中小企業向け設定解説資料
（Microsoft Teams Meeting）

Ver1.1（2024.03）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）
総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、Microsoft Teams Meeting（以後、単に Teams と記載）を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的としています。

(イ) 前提条件

本製品（Teams）のライセンス形態は無償ライセンスと Teams 及び複数の Office アプリケーション含む有償エディションが存在します（2023 年 11 月 7 日現在）。利用するライセンス形態により使用できる機能が異なります。**本資料は「Microsoft 365 Business Basic」ライセンスの利用を前提としています。**Teams 無料版（クラシック）を利用している場合は 2023 年 04 月 12 日に提供終了となったため、新しく提供される Teams 無料版にサインアップが必要です（ユーザデータ及びストレージは移行されないため再設定が必要です）。

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、第 4 章では利用者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。
4 利用者向け作業	対象のチェックリスト項目に対する利用者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2023 年 11 月 7 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-5 アクセス制御・認可 **オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。**	・ロビー機能の有効化	P.7
7-3 インシデント対応・ログ管理 **テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集する。**	・監査ログレポートの確認	P.10
9-1 アカウント・認証管理 **テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。**	・パスワード有効期限ポリシーの設定	P.13
9-2 アカウント・認証管理 **テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。**	・パスワード変更要求設定	P.15
9-4 アカウント・認証管理 **テレワークで利用する各システムへのアクセスには、多要素認証を求めるよう設定する。**	・多要素認証の有効化	P.17
10-1 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限は、業務上必要な最小限の人に付与する。**	・管理者権限の付与	P.19
10-2 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用する。**	・管理者ユーザーのパスワード	P.21
10-3 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用する。**	・管理者権限の管理	P.21

表３．チェックリスト項目と利用者向け作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-3　アクセス制御・認可 **オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。**	・ミーティング時の本人確認	P.22
3-4　アクセス制御・認可 **オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。**	・会議 URL の取り扱い	P.22
3-5　アクセス制御・認可 **オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。**	・不適切な参加者の退室	P.23
4-1　物理セキュリティ **テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。**	・第三者からの盗聴・のぞき見の対策	P.24
5-2　脆弱性管理 **テレワーク端末の OS やアプリケーションに対して最新のセキュリティアップデートを適用するよう周知する。**	・アプリケーションの最新化	P.24
6-1　通信暗号化 **Web メール、チャット、オンライン会議、クラウドストレージ等のクラウドサービスを利用する場合（特に ID・パスワード等の入力を求められる場合）は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。**	・HTTPS 通信の確認 ・サービス接続先の確認	P.25 P.25
8-5　データ保護 **オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。**	・ミーティング情報の件名に機密情報の記載禁止 ・ミーティング録画ファイルの削除	P.25 P.26
9-1　アカウント・認証管理 **テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。**	・パスワード強度	P.28
9-3　アカウント・認証管理 **テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合、それ以上のパスワード入力を受け付けないよう設定する。**	・パスワード入力制限	P.28

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1 チェックリスト 3-5 への対応

3-1-1　ロビー機能の有効化

ロビー機能により、ホストはミーティングに参加する参加者を制御することができます。
ロビーは、参加者を直接会議に参加させず、一旦ロビーに待機させ、主催者が参加を許可した場合にのみ、ミーティングに入室させる機能です。**想定していない参加者がミーティングに参加できないようにすることで、安全なミーティングを確保します**。

【手順①】
Teams 管理センター（https://admin.teams.microsoft.com）にログインするとミーティングに関連する設定画面が表示されます。

【手順②】

「会議」-「会議ポリシー」と進みポリシーの管理と進みます。

デフォルトで適用されているポリシーは「グローバル（組織全体の既定値）」になるため、ここではこちらのポリシーで変更します。対象のポリシーをクリックします。

【手順③】

次に「会議への参加とロビー」の設定項目を設定します。

以下のように設定を変更します。

- 匿名ユーザーが会議に参加できます：オフ
- ロビーをバイパスできるユーザー：組織内のユーザー（※1）
- ダイヤルインしている人はロビーをバイパスできる：オフ（※2）

