CloudShift

Stylez

株式会社スタイルズ

2023年9月26日

ADとAzureADの統合によるIDの一元管理

aws partner network

aws PARTNER Select Tier Services

RANCHER PARTNER NETWORK

ZABBIX CERTIFIED PARTNER

Nextcloud Platinum Partner

vmware PARTNER PROFESSIONAL SOLUTION PROVIDER

自己紹介

- **磯部　雄貴（yuki isobe）**
- **株式会社スタイルズ**
  - ゼロトラスト関連チームでIDaaS等を担当

本日、お話しする内容

対象

- これからAzureADを導入したい方
- ADとAzureADのID管理を統合したい方

ゴール

- AzureADの主な機能とID管理に関して理解する
- ADとAzureAD間のIDを同期する方法を理解する

AzureADについて

AzureADは2023年中に名称が「Microsoft Entra ID 」に変更されます。

本セミナーではAzureADと表記していますが、今後は「Microsoft Entra ID 」となりますので、名称変更後は読み替えてください。

セミナー概要

- **IDaaS、AzureADとは**
  ⇒AzureADを使うとどのようなことができるか説明
- **ADとAzureADをID統合する**
  ⇒ADとAzureADを使う上での問題、解決するためのID統合について説明
- **デバイス情報の同期**
  ⇒ユーザ情報だけでなく、デバイス情報の同期について説明
- **統合する際の注意点**
  ⇒ID統合をする上で注意すべきことを説明

IDaaS、AzureADとは？

はじめに

クラウドサービスやテレワークの普及、ランサムウェア被害の拡大などの背景から、
「ゼロトラストセキュリティ」への移行が求められています。

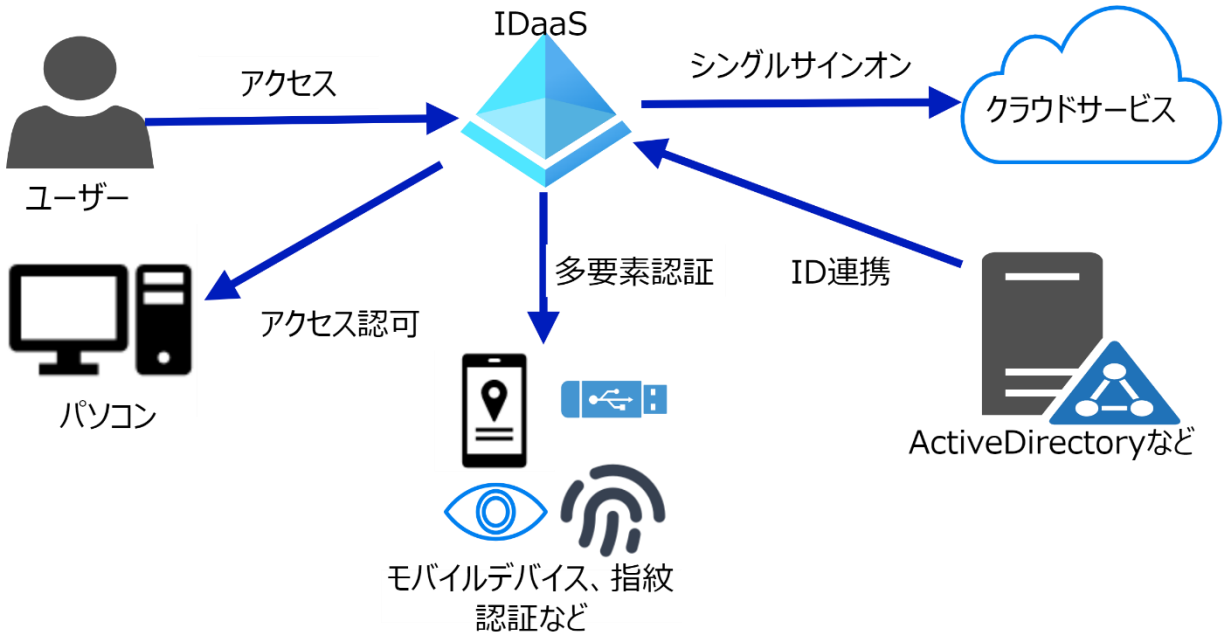
ゼロトラスト（すべてを信頼しない）で、重要な要素は『本人』であるかどうか
『本人』を特定するクラウド認証基盤が

