレス戦略を導入しているのはわずか 6% にすぎません。

以下の国では、組織にパスワードレス戦略を導入することを検討すると回答した割合が高くなっています。



一方、以下の国では、パスワードレス戦略の導入を現在検討している割合が低いことがわかりました。

興味深いことに、現在パスワードレス戦略の導入を検討している割合が低い一部の国は、パスワードレス戦略を実際に実施している割合が高い国でもあり、日本 (回答者のほぼ 10%) とドイツ (9%) は、組織内で現在パスワードレス戦略を導入している、またはすでに導入済みであると回答しています。

パスワードレス ソリューションを導入する理由としてほとんどの国の回答者の間で共通しているのは、企業のセキュリティ全体の強化 (平均 44%) で、次いでユーザーエクスペリエンスの向上が挙げられています。対照的にシンガポールでは、ユーザーエクスペリエンスの向上を挙げた回答者が最も多くなっていました (53%)。

これは重要なポイントです。パスワードレス戦略を正しく実施すればユーザーエクスペリエンスが向上し、効果的なポリシーを積み重ねて適用することで、組織のワークプレイス、ワークフォース、ワークロードの安心 / 安全を確保できるということです。

Duo のデータを確認したところ、手間のかからない認証方式への移行が進んでいる企業の増加に伴い、生体認証の使用率が前年比で 48% 増加していることがわかりました。Duo Push を利用した認証の割合も、前年比で 30% 増加しています。これらの調査結果から、企業が手間のかからない認証方式を目指して、パスワード方式から移行していることがわかります。

また、WebAuthn 方式または Universal Second Factor (U2F) 方式のいずれかを使用するアプリケーション全体の割合が、昨年 35% に増加したことも注目に値します。

3.0

デバイス数

分散型のハイブリッドワーク環境は、緊急対応から事実上の標準に進化し、企業はそれに対応しています。変化しやすい環境のセキュリティを制御することは、企業にとって困難な課題です。強力な認証方式は ID の確認には役立ちますが、従業員が実際に信頼できるネットワークを使用し、データを適切に保護しているかどうかを確認するのはほぼ不可能です。

ノートパソコンやスマートフォンなどのデバイスは、セキュリティの観点から重要な要素です。企業は、それらのデバイスのセキュリティ態勢を把握できる必要があります。デバイスのセキュリティ態勢を良好に保ち、最新または 1 つ前のパッチを適用することが重要です。デバイスの状態を適切に管理することは、場所、オペレーティングシステム、暗号化ステータスなどの制御に役立ちます。

企業は、自社環境内におけるデバイスの適切なセキュリティ態勢をどのように定義するかを検討する必要があります。

さらに細かく言えば、ユーザーのプライバシーを侵害することなく、自社ネットワーク上のデバイスを可視化する方法を検討すべきです。多くの組織は、従業員の個人用デバイスを活用してテレワークをさらに拡大していますが、そういった組織は個人のデバイスをどのように保護するのでしょうか。

デバイスが会社所有であろうと個人所有であろうと、強力なゼロトラスト戦略は、デバイスの信頼を確立することから始まります。

Duo のデータを確認したところ、デバイスの暗号化が対前年比で劇的に増加していることがわかりました。昨年、暗号化が有効になっていたのは、Duo Endpoint Health アプリケーションを搭載したデバイスの 74% でしたが、2021 年には 90% にまで増加しました。この増加は、環境を保護する上で歓迎すべき傾向です。

もう 1 つ注目すべき点は、Duo Endpoint Health アプリケーションがインストールされたデバイスで、ファイアウォールが使用されている割合が増加したことです。2020 年以降、ファイアウォールが有効になっているデバイスは 94% でしたが、2021 年には 96% にまで増加しました。

デバイスベースのポリシー

企業がセキュリティの問題に対応してリスクを軽減しようとしている場合、デバイスベースのポリシーを実装して適用し、セキュアで信頼できるデバイスだけがアプリケーションやサービスにアクセスできるようにすることが重要です。

このようなデバイスベースのポリシーを適用することで、侵害された可能性のあるデバイスやリスクのあるデバイスがデータにアクセスできないようにすることが可能になります。企業のセキュリティ管理者は、デバイスの特定のセキュリティ状態に基づいて、管理対象、管理対象外を問わずすべてのデバイスにセキュリティポリシーを適用し、デバイスからのアクセスをブロックまたは許可することができます。

