サイバーセキュリティ通信 Vol.6

令和２年７月
【長崎県サイバーセキュリティに関する相互協力協定機関】

サイバァちゃん

ビジネスメール詐欺に注意！

最近、長崎県内においても、メールにおいて取引先や経営者等になりすまし、企業の担当者を騙して犯人の口座に送金させるビジネスメール詐欺が発生しています。

ビジネスメール詐欺（Business E-mail Compromise ： 通称“BEC”）

どんな手口？

○ 取引先との請求書の偽装
取引先とのメールのやり取りの最中に割り込み、偽の請求書を送る。

○ 経営者へのなりすまし
メールにおいて自社の経営者を騙り、偽の振込先に振り込ませる。

○ 社外の権威ある第三者になりすまし、振り込ませる
会社から依頼を受けた弁護士などと偽り、犯人の口座に送金させる。

○ 詐欺の準備行為と思われる情報の詐取
人事部等になりすまし、今後の詐欺に利用するため、従業員の情報を詐取する

○ 本物と同じ又はよく似たメールアドレスの使用
本物と同じメールアドレスを偽装したり、よく似たメールアドレスを使用する。

代表的な攻撃手法

○ 犯人が何らかの方法で、取引先との連絡を盗み見し、取引先の正規メールアドレスに酷似した偽のメールアドレスから、正規の取引にかかる請求を行う。
その際、『従来の口座が使用できなくなった』など様々な理由をつけて、犯人の口座に送金するよう指示する。

○ 犯人が出張中の経営陣になりすまし、取引に必要な費用を送金するよう指示、その際、契約が成立がするまで口外しないようにとの指示を受け、被害に気づくのが遅れてしまう。

被害を予防するために

○ 普段と異なるメールに注意
不審なメールは社内で相談・連絡し、情報共有する。

○ 電信送金に関する社内規定の整備
メールの内容に、急な振込先や決済手段の変更等が含まれていた場合、取引先へメール以外の方法で確認する。

○ ウイルス・不正アクセス対策
セキュリティソフトを導入し、最新の状態にする、メールアカウントに推測されにくい複雑なパスワードを設定する、多要素認証の導入を検討する。　など

長崎県警察本部サイバー犯罪対策課　095-820-0110（3451・3452）　ﾒｰﾙｱﾄﾞﾚｽ e103108@police.pref.nagasaki.jp