IDaaS（Identity as a Service）

AzureADをIDaaSとして使う

Microsoft365（旧Office365など）を契約しているとAzureADが付加されており、IDaaSとして活用することが可能です。

AzureAD（IDaaS）の機能により、クラウドサービスに対する不正アクセスの防止やユーザの利便性向上が図れます。

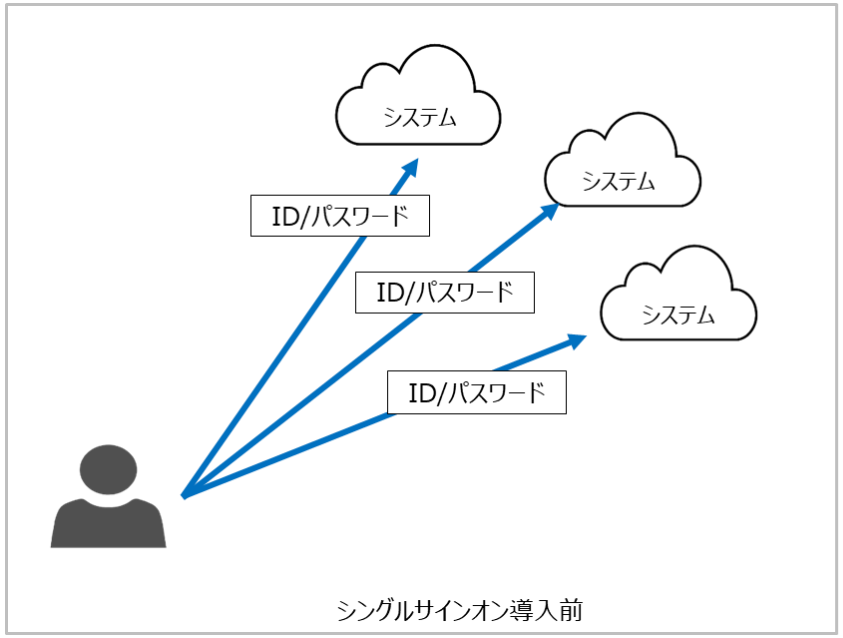


AzureAD（シングルサインオン）

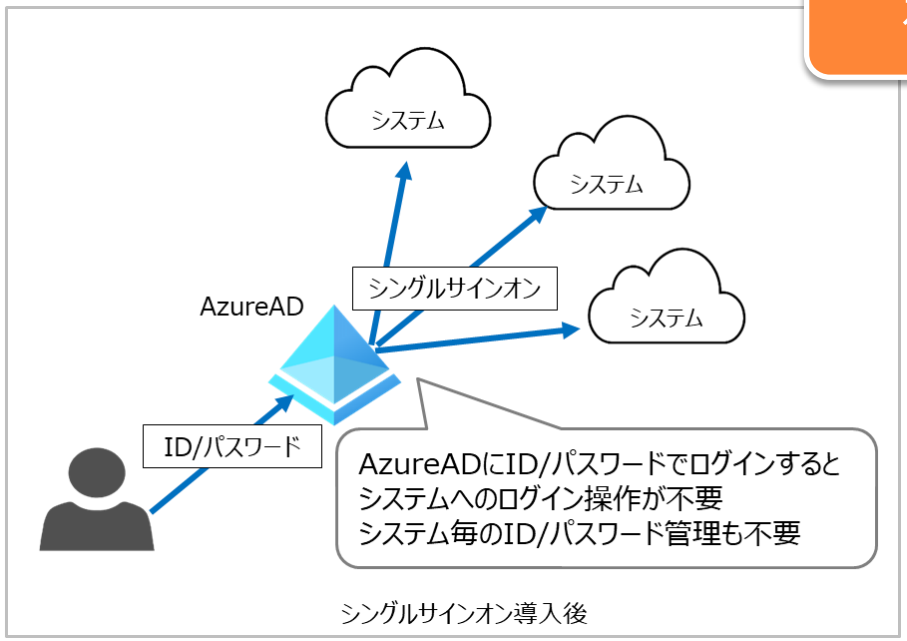
シングルサインオン機能により、複数のシステムをAzureADがまとめて認証することができる。

- ✓ AzureADへログインすればシステム毎のログイン操作は不要
- ✓ ID、パスワードは１つだけ管理。各システムのパスワード管理は不要
- ✓ IDの管理対象が減ることによりパスワードの使いまわしやアカウントロックも減少

