

ニンテンドーアカウントへの パスキー導入



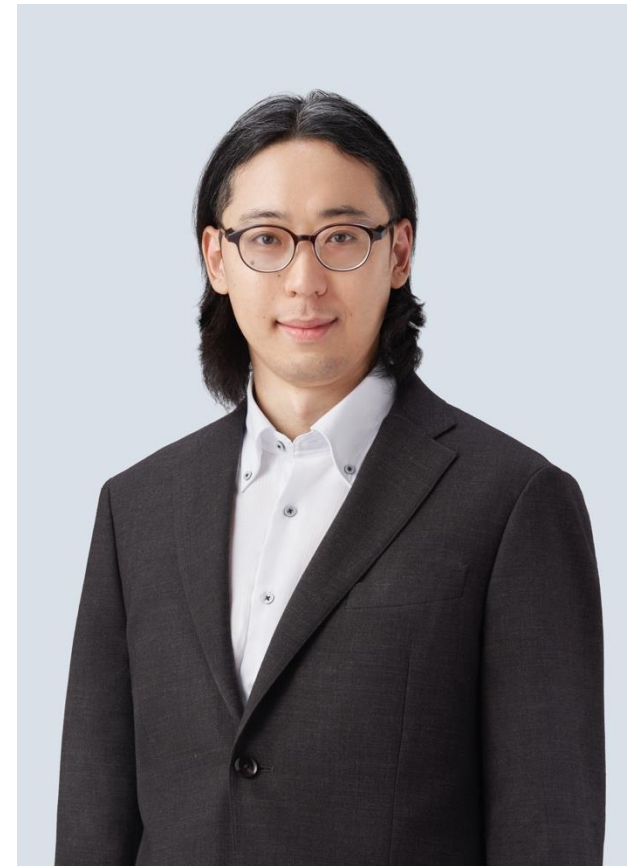
池内 弘樹

ニンテンドーアカウント
TechLead



竹本 隼人

パスキー導入
Project Lead



稲葉 純

FIDOサーバー
開発担当

発表の流れ

パスワード導入の動機

パスワード導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスワード導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスワードでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスワード利用

パスワードリリース時のサポート

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

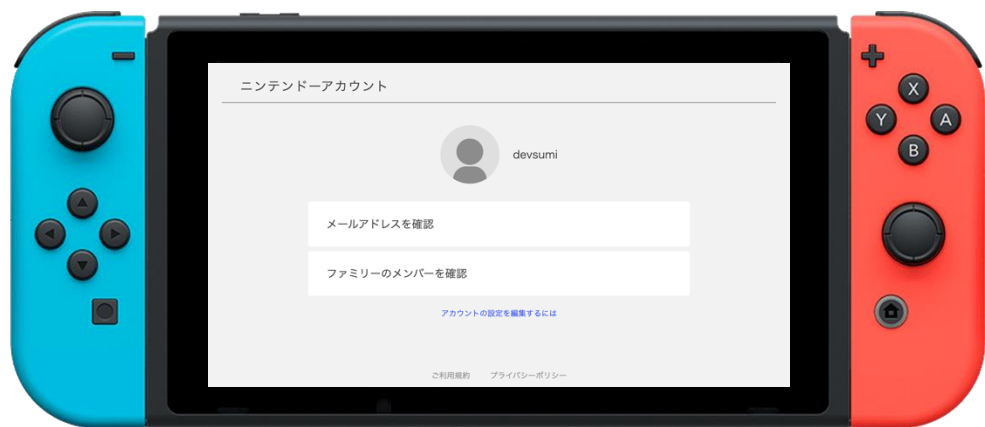
ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

ニンテンドーアカウントについて

- 任天堂のサービスを利用するためのアカウント
- Nintendo Switch、スマートフォンアプリ、Web ブラウザなどで利用できる



ニンテンドーアカウントについて



ニンテンドーアカウトについて



ニンテンドーアカウントに関する数字

リリース

対象の国・地域

アカウント数

2015年

164

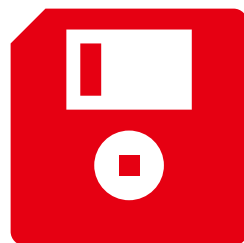
3.6億以上

*2024年9月時点

ニンテンドーアカウントに蓄積される資産



購買履歴



セーブデータ



フレンド



体験履歴

ニンテンドーアカウント

- ログインできないと様々なサービスや施設が利用できない
- 不正アクセスされると、蓄積した資産を失いかねない
- 複雑で利用の難しい認証はお客様体験を阻害する

より簡単で安全な認証手段の導入

利用可能な認証手段

パスワード

IDとパスワードを用いた認証

メールアドレス

メールへ送信するワンタイムパスワード認証

SMS

SMSへ送信するワンタイムパスワード認証

TOTP

Google Authenticator などを用いた認証

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

導入以前のニンテンドーアカウントの課題

1. パスワードに関する課題
2. メールアドレスに関する課題

パスキーで解決可能？

1. パスワードに関する課題

- 簡単に推測できるパスワードの登録を防げない
- どこかで漏洩済みのパスワードが利用されている可能性がある
- リスト攻撃の対象になる
- リスクベース認証や WAF の導入は抜本的な対策にはならない

