安全なデバイス＆信頼できるユーザのみアクセスを許可する
ゼロトラストネットワークソリューション

Jamf Connect ZTNA

セキュアなビジネス接続をリーズナブルに実現

モバイルデバイスを用いて社外からさまざまなクラウドサービスを利用することが当たり前になった現在の業務環境では、「通信（ネットワークアクセス）」のセキュリティを見直す必要があります。そこで「守るべき情報資産にアクセスするものはすべて信用せずにその安全性を検証する」というゼロトラストセキュリティの考え方に基づき、従来のVPNに変わるリモートアクセスの手段として注目されているのが「ZTNA（ゼロトラストネットワークアクセス）」です。従来型のVPNが一度ユーザ認証をすればすべての社内リソースへのアクセスを基本的に許可するのに対し、ZTNAはアプリケーションやデータへアクセスするたびにユーザを評価し、明示的に許可されていないアクセスをすべて拒否することで安全性を担保します。

「SDP（ソフトウェア定義の境界）」とも呼ばれる、この最新のアプローチをIT管理者が確実かつ簡単に実現できるのが「Jamf Connect ZTNA」です。 macOSやiOS、iPadOS、Android、Windowsに対応したJamf Connect ZTNAを利用すれば、従業員が業務利用するSaaSやオンプレミスのアプリごとにJamf Connect ZTNA経由で接続するように設定できます。接続はアプリごとにトンネルを構築し、1つのトンネルには1つのアプリのトラフィックしか流さないため、万が一セキュリティインシデントが生じてもほかのアプリやネットワークには影響を及ぼしません。

●低レイヤーで通信を行うJamf Connect ZTNA

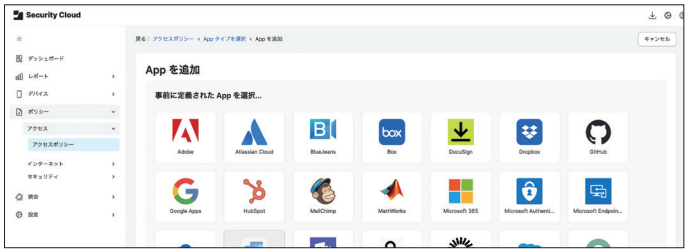
	Jamf Connect	一般的なSASE
L7	アプリケーション層	アプリケーション層
L6	プレゼンテーション層	プレゼンテーション層
L5	セッション層	セッション層
L4	トランスポート層	トランスポート層
L3	ネットワーク層	ネットワーク層
L2	データリンク層	データリンク層
L1	物理層	物理層

OSI参照モデルの7階層で示すと、Jamf Connect ZTNAはネットワーク層（L3）で通信（データのルーティング）を行います。物理層に近い低レイヤーなため、リバースプロキシを利用してアプリケーション層（L7）で通信内容を復号する一般的なSASE製品と比べて処理負荷が少なく、レイテンシーが発生しにくいのが特徴です。また、HTTPベースの制御が中心となるアプリケーション層での通信に対して、Jamf Connect ZTNAは多くの接続プロトコル（HTTP/S、SSH、RDP、VoIPなど）をサポートし、アプリケーションの種類を選ぶことなく、あらゆる通信に対応します。

また、専用ポータル（Jamf Security Cloud）を利用してアプリごとにきめ細やかなアクセスポリシーを作成することも可能です。

具体的には、Jamfの強みであるデバイストラスト（MDMとの連携によるデバイス認証）を活かしてMDMで管理されたデバイスのみ、または特定のグループのみアクセスを許可するように設定できます。さらに、Jamf Protectと連携すれば、接続のたびにデバイスの脅威判定を行い、デバイスポスチャを評価して一定のセキュリティリスクのあるデバイスからのアプリケーションへのアクセスをブロックすることも可能です。

