

JNSA アイデンティティ管理WG10周年記念
「企業及びクラウドにおけるアイデンティティ管理セミナー」

Active Directory 15 年の歩みとこれから

日本マイクロソフト株式会社
プリンシパル テクニカル エバンジェリスト
安納 順一 Junichi Anno

ざっくりと History

2000年 Windows 2000 Server に Active Directory を実装

- Kerberos / LDAP / NTLM / NIS / Radius / 802.1x に対応

2005年 Windows Server 2003 R2 に Federation Service 実装するも、市場からはほぼ無視状態

2008年 Active Directory のブランディングを変更

AD Domain Services : ドメインコントローラー

AD Lightweight Directory Services : LDAP

AD Certificate Services : 証明書サービス

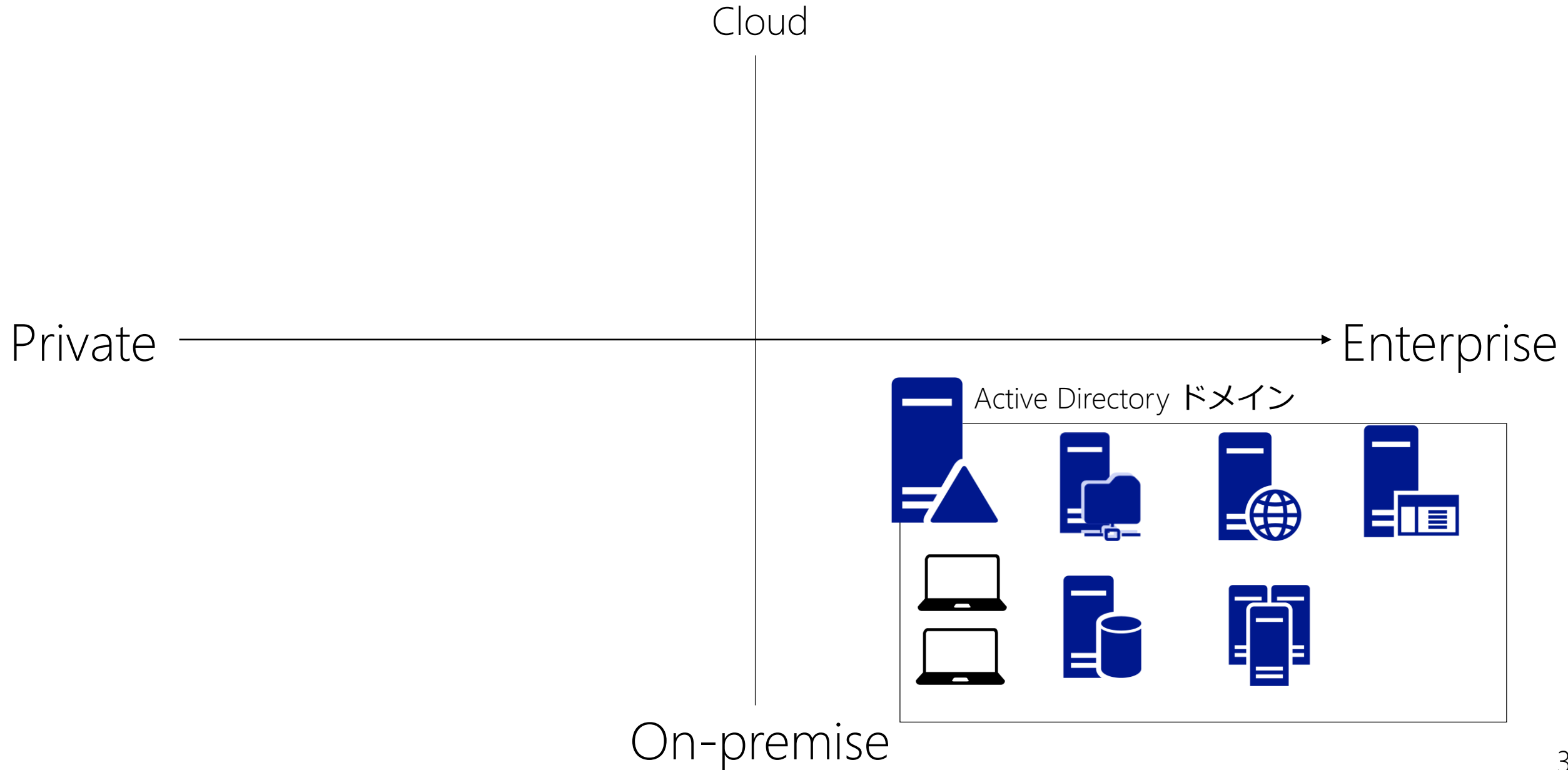
AD Rights Management Services : 権限管理サービス

AD Federation Services : フェデレーションサービス

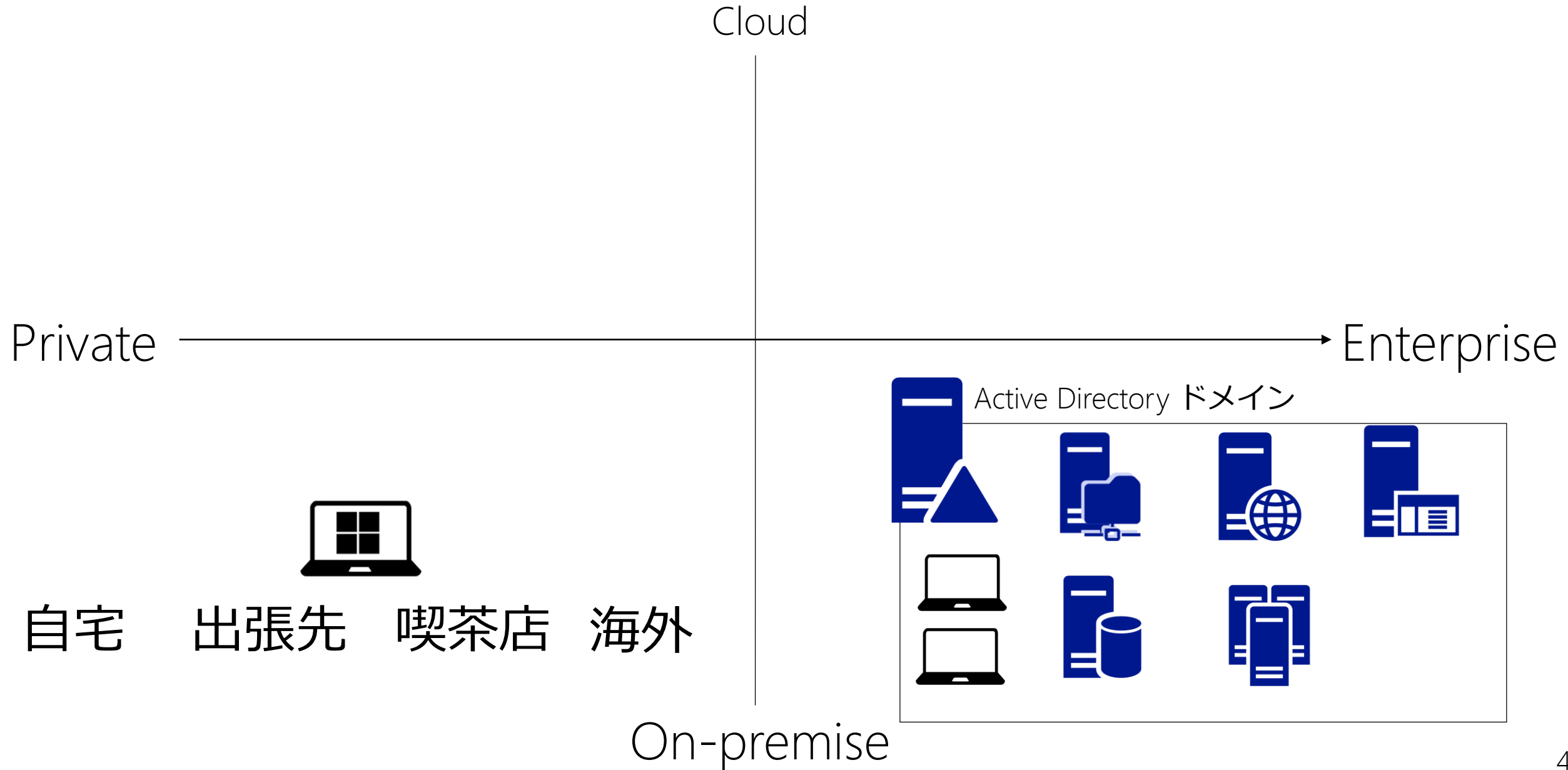
2013年 SaaS タイプの IdP (IDaaS) Azure Active Directory 登場

