J-CSIP
Initiative for Cyber Security Information sharing Partnership of Japan

ビジネスメール詐欺「BEC」に関する事例と注意喚起
（第三報）

～ 巧妙化する日本語の偽メール、継続する攻撃に引き続き警戒を ～

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

ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）

～ 巧妙化する日本語の偽メール、継続する攻撃に引き続き警戒を ～

目次

ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）

～ 巧妙化する日本語の偽メール、継続する攻撃に引き続き警戒を ～

2020 年 4 月 27 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、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「BEC」の事例と騙しの手口について紹介し、注意喚起を行うものです。

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取り扱う部門の方
- 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

IPA 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。

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がありますが、国内企業が直接狙われる事例も確認している状況となっています。

本書で紹介する、2020 年 3 月に発生した日本語のビジネスメール詐欺（事例 1）では、文章に不自然な点が少なく、また、元々は英語で行われていた攻撃が「日本語化」したものであることを示す痕跡が確認できており、日本国内の企業・組織が本格的に標的となりつつある兆候に見受けられます。また、2020 年 3 月から 4 月にかけ、新型コロナウイルス感染症（COVID-19）の話題を文章の書き出しとする英文のビジネスメール詐欺（事例 3）も複数確認しています。

ビジネスメール詐欺による攻撃は止むことなく、巧妙化が進んでいるように思われます。今後も引き続き、あらゆる国内企業・組織が攻撃対象となる可能性があり、注意が必要です。

本書は 2017 年 BEC 注意喚起、2018 年 BEC 注意喚起に続く第三報として、ビジネスメール詐欺の事例と、その騙しの手口について紹介し、改めて注意喚起を行うものです。読者の方々へは、本書を通じて、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避けていただきたいと考えています。

1.1 ビジネスメール詐欺「BEC」の概要

ビジネスメール詐欺（Business E-mail Compromise：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 2019 年 7 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 166,349 件、被害総額は約 262 億（26,201,775,589）米ドル（未遂を含む）にのぼっています [4]。1 件あたりの平均被害額は約 16 万米ドル（日本円では約 1,700 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。

---

[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] Business Email Compromise The $26 Billion Scam （IC3）
https://www.ic3.gov/media/2019/190910.aspx

また、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[5]。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。

本書では、攻撃者によって行われたビジネスメール詐欺の実事例を紹介し、その巧妙な騙しの手口について説明します。「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。実際に、IC3 に報告されている被害件数や被害額の多さは、攻撃者の巧妙な手口によって、多数の組織・企業の担当者が騙さ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取り扱う部門の担当者においては、ビジネスメール詐欺について知っていただくことが非常に重要です。攻撃者に騙されないよう、本書および 2017 年 BEC 注意喚起、2018 年 BEC 注意喚起の事例をもとに、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 5 つのタイプを紹介し、次に 2 章でこれまで J-CSIP に情報提供のあった事例や IPA が独自に入手した事例を整理し、3 つの事例を紹介します。

そして、3 章でビジネスメール詐欺への対策について説明します。

参考：国内企業が関係するビジネスメール詐欺の被害事例

2019 年 8 月に大手自動車部品メーカの欧州の子会社で外部者による虚偽の指示により約 40 億円の資金が流出したという報道がありました。

また、2019 年 9 月下旬に大手新聞社の米国子会社で経営幹部を装った攻撃者による虚偽の指示に基づいて約 2,900 万ドル（約 32 億円）が流出したという報道もありました。

それぞれ、手口などの詳細は明らかではありませんが、広く報道された、2017 年 12 月の大手航空会社が約 3 億円を超える被害があったという事例以降も、継続してビジネスメール詐欺の被害が発生している状況です。

[5] 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 5 つのタイプ

IC3[6]やトレンドマイクロ社 [7]では、ビジネスメール詐欺の手口を主に次の 5 つのタイプに分類しており、本書でも、この分類のどれに該当するかを示している箇所があります。

この 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
  - （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、偽の振り込み先に振り込ませる
- 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詐取する

---

[6] 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。

[7] 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）
http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Billion-Dollar+Scams%3A+The+Numbers+Behind+Business+Email+Compromise

2　ビジネスメール詐欺事例と手口の紹介

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から注意喚起がなされています。本書では、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において実際に発生した事例を、情報提供元の許可のもと、詳細な内容を紹介し、攻撃者が詐欺の過程で使った騙しの手口について解説します。

IPA では、2015 年から 2020 年 3 月にかけて発生したビジネスメール詐欺に関する **114 件**の情報提供を受けており、うち **17 件**で金銭的被害が確認されています。

2.1 節以降は、これら 114 件の事例の中から、2020 年以降、新たな手口や特徴がみられた 3 件の事例を紹介します。なお、いずれの事例もタイプ 2:経営者等へのなりすましに該当する事例です。

- ◆ 事例 1「日本語化」された CEO 詐称の攻撃（2020 年 3 月）
  - ➢ タイプ 2:経営者等へのなりすまし
  - ➢ 日本国内企業の CEO を詐称し、同企業のグループ企業の CEO に対して偽メール送信
  - ➢ 攻撃者は日本語のメールでやりとり
  - ➢ ほぼ同内容のメールで、海外企業へ行われたであろう英語での攻撃の痕跡も観測

- ◆ 事例 2 国内企業の CEO を詐称する日本語メールの攻撃（2020 年 1 月）
  - ➢ タイプ 2:経営者等へのなりすまし
  - ➢ 日本国内企業の CEO を詐称し、同企業内の担当者に対して偽メール送信
  - ➢ 攻撃者は日本語のメールでやりとり

- ◆ 事例 3 新型コロナウイルス感染症の話題を含めたメールによる攻撃（2020 年 3 月～4 月）
  - ➢ タイプ 2:経営者等へのなりすまし
  - ➢ 海外企業に対して行われたと思われる攻撃の痕跡
  - ➢ 攻撃者は海外企業の CEO を詐称し、同企業内の担当者に対して偽メール送信

