ビジネスメール詐欺に注意

対策などまとめた特設ページを開設

独立行政法人情報処理推進機構（IPA）は9月28日、ビジネスメール詐欺（Business E-mail Compromise：BEC）の手口や対策、関連情報をまとめた特設ページを公開した（QRコード参照）。

ビジネスメール詐欺とは、巧妙に細工したメールのやりとりで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詐欺の手口である。本連載Vol・38「ビジネスメール詐欺 国内企業も標的に」（QRコード参照）でも取り上げて注意喚起を行ったが、米国連邦捜査局（FBI）や米国インターネット犯罪苦情センター（IC3）が公開している情報によると、年々被害は増加傾向にある。改めて注意喚起を行いたい。

巧妙化する手口

IPAでは、主に「取引先との請求書の偽装」「経営者などへのなりすまし」の2タイプの手口を確認している。

「取引先との請求書の偽装」は、取引先と請求に係るやりとりをメールなどで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書を送り付け、振り込みをさせるというものである。

「経営者などへのなりすまし」は、攻撃者が企業の経営者や企業幹部（役員）などになりすまし、企業の従業員に攻撃者の用意した口座へ振り込みをさせるというものである。

ビジネスメール詐欺は、メールのなりすましなどのサイバー攻撃の手法を用いつつ、巧妙に人を騙す手口である。そのためシステムやセキュリティソフトによる機械的な防御、偽メールの排除が難しいことが被害抑止を難しくしている。

従って、まずは企業や組織の従業員に、このような詐欺の手口があるということを知っていただく必要がある。その上で、次のような対策を行うことが望ましい。

・普段と異なるメールに注意し、不審なメールは社内で情報共有する
・電信送金に関する社内規定を整備し、急な振込先や決済手段の変更などが発生した場合、取引先へメール以外の方法で確認する
・ウイルス・不正アクセス対策を実施する。具体的には、セキュリティソフトの導入、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、メールシステムでの多要素認証やアクセス制限の導入を検討するなど
・警察や銀行へ連絡を早期に送金のキャンセルや組み戻しの手続きを依頼する

原因調査と社内外への注意喚起を

ビジネスメール詐欺の被害が判明した場合、次のような対応を行うことが有効である。

・偽の口座へ送金を行ってしまった場合、送金に利用した銀行へ、資料としてログを含め証跡の提示を求められる可能性があるため、可能な限り攻撃者から送られてきたメールなどは確保し、状況の把握やどのような経緯でメールが送られてきたかなどをまとめておく
・ビジネスメール詐欺が判明した際に、暫定対応と原因調査を行う。具体的には、関係者のPCに対するウイルスチェックの実施、関係者のメールアカウントのパスワード変更、関係者のメールアカウントへの不正アクセス痕跡の調査、関係者へメールアカウントを不正利用される原因に覚えがないかヒアリング、社内外へ向けた注意喚起など

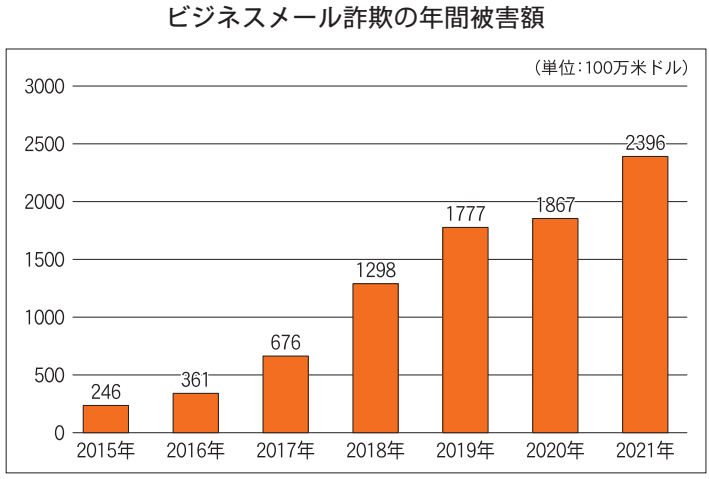
◇　◇　◇

手口や対策の詳細や、被害事例については、特設ページを確認してほしい。同様被害の早期発見や未然防止といったセキュリティ上の取り組みの促進につながることを期待する。

（独立行政法人情報処理推進機構・江島将和）

「取引先との請求書の偽装」のイメージ

ビジネスメール詐欺の年間被害額



IC3報告書を基にIPA作成

BEC対策特設ページ

連載Vol・38（日商Assist Biz）