

## Google 認証ワンタイムパスワードを使って Windows にログイン

2013年12月27日 / カテゴリ: [認証端末](#), [ソリューション](#) / 投稿者: [Igor](#)

### 2-step verification

Keep the bad guys out of your account by using both your password and your phone.



コンピューターまたはユーザー アカウントへのアクセスは、通常、パスワードによって保護されています。しかし、機密性の高いデータを保存している場合、パスワードだけでは十分とは言えません。攻撃を受けた場合に、機密性の高い情報やデータを抜き取られるすきを与えたくはないでしょう。そのため、**Google 認証**と Yubikey HOTP のサポートを [Rohos Logon Key](#) に追加しました。Windows のログインが、TBOTP (タイムベース ワンタイムパスワード) と HOTP (カウンターベース ワンタイム パスワード) コードを使用した高セキュリティ モードで実行されるようになりました。

**Android、iOS、BlackBerry 携帯端末**をお持ちの場合、Google 認証プログラムをご利用下さい。コンピューターを、強力なワンタイム パスワード (OTP) で保護します。ワンタイム パスワード (OTP) とは、特別なデバイスまたはプログラムで生成されたパスワードで、生成された直後の一度限り有効です。このようなパスワードを盗み見したり、キャプチャしたりすることはできません。同じパスワードを再度入力した場合や、指定された有効時間を過ぎてからパスワードを入力した場合には、認証に失敗します。コンピューターにログインする度に、携帯端末からの新しいワンタイム パスワード (OTP) が要求されます。

Rohos Logon Key プログラムに統合された Google 認証が、あなたの PC のログイン用のキーになります。携帯端末の中に、いつも秘密のキーを持ち歩いているようなものです。Windows パスワードを手動で入力する必要はなく、プログラムが代わりにやってくれます。便利かつ信頼できます。OTP トークンも他の種類のキーと併用することができます。つまり、OTP トークンとフラッシュ ドライブの両方を設定し、その時に応じて使用するものを選択できます。

## Google 認証アプリケーションを使用して、PC にログインする方法

Android 携帯端末を例に、Google 認証アプリケーションのワンタイムパスワードを使用して Rohos Logon Key for Windows を設定する方法を紹介します。

2020 Copyright Tesline-Service SRL All rights reserved.

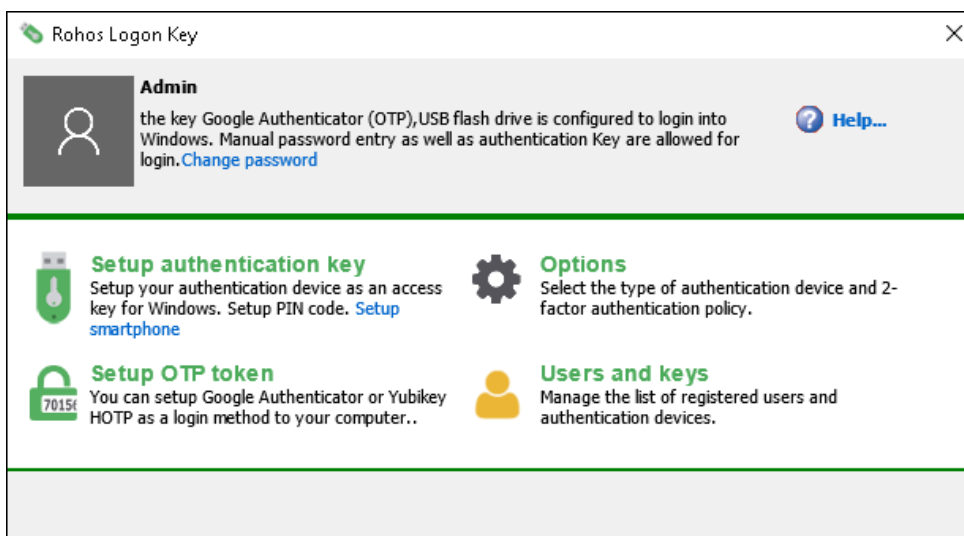
翻訳: 株式会社ネクステッジテクノロジー

[www.shareEDGE.com](http://www.shareEDGE.com)

