

【kUTMみまもりサポート】 二要素認証設定マニュアル

株式会社KDDIウェブコミュニケーションズ

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。
- ❑ トークンアプリは弊社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弊社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](#)

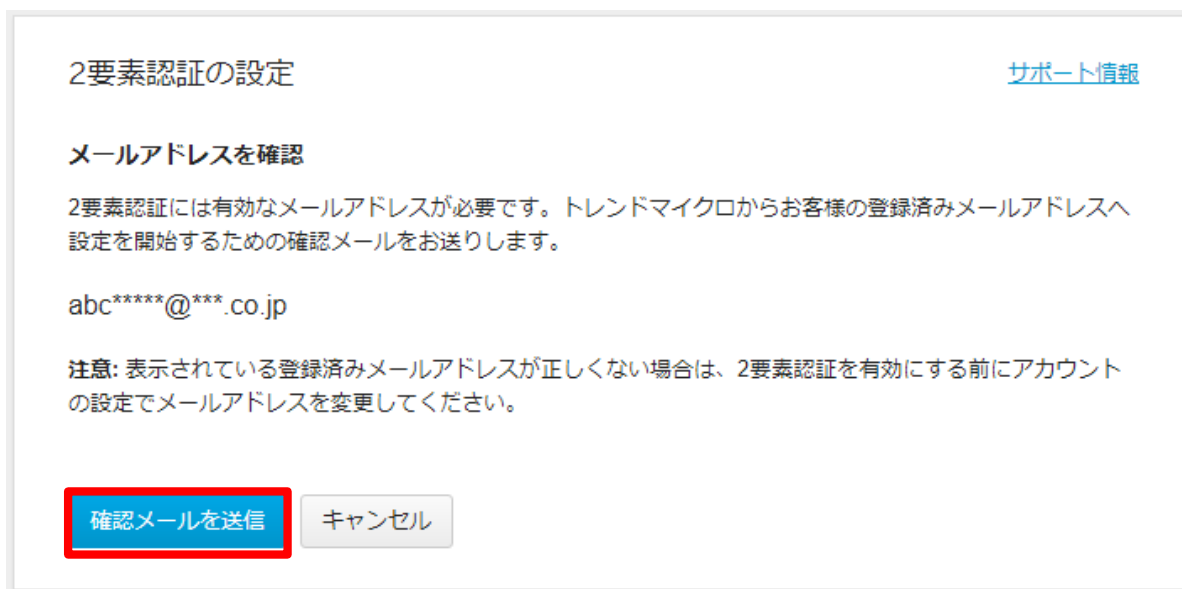
今後このメッセージを表示しない [危険性を理解したうえで、スキップします](#)

- [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

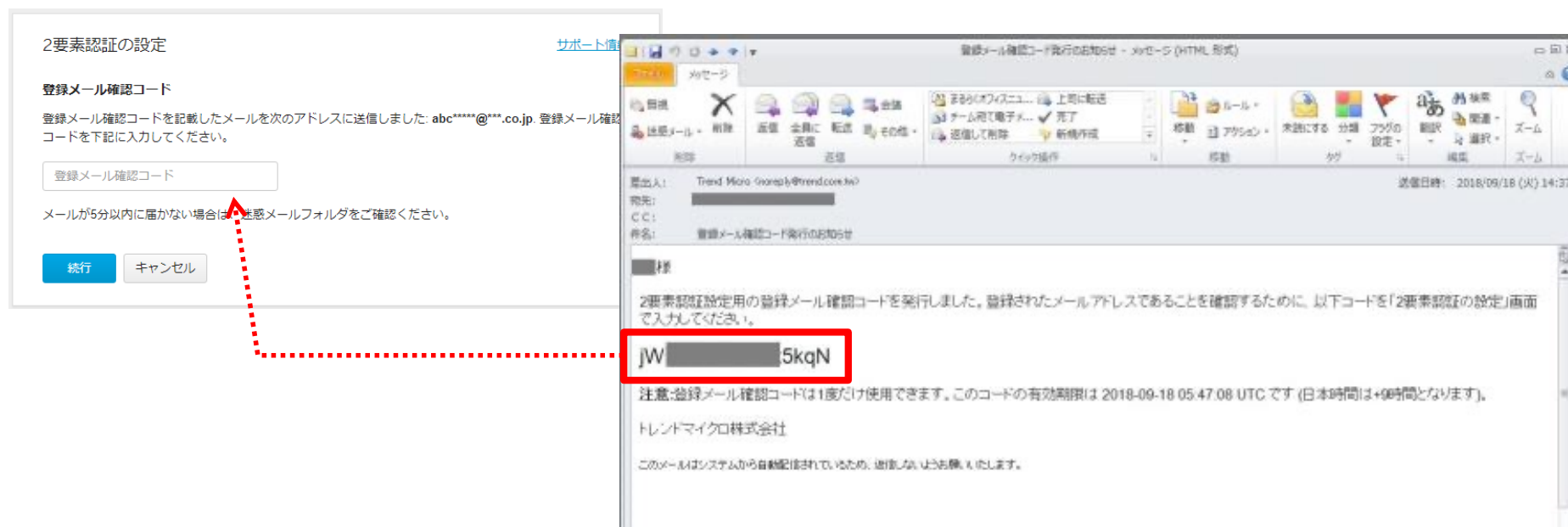
1. 管理者が利用するモバイルデバイス (iOS/Android) に「Google Authenticator」をインストールします。
 - App StoreまたはGoogle Playを立ち上げ、「Google認証」と検索
 - 「Google Authenticator」を選択し、インストールを実施



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。

TREND MICRO | 2要素認証

2要素認証の設定 [サポート情報](#)

Google認証システムアプリを設定する

① Google認証システムアプリをインストールする
お使いのモバイルデバイスのアプリストアから、Google認証システムアプリをインストールします。

② Google認証システムアプリにアカウントを追加する
Google認証システムアプリを開き、QRコードをスキャンしてアカウントを追加します。

QRコード
Google認証システムアプリでQRコードをスキャンします。

注意: アカウントへの不正アクセスを防止するため、第三者の目に触れないところでQRコードを表示することをお勧めします。

QRコードを表示する

③ アカウントが正しく設定されたことを確認する
Google認証システムアプリにアカウントを追加したら、Google認証システムアプリで生成された6桁のコードを入力して、認証が正しく機能していることを確認します。

