コロナに負けるな!! Microsoft 365 で DX

本セミナーは、中堅・中小企業の皆様の DX (デジタル トランスフォーメーション) を推進するための具体的な IT 活用方法を、Demo も交えてご紹介するセミナー 9 回シリーズのひとつです。
各回単独ご視聴でも価値がありますが、シリーズでご視聴いただくことで、Microsoft 365 を活用して、コロナに負けずにご一緒に DX を進めていただくことができます。

回	レベル	セミナー タイトル	対応ソリューション
1	初級	リモートワークに最適！ Microsoft Teams のオンライン会議	Microsoft 365 Business Basic (Office 365 E1)
2		Microsoft Teams の真の実力 1 (チームとチャネル)	
3		Microsoft Teams の真の実力 2 (ファイル共有、アプリ活用、電話活用)	
4	中級	Microsoft 365 によるインテリジェントなドキュメント作成	Microsoft 365 Business Standard (Office 365 E3)
5		Microsoft Teams × アプリによる業務効率化	
6		アプリとワークフロー活用によるペーパーレス化	
7	上級	安全・安心の Windows 10 と標的型メール攻撃対策	Microsoft 365 Business Premium (Microsoft 365 E3)
8		デバイスの簡単な導入と安全の確保	
9		今こそ Microsoft 365 でゼロ トラスト ネットワーク	

※ セミナー タイトルは変更される場合がございますので、ご留意ください。

ご注意

- 本資料の画面や仕様、URL などは、資料作成時点のものです。
- クラウド サービスのため、画面や仕様、URL などは変更されている場合がございますのでご注意ください。

第 9 回
今こそ Microsoft 365 で
ゼロ トラスト ネットワーク

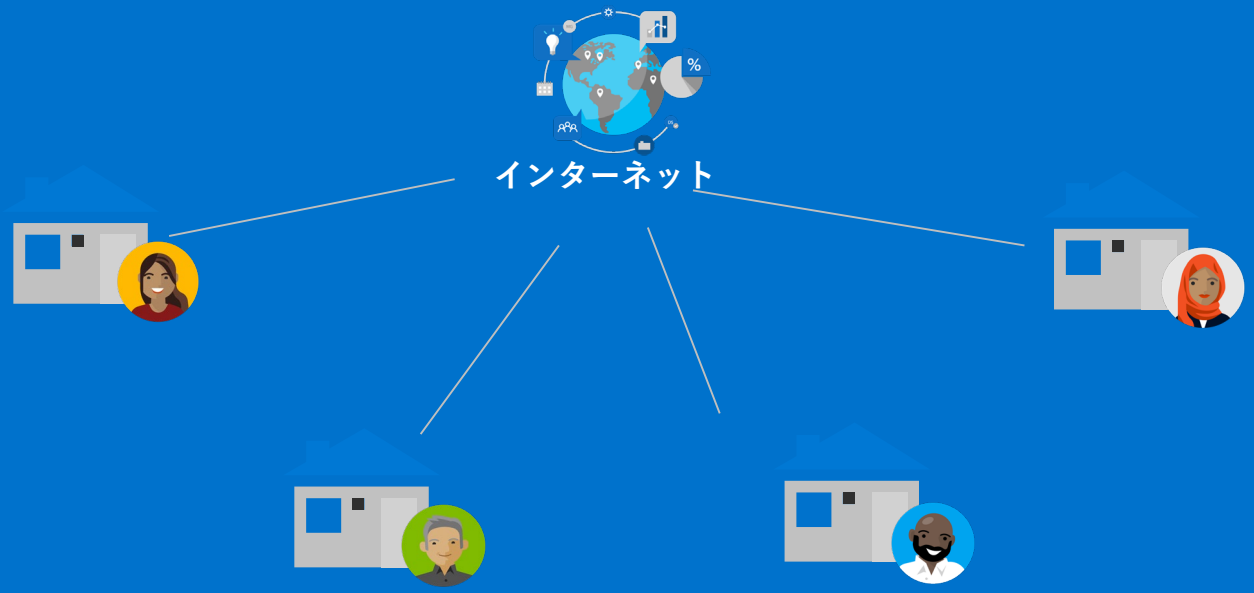
本日の内容

- 課題認識
- ゼロトラスト ネットワーク セキュリティとは
- ゼロトラスト ネットワーク に基づいたセキュリティ対策のメイン
- Microsoft 365 とは

課題認識

直面している IT 環境の課題

従業員が分散してリモートで働いている環境下でも、常につながり、生産性を保てるようにすると共に、サイバー脅威やデータ損失からビジネスを守らなければなりません



在宅勤務の従業員

多くの個人用モバイル デバイス

COVID-19 に便乗した
フィッシングと
ランサムウェアの増加

COVID-19 に関連したサイバー攻撃が増加

悪意のあるサイバー集団が COVID-19 を悪用

「...サイバー犯罪グループは、個人、中堅中小企業、大企業を標的に COVID-19 に関連したフィッシング詐欺やフィッシング メールを仕掛けています」

-米国国土安全保障省、2020 年 4 月 8 日、CISA Alert (AA20-099A) (英語)

サイバー攻撃が 5 倍に増加、WHO は警戒を促す

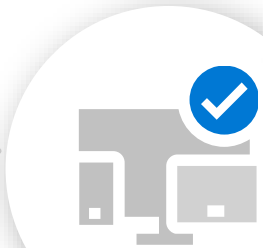
「COVID-19 の感染爆発が始まって以来、WHO スタッフに対するサイバー攻撃や一般市民を標的としたフィッシング メールの件数が劇的に増加しています」

世界保健機関、2020 年 4 月 23 日のニュース リリース (英語)

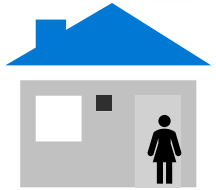
在宅勤務への移行がもたらす疑問と課題

増加するフィッシング攻撃から従業員を保護するにはどうすればよい?

従業員が使用するデバイスの安全を確保するには?



従業員が自宅から必要不可欠なオンプレミスアプリにアクセスできるようにするには?



機密データが個人用デバイスに残らないようにするには?

