ゼロトラスト・セキュリティ
導入支援サービスのご紹介

株式会社QES

株式会社QES について

会社概要

商　　号	株式会社QES
設　　立	1983年3月1日
資 本 金	2億5000万円
代 表 者	代表取締役社長 和智徳男
拠　　点	東京（本社）, 大阪
売 上 高	108億円（2021年度）
従業員数	221人（2021年4月現在）
株　　主	株式会社 QUICK
関係企業	株式会社 日本経済新聞社
許 認 可	プライバシーマーク：10820787(08) ISO/IEC27001:2013（ISMS） 一級建築士事務所: 東京都知事登録第49085号 労働者派遣事業：派13-309151 他

QESの強み

豊富な経験と技術力	大規模な構築・移行 実績多数
システムソリューションでは、Microsoftソリューションは2003年から、仮想化への取り組みは2004年から、積み重ねた経験と技術があります。	システムソリューションでは、数千アカウントの構築や移行を行った実績が数多くあります。大規模構築、移行に対応できる能力に富んでいます。
提案・解決力	**ワンストップで提供**
システム、オフィスのソリューションで、幅広い製品を取り扱う中からお客様の目的に合わせたご提案をします。	システム、オフィスのソリューションで、お客様のご予算に合わせてハード、ソフトの選定から作業まで、ワンストップで対応することができます。

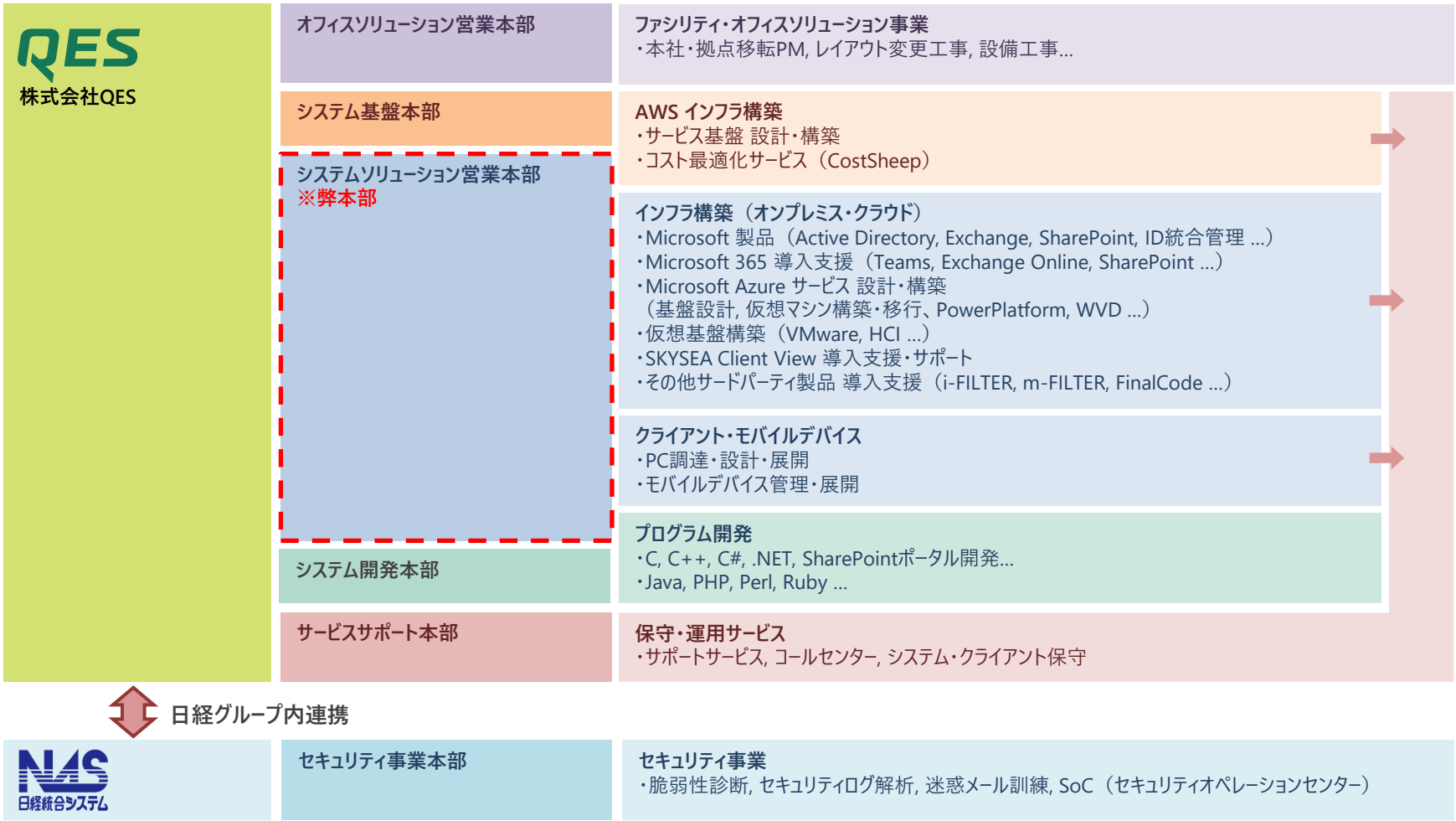
Microsoft とのパートナーシップについて

QES は長年にわたり Microsoft 製品を活用したインテグレーション・開発に携わり、その実績と専門知識から多くのカテゴリでゴールドパートナー認定を取得しています。また、マイクロソフト社とは営業面での協力や教育プログラムでの登壇など、様々な面で深く協業を進めています。

Microsoft Partner
Microsoft
Gold Application Integration
Gold Data Analytics
Gold Application Development
Gold Collaboration and Content
Gold Datacenter

株式会社QES 事業体制について

QESは日経グループを代表するITベンダーとして、最新のインフラ基盤からクライアント、プログラム開発、納品後の保守運用まで、フルラインナップのサービス提供を行っております



目次

ゼロトラスト導入支援サービス

「ゼロトラスト・セキュリティ」は「すべてのアクセスを危険なものとみなし、常に検証しセキュリティを確保する」考え方をとる最新のセキュリティ・フレームワークです。

一見わかりづらい「ゼロトラスト・セキュリティ」の実現・移行を「Microsoft 365」シリーズや幅広い製品を組み合わせてロードマップ作成からお手伝いします。

Microsoft 365シリーズで実現するゼロトラスト

Teams や Exchange Online で導入が進む「Microsoft 365」ライセンスで利用できるサービスを中心に、ゼロトラストを実現する機能の導入をお手伝いします。

