WINMAGIC

ホワイトペーパー

次世代多要素認証

ゼロトラストセキュリティモデルに対応したユーザ認証



高度な攻撃に対しては、より高度な認証が必要

多要素認証の従来の形式は、エンドポイントデバイスがユーザ ID やアクセス権限を確認する上で、長年推奨される方法とみなされてきました。しかし、リモートアクセスの使用が大幅に拡大し、サイバー犯罪者がますます巧妙化する中、従来の多要素認証は徐々に推奨される認証方法ではなくなってきています。

近年のサイバー攻撃では、世界で最も安全であると考えられていた対象が、巧妙なハッカーにより攻撃を受ける可能性があることが示されました。攻撃者の知識が豊富で、積極的に攻撃に取り組んでいる場合、単純に「安全である」だけでは不十分です。

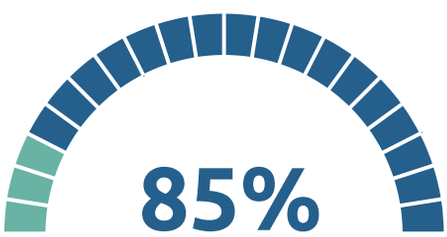
政府のサイバーセキュリティ専門家たちはこのことを把握しており、世界に対して警告を発しています。2021 年 5 月、ホワイトハウスは、米国のサイバーセキュリティの改善を目的に、大統領令を発令しました。この命令では、従来の多要素認証の欠陥を指摘しており、企業や組織のセキュリティ戦略にゼロトラストのアプローチを導入することを推奨しています。このホワイトペーパーでは、従来の多要素認証の欠点、および新しいアプローチによるゼロトラスト認証の強化、導入・使用の利便性の向上について深く掘り下げています。

巧妙化するハッカー

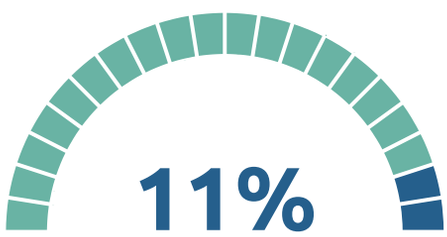
従来の多要素認証の利用だけでは不十分である理由を理解するには、Cozy Bear や Lapsus$ の不正行為者による最近のセキュリティ侵害を見れば明白です。これらのハッカーによる「多要素認証プロンプト爆弾」などの巧妙な手口により、Microsoft や Okta、Nvidia、Cisco、Intel などの多数の企業、および財務省や法務省、エネルギー省、ペンタゴンなどの複数の連邦政府機関がセキュリティ侵害を受けました[1]。

多要素認証プロンプト爆弾は、プッシュ攻撃の 1 つの形式で、ハッカーは、ユーザにプロンプト爆弾攻撃を行い、偽の認証を受け入れるよう試みます。このような攻撃は、スマートフォンの認証アプリで受信する多数のプロンプトで疲れていることが多いユーザが、誤って「承認」を押した場合などに成功します。

Cozy Bear と Lapsus$ の攻撃は、両者とも多要素認証の脆弱性を悪用しています。SolarWinds へのハッキング事件の影響により、大きな損害と被害コストが発生しました。2021 年に調査会社の Sapio2 が実施した、米国、英国、およびシンガポールの大手企業に対するアンケートによると、次のことが明らかになりました。



調査対象企業の 85% が、SolarWinds 攻撃に影響を受けた
（影響大は 31%）



SolarWinds の攻撃により、各企業は平均で年間収益の 11% を失った

Cozy Bear と Lapsus$ のセキュリティ侵害を通して、多要素認証は難攻不落の壁ではないことが証明されました。また、ハッカーは今後も同じ攻撃ベクトルを利用する可能性があり、その場合、膨大なコストがかかることが示されました。

[1] https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/
[2] https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf

米国政府の対応

巧妙化するサイバー攻撃の増大を受け、米国政府は 2021 年、国家のサイバーセキュリティ向上に関する大統領令 14028 を支持するため、「連邦政府ゼロトラスト戦略」を発表しました。このゼロトラスト戦略では、SMS テキストや OTP、プッシュ通知を利用する多要素認証方式はフィッシング耐性がないと宣言しており、政府職員や請負業者に対して、これらの多要素認証ソリューションの使用を中止することを求めました [3]。

