

100年使える 本物の多要素認証 ガイドブック

各認証方式のポイントを理解して
パスワードから脱却

サプライチェーンに対するランサムウェア攻撃をはじめ、情報セキュリティリスクが高まっています。これに対処するため、各業界の情報セキュリティガイドライン（以下、ガイドライン）では、業務システムにログインする際の認証方法に「多要素認証（MFA / Multi-Factor Authentication の略）」を要請または推奨しています。

多要素認証には、パスワードを使わない「パスワードレス多要素認証」が効果的です。なぜ「パスワードレス多要素認証」が効果的なのか？そもそも多要素認証とは何か？そして各認証方式のメリット・デメリットを解説。さらに、おすすめのソリューションをご提案します。

このガイドブックをお読みいただくと、以下のポイントを知ることができます。

1 多要素認証とは？

ログイン時のセキュリティを高めるために「知識」「所有物」「生体」のうち2つ以上の異なる認証を組み合わせる方式。多くの業界ガイドラインが採用を推奨している。同じ種類の組み合わせ（知識+知識など）は多要素認証にはならない。

2 どの組み合わせが良い？

組み合わせには必ず知識認証を入れるべき理由を説明。また、知識認証と所有物認証の組み合わせがコストパフォーマンスに優れる。生体認証は使いやすさの点で好まれるが、誤判定やコストが課題となる。

3 知識認証のおすすめは？

知識認証は、パスワードや暗証番号のような「文字や数字」による認証が有名だが、「場所と順番のパターン」による認証（パターン認証）もある。パターン認証を取り入れ、安全性と利便性の両立を低コストで実現する「パスワードレス多要素認証」を紹介。

4 各業界ガイドライン

巻末付録として、多要素認証を要請または推奨する主な業界ガイドラインとその要旨の一覧を掲載。

1. 各業界ガイドラインが要請する多要素認証
 2. 「多要素認証」とは
 3. 多要素認証の導入で考えるべきポイント
 4. 多要素認証におすすめの PassLogic の「パスワードレス多要素認証」
 5. まとめ
- 付録：多要素認証を要請する主な業界ガイドライン一覧

各業界ガイドラインが要請する多要素認証

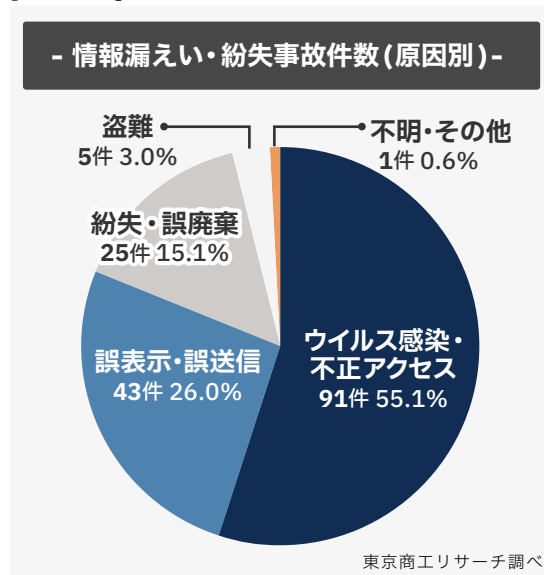
不正アクセスによる情報漏洩リスク

テレワークやハイブリッドワークなどの新しい働き方が定着し、社員が社外から社内システムにアクセスする機会が増えた結果、情報漏えいのリスクがかつてないほど高まっています。

東京商工リサーチの調査によると、上場企業における 2022 年の情報漏えい事故の件数は 165 件で、過去最多を 2 年連続で更新しています。

原因別で最も多かったのが「ウイルス感染・不正アクセス」の 91 件（55.1%）でした（グラフ -1）。さらに「不正アクセス」は個人情報漏えい事故のうち、漏えい人数の多かった事故原因の上位を占めています（表 -1）。つまり、不正アクセスは、被害件数が多いうえに被害規模も大きくなることが分かります。

