

一官-大シ YPSG-2018-技術-023-01

学校法人 横浜市立大学

ICT 推進課 御中

付録（11）

多要素認証 ユーザーマニュアル

2019年1月30日

日本電気株式会社

改版履歴

更新日	内容	更新者
2019/1/18	新規作成	DT 飯田
2019/1/28	3.1.1.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合 文言追加 3.1.1.2 「認証用電話」 — 「電話する」を選択した場合 文言追加 3.1.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択した場合 文言追加 3.1.1.5 「モバイルアプリ」 — 「確認コードを使用する」を選択した場合 文言追加 3.2.2.1 アプリケーションパスワードを入力する 文言修正 3.3.2.1 「保存されたログイン情報」を削除する 新規追加	DT 飯田
2019/1/30	3.2.2 Outlook2013 で認証を行う 文言修正 3.2.2.1 アプリケーションパスワードを入力する 文言修正 3.3.2.1 「保存されたログイン情報」を削除する 文言修正 画面キャプチャ変更 3.1.1.6 POP または IMAP 接続の場合 文言修正	DT 飯田
2019/4/1	ブラウザでの多要素認証の保持期間 「今後××日間はこのメッセージを表示しない」を 14 日間 ⇒ 60 日間 に変更	YCU
2020/11/20	目次 ページ番号修正 4.4 アプリケーションパスワード 文言修正 画面キャプチャ変更	YCU

目次

1	はじめに（多要素認証の導入）	5
1.1	多要素認証（Multi-Factor Authentication）とは	5
1.2	適用対象範囲	5
1.3	初期設定(電話登録)	5
1.4	多要素認証が要求される範囲	5
1.5	用語定義	6
1.6	導入する多要素認証について	6
1.7	本ユーザーマニュアルについて	7
2	多要素認証の設定 ※初期設定(電話登録)	8
2.1	多要素認証方法を選択する	8
2.1.1	「認証用電話」 — 「テキストメッセージでコードを送信する」を選択する場合	11
2.1.2	「認証用電話」 — 「電話する」を選択する場合	14
2.1.3	「会社電話」を設定する場合	17
2.1.4	「モバイルアプリ」 — 「確認のため通知を受け取る」を選択する場合	18
2.1.5	「モバイルアプリ」 — 「確認コードを使用する」を選択する場合	29
3	メールの多要素認証	41
3.1	Outlook2016	41
3.1.1	Outlook2016 で認証を行う	42
3.1.2	Outlook2016 からメールを確認する	57
3.2	Outlook2013	58
3.2.1	Outlook2013 を起動する	58
3.2.2	Outlook2013 で認証を行う	58
3.2.3	Outlook2013 からメールを確認する	59
3.3	Thunderbird	60
3.3.1	Thunderbird を起動する	60
3.3.2	Thunderbird で認証を行う	60
3.3.3	Thunderbird からメールを確認する	65
3.4	MacMail	66
3.4.1	MacMail を起動する	66
3.4.2	MacMail で認証を行う	66
3.4.3	MacMail からメールを確認する	68
3.5	WEB ブラウザ(Microsoft Edge)	69
3.5.1	Office365 サインイン画面を表示する	69
3.5.2	Office 365 で認証を行う	69
3.5.3	WEB ブラウザ(Microsoft Edge)からメールを確認する	77

4	その他の設定	79
4.1	既定の認証方法の変更	80
4.1.1	「認証用電話にコードを送信する」に設定する場合	83
4.1.2	「認証電話に電話をかける」に設定する場合	85
4.1.3	「会社電話にかける」に設定する場合	87
4.1.4	「アプリケーションで通知する」に設定する場合	87
4.1.5	「アプリの確認コードを使用する」に設定する場合	95
4.2	代替の認証方法	98
4.2.1	代替の認証方法の設定	98
4.2.2	代替の認証方法を利用する	103
4.3	信頼済みデバイス	105
4.3.1	信頼済みデバイスを登録する	105
4.3.2	信頼済みデバイスを解除する	106
4.4	アプリケーションパスワード	110
4.4.1	アプリケーションパスワードの作成方法	110
4.4.2	アプリケーションパスワードの削除方法	113
4.5	「Microsoft Outlook」のバージョンの確認手順	114
4.6	Outlook2016 のメールの接続の種類の確認	116

1 はじめに（多要素認証の導入）

Microsoft Office 365 の利用にあたり、外部からの不正アクセスやなりすまし対策のため、同クラウドシステムに用意されているセキュリティ強化機能の 1 つである多要素認証の機能を有効にし、一層のセキュリティ強化を図ります。

1.1 多要素認証（Multi-Factor Authentication）とは

メールソフト等にログインする際、従来は ID とパスワードのみで本人確認をしていましたが、それ以外の要素も加え、本人を認証する方式のことです。従来の認証方式と比較しセキュリティが強化され、外部からの不正アクセスやなりすまし対策に有効な認証方式です。

1.2 適用対象範囲

全学生・教職員

1.3 初期設定(電話登録)

機能活用の有無にかかわらず、対象者全員が、初期設定として携帯電話や固定電話の登録を行う必要があります。

1.4 多要素認証が要求される範囲

学外から本学の Office 365 にサインインする場合。

※ 学内からサインインする場合、多要素認証は要求されません。

1.5 用語定義

本書で使用する主な用語について記載します。

用語	説明
Office 365	Microsoft 社が提供するクラウドグループウェアサービス
アプリケーションパスワード (アプリパスワード)	Office 365 アカウントにアクセスするためのアクセス許可をアプリまたはデバイスに付与するコード ※ Outlook2016 以外のメールソフト (Outlook2013、Thunderbird 等) を利用している場合や、Outlook2016 で Exchange 以外の接続の種類 (POP や IMAP など) を選択している場合 (詳細は「4.6 Outlook2016 のメールの接続の種類の確認」をご参照ください。) に使用します。
学内	以下の学内ネットワークから Office 365 にアクセスする場合を指します。 <ul style="list-style-type: none">学内無線 LAN (YCUWL)教育研究 LAN事務 LAN
学外	学内ネットワーク以外の、自宅などから Office 365 にアクセスする場合を指します。 ※ 学内においても、携帯電話のキャリア回線を使ってアクセスする場合は、学外に該当します。

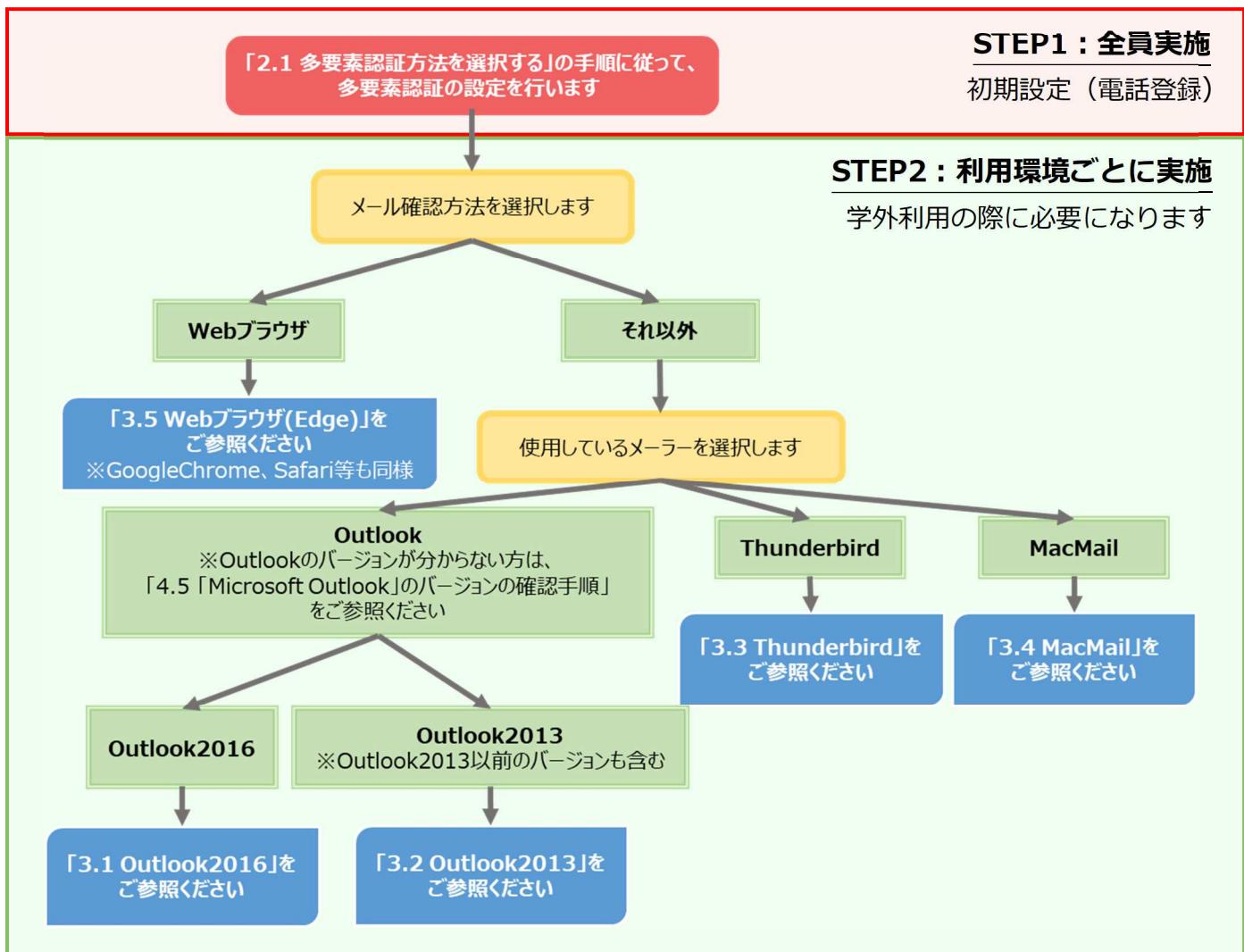
1.6 導入する多要素認証について

Microsoft Office 365 のサインインの仕組みを利用し、デバイス(PC 等)ごとにソフトウェア(WEB ブラウザやメールソフト等)単位で認証を行います。

一度多要素認証を行うと一定期間は認証状態が保持されますが、認証状態が保持されていない他の PC やブラウザ、メールソフトなどでサインインした場合は、その都度、多要素認証を要求されます。

1.7 本ユーザーマニュアルについて

本ユーザーマニュアルは、以下のワークフローに沿って、ご自身の使用しているOS、メールをご確認いただき、該当の章をご参照ください。



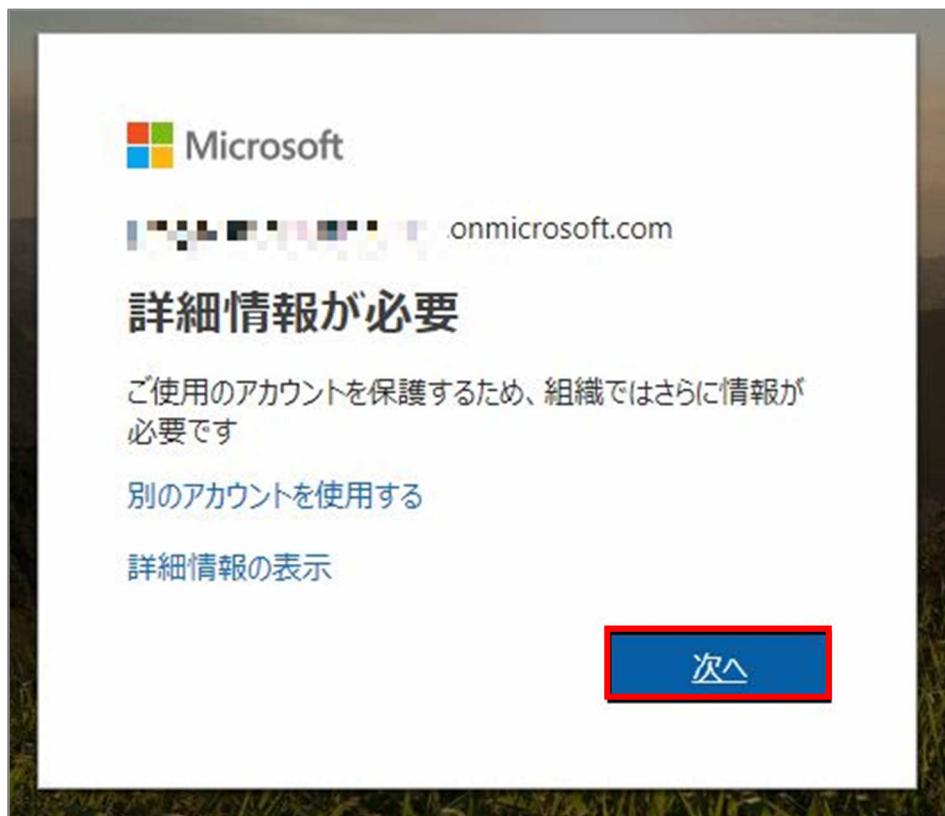
2 多要素認証の設定 ※初期設定(電話登録)

2.1 多要素認証方法を選択する

本学のOffice 365は多要素認証が導入されています。多要素認証が有効になったユーザーで本学Office 365にサインインする際は、初回のみ以下の手順で多要素認証設定を行う必要があります。

- ① Office 365のURL <http://portal.office.com/>

にアクセスし、ユーザー名とパスワードを入力後、以下の画面が表示されたら「次へ」をクリックします。



② 以下の画面から多要素認証設定を実施します。

多要素認証は、「会社電話」を除く、下表の4つの方法の中から選択することができます。ご自身の利用状況により、使いやすい方法を選択してください。(推奨方式は、「認証用電話にコードを送信する」となります。)



項目	方法	説明	設定手順
認証用 電話	テキスト メッセージ (SMS/ ショートメール) ※ 推奨方式	登録した携帯電話の電話番号宛てにテキストメッセージ（ショートメール）が送信されます。 自宅の固定電話等、テキストメッセージ（ショートメール）が送信できない電話は「認証電話に電話をかける」方法を設定してください。	2.1.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択する場合
	電話	登録した電話番号宛てに電話がかかります。音声の指示に従って操作をします。	2.1.2 「認証用電話」 — 「電話する」を選択する場合
会社電話	システム連携された会社電話のことを指すため、本学では利用できません。		2.1.3 「会社電話」を設定する場合
モバイル アプリ	通知	モバイルアプリケーション（Microsoft Authenticator）でサインインの許可を求めるダイアログが表示されます。 「Microsoft Authenticator」は、Android、iOS、Windows Phone で利用できます。	2.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択する場合
	確認コード	モバイルアプリケーション（Microsoft Authenticator）にコードが送信されま	2.1.5 「モバイルアプリ」 — 「確認コード」

		<p>す。 「Microsoft Authenticator」は、Android、iOS、 Windows Phone で利用できます。</p>	<p>を使用する」を選択 する場合</p>
--	--	--	---------------------------

2.1.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択する場合

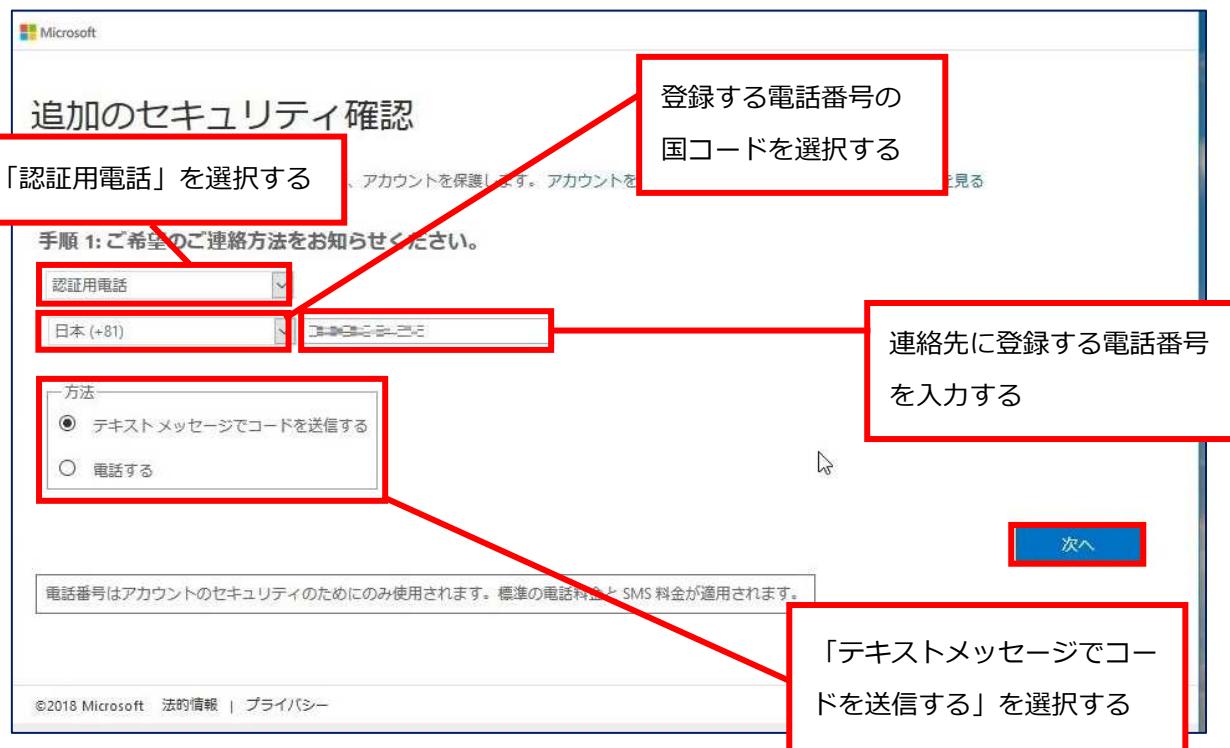
指定した認証用電話の電話番号宛に、ショートメール(SMS)で 6 衔の数字のコードが送信される認証方法です。

登録する電話番号の形式は、以下のどちらでもかまいません。

- 0 から始まる国内電話の形式 (例 : 03-1234-5678)
- 国番号から始まる国際電話の形式 (例 : 813-1234-5678)

※ テキストメッセージはショートメール(SMS)で送信されるため、固定電話では使用できません。

① PC 上の画面で以下の通り設定し、「次へ」をクリックします。



- ② 登録した電話番号宛てにショートメール(SMS)で 6 行の数字のコードが送信されるので、記載されたコードを以下の画面の入力フォームに入力して「確認」をクリックします。



Microsoft

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 2: お客様の電話 +81 90XXXXXX にテキスト メッセージを送信しました

確認コードを受け取ったら、ここに入力してください

キャンセル 確認

©2018 Microsoft | 法的情報 | プライバシー

③ 以下の画面でアプリ パスワード(アプリケーションパスワード)を発行します。

「完了」をクリックし、多要素認証方法の設定を完了します。

- ※ 「アプリ パスワード(アプリケーションパスワード)」は Outlook2016 以外のメールソフト (Outlook2013、Thunderbird 等) を利用している場合や、Outlook2016 で Exchange 以外の接続の種類 (POP や IMAP など) を選択している場合 (詳細は「4.6 Outlook2016 のメールの接続の種類の確認」をご参照ください。) に使用します。
- ※ 本画面以降、生成されたアプリケーションパスワードを確認することはできません。メモ帳などに保存してください。



2.1.2 「認証用電話」 — 「電話する」を選択する場合

指定した認証用電話の電話番号宛に、電話がかかる認証方法です。

登録する電話番号の形式は、以下のどちらでもかまいません。

- 0 から始まる国内電話の形式 (例 : 03-1234-5678)
- 国番号から始まる国際電話の形式 (例 : 813-1234-5678)

① 以下の画面で以下の通り設定し、「次へ」をクリックします。



- ② 以下の画面が表示されたら、登録した電話番号宛てに電話が掛かります。音声の指示に従って操作をすると自動で③の画面に切り替わります。

(「#」を押すように音声指示があります。アナログ回線の場合は「*」を押してから「#」を押す必要があります。)



③ 以下の画面でアプリ パスワード(アプリケーションパスワード)を発行します。

「完了」をクリックし、多要素認証方法の設定を完了します。

- ※ 「アプリ パスワード(アプリケーションパスワード)」は Outlook2016 以外のメールソフト (Outlook2013、Thunderbird 等) を利用している場合や、Outlook2016 で Exchange 以外の接続の種類 (POP や IMAP など) を選択している場合 (詳細は「4.6 Outlook2016 のメールの接続の種類の確認」をご参照ください。) に使用します。
- ※ 本画面以降、生成されたアプリケーションパスワードを確認することはできません。メモ帳などに保存してください。



2.1.3 「会社電話」を設定する場合

システム連携された会社電話のことを指すため、本学では利用できません。

2.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択する場合

モバイルアプリを使用する認証方法です。

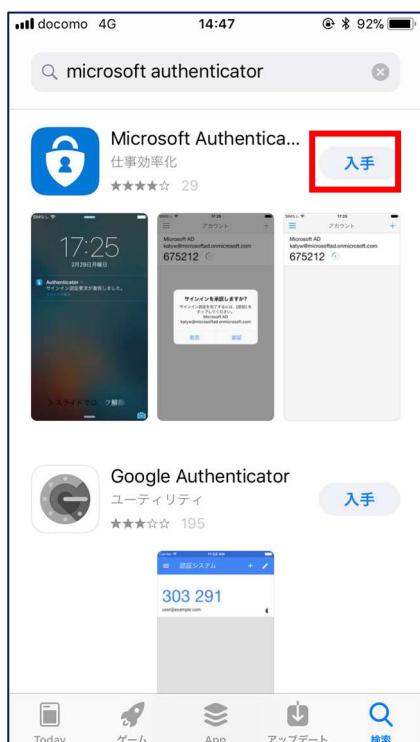
本認証方法による設定をする場合は、スマートフォンに「Microsoft Authenticator」（以下スマートフォンアプリ）を事前にインストールしてください。

インストール方法は以下の通りです。

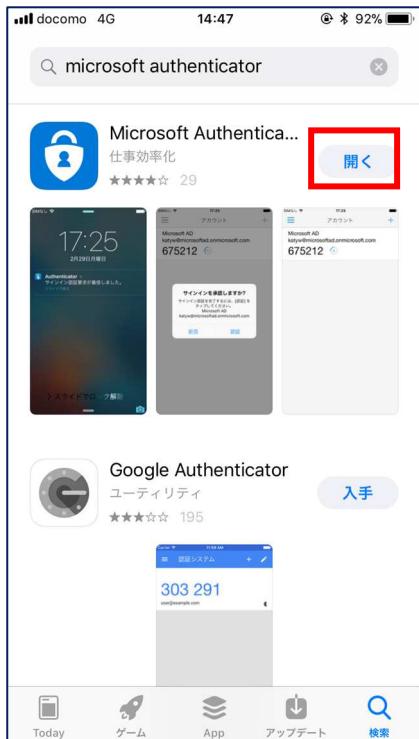
【iOS の場合】

- ① 「App Store」を起動して「Microsoft Authenticator」を検索します。

以下の画面が表示されたら画面右上の「入手」ボタンをタップします。



② 「入手」ボタンが「開く」ボタンになればインストール完了です。



【Android の場合】

① 「Google Play ストア」を起動して「Microsoft Authenticator」を検索します。

以下の画面が表示されたら画面右上の「インストール」ボタンをタップします。

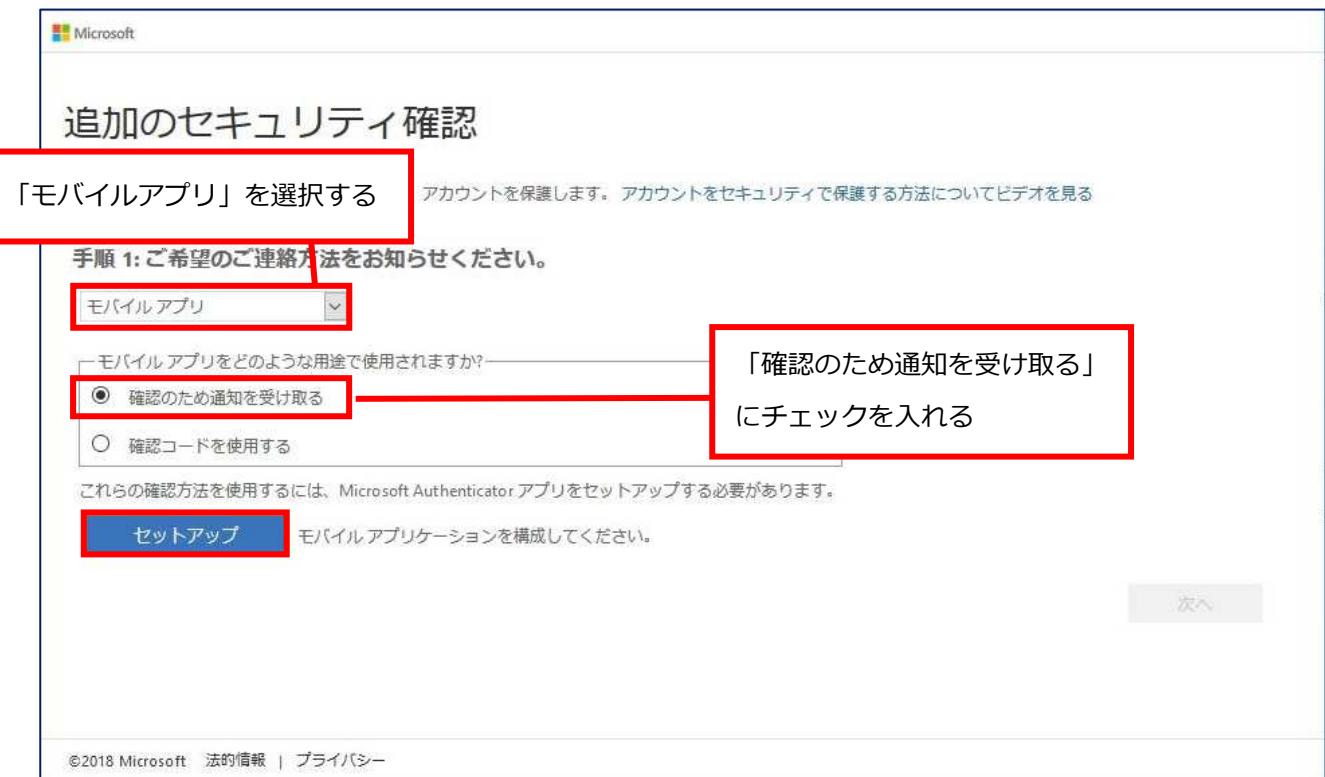


② 以下の画面が表示されたらインストール完了です。



【PC 上での操作 その1】

① PC 画面上で以下の通り設定し、「セットアップ」ボタンをクリックします。



② 「モバイルアプリケーションの構成」画面が表示されたら、スマートフォンでの操作を実施します。



【iOS の場合】

① スマートフォンアプリを起動して画面右上の「+」ボタンをタップします。

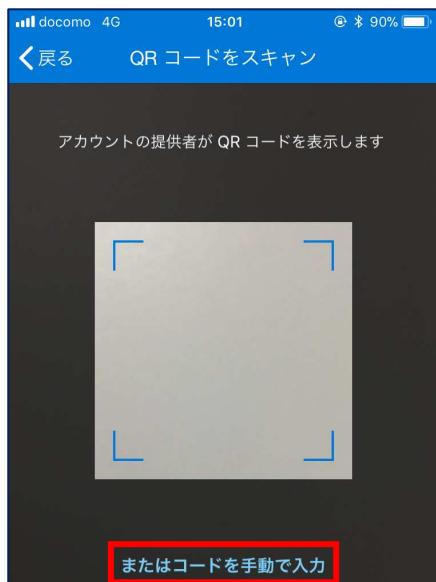


端末によっては、「アカウントを追加すると、バックアップから回復できなくなります。」と表示されますが、「続行」をタップしてください。

② 「アカウントの追加」画面で「職場または学校アカウント」をタップします。



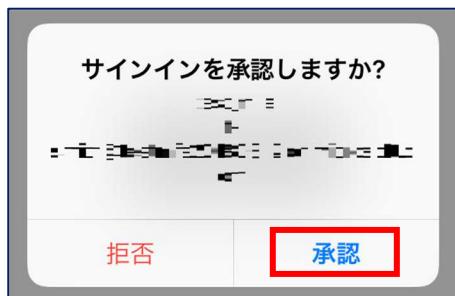
③ 以下の画面から、「モバイルアプリケーションの構成」画面に表示された QR コードを読み取ります。



