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。

目次

- 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

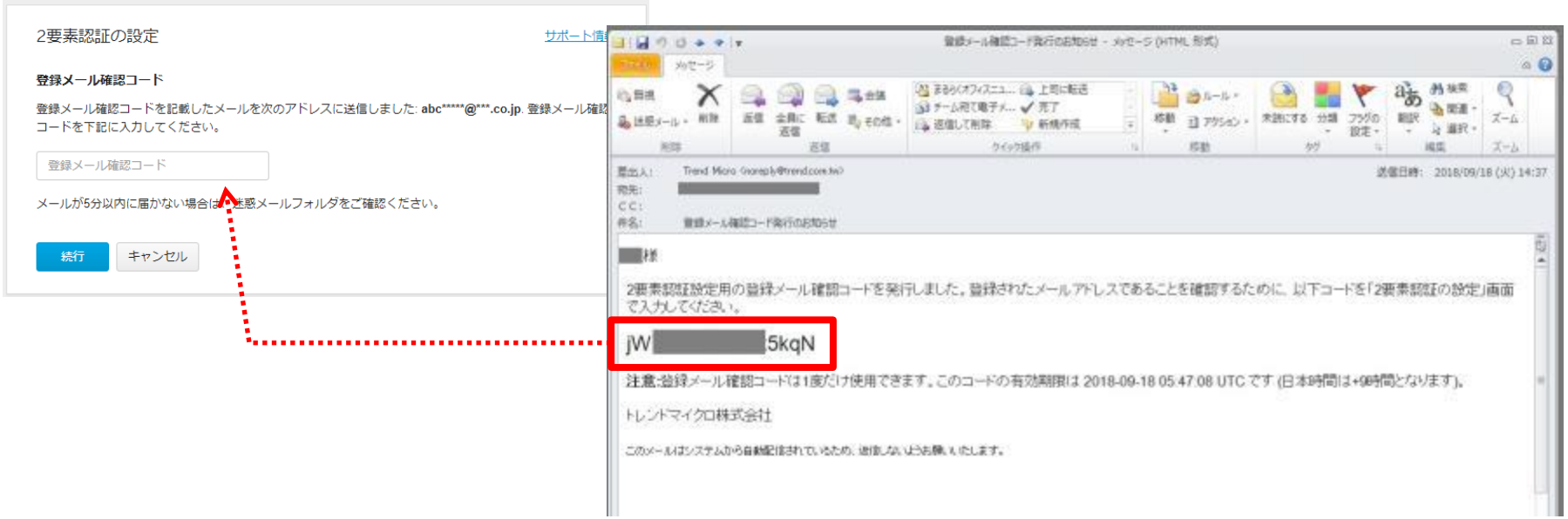
スマートフォン(iOS/Android)における設定方法　1/6

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。

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。

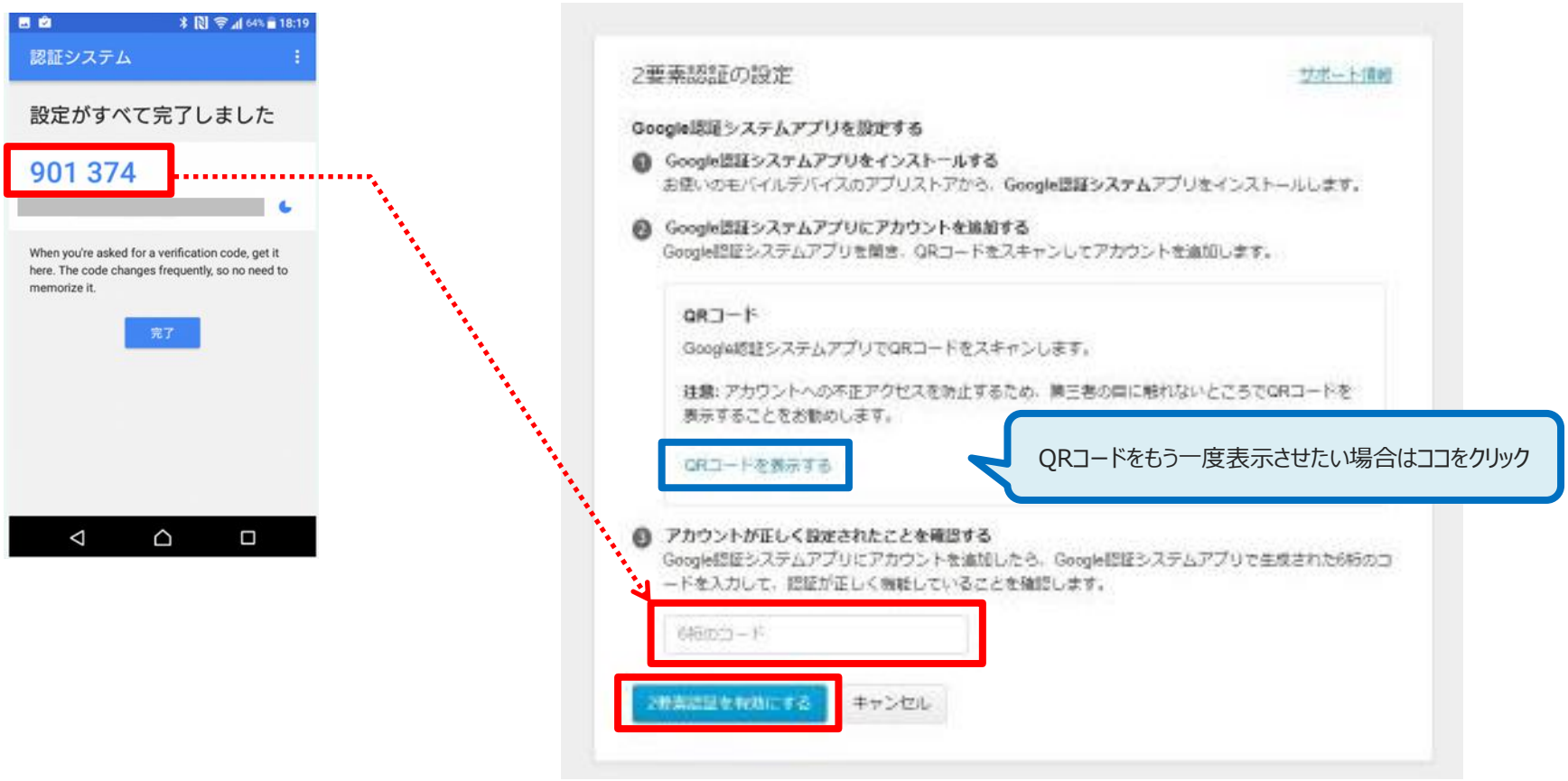
スマートフォン(iOS/Android)における設定方法　4/6

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。

※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

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。



スマートフォン(iOS/Android)における設定方法　6/6

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。

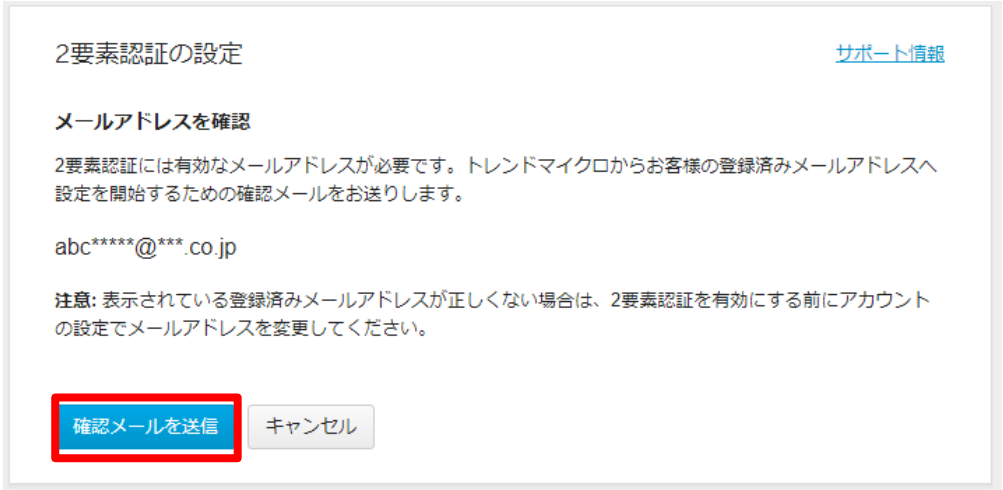
Windowsにおける設定方法　1/9

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。

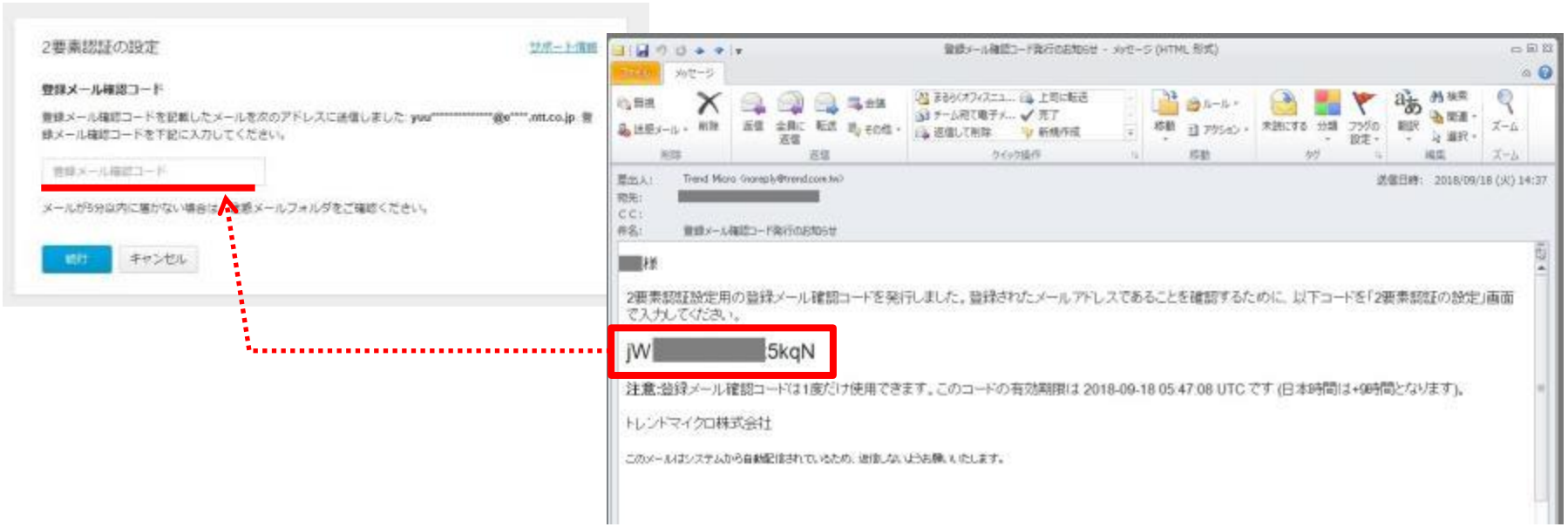
①WinAuth
二要素認証のワンタイムパスワードを発行するためのソフト
https://github.com/winauth/winauth/releases
※WinAuth-3.5.1zipをダウンロード
※今後、管理コンソール画面へログインするときに必要となります。

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。



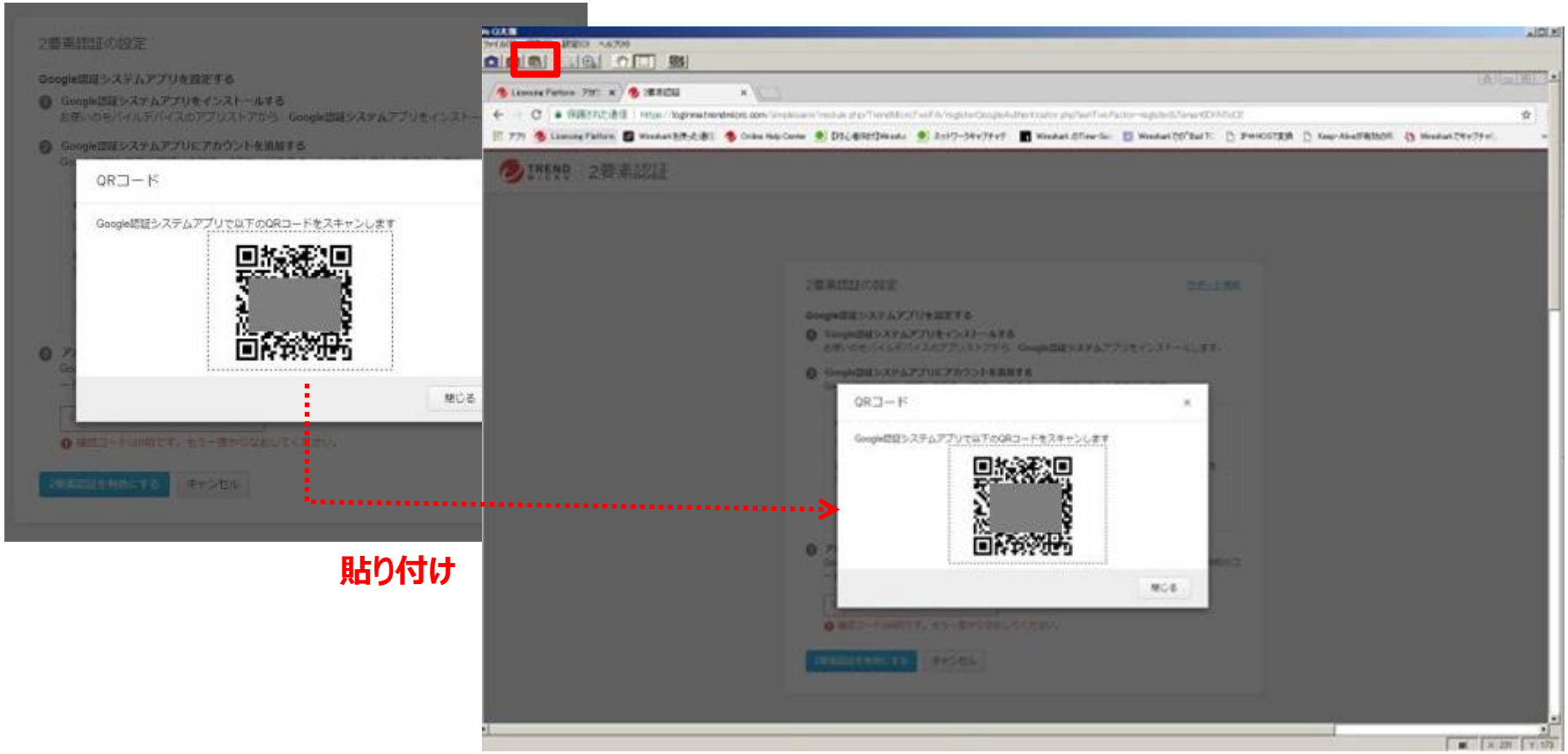
3. 「登録メール確認コード」画面が表示されます。
ご契約時に登録したメールアドレス宛に
下記メールが届きますので、登録メール確認コードを入力し「続行」をクリックします。