※ 1：より厳しく制限したい場合は、全てユーザー（全員）を選択することもできます。

※ 2：ダイヤルインしている人とは Web 会議接続用の電話番号を使って参加するユーザーを示します。

最後に「保存」をクリックします。

以上でロビー機能を有効化するポリシーの設定が完了します。

- **注意事項**

  ポリシーの反映に関しては最大 24 時間のリードタイムが発生します。

  即時反映されませんのでご注意ください。

3-2 チェックリスト 7-3 への対応

3-2-1　監査ログ/レポートの確認

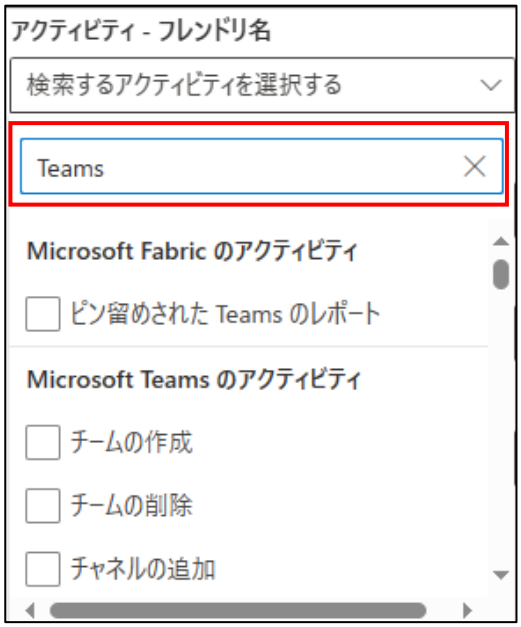
監査ログより、Teams 関連のアクティビティを確認することができます。**ユーザーの不正操作がないか確認することにより Teams のセキュアな運用を行うことができます。**

監査ログの確認

以下の手順で監査ログを確認します。

Microsoft Purview コンプライアンスの「ソリューション」の「監査」をクリックし、「検索」からアクティビティと開始日、終了日、ユーザー、ファイル、フォルダーまたはサイトを入力して監査ログを検索します。

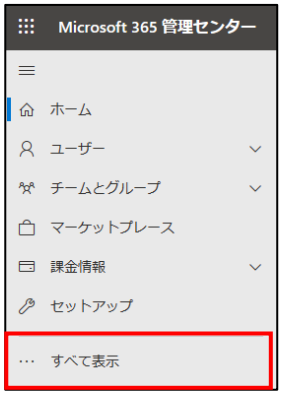
上記画面の「検索するアクティビティを選択する」をクリックし、「Teams」をキーワードに検索すると、Teams 関連のアクティビティを表示されます。確認したい項目にチェックし、ログを検索します。



ユーザー利用状況確認

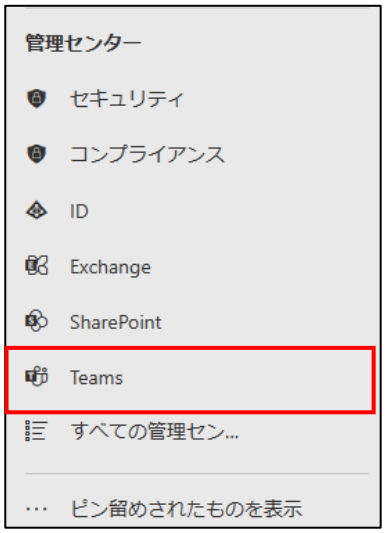
【手順①】

管理センターの「すべてを表示」をクリックします。



【手順②】

管理センターの「Teams」を開きます。



【手順③】

「分析＆レポート」の「使用状況レポート」をクリックし、「レポートの表示」から、レポートの種類と日付の範囲を選択します。その後、「レポートを実行」をクリックしてレポートを確認します。

以下は、レポートの種類を「Teams ユーザーの利用状況」で日付の範囲を過去 90 日間とした場合です。

3-3 チェックリスト 9-1 への対応

3-3-1　パスワード有効期限ポリシーの設定

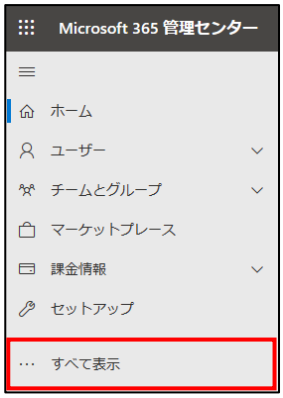
管理者は、ユーザーのパスワードの有効期限を設定することができます。デフォルトでは、パスワードの有効期限は 無期限に設定されています。最近の研究では、強制的なパスワードの変更はメリットよりデメリットの方が大きいことが強く示唆されています。パスワードの有効期限が短すぎると、パスワード強度の弱いパスワードやパスワードの再利用、または古いパスワードを使いまわすユーザーが多くなる可能性があります。

パスワードを無期限に設定する場合は、多要素認証を有効にすることを推奨します。

【参考】組織のパスワード有効期限ポリシーを設定します。
URL：https://docs.microsoft.com/ja-jp/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

