



先進認証(OAuth2.0) 設定ガイド ～ Microsoft365編 ～



Index

01	はじめに	4
1.	概要	4
2.	前提条件	4
3.	本書の対象者	4
4.	注意事項	5
5.	登録商標	5
02	管理者による事前準備	6
1.	管理者による事前設定（Azure）	6
2.	管理者による事前設定（desknet's NEO）	17
3.	事前設定をすべて完了した後の流れについて	19
03	管理者設定のメールサーバー設定	20
1.	管理者設定のメールサーバー設定	20
2.	設定後の流れについて	24
04	「ウェブメール」の設定	25
1.	ウェブメールのアカウント設定	25
2.	アカウント個別にOAuth認証を行う	31
3.	ウェブメール機能単体のメールサーバー設定	36
05	「ウェブメールIMAP」の設定	38
1.	ウェブメールIMAPのメールサーバー設定	38
2.	ウェブメールIMAPのアカウント設定	41
3.	アカウント個別にOAuth認証を行う	44



Index

06 「ファイル転送」の設定 49

- 1. ファイル転送の送信メールサーバー設定 49
- 2. 各ユーザー毎の差出人設定 54

07 「安否確認」の設定 57

- 安否確認の配信メールサーバー設定 57

08 クライアントシークレットの更新手順 62

- クライアントシークレットの再発行 62



01

はじめに

1. 概要

2022年10月1日よりMicrosoft 365(Exchange Online)の基本認証が順次廃止されています。ウェブメールおよびウェブメールIMAP、その他メール送信を伴う機能をご利用で、Microsoft 365をメールサーバーとしてご利用のお客様は、先進認証(OAuth 2.0)での設定が必要となります。

※本書は、desknet's NEO「V6.1 R1.0」以上において、Microsoft 365(Exchange Online)での先進認証(OAuth 2.0)の設定方法を記載しています。

2. 前提条件

前提条件は下記のとおりです。

1. Microsoft 365のメールサービスをご利用である事。
2. ご利用のdesknet's NEOのバージョンが「V6.1 R1.0」以上であること。
3. desknet's NEOのサーバーがSSL (https://~で始まるURL) に対応していること。
4. desknet's NEOのサーバーから以下のURLに対しアクセスが可能であること。
(※https通信の許可が必要です。)

3. 本書の対象者

以下の利用者を対象としています。

<管理者で行う場合>

- desknet's NEO システム管理者の権限を持ったユーザー
- Microsoft 365 グローバル管理者アカウントユーザー

<各ユーザーが個別に行う場合>

- desknet's NEO 一般ユーザー かつMicrosoft 365 アカウントを持ったユーザー



4. 注意事項

必ず下記注意事項を確認し、ご了承頂いた上で ご利用頂きます様、お願い申し上げます。

【本書の記載に関する注意事項】

- 本書内で記載されている外部URLは、**2026年8月1日 現在**のものです。また、本書内のMicrosoft 365、Azure に関する画面および説明は**2026年8月1日現在**のものです。
- Azureの画面構成や前提条件のプランに関する内容は、お客様のご利用状況やMicrosoft 社の仕様変更等により実際の画面やサービスと同一でない場合がございます。
- Azure設定に関して、**本連携機能に関する部分以外（本書掲載内容の範囲外）**のお問い合わせは、**お答えできない**場合がございます。

5. 登録商標

本書に掲載されている商品またはサービスなどの名称は、各社の商標または登録商標です。

- Microsoft AzureおよびMicrosoft Entra IDは、米国Microsoft Corporationの米国および、その他の国における登録商標または商標です。
- Windows、Microsoft、Outlook、Word、Excel、PowerPoint、Office 365、Edge、および各製品のロゴは、Microsoft Corporationの米国及びその他の国における商標または登録商標です。
- その他会社名、各製品名は、一般に各社の商標または登録商標です。



02

管理者による事前準備

- 本項の操作は、desknet's NEOシステム管理者および、Microsoft 365グローバル管理者アカウントの権限が必要です。
- ✓ • 既にMicrosoft 365を利用開始している状態を想定しています。
Microsoft 365の利用開始方法、設定につきましては、Microsoft社のドキュメントをご確認ください。

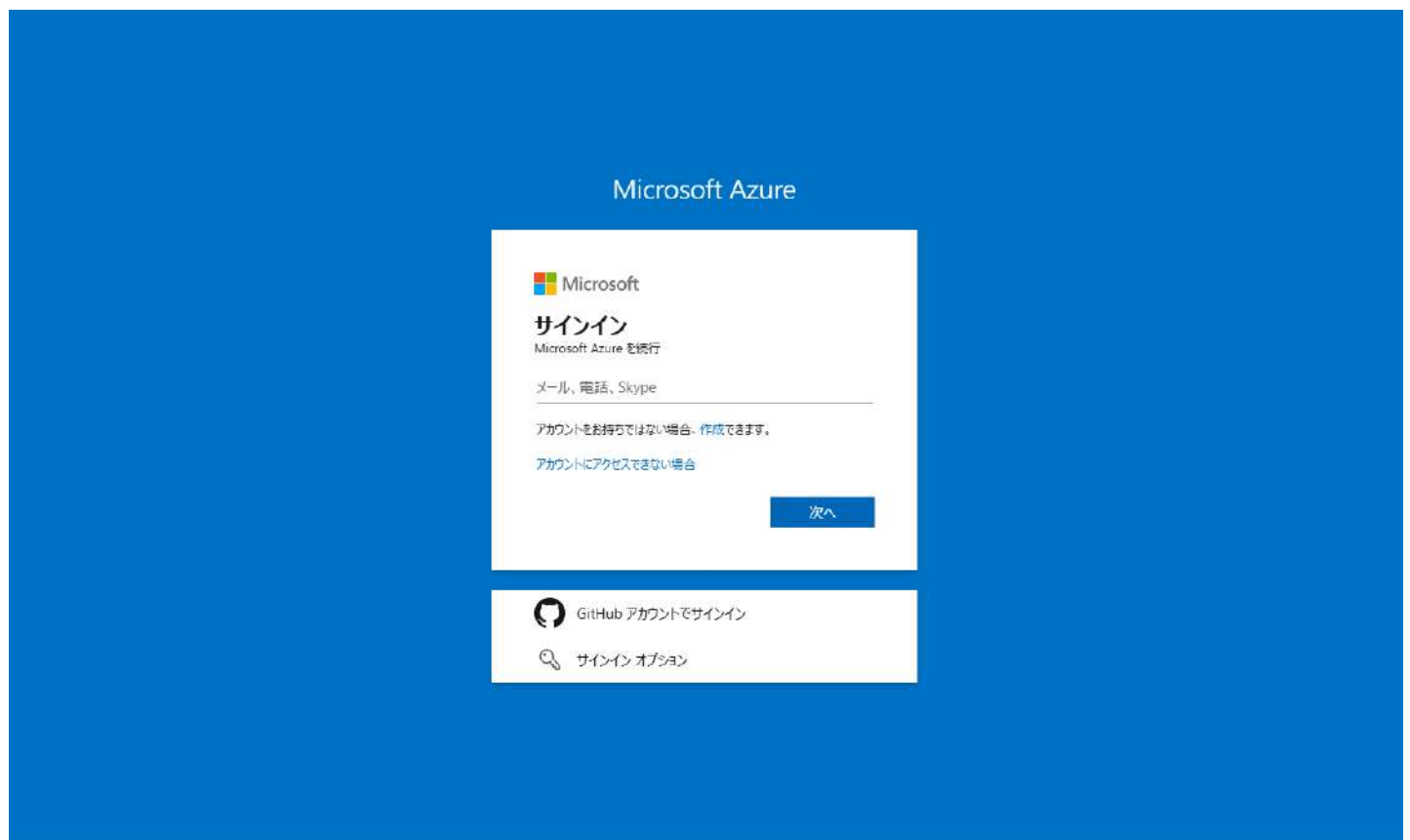
1.管理者による事前設定（Azure）

OAuth認証設定を行うにあたり、まず初めにAzureにアクセスし、認証を行うためのアプリ設定を行います。

(1)Azureポータルにログインします。

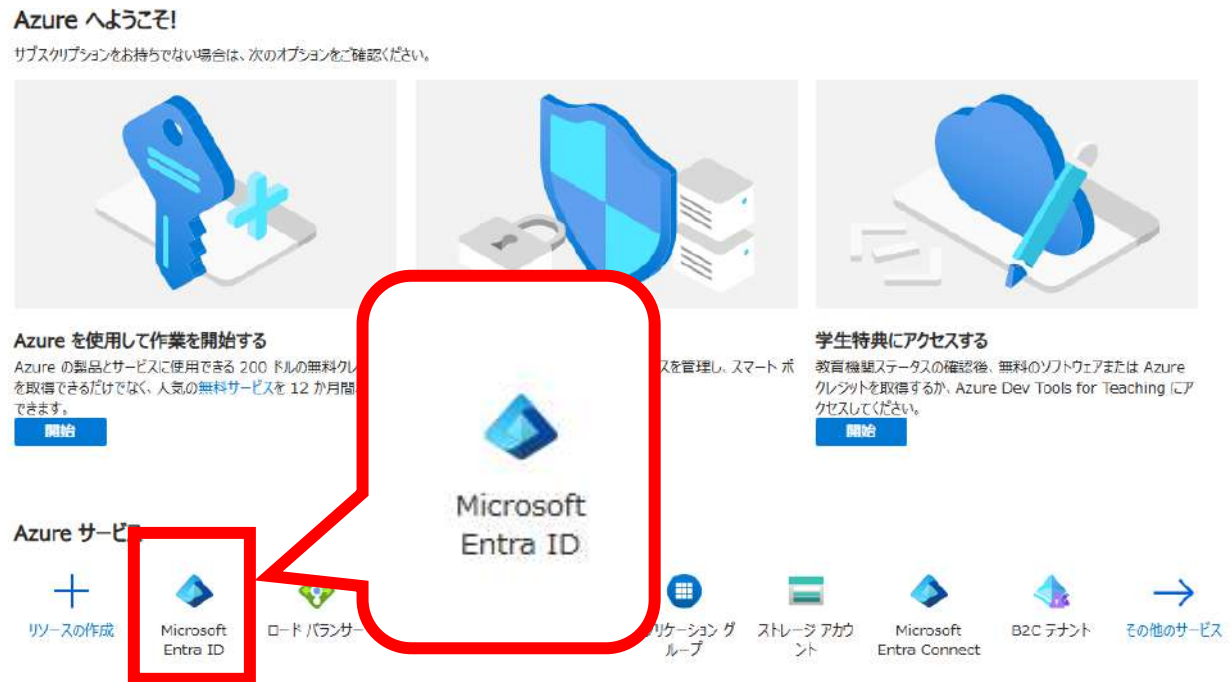
<https://portal.azure.com/#home>

上記リンクにアクセスしますと、以下の画像のようにサインイン画面が開かれますので、Microsoft 365グローバル管理者アカウントにて、Azureにサインインしてください。

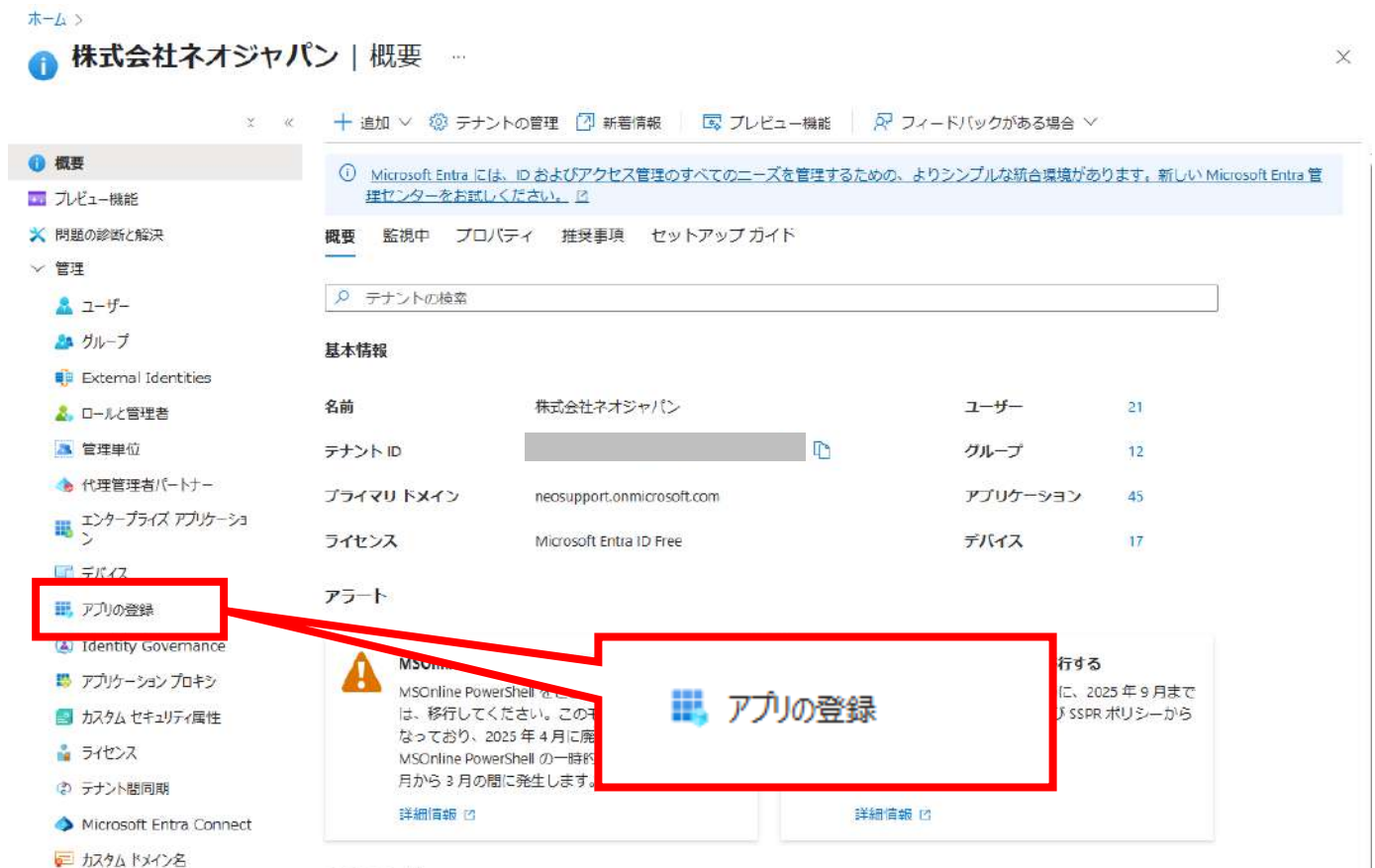


02 管理者による事前準備

(2)サインインすると下記画面が表示されますので、「**Microsoft Entra ID**」をクリックしてください。



(3)画面左側サブメニューにある「管理」の下にある「**アプリの登録**」をクリックします。



02 管理者による事前準備

(4)画面上部の「+ 新規登録」をクリックします。

ホーム > 株式会社ネオジャパン

株式会社ネオジャパン | アプリの登録

概要 プレビュー機能 問題の診断と解決 管理 ユーザー グループ External Identities ロールと管理者 管理単位 代理管理者パートナー エンタープライズ アプリケーション デバイス **アプリの登録** Identity Governance

+ 新規登録 エンドポイント トラブルシューティング 最新の情報に更新 ダウンロード プレビュー機能 フィードバックがある場合

2020 年 6 月 30 日以降、Azure AD とセキュリティ更新プログラムは今後も提供され、アップグレードする必要があります。詳細情報

機能はもう追加されません。テクニカル サポート (MSAL) および Microsoft Graph に

すべてのアプリケーション: **所有しているアプリケーション**

表示名またはアプリケーション (クライアント) ID を入力し始めると結果がフィ...

+ フィルターの追加

3 個のアプリケーションが見つかりました

表示名 ↑	アプリケーション (クライアント) ID	作成日 ↑↓	証明書とシークレット

(5)必要事項を入力し、[登録] ボタンをクリックします。

ホーム > 株式会社ネオジャパン | アプリの登録 >

アプリケーションの登録

* 名前
このアプリケーションのユーザー向け表示名 (後で変更できます)。

サポートされているアカウントの種類
このアプリケーションを使用したりこの API にアクセスしたりできるのはどれですか?

☒ この組織ディレクトリのみに含まれるアカウント (株式会社ネオジャパン のみ - シングル テナント) ②

☐ 任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Microsoft Entra ID テナント - マルチテナント) と個人用の Microsoft アカウント (Skype、Xbox など)

☐ 個人用 Microsoft アカウントのみ

選択に関する詳細...

リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

プラットフォームの選択 例: https://example.com/auth ③

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [エンタープライズ アプリケーション] から追加して統合します。

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります

登録

入力値については次のページをご確認ください。

02 管理者による事前準備

項目	入力値
①名前	任意の名称を入力します（例：desknet's NEO）
②サポートされているアカウントの種類	「この組織ディレクトリのみに含まれるアカウント」を選択します。
③リダイレクトURL（省略可能）	プラットフォームの選択：Web URL： https://(desknet's NEOサーバーのホスト名)/dneores/dneo/html/dnoauth.html https://(desknet's NEOサーバーのホスト名)/dneospres/dneo/html/dnoauth.html (desknet's NEOサーバーのホスト名) は接続URLのドメイン部分を入力します 例：https://XXX.dn-cloud.com/cgi-bin/dneo/dneo.cgi の場合 「XXX.dn-cloud.com」を入力します。

(6)アプリの作成が正常に完了すると、作成したアプリの情報画面が表示されます。
 「アプリケーションID（クライアントID）」の値をコピーしてください。



ホーム > 株式会社ネオジャパン | アプリの登録 >

desknet's NEO OAuth

検索 削除 エンドポイント プレビュー機能

概要

クイックスタート

統合アシスタント

問題の診断と解決

管理

サポート + トラブルシューティング

基本

表示名
desknet's NEO OAuth

アプリケーション (クライアント) ID

オブジェクトID

ディレクトリ (テナント) ID

クライアントの資格情報
証明書またはシークレットの追加

リダイレクト URI
1 個の Web、0 個の SPA、0 個のパブリック クライアント

アプリケーション ID の URI
アプリケーション ID URI の追加

ローカル ディレクトリでのマネージド アプリケーション
okamototest3

オブジェクトID、ディレクトリ (テナント) IDとお間違えないようご注意ください。

(7)画面左部のメニューから「管理」の下にある「証明書とシークレット」をクリックします。



ホーム > 株式会社ネオジャパン | アプリの登録 >

desknet's NEO OAuth

検索 削除 エンドポイント プレビュー機能

概要

クイックスタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

認証

証明書とシークレット

トークン構成

証明書とシークレット

クライアントの資格情報
証明書またはシークレットの追加

リダイレクト URI
1 個の Web、0 個の SPA、0 個のパブリック クライアント

アプリケーション ID の URI
アプリケーション ID URI の追加

ローカル ディレクトリでのマネージド アプリケーション

02 管理者による事前準備

(8) 「+新しいクライアントシークレット」をクリックします。

ホーム > 株式会社ネオジャパン | アプリの登録 > desknet's NEO OAuth

desknet's NEO OAuth | 証明書とシークレット

検索 フィードバックがある場合

概要

クイックスタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション

+ 新しいクライアント シークレット

証明書 (0) クライアント シークレット (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID
このアプリケーションのクライアント シークレットは作成されていません。			

(9) 必要事項を入力し [追加] ボタンをクリックします。

クライアント シークレットの追加

説明 ① このクライアント シークレットの説明を入力してください

有効期限 ② 推奨: 180 日 (6 か月)

追加 キャンセル

①説明：任意の説明を入力します。(未入力でも問題ありません)

②有効期限：クライアントシークレットの有効期限を設定します。

この有効期限が切れますとクライアントシークレットが使用できなくなり、メールの送受信が行えなくなります。
有効期限が切れた場合、(8)、(9)、(10)のクライアントシークレットの追加操作を行っていただき新しいクライアントシークレットの値を更新してください。

02 管理者による事前準備

(10)作成したクライアントシークレットの「値」をコピーします。

証明書 (0) クライアント シークレット (1) フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値 ①	シークレット ID
desknet's NEO	2025/10/8	...	...

