

本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議（第1回）

当人認証手法の具体例について

令和7年9月 デジタル庁 トラストタスクフォース

はじめに

本資料の位置づけ

- 本人確認ガイドラインの改定にあわせ、具体的な手法例等を取りまとめた「解説書」を準備中。
- 本資料は「[解説書](#)」に掲載予定の**主要な本人確認手法に関して、その概要、脅威耐性、考慮事項、その他の関連するコラム**の案を、有識者会議での協議用資料として取りまとめたものである。

本人確認ガイドライン 本編 (改定版の発行に向け現在手続中)

位置づけ：Normative (遵守する内容)

本人確認の概念、基本的な枠組み、検討のプロセスなど、原則的・普遍的で陳腐化しにくい情報をとりまとめる

読み手の負担を軽減するため、本編はできる限りシンプルな内容に留めてページ数を抑え、参考情報は「解説書」に移動する

比較的長期間の改定サイクルを想定

デジタル社会推進標準ガイドライン DS-511

行政手続等での本人確認における
デジタルアイデンティティの取扱い
に関するガイドライン

2025年(令和7年)XX月XX日
デジタル庁

【ドキュメントの位置付け】

Normative: 政府情報システムの整備及び管理に関するルールとして遵守する内容を定めたドキュメント

【キーワード】

本人確認、デジタルアイデンティティ、身元確認、本人認証、フェデレーション、対象手続のデジタル化、マイナンバーカード、公的個人認証

【概要】

国の行政機関が行政手続等において申請者の本人確認を行う際のデジタルアイデンティティに関する枠組み、対策基準、リスクの評価手順、本人確認手法の選定方法等を示した標準ガイドライン附属文書。

本人確認ガイドライン 解説書 (仮称) (2025年度内の発行に向け執筆中)

位置づけ：Informative (参考情報)

本人確認ガイドライン本編の参考資料として、

- 採用候補となる**具体的手法**
 - 実際の事例、留意点
 - 検討用ワークシート
- などの情報をとりまとめる

技術や脅威の動向等を踏まえつつ、比較的短期間のサイクルでの継続的な改定を行う運用を想定

デジタル社会推進実践ガイドブック DS-512

行政手続等での本人確認における
デジタルアイデンティティの取扱い
に関するガイドライン
解説書

2025年(令和x年)XX月XX日
デジタル庁

【ドキュメントの位置付け】

Informative
参考とするドキュメント

【キーワード】

本人確認、デジタルアイデンティティ、身元確認、本人認証、フェデレーション、行政手続のデジタル化、マイナンバーカード、公的個人認証

【概要】

「DS-511 行政手続等における本人確認及びデジタルアイデンティティに関するガイドライン」に基づく本人確認手法の検討にあたる解説や補足を記載した参考文書。

はじめに

解説書に記載予定の具体手法一覧（当人認証手法）

- 本人確認ガイドライン解説書では、以下の当人認証手法を具体例として掲載することを予定している。

掲載予定の当人認証手法

- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

当人認証に関連するコラム

コラム1) フィッシング攻撃への耐性について

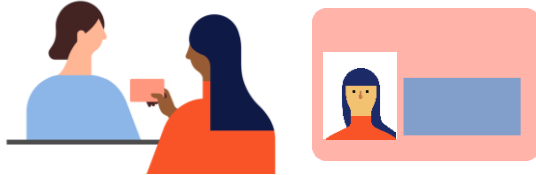
当⼈認証の概要

（「本人確認ガイドライン改定方針 令和6年度とりまとめ」より一部抜粋・編集）

本人確認の基本的要素

- 本人確認ガイドライン改定案では、本人確認の構成要素を「身元確認」、「当人認証」及び「フェデレーション」とし、それぞれを以下のように定義。

身元確認 (Identity Proofing)

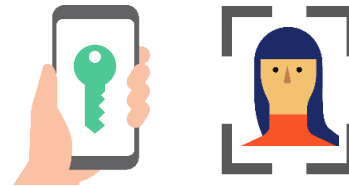


申請者を一意に識別するとともに、その実在性を確認すること。

具体的には、申請者の属性情報を収集することで、申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認する。