お客様の状況から段階的な実現ロードマップを作成

「ゼロトラスト」は大きな変革であり、実現には中長期のロードマップが必要です。スモールスタートから大規模移行まで、段階的な移行を継続的にお手伝いします。

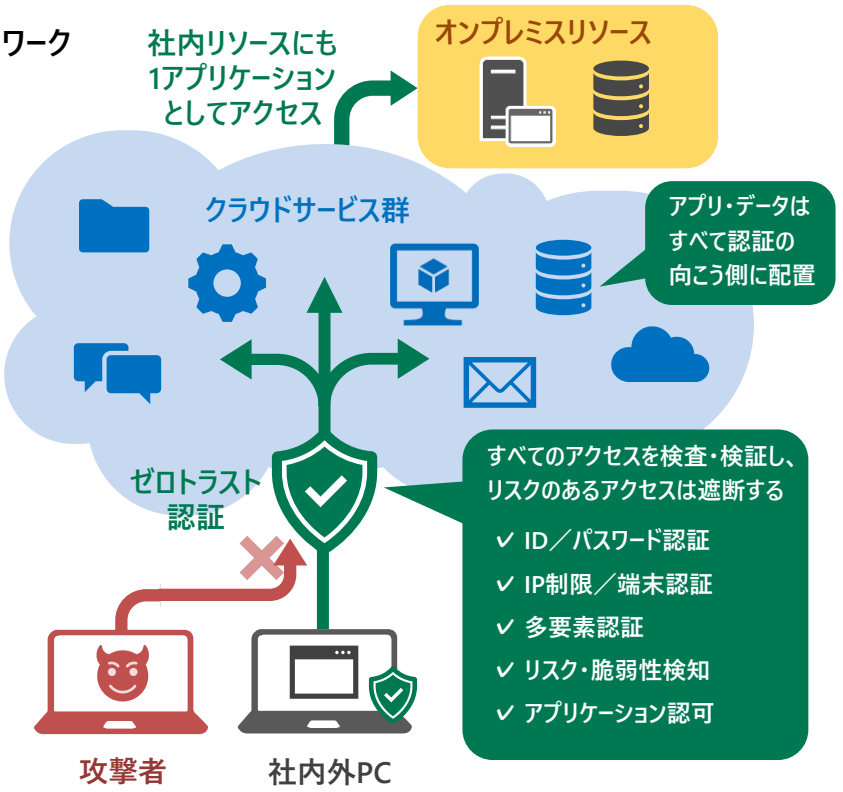
ハイブリッド・他ベンダー製品の組合せで幅広い要件に対応

Microsoft 製品に限らず、幅広い取扱い製品の組合せでお客様環境に合わせた機能実現が可能です。オンプレミス社内システムとのハイブリッド構成もご相談ください。

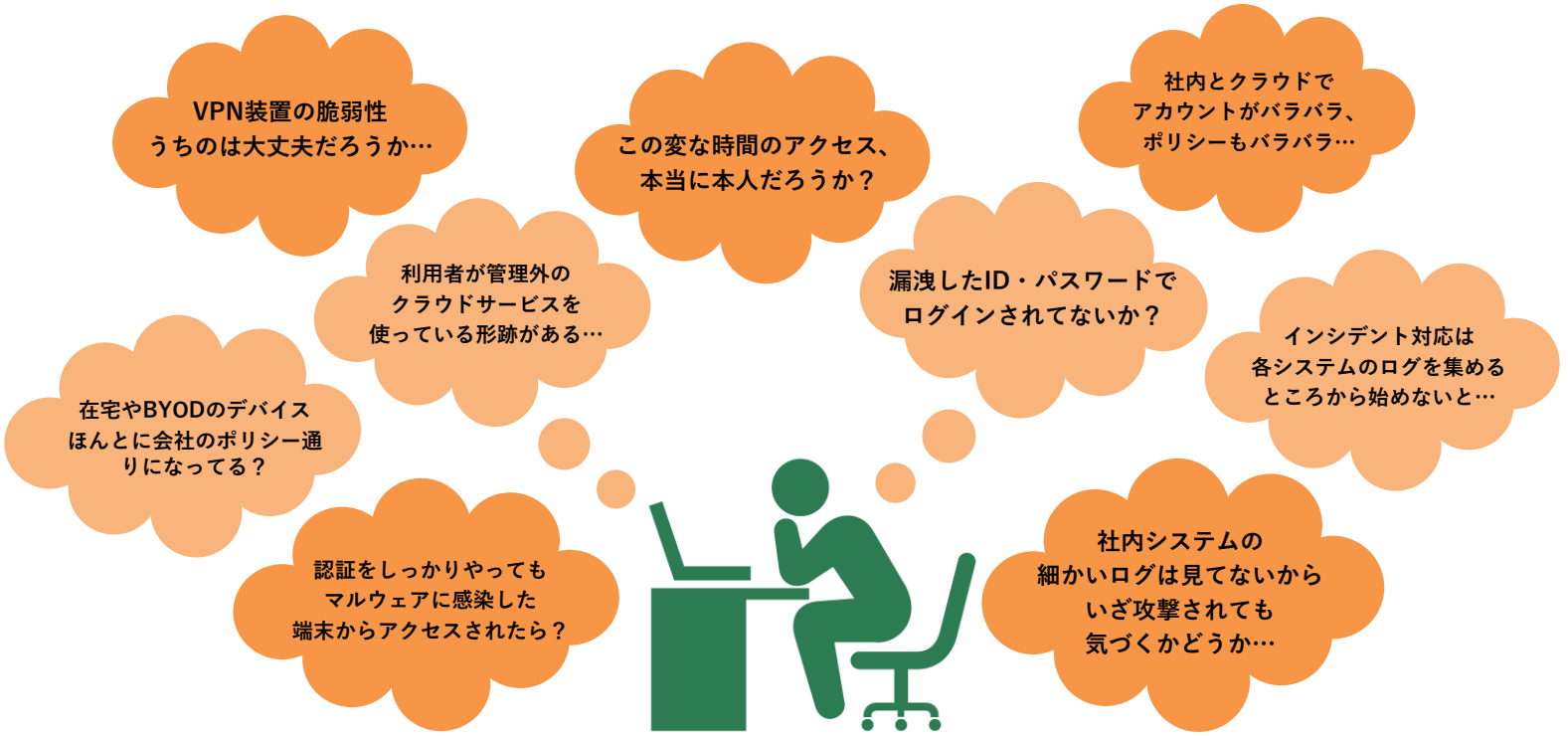
ゼロトラストとは

「ゼロトラスト・セキュリティ」は米調査会社「Forrester Research」社が提唱した、複雑化し続ける企業のセキュリティ対策を整理・一本化する新たなフレームワークです。
その名前（Zero-Trust）の通り、すべてのアクセスを信頼せず、統一した認証とポリシーでデータを守るのが考え方の基本となります。

