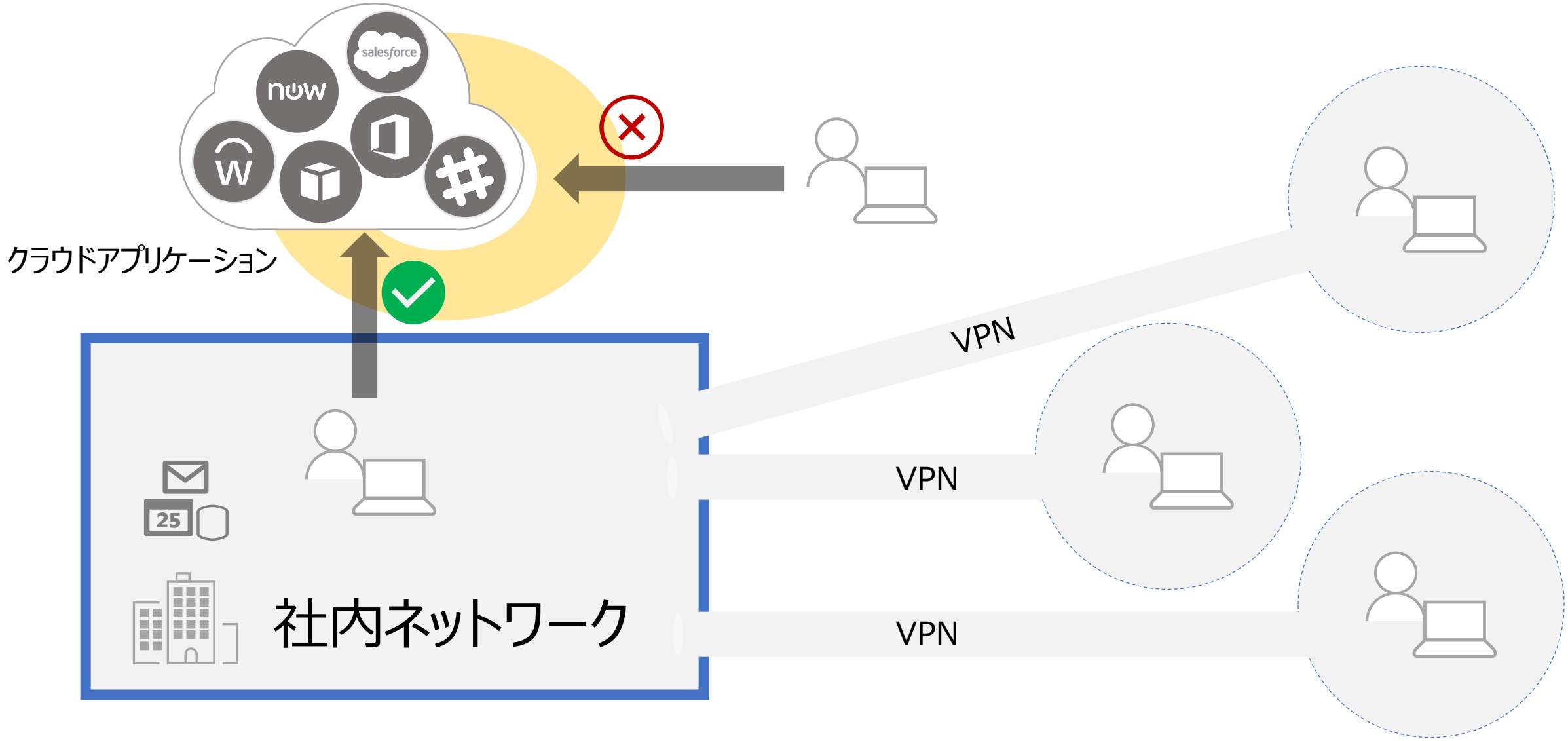
よく見られる現状 – “これをやめたいです”



端末 MDM 管理して
どこからでも SaaS アクセス許可
これで OK?

端末 MDM 管理して
どこからでも SaaS アクセス許可
これで OK?

とても大事で重要な初期ステップであることに間違いはありません

	Traditional	Advanced	Optimal
 Identities	• オンプレミス ID 製品を利用 • オンプレアプリとクラウドアプリの SSO 未実装 • ID のリスク検知が限定的	• Cloud Identity がオンプレ ID と連携済み • クラウドベースのアクセスコントロールが実装済みである • すべてのユーザーが多要素認証を利用 • 特権付与は最小化され JIT 管理されている	• ユーザーはパスワードレス認証でリソースを利用 • ユーザー、端末、場所および振舞いをリアルタイムで分析し、必要な制御を自動適用
 Devices	• 端末は AD ドメイン参加、GPO や SCCM により管理 • データにアクセスするためには社内ネットワーク上にいることが必要	• デバイスはクラウド ID 基盤に登録されている • リソースアクセスはクラウド ID 基盤に参加している端末からのみ可能 • 社給、個人端末双方に情報漏洩対策がが適用されている	• エンドポイント (端末) 上での脅威検出が有効になっていてデバイスリスクとして加味されている • デバイスリスクをベースとしたアクセスコントロールが社給、個人双方の端末で有効になっている
 Apps	• オンプレミスアプリケーションは物理ネットワークまたは VPN 経由でのみアクセス可能 • ミッションクリティカルなアプリがエンドユーザーからアクセス可能になっている	• クラウド ID 基盤にすべてのクラウドアプリケーションが連携 (シングルサインオン、プロビジョニング) されている • オンプレミスアプリもクラウドからの利用が可能に、クラウドアプリとの SSO も実装されている • ユーザーによるアプリケーション同意の制御が行われている • シャドー IT 検出の仕組みが存在する • アプリケーションアクティビティの統合監視	• アプリケーションアクセス権限は必要最低限に保たれ、継続的にアクセス権限検証が行われている • すべてのアプリに対してセッション内部の監視と自動応答を伴う動的なコントロールが行われている
 Infrastructure	• インフラアクセス権限管理は手動で行われている • アプリ・データ管理をしているサーバーの構成管理が実施されている	• インフラ管理上通常と異なる振舞いを検知して通知を行う • リソースへのアクセス許可は JIT 管理されている • リソースには統一のネーミングやタグ付けルールが適用される	• 容認されていない/ルールにそぐわないリソースデプロイはブロックされアラート通知される • すべてのワークロードに対して粒度の細かいアクセスコントロールが実装されそれが可視化されている • ユーザーによるリソースアクセスは区画化されている
 Network	• ネットワークは区画管理されておらずフラットな状態になっている • 最小限の脅威保護と静的なトラフィック制御 • 社内ネットワークのトラフィックは暗号化されていない	• ネットワークは用途に応じセグメンテーションされ各出入り口の適切なコントロールが強制されている • 既知の脅威に対するクラウドネイティブな保護 • ユーザーからアプリケーション、インフラリソースへの内部トラフィックは暗号化されている	• より深いコンポーネントごとのネットワークセグメンテーションと強力な外部アクセスに対する境界防御 • ML ベースの脅威保護と振舞いベースのフィルタリング処理 • すべてのトラフィックは暗号化されている
 Data	• データアクセスはデータの重要度ではなく境界で制御されている • 重要度ラベルは一貫性のないデータ分類をベースとして手動で適用されてる	• データはキーワードと正規表現によって分類、ラベル付けされている • アクセス有無は暗号化によって管理されている	• データ分類が機械学習ベースで行われている • データアクセス制御はクラウドベースの制御エンジンにより行われている • DLP ポリシーによる暗号化、トラッキングによるセキュアなデータ管理

Zero Trust Deployment Center | Microsoft Docs

	Traditional	Advanced	Optimal
Identities	• オンプレミス ID 製品を利用 • オンプレアプリとクラウドアプリの SSO 未実装 • ID のリスク検知が限定的	• Cloud Identity がオンプレ ID と連携済み • クラウドベースのアクセスコントロールが実装済みである • すべてのユーザーが多要素認証を利用 • 特権付与は最小化され JIT 管理されている	• ユーザーはパスワードレス認証でリソースを利用 • ユーザー、端末、場所および振舞いをリアルタイムで分析し、必要な制御を自動適用
Devices	• 端末は AD ドメイン参加、GPO や SCCM により管理 • データにアクセスするためには社内ネットワーク上にいることが必要	• デバイスはクラウド ID 基盤に登録されている • リソースアクセスはクラウド ID 基盤に参加している端末からのみ可能 • 社給、個人端末双方に情報漏洩対策がが適用されている	• エンドポイント (端末) 上での脅威検出が有効になっていてデバイスリスクとして加味されている • デバイスリスクをベースとしたアクセスコントロールが社給、個人双方の端末で有効になっている
Apps	• オンプレミスアプリケーションは物理ネットワークまたは VPN 経由でのみアクセス可能 • ミッションクリティカルなアプリがエンドユーザーからアクセス可能になっている	• クラウド ID 基盤にすべてのクラウドアプリケーションが連携 (シングルサインオン、プロビジョニング) されている • オンプレミスアプリもクラウドからの利用が可能に、クラウドアプリとの SSO も実装されている • ユーザーによるアプリケーション同意の制御が行われている • シャドー IT 検出の仕組みが存在する • アプリケーションアクティビティの統合監視	• アプリケーションアクセス権限は必要最低限に保たれ、継続的にアクセス権限検証が行われている • すべてのアプリに対してセッション内部の監視と自動応答を伴う動的なコントロールが行われている
Infrastructure	• インフラアクセス権限管理は手動で行われている • アプリ・データ管理をしているサーバーの構成管理が実施されている	• インフラ管理上通常と異なる振舞いを検知して通知を行う • リソースへのアクセス許可は JIT 管理されている • リソースには統一のネーミングやタグ付けルールが適用される	• 容認されていない/ルールにそぐわないリソースデプロイはブロックされアラート通知される • すべてのワークロードに対して粒度の細かいアクセスコントロールが実装されそれが可視化されている • ユーザーによるリソースアクセスは区画化されている
Network	• ネットワークは区画管理されておらずフラットな状態になっている • 最小限の脅威保護と静的なトラフィック制御 • 社内ネットワークのトラフィックは暗号化されていない	• ネットワークは用途に応じセグメンテーションされ各出入り口の適切なコントロールが強制されている • 既知の脅威に対するクラウドネイティブな保護 • ユーザーからアプリケーション、インフラリソースへの内部トラフィックは暗号化されている	• より深いコンポーネントごとのネットワークセグメンテーションと強力な外部アクセスに対する境界防御 • ML ベースの脅威保護と振舞いベースのフィルタリング処理 • すべてのトラフィックは暗号化されている
Data	• データアクセスはデータの重要度ではなく境界で制御されている • 重要度ラベルは一貫性のないデータ分類をベースとして手動で適用されてる	• データはキーワードと正規表現によって分類、ラベル付けされている • アクセス有無は暗号化によって管理されている	• データ分類が機械学習ベースで行われている • データアクセス制御はクラウドベースの制御エンジンにより行われている • DLP ポリシーによる暗号化、トラッキングによるセキュアなデータ管理