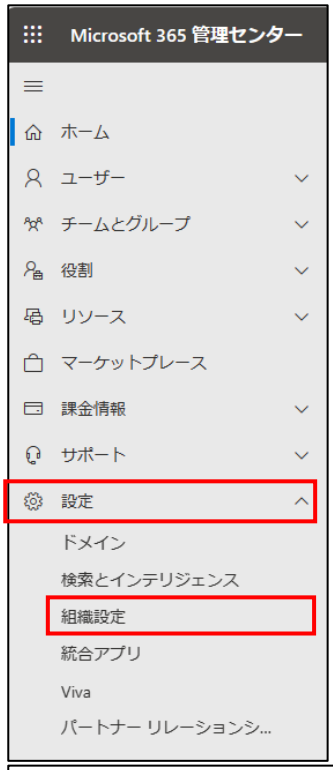
【手順①】

管理センターにアクセスし、「すべてを表示」をクリックします。



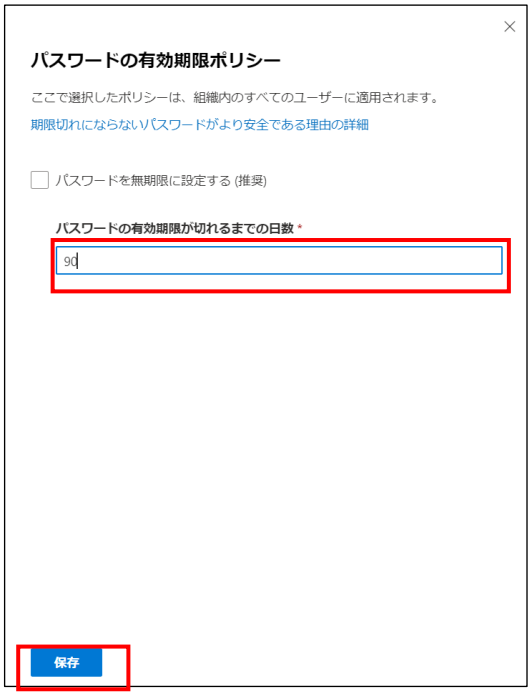
【手順②】

管理センターの「設定」の「組織設定」から「セキュリティとプライバシー」をクリックします。



【手順③】

「パスワードの有効期限ポリシー」でデフォルトの「パスワードを無期限に設定する」のチェックを外し、パスワードの有効期限が切れるまでの日数を入力後、「保存」をクリックすることで有効期限を変更することができます。



3-4 チェックリスト 9-2 への対応

3-4-1　パスワード変更要求設定

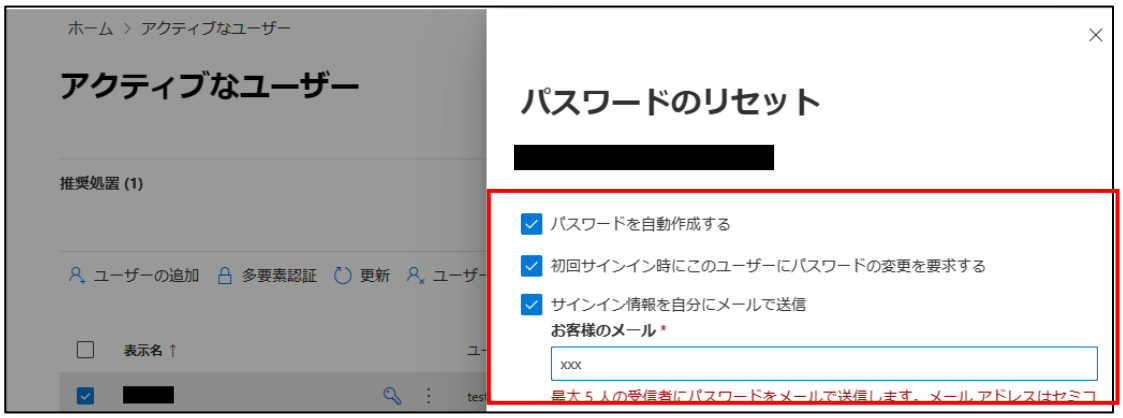
ユーザーアカウント発行時やパスワードをリセットする際に、「初回サインイン時にこのユーザーにパスワードの変更を要求する」にチェックを入れておくことで、ユーザーがサインイン時に管理者から知らされたパスワードでログイン後、パスワード変更を要求することができます。**これにより、ユーザーが初期パスワードやリセットしたパスワードを変更せずに使い続けることを防ぐことができます。**

【手順①】

管理センターにアクセスし、「ユーザー」の「アクティブなユーザー」からユーザーを選択し、「パスワードのリセット」をクリックします。

【手順②】

パスワードを自動生成する場合は、「パスワードを自動生成する」にチェックをいれたまま「パスワードのリセット」をクリックします。



パスワードを手動で作成する場合は、「パスワードを自動生成する」チェックを外し、パスワードを入力後、「パスワードのリセット」をクリックします。

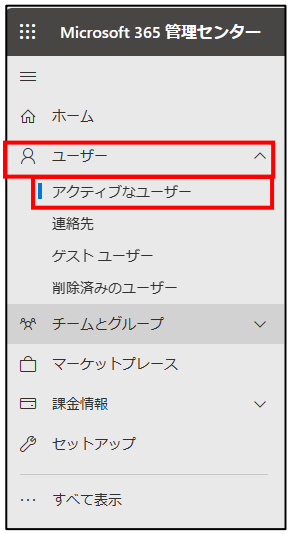
3-5 チェックリスト 9-4 への対応

3-5-1　多要素認証の有効化

多要素認証を有効化することにより、ログインするためにパスワードだけでなく SMS で受け取った一時的なコードなど追加の認証情報が求められるようになります。**多要素認証の設定によりパスワードが破られた場合でも、不正ログインを防ぐことができます。**