当人認証 (Authentication)

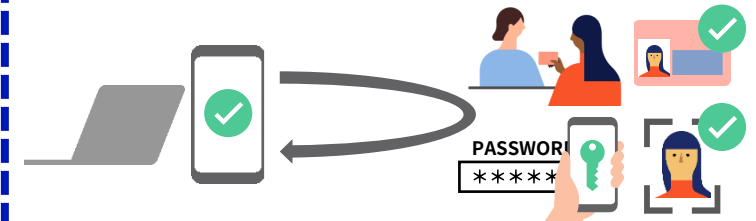
PASSWORD:



申請者の**当人性を確認**すること。

具体的には、対象手続を利用しようとする者が、身元確認時に登録された者同一の人物であることを、申請者と紐づけて登録した認証器を用いて確認する。

フェデレーション (Federation)

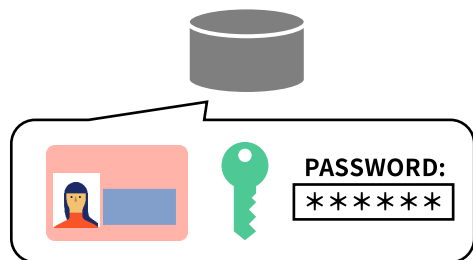


身元確認や当人認証を、他者に依拠して実現すること。

具体的には、信頼できるIDプロバイダと連携し、IDプロバイダによって行われた身元確認や当人認証の結果に関する情報を入手することで、対象手続における本人確認を実現する。

当人認証のライフサイクルに沿った対策の定義

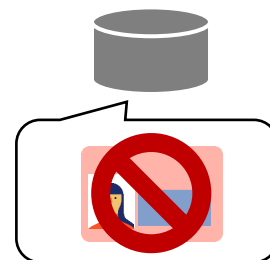
- 当人認証におけるプロセスとして「認証器の登録」、「当人認証の実施」、「盗難・紛失時の対応」、「アカウント回復」を定義し、認証器のライフサイクルに沿って必要となる対策や留意事項を定義。



アカウント登録時等の身元確認プロセスにおいて認証器を登録するなどして、当人認証に用いる認証器を利用者と紐づけて登録する。



手続やサービスを利用しようとする申請者が、あらかじめ登録されている利用者と同一の人物であることを、認証器によって確認する。



利用者から認証器の盗難や紛失の報告を受けた際に、認証器の無効化やアカウントの停止等の対応を行う。



認証器の盗難・紛失、故障による交換、パスワードの忘失などによって利用者がアカウントにログインできなくなった状態を回復する

当人認証における脅威

- 当人認証における脅威は、リアルタイム中継型のフィッシング攻撃など、昨今の脅威動向等を踏まえ最新化。

No.	主な脅威	脅威の概要	対策例
1	オンライン上でのパスワードの推測	総当たりやパスワードリスト等により繰り返しログインを試行することで、なりすましを行う	パスワードの複雑性の確保、一定時間あたりの認証回数の制限、多要素認証の採用
2	盗聴・リプレイ攻撃	通信を盗聴し、パスワード等の認証情報を窃取することでなりすましを試みる、同じ内容を再送信することでなりすましを行う	通信の暗号化、チャレンジレスポンス方式の採用、nonceの導入、ワンタイムパスワードの採用
3	パスワードや認証器の盗用	他サービスから漏えいしたパスワード、盗難したICカード等を用いてなりすましを行う	多要素認証の採用
4	フィッシング攻撃	利用者を偽のサイトに誘導し、入力されたパスワード等を攻撃者が窃取したり、 正規のサイトにリアルタイムに中継 したりすることで、なりすましを行う	フィッシング耐性 を有する認証技術の採用 ※ ワンタイムパスワード等はリアルタイム中継型への耐性を有さない点に留意
5	暗号鍵の不正な取り出し・複製	秘密鍵が格納されたデバイスに対し、物理的な解析やサイドチャンネル攻撃等を行うことにより、秘密鍵を不正に取り出そうとする	耐タンパ性を有するハードウェアの利用等

