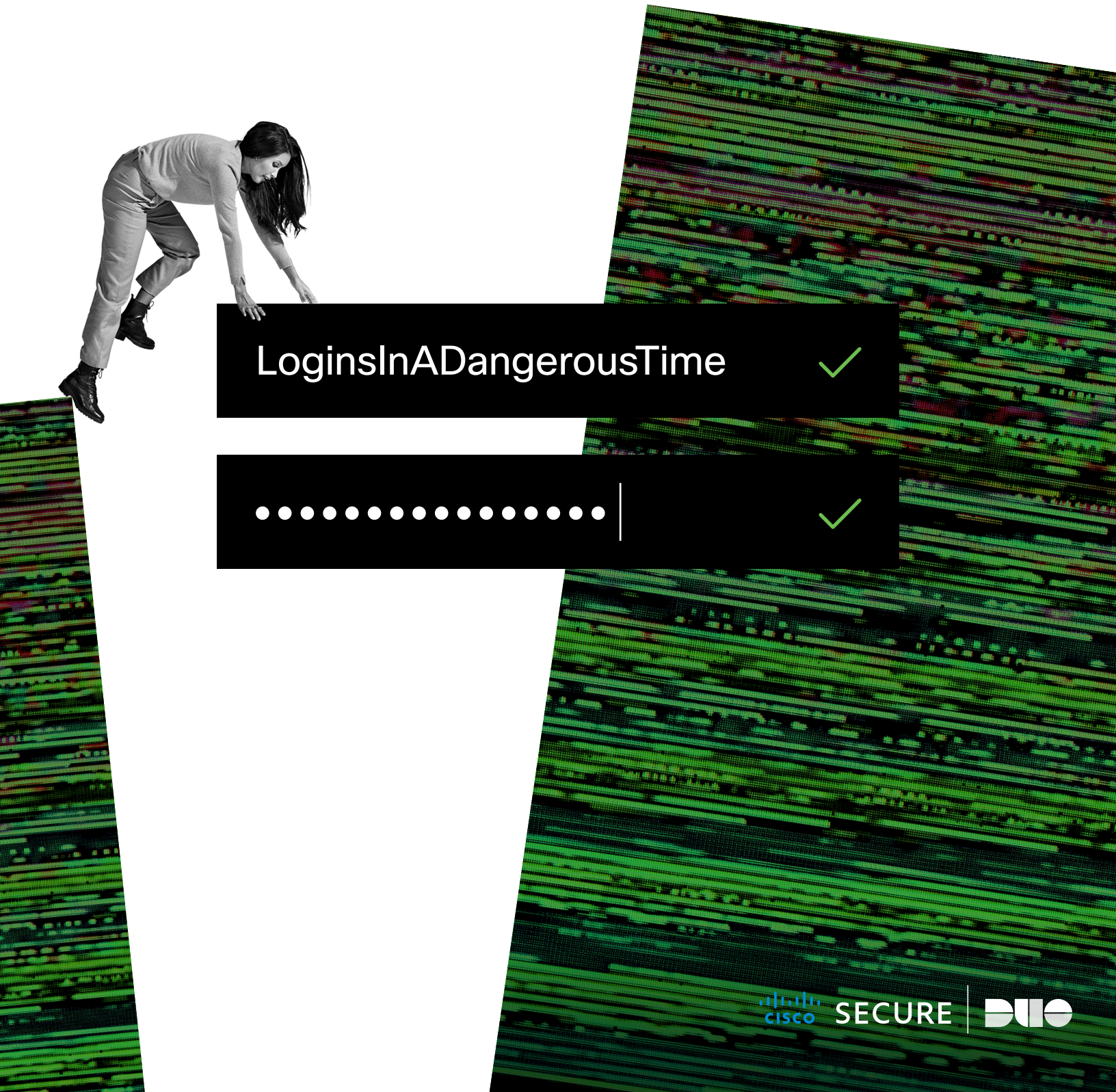
2022 年 Duo

Trusted Access レポート



著者
DAVE LEWIS

データサイエンス
BEN EDWARDS
CYENTIA INSTITUTE 社

編集
CHRYSTA CHERRIE

設計および開発
MARLA JONES
TRACY TOEPFER

2022 年 Duo

Trusted Access レポート

危険な時代のログイン

バージョン 1.0

危険な時代のログイン

Trusted Access レポートは、Duo 製品のデータとお客様による Duo の活用方法を分析し、結果をまとめた年次レポートです。本年のレポートは、私たちが現在置かれている状況を反映して、**昨年のレポート**とは明らかに様相が異なっています。

このレポートの目的は、恐怖、不確実性、疑念を増やすことではありません。むしろ、今日セキュリティが置かれた状況の重大さを理解するためにご活用ください。世界的な紛争がデジタル領域に飛び火している今、個人から企業までの包括的な保護という構想に対する危機感が強まっています。

本レポートでは、この一年間で北米、中南米、ヨーロッパ、中東、アジア太平洋の顧客ベースにわたり約 5,000 万の異なるデバイスから収集された、130 億以上の認証に関する調査結果データを検証します。

主な調査結果の中には、いくつかの明るい兆しも見られました。パスワードレス認証の導入が増え続けていることがわかりましたし、Duo を使用した認証数は 41% 増加しました。一方、生体認証を利用できる携帯電話の割合は過去数年間着実な増加を見せていましたが、81% で停滞しています。また、大変興味深いことに、地理情報に基づいたブロックポリシーを活用している組織がほとんどないこともわかりました。防御側は、サイバーセキュリティ関連の脅威に対抗するために役立つあらゆる情報を必要としているため、この状況を把握できたのは朗報です。

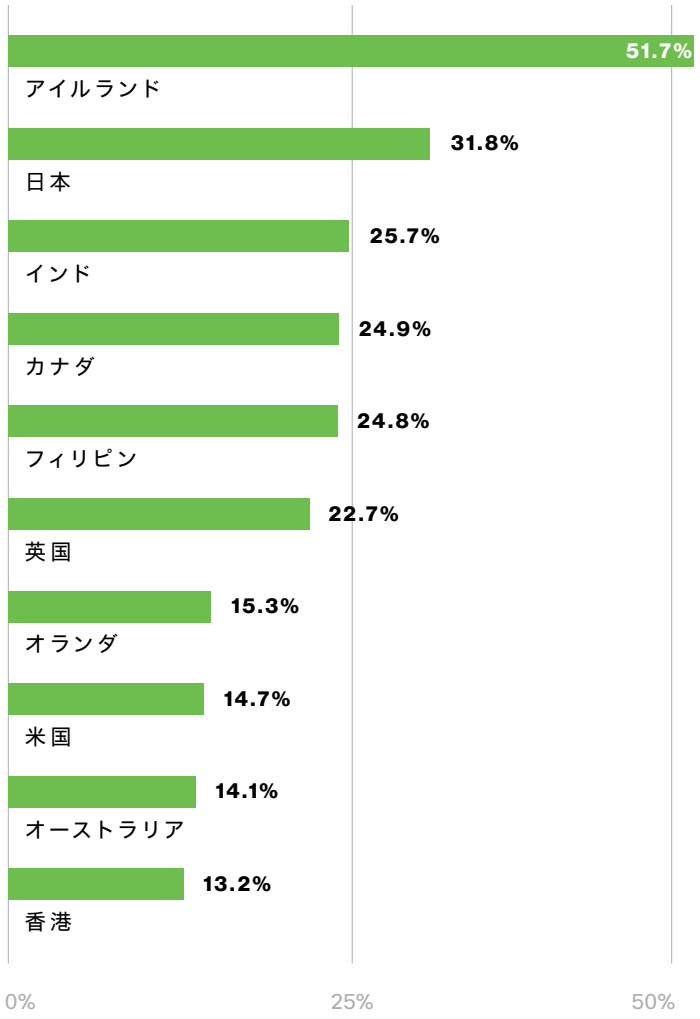
以前のレポートではパスワードの複雑さについて論じましたが、今回は多要素認証 (MFA) とパスワードレステクノロジーへの投資がビジネスを展開するために必須のコストであるという点について議論を展開します。

ここで紹介するテクノロジーは、直面するさまざまな攻撃者からの保護策として、組織のリスクを軽減するのに非常に大きな役割を果たします。

近代の先進国同士の対立により属国のために戦地に送り出された、長く語り継がれる伝説の戦士の苦境を例にとってみましょう。ギリシャ軍がファランクスを形成して戦闘に参加して以来、テクノロジーは常に攻撃の成功にも失敗にも寄与してきました。たとえばカタパルト、マスケット銃、Enigma Machine といったテクノロジーが登場しました。サイバー戦争も、表面上はこうしたテクノロジーと相違ありません。現在でも実際の武力衝突の最中に置かれた戦闘員がいます。テクノロジーによって片方の陣営が有利になるというのは、いつの時代にも共通して言えることです。そして最新のテクノロジーは、悪意のあるソフトウェアを介してコンピュータを侵害する機能をもたらしました。その結果、一層大規模な監視作戦の実施、そして何より、インテリジェンスの収集および処理能力が向上しました。情報革命が現代の武力衝突に影響を与えていることは間違いありません。

このような脅威に直面していることを受け、アイルランド、日本、インド、カナダ、フィリピンをはじめ世界で MFA 認証の導入が進んでいることが確認されています。このことから、多くの国々が課題に立ち向かい、今日の脅威から自国のシステムを防御しようとしていることがわかります。この世界的な脅威環境がもたらしている影響は、このレポートで検証する Duo 製品の使用状況データで確認できます。

図 1：認証数が最も多い国における対前年比 MFA 増加率



RAND Corporation が**文書**『Cyberwar is Coming (サイバー戦争がやってくる)』を発行してから約 30 年が経ちました。この文書はサイバー戦争の概念に言及していますが、著者が思い描いていた、直面する課題に対処するには知識を機能に転換しなければならないという考えが現実のものとなりました。現在のウクライナでの戦争を例にとると、情報を収集し被害を及ぼすために、双方が互いのネットワークやシステムへの侵害を試みています。

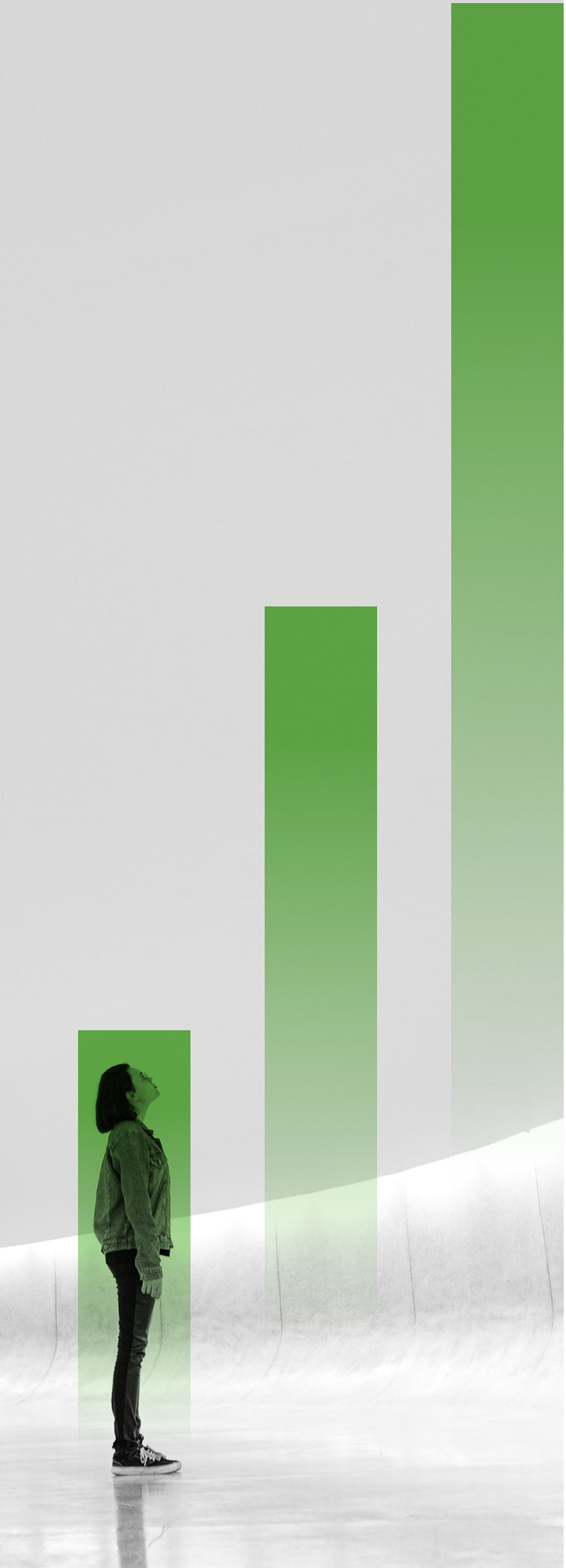
サイバー戦争能力の増強を目指すウクライナ政府は、ハッカーの助けを借りてロシアの標的を攻撃しました。こうしたハッカーたちは、破壊的な機能を活用するだけでなく、ウクライナの自国の防衛力を強化するためにオープンソース インテリジェンス (OSINT) データも収集しています。

監視は今日の戦闘において欠かせない要素となっています。核戦争には相互確実破壊 (MAD) などの抑止力がありますが、サイバー戦争にはこれに匹敵するものがありません。歴史上、監視行為は何度も繰り返されてきましたが、GPS、携帯電話プロバイダー、衛星画像を駆使する現在の紛争ほど監視が広く実施されたことは、かつてありませんでした。

情報収集はサイバー戦争に不可欠です。ウクライナでの戦争を例にすると、戦場での装甲車の標的化から、サプライチェーンの分断、軍艦の破壊にいたるまで、私たちは情報セキュリティが重要な役割を果たしたシーンを目の当たりにしました。これらはすべて実際の戦場でのみ行われたように見えるかもしれませんが、コンピュータベースの OSINT データの援助があったことは明らかです。これに対抗するために、防御側は攻撃側のシステムやリソースへのアクセス能力の破壊を試みています。

Duo は、ウクライナや、重要な政治的出来事を経験したその他の地域 (香港など) に拠点を置く組織が、さまざまな国から認証を試みていることを確認しました。WebAuthn などのパスワードレステクノロジーとともに、攻撃的な攻撃対象領域の大部分に対抗できる強力なインテリジェンス機能を導入することは、インターネットにアクセスできるどの国にとっても、攻撃および防御戦略の観点から見て、サイバーセキュリティに対するある程度の投資になります。

サイバー戦争は、独立した戦場ではなく、戦力を増強する手段です。ギリシャが導入したファランクスと同様に、サイバー戦争は現代の戦争の在り方に根本的な変化をもたらしました。RAND 文書で紹介された、サイバー戦争が軍縮につながるという考えは実を結んでいません。サイバー戦争は解決策ではありません。そして Stuxnet に関して言えば、影響がサイバー空間を超えて実空間に及んだことは明らかです。この事例は、敵に対抗するための道具としてサイバー戦争が加わったことの証拠になります。



今日の世界には多くの危険があります。このことについて誰も驚くことはないでしょうが、繰り返して伝えることに価値があります。

私たちが過去のツールに依存し、それらのツールを使用して敵を倒そうとすれば、自分たちの首を絞めることになります。

攻撃者は、私たちに不当な危害を与える新たな興味深い方法を常に模索しています。脅威を不法な金銭的利益を得るためのツールとして捉えるだけでなく、致命的な戦闘能力をさらに増強するものと考えて議論を行うと、サイバーセキュリティの問題に対処するために必要となる重要な機能が、いかに先見の明であったかがわかります。

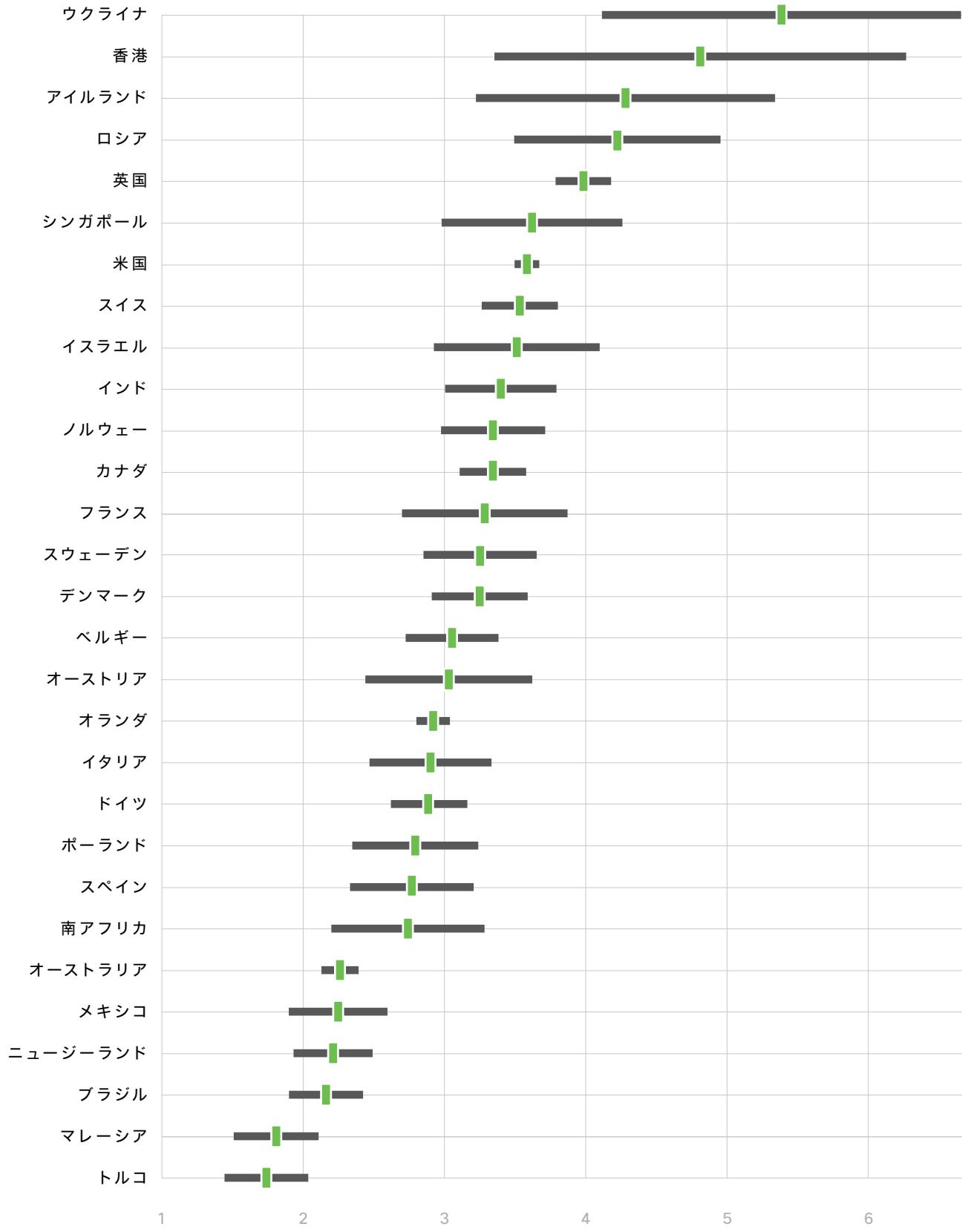
しかし、まだ望みはあります。Duo は、防御側の組織に有利になるよう局面が変化する兆候を確認しています。攻撃者は、多要素認証 (MFA) で保護されたシステムに遭遇すると、多くの場合認証の継続が難しいと判断するため、妨害行為は減少します。この行動には説明がつきます。MFA に遭遇した攻撃者は、多くの場合 MFA に関わろうとせず他のターゲットに移動します。より易しいターゲットの方が成功を収めやすいからです。実際、特定の地理的な場所を拒否する何らかのポリシーを使用する組織の割合は、2020 年以降 20% 減少しています。

しかし、組織が明示的に拒否しているのはどのような国からの認証でしょうか。図 3 は、拒否された上位 20 ヵ国を示しています。2022 年の例を挙げると、具体的な拒否ポリシーを持つ組織の 82% がロシアからの認証を拒否しました。このグラフで注目すべきことは、上位 20 ヵ国を対象とする拒否ポリシーは実際に減少している一方で、上位 6 ヵ国を対象とするポリシーは比較的変動がないことです。このグラフの外れ値であるベラルーシは、全体の 20 位から 8 位に急上昇しました。

この数年間を振り返ると、ハイブリッドワーク環境への大規模な移行が世界的に見られました。在宅勤務は時折行われる程度でしたが、企業はビジネスを継続していくために、ほぼ一夜にしてワークフォース全体を在宅勤務に移行させました。

図 2：さまざまな場所に拠点を置く組織が認証を受ける国の平均数

縦軸は組織の主要拠点です。中央の緑の長方形は平均値を表し、灰色のバーは平均の推定値の 95% 信頼区間を表します。たとえば、ウクライナに拠点を置く組織は、平均して約 5.5 の異なる国から認証を受けています。

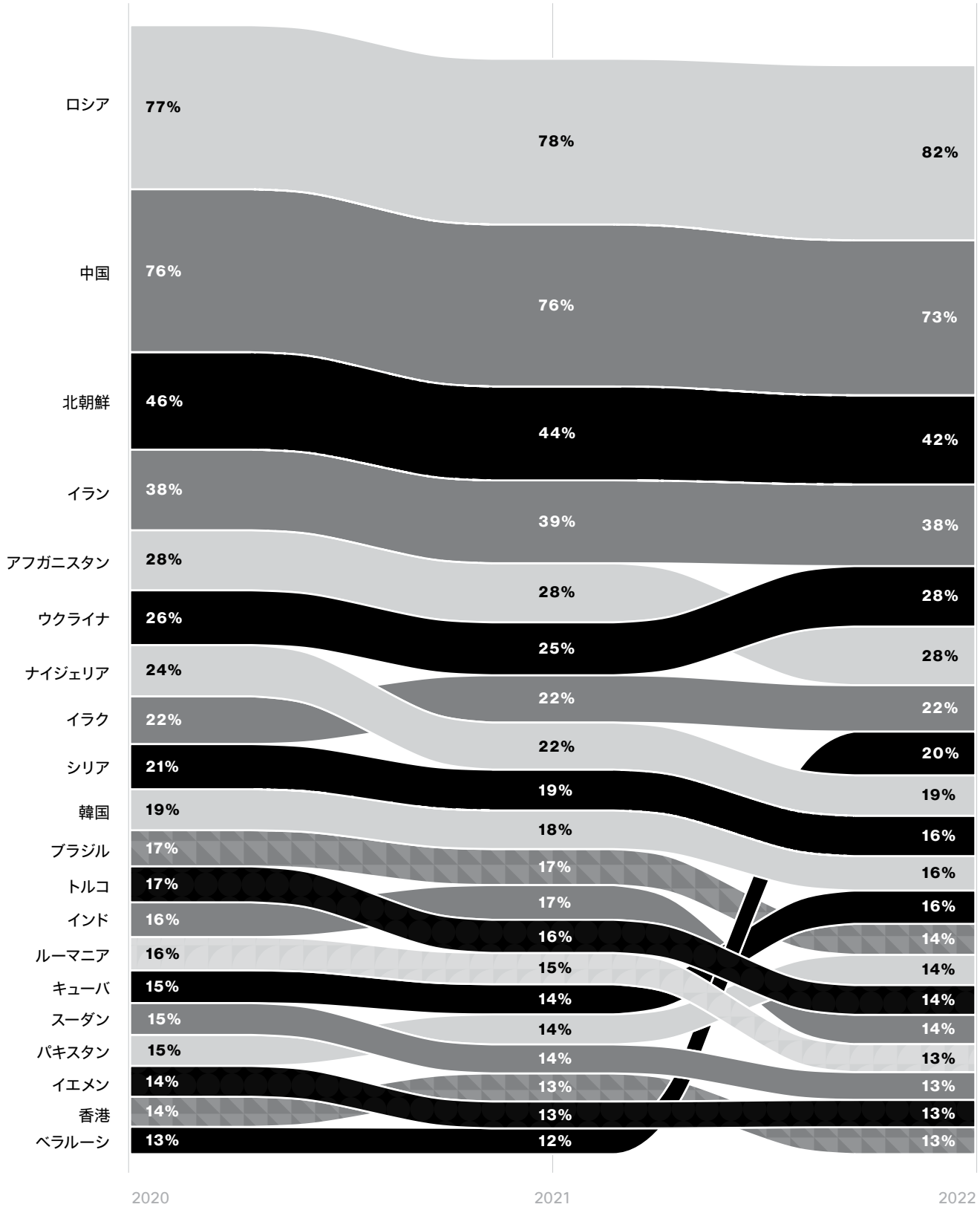


昨年のレポートでは、家の鍵と同等の機能を持つものとして、非常に古いセキュリティ管理であるパスワードに言及しました。本来はアクセスできないリソースにアクセスするために企業や個人を狙う攻撃者は、パスワードが鍵に似ていることを認識しています。実際の戦争に従事している国は、大義を支え、標的を監視し、さらには敵を破滅させるために、盗み出したパスワードも駆使してデータや知的財産を手に入れています。

MFA は、組織が侵入に対する防御を強化するために使用できる 1 つの手段です。MFA によって、敵が組織や個人を攻撃するための最も簡単な手段の 1 つを排除または削減できます。想像してみてください。敵が盗み出したアクセスを 1 日使用できるだけで、どれだけの損害をもたらすことができるでしょうか。多くの場合データ侵害は何週間も発見されないこと考慮すると、起こり得ることを想像するだけで恐ろしくなります。

現在、サイバーセキュリティは転換期を迎えています。MFA がどの組織にとっても基本的な要件であることは明らかです。世界中の企業はこれまで、企業全体の保護ではなく、ミッションクリティカルな資産を保護するために MFA を活用してきました。COVID-19 パンデミックから、世界はいくつかの貴重な教訓を学びました。企業は、ワークフォースをハイブリッドモデルに移行させるにあたり、アクセスを保護するより優れた手段を見出す必要性に直面しました。企業のセキュリティチームは、スタッフの在宅勤務に起因する非常に多くの変動要素のリスクを減らす手段として、すべてのアクセスに MFA を追加する措置を講じました。

図 3 : アカウントが過去 3 年間にポリシーによって拒否した国



方法論

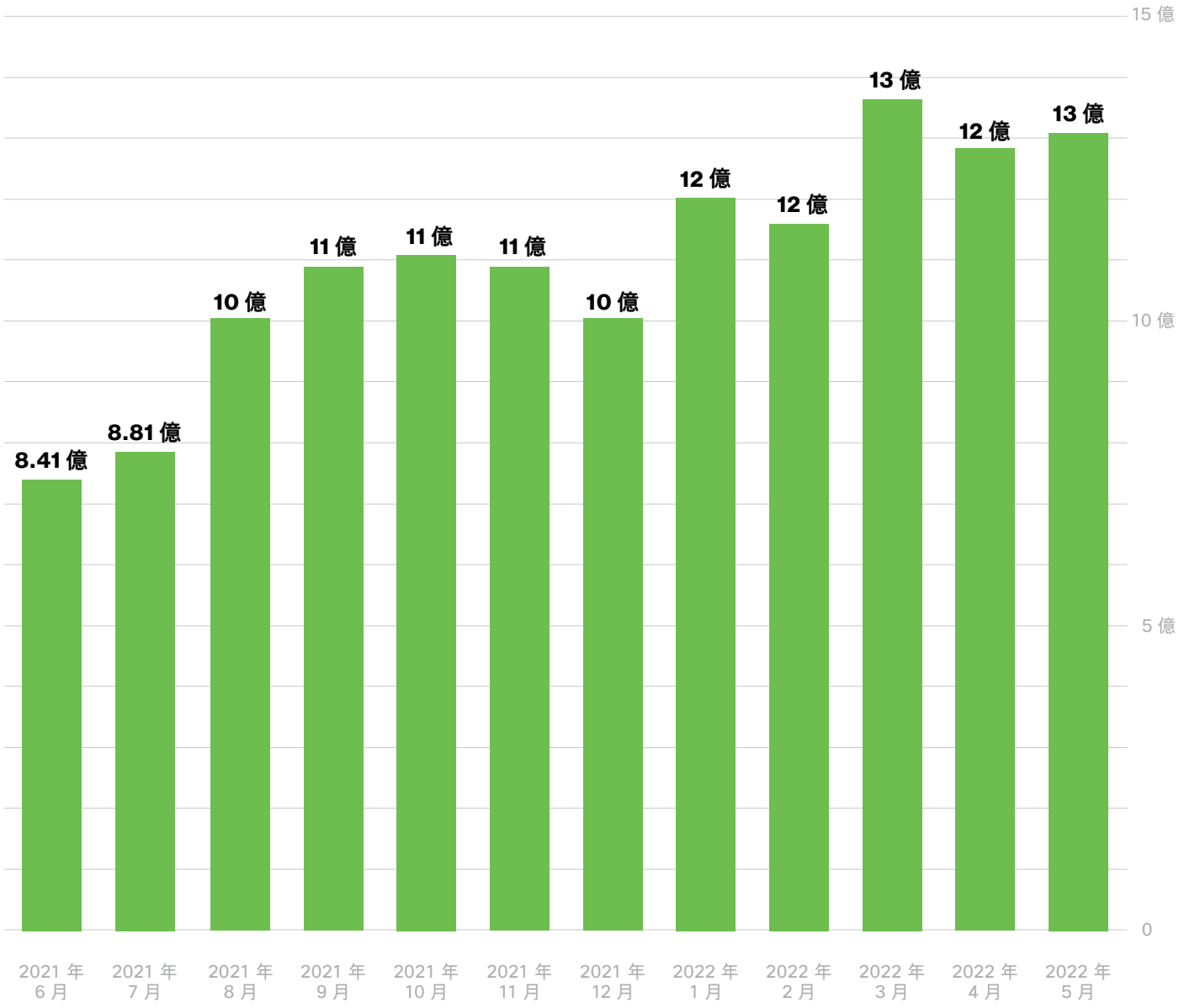
ゼロトラストセキュリティ戦略には、ユーザー、デバイス、アプリケーションという 3 つの柱があります。そのため、以下の質問が重要になります。

- 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？
- 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？
- 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 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 4,900 万台を超えるデバイス、49 万種類を超えるアプリケーション、および 130 億件 (月間約 11 億件) の認証に関するデータを分析しました。Duo では、2021 年 6 月 1 日から 2022 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、2022 年 5 月 31 日にメトリクスを測定しました。

前年との比較のために、2020 年の認証期間を 2021 年 6 月 1 日から 2022 年 5 月 31 日までと定義しました。認証以外の 2022 年のデータについては、2022 年 5 月 31 日にメトリクスを測定しました。

図 4：月別合計認証数



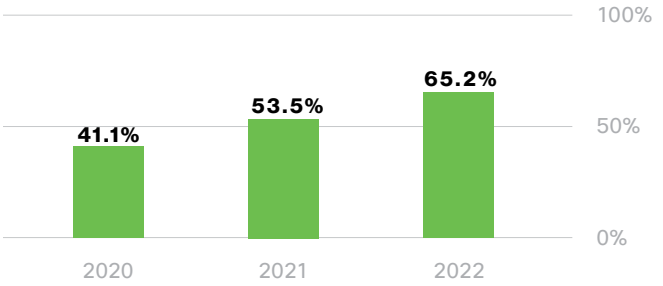
主な調査結果

上位 10 のトレンドの概要

01 パスワードレスの採用の増加が続く

Duo のデータによると、2019 年 4 月以降、WebAuthn 認証を許可するアカウントの割合が 50% 増加し、WebAuthn の使用が 5 倍増加しました。

図 5：増加が続くパスワードレス認証



02 生体認証の導入が停滞

生体認証を利用できる携帯電話の割合は 81% あたりを推移し (2021 年から若干増加)、生体認証の全面的な導入への進捗は停滞しています。

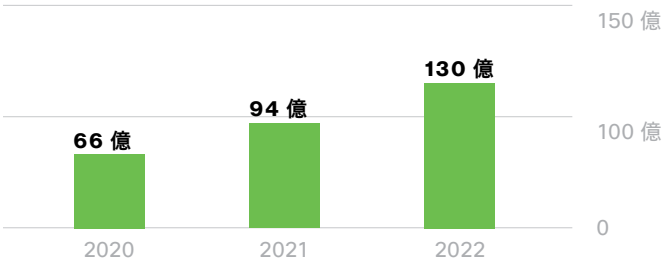
03 PUSH の利用が増加

最も使用されている認証方式は Duo Push で、全認証の 27.6% を占めています。

04 MFA によるパスワードの強化が続く

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 を使用した MFA 認証の数は、過去 1 年間で 38% 増加しました。

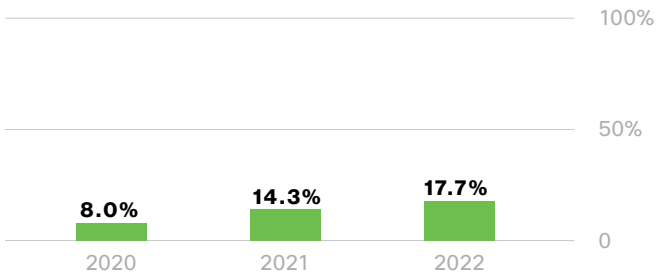
図 6：MFA 認証総数



05 増加が続くクラウドの使用

認証数の増加はクラウドアプリケーションに起因しています。2022 年はクラウドアプリケーションの割合が 24% 増加しました。

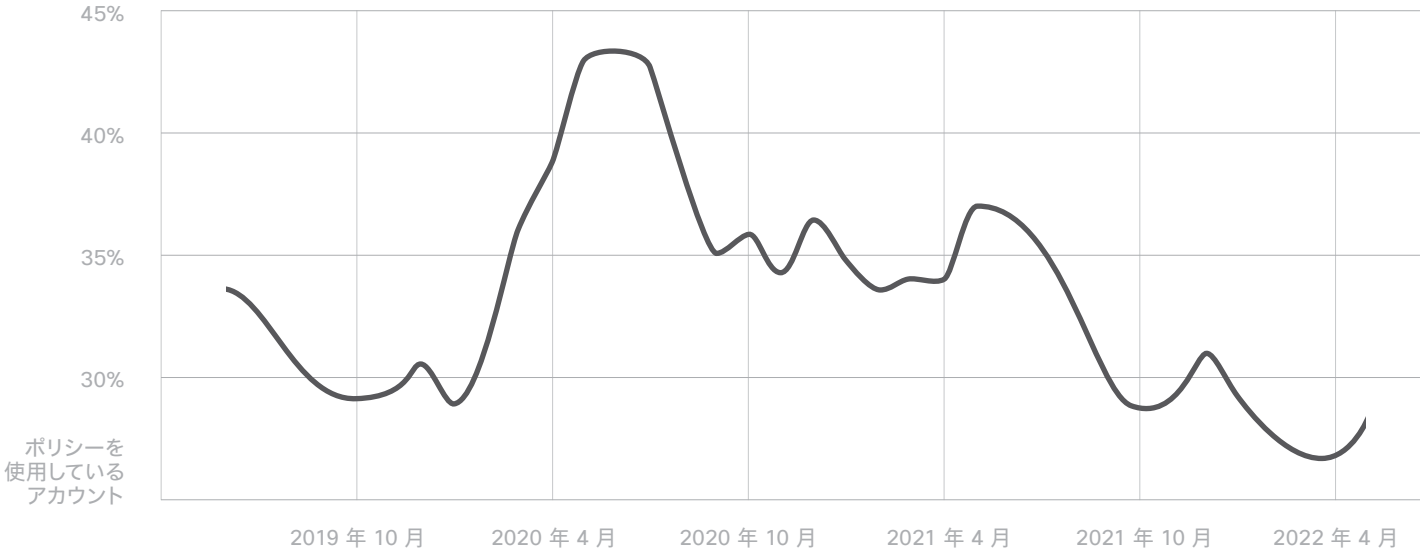
図 7：クラウドアプリケーションの対前年増加率



06 オフィスへの復帰

リモートアクセス認証は 2020 年にピークに達しましたが、それ以降は減少が続き、パンデミック発生前のレベルよりも低くなっています。

図 8：リモート アクセス アプリケーションの認証



07 ブロックされたロケーション

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。明示的な拒否または許可ポリシーを導入している組織は 1% 未満です。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。

08 古いソフトウェアを搭載したデバイスによる認証失敗が増加

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、2021 年から 2022 年の間に 51.8% 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 7.1% 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。

09 企業が時代とともに進化

2022 年 2 月にロシアがウクライナへの侵攻を開始すると、ウクライナ国内からの認証が大幅に減少していることが確認されました。ウクライナ国民の日常生活が一変したのですから、当然のことです。このことは、やがてアクセスを必要とするときに取得可能なあらゆる場所から安全に認証を受ける必要があるモバイル利用者の問題へと化していきました。システムにログインする人の身元を確認することの重要性がさらに高まっています。

今日のニーズに対応するためには、セキュリティ管理の強化が必要です。パスワードは長い間セキュリティ管理の手段と考えられてきましたが、今日ではパスワードの有用性に限界があることを理解しています。MFA やパスワードレス認証といった最先端のセキュリティ管理に移行することで、認証されている人物が実際にしかるべき本人であるという確信をはるかに高めることができます。一方、パスワードを管理手段として使用する場合は、最善の結果が得られることを期待するしかありません。

昨年のレポートでは、セキュリティ手段としてパスワードと家の鍵を比較しました。確かに、自分と自分の資産を守るためにドアに鍵をかけることはできますが、正面玄関から入ってくる人が、実際にしかるべき本人であることを実証できるものは何もありません。かつてから使用されているパスワードが有効だった時代は終わりました。

私たちの社会は、世界的なパンデミックと闘う段階から、世界的な軍事紛争に対処する段階へと移行しました。この軍事的衝突はサイバー領域に波及し、戦地とは遠く離れた個人や組織に直接的影響を与えています。推奨されないセキュリティ管理への対応が、いまだかつてないほど急務になっています。

ハイブリッドワーク環境は、企業が機能し続けるために利用できる明らかな選択肢としての地位を確立しました。敵もまた、この新しい現実に適応しています。ハイブリッドワーカーのワークライフバランスは、安全かつ確実に仕事を遂行できるようにするセキュリティ機能によって強化する必要があります。

世界中の企業が、この新しいパラダイムに適応する必要性を認識しています。私たちは、緊急事態に対処する段階から、ハイブリッドワークに対応する機能を維持および拡張するための最適な長期戦略を策定する段階へと移行しました。

ユーザーエクスペリエンスの向上

世界中の従業員がハイブリッド方式で働いている現在、セキュリティがユーザーに広く受け入れられるように、全体的な要件を継続的に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。

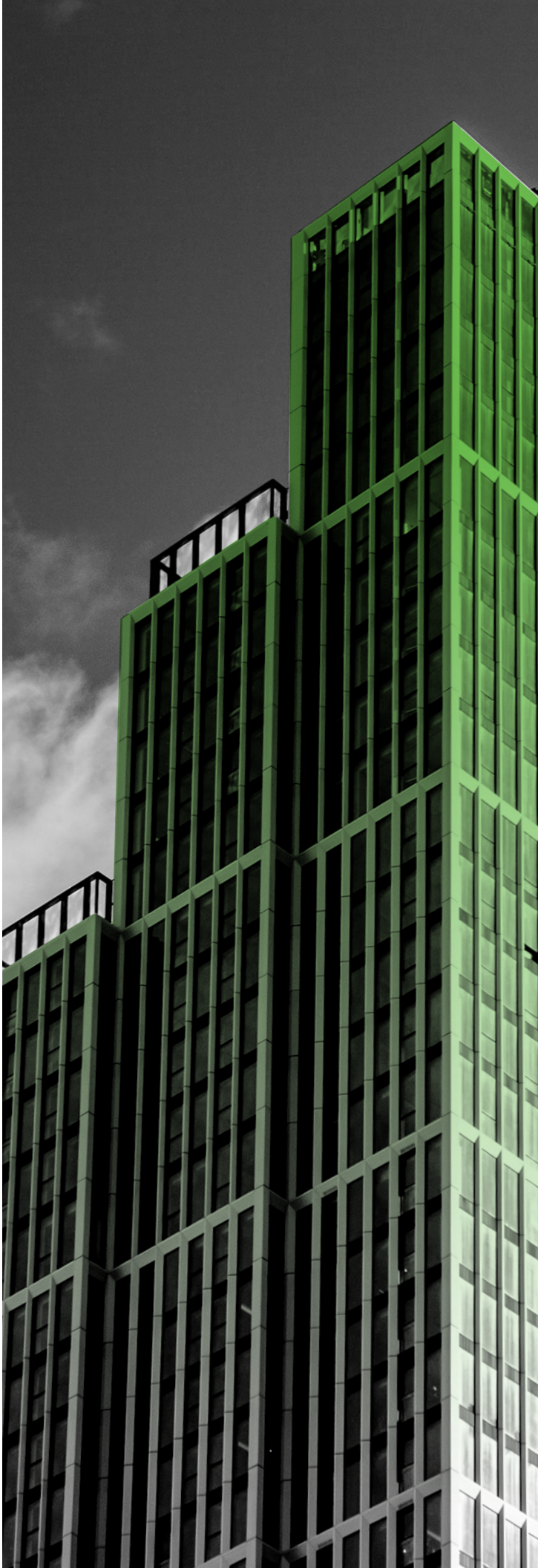
これまでのセキュリティワークフローは、サポート期間が過ぎて効果がなくなったセキュリティ制御機能を使用することで、成果をあげられていませんでした。その最たる例がパスワードです。物理的なオフィスの場所に縛られることなくグローバルに分散したワークフォースに対応しようと、セキュリティはさらに効率化が進んでいます。

このレポートを作成するために、Duo は Cyentia Institution 社と提携して、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 4,900 万台を超えるデバイス、49 万種類を超えるアプリケーション、および月間約 11 億件の認証に関するデータを分析しました。Duo では、2021 年 6 月 1 日から 2022 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、2022 年 5 月 31 日にメトリクスを測定しました。

デバイス：4,900 万台以上

アプリケーション：49 万種以上

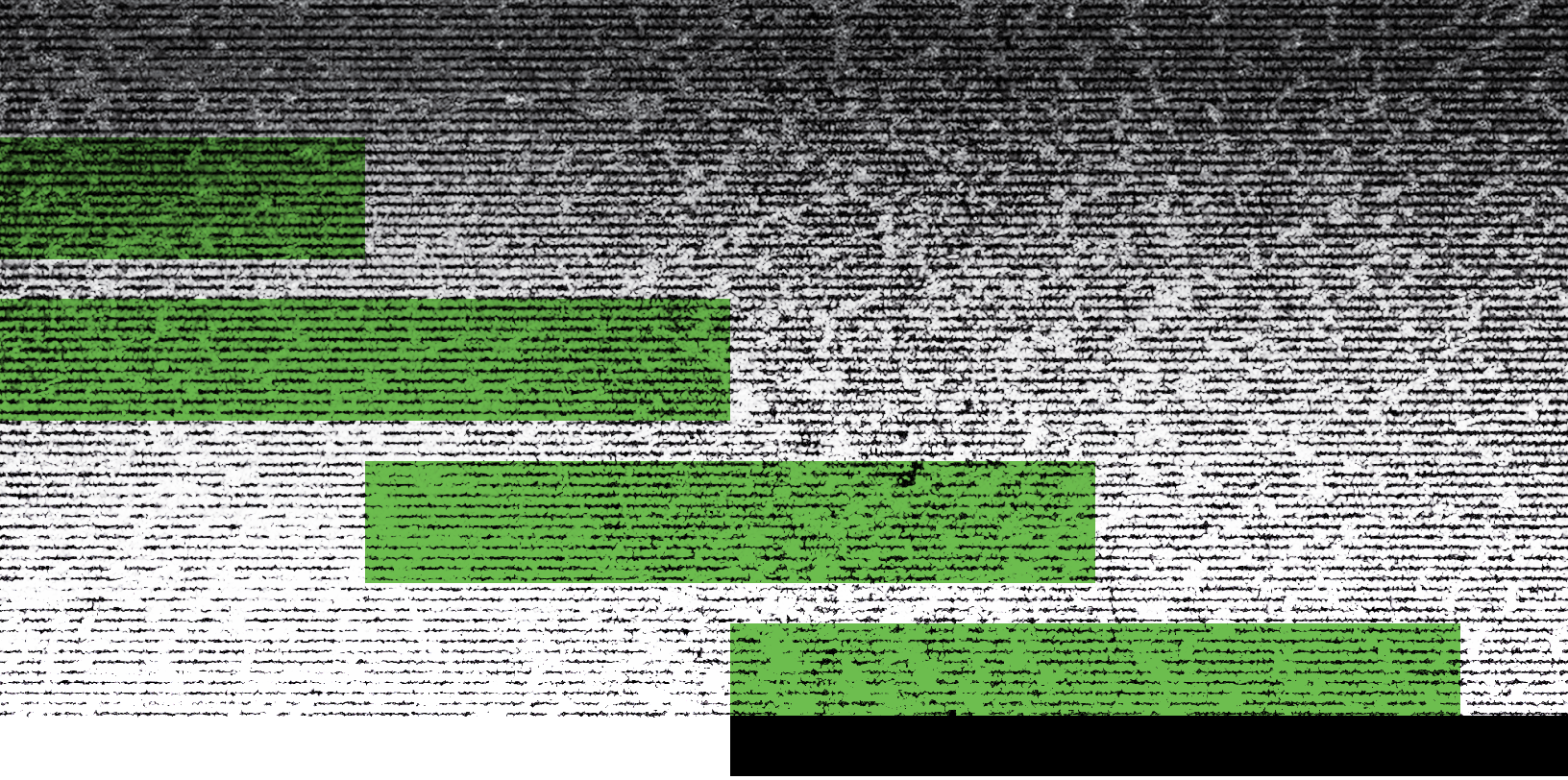
1 ヵ月あたりの平均認証件数：11.06 億以上



Talos の視点

シスコファミリの強みの 1 つは、Duo チームに加えて、Talos Intelligence チームの貴重な貢献を得られることです。Talos は、防御に関するガイダンス、フォレンジック分析、インテリジェンスを提供し、脅威ハンティング活動に従事することで、**ウクライナ政府を積極的に支援**しています。

ロシアのアプローチを分析した Talos は、彼らのサイバー能力が 3 つに大きく分類されていることを発見しました。まずはサイバー攻撃です。サイバー攻撃には、運用テクノロジーを停止させることを目的とする分散型サービス拒否攻撃や破壊的な攻撃が含まれますが、これらに限定されるものではありません。2 つ目は、サプライチェーンなどの複雑なシステムに対する一斉攻撃です。3 つ目は虚偽情報作戦です。これは、戦争に対する世界的な見方を変えることや、内部の反対意見、民族的、宗教的、政治的な分裂を不当に利用することを目的として使用されています。



さまざまなサイバー犯罪グループがロシア側に付くことを選択したため、激しい分裂も生じました。たとえば、ランサムウェア集団 Conti は、この戦争でロシア側を支援することを選択し、ウクライナを支援する西側諸国を標的にすると発表しました。

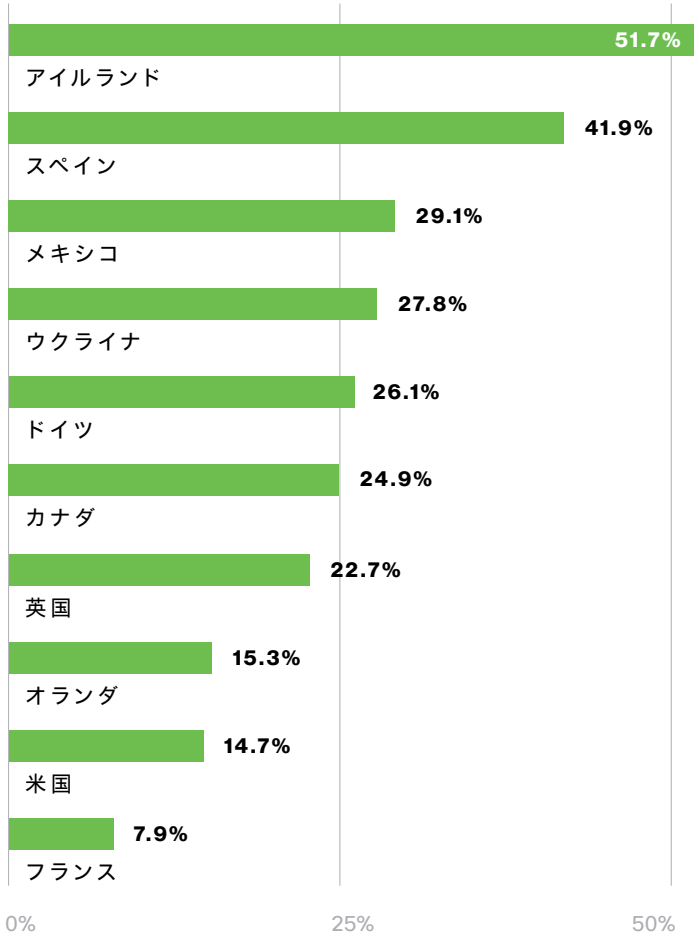
Anonymous は、戦争に直接対応してロシアのシステムを侵害する作戦を開始しました。明らかになった共通点としては、設定ミス、パッチの欠落、および盗み出した静的パスワードを活用して、システムに絶え間なく攻撃が仕掛けられたことが挙げられます。

MFA の使用が世界的に増加

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 15% 増加しましたが、北側に隣接するカナダでの増加は 25% でした。アイルランドでは、同時期に 52% 増加しています。

アジア太平洋地域では、日本で増加傾向が見られ、認証が 32% 増加しました。ニュージーランドは 30% 増加し、インドネシアでは 27% の大幅な増加が見られました。

図 9：南北アメリカおよび EMEA 地域で認証件数が最も多い国における対前年 MFA 増加率



しかし、すべての国で認証件数が増加したわけではありません。

図 11 は、MFA 認証の割合が大幅に低下した国の詳しい内訳です。

認証件数の 15% の跳ね返りは、2022 年の視点で見ると興味深いですが、昨年のレポートでは 37% の大幅な減少が見られたことに注意する必要があります。これは単なる修正だった可能性があります。

NATO 加盟国のチェコ共和国で認証件数が大幅に増加したのは、ロシアに忠誠を誓うサイバー攻撃者からの同国を狙ったサイバー攻撃が増加したことが原因と考えられます。たとえば、チェコテレビ、CT24、チェコラジオのニュースサーバーはいずれも、**2022 年 4 月に分散型サービス拒否攻撃を受けました。**

図 10：APAC 地域で認証件数が最も多い国における対前年 MFA 増加率

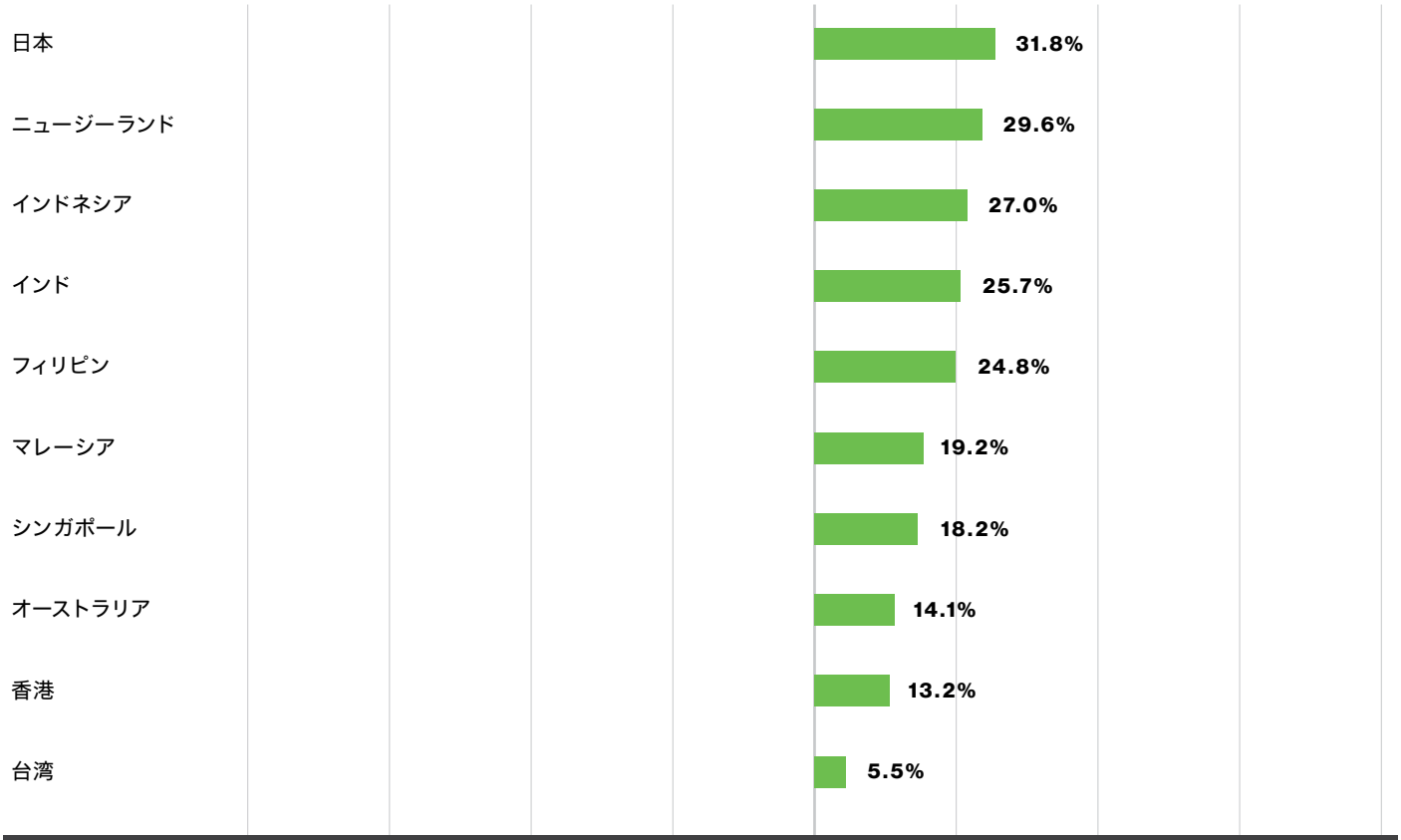
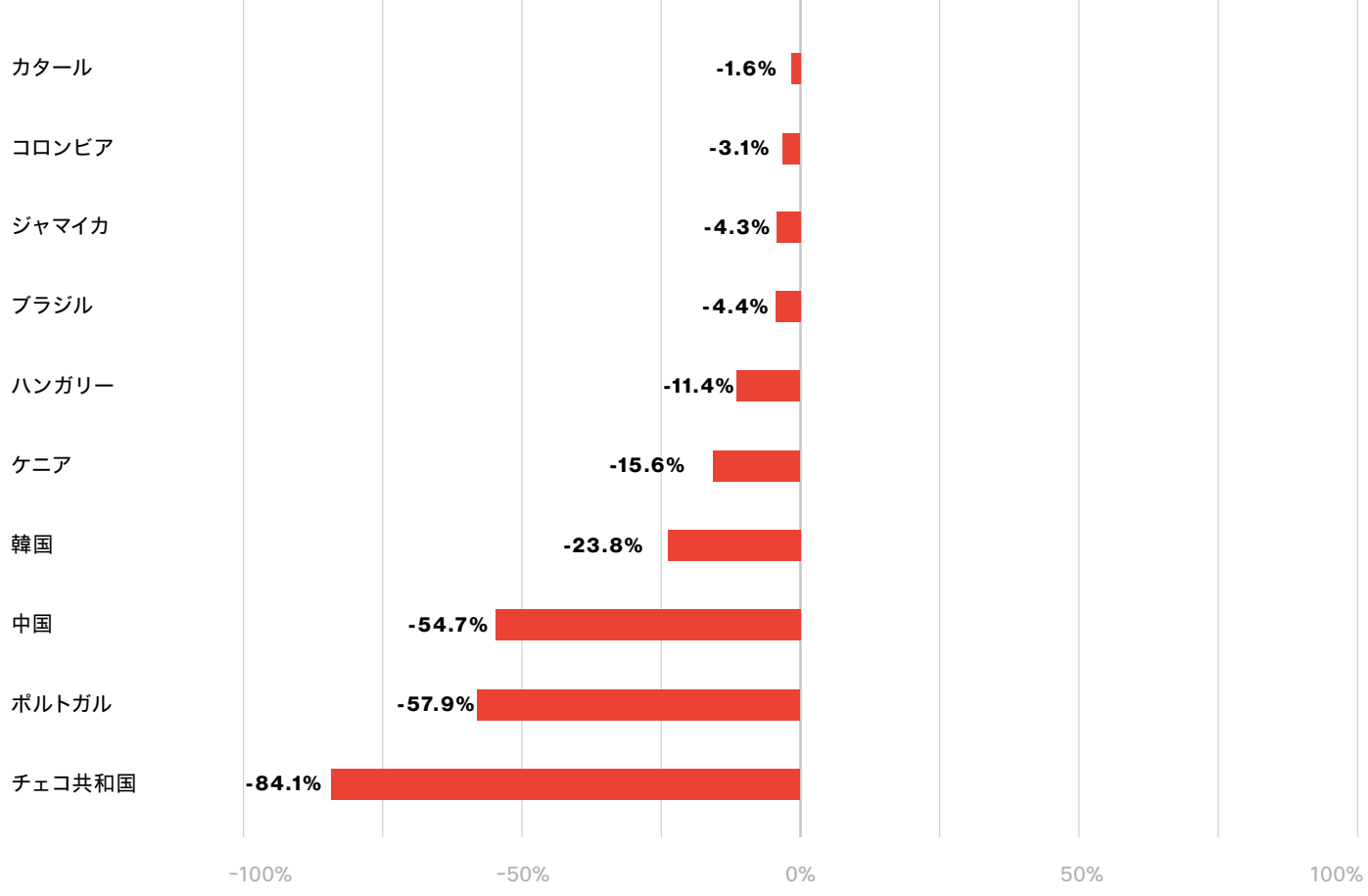
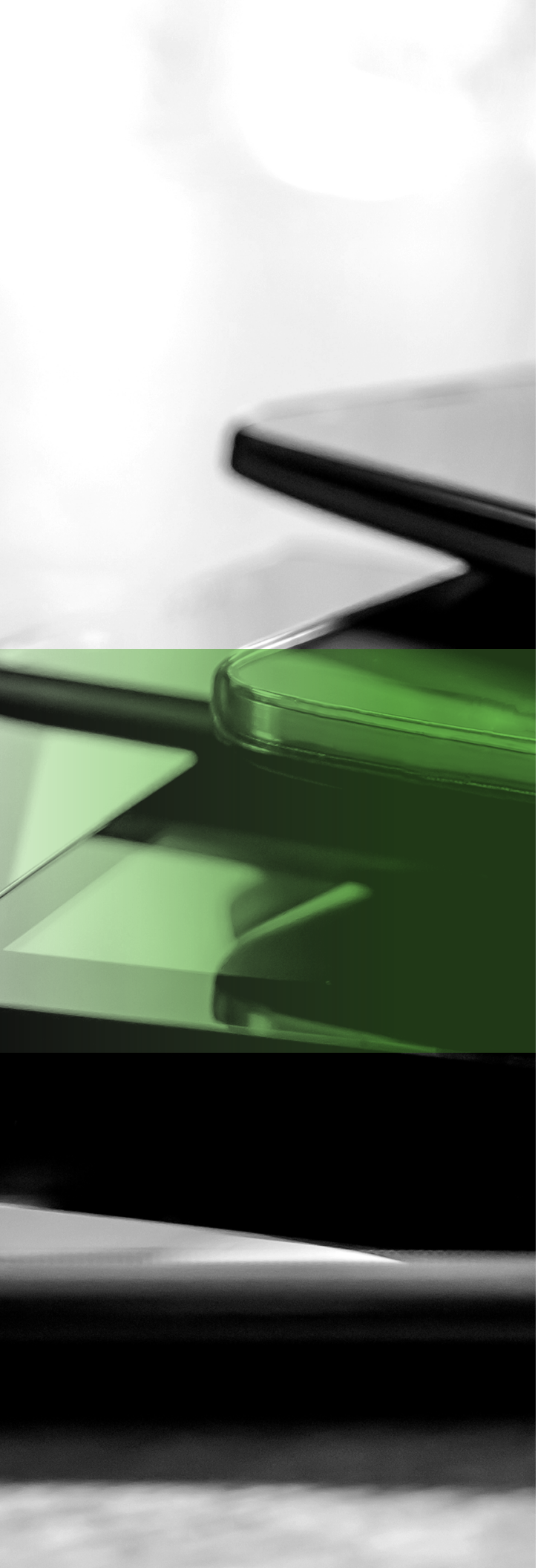