【手順①】

管理センターにアクセスし、「ユーザー」の「アクティブなユーザー」をクリックします。

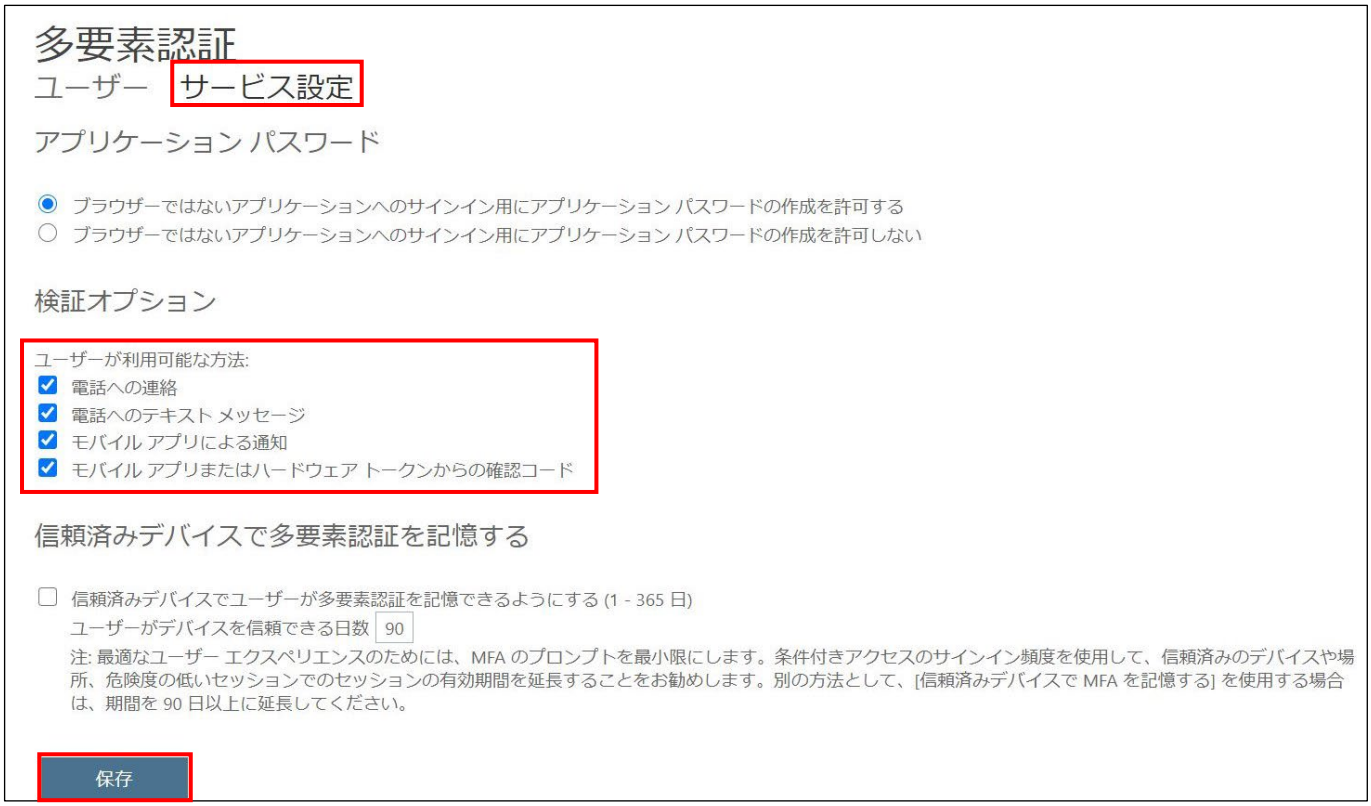


【手順②】

「多要素認証」をクリックすると、多要素認証の設定画面が開きます。

【手順③】

画面内の「サービス設定」をクリックします。検証オプションにはユーザーが利用可能な方法を指定し、保存します。「信頼済みデバイスで多要素認証を記憶する」を設定すると、信頼済みデバイスからのサインインの場合に多要素認証を省略することができます。

