サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 4 月～6 月]

2023 年 8 月 22 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

サイバー情報共有イニシアティブ（J-CSIP）[1]について、2023 年 6 月末時点の運用体制と、2023 年 4 月～6 月期（以下、本四半期）の運用状況を報告する。1 章、2 章では本四半期の全体状況を、3 章では本四半期で把握・分析した特徴的な攻撃事例を、4 章では IPA で観測している 2 つの CEO 詐欺の続報について解説する。

目次

[1] IPA が情報ハブ（集約点）となり、サイバー攻撃等に関する情報を参加組織間で共有する取り組み。
https://www.ipa.go.jp/security/j-csip/about.html

1　運用体制

本四半期では、参加組織の増減はなく、全体で 13 業界 279 組織[2]＋2 情報連携体制（医療業界 4 団体およびその会員約 5,500 組織、水道関連事業者等 9 組織）の体制となっている（図 1）。

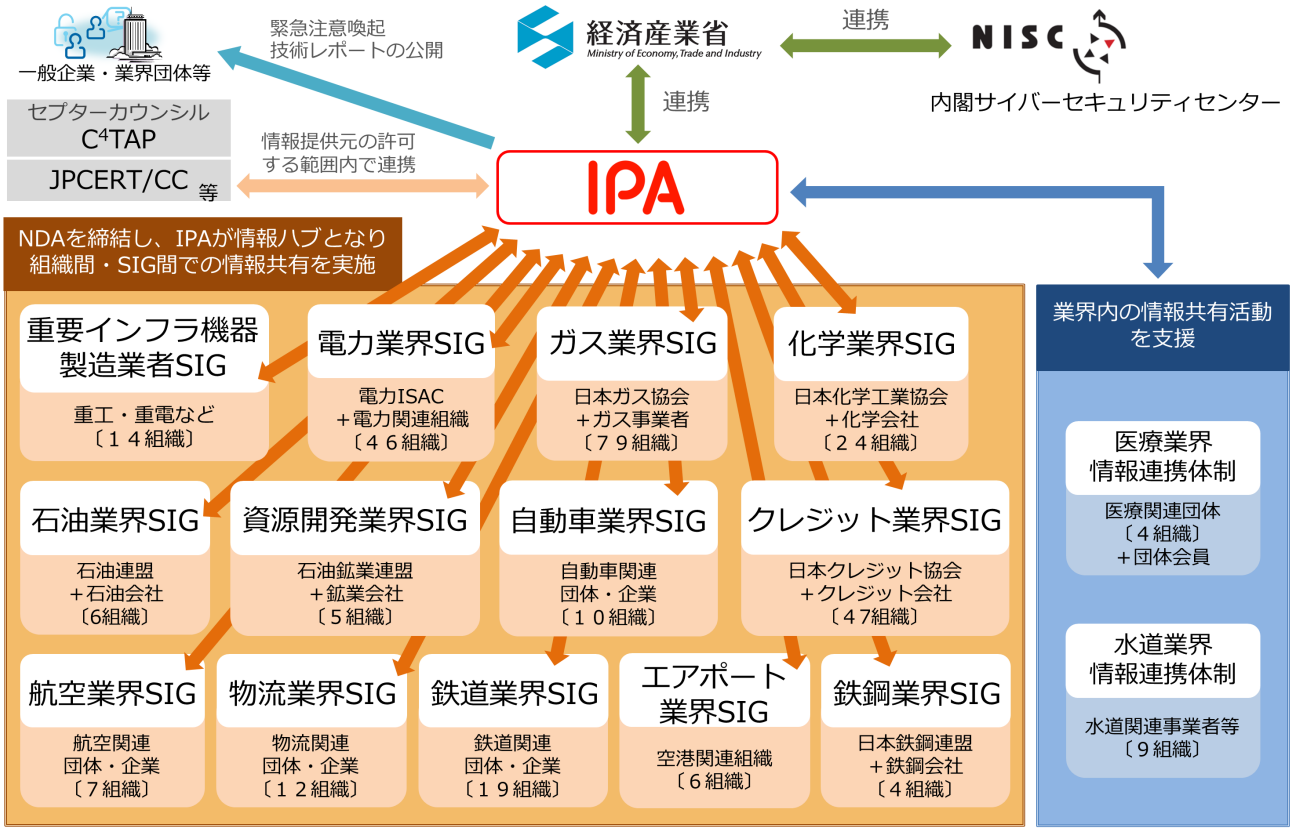

図 1 J-CSIP の体制図

[2] 複数業界に関係する組織が、複数の SIG に所属するケースもある。ここでは延べ数としている。

2　運用状況（2023 年 4 月～6 月）

2023 年 4 月～6 月の運用状況について、2.1 節で情報提供・情報共有の実施件数を、2.2 節と 2.3 節で参加組織から提供された情報や IPA が収集し共有した情報を報告する。

2.1 情報提供・情報共有の実施件数

2023 年 4 月～6 月に、J-CSIP 参加組織から IPA に対し、サイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の情報提供が行われた件数と、それらの情報をもとに IPA から J-CSIP 参加組織へ情報共有を実施した件数（6 月末時点、13 の SIG、全 279 参加組織と、2 つの情報連携体制での合算）を、表 1 に示す。

表 1 情報提供および情報共有の状況

項番	項目	2022 年		2023 年	
		7 月～9 月	10 月～12 月	1 月～3 月	**4 月～6 月**
1	IPA への情報提供件数	22 件	26 件	59 件	**26 件**
2	参加組織への情報共有実施件数 ※1	38 件	25 件	22 件	**23 件※2**

※1 同等の攻撃情報（不審メール等）が複数情報提供された際に情報共有を 1 件に集約して配付することや、広く無差別にばらまかれたウイルスメール等、情報共有対象としない場合があるため、情報提供件数と情報共有実施件数には差が生じる。

※2 IPA が独自に入手した情報で、J-CSIP 参加組織へ情報共有を行ったもの **12 件**を含む。

本四半期は情報提供件数が **26 件**であり、うち標的型攻撃に関する情報（攻撃メールや検体等）とみなしたものは **3 件**であった。

2.2 参加組織から提供された情報

参加組織からは、次にあげるような情報が IPA へ提供された。

- 電話を併用したビジネスメール詐欺（BEC）に関する情報提供があった。情報提供元の会長と専務になりすました攻撃者から、海外関連会社の社長に対して、偽の依頼に関するメールと電話があったというものであった。海外関連会社の社長が、攻撃者との電話の中で、相手が本人ではないことに気づいたため、金銭的被害は生じなかった。事案発覚の経緯やメールの内容・電話の内容について、3.1 節で述べる。

- 偽造文書を使用した BEC に関する情報提供があった。情報提供元と取引先とのメールが盗み見られ、それを悪用した偽のメールが、攻撃者から取引先に送られたというものである。偽造文書には、日本の税制変更により損失が発生するため、銀行の支払い先口座を変更することを指示するような内容が記載されていた。事案発覚の経緯や、メール・偽造文書の内容について、3.2 節で述べる。

- 情報提供元が管理しているウェブサイトに対する不審なアクセスを WAF（Web Application Firewall）により検知したという情報提供があった。当該アクセスは、ウェブサイトに特定の脆弱性がないかを調査するためのスキャン行為と考えられるものであった。なお、当該アクセスを受けたウェブサイトは、海外のクラウドサーバー上で現地向けに用意したものであった。当該内容を参加組織へ情報共有したとこ

ろ、別の参加組織においても同様のアクセスが確認されており、広く脆弱性のあるサーバーを狙った攻撃またはその準備行為であると考えられる。
企業においては、自社のウェブサイト以外にも関連会社や事業・製品・イベント関連等、多数のウェブサイトを運用している場合もあるが、すべてのウェブサイトにおいて不要なサービスの停止やポートの閉塞、利用しているアプリケーションのバージョンや脆弱性有無の確認等、セキュリティ点検を漏れなく行ってほしい。

