RAS 二要素認証簡易設定ガイド

21.1

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
スイス
Tel: + 41 52 672 20 30
www.parallels.com/jp

目次

はじめに **4**
本ガイドの目的 4
注意事項 4
適用範囲 4
表記規則 4

概要 **5**
RAS 二要素認証とは 5

検証環境の構成 **8**

構築手順 **8**
事前準備 8
多要素認証の設定（Google Authenticator の場合） 9
多要素認証の設定（Email の場合） 17
利用者側の設定（Google Authenticator の場合） 22
参考情報 Web からアクセスした場合の QR コード画面 30
参考情報 iPad からアクセスした場合の QR コード画面 31
利用者側の設定（Email の場合） 34

はじめに

本ガイドの目的

本ガイドは、Parallels® Remote Application Server (以降 RAS) の評価を目的に、初めて環境を構築されようとしているお客様や、販売店のエンジニア様に、シンプルなシステム構成で構築を完了し、RAS のリモート アクセスをお試しいただき体験いただくことを目的としております。

RAS 管理者ガイド (日本語) を、弊社 Web サイトに公開しておりますが、公開資料を補足する内容となっております。ぜひ、RAS 製品のシンプルで、かつ操作性の良いリモート アクセスを評価いただければ幸いです。

RAS 管理者ガイドを含むマニュアルの公開ページ
https://www.parallels.com/jp/products/ras/resources/

注意事項

- 本ガイドで紹介した仮想ネットワークおよび仮想サーバー等の導入に関しては自己責任での利用をお願いいたします。
- 本ガイドで示す環境構築および運用手順の実行に関しては、所属する組織等のセキュリティポリシーに必ず従ってください。
- 本ガイドに記載されている画面例、URL 等はガイド記載時のものとなるため、画面仕様が実際の画面とは異なることがありますのでご注意ください。
- 本ガイドに記載されている内容は、改善のため予告なしに変更される場合があります。あらかじめご了承下さい。
- 評価の際は、是非、インストール メディアのバージョンを含め、本ガイドの最新バージョンをご使用されることを推奨いたします。

適用範囲

本ガイドは、以下バージョンを対象としています。

- RAS Ver. 21.1

表記規則

本ガイド内の表記は、以下の規則に沿って行われています。

- RAS の画面に表示されるメニュー名/タブ名/プロパティ項目名/値/ボタン名は、[ ] で囲んで表記しています。
- 可変の値は < > で囲んで表記しています。

概要

本ガイドでは、Parallels® RAS 二要素認証の設定方法について説明します。本資料作成時点で追加のコストが発生しない Google Authenticator と Email を用いた簡易な二要素認証の実現方法について説明します。

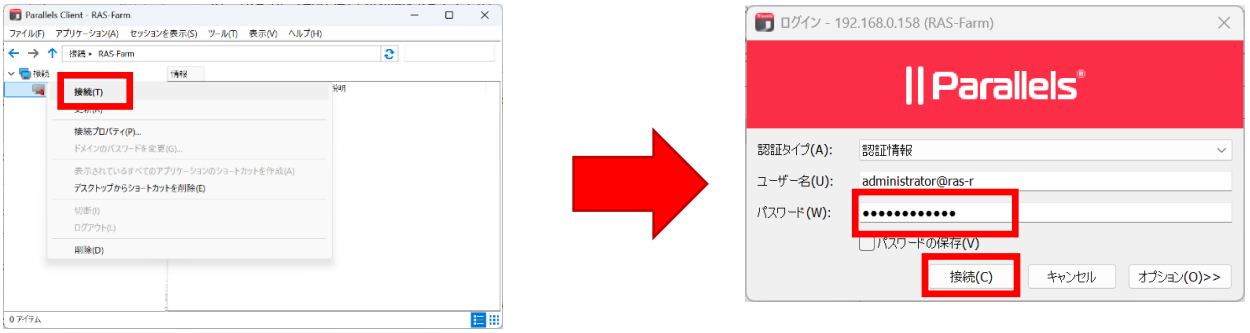
RAS 二要素認証とは

Parallels RAS では、一般的な利用方法として、RAS Client もしくはウェブブラウザーから RAS に接続する際にユーザー認証を求められます。Active Directory を利用してユーザーやコンピューターを管理することを推奨しています。

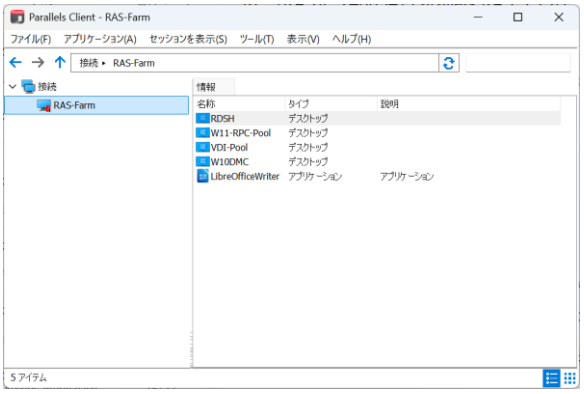
Active Directory を利用した場合、RAS Client から RAS 環境に接続する場合と、Web ブラウザから接続する場合では画面の表示が若干異なります。以下のような画面の流れで RAS 環境にログインし、認証情報を入力することにより、RAS 環境に接続してデスクトップやアプリケーションを利用することができます。

RAS Client の場合

既に RAS の接続先が登録されている RAS Client から RAS 環境に接続します、認証情報を尋ねるポップアップが表示されるため、必要な情報を入力して[接続]をクリックします。



接続に使用したユーザーアカウントに使用が許可されているデスクトップやアプリケーションの一覧が表示されるため、利用したいアイコンをダブルクリックして接続、利用します。

