# CSPビジネスイントロダクション ④＜M365 提案 セキュリティ編＞

**TD SYNNEX 株式会社**
アドバンスドソリューション部門　マルチクラウドPM本部
マイクロソフトクラウドビジネス開発部
千葉　忠則

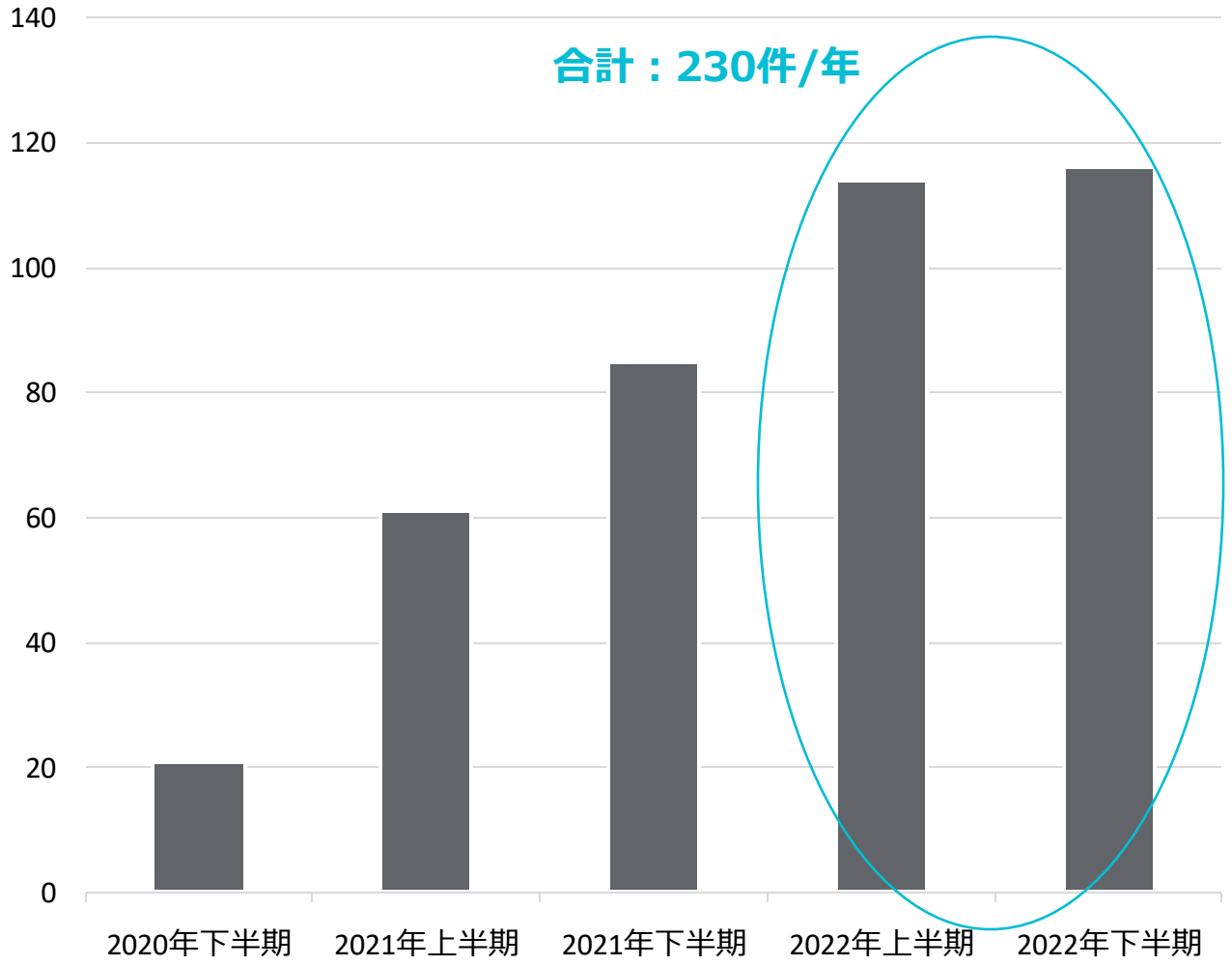
June 2023

# Agenda

| | |
|---|---|
| Microsoft 365 のセキュリティ | • Microsoft 365 に含まれるセキュリティ機能<br>• Microsoft でセキュリティツールを統一するメリット |
| Enterprise Mobility + Security | • Azure Active Directory Premium<br>• Intune<br>• Azure Information Protection |
| Microsoft Defender | • Defender for Office 365<br>• Defender for Business |
| パートナー様支援 | • EMS導入支援<br>• Defender for Business 導入支援<br>• Defender for Business 運用支援 |

# イントロダクション

# ランサムウェアによる被害件数



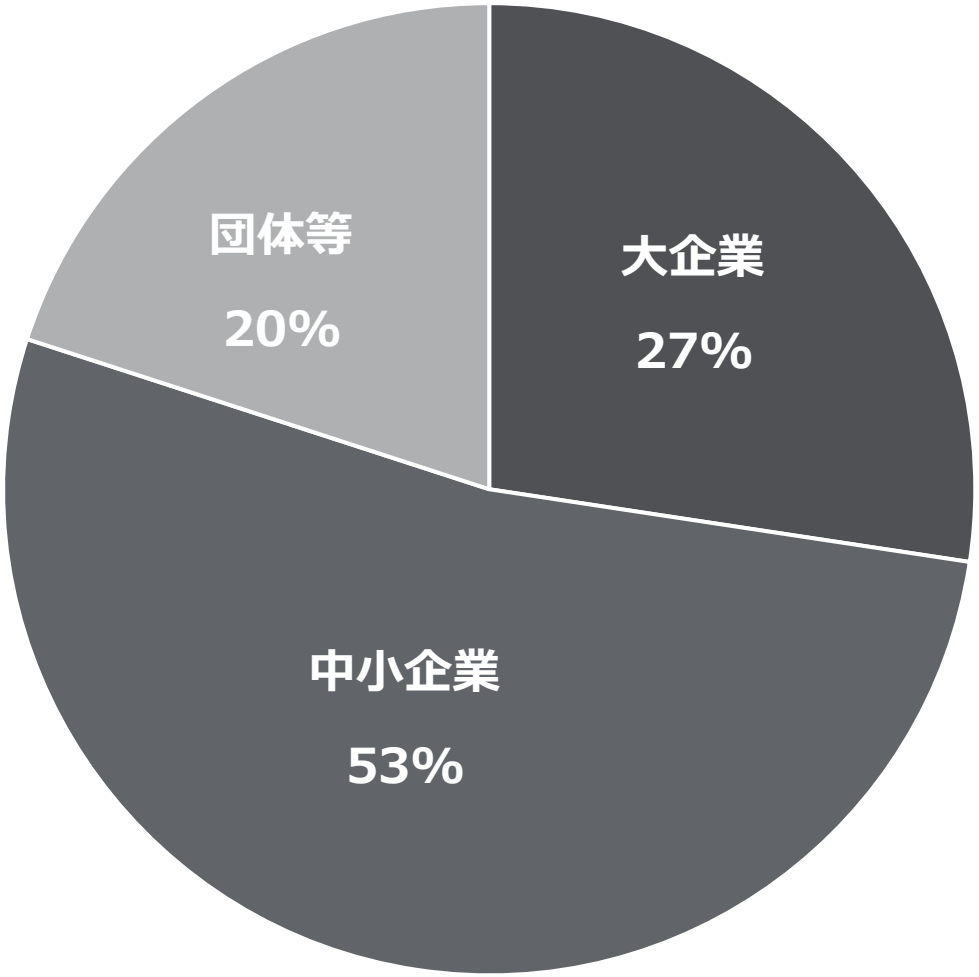

ランサムウェアの被害は、報告のあったものだけで

**年間230件** に上っている

※警察庁発表

警察庁：令和４年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

# ランサムウェア被害の組織規模



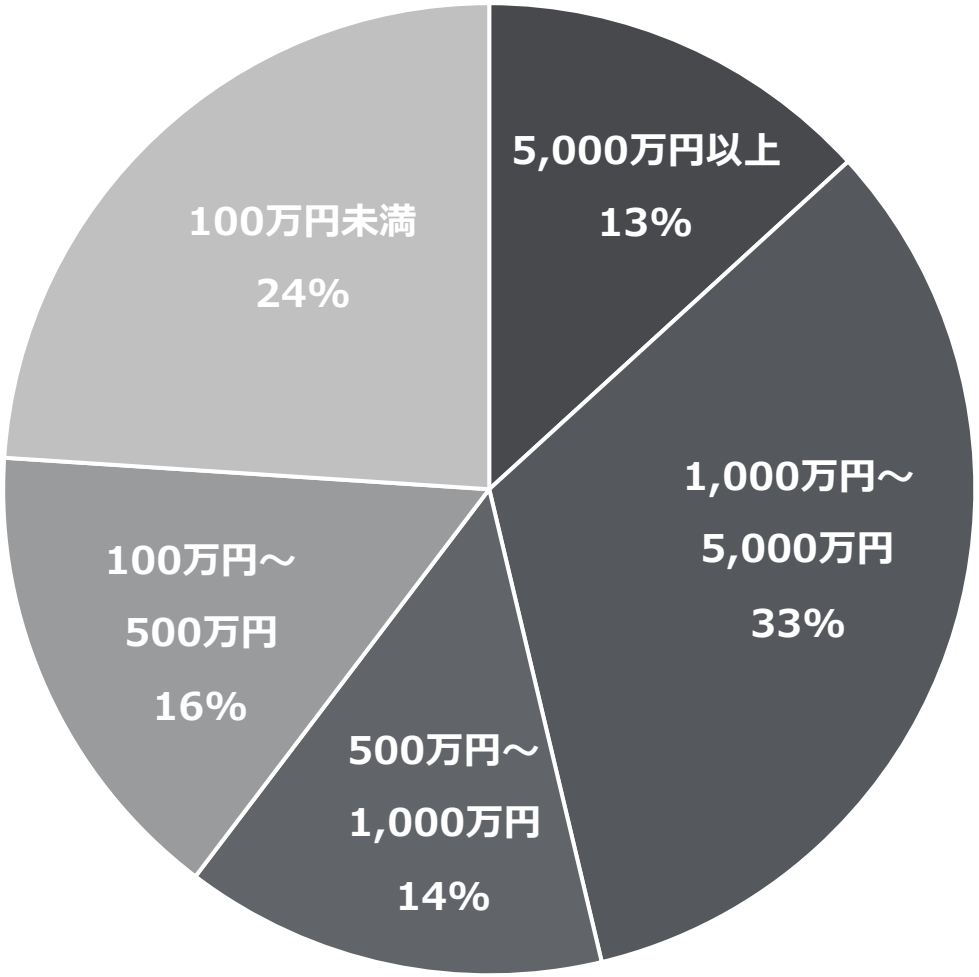

ランサムウェア被害の組織は、

**中小企業が半数以上**

※警察庁発表

警察庁：令和４年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
※「大企業」「中小企業」は。中小企業基本法に基づく分類

