マンスリー・ハイライト　拝啓社長殿

マネジメントのための経営財務情報

今回のテーマ：　ビジネスメール詐欺の被害実態と対策

標的型メール攻撃やビジネスメール詐欺（Business E-mail Compromise：BEC）は近年増加傾向にあります(2019/9/26 警察庁)。「BEC に関する実態調査 2018」(トレンドマイクロ社)では全体の約 4 割が BEC 攻撃を経験し、その内の約 6 割が送金口座の変更や至急案件等による送金依頼メールを実際に受信し、その内の 1 割弱(調査全体の 2%)が実際に指定口座に送金してしまったことが分かっています。

送金被害額の約 5 割が 5,000 万円未満ですが、億単位の送金被害も発生しています。最近では、日本航空では 2017 年 9 月に 3. 8 億円の BEC 被害を受け、トヨタ紡績ヨーロッパでは 2019 年 8 月に約 40 億円の資金が流出し、BEC 被害の可能性が指摘されています(2019/9/6 日本経済新聞、Forbes)。

ビジネスメール詐欺

ビジネスメール詐欺(BEC)は、偽の電子メールを企業に送り、従業員を騙して送金取引に係る資金を搾取する詐欺行為や、自社の役員や従業員に関する個人情報・業務提携先に関する情報・非公開の機密情報といった特定の情報の窃取する行為を指します。

業務に偽装した標的型メール攻撃を組み合わせ、添付ファイルの開封等を誘導して不正プログラムを感染させることにより、企業のメール内容等を窃取したうえで上記の詐欺行為を仕掛けてくるようなケースもあります。

2019 年セキュリティ対策投資額は約 6 割の企業が前年同水準に留まり、多くの企業が同投資に関し「予算の確保」「導入効果の測定が困難」として課題の顕在化を指摘しています（IDCJapan2019 年国内企業の情報セキュリティ対策実態調査結果)。

ビジネスメール詐欺の類型と主な対策例

類型	主な対策例
・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	・振込先の変更・内密・迅速な行動を促す請求は疑い、社内で他の担当者と情報共有して確認する ・メール以外の手段も使用し、その際電話番号等はメール内署名記載を頼らずに既知のものを使用する ・普段とは異なる言い回しや表現の誤りには注意する
・経営者や顧問弁護士を騙り、偽の振込先に振込ませる ・経営層や人事部を騙り、従業員の情報を窃取し今後の詐欺に利用する	
・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	・会社のメールアカウントは多要素認証を行い、当事者しか持たないもの(トークン等)を使用する ・返信時に相手先のメールアドレスの変更の有無を確認、変更事実の有無を電話等で別途確認する

お見逃しなく！

海外取引メールなど外国語による BEC が多く発生していますが、2018 年に日本語で CEO を騙る事案、日本人による BEC 事案も発生しており、国内取引がメインの企業も注意が必要です。