クラウドと「ゼロトラスト」を前提としたネットワーク



クラウド利用やテレワーク、サイバー攻撃の時代にシステム管理者の悩みは尽きない

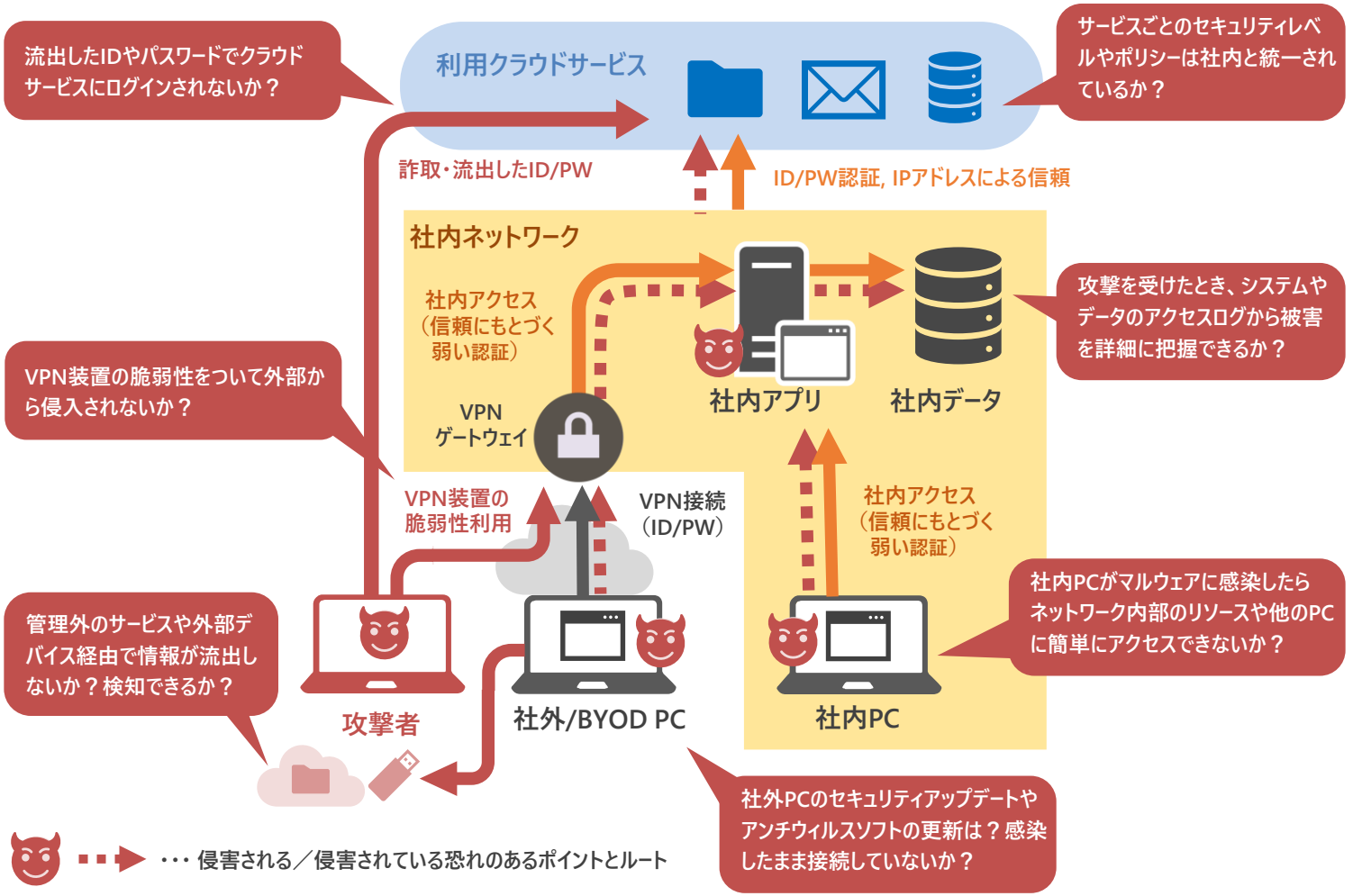


クラウドサービスの利用拡大
- 外部へのデータ・権限の分散
- セキュリティ考慮の複雑化
- シャドーITの隠れた進行

サイバー攻撃の被害拡大
- 標的型攻撃の高度化、長期化
- マルウェア・ランサムウェアの進化

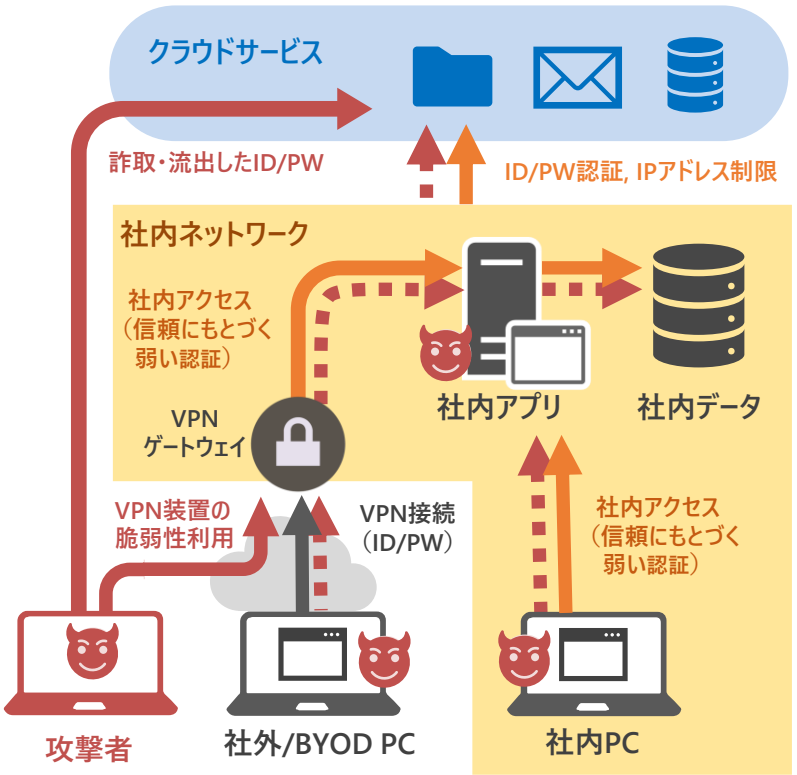
テレワークの導入・急拡大
- デバイスの多様化、BYODによるポリシー管理
- VPN設備の脆弱性リスク

