GMO トラスト・ログイン

第 5 回

マトリックス認証、PKI 認証、IC カード認証

前回は「生体認証」、「次世代認証 FIDO」メソッドについて解説しました。今回は「マトリックス認証」、「PKI 認証」、「IC カード（スマートカード）認証」について解説いたします。

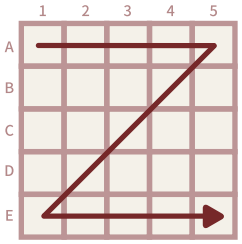
まだある認証方式

第 3 回、第 4 回で解説してきました「ワンタイムパスワード」「生体認証」「FIDO」は多要素認証のメソッドとして非常によく使われております。これ以外にもさまざまな認証方式があります。トークンを使用しないちょっと変わったワンタイムパスワード認証である「マトリックス認証」や古くから使われている公開鍵暗号基盤を使用した「PKI 認証」、IC カードを使用した「IC カード認証」などの認証方式があります。今回はこれらの認証方式について解説します。

マトリックス認証

マトリックス認証とは認証時に碁盤の目のようなマスにランダムに並んだ英数字を、事前に決めたマス目の順番を選択して認証する方法です。ユーザはあらかじめ自分の覚えやすい文字や記号をなぞるような形でマス目を登録します。認証実行時はマス目にランダムな文字が入り、事前に決めた順番にマスを選択した文字列がパスワードとなります。毎回ランダムにマス目の文字が変わるため、毎回パスワードが異なることになります。一度使用したマス目の文字の並びは二度と同じ並び方にならないため、ワンタイムパスワードと同じく、入力した文字の順番を盗まれたとしても、二度と使用できないため、セキュリティリスクを減らすことができます。

例えば、下のようなマス目があった場合に、Z をなぞるようにマス目を選択しています。この並び順は (列 , 行) として次のようになります。
(A1),(B1),(C1),(D1),(E1),(D2),(C3),(B4),(A5),(B5),(C5),(D5),(E5)



	1	2	3	4	5
A	3	A	I	9	D
B	K	M	F	7	X
C	4	L	U	G	2
D	B	S	Y	8	Z
E	W	Q	5	0	V

パスワード
3AI9D7USWQ50V

つづいて、ユーザが認証時には認証ページで次のようなマス目と文字が表示されたとします。

この場合、文字の並び順は “3, A, I, 9, D, 7, U, S, W, Q, 5, 0, V” となります。認証ページにはこのようなマス目が表示され、ユーザが上記の順に文字を選択していきます。ユーザが再度認証するときはマス目の文字が更新されるため同じ順番で選択しても異なる文字列となります。のマトリックス認証は、記憶とワンタイムパスワードの組み合わせの認証方式であると言うことができます。マトリックス認証のメリットとしてはトークンが不要、パスワードは使い捨てであることです。デメリットとしてはユーザの記憶によりマスの並び順が決まるため、ユーザが忘れるリスクがあります。また、簡単な並び順を登録した場合はハッキングされるリスクがあります。

マトリックス認証の特徴

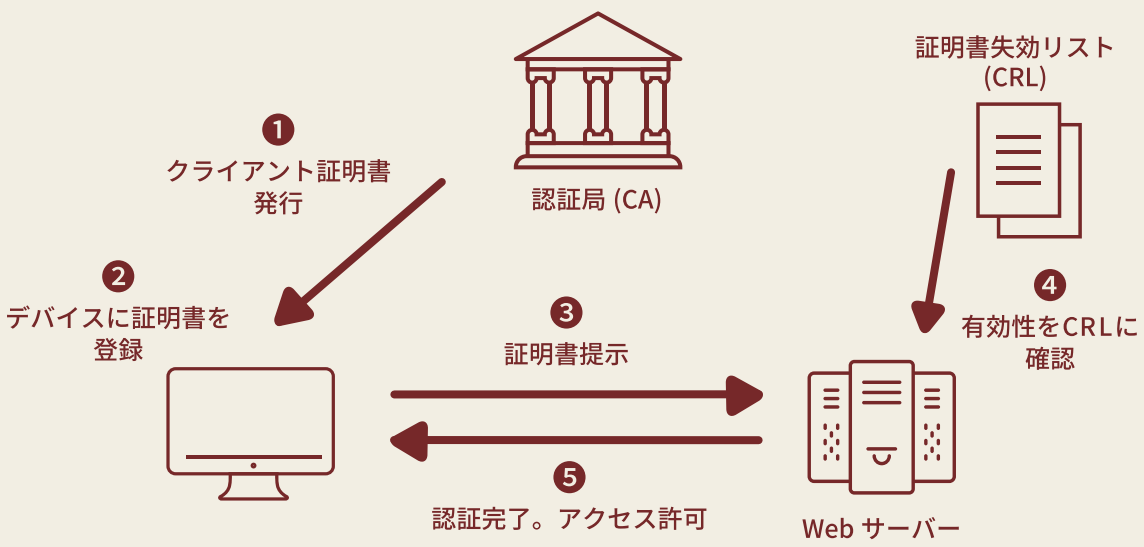
メリット	デメリット
トークン不要	ユーザーが選択マス順忘れへの対応
リーダー不要	使用端末の解像度により認証ページが読みにくくなる場合がある
パスワードが使い捨て	
使用端末を選ばない	Web上の認証ページにアクセスする必要がある