つまり、

パスワードのみでセキュアなアカウント運用は難しい

2. メールアドレスに関する課題

メールサービス自体は他社で運営されている



そのため・・・

メールアカウントが侵害されるかどうかは他社に依存する



侵害されてしまうと・・・

アカウントが
乗っ取られてしまう

アカウント
リカバリーができない

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

パスキーとは

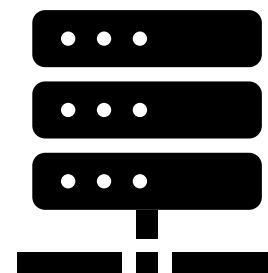


指紋などで認証



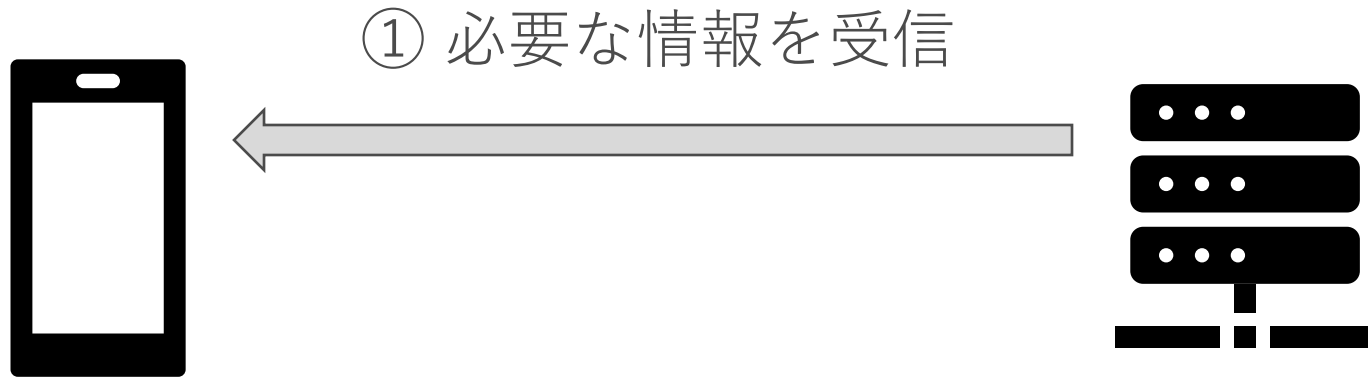
パスワードとは

登録時



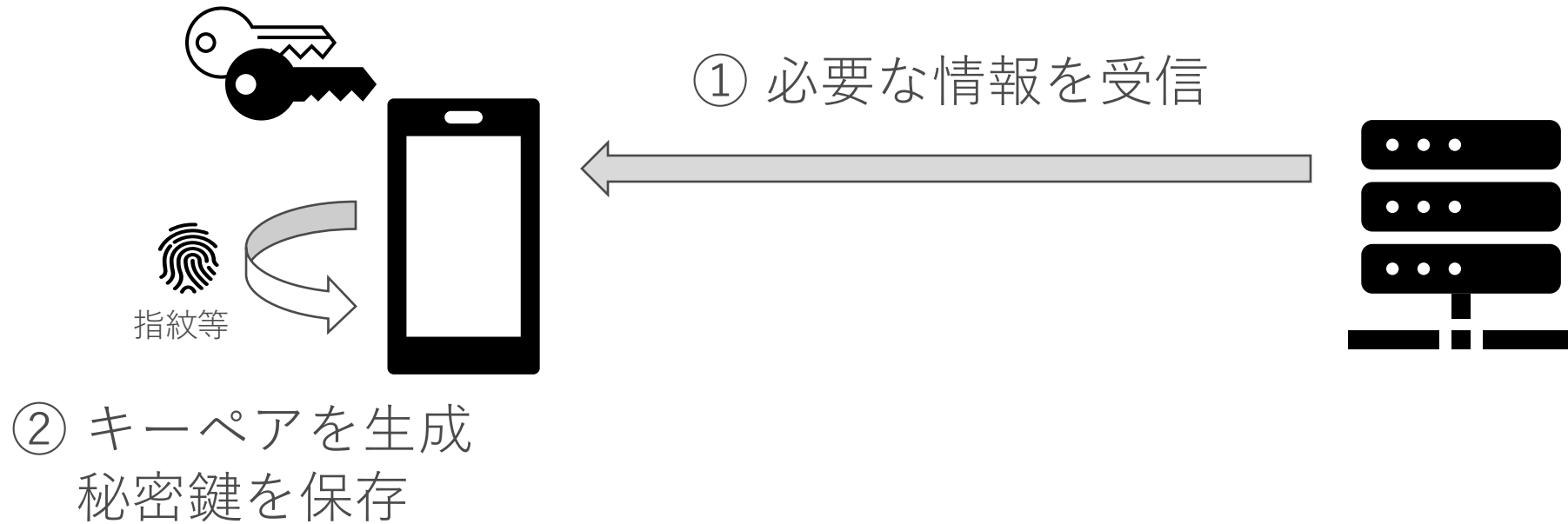
パスキーとは

登録時



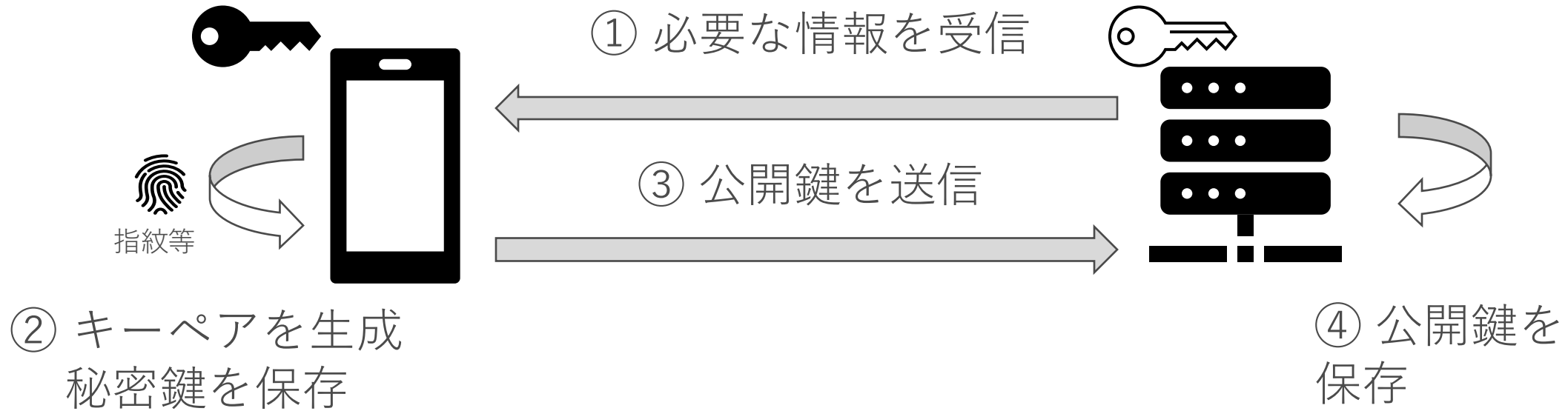
パスキーとは

登録時



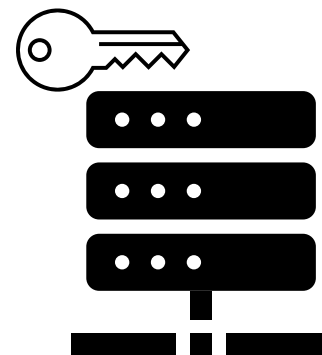
パスキーとは

登録時



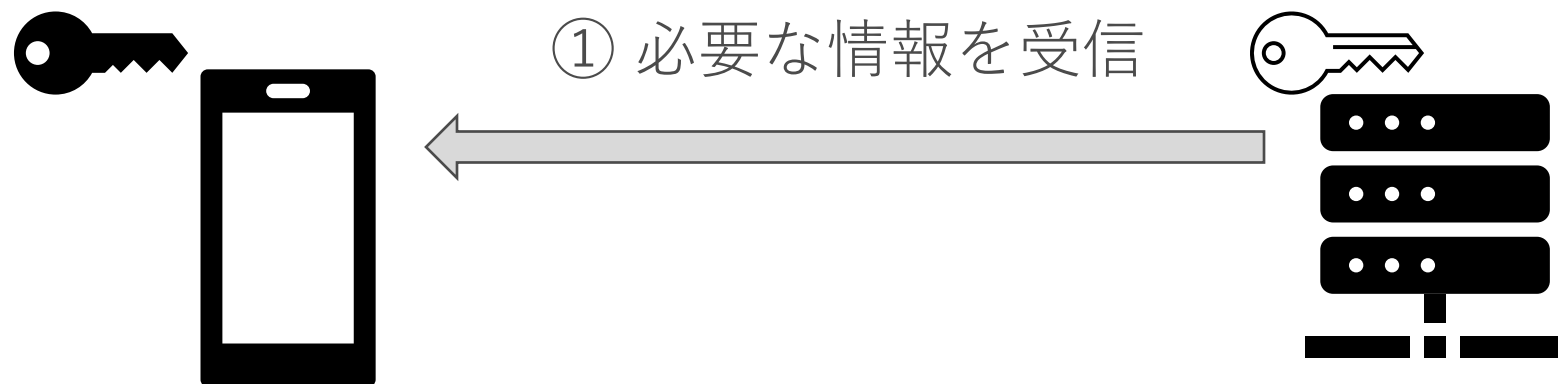
パスキーとは

認証時



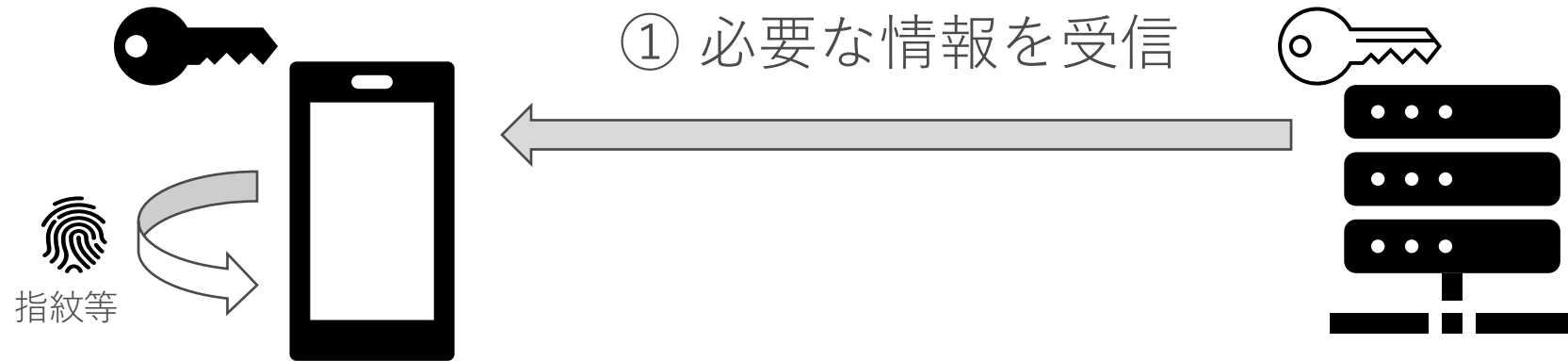
パスキーとは

認証時



パスキーとは

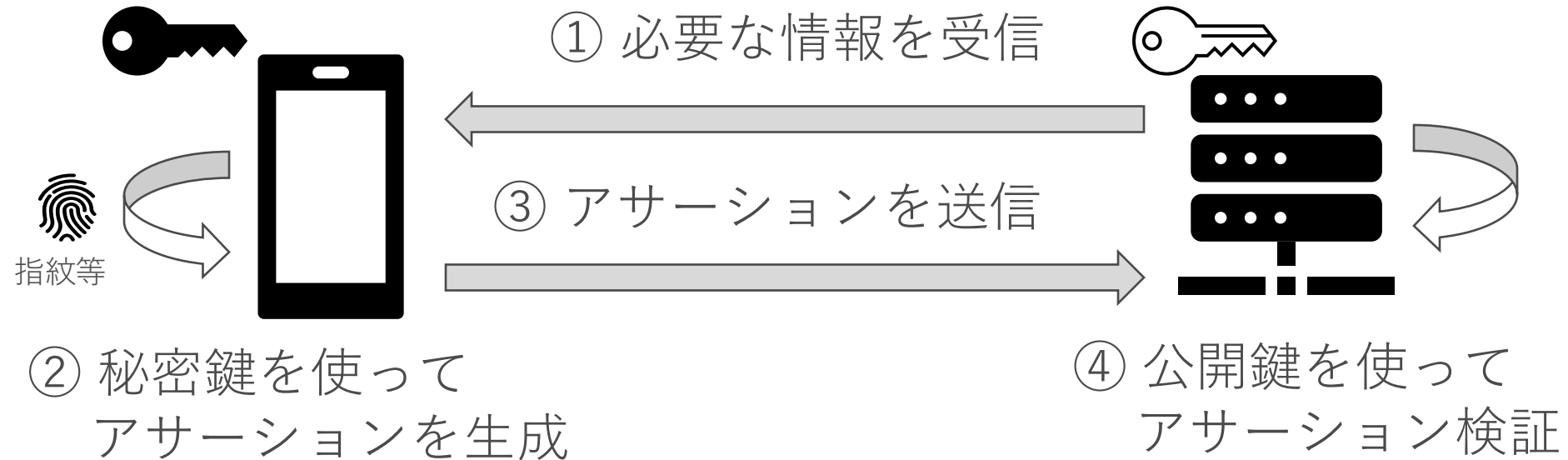
認証時



- ② 秘密鍵を使って
アサーションを生成

パスキーとは

認証時



パスキーとは

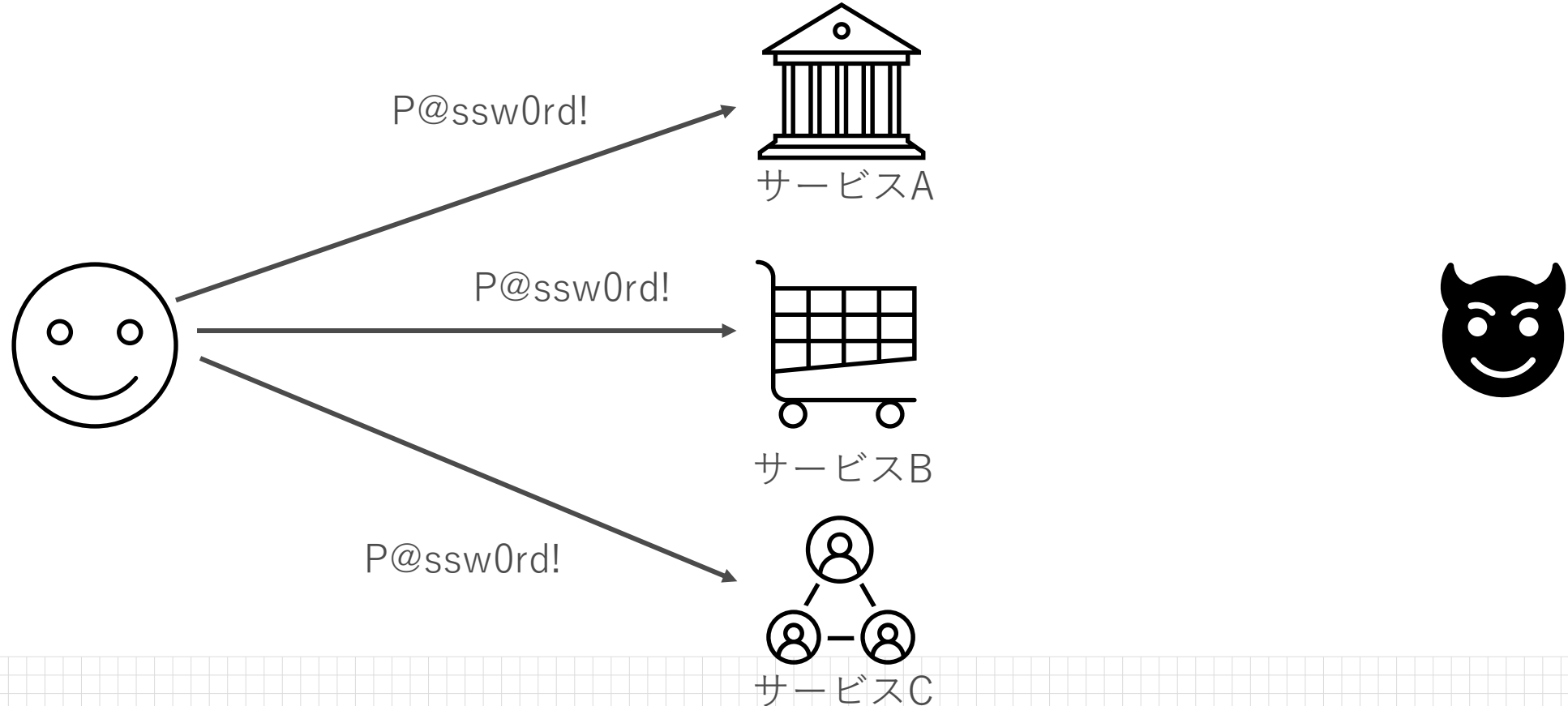
- このキーペアやアサーションの生成を**ブラウザの API 経由**で行うことができる

```
// キーペアの生成
let options = {
  publicKey: {
    rp: {...},
    user: {...},
    ...
  }
};
navigator.credentials.create(options)
  .then((credential) => {
    // サーバーに公開鍵を送信
  })
  .catch((err) => {
    console.log("エラー", err);
  });
```

```
// アサーションの生成
let options = {
  publicKey: {...},
};
navigator.credentials.get(options)
  .then((assertion) => {
    // サーバーにアサーションを送信
  })
  .catch((err) => {
    console.log("エラー", err);
  });
```