6桁のコード

2要素認証を有効にする

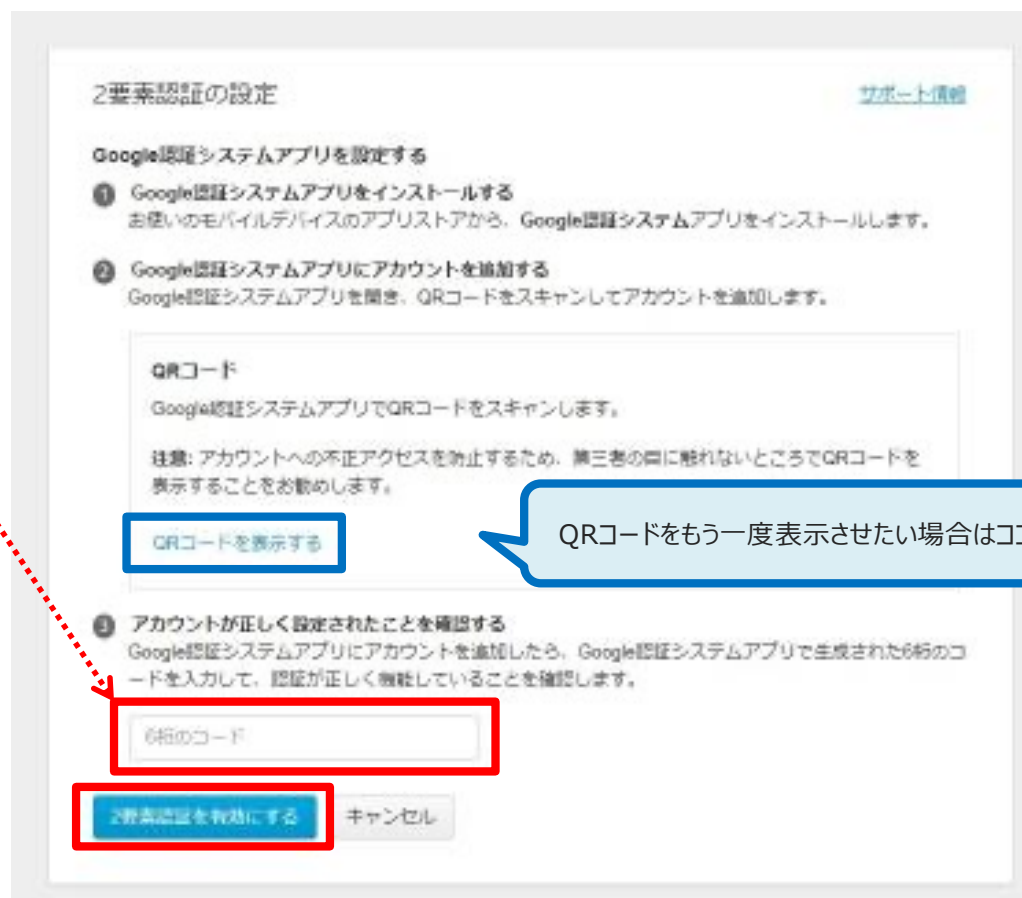
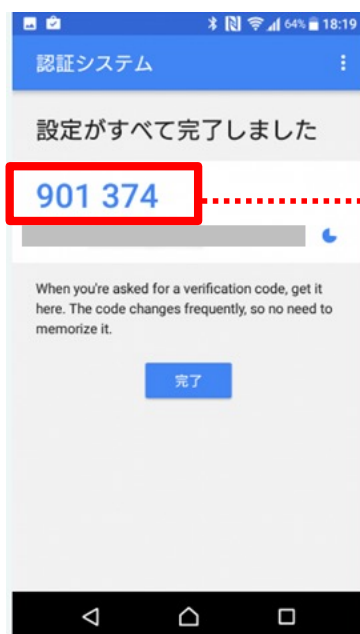
スマートフォン(iOS/Android)における設定方法 4/6

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。



※アプリの起動後、左記の画面が表示された場合は、
右上の「+」をクリックし、「バーコードをスキャン」をクリックします

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桁のコード入力が必要になります。

The screenshot shows the '2要素認証' (2-Factor Authentication) settings page in the Trend Micro Licensing Platform. The page includes the Trend Micro logo, the title '2要素認証', and a 'サポート情報' (Support Information) link. A descriptive paragraph explains that 2FA enhances account security. Below this is a table with three rows: '状況' (Status) set to '有効' (Enabled) with options to '無効にする' (Disable) or 'デバイスの変更' (Change device); '認証方法' (Authentication Method) set to 'Google認証システムアプリ' (Google Authenticator 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 provides instructions on how to use the emergency access code if the user cannot receive the 2FA code.

TREND MICRO | 2要素認証 Licensing Platform

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。万が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****@****.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（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-3.5.1zip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み取るためのソフト

<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。

2要素認証の設定 [サポート情報](#)

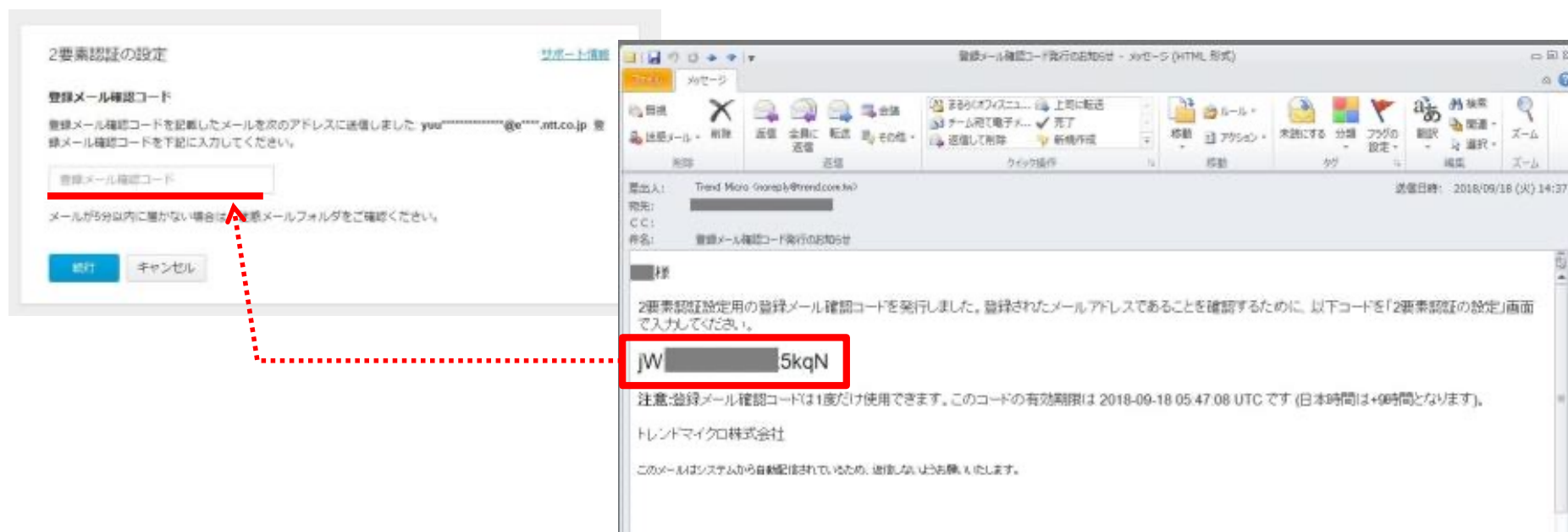
メールアドレスを確認

2要素認証には有効なメールアドレスが必要です。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設定を開始するための確認メールをお送りします。

abc*****@***.co.jp

注意: 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、2要素認証を有効にする前に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。

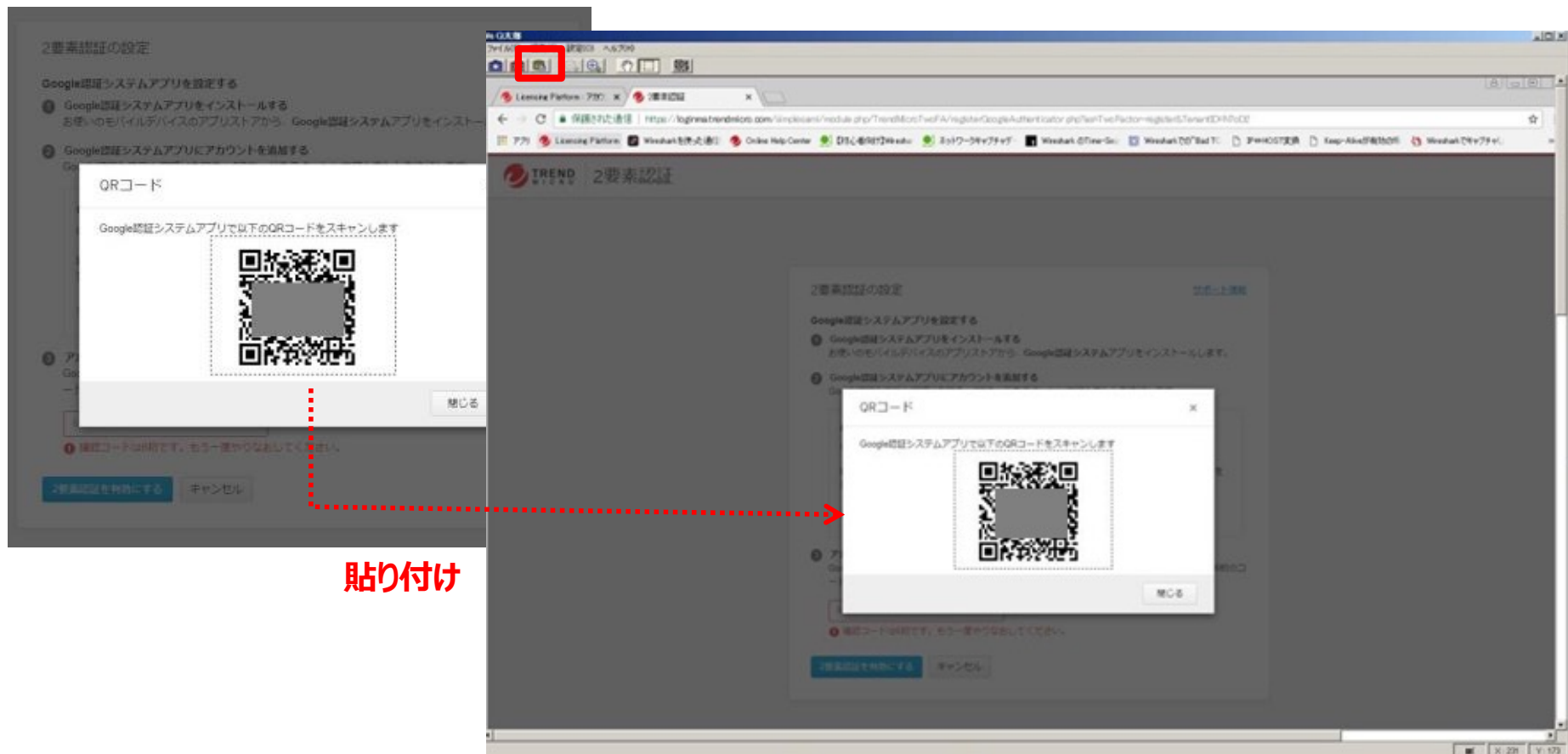
3. 「登録メール確認コード」画面が表示されます。
ご契約時に登録したメールアドレス宛に
下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。



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、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。

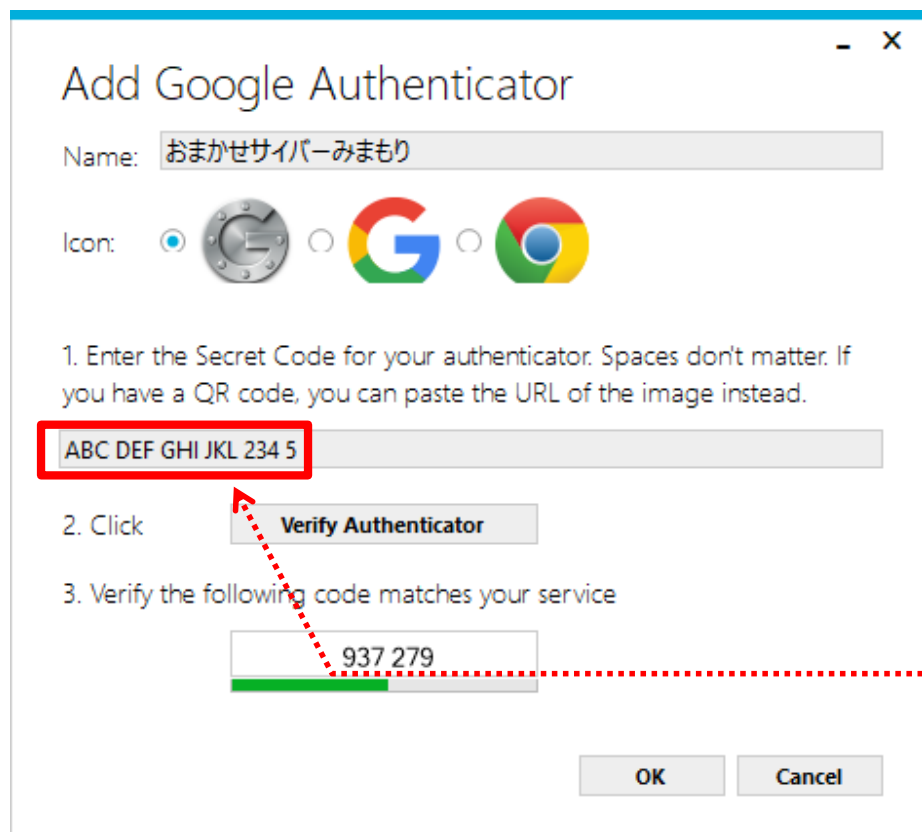


7. 下記赤枠のボタンをクリック後QRコードを左クリックしたままマウスで囲むとQRコードがデコードされます。



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。

Protection

1 Select how you would like to protect your authenticators. Using a password is strongly recommended, otherwise your authenticators could be read and stolen by malware running on your computer.

Protect with my own password
Your authenticators will be encrypted using your own password and you will need to enter your password to open WinAuth. Your authenticators will be inaccessible if you forget your password and you do not have a backup.

Password

Verify

Additionally, you can protect and encrypt your data using the built-in Windows account encryption. This will lock your authenticators to this computer or user so they cannot be opened even if the files are copied. You MUST turn this off if you are going to reformat your disk, re-install Windows or delete this user account.

Encrypt to only be useable on this computer

And only by the current user on this computer

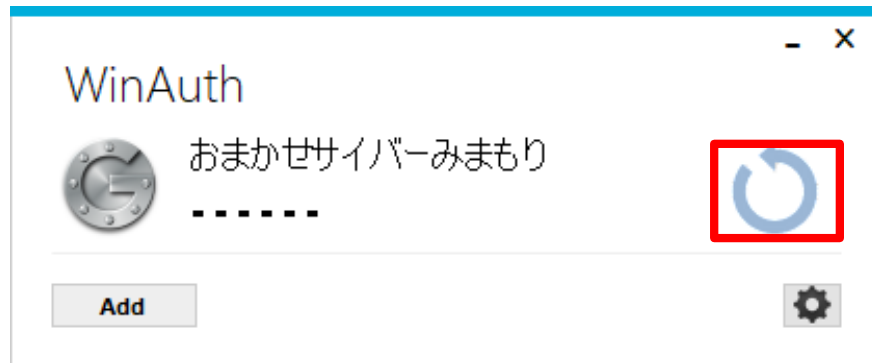
Lock with a YubiKey

Your YubiKey must support Challenge-Response using HMAC-SHA1 in one of its slots. Use the YubiKey personalization tool to configure the slot or click the Configure Slot button.

Slot 1

2

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桁のコード入力が必要になります。

The screenshot shows the '2要素認証' (2-Factor Authentication) settings page in the Trend Micro Licensing Platform. The page header includes the Trend Micro logo and the text '2要素認証' and 'Licensing Platform'. The main content area is titled '2要素認証' and includes a 'サポート情報' (Support Information) link. Below the title, there is a paragraph explaining that 2FA enhances account security and protects against password leaks and unauthorized access to SaaS products. A table below lists the current status and settings:

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み取るためのソフト

※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。

2要素認証の設定 [サポート情報](#)

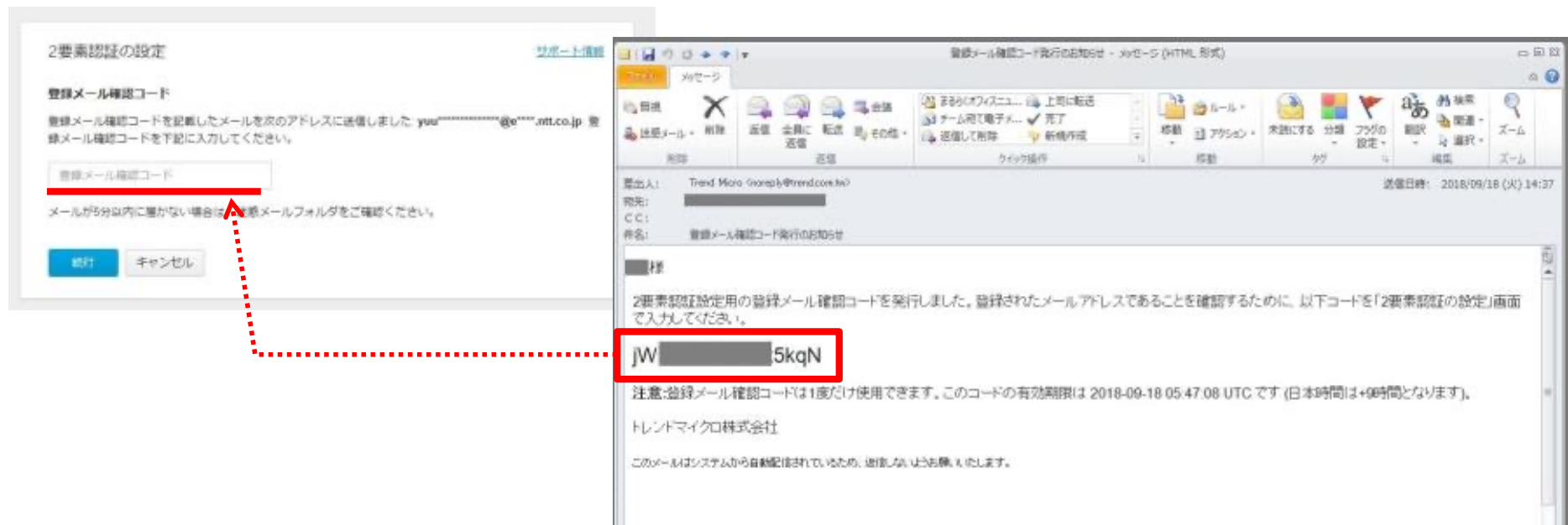
メールアドレスを確認

2要素認証には有効なメールアドレスが必要です。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設定を開始するための確認メールをお送りします。

abc*****@***.co.jp

注意: 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、2要素認証を有効にする前に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。