Gartner®

マイクロソフトのセキュリティ ― ガートナーの 5 つのマジック クアドラントでリーダーの評価を獲得

アクセス
管理

Cloud Access
Security Broker

エンタープライズ情報
アーカイブ

エンドポイント
保護プラットフォーム

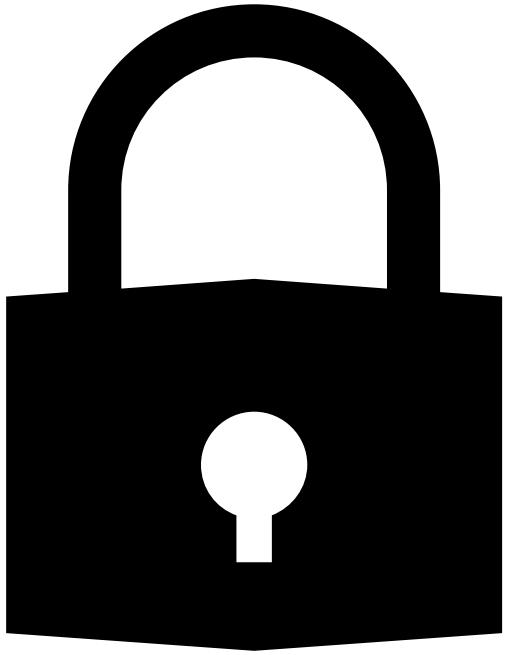
統合エンドポイント
管理ツール

*Gartner『Magic Quadrant for Access Management』、Michael Kelley、Abhyuday Data、Henrique、Teixeira、2019 年 8 月
*Gartner『Magic Quadrant for Cloud Access Security Brokers』、Steve Riley、Craig Lawson、2019 年 10 月
*Gartner『Magic Quadrant for Enterprise Information Archiving』、Julian Tirsu、Michael Hoech、2019 年 11 月
*Gartner『Magic Quadrant for Endpoint Protection Platforms』、Peter Firstbrook、Dionisio Zumerle、Prateek Bhajanka、Lawrence Pingree、Paul Webber、2019 年 8 月
*Gartner『Magic Quadrant for Unified Endpoint Management Tools』、Chris Silva、Manjunath Bhat、Rich Doheny、Rob Smith、2019 年 8 月

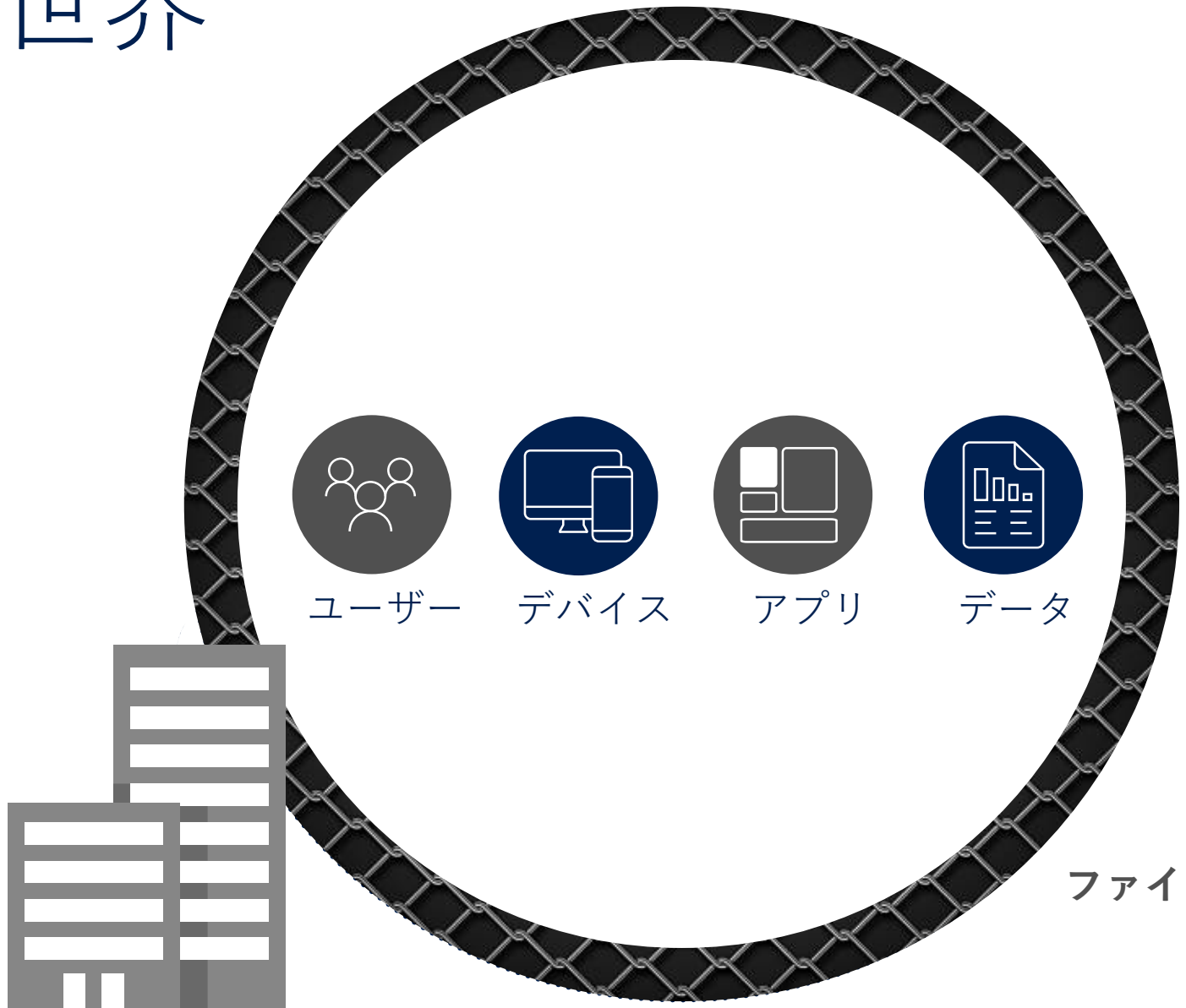
ゼロトラスト ネットワーク セキュリティとは

セキュリティ対策ベストプラクティス

- 今日のトレンドに合わせてセキュリティ対策を変えていく必要性
- マインドセットを変える必要性



従来の世界

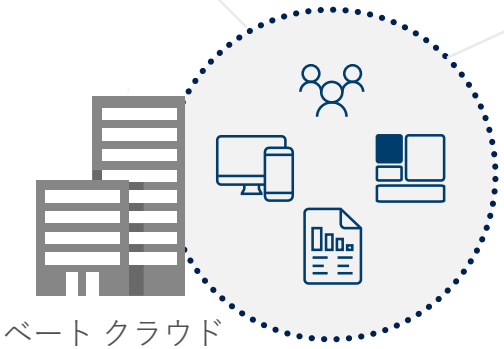


“inside is good, outside is bad”