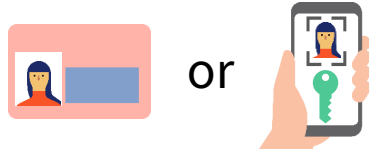
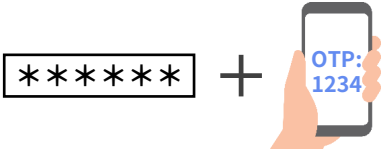

当人認証保証レベルの見直し

- 当人認証保証レベルは、フィッシング攻撃など最新の脅威動向、技術動向、国民向けの行政手続等において想定されるリスク等を考慮し、**脅威耐性の観点から各レベルの対策基準を見直し。**

保証レベル	脅威への耐性要件				
	オンライン上でのパスワード推測	盗聴・リプレイ攻撃	パスワードや認証器の盗用	フィッシング攻撃	暗号鍵の不正な取り出し・複製
当人認証保証レベル3	必須	必須	必須 ※単要素の盗用への耐性	必須 ※すべての利用者に対しフィッシング耐性のある手法を強制する	必須
当人認証保証レベル2	必須	必須	必須 ※単要素の盗用への耐性	推奨 ※希望する利用者に対しフィッシング耐性のある手法を提供する	必須 ※公開鍵認証の場合のみ
当人認証保証レベル1	必須	必須	不要	不要	不要

当人認証保証レベルの見直し（該当する手法例）

- それぞれの当人認証保証レベルに該当する手法例は以下のとおり。

保証レベル	該当する手法例 (代表的なもの)	補足
<p>当人認証 保証レベル3</p>	<p>フィッシング耐性を有する多要素認証 例)</p> <ul style="list-style-type: none"> マイナンバーカードの利用者証明 パスキー 	<p>フィッシング耐性の有無は、サービス側の実装にも依存することに注意。</p>
<p>当人認証 保証レベル2</p>	<p>フィッシング耐性を有さない多要素認証 例)</p> <ul style="list-style-type: none"> パスワード認証 +ワンタイムパスワード認証 	<p>左記の手法に加えて、希望する利用者にはフィッシング耐性を有する手法を提供できるようにする必要がある。</p>
<p>当人認証 保証レベル1</p>	<p>単要素認証（又は多要素認証） 例)</p> <ul style="list-style-type: none"> パスワード認証 ワンタイムパスワード認証 USB接続型セキュリティキー 	<p>—</p>

2. 当人認証手法の具体例

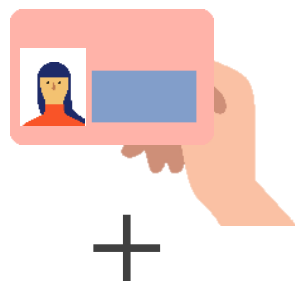
- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

1) 実物のマイナンバーカード（利用者証明）

実物のマイナンバーカード（利用者証明）の概要と脅威耐性

- マイナンバーカードの「利用者証明用電子証明書」を用いることで、Webサイト等へのログイン時において、公開鍵認証による本人認証を行うことができる。適切なフィッシング対策（mTLS、ドメイン名の制限等）を講じることで、[当人認証保証レベル3](#)の本人認証を実現できる。

マイナンバーカード
：所有物認証



利用者証明用暗証番号
(数字4桁)
：知識認証

No.	脅威	本手法による耐性
1	オンライン上でのパスワードの推測	パスワード等を利用しないため攻撃を受けない (暗証番号はオンライン上での推測攻撃を受けない)
2	盗聴・リプレイ攻撃	TLSによる通信の暗号化、チャレンジレスポンス方式等により対策
3	パスワードや認証器の盗用	利用者証明用電子証明書の利用時には暗証番号が必要であるため、知識+所有による多要素認証によって対策
4	フィッシング攻撃	mTLS、接続先ドメイン名の制限等により対策
5	暗号鍵の不正な取り出し・複製	マイナンバーカードのICチップの耐タンパ性により対策