もしくは「またはコードを手動で入力」をタップし、表示された以下右の画面に QR コードと同時に表示されたコードと URL を直接入力して「完了」をタップします。



④ 以下のダイアログが出力されたら「承認」をタップします。



【Android の場合】

- ① スマートフォンアプリを起動して画面中央の「+」をタップします。



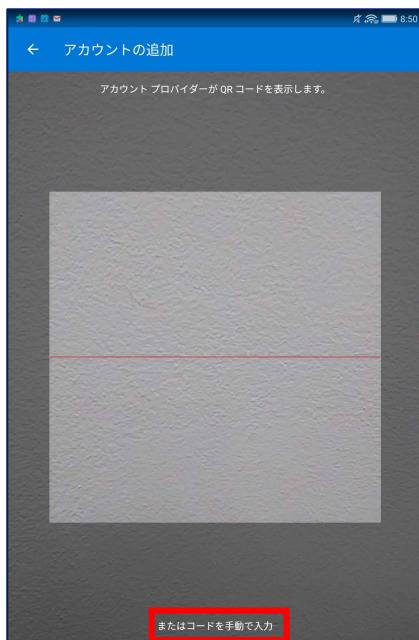
- ② 画面右上の「⋮」ボタンをタップし、「アカウントの追加」をタップします。



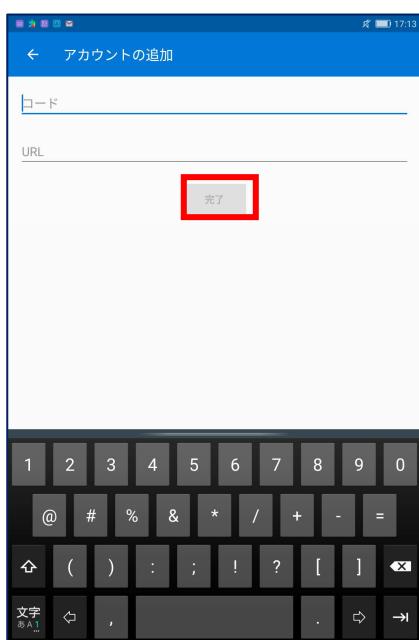
- ③ 「アカウントの追加」画面で「職場または学校アカウント」をタップします。



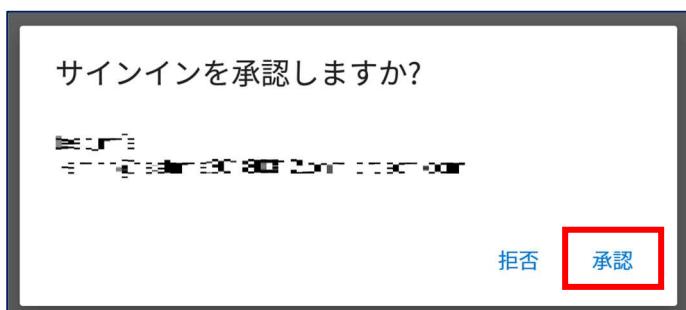
④ 以下の画面から「モバイルアプリケーションの構成」画面に表示された QR コードを読み取ります。



もしくは「またはコードを手動で入力」をタップし、表示された以下の画面に QR コードと同時に表示されたコードと URL を直接入力して「完了」ボタンをタップします。



⑤ 以下のダイアログが出力されたら「承認」をタップします。



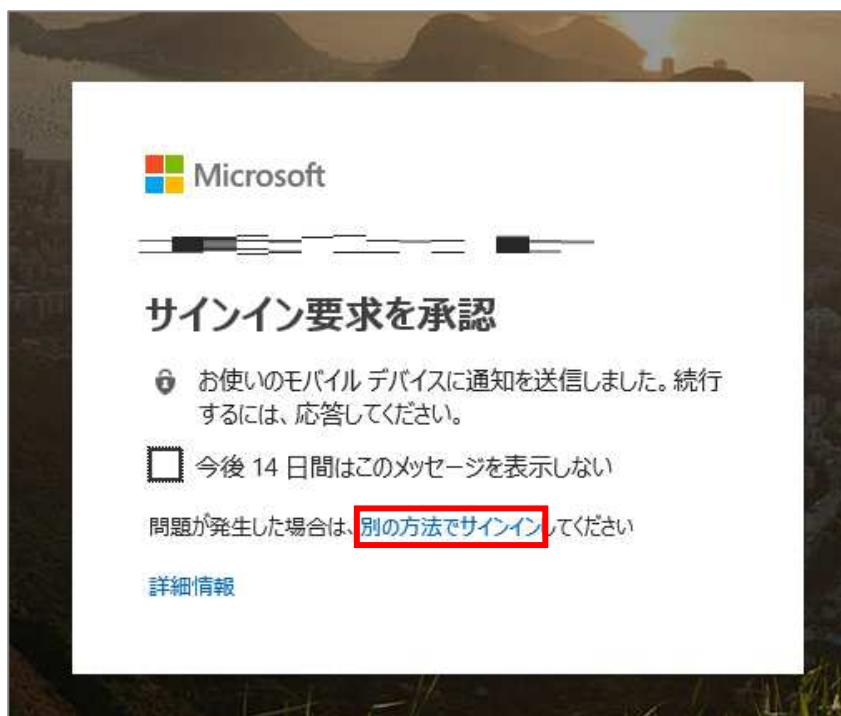
【PC 上での操作 その 2】

- ① PC 画面上で以下の画面が表示されたら、誤操作によるアプリの削除等モバイルアプリが使用できない場合に備え、連絡先電話番号を入力し、「次へ」をクリックします。
- 登録する電話番号の形式は、以下のどちらでもかまいません。
- 0 から始まる国内電話の形式 (例 : 03-1234-5678)
 - 国番号から始まる国際電話の形式 (例 : 813-1234-5678)



【モバイルアプリが使用できない場合のサインイン方法】

- ① 以下の画面で「別の方法でサインイン」をクリックします。



- ② 以下の画面で、登録した連絡先電話番号宛にショートメール(SMS)が送信する、または電話を掛けるかを選択します。電話番号は下2行のみ表示されます。



※ この操作によって「認証用電話」による認証を行うことができます。

各サインイン方法の詳細については、「3.5.2.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合」、「3.5.2.2 「認証用電話」 — 「電話する」を選択する場合」をそれぞれご参照ください。

③ 以下の画面でアプリ パスワード(アプリケーションパスワード)を発行します。

「完了」をクリックし、多要素認証方法の設定を完了します。

- ※ 「アプリ パスワード(アプリケーションパスワード)」は Outlook2016 以外のメールソフト (Outlook2013、Thunderbird 等) を利用している場合や、Outlook2016 で Exchange 以外の接続の種類 (POP や IMAP など) を選択している場合 (詳細は「4.6 Outlook2016 のメールの接続の種類の確認」をご参照ください。) に使用します。
- ※ 本画面以降、生成されたアプリケーションパスワードを確認することはできません。メモ帳などに保存してください。

Microsoft

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

ステップ 4: 既存のアプリケーションを引き続き使用する

Outlook、Apple Mail、また Microsoft Office などのアプリでは、アカウントの保護のために電話を使用することはできません。これらのアプリを使用するには、職場または学校アカウントのパスワードの代わりに新たなアプリパスワードを作成する必要があります。詳細情報を見る

このアプリ パスワードで今すぐ開始:

新しいアプリケーションパスワードを生成するには、このアプリ パスワードで今すぐ開始:

完了

©2018 Microsoft 法的情報 | プライバシー

2.1.5 「モバイルアプリ」 — 「確認コードを使用する」を選択する場合

モバイルアプリを使用する認証方法です。

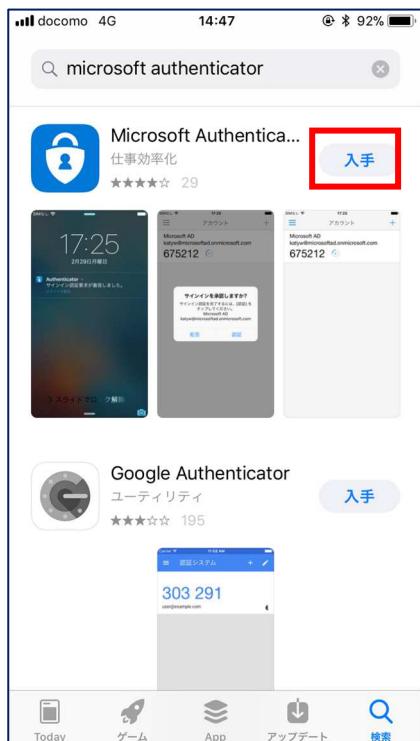
本認証方法による設定をする場合は、スマートフォンに「Microsoft Authenticator」(以下スマートフォンアプリ)を事前にインストールしてください。

インストール方法は以下の通りです。

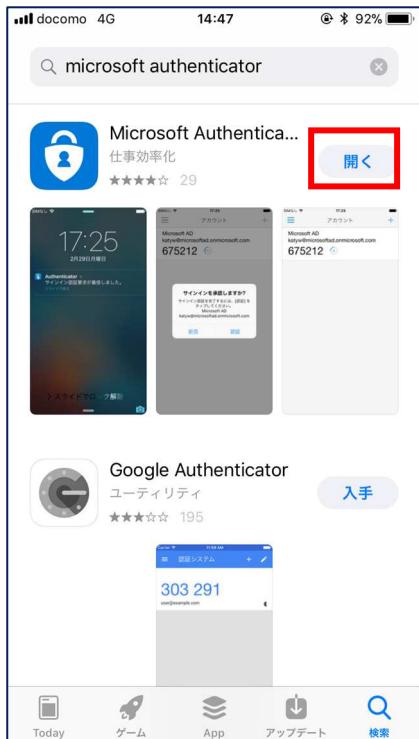
【iOS の場合】

- ① 「App Store」を起動して「Microsoft Authenticator」を検索します。

以下の画面が表示されたら画面右上の「入手」ボタンをタップします。



② 「入手」ボタンが「開く」ボタンになればインストール完了です。



【Android の場合】

① 「Google Play ストア」を起動して「Microsoft Authenticator」を検索します。

以下の画面が表示されたら画面右上の「インストール」ボタンをタップします。

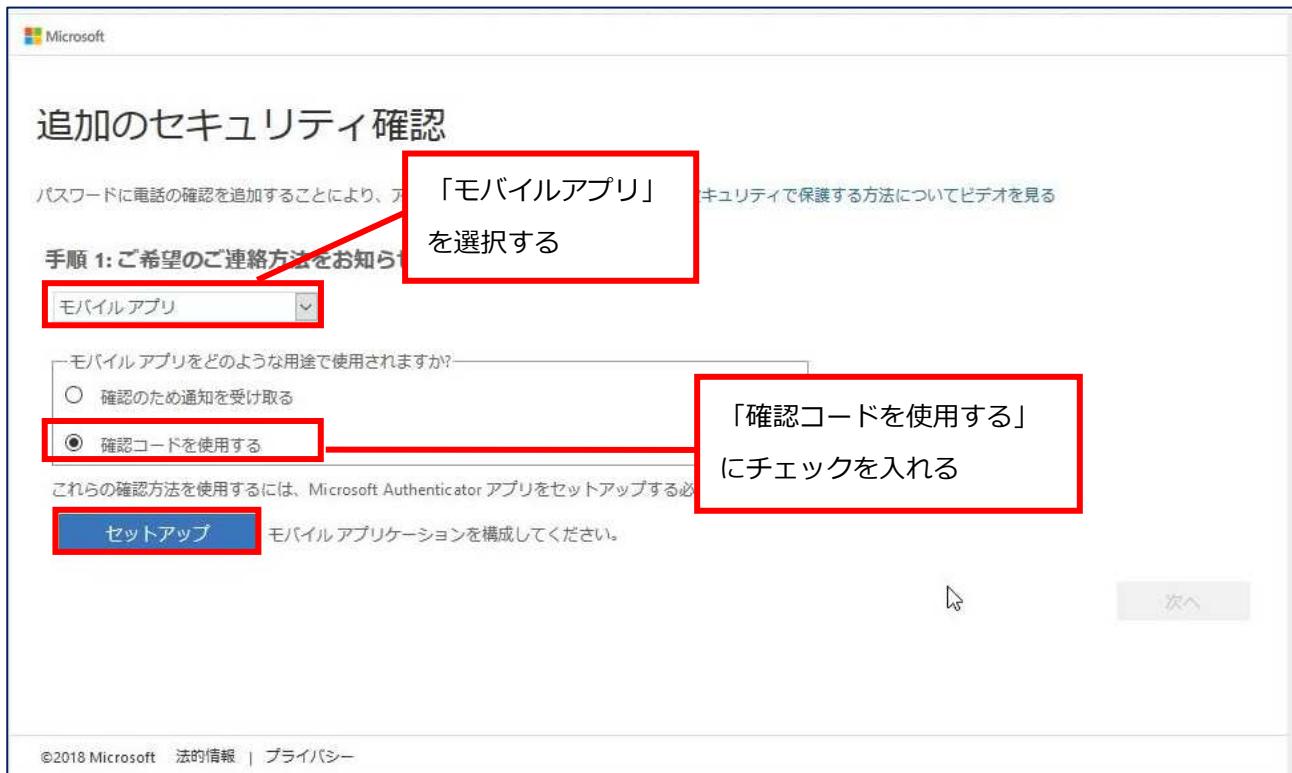


② 以下の画面が表示されたらインストール完了です。



【PC 上での操作 その1】

① PC 画面上で以下の通り設定し、「セットアップ」ボタンをクリックします。



② 「モバイルアプリケーションの構成」画面が表示されたらスマートフォンでの操作を実施します。



【iOS の場合】

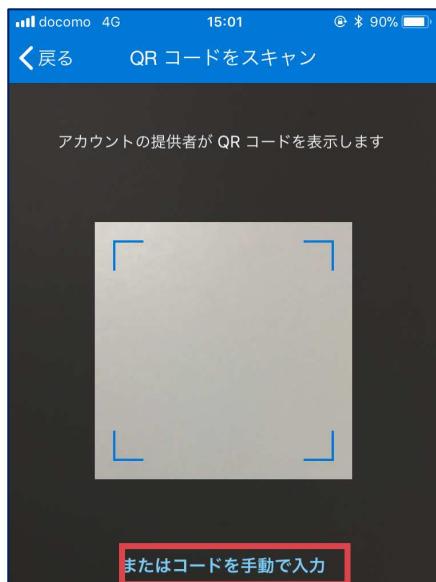
① スマートフォンアプリを起動して画面右上の「+」ボタンをタップします。



② 「アカウントの追加」画面で「職場または学校アカウント」をタップします。



③ 以下の画面から「モバイルアプリケーションの構成」画面に表示された QR コードを読み取り



もしくは「またはコードを手動で入力」をタップして表示された以下右の画面に QR コードと同時に表示されたコードと URL を直接入力して「完了」ボタンをタップします。



【Android の場合】

- ① スマートフォンアプリを起動して画面中央の「+」をタップします



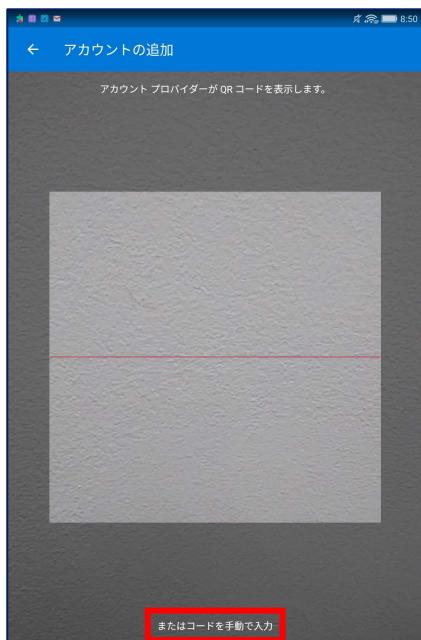
- ② 画面右上の「⋮」ボタンをタップして「アカウントの追加」を続けてタップします。



- ③ 「アカウントの追加」画面で「職場または学校アカウント」をタップします。



④ 以下の画面から「モバイルアプリケーションの構成」画面に表示された QR コードを読み取ります。

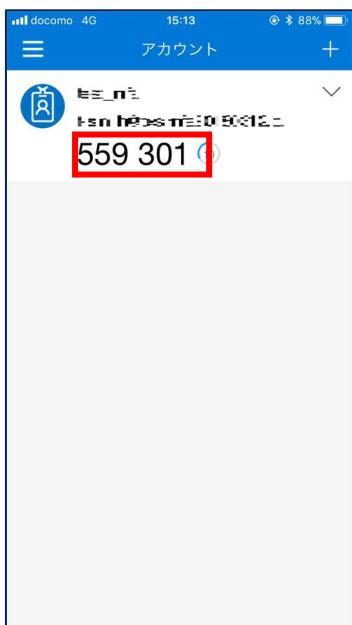


もしくは「またはコードを手動で入力」をタップし、表示された以下の画面に QR コードと同時に表示されたコードと URL を直接入力して「完了」ボタンをタップします。

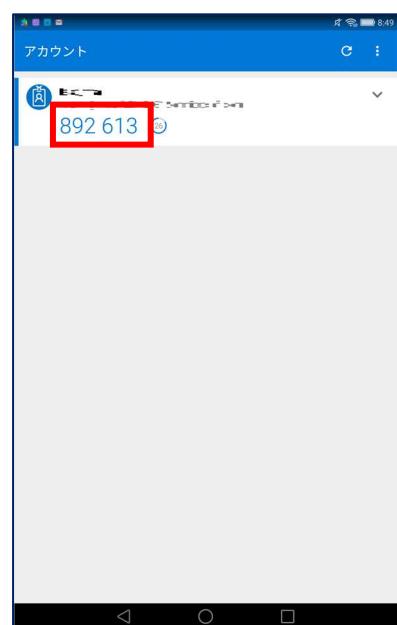


- ⑤ モバイルアプリケーションにアカウントが追加されると、以下のように 6 行の確認コードが表示されます。

【iOS 画面】



【Android 画面】

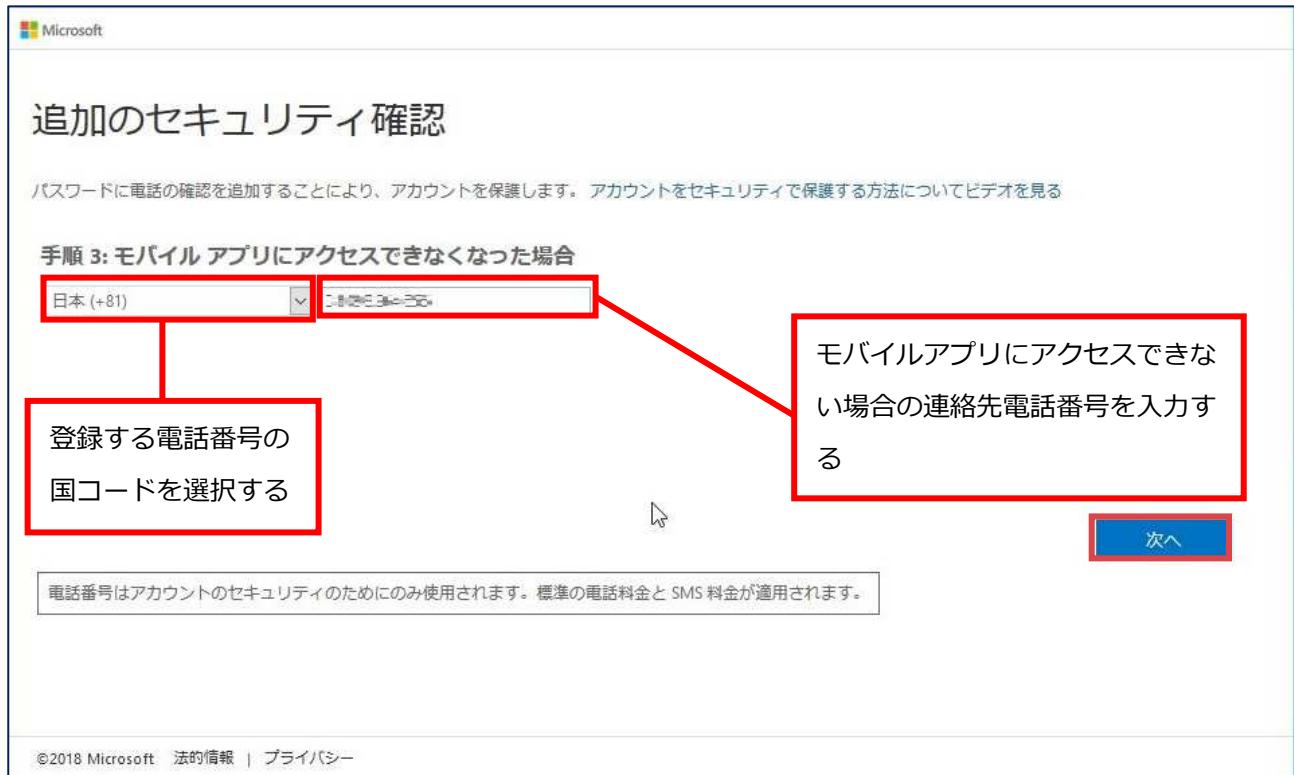


【PC 上での操作 その 2】

- ① 確認コードを入力して、「確認」をクリックします。

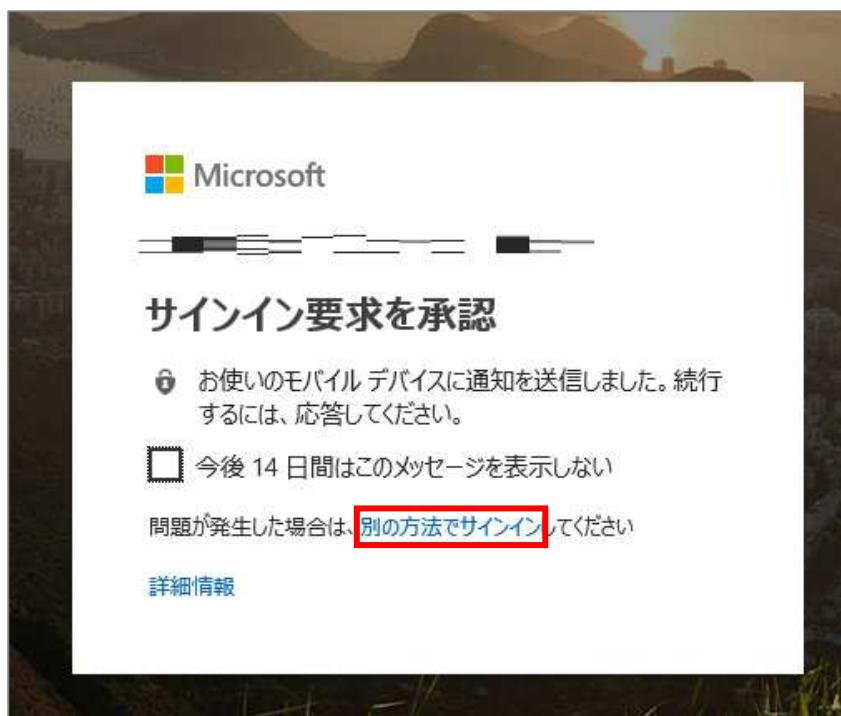


- ② PC 画面上で以下の画面が表示されたら、誤操作によるアプリの削除等モバイルアプリが使用できない場合に備え、連絡先電話番号を入力し、「次へ」をクリックします。
- 登録する電話番号の形式は、以下のどちらでもかまいません。
- 0 から始まる国内電話の形式 (例 : 03-1234-5678)
 - 国番号から始まる国際電話の形式 (例 : 813-1234-5678)



【モバイルアプリが使用できない場合のサインイン方法】

- ① 以下の画面で「別の方法でサインイン」をクリックします。



- ② 以下の画面で、登録した連絡先電話番号宛にショートメール(SMS)が送信する、または電話を掛けるかを選択します。電話番号は下2行のみ表示されます。



※ この操作によって「認証用電話」による認証を行うことができます。

各サインイン方法の詳細については、「3.5.2.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合」、「3.5.2.2 「認証用電話」 — 「電話する」を選択する場合」をそれぞれご参照ください。

【PC 上での操作 その 3】

① 以下の画面でアプリ パスワード(アプリケーションパスワード)を発行します。

「完了」をクリックし、多要素認証方法の設定を完了します。

※ 「アプリ パスワード(アプリケーションパスワード)」は Outlook2016 以外のメールソフト (Outlook2013、Thunderbird 等) を利用している場合や、Outlook2016 で Exchange 以外の接続の種類 (POP や IMAP など) を選択している場合 (詳細は「4.6 Outlook2016 のメールの接続の種類の確認」をご参照ください。) に使用します。

