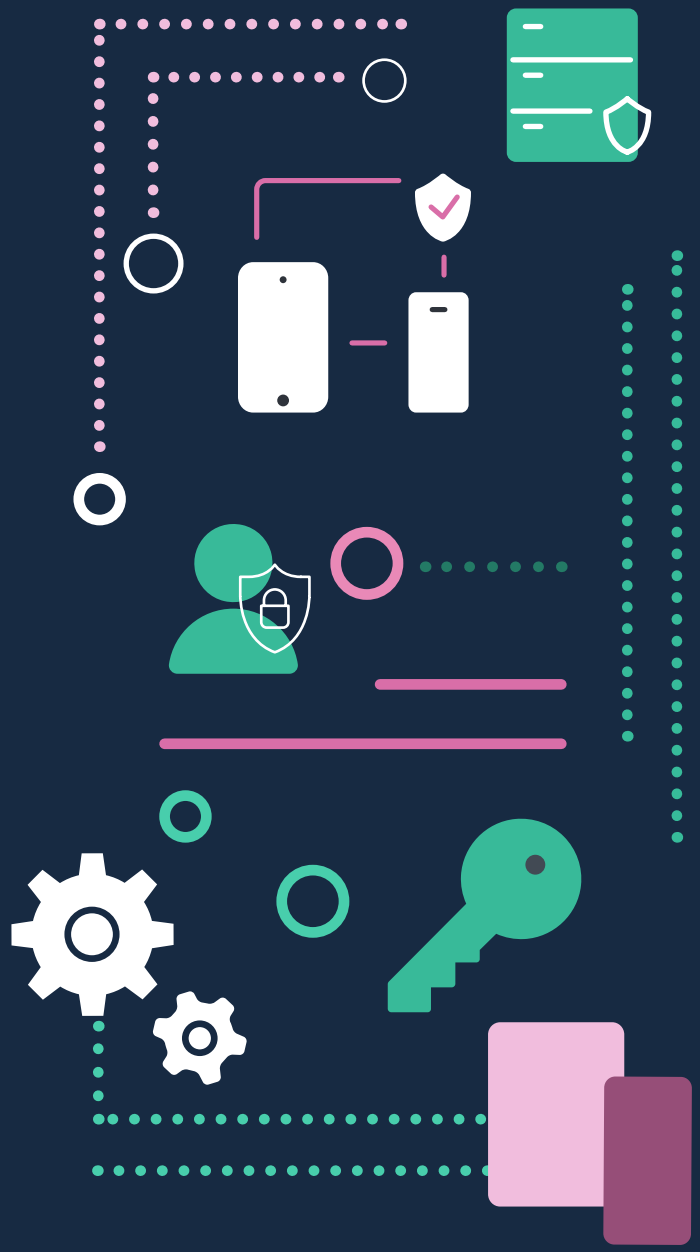


jamf

アイデンティティ管理とセキュリティ

上級者ガイド

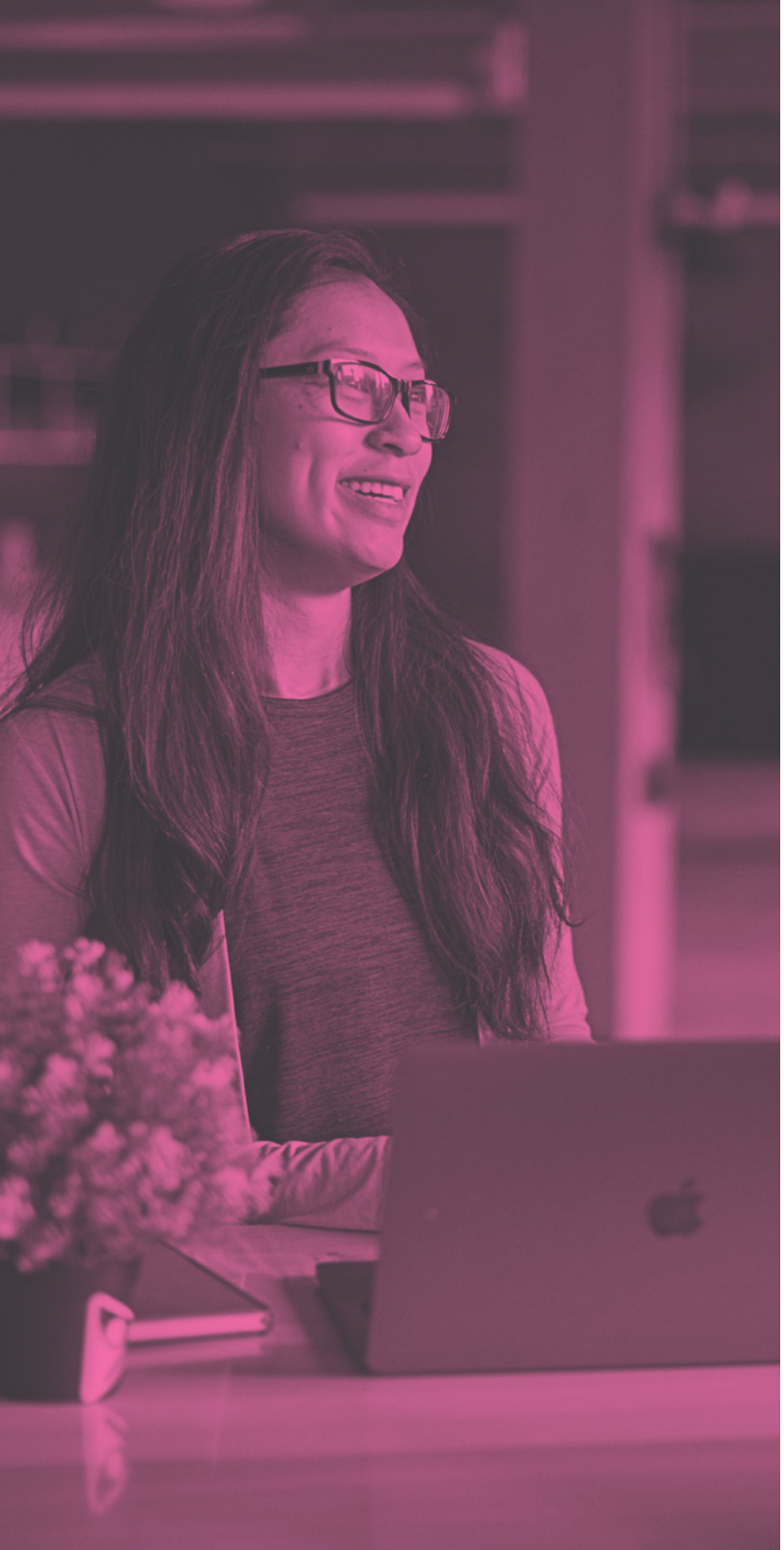
どのワーカーにも独自のアイデンティティがあります

多くの組織がリモートワークの需要に応えようとする中で、アイデンティティ管理の重要性はこの10年余りで極めて明白なものとなりました。「アイデンティティ管理 初心者ガイド」でも触れたように、オンプレミスからクラウドへの移行により、多くの組織が最新のアイデンティティ管理に一歩近づいています。しかし、ゼロトラストのセキュリティ目標を達成したいと願う組織は、単なる認証プロセスを超えたアイデンティティ管理を目指す必要があります。

ゼロトラストのもっとも重要な原則は、ユーザとサービスを繋ぐ上で機能する多くの要素を「決して信用しない」ということにあります。そして、その中でも最大の要素であるネットワークは、何があっても決して信用してはなりません。このガイドでは、アイデンティティ管理とセキュリティの計画を始める際に考慮すべき複数のテクノロジーや事項について説明します。ゼロトラストについて説明したeBook「ゼロトラストネットワークアクセス 初心者ガイド」をまだご覧になっていない場合は、そこから始めることをお勧めします。ここからは、初歩的レベルの知識を高度なレベルへと引き上げていくために、先に挙げた2つのeBookで取り上げたトピックについてさらに深く掘り下げていきます。

このガイドでは以下の点について説明します。

- **最新の認証プロセス**
- **ネットワークトラフィックを保護するテクノロジー**
- **条件付きアクセスのワークフローを追加する方法**
- **これらすべてをJamfで実現する方法**



ストレスフリーな最新の認証プロセス

「アイデンティティ管理初心者ガイド」では、認証と認可の違いについて説明しましたが、今回は最新のサービスで実際にシングルサインオン（SSO）を実現する方法について見ていきましょう。

ユーザのアイデンティティを検証する方法はたくさんありますが、その中で現在もっとも一般的なのは、SAML（Security Assertion Markup Language）、そしてOAuthとOpenID Connect（OIDC）を組み合わせたものです。いずれのシステムも、アイデンティティプロバイダ（IdP）と呼ばれる「信頼できる情報源」に照会してユーザを認証し、ユーザのアイデンティティを証明するために他のサービスと共有できるコードを生成します。Active DirectoryでKerberosに慣れ親しんでいる人なら、多くの類似点を見つけることができるはずです。

ストレスフリーな
最新の認証プロセス

管理者にとっての重要ポイントは以下の通りです。

- SAML認証では、XMLの署名済みブロックであるアサーションが生成され、それによって認証されたユーザを識別し、他のサービスに照会します。
- SAMLでは、SAML認証プロバイダと通信する際に各サービスに対して個別の証明書を要求するため、ネイティブアプリまたはユーザのデバイス上にあるアプリケーションを使用するプロセスが複雑になります。
- OIDCはOAuthと連携してXMLではなく署名付きJWT（JSON Web Token）を生成しますが、これはSAMLアサーションと似た機能を提供します。
- OIDCには、JWTのIDトークンを生成できるというメリットがあります。これは、ポータブルなユーザ記録のようなもので、その有効性を証明するために署名もされています。

SAMLまたはOIDC/OAuth経由でサービスへの認証を行う場合、ユーザのパスワードは IdPによってのみ処理され、サービスがそれを取得することはありません。代わりに、サービスはIdPによって署名された SAMLアサーションまたはOAuthのアクセストークンを取得します。この2つの方法には実装における細かい違いはあるものの、どちらも非常に安全かつ最新で拡張可能な認証方法をユーザに提供します。

