

君のログインを守る最新防衛術



MFAとパスキー、そして「SIMスワップ」の罠

ログインを守る「多要素認証 (MFA)」の超基本

城の門に「パスワード」という南京錠を1つかけるだけの時代は終わりました。

現在の常識は、種類の違う「2つの鍵」を組み合わせること。

すでに「スマホに届くSMSコード」を組み合わせている人は、素晴らしい第一歩を踏み出しています。



なぜ二段階認証 (SMS) が突破されるのか？

犯人が狙う「リアルタイムフィッシング」の手口

SMSに届くコードの有効期限が「30秒」あっても意味がありません。
犯人のコンピューターは、君が入力したコードを「0.1秒」で本物のサイト
へ横流しします。君自身が、無意識のうちに犯人のために城門の鍵を
開けてしまっているのです。



ユーザー

ID / パスワード /
30秒有効なSMSコード



偽サイト
(中継サーバー)

0.1秒で即座に横流し



本物のサイト

最も身近なSMS認証の死角：「SIMスワップ詐欺」

スマホを落としていなくても、電話番号ごと奪われる手口があります。犯人が携帯会社を騙して君の番号を乗っ取ると、君のスマホは突然「圏外」に。その15分後、すべてのアカウントの認証コードは「犯人のスマホ」に届くようになり、デジタル資産が消滅します。

君のスマホ



犯人のスマホ



次世代の最強の鍵「パスキー (Passkey)」

次世代の最強の鍵 「パスキー (Passkey)」

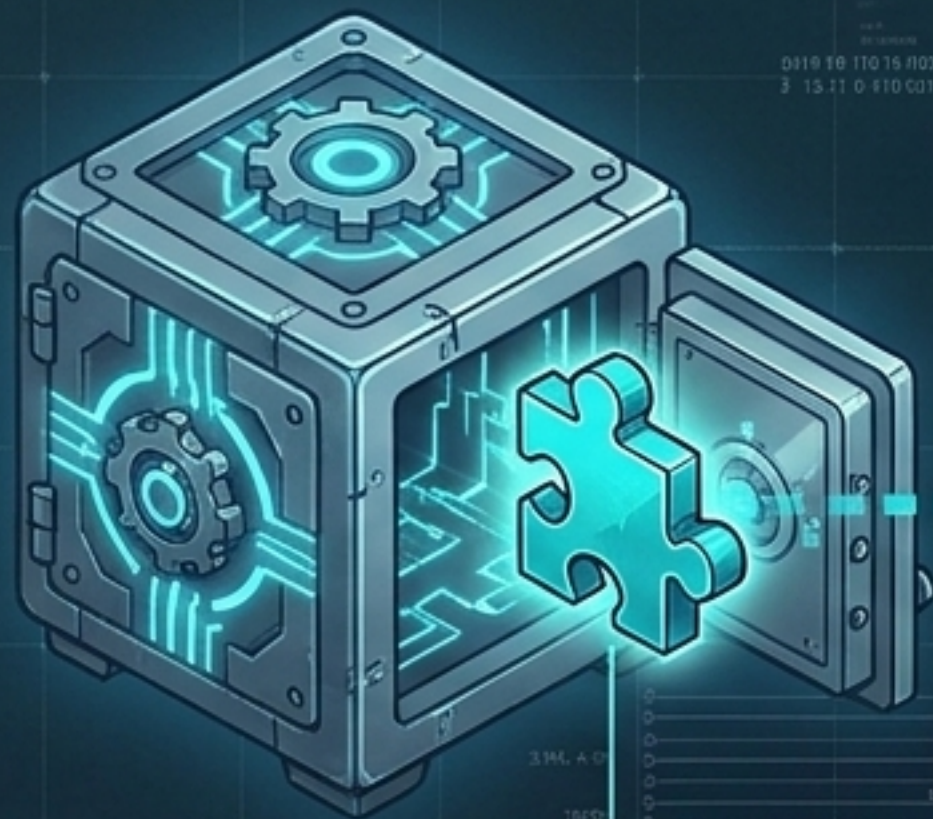
パスワードはもう不要。顔や指紋で一瞬でログイン。
「覚える必要がない」のに、これまでのどんな鍵よりも
強固な次世代の標準装備です。



フィッシングが「原理的に」通用しない理由

一番大切なコア（秘密鍵）は、スマホの外に絶対に出ません。偽サイトには反応すらしないため、盗まれる情報が「最初から存在しない」のです。人間が騙されても、システムが自動でブロックしてくれます。

スマホ（手元）



秘密鍵
（コアパーツ）

本物のサーバー



公開鍵

偽サイト



枠がないため無反応

旧式の鍵 vs 次世代の鍵

	認証スピード	記憶の必要性	フィッシング耐性	SIMスワップ耐性
旧式の鍵 (パスワード+SMS)	遅い	必要 (忘れるリスク)	✗ 突破される (AiTM)	✗ 奪われる
次世代の鍵 (パスキー)	⚡ 爆速 (顔/指紋)	不要 (スマホに内蔵)	🛡 防御 (原理的に無効化)	🛡 防御 (電話番号は無関係)

ただし、パスキーにも 「死角」がある

パスキーを保管している大元の「Google」や「Apple」のアカウント自体が乗っ取られると、元も子もありません。
玄関の鍵が最高でも、合鍵の管理会社が乗っ取られればアウトです。



今日からできるログイン防衛アクション

DEFENSE LEVEL MAX



アクション1: SMS認証をやめ、
「認証アプリ (Google Authenticator等)」に切り替える



アクション2: よく使う SNS やゲーム、ネット銀行に
「パスキー」を登録する



アクション3: 大元である Apple ID / Google アカウント
のセキュリティ設定 (二段階認証) を最強にする

君たちのデジタル資産を守れるのは、君たち自身の今日のアクションだけだ。