利便性向上



シングルサインオン導入前



シングルサインオン導入後

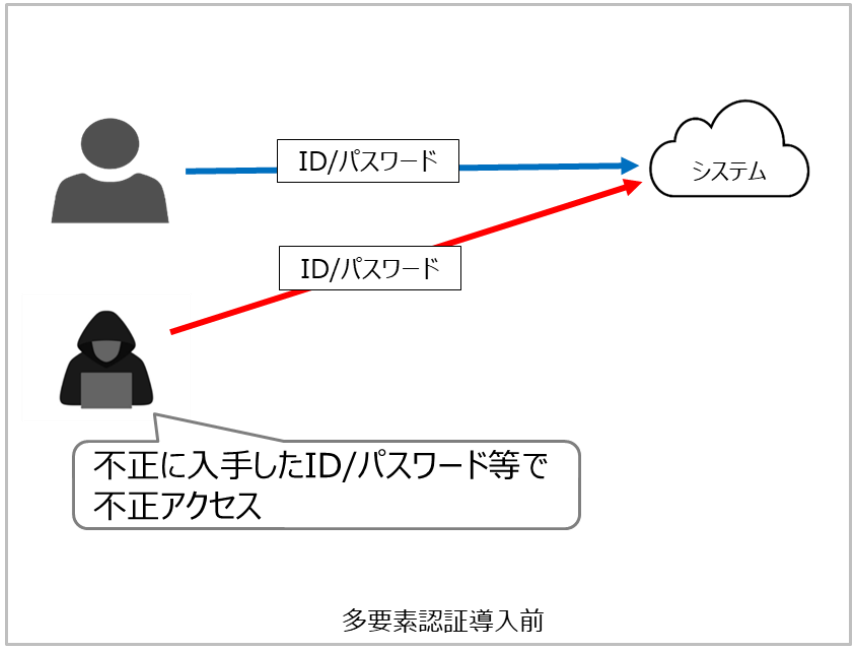
AzureAD（多要素認証）

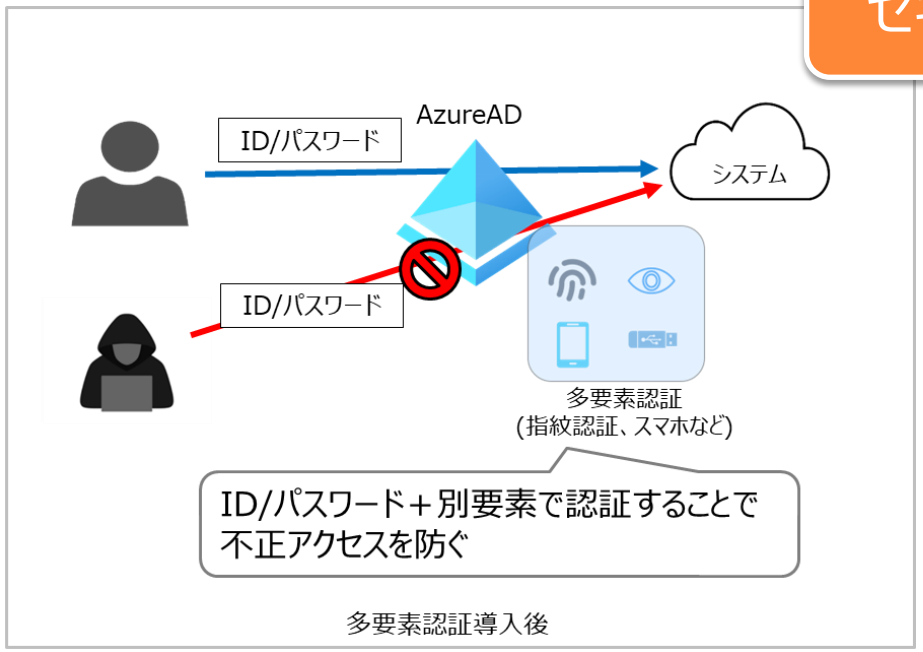
多要素認証は、ID/パスワードが流出しても別の要素で不正アクセスを防止

IPA 2023年 組織向け10大脅威の対策として、『多要素認証』が以下脅威で有効 (※1)
１位：ランサムウェアによる被害
５位：テレワーク等のニューノーマルな働き方を狙った攻撃
７位：ビジネスメール詐欺による金銭被害