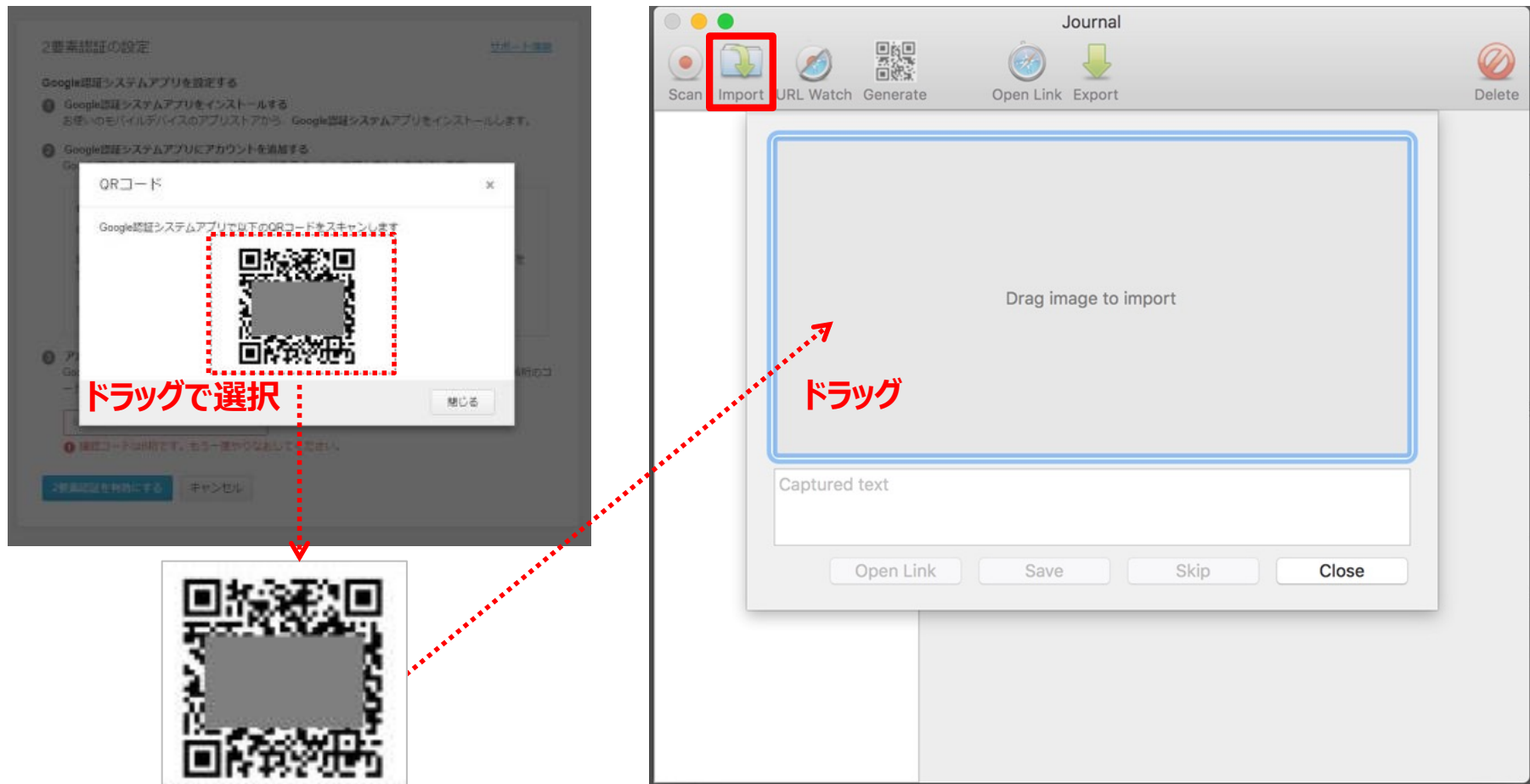
3. 「登録メール確認コード」画面が表示されます。
ご契約時に登録したメールアドレス宛に
下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。