1) 実物のマイナンバーカード（利用者証明）

実物のマイナンバーカード（利用者証明）の考慮事項

「基本的な考え方」の観点 (ガイドライン本編より)	考慮事項
事業目的の遂行 公平性	<ul style="list-style-type: none">マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
プライバシー	<ul style="list-style-type: none">特筆すべき考慮事項はない。
アクセシビリティ 及びユーザビリティ	<ul style="list-style-type: none">マイナンバーカードの暗証番号を覚えていない方への考慮が必要である。
セキュリティ	<ul style="list-style-type: none">暗証番号とともにマイナンバーカードの盗用や貸し借りが行われた場合は、第三者による不正ログインを検知できない。
その他	<ul style="list-style-type: none">この機能の取扱いは、公的個人認証法に基づく必要がある。

2. 当人認証手法の具体例

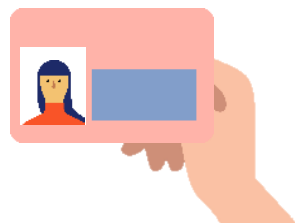
- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

2) 実物のマイナンバーカード（利用者証明（かざし利用））

実物のマイナンバーカード（利用者証明（かざし利用））の概要と脅威耐性

- マイナンバーカードの「利用者証明用電子証明書」は、対面等の特定の条件下において、暗証番号の入力を必要としない利用※が可能であり、これを「かざし利用」という。 ※初回利用時は、利用者証明用暗証番号の入力が必要。
- 単要素認証に該当し、[当人認証保証レベル1](#)の当人認証を実現できる。

マイナンバーカード
：所有物認証



No.	脅威	本手法による耐性
1	オンライン上でのパスワードの推測	—（オンラインでは利用できない）
2	盗聴・リプレイ攻撃	—（オンラインでは利用できない）
3	パスワードや認証器の盗用	マイナンバーカードを盗用された場合の耐性は有さない
4	フィッシング攻撃	—（オンラインでは利用できない）
5	暗号鍵の不正な取り出し・複製	マイナンバーカードのICチップの耐タンパ性により対策

2) 実物のマイナンバーカード（利用者証明（かざし利用））

実物のマイナンバーカード（利用者証明（かざし利用））の考慮事項

「基本的な考え方」の観点 (ガイドライン本編より)	考慮事項
事業目的の遂行 公平性	<ul style="list-style-type: none">マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
プライバシー	<ul style="list-style-type: none">特筆すべき考慮事項なし
アクセシビリティ 及びユーザビリティ	<ul style="list-style-type: none">「かざし利用」であっても、初回利用時には暗証番号入力が必要であるため、マイナンバーカードの暗証番号を覚えていない方への考慮が必要である。
セキュリティ	<ul style="list-style-type: none">2回目以降は暗証番号入力が必要ないため、マイナンバーカードが盗用された場合のリスクの考慮が必要である。
その他	<ul style="list-style-type: none">この機能の取扱いは、公的個人認証法に基づく必要がある。かざし利用には、デジタル庁が提供する「マイナンバーカードかざし利用クライアントソフト」が必要である。

2. 当人認証手法の具体例

- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

3) スマートフォンのマイナンバーカード（利用者証明）

スマートフォンのマイナンバーカード（利用者証明）の概要と脅威耐性

- スマートフォンのマイナンバーカードの「利用者証明用電子証明書」を用いることで、実物のマイナンバーカードと同じく、公開鍵認証による本人認証を行うことができる。適切なフィッシング対策（mTLS、ドメイン名の制限等）を講じることで、[本人認証保証レベル3](#)の本人認証を実現できる。

スマートフォンの
マイナンバーカード
：所有物認証



+

スマートフォンで実行される本人認証
：顔認証、指紋認証等



No.	脅威	本手法による耐性
1	オンライン上でのパスワードの推測	パスワード等を利用しないため攻撃を受けない (暗証番号はオンライン上での推測攻撃を受けない)
2	盗聴・リプレイ攻撃	TLSによる通信の暗号化、チャレンジレスポンス方式等により対策
3	パスワードや認証器の盗用	利用者証明用電子証明書の利用時には顔認証、指紋認証等が必要であるため、多要素認証によって対策
4	フィッシング攻撃	mTLS、接続先ドメイン名の制限等により対策
5	暗号鍵の不正な取り出し・複製	スマートフォン用の利用者証明用電子証明書は、スマートフォンの安全な領域に格納され、不正な取り出しや電子的な複製攻撃への耐性を備える

3) スマートフォンのマイナンバーカード（利用者証明）

スマートフォンのマイナンバーカード（利用者証明）の考慮事項

「基本的な考え方」の観点 (ガイドライン本編より)	考慮事項
事業目的の遂行 公平性	<ul style="list-style-type: none">マイナンバーカードを保有していない方、暗証番号を覚えていない方、紛失中の方などの存在を考慮し、事業目的や公平性の観点から必要と判断される場合には、他の手法との併用や例外措置を検討する必要がある。
プライバシー	<ul style="list-style-type: none">特筆すべき考慮事項はない。
アクセシビリティ 及びユーザビリティ	<ul style="list-style-type: none">実物のマイナンバーカードと比べ、カードの読み取りが必要ない。また、暗証番号入力についても生体認証等で代替できる。スマートフォンを保有しない方、操作に慣れていない方などへの配慮が必要である。
セキュリティ	<ul style="list-style-type: none">暗証番号とともにスマートフォンの盗用や貸し借りが行われた場合は、第三者による不正ログインを検知できない。
その他	<ul style="list-style-type: none">この機能の取扱いは、公的個人認証法に基づく必要がある。

2. 当人認証手法の具体例

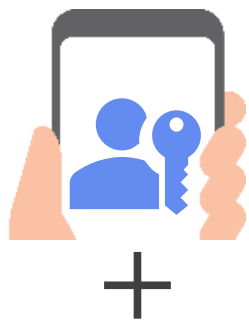
- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

4) パスキー

パスキーの概要と脅威耐性

- パスキーは、FIDO標準に基づきパスワードに代わる認証方式として普及が進められている手法である。フィッシング耐性を有しており、多要素認証として機能するため、[当人認証保証レベル3](#)の当人認証を実現できる。
- なお、デバイス間で同期できる方式は「同期パスキー」、特定のデバイスから取り出せない方式のものは「デバイス固定パスキー」と呼ばれる。

デバイスに格納されたパスキー
(秘密鍵)



パスキーの利用時に実行される
当人認証 (ローカルユーザー検証)
(生体認証又は知識認証)



No.	脅威	本手法による耐性
1	オンライン上でのパスワードの推測	パスワード等を利用しないため攻撃を受けない (暗証番号はオンライン上での推測攻撃を受けない)
2	盗聴・リプレイ攻撃	TLSによる通信の暗号化、チャレンジレスポンス方式等により対策
3	パスワードや認証器の盗用	パスキー利用時に生体認証又は知識認証による当人認証 (ローカルユーザー検証)を行うことで対策
4	フィッシング攻撃	パスキーがドメイン名と紐付けられる (Domain Name Binding) ことによりフィッシング耐性を有する (紐づけられたドメイン名以外では使用できない)
5	暗号鍵の不正な取り出し・複製	多くの場合、パスキーはデバイス内の安全な領域に格納される実装となっている。また、同期パスキーについては、エンドツーエンドでの暗号化により保護される。

