クラウドに新しい力をプラスする

AZ Power

ゼロトラストで実現する
次世代のセキュリティ戦略
～Microsoft365活用の鍵～

Microsoft
Solutions Partner

AZPower株式会社はMicrosoft AI Cloud Partner ProgramのSolutions Partnerです。

はじめに

本日の予定

1. 会社紹介

2. ゼロトラストモデルの基本概念

3. ゼロトラストモデルのサンプル事例

4. AZPowerソリューション紹介

5. 無料相談会・アセスメントサービスご紹介

6. まとめ

自己紹介

AZPower株式会社
Manager
Sales Division

磯木　雄斗

y.isoki@azpower.co.jp

〒101-0047
東京都千代田区内神田２丁目４－２
一広グローバルビル
https://azpower.co.jp

Microsoft Solutions Partner

略歴

Azure・Microsoft365のソリューション提案を専門とし、企業のデジタルトランスフォーメーションを支援。

AZPowerに参画し、クラウド技術の活用による業務効率化に向けた戦略を提供しております。

以下のようなマイクロソフトソリューションの提案および対応実績があります。（一部抜粋）

- ✓ 法律事務所様向けゼロトラストセキュリティ提案
- ✓ 配送業向けAzure Virtual Desktop提案
- ✓ 警備業向けAzure環境構築提案
- ✓ 流通業向けAzure OpenAI Service提案

保有資格 / 実績

◆ 資格

- Azure Fundamentals【AZ-900】
- Microsoft 365 Certified: Fundamentals【MS-900】
- AI Fundamentals【AI-900】
- Azure Data Fundamentals【DP-900】
- Security,Compliance,and Identity Fundamentals【SC-900】
- Power Platform Fundamentals【PL-900】

会社概要

コア・バリュー　　クラウドに新しい力（価値）をプラスしてお客様のビジネスを変革します

会社名	AZPower株式会社
本社住所	〒101-0047 東京都千代田区内神田２丁目４ 一広グローバルビル
資本金	332,500,000円
事業種別	生成AIを活用したインテグレーションサービス事業 クラウドインテグレーションサービス事業 マイクロソフトクラウドのリセール事業

AZPowre株式会社は、Microsoftが推奨するAzure OpenAI Service リファレンスアーキテクチャ 賛同パートナーです。

https://www.microsoft.com/ja-jp/biz/find-new-value-on-azure/ai-biz.aspx

Microsoftとのパートナーシップについて
Solutions Partner

Microsoft Solutions Partner

- ✓ インフラストラクチャ
- ✓ デジタルおよびアプリイノベーション
- ✓ データと AI
- ✓ セキュリティ
- ✓ モダン ワーク

AZPowerはマイクロソフト社より6分野中5つの分野で
Solutions Partnerとして認定されております。

Azure領域

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Data & AI
Azure

Microsoft365 & Azure領域

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Security

MicrosoftとのパートナーシップについてSpecialization

Specialization

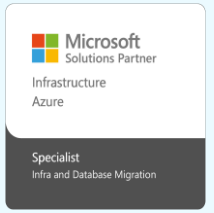
特定のソリューション分野おいて高度な専門性を有し、卓越した能力を持つパートナーであることを第三者機関の審査を経て表すマイクロソフトの制度

