GMO トラスト・ログイン

第３回

ワンタイムパスワード

前回は多要素認証の種類やメソッド（認証方式）について説明しました。非常にたくさんメソッドがあるので驚いたのではないでしょうか。今回はメソッドの中で一番ポピュラーな「ワンタイムパスワード」について解説します。

ワンタイムパスワードとは

「ワンタイムパスワード」とは定期的に更新される特定のアルゴリズム（規則）に基づいて生成されるパスワードを使用して認証を行うシステムです。このパスワードは一度きりしか使えないため「使い捨てパスワード」と呼ばれることもあります。ワンタイムパスワードを使用する場合、パスワードを生成しユーザに表示するためのデバイスが必要となります。このデバイスは「トークン」または「セキュリティトークン」と呼ばれています。

ユーザがワンタイムパスワードをハッカーに盗まれてしまった場合でも、盗まれたパスワードと同じパスワードは二度と使用できないため、ハッカーはシステムへアクセスすることはできません。

ワンタイムパスワードを他のメソッドと比べたときのメリットはリーダーデバイスが不要なため使用する端末を選びません。リーダーデバイスのコストも発生しません。PC とモバイルの両方でシステムへアクセスしたい場合に非常に有効です。デメリットとしてはトークンを忘れてしまうとシステムへアクセスできなくなります。また、紛失してしまった場合はトークンの入手と再度初期登録が必要となります。

ワンタイムパスワードの特徴

メリット	デメリット
リーダーデバイス不要 比較的安価に導入可能	トークンを忘れるとアクセス不可 紛失時に再度トークン入手と登録

次のページからトークンの種類、ワンタイムパスワードのアルゴリズム、ユーザのデバイスを使用したワンタイムパスワードについてご説明いたします。

ワンタイムパスワードのさまざまなトークン

ワンタイムパスワードのトークンには主に次の種類があります。

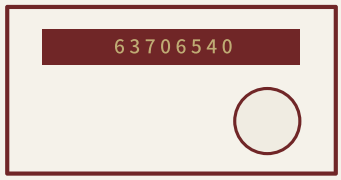
1. ハードウェアトークン

ハードウェアトークンは生成されたワンタイムパスワードを表示するディスプレイを持った小型の電子機器です。ハードウェアトークンには「キーホルダー型」、「カード型」、「電卓型」といった形状で持ち運びが容易に設計されています。

ハードウェアトークンには電子機器内部にワンタイムパスワードを生成するアルゴリズムがチップとして搭載されています。導入時には初期費用としてトークンの購入費用が発生します。一般的に電池が切れると使用できなくなります。

キーホルダー型

カード型



電卓型

2. ソフトウェアトークン

ソフトウェアトークンはアプリケーションとして実装されたワンタイムパスワードを生成するプログラムです。主にスマートフォン用アプリケーションとして提供されています。このアプリケーションをスマートフォンにインストールし認証サーバに登録することで、アプリケーションがアルゴリズムに従って計算したワンタイムパスワードを表示し使用することができるようになります。

スマートフォンアプリの認証サーバへの登録はアプリを起動し PC 等のブラウザで各ユーザの登録用 Web サイトへアクセスします。登録ページに表示される QR コードをスマートフォンのカメラで読み取ることで登録が完了します。
ユーザはセルフサービスで登録する必要があります。電池切れ等の心配がないため、スマートフォンが使用できる限りワンタイムパスワードも使用可能です。常に携帯しているスマートフォンを使用するため忘れるリスクは低いものとなります。（スマートフォン自体を忘れると使用できませんが）

スマートフォンを紛失もしくは、買い替える場合はアプリケーションのインストールと認証サーバへの再登録作業が必要となります。使用するスマートフォンの OS バージョンにアプリケーションが対応していないと使用できないため、OS のアップデート時は注意が必要です。

ワンタイムパスワードのさまざまなトークン

ハードウェアトークンとソフトウェアトークンの特徴

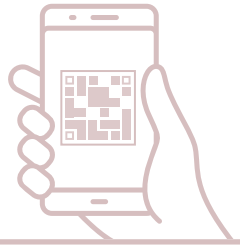
トークンの種類	提供方法	コスト
	注意事項	
ハードウェア	キーホルダー型 カード型	×
	紛失時および電池切れ時は再購入必要	
ソフトウェア	スマートフォンへ アプリをインストール	○
	スマートフォン機種変更時、再インストールと再登録必要 スマートフォン OS のバージョンに対応している必要あり	

スマートフォンアプリケーション使用時の登録手順

1 スマートフォンへアプリインストール

2 PC のブラウザで登録ページへアクセス

3 ブラウザに表示される QR コードを読み取る

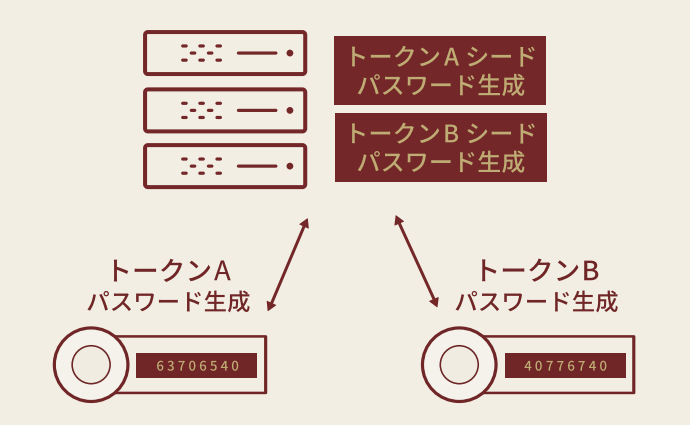


4 登録完了。ワンタイムパスワード表示

ワンタイムパスワード使用時の構成

ワンタイムパスワードを使用する場合、認証サーバでワンタイムパスワードを計算する仕組みと、利用者のトークンでワンタイムパスワードを計算する仕組みが必要となります。この計算アルゴリズムが認証サーバとトークンで同じものを使用することで計算結果となるパスワードが一致しているかどうか比較されます。