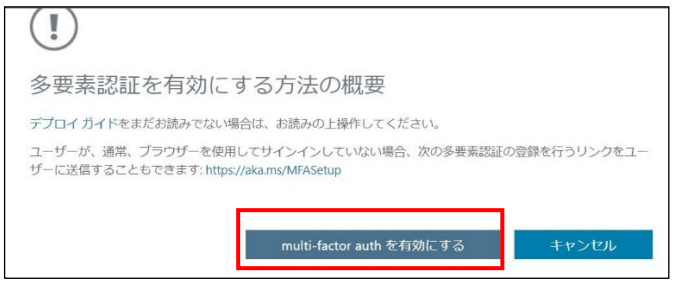


【手順④】

多要素認証の設定画面の「ユーザー」から多要素認証を有効化するユーザーを（一括）選択し、「quick steps」の「有効にする」をクリックします。

【手順⑤】

「multi-factor auth を有効にする」をクリックし、「更新が正常に完了しました」と表示されたら「閉じる」をクリックします。



参考情報：Azure AD Multi-Factor Authentication のデプロイを計画する
URL：https://docs.microsoft.com/ja-JP/azure/active-directory/authentication/howto-mfa-getstarted?redirectedfrom=MSDN#

3-6 チェックリスト 10-1 への対応

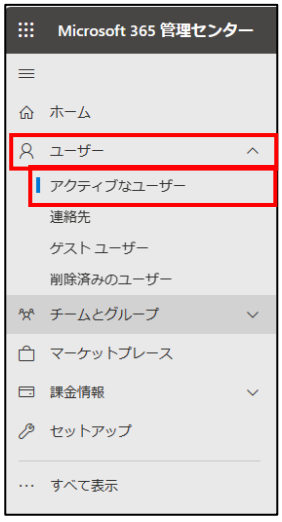
3-6-1　管理者権限の付与

管理者権限を付与するユーザーを限定することで、本製品の設定変更をできるユーザーを必要最小限に抑え、**悪意のあるユーザーにより、意図しない設定変更が行われるリスクを低減**することができます。

下記手順によりユーザーに管理者権限を付与することができます。

【手順①】

管理センターにアクセスし、「ユーザー」の「アクティブなユーザー」をクリックします。

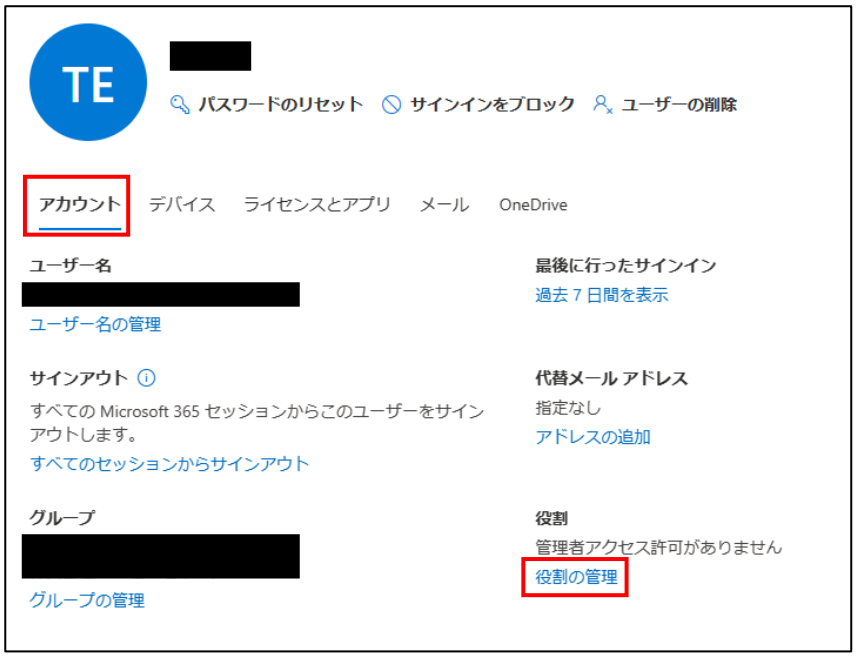


【手順②】

管理者権限を付与するユーザーを選択します。

【手順③】

「アカウント」-「役割」の「役割の管理」をクリックします。



【手順④】

「管理センターに対するアクセス許可」を選択します。Teams 管理者とする場合は「Teams 管理者」を選択し、全体管理者とする場合は「グローバル管理者」を選択します。

その他のアプリケーションの管理者として設定する場合は、目的に応じた役割を選択し、「変更の保存」をクリックします。

3-7 チェックリスト 10-2 への対応

3-7-1　管理者ユーザーのパスワード強度

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「中小企業等向けテレワークセキュリティの手引き」のP.96 に記載の「パスワード強度」を参考に設定することを推奨します。

【参考】Microsoft 365 パスワードに関するパスワード ポリシーの推奨事項
URL：https://docs.microsoft.com/ja-jp/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

3-8 チェックリスト 10-3 への対応

3-8-1　管理者権限の管理

作業ミスによるシステムやデータへの悪影響を防ぐために、**一般ユーザーのアカウントを作成し、普段はそのアカウントを利用、管理者用アカウントの利用は最小限に留める**ことを推奨します。

