#02

二要素認証の必要性

2026年04月02日（木）

セキュリティコラム

琉球大学 UNIVERSITY OF THE RYUKYUS

「数秒の不便」が命と組織を救う。私たちが二要素認証（2FA）を手放してはいけない絶対的な理由

　IDとパスワードを入力した直後、スマートフォンを取り出して6桁の数字を確認し、それを制限時間内に入力する。あるいは、認証アプリを開いて「承認」ボタンをタップする。二要素認証（2FA）や多要素認証（MFA）を求められるたびに、「面倒だ」「不便だ」と感じる人は少なくないでしょう。

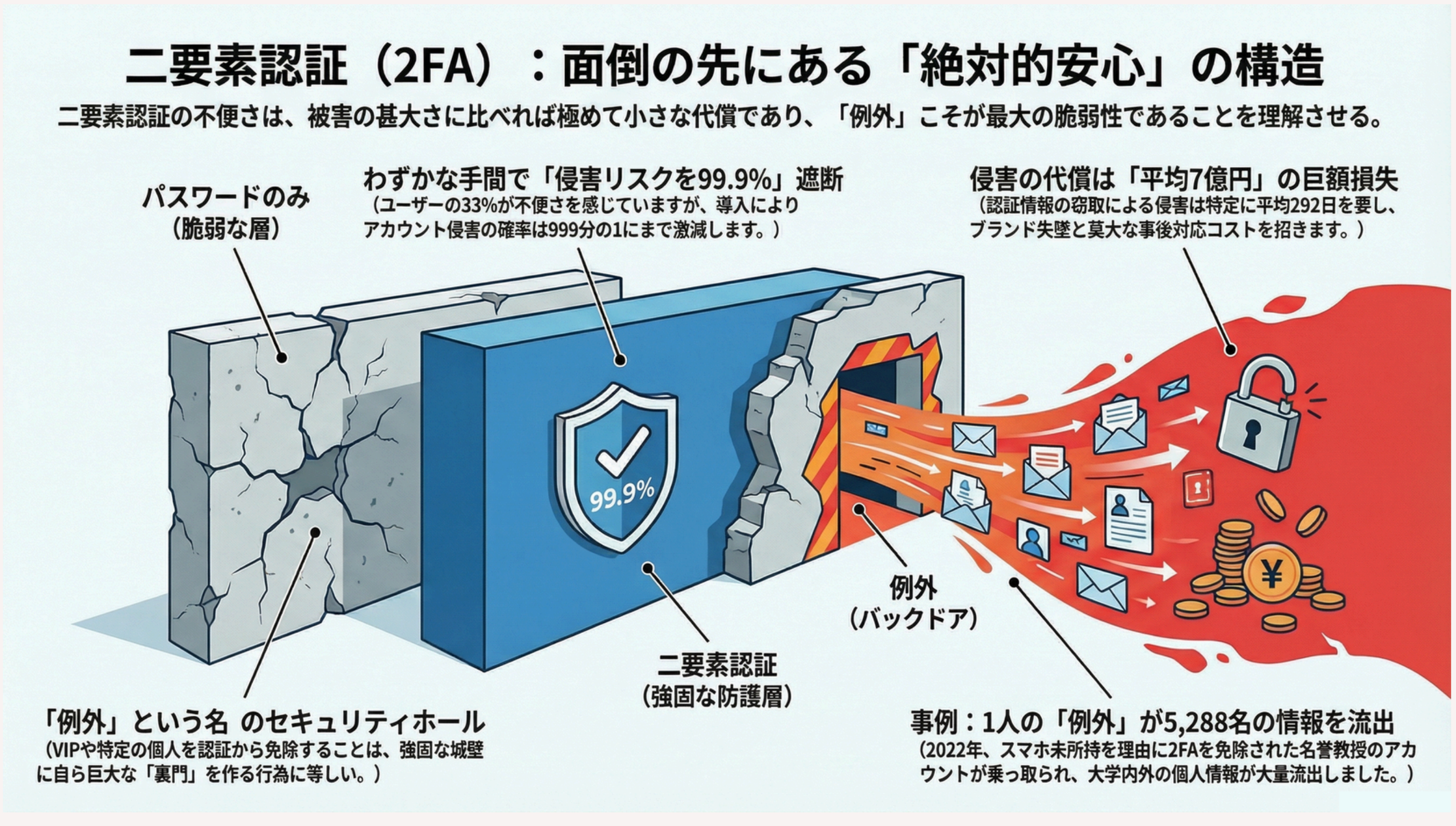
　実際、グローバルな調査でも33%の人が多要素認証を「煩わしい」と感じています。特に日本人はその傾向が強く、ワンタイムパスワードによるアカウント認証に不満を抱いている人は54%に上り、世界平均の39%を大きく上回っています。また、別の調査でも約4割のユーザーが「二段階認証は使いにくい」と回答しており、私たちの多くがこの追加の手順にストレスを感じているのが実情です。

