



ビジネスメール詐欺にご注意!!

日本航空(JAL)は、昨年12月20日、2件のビジネスメール詐欺(BEC)で、約3億8,000万円の被害を受けたと発表しました。

ビジネスメール詐欺とは、巧妙に細工したメールのやり取りにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口です。

ビジネスメール詐欺は、次に示す5つのタイプに分類できます。

タイプ1:取引先との請求書の偽装

(例) 取引のメールの最中に割り込み、偽の請求書(振込先)を送る。

タイプ2:経営者等へのなりすまし

(例) 経営者を騙り、偽の振込先に振り込ませる。

タイプ3:窃取した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を行う。

タイプ4: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などになりすまし、振り込ませる。

タイプ5:詐欺の準備行為と思われる情報の窃取

(例) 経営層などになりすまし、今後の詐欺に利用するため、社内の従業員の情報を窃取する。



攻撃の事実を知ることが第一歩!!

ビジネスメール詐欺の被害に遭わないためには、まずこのような攻撃があるという事実を知ることが重要です。ビジネスメール詐欺は、電子メールに依存した企業間のビジネス活動につけ込み、巧妙な罠を仕掛けていきますので、技術的な対策だけで防御することは難しく、一人ひとりがその手口を理解し、次のような対策を行ってください。

● 送金前のチェックの強化

ビジネスメール詐欺を想定し、送金などの際のチェック体制を強化する。振込先が変更となった場合、電話などメール以外の方法で確認する。

● 普段とは異なるメールに注意

普段とは異なる言い回しや文脈、送信者のメールアドレスなど、不審なメールには注意する。

● 基本的なウイルス・不正アクセス対策

不審なメールの添付ファイルを開かないように注意するとともに、OSやアプリケーション・セキュリティソフトを最新に保ち、パスワードには複雑なものを設定する。



※詳しくはIPAのWebサイトを
確認してください。



サイバー犯罪(インターネットに関する犯罪)の通報やご相談は...

石川県警察本部生活環境課サイバー犯罪対策室



076-225-0110



cyber@police.pref.ishikawa.lg.jp