【グラフ -1】



【表 -1】

順位	社名	理由	漏えい・紛失人数
1位	小売業 J 社	誤表示・誤送信	1,913,854 人
2位	製造業 M 社	不正アクセス	1,648,922 人
3位	サービス業 M 社	不正アクセス	460,988 人
4位	製造業 T 社	誤表示・誤送信	296,019 人
5位	情報・通信業 R 社	誤表示・誤送信	250,000 人
6位	製造業 W 社	不正アクセス	149,483 人
7位	製造業 T 社	誤表示・誤送信	140,000 人
8位	小売業 N 社	不正アクセス	132,000 人
9位	製造業 B 社	不正アクセス	127,359 人
10位	製造業 P 社	不正アクセス	103,935 人

※情報漏えい・紛失件数は「可能性がある」を含む。個人情報の不適切な取扱いの結果生じた事例なども対象としている。

業界ガイドラインが多要素認証の適用範囲を拡大

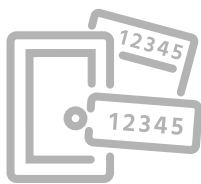
このような状況のなか、各業界のセキュリティガイドラインでは不正アクセス対策として、社内システムの入口の認証に「多要素認証」の導入が推奨されており、特に医療業界、教育業界、行政機関など、個人情報をはじめとした機密情報を扱う

組織では、強く推奨されています。また、サプライチェーンに対するランサムウェア被害の拡大により、業界を限定せずに対応が必須な状況といえます。

「多要素認証」とは

では、多要素認証とはどのような認証方法なのでしょうか？

多要素認証とは、認証の信頼性を高めるために「知識」「所有物」「生体」のうち異なる複数の要素を組み合わせることで、認証を強化する方法です。事実上、要素を2つ（二要素）を組み合わせることが多いので「二要素認証」とも呼ばれています。



所有物認証



生体認証



知識認証

多要素認証を構成する3つの認証要素とその特徴

それぞれの認証要素の安全面、運用面、コスト面におけるメリットとデメリットを見ていきましょう。

所有物認証

特定の物理的なアイテムやデバイスといった「所有物」を使用して認証する方法です。実際にモノを持っている必要があるため、ネットワーク越しの不正アクセスに耐性があります。端末内に保存された「デジタル証明書」も所有物認証になります。

代表例



- IC カード
- ワンタイムパスワード用トークン
- デジタル証明書

メリット

- 物理的なアイテムやデバイスを使用するため、オンラインでの攻撃に対して耐性がある。
- シンプルな仕組みのため、使い方が分かりやすい。

デメリット

- 物理的なアイテムやデバイスの導入・管理・保守にコストがかかる。
- 紛失や故障、盗難のリスクがある。
- 物理的なアイテムやデバイスを持ち歩き、使用時に取り出す必要がある。

生体認証

指紋や顔、虹彩（瞳の模様）など、身体の一部の「生体」情報を使用して認証する方法です。モノの持ち運びを意識する必要がないことや、簡単さが好まれています。ただし、生体情報を読み取るデバイスが必要なためコストがかかります。さらに、バックアップからの復帰にパスワードが必要となるため、パスワード漏えいのリスクが残ります。

代表例



- 指紋
- 顔
- 静脈
- 虹彩
- 声紋

メリット

- 偽造が困難であり、他人によるなりすましを防ぐことができる。※
- 何も持ち歩く必要がなく簡単で便利。
- 瞬時に認識され迅速な認証が可能。
- 紛失や盗難のリスクが低い。

デメリット

- 生体情報を読み取るためのデバイスが必要。
- ケガや発汗など、特定の状況で認識エラーになる可能性がある。
- 生体情報は変更できないため一度漏えいすると永続的に悪用される可能性がある。
- バックアップからの復帰にパスワードの管理が必要。

※ 現在はまだ偽造やなりすましは困難ですが、技術の発達により将来的には簡単になる可能性があります。

知識認証

利用者があらかじめ登録した文字や数字などの「知識」つまり記憶を使用して認証する方法です。パスワードや PIN コードなどがこれにあたります。ある個人だけが知っている記憶を、他人が脳内から引き出すのは非常に難しいため、不正を防ぐことができます。必要なのは記憶だけなので、コストもかかりません。しかし、人の記憶力に依存しているため、管理に大きな課題があります。