Solutions Partnerの上位資格として「高度な専門性を有する企業」を認定する「Specialization」を取得しております。

2024年7月、AIおよびML分野でのSpecialization取得。

AZPowerはマイクロソフト社の「Specialization」を日本ではじめて取得したパートナーです。

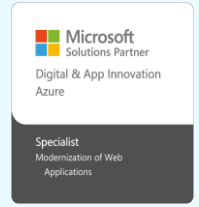
Azureのインフラ分野での高度な専門性



2020年10月9日、国内パートナーとして第一号の取得。

＋

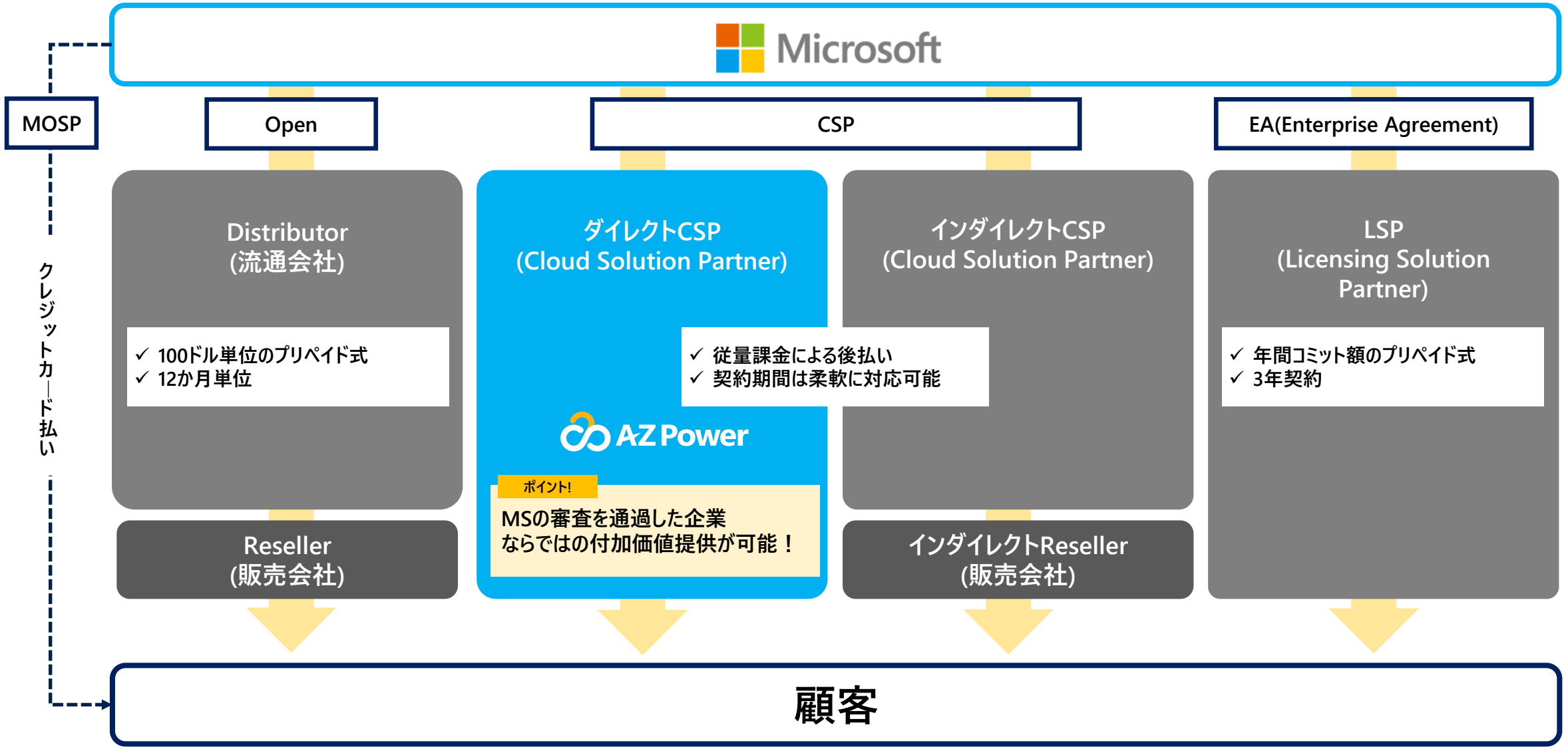
Azureにおけるアプリケーション開発分野での高度な専門性



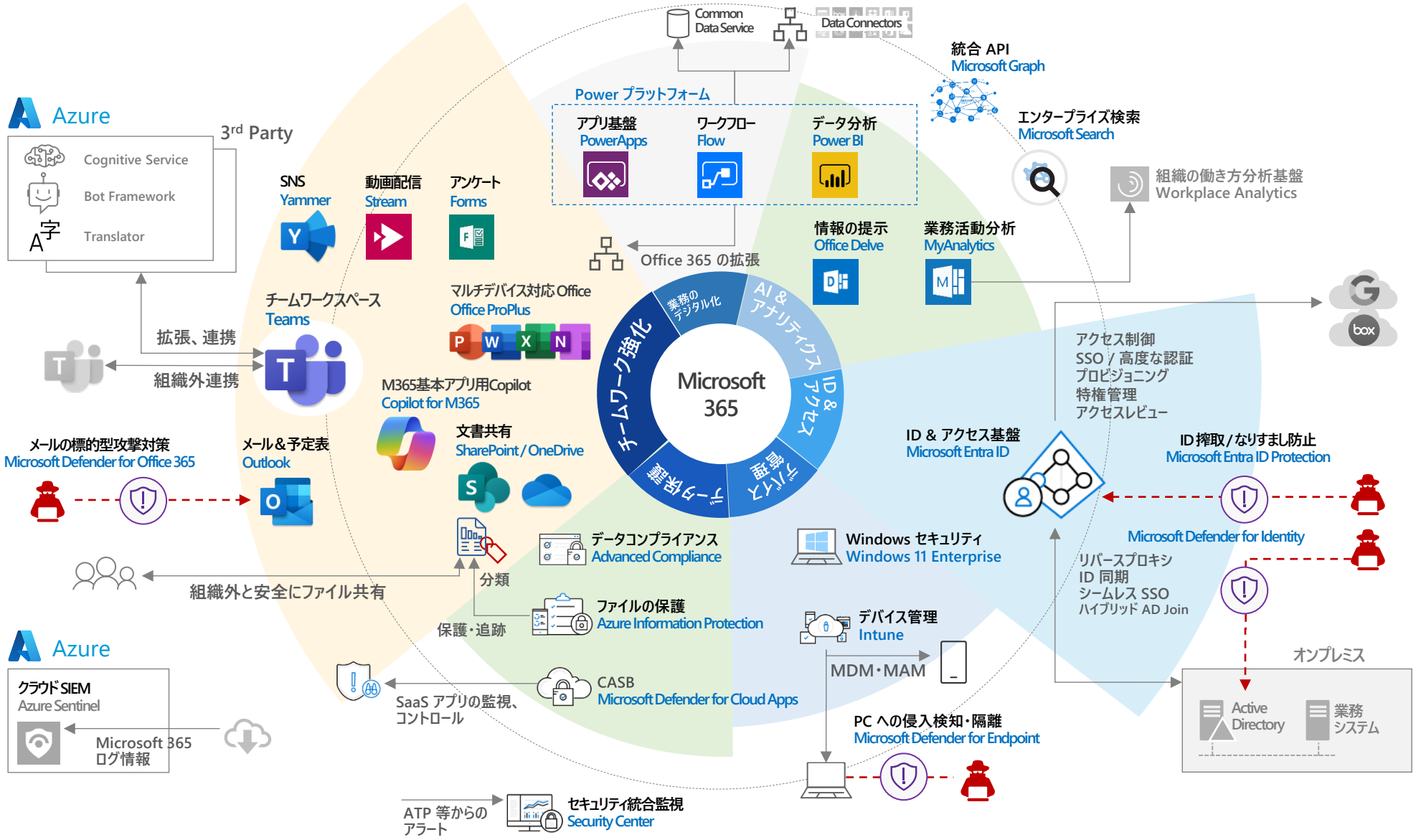
2021年7月6日取得、インフラ分野に続いて2つ目の取得。

AZPowerは「Solutions Partner」および「Specialization」からMicrosoft製品を適正に取り扱うことのできるパートナーとして認定されています。
Azure・Micorosoft365 専門のクラウドインテグレーターとして、安心してお客様のMicrosoft Cloud活用をワンストップでおまかせください。

ダイレクトCSPパートナーについて

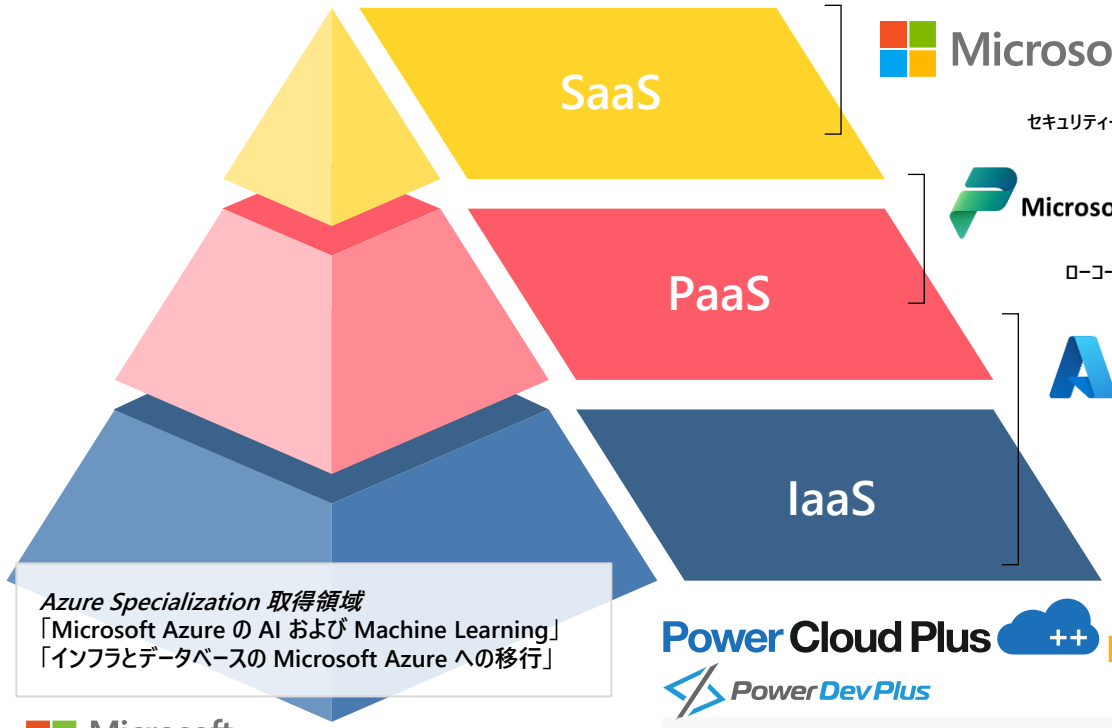


Microsoft365 全体像



AZPower 事業領域

Azure・M365ソリューションを活用したクラウドインテグレーションサービス



Microsoft 365
セキュリティー ＋ O365

Microsoft Power Platform
ローコード／ノーコード／RPA

Azure
IaaS ＋ PaaS

Azure Specialization 取得領域
「Microsoft Azure の AI および Machine Learning」
「インフラとデータベースの Microsoft Azure への移行」

Microsoft Solutions Partner

MS資格取得数 36分野 171資格

Power Cloud Plus ++
Power Support PLUS
Powered by AZ Power
PowerDevPlus

- ネットワーク、ID管理を強みとしたインテグレーションサービス
- フルクラウドオフィスリファレンス
- Azure、M365ライセンス提供 (CSP)
- PaaSを活用したフルクラウドアプリ開発
- クラウドサポート

PaaSを活用した独自開発アプリケーション

PowerGenAI
Integration with Azure OpenAI Service
Azure OpenAI Serviceを利用した
企業専用ChatGPTインテグレーションサービス

Learning Platform
PowerSKILL
カスタマイズ自由
大企業向けクラウド型LMSサービス

CREW SYSTEMS
クラウド型AI監視カメラサービス

PaaSを組み合わせ、拡張性や柔軟性の高い
アプリケーションを弊社独自で開発しております。

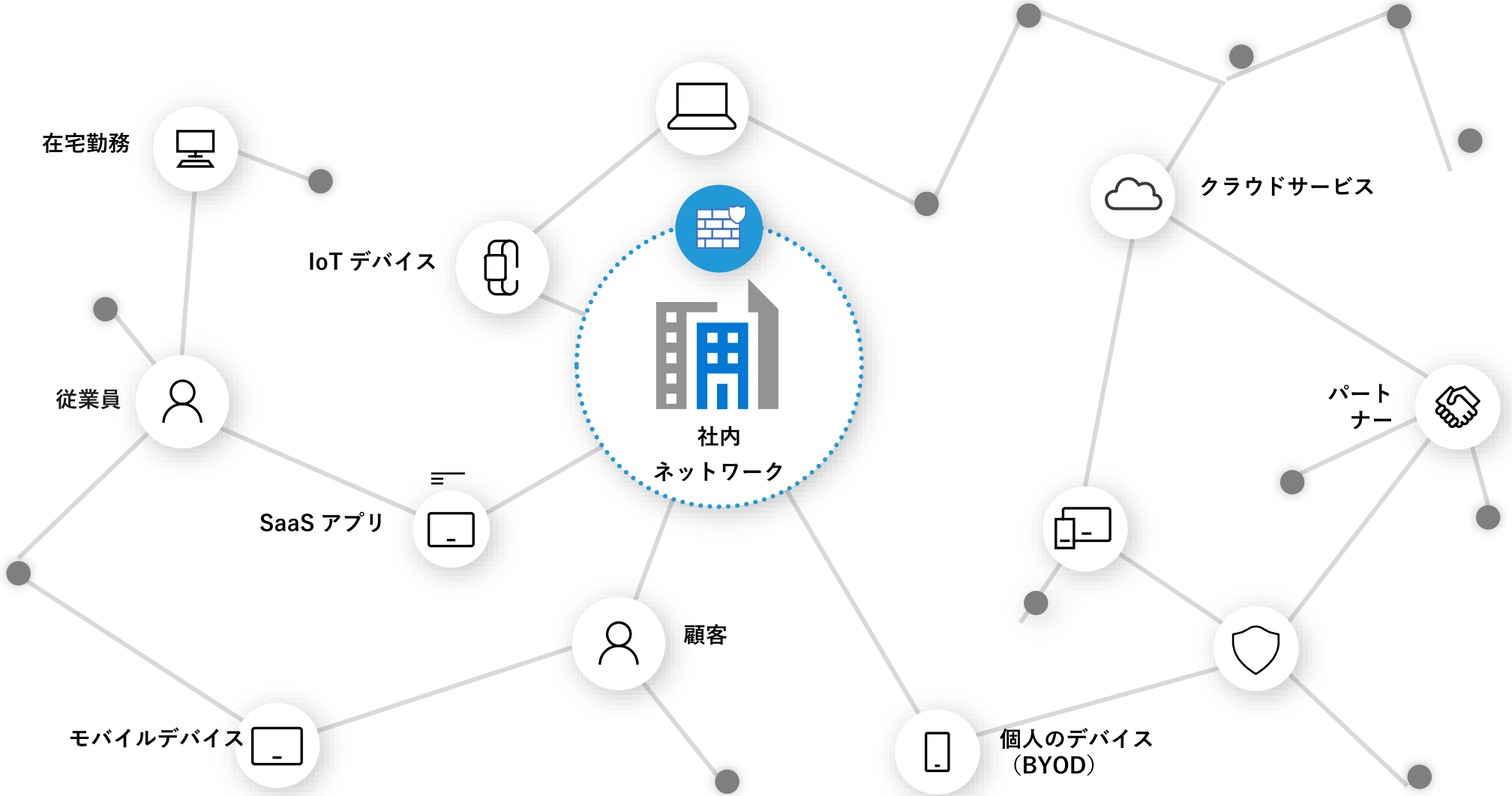
市場からニーズの多い生成AIのチャットアプリ、
社内外の情報を組み合わせ学習管理が行える
LMS、場所問わず一元管理が可能なクラウド管理
型の監視カメラサービスを展開しております。