PKI 認証

PKI（Public-Key Infrastructure 公開鍵暗号化基盤）認証は公開鍵暗号を利用した認証方式です。公開鍵と秘密鍵のキーペアーからなる公開鍵暗号化方式を利用して電子証明書を使って認証します。電子証明書と聞くとインターネットの Web サーバへアクセスするとき SSL/TLS で通信を暗号化するときに使用されるサーバ証明書を思い浮かべる方も多いと思います。個人の認証を行うときは電子証明書のクライアント証明書が使用されます。クライアント証明書を使用されることから PKI 認証はクライアント証明書認証とも呼ばれています。クライアント証明書は PKI 基盤の認証局（CA: Certificate Authority）から発行されます。PKI 認証では正しい認証局から発行されたクライアント証明書であること、そのクライアント証明書が有効であることが確認されることで認証されます。クライアント証明書の有効性は証明書失効リスト (CRL : Certificate Revocation List) や OCSP(Online Certificate Status Protocol) により確認されます。

クライアント証明書による PKI 認証を行うには次のような手順になります。なお、この手順の前提として事前に Web サーバ側に認証局が発行するルート証明書を登録している必要があります。

PKI 認証（クライアント証明書認証）手順

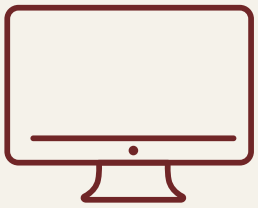


第 5 回　マトリックス認証、PKI 認証、IC カード認証

クライアント証明書はファイルまたはテキストとして発行されます。それをどのように使用するかをあらかじめ運用方法として決めておく必要があります。
主なクライアント証明書の使用方法として次のようなものがあります。

PKI 認証（クライアント証明書認証）方法

デバイスに登録



IC カードに登録

USBセキュリティキーに登録

デバイスに登録する場合は、Windows の証明書管理機能、ブラウザの証明書管理機能、iOS の証明書管理機能などを使用します。E-mail などでユーザのクライアント証明書を配布し各証明書管理機能で登録することが可能です。注意点としては証明書のフォーマットが各デバイスによって異なる場合があるのであらかじめユーザが使用するデバイスに合わせて変換してから送付する必要があります。

IC カードに登録する場合は、ユーザへ IC カードを配布する前にクライアント証明書を IC カードにコピーする必要があります。また、IC カードを使用する場合ユーザの使用する端末に IC カードリーダーが必要となります。IC カードを使用したクライアント証明書認証は e-Tax などの公的な機関でインターネット経由の電子申告や、電子納税などの公的サービスでも使用されています。

USB セキュリティキーを使用する場合はクライアント証明書認証に対応したセキュリティキーを使用してユーザへの配布前にクライアント証明書をコピーする必要があります。使用する端末には USB ポートが必須となります。

なお、クライアント証明書をファイル形式で直接ユーザに配布しユーザのデバイスに登録させる場合はユーザが自分の使用するデバイスにいくつも登録することが可能となるデメリットがあります。また、クライアント証明書のファイル管理もユーザに徹底させる必要があります。

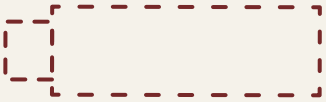
クライアント証明書認証を運用する上では次のような注意点があります。

クライアント証明書認証を運用する際の注意点

証明書の有効期限の管理

登録したデバイスの紛失

IC カード、USBセキュリティキーの紛失



証明書は認証局から発行される時にその有効期限が指定されます。一般的には発行後 1 年、2 年、3 年がよく利用され、期間が長いほど 1 年あたりの証明書費用が安くなります。有効期限が切れた場合、認証局からの再発行と既存の証明書との入れ替え作業が必要となります。期限が切れると認証できなくなるため有効期限の管理は非常に重要です。

証明書を登録したデバイスや証明書が登録されている IC カードや USB セキュリティキーを紛失した場合、証明書の失効処理が必要となります。紛失したユーザは管理者に紛失の連絡を行い、管理者が証明書を発行した認証局へ証明書の失効手続きを実施し、証明書の再発行を行います。執行手続きを実施すると失効させた証明書の情報が証明書失効リスト (CRL) に登録されます。再発行された証明書は新しいデバイスへの登録および新しい IC カードや USB セキュリティキーに登録します。

