GMO トラスト・ログイン

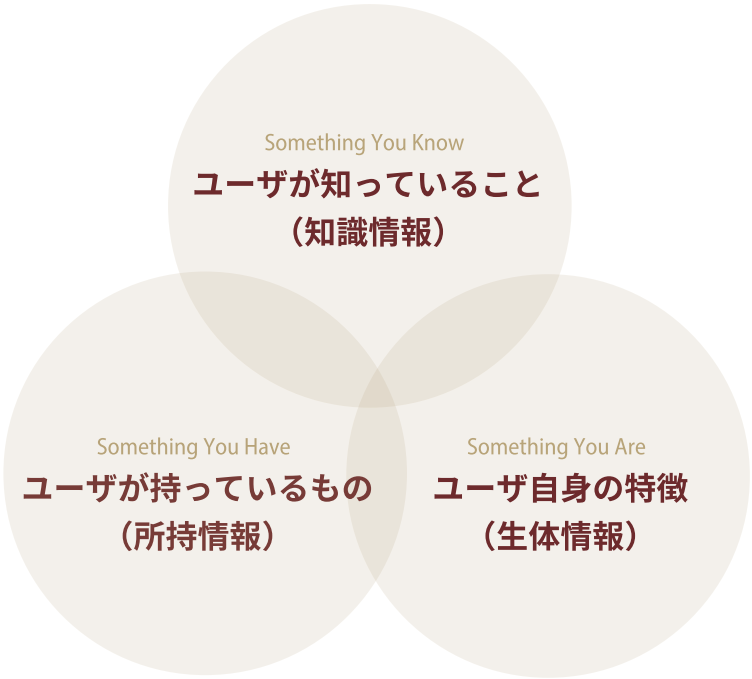
第 2 回

多要素認証の種類と方法

前回は身近な例から多要素認証について説明しました。普段使っている銀行の ATM やクレジットカードなどで多要素認証が身近に使われているということが理解いただけたかと思います。今回は多要素認証の種類や認証方式について説明します。

多要素認証の 3 要素

多要素認証で使われる要素には 3 つの種類があります。一つ目は皆さんがよく使っているパスワードのような「ユーザが知っていること（知識情報）」、二つ目は IC キャッシュカードのような「ユーザが持っているもの（所持）」、三つ目は指紋のような「ユーザ自身の特徴」の三つです。



これらの３つの種類のことを「要素」と呼びます。そのため多要素認証の「多要素」とはこの３つの要素の中から２つ以上の要素で認証することを言います。よく間違いやすいのが「パスワード」と「PIN 番号」のようにどちらもユーザが知っている知識情報で認証することは１種類の要素の２つの方法を使用しているので多要素認証とは言いません。この場合「2 段階認証」のように呼ばれることがあります。個人情報の流出やパスワードのハッキングなどがあった場合、ユーザが知っていることの「パスワード」と「PIN 番号」の二つが同時に漏れてしまう可能性があります。異なる要素で認証することでこのようなリスクを回避することができます。

多要素認証では２つ以上の要素を使用してログインユーザが確実に登録されている本人であることを認証します。

各要素に属する認証方式

多要素認証の３つの要素にはそれぞれ様々な認証方式が含まれます。ここではそれぞれの要素に含まれる主な認証方式を説明します。この認証方式のことを「認証メソッド（Method）」と呼ばれます。

各要素に属する認証方式

ユーザが知っていること（知識情報）

認証メソッド	特徴
ID・パスワード	ユーザに与えられた ID とユーザが知っているパスワードを使った認証方式。
PIN 番号	４桁から６桁の数字。セキュリティレベルが非常に低い。スマホのロック解除や認証デバイスを使用するためのロック解除、多要素認証前提の暗証番号などで使用。
秘密の質問 （シークレットクエスチョン）	事前に登録したユーザが知っている質問と回答の組み合わせ。質問はシステム管理が指定するものとユーザ自身が指定することがある。複数の質問と回答の組み合わせを登録させその中のいくつかがランダムに質問される。パスワードを忘れたときの再設定時などに使用される。
マトリクス認証	毎回異なる数字や文字がランダムに碁盤目状に並ぶ表の中から、事前にユーザが指定したマスの位置に表示された値を送信し認証する。

