TD SYNNEX

在宅勤務時でも Microsoft 365へ 安心アクセス！

～Windows 10 編～

※2022年3月時点の情報です。内容は変更になる可能性があります。

アジェンダ

- Microsoft 365アクセス時の問題点
- 在宅勤務時でも安心してMicrosoft 365へアクセスする為に
- ユーザー利用の流れ
- Windows 10を管理する「Microsoft Intune」
- Windows 10を制御する「Azure AD Premium」
- ユーザー側での設定の流れ
- 管理者側での設定の流れ
- 本日ご紹介した在宅勤務でも安全な機能が使えるプラン
- まとめ

Microsoft 365アクセス時の問題点

Microsoft 365を制限せずに利用するのは、便利ではあるが問題点が…

［例］

サインイン情報を知っていれば
誰でもどこからでもアクセス可能

ID/PW漏洩による
不正アクセス

情報流出のリスク

セキュリティリスクが高く
安心安全ではない状態

Microsoft 365を
安心安全に利用するには

［例］

会社が許可した
デバイス

会社が設定した
ルール

限定条件からのみアクセスを
管理・制御することで、安心安全な
Microsoft 365へのアクセスが可能に!

在宅勤務時でも安心してMicrosoft 365へアクセスする為に

TD SYNNEX

Microsoft 365へのアクセスを行うには以下の2つがお勧めです！

Microsoft Intune

デバイス管理

×

Azure AD Premium

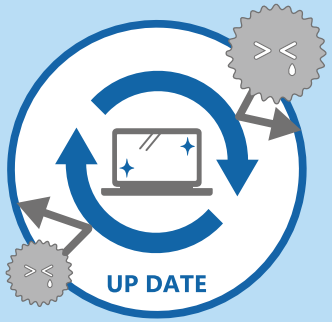
条件を合わせたアクセス制御

アクセスできるデバイスを管理・制御することで、安心安全なMicrosoft 365へのアクセスを実現

管理・制御が
できている場合

決められた
デバイスからのアクセス

もしもの時の
リモートワイプ

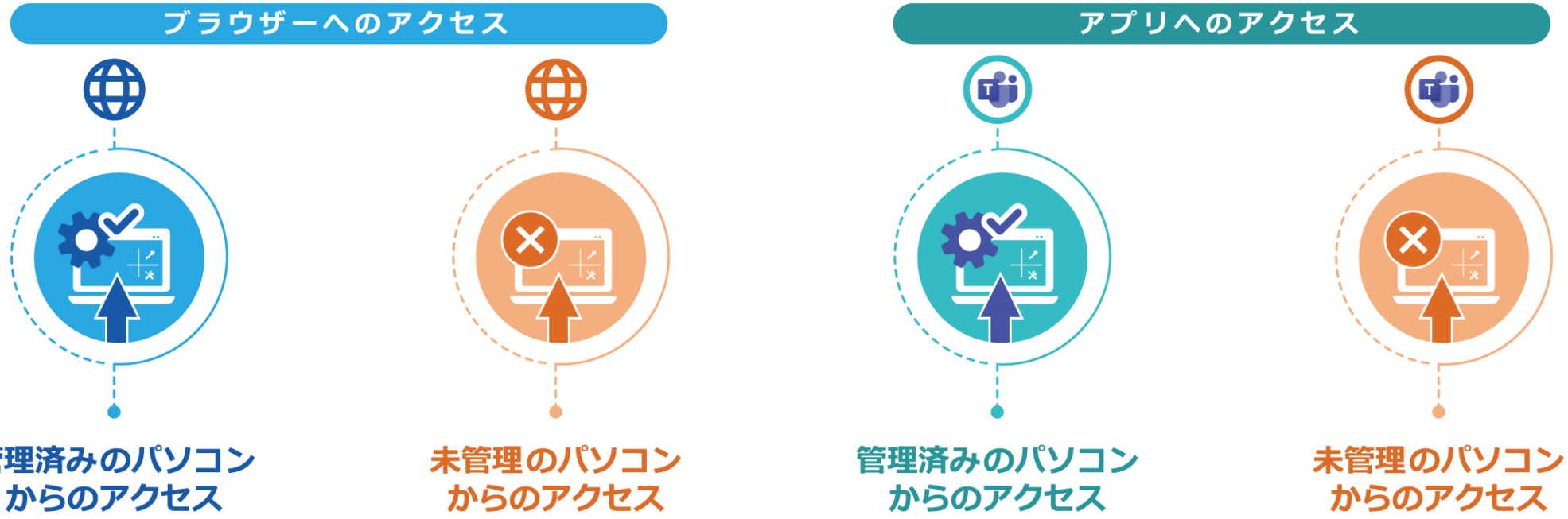


Windowsの
バージョンを管理

会社のルールに
沿った運用が可能

ユーザー利用の流れ

Intuneにより管理済みのパソコンと未管理のパソコンからそれぞれ、Microsoft 365へアクセスした際の実際の動きを確認していきましょう

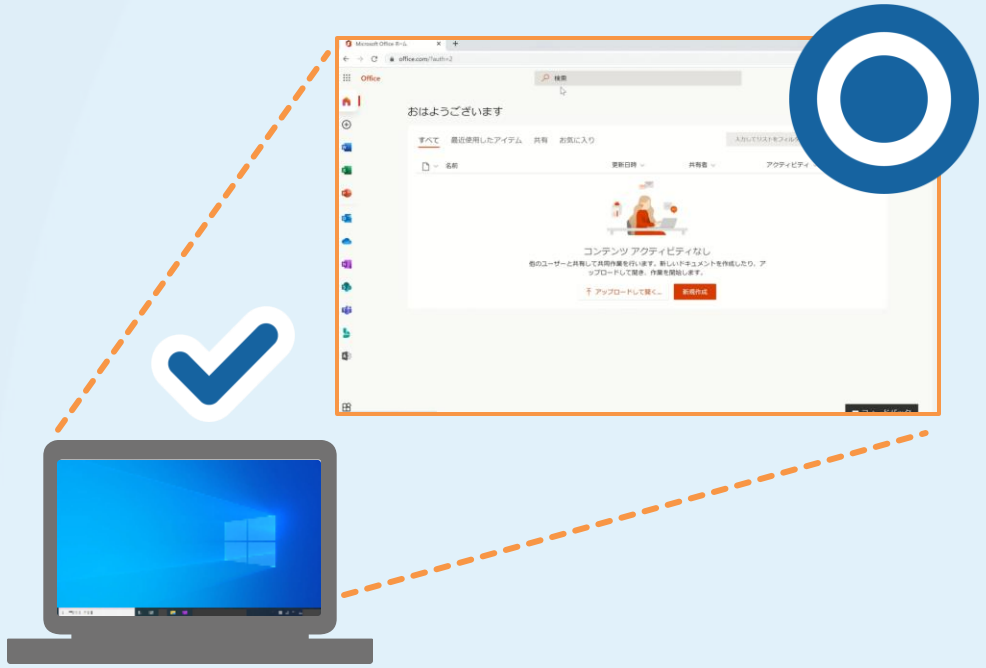


※Intuneにより未管理のパソコンからはアクセスできない様にAzure AD Premiumにて制御しています
※アプリへのアクセスは例として、**Teamsへのサインイン**を実施しています

