Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

A-2

アクセス制御では防げない！？ パスワード漏えいの仕組みと対策講座

日本マイクロソフト株式会社
クラウド＆ソリューション事業本部 モダンワークプレイス統括本部
成田 翔 CISSP, CEH

Microsoft

このセッションの後

- 認証に対する実際の攻撃手法を**知り**、
  認証セキュリティ強化の**きっかけに**していただく

なぜパスワード漏えいが問題か

- **攻撃に使用される**
  - 企業ネットワーク内の横展開
  - リモートからの VPN 接続
  - 脅迫メール
  - ブラックマーケットへの流出 (＝アカウント リストとして再利用)

- **パスワードは無効に出来ない**
  - AD / Azure AD はパスワードありき
  - パスワードレスや MFA はパスワード自体の窃取リスクを軽減しない

INCIDENT DETAILS ///

This APT group targets organizations across multiple industries, including government agencies, financial institutions, and technology companies.

Conditional access could have prevented unauthorized access.

Logging and auditing non-owner mailbox access would have detected malicious behavior.

Logging, at the time of this incident, was not enabled by default.

MONITORING & INTERCEPTION

PARTNER & VENDOR

COMMAND & CONTROL

ACTIONS ON OBJECTIVE

EXFILTRATE DATA

Multi-factor authentication (MFA) could have prevented this attack.

ERROR OR NEGLECT

CONTROLS ENVASION

DELIVERY

PASSWORD SPRAY

EXPLOITATION

DART engaged

DAYS // 01–11

APT group compromises privileged user's non-MFA-enabled Office 365 account.

DAYS // 016–163

Threat actors perform mailbox searches across Office 365 environment.

Attacker uses stolen credentials to VPN into corporate network, searches for intellectual property.

Office 365

EXFILTRATE DATA

DAYS // 137–218

Threat actor changes search and exfiltration technique, leveraging Compliance Search to allow for precision searches.

Introducing Compliance Search in Office 365 - Microsoft 365 Blog—Compliance Search is a new addition to the Office 365 Compliance Center, designed for times when the full-fledged search case management of eDiscovery search isn't required.

DAYS // 137–143

Threat actors create rules in company's IT environment to automate data exfiltration to a third-party cloud storage solution.

USE COMPROMISED CREDIENTIAL

MONITORING & INTERCEPTION

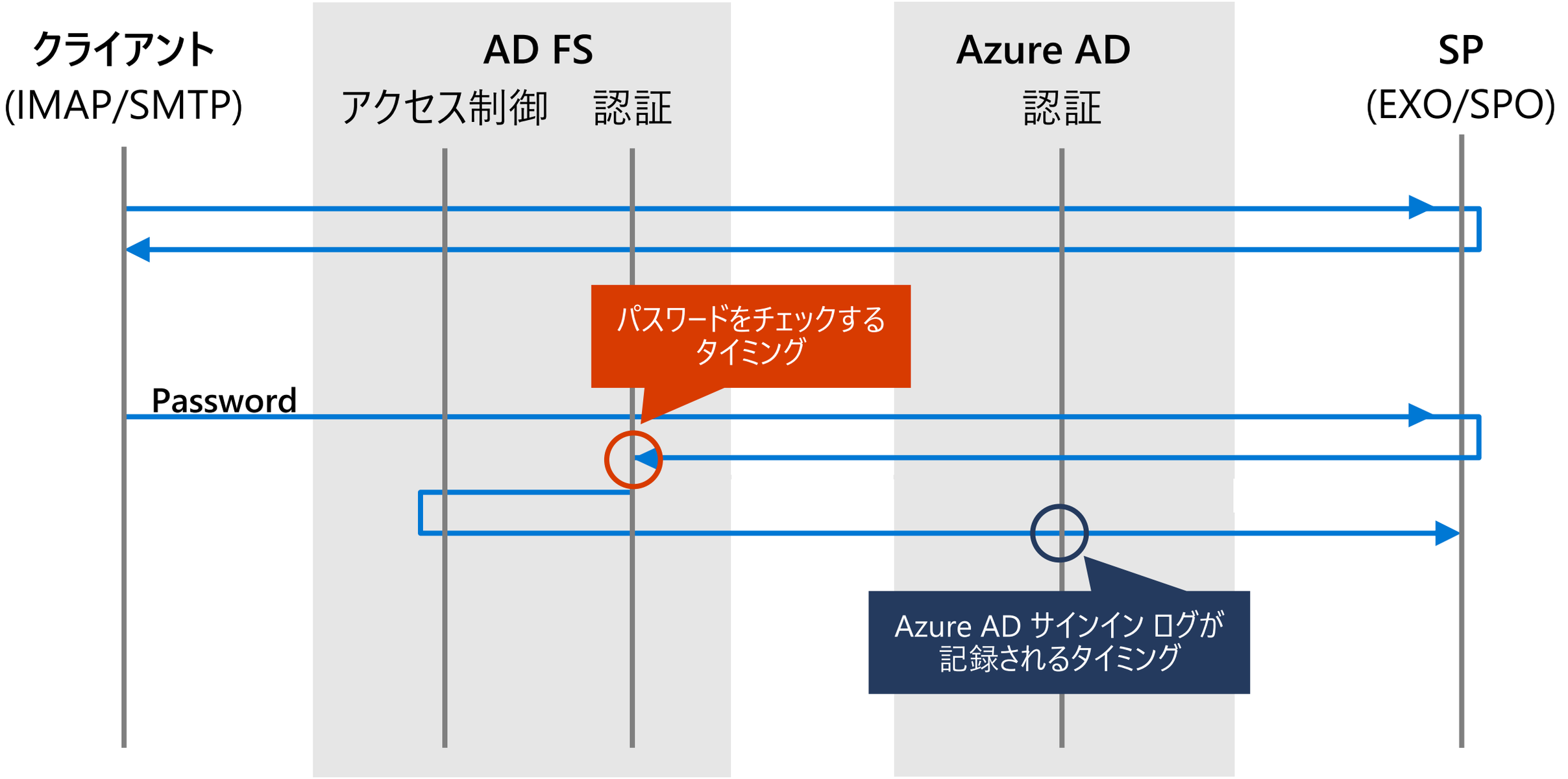
Company did not have VPN monitoring enabled.

Multi-factor authentication could have prevented the threat actors from accessing the environment through the VPN.

代表的なパスワード漏えい経路

- NTDS.DIT
- lsass.exe
- Breach Replay
- フィッシング
- パスワード スプレー

パスワードに対する攻撃の場所 (レガシー認証)



Date	Status	Location	Client app	Risk state	Risk level (aggregate)	Risk level (real-time)
2/3/2020, 12:37:53 AM	Failure	noumea, sud, nc	Unknown	At risk	High	Medium
2/2/2020, 5:04:16 PM	Failure	nanjing, jiangsu, cn	Unknown	At risk	High	Low
2/2/2020, 10:15:59 AM	Failure	bangkok, krung thep, th	Unknown	At risk	High	Medium
2/2/2020, 2:37:15 AM	Failure	tarzana, california, us	Unknown	At risk	High	Medium
2/1/2020, 7:31:08 PM	Failure	Kunming, Yunnan, CN	Unknown	At risk	High	Medium
1/24/2020, 9:08:35 AM	Failure	Nanjing, Jiangsu, CN	Unknown	At risk	High	Medium
1/22/2020, 6:24:07 PM	Failure	Chongqing, Chongqing, CN	Unknown	At risk	High	Medium
1/22/2020, 8:59:58 AM	Success	Al Qahirah, Al Qahirah, EG	Unknown	At risk	High	Medium
1/22/2020, 8:06:56 AM	Failure	Xicheng Qu, Beijing Shi, CN	Unknown	At risk	High	Medium
1/22/2020, 5:28:44 AM	Failure	Nanning, Guangxi, CN	Unknown	At risk	High	Medium
1/20/2020, 5:58:06 PM	Failure	Buenos Aires, Ciudad De Buenos Aires, AR	Unknown	At risk	High	High
1/20/2020, 1:05:06 PM	Failure	Al Qahirah, Al Qahirah, EG	Unknown	At risk	High	Medium
1/19/2020, 12:52:41 PM	Failure	Hefei, Anhui, CN	Unknown	At risk	High	Medium
1/19/2020, 12:40:08 PM	Failure	Nanjing, Jiangsu, CN	Unknown	At risk	High	Medium
1/19/2020, 8:17:41 AM	Failure	Changchun, Jilin, CN	Unknown	At risk	High	Medium
1/19/2020, 7:36:33 AM	Failure	Americana (Guadalajara), Jalisco, MX	Unknown	At risk	High	High
1/19/2020, 7:13:58 AM	Failure	Buenos Aires, Ciudad De Buenos Aires, AR	Unknown	At risk	High	High