一般的な「境界型ネットワーク＋クラウド」の企業が晒されているリスク・脅威のマップ

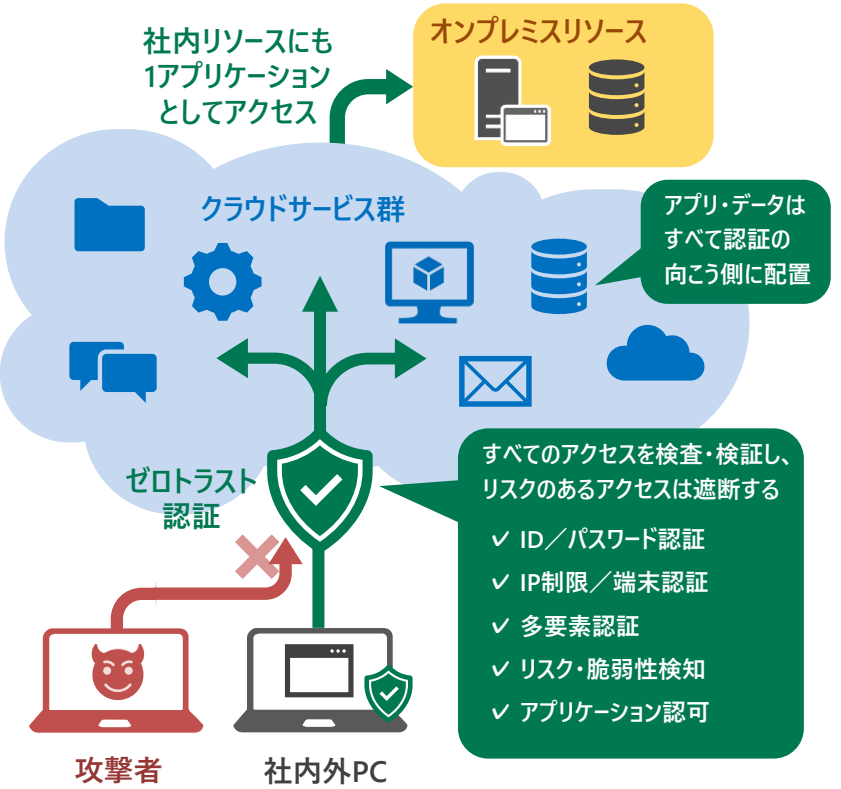


ゼロトラスト実現によるセキュリティ課題解決のイメージ

従来の「境界型ネットワーク」とクラウドの混在



クラウドと「ゼロトラスト」を前提としたネットワーク



・・・ 侵害される／侵害されている恐れのあるポイントとルート

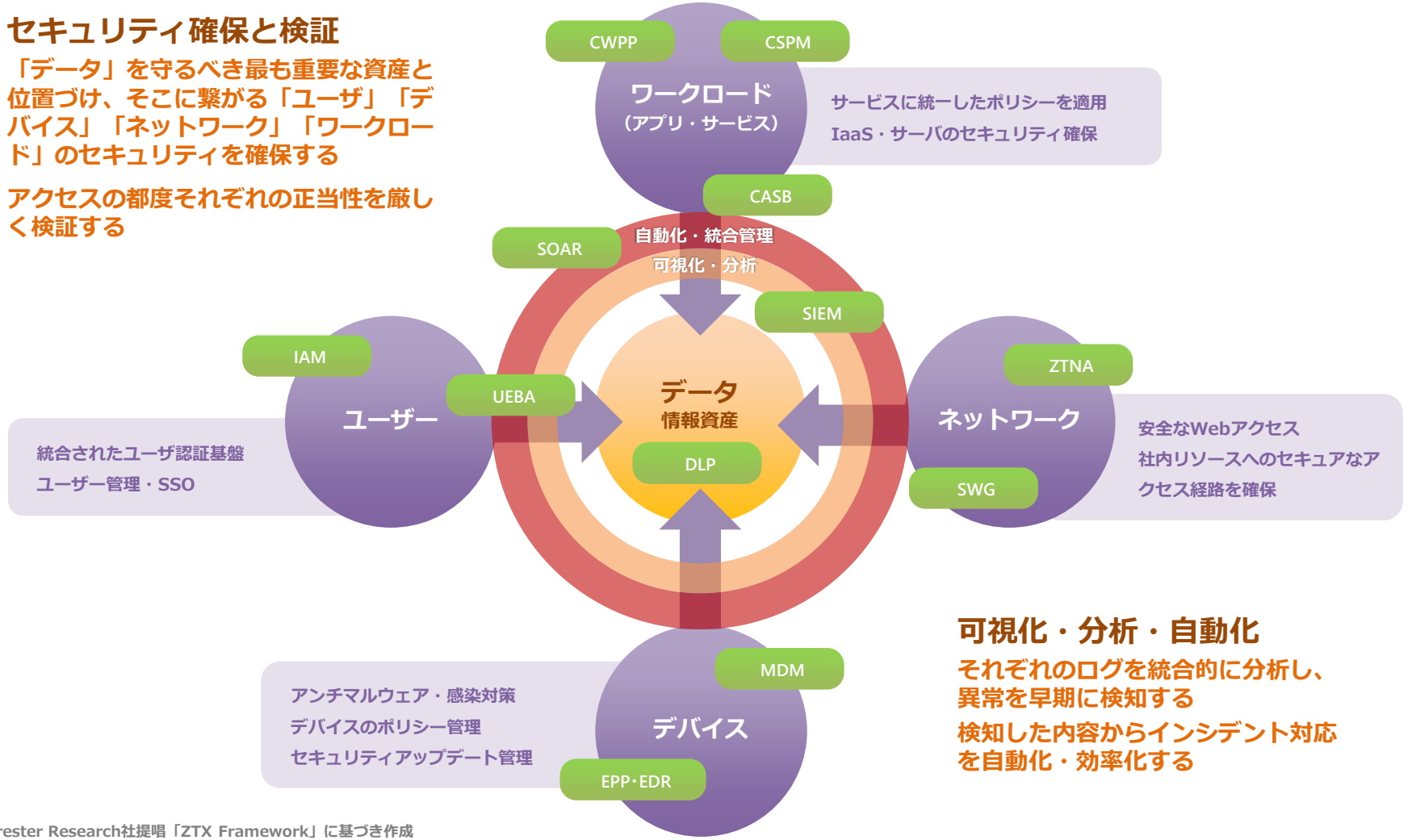
ZTX（Zero Trust eXtended）フレームワークによる整理

「データ」にアクセスする4つの要素と「可視化・分析」「自動化」を加えた７つの構成要素

セキュリティ確保と検証

「データ」を守るべき最も重要な資産と位置づけ、そこに繋がる「ユーザ」「デバイス」「ネットワーク」「ワークロード」のセキュリティを確保する

アクセスの都度それぞれの正当性を厳しく検証する



可視化・分析・自動化

それぞれのログを統合的に分析し、異常を早期に検知する

検知した内容からインシデント対応を自動化・効率化する

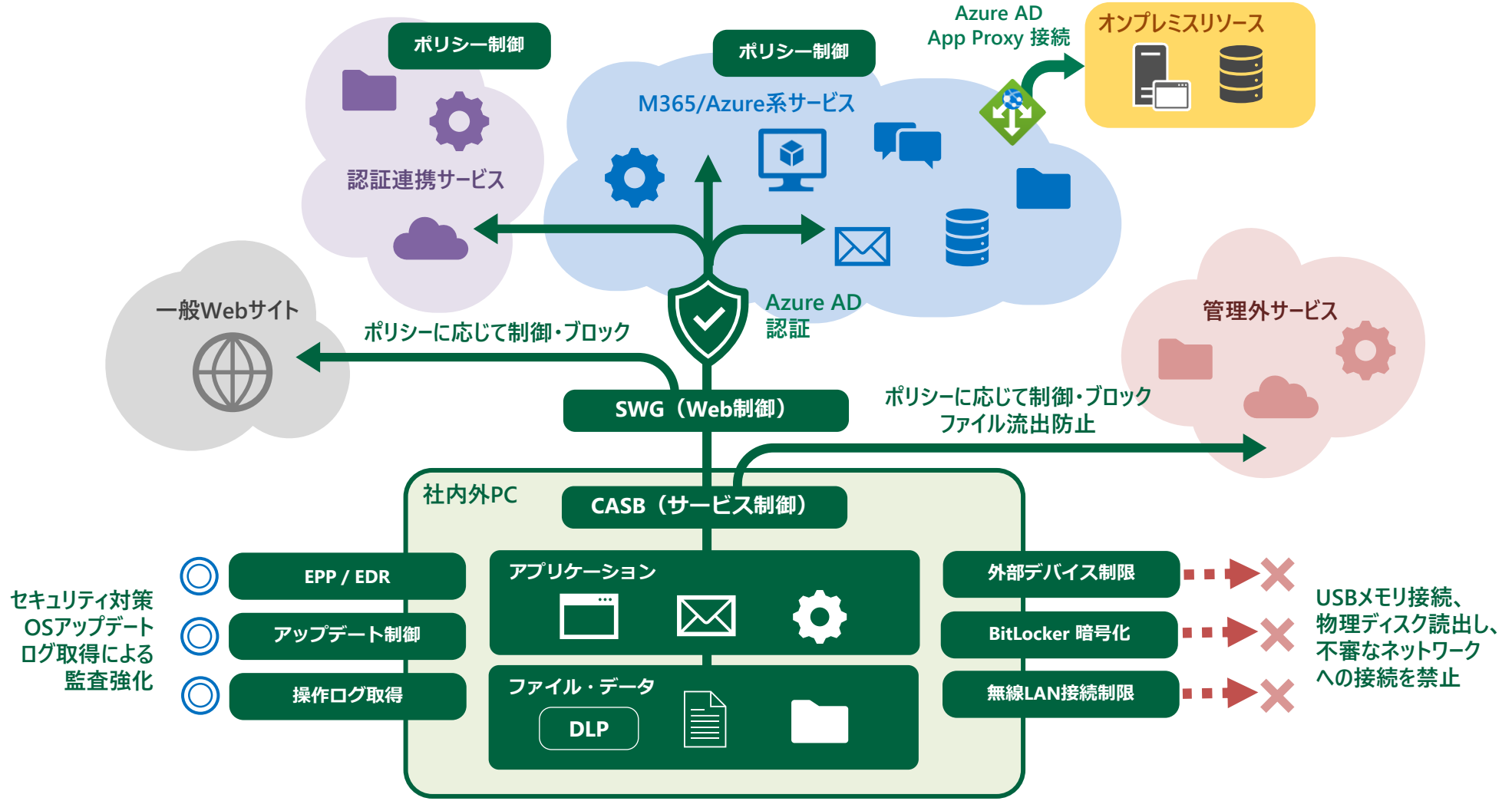
※Forrester Research社提唱「ZTX Framework」に基づき作成

ZTX（Zero Trust eXtended）フレームワークによる整理

「データ」にアクセスする4つの要素と「可視化・分析」「自動化」を加えた７つの構成要素

No	構成要素	コンポーネント・機能	概要
1	**アイデンティティ・セキュリティ** ID管理・認証・認可	IAM（Identify and Access Management）	ID管理、シングルサインオン（SSO）、デバイス環境とポリシーに基づく高度なアクセス条件制御
2	**ネットワーク・セキュリティ** ネットワーク経路のセキュリティを確保する	SWG（Secure Web Gateway）	クラウドプロキシ等によるWebアクセスセキュリティ
		SDP（Software Defined Perimeter）， ZTNA（Zero Trust Network Access）	社内アプリケーションの安全なインターネット接続
3	**デバイス・セキュリティ** デバイスのセキュリティ・管理・監視	EDR（Endpoint Detection and Response）	侵害監視・対応
		EPP（Endpoint Protection Platform）	アンチマルウェア・アンチウィルス
		MDM（Mobile Device Management）	デバイス管理
		アップデート管理	OSによるアップデート管理
4	**ワークロード・セキュリティ** サービス・IT資産のセキュリティ確保・監視	CWPP（Cloud Workload Protection Platform）	サービス・IaaSの管理・監視
		CSPM (Cloud Security Posture Management）	サービスの設定・ポリシー不備監視
5	**データ・セキュリティ** データ保護・情報漏洩対策	DLP（Data Loss Prevention）	情報のタグ付け・監視による情報流出対策
6	**可視化と分析** アクセス状況・ログの分析による制御・可視化	CASB（Cloud Access Security Broker）	クラウドサービスアクセス制御