必ず「値」をコピー シークレットIDと間違えないようご注意ください

値 ①

シークレット ID

※注意※

この値をコピーせずに画面遷移し、再度クライアントシークレット画面にアクセスすると、値にマスクがかかり、値のコピーすることができません。

値を発行後すぐにコピーするようお願いします。

コピーせず画面遷移した場合は、再度クライアントシークレットの再発行の操作を行ってください。

(11)画面左部のメニューから「管理」の下にある「API のアクセス許可」をクリックします。

ホーム > 株式会社ネオジャパン | アプリの登録 > desknet's NEO OAuth

desknet's NEO OAuth | API のアクセス許可

検索 最新の情報に更新 フィードバックがある場合

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランドとプロパティ

認証

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

⚠ テナント全体の同意を付与すると、そのアプリケーションに対してテナント全体に既に付与されているアクセス許可が取り消される場合があります。ユーザーが自分の代わりに付与済みのアクセス許可は影響を受けません。 [詳細情報](#)

🔗 API のアクセス許可 この列には、ご自分の組織や、こ

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環として、ユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ✓ 株式会社ネオジャパンに管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	いいえ	...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)をお試しください。

02 管理者による事前準備

(12) 「+ アクセス許可の追加」をクリックします。

ホーム > 株式会社ネオジャパン | アプリの登録 > desknet's NEO OAuth

desknet's NEO OAuth | API のアクセス許可

検索 最新の情報に更新 フィードバックがある場合

概要
クイックスタート
統合アシスタント
問題の診断と解決
管理
ブランド化とプロパティ
認証
証明書とシークレット
トークン構成
API のアクセス許可
API の公開
アプリ ロール
所有者
ロールと管理者
マニフェスト
サポート + トラブルシューティング

テナント全体の同意を付与すると、そのアプリケーションのアクセス許可は影響を受けません。 [詳細情報](#)

“管理者の同意が必要” 列には、組織の既定値のアプリが使用される組織の値が反映されていません。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環として、管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可が表示されます。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 株式会社ネオジャパンに管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				...
UserRead	委任済み	Sign in and read user profile	いいえ	...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)をお試しください。

(13) 「Microsoft Graph」をクリックします。

API アクセス許可の要求

API を選択します

Microsoft API 所属する組織で使用している API 自分の API

よく使用される Microsoft API



Microsoft Graph

Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Microsoft Entra ID、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。



Azure Communication Services

Microsoft Teams で使用されるのと同じセキュリティで保護された CPaaS プラットフォームを使用した豊富なコミュニケーション エクスペリエンス



Azure Rights Management Services

検証済みのユーザーに、保護されたコンテンツの読み取りと書き込みを許可します



Azure Service Management

Azure portal で利用できる機能の大部分へのプログラムによるアクセス

02 管理者による事前準備

(14)「委任されたアクセス許可」をクリックします。

API アクセス許可の要求

×

[すべての API](#)

Microsoft Graph

<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデモンとして実行されます。

(15)キーワード検索で「offline_access」と検索していただき、検索結果の「OpenId アクセス許可」の「offline_access」にチェックを入れ「アクセス許可の追加」ボタンをクリックします。

API アクセス許可の要求

×

[すべての API](#)

Microsoft Graph

<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデモンとして実行されます。

アクセス許可を選択する

① 「offline_access」と入力する

[すべて展開](#)

offline_access

ⓘ "管理者の同意が必要" 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

アクセス許可

② 「OpenId アクセス許可」の「offline_access」であることを確認しチェックを入れる

OpenId アクセス許可 (1)



offline_access ⓘ

Maintain access to data you have given it access to

いいえ

③ 「アクセス許可の追加」ボタンをクリックする

アクセス許可の追加

破棄

02 管理者による事前準備

(16)再度APIアクセス許可の要求画面を開き、キーワード検索で「IMAP.AccessAsUser.All」と検索していただき、検索結果の「IMAP」の「IMAP.AccessAsUser.All」にチェックを入れ「アクセス許可の追加」ボタンをクリックします。

API アクセス許可の要求

[すべての API](#)

Microsoft Graph

<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンドサービスまたはデーモンとして実行されます。

アクセス許可を選択する

① 「IMAP.AccessAsUser.All」と入力する

[すべて展開](#)

IMAP.AccessAsUser.All

「管理者の同意が必要」列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。[詳細情報](#)

アクセス許可

② 「IMAP」の「IMAP.AccessAsUser.All」であることを確認しチェックを入れる

IMAP (1)



IMAP.AccessAsUser.All ⓘ

Read and write access to mailboxes via IMAP.

いいえ

③ 「アクセス許可の追加」ボタンをクリックする

アクセス許可の追加

破棄



02 管理者による事前準備

(17)再度APIアクセス許可の要求画面を開き、キーワード検索で「POP.AccessAsUser.All」と検索していただき、検索結果の「POP」の「POP.AccessAsUser.All」にチェックを入れ「アクセス許可の追加」ボタンをクリックします。

API アクセス許可の要求

[すべての API](#)

Microsoft Graph

<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデーモンとして実行されます。

アクセス許可を選択する

① 「POP.AccessAsUser.All」と入力する

[すべて展開](#)

POP.AccessAsUser.All



"管理者の同意が必要" 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

アクセス許可

② 「POP」の「POP.AccessAsUser.All」であることを確認しチェックを入れる

POP (1)



POP.AccessAsUser.All ⓘ

Read and write access to mailboxes via POP.

いいえ

③ 「アクセス許可の追加」ボタンをクリックする

アクセス許可の追加

破棄



02 管理者による事前準備

(18)再度APIアクセス許可の要求画面を開き、キーワード検索で「SMTP.Send」と検索していただき、検索結果の「SMTP」の「SMTP.Send」にチェックを入れ「アクセス許可の追加」ボタンをクリックします。

API アクセス許可の要求

[すべての API](#)

Microsoft Graph

<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーとして、バックグラウンド サービスまたはデモンとして実行されます。

アクセス許可を選択する

① 「SMTP.Send」と入力する

[すべて展開](#)

SMTP.Send

「管理者の同意が必要」列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

アクセス許可

② 「SMTP」の「SMTP.Send」であることを確認しチェックを入れる

SMTP (1)



SMTP.Send ⓘ

Send emails from mailboxes using SMTP AUTH.

いいえ

③ 「アクセス許可の追加」ボタンをクリックする

アクセス許可の追加

破棄

上記設定がすべて完了しますと、下記画像のようにアクセス許可の一覧が表示されます。

[+ アクセス許可の追加](#) [✓ 株式会社ネオジャパンに管理者の同意を与えます](#)

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (5)				
IMAP.AccessAsUser.All	委任済み	Read and write access to mailboxes via IMAP.	いいえ	✓ 株式会社ネオジャパンに...
offline_access	委任済み	Maintain access to data you have given it access to	いいえ	✓ 株式会社ネオジャパンに...
POP.AccessAsUser.All	委任済み	Read and write access to mailboxes via POP.	いいえ	✓ 株式会社ネオジャパンに...
SMTP.Send	委任済み	Send emails from mailboxes using SMTP AUTH.	いいえ	✓ 株式会社ネオジャパンに...
User.Read	委任済み	Sign in and read user profile	いいえ	✓ 株式会社ネオジャパンに...

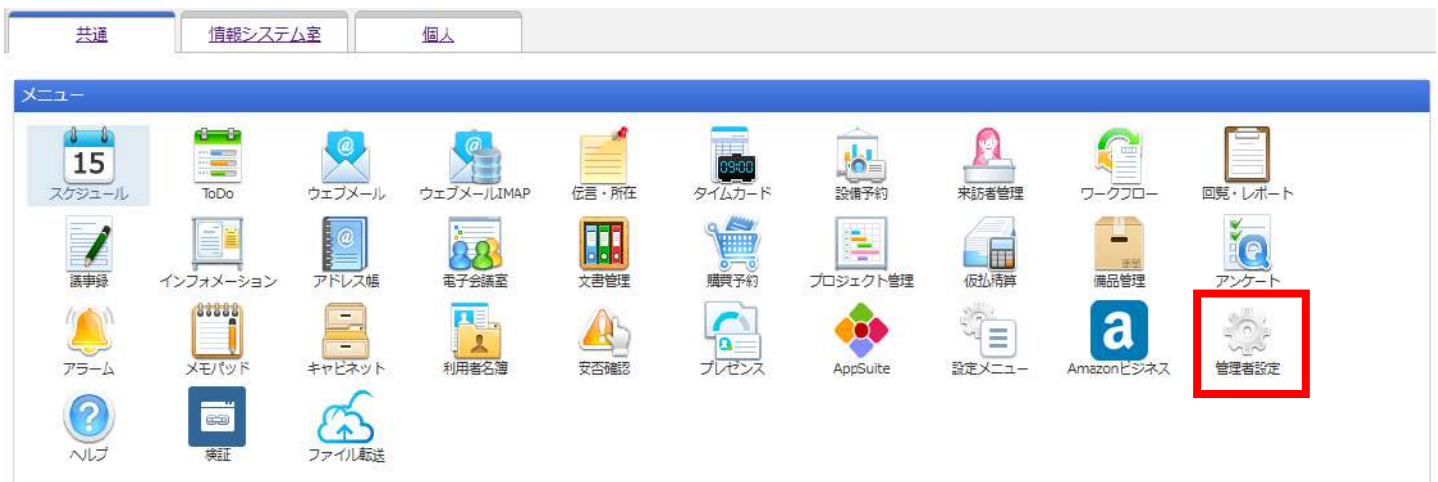
Azureでの設定は以上になります。次ページからはdesknet's NEOでの設定になります。

2.管理者による事前設定（desknet's NEO）

[管理者による事前設定（Azure）](#)にて設定したアプリ情報を用いて

desknet's NEO側でOAuth認可サーバーの登録する手順を記載いたします。

- (1)管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「**管理者設定**」の歯車アイコンをクリックします。



- (2)管理者設定画面の右上の歯車アイコンをクリックし、システム設定 > OAuth認可サーバー設定 を選択します。



02 管理者による事前準備

(3)OAuth認可サーバー設定で「認可サーバーの追加」ボタンをクリックします。

(4)登録画面にて必要事項を記入いたします。

項目	入力値
①認可サーバー名	任意の認可サーバー名を入力します。 ※“OAuth認証”等、分かりやすい名称を推奨します。
②サービス	Microsoft365を選択します。
③クライアントID	「 管理者による事前設定 (Azure) 」の⑥でコピーしたクライアントIDを入力します。
④クライアントシークレット	「 管理者による事前設定 (Azure) 」の⑩でコピーしたクライアントシークレットを入力します。

desknet's NEO上での事前設定は以上になります。これから先はお客様がご利用になる機能によって設定する箇所が異なりますので、次ページをご確認ください。

3.事前設定がすべて完了した後の流れについて

[管理者による事前設定 \(Azure\)](#) と、[管理者による事前設定 \(desknet's NEO\)](#) がすべて完了した後は、各機能でメールサーバー設定を行っていただき、メールが利用できるようになりますが、**ご利用ケースによって設定箇所が異なります。**

下記の目次からご利用ケースに沿った設定ページに移動してください。

1. スケジュールやワークフロー機能等の**通知メール機能**を使用したい

もしくはウェブメールやファイル転送など**複数機能で一括**でMicrosoft365のメールサーバーを設定したい

[管理者設定のメールサーバー設定を行う](#)

※ウェブメールIMAPは管理者設定のメールサーバー機能を使用することができません。

3のIMAPのメールサーバー設定から設定を行っていただきますようお願いいたします。

2. **ウェブメール機能**のみMicrosoft365のメールサーバー設定を設定しアカウントを設定したい

[ウェブメール機能のメールサーバー設定を行う](#)

3. **ウェブメールIMAP機能**を利用したい

[ウェブメールIMAPのメールサーバー設定を行う](#)

4. **ファイル転送機能**のみMicrosoft365のメールサーバー設定を行いたい

[ファイル転送のメールサーバー設定を行う](#)

5. **安否確認機能**のみMicrosoft365のメールサーバー設定を行いたい

[安否確認機能のメールサーバー設定を行う](#)



管理者設定のメールサーバー設定

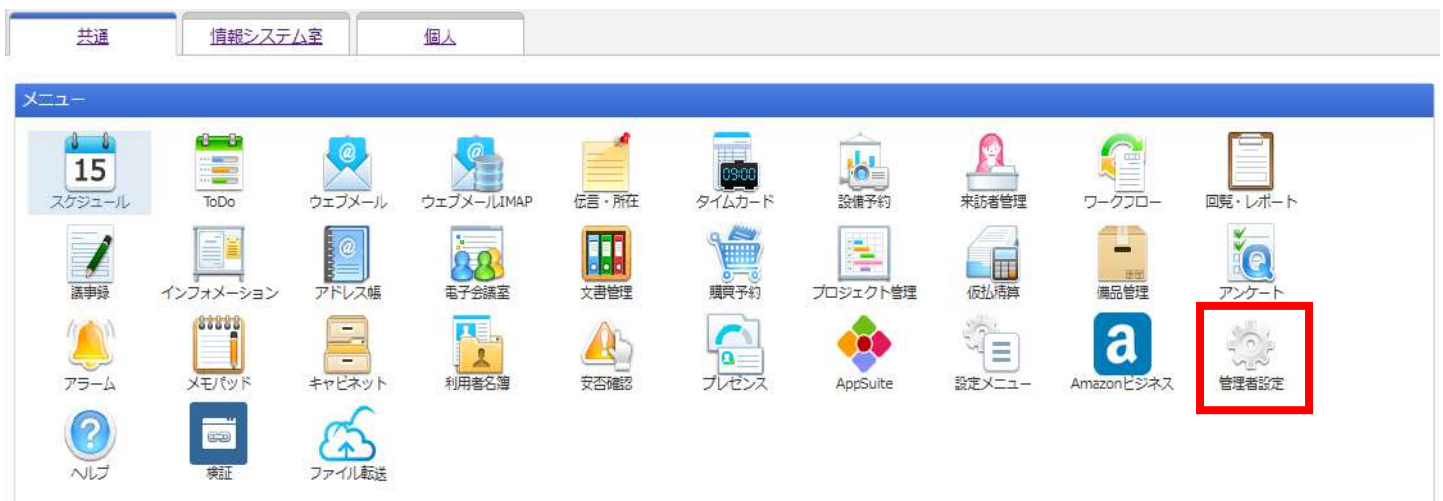
管理者による事前設定 (Azure) と、管理者による事前設定 (desknet's NEO) がすべて完了した後の設定になります。

スケジュールやワークフロー機能等の**通知メール機能**を使用したい

もしくはウェブメールやファイル転送など**複数機能で一括**でMicrosoft365のメールサーバーを設定したい場合はこちらから設定いただきますようお願いいたします。

1. 管理者設定のメールサーバー設定

(1) 管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「**管理者設定**」の歯車アイコンをクリックします。



(2) 管理者設定画面の右上のスパナアイコンをクリックし、**システム設定 > メールサーバー設定** を選択します。



03 管理者設定のメールサーバー設定

(2)メールサーバー設定画面にて必要事項を記入します。

管理者設定 > システム設定

設定機能： 管理者設定

変更

メールサーバー設定

受信メールサーバー：(POP3)

サーバー名：

ポート番号： ※ 通常は110で設定します。

通信の保護：

なし

※ この値は、以下の機能で使います。

・ウェブメール：「アカウント設定」

・文書管理：「メール取込設定」

送信メールサーバー：(SMTP)

サーバー名：

smtp.office365.com

 ①

ポート番号：

587

 ②

通信の保護：

STARTTLS

 ③

STARTTLS通信時の認証について

メール送信時の認証

認証しない

POP before SMTP

SMTP認証

XOAUTH2認証

認証方式：

標準

認証方式：

LOGIN

OAuth認可サーバー：

OAuth認証

 ④

※ この値は、以下の機能で使います。

・ウェブメール：「アカウント設定」

・安否確認：「配信メールサーバー設定」

・ファイル転送：「送信メールサーバー設定」

※ この値は、メール通知機能を「使用する」とした場合に利用されます。

サーバータイムアウト(秒)：

60

項目	入力値
①サーバー名	「smtp.office365.com」を入力します。
②ポート番号	「587」を記入します。
③通信の保護	「STARTTLS」を選択します。
④メール送信時の認証	「XOAUTH2認証」を選択し、「OAuth認可サーバー」では こちら で登録しました認可サーバーを選択します。

設定は次ページへ続きます。



03 管理者設定のメールサーバー設定

メール通知設定

メール通知機能 : 使用する ▼
※ この値を「使用する」とした場合、以下のことが行えます。
▶ [メール通知利用機能一覧](#)

送信元メールアドレス : ☐ メール送信ユーザーの職場用メールアドレス
※ 「メール送信時の認証」で「XOAUTH2認証」を選択した場合、この項目は選択できません。

☐ [会社情報設定]で設定されたメールアドレス
→(未設定)

☒ 任意のメールアドレス

※ 「"表示名"<メールアドレス>」、「<メールアドレス>」、「メールアドレス」のいずれかの形式で入力してください。
例) 「"ネオジャパン"<desknets@your.domain>」、「<desknets@your.domain>」、「desknets@your.domain」

送信時の認証情報 : ユーザーID :
パスワード :
 (未認証)

※ 「メール送信時の認証」で「XOAUTH2認証」を選択した場合は、「OAuth認可サーバー」で選択したサーバーに対して[OAuth認可サーバー認証]で認証してください。
※ 「OAuth認可サーバー」でサーバーを選択した場合に[OAuth認可サーバー認証]ボタンが有効になります。