PKI 認証（クライアント証明書認証）の特徴

登録方法	メリット	デメリット
デバイスへ直接登録	トークン等の追加費用不要	有効期限の管理が必要
		デバイスの紛失リスクあり
	枯れた技術で強固なセキュリティ	ユーザによる端末への登録作業が必要
IC カード USB セキュリティキー	枯れた技術で強固なセキュリティ	有効期限の管理が必要
		デバイスの紛失リスクあり
		IC カードリーダーもしくは、 ISB ポート必要

IC カード（スマートカード）認証

IC カード認証はスマートカード認証とも呼ばれています。IC カードはプラスチックのカードに IC チップを搭載し記憶と演算を行うことができるカード型デバイスです。IC カードには IC チップがむき出しになった接触型と IC チップを内部に埋め込んだ非接触型があります。非接触型の場合カードをカードリーダーに近づけるだけで通信することができます。みなさまも交通系 IC カード（SUICA、PASMO、ICOCA など）でよく利用していると思います。接触型はクレジットカードでよく利用され、カード支払い時に専用の端末にカードを差し込んで PIN 番号を入力して決済したことがあるのではないでしょうか。また、IC カードは偽造が非常に難しいという利点があります。その反面、紛失や盗難といったリスクがあります。

IC カード種類	使用方法	使用例
接触型	カードリーダーに挿入	・クレジットカード ・キャッシュカード ・ETC カード
非接触型	カードリーダーにかざす	・交通系 IC カード ・電子マネー （Edy、iD、クイックペイなど）

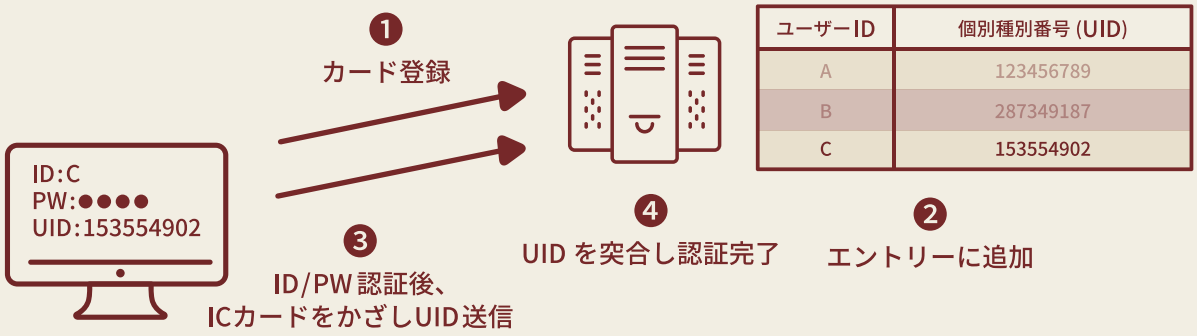
IC カード認証はこの IC カードをユーザ認証に使用します。IC カード認証にはクライアント証明書を使用した PKI 認証と、IC カードの固有 ID 番号を使用した認証方法があります。

接触型の IC カードでは上述した PKI 認証が使われます。IC カードにクライアント証明書を格納し、認証時に IC カードリーダーに挿入し PIN 番号を入力してクライアント証明書を IC カードから読み出して認証します。

非接触型の IC カードには NFC(Near Field Communication) と呼ばれる近距離無線通信の規格があり、その中にソニーが開発した FeliCa、オランダのフィリップス社が開発した Mifare があります。国内では FeliCa、海外では Mifare が高いシェアを占めています。非接触型 IC カードは書き換えられない固有 ID 番号（FeliCa で IDm、Mifare では UID）を持ち、この固有 ID 番号を利用して IC カード認証を実現しています。IC カードがあらかじめ持っている情報を使用するため、クライアント証明書をコピーする必要がありません。

また、すでに IC カードを入館用途などで社員に配布している場合、その IC カードをそのまま IC カード認証に使用することが可能です。

ICカード認証（スマートカード認証）手順



ICカード認証の特徴

ICカードの種類	メリット	デメリット
接触型	PKI認証と組み合わせて強固な認証を実現	紛失リスクがある
		リーダー初期費用必要
		リーダーへ挿入が必要
		リーダーが使用可能な端末でのみ使用可能
非接触型	すでに配布済みのICカードを使用可能	紛失リスクがある
		リーダー初期費用が必要
	リーダーにかざすだけで認証可能	リーダーが使用可能な端末でのみ使用可能

今回は「マトリックス認証」、「PKI認証」、「ICカード認証」についてそれぞれ説明しました。
これまで説明した「ワンタイムパスワード」や「生体認証」、
「FIDO認証」と合わせて多要素認証には様々な選択肢があることを
ご理解いただけたのではないでしょうか。

お問い合わせ
(GMOグローバルサイン株式会社)
03-6370-6540
support-jp@globalsign.com