# ランサムウェア被害の調査・復旧費用




ランサムウェア被害による調査・復旧に

**1,000万円以上を要したケースが 46%**

※警察庁発表

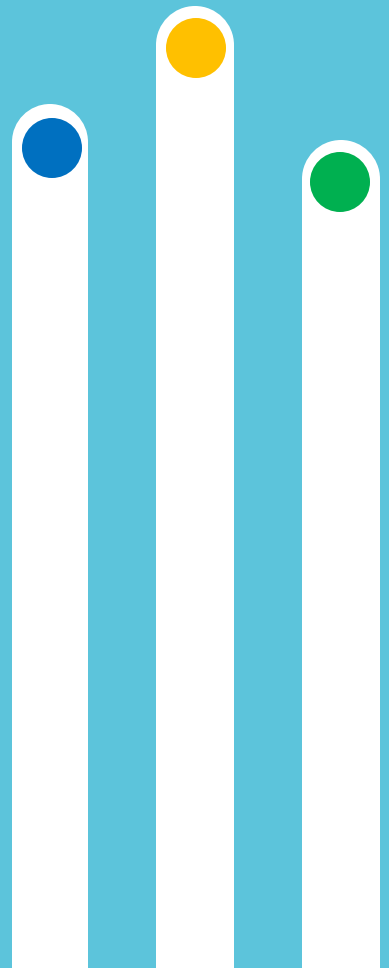
警察庁：令和４年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

# サイバー攻撃の被害の内容

| 「個人」向け脅威 | 順位 | 「組織」向け脅威 |
|---|---|---|
| フィッシングによる個人情報等の詐取 | 1 | ランサムウェアによる被害 |
| ネット上の誹謗・中傷・デマ | 2 | サプライチェーンの弱点を悪用した攻撃 |
| メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | 3 | 標的型攻撃による機密情報の窃取 |
| クレジットカード情報の不正利用 | 4 | 内部不正による情報漏えい |
| スマホ決済の不正利用 | 5 | テレワーク等のニューノーマルな働き方を狙った攻撃 |
| 不正アプリによるスマートフォン利用者への被害 | 6 | 不正プログラムの公開前を狙う攻撃<br>（ゼロディ攻撃） |
| 偽警告によるインターネット詐欺 | 7 | ビジネスメール詐欺による金銭被害 |
| インターネット上のサービスからの個人情報の窃取 | 8 | 脆弱性対策情報の公開に伴う悪用増加 |
| インターネット上のサービスへの不正ログイン | 9 | 不注意による情報漏えい等の被害 |
| ワンクリック請求等の不正請求による金銭被害 | 10 | 犯罪のビジネス化<br>（アンダーグラウンドサービス） |

IPA：情報セキュリティ10大脅威 2023より https://www.ipa.go.jp/security/10threats/10threats2023.html

# 驚異的な速度で進むサイバー攻撃



**1,287件**

1秒間に発生しているパスワード攻撃数
毎年120%増加し続けている

**1 時間 1 2 分**

フィッシングメールの被害に遭った場合に攻撃者が個人情報に到達するまでの平均時間

**1 時間 4 2 分**

デバイスが侵害されてから、攻撃者が社内ネットワークでラテラルムーブメント（遠隔でシステムに侵入する動き）を始めるまでの平均時間

# Microsoft 365 のセキュリティ

# マイクロソフトのサイバー攻撃への取り組み

TD SYNNEX

Microsoft Security

**200億ドル**

今後 5年間におけるセキュリティへの投資

**100億ドル**

昨年のセキュリティ事業の収益

**約300億のメール攻撃**

**約310億回の認証攻撃**

**約60億個のマルウェア**

昨年、マイクロソフトが阻止した脅威

Microsoft は セキュリティのエキスパート であり
世界最大級のクラウドプラットフォーマー

セキュリティは "製品を選択する" から
"プラットフォームの最大活用" にシフト

**ビルトイン セキュリティへ**

# 第三者機関によるセキュリティ評価

TD SYNNEX

ガートナー マジック クアドラントの
5 部門で「リーダー」の評価を獲得
※1

IDC MarketScape 「Modern Endpoint Security for Enterprise and Small and Midsize Businesses」部門で 「リーダー」の評価を獲得※2


### Microsoft サイバー防御オペレーション センター (CDOC)

サイバー防御オペレーション センターでは Microsoft 全社からセキュリティ対応の専門家を募り、脅威に対するリアルタイムでの保護、検出、対応に取り組んでいます。

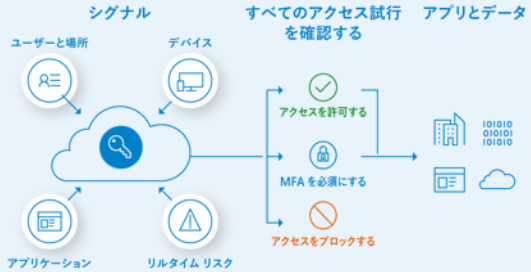
このセンターは 24 時間 365 日体制の専任チームを擁しており、セ キュリティの脅威に対する迅速な対応と解決を実現するために、Microsoft 全体の何千ものセキュリティ専門家、データサイエンティスト、製品エンジニアと共に脅威にリアルタイムで対抗しています。

※1 下記の 5 部門に相当
Gartner「Magic Quadrant for Access Management」、Henrique Teixeira、Abhyuday Data、Michael Kelley、2021 年 11 月
Gartner「Magic Quadrant for Cloud Access Security Brokers」、Craig Lawson、Steve Riley、2020 年 10 月
Gartner「Magic Quadrant for Enterprise Information Archiving」、Michael Hoech、Jeff Vogel、2020 年 10 月
Gartner「Magic Quadrant for Endpoint Protection Platforms」、Paul Webber、Rob Smith、Prateek Bhajanka、Mark Harris、Peter Firstbrook、2021 年 5 月
Gartner「Magic Quadrant for Unified Endpoint Management」、Dan Wilson、Chris Silva、Tom Cipolla、2021 年 8 月
※2 Microsoft、IDC MarketScape の「Modern Endpoint Security for Enterprise and Small and Midsize Businesses」部門で「リーダー」の評価を獲得 - Microsoft Security ブログ (英語 )

# Microsoft 365 のセキュリティ機能

- Microsoft 365 には多くのセキュリティ機能が盛り込まれています。
- Microsoft 365 ビジネスプランの「Microsoft 365 Business Premium」は、企業が必要とするセキュリティ機能の多くをカバーできるようになっています。

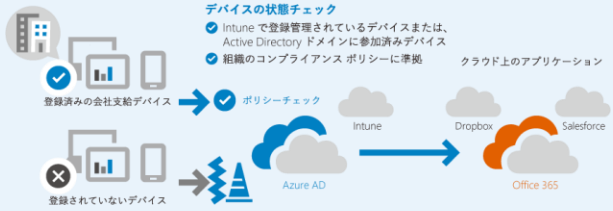
### 条件付きアクセス



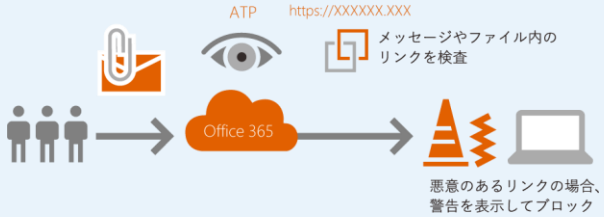

### 多要素認証（MFA）


### ファイルやメールを暗号化して保護

### Windows PC とモバイルデバイスを管理コンソールから一元管理




### クラウド ベースの電子メール フィルタリング サービス




### 訴訟対策としてすべてのメールデータを管理者側で保持

など

# Microsoft 365 のプラン

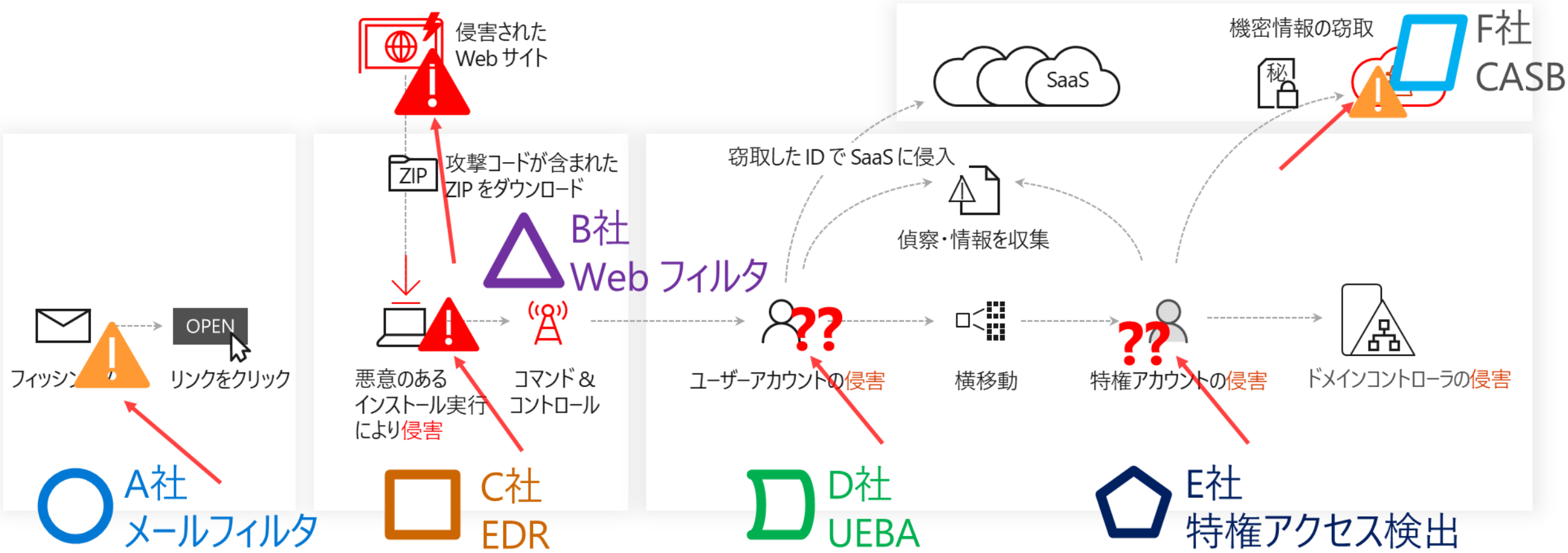
TD SYNNEX

| 対象 | | for Business（中小企業向け） | | | |
|---|---|---|---|---|---|
| 最大ユーザー数 | | 300 | | | |
| プラン名 | | Microsoft 365 Apps for business | Microsoft 365 Business Basic | Microsoft 365 Business Standard | Microsoft 365 Business Premium |
| 参考価格(1ユーザー) | 月額（年契約月払い） | 1,030 | 750 | 1,560 | 2,750 |
| | 年額（年契約年払い） | 12,360 | 9,000 | 18,720 | 33,000 |
| Officeアプリケーション(Business)<br>（1ユーザーができるインストール可能台数） | ※Windows PCのみ利用可<br>1ユーザー計15台（デスクトップ5台、タブレット5台、スマホ5台） | ● | | ● | ● |
| Office Online | Webブラウザで利用できるOffice（） | ● | ● | ● | ● |
| One Drive for Business | 個人用ストレージ（1TB/ユーザー毎） | ● | ● | ● | ● |
| Exchange Online | Exchange Online Plan1(メール容量50GB/1ユーザー) | | ● | ● | ● |
| SharePoint Online | 組織ポータルサイト(1TB+(10GB×ユーザー数)=合計容量 | | ● | ● | ● |
| Yammer | 法人向けSNS | | ● | ● | ● |
| Microsoft Teams | IM、Web通話、Web会議、ファイル共有アプリケーション | | ● | ● | ● |
| Power Apps | ローコードアプリケーション開発 | | ● | ● | ● |
| Power Automate | プロセス自動化ツール | | クラウドフローのみ | クラウドフローのみ | ● |
| Azure AD Premium P1 | ID とアクセス管理 | | | | ● |
| Microsoft Intune | デバイスとアプリの管理 | | | | ● |
| Azure Information Protection P1 | 情報の保護 | | | | ● |
| Microsoft Defender for Office365 | 脅威からの保護 | | | | ● |
| Microsoft Defender for Business | クライアント端末セキュリティ（EDR） | | | | ● |