社内は安全、社外は危険

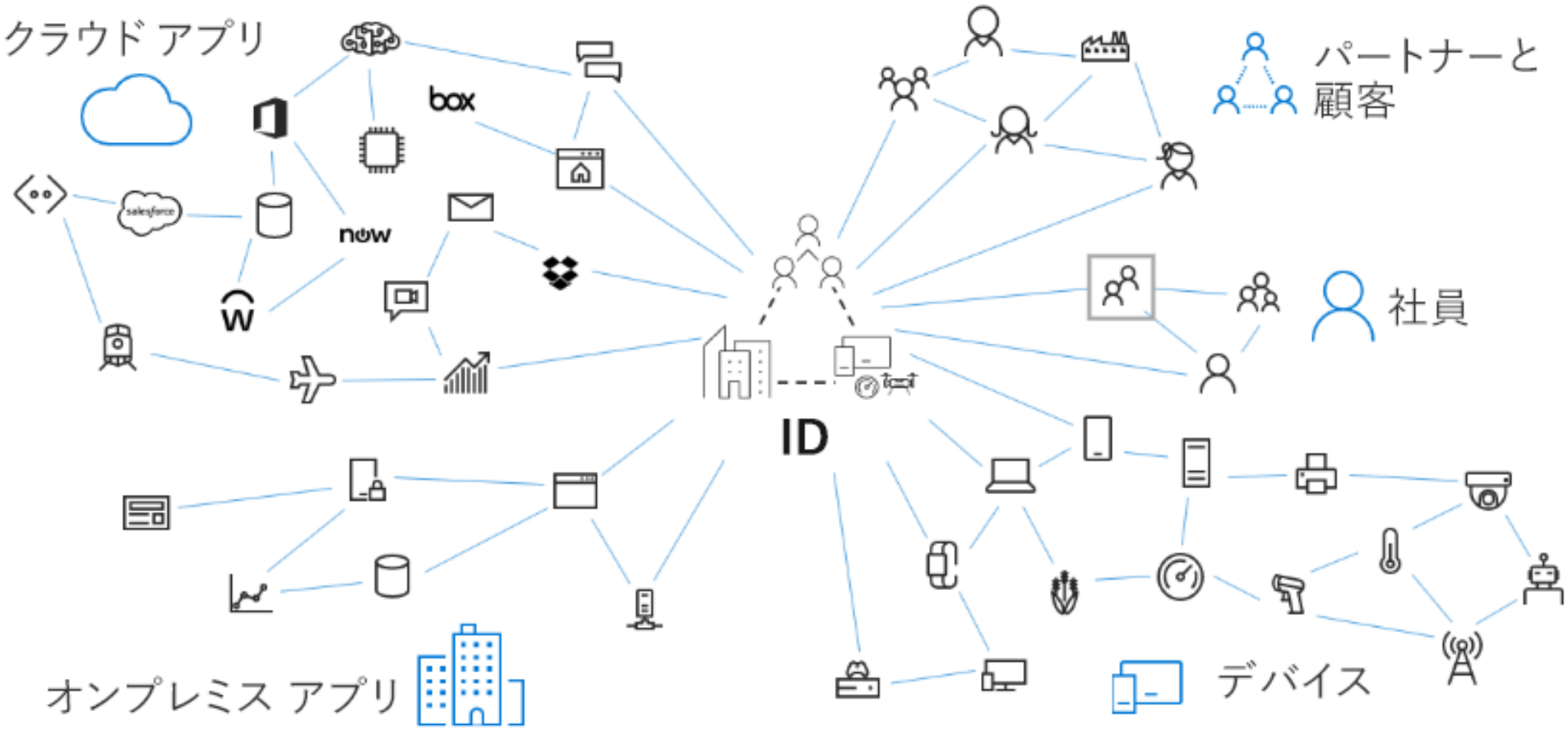
Zero Trust Security Model

ゼロ トラスト セキュリティ モデル



オンプレミス / プライベート クラウド

ID が今日の境界である

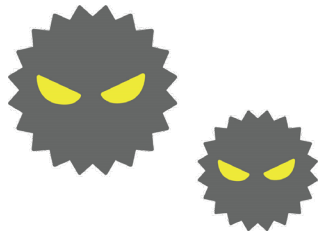


狙われる可能性のある非推奨構成

社内からは、Microsoft 365 にアクセスできるが、社外からは、Microsoft 365 にアクセスできない

しかるに、社外から Microsoft 365 にアクセスするときは、VPN で一旦社内に入ってから Microsoft 365 にアクセスする

持ち出している端末のウィルス感染などにより、社外のリスクを社内に持ち込むこととなり非常に危険	クラウド サービスが想定しない利用方法



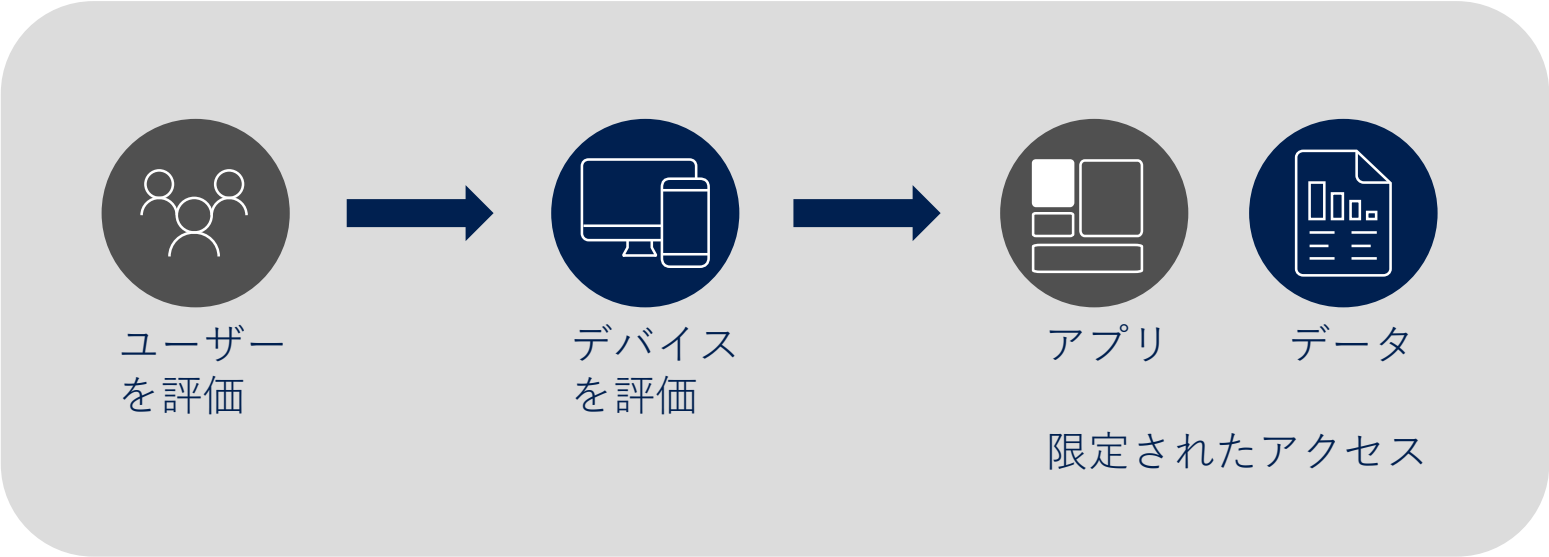
ゼロトラスト ネットワーク セキュリティ という考え方

- 基本理念
  - 場所 (社内ネットワーク) を信用する、ということをやめましょう
  - アプリケーションアクセスの正当性を常に検証しましょう

- 成り立ち
  - Forrester Research が 2010 年に提唱
  - http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
- Google 社やシスコ社のセキュリティモデルなどに代表される
  - https://cloud.google.com/beyondcorp/