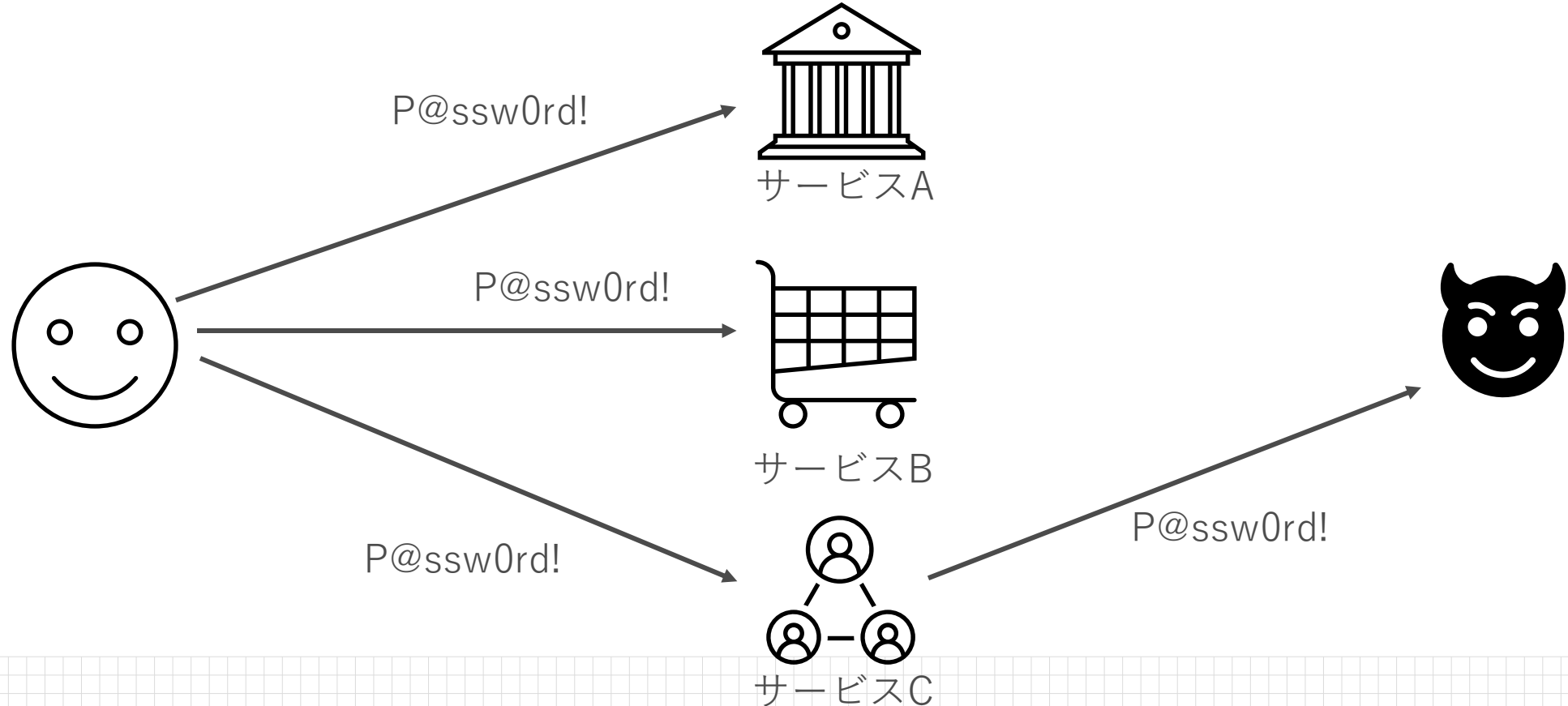
パスワードとの比較

1. 他サービスとの使いまわしの観点



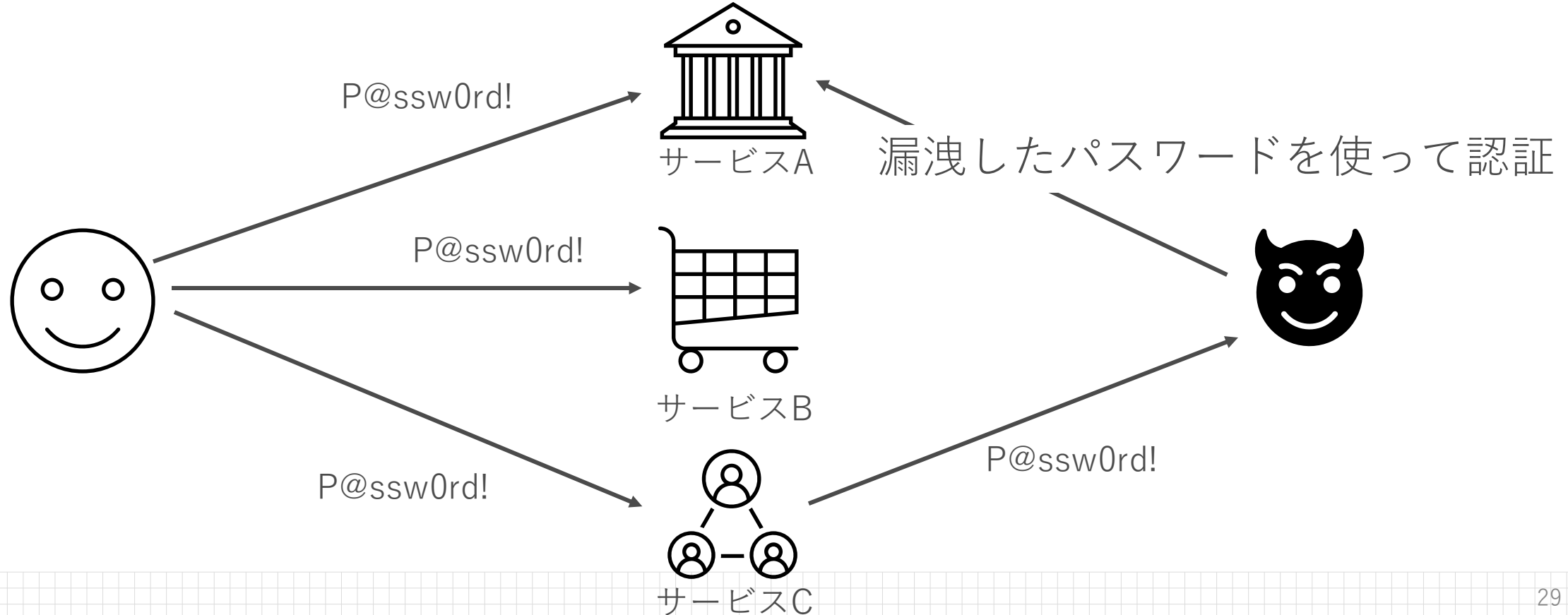
パスワードとの比較

1. 他サービスとの使いまわしの観点



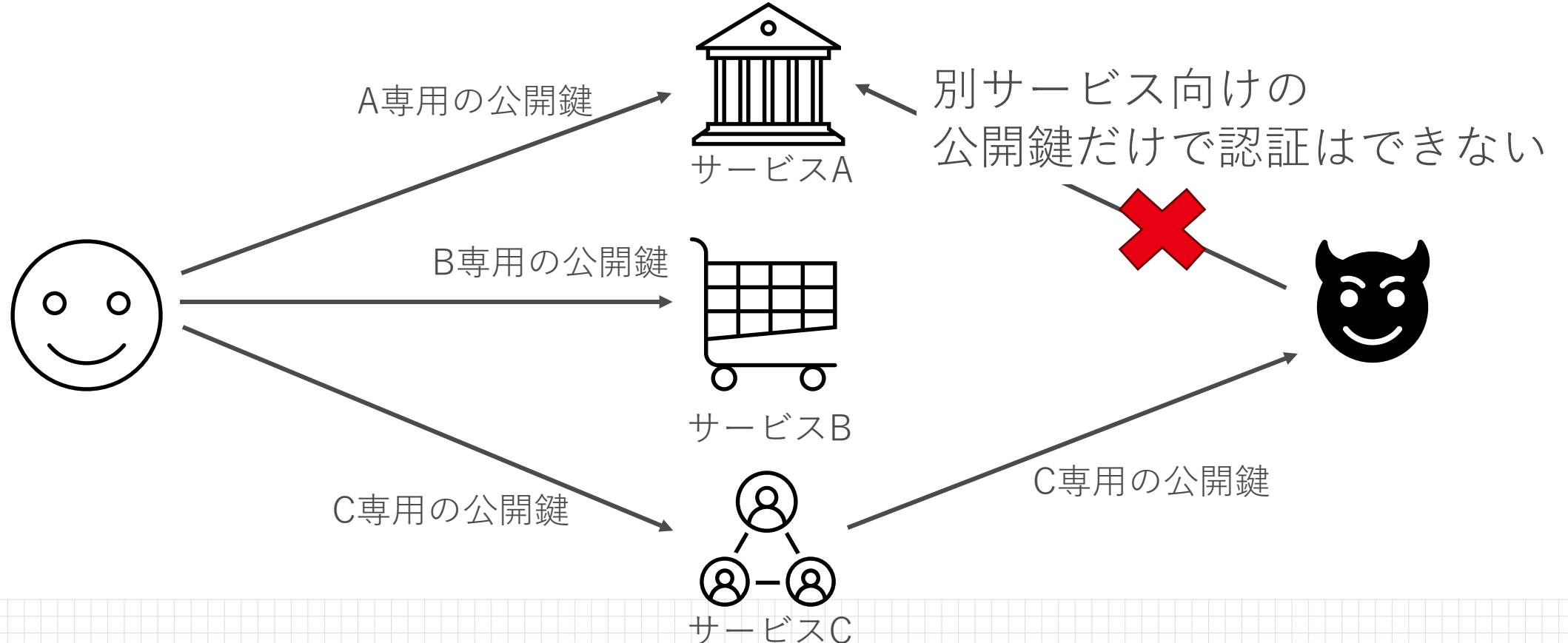
パスワードとの比較

1. 他サービスとの使いまわしの観点



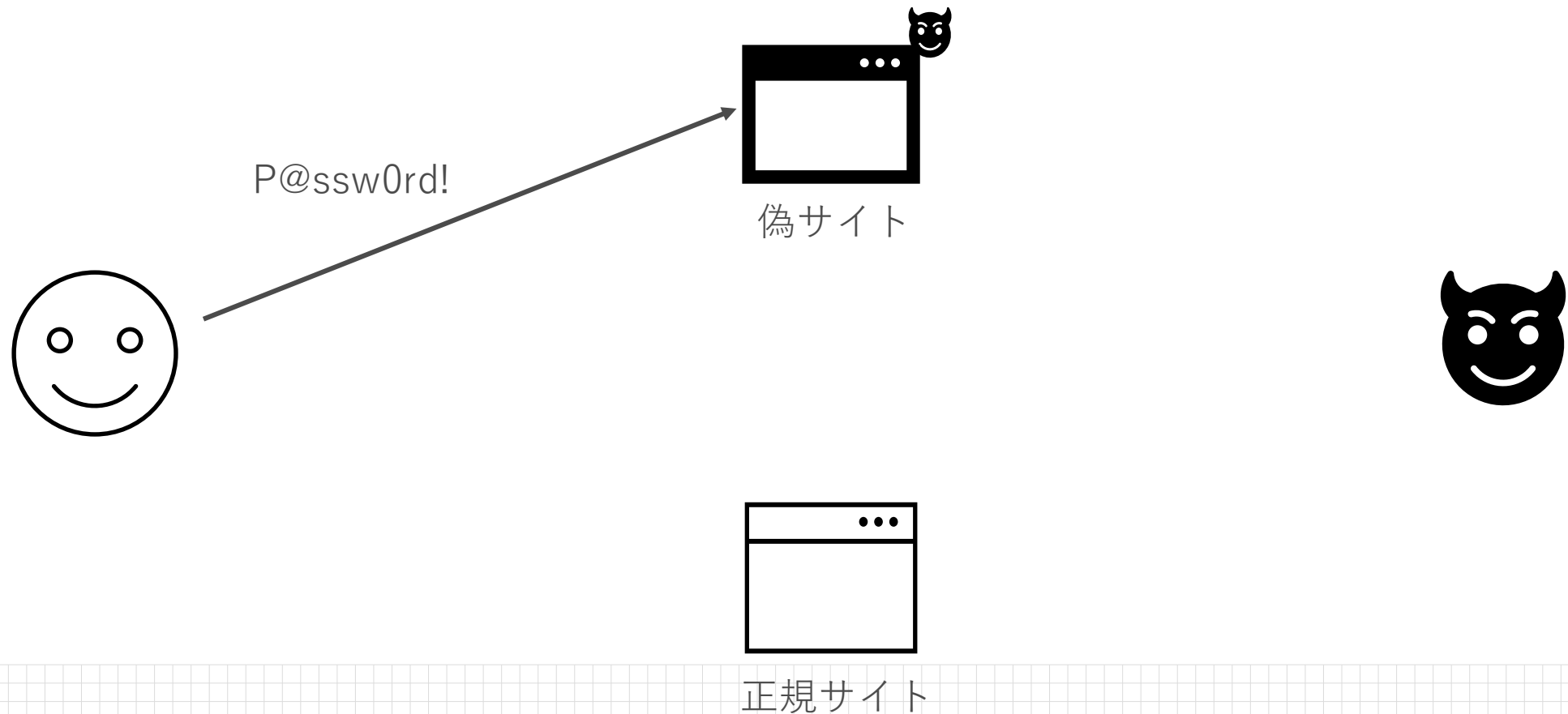
パスワードとの比較

1. 他サービスとの使いまわしの観点



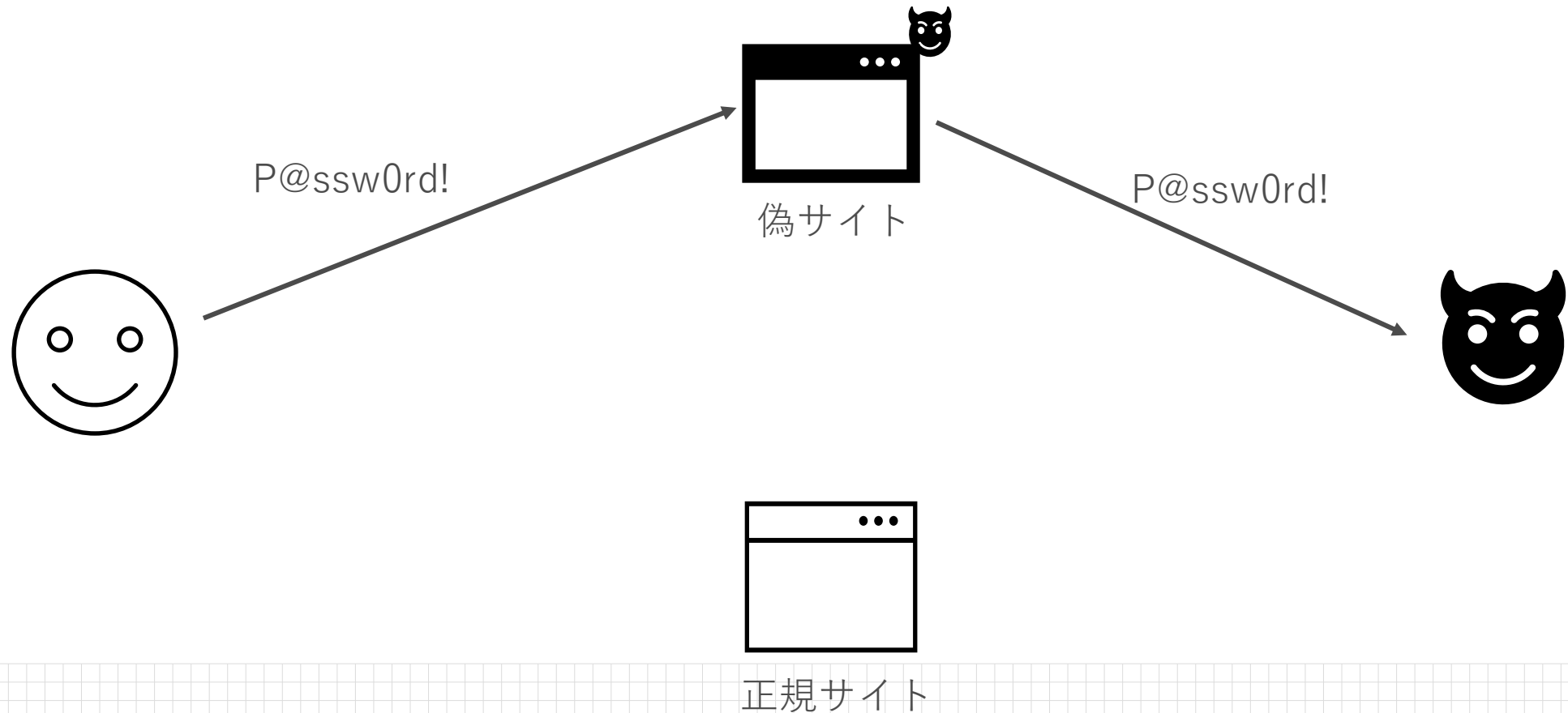
パスワードとの比較

2. 偽サイトへの入力の観点



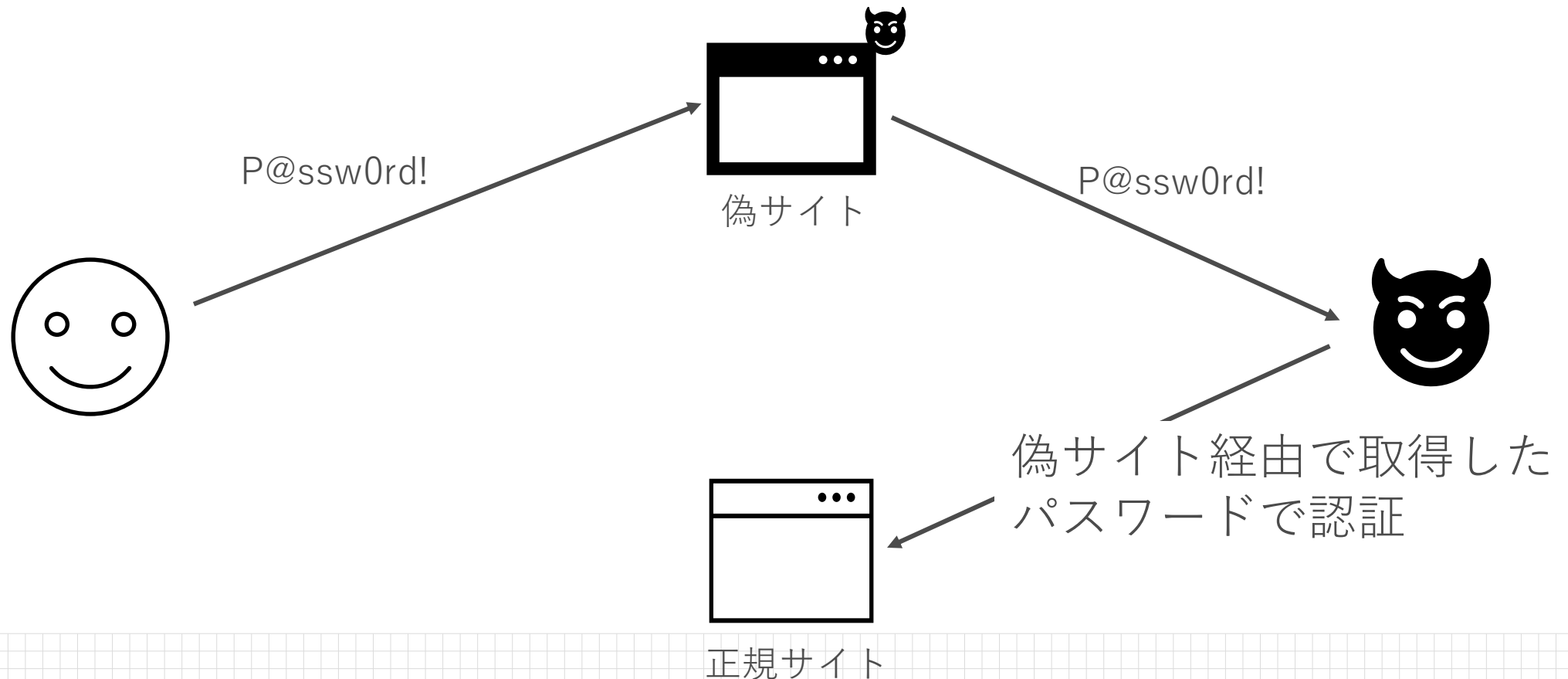