※ 本画面以降、生成されたアプリケーションパスワードを確認することはできません。メモ帳などに保存してください。

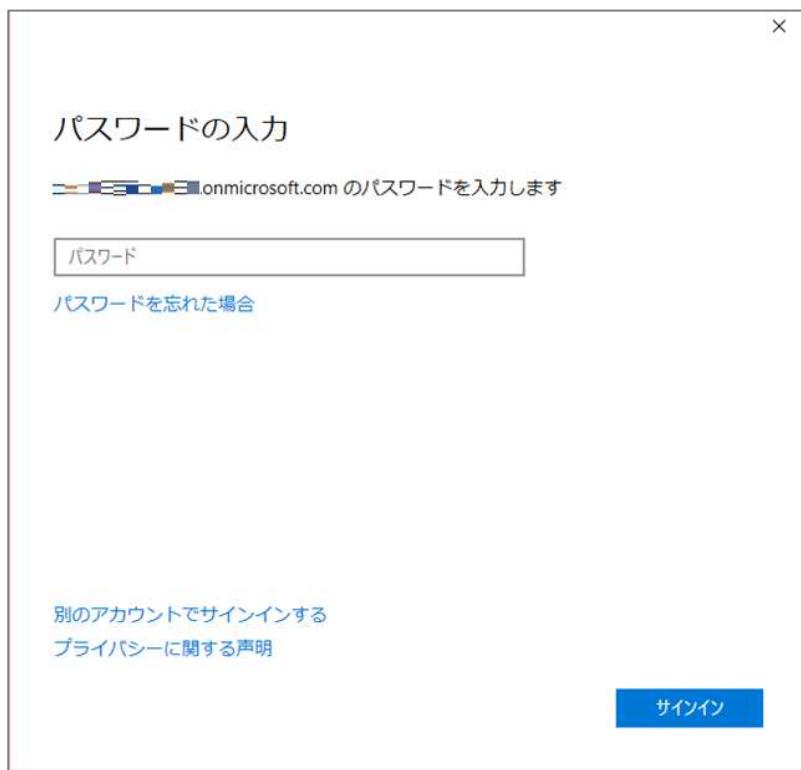


3 メーラーの多要素認証

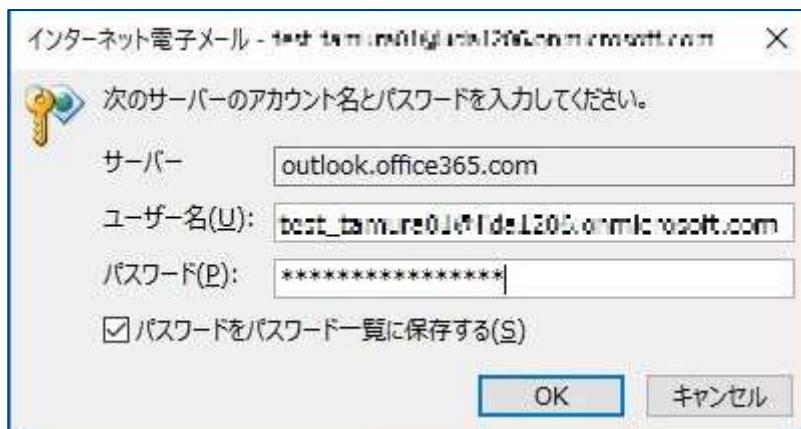
3.1 Outlook2016

Outlook2016 を使用している場合は、本章を確認します。

※ 「2.1 多要素認証方法を選択する」の設定を行っていない場合は、以下の画面が表示されます。通常のパスワードを入力し、「サインイン」をクリックすることで、多要素認証方法の設定を行うことができます。設定方法は「2.1 多要素認証方法を選択する」をご参照ください。



Exchange 以外の接続の種類（POP や IMAP など）を選択している場合は、上記の画面ではなく下記の画面が表示される場合があります。その場合は、「3.1.1.6 POP または IMAP 接続の場合」をご参照ください。



3.1.1 Outlook2016 で認証を行う

「2.1 多要素認証方法を選択する」で選択した内容により、Outlook2016 の認証手順が異なりますので、ご自身の設定を確認してください。

Outlook2016 では、一度認証を行うと認証情報が 90 日間保持され、起動の度に保持期限が更新されるため、再認証は不要です。

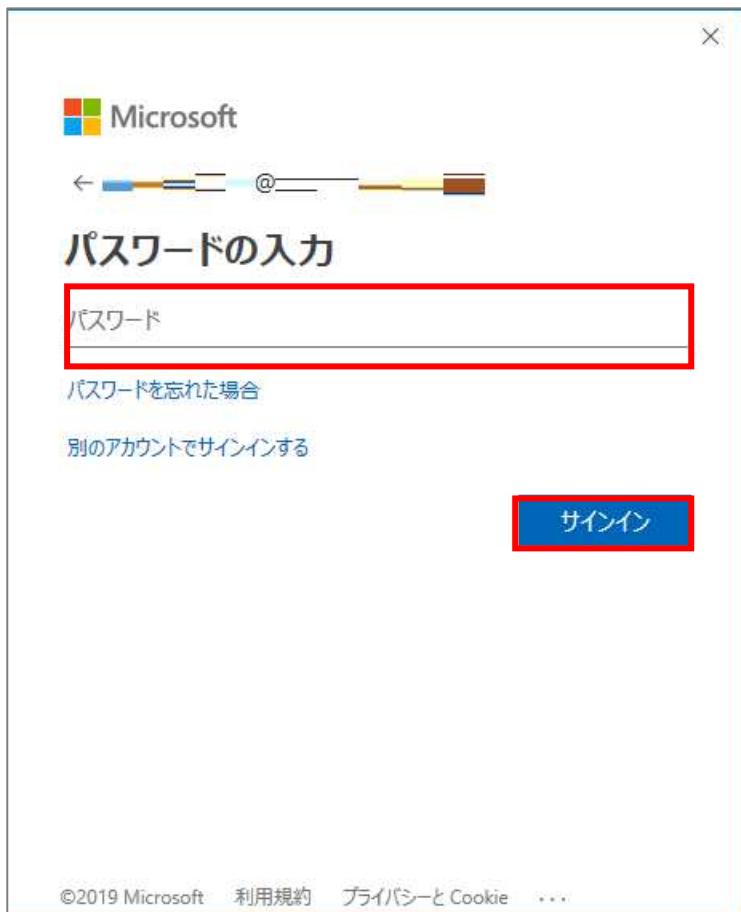
多要素認証の設定		Outlook2016 の認証手順
項目	方法	
認証用電話	テキストメッセージ (ショートメール) ※ 推奨方式	3.1.1.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合
	電話	3.1.1.2 「認証用電話」 — 「電話する」を選択した場合
会社電話	利用不可	3.1.1.3 「会社電話」を選択した場合
モバイルアプリ	通知	3.1.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択した場合
	確認コード	3.1.1.5 「モバイルアプリ」 — 「確認コードを使用する」を選択した場合

3.1.1.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合

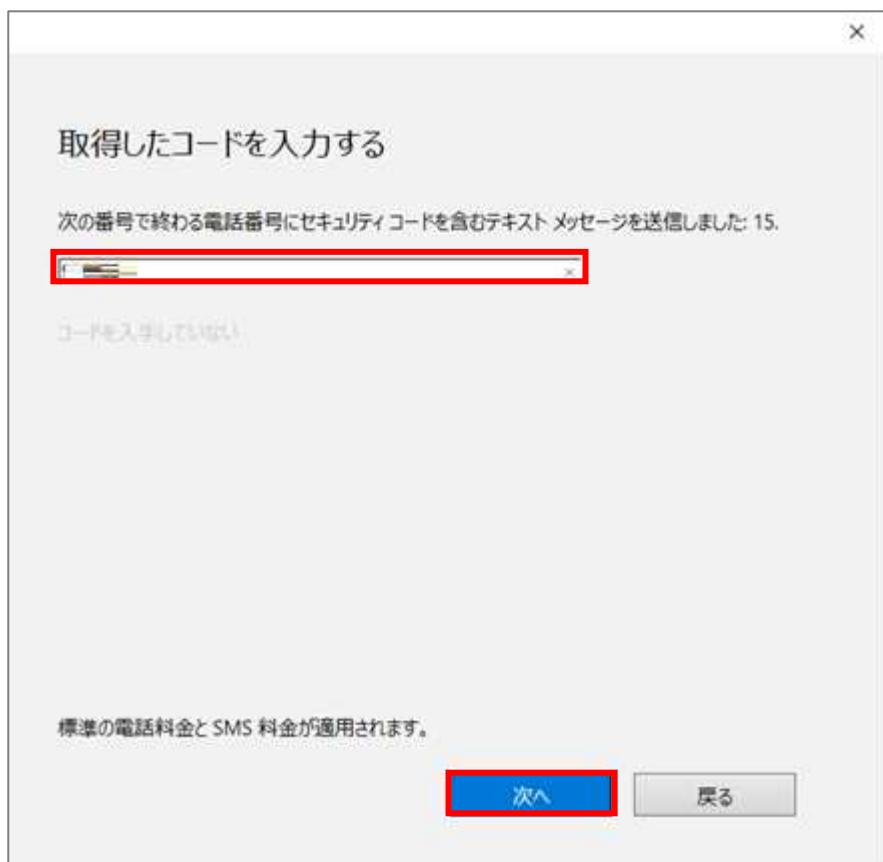
テキストメッセージによる認証を選択した場合の認証方法は、以下の通りです。

- ① Outlook2016 を起動します。

起動時に ID/パスワードの入力画面が表示される場合があります。その場合は、パスワードを入力し、「サインイン」をクリックします。



- ② 登録した電話番号宛てに自動でショートメール(SMS)で 6 行の数字のコードが送信されるため、記載されたコードを以下の画面の入力フォームに入力し、「次へ」をクリックします。



- ③ Outlook2016 の画面に自動で切り替わります。

3.1.1.2 「認証用電話」 — 「電話する」を選択した場合

電話による認証を選択した場合の認証方法は、以下の通りです。

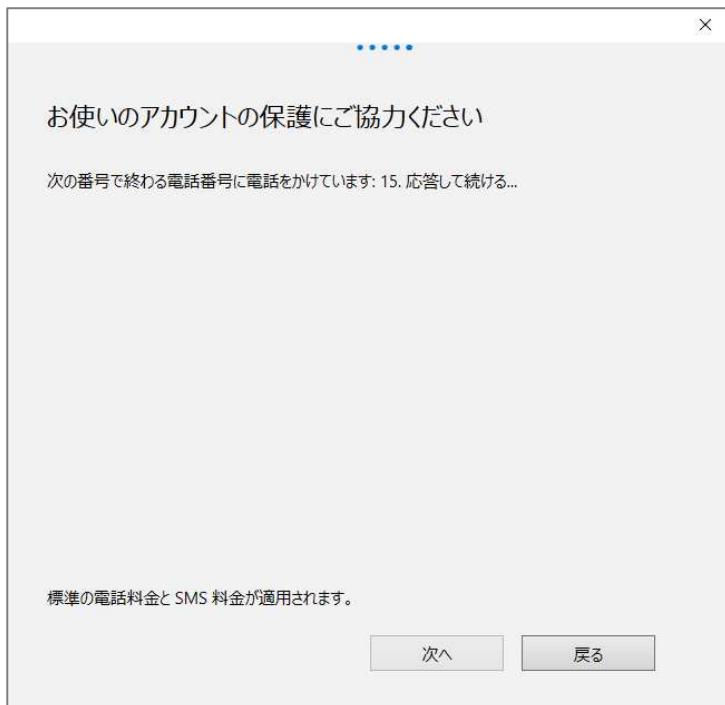
- ① Outlook2016 を起動します。

起動時に ID/パスワードの入力画面が表示される場合があります。その場合は、パスワードを入力し、「サインイン」をクリックします。

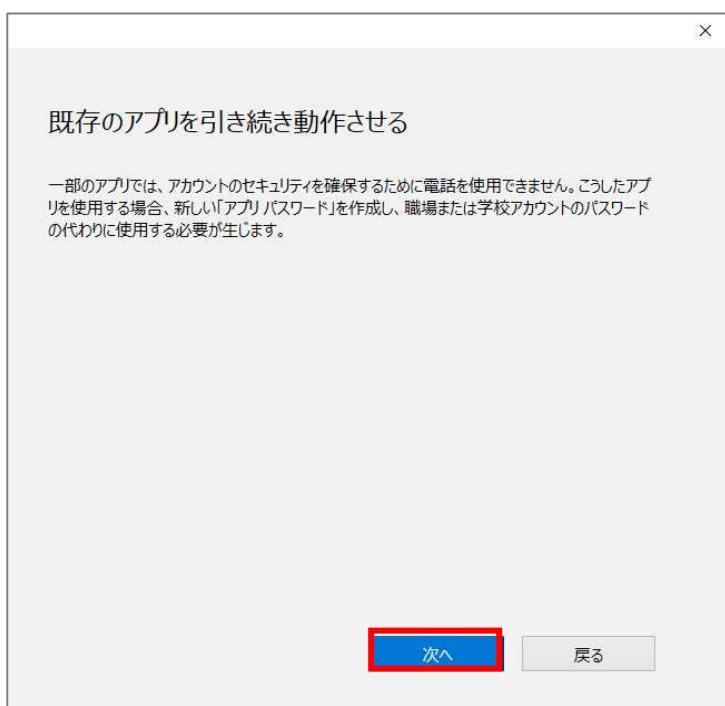


- ② 以下の画面が表示されたら、登録した電話番号宛てに電話が掛かります。音声の指示に従って操作を行います。

(「#」を押すように音声指示があります。アナログ回線の場合は「*」を押してから「#」を押す必要があります。)



- ③ 「次へ」をクリックします。



- ④ Outlook2016 の画面に自動で切り替わります。

3.1.1.3 「会社電話」を選択した場合

システム連携された会社電話のことを指すため、本学では利用できません。

3.1.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択した場合

通知による認証を選択した場合の認証方法は、以下の通りです。

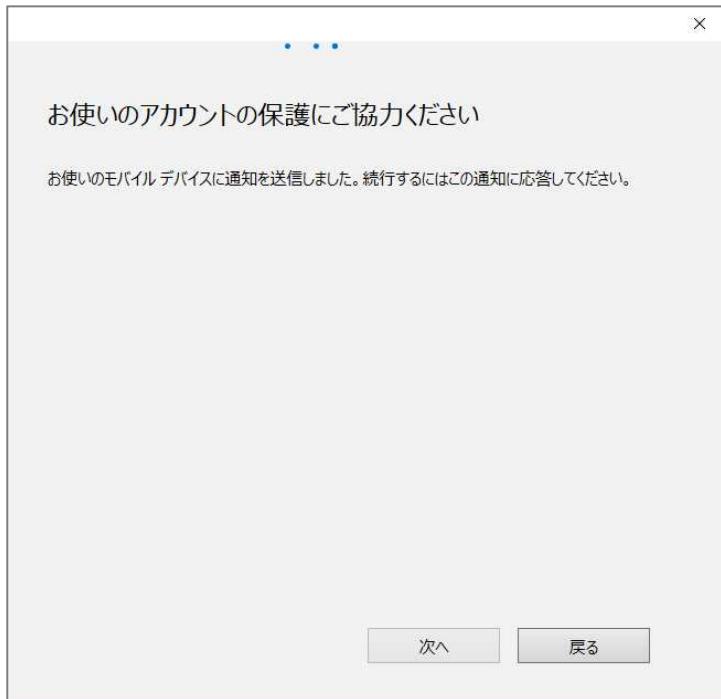
- ① Outlook2016 を起動します。

起動時に ID/パスワードの入力画面が表示される場合があります。その場合は、パスワードを入力し、「サインイン」をクリックします。

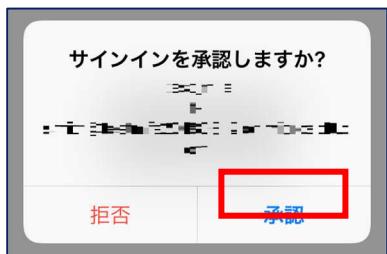


- ② モバイルアプリを起動すると、サインインの許可を求めるダイアログが表示されるため、「承認」をタップします。

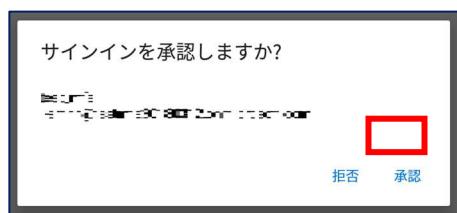
【Outlook2016 の画面】



【iOS 画面】

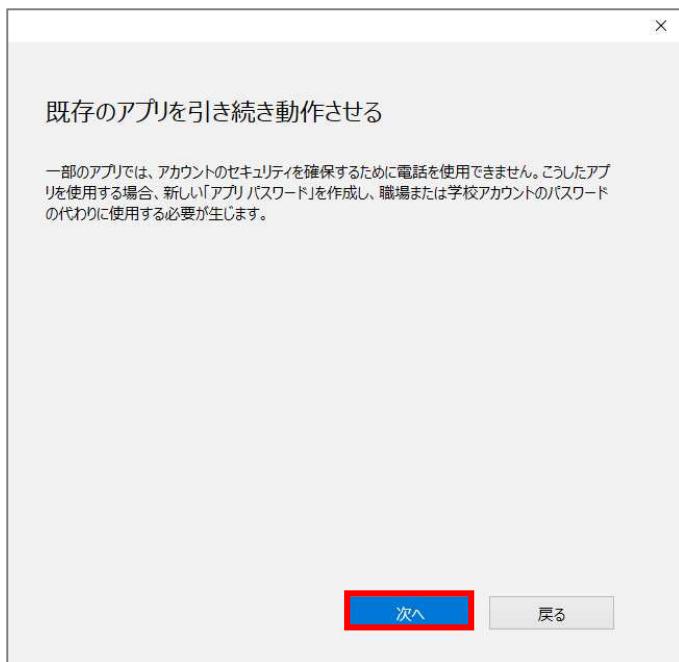


【Android 画面】



③ 「次へ」をクリックします。

【Outlook2016】



④ Outlook2016 の画面に自動で切り替わります。

3.1.1.5 「モバイルアプリ」 — 「確認コードを使用する」を選択した場合

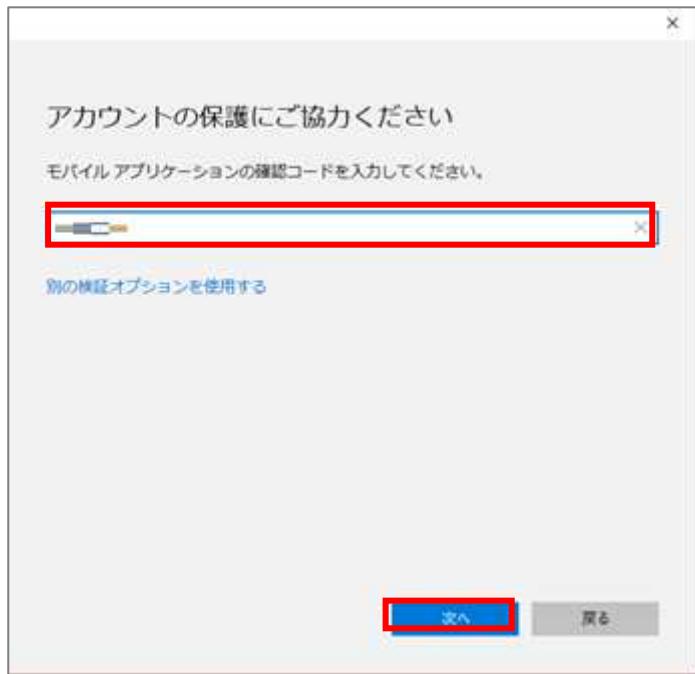
確認コードによる認証を選択した場合の認証方法は、以下の通りです。

- ① Outlook2016 を起動します。

起動時に ID/パスワードの入力画面が表示される場合があります。その場合は、パスワードを入力し、「サインイン」をクリックします。



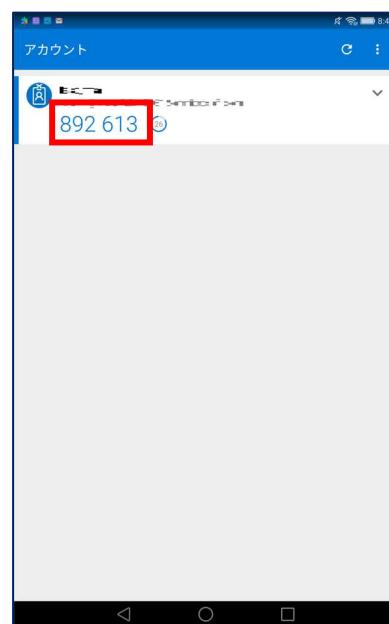
- ② 入力フォームにモバイルアプリケーションに表示された 6 行の認証コードを入力し、「次へ」をクリックします。



【iOS画面】



【Android 画面】



- ③ Outlook2016 の画面に自動で切り替わります。

3.1.1.6 POP または IMAP 接続の場合

接続方法が POP または IMAP の場合の認証方法は、以下の通りです。

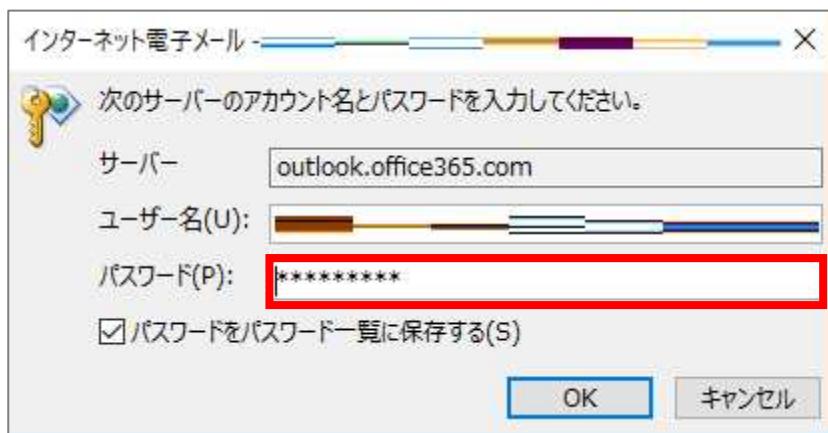
POP または IMAP 接続では、一度アプリケーションパスワードによる認証を行うことで認証情報が保持されるため、再認証は不要です。

【POP 接続】

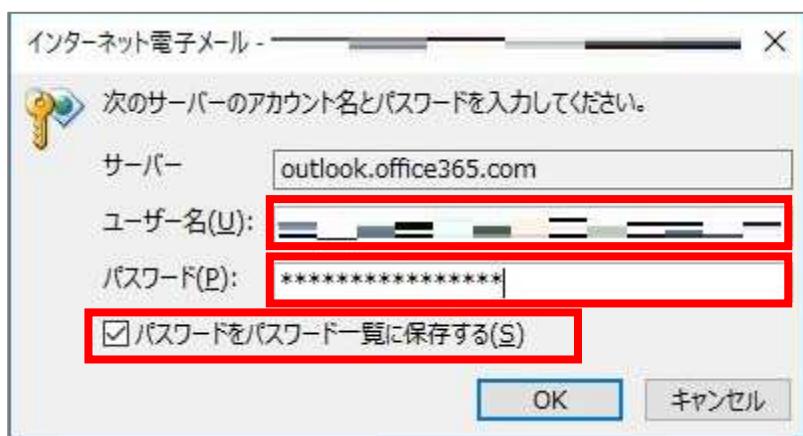
① Outlook2016 を起動します。

② 以下の画面が表示されます。

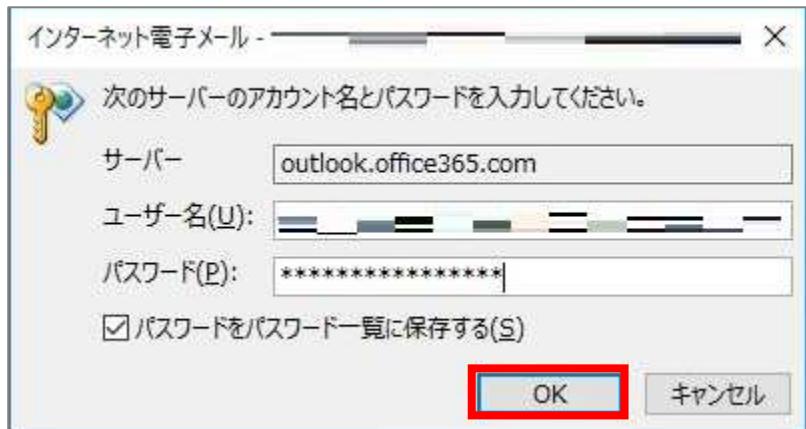
入力フォームの「パスワード」に、今まで使用していたパスワードが入力済みの状態で表示されるため、削除します。



③ 入力フォームの「ユーザー名」に個人メールアドレス、「パスワード」に「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力し、「パスワードをパスワード一覧に保存する」にチェックを入れます。



④ 「OK」をクリックします。



※ アプリケーションパスワードを入力して認証されたことが確認できた後は、第3者に漏洩することを防ぐため、アプリケーションパスワードのメモ等は必ず削除してください。

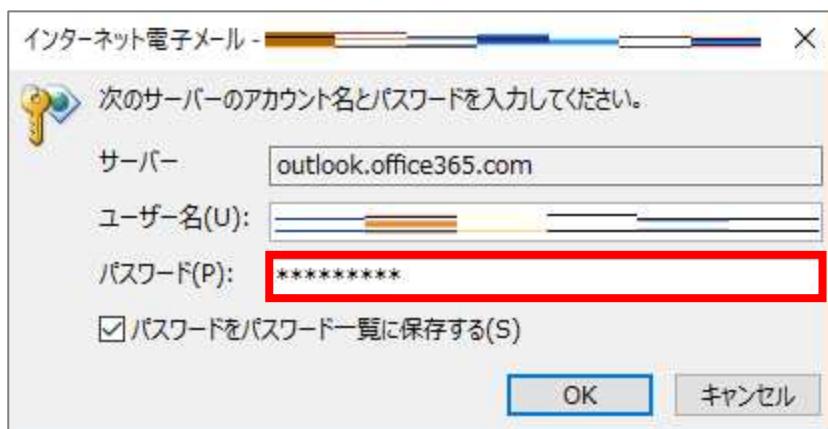
⑤ Outlook2016の画面に自動で切り替わります。

【IMAP 接続】

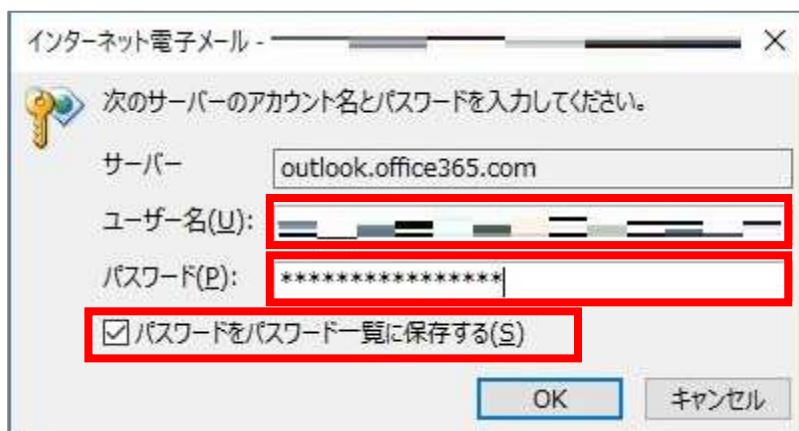
① Outlook2016 を起動します。

② 以下の画面が表示されます。

入力フォームの「パスワード」に、今まで使用していたパスワードが入力済みの状態で表示されるため、削除します。

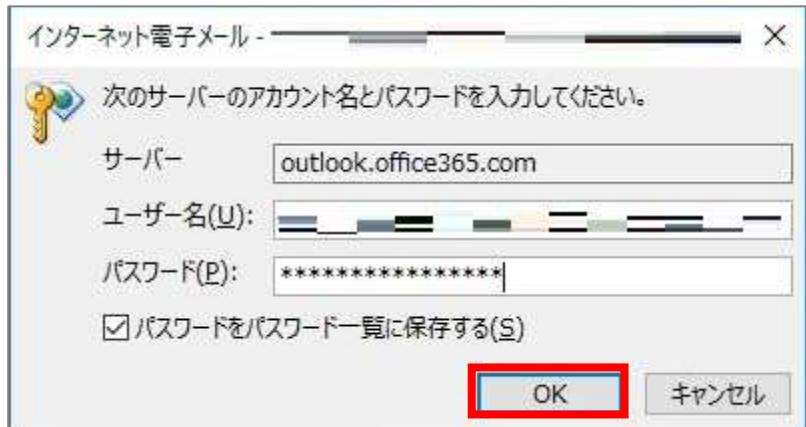


③ 入力フォームの「ユーザー名」に個人メールアドレス、「パスワード」に「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力し、「パスワードをパスワード一覧に保存する」にチェックを入れます。



