

Microsoft からのアップデート

SINET-Azure 閉域網接続

Microsoft製品で実現するゼロトラスト

日本マイクロソフト株式会社パブリックセクター事業本部/クラウドアーキテクト
大阪工業大学ロボティクス&デザイン工学部/客員教授

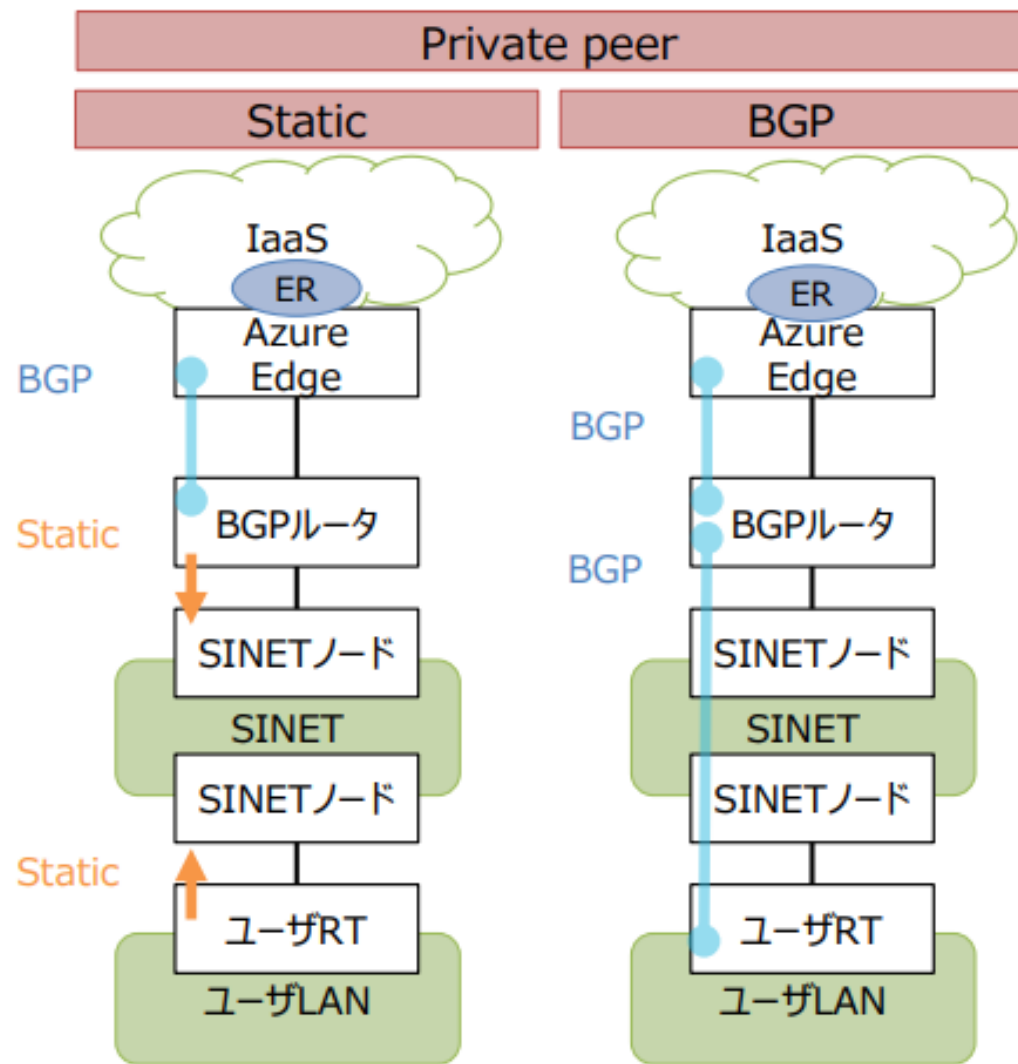
中田 寿穂

Azure – SINET Connection

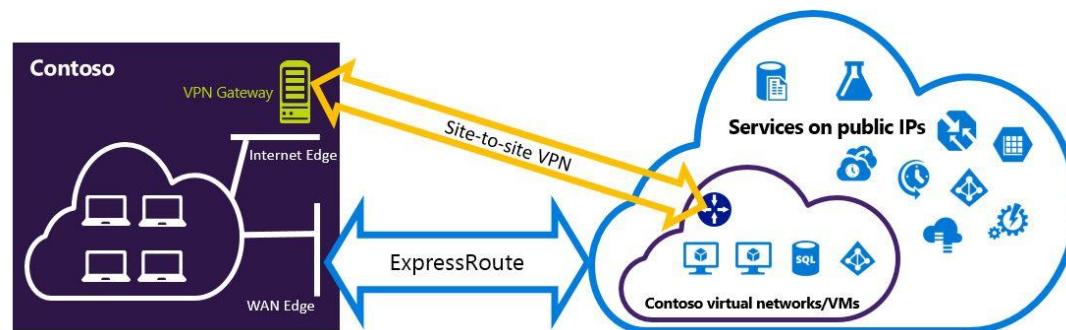
An abstract graphic of a network or data structure, consisting of numerous small blue dots connected by thin white lines, forming a complex, interconnected web. The graphic is positioned on the right side of the slide, with a gradient background transitioning from light blue on the left to dark blue on the right.

- ①ネットワーク帯域を従来の2倍に拡張
- ②BGP Routing のサポート
- ③MS Peering のサポート

Azure – SINET アップデート BGP Routing のサポート

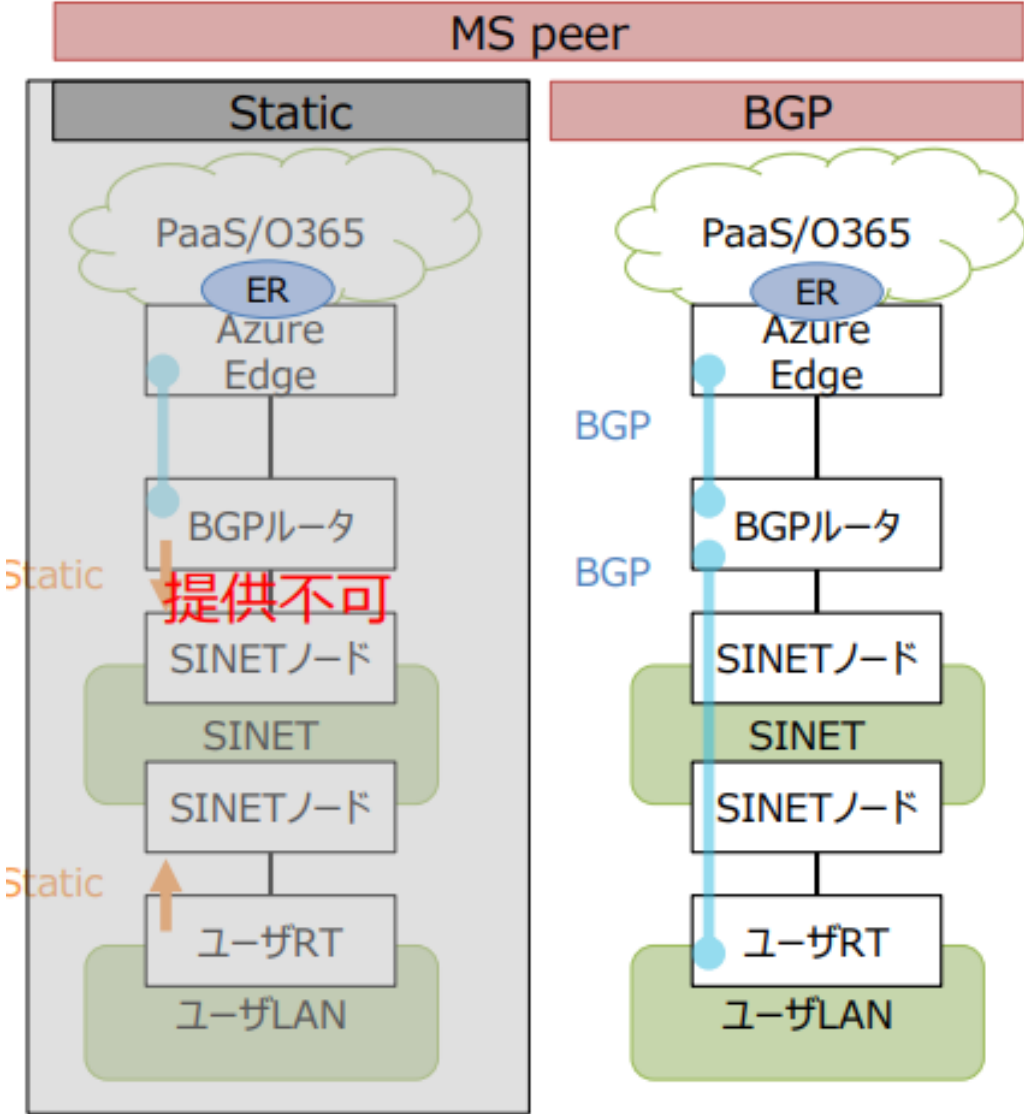


- ✓ お客様拠点の BGP ルーターでルーティング設定ができるようになります。
- ✓ ExpressRoute のフェールオーバーパスとして、IP Sec VPN を構成できるようになります。

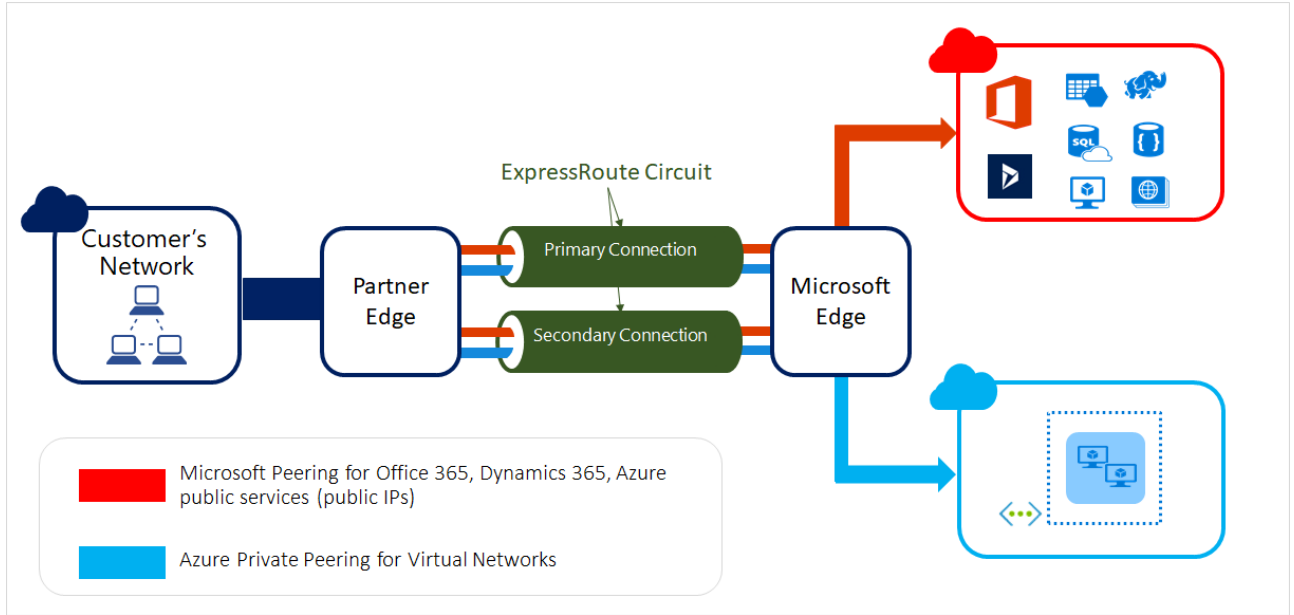


Azure – SINET アップデート

Microsoft Peering のサポート



MS Peering をサポートすることで、Microsoft オンラインサービス (Microsoft 365, Dynamics 365, Azure PaaS など)の通信を ExpressRouteを通すことができます。