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。



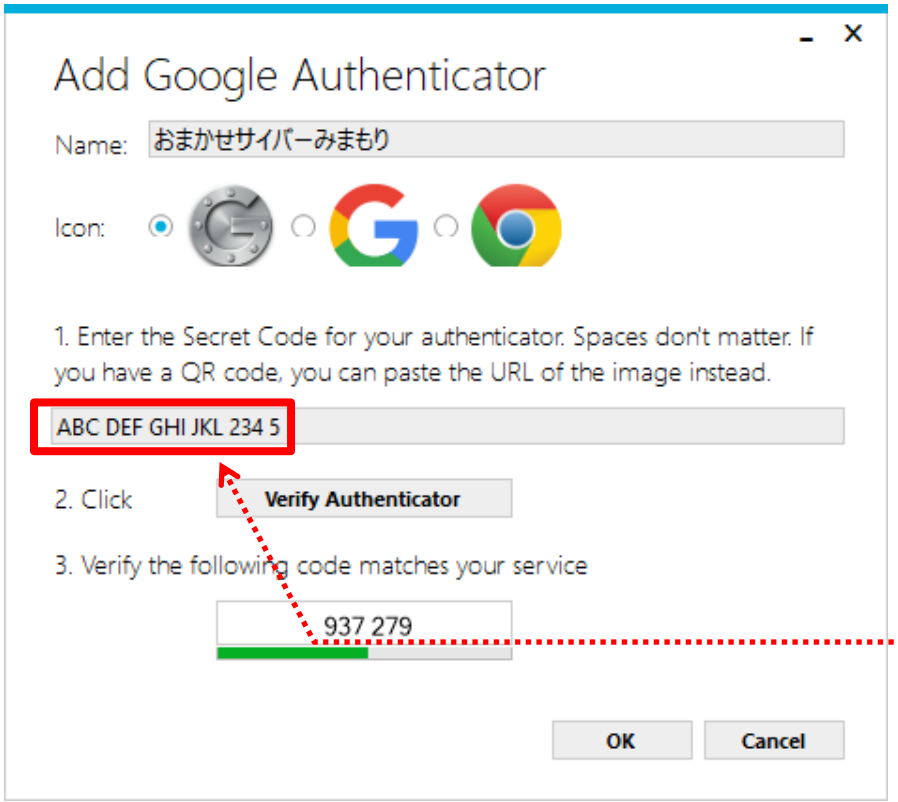
Windowsにおける設定方法　5/9

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。

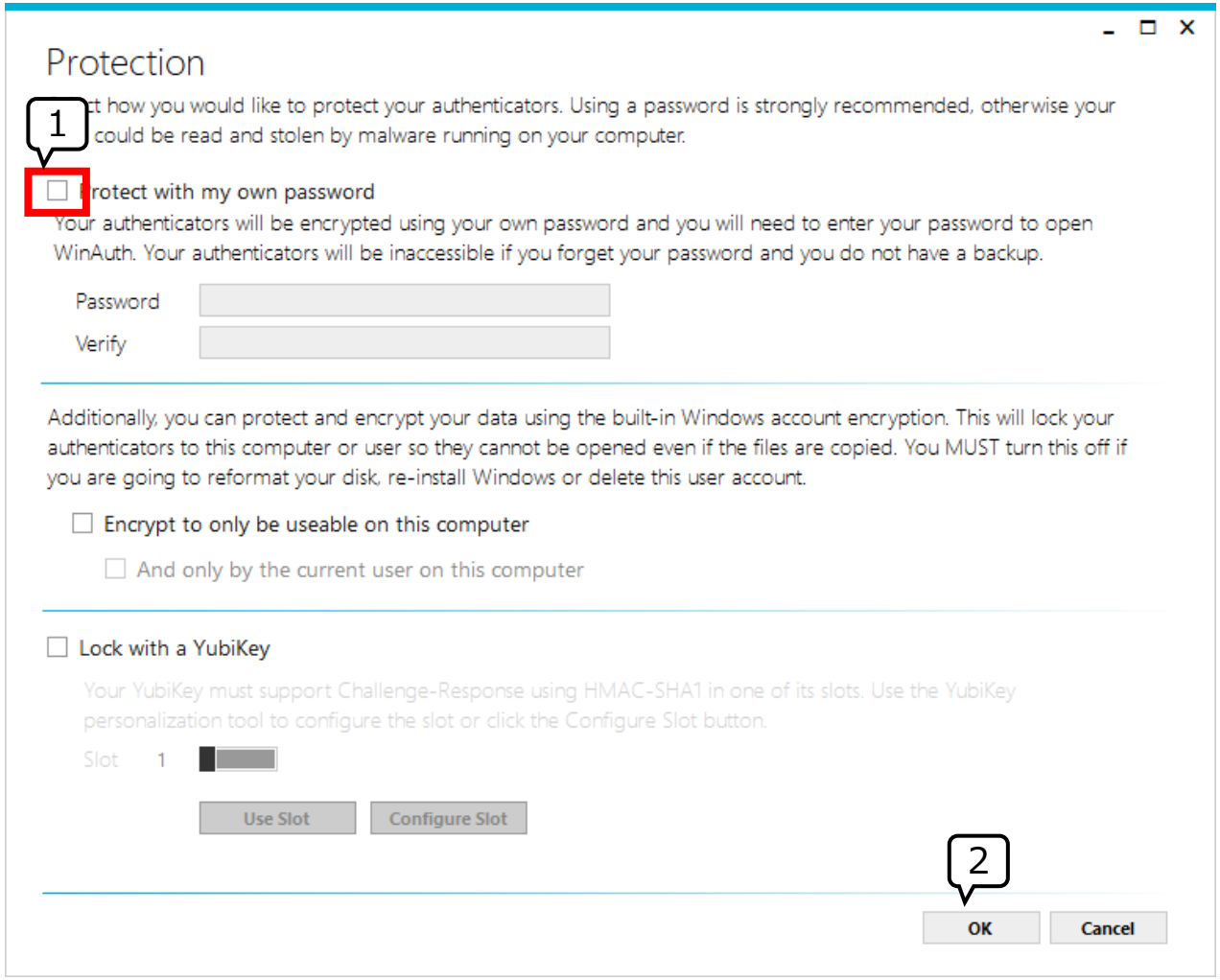
Windowsにおける設定方法　6/9

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。

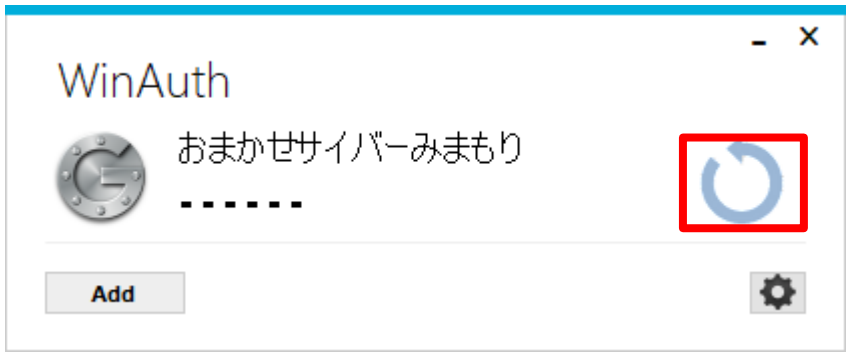


