そのメール、本当に信じて大丈夫？

～日本企業を狙う**ＢＥＣ（ビジネスメール詐欺）**の脅威拡大
新型コロナウイルス感染症の事例発生、さらに巧妙悪質に！～

○　BEC (**B**usiness **E**mail **C**ompromise) とは

- 日本語では“ビジネスメール詐欺”などと訳される
- 取引先、自社役員、外部の弁護士などを装い、業務関連のメールを送信し、送金を要求する詐欺
- **新型コロナウイルス感染症への対応名目**の事例が発生
- 被害額は、極めて高額

○　被害の概要

- 世界的な情勢（ＦＢＩの発表）
  2016年6月～2019年7月　世界177カ国
  約16万6千件　被害額　約262億米ドル（未遂含む）

- 国内企業に関する事例
  2017年12月　大手航空会社　３億円超の被害の報道
  2019年　8月　大手自動車部品メーカーの子会社
  約40億円の資金流出の報道
  2019年　9月　大手新聞社の子会社
  約2,900万ドルの資金流出の報道　など

岡山県警察本部　サイバー犯罪対策課

○　メールで注意するポイント

1　メール内容

・内密な取引や至急の取引への振込要求

・振込先口座や決済手段の変更

2　メールアドレス

・類似ドメインの使用（１文字違いなど）

（例）正　example@example.com　(小文字のエル)

　　偽　example@examp1e.com　(半角数字の１)

・表示の偽装（送信者欄など）

○　被害を防ぐために

重要!

まずは、

・電子メールを使うあらゆる企業・団体が狙われる

・セキュリティ対策が不十分であるほど狙われやすい

ことを認識し、被害防止のため、以下の事項を心がけて下さい

確認手段の確立
- メール以外の確認手段（電話、ＦＡＸなど）
- 確認先部署の設定

自社の社内規定整備
- 担当部署の明確化
- 複数担当者によるチェック

ウイルス・不正アクセス対策
- セキュリティソフト導入
- ＯＳなどの定期更新
- パスワード設定見直し

組織内外の情報共有
- 部内の情報共有
- 取引先への注意喚起

→より詳しく知りたい方は

参考　独立行政法人 情報処理推進機構
【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（第３報）
https://www.ipa.go.jp/security/announce/2020-bec.html

岡山県警察本部　サイバー犯罪対策課