Failure

Location	noumea, sud, nc
Date	2/3/2020, 12:37:53 AM
Status	Failure
Sign-in error code	50053
Failure reason	Account is locked because user tried to sign in too many times with an incorrect user ID or password.
Client app	IMAP4

Proxy/VPN Detection:	**true**
VPN:	**false**
TOR:	**false**
Fraud Score	**100**
	75+ is suspicious | 85+ is high risk
Recent Abuse:	**true**
Bot Activity:	**true**

Success

Location	Al Qahirah, Al Qahirah, EG
Date	1/22/2020, 8:59:58 AM
Status	Success
Client app	IMAP4

Proxy/VPN Detection:	**true**
VPN:	**false**
TOR:	**false**
Fraud Score	**89**
	75+ is suspicious | 85+ is high risk
Recent Abuse:	**true**
Bot Activity:	**true**

Identity Protection によるリスク検知

DETECTION TYPE	DETECTION RISK STATE	TIME DETECTED	DETECTION TIMING
Malicious IP address	At risk	1/23/2020, 3:12 AM	Offline

Risk level	High	Sign-in time	1/22/2020, 8:59 AM	Token issuer type	Azure AD
Risk detail	-	IP address	[redacted]		
Source	Identity Protection	Sign-in location	Al Qahirah, Al Qahirah, EG		
Detection last updated	1/23/2020, 3:38 AM	Sign-in client	CBAInPROD		

Unfamiliar sign-in properties	At risk	1/22/2020, 8:59 AM	Real-time

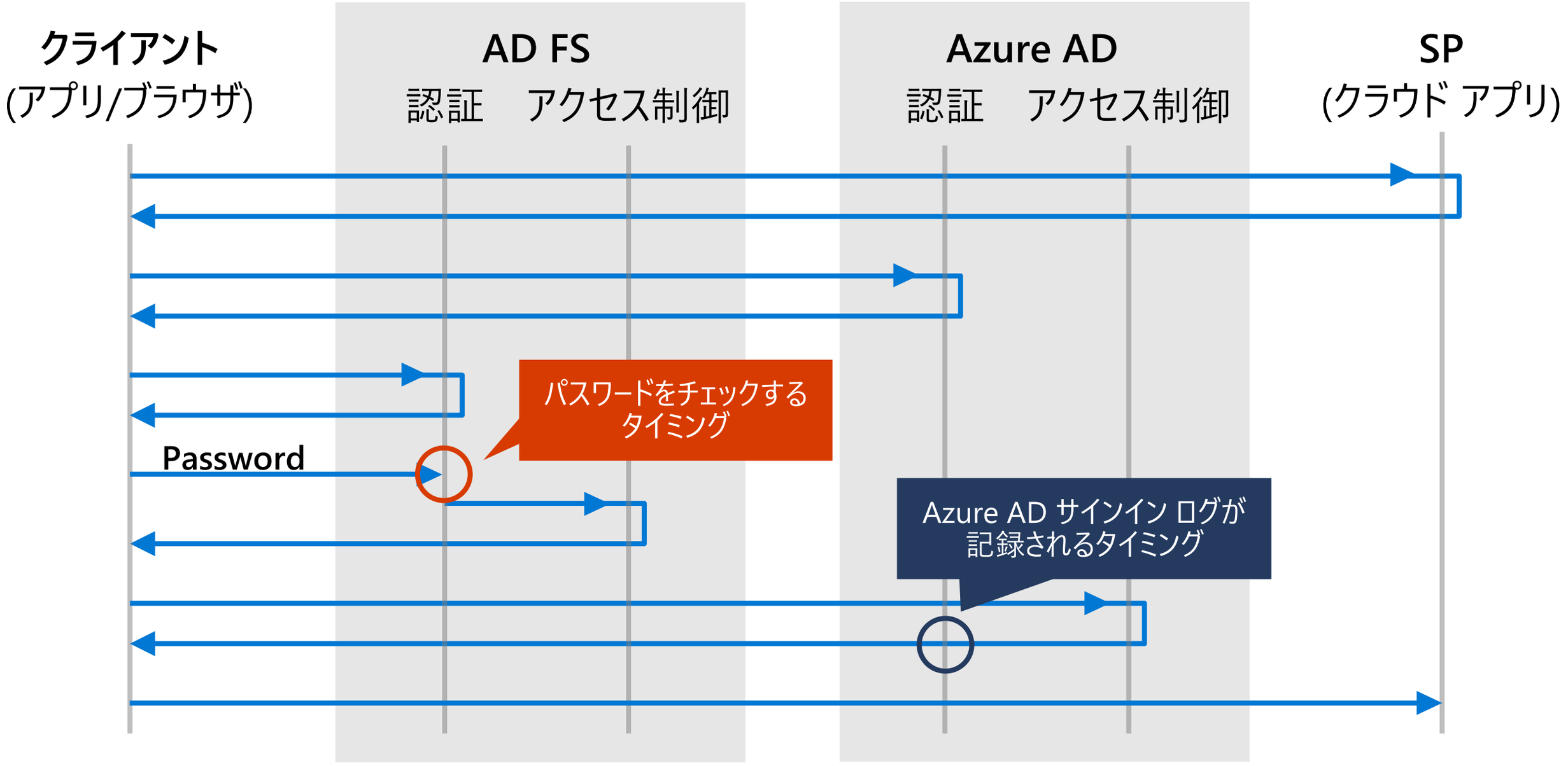
Risk level	Medium	Sign-in time	1/22/2020, 8:59 AM	Token issuer type	Azure AD
Risk detail	-	IP address	[redacted]		
Source	Identity Protection	Sign-in location	Al Qahirah, Al Qahirah, EG		
Detection last updated	1/23/2020, 3:38 AM	Sign-in client	CBAInPROD		

リスクが検知されたサインインの傾向

Date	Status	Location	Client app	Operating system	Device browser
1/22/2020, 8:18:52 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/22/2020, 8:15:57 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/22/2020, 8:14:57 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/22/2020, 8:14:54 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/22/2020, 8:14:54 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/22/2020, 8:59:58 AM	Success	Al Qahirah, Al Qahirah, EG	Unknown		
1/21/2020, 6:45:03 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/21/2020, 6:44:33 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/21/2020, 6:44:32 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/21/2020, 5:41:42 PM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/21/2020, 9:22:39 AM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/21/2020, 9:22:09 AM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		
1/21/2020, 9:21:49 AM	Success	Chiyoda-Ku, Tokyo, JP	Other clients		

←IMAP4

パスワードに対する攻撃の場所 (モダン認証)



Identity Protection によるリスク検知

DETECTION TYPE	DETECTION RISK STATE	TIME DETECTED	DETECTION TIMING
Atypical travel	At risk	1/4/2020, 9:39 PM	Offline

Risk level	Medium	1st sign-in time	1/4/2020, 9:19 PM	2nd sign-in time	1/4/2020, 9:38 PM
Risk detail	-	1st sign-in IP	[redacted].65	2nd sign-in IP	[redacted].51
Source	Identity Protection	1st sign-in location	Isogo-Ku, Kanagawa, JP	2nd sign-in location	Berg (Linkopings), Ostergotlands Lan, SE
Detection last updated	1/4/2020, 9:39 PM	1st sign-in client		2nd sign-in client	Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Token issuer type	Azure AD		
Travel duration	19:8		

DETECTION TYPE	DETECTION RISK STATE	TIME DETECTED	DETECTION TIMING
Unfamiliar sign-in properties	At risk	1/4/2020, 9:38 PM	Real-time

Risk level	Medium	Sign-in time	1/4/2020, 9:38 PM
Risk detail	-	IP address	[redacted].51
Source	Identity Protection	Sign-in location	Linkoping, Ostergotlands Lan, SE
Detection last updated	1/4/2020, 9:39 PM	Sign-in client	Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Token issuer type	Azure AD

Date	Status	Location	Client app	Operating system	Device browser
1/4/2020, 9:38:53 PM	Success	Linkoping, Ostergotlands Lan, SE	Browser	Windows 10	Opera 65.0.3467
1/4/2020, 9:38:51 PM	Success	Linkoping, Ostergotlands Lan, SE	Browser	Windows 10	Opera 65.0.3467
1/4/2020, 9:38:47 PM	Success	Linkoping, Ostergotlands Lan, SE	Browser	Windows 10	Opera 65.0.3467
1/4/2020, 9:38:26 PM	Success	Linkoping, Ostergotlands Lan, SE	Browser	Windows 10	Opera 65.0.3467
1/4/2020, 9:38:21 PM	Success	Linkoping, Ostergotlands Lan, SE	Browser	Windows 10	Opera 65.0.3467
1/4/2020, 7:07:40 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:07:16 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:07:07 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:07:06 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:07:05 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:07:04 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:07:04 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:06:56 AM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/4/2020, 7:06:53 AM	Interrupted	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0
1/3/2020, 8:01:48 PM	Success	Chiyoda-Ku, Tokyo, JP	Browser	Windows 10	IE 11.0

