パソコンと本人確認

2013年9月28日

豊川　洋

本人確認とは？

https://www.gov-online.go.jp/useful/article/201610/1.html#section1

- 自分が自分であることを証明する手段
  - マイナンバーカード
  - 自動車免許証
  - パスポート（**2020年2月3日以前**のもの）
    - 本人が対面で証明する手段
      1. 自分の顔写真があること
      2. 住所、名前、生年月日が記載され、本人がそのことを確認できること
    - 本人が対面でないときに証明する手段は？

本人が対面でないときに確認する手段は？

- 本人しか持っていない手段で確認
  - 現在では、携帯電話（スマートホン）を各自一台を所有している。
    - その電話番号は、一台一台に割り当てられていて本人確認の手段になりうる。
  - また、メールアドレスも個人が一つ以上のアドレスを所有しており、本人確認の手段になりうる。
    - 但し、共通アドレス（共有アドレス（例えば家族間の））は、本人確認の手段には不適。
  - 本人が所有するキャリア（パソコン、携帯電話、タブレットなど）
    - 一台一台にIPアドレスが割り当てられている。

芦屋市役所の本人確認の書類

shimin/documents/honinkakuninshoruiichiran.pdfhttps://www.city.ashiya.lg.jp/

- 原則（官公所発行の写真付き証明書）
  - 運転免許証
  - マイナンバーカード
  - パスポート
  - 写真付き住民基本台帳
  - 写真なし住民基本台帳（暗証番号で本人確認出来るとき）
- それ以外は2種類必要
  - 健康保険証
  - 後期高齢者医療被保険者証
  - 介護保険証
  - 年金手帳
    - 氏名＋住所、氏名＋生年月日等が分かるもの

本人確認と多要素認証との違い
（セキュリティに関する用語）

- 本人確認
  - 身元を確認することです。例えば、あなたがあるサービスに登録する場合、**身分証明書**や**免許証**などの**公的な書類**を提出して、自分が本人であることを証明することが必要です。
- 多要素認証
  - ログイン時にパスワードの他に、**別の認証方法を追加**することで、より**高いセキュリティを実現**する方法です。例えば、ログイン時にパスワードとSMSで送信されたコードの2つの要素を入力することで、本人確認を行い、ログインすることができます。

多要素認証、二要素認証、二段階認証の違い

- 多要素認証とは
  - PC・サーバーへのアクセス時やクラウドサービスへのログイン時などに、**2つ以上の"要素"によって行う認証**を指します。
- 認証の**3要素**
  - **知識要素**
    - その人が知っている情報。例えば**ID/パスワード、PINコード、秘密の質問**など。
  - **所有要素**
    - その人が持っているものに付随する情報。例えば**携帯電話やスマートフォンを使ったSMS認証**やアプリ認証、ICカード、トークン（ワンタイムパスワードを生成する端末）などが挙げられます。
  - **生体要素**
    - その人の身体情報。**顔や指紋、虹彩（目の膜）、声紋、静脈**のほか、**位置情報**も生体要素に含まれます。

二要素認証と二段階認証の違い

二要素の方が高いセキュリティ

- **二要素認証**
  - **２つの要素を使った本人認証のことです。多要素認証の一部といえます。**
- **二段階認証**
  - **認証の段階を2回経て認証しますが、要素の数は問われません。**
- 例えば、ID・パスワードでログインを行ったあと「秘密の質問」の答えを入力する認証方式があります。この方式では認証の段階を2つ踏むため"二段階認証"といえます。
- しかし、「パスワード」と「秘密の質問」はいずれも**知識要素**のため、一要素の認証です。
- 万一サイバー攻撃を受けた際は2つの知識要素が同時に流出する可能性も考えられることから、認証の"段階"が多ければ必ず認証が強固になるとはいえません。
- 二段階認証と二要素認証は混同されやすいのですが、"二段階認証"と紹介されていても、認証の要素は1つだけである場合もあります。
- 二段階認証であれば二要素認証でもあるとは限らないため注意が必要です。