9．Protect with my own passwordのチェックをはずし、「OK」をクリックします。



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桁のコード入力が必要になります。

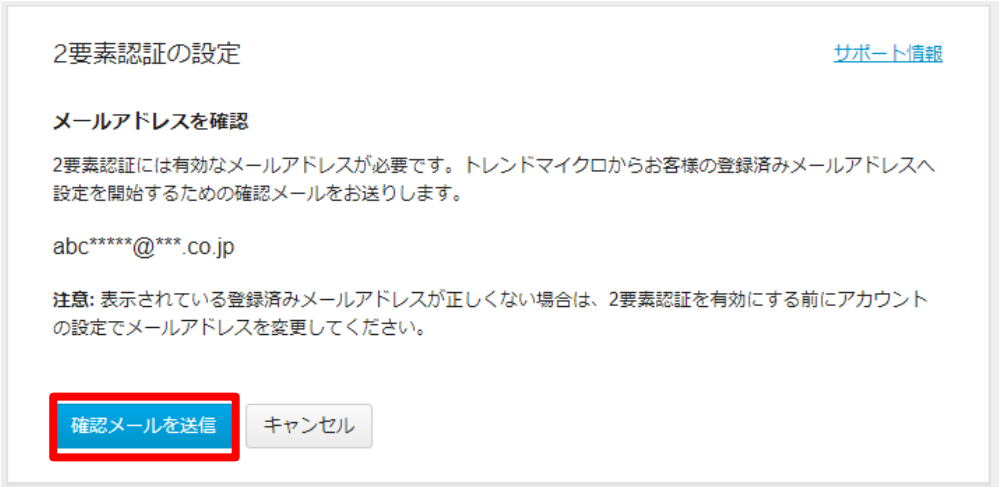
MacOSにおける設定方法　1/8

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

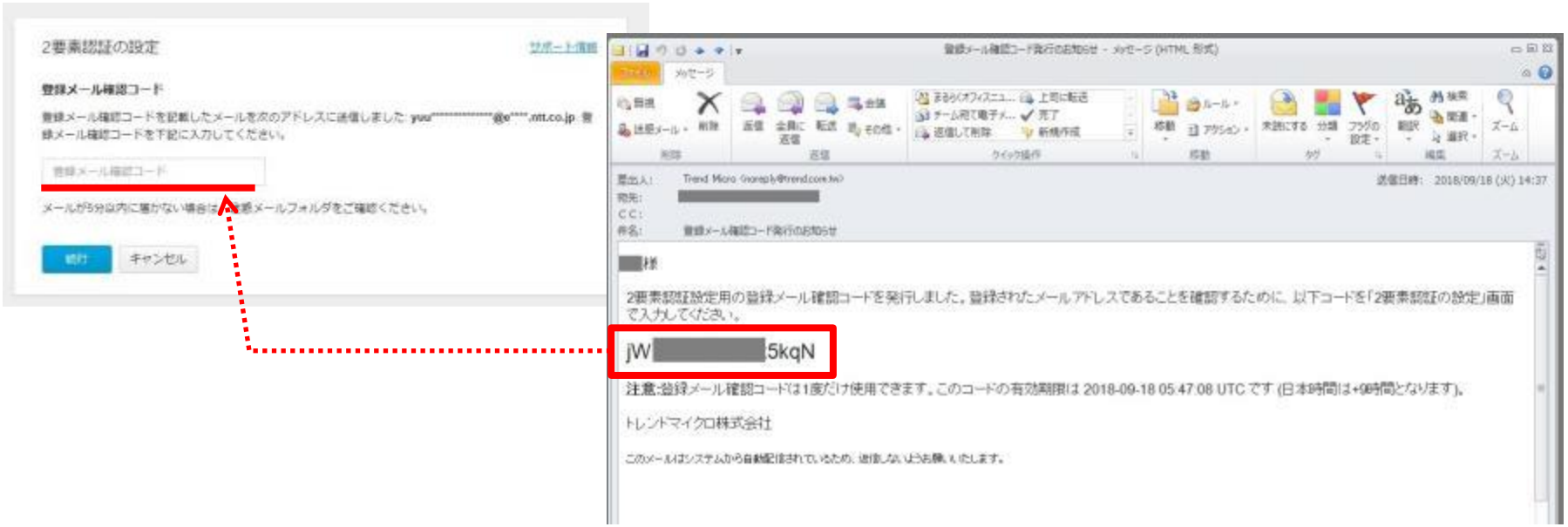
②QR Journal
QRコードの画面キャプチャからコードの情報を読取るためのソフト
※設定の過程のみで必要となります。
　二要素認証の設定完了後はアンインストールしても問題ございません。