パスワードとの比較

2. 偽サイトへの入力の観点



パスワードとの比較

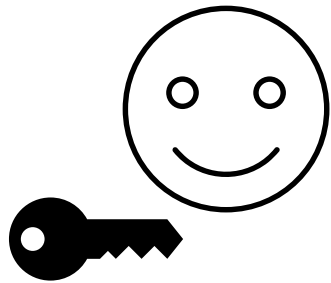
2. 偽サイトへの入力の観点



パスワードとの比較

2. 偽サイトへの入力の観点

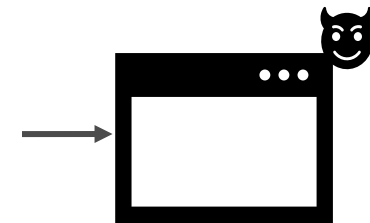
登録したはずのパスキーが
選べない・・・



正規サイト用
パスキー



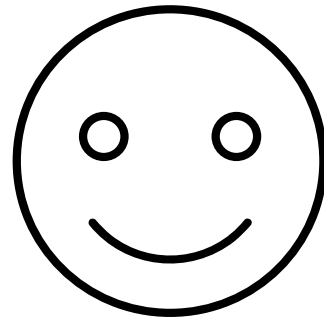
別のサービスなので
パスキーが使えない



偽サイト

パスワードとの比較

3. お客様の使いやすさの観点

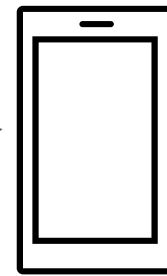
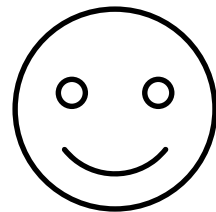