		SIEM（Security Informataion and Event Management）	各製品ログの収集・統合的なログ分析
		UEBA（User and Entity Behavior Analytics）	ユーザー・機器等のふるまい分析による異常検知
7	**自動化** インシデント対応の自動化・効率化	SOAR（Security Orchestration and Automation Response）	様々なログ分析とサービス連携によるインシデント対応の自動化・効率化

ゼロトラストに基づくセキュリティ確保を行ったデバイスとサービス利用の流れ



Microsoft 365・Azureシリーズにおけるゼロトラストのサービス構成

No	構成要素	機能	製品・機能概要	M365/Azure 機能	必要ライセンス
1	**アイデンティティ・セキュリティ** ID管理・認証・認可	IAM	ID管理、シングルサインオン（SSO）、デバイス環境とポリシーに基づく高度なアクセス条件制御	Azure AD, 条件付きアクセスポリシー	Microsoft 365 E3
2	**ネットワーク・セキュリティ** ネットワーク経路のセキュリティを確保する	SWG	クラウドプロキシ等によるWebアクセスセキュリティ	Microsoft Defender for Endpoint（プレビュー）	Microsoft 365 E5
		SDP, ZTNA	社内アプリケーションの安全なインターネット接続	Azure AD Application Proxy	Microsoft 365 E3
3	**デバイス・セキュリティ** デバイスのセキュリティ・管理・監視	EDR	侵害監視・対応	Microsoft Defender for Endpoint	Microsoft 365 E5
		EPP	アンチマルウェア・アンチウィルス	Microsoft Defender for Endpoint	Microsoft 365 E5
		MDM	デバイス管理	Intune	Microsoft 365 E3
		アップデート管理	OSによるアップデート管理	MECM, WSUS	MS 個別ライセンス
4	**ワークロード・セキュリティ** サービス・IT資産のセキュリティ確保・監視	CWPP	サービス・IaaSの管理・監視	Azure Defender	Azure 個別機能
		CSPM	サービスの設定・ポリシー不備監視	Azure Security Center（Azureのみ）	Azure 標準機能
5	**データ・セキュリティ** データ保護・情報漏洩対策	DLP	情報のタグ付け・監視による情報流出対策	Azure Information Protection	Microsoft 365 E3 ※一部機能には E5 が必要
6	**可視化と分析** アクセス状況・ログの分析による制御・可視化	CASB	クラウドサービスアクセス制御	Cloud App Security	Microsoft 365 E5
		SIEM	各製品ログの収集・統合的なログ分析	Azure Sentinel	Azure 個別機能
		UEBA	ユーザー・機器等のふるまい分析による異常検知	Azure AD Identity Protection	Microsoft 365 E5
7	**自動化** インシデント対応の自動化・効率化	SOAR	様々なログ分析とサービス連携によるインシデント対応の自動化・効率化	Azure Sentinel	Azure 個別機能