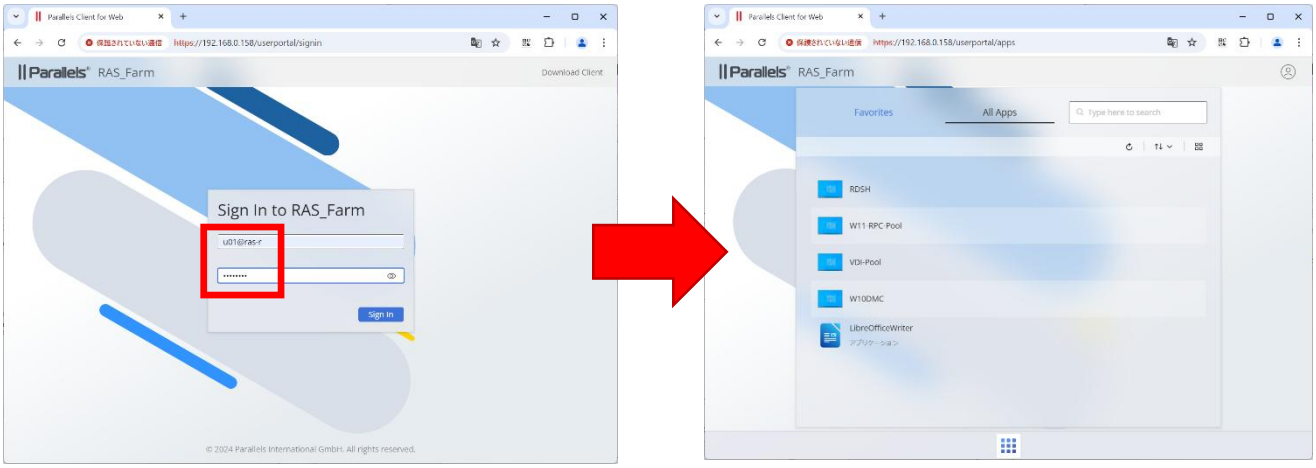


※RAS Client の設定手順は以下をご参照ください

https://jp.learn.corel.com/business/parallels-ras-client-handbook/

Web からの接続の場合

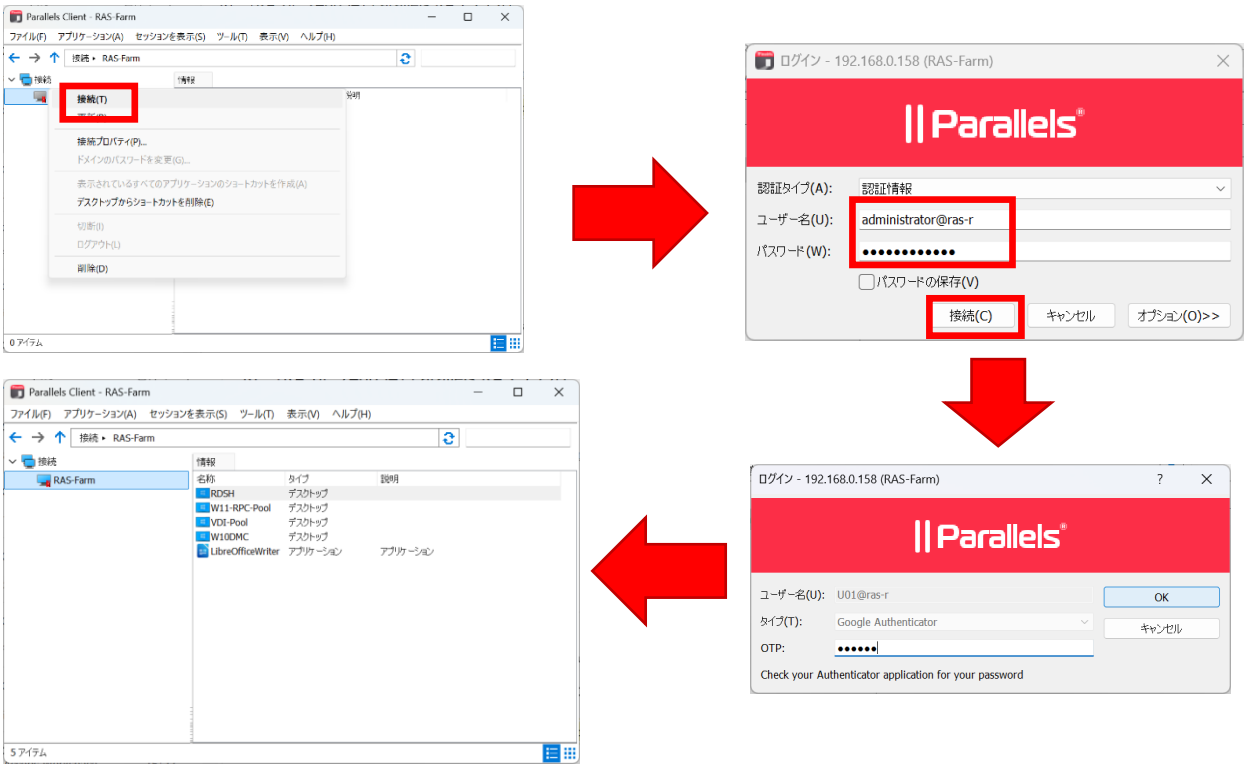
ウェブブラウザーで RAS 接続先の URL を入力して接続すると、認証情報を尋ねる画面が表示されるため、必要な情報を入力して[Sign In]をクリックします。ポップアップが表示されるため、必要な情報を入力して[接続]をクリックします。接続に使用したユーザーアカウントに使用が許可されているデスクトップやアプリケーションの一覧が表示されるため、利用したいアイコンをクリックして接続、利用します。



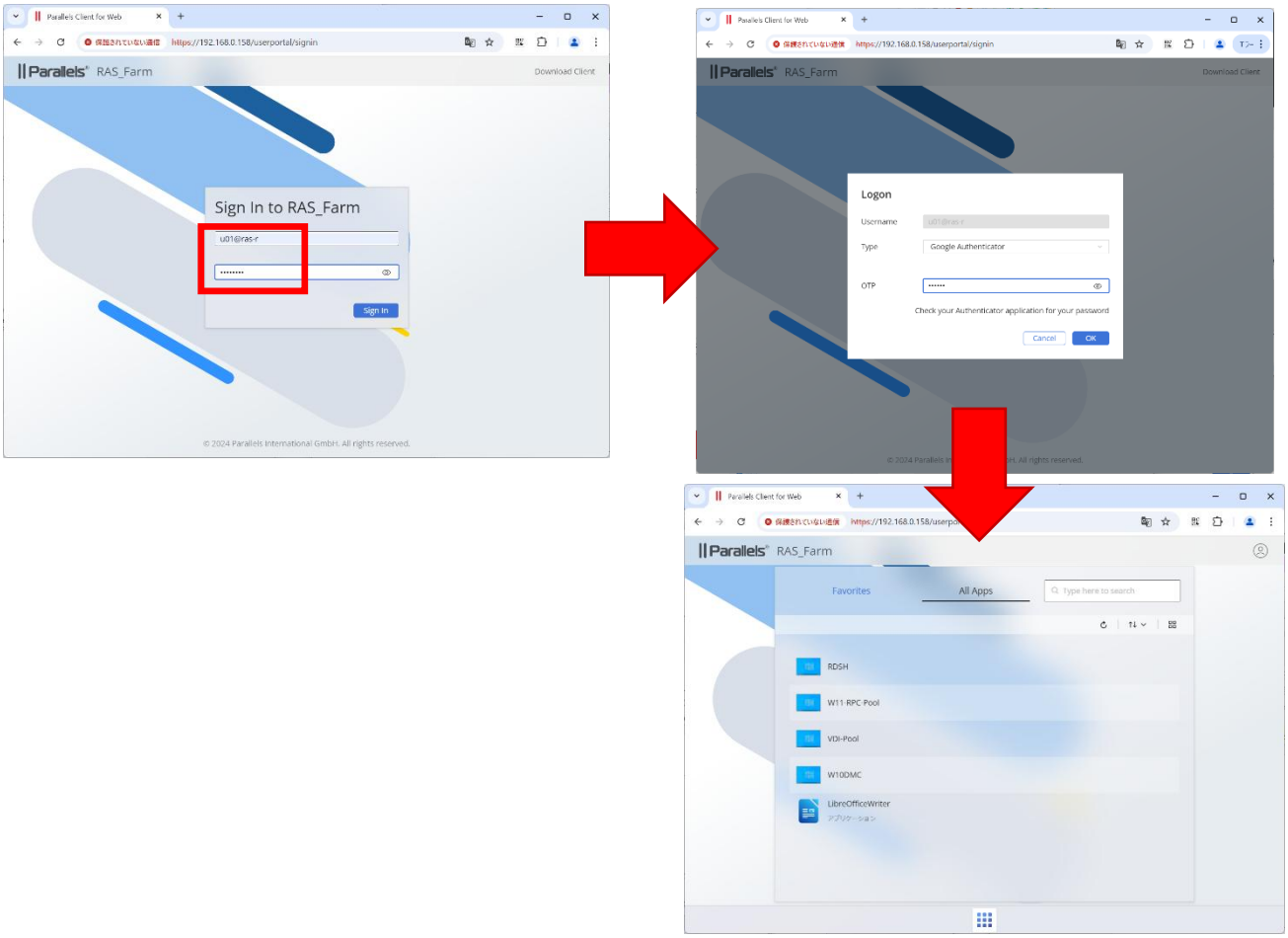
二要素認証の機能を追加することにより、ユーザー名とパスワードだけのシンプルな認証に加えてワンタイムパスワードの機能を追加することが可能です。ワンタイムパスワードの機能を追加することで、認証におけるセキュリティ強度をより高めることが可能です。

以下はワンタイムパスワードを利用した場合のログインの流れです。ここでは Google Authenticator を使用しています。

RAS Client の場合



Web から接続の場合



検証環境の構成

本ガイドであつかう検証環境について説明します。接続元であるクライアント側のコンポーネントは、Windows OS の物理マシンを使用します。

Parallels RAS 管理コンポーネントをインストールするサーバーを 1 台用意し、リモートから接続できる環境を用意しておきます。ここでは RDSH（Windows Server）のデスクトップ、Windows11 のデスクトップ、Windows 10 のデスクトップ、Windows Server 上で動作しているアプリケーションなどを事前に登録済です。

デスクトップやアプリケーションの設定方法については以下のサイトをご参照ください。

https://jp.learn.corel.com/volume-licensing/resources/#pras

項番	マシン	役割	OS
1	RAS Secure Gateway	RAS 環境へのログオン入り口。	Windows Server 2022
2	RAS Connection Broker 兼 RAS Console	RAS 環境への接続誘導、設定の保持。	Windows Server 2022
3	Active Directory	ユーザー認証。マシン登録。	Windows Server 2022
4	接続先リモート PC 用物理マシン	リモート PC 接続先である物理マシン。	Windows 10
5	クライアント マシン	ユーザーが Parallels Client を使用し、VDI にリモート接続するための物理マシン。	Windows 10 *1

構築手順

RAS 環境を利用する際に、二要素認証を実施、設定するための構築手順を説明します。

事前準備

本ガイドでは、二要素認証の設定方法に限定して説明するため、事前に Active Directory を利用した環境で、RAS のデスクトップやアプリケーションの公開・設定が既に完了していることを前提としています。

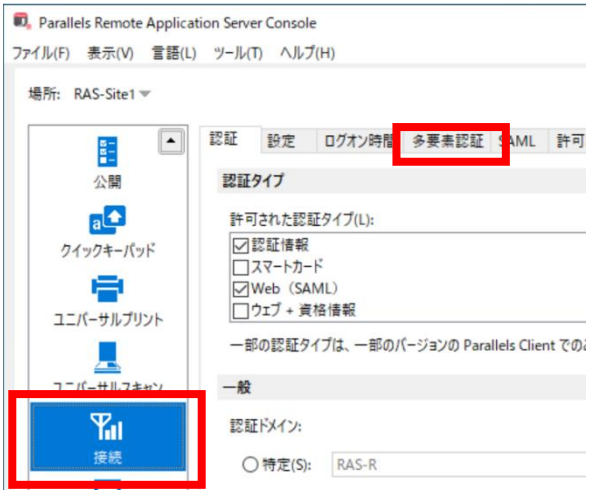
RAS 環境の構築やデスクトップやアプリケーションの設定・公開方法については以下のサイトをご参照ください。

https://jp.learn.corel.com/volume-licensing/resources/#pras

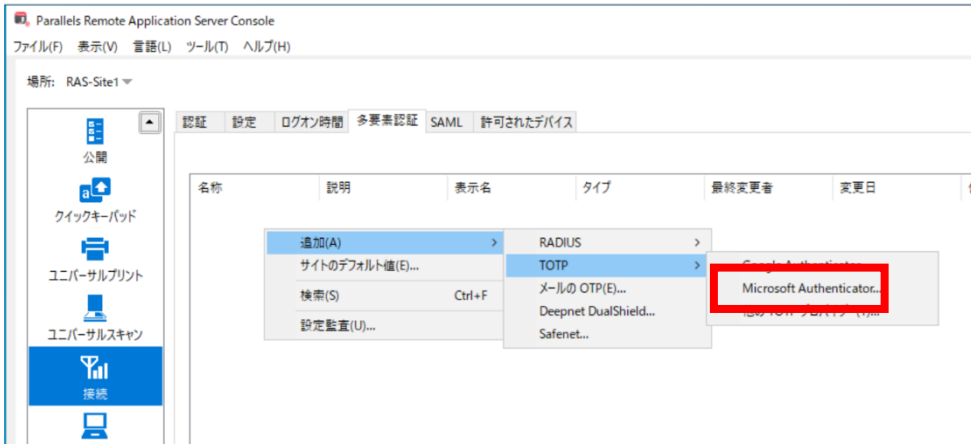
多要素認証の設定（Google Authenticator の場合）

多要素認証は管理コンソールから設定します。ここではプライマリーのコネクションブローカーにサインインして、管理コンソール[Parallels Remote Application Server Console]を起動します。