2015年 Windows 10 で Azure AD Join をサポート。

当初の Active Directory は中を守るもの

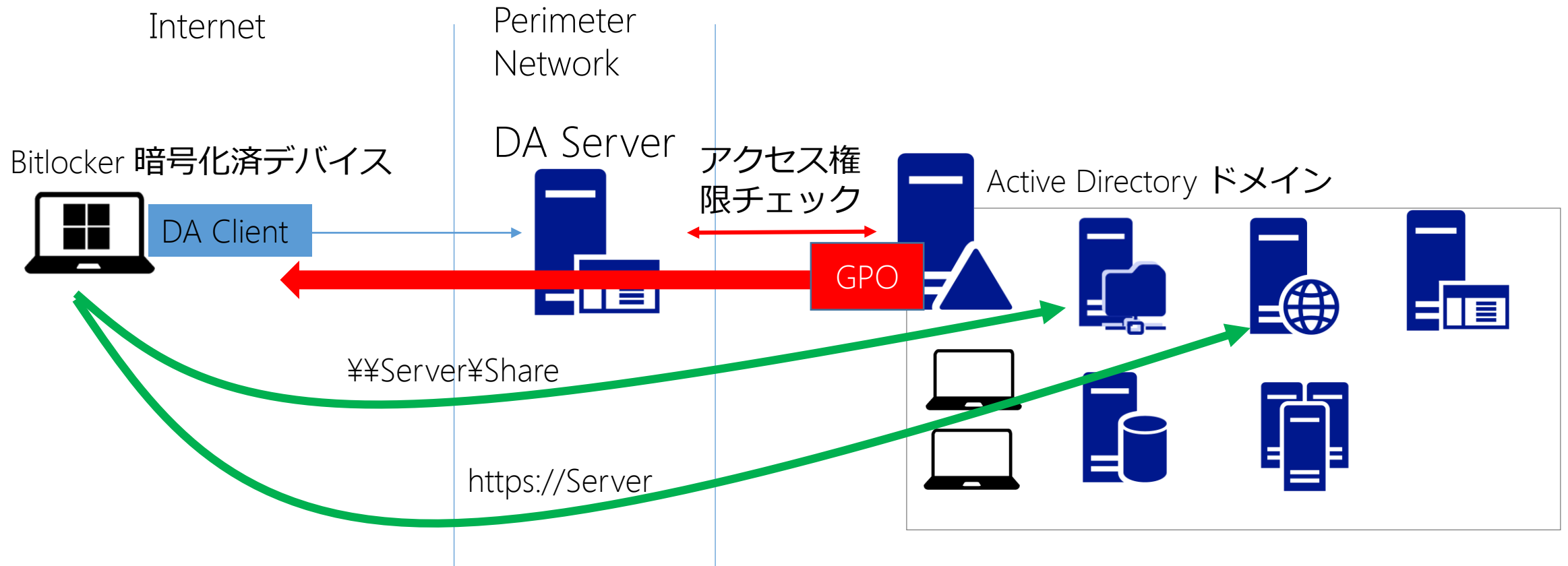


2008年～働き方の変化と Consumerization of IT の波

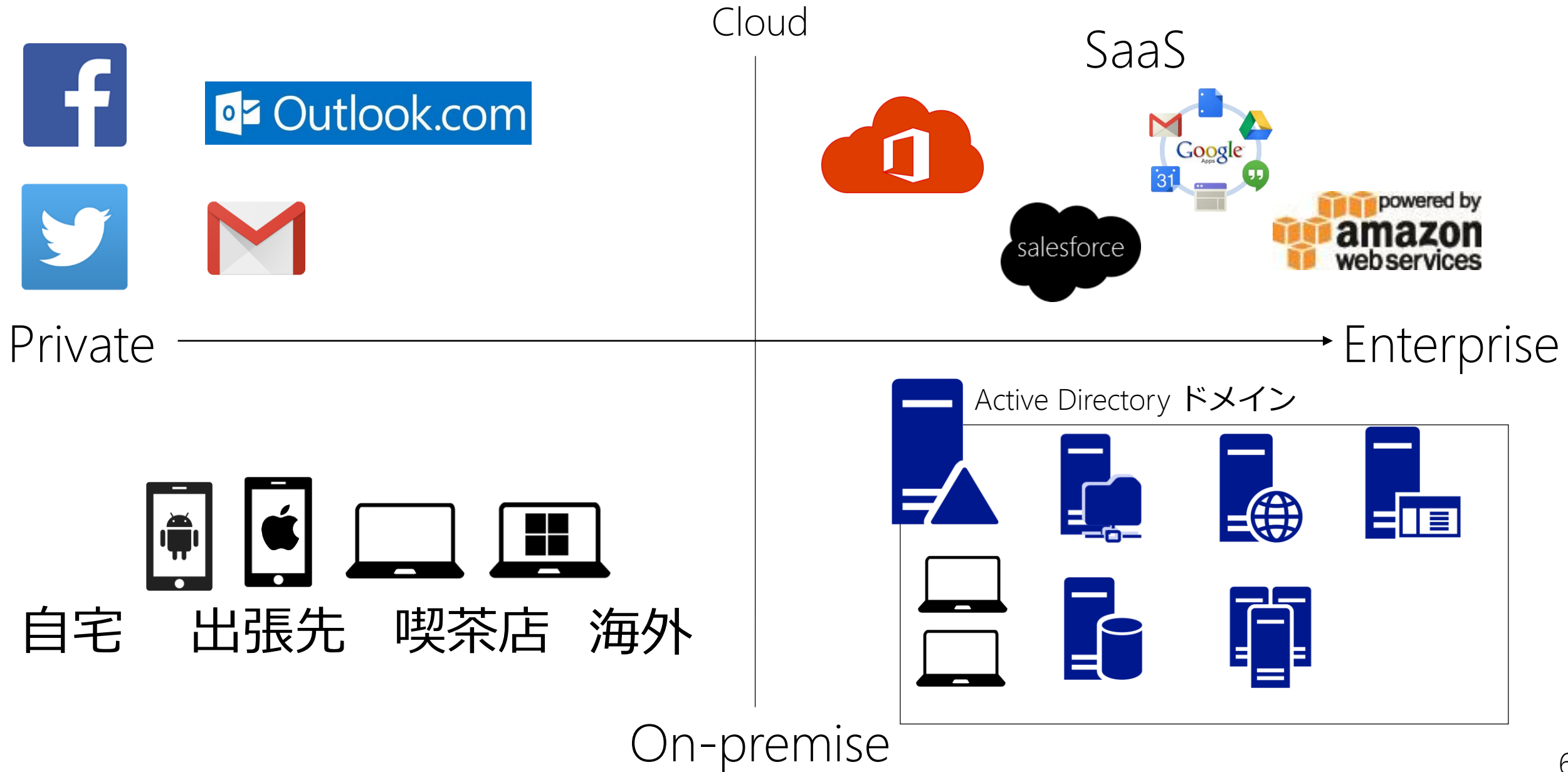


Direct Access (Windows Server 2008) for Windows Client

- Always Connected な VPN、PC起動と同時に有効化
- DA Client の活性化はセキュリティポリシーで制御
- 社内と社外とで使い方に違いを作らない
- 対象は ドメインに参加している Windows 7 以降