2年前に登録したパスワード
なんだっけ・・・？

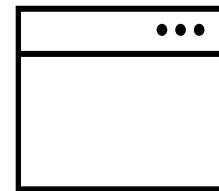
パスワードとの比較

3. お客様の使いやすさの観点

どっちも同じ方法で認証できる！



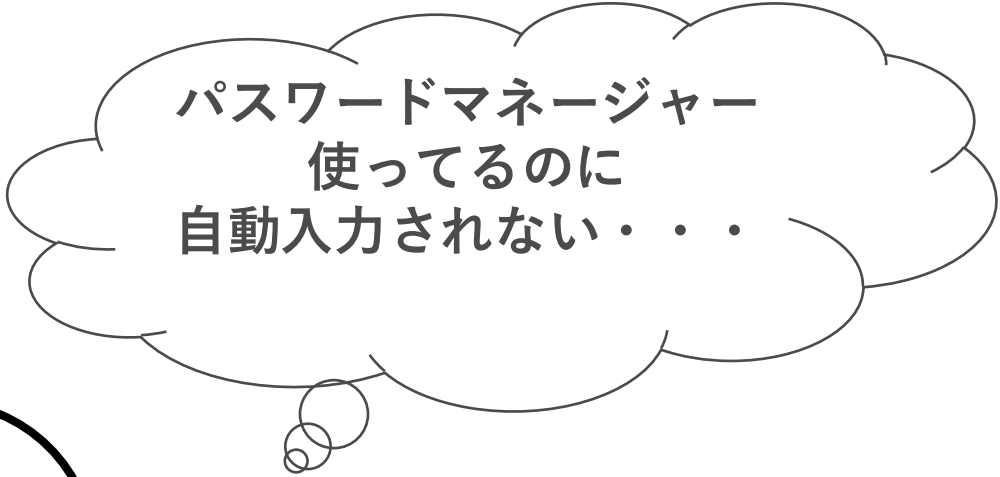
毎日使うスマートフォン



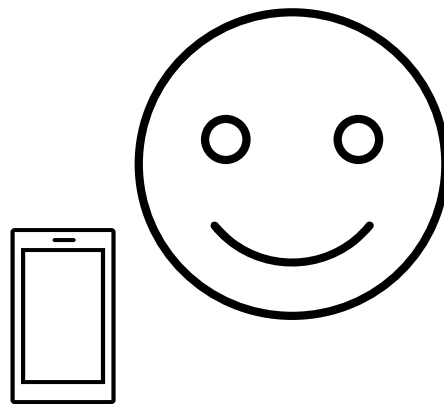
年に1回使う
Web サービス

パスワードとの比較

4. 適切な利用の難易度の観点



パスワードマネージャー
使ってるのに
自動入力されない・・・



パスワードとの比較

4. 適切な利用の難易度の観点



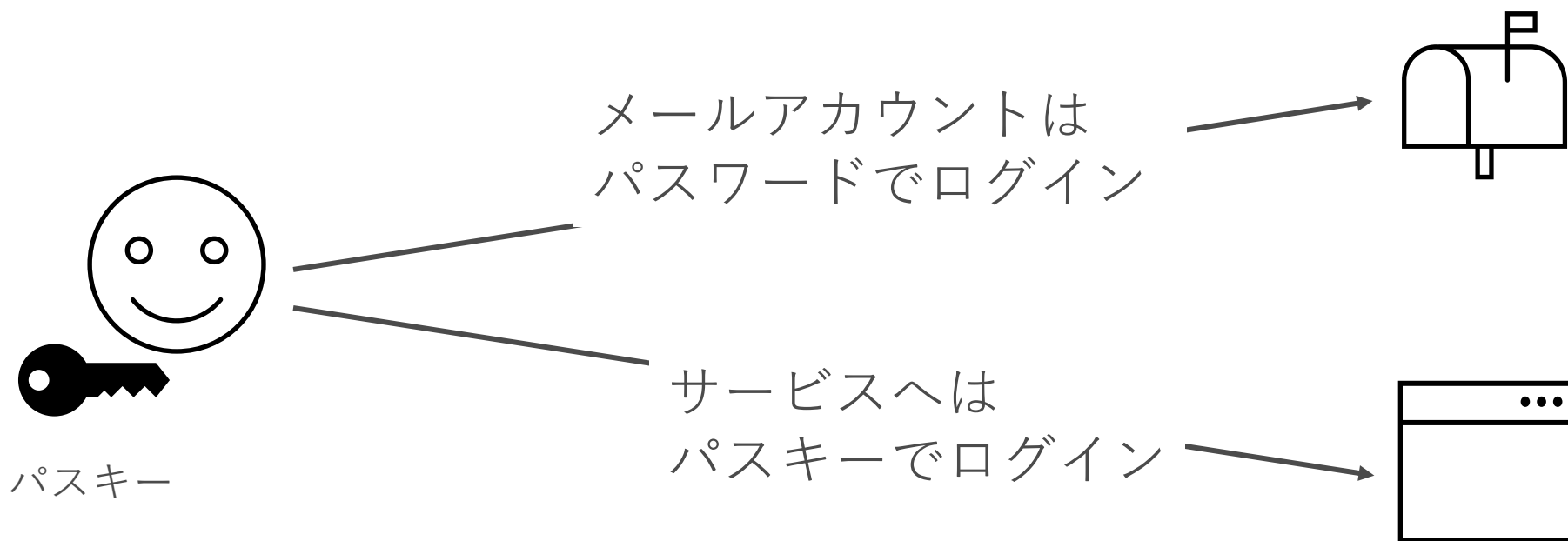
パスワードとの比較

4. 適切な利用の難易度の観点



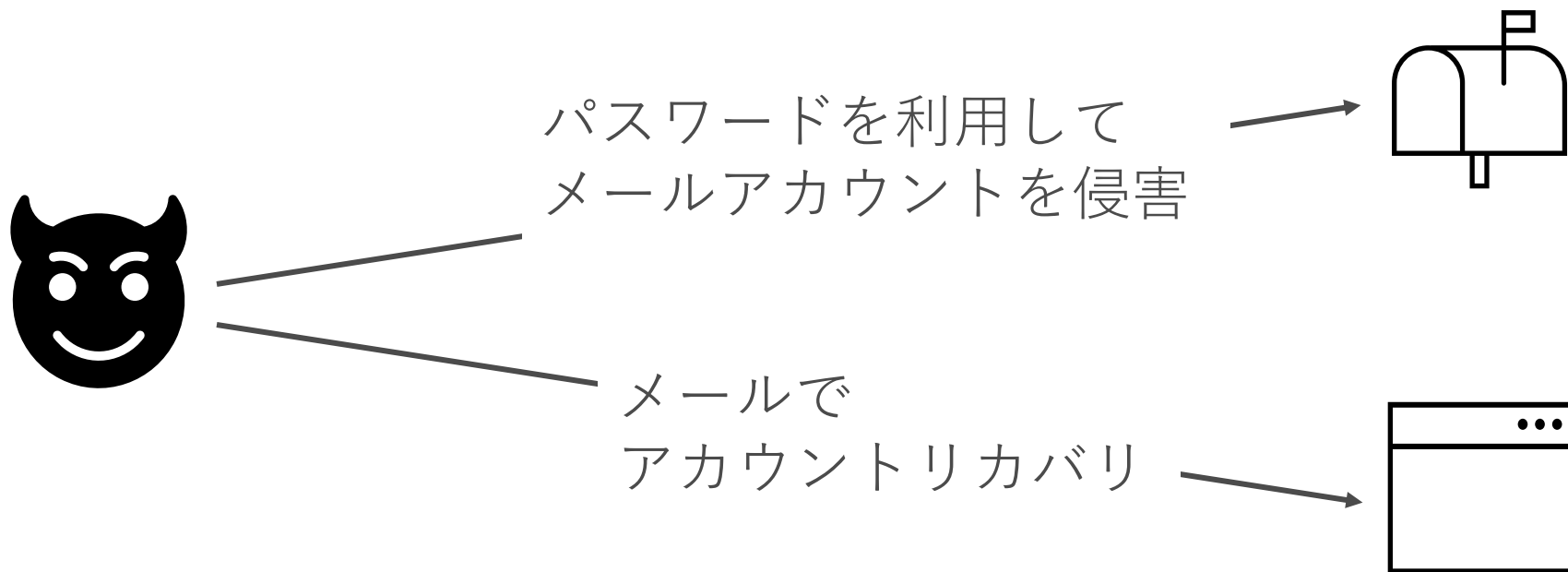
メールアドレスの課題は？

サービスにパスキーを導入しても メールアドレスの保護はできない



メールアドレスの課題は？

サービスにパスキーを導入しても メールアドレスの保護はできない



パスキーで課題を解消できるかへの答え

- ✓ 1. パスワードの課題は解決できそう
- ? 2. メールアドレスの課題はこの時点では未解決

→パスキーをどう導入するかがポイントになる

発表の流れ

パスワード導入の動機

パスワード導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスワード導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスワードでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスワード利用

パスワードリリース時のサポート

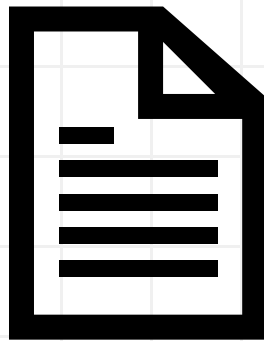
認証ポリシーとは

利用可能な認証手段

を

どのような場面

で求めるかを定めたルール・ガイドライン



利用可能な認証手段

パスワード

IDとパスワードを用いた認証

メールアドレス

メールへ送信するワンタイムパスワード認証

SMS

SMSへ送信するワンタイムパスワード認証

TOTP