※記載価格は推定小売価格（税抜）になります。
※2023年4月現在でのBusinessプラン一覧になります。

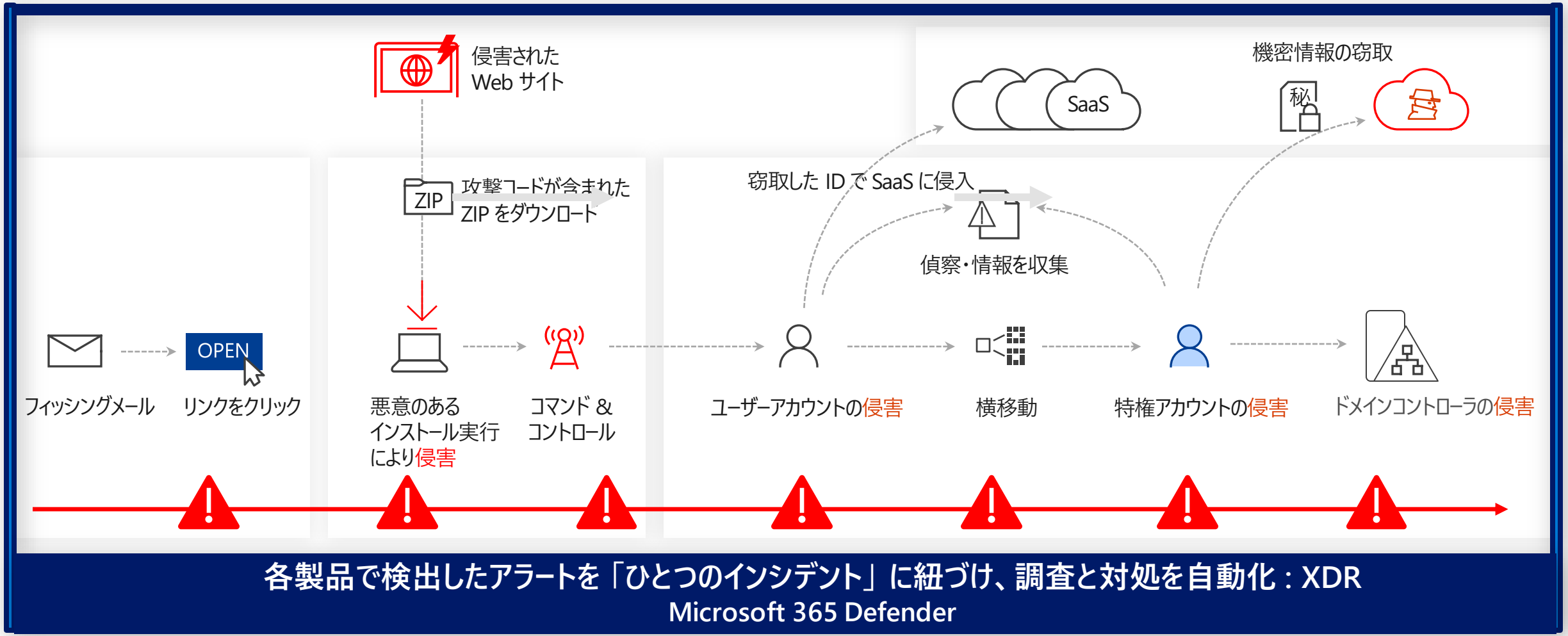
# セキュリティツールを Microsoft に統一するメリット

- セキュリティ製品がサイロ化されている場合、発生しているインシデントの「数」を把握しづらくなります。



# セキュリティツールを Microsoft に統一するメリット

- **各セキュリティツールが連携し、検出したアラートを「ひとつのインシデント」に紐づけてくれます。**



# Enterprise Mobility + Security

（通称：EMS）

# EMSに含まれるアプリケーション

**クラウドの ID と アクセスの管理**

**Azure Active Directory Premium P1**

**月額：750円/ユーザー**

**デバイスと アプリの管理**

**Microsoft Intune**

**月額：1,000円/ユーザー**

**企業の ドキュメント保護**

**Azure Information Protection Premium P1**

**月額：250円/ユーザー**

# Enterprise Mobility + Security E3
# 月額：1,320円/ユーザー

表記価格は2023年4月時点の年契約月払いの定価（税抜）となります。

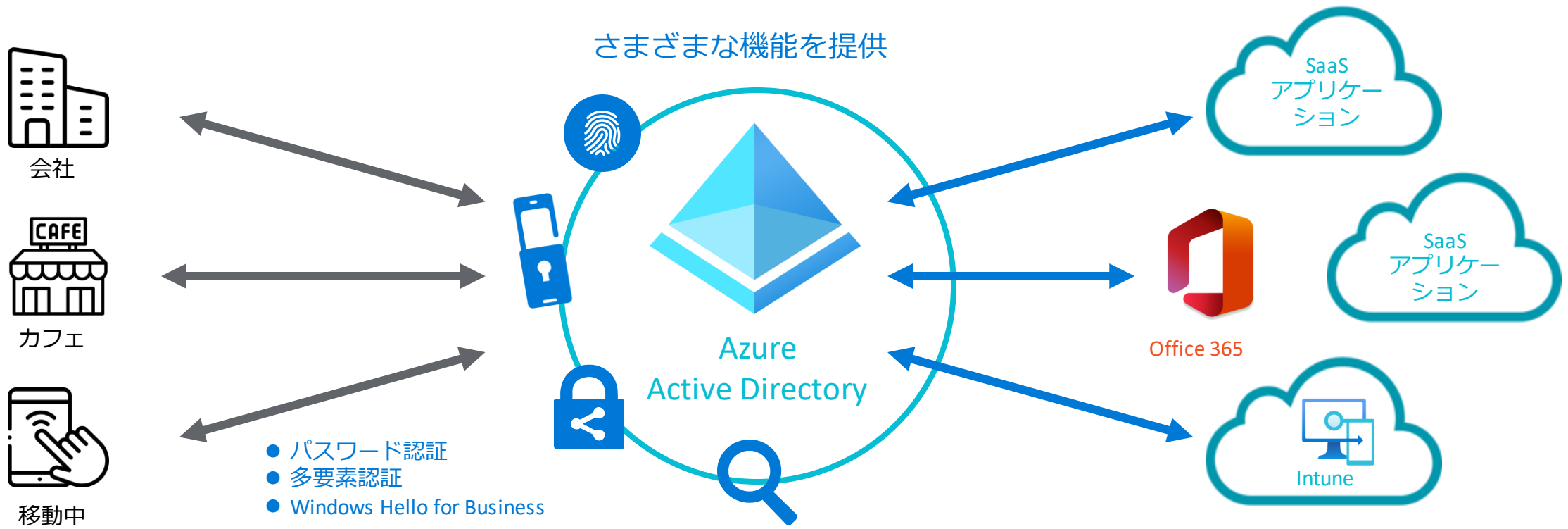
# アクセス制御

## -Azure Active Directory Premium

# 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

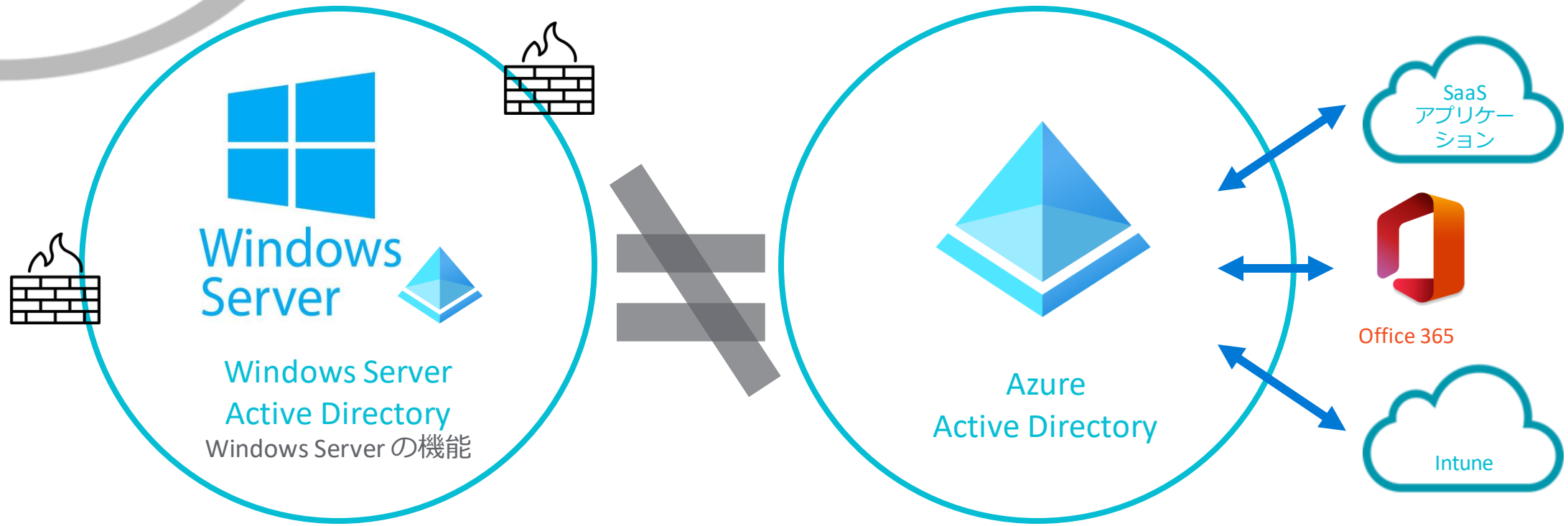
- Microsoft Azure が提供するサービスの1つ
- Office 365 や Intune の認証サービス
- オンプレミス Active Directory と統合できる



# オンプレミス Active Directory と Azure AD は、

TD SYNNEX

完全に
別のものです！



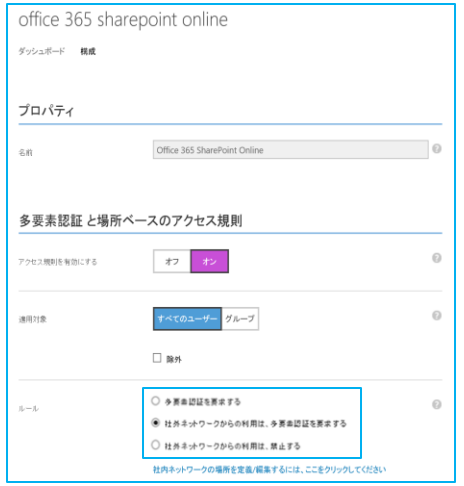
# Azure AD Premium による条件付きアクセス

TD SYNNEX

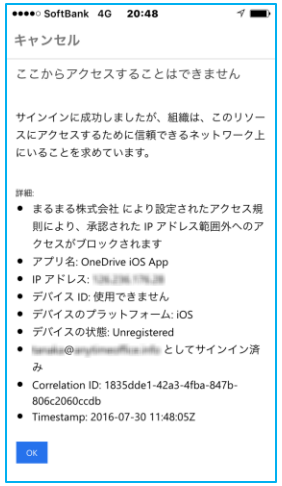
Exchange Online、 SharePoint Online、 Yammer、 その他 SaaS アプリ などのサービス単位に
利用条件を設定可能

| カテゴリー | **設定１ 多要素認証必要**<br>人事・個人情報を扱うようなアプリで | **設定２ 社外ネットワークのみ多要素認証**<br>基本社内からのみ利用で<br>社外利用をどうしても許可したいアプリで | **設定３ 社外ネットワークからの利用禁止**<br>社内のみに限定して利用 |
|---|---|---|---|
| 社外からのアクセス | ○ 二要素認証でのみ接続可 | ○ 二要素認証でのみ接続可 | × 社外からの接続禁止 |
| 社内からのアクセス | ○ 二要素認証でのみ接続可 | ○ 通常の認証で接続可 | ○ 通常の認証で接続可 |

- IPアドレス指定による社内ネットワークと社外ネットワークを特定し、社外からのアクセスを禁止
  - Azure AD Premium Plan1のライセンスが必要
  - ADFSとの連携が可能（オプション）
- 多要素認証による、IDの不正利用の防止
  - 電話からPIN番号を入力
  - 認証アプリ (Multi-Factor Auth) にPIN番号を入力
  - ショートメッセージにPIN番号を送信
- パスコードの代わりに指紋認証も使用（iOS/Android）



管理画面



アクセス時の画面

# デバイス制御
## -Microsoft Intune

# Microsoft Intune とは

Office 365 との連携によるメリット

## MDM
## モバイル デバイスの管理
## （デバイス制御・紛失対策）

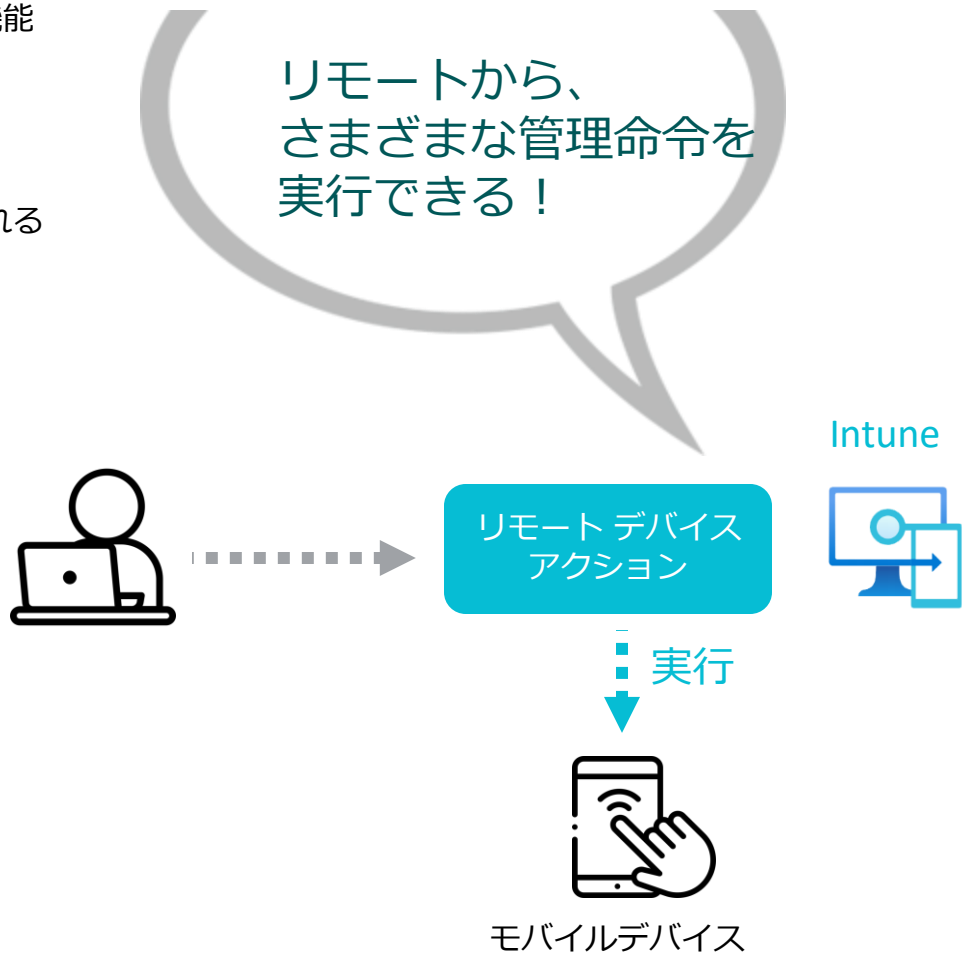
- インベントリ収集
- セキュリティ ポリシーの管理
- リモート ワイプ
- Wi-Fi / VPN /証明書/メール設定の配布
- Apple Configuratorのサポート
- セレクティブ ワイプ
- 企業所有デバイスのキッティング効率化
- 使用条件の同意の取得

## MAM/MCM
## アプリ/コンテンツの保護
## （情報漏洩対策）

- デバイスへのアプリのプッシュ インストール
- アプリ単位のコピー & ペーストの制御
- アプリ単位の VPN 設定
- LOB アプリのラッピング
- Office Apps のラッピング
- Manage Browser / PDF Viewer の提供
- 未許可アプリの利用状況取得
- メールを利用するデバイスの検疫