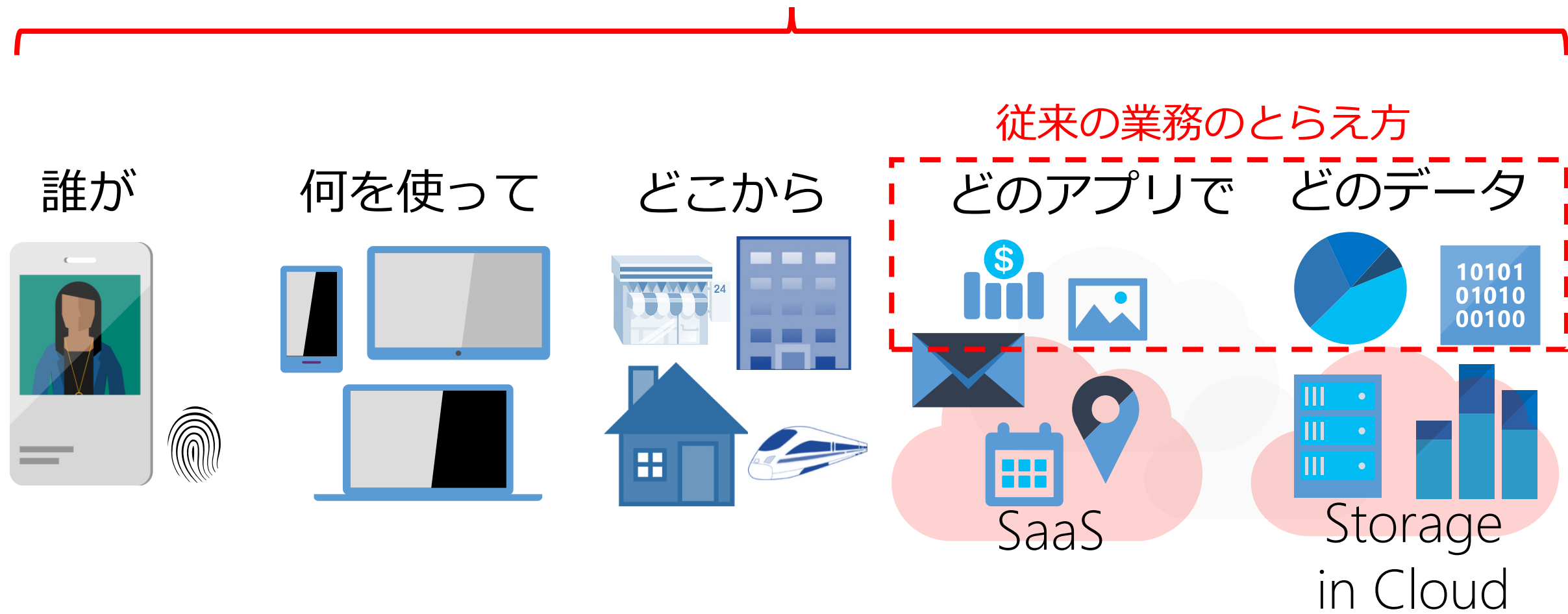


クラウドとモバイルデバイスの登場



業務形態の見直し

クラウドやモバイルデバイスの登場により、業務を広くとらえる必要が出てきた

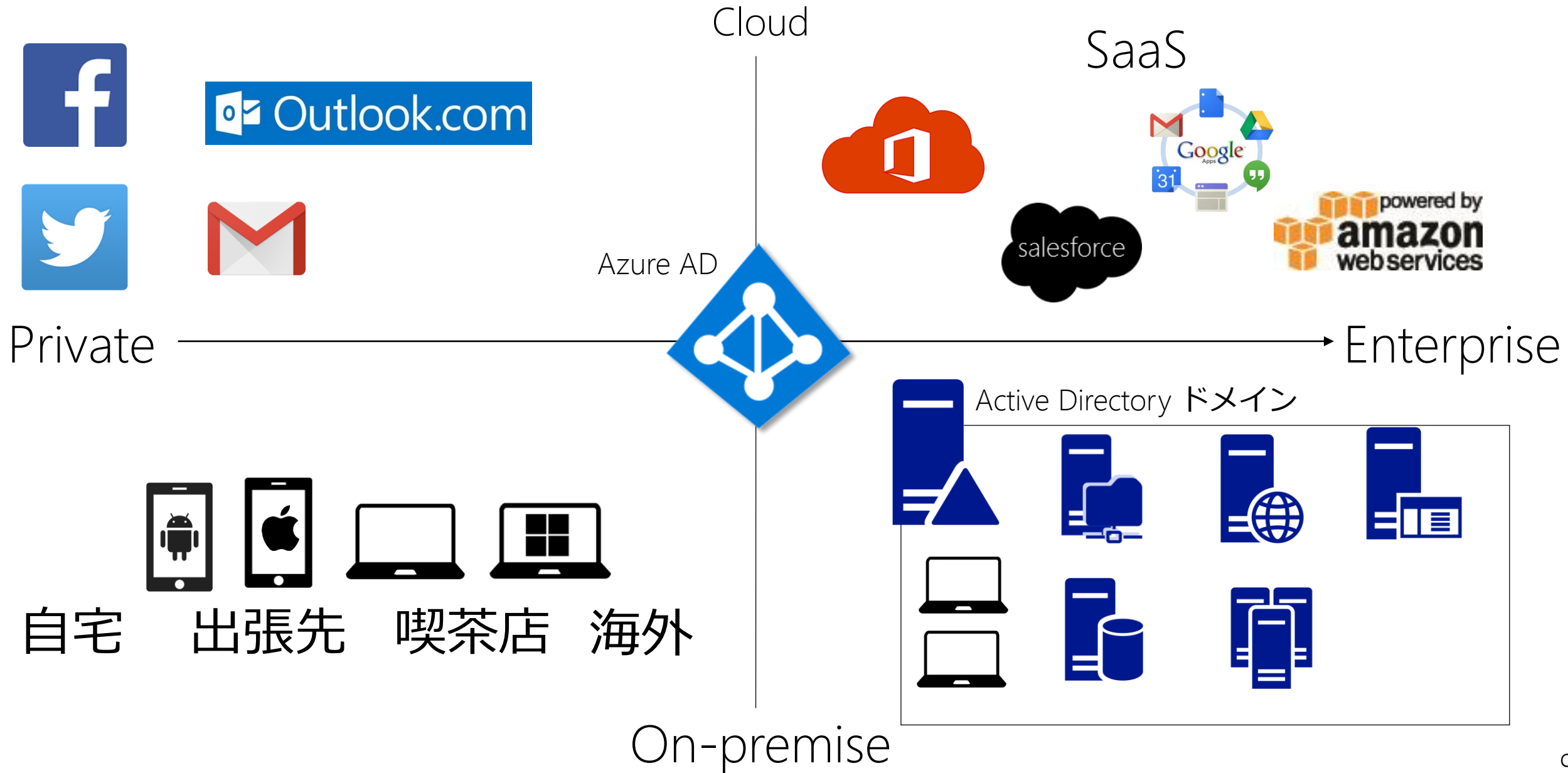


城下町

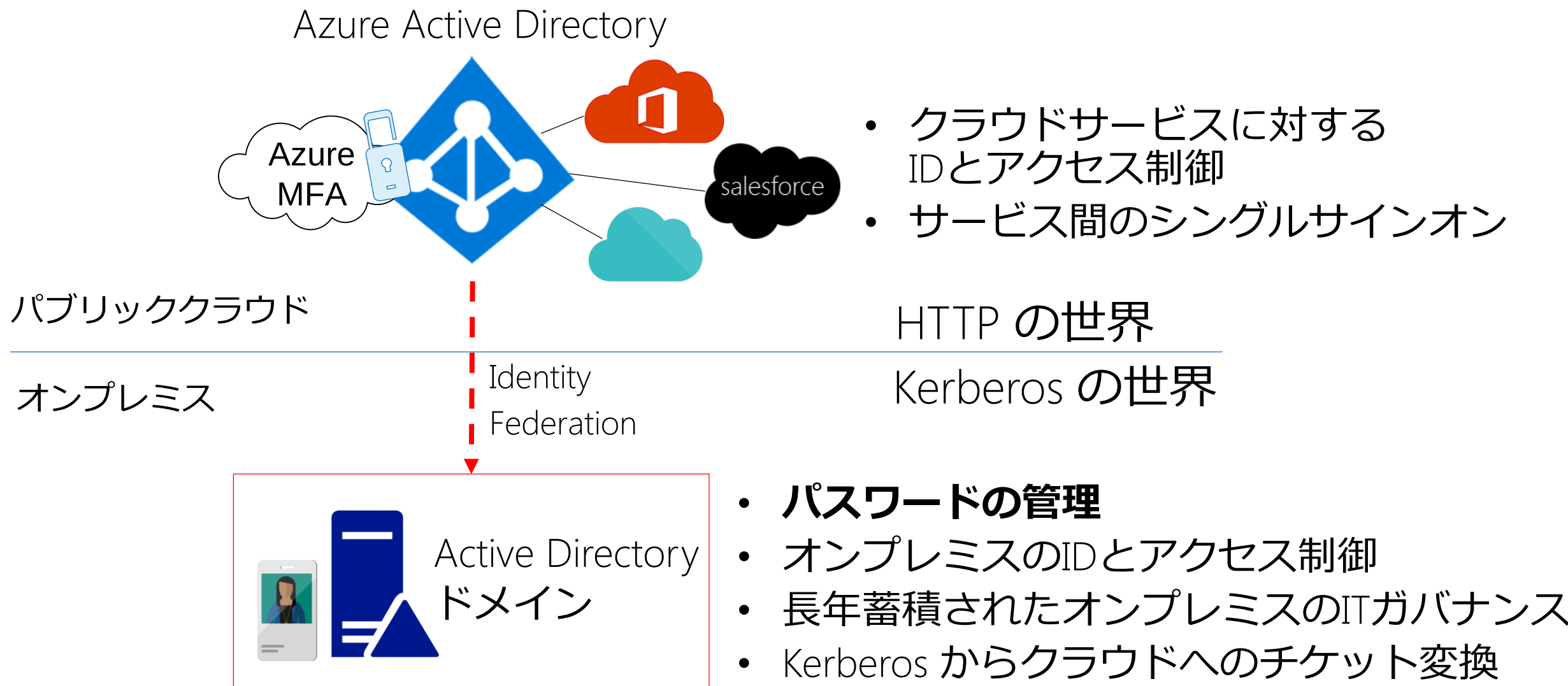
関所



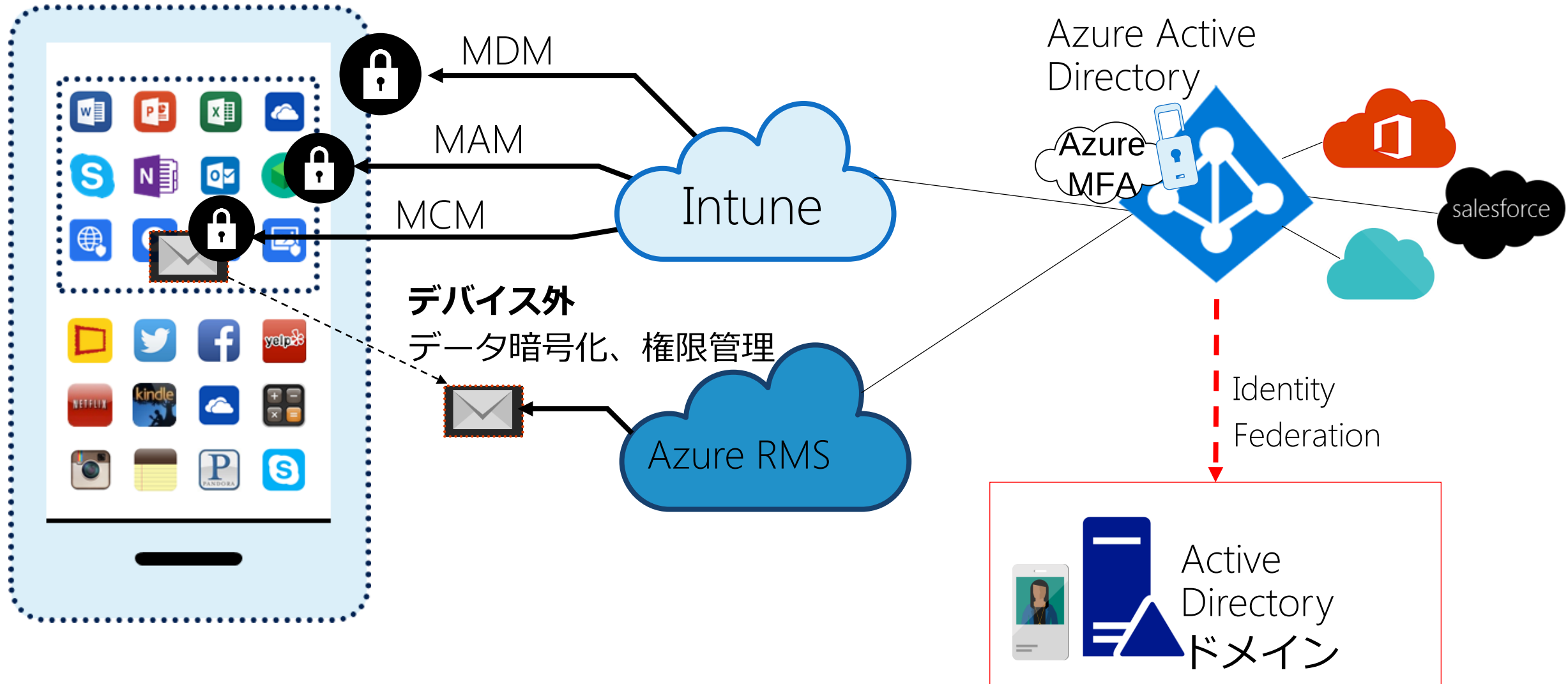
関所となるセキュリティハブの必要性



クラウドとオンプレミスのフェデレーション

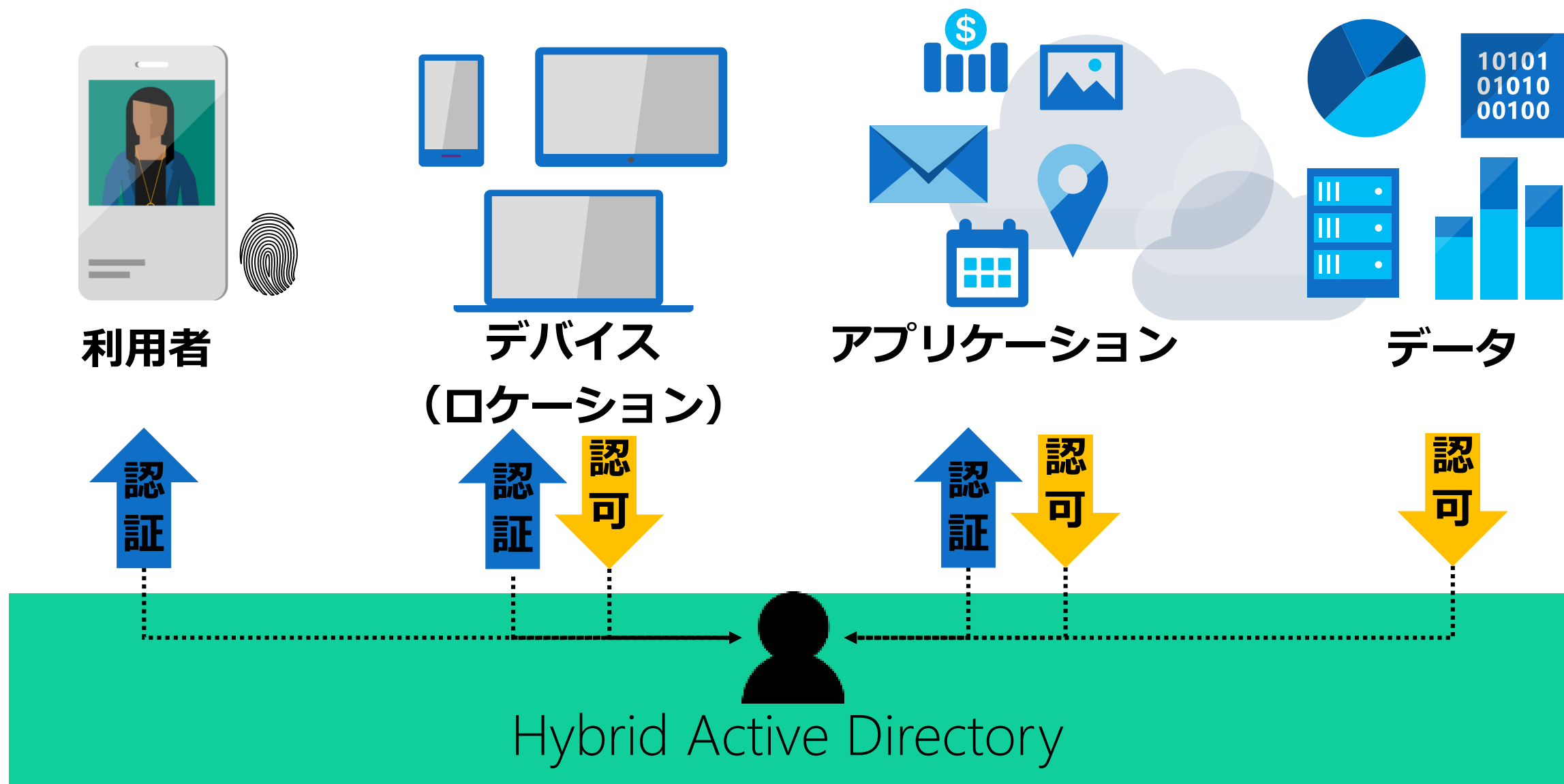


ユーザーを中心としたデバイス、アプリ、データ防衛

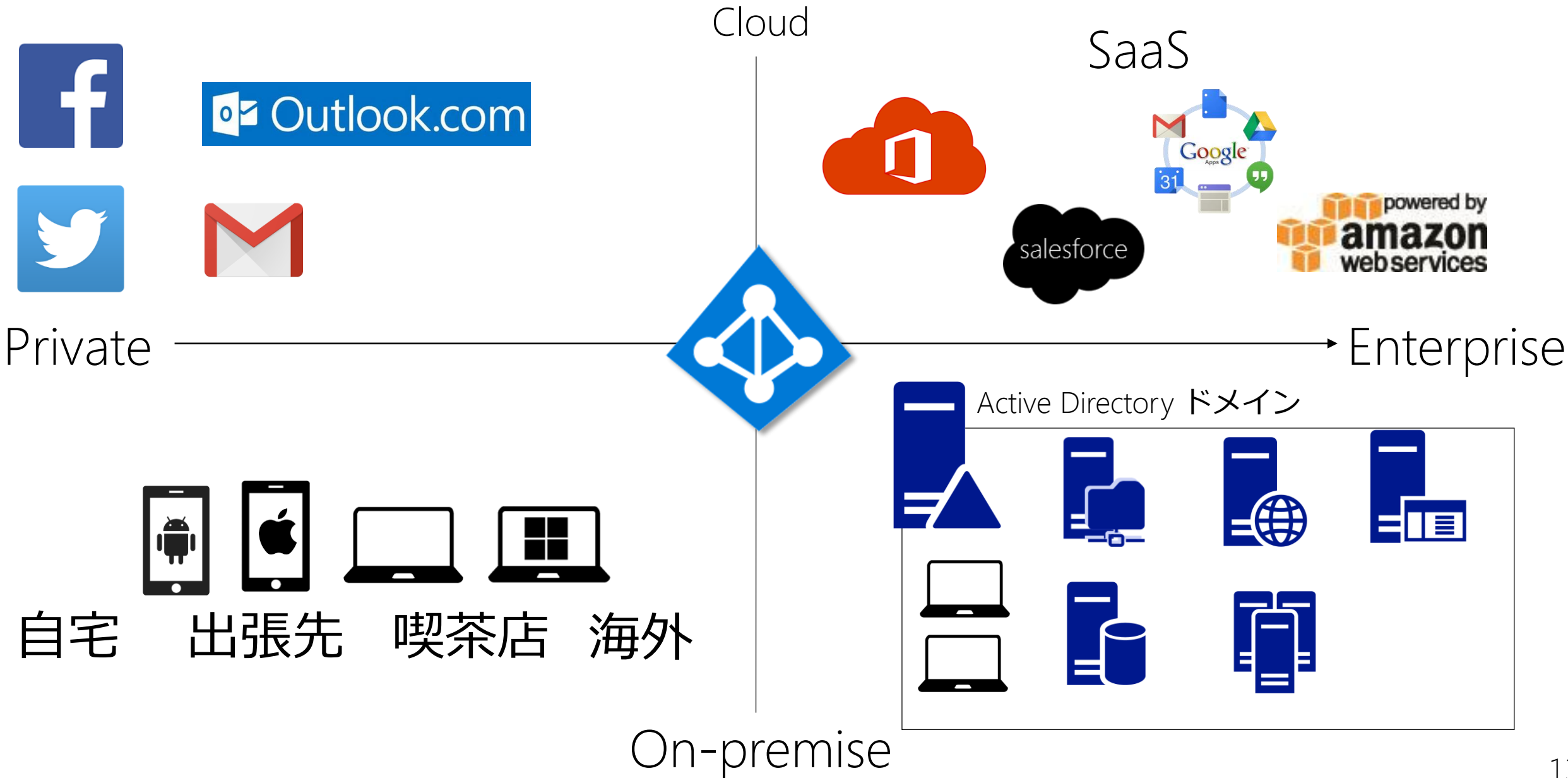


People-Centric IT ～ ID を中心とした多層防御

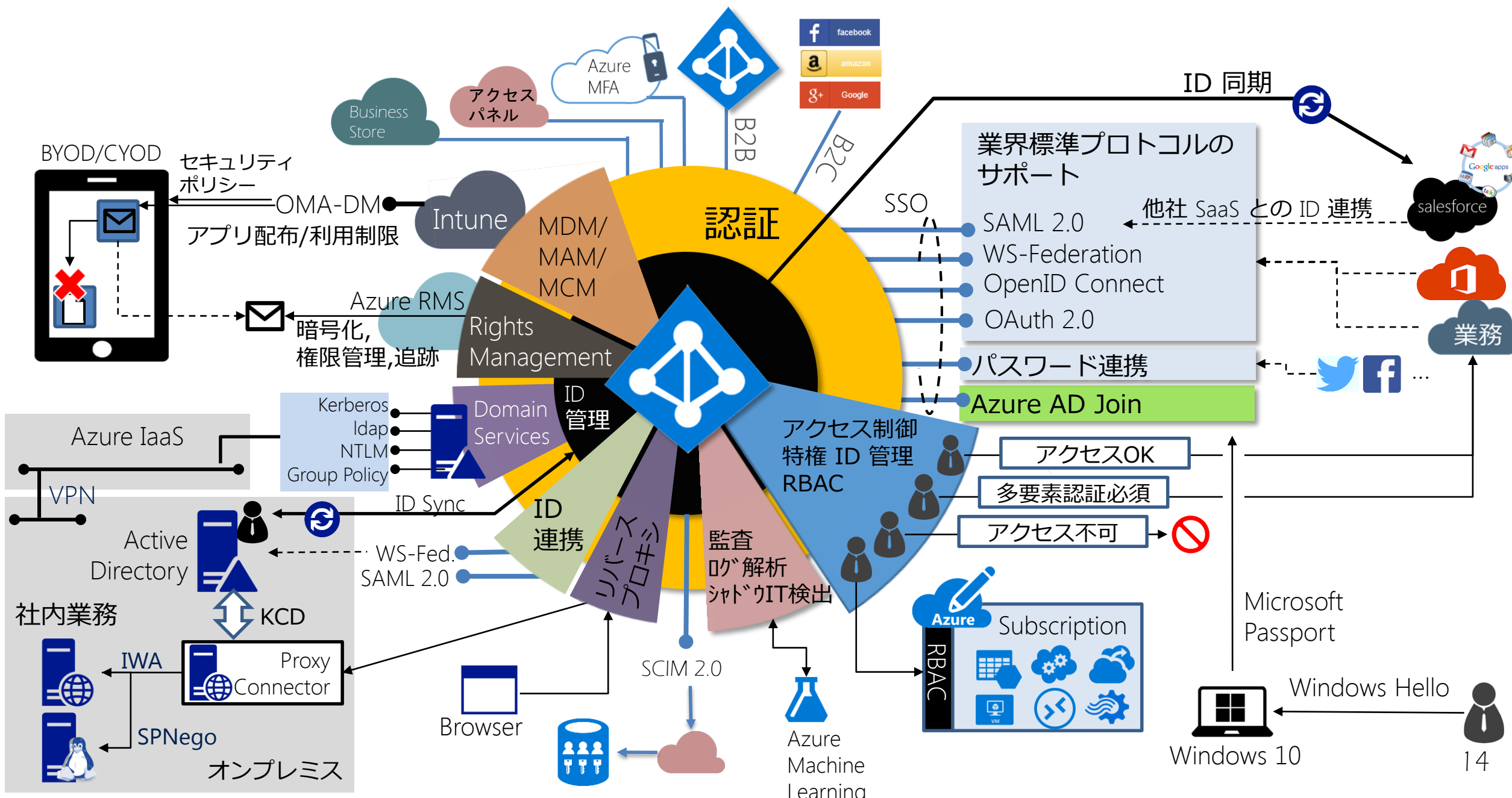
守るためには「対象の特定」が必要であり、合理的な特定には「関所」が必要



Identity is the Control Plane



Identity is Control Plane



(参考)Azure Active Directory 各エディション と Office 365 IAM の比較

2015.11.18 版

		Azure Active Directory Free	Azure Active Directory Basic	Azure Active Directory Premium	Office 365 IAM
Common Features	ディレクトリサービス	500,000 Object Limit	No Object Limit	No Object Limit	No Object limit for Office 365 user
	ユーザー/グループ管理（追加、削除、更新）	Yes	Yes	Yes	Yes
	AADと統合されたアプリ（SaaS/LOB）間の SSO（ユーザーあたり）	10 apps per user	10 apps per user	No Limit	10 apps per user
	ユーザーベースのアクセス管理/プロビジョニング	Yes	Yes	Yes	Yes
	Azure AD Connect	Yes	Yes	Yes	Yes
	セキュリティレポート	3 Basic Reports	3 Basic Reports	Advanced	3 Basic Reports
	B2B（Preview）	Yes	Yes	Yes	Yes
	B2C（Preview）	Yes 別料金	Yes 別料金	Yes 別料金	
	ドメインサービス（Preview）	Yes 別料金	Yes 別料金	Yes 別料金	
Premium+ Basic Features	グループベースのアクセス管理/プロビジョニング		Yes	Yes	
	ブランディング機能 (Logon Pages/Access Panel customization)		Yes	Yes	Yes
	セルフサービス パスワードリセット		Yes	Yes	
	アプリケーションプロキシ		Yes	Yes	
	SLA		Yes 99.9	Yes 99.9	Yes 99.9
Premium Features	Azure AD Connect 拡張属性、デバイス、NGC の書き戻し			Yes	
	セルフサービス グループ管理			Yes	
	パスワードのオンプレミスに書き戻し機能			Yes	
	高度なセキュリティレポート			Yes	
	多要素認証プロバイダー（クラウド&オンプレミス）			Yes	Office 365 に制限
	MIM CAL + MIM Server CAL			Yes	
	管理機能の委任			Yes	
	Cloud App Discovery			Yes	
	Azure AD Connect Health			Yes	
	特権ID管理 2015年10月 GA済			Yes	
	動的グループ管理(Preview)			Yes	
	アプリ追加のセルフサービス（Preview）			Yes	
	多要素認証 と場所ベースのアクセスルール（Preview）			Yes	
	SCIM 2.0（outbound : Azure AD ⇒ External Store）			Yes	

Active Directory のこれから

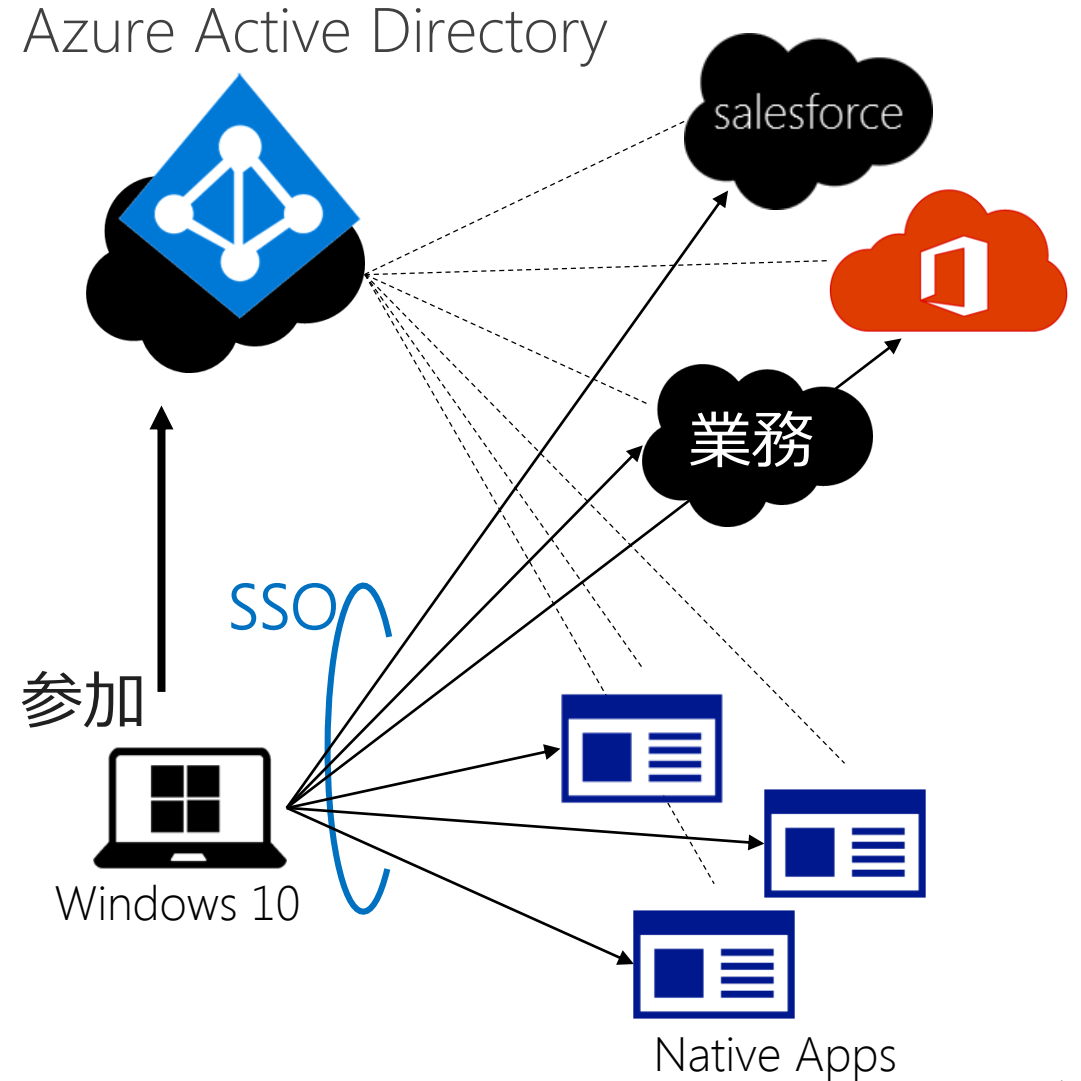
オンプレミス主導からクラウド主導へ

主役は徐々に IDaaS へ

- Azure AD Join from Windows 10
- Azure AD DRS (デバイス登録サービス)
- Azure AD MFA (多要素認証) Provider
- Azure AD Domain Services
- Azure AD B2B
- Azure AD B2C
- Azure Application Proxy
- Azure AD RBAC for Azure Resource Manager
- Azure KeyVault

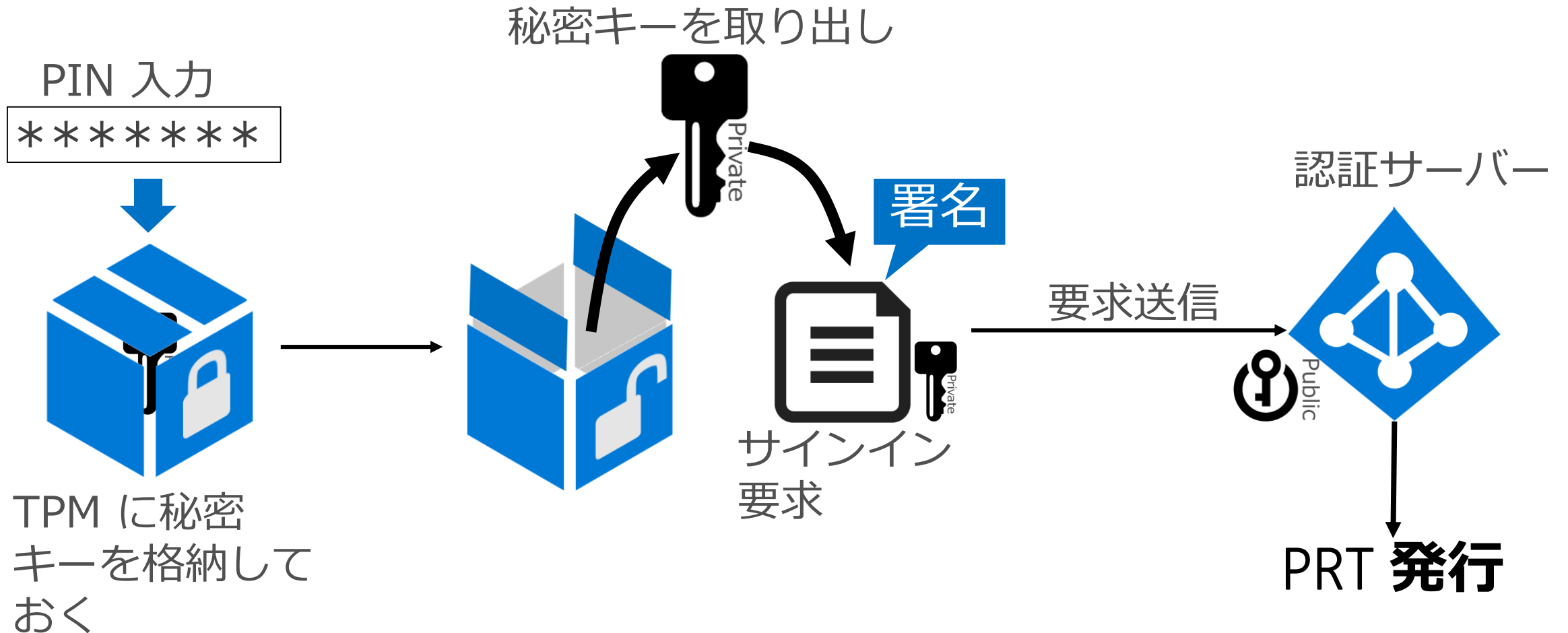
Azure AD Join

- Windows 10 は Azure Active Directory に参加できる
- Azure AD に参加すると
 - Microsoft Passport **が活性化**し、以下のサービス間は完全な SSO
 - ✓ Azure AD に関連付けられたサービス
 - ✓ Web Account Manager に対応し、Azure AD を使用する Windows 10 ネイティブアプリ
 - Microsoft Intune を契約している場合、自動的にプロビジョニングされる