４利用者向け作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

４-１ チェックリスト 3-3 への対応

４-１-１　　ミーティング時の本人確認

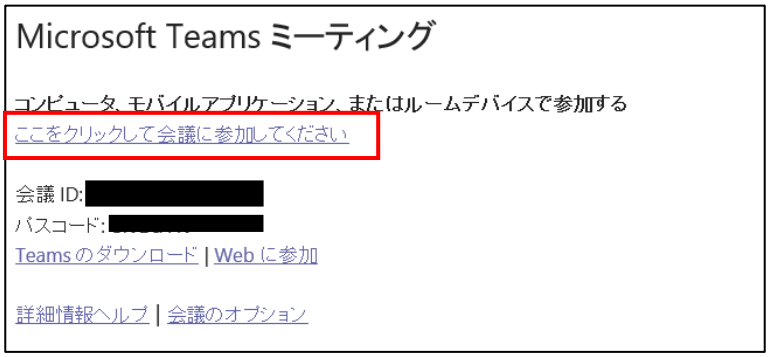
ミーティングは、特別なアクセス制御を行わない限り**誰でも参加することができます**。
また、ミーティング参加時の参加者としての表示名は、参加者側で自由に設定ができます。
なりすました不正ユーザー（※）が参加していないか確認するために、ミーティング開始時や途中参加者が入った場合はカメラの映像とマイクを有効化させ、映像と音声で本人確認することを推奨します。

※　：なりすました不正ユーザーによる機密情報の取得イメージ

４-２ チェックリスト 3-4 への対応

４-２-１　　会議 URL の取り扱い

会議に対してパスワードを設定できないため、会議 URL が漏洩した場合は不正なユーザーが URL にアクセスし簡単に会議室（またはロビー）へ入室することができてしまいます。
このため、不適切な人に会議 URL や会議 ID/PW を送付しないよう注意することが重要です。

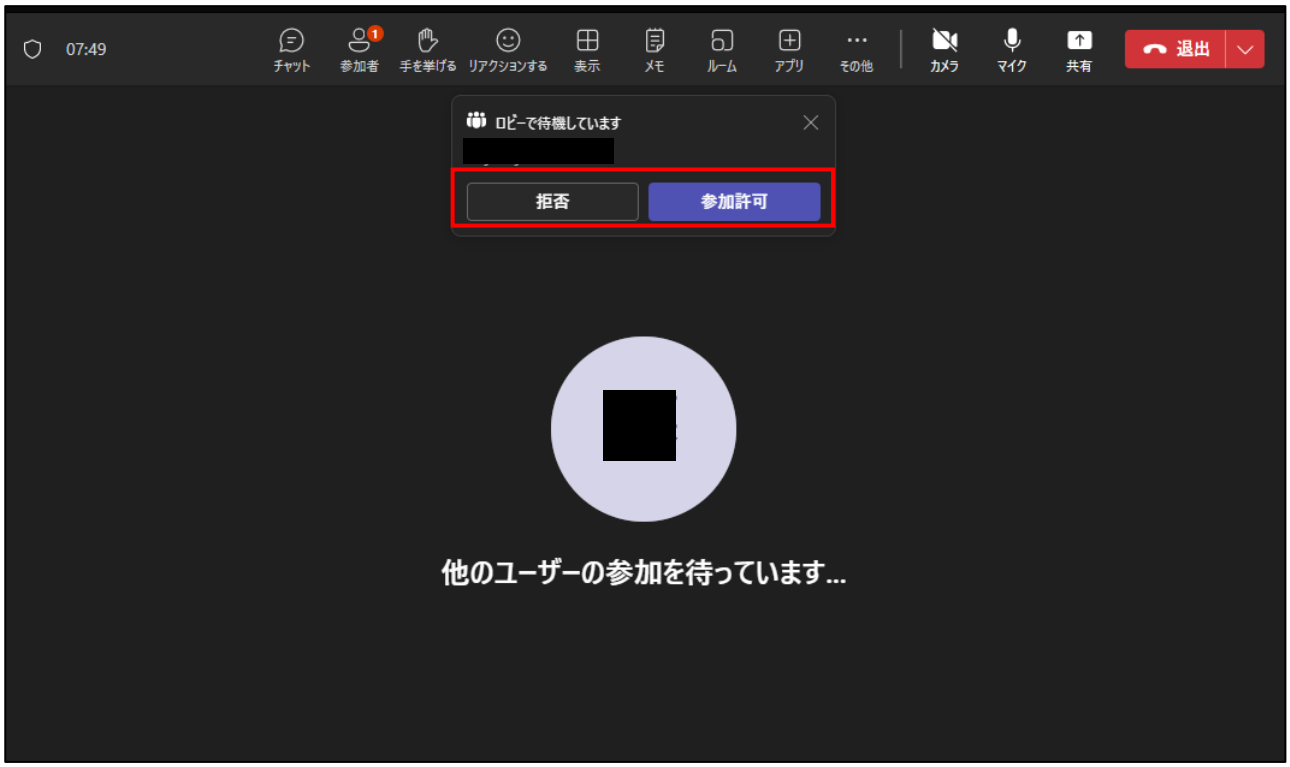


4-3 チェックリスト 3-5 への対応

4-3-1　不適切な参加者の退室

Teams のロビーには、会議 URL を知っていれば、**誰でも入室できてしまいます。**そのため主催者は、ロビー機能を利用し待機している参加者名を確認し、予め招待している参加者のみ許可するようにします。

