

Case①

端末のセキュリティと管理

- 端末からの情報漏えい防止
- ゼロタッチによるシームレスな展開
- VDI基盤の準備・構築・運用

Case②

運用の高度化・効率化

- 端末管理などのルーティンワークからの解放
- ネットワーク機器の運用省力化
- エキスパートによるセキュリティ運用高度化

Case③

ゼロトラスト・ネットワーク

- ゼロトラスト化の段階的な検討
- 閉域網のデータ量軽減
- 業務端末でのインターネット分離

Case④

アプリケーション

- M365の導入・移行
- M365チーム乱立防止、データバックアップ
- 既存アプリケーションの延命

端末のセキュリティと管理

いつでもどこでも安全・安心に利用できるクライアント環境には、**管理と端末そのもののセキュリティが重要**

自宅・サテライト



パッチ未適用などの管理不備リスク
自宅での初期キッティング

A

端末の遠隔管理とゼロタッチ

Intune

Autopilot

インターネットベースの資産管理及び
デバイス状態の把握・制御

端末の持ち出し



紛失・盗難リスク

B

端末そのもののセキュリティ

秘密分散

揮発型

VDI + シンクライアント

セキュリティ要件に応じた、クライアント
の提供

ベースオフィス



オンプレミスとクラウドでの
端末の共同管理

C

オンプレミスとクラウドの
ハイブリッド運用

Intune-MECM連携

企業のネットワーク構成や管理要件などに
応じた、クラウド管理とオンプレミス管理の
最適化

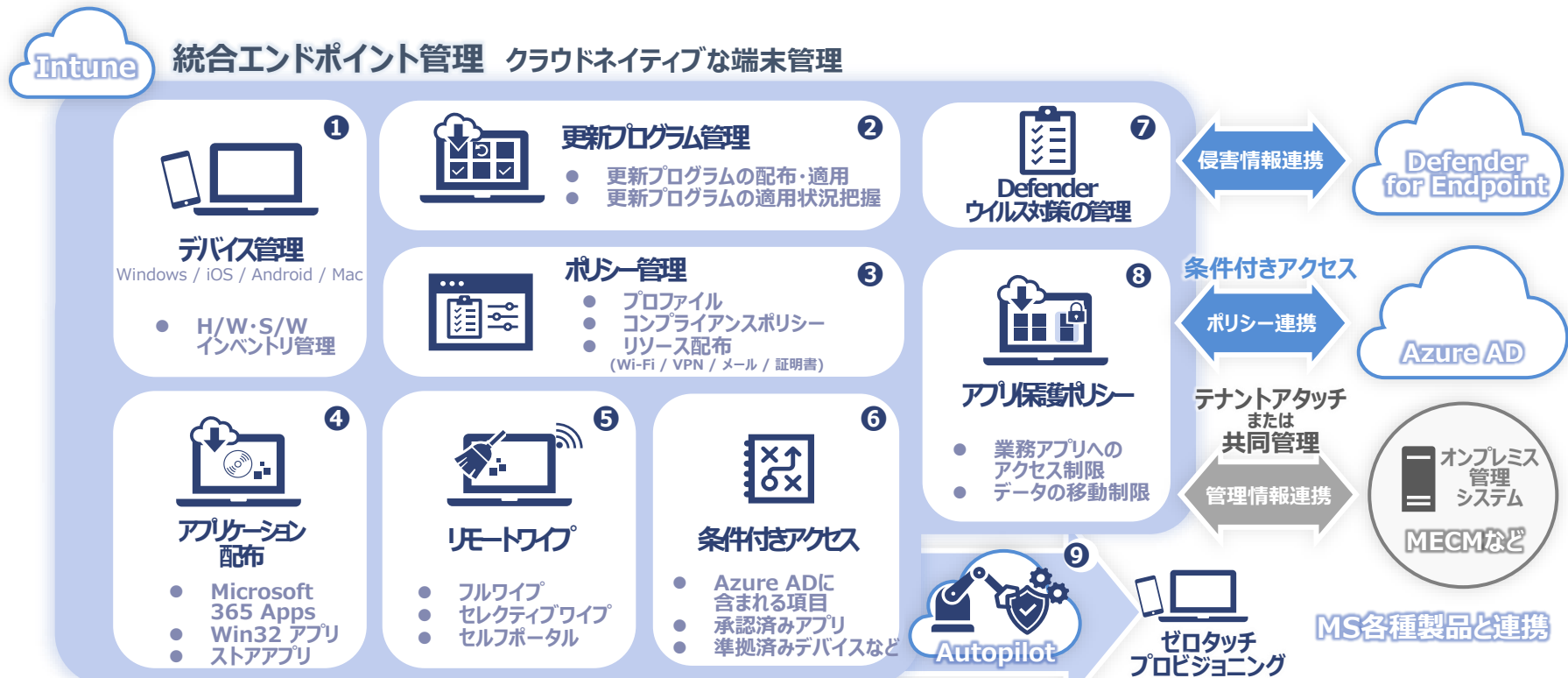
Intune：Microsoft社製の端末管理SaaS

Autopilot：Windows PCをクラウド経由で自動セットアップするMicrosoft社製ツール

MECM：Microsoft Endpoint Configuration Manager, Microsoft社製のオンプレミス端末管理ツール

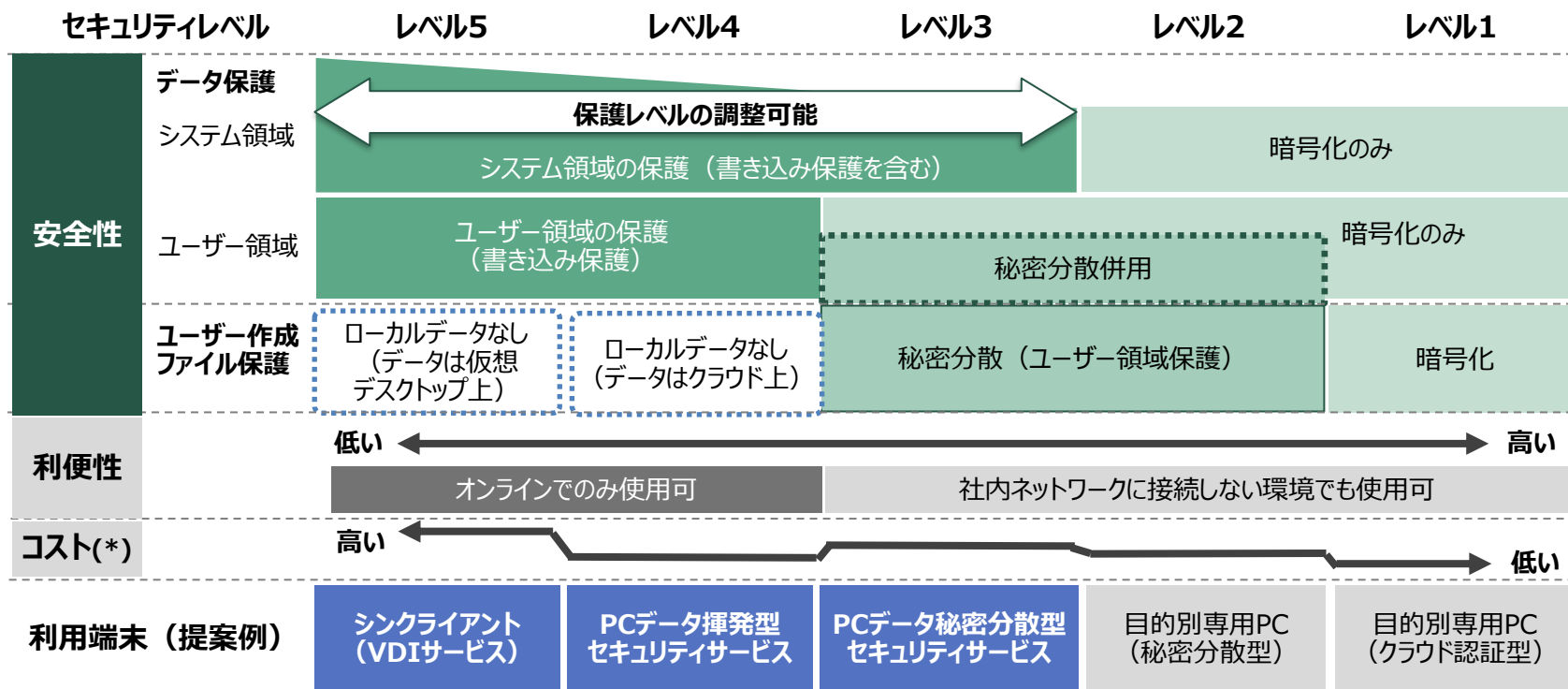
A 端末の遠隔管理とゼロタッチ

「Intune」 Azure ADやDefender for Endpoint、オンプレミスのMECMなどと連携して端末を管理
 「Autopilot」 Intuneと連携しWindows PCのセットアップを自動化