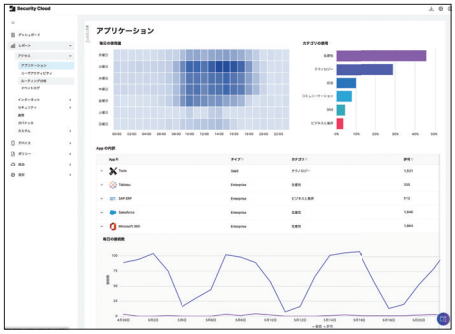
●アプリごとにアクセスポリシーを設定可能



Jamf Connect ZTNA経由でインターネットへ接続するアプリごとにJamf Security Cloud上で設定を行えます。ユーザ個人で使用するアプリは、直接インターネットへつなぐことでプライバシーを保護します。

Jamf Connect ZTNAはクラウドIdPの資格情報を用いてユーザ認証を行うため、新たなアカウントの設定は必要ありません。また、ユーザ認証に必要なJamf Trustアプリやアクティベーションプロファイルは MDMを使用して展開できるなど、IT管理者／ユーザともに簡単に使い始められるのも特徴です。加えて、従来型のVPNと比べて接続アプリの追加やネットワーク設定をクラウド上で完結できることによる運用コストの削減や、次世代VPNプロトコル「WireGuard」による超高速アクセス、グラフィカルで見やすい管理コンソールによる効率的な管理も実現します。こうしたさまざまな特徴を備えるJamf Connect ZTNAは一般的なSASEベンダーが提供するZTNAよりも安価に導入できるため、「脱VPN」を目指す企業のみならず、設定の複雑さや通信速度、価格面で既存のZTNAに不満を感じる企業にも最適です。

●グラフィカルなインターフェイスで可視化



Jamf Security Cloudでは、Jamf Connect ZTNA経由で通信を行ったアプリの使用量やカテゴリ、内訳、接続数に加え、どのユーザがどのゲートウェイを使って、どのアプリを使用したかなどをグラフィカルなインターフェイスで確認できます。

Jamf Connect ZTNAの優位性

1 次世代VPNによる高速通信とバッテリの持ちの良さ

Jamf Connect ZTNAが実装するWireGuardは、従来のVPNプロトコルと比較して約4倍のスループットを実現します。また、Wi-Fiからモバイル回線へ通信が切り替わるときでも迅速に新しい接続を確立し、ほぼ途切れることのない安定した通信が可能です。さらに、業務に必要なアプリの通信だけを暗号化してJamf Connect ZTNAに接続することから、デバイス側のオーバーヘッドが少なくバッテリ消費を抑えられるのもメリット。一定の帯域幅を持つネットワークでも、多くのデバイスが最小限のリソースで高速かつ安全に接続先アプリを利用でき、従来のVPNよりもはるかに快適でストレスフリーなユーザ体験を提供します。

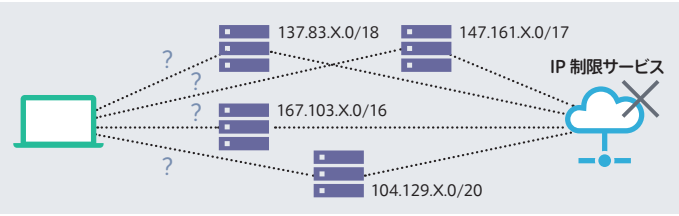
高速で安定した通信を実現する WireGuard は、最先端の暗号技術を採用した高レベルのセキュリティを提供するなど、さまざまな特徴を持つ次世代 VPN プロトコルです。