- 情報提供元の海外関連会社（A 社）の従業員になりすました攻撃者から、A 社とは異なる国の関連会社（B 社）の従業員に対して、詐欺目的と思われるメールと電話があったという情報提供を受けた。攻撃者からのメールと電話は、いずれも出張用の旅券を手配するため、B 社で利用する旅行代理店を紹介してほしいと称する内容であった。攻撃者の最終的な目的は不明だが、旅行代理店から航空券を詐取し、現金化することを企図したものであったと考えられる。攻撃は複数の国の関連会社で確認されたが、いずれの組織においても金銭的被害は生じていなかった。標的組織の従業員に対して、直接、金銭の振り込みを要求するのではなく、本件のように旅行代理店から航空券を詐取するというような換金目的の詐欺攻撃にも注意が必要である。このような場合においても、他の BEC と同様に、普段とは異なるメールや電話を受けた際には社内で相談・連絡し、情報共有をするといった対策が重要である。

- 情報提供元の組織を騙るフィッシングメールおよびフィッシングサイトに関する情報提供を受けた。情報提供元に対して、当該フィッシングメールに関する問い合わせが複数あったことから、当該企業を騙るフィッシング行為の存在が発覚した。その後、情報提供元では、フィッシング行為への注意喚起を行った。当該フィッシングサイトには、情報提供元の組織が使用するロゴを一部改変したものが悪用されていた。また、HTML の frame 要素を悪用し、情報提供元の正規ウェブサイトのコンテンツを読み込むことで、フィッシングサイトを正規のウェブサイトに見せかける細工（クリックジャッキング攻撃）がされていた。なお、当該フィッシングサイトの IP アドレスには、別の組織の詐称用ドメインが紐づいていたことから、複数の企業に対して同様の手口での攻撃が行われていると推測される。
本件のようなフィッシング行為を防ぐこと自体は難しいが、問い合わせ窓口等へ連絡があった場合には、軽視することなく事実確認を行い、必要ならば自社のウェブサイト等を通じて注意喚起を行ってほしい。これにより、フィッシングメールを受信した一般利用者が、フィッシングメールかどうかを判断する手助けになる場合もあり、被害を低減できる。また、ウェブサイトにおいては、IPA が公開している「安全なウェブサイトを作り方 [3]」を参考にしていただき、外部ドメインからの frame 要素や iframe 要素による読み込みを制限する設定 [4]等を検討していただきたい。

---

[3] IPA 安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity/index.html
[4] IPA 安全なウェブサイトの作り方 － 1.9 クリックジャッキング
https://www.ipa.go.jp/security/vuln/websecurity/clickjacking.html

2.3 IPA が収集し共有した情報

IPA では公開情報を含めサイバー攻撃の情報を収集し、必要に応じてこれらの情報を参加組織へ情報共有するといった活動を行っている。本四半期に IPA が収集し共有を行った情報について、その一部を報告する。

- 次の 2 つの BEC について、本四半期においても引き続き、参加組織からの情報提供や、IPA の独自調査による類似メール検体を複数入手している。

(1) 複数組織へ行われた CEO を詐称する一連の攻撃
2019 年 7 月以降、継続して観測しており、国内外の複数の組織を対象として行われている痕跡を確認している。メールの件名や内容は時期ごとに変化が見られるが、メールのヘッダー情報に類似する点があるため、一連の攻撃は同一の攻撃者によるものと推測している。
「3.1 海外関連会社を狙った電話を併用する攻撃」で紹介する事例も、この攻撃の一つであると判断している。