図 11：認証件数が多い国における認証件数の減少率





デバイスの可視性

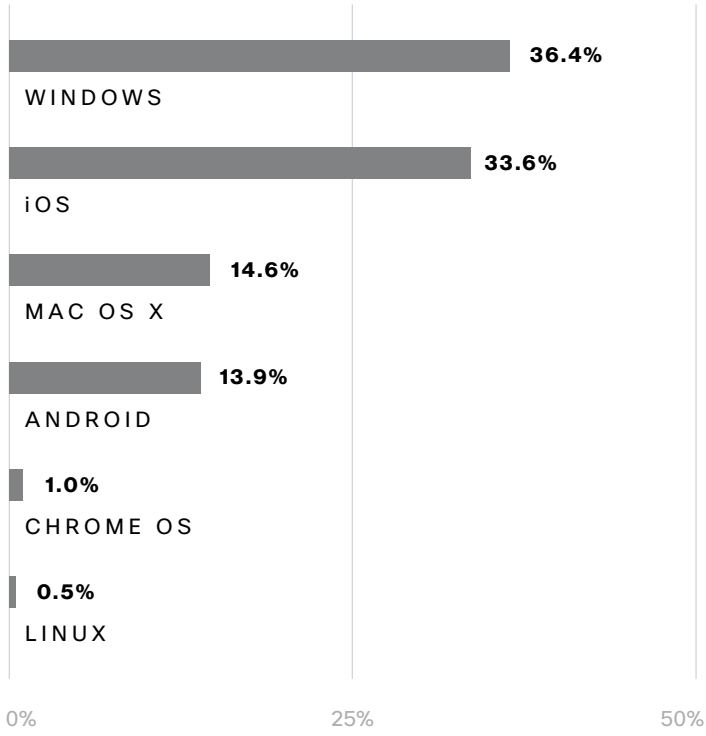
デバイスの信頼性を確立するには、アプリケーションやデータにアクセスするデバイスを可視化する必要があります。中でも、デバイスで実行されているオペレーティングシステムとブラウザ、およびそれらの OS とブラウザが最新のものであるかどうかを把握することで、信頼できるデバイスかどうかを判断できます。まず、Duo のお客様が使用しているブラウザと OS を見てみましょう。

最も普及している 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、以下に示したのが Duo のお客様が使用する上位の OS です。

Microsoft の熱心な支持者が相変わらず群を抜いていますが、注目するのは iOS が 27% を占め、強力な 2 番手になっていることです。現在はより多くの人々がハイブリッド環境の中、自分に最も適した方法で働いています、これまで非従来型とみなされてきたオペレーティング システム プラットフォームを利用する人が増加を続け、新しいパラダイムが生まれています。Linux は、残念ながら大幅に立ち遅れたままです。

図 12：オペレーティングシステム別のエンドポイントの割合



デバイス

企業は、金銭的および政治的な動機を持つオンライン攻撃者と戦う必要があることを理解しています。これに加え、緊急事態の対応策から事実上の標準へと進化した分散するハイブリッドワークフォースをサポートする必要もあります。明かりをつけておくだけで企業を保護できた時代もありましたが、今では企業を保護するためにあらゆる種類の外部攻撃からの防御が必要です。企業にとっては引き続き、デバイスの保護策と強力な認証の両方を確保することが課題です。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。

ノートパソコンや携帯電話などのデバイスは、ビジネスに欠かせないツールであるため、これらの資産を保護することは不可欠です。企業は、こうした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。多くの組織が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、そういった組織で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。

私たちは今年、Duo Device Health アプリによって収集したデータを詳しく調べ、さらに詳しい分析を実施しました。特に目指したのは、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ることでした。暗号化機能付きデバイスの割合が 90% から 87.2% に減少し、ファイアウォールの使用率が 96% から 88.4% に減少していたため、この状況を把握することが重要でした。しかしその主な原因は、大量のデバイスを使用しているいくつかのアカウントでした。

組織単位で見ると、検出可能なデバイス暗号化を導入している企業の大半 (64%) で、暗号化機能付きデバイスの割合が増加していました。実際、平均値で見ると、組織の暗号化使用率は 43% 増加し、ファイアウォール使用率は 26% 増加しました。[1]

1 これらは、算術平均や中央値ではなく、幾何平均です。幾何平均を使用した理由は、一部の組織でこれらの保護を備えたデバイスの割合がごくわずかからほぼ 100% へと桁違いに増加したためです。「典型的」な値に焦点を当てるために、こうしたタイプの測定に対しては安定している統計を使用しました。

デバイスベースのポリシー

以前のレポートでは、組織が対処すべきセキュリティ負債の削減について議論しました。組織にとってこの課題への最善の対処方法は、リスクの削減です。たとえば、**デバイスベースのポリシー**を利用して、環境内の資産に統一されたポリシーを確実に適用する方法があります。

デバイスベースのポリシーを使用すると、システムやデータの侵害につながりうる企業の資産の全体的なリスクポスチャを低下させることができます。デジタル企業の防御担当者は、ドメイン内のすべての管理対象デバイスをカバーするセキュリティポリシーを適用しなければなりません。管理対象外であっても、ネットワークへのアクセスが許可されているデバイスは、そのセキュリティポスチャに基づいてアクセスを制御できる必要があるのです。

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。

すべての認証のうち、5.5% 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 32% 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 1.2% でした。おそらく、こうしたことよりも興味深いのは、どのポリシーが認証の失敗に特に大きな影響を与えるかということです。

図 13：特定のポリシーに起因して失敗した認証の割合

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（相対的）割合を占めていることがわかります。

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。

図 14：ポリシーを使用しているアカウントと、ポリシーが認証拒否にもたらす影響

ここでは、「未登録ユーザー」が外れ値として除外されていることに注意してください。

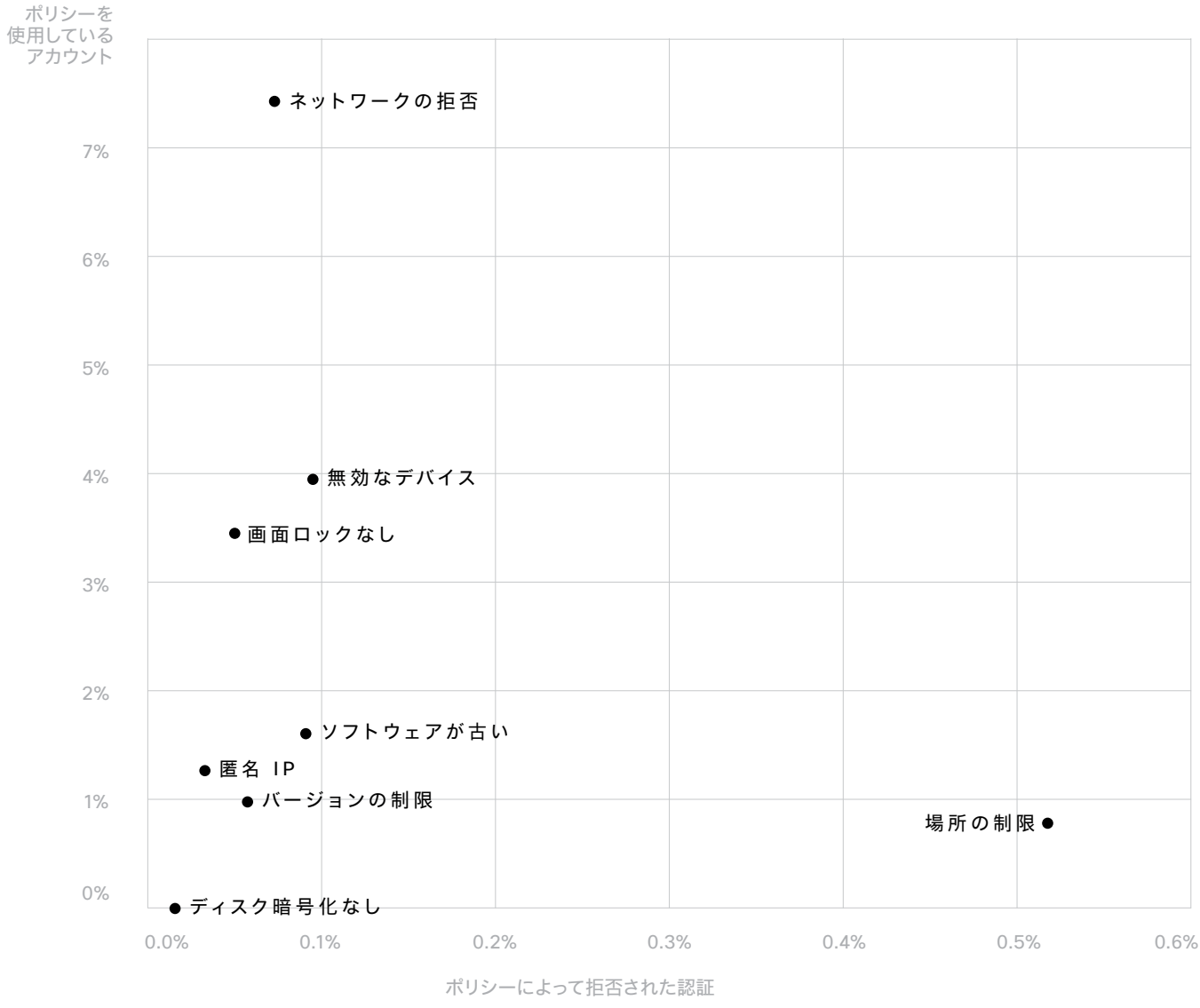
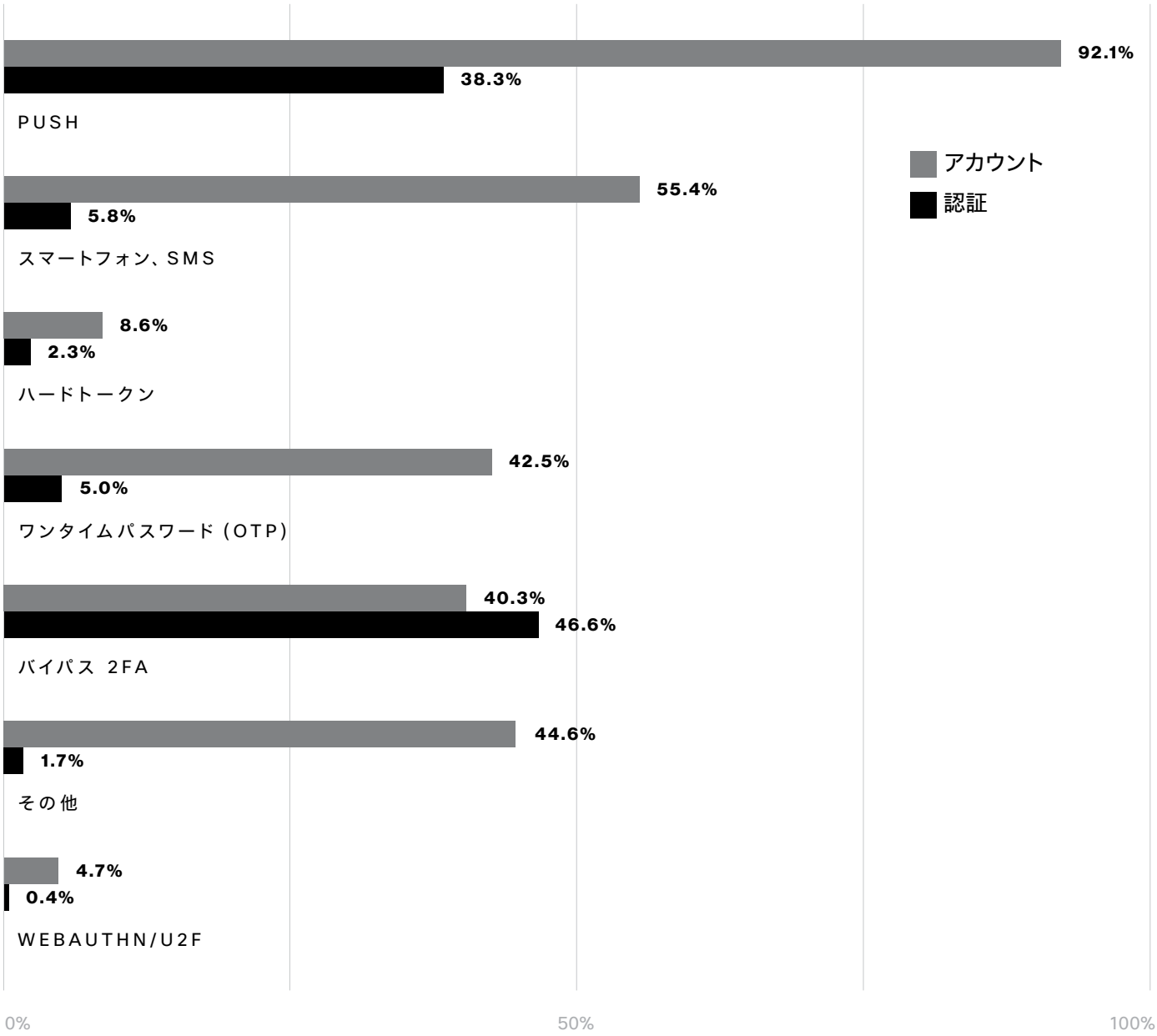
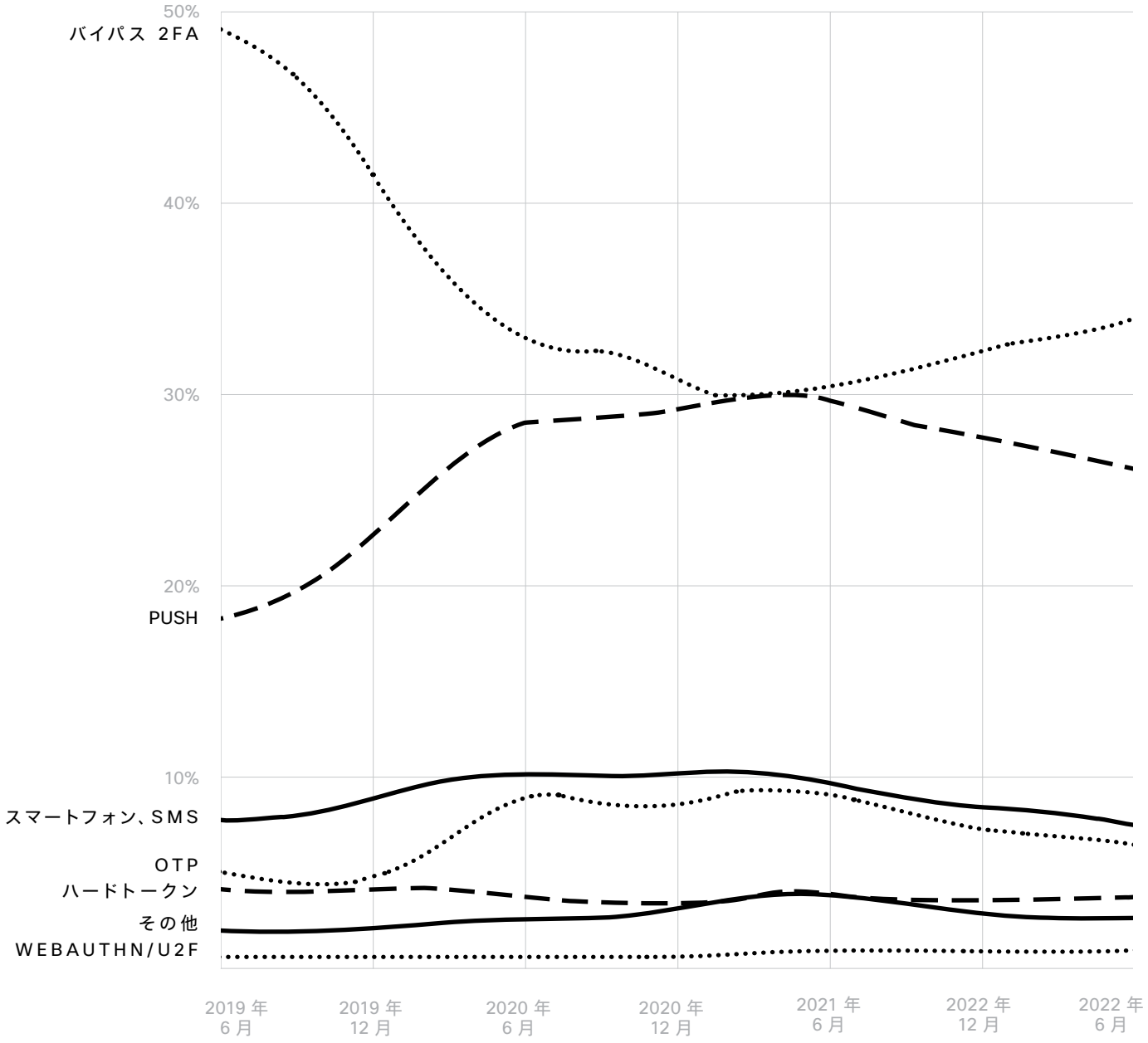