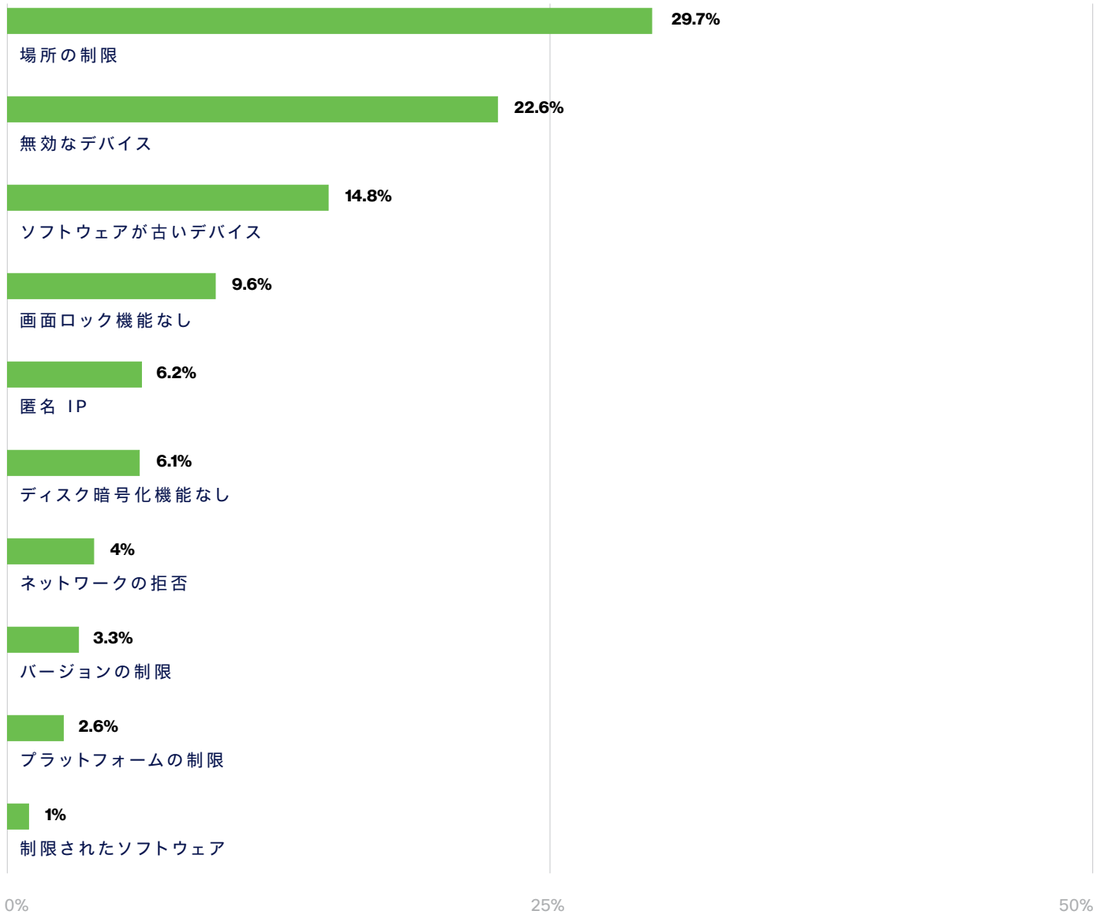
「Duo のお客様は、あらゆる組織におけるセキュリティ制御の基本は、セキュアな認証エクスペリエンスであることを認識されています。また、すべての従業員、請負業者、パートナーが把握できる制御であることも必要です。Continuous Trusted Access ポリシーを適用して認証を管理することで、システムとデータが保護されます。Continuous Trusted Access では、ユーザーは、状態に応じた適切なセキュリティ エクスペリエンスを得られます。追加のチェックは必要な場合にのみ実施されます。これにより最適なユーザーエクスペリエンスを実現し、新たなコンプライアンス要件に対応しながら、セキュリティ管理をシンプルにできます」

Helen Patton
Duo Security CISO サポート

利用頻度の高いポリシー上位 10

アクセスするデバイスがセキュリティポリシーの条件を満たしていない場合、ユーザーは認証されないか、デバイスの更新を求められます。Duo のデータによると、ポリシーによって認証が拒否されたり、ログインがブロックされたりする理由は、制限されている場所、無効なデバイス、ソフトウェアが古いデバイスからのアクセスなどです。ユーザーが認証を試みたときに、ユーザーのデバイスが、選択された認証方式をサポートしていない場合、そのデバイスは「無効」と分類されます。

認証をブロックしたポリシーの上位 10 種類



全体として、全認証の 7.6% が拒否されていたことがわかりました。その 7.6% の内訳を調べたところ、40% 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。これに対して、ユーザーが制限されたネットワークまたは場所から接続しようとしたことが原因なのはわずか 0.1% でした。

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、アクセスしようとすべきで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。

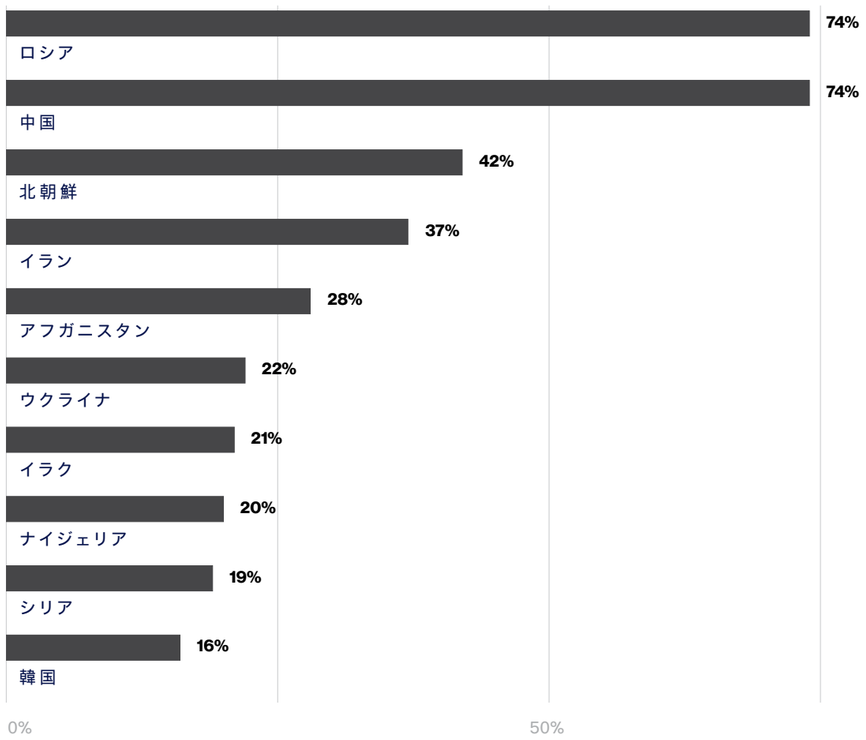
ポリシーに関するデータを確認したところ、いくつかの注目すべきことがわかりました。Duo Push ベースの認証は、グローバルのポリシー全体の 99.5% に設定されていました。モバイルのワンタイムパスコードは、定義されたポリシーの 98% に含まれていて、U2F は 86.6% でした。興味深い点の 1 つは、WebAuthn がグローバルポリシーの 55% に含まれていたことです。これは、パスワードレス導入が進んでいることを示す明るい指標です。WebAuthn は、2019 年 3 月に W3C によって初めて公開されたオープンスタンダードです。