Google Authenticator などを用いた認証

パスキー

ユーザー認証を求める場面

ログイン

ニンテンドーアカウントでサービスを利用する時に求める

再認証

ログイン済みでもソフト購入前の決済時など、重要な操作の前に求める

アカウントリカバリー

パスワードを忘れてしまった場合などに別の認証手段を使った復旧を行うために求める

認証ポリシー

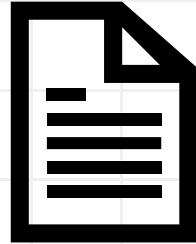
パスワード

メールアドレス

SMS

TOTP

パスキー



ログイン

再認証

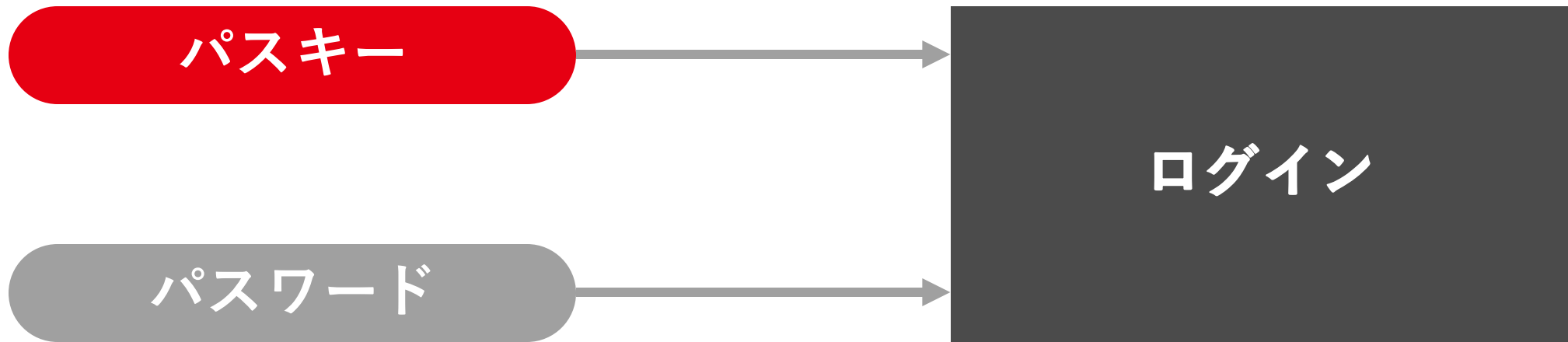
アカウントリカバリー

認証ポリシーの必要性

パスキーはパスワードに比べて強度の高い認証方法

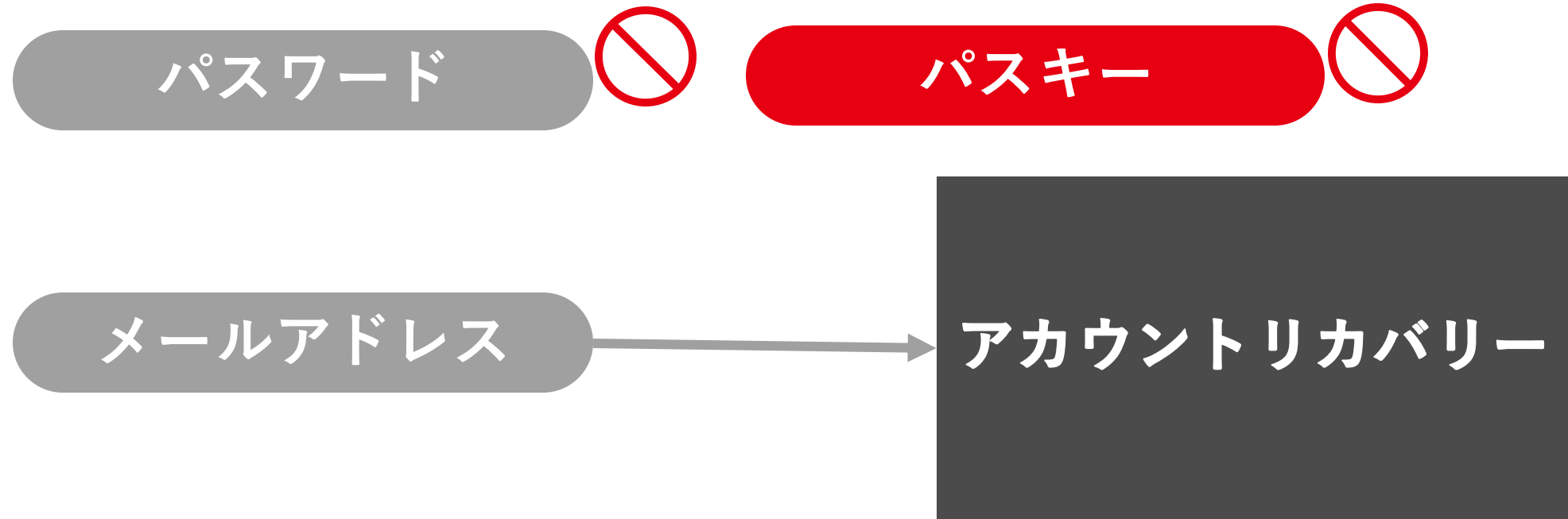
しかし、パスキーをサービスに導入したからといって
サービス全体の認証強度が上がるわけではない

例1：パスキーとパスワードの併用



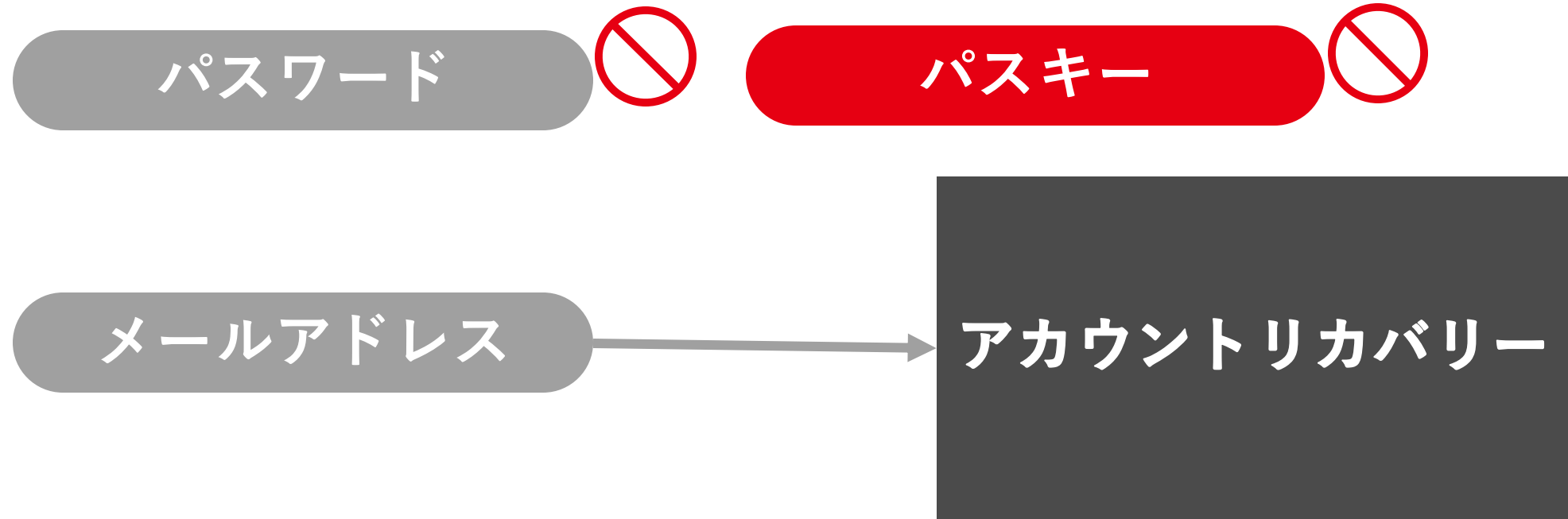
全体の認証強度 = パスワードの認証強度

例2：メールアドレスによるアカウントリカバリー



全体の認証強度 = メールアドレスの認証強度
= メールアドレス依存

例2：メールアドレスによるアカウントリカバリー



全体の認証強度 = メールアドレスの認証強度
= メールアドレス依存

認証ポリシーの必要性

- 単純に新しい認証手段をサポートしたからといって、全体の認証強度は変わらない
- サービスの性質・課題に適した認証強度であることが重要

→ 認証ポリシーを定めて適用する

ニンテンドーアカウントの性質と課題

- 様々な場面で利用できるような**簡単さと安全性のバランス**を重視
- パスワード認証の安全さに対する課題感
- メールアドレス依存への課題感

→ パスワードよりも高い認証強度になるように

→ メールアドレス依存を回避できるように

指針としたガイドライン

- NIST(米国国立標準技術研究所)が発行する
Digital Identity guidelines(NIST SP 800-63-3)を指針とした
- 認証方法ごとに定義されている
AAL(Authenticator Assurance Level – 認証保証レベル)を採用