ストレスフリーな最新の認証プロセス

以下はSAMLアサーションの例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                     AssertionConsumerServiceURL="https://[servername].jamfcloud.com/saml/SSO"
                     Destination="https://login.microsoftonline.com/[tenant]/saml2"
                     ForceAuthn="false"
                     ID="a4a9efd7a384732928bf1bdbg2afab3"
                     IsPassive="false"
                     IssueInstant="2021-04-02T16:30:58.826Z"
                     ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                     Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://[servername].jamfcloud.com/saml/metadata</saml2:Issuer>
</saml2p:AuthnRequest>
```

それに対し、OAuthトークンは以下のようになっています。

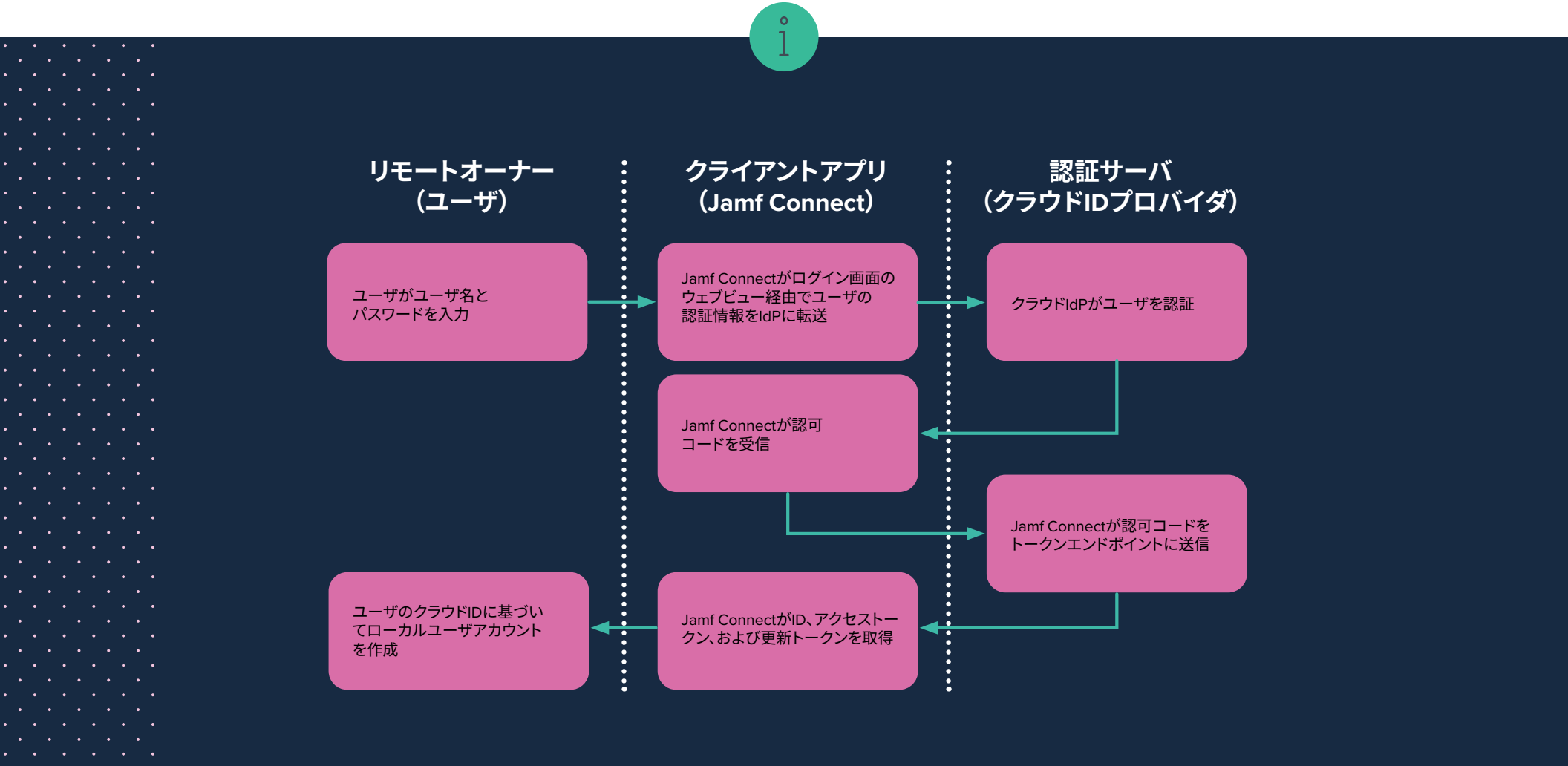
```
"app_displayname": "My Sample OIDC App Name",
  "appid": "2520beb2-535e-4e42-bf70-1d4cd5429551",
  "appidacr": "0",
  "family_name": "Lastname",
  "given_name": "Firstname",
  "idtyp": "user",
  "ipaddr": "52.205.5.180",
  "name": "Firstname Lastname",
  "oid": "0fa4b783-1c00-4765-b40d-c2b72de03079",
  "onprem_sid": "S-1-5-21-1861720204-2608728089-2580082577-1523",
  "platf": "5",
  "puid": "100320004CDFC4DB",
  "rh": "0.AQ4A2rA-GiB-Uuy8iVxxpwOALK-ICVeU0JOy3AdTNVClVFOAQ8.",
```

(*) 上記はトークンの一部のみとなり、完全なトークンを示していません。

JAMFでSAMLとOICD CONNECT/OAUTHを使用する

Jamf ProはSAMLを、そしてJamf ConnectとJamf ProtectはOIDC/OAuthを使用します。Jamf ConnectでSAMLが適用できないのは、証明書が必要とされ、さらに信頼性が確立されていないデバイスに証明書やプライベートキーをプッシュする必要があるからです。これにより、Jamfは各サービスにおいてユーザを細かく管理することなく、クラウドIdPを通して多要素認証を簡単にサポートできます。

以下の図は、Jamf ConnectがOIDCの認可コードグラントを使用して、認可コードと引き換えにユーザのクラウドユーザ名とパスワードを認証し、それをユーザのIdPトークンエンドポイントに送信する仕組みを示しています。



最新の認証と IDPのフェデレーション

IdPのフェデレーションのことに触れずに、最新の認証方法について語ることはできません。Microsoft Office 365でMicrosoft Entra IDを使用する場合でも、実際のIDのフェデレーションは、ユーザのパスワードに関して「真実」を把握しているOktaを通して行われます。フェデレーションでは多数のリダイレクトが必要になることもあり非常に複雑ですが、IdPが認証を別のIdPに引き継ぐことができるというのが基本的なコンセプトです。

