



おまかせサイバーみまもり



おまかせアンチウイルス

おまかせサイバーみまもり おまかせアンチウイルス おまかせデータレスPC 二要素認証設定マニュアル

2025. 7
NTT東日本株式会社

二要素認証について

- 管理コンソールのログインにあたり、従来のID・パスワードに加えて“ワンタイムパスワード”を用いて認証を行うことで、セキュリティをさらに強化（第三者からの管理コンソールへの不正にログインを防止）することができます。
- ご利用の場合には、お手持ちのPCやスマートフォンに、第三者の提供するトークンアプリをインストール・設定する必要があります。
- 本ドキュメントでは、代表的なトークンアプリにおける設定方法をご説明いたします。
- トークンアプリはNTT東日本およびトレンドマイクロ社の提供するものではなく、これをご利用になったことにより何らかの損害が発生した場合でもNTT東日本およびトレンドマイクロ社では責任を負いかねますので、ご了承ください。

二要素認証未設定時、管理コンソールにログインすると下記のメッセージが表示されます。

⚠ セキュリティをさらに強化

サイバー犯罪が高度化するにつれて、不正アクセスからインターネットアカウントを保護するにはパスワード保護だけでは不十分な場合があります。アカウントを適切に保護するために、2要素認証をただちに有効にすることを強く推奨します。



2要素認証とは
2要素認証により、モバイルデバイスを使ってアカウントへのサインイン時に本人確認を行うことが可能になります。2要素認証によりセキュリティが強化され、パスワードが盗まれた場合でも、不正アクセスを防ぐことができます。
[詳細](#)

2要素認証が重要な理由
サイバー犯罪者によって本アカウントに不正アクセスされた場合、本コンソールからアクセス可能なトレンドマイクロ製品の保護をすべてオフにされる恐れがあります。それにより個人データ、企業機密、銀行情報への不正アクセスや、盗用、ランサムウェア、破損などの被害を受けやすくなる可能性があります。トレンドマイクロはアカウントを保護するために、2要素認証をただちに有効にすることを強く推奨します。

2要素認証設定を行う

今後このメッセージを表示しない 危険性を理解したうえで、スキップします

- スマートフォン(iOS/Android)における設定方法 . . . P4
- Windowsにおける設定方法 . . . P10
- MacOSにおける設定方法 . . . P19
- Chromeアドオンによる設定方法 . . . P27
- 二要素認証を設定したトークンアプリを紛失、削除してしまった場合 . . . P33

スマートフォン(iOS/Android)における設定方法 1/6

- 管理者が利用するモバイルデバイス (iOS/Android) に「Google Authenticator」をインストールします。
 - App StoreまたはGoogle Playを立ち上げ、「Google認証」と検索
 - 「Google Authenticator」を選択し、インストールを実施