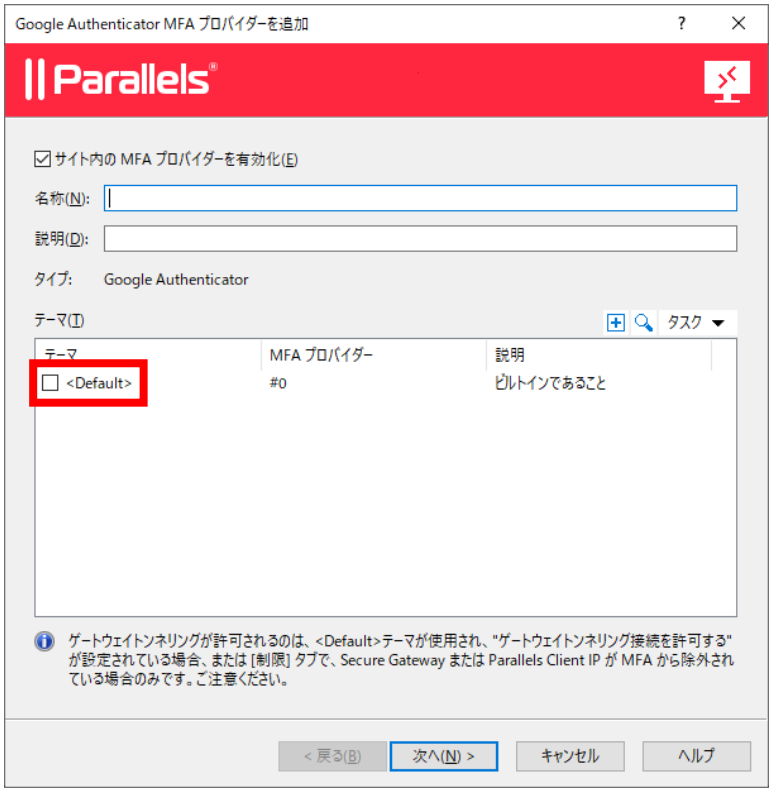
1　RAS Console を起動し、左側のペインで、[接続]をクリックし、右側のペインで[多要素認証]タブをクリックします。



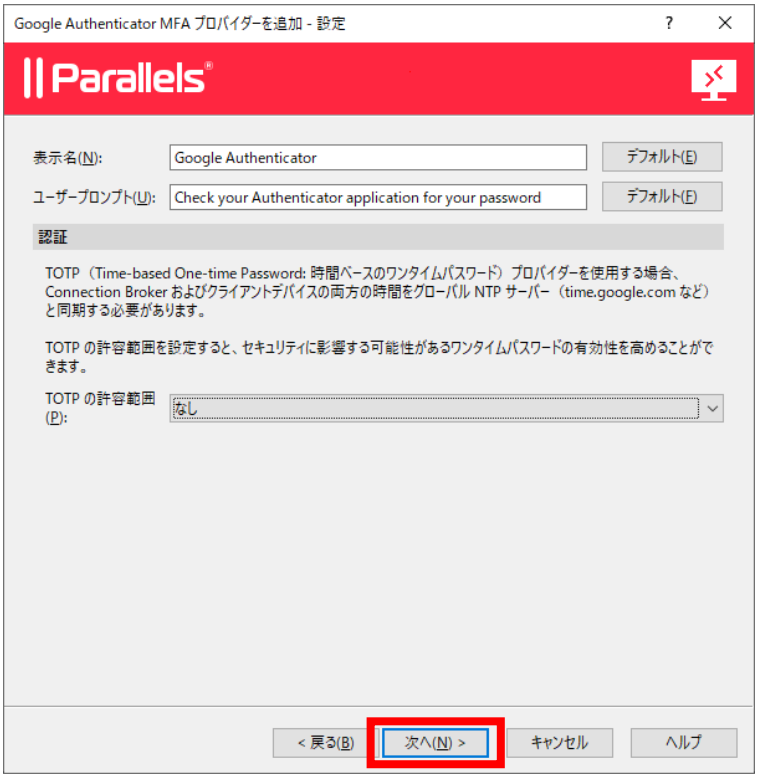
2　右側のペインの任意の場所で右クリックし、[追加]、[TOTP]をクリックし、今回は Google Authenticator を使用するため、[Google Authenticator]をクリックします。



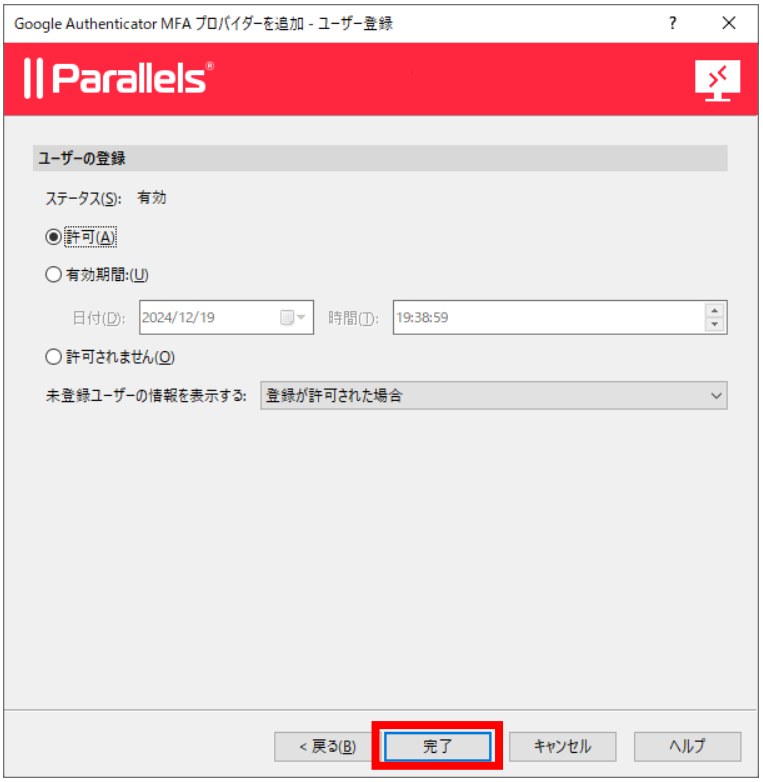
3 [名前]に任意の名前を設定し、設定したいテーマにチェックをして（ここでは「Default」）、[次へ] をクリックします。



