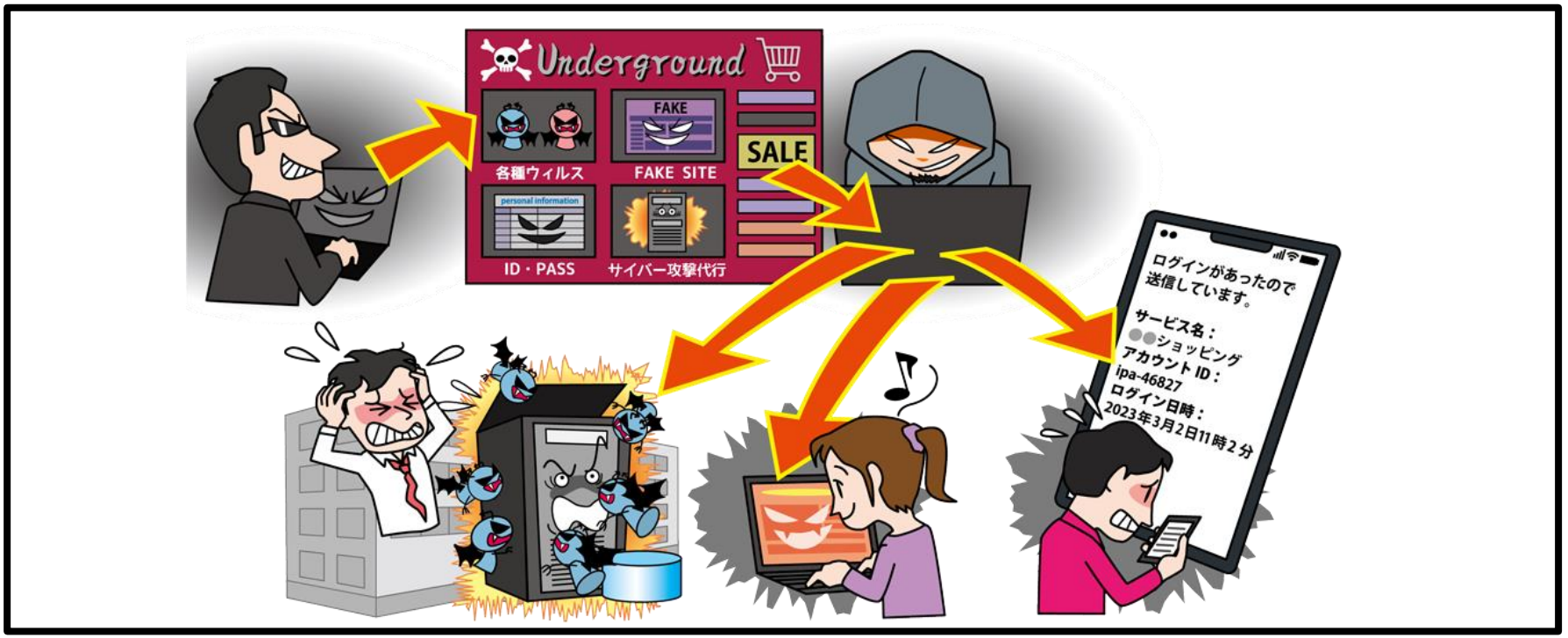
【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～



- サイバー犯罪に使用する**サービスやツール等の取引市場**
- 通常のブラウザでは検索できないウェブサイト上に存在
- 専門知識は不要で**容易にサイバー攻撃が可能**

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

- 攻撃手口
  - 購入したサービスやツールを利用して攻撃
    - ・攻撃の**代行サービス**や攻撃に利用できる**ツール**の取引
  - 購入した認証情報を利用してウェブへ不正ログイン
    - ・窃取した**個人情報や認証情報**を販売・購入
  - サイバー犯罪に加担する人材のリクルート
    - ・組織的に行われる**サイバー犯罪の人材確保**

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

- 2022年の事例/傾向①
  - 窃取した個人情報をダークウェブで売買（※1）
    - 2022年1月、クローズアップ現代によると、フィッシング等で窃取された個人情報がブラックマーケットで売買されていた
    - 大手ショッピングサイトのアカウント情報や個人情報も売買
    - 売買されている個人情報にはセキュリティコードもセットとなったクレジットカード情報、免許証や保険証の情報、パスポートの画像等が存在
    - 販売されている情報はフィッシングだけでなく企業から不正に窃取したとみられる

【出典】

※1　追跡！サイバー犯罪組織　コロナ禍の日本を狙う闇（NHK）

https://www.nhk.or.jp/gendai/articles/4631/

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

2022年の事例/傾向②

窃取された個人情報がダークウェブに流出(※1)

- 2022年9月、ダイナムジャパンホールディングスは**個人情報の流出**を確認したことを公表
- 同社のサーバーが**ランサムウェアによる攻撃**を受け、データを暗号化され、この際のアラートで被害が発覚
- グループ会社が運営する店舗の地権者の氏名や口座情報等2,042件や、入金情報172件、取引先に関する名刺情報や証券口座情報1,218件等が**流出**
- 流出した情報はいずれも**ダークウェブ上で公開**されていた

【出典】

※1 ダークウェブで個人情報流出を確認 - ダイナムJHD（Security NEXT）
https://www.security-next.com/140249

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

経営者

- 組織としての対応体制の確立
  - 問題に対応できる**体制（CSIRT等）構築**
  - **予算の確保と**継続的な対策の実施

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

システム管理者

・被害の予防

- DDoSの**攻撃の影響を緩和する**ISPやCDN等のサービス利用
- システムの冗長化など**軽減策**

・被害を受けた時の対応

- **組織の方針に従い各所へ報告、相談**する
  上司、CSIRT、関係組織、公的機関等
- 通信制御（DDoS攻撃元をブロック等）
- ウェブサイト停止時の**代替サーバの用意**と**告知手段の整備**
- 影響調査および原因の追究

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

PC利用者

- 被害の予防
  - セキュリティ**教育**
  - 受信メール、ウェブサイトの**十分な確認**
    不信なメールのリンクをクリックしたり、添付ファイルを開かない
  - 迅速に**更新プログラムを適用**する
  - セキュリティソフトの導入
  - 多要素認証方式などの認証方式の利用

【10位】犯罪のビジネス化（アンダーグラウンドサービス）

～攻撃者もショッピング。商品はあなたの情報～

対策一覧（一例）

PC利用者

・被害の早期検知

－不審なログイン履歴の確認

・被害を受けた後の対策

－組織の方針に従い各所へ**報告、相談**する

上司、CSIRT、関係組織、公的機関等

－バックアップからの普及