- 管理コンソールの「2要素認証の設定」画面にて、「確認メールを送信」をクリックします。

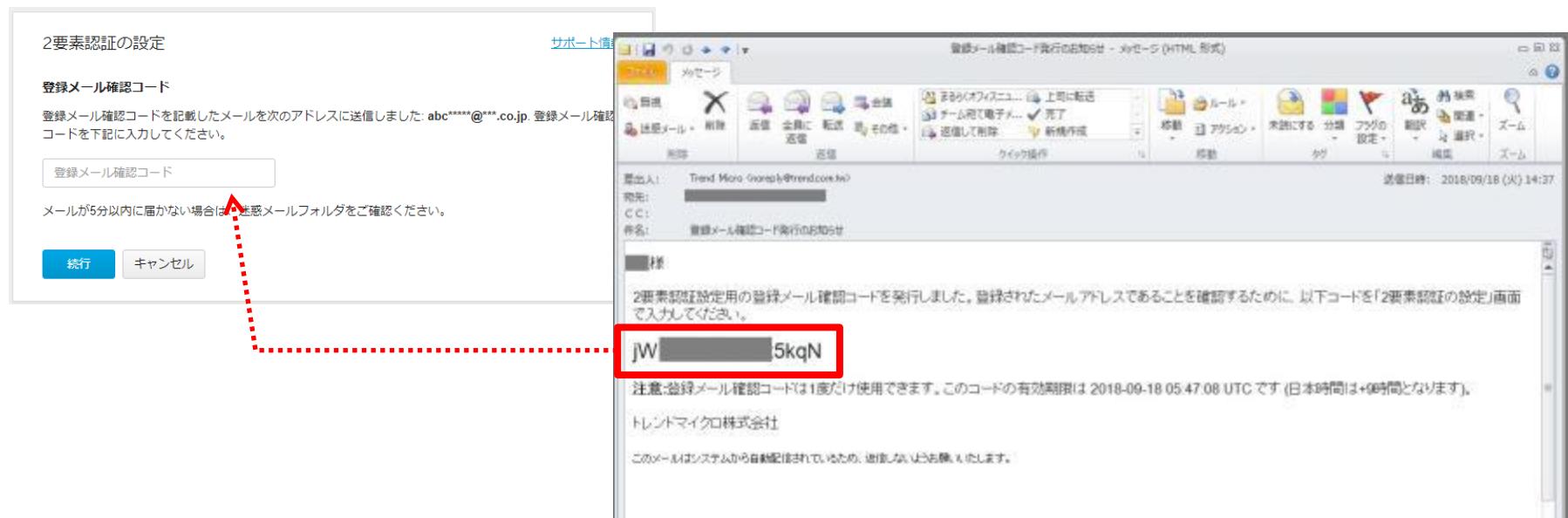


スマートフォン(iOS/Android)における設定方法 2/6

3. 「登録メール確認コード」画面が表示されます。

ご契約時に登録したメールアドレス宛に

下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。



スマートフォン(iOS/Android)における設定方法 3/6

4. 下記画面が表示されます。「QRコードを表示する」をクリックします。



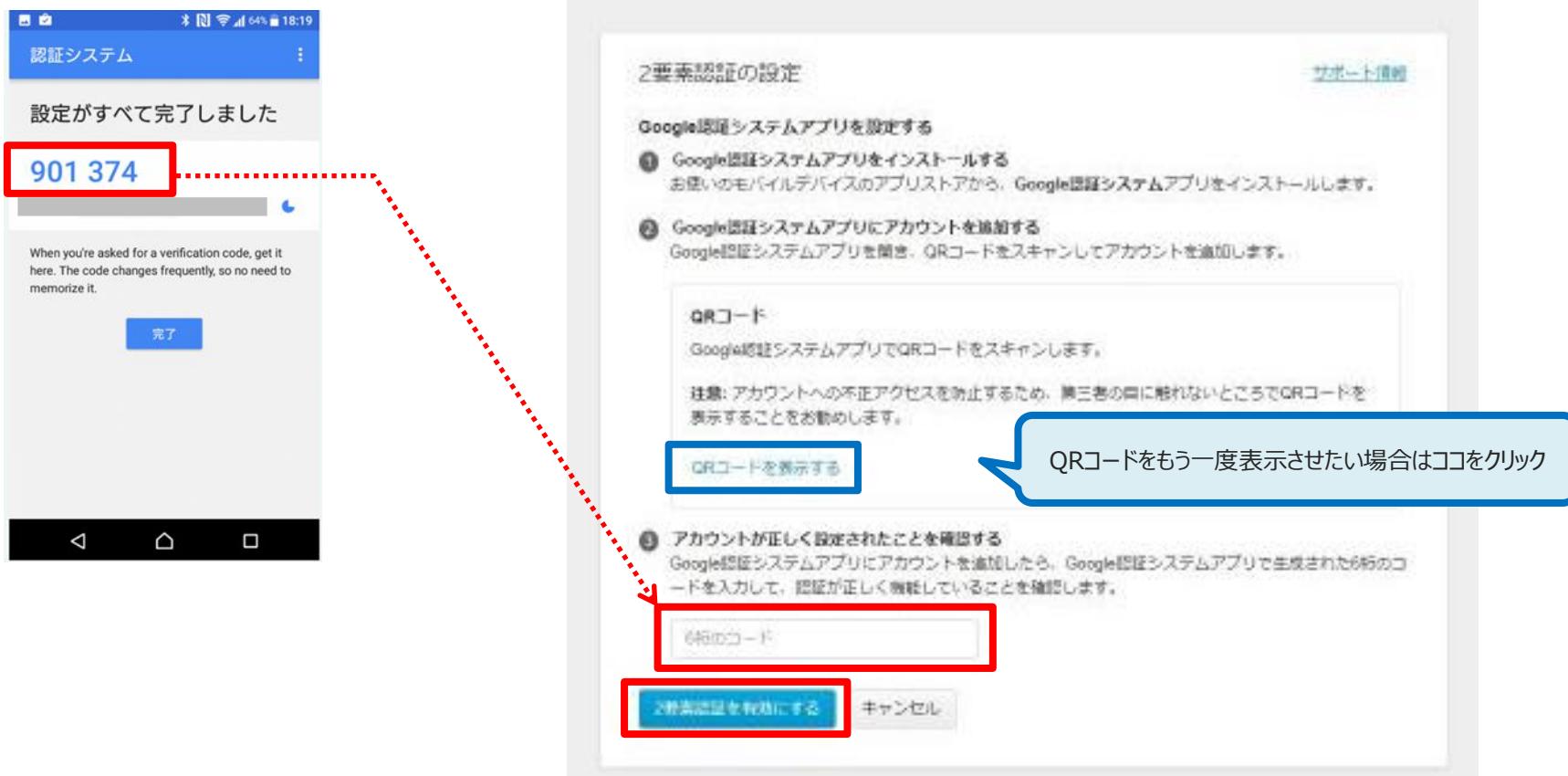
スマートフォン(iOS/Android)における設定方法 4/6

5. QRコードが表示されます。
6. インストールした「Google Authenticator」を起動し、「開始」>「バーコードをスキャン」をクリックします。
7. カメラが起動するため、手順 7 で表示したQRコードを読み取ります。



スマートフォン(iOS/Android)における設定方法 5/6

8. 無事にQRコードが読み取れると、「Google Authenticator」アプリにランダムな6桁の数字が表示されます。それを③に入力し「2要素認証を有効にする」をクリックします。



9. 登録が完了すると下記画面が表示されます。

次回以降のログインは、「Google Authenticator」を起動し、生成した 6 行のコード入力が必要になります。

The screenshot shows the Trend Micro Licensing Platform interface. At the top, there is a red header bar. Below it, the Trend Micro logo and the text "2要素認証" (Two-Factor Authentication) are on the left, and "Licensing Platform" is on the right. The main content area has a white background with a light gray border. It contains the following information:

| 状況: | 有効 | 無効にする | | デバイスの変更 |
|--------------|-----------------|-------|--|---------|
| 認証方法: | Google認証システムアプリ | | | |
| 登録済みメールアドレス: | abc****@**.com | | | |

注意: 選択した認証方法を使用して確認コードを取得できない場合は、トレンドマイクロからお客様の登録済みメールアドレスへ、1回限り使用できる緊急アクセスコードをお送りすることができます。表示されている登録済みメールアドレスが正しくない場合は、アカウントの設定でメールアドレスを変更してください。

Windowsにおける設定方法 1/9

1. 管理者が利用するデバイス（Windows）に①②の二つをインストールします。

①WinAuth

二要素認証のワンタイムパスワードを発行するためのソフト

<https://github.com/winauth/winauth/releases>

※WinAuth-3.5.1.zipをダウンロード

※今後、管理コンソール画面へログインするときに必要となります。

②Q太郎

QRコードの画面キャプチャからコードの情報を読取るためのソフト

<https://www.vector.co.jp/soft/dl/win95/writing/se399854.html>

※設定の過程のみで必要となります。

二要素認証の設定完了後はアンインストールしても問題ございません。

2. 管理コンソールの

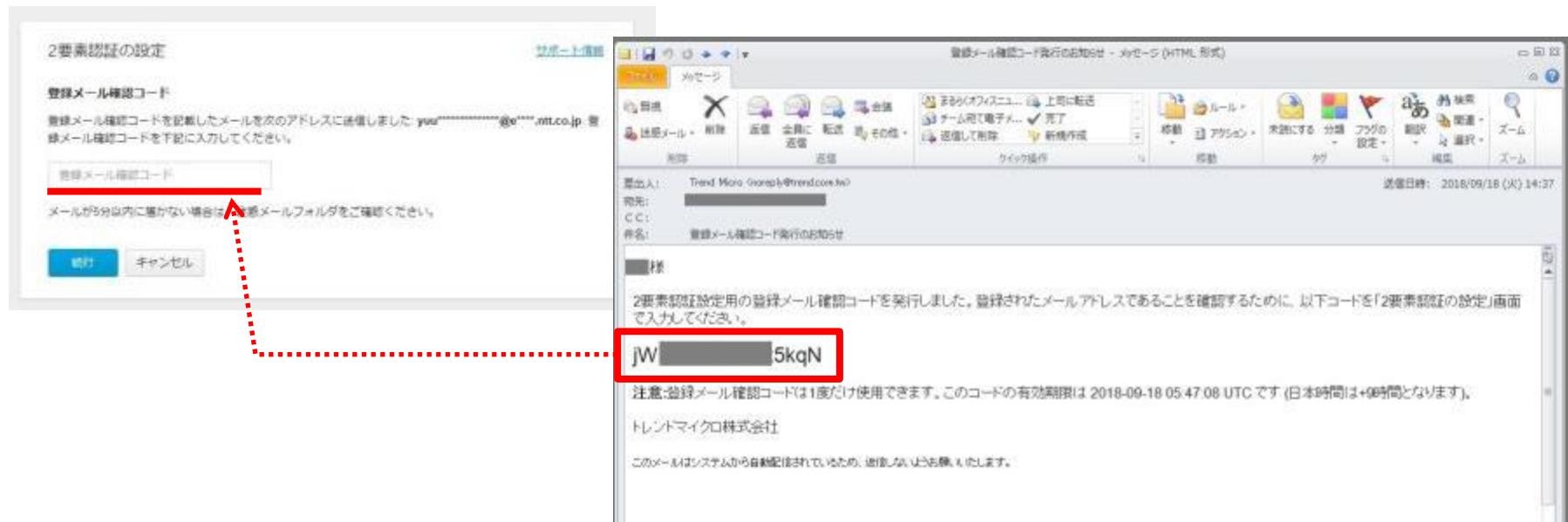
「2要素認証の設定」画面にて、「確認メールを送信」をクリックします。



3. 「登録メール確認コード」画面が表示されます。

ご契約時に登録したメールアドレス宛に

下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。

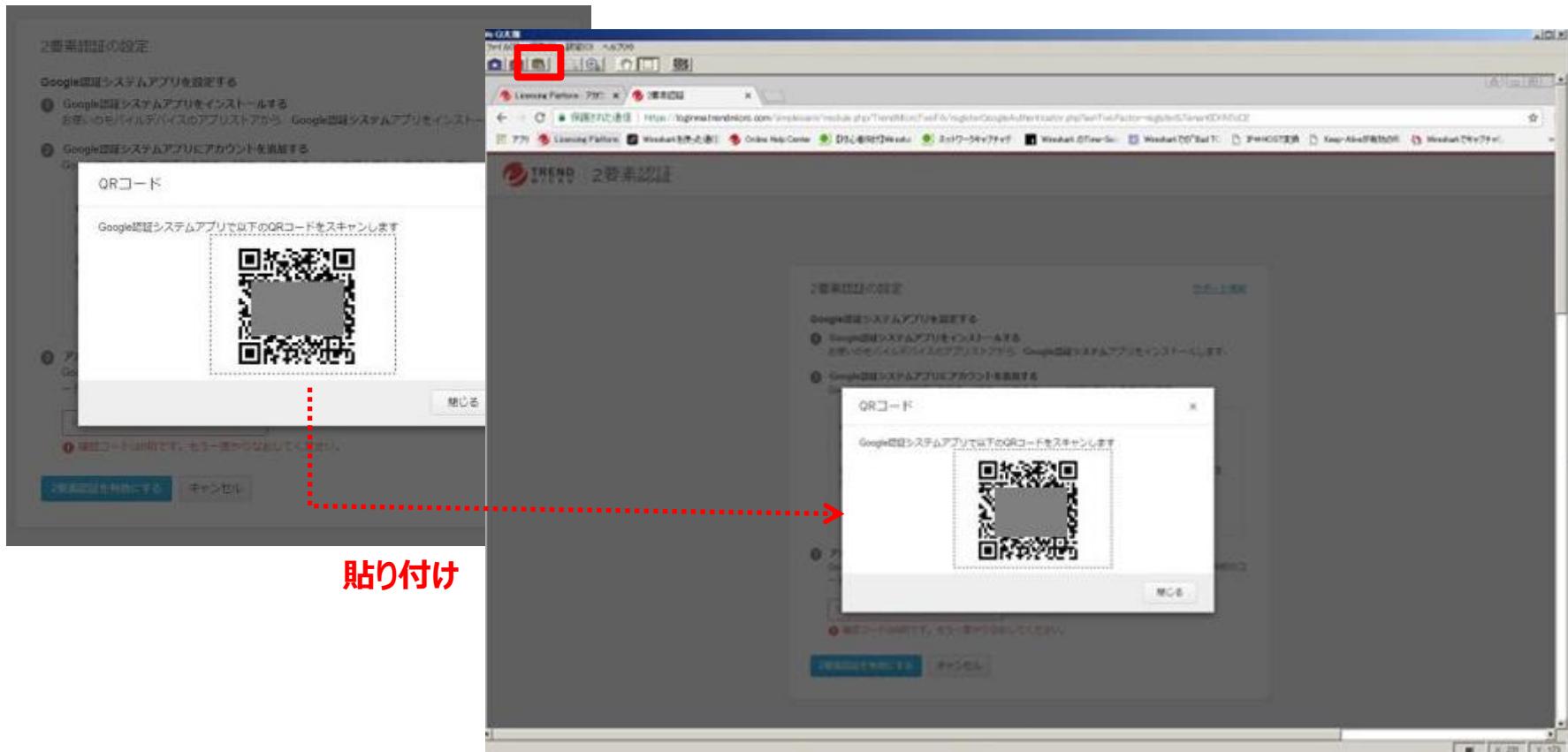


4. 下記画面が表示されます。「QRコードを表示する」をクリックします。



Windowsにおける設定方法 4/9

5. QRコードが表示されるので、PrintScreenで画面をキャプチャします。
6. ダウンロードした「Q太郎」を起動し（QTAROU.exeをダブルクリック）、
下記赤枠ボタンをクリックするとPrintScreenした画面がQ太郎に貼り付けされます。



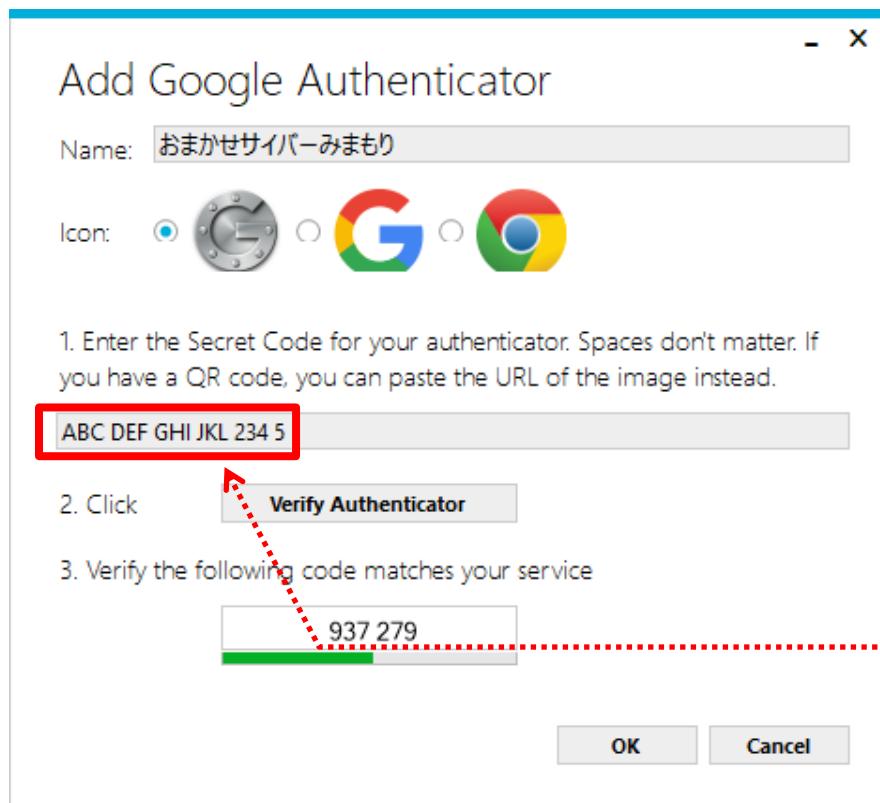
Windowsにおける設定方法 5/9

7. 下記赤枠のボタンをクリック後QRコードを左クリックしたままマウスで囲むとQRコードがデコードされます。

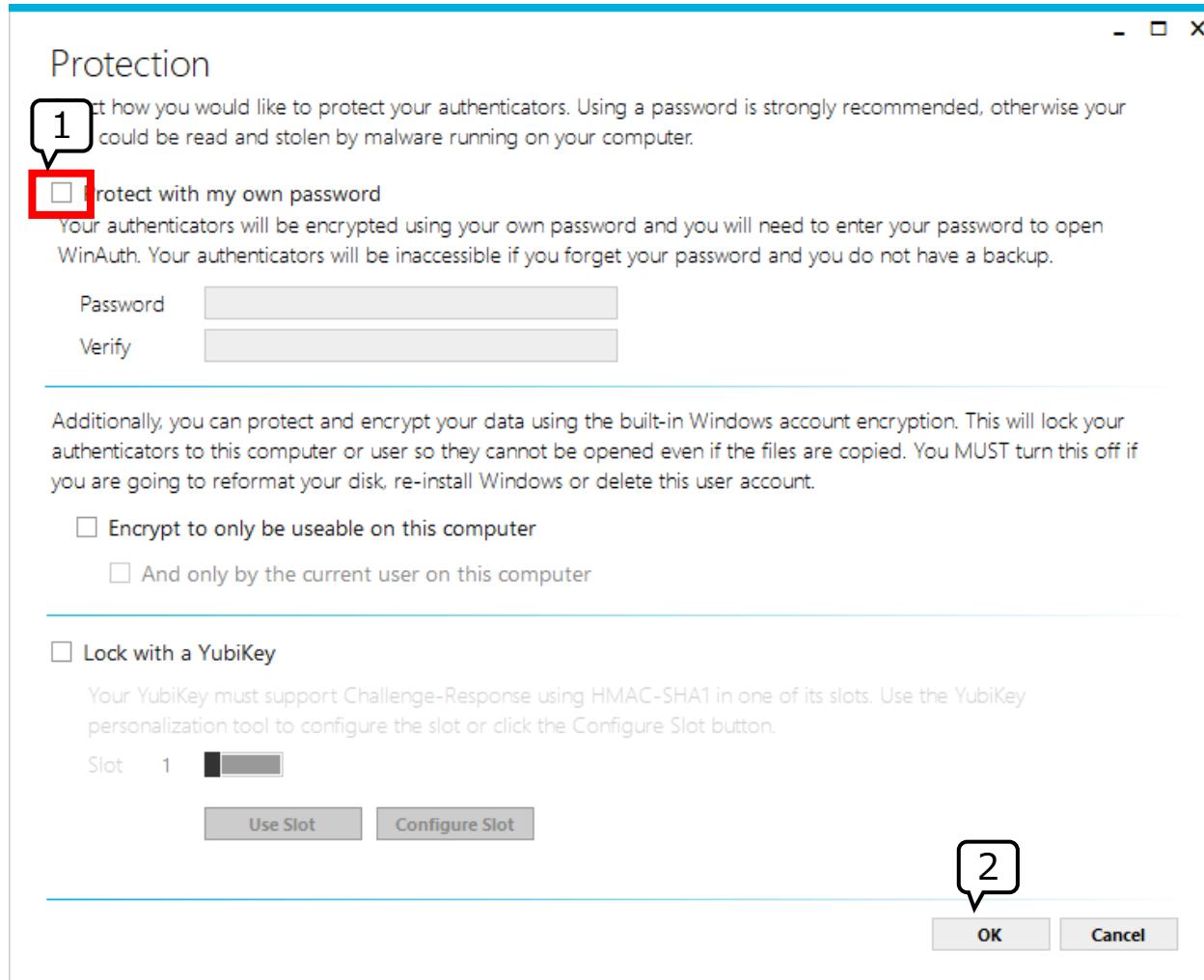


8. WinAuthを立ち上げて下記を行います。（WinAuth.exeをダブルクリック）

- WinAuthの画面が表示されたら、addボタンをクリックすると認証方式（Google、Microsoft等）が複数表示されるので、Googleをクリックします。下記Add Google Authenticator 画面が表示されます。
- Name : 任意の名前を入力します
- Icon : 任意のアイコンを選択します
- QRコード デコード結果の「=」から「&」の間の文字列をコピーし、項目1に貼り付けます
- Verify Authenticator ボタンをクリックします。
- OKボタンをクリックします。

