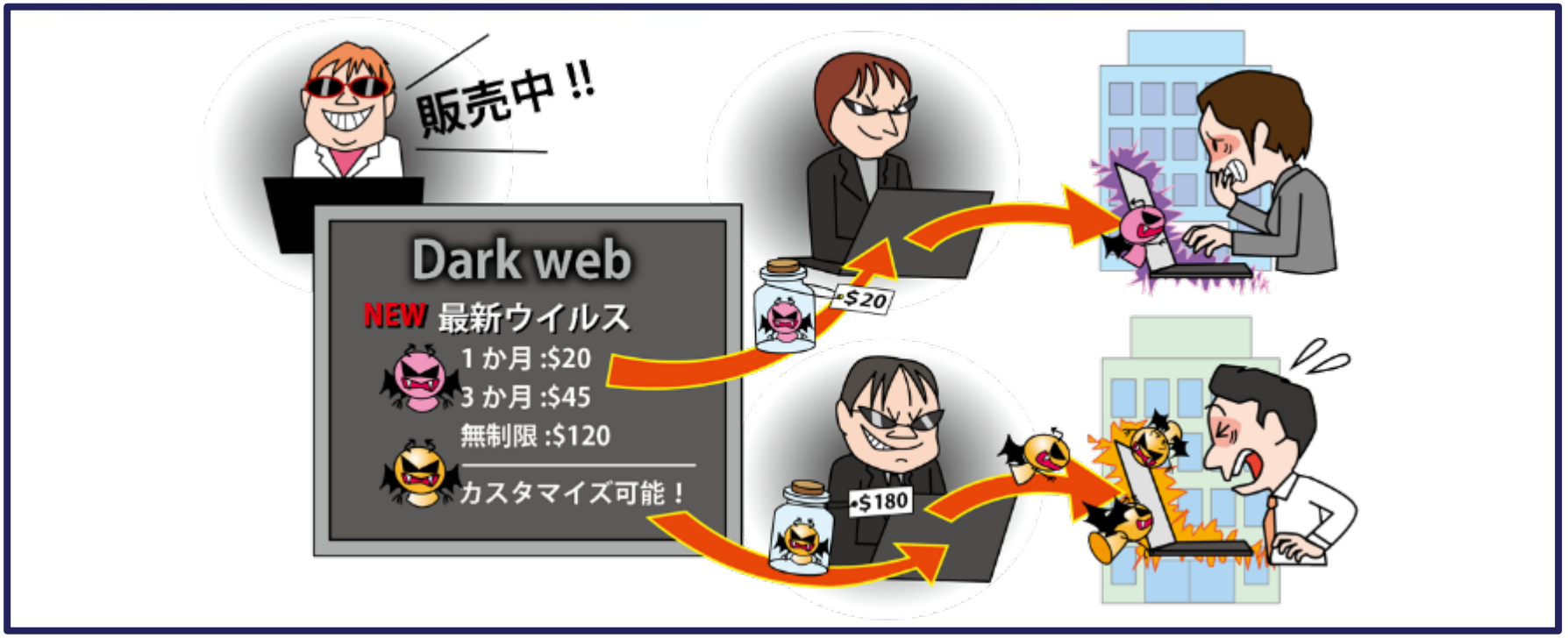
【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～



- 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が存在する
- 通常のブラウザでは検索できないWebサイト上に存在する
- 専門知識は不要で容易にサイバー攻撃が可能になってきている

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **攻撃手口**
  - **購入したサービスやツールを利用して攻撃する**
    - 攻撃の代行サービスや攻撃に利用できるツールを取引する
      - ランサムウェアや不正アクセスの手段を販売するサービスが確認されている
  - **購入した認証情報を利用してWebへ不正ログインする**
    - 窃取した個人情報や認証情報を販売・購入してWebサービス等に不正ログインする
  - **サイバー犯罪に加担する人材のリクルートをする**
    - 組織的に行われるサイバー犯罪の人材確保をする

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **2023年の事例/傾向①**
  - **ChatGPTのアカウントを売買**
    - 2023年4月、チェック・ポイント・リサーチはChatGPTの有料アカウントの取引増加を警告した
    - アカウントを乗っ取ることにより情報の漏えいにつながり、有料アカウントに紐づいているクレジットカード情報等の窃取が可能になる
    - 宣伝目的で最初にいくつかの有料アカウントを無料で提供し、巧妙に購入につなげようとしているものもある

【出典】 チェック・ポイント・リサーチ、ChatGPTに関する新たな懸念となる窃取された有料アカウントの売買増加を確認(PR TIMES)
https://prtimes.jp/main/html/rd/p/000000202.000021207.html
New ChatGPT4.0 Concerns: A Market for Stolen Premium Accounts(Check Point Software Technologies Ltd.)
https://blog.checkpoint.com/security/new-chatgpt4-0-concerns-a-market-for-stolen-premium-accounts/

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **2023年の事例/傾向②**
  - **国内製造業の情報がダークウェブに流出**
    - 2023年6月、アイギステックは国内の主要製造業30社について、ダークウェブへのアカウント情報漏えい状況調査結果を発表した
    - 調査対象の30社全てでダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明した
    - 特に製造業は、過去調査した金融機関、行政機関の結果と比較すると情報漏えい件数やハッキング数等においてすべて上回っていた

【出典】 国内主要製造業30社、ダークウェブ への情報流出調査結果(株式会社アイギステック)
https://www.aegistech.jp/news/view/id/23#u

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **2023年の事例/傾向③**
  - **月額でウイルスを販売し、サポートも存在**
    - 2023年10月、Fortinetは情報窃取ウイルス「ExelaStealer」が登場したことを注意喚起した
    - このウイルスはWindowsプラットフォームを標的にしたもので、クレジットカード等の情報を窃取する
    - 月額や買い切りで利用する方法があり、ダークウェブ上で、月額20ドルと、安価に提供されている。また、カスタマイズサービスも提供されていた。

【出典】 月額20ドル・3カ月45ドル・無期限120ドルのお買い得マルウェア登場、警戒を(TECH+)
https://news.mynavi.jp/techplus/article/20231023-2800152/

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

♦ 対策

攻撃に使用されるツールやサービスの目的・仕様によって対策は異なる。
より具体的な対策については本書の他の脅威を参照すること。

• 組織(経営者層)

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(システム管理者)**

【被害の予防】

- DDoS攻撃の影響を緩和するISP(インターネットサービスプロバイダー)やCDN(コンテンツデリバリーネットワーク)等を利用する
- システムの冗長化等の軽減策を検討する
- Torノードの検知/ブロックする
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

【被害の早期検知】

- ダークウェブを監視する
  - 監視サービス等を用いて、自組織に影響のある攻撃情報や流出情報の存在を確認する

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(システム管理者)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 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)
- Webサイト停止時の代替サーバーの用意と告知手段の整備をする
- 適切なバックアップ運用(復旧作業)を行う
- インシデント対応体制を整備し、対応する

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(PC利用者)**

【被害の予防】

- 情報リテラシー、モラルを向上させる
- メールの添付ファイル開封や、メールや SMSのリンク、URLのクリックを安易にしない
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
- 多要素認証方式などの認証方式を利用する

【10位】犯罪のビジネス化(アンダーグラウンドサービス)

～そのパスワード、すでに誰かが知っているかも？～

- **対策**
  - **組織(PC利用者)**

【被害の早期検知】

- 不審なログイン履歴を確認する

【被害を受けた後の対策】

- インシデント対応体制を整備し、対応する