  - https://www.cisco.com/c/ja_jp/products/security/zero-trust.html
- Microsoft 365 を使った実現方法のガイダンス
  - https://blogs.technet.microsoft.com/jpazureid/2018/06/29/building-zero-trust-networks-with-microsoft-365/

ゼロ トラスト セキュリティ モデル

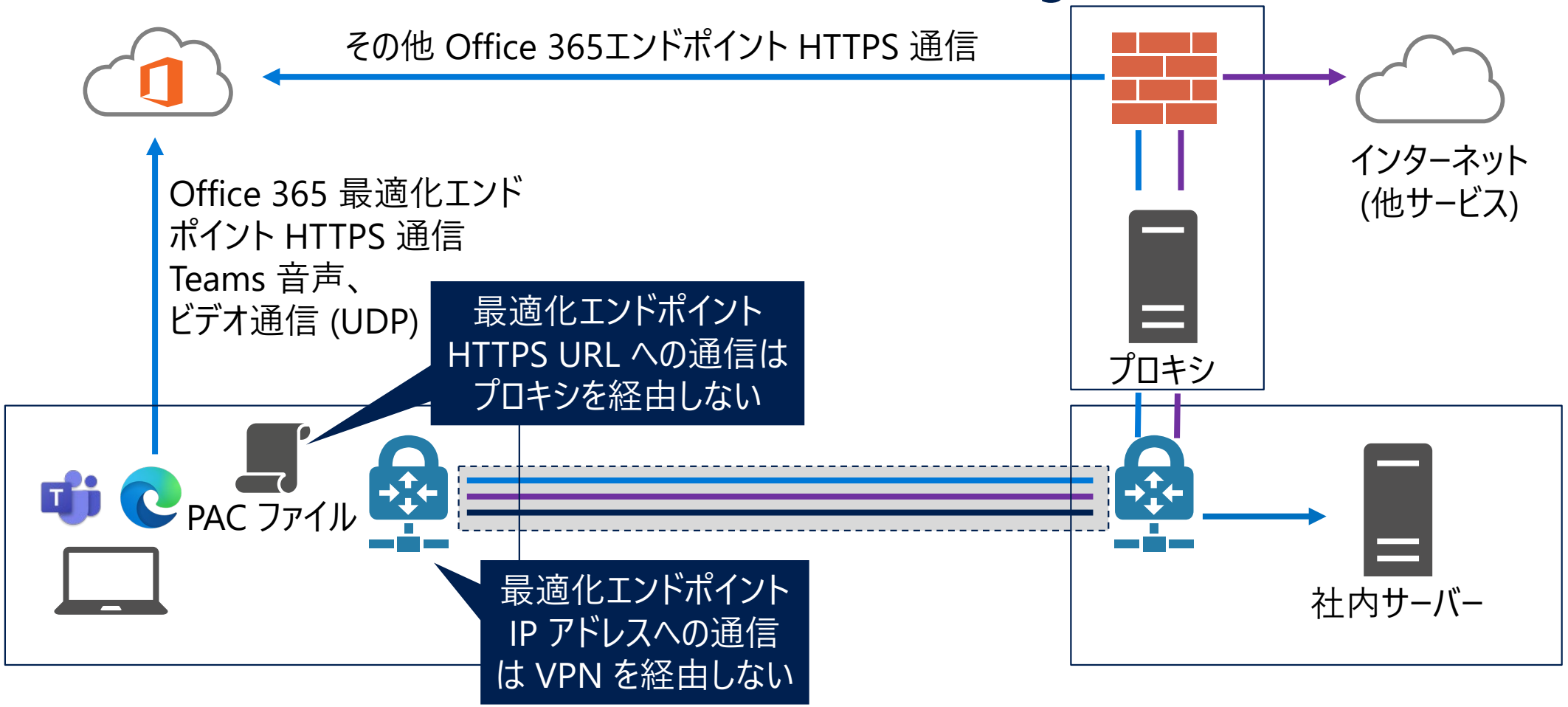
“侵入されることが前提” と考える



- ユーザーとデバイスを動的に評価
- ユーザーとデバイスに適切なポリシーを適用
- ただし、企業のデータとリソースを保護しつつ、ユーザーに生産的な環境を提供

VPN スプリットトンネリング

Microsoft Teams、SharePoint Online、Exchange Online のみ直接通信に



VPN スプリット トンネリングを使用してリモート ユーザーの Office 365 の接続を最適化する
https://docs.microsoft.com/ja-jp/office365/enterprise/office-365-vpn-split-tunnel

ゼロトラスト ネットワーク に基づいたセキュリティ対策のメイン

拡大する脅威への対応

攻撃の投資対効果を下げる 4 つのフェーズ

必要最低限の対策

セキュリティ既定値

Azure Active Directory のセキュリティ既定値は、一般的な攻撃に対して事前に構成されたセキュリティ設定が含まれ、セキュリティの実現をいっそう容易にし、組織を保護するために役立ちます。

