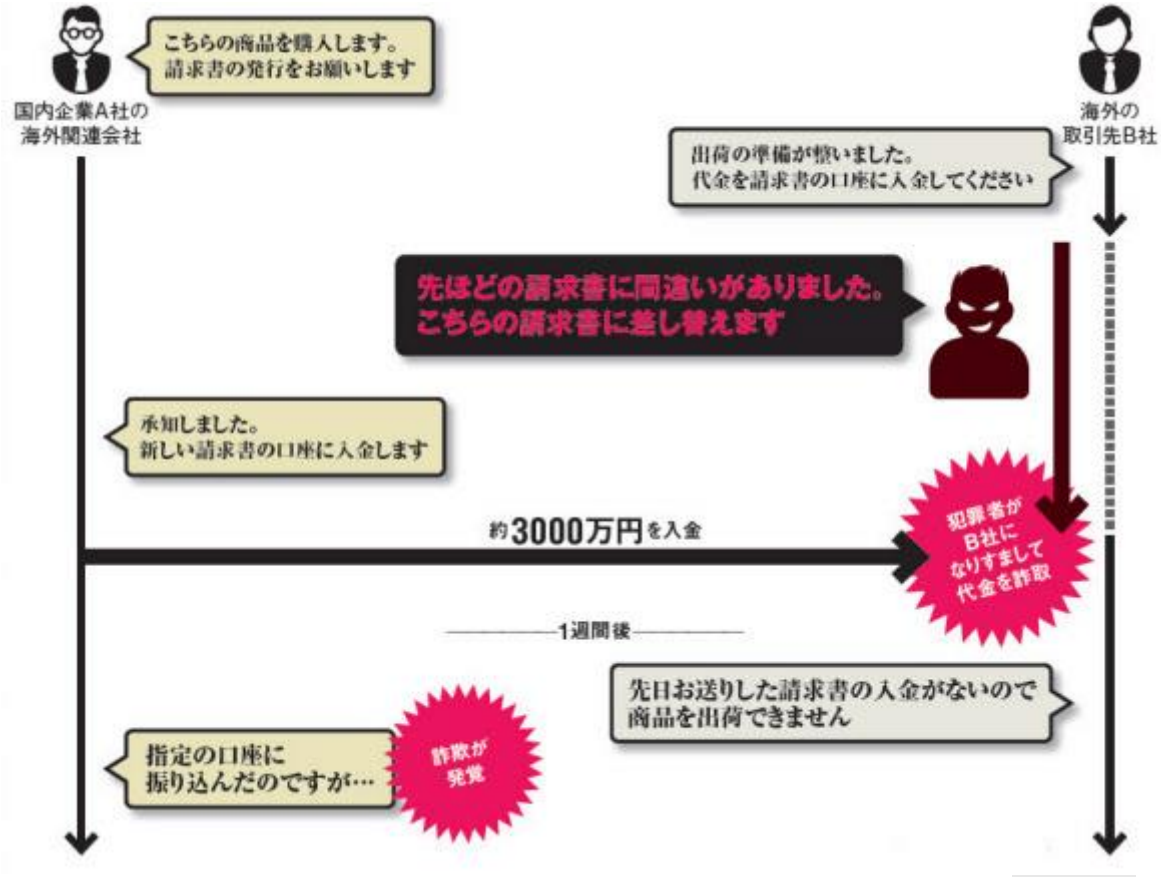
そのメールは詐欺だ！　手口が「進化」、対策は３つ

ネット・ＩＴ
コラム（テクノロジー）
科学＆新技術
2018/1/16 6:30［有料会員限定］
日経コンピュータ

　取引先や経営層を装い、メールで入金を促す「ビジネスメール詐欺」。金融機関やセキュリティー関連企業などによる注意喚起もむなしく、攻撃がやむ気配はなく、手口も「進化」してきている。自社が被害に遭うばかりか取引先からの送金を奪われるケースも。周知徹底と迅速な対応、そして原因追究への備えが明暗を分ける。

■入金したはずなのに

　「入金が確認できません」。ある国内企業（A 社とする）の海外関連会社に勤める社員は取引先（同 B 社）からの 1 通のメールに目を疑った。1 週間ほど前、請求書に書かれた口座に約 3000 万円を入金したはず。いったい何が起こったのか――。