④ 「OK」をクリックします。

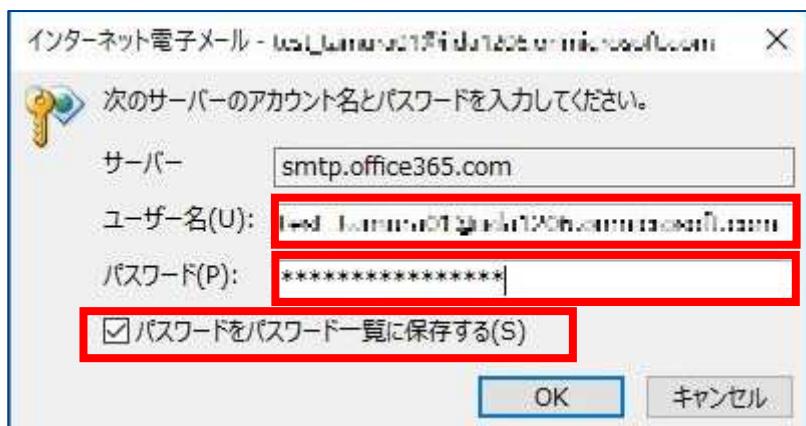
※ 再度以下の画面が表示されることがあります。その場合は、③と同様に入力フォームの「ユーザー名」に個人メールアドレス、「パスワード」に「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力し、「パスワードをパスワード一覧に保存する」にチェックを入れ、「OK」をクリックします。



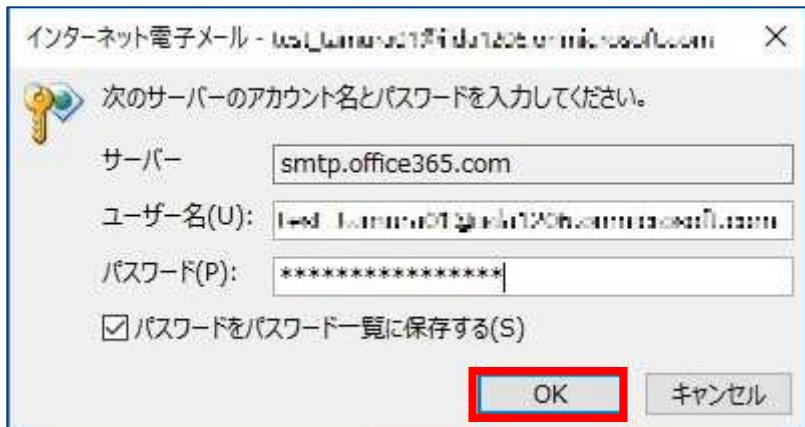
⑤ Outlook2016 の画面に自動で切り替わります。

⑥ IMAP ではメールの送信時も同様に以下の画面が表示されます。

入力フォームの「ユーザー名」に個人メールアドレス、「パスワード」に「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力し、「パスワードをパスワード一覧に保存する」にチェックを入れます。



⑦ 「OK」をクリックします。



※ アプリケーションパスワードを入力して認証されたことが確認できた後は、第3者に漏洩することを防ぐため、アプリケーションパスワードのメモ等は必ず削除してください。

3.1.2 Outlook2016 からメールを確認する

正常に認証が完了すると、自動でメールが受信され、通常通りメールを確認することができます。

Outlook2016 を 90 日間一度も起動しなかった場合は、再認証が必要です。(IMAP、POP 接続時の場合はアプリケーションパスワードのため再認証不要。) 「3.1.1 Outlook2016 で認証を行う」から再度、手順を実施してください。

3.2 Outlook2013

Outlook2013 を使用している場合は、本章を確認します。

3.2.1 Outlook2013 を起動する

PC を立ち上げ、Outlook2013 を起動します。

3.2.2 Outlook2013 で認証を行う

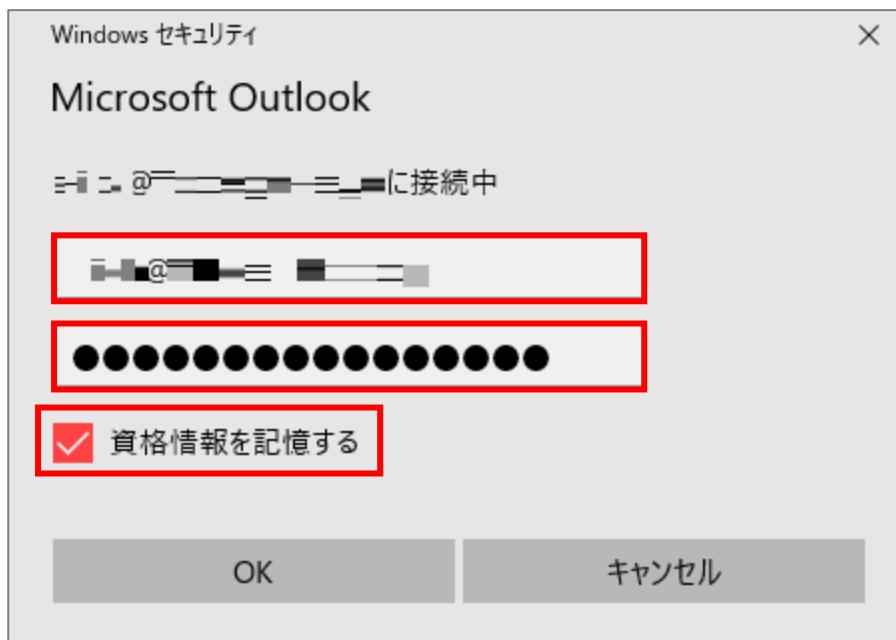
Outlook2013 で認証を行う方法は、以下の通りです。

Outlook2013 では、一度アプリケーションパスワードによる認証を行うことで認証情報が保持されるため、再認証は不要です。

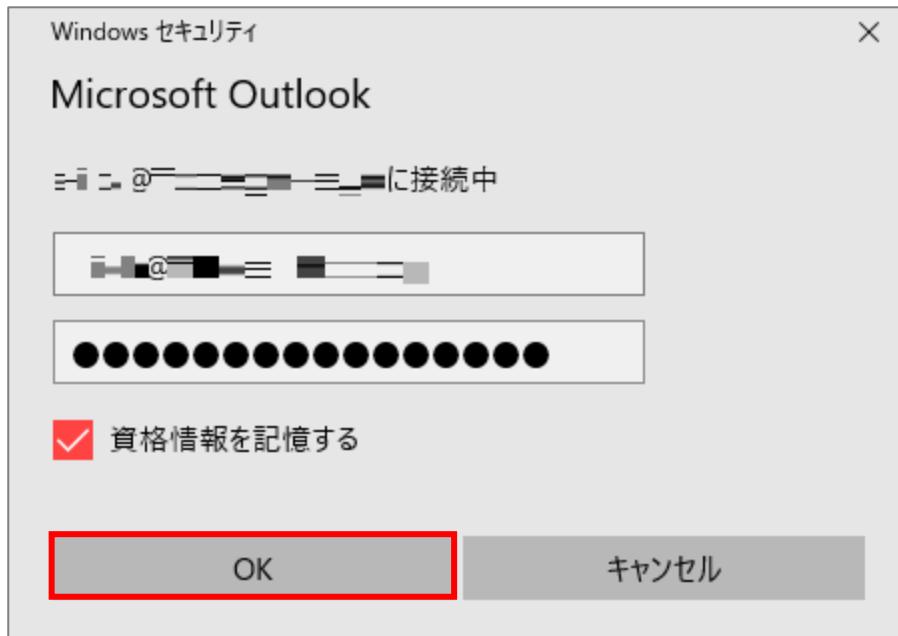
3.2.2.1 アプリケーションパスワードを入力する

アプリケーションパスワードを入力する方法は、以下の通りです。

- ① Outlook2013 を起動します。
- ② 以下の画面の入力フォームに個人メールアドレスと「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力し、「資格情報を記憶する」にチェックを入れます。
※ 学外から接続する場合は、通常のパスワードではエラーになり、認証することができません。



③ 「OK」をクリックします。



※ アプリケーションパスワードを入力して認証されたことが確認できた後は、第3者に漏洩することを防ぐため、アプリケーションパスワードのメモ等は必ず削除してください。

④ Outlook2013 の画面に自動で切り替わります。

3.2.3 Outlook2013 からメールを確認する

正常に認証が完了すると、自動でメールが受信され、通常通りメールを確認することができます。

3.3 Thunderbird

Thunderbird を使用している場合は、本章を確認します。

多要素認証が有効なユーザー アカウントを Thunderbird に登録して利用する場合、アプリケーション パスワードを使用する必要があります。

アプリケーション パスワードによる認証が発生するタイミングは以下の通りです。

- **Thunderbird 起動時 (IMAP/POP 認証)**

Thunderbird を起動した際、受信サーバー (IMAP/POP) との認証が都度必要になりますが、一度認証時に「パスワード マネージャーにこのパスワードを保存する。」にチェックを入れた場合、以後 Thunderbird 起動時に認証を求められることはなくなります。

- **Thunderbird を使用してのメール送信時 (SMTP 認証)**

メール送信する際、送信サーバー (SMTP) との認証が都度必要になりますが、一度認証時に「パスワード マネージャーにこのパスワードを保存する。」にチェックを入れた場合、以後メール送信時に認証を求められることはなくなります。

3.3.1 Thunderbird を起動する

PC を立ち上げ、Thunderbird を起動します。

3.3.2 Thunderbird で認証を行う

Thunderbird で認証を行う方法は以下の通りです。

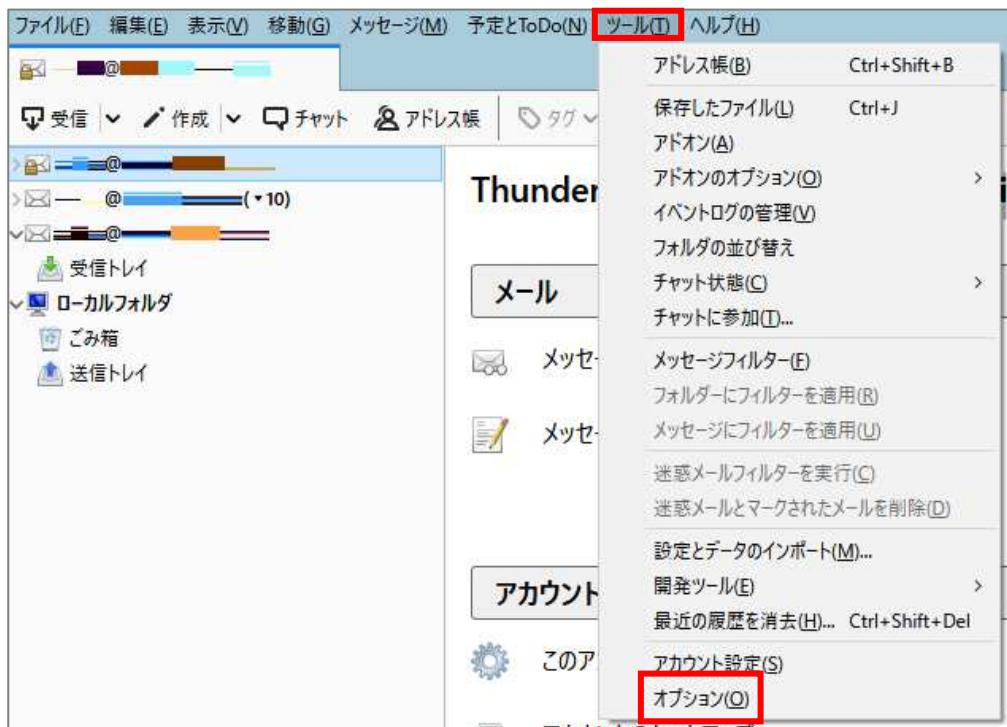
3.3.2.1 「保存されたログイン情報」を削除する

Thunderbird を使用する場合、アプリケーションパスワードで認証を行うために、Thunderbird から今まで使用していたパスワード情報を削除する必要があります。今まで使用していたパスワード情報を削除しなかった場合、学外から Thunderbird を使用することができなくなります。

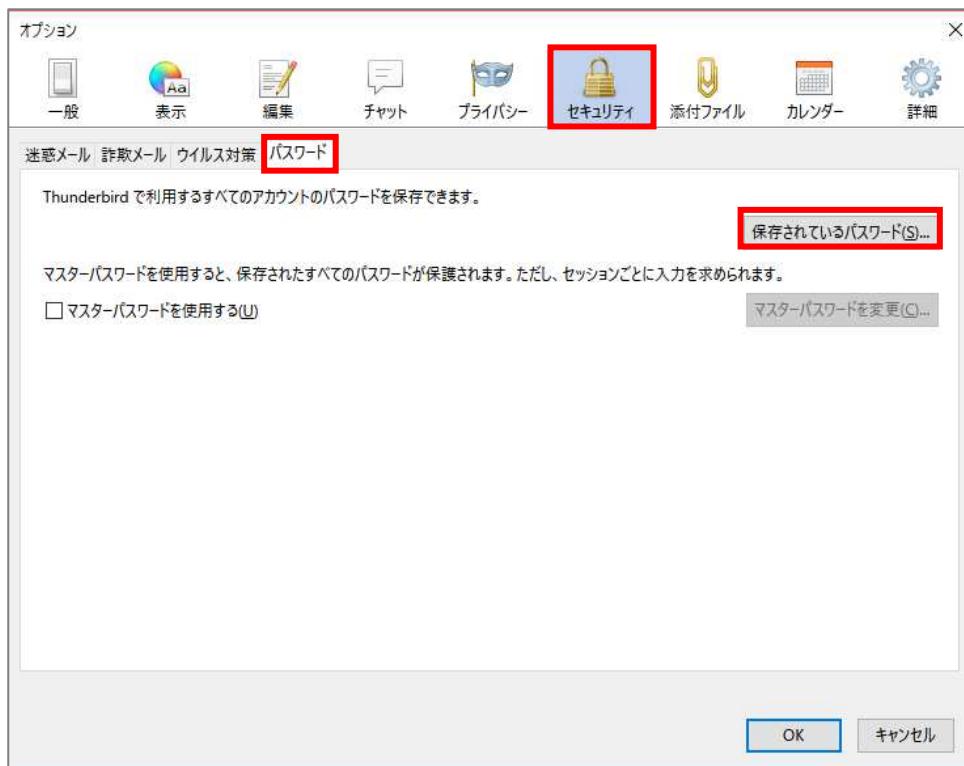
一度パスワード情報を削除した場合、以降アプリケーションパスワードを変更しない限り、パスワード情報を削除する必要はありません。

パスワード情報を削除する方法は以下の通りです。

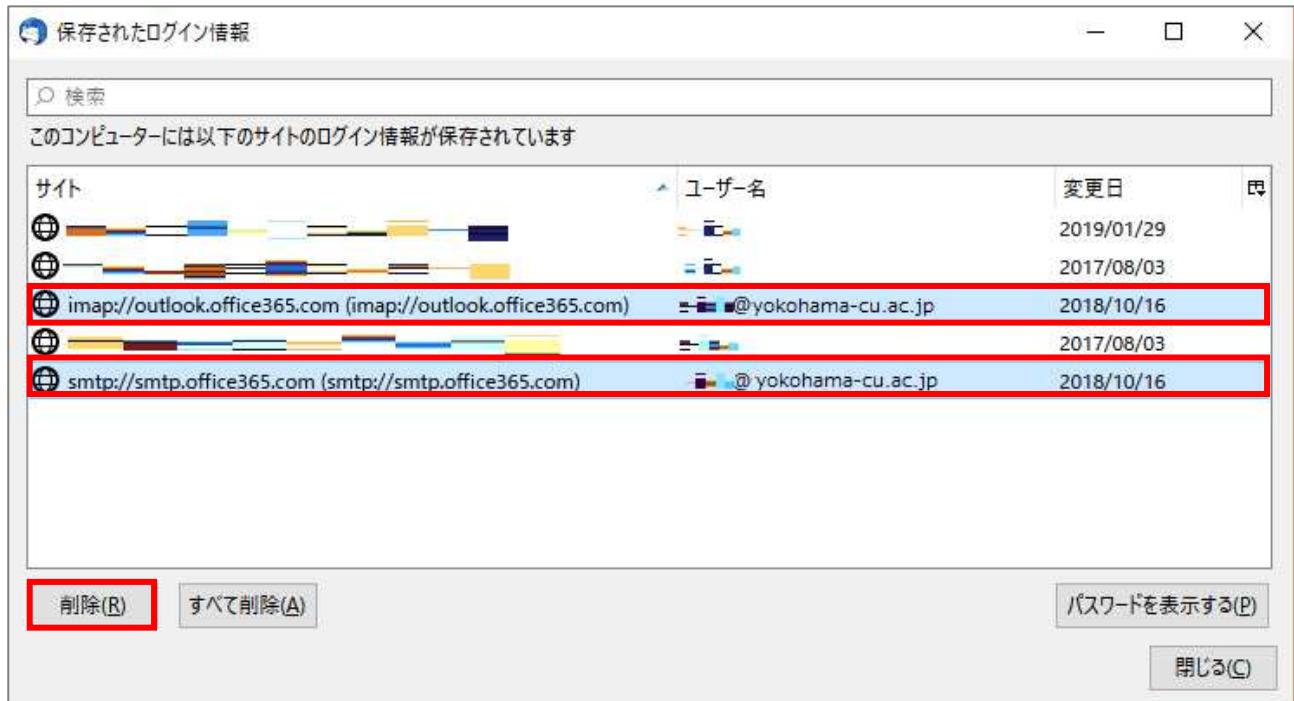
- ① 「ツール」をクリックし、表示されたメニューから「オプション」をクリックします。



- ② 「セキュリティ」をクリックし、表示されたタブから「パスワード」を選択、「保存されているパスワード」をクリックします。



- ③ 「サイト」欄に「imap://imap-mail.outlook.com(imap://imap-mail.outlook.com)」、「smtp://smtp-mail.outlook.com(smtp://smtp-mail.outlook.com)」、「pop://pop-mail.outlook.com(pop://pop-mail.outlook.com)」のいずれかが表示されます。表示されたものをすべて選択し、「ユーザー名」が本学のメールアドレスであることを確認します。他に選択されているものがないことを確認し、「削除」をクリックします。



- ④ Thunderbird を再起動します。

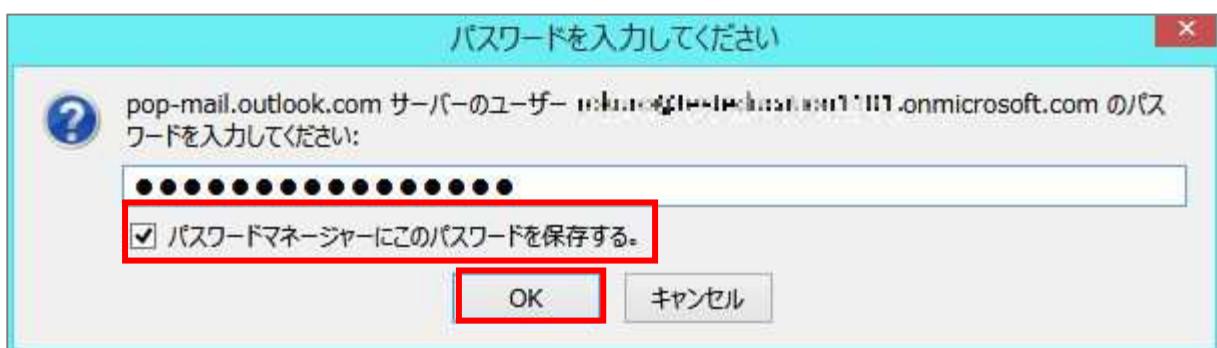
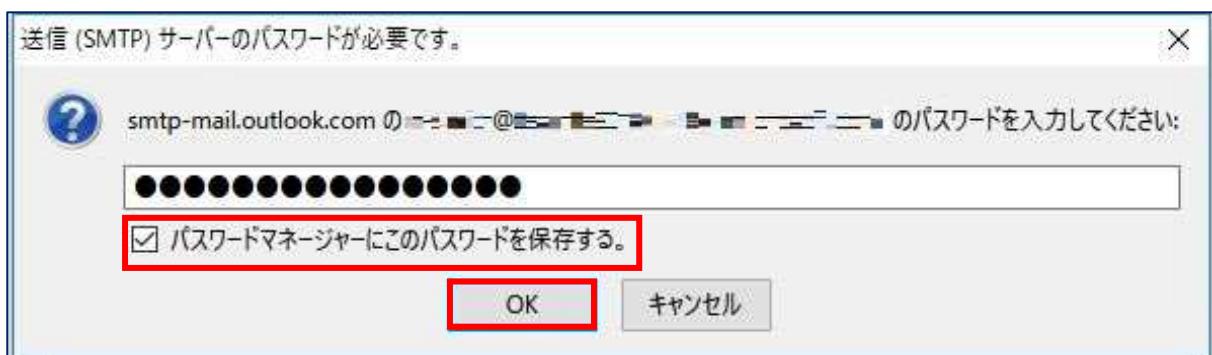
3.3.2.2 アプリケーションパスワードを入力する

アプリケーションパスワードによる認証が発生したときの設定方法は以下の通りです。

- ① Thunderbird でメールを送信または受信をした後、以下のいずれかの認証ダイアログが表示されたら、「新しいパスワードを入力」をクリックします。表示されない場合は②の手順に進みます。



- ② 以下のいずれかの認証ダイアログが表示されたら、入力フォームに「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力します。「パスワードマネージャーにこのパスワードを保存する。」の左側のチェックボックスにチェックを入れ、「OK」をクリックします。



- ※ アプリケーションパスワードを入力して認証されたことが確認できた後は、第3者に漏洩することを防ぐため、アプリケーションパスワードのメモ等は必ず削除してください。

3.3.3 Thunderbird からメールを確認する

正常に認証が完了すると、自動でメールが受信され、通常通りメールを確認することができます。

3.4 MacMail

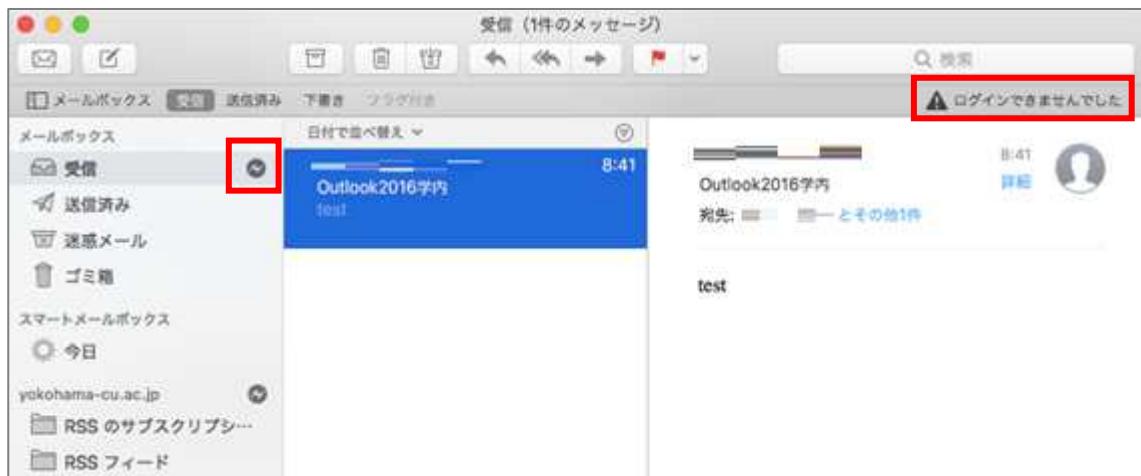
MacMail を使用している場合は、本章を確認します。

多要素認証が有効なユーザーアカウントを MacMail に登録して利用する場合、アプリケーションパスワードを使用する必要があります。

3.4.1 MacMail を起動する

PC を立ち上げ、MacMail を起動します。

左メニューの「受信」の横にオフラインマーク、右上に「ログインできませんでした」が表示されていることを確認します。



3.4.2 MacMail で認証を行う

MacMail で認証を行う方法は以下の通りです。

3.4.2.1 アプリケーションパスワードを入力する

アプリケーションパスワードによる認証が発生したときの設定方法は以下の通りです。

- ① 「ログインできませんでした」をクリックし、認証ダイアログを表示します。

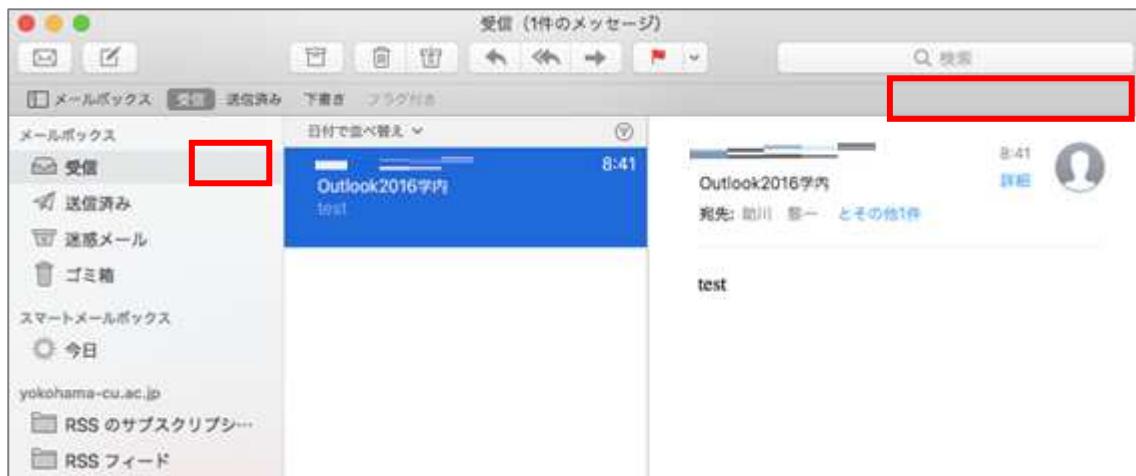


- ② パスワードの入力フォームに、「2.1 多要素認証方法を選択する」で取得したアプリケーションパスワードを入力し、「OK」をクリックします。



※ アプリケーションパスワードを入力して認証されたことが確認できた後は、第3者に漏洩することを防ぐため、アプリケーションパスワードのメモ等は必ず削除してください。