テナントでは、次のセキュリティ構成が有効になります。

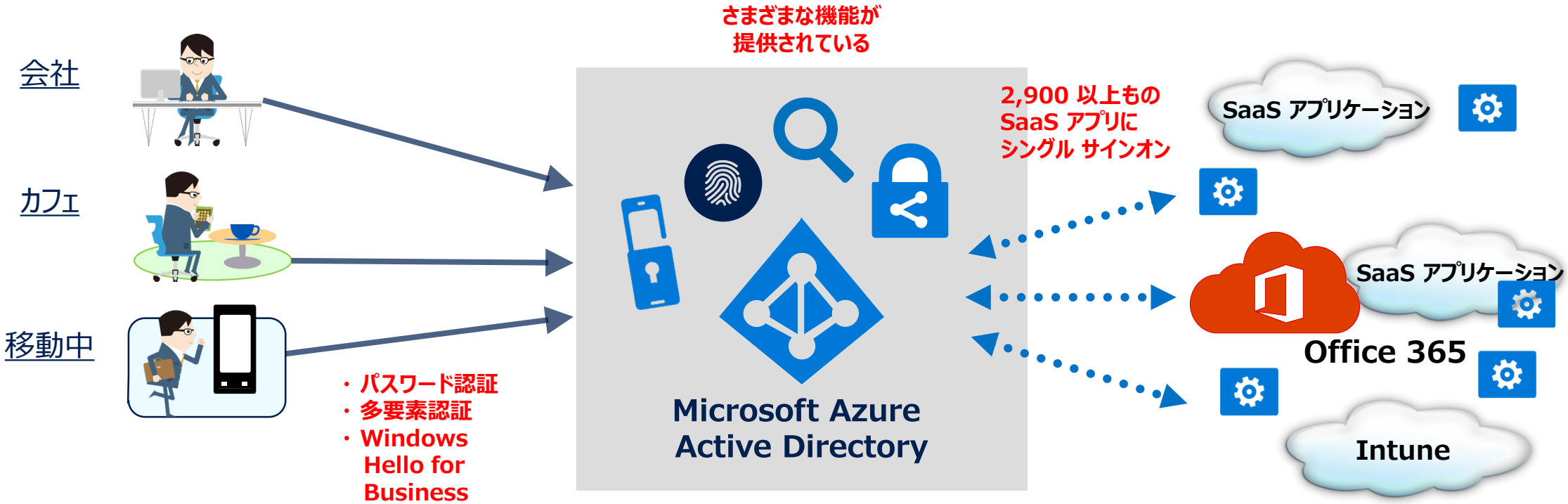
- **すべてのユーザーに対する多要素認証の登録が必須**
- **管理者に多要素認証の実行を要求**
- **ユーザーに多要素認証の実行を要求**
- **レガシ認証プロトコルをブロック**
- **特権が必要な作業を保護**

※条件付きアクセスを使用しており、環境で条件付きアクセス ポリシーを有効にしている場合、セキュリティ既定値は使用できません。

セキュリティの既定値群とは
https://docs.microsoft.com/ja-jp/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

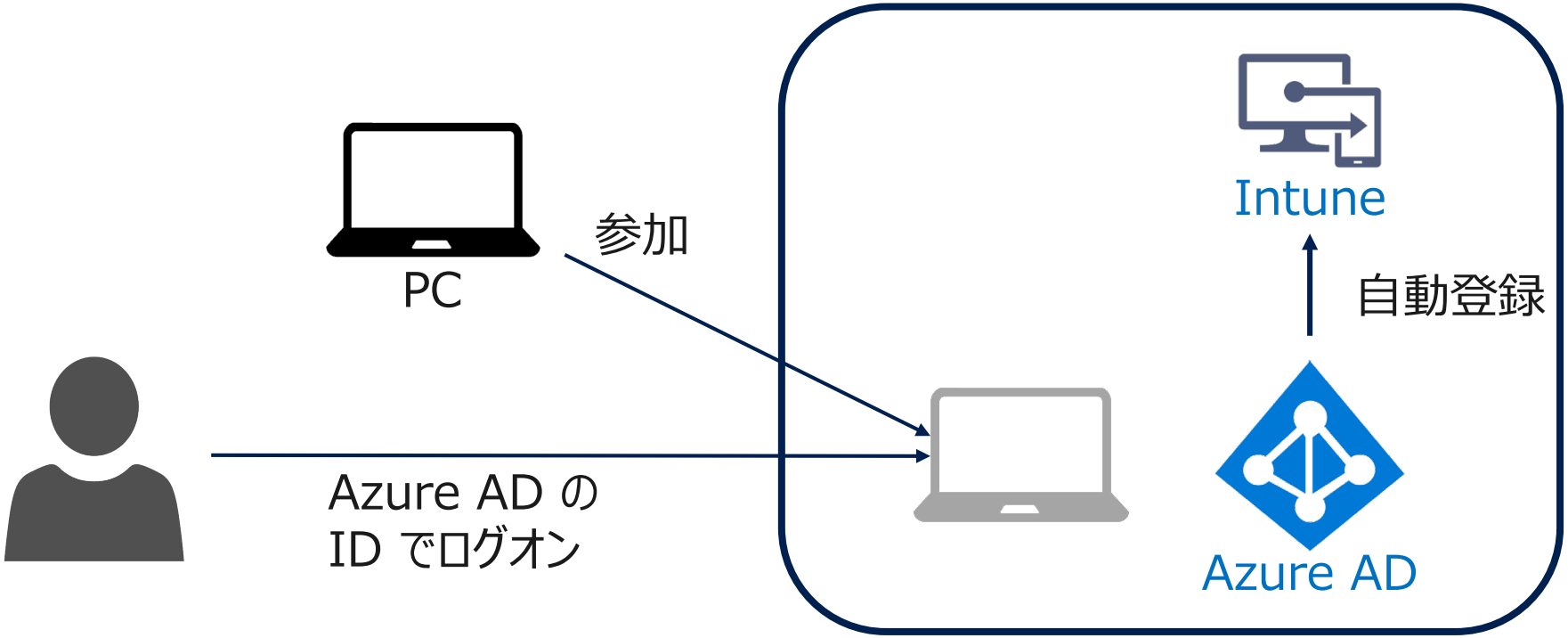
Azure Active Directory（Azure AD）とは

- マイクロソフトが提供する、マルチテナント対応のクラウド ベースのディレクトリ サービス
  - Microsoft Azure が提供するサービスの 1 つ
  - Office 365 や Intune の認証サービス
  - オンプレミス Active Directory と統合できる



