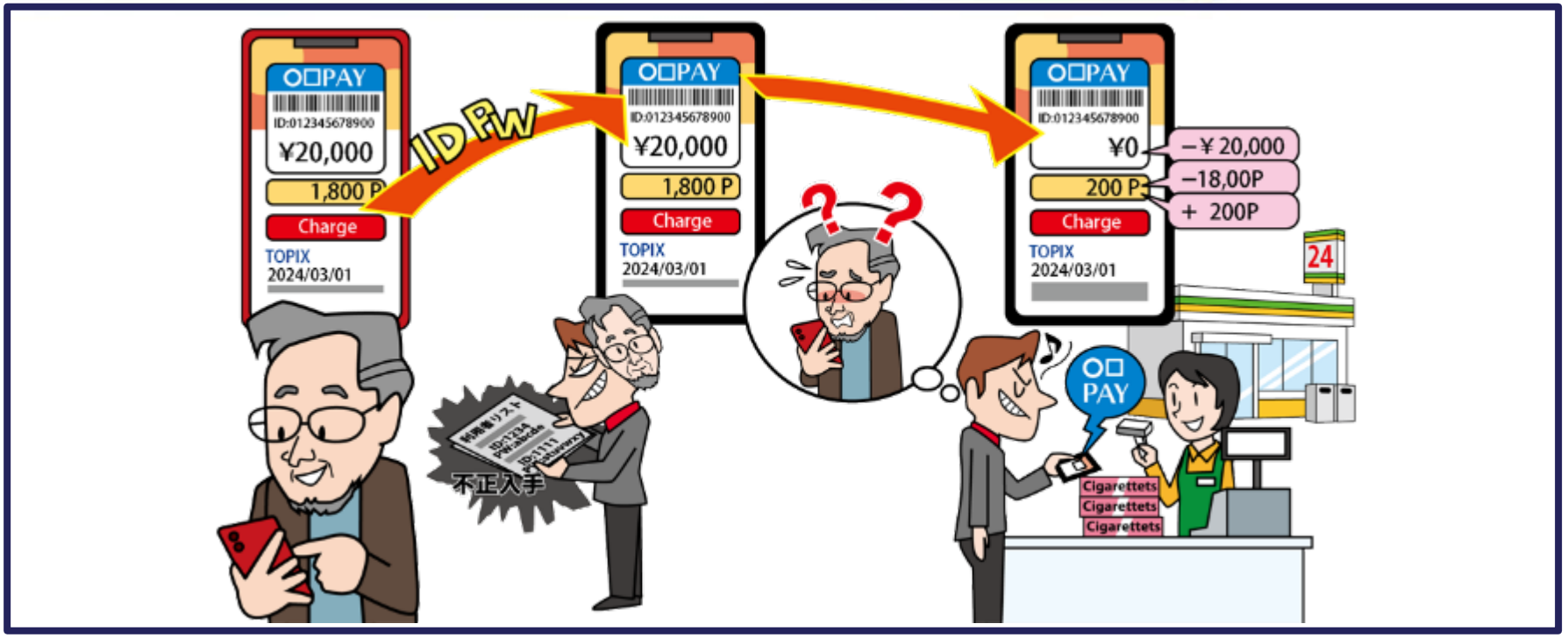
スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～



- スマホ決済サービスに不正ログインして<u>アカウントを乗っ取る</u>
- スマホ決済サービスの<u>脆弱性等の不備を悪用</u>
- クレジットカード情報等の<u>窃取</u>や、利用者が<u>意図しない金銭取引</u>を行う

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **攻撃手口**
  - **不正アクセスによるアカウントの乗っ取り**
    - 過去に漏えいしたパスワードをリスト化し、不正ログインを試みる
      ※パスワードリスト攻撃と呼ばれる攻撃手口
    - フィッシング攻撃等により詐取したIDやパスワードで不正ログインを試みる
    - パスワードの使いまわしを想定して、同一のパスワードで複数のサービスへの不正ログインを試みる
    - 多要素認証等のセキュリティ機能を利用していない場合、パスワードのみでログインが可能になるため、不正ログインされやすくなる