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。

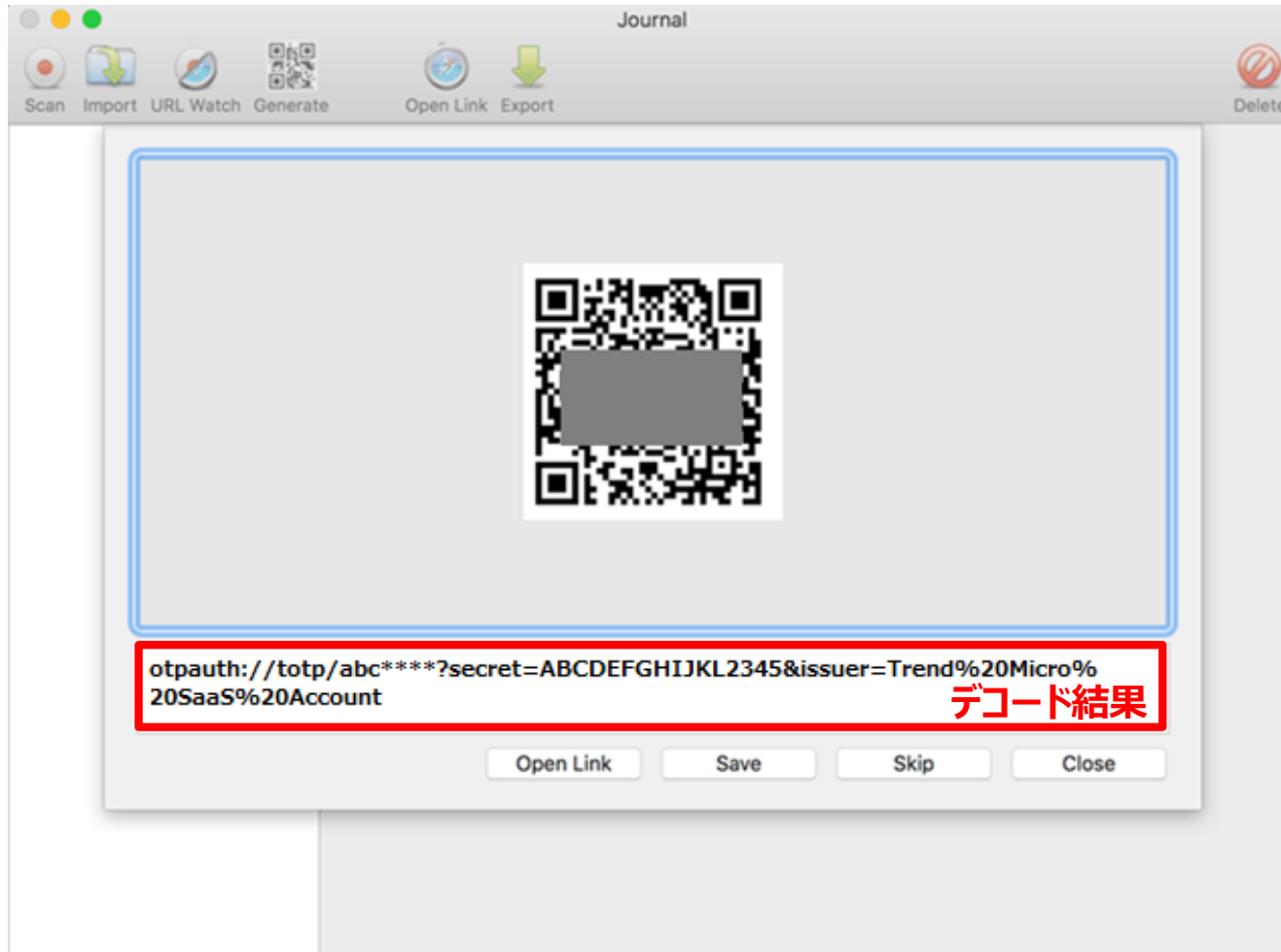


5. QRコードが表示されるので、「command + shift + 4」を同時に押し、ドラッグしてQRコード画面をキャプチャします。
6. インストールした「QR Journal」を起動します。
※App Store> [購入済み]をクリックすると、インストールしたQR Journalを開くことができます。
7. 下記赤枠ボタン(Import)をクリックし、「Drag image to import」の枠内にPrintScreenした画面をドラッグします。



スクリーンショットファイル生成

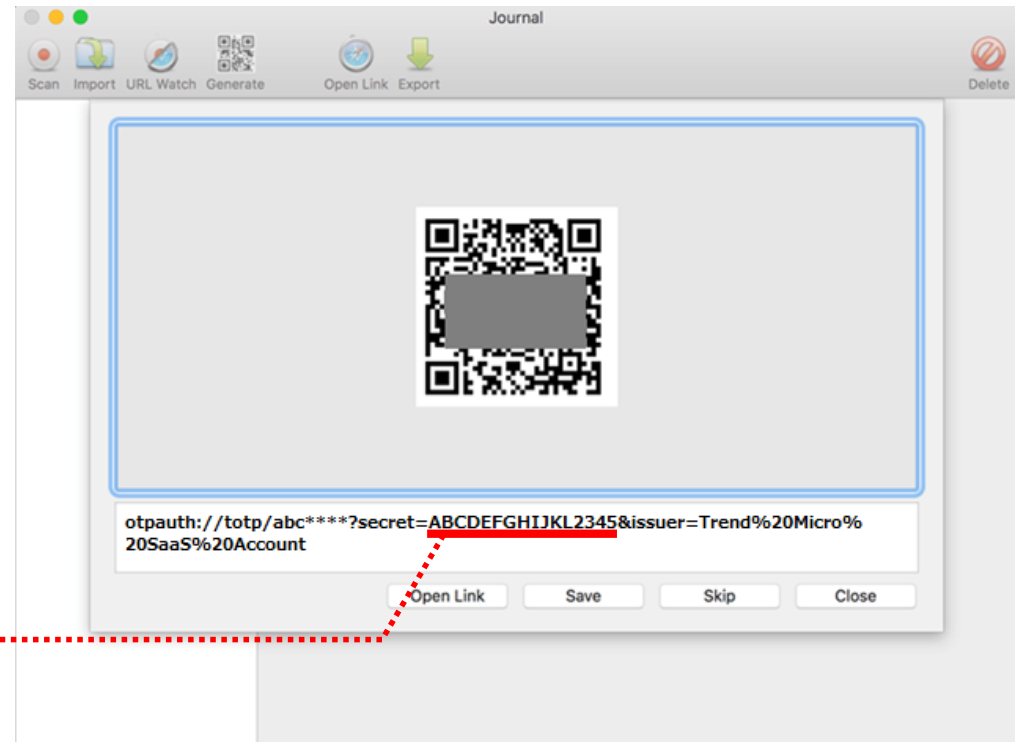
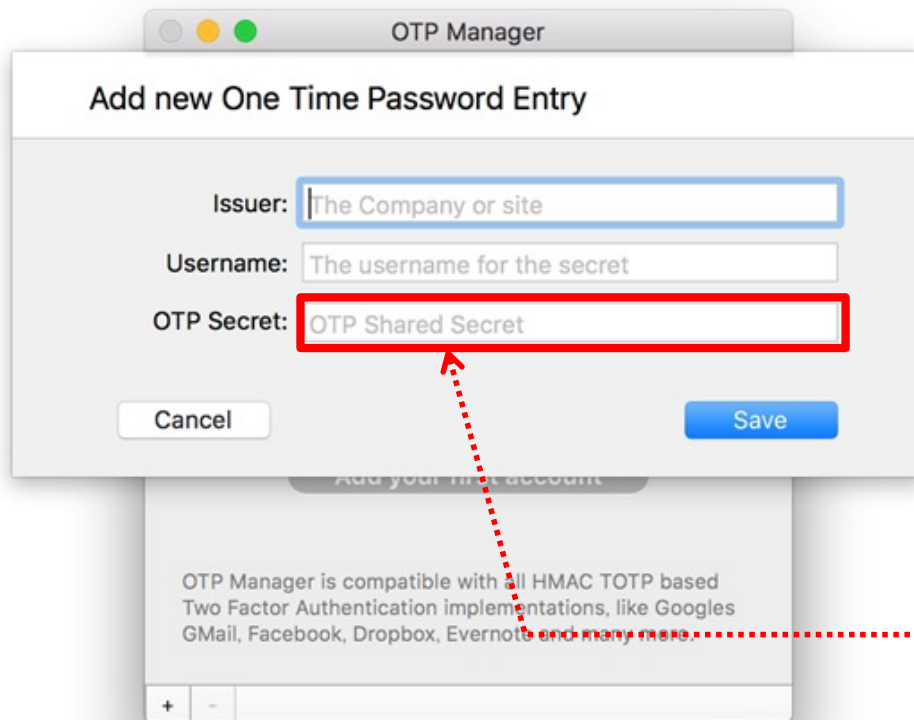
7. QRコードがデコードされます。



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1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桁のコード入力が必要になります。



The screenshot shows the '2要素認証' (2-Factor Authentication) settings page in the Trend Micro Licensing Platform. The page header includes the Trend Micro logo, the title '2要素認証', and the text 'Licensing Platform'. The main content area contains 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。