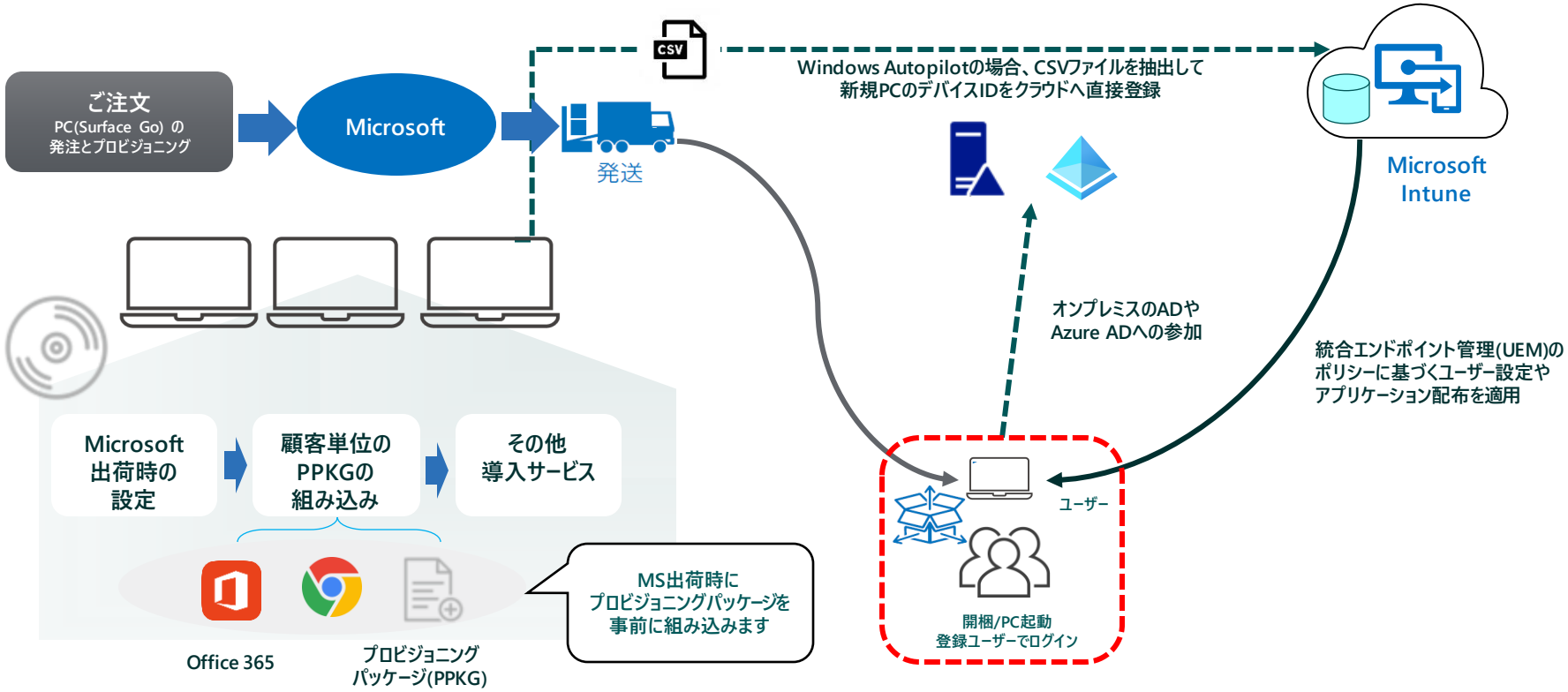
# 管理者によるリモート管理例

- アクティブ化ロックのバイパス（iOS）
  - ✓ iOS 8.0 以降向けの iPhone を探すアプリの機能である iOS のアクティブ化ロック機能の管理
- 新しく開始（Windows 10）
  - ✓ Creators Update が稼働する Windows 10 PC にインストールされている すべてのアプリが削除され、PC が Windows の最新バージョンに自動的に更新される
- リモート コントロール（Android）
  - ✓ 別売りの TeamViewer ソフトウェアを利用して、Android デバイスを使用するユーザーにリモート アシスタンス機能を提供
- 再起動
- 紛失モード
  - ✓ デバイスのすべての利用がブロックされ、デバイスの検索を実行できる
- リモート ロック
- パスコードのリセット
- 出荷時の設定に戻す
- デバイスの検索
  - ✓ 紛失した、または、盗まれた iOS デバイスの場所をマップに表示する　など



# AutoPilot （キッティングの自動化）

Windows Autopilotを利用することでクラウドベースの仕組みを用いてPC初期展開を可能にします。
従来のイメージクローニングや手動のPCセットアップの手間と工数をなくし、企業でのリモートワークの
仕組みを導入する際のハードルを下げてモダンワークを実現します。



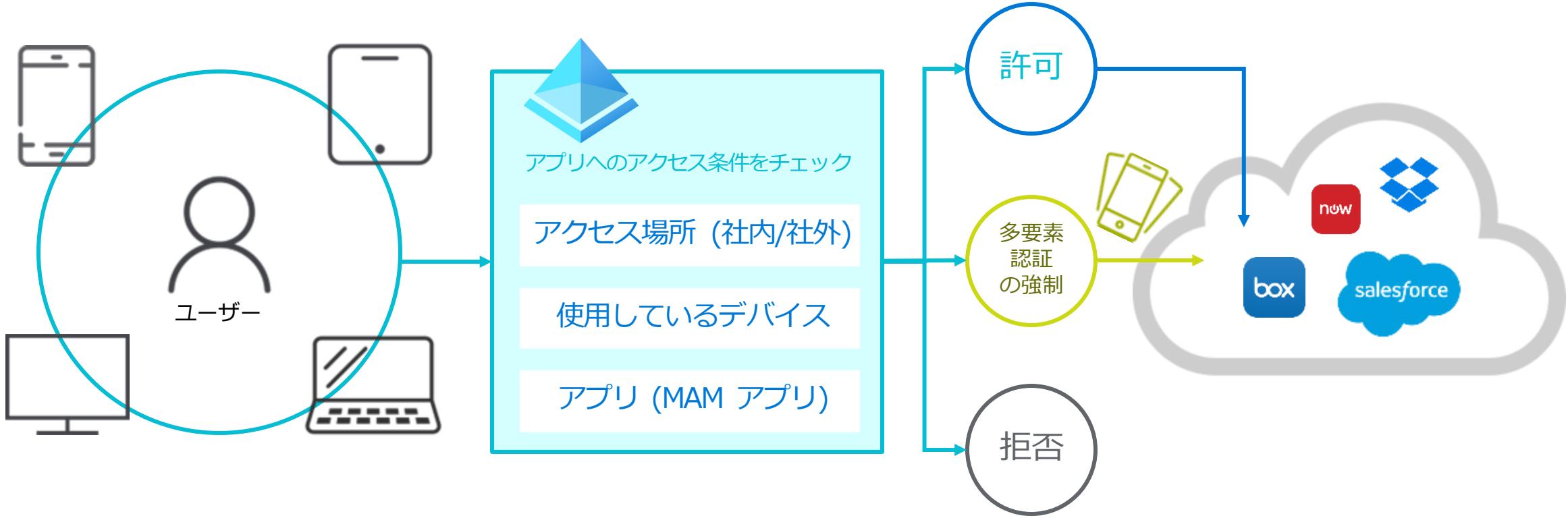

Autopilot 対応デバイスメーカーはMicrosoft以外にも多数！
一覧はこちら

# より高度なアクセス制御

## -Azure AD Premium P1 + Microsoft Intune

# Azure AD Premium + Intune による条件付きアクセス

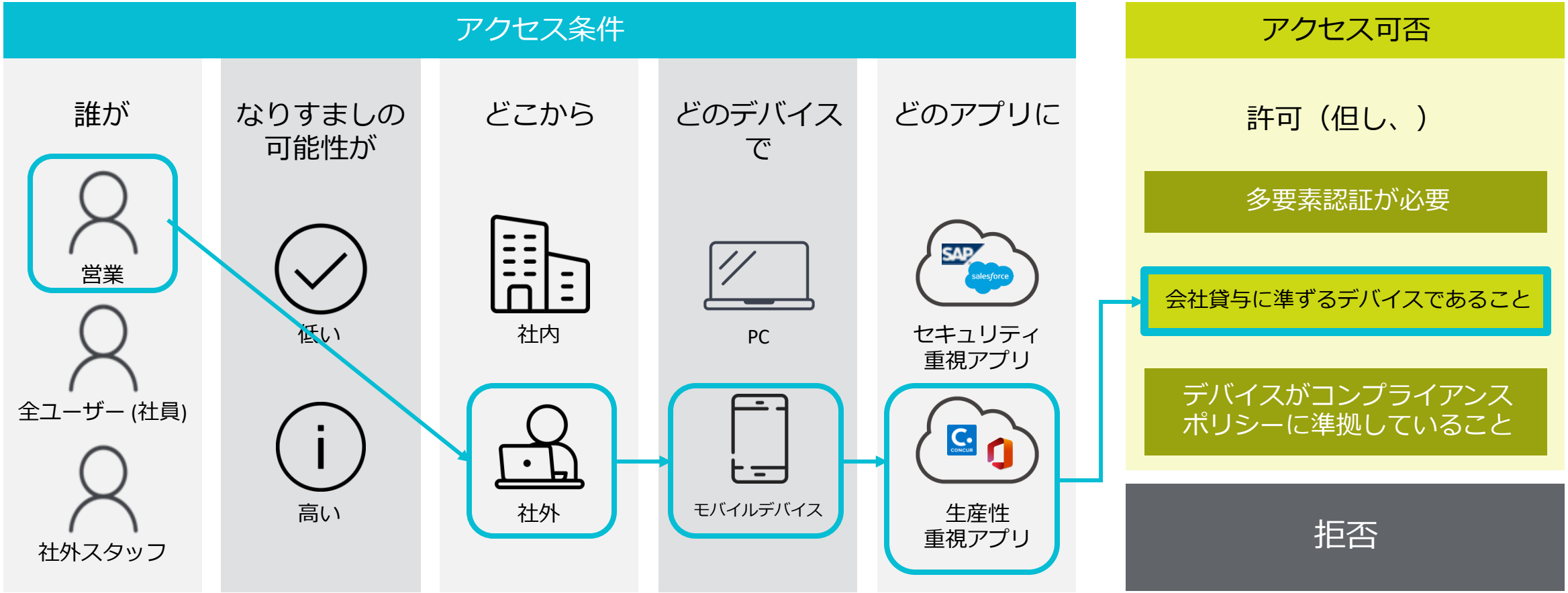
- 様々な“条件”によってアプリケーションへのアクセスを制御する
- Azure Active Directory Premium で認証を統合することで、様々な条件でアクセス制御が可能




※ 条件付きアクセスは EMS E3 のうち、Azure Active Directory Premium P1 以上と Microsoft Intune のライセンスによって提供されるサービスです