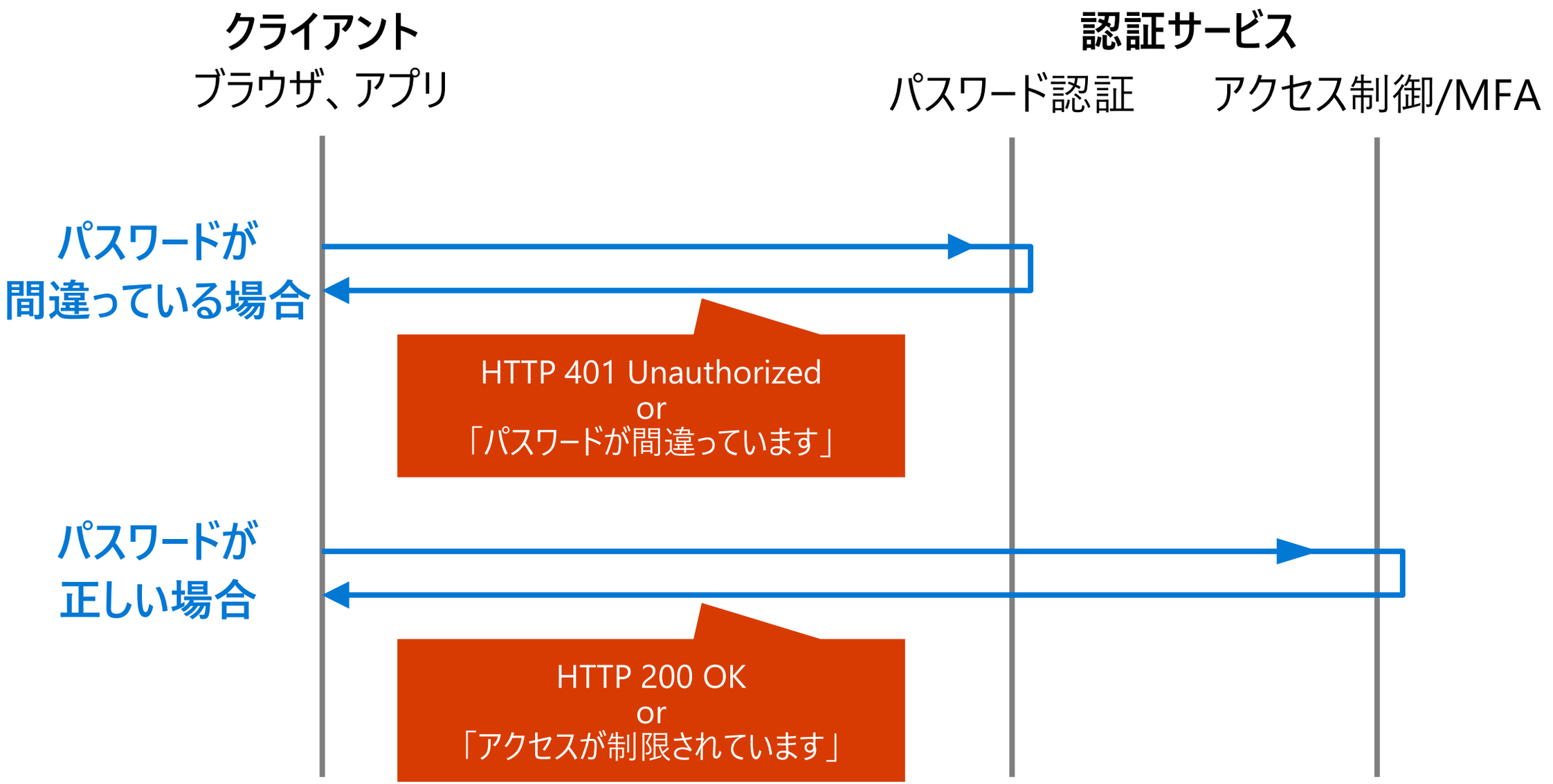
企業 A

Username	Application	Resource	Location	Status	Browser	Operating Sy
ats [redacted]	O365 Suite UX	Windows Azure Active Directory	Vilnius, Vilniaus Apskritis, LT	Failure	Chrome 43.0.2357	Windows 8
ats [redacted]	O365 Suite UX	Windows Azure Active Directory	New York, New York, US	Failure	Chrome 43.0.2357	Windows 8