画像の拡大

国内企業の海外関連会社が遭ったビジネスメール詐欺被害（出所：A 社への取材を基に構成）

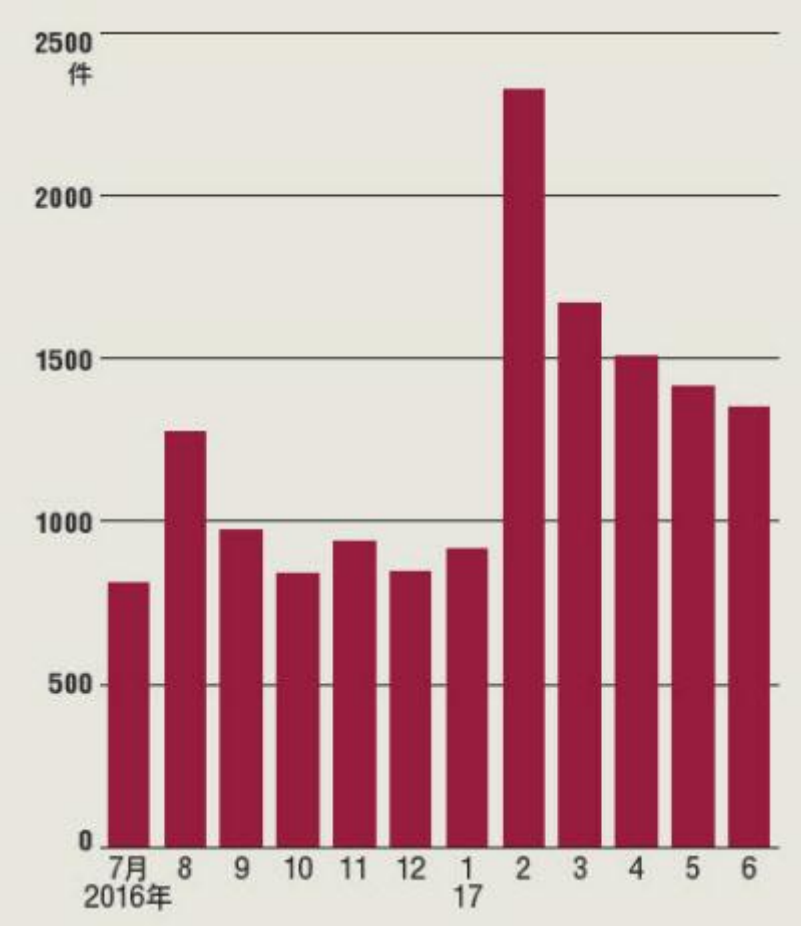
2017 年に実際に発生した「ビジネスメール詐欺（Business E-mail Compromise：BEC）」の事件だ。企業版の「振り込め詐欺」とでも言うべき詐欺犯罪で、業務上のメールのやり取りに巧妙に入り込んでくる。A 社の場合、B 社から届いた請求書の訂正メールが、実は B 社になりすました犯罪者によるものだった。

あまりに良いタイミングでメールのやり取りに入り込んできたため、なりすましを疑うこともなく犯罪者の口座に入金してしまった。後に B 社のメールアカウントが乗っ取られたことが分かったが、責任の所在は明確にできない。犯人は見つかっておらず、約 3000 万円は回収できないままだ。

■前触れのフィッシング攻撃が急増

脅威は世界を襲っている。米連邦捜査局（FBI）によれば、2016 年までの約 3 年間でビジネスメール詐欺の被害総額は世界で約 53 億ドル（約 6000 億円）に達したという。日本も例外ではなく 2014 年ごろからビジネスメール詐欺が見つかるようになった。

トレンドマイクロが国内企業を対象に調べたところ、「2016 年にビジネス詐欺メールを受信した」企業が 13.4%あった。その 7.4%が「ビジネスメール詐欺で金銭的な被害を受けた」という。



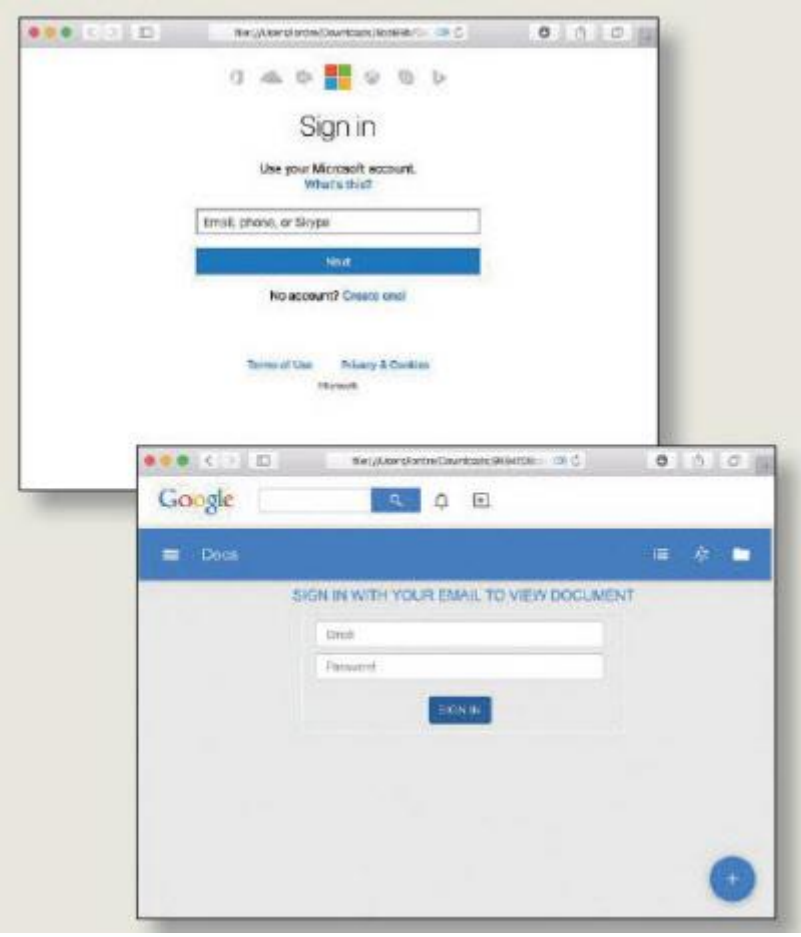
画像の拡大

世界のビジネスメール詐欺関連のフィッシング攻撃件数（出所：トレンドマイクロ）

脅威の高まりを受け 2016 年ごろから金融機関や一部の都道府県警などが注意を呼び掛けてきたが、「減るどころか増える傾向にある」（三菱東京 UFJ 銀行の松野善方顧客保護推進室長）。特に海外とのやり取りが多い企業では顕著

だ。伊藤忠商事の佐藤元彦上級サイバーセキュリティ分析官は「観測し始めた2014 年から毎年 2 倍のペースで詐欺メールが増えている印象だ。今のところ当社の被害は無いが注意喚起を強化している」と話す。

詐欺行為はさらに増えそうだ。「ビジネスメール詐欺に使うため、メールのログイン情報を奪い取ろうとするフィッシング（詐欺）攻撃の件数が 2017 年に入って急増している」（トレンドマイクロの染谷征良上級セキュリティエバンジェリスト）からだ。犯罪者はメールのみで詐欺を仕掛ける。フィッシング攻撃の増加はビジネスメール詐欺の増加の前触れだ。



画像の拡大

メールのパスワードを入力させる不正サイトの例（画像提供：トレンドマイクロ）

2017年4月に注意喚起のレポートを公開した情報処理推進機構(IPA)には、その後も複数の相談が寄せられている。例えば6月2日。サイバー攻撃情報の共有活動に参加する企業から、ビジネスメール詐欺を試みる英文メールを受信したとの情報提供を受けた。

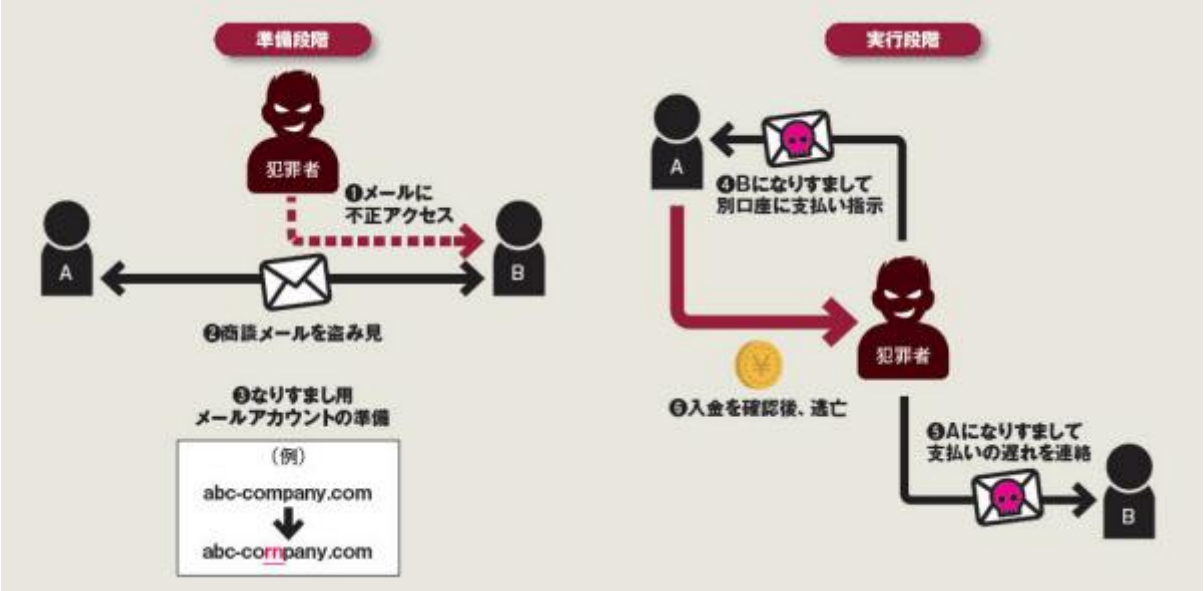
その会社の最高経営責任者（CEO）になりすまし、最高財務責任者（CFO）に振り込みを指示するメールを送ってきたという。冒頭の被害のような「やり取り型」ではなく、経営層になりすまして振り込ませる「CxO型」と呼ばれるタイプだ。同月6日には返信先のメールアドレスが一致する同じ手口の詐欺メールが別の会社にも届いた。

「欧州の取引先から受け取るはずの500万円をビジネスメール詐欺で奪われたという相談もあった」とIPAの松坂志技術本部セキュリティセンター調査役は明かす。冒頭の被害とは逆のパターンだ。自社が犯罪者に送金してしまうリスクのほかに、犯罪者が自社になりすますリスクもあるのだ。

■1カ月以上にわたり盗み見

日本企業が被害に遭いやすいのは、犯罪者が海外の取引先になりすます手口だ。振込口座の変更やフリーメールの日常利用といった商習慣の違い、英語でのやり取り、会計システムの違い、振り込みに関するガバナンスの違いなどが、「まさか」の事態を誘発する。

犯罪者は担当者同士がメールで商談を進めている間、不正アクセスしたメールシステムでやり取りを盗み見る。ビジネスメール詐欺を分析するある国内企業のIT担当者は「1カ月以上は観察することが多い」と指摘する。観察と並行して攻撃対象のメールアドレスと見た目が似ている詐欺用のメールアドレスを用意する。



画像の拡大

ビジネスメール詐欺の典型的な手口

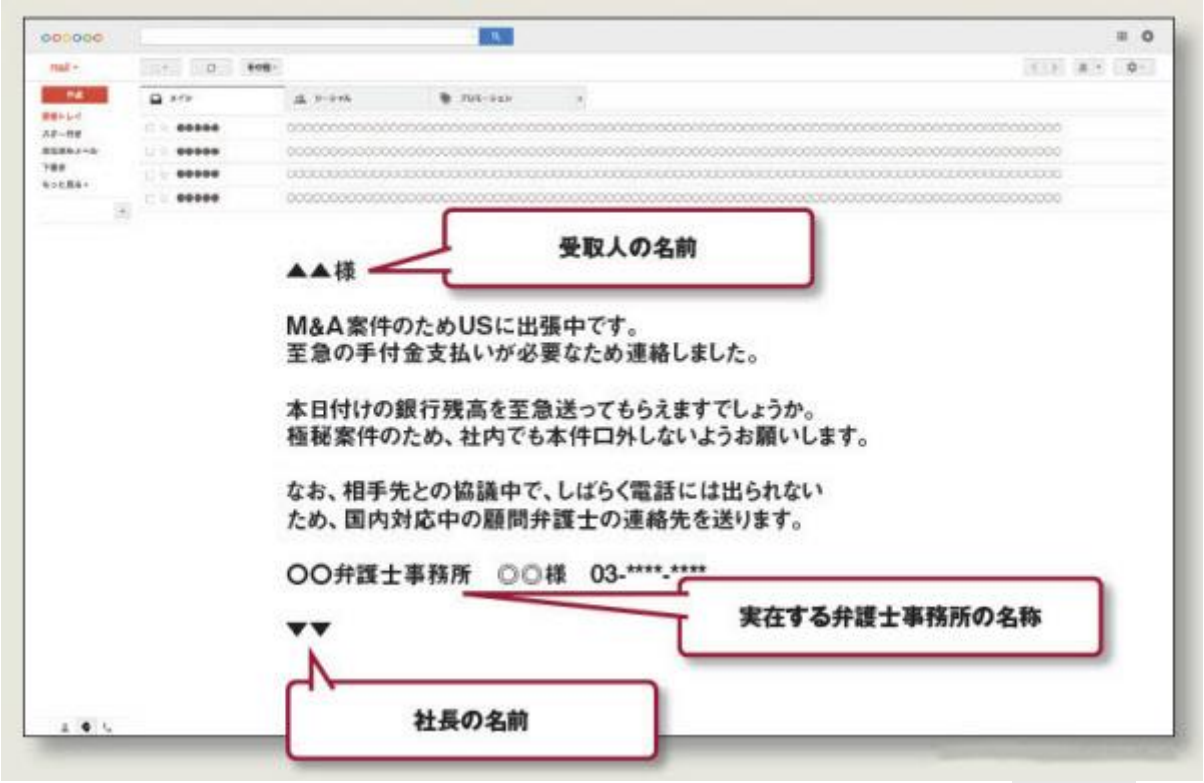
商談の大詰め、請求段階に入ったところで犯罪者は詐欺用のメールアドレスを使い、取引先になりすましたメールを送る。「監査中なので通常とは違う口座になる」「トラブルのためメイン銀行で入金を受けられない」といったもっともらしい理由をつけて犯罪者の口座を指定してくる。

請求書の PDF を偽装するのでサインももちろん本物と一緒で、口座情報のみを精巧に書き換えるケースがあるという。「アドレスや請求書の偽装は後からよく見れば分かるもの。だが、商談の流れに絶妙なタイミングで入り込んでくるので、気付けというほうが難しい」（冒頭の企業の IT 担当者）。

CxO 型の手口では、「極秘の M&A（合併・買収）案件だから社内でも口外するな」「これから詰めの会議なのでしばらく電話に出られない」といった理由をつけて振り込みを指示してくる。機密性が高い案件だと思わせて口止めし、発覚を免れようとするのだ。

英語圏が中心だったビジネスメール詐欺だが、トレンドマイクロの染谷氏は「米国で流行したサイバー犯罪が日本で流行するまでの期間がどんどん短くな

っている」と指摘する。ある国内企業には 2017 年になって日本語の CxO 型メールが届いた。



画像の拡大

ある企業に届いた日本語の詐欺メールの文面（出所：実例を基に日経コンピュータが作成）

受信した企業の IT 担当者は「過去にはなかったケース。自然な日本語の文章になっていて驚いた。日本人の関与も感じさせる」と話す。国内取引のみの企業にもビジネスメール詐欺は対岸の火事ではなくなっているのだ。

■まず周知、即時対応も不可欠

ビジネスメール詐欺は IT（情報技術）による対策だけでは不十分。システム部門は対策として 3 つの策を社内に広めたい。

まずはリスク管理部門などに働きかけ、海外拠点を含め、社員全員に詐欺の存在を周知する。存在を知れば、不自然さを読み取る感度は高くなる。

画像の拡大

3つの対策

三菱東京UFJ銀行は9月にビジネスメール詐欺への注意を喚起する文書を全店に配布し、取引先に配るように指示を出した。「不自然な口座変更があったら従来から知っている電話など、必ずメール以外の手段で確認する作業を浸透させて、詐欺を未然に防いでほしい」と同行の松野室長は呼びかける。

2つ目は攻撃を受けたと気付いたら即座に動くことだ。仮に送金を指示した後でも即座に銀行にかけ合えば、送金を止められるケースがある。特に海外送金は指示から送金に時間がかかる。

即座の対応で参考になるのが伊藤忠商事だ。詐欺のメールを受信したと相談を受けたら、それ以上の盗み見をストップさせるため、すぐに受信者や取引に関わる社員のメールアカウントのパスワードをリセットする。さらに転送ルールなどが勝手に設定されていないかを確認させる。

乗っ取られるのは、ほとんどがウェブブラウザーでアクセスできるタイプのメールシステムという。乗っ取り防止には2段階認証の導入や普段と異なる端末からのログイン時に警告を発する機能の利用なども有効だ。

最後の対策は原因追究の体制を整えておくこと。ビジネスメール詐欺は自社と取引先のどちらかのメールへの不正アクセスが発端となる。自社をかたるメールで取引先が詐欺に遭うケースもある。自社のメールに不正アクセスがなかったかどうかの分析・証明が自社を守ることにつながる。

自社でメールサーバーを持って入ればアクセス履歴を入手・分析できるが、厄介なのがクラウドベースのメールサービスだ。ほとんどの事業者がアクセス履歴の提供を明言していない。どんな履歴データをどれだけ取得できるかを事業者から確認して、いざというときに備えるべきだろう。

（日経コンピュータ　竹居智久