2.1 事例 1 「日本語化」された CEO 詐称の攻撃

本事例は、日本語と英語で行われた、メールの内容が同一のビジネスメール詐欺の事例です。すなわち、元は英語で行われていた攻撃が**「日本語化」され、日本の企業へ着信した**ものと思われます。本事例の攻撃者は、英語に加え、日本語をある程度使うことができる（あるいは、十分に妥当な翻訳作業が可能な）者であり、日本を本格的に狙い始めたものであると推測しています。

2.1.1 日本語による攻撃の観測

2020 年 3 月、日本国内の企業（A 社）の複数のグループ企業の CEO に対し、A 社の CEO を騙る攻撃者から、新規の買収について協力してほしいと称する、日本語の偽のメールが送られました。メールの差出人には、本物の CEO の氏名とメールアドレスが使われていました。

本事例では、メールの受信者が不審であることに気づくことができたため、金銭的な被害は発生していません。

複数着信したうち 1 社の受信者が返信しており、これに対しては、攻撃者から 2 通目のメールが着信しました。これら 2 通のメールは、**日本語の文面には不自然な点が少なく**、日本の企業・組織を直接的に狙うビジネスメール詐欺として、危険度の高いものであると考えています。

（1）攻撃者からのメール

実際に攻撃の中でやりとりされたメールは次の通りです。

A 社の CEO を詐称した攻撃者からの最初のメールは、A 社グループ企業の CEO に対し、買収に関して弁護士から連絡があったかという内容が、日本語で書かれていました。リアリティを増すためと思われますが、実在すると思われる弁護士の名前も挙げられていました。

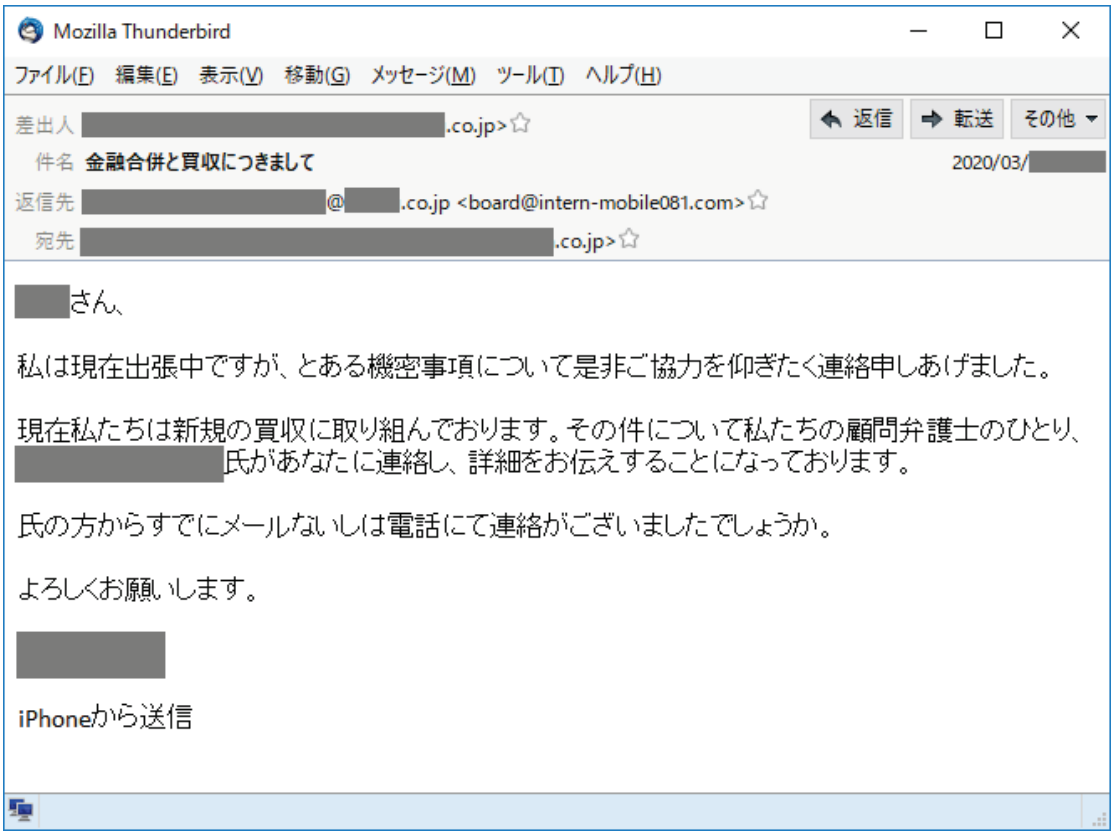

図 2-1 事例 1：攻撃者からのメール（日本語） 1通目

このメールに対し、受信したうちの 1 社が返信をしたところ、続いて次の文面のメールが攻撃者から送られてきました。内容は、外国企業の買収のため、外部の弁護士と協力して支払いを実施してほしい、このことは秘密としてほしい、というものです。このメールにさらに返信をした場合、弁護士になりすました一人二役の攻撃者から、何らかの連絡があるものと考えられます。

2 通目のメールの文面は、複雑な内容でありながら、全体的に日本語として明らかにおかしい点は見られません。ただ、言い回しの一部に、英語から翻訳したような印象を受けます。

私たちは現在、国際的な規模でより活躍すべく外国の企業の買収を進めております。
本オペレーションは市場当局の監督を受けて進められておりますが、情報の漏洩
があった場合、プロジェクトのキャンセルを強いられますので細心のご注意をお
願い申し上げます。

私たちは売却側と独占契約を締結しております。そしてその契約の条件に従い、
本日最初の支払いをしなくてはなりません。

本社からの買収を完了する間際でしたが、財政上の理由で財務アドバイザーから
別の解決策を見つけるよう提言を受けました。
そこで今回のオペレーションを支援して頂けるエージェントとして、私たちはあ
なたを当社の唯一の代理人として選択させて頂きました。

会社の利益を考慮し、私たちはあなたの支店から取引を締結することを決定しま
したのでよろしくお願いいたします。
子会社が売却者に直接支払いを行い、その合計総額は数日以内に本社から返金さ
れます。

香港の[redacted]の外部弁護士がこの取引での私たちの代理人となります。
[redacted]氏と協力して頂けるようお願いいたします。
氏が近日中にあなたに連絡をいたします。そしてすべてのプロセスをご説明しま
す。その際、私たちの会計の詳細のいくつかを彼に提供して頂きたいと存じま
す。それにより、氏は合併計画をまとめることが可能になります。

ぜひあなたのプロフェッショナリズムとご裁量にお任せしたく存ずると同時に、
このオペレーションに関して黙秘をお願いいたします。

よろしくお願いします。

図 2-2 事例 1:攻撃者からのメール(日本語) 2通目

（2） 返信先（Reply-To ヘッダ）の悪用

本事例の攻撃者は、なりすましメールを送る際、メールの差出人（From）ヘッダには、正しい A 社 CEO の名前とメールアドレスを設定しつつ、メールの返信先（Reply-To ヘッダ）には攻撃者が使用する偽のメールアドレスを設定する細工を行っていました。

Reply-To: A 社 CEO の本物の名前 メールアドレス <攻撃者のメールアドレス>

このように細工された状態では、受信者が「返信」ボタンをクリックするなどして、そのメールへの返信メールを作成すると、メールの作成画面では、差出人（From）ではなく、Reply-To ヘッダに設定された攻撃者のメールアドレスが宛先となります。ただし、メーラの画面上、表示名の部分にはＡ社 CEO の本物の名前が表示されます。攻撃者は、メールの受信者に対し、メールが本物であると錯覚させつつ、実際の返信メールは A 社 CEO には届かないようにしていたということです。

2.1.2　原文と思われる英語による攻撃

IPA で把握している他のビジネスメール詐欺の案件と比較調査したところ、ある海外企業（B 社）の財務会計部門の従業員に対し、B 社の CEO を騙る攻撃者から偽のメールが送られたと思われる案件（2019 年 11 月）について、2.1.1 に示した日本語のメールに非常に近い攻撃であることを確認しました。

実際に確認したメールは次の通りです。この事例では、偽メールが着信した B 社の従業員が攻撃者へ返信を行っており、攻撃者からは 2 通目のメールも送られてきています。英語と日本語の違いはありますが、1 通目のメールだけでなく、2 通目のメールについても、2.1.1 のメールとほぼ同じ内容です。また、本物の CEO の氏名とメールアドレスを詐称している手口、返信先（Reply-To ヘッダ）を悪用する手口等についても共通点がみられました。

このことから、これらの攻撃者は同一もしくは近い関係にあり、また、これまでは英語の文面で攻撃を行っていたところ、文面を「日本語化」させ、日本を対象として攻撃をしてきたものと推定しています。2 通目のメールについては、受信者からの返信の内容によらず同等の文面を返してきています。すなわち、パターン化した手口で、複数の対象へ攻撃を繰り返しているものと思われます。

