IPA Information-technology Promotion Agency, Japan

ビジネスメール詐欺「BEC」に関する事例と注意喚起

要約版

この注意喚起に関する詳しい資料は、次のURLで公開しています。
https://www.ipa.go.jp/security/announce/20170403-bec.html

2017年4月3日

独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

ビジネスメール詐欺の概要

ビジネスメール詐欺（Business E-mail Compromise：BEC）とは、巧妙に細工したメールのやりとりにより、企業の担当者を騙し、**攻撃者の用意した口座へ送金させる詐欺の手口**です。国内企業や海外関連企業、あるいはその取引先が狙われ金銭被害が発生しており、また、国内でも逮捕者が出るなど、注意が必要な状況にあります。

ビジネスメール詐欺は、次に示す5つのタイプに分類できます。

タイプ1：取引先との請求書の偽装

（例）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：経営者等へのなりすまし

（例）経営者を騙り、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

（例）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なりすまし

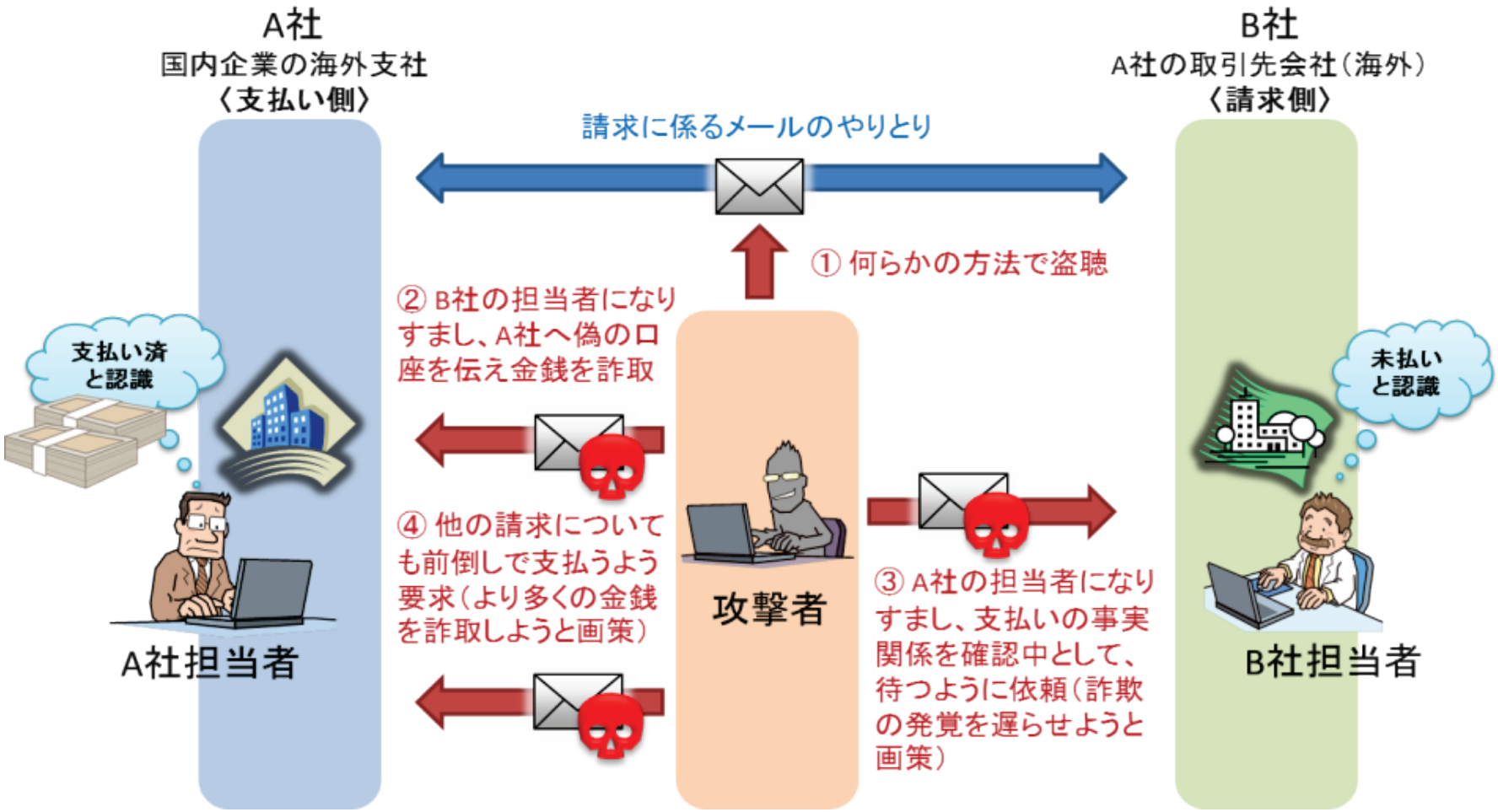
（例）社長から指示を受けた弁護士といった人物になりすまし、振り込ませる

タイプ5：詐欺の準備行為と思われる情報の詐取

（例）経営層や人事部になりすまし、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

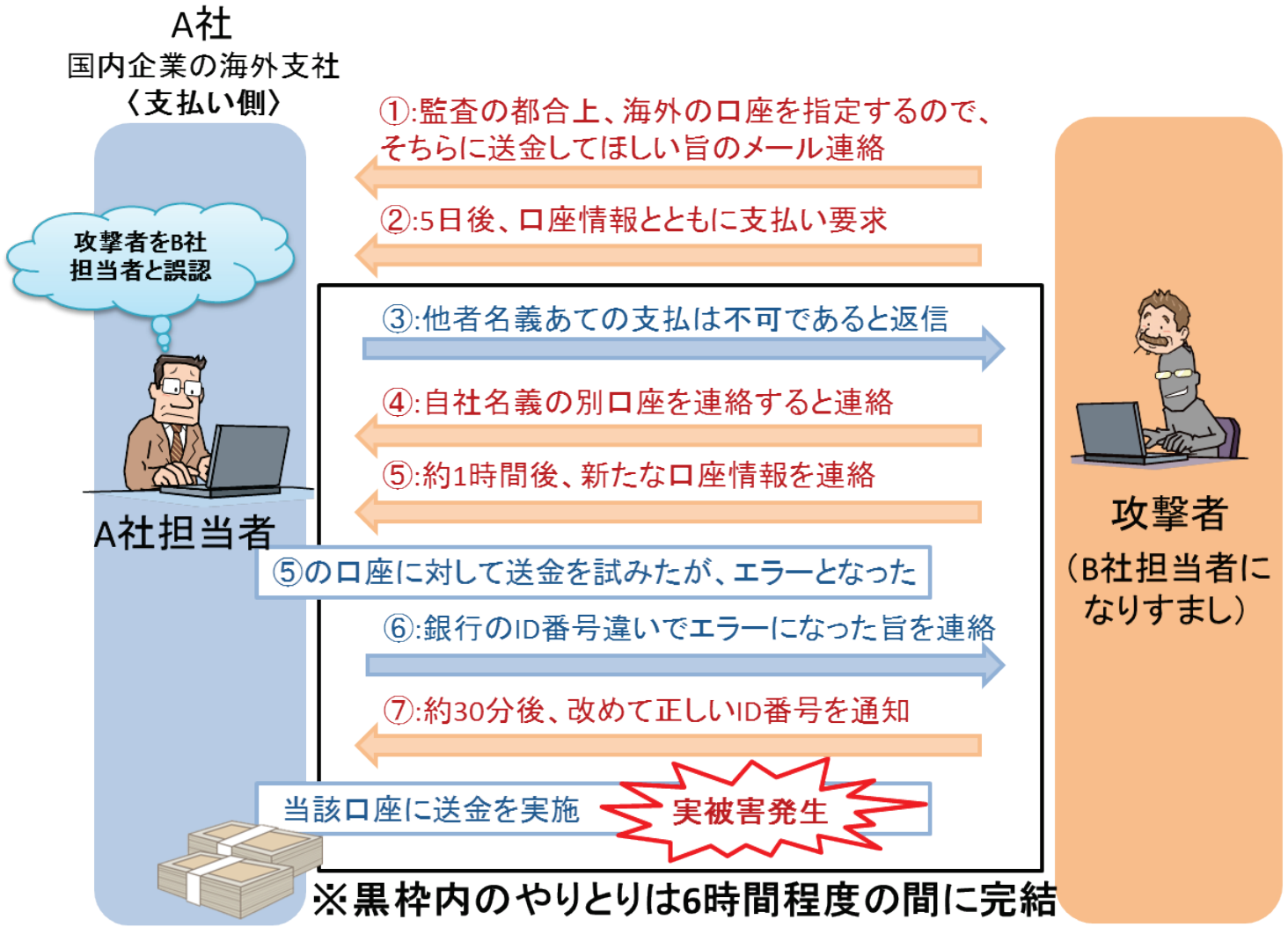
ビジネスメール詐欺の事例

ビジネスメール詐欺の事例の一つを紹介します。この事例では、ある**国内企業の海外支社（A社）が狙われました**。攻撃者は、事前に何らかの方法で取引に関わるメールを盗聴して、A社の取引先であるB社になりすまし、不正な送金依頼をしてきました。更に、B社に対しては、A社の担当者になりすましたメールも送っていました。



不正な送金依頼の流れ

