



2022年10月  
第14号



# ビジネスメール詐欺対策について

ビジネスメール詐欺とは、巧妙な手口を駆使した偽の電子メールを組織・企業に送付して、従業員を騙して**送金取引に係る資金をだまし取る**といった、金銭が狙われるサイバー攻撃です。取引に関する資金を詐取することから、**一度の被害額が大きい**のも特徴です。

このビジネスメール詐欺の中でも、事例が多いパターンが2種類あります。

## 【パターン1：取引先との請求書の偽装】

取引先と請求に関するやり取りをメールで行っている際に、攻撃者が取引先になりすまし、「振込先が変わりました」などと攻撃者が用意した口座を送金先として指定したり、送金先を攻撃者が用意した口座に差し替えた請求書を送りつけて、振り込みをさせるパターン



## 【パターン2：経営者になりすまし】

攻撃者が企業の経営者や幹部などになりすまし、金銭管理を担当する従業員などに「秘密の案件がある」「相談したいことがある」といった問い合わせから始まり、最終的には従業員に攻撃者の用意した口座へ送金させるパターン



いずれのパターンでも、取引先や経営者などの情報やメールのやり取りが攻撃者によって盗まれている場合が多いです。

情報を盗むマルウェアを利用している場合もあります。

## 対策

- ・取引先と**メール以外**で確認
- ・**普段と異なるメールアドレス**や**フリーメール**に要注意
- ・不審に感じたら**組織内外で情報共有**
- ・メールの返信は『返信』ではなく『**転送**』を利用して登録のアドレスに実施
- ・ウイルス・不正アクセス対策の実施
- ・**電子署名**の付与

これ以外にも様々な対策がありますが、**組織の一人一人がどういう攻撃があるのかを理解することが重要です！**

出展：IPA ビジネスメール詐欺(BEC)対策の特徴と対策  
<https://www.ipa.go.jp/files/000102392.pdf>

**被害が判明したらすぐに警察に通報を！**

Twitter



@IP\_cybertaisaku

石川県警察本部生活安全部サイバー犯罪対策課



076-225-0110



cyber@police.pref.ishikawa.lg.jp

Instagram



IP\_cybertaisaku