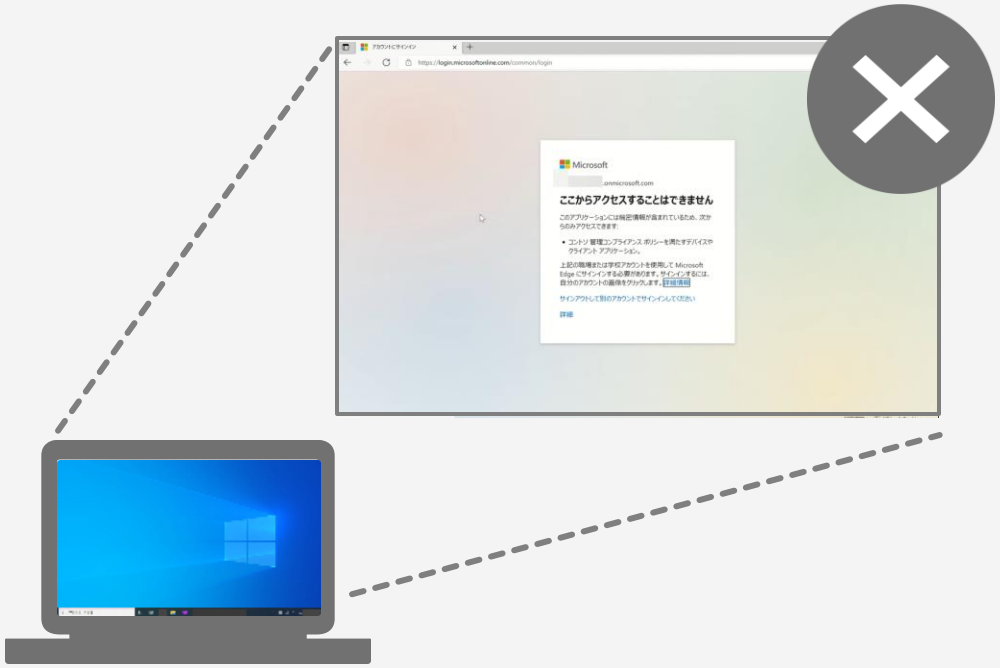
ブラウザーへのアクセス

TD SYNNEX

管理済みのパソコンからのアクセス



未管理のパソコンからのアクセス



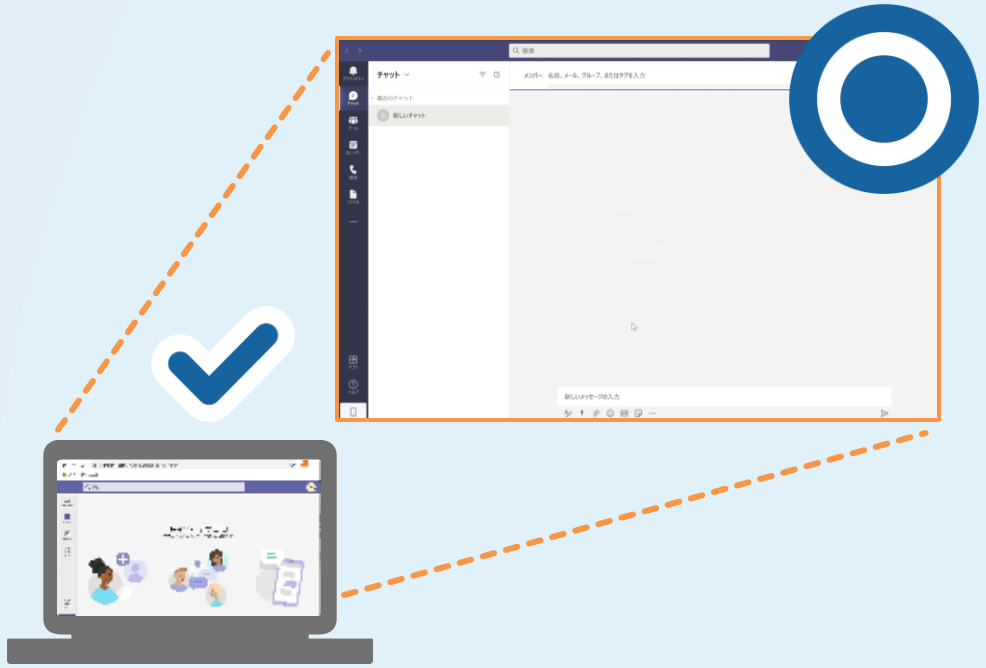
管理済みのパソコンであればMicrosoft 365にアクセスできますが、
未管理のパソコンからのブラウザーアクセスはブロックされ、
アクセスすることができません

動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

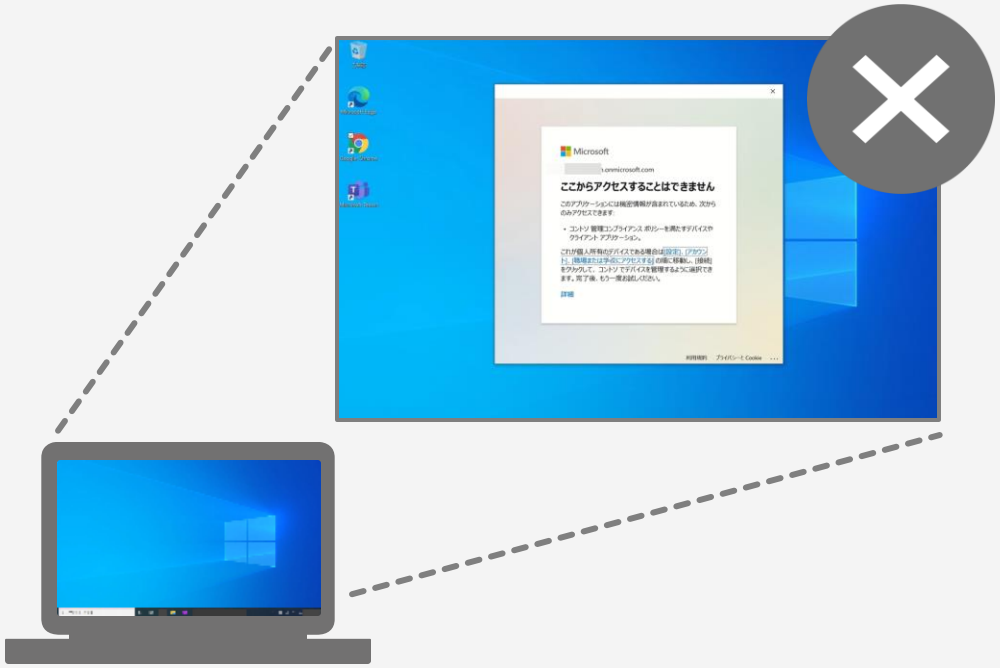
Teamsアプリへのアクセス

TD SYNNEX

管理済みのパソコンからTeamsアプリにアクセス



未管理のパソコンからTeamsアプリにアクセス



管理済みのパソコンであれば、Teamsアプリにアクセスできますが、
未管理のパソコンからのTeamsアプリへのアクセスはブロックされ、
アクセスすることができません

