ゼロトラスト型セキュリティサービス
導入支援/運用支援サービスのご紹介

目次

当社のゼロトラスト型セキュリティサービスとは

NTTドコモソリューションズのゼロトラスト型セキュリティサービス

■ ドコモグループやNTTグループのゼロトラスト型セキュリティの導入、運用ノウハウを一般のお客様にご提供
■ 本サービスの導入により、エンドユーザはインターネット環境で安心、安全、快適に日常業務ができる

導入ノウハウ

✓ Cisco製品<Umbrella, Duo>の導入手順
✓ MS製品<Entra ID(旧Azure AD), Intune…>の導入手順

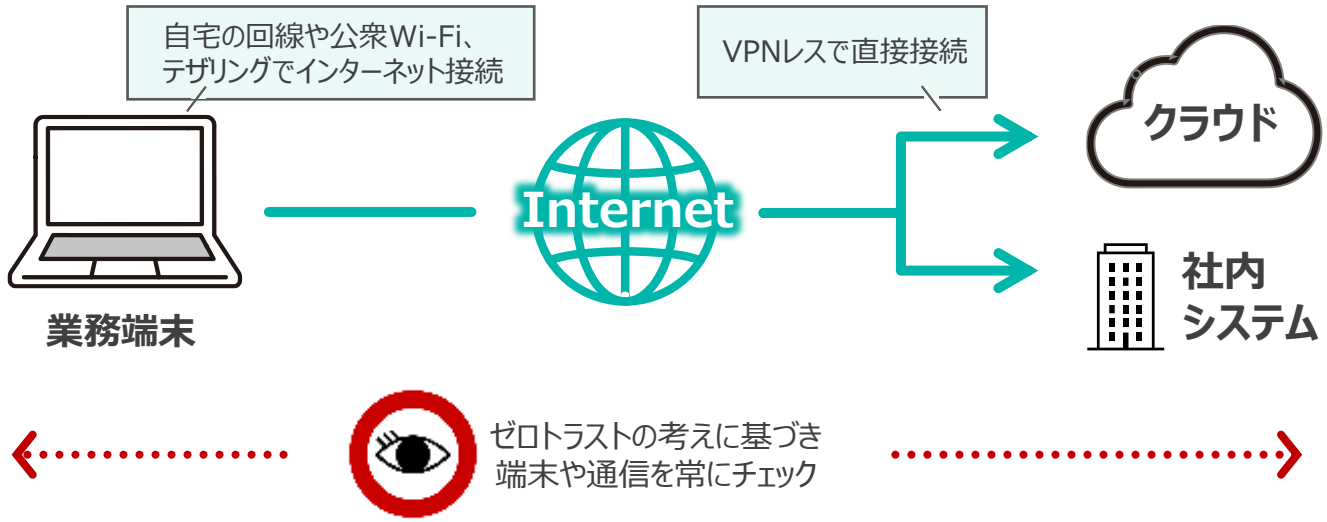
etc…

＋

運用ノウハウ

✓ 当社SOCのEDRアラート対応
✓ 当社SOCのSWGブロックリスト登録
✓ Intuneのポリシーカスタマイズ

etc…

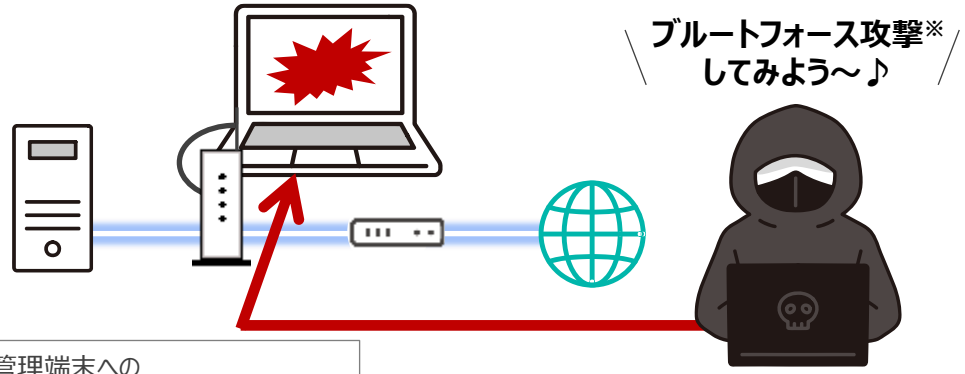


インターネット環境の外部脅威、内部脅威に対応！

インターネット環境における外部脅威・内部脅威

事例1 外部からの攻撃

自宅ルータを設定変更し、オンラインゲーム用サーバを外部に公開
自宅ルータに繋げた持出端末が外部公開され
攻撃者がRDPでログオン試行

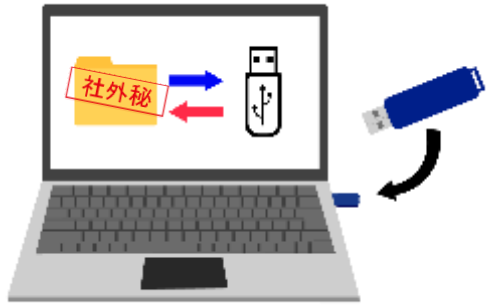


参考 ドコモ管理端末への
不正ログオン試行回数：2～3回/年

※パスワードの考えられるすべての組み合わせを試す方法

事例2 内部犯行

自宅等、周囲の目が無い環境で持出端末を利用
USBメモリの接続やプリンタ追加が
規制されておらず、情報持出



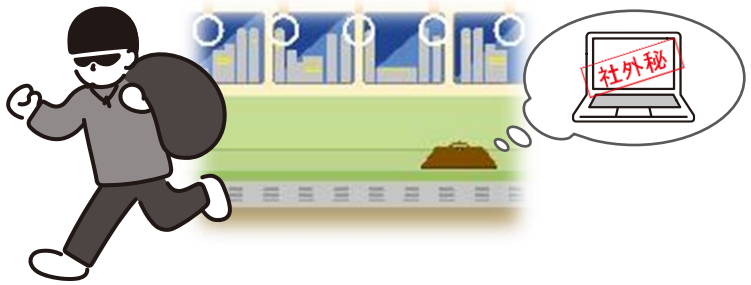
事例3 外部からの攻撃/内部犯行

会社で許可されているクラウドサービスに会社NW以外からアクセス
アクセス元デバイスの制限や
多要素認証が設定されておらず、情報持出

参考 M365ドコモテナントへの
不正ログオン試行回数：2～3回/月

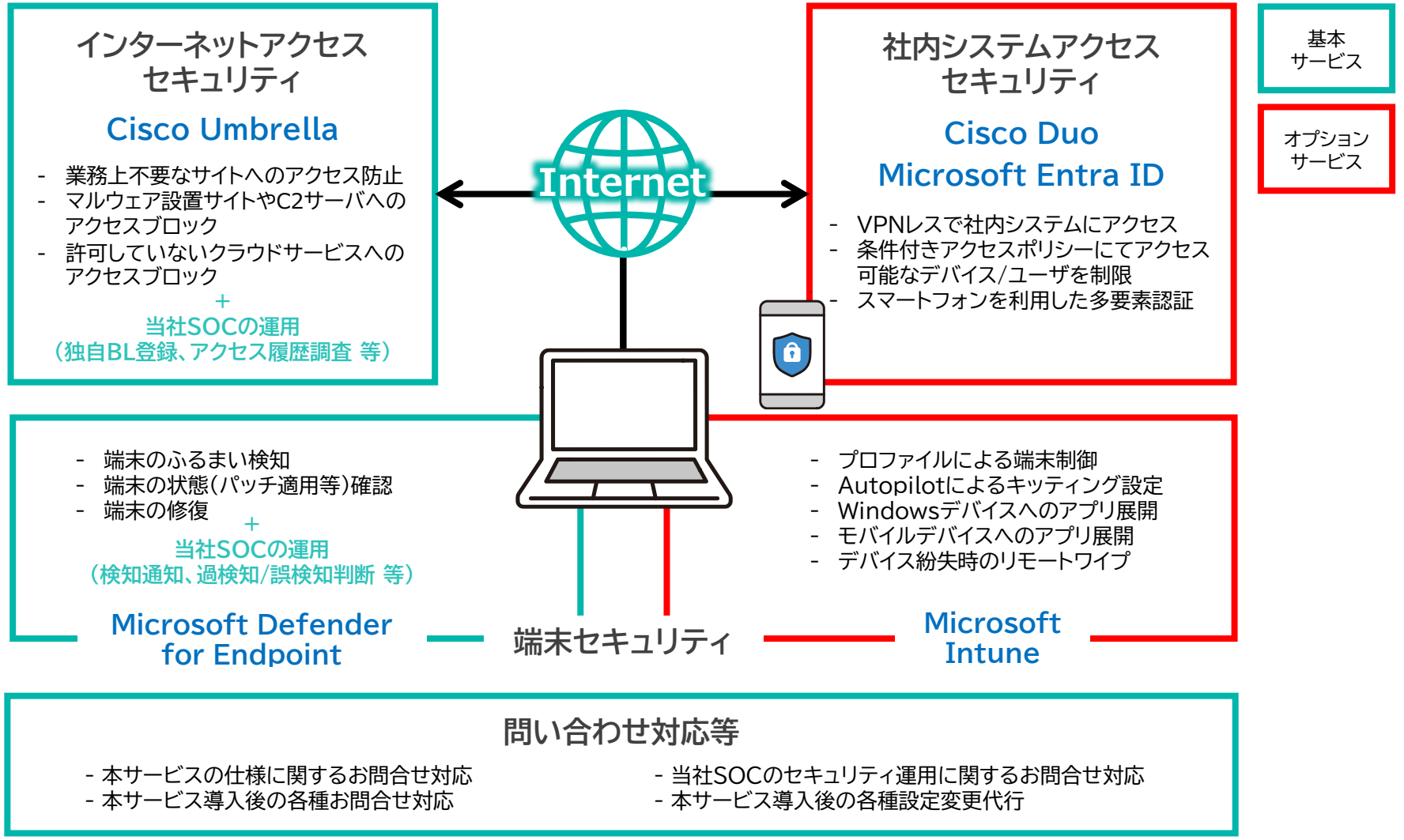
事例4 過失

飲酒により持出端末を紛失
悪意のある第三者に端末が盗まれ、
端末内の組織データが流出



サービス概要

- ゼロトラスト型セキュリティの実装に必要となるCiscoやMicrosoftのサービスの導入、および運用支援をサービスとしてご提供
- Cisco系サービスについては当社からライセンスを提供



サービスメニュー/提供価格

●初期費用

	項目		説明	価格(税抜)
基本	インターネットアクセス セキュリティ	導入支援	Cisco Umbrella SIG Essentialsの導入における初期設定※ ※AL/BL設定、SSL可視化除外設定、ブロック画面のカスタマイズ　等	¥1,500,000
	端末セキュリティ (MDE)	導入支援	当社のSOCがMicrosoft Defender for Endpoint P2を運用するにあたっての初期設定手順の提供	¥250,000
オプション	社内システムアクセス セキュリティ	導入支援	インターネット回線での社内システムアクセスを実現するためのDuo Network Gatewayの構築および Duoの設定	¥5,000,000
	端末セキュリティ (Intune)	導入支援	Microsoft Intuneの各種ポリシー設定	¥5,000,000

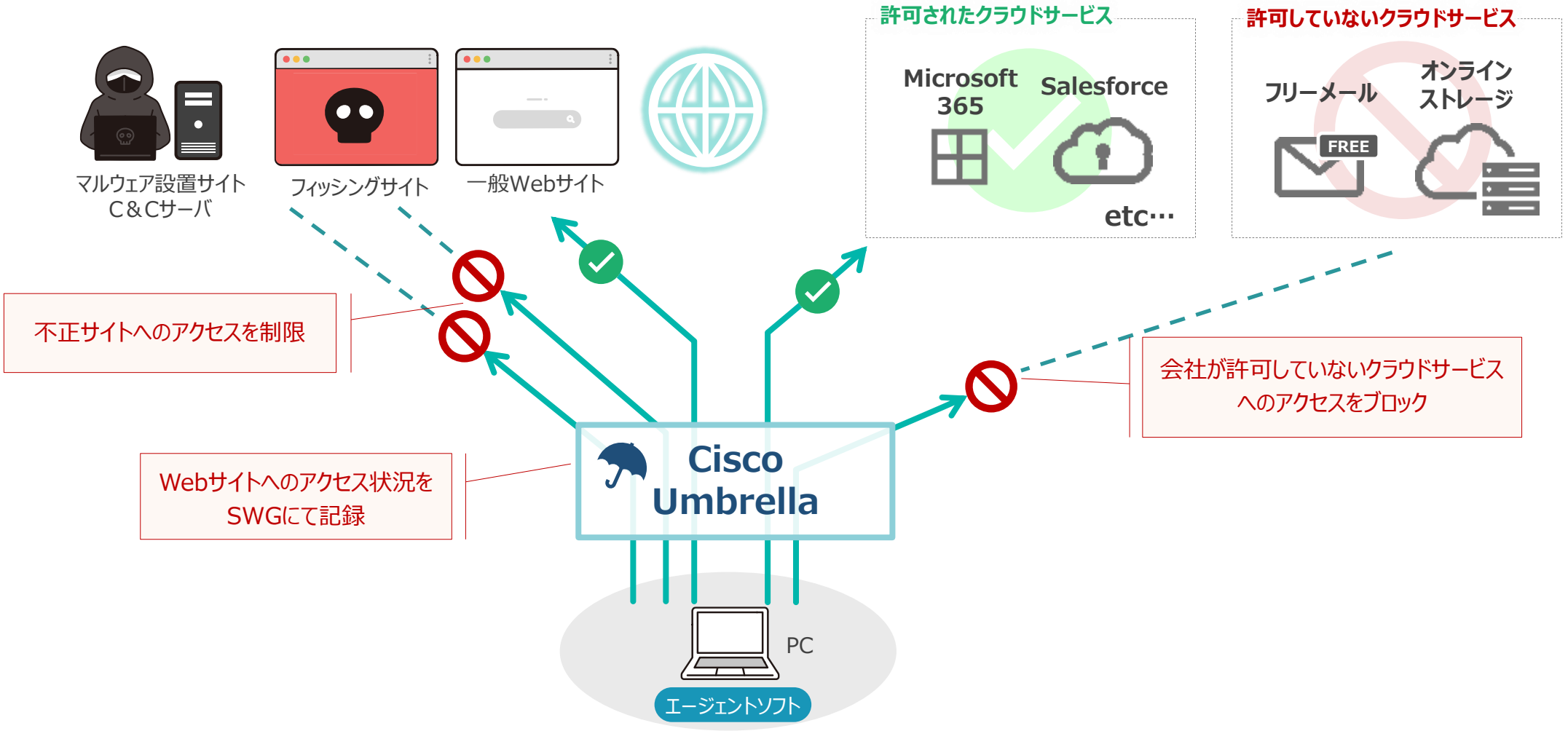
●月額費用(年額一括前払いの場合)

