ポチっちゃ☆ダメじろー

Cyber Security News

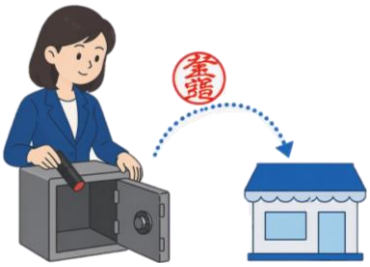
R8.6

パスワードだけの認証はもう限界です。

自社サービスにパスキーを導入し、
安全で快適なログインを実現しましょう！

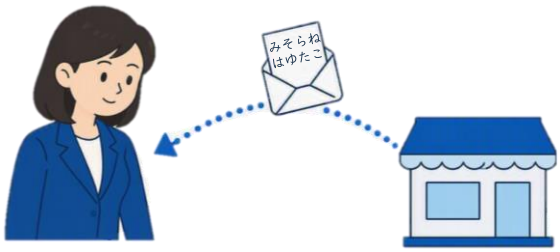
手紙のやり取りにたとえるパスキーの仕組み

① 印鑑作成 （鍵ペア作成）



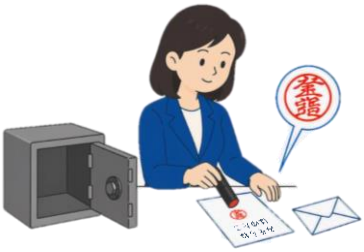
利用者が印鑑を作成し、金庫に保管。
印影をサービス事業者に提出。
（印鑑＝秘密鍵、印影＝公開鍵、金庫＝スマホ）

② 手紙の送付 （認証要求）



サービス事業者がランダムな文字列の手紙を送付。
（チャレンジ送信）

③ 手紙に押印 （本人確認・電子署名）



利用者が顔認証や指紋認証を行い、
金庫から印鑑を取り出して押印。

④ 印鑑の照合 （署名検証）

サービス事業者が
- 登録済の印影と一致するか
- 手紙の内容が②と一致するか　を確認。

パスキー導入の主なメリット

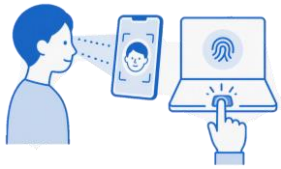
漏えいリスク低減

秘密鍵は端末の安全な領域に保存されるため、漏えい被害を抑制

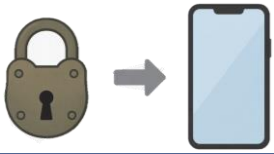
ブランド・信頼の維持

偽サイトでは認証できないため、
自社ブランドの悪用を防ぎ、
企業イメージを守る

利用者満足度の向上



パスワード入力不要。
顔認証・指紋認証ですぐログイン



パスワードから、パスキーへ。

パスワード漏えいやフィッシングのリスクから利用者を守るために。
より安全な認証方式として、パスキーの導入を御検討ください。

W・P・P

和歌山県警察本部サイバー犯罪対策課

警察庁
National Police Agency