ゼロトラストモデルの基本概念

IT を取り巻く社会環境の変化

働き方の変化

Covid-19 以降、リモートワークのニーズが急速に高まる



中堅中小企業の主な課題

分散型ワークを改善

セキュリティを確保

コストを削減

さまざまな場所で
働く従業員

多くの個人用
モバイル デバイス

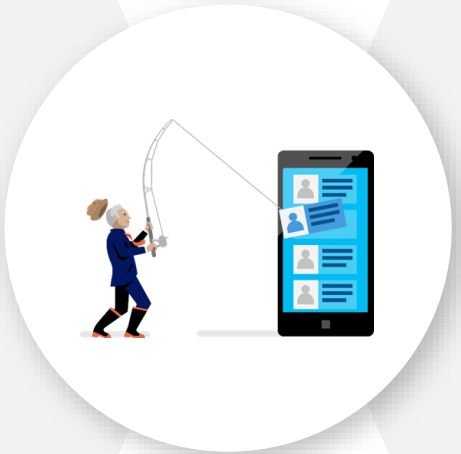
フィッシングや
ランサムウェアの増加

中堅・中小企業を標的とするランサムウェアなどのサイバー攻撃が増えている

COVID-19 に便乗する悪質なサイバー攻撃者

「... サイバー犯罪者は、個人、中堅中小企業、大規模組織を標的として COVID-19 に関連する詐欺やフィッシング メールの送信を行っています」

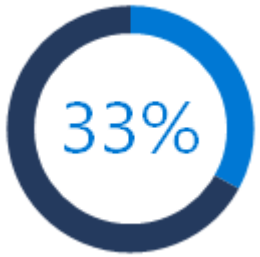
米国国土安全保障省、2020 年 4 月 8 日、CISA Alert (AA20-099A) (英語)



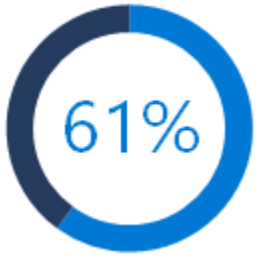
ランサムウェア攻撃の増加

「... ランサムウェアの被害者の約半分 ～ 3/4 は小規模企業で、全体として ランサムウェア攻撃はこの 1 年間で 約 300% 増加しています」

米国国土安全保障省長官 Alejandro Mayorkas 氏、2021 年 05 月 06 日、ABC 報道 (英語)



全サイバー攻撃の **1/3** は小規模企業が標的[1]



最近サイバー攻撃を受けた小規模企業の 61% は業務を停止[2]

10.8 万ドル

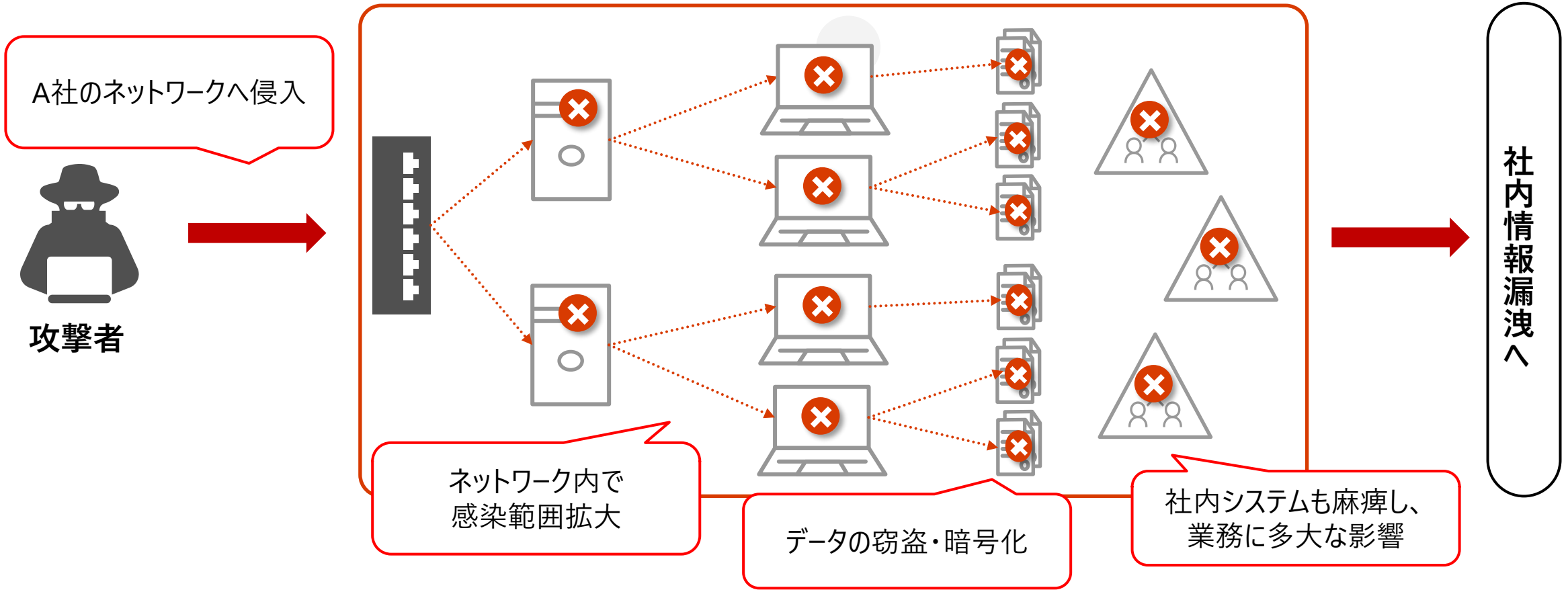
SMB のデータ侵害の平均被害額[3]

出典: 1 「Introduction to the 2020 DBIR」、Verizon Enterprise Solutions (英語) | 2 マイクロソフトの委託による Forrester の調査、2020 年 | 3 Kaspersky、「Global Corporate IT Security Risks Survey」、2019 年 (英語)

A社におけるサイバー攻撃(ランサムウェア)の事例

時系列

①ネットワークへ侵入・ランサムウェア送信 → ②ランサムウェア感染・データ暗号化 → ③データ復旧と引き換えに金銭要求 → ④データ公開と引き換えに金銭要求



これからの時代の
新しいセキュリティモデル＝ゼロトラストモデル

「境界型ネットワーク・セキュリティの限界」とされる今こそ、
新しい時代のセキュリティモデルを

「守られた領域はない」＝ 0 trust
ZERO

Office 365　Azure

0 trust
ZERO
×
Microsoft 365

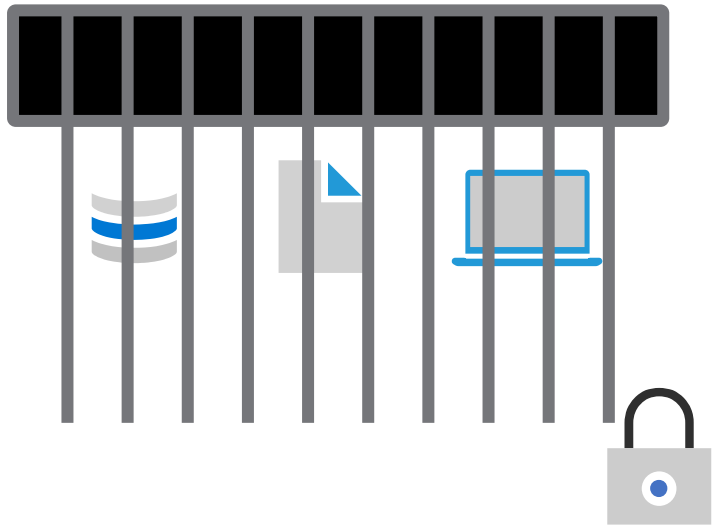
ゼロトラストとは??