NIST AALとは – 認証の3要素



something **you know**

本人のみが知っている



something **you have**

本人のみが持っている

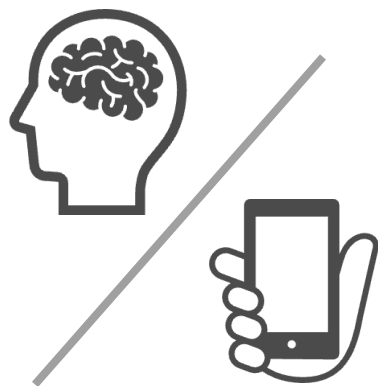


something **you are**

本人である情報

NIST AALとは – 3段階の認証保証レベル

AAL 1



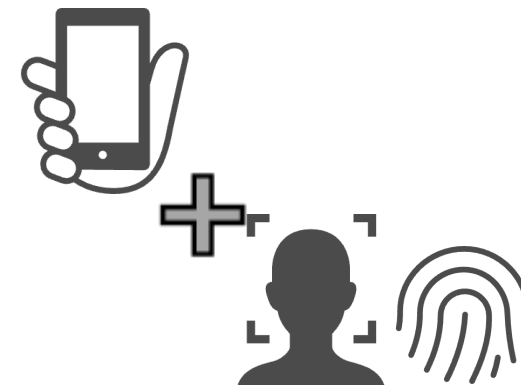
単一の認証要素で

AAL 2



複数の認証要素で

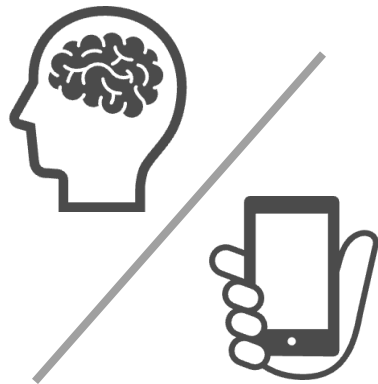
AAL 3



複数の認証要素で
フィッシング耐性あり
非常に高い信頼性

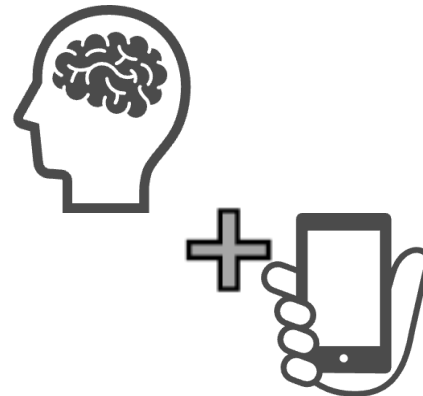
NIST AALとは – 3段階の認証保証レベル

AAL 1



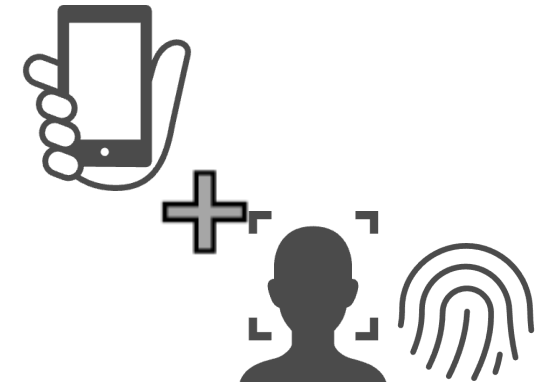
単一の認証要素で

AAL 2



複数の認証要素で

AAL 3



複数の認証要素で
フィッシング耐性あり
非常に高い信頼性

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

**ニンテンドーアカウントにおける
「認証ポリシー」**

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

認証ポリシーを構成する要素

- AAL を利用した独自の認証保証レベルの定義
- リスク評価や履歴に基づいた認証保証レベルの強化・緩和

認証ポリシーを構成する要素

- **AAL を利用した独自の認証保証レベルの定義**
- リスク評価や履歴に基づいた認証保証レベルの強化・緩和

AALを利用した独自の認証レベルの定義

認証保証レベル 1
(AAL1 をもとに定義)

パスワード単体

認証保証レベル 2
(AAL2 | AAL3 をもとに定義)

パスワード + メールアドレス

パスワード + SMS

パスワード + TOTP

パスキー

どのレベルを求めるか

パスキーを設定した場合は レベル2 を求める

認証保証レベル 1



パスキーを設定

認証保証レベル 2



パスキー設定済みの場合のログイン



認証保証レベル 2

パスキー

パスワード + メールアドレス

パスワード + SMS

パスワード + TOTP

パスワード

ログイン



パスワード設定済みのアカウントリカバリー



認証保証レベル 2

パスワード



パスワード



メールアドレス + SMS



アカウントリカバリー

メールアドレス



認証ポリシーを構成する要素

- AAL を利用した独自の認証保証レベルの定義
- **リスク評価や履歴に基づいた認証保証レベルの強化・緩和**

リスクベース認証



認証保証レベル 1

パスワード

+

メールアドレス

認証リスクを判定

ログイン

攻撃リスクをもとに追加の認証を求めて、認証保証レベル2 に引き上げ

操作の重要度に応じた再認証



認証保証レベル 1

パスワード

+

メールアドレス



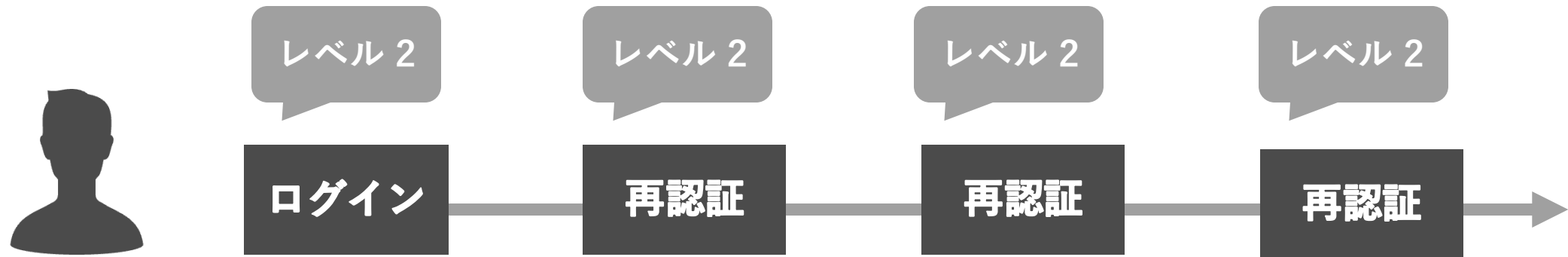
重要度が高い
操作前の再認証

(パスワードの変更など)

操作の重要性を定義し、重要度が高い操作前には高い認証保証レベルを求める

認証履歴を利用した緩和

ログイン・再認証のたびに常に 認証保証レベル2 を求めると、
体験が損なわれてしまう



認証履歴を利用した緩和

パスワード認証

ログイン

認証保証レベル2 を求める再認証

know要素を求める

AAL2が必要

→“別要素 have”の認証だけを求める



AAL2(know + have)とみなす

ニンテンドーアカウントの認証ポリシー

AAL を利用した独自の認証保証レベルの定義
リスク評価や履歴に基づいた認証保証レベルの強化・緩和

TOTP

パスキー



再認証

アカウントリカバリー

認証ポリシーを作成するメリット

- ガイドラインベース・ルールベースによる恩恵
 - ルールの見える化
 - 新しい認証方法を入れる時にスムーズ

認証ポリシー作成時に苦労した点

- 認証ポリシーを稼働中のシステムに適用するのは大工事
- 体験とセキュリティのバランスを考える必要性
 - NIST AAL をそのまま利用すれば仕様としてはシンプル
 - 追加のルールを入れるほど仕様は複雑化
 - 運用のしやすさとはトレードオフ

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

ログイン

- 画面下部にパスキーでログイン専用ボタンを用意
 - パスキーログインのセクションを追加
- 多くのお客様の体験を変えないことを最優先
 - 大きくログイン画面を変えていない
 - パスワードのフォームはそのまま