B 端末そのもののセキュリティ

必要なセキュリティレベルや利便性、コストに応じた最適な施策をご提案



(*) PC1台あたりに換算した際のコスト。レベル2、3、4のコストは、使用するサービスの選択や設定によって異なります。

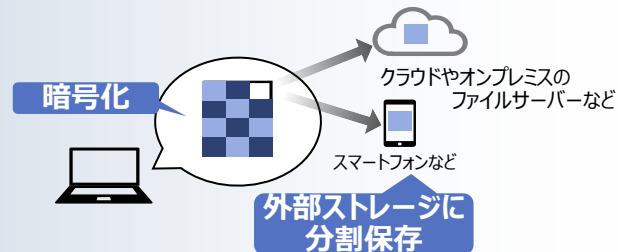
VDI：Virtual Desktop Infrastructure、デスクトップ環境を仮想化してサーバー上に集約する仕組み

B 端末そのもののセキュリティ

PCデータ揮発型セキュリティサービス



PCデータ秘密分散型セキュリティサービス



PCデータ揮発型

PCデータ秘密分散型

説明

シャットダウン時にデータを揮発

シャットダウン時にデータを分散保存

セキュリティ強度

PCにデータは残らない

PCに(閲覧できない)データが残る

ユーザビリティ

データのダウンロードが必要

PCにデータあるのですぐに利用できる

ネットワーク接続

オンラインでのみ使用可

社内ネットワークに接続しない環境でも使用可

通信量

多い(データの取得・格納が必要)

少ない(データはPC内にある)