- 特定の技術や製品、ソリューションを指す言葉ではありません。
- ネットワークロケーションをベースとしたデバイスやユーザーを**暗黙的に信頼せず**
  常にアクセスの信頼性を検証することで情報資産を保護する**セキュリティの考え方・概念・戦略**の事です。

従来の境界防御との違い

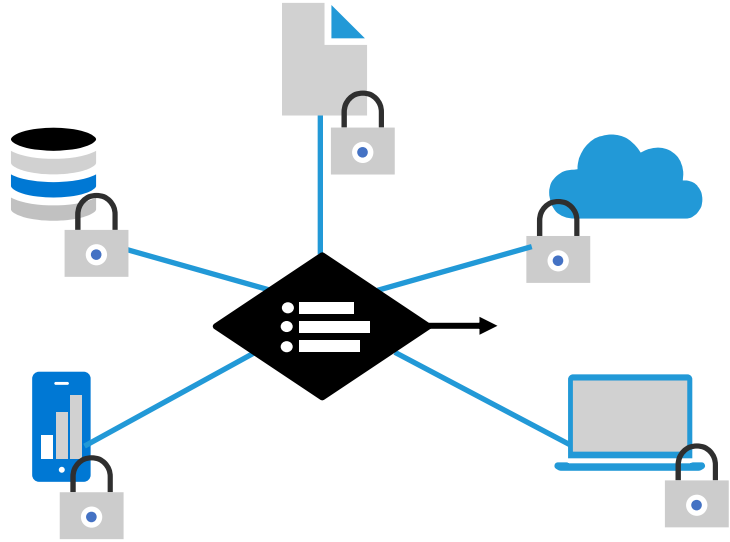
セキュリティを簡素化し、より効果的にする

ゼロトラストとは、ネットワークロケーションをベースとしたデバイスやユーザーを暗黙的に信頼せず、常にアクセスの信頼性を検証することで情報資産を保護するセキュリティの考え方・概念・戦略の事です。



従来型のアプローチ（境界防御）

全ての物を “セキュア” ネットワークで制限



ゼロトラスト

ポリシーを用いてどこでも資産を保護

ゼロ トラストは優れたセキュリティの基盤

ID を保護、管理

マルチプラットフォームで
脅威から防御

データ資産全体にわたり
機密情報を保護

- 多要素認証により、パスワードの紛失や盗難時の不正アクセスからデータを保護します。
- 高度なサイバー脅威を防ぎ、フィッシング、ランサムウェア、データ損失に対するエンタープライズ レベルの保護でビジネス データを守ります。

Microsoft製品(一部抜粋)


Microsoft Defender


Microsoft Intune


Azure Information Protection


Microsoft Entra ID

上記のセキュリティ基盤の構築を実現するソリューションについて次ページ以降ご説明いたします。

中堅中小企業向けの Microsoft 365 オファー

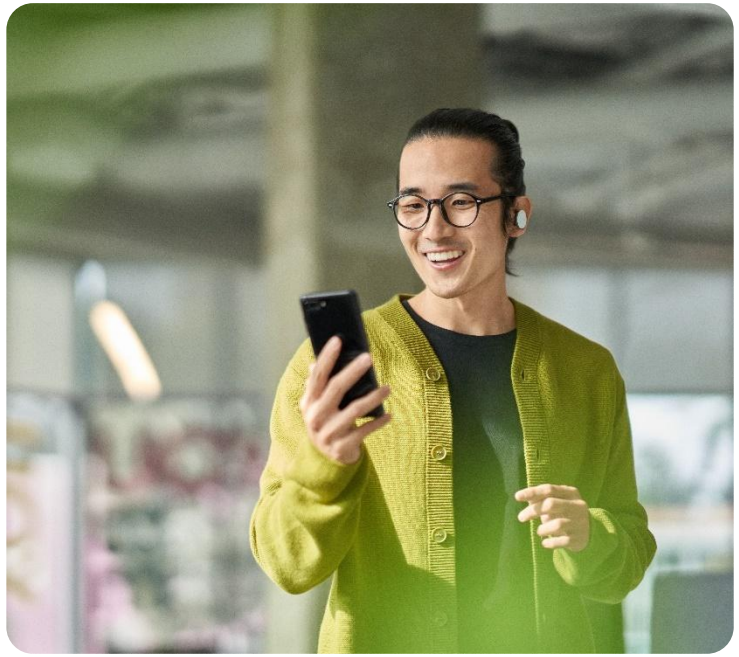
いますぐ安全・安心にウェブ会議を	チームワークをリーズナブルに	業務効率化を実現	業務効率とコミュニケーションを最大化	推奨！ 管理の効率化と最新セキュリティ
Microsoft Teams Essentials	**Microsoft 365 Business Basic**	**Microsoft 365 Business Apps for business**	**Microsoft 365 Business Standard**	**Microsoft 365 Business Premium**
Microsoft 365 アプリケーション オンライン版 Office	Microsoft 365 アプリケーション オンライン版 Office	Microsoft 365 アプリケーション モバイルアプリ対応 1ユーザーあたりPC・Mac5台、スマートフォン 5 台、タブレット 5 台まで利用可能。	Microsoft 365 アプリケーション モバイルアプリ対応 1ユーザーあたりPC・Mac5台、スマートフォン 5 台、タブレット 5 台まで利用可能。	Microsoft 365 アプリケーション モバイルアプリ対応 1ユーザーあたりPC・Mac5台、スマートフォン 5 台、タブレット 5 台まで利用可能。
含まれるサービス	含まれるサービス	含まれるサービス	含まれるサービス AI ビジネス向けAIチャット ～業務データを入力しても安心！ 入力データ、出力結果は保存・利用されません	含まれるサービス AI ビジネス向けAIチャット ～業務データを入力しても安心！ 入力データ、出力結果は保存・利用されません 管理・セキュリティ **デバイスとセキュリティの一元管理**、情報漏えい対策、PC 自動セットアップツール、管理ポータルなど、これまで大企業でしか利用できなかった**堅牢なセキュリティ環境を提供**。

Microsoft 365 Business Premium のメリット

どこからでも安心して仕事ができる

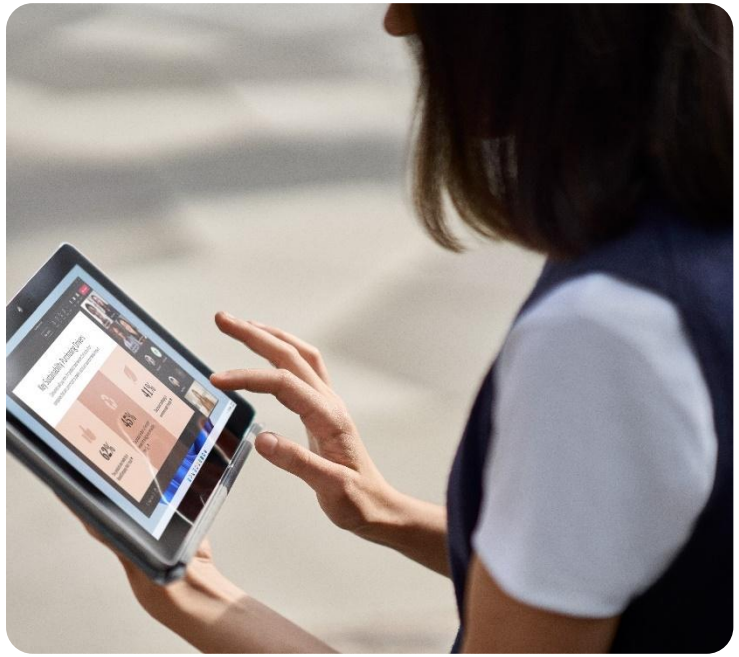
充実した機能と使いやすさ

- 1 つのソリューションで生産性とセキュリティを両立
- クラウド プラットフォームのため導入が簡単
- すぐに使用を開始できる



コスト削減

- 複数のポイント ソリューションにかかるコストを回避
- ヘルプデスクのコストを削減
- ライセンスの複雑さを解消



エンタープライズ レベルのテクノロジ

- 多くのエンタープライズから信頼を得る統合セキュリティ
- AI を活用した脅威インテリジェンス
- 評価の高いセキュリティ ベンダー

世界最大・最高品質水準のマイクロソフト セキュリティについて

Microsoftは世界中で稼働しているMicrosoft 製品を通して、防犯センサーのようにサイバー攻撃を地球規模で監視し、24時間 365日体制で AI+セキュリティ専門家が対応しています。また第三者機関からも最高レベルの評価を獲得した世界最高水準のセキュリティ技術を提供しています。

今後 5 年間で **200 億ドル**
(約 2.5 兆円)**の投資**

サイバーセキュリティーセンターにて
24 時間 365 日体制で脅威に対する
リアルタイムでの保護、検出、対応

Windows	Azure	Xbox	ID	メール	ドキュメント	Web
12 億以上	10 億以上	6,500 万以上	6,300 億以上	4,700 億以上	6,000 億以上	180 億以上
プラットフォーム			トランザクション			