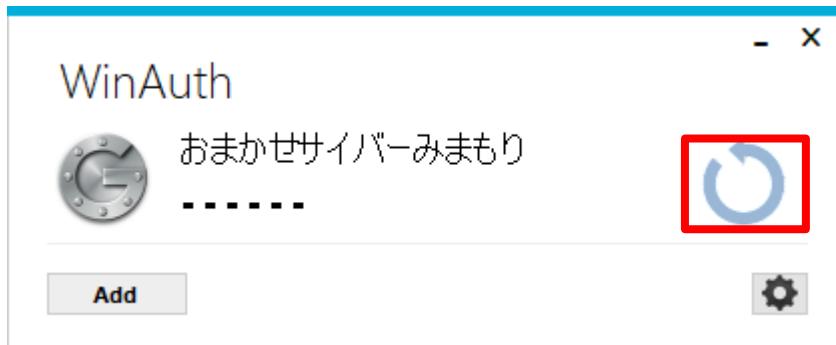


9. Protect with my own passwordのチェックをはずし、「OK」をクリックします。



Windowsにおける設定方法 8/9

10. WinAuthのリフレッシュボタンをクリックし、6桁のコードを生成します。
11. 6桁のコードが時間切れになる前に、管理コンソールの2要素認証登録画面のパスワード入力箇所へ入力し「2要素認証を有効にする」ボタンをクリックします。



14. 登録が完了すると下記画面が表示されます。

次回以降のログインは、「WinAuth」を起動し、生成した 6 行のコード入力が必要になります。

The screenshot shows a web interface for Trend Micro's Licensing Platform. At the top left is the Trend Micro logo and the text "2要素認証". At the top right is the text "Licensing Platform". The main content area has a title "2要素認証" and a "サポート情報" link. Below this, a paragraph explains that 2-factor authentication strengthens account security by preventing password theft even if the primary password is compromised. It also mentions that it protects against unauthorized access to SaaS products. There are three configuration sections: "状況:" (Status) set to "有効" (Enabled), "無効にする" (Disable) and "デバイスの変更" (Change device) links; "認証方法:" (Authentication method) set to "Google認証システムアプリ" (Google Authentication System App); and "登録済みメールアドレス:" (Registered email address) set to "abc****@**.com". A note at the bottom states that users can receive emergency access codes via email if they cannot use the chosen method.

| 状況: | 有効 | 無効にする | | デバイスの変更 |
|--------------|-----------------|-------|--|---------|
| 認証方法: | Google認証システムアプリ | | | |
| 登録済みメールアドレス: | abc****@**.com | | | |

注意: 選択した認証方法を使用して確認コードを取得できない場合は、トレンドマイクロからお客様の登録済みメールアドレスへ、1回限り使用できる緊急アクセスコードをお送りすることができます。表示されている登録済みメールアドレスが正しくない場合は、アカウントの設定でメールアドレスを変更してください。