2 企業固有のグローバルIPアドレスを容易に取得可能

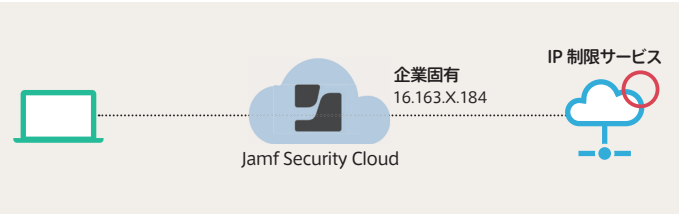
ZTNAを経由してインターネット上のSaaSアプリなどへアクセスする際の接続元のIPアドレスは、ZTNAソリューションが提供するクラウド（データセンター）のIPアドレスになるのが一般的です。そのため、IP制限サービスにアクセスする際はIPアドレスを固定する必要がありますが、一般的なSASEベンダーが提供するZTNAでは、「企業固有のグローバルIPアドレス」を利用するために上位プランへのアップグレードが必要になったり、接続用のサーバを別途立てるなどの手間が発生することがあります。その点、Jamf Connect ZTNAは「完全にユニークな」企業固有のグローバルIPの取得や、IP制限サービスへのアクセス制御を容易に行えます※。

※グローバル IP アドレスの付与には一定の条件があります。

●一般的なSASE



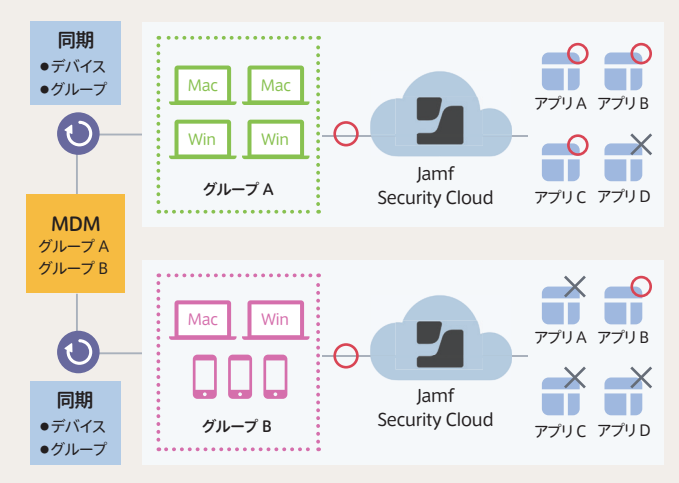
●Jamf Connect ZTNA



IP 制限サービスへのアクセスの際に企業固有のグローバル IP アドレスの取得が難しい一般的な SASE 製品に対して、Jamf Connect ZTNA は標準で対応します。グローバル IP の冗長化も可能です。