利便性と安全性を向上する日立独自機能

安全性

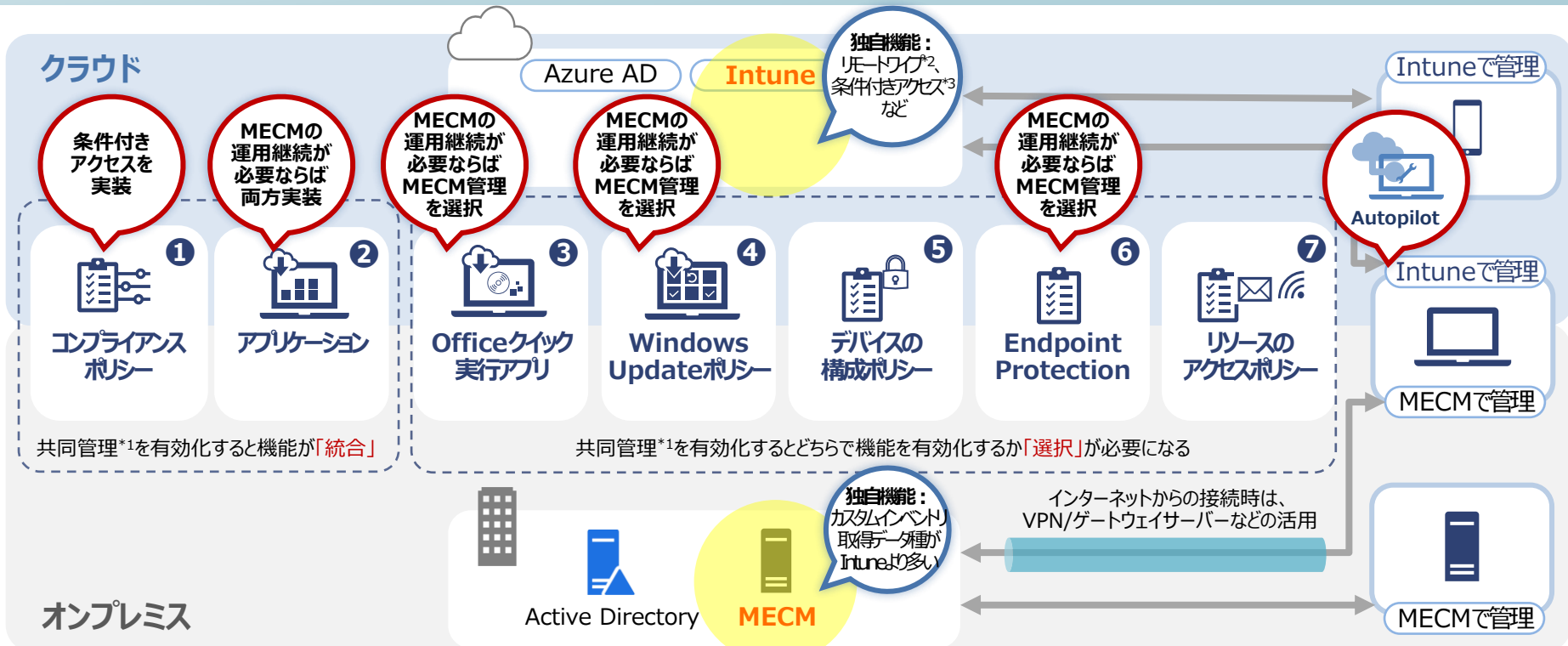
- ・一定時間の無操作を自動検知し、強制シャットダウン
- ・USBメモリーなど外部デバイス出力制限
- ・ユーザーでの設定変更防止

利便性

- ・アプリケーションや辞書データなど、機密性がない情報は保持
- ・ユーザー操作でOSを復旧(ローカルリカバリ)