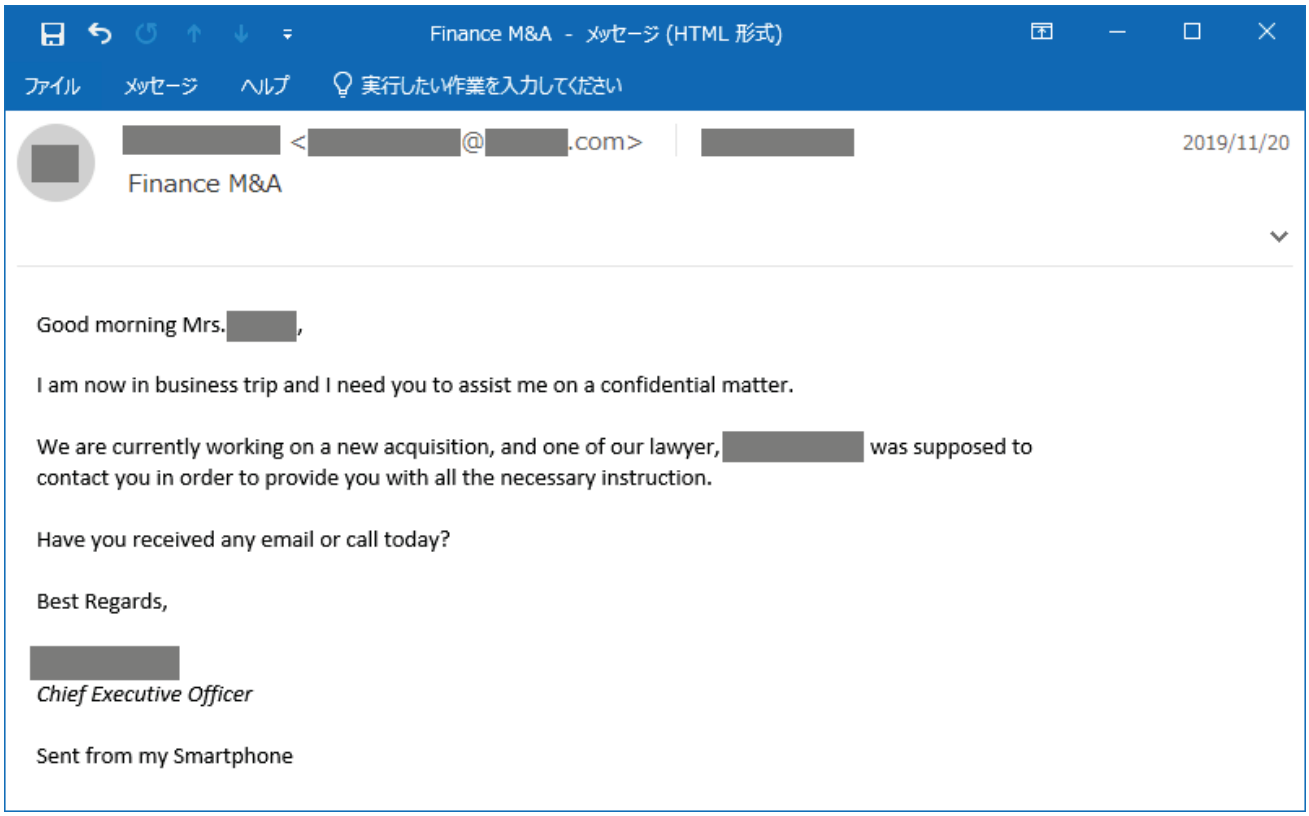

図 2-3 事例 1：攻撃者からのメール（英語）1 通目

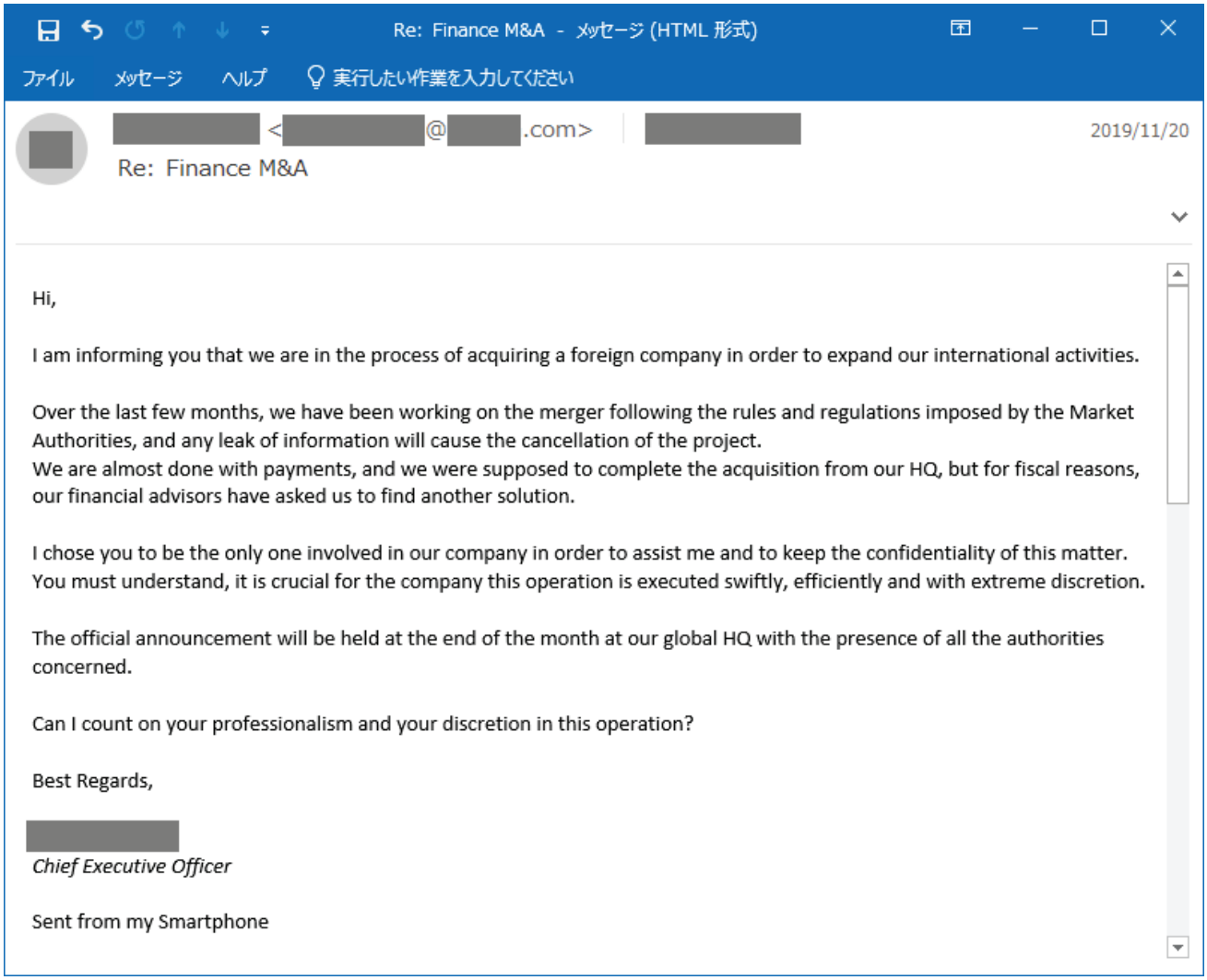

図 2-4 事例 1:攻撃者からのメール(英語) 2 通目

2.1.3　本事例の攻撃の観測状況と特徴

本件の「日本語化」されたビジネスメール詐欺の攻撃について、さらに調査を継続し、また情報提供を受けたところ、日本語の同一の文面で、2.1.1 の A 社とは別の組織へ 1 件着信したことを確認しました。また、英語（原文）の攻撃メールについては、2.1.2 の B 社とは別に、5 件のメールが別々の企業に着信した痕跡を確認しました。

これらの同種と思われる一連の攻撃メールについて、IPA では合計 8 件（日本語 2 件、英語 6 件）確認したことになります。メールの宛先は特定の業種に偏ってはおらず、「日本語化」された攻撃が、今後広く日本の組織・企業へ行われる可能性があり、注意が必要です。

本事例の補足的な情報として、8 件のメールに見られる共通した特徴について次に示します。

- メールの宛先は、国内外の複数の企業（CEO 等と思われるメールアドレス）である。
- 実在する CEO を詐称している。
- 攻撃者が使用したメールアドレスはさまざまに異なるが、命名に規則性がある。具体的には、返信先メールアドレス（Reply-To ヘッダ）で、「board」という単語がローカル名に使われており、ドメイン部分には「intern」と「mobile」という単語を組み合わせたメールアドレスが使用されている。
  - 2.1.1 の例では「board @ intern-mobile081 . com」というメールアドレス。
- 英語と日本語の差はあるが、件名や本文はほぼ同じ内容である。最初に着信するメール（1 通目）の本文は 5 行～10 行程度の簡素なもので、「出張中であるが、企業買収について協力してほしいことがある」といった内容が書かれている。
- メールの着信時期は、確認できている限り、2019 年 11 月 20 日から 2020 年 3 月 25 日である。
- メールの送信に「SendGrid」というメールサービスを使用している。SendGrid が提供する機能として、受信者がメールを開封したことを送信者が追跡できる仕掛け（ウェブビーコン）をメールに埋め込むことが可能であり、実際に、SendGrid のビーコンと思われる HTML タグが一部のメール検体で確認できている。
  - 攻撃者が意図的に開封状況の追跡を行っているものであるか不明だが、この点も、攻撃手口の巧妙化を示している可能性がある。