ユーザが持っているもの（所持情報）

認証メソッド	特徴
IC カード （スマートカード）	事前に登録したユーザが知っている質問と回答の組み合わせ。質問はシステム管理が指定するものとユーザ自身が指定することがある。複数の質問と回答の組み合わせを登録させその中のいくつかがランダムに質問される。パスワードを忘れたときの再設定時などに使用される。
ワンタイムパスワード	定期的に更新されるランダムな数字列を表示するデバイス。ここに表示される数字列がワンタイムパスワードと呼ばれる。ワンタイムパスワードは定期的に更新されるため一度使った値を再利用することができない。デバイスはメーカー毎に様々なものがある。キーホルダータイプやスマホアプリで提供されるソフトウェアタイプもある。
USB トークン	USB メモリのような形状で内部に電子証明書の「鍵」を保存できる仕組みになっている USB デバイス。認証時に USB ポートに差し込んで「鍵」を読みだして認証する。
FIDO U2F	次世代認証方式として有望視されている FIDO アライアンスが規格を標準化している認証方式。FIDO U2F と呼ばれる規格が USB タイプのデバイスで提供される。認証時に USB ポートに挿入し金属部分を指で触れる。

各要素に属する認証方式

ユーザが持っているもの（所持情報）

認証メソッド	特徴
SMS 認証	SMS（ショートメッセージサービス）は携帯電話の電話番号へ短文のメールを送信する仕組み。SMS 認証は認証時にサーバよりユーザの携帯電話へ SMS でワンタイムパスワードが送信され、その内容を入力して認証する。
E-mail 認証	認証時にサーバよりユーザへメールでワンタイムパスワードが送信されその内容を入力して認証する。メールアドレスにアクセスできる端末を持っていることで認証が可能となるが、メールは複数のデバイスからアクセス可能なためセキュリティレベルとしては低い。
ボイスコール	認証時にユーザの携帯電話へ電話が着信しワンタイムパスワードが読み上げられる。ユーザは読み上げられたパスワードを入力することで認証する。
スマホアプリ認証	スマートフォンに専用のアプリケーションをインストールし認証する。ログイン時にスマホアプリからアクセスを承認するかどうかを確認され「承認」をタップすることで認証される。
Bluetooth Smart 認証デバイス	Bluetooth 接続型の認証デバイス。あらかじめログイン端末とペアリングしておき認証時に Bluetooth 接続されていることで認証する。
暗号表認証	ランダムな英数字が表となっている暗号表を事前にユーザに配布し、認証時に指定された行と列に該当する値を順次入力することで認証する。

ユーザ自身の特徴（生体情報）

認証メソッド	特徴
指紋認証	ユーザの指紋情報により認証する。指紋を読み取る専用のデバイスが必要。
顔認証	ユーザの顔を認識し認証する。カメラ付きのデバイスが必要。
虹彩認証、網膜認証	ユーザの目の虹彩または網膜により認証する。虹彩または網膜を読み取る専用のデバイスが必要。
静脈認証	ユーザの手の静脈により認証する。静脈を読み取る専用のデバイスが必要。
FIDO UAF	FIDO アライアンスが標準化している次世代認証方式の生体認証規格。スマートフォン用の生体認証機能を標準化している。

セキュリティ対策とユーザ利便性の両立を実現する多要素認証

多要素認証の要素とそれぞれの認証メソッドについて見てきました。では、ここでなぜ多要素認証が必要となるのかについて考えてみましょう。これまでの主な本人確認方法としてパスワードが多く使われてきました。セキュリティ被害が社会問題となるたびにパスワードの複雑性や定期的な変更する頻度を短くするなど対策を講じてきました。ただしこのような対策ではユーザの利便性は損なわれ、長くて複雑なパスワードをユーザが記憶しておかなくてはなりません、またパスワードを忘れてしまうことも頻繁に発生しそのたびにリセットの依頼を行う必要がありました。そこで、ユーザの利便性を損なわずにセキュリティを強化する方法として多要素認証が使用されています。パスワード以外の要素でも認証するため、パスワードの複雑性や短期間の変更を行う必要がなくなります。