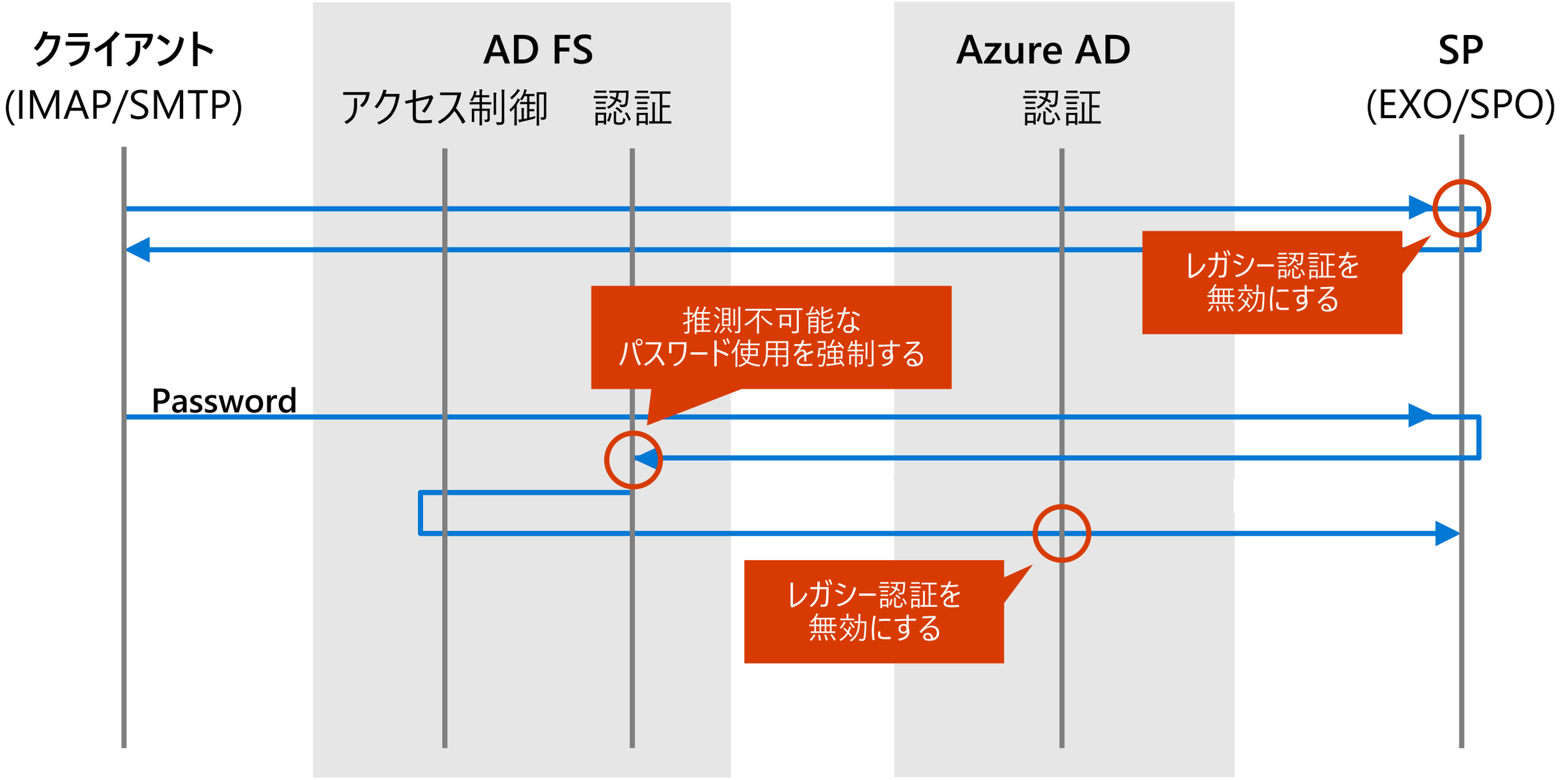
企業 B

Username	Application	Resource	Location	Status	Browser	Operating Sy
ca [redacted]	O365 Suite UX	Windows Azure Active Direc	Bangkok, Krung Thep, TH	Failure	Chrome 43.0.2357	Windows 8
ca [redacted]	O365 Suite UX	Windows Azure Active Direc	Silver Spring, Maryland, US	Failure	Chrome 43.0.2357	Windows 8
da [redacted]	O365 Suite UX	Windows Azure Active Direc	Greenville, South Carolina, US	Failure	Chrome 43.0.2357	Windows 8
er [redacted]	Office 365 Exchange Online		Tarrytown, New York, US	Failure	Chrome 43.0.2357	Windows 8
el [redacted]	Office 365 Exchange Online		Norristown, Pennsylvania, US	Failure	Chrome 43.0.2357	Windows 8
do [redacted]	Office 365 Exchange Online		Chicago, Illinois, US	Failure	Chrome 43.0.2357	Windows 8
de [redacted]	Office 365 Exchange Online		Austin, Texas, US	Failure	Chrome 43.0.2357	Windows 8
de [redacted]	Office 365 Exchange Online		Phoenix, Arizona, US	Failure	Chrome 43.0.2357	Windows 8
da [redacted]	Office 365 Exchange Online		Colleyville, Texas, US	Failure	Chrome 43.0.2357	Windows 8
cr [redacted]	Office 365 Exchange Online		Holly Ridge, North Carolina, US	Failure	Chrome 43.0.2357	Windows 8
ch [redacted]	Office 365 Exchange Online		Buffalo, New York, US	Failure	Chrome 43.0.2357	Windows 8
ch [redacted]	Office 365 Exchange Online		Brooklyn, New York, US	Failure	Chrome 43.0.2357	Windows 8
ch [redacted]	Office 365 Exchange Online		Los Angeles, California, US	Failure	Chrome 43.0.2357	Windows 8
be [redacted]	Office 365 Exchange Online		Los Angeles, California, US	Failure	Chrome 43.0.2357	Windows 8
bl [redacted]	Office 365 Exchange Online		Durham, North Carolina, US	Failure	Chrome 43.0.2357	Windows 8
ba [redacted]	Office 365 Exchange Online		San Francisco, California, US	Failure	Chrome 43.0.2357	Windows 8
an [redacted]	Office 365 Exchange Online		Los Angeles, California, US	Failure	Chrome 43.0.2357	Windows 8
al [redacted]	Office 365 Exchange Online		Scottsdale, Arizona, US	Failure	Chrome 43.0.2357	Windows 8