- ③ 左メニューの「受信」のオフラインマーク、右上の「ログインできませんでした」が表示されていないことを確認します。



3.4.3 MacMail からメールを確認する

正常に認証が完了すると、自動でメールが受信され、通常通りメールを確認することができます。

3.5 WEB ブラウザ(Microsoft Edge)

Web ブラウザを使用している場合は、本章を確認します。

本章では、Web ブラウザの代表として Microsoft Edge の画面を使用します。

3.5.1 Office365 サインイン画面を表示する

以下の URL にアクセスし、Office 365 サインイン画面を表示します。

<http://portal.office.com/>

3.5.2 Office 365 で認証を行う

Office 365 で認証を行う方法は以下の通りです。

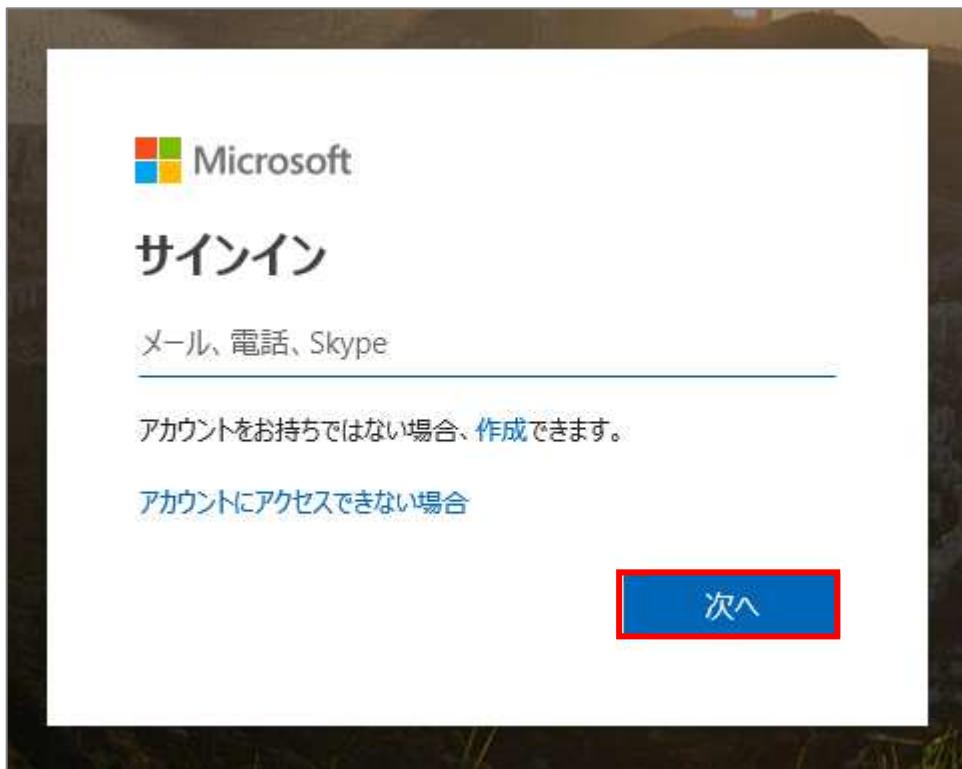
「2.1 多要素認証方法を選択する」で選択した内容により、手順が異なりますので、ご自身の設定を確認してください。

多要素認証の設定		WEB ブラウザ(Microsoft Edge)の認証手順
項目	方法	
認証用電話	テキストメッセージ (ショートメール) ※ 推奨方式	3.5.2.1「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合
	電話	3.5.2.2「認証用電話」 — 「電話する」を選択する場合
会社電話	利用不可	3.5.2.3「会社電話」を設定した場合はじめに(多要素認証の導入)
モバイルアプリ	通知	3.5.2.4「モバイルアプリ」 — 「確認のため通知を受け取る」を選択した場合
	確認コード	3.5.2.5「モバイルアプリ」 — 「確認コードを使用する」を選択した場合

3.5.2.1 「認証用電話」 — 「テキストメッセージでコードを送信する」を選択した場合

テキストメッセージによる認証を選択した場合の認証方法は、以下の通りです。

- ① Office 365 の「サインイン画面」で個人メールアドレスを入力し、「次へ」ボタンをクリックします。



- ② 「パスワードの入力」画面でパスワードを入力し、「サインイン」ボタンをクリックします。

- ③ 登録した電話番号宛にテキストメッセージ(ショートメール)が送信されるので、内容に記載された確認コードを画面の入力フォームに入力し、「検証」をクリックします。Office 365 ホーム画面には自動で切り替わります。

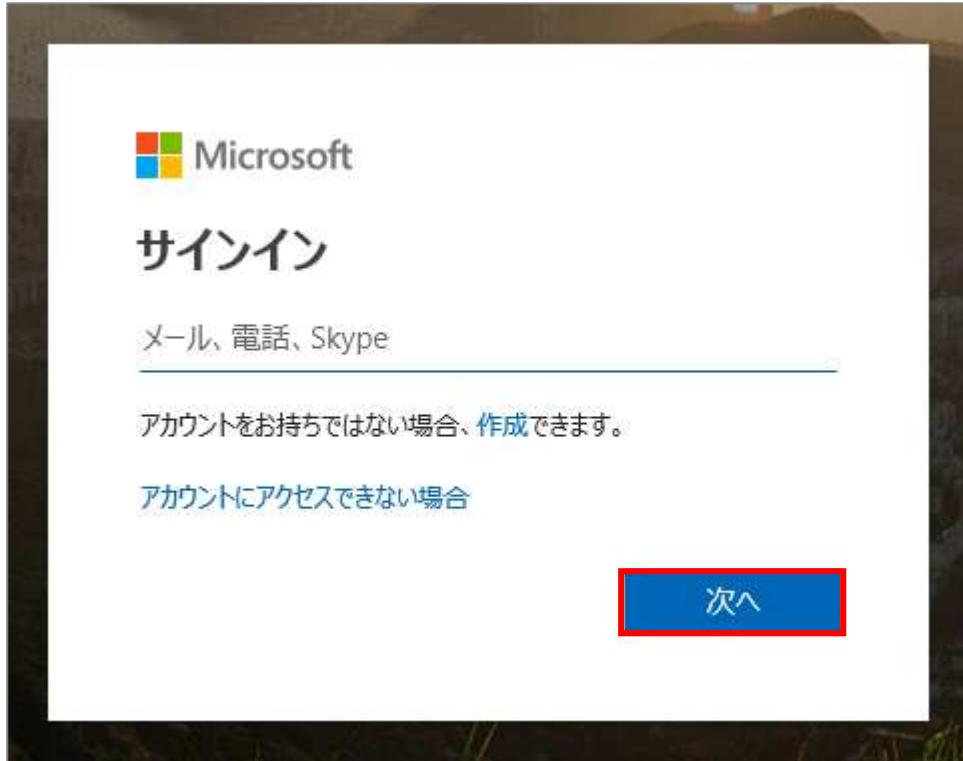


※「今後 60 日間はこのメッセージを表示しない」にチェックを入れ認証すると、当該期間は同じ端末での同じブラウザからのサインインにおいては多要素認証を省略できます。60 日経過後、再度多要素認証を行う必要があります。(詳細は、「4.3 信頼済みデバイス」をご参照ください。)

3.5.2.2 「認証用電話」 — 「電話する」を選択する場合

電話による認証を選択した場合の認証方法は、以下の通りです。

- ① Office 365 の「サインイン画面」で個人メールアドレスを入力し、「次へ」ボタンをクリックします。



- ② 「パスワードの入力」画面でパスワードを入力し、「サインイン」ボタンをクリックします。

- ③ 登録した電話番号宛てに電話がかかるため、音声の指示に従って操作をしてください。Office 365 ホーム画面には自動で切り替わります。



- ※ 「#」を押すように音声指示がありますが、アナログ回線の場合は「*」を押してから、「#」を押す必要があります。
- ※ 「今後 60 日間はこのメッセージを表示しない」にチェックを入れ認証すると、当該期間は同じ端末での同じブラウザからのサインインにおいては多要素認証を省略できます。60 日経過後、再度多要素認証を行う必要があります。(詳細は、「4.3 信頼済みデバイス」をご参照ください。)

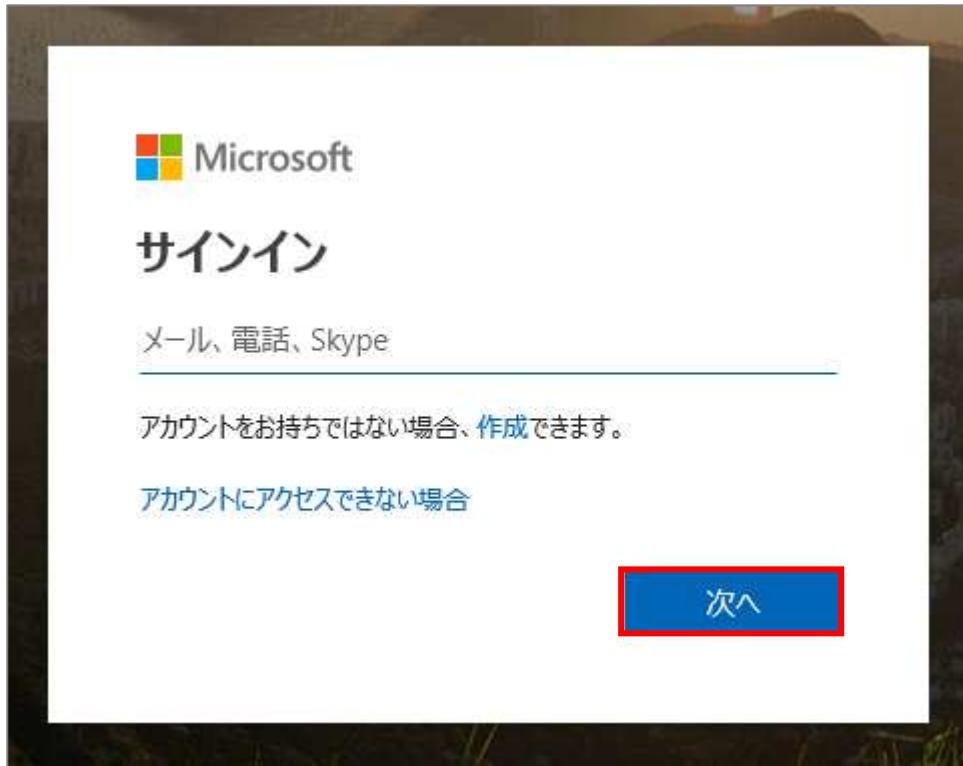
3.5.2.3 「会社電話」を設定した場合

システム連携された会社電話のことを指すため、本学では利用できません。

3.5.2.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択した場合

通知による認証を選択した場合の認証方法は、以下の通りです。

- ① Office 365 の「サインイン画面」で個人メールアドレスを入力し、「次へ」ボタンをクリックします。



- ② 「パスワードの入力」画面でパスワードを入力し、「サインイン」ボタンをクリックします。

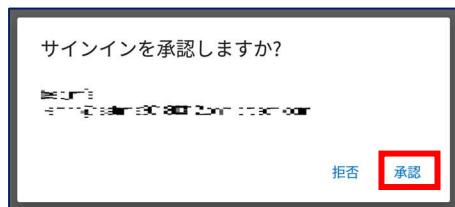
- ③ モバイルアプリを起動するとサインインの許可を求めるダイアログが表示されるので「承認」をタップします。Office 365 ホーム画面には自動で切り替わります。



【iOS 画面】



【Android 画面】

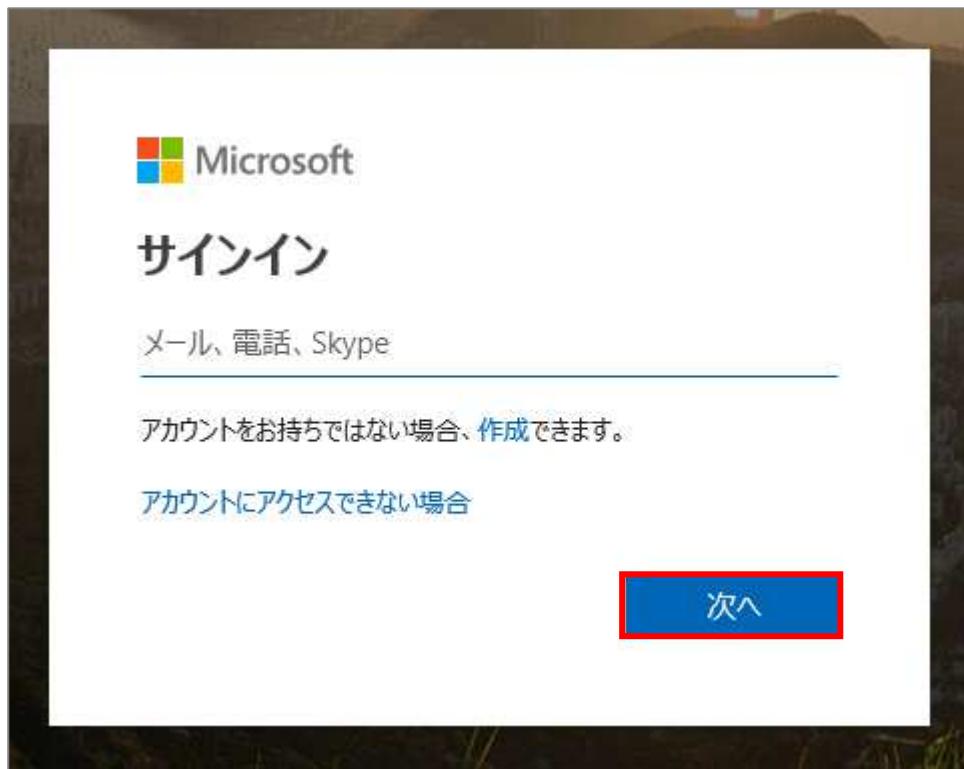


※「今後 60 日間はこのメッセージを表示しない」にチェックを入れ認証すると、当該期間は同じ端末での同じブラウザからのサインインにおいては多要素認証を省略できます。60 日経過後、再度多要素認証を行う必要があります。（詳細は、「4.3 信頼済みデバイス」をご参照ください。）

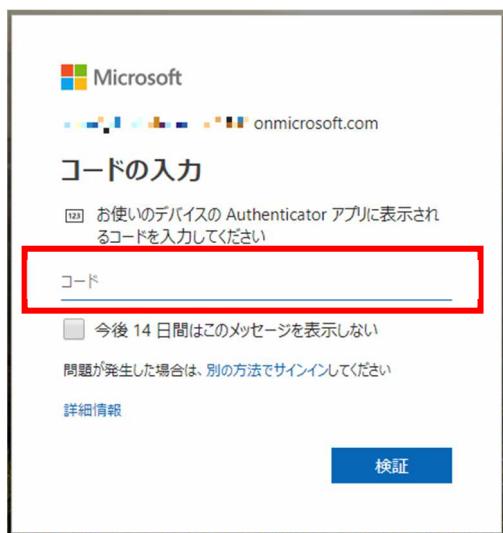
3.5.2.5 「モバイルアプリ」 — 「確認コードを使用する」を選択した場合

確認コードによる認証を選択した場合の認証方法は、以下の通りです。

- ① Office 365 の「サインイン画面」で個人メールアドレスを入力し、「次へ」ボタンをクリックします。



- ② 「パスワードの入力」画面でパスワードを入力し、「サインイン」ボタンをクリックします。
- ③ 入力フォームにモバイルアプリケーションに表示された 6 衡の認証コードを入力し、「検証」ボタンをクリックします。Office 365 ホーム画面には自動で切り替わります。



※ 「今後 60 日間はこのメッセージを表示しない」にチェックを入れ認証すると、当該期間は同じ端末での同じブラウザからのサインインにおいては多要素認証を省略できます。60 日経過後、再度多要素認証を行う必要があります。(詳細は、「4.3 信頼済みデバイス」をご参照ください。)

【iOS 画面】



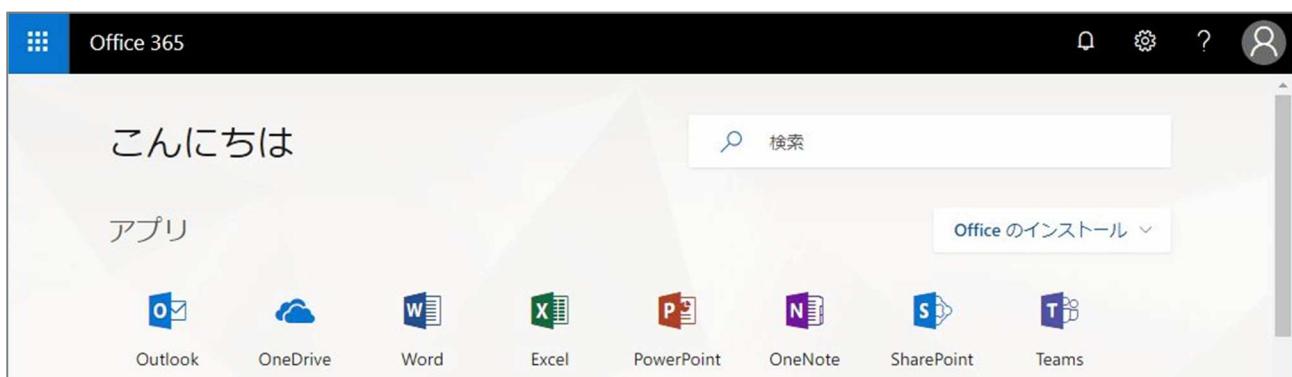
【Android 画面】



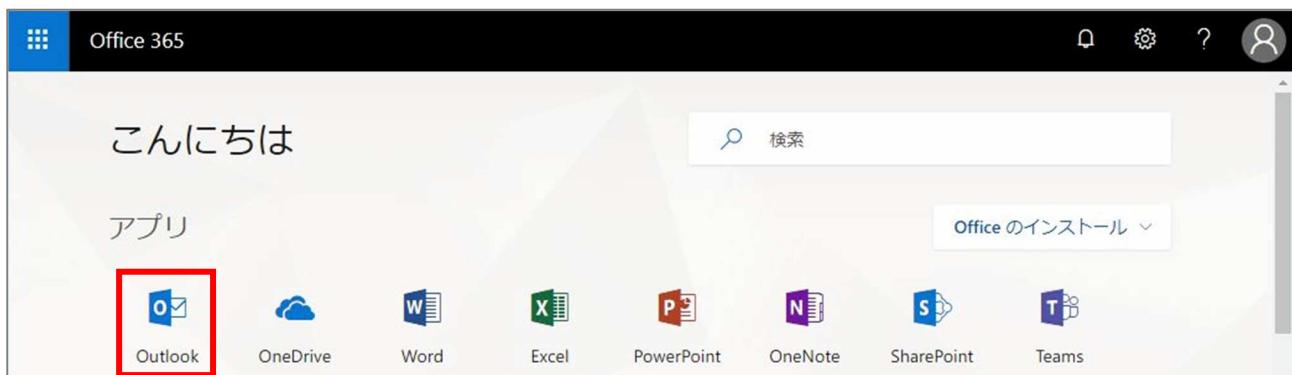
3.5.3 WEB ブラウザ(Microsoft Edge)からメールを確認する

WEB ブラウザ(Microsoft Edge)からメールを確認する方法は以下の通りです。

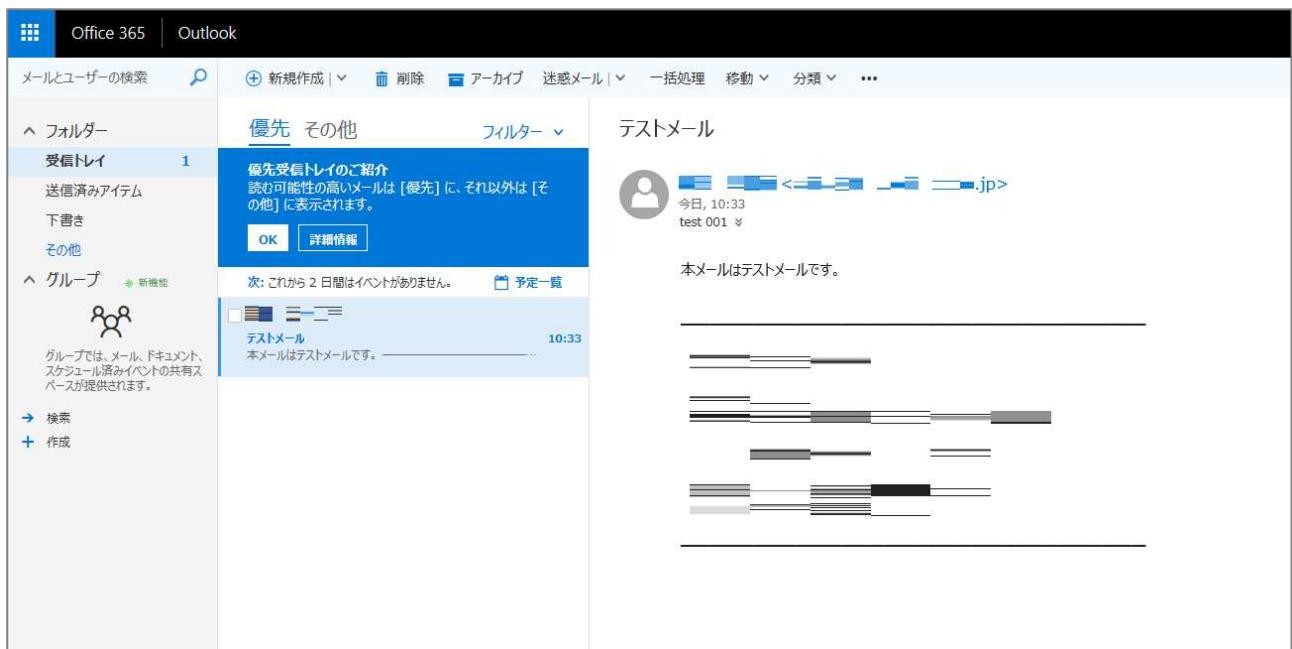
- ① 「3.5.2 Office 365 で認証を行う」の手順で Office 365 にサインインします。



- ② 「Outlook」をクリックします。



③ メール画面が表示されます。



The screenshot shows the Microsoft Outlook interface. The top navigation bar includes 'Office 365' and 'Outlook'. The left sidebar shows a '受信トレイ' (Inbox) with 1 item, '送信済みアイテム', '下書き', and 'その他'. A 'グループ' (Group) section is also present. The main area displays an email from 'test 001' with the subject 'テストメール'. The email body contains the text '本メールはテストメールです。' (This email is a test email). A small preview of the email body is shown above the main content. A modal window titled '優先 その他' (Priority, Others) provides information about the '優先受信トレイ' (Priority In-Box) feature, stating that high-priority emails are shown in the 'Priority' box and others in the 'Others' box. Buttons for 'OK' and '詳細情報' (Detailed Information) are available in the modal.

