本人確認とは

2025-09　　デジタル庁　トラストタスクフォース

デジタル庁
Digital Agency

アイデンティティ管理の重要性

- サイバー犯罪の多くの事例はアイデンティティ管理（IAM：Identity and Access Management)の問題に起因
  - 脆弱性の悪用等よりもさらに多い
- IAMの失敗につながるもの
  - フィッシングによる認証情報（パスワード等）の盗用。リアルタイムフィッシングでは多要素認証でも攻撃を防げない場合あり
  - 券面が偽造された身分証の活用
  - ソーシャルエンジニアリング
- 安全性とプライバシー・使いやすさのバランス

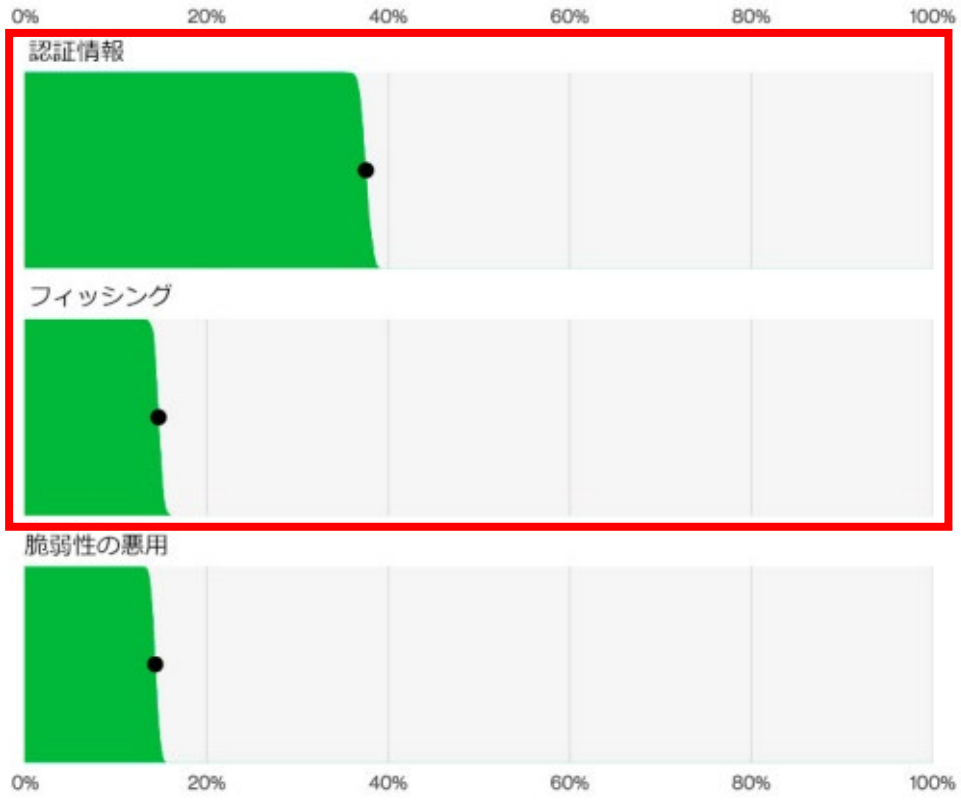


図1. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な侵入手段（n=6,963）

⇒「正しく利用する／させるため」の仕組み、枠組みが重要

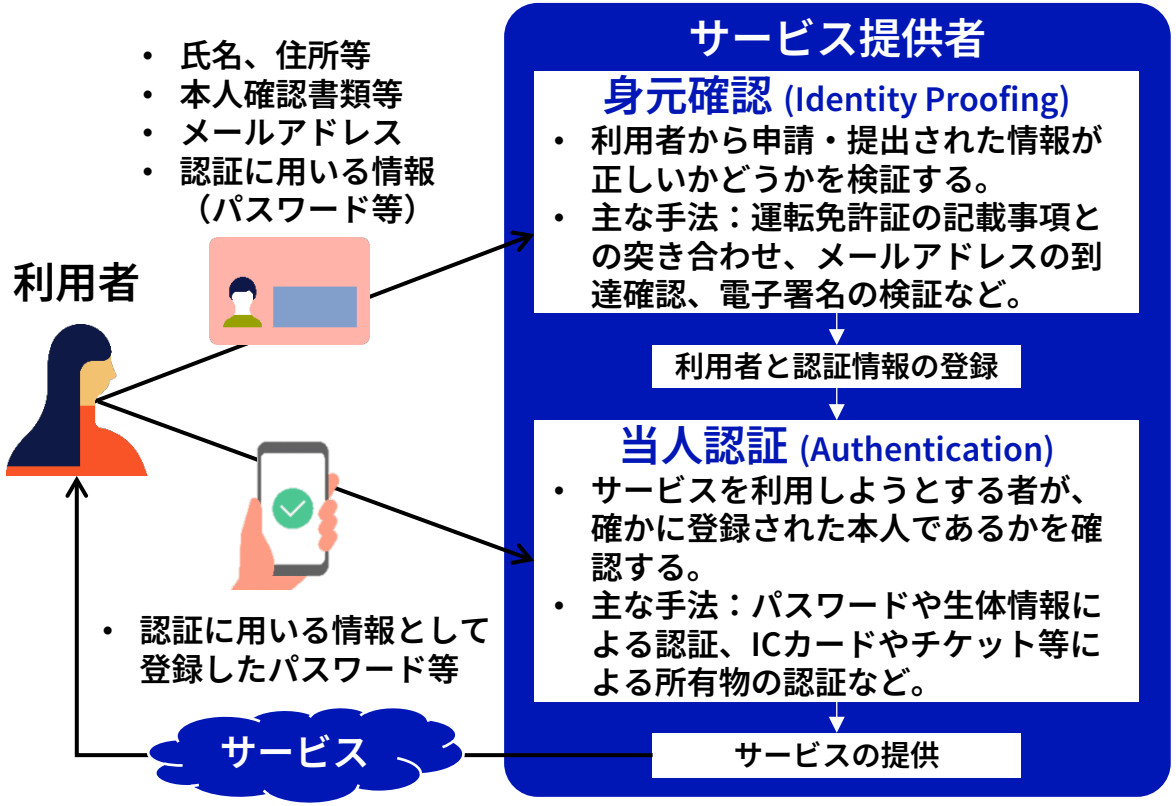
Verizon「2024年度 DBIR データ漏洩/侵害調査報告書」https://www.verizon.com/business/resources/ja/reports/2024-dbir-data-breach-investigations-report.pdf

本人確認（身元確認・当人認証）：アイデンティティ管理の中心

本人確認の主な構成要素として、利用者の身元を特定して利用者として登録する「身元確認 (Identity Proofing)」と、既に登録された本人であることを確認する「当人認証 (Authentication)」の2つ*がある。

※それぞれの要素単体（とくに身元確認）について「本人確認」と呼ぶ場合もあるが、本スライドにおいては、これら２つの要素を総称したものを「本人確認」、個々の要素を指す際には「身元確認」「当人認証」と区別する。

身元確認・当人認証のレベルは、プライバシーやユーザビリティの観点も踏まえると、いずれも「高ければよい」ものではなく、サービスの特性やリスクに応じて選択される。



①「身元確認 (Identity Proofing)」

サービス提供に必要な利用者情報を収集・検証する行為（利用者情報：氏名、住所、メールアドレス等）

- サービス利用申請、ユーザ登録など、サービスの初回利用時に行われることが一般的
- 収集する情報や検証内容（改ざん有無の確認等）は、サービスによって異なる

②「当人認証 (Authentication)」

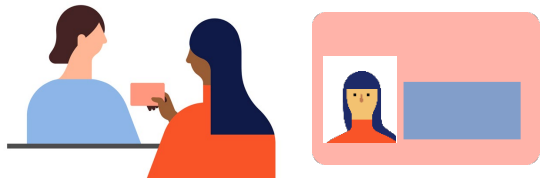
サービスを利用しようとする者が「あらかじめ登録された本人」であることを確認する行為

- Webサイトへのログイン時のパスワード、パスキー等による認証、マイナンバーカードを利用した認証など
- なりすまし時のリスク等に応じて、認証強度が選択される（多要素認証など）

本人確認の基本的要素を定義

- 本人確認の構成要素である「身元確認」と「当人認証」を明確に定義し、概念図を示す。
- また、身元確認や当人認証を他者に依拠して実現する「フェデレーション」という概念を、今回の改定において新たに定義する。

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。

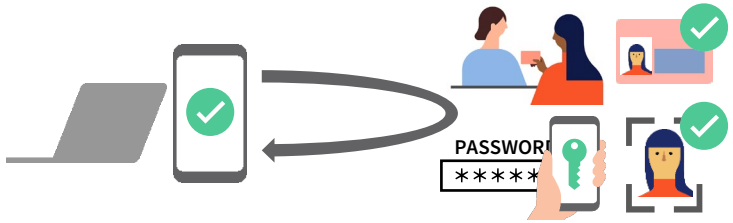
具体的には、申請者の属性情報を収集することで、申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認する。

当人認証（Authentication）

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と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）



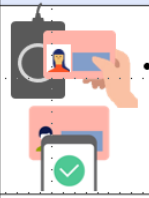
身元確認や当人認証を、他者に依拠して実現すること。

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。

身元確認の保証レベル ＝ IAL（Identity Assurance Level）

- **身元確認の強度（これを身元確認の「保証レベル」という。）は、IALという尺度で表される。**
- **定義は各国のガイドライン等で異なるが、我が国では利用可能な本人確認書類の普及状況、本人確認書類の偽造による被害状況等を考慮し、IAL1～IAL3の3段階を定義。**
- **IALは高ければ良いものではない。必要な情報が多いとサービスを受けられない人が出て公平性が損なわれる恐れがある。またプライバシーの観点からは必要以上の個人情報を収集すべきではない。当該サービスのリスクに応じた適切なIALを選択することが重要である。**

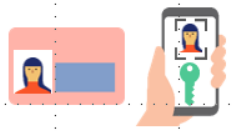
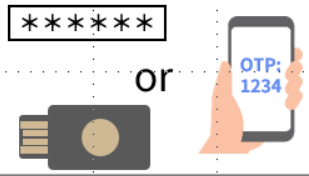
IALのレベル別要件のイメージ（DS-511から一部を抜粋、要約）

保証レベル	保証レベルの位置づけ	
	本人確認書類の検証手法	本人確認書類が申請者のものであることの検証方法
IAL3	 ・ICチップ等による**デジタル的な検証を必須**とし、**偽造や改ざんに対する厳格な耐性**を確保するレベルとする。	暗証番号: ＊＊＊＊ ・本人確認書類の盗用に対し、**対面での容貌の確認、非対面での容貌の確認**又は**暗証番号による検証**を必須とする。 ・本人確認書類の貸し借りに対しては、対象手続のリスクに応じた個別検討を行うこととする。
IAL2	・本人確認書類の**対面での物理的な検査等も許容**する。ただし検証強度を考慮しカメラ越しや複写物による検査（非対面で物理検査）は不可とし、一定の耐性を確保する。	
IAL1	・保証レベル2までの手法に加えて、**非対面での物理的検査（カメラでの撮影、複写物の郵送等）も許容**する。偽造・改ざんへの簡易的な耐性をもつレベルとして位置付ける。	・保証レベル2までの手法に加えて、**住所への到達確認による検証**も許容する。（本人確認書類に記載されている住所に居住していることの確認をもって、本人確認書類との紐づきを検証する手法）

当人認証の保証レベル ＝ AAL（Authenticator Assurance Level ）

- 当人認証の強度も同様に、AALという尺度で表される。我が国では米国NISTを参考として3段階を定義。
- 一般に、AALが高くなるほど手順が複雑になり利便性が低下する。また、認証に用いる機器等を用意できない者がいる場合など公平性が損なわれる恐れもある。IALと同様に「高ければよい」ものではなく、適切な保証レベル選択が必要。

AALのレベル別要件のイメージ（ DS-511から一部を抜粋、要約）

保証レベル	対策基準	
	認証要素	脅威への耐性要件
AAL3	**公開鍵認証を含む多要素認証** 例） ・ 暗証番号付きのICカード ・ パスキー 	・ **フィッシング耐性（必須）** ＋ ・ 保証レベル2の耐性
AAL2	**多要素認証** 例） ・ AAL3の手法 ・ パスワード ＋ワンタイムパスワード 	・ **フィッシング耐性（推奨）** ・ **認証器等の盗用に対する耐性** ＋ ・ 保証レベル1の耐性
AAL1	**単要素認証**（又は多要素認証） 例） ・ AAL2の手法 ・ パスワード ・ ワンタイムパスワード 	・ 盗聴 ・ リプレイ攻撃 ・ オンライン上での認証情報の推測

IALとAALの組合せは、サービスの性質に応じてそれぞれ異なる

- IALとAALはいずれも「高ければよい」ものではない（不必要な個人情報の収集によるプライバシー侵害、手続きの複雑化によるユーザビリティの低下、必要な機器の増加による公平性の低下など）ため、サービスの特性やリスクに応じて選択する。
- また、IALとAALの高低は必ずしも連動しない。「IALは高レベルが必要だが、AALは低くてもよい」サービスもあれば、その逆の場合もある。

（参考）IALとAALの組合せと代表的サービス例

AAL高

有償クラウドサービス等
- 利用者が誰であろうと、請求さえできればよい → IAL低
- 不正ログイン時には金銭的被害が発生しうる、機微情報の漏洩など影響が大きいため認証は強固に → AAL高

個人情報や機密情報を扱うサービス等
- 個人情報を扱うため確実な身元確認が必要 → IAL高
- 不正ログイン時には情報漏洩、サービスの不正利用等の影響が大きいため認証は強固に → AAL高

IAL低 ―――――――――――――――――――――――――――――――― IAL高

機微な情報を扱わない無料サービス等
- 無償であるため誰でも良いし、複数登録してもよい → IAL低
- 不正ログインの影響も限定的である → AAL低

申請サービス等
- 多重申請や不正申請を防止しなければならない → IAL高
- 申請サービスであるため不正ログインされても個人情報は閲覧されず、勝手に申請されても後段のチェックで被害が起きにくいなど、なりすまし等の影響が小さい → AAL低

AAL低

デジタル庁

Digital Agency