富山県警察本部　サイバー犯罪対策課

サイバーセキュリティの置き薬

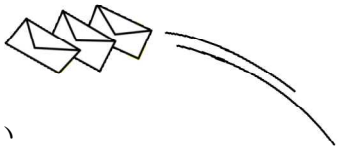
平成30年
第6号

ビジネスメール詐欺はご存知ですか？

ビジネスメール詐欺とは

実際の取引先相手や自社の経営者層等になりすまし、メールを使って振込先口座の変更等を指示するなどしてお金を騙し取る手口です。

ケース１　取引先担当者等になりすまし



・財務調査が入っており、従来の口座が使用できない
・従来の口座が不正取引に使用され、凍結されてしまった
・技術的な問題が発生しており、従来の口座が使用できない

など様々な理由をつけて、メールで振込先口座の変更を指示してくる例

標的型メール攻撃で狙われた情報（取引先や顧客とやり取りしたメール）が悪用されるかも

ケース２　経営者層等になりすまし

・　極秘の買収案件で、資金が必要になった

などの理由で指定する口座への入金を指示した上で、さらに

・　緊急かつ内密に送金してほしい
・　飛行機に乗るので連絡が取れなくなる

などと付け加えて、担当者のみに判断させ、詐欺であることが発覚するのを防ごうとする例

これ以外にも、法律事務所や弁護士といった社外の権威のある第三者になりすましたり、取引先のメールアカウントを乗っ取り犯人の口座に誘導したりする等の手法もあります。

【ビジネスメール詐欺を防ぐ対策】

○ 送金や情報提供を促すメールは注意深く確認する。
○ メール以外の方法で確認する。
○ 規則に従って（承認プロセスを経る等）行動する。
○ OS・ソフトウェアを最新の状態にしておく。
○ メールの添付ファイルは安易に開かない。
○ メールに記載されたURLをクリックしない。

標的型攻撃メールの時と同様に、不審メールが届いた際は、組織内で**情報共有**することが**重要**です。

※サイバーセキュリティの置き薬とは
富山の薬売りで親しまれている「置き薬」になぞらえて、皆さんのサイバーセキュリティ対策の助けとなる様に情報を発信していくものです。