代表例



- パスワード
- PIN コード
- 秘密の質問
- パターン

メリット

- 他人の記憶を引き出すのは困難。
- 実装や管理にかかるコストが低い。
- 認証時に専用のデバイスが必要ない。
- リセットや再発行が簡単。

デメリット

- フィッシングやパスワード攻撃への脆弱性。
- 複数のパスワード管理が面倒、覚えられない。
- 使い回しにより安全性が著しく低下する。

多要素認証の導入で考えるべきポイント

高い安全性を保ちつつ、簡単さとコスト削減も追及するためには、どのようなことを考慮すればいいのでしょうか。そのポイントを整理します。

パスワードはリスクが大き過ぎる

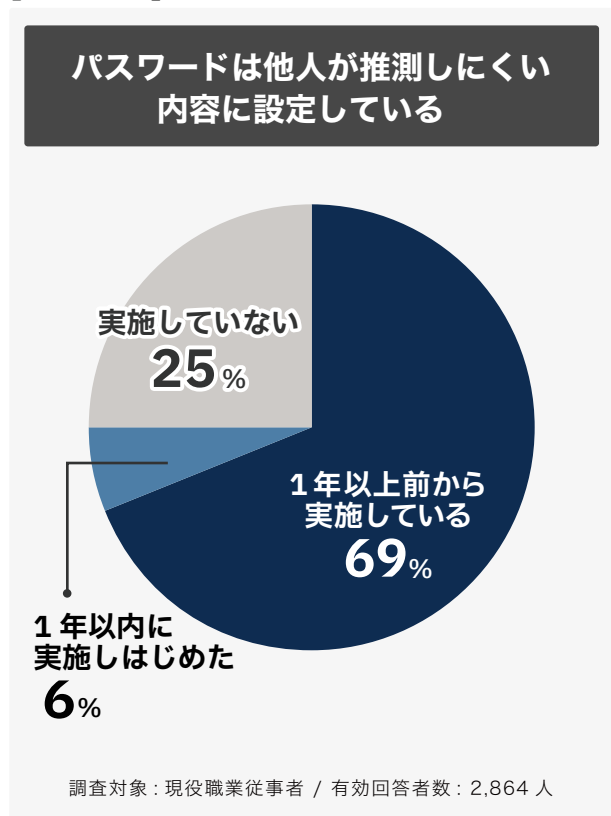
多要素認証の組み合わせの1つとして最もよく使われるのは「パスワード」です。しかし、知識認証の代表であるパスワードには大きく2つのリスクが存在します。

1つめは「簡単なパスワードにすると推測されやすいこと」です。覚えやすいように簡単なパスワードを使うと、類推攻撃やリスト型攻撃、辞書攻撃などによって推測されて不正アクセスを許すリスクが高まります。IPA（独立行政法人情報処理推進機構。国のIT政策実施機関）の調査によると、他

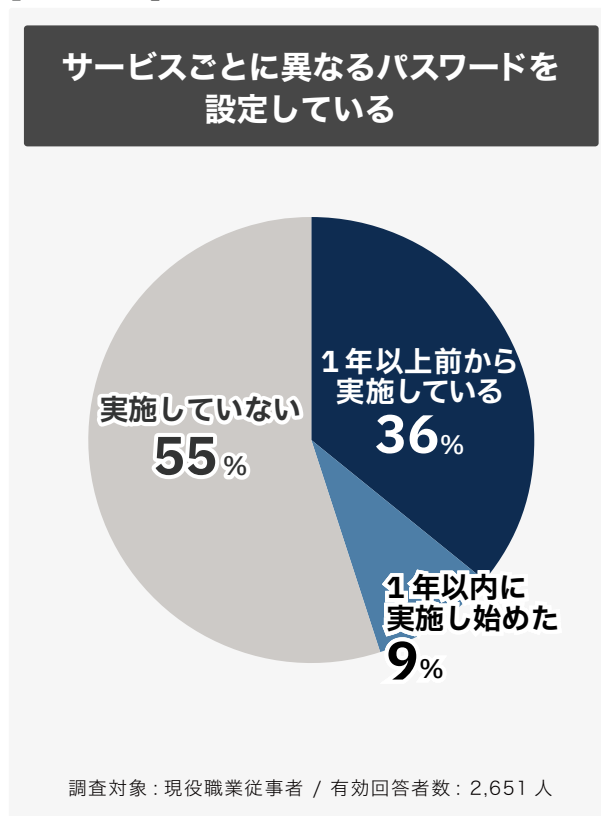
人に推測されやすいパスワード（氏名や誕生日など）を設定していると答えた人が全体の4分の1を占めていました（グラフ-2）。

2つめは「漏えいすると簡単にログインされてしまうこと」です。特に、パスワードを使い回していると、1つのサービスで漏えいしたパスワードで、別のサービスにログインされるリスクが高まります。同じIPAの調査では、複数のサービスでパスワードを使い回していると答えた人が、なんと全体の半分以上を占めていました（グラフ-3）。

【グラフ-2】

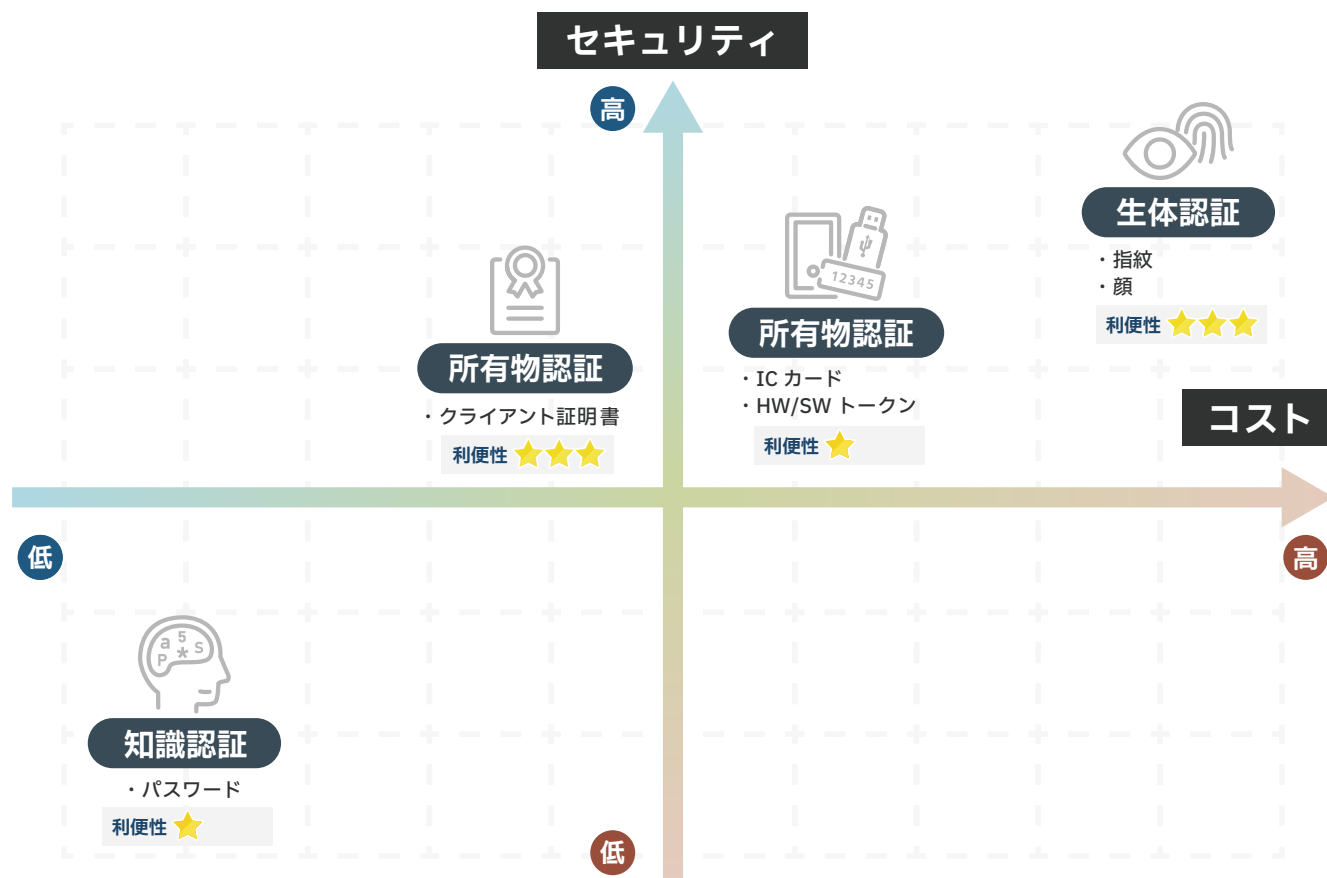


【グラフ-3】



[出展：IPA「2022年度情報セキュリティの倫理に対する意識調査_職業軸」報告書]