2.2 事例 2 国内企業の CEO を詐称する日本語メールの攻撃

2020 年 1 月、日本国内の企業(A 社)の従業員に対し、A 社の役員を騙る攻撃者から、緊急の送金依頼を装うビジネスメール詐欺が試みられました。メールの差出人は、本物の A 社役員の氏名とメールアドレスが使われました。これは、ビジネスメール詐欺の 5 つのタイプのうち、「タイプ 2:経営者等へのなりすまし」に該当します。

本事例では、A 社の担当者がやり取りの途中で不審であることに気づいたため、金銭的な被害は発生していません。

本事例の特徴として、**攻撃者から送られてきたメールは日本語**で書かれており、**攻撃者が送金先として指定した銀行口座も日本国内のもの**であった点が挙げられます。なお、いずれのメールでも、日本語に不自然な点が見られました。

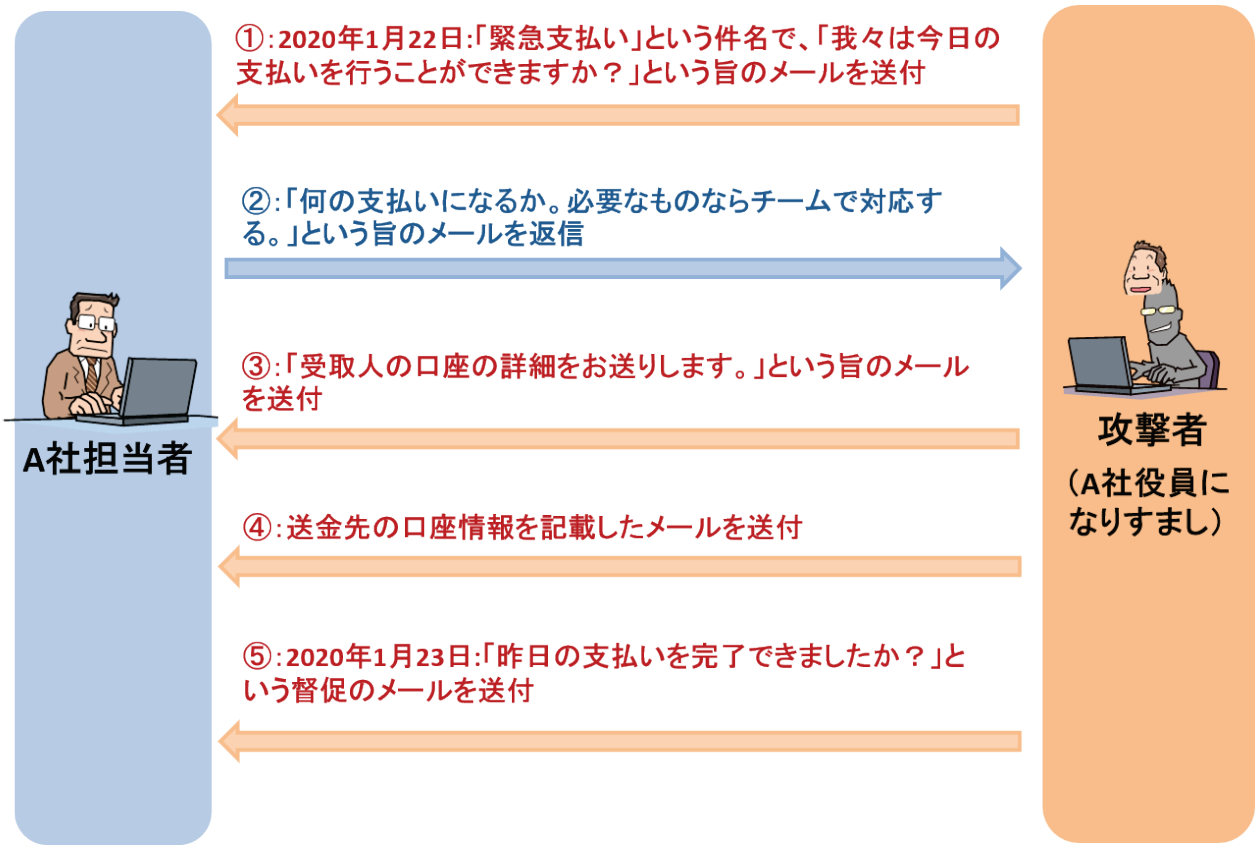

図 2-5 攻撃者とのやりとり

2020 年 1 月 22 日、攻撃者は A 社の役員になりすまし、今日支払いを行うことができるかという内容のメールを送り付けてきました。これに対し、A 社の担当者は、必要であればチームで支払いについて対応するという旨を攻撃者に返信しています。A 社担当者からメールを返信した約 20 分後、攻撃者から口座の情報を送るというメールが着信し、さらにその約 2 時間 30 分後、銀行の口座情報が記載されたメールが着信しました。また、その翌日にも、攻撃者から昨日の支払いは完了したかという督促のメールが送られてきました。

本事例でメールが着信した A 社の担当者は、企業内の金銭を取り扱うような、ビジネスメール詐欺の攻撃対象になりうる人物であったとのことです。攻撃者が、どのようにしてこの担当者を標的に選定できたのかは不明です。

