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）関連資料

# 設定解説資料
# （Exchange Online）

**ver1.0**（2023.07）

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、Exchange Online 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

本製品のライセンス形態は Exchange Online 単体の有償プランと Exchange Online 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（2022 年 11 月 1 日現在）。利用するライセンス種類により使用可能な機能が異なります。**本資料では「Microsoft 365 Business Basic」ライセンスの利用を前提**としています。

(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、2022 年 11 月 1 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 |
|---|---|---|
| **2-2 マルウェア対策**<br>**不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。** | ・迷惑メール対応と除外設定 | P.6 |
| **7-3 インシデント対応・ログ管理**<br>**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。** | ・レポート/監査ログの確認 | P.10 |
| **9-1 アカウント・認証管理**<br>**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**<br>**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**<br>**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**<br>**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**<br>**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。** | ・管理者権限アカウントのパスワード | P.21 |
| **10-3 特権管理**<br>**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 |
|---|---|---|
| **6-1　通信暗号化**<br>**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<br>・サービス接続先の確認 | P.22<br>P.22 |
| **9-1　アカウント・認証管理**<br>**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。** | ・パスワード要件 | P.23 |
| **9-2　アカウント・認証管理**<br>**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。** | ・初期パスワード設定変更 | P.23 |
| **9-3　アカウント・認証管理**<br>**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.25 |
| **9-4　アカウント・認証管理**<br>**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。** | ・多要素認証の設定 | P.25 |

# 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 2-2 への対応

### 3-1-1　　迷惑メール対応と除外設定

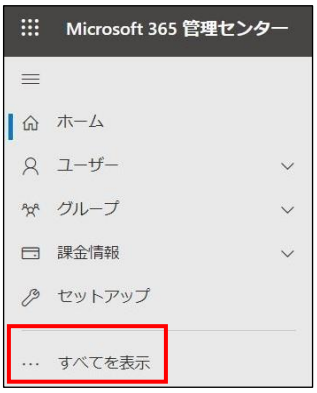
迷惑メールの除外設定を行うことで、**ユーザーが受信する不審メールや迷惑メールを抑制することができ、メールからのマルウェア感染リスクを低減させることができます**。また、不審メールを開封しない、不審メール内記載の URL をクリックしない、不審メールの添付ファイルを開かない、などをユーザーへ継続的に注意喚起することで、**ユーザーの不審メールに対する意識を高めマルウェア感染の被害のリスクを低減する**ことが見込めます。

#### 迷惑メール等から保護する設定

不審なメールを受信した際に自動的に除外する機能を有効化します。

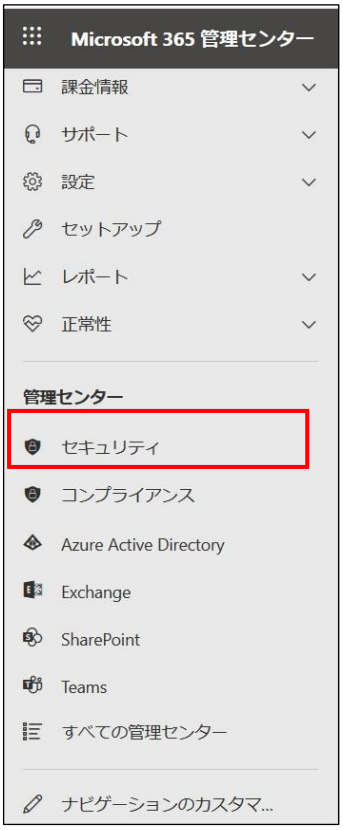
**【手順①】**

Microsoft 365 管理センターの「すべてを表示」をクリックします。



**【手順②】**

「セキュリティ」をクリックし、Microsoft 365 Defender のページを開きます。




**【手順③】**

「メールとコラボレーション」-「ポリシーとルール」-「脅威ポリシー」をクリックします。

**【手順④】**

テンプレート化されたポリシーから「既定のセキュリティポリシー」を開きます。


**【手順⑤】**

例として標準的な保護を適用します。トグルバーの「標準的な保護はオンです」が有効化されていることを確認し、「保護設定を管理する」をクリックします。

**【手順⑥】**

Exchange Online Protection の適用先を選択し、「次へ」をクリックします。

※　後続の手順として、「Defender for office365 連携」と「なりすまし防止」に関して表示された場合は、同様に適用範囲を指定します。


**【手順⑦】**

「変更を確認し確定する」画面になるので、「確定」をクリックし、「完了」をクリックします。

## 3-2　チェックリスト 7-3 への対応

### 3-2-1　　レポート/監査ログの確認

監査ログを有効にすることで、ユーザーや管理者の Exchange メール関連のアクティビティ履歴を確認することができます。**ユーザーが不正アクセス/不正操作をしていないか確認することにより Exchange Online 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