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。



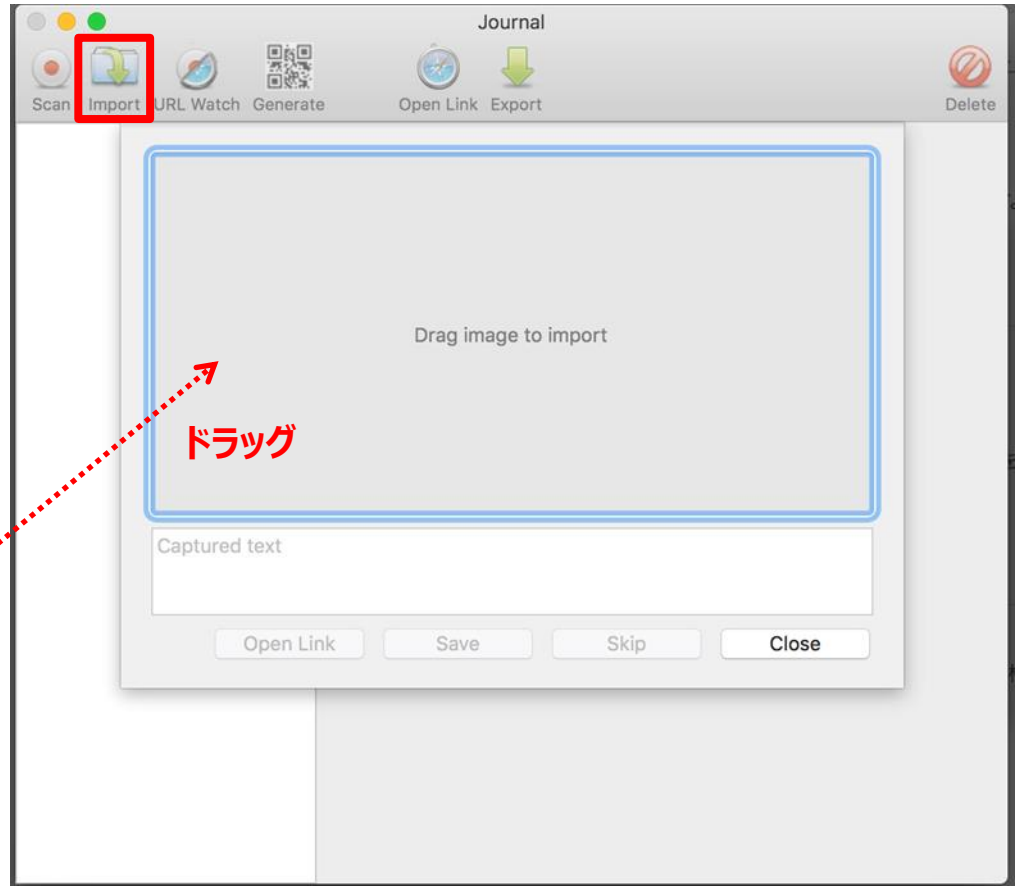
MacOSにおける設定方法　3/8

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。

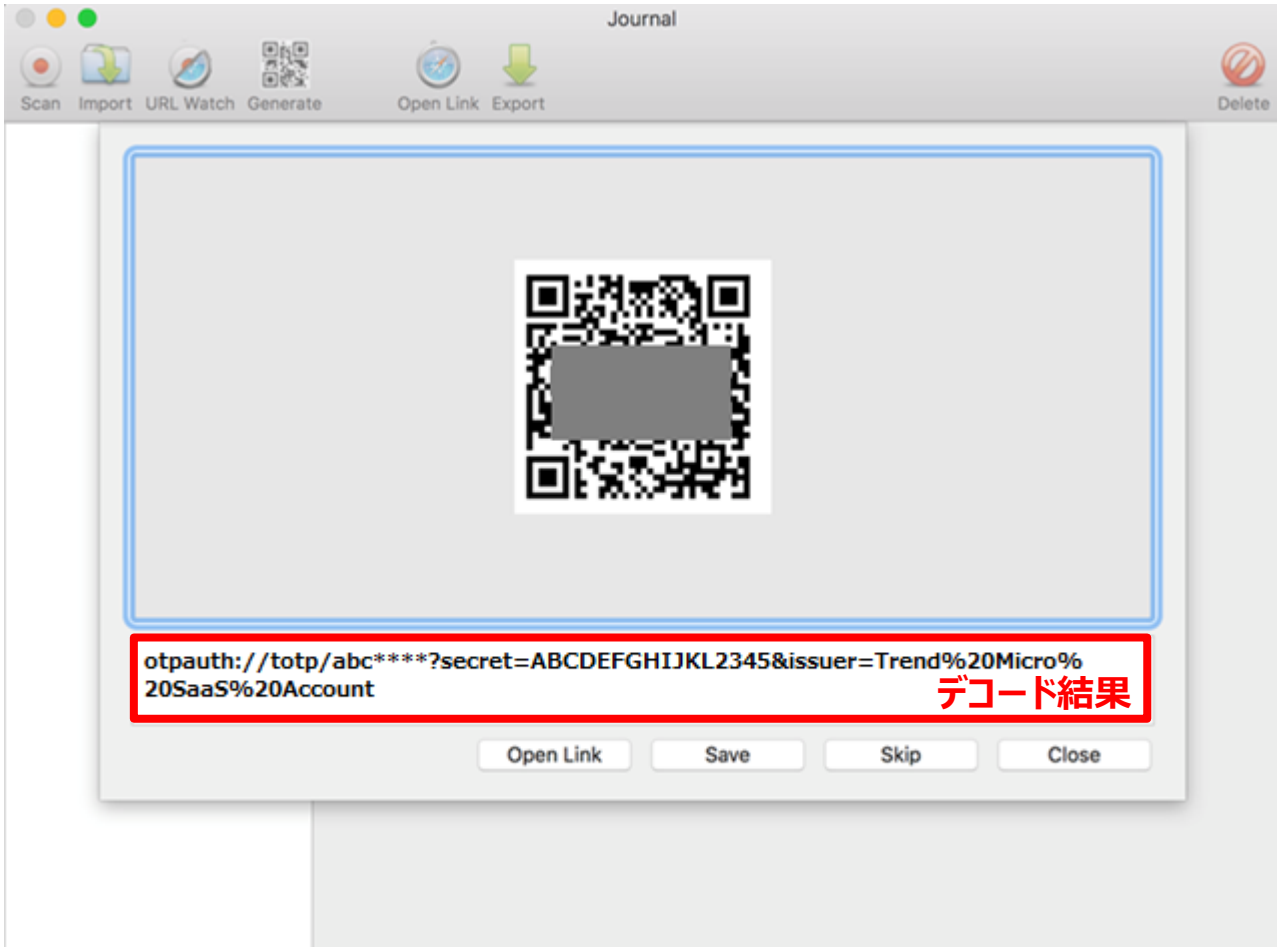
MacOSにおける設定方法　4/8