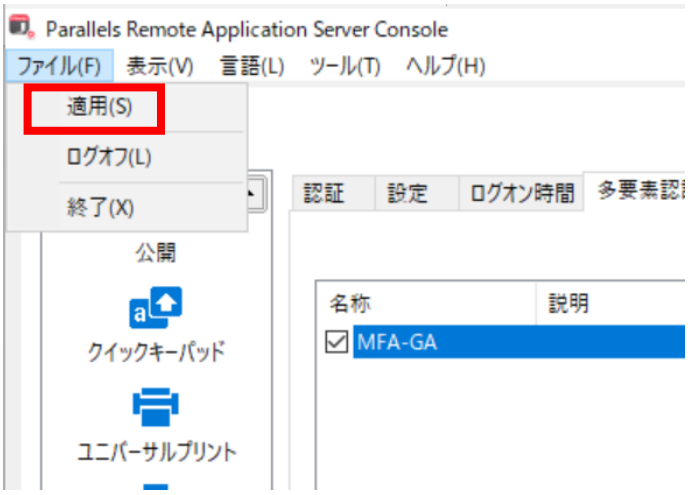
4 次の画面では、今回はデフォルトのまま[次へ]をクリックします。



5　このまま利用を許可するため、デフォルトのまま[完了]をクリックします。

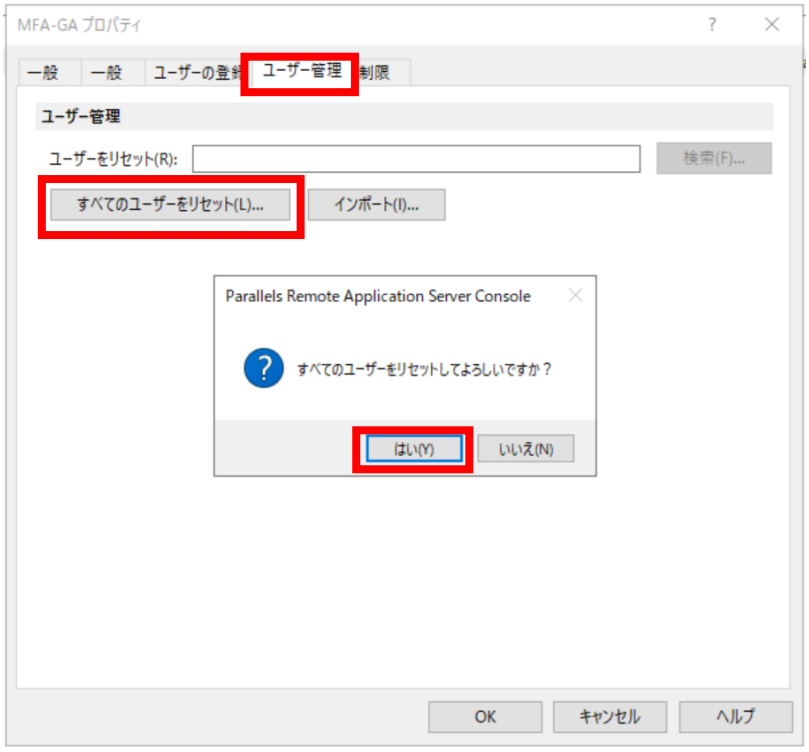


6　設定を保存するために[適用]を実行します。管理コンソールの右下または管理コンソール右上の[ファイル]から[適用]をクリックします。

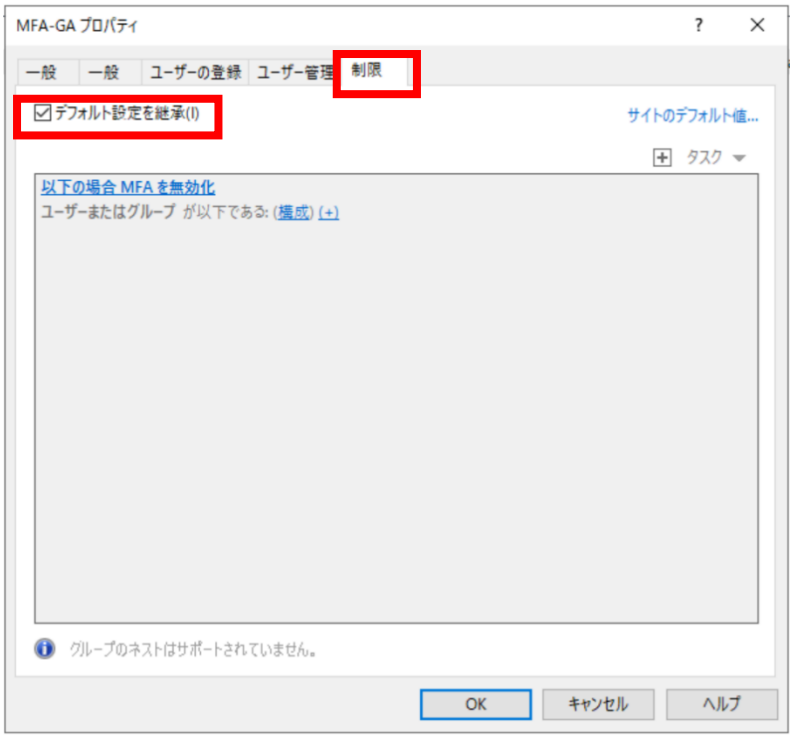


7　作成した多要素認証の設定を右クリックして[プロパティ]を開きます

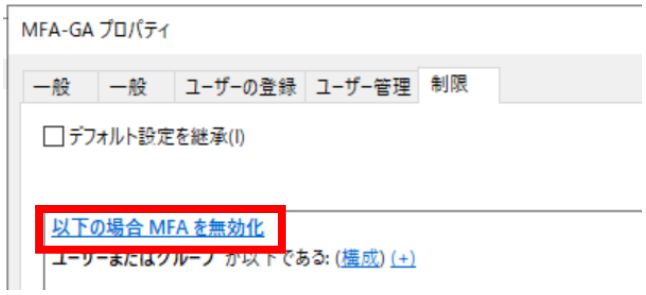
8　[ユーザー管理]タブを選択し、一度全てのユーザーをリセットしておきます。[すべてのユーザーをリセット]をクリックして、ポップアップ画面で[はい]をクリックします。



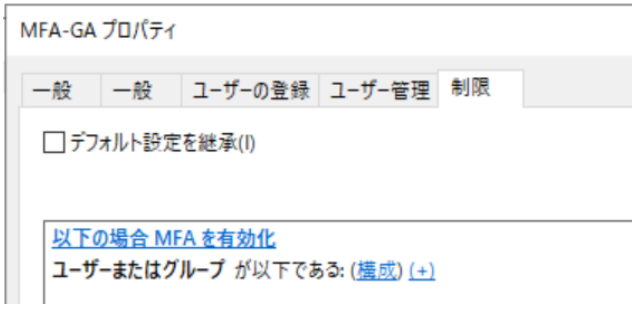
9　続いて[制限]タブをクリックします。今回はサイトのデフォルト値を使わずにこの設定のための制限を設定するため[デフォルト値を継承]のチェックを外します。前のステップで設定したテーマを利用するすべてのユーザーにMFAを強制する場合はこの設定は不要です。



10　[以下の場合 MFA を無効化]をクリックして[以下の場合 MFA を有効化]に変更します。

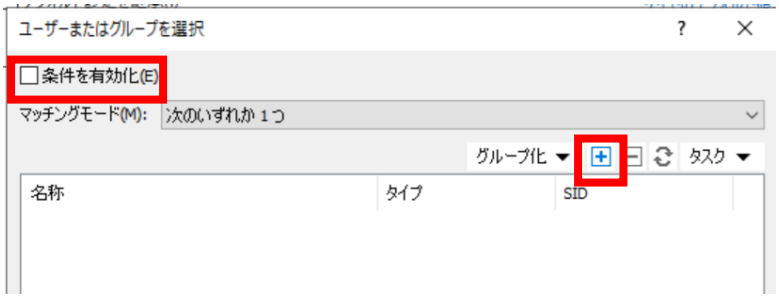


クリック後

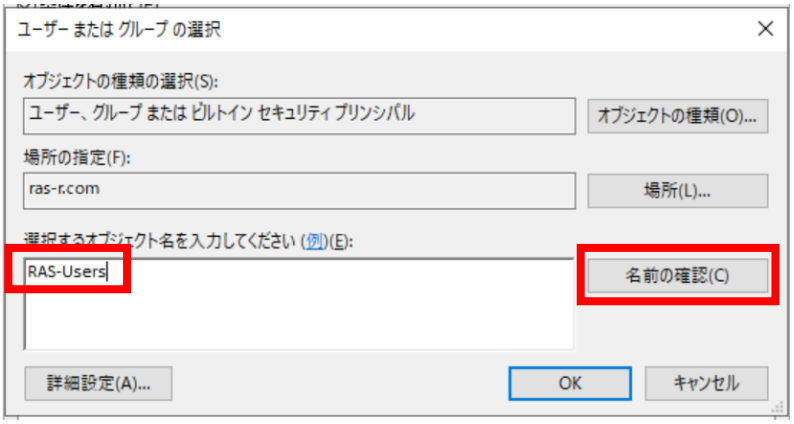


11　[ユーザーまたはグループが以下である]の[構成]をクリックします。

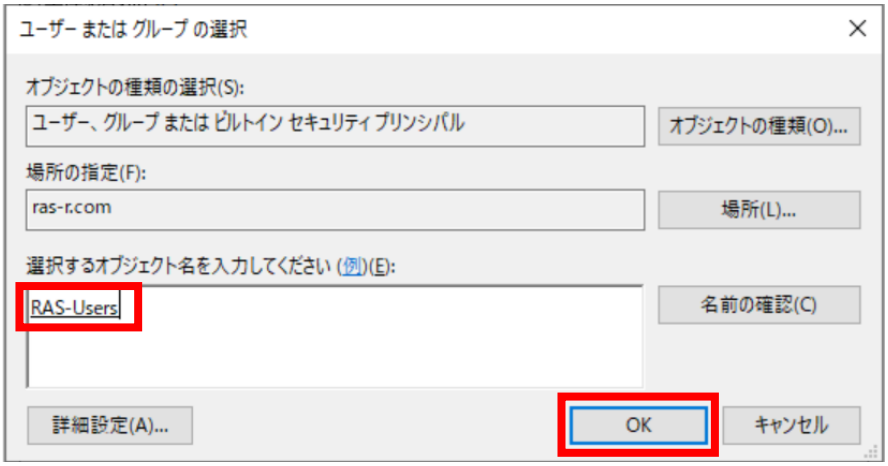
12　[ユーザーまたはグループを編集]の画面が表示されるので、[条件を有効化]にチェックを入れて、[＋]ボタンをクリックします。



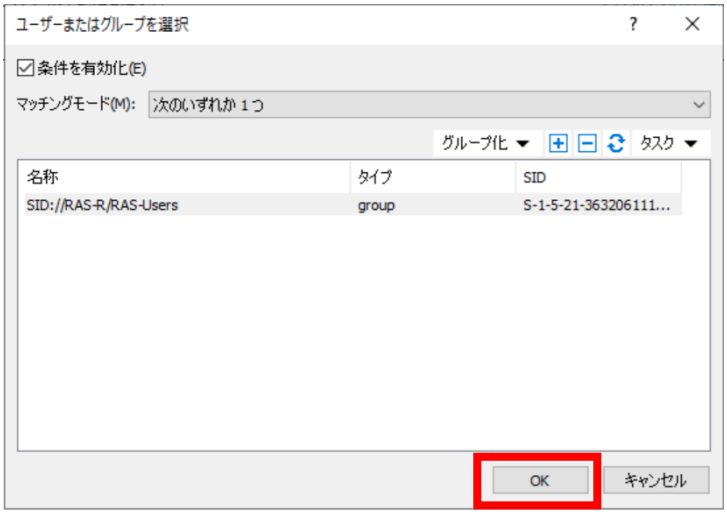
13　[ユーザーまたはグループの選択]画面がポップアップされるので適用するグループを設定します。ここでは事前に設定した RAS 利用者用のグループを入力し、[名前の確認]をクリックします。