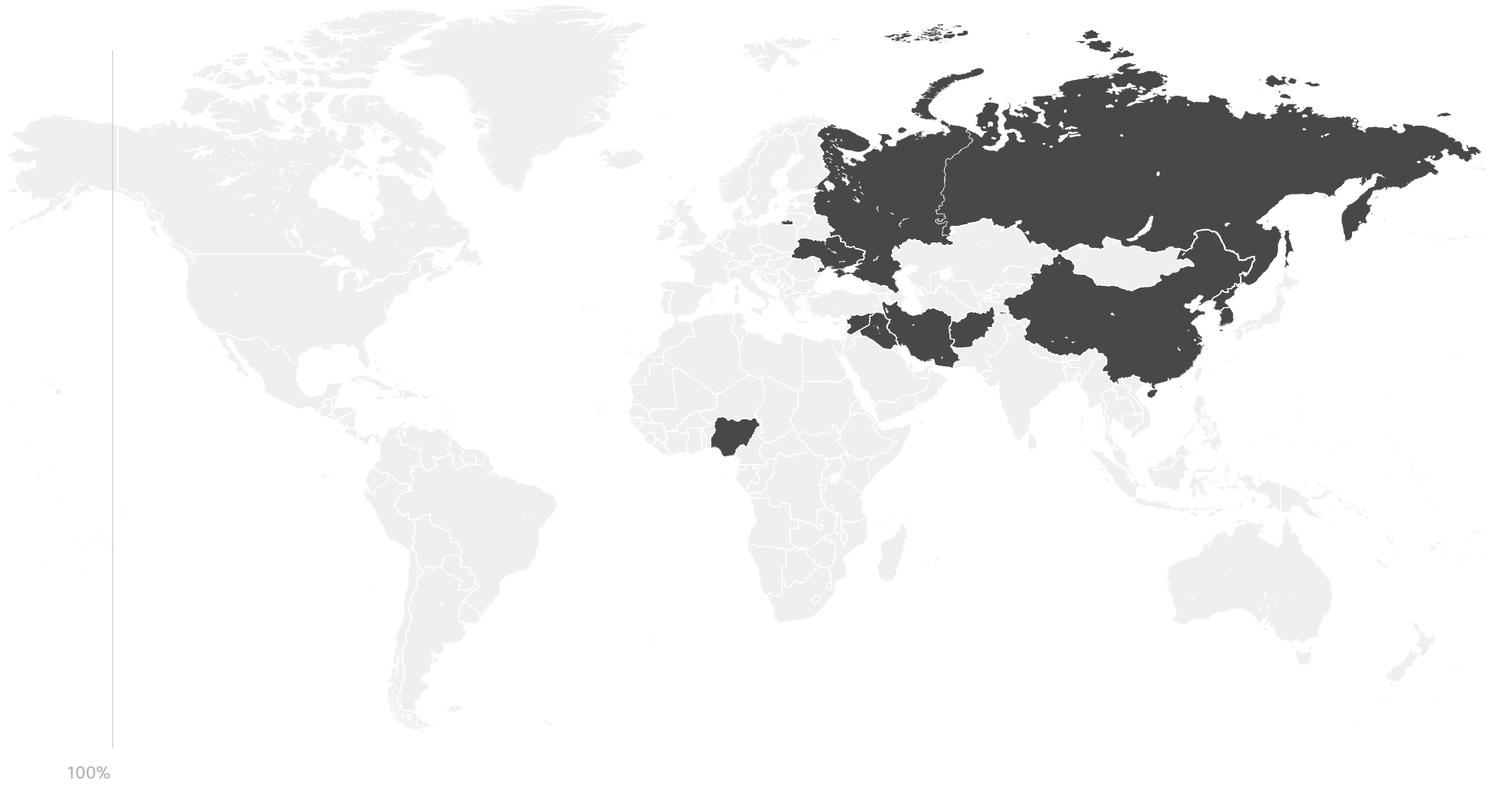
制限された上位の国

Duo のお客様がよく利用するポリシーを確認すると、アクセスを拒否している場所から、お客様がセキュリティの観点でどの国をリスクが高いと見なしているかがわかります。背景はさまざまですが、主な理由は、ブロックされた国の多くを、防御すべき攻撃の発生ポイントと見なしているためです。対象はお客様によって異なり、約 250 の国と地域からのアクセスが制限されています。Duo のデータから、場所の制限が含まれるすべてのポリシーによってブロックされた割合が高い国は、以下の 10 ヵ国であることがわかりました。