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



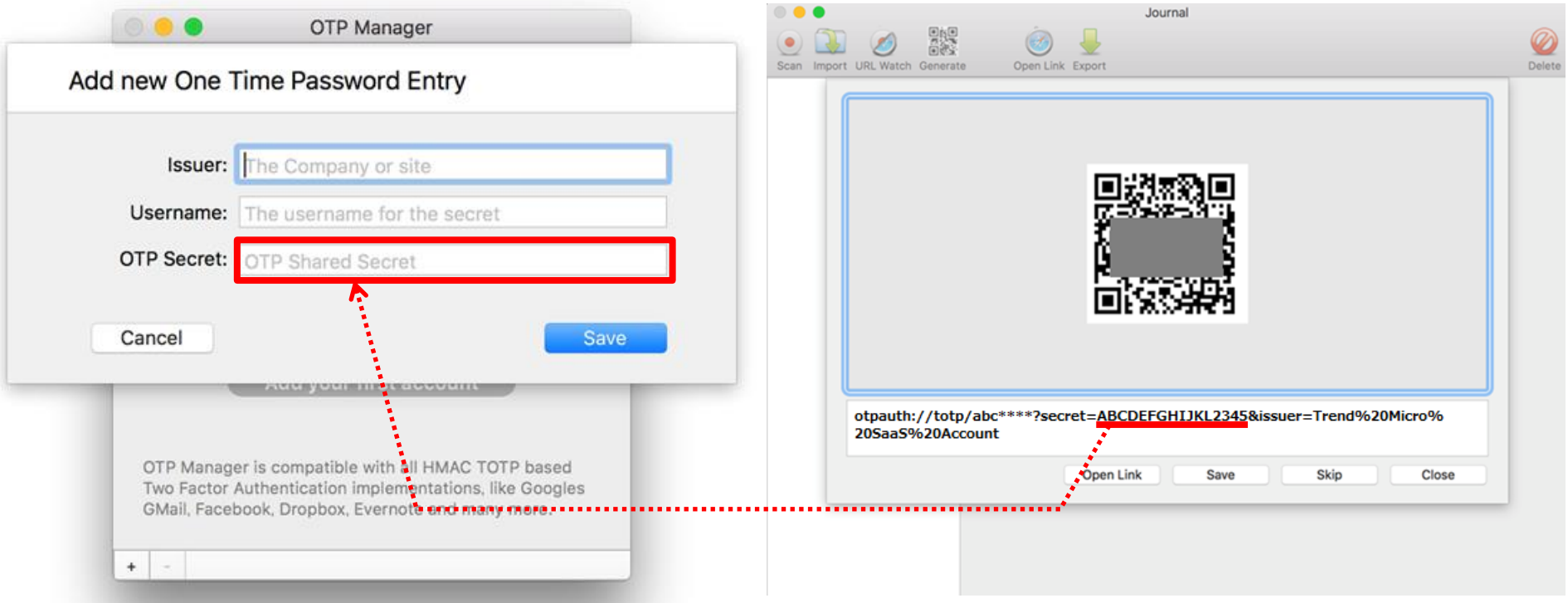
7．QRコードがデコードされます。



MacOSにおける設定方法　6/8

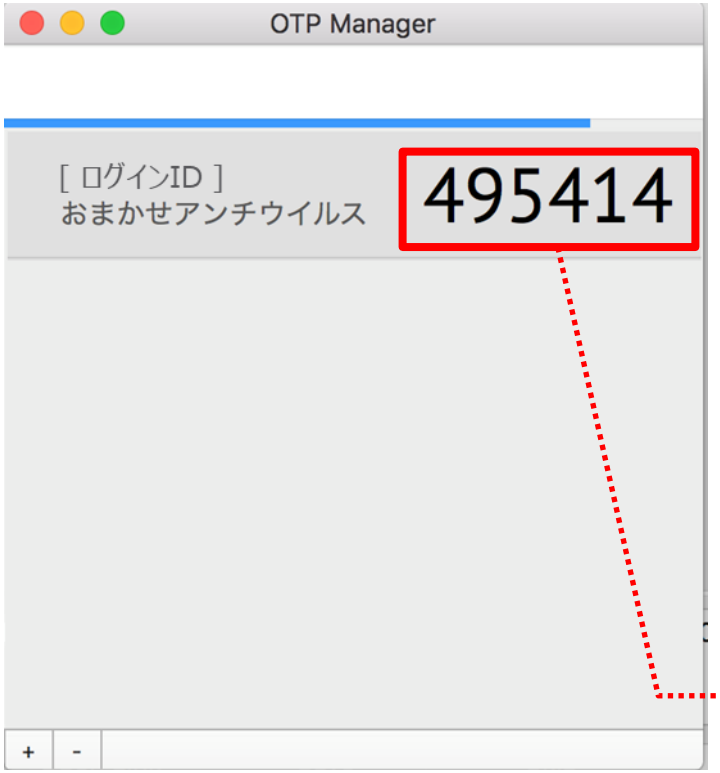
8．OTP Managerを立ち上げて下記を行います。
※App Store＞ [購入済み]をクリックすると、インストールしたOTP Managerを開くことができます。