※1：情報セキュリティ10大脅威 2023：IPA 独立行政法人 情報処理推進機構

セキュリティ向上



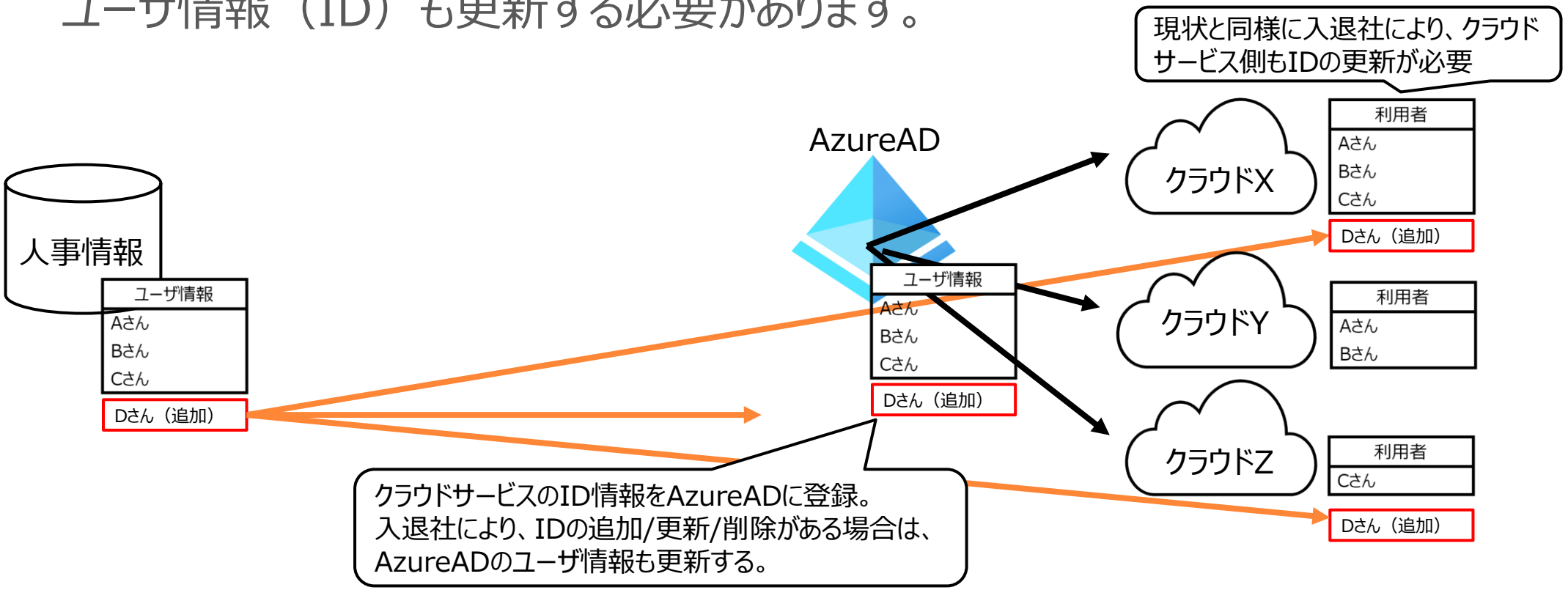


ADとAzureADをID統合する

AzureADの機能を利用する前提作業

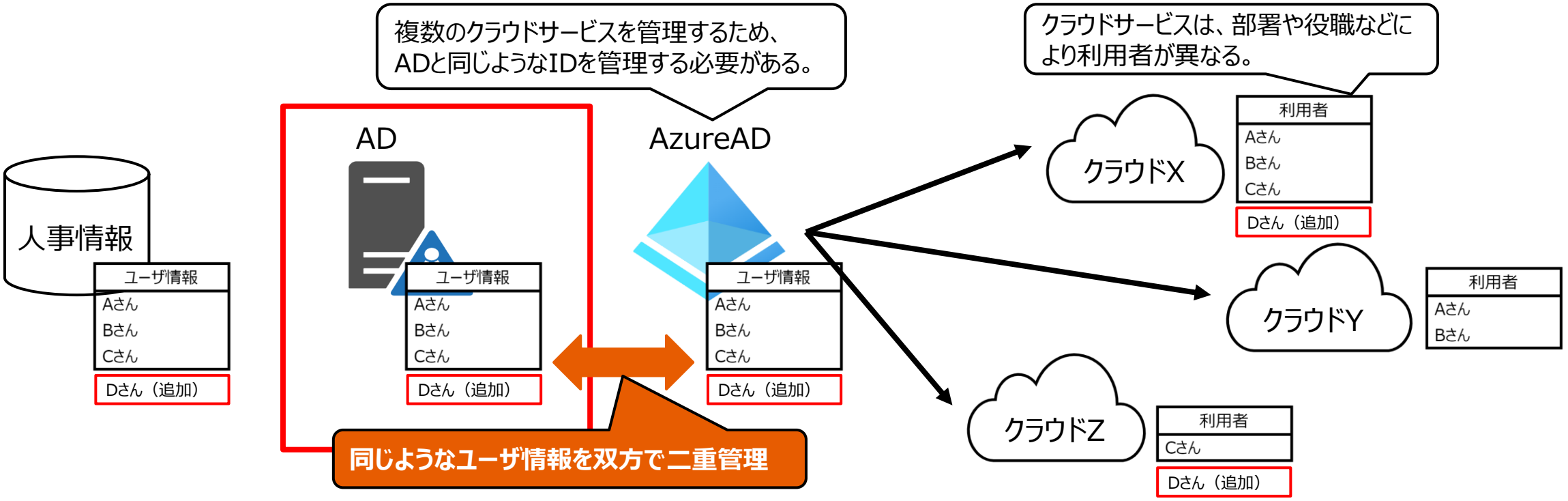
シングルサインオンや多要素認証を導入するには、クラウドサービス（SaaS）のIDをAzureADで管理、運用する必要がある。