# 条件付きアクセス ポリシー例

営業部の社員はモバイルデバイスでアクセスする際に社給デバイスが必要




※ Office 365 では、アクセスを完全に制御するには ADFS との組み合わせが必要になる場合があります

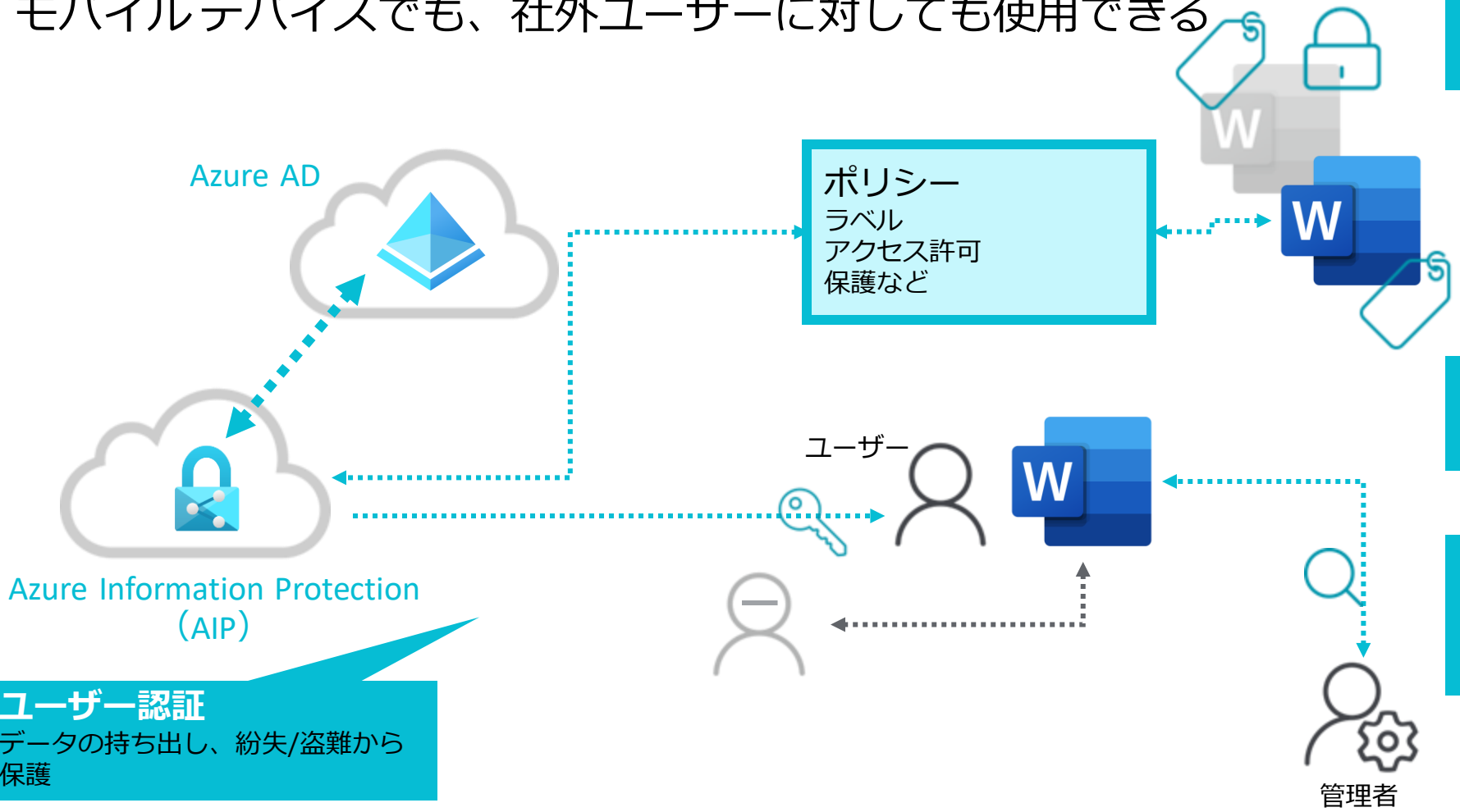
# ドキュメント保護

## -Azure Information Protection

# Azure Information Protection とは

組織のコンテンツ（文書や電子メール）の分類管理と保護の基盤

- 情報漏えいを防ぐためのソリューション
- モバイルデバイスでも、社外ユーザーに対しても使用できる




**ドキュメントの分類と暗号化**
ドキュメントの内容に基づいて
暗号化対象を自動的に判断し、
暗号化を設定

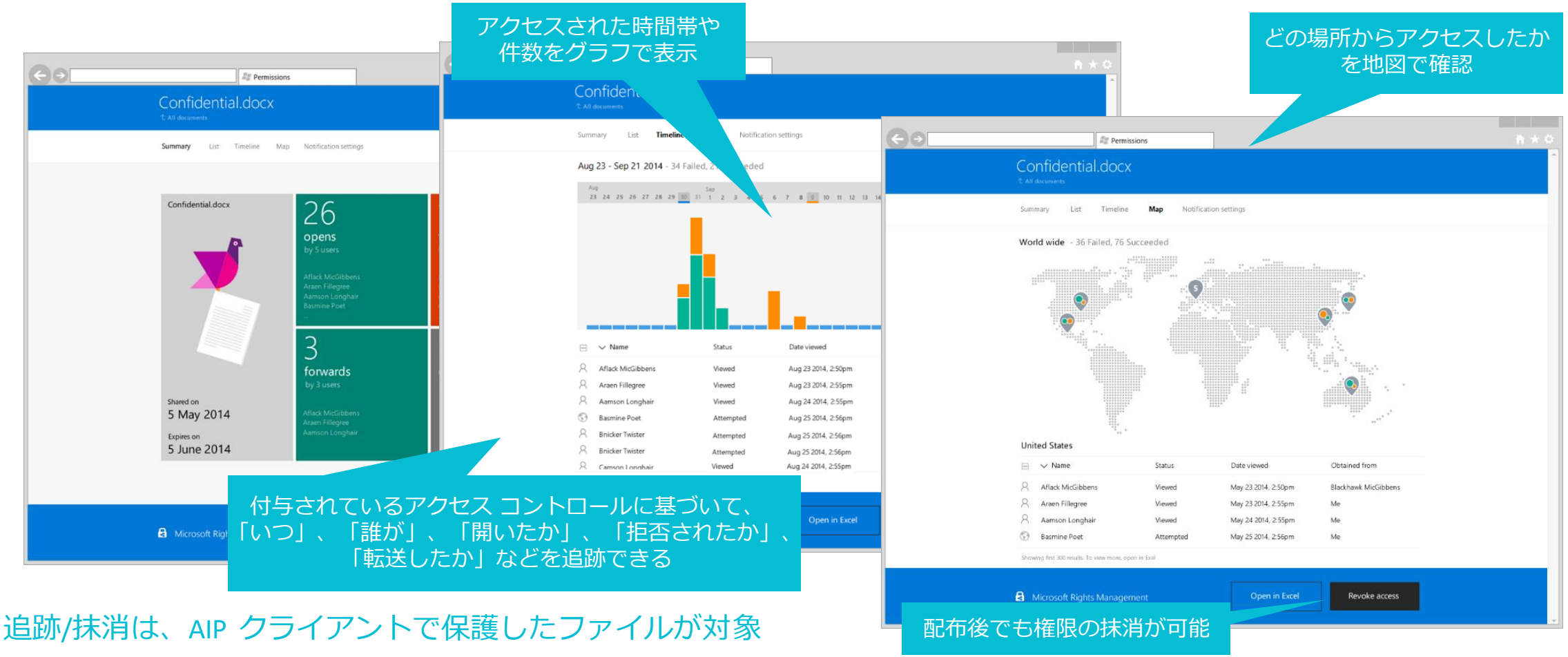
**権限の制御**
意図した権限範囲内の共有

**追跡と対処**
ドキュメントのアクセス状況の
追跡と不正アクセス発生時に
権限をはく奪

**ユーザー認証**
データの持ち出し、紛失/盗難から
保護

# 対象ファイルの追跡～権限取り消しについて

- 組織の管理者とエンドユーザーは、共有コンテンツの利用状況の監視/追跡が可能
- コンテンツの共有後に、アクセス権限の取り消しが可能




※ 追跡/抹消は、AIP クライアントで保護したファイルが対象

# Microsoft Defender

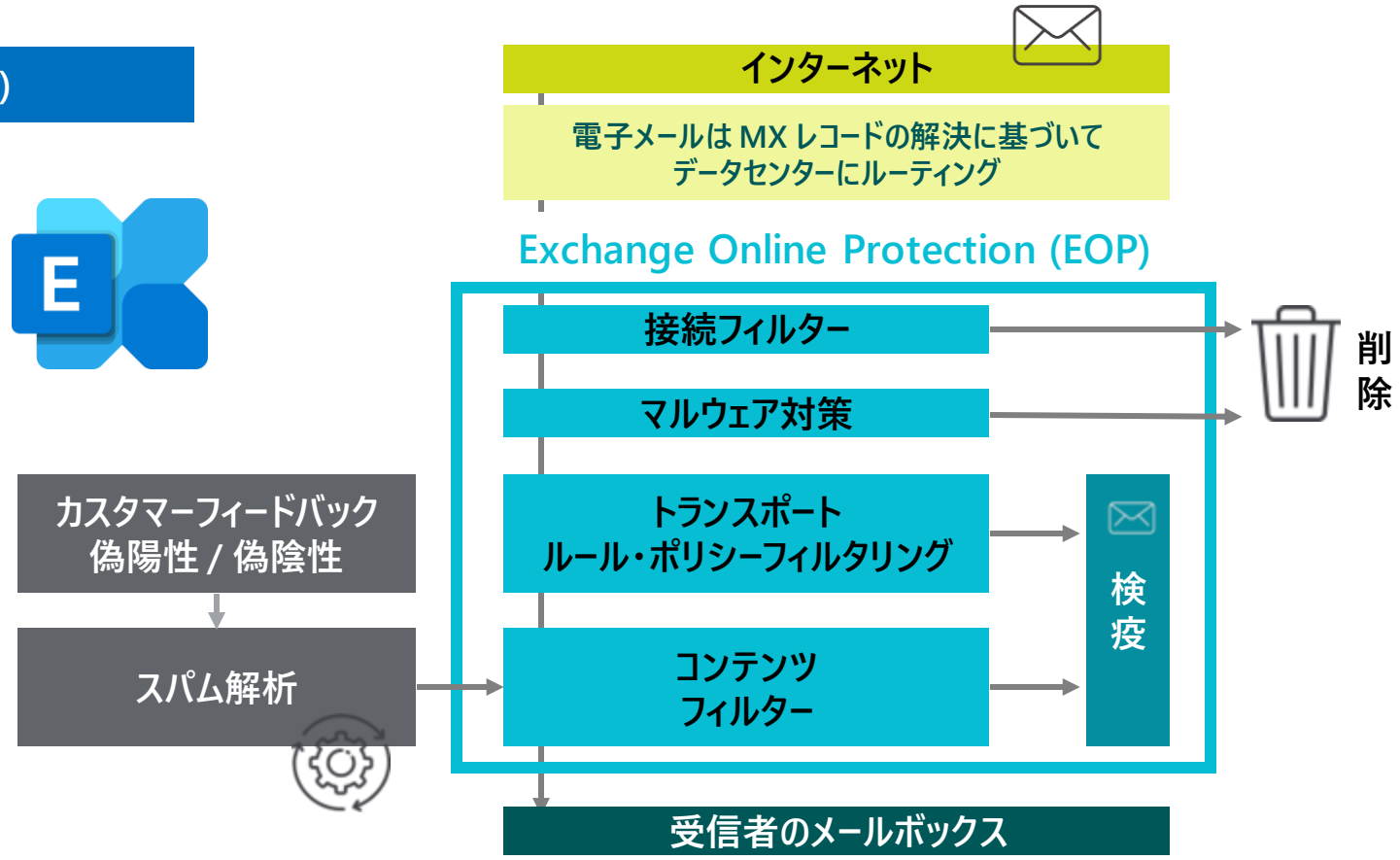
# メールセキュリティ
## -Microsoft Defender for Office 365