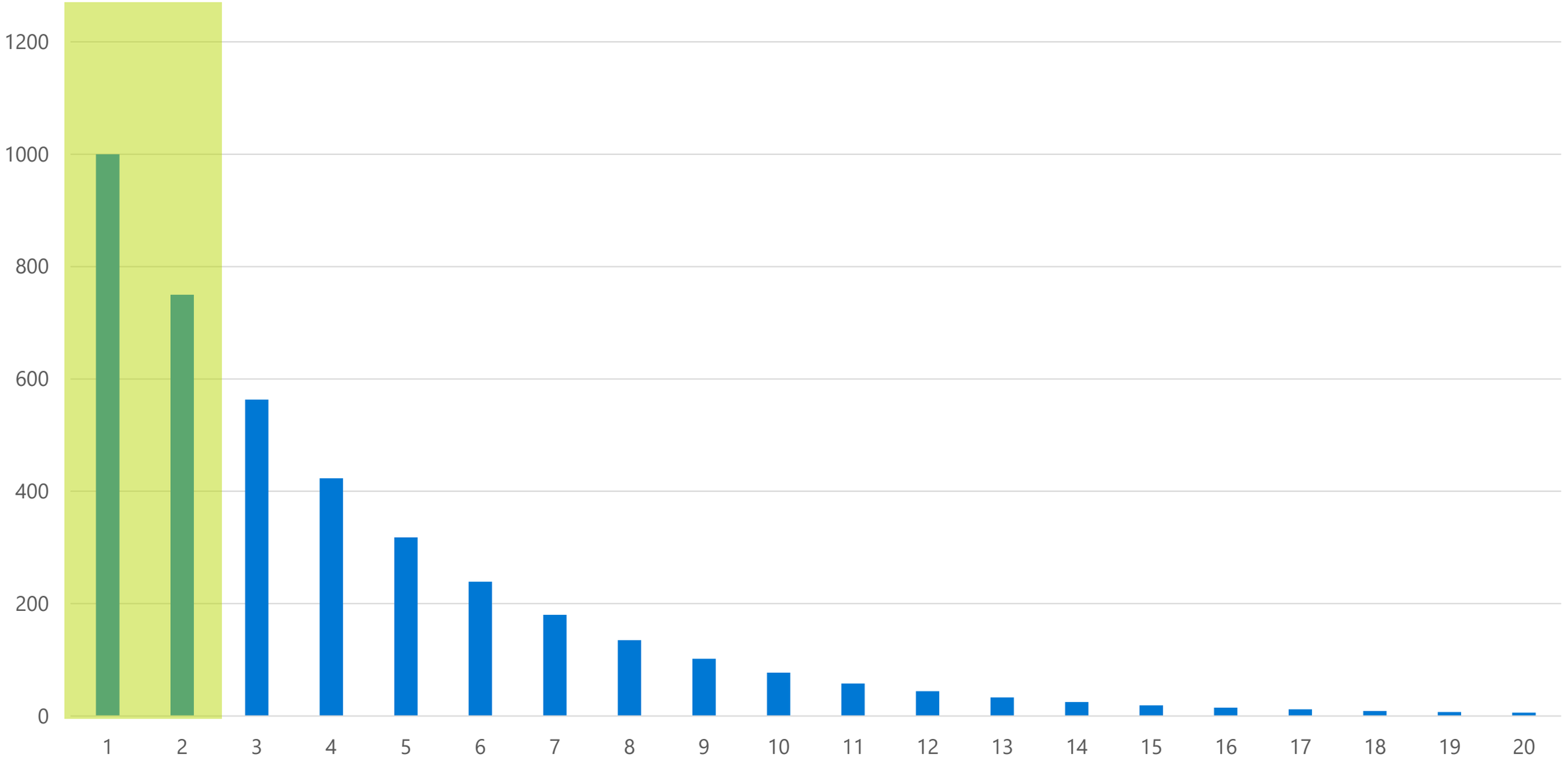
アクセス制御をしてもパスワード自体は漏えいする



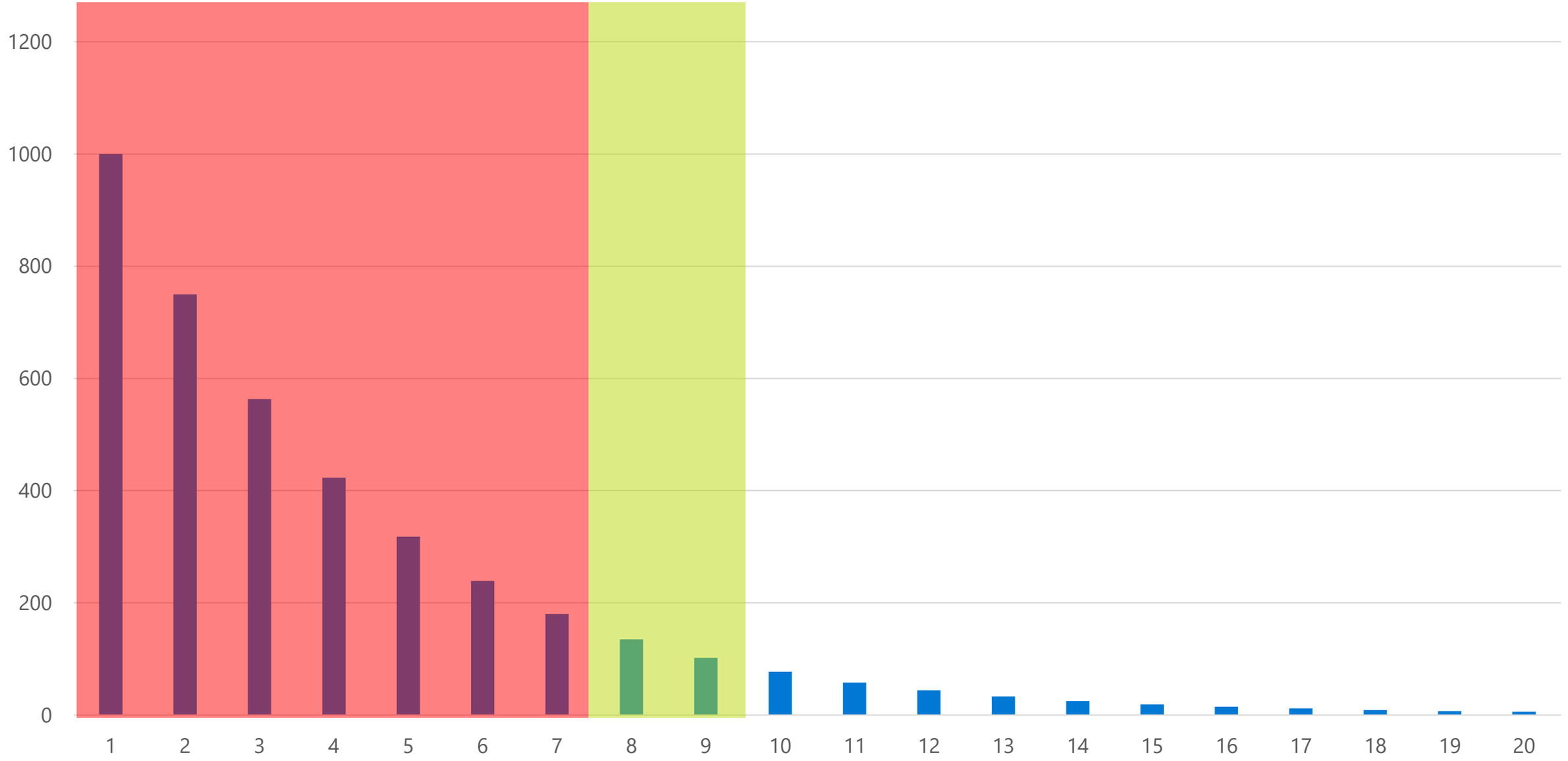
パスワード スプレーへの対応



Count of passwords by rank



Count of passwords by rank



Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

Demo

パスワード スプレー攻撃と対策

・レガシー認証の廃止 (条件付きアクセス vs EXO 認証ポリシー)

・Azure AD Password Protection

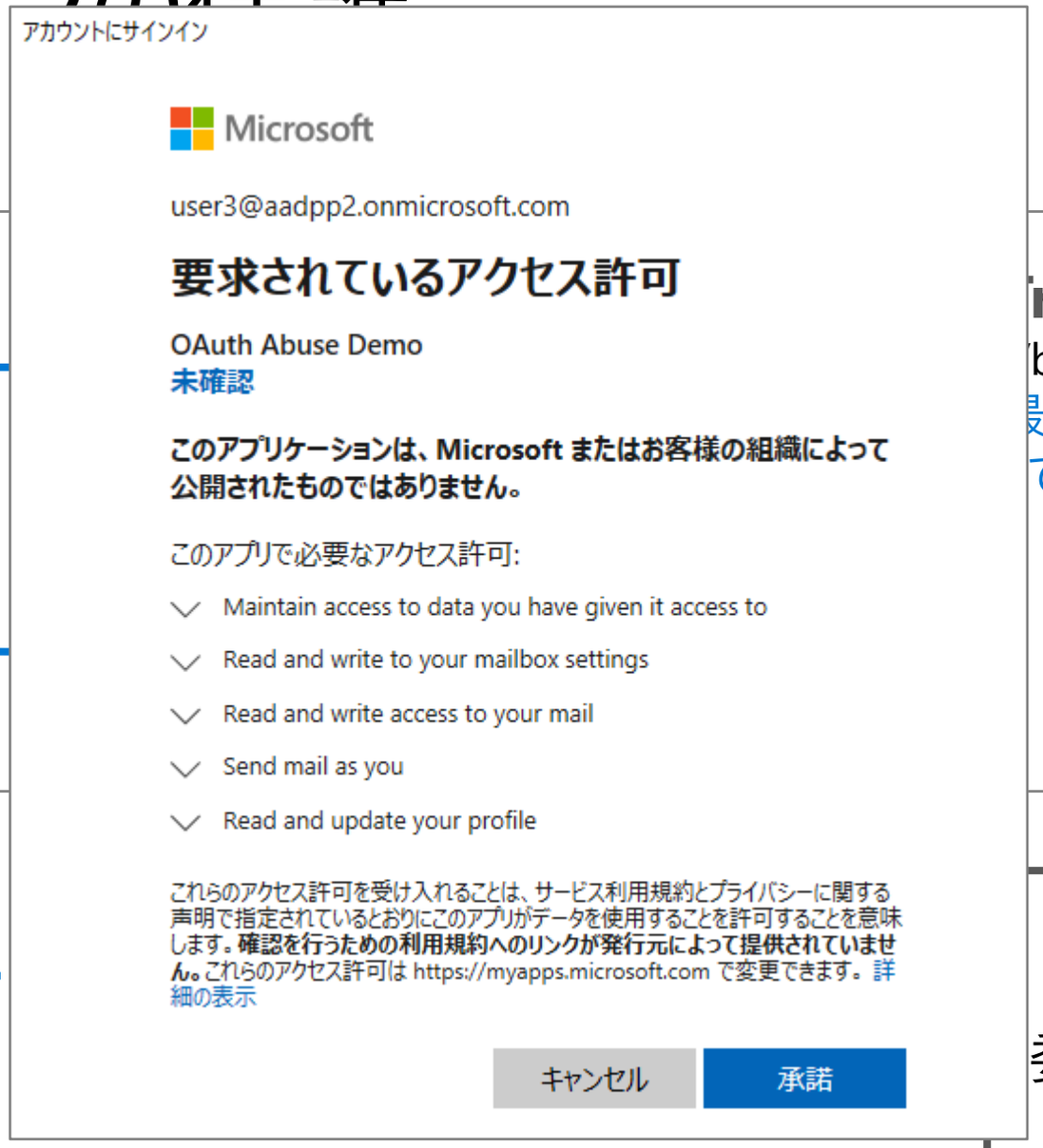
Microsoft

アクセストークンの保護

持ち出し

サインイン

同意



rust Summit 2019
/biz/security/summit-online.aspx
最新の攻撃手法と対策のご紹介
てきたセッション管理の重要性—

委任されたアクセス許可
(ユーザーの同意)

サービス プリンシパルはユーザーを偽装できる

- **Azure AD セキュリティ プリンシパル**
  - User = ユーザー プリンシパル
  - Application = サービス プリンシパル
    - Exchange Online, OneDrive for Business, Teams, Microsoft Graph…

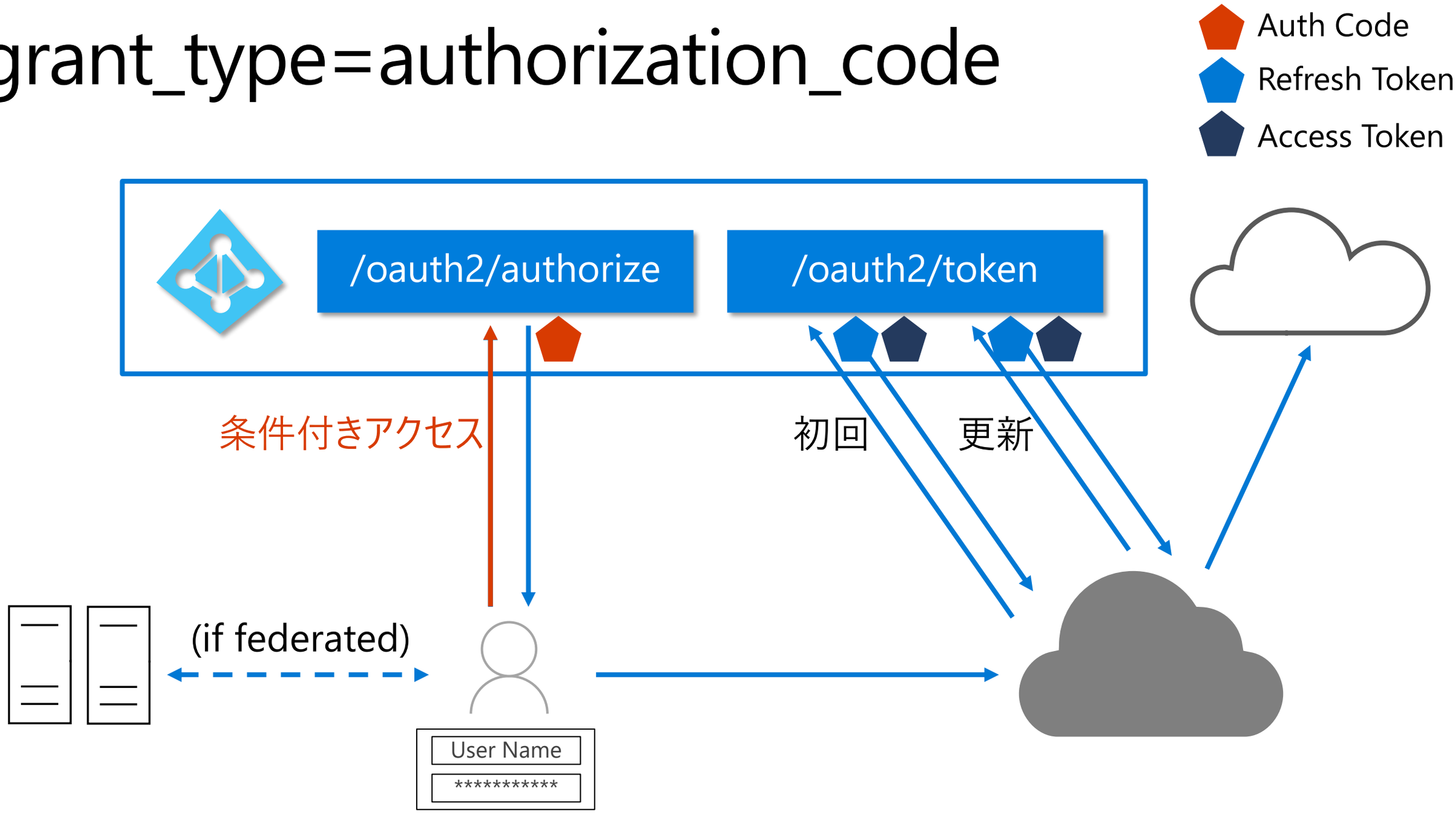
- **Application (サービス プリンシパル) の権限**
  - アプリケーションの許可
    - サインインしたユーザーなしで、バック グラウンド サービスとして API にアクセスする
  - 委任されたアクセス許可
    - サインインしたユーザーとして API にアクセスする