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。



MacOSにおける設定方法　7/8

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。



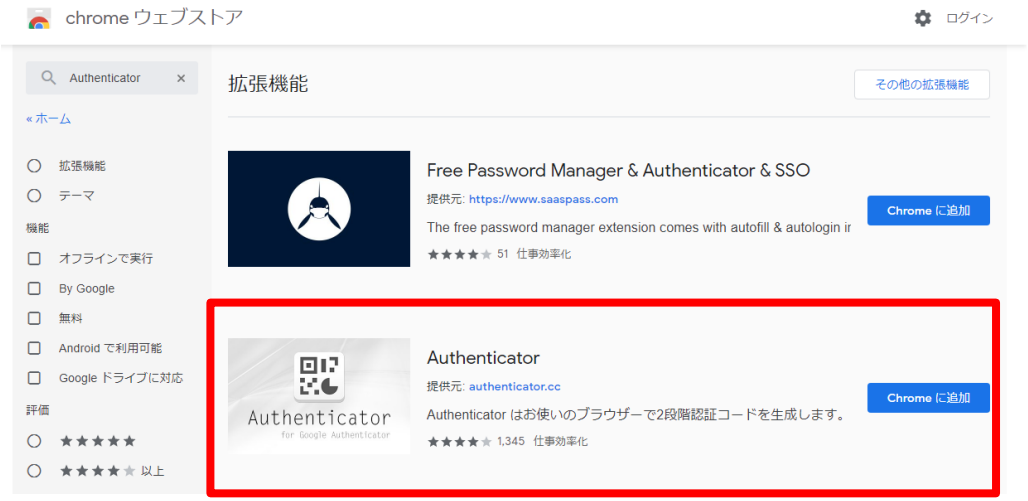
MacOSにおける設定方法　8/8

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。

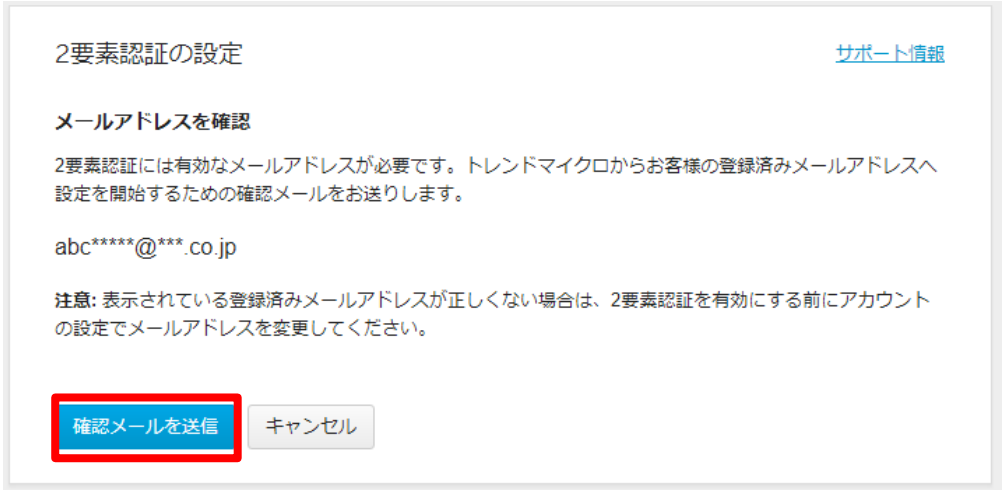
Chromeアドオンを用いた設定方法　1/6

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

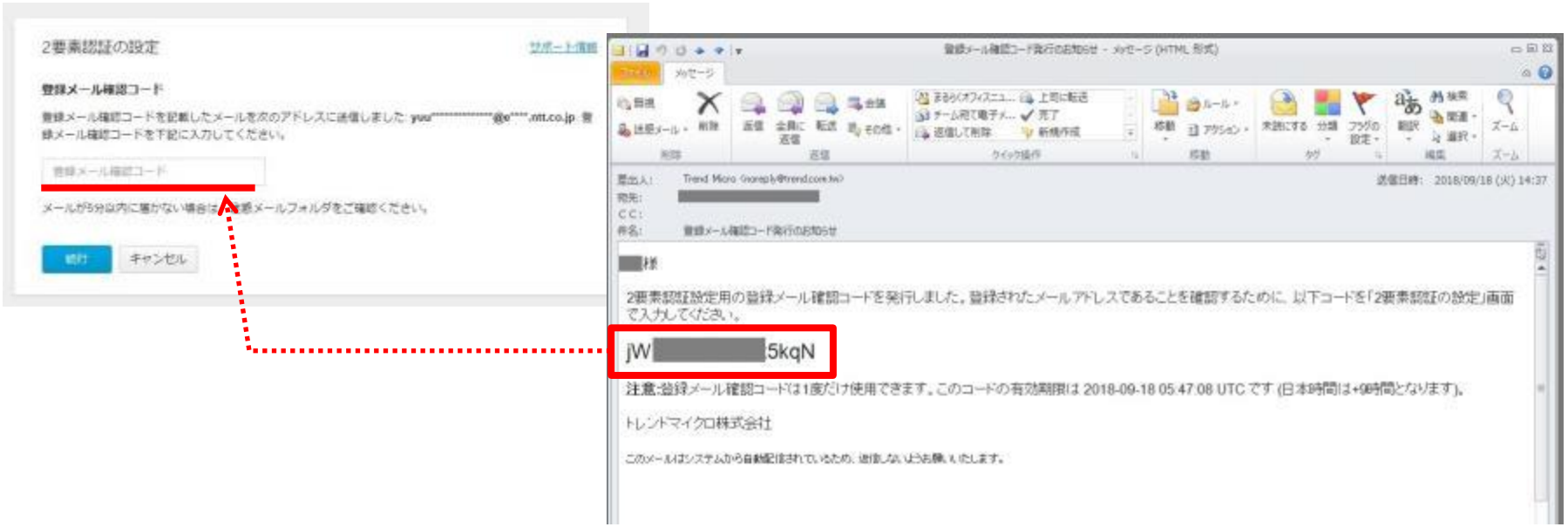


2. 管理コンソールの
   「２要素認証の設定」画面にて、「確認メールを送信」をクリックします。



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。

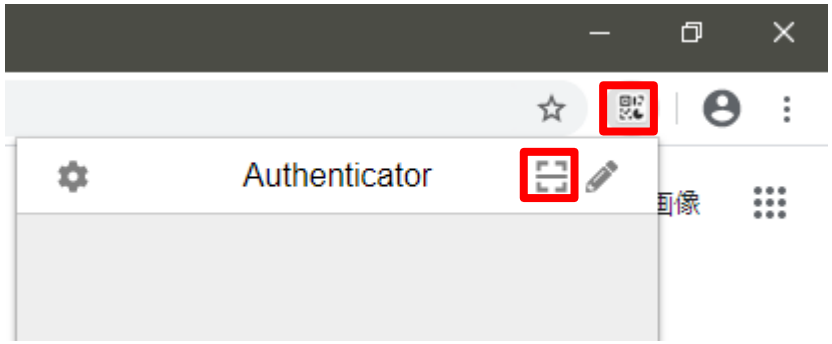


Chromeアドオンを用いた設定方法　3/6

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。

Chromeアドオンを用いた設定方法　4/6

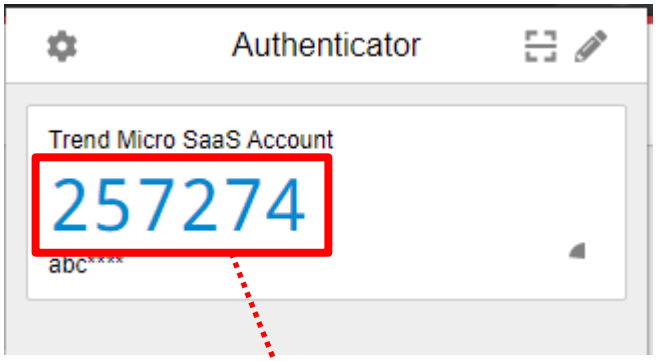