4) パスキー

パスキーの考慮事項

「基本的な考え方」の観点 (ガイドライン本編より)	考慮事項
事業目的の遂行	以下の事項による事業目的や公平性への影響の考慮が必要。 <ul style="list-style-type: none">• パスキーを利用可能なデバイスの所持が前提となる• 複数の利用者が端末を共用するケースでの利用は困難である
公平性	
プライバシー	<ul style="list-style-type: none">• 特筆すべき考慮事項はない。
アクセシビリティ 及びユーザビリティ	<ul style="list-style-type: none">• パスワード認証など他の認証手法と比べて比較的新しい手法であるため、利用者の理解度・認知度には留意が必要である。
セキュリティ	<ul style="list-style-type: none">• 同期パスキーの場合、同期に利用するクラウドサービスのアカウントが乗っ取られた場合のリスクの考慮が必要である。• 利用者がパスキーにアクセスできなくなった場合のアカウント回復方法は、アカウントの乗っ取り等の攻撃に悪用されるリスクを考慮した手法やプロセスを設計する必要がある。
その他	<ul style="list-style-type: none">• 利用者側のデバイスやOS、同期に利用するクラウドサービスによって、実装の差異が生じる点に留意が必要である。 (例：デバイス内に保存される秘密鍵の保護方法、ローカルユーザー検証の挙動、同期パスキーのバックアップ可否やリカバリ方法などは、利用者側の環境等に依存する。)

2. 当人認証手法の具体例

- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

5) パスワード認証

パスワード認証の概要と脅威耐性

- パスワード認証は、あらかじめ登録しておいた文字列によって利用者を認証する方式である。
- 知識認証に該当し、単独で用いる場合は[当人認証保証レベル1に該当](#)する。

パスワード認証

No.	脅威	本手法による耐性
1	オンライン上でのパスワードの推測	パスワードの複雑性の確保、一定時間当たりの認証試行回数の制限等により対策
2	盗聴・リプレイ攻撃	TLSによる通信の暗号化により対策
3	パスワードや認証器の盗用	耐性なし
4	フィッシング攻撃	耐性なし
5	暗号鍵の不正な取り出し・複製	— (暗号鍵は利用しない)

5) パスワード認証

パスワード認証の考慮事項

「基本的な考え方」の観点 (ガイドライン本編より)	考慮事項
事業目的の遂行	<ul style="list-style-type: none">特筆すべき考慮事項はない。
公平性	
プライバシー	<ul style="list-style-type: none">特筆すべき考慮事項はない。
アクセシビリティ 及びユーザビリティ	<ul style="list-style-type: none">パスワードの設定や管理は一般に煩雑であり、ユーザビリティが高い方式とはいえない。
セキュリティ	<ul style="list-style-type: none">利用者を偽のサイトに誘導してパスワードを窃取するフィッシング攻撃に対して脆弱である。利用者側が複数のサービスで同じパスワードを使い回すことが少なくなく、他のサービスから漏えいしたパスワードによって不正アクセスを受けるリスクがある。パスワードの使い回しが原因であっても、サービス提供側に不正アクセスについての一定の責任が問われるケースもある。しかしながら、パスワードの使いまわしはサービス側で検知することはできないため、根本的な対策は難しい。
その他	<ul style="list-style-type: none">実装に関する詳細な要求事項は、NIST SP 800-63B-4を参考とすること。パスワードマネージャーの利用を阻害する実装は、ユーザビリティを低下させるだけでなくフィッシング攻撃に対しても脆弱となる。利用者がパスワードマネージャーを円滑に利用できる実装とすべきである。

5) パスワード認証

(参考) NIST SP 800-63-4でのパスワードに関する要件 (一部抜粋・要約)

- パスワード認証の実装においては、NIST SP 800-63B-4「3.1.1. Passwords」における要求事項を参考とされたい。
- 参考とすべきNISTの要求事項の一部を抜粋・要約して以下に示す。

