8 BEC（ベック）ビジネス詐欺メール

●ビジネス詐欺メールとは

ビジネスメール詐欺（BEC：Business E-mail Compromise）は、特定の企業をターゲットにしたものです。用意周到に事前に何らかの方法で従業員のメールを盗み見たうえで、偽のメールを送り資金をだましとる巧妙な詐欺の手口です。

実際の被害事例では、犯人は、正規の取引先からの請求書がPDFで届いた直後に偽の請求書を送信していて、そっくりのフォーマットで「訂正版」としていたそうです。また、送信元メールアドレスも、正規の担当者のアドレスに似せたものを使用していました。

●ビジネスメール詐欺の手口

海外では何年も前からビジネスメール詐欺の被害が報告されており、米国連邦捜査局（FBI）の2022 Internet Crime Reportによると2022年のビジネスメール詐欺の被害額は27億ドル以上ともいわれています。

過去の事例では、取引先を装った手口のほか、社長や経営幹部になりすました振込み依頼メールや弁護士・法律事務所になりすますなど、さまざまな手口が報告されています。

右の図のとおり、①攻撃者が標的のメールのやりとりを盗聴し、②攻撃者が取引先を装い、標的へ偽メールを送ります。③で標的となった従業員がだまされて送金し、④攻撃者の用意した口座に入金されます。犯罪者は詐欺にかける企業をよく調べて、社内の決裁処理も熟知したうえで、通常メールに紛らせて詐欺メールを送ってくるのです。大変巧妙な手口のため、“ビジネスメール詐欺”という手口を知らなければ、見破るのは非常に難しくなっています。

メールの特徴

米国インターネット犯罪苦情センター（IC3）やトレンドマイクロ社では、ビジネスメール詐欺の手口を主に次の5つの特徴に分類しています。

1．取引先になりすまし偽の請求書を送る
2．経営者や企業幹部になりすます
3．メールアカウントを侵害する
　ある企業の従業員のメールアカウントが乗っ取られ、取引先に対して請求書の支払い依頼メールが送信される
4．弁護士などの権威ある第三者になりすます
　企業の顧問弁護士などになりすまし、緊急を要する機密の案件で早急に送金を指示するようなメールが送信される
5．詐欺準備としての情報をだましとる
　金銭ではなく、詐欺を行うために企業の特定の従業員の情報をぬすみとるようなメールが送信される

対処法

周到に準備されているため、正規のメールとそっくりの偽メールを見抜くのは非常に難しくなっています。

そのため、特に企業における資金取引に関係する担当者の方は、ビジネスメール詐欺の脅威を知り、あらかじめ対策を制度化しておくことが重要です。

例えば、送金に関するメールの場合は、電話などのメール以外の方法で口座の確認をするなど2ファクタの認証プロセスを設けるなどが有効です。普段と異なる対応を求められた場合は、担当者だけで判断せず、必ず社内の認証プロセスを経たうえで処理を行うことを担当者や従業員に周知徹底しておくようにしましょう。

ビジネスメール詐欺については、以下のサイトでも詳しく注意喚起をしていますので、社内の資金取引に関する部署へ周知する際の参考としてください。

参考サイト

✓（独）情報処理推進機構（IPA）：ビジネスメール詐欺（BEC）対策特設ページ
https://www.ipa.go.jp/security/bec/about.html