	大項目	小項目		説明	価格(税抜)
基本	利用料(固定)	SOC定期レポート ＋ 問い合わせ対応 等		インターネットアクセスセキュリティおよび端末セキュリティ(MDE)関連の定期レポート(月1回) 5チケット分の問い合わせ対応(2.5H分)	¥200,000 /社
	利用料(変動)	インターネットアクセス セキュリティ	ライセンス販売	Cisco Umbrella SIG Essentialsのライセンスを販売	¥2,400 /ユーザ
			運用支援	当社のSOCによるセキュリティ運用	
		端末セキュリティ (MDE)	運用支援	当社のSOCによるセキュリティ運用	
	チケット料	問い合わせ対応 等		本サービスに関するお客様からの問い合わせへの対応やお客様の依頼による各種設定変更等の 代行作業費用 ※1チケットあたり30分の対応稼働を提供	¥5,000 /チケット
オプション	利用料	社内システムアクセス セキュリティ	ライセンス販売	Cisco Duo Beyondのライセンスを販売	¥2,400 /ユーザ

インターネットアクセスセキュリティ

インターネットアクセスセキュリティ－機能のご紹介－

- Secure Web Gateway(Cisco Umbrella)を利用し、自宅NWや公衆Wi-Fi経由のインターネットアクセスを制御
- 標的型攻撃によるマルウェア感染、フィッシングサイトによる認証情報の搾取を防止
- 悪意のある社員によるオンラインストレージやメールサービスを経由した内部犯行を防止



インターネットアクセスセキュリティ－導入支援サービスのご紹介－

docomo Solutions

導入支援サービス作業範囲

作業項目	作業担当	作業内容
管理者アカウント作成	お客様(管理者)	当社が環境設定およびSOC運用で利用するアカウントの作成
導入ヒアリングシート作成	お客様(管理者)	コンテンツカテゴリ、AL、BL等の初期設定内容の記入
環境設定	当社	御社用テナントの環境設定
各種ポリシー初期設定	当社	導入ヒアリングシートの記入内容の初期設定
接続先リスト設定	当社	AL/BLの設定
可視化除外設定	当社	可視化除外する接続先の設定
ダイレクトアクセス設定	当社	Umbrellaをバイパスする接続先の設定
コンテンツカテゴリ設定	当社	接続をブロック、もしくは抑止するコンテンツカテゴリの設定
ブロック画面設定	当社	ブロック画面のイメージ、出力文言の設定
クライアントアプリ等配置	お客様(管理者)	クライアントアプリ、構成ファイル、証明書を所定のファイルサーバに配置
クライアントアプリ等ダウンロード	お客様(エンドユーザ)	Umbrella導入端末へのクライアントアプリ等ダウンロード
クライアントアプリインストール	お客様(エンドユーザ)	Umbrella導入端末へのクライアントアプリインストール
構成ファイル配置	お客様(エンドユーザ)	Umbrella導入端末内の所定のフォルダに構成ファイル配置
証明書インポート	お客様(エンドユーザ)	Umbrella導入端末内に証明書インポート

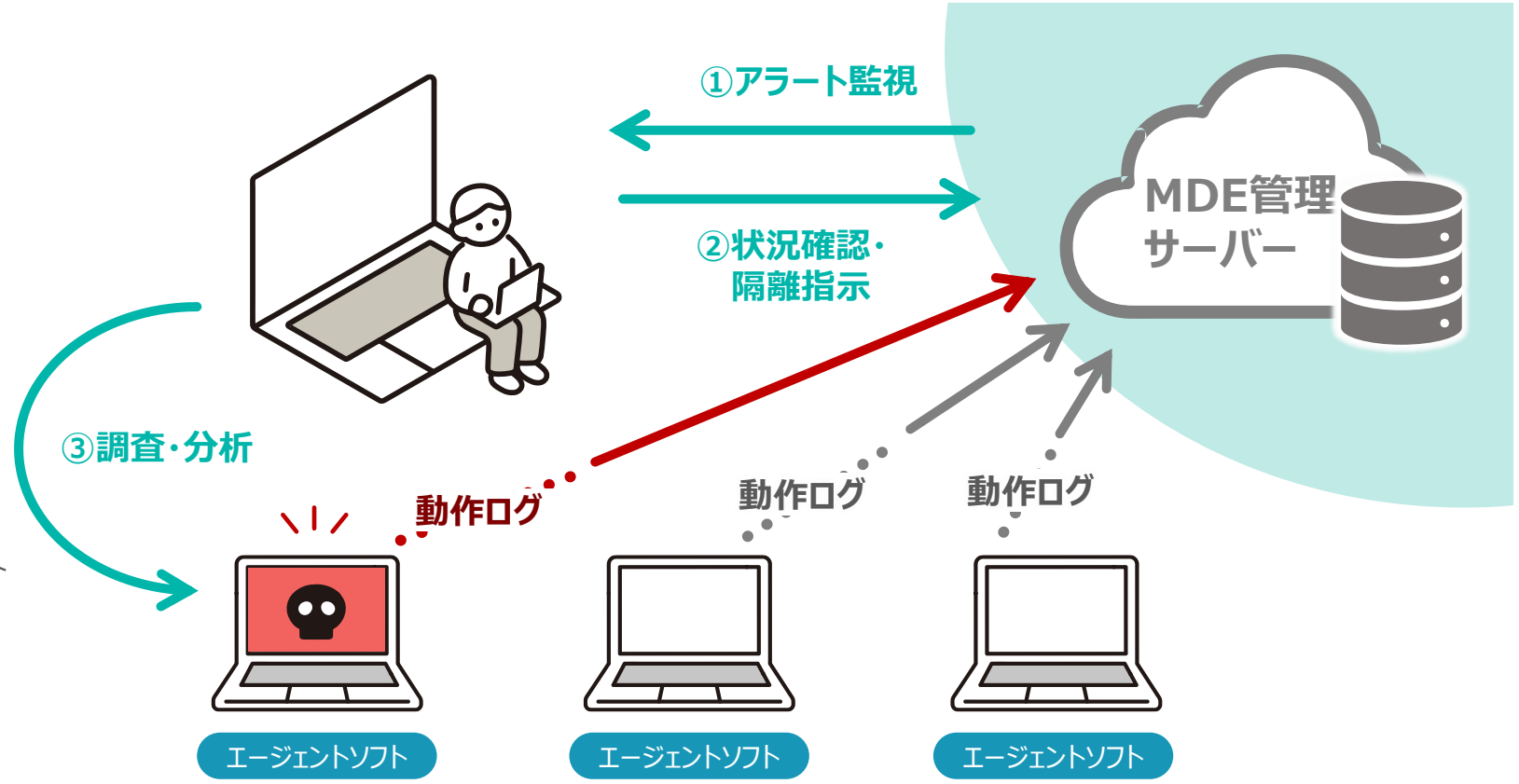
端末セキュリティ(MDE)

端末セキュリティ(MDE)－機能のご紹介－

■ IT管理者の目が届かない環境でも、端末のふるまいを監視し、有事にはリモートで論理抜線することが可能
└ 論理抜線ができるようになることで、万が一のマルウェア感染時の被害拡大を防止
└ 動作ログだけでなく端末の構成情報も取得しているので、パッチ未適用端末の特定も可能

POINT

- ふるまい検知機能により高度化している攻撃への対応が可能
- 管理者によるPCのNWからの切り離しが可能となるためインシデントの早期対処が可能



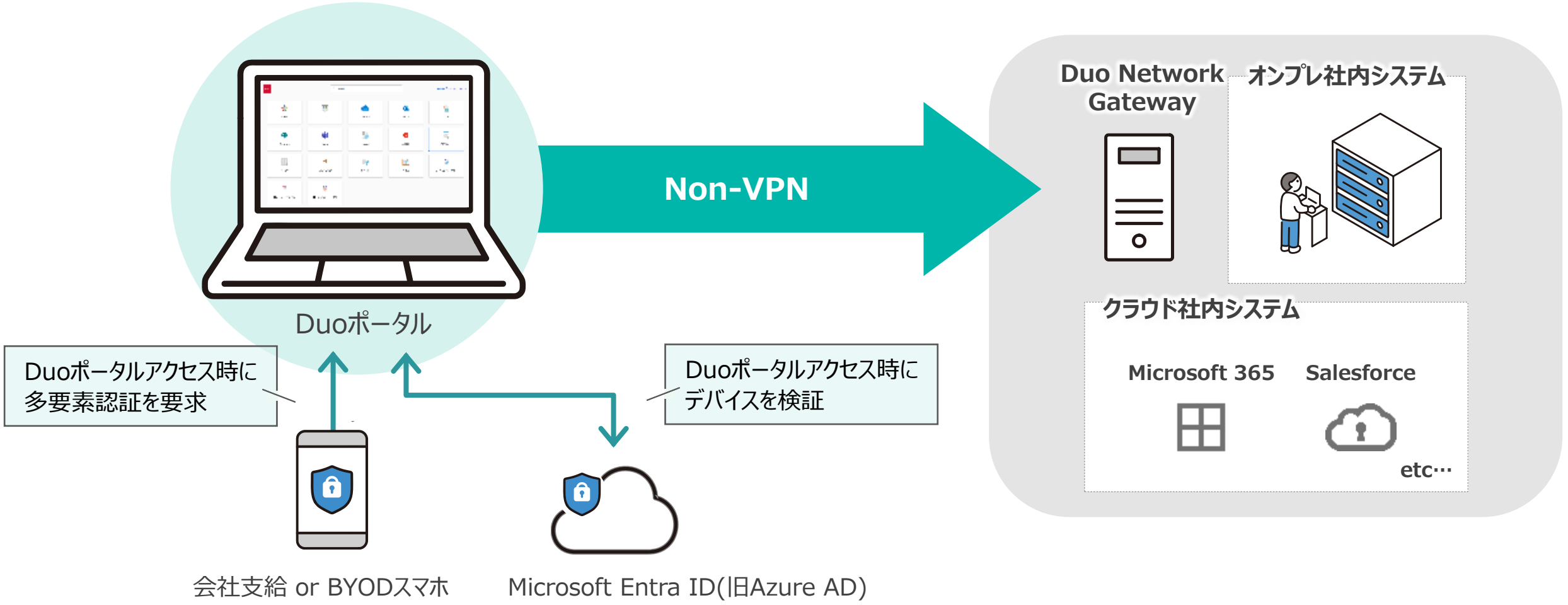
端末セキュリティ(MDE)－導入支援サービスのご紹介－

導入支援サービス範囲

作業項目	作業担当	作業内容
テナント作成	お客様	Entra ID(旧Azure AD)およびMicrosoft Defender for Endpointのテナントを作成する
オンボードスクリプト準備	お客様	試験用端末のMicrosoft Defender for Endpointを有効化するためのスクリプトを取得する
Entra ID(旧Azure AD)テナント設定	お客様	以下を実施する -多要素認証無効化 -SOCユーザの招待 -SOCユーザのグループ作成
Microsoft Defender for Endpoint テナント設定	お客様	以下を実施する -利用機能の有効化 -ロールの作成とSOCグループへのロール割り当て
導入端末先行試験	お客様 当社	オンボードスクリプトを用いて先行試験用端末のMicrosoft Defender for Endpointを有効化し、以下試験を行う -アラート受信テスト -論理抜線テスト
端末でのオンボード	お客様 (管理者 or エンドユーザ)	オンボードスクリプトやグループポリシー、Intune等を用いて、エンドユーザの端末上でMicrosoft Defender for Endpointを有効化する

社内システムアクセスセキュリティ

- IDaaS<Entra ID(旧Azure AD)> + Identity-Aware Proxy + MFA(Cisco Duo)で社内システムにセキュアにアクセス
  - VPNを張らずに社内システムにアクセス可能
  - 多要素認証の要求と、アクセス時のデバイスの検証により、悪意のある第三者によるアクセスを防止



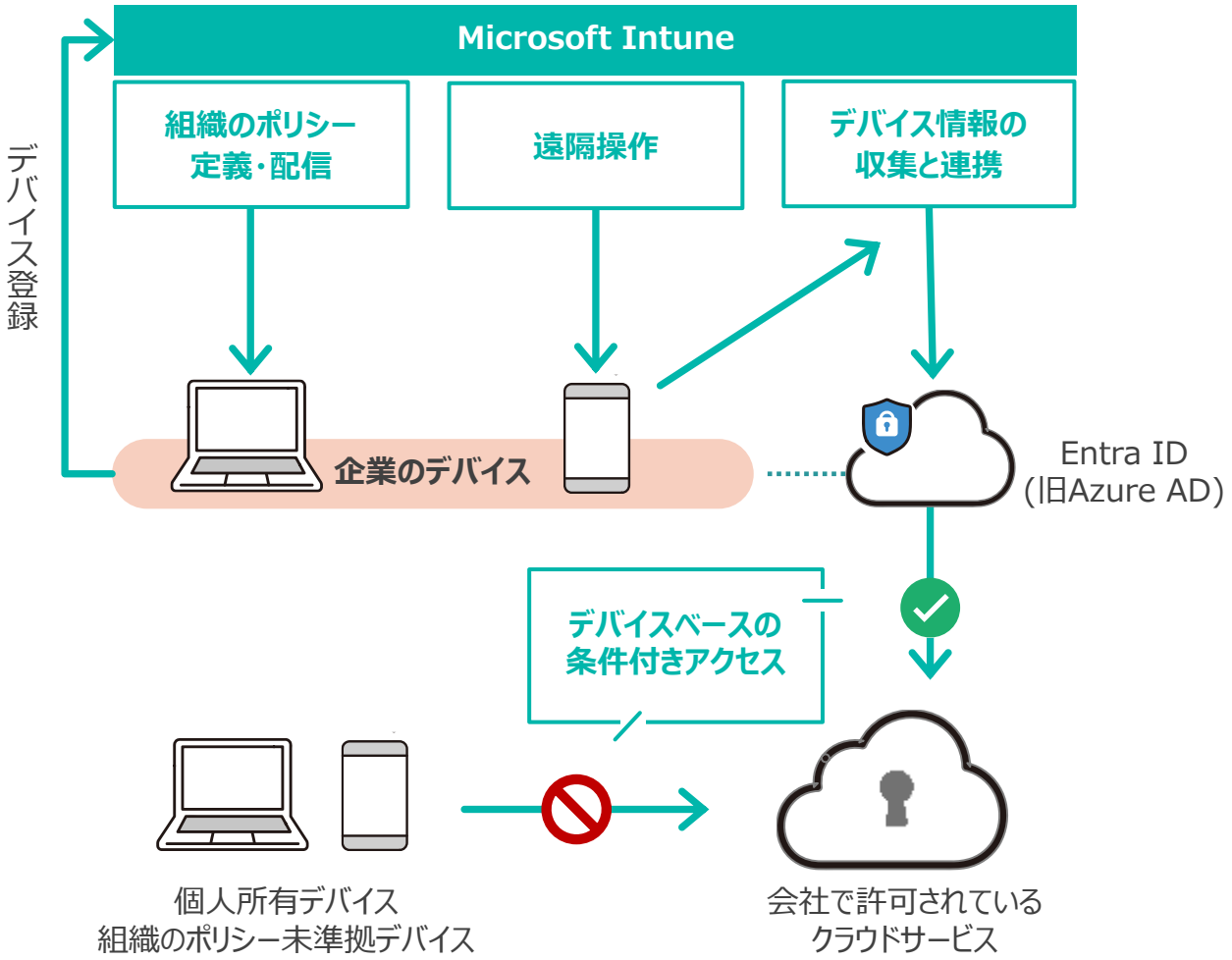
作業項目	作業内容
ヒアリングシート説明	初期設定に関するヒアリングシートを提示し、内容について説明する
Duo管理画面設定	Duo管理画面にてアカウント、ポリシー、アプリケーション、ユーザ、シングルサインオンに関連する設定を実施する
Duo Network Gateway (DNG)インストール	お客様準備のオンプレミスサーバ、もしくはAmazon Web Services(AWS)上のサーバにDNGをインストールする
DNG管理画面設定	DNG管理画面にてDNGへのシングルサインオンやDuo経由でアクセスする社内システムに関連する設定を実施する
Microsoft Entra ID(旧Azure AD) 連携設定	Duo管理画面でMicrosoft Entra ID(旧Azure AD)をアプリケーション追加するとともにMicrosoft Entra ID(旧Azure AD)側の操作手順書を提供する
設定後の試験	上記各種設定が正しく行われているか試験する
チューニング	お客様の動作確認試験の結果、設定に問題がある場合は設定を修正する