そして 2023 年 1 月末までに、フィッシング耐性のある多要素認証を政府組織全体で使用し、政府や請負業者の職員に提供することが義務付けられました。民間の企業や組織も、同様に対応することが賢明だと思われます。



[3] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

ゼロトラストとは？

ゼロトラストはサイバーセキュリティ管理のアプローチの 1 つで、システムにアクセスするすべてのエンドポイントデバイスやユーザを信頼しないことを前提としています。この大統領令の記述を以下に紹介します。

「ゼロトラストアーキテクチャ」とは、脅威は（従来の）ネットワーク境界の内側にも外側にも存在するという認識に基づいたセキュリティモデルで、システム管理とサイバーセキュリティ戦略の原則です。ゼロトラストセキュリティモデルでは、特定の要素やノードおよびサービスからのアクセスを暗黙に信頼（許可）することを禁止し、継続的に複数のソースからリアルタイムに取得した情報を常時（アクセスの度に）検証した上で、アクセス（応答）の可否を判断する必要があります [4]。

したがって、ゼロトラストセキュリティモデルに完全に対応するには、特定の要素を信頼せず、すべての要素に対して継続的かつ常時信頼性を確認することが可能な認証方法が必要になり、従来の多要素認証では対応できません。

[4]https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

従来の多要素認証がゼロトラストセキュリティモデルに対応しない理由

上記で説明したとおり、従来の多要素認証は、フィッシング耐性がありません。従来の多要素認証ソリューションの多くが、スマートフォンを利用していることが理由の 1 つです。サーバは、ユーザを直接確認することができないため、これらのソリューションはスマートフォンを念頭に置いてユーザを確認しています。

スマートフォンを利用する認証に対する攻撃の一例として、「SIM スワップ」攻撃などが挙げられます。SIM スワップは、攻撃者が、悪意のあるさまざまな手口を駆使してモバイルサービスプロバイダを誘導して、攻撃者が所有する SIM にユーザの電話番号が割り当てられた場合に発生します。SIM が交換されると、攻撃者は、ログインして SMS OTP を受信し、OTP を入力してアクセスすることができます。これらの理由により、米国国立標準技術研究所（NIST）は、2 つ目の認証要素として SMS を使用することを制限しました。

問題は、帯域外スマートフォンを使用して認証デバイスとエンドポイントデバイスを関連付ける場合、新たな脆弱性が発生するということです。帯域外スマートフォンを使用している場合、ユーザは、フィッシング耐性を持たない手段（SMS テキスト）を利用して認証デバイスとエンドポイントデバイス間の関連付けを確立する必要があるためです。すべてのセキュリティ侵害の 87% は人的ミスの結果であり、ユーザにアクションの実行を求めるソリューションは、本質的に脆弱です。

新しい考え方

安全なリモート認証には多要素認証が必要だという考えは、リモートサーバ（サービスプロバイダ（SP））は、必ずユーザ（つまり、サービスを受けるエンティティ）を認証する必要があるという古い考えから来ています。先程述べたとおり、これは、責任を認証操作を実行するユーザに押し付けるものです。このようなアクションは通常、モバイルデバイスを利用して、SMS テキストで受信したパスコードの入力、プッシュ通知への応答、OTP の入力を行います。これらの方法は、いずれもフィッシング耐性がありません。

より安全で効率的、かつ使いやすいアプローチとしては、次のように、認証を 2 段階のプロセスにすることです。

手順 01

エンドポイントデバイスを使用するために、ユーザ自身がエンドポイントデバイスに認証を行います。

手順 02

エンドポイントデバイスが（ユーザの代わりに）サーバに対して公開鍵暗号方式の認証を行います。この際、ユーザは認証操作を一切行いません。

このアプローチは、次のように複数のメリットがあります。



このアプローチは、エンドポイントデバイス内の既存の TPM 暗号化チップを利用することで、ユーザが行うより何倍も強力な、公開鍵暗号方式による解読不可能な認証を実現します。



OTP を入力したり、モバイル認証アプリの「同意」を押すなど、ユーザの認証操作は一切必要ありません。



エンドポイントデバイスを継続的かつ常時検証することで、ゼロトラストを実現します。



他の認証デバイスは必要ありません。



ユーザエクスペリエンスが改善され、シームレスになります。



IT 管理が容易になります。



IT の総所有コストが低減します。

エンドポイントデバイスで、ユーザを確実に認証・確認できるのでしょうか？もちろんです。これは、数百万のユーザが日々 Windows にログインする場合など、エンドポイントデバイスが登場して以来、常に行っていたことです。結局、目の前のユーザを確認するには、リモートサーバより、エンドポイントデバイスのほうが適切なポジションにいると言えます。