図 15：アカウントと認証によって使用される要素



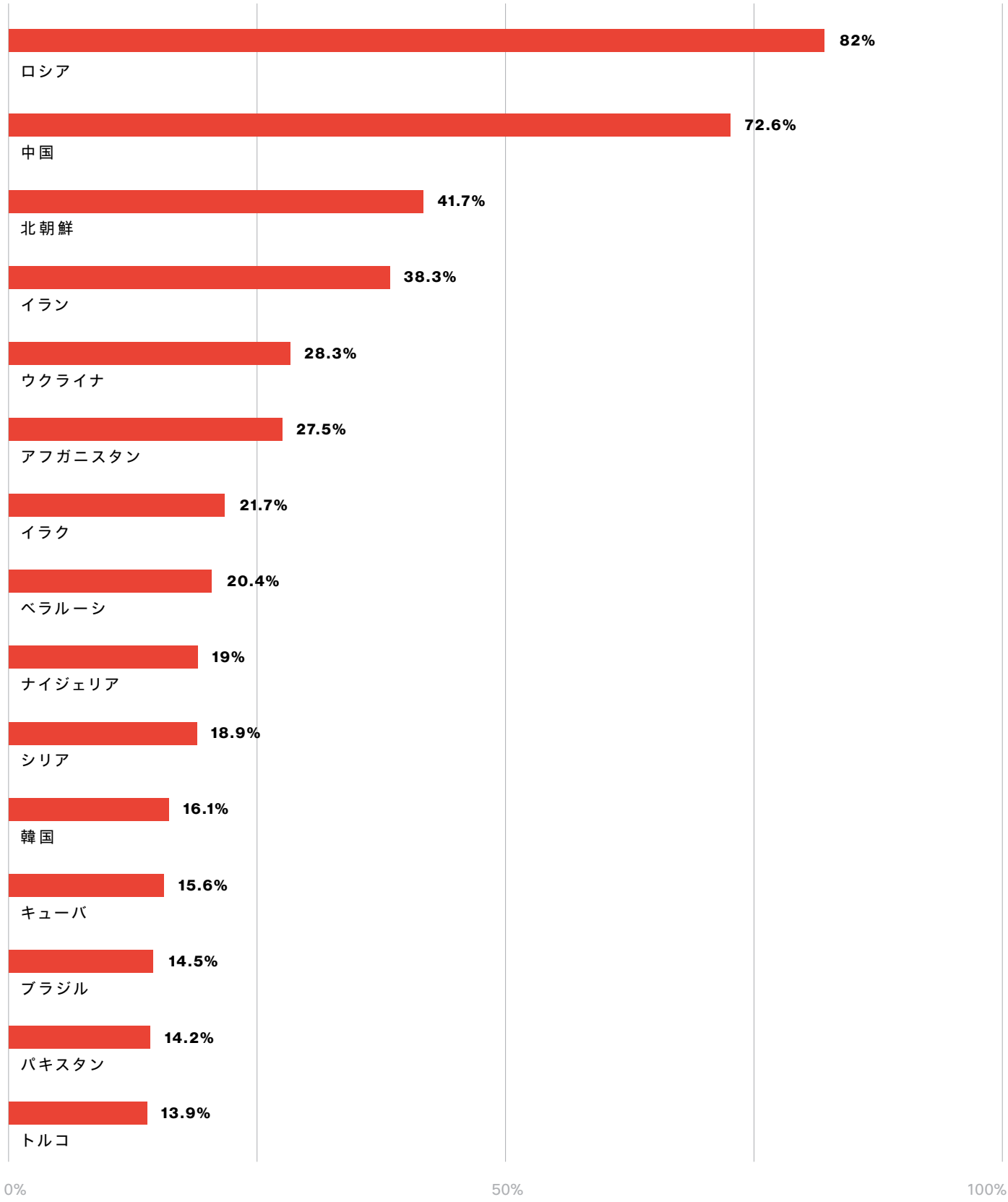
ポリシーに関するデータを確認したところ、いくつかの注目すべきことがわかりました。Duo Push ベースの認証は、全世界のアカウントの 92% で使用されていました。Duo Push は Duo 製品の主な焦点であり、99% 以上のアカウントがこの要素を有効にしているため、この結果は当然です。これ以上に興味深いのは、おそらくギャップが見られる要素の方でしょう。上記で見たように、WebAuthn は約 66% のアカウントで有効になっているにもかかわらず、実際に認証に使用しているのは 2.2% のみでした。ワンタイムパスコードは 98% のポリシーで有効になっていますが、この方法を利用したアカウントは 55% のみで、認証の 6% でしか使用されませんでした。

図 16：認証で使用される要素の時系列の変化



これらの要素の使用状況を時系列で調べた興味深い調査結果を、図 16 に示しました。この図からわかるように、Push が着実な増加を見せ、2FA バイパスを完全に追い越すと思われましたが、Push は 2 番手にとどまりました。人気が低い要素を見ると、順位にあまり変動はありませんが、ここ数年で OTP の使用が増加し、スマートフォン / SMS とほぼ同じ割合になっています。

図 17：特定の国からの認証を拒否するアカウントの割合



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み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みなしているためです。これらの国はお客様によって異なります。Duo のデータを確認したところ、リスクのある国に焦点を当てたポリシーに基づいてアクセスが制限された場所の上位として、以下に示す国を特定できました。

Duo の調査結果によると、場所の制限ポリシーを導入している企業の約 91% が、ロシアまたは中国からのアクセスを制限しています (60% は両方の国を制限)。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、ベラルーシ、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)。

私たちにとってのもう 1 つの疑問は、「制限された地域から発信されたことが原因でブロックされた認証の割合はどれくらいか、これらの結果を上記の結果と比較するとどうなるか」です。これを図 18 に示します。中国は、ポリシーによって認証がブロックされる割合が高いだけでなく、場所が原因で最も多く認証失敗が発生している国でもあります。

ここで興味深いケースが、米国です。米国からの認証をブロックしている組織は 1% 未満に過ぎませんが、米国からの認証件数が多いため、場所ごとの認証失敗の合計数が 2 番目に多くなっています。

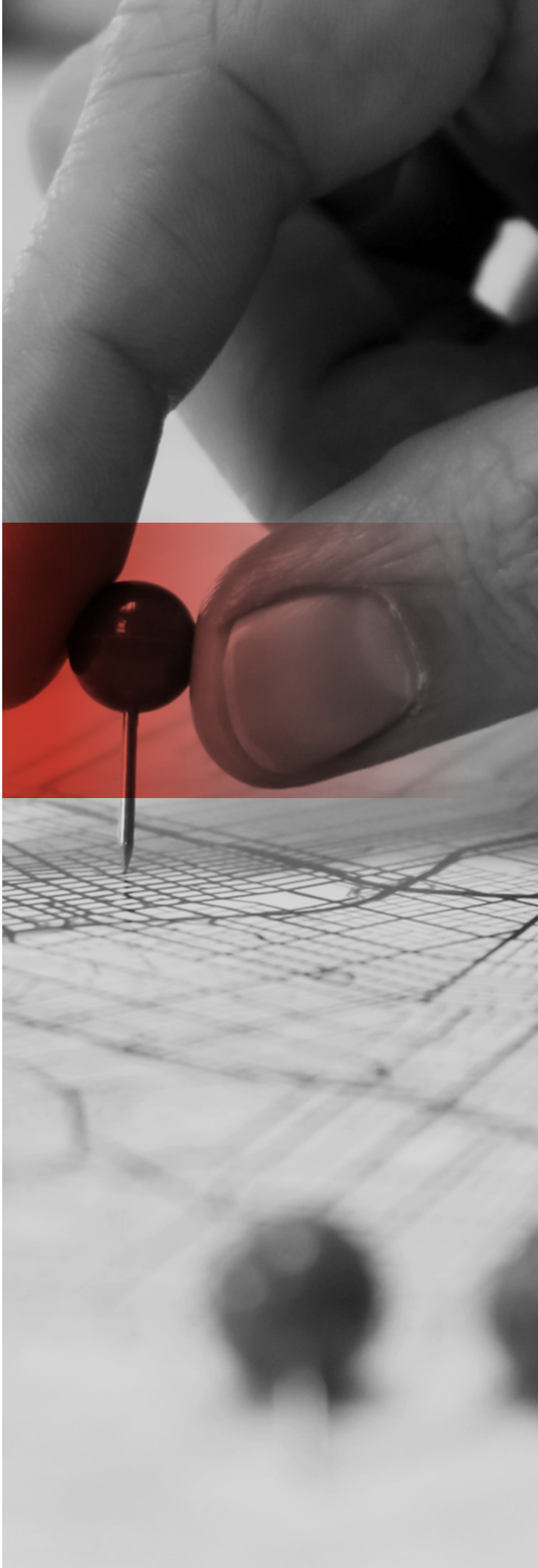
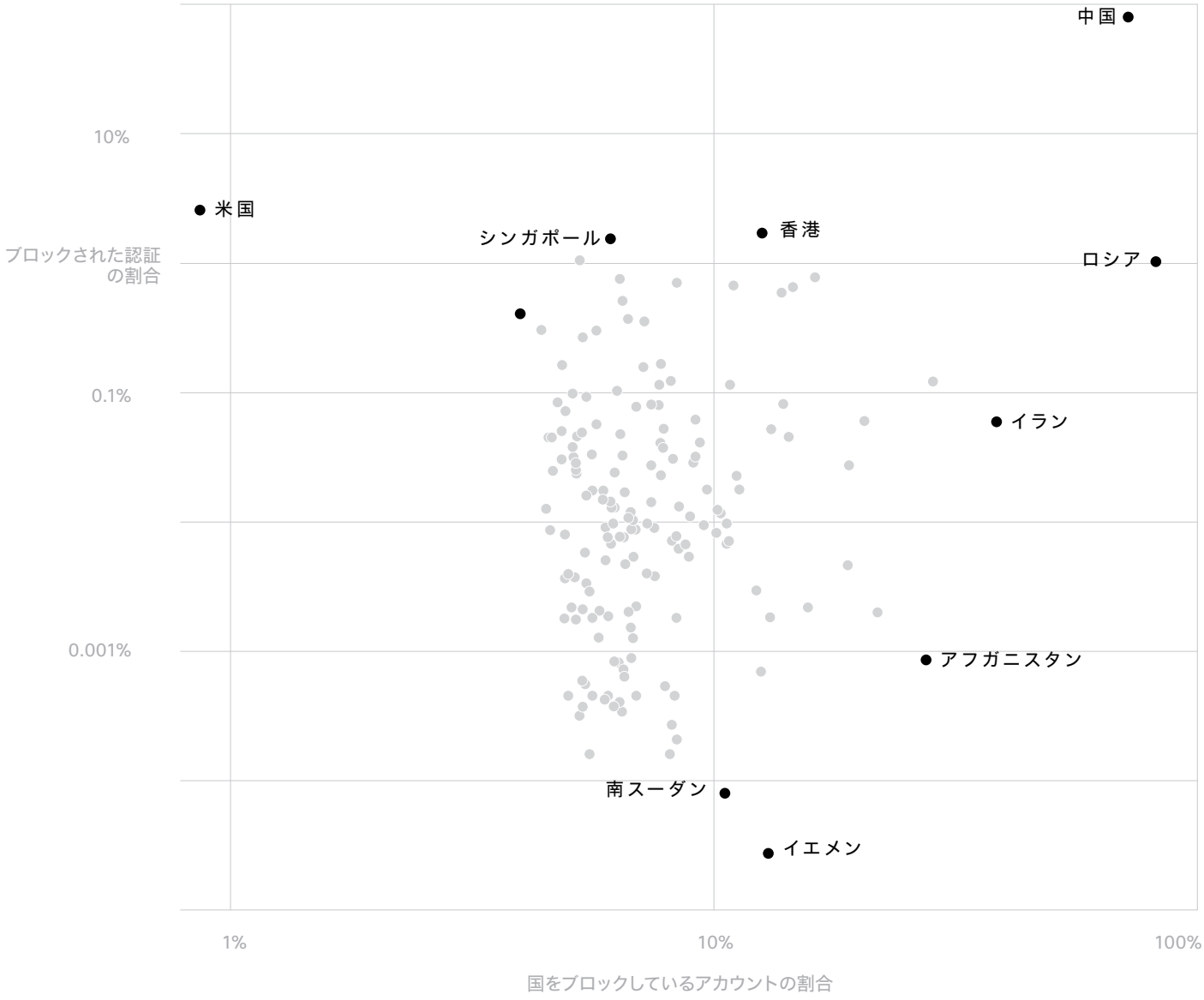


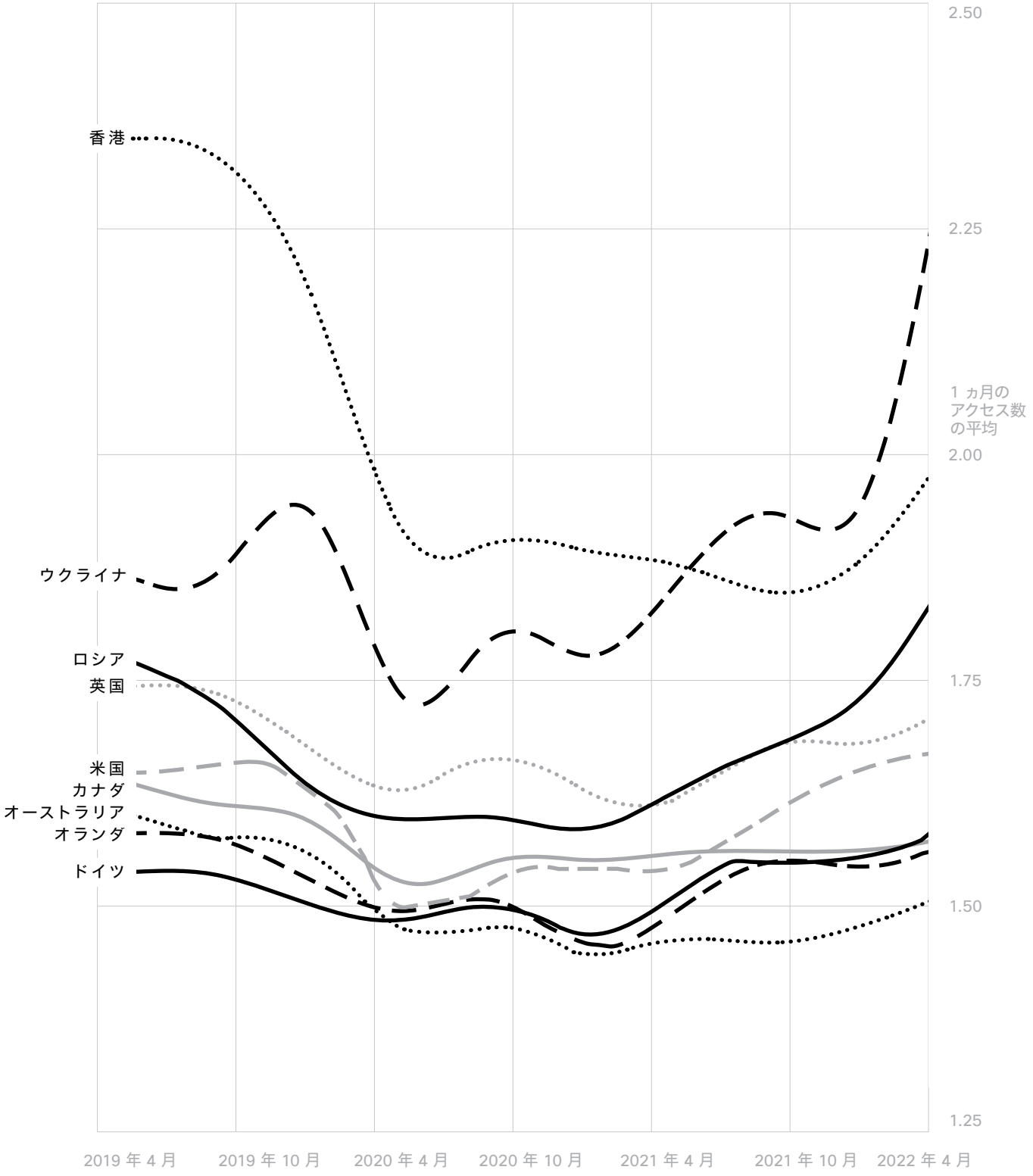
図 18 : 特定の国をブロックしているアカウントとブロックされた認証の割合

X 軸と Y 軸には対数スケールのラベルが付けられていることに注意してください。各点は国を表します。外縁にある複数の国が特に興味深い動き（認証のブロック率が高い、またはその国をブロックするポリシーの割合が大きい）を示しているため、これらの国を強調する表示形式にしています。

