



# ゼロトラスト への信頼

より最新のセキュリティアプローチへの切り替え



# 進化し続けるワークフォース

人々は、グローバルに展開されるビジネスでの働き方における効率化および効果化の実現を模索しています

このような新しい働き方と並行して、テクノロジーの進歩によって人々はあらゆる場所の、ほとんどすべてのデバイスから必要なものすべてにアクセスできるようになりつつあります。これらの変化によって、労働を取り巻く環境ではさまざまな飛躍や結びつきが可能となり、企業は従業員がどこにいても、モバイルや仕事上のニーズのサポートで遅れを取らないように全力を尽くしています。

このサポートを行うにあたり、IT管理者は従業員が生産性を維持できるよう、どこにいてもすべての必要な物事にスムーズにアクセスできる完全な自由を与えると同時にデータの安全を保つという、新たな課題の克服と順応が求められます。



ほぼ一夜にして、企業ネットワークのコンセプトは、最新のリモートでの労働環境では不十分であるとみなされるようになりました。そのため、企業ネットワークのコンセプトは、常に変化しているグローバルな働き方への柔軟性に欠け、IT担当者がただちに対応できないヘルプデスクチケットという形で経費を増やし、データの漏えいによるセキュリティリスクも増大させました。変化に対応するために、テクノロジーのほかの要素はさまざまに進歩を遂げており、安全なアクセスを実現するためのより優れた方法が必要でした。

アイデンティティ中心のアプローチを使った、より効果的なセキュリティのモデルであるゼロトラストを体験してみてください



# ゼロトラストセキュリティモデルとは？

ゼロトラストの核心部分は、新しいコンセプトではありません。実際、Forrester Research社のジョン・キンダーバーグ氏が社内ネットワークは信頼できるという考え方を捨て、境界の内外に関わらず、すべてのネットワーク上のトラフィックは信用できないと見なすゼロトラストの原点という概念を開発してから10年以上が経過しています。彼のコンセプトは「決して信頼しない、常に確認する」という言葉に集約されます。

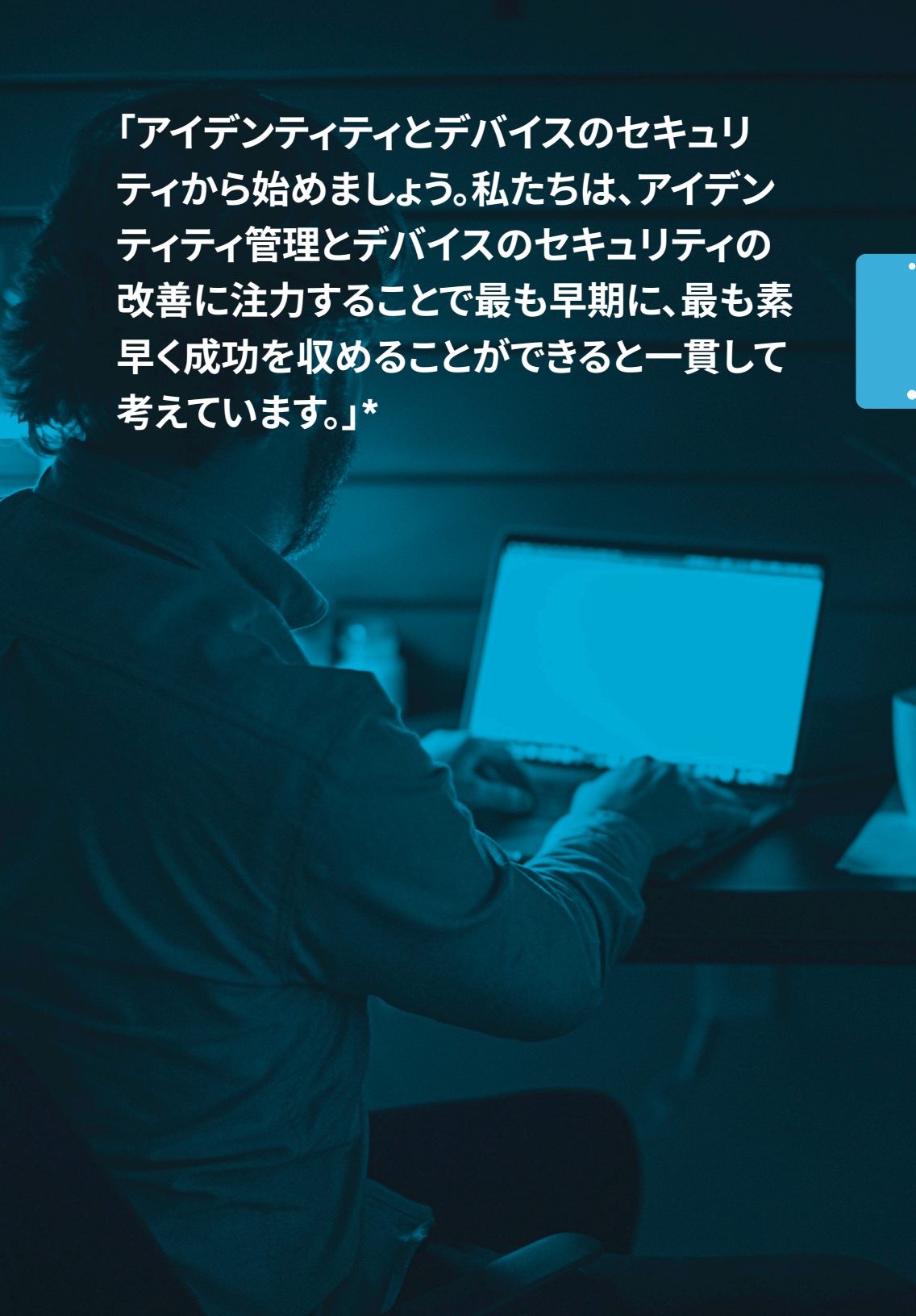
## ゼロトラストのコンセプトには、「決して信頼しない」に加えて、3つの指針があります