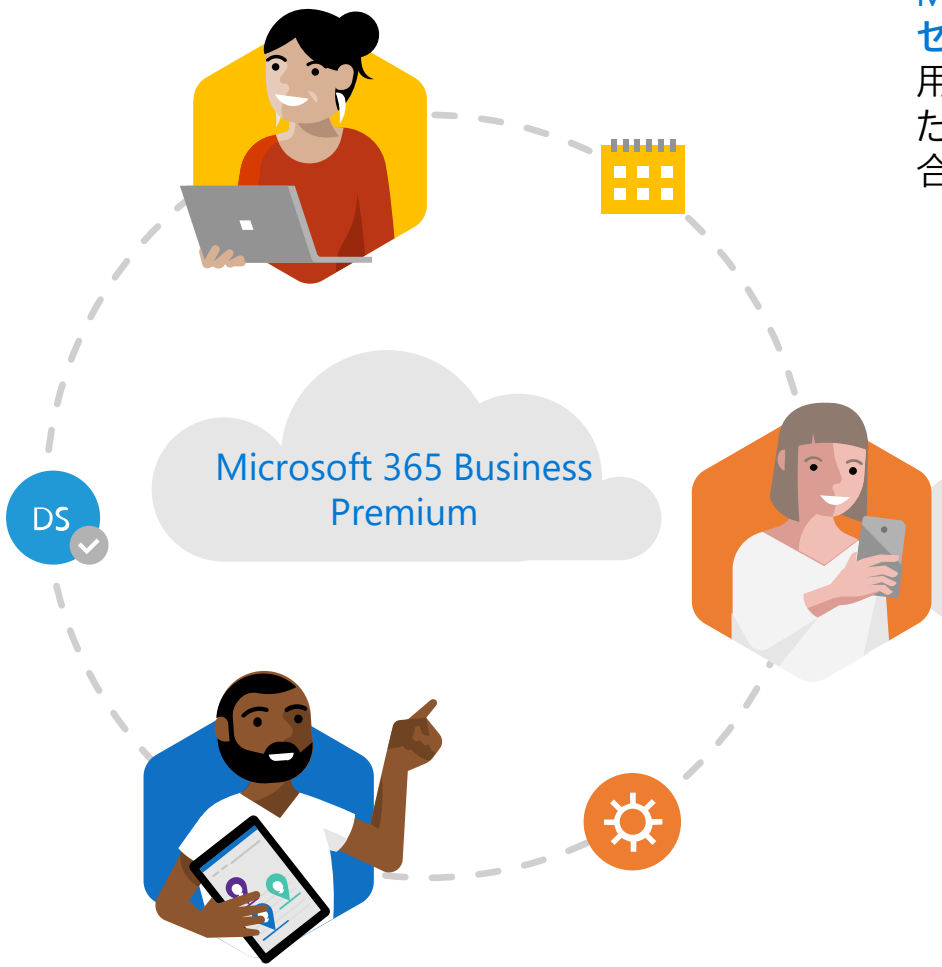
86万
サイバー攻撃の被害にあわない
ように保護している組織数

65兆
日々分析する
脅威シグナル数

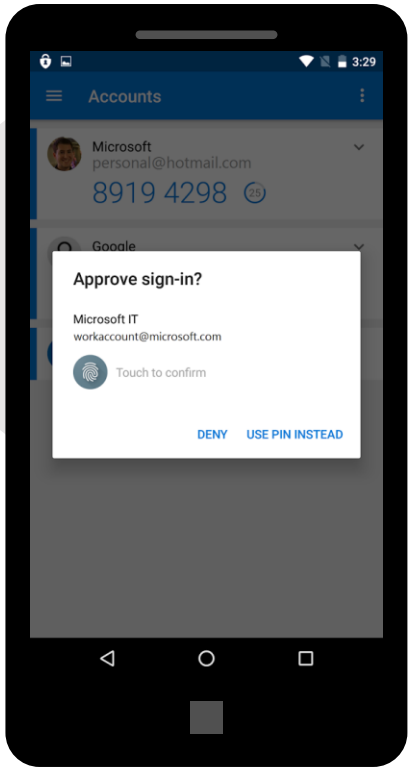
370億
昨年阻止した
E メールの脅威数

275万
犯罪に関連する
Webサイトをブロックした数

業務データへの安全なアクセス



Microsoft 365 Business Premium では、高度な多要素認証 (MFA) と条件付きアクセス ポリシーを適用し、必要なときに必要な場所から適切なユーザーだけが業務データを利用できるようにします。
たとえば、条件付きアクセスや MFA により、取引のない国からログインの試行があった場合に、アクセスをブロックしたり、追加の認証を要求したりするポリシーを設定できます。



Microsoft Entra ID Premium Plan 1

ID およびアクセス ガバナンス

多要素認証

条件付きアクセス ポリシー

99% 多要素認証で阻止できる ID 攻撃の割合[1]

出典: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ (英語) (マイクロソフトの社内調査に基づく)

個人デバイス上の業務データの保護

Microsoft 365 Business Premium **では、Intune アプリ保護ポリシーを設定**することで、業務アプリと個人アプリを分離できます。管理者は、業務上のドキュメントや添付ファイルを OneDrive for Business といった承認済みの安全な業務ファイル共有のみに保存するように指定して、機密情報を保護できます。

58%

適切なセキュリティ プロトコルが設定されている従業員デバイスの割合。すべての従業員を対象にセキュリティ トレーニングを実施していると回答したのは全体の 1/5 未満[1]

出典: マイクロソフトの委託による Forrester Consulting の調査、2019 年 10 月に SMB (従業員数 1 ～ 499 人) を対象に行った調査

ランサムウェアからの保護

Microsoft 365 Business Premium では、Microsoft Defender などの機能によってデバイスを保護します。

Microsoft Defender が、[デスクトップ] や [ドキュメント] などの使用頻度の高いフォルダーへの不正アクセスを防止します。

つまり、不正なアプリ、スクリプト、実行ファイルによるアクセスが不可能になるので、フォルダーに格納されているファイルを暗号化しようとするランサムウェアもブロックされます。

ランサムウェア
攻撃に関連するダウンタイムの平均被害額の上昇率[1]

94%

※2020年度

Microsoft 365 Business Premium

Microsoft 365 Business Premium でランサムウェア被害を防ぐ 3 つの方法

①不審な差出人からのメールのサンドボックスと安全なリンク

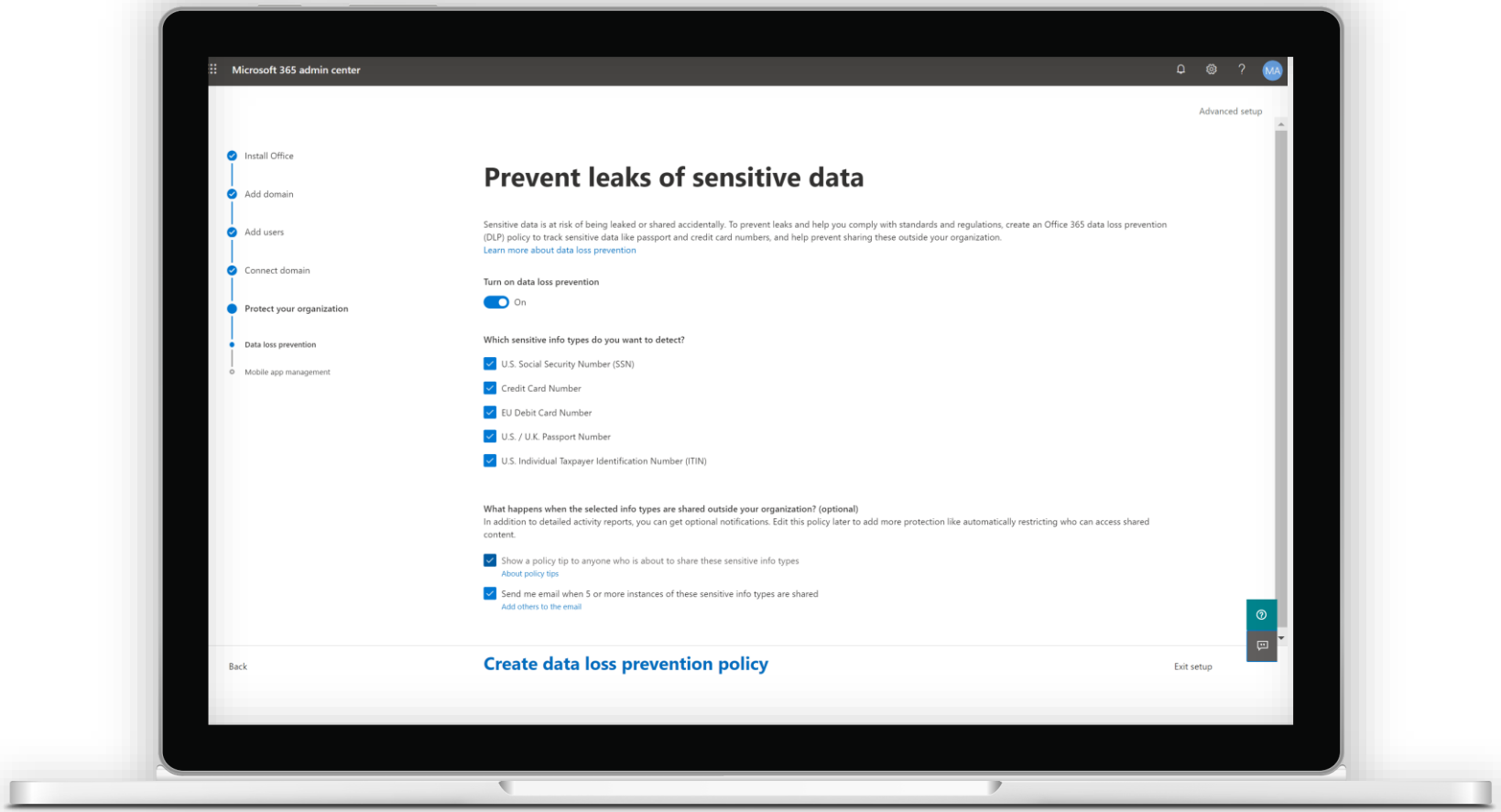
②Microsoft Defender ATP のデバイス保護

③OneDrive for Business によるファイル回復

出典: 「Datto's 2020 Global State of the Channel Ransomware Report (英語)」、世界各地の MSP 1,000 社以上への調査の統計