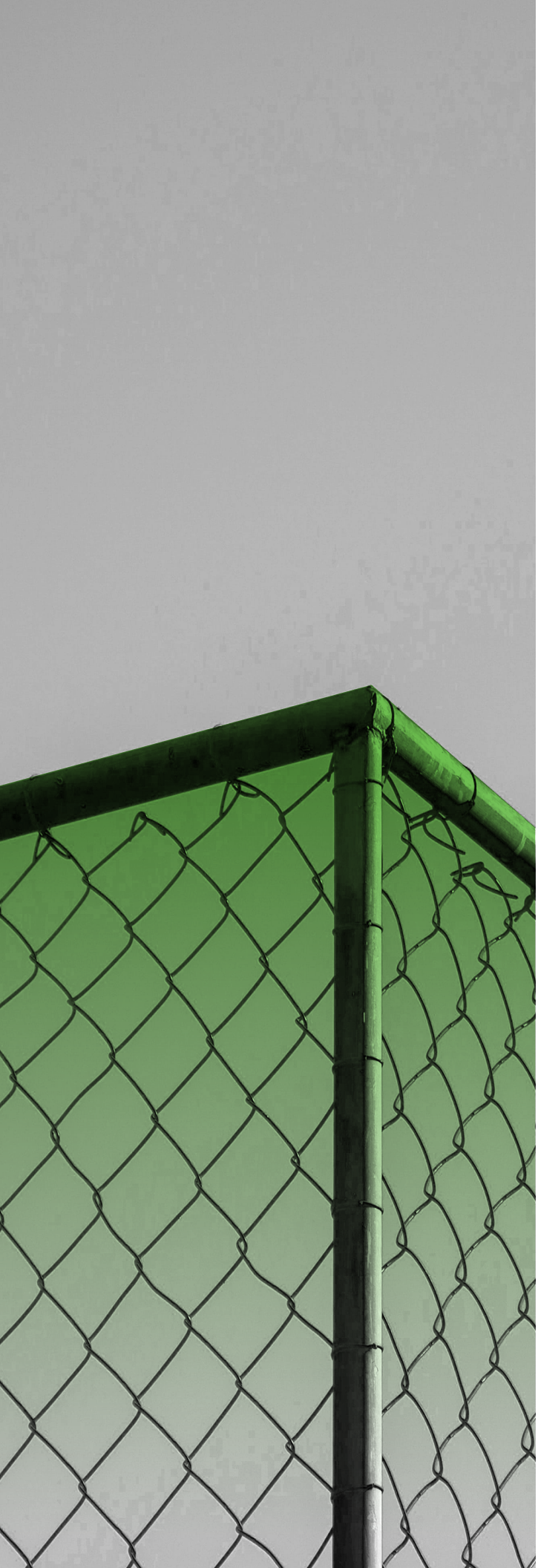


この結果から、さらに興味をそそる疑問が生じます。ユーザーは仮想プライベートネットワーク (VPN) を介してこれらのポリシー制限下で認証を試みているのでしょうか。この事実については図 2 で触れ、政治的に重要な出来事を経験している地域、つまりウクライナや香港の組織は、より安定した地域の組織よりも、多くの国から認証を受ける傾向があると説明しました。次の図は、ユーザーが認証を受ける国の平均数を時系列で追跡したもので、その変化を時系列で確認できます。

図 19：世界のさまざまな国に拠点を置く組織のユーザーが認証を受ける国数の変化



2019 年初頭から 2020 年初頭までの大規模な民主化デモが行われた時期は、香港の平均値が高い状態が続きましたが、コロナ渦のロックダウンで多くの人々が自宅待機になると状況は変化しました。2022 年初頭になると、ロシアによるウクライナ侵攻によって、ウクライナとロシアの両方が短期間で急増しました。



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。そのため、認証の失敗率にも差が見られます。注目度が常に高い主要産業である教育、金融、情報技術 (IT) / 通信に焦点を当てると、いくつかの顕著な違いが見られます。教育および金融産業では、ポリシーの適用による認証失敗の最大の理由は「ユーザーが許可されたグループに属していない」ですが、通信産業での最大の認証失敗理由は場所の制限です。これら 3 つの産業を見ると、無効なデバイスのブロック数が最も多いのは金融産業なので、金融機関がユーザーに使用を許可するデバイスに対するポリシーは、他の産業よりも厳しい可能性があります。

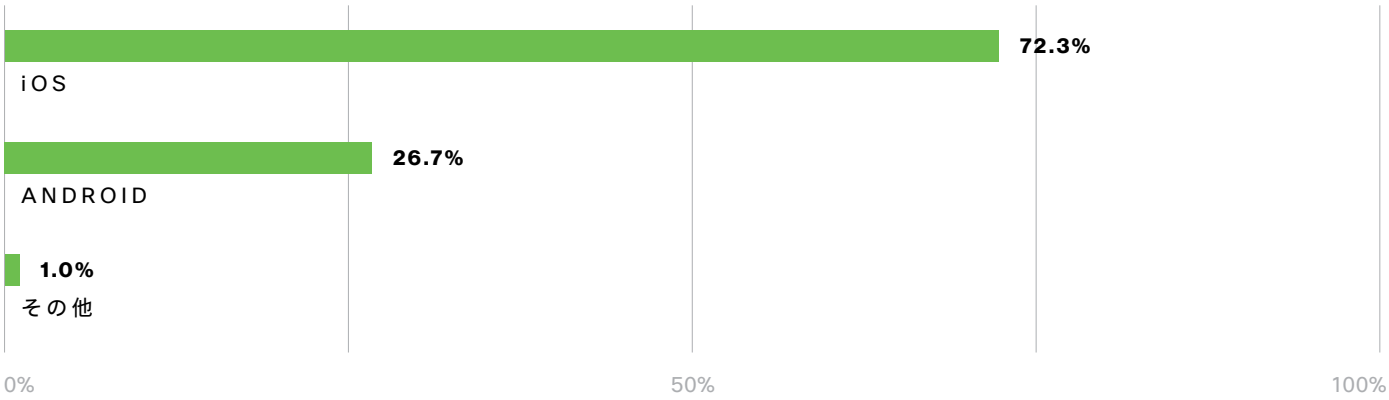
この表には、認証失敗のすべての理由が含まれていないことに注意してください。具体的に言うと、最も一般的な理由である「ユーザーの登録し忘れ」が含まれていません。「未登録ユーザー」はすべての業種で共通して多くなっていますので、ここでは類似する傾向ではなく、業種間の顕著な違いに注目します。

図 20：主要産業での特定のポリシーによる認証失敗

パーセンテージは、すべての認証に対する割合です。

	教育	金融	IT/ 通信
バージョンの制限	0.0002%	0.004%	0.009%
ユーザーが許可されたグループに属していない	0.01%	0.04%	0.02%
ソフトウェアが古い	0.001%	0.005%	0.01%
画面ロックなし	0.002%	0.004%	0.003%
ディスク暗号化なし	0.00002%	0.001%	0.003%
場所の制限	0.003%	0.004%	0.1%
無効なデバイス	0.004%	0.01%	0.006%
ネットワークの拒否	0.000009%	0.002%	0.0004%
匿名 IP	0.001%	0.002%	0.003%

図 21：携帯電話プラットフォームの割合



iOS の普及

Apple の iOS が依然として最も多く利用され、デバイスの約 72.3% を占めています。iOS の強さは注目に値します。iOS はこの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 26.7% とはるかに低くなっています。ポリシーの観点で言うと、この状況は環境のセキュリティを強化しようとしている組織にとって朗報です。iOS はセキュリティを最優先して構築され、オペレーティングシステムの最新バージョンでは、パッチ適用がデフォルトで有効になっています。昨年のレポートの 67% から 72.3% に使用率が増加していることから、Duo の顧客ベース内でも iOS の採用が増え続けていることがわかります。

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。モバイルプラットフォーム別の内訳を見ると、Mobile Safari が 1 位、Chrome Mobile が 2 位です。

図 22 : タイプ別デスクトップブラウザ

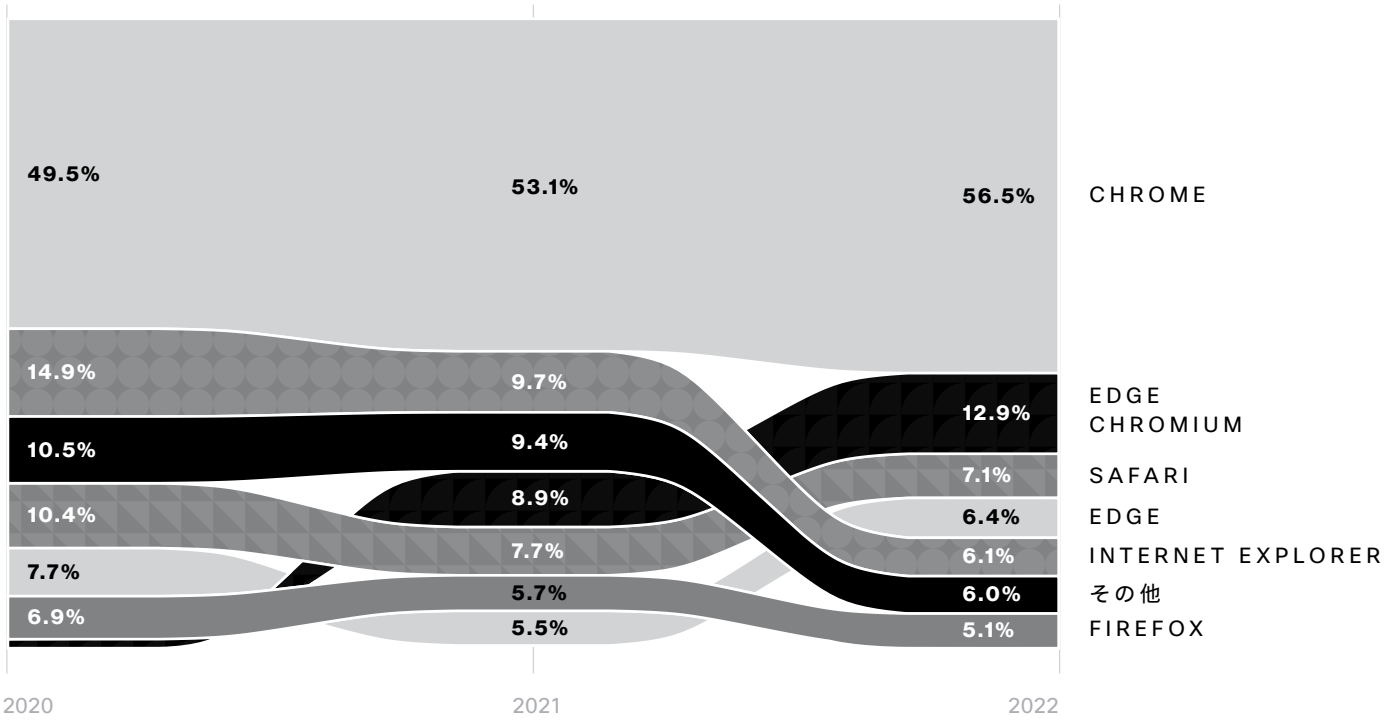
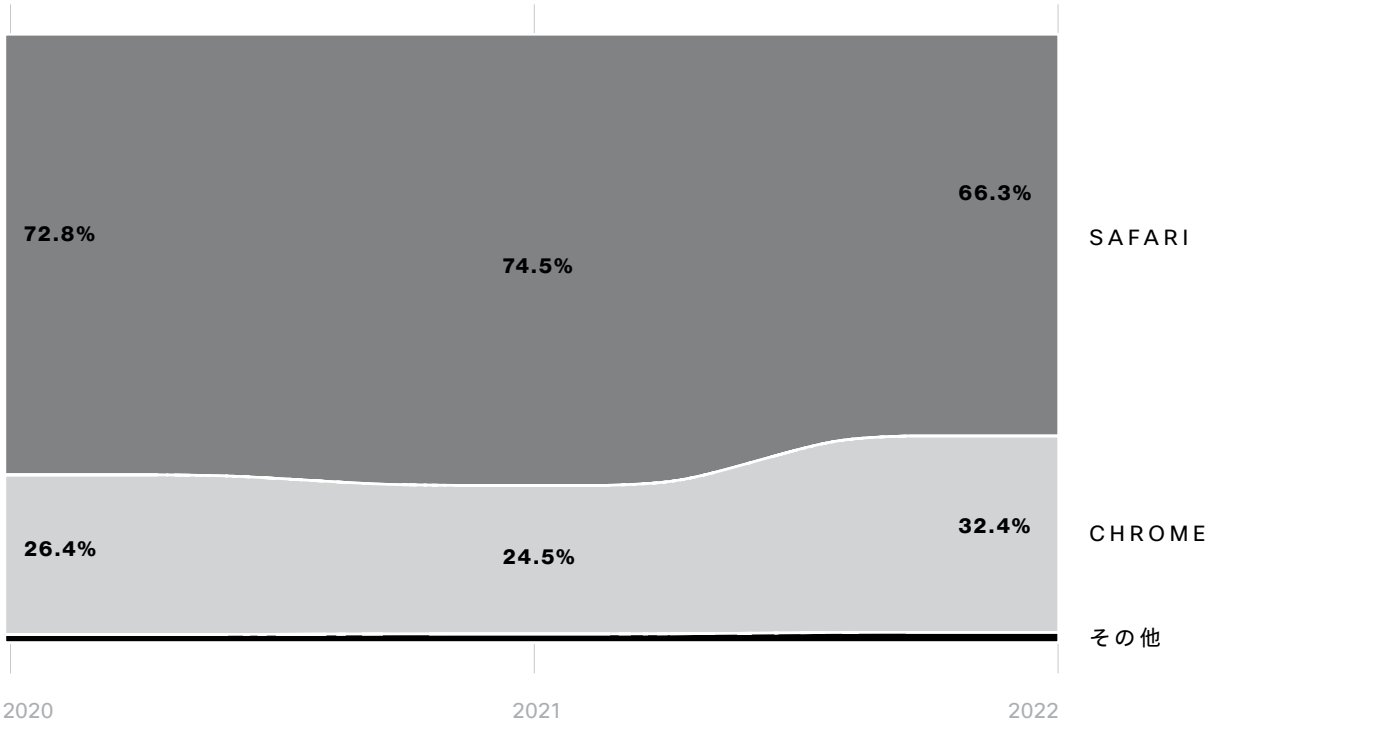


図 22 : タイプ別モバイルブラウザ



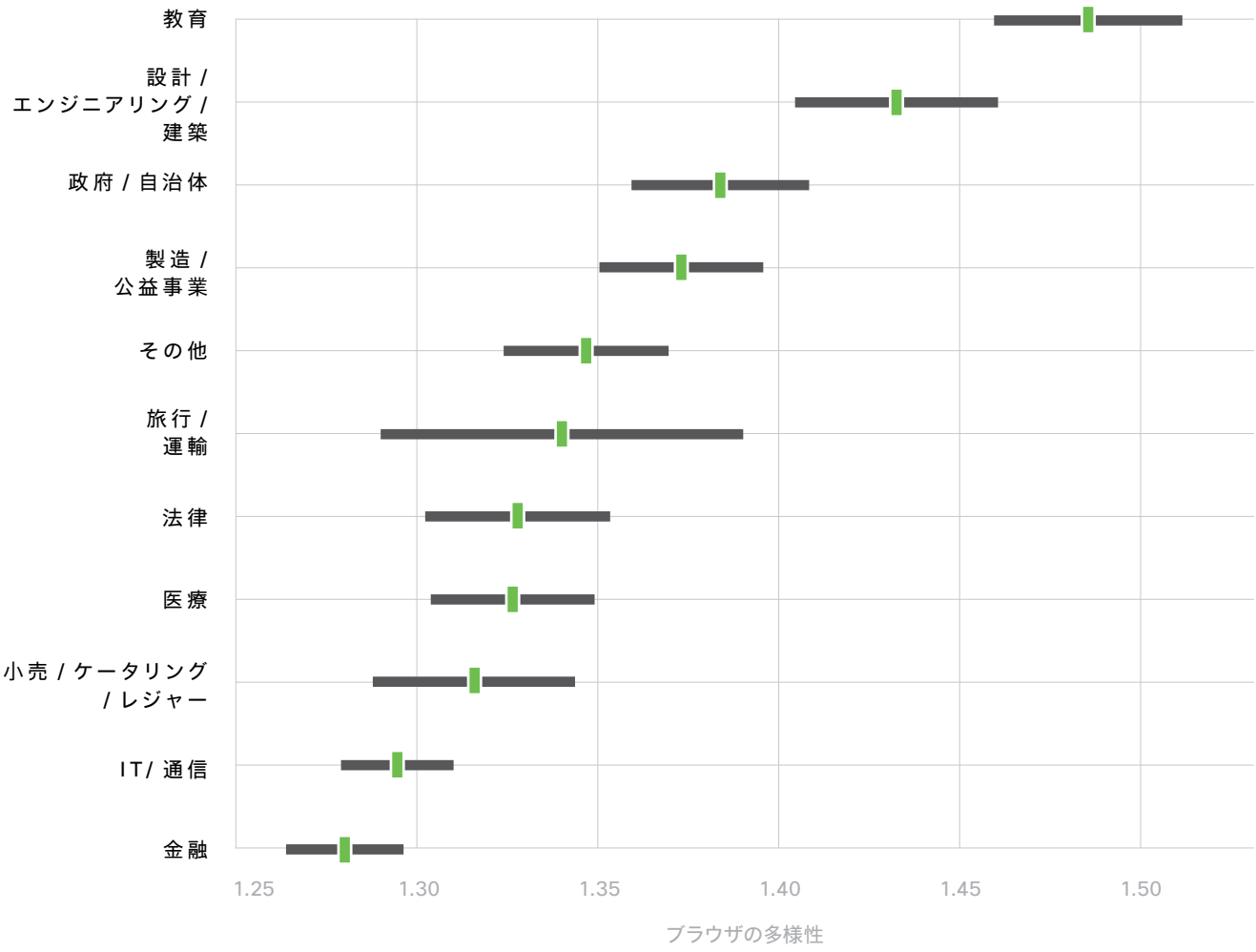
MFA 経由でアクセスするアカウントを確認すると、以下の表に示したように、使用するブラウザに関連する興味深い内訳が見つかりました。具体的に言うと、ほとんどの組織で、「主要な」モバイルブラウザである Safari (iOS) と Chrome (Android) の使用率がかなり均等に分散しています。両方を使用する組織も、一方の OS を主に使用している組織もあるようですが、「非従来型」ブラウザを使用する組織はごくわずかです。ただし教育産業は、豊富な種類のブラウザを使用しているため、この表では際立っています。教育機関の 45% で、1 人以上のユーザーがモバイル Firefox を使用しています。次にこの OS の使用率が高いのは医療機関です。データを確認してみると、教育機関全体の 23% で、Opera ブラウザのモバイルバージョンが使用されていることがわかります。対照的に、このブラウザを使用しているユーザーが 3% を超える業種は他にはありません。