- すべてのリソースは場所を問わず、安全なマシンから安全な方法でアクセスしなければならない
- アクセス制御は、ユーザのアイデンティティとそのユーザがアクセスすることを許可されているものに関連した「知る必要性」ベースで行われなければならない
- 組織は、すべてのトラフィックの検査をし、ログを記録して、ユーザが正しい行動をとっていることを確認しなければならない




この最初のコンセプトが展開されてから10年以上、チェイス・カニングハム氏が「セキュリティの中心はユーザであるべきだ」と強調するなど、強化および見直しが行われてきました。この概念は、クラウド認証の進歩、デバイスセキュリティ、アイデンティティとアクセス管理の向上、そしてエンドポイントセキュリティソリューションを最新のアクセス制御とセキュリティの基礎とすることで、実現可能な現実となったのです。





「アイデンティティとデバイスのセキュリティから始めましょう。私たちは、アイデンティティ管理とデバイスのセキュリティの改善に注力することで最も早期に、最も素早く成功を収めることができると一貫して考えています。」\*



セキュリティの「人間的な」側面に重点を置くことで、誰がシステムにアクセスするのか、そしてどんなアクセス制御を持っているのかに、注意を向けられるようになります。そこで、Oktaのようなクラウドアイデンティティプロバイダが非常に重要な役割を果たすことになります。クラウドアイデンティティを活用することで、適切な人材が適切なレベルでリソースへのアクセスを確実にします。これらのユーザは、わずらわしさを増やすことなく、アクセスが必要な時はいつでも、どこからでも生産性を向上するために必要なものにアクセス権を持ちます。

このように、アクセス権を求める個人のアイデンティティに対する信頼性を確保するためのユーザ対応と指針が、組織をゼロトラストのアーキテクチャと成功へと導きます。ただし、この旅路においては、適切なパートナーの活用が極めて重要です。



# ゼロトラストでセキュリティ向上を実現


ゼロトラストの構成要素が人々を最も重視しているのと同様に、組織はセキュリティそのものと同じくらいユーザ体験に配慮する必要があります。優先事項は、もはや「1.セキュリティ 2.ユーザ体験」ではなく「1A.セキュリティ 1B.ユーザ体験」です。

残念ながら、従来は、セキュリティ要件の強化は、従業員にとって大きな負担となり、アクセスするために余分な手順を踏むように強制しなければなりませんでしたが、もうその必要はありません。

Okta Identity CloudとJamf Connectにより、組織はスムーズなシングルサインオンでアプリやデバイス全体のIDを一致させ、高いレベルでユーザの信頼を確保し、次のようなオプションを提供できるようになります

- 常識にとらわれないプロビジョニングと認証
- クラウドベースの認証情報の同期の維持
- ビジネス上重要なアプリへのパスワードレスアクセス





## Jamf Connectは、ほとんどのモバイルデバイス管理ソリューションに対応しています

しかし、Jamf ProおよびOkta Device Trustを組み合わせることで、管理されていないおよび信頼できないMacやユーザが企業アプリや重要な情報にアクセスするのをIT担当者が防御できるようになります。OktaのDevice Trust機能によって、管理者はユーザが組織の最も重要な資産であるデータにアクセスする際に、安全で既知のデバイスだけを利用するように要求できます。これらの3つを組み合わせることで、ユーザはどこで仕事をするにしてもログインし、認証情報を確認し、どこにいても3層構造のセキュリティ要塞のような形でシームレスかつ安全にアクセスすることができるようになります。オフィスでも、自宅や外出先でも、ユーザのアイデンティティが確認することができるようになり、ユーザは必要なものを手に入れ、IT担当者はすべてが安全であることを知ることができます。