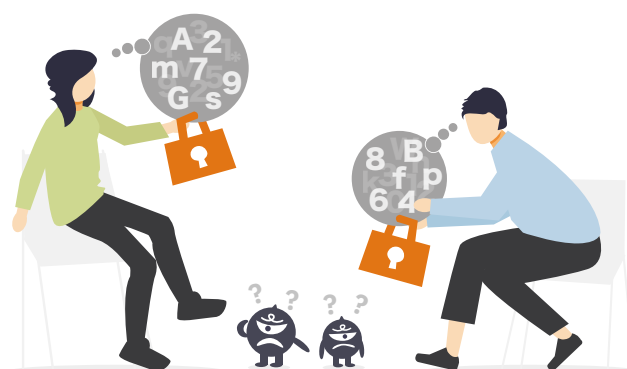
この対策として、管理者がパスワードポリシー（パスワードに関するルール。長く複雑なパスワードの設定や、使い回し禁止などのルール）を策定しても、実際に利用者が実践しているかを確認するのは困難です。



実は優れている知識認証

知識認証の代表であるパスワードには、非常に大きなリスクがあることを説明しました。しかし一方で、知識認証には優れた強みがあります。例えば、自分の脳内から出さずに秘密にしておけば「窃取される心配がない」ということ。本人に漏らす意思がない限り、攻撃者が脳内の記憶を窃取するには、暴力的な攻撃をしなくてはなりません。このため攻撃者にとっては、所有物を盗んだり、生体情報を複製するよりも、比較にならないほど大きなコストを支払い、リスクを負うことになります。

また、所有物認証や生体認証と異なり、ICカードやスマートフォン、指紋認証リーダーやセンサーカメラなどの「モノが不要」なことも強みです。紛失・盗難の心配がないのはもちろん、記憶さえしていれば簡単に取り出せます。持ち歩き・取り出しが必要なく、準備や管理が要らないことにつ



ながり、利用者や管理者にとって大きなメリットとなります。

つまり、知識認証のこれらの強みを生かした「パスワードではない知識認証」があれば、それは非常に優れた認証方法だといえます。

多要素認証におすすめの PassLogic の「パスワードレス多要素認証」

そこで、多要素認証の導入をご検討の方におすすめしたいのが、PassLogic（パスロジック）の「パスワードレス多要素認証」です。おすすめの理由をこれからご説明します。



パスワードではない知識認証で高いセキュリティ

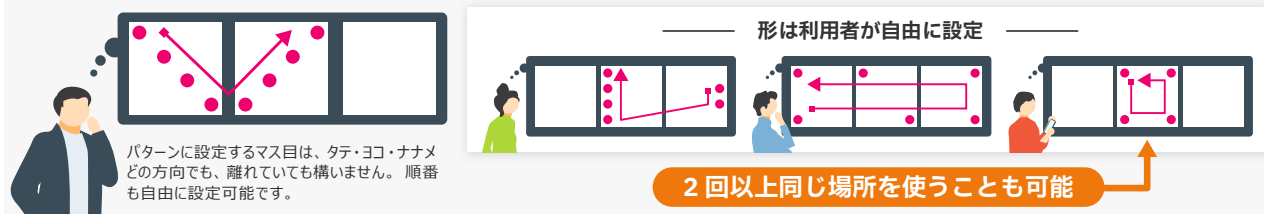
PassLogic の認証方法は「パターン」による知識認証を利用します。ログイン画面の乱数表から、事前に決めておいた1つのパターンに沿って数字を読み取り、入力します。乱数表は毎回変わるため、入力する数字も毎回変わる「ワンタイムパスワード」になります。覚えるのは、たった1つのパターンだけ。複数のパスワードを覚えたり管理したりする必要が