Microsoft 365・Azureシリーズを中心としたソリューションでゼロトラストを構成します

Azure AD
【ID統合管理】

Microsoft 365・Azureで利用できる統合ID管理サービス（IDaaS, IAM）です。各クラウドサービスと認証連携でき、「条件付きアクセス」は各アクセスを様々な条件に応じて検証・判定することができる、ゼロトラスト実現の中核となる機能です。

Microsoft Intune
【デバイス管理】

Microsoft 365と連携するデバイス管理サービス（MDM）です。MDMとしてデバイス管理を行えることに加え、「Azure AD 条件付きアクセス」と連動させることで、デバイスのセキュリティ・コンプライアンスの適合状況を認証条件に含めることができるようになります。

Azure AD Application Proxy
【アプリケーションアクセス】

Microsoft 365で利用できる、社内Webアプリへの中継サービスです。社内アプリをAzureと接続し、1つのクラウドサービスのように社内ユーザに安全に公開することが可能です。

Azure Virtual Desktop
【仮想デスクトップ】

Azure上で利用できる仮想デスクトップサービスです。Azureを社内と接続することで、厳しい認証を行ったうえで画面転送により安全に社内リソースやアプリにアクセスさせることができます。

EPP・EDR
【デバイスセキュリティ】

エンドポイントセキュリティはウィルス・マルウェア対策の基本であり中核です。QESではMicrosoft 365に含まれるWindows Defenderの他、お客様環境に合わせて多様なEPP・EDRのご提供が可能です。

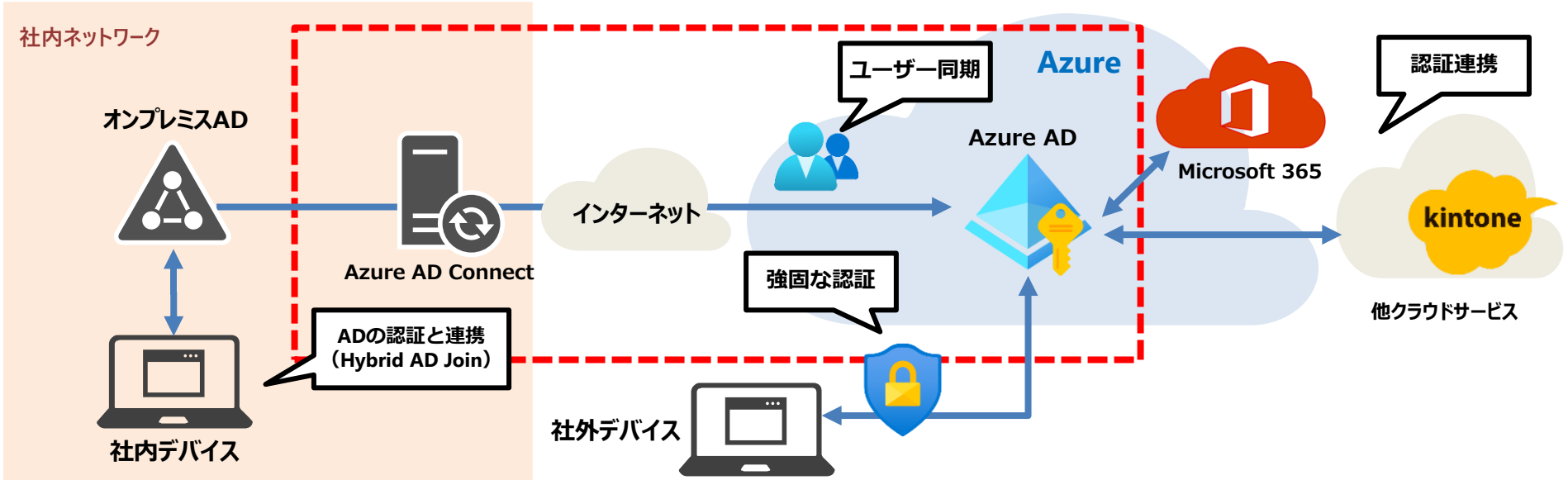
Netskope
【クラウドサービス制御】

NetskopeはCASB（クラウドサービス制御）を中心としたネットワークセキュリティ製品です。クラウドサービスへのアクセスを一元的に制御・制限し、シャドーITの検出、データ流出防止を実現します。Microsoft 365を導入されていないお客様にもお勧めします。

Azure AD によるID管理・統合クラウド認証

Azure AD はMicrosoft 365／Azure の基礎となるID管理システムです。**多様な認証要素とサービス連携でクラウドの認証を強固に・統合的に管理**することができます。

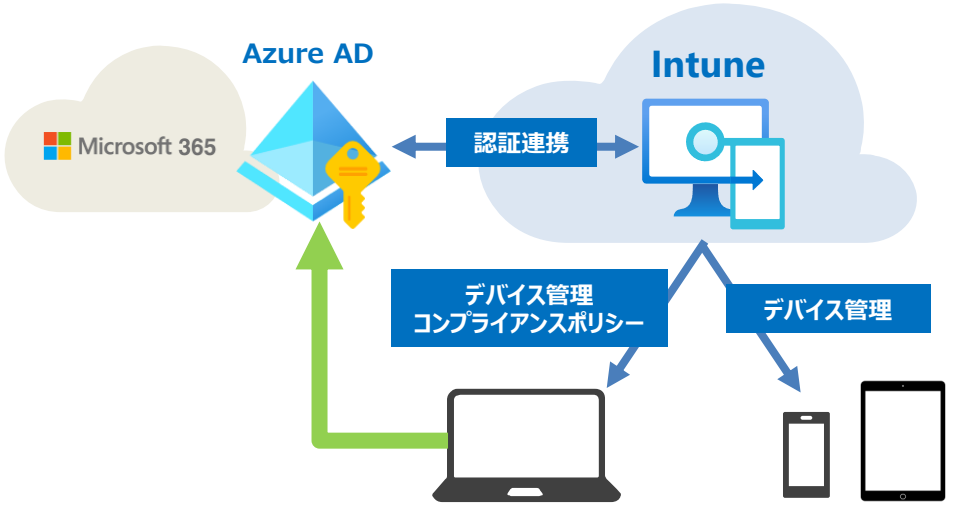
- Microsoft 365シリーズや他クラウドサービスへの認証連携・シングルサインオン（SSO）
- デバイス管理状況、スマホコード、IPや諸情報を条件にできる強固な多要素認証（条件付きアクセス）
- オンプレミスActive Directoryとの同期、認証連携（Hybrid AD Join）