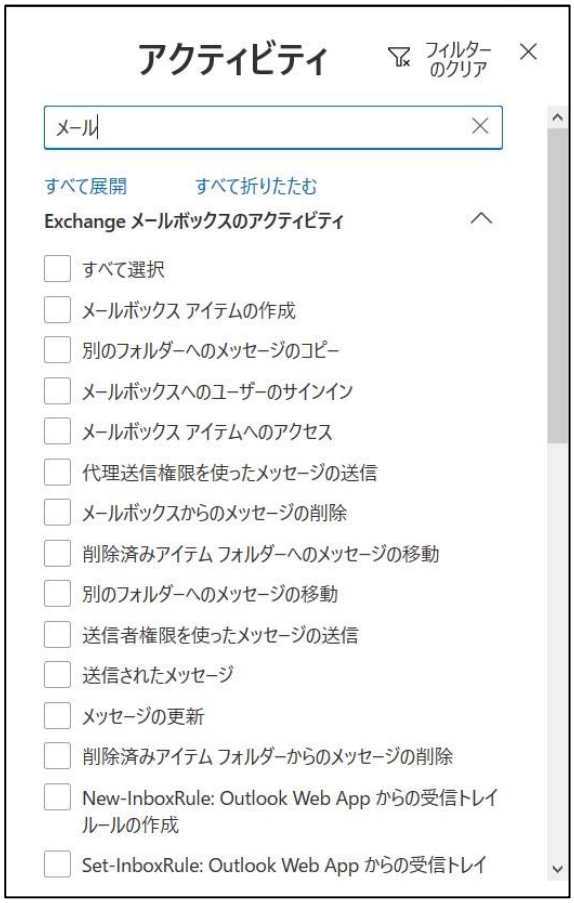
以下の手順で監査ログを確認します。

**【手順】**

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。


Microsoft コンプライアンスセンター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。

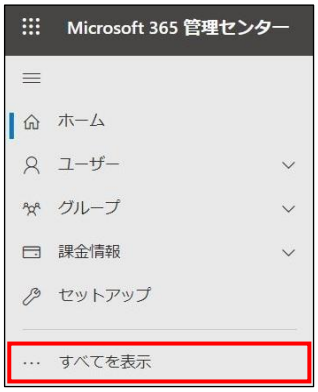
以下、Exchange メール関連のアクティビティに絞る場合です。上記画面「すべてのアクティビティを表示」をクリックし、「メール」をキーワードに検索すると、メール関連のアクティビティが表示されます。確認したい項目にチェックし、ログを検索します。




## レポート－メールフロー利用状況確認

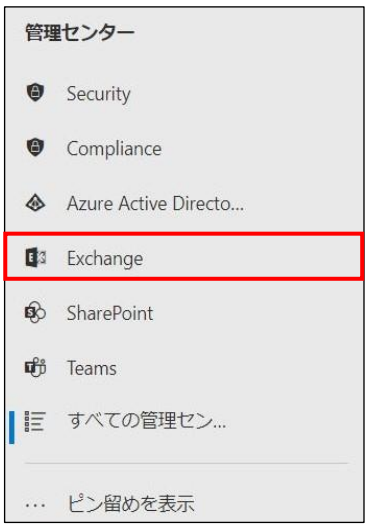
**【手順①】**

管理センターの「すべてを表示」をクリックします。



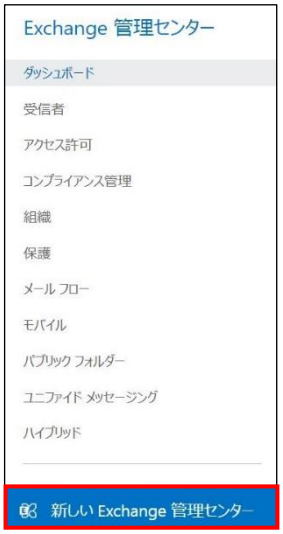
**【手順②】**

「Exchange」を開きます。




**【手順③】**

「新しい Exchange 管理センター」をクリックします。



**【手順④】**

「レポート」の「メールフロー」を開き、各種レポートの名前をクリックし、レポートを参照することができます。


## 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

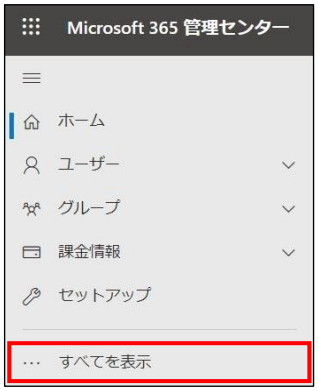
管理者は、ユーザーのパスワードの有効期限を設定することができます。デフォルトでは、パスワードの有効期限は 90 日に設定されています。最近の研究では、強制的なパスワードの変更はメリットよりデメリットの方が大きいことが強く示唆されています。パスワードの有効期限が短すぎると、パスワード強度の弱いパスワードやパスワードの再利用、または古いパスワードを使いまわすユーザーが多くなる可能性があります。