Microsoft Passport

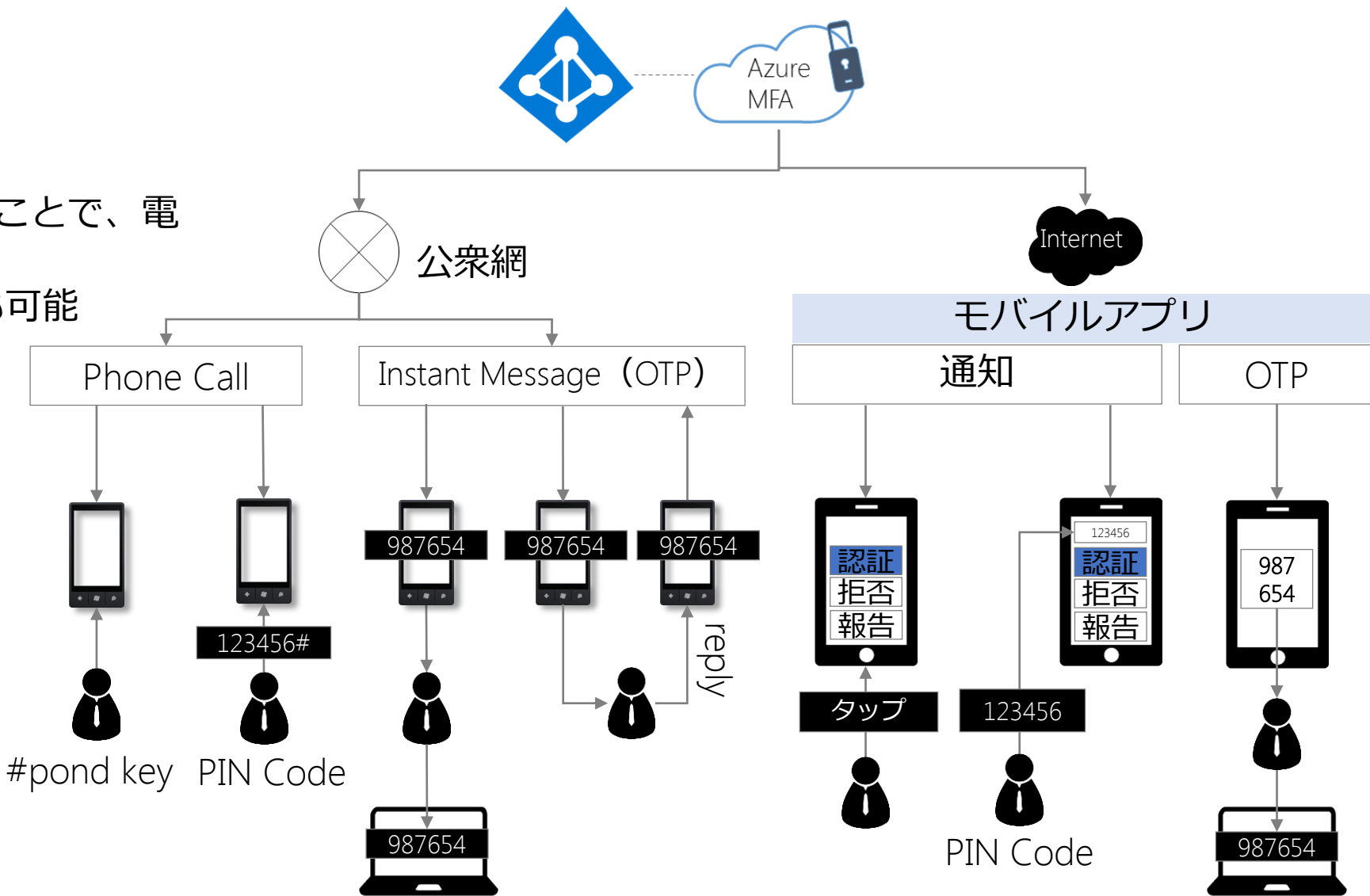
パスワードではなく、署名付きサインイン要求を送付する



Azure AD MFA

- 複数の電話番号設定可能
- 2つ以上のオプションを設定することで、電話紛失等へのリスクを回避
- オンプレミス AD からのキックも可能

PIN : 利用者が設定したコード
OTP : MFA プロバイダーが生成したワンタイムパスワード
(有効期間は規定で60秒)
※入力ミスの最大回数を設定できる

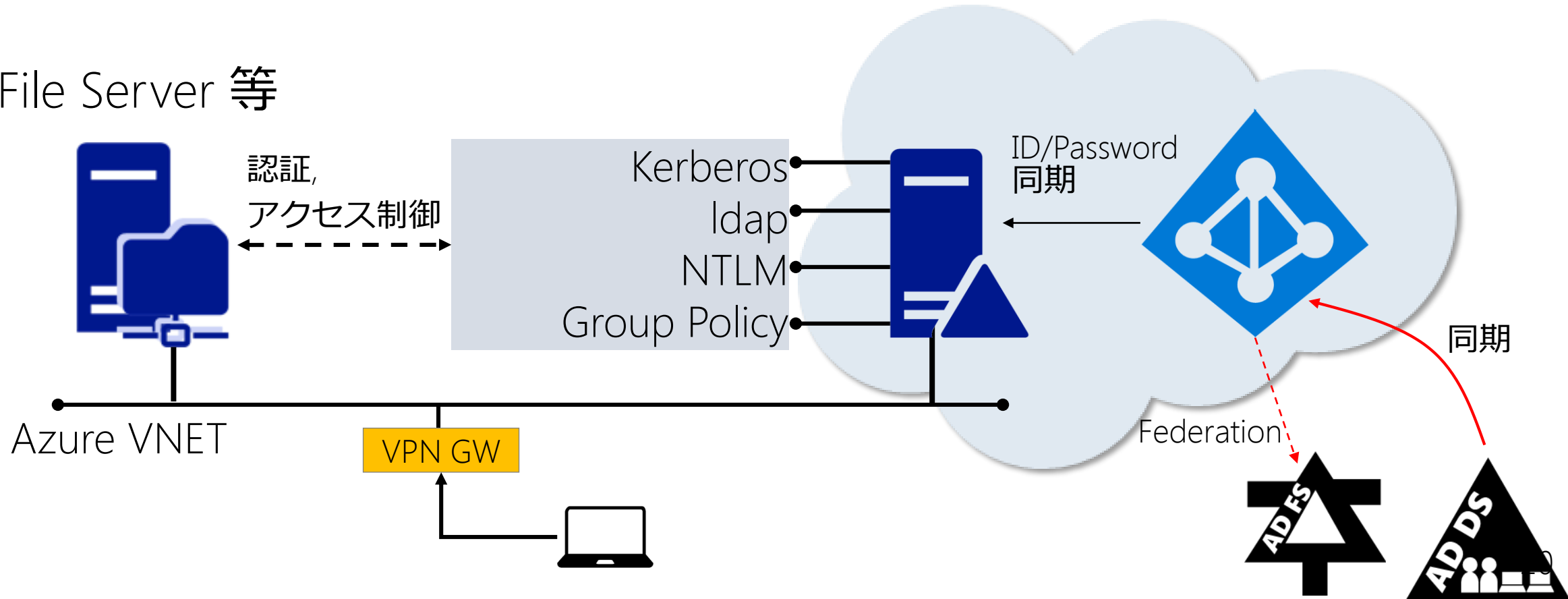


Azure MFA	○		○		○		○
Azure MFA + MFA Server	○	○	○	○	○	○	○

Azure AD Domain Services preview

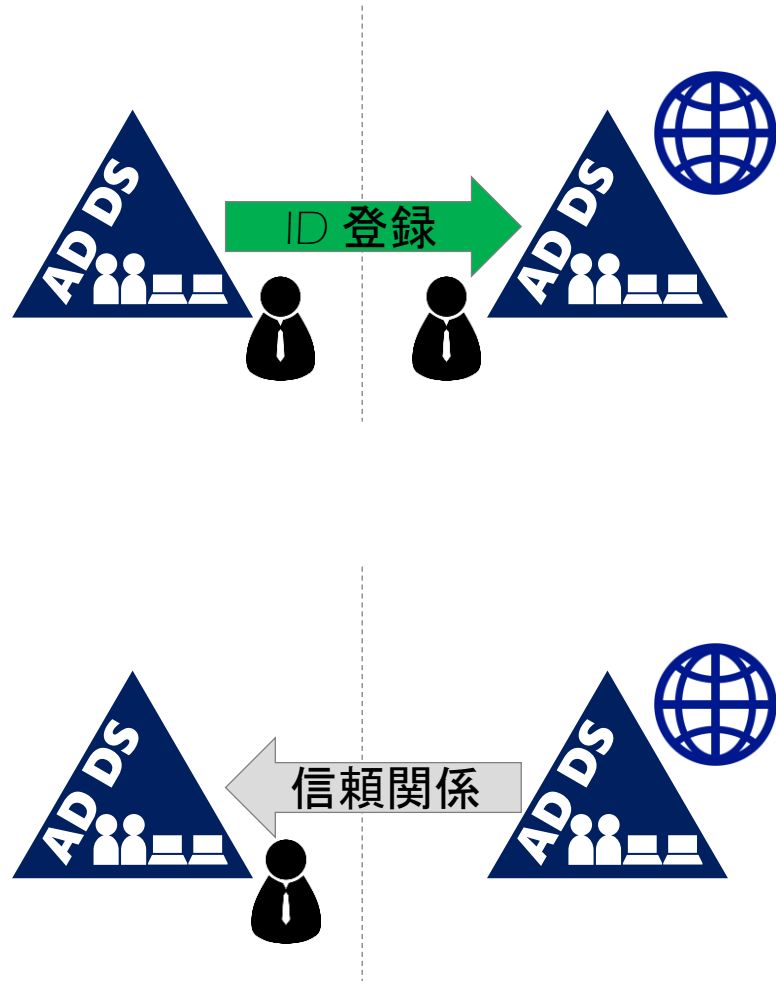
- Azure Active Directory をドメインコントローラーとして使用する機能
 - 正確には、Azure AD テナントと同期するドメインコントローラーを Azure VNET 上に自動展開するサービス
- **(注意) 複製方向は Azure AD ⇒ ドメインコントローラー**