パスキーログインが可能な時のための工夫

- ConditionalUI のサポート
 - 設定されたパスキーがある場合は、サジェストされるようになる



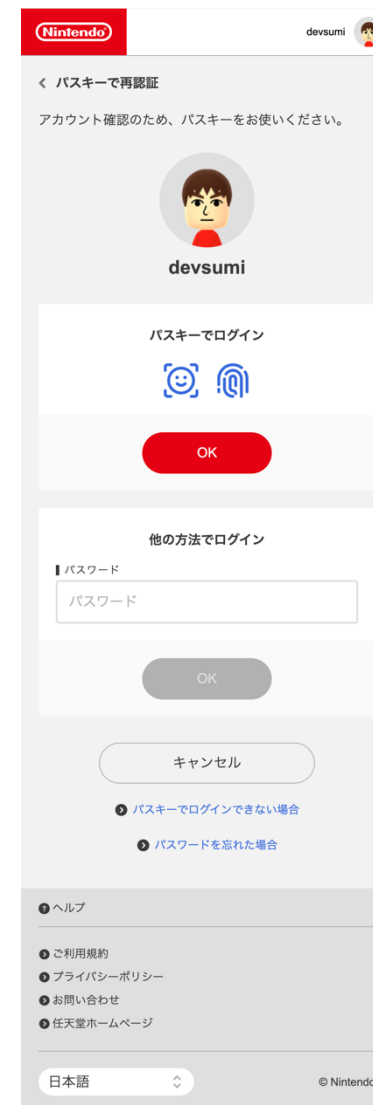
パスキーログインが可能な時のための工夫

- パスキーを使ったことがあるブラウザでは、パスキーログインへ誘導
- フラグとなるcookieを付与してハンドリング



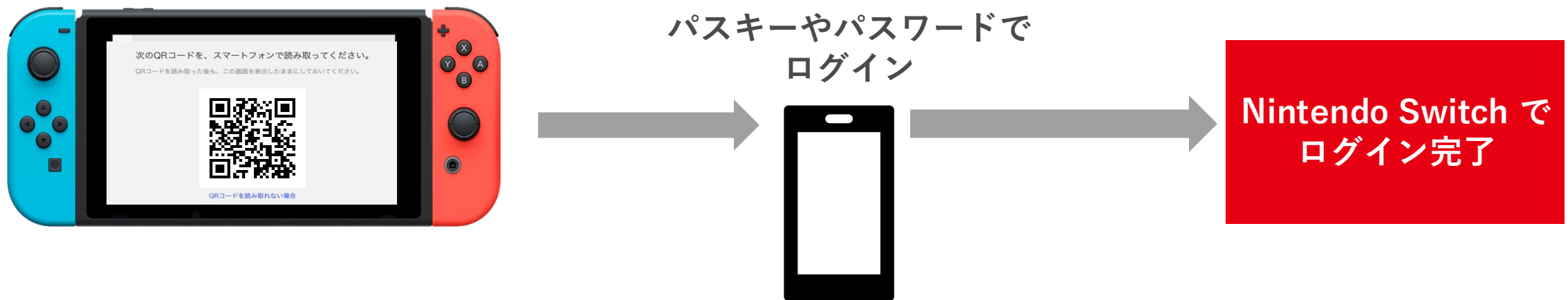
再認証

- 再認証は認証するお客様を特定できる
- パスキー登録済みのお客様であれば優先的にパスキーログインを促したいため、画面上部に表示
- 念の為、他の認証も使えるように
 - 既存のパスワードフォームを下段に用意
 - かつ他の認証手段のリンクを用意



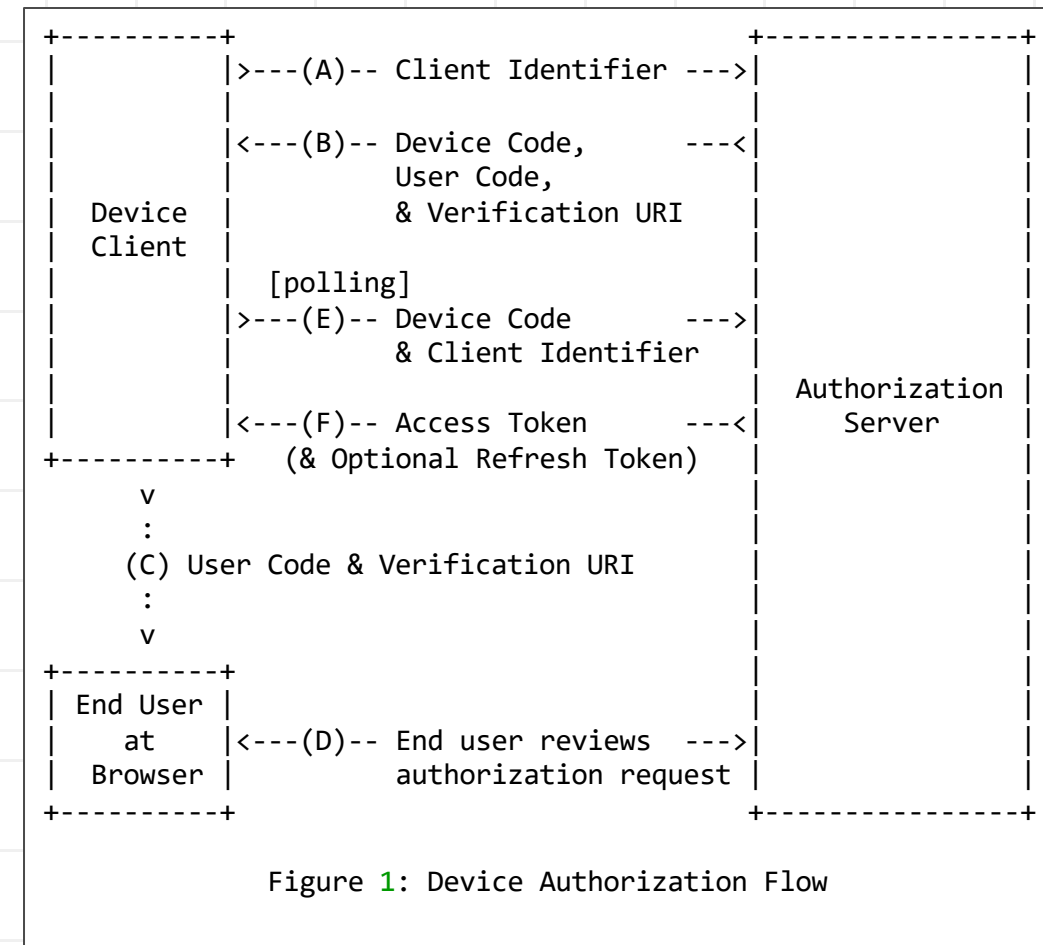
Nintendo Switchからのログイン

- Nintendo Switch はパスキー非対応プラットフォーム
- QRコードを使ってスマートフォンへ誘導するシーケンスを用意
 - パスキーやパスワードマネージャーを利用した Nintendo Switch上でのログインの実現



Nintendo Switchからのログイン仕様

- RFC 8628 - OAuth2.0 Device Authorization Grant を参考



Nintendo Switchからのログイン仕様

- Security Considerations を参考にすると
 - ログイン操作する端末であるスマートフォン、
 - ログイン状態を付与する端末である Nintendo Switch、
 - これらが物理的に近くにあることを担保する必要がある
- 被害を最小限にするよう工夫
 - Switch以外からこの認証フローを利用できないよう制限
 - リスクのある時にはインタラクションを追加

Nintendo Switchからのログイン仕様

- Security Considerations を参考にすると
 - ログイン操作する端末であるスマートフォン、
 - ログイン状態を付与する端末である Nintendo Switch、
 - これらが物理的に近くにあることを担保する必要がある
- 被害を最小限にするよう工夫
 - Switch以外からこの認証フローを利用できないよう制限
 - リスクのある時にはインタラクションを追加

発表の流れ

パスキー導入の動機

パスキー導入に向けた
「認証ポリシー」の整備

ニンテンドーアカウント
へのパスキー導入

ニンテンドーアカウントについて

ユーザー認証における課題

パスキーでの課題解決

「認証ポリシー」について

ニンテンドーアカウントにおける
「認証ポリシー」

ニンテンドーアカウントでのパスキー利用

パスキーリリース時のサポート

サポートページの用意

- 2023年パスキー元年でのリリースだった
 - 安心・安全の観点を伝えたい
- CS Teamと協力してサポートページを用意
- 日本向けだけでなく展開国向けに

ニンテンドーアカウント サポート パスキー



ニンテンドーアカウントのログインや各種サービスのアカウント再認証時には、パスワードの代わりに「パスキー」と呼ばれる仕組みを利用することができます。パスワードや二段階認証に比べて、より簡単、安全ですので、設定することをおすすめします。



このページは、
日本語で表示されています。

パスキーの設定

パスキーの設定

パスワードの代わりにお使いの端末を使った認証により、ニンテンドーアカウントにログインすることができます。

- ※ 生体情報がニンテンドーアカウントに送信・保存されることはありません。
- ※ パスキーを設定した後も、メールアドレスとパスワードは引き続き管理をお願いします。パスキーを設定した機器を機種変更したり、紛失したりした場合に、メールアドレスとパスワードを使用した本人確認が必要になることがあります。
- ※ ご使用の機器/OSバージョン/ブラウザによっては正常に動作しない可能性があります。



キャンセル 設定する

● パスキーについて

How to Manage Passkey Authentication for a Nintendo Account

Applies to: Nintendo Switch Family, Nintendo Switch, Nintendo Switch Lite, Nintendo Switch - OLED Model, Nintendo Account

Steps for registering, reviewing, or removing passkeys for your Nintendo Account.

Information

Registering a passkey with your Nintendo Account adds an additional layer of security that can help prevent unauthorized access to the account. When signing in to your account, you can choose to use your passkey to sign in instead of your email address or sign-in ID and password. Your passkey is saved in advance on your smartphone or other device, and this is retrieved by accessing that device when signing in.

Note: Biometric data is not sent to or saved in your Nintendo Account.

- Even after registering a passkey, you should continue to manage your e-mail address and password. In the event that you change or lose your device with the registered passkey, your e-mail address and password will be used to confirm your identity.
- Passkeys may not function correctly if they are incompatible with the device, operating system, or browser you are using.

What to do

- [Register a passkey to a Nintendo Account](#)
- [Review registered passkeys](#)
- [Remove a registered passkey](#)

Top articles

- [How to Delete a Nintendo Account](#)
- [Nintendo Account FAQ](#)
- [How to Transfer Digital Games / Nintendo Accounts Between Nintendo Switch Consoles](#)
- [How to Adjust Nintendo Account Profile Settings](#)
- [Forgot Nintendo Account Sign-In Info](#)
- [How to Play Your Games Across Multiple Nintendo Switch Systems](#)



技術面での対応

JS 上のエラー収集

- 黎明期のためWebAuthn仕様改定等の動きが多い
- すべてのお客様の環境での状況の把握が難しい
- JS上のエラーをキャッチしてサーバー送信し集計

E2Eテストの対応

- デプロイパイプラインでPuppeteerで E2E テストを実施
- Chrome DevTools Protocol で Virtual Authenticators を用意
- これによりWebAuthn APIが利用でき、パスキーテストも対応

今後に向けて

- 普及活動していても設定までしてもらうのは難しい
 - SNSでの普及活動 / パスキーエンドポイントの設置
- 利用している中での自然な訴求の検討
 - パスキー仕様策定としても議論されている
- Device Authorization Grant → Hybrid transports
 - サーバー経由でのやり取り → デバイス間でのやり取り
 - 体験面の改善 ↗
 - フィッシング耐性 ○



パスキーエンドポイント

まとめ

- パスキーを導入するにはサービス全体の認証ポリシーと導入の結果何を達成したいかを定める事が重要
- ニンテンドーアカウントにおいては、パスキー導入は強い認証手段の追加と扱いサービス全体の認証強度の向上を目指した
- Authenticator Assurance Level (AAL) を参考にした認証ポリシーの整理が鍵となった



**NINTENDO
SYSTEMS**