4 その他の設定

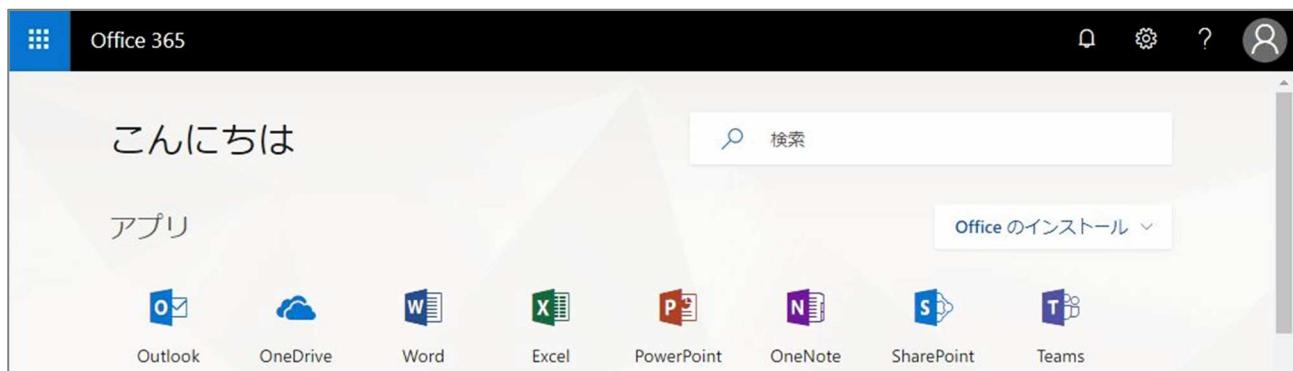
本章では、以下の多要素認証に関する設定について記載します。

設定	説明	手順
既定の認証方法の変更	現在選択している多要素認証方式から、異なる方式に変更する際の手順です。	4.1 既定の認証方法の変更
代替の認証方法	現在選択している多要素認証方式が利用できない場合に備えて、異なる代替の方式を設定する手順です。	4.2 代替の認証方法
信頼済みデバイス	利用している端末を信頼済みデバイスへ登録/解除する手順です。 ※ 信頼済みデバイスへの登録とは、サインイン時に「今後 XX 日はこのメッセージを表示しない」オプションを選択してサインインすると、その後同じ端末の同じブラウザでサインインした時の多要素認証を一定期間省略させることができる機能です。 ※ WEB ブラウザから Office 365 にサインインする場合のみの機能です。	4.3 信頼済みデバイス
アプリケーション パスワード	アプリケーションパスワードを新規作成する手順、作成したアプリケーションパスワードを削除する手順です。	4.4 アプリケーションパスワード
「Microsoft Outlook」 のバージョン確認手順	使用している「Microsoft Outlook」のバージョンを確認する手順です。	4.5 「Microsoft Outlook」のバージョンの確認手順
Outlook2016 のメール の接続の種類の確認	現在の Outlook2016 のメールの接続の種類を確認する手順です。	4.6 Outlook2016 のメールの接続の種類の確認

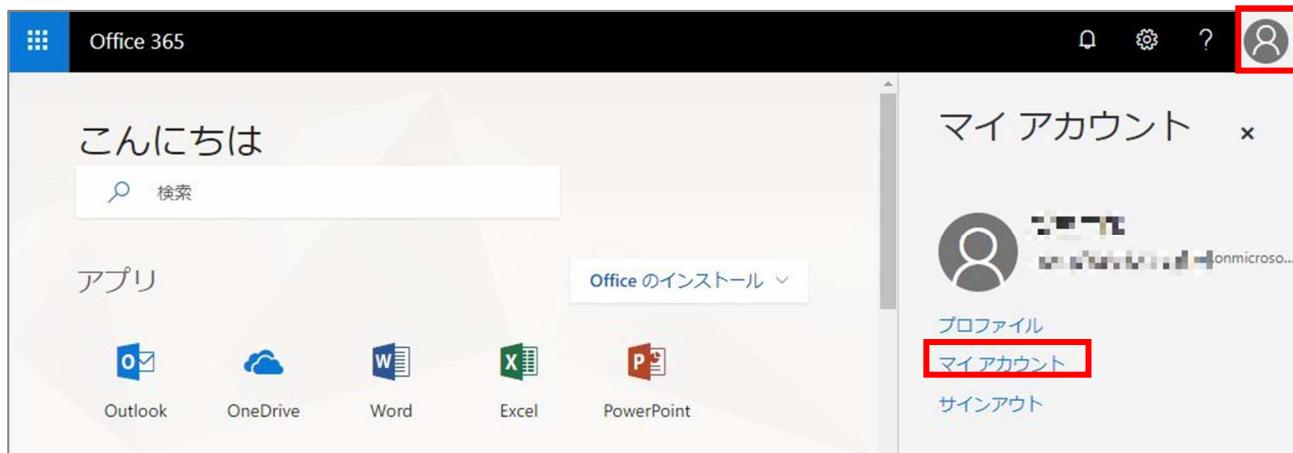
4.1 既定の認証方法の変更

多要素認証として設定した「既定の認証方法」を変更する際は以下の操作を実行します。

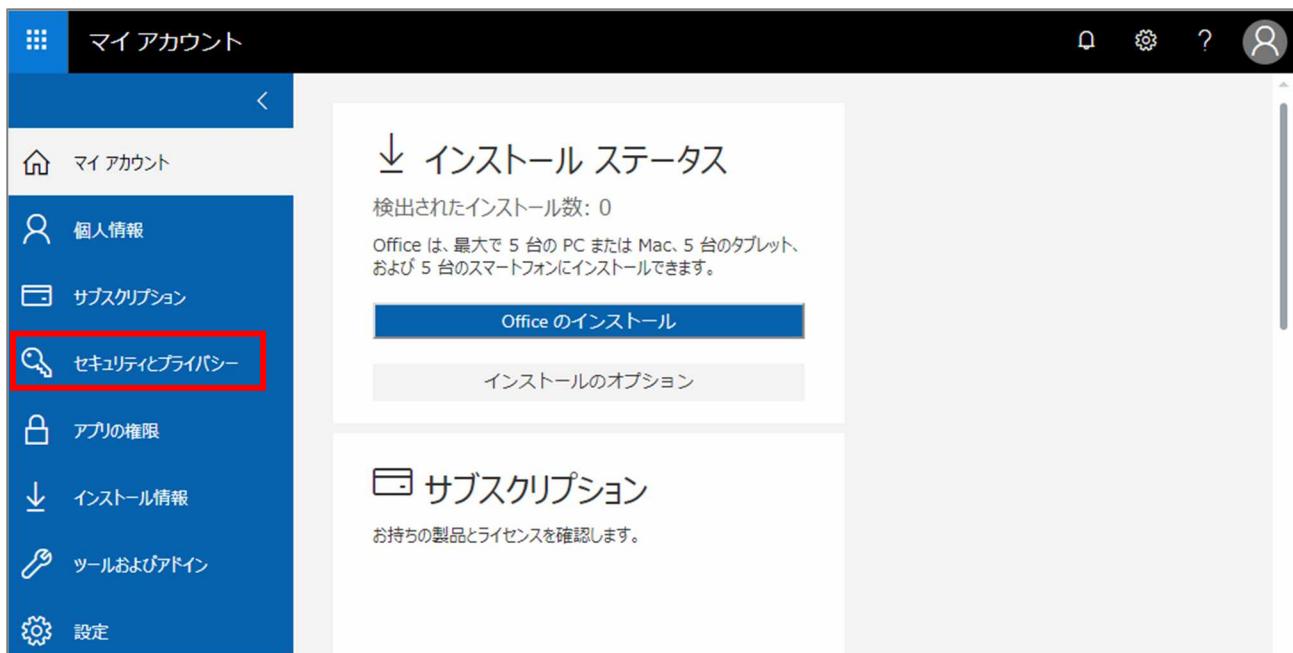
- ① 本学のOffice 365画面を表示します。



- ② 画面右上のユーザーインサートアイコンをクリックした後、画面右側の「マイアカウント」をクリックします。



- ③ 「マイアカウント」画面が表示されたら、左メニューの「セキュリティとプライバシー」をクリックします。



- ④ 「追加のセキュリティ検証」の「セキュリティ検証設定を追加または変更します。」をクリックします。



⑤ 「アカウントのセキュリティに使用する電話番号を更新します。」をクリックします。

マイアカウント

セキュリティとプライバシー

パスワード
パスワードを変更します。

連絡先の選択
連絡を受ける方法と理由を管理します。

オン

組織のプライバシーに関する声明
組織のプライバシーに関する声明を表示します

追加のセキュリティ検証
アカウントのセキュリティを強化するため、管理者によって追加のセキュリティ検証が有効化されました。

Office 365 にサインインするには、パスワードを入力し、携帯電話に送信されてくるセキュリティ メッセージに返信する必要があります。

アカウントのセキュリティに使用する電話番号を更新します。

コンピューターまたはスマート フォンにインストールされている一部のアプリにサインインするために、アプリ パスワードを作成する必要があります。アプリによる指示が表示された場合は、職場または学校アカウントのパスワードではなくアプリ パスワードを入力してください。

⑥ 「追加のセキュリティ確認」画面が開いたことを確認します。

Office 365

追加のセキュリティ確認 アプリケーション パスワード

パスワードを使用してサインインする場合、登録されていてサインインする問題が発生しづらくなります。アカウントのセキュリティを強化するため、管理者によって追加のセキュリティ検証が有効化されました。

ここで選択されている方法が既定で使用される

既定ではこの確認オプションが使用されます。

認証用電話に電話をかける

応答に使用する方法を選択してください。

次のオプションの 1 つまたは複数をセットアップしてください。詳細情報を見る

認証用電話

日本 (+81)

090-1111-2222

内線

会社電話

国/地域を選択してください

代替の認証用電話

国/地域を選択してください

認証アプリ

Authenticator アプリの設定

使用する方法とその詳細
複数選択も可能
(既定の設定以外は、代替の認証方法となります。)

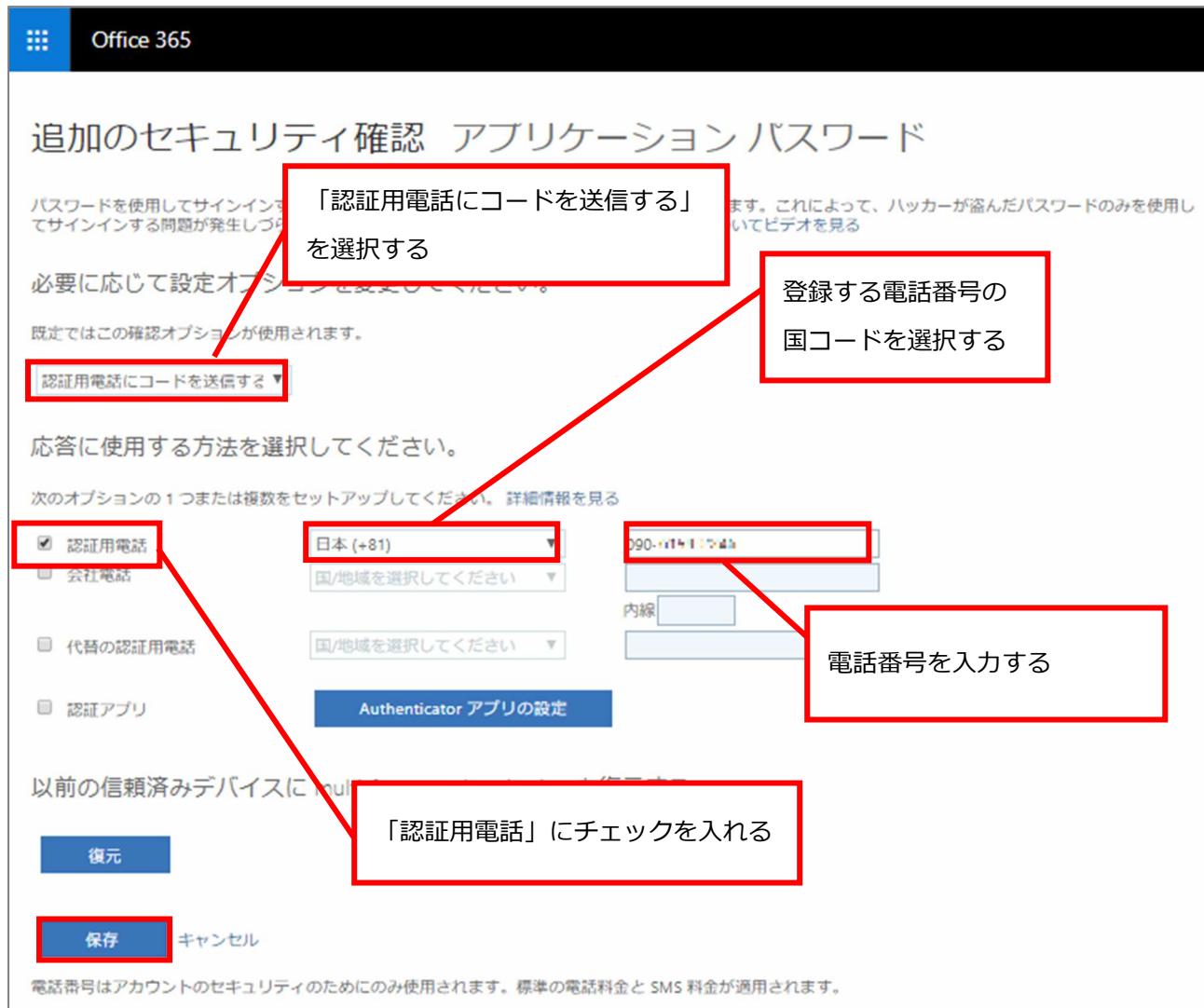
以前の信頼済みデバイスに multi-factor authentication を復元する

復元

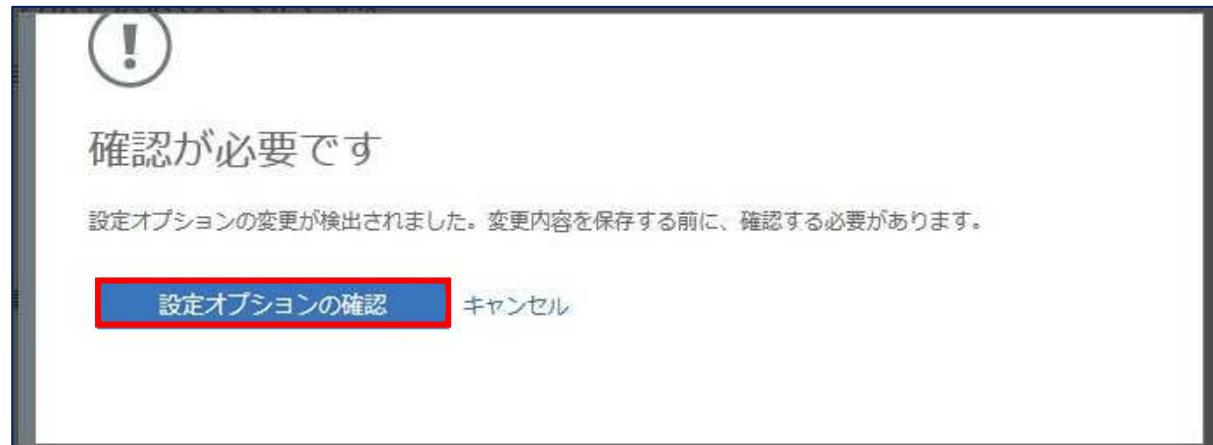
以降の操作は各認証方法によって異なります。

4.1.1 「認証用電話にコードを送信する」に設定する場合

- ① 以下の通り設定し、「保存」ボタンをクリックします。



- ② 以下の画面が表示されたら、「設定オプションの確認」ボタンをクリックします。



- ③ 登録した電話番号宛てにテキストメッセージ（ショートメール）が送信されるので、内容に記載された確認コードを入力フォームに入力し、「確認」をクリックします。

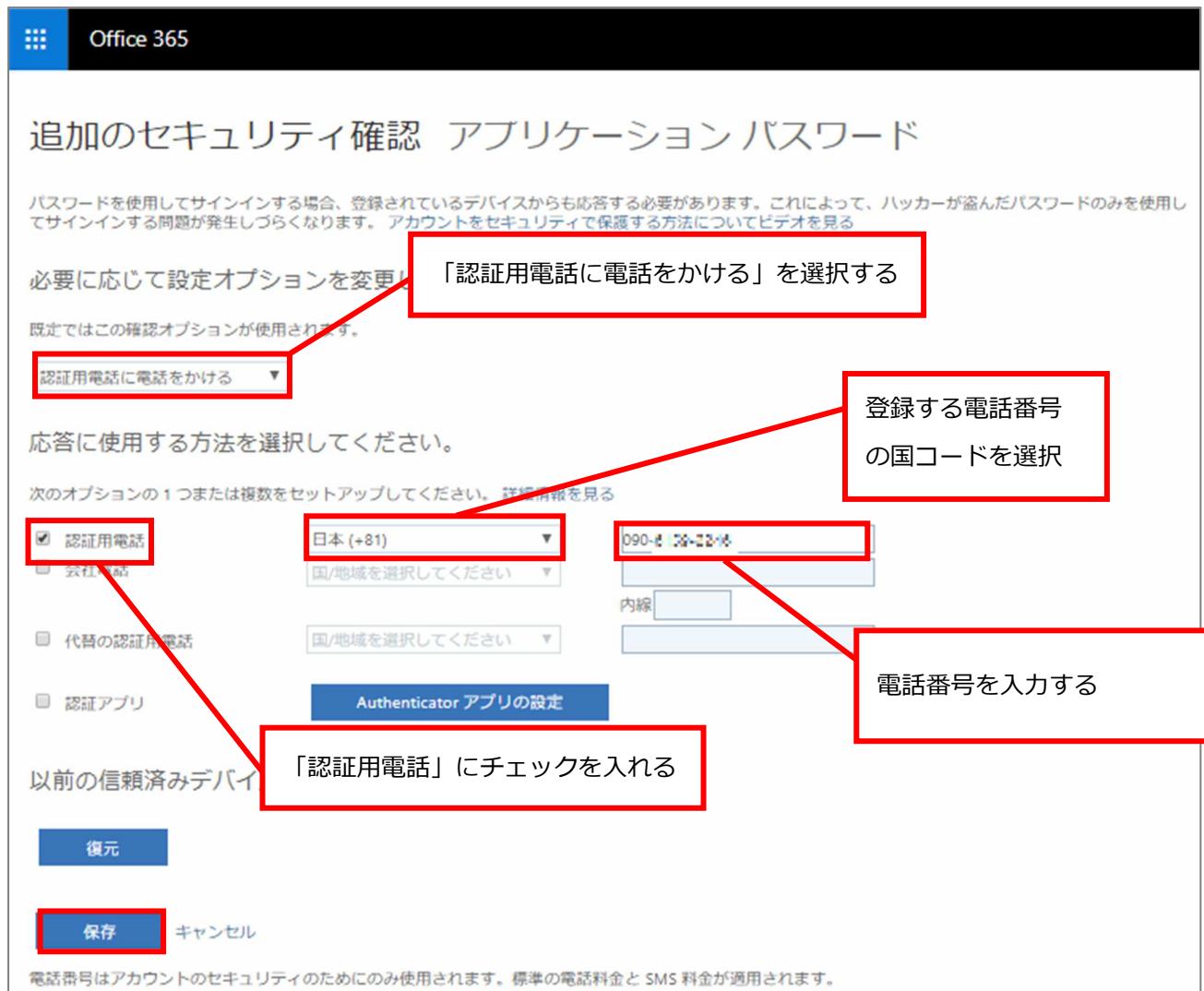


- ④ 以下の画面に自動で切り替わるため、「閉じる」をクリックして設定を終了します。

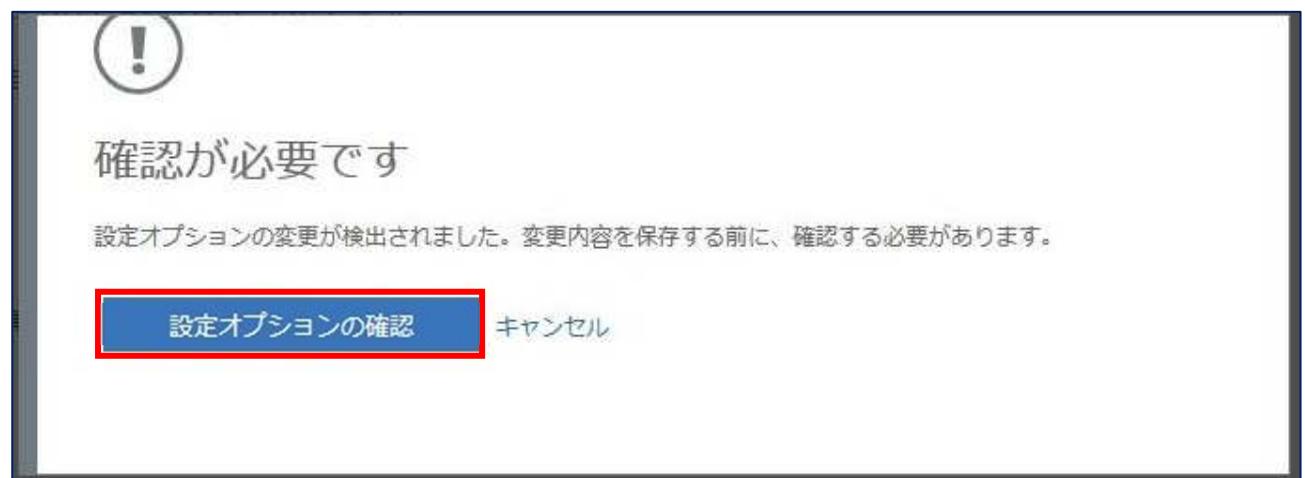


4.1.2 「認証電話に電話をかける」に設定する場合

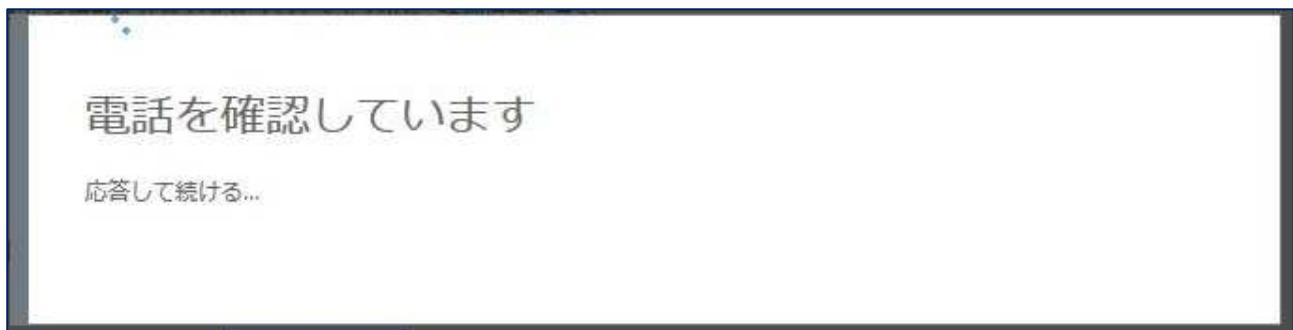
- ① 以下の通り設定し、「保存」をクリックします。



- ② 以下の画面が表示されたら、「設定オプションの確認」をクリックします。



- ③ 登録した電話番号宛てに電話がかかります。音声の指示に従って操作をしてください。



- ④ 以下の画面に自動で切り替わるため、「閉じる」をクリックし、設定を終了します。



4.1.3 「会社電話にかける」に設定する場合

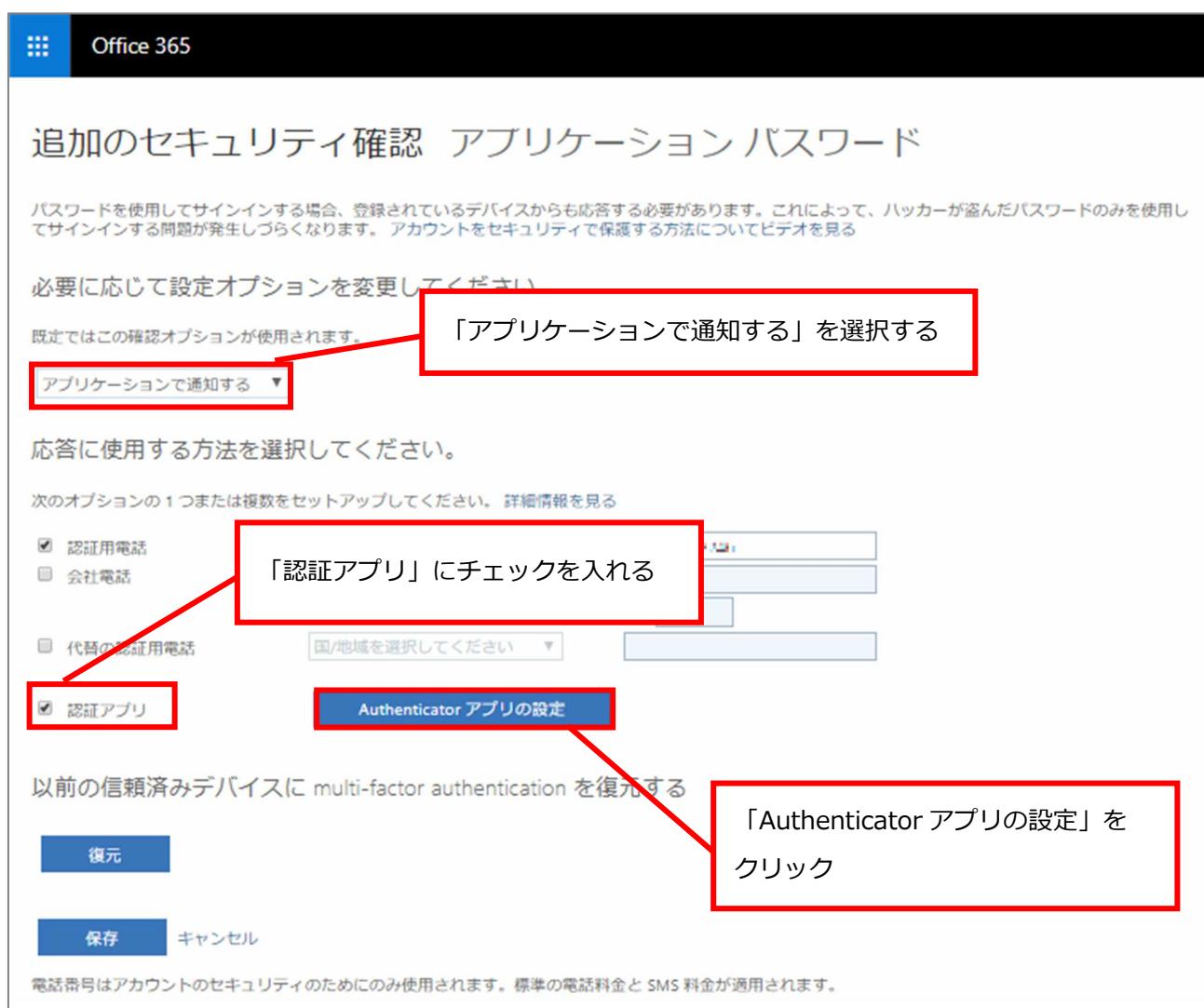
システム連携された会社電話のことを指すため、本学では利用できません。

4.1.4 「アプリケーションで通知する」に設定する場合

この認証方法は事前にスマートフォンにアプリをインストールする必要があります。インストール方法は「2.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択する場合」、「2.1.5 「モバイルアプリ」 — 「確認コードを使用する」を選択する場合」をご参考ください。

【PC 上での操作 その 1】

- ① 以下の通り設定します。はじめてモバイルアプリケーションを使う場合は「Authenticator アプリの設定」ボタンをクリックします。
すでにモバイルアプリケーションを設定済みの場合は、【PC 上での操作 その 2】①に進みます。

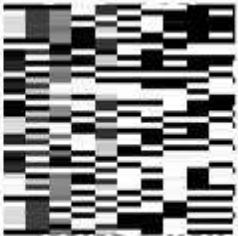


- ② 「Authenticator アプリの設定」ボタンをクリックした後、「モバイルアプリケーションの構成」画面が表示されたら、スマートフォンでの操作を実行します。

モバイルアプリケーションの構成

次の手順でモバイルアプリケーションを構成してください。

1. Windows Phone、Android、または iOS の Microsoft Authenticator アプリをインストールします。
2. アプリでアカウントを追加し、"職場または学校アカウント" を選択します。
3. 下の画像をスキャンしてください。



通知をオフにしてアプリを構成

画像をスキャンできない場合は、アプリケーションに次の情報を入力してください。

コード: 123456

URL: <https://contoso.com>

アプリケーションに 6 行のコードが表示されている場合、[次へ] を選択します。

次へ キャンセル

【iOS の場合】

- ① スマートフォンアプリを起動して画面右上の「+」ボタンをタップします。



- ② 「アカウントの追加」画面で「職場または学校アカウント」をタップします。



- ③ 以下左の画面から「モバイルアプリケーションの構成」画面に表示された QR コードを読み取ります。



もしくは「またはコードを手動で入力」をタップして表示された以下右の画面に QR コードと同時に表示されたコードと URL を直接入力して「完了」ボタンをタップします。

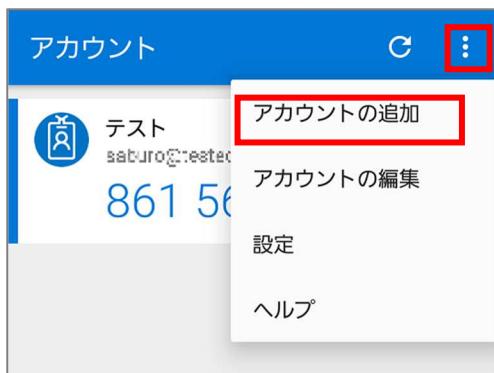


【Android の場合】

- ① スマートフォンアプリを起動して画面中央の「+」をタップします。画面右上の「⋮」ボタンをタップして「アカウントの追加」を続けてタップします。



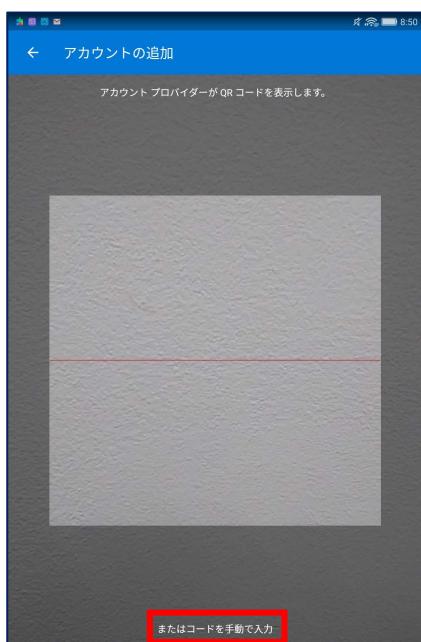
② 画面右上の「⋮」ボタンをタップして「アカウントの追加」を続けてタップします。