機密データの保護

Microsoft 365 Business Premium **では、データ損失防止などの高度な機能や Azure Information Protection を利用**して、顧客情報や従業員情報、業務上の機密データ、社会保障番号、クレジット カード番号などの機密データを分類して保護できます。



55% 以上

従業員が個人デバイスにデータを残したまま退職することを懸念していると回答した SMB の割合[1]

出典: SMB (従業員数 2 ～ 299 人) を対象に行ったマイクロソフトの社内調査

M365 を利活用したセキュリティ対策について

	事前対策		事後対策		
NIST サイバーセキュリティフレームワーク	IDENTITY	PROTECT	DETECT	RESPOND	RECOVER
	特定 資産に対する脅威とセキュリティリスクを理解する	**防御** ビジネスを継続するため、資産を脅威から保護する	**検知** セキュリティイベントを確実に検出する	**対応** セキュリティインシデントに適切に対処する	**復旧** 阻害されたものを元の状態に修復する

ユーザID	Microsoft Entra ID P1		Microsoft Entra ID P2
	ID登録・管理	アクセス制御 多要素認証 ◀ 信頼性の評価	クラウドIDに対する攻撃検出、自動調査、自動対処
			Microsoft Defender for Identity
			オンプレミスIDに対する攻撃検出、自動調査
デバイス	Intune		Microsoft Defender for Endpoint
	デバイス登録 /管理(MDM) アプリ登録 / 管理(MAM) 脆弱性の管理(TVM)	盗難対策(暗号化・ワイプ)	デバイスに対する攻撃検出、自動調査、自動対処
		Defender Antivirus	
		既知のウイルス対策	
アプリ	Microsoft Defender for Cloud Apps		
	管理対象アプリの識別(Shadowアプリの検出)		アプリに対する攻撃検出、自動調査、自動対処
メール	Exchange Online Protection		Microsoft Defender for Office365
	管理対象アプリの識別(Shadowアプリの検出)		標的型メール、危険なOfficeファイルの検出、自動調査、自動対処
データ	Microsoft Purview Information Protection		Insider Risk Management
	機密情報のラベリング	機密情報の保護(暗号化)	内部不正(機密情報漏洩や規制違反のリスク等)対策
		Data Protection & Governance	eDiscovery & Audit
		メールやチャット、クラウドストレージ、デバイスからの情報流出の防止(DLP)	Office365監査ログの1年保管

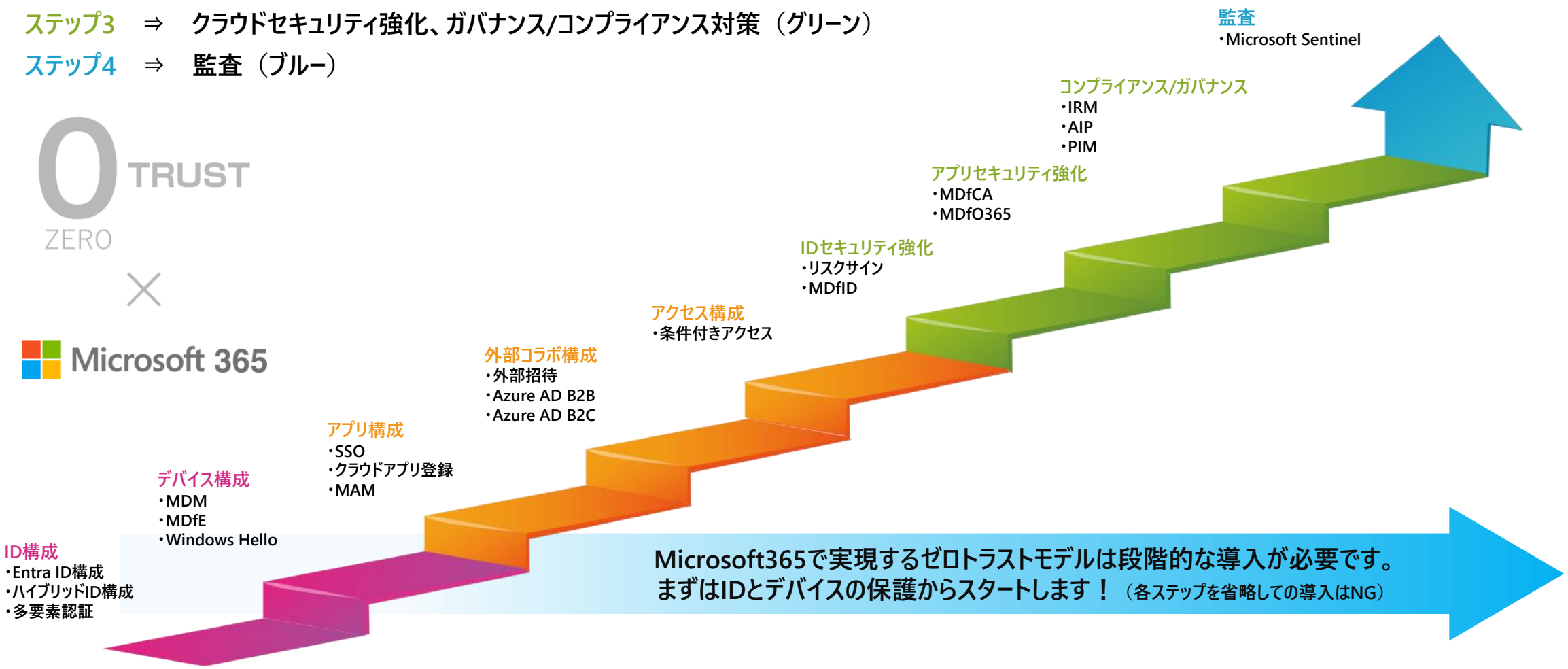
最優先に取り組みべき内容

	事前対策		事後対策		
NIST サイバーセキュリティフレームワーク	IDENTITY	PROTECT	DETECT	RESPOND	RECOVER
	特定 資産に対する脅威とセキュリティリスクを理解する	**防御** ビジネスを継続するため、資産を脅威から保護する	**検知** セキュリティイベントを確実に検出する	**対応** セキュリティインシデントに適切に対処する	**復旧** 阻害されたものを元の状態に修復する

ユーザID	Microsoft Entra ID P1			Microsoft Entra ID P2	
	ID登録・管理	アクセス制御 多要素認証	◀ 信頼性の評価	クラウドIDに対する攻撃検出、自動調査、自動対処	
				Microsoft Defender for Identity	
				オンプレミスIDに対する攻撃検出、自動調査	
デバイス	Intune			Microsoft Defender for Endpoint	
	デバイス登録 /管理(MDM) アプリ登録 / 管理(MAM) 脆弱性の管理(TVM)	盗難対策(暗号化・ワイプ)		デバイスに対する攻撃検出、自動調査、自動対処	
		Defender Antivirus			
		既知のウイルス対策			
アプリ	Microsoft Defender for Cloud Apps				
	管理対象アプリの識別(Shadowアプリの検出)			アプリに対する攻撃検出 自動調査、自動対処	
メール	Exchange Online Protection			Microsoft Defender for Office365	
	管理対象アプリの識別(Shadowアプリの検出)			標的型メール、危険なOfficeファイルの検出、自動調査、自動対処	
データ	Microsoft Purview Information Protection			Insider Risk Management	
	機密情報のラベリング	機密情報の保護(暗号化)		内部不正(機密情報漏洩や規制違反のリスク等)対策	
		Data Protection & Governance		eDiscovery & Audit	
		メールやチャット、クラウドストレージ、デバイスからの情報流出の防止(DLP)		Office365監査ログの1年保管	