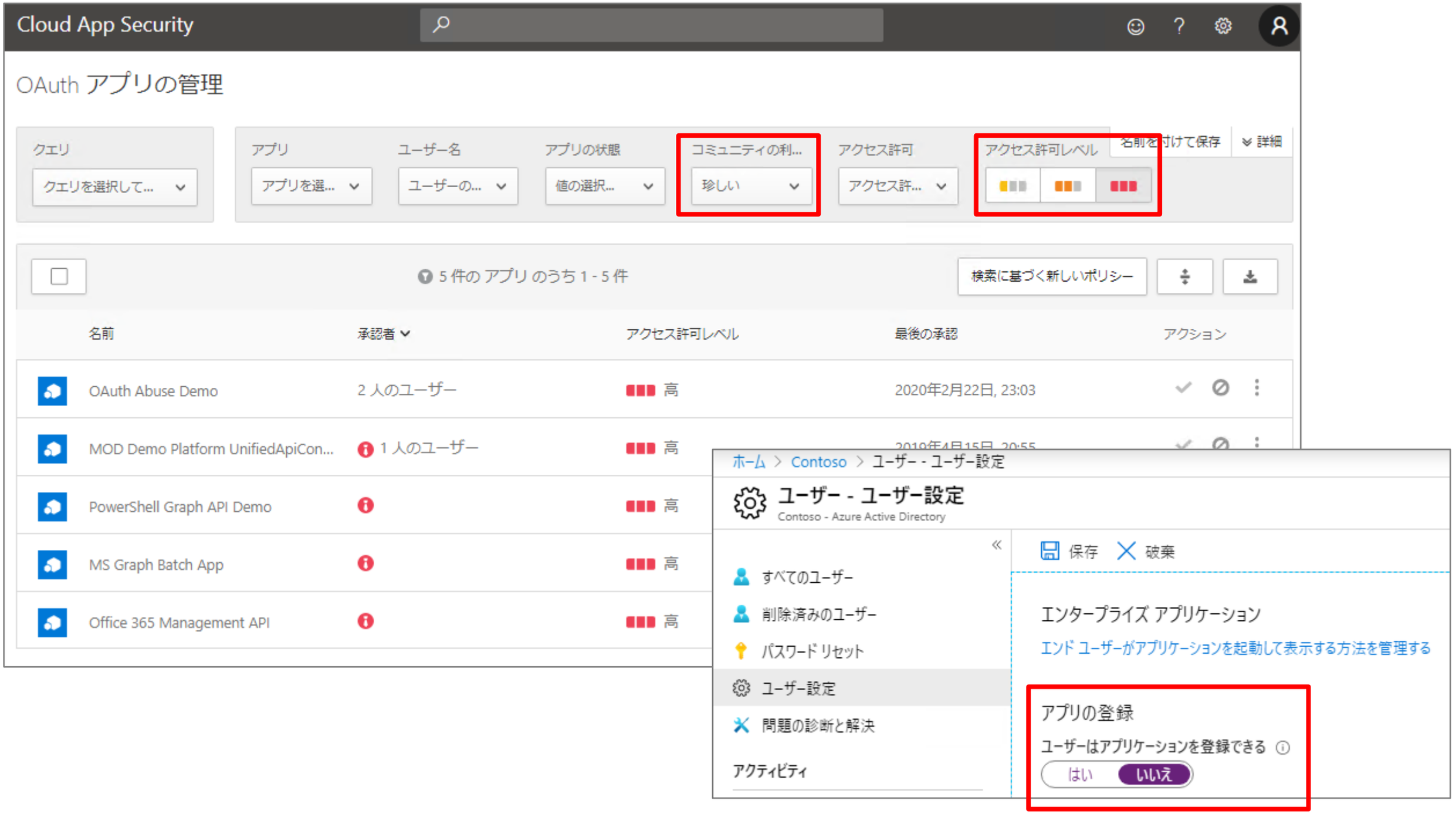
Consent Abuse / OAuth Abuse

- **OAuth 2.0**
  - ユーザーの同意のもと、サービス プリンシパルに対して認可情報を委譲する
  - パスワードをサービスに渡す必要がなく、委譲する認可の範囲を限定できる

- **攻撃者のメリット**
  - MFA / 条件付きアクセスの制限を受けない
  - アクセス トークンを一度取得すると長期間アクセスできる
  - ユーザーがパスワードを変更してもアクセスを失わない
  - AAD サインイン ログに記録されない

grant_type=authorization_code




Cloud App Security
OAuth アプリの管理
クエリ
クエリを選択して...
アプリ
アプリを選...
ユーザー名
ユーザーの...
アプリの状態
値の選択...
コミュニティの利...
珍しい
アクセス許可
アクセス許...
アクセス許可レベル
名前を付けて保存
詳細
5 件の アプリ のうち 1 - 5 件
検索に基づく新しいポリシー
名前
承認者
アクセス許可レベル
最後の承認
アクション
OAuth Abuse Demo
2 人のユーザー
高
2020年2月22日, 23:03
MOD Demo Platform UnifiedApiCon...
1 人のユーザー
高
PowerShell Graph API Demo
高
MS Graph Batch App
高
Office 365 Management API
高
ホーム > Contoso > ユーザー - ユーザー設定
ユーザー - ユーザー設定
Contoso - Azure Active Directory
すべてのユーザー
削除済みのユーザー
パスワード リセット
ユーザー設定
問題の診断と解決
アクティビティ
保存
破棄
エンタープライズ アプリケーション
エンド ユーザーがアプリケーションを起動して表示する方法を管理する
アプリの登録
ユーザーはアプリケーションを登録できる
はい
いいえ

Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

Demo

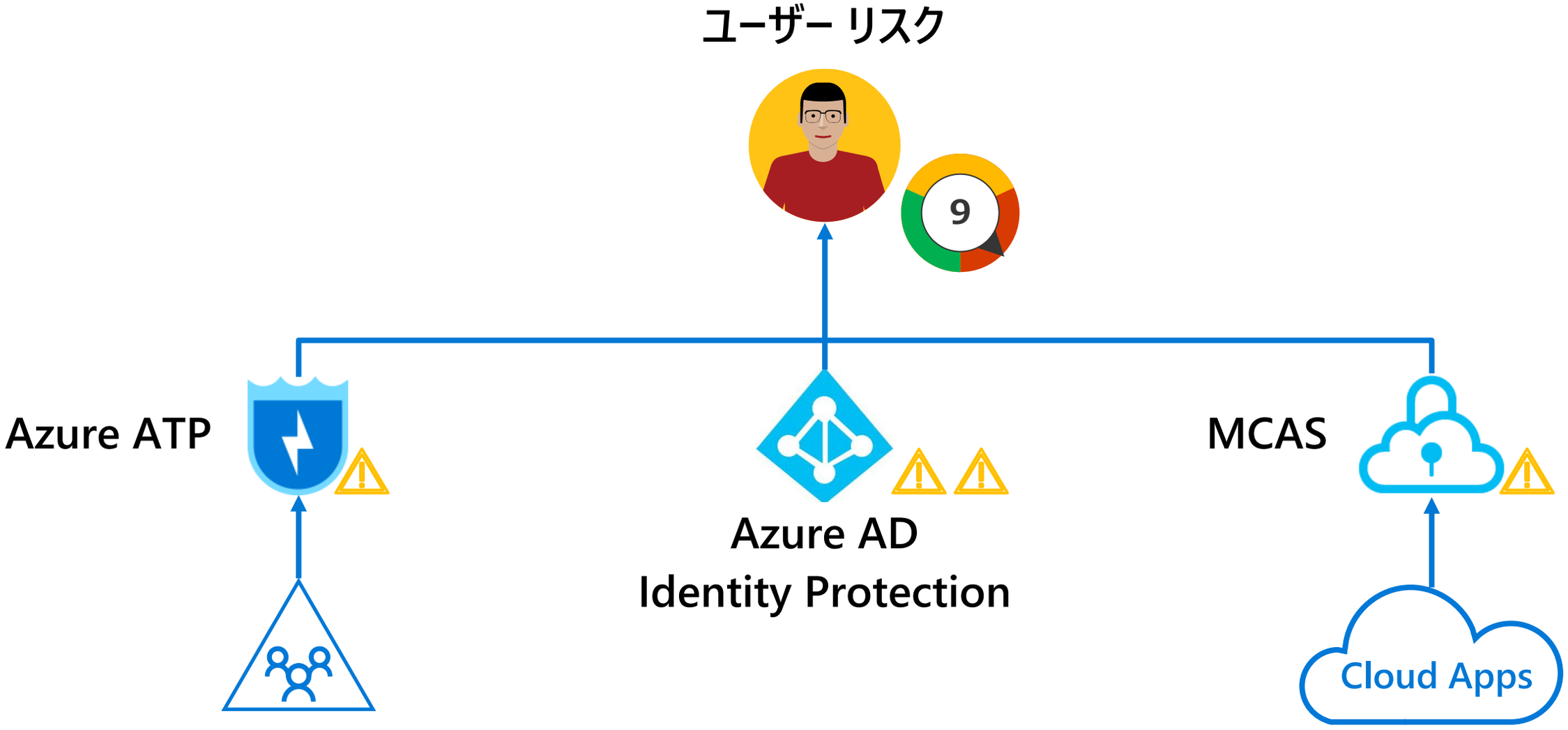
アクセス トークンの窃取と対策

・Consent Abuse

・MCAS

Microsoft

ユーザー リスクに基づいた自動対処



Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

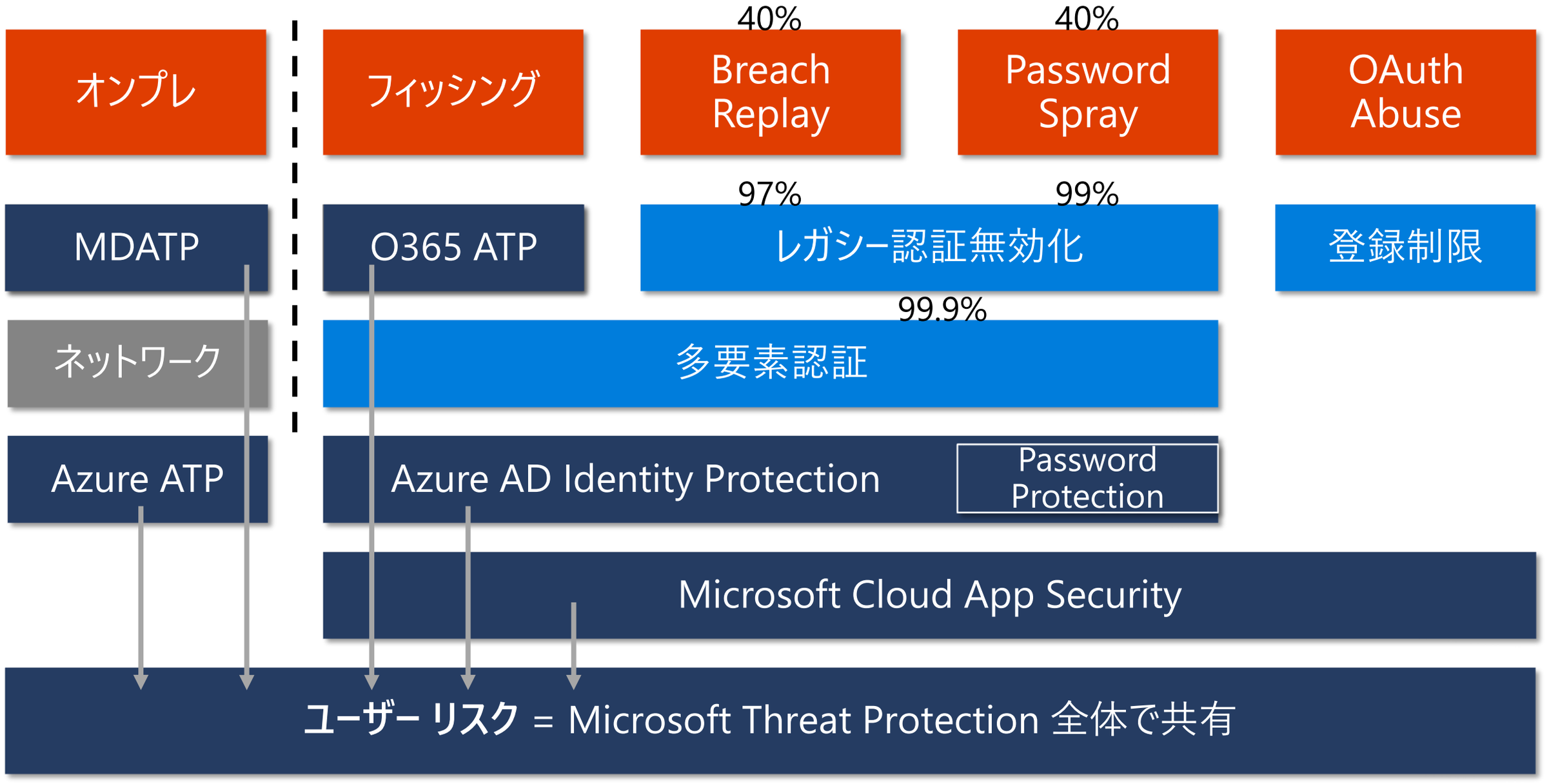
Demo

ユーザー リスクに基づいた自動対処

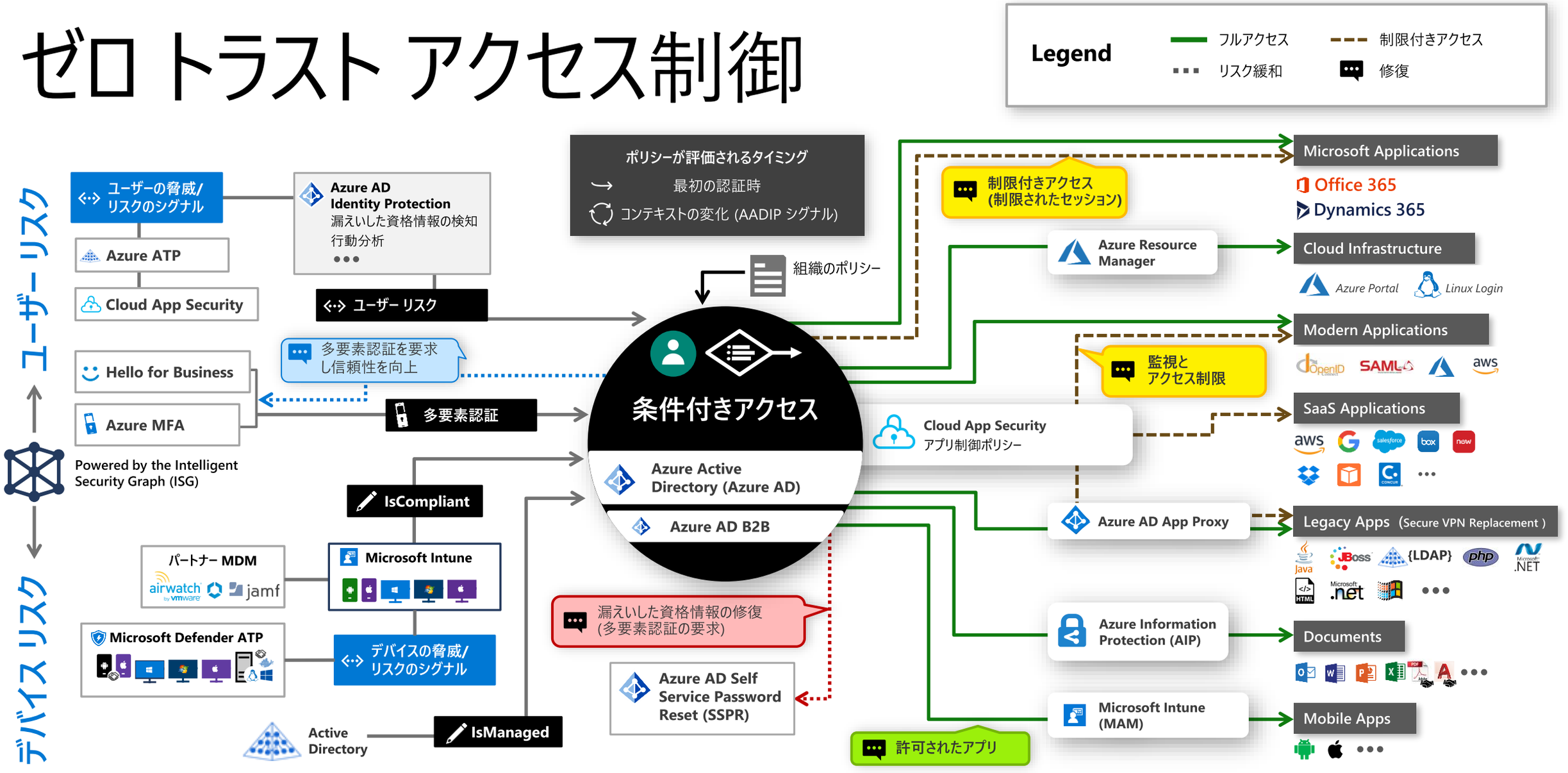
- Azure AD Identity Protection
- MCAS

Microsoft

パスワード/トークン窃取への対応まとめ



ゼロ トラスト アクセス制御

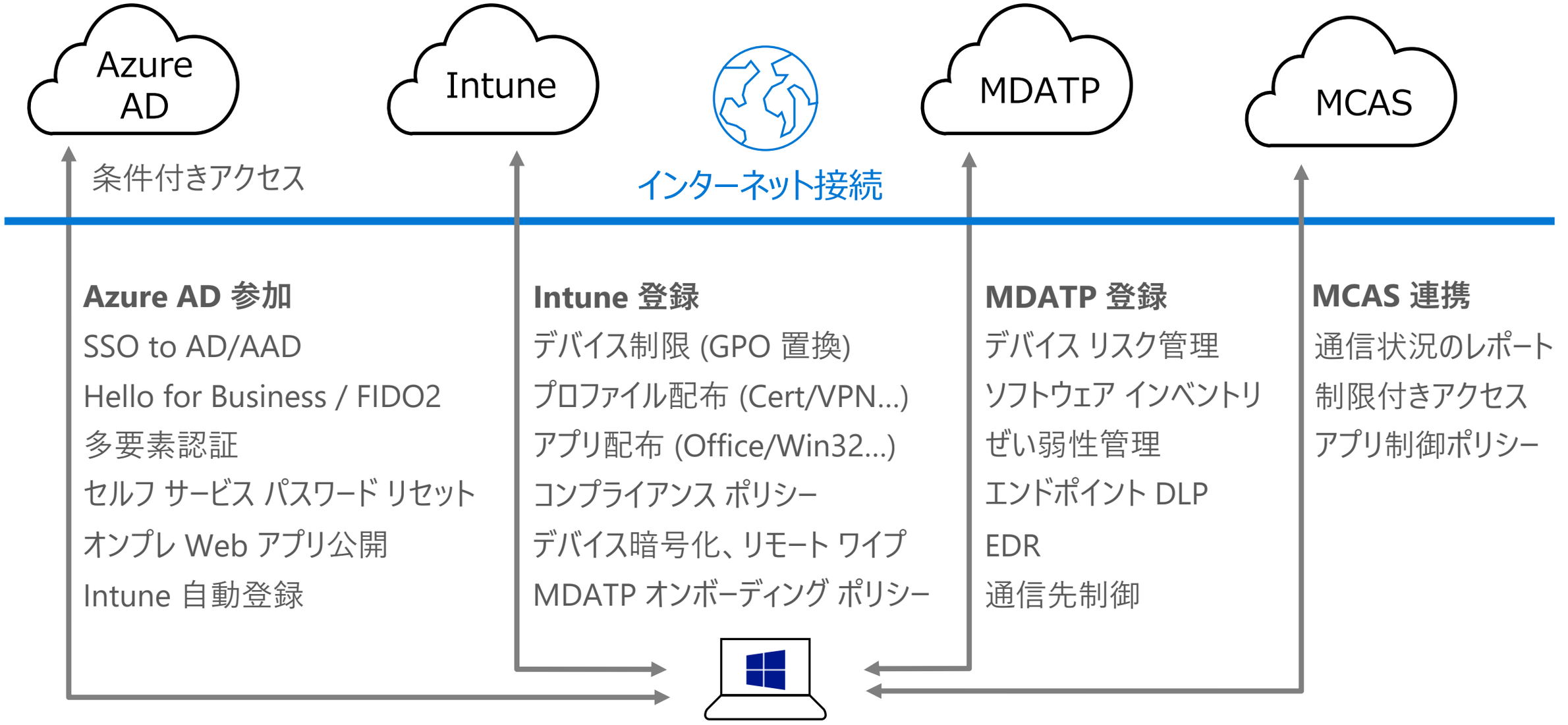


シグナル
to make an informed decision

判断
based on organizational policy

強制
of policy across resources

M365 で実現するデバイスのモダン管理



Azure AD 参加済みデバイス上でオンプレミス リソースへの SSO が機能するしくみ

2019/06/28 •

Azure Active Directory (Azure AD) に参加しているデバイスによって、ご利用のテナントのクラウド アプリへのシングル サインオン (SSO) エクスペリエンスが提供されることは、おそらく驚くことではありません。 ご利用の環境にオンプレミスの Active Directory (AD) がある場合、それらのデバイスでの SSO エクスペリエンスをその AD に拡張できます。

この記事では、この動作のしくみについて説明します。

前提条件

Azure AD 参加済みマシンが組織のネットワークに接続されていない場合は、VPN または他のネットワーク インフラストラクチャが必要です。 オンプレミスの SSO には、オンプレミスの AD DS ドメイン コントローラーとの見通し内通信が必要です。

しくみ

1 つのユーザー名とパスワードを覚えておくだけでよいため、SSO によってリソースへのアクセスが簡略化され、ご利用の環境のセキュリティが向上します。 ユーザーは Azure AD 参加済みデバイスを使用して、ご利用の環境内のクラウド アプリへの SSO エクスペリエンスを既に手に入れています。 ご利用の環境内に Azure AD とオンプレミス AD がある場合は、SSO エクスペリエンスの範囲をオンプレミスの業種 (LOB) アプリ、ファイル共有、およびプリンターにまで拡張することをおそらく希望するでしょう。

Azure AD 参加済みデバイスには、オンプレミス AD 環境についての情報はありません (その環境に参加していないた