Zero Trust における Azure AD の位置づけ

6-1 前提

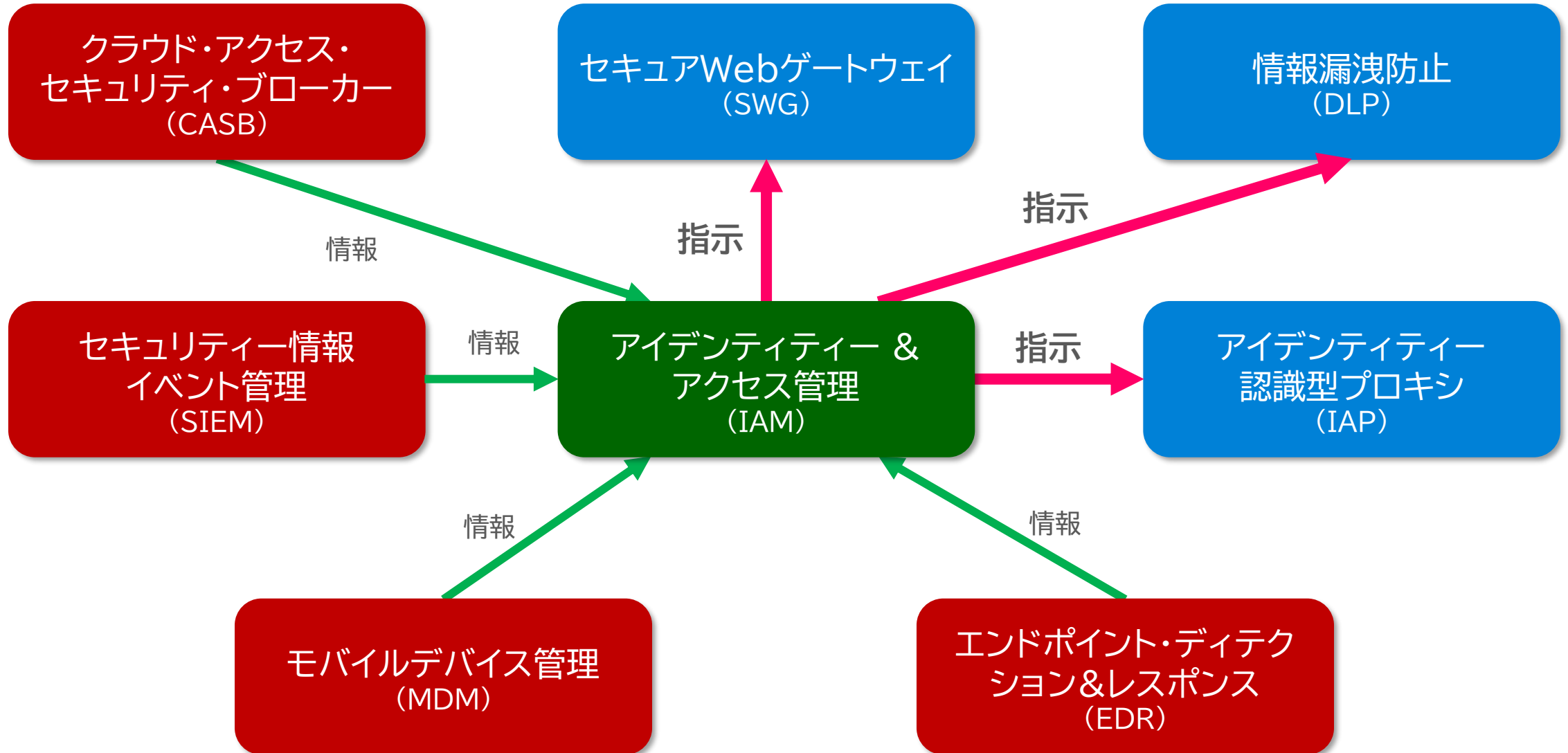
本ハンドブック発行時点（令和3年5月）時点では、自治体や学校により、校務系システムをはじめとしたオンプレミス型環境が残存していることが想定されます。本章では、校務系システムやオンプレミス型の環境における対策方法を示します。

なお、とりわけ校務系システムの機密性を確保する方法として、旧来は、ネットワーク制御を中心とした境界防御型が一般的でしたが、特に昨今の働き方改革や休校時対応によるリモートワーク等を行う際には、端末への対策を中心としたアクセス制御型への移行又は組み込みがより有効な手段となりえます。それぞれの差異を認識し、特徴に応じた適切な対応を行いましょう（詳細については、6-4を参照）。