　仕事に集中している時や、急いでシステムにログインしたい時に立ちはだかるこの「追加の手間」は、確かにユーザーの利便性を損なうものです。しかし、現代のサイバー脅威を前にして、私たちはこの一時的な不便さを「必須の代償」として受け入れなければなりません。

パスワード単体の脆弱性と、2FAの圧倒的な防御力

　パスワードだけに依存したセキュリティは、もはや「鍵のかかっていないドア」に等しい状態です。サイバー攻撃による不正アクセスの大部分は、使い回されたパスワードや、巧妙なフィッシングによって盗まれた情報から発生しています。

　一方で、二要素認証を導入するだけで、アカウントが侵害される確率は「999分の1」にまで劇的に低下します。また、多要素認証はアカウント乗っ取り攻撃の実に99.9%以上をブロックできるというデータもあります。パスワードという「知識」に、スマートフォンなどの「所持」という別次元の要素を組み合わせるだけで、攻撃者の侵入難易度は絶望的なまでに跳ね上がるのです。



【事例1】2FAがなかったために起きた152億円の悲劇

　この「たった一手間」を省いたがゆえに、壊滅的な被害を被った事例があります。 2026年2月、神奈川県の医療機関が大規模なランサムウェア攻撃の標的となりました。深夜、入院患者が緊急時に看護師を呼ぶための生命線である「ナースコール」が突然鳴らなくなり、システムが暗号化されたのです。攻撃者は患者約13万人と職員約1,700人分の個人情報を窃取し、日本円にして約152億円という異常とも言える巨額の身代金を要求しました。

　この大惨事の入り口となったのは、ナースコールシステムの「保守用VPN装置」でした。この機器には、IDとパスワードのみの単一要素認証しか設定されていませんでした。もしここに二要素認証が導入されていれば、攻撃者がパスワードを入手したとしても第2の認証を突破できず、不正侵入を未然に防ぐことができた可能性が極めて高いのです。

【事例2】「特権」と「例外」が招いた5000人の個人情報漏洩

　さらに恐ろしいのは、システムとして2FAを導入していても、「偉い人だから」「不便だから」という理由で適用を除外してしまうケースです。

　2022年12月に発覚した某地方県立大学における不正アクセス事案の経緯は以下の様なものでした

　同大学では、パスワードの入力に加えて、SMSや電話で確認コードを提示する「二要素認証」をセキュリティの原則としていました。しかし、ある名誉教授が「スマートフォン等を所持していない」と申し出たため、大学側は特例としてこの名誉教授のアカウントを二要素認証の適用から除外（免除）していました。

　二要素認証の保護が外されていたことに加え、この名誉教授が設定していたパスワードが短く、他のサイトでも使い回している簡単なものであったため、海外からの不正ログインを容易に許す結果となりました。

　乗っ取られた名誉教授のメールアカウントから、1,200件以上の不審な英文スパムメールが送信されました。さらに、教職員や学生、公開講座の受講者に加え、名誉教授のアドレス帳に登録されていた他大学や企業関係者の連絡先など、合計で5,288人分の個人情報（氏名、メールアドレス、所属部署、役職、電話番号など）が漏洩した可能性が判明しました。

「数秒の不便」は究極の保険である

　テクノロジーの進化により、パスワードレスで快適な認証基盤が整う未来はすぐそこまで来ています。しかし、それらが完全に社会へ浸透するまでの間、私たちは現在の二要素認証を決して手放してはなりません。

　ログイン時の「わずか数秒の不便さ」は、時に152億円の身代金要求から組織を守り、医療の停止を防ぎ、サプライチェーンの崩壊を食い止める「究極の保険」です。情報社会における自己防衛は、車に乗る時にシートベルトを締めるのと同じです。最初は少し窮屈に感じるかもしれませんが、万が一の激突時にあなたの命を救うのは、その窮屈な一本のベルトなのです。二要素認証は、もはや「あれば安心」なオプションではなく、現代社会を生き抜くための
「必須のパスポート」であると認識すべきでしょう。

【参考リンク】

- Two Factor Authentication Statistics By Customers, Industry, Technology, Demographic, Usage And Facts (2025)
  https://electroiq.com/stats/two-factor-authentication-statistics/
- Multi-Factor Authentication (MFA) Statistics You Need To Know In 2025
  https://expertinsights.com/user-auth/multi-factor-authentication-statistics

ふちがみ　しんいち
淵上 真一

日本電気株式会社 Corporate Executive CISO
NECセキュリティ株式会社 取締役
ベンチャー系システムインテグレータでのネットワークエンジニアを経て、専門学校グループを運営する学校法人に転職。
教員経験を経て、社外では司法、防衛関連のセキュリティトレーニングを手掛ける。2018年よりNECグループ全社セキュリティ統括を担当。

ISC2 認定主任講師、Cisco Networking Academy Instructor Trainer
情報処理安全確保支援士集合講習認定講師、北海道大学 客員研究員
サイバー安全保障人材基盤協会理事、日本情報経済社会推進協会（JIPDEC）評議員、警察大学校嘱託講師、Hardening Project実行委員