1. 管理者が利用するデバイス（Mac）でApp Storeを開き、①②の二つをインストールします。

①OTP Manager

二要素認証のワンタイムパスワードを発行するためのソフト

②QR Journal

QRコードの画面キャプチャからコードの情報を読取るためのソフト

※設定の過程のみで必要となります。

二要素認証の設定完了後はアンインストールしても問題ございません。

2. 管理コンソールの

「2要素認証の設定」画面にて、「確認メールを送信」をクリックします。

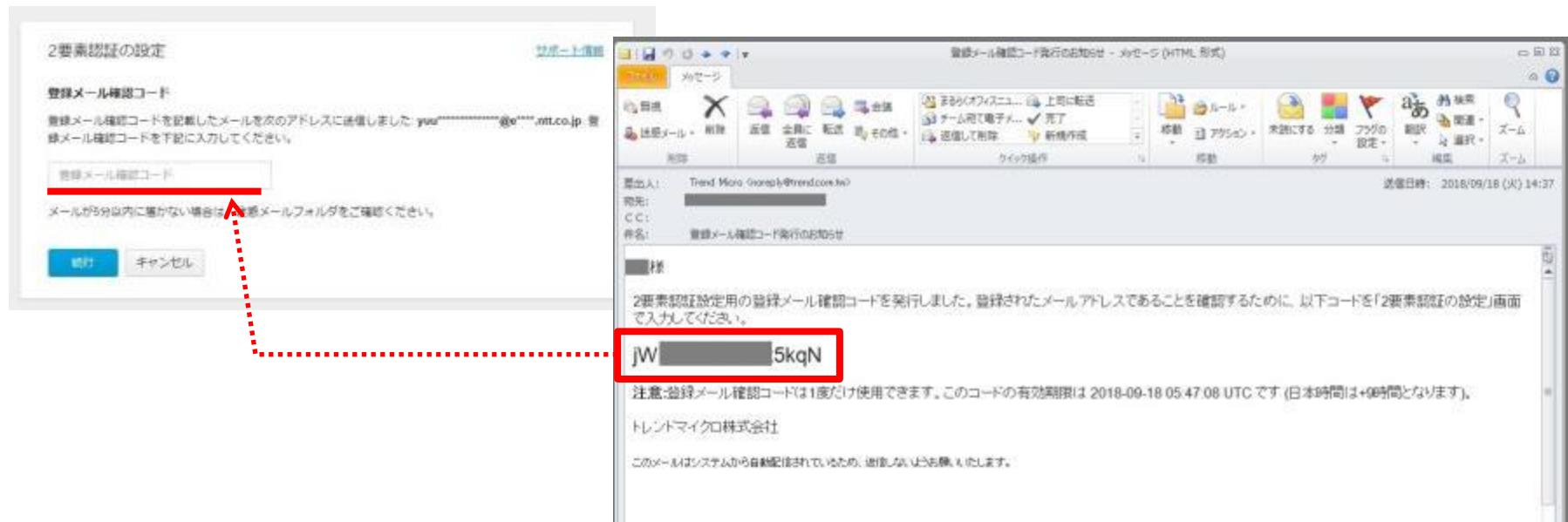


MacOSにおける設定方法 2/8

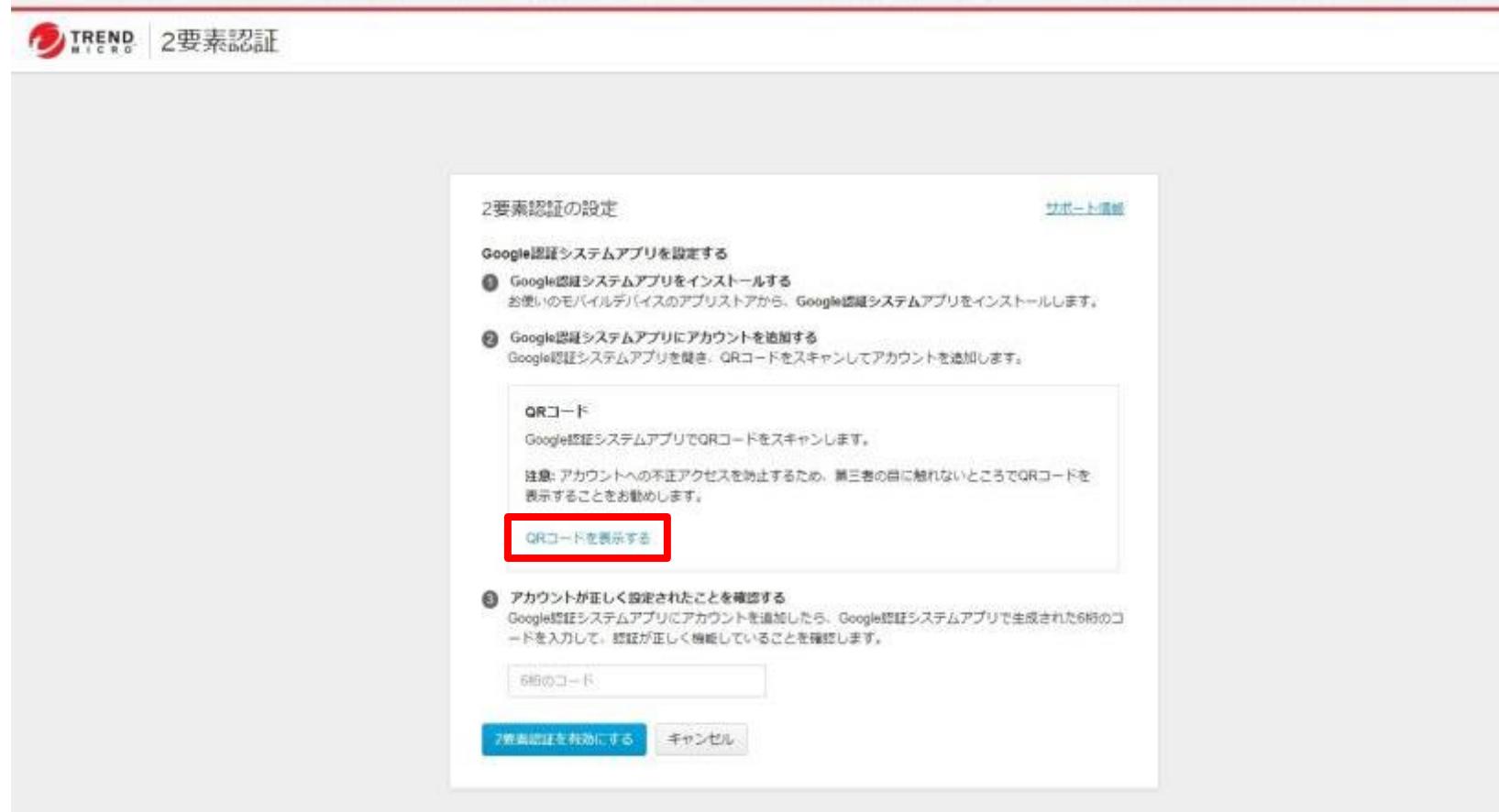
3. 「登録メール確認コード」画面が表示されます。

ご契約時に登録したメールアドレス宛に

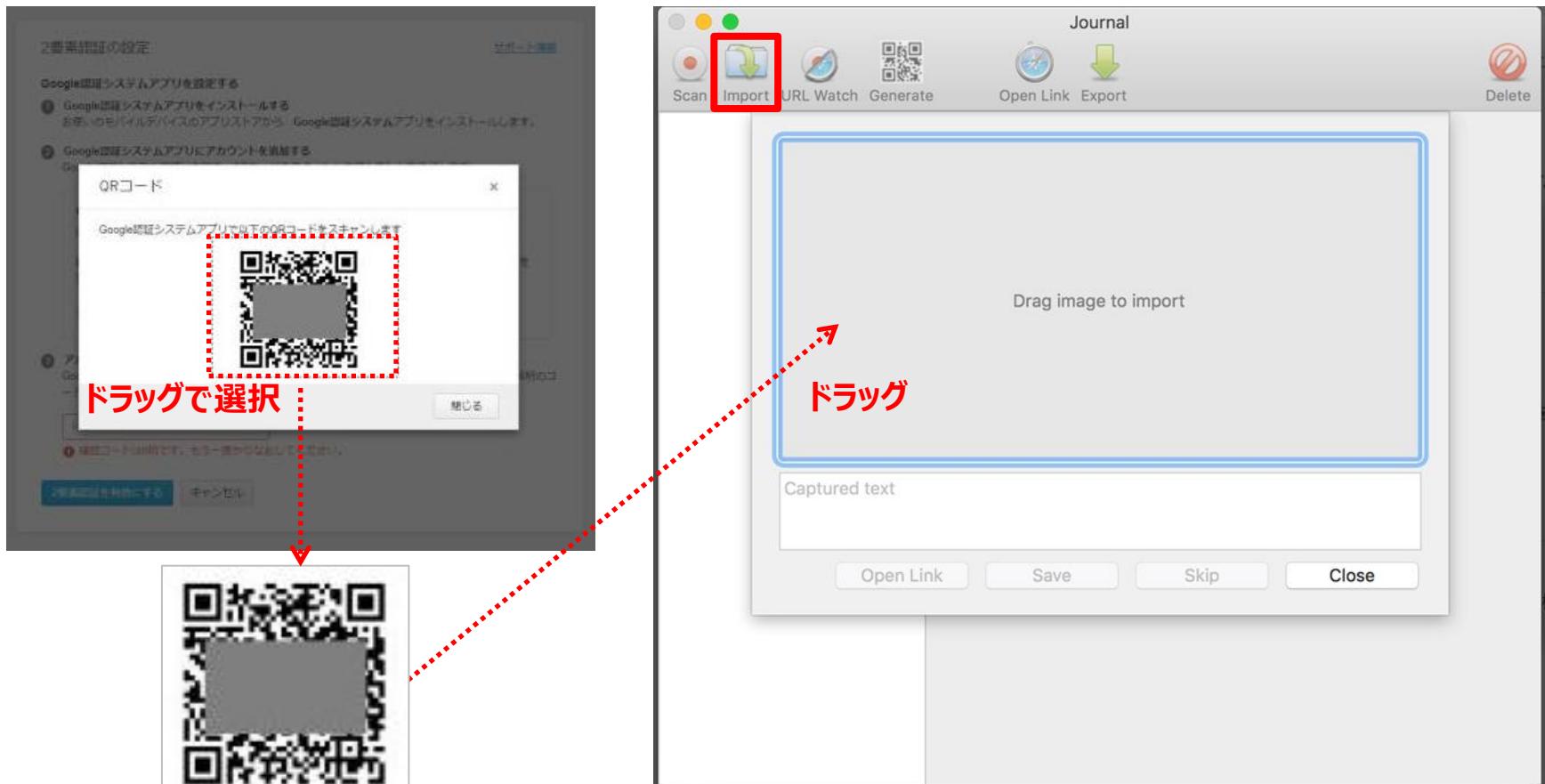
下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。



