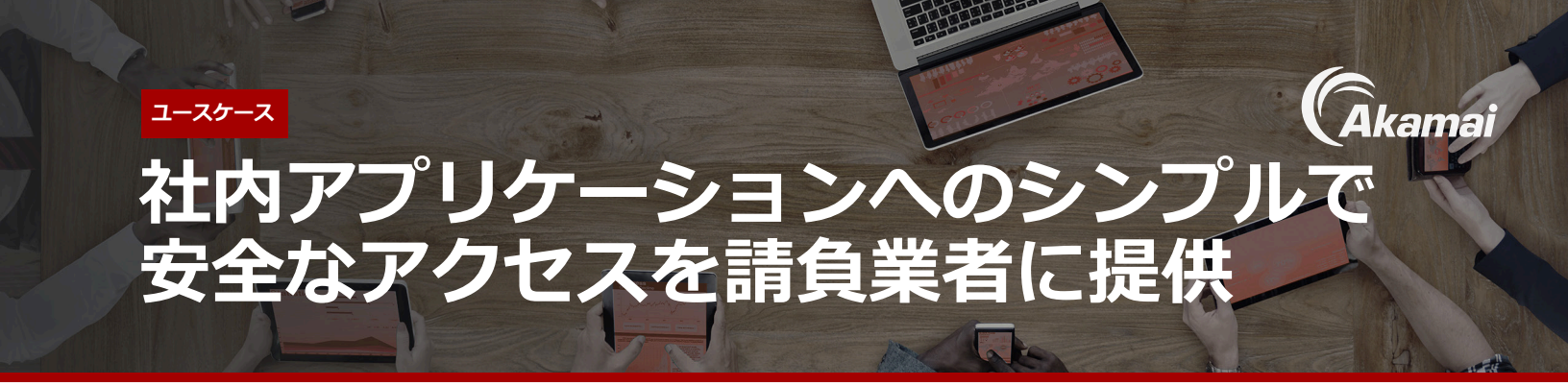


ユースケース

社内アプリケーションへのシンプルで安全なアクセスを請負業者に提供

エグゼクティブサマリー

デジタル変革により世界規模でビジネスの姿は変化し続けています。労働力のエコシステムは拡大しています。多くの企業では請負業者やサプライヤー、パートナーなどのサードパーティーに、ファイアウォールの内側にあるエンタープライズアプリケーションへのアクセスを提供しています。その理由はさまざまですが、ただ一つ不可欠なことがあります。それは、ユーザーグループは管理領域の外側にいるので、アクセスは安全でなければならないということです。

契約社員は、ほぼ
2 社に 1 社
の割合で就業し、
全従業員の
20%～60%を
占めています。[1]

これまでは、VPN や VDI の他、クライアント側のハードウェアやソフトウェア、セキュリティ、IAM、ポリシー関連の設定などのさまざまなソリューションを提供することで、IT は各ユーザーがネットワークや必要なアプリケーションにアクセスできるようにしてきました。さらに、多くの IT 部門では、セキュリティ管理の強化の一環として、請負業者やサプライヤーにハードウェアを提供し、物理的な対策を実施していました。しかしこの方法には拡張性がなく、ほとんどのエンタープライズ組織には適していませんでした。また、サードパーティーによる認証情報の紛失、盗難、誤用はなくならず、依然としてセキュリティ違反が発生していました。

このため、多くの企業ではゼロ・トラスト・セキュリティ・モデルを採用しています。このモデルは、「決して信頼せず必ず確認せよ」というポリシーを前提としています。このアプローチでは、アプリケーションやデータを配信する前に、すべてのデバイスとユーザーに対して認証と許可を行い、アクセスの提供はネットワークレベルではなく、アプリケーションレベルでのみ行われます。さらに、アプリケーションへのアクセスはロギングや行動分析によって監視されます。

20%
の企業が
認定請負業者やベンダーからの
不正アクセスがあったことを
報告しています。[2]

