中小企業の

セキュリティー対策

—12—

ビジネスメール詐欺拡大

巧妙に細工し 偽口座へ送金促す

企業に甚大な被害を及ぼす新たな脅威として「ビジネスメール詐欺（Business E-mail Compromise：BEC）」が全世界に拡大している。巧妙に細工したメールのやりとりにより、企業の担当者をだまし、攻撃者の用意した口座へ送金させる手口の詐欺である。

これまでは主に海外の企業が被害に遭ってきたが、2016年以降、海外取引をしている国内企業やその関連企業、あるいはその取引先が狙われ被害が確認されている。17年末には航空会社にて約3億8千万円の被害が報道されるなど、注意が必要な状況となってきている。

ビジネスメール詐欺は、次に示す五つのタイプに分類できる。

【タイプ1：取引先との請求書の偽装】

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。

【タイプ2：経営者などへの成り済まし】

経営者をかたり、偽の振込先に振り込ませる。

【タイプ3：窃取メールアカウントの悪用】

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。

【タイプ4：社外の権威ある第三者への成り済まし】

社長から指示を受けた弁護士といった人物に成り済まし、振り込ませる。

【タイプ5：詐欺の準備行為と思われる情報の詐取】

経営層や人事部に成り済まし、今後の詐欺に利用するため、社内の従業員の情報を窃取する。

攻撃者は、その過程において、偽のメールアドレスを使うだけでなく、さまざまなだましのテクニックを駆使してくることが確認されている。

例1：請求者側と支払者側の両方に成り済まし、取引に関わる二つの企業を同時にだます

例2：メールの同報先（CCなど）も偽物に差し替え、他の関係者にはメールが届かないよう細工する

例3：メールの引用部分にある、過去のメールのやりとりの部分について、都合の悪い部分を改変する

手口の悪質さ・巧妙さに関しては、諜報活動などを目的とする〝標的型サイバー攻撃〟とも通じるところがある。

手口を理解し 一人一人が対策

ビジネスメール詐欺の被害に遭わないようにするには、まずこのような攻撃があるという事実を知ることが重要だ。また、この手口は、根本的には「詐欺」なのだが、電子メールに依存した企業間のビジネス活動に付け込み、巧妙な罠を仕掛けてくる。これに対し、技術的な対策だけでは防御することが難しく、一人一人が手口を理解し、次のような対策を行ってほしい。

【対策1：送金前のチェックの強化】

ビジネスメール詐欺を想定し、送金などの際のチェック体制を強化する。振込先の変更のような場合、電話やFAXなどメール以外の方法で確認する。

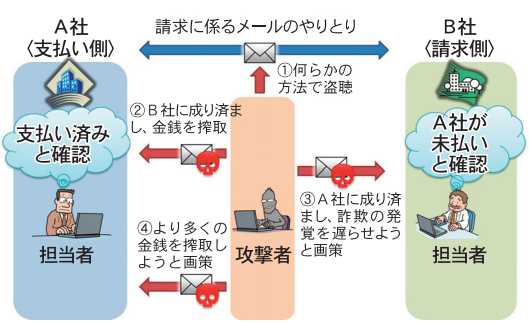
【対策2：普段とは異なるメールに注意】

普段とは異なる言い回しや文脈、送信者のメールアドレスなど、怪しいと思うメールには注意する。

【対策3：基本的なウイルス・不正アクセス対策】

不審なメールの添付ファイルを開かないよう注意する。また、OSやアプリケーション・セキュリティーソフトを最新に保ち、パスワードには複雑なものを設定する。

独立行政法人情報処理推進機構（IPA）では注意喚起とともに、レポート「ビジネスメール詐欺『BEC』に関する事例と注意喚起」を公開している。具体的な内容はIPAのホームページ（https://www.ipa.go.jp/security/index.html）を確認してほしい。

（独立行政法人情報処理推進機構・江島将和）

ビジネスメール詐欺の手口