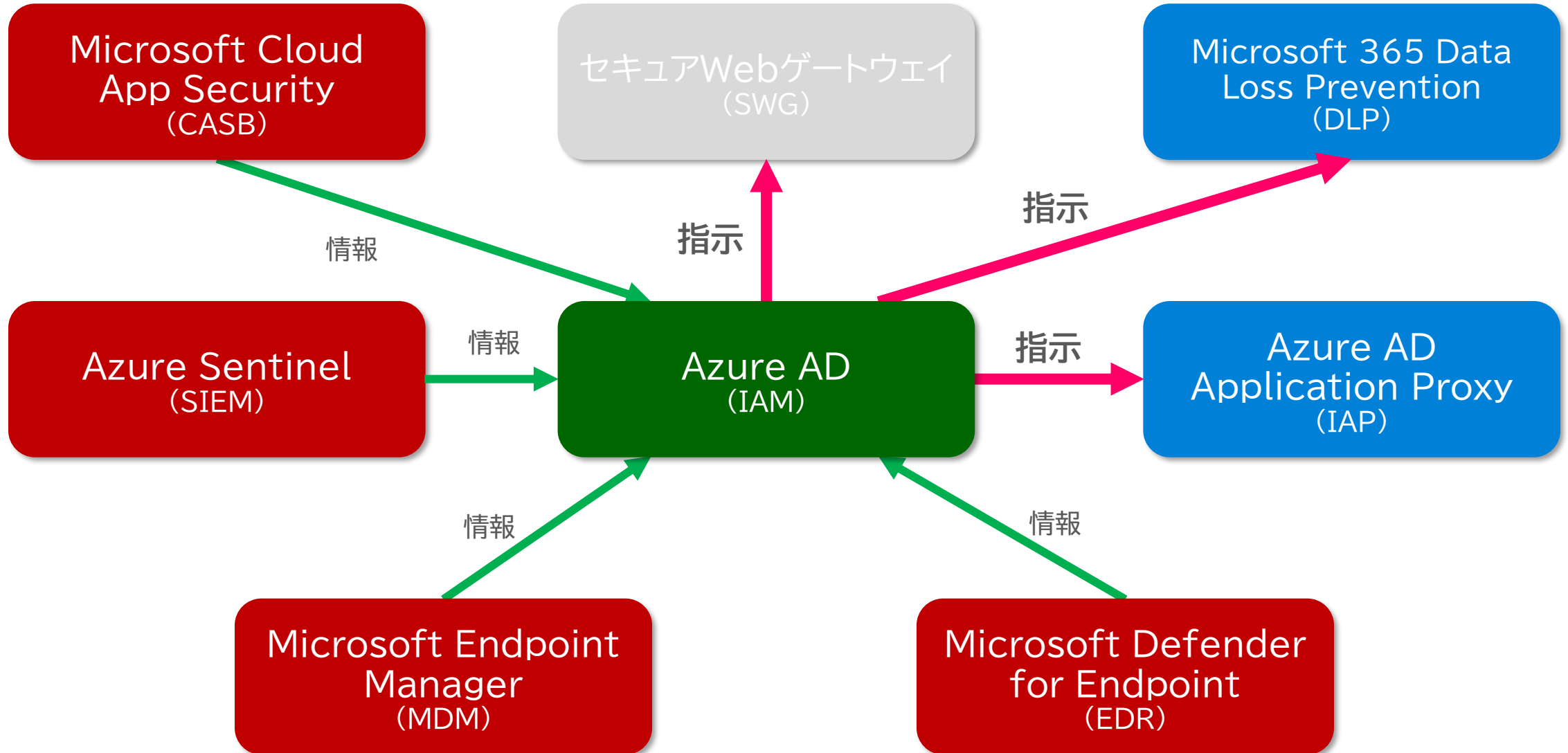
図表 1 2 アクセス認証型と境界防御型の違い

アクセス認証型 (ゼロトラスト)	境界防御型
端末の認証やセキュリティ対策を充実させ、それぞれのリソースへのアクセス認証や通信の保護を徹底することで、ネットワークによる制限を必要としない手法。 接続するネットワークを限定しないため、リモートワーク等の働き方改革の推進に有効。	内部ネットワークと外部ネットワークを明確に切り離すことで、機密性を高める手法。 学校内からの通信のみに限定した場合に有効。