ほとんどの場合、SAMLまたはOIDCを介してIdPと統合できるサービスを使用していれば、他のプロバイダとのフェデレーションがあるかどうかを知る必要も、気にする必要もありません。

多要素認証（MFA）

ここからは、多要素認証（MFA）とパスワードレス認証についても見ていきましょう。

ログイン認証情報の盗難は、今日の組織が直面するセキュリティ問題の中でも上位に位置するものです。世界経済フォーラムよると、データ漏洩の80%はパスワードの盗難や脆弱性が原因であるにもかかわらず、このような問題に対処するために費やされている額は10%にも満たないということです。多くの組織では、対策としてIdPを活用してMFAやパスワードレスセキュリティを採用しています。

IdPは、多種多様なMFAソリューションに対応しており、パスワードレスのソリューションにもある程度は対応しています。従来のMFAはワンタイムパスワード（OTP）をベースにしているものがほとんどで、ユーザはパスワードに加えてその都度変化する数字を入力する必要がありました。この番号は、液晶画面付きの小型キーホルダーか、デバイスに搭載されたアプリケーションで生成されました。

多くのIdPは、ユーザにとって使い勝手の良い方法を提供するためにモバイルデバイス用のアプリを用意しています。ユーザがパスワードを入力するとデバイスにプッシュ通知が送信され、ユーザは何らかの生体認証（Face IDやTouch IDなど）を使って、通知に応答しているのが本人であることを証明します。

最近注目を浴びている多要素認証として挙げられるのが、FIDO（Fast Identity Online）です。これはプライバシーとセキュリティに重点を置いた認証方法で、最新のウェブブラウザのほとんどに内蔵されており、外付けのセキュリティキーとして提供されることもあります。FIDOやその他のMFAは、ユーザが実際にパスワードを入力する必要のない「パスワードレス認証」にも使用することが可能です。この場合、MFAは認証プロセス全体に対して使用されます。

Jamfの製品は様々なMFAオプションをサポートしています。IdPによる認証は多くの場合ウェブビュー内で実施されるため、MFAの仕様の構成や設定はすべてIdP自身によって処理されます。

例えばJamf Connectでは、Okta Authentication APIを使用して以下のような初期タスクを構成することができます。

- ローカルアカウントのクラウド認証
- パスワード同期
- ユーザのOktaへのサインイン

このAPIの詳細については、Oktaの開発者ドキュメントをご覧ください。

VPNを超えるソリューション

ゼロトラスト以前は、ユーザのデバイスとサービスプロバイダ間のトラフィックを保護したい場合、VPN（仮想プライベートネットワーク）を使用してユーザのすべての通信を保護する場合がほとんどでした。VPNは今でも多くのIT部門に活用されている非常に便利なツールですが、いくつかのデメリットがあります。

- ほとんどの場合、クライアントソフトウェアが必要となる
- クラウド認証に対応していない場合がある
- ネットワークに専用のハードウェアが必要で、クラウドベーのサービスを保護できない場合がある
- モバイルデバイスでのユーザエクスペリエンスが貧弱

ほとんどのユーザは自宅で高速インターネットを使用しており、大量のトラフィックを処理できるVPNを採用するとなれば費用が嵩むことが予想されます。

ゼロトラスト
ネットワークアクセス

ZTNA（ゼロトラストネットワークアクセス）は、クライアントをセキュアな方法でサービスに接続するための最新のコンセプトです。ZTNAがあれば、VPNが必要なくなるだけでなく、ほとんどの場合クライアントソフトウェアさえ必要ありません。その代わり、ユーザはウェブブラウザを通してZTNAサービスに接続し、最新の認証方法を通してセキュアなアクセスを手に入れることができます。