また、エンドポイントデバイスでは、ユーザの存在だけでなく、サービスにアクセスするユーザの意図も確認できます。これは、明示的に意図を関連付けるために、ユーザが利用するプッシュ認証などの帯域外の方式とは異なります。ボタンを押したり顔認証スキャンを送信するなど、ローカル操作（ローカルジェスチャ）では、ユーザの正確な意図はリモートサーバに伝えられません。

今さら特筆することではありませんが、エンドポイントデバイスを使用して再認証を行うことは、新しいことではありません。すでに大半の Web サイトやエンタープライズソリューションでは、エンドポイントデバイス上の Cookie を何らかの形で利用して、再認証を行っています。ただし、SolarWinds の多要素認証を迂回した攻撃で明らかになったように、Cookie は脆弱であり、巧妙なハッカーに対して安全性を確保することはできません。TPM が搭載されたエンドポイントデバイスは、Cookie より、認証および再認証の安全性が大幅に向上します。

暗号化の価値

オンラインでは、視聴する音声から Webcam の動画まで、すべてがデータです。これらのデータはすべて、リアルタイムでも操作することが可能です。データを保護しゼロトラストに対応した最適なテクノロジーは、暗号化です。データの完全性、機密性、信頼性、否認防止を保証できるのは、暗号化のみであるためです。

暗号化は、防御に最適です。データを保護したり、デバイスやユーザを認証する場合、新しい暗号鍵の生成は、ミリ秒単位で簡単に行うことが可能です。反対に、鍵を発見したり攻撃する場合、時間は無限にかかります。地球上のすべてのコンピュータを使用しても何百年も取り組む必要があります。このような理由から、オンラインデータを最適に防御するには、暗号化を使用して攻撃を防止することです。

ソリューション：MagicEndpoint

従来の多要素認証の限界を回避し、本ホワイトペーパーで説明してきた認証に対する新しい考え方を実証する、そしてゼロトラストセキュリティモデルに完全に対応できるソリューションが登場しました。それはウィンマジックの MagicEndpoint です。MagicEndpoint は、エンドポイントデバイスを活用してリモートアクセスを保護するパスワードレス認証ソリューションで、ユーザのサーバへの認証操作や追加のデバイスは一切必要ありません。シームレスでフィッシング耐性があり、動作していることをユーザが意識する必要はありません。

ゼロトラストに対応した、次世代多要素認証を実現する MagicEndpoint の詳細については、**winmagic.com/ja/home-jp/** にアクセスするか、**こちら**から当社までお問い合わせください。



ウィンマジック

認証し、暗号化し、成し遂げる。

詳細は、ウィンマジックにお問い合わせください

ウィンマジックは、サイバーセキュリティソリューションを開発してきた業界を代表する企業であり、25 年以上にわたってエンドポイント暗号化を進化させてきました。エンドポイントセキュリティに関する豊富な経験と、継続的なイノベーションへのコミットメントにより、世界中の 2,500 以上の企業や政府機関がウィンマジックの製品を信頼して使用しており、全世界で 300 万以上のアクティブライセンスが利用されています。ウィンマジックの認証および暗号化製品は、ノートパソコン、物理データセンター、仮想データセンター、オンプレミス、クラウドなどのあらゆる環境にあるデータを保護します。ウィンマジックのソリューションは、プラットフォームに依存せず、Windows、Linux、Mac デバイスのデータを保護できます。ウィンマジックは、サイバー攻撃の脅威やデータの損失から企業を保護し、プライバシーや法規制のコンプライアンス要件を満たすことができるように支援しており、幅広い評価を得ています。ウィンマジックは、セキュアでシームレスな認証と暗号化を実現します。お客様が、従業員とデータが確実に保護されていることを実感しながら、自由に活動できるようになり、アイデアを共有し、目標を達成できるようなソリューションを提供しています。詳細については、winmagic.com/ja/home-jp/ を参照してください。



WINMAGIC

米国 / カナダ
+1 888 879 5879

欧州 / 中近東 / アフリカ
+49 69 175 370 530

日本
+03 5403 6950

詳細は、こちらをクリックするか、
ウィンマジックまでお問い合わせください。