ロビーの参加者を許可するにはミーティング画面の上部に出てくる「ロビーで待機しています」の表示の「参加許可」をクリックします。
対象メンバーでなければ「拒否」をクリックするとロビーから強制退場となります。



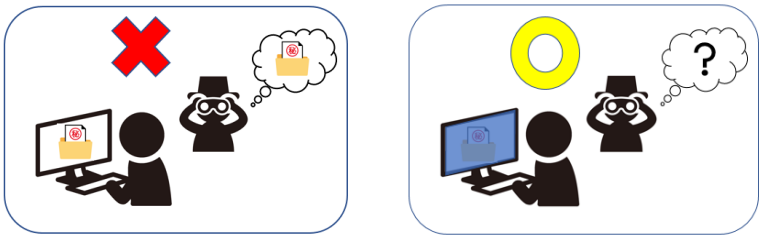
- **注意事項**

悪意のあるユーザーは名前をなりすまして参加する可能性があります。
可能であればミーティング冒頭で参加者のカメラ機能を有効化して顔や音声で本人確認を実施することを推奨します。

4-4 チェックリスト 4-1 への対応

4-4-1　第三者からの盗聴・のぞき見の対策

オフィス外で利用する場合は、第三者から盗聴・盗み見されないように注意する必要があります。端末上に投影されている会議資料などがのぞき見されないように**のぞき見防止フィルタを利用する**、会議音声が外部に漏れないようにイヤホンを利用する、など利用シーンにおいた対策が必要です。



4-5 チェックリスト 5-2 への対応

4-5-1　アプリケーションの最新化

製品提供元からリリースされている最新バージョンのアプリケーションを利用します。最新バージョンを利用することは、アプリケーションの脆弱性をついたサイバー攻撃に対して有効な対策となりますので、定期的にアップデートがないか確認をすることを推奨します。

4-6 チェックリスト 6-1 への対応

4-6-1　HTTPS 通信の確認

ユーザーがアクセスする Teams Meeting の Web アプリ版への通信は基本的に HTTPS で暗号化されています。

4-6-2　サービス接続先の確認

Teams Meeting の URL として、第三者から共有されたものについては、**不正なアクセス先（Teams のドメインではないケース等）でないことを確認する**ようにします。

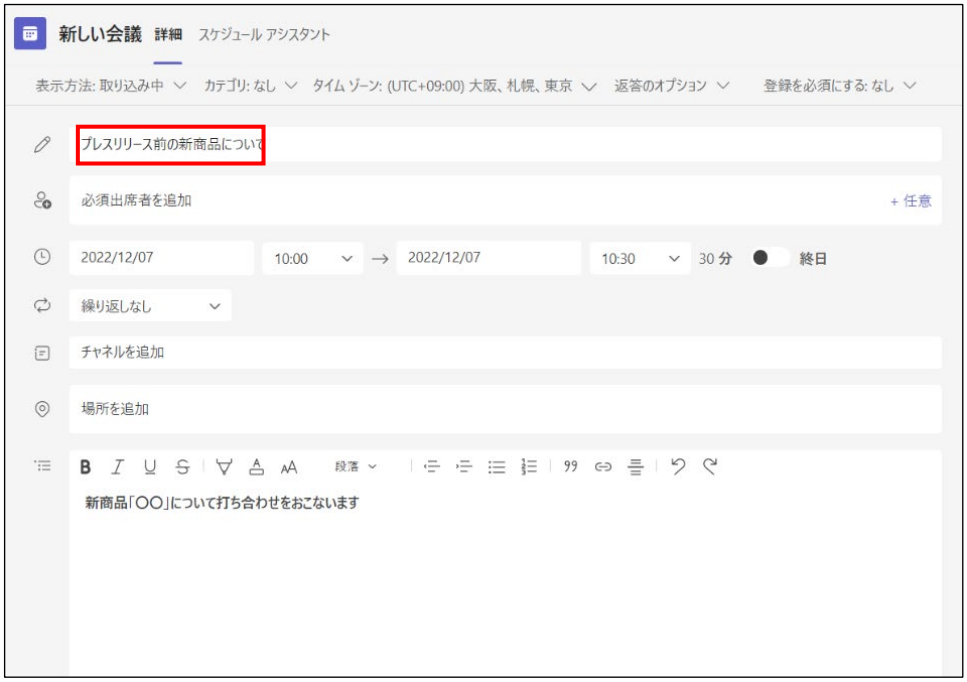
また、**使用するアカウントが、個人アカウントではなく、業務利用アカウントを使用していることを確認し、Teams Meeting にアクセスします。**