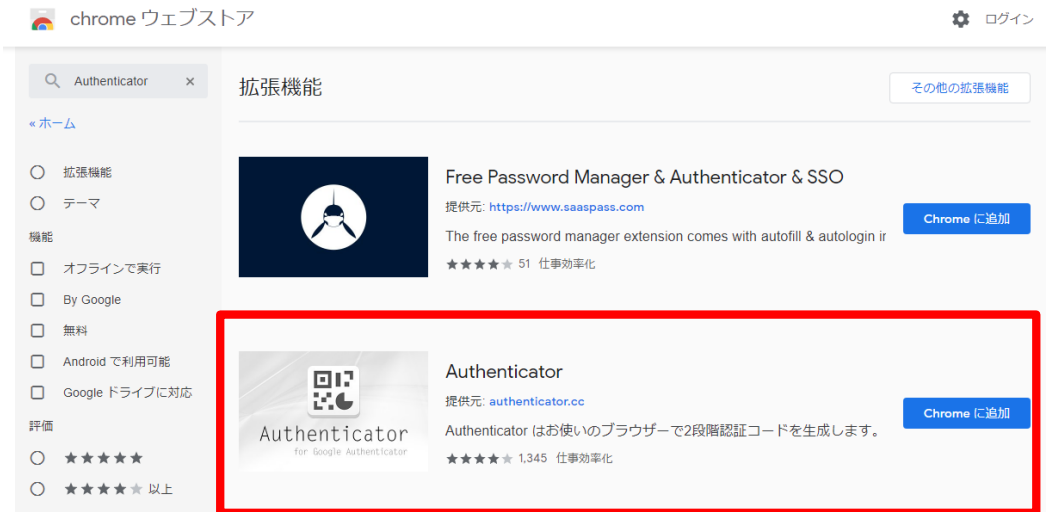
状況:	有効	無効にする		デバイスの変更
認証方法:	Google認証システムアプリ			
登録済みメールアドレス:	abc****@****.com			

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。

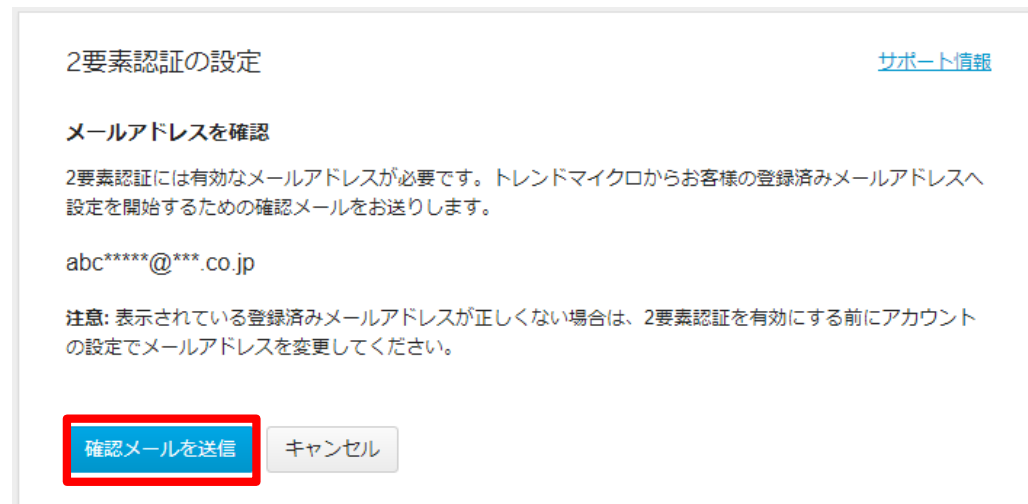
1. 管理者が利用するデバイス上のChromeブラウザでChromeウェブストアを開き、下記アドオンを「Chromeに追加」します。

•Authenticator

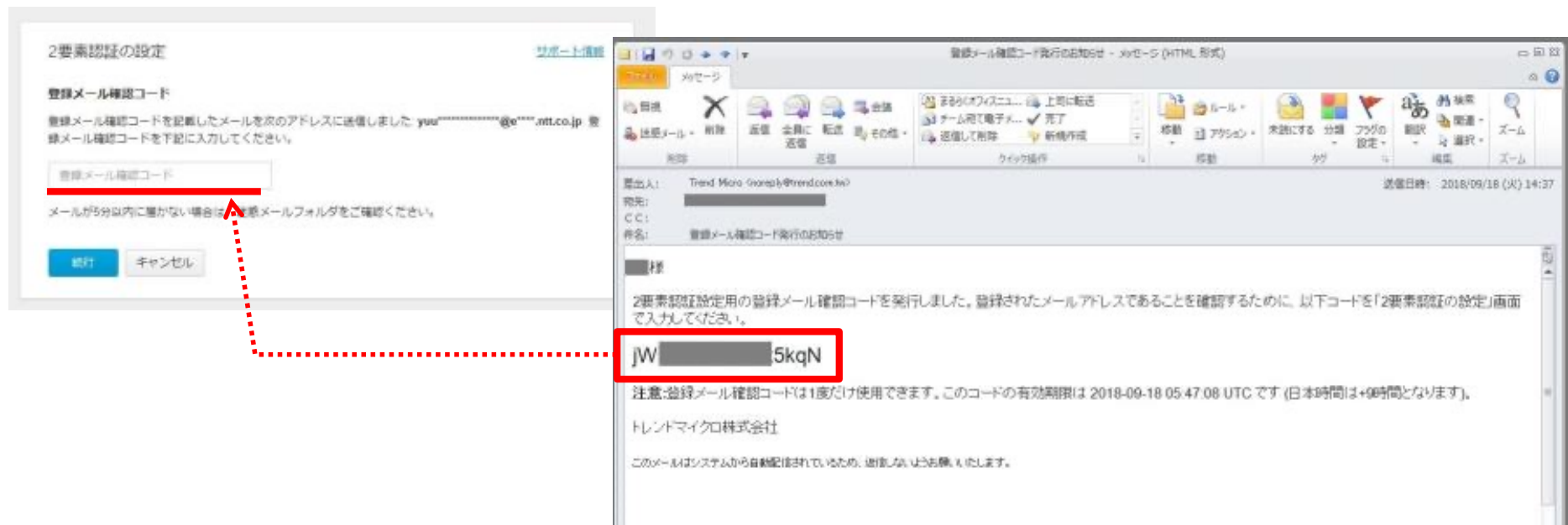
二要素認証のワンタイムパスワードを発行するためのアドオン



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。



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。

TREND MICRO | 2要素認証

2要素認証の設定 [サポート情報](#)