従来のアクセステクノロジーのリスク：これが緊急課題である理由

従来のアクセステクノロジーは、過去のネットワークとビジネス環境に合わせて作られたものです。ほとんどのアクセスシステムはさまざまなテクノロジーを継ぎ接ぎしたものなので、IT にとって管理が複雑であり、もちろん安全性に欠けています。VPN のような従来のアクセスソリューションでは、組織のネットワークにエントリーポイントを作り出すために、ファイアウォールに穴をあける必要があります。違反が発生するとラテラルムーブメント（横方向の移動）が可能になり、ユーザーはアクセスしているアプリケーションを超えて移動することができてしまいます。

また VPN はセキュリティだけでなく、インテリジェンスも欠いています。VPN には接続性の提供と、日々のオンボーディングやオフボーディング、一般的なトラッキングの複雑さを管理するために、多くの追加システムが必要です。そして誰が実際に接続しているのかを検証しておらず、ユーザーの認証情報が正しいかどうかだけをチェックしています。

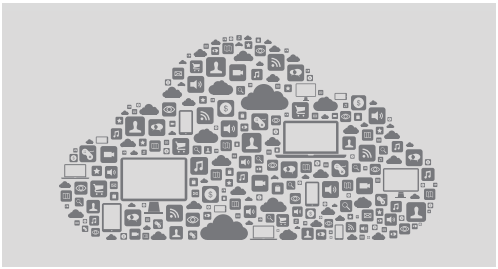
ビジネスリーダーの約 4 人に 1 人（23%）が
自社の契約社員の数を明確に把握
していません。[3]

こうしたセキュリティリスクやセットアップの複雑さ、コンプライアンスとレポート作成のためのユーザーアクセスに対する可視性の欠如などの理由により、従来のアクセステクノロジーは廃止する必要があります。企業はカスタムメードのアプリケーションへのアクセスに対し、リモートで簡単に制限が可能なシステムに移行する必要があります。これにより貴重な IT リソースと予算の制約から解放されます。

社内アプリケーションへのシンプルで安全なアクセスを請負業者に提供

クラウドを使用して請負業者にシンプルで安全なアクセスを提供

ゼロ・トラスト・セキュリティ・モデルへの移行を支援する、高速でシンプル、かつ安全なアクセスソリューションがすでにクラウドには存在します。クラウドネイティブのアクセスソリューションは、すべてのインバウンド・ファイアウォール・ポートを閉じ、許可されたユーザーとデバイスのみがネットワーク全体ではなく必要な社内アプリケーションにアクセスできるようにする独自のクラウドアーキテクチャです。つまりアプリケーションがインターネットや公衆回線から隠されるため、アプリケーションに直接アクセスすることは誰にもできません。



また、クラウドネイティブのソリューションは既存の複雑なアクセス・テクノロジー・スタックを 1 つに集約することができます。この 1 つに集約されたサービスでは、データパスの保護、シングルサインオン、ID アクセス、アプリケーションセキュリティ、可視化、管理の機能が提供されます。クラウド・アクセス・サービスは、どのネットワーク環境へも統合ポータルを利用して 1 か所の制御ポイントから数分で実装が可能です。コストも、従来の数分の 1 しかかかりません。この結果、請負業者に極めて安全性の高いアクセスモデルを提供でき、IT 部門は複雑な管理作業が削減され、また容易に報告と追跡が行えるようになります。

ゼロ・トラスト・セキュリティ・モデルの導入について詳しくは、**「Akamai がゼロ・トラストに効果的な理由」**をご覧ください。また、請負業者へシンプルで安全な接続を提供する、クラウドベースの集中管理型で拡張が簡単な Akamai ソリューションについては、**akamai.com/eaa** をご覧ください。

出典

1) http://workforce-solutions.workmarket.com/rs/908-UMC-610/images/2017_Workforce_Compliance_Report.pdf
2) IDC Remote Access and Security Report (IDC リモートアクセスとセキュリティレポート) https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
3) http://workforce-solutions.workmarket.com/rs/908-UMC-610/images/2017_Workforce_Compliance_Report.pdf

Akamai