オンプレミスとクラウドのクラウドのハイブリッド運用

Intune/MECMには機能差異があり、お客様のポリシーに応じ適切な設計が必要
お客さまと並走しながら要件ヒアリングやPoCを実施し、設計を推進

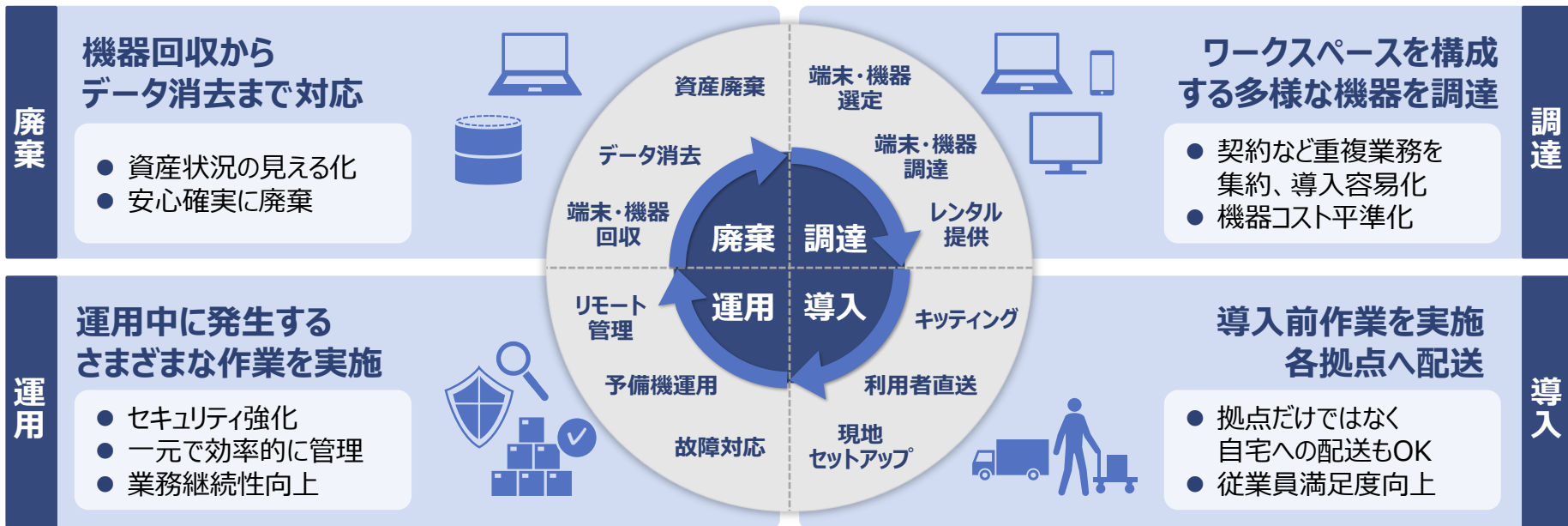


*1共同管理：MECMのデバイス情報をIntuneに同期させることで、MECMとIntuneの両方でWindowsデバイスを管理できるようになる機能

*2 遠隔でデバイスを初期化する機能 *3 パッチ未適用機器をアクセス不可にするといったアクセス制御機能

IT部門のお悩みにお応えする「統合クライアントサービス」

IT機器の調達から運用保守、利用後の回収、廃棄までをアウトソースしてIT部門の負荷を軽減することで、注力すべきIT企画業務に専念



IT人財の
コア業務への
リソースシフト



ITガバナンス
強化

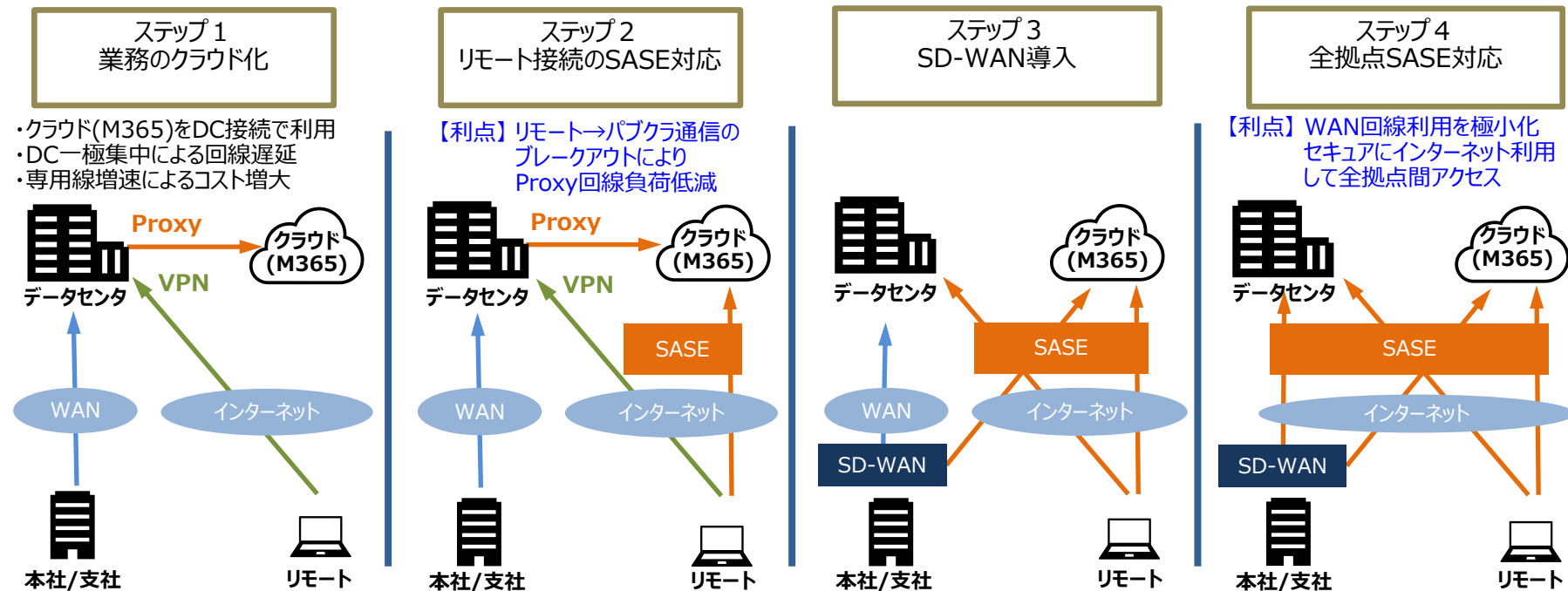


ITコスト
平準化

インターネット主体、ゼロトラスト型セキュリティを支援

お客様の業務のクラウド化に合わせ、PoC検証を踏まえ、SASE、SD-WANを順次導入

■ 導入例



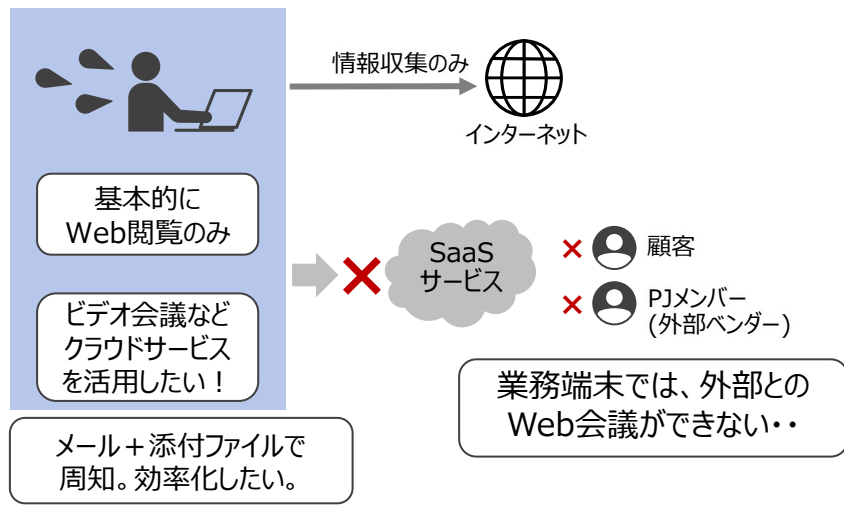
SASE : Secure Access Service Edge, ネットワークとネットワークセキュリティを統合し、提供するクラウドサービス
SD-WAN : Software Defined Networking, 仮想的なWANをソフトウェアを用いて管理する技術

お客さまの現在のIT環境に合わせてM365の導入を支援

スマートワークの推進のために、まずはMicrosoft 365導入によるコミュニケーション基盤の整備が重要

導入前の課題

- 情報漏えいのリスクから守るためインターネットアクセスを制限。クラウドサービスの利用に制限が生じていた。
- 従業員の業務端末からWeb会議が主催できない。
(参加招待を受ける場合においても別途インターネット接続端末が必要)



導入後（従業員のメリット）

「Microsoft 365導入/技術支援サービス」
現在のインフラ環境にクラウド活用をあてはめ、
外部とのコラボレーション基盤を実現