Azure AD 参加

クラウドを中心とした管理を行う場合に適している
Azure AD の ID で、PC にログオン



Azure AD Premium P1 の条件付きアクセス

- 標的型攻撃の入口対策の 1 つ
- Intune を組み合わせると、デバイス ベースのアクセス制御を行える

Microsoft Intune

PC & モバイルデバイス
管理
(MDM)

モバイルアプリ
管理
(MAM)

条件付きアクセス
- ポリシー準拠
- 保護アプリ

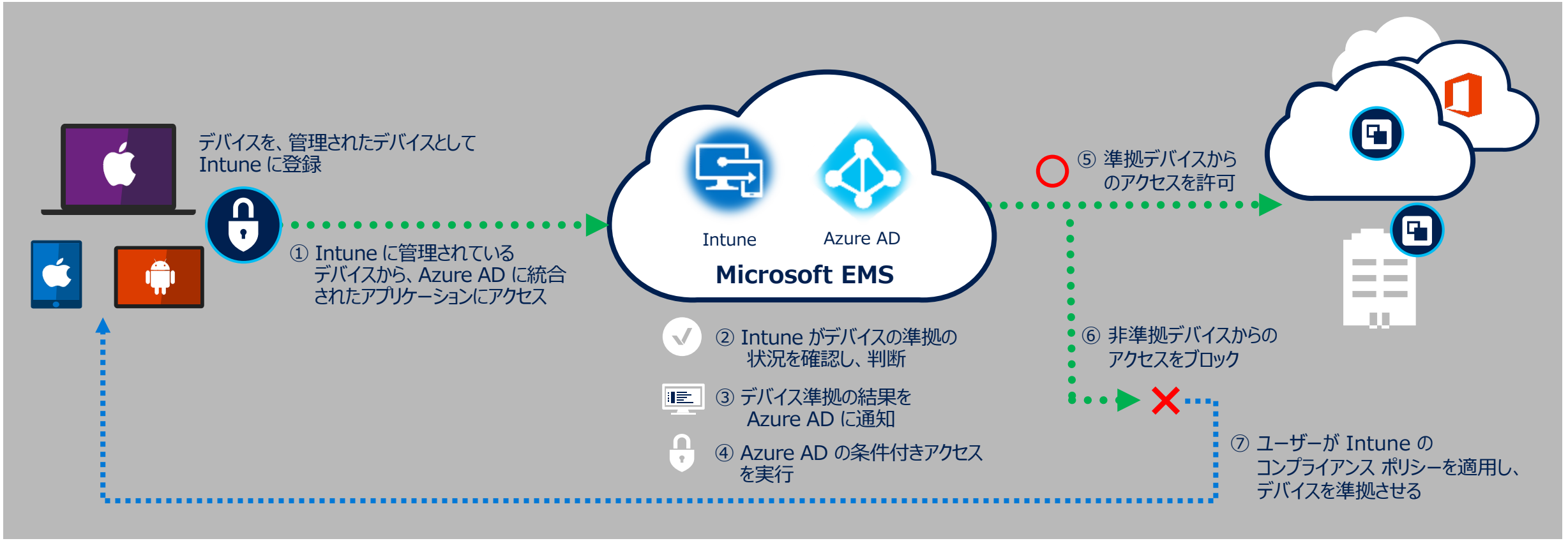
OS レベルの機能管理

アプリレベルで
会社データを保護

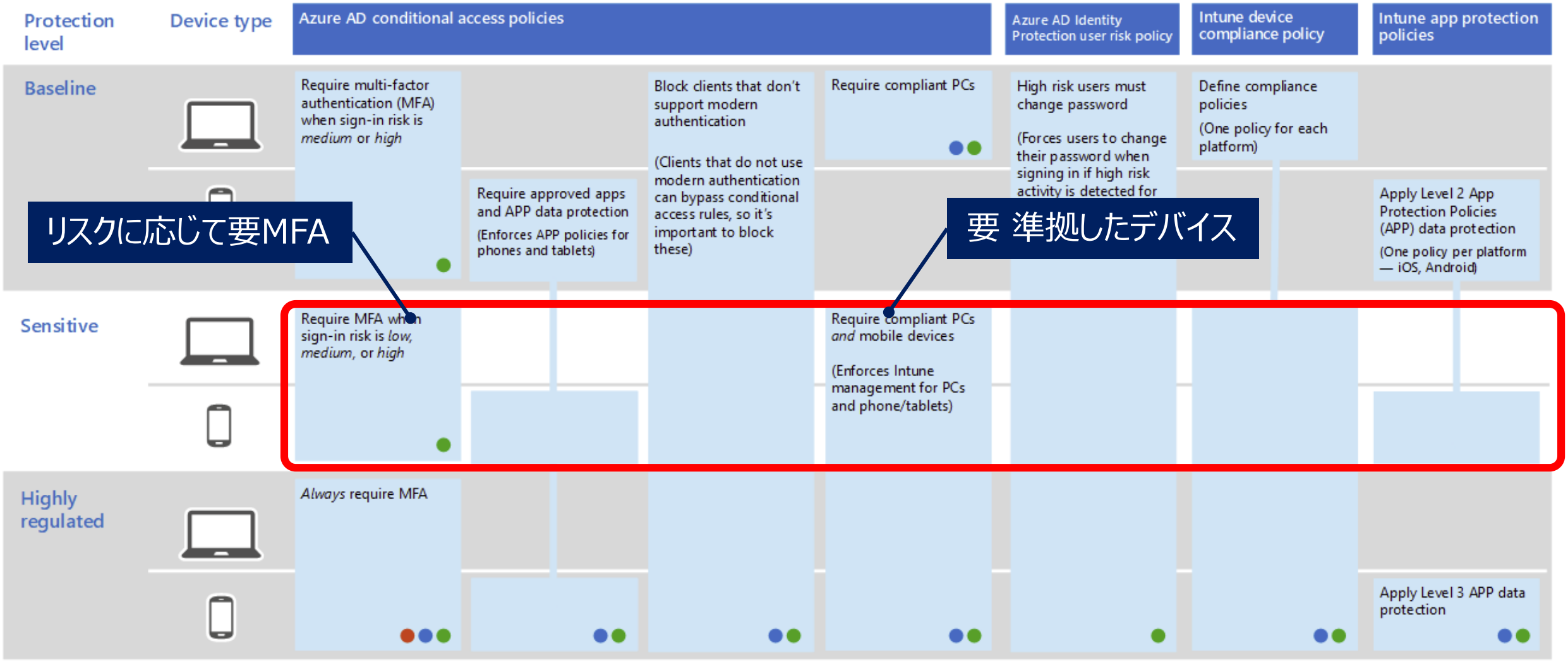
メール、Office 365、
他クラウドサービスの
アクセス制御(AAD連携)