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **攻撃手口**
  - **サービスのセキュリティ上の不備を悪用**
    - 決済用システムやアプリの脆弱性を悪用し、利用者の意図しない決済を行う
    - 当該サービスだけでなく、金融機関等の他のサービスとの連携にセキュリティ上の不備があると悪用される場合がある
    - 多要素認証が提供されていない場合、攻撃者に悪用されやすくなり、サービス利用状況の通知サービスが提供されていない場合、正規の利用者が被害に気が付きにくくなる

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **攻撃手口**
  - **不正に入手したスマートフォンで決済をする**
    - ロックをかけていない、またはロックを解除した状態のスマートフォンを紛失したり、盗難されると不正にスマホ決済を利用される
    - 攻撃者がeSIM（スマホ等に内蔵されたデジタルSIM）を乗っ取り、不正にスマホ決済を利用する

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **2023年の事例/傾向①**
  - **「PayPay」を用いて自身のアカウントに不正送金**
    - 2023年4月、「PayPay」の他人のアカウントから、自身のアカウントに約8万円を不正送金した容疑者を兵庫県警が逮捕した
    - 容疑者と被害者は飲食店で知り合い、被害者は自身のスマートフォンのロックが解除されていたことと「PayPay」の残高がなくなっていたことに気が付き警察に相談した
    - その後、送金履歴等から容疑者が特定された

【出典】 ＰａｙＰａｙの送金で８万円をだまし取る 神戸市職員を逮捕（産経新聞）
https://www.sankei.com/article/20230412-XQE4VBCLEFMZTGDR4YSJUDUWVY/

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **2023年の事例/傾向②**
  - **他人の「auPAY」アカウントで不正に決済**
    - 2023年1月、佐賀県警と蕨署等が不正アクセス禁止法違反と詐欺等の疑いで中国籍の男女を再逮捕した
    - 容疑者はコンビニエンスストアで「auPAY」を使用し、他人名義の決済用バーコードを用いて約55,000円の物品を購入していた。
    - その後、被害者が不正な決済に気が付き、佐賀県警に相談したことで事件が発覚した。その後、店舗の防犯カメラの映像等から容疑者が特定された

【出典】 レジで支払った女逮捕、一緒にいた男も…関係ない女性の「auPAY」を使っていた　夜のコンビニで（埼玉新聞）
https://www.saitama-np.co.jp/articles/15070/postDetail

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **2023年の事例/傾向③**
  - **スマートフォンを乗っ取り、スマホ決済を不正に利用**
    - 2023年9月、名古屋県警等がブラジル国籍の容疑者を詐欺容疑で逮捕した
    - 容疑者は他人名義の決済サービスを利用して約8,000円相当の物品を不正に購入した疑いがあった
    - 被害者の女性のスマートフォンの「eSIM」（スマホ等に内蔵されたデジタルSIM）を乗っ取って不正に決済したと見られている

【出典】 スマホ決済不正利用容疑　３９歳逮捕　ｅＳＩＭ乗っ取りか（読売新聞オンライン）
https://www.yomiuri.co.jp/local/aichi/news/20230927-OYTNT50233/

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **対策**
  - **スマホ決済サービスの利用者**

【被害の予防】

- 多要素認証の設定を有効にする
- クレジットカード連携をする場合は3Dセキュアを利用する
- パスワードは長く、複雑にする
- パスワードを使い回さない
- パスワード管理ソフトを利用する
- パスワードを他人に教えない
- 提供されているならば、パスキーを利用する
- フィッシングに注意する
- 利用していないサービスからは退会する
- スマートフォンの紛失対策をする（画面ロック等のセキュリティ対策を実施）

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

IPA

- **対策**
  - **スマホ決済サービスの利用者**

【被害の早期検知】

- スマホ決済サービスの利用状況通知機能の利用および利用履歴を定期的に確認する
- 連携する銀行口座の出金履歴を確認する

【被害を受けた後の対応】

- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する
- サービス運営者（コールセンター等）へ相談する
- 連携している金融機関へ相談する
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※1

【参考】※1 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html