「ユーザが持っているもの（所持）」の認証メソッドを使用する場合ユーザは認証用のデバイスを常に携帯しておけばよいことになります。それが日常から携帯している社員証（IC カード）、交通系 IC カード、携帯電話およびスマートフォンを使用する場合はデバイスを追加で持つ必要もありません。また、「ユーザ自身の特徴（生体認証）」を使用する場合は何か携帯する必要もありませんのでデバイスを忘れるといったこともありません。
パスワードと合わせてもう一つ追加の認証を行うことでハッキング等によりパスワードが解読・漏洩されても、もう一つの認証が通らないためシステムへの不正アクセスを防ぐことがユーザへの追加負担を少なく実現できることとなります。

多要素認証の導入と運用容易性

次に自社のシステムを保護するのにどのような認証メソッドを選択すればよいのかを検討するにはそれぞれの認証メソッドのメリット・デメリットを理解する必要があります。ここでは多要素認証導入時に検討すべき事項について、それぞれの認証メソッドの導入容易性、運用容易性、向いているシステムの観点から解説します。導入容易性は初期デバイスコストおよび初期設定の複雑性、教育コストがポイントになります。運用容易性はランニングコスト、紛失時の無効化手順、ユーザの利便性がポイントとなります。

物理デバイスタイプ（キーホルダ型ワンタイムパスワード、IC カード、Bluetooth）

物理的な認証デバイスが必要なものは導入コストと運用コストを検討します。また、紛失時の無効化手順および再発行の手順をあらかじめ決めておく必要があります。また、IC カードをすでに社員証などで導入している場合は流用可能の場合がありますが IC カードリーダーの導入コストが発生します。使用方法はどれも容易なため教育コストは低く抑えられます。

多要素認証の導入と運用容易性

生体認証
（指紋認証、虹彩認証、静脈認証などの生体認証）

生体認証を実施するには読み取り装置としてリーダーが必要になります。アクセスする端末へリーダーが搭載されているか、取り付け可能なものなのか検討する必要があります。導入時にはリーダーの初期コストが発生します。指紋認証のように異なるベンダーのリーダーでも共通で用可能な場合がありますが、通常は使用するユーザの端末すべてにリーダー導入コストが発生します。そのため複数のユーザが共有の端末を使用するような業務に向いています。使用方法は比較的容易なため教育コストは低く抑えられます。生体認証は紛失のリスクはありません。

USB 接続タイプ
（指紋認証、虹彩認証、静脈認証などの生体認証）

使用するときにアクセス端末に USB 接続が必要メソッドは PC に使用が限定されます。標準の USB 端子がないモバイル端末からでは使用できません。価格は安価で電源も不要なため運用コストもかかりません。使用方法は比較的容易です。

スマートホンアプリ
（指紋認証、虹彩認証、静脈認証などの生体認証）

既存のスマートフォンにアプリを導入するだけで運用できるので導入コストは低く抑えることができます。スマートフォンを会社支給されていないユーザの場合は個人スマートフォンにインストールすることが必要となります。また、各自のスマホ OS バージョン（Android、iOS）についてアプリが対応しているかどうか確認する必要があります。アプリのインストールと初期設定および認証時のアプリの使用方法をユーザに教育する必要があります。

多要素認証の導入と運用容易性

携帯電話タイプ（SMS 認証、ボイスコール）

既存の携帯電話だけで運用可能なため導入コストは抑えることができます。使用方法も容易なため教育コストも抑えられます。SMS やボイスコールは認証毎にサーバ側からのユーザの携帯電話へ発呼するため認証毎に発呼費用が発生します。ユーザは携帯電話が通じるエリア内にいる必要があります。

タイプ	導入費用	運用費用	教育費用	紛失時の費用
	その他			
物理デバイスタイプ	△	△	○	×
	電池式の場合は交換が必要			
生体認証	×	○	○	○
	デバイス費用が高価なため共有端末向き			
USB 接続タイプ	△	○	○	×
	PC でのみ使用可能			
スマートホン アプリタイプ	×	×	△	△
	個人スマホを利用する場合はユーザとの合意が必要			
携帯電話タイプ	○	△	○	△
	通話エリア内でのみ使用可能			

今回は多要素認証の要素と認証メソッドについてどういうものが提供されているのか、
またそれぞれの主な特徴について解説しました。
次回からはそれぞれの認証メソッドについて仕組みや特徴についてより詳細に説明していきます。

お問い合わせ
（GMOグローバルサイン株式会社）
03-4545-2303
support-jp@globalsign.com