F－CSNET通信かわら版

令和5年1月

ビジネスメール詐欺に注意！

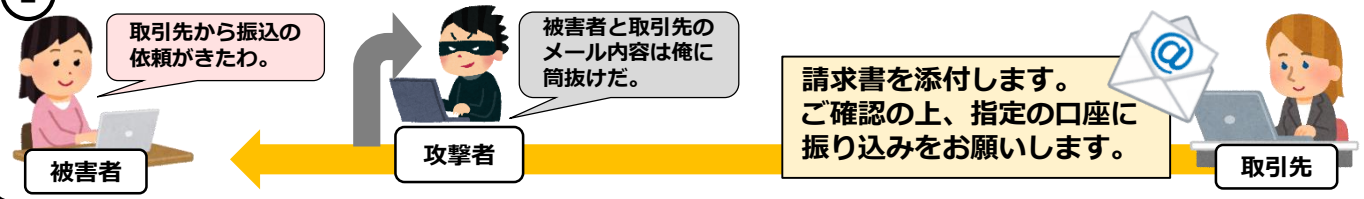
ビジネスメール詐欺（BEC）とは、巧妙に細工したメールのやりとりを通じて、企業の担当者をだまし、攻撃者が準備した口座へ送金させる詐欺の手口です。

従来、BECは英語が使用されていたため、海外との取引がある企業は要注意でしたが、現在は日本語の事例も確認されています。また、手口も巧妙化しているため、営業・渉外・財務・経理・会計等、各担当者の方は注意が必要です。

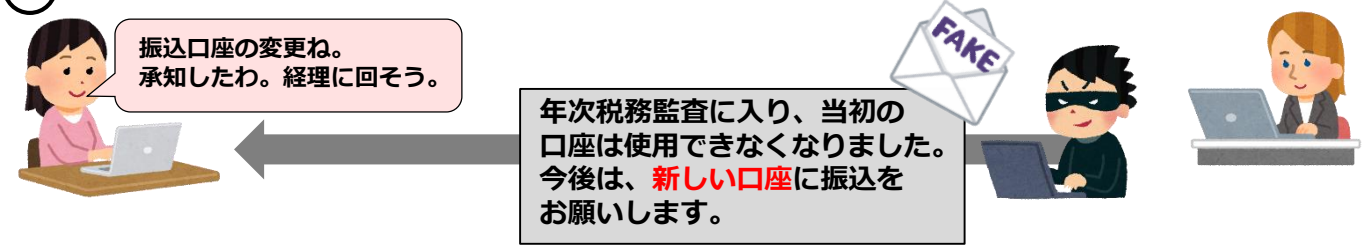
＊ BEC … Business Email Compromise（ビジネス・イーメール・コンプロマイズ）の略

ビジネスメール詐欺の一例をご紹介します。

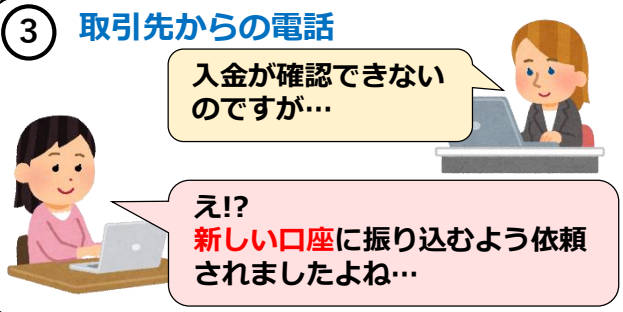
① 攻撃者が、取引先からの正規のメールを傍受



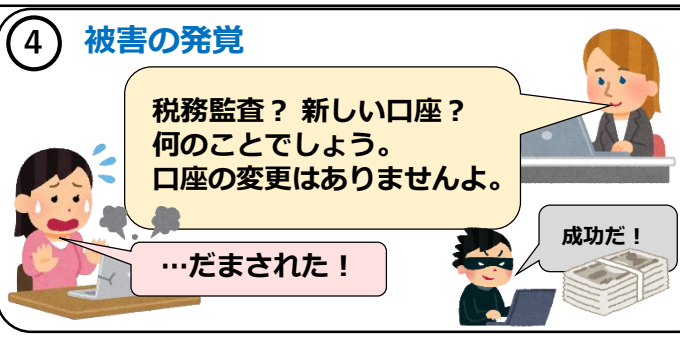
② 続いて、取引先になりすました攻撃者からの偽メール



③ 取引先からの電話



④ 被害の発覚



ビジネスメール詐欺による被害を防止するため、以下の点に注意してください。

① 取引先にメール以外の方法で確認　…　電話で直接確認するのは非常に有効です。
② 不審なメールに気づいたら、すぐに適切な部門に報告　…　素早く組織内で共有しましょう。
③ だまされたと気づいたら、すぐに送金依頼した銀行に連絡　…　取り戻せる場合もあります。
④ 送金に関する社内規定の整備　…　送金先の確認徹底を規定に盛り込みましょう。
⑤ メールサービスへの不正アクセスを防ぐ　…　セキュリティ更新で防御を固めましょう。

また、独立行政法人情報処理推進機構（IPA）は、「ビジネスメール詐欺の事例集を見る」の標題で、同機構が確認したBEC事例により注意喚起していますので、是非ご覧ください。

https://www.ipa.go.jp/security/bec/bec_cases.html

◆ 福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止・拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などをTwitterやホームページに掲載していますので、ぜひご覧ください。

【Twitter】

【HP】