Microsoft Intune

Intune は Microsoft 365 シリーズで使用できるデバイス管理サービス（MDM/MAM）です。iOS/Android のモバイルデバイスを MDM として管理・制御できることに加え、**Windows 10 デバイスに対しては、さらに踏み込んだポリシーの適用を行い、それを Azure AD の認証要素として設定することができます**。

- BitLocker 暗号化、一定以上の Windows バージョン、ファイアウォール有効化、ウィルス対策 をコンプライアンスポリシーとして要求する
- パスコードポリシー、機能制限ポリシー、リモートロック・ワイプ

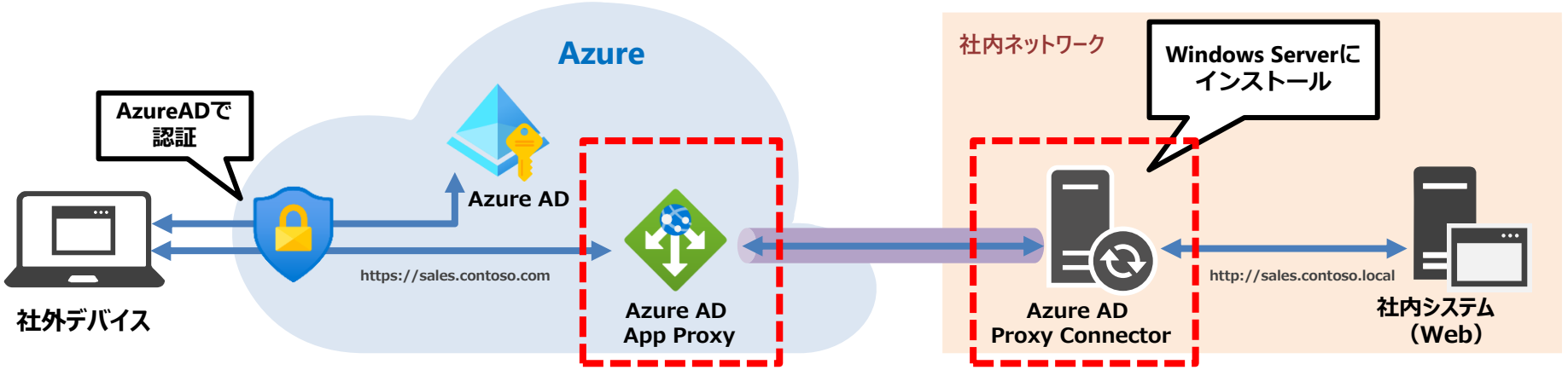


Azure AD アプリケーションプロキシ を使用した社外からの社内システムアクセス

社内に中継サーバを構成してAzure ADに登録することで、
社外から Azure 認証経由で安全に社内システムへアクセスさせることができます。

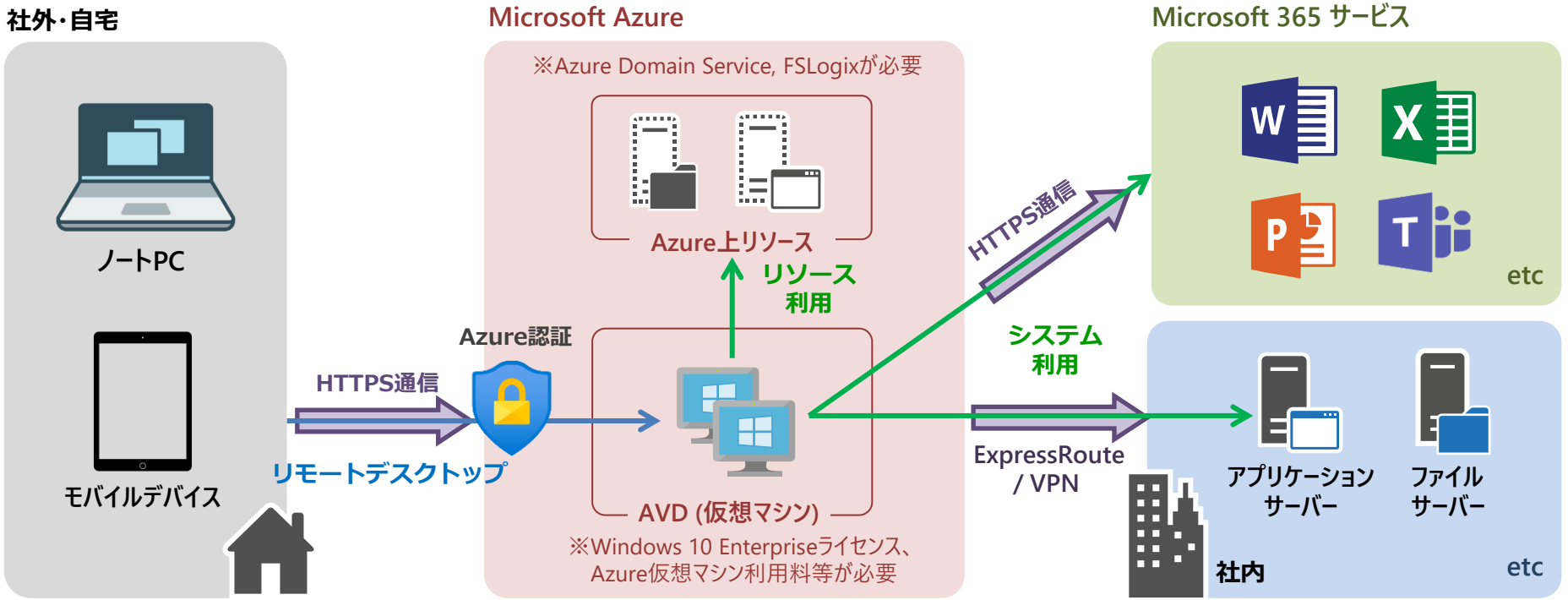
- VPNに頼らない社内Webアプリへのアクセス
- Azure AD を使った強固な多要素認証が使用可能
- 社内システムに対するシングルサインオンを構成可能
- Azure AD Premium P1 以上のライセンスで利用可能
- 社内の Proxy Connector から Azure に対してセッションを張るため社内IPの外部公開が不要

Azure AD アプリケーションプロキシ 構成イメージ



Azure Virtual Desktop（旧称 Windows Virtual Desktop） クラウド仮想デスクトップ

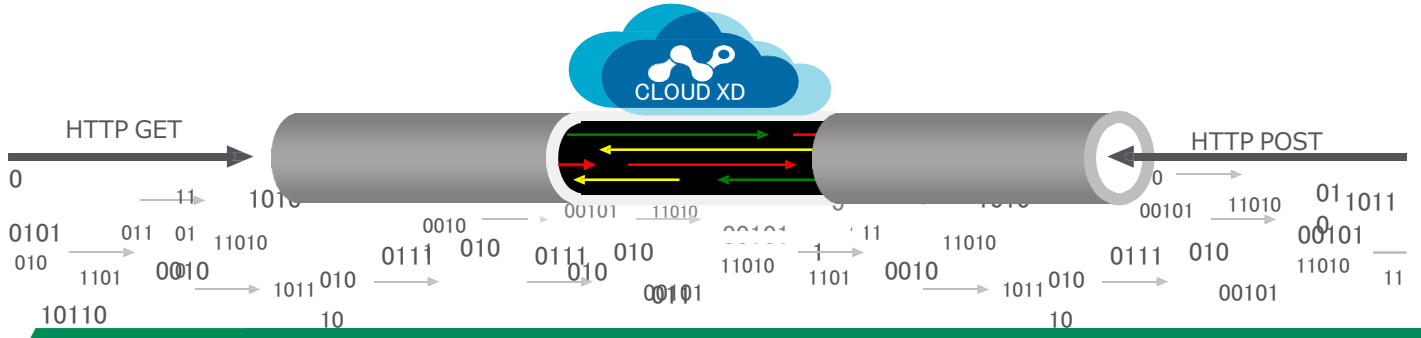
1. 社内に物理的なPCが必要なく、どの端末からでも同じ環境・社内システムを使用できます
2. Azure認証では「ID・パスワード」「端末情報認証」「コード認証」等を組み合わせセキュアに認証できます
3. Microsoft365 Business Premium, E3 以上でWindowsライセンスをお持ちの場合にはお得に利用できます



Netskope CASB

Netskopeは代表的な**CASB（Cloud Access Security Broker）製品**です。

デバイスが行うすべてのWeb通信を可視化・分析し、33,000以上のWeb・クラウドサービスの評価・アクセス制御、2,400以上のサービスの操作内容をコントロールし、シャドーITの可視化やデータ保護を実現します。



Microsoft 365・Azureシリーズを利用したゼロトラスト実現のロードマップ

長期的に段階を踏んだロードマップの作成から QES がお手伝いします。
まず安全なクラウドの領域を確保し、そこへアプリ・データを移行して利用範囲を拡大していきながら、セキュリティやコンプライアンス強化を行う流れをお勧めします。

各フェーズで主に必要な Microsoft 365・Azure ライセンス

Microsoft 365 E3（または Business Premium）	Microsoft 365 E5
	Azure Defender / Azure Sentinel

※実現されたい機能・要件により上記のほかにもライセンス・費用が必要となる場合があります

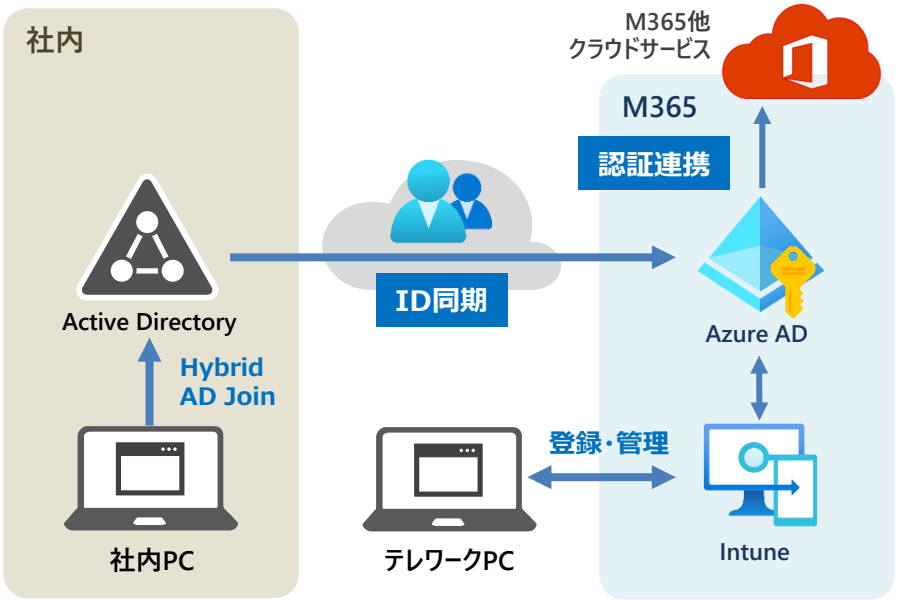
A社：社内ADとAzure ADを同期し社内外のデバイス管理と認証を統合

顧客　製造業 500～1000名企業様

課題　クラウド認証の強度を強め、テレワークPCの管理・認証も統合したい

解決　オンプレミスADとAzure ADを同期・連携するよう構成し（Hybrid AD Join）、テレワークPCをIntuneで管理することで、クラウドサービスの認証条件としてPCがADまたはIntuneで管理されていること、管理ポリシーに適合していることを追加しました。

構成　Azure AD（AADC, 条件付きアクセス）, Intune



B社： 社外PCに対してAzure AD Application Proxyで安全に社内アプリを公開

顧客　金融系 300～500名企業様

課題　持ち出しで使う社外PCを管理し、安全に社内アプリ（事務、ファイル閲覧）に接続させたい

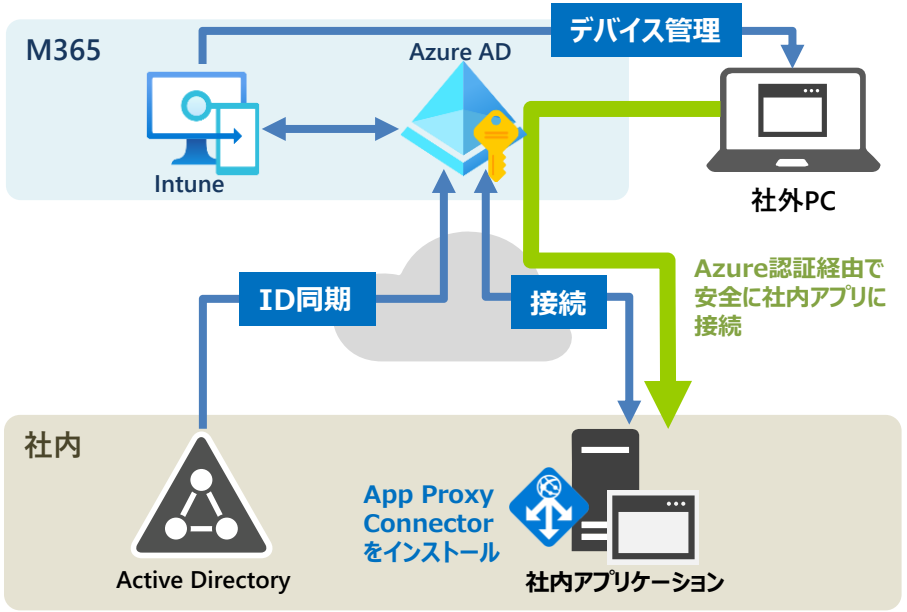
解決　社外デバイスをIntuneで管理し、App Proxyを構成して社内アプリをAzureに接続、

多要素認証を経由した安全なアクセスだけ社内アプリに接続できるよう設計しました。

App Proxyは内部からAzureにセッションを張るため、社内ネットワークを公開する

必要がなく、ネットワーク設計の変更が発生しない点も大きなメリットです。

構成　Azure AD（AADC, 条件付きアクセス）, Intune, Azure App Proxy



ご検討のほど宜しくお願い致します