例えば、入退社等によりユーザの追加/更新/削除が必要な場合、AzureADのユーザ情報（ID）も更新する必要があります。



ユーザ情報の二重管理について

社内でAD（ActiveDirectory）を運用している場合、
パソコンにログインするドメインユーザでも同じようにユーザ情報を更新していないでしょうか？

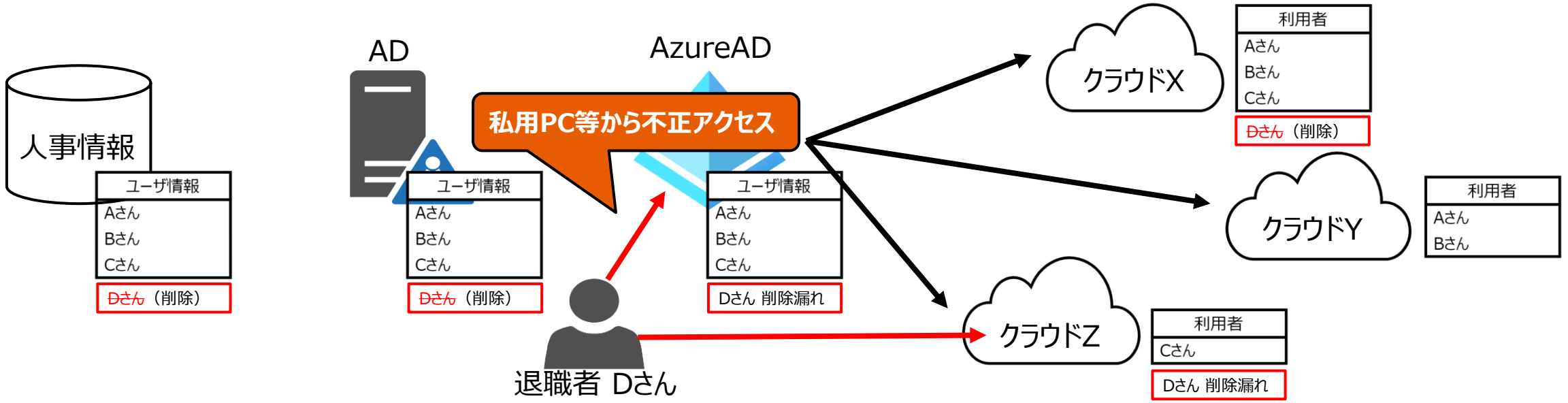


ADとAzureADの両方でユーザー情報を二重で管理、運用することになる

ユーザー情報の二重管理によるリスク

ADとAzureADの両方でユーザー情報を二重で管理、運用することにより、

- ✓ ユーザ情報の更新等にかかる運用作業が二重でかかる。
- ✓ 入退社等で更新ミスや更新漏れが発生する。

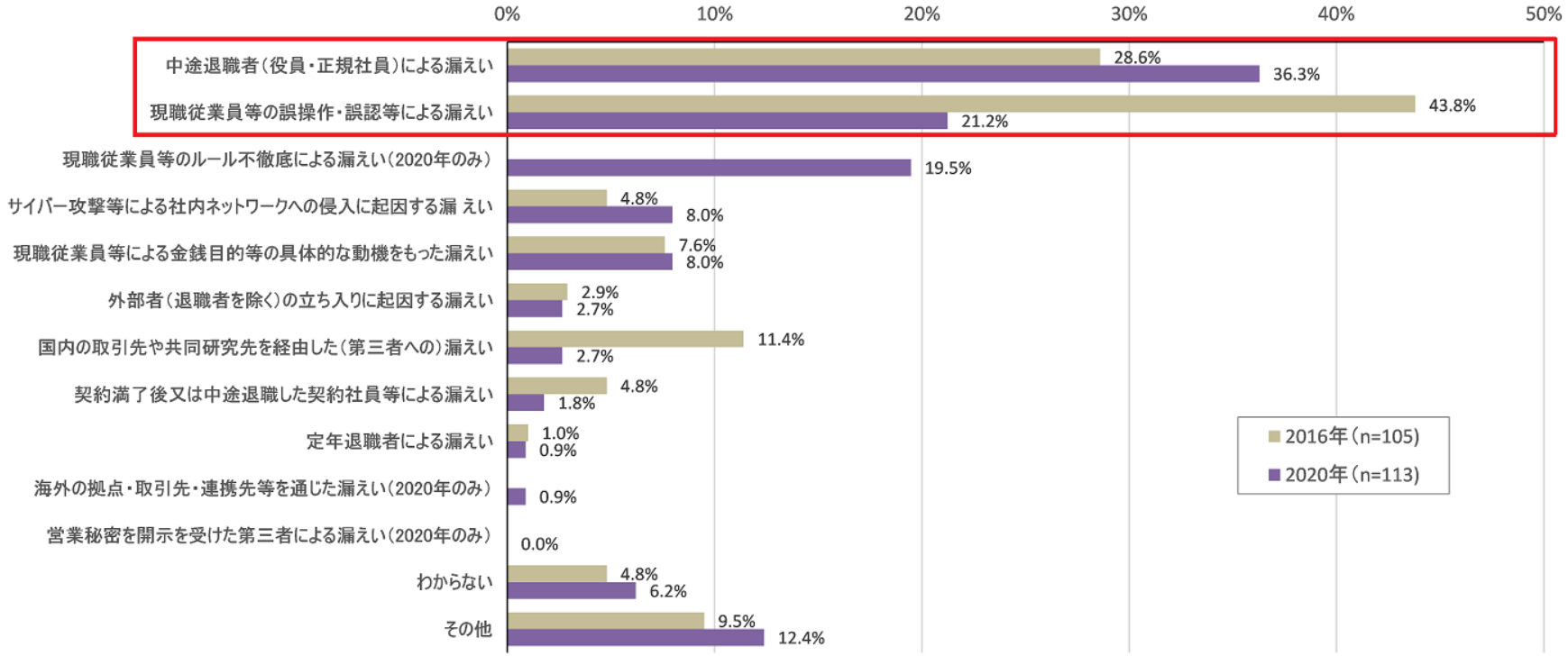


クラウドサービスでアクセス制限等をかけていない場合、退職者の
ID更新漏れ等があると、社外から不正アクセスや情報漏洩の恐れがある

中途退職者による情報漏洩について

IPAによる2020年企業における情報漏洩の実態調査では、誤操作やサイバー攻撃より中途退職者による情報漏洩が一番多い結果となった。（36.3%）

調査結果は、退職後やクラウドサービス等の不正アクセスに限らないため、ID管理を適切に運用してもすべて防げるわけではないが、容易にアクセスできない環境を作る必要がある。

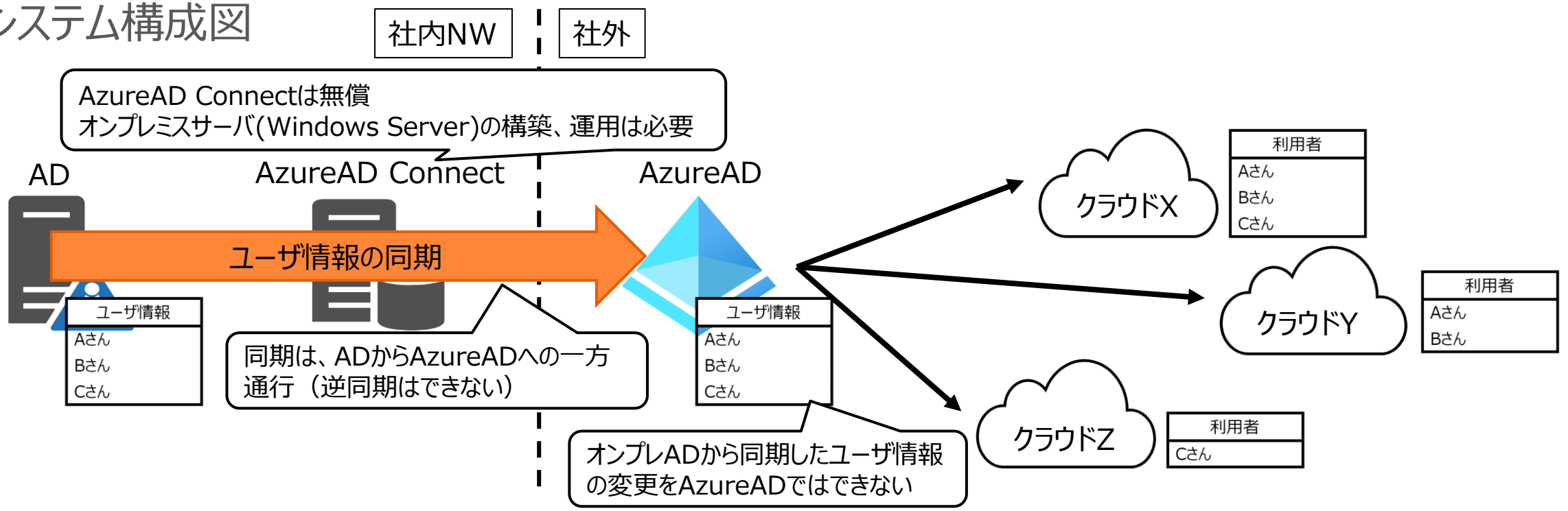


「企業における営業秘密管理に関する実態調査2020」報告書について：IPA 独立行政法人 情報処理推進機構

ADとAzureADをID統合する

IDの更新漏れをなくす対策の一つとして、ADとAzureADのIDを統合
AzureAD Connectにより、ADで更新したID情報をAzureADに同期できる

■システム構成図



AzureAD Connectにより、ADのユーザ情報を
AzureADへ同期して作業負荷や作業ミス、作業漏れを低減

AzureAD Connect導入ケース

- ケース１

ADがあり、これからAzureADおよびMicrosoft365等を導入予定

⇒AzureADおよびMicrosoft365等導入時に、AzureAD Connectも併せて導入推奨

後日、同期が必要になった場合、IDのマッチング作業が必要になるため。

- ケース２

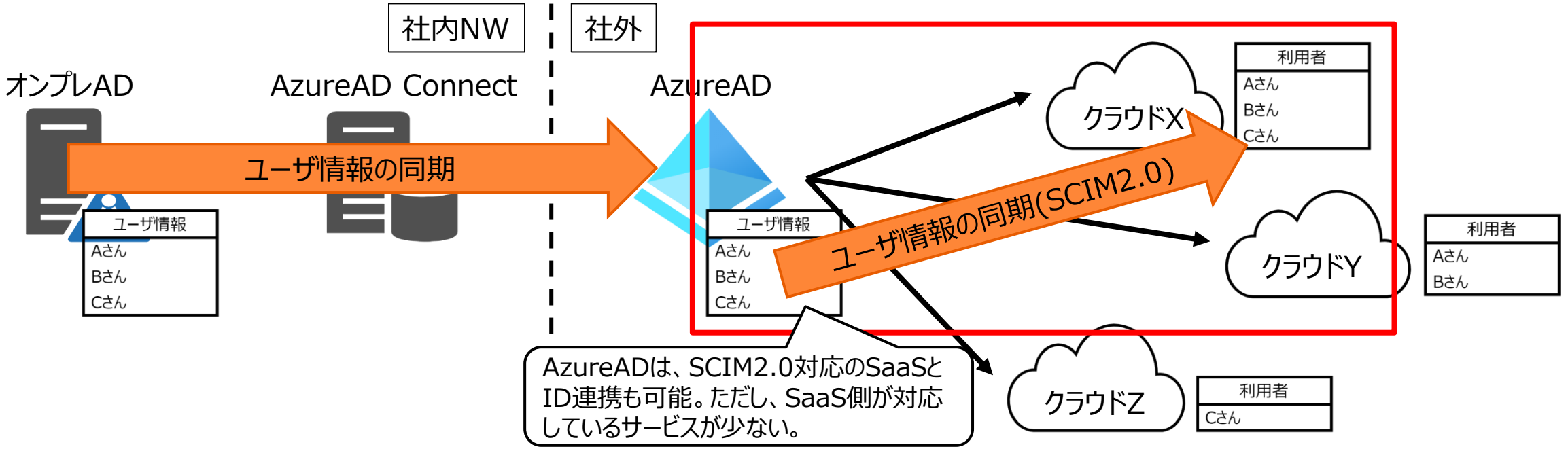
既にADとAzureADでIDの二重管理をしている

⇒後からでもADとAzureADのIDはAzureAD Connectで統合が可能。

ただし、ADとAzureADをUPN等で値を一致させるなどのマッチングが必要。

AzureADとクラウドサービス間のID連携

SaaS等のクラウドサービス側のユーザ情報をAzureADと同期することも可能。ただし、
ユーザ情報の同期には、SCIM2.0に対応が必要であり、国内は対応済みサービスが少ない。



弊社『IDプロビジョニングツール』では、SCIM2.0未対応のクラウドサービスに対して
CSVやAPI等のユーザ更新機能を使って、AzureADのユーザ情報を連携可能

ADとAzureADの主な違い

ADを廃止して、ID管理をAzureADに集約できないのか？

AzureADはADの機能を包含しているわけではなく、役割も違います。

⇒ADを廃止してAzureADへ移行したい場合、ADで認証しているアプリやデバイス制御などを洗い出し、ADまわりのシステムや機能の見直しが必要

■ADとAzureADの主な違い

分類		ActiveDirectory	AzureAD
ID	主な管理対象	社内ネットワークで使うID管理	クラウドサービス等で使うID管理
デバイス	主な管理対象	Windowsパソコン	Windowsパソコン、スマートフォン
	管理方法	グループポリシー	管理方法なし (Microsoft Intuneを使う必要あり)
アプリ	AD機能	認証、アクセス制御、DNS、DHCP、NTP 等	認証、アクセス制御
	主な連携先	社内システム、ファイルサーバ 等	SaaS、Webアプリ 等
	認証方法	LDAP、Windows統合認証 (NTLM,Kerberos)	SAML、OpenID Connect 等