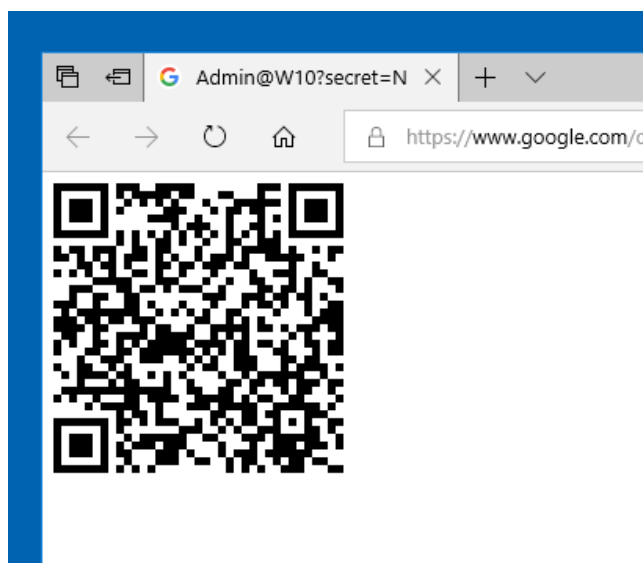
1. **Google 認証**アプリケーションが携帯端末にインストールされていることを確認します（QRコード スキャンのために、Google Lens や Barcode Scanner も追加でインストールする必要があるかもしれません）。

2. アプリケーションが携帯端末にインストールされていることが確認できたら、PC での Rohos Logon Key の設定を始められます。

- 最新版の Rohos Logon Key v3.4 for Windows をインストールします。
- Rohos Logon を開き、**[OTP トークンの設定]**をクリックします。



- **[Google 認証]**を選択し、**[QRコードを表示]**をクリックします。



携帯端末で Google 認証を起動し、QRコードをスキャンします。そのために、PCモニターに表示されている QRコードを携帯端末でスキャンできる位置に持っていきます。

- オプションとして、Windows のパスワードを入力することができます。入力した場合、Windows ログインとパスワードが OTP コードだけで行えます。状況によっては、セキュリティ面で弱くなってしまうことがあります。

2020 Copyright Tesline-Service SRL All rights reserved.

翻訳: 株式会社ネクステッジテクノロジー

www.shareEDGE.com

パスワード欄を空欄のままにした場合、Windows ログインには、ユーザー名、パスワード、ワンタイムパスワード（OTP）全てが必要です。

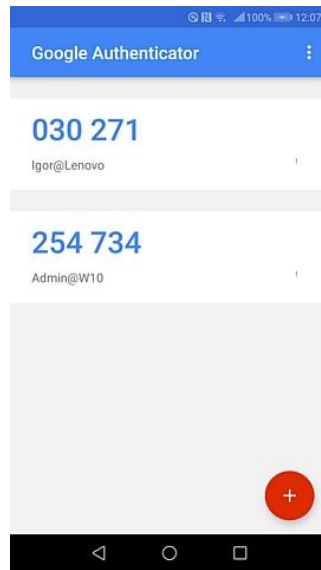
- **[OTP ログインを有効にする]**ボタンをクリックします。

設定完了です!この時点から、携帯端末が Windows PC のアクセスキーとしての役割を果たすことになります。

つまり、Google OTP を統合した携帯端末が、Windows PC のログインやロック解除のためのデジタルキーのような働きをするということです。



Google 認証は、それぞれの PC にコンピューター名を割り当て、Rohos Logon プログラムの名前を登録します。それゆえ、一つの携帯端末を複数の PC（会社のPC、ノートパソコン、その他のPC）用保護キーとして使用することができます。



右のスマートフォン画面のスクリーンショットを見ると、Google 認証が、2台の PC のログイン用に設定されていることがわかります。混乱を避けるため、それぞれの PC の名前は、ワンタイム パスワードの下に表示されます。ワンタイム パスワードの右側には、パスワード入力有効時間の 30秒タイマーが表示されます。30秒経過後は、新しいパスワードが生成されます。

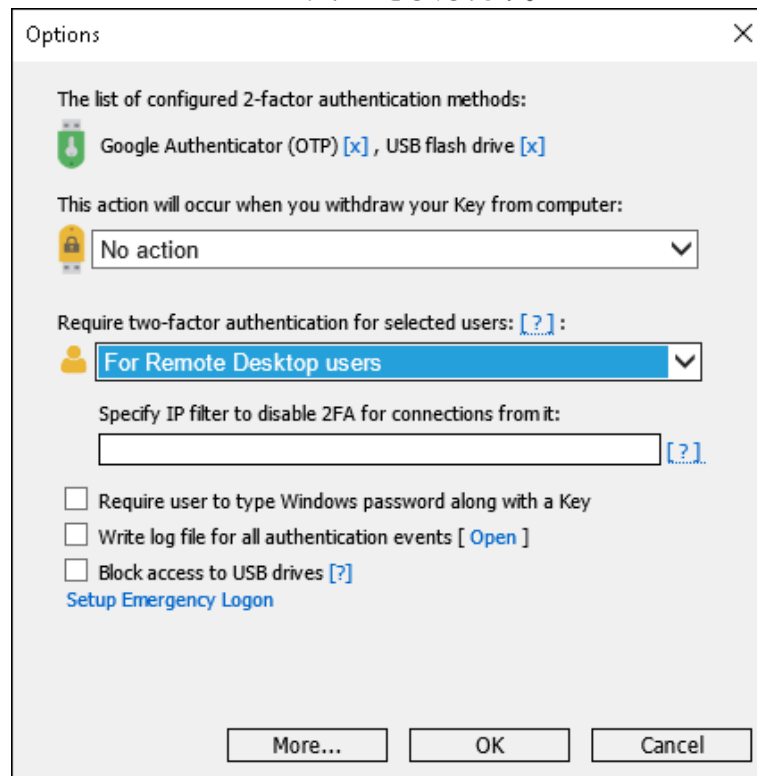
### 3.強力な二要素認証をより強力に

Windows へのログインは、従来の Windows パスワードを使用した方法と、Rohos Logon Key アイコンを使用した方法（Google 認証の OTP コード）どちらからでも行うことができます。

Windows 認証をより強力で安全なものにするためには、Rohos の二要素認証を有効にする必要があります。

Rohos Logon Key を開き、[オプション]メニューを選択後、一覧から、**[指定ユーザーには二要素認証を要求]**を選択します。これにより、指定したすべてのユーザーに対して、強化された二要素認証が要求されます。

そのため、ログイン時には、ワンタイム パスワードと Windows パスワードの両方が要求されます。パスワードだけではログインできなくなります。



4.[すべてのユーザー]を選択した場合、[緊急ログオン]オプションの設定を忘れずに行ってください。設定を行うことにより、携帯端末が利用できない場合でも、Windows PC にアクセスできます。

Windows の二要素認証を使用することをお勧めします。Windows 認証ボックスでの 2段階認証の場合、ワンタイムパスワード (OTP) と Windows パスワードの両方の入力が要求されます。二要素認証でのログインは、二重に保護することで、あなたのデータにアクセスする必要のない人がデータにアクセスできないようにします。頭の回転が速く、テクノロジーに関する知識が豊富な子供たちが、あなたの個人情報を勝手に操作することのないようにします。

**注意:** Google 認証を設定後は、携帯端末を忘れずに持って出かけてください。携帯端末が手元がない場合、Rohos Logon Key の緊急ログオン機能からのログインしかできなくなります。コンピューターがセーフ モードで起動されている場合でも、ワンタイム パスワード (OTP) が要求されます。これにより、コンピューターがハッキングされることを防ぐことができます。

## Yubikey HOTP 設定を使用して Windows ログインを行う方法

2020 Copyright Iesline-Service SRL All rights reserved.

翻訳: 株式会社ネクステッジテクノロジー

www.shareEDGE.com

無料 configuration slot のある Yubikey 2.0 と Yubikey Personalization Tool が必要です。

まず、Rohos Logon Key の設定を次のように行ないます。

**[オプション]**メニューから、[Google authenticator (OATH)]を選択します。

Setup OTP token

You can setup Google Authenticator or Yubikey HOTP as a login method to your computer. In order to log into Windows you will need to enter OTP or OTP + Password.

User: **Admin**, [Select user...](#)

Setup the type of OTP authentication:

Google Authenticator TOTP [Display QR code](#), [Copy code](#)

Yubikey HOTP [Copy secret key](#)

By Email or SMS :

Token secret key:

OTP refresh time:

Please enter the user Windows password (optional) :

[View the log of created users...](#)  
[OTP Settings...](#)

1. Rohos を開き、**[OTP トークンの設定]**を選択します。

Google Authenticator と Yubikey が既に PC にインストールされている場合、**[OTP ログインを無効にする]**をクリックします。

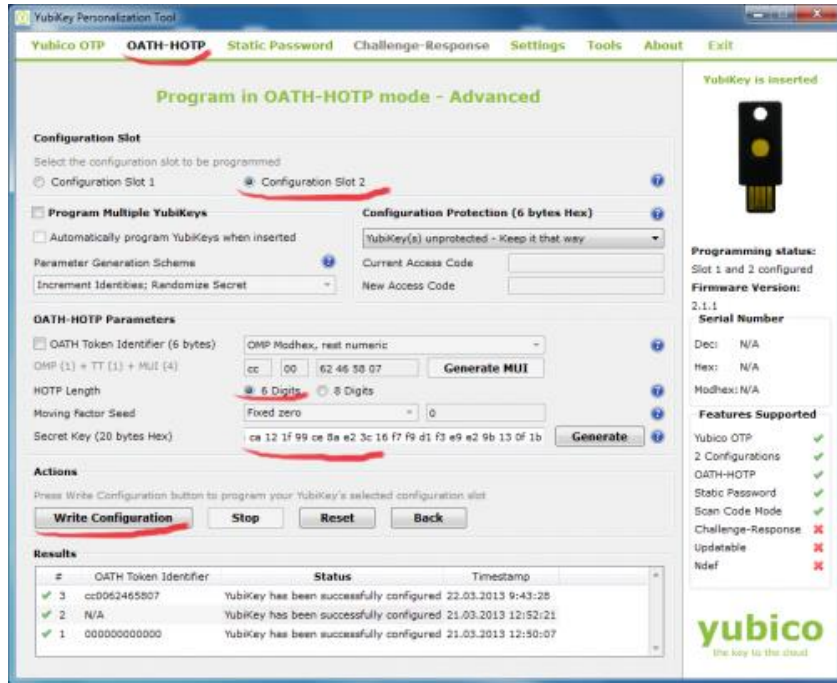
2. [Yubikey HOTP]を選択し、**[秘密キーをコピー]**をクリックすると、クリップボードに 20 バイトの 16進法文字列がコピーされます。コピーした秘密キーは、後程 Yubikey Personalization Tool で使用します。

3. [OTP ログインを有効にする]をクリックします。

Yubikey に HOTP 設定のセットアップを行います。

### **Yubikey second slot (HOTP) の設定に Yubikey Personalization Tool を使用**

Yubikey を PC に挿入し、Yubikey Personalization Tool を開きます。



1. [OATH - HOTP]メニューの[Advanced (詳細)]ボタンをクリックします。
2. 無料の Configuration Slot を選択します。デフォルトでは、slot 2 が無料です。
3. [HOTP Length]が 6 に設定されていることを確認します。
4. [OATH token Identifier]オプションのチェックをはずします。
5. [Secret Key]欄に、コピーした秘密のキーをクリップボードから貼り付けます (Ctrl+A and Ctrl+Vキーを使用)。  
20文字のキーが貼り付けられない場合は、Rohos Logon Key を起動し、[USBキーの設定]ダイアログボックスで再度コピーします。
6. [Write Configuration]をクリックします。

ここまでの設定で、YubiKey slot 2 が、Windows ログインに使用する準備ができました。PC を再起動し、ようこそ画面で Rohos Logon Key を選択します。カーソルを OTP フィールドに移動させ、Yubikey を長押しします。

Rohos Logon Key は HOTP コード、OATH 認識子あり/なしどちらにも対応しています。

cc0062465807101069 または

101069

最後の6桁が認証されます。



## OTP コードを SMS/メールで携帯端末に送信

Rohos Logon Key は、Remote Desktop ユーザーに対して、自動二要素認証の利用を可能にします。Remote Desktop ログイン時に、Rohos は自動で、OTP コードをユーザーの電話番号への SMS、またはメールで送ります。

ターミナル サーバーが次の条件を満たしている必要があります。

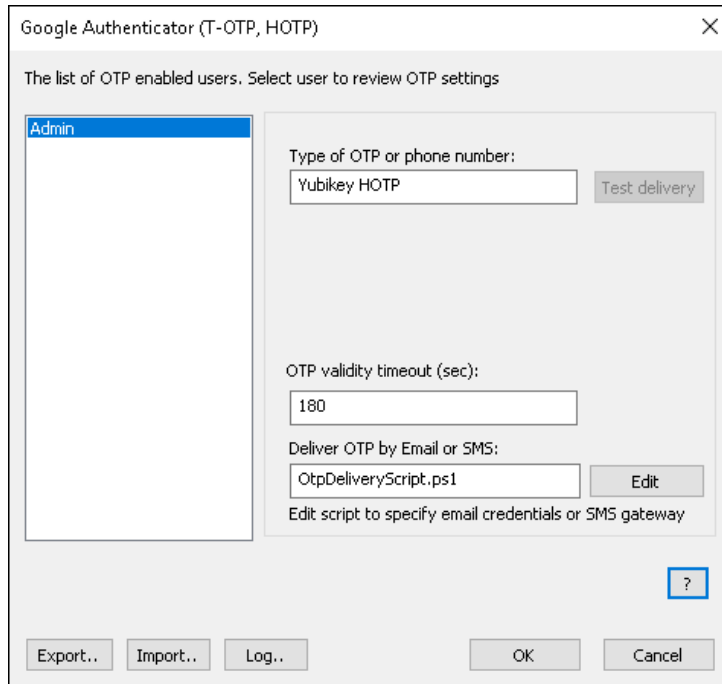
- 電話/携帯番号の欄にユーザーの携帯電話番号が入力されている、またはメールアドレス欄が入力されていること
- Rohos Logon Key が SMS ゲートウェイ サービスまたはメール情報によって設定されていること

### SMS ゲートウェイまたは他の OTP 送信方法を設定

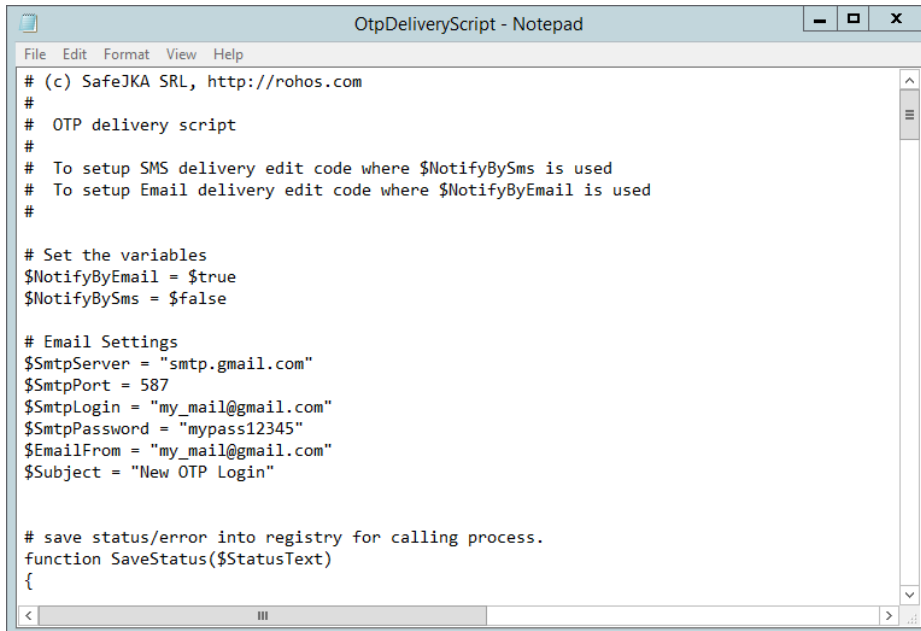
必要要件:

1. PowerShell v.3 以上 (Windows 2012 R2 以上);  
または Windows 2008 ([アップデート含む](#))
2. スクリプト実行ポリシーが有効になっている。  
有効にするには、PowerShell ISE (x86)で [Set-ExecutionPolicy -ExecutionPolicy RemoteSigned]コマンドを実行します。PowerShell と PowerShell (x86) の両方を管理者権限で実行し、[スクリーンショットに表示](#)されるコマンドを実行します。
3. SMS メッセージ送信のための サードパーティ SMS ゲートウェイ ¥ 送信サービス (HTTP API)

Rohos Logon Key を開き、[OTP トークンの設定]から[OTP 設定...]を選択します。



1. [編集]をクリックし、OtpDeliveryScript.ps1 ファイルを開き、メールオプションを編集します。メールオプションには、smtp サーバー、送信用アドレスのメールアドレスとパスワードの情報等が含まれます。



SMS 送信の設定には、以下の文字列を使用します。

```
$SmsGatewayUrl = "https://api.clickatell.com/http/sendmsg?api_id=xxxx&user=xxxx&password=xxxx
&to=${$AdUserName.telephoneNumber}&text=${$SmsNotificationText}"
```

2020 Copyright Tesline-Service SRL All rights reserved.

翻訳: 株式会社ネクステッジテクノロジー

www.shareEDGE.com

xxxx URL パラメーターが SMS プロバイダー HTTP API URLになる用にカスタマイズします;

`$(($AdUserName.telephoneNumber)` と `$(($AdUserName.telephoneNumber)` は両方共スクリプト変数なので、さわる必要はありません。

#### 一般的な SMS 送信サービスの一例:

```
$SmsGatewayUrl = "https://api.clickatell.com/http/sendmsg?api_id=xxxx&user=xxxx&password=xxxx  
&to=$(($AdUserName.telephoneNumber)&text=$(($SmsNotificationText))"
```

```
$SmsGatewayUrl = "https://api-mapper.clicksend.com/http/v2/send.php?method=http&username=x  
xxx&key=xxxx&to=$(($AdUserName.mobile)&message=$(($SmsNotificationText))"
```

左側の一覧からユーザーを選択、または電話番号またはメールアドレスを入力して、[テスト送信]ボタンをクリックすると、OTP コードを指定した方法で送信できます。注意:OTP コードの送信に gmail を使用する場合、gmail の設定で、[安全性の低いアプリを許可する]をオンにする必要があります。

<https://support.google.com/accounts/answer/6010255?hl=ja>

#### OTP 送信方法 (メール) の設定に関する詳細

Remote Desktop ログインの SMS 認証を有効にする:



## Google 認証を使用して Windows にログインする利点

- 二要素認証を使用した、より安全性の高い Windows 認証  
Windows パスワードと 携帯端末の両方をログイン時に要求

2020 Copyright Tesline-Service SRL All rights reserved.

翻訳: 株式会社ネクステッジテクノロジー

[www.shareEDGE.com](http://www.shareEDGE.com)

- YubiKey または OTP (SMS 送信) は、ドライバーやソフトウェアが新たに必要になることはありません。
- Google 認証の場合、コンピューターに接続する必要がないので USBポート不要
- Google 認証、YubiKey、もしくは携帯端末のみを使用したログイン、いずれかまたは組み合わせて使用が可能
- ネットワーク管理者が通常のパスワードのみを使用してログイン可能
- 安全な二要素認証で Windows Remote Desktop へのログインでありながら、ユーザーの一覧、グループ メンバー、リモートデスクトップ接続ユーザーのみなど、柔軟な認証方針

### Rohos Logon Key をダウンロード

このアップデートは、Rohos Logon Key 登録ユーザーであれば無料で利用できます。April v.3.0 アップデートより有料となります。

**タグ:** [Android 携帯端末をキーとして使用](#)、[Google 認証](#)、[Rohos Logon Key](#)、[二要素認証](#)、[Windows 8](#)