**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

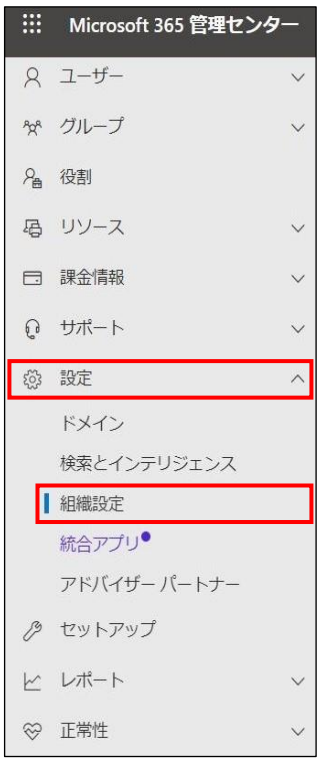
**【手順①】**

管理センターにアクセスして、「すべてを表示」をクリックします。



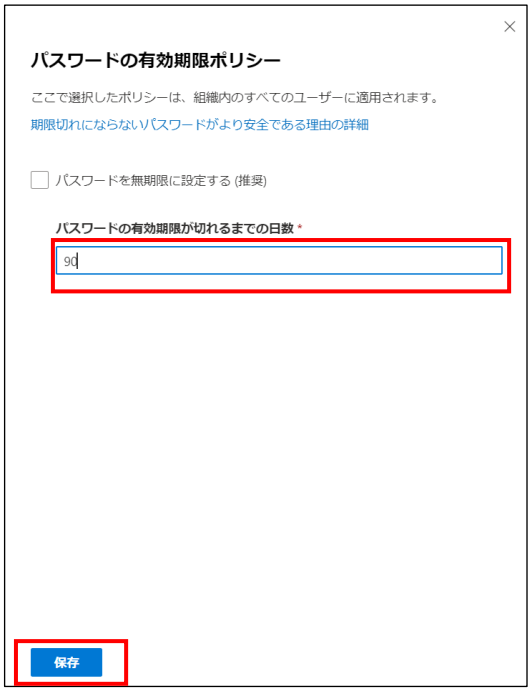
**【手順②】**

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」でパスワードの有効期限が切れるまでの日数（デフォルト 90 日）と保存することで有効期限の編集ができます。



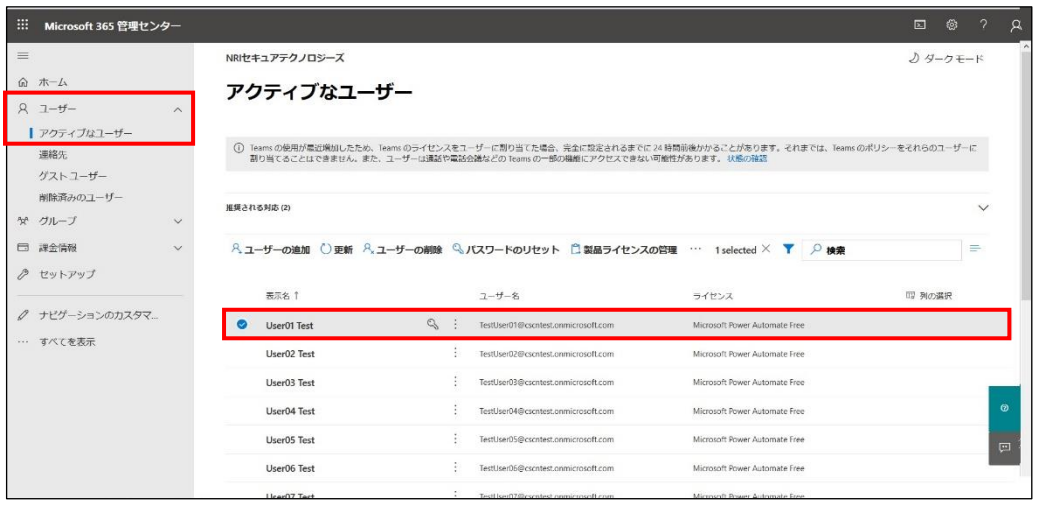

## 3-4　チェックリスト 9-2 への対応

### 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。**

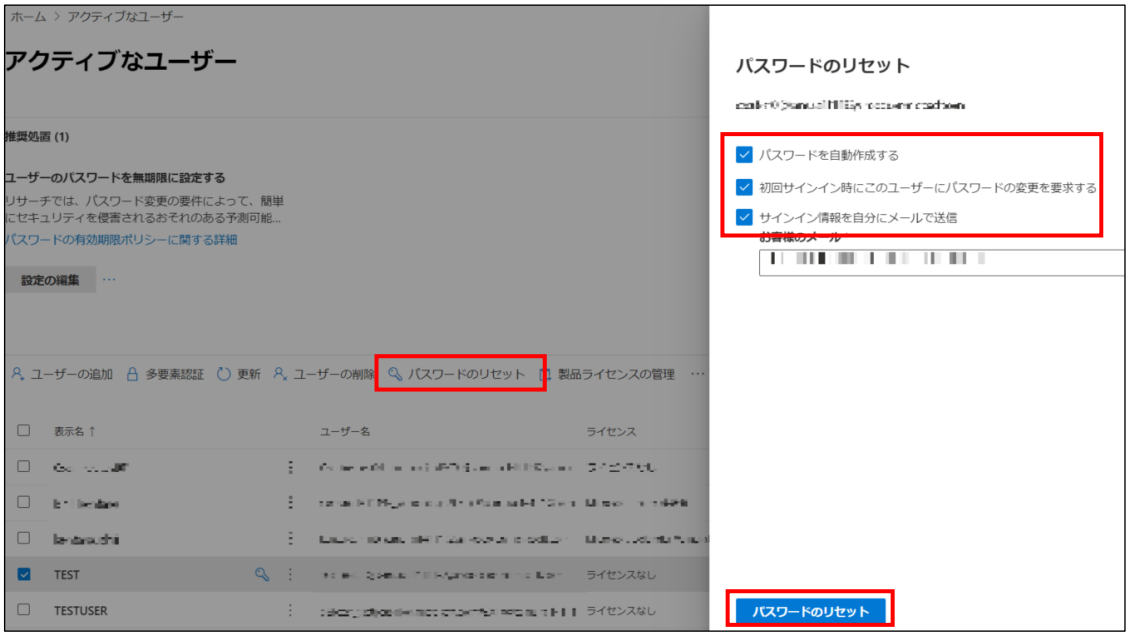
**【手順①】**

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」-「パスワードのリセット」からユーザーを選択します。

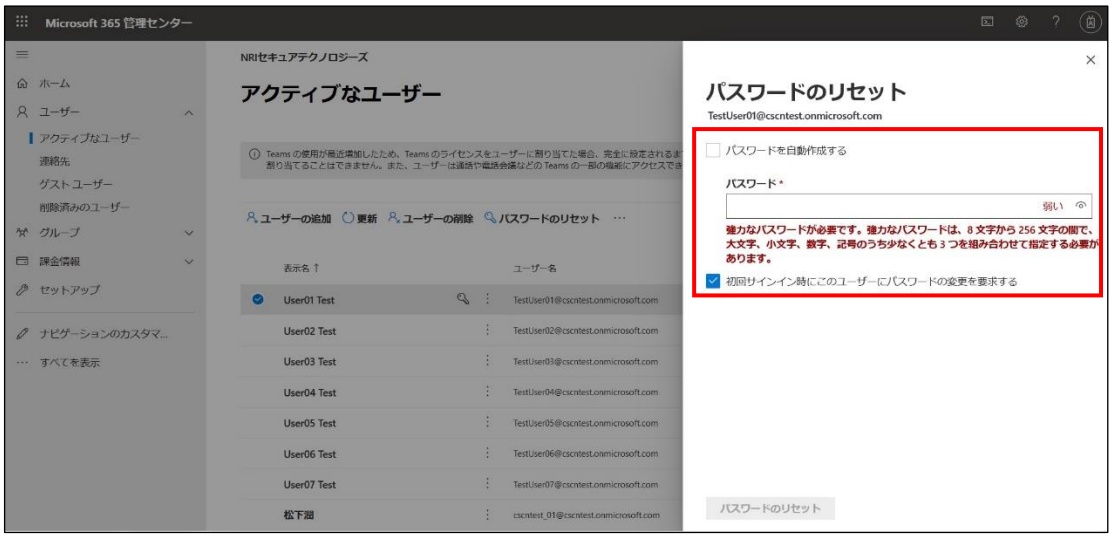


**【手順②】**

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。




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。



