「ビジネスメール詐欺に対する注意喚起」（出典：IPA 他）の一部を編集、

文責：河東岩夫威、作成日：平成 30 年 05 月 31 日

【はじめに】: 2016 年には身代金要求型不正プログラム「ランサムウェア 2」が世界中で猛威を振るい、重要なデータと引き換えに個人・法人が身代金を要求される被害が急増したが、その影に隠れ、法人組織に甚大な被害を及ぼす新たな脅威が全世界に拡大している。この脅威は法人組織の従業員を騙し、不正な送金処理を実施させる詐欺の手口で「ビジネスメール詐欺：Business Email Compromise(BEC)」と呼ばれる。日本国内ではまだ認知は低いものの、米国連邦捜査局(FBI)からは既にその被害の深刻さが公表されている。ランサムウェアと比較しても BEC がサイバー犯罪者にとって高額な収益を得ることができる手口であるので、2017 年にはより多くのサイバー犯罪者が BEC に注目し、その被害も増加すると予測されている。今後、日本でも増加することが予測されるため、日本国内の法人組織では BEC の脅威を理解し、対策を実施していく必要がある。ビジネスメール詐欺は巧妙に細工したメールのやり取りによって企業の担当者をだまし、攻撃者が用意した口座に送金させる詐欺で 2 月にはこれに伴う逮捕者が出たとの報道もあった。国内でも J-CSIP に加入する複数企業からこうした手口の攻撃が起きており、実際に被害が生じているという。

【ビジネスメール詐欺のタイプ】: IPA(独立行政法人情報処理推進機構)では情報提供を受けた事例の記録を分析し、ビジネスメール詐欺を以下の 5 項目のタイプに分類した。

1)取引先との請求書の偽装、2)経営者等へのなりすまし、3)接種メールアカウントの悪用、4)社外の権威ある第三者へのなりすまし、5)詐欺の準備行為と思われる情報の詐取

【内部統制上の対策】: BEC は、その攻撃手法の特性上、セキュリティソリューションで防ぎきることが難しい脅威である。BEC の手口の中で用いられる、フィッシングメール、キーロガーが添付されたメールはメールセキュリティ対策製品で防ぐことができるが、最終的に送られてくる偽の送金指示メールや支払い依頼メール等は通常の業務メールのやり取りと何ら変わらない形で送られてくるため、メールセキュリティ対策製品をすり抜けてくることが想定される。そのため、BEC の脅威に対しては、その手口に騙されないために内部統制上、次のような送金処理に関する決済手順の整備・徹底や自組織の従業員の教育を行い、リスクをできる限り低減することが非常に重要である。

1. **送金処理に関する社内整備：** BEC による不正送金は高額の被害をもたらす危険性が高いため、リスクを低減させるためにも以下の 4 項目の決済処理に関するポリシーや手順の整備が必要である。

1)送金処理に関する社内ポリシーならびに処理・承認のプロセスや手順を文書化する。

2)一定額を超える送金処理の場合、稟議制度といった複数の階層、段階を通さないと承認されないような仕組みを制度化する。

3)高額か否かに関わらず送金処理については社内システム上登録されたものしか処理できない仕組みにする。

4)振込先の変更等の手続きはメール等で行うのではなく書面での通知や本人確認ができているもののみを処理できるようにする。

2. **従業員に対する教育：** 標的組織の幹部や従業員になりすました偽の送金指示メール、支払い依頼メール等を受信した場合に備え、従業員に以下の 5 項目を徹底させるセキュリティ教育の実施が有効である。

1)従業員に対して自組織のセキュリティポリシーを徹底させる。

2)不自然な形で自組織幹部から緊急の送金依頼案件等のメールを受信した従業員はメールを注意深く精査し、依頼案件が妥当であるか慎重に確認する。

3)クラウドメールサービスを利用している場合、特に認証情報を詐取しようとするフィッシングメールに注意する。

4)取引先の支払い情報が変更される場合、自組織の承認プロセスに従って処理するよう従業員に徹底させる。

5)送金依頼案件の場合、メールに記載された電話番号ではなく、いつも使用している取引先や幹部の電話番号等に直接連絡してダブルチェックを行う。