

# 滋賀県警察からのお知らせ

## ビジネスメール詐欺「BEC」に注意

ビジネスメール詐欺（Business E-mail Compromise : BEC）とは、巧妙に細工したメールのやりとりにより、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。国内企業や海外関連企業、あるいはその取引先が狙われる金銭被害が発生しており、国内でも逮捕者が出るなど、注意が必要な状況にあります。



### ビジネスメール詐欺のタイプ

#### 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といった人物になりすまし、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搾取

(例) 経営層や人事部になりすまし、詐欺に利用するため、社内の従業員の情報を窃取する。

### ビジネスメール詐欺への対策

ビジネスメール詐欺の手口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、巧妙な罠をしかけてきます。

技術的な対策だけでは防御することが難しいので、手口を理解し、対策を行って下さい。

#### 対策 1 送金前のチェックの強化

ビジネスメール詐欺を想定し、送金等の際のチェック体制を強化しましょう。振込先の変更のような場合、電話や FAX などメール以外の方法で確認しましょう。

#### 対策 2 普段とは異なるメールに注意

普段とは異なる文脈や、送信者のメールアドレス等怪しいと思うメールには注意しましょう。

#### 対策 3 基本的なウィルス・不正アクセス対策

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、パスワードは複雑なものに設定し、不審なメールの添付ファイルを開かないよう注意しましょう。