場所を制限するポリシーを導入している企業の約 74% が、ロシアと中国からのアクセスを制限しています。また、Duo は、Office of Foreign Assets Control (OFAC; 米国財務省外国資産管理局) の制裁リストに記載されている場所からの認証要求を自動的に拒否します。リストには、クリミア、キューバ、イラン、北朝鮮、スーダン、シリアに位置する IP アドレスが含まれています (本レポートの執筆時点)。

制限された上位の国





適用数が多いポリシー（業種別）

Duo のデータから、業種によって、デバイスの信頼性を確立するために適用されているポリシーが異なることもわかっています。たとえば教育機関は、無効なデバイスからの認証を毎月ブロックしている件数が他の業種よりも多くなっています。一方金融サービス機関は、画面ロックを使用していないデバイスをブロックするポリシーを最も多く導入しています。

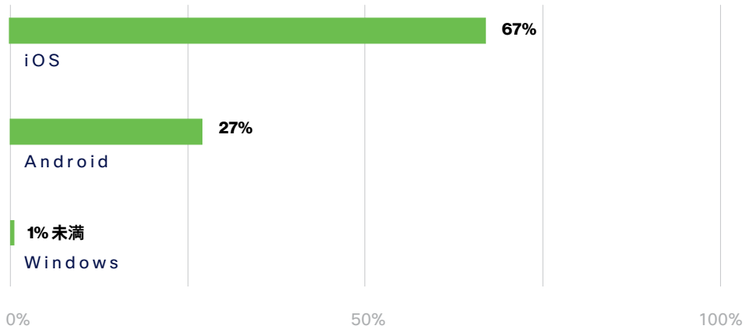
導入数が多いポリシー（業種別）

ポリシー	最も多い業種
未登録ユーザーのブロック	テクノロジー
許可されていないユーザー	金融
場所の制限	IT/ 通信
無効なデバイス	教育
ソフトウェアが古いデバイス	テクノロジー
画面ロック機能なし	教育
ネットワークの拒否	IT/ 通信
バージョンの制限	テクノロジー
ディスク暗号化機能なし	テクノロジー
匿名 IP	教育

iOS の利用状況

Apple の iOS が依然として最も多く利用されていて、デバイスの約 67% を占めています。

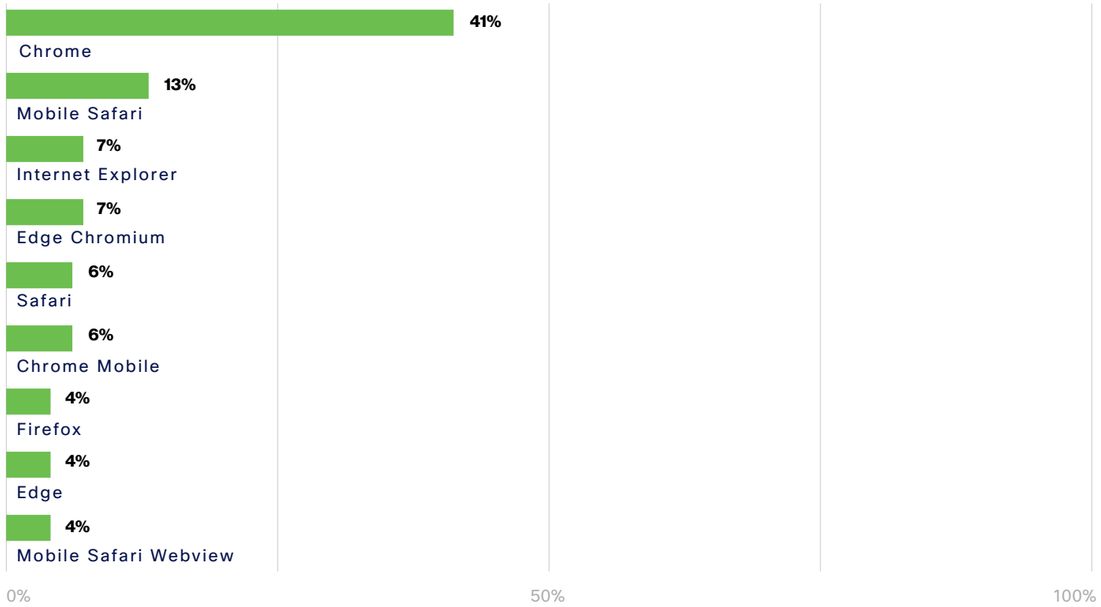
モバイル OS の利用状況



圧倒的な強さを見せる Chrome

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です。Chrome 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

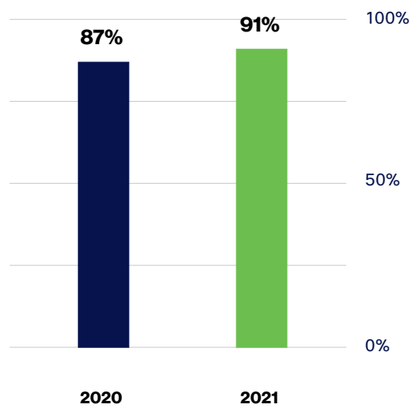


セキュリティ態勢を強化するブラウザ

毎年 Duo では、セキュリティの観点から Web ブラウザがどのように機能しているのかを確認しています。今年の結果から、1 つ希望が持てることがわかりました。2020 年には、ブラウザの 81% に Flash がインストールされていなかったのです。この結果を裏付けるように、Flash は、2020 年 12 月 31 日に**サポートが終了**しました。ユーザーの安全を確保するために、Adobe 社はさらに一歩踏み込み、2021 年 1 月 12 日以降、Flash コンテンツが Flash Player で実行されないようにブロックしました。その結果、2021 年には Flash を実行するシステム数が激減し、現在では 95% のシステムで Flash がインストールされていません。