これは、教育産業の IT とセキュリティが、他の業種よりもはるかにダイナミックであることを示す例の 1 つです。このダイナミズムは、学術機関のユーザー数の多さと多様性にのみに起因している可能性があります。しかし、学術機関の多くが幅広い地域に分散していることも加味すると、ダイナミズムというのが認識しづらいデバイスやソフトウェアを把握するための秘策となります。上の図は、特定のタイプのブラウザを使用している組織の割合のみを示していますが、これは教育産業のブラウザが本当に「多様」であることを意味しているのでしょうか。
では詳しく検証してみましょう。

図 23：業種別のモバイルブラウザを使用しているアカウントの割合

	SAFARI	CHROME	FIREFOX	EDGE CHROMIUM	OPERA
旅行 / 運輸	61.4%	53.3%	10.0%	7.2%	1.7%
小売 / ケータリング / レジャー	58.4%	50.5%	9.6%	7.6%	2.3%
その他	52.2%	41.4%	4.0%	3.0%	0.3%
製造 / 公益事業	58.7%	50.7%	6.9%	6.5%	1.5%
法律	63.7%	44.2%	4.6%	4.1%	0.5%
IT/ 通信	47.3%	44.4%	10.8%	7.5%	1.9%
医療	65.4%	58.1%	13.2%	12.0%	2.9%
政府 / 自治体	63.8%	55.3%	10.7%	7.7%	1.8%
金融	56.5%	45.5%	6.0%	5.9%	0.9%
教育	73.8%	70.0%	44.7%	36.7%	23.0%
設計 / エンジニアリング / 建築	65.0%	51.5%	5.6%	6.1%	1.0%

図 24：業界別のブラウザの多様性



ここでの多様性とは何を意味するのでしょうか。この文脈で「多様性」という言葉を使うのは珍しいかもしれませんが、Duo の調査の科学的概念を説明するのには効果的です。ここでは、生態学からシャノンの多様度指数と呼ばれる計算を借用します。この指数は、特定の生態系に存在する生物の多様性を理解する手段として開発されたもので、私たちが多様性と考える 2 つの面 (異なる種の数とその相対的優占度) から 1 つの値を導出することを試みます。

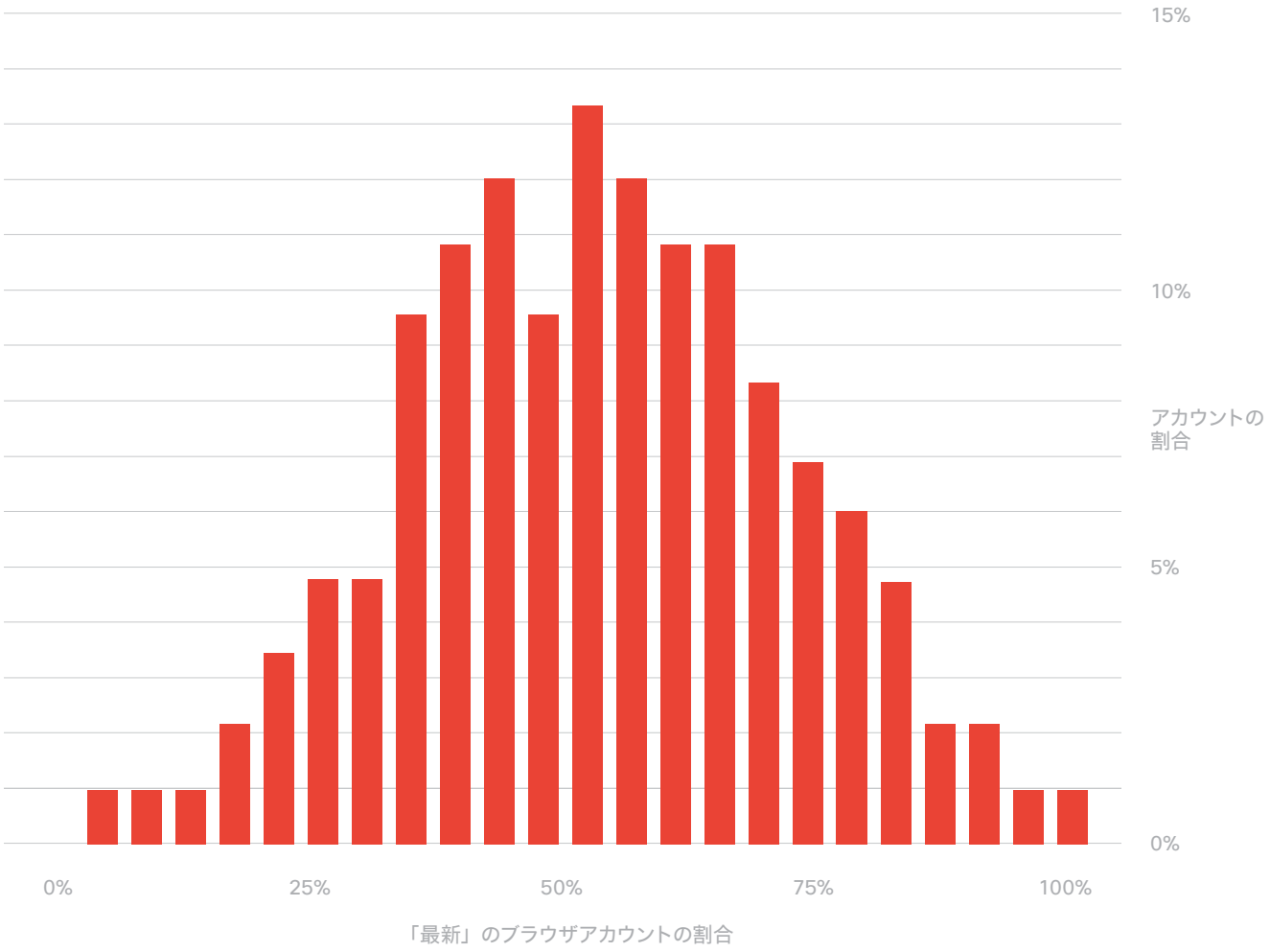
たとえば、100 種類の昆虫がいる生態系は多様だと考えられるかもしれませんが、その 99.9% が蚊である場合、その生態系はそれほど多様ではないでしょう。シャノンの多様度指数は、各種のすべての個体の割合を調べ、次のように計算します。

$$\text{多様性} = -\sum\ p \log (p)$$

ここでの「種」はブラウザであり、図 24 はこのブラウザの多様性を示しています。

今年明らかになった注目すべきデータポイントは、金融機関と比較した、教育機関で使用される Web ブラウザの多様性です。具体的に言うと、大半の教育機関でごくわずかな数の稀有なブラウザが使用されているのではなく、ほとんどの組織で多数のさまざまな「種」のブラウザが使用されていることが判明しました。

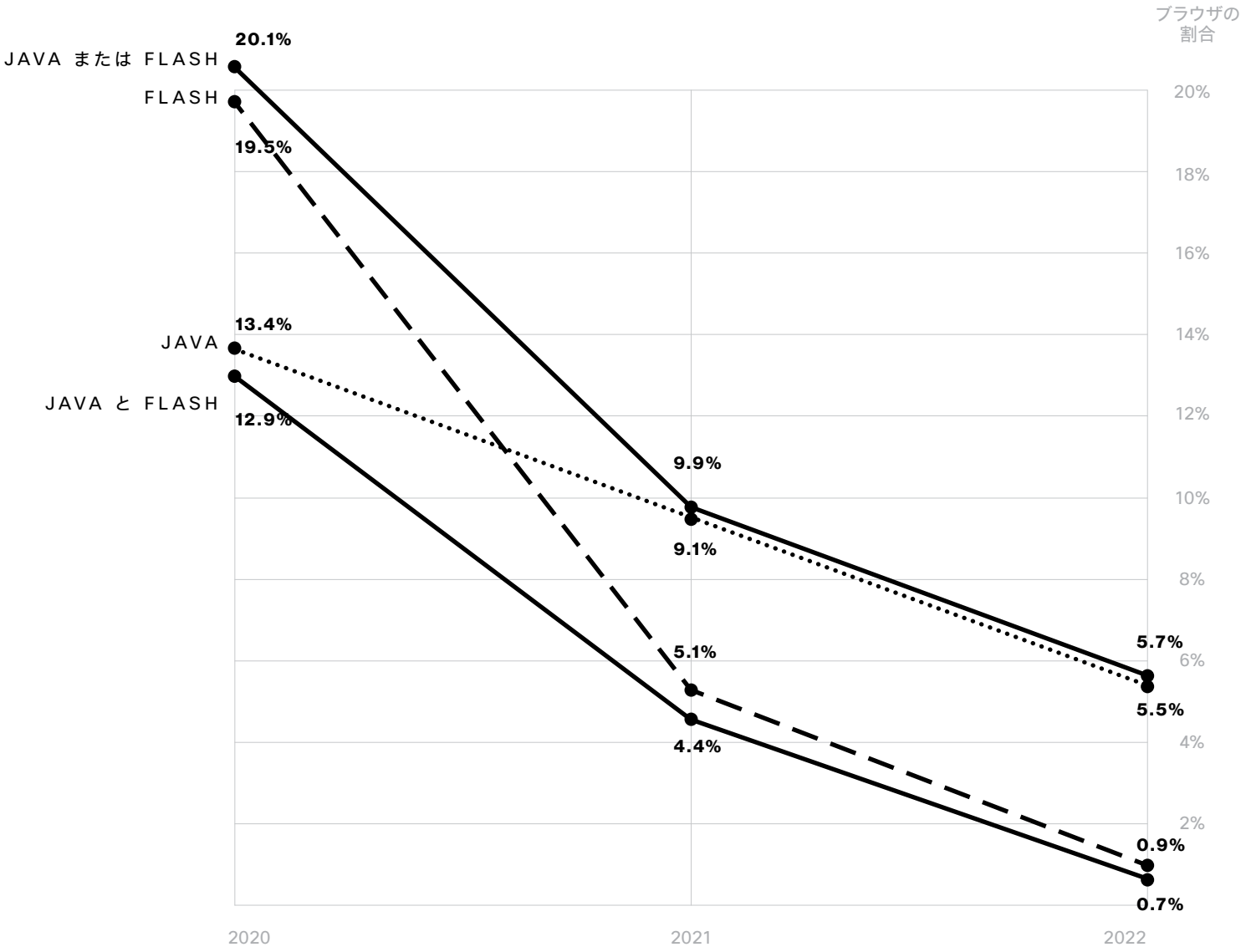
図 25：組織内で使用されている古いブラウザの分布



すべてのブラウザの 42% がパッチを適用して最新の状態になっていることは朗報ですが、問題となるのは 50.3% のブラウザが最新の状態でないということです。残りの 8% のうち、わずかですが (しかし恐ろしいことですが) 2% は「サポートが終了」し、残りの 6% は「不明」、つまりブラウザのバージョンを評価できませんでした。

図 26：FLASH と JAVA の経時的変化

注:このグラフの「Flash」と「Java」の線は、そのソフトウェアがインストールされているブラウザの割合を示していますが、必ずしもそのソフトウェアだけではありません。Java の状況を理解するには、特定の年の「Java」の数値から「Java と Flash」の数値を引いてください。

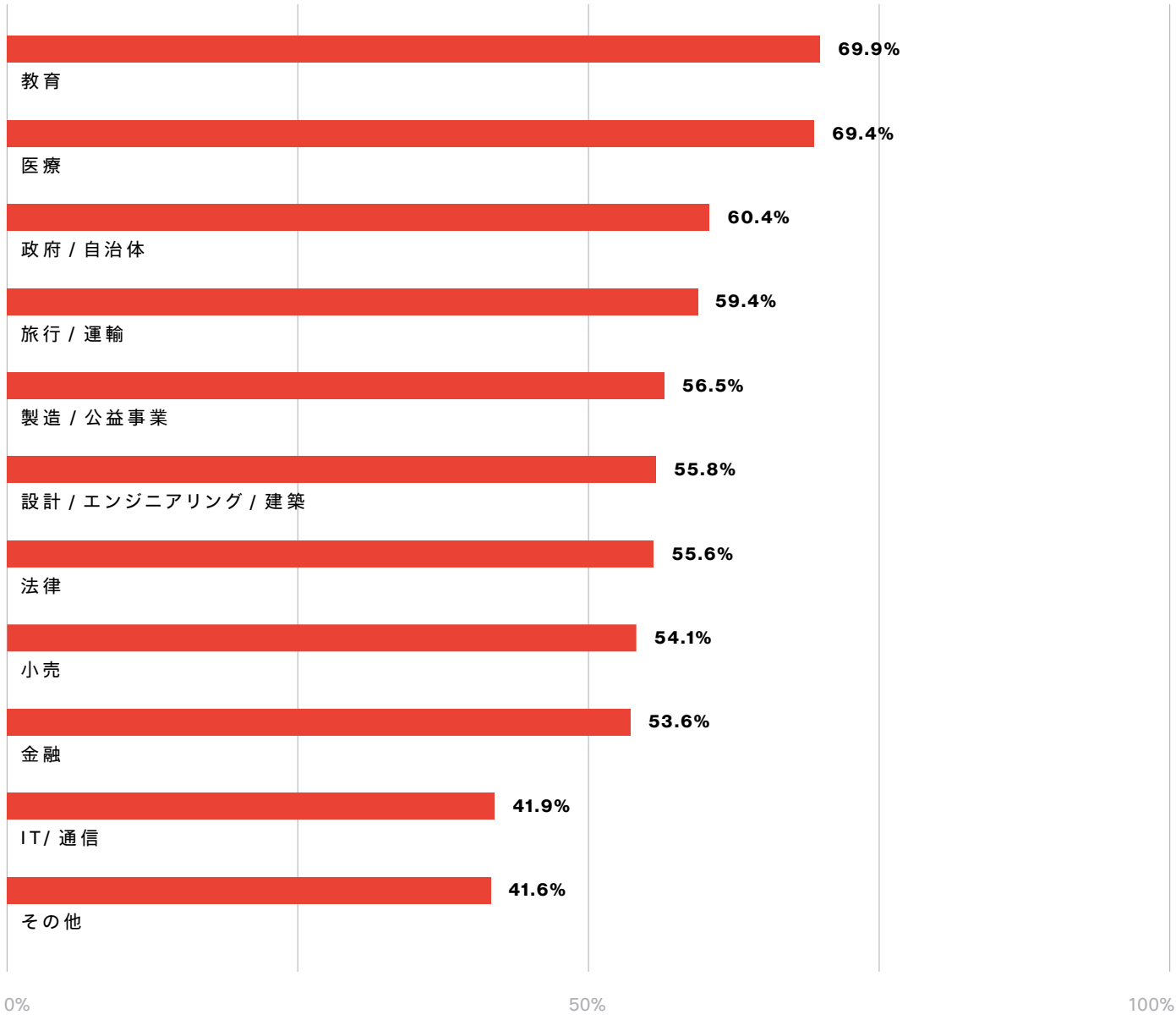


セキュリティ態勢を強化するブラウザ

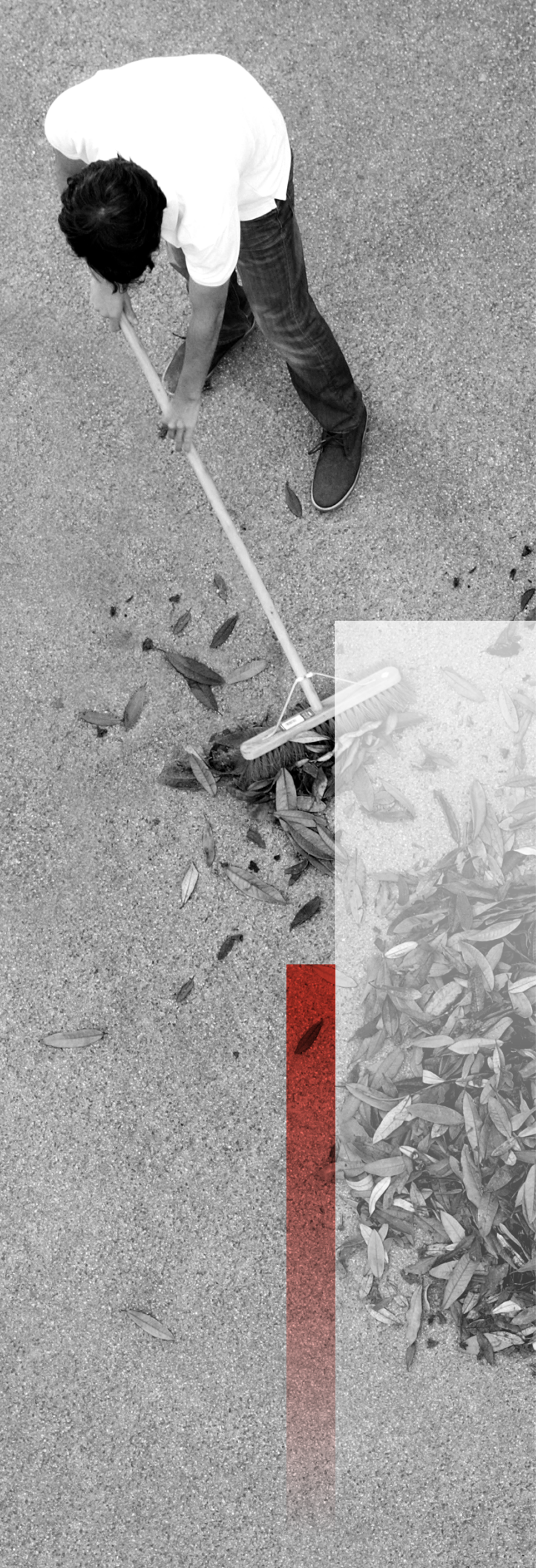
毎年、Web ブラウザのセキュリティ態勢を確認していますが、昨年は有望な情報が確認されました。2020 年には、ブラウザの 81% に Flash がインストールされていなかったのです。この結果を裏付けるように、Flash は、2020 年 12 月 31 日に**サポートが終了**しました。ユーザーの安全を確保するために、Adobe 社はさらに一歩踏み込み、2021 年 1 月 12 日以降、Flash コンテンツが Flash Player で実行されないようにブロックしました。その結果、Flash を実行するシステムの数は 2021 年に劇的に低下し、現在では 95% のシステムにインストールされていません。2022 年には、その数は 99.1% に増加しました。しかし 1 つの疑問が残ります。Java はまだ利用されているのでしょうか。