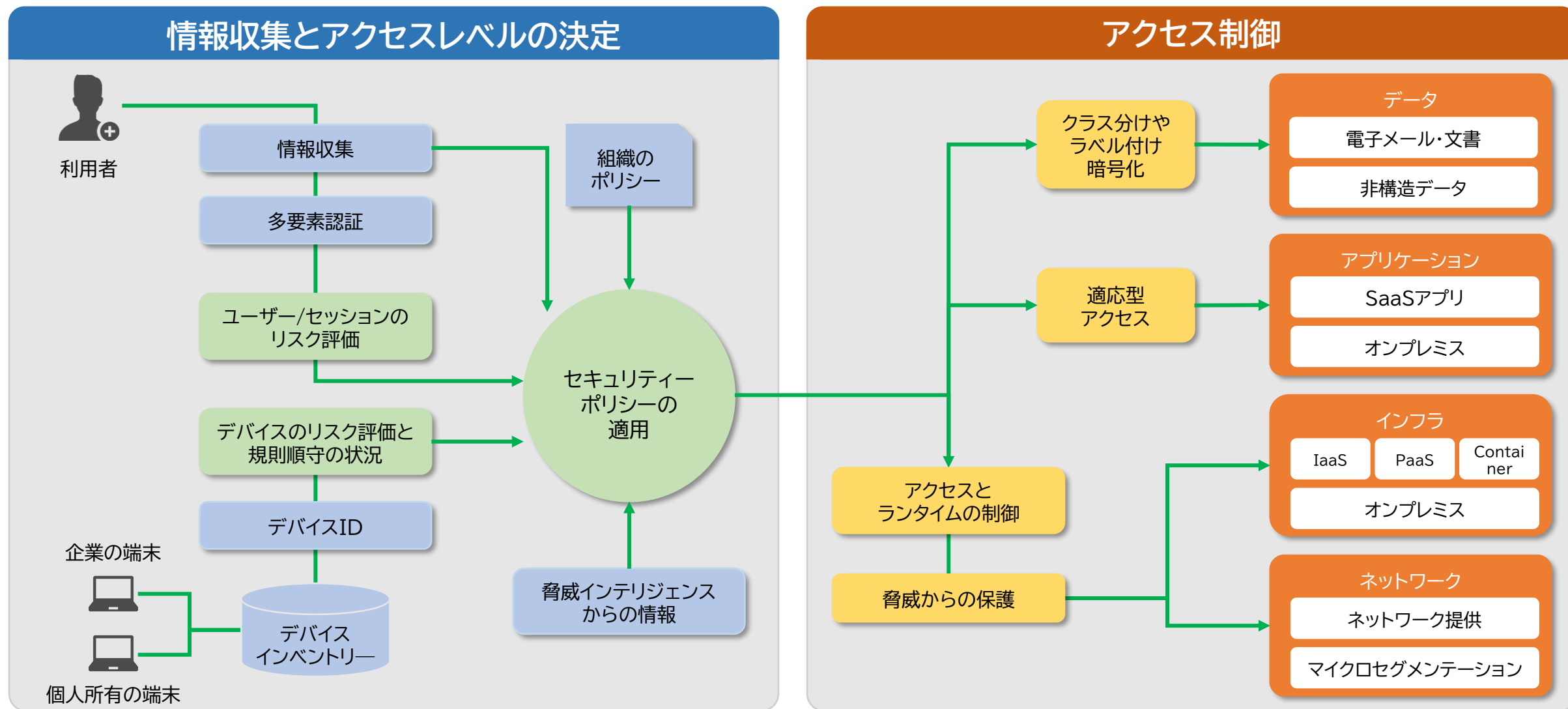
Zero Trust に必要な技術



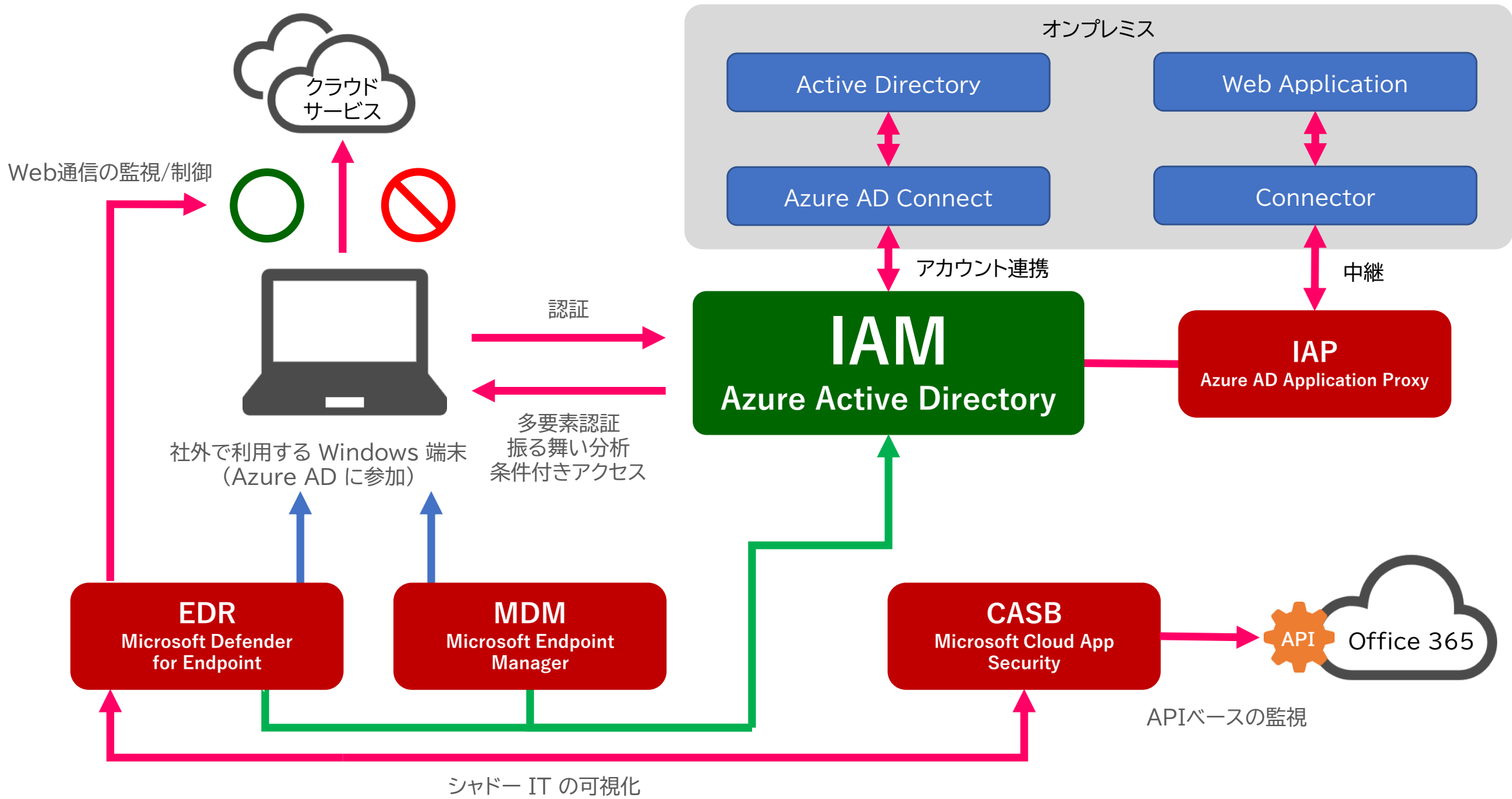
Microsoft 製品のカバレッジ



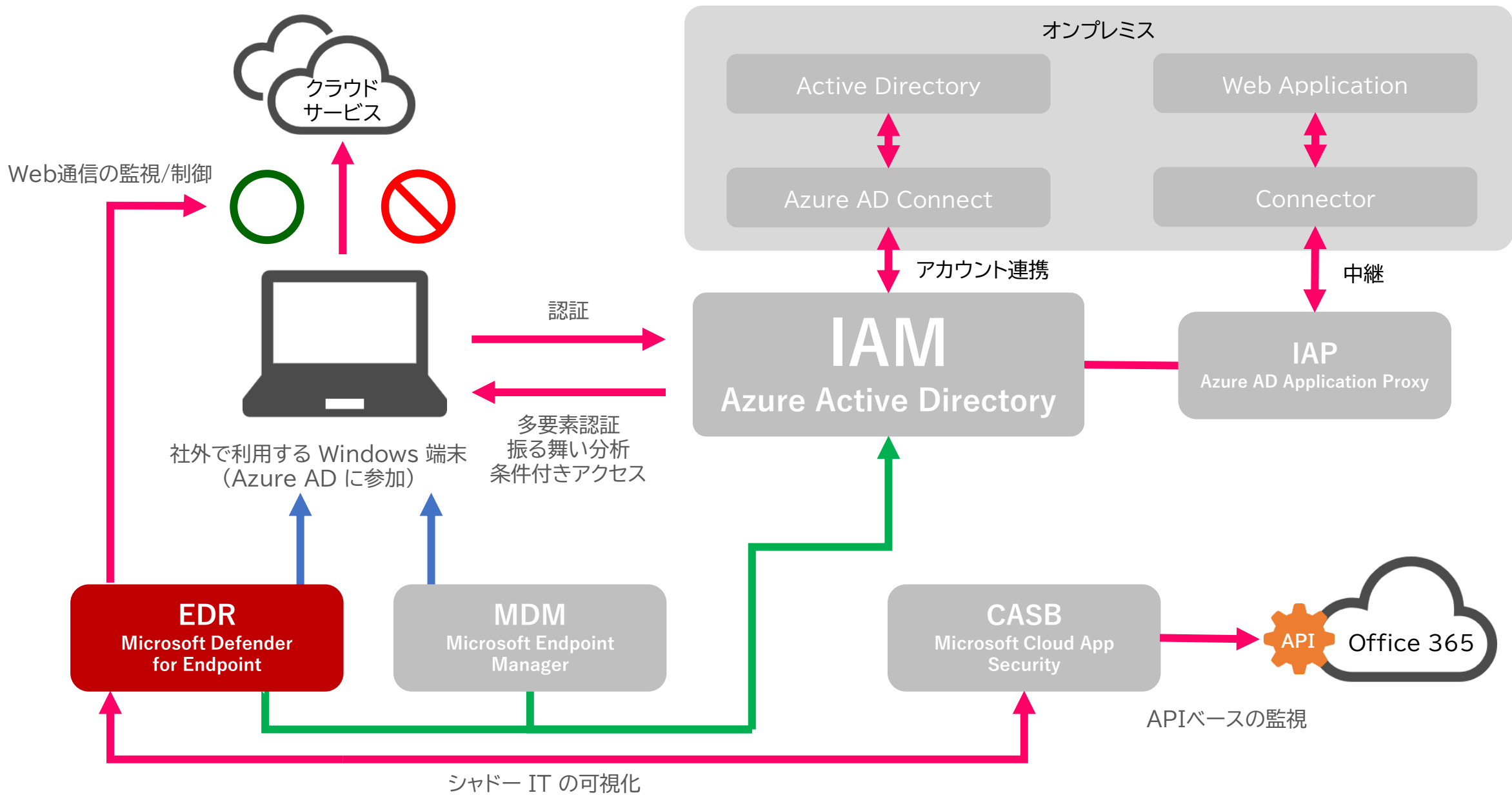
Microsoft が考える Zero Trust strategy



Microsoft 製品で構築する Zero Trust



Microsoft 製品で構築する Zero Trust



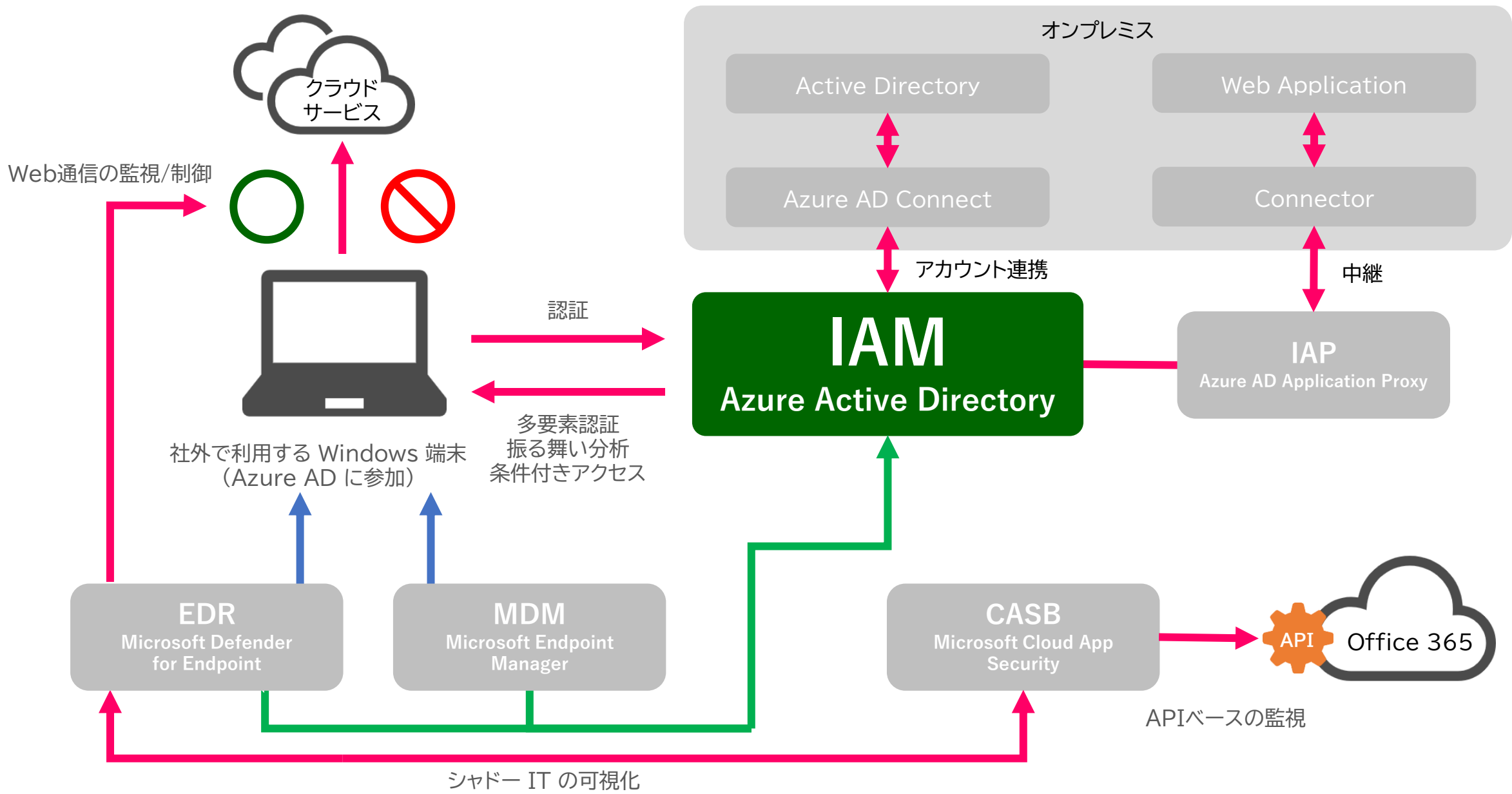