Java はどうでしょうか。Duo のデータによると、2020 年にはブラウザの 87% に Java がインストールされていませんでした。2021 年には、その割合が 91% にまで増加しました。

Java をインストールしていないブラウザ



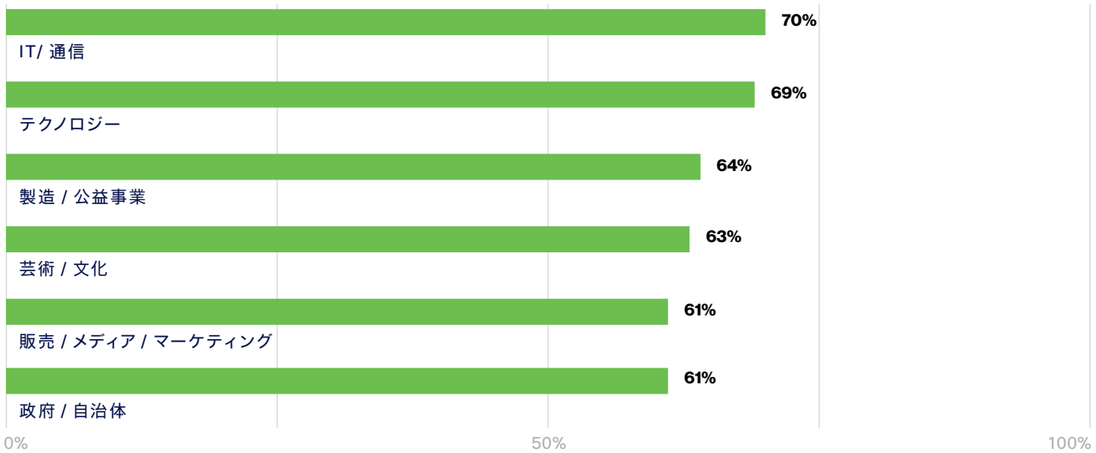
古いソフトウェアを利用しているデバイスの一掃

コラボレーション テクノロジーを活用する企業が増えたため、信頼できるユーザーを明確に特定できることは、セキュリティ戦略の 1 つの要素にすぎません。デバイスのウイルス対策とセキュリティは、現在の標準、もしくは、少なくとも最新のリビジョンに準拠する必要があります。古いソフトウェアを利用しているデバイスは、パッチが適用されていないことによる脆弱性やシステムの設定ミスにより、企業環境のリスクを意図せず高めてしまう可能性があります。その結果、企業が悪意のあるソフトウェアやランサムウェア、データ漏洩などの脅威にさらされることになります。

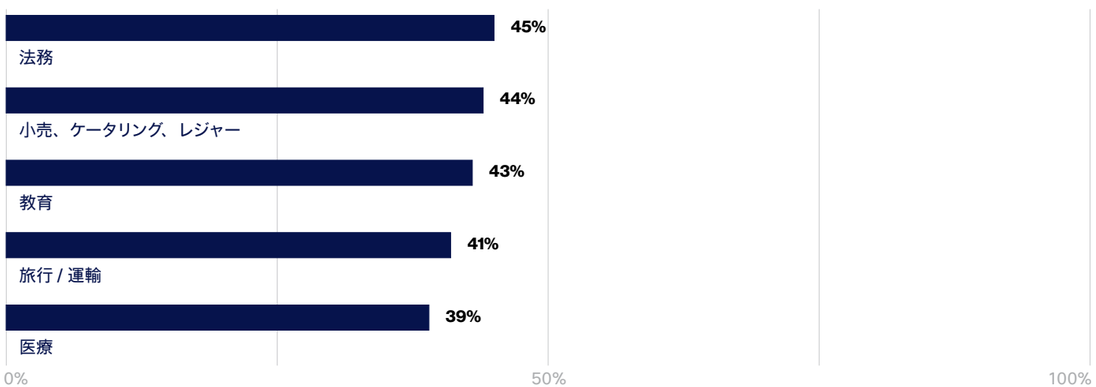
最新のパッチが適用されたエンドポイントの割合は、業種によって大きく異なります。

Duo の調査によると、テクノロジーに精通した業種では、最新のデバイスを使用しているユーザーが多い傾向にあります。一方、新しいテクノロジーの導入が遅れている業種や、手間がかかる時代遅れのシステムを利用している業種では、一般的に、古いデバイスを多く利用しています。