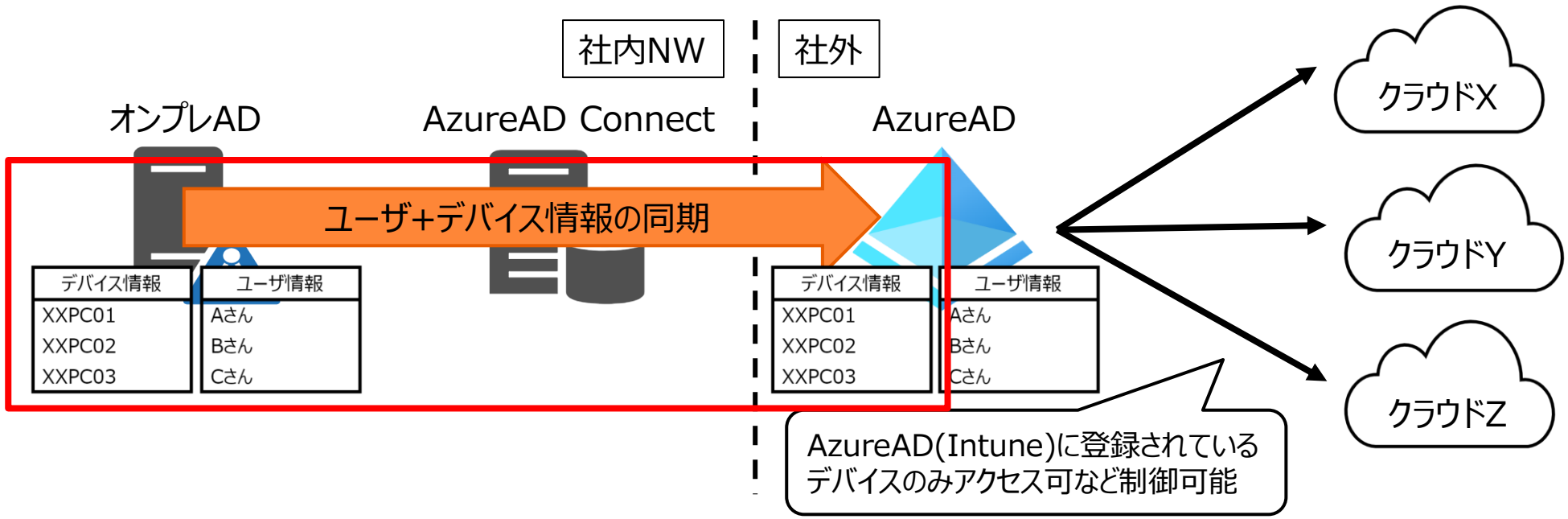
デバイス情報の同期

デバイス情報の同期

AzureAD Connectでは、ユーザ情報(ID)以外にデバイス情報も同期することが可能

デバイス情報を同期することにより、

- AzureADにデバイスが登録できる（Hybrid AzureAD Join）
- デバイス情報を使ったデバイスアクセス制御も可能（AzureAD P1ライセンス以上）
- Microsoft Intune (デバイス管理) へのデバイス登録が容易になる



デバイスアクセス制御の実現

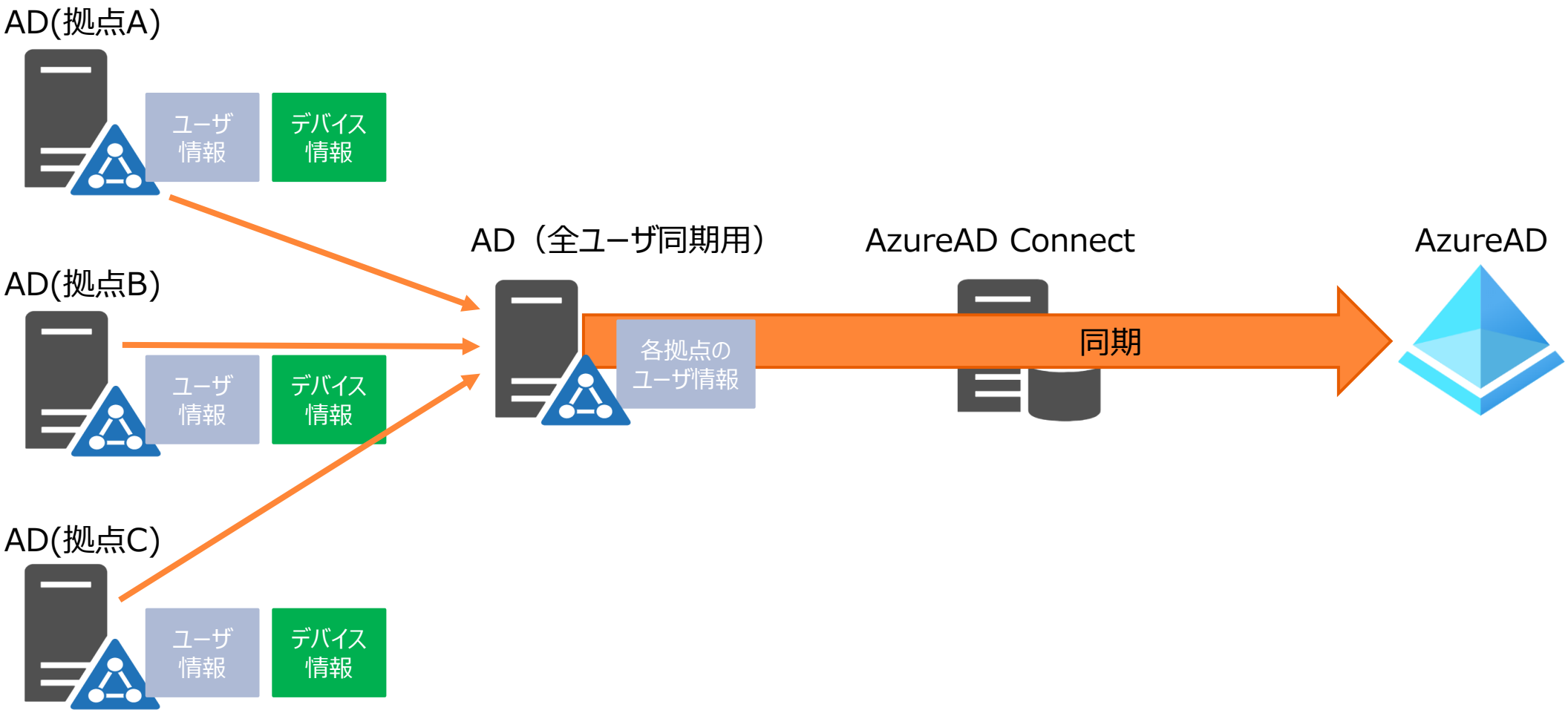
デバイスアクセス制御を実現するには、Microsoft Intuneへのデバイス登録が必要
※Microsoft Intune： Microsoftのデバイス管理ツール

ADがあればAzureAD Connectのデバイス同期でAzureADにデバイスを登録できますが
複数のADを運用している場合、AzureAD Connectで同期するADが
ユーザ情報とデバイス情報をセットで管理している必要がある。