追加情報

多要素認証とは

インターネット上で行う**本人確認方法**の1つで
複数の要素を組み合わせて確認する

- パスワード
- 暗証番号

- SMS認証
- アプリ認証

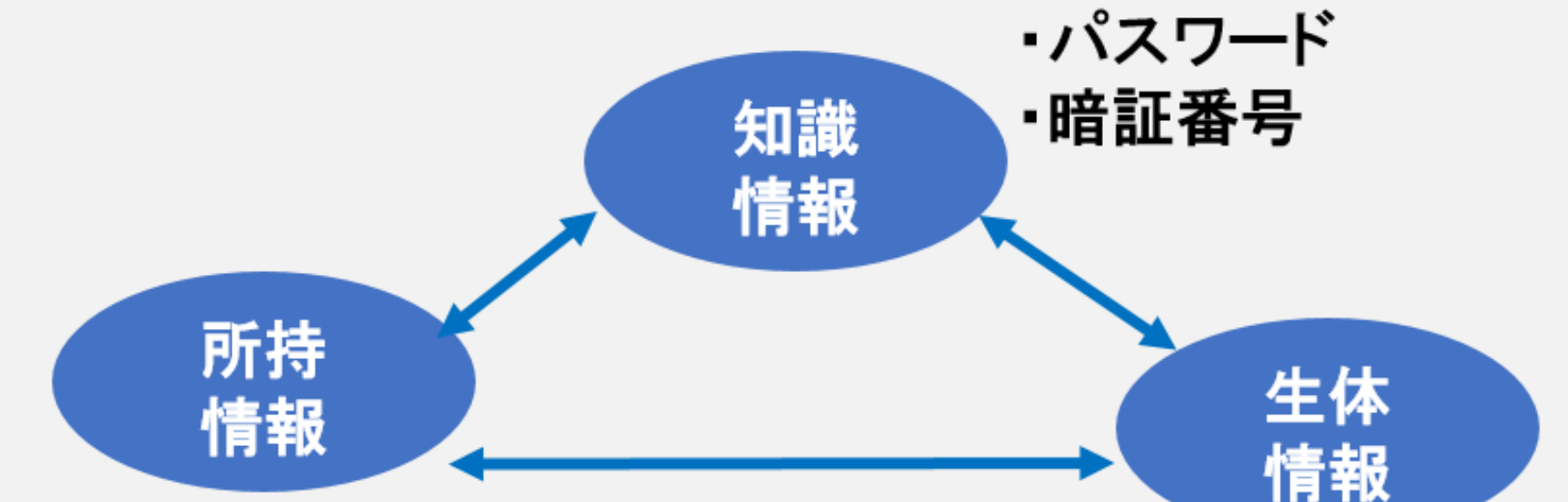
- 指紋認証
- 顔認証

セキュリティ強化に役立つ

アカウント侵害攻撃の 99.9% 以上をブロック

多要素認証とは

インターネット上で行う**本人確認方法**の1つで
複数の要素を組み合わせて確認する



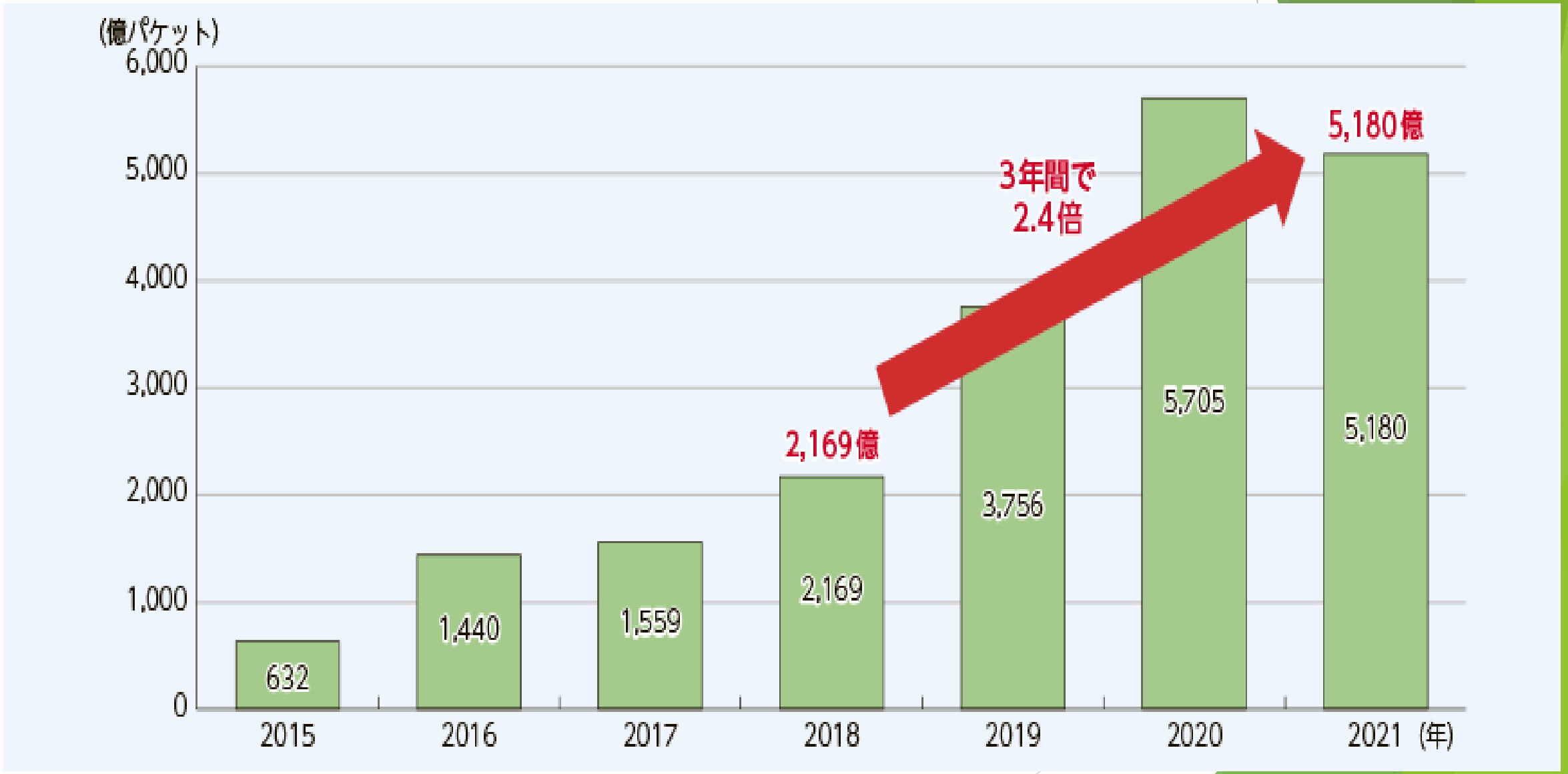
多要素認証が必要な理由

サイバー攻撃が増加している

パスワードでのセキュリティに限界が来ている

インターネットバンキングなど多要素認証が必要なシステムが増えた

【NICTERにおけるサイバー攻撃関連の通信数の推移】



多要素認証を導入するメリット

メリット1 セキュリティが向上する

メリット2 パスワードを覚える必要がなく利便性が上がる

メリット3 コンプライアンスが実現できる

⑤　被害発生口座に係る口座連携時の認証方法・資金移動業者等による取引時確認方法

（単位：口座数）

		資金移動業者等による取引時確認方法	
		他の事業者への依拠による取引時確認	資金移動業者等自らが取引時確認
口座連携時の認証方法	一要素認証	584（64%）	225（25%）
	多要素認証	68（8%）	30（3%）

○ 不正出金被害が発生した口座のうち銀行が資金移動業者の行う取引時確認の手法を把握している 907 口座についてみると、