最新状態のデバイスの割合が多い業種



ソフトウェアが古いデバイスの割合が多い業種



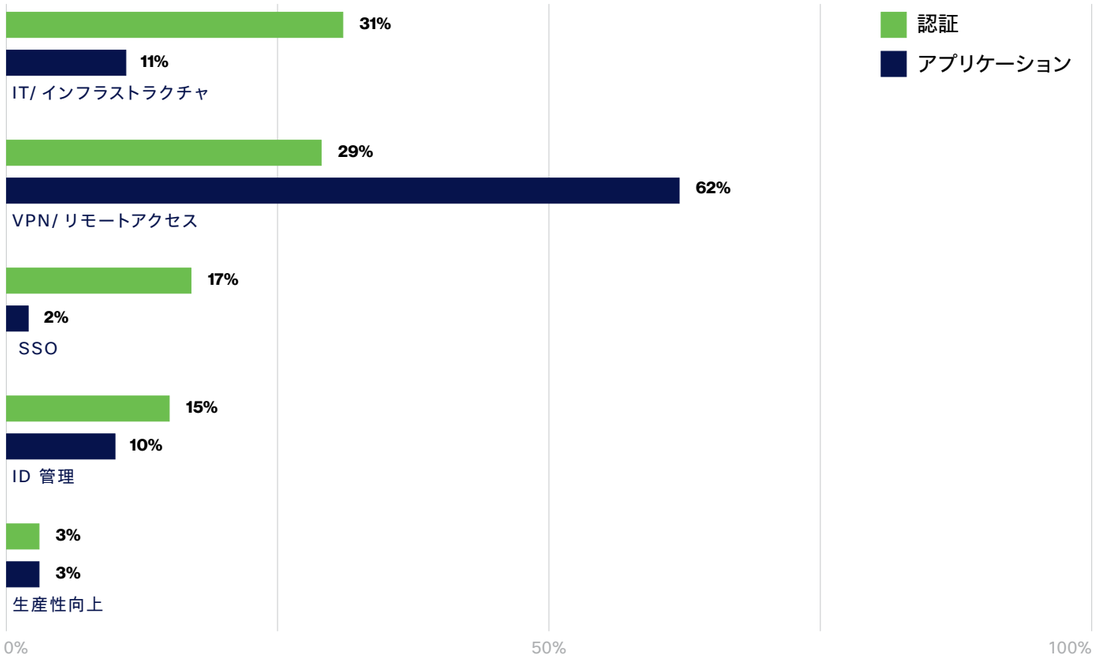
4.0

アプリケーション

企業は、ユーザーやデバイスがアプリケーションやデータに安全にアクセスできるようにするためには、セキュアなアクセスが必要であることを学んでいます。ハイブリッドワーカーが増えている今の状況では、デバイス、ユーザー、データを保護する必要性がこれまで以上に高まっています。これまで多くの組織が、ハイブリッドワーク環境について、あれば便利なものとしか考えていませんでしたが、今やそれ以上の価値があることに気付いています。リモートから業務を遂行できることは、事業を継続するための確実な方法なのです。

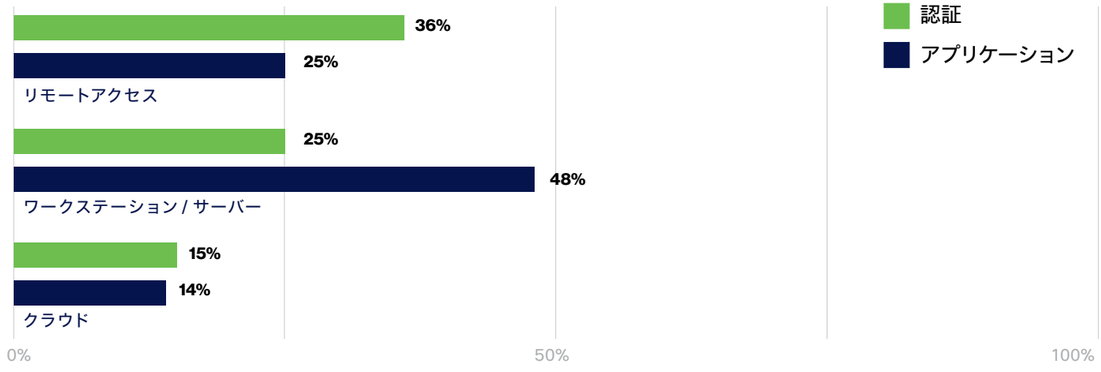
今回、Duo のお客様がアクセスする最も一般的なアプリケーションのカテゴリを調査しました。

アクセスが多いアプリケーションのカテゴリ



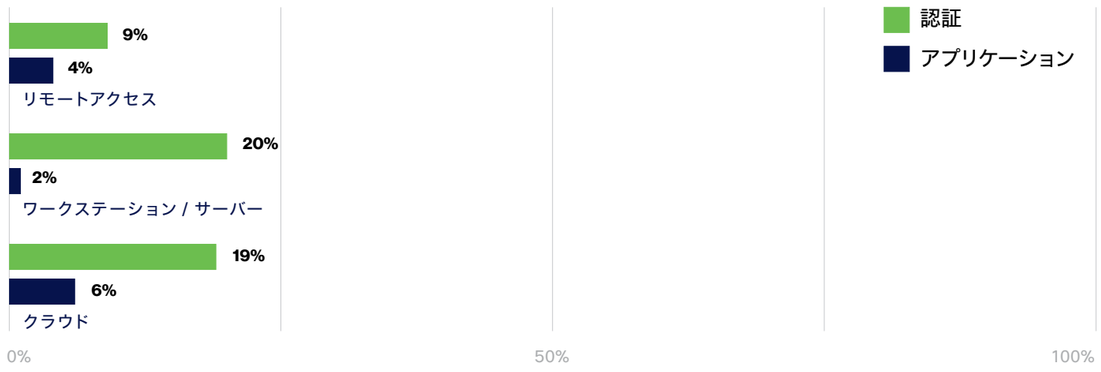
また、アプリケーションへのアクセスについても、アクセスを許可するリソースのカテゴリだけでなく、リソースのタイプについても確認しました。