次のケースは、同期するADにユーザ情報とデバイス情報がセットで管理されていないため、
ADの構成を見直す必要がある。

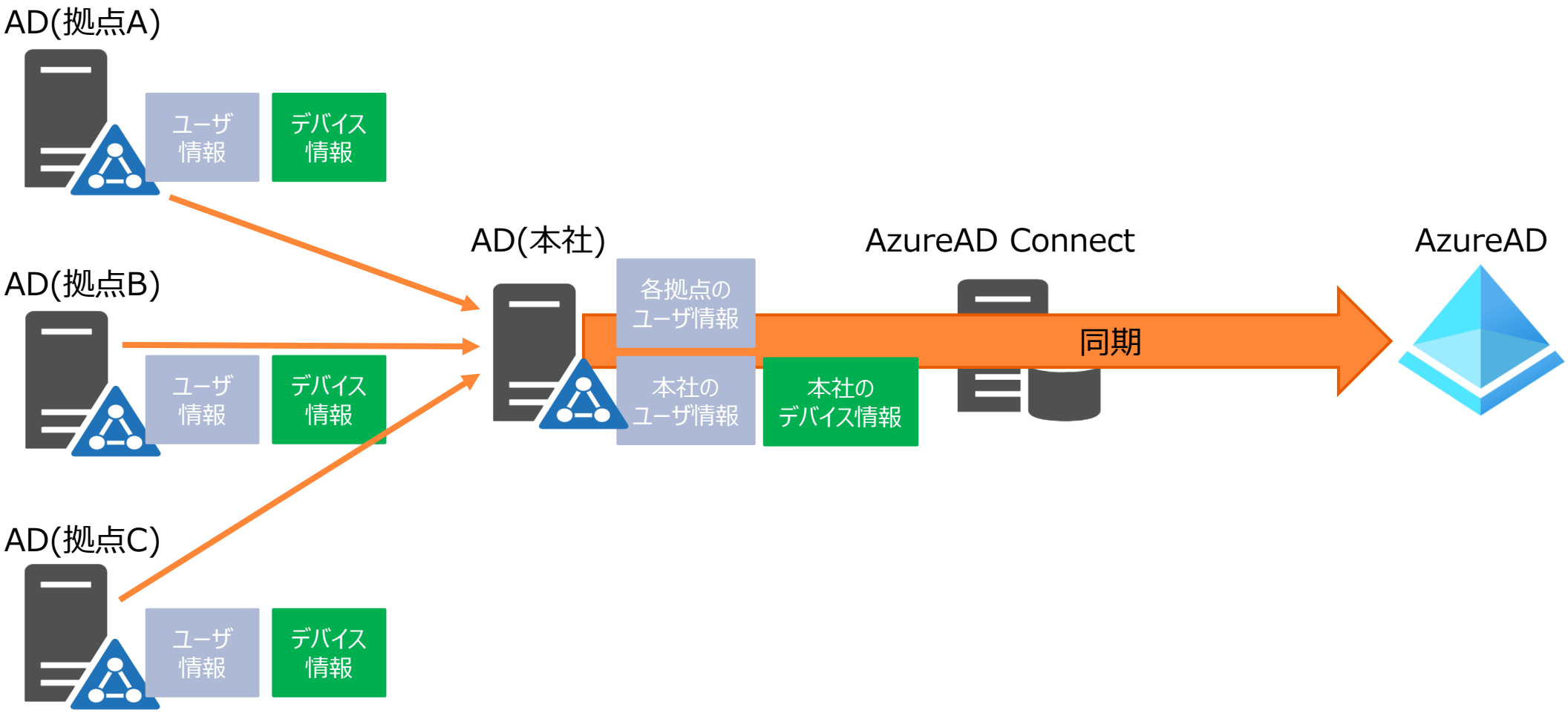
デバイスアクセス制御ができない（ケース１）

１．全ユーザ同期用のADを作成し、デバイス情報は各拠点のADで管理



デバイスアクセス制御ができない（ケース２）

２．本社ADに全ユーザ登録して同期先に設定。拠点のデバイスは各拠点のADで管理



デバイスアクセス制御の実現

デバイスアクセス制御を実現するには、AzureAD(Intune)へのデバイス登録が必要ですが

AzureAD Connectによるデバイス同期以外でも、AzureAD(Intune)にデバイスを登録することができます。

先ほどのケースに該当し、オンプレADの構成等の見直しが困難な場合、個別にAzureAD(Intune)へ登録する方法（AzureAD Registered）もご検討ください。

ただし、ユーザによるAzureAD(Intune)への登録作業が必要であったり、セルフサービスパスワードセット機能（SSPR）が使えない等があります。

統合する際の注意点

ADからAzureADへ同期する場合の注意点

【既にAzureADを（O365等で）運用している場合】

- 既存のAzureADとADを紐づけるための情報が必要

UPNやProxyAddressなどをAzureAD・AD双方でそろえる必要があります。

マッチングが失敗するとAzureAD側に新規ユーザが作成されます。

その場合、AzureAD側ではユーザ情報を修正できないため、一度同期を外してから修正するなど、時間がかかります。

- ドメイン情報の統合

ADとAzureADのドメインを合わせる必要があるため、AzureADでカスタムドメインを作成したり、ADのUPNサフィックスを追加する必要があります。

例：ADのドメインが「xxx.local」の場合

　　AzureADのドメインが「xxx.onmicrosoft.com」の場合

さいごに

本日紹介したAD⇒AzureADへの同期には以下メリットがあります。

・IDaaS初期導入時のユーザ登録作業をする必要がなくなる
・IDaaS導入後のID管理作業負荷軽減
　⇒新規作成、変更、削除作業などの負荷を減らせる
・ID管理作業の一元化による作業ミス、作業漏れのリスク低下

スタイルズはIDaaSサービスの導入を支援いたします！

スタイルズ IDaaSサービス

『IDaaSサービス』と『IDaaS＆ゼロトラストコラム』

■スタイルズのIDaaSサービス内容

- AzureADによるIDaaS実現（シングルサインオンと多要素認証の実現）
- ADとの連携
- SAML非対応のSaaSや社内Webシステムも対応
- IDプロビジョニング（IDや権限の連携）も対応
- IDaaS初期導入支援サービス（ポイントでの技術支援サービス）

実績豊富なエンジニア集団の技術と開発ツールで「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

https://www.stylez.co.jp

東京都千代田区神田小川町1-2　風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進