5．Chromeブラウザ右上に表示された「Authenticator」のアイコンをクリックした後、スキャンアイコンをクリックします。



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。



Chromeアドオンを用いた設定方法　6/6

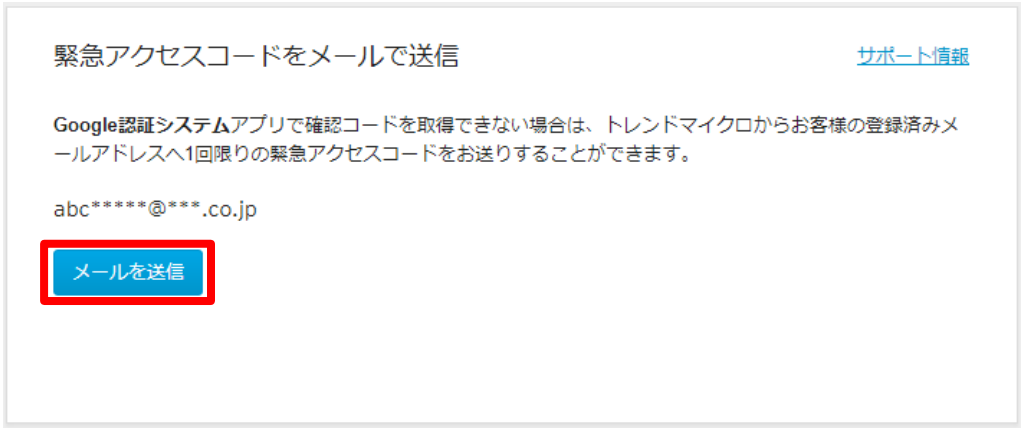
14.　登録が完了すると下記画面が表示されます。
　　次回以降のログインは、「Authenticator」をクリックし、表示される６桁のコード入力が必要になります。

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。

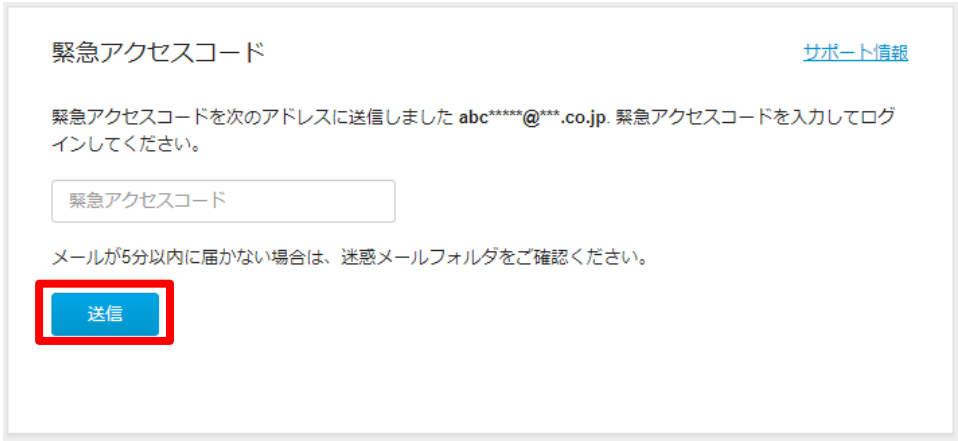
1．　ID/パスワード入力後に二要素認証確認コード入力画面で、「緊急アクセスコードをメールで送信」をクリックします。

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。



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。

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。確認メッセージがでるので「無効にする」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　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。