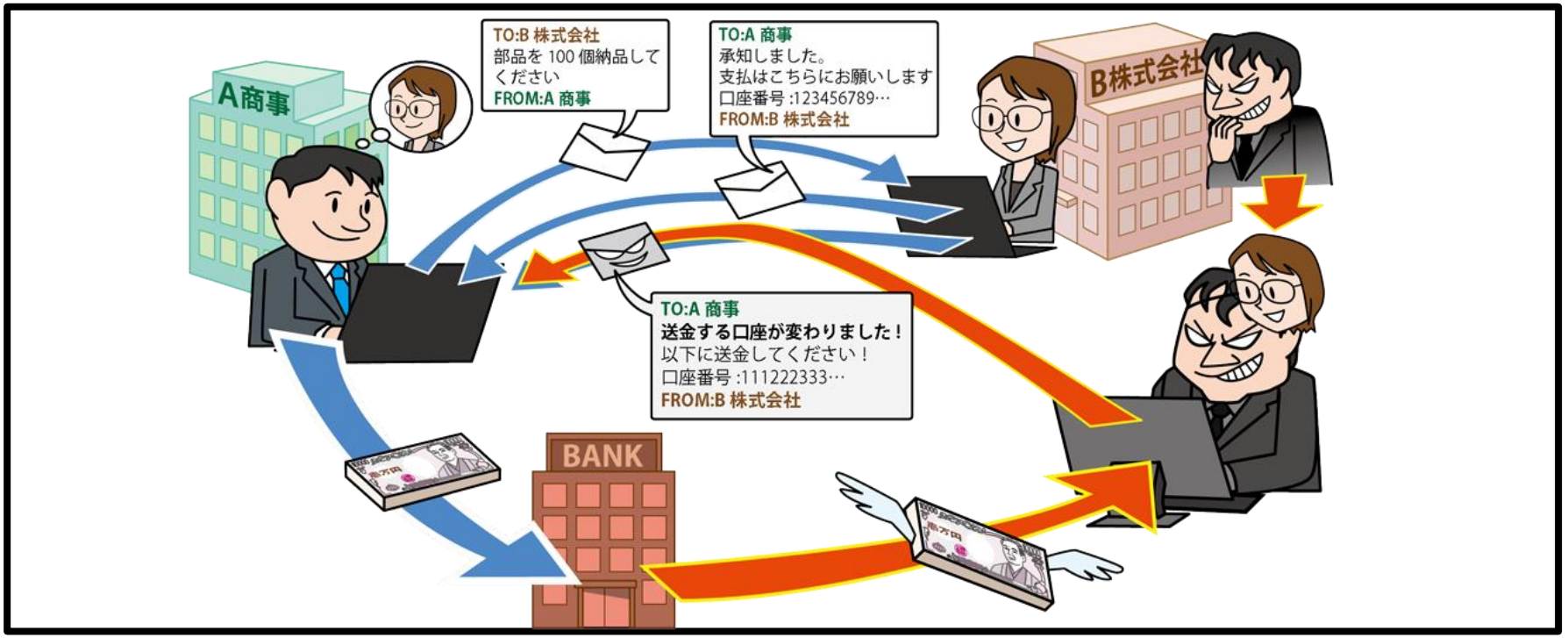
【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～



- 取引先や経営者とやりとりするような**ビジネスメールを装う**
- メールを巧妙に細工し、企業の**金銭を取り扱う担当者を騙す**
- 攻撃者が用意した口座へ送金させる

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

● 攻撃手口

・何らかの手段を用いて標的組織の業務情報等を窃取
・窃取した情報を悪用したメールで送金依頼（金銭詐取）

- 取引先との**請求書を偽装**
- 経営者等への**なりすまし**
- 窃取した**標的組織のメールアカウント**の悪用
- 社外の権威ある第三者への**なりすまし**
- 詐欺の準備行為と思われる情報の窃取

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

- 2022年の事例/傾向①
  - 正規のメールアドレスを乗っ取ったBEC(※1)
    - 2022年7月、サイバー情報共有イニシアティブ(J-CSIP)参加組織が**請求側企業の担当者になりすました**詐欺のメールを受信
    - 攻撃者は請求側担当者の**メールアドレスを乗っ取り**、支払側企業に**入金先の口座を変更**するように指示
    - メールのやり取りの際、Ccに請求側企業の関係者のメールアドレスに似せた偽のメールアドレスが指定されており、**詐欺の発覚を避ける巧妙な手口**

【出典】
※1 サイバー情報共有イニシアティブ(J-CSIP)運用状況[2022年4月～6月](IPA)
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000100056.pdf

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

- 2022年の事例/傾向②
  - 偽メールに従い送金し…後日、詐欺発覚 (※1)
    - 2022年11月、人材育成を行うウィルソン・ラーニングワールドワイドは**子会社2社**における同年9月の**ビジネスメール詐欺被害**を公表
    - 子会社は**悪意ある第三者より支払代金の送金を指示するメール**を受け取り、2社合わせて約530万円を送金
    - 送金後に詐欺の可能性に気付き、デジタルフォレンジック等による**事実関係確認、保険会社、捜査機関に対し相談等**を実施

【出典】
※1 当社子会社における資金流出事案の発生 並びに特別損失の計上に関するお知らせ(ウィルソン・ラーニング ワールドワイド株式会社)
https://ssl4.eir-parts.net/doc/9610/tdnet/2203725/00.pdf

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

● 対策

・被害の予防

－ビジネスメール詐欺への**認識を深める**

－**ガバナンスが機能**する業務フローの構築

　　個人の判断や命令で取引が行われないルールやシステムの構築

－**メールに依存しない**業務フローの構築

－メールに電子証明を付与（S/MIMEやPGP） **※なりすまし防止**

－DMARCを導入する　**※ドメイン認証失敗時のメール処理を判断する**

<メールの真正性の確認>

－メールだけでなく複数の手段で事実確認

－以下のようなメールに注意する

　普段とは異なる表現／**送信元のメールドメイン**／**判断を急がせる**

<メールアカウントの適切な管理>

－**パスワードの適切な管理**や**ログイン通知**機能、**多要素認証**等の利用

【7位】ビジネスメール詐欺による金銭被害

～そのメール、相手が誰か分かりますか？～

● 対策

・被害を受けた後の対応

- 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
- メールアカウントの設定を確認する
  攻撃者による**不正な転送設定**や**フォルダー振り分け設定等**を
  されていないか確認
- 被害を受けたメールサーバー上の**全メールアカウントのパスワード変更**