Google認証システムアプリを設定する

- 1 Google認証システムアプリをインストールする
お使いのモバイルデバイスのアプリストアから、Google認証システムアプリをインストールします。
- 2 Google認証システムアプリにアカウントを追加する
Google認証システムアプリを開き、QRコードをスキャンしてアカウントを追加します。

QRコード
Google認証システムアプリでQRコードをスキャンします。

注意: アカウントへの不正アクセスを防止するため、第三者の目に触れないところでQRコードを表示することをお勧めします。

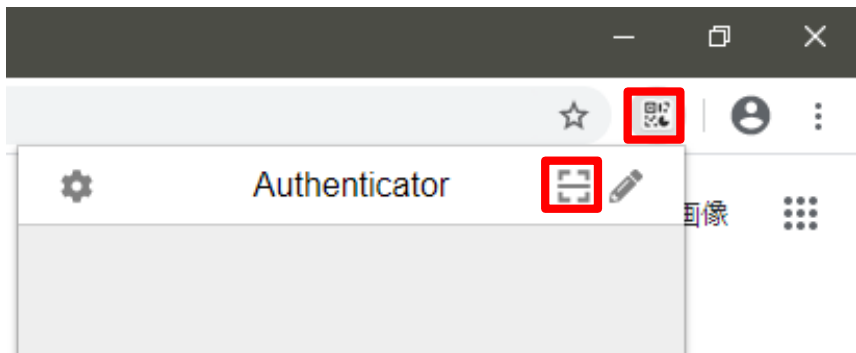
QRコードを表示する

- 3 アカウントが正しく設定されたことを確認する
Google認証システムアプリにアカウントを追加したら、Google認証システムアプリで生成された6桁のコードを入力して、認証が正しく機能していることを確認します。

6桁のコード

[2要素認証を有効にする](#) [キャンセル](#)

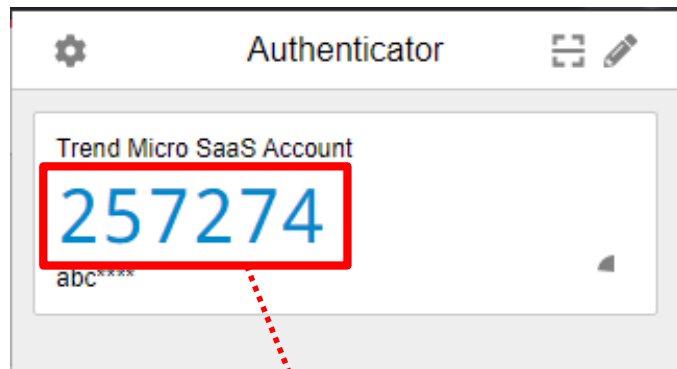
5. Chromeブラウザ右上に表示された「Authenticator」のアイコンをクリックした後、スキャンアイコンをクリックします。



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。



- 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。
- 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桁のコード入力が必要になります。

The screenshot shows the '2要素認証' (2-Factor Authentication) settings page in the Trend Micro Licensing Platform. The page header includes the Trend Micro logo, the title '2要素認証', and the text 'Licensing Platform'. The main content area contains the following information:

- 2要素認証** (2-Factor Authentication) with a [サポート情報](#) (Support Information) link.
- Text: 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。万が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 (Active) | 無効にする (Deactivate) | [デバイスの変更](#) (Change Device)
- 認証方法:** Google認証システムアプリ (Google Authenticator)
- 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。

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 1/5

- 二要素認証を設定したトーク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、またトーク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。



確認コード [サポート情報](#)

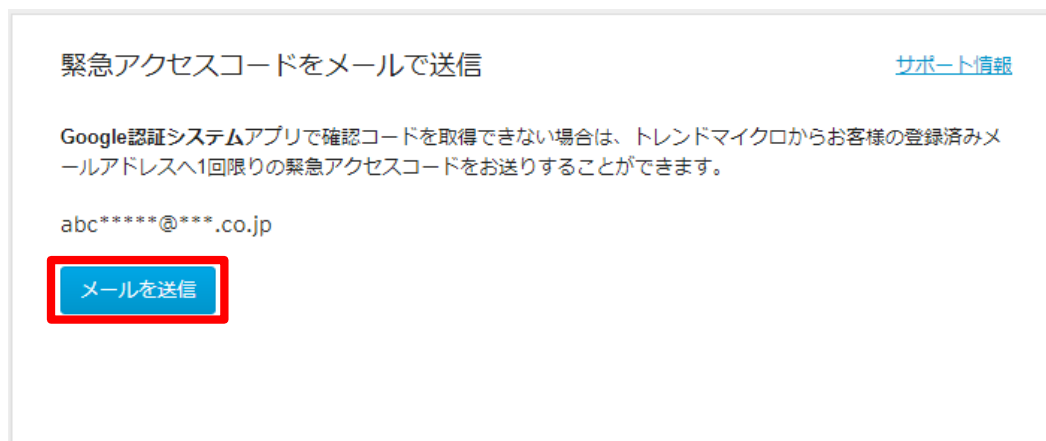
お使いのモバイルデバイスからGoogle認証システムアプリを使用してトレンドマイクロSaaS製品用の確認コードを取得し、そのコードを入力してログインしてください。

6桁のコード

送信

[緊急アクセスコードをメールで送信](#)

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。



緊急アクセスコードをメールで送信 [サポート情報](#)

Google認証システムアプリで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回限りの緊急アクセスコードをお送りすることができます。

abc*****@***.co.jp

メールを送信

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 [サポート情報](#)

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。



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 this is a red navigation bar with three items: '登録済みの製品/サービス', 'ヘルプ', and a dropdown arrow. Underneath the navigation bar is the section title 'ユーザ登録情報'. A table-like structure displays the following information:

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

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 2FA settings page. The page title is "2要素認証" (Two-Factor Authentication). The status is "有効" (Enabled). The authentication method is "Google認証システムアプリ" (Google Authenticator app). The registered email address is "abc*****@***.co.jp". A confirmation dialog box is overlaid on the page, asking "2要素認証を無効にする" (Disable two-factor authentication) and "2要素認証を無効にしますか?" (Do you want to disable two-factor authentication?). The dialog box has a yellow warning icon and a close button (X). The "無効にする" (Disable) button is highlighted with a red box, and the "キャンセル" (Cancel) button is also visible.

TREND MICRO | 2要素認証 [サポート情報](#)

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削除すると、Trend Microからお客様に送られる緊急アクセスコードが利用できなくなります。登録済みメール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要素認証を無効にす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

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。



2要素認証

[サポート情報](#)

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: 無効

[2要素認証を有効にする](#)