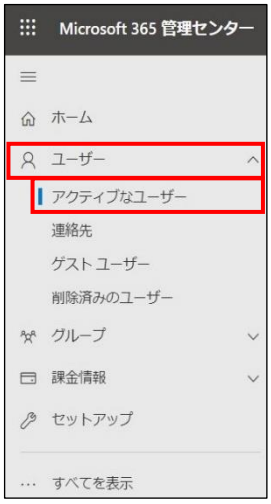
## 3-5　チェックリスト 9-4 への対応

### 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て、「ユーザー」の「アクティブなユーザー」をクリックします。

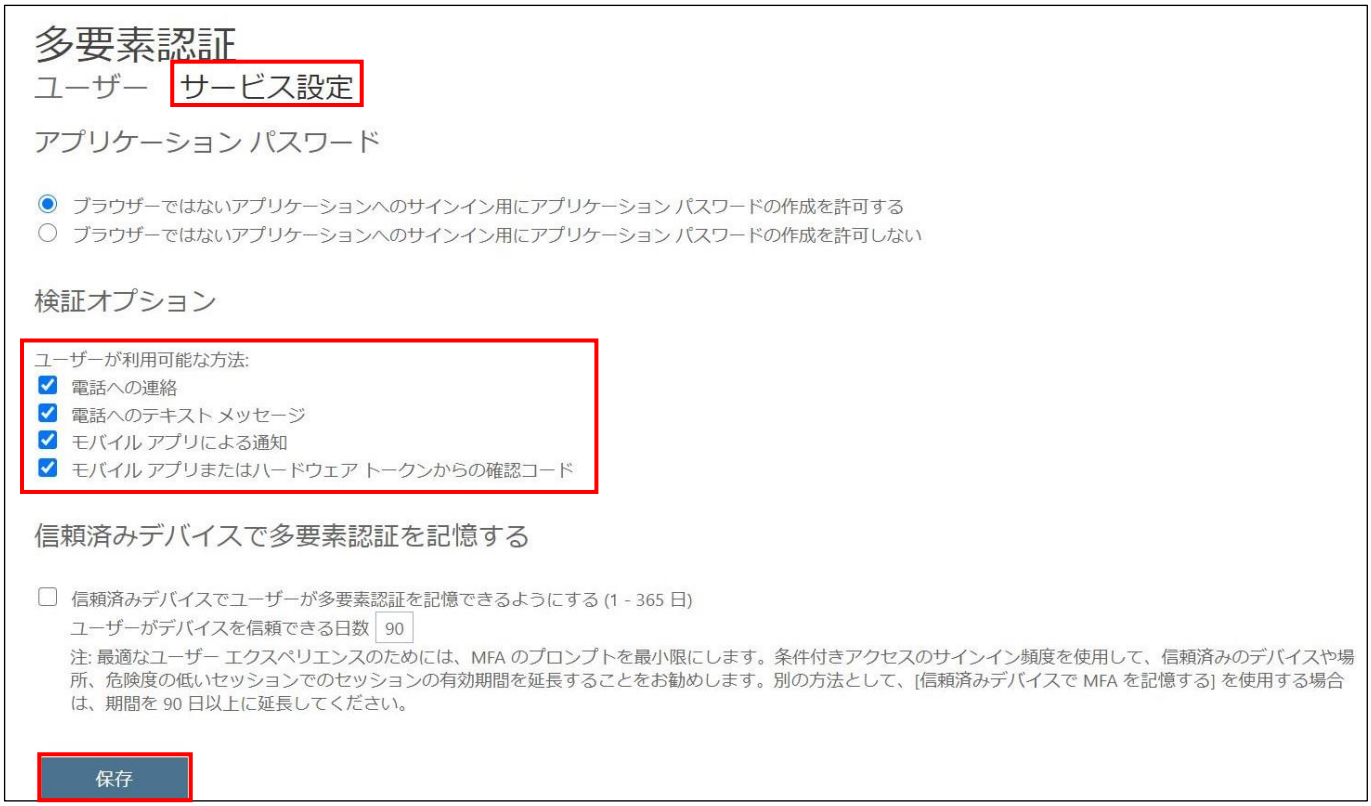



**【手順②】**

「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

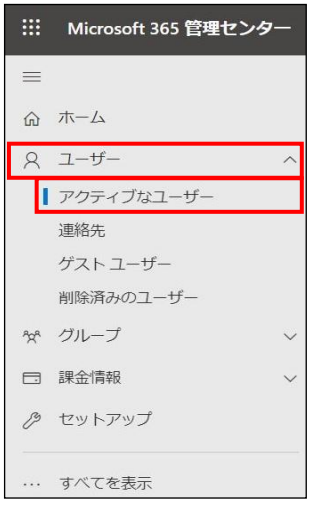
### 3-6-1　　管理者権限の付与

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て、「ユーザー」の「アクティブなユーザー」をクリックします。