Oktaのようなアイデンティティプロバイダを使用することで、ユーザ、グループ、パスワードおよびリソースへのアクセスを、クラウドで安全に一元管理し、リモートで管理できるようになります。また、Jamf ConnectとJamf Proを使用して、セキュアに展開されたすべてのユーザのプログラム、アプリケーション、リソースにまたがるシングルサインオン(SSO)が可能になります。これでIT担当者は、ユーザがどこからリソースにアクセスするかに関わらず、高いレベルのセキュリティが保たれていると分かります。このように労働者に柔軟性を与えることで、IT担当者はセキュリティを強化しながら、労働者の効率と効果を実際に向上させることができます。

jamf | CONNECT

okta

JAMF CONNECT  
トライアルのお問合せ

OKTAの詳細について

# ユーザからデバイスへ、 信頼を拡大する



「決して信頼しない、常に確認する」は、デバイスそのものの検証も含まれています。ユーザIDの確認はセキュリティ対策の主要な部分ですが、ユーザがリソースにアクセスしているマシンを確認できれば、さらに防御力を高めることができます。Symantec社の2019年度Internet Security Threat Reportによると、「組織内で使われるデバイスのうち、36台に1台はハイリスクに分類される」ことが分かりました。特に個人所有 (BYOD)のデバイス使用の人気のよって、リスクは高まっています。重要なリソースへのアクセスを許可する前にデバイスの安全なステータスを確保するという「デフォルト否定」アプローチは、ゼロトラストモデルで最も重要なものです。

Venafiによると「ゼロトラスト環境では、各マシンが独自のIDを持つ必要があります。また、そのマシンのIDが有効であることを検証することが必要です」。

ありがたいことに、Venafiの Trust Protection Platformの統合は、Jamf Proとの新たな統合を通じて、TLSベースの信頼認証とマシンIDの管理を、合理的でシンプルなプロセスに変えてくれるのです。この統合によって、何千台ものデバイスに対して任意の数の認証局から、多数の証明書を自動的に発行したり、失効させたりすることができるようになりました。設定プロファイルと柔軟なスコープを使って、保存された証明書の構成を特定のグループの共通デバイスに適用することもできます。Venafiのプラットフォームでは、特別にカスタマイズされたポリシーも同様に管理できるようになるため、同時の証明書を使用する場合に柔軟に対応することができます。これにより、企業または個人所有 (BYOD)のデバイスであっても、重要なWiFi、VPNやその他の企業や組織のリソースへのアクセスが許可される前に、同一の安全信頼レベル水準を共有できます。Venafiの統合により、お客さまのマシンやデバイスに高速かつ大規模なアイデンティティセキュリティを提供し、ゼロトラストへの取り組みを完全に完了させることができます。



VENAFI®

VENAFIの詳細について

# 今すぐ切り替えを 始めましょう

モバイルの世界では、かつて「企業ネットワーク」で実現していたことが、常に移動しながらでも可能であることが求められるようになりました。いくつかの企業は、オンプレミスのMicrosoft Active Directoryしか知りません。Active Directory (AD) はアイデンティティと認証を提供しており、ディレクトリ外からの保護を行っています。ただし、ユーザがドメイン上においてオフィスの壁の中にいなければならないため、制限が多く、もはや十分ではありません。今日のユーザとデバイスは完全に壁の外でやり取りするため、これはもはや機能しません。

ファイアウォールや企業境界の背後にあるセキュリティの誤った認識を取り除くことで、IT担当者およびセキュリティチームは、アクセス制御、デバイス、およびリソースのセキュリティをより頻繁に評価できるようになります。企業ネットワーク上にしかない信頼の壁を壊し、最新のテクノロジーに適応することで、ユーザとデバイスをより強固に保護し、従業員の生産性を向上させることができます。アクセス、デバイスおよびデータのリスクを検証することで、リモートで働く従業員に業務上で必要なツールを自信をもって提供できるようになります。ユーザにとって合理的で直感的な方法で、わずらわしさが少ない安全なアクセスを実現します。Appleが意図したように。

## 出典:

Forrester『A Practical Guide To A Zero Trust Implementation (ゼロトラストを導入するための実践的なガイド)』2020年1月 <https://reprints.forrester.com/#/assets/2/53/RES157736/reports>

Venafi『Why Zero Trust Requires Machine Identity Protection (なぜゼロトラストがマシンID保護を必要とするのか)』2019年5月

<https://www.venafi.com/blog/why-zero-trust-requires-machine-identity-protection>

# ゼロトラスト の旅を始めま しょう

jamf | CONNECT

JAMF CONNECT  
トライアルのお問合せ