項目	参考とすべき要求事項 (一部抜粋・要約)
パスワードの長さ	<ul style="list-style-type: none">• 単要素認証として利用する場合は15文字以上、多要素認証の一要素として利用する場合は8文字以上としなければならない。• 設定可能なパスワードの最大長は少なくとも64文字とすべき。
異なる文字種の混在を要求することの禁止	<ul style="list-style-type: none">• 異なる文字種の混在などを要求してはならない。
定期的な変更の禁止	<ul style="list-style-type: none">• 利用者に対して、定期的なパスワードの変更を求めてはならない。 ただし、パスワードが侵害された証拠がある場合には、パスワードの変更を求めなければならない。
秘密の質問等の禁止	<ul style="list-style-type: none">• パスワードを思い出すための「ヒント」や「秘密の質問」(「最初に飼ったペットの名前は」)は実装してはならない。
パスワードマネージャー及び自動入力の許可	<ul style="list-style-type: none">• パスワードマネージャー及び自動入力機能(オートフィル機能)の利用を許可しなければならない。パスワードの貼り付け(ペースト)についても、自動入力ができない場合を考慮して許可すべきである。

2. 当人認証手法の具体例

- 1) 実物のマイナンバーカード（利用者証明）
- 2) 実物のマイナンバーカード（利用者証明（かざし利用））
- 3) スマートフォンのマイナンバーカード（利用者証明）
- 4) パスキー
- 5) パスワード認証
- 6) パスワード認証＋ワンタイムパスワード

6) パスワード認証+ワンタイムパスワード

パスワード認証+ワンタイムパスワード認証の概要と脅威耐性

- パスワード認証に加えて、ワンタイムパスワードによる認証を組み合わせる方式。ワンタイムパスワードは、スマートフォンの認証アプリ等によって生成する方法や、SMSや電子メールなどの別経路で送信する方法がある。
- 知識認証+所有物認証による多要素認証とみなせ、[当人認証保証レベル2に該当する](#)。フィッシング攻撃への耐性は有さない。また、ワンタイムパスワードの生成又は送信方法によっても脅威や留意事項が異なる。



No.	脅威	本手法による耐性
1	オンライン上でのパスワードの推測	パスワード認証の複雑性の確保、一定時間当たりの認証試行回数の制限等により対策
2	盗聴・リプレイ攻撃	TLSによる通信の暗号化により対策
3	パスワードや認証器の盗用	知識認証+所有物認証による多要素認証により対策
4	フィッシング攻撃	耐性なし
5	暗号鍵の不正な取り出し・複製	— (暗号鍵は利用しない)

6) パスワード認証+ワンタイムパスワード

パスワード認証+ワンタイムパスワード認証の考慮事項

「基本的な考え方」の観点 (ガイドライン本編より)	考慮事項
事業目的の遂行	<ul style="list-style-type: none">ワンタイムパスワードの利用環境（スマートフォンの認証アプリ、携帯電話番号、電子メールアドレス等）が必要となることによる影響を考慮すること。
公平性	
プライバシー	<ul style="list-style-type: none">ワンタイムパスワードを送信するために利用者の連絡先情報を取得する際は、その利用目的を明確に通知する、目的外利用を統制するなどの考慮が必要。
アクセシビリティ 及びユーザビリティ	<ul style="list-style-type: none">ワンタイムパスワードの入力の手間が生じることへの考慮が必要。SMSを用いる場合は、認証コードをソフトウェアキーボードに表示し、ワンタップで入力できる仕組みの利用を検討すべき。
セキュリティ	<ul style="list-style-type: none">利用者を偽のサイトに誘導してパスワードやワンタイムパスワードを窃取するフィッシング攻撃に対して脆弱である。ワンタイムパスワードの生成又は送信手段によって異なる事項への考慮が必要（次頁を参照）。
その他	<ul style="list-style-type: none">特になし

6) パスワード認証+ワンタイムパスワード

ワンタイムパスワードの方式による考慮事項

方式	ユーザの所有するデバイスで Time-based OTPを生成	ユーザの連絡先に対して認証コードを送信 (Out-of-band Authenticator)	
	スマートフォンの 認証アプリで生成	SMSにより 認証コードを送信	電子メールにより 認証コードを送信
考慮すべき リスク	<ul style="list-style-type: none"> 認証アプリに紐づくアカウントが乗っ取られ、攻撃者にワンタイムパスワードが窃取される ワンタイムパスワードの生成に係るシード値が漏洩し、攻撃者側の環境でワンタイムパスワードを生成される 	<ul style="list-style-type: none"> SIM スワッピング攻撃により利用者が携帯電話番号を不正に奪取される 第三者によってSMS等の認証代行が行われる 通信が暗号化されておらず、経由する通信網に脆弱なプロトコルが用いられていた場合にSMSが盗聴される 	<ul style="list-style-type: none"> 電子メールアカウントが乗っ取られ、認証コードが奪取される 電子メールの中継中の盗聴により認証コードを奪取される メールの自動転送、メールアカウントの共有などが不適切に行われる
その他の 考慮事項	<ul style="list-style-type: none"> ハードウェアベースのTOTPトークンも存在するが、トークンの物理的な配付が必要となるため、利用者が不特定多数となる行政手続等には利用しにくい 	<ul style="list-style-type: none"> SMSではなく音声通話によって認証コードの授受を行う方式についても、SMSと同様のリスク考慮が必要 	<ul style="list-style-type: none"> 電子メールを利用することが標的型攻撃の起点になり得る点の考慮も必要

WebOTP APIを利用したSMSでの認証コード送信について

WebOTP APIの概要・メリット

- ブラウザのWebOTP APIを利用することで、SMSで送信する認証コードをWebサイトのドメイン名と紐づけることができる。
- 紐づけられたドメイン名のWebサイトでのみ認証コードのオートフィル候補が表示され、**利用者はワンタップでコード入力が可能**になる。また、フィッシングサイトに対しては認証コードの入力候補が表示されないため、**利用者側がフィッシングを検知しやすくなる**と期待される。
- 上記のようなメリットを踏まえ、SMSでの認証コード送信を採用する場合には積極的に利用すべきである。

フィッシング攻撃への耐性について

- 認証コードの入力候補が表示されない場合でも、**利用者がその仕組みを認識していないと、手入力によってコードが入力され得る。**
- また、利用者がWebOTP APIに対応していないブラウザを利用している場合、SMSを受信する端末と認証コードを入力する端末が別の場合など、**認証コードの手入力が必要となる場面は残存**するため、フィッシング攻撃のリスクを軽減する効果はあっても、**確実な対策とはならない点に留意が必要**である。
(後述する「フィッシング耐性」には該当しない。)

2. 当人認証手法に関するその他の解説（コラム）

コラム1) フィッシング耐性について

コラム：フィッシング耐性について

- 当人認証保証レベル2及び3において求める「フィッシング耐性」とは、フィッシングサイトへ認証情報が渡ることを、利用者の注意に依存することなく防ぐことができる仕組み（プロトコル）を利用することを意味する。したがって、パスワードや乱数等を手動で入力する方法は、フィッシング耐性を有さない。
- 技術的な要求事項については、NIST SP 800-63B-4を参考とすること。以下にその概要を示す。

No.	分類	概要・解説	例
1	チャンネルバインディング (Channel Binding)	<p>TLSのチャンネル識別子と利用者の認証器出力とを、署名等によって暗号的に紐づけることで、フィッシングサイトによる中継を防止する。</p> <p>もし認証器出力がフィッシングサイトによって正規のサイトに中継された場合でも、紐づけられたTLSのチャンネル識別子が異なることによってフィッシング攻撃を検知できる。チャンネル識別子が偽造された場合は署名検証によって検知できる。</p>	電子証明書を格納したICカードを用いたクライアント認証 TLS (RFC8446)
2	検証者名バインディング (Verifier Name Binding)	<p>検証者の識別子（ドメイン名など）と利用者の認証器出力とを紐づけることで、フィッシングサイトによる中継を防止する。</p> <p>紐づけの方法は、検証者の識別子を使用して認証情報を選択する、検証者の識別子を使用して認証情報を導出する、検証者識別子を使用して認証器出力に暗号的に署名するなどの方法がある。</p>	FIDO2に基づく認証器によって使用されるWebAuthn

デジタル庁
Digital Agency