Microsoft Defender Family



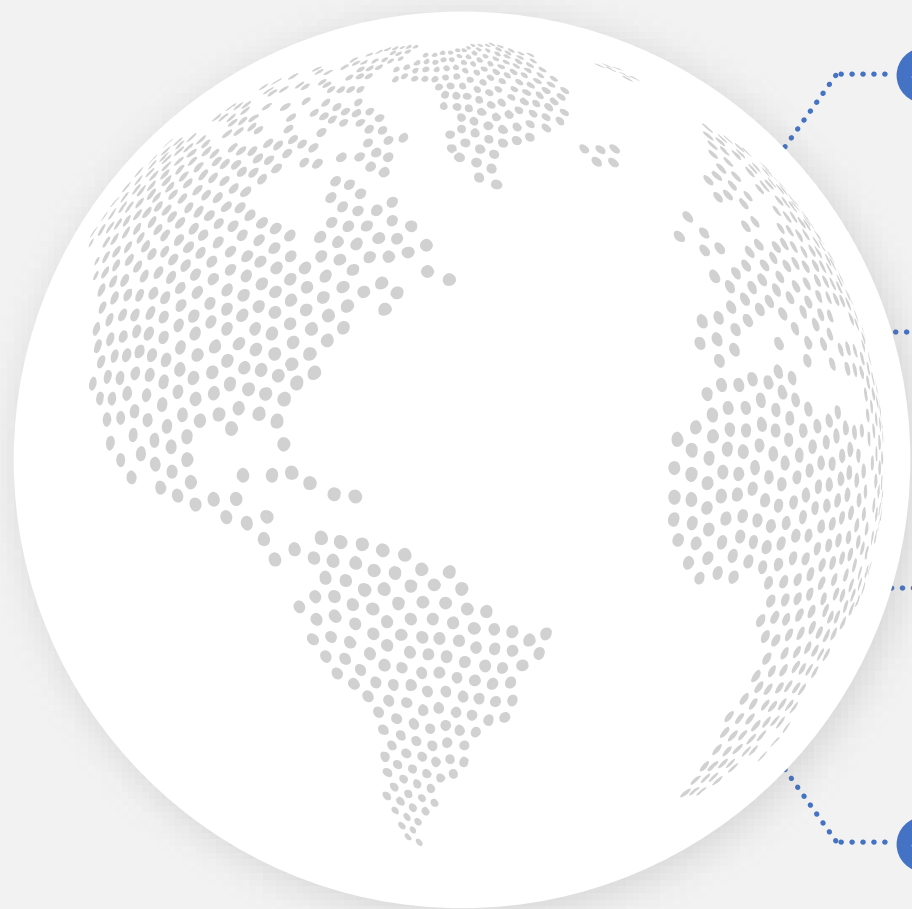
機能名	主な内容	Win 10 Pro Education	Win 10 Education A3	Win 10 Education A5
Microsoft Defender ウィルス対策	ウィルス対策	●	●	●
Microsoft Defender ファイアウォール	パーソナルファイアウォール	●	●	●
Microsoft Defender Smart Screen	危険なWebサイトからの保護	●	●	●
Microsoft Defender Exploit Guard	ランサムウェア対策	●	●※1	●※1
Microsoft Defender Device Guard	標的型攻撃からのデバイス保護		●	●
Microsoft Defender Application Control	ホワイトリストベースのアプリケーションの制御		●	●
Microsoft Defender Credential Guard	標的型攻撃からの資格情報の保護		●	●
Microsoft Defender Application Guard	仮想ブラウザ		●	●
Microsoft Defender for Endpoint (旧 ATP)	EDRなどセキュリティ統合監視・管理			●