# Exchange Online の標準セキュリティ

- Microsoft 365 のメールサービス Exchange Online には、標準のセキュリティ対策として Exchange Online Protection (EOP) がセットされています。

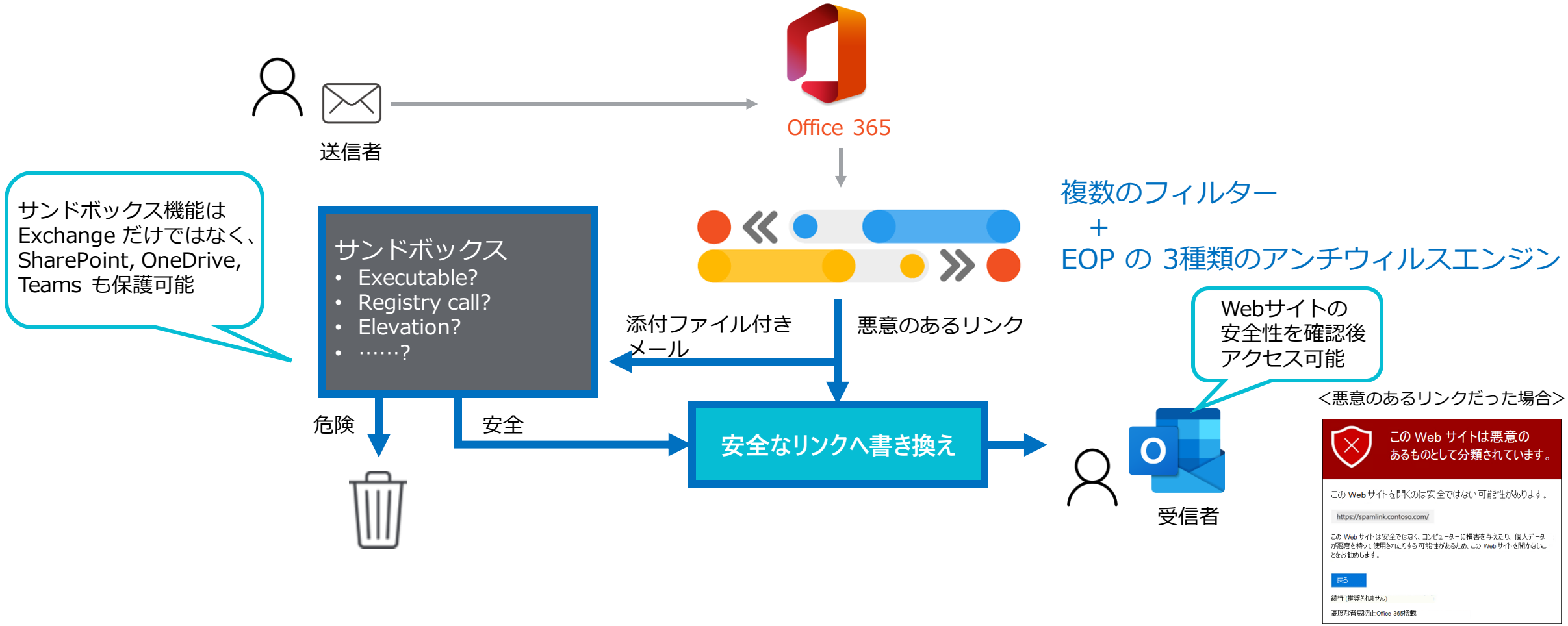
**Exchange Online Protection (EOP)**

- ✓ スパム
- ✓ フィッシング
- ✓ マルウェア
- ✓ バルク メール
- ✓ スプーフィング インテリジェンス
- ✓ 偽装の検出
- ✓ 管理者検疫
- ✓ 管理者とユーザーによる誤検知と検出漏れの報告
- ✓ URL およびファイルの許可/禁止
- ✓ レポート



# Microsoft Defender for Office 365

- Exchange Online の標的型攻撃対策として、Microsoft Defender for Office 365 がご検討頂けます。



# クライアントセキュリティ
## -Microsoft Defender for Business

# Microsoft Defender for Business

TD SYNNEX

- ランサムウェアなどによるサイバー攻撃が多様化している今、Windows OS 標準搭載のウィルス対策機能に **Microsoft Defender for Business** をプラスして、最高レベルのセキュリティ対策を実現

OS 標準搭載 ウイルス対策

Microsoft Defender **ウイルス対策**

Windows

防御

OS標準機能で、ウィルス侵入前の **防御** ができる

＋

OS 標準搭載のウイルス対策を**更に強化**

Microsoft Defender for Business

（マイクロソフト・ディフェンダー・フォー・ビジネス）

脅威と脆弱性の管理

攻撃表面の縮小

次世代の保護

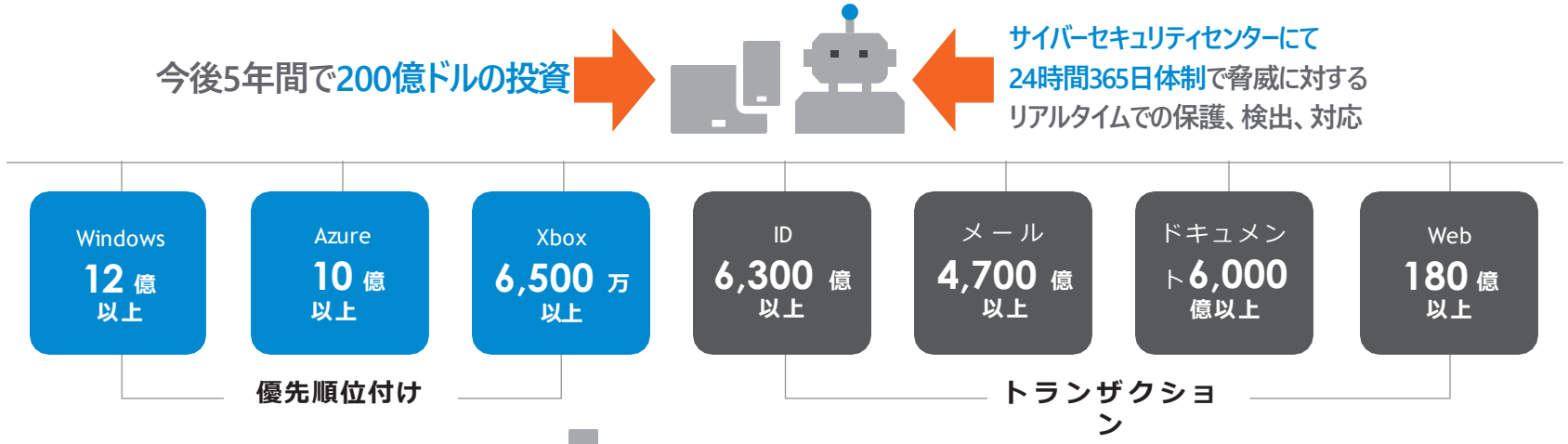
アラート検出と対処

自動調査と修復

ウィルス侵入後の **検知・対応・修復** もできる

# 世界随一のサイバー攻撃への防御力を誇る Microsoft のセキュリティ知見を提供

Microsoft は、米国国防総省に次いで世界で 2 番目に多くのサイバー攻撃を受けている組織と言われています。
世界中でご利用いただいている Microsoft 製品を通してサイバー攻撃を地球規模で監視、24 時間 365 日体制で、
AI + セキュリティ専門家による対応を通じ世界最高水準のセキュリティを提供します。




**3,000 億**
2019年にプロファイルされ、分析されたユーザーアクティビティの件数

**23 億**
1日に発見されるエンドポイントの脆弱性

**110 億**
2019年にブロックされた悪意ある / 疑わしいメッセージ

**120 億**
2019年に調査、監視、制御されたクラウドアクティビティの件数

# Windows 10/11 と最高レベルの親和性

Windows 10/11 を利用している場合、簡単なオンボーディング作業のみで利用が開始できます。面倒なソフトウェアの最新化などはWindows Update に任せることができ、メンテナンス フリーで利用者にわずらわしさを感じさせません。

## 大企業同等のセキュリティ

大企業向け製品と同等のセキュリティ機能が、中堅・中小企業向けに最適化、1ユーザーから購入可能

## 攻撃への耐性

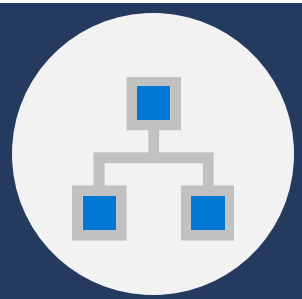
万が一サイバー攻撃を受けてもプログラムやサービス停止など影響は最低限

## メンテナンスフリー

Windowsにプレインストール済みWindows Updateの適用で更新手間いらず

## 高パフォーマンス

パソコンへの負荷が非常に低く、通信データも1台あたり1日 5MB 程度



## 様々な製品と連携

Microsoft 365 はもちろんさまざまな製品と連携できるマルチOS対応※も

# 自動調査と修復

脅威に遭遇した時、影響が本当にあったのか確認するのは管理者の役割です。
しかし規模の小さい組織ほど、この役割にかけられるコストが小さいことは明白です。
Microsoft Defender for Business は AI を活用した自動対処の機能を備えています。