ゼロトラスト導入ステップ

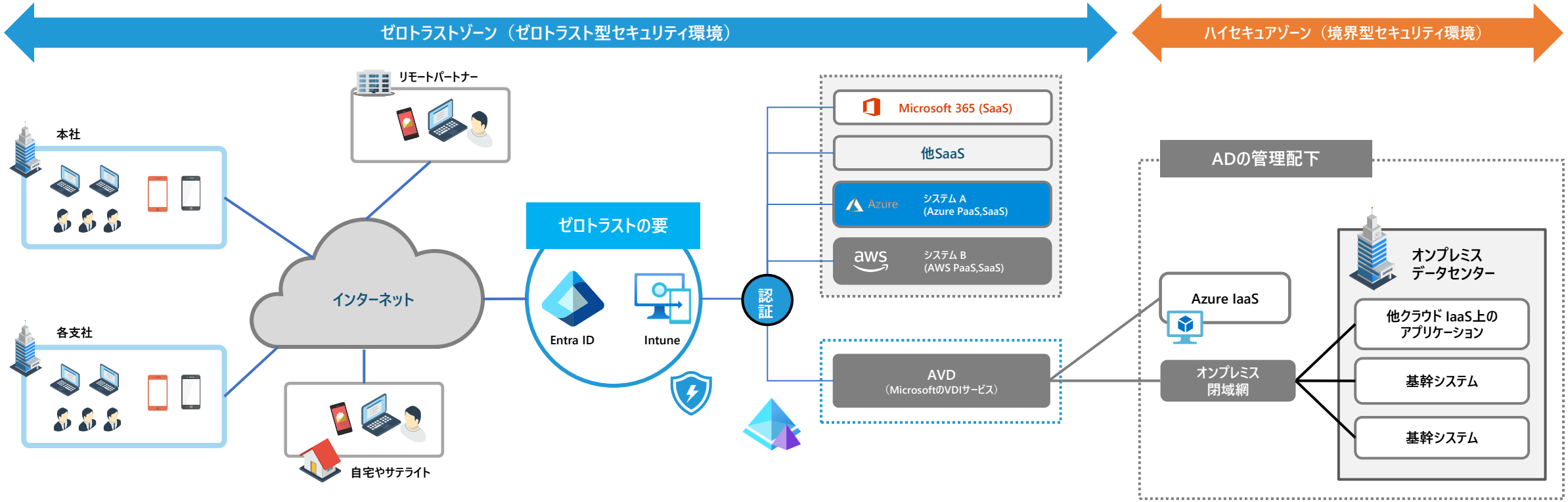
ステップ1 ⇒ ID/デバイス侵害からの保護（ピンク）
ステップ2 ⇒ クラウドアプリへの安全なアクセス（オレンジ）
ステップ3 ⇒ クラウドセキュリティ強化、ガバナンス/コンプライアンス対策（グリーン）
ステップ4 ⇒ 監査（ブルー）



ゼロトラストモデルのサンプル事例

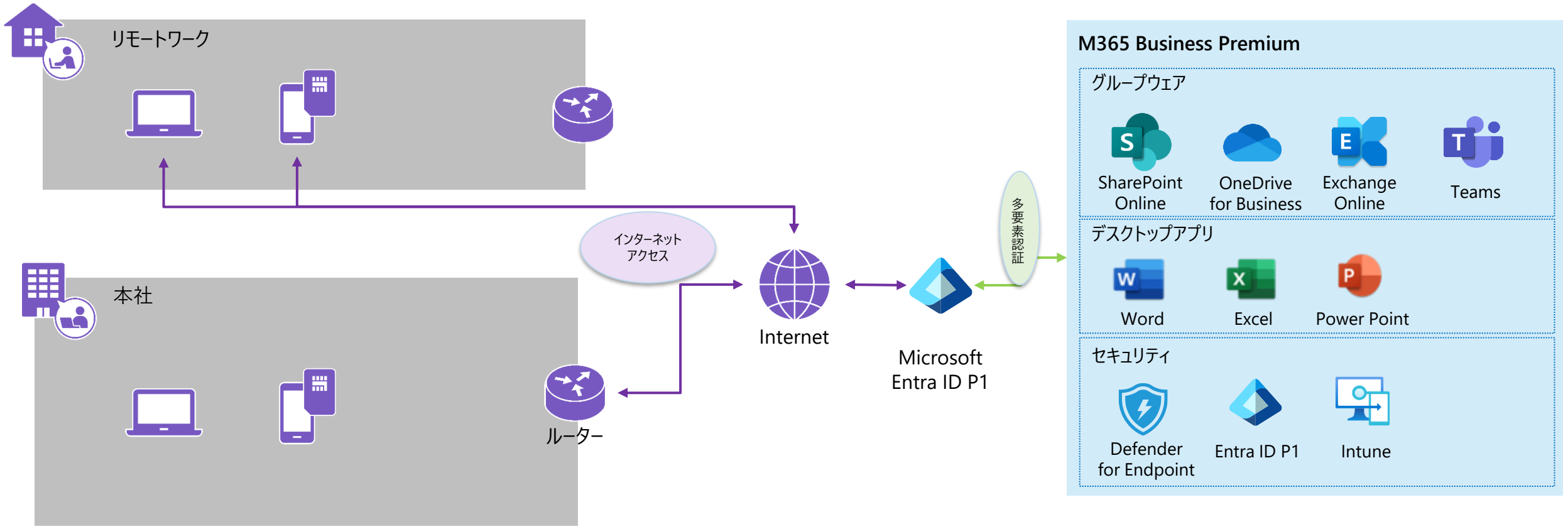
事例1：認証基盤の整備・デバイスとアプリのマイクロセグメンテーション化

- ✓ Microsoft Entra IDとIntuneを要に1人 1 IDを原則とし、ユーザーに紐づく適切なデバイスからの適切なリソースへアクセスを行う環境を実現
- ✓ ゼロトラスト型にできない社内システム・アプリケーションは「ハイセキュアゾーン」に配置
- ✓ 「ハイセキュアゾーン」とは技術的に境界型セキュリティでないと守れない資産を配置するゾーンと定義
- ✓ エンドユーザはゼロトラスト型 FAT 端末を利用し、「ハイセキュアゾーン」へは AVDを利用



事例2：Microsoft365 Business Premiumで実現するゼロトラストセキュリティ

- ✓ Microsoft Entra IDによるクライアント/ID単位での安全性の確保、インターネットを介した社内システムへの安全なアクセスの実現
- ✓ Microsoft Intuneを活用したPC・モバイル管理やポリシーの適用やデバイスのセキュリティ対策の一括管理
- ✓ Defenderによる常時監視/また侵入したウイルスに対する検知・対応・修復



AZPowerソリューション紹介

PowerCloudPlusとは

Power Cloud PLUS

Azure & Microsoft365 Integration Service

Powered by AZ Power

https://pcp.azpower.co.jp/

Microsoft Cloud専門インテグレーターのAZPower株式会社が提供する
クラウドインテグレーションサービスの総称です。

インテグレーション メニュー	認証とセキュリティ	災害復旧と事業継続	リモートワーク環境構築
	連携・統合	Azure IaaSへの移行	ファイルサーバー移行
コンサルテーション メニュー	Azure移行戦略ガイドサービス	Azure最適化レビューサービス	Azureセキュリティ・コンプライアンス 強化サービス
サポートメニュー	Plan A Microsoft Azure Microsoft 365	Plan B Microsoft Azure Microsoft 365	Plan C Microsoft Azure Microsoft 365
			Plan S Microsoft Azure Microsoft 365

インテグレーションメニュー

Azure & Microsoft365
Integration Service

PowerCloud PLUS

Microsoft Entra ID ゼロトラスト導入支援

Microsoft 365

任意のデバイスやアプリケーションからの安全なアクセスを可能にする

あらゆるデバイスやアプリケーションから安全にアクセスするためのソリューションを提供します。信頼しない、常に検証するという原則に基づいたZero Trustモデルを導入し、企業のセキュリティを強化します。これにより、データの保護とビジネスの継続性を確保します。

作業項目	Azureサブスクリプション払出し／Microsoft Entra ID Premium P1 ライセンス払出し／Microsoft Intune ライセンス払出し／Microsoft Entra IDアカウントの作成／要件確認／多要素認証設計／条件付きアクセス設計／デバイスコンプライアンスポリシー設計／管理者向けスキルトランスファー

Endpoint Security 導入支援

Microsoft 365

Microsoft Defender 製品群を活用し、エンドポイントのセキュリティを強化

Microsoft Defender for Business（for Endpoint）によるEDRを構築し、エンドポイント セキュリティ ソリューションで、ランサムウェア、マルウェア、フィッシングなどの脅威からデバイスを保護します

作業項目	Microsoft Defender for Business(Endpoint) ライセンス払出し／ライセンス割当／要件確認／セキュリティ ロール設定／電子メール通知設定／デバイスへのオンボード／管理者向けスキルトランスファー

AVDリモートワークソリューション

Microsoft Azure

Azure Virtual Desktop（AVD）を使ってリモートワーク環境を高速で構築。

Azure Virtual Desktopを活用して迅速にリモートワーク環境を構築します。セキュリティ対策からユーザー教育まで、安全で効率的なリモートワークの実現を全面的にサポートします。

AVD with ゼロトラストセキュリティ

Microsoft Azure　Microsoft 365

AVD ＋ ゼロトラストを用いた、よりセキュアなリモートワーク環境の構築。

Azure Virtual Desktopとゼロトラストモデルを組み合わせて、高度にセキュアなリモートワーク環境を構築します。信頼性と安全性を確保しながら、効率的なリモートワーク体験を提供します。