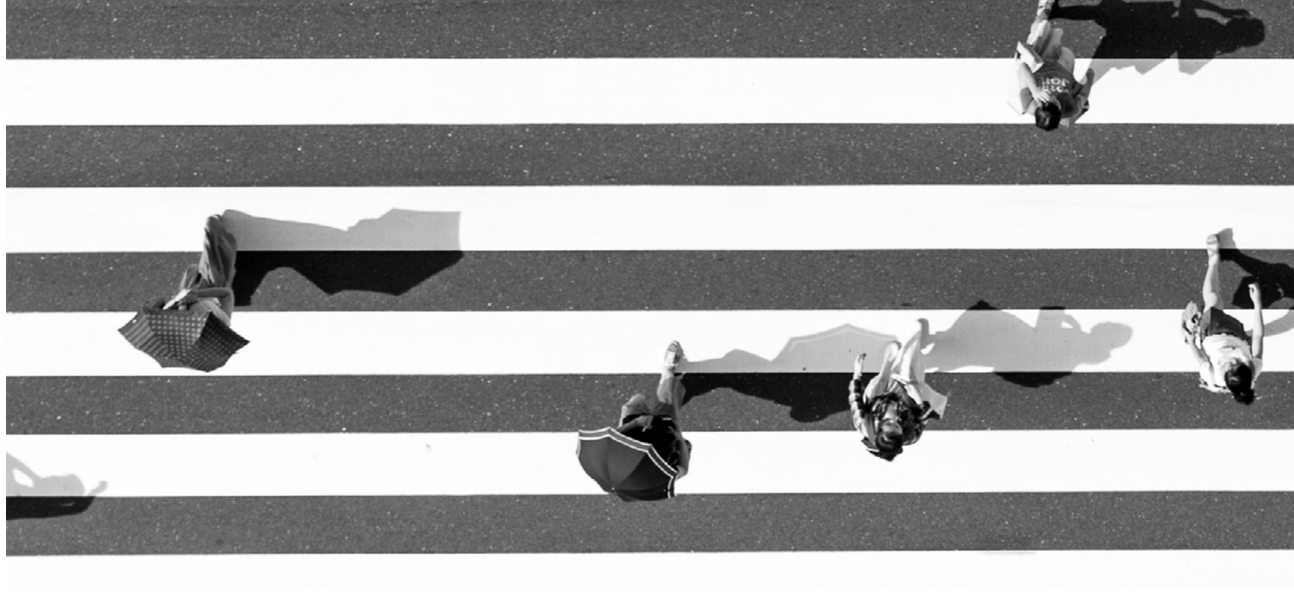
アクセスが多いアプリケーションのタイプ



2020 年から 2021 年にかけてリモートアクセスとクラウドアプリケーションの利用が増え続け、今後もかなりの期間にわたってその傾向が続くと予想されます。またデータは、アプリケーション全体の利用状況と比較して、これらのカテゴリのアプリケーションの利用状況がどのように変化しているかも示しています。

アプリケーション利用率の変化





5.0 サマリー

この 1 年間で多くの教訓が得られました。企業は、中核となる IT セキュリティ機能を効率化して、ハイブリッドワーカーが自分の本来の業務に集中できるようにし、企業内で長く続いているセキュリティ問題に対処する必要があります。

ハイブリッドワークモデルとハイブリッドビジネスモデルが、業務を遂行するための標準的な手順になりました。2020 年の組織は、大規模なハイブリッドワーク環境に急に移行しなければなりませんでしたが、今後も多くの業種において、ハイブリッドモデルが職場文化の中心としてそのまま残るでしょう。企業は、こうした対応を実施する中で、この環境でも生産性を向上できることに気付き、成長を遂げています。多くの組織は、今後も従業員にハイブリッドモデルを引き続き適用する意向を示しています。

一方、ハイブリッドモデルの急拡大によって、新たなセキュリティ課題も発生しました。特に重要なのは、ビジネスに新たなリスクをもたらすことなく従業員が安全に業務を遂行できるようにすることです。企業がリモートアクセス戦略を導入する中で、ユーザーとデバイスおよび、ユーザーとデバイスからのアプリケーションへのアクセスを保護する必要があるという、重要なテーマが浮上しました。

「ゼロトラストアプローチを採用することで、セキュリティの問題に対応できます。セキュリティの問題は時間が経つにつれて拡大し、さまざまな形で影響を及ぼします。デバイスや資産、更新が必要なシステムを可視化できない、簡単な設定ミスを検知できないといった影響です。セキュリティ問題は蓄積していくため、どこかの段階で解消する必要があります。

ゼロトラストなどのアプローチでは、特定のポリシー要件を満たしている場合にのみアクセスを許可するため、このような問題を特定して解消できます。簡単な例としては、デバイスのステータスを確認し、更新プログラムが適用されるまでアクセスを制限することが挙げられます。このように標準的な一定のプロセスを適用することで現在の問題を解消し、さらに問題が拡大することを防止できます。その結果、デバイスが制御不能になるリスクが軽減されます。