## 自動調査

アラートを自動的に調査し、複雑な脅威を数分で修正

- アナリストが実行する理想的な手順を模倣
- ファイルまたはメモリ ベースの攻撃に有効
- 無制限のキャパシティで 24 時間 365 日動作

# 製品ラインナップについて

TD SYNNEX

**Microsoft Defender for Business で**
**端末セキュリティのみ切り出して対応可能**

## Microsoft Defender for Business

EDR 単体製品 **価格 ¥380 ユーザー/月**

Windows OS 標準のセキュリティ対策ソフトを強化して、
さらにEDR 機能を追加したい場合にはこちらを選択

Microsoft Defender for Business

**Microsoft 365 Business Premium でゼロ トラスト型セキュリティ対策が実現可能**

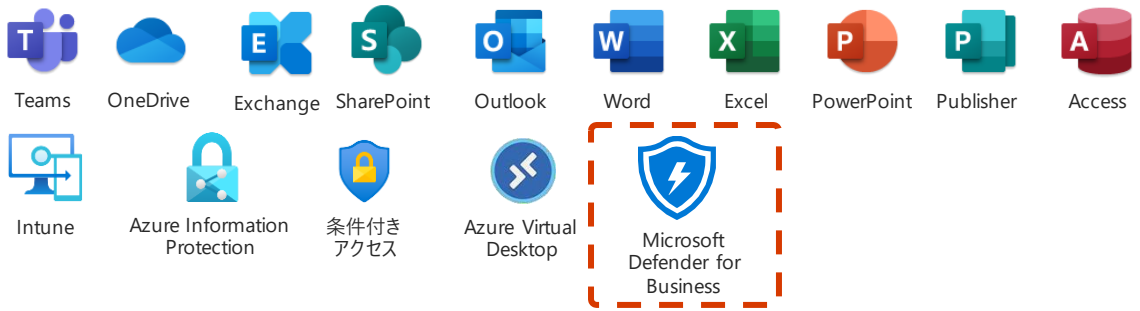
## Microsoft 365 Business Premium

クラウドサービス、デスクトップアプリ 高度なセキュリティ

Microsoft 365 の機能と Azure AD P1/Intune が提供されます。

Office アプリとクラウドサービスに包括的なセキュリティを組み合わせたプランです。

ビジネスを高度なサイバー脅威から守るのに役立ちます。



# Microsoft 365 のプラン（再掲）

TD SYNNEX

| 対象 | | for Business（中小企業向け） | | | |
|---|---|---|---|---|---|
| 最大ユーザー数 | | 300 | | | |
| プラン名 | | Microsoft 365 Apps for business | Microsoft 365 Business Basic | Microsoft 365 Business Standard | Microsoft 365 Business Premium |
| 参考価格(1ユーザー) | 月額（年契約月払い） | 1,030 | 750 | 1,560 | 2,750 |
| | 年額（年契約年払い） | 12,360 | 9,000 | 18,720 | 33,000 |
| Officeアプリケーション(Business)<br>（1ユーザーができるインストール可能台数） | ※Windows PCのみ利用可<br>1ユーザー計15台（デスクトップ5台、タブレット5台、スマホ5台） | ● | | ● | ● |
| Office Online | Webブラウザで利用できるOffice（ ） | ● | ● | ● | ● |
| One Drive for Business | 個人用ストレージ（1TB/ユーザー毎） | ● | ● | ● | ● |
| Exchange Online | Exchange Online Plan1(メール容量50GB/1ユーザー) | | ● | ● | ● |
| SharePoint Online | 組織ポータルサイト(1TB+(10GB×ユーザー数)=合計容量 | | ● | ● | ● |
| Yammer | 法人向けSNS | | ● | ● | ● |
| Microsoft Teams | IM、Web通話、Web会議、ファイル共有アプリケーション | | ● | ● | ● |
| Power Apps | ローコードアプリケーション開発 | | ● | ● | ● |
| Power Automate | プロセス自動化ツール | | クラウドフローのみ | クラウドフローのみ | ● |
| Azure AD Premium P1 | ID とアクセス管理 | | | | ● |
| Microsoft Intune | デバイスとアプリの管理 | | | | ● |
| Azure Information Protection P1 | 情報の保護 | | | | ● |
| Microsoft Defender for Office365 | 脅威からの保護 | | | | ● |
| Microsoft Defender for Business | クライアント端末セキュリティ（EDR） | | | | ● |

※記載価格は推定小売価格（税抜）になります。
※2023年4月現在でのBusinessプラン一覧になります。

# TD SYNNEX によるパートナー様支援

## -導入支援サービス

# EMS導入支援パッケージ

EMS (Enterprise  Mobility + Security) 導入支援パッケージ

| パッケージ名 | Security Standard | Security Premium | 内容 |
|---|---|---|---|
| ヒアリング | ○ | 案件毎にサービスをカスタマイズ | 弊社指定のヒアリングシートに必要事項を記載いただきます。 |
| 条件付きアクセス構成 | ○ | | コンプライアンスポリシー準拠デバイスおよびIPアドレスによる制御を前提とした条件付きアクセスを構成します。 |
| コンプライアンスポリシー作成 | ○ | | 利用デバイスに対するコンプライアンスポリシーを作成します。<br>作成対象はWin10、iOS、Android を前提としております。 |
| 管理者向けトレーニングの実施 | ○ | | 弊社作成のポリシー改編方法やその適用についてなどが記載されたマニュアルのご提供と管理者向けトレーニングを実施いたします。 |
| 導入コンサルティング | ○ | | 経験豊富は専任コンサルタントがお客様環境に合わせたベストな導入をご提案いたします。 |
| 展開支援 | - | | 本番展開に向けた設定変更・適用作業を弊社エンジニアがお客様に代わり対応いたします。 |
| アフターフォロー | - | | 本番展開後における期間限定のアフターフォローサービスとなります。<br>運用フェーズでの各種ご質問に弊社エンジニアが回答いたします。 |

※ 作成する条件付きアクセスポリシーは基本アクセスポリシー x 1と例外ブロックポリシー x 1を前提としております。
※ 作成するコンプライアンスポリシーは、Win10 x 1、iOS or Android x 1を前提としております。
※ プロジェクト期間はご注文から概ね2ヶ月間を前提としております

# その他オプション

| オプション | 内容 |
| --- | --- |
| デバイス構成プロファイル設定 | Intune登録されたWin10デバイスへ各種設定を行うための構成プロファイルを作成し、配布を行います。 |
| Apple Business Manager<br>連携 | Apple Business Manager(ABM)とIntuneの連携を行います。<br>Intuneへのデバイス登録、ABMで購入したアプリの管理、作成済みの構成プロフィアルの配布設定等を対応します。 |
| BYOD 設定<br>(MAMポリシー作成) | BYOD(iOS、Android)で業務アプリを使用する際に情報漏洩を防止するためのMAMポリシーを作成します。<br>Intune MAM対応アプリであれば、基本的に対応可能です。 |
| ゼロタッチデプロイ (Autopilot)<br>導入支援 | Autopilotテクノロジを使用したWin10デバイスのゼロタッチデプロイを設定します。<br>ゼロタッチによるAzureADデバイス登録と、各種アプリ・構成の配布について設定を行います。 |
| AIP (Azure Information Protection)<br>導入支援 | 秘密度ラベルの作成、運用方法について支援します。<br>秘密度ラベルとデータ損失防止 (DLP)の連携についても対応します。 |
| EMS 運用技術支援 | EMS各種製品の運用及び製品間連携を技術支援します。<br>セキュリティセンター、コンプライアンスセンターの利活用についても運用面、技術面から支援します。 |

※ 提供価格については別途お問合せください。

# Microsoft Defender 導入支援

TD SYNNEX

## Defender for Business 導入支援

初期セットアップ
管理者マニュアル
管理者トレーニング

## Defender for Office 365 導入支援

初期セットアップ
管理者マニュアル
管理者トレーニング

## データバックアップ導入支援

初期セットアップ
管理者マニュアル
管理者トレーニング

## マルウェア対策パッケージ

初期セットアップ
管理者マニュアル
管理者トレーニング

# 監視レポート/リモート運用代行サービスについて

TD SYNNEX

## 監視レポート

| 1次レポート | 2次レポート | 月次レポート | お問い合わせ対応 | バイリンガルサポート |
|---|---|---|---|---|
| アラート発生後<br>1時間以内に<br>1次レポートをご提供<br>(24時間365日/メール) | 発生したアラートを<br>エンジニアが分析し、<br>誤検知やマルウェアの感染<br>など事象を明確にします | 月初から5営業日以内に<br>月次レポートをご提供 | ご提供したレポートに関するお問合せに回答します<br>(平日9:00-17:00/メール/含バイリンガル) | 日本語、英語によるレポートのご提供及び、メールでのサポートを受け付けます。 |

## リモート運用代行

| 業務代行 | レポート分析・対応 | 端末隔離 | ポリシー変更 | その他 |
|---|---|---|---|---|
| セキュリティに精通したスペシャリストがDefender運用担当者として業務を代行いたします | 監視レポートの分析や<br>対策検討と<br>必要な作業の実施 | インシデント発生時に危険度が高いと判断された端末を隔離し、インシデント処理後、隔離から解放し再接続します | 誤検知や過検知が発生した場合、ポリシー変更、保護設定、許可リスト、除外設定等の業務を代行 | ポリシー見直し、<br>PC入替時に伴う作業など<br>必要となる作業代行 |

# まとめ

サイバー攻撃の標的となっている**中小企業**では、**セキュリティ対策**が欠かせない

**Microsoft** はセキュリティの**エキスパート**
- ✓ 1年間で阻止したメール攻撃の数、**約300億**
- ✓ 今後5年間でセキュリティ分野に**200億ドルの投資**
- ✓ 複数の評価機関から**リーダー**として認定

**セキュリティツール**を Microsoft で**統一**すると管理工数が大幅削減

**EMS**はアクセス制御・デバイス制御・ドキュメント保護の**3つ**がセットになったプラン

Microsoft Defender **for Office 365** は**サンドボックス機能**を提供

Microsoft Defender **for Business** は**EDR機能**を提供

Microsoft 365 を選ぶなら、セキュリティ機能もついた
**Microsoft 365 Business Premium**がおすすめ

TD SYNNEXなら**導入支援**・運用支援も**ご提供**可能

# お問い合わせ窓口について

## 営業担当

**お見積り**依頼
**請求**に関するお問い合わせ
**永続ライセンス**のお問い合わせ

## CSP専門チーム
## BD、エンジニア

**CSP クラウド相談デスク**
jp_microsoftcsp@tdsynnex.com

**お手数ですが営業担当を**
**CCに入れて送信ください。**

**MSクラウド案件**に関するご相談
プラン選定、機能仕様確認
ライセンスに関するご質問
勉強会対応、案件同行対応

## StreamOne Stellr サポート

StreamOne Stellr Support
streamonestellr_jp@tdsynnex.com

※弊社営業時間内での
対応とさせて頂きます。

**StreamOne Stellr操作**に関するご質問
処理エラーについてのご質問
既存テナントの紐づけ依頼


Thank You