AVD & M365 統合環境構築

Microsoft Azure　Microsoft 365

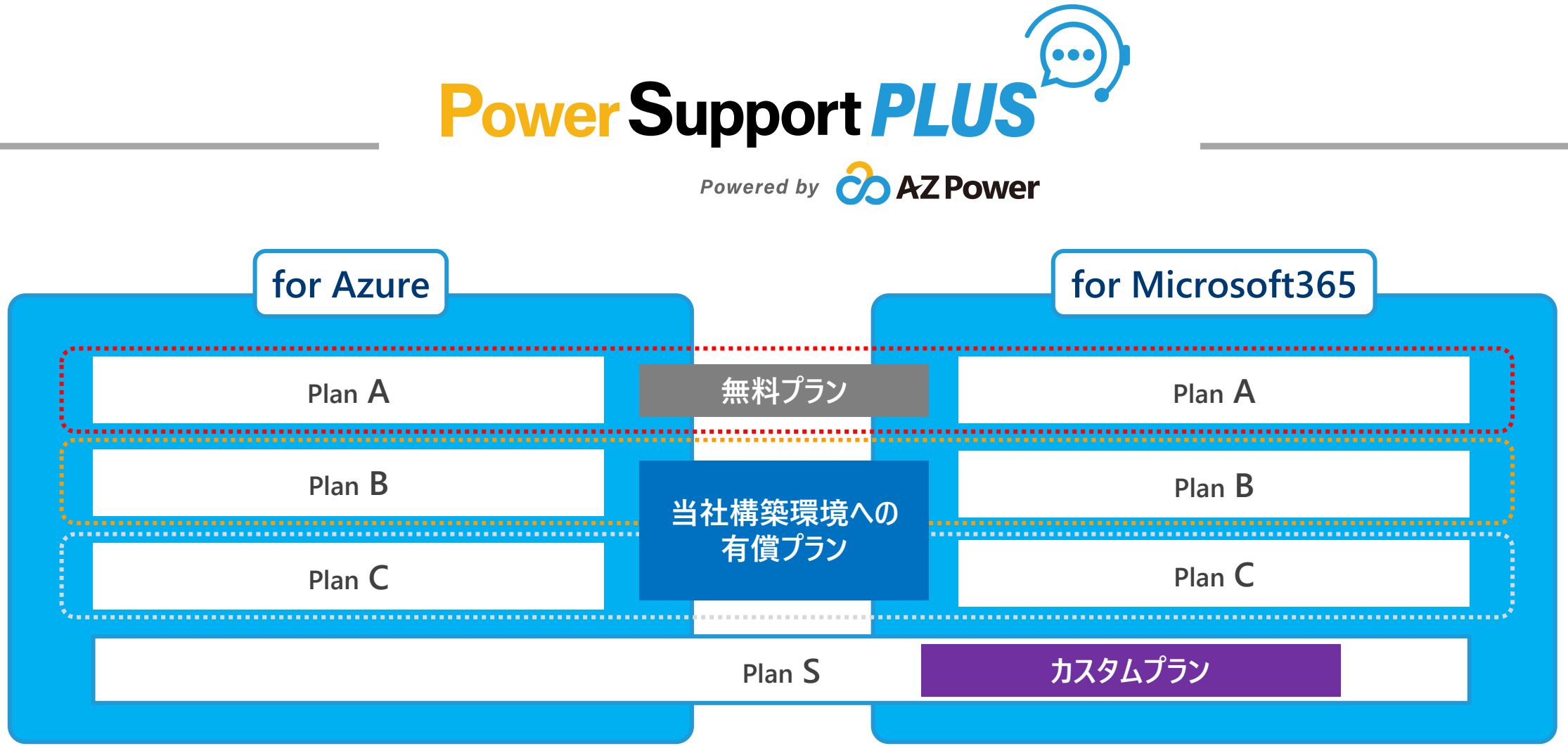
AVD ＋ Microsoft 365の統合を図り、より効率的なリモートワーク環境を実現。

Azure Virtual DesktopとMicrosoft 365（Teams, SharePoint, OneDrive）を統合し、効率的なリモートワーク環境を実現します。コラボレーションと生産性を向上させるための一体化されたソリューションを提供します。

サポートメニュー

Power Support PLUS

AZPowerサポートプラン「PowerSupportPlus」



無料相談会・アセスメントサービスご紹介

無料相談会・勉強会について

Microsoft Azure 無料相談会

企業のクラウド導入を支援するため、Microsoft Azure（以下「Azure」）無料相談会を開催します。クラウド移行や運用に関する疑問にお応えし、Azureを活用することで得られる多くのメリットをわかりやすくご説明します。
本相談会では、Azureを活用したクラウド移行のプロセスや運用、コスト削減の具体例をご紹介し、企業のニーズに合った最適なクラウド導入プランをご提案します。さらに、Azureが提供する生成AIの活用方法についても詳しくご紹介します。

ゼロトラストセキュリティ勉強会

多くの企業が既にOffice 365を代表としたMicrosoftのクラウドサービスを利用しています。これらのサービスは、Microsoftが提供するゼロトラストセキュリティフレームワークサービスと直接連携しており、追加のアプライアンス製品などのハードウェアやソフトウェアの導入なしにセキュリティ機能を大幅に強化することできます。
この勉強会では、Microsoft 365で提供可能な ゼロトラストセキュリティ原則に基づき、既存のMicrosoftエコシステムを用いて強固なセキュリティを実現する方法を学ぶことができます。

Microsoft365 オンライン勉強会

Microsoft 365は、日々の業務に欠かせないビジネスツールやセキュリティ機能を統合したクラウドベースのパッケージソリューションです。
「Microsoft 365オンライン勉強会」では、Microsoft365とはいったい何か？なぜ、企業が Microsoft 365 を選ぶのか？　というようなお悩みをお持ちの方におすすめです。
勉強会を通じて、お客様のニーズに合ったプランを選定し、特定の業務に最適なアドオンなどもご提案します。

アセスメントサービス(Rapid Securityアセスメント)について

ID管理、Office 365、Azure環境、エンドポイントに対してセキュリティに関する状態と潜在的なセキュリティリスクを把握します

Microsoft Entra ID

Office 365
SharePoint

エンド ポイント

セキュリティ アセスメントのメリット

データ漏洩するリスクへの懸念

現在のセキュリティの状態と潜在的な脆弱性の確認

認証情報の盗難、不正などを防ぐシステムの対応

セキュリティを強化するためのロードマップに必要な情報の提供

セキュリティ対策の優先順位がつけられない

お客様環境のデータに基づいたアクションプラン

まとめ

Microsoft 365 Business Premiumによる多層化セキュリティ

Microsoft 365 Business Premium

ID のセキュリティ	デバイスのセキュリティ	アプリケーションのセキュリティ	ドキュメントのセキュリティ
ユーザー	デバイス	アプリケーション	ドキュメント




Microsoft Entra IDを活用することで高度な多要素認証 (MFA) と条件付きアクセス ポリシーを適用し、必要なときに必要な場所から適切なユーザーだけが業務データを利用できるようにします。

Microsoft Intuneはリモートワーク環境に最適で、どこからでもデバイスを管理できる利便性があります。また、ソフトウェアの更新やパッチ適用を自動化することで、IT管理の効率を大幅に向上させます。

さらに、企業のセキュリティポリシーに準拠したデバイス管理を行い、コンプライアンスを維持します。

Microsoft Defender などの機能によってデバイス・アプリケーションを保護します。

またクラウドベースの管理により、どこからでもセキュリティ状況を監視・管理できる利便性があります。

Azure Information Protectionは、企業データの分類とラベル付けを自動化し、機密情報の保護を強化します。

データの暗号化により、情報が不正アクセスから守られます。また、ユーザーの行動を監視し、異常な活動を検出して迅速に対応します。

Microsoft365 Business Premiumを活用したゼロトラスト環境をご提案いたします！

Microsoft365&Azureで実現するゼロトラストモデルのご提案

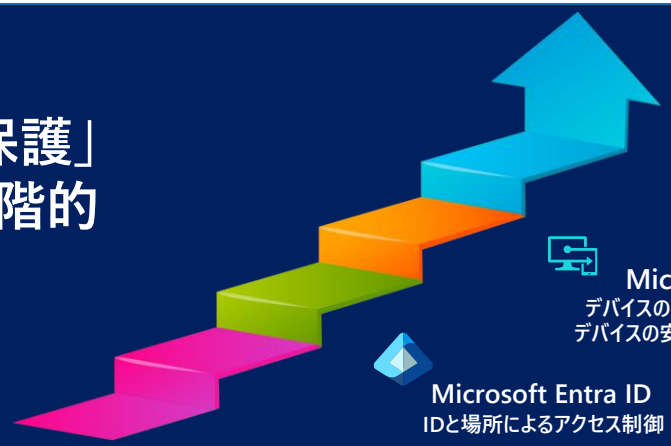



現在、社会全体にリモートワークができることが求められています

リモートワークに求められるセキュリティ対策とは？

デバイスの安全を確認したい
最新の脅威への対処・予防
リモートから管理したい
社内ネットワーク（境界型ネットワーク）の外でもしっかり保護したい
インシデント対応は極力自動化

AZPowerでは、ゼロトラストの基本となる「ユーザー保護」「デバイス保護」からセキュリティ対策をご提案し、要件・予算に応じた部分的かつ段階的なセキュリティ導入を支援いたします！



クラウドに新しい力をプラスする

AZ Power

クラウドに、テクノロジーであたらしい力をプラスし、世界中のお客様の
デジタル変革（デジタルテクノロジーによるビジネスイノベーション）を実現する。

弊社サービスに関するお問い合わせ・ご相談は下記メールまで

ap-sales@azpower.co.jp

AZPower株式会社