ZTNAソリューションは本来、最新の認証方法を追加することが困難な旧式のオンプレミスサービスを保護するために生まれましたが、現在ではクラウドベースのサービスをZTNAで保護したいと考える組織が増えています。ZTNAソリューションには、クラウドベースのものもあれば、自社のデータセンター内で管理できるものもあります。より堅牢なZTNAソリューションは、ウェブトラフィック以外のものも保護できるため、ネットワークへのセキュアなアクセスを確保する目的でVPNを利用する必要がなくなる可能性があります。

JamfでZTNAを利用する方法について詳しく見る

Jamf ConnectのZTNAソリューションは、最新のコンピューティング技術を念頭に置いて作られており、リスクを意識したポリシー管理とアプリケーション毎のマイクロトンネルを備えたアイデンティティベースのセキュリティモデルを取り入れています。

条件付きアクセス

堅牢なゼロトラストアーキテクチャには、しばしば条件付きアクセスやデバイストラストの要素が含まれています。この場合、デバイスの状態そのものが、接続の信頼性を決定する上で重要な判断材料となります。そのため、デバイスを管理することは、デバイスのリスクをより深く理解し、信頼できるデバイスでアプリケーションを使用しようとするどの正規ユーザに、データやリソースへのアクセスを許可するのかを決定する上で役立ちます。

条件付きアクセスでは通常、デバイスに搭載されているOSのバージョン、適用されているセキュリティポリシー、またはデバイスのセキュリティ態勢を決定するその他の多くの属性を把握するために、ローカルエージェントまたはデバイス管理ソリューションをIdPと連携させます。その上でIdPは、アクセスを許可するか、必要であればユーザを完全に認証する前に追加のMFAなど、追加の認証を要求することができます。

条件付きアクセスは、その名の通り、ユーザがどのアプリを使おうとしているのかによって条件付けが行われます。例えばITへの問い合わせシステムなどの場合は、MFAが必要とされなかったりセキュリティが厳しくないケースも考えられますが、ソースコードリポジトリへのアクセスなどの場合は、MFAに成功するのはもちろんのこと、企業所有の管理対象デバイスを使用していることが求められます。

Centrify、Duo Security、Microsoft、Ping Identity、Okta、Salesforceなど、アイデンティティ管理やサービスへのアクセス管理を支援するベンダーは数多く存在します。こういったツールの多くは、クラウドIdPなどの既存の認証インフラストラクチャと連動し、前述のプロトコル（OIDCおよびSAML）を使用してアイデンティティをクラウドサービスまで繋げることができます。

その例として、JamfとMicrosoftの連携により実現した条件付きアクセスについて見てみましょう。Jamf Proは、Enterprise Mobility + Security（EMS）の条件付きアクセスを活用することで、Microsoft Office 365にアクセスするためのポリシーをデバイスに強制適用することができます。これにより、Jamfによって管理されたMacは、Microsoft Endpoint Managerのデバイスのコンプライアンスポリシーを満たしていれば、Microsoftアプリケーションにアクセスできます。Macのデータがクラウドにあれば、Endpoint ManagerとEMSがJamfとフルに統合し、デバイス上で管理機能を提供してくれます。管理されていないMacがメールやその他のクラウドサービスへのアクセスを要求した場合、IT部門はJamf Proのユーザ主導の登録プロセスを有効にし、アクセスを許可する前に安全でないデバイスや管理されていないデバイスを管理下に置こうとします。

JAMFの条件付きアクセスは、MICROSOFTだけでなく、GOOGLEやAWSといった業界の主要リーダーもサポートしています。

ユーザの認証情報がMicrosoftによって検証され、デバイスの認証情報がJamfによって検証されると、ユーザのリスク、デバイスのリスク（組織のポリシーに準拠しているかどうか）、アプリケーションのリスク（どのようなアプリが使用されているか）の分析が実行され、クラウドリソースからのアクセスを許可するかブロックするかをリアルタイムで決定することができます。

これにより、組織は以下の検証を通じて多要素認証をさらに拡張することができるようになりました。

1. ユーザ名とパスワード
2. コードとトークン
3. デバイスのコンプライアンス

これにより、ユースケースのコンテキストに基づいて適切なアクセスを文脈的および動的に提供し、様々なデバイスを使い様々なロケーションで働くワークフォースが必要とする適応性と柔軟性のある境界線が実現します。

エンドポイントセキュリティ

アイデンティティ管理を通して実行されるセキュリティ対策は、オフィス勤務かリモート勤務かに関わらず、従業員のライフサイクル全般を通じてエンドユーザとITの双方に影響を及ぼします。そして、従業員とエンタープライズのリソースを繋げるSaaSアプリケーションは、エンドポイント、ユーザ、企業データに対するリスクを軽減する機会を提供してくれます。

エンドポイントセキュリティとは、エンドユーザのデバイスやエンドポイントが悪意のある攻撃者に悪用されるリスクを軽減するためのものです。デバイスとデータが認可を受けたユーザによって正当な目的のために使用されていることを確認することは、特にデータが様々なSaaSアプリケーションに散らばっている今、ますます重要になっています。この目標を達成するためには、様々な不確定要素が正しく機能する必要があります。そしてそこには、アイデンティティ管理だけでなく、ウィルス対策、セキュリティの構成管理、エンドポイントのインシデント検出と対応などが含まれます。

マルウェア、アドウェア、その他の迷惑なソフトウェアの問題が発生する前に対策をしておくのは大切ですが、デバイスへの影響がメリットを上回ってしまえば、エンドユーザの生産性を妨げるだけです。このことから、Windowsを狙った脅威をMac上で探すのではなく、Macを狙った攻撃を効果的に検出し、修復してくれるウィルス対策を導入するのがベストです。セキュリティに関して考えなければならないことはたくさんありますが、Jamfは前述のすべての面においてサポートを提供することができます。

Jamf Proに内蔵されたセキュリティツールやJamf Connectが提供するアイデンティティ管理機能に加えて、Jamf Protectは組織のセキュリティ環境にシームレスに適応し、マルウェアの阻止やAppleを狙った脅威からの保護、エンドポイントのコンプライアンス監視などを提供してくれます。

複数のセキュリティツールを備えた複雑な環境を持つ組織については、やはりMicrosoftとJamfの機能を組み合わせて活用するのがベストかもしれません。IT管理者やセキュリティチームは、使い慣れた単一の画面からMacフリート全体のセキュリティアクティビティを確認することができます。また、Jamf Protectは、最小限の構成でMac固有のすべてのセキュリティデータとアラートをAzure Sentinelに直接プッシュしてくれます。マルウェアに代表される不審、または悪意のあるアクティビティに関する通知はすべて、既存のワークフローに簡単に統合できるため、セキュリティ担当者の労力や時間はほとんど必要ありません。さらに、Azure SentinelのJamf Protectの攻撃検出と口グ情報で拡張することもできます。これにより、すべてのMacデバイスに対する幅広い攻撃を特定・修復しながら、組織全体のセキュリティを向上させることが可能になります。

セキュリティ態勢を再調整するためのアイデンティティ管理

従来の境界ベースのセキュリティモデルを見直す時期に来ています。既存のIdPの活用方法を見直すことで、組織は最新のセキュリティとゼロトラストを同時に達成することができます。ユーザとデータが分散する今、組織はこういった変化に対応する最新のソリューションを必要としています。エンドポイントのセキュリティを確保するために、デバイスベースのセキュリティ、ユーザベースのセキュリティ、多要素認証、そしてそれ以外についても考えなければなりません。

Jamfでは、それらすべてを一度に実現する方法を提供しています。より良いセキュリティはここから始まります。

まずは無料トライアルから

または、販売代理店までお問い合わせください。