動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

Windows 10を管理する「Microsoft Intune」

デバイス管理機能を提供するプランで、**Microsoft 365のセキュリティを向上させる**ことが可能です
具体的に出来ることの一例をあげます

デバイス管理

Windows 10以外にも mac OS
Android OS・iOS の管理も可能に

アプリケーション管理

主にスマートフォン、タブレットの
アプリケーションを管理可能

条件付きアクセス

会社のルールに沿ったアクセス
（Azure AD Premiumとの組み合わせ）

デバイス管理で、リモートワイプも可能に! もしもの時に得られる安心のセキュリティ！
これからの**Microsoft 365利用に欠かせないサービス**です

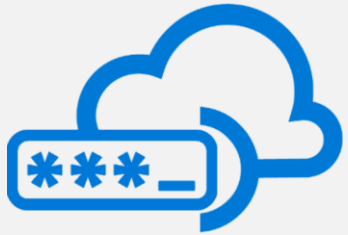
Windows 10を制御する「Azure AD Premium」

高度な認証やアクセス制御を提供するプランで、**Microsoft 365のセキュリティを向上させる**ことが可能です
Windows 10を制御する以外に、具体的に出来ることの一例をあげます

セルフパスワードリセット

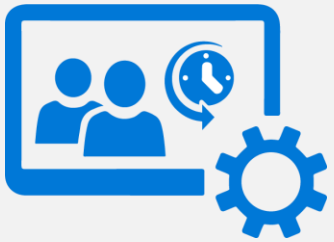
ユーザーがPWを忘れた場合に
自身で再発行

シングルサインオン



Microsoft 365や他のクラウド
サービスへシングルサインイン

グループの有効期限設定



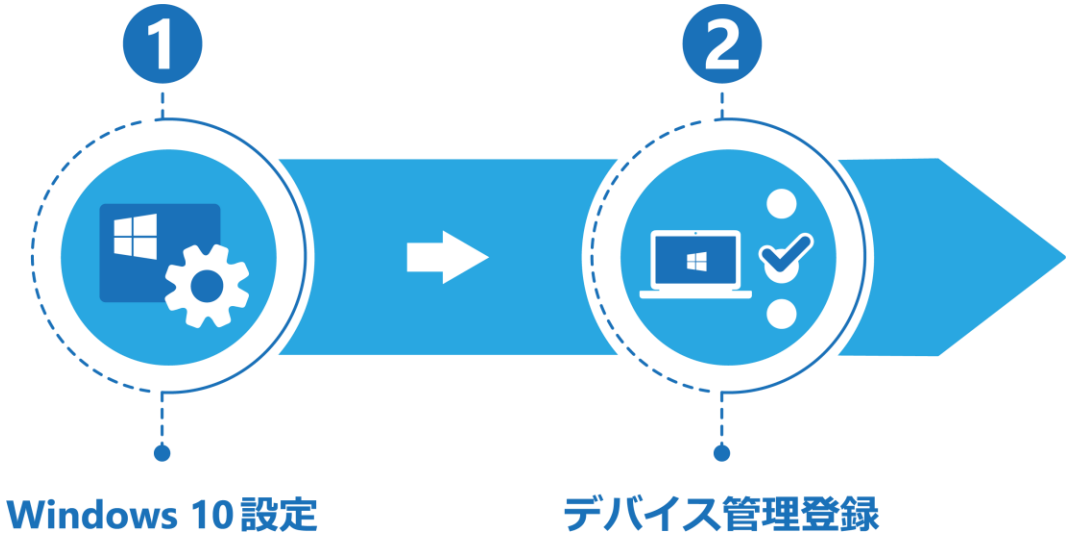
グループを制御し、作成したTeams
のチームに有効期限設定が可能に

etc...