なくなります。記憶するのはパスワードではないので、社員がプライベートで使っているパスワードとの使い回しを心配することもなくなります。

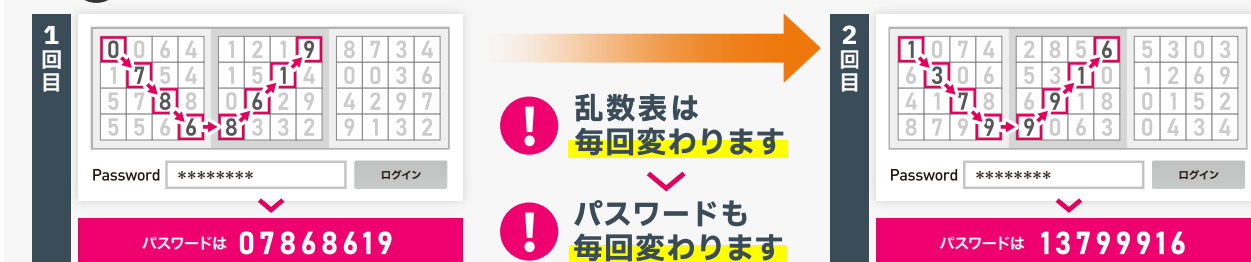
この仕組みを「機器（デバイス）が必要ないワンタイムパスワード」なことから「デバイスレス・ワンタイムパスワード」といいます。

■ デバイスレス・ワンタイムパスワードの仕組み

STEP 1 “マスの位置”と“順番”から「パターン」を作成・登録します。



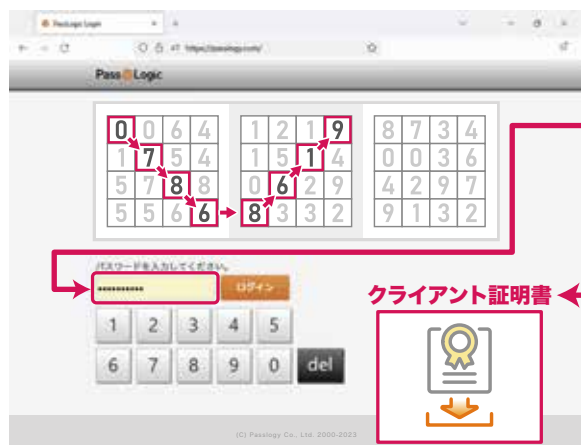
STEP 2 「パターン」に表示されている数字が、パスワードになります。



デバイスが不要で簡単、低コスト

PassLogic の「パスワードレス多要素認証」は
 “本人だけが知っているパターン” と、「デジタル
 証明書」がインストールされた “組織が使用を許
 可した端末を持っている” という「知識認証」+

「所有物認証」の組み合わせで実現します。この
 組み合わせであれば、ブラウザだけで多要素認証
 が完結します。



パターンに沿って読み取った数字
 を入力（デバイスレス・ワンタイム
 パスワード）

あらかじめ PC にデジタル証明書
 をインストール（クライアント証
 明書）

クライアント証明書



知識認証

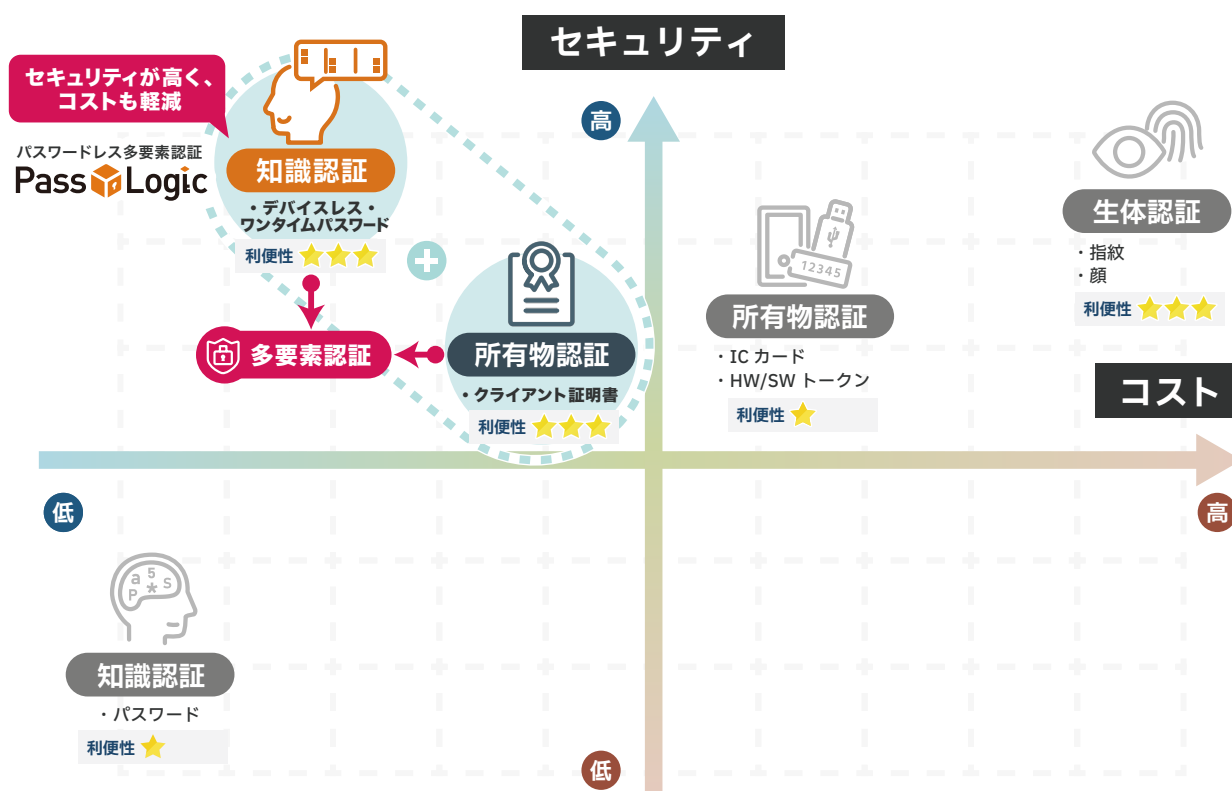
+

所有物認証

||

多要素認証

さらに、実際に業務に使用する端末以外に、認証用デバイスを用意する必要がないので、管理者にとっては
 導入・運用コストが削減され、利用者にとっては持ち運び・取り出しの手間もかからない「安全性・利便性・
 コスト」のバランスに優れた理想的な多要素認証を構築することができます。



PassLogic のその他の機能

PassLogic は多要素認証による不正アクセス対策だけでなく、多機能な認証プラットフォームとしても、企業や組織の多様なニーズにお応えできます。

PassLogic の機能の一例

- ・シングルサインオン（SSO）
- ・Windows OS への認証強化
- ・アクセスコントロール
- ・ユーザー情報の自動更新

…などの機能を搭載しています。

PassLogic
製品サイト



クリックでサイトに
ジャンプします。

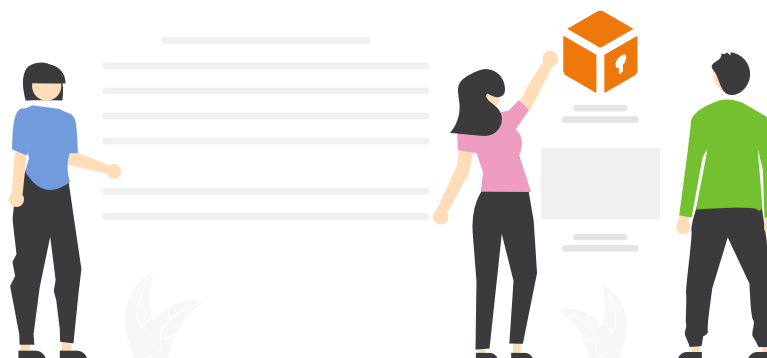
まとめ

各業界のガイドラインが要求する「多要素認証」に対応することは、不正アクセス対策を強化するだけでなく、関連する規制要件に適合することで企業の対外的な信頼性も向上します。

多要素認証は、組み合わせた認証方法が相互に補完して強みを生かすことが重要です。その組み合わせの1つに、脳内の記憶を利用する知識認証を使うことが、長期間の安定運用とコストメリットをもたらします。ただし、知識認証の代表格であるパスワードにはリスクがあるため、それを解消した知識認証方式が必要です。

そこで、パスワードに代わり、「パターンによる知識認証」で「パスワードレス多要素認証」を実現するのが「PassLogic」です。

無料評価版をご用意していますので、ぜひお試しください。





付録：多要素認証を要請する主な業界ガイドライン一覧

発行省庁	ガイドライン名称	多要素認証を要請する記述の要約
内閣官房 内閣サイバーセキュリティセンター	政府機関等の対策基準策定のためのガイドライン（令和5年度版）	インターネット等から直接クラウドサービスへアクセスを許可する場合は、多要素主体認証方式による主体認証を基本方針とする。クラウドサービスの管理コンソールに管理者がログインする場合は、多要素主体認証を利用する。ウェブコンテンツを更新する際の認証に多要素主体認証を設ける。リモートメンテナンスを行う主体の認証において多要素主体認証を用いる。情報システムの基盤を管理又は制御するソフトウェアを導入する端末などには、多要素主体認証を用いる。多要素主体認証の一つとして生体情報を利用する場合は、誤認や誤否の可能性があるという課題を考慮すること。リモートアクセスに対し多要素主体認証を行うこと。
デジタル庁	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	管理者アカウントによるアクセスには多要素認証等を用いる。
総務省	地方公共団体における 情報セキュリティポリシーに関するガイドライン（令和5年3月版）	マイナンバー利用事務系、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合、クラウドサービスにアクセスする場合には多要素認証の対策を必要とする。
	テレワークセキュリティガイドライン第5版	システム・セキュリティ管理者が実施すべき対策に、社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り多要素認証を強制する。
	クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）	情報資産へのアクセス制御となりすまし対策として、高い機密性、完全性が求められるサービスでは、多要素認証を採用する。
	5Gセキュリティガイドライン第1版	セキュリティ対策要件として、施設への物理的なアクセス許可は多要素認証によって本人認証を行う。
	スマートシティセキュリティガイドライン（第2.0版）	特権を持つ利用者のシステムへのネットワーク経由でのログインに対して、多要素認証を採用する。
文部科学省	教育情報セキュリティポリシーに関するガイドライン	校務情報等の重要な情報資産へのアクセスについては、多要素認証を必須とする。児童生徒におけるID及びパスワード等の管理において、本人確認を厳格に行う必要がある場合においては多要素認証を設定することが望ましい。学習用ツールへのシングルサインオンは、必要に応じて多要素認証と組み合わせる。
厚生労働省	医療情報システムの安全管理に関するガイドライン第6.0版システム運用編	令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新する際は、二要素認証を採用するシステムの導入、又はこれに相当する対応を行う。
経済産業省	医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第1.1版	医療情報システムの利用者認証における考慮事項として、医療情報の機密性の高さや攻撃手法の高度化に鑑み、多要素認証を可能な限り早期に採用すべきである。
独立行政法人情報処理推進機構	組織における内部不正防止ガイドライン第5版	組織内外に分散する重要情報について、アクセス権限を細かく設定して保護し、端末のクライアント証明書認証や利用者の多要素認証などを導入すること。
産業サイバーセキュリティ研究会	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.0	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合は、多要素認証の対策を行うこと。
一般社団法人 日本自動車工業会／ 一般社団法人 日本自動車部品工業会	自工会／部工会・サイバーセキュリティガイドライン 2.0 版	機密レベルが高い情報を取り扱うシステム、特権アカウント、リモートアクセスを対象とした、インターネットを経由した認証においては、多要素認証を実装すること。
各府省情報化統括責任者(CIO)連絡会議	行政手続におけるオンラインによる本人確認の手法に関するガイドライン	オンラインにおける本人確認の手法として、遠隔又は対面での身元確認では、マイナンバーカード若しくはこれによることができない場合、多要素認証による本人認証を実施。

2023年7月21日時点



PASSLOGIC™ パスロジ株式会社

〒101-0051 東京都千代田区神田神保町1丁目6-1

<https://www.passlogy.com/>

PassLogic

<https://passlogy.jp/>



クリックでサイトに
ジャンプします。