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。翌年、Java がインストールされていないシステムの割合は 91% に増加し、2022 年には、その数は 97% に増加しました。

図 27 : JAVA を実行するブラウザを少なくとも 1 つ使用している組織



システムからの Flash と Java の削除の進行状況を業種別に見ると、目に見える違いがあることがわかります。Flash がようやくなくなったと言えれば素晴らしいのですが、約 1% の組織でいまだに Flash をインストールしているとなると、約 34 万台のシステムに何らかのバージョンの Flash が今なお存在していることになります。



不適切なデバイスの一掃

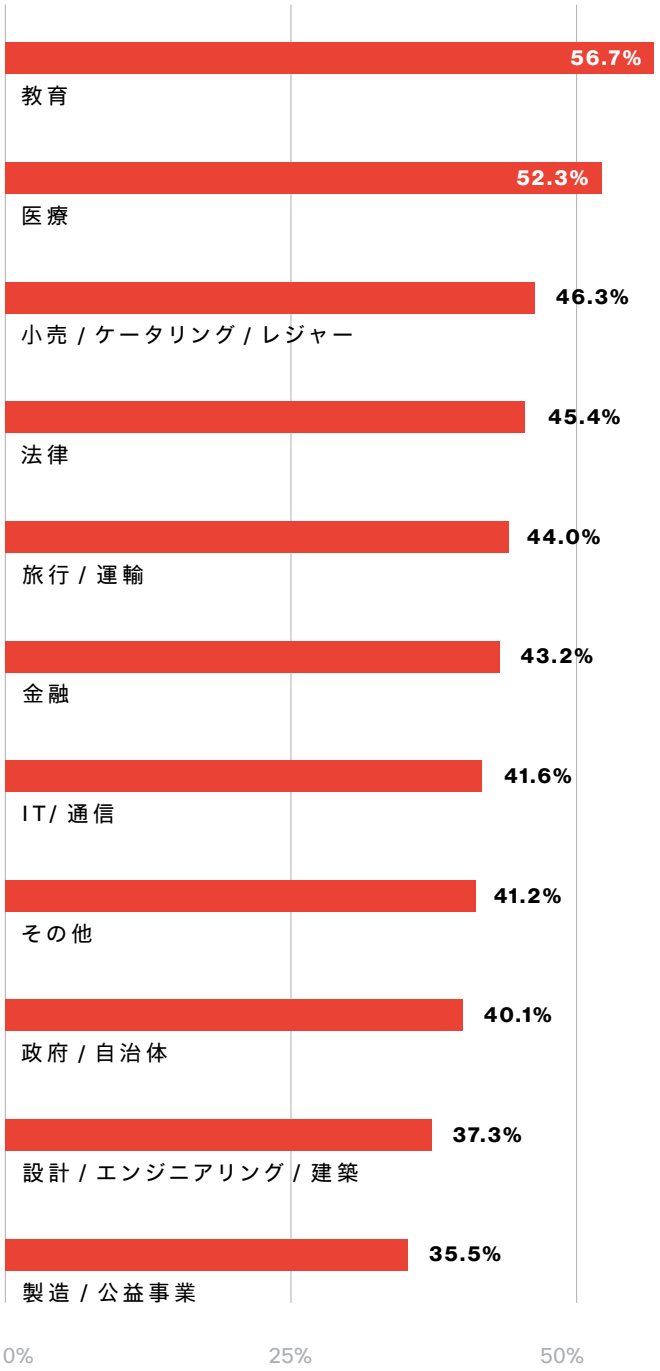
デバイスの衛生状態を維持することは、企業にとって不可欠です。非常に多くの組織にハイブリッドワーク環境が存在するため、従業員が仕事に使用するデバイスのポスチャを考慮する必要があります。システムにパッチを適用していなければ、現代の組織は潜在する回避可能なリスクに自らをさらしていることになります。

例を挙げましょう。ある記者が何年も前に働いていた会社で、私たちは脆弱性を調査すべくすべてのラップトップとデスクトップをスキャンしました。その会社で最も安全なデバイスは自身のラップトップであることが判明しましたが、検出された高リスクの脆弱性は 267 個でした。移動を伴うスタッフを多数抱えていたことを考慮すると、これは組織にとって明らかに危険な事態でした。組織にとってこのリスクは、回避できたはずのものでした。

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。この調査では、最新バージョンのオペレーティングシステムを実行しているデバイスを「最新の状態」とみなすものとします。

驚きには値しませんが、この割合でも教育産業がトップです。ブラウザやオペレーティングシステムの多様性の高さを考えると、教育機関がすべてを最新の状態に保つのに苦労しているのにも無理はありません。毎年「セキュリティ不足ライン」を下回る傾向にあるもう 1 つの産業が医療です。このグラフの下部には驚きの結果が見られます。政府 / 自治体で最新の状態でないブラウザの割合がわずか 40% になっていたのです。厳しい指導とエンドポイントの制御が功を奏し、この割合が低く抑えられた可能性があります。

図 28：業種別の最新の状態でないブラウザの割合

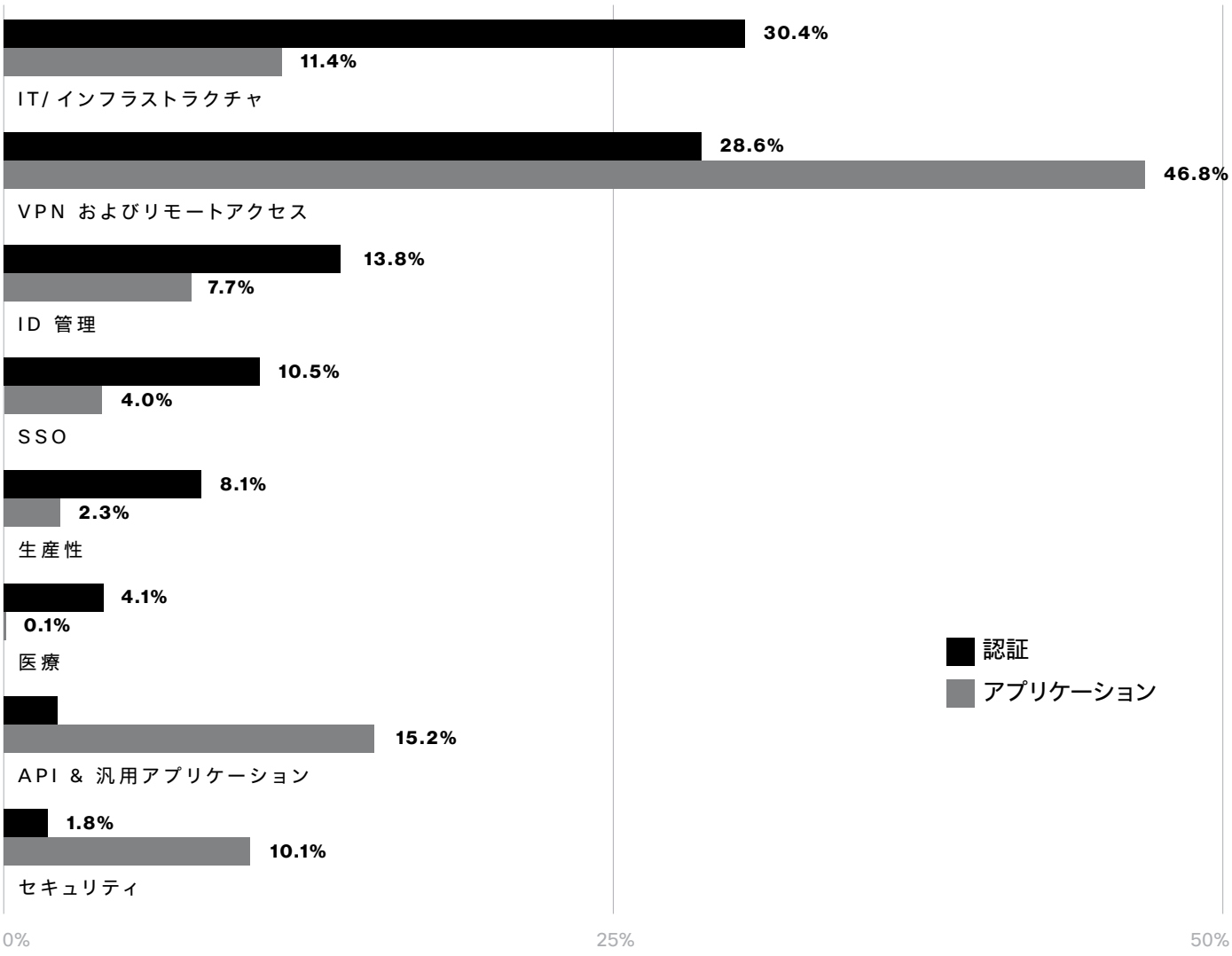


アプリケーション

企業は、ユーザー、デバイス、データを確実に保護するために、安全なアクセスが必要であることを理解しています。安全なアクセスは今日のあらゆる環境に不可欠です。かつての在宅勤務が贅沢とみなされていた時代は終わり、今や在宅勤務は通常のビジネスモデルの一部になっています。

今回は、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。IT/ インフラストラクチャは認証件数では最も多く、僅差で VPN を上回っていますが、アプリケーションの割合では第 3 位にとどまっています。

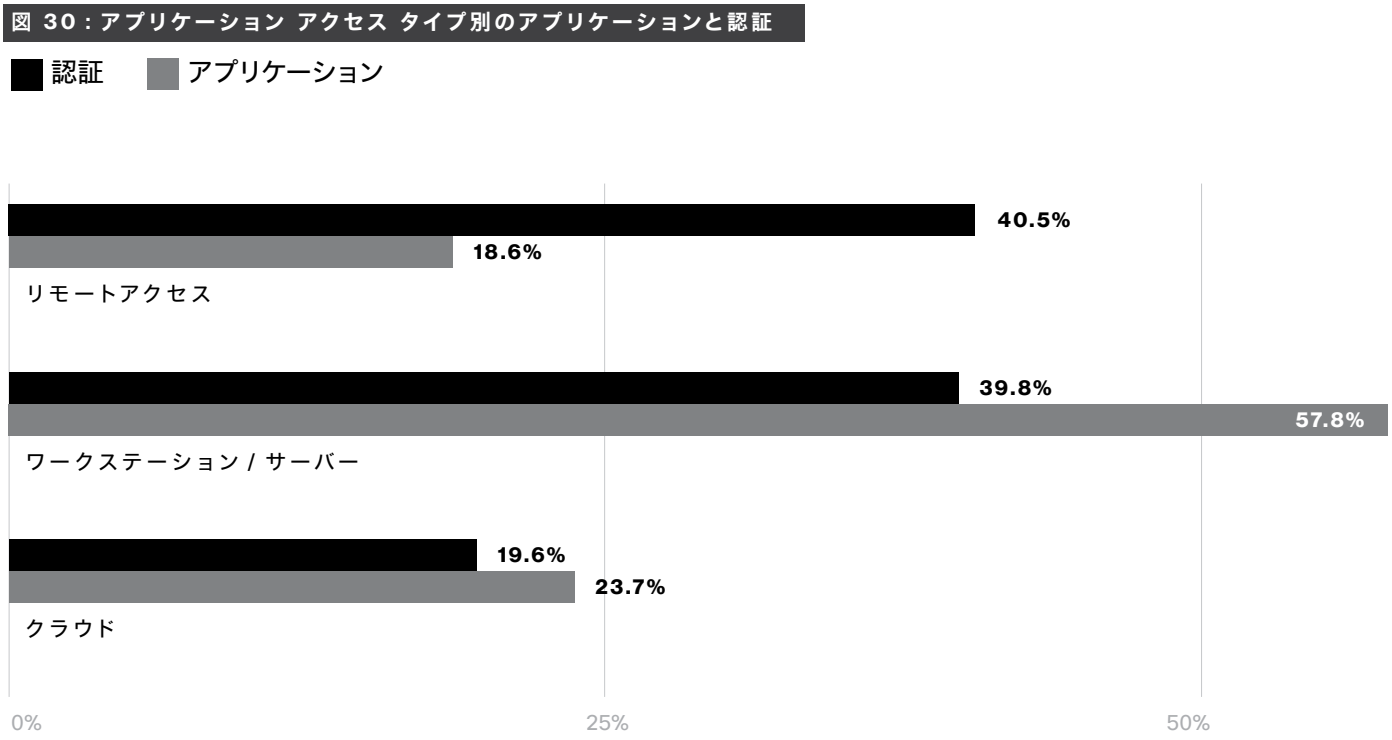
図 29：認証およびアプリケーション総数別の上位アプリケーションカテゴリ



このレポートでは、機能ごとの比較に加えて、提供するアクセスのタイプごとでもアプリケーションを比較しました。リモートアクセスとワークステーション / サーバーアプリケーションは、認証件数の差はわずかですが、リモートアクセスは、アプリケーションの割合では第 3 位です。これは、ほとんどの組織が、単一の VPN またはいくつかのリモートアクセス製品を使用する一方、認証が必要な生産性アプリケーションを数多く使用しているためだと考えられます。ほとんどのユーザーは、そのリモート アクセス アプリケーションを毎日使用することになるため、認証件数は多くなりますが、アプリケーションの数はわずかです。

2021 年から 2022 年にかけてリモートアクセスおよび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。

図 30 : アプリケーション アクセス タイプ別のアプリケーションと認証



アプリケーション利用率の変化

リモートアクセス：

- 認証の割合が -18% 縮小
- アプリケーションの割合が 17.4% 増加

ワークステーション / サーバー：

- アプリケーションの割合が -20% 縮小
- 認証の割合が 24% 増加

クラウドアプリ：

- 認証の割合が -6.6% 縮小
- アプリケーションの割合が 23% 増加

保護されているアプリケーションの割合が拡大しています。元の MFA を拡大し、かつてないほど多くのアプリケーションに対応したすべての組織に敬意を表します。併せてシングルサインオン (SSO) を使用すれば、これらのレベルの保護を導入した企業の全体的なセキュリティ態勢をさらに改善できるでしょう。

まとめ

この一年、あるいはここ数ヵ月でさえも、世界中の防御担当者の状況は大きく変化しました。組織は、ハイブリッドワーク機能の設計にかなりの時間と労力を費やしてきましたが、シスコの Talos Intelligence チームが説明したような現在の脅威の状況に対抗するためには、自社環境にセキュリティレジリエンスが組み込まれていることを再確認する必要があります。

組織にセキュリティの負債が残っていれば、敵の標的となりうる可能性を提供し続けることになります。企業は、技術を磨くとともに、アクセス制御や耐用年数を過ぎても使用されている可能性がある非推奨システムへの対処にさらに注力する必要があります。パッチに対しては、セキュリティ担当者が長年悪影響を与えてきました。パッチを適用すべきだったのに誰もパッチを適用したがらなかったからです。その結果、現実的には現代の企業に影響を与えるはずがない、昔の脆弱性が悪用されるという問題が起きています。しかも、攻撃者は回線上で待機しています。

多要素認証および / またはパスワードレス認証モデルを利用することは、現代の企業にとって不可欠です。防御担当者は Talos などのソースから膨大な量の脅威インテリジェンスを使用できます。ですから、この知識を活用して機能に転換し、環境を可能な限り効果的に保護する必要があります。

ハイブリッドワークモデルが確実に定着した今、私たちがすべきことは、必要なセキュリティレジリエンスを確立し、企業に機能を提供してセキュリティ意識を高めることです。

私たちは、ユーザーが働いている場所を問わず、安全性が確保されているという安心感を持って職務に集中できるようにする必要があります。

今日軍事的に敵対する当事者たちは、相手の運命を変えるためにインターネットを利用することのメリットを学びました。サイバー戦争は、かつて予測されていたように、実際の紛争の原理ではありません。むしろ、ギリシャ人が何世紀も前に習得して登場したファランクスのように、紛争にとって不可欠な要素となっています。防御者としての私たちの責務は、このような新しい困難な時期であっても、人、データ、および情報を保護するための明確な戦略を確立できるようにすることです。

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。パスワードレス ソリューションと組み合わせたゼロトラストなどの戦略は、総合的なセキュリティを向上させるための大きな一歩です。ユーザーエクスペリエンスに重点を置いてセキュリティを幅広く受け入れてもらうことが可能になるため、リスクを軽減できます。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。多要素認証や、WebAuthn などのパスワードレステクノロジーを利用し、強力なセキュリティ インテリジェンスを活用することで、企業のリスクを下げることができます。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。

参考資料

1. 「2021 年 Duo Trusted Access レポート : パスワードレスの未来への道」、Duo Security、2021 年 10 月 14 日
2. 「サイバー戦争がやってくる！ (Cyberwar is Coming!)」、RAND Corporation 社、1993 年
3. 「ウクライナで GoMet バックドアを使用した攻撃を確認」、Cisco Talos、2022 年 7 月 21 日
4. 「サイバー攻撃がルーマニア政府の Web サイトを攻撃 (Cyber Attacks Hit Romanian Government Websites)」、BalkanInsight、2022 年 4 月 29 日
5. アプリケーション向け適応型認証ポリシー、Duo Security
6. Adobe Flash Player EOL 企業向け情報ページ、Adobe 社、2021 年 1 月 13 日

「世界は進化を続け、企業は世界中どこからでも安全に働く方法を従業員に基本として提供する必要性に直面しています」

シスコ セキュリティ アーキテクチャ / リサーチ担当ディレクタ、**Josephina Fernandez**

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。

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ーです。Duo は、Cisco Secure の Zero Trust 製品の重要な柱の 1 つであり、デバイスや IT アプリケーション、環境を問わずあらゆるユーザー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 40,000 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。以下のサイトから、無料でお試しください。

duo.com

Cisco Secure は、最高水準のセキュリティを目指して開発されています。導入、管理、使用が簡単な、顧客中心の合理化されたアプローチを通じてセキュリティを確保できるだけでなく、すべての要素が連携して機能します。Fortune 100 社のすべての企業に最も包括的で統合されたプラットフォームを提供し、どこにいても安全に仕事が行えるように支援しています。シスコのソリューションがエクスペリエンスをどのようにシンプル化し、成功を加速させ、未来を保護するかについては、以下のサイトをご覧ください。

cisco.com/jp/go/secure