③ 「アカウントの追加」画面で「職場または学校アカウント」をタップします。



④ 以下左の画面から「モバイルアプリケーションの構成」画面に表示されたQRコードを読み取ります。



もしくは「またはコードを手動で入力」をタップして表示された以下右の画面に QR コードと同時に表示されたコードと URL を直接入力して「完了」ボタンをタップします。



【PC 上での操作 その2】

- ① PC 上で以下の通り確認し、「保存」ボタンをクリックします。

追加のセキュリティ確認 アプリケーションパスワード

パスワードを使用してサインインする場合、登録されているデバイスからも応答する必要があります。これによって、ハッカーが盗んだパスワードのみを使用してサインインする問題が発生しづらくなります。アカウントをセキュリティで保護する方法についてビデオを見る

必要に応じて設定オプションを変更してください。

既定ではこの確認オプションが使用されます。

「アプリケーションで通知する」を選択する

応答に使用する方法を選択してください。

次のオプションの1つまたは複数をセットアップしてください。 詳細情報を見る

認証用電話

日本 (+81) 090 1234 5678
国/地域を選択してください

会社電話
内線

代替の認証用電話
国/地域を選択してください

認証アプリ

Authenticator アプリの設定

認証アプリ - 1 件削除

以前の信頼済みデバイスに multi-factor authentication を追加する

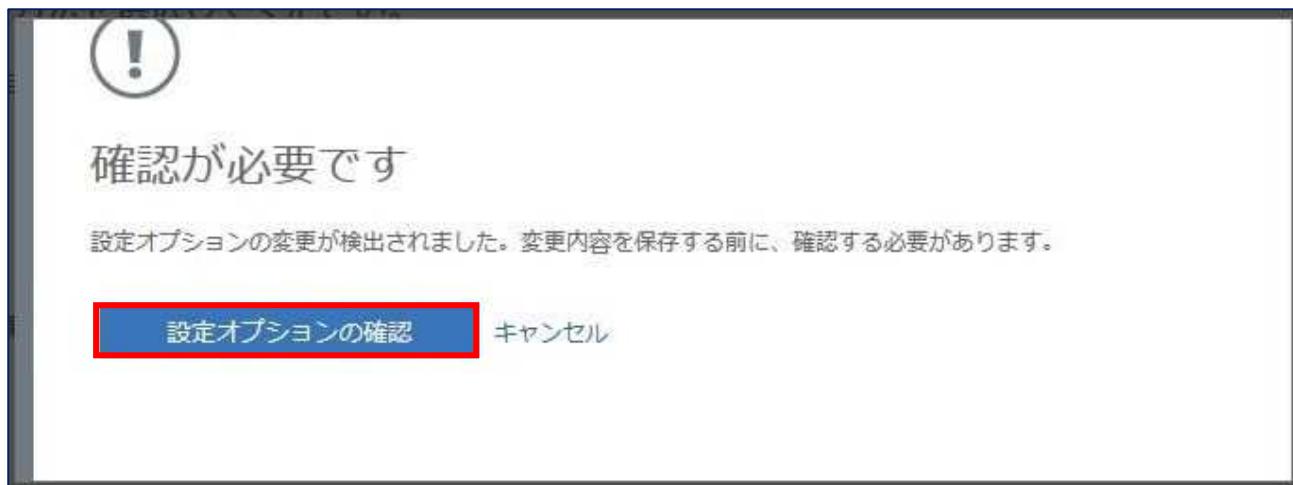
「認証アプリ」にチェックが付いており、機種名が表示されている

復元

保存 キャンセル

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。

② 以下の画面が表示されたら、「設定オプションの確認」をクリックします。

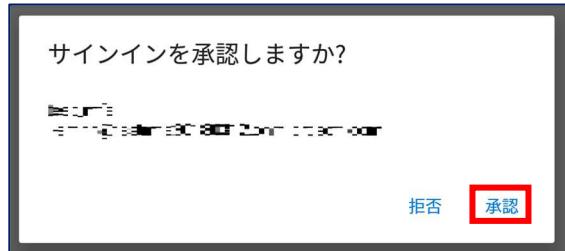


③ モバイルアプリを起動するとサインインの許可を求めるダイアログが表示されるため、「承認」をタップします。

【iOS 画面】



【Android 画面】



④ 以下の画面に自動で切り替わるため、「閉じる」をクリックして設定を終了します。



4.1.5 「アプリの確認コードを使用する」に設定する場合

- ① 以下の通り設定します。はじめてモバイルアプリケーションを使う場合は「Authenticator アプリの設定」をクリックし設定を行います。「保存」をクリックします。

Office 365

追加のセキュリティ確認 アプリケーション パスワード

パスワードを使用してサインインする場合、登録されているデバイスからも応答する必要があります。これによって、ハッカーが盗んだパスワードのみを使用してサインインする問題が発生しづらくなります。アカウントをセキュリティで保護する方法についてビデオを見る

必要に応じて設定オプションを変更してください。

既定ではこの確認オプションが使用されます。

「アプリの確認コードを使用する」を選択する

「アプリの確認コードを使用する▼」

応答に使用する方法を選択してください。

次のオプションの 1 つまたは複数をセットアップしてください。 詳細情報を見る

認証用電話

会社電話

代替の認証用電話

国/地域を選択してください ▾

「認証アプリ」にチェックを入れる

認証アプリ

Authenticator アプリの設定

認証アプリ - ~~none~~ 削除

はじめてモバイルアプリケーションを使う場合は「Authenticator アプリの設定」をクリック

すでにモバイルアプリケーションを設定済みの場合は機種名を確認

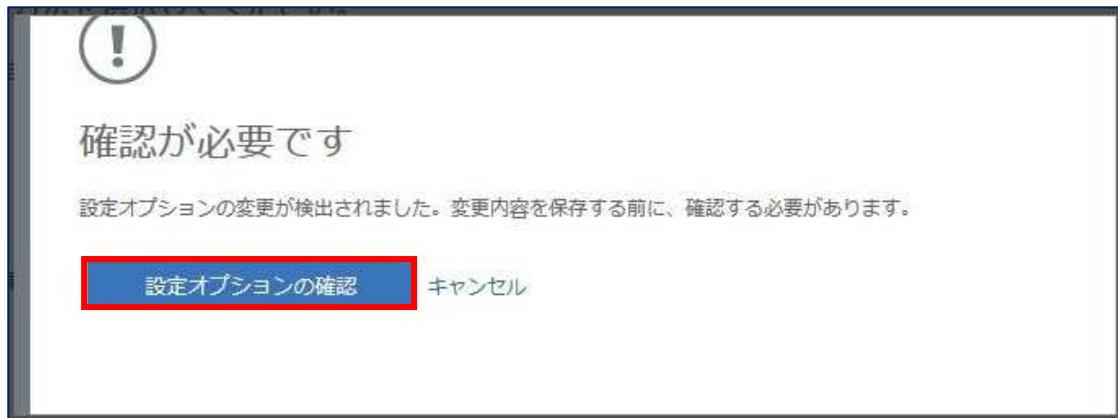
復元

保存 キャンセル

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。

※ はじめてモバイルアプリケーションを使う場合は、「2.1.5「モバイルアプリ」—「確認コードを使用する」を選択する場合」の【PC 上での操作 その 1】②の手順から設定を行います。

② 以下の画面が表示されたら、「設定オプションの確認」ボタンをクリックします。



③ 「設定オプションの確認」ボタンをクリックした後、以下の画面が表示されます。

入力フォームにモバイルアプリケーションに表示された 6 衔の認証コードを入力し、「確認」をクリックします。



【iOS画面】



【Android 画面】



- ④ 以下の画面に自動で切り替わるため、「閉じる」をクリックして設定を終了します。



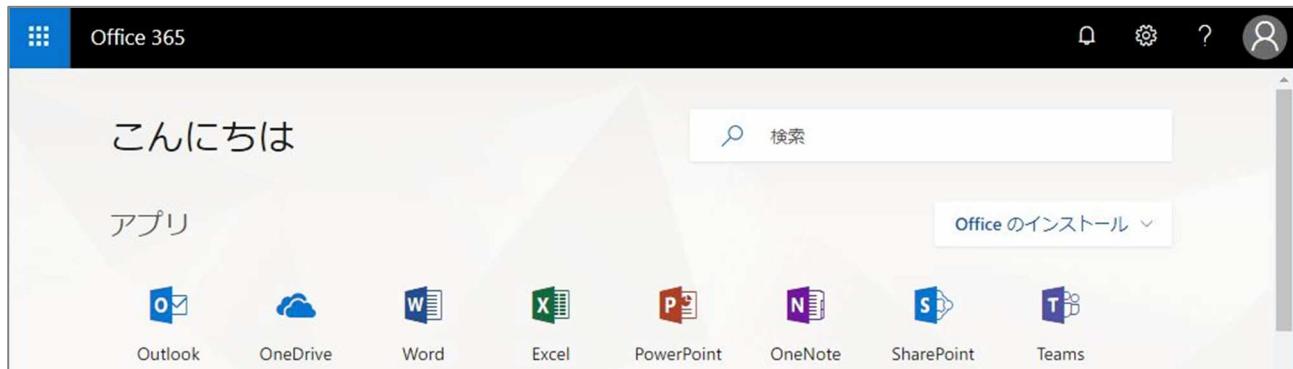
4.2 代替の認証方法

既定の認証方法が利用できない場合に備えて、代替の認証方法を設定し、使用することができます。

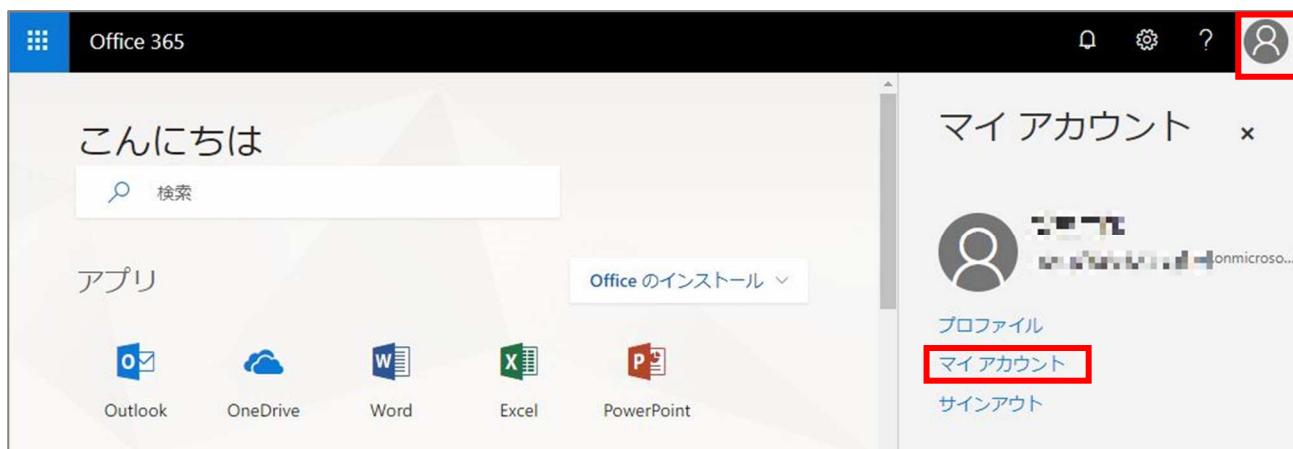
- ※ 自宅や外出先で本学の Office 365 やメールを確認する可能性のある場合は、その場所で確認可能な認証方法を事前登録していないと、サインインすることができません。そのため、代替の認証方法を 1 つ以上登録することを推奨します。

4.2.1 代替の認証方法の設定

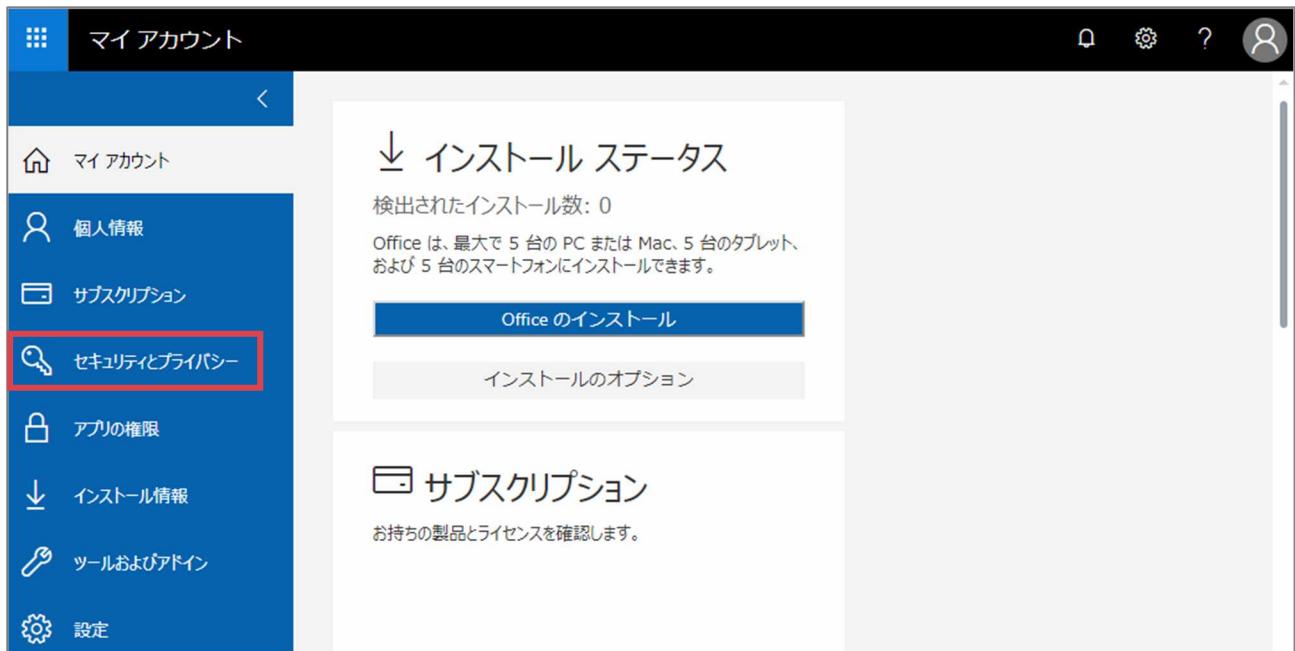
- ① 本学の Office 365 画面を表示します。



- ② 画面右上のユーザーアイコンをクリックした後、画面右下に表示された「マイアカウント」をクリックします。



- ③ 「マイアカウント」画面が表示されたら、左メニューの「セキュリティとプライバシー」をクリックします。



- ④ 「追加のセキュリティ検証」の「セキュリティ検証設定を追加または変更します。」をクリックします。



⑤ 「アカウントのセキュリティに使用する電話番号を更新します。」をクリックします。



マイアカウント

セキュリティとプライバシー

パスワード

パスワードを変更します。

連絡先の選択

連絡を受ける方法と理由を管理します。

オン

組織のプライバシーに関する声明

組織のプライバシーに関する声明を表示します

追加のセキュリティ検証

アカウントのセキュリティを強化するため、管理者によって追加のセキュリティ検証が有効化されました。

Office 365 にサインインするには、パスワードを入力し、携帯電話に送信されてくるセキュリティメッセージに返信する必要があります。

アカウントのセキュリティに使用する電話番号を更新します。

コンピューターまたはスマートフォンにインストールされている一部のアプリにサインインするために、アプリパスワードを作成する必要があります。アプリによる指示が表示された場合は、職場または学校アカウントのパスワードではなくアプリパスワードを入力してください。

⑥ 「追加のセキュリティ確認」画面で以下の通り設定し、「保存」ボタンをクリックします。

複数の代替の認証方法を設定することができます。

Office 365

追加のセキュリティ確認 アプリケーション パスワード

パスワードを使用してサインインする場合、登録されているデバイスからも応答する必要があります。これによって、ハッカーが盗んだパスワードのみを使用してサインインする問題が発生しづらくなります。アカウントをセキュリティで保護する方法についてビデオを見る

必要に応じて設定オプションを変更してください。

既定ではこの確認オプションが使用されます。

認証用電話に電話をかける ▾

応答に使用する方法を選択してください。

次のオプションの 1 つまたは複数をセットアップしてください。 詳細情報を見る

① 認証用電話 日本 (+81) 090-1234-5678
② 会社電話 国/地域を選択してください

③ 代替の認証用電話 日本 (+81) 03-1234-5678
④ 認証アプリ

Authenticator アプリの設定

以前の信頼済みデバイスに multi-factor authentication が登録されています。

「代替の認証方法」にチェックを入れて設定します

復元

保存 キャンセル

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。

項目番	項目	説明
①	認証用電話	「国コード」と「電話番号」を入力します。
②	会社電話	システム連携された会社電話のことを指すため、本学では利用できません。
③	代替の認証用電話	「国コード」と「電話番号」を入力します。 ※ 認証用電話以外の電話を設定して下さい。 ※ 代替の認証用電話として登録した電話番号にはテキストメッセージ（ショートメール）を送信できません。電話による認証のみとなります。
④	認証アプリ	チェック後に「Authenticator アプリの設定」ボタンをクリックし、初期セットアップを実行します。 手順については「2.1.4 「モバイルアプリ」 — 「確認のため通知を受け取る」を選択する場合」、「2.1.5 「モバイルアプリ」 — 「確認コードを使用する」を選択する場合」をご参照ください。

- ⑦ 以下の画面に自動で切り替わるため、「閉じる」をクリックして設定を終了します。



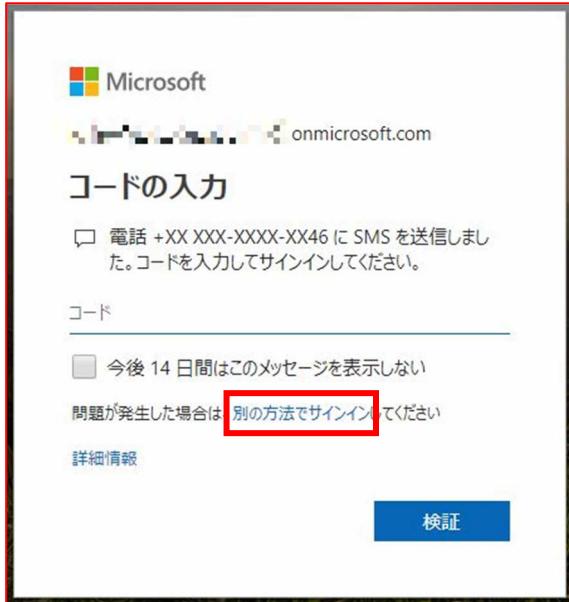
4.2.2 代替の認証方法を利用する

代替の認証用電話を設定したユーザーで、本学の Office 365 にサインインする場合は、以下の手順でサインインします。[\(http://portal.office.com/ \)](http://portal.office.com/)

- ① 以下の画面が表示されたら、「別の方法でサインイン」をクリックします。

※ 既定の認証方法により、以下のいずれかの画面が表示されます。

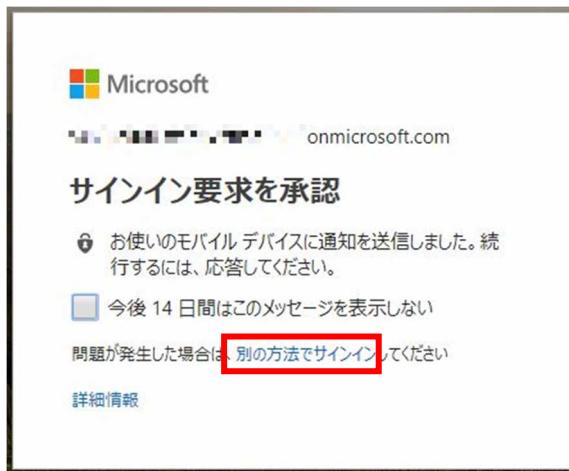
【認証用電話の「テキストメッセージによる認証」の場合】



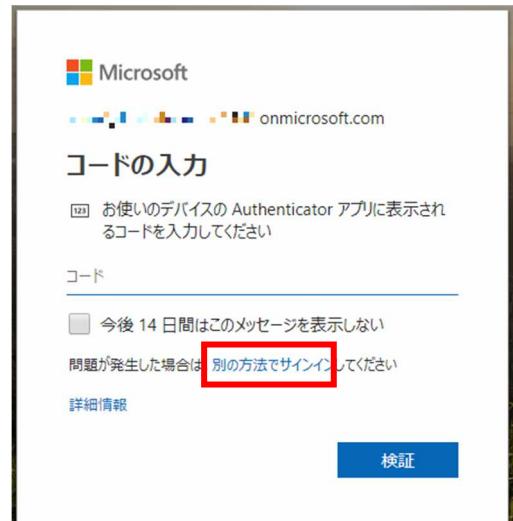
【認証用電話の「電話による認証」の場合】



【アプリの「通知による認証」の場合】



【アプリの「確認コードによる認証」の場合】



- ② 「代替の認証方法」に設定している認証方法が表示されますので、利用する認証方法を選択してください。



4.3 信頼済みデバイス

サインイン時に「今後 XX 日はこのメッセージを表示しない」オプションを選択してサインインすると、操作端末が信頼済みデバイスに登録され、その後同じ端末の同じブラウザでサインインした時の多要素認証を一定期間省略することができます。

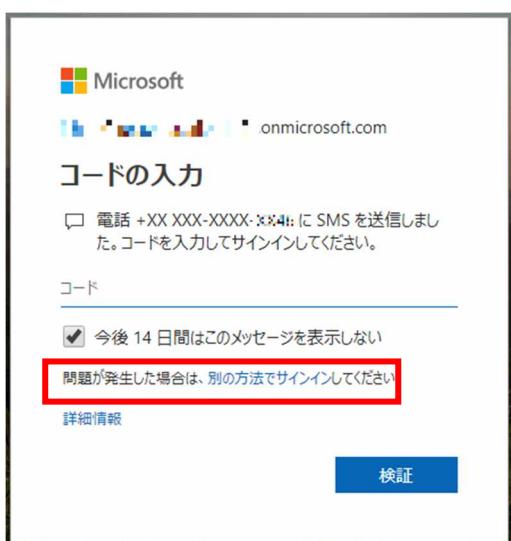
4.3.1 信頼済みデバイスを登録する

認証方法を設定したユーザーで本学の Office 365 にサインインします。（<http://portal.office.com/>）

- ① 以下の画面が表示されたら、「今後 XX 日間はこのメッセージを表示しない」の左横のチェックボックスにチェックを入れ、多要素認証の操作を実施してサインインします。

※ 既定の認証方法により、以下のいずれかの画面が表示されます。

【認証用電話の「テキストメッセージによる認証」の場合】



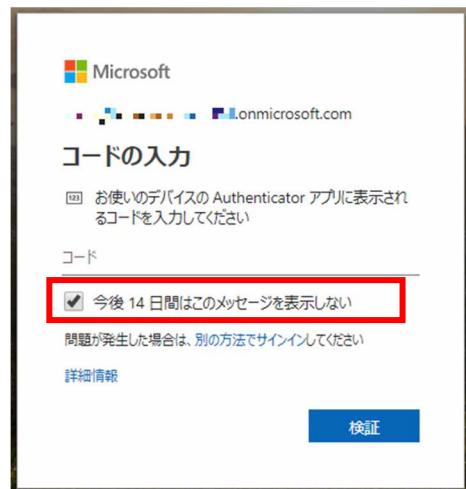
【認証用電話の「電話による認証」の場合】



【アプリの「通知による認証」の場合】



【アプリの「確認コードによる認証」の場合】

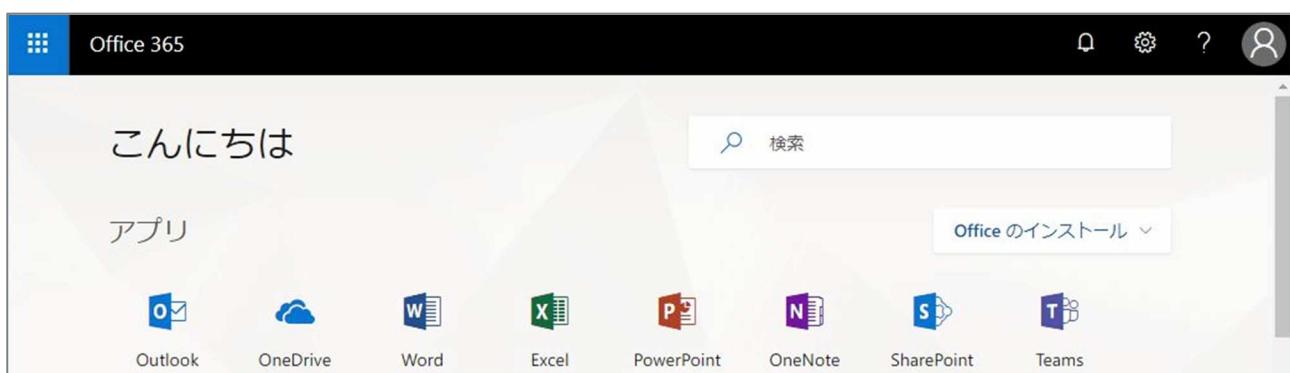


- ※ 「今後 XX 日間はこのメッセージを表示しない」の「XX」は管理者が設定した日数が表示されます。
- ※ 本手順に沿って信頼済みデバイスに登録した端末からのサインインであっても、以下の場合は多要素認証を要求されます。
 - 信頼済みデバイスへの登録操作を実施したブラウザとは別のブラウザを使用してサインインした場合。
 - 信頼済みデバイスへの登録操作を実施したブラウザの Cookie を削除した場合。
 - 管理者が設定した「今後 XX 日間はこのメッセージを表示しない」の「XX 日間」を経過した場合。