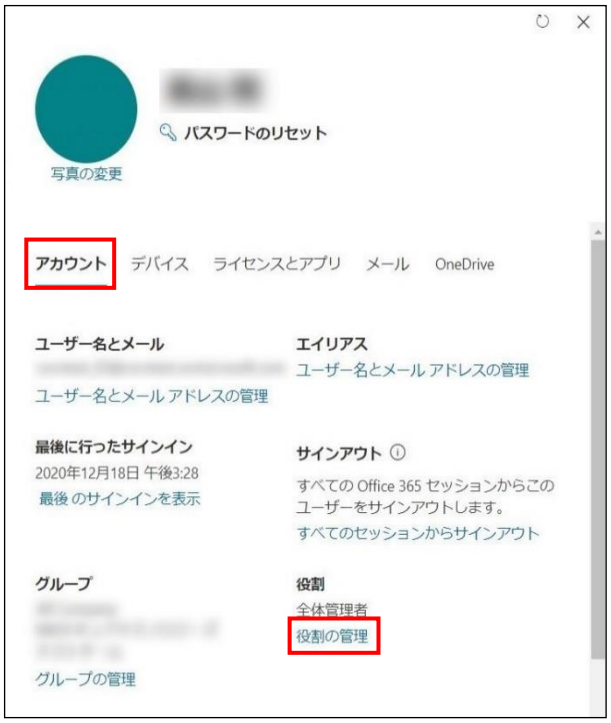


**【手順②】**

管理者権限を付与するユーザーを選択します。


**【手順③】**

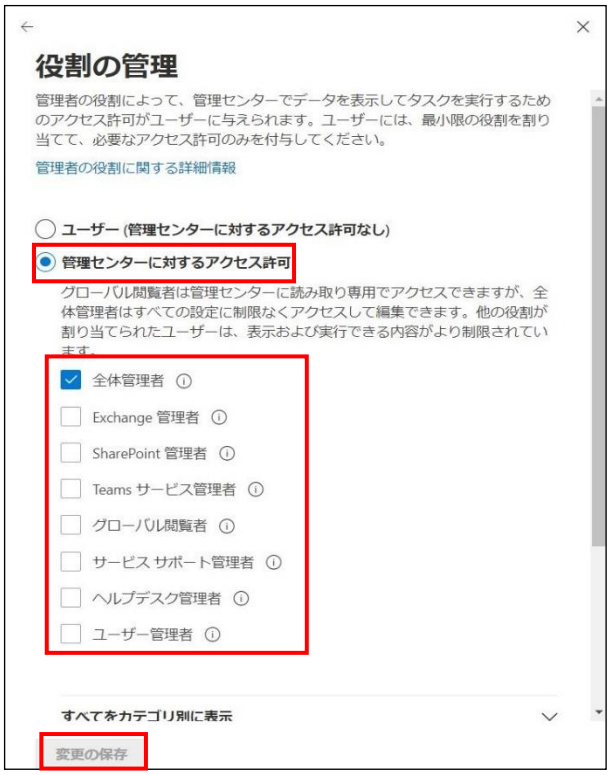
「アカウント」-「役割」の「役割の管理」をクリックします。



**【手順④】**

「管理センターに対するアクセス許可」にチェックを入れ、Exchange 管理者とする場合は「Exchange 管理者」を選択し、全体管理者とする場合は「全体管理者」を選択します。

その他のアプリケーションの管理者も設定する場合は、目的に応じた管理者の役割を選択し、「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　　管理者権限アカウントのパスワード強度

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】安全なパスワードを作成してアカウントのセキュリティを強化する
URL：https://support.google.com/accounts/answer/32040?hl=ja

## 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 6-1 への対応

### ４-１-１　HTTPS 通信の確認

ユーザーがアクセスする Exchange Online の Web アプリ版の Outlook on the web への通信は基本的に HTTPS で暗号化されています。

### ４-１-２　サービス接続先の確認

Outlook on the web 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（Exchange Online 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、Outlook on the web にアクセスします。**