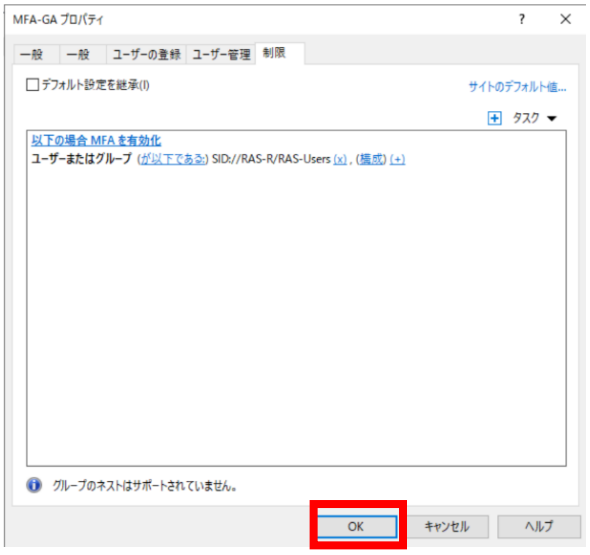
14 オブジェクト名の下にアンダーラインが表示されて、名前の確認が完了したら、[OK]をクリックします。



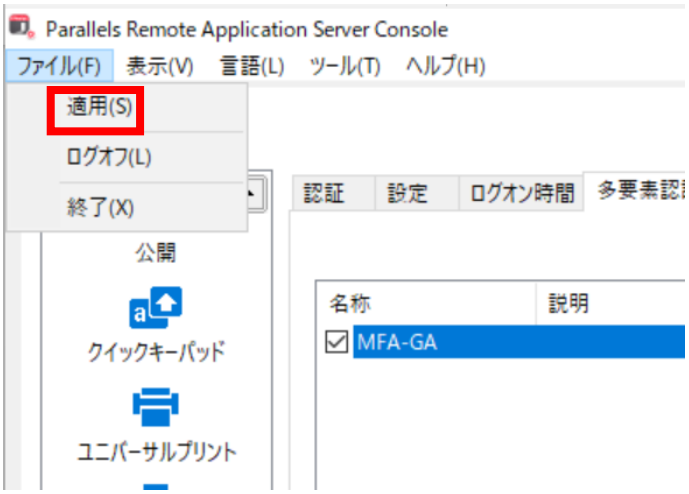
15 前の画面に戻るので[OK]をクリックして閉じます。



16 再度前の画面に戻るので、[OK]をクリックして閉じます。



17　再度設定を保存するために[適用]を実行します。管理コンソールの右下または管理コンソール右上の[ファイル]から[適用]をクリックします。



18　サーバー側の設定はこれで終了です。

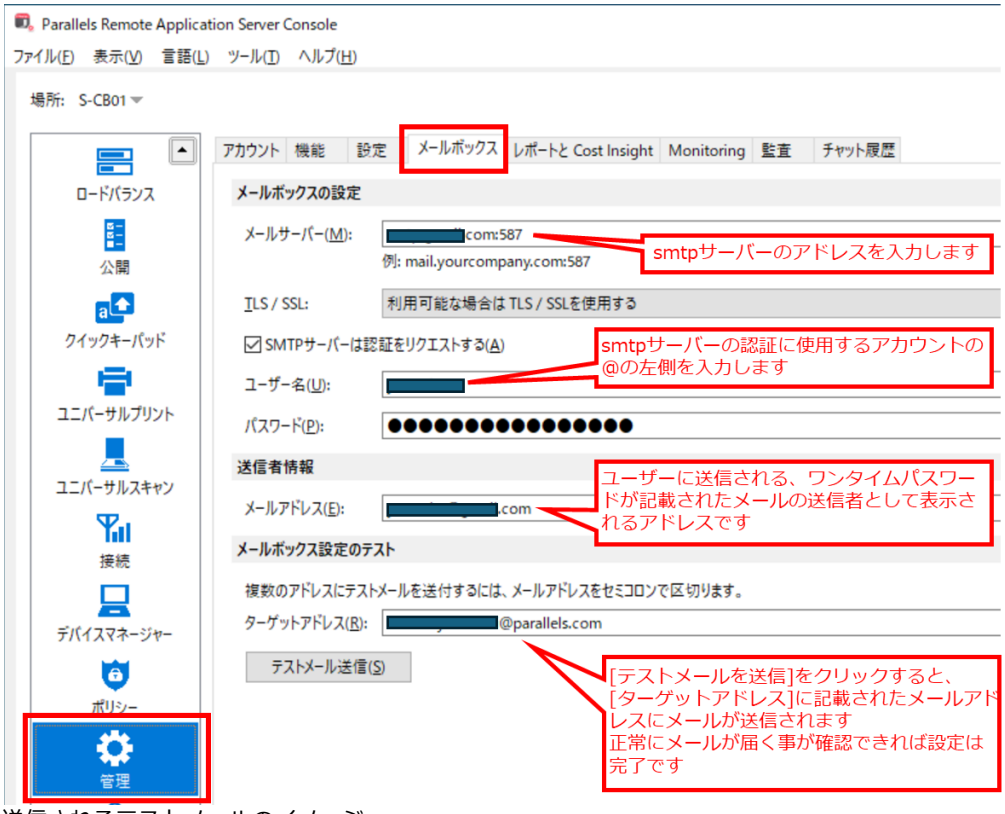
多要素認証の設定（Email の場合）

事前準備１：メールボックスの設定

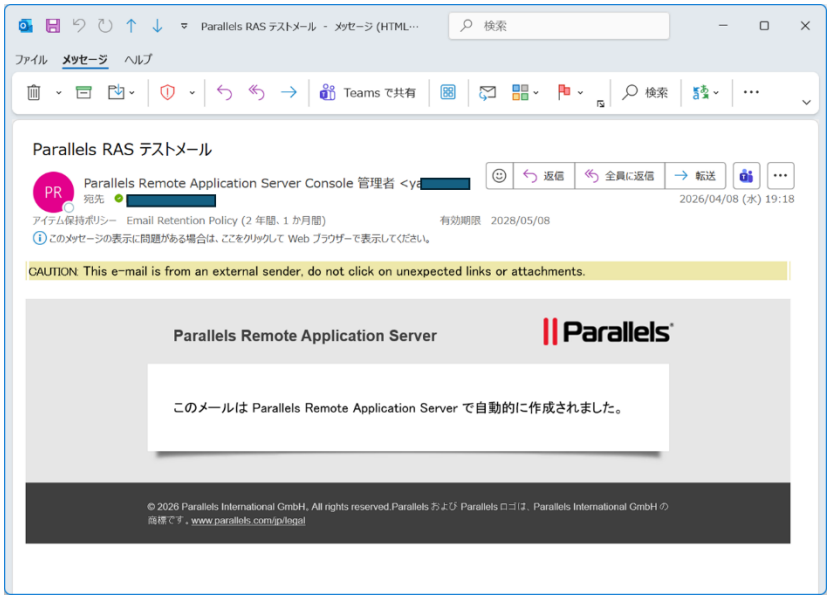
Email で多要素認証を実施する場合、RAS サーバーからメールを送信する必要があるため、まずメールボックスの設定を行います。

Connection Broker からメールを送信するためには、送信用のメールアドレスを設定する必要があります。

コネクションブローカーにサインインして、管理コンソール[Parallels Remote Application Server Console]を起動します。左ペインで[管理]タブを選択し、[メールボックス]タブを選択して、必要な情報を入力します。



送信されるテストメールのイメージ



注：

送信用 Email アドレスに特別な制限はありませんが、Web メールのサービスなどを利用する場合、最近は二要素認証を求めるケースが増えています。二要素認証が必須のメールアドレスは使用できません。

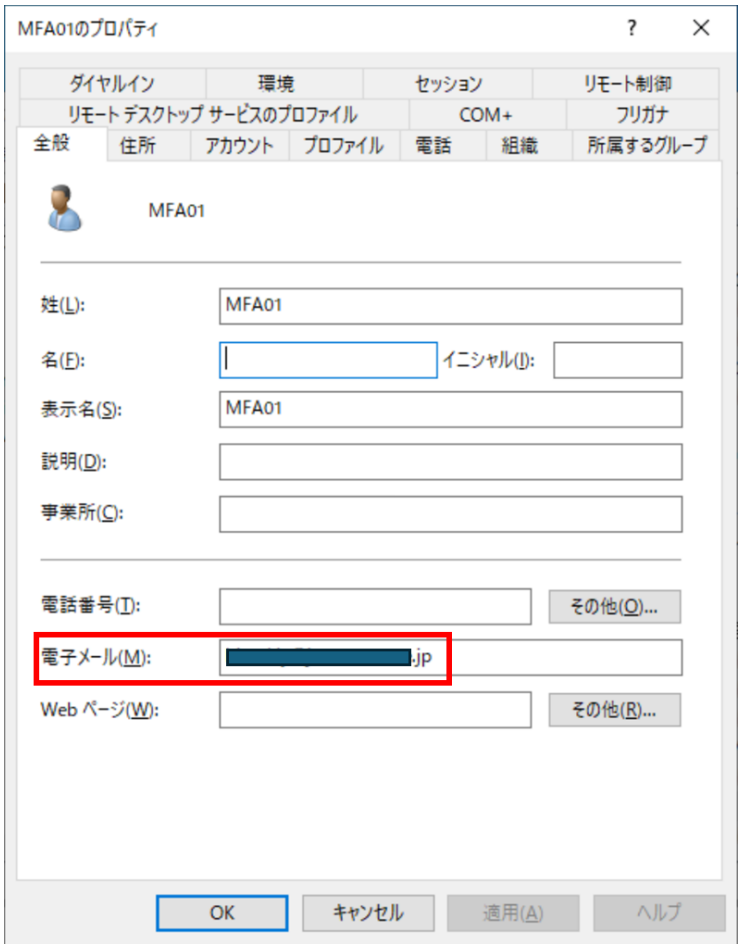
例えば、Gmail などはアプリケーションようのパスワードを設定して二要素認証を回避する方法があるので、利用するメールシステム毎に確認の上、設定してください。