(2)「日本語化(多言語化)」された CEO 詐欺の攻撃
2019 年 11 月以降、継続して観測しており、国内外の複数の組織を対象として行われている痕跡を確認している。メールの件名や内容は変化が見られるが、M&A 案件への対応を依頼するといった同じようなメール内容であり、メールのヘッダー情報や、「SendGrid」「SMTP2GO」「Sendinblue」「Fastmail」「Mailgun」というメールサービスを使用している等、類似する点がみられる。そのため、一連の攻撃は同一の攻撃者によるものと推測している

これまで入手したメール件数やメールの特徴などの詳細について、4 章で述べる。

3　ビジネスメール詐欺（BEC）の攻撃事例

本四半期では、J-CSIP 参加組織から 3 件のビジネスメール詐欺（BEC）について情報提供があった。2 件については、IPA で継続的に観測している「複数組織へ行われた CEO を詐称する一連の攻撃」とみられるものであり、そのうち 1 件については電話を併用する攻撃であった。もう 1 件については、偽造文書を使い取引先に対して支払い先の口座を変更することを企図した BEC であった。

本章では、電話を併用する攻撃と偽造文書を使う攻撃の事例について詳しく説明する。

3.1 海外関連会社を狙った電話を併用する攻撃

本事例は、2023 年 5 月、J-CSIP の参加組織(以下、A 社)の海外関連会社（以下、B 社）の社長に対し、A 社の会長および専務になりすました攻撃者から、偽のメールと電話が着信したものである。

本件においては、攻撃者からの電話を受けた B 社社長がなりすましに気付いたことで、金銭的な被害は発生しなかった。

なお、A 社では本件とほぼ同時期に、海外の商工会より、日系企業を狙う本件と類似した手口の BEC について注意喚起を受けていた。このことから、同時期に日系企業を対象とした BEC が複数行われていた可能性も考えられる。今後も同様の攻撃が発生する恐れもあり、引き続き注意が必要と思われる。