Zero Trust Deployment Center | Microsoft Docs

M 社の事例

認証は**パスワードレスまたは多要素認証**が必須

従業員は自分の端末を**端末管理システムに自分で登録**することができ、自社リソースへのアクセスを開始できる

セキュリティ部門は**各社員端末のデバイス健康状態を確認**し、サービスごとのアクセス制御を強制することができる

従業員とゲストは**管理されていない端末から社内リソースに安全にアクセスする**ための方法が提供されている

従業員は Web やデスクトップアプリから**自身の希望するアプリケーション**を発見して利用開始することができる

はじめの一歩

Identities/ユーザー	• オンプレミス ID 製品を利用 • オンプレアプリとクラウドアプリの SSO 未実装 • ID のリスク検知が限定的	• Cloud Identity がオンプレ ID と連携済み • クラウドベースのアクセスコントロールが実装済み • すべてのユーザーが多要素認証を利用 • 特権付与は最小化され JIT 管理されている	• ユーザーはパスワードレス認証でリソースを利用 • ユーザー、端末、場所および振舞いをリアルタイムで分析し、必要な制御を自動適用
Devices	• 端末は AD ドメイン参加、GPO や SCCM により管理 • データにアクセスするためには社内ネットワーク上にいることが必要	• デバイスはクラウド ID 基盤に登録されている • リソースアクセスはクラウド ID 基盤に参加している端末からのみ可能 • 社給、個人端末双方に情報漏洩対策がが適用されている	• エンドポイント (端末) 上での脅威検出が有効になっていてデバイスリスクとして加味されている • デバイスリスクをベースとしたアクセスコントロールが社給、個人双方の端末で有効になっている
Apps	• オンプレミスアプリケーションは物理ネットワークまたは VPN 経由でのみアクセス可能 • ミッションクリティカルなアプリがエンドユーザーからアクセス可能になっている	• クラウド ID 基盤にすべてのクラウドアプリケーションが連携されている • オンプレミスアプリもクラウドからの利用が可能に、クラウドアプリとの SSO も実装されている • ユーザーによるアプリケーション同意の制御が行われている • シャドー IT 検出の仕組みが存在する • アプリケーションアクティビティの統合監視	• アプリケーションアクセス権限は必要最低限に保たれ、継続的にアクセス権限検証が行われている • すべてのアプリに対してセッション内部の監視と自動応答を伴う動的なコントロールが行われている
Infrastructure	• インフラアクセス権限管理は手動で行われている • アプリ・データ管理をしているサーバーの構成管理が実施されている	• インフラ管理上通常と異なる振舞いを検知して通知を行う • リソースへのアクセス許可は JIT 管理されている • リソースには統一のネーミングやタグ付けルールが適用される	• 容認されていないリルールにそぐわないリソースデプロイはブロックされアラート通知される • すべてのワークロードに対して粒度の細かいアクセスコントロールが実装されそれが可視化されている • ユーザーによるリソースアクセスは区画化されている
Network	• ネットワークは区画管理されておらずフラットな状態になっている • 最小限の脅威保護と静的なトラフィック制御 • 社内ネットワークのトラフィックは暗号化されていない	• ネットワークは用途に応じセグメンテーションされ各出入り口の適切なコントロールが強制されている • 既知の脅威に対するクラウドネイティブな保護 • ユーザーからアプリケーション、インフラリソースへの内部トラフィックは暗号化されている	• より深いコンポーネントごとのネットワークセグメンテーションと強力な外部アクセスに対する境界防御 • ML ベースの脅威保護と振舞いベースのフィルタリング処理 • すべてのトラフィックは暗号化されている
Data	• データアクセスはデータの重要度ではなく境界で制御されている • 重要度ラベルは一貫性のないデータ分類をベースとして手動で適用されてる	• データはキーワードと正規表現によって分類、ラベル付けされている • アクセス有無は暗号化によって管理されている	• データ分類が機械学習ベースで行われている • データアクセス制御はクラウドベースの制御エンジンにより行われている • DLP ポリシーによる暗号化、トラッキングによるセキュアなデータ管理

クラウドベースのアクセスコントロールを導入
すべてのユーザーに多要素認証
特権管理は Just-in-time の考え方を導入

デバイスを Cloud Identity 基盤に登録
リソースアクセスは安全な端末からのみ許可

すべてのアプリケーションをクラウドベースのアクセスコントロールの対象に
オンプレミスアプリケーションのインターネットアクセスを VPN 以外で