Windows Hello for Business を使用して Azure AD に参加しているデバイスをオンプレミスのシングル サインオン用に構成する

2018/08/19 •

適用対象

- Windows 10
- Azure Active Directory に参加済み
- ハイブリッド展開
- キー信頼モデル

前提条件

Azure Active Directory (Azure AD) に参加しているデバイスを既存のハイブリッド展開に追加する前に、既存の展開で Azure AD に参加しているデバイスをサポートできることを確認する必要があります。 ハイブリッドの Azure AD に参加しているデバイスとは異なり、Azure AD に参加しているデバイスには Active Directory ドメインとの関係はありません。この要素により、ユーザーの Active Directory に対する認証方法が変わります。 次の構成を検証して、Azure AD に参加しているデバイスがサポートされることを確認します。

- Azure Active Directory Connect の同期
- デバイスの登録
- 証明書失効リスト (CRL) 配布ポイント (CDP)
- 2016 ドメイン コントローラー
- ドメイン コントローラー証明書

Azure Active Directory Connect の同期

ここまでの振り返り

- **パスワードは狙われている**
  - 日和見的 (自動的、無差別的) な攻撃から標的型攻撃まで
  - レガシー認証の無効化と Password Protection で攻撃面積の最小化
  - 多要素認証と条件付きアクセス ポリシーを確実に適用する

- **アクセス トークンは狙われている**
  - OAuth 認証フローを悪用したフィッシング手法に注意
  - アプリの登録制限で攻撃面積の最小化
  - ユーザー プリンシパルが要求するアクセス トークン悪用は条件付きアクセスで保護
  - サービス プリンシパルが要求するアクセス トークン悪用は MCAS で監視

ここまでの振り返り

- **ゼロ トラスト アクセス制御**
  - “ユーザー リスク” と “デバイス リスク” を管理するという考え方
  - リスクに対しては組織のポリシー (ブロック、MFA、制限) を強制する

- **ゼロ トラストは “ユーザーのため”**
  - “いつでも、どこでも” を支援する統合されたシンプルなオペレーションを構築する
    - デバイス自動プロビジョニング (企業ポリシーが適用された BYOD の検討)
    - リスク検出やパスワード リセットで共通で利用できる多要素認証
    - ユーザーやサインインのリスク検知に支えられたパスワード無期限化
    - パスワード レス

Microsoft

Microsoft
DIGITAL TRUST
SECURITY

#digitaltrust