← 変更

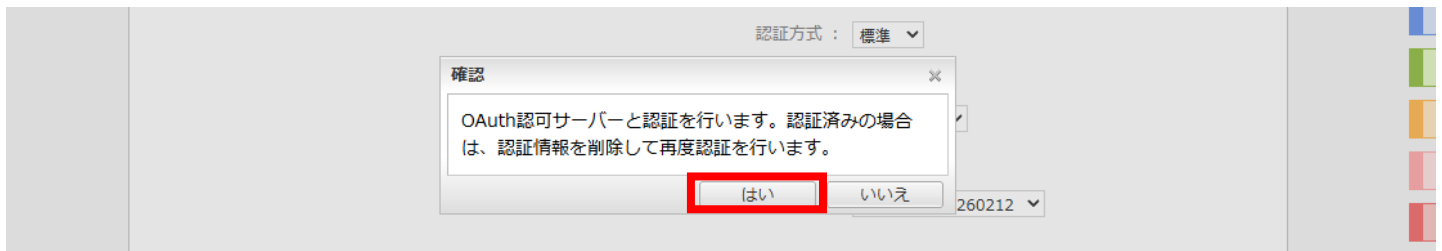
項目	入力値
⑤送信元メールアドレス	「[会社情報設定]で設定されたメールアドレス」もしくは「任意のメールアドレス」を選択しメールアドレスを設定します。
⑥送信時の認証情報（ユーザーID）	⑤で設定した送信元メールアドレスと同じメールアドレスを入力します。
⑦OAuth認可サーバー認証	ボタンを押して認証を実施します（Microsoft365の画面が立ち上がり認証を行います） ※必ず⑤で指定した送信元メールアドレスと同じアカウントでサインインした状態で認証を行ってください。 一度ブラウザ上からMicrosoft365のサインアウトを実施していただき、認証ボタンを押しますとMicrosoft365のサインイン画面が表示され、対象のアカウントでサインインすると確実に正しく認証できます。

⑦のOAuth認可サーバー認証の具体的な流れについては次ページでご案内します。

03 管理者設定のメールサーバー設定

OAuth認可サーバーのボタンを押しますと下記ダイアログが表示されますので「はい」を押します。

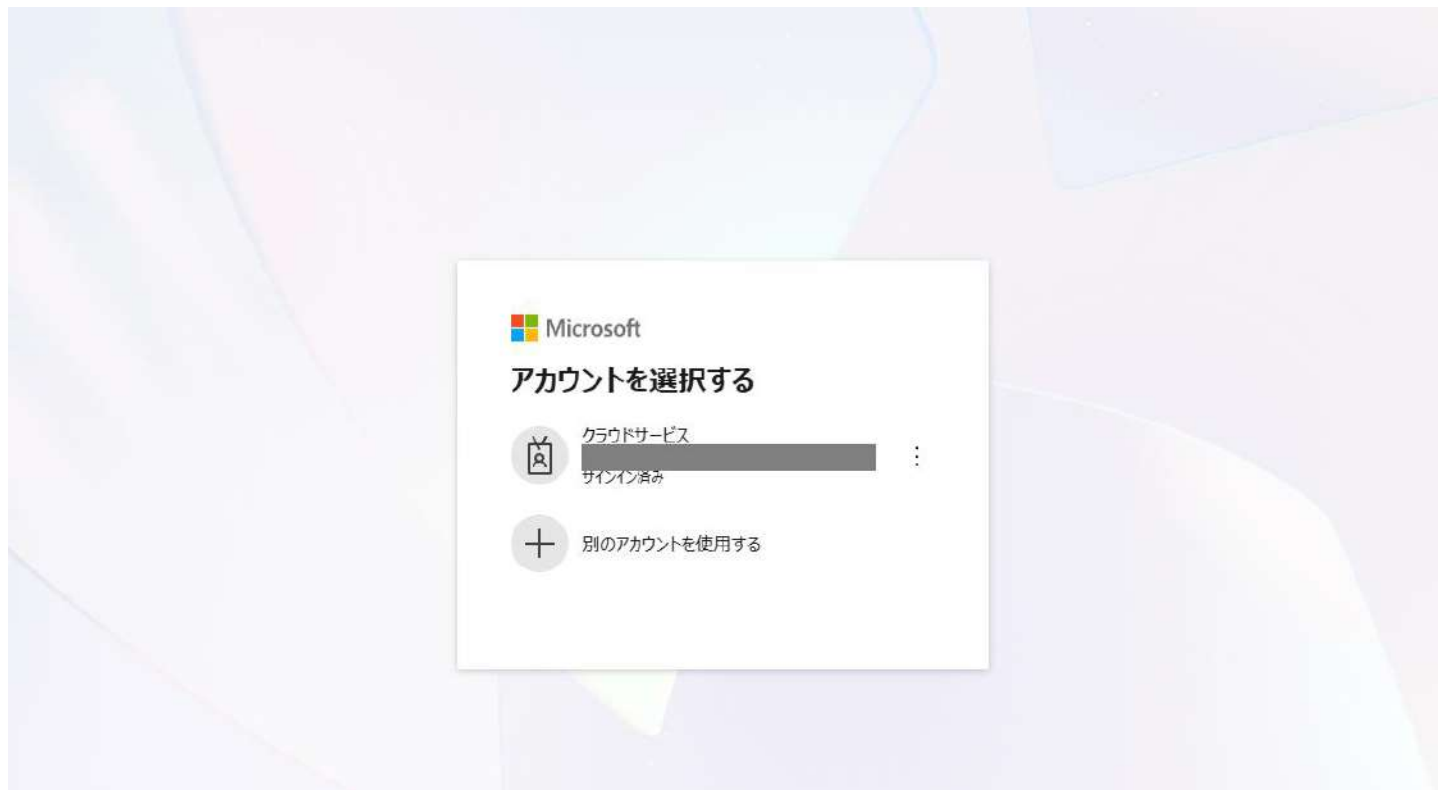
※認証を実施する前にブラウザ上からMicrosoft365アカウントからサインアウトすることをお勧めします。



「はい」を押した後にMicrosoft365のサインイン画面が表示されますので、

送信元メールアドレスのアカウントと同じアカウントを選択

(同じアカウントが表示されていない場合は「別のアカウントを使用する」を選択) していただき、サインインを実施します。



サインインが完了しますと「(認証日時)認証済み」と表記され、認証処理が完了となります。



「管理者設定」のメールサーバー設定は以上になります。

利用したい機能によって次の設定箇所が異なりますので、次ページをご確認ください。



2.設定後の流れについて

- ・ **スケジュールやワークフロー等の通知メールを使用し、ウェブメール、ファイル転送、安否確認機能は使用しない場合**

→設定は以上になります。各機能で通知メールをお試しいただき、メールが送信されるかご確認いただきますようお願いいたします。

- ・ **ウェブメール機能を使用したい場合**

→ウェブメール機能のアカウント設定でアカウント情報の入力と認証操作が必要となります。

以下から設定いただきますようお願いいたします。

[ウェブメール機能でアカウント設定を行う](#)

- ・ **ファイル転送機能を使用したい場合**

→ファイル転送機能のメールサーバー設定にて、使用するサーバー設定の選択と認証操作が必要となります。

以下から設定いただきますようお願いいたします。

[ファイル転送機能のメールサーバー設定を行う](#)

- ・ **安否確認機能を使用したい場合**

→安否確認機能のメールサーバー設定にて、使用するサーバー設定の選択と認証操作が必要となります。

以下から設定いただきますようお願いいたします。

[安否確認機能のメールサーバー設定を行う](#)



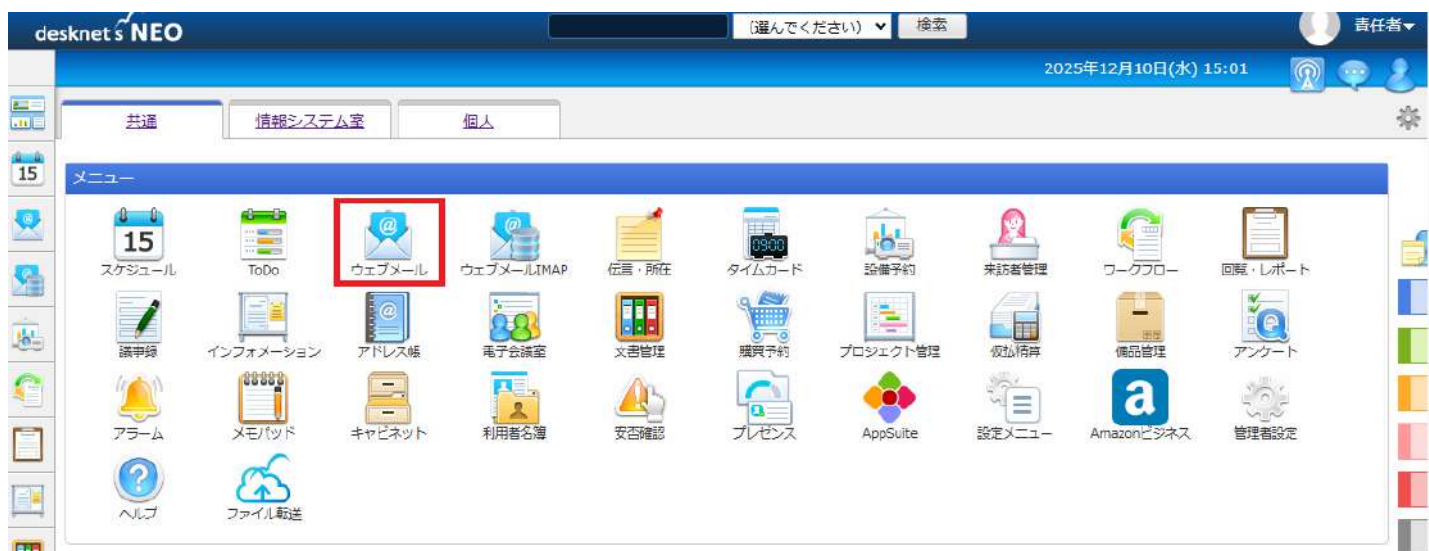
04

ウェブメール機能の設定

管理者による事前設定 (Azure) と、管理者による事前設定 (desknet's NEO) がすべて完了した後の設定になります。

1.ウェブメール機能のアカウント設定

(1)管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「ウェブメール」のアイコンをクリックします。



(2)各ユーザーでメール機能を使用するためのアカウント設定を行います。

「ウェブメールは別ウィンドウで開かれます～」の画面から右上の歯車アイコンをクリックし、「機能管理 > 個人アカウント設定 > アカウント設定」を選択します。



04 ウェブメール機能の設定

(3)アカウント設定画面で設定させたいアカウント名をクリックします。

ウェブメール > 機能管理 > 個人アカウント設定 > アカウント設定

← 利用させる 利用させない 全3件

組織選択 情報システム室

☐ 氏名	アカウント名	メール受信	利用
☐ ユーザーA	該当するデータはありません。		利用させる
☐ ユーザーB	該当するデータはありません。		利用させる
☐ ユーザーC	該当するデータはありません。		利用させる

← 利用させる 利用させない 全3件

Copyright (C)2012-2025 NEOJAPAN Inc. All Rights Reserved.

(4)[アカウントの追加]のボタンをクリックします。

ウェブメール > 機能管理 > 個人アカウント設定 > アカウント設定

← **アカウントの追加** 通常使用するアカウントの変更

該当するデータはありません。

← アカウントの追加 | 通常使用するアカウントの変更

Copyright (C)2012-2025 NEOJAPAN Inc. All Rights Reserved.

04 ウェブメール機能の設定

(5)アカウントの設定画面で各種設定を行います。入力する値は次ページをご確認ください。

追加

キャンセル

アカウントの追加

アカウント名(*) :

ユーザーA

メール受信

行う

表示名 :

ユーザーA

メールアドレス(*) :

受信時のログ :

☒ 出力しない

☐ 出力する

※ 「出力する」を選択した場合、メールを受信する際のメールサーバーとの通信ログを出力します。

送信時のログ :

☒ 出力しない

☐ 出力する

※ 「出力する」を選択した場合、メールを送信する際のメールサーバーとの通信ログを出力します。

受信メールサーバー

サーバー(POP3) :

☐ 管理者設定の[メールサーバー設定]で設定された受信メールサーバー(POP3)を使用する。

サーバー名 :

未設定

ポート番号 :

未設定

通信の保護 :

なし

☒ ウェブメールのメールサーバー設定で設定された受信メールサーバー(POP3)を使用する。

サーバー名 :

outlook.office365.com

ポート番号 :

995

通信の保護 :

SSL/TLS

☐ 個別に設定する。

サーバー名 :

ポート番号 :

110

※ 通常は110で設定します。

通信の保護 :

なし

ユーザーID :

パスワード :

認証方式 :

☐ 標準

☐ 標準(APOP)

☒ XOAUTH2

OAuth認可サーバー :

OAuth認証

認証

(未認証)

※ メールサーバーとして、Google、Microsoft 365を使用する場合、XOAUTH2を選択し、OAuth認可サーバーを選択して認証を行ってください。

サーバータイムアウト(秒) :

60

その他設定 :

☐ 受信メールをサーバーに残す。サーバーに残す日数 :

※ 受信したメールの「受信日時」から入力した日数を経過したメールをサーバーから削除します。

※ 日数が未入力の場合は無期限にサーバーに残ります。



04 ウェブメール機能の設定

項目	入力値
①メールアドレス	対象アカウントのメールアドレス情報を入力します。
②サーバー(POP3)	お客様の設定状況にて設定値が異なります。 ・管理者設定のメールサーバー設定にてメールサーバーを設定済みの場合 →「管理者設定の[メールサーバー設定]で設定された受信メールサーバー(POP3)を使用する。」を選択します。 ・ウェブメール機能のメールサーバー設定を設定済みの場合 →「ウェブメールのメールサーバー設定で設定された受信メールサーバー(POP3)を使用する。」を選択します。 ウェブメール機能のみMicrosoft365のメールサーバー設定を行いたい場合は こちら からメールサーバー設定を行ってください。 ・上記未設定で対象アカウントのみMicrosoft365のメールサーバー設定を行いたい場合 →「個別に設定する」を設定し、以下の設定値を入力します。 サーバー名：outlook.office365.com ポート番号：995 通信の保護：SSL/TLS
③ユーザーID	①で入力したメールアドレスを入力します。
④認証方式	「XOAUTH2」を選択し、OAuth認可サーバー認証は 管理者設定による事前設定 (desknet's NEO) で設定したOAuth認可サーバー設定を選択します。 ※「認証」のボタンでは、必ず①で指定したメールアドレスと同じMicrosoft365アカウントでサインインした状態で認証を行う必要がございます。 管理者にて対象のMicrosoft365アカウントでサインインできない場合、こちらのボタンを押さないで未認証のままでも設定は保存いただけます。一般アカウントで対象のMicrosoft365アカウントでサインインして認証を行う場合は、31ページからの手順で認証を実施してください。
⑤その他設定	受信したメールをメールサーバー上に残すかどうかの設定を行います。 ※Outlook等の他のメーラーで対象のメールアドレスのメールを確認することがある場合は必ずチェックを入れてください。

送信メールサーバー設定の設定値は次ページになります。



04 ウェブメール機能の設定

送信メールサーバー設定の設定画面になります。入力値は次ページをご確認ください。

送信メールサーバー

サーバー(SMTP) : ☐ 管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。

サーバー名 : smtp.gmail.com

ポート番号 : 465

通信の保護 : SSL/TLS

送信時の認証 : SMTP認証

☒ ウェブメールのメールサーバー設定で設定された送信メールサーバー(SMTP)を使用する。

サーバー名 : smtp.office365.com

ポート番号 : 587

通信の保護 : STARTTLS

送信時の認証 : XOAUTH2認証(OAuth認証)

☐ 個別に設定する。

サーバー名 :

ポート番号 : ※ 通常は25で設定します。

通信の保護 : なし

▶ [STARTTLS通信時の認証について](#)

送信時の認証 : ☒ 認証しない

☐ POP before SMTP

※ この値を選択した場合、メール送信する際に受信メールサーバーの認証を行います。

☐ SMTP認証

認証方式 : CRAM-MD5

☐ XOAUTH2認証

OAuth認可サーバー : なし

※ この値を選択した場合、メール送信する際にXOAUTH2認証を行います。

送信時の認証情報 :

ユーザーID :

パスワード :

(未認証)

※ 「送信時の認証」に「SMTP認証」を選択している場合、「ユーザーID」と「パスワード」を設定してください。省略した場合は、受信メールサーバーのユーザーIDとパスワードで認証します。

※ 「送信時の認証」に「XOAUTH2認証」を選択している場合、「ユーザーID」を設定し、「OAuth認可サーバー」で選択したサーバーに対して[OAuth認可サーバー認証]で認証してください。

※ (*)は必須項目です。

04 ウェブメール機能の設定

項目	入力値
⑥サーバー(SMTP)	お客様の設定状況にて設定値が異なります。 ・ 管理者設定のメールサーバー設定にてメールサーバーを設定済みの場合 → 「管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。」を選択します。 ・ ウェブメール機能のメールサーバー設定を設定済みの場合 → 「ウェブメールのメールサーバー設定で設定された送信メールサーバー(SMTP)を使用する。」を選択します。 ウェブメール機能のみMicrosoft365のメールサーバー設定を行いたい場合はこちらからメールサーバー設定を行ってください。 ・ 上記未設定で対象アカウントのみMicrosoft365のメールサーバー設定を行いたい場合 → 「個別に設定する」を設定し、以下の設定値を入力します。 サーバー名：smtp.office365.com ポート番号：587 通信の保護：STARTTLS
⑦送信時の認証情報	送信時の認証情報を入力します。「ユーザーID」の項目は、①のメールアドレスと同じ値を入力します。 ※「OAuth認可サーバー認証」のボタンでは、必ず①で指定したメールアドレスと同じMicrosoft365アカウントでサインインした状態で認証を行う必要がございます。 管理者にて対象のMicrosoft365アカウントでサインインできない場合、こちらのボタンを押さないで未認証のままでも設定は保存いただけます。一般アカウントで対象のMicrosoft365アカウントでサインインして認証を行う場合は、次ページの手順で認証を実施してください。

設定後「追加」ボタンを押しますとアカウントが登録されます。
管理者にてアカウント設定を行う手順は以上になります。
アカウント個別にOAuth認証を実施する手順は次ページをご確認ください。

2. アカウント個別にOAuth認証を行う

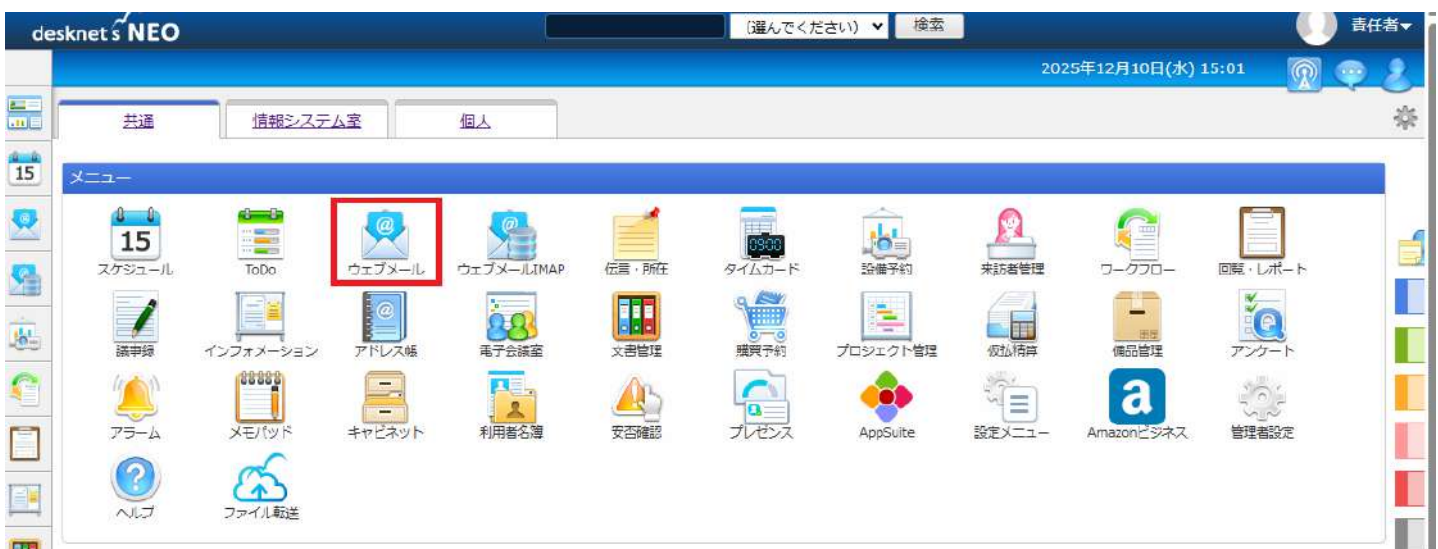
[ウェブメール機能のアカウント設定](#)にてアカウント登録後、

個別にアカウントでOAuth認証を行う手順になります。

※ユーザーで認証を行う場合は【管理者設定】 - 【共通設定】にて

「個人毎のアカウント設定」欄が「許可する」と設定されている必要があります。

(1)対象のアカウントでログイン後、トップ画面のメニューから「ウェブメール」をクリックします。

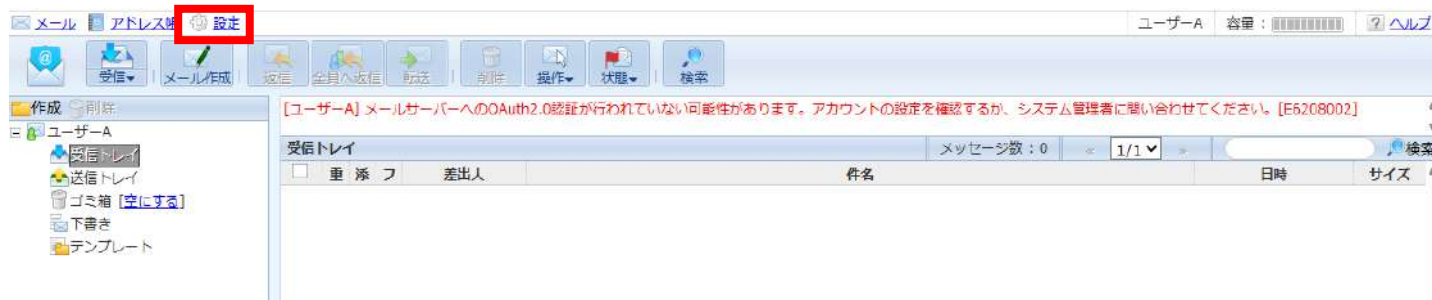


(2)クリックすると別ウィンドウが開かれますが、開かれない場合、
画像にある「ウェブメール」のリンクをクリックします。



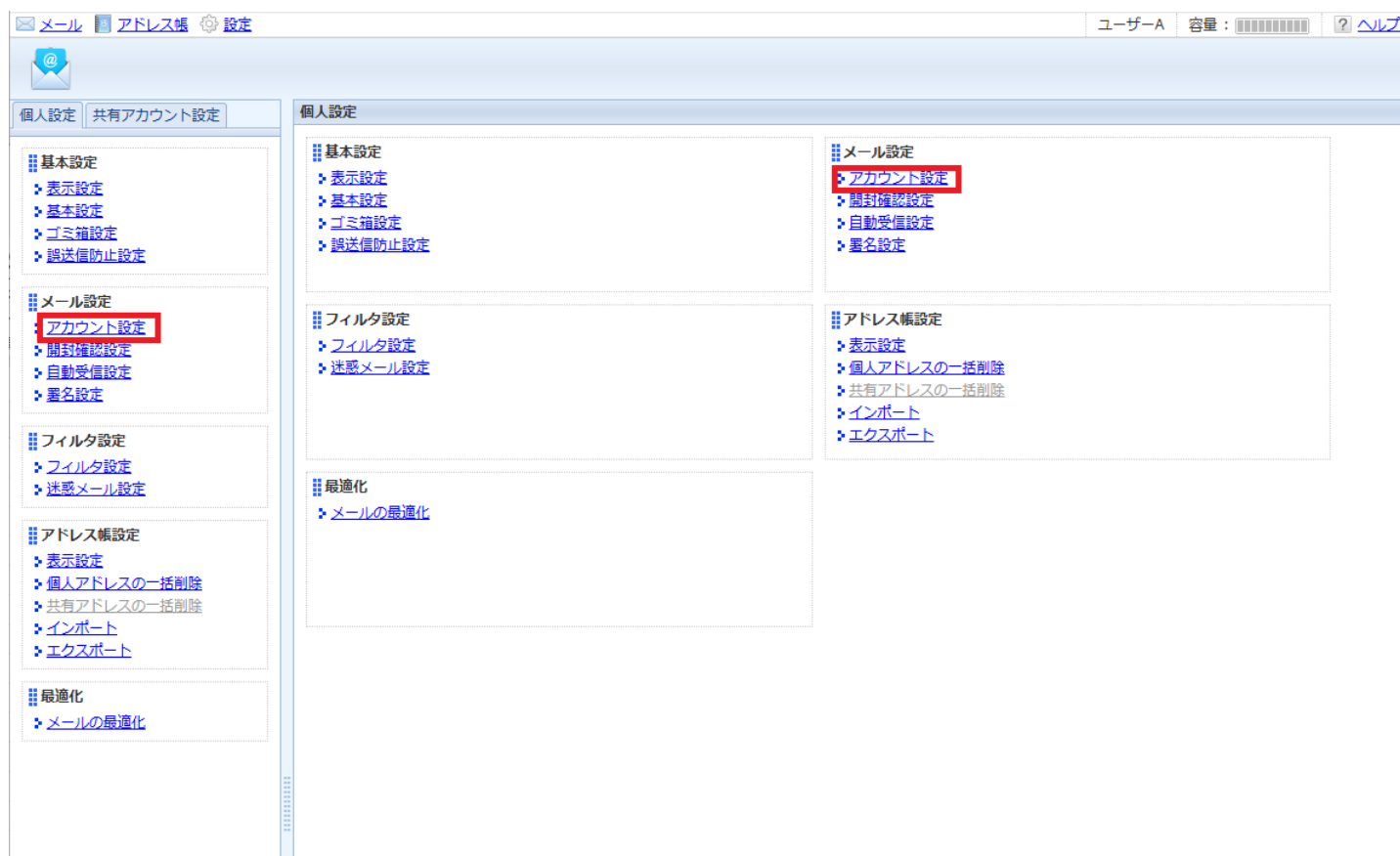
04 ウェブメール機能の設定

(3)受信トレイ画面左上にあります「設定」のリンクをクリックします。



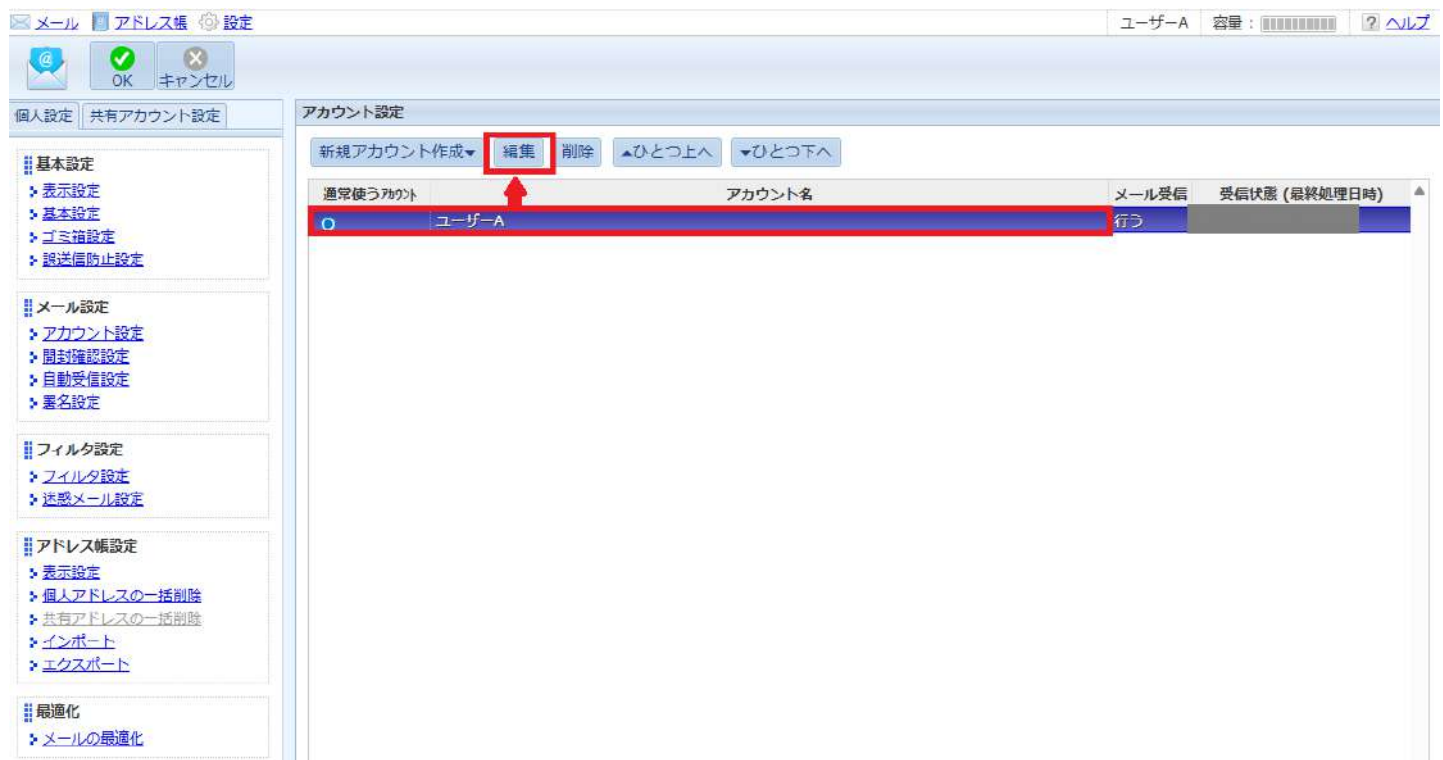
機能管理でアカウントを先に作成し、そこでOAUTH認証の操作を行っていない場合、上記のエラーが表示されますが、そのまま「設定」のリンクをクリックしてください。

(4)各種設定の中の「アカウント設定」のリンクをクリックします。



04 ウェブメール機能の設定

(5)アカウント名をクリックし選択した状態で上部の「編集」ボタンをクリックします。



(6)アカウント設定画面の「受信メールサーバー(POP3)」の中にあります「認証方式」にて「XOAUTH2」を選択します。OAuth認可サーバーは[管理者設定による事前設定 \(desknet's NEO\)](#)で設定したOAuth認可サーバー設定を選択します。

受信メールサーバー(POP3)

メールサーバー情報

☐ 管理者設定の[メールサーバー設定]で設定された受信メールサーバー(POP3)を使用する。
 サーバー名: 未設定
 ポート番号: 未設定
 通信の保護: なし

☒ ウェブメールのメールサーバー設定で設定された受信メールサーバー(POP3)を使用する。
 サーバー名: outlook.office365.com
 ポート番号: 995
 通信の保護: SSL/TLS

☐ 個別に設定する。
 サーバー名:
 ポート番号: ※ 通常は110で設定します。
 通信の保護:

ユーザーID

パスワード

認証方式

☐ 標準
☐ 標準(APOP)
☒ XOAUTH2
 OAuth認可サーバー: (未認証)

※ メールサーバーとして、Google、Microsoft 365を使用する場合、XOAUTH2を選択し、OAuth認可サーバーを選択して認証を行ってください。

04 ウェブメール機能の設定

(7)「送信メールサーバー(SMTP)」の設定では「送信時の認証情報」のユーザーIDにて
アカウント設定のメールアドレス情報を入力します。

送信メールサーバー(SMTP)	
メールサーバー情報	☐ 管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。 サーバー名：未設定 ポート番号：未設定 通信の保護：なし 送信時の認証：認証しない ☒ ウェブメールのメールサーバー設定で設定された送信メールサーバー(SMTP)を使用する。 サーバー名：smtp.office365.com ポート番号：587 通信の保護：STARTTLS 送信時の認証：XOAUTH2認証(OAuth認証) ☐ 個別に設定する。 サーバー名： ポート番号： 25 ※ 通常は25で設定します。 通信の保護： なし ▶ STARTTLS通信時の認証について 送信時の認証：☒ 認証しない ☐ POP before SMTP ※ この値を選択した場合、メール送信する際に受信メールサーバーの認証を行います。 ☐ SMTP認証 認証方式： CRAM-MD5 ※ この値を選択した場合、メール送信する際にSMTP認証を行います。 ☐ XOAUTH2認証 OAuth認可サーバー： なし ※ この値を選択した場合、メール送信する際にXOAUTH2認証を行います。
送信時の認証情報	ユーザーID： @neosupport.onmicrosoft.com パスワード： OAuth認可サーバー認証 (未認証) ※ 「送信時の認証」に「SMTP認証」を選択している場合、「ユーザーID」と「パスワード」を設定してください。省略した場合は、受信メールサーバーのユーザーIDとパスワードで認証します。 ※ 「送信時の認証」に「XOAUTH2認証」を選択している場合、「ユーザーID」を設定し、「OAuth認可サーバー」で選択したサーバーに対して[OAuth認可サーバー認証]で認証してください。

上記設定後、「OAuth認可サーバー認証」のボタンを押して認証操作を行います。

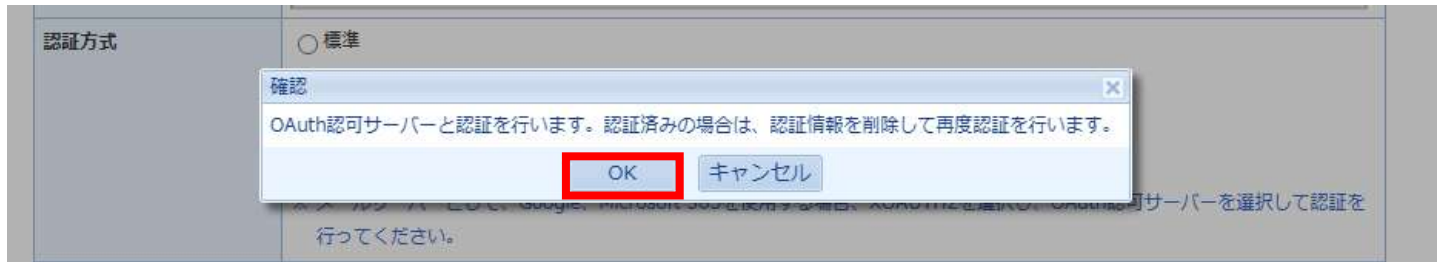
認証の流れについては次のページでご案内いたします。

※ 認証を実施する前にブラウザ上からMicrosoft365アカウントからサインアウトすることをお勧めします。

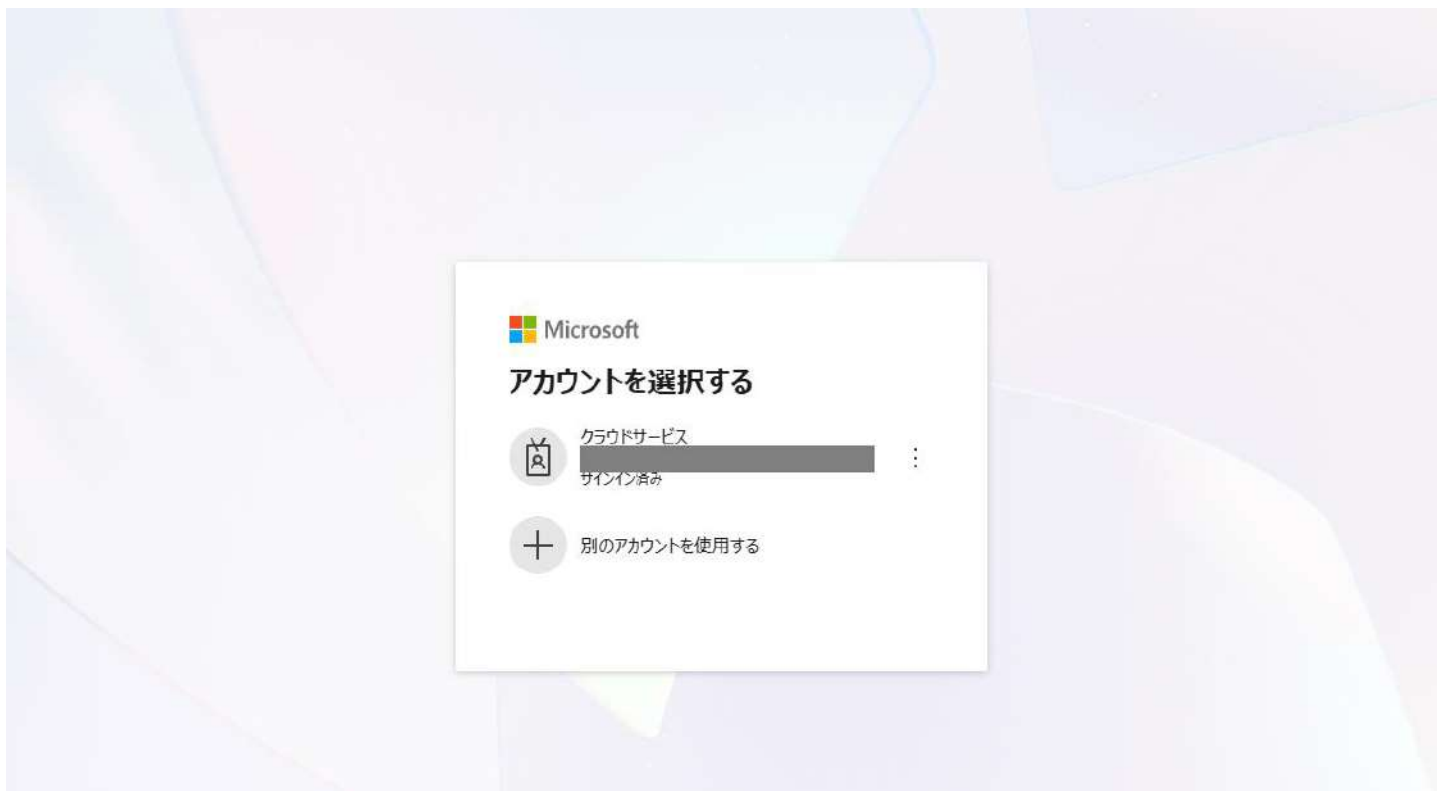


04 ウェブメール機能の設定

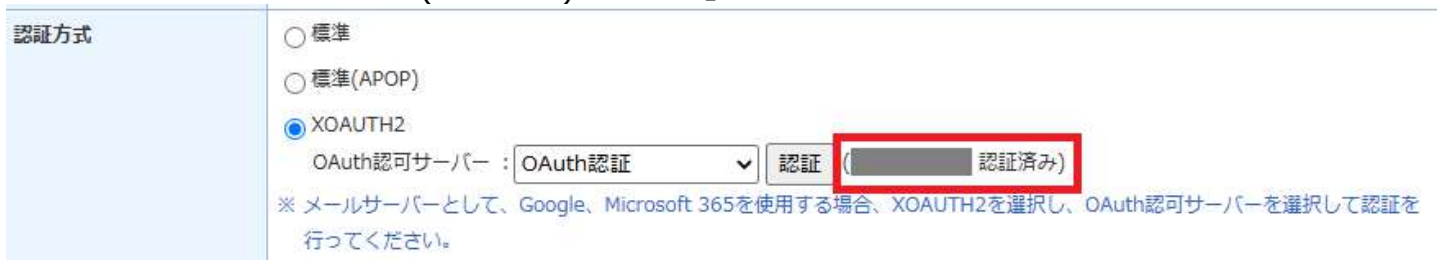
OAuth認可サーバーのボタンを押しますと下記ダイアログが表示されますので「OK」を押します。



「OK」を押した後にMicrosoft365のサインイン画面が表示されますので、
送信元メールアドレスのアカウントと同じアカウントを選択
 （同じアカウントが表示されていない場合は「別のアカウントを使用する」を選択）
 していただき、サインインを実施します。



サインインが完了しますと「(認証日時)認証済み」と表記され、認証処理が完了となります。



アカウント個別にOAuth認証を行う操作は以上になります。



3.ウェブメール機能単体のメールサーバー設定

ウェブメール機能のみMicrosoft365のメールを使用しする場合の、メールサーバー設定を行うための設定手順になります。

- (1)desknet's NEOに管理者権限を持ったユーザーでログインしていただき、メニューの「ウェブメール」のアイコンをクリックします。



- (2)「ウェブメールは別ウィンドウで開かれます～」の画面が表示されますので、その画面右上の歯車アイコンをクリックし、**システム管理 > メールサーバー設定** を選択します。



04 ウェブメール機能の設定

(3)メールサーバー設定画面が開かれますので、以下の設定値で入力します。

ウェブメール > システム管理

設定機能：ウェブメール

変更

メールサーバー設定

受信メールサーバー：(POP3)

サーバー名：outlook.office365.com

ポート番号：995 ※ 通常は110で設定します。

通信の保護：SSL/TLS

送信メールサーバー：(SMTP)

サーバー名：smtp.office365.com

ポート番号：587 ※ 通常は25で設定します。

通信の保護：STARTTLS

STARTTLS通信時の認証について

メール送信時の認証：○ 認証しない

○ POP before SMTP

※ この値を選択した場合、メール送信する際に受信メールサーバーの認証を行います。

○ SMTP認証

認証方式：LOGIN

※ この値を選択した場合、メール送信する際にSMTP認証を行います。

● XOAUTH2認証

OAuth認可サーバー：OAuth認証

※ この値を選択した場合、OAuth2認証を行います。

サーバータイムアウト(秒)：60

変更

項目	入力値
①受信メールサーバー(POP3)：サーバー名	「outlook.office365.com」を入力します。
②受信メールサーバー(POP3)：ポート番号	「995」を記入します。
③受信メールサーバー(POP3)：通信の保護	「SSL/TLS」を選択します。
④送信メールサーバー(SMTP)：サーバー名	「smtp.office365.com」を入力します。
⑤送信メールサーバー(SMTP)：ポート番号	「587」を記入します。
⑥受信メールサーバー(POP3)：通信の保護	「STARTTLS」を選択します。
⑦メール送信時の認証	「XOAUTH2認証」を選択し、「OAuth認可サーバー」ではこちらで登録しました認可サーバーを選択します。

メールサーバー設定は以上になります。「変更」ボタンを押して更新を完了します。

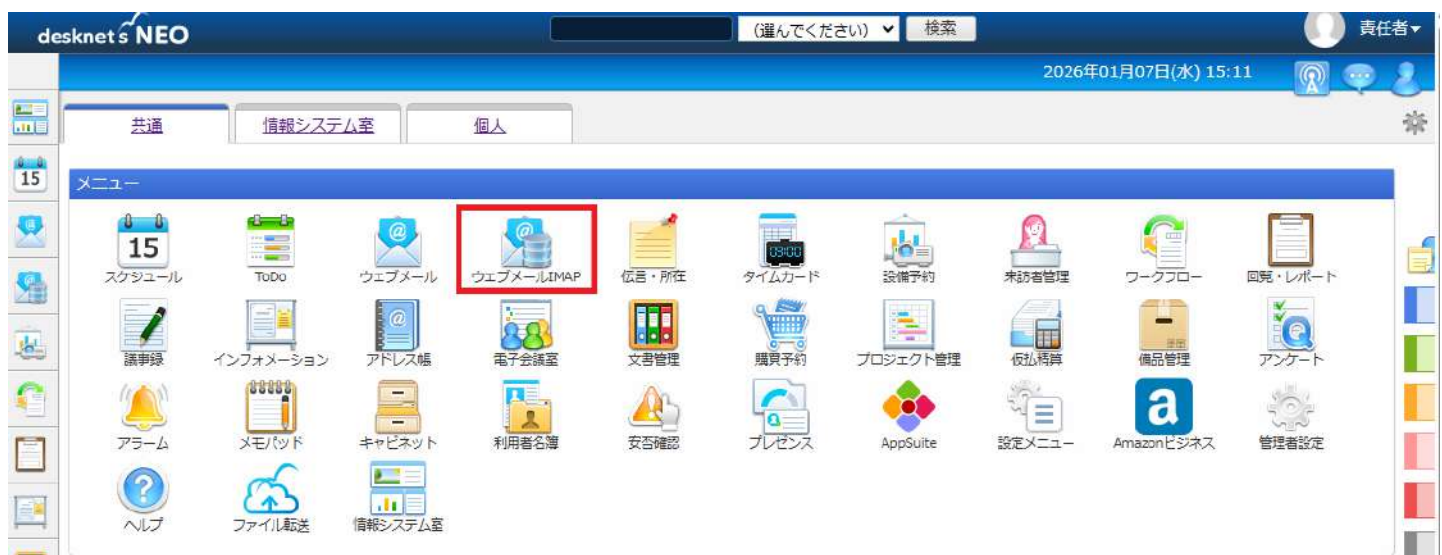
ウェブメールIMAP機能の設定

管理者による事前設定 (Azure) と、管理者による事前設定 (desknet's NEO) の設定がすべて完了した後の設定する項目になります。

ウェブメールIMAPは機能内でのメールサーバー設定が必要となるので、サーバー設定からアカウント設定までの手順を掲載いたします。

1.ウェブメールIMAPのメールサーバー設定

(1)管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「ウェブメールIMAP」のアイコンをクリックします。



(2)「ウェブメールIMAPは別ウィンドウで開かれます～」の画面が表示されますので、その画面右上の歯車アイコンをクリックし、**システム管理 > メールサーバー設定** を選択します。



05 ウェブメールIMAP機能の設定

(3)メールサーバー設定画面が開かれますので、設定値を入力し、「変更」ボタンを押して完了します。

ウェブメールIMAP > システム管理

設定機能: ウェブメールIMAP

変更

メールサーバー設定

受信メールサーバー :
(IMAP)

サーバー名 : outlook.office365.com ①

ポート番号 : 993 ※ 通常は143で設定します。 ②

通信の保護 : SSL/TLS ③

送信メールサーバー :
(SMTP)

サーバー名 : smtp.office365.com ④

ポート番号 : 587 ※ 通常は25で設定します。 ⑤

通信の保護 : SSL/TLS ⑥

STARTTLS通信時の認証について

メール送信時の認証 : ☐ 認証しない

☐ SMTP認証

認証方式 : CRAM-MD5

※ この値を選択した場合、メール送信する際にSMTP認証を行います。

☒ XOAUTH2認証

OAuth認可サーバー : なし ⑦

※ この値を選択した場合、OAuth2認証を行います。

OAuth認証

サーバータイムアウト(秒) : 60

ルートフォルダ :

送信トレイフォルダ名 : 送信済みアイテム ⑧

ゴミ箱フォルダ名 : 削除済みアイテム ⑨

下書きフォルダ名 : 下書き ⑩

メール一覧の取得方法 : ☐ SORTコマンドを使用しない。

※ 通常はチェックを外してご使用ください。

※ チェックした場合、IMAPサーバーがSORTコマンドに対応していても、強制的にSORTコマンドを使用せずにメール一覧を取得します。

変更

具体的な設定値については次ページをご確認ください。

05 ウェブメールIMAP機能の設定

項目	入力値
①受信メールサーバー(IMAP) : サーバー名	「outlook.office365.com」を入力します。
②受信メールサーバー(IMAP) : ポート番号	「993」を記入します。
③受信メールサーバー(IMAP) : 通信の保護	「SSL/TLS」を選択します。
④送信メールサーバー(SMTP) : サーバー名	「smtp.office365.com」を入力します。
⑤送信メールサーバー(SMTP) : ポート番号	「587」を記入します。
⑥受信メールサーバー(POP3) : 通信の保護	「STARTTLS」を選択します。
⑦メール送信時の認証	「XOAUTH2認証」を選択し、「OAuth認可サーバー」では こちら で登録しました認可サーバーを選択します。
⑧送信トレイフォルダ名	「送信済みアイテム」を入力します。 (Outlookでの構成フォルダ名が日本語で設定されている場合)
⑨ゴミ箱フォルダ名	「削除済みアイテム」を入力します。 (Outlookでの構成フォルダ名が日本語で設定されている場合)
⑩下書きフォルダ名	「下書き」を入力します。 (Outlookでの構成フォルダ名が日本語で設定されている場合)



2. ウェブメールIMAPのアカウント設定を行う

ウェブメールIMAPのメールサーバー設定後、各アカウントの設定操作を行います。

(1) 管理者アカウントでログイン後、トップ画面のメニューから「ウェブメールIMAP」をクリックします。



(2) 「ウェブメールIMAPは別ウィンドウで開かれます～」の画面から

右上の歯車アイコンをクリックし、機能管理 > アカウント設定 を選択します。



05 ウェブメールIMAP機能の設定

(3)アカウント設定画面で設定させたいアカウント名をクリックします。



(4)アカウントの設定画面で各種設定を行います。入力する値は次のページをご確認ください。

アカウントの追加

表示名 : ユーザー-A

メールアドレス(*) : [redacted]@neosupport.onmicrosoft.com ①

受信時のログ : ☒ 出力しない ☐ 出力する
※「出力する」を選択した場合、メールを受信する際のメールサーバーとの通信ログを出力します。

送信時のログ : ☒ 出力しない ☐ 出力する
※「出力する」を選択した場合、メールを送信する際のメールサーバーとの通信ログを出力します。

受信メールサーバー

ユーザーID(*) : [redacted]@neosupport.onnr ②

パスワード : [redacted]

認証方式 : ☐ 標準 ☒ XOAUTH2

OAuth認可サーバー : OAuth認証 (選択済み) ③
[認証] (未認証)

※ メールサーバーとして、G...を使用する場合、XOAUTH2を選択し、OAuth認可サーバーを選択して認証を行ってください。

送信メールサーバー

送信時の認証情報 : 認証方式 : XOAUTH2認証(OAuth認証)

ユーザーID : [redacted]@neosupport.onnr ④

パスワード : [redacted]

[OAuth認可サーバー認証] (未認証)

※「認証方式」に「SMTP認証」が選択されている場合、「ユーザーID」と「パスワード」を設定してください。
省略した場合は、受信メールサーバーの「ユーザーID」と「パスワード」で認証します。
※「認証方式」に「XOAUTH2認証」が選択されている場合、「ユーザーID」を設定し、[OAuth認可サーバー認証]で認証してください。

※ (*)は必須項目です。

05 ウェブメールIMAP機能の設定

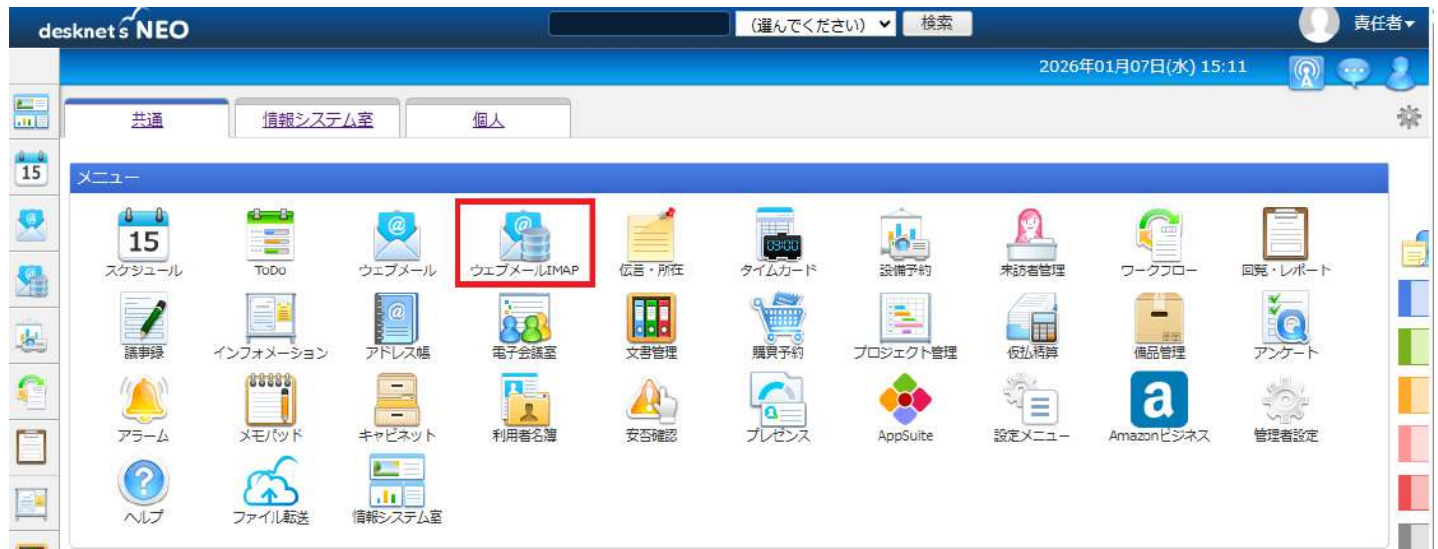
項目	入力値
①メールアドレス	対象アカウントの任意のメールアドレスを入力します。
②ユーザーID (受信メールサーバー)	①で入力したメールアドレスと同じメールアドレスを入力します。 ※OAUTH認証の場合、下のパスワード入力是不要となります。
③認証方式	「XOAUTH2認証」を選択し、「OAuth認可サーバー」では こちら で登録しました認可サーバーを選択します。 ※「認証」のボタンでは、必ず①で指定したメールアドレスと同じMicrosoft365アカウントでサインインした状態で認証を行う必要がありますが、管理者にて対象のMicrosoft365アカウントでサインインできない場合、こちらのボタンを押さないで未認証のままでも設定は保存いただけます。 一般アカウントで対象のMicrosoft365アカウントでサインインして認証を行う場合次ページの「個人アカウントからOAuth認証を実施する」の手順をご確認ください。
④ユーザーID (送信メールサーバー)	①で入力したメールアドレスと同じメールアドレスを入力します



3.アカウント個別にOAuth認証を行う

ウェブメールIMAPのメールサーバー設定後、各アカウントの設定操作を行います。

(1)認証を行うアカウントでログイン後、トップ画面のメニューから「ウェブメールIMAP」をクリックし、受信トレイ画面を開きます。

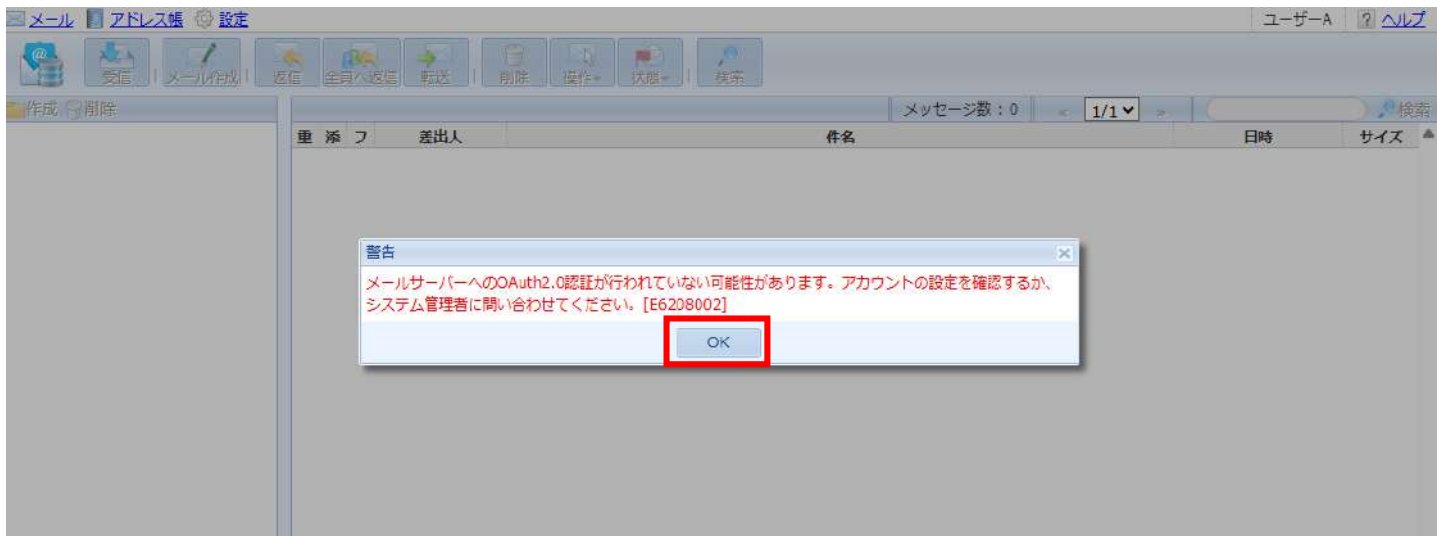


別ウィンドウで自動的に受信トレイが開けない場合、
画像にある「ウェブメールIMAP」のリンクをクリックします。



05 ウェブメールIMAP機能の設定

(2) OAuth認証が未実施の状態で受信トレイ画面を開くと画像のようにエラーが表示されますので、「OK」ボタンを押します。



(3) 受信トレイ画面左上にあります「設定」のリンクをクリックします。



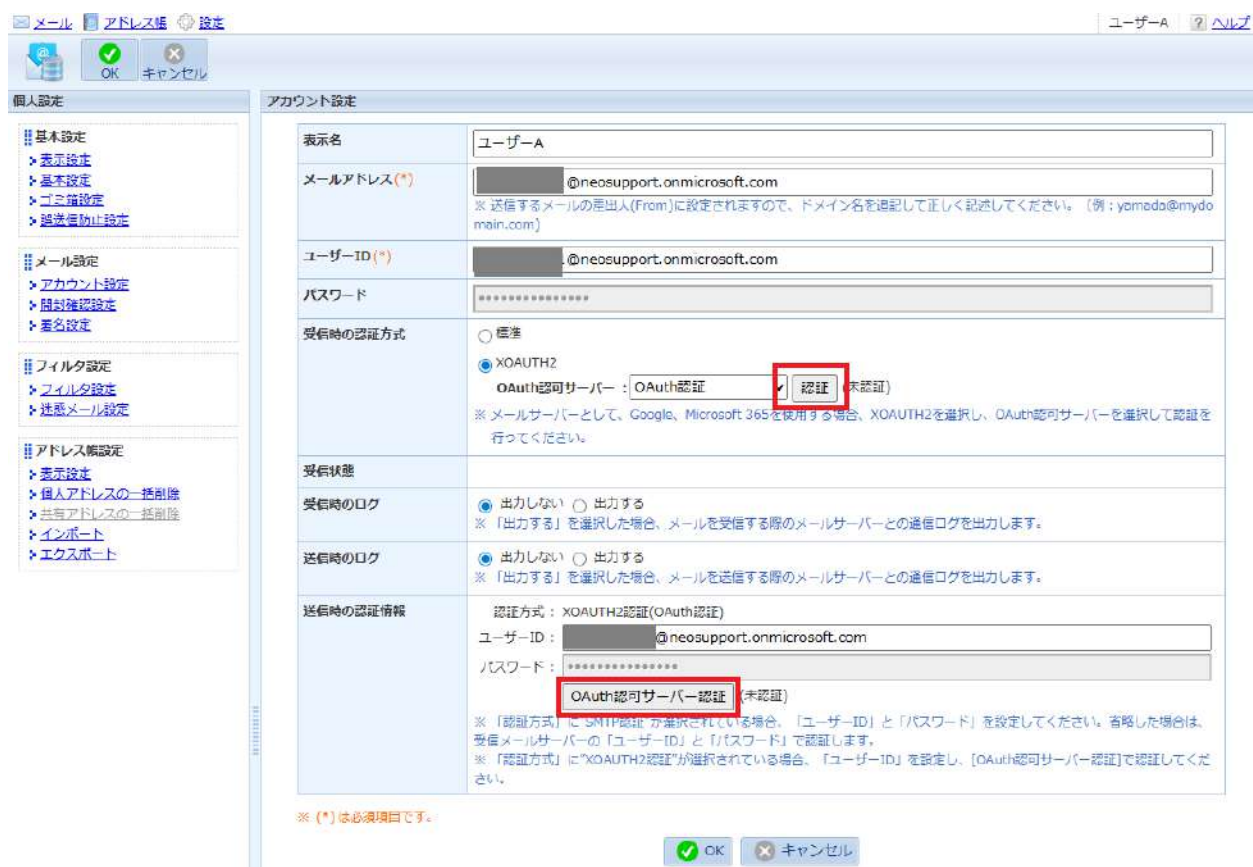
05 ウェブメールIMAP機能の設定

(4)各種設定の中の「アカウント設定」のリンクをクリックします。



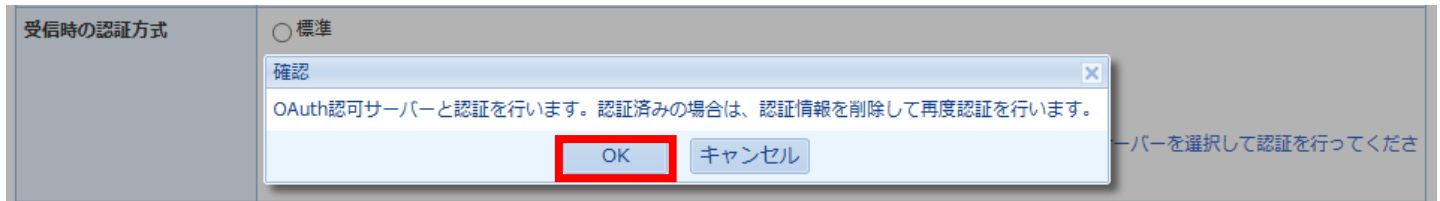
(5)アカウント設定画面に遷移されますので、その中の「認証」もしくは「OAuth認可サーバー認証」ボタンを押します。

※認証を実施する前にブラウザ上からMicrosoft365アカウントからサインアウトすることをお勧めします。

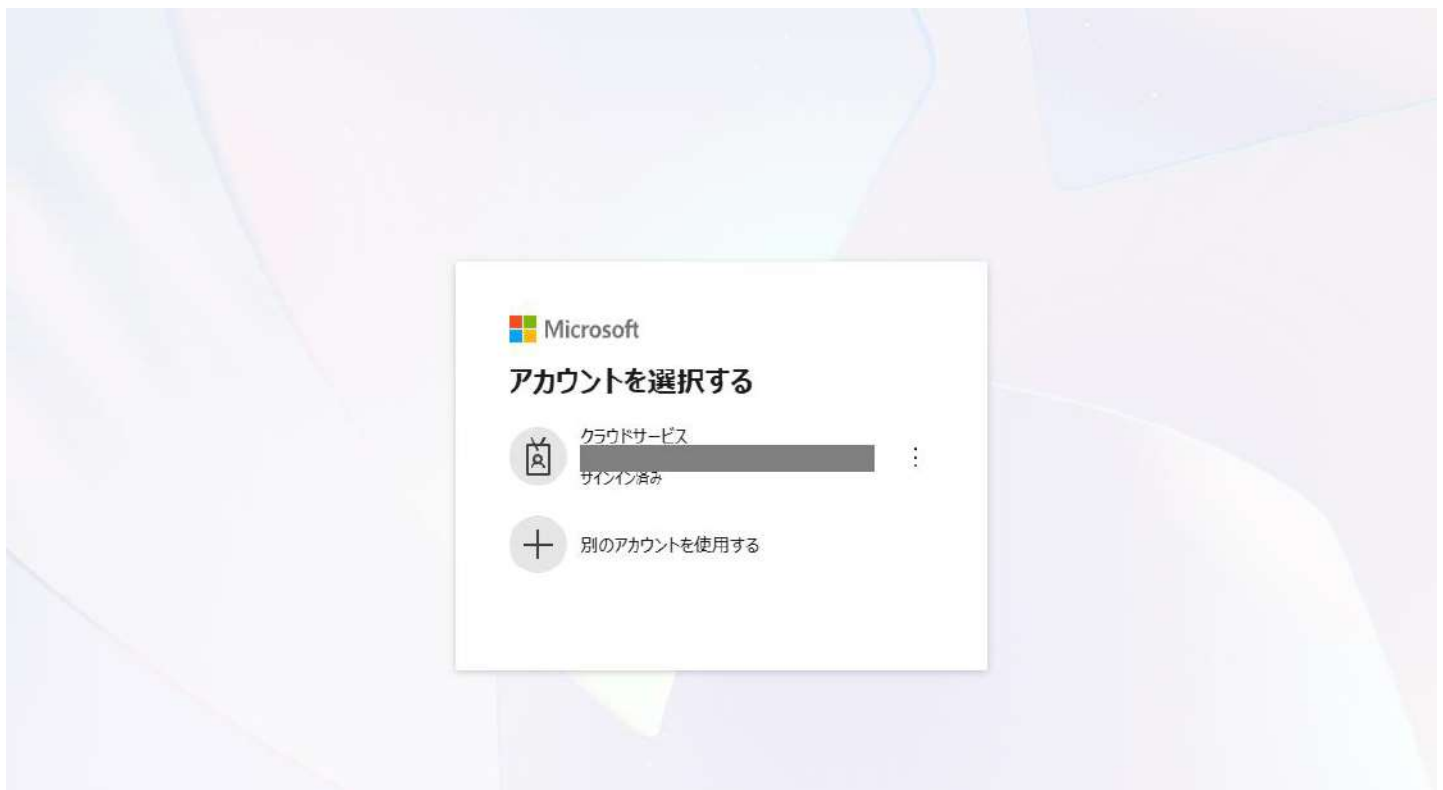


05 ウェブメールIMAP機能の設定

(6) OAuth認可サーバーのボタンを押しますと下記ダイアログが表示されますので「OK」を押します。



(7) 「OK」を押した後にMicrosoft365のサインイン画面が表示されますので、
送信元メールアドレスのアカウントと同じアカウントを選択
(同じアカウントが表示されていない場合は「別のアカウントを使用する」を選択)
していただき、サインインを実施します。



05 ウェブメールIMAP機能の設定

サインインが完了しますと「(認証日時)認証済み」と表記され、認証処理が完了となります。

アカウント設定	
表示名	ユーザーA
メールアドレス(*)	@neosupport.onmicrosoft.com ※ 送信するメールの差出人(From)に設定されますので、ドメイン名を追記して正しく記述してください。(例: yamada@mydomain.com)
ユーザーID(*)	@neosupport.onmicrosoft.com
パスワード	
受信時の認証方式	☐ 標準 ☒ XOAUTH2 OAuth認可サーバー: OAuth認証 認証 (認証済み) ※ メールサーバーとして、Google、Microsoft 365を使用する場合、XOAUTH2を選択し、OAuth認可サーバーを選択して認証を行ってください。
受信状態	
受信時のログ	☒ 出力しない ☐ 出力する ※ 「出力する」を選択した場合、メールを受信する際のメールサーバーとの通信ログを出力します。
送信時のログ	☒ 出力しない ☐ 出力する ※ 「出力する」を選択した場合、メールを送信する際のメールサーバーとの通信ログを出力します。
送信時の認証情報	認証方式: XOAUTH2認証(OAuth認証) ユーザーID: @neosupport.onmicrosoft.com パスワード: OAuth認可サーバー認証: (認証済み) ※ 「認証方式」に「SMTP認証」が選択されている場合、「ユーザーID」と「パスワード」を設定してください。省略した場合は、受信メールサーバーの「ユーザーID」と「パスワード」で認証します。 ※ 「認証方式」に「XOAUTH2認証」が選択されている場合、「ユーザーID」を設定し、[OAuth認可サーバー認証]で認証してください。

※ (*)は必須項目です。

上記対応を完了しますとウェブメールIMAPにてメールの送受信の操作が行えるようになります。

06

ファイル転送機能の設定

管理者による事前設定 (Azure) と、管理者による事前設定 (desknet's NEO) の設定がすべて完了した後の設定する項目になります。

ファイル転送機能をご利用いただく際の手順になりますので、ご利用になる場合以下の手順をご確認ください。

※ファイル転送機能はデフォルトは使用しない設定となっておりますので、メニューにファイル転送アイコンが表示されない場合、下記リンクのご利用ガイドをご参考に表示するための設定を行ってください。

<https://www.desknet.com/neo/drive/guide/>

1. ファイル転送の送信メールサーバー設定

(1) 管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「ファイル転送」のアイコンをクリックします。



(2) 画面右上の歯車アイコンをクリックし、システム管理 > 送信メールサーバー設定 を選択します。



06 ファイル転送機能の設定

(3)送信メールサーバーで各種設定を行います。入力する値は[51ページ](#)をご確認ください。

ファイル転送 > システム管理

設定機能： ファイル転送

変更

送信メールサーバー設定

サーバー(SMTP) : ☐ 管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。

サーバー名 : smtp.office365.com

ポート番号 : 587

通信の保護 : STARTTLS

送信時の認証 : XOAUTH2認証(OAuth認証)

☒ 個別に設定する。

サーバー名 :

ポート番号 : ※ 通常は25で設定します。

通信の保護 :

[STARTTLS通信時の認証について](#)

送信時の認証 : ☐ 認証しない

☐ POP before SMTP

受信メールサーバー :

(POP3)

ポート番号 : ※ 通常は110で設定します。

通信の保護 :

認証方式 :

サーバータイムアウト :

(秒)

※ この値を選択した場合、メール送信する際に受信メールサーバーの認証を行います。

☐ SMTP認証

認証方式 :

※ この値を選択した場合、メール送信する際にSMTP認証を行います。

☒ XOAUTH2認証

OAuth認可サーバー :

※ この値を選択した場合、メール送信する際にXOAUTH2認証を行います。

①

06 ファイル転送機能の設定

送信元メールアドレス : ☐ 管理者設定の[メールサーバー設定]で設定された送信元メールアドレス

→ @neosupport.onmicrosoft.com

②

☒ 任意のメールアドレス

※「[表示名]<メールアドレス>」、「<メールアドレス>」、「メールアドレス」のいずれかの形式で入力してください。

例)「ネオジャパン」<desknets@your.domain>、「<desknets@your.domain>」、「desknets@your.domain」

送信時の認証情報 :

ユーザーID :

パスワード :

③

(未認証)

※「送信時の認証情報」で設定した内容は「個別に設定する」を選択した場合に利用されます。

※「管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する」を選択した場合、[管理者設定 > システム設定 > メールサーバー設定]で設定された認証情報で認証します。

※「個別に設定する」を選択し、「送信時の認証」で「XOAUTH2認証」を選択した場合は、「OAuth認可サーバー」で選択したサーバーに対して[OAuth認可サーバー認証]で認証してください。

※「OAuth認可サーバー」でサーバーを選択した場合に[OAuth認可サーバー認証]ボタンが有効になります。

送信メールサーバー確認

送信確認 : 送信先

※ [送信]ボタンを押すと、入力されている送信メールサーバー設定でメールの送信ができることを確認することができます。

※ [送信]ボタンを押しても、入力された内容は保存されません。内容入力後、[変更]ボタンを押して設定を保存してください。



06 ファイル転送機能の設定

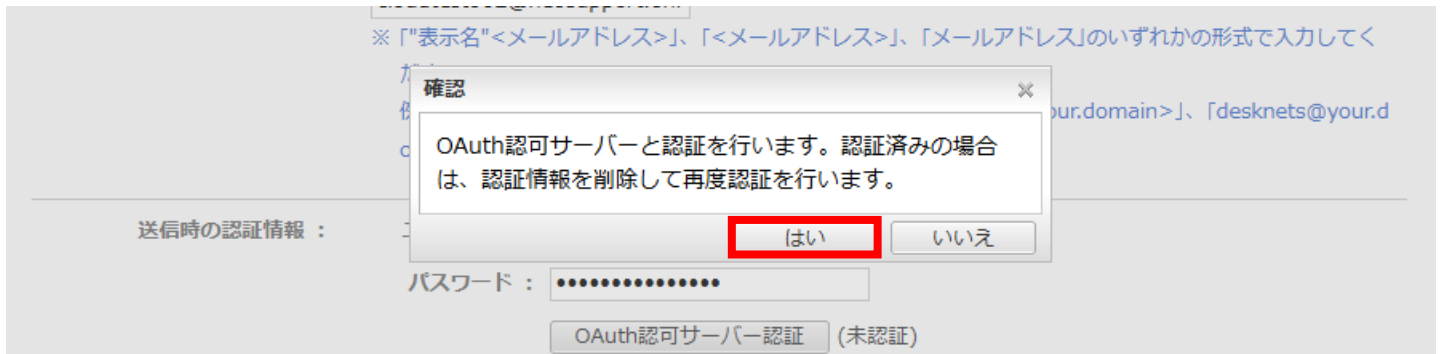
項目	入力値
①サーバー (SMTP)	お客様の設定状況にて設定値が異なります。 ・ 管理者設定のメールサーバー設定にてメールサーバーを設定済みの場合 → 「管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。」を選択します。 ・ 上記未設定でファイル転送のみでMicrosoft365のメールサーバー設定を行いたい場合 → 「個別に設定する」を設定し、以下の設定値を入力します。 サーバー名：smtp.office365.com ポート番号：587 通信の保護：STARTTLS 送信時の認証情報：XOAUTH2認証 「OAuth認可サーバー」ではこちらで登録しました認可サーバーを選択します。
②送信元メールアドレス	「管理者設定の[メールサーバー設定]で設定された送信元メールアドレス」もしくは「任意のメールアドレス」を選択し、メールアドレスを設定します。
③送信時の認証情報	ユーザーIDの欄には①で設定しているメールアドレスと同じメールアドレスを入力します。※パスワード入力は不要です。 「OAuth認可サーバー」ボタンを押して認証を行います。 認証の流れは次ページで案内いたします。



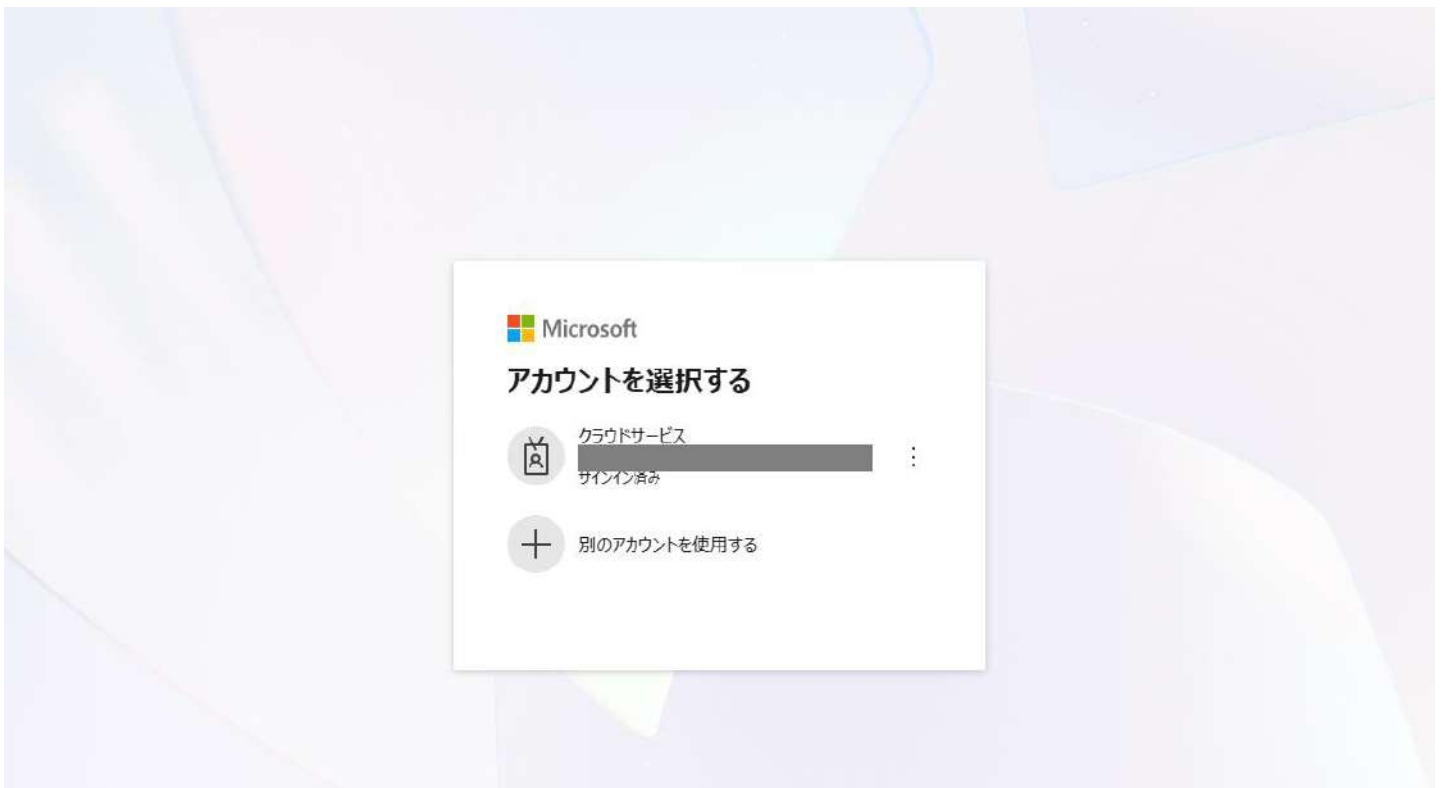
06 ファイル転送機能の設定

「OAuth認可サーバー認証」のボタンを押しますと
下記ダイアログが表示されますので「はい」を押します。

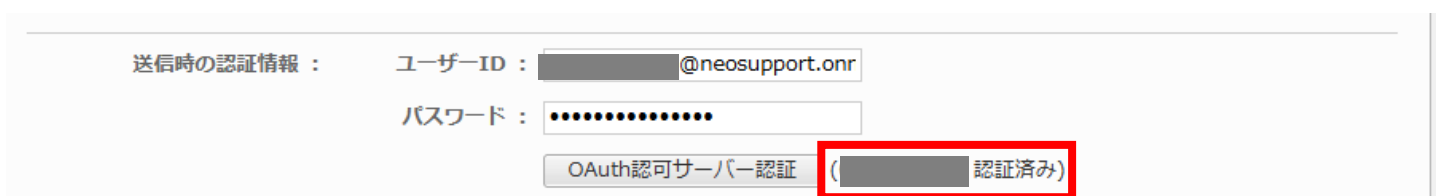
※認証を実施する前にブラウザ上からMicrosoft365アカウントからサインアウトすることをお勧めします。



「はい」を押した後にMicrosoft365のサインイン画面が表示されますので、
送信元メールアドレスのアカウントと同じアカウントを選択
(同じアカウントが表示されていない場合は「別のアカウントを使用する」を選択)
していただき、サインインを実施します。



サインインが完了しますと「(認証日時)認証済み」と表記され、認証処理が完了となります



2.個別に差出人設定を行う

ファイル転送機能でメールの差出人を個別に設定を行いたい場合、送信元メールアドレスの設定が必要となります。手順を以下に掲載いたします。

- ①ファイル転送画面で上部のポップアップで「差出人設定へ移動」と表示されている場合はそちらをクリックし、表示されていなければ右上の歯車アイコンをクリックし、**個人設定 > 差出人設定** を選択します。



- ②差出人設定画面にて設定を行います。設定値は次ページをご確認ください。

06 ファイル転送機能の設定

ファイル転送

変更

差出人設定

メールアドレス： ☐ ウェブメールの[アカウント設定]で設定されているメールアカウントの情報を使用する。

アカウント名：

表示名：

メールアドレス：

※ "通常使用するアカウント"に設定されているアカウント情報を使用します。

☒ 任意のメールアドレス ①

メールサーバー： (SMTP) サーバー名： smtp.office365.com

ポート番号： 587

通信の保護： STARTTLS

送信時の認証： XOAUTH2認証(OAUTH認証 (Microsoft365) beta)

送信元メール： 表示名： ②

アドレス メールアドレス： ③

ユーザーID： ④

パスワード： ⑤

※ 管理者が設定したメールサーバー(SMTP)を使用します。

☐ 管理者が設定した差出人メールアドレスを使用する。

送信元メール： @neosupport.onmicrosoft.com

アドレス

※ 管理者が設定したメールサーバー(SMTP)を使用します。

変更

Copyright (C)2012-2025 NEOJAPAN Inc. All Rights Reserved.

項目	入力値
①メールアドレス	任意のメールアドレスを選択します。
②表示名	任意の表示名を入力します。
③メールアドレス (送信元メールアドレス)	差出人とするメールアドレスを入力します。
④ユーザーID	③で入力した同じメールアドレスを入力します。
⑤パスワード	「OAuth認可サーバー認証」ボタンを押して 設定しているメールアドレスと同じMicrosoft365アカウントで 認証を行います。※パスワード入力不要です。 認証の流れは次ページで案内いたします。

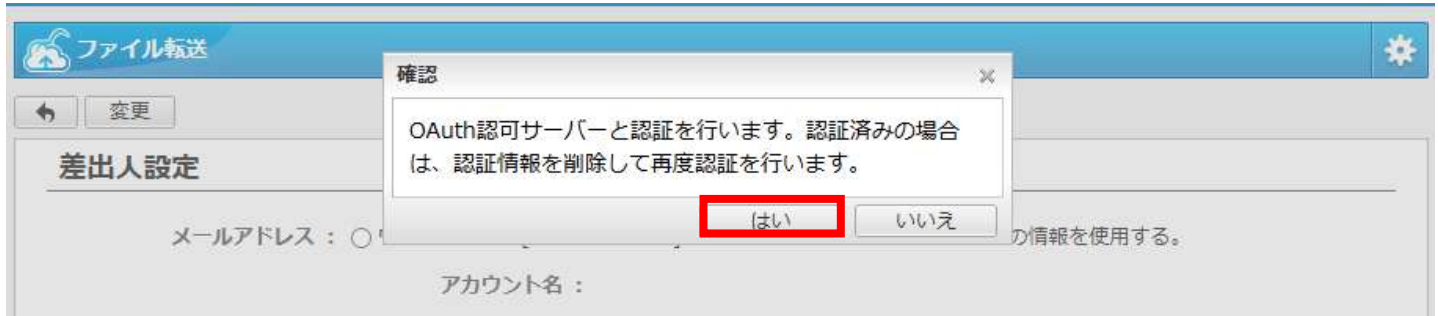
Copyright © 2026 NEOJAPAN, Inc. All Rights Reserved.

55

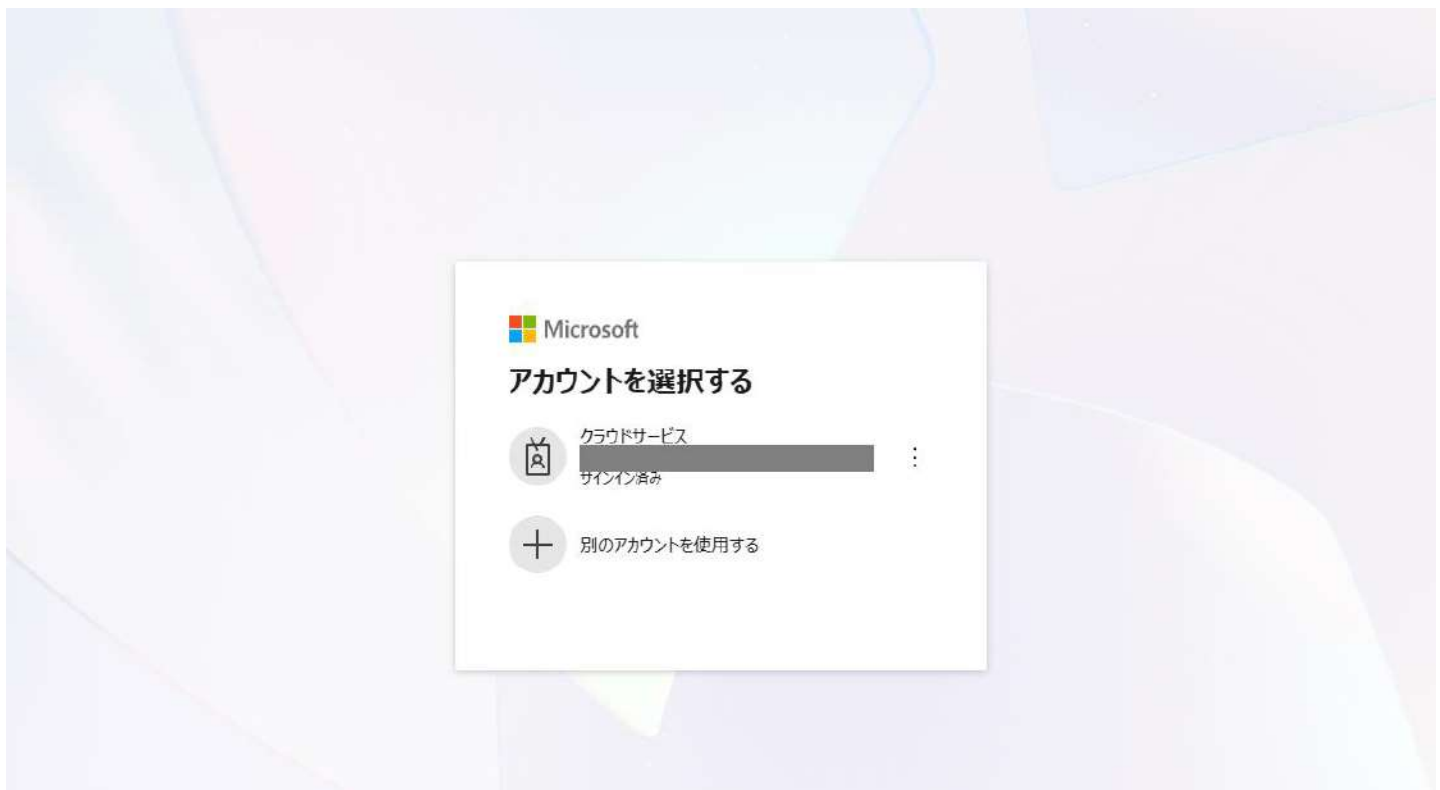
06 ファイル転送機能の設定

「OAuth認可サーバー認証」のボタンを押しますと
下記ダイアログが表示されますので「はい」を押します。

※認証を実施する前にブラウザ上からMicrosoft365アカウントからサインアウトすることをお勧めします。



「はい」を押した後にMicrosoft365のサインイン画面が表示されますので、
送信元メールアドレスのアカウントと同じアカウントを選択
(同じアカウントが表示されていない場合は「別のアカウントを使用する」を選択)
していただき、サインインを実施します。



サインインが完了しますと「(認証日時)認証済み」と表記され、認証処理が完了となります

送信元メール :	表示名 :	株式会社ネオジャパン
アドレス	メールアドレス :	@neosupport.onmicrosoft.com
	ユーザーID :	@neosupport.onr
	パスワード :	
	OAuth認可サーバー認証	(..... 認証済み)

07

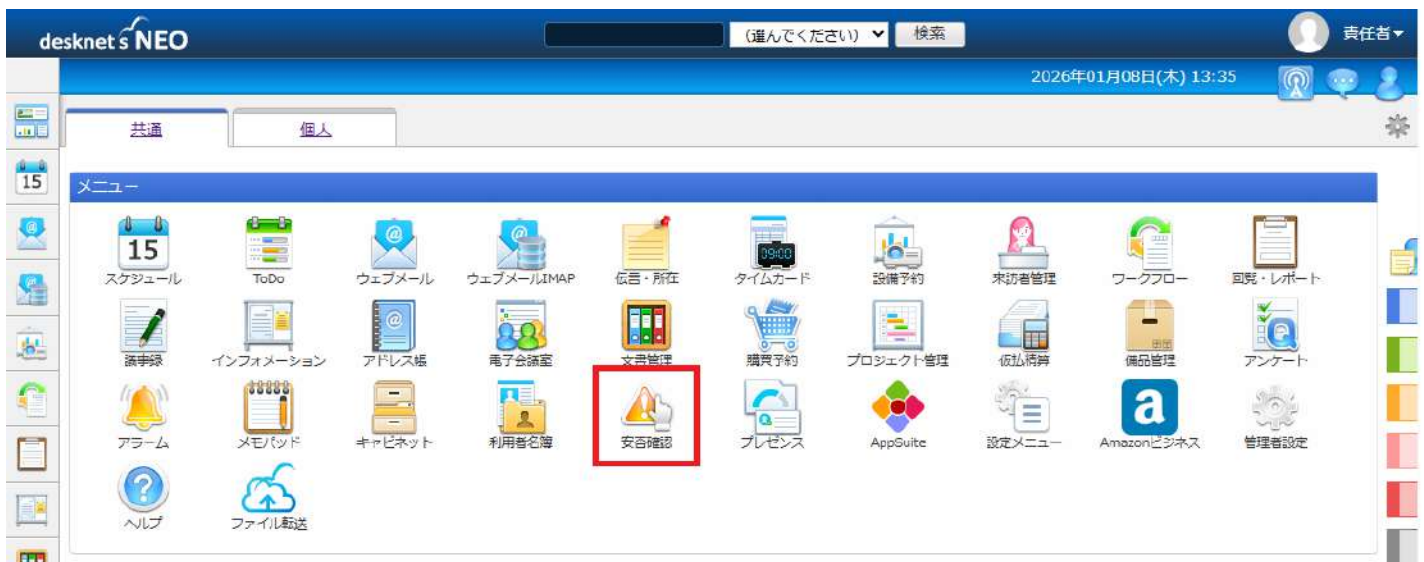
安否確認機能の設定

管理者による事前設定 (Azure) と、管理者による事前設定 (desknet's NEO) の設定がすべて完了した後の設定する項目になります。

安否確認機能をご利用いただく際の手順になりますので、ご利用になる場合以下の手順をご確認ください。

安否確認のメールサーバー設定

(1) 管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「**安否確認**」のアイコンをクリックします。



(2) 画面右上の歯車アイコンをクリックし、**システム管理 > 配信メールサーバー設定** を選択します。



07 安否確認機能の設定

(3)配信メールサーバーで各種設定を行います。入力する値は次の次ページをご確認ください。

 安否確認 > システム管理

設定機能： 安否確認 

◀ 変更

配信メールサーバー設定

サーバー(SMTP)： ☐ 管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。

サーバー名： smtp.office365.com

ポート番号： 587

通信の保護： STARTTLS

送信時の認証： XOAUTH2認証(OAuth認証)

☒ 個別に設定する。

サーバー名：

ポート番号： ※ 通常は25で設定します。

通信の保護： ▼

▶ [STARTTLS通信時の認証について](#)

送信時の認証： ☐ 認証しない

☐ POP before SMTP

受信メールサーバー：

(POP3)

ポート番号： ※ 通常は110で設定します。

通信の保護： ▼

認証方式： ▼

サーバータイムアウト：

(秒)

※ この値を選択した場合、メール送信する際に受信メールサーバーの認証を行います。

☐ SMTP認証

認証方式： ▼

※ この値を選択した場合、メール送信する際にSMTP認証を行います。

☒ XOAUTH2認証

OAuth認可サーバー： ▼

※ この値を選択した場合、メール送信する際にXOAUTH2認証を行います。

1

07 安否確認機能の設定

メール送信元アドレス : ☐ 管理者設定の[メールサーバー設定]で設定されたメール送信元アドレス
→

☒ 任意のメールアドレス

②

※「表示名」「メールアドレス」、「<メールアドレス>」、「メールアドレス」のいずれかの形式で入力してください。

例) 「ネオジャパン」<desknets@your.domain>、「<desknets@your.domain>」、「desknets@your.domain」

送信時の認証情報 : ユーザーID :

パスワード :

(未認証)

③

※ 「送信時の認証情報」で設定した内容は「個別に設定する」を選択した場合に利用されます。

※ 「管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する」を選択した場合、[管理者設定 > システム設定 > メールサーバー設定]で設定された認証情報で認証します。

※ 「個別に設定する」を選択し、「送信時の認証」で「XOAUTH2認証」を選択した場合は、「OAuth認可サーバー」で選択したサーバーに対して[OAuth認可サーバー認証]で認証してください。

※ 「OAuth認可サーバー」でサーバーを選択した場合に[OAuth認可サーバー認証]ボタンが有効になります。

配信メールサーバー確認

配信確認 : 送信先

※ [送信]ボタンを押すと、入力されている配信メールサーバー設定でメールの送信ができることを確認することができます。

※ [送信]ボタンを押しても、入力された内容は保存されません。内容入力後、[変更]ボタンを押して設定を保存してください。

07 安否確認機能の設定

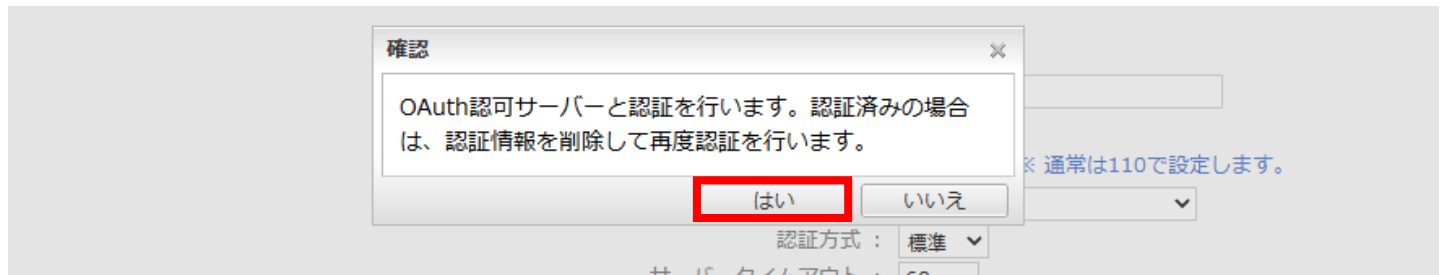
項目	入力値
①サーバー (SMTP)	お客様の設定状況にて設定値が異なります。 ・ 管理者設定のメールサーバー設定にてメールサーバーを設定済みの場合 → 「管理者設定の[メールサーバー設定]で設定された送信メールサーバー(SMTP)を使用する。」を選択します。 ・ 上記未設定で安否確認のみでMicrosoft365のメールサーバー設定を行いたい場合 → 「個別に設定する」を設定し、以下の設定値を入力します。 サーバー名：smtp.office365.com ポート番号：587 通信の保護：STARTTLS 送信時の認証情報：XOAUTH2認証 「OAuth認可サーバー」ではこちらで登録しました認可サーバーを選択します。
②送信元メールアドレス	「管理者設定の[メールサーバー設定]で設定された送信元メールアドレス」もしくは「任意のメールアドレス」を選択し、メールアドレスを設定します。
③送信時の認証情報	ユーザーIDの欄には①で設定しているメールアドレスと同じメールアドレスを入力します。※パスワード入力は不要です。 「OAuth認可サーバー」ボタンを押して認証を行います。 認証の流れは次ページで案内いたします。



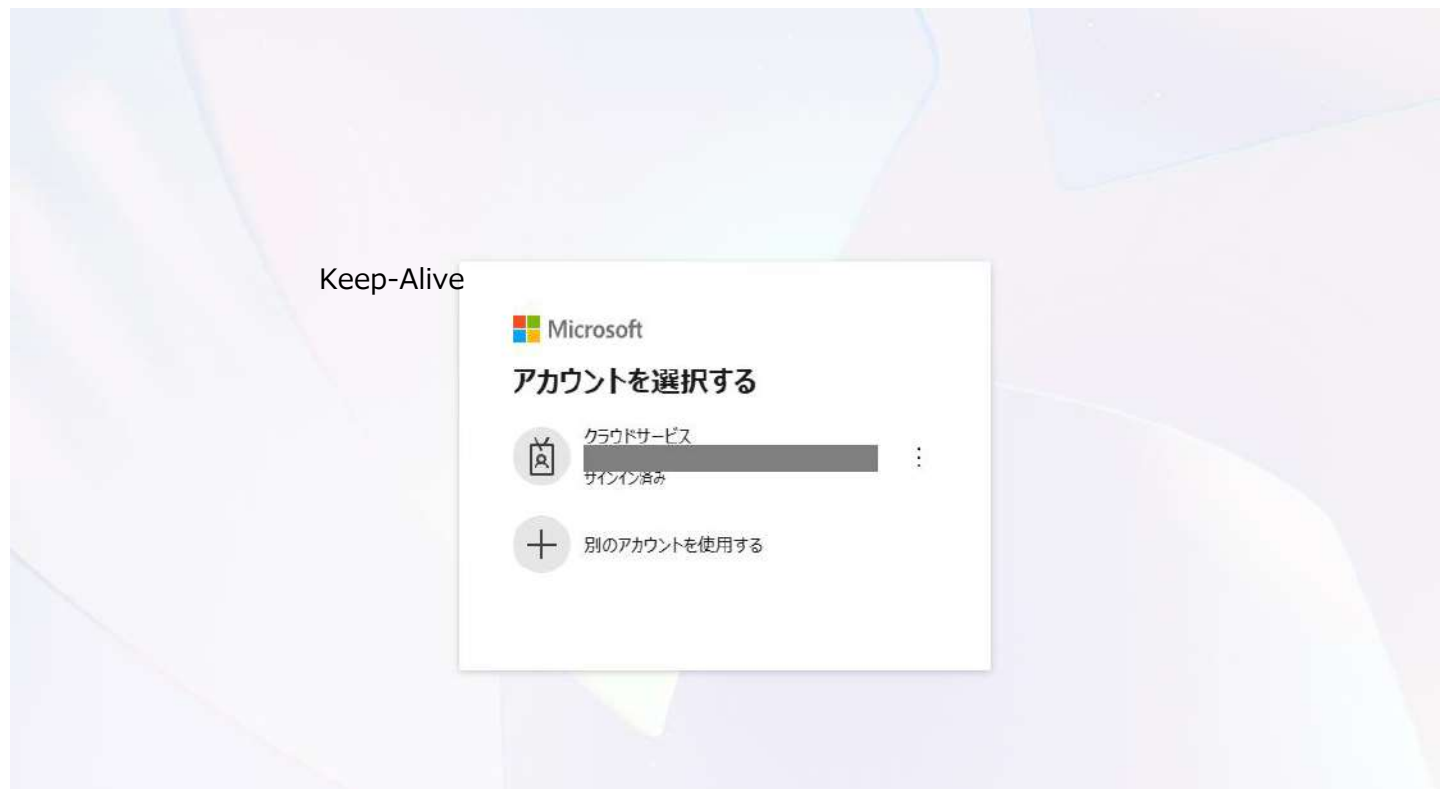
07 安否確認機能の設定

「OAuth認可サーバー認証」のボタンを押しますと
下記ダイアログが表示されますので「はい」を押します。

※認証を実施する前にブラウザ上からMicrosoft365アカウントからサインアウトすることをお勧めします。



「はい」を押した後にMicrosoft365のサインイン画面が表示されますので、
送信元メールアドレスのアカウントと同じアカウントを選択
(同じアカウントが表示されていない場合は「別のアカウントを使用する」を選択)
していただき、サインインを実施します。



サインインが完了しますと「(認証日時)認証済み」と表記され、認証処理が完了となります。

送信時の認証情報：	ユーザーID：	...@neosupport.onr
	パスワード：	
	OAuth認可サーバー認証	(認証日時) 認証済み



08

クライアントシークレットの更新手順

各機能でメールを利用するための設定手順は前ページにて以上になります。

この章ではメール運用時にクライアントシークレットの有効期限が切れた際の対処法についてご案内します。

クライアントシークレットの再発行

[管理者による事前設定 \(Azure\)](#) にて発行したクライアントシークレットの有効期限が切れますと、

「アクセストークン取得対象のサイトへの接続に失敗しました。システム管理者に問い合わせてください。

またdeskne'sNEOのインストールされているサーバーから

アクセストークン取得対象のサイトへ通信が可能か確認してください。[E6208001]

というメッセージが表示され、メール機能がご利用いただけなくなります。

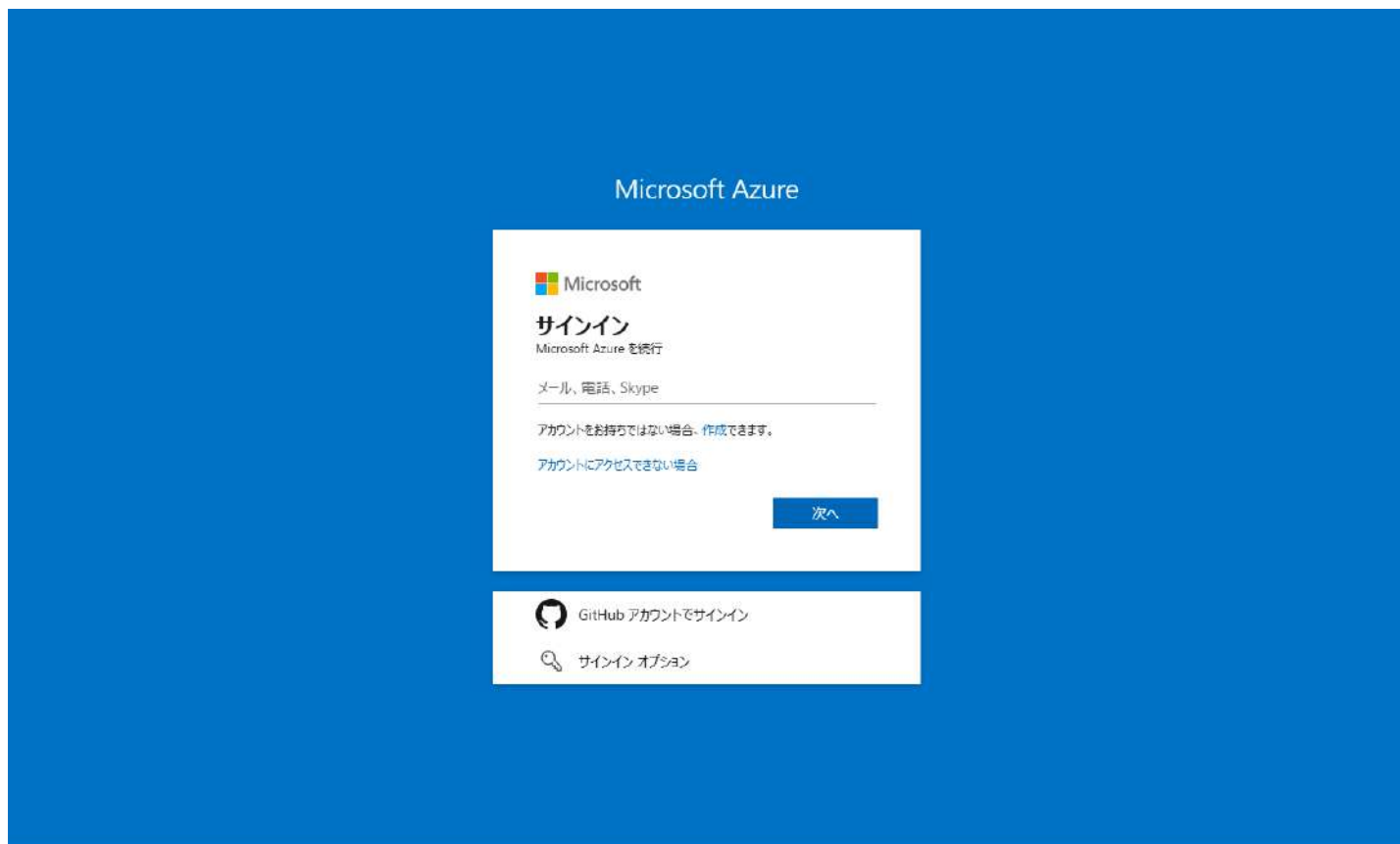
クライアントシークレットを再発行して、desknet's NEOの設定を更新する手順を以下に掲載いたします。

(1)Azureポータルにログインします。

<https://portal.azure.com/#home>

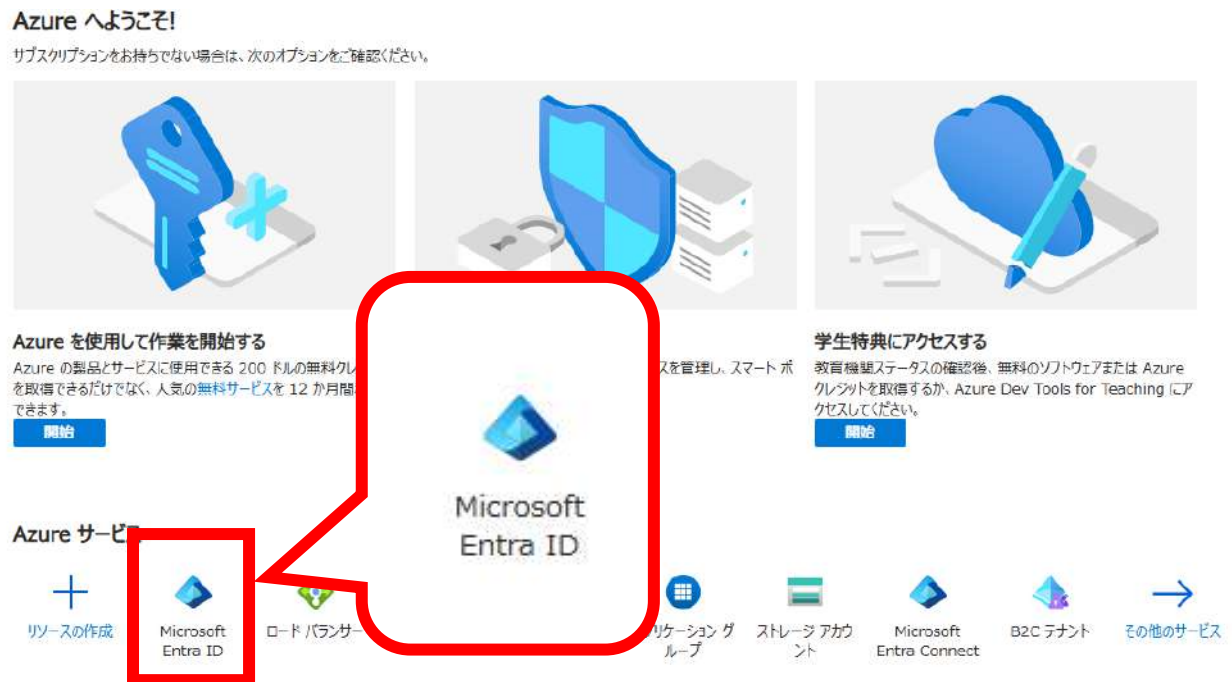
上記リンクにアクセスしますと、以下の画像のようにサインイン画面が開かれますので、

Microsoft 365グローバル管理者アカウントにて、Azureにサインインしてください。



08 クライアントシークレットの更新手順

(2) サインインすると下記画面が表示されますので、「**Microsoft Entra ID**」をクリックしてください。



(3) 画面左側サブメニューにある「管理」の下にある「**アプリの登録**」をクリックします。



08 クライアントシークレットの更新手順

(4) アプリの一覧からOAUTH認証用に登録している対象の**アプリの名前をクリック**します。

ホーム > 株式会社ネオジャパン | アプリの登録

概要 プレビュー機能 問題の診断と解決 管理

ユーザー グループ External Identities ロールと管理者 管理単位 代理管理者パートナー エンタープライズ アプリケーション デバイス **アプリの登録** Identity Governance

2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および Azure Active Directory Graph に新しい機能はもう追加されません。テクニカル サポートとセキュリティ更新プログラムは今後も提供されますが、機能更新プログラムは提供されません。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft Graph にアップグレードする必要があります。詳細情報

すべてのアプリケーション 所有しているアプリケーション 削除されたアプリケーション

表示名またはアプリケーション (クライアント) ID を入力し始めると結果がフィ...

3 個のアプリケーションが見つかりました

表示名 ↑↓	アプリケーション (クライアント) ID	作成日 ↑↓	証明書とシークレット
			有効期限切れ

クライアントシークレットの有効期限が切れますと、「有効期限切れ」の表記になります。

(5) 画面左部のメニューから「管理」の下にある「証明書とシークレット」をクリックします。

ホーム > 株式会社ネオジャパン | アプリの登録 >

desknet's NEO OAuth

検索 削除 エンドポイント プレビュー機能

概要 クイック スタート 統合アシスタント 問題の診断と解決 管理

ブランド化とプロパティ 認証 **証明書とシークレット** トークン構成

クライアントの資格情報
証明書またはシークレットの追加
リダイレクト URI
1 個の Web、0 個の SPA、0 個のパブリック クライアント
アプリケーション ID の URI
アプリケーション ID URI の追加
ローカル ディレクトリでのマネージド アプリケーション

証明書とシークレット

サポートされているアカウントの種類
所属する組織のみ

08 クライアントシークレットの更新手順

(6)有効期限が切れているクライアントシークレットを削除します。

右側にあるゴミ箱アイコンをクリックして削除します。

desknet's NEO OAuth | 証明書とシークレット

検索 フィードバックがある場合

概要
クイック スタート
統合アシスタント
問題の診断と解決
管理

ブランド化とプロパティ
Authentication (Preview)
証明書とシークレット
トークン構成
API のアクセス許可
API の公開
アプリ ロール
所有者
ロールと管理者
マニフェスト
サポート + トラブルシューティング

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (1)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID

有効期限が切れていますと赤色の！アイコンが表示されます。

(7) 「+新しいクライアントシークレット」をクリックします。

ホーム > 株式会社ネオジャパン | アプリの登録 > desknet's NEO OAuth

desknet's NEO OAuth | 証明書とシークレット

検索 フィードバックがある場合

概要
クイック スタート
統合アシスタント
問題の診断と解決
管理

ブランド化とプロパティ
認証
証明書とシークレット
トークン構成
API のアクセス許可
API の公開
アプリ ロール
所有者
ロールと管理者
マニフェスト
サポート + トラブルシューティング

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアント シークレット (0)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID
このアプリケーションのクライアント シークレットは作成されていません。			

08 クライアントシークレットの更新手順

(8)必要事項を入力し「追加」ボタンをクリックします。

クライアントシークレットの追加

説明 ① このクライアントシークレットの説明を入力してください

有効期限 ② 推奨: 180 日 (6 か月) ▼

追加 キャンセル

①説明：任意の説明を入力します。（未入力でも問題ありません）

②有効期限：クライアントシークレットの有効期限を設定します。

(9)作成したクライアントシークレットの「値」をコピーします。

証明書 (0) クライアントシークレット (1) フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアントシークレット

説明	有効期限	値 ①	シークレット ID
desknet's NEO			

必ず「値」をコピー シークレットIDと間違えないようご注意ください

値 ①	シークレット ID

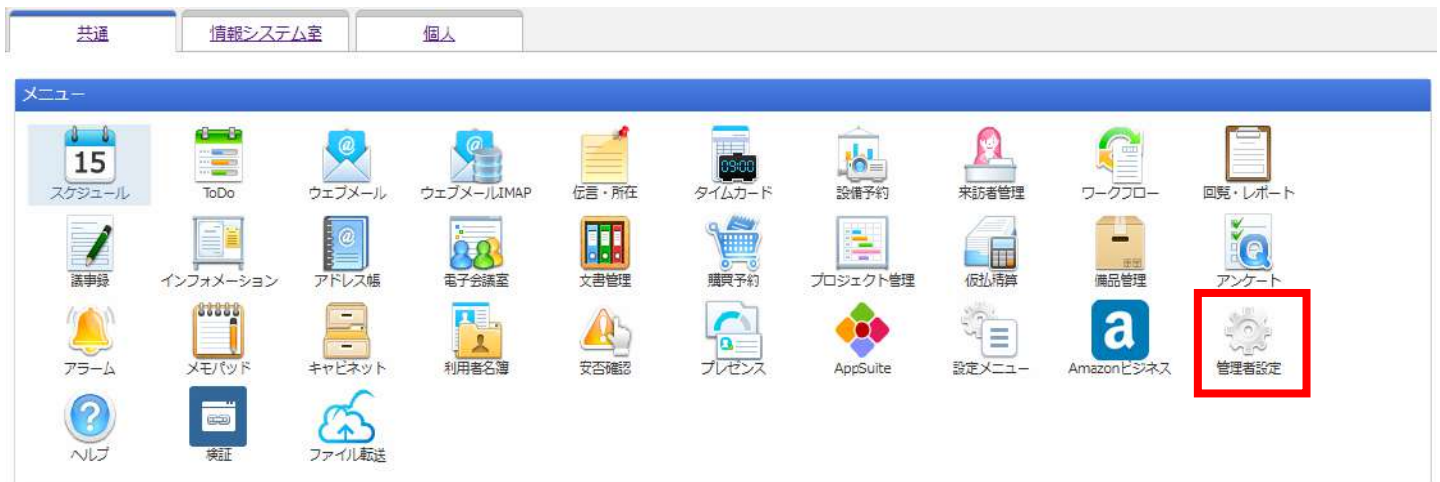
※注意※

この値をコピーせずに画面遷移し、再度クライアントシークレット画面にアクセスすると、値にマスクがかかり、値のコピーすることができません。
値を発行後すぐにコピーするようお願いします。
コピーせず画面遷移した場合は、再度クライアントシークレットの再発行の操作を行ってください。

Azure側の設定は以上になります。次ページからdesknet's NEOの画面にて操作を行います。

08 クライアントシークレットの更新手順

(10)管理者アカウントにてdesknet's NEOにログインし、ポータル画面のメニューから「管理者設定」の歯車アイコンをクリックします。



(11)管理者設定画面の右上の歯車アイコンをクリックし、
システム設定 > OAuth認可サーバー設定 を選択します。



08 クライアントシークレットの更新手順

(12) OAuth認可サーバー設定で登録している認可サーバー名をクリックします。



(13) クライアントシークレットの更新を行います。

(9)でコピーしました値を「クライアントシークレット」に入力し上書き更新を行います。



クライアントシークレット更新の流れは以上になります。

更新後メールの送受信が正常に行えるかご確認ください。

改版履歴

- ・ 2026 年 8 月 19 日 第1版

株式会社ネオジャパン

〒220-8110 神奈川県横浜市西区みなとみらい 2-2-1 横浜ランドマークタワー10 階

 クラウド版カスタマーセンター

0120-365-800

営業時間：平日9:00～17:30（土日祝日、弊社指定休日を除く）

 メールでのお問い合わせ

cloudsupport@desknet's.com