コンプライアンス ポリシーと条件付きアクセス

Windows 10、iOS、macOS、Android デバイスからアプリケーションへのアクセスを、Azure AD の条件付きアクセスを使用して、デバイス ベースで制御できる



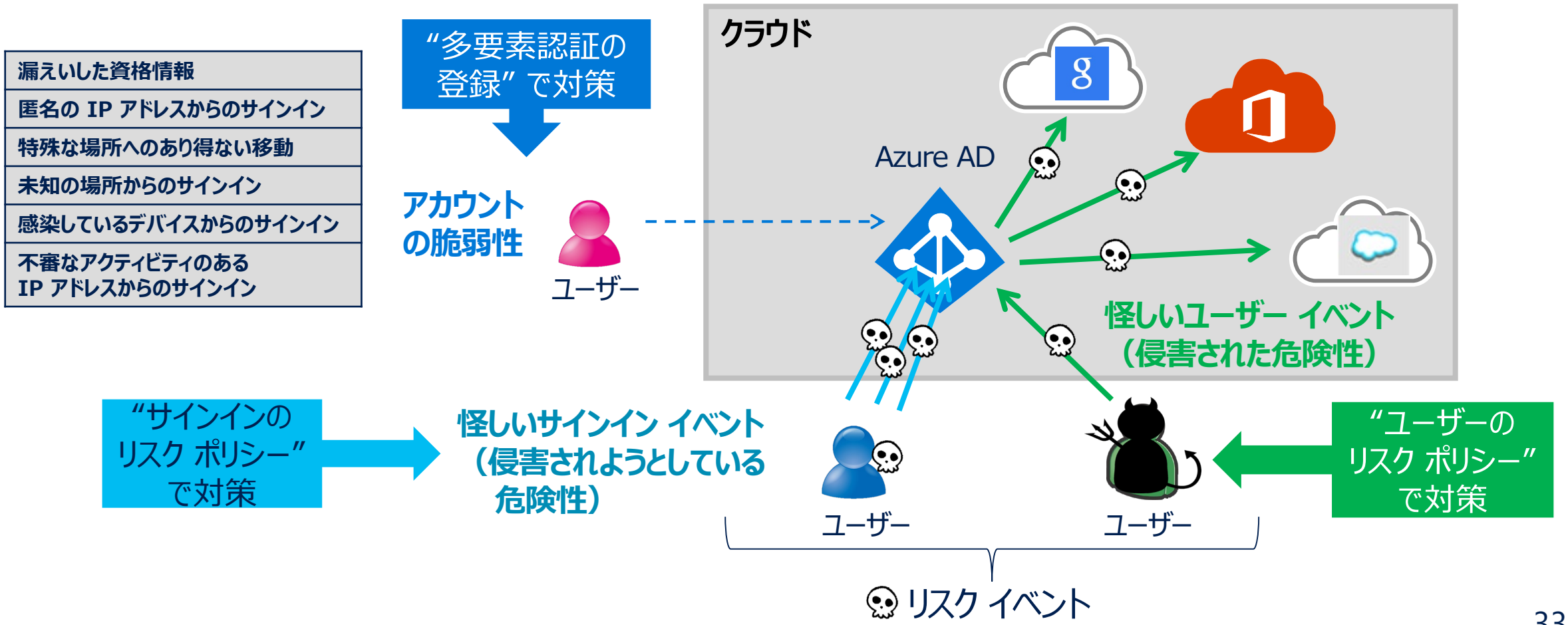
[参考] M365 Golden Config を参考にしてポリシー設計する



共通 ID とデバイスのアクセス ポリシー
https://docs.microsoft.com/ja-jp/microsoft-365/enterprise/identity-access-policies

[参考] Azure AD Premium の ID 保護 (Azure AD Premium P2)

- 脆弱なアカウント、怪しいユーザー操作（リスク イベント）を検出し、リスク レベルに基づいて、ポリシーを実行してくれる



[参考] 高まるセキュリティの脅威に対応する 完全なエンドポイント セキュリティ ソリューション

Microsoft Defender ATP

EDR（Endpoint Detection and Response）と呼ばれる、侵入されたときの対処を前提としてセキュリティである Microsoft Defender ATP は、
PC などエンドポイントがサイバー攻撃を受けることを前提に、脅威の検知や除去などの初動対処を円滑に行い、
最小限の被害に抑えることを目的としたセキュリティ対策です。

脅威および脆弱性管理

エンドポイントの脆弱性や構成ミスの検出、優先順位付け、
および修復を行います。

エンドポイントの検知と応答

最初の 2 つのセキュリティの防御を通過した可能性がある、高度な
脅威の検出、調査、対応を行えるように組み込まれています。

攻撃面の縮小

悪意のある IP アドレス、ドメイン、URL へのアクセスが
制御されます。

調査と修復の自動化

高度な脅威にすばやく対応するための機能と並行して、
自動調査と自動修復の機能を提供しています。

次世代の保護(ウイルス対策)

ネットワークのセキュリティの境界をさらに強化するために、
あらゆる種類の新たな脅威を捕えるように作られた次世代の
保護が使用されます。

Microsoft 脅威エキスパート

専門的なレベルの監視と分析を使用してセキュリティ操作センターを
提供する管理された脅威を探すサービスです。お客様のネットワークに
対する最も重要な脅威を事前に検索します。