注：Duo Network Gateway(DNG)をインストールするサーバ(オンプレorAWS)の準備、
および、DNG ⇔ お客様社内LAN間のネットワーク構築はお客様にて実施いただく前提となります。

端末セキュリティ(Intune)

端末セキュリティ(Intune)－機能のご紹介－

■ Microsoft Intuneを利用し、企業のデバイスを登録することで、組織のポリシーに沿った
デバイスの管理・運用が可能となりリモートワーク環境におけるリスクを低減させることができる



組織のポリシー定義・配信
(MDM：Mobile Device Management)

- Windowsデバイスの設定を強制
- Windowsデバイスの更新プログラムを管理
- Windowsデバイスの自動キッティング
- Windows/iOS/Androidデバイスにアプリケーションを配布
  (MAM：Mobile Application Management)
- iOS/Androidデバイスのアプリ間のデータ共有を制限

遠隔操作

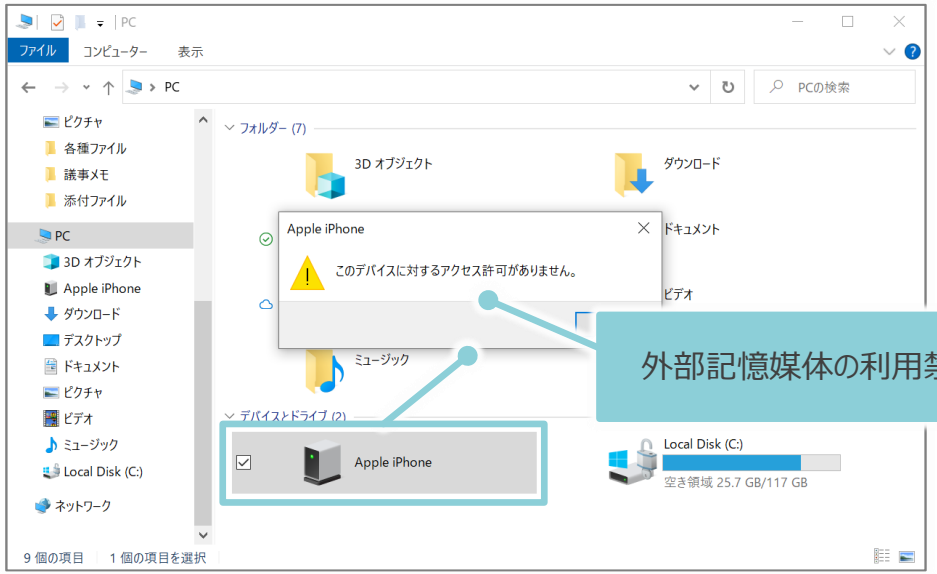
- デバイス紛失時に遠隔でデータ消去
- iOS/Androidデバイスで長期間未使用時に組織データを消去

デバイス情報の収集と連携/デバイスベースの条件付きアクセス

- Windows/iOS/AndroidデバイスのOSバージョンに応じた
  クラウドサービスへのアクセス制御
- 個人所有デバイスのクラウドサービスへのアクセス拒否
- クラウドサービスへのアクセス時に多要素認証を強制

組織のポリシー定義・配信 –(MDM)Windowsデバイスの設定を強制 –

リモートデスクトップを
無効にすることを強制



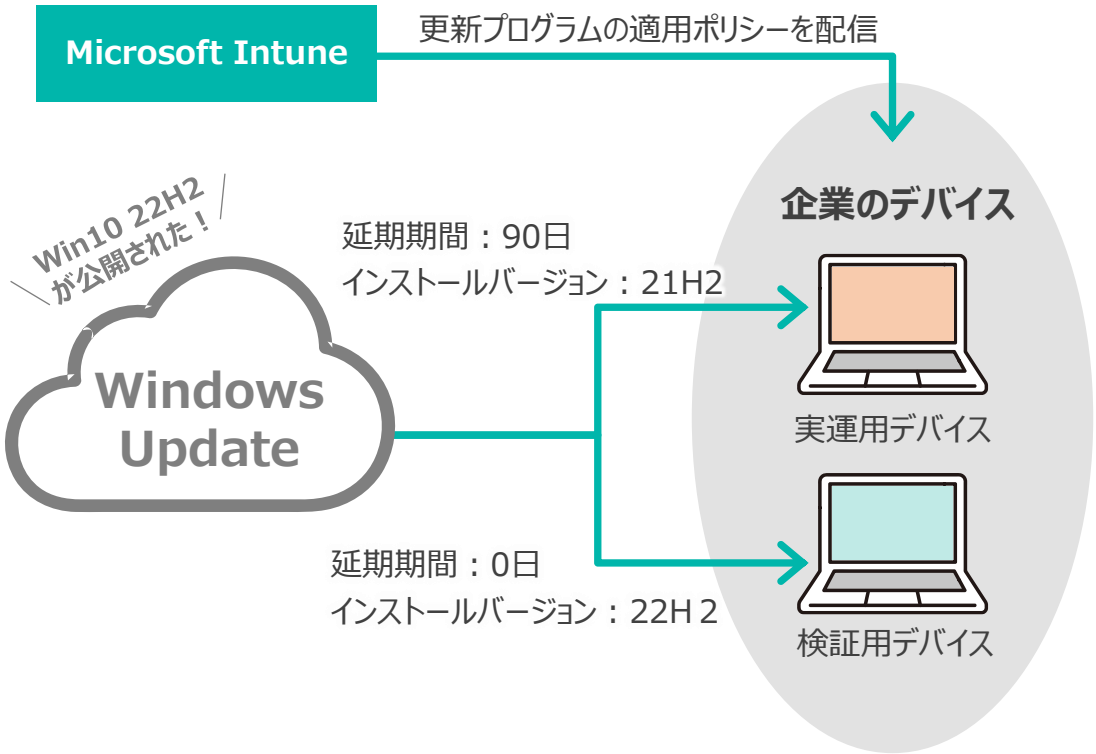
外部記憶媒体の利用禁止

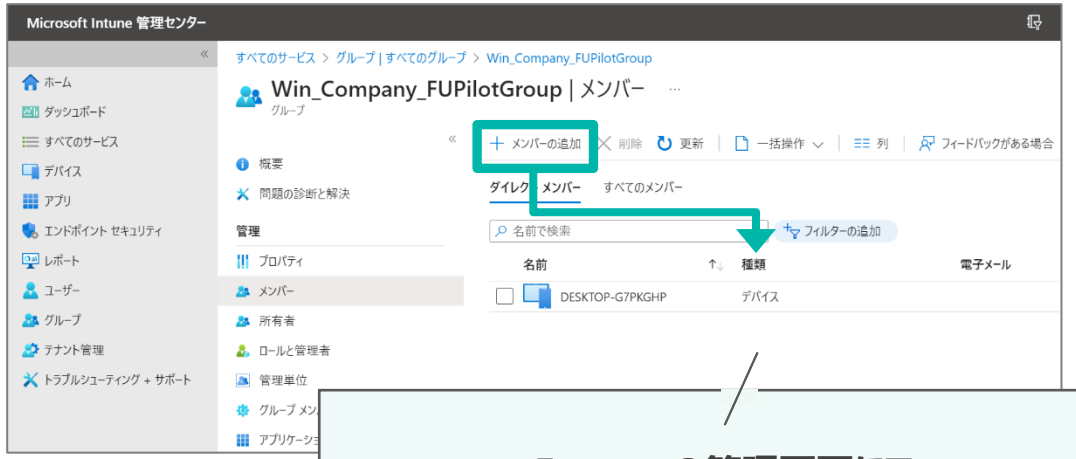
プリンタの追加を禁止

Windows Defenderの
設定を強制

組織のポリシー定義・配信 –(MDM)Windowsデバイスの更新プログラムを管理–

- WindowsデバイスのOSのバージョンの統制をとるために、更新プログラムの管理をすることが可能
  - エンドユーザの誤操作により、IT担当者がサポートできない、あるいは意図しないバージョンになることを防止
  - 更新プログラムが公開されたのち、一部のデバイスにて先行で検証してから、実運用デバイスに配布可能





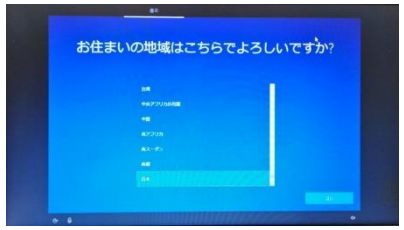
Intuneの管理画面にて
所定のグループにデバイスを追加することで
簡単に検証用デバイスとすることが可能

組織のポリシー定義・配信 –(MDM)Windowsデバイスの自動キッティング–

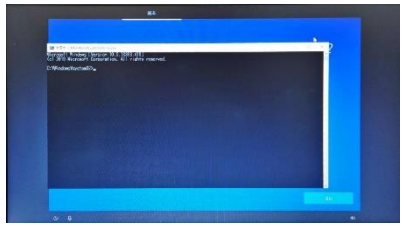
■ 企業のIT管理者が、工場出荷状態のデバイスをIntuneに登録するだけで自動キッティングが可能

IT管理者側の作業

- 端末の電源をON



- コマンドプロンプト起動



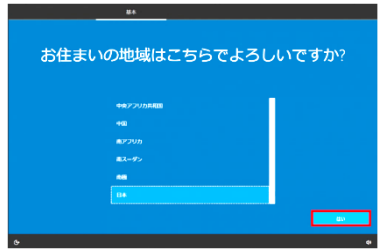
- 右記コマンドを実行

```
PowerShell.exe -ExecutionPolicy Bypass
Install-Script -name Get-WindowsAutopilotInfo -Force
Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
Get-WindowsAutoPilotInfo -Online
```

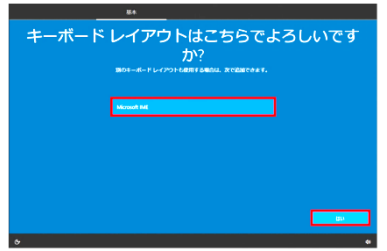
- グローバル管理者でM365にログイン
- Intuneへのデバイス登録完了

利用者側の作業

- 端末の電源をON



- 地域・キーボード等の設定



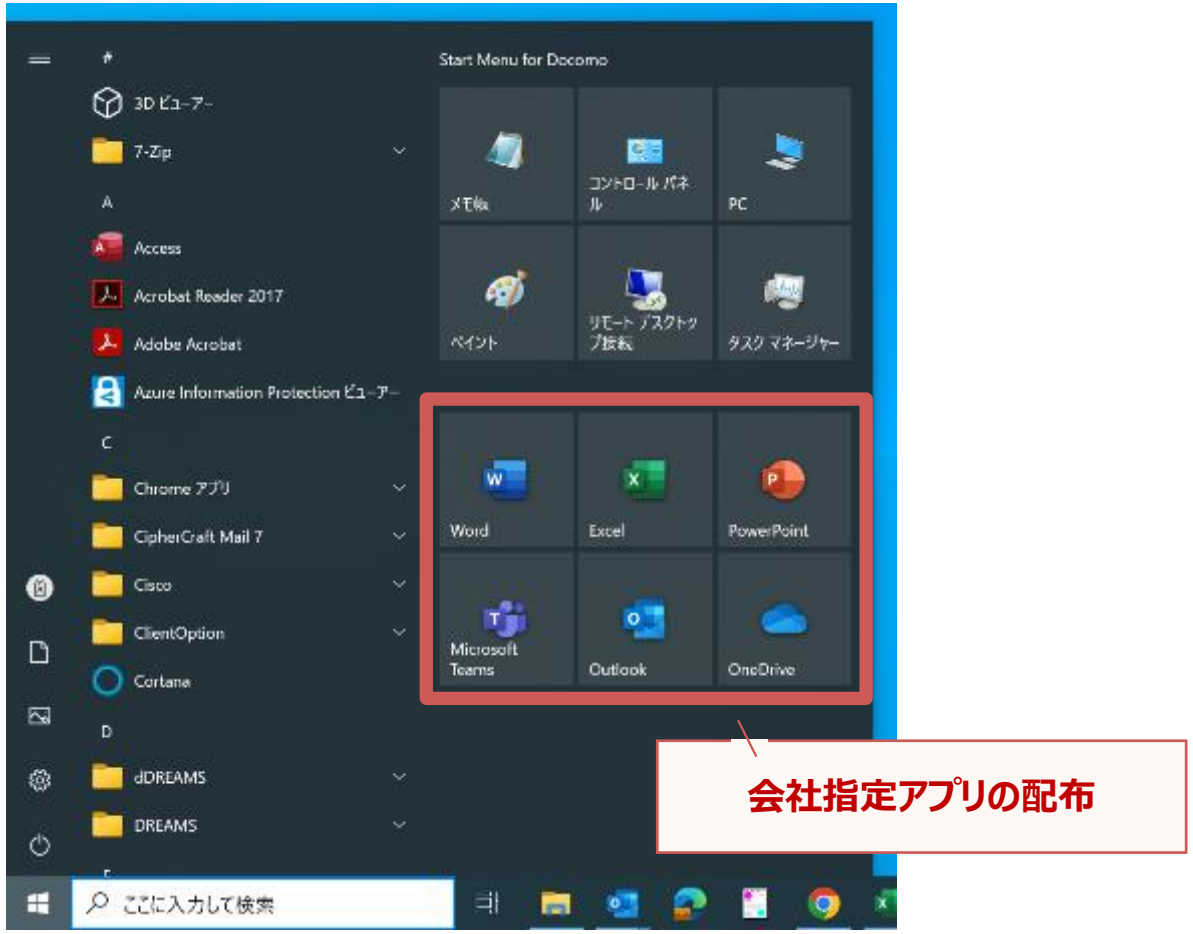
- M365アカウントで
  デバイスにログイン

- 1時間程度端末を放置
- 初期セットアップ完了

■ 会社貸与端末で利用アプリケーションを配布することが可能（Microsoft系以外のアプリケーションも配布可能）

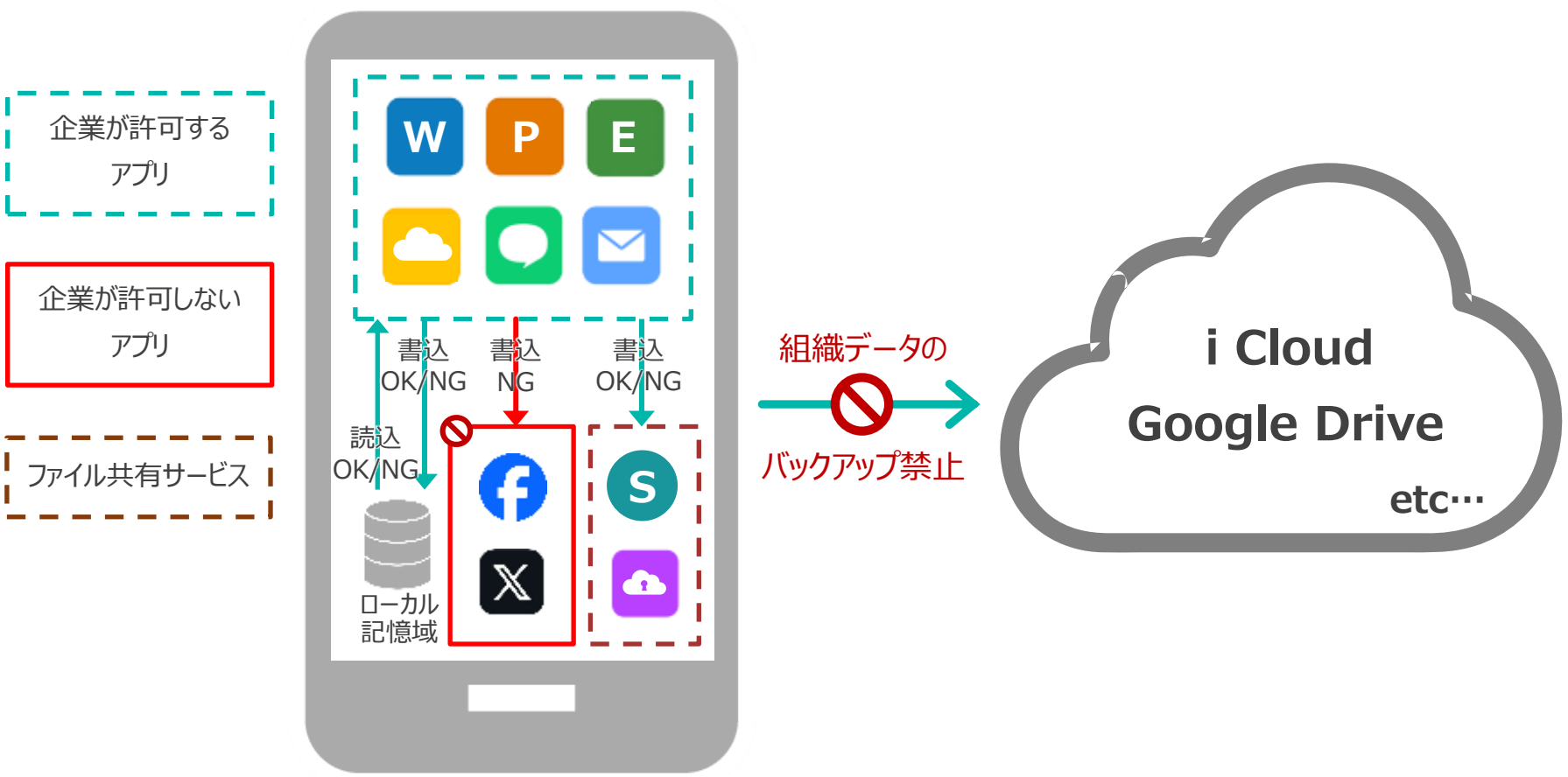
iOS

Windows



組織のポリシー定義・配信 –(MAM) iOS/Androidデバイスのアプリ間のデータ共有を制限–

- デバイスのローカル記憶域(HDD、SDカード等）への組織データの保存を制御可能
- 企業が許可しないアプリケーションに、組織データを書き込むことを禁止
- SharePointやbox等、企業データの保存先とするファイル共有サービスを制御
- 組織データのGoogleドライブ/iCloudへのバックアップ禁止

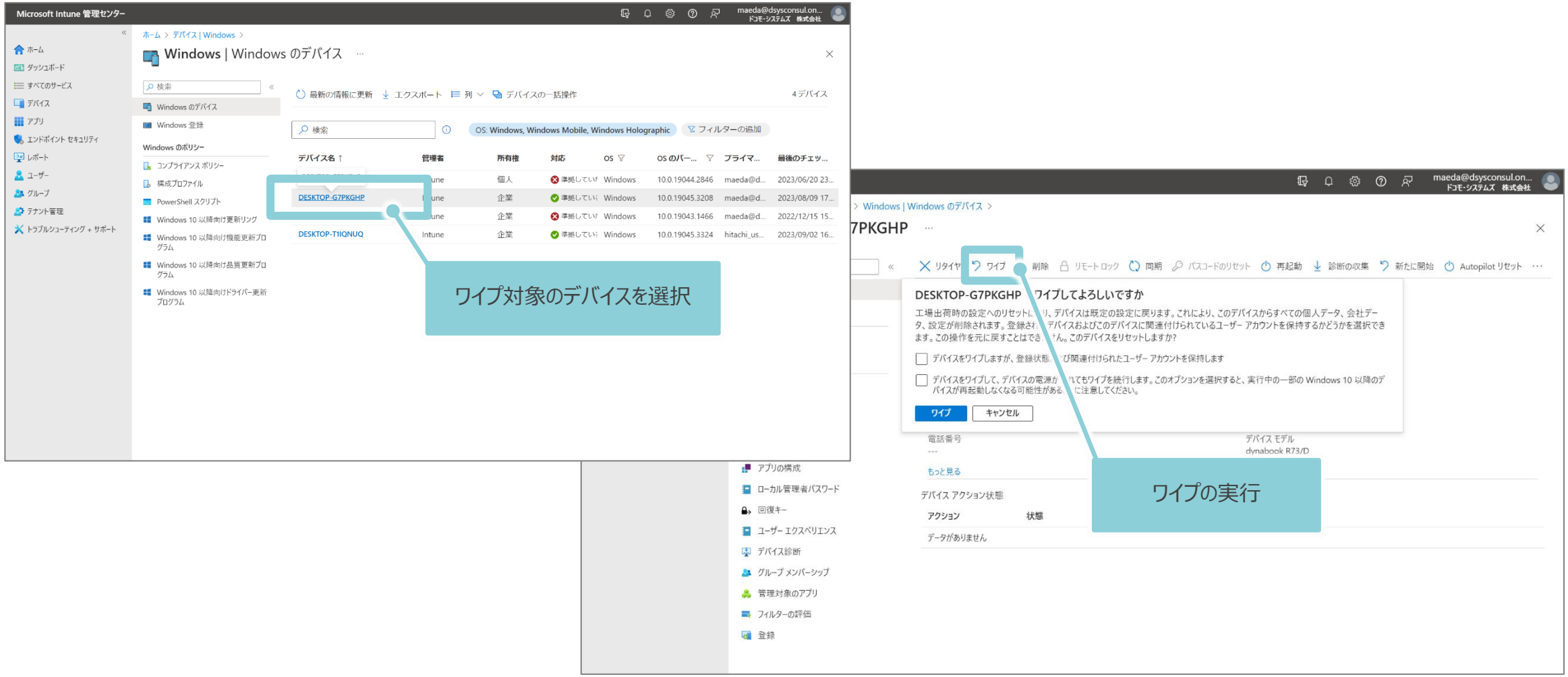


組織データのファイルをローカル記憶域に
保存した際のエラー

組織データのExcelからテキストをコピーし
Yahooの検索ボックスに張り付けた際のエラー

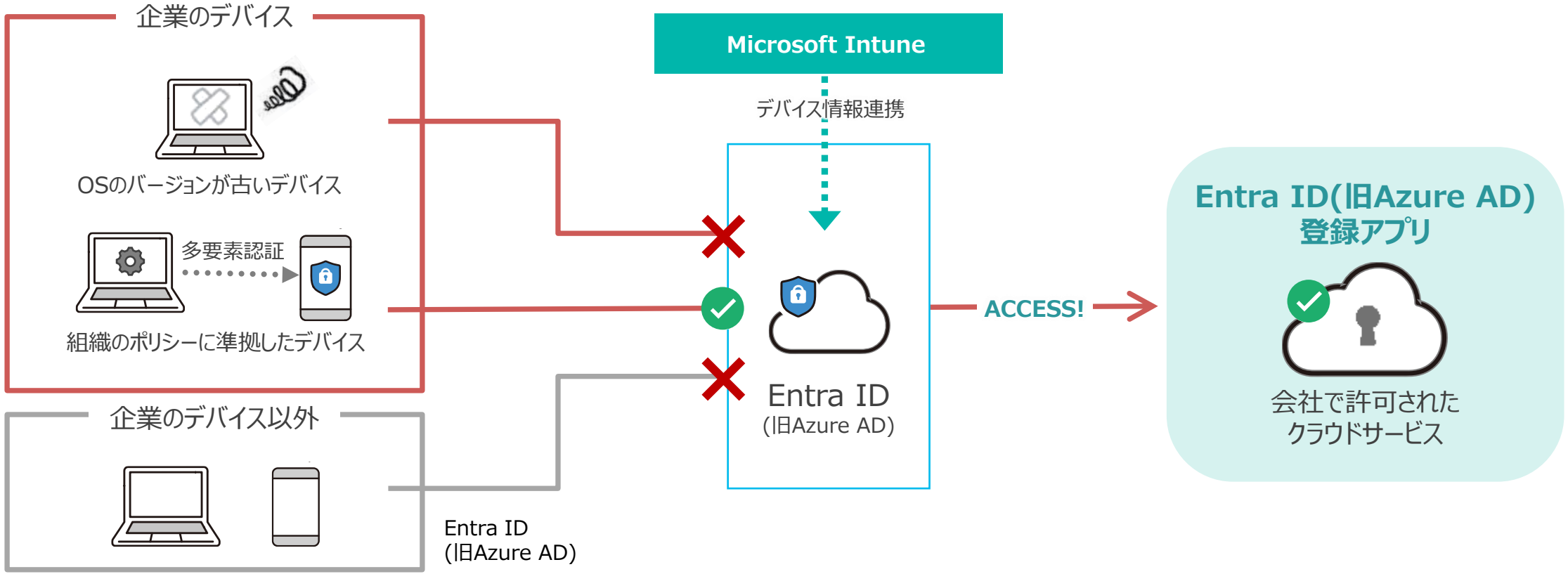
遠隔操作

- Microsoft Intune管理センタにて対象デバイスを選択し、ワイプを実行することができる
- 長期未使用のiOS/Androidデバイスに対して、期日を設定して自動的に組織データを削除することも可能



デバイス情報の収集と連携/デバイスベースの条件付きアクセス

- Microsoft IntuneとEntra ID(旧Azure AD)を連携させることにより、デバイスの情報を元にしたクラウドサービスへのアクセス制御が可能となる
- Entra ID(旧Azure AD)に登録したアプリケーションに対して以下のようなアクセス制御が可能
  - OSバージョンによる、アクセス制御（ex.Win10 バージョン22H2以上はアクセス可能、iOSバージョン16以上はアクセス可能）
  - 企業のデバイスであるか否かでのアクセス制御
- Entra ID(旧Azure AD)に登録したアプリケーションにアクセスする際に多要素認証を求めることが可能



端末セキュリティ(Intune) 導入支援サービスのご紹介

作業項目	作業内容
ヒアリングシート説明	初期設定に関するヒアリングシートを提示し、内容について説明する
アプリケーション配布設定	Windowsデバイスを対象に、本基本サービスの利用に必要となるアプリケーションや、お客様指定のアプリケーションの配布設定をするiOS/Androidデバイスを対象に、お客様指定のアプリケーションの配布設定をする
デバイス構成プロファイル設定	Windowsデバイスを対象に、端末のセキュリティ対策向上のためのデバイス構成管理設定をする
アプリ保護ポリシー設定	iOS/Androidデバイスを対象に、組織データを保護するための各アプリケーションの動作設定をする
更新リング/機能更新プログラム設定	Windowsデバイスを対象に、Windows OSの更新プログラムの配布設定をする
コンプライアンスポリシー設定	Windows/iOS/Androidデバイスを対象に、不正なデバイスの利用を防ぐためのポリシー設定をする
条件付きアクセス設定	Windows/iOS/Androidデバイスを対象に、クラウドサービスへのアクセス時のポリシー設定をする
エンドポイントセキュリティ設定	Windowsデバイスを対象に、Windows Defenderの動作設定をする
Autopilot設定	Windowsデバイスを対象に初期出荷状態の端末の自動キッティングの設定をする
その他設定	iOSデバイスを管理するためのMDMプッシュ証明書等、Intuneを利用するための各種設定をする
設定後の試験	上記各種設定が正しく行われているか試験する
チューニング	お客様の動作確認試験の結果、設定に問題がある場合は設定を修正する

運用支援

運用支援サービスのご紹介

■ 当社のSOCが、お客様に成り代わって必要なセキュリティ運用を実施
■ 運用上発生した問題、カスタマイズ要望等にも当社技術担当が対応

● SOCによるセキュリティ運用支援

項目	運用内容	対応日時 /対応頻度
アラート解析	Microsoft Defender for Endpoint、Cisco Umbrellaのアラートを解析し、過検知/誤検知判断をする	営業日の 10:00-17:00
アラート対処	アラート解析の結果、過検知/誤検知でなかった場合は論理抜線、アラート内容の解析、アクセスログ調査、ブロックリスト追加等の対応を行う	
アラート通知	アラートの内容や、対処内容、推奨対応事項等についてお客様管理者に通知する	
自動論理抜線	お客様との事前の取り決めに応じて、Microsoft Defender for EndpointのHighアラートの発生後、60分以内に自動的に論理抜線する	全日 (24時間)
論理抜線解除	お客様の申告を元に論理抜線を解除する	営業日の 10:00-17:00
ブロックリスト追加	SOCが独自に悪性の宛先の情報を入手した場合に、Cisco Umbrellaのブロックリストを追加する	営業日の 10:00-17:00
定期レポート	月1回、セキュリティ運用状況レポートを作成し、お客様管理者に送付する	毎月1回

● 技術担当による運用支援

問い合わせ対応等 依頼種別	有償 /無償	対応例
本サービスの仕様に関するお問合せ	無償	–
SOCセキュリティ運用の対応内容に関するお問合せ	無償	–
上記以外の各種お問合せ	有償 ※	特定のWebサイトやアプリケーションが利用できない等、本サービスが原因と推測される事象の原因調査と対応
本サービス導入後の各種設定変更	有償 ※	本サービスにてテンプレート化されている、ドコモグループのノウハウに当てはまらない、個別のカスタマイズ設定の対応 Ex. - Umbrellaのポリシーを部署毎に分けたいので、新規でポリシーを作成してほしい - USBメモリを一時的に許可してほしいのでIntuneの設定変更をしてほしい

※ご依頼をいただいた都度、消費チケット数をお見積りし、お客様に消費チケット数の合意を得た上で対応を実施いたします

まずはお問い合わせください

まずは公式サイトからお問い合わせください。弊社の営業担当者がお客様をサポートさせていただきます。

https://www.nttcom.co.jp/dscb/zerotrust/

QRからも
読み込めます

忙しいあなたに
安心の毎日を、
コムウェアの
ゼロトラストで。