## 4-2　チェックリスト 9-1 への対応

### 4-2-1　　パスワード要件

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

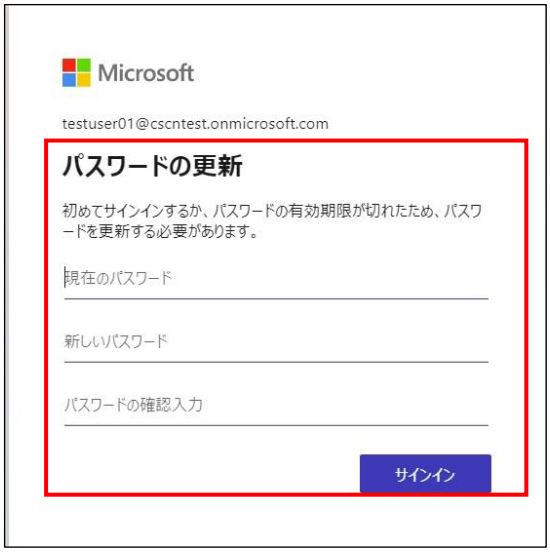
## 4-3　チェックリスト 9-2 への対応

### 4-3-1　　初期パスワード設定変更

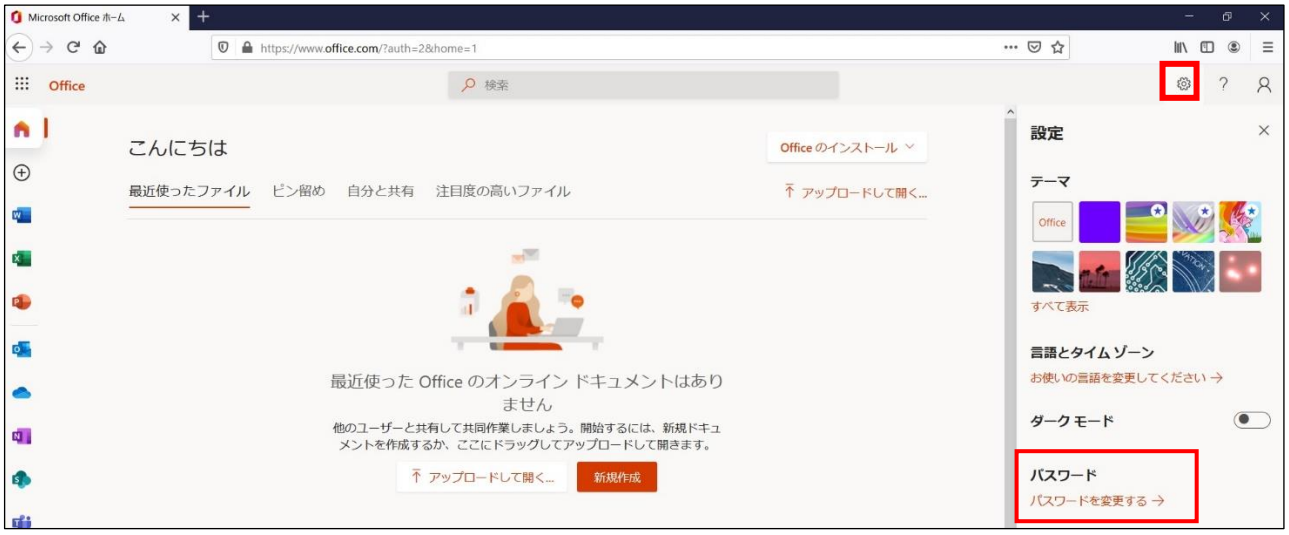
初期パスワードは、誰が把握しているかわからないため、速やかにパスワード要件を満たすものに変更することで、**悪意のある第三者から不正アクセスされるリスクを低減することができます。**

**【手順】**

初回ログインした際に「パスワードの更新」画面に遷移した場合は、指示に従いパスワードを変更します。

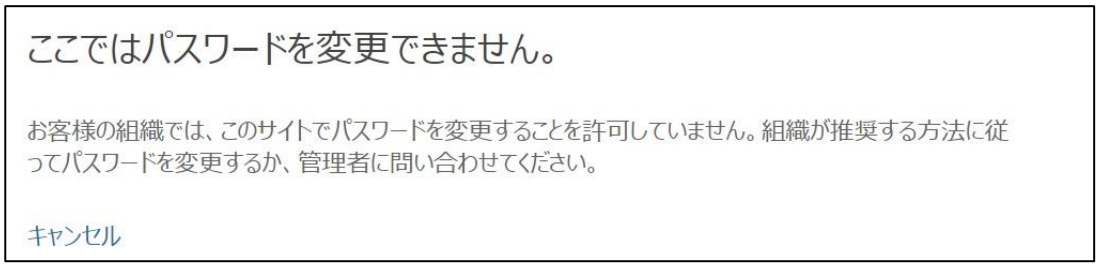


初回ログイン時にパスワードの更新画面に遷移しない場合は、Microsoft Office ホーム（https://www.office.com/?auth=2）より、右上の「設定」（歯車アイコン）をクリックし、「パスワードを変更する」から変更します。





職場によっては、上記手順でパスワード変更を許可していない組織もありますので、その場合は組織が推奨する方法に従ってパスワード変更を実施してください（許可されていない場合、以下のような画面になります）。



## 4-4　チェックリスト 9-3 への対応

### 4-4-1　　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。

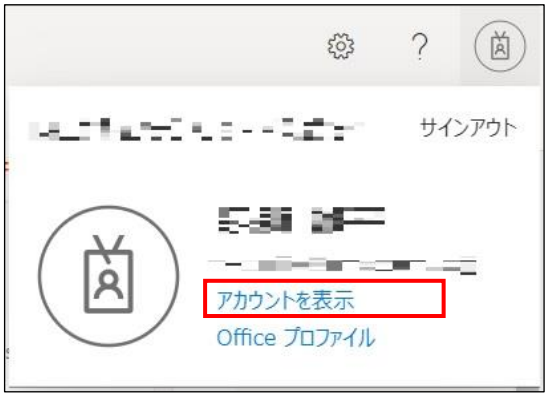
## 4-5　チェックリスト 9-4 への対応

### 4-5-1　　多要素認証の設定

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】**

右上の「マイアカウント」の「マイアカウントの表示」をクリックします。



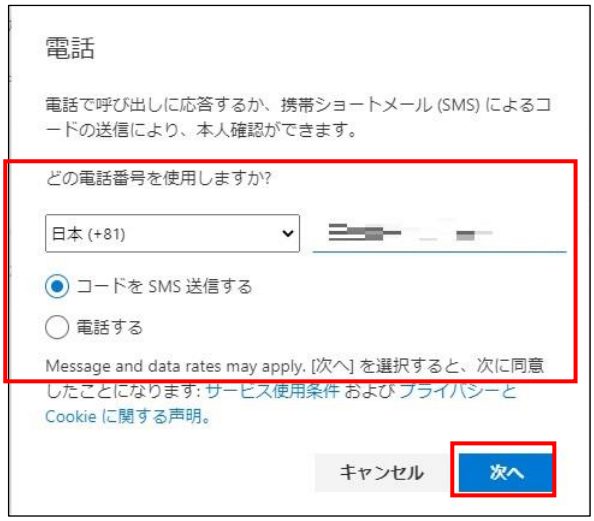
**【手順②】**

「セキュリティ情報」の「方法の追加」から認証方法を選択し、画面の説明に沿って設定を行います。追加できる方法は、所属組織によって異なるため、所属組織の指示に従って追加する方法を選択します。