事前準備 2 ：Email アドレスの設定

Email を使用した多要素認証を実施する場合、ワンタイムパスワードを送信するメールアドレスを設定する必要があります。

設定方法には二種類あります。一つは Active Directory のユーザーのプロパティでユーザー毎に設定します。

ユーザー毎に Active Directory のユーザーのプロパティの全般の電子メールにアドレスを設定します。



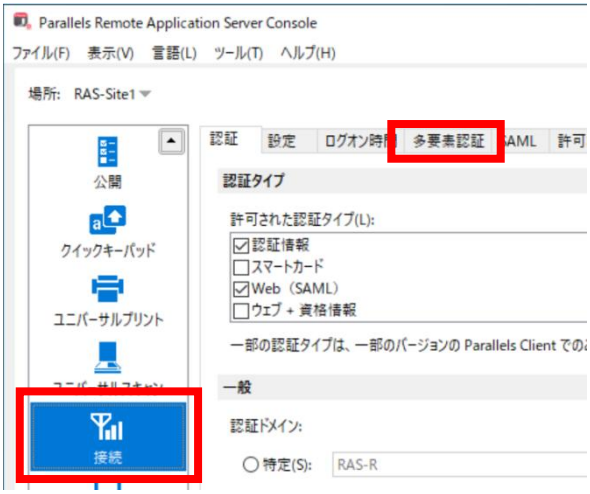
もう一つは Email での認証設定後、初めてファームにログオンする際に、ユーザー自身に入力させる方法です。

Email アドレスは RAS の内部データベースに保存されます。

実際の設定

RAS Console を起動し、左側のペインで、[接続]をクリックし、右側のペインで[多要素認証]タブをクリックします。

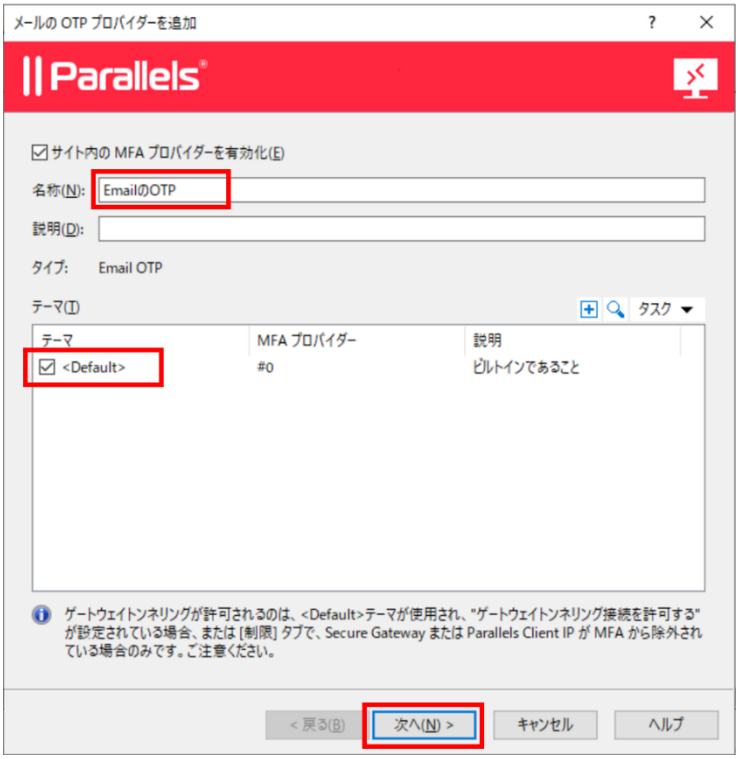
1 RAS Console を起動し、左側のペインで、[接続]をクリックし、右側のペインで[多要素認証]タブをクリックします。



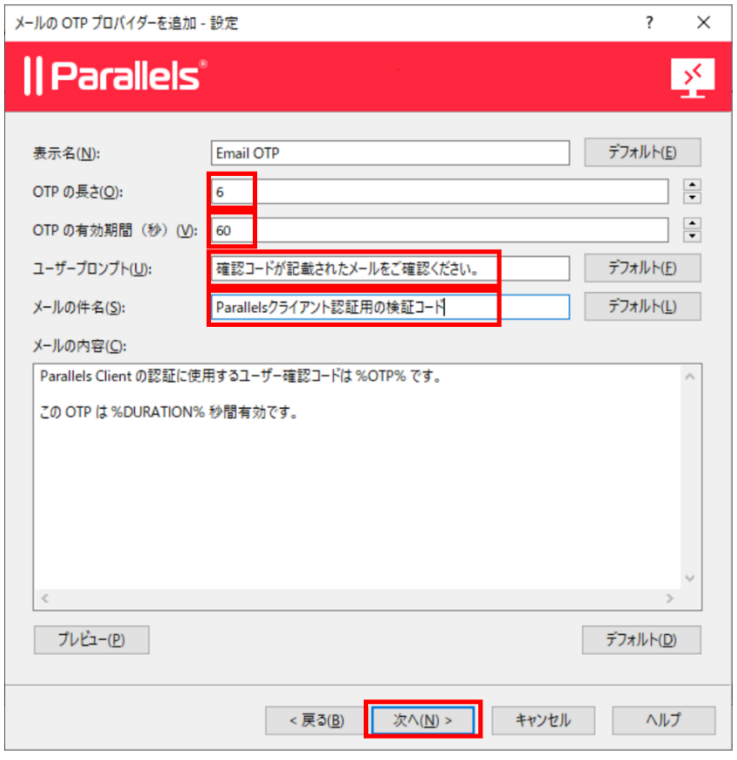
2 右側のペインの[＋]をクリックし、[メールの OTP]をクリックします。

3 [名称]に任意の名前を入力し、[テーマ]を選択して（ここではデフォルトしか存在しないため[Default]を選択）[次へ] をクリックします。

注：一つのテーマには一つの MFA プロバイダーしか設定できません。例えば、Google Authenticator と Email の両方の多要素認証を設定したい場合は、テーマも複数作成する必要があります。



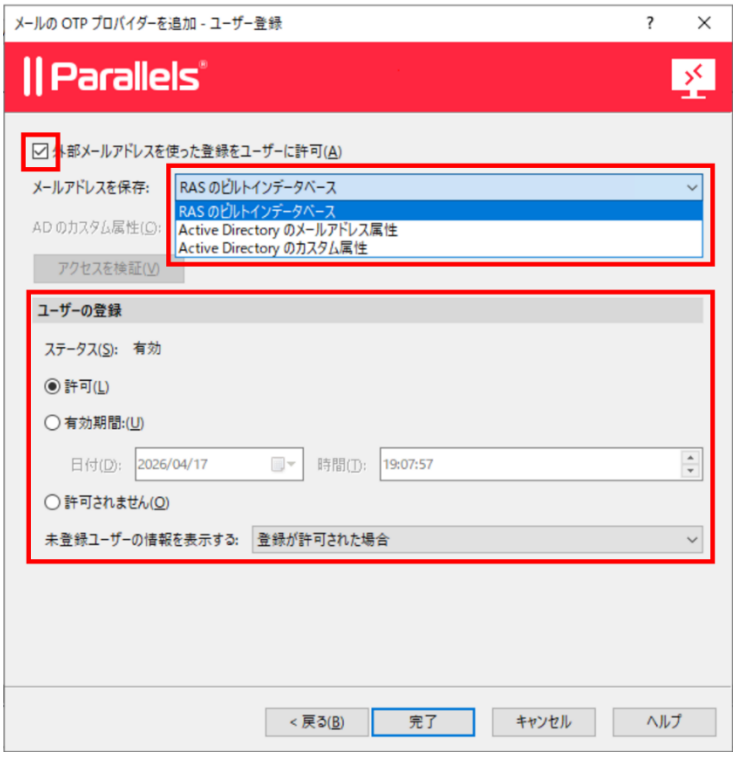
4 次の画面では、[OTP の長さ]（OTP の桁数）、[OTP の有効期間]、[ユーザープロンプト]、[メールの件名]などの設定を必要に応じて変更して、[次へ]をクリックします。（ここではデフォルトから少し変更しています）



5　次の画面では OTP を送付するメールアドレスの情報をどのように管理するか指定します。Active Directory のメール属性を利用するケースと、ユーザーが入力した情報を RAS のデータベースに格納して利用するケースの 2 つのパターンがあります。