3 証明書いらずのデバイス認証

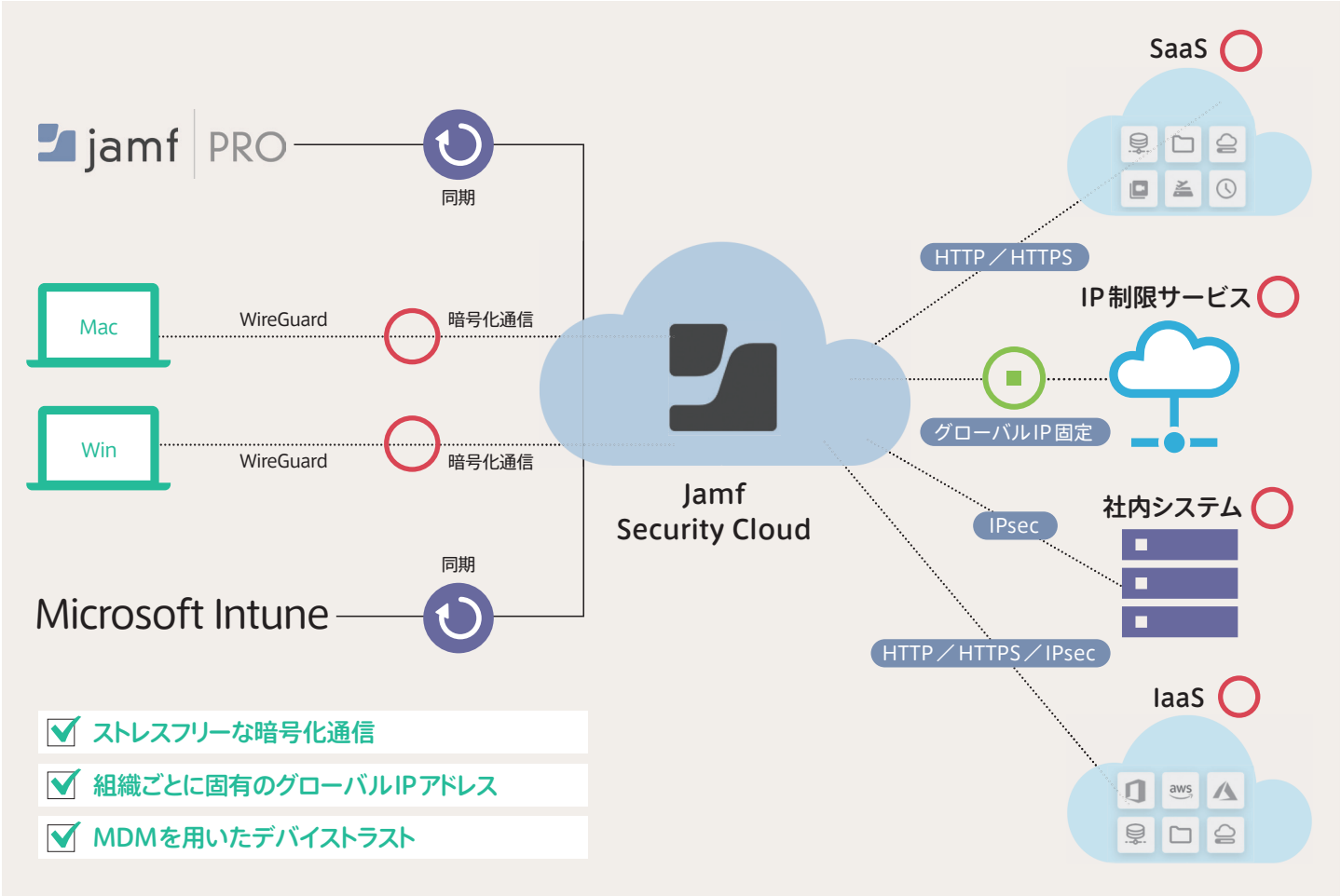
さまざまなMDMと連携するJamf Connect ZTNAを使えば、MDMに登録されている安全なデバイスのみを企業リソースへアクセスさせることが可能です。一般的なSASEベンダーが提供するZTNAでは、証明書の配布や端末のシリアル番号を利用して「デバイスが管理されている」ことの情報は取得できるものの、設定や運用が大変になりがちです。Jamf Connect ZTNAではMDMを用いたデバイス認証の有効化や、未管理のデバイスを利用したアクセス制限をJamf Security Cloudから簡単に設定できます。また、MDMのグループ情報（Jamf Proの場合は「スマートグループ」）を同期して、特定のグループに属している端末のみアクセスを許可することもできます。



デバイスの情報やグループの情報を MDM と同期できるため、特定のグループに属している安全なデバイスのみ特定のアプリだけに接続させるといった高いレベルのアクセス制御が行えます。

Jamf Connect ZTNAの利用イメージ①

Windows & Macの混在環境で「デバイストラスト」による よりセキュアなリモートアクセスを実現



従来型VPNやSASEにないメリット

社内にWindows PCとMacが混在する環境において、Jamfはそれぞれのプラットフォームに最適化したMDMでデバイス管理することをおすすめしています。1つで複数のプラットフォームをカバーする汎用的なMDMよりも、Macの管理においてはApple製品に特化したJamf Proを利用するほうがよりきめ細やかなデバイス管理を行えるからです。