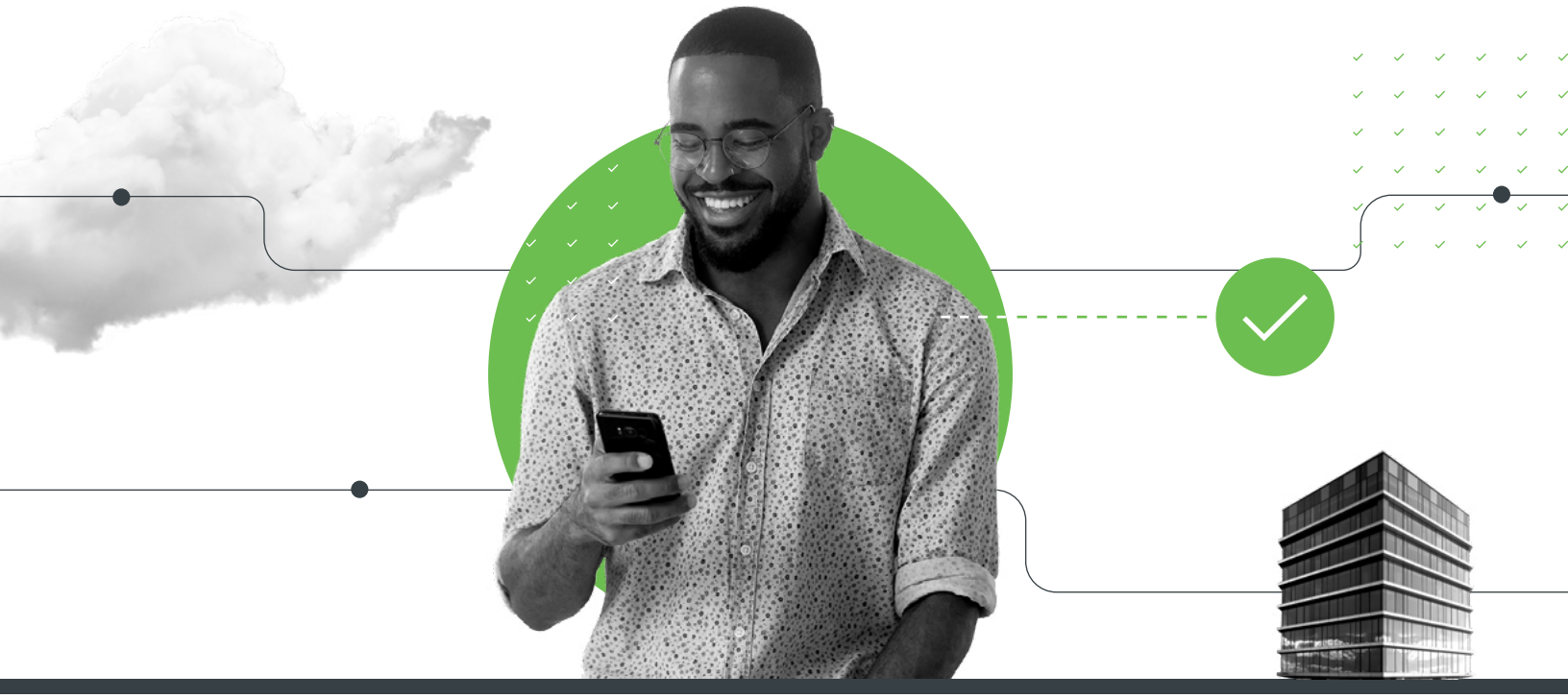
特に注目すべきは、特定の個人データへのアクセスを制限するプライバシー要件の遵守です。多くの場合、過剰な権限が与えられてしまう原因は、スタッフとロールが内部で変更されてしまうことです。変更時に JLM プロセスを適用して管理されていない可能性があります。そのため、必要ないデータに対する過剰な権限が多くのユーザーに付与されてしまいます。

ゼロトラストの原則を適用し、過剰な権限を付与しないようにすることで、組織はコンプライアンスを確保し、このようなセキュリティ問題を解消することができます。同様に、非アクティブなアカウントの数を減らすのにも有効なことが確認されています。これは、時間の経過とともに発生する可能性がある別の形の問題ですが、容易に特定して解消できます」

Richard Archdeacon
Duo Security CISO サポート

Duo が世界中の企業や組織を支援するためには、企業の可視性を高め、ポリシー管理についてより深く理解する必要があります。また、セキュリティチームが現在のリソースでさらに多くのことができるように、自動化を促進することも重要です。ゼロトラストやパスワードレス化などの戦略により、組織のリスクを軽減しながらセキュリティを強化できます。ユーザーエクスペリエンスに重点を置くことで、セキュリティがユーザーに受け入れられやすくなります。最後に、ポリシー適用に対する賢明なアプローチにより、セキュリティチームが業務を安心 / 安全に遂行できるようになります。

Duo の使命は、自宅、オフィス、その他のどのような場所で業務を遂行する場合でも、あらゆる規模の組織がアプリケーションにより安全にアクセスできるようにすることです。ハイブリッドワークモデルにおける Duo のアクセスセキュリティは、場所を問わずに、すべてのユーザー、デバイス、アプリケーションを保護するように設計されています。



「ハイブリッドな職場環境は、従業員がどこからでも安全につながり、効率よく仕事できる必要があります。そのために当社は、クラウド導入の促進、確実なリモート接続戦略の策定、セキュア アクセス サービス エッジ（SASE）の導入を進めています」

Binaya Sharma 氏
IT インフラストラクチャ担当ディレクタ
TechnoPro 社

duo.com から 30 日間の無料トライアルを開始し、すぐにすべてのユーザー、デバイス、アプリケーションを保護してください。

The bridge to possible

シスコ グループの一員となった Duo Security は、業界をリードする多要素認証（MFA）およびセキュアアクセスのプロバイダです。Duo は、シスコ ゼロトラスト製品の重要な柱の 1 つであり、さまざまな IT アプリケーションや環境において、ユーザー、デバイス、場所を問わずにアクセスを保護する最も包括的なアプローチです。Duo は、Bird、Facebook、Lyft、ミシガン大学、Yelp、Zillow など、世界 25,000 社以上のお客様に信頼されているパートナーです。Duo はミシガン州アナーバーで設立され、テキサス州オースチン、カリフォルニア州サンフランシスコ、ロンドンにもオフィスを構えています。