（1） 攻撃者からのメール

実際に攻撃の中でやりとりされたメールの内容については次の通りです。

攻撃者からの最初のメール（図 2-6）では、A 社の担当者に対して、今日の支払いが可能かという内容が金額とともに日本語で書かれていました。

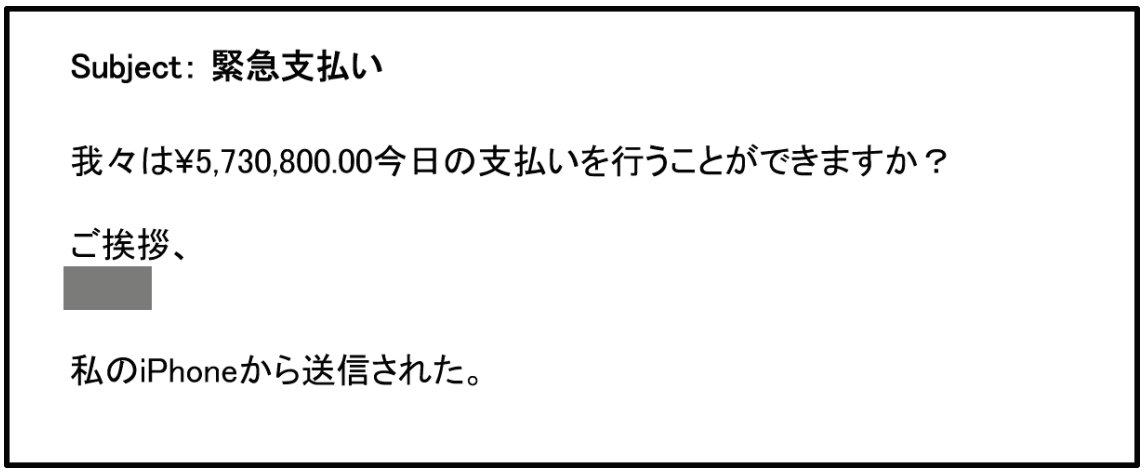

図 2-6 攻撃者からのメール（1 通目）

さらに、このメールに対して、A 社の担当者が返信した後、攻撃者から口座情報を送るというメールが着信し、続いて銀行口座の情報が次のような内容で送られてきました（図 2-7）。

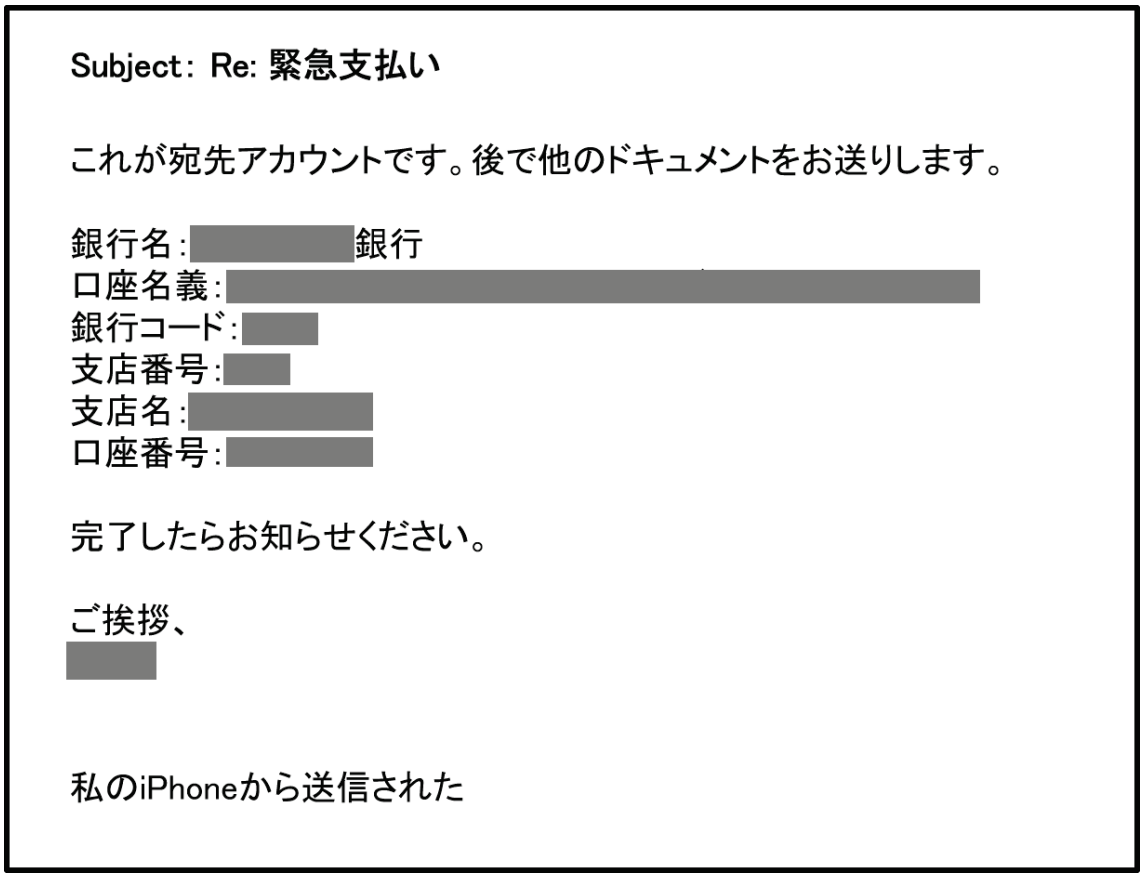

図 2-7 攻撃者からのメール（3 通目）

（2） 返信先（Reply-To ヘッダ）の悪用

本事例の攻撃者は、なりすましメールを送る際、メールの差出人（From）ヘッダには、正しい A 社役員の名前とメールアドレスを設定しつつ、メールの返信先（Reply-To ヘッダ）には攻撃者が使用するフリーメールアドレスを設定する細工を行っていました。

Reply-To: A 社役員の本物の表示名 〈攻撃者のメールアドレス〉

このように細工された状態では、受信者が「返信」ボタンをクリックするなどして、そのメールへの返信メールを作成すると、メールの作成画面では、差出人（From）ではなく、Reply-To ヘッダに設定された攻撃者のメールアドレスが宛先となります。ただし、メーラの画面上、表示名の部分には A 社役員の本物の名前が表示されます。攻撃者は、メールの受信者に対し、メールが本物であると錯覚させつつ、実際の返信メールは A 社役員には届かないようにしていたということです。

2.3 事例 3 新型コロナウイルス感染症の話題を含めたメールによる攻撃

2020 年 3 月、新型コロナウイルス感染症（COVID-19）に関する話題をメール本文中に含んだ、海外の企業へ着信したと考えられるビジネスメール詐欺のメールを入手しました。IPA で類似のメールがないか調査を行っていたところ、2020 年 4 月以降も同種のメールが別の海外の企業へ着信していると思われる痕跡を確認し、J-CSIP の参加組織からも、類似のメールが実際に着信したという情報提供を受けています。

