ビジネスメール詐欺（BEC）の特徴と対策

独立行政法人情報処理推進機構
セキュリティセンター

ビジネスメール詐欺（BEC）の特徴と対策

目次

ビジネスメール詐欺（BEC）の特徴と対策

初版公開：2022 年 9 月 28 日
第二版公開：2023 年 2 月 9 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

本書の要旨

本レポートは、ビジネスメール詐欺（Business E-mail Compromise：BEC）について、広く企業・組織の啓発に利用していただく事を目的とした資料です。ビジネスメール詐欺の概要とともに、攻撃のタイプ、代表的な攻撃の手口を紹介し、対策と被害に遭ってしまった際の対応について説明しています。また、IPA（独立行政法人情報処理推進機構）が運営しているサイバー情報共有イニシアティブ [1]（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan、ジェイシップ）の参加組織をはじめ、国内企業の方々から情報提供いただいたビジネスメール詐欺の統計情報も合わせて掲載しています。

本書の対象読者

本書では、次の方々を主な対象読者と想定しています。

- 企業の経理・財務部門といった金銭管理を行う部門の方
- 取引先と請求書などを通して金銭的なやりとりを行う方

なお、本書で紹介する事例や手口は、営業秘密の詐取や標的型サイバー攻撃とも通じるところがあり、組織・企業の従業員の方々全般へも参考にしていただける内容となっています。

[1] サイバー情報共有イニシアティブ（IPA）
https://www.ipa.go.jp/security/J-CSIP/

1　はじめに

ビジネスメール詐欺は、IPA が毎年公開している「情報セキュリティ 10 大脅威」において、2018 年以降、毎年ランクインしている危険性の高い脅威です。海外での被害状況も年々深刻なものとなっており、国内においてもその被害にあったという企業が後を絶ちません。

IPA では、J-CSIP の情報共有の活動[2]で得られた情報をもとに、2017 年 4 月、ビジネスメール詐欺（BEC）に関する注意喚起[3]（以降、2017 年 BEC 注意喚起）を行いました。その後、2018 年 7 月に IPA として初めて日本語でのビジネスメール詐欺の情報提供を受けたことから、これを含め 5 つの事例とともに、2018 年 8 月、続報として再び注意喚起（以降、2018 年 BEC 注意喚起）を行いました。そして、2020 年 4 月に英語で行われていた攻撃が「日本語化」した攻撃メールの事例や新型コロナウイルス感染症（COVID-19）を攻撃メールの題材とした事例を含めた 3 つの事例とともに 3 回目の注意喚起（以降、2020 年 BEC 注意喚起）を行いました。

しかしながら、その後も、J-CSIP 参加組織のみならず、一般の組織・企業からもビジネスメール詐欺の発生について IPA へ情報提供や相談が続いています。その多くは日本企業の海外支社等が標的となっている傾向にありますが、国内企業が直接狙われる事例も確認しており、実際に偽の口座へ振り込んでしまったという被害も複数寄せられています。

本書では、ビジネスメール詐欺対策の被害防止を目的として、IPA への情報提供の統計情報とともに、代表的な手口や、被害に遭ってしまった際の対応、被害に遭わないようにするための対策等、ビジネスメール詐欺全般の情報を説明します。

本書の公開に合わせて、ビジネスメール詐欺対策の情報を集約した特設ページ[4]（以降、BEC 対策特設ページ）も公開しています。当該ページでは、ビジネスメール詐欺の手口と対策を映像で説明するコンテンツ[5]（日本語字幕版と英語字幕版があります）や、掲示／配付用の A4 サイズ資料、また IPA で確認している事例を詳細に説明したレポートも掲載しています。

読者の方々へは、本書や BEC 対策特設ページに掲載した各種コンテンツを通じて、この脅威について知っていただき、十分な対策を講じ、同様の手口による被害を未然に防いでいただきたいと考えています。また、継続的な情報発信のため、ビジネスメール詐欺に関する情報があれば、IPA へご相談・ご提供をいただければ幸いです。

---

[2] J-CSIP は、IPA を情報のハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組み。

[3] 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口 （IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

[4] ビジネスメール詐欺特設ページ
https://www.ipa.go.jp/security/bec/index.html

[5] What’s BEC？ ～ビジネスメール詐欺 手口と対策 ～
https://www.ipa.go.jp/security/keihatsu/videos/

1.1 ビジネスメール詐欺（BEC）の概要

ビジネスメール詐欺（BEC）とは、巧妙な騙しの手口を駆使した、偽の電子メールを組織・企業に送り付け、従業員を騙して送金取引に係る資金を詐取するといった、金銭的な被害をもたらすサイバー攻撃です。詐欺行為の準備として、企業内の従業員などの情報が狙われたり、情報を窃取するウイルスが悪用されることもあります。

BEC は、「ビジネスメール詐欺」以外にも、「ビジネス電子メール詐欺」や「外国送金詐欺」などとも呼ばれています（本書ではビジネスメール詐欺と呼びます）。

米国連邦捜査局（Federal Bureau of Investigation：FBI）によると、2016 年 6 月から 2021 年 12 月までに、米国インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）を含む複数の情報源に報告されたビジネスメール詐欺の発生件数は、全米 50 州と 177 か国で 241,206 件、被害総額は約 433 億（43,312,749,946）米ドル（未遂を含む）にのぼっています[6]。1 件あたりの平均被害額は約 18 万米ドル（日本円では約 2,300 万円）にもなり、非常に大きな被害をもたらす脅威となっています。また、被害額について、IC3 の年次報告書[7]に記載された年間被害総額をまとめると（図 1）、年々その被害額が増加していることも分かります。

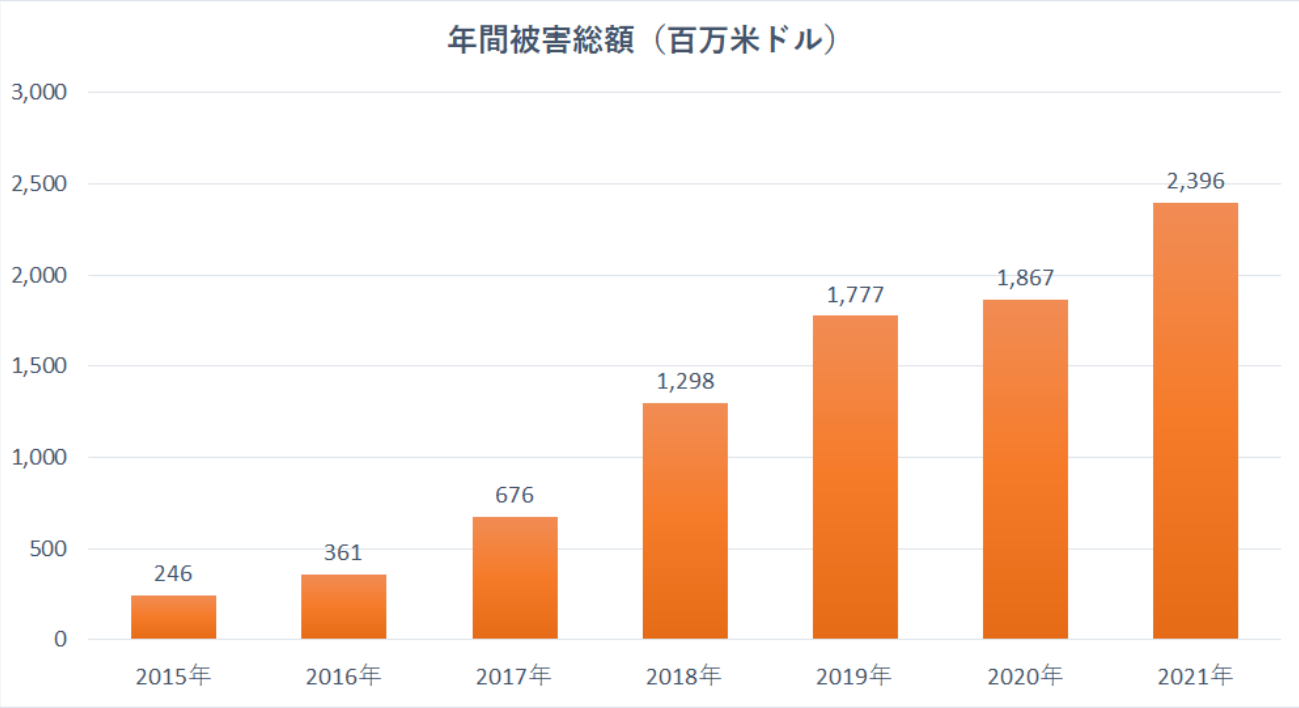

図 1 IC3 の年次報告書による年間被害額（各年次報告書を基に IPA で作成）

[6] Business Email Compromise: The $43 Billion Scam（IC3）
https://www.ic3.gov/Media/Y2022/PSA220504

[7] IC3 Annual Reports(IC3)
https://www.ic3.gov/Home/AnnualReports

さらに、JPCERT/CC が 2019 年に実施した、国内企業 12 社を対象としたビジネスメール詐欺の調査結果では、不正な請求額の合計（被害の有無に拠らない）が約 24 億円であったと報告されています [8]。この調査結果からも、ビジネスメール詐欺が国内の企業・組織において注意を要する脅威であると言えます。

このほか、ビジネスメール詐欺は、警察、国内の金融機関やセキュリティ事業者等、複数の組織から注意喚起がなされています。国内外を含めビジネスメール詐欺に関連した容疑者が逮捕されるといった報道も多数あります。しかしながら、IC3 の報告にある被害件数に表れているように、ビジネスメール詐欺は継続して行われていることを示しています。

企業での送金取引に関係する担当者、特に経理・財務部門など金銭管理を行う部門の担当者においては、ビジネスメール詐欺の手口について知っていただくことが非常に重要です。「このような詐欺がある」ということすらも知らなければ、受信したメールなどに多少不自然な点があっても、騙されてしまいかねません。攻撃者に騙されないよう、BEC 対策特設ページにある情報や事例をもとに、組織内の対策や意識の向上に役立ててください。

なお、メールを駆使した巧妙な騙しの手口は、主に諜報活動を目的とする「標的型サイバー攻撃」とも通じるところがあり、経理・財務部門などに限らず、組織・企業の従業員全般へも参考になると思われます。

本書は、まず 1.2 節でビジネスメール詐欺のタイプを紹介し、次に 2 章でこれまで IPA に情報提供のあった事例を整理し統計情報等を紹介します。3 章ではビジネスメール詐欺の代表的な手口を説明します。

そして、4 章でビジネスメール詐欺被害に遭ってしまった場合の対応、5 章でビジネスメール詐欺への対策について説明します。

[8] ビジネスメール詐欺の実態調査報告書 （JPCERT コーディネーションセンター（JPCERT/CC））
https://www.jpcert.or.jp/research/20200325_BEC-survey.pdf

1.2 ビジネスメール詐欺の 2 つのタイプ

本書では、これまで IPA で確認している事例から、ビジネスメール詐欺を次の 2 つのタイプに分類して説明します。

なお、IC3[9]やトレンドマイクロ社[10]では、詐欺行為の準備等といった手口も含め 5 つのタイプに分類しています。5 つのタイプについては、IPA の 2017 年 BEC 注意喚起で説明しています。本書では詳細を省略しますので、必要に応じてそちらを参照してください。

- タイプ 1：取引先との請求書の偽装

  このタイプは、取引先等と請求に係るやりとりをメールなどで行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等を送り付け、振り込みをさせるというものです。このとき、攻撃者は取引に係るメールのやりとりをなんらかの方法によって事前に盗み見て、取引や請求に関する情報や、関係している従業員のメールアドレスや氏名等を入手していることがあります。

  攻撃者は最終的に支払側の企業の担当者を騙し、攻撃者の口座へ送金をさせようとします。IPA では、海外の企業と取引を行っている企業で多く確認しています。

  この手口は、「偽の請求書詐欺（The Bogus Invoice Scheme）」や、「サプライヤー詐欺（The Supplier Swindle）」、「請求書偽装の手口（Invoice Modification Scheme）」などと呼ばれています。

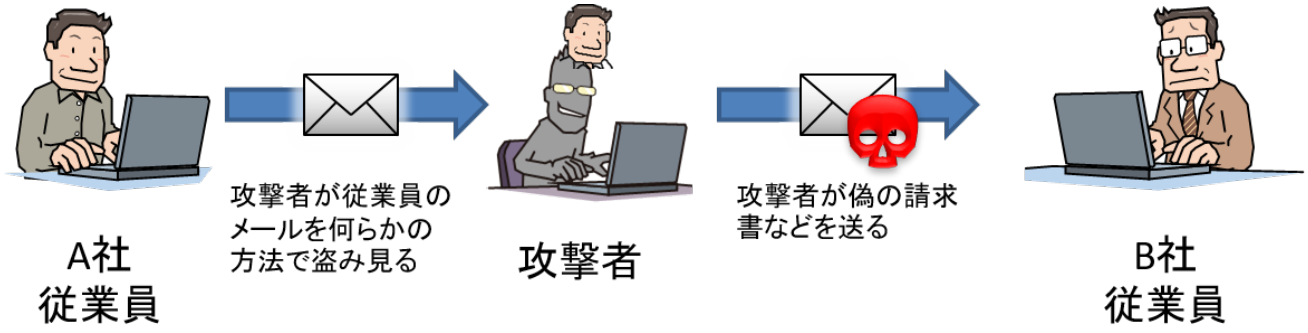

図 2 タイプ 1：取引先との請求書の偽装

一例として、IPA で確認しているタイプ 1 の攻撃事例では次のようなケースがあることを確認しています。

- 自組織の担当者を騙る攻撃者から、海外取引先担当者へ、偽の口座に送金先の変更を依頼する偽のメールが送られた。
- 海外取引先担当者を騙る攻撃者から、自組織の担当者へ、請求書の変更と称して、偽口座に改ざんされた請求書が添付された偽のメールが送られた。
- 海外子会社の担当者を騙る攻撃者から、自組織の担当者へ、偽の口座に送金先の変更を依頼する偽のメールが送られた。

等

---

[9] Business E-mail Compromise: The 3.1 Billion Dollar Scam （IC3）
https://www.ic3.gov/media/2016/160614.aspx
※ 5 つのタイプの原典はこちらを参照してください。

[10] 多額の損失をもたらすビジネスメール詐欺「BEC」（トレンドマイクロ）
https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/3151/billiondollar-scams-the-numbers-behind-business-email-compromise

- タイプ 2:経営者等へのなりすまし

このタイプは、攻撃者が企業の経営者や企業幹部(役員)などになりすまし、企業の従業員に攻撃者の用意した口座へ振り込みをさせるというものです。このとき、事前に攻撃者はなんらかの方法によって、企業の役員などのメールアドレスを調べ、より本物らしくなりすましを行う場合もあります。

攻撃先としては、企業内の財務・経理担当者といった金銭管理を行う部門が狙われる傾向にあります。IPA では、「秘密の案件で相談がある」や、「相談したいことがあるので少し時間があるか」といった経営層からの問い合わせを装う手口を多く確認しています。

この手口は、「CEO 詐欺(CEO Fraud)」や、「企業幹部詐欺(Business Executive Scam)」、「なりすまし詐欺(Masquerading)」などと呼ばれています。

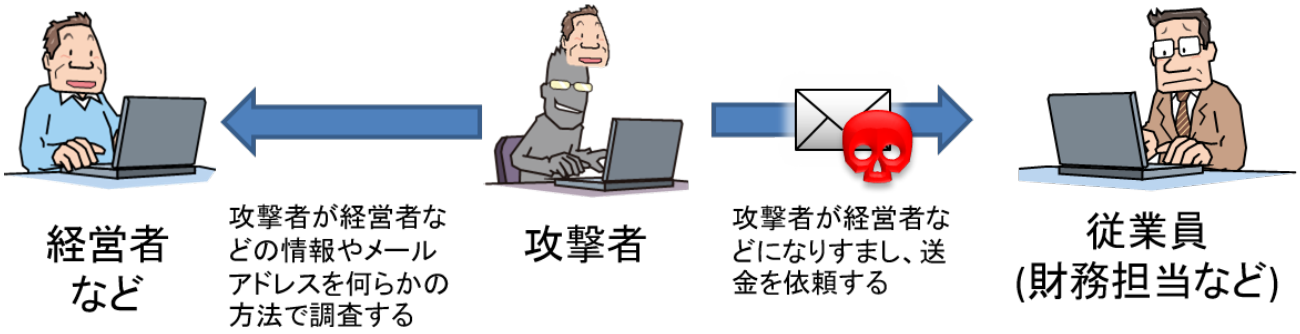

図 3 タイプ 2:経営者等へのなりすまし

一例として、IPA で確認しているタイプ 2 の攻撃事例では次のようなケースがあることを確認しています。

- 自組織の経営層を騙る攻撃者から、自組織の従業員へ偽のメールが送られた。
- 親会社の経営層を騙る攻撃者から、子会社の経営層へ偽のメールが送られた。
- 親会社の経営者を騙る攻撃者から、海外の関連会社の経営層へ偽のメールが送られた。
- 海外関連会社の経営層から、自組織の従業員へ偽のメールが送られた。
- 海外関連会社の経営層から、別の海外関連会社の経営層へ偽のメールが送られた。

等

これらタイプ 1、タイプ 2 のそれぞれ具体的な事例内容については、BEC 対策特設ページにある各事例を参照ください。

2　IPA へ情報提供されたビジネスメール詐欺事例の統計情報

IPA では、J-CSIP の参加組織や、個別に IPA へ情報提供いただいた組織等から、次に示す通り、2015 年から 2022 年 7 月にかけて発生したビジネスメール詐欺に関する **292 件**の情報提供（J-CSIP 内の組織から 228 件、J-CSIP 外の組織から 64 件）を受けており、うち **27 件**で金銭的被害が確認されています。

この中で、「タイプ 1：取引先との請求書の偽装」に該当する事例は **66 件**、「タイプ 2：経営者等へのなりすまし」に該当する事例は **226 件**を確認しています。

日本語で行われたビジネスメール詐欺は **26 件**確認しており、その他の事例では主に英語が使われていました。なお、日本語のビジネスメール詐欺の事例はいずれもタイプ 2 による攻撃でした。

表 1 IPA で確認しているビジネスメール詐欺の事例件数

情報提供年	情報提供件数		被害あり件数	タイプ 1	タイプ 2
	J-CSIP 内	J-CSIP 外			
2015 年	1	0	0	0	1
2016 年	3	0	2	3	0
2017 年	4	1	1	3	2
2018 年	10	5	4	12	3
2019 年	42	9	9	15	36
2020 年	123	32	2	9	146
2021 年	32	14	7	13	33
2022 年 ※	13	3	2	11	5
合計	228 件	64 件	27 件	66 件	226 件

※　2022 年 1 月から 2022 年 7 月末時点までの件数を表しています。

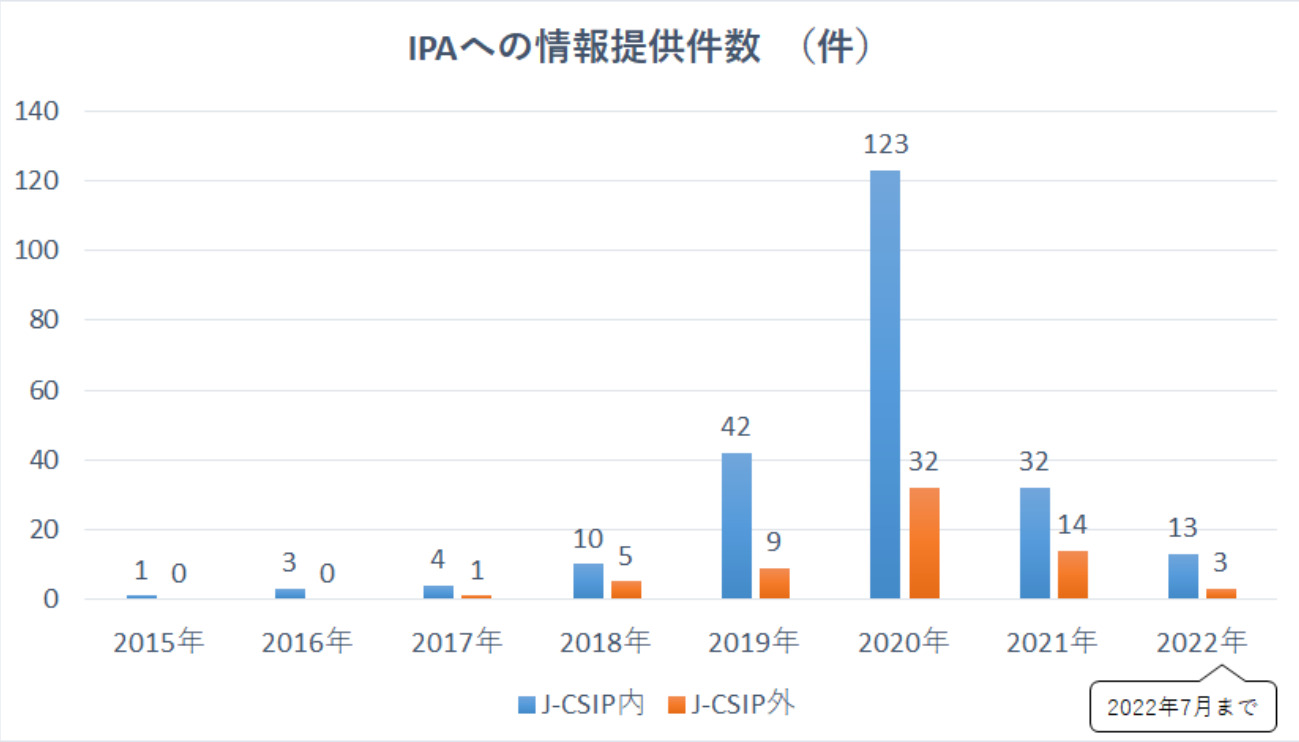

図 4 IPA で確認しているビジネスメール詐欺の事例件数

3　ビジネスメール詐欺の代表的な手口の紹介

ビジネスメール詐欺には大きく分けて、準備段階のステップと、金銭を詐取するためのステップがあります。準備段階のステップではメールの盗み見等で情報収集を行い、その後、金銭を詐取するステップでメールのやりとりを行って相手を騙し、金銭の詐取を試みます。本章では、IPA で把握した複数の事例から、ビジネスメール詐欺の各ステップで使われる代表的な手口について解説します。特にタイプ 1 では、いずれのステップでも支払側と請求側の双方が標的となり得るため、注意が必要です。詳細な事例の内容は、BEC 対策特設ページに掲載しています。

3.1 準備段階のステップで使われる手口

タイプ 1 の取引先へのなりすましでは、攻撃者は取引に係るメールのやりとりを盗み見ている可能性があります。この方法として、情報を窃取するウイルスへの感染や、メールアカウントへ不正アクセス [11]し盗み見る、メールアカウントに不正な転送設定（図 5）を行い、メールを攻撃者へ転送し盗み見るといったことが考えられます。また、通常では利用者が確認しないであろうフォルダへメールの振り分け設定を行い、攻撃が行われていることに気づきにくくするといった手口も確認しています。

また、タイプ 2 の経営者等へのなりすましでは、ソーシャルメディアや組織のホームページなどの公開情報から氏名やメールアドレスといった情報を収集する手口が考えられます。

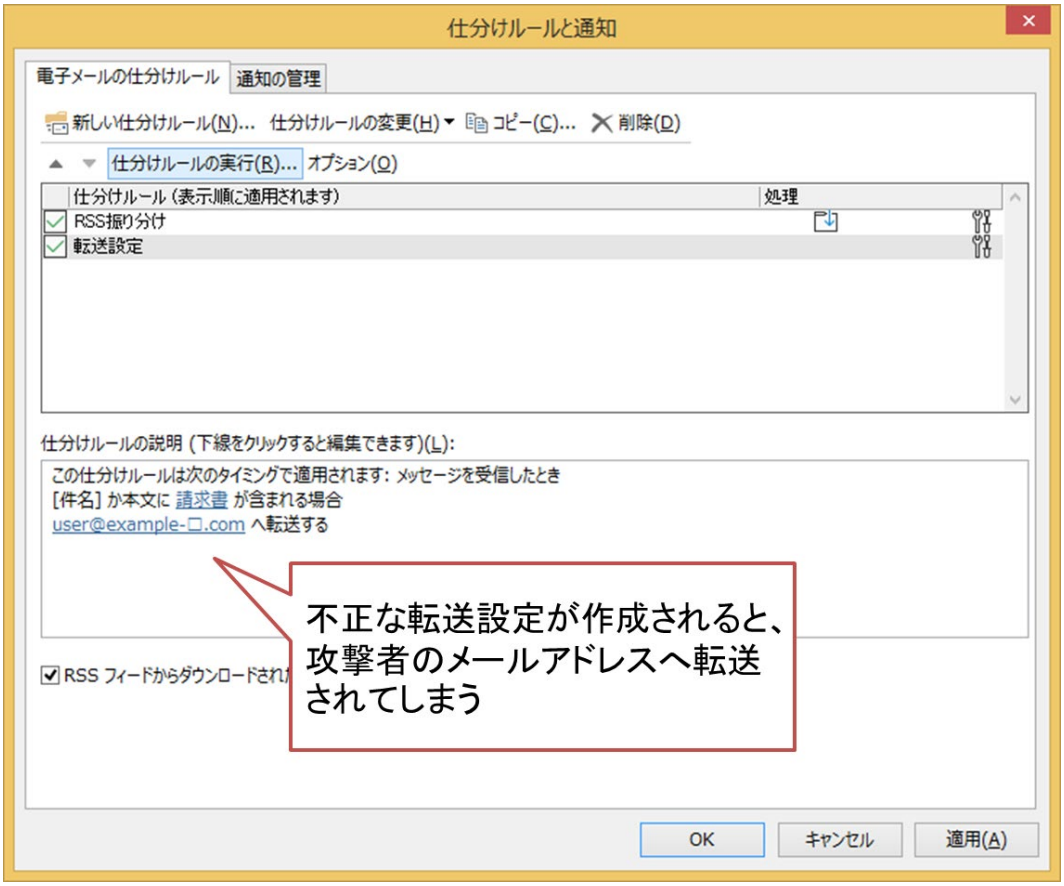

図 5 不正な転送設定例（Outlook）

[11] 攻撃者はメールアカウントに不正アクセスするため、事前になんらかの方法によってメールアドレスとパスワードを入手していると考えられます。この方法としてフィッシングメールによる情報の窃取等も考えられるため、フィッシングメールへの対策等も必要になるでしょう。

3.2 金銭を詐取するためのステップで使われる手口

金銭を詐取するためのステップで使われる手口を、相手を信じ込ませる騙しの手口と、技術的な攻撃の手口に分けて解説します。

3.2.1 相手を信じ込ませる騙しの手口

ビジネスメール詐欺では、攻撃者はメールの内容やメールの送信元が本物であると信じ込ませるような内容のメールを送ってきます。この相手を信じ込ませる手口についていくつか紹介します。

◆ 振込先口座の変更依頼

これはタイプ 1 でよくみられるメールの内容で、攻撃者が事前になんらかの方法で、取引に係るメールを盗み見ていて、全く不自然さがないよう支払いのタイミングを見計らって、支払側へ偽の口座情報を送るという手口です。このメールの特徴としては、「監査によって一時的にいつもの口座が使えないので別の口座へ振り込んで欲しい」や、「支払い内容に一部間違いがあったので修正した請求書を送る（支払先の口座を修正した請求書を添付している）」といった理由で、別の口座への支払いを要求する手口を多く確認しています。実際に送られてくる請求書等は本物の請求書を流用して振込口座を改変[12]して送ってくることもあり、偽物であると見分けにくい事例もあります。

◆ 秘密の案件で相談があるという依頼

これはタイプ 2 でよくみられるメールの内容で、企業・組織の役員や経営層になりすました攻撃者から送られてくる手口です。このメールの特徴として、M&A（企業の合併買収）等を理由として、「秘密の案件で相談がある」や、「弁護士から連絡があったか」といった内容のメールを送り付けてきます。このように、他の従業員へ相談させないようにすることで詐欺とばれにくくする、また何度かメールのやりとりさせることで本物の相手と信じ込ませようとしているものと考えられます。その後、メールへ返信することで、偽の口座へ入金をしてほしいと依頼のメールが返ってくる事例も確認しています。

◆ 時節に合った内容

新型コロナウイルス感染症（COVID-19）を理由とした内容（都市のロックダウン等）で偽のメールが送られてくることを確認しています。これ以外にも、企業の賞与支給時期を見計らって送られてくる偽のメール等も確認しています。時節に合った内容とすることで、メールの内容を本物と思わせ（そういう事情があるのだと思わせる）ようとしているものと考えられます。

◆ 引用部分の改変

タイプ 1 では、取引先とのメールのやりとりの中で攻撃者が割り込んでくるため、攻撃者にとって都合の悪い内容や、署名部分に記載されているメールアドレスや電話番号といった内容を改変してきます。引用部分の過去のやりとりを見返しても偽の内容となっていれば相手はそのまま信じてしまうことにもなりかねません。また、改変しないままだと、正規の取引先に連絡を取られてしまう可能性もあります。そのため、これらは攻撃を発見しにくくするための手口であろうと考えられます。

---

[12] PDF ファイルの請求書の改変では、「RAD PDF」と呼ばれる編集ツールを利用している事例を複数確認しています。ただし、本ツールを利用して作成された PDF だからといって、必ずしも悪意のある PDF ファイルというわけではありません。

◆　**支払側にもなりすます**

タイプ 1 では、攻撃者が支払側の組織になりすまし、請求側の組織に対しても、偽のメールを送る事案を確認しています。

支払側が偽の口座へ入金してしまうことにより、正規の取引先への支払いがストップすると、状況確認などのために請求側が支払側に連絡し、詐欺が露見する可能性があります。攻撃者は、支払い遅延の（嘘の）理由を示す偽のメールを送ることで、ビジネスメール詐欺の発覚をできるだけ遅らせようと試みてきます。

また、支払側が、本物の請求側でないと用意できないような文書や証明書などを提示するよう、請求側になりすました攻撃者に要求することがあります。こういった場合でも、攻撃者は巧みに支払側になりすまし、請求側を騙して、それら正規の文書などを入手します。そして必要に応じて改ざんした上で、支払側に送ります。

攻撃者は、詐欺の露見を防ぐため、請求側と支払側の両方になりすまし、両方を騙すのです。

3.2.2　技術的な攻撃の手口

ここでは、ビジネスメール詐欺のメールで使われる、電子メールに特有の技術的な攻撃の手口についていくつか紹介します。

◆　**詐称用ドメイン**

攻撃者はなりすましメールを送る際に、企業・組織のドメインに似せた詐称用のドメインを取得することがあります。例えば、正規のドメインから 1 文字違いであったり、誤認しやすい文字（「m」を「r」と「n」にする等）に変更したり、トップレベルドメインが異なるといったケースが多く確認されています（図 6 の①～⑤）。

また、詐称用ドメインの取得はなりすましメールの前日に取得する場合を多く確認しています。これは、企業・組織によっては自身の類似ドメインが取得されていないか定期的にチェックしている場合があり、このチェックで発見されにくくするためと考えられます。

■本物のメールアドレス	alice @ company-☐ . com	
■偽物のメールアドレス	① alice @ compnay-☐ . com	一文字入れ替える
	② alice @ companys-☐ . com	一文字追加
	aalice @ company-☐ . com	
	③ alice @ comp ny-☐ . com	一文字削除
	④ alice @ cornpany-☐ . com	誤認しやすい文字へ変更
	⑤ alice @ company-☐ . net	トップレベルドメインを変更
	⑥ alice-company-☐ @ freemail.com	フリーメールアドレスを使う

図 6 攻撃者が使う偽のメールアドレスのパターン例

◆　**フリーメールアドレスの悪用**

なりすましメールでは、偽の詐称用ドメインの取得の他、フリーメールアドレスを使って、正規の企業のドメインに似たメールアドレスを取得してくることも確認しています（図 5 の⑥）。特に、mail.com[13]という海外のサイトで取得できるフリーメールアドレスのドメインが悪用されているケースを複数確認しています。

◆　**差出人の表示名に正しいメールアドレスを使う**

なりすましメールの差出人（From）メールアドレスに、正規のメールの差出人名やメールアドレスを表示名として設定し、実際は偽のメールアドレスから送付されてきているにも関わらず、本物のように見せかける手口を確認しています。一見すると正しいメールアドレスからの送付に見えるように細工しています。この状況でメールへの返信を行うと、あたかも本物のメールアドレスに返信するように見えますが、偽のメールアドレス宛にメールが送信されてしまいます（図 7）。

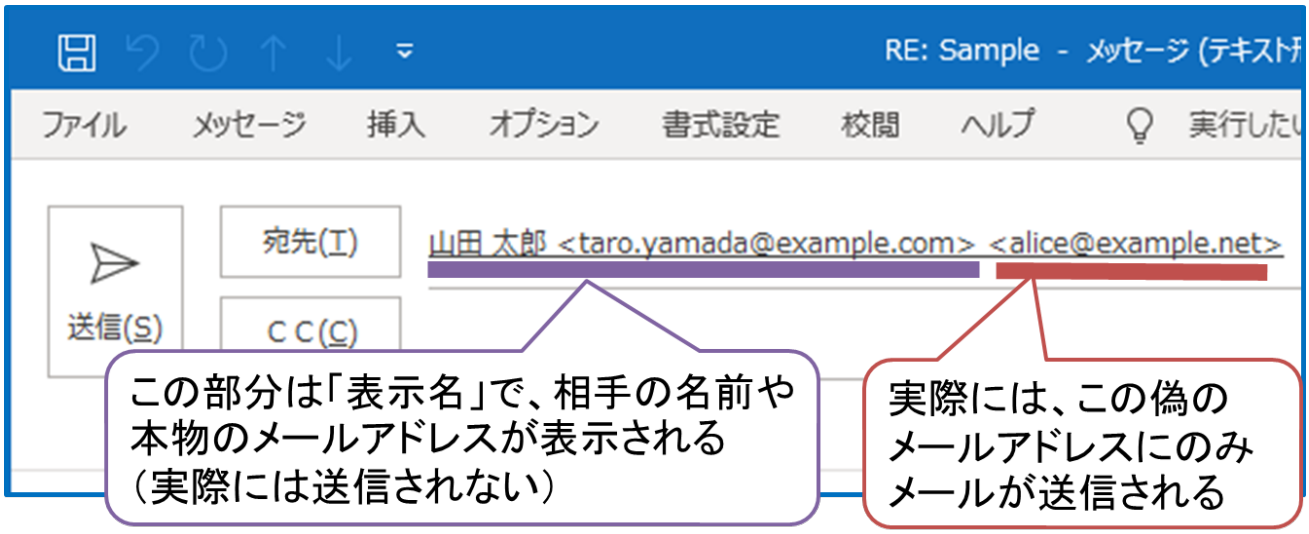

図 7 表示名の偽装の手口の例

[13] Mail.com
https://www.mail.com/
2022 年 7 月時点で 191 ドメインのメールアドレスが取得可能となっています。

◆　**返信先を偽のメールアドレスに設定する**

攻撃者から送られてくるメールの差出人（From）メールアドレスは企業の正規のメールアドレスを使いつつ、返信先（Reply-To ヘッダ）に偽のメールアドレスを設定している事例も多く確認されています。着信したメール自体は正規のメールアドレスですが、返信ボタンをクリックして返信する際、送り先が（差出人のメールアドレスではなく）偽のメールアドレスになってしまいます（図 8）。

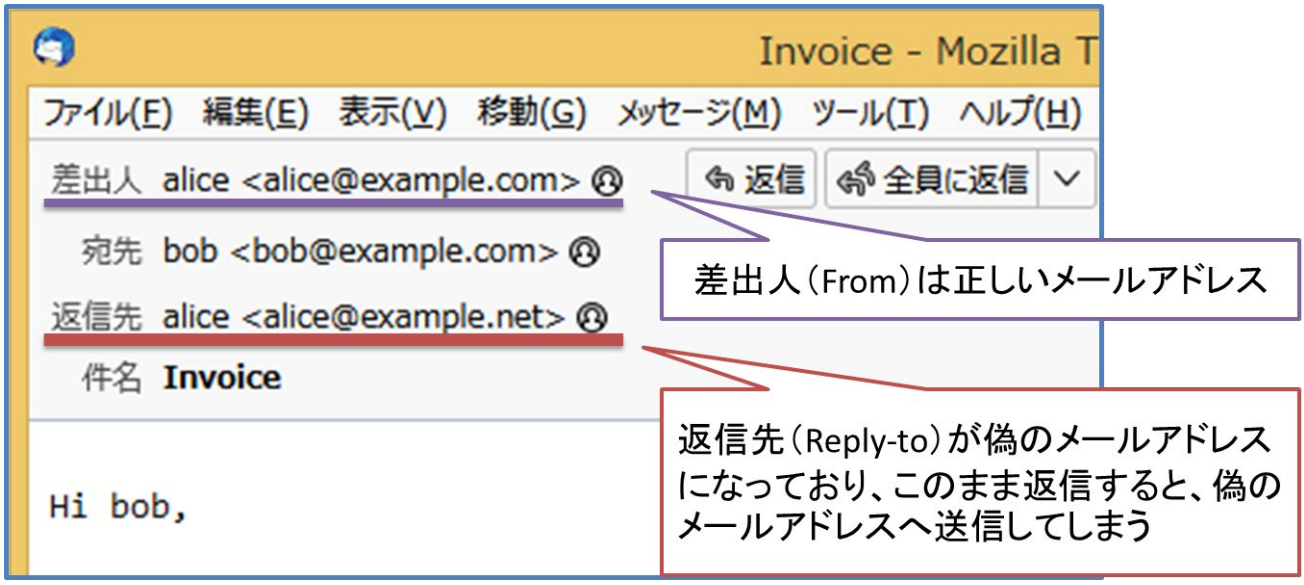

図 8 返信先に偽のメールアドレスを設定する手口の例

◆　**同報先（CC）の改変**

ビジネスメールでは、その取引やメールの内容に関係のある人物を同報先として CC に設定してメールをすることが多くあります。攻撃者はその CC にあるメールアドレスも偽のメールアドレスに改変してきます（図 9）。これは、同報先の人物へメールが送られることで偽のメールであることが発覚することを避けるためで、詐欺の発見を遅らせる意図があります。

図 9 同報先（CC）の改変の手口の例

4　ビジネスメール詐欺被害に遭ってしまったら

本章では、ビジネスメール詐欺被害に遭ってしまった場合、どのような対応をとるべきなのかを説明します。また、ビジネスメール詐欺では、被害者になることもあれば、意図せず攻撃者に加担してしまう可能性もありうるため、それぞれの立場によって注意していただきたい点もあわせて説明します。

4.1 ビジネスメール詐欺被害が判明した場合の対応

ビジネスメール詐欺の被害が判明した場合、次のような対応を行うことが有効です。

◆　送金のキャンセルや組み戻し手続き

もし、攻撃者から送られてきた偽の口座へ送金を行ってしまった場合、送金に利用した銀行へ、早期に送金のキャンセルや組み戻しの手続きを依頼しましょう。

また、海外拠点で振り込みをしてしまった場合や、振込先の口座が海外であった場合、当該地域の現地警察へ連絡し、偽の口座の凍結や資金の回収について相談することが必要です。偽口座が米国にある場合、FBI や IC3 へ通報することも有効です。

なお、これまで IPA で確認している事例では、すでに攻撃者によって送金した資金が引き出された後で、回収できなかったという事例も多数確認しています。このような手続きを行ったからといって必ずしも資金が回復できるとは限りませんが、送金後すぐに銀行に連絡することは有効な手段です。

◆　状況把握、時系列記録、証跡の収集

警察や銀行へ連絡を行うにあたり、調査のために資料としてログを含め証跡の提示を求められる可能性があります。このため、可能な限り攻撃者から送られてきたメール等は確保し、状況の把握やどのような経緯でメールが送られてきたか等をまとめておくことを勧めます。

また、取引先に対して偽のメールが送られてくるといった場合もあるため、取引先にも偽のメールの確保や状況調査等を依頼する必要があります。このとき、攻撃者にメールが盗み見られている可能性もあり、メール以外の方法で取引先に連絡を取る必要があるため、事前に緊急時の連絡経路は決めておくことを勧めます。

なお、内部犯行による可能性があることも考えられるため、調査の際には最小限の関係者で調査を行う等注意が必要です。

◆　暫定対応と原因調査

ビジネスメール詐欺が判明した際に、関係者全員が次の対応を行う必要があります。このとき、自組織だけでなく、取引先の担当者へも連絡し、対応を依頼するべきでしょう。

- 関係者の PC に対するウイルスチェックの実施

  情報を窃取するウイルスへの感染がないかをチェックする。

- 関係者のメールアカウントのパスワード変更

  関係者全員のメールアカウントのパスワードを変更する。このとき、他のサービスと使い回しをしていない複雑なパスワードを設定する。

また、取引先とのメールのやりとりが攻撃者に盗み見られている可能性があるため、次のような原因の調査を行うことが望ましいと考えます（自組織で行うことが難しければ、セキュリティ専門会社等へ調査を依

頼することも有効です）。なお、原因調査は自組織だけではなく、取引先でも調査をするよう依頼する必要があります。

- 関係者のメールアカウントへの不正アクセス痕跡の調査

関係者のメールアカウントへ不審なアクセス痕跡がなかったか、ログの調査等を実施する。特に海外からの不審なアクセスがなかったかをチェックする。

- 関係者のメールアカウントに不審な設定が行われていないか調査

メールアカウントに対し、外部へのメールの転送設定や、普段見ないフォルダへの振り分け設定等がないか調査をする。

- 関係者へのヒアリング

1 年以内程度を目安に、不審なメールを開いていないか、フィッシングサイトのようなサイトでメールアドレスやパスワードを入力した覚えはないか、メールアカウントのパスワードは他のサービス等と使い回しをしていないか等をヒアリングする。

なお、これらの調査を行ったとしても必ずしも原因が特定できるわけではありません。IPA で確認している事例でも原因について不明であったケースも多く確認しています。

取引先側に問題がありそうだと推測できても、ビジネス上の関係性から、原因調査を依頼できなかったという相談も多くあります。可能であれば、平時から、あるいはビジネスを開始する前に、このようなセキュリティインシデントが発生した場合の対応方針について合意しておくといった対策も検討してください。

◆ 社内外へ向けた注意喚起とグループ会社等含めた情報共有

ビジネスメール詐欺は自組織や取引先へなりすまし、偽のメールを送ってきます。特に自組織を詐称された場合、今後も偽のメールが送られることもあるため社内外へ注意喚起を行うことも有効です。

また、グループ企業等になりすまし、同じグループ企業内へ攻撃が行われる事例もあります。グループ企業間で事例を詳しく共有し、類似した攻撃を受けないように備えるべきでしょう。

4.2 被害原因と被害者それぞれの立場で考えられること

ビジネスメール詐欺では、被害に至る前に攻撃者によってメールが盗み見られているケースがあります。特にタイプ 1 の場合、自組織と取引先のやりとりの中で被害にあった際には、被害者（金銭的被害を負ってしまった側）の立場もさることながら、その原因がどちらにあったのかといった点も注意しなければなりません。

これらのケースは表 2 にまとめているように、被害者が取引先で自組織にセキュリティ上の原因がある（メールアカウントが乗っ取られてしまった等）場合、金銭的な被害があったということから損害の補填を求める訴訟等のリスクもあることは注意しなければなりません。なお、メールが盗み見られたのではなく、ただ本物に似通ったメールアドレスから送られたメールに騙されてしまった（タイプ 2 等で見られるケース）場合、偽のメールであると気づけなかったという点が被害原因になることも考えられます。

このように、まずは”なりすまされない”ために必要な対策を取ることも重要ですが、攻撃が発生した場合、被害範囲の特定、原因究明等の初動対応で必要となる費用のほか、取引先等から損害賠償を求められた場合に対応できる措置等を検討しておくことも必要です。

表 2 被害原因と被害者の組み合わせによる問題点

		被害者（金銭的な被害を受けた側）	
		自組織	取引先
被害原因	自組織	■自組織内の問題 取引先になりすました偽のメールが自組織内へ着信している状況です。 取引先へ誤って疑いをかけないように対応をする必要があります。 また、正規の支払いが行われていないため、取引先から支払いを求められることも考えられます。	■取引先が偽メールに気づけなかった 自組織になりすました偽のメールが取引先へ着信している状況です。 その原因の一つが、自組織側のセキュリティ上の問題だったという状況で、損害賠償の請求や訴訟等のトラブルに発展する可能性があります。
	取引先	■自組織が偽メールに気づけなかった 取引先になりすました偽のメールが自組織内へ着信している状況です。 取引先が調査対応に非協力的な場合もあり、対応が難しくなるケースも考えられます。 損失の補填について、取引先と調整の余地がある場合があります。	■取引先の問題 自組織になりすました偽のメールが取引先へ着信している状況です。 自組織側の問題ではなくとも、取引先から調査協力を求められる可能性があります。 また、原因が自組織にあったのではと取引先から疑いをかけられてしまう可能性もあります。

5　ビジネスメール詐欺への対策

本書で示したように、ビジネスメール詐欺では、巧妙なソーシャルエンジニアリングの手口の応用や流行する時事情報を取り入れてくるなど、様々な手法を駆使した攻撃が行われます。また、企業や組織の、どの従業員が、いつ攻撃の対象となるかは分かりません。このような攻撃に対抗するため、ビジネスメール詐欺について理解するとともに、不審なメールなどへの意識を高めておくことが重要です。

ビジネスメール詐欺の被害にあわないようにするには、次のような対策を行うことが望ましいと考えます。これらの対策は、諜報活動を目的とするような標的型サイバー攻撃における、標的型攻撃メールへの対策とも共通する点があります。

◆　取引先とのメール以外の方法での確認

振込先の口座の変更といった、通常とは異なる対応を求められた場合は、送金を実施する前に、電話やFAX などメールとは異なる手段で、取引先に事実を確認することを勧めます。メールに書かれている署名欄は攻撃者によって偽装されている可能性があるため、信頼できる方法で入手した連絡先を使ってください。

特に、突然の振込先の変更、決済手段の変更を求められた場合や、急な対応を促すような請求や送金の依頼メールは、ビジネスメール詐欺ではないか、よく確認することを勧めます。

◆　社内規程の整備

「メール以外の方法での確認」といった手順を含む、ビジネスメール詐欺への対策を念頭に置いた、電信送金に関する社内規程を整備することも必要です。複数の担当者によるチェック体制を徹底するといった対策も有効です。

◆　普段とは異なるメールやフリーメールに注意

ビジネスメール詐欺では、海外取引におけるメールでのやりとりで多く発生しています。英語が母国語ではない国との取引の場合、多少間違った英語でのメールが着信したとしても不思議ではありません。しかし、その中でも、普段とは異なる言い回しや表現の誤りには注意が必要です。

また、攻撃者がフリーメールサービスで取得したメールアドレスを使い、「表示名」の部分に細工をして、偽メールを送信してくるケースも多くみられます。フリーメールサービスから着信したメールについて、受信者向けに、件名や本文へその旨の注意喚起を追加するシステムを採用することにより、偽メールを見分けやすくなります。

攻撃者がメールを偽装する方法は様々ですが、「偽のメールだと気付かず返信する場合でも、送信先となっている（偽の）メールアドレスに注意していれば、見抜ける可能性があった」事例が多くみられます。メールのやりとりの最中で、いつの間にか相手が別人に入れ替わっているという状況は、なかなか想像しにくいものですが、その可能性を忘れないようにしてください。

◆　不審と感じた場合の組織内外での情報共有

ビジネスメール詐欺に限らず、メールは様々なサイバー攻撃の入口の一つであり、注意深く扱うべきです。不審なメールに担当者が気づけることは重要ですが、それと同時に、その情報を適切な部門に報告できる体制が重要です。不審なメールなどの情報を集約して周知することで、他の担当者に届いた攻撃メールに気づくことができ、自組織に対する悪意ある行為を認識することで、深刻な被害を防ぐことができるかもしれません。

ビジネスメール詐欺の場合、なんらかの不審な兆候が、取引先への攻撃を明らかにする可能性もありま

す。従って、取引先との連絡・情報共有も重要です。

また、自組織を詐称したビジネスメール詐欺を認知した場合は、取引先全体あるいは一般に向けて注意喚起を公開することを検討してもよいでしょう。

◆ ウイルス・不正アクセス対策

ビジネスメール詐欺では、攻撃や被害に至る前に、なんらかの方法でメールが盗み見られている事例が多くあります。原因は、メールの内容やメールアカウントの情報を窃取するウイルス感染や、メールサーバへの不正アクセス等が考えられます。

「不審なメールの添付ファイルは開かない」、「セキュリティソフトを導入し、最新の状態を維持する」、「OSやアプリケーションの修正プログラムを適用し、最新の状態を維持する」といった、基本的なウイルス対策の実施が不可欠です。

また、特に、メールアカウントやメールサーバ（サービス）の防御が重要です。「メールアカウントに推測されにくい複雑なパスワードを設定する」、「他のサービスとパスワードを使い回さない」、「多要素認証を設定する」、「社外からアクセス可能なメールサーバやクラウドサービスを使用している場合、アクセス元を制限したり、不審なログインを監視する」といった、職員のメールを不正アクセスから守る対策が必要です。

クラウドサービス特有の対策については IC3 の注意喚起[14]も参照してください。また、Office 365 のメールアカウントが乗っ取られ、利用者本人が設定していない転送設定やフォルダの振り分け設定がされている等、不正利用の兆候がある場合の対処方法[15]が Microsoft 社より公開されています。

◆ 電子署名の付与

取引先との間で請求書などの重要情報をメールで送受信する際は、電子署名を付けるといった、なりすましを防止する対策も有効です。

◆ 類似ドメインの調査

ビジネスメール詐欺の攻撃者が、企業・組織のドメイン名に似た「詐称用ドメイン」を取得し、その取引先へ攻撃を行う事例が非常に多く確認されています。ビジネスメール詐欺に限らず、自組織を詐称するフィッシング攻撃や、自組織に関わる悪意のある活動全般を把握するため、定期的に、自組織に似たドメイン名が取得されていないかを調査・確認するという対策があります。

この調査自体には意義があると考えられますが、このような類似ドメインのバリエーションは無数に存在する上、攻撃者が偽メールを送信する当日に「詐称用ドメイン」の取得を行うようなケースもあります。このため、ビジネスメール詐欺への即応的な対策という観点においては、効果が限定的であると思われます。費用対効果等を考慮して検討にあたってください。

このほか、p.4 で挙げた「ビジネスメール詐欺の実態調査報告書」（JPCERT/CC）にも多くの情報と対策案が掲載されているため、参考としてください。全体的には、「多層防御」の考え方に基づき、ビジネスメール詐欺への対策のみならず、他のサイバー攻撃全般への対策として、これら複数の防御層を設けるようにしてください。

---

[14] Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion (IC3)
https://www.ic3.gov/media/2020/200406.aspx

[15] 侵害された Office 365 電子メール アカウントへの対応（マイクロソフト社）
https://docs.microsoft.com/ja-jp/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account

参考： IC3 によるビジネスメール詐欺への対策

IC3 のサイトには、次に挙げるビジネスメール詐欺への対策が掲載されています [16]。

- ウェブベースの無料電子メールアカウントは利用せず、会社用のドメイン名を取得し、そのドメイン名を利用してください。
- ソーシャルメディアや企業のウェブサイトに投稿されている、職務や組織内の階層関係、不在にする時間の情報に注意してください。
- 内密にお願いしますという要求や、迅速な行動を求める要求に対しては、ビジネスメール詐欺の攻撃ではないか疑ってください。
- 既存の財務プロセスに対して、2 段階認証プロセスの実施などを含め、次のようなセキュリティシステムや手順を検討してください。
  - 請求にかかる重要な手続きの確認のため、電話など他の通信チャネルを持つようにしてください。このとき、攻撃者からの傍受を防ぐため、なるべく早く手段を確立してください。
  - 取引による電子メールでのやりとりは、双方で電子署名を使用するようにしてください。
  - 不審なメールを受信した場合、組織内の適切な部署に報告し、そのメールを削除してください。ウイルスが含まれている可能性があるため、添付ファイルの開封や、メール内の URL などはアクセスしないでください。（IPA 注：不審なメールをシステム管理部門等が確保するまでは、削除しないことを勧めます）
  - 電子メールを相手に返信する場合、「返信」ではなく「転送」を選択し、正しいメールアドレスを入力して返信をしてください。
  - 企業の電子メールアカウントに 2 つの要素による認証を実装することを検討してください。2 つの要素は、当事者しか知りえない情報（パスワードなど）と、当事者しか持たないもの（トークンなど）を使ってください。
- 企業間のやりとりで使われていたメールアドレスの変化（個人メールアドレスへ連絡を要求されるなど）が発生した場合、そのリクエストは不正である可能性があるため、電話などによって正しい相手であるかを確認してください。
- 企業の電子メールに似た記号をもつ電子メールにフラグを立てるなどの侵入検知システムのルールを作成してください。例えば、abc_company.com という正規のメールアドレスに対して、abc-company.com のようなメールアドレスのメールが着信した場合、不正な電子メールであるとフラグを立てるものです。
- 実際の企業ドメインとは若干異なるすべてのドメインをメールフィルタなどに登録してください。
- 支払いに係る変更があった場合、組織内の 2 人以上の署名が必要など 2 段階認証を設定してください。
- 電話による相手確認を行う場合、電子メールの署名に記載されている電話番号ではなく、既知の電話番号を使用して確認してください。
- 取引相手の慣習、取引にかかる送金の遅延とその理由、支払金額などを把握してください。
- 送金先の変更などに関するすべての電子メールの要求を注意深く精査し、その要求が正規のものであるかを判断してください。

上記以外の追加情報などは、米国司法省のサイト [17]にある「Best Practices for Victim Response and Reporting of Cyber Incidents」に掲載されています。

---

[16] Business E-mail Compromise: The 3.1 Billion Dollar Scam (IC3)
https://www.ic3.gov/media/2016/160614.aspx

[17] United States Department of Justice （DOJ）
https://www.justice.gov/

6　おわりに／謝辞

ビジネスメール詐欺は、組織に多額の損失を与えうる脅威であり、その被害件数も増加傾向にあります。海外の他、国内でも複数の事件が報道されている状況ではありますが、詳しい事例の情報は、まだまだ多くありません。

この状況から、IPA では 3 回（2017 年 4 月、2018 年 8 月、2020 年 4 月）に渡ってビジネスメール詐欺の注意喚起を行いました。注意喚起後も J-CSIP の参加組織や、一般の組織・企業からビジネスメール詐欺の情報提供や相談が続いています。相談の中には、実際に偽の口座へ振り込んでしまったというものもあり、さらに広くビジネスメール詐欺の脅威を知ってもらうべく、本書および BEC 対策特設ページを公開しました。

本書では、J-CSIP の参加組織のみならず、一般の組織・企業からも情報提供をいただき、ビジネスメール詐欺の統計情報や手口について、詳しく紹介しました。また、BEC 対策特設ページでは、情報提供元の組織様からいただいた詳細な事例を紹介する資料も掲載しています。情報提供元の組織様においては、匿名とすることが前提とはいえ、このような貴重な情報の提供と開示許可をいただいていることに、深く謝意を申し上げます。

IPA は、J-CSIP を含め、国内の関連機関・組織とも連携を進めながら、情報の共有と集約を通し、サイバー攻撃に対する組織および組織群の防衛力の向上を推進していきます。

以上