※厳密には Active Directory のカスタム属性を使用する方法もありますが、一般的ではないのでここでは触れません。

ユーザーの登録期間の制限も可能ですが、ここではデフォルトのまま[完了]をクリックします。

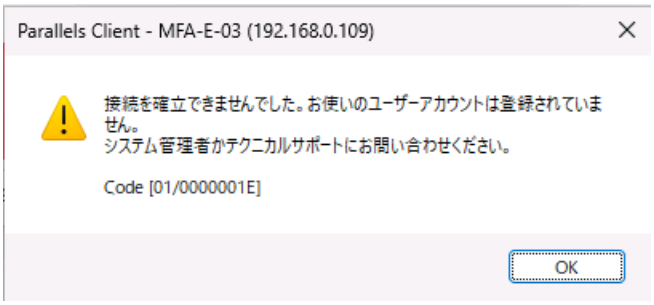


6　Active Directory のユーザーアカウントのプロパティのメールアドレスを利用する場合は、「Active Directory のメールアドレス属性」を選択します。

7　ユーザーにメールアドレスの入力を求める場合は、「RAS のビルトインデータベース」を選択します。ユーザーに登録してもらう必要があるため、「ユーザーの登録」は「許可」を選択します。

登録作業に期間の制限を設けたい場合は「有効期間」を設定します。

補足：「未登録ユーザーの情報を表示する」設定で「常に」を選択した場合は、メールアドレスが登録されていない場合、接続時にユーザー名、パスワード入力後に下記のメッセージが表示されます。有効期間を過ぎて登録できなかった場合も同様です。「常に」を選択しなかった場合は OTP の入力画面が表示されますが、ユーザーは OTP を入手できないため、ログオンできない状態が継続します。

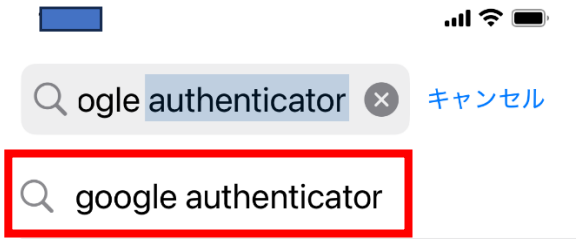


利用者側の設定（Google Authenticator の場合）

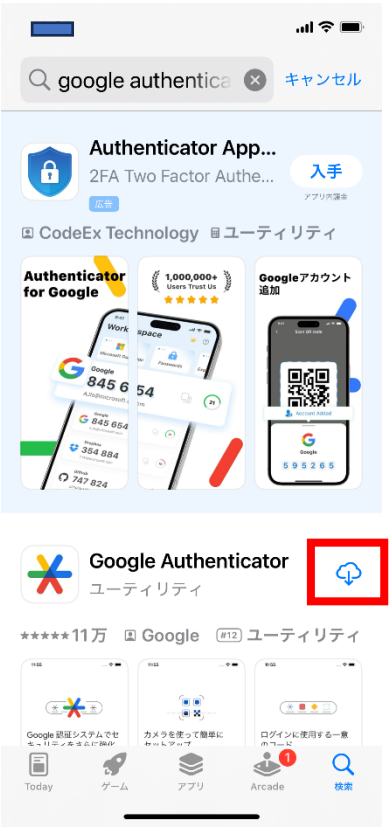
Google Authenticator を利用するためには、スマートフォンへの Google Authenticator アプリのインストレーションと設定が必要です。（ブラウザでの利用も可能ですが、セキュリティ強度が落ちるため推奨しません）

1 スマートフォンに Google Authenticator のアプリをインストールします。ここでは iPhone を例に説明します。

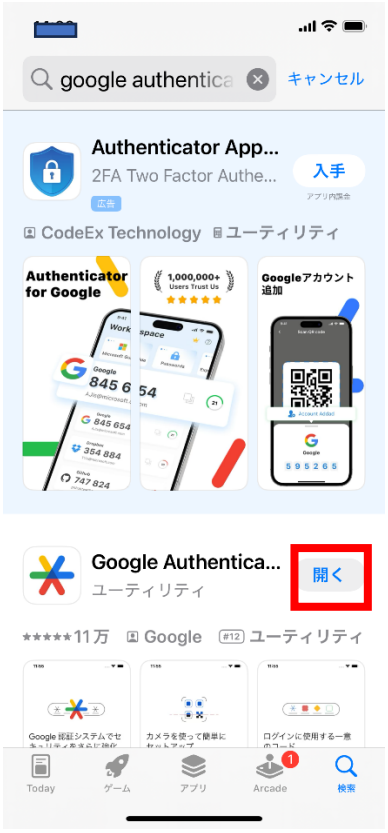
2 iPhone の App Store で検索を開き、検索ボックスに Google Authenticator と入力します。google authenticator がリストされるので、タップします



3 Google Authenticator が表示されるのでダウンロードボタンをタップしてインストールします。



4　インストールが完了したら[開く]をタップして Google Authenticator を起動します。

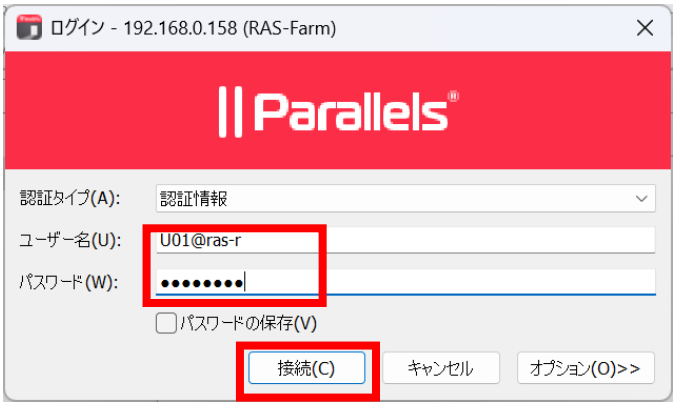


5　Google Authenticator の初期画面が表示されるので、[開始]をタップします。

6 既に iPhone で Google アカウントにサインインしている場合は、そのアカウントを利用するか聞いてきます。ここではサインインすることなく利用するため、[アカウントなしで Authenticator を使用]をタップします。

7 認証システムのコードがない旨表示されます。このタイミングで一度、iPhone の作業は中断して、RAS Client の作業を行います。

8　既にログインしている場合は一度ログアウトして、ログインします。認証情報を求められるため、必要な情報を入力して[接続]をクリックします。



9　以下のような画面が表示されるため、QR コードを読み取るため、iPhone での操作に戻ります。

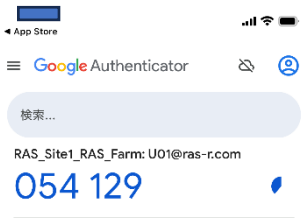
10　iPhone の Google Authenticator の停止していた画面で[コードを追加]をタップします。

11　認証システムのコードの追加は２通りあります。一つは QR コードをスキャンする方法、もう一つは認証コードを入力する方法です。ここではＱＲコードを利用する方法で進めます。[QR コードをスキャン]をタップします。