・一要素認証により口座連携をしている口座は 809 口座（89%）、
・他の事業者への依拠による取引時確認を実施している口座は 652 口座（72%）、
・他の事業者への依拠による取引時確認を行い、一要素認証により口座連携している口座は 584 口座（64%）
となっている。

（注）多要素認証を導入しているが被害が発生した事案では、多要素認証の中でも他の方式と比べて堅牢性が劣ると考えられる認証方式を採用していたことが認められた。

多要素認証を導入するデメリット

デメリット1

導入や運用にコストがかかる

デメリット2

やり方によっては認証に時間がかかり効率性が下がる

多要素認証の導入がおすすめな理由

理由1

多要素認証導入・運用にかかるコストより
セキュリティ事故で起きる損害の方が大きい

理由2

現段階でのセキュリティ技術の中では
多要素認証の信頼性が高い

多要素認証を導入する時の注意点

注意点1

認証情報はきちんと保管し使いまわししない

注意点2

面倒でもログイン状態を維持しない

注意点3

多要素認証以外のセキュリティ対策を怠らない

多要素認証とは

インターネット上で行う**本人確認方法**の1つで
複数の要素を組み合わせて確認する

セキュリティ強化に役立つ

アカウント侵害攻撃の 99.9% 以上をブロック

多要素認証に使う情報は次の3つ

知識情報（その人だけが知っていること）	ID、パスワード、秘密の質問など
所持情報（その人だけが持っている物）	ICカード、スマートフォン、セキュリティキーなど
生体情報（その人の身体の特徴）	顔認証、指紋認証、網膜認証、静脈認証など