認証アプリを方法として追加する場合は、スマートフォンが必要です。

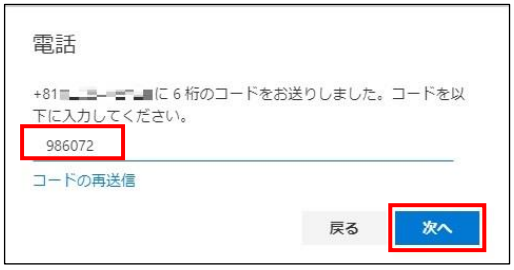

**【手順③】**

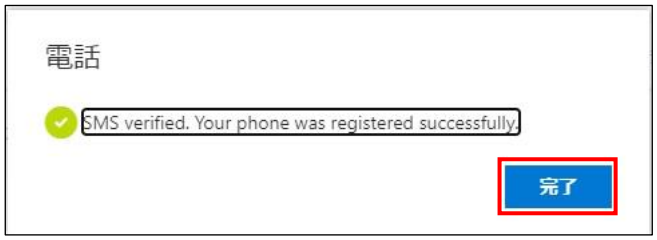
手順②で「電話」を選択した場合、携帯番号を入力して、「コードを SMS に送信する」か「電話する」のいずれかにチェック後、「次へ」をクリックします。



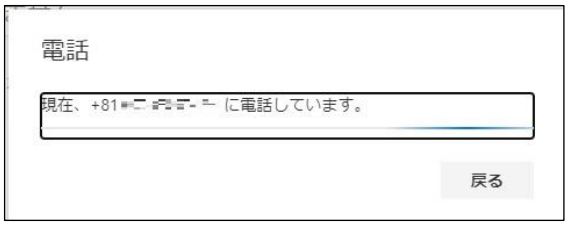
**【手順④】**

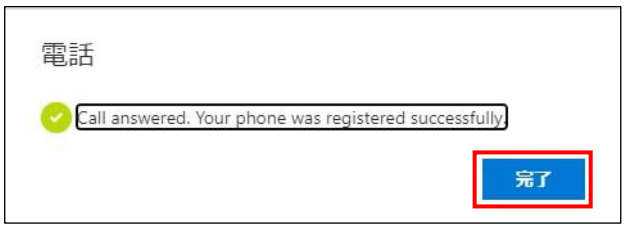
手順③で「コードを SMS に送信する」を選択した場合、指定した携帯番号に送られてくる認証コードを入力し、「次へ」をクリック後、「完了」をクリックします。




手順③で「電話する」を選択した場合、指定した電話番号に電話がかかってくるので、指示に従って操作を行います。操作完了後、下記右側の画面に遷移するので、「完了」をクリックします。



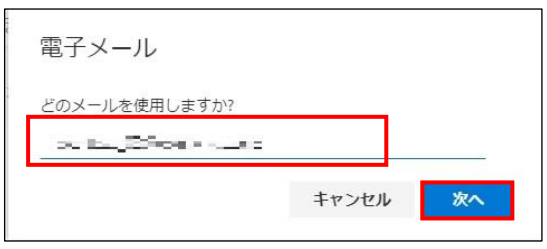



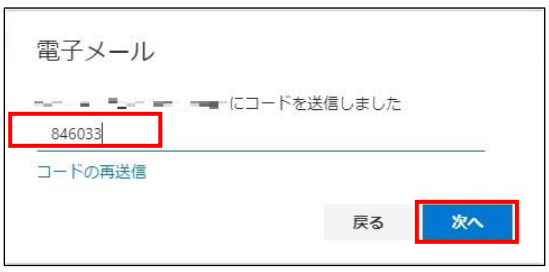

＜その他の追加方法＞

手順②で「代替の電話」または「会社電話」を選択した場合は、「電話する」のみとなります。


手順②で「電子メール」を選択した場合、指定したメールアドレスに送られてくる認証コードを入力後、「次へ」をクリックします。

※　会社のメールアドレスは使用できませんので、別のメールアドレスを使用する必要があります。



【参考】Azure AD Multi-Factor Authentication のデプロイを計画する - 認証方法を計画する

URL: https://docs.microsoft.com/ja-JP/azure/active-directory/authentication/howto-mfa-getstarted?redirectedfrom=MSDN#plan-authentication-methods