※1 A3およびA5 では、より高度な監視機能とレポート機能が利用できます。

Microsoft 製品で構築する Zero Trust



Azure AD のオープンで相互運用可能なエコシステム



✓ シングルサインオン



SAML v2.0



✓ プロビジョニング

SCIM

✓ パスワードレス



WebAuthn

✓ De-centralized アイデンティティ



Azure Active Directory



	FREE	OFFICE 365 APPS	for Education	PREMIUM P1	PREMIUM P2
Core Identity and Access Management					
Directory Objects ¹	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit	No Object Limit
Single Sign-On (SSO) ²	up to 10 apps	up to 10 apps	up to 10 apps	unlimited	unlimited
User provisioning	Available	Available	Available	Available	Available
Federated Authentication (ADFS or 3rd party IDP)	Available	Available	Available	Available	Available
User and group management (add/update/delete)	Available	Available	Available	Available	Available
Device registration	Available	Available	Available	Available	Available
Cloud Authentication (Pass-Through Auth, Password Hash sync, Seamless SSO)	Available	Available	Available	Available	Available
Azure AD Connect sync (extend on-premises directories to Azure AD)	Available	Available	Available	Available	Available
Self-Service Password Change for cloud users	Available	Available	Available	Available	Available
Azure AD Join: desktop SSO & administrator bitlocker recovery	Available	Available	Available	Available	Available
Password Protection (global banned password)	Available	Available	Available	Available	Available
Multi-Factor Authentication ³	Available	Available	Available	Available	Available
Basic security and usage reports	Available	Available	Available	Available	Available
Business to Business Collaboration					
Azure AD features for guest users ⁴	Available	Available	Available	Available	Available
Identity & Access Management for Office 365 apps					
Company branding (customization of logon & logout pages, access panel)	Not available	Available	Available	Available	Available
Self-service password reset for cloud users	Not available	Available	Available	Available	Available
Service Level Agreement (SLA)	Not available	Available	Available	Available	Available
Device write-back (device objects two-way synchronization between on-premises directories and Azure)	Not available	Available	Available	Available	Available
Premium Features					
Password Protection (custom banned password)	Not available	Not available	Not available	Available	Available
Password Protection for Windows Server Active Directory (global & custom banned password)	Not available	Not available	Not available	Available	Available
Self-service password reset/change/unlock with on-premises write-back	Not available	Not available	Not available	Available	Available
Group access management	Not available	Not available	Not available	Available	Available
Microsoft Cloud App Discovery ⁵	Not available	Not available	Not available	Available	Available
Azure AD Join: MDM auto enrollment & local admin policy customization	Not available	Not available	Available	Available	Available
Azure AD Join: self-service bitlocker recovery, enterprise state roaming	Not available	Not available	Available	Available	Available
Advanced security and usage reports	Not available	Not available	Not available	Available	Available
Hybrid Identities					
Application Proxy	Not available	Not available	Not available	Available	Available
Microsoft Identity Manager user CAL ⁶	Not available	Not available	Not available	Available	Available
Connect Health ⁷	Not available	Not available	Not available	Available	Available

Azure Active Directory



	FREE	OFFICE 365 APPS	for Education	PREMIUM P1	PREMIUM P2
Advanced Group Access Management					
Dynamic groups	Not available	Not available	Not available	Available	Available
Group creation permission delegation	Not available	Not available	Not available	Available	Available
Group naming policy	Not available	Not available	Not available	Available	Available
Group expiration	Not available	Not available	Not available	Available	Available
Usage guidelines	Not available	Not available	Not available	Available	Available
Default classification	Not available	Not available	Not available	Available	Available
Conditional Access					
Conditional Access based on group, location, and device status	Not available	Not available	Not available	Available	Available
Azure Information Protection integration	Not available	Not available	Not available	Available	Available
SharePoint limited access	Not available	Not available	Not available	Available	Available
Terms of Use (set up terms of use for specific access)	Not available	Not available	Not available	Available	Available
Multi-Factor Authentication with Conditional Access	Not available	Not available	Not available	Available	Available
Microsoft Cloud App Security integration	Not available	Not available	Not available	Available	Available
3rd party MFA partner integrationPreview	Not available	Not available	Not available	Available	Available
3rd party identity governance partners integration	Not available	Not available	Not available	Available	Available
Identity Protection					
Vulnerabilities and risky accounts detection	Not available	Not available	Not available	Not available	Available
Risk events investigation	Not available	Not available	Not available	Not available	Available
Risk based Conditional Access policies	Not available	Not available	Not available	Not available	Available
Identity Governance					
Privileged Identity Management (PIM)	Not available	Not available	Not available	Not available	Available
Access Reviews	Not available	Not available	Not available	Not available	Available
Entitlement Management	Not available	Not available	Not available	Not available	Available
Price	Free	Included with O365		\$6 user/month	\$9 user/month

Go passwordless Hands-on tour in Azure AD with FIDO2 keys and Temporary Access Pass



セキュリティ バイ デザインによりパスワードレスを実現



Windows 11、チップからクラウドまでのセキュリティ バイ デザインを実現

2021年7月6日 | Japan News Center

デビッド ウェストン (David Weston)
エンタープライズ & OS セキュリティ担当ディレクター

※本ブログは、米国時間 6 月 25 日に公開された "[Windows 11 enables security by design from the chip to the cloud](https://news.microsoft.com/ja-jp/2021/07/06/210706-windows-11-enables-security-by-design-from-the-chip-to-the-cloud/?fbclid=IwAR09I1B0Q6J66IMF3qzwRZ1aqZPglEnL5Dk3fcEdfX85ANSeUdd65yVnPJA)" の抄訳を基に掲載しています。



<https://news.microsoft.com/ja-jp/2021/07/06/210706-windows-11-enables-security-by-design-from-the-chip-to-the-cloud/?fbclid=IwAR09I1B0Q6J66IMF3qzwRZ1aqZPglEnL5Dk3fcEdfX85ANSeUdd65yVnPJA>

端末の認証基盤は

Active Directory から [Azure Active Directory](#) へ

マイクロソフトのサポートを装った詐欺にご注意ください

<https://news.microsoft.com/ja-jp/2021/01/29/210129-information/>

