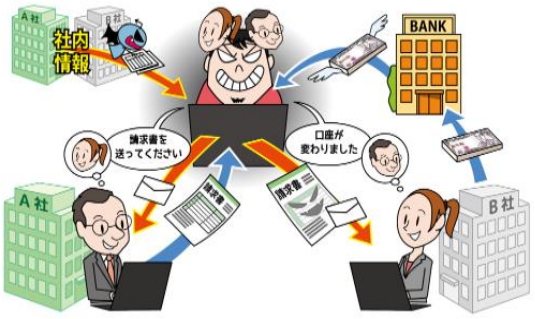
ビジネスメール詐欺に御注意を！

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、犯罪者が標的組織や企業の業務情報等を盗み、その盗んだ情報を悪用して、取引先や標的組織・企業の経営者等になりすまし、偽の電子メールで標的組織・企業の従業員を騙して送金取引に係る資金を騙し取る等の金銭被害をもたらすサイバー攻撃です。

ビジネスメール詐欺は、世界中で大きな被害をもたらしており、今後、被害が拡大するおそれがあります。

日本国内においても、継続して被害が発生しており、新型コロナウイルス感染症に関する内容が含まれたビジネスメール詐欺も確認されています。

ビジネスメール詐欺の手口（5つのタイプ）



（出典　IPA 独立行政法人情報処理推進機構）

- **取引先との請求書の偽装**
  （例） 取引メールのやりとりに割り込み、偽の請求書（振込先）を送る。
- **経営者等へのなりすまし**
  （例） 経営者を騙り、偽の振り込み先に振り込ませる。
- **盗んだメールアカウントの悪用**
  （例） メールアカウントを乗っ取り、取引先に対して詐欺メールを送る。
- **社外の権威ある第三者へのなりすまし**
  （例） 社長から指示を受けた弁護士といった人物になりすまし、振り込ませる。
- **詐欺の準備行為と思われる情報の収集**
  （例） 経営層や人事部になりすまし、今後の詐欺に利用するため、社内の従業員の情報を騙し取る。

対策

- **偽装メールでないかの確認**
  送金に関するメールを受信した際は、送信元のメールアドレスが本来の取引先等のメールアドレスに偽装されていないか、メールドメインをよく確認するとともに、内容や文章に不自然なところがないか確認する。
  また、取引担当者等に対して電話など、メール以外の方法で送金内容について確認する。（メールに記載されている電話番号は偽装されている可能性があるため、あらかじめ名刺交換等により入手している名刺に記載されている番号等に連絡する。）
- **添付ファイルやリンク先を不用意に開かない**
  犯罪者は標的組織・企業のパソコンをマルウェアに感染させたり、フィッシングサイトに誘導して、事前に社内の情報を収集しようとするので、添付ファイルやリンク先を不用意に開かない。
- **ウイルス対策の徹底**
  OS、ソフトウェア及びウイルス対策ソフトは、アップデートにより、最新の状態を保つ。
- **メールアカウントの適切な管理**
  犯罪者はメールサーバへ不正アクセスして、メールを盗み見ようとするので、メールアカウントには複雑なパスワードを設定し、パスワードの使い回しをしない。

【参考】 IPA 独立行政法人情報処理推進機構「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」（https://www.ipa.go.jp/files/000081866.pdf）
警察庁サイバー犯罪プロジェクト「ビジネスメール詐欺に注意！」（https://www.npa.go.jp/cyber/bec/index.html）

岩手県警察本部サイバー犯罪対策課の公式ツイッターはQRコードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

@Iwate_cyber

岩手県警察本部生活安全部サイバー犯罪対策課
令和3年8月 30 日発行