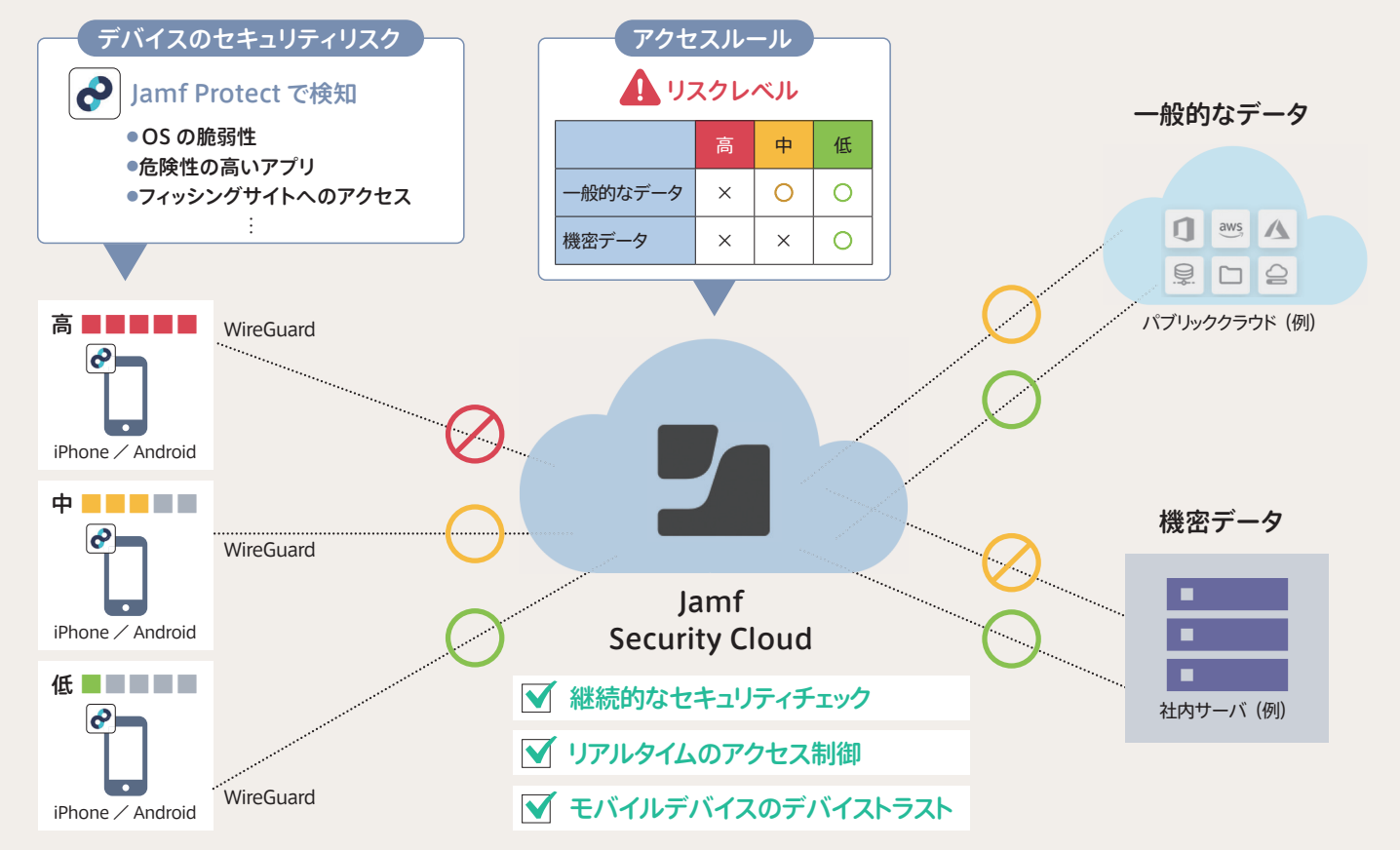
そうした複数のMDMが存在するWindowsとMacの混在環境において、Jamf Connect ZTNAはMDMを用いた「デバイストラスト」による、よりセキュアなゼロトラストネットワークアクセスを実現します。その鍵となるのが、Jamf Security Cloudに搭載される「UEM Connect」です。この機能を利用することで、IT管理者はJamf ProやMicrosoft Intune、他社MDM（VMware WorkspaceONE、Ivanti Neurons for MDM：旧MobileIronなど）のデバイス情報とグループ情報を同期することができます。また、MDMまたはUEM内のデバイスグループをそのまま利用しながらアクセスポリシーを迅速に定義し、確実にMDMによって管理されたデバイスのみをグループごとに、Jamf Connect ZTNA経由で安全に企業リソースへ接続させることが可能です。多額のライセンスフィーのかかる証明書ベースでのデバイス認証とは異なり、「すでに導入しているMDMを用いたデバイストラスト」が容易に行えるのが大きな特徴です。