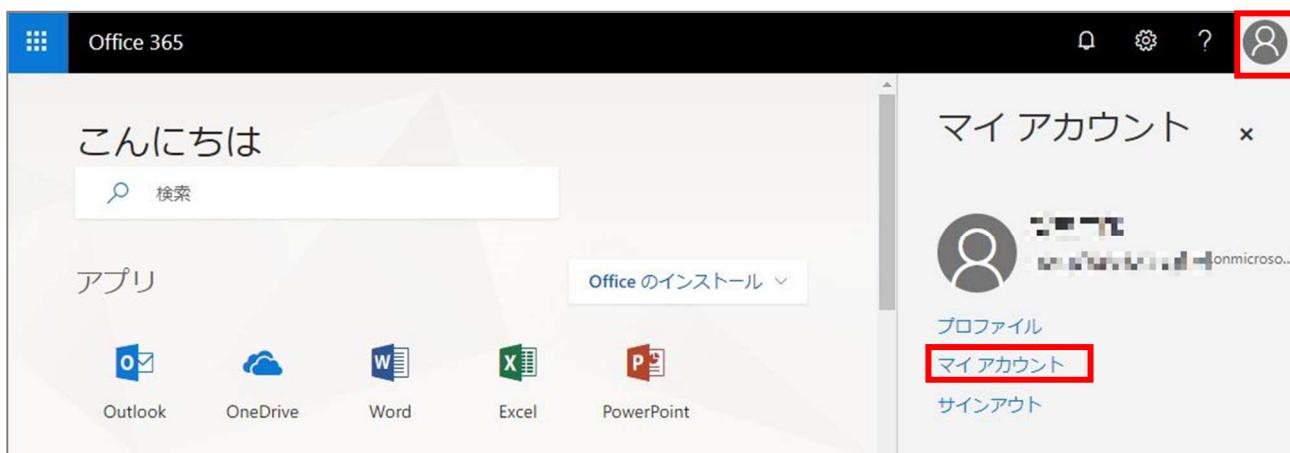
4.3.2 信頼済みデバイスを解除する

信頼済みデバイスとして登録した端末を信頼済みデバイスから解除する方法は、以下の通りです。

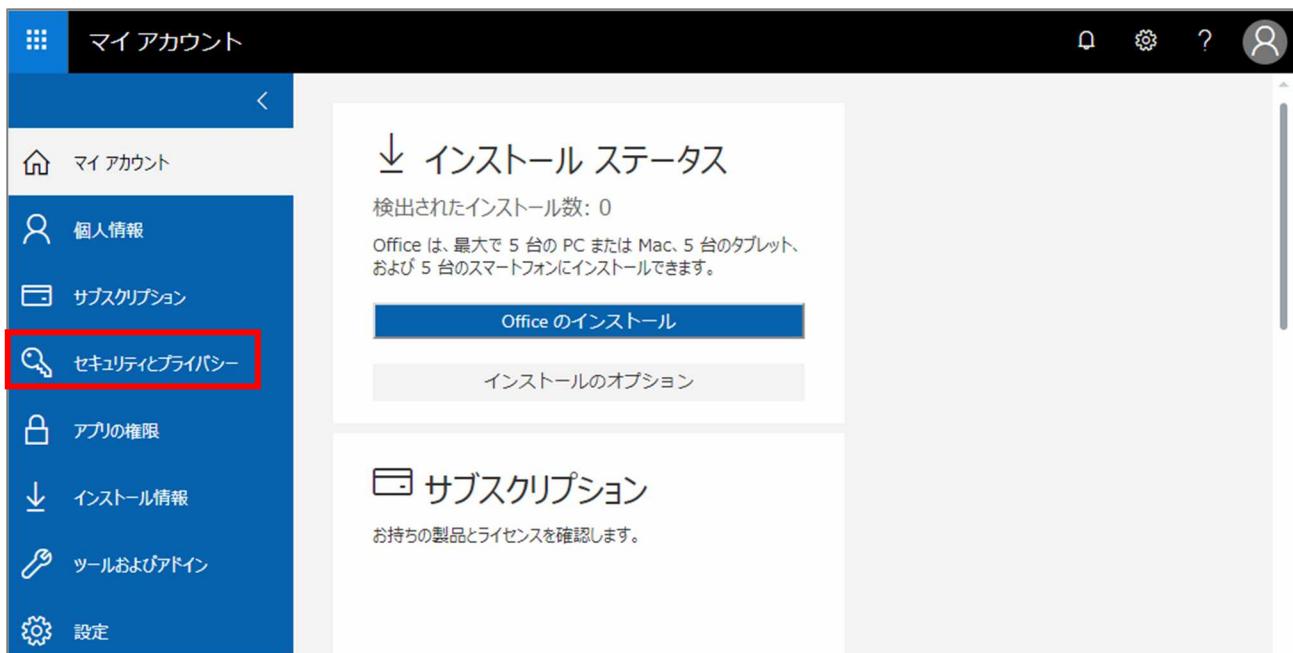
- ① 本学の Office 365 画面を表示します。



- ② 画面右上のユーザーアイコンをクリックした後、画面右下に表示された「マイアカウント」をクリックします。



- ③ 「マイアカウント」画面が表示されたら、左メニューの「セキュリティとプライバシー」をクリックします。



- ④ 「追加のセキュリティ検証」の「セキュリティ検証設定を追加または変更します。」をクリックします。



⑤ 「アカウントのセキュリティに使用する電話番号を更新します。」をクリックします。

マイアカウント

セキュリティとプライバシー

パスワード
パスワードを変更します。

連絡先の選択
連絡を受ける方法と理由を管理します。

オン

組織のプライバシーに関する声明
組織のプライバシーに関する声明を表示します

追加のセキュリティ検証
アカウントのセキュリティを強化するため、管理者によって追加のセキュリティ検証が有効化されました。

Office 365 にサインインするには、パスワードを入力し、携帯電話に送信されてくるセキュリティ メッセージに返信する必要があります。

アカウントのセキュリティに使用する電話番号を更新します。

コンピューターまたはスマート フォンにインストールされている一部のアプリにサインインするために、アプリ パスワードを作成する必要があります。アプリによる指示が表示された場合は、職場または学校アカウントのパスワードではなくアプリ パスワードを入力してください。

⑥ 「追加のセキュリティ確認」画面が表示されたら、「復元」をクリックします。

Office 365

追加のセキュリティ確認 アプリケーション パスワード

パスワードを使用してサインインする場合、登録されているデバイスからも応答する必要があります。これによって、ハッカーが盗んだパスワードのみを使用してサインインする問題が発生しづらくなります。アカウントをセキュリティで保護する方法についてビデオを見る

必要に応じて設定オプションを変更してください。

既定ではこの確認オプションが使用されます。

認証用電話にコードを送信する ▾

応答に使用する方法を選択してください。

次のオプションの 1 つまたは複数をセットアップしてください。 詳細情報を見る

認証用電話 日本 (+81) 091 123 4567
 会社電話 国/地域を選択してください 03-0000-0001
 代替の認証用電話 日本 (+81) 03 123 4567
 認証アプリ Authenticator アプリの設定

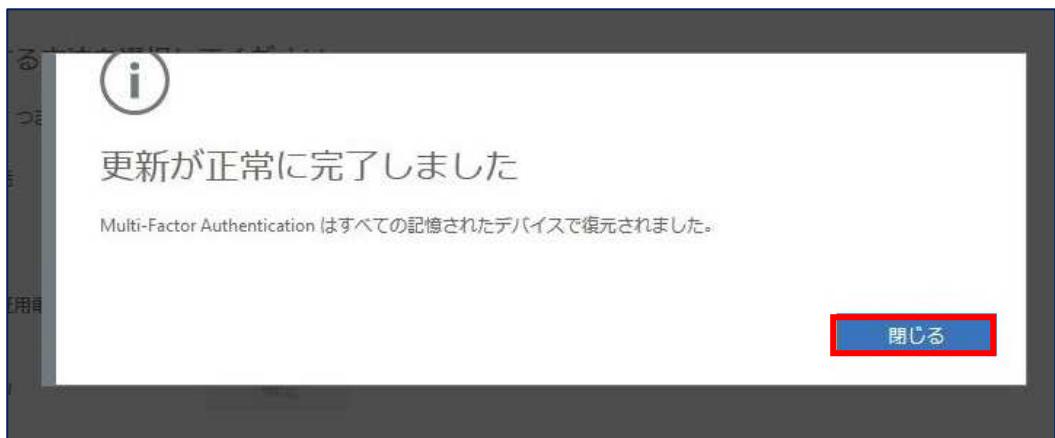
以前の信頼済みデバイスに multi-factor authentication を復元する

復元

保存 キャンセル

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。

⑦ 以下の画面が表示されたら、「閉じる」をクリックします。



⑧ 「追加のセキュリティ確認」画面で「キャンセル」をクリックし、操作を終了します。

Office 365

追加のセキュリティ確認 アプリケーション パスワード

パスワードを使用してサインインする場合、登録されているデバイスからも応答する必要があります。これによって、ハッカーが盗んだパスワードのみを使用してサインインする問題が発生しづらくなります。アカウントをセキュリティで保護する方法についてビデオを見る

必要に応じて設定オプションを変更してください。

既定ではこの確認オプションが使用されます。

認証用電話にコードを送信する ▾

応答に使用する方法を選択してください。

次のオプションの 1 つまたは複数をセットアップしてください。 詳細情報を見る

認証用電話

会社電話

代替の認証用電話

認証アプリ

以前の信頼済みデバイスに multi-factor authentication を復元する

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。

※ 本手順によって信頼済みデバイスの登録を解除した場合、対象ユーザーが信頼済みにした全端末の全プラウザの登録が解除されます。

4.4 アプリケーションパスワード

先進認証に対応していないアプリケーション(Outlook2013、Thunderbird 等)や Outlook2016 を Exchange 以外の接続の種類 (POP や IMAP など) で使用している場合 (詳細は「4.6 Outlook2016 のメールの接続の種類の確認」をご参照ください。) に多要素認証が有効であるユーザーでサインインする場合、「アプリケーションパスワード」を使用します。

アプリケーションパスワードは多要素認証設定時に発行されますが、別のアプリケーションパスワードを作成したり、削除したりすることもできます。

4.4.1 アプリケーションパスワードの作成方法

アプリケーションパスワードを作成する手順は以下の通りです。

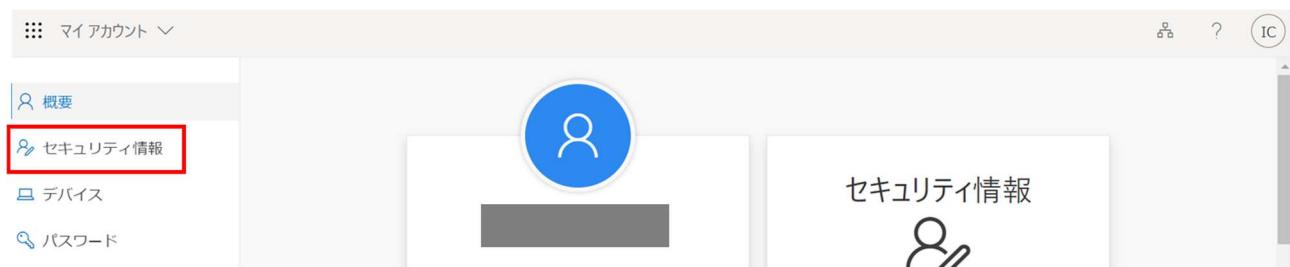
- ① 本学の Office 365 画面を表示します。



- ② 画面右上のユーザーアイコンをクリックした後、画面右下に表示された「アカウントを表示」をクリックします。

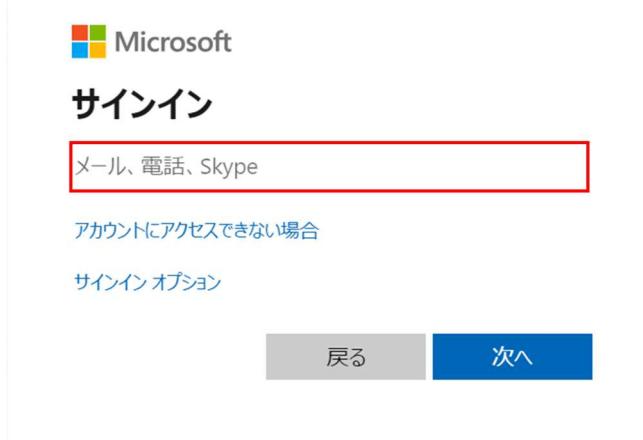


③ 「マイアカウント」画面が表示されたら、左メニューの「セキュリティ情報」をクリックします。



The screenshot shows the Microsoft My Account interface. The left sidebar has a red box around the 'Security Information' link. The main area shows a blue user icon and a 'Security Information' section with a blue user icon.

④ 「サインイン」画面が表示されたら、ユーザー名とパスワードを入力します。



The screenshot shows the Microsoft Sign-in page. The 'Sign-in options' input field is highlighted with a red box. Below it are links for 'Account access issues' and 'Sign-in options'. At the bottom are 'Back' and 'Next' buttons.

⑤ 「セキュリティ情報」画面が表示されたら、「方法の追加」をクリックします。



The screenshot shows the Microsoft Security Information page. The 'Add method' button is highlighted with a red box. The page also shows a table with two rows: 'Phone' and 'App password'. At the bottom is a note about signing out if a device is lost.

⑥ 「アプリパスワード」を選択し、「追加」をクリックします。



⑦ アプリケーションパスワードの名前を入力し、「次へ」をクリックします。

※ 本画面では一例として、「AppliPassWord」と入力しています。



⑧ 以下の画面が表示されたら「パスワード」横のコピーマークをクリックし、アプリケーションパスワードをコピーし、「完了」をクリックします。

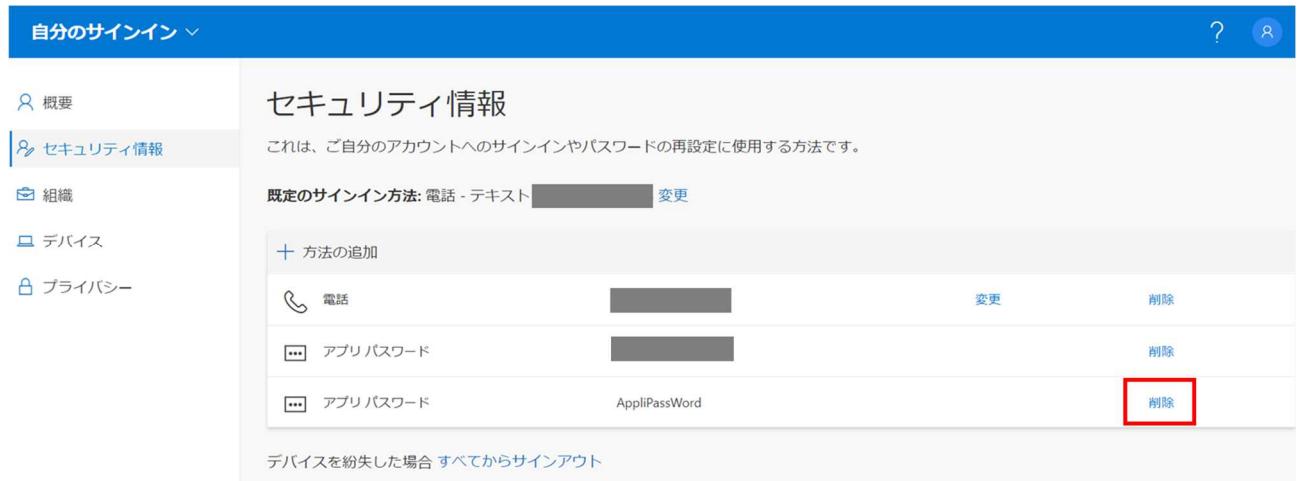
※ 本画面以降、生成されたアプリケーションパスワードを確認することはできません。メモ帳などに保存してください。



4.4.2 アプリケーションパスワードの削除方法

アプリケーションパスワードを削除する手順は以下の通りです。

- ① 「アプリケーションパスワード」画面を開き、削除したいアプリケーションパスワードの右に表示される「削除」をクリックします。



自分のサインイン

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

既定のサインイン方法: 電話 - テキスト [変更]

方法の追加

方法	値	操作
電話	[REDACTED]	変更 削除
アプリ パスワード	[REDACTED]	削除
アプリ パスワード	AppliPassWord	削除

デバイスを紛失した場合 すべてからサインアウト

- ② 以下の画面が表示されたら「OK」をクリックします。



自分のサインイン

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

既定のサインイン方法: 電話 - テキスト [変更]

方法の追加

アプリ パスワードの削除

この方法を削除しますか?

OK キャンセル

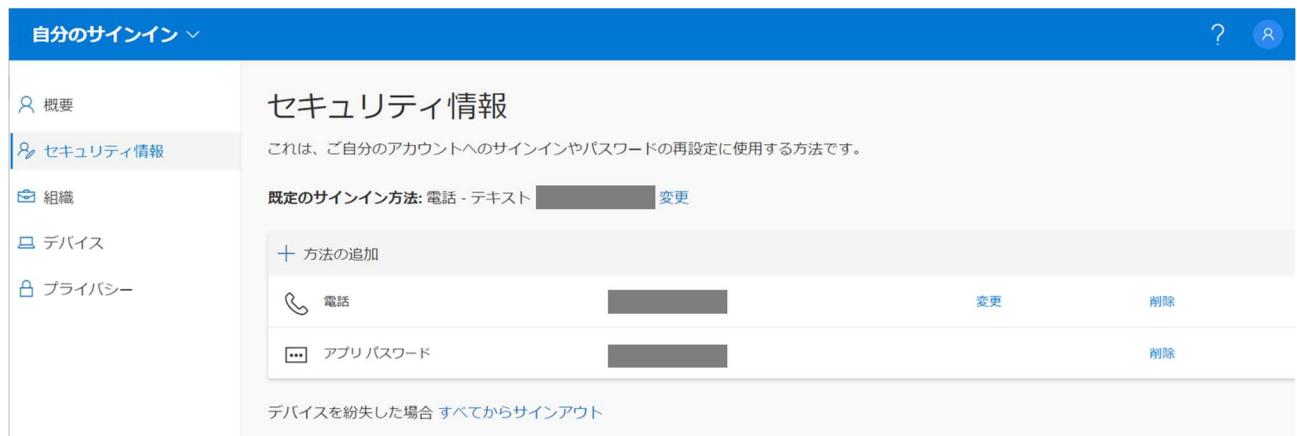
変更 削除

削除

削除

デバイスを紛失した場合 すべてからサインアウト

- ③ 「アプリケーションパスワード」画面に戻り、選択したアプリケーションパスワードが削除されていることを確認します。



自分のサインイン

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

既定のサインイン方法: 電話 - テキスト [変更]

方法の追加

方法	値	操作
電話	[REDACTED]	変更 削除
アプリ パスワード	[REDACTED]	削除

デバイスを紛失した場合 すべてからサインアウト

4.5 「Microsoft Outlook」のバージョンの確認手順

以下の手順で「Microsoft Outlook」のバージョンを確認します。

- ① Outlook クライアントを起動し、Outlook ホーム画面左上の「ファイル」タブをクリックします。



- ② サイドバーに表示された「Office アカウント」をクリックします。

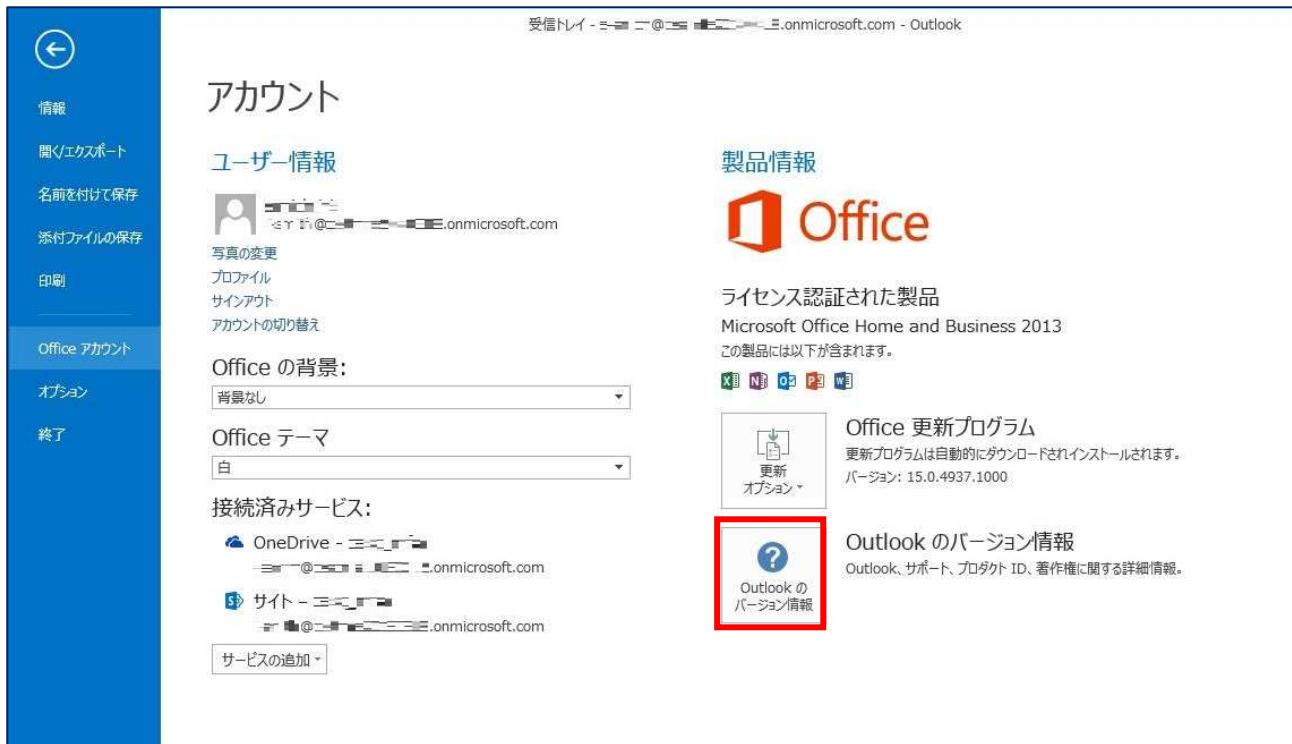


【補足】

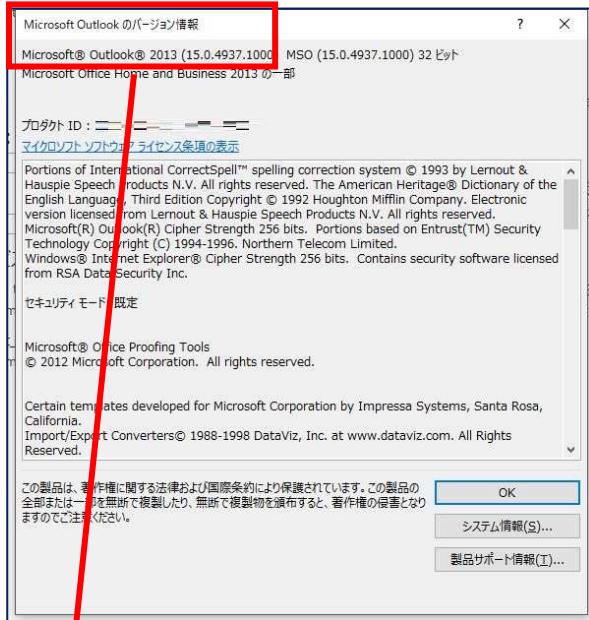
「Microsoft Outlook 2010」のバージョン確認手順は以下の通りです。

- ① Outlook ホーム画面左上の「ファイル」タブをクリックします。
- ② 左メニューから「ヘルプ」をクリックします。
- ③ 右画面に表示される「バージョンと著作権の追加情報」をクリックします。
- ④ 「Microsoft Outlook のバージョン情報」画面上部にバージョンが表示された値を確認します。

③ 画面に表示された「Outlook のバージョン情報」をクリックします。



④ 「Microsoft Outlook のバージョン情報」画面上部の赤枠で示した値を確認します。



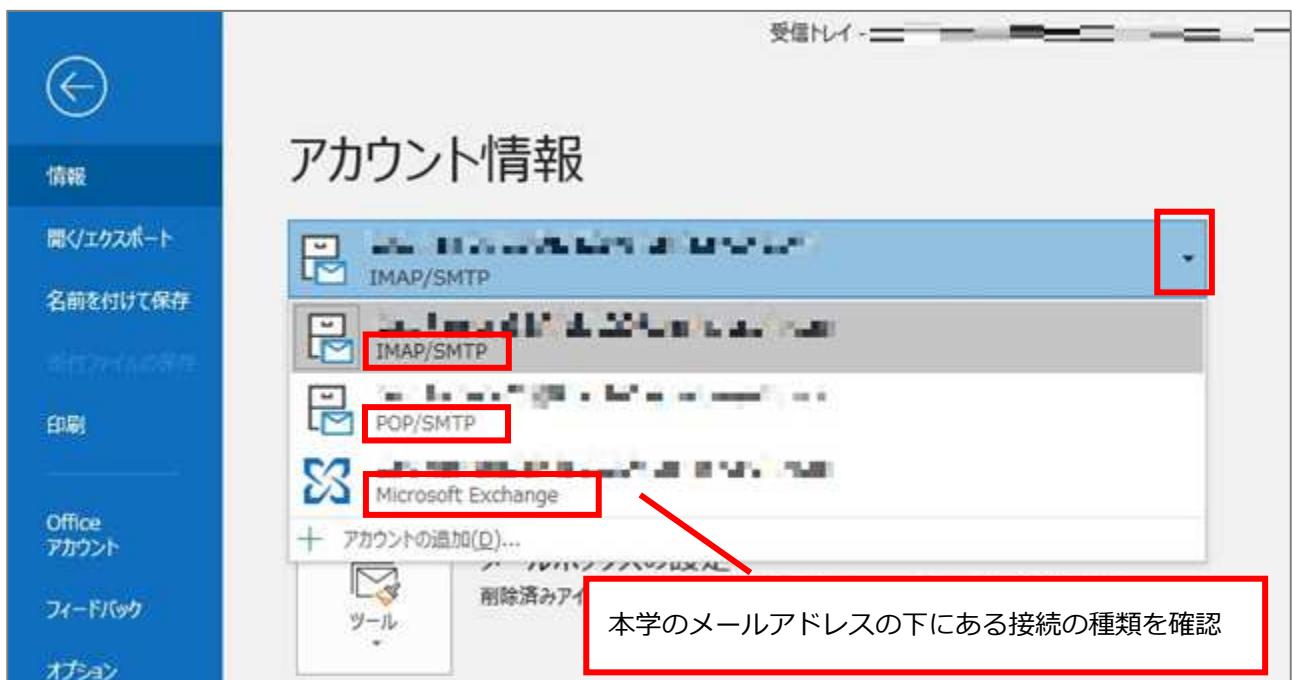
4.6 Outlook2016 のメールの接続の種類の確認

以下の手順で Outlook2016 のメールの接続の種類を確認します。

- ① Outlook2016 を起動し、ホーム画面左上の「ファイル」タブをクリックします。



- ② アカウント情報の「▼」をクリックします。本学のメールアドレスの下に表示される接続が、使用されている接続の種類となります。



以上