各トークンにはシードと呼ばれる固有の値が割り当てられ、シードをアルゴリズムに従って計算させトークン毎にワンタイムパスワードを生成しています。サーバではすべての登録されているトークンのパスワードを生成しています。



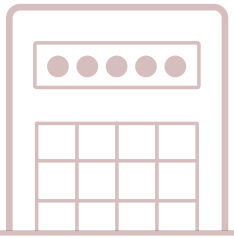
ワンタイムパスワードを使った多要素認証の使用例

ワンタイムパスワードを使用する多要素認証のシステムでは、一般的に次のようなフローで認証を行います。トークンに表示されるパスワードは定期的に更新されてしまうので入力を間違えないように行います。

1 ワンタイムパスワードを
使用する認証ページへアクセスする

2 ユーザ ID・パスワードを使用して
一段階目の認証を実施する

3 トークンに表示される
ワンタイムパスワードを入力する



4 ログイン完了

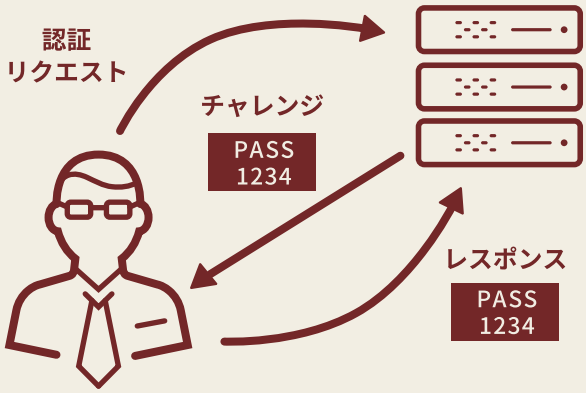
パスワード生成のアルゴリズム

ワンタイムパスワードを生成するアルゴリズムには主に次のようなものがあります。

時刻同期型

現在の時刻と各トークンのシード値を元にパスワードを計算させ生成します。同じ時刻に同じパスワードを生成する必要があるため、トークンと認証サーバで時刻が同期している必要があります。通常は 30 秒毎にパスワードを再生成します。そのため、トークンに表示されるパスワードが更新される前に認証を完了させる必要があります。

チャレンジ・レスポンス型



チャレンジ・レスポンス型のトークンには数字が入力できるように電卓のようなキーがあります。使用者が認証ページにアクセスすると、認証サーバから「チャレンジ」と呼ばれる値が表示されます、この値をトークンのキーで入力するとトークンがワンタイムパスワードを生成して表示します。認証サーバ側でも同様に同じチャレンジからパスワードを生成し比較します。

生成回数型

生成回数型はこれまで使用したワンタイムパスワードの回数によってパスワードを変化させる方式です。この回数をカウンターと呼びます。各トークンのシードの値とカウンターの値によりパスワードが生成されます。回数型のトークンにはパスワードを生成させるためのボタンがあり、生成ボタンを押すとカウンターが繰り上がります。認証サーバでも認証のたびにカウンターを繰り上げていきます。
トークン上でパスワード生成を実施し、そのパスワードで認証処理を行わなかった場合トークンと認証サーバでカウンターがずれてしまうことが発生します。この場合カウンターを同期させることが必要となり、カウンター同期の手順を実行します。

その他のワンタイムパスワード

認証サーバとトークンでそれぞれ生成する仕組みの他に、認証サーバが一時的なパスワードを生成しユーザが持っているデバイスへ直接送信するものがあります。これは厳密にはワンタイムパスワードとは違う仕組みですが広義でワンタイムパスワードの一種とみなされることがあります。これらのパスワードは特定の時間で使えなくなります。再度ログインを行うときには、異なるパスワードが送信されます。
直接送信する仕組みには次のようなものがあります。

SMS
（ショートメッセージサービス）

SMS メッセージとしてユーザの携帯電話へ送信する

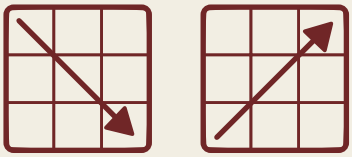
E-mail

E-mail アドレスへ送信する

ボイスコール

ユーザの携帯電話へコールしワンタイムパスワードを音声で読み上げる。

マトリックス認証



碁盤目状のマスが表示され、毎ログイン時に各マスに異なる値が表示される。ユーザは事前に決めた複数のマスとその並び順を指定する。ログイン時には指定したマスに表示された値を順番に入力する。

ワンタイムパスワードのトークンにはハードウェアトークンとソフトウェアトークンがあり、
ワンタイムパスワード生成のアルゴリズムも複数あるため
実際の導入には運用方法および導入コストを比較検討する必要があります。
導入が比較的手軽でセキュリティレベルを高められる多要素認証メソッドが
ワンタイムパスワードと言えるでしょう。