4-7 チェックリスト 8-5 への対応

ここでは、**ミーティング利用時に利用者（主催者）が注意すべき事項と設定**について記載します。

4-7-1　ミーティング情報の件名に機密情報の記載禁止

会議名などに**機密情報が含まれている場合、間違った相手に招待メールを送信してしまうと情報漏洩してしまいます**。Teams ではミーティングをスケジュールする際に、件名と議題を記載する項目がありますが、機密情報を記載せずに参加者同士が分かる内容で記載することを推奨します。



4-7-2　ミーティング録画ファイルの削除

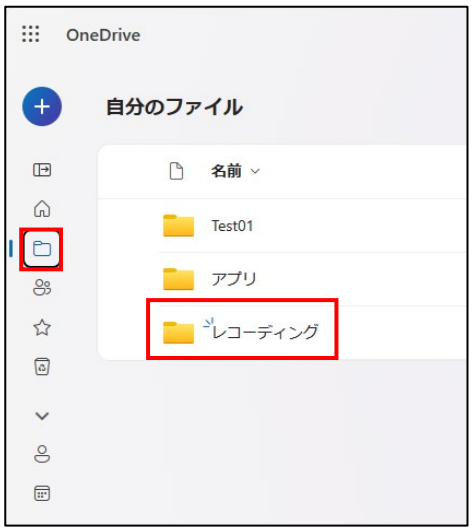
Teams の会議で録画したビデオは OneDrive（チャネル以外の会議の場合）または SharePoint（チャネル会議の場合）に保管されます。不要になった録画ファイルを削除することで、**悪意のあるユーザーによる持ち出しやサイバー攻撃を受けた際の機密情報漏洩のリスクを低減することができます**。

OneDrive の場合

以下の手順でビデオを削除します。

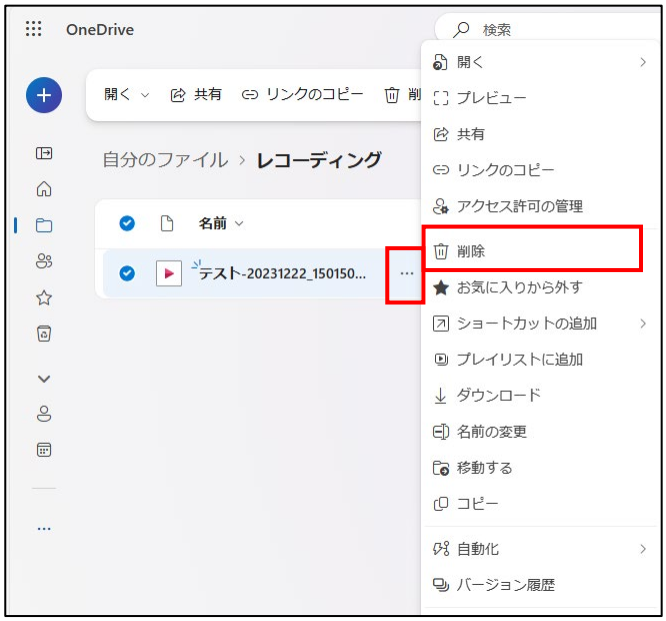
【手順①】

OneDrive にログインし、自分のファイル内の「レコーディング」をクリックします。



【手順②】

「レコーディング」内の該当の動画ファイルの「その他アクション（…）」をクリック後、「削除」を選択します。



【手順③】

該当の動画ファイルが削除されているか確認します。

SharePoint の場合

以下の手順でビデオを削除します。

【手順①】

SharePoint にログインし、ドキュメント内の「Recordings」をクリックします。

【手順②】

「Recordings」内該当の動画ファイルの「その他アクション（…）」をクリック後、「削除」を選択します。

上記のようにポップアップが表示されるので「削除」をクリックすると削除されます。

4-8 チェックリスト 9-1 への対応

4-8-1　　パスワード強度

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「中小企業等向けテレワークセキュリティの手引き」の P.96 に記載の「パスワード強度」を参考に設定することを推奨します。

【参考】パスワード ポリシーの推奨事項
URL：https://docs.microsoft.com/ja-jp/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

4-9 チェックリスト 9-3 への対応

4-9-1　　パスワード入力制限

不正なパスワードで**サインインに 10 回失敗**するとユーザーは **1 分間ロックアウト**されます。最初は 1 分間ですが、その後に**サインインの失敗続くと、より長い時間ロックアウト**されます。