File Server 等

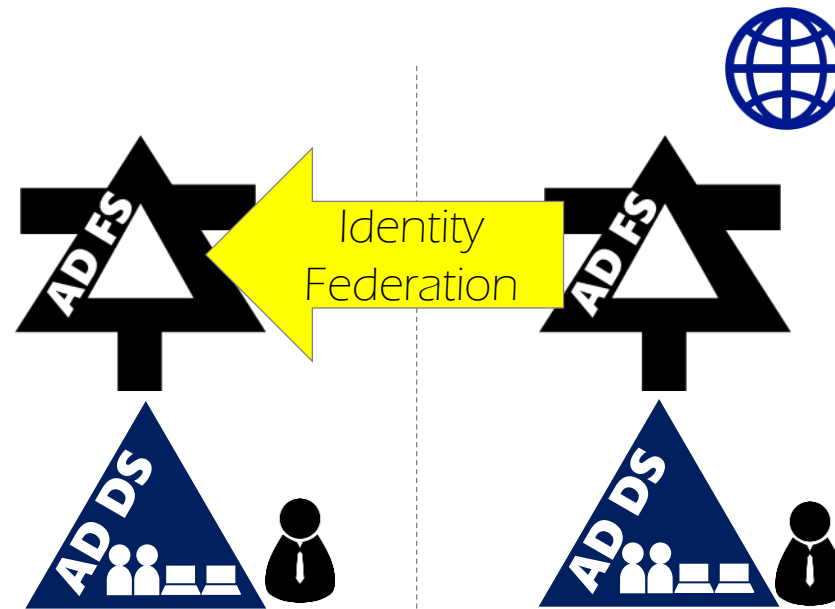


B2B 組織/企業間連携パターン

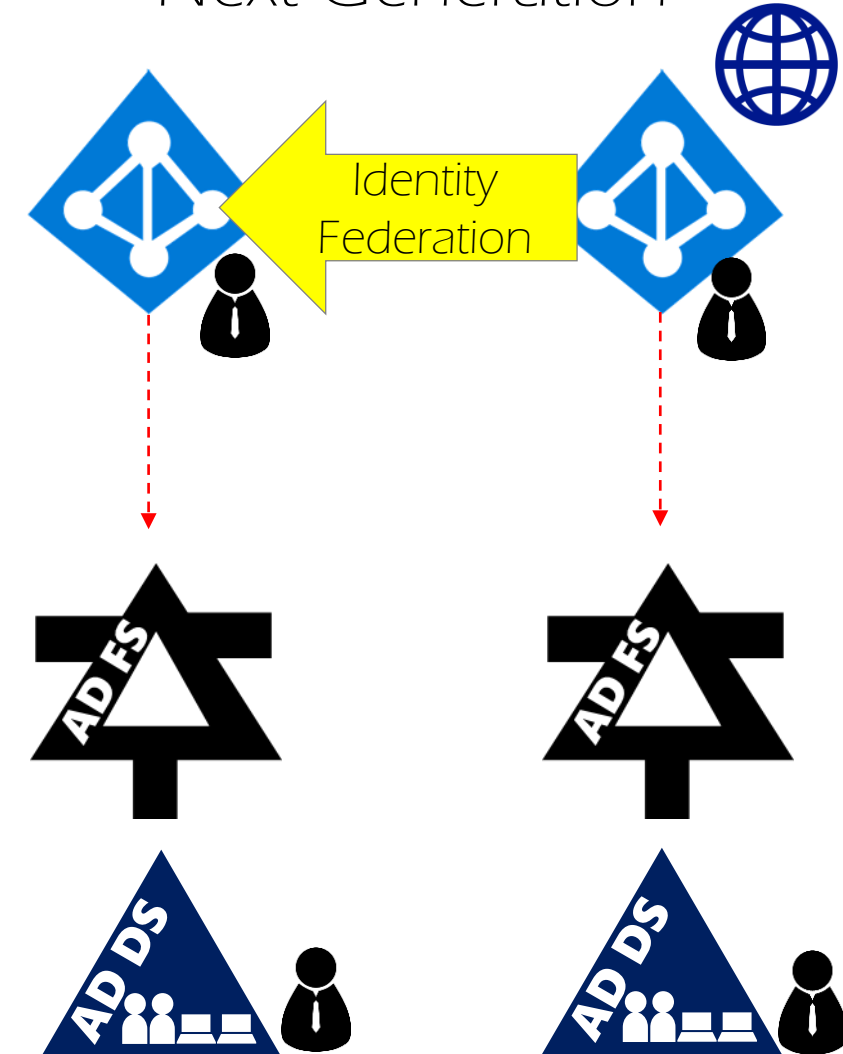
Traditional



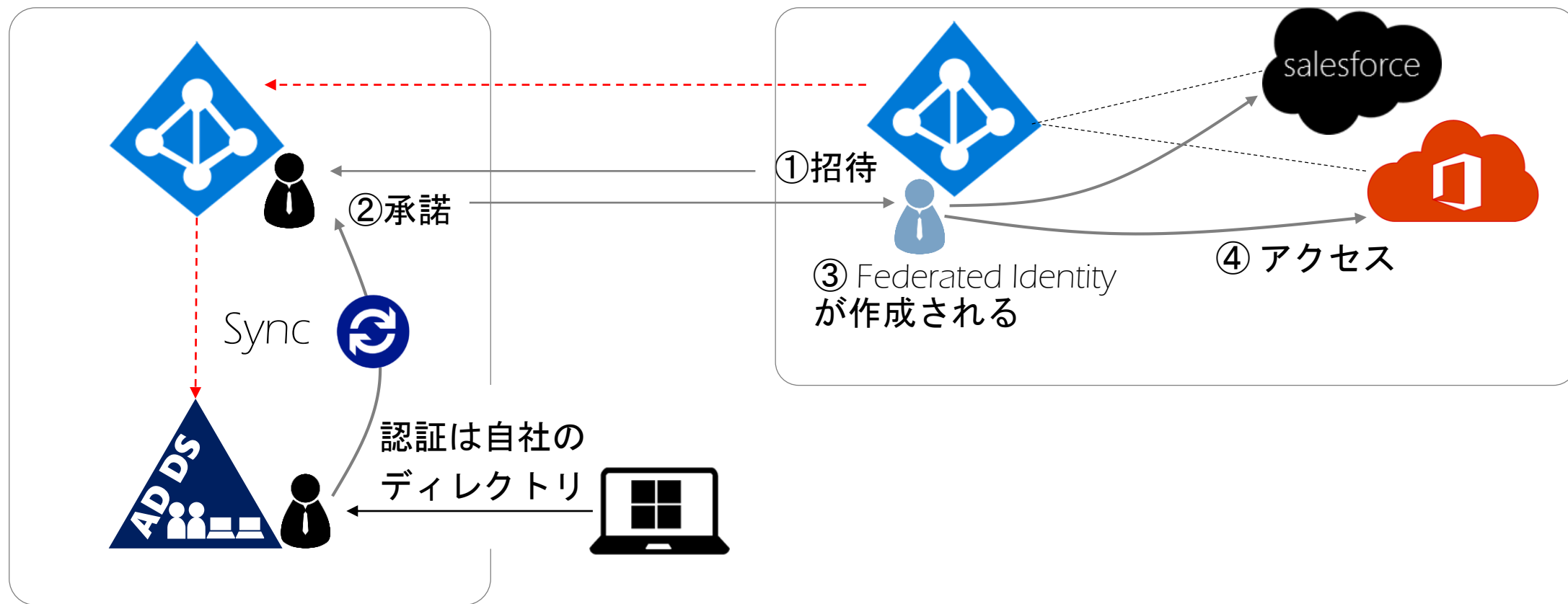
Modern



Next Generation



- 異なるAzure AD テナント間で Identity Federation
- Azure AD のすべてのエディションで利用可能

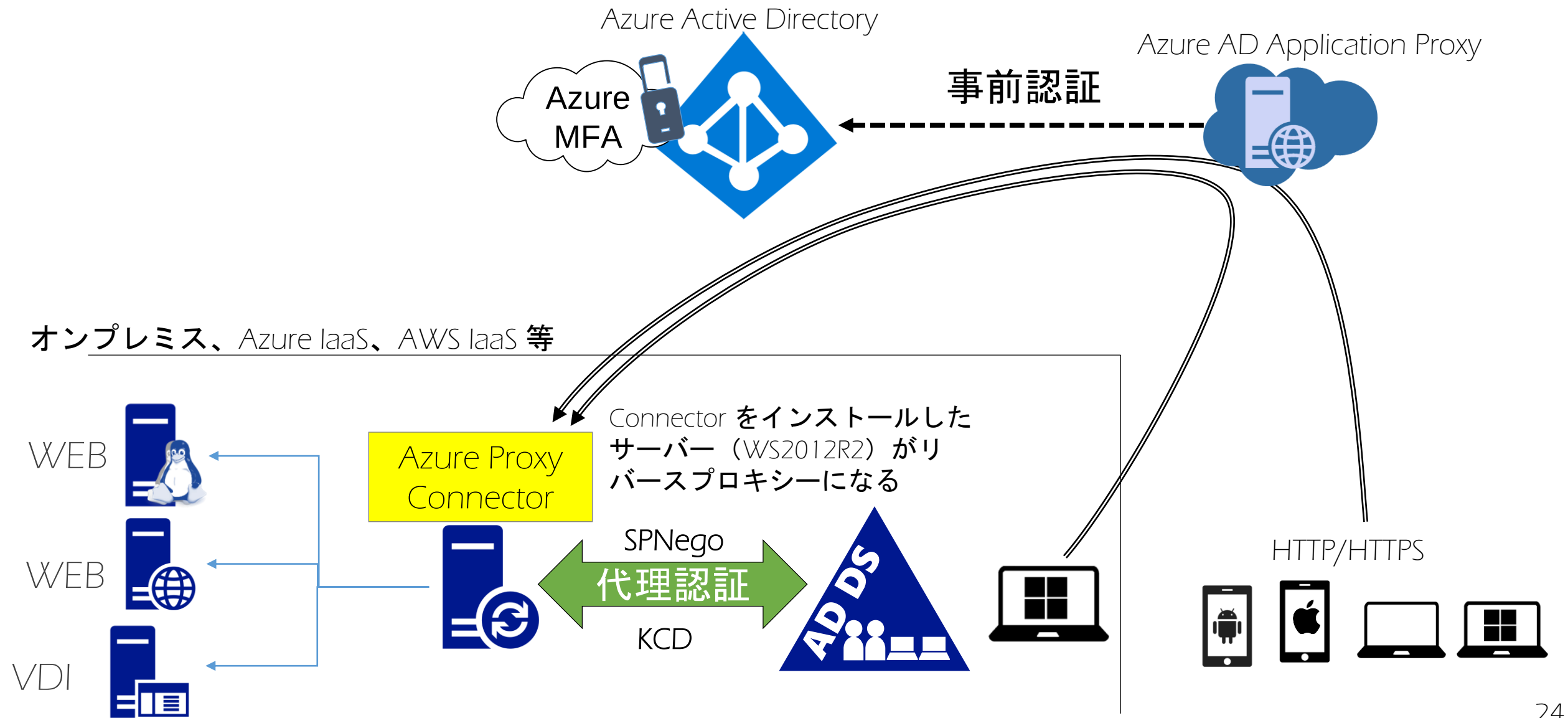


Azure AD B2C preview



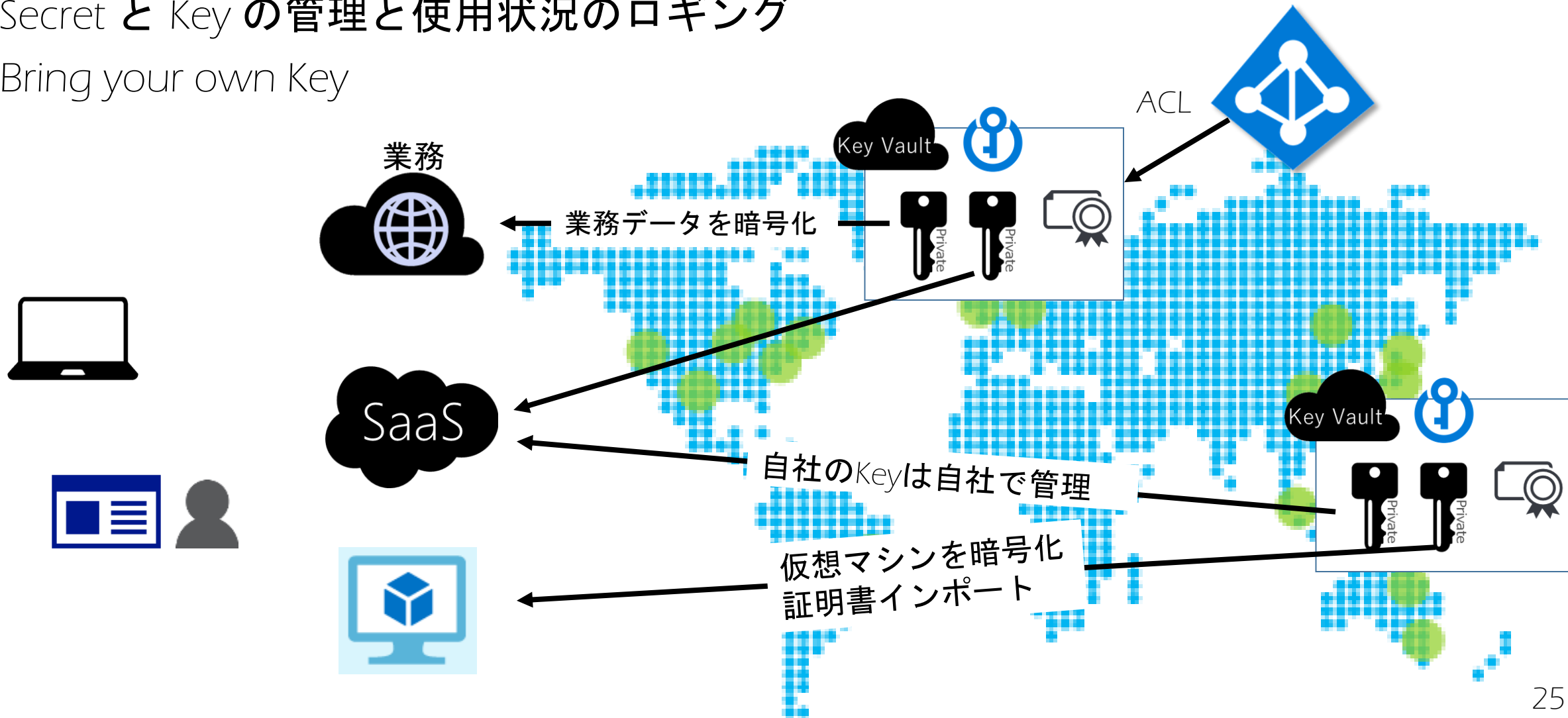
※現時点ではソーシャル IdP から取得するクレームを拡張することができないため、B2Cディレクトリに属性を用意しておく必要がある

Azure AD アプリケーションプロキシ ※Azure AD Basic/Premium 必須



Azure Key Vault

- HSM as a Service（キーを管理するリージョンを指定できる）
- Secret と Key の管理と使用状況のロギング
- Bring your own Key



まとめ

- まずは Hybrid Active Directory から
- クラウドサービスは Azure AD に接続
- Microsoft Intune と Azure RMS を加えて多層防御
- 5 年後は Azure AD を中心とした IDaaS の世界へ