攻撃者とのやりとり

攻撃者とのやりとりの概要を図 2 に示す。

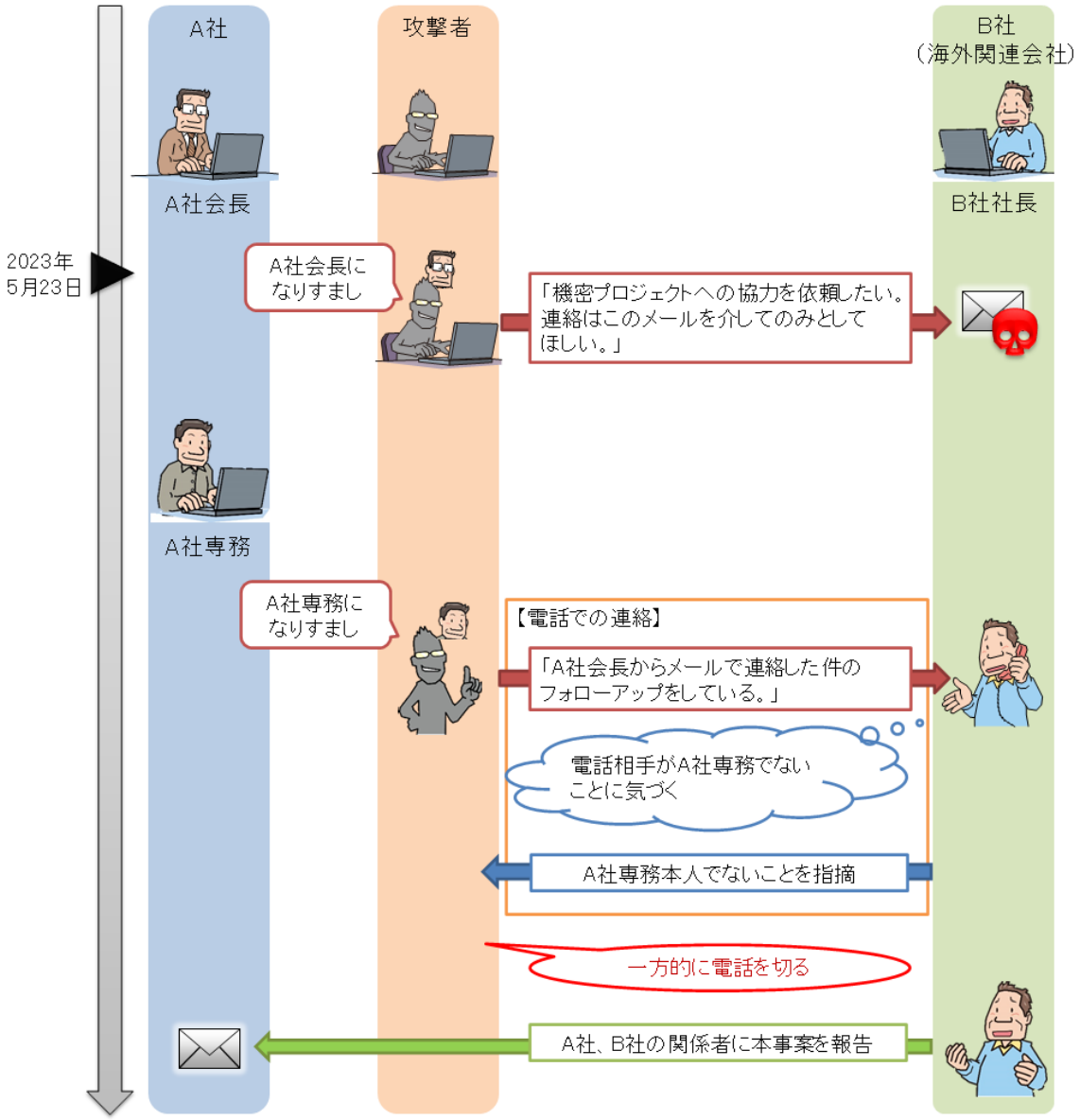

図 2 攻撃者とのやりとり(2023 年 5 月)

本件において、攻撃者が B 社社長に対して試みたやりとりは、メールと電話それぞれ 1 件ずつであった。なお、攻撃者がなりすました A 社会長と A 社専務はいずれも日本人であり、B 社社長は外国人であった。

攻撃者からのメールの内容について

攻撃者から送られたメールを図 3 に示す。件名と本文は英語で記載されていた。

図 3 攻撃者から送られたメール

攻撃者からのメールは、機密性の高いプロジェクトへの協力を依頼したいという内容であり、文中では実在する会計・法律事務所の従業員の名前も挙げられていた。

なお、本メールに用いられた文面には、4.1 節にて後述する「複数組織へ行われた CEO を詐称する一連の攻撃」として IPA が複数観測しているメール[5]とほぼ同一のものが用いられていた。そのことから、本件についても一連の攻撃のうちの一つであることと推測している。

[5] IPA にて確認した類似メールには、宛先に A 社とは別の J-CSIP 参加組織の海外関係企業が設定されたものも存在した。そのため、IPA では、当該の J-CSIP 参加組織に情報共有を実施した。

偽のメールアドレスの使用

攻撃者はメールの差出人が A 社会長であるかのように偽装するため、差出人(From)に表示される表示名(スクリーンネーム)に A 社会長の氏名(英語表記)を、メールアドレスには A 社会長のメールアドレスに似た、実在しないメールアドレスを設定していた。

設定されたメールアドレスは、図 4 に示すように、ドメイン部が A 社で使用しているメールアドレスと同一であり、ローカル部は A 社会長の氏名を含むものであった。

■なりすまされた人物の名前を「山田 太郎(Yamada Taro)」さんとした場合の例

本物のメールアドレス表示　：　Taro Yamada < t.yamada @ [A社の正規ドメイン] >

偽のメールアドレス表示　：　Taro Yamada < **taro**_yamada @ [A社の正規ドメイン