12　アプリケーションのカメラへのアクセス許可を求められるため、許可をタップします。

13　QR コードをスキャンする画面が表示されるため、緑色の四角の中に 9 のステップで表示された QR コードを投影します。

14　QR コードが認識されると、以下のようなワンタイムパスワードの画面が表示されます。数字の右側の円グラフは表示されているパスワードの有効期限です。デフォルトでは 30 秒毎にリフレッシュされます。



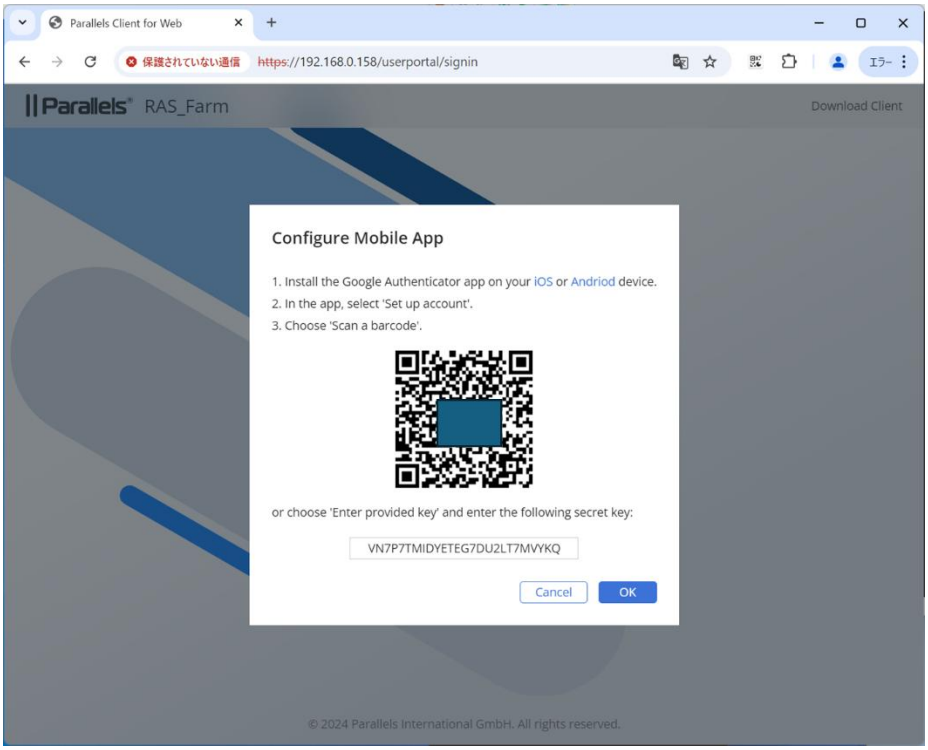
15　RAS Client に戻り、以下の画面で[次へ]をクリックします。

16 ワンタイムパスワードの入力を求められるため、[OTP]欄に iPhone に表示されているワンタイムパスワードを入力して[OK]をクリックします。

17 成功した旨のポップアップが表示されるため、[OK]をクリックして、デスクトップやアプリケーションの利用を開始します。

参考情報 Web からアクセスした場合の QR コード画面

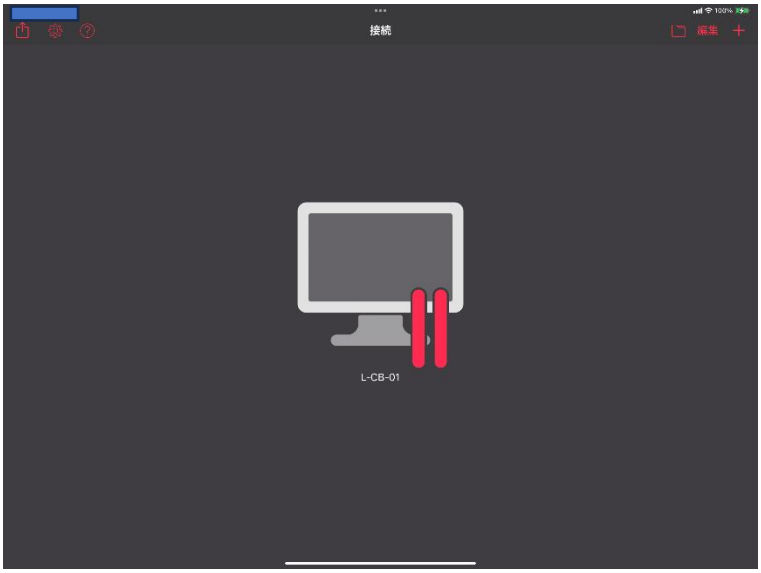
Web からアクセスした場合の、Google Authenticator の QR コード設定画面は下記のイメージです。



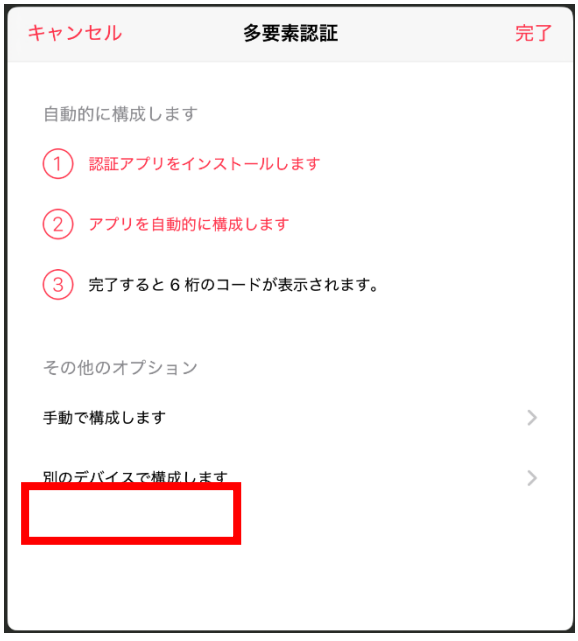
参考情報 iPad からアクセスした場合の QR コード画面

iPad からアクセスした場合の画面遷移は以下のようになります。

1　iPad の RAS Client から設定済の RAS へ接続するため、アイコンをタップします。

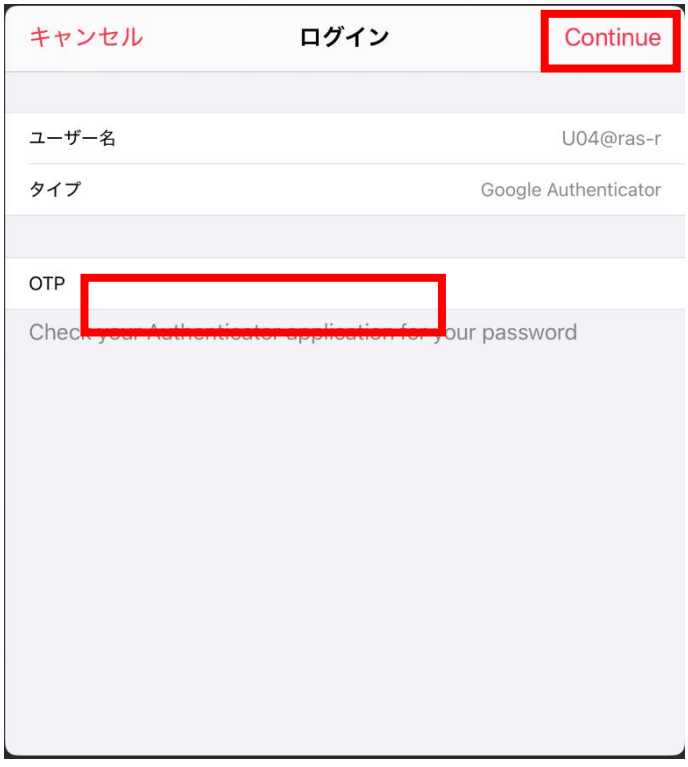


2　初めて多要素認証を利用する場合は以下の画面が表示されます。ここでは iPhone を使って多要素認証を実現するため、[別のデバイスで構成します]をタップします。



3 QR コードが表示されるため、前述の手順と同じように iPhone にインストールした Google Authenticator アプリで QR コードを読み取ります。

4 ワンタイムパスワードの入力画面が表示されるため、iPhone に表示されているワンタイムパスワードを入力して[Continue]をタップします。



5　初回のみ以下のメッセージが表示されます。[OK]をタップして、RAS をご利用ください。

利用者側の設定（Email の場合）

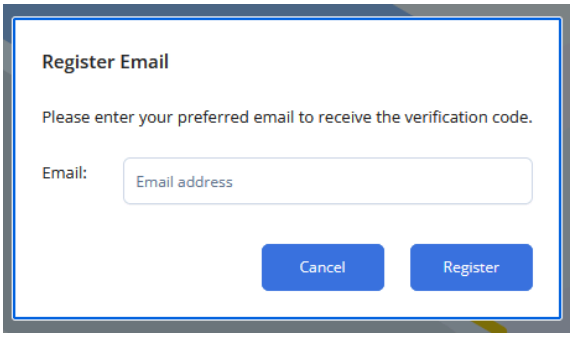
Email を使用した OTP を利用する場合、利用者側でアプリケーション等を用意する必要はありません。ただし、管理者の設定ではなく、利用者が Email アドレスを指定するように管理者が設定した場合は、設定後の初回のファームログオン時に OTP の送付先となる Email アドレスを指定する画面が表示されます。

※管理者が設定した場合は以下のステップは表示されません。

管理者の設定後、初回ファーム接続時に以下の画面が表示され、Email アドレスの登録を促されます。OTP の受診に使う Email アドレスを入力して OK をクリックします。ブラウザ利用時は同様に Email アドレスを入力して Register をクリックします。

RAS Client の場合

Web Client の場合



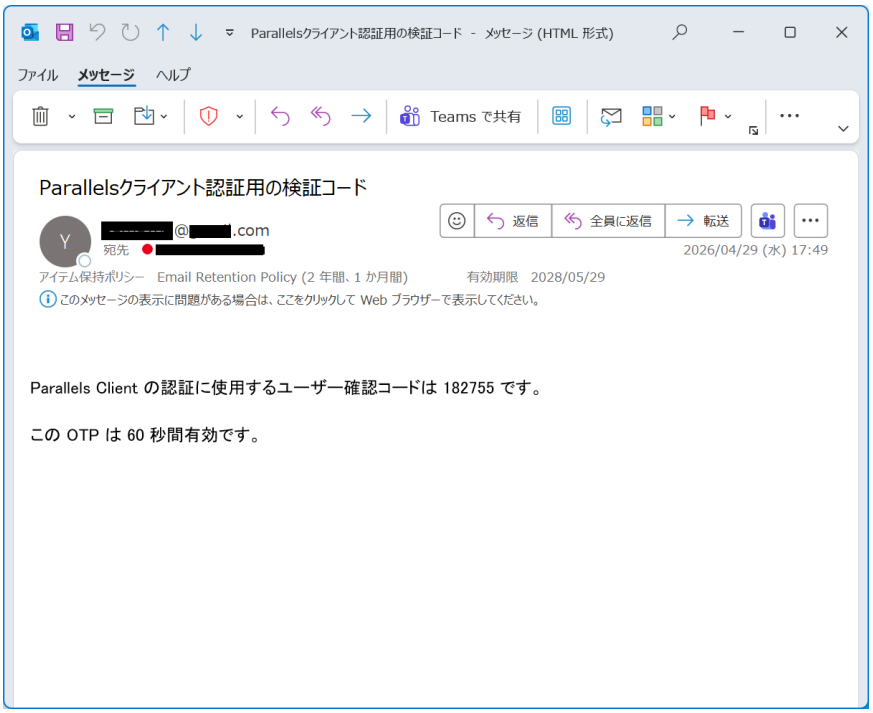
上記画面は初回のみ表示されます。

次に以下の画面が表示されます。登録したメールアドレス宛に送信されたユーザー確認コードを入力して OK をクリックしてログオン完了です。

※管理者が事前に Active Directory にメールアドレスを設定している場合は以下の画面が最初から表示されます。

２回目以降はユーザー名、パスワード入力後はこの画面が表示されるようになります。また管理者側が設定した場合もこの画面が最初から表示されます。

ユーザーに送付されるユーザー確認コードのメールは以下のイメージです。



OTP の長さと有効期間は管理者の設定によります。