前ページの事例の②の部分では、下図のような流れで偽の口座への振り込み（被害）に至るメールのやりとりがありました。この際、攻撃者はB社の本物のメールアドレスに近い**偽のメールアドレス**を使っていました。



攻撃者がなりすます偽のメールアドレス

ビジネスメール詐欺では、攻撃者が企業の担当者を欺くため、次のようなパターンで偽のメールアドレスを使ってきます。メールの送信者欄を注意深く確認し、不審なメールアドレスであると見抜くことが重要です。

■本物のメールアドレス		alice @ company-a . com
■偽物のメールアドレス	①	alice @ compnay-a . com
	②	alice @ companys-a . com
		aalice @ company-a . com
	③	alice @ comp ny-a . com
	④	alice @ cornpany-a . com
	⑤	alice-company-a @ freemail.com

① メールアドレスを1文字入れ替える
② メールアドレスに1文字追加する
③ メールアドレスを1文字削除する
④ メールアドレスの一部を誤認しやすい文字に置き換える（例：m（M） → rn（RN））
⑤ フリーメールサービスを使いそれらしいメールアドレスを作る

ビジネスメール詐欺への対策

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です。また、この手口は、根本的には「詐欺」なのですが、電子メールに依存した企業間のビジネス活動につけこみ、巧妙な罠を仕掛けてきます。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、ひとりひとりが手口を理解し、次のような対策を行ってください。

●送金前のチェックの強化

ビジネスメール詐欺を想定し、送金等の際のチェック体制を強化しましょう。
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しましょう。

●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しましょう。

●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。OSやアプリケーション・セキュリティソフトを最新に保ち、パスワードには複雑なものを設定しましょう。

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan