プレスリリース
2019 年 7 月 26 日
独立行政法人情報処理推進機構

本年確認されたビジネスメール詐欺の事例を解説、J-CSIP 運用状況レポートを公開

～「新規取引」において「振込口座が偽か否かの確認を難しくさせる」手口を確認～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、国内重要産業における標的型攻撃の情報共有の枠組みである、サイバー情報共有イニシアティブ（J-CSIP）[*1] の運用状況レポート（2019 年 4 月-6 月）を公開しました。この中で、本年 4 月以降に確認されたビジネスメール詐欺（以後、BEC [*2]）の攻撃事例のうち 2 件を解説しています。

URL：https://www.ipa.go.jp/files/000076713.pdf

IPA が本日公開した J-CSIP の運用状況レポートでは、運用している参加組織の総数、および活動の主軸である、参加組織から寄せられたサイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の提供が行われた件数と、それらの情報をもとに参加組織へ情報共有を実施した件数をまとめています。

これに加え、2019 年 4 月以降に確認された BEC の攻撃事例のうち 2 件を解説しています。その中でも特筆すべきは、「新規の取引先への最初の支払いの時点」で攻撃が行われ、かつ「振込口座が偽か否かの確認を難しくさせる」手口が確認されたことです。

具体的には、新規取引先とのやり取りに介入して、偽口座を記載した見積書を「差し替え」と称して送付し、本物の見積書の破棄を依頼する、という手口です。本件では、取引の開始前からメールが盗み見られていたものと考えられます。巧妙なのは、あくまでも**見積金額の変更**という趣旨の偽メールで見積書の差し替えを依頼しつつも、**書類上は振込口座も改変**していた点です。加えて、直前に送られた見積書（正規の取引先から送られた本物の見積書）の破棄を促し、振込先が偽口座に変わったことの発覚を難しくさせていました。

BEC は手口が巧妙なだけでなく、一般的に金銭被害が多額になる傾向があります。一方、システムやセキュリティソフトによる機械的な防御だけでは、偽メールの排除が難しく、対策が困難でもあります。被害の防止には、取引を行う担当者だけでなく、決済処理を行う経理部門等もこの手口を認識し、チェック体制を整備することが必要です。今回の事例は、相手が新規取引先であったため、過去の支払い実績もなく、見破ることが難しいものです。必要に応じ、既存のチェック体制の見直しも検討することを勧めます。

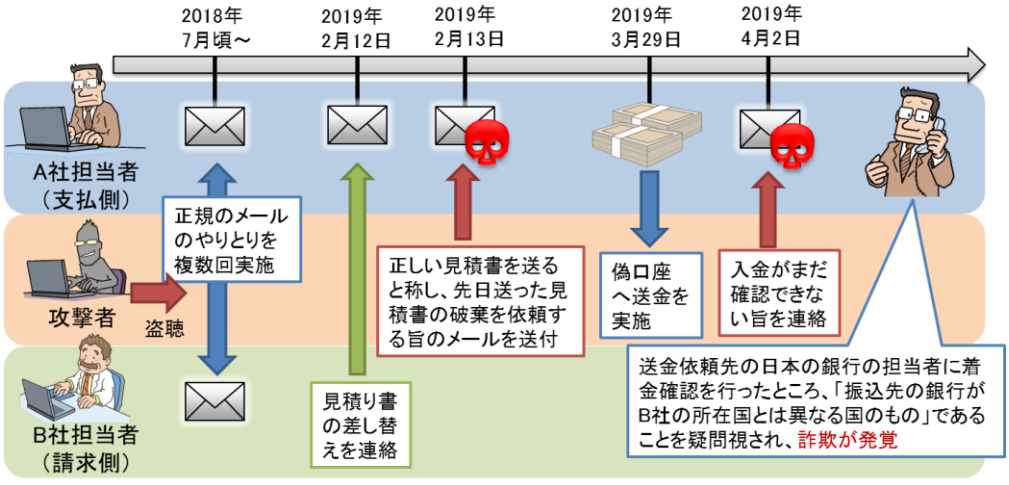

図 1 ：メールでの一連のやりとり

[*1] https://www.ipa.go.jp/security/J-CSIP/index.html
[*2] Business E-mail Compromise

IPA では BEC の手口について引き続き注意が必要と考えています。手口の詳細などはレポートをご確認ください。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　松坂／伊藤（博）
Tel: 03-5978-7535　E-mail: isec-info@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部　広報戦略グループ　白石／伊藤（美）
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp