JPCERT CC®

ビジネスメール詐欺の実態調査報告書

一般社団法人 **JPCERT** コーディネーションセンター

2020 年 **3** 月 **25** 日

JPCERT CC®

目次

1. はじめに

1.1. 本報告書の要旨

本報告書は、ビジネスメール詐欺（Business E-mail Compromise：BEC、以下、BEC）の被害の実態を明らかにするために、一般社団法人 JPCERT コーディネーションセンター （以下、JPCERT/CC）が実施した実態調査の結果をまとめ、組織が取るべき対策をまとめたものである。

1.2. 本報告書が想定している読者

本報告書は次のような方々を読者として想定している。

- 情報システム部門（IT 部門）
- 情報セキュリティ部門（CSIRT）
- 経営層（主にシステム・経理・リスク・法務部門担当）など

1.3. 本報告書の目的

BEC は、2015 年に米国連邦捜査局（Federal Bureau of Investigation：FBI） が情報を公開して以降、広く知られるようになったが、被害は未だ増えている状況である。米国連邦捜査局（FBI）の米国インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）に報告された被害件数などのデータによると、2013 年 10 月から 2016 年 5 月までの期間において、BEC の被害件数は米国内外で 22,143 件、被害額は約 31 億（$3,086,250,090）米ドルだった 一方、2016 年 6 月から 2019 年 7 月までの期間では、被害件数は 166,349 件、被害額は約 262 億（$26,201,775,589）米ドルと大きく増加している。

日本においても、2017 年以降、独立行政法人 情報処理推進機構（以下、IPA）や警察庁、トレンドマイクロ社などが BEC に関する情報を公開し注意を呼びかけている。また、同年末頃には日本国内の組織での詐欺の被害が大きく報じられ、2018 年には日本語のメールによる BEC が確認されるなど、日本国内における脅威への警戒の重要性も高まっている。

こうした状況を踏まえ、JPCERT/CC では BEC の被害を最小化するためには、脅威の実態を明らかにし、その結果を踏まえた対策や対応を広く国内組織に発信する必要があると考え、BEC に関するアンケートやヒアリングを実施した。
さらに、調査結果や公開情報などをもとに脅威の動向や変遷を踏まえ、BEC に対して組織がとるべき行動などを本報告書にまとめた。

2. ビジネスメール詐欺とは

BEC については、様々な組織が情報を発信している。組織によって定義は異なるものの、「取引先などになりすました電子メールを送って送金を促す詐欺行為」という点は共通している。

2015 年初め頃から、米国インターネット犯罪苦情センター（IC3）が BEC に関する警告を公開し始め、同年 1 月には BEC を、「定期的に海外のサプライヤーや取引先と電信送金を行う組織を標的とした、高度な詐欺行為」として説明している [1]。同じくメールを使った詐欺行為として、恋人の振りをするなどして金銭を要求する「ロマンス詐欺」や、宝くじの抽選番号を事前に通知するなどとして金銭を要求する「宝くじ詐欺」などが挙げられる。また、BEC で法人を狙う詐欺集団が、主に個人を標的としてロマンス詐欺や宝くじ詐欺などを行うことも明らかになっている [2]。いずれもメールを用いて行われる詐欺行為として、BEC やロマンス詐欺などは同じ詐欺の種類として取り上げられる場合があるが、その標的や手法などが異なることから、本報告書では BEC に限定して解説を進めていく。実際、FBI IC3 の統計においては BEC とロマンス詐欺は別々に被害件数や被害額の統計が算出されている。[3]

本報告書では、取引先などになりすまし電子メールを送って送金を促す詐欺行為を BEC として論じる。（いわゆるフィッシングは除く）

---

1 Business E-mail Compromise
https://www.ic3.gov/media/2015/150122.aspx

2 281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes
https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds

3 2018 Internet Crime Report
https://pdf.ic3.gov/2018_IC3Report.pdf

3. ビジネスメール詐欺の実態調査

3.1. 調査の概要

本調査は、未遂を含めた BEC の個々の事案の詳細について回答を求めたアンケートを JPCERT/CC が作成し、日本貿易会 ISAC、石油化学工業協会などに協力を求め、調査の趣旨に賛同した 12 組織から得た 117 件の回答をまとめた。さらに、アンケートに応じた組織の中から 6 組織については訪問した上で BEC 事案の詳細や、BEC に対する対策状況についてヒアリングを実施した。

実施期間	2019 年 7 月 8 日（月）～ 2019 年 11 月 22 日（金）
実施対象	日本貿易会 ISAC　（賛同組織） 石油化学工業協会（賛同組織）他
方法	アンケート および 対面によるヒアリング
調査名	Business E-mail Compromise（BEC）実態調査
調査概要	各組織における BEC 発生状況や取組み状況　など
回答組織数	アンケート：12 社、ヒアリング：6 社

3.2. 調査結果

3.2.1. 関係国・使用言語

［表 1］は、関係国（発生した BEC における関係組織の所在地）と使用言語をまとめたものである。
関係国は調査対象組織のビジネスモデルに依存するところでもあるが、アジア圏の拠点または取引先との間で発生している事案が多かった。
使用言語は英語が圧倒的に多く、日本語を使用した事案もあった。

［表 1: 関係国・使用する言語の状況］

関係国	件数
日本	41 件
中国	19 件
アメリカ	18 件
インド	11 件
シンガポール	10 件
韓国	7 件
タイ	6 件

使用言語	件数
英語	108 件
日本語	8 件
中国語	2 件
インドネシア語	1 件
フランス語	1 件
ポルトガル語	1 件

※複数の所在地、言語が含まれる事案は重複カウント
＜その他関係国＞
インドネシア、イギリス、ドイツ、ブラジル、ベトナム、マレーシア、オーストラリア、スリランカ、ベルギー、モーリシャス、トルコ、フィリピン、台湾、UAE、ウズベキスタン、エジプト、カタール、スウェーデン、スペイン、チュニジア、ドバイ、ハイチ、パキスタン、パナマ、ベラルーシ、ミャンマー、メキシコ、ラオス、ロシア

3.2.2. 分類

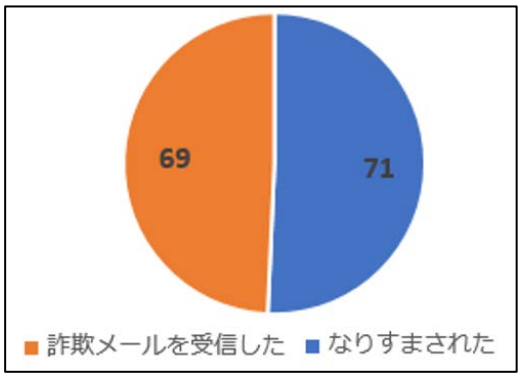
BEC 事案の分類にも様々なやり方があるが、今回は IPA が定義する「ビジネスメール詐欺の 5 つのタイプ」[4]に従って分類する。

［表 2: IPA「ビジネスメール詐欺の 5 つのタイプ」と収集した事案における各タイプの確認］

IPA「ビジネスメール詐欺の 5 つのタイプ」	分類結果
【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	確認
【タイプ 2】経営者等へのなりすまし 例）経営者を騙り、偽の振り込み先に振り込ませる	確認
【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	確認
【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	未確認
【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、従業員の情報を詐取する	確認

IPA が分類する 5 つのタイプのうち、【タイプ 4】「社外の権威ある第三者へのなりすまし」を除く 4 つのタイプに該当する事案が確認された。中でも、【タイプ 1】「取引先との請求書の偽装」に該当する事案が最も多く、全体の約 75 %を占めた。次いで、【タイプ 2】「経営者等へのなりすまし」が多く、役職別では CEO や CFO のなりすましが見られた。また、役員のメールアカウントが窃取され、偽の振り込み先に振り込みを誘導されるなど複数のタイプの要素をあわせ持った事案もあった。

次に“なりすまされた組織”の存在について述べる。これまでに公開されている BEC に関するレポートや報告書、または記事においては金銭を窃取された組織 （もしくは窃取されかけた組織） が注目されることが多い。しかしながら、詐欺メールを受信した組織が存在する一方で“なりすまされた組織”が存在することも留意したい。［図 1］に示すとおり、収集した事案においてもその傾向は顕著に出ており、“詐欺メールを受信した”事案と“なりすまされた”事案は、ほぼ同数であった BEC に対する立場の違いを認識することは、対策や対応を検討するうえで、ポイントになる。



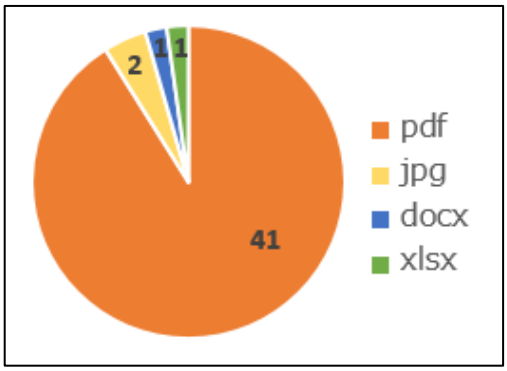
［図 1:BEC に対する立場の違い］

[4] ビジネスメール詐欺「BEC」に関する事例と注意喚起（続報）
https://www.ipa.go.jp/files/000068781.pdf

3.2.3. 手法

3.2.3.1. 請求書の偽造

「ビジネスメール詐欺の 5 つのタイプ」のうち、最も多かったタイプが【タイプ 1】「取引先との請求書の偽装」である。実際の取引で用いられる請求書が改ざんされ、BEC に用いられた事案もしばしば見られた。調査では、事案ごとに添付ファイルの有無と、添付ファイルが用いられていた場合にはファイル形式や作成日時を質問した。結果、添付ファイルのファイル形式は PDF が 9 割を占めており、作成には無料の変換ソフトや変換サイトが多く使用されていた。また、プロパティに記録されている作成日時については関係国と異なるタイムゾーンが設定されていることもあり、BEC を見極める判断材料の一つとして考えられる。



［図 2:添付ファイル種類］

［表 3:添付ファイルの PDF 変換に用いられていたソフトまたはサイト例］

PDF 変換ソフト
3-Heights™Document Converter
Adobe Acrobat
Excel for Office 365
GPL Ghostscript
Microsoft Word
Quartz PDF Context
PDFill FREE PDF Tools
PDFlib
RAD PDF 管理ツール
SAMBox
Skia/PDF

PDF 変換サイト
Convert-JPG-to-PDF.net
Zamzar
Online PDF-Converter
pdf-tools.com
Sejda SDK
Zamzar

改ざんされた請求書は、請求内容に不自然な点があったり、テキストボックスを切り貼りした安易な作りだったりと、注意深く確認すると BEC の被害を未然に防ぐことができる場合があった。

また、偽装請求書に差替えるなど、振込先口座を変更する際には理由が添えられていることが多い。右表は調査で確認した口座変更が必要な理由である。いずれも、一見すると正当な理由に受取られがちであるが、実際に BEC の事案に用いられた理由であることを認識しておく必要がある。なお、今回は“年次監査”を理由として通常口座が利用できない旨の連絡をしてくる事案が多かった。

［表 4: 口座変更に用いられた理由］

＜口座変更理由＞
- ✓ 年次監査を受けており口座が利用できない
- ✓ 税金の問題によりメイン口座が審査中
- ✓ 小切手発行のためメイン口座の財務記録中
- ✓ 制度改正による為替レート変更
- ✓ 銀行の吸収合併によるもの　など

3.2.3.2. 詐称のタイミング

攻撃者は、請求書発行時から払込が行われる前に偽装された請求書を送付するなど、口座変更を指示する傾向が強い。また、BEC は新規取引の契約を締結する過程でも発生しており、この場合、既存口座との比較などによる気づきの機会がないので既存取引に比べて見極めることが困難との意見もあった。

［表 5:詐称のタイミング］

詐称タイミング	
請求書発行前	13 件
請求書発行前のプロセスにおける詐称	
請求書発行時	33 件
請求書発行プロセスにおける詐称	
振込前	29 件
請求書発行から振込までのプロセスにおける詐称	
振込後	3 件
振込後の詐称	
その他	28 件
支払プロセスに関わらず発生した詐称	

3.2.3.3. なりすまし

「ビジネスメール詐欺の 5 つのタイプ」のうち、次いで多かったのは【タイプ 2】「経営者等へのなりすまし」である。「3.2.2.**分類**」に記述のとおり、役職別では CEO や CFO へのなりすましを確認しているが、新たな手口として、攻撃者が経営者と秘書の 2 名になりすました事案があった。この事案では、秘書と名乗る者から翌日に CEO から取引指示があること、自分（秘書）は翌日不在となる旨をあらかじめ伝えておき、翌日に CEO になりすました者から送金指示があった。BEC に関する関心や警戒が高まる中、相手先を信用させるために複数の登場人物になりすましたものと思われる。
なりすましという観点からは、【タイプ 2】「経営者等へのなりすまし」に限らず、【タイプ 1】「取引先との請求書の偽装」でも自組織の役職員になります事案も多かった。なりすましの手法は、類似ドメインの使用が散見され、異なる TLD（top-level domain） を使用したり、文字列を改変したりするなど従来と同様の手口が用いられている。

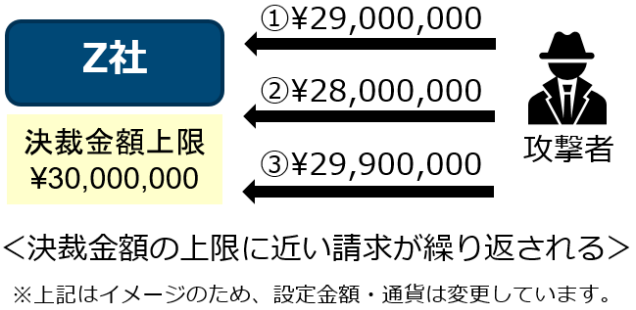
3.2.3.4. アカウント乗っ取り

アンケートでは、BEC の送信元メールサービスについても確認した。攻撃者がフリーのメールサービスでアカウントを作成し、攻撃に用いる場合もあるが、「ビジネスメール詐欺の 5 つのタイプ」の【タイプ 3】「窃取メールアカウントの悪用」に定義されているとおり、メールアカウントが乗っ取られ、悪用された事案も複数あった。今回は調査対象組織が管理するメールサービスのアカウント侵害はなかったものの、フリーのメールサービスや、海外拠点が独自に導入したクラウド型のメールサービスでアカウント侵害があった。ヒアリングの結果、アカウント侵害に繋がった原因としてフィッシングやマルウエアによる認証情報の窃取や、ブルートフォースアタック（総当たり攻撃）が挙げられた。

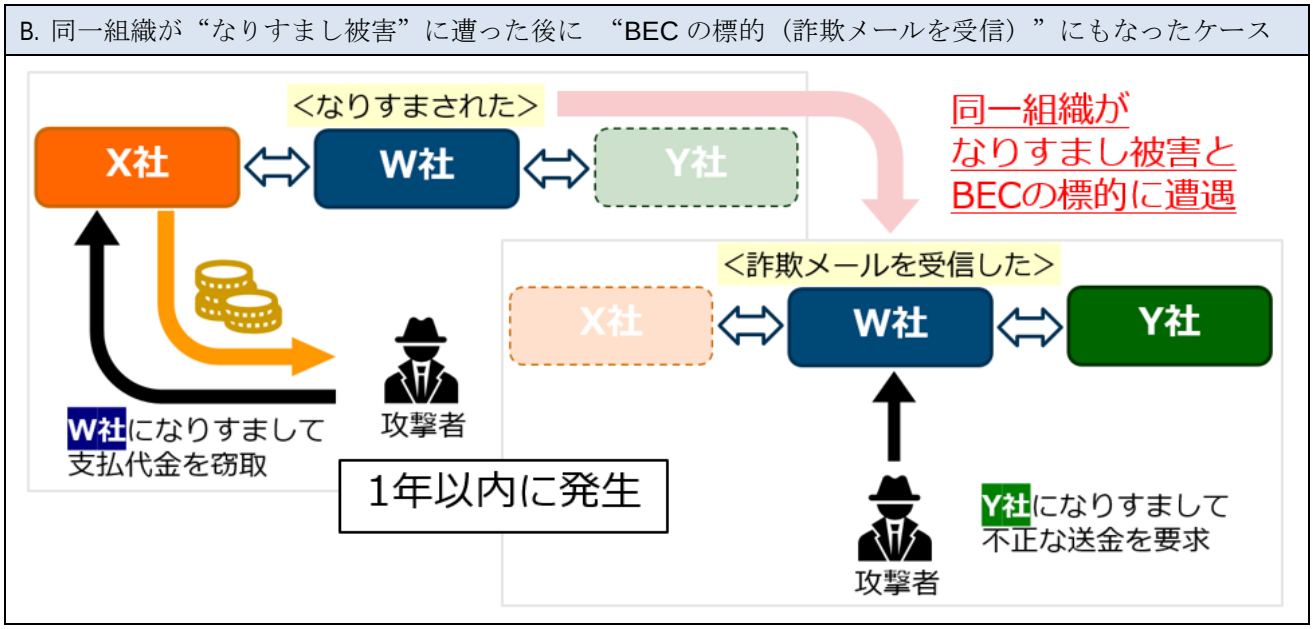
3.2.3.5. 内部精通者関与の可能性

収集した事案の中には、関係者しか知り得ない情報を使い BEC が試みられたケースもあった。一例として、「A. 決裁金額の上限に限りなく近い請求が繰り返し行われたケース」や、下図のとおり「B. 同一組織が“なりすまし被害”に遭った後に“BEC の標的（詐欺メールを受信）”にもなったケース」を確認している。BEC の準備行為として情報収集が行われる場合があるものの、本来、外部の者が知り得ない決裁金額の上限や複数の取引内容の情報を用いて BEC が行われている実態を踏まえると、内部に精通した関係者が関与している可能性も否定できない。

A. 決裁上限額に限りなく近い請求が繰り返されたケース



B. 同一組織が“なりすまし被害”に遭った後に “BEC の標的（詐欺メールを受信）”にもなったケース



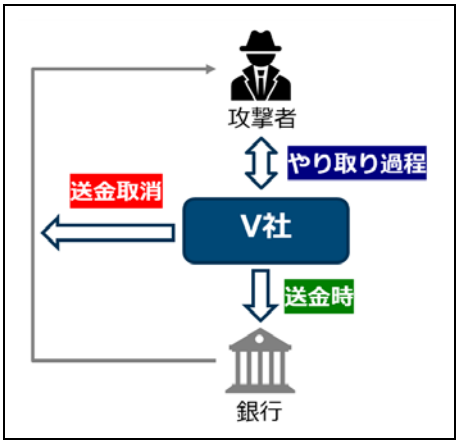
［図 3: 内部精通者が関与している可能性のある事例］

3.3. 被害状況

請求は基本的に外貨建ての送金を指示するものであったが、大半の事案では BEC と気づいて実害には至らなかった。
BEC と気づいた経緯と実害を免れた理由は次のとおりである。

①メールのやり取りの中で BEC と気づいた
②送金先の口座が凍結されていたなどの理由で送金できなかった
③取引先から督促を受けて気づき、送金を取り消すことができた

特に①メールのやり取りの中で気づく場合が最も多く、不審な点を感じた時点でメール以外の連絡手段（電話・メッセージアプリなど）を用いて相手先に確認をとり、被害を回避している。



［図 4:回避したタイミング］

調査結果から気づきの例を右表のとおり示す。不自然なローカル言語とは現地スタッフが確認して不自然と感じるレベルであり、駐在員などが気づくことは困難と思われる。

［表 6: やり取りの過程における気づきの例］

＜気づきの例＞
✓ 支払済の請求・請求書の体裁が不自然
✓ 見慣れない地域への送金
✓ 送金先口座の凍結
✓ 不自然なローカル言語　など

被害を回避した事案がある一方、日本円に換算すると数百万～数千万単位の被害に遭った事案もあった。被害金額に幅があるのは、取引内容に応じて請求金額が異なるためであり、攻撃者は取引内容を十分に把握した上で BEC を仕掛けていることがわかる。
被害に遭った場合も一部の事案では、送金先口座の凍結により口座残高に応じた配分を受けられたり、犯罪保険による求償により被害額を取り戻すことができたりするなどの事案があった。ただし、これらには課題もある。一つ目の課題は、煩雑な手続きである。BEC の被害を証明するにあたっては銀行や保険会社などに多くの書類を提出することに加え、海外の金融機関が関わる場合は現地のローカル言語で対応するなど、非常に負荷が高い。二つ目は戻入のタイミングである。仮に被害金額が戻ってきたとしても決算を跨ぐと経理処理上は益金となることから、被害額の回収に踏み出せないケースも存在するようである。なお、被害有無に関わらず今回把握した BEC による不正な請求額の合計（日本円換算）は約 24 億円だった。

3.4. 調査結果からの教訓

調査を通じて、次の教訓を得た。

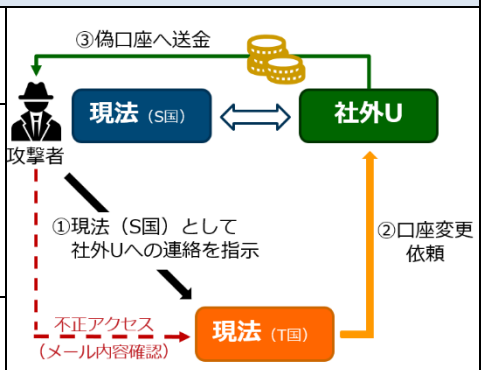
- BEC は、攻撃者と被害組織が 1 対 1 で対峙するだけでなく、複数の組織や人物が関わる事案もある
- BEC の事案の中には、先行する他のインシデントが関連して発生したものがある
- BEC への対策は、騙されないことばかりではなく、なりすまされないための対策も必要である

3.4.1. 構造の複雑化

これまでに公開されている BEC に関するレポートや報告書、または記事においては、A 社⇔B 社間や A 社役員⇔A 社従業員などのように 1 対 1 の関係の中で発生している事案について述べられていることが多い。
調査結果の多くが 1 対 1 のやり取りによるものであったが、1 対 n や、n 対 n など複数の関係者や組織が関与した事案もあった。その一例を示す。

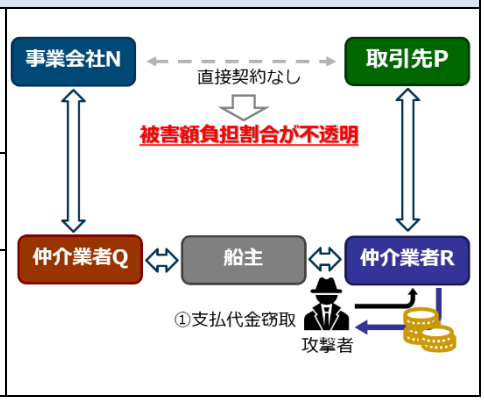
C. グループ他組織を巻き込んだケース

概要	■現地法人（S 国）と社外 U の取引プロセスで発生 ■社外 U から現地法人（S 国）への支払代金を窃取
手口	■攻撃者は現地法人（S 国）になりすまして 現地法人(T 国) に社外 U への口座変更依頼を指示 ■現地法人（T 国）は社外 U に口座変更を依頼 ■社外 U は偽口座へ支払代金を送金
ポイント	■現地法人（T 国）と社外 U は正規のやり取り ■グループ他組織を利用して信用を獲得



D. 仲介業者（ブローカー）を介したケース

概要	■事業会社 N と取引先 P の取引プロセスで発生 ■支払代金は仲介業者を介してやり取り ■仲介業者 R から船主への支払代金を窃取
手口	■攻撃者は船主になりすまして支払口座を偽装 ■仲介業者 R は偽口座へ支払代金を送金
ポイント	■事業会社 N と取引先 P には直接的な契約なし ■直接契約が存在せず、複数組織が関与している ことから被害額の負担割合が争点



［図 5: 複数の関係者や組織が関与した事例］

これらの事案は取引過程において第三者が介在したり、結果として直接的な契約関係のない組織間で BEC が発生したりすることにより複数の関係者や組織が関与したケースである。
こうした構造関係にあった場合、原因の特定が困難になるとともに、損害に対する負担割合など法的解決に労力を割くことになりかねない。いずれにおいても、BEC を考える上では加害者と被害者という単純な構造ではなく、複数の登場人物や組織が関与する可能性があることを念頭に行動する必要がある。

3.4.2. 関連インシデントの存在

原則として、組織間の取引内容を担当者など関係者以外が入手することは困難である。しかしながら、数万円から数億円と幅広い請求金額が設定されていたことや、正規の請求書を受信した直後に改ざんされた請求書が届くなど、攻撃者が取引内容を事前に把握しているのではないかと推測される事案が多く確認された。
ある組織においては、社内調査の結果から BEC が発覚する直前に利用者がフィッシングサイトにアクセスし、メールサービスの認証情報を入力したことを確認しており、取引内容が外部に漏えいしたきっかけととらえていた。他の組織においては後の社内調査においてマルウエアへの感染を確認したとのことであった。
いずれの場合にも共通することは、BEC が発覚する前に行われた行為であるということである。我々はインシデントに直面した際、目の前で起こっている事象そのものに注目してしまい、何故、攻撃者が取引内容を入手しているのか、どのようにしてメールシステムのアカウントを取得したのかといったことに対して疎い。しかしながら、先行して発生したセキュリティインシデントで得た情報が BEC に悪用されている可能性があることを認識する必要がある。
万が一、自組織や関係先でアカウント侵害や情報漏えいなどのインシデントが発生した際には、漏えいした情報が BEC に悪用される可能性も踏まえて組織内の注意喚起など、BEC に対する警戒を高めることを推奨する。

3.4.3. 異なる立場

もう一つ抑えておきたいポイントは、被害者になることもあれば加害者に加担していることもあるということである。サイバーセキュリティにおいても、自組織のインフラがサイバー攻撃の踏み台として悪用されるケースがあるように、BEC においても、同様にどの組織でも起こり得る可能性がある。同時に、自組織の防御を優先するあまり対策が後手になるなど、盲点になりやすい問題でもある。
「3.2.2 分類」に記述のとおり、今回の調査では“詐欺メールを受信した組織”だけではなく “なりすまされた組織”も存在し、その数はほぼ同数であった。“なりすまされる”場合については、BEC が商取引に関連した詐欺であるという特徴を踏まえると、民事という観点から金銭被害を被った組織（以下、ダマされた組織） から損害の補填を求める訴訟を起こされる可能性がある。BEC の対策を考える上では実際に金銭を支払ってしまい損害が生じてしまうことだけではなく、被害組織から賠償を求められることを想定して“なりすまされない”ための対策や、賠償を求められた場合に対抗できる措置などの準備も必要となる。

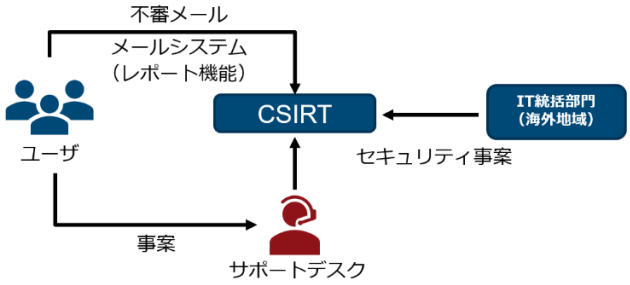
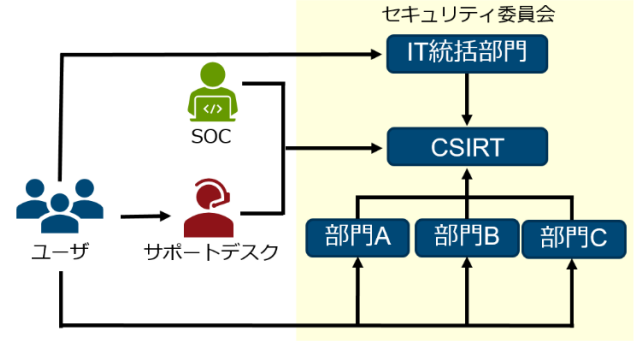
3.5. 対策

ここまでは、調査を通じて明らかとなった具体的な手法や特徴、被害状況をまとめた。ヒアリングでは BEC に対する取組み状況についても確認しており、大きく分けて実務面からのアプローチと技術面からのアプローチがあることがわかった。本節ではこれらの観点から組織が実施している対策状況をまとめる。

3.5.1. 実務面

3.5.1.1. 体制

BEC の被害を未然に防止するためには事象に気づく必要がある。報告先や相談窓口は BEC が E メールに起因することからサポートデスクなど IT 障害を取り扱う部署が担う場合や、明確な報告先や相談窓口が定まっておらず、営業統括部門や経理部門など利用者の判断に委ねられている場合が多いと思われる。これらの場合、BEC が他の案件などに埋もれてしまう懸念があり、BEC に気づかない恐れがある。
効率的に BEC に対応している組織の特徴として、IT 障害とメールに関する報告・相談先を分けるなど、総務・法務・経理・営業といった関係部門と、BEC に関する情報を共有する機会を設けるなど、自組織の BEC に関する情報が BEC の対応をする部門に集まりやすい体制を整えている組織が多い。

【例 1】報告・相談経路を分ける体制	【例 2】BEC を漏れなく把握する体制
	

［図 6: BEC に対して効率的に対応している組織の体制　（例）］

3.5.1.2. 訓練・研修

多くの組織において、これまでに公開されている BEC のレポートや報告書に記載のある研修や訓練を実施していることがわかった。
いずれの組織も訓練は、標的型攻撃などサイバー攻撃を念頭に置いた不審メール訓練に含めて実施している。
研修については、E ラーニングによる全社的な教育コンテンツの提供に加え、自組織で受領した BEC から得た気づきなどを注意喚起として定期的に利用者に通知している組織や、支払決裁権限を持つ管理職を対象に法務・財務・IT 部門が共同して集合型研修を開催し、IT に関する知識のみならず諸外国の法令や支払フロー、気づきのポイントなど多角的な観点から情報を提供している組織もあった。

これらの取組みに対する効果については、組織ごとに異なる回答を得た。集合型研修を実施している組織については一定の効果があったため同研修を動画コンテンツとして全社に展開を予定しているとのことであった。一方、訓練・研修を実施する必要性は理解しつつも、利用者に依存する取組みだけでは対策として不十分であり、事案に関する社内の情報を早くキャッチアップできる体制作りに注力しているという組織もあった。

3.5.1.3. 支払プロセスの見直し

支払プロセスの見直しは、一般的な対策として様々な公的機関やセキュリティベンダからも紹介されており、実際に見直したという組織もあった。具体的には営業部門のチェックに加え、経理部門のチェックも行うこととし、支払プロセスの強化を図っていた。

3.5.2. 技術面

3.5.2.1. 検知機能

実務面からのアプローチにおいても触れたが、BEC を防止する為にはまず、検知する必要がある。検知するためには受信者への気づきや簡易な報告スキームの構築がポイントとなる。ある組織では、過去 3 ヶ月受信していないドメインからのメールを受信した場合、受信者へ注意を促すポップアップを表示する機能を提供している。
他の組織では、不審メールを報告するためのボタンをメールシステムの受信ボックスに設け、不審メールの報告に係る手間を省力化する取組みを行っている。

3.5.2.2. 類似ドメインモニタリング

BEC では、実在するドメインに類似したドメイン（類似ドメイン）を送信元アドレスに用いられる用いることが多い。類似ドメインは BEC に限った問題はないが、対策として、有償のサービスを用いて類似ドメインの登録状況をモニタリングし、類似ドメインが確認された場合には、社内への注意喚起やメールシステムの遮断の対応を実施している組織があった。この組織によれば、正規ドメインを作成してから平均して 2 日程度で類似ドメインが作成される傾向であるとともに、日々生成される類似ドメインの数量から対策に切りがない状況とのことであった。「3.2.3.3 なりすまし」で触れたとおり、異なる TLD（top-level domain）を使用したり、文字列を改変したりするなど、類似ドメインの作成パターンのバリエーションが豊富であることを踏まえると期待される効果は高くないことが理解できる。

4. ビジネスメール詐欺の海外における状況

BEC の脅威に関する海外の状況や、取組みを紹介する。BEC による被害が年々増加している米国を中心として、組織や国を超えたコミュニティが結成され、BEC の被害を減らす取組みを続けている。また、金融機関や法執行機関が連携することで、BEC に関与した容疑者の摘発や逮捕に繋がった事例も複数公開されている。

4.1. 国際的な取組み

BEC の脅威に対抗するため、2015 年 12 月に「The Business Email Compromise List」というコミュニティが創立された[5]。元々BEC の脅威に関する情報交換や手法の分析などを目的として活動を開始し、その後参加者が増えるにつれ、被害者を保護するための活動も積極的に行っている[6]。2018 年 10 月には、その業績が認められ、創設者兼管理者である Ronnie Tokazowski 氏が、M3AAWG JD Falk Award を受賞している。[7]
参加者は、コミュニティで得た情報を所属組織でも BEC 抑止に向けた活動に役立てており、そこには法執行機関に加え、メールアカウントを停止できるメールサービスプロバイダや、送金に関わる金融機関などが含まれる。また、攻撃者が不正な送金を要求する前に、マルウエアなどを使用して組織から情報を窃取する事案も報告されていることから、セキュリティベンダも協力している。このように、一組織、一業界、一国では BEC の脅威に対抗することは難しいことから、今後も様々な国や組織の連携が促進されていくことが望ましい。

4.2. 金融機関の取り組み

米国では、各金融機関が犯罪に関連すると疑われる取引などを財務省に報告する制度（SAR - Suspicious Activity Reporting）を通じて、不審な取引の情報が集約されている。[8] これらは、財務省の米金融犯罪捜査網（FinCEN - Financial Crimes Enforcement Network）に届けられ、FinCEN や法執行機関などが犯罪捜査にあたり参照する。こうした取組みにより、FinCEN や法執行機関が協力して資金を取り戻す場合もあり、特に 24 時間以内に届けられた支払いについては、資金回収に成功することが多いという。FinCEN は、効果的に調査を進めるため、BEC について次のような情報を報告するよう米国内に所在する各金融機関に求めている。

---

5 How Do You Fight a $12B Fraud Problem? One Scammer at a Time
https://krebsonsecurity.com/tag/bec-mailing-list/

6 “Under the Radar” Industry Group Fighting BEC Phishing Receives 2018 M3AAWG JD Falk Award
https://www.m3aawg.org/Rel-FalkAward-2018

7 SilverTerrier 2018: ナイジェリアのビジネス メール詐欺(BEC)
https://www.paloaltonetworks.jp/company/in-the-news/2019/silverterrier-2018-nigerian-business-email-compromise

8 Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes
https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated BEC Advisory FINAL 508.pdf#page=9

［表 7: FinCEN が BEC に関して米国内に所在する各金融機関へ求める報告事項］

取引詳細	
(1)	日付、金額
(2)	仕向人情報、口座番号、金融機関
(3)	被仕向人情報、口座番号、金融機関
(4)	仲介金融機関（あれば）

手法		
(1)		メールアドレス、関連 IP アドレス、受信日時
(2)		疑わしいメール内容、タイミング、関係者
(3)		サイバーに関係する状況
	(a)	メールの自動転送設定
	(b)	メールのフィルタ設定
	(c)	マルウエア感染の有無
	(d)	認証突破方法

4.3. 逮捕事例

2018 年には、米国 FBI が、各国の法執行機関や民間組織などと協力し、BEC の大規模な摘発活動を実施した。Operation WireWire と称して約 6 か月行われたこの作戦は、米国、ナイジェリア、カナダ、モーリシャス、ポーランドなどで計 74 名の逮捕に繋がった。[9] 翌 2019 年の Operation reWired と称した作戦では、計 281 名の逮捕に繋がったことが明らかになっており、日本人の逮捕者も出ている。同年には、警視庁が FBI と連携して捜査を行い、国際的犯罪組織に加担し詐欺を働いた容疑で日本人を逮捕したという事例も報じられている。

このような詐欺の摘発には、法執行機関との連携が不可欠である。BEC の脅威についても、法執行機関や民間組織などの間でより一層連携が深まることで、犯罪者の逮捕や、逮捕事例を公表することによる犯罪の抑止に繋がることが期待される。

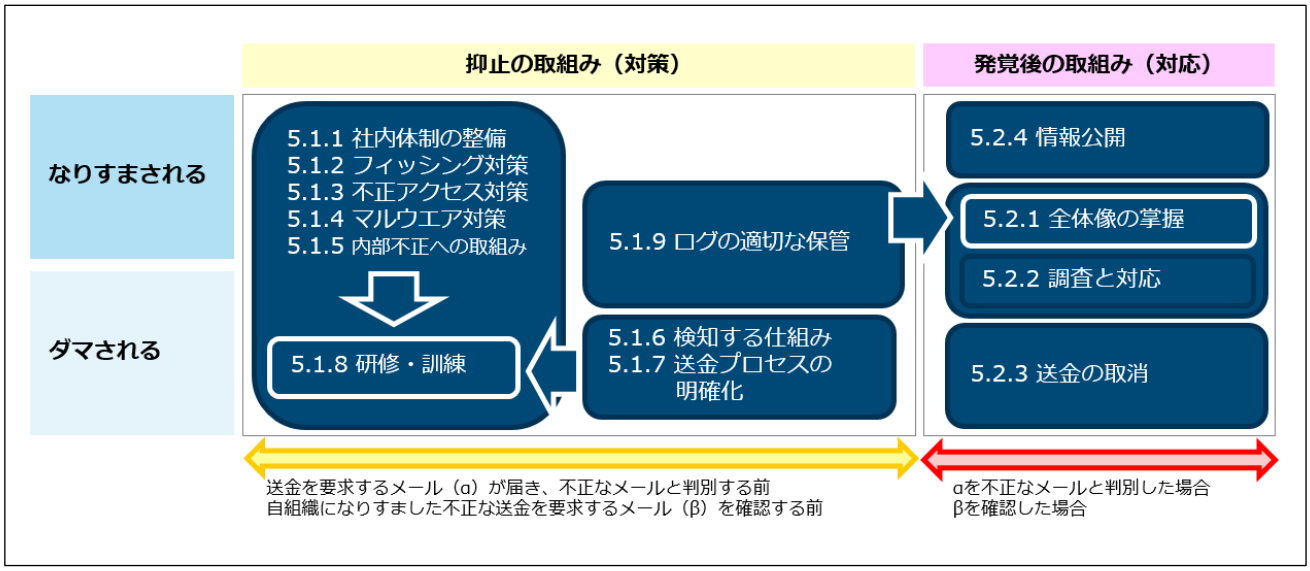
[9] International Business E-Mail Compromise Takedown
https://www.fbi.gov/news/stories/international-bec-takedown-061118

5. ビジネスメール詐欺の対策/対応

BEC の被害は、IT 部門の対策のみで防ぐことは難しく、送金業務を担う経理部門においても疑わしい送金依頼を見抜き依頼元に確認を求めるなどが必要である。一方、取引先で発生した BEC 被害において自社の部門や個人の名前が用いられていた場合には、IT 部門がログなどを分析することにより、自組織に過失がないことを証明できる可能性もある。このように、BEC に対しては IT 部門が提供する技術的な知識・スキルに加え、関係部門の担務に応じた行動を組み合わせることにより、組織全体の課題として取り組むべきである。

本章では、BEC への取組みを、抑止の取組み（対策）と発覚後の取組み（対応）に分けて紹介する。

なお、組織ごとにインシデントの定義は異なるが、本報告書では送金を要求するメールが届き、そのメールが不正なメールであると判別したタイミングまたは、自組織になりすました不正な送金を要求するメールを確認したタイミングをもって抑止と発覚後の取組みの切り分けを行うものとする。



［図 7: BEC の対策と対応］

5.1. 平時の取組み（対策）

5.1.1. 社内体制の整備

BEC またはその疑いに気づいた場合の社内体制や、エスカレーションルールが整備されていれば、組織として迅速に対応することができる。BEC に狙われる可能性があるとの共通認識の下、送金を金融機関に依頼する経理部門やメールやシステムの運用を担当する IT 部門、法的な問題が伴う場合に対応する法務部門、社外取引先との折衝を行う営業部門などが連携する体制を整備しておくことが望ましい。また、調査結果のとおり BEC は日本国外で発生することが多いことからも、海外拠点との連絡体制も整備および点検しておく必要がある。

5.1.2. フィッシング対策

Office 365 などの Web ベースのメールサービスを使用している場合、フィッシングにより認証情報を窃取される可能性がある。認証情報が窃取されメールアカウントが乗っ取られると、送受信の履歴から取引先とのやり取りを攻撃者に把握されたり、本人になりすましたメールを送信されたりすることもある。フィッシングを見分け、認証情報を窃取されることを防ぐためのトレーニングや啓発活動を利用者に対して実施する。[10]

5.1.3. 不正アクセス対策

メールアカウントの認証は、ブルートフォース攻撃などを通じて突破される可能性もある。メールアカウントの乗っ取りを防ぐためにメールサービスにおける強固なパスワードの使用、パスワードの使いまわしの禁止、多要素認証の導入など認証強化の取組みも推奨する。

5.1.4. マルウエア対策

不正な送金要求が行われる準備段階として、標的の組織から関連情報を窃取するために攻撃者が情報収集機能を有するマルウエアを使用した事案もあった。このことからもマルウエア感染に対する対策や万が一、感染してしまった場合に備えてマルウエアが行う社外への通信を検知するための対策も講じる必要がある。

5.1.5. 内部不正への取組み

「3.2.3.5 内部精通者関与の可能性」でも触れたとおり、決裁金額や攻撃対象を変えて BEC が繰り返し行われている事案では、内部に精通した関係者が関与している可能性も否定できない。内部に精通した関係者として考えられるのは役職員、退職者、取引先などであるが、対策の検討にあたっては、意図せず BEC に関与してしまう場合と主犯もしくは共犯として BEC に関与する場合を考慮する必要がある。
意図せず BEC に関与する場合は、内部情報を外部に漏らしてはいけないといった旨の教育を徹底することや、必要以上のユーザが必要以上の情報に触れたり、作業を行えたりしないようにアクセス権限を制限するなどの対策が考えられる。主犯もしくは共犯として BEC に関与する場合は、良心にもとづく行動は期待できないため、罰則など内部不正に対する組織の姿勢を示すことや、個人所有の機器や記憶媒体の持ち込み制限、アクセスログのモニタリングなど犯行を難しくしたり、犯行の見返りを減らすといった対策が求められる。
IPA が公開する「組織における内部不正防止ガイドライン」[11]には基本方針から、技術的管理、証拠確保、事後管理など具体的な対策が示されている。対策の検討にあたってはご一読いただきたい。

---

10 フィッシング対策ガイドライン
https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

11 組織における内部不正防止ガイドライン
https://www.ipa.go.jp/security/fy24/reports/insider/

なお、退職後に組織と疎遠になりがちな退職者に対しては本人が在籍している間に可能な限り対策を実施することが望ましい。誓約書の取り交わしや不要 ID の速やかな削除に加えて、不正な情報持ち出しがないか退職予定者の操作ログを確認するなど踏み込んだ対策が効果的である。慣習の違いなどから海外では国内に比べて退職時の取扱いが曖昧になる可能性もあることから、海外拠点に対しては退職者に対する対策実施状況を示すエビデンスの提出を求めるなど、積極的に関与すべきである。

5.1.6. 検知する仕組み

不正な送金を要求するメールを遮断し、メール受信者の手元に届かなければ BEC の被害を防ぐことができるものの、その多くはマルウエアが添付されているわけでもなく、不正な URL も含まないためウイルス対策ソフトなどによる機械的な駆除や防御ができない。また、正規の取引メールかのように作り込まれたメールはスパムメールや迷惑メールのフィルタで判別することも困難である。
組織に届く BEC を検知して被害を未然に防ぐためには、フリーメールアドレスから送信されたメールには警告メッセージを添えたり、一定期間やり取りのないドメインから受信したメールには、その旨を表示したりするなど、システムの機能を活用して、視覚的に受信者に対して注意を促すことで不正な送金を要求するメールへの気づきを与える効果が期待できる。
技術的な対策に加えて、業務プロセスの側面からのアプローチも有効である。BEC が商取引のプロセスで発生する詐欺行為であるという特性を踏まえ、あるべき取引プロセスとの比較を実務者に実施させることで、不審な点への気づきを促すことが期待できる。具体的には、過去の取引とメールで指示された取引の内容を並記したチェックシートを作成し、相違点を確認することが効果的である。チェックシートは BEC を早期に検知するという観点から請求に関するメールの受信者や二次チェックを行う者が作成／検証することが重要である。

［表 8:BEC 検知のためのチェック項目］

	既存取引（通常）	調査対象メール	不審点
(1) 依頼元			
送信元の組織名	株式会社〇〇	株式会社〇〇	□
送信元の担当者名	ABC 氏	ABC 氏	□
送信元の担当者電話番号	（xx）xxxx-xxxx	（xx）xxxx-xxxx	□
受信者メールアドレス	tantou@△△△cert.or.jp	tantou@△△△cert.or.jp	□
送信元メールアドレス ※偽装の可能性もあるため メールヘッダーから確認	abc@□□□tech.com	abc@□□□tach.com	■
(2) 支払いおよび口座情報			
支払い金額	7,800,000 円（税込）	7,800,000 円（税込）	□
金融機関名	△△銀行	◇◇ Bank	■
支払先口座情報（所在地）	××支店（××国）	□□支店（□□国）	■
口座番号	xxx-xxxxxxxx	yyy-yyyyyyy	■
(3) 関連情報			
■ タイムゾーン			
メール送信日時	+0900 UTC	+0100 UTC	■
添付ファイル作成日時	+0900 UTC	+0100 UTC	■

(4) メモ、気づいたポイント

- 支払先の金融機関や口座情報、送信元メールアドレスがこれまでのものと異なっている。
- 情報セキュリティ部門の確認により、メール送信日時や添付ファイルの作成日時のタイムゾーンも、これまでのものとは異なっている。
- 第三者が「株式会社〇〇」になりすまして担当者へ送金を要求しているとみられる。
- 第三者は「株式会社〇〇」の担当者名「ABC 氏」になりすまし、これまでと同額の支払い金額「7,800,000 円（税込）」を要求していることから、既存取引の内容に関する情報を入手している可能性がある。
- 双方のメールアドレスについて侵害がないか確認を要する。
  - tantou@△△△cert.or.jp
  - abc@□□□tech.com

5.1.7. 送金プロセスの明確化

不正な送金を要求するメールは受信者を“ダマす”ために様々な工夫がなされている。至急の振込が必要だとして受信者を焦らせたり、上司や幹部などになりすまして受信者にプレッシャーをかけたりするなど、心理的に受信者を動揺させる文面になっていることが多い。こうした手口に乗せられて送金してしまうことを防ぐため、社内の送金のプロセスに、客観的な立場から冷静な二次チェックができる体制を組み込んでおく必要がある。 日ごろからスケジュールに余裕を持った送金処理を行うべきであることは言うまでもない。

5.1.8. 研修・訓練

一般的にセキュリティ対策は、利用者の意識が低かったり、対策の具体的な手順が浸透していなかったりと、十分な効果が得られない。脅威を理解させて警戒心を高め、利用者に対策方法を身に着けさせるためには、研修や訓練を繰り返し実施することが必要である。
BEC 対策においては、利用者に対して BEC に巻き込まれる可能性があるとの警戒心を持たせることと、代表的な手口を利用者に示し、そうした手口に簡単には引っかからないための注意すべきポイントを理解させることが重要である。
下表は調査結果から抽出された BEC に関係したメールと見抜くための勘所である。

［表 9: BEC に関係するメール・メッセージを見抜くための勘所］

□	定常的なメールだが、発信元メールアドレスが以前と異なる
□	定常的なメールだが、発信された時間帯やメールの文面 (言い回し等)が以前と異なる
□	メールが営業時間終了間際や週末直前に届き、変則的な処理の要求を急かせている
□	過去に取引がない会社から初めて届いたメール
□	メール以外の事前連絡なしに上司や幹部からメールで指示している
□	以前に送金したことのない口座への送金を要求している

こうした勘所を実例とともに示すことによって、BEC を見抜くスキルを養うとともに、社外から送金依頼をメールで受け取る担当者が、送金処理を担当部門に依頼する際に、「5.1.6 検知する仕組み」で示したチェックシートを添付することを義務付けることにより、BEC に気づく確率を高めることができる。表 9 に示したようなメールであっても、BEC とは無縁の正規の商取引である可能性もあるため、一旦は BEC を疑って、相手にメール以外の方法（電話や対面など）で確認を行うことが望ましい。こうした取り組みは手間を取ることがあっても合理的な慎重さとして相手の理解を得られるはずである。なお、電話で確認する際には、送金を要求するメールの本文に記載された連絡先ではなく、名刺交換など他の方法で入手した電話番号を用いることも、研修や訓練を通じて関係者に徹底すべきである。

5.1.9. ログの適切な保管

インシデント対応の過程において、状況把握や調査のために操作ログなどの記録を確認するが、BEC も例外ではなく、メールやシステムログを適切に保管していない場合、原因特定や状況把握に至らないことがある。例えば、メールアカウントの監査ログを適切に記録していなかったために、直近のログイン履歴しか残っておらず、攻撃者がアカウントを侵害した事実が確認できなかったり、メール受信者が調査対象のメールを不審に思い削除してしまったりしたため、その後の調査が困難になる場合もある[12]。“なりすまされる”事案においては対外的な側面からもメールやシステムログの保管が重要となる。“ダマされた”組織から損害の補填を求められた場合、対抗するための証跡を準備するのは自組織である。

また、自組織が“ダマされて”金銭を振り込んでしまい、送金の取り消しを要請する場合、金融機関から送金を取り消すための根拠（該当の取引が BEC 被害によるものであることを証明できるデータなど）を要求されることがある。このように、メールやシステムログなどのデータは状況把握や対外的な折衝において必要となる場合があることからも保管規則などを定め、適切に保管することが望ましい。

具体的には、BEC がメールを介して発生する事案であることからも、メールログやログイン履歴を含むメールアカウントの監査ログを取得する。また、他のインシデントが関連していることを想定して、プロキシサーバやファイアウォールなどの通信ログや Active Directory など操作ログの取得も推奨する。
ログの出力にあたっては、設定が必要な場合もあることに留意するとともに、保管場所を確保する必要もある。保管場所ともに課題に挙がるのが保管期間である。BEC は代金未払をきっかけに被害が明らかとなることを踏まえると比較的短い期間を遡って調査するが、関連するインシデントの調査を考慮した場合、相当期間のログを確認する必要がある。
JPCERT/CC では、対応支援経験等を踏まえ、高度サイバー攻撃（APT 攻撃）を考慮したログの保管期間は最低 1 年以上を推奨しており、BEC についても同等の保管期間が相当である。[13]

12 Incident Response Casefile – A successful BEC leveraging lookalike domains
https://research.checkpoint.com/2019/incident-response-casefile-a-successful-bec-leveraging-lookalike-domains/

13 高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/apt-loganalysis.html
高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて
https://www.jpcert.or.jp/research/apt-guide.html
ログを活用した Active Directory に対する攻撃の検知と対策
https://www.jpcert.or.jp/research/AD.html

5.2. 発覚後の取組み（対応）

5.2.1. 全体像の掌握

不正な送金を要求するメールと判別した場合や、自組織になりすました不正な送金を要求するメールを確認した場合は、状況を正確に把握し、とるべき行動を明確にすることを目的として次に揚げる事項を整理する。

1）全体像

昨今の BEC は 1 対 n、n 対 n の関係者や組織が関与することもあることから、登場人物を洗い出し、互いの関係を明らかにすることで事象の全体像を把握する。その際、関係図などを用いて可視化することで状況を把握し易くなるだけではなく、担当者同士の認識誤りを防ぐことができる。

2）自組織の立場

全体像を把握した後、自組織が「BEC を受信した」立場なのか、「なりすまされた」立場なのかを確認する。前者では送金有無を確認し、送金実績がある場合は速やかに後述 5.2.3 BEC 被害による送金の取り消しの対応を行う。後者においても相手先での送金有無を確認し、送金実績がある場合は速やかに金融機関への送金取消を指示する。なりすまされた組織は取引先の送金有無に関わらず、なりすまされたメールの送信ドメインを確認し、自組織が業務上使用するドメインであるか否かを確認するとともに、情報公開（5.2.4 自組織になりすました BEC を認知した時の情報公開 参照）に向けた準備を行う。業務上使用するドメインのメールアドレスから不正な送金を要求するメールが送信されている場合は自組織のメールアカウントが侵害されている可能性が高いため、5.2.2 先行するインシデントの調査と対応に着手する。

3）内部情報の有無

BEC に用いられた情報について、取引関係者や自組織の者ではなければ知り得ない情報が含まれているか否かを確認する。こうした情報が含まれている場合は攻撃者にメール内容を閲覧されていたり、他のインシデントを起因とした情報漏えいが発生している可能性があるため、「5.2.2 先行するインシデントの調査と対応」に着手する。

これらは送金を要求するメール内容やメールログの確認、受信者へのヒアリングなどを通じて行う。日ごろから「5.1.6. 検知する仕組み」で示したチェックシートを使用している場合は、既に情報がまとめられていることからもチェックシートを活用することで効率よく状況を把握することができる。

5.2.2. 先行するインシデントの調査と対応

状況を把握した後、必要に応じてメールアカウントのパスワードを変更するなど、侵害を想定した対応を実施する。特にメールの内容が、内規など自組織固有の内部情報に関係するものであれば、攻撃者が既に自組織に関する情報を入手している可能性がある。このような場合、攻撃者が過去のメールのやりとりなどを閲覧している可能性もあるため、自組織や取引先など関係者のアカウント侵害有無を確認する必要がある。メールアカウントが侵害されている場合、メールの転送設定や、受信メールを削除するような設定が追加されていることもあるため、パスワード変更のみではなく設定の見直しを行う。また、フィッシング、不正アクセス、マルウエア感染などアカウント侵害や情報漏えいの原因の特定など、インシデント対応を行う。

5.2.3. 騙されて行った送金の取消

金融機関に依頼することにより、送金を取り消すことができる可能性もある。BEC であると気づかずに金融機関に送金を依頼してしまった場合、まずは、送金を依頼した金融機関に一刻も早く相談することを推奨する。送金取消の手続きを進めるにあたって、金融機関側が BEC 被害に遭った事実など情報の提示を求める場合もあることから、調査結果や保管しているメール、ログなどを準備しておくことが望ましい。

5.2.4. 自組織になりすました BEC を認知した時の情報公開

自組織になりすました BEC が試みられていることが、外部からの通知や問合せ等から判明した場合には、同様の試みが広い範囲の組織に実施されている可能性を想定し、被害拡大を防止するため、事実を可能な限り速やかに公開することが肝要である。情報を受け取った組織が調査や組織内での注意喚起に活用できるよう、伝える内容には、送信元メールアドレス（偽装されていることを考慮し、メールログから抽出）や送金先口座（銀行名、支店名、口座番号、口座名義人名）などの具体的な情報を含めることが望ましい。手段としては、取引先にメールなどで個別に通知する他、ホームページで注意を喚起するなどの方法がある。

6. おわりに

今回の取組みを通じて、BEC の被害や対策の事例と 3 つの留意点、すなわち、複数の登場人物や組織が関与している場合があること、事前に関連インシデントが発生している可能性があること、被害者でもあり加害者にもなりえることが明らかになった。BEC の被害を防ぐためにはこれらを踏まえた行動をとることが望ましい。

対策では、“ダマされない”ための対策に加え、“なりすまされない”ための対策も検討する必要がある。調査結果から自組織が“なりすまされない”ために自組織のドメインと類似したドメインの登録状況をモニタリングする組織もあったが、運用コストが高く、実現性を含めたその効果は組織の体力に依存する。“なりすまされない”ためには攻撃者からアカウントを保護するため、フィッシングや不正アクセス、マルウエアなど一般的なセキュリティ対策も有効である。また、自組織が被害に遭った場合に備えて普段からメールやシステムログを適切に保管することが推奨される。メールやシステムログは自組織が“なりすまされた”場合の証跡になるだけでなく、“ダマされた”場合の内部調査や対外的な折衝においても活用することができる。

BEC には、必ずしもシステム的に選り分ける要素が備わっていないことから、組織に届く前に遮断することは困難である。こうした状況下で“ダマされない”ためには受信することを想定していないメールを検知する仕組み作りが有効となる。既述のとおり、検知方法としてフリーメールを受信した際の警告表示など、システム面からのサポートも考えられるが、取引内容を熟知した担当者や決済段階での二次チェックなど実務面からのアプローチも重要である。このことからも、BEC への取組みは IT 部門だけではなく、組織全体で取り組むべき問題であるといえる。少し踏み込んだ言い方をするのであれば、金銭被害により組織に損害を与える BEC は経営課題の一つとして捉え、経営層自らが積極的に対応を検討すべき事象といえるのではないか。

本報告書は、日本国内における BEC 被害の増加を受け、それらを少しでも軽減することを目的として、取引の当事者である組織が取組むべきポイントに重きを置いて作成した。今後、BEC の対策に取り組む組織においてはこれらのポイントを踏まえて脅威に対する備えを準備いただくとともに、既に取り組んでいる組織においては自組織の対策状況と比較し、改善の参考資料として活用いただければ幸いである。

なお、BEC は金銭窃取を目的とした詐欺という犯罪行為であり手口も高度化していることから、標的になる組織の努力だけでは減らすことができない。被害を抑止するためには、攻撃者の取締りなど犯罪行為の抑制、BEC に用いられた不正なメールアカウントの停止や、銀行口座の凍結など法執行機関、メールプロバイダー、金融機関などの協力も必要である。海外での「The Business Email Compromise List」のように、日本国内においても、公的機関と民間組織が協力して BEC に立ち向かう環境が整うことを期待するとともに、環境が整った際には読者のみなさまにも情報提供など、積極的に活用いただくことをお願いしたい。

7. 謝辞

最後に、本調査におけるアンケートやヒアリングにご協力いただいた組織の皆様には感謝を申し上げる。また、本報告書の執筆や編集にご協力いただいた伊藤忠商事、JPCERT/CC 専門委員 佐藤 元彦氏、IPA 松坂 志氏、竹内 智子氏、マクニカネットワークス 政本 憲蔵氏に感謝の意を表し、本報告書の締めとさせていただく。