また、一般的なSASE製品のZTNAと比較すると、SaaSやIaaS、IP制限サービス、社内システムといった接続先には違いはないものの、WireGuardの採用による高速アクセスや、企業固有のグローバルIPの取得が可能なのも大きなメリットです。

さらに、社内システムと接続する際の通信プロトコルに「IPsec」を採用するのも、Jamf Connect ZTNAならではの特徴です。「SSL-VPN」によって通信する従来型のVPNはポートスキャンによって社内ネットワークが見えやすく、かつ通信機器の脆弱性をついたサイバー攻撃によるセキュリティインシデントが懸念されます。一方、SSL-VPNと比べてより低レイヤーのネットワーク層で動作するIPsecははるかにセキュアなプロトコルであり、「IP LockDown」を行ってJamf Security Cloud（Jamf Connect ZTNA経由）の通信以外を受けつけないようにすることもできます。

Jamf Connect ZTNAの利用イメージ❷

Jamf Protectと連携してデバイスの危険度を判定!
モバイルデバイスのリアルタイムのアクセス制御が可能



デバイスの健全性をチェック

マルウェアやフィッシングなどの脅威による被害が年々深刻化する現代においては、外出先へ持ち出すことの多いモバイルデバイスからの企業リソースへのアクセスをよりセキュアに行う必要があります。Jamf Connect ZTNAはiPhoneやiPad、Androidのゼロトラストネットワークアクセスを PC同様に実現するだけではなく、エンドポイントセキュリティソリューションの「Jamf Protect」と連携することで、デバイスのセキュリティリスクに応じたアクセス制御を行うことができます。たとえば、OSに脆弱性を抱えていたり、危険性の高いアプリをインストールしていたり、フィッシングサイトへアクセスしていたりするデバイスは社内リソースにアクセスさせないようにするなど、Jamf Security Cloud上でデバイスのリスクレベルに応じた柔軟なアクセスコントロールが可能です。

ここでの重要なポイントは、こうしたアクセス制御が継続的かつリアルタイムに行われることです。Jamf Protectによって判定されたデバイスのセキュリティリスクレベルの情報は常にJamf Security Cloud経由でJamf Connect ZTNAにも同期されます。つまり、デバイスのリスクレベルが上がった瞬間に企業リソースへのアクセスを瞬時にブロックすることができるのです。このようなアクセスコントロールの仕組みとしてはMicrosoft Entra IDのデバイスコンプライアンスが有名ですが、Entra IDでは基本的にはMicrosoft 365などのクラウドサービスへログインするときにしか判定が行われません。Jamf ProtectとJamf Connect ZTNAの連携であればあらゆる企業リソースへのアクセスに対して、モバイルデバイスのデバイストラストによるアクセス制御が常に可能です。

※本資料の記載内容は2024年8月時点のものです。

jamf
www.jamf.com/ja/

Jamf Japan 合同会社
東京都港区虎ノ門4丁目1－1 神谷町トラストタワー 25 階
Tel : 050-1790-2200
japan@jamf.com