クラウドを活用する中、会社のルールに則った運用を実現！
これからの**Microsoft 365利用に欠かせないサービス**です

ユーザー側での設定の流れ

以下の流れに沿って、ユーザー（利用者）が必要になる設定を確認していきましょう

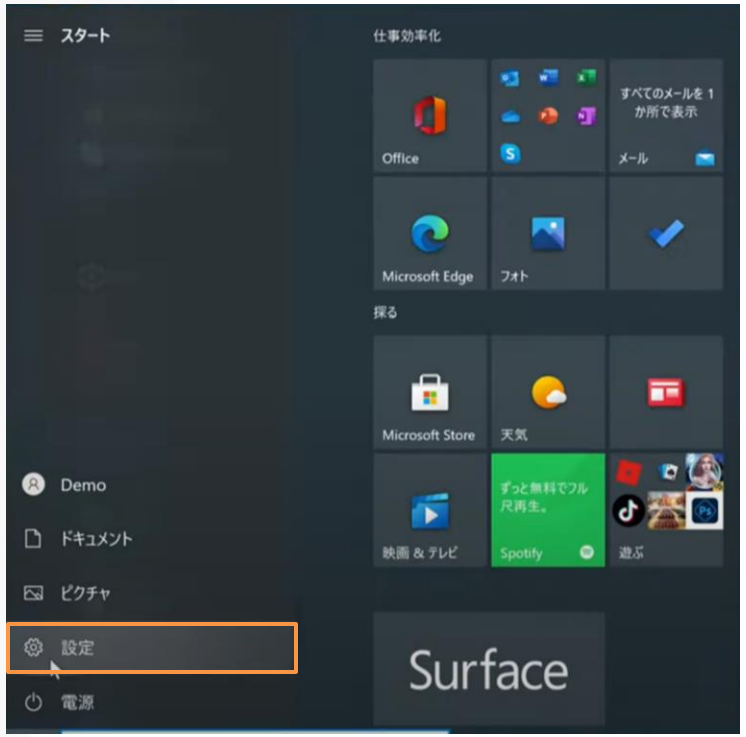


※設定にはPC管理者である必要がございますので、事前にご確認をお願いします

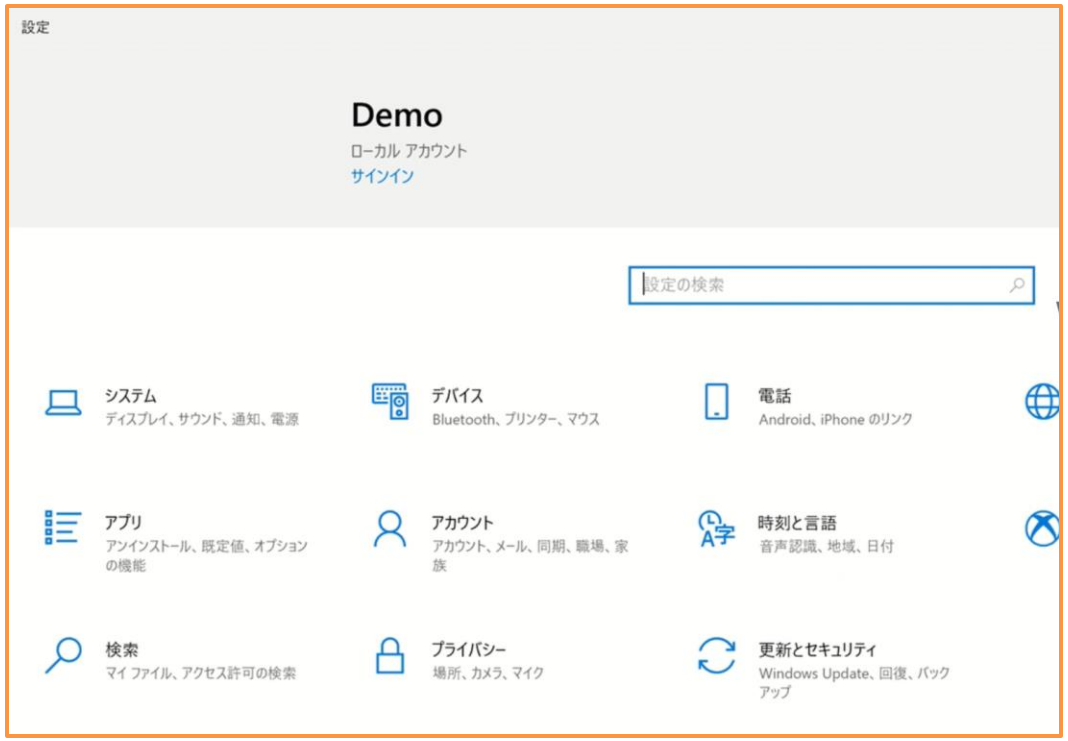
Windows 10の設定を表示

事前準備としてWindows の設定を開きます

Windows10の設定を選択



設定が開きます



動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

デバイス管理登録

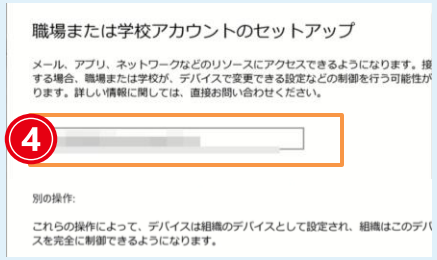
TD SYNNEX