文面やメールヘッダ等の特徴から、この一連のビジネスメール詐欺は、同一の攻撃者または攻撃グループによるものと推定しています。また、着信している企業・組織を確認した結果、特定の組織や業種を狙うものではなく、複数の業種に対して試みられているものと推測しています。

攻撃メールの本文では、新型コロナウイルス感染症の話題を文章の書き出しとして使用した上で、「外国企業との機密の案件で助けが必要だ」といった内容が書かれています。また、メールの差出人は実在すると考えられる CEO の名前やメールアドレスが使われています。このメールに返信をした場合、何らかの口実とともに、攻撃者の口座への送金依頼に話が進むものと思われます。

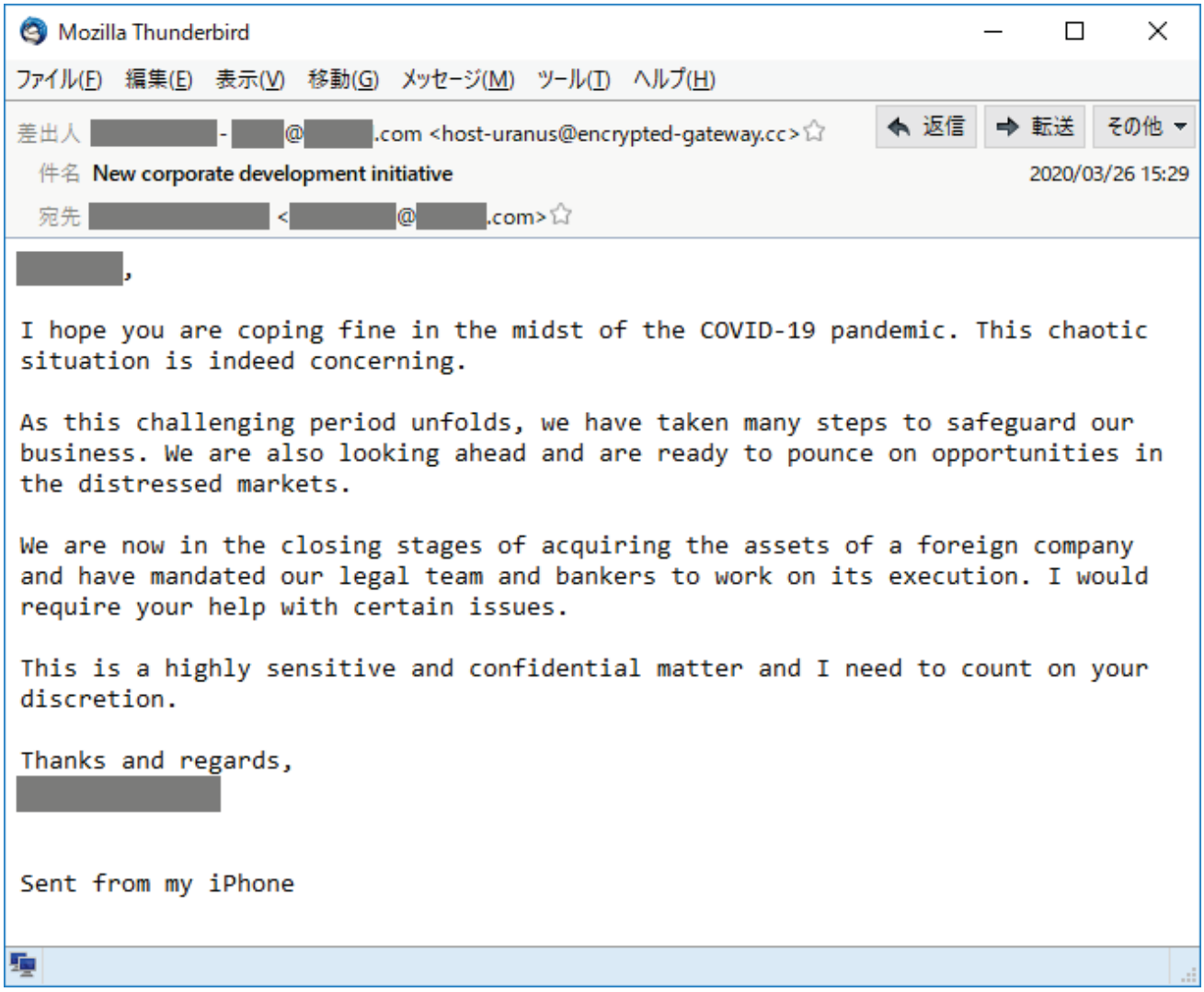

図 2-8 攻撃メールの例（2020 年 3 月に着信したメール）

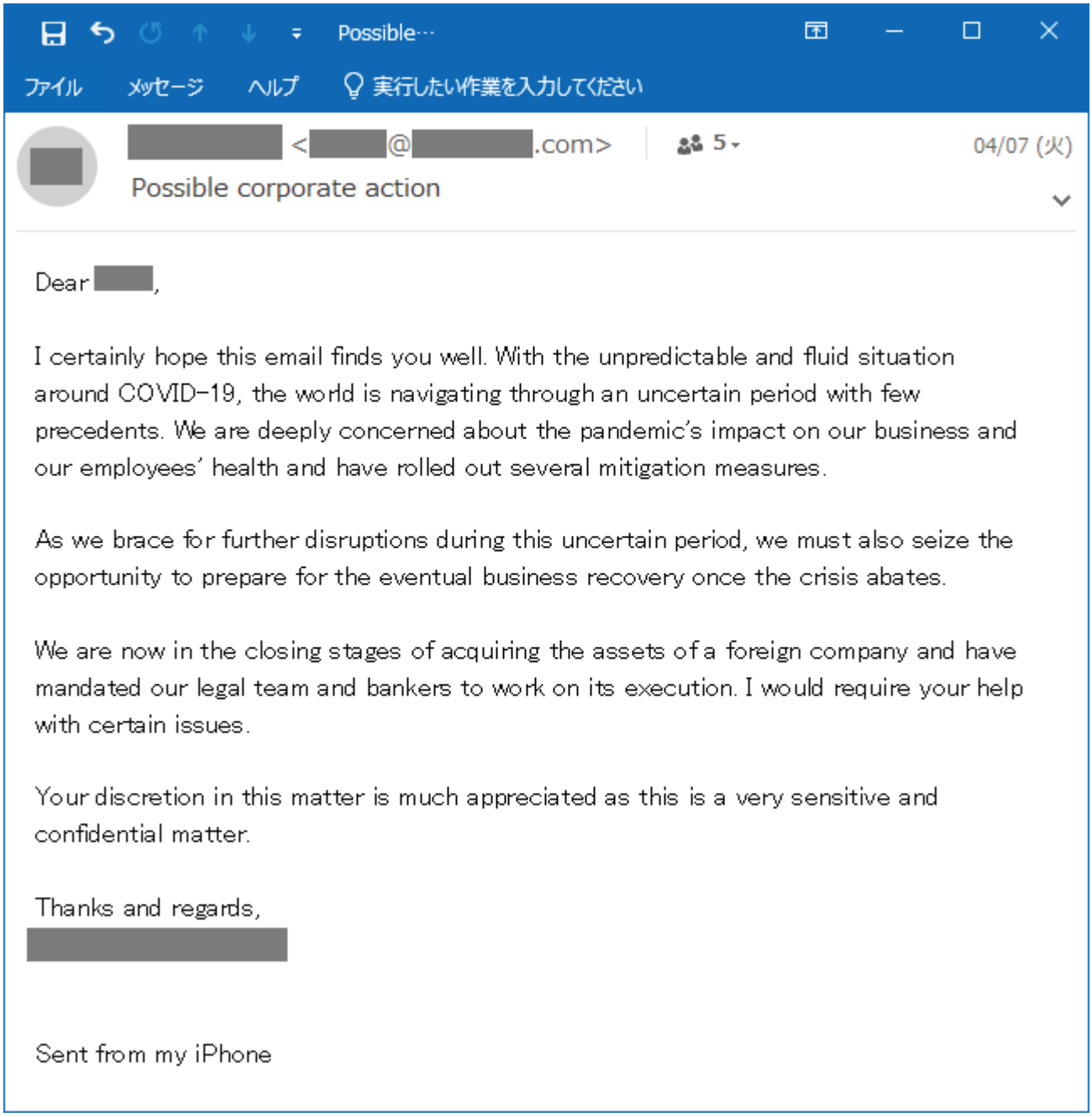

図 2-9 攻撃メールの例（2020 年 4 月に着信したメール）

更に、これらのメールについては、IPA が公開している「サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2019 年 10 月～12 月]」のレポートに掲載した、より過去から確認している、複数組織に対する CEO を詐称する一連の攻撃とも、一部特徴が重複しています。すなわち、同一の攻撃者が、攻撃手口に新型コロナウイルス感染症の話題を取り込んだものであろうと推測しています [8]。

[8] サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2019 年 10 月～12 月] （IPA）
https://www.ipa.go.jp/files/000080133.pdf

企業・組織が相対している敵は「偽メール」ではなく、そのメールを送り付けている攻撃者（人間）であり、その攻撃者は手口をアップデートしながら、複数の組織へ向け執拗に攻撃を繰り返しています。ここで紹介したメールが偽物であると見破ることが容易に思えたとしても、攻撃者を侮るべきではありません。

参考：新型コロナウイルス感染症の拡大を悪用するビジネスメール詐欺

IC3 が 2020 年 4 月 1 日に公開した注意喚起 [9]、および FBI が 2020 年 4 月 6 日に公開したプレスリリース [10]において、新型コロナウイルス感染症が拡大している状況を悪用するビジネスメール詐欺について、注意が呼びかけられています。

具体的には、次に示す手口の例が挙げられています。

- 取引先になりすました攻撃者が、「新型コロナウイルス感染症（による影響）のため、通常の取引手続きではない方法で支払ってほしい」と要求してくる。
- 金融機関が、ある企業の CEO と名乗る者からメールを受信。その者は、「従前から 100 万ドルの送金を予定していたが、"新型コロナウイルスの拡大に伴う検疫処置と警戒のため" 受取人口座の変更と、支払いの前倒しをしてほしい」と要求。そのメールアドレスは、本物の CEO のメールアドレスから 1 文字だけ変更されたものであった。
- ある銀行の取引先が、その取引先の中国の顧客と名乗る者からメールを受信。その顧客は、「全ての請求書の支払い先について、通常の銀行口座が "コロナウイルス監査" により使用できなくなったため、異なる銀行へ変更してほしい」と要求。被害者は、詐欺だと気付くまで、いくつかの送金を行ってしまった。

現在、あらゆる企業・組織が困難な状況にあり、予定外の対応も多く発生している状況ではありますが、この状況を悪用するような口実に騙されないよう、注意が必要です。

[9] Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments (IC3) https://www.ic3.gov/media/2020/200401.aspx

[10] FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic (FBI) https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

3　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、何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、例えば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、何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。

クラウドサービスに特有の対策については IC3 の注意喚起 [11]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 [12]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.3 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。

---

[11] 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

[12] 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 [13]。

- 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 [14]にある「Best Practices for Victim Response and Reporting of Cyber Incidents」に掲載されています。

---

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

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

4　おわりに／謝辞

ビジネスメール詐欺は、攻撃が成功してしまうと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。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。

この状況を受け、IPA では 2 回（2017 年 4 月、2018 年 8 月）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。今回、巧妙化した日本語によるビジネスメール詐欺の事例や新型コロナウイルス感染症を話題として用いるメール等を確認したことで、ビジネスメール詐欺の脅威が継続していることを踏まえ、再び注意喚起を行うこととしました。

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、実際のビジネスメール詐欺の事例とその手口について、情報提供元から開示許可をいただいた上で、詳しく紹介しました。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、深く謝意を表します。

J-CSIP は、今後も情報共有の運用を着実に行い、また、参加組織の拡大、情報共有の効率向上等を図っていくとともに、情報の集約と横断分析によって得られる情報など、共有する情報の拡充を進めていきます。そして、J-CSIP 外の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