4. 下記画面が表示されます。「QRコードを表示する」をクリックします。

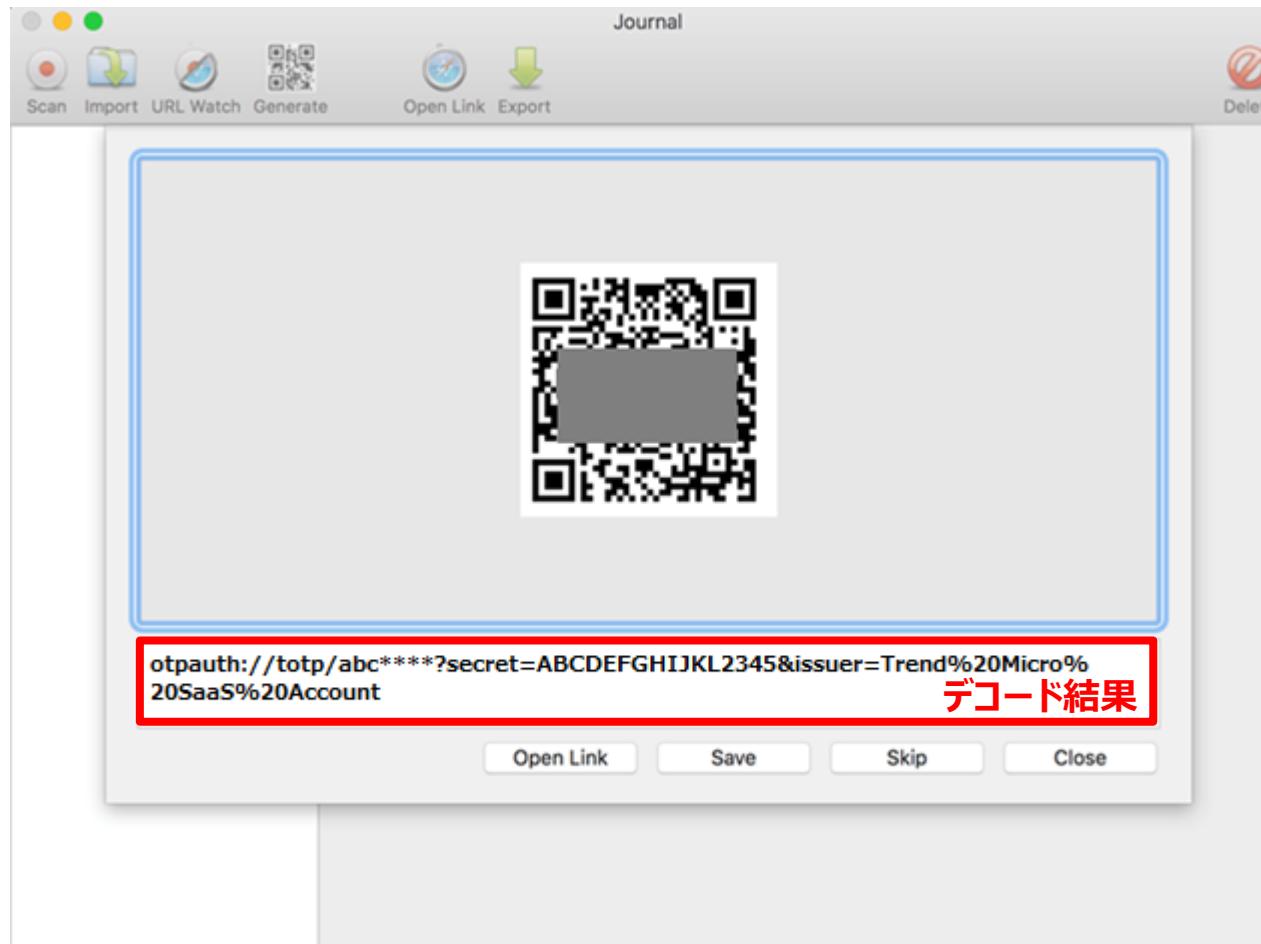


5. QRコードが表示されるので、「command + shift + 4」を同時に押し、ドラッグしてQRコード画面をキャプチャします。
6. インストールした「QR Journal」を起動します。
※App Store>[購入済み]をクリックすると、インストールしたQR Journalを開くことができます。
7. 下記赤枠ボタン(Import)をクリックし、「Drag image to import」の枠内にPrintScreenした画面をドラッグします。



スクリーンショットファイル生成

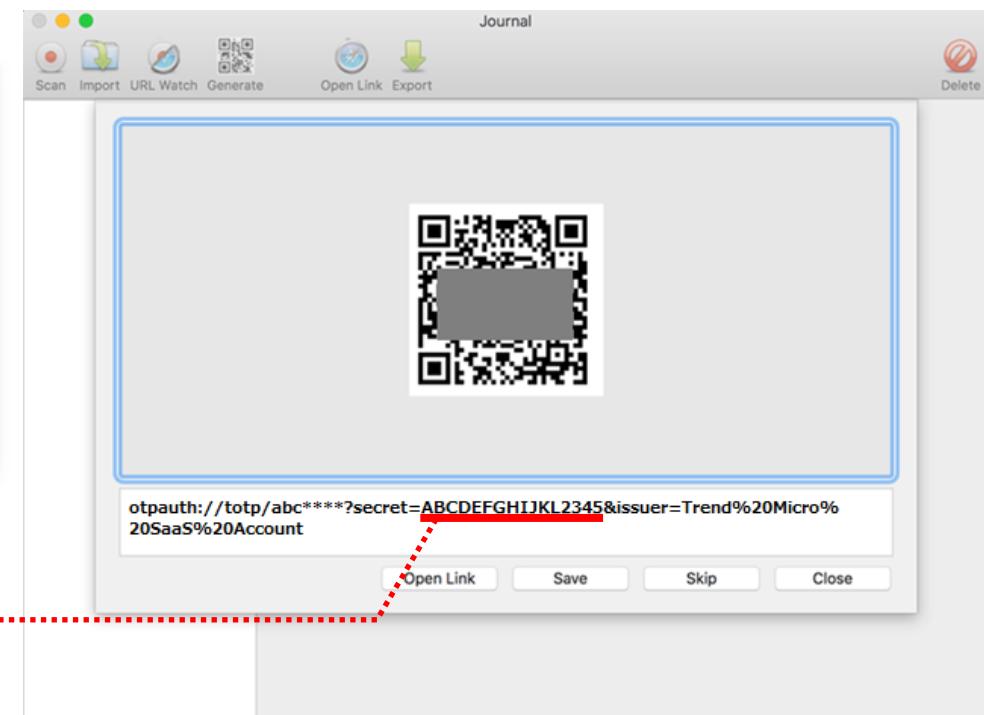
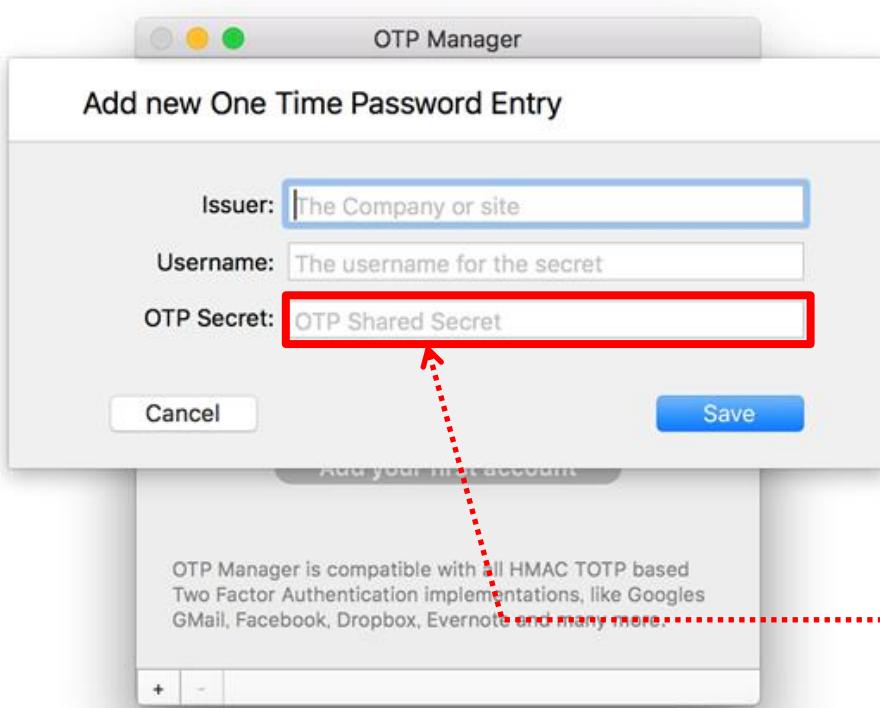
7. QRコードがデコードされます。



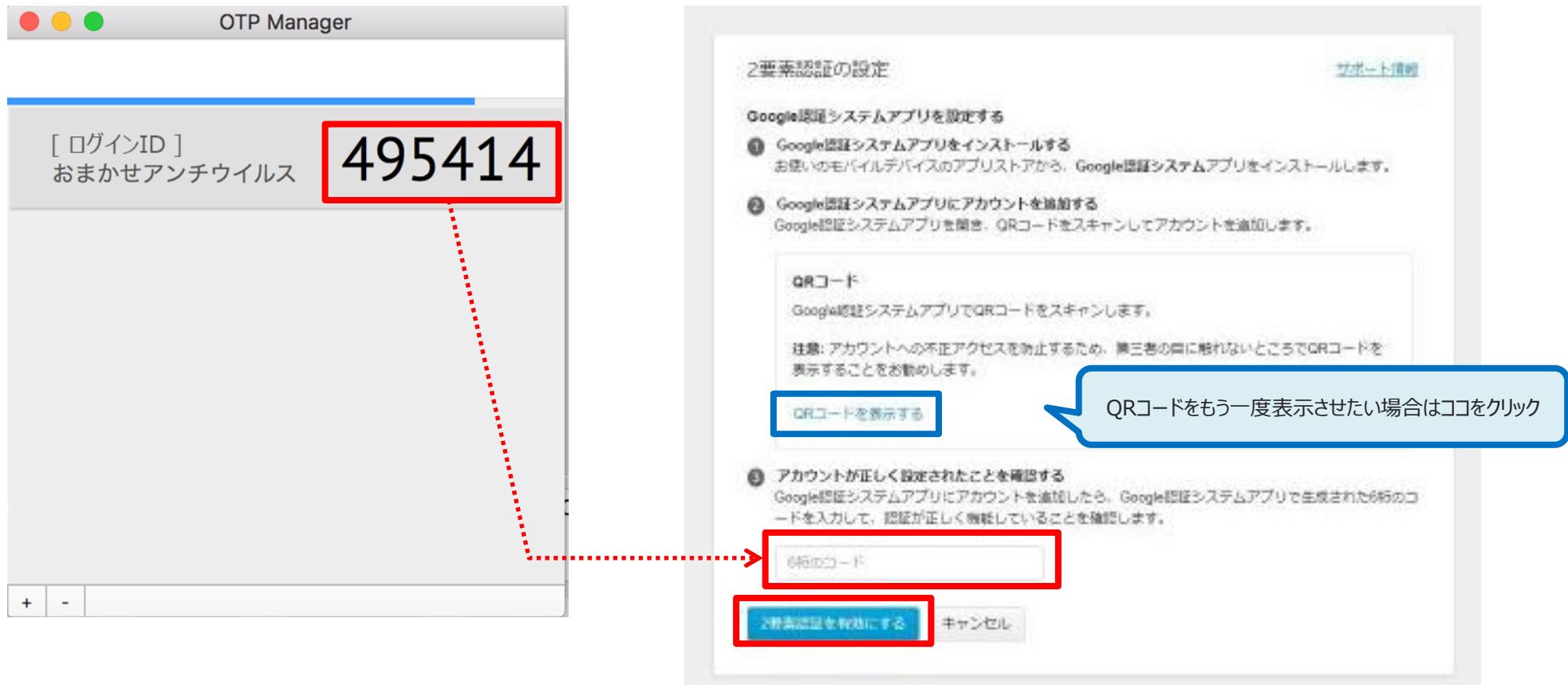
8. OTP Managerを立ち上げて下記を行います。

※App Store>[購入済み]をクリックすると、インストールしたOTP Managerを開くことができます。

- ① OTP Managerの画面が表示されたら、「Add your first account」ボタンをクリックします。
- ② Issuer : 任意の登録名称を入力します
- ③ Username : ログインIDを入力します
- ④ OTP Secret : QRコード デコード結果の「=」から「&」の間の文字列をコピーし、項目④に貼り付けます
- ⑤ 「Save」ボタンをクリックします。



10. OTP Managerの登録が完了し、ワンタイムパスワードが表示されます。
11. 6桁のコードが時間切れになる前に、管理コンソールの2要素認証登録画面のパスワード入力箇所へ入力し「2要素認証を有効にする」ボタンをクリックします。



14. 登録が完了すると下記画面が表示されます。

次回以降のログインは、「OTP Manager」を起動し、生成した 6 行のコード入力が必要になります。

The screenshot shows a web interface for Trend Micro's Licensing Platform. At the top left is the Trend Micro logo and the text "2要素認証". At the top right is the text "Licensing Platform". The main content area has a title "2要素認証" and a "サポート情報" link. Below this, there is a note about two-factor authentication (2FA) improving account security by preventing password theft even if a password is leaked. It lists the current status as "有効" (Enabled), the verification method as "Google認証システムアプリ" (Google Authentication System App), and the registered email address as "abc****@**.com". A note at the bottom states that if a confirmation code cannot be obtained, a one-time emergency access code will be sent to the registered email address.

| 状況: | 有効 | 無効にする デバイスの変更 |
|--------------|-----------------|---------------------------------|
| 認証方法: | Google認証システムアプリ | |
| 登録済みメールアドレス: | abc****@**.com | |

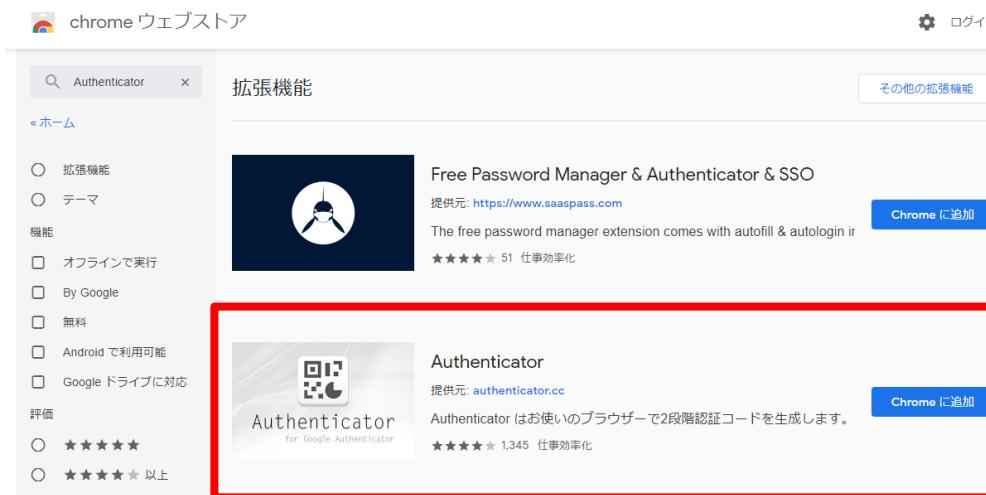
注意: 選択した認証方法を使用して確認コードを取得できない場合は、トレンドマイクロからお客様の登録済みメールアドレスへ、1回限り使用できる緊急アクセスコードをお送りすることができます。表示されている登録済みメールアドレスが正しくない場合は、アカウントの設定でメールアドレスを変更してください。

Chromeアドオンを用いた設定方法 1/6

1. 管理者が利用するデバイス上のChromeブラウザでChromeウェブストアを開き、下記アドオンを「Chromeに追加」します。

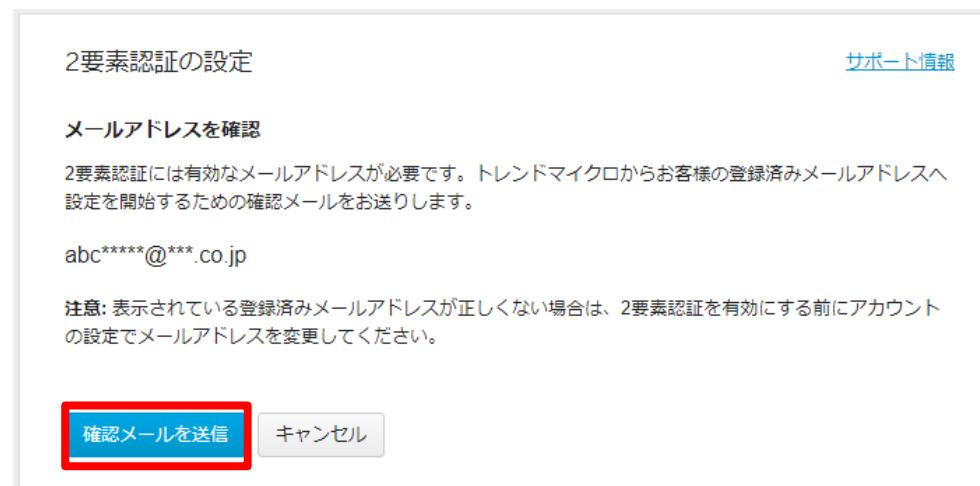
・Authenticator

二要素認証のワンタイムパスワードを発行するためのアドオン



2. 管理コンソールの

「2要素認証の設定」画面にて、「確認メールを送信」をクリックします。



Chromeアドオンを用いた設定方法 2/6

3. 「登録メール確認コード」画面が表示されます。

ご契約時に登録したメールアドレス宛に

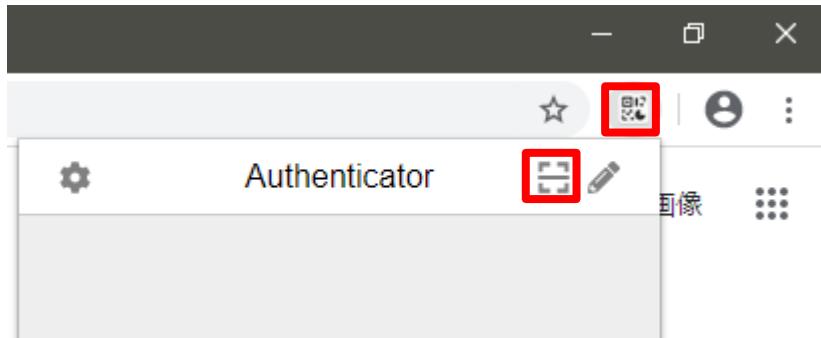
下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。



4. 下記画面が表示される。「QRコードを表示する」をクリックします。



5. Chromeブラウザ右上に表示された「Authenticator」のアイコンをクリックした後、スキャンアイコンをクリックします。

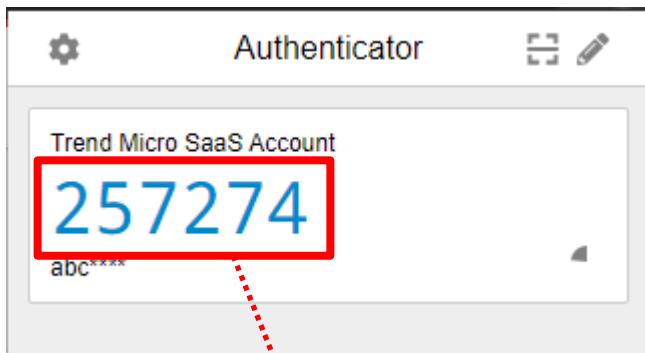


6. 下記赤枠のボタンをクリック後QRコードを左クリックしたままマウスで囲みます。
正しく登録完了すると、右図のメッセージが表示されます。



Chromeアドオンを用いた設定方法 5/6

7. 再度、Chromeブラウザ右上に表示された「Authenticator」のアイコンをクリックすると、ワンタイムパスワードが表示されます。
8. 6桁のコードが時間切れになる前に、管理コンソールの2要素認証登録画面のパスワード入力箇所へ入力し、「2要素認証を有効にする」ボタンをクリックします。



14. 登録が完了すると下記画面が表示されます。

次回以降のログインは、「Authenticator」をクリックし、表示される6行のコード入力が必要になります。

The screenshot shows a web page from the Trend Micro Licensing Platform. At the top left is the Trend Micro logo and the text "2要素認証". At the top right is the text "Licensing Platform". The main content area has a title "2要素認証" and a "サポート情報" link. Below this, there is a message about two-factor authentication: "2要素認証を使用することで、アカウントのセキュリティを強化できます。万一パスワード漏えいトラブルが発生した場合でも、お客様のクラウド型サービス (SaaS) 製品コンソールを不正アクセスから守ります。". There are three table rows with the following data:

| 状況: | 有効 | 無効にする | | デバイスの変更 |
|--------------|-----------------|-------|--|---------|
| 認証方法: | Google認証システムアプリ | | | |
| 登録済みメールアドレス: | abc****@***.com | | | |

Below the table, a note states: "注意: 選択した認証方法を使用して確認コードを取得できない場合は、トレンドマイクロからお客様の登録済みメールアドレスへ、1回限り使用できる緊急アクセスコードをお送りすることができます。表示されている登録済みメールアドレスが正しくない場合は、アカウントの設定でメールアドレスを変更してください。"

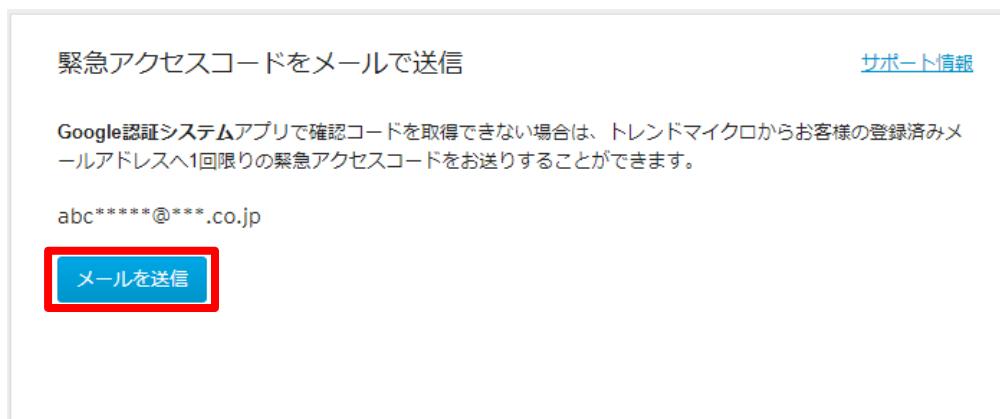
二要素認証を設定したトーカンアプリを紛失、削除してしまった場合 1/5

- 二要素認証を設定したトーカンアプリが入ったスマートフォンを紛失・破損してしまった場合、またトーカンアプリを削除してしまった場合など、下記の方法でログインおよび二要素認証の無効化を実施します。
- 引き続き二要素認証をご利用の場合は、無効化した後に改めて有効化と設定をお願いいたします。

1. ID/パスワード入力後に二要素認証確認コード入力画面で、「緊急アクセスコードをメールで送信」をクリックします。



2. 送信先メールアドレスを確認して「メールを送信」をクリックします。



二要素認証を設定したトークンアプリを紛失、削除してしまった場合 2/5

3. メールで届いた緊急アクセスコードを入力し「送信」ボタンをクリックします。

緊急アクセスコード

緊急アクセスコードを次のアドレスに送信しました abc****@**.co.jp. 緊急アクセスコードを入力してログインしてください。

緊急アクセスコード

メールが5分以内に届かない場合は、迷惑メールフォルダをご確認ください。

送信

4. ログイン後、右上のメニューから「ユーザ登録情報」をクリックします。



二要素認証を設定したトークンアプリを紛失、削除してしまった場合 3/5

5. 2要素認証の「設定」をクリックします。

The screenshot shows a user profile page for 'SAMPLE_USER'. At the top right, there is a user icon and the text 'SAMPLE_USER'. Below the header, there are two navigation links: '登録済みの製品/サービス' (Registered Products/Services) and 'ヘルプ ▾' (Help). The main content area is titled 'ユーザ登録情報' (User Registration Information). It displays three fields: 'アカウント名:' (Account Name: SAMPLE_USER), 'パスワード:' (Password: [パスワードの変更](#)), and '2要素認証:' (Two-factor authentication: 有効 [設定](#)). The '設定' link under '2要素認証' is highlighted with a red box.

| | |
|---------|--------------------------|
| アカウント名: | SAMPLE_USER |
| パスワード: | パスワードの変更 |
| 2要素認証: | 有効 設定 |

二要素認証を設定したトークンアプリを紛失、削除してしまった場合 4/5

6. 「無効にする」をクリックします。確認メッセージがあるので「無効にする」をクリックします。

The screenshot shows the Trend Micro 2-factor authentication settings interface. At the top, there's a header with the Trend Micro logo and the text "2要素認証". Below it, a main section titled "2要素認証" contains a paragraph about how 2FA strengthens account security. It lists the current status as "有効" (Enabled), the verification method as "Google認証システムアプリ" (Google Authenticator App), and the registered email address as "abc*****@***.co.jp". A note below the email address provides instructions for emergency access if the app is lost or deleted. A red box highlights the "無効にする" (Disable) button in the top right corner of this section. A modal dialog box is overlaid on the page, containing a warning icon, the text "2要素認証を無効にする" (Disable 2-factor authentication), a detailed explanation of what happens when 2FA is disabled, and a question "2要素認証を無効にしますか?" (Do you want to disable 2-factor authentication?). The "無効にする" button in the dialog is also highlighted with a red box.

2要素認証

2要素認証を使用することで、アカウントのセキュリティを強化できます。万一パスワード漏えいトラブルが発生した場合でも、お客様のクラウド型サービス (SaaS) 製品コンソールを不正アクセスから守ります。

状況: 有効 | 無効にする | デバイスの変更

認証方法: Google認証システムアプリ

登録済みメールアドレス: abc*****@***.co.jp

注意: 選択した認証方法を
レンドマイクロからお客様へ
届ける緊急アクセスコード
登録済みメールアドレス
アドレスを変更してください

2要素認証を無効にする

2要素認証を無効になるとアカウントのセキュリティ強化機能は追加されず、製品コンソールにアカウントとパスワードだけでログインできます。

2要素認証を無効にしますか?

無効にする キャンセル

二要素認証を設定したトークンアプリを紛失、削除してしまった場合 5/5

7. 改めて設定する場合は「2要素認証有効にする」をクリックし、本ドキュメントの設定手順に従って設定を実施してください。

The screenshot shows a user interface for managing two-factor authentication (2FA) settings. At the top left is the Trend Micro logo. To its right, the text "2要素認証" (2FA) is displayed. Below this is a large central box containing the following information:

2要素認証 [サポート情報](#)

2要素認証を使用することで、アカウントのセキュリティを強化できます。万一パスワード漏えいトラブルが発生した場合でも、お客様のクラウド型サービス (SaaS) 製品コンソールを不正アクセスから守ります。

状況: **無効** [2要素認証を有効にする](#)

The link "2要素認証を有効にする" is highlighted with a red rectangular border.