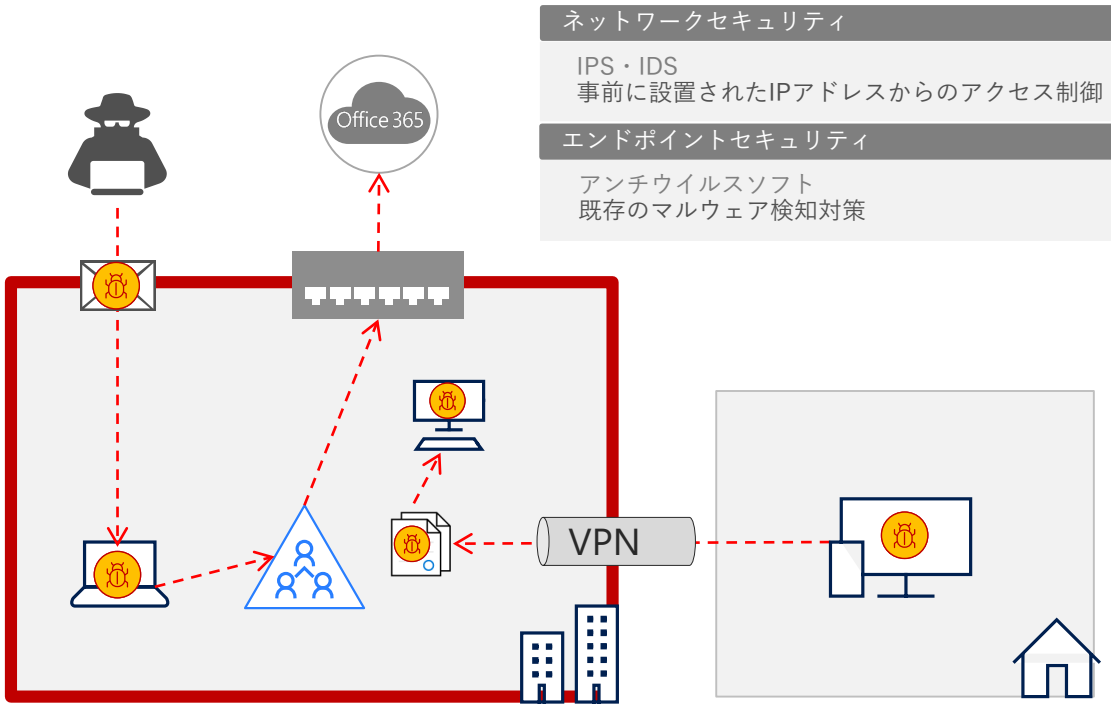
※Microsoft Defender ATP は、Microsoft Defender for Endpoint に名称変更されました。

リモートワークにおけるゼロ・トラストセキュリティ

＜従来＞

場所依存したネットワーク重視のセキュリティ対策

- リモートワークによりVPN/プロキシがひっ迫する
- ネットワークセキュリティ内に侵入されると検知するシステムが弱い
- 一台感染すれば他のデバイスも感染可能に



ネットワークセキュリティ

IPS・IDS
事前に設置されたIPアドレスからのアクセス制御

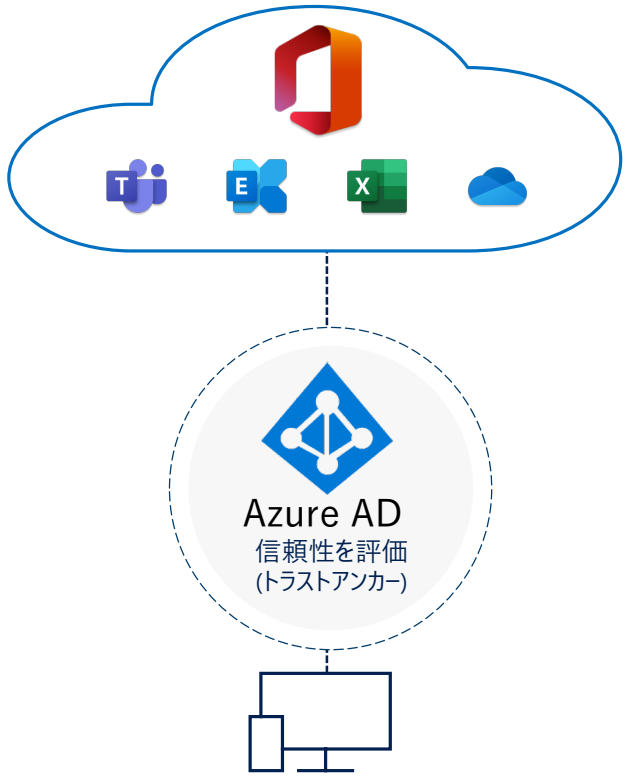
エンドポイントセキュリティ

アンチウイルスソフト
既存のマルウェア検知対策

＜今後＞

ゼロトラストセキュリティ対策

- Azure ADを基盤としたクラウド認証で直接インターネットへ接続
- ID・デバイス・アプリ・データそれぞれで検知・対処するセンサーを搭載
- 一台感染しても自動修復で感染拡大防止



データセキュリティ

Azure Information Protection
機密情報の自動ラベリングおよび暗号化

アプリセキュリティ

Microsoft Cloud App Security
シャドーITの検出 & アプリ異常行動検知

メールセキュリティ

Office 365 ATP
メールセキュリティ対策（検知・削除）

ID 保護

Azure AD Identity Protection
不正アクセスの検知および自動対処

Azure ATP
ユーザの振る舞い検知

エンドポイントセキュリティ

Microsoft Defender ATP
エンドポイント脅威の振る舞い検知・自動調査および自動対処

Microsoft 365 とは

課題解決にクラウドの Microsoft 365

Microsoft 365 とは、Office アプリケーションを含む Microsoft のクラウドソリューションを利用できるサービス

常に最新の Office アプリケーション

クラウドから ダウンロード

モバイル含め 15 台まで インストール

Exchange Online

メール

スケジュール

タスク管理

SharePoint Online

掲示板

チーム文書管理

情報共有

Microsoft 365 を利用すると、常に最新の Office アプリケーションを利用することはもちろん、場所やデバイスに関係なく効率よく作業することができます。
Exchange Online によるメール・スケジュール・連絡先管理、SharePoint Online による情報・ドキュメント共有、Microsoft Teams によるチャットやオンライン会議も可能。
大容量 1 TB のオンライン ストレージも標準で提供。
エンタープライズレベルのセキュリティで企業を守ります。

1 TB OneDrive for Business

チーム文書管理

情報共有

Microsoft Teams

チャットスペースの ワークスペース

オンライン会議

Security

サイバー攻撃に 対する防御

ビジネス データ保護

デバイスの 管理

中堅中小企業様向け (300名以下) プラン 一覧

2020年8月1日から提供開始

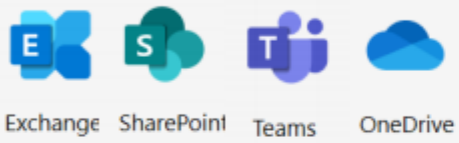
Remote Work Starter Plan

クラウド サービス　参考価格 1ユーザーあたり399円

既にお持ちのOffice付きのPC環境のまま
すぐにご利用いただけます

Microsoft 365 Business Basic

クラウド サービス



Microsoft 365 Business Standard

クラウド サービス、デスクトップ アプリ

Microsoft 365 Business Premium

クラウド サービス、デスクトップ アプリ、
セキュリティ

Microsoft 365 Apps for business

デスクトップ アプリ

注意: すべての機能、製品ロゴを表示しているわけではありません

Se

Microsoft