アカウントから「職場または学校にアクセスする」にデバイスを登録します

アカウントを選択

職場または学校にアクセスするを選択 接続を選択

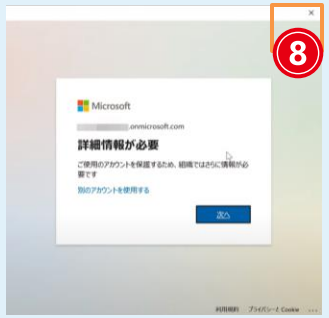
Microsoft 365で使用するアカウント（メールアドレス）を入力



5 次へ を選択

パスワードを入力 サインインを選択

×を選択

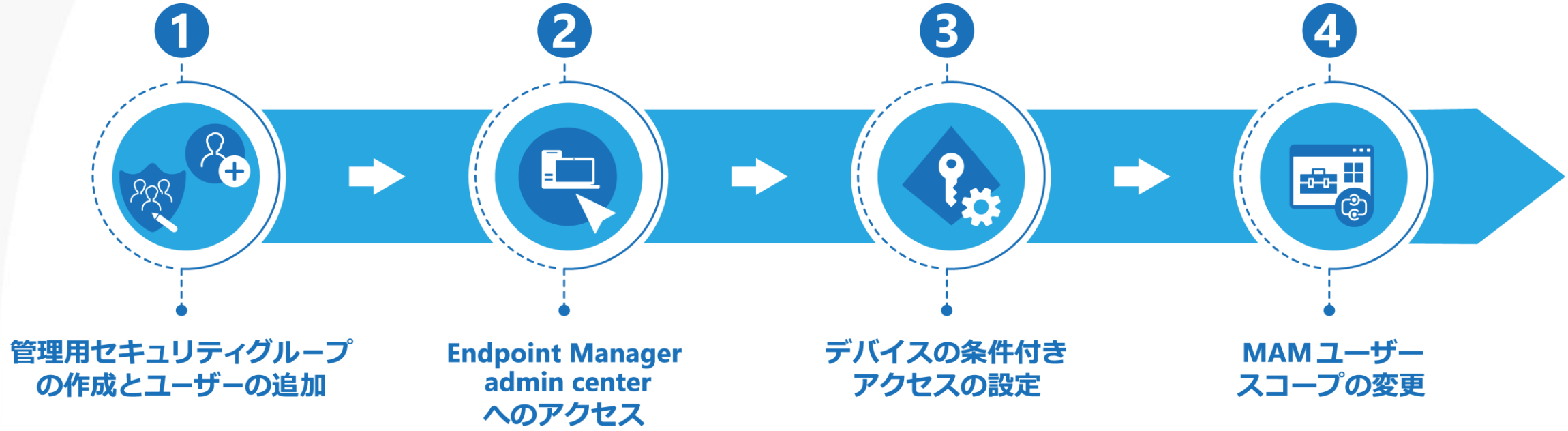


CHECK! 設定したアカウント名が表示されれば完了！

動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

管理者側での設定の流れ

以下の流れに沿って、管理者が必要になる設定を確認していきましょう



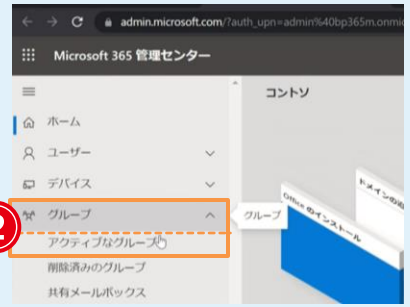
※設定にはMicrosoft 365の管理者である必要がございますので、事前にご確認をお願いします

管理用セキュリティグループの作成とユーザーの追加①

セキュリティーグループを作成し、その中に管理したいメンバーを追加します
ルール適用をコントロールするために、グループのメンテナンスを行います

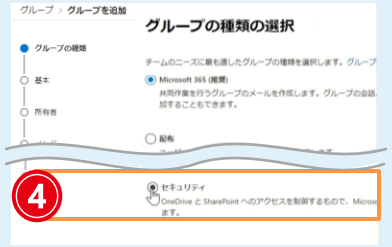
☑ Microsoft 365管理センターへアクセス→管理を選択

☑ グループで制御したいため、
グループ→アクティブなグループを選択



☑ グループの追加を選択

☑ セキュリティにチェック



⑤ **次へ** を選択

☑ グループ名を入力

⑦ **次へ** を選択

⑧ **グループを作成** を選択

⑨ **閉じる** を選択

動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

管理用セキュリティグループの作成とユーザーの追加②

TD SYNNEX

作成したグループを選択

グループの所有者の追加を選択　追加を選択

＋所有者の追加を選択

グループの管理者を選択　追加を選択

CHECK! 一覧に追加されたことを確認　戻るを選択

メンバータブを選択　すべてのメンバーの表示と管理を選択

＋メンバーの追加を選択

追加したいメンバーを選択　追加を選択

完了！

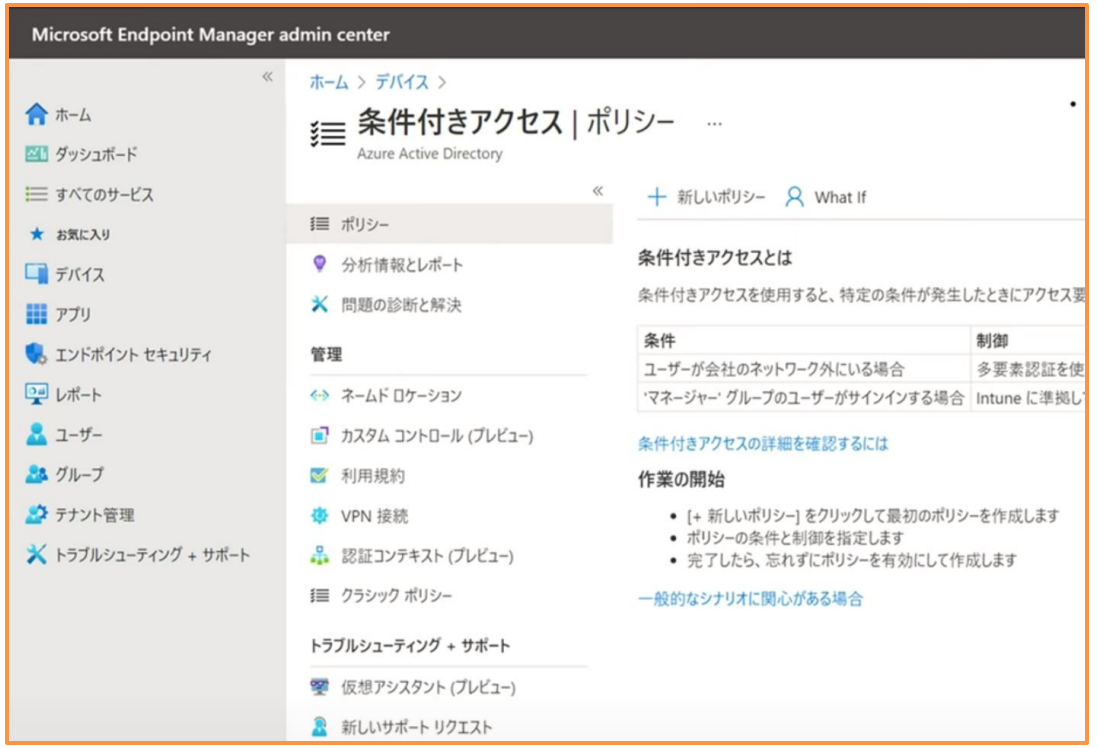
動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

Endpoint Manager admin center へのアクセス

エンドポイントマネージャーにアクセスします

Microsoft 365管理センターの管理センターから、エンドポイントマネージャーを選択

エンドポイントマネージャーにアクセス



動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

デバイスの条件付きアクセスの設定①

作成したセキュリティーグループに対して、Windowsデバイスからのアクセス、ブラウザーとデスクトップクライアントからMicrosoft 365へアクセスする設定を行います

動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

デバイスの条件付きアクセスの設定②

TD SYNNEX

条件→0個の条件が選択されましたを選択

デバイスプラットフォームの未構成を選択

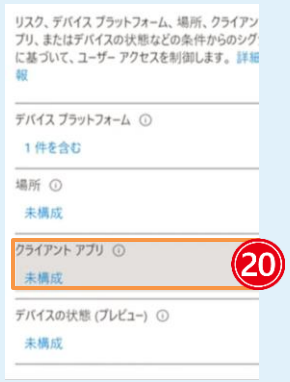
構成をはいに変更

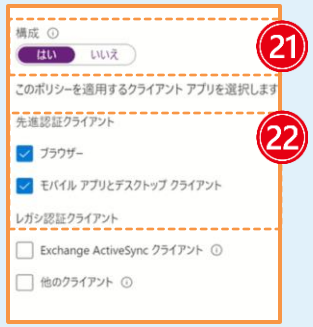
デバイスプラッフォームの選択にチェック

Windowsにチェック

完了 を選択 19

クライアントアプリから未構成を選択





構成をはいに変更

先進認証クライアント→ブラウザーと、モバイルアプリとデスクトップクライアントのみにチェック

完了 を選択 23

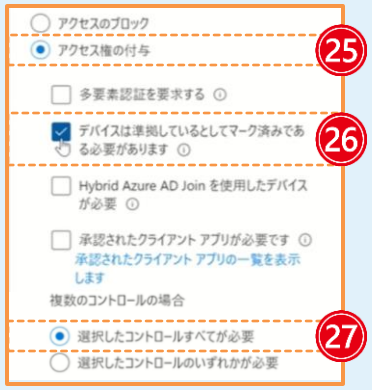
アクセス制御の許可から0個のコントロールが選択されましたを選択

アクセス権の付与にチェック

デバイスは準拠しているとしてマーク済みである必要がありますにチェック

選択したコントロールすべてが必要にチェック

選択 を選択 28



ポリシーの有効化をオンに変更

作成 を選択 30

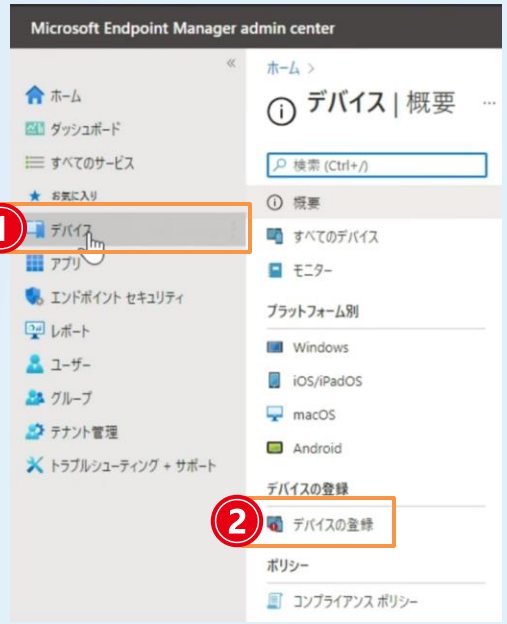
設定完了！

動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

MAM ユーザースコープの変更

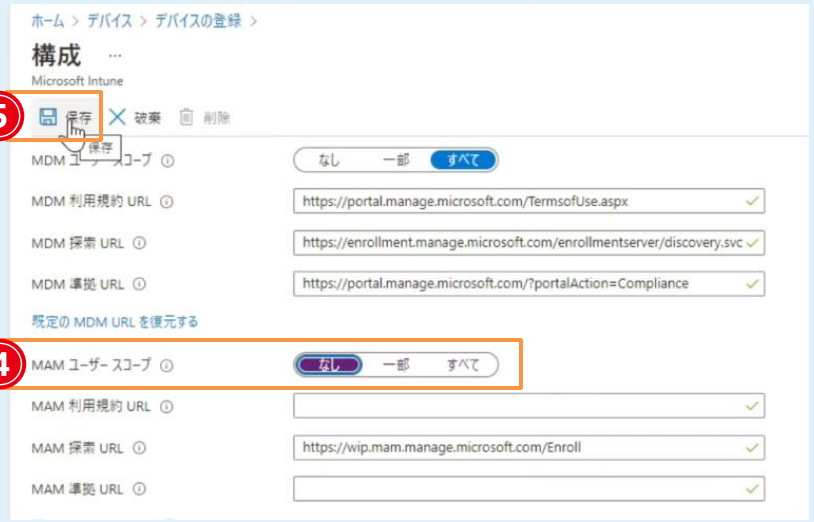
MAMのスコープから外す設定を行います
今回の設定では、MAMの対象から外すことで、Microsoft 365にアクセス可能となります

☑ デバイスを選択　☑ デバイスの登録を選択



☑ 自動登録を選択

☑ MAMユーザースコープをなしに変更　☑ 保存を選択



動画でチェックしたい方は[こちらより]
もしくはQRコードよりご確認ください

本日ご紹介した在宅勤務でも安全な機能が使えるプラン

TD SYNNEX

本日ご紹介したMicrosoft 365のサービスをお使いいただくには

スイートプラン

OfficeやOffice 365以外にもセキュリティ強化サービスが含まれたプラン

Microsoft 365 Business Premium
※既にAzure AD Premium Plan1が含まれます

Microsoft 365 E3
※既にEnterprise Mobility+securityE3が含まれます

Microsoft 365 E5
※既にEnterprise Mobility+securityE5が含まれます

中小企業様向けスイートプラン

Microsoft 365 Business Standard
※既にMicrosoft 365 Apps for Businessが含まれます

Microsoft 365 Business Basic

大規模ユーザーにも対応したプラン

Office 365 E1

Office 365 E5
※既にMicrosoft365 Apps for Enterpriseが含まれま

Office 365 E3
※既にMicrosoft365 Apps for Enterpriseが含まれます

お持ちのプランが不明な場合は、
販売店様までお問い合わせください!

オプションでプランを選択・追加できます！

セキュリティ系サービス スイートプラン

- Enterprise Mobility + Security E3
- Enterprise Mobility + Security E5

まとめ

在宅勤務時でも安心してMicrosoft 365を使ってもらいたい と思っている皆様に必見！

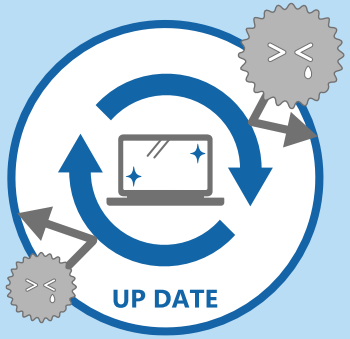
point

❶ 会社ルールを設定　　**❷ 運用ガイドラインを作成**　　**❸ 社内周知**

管理・制御が
できている場合

決められた
デバイスからのアクセス

もしもの時の
リモートワイプ



Windowsの
バージョンを管理

是非、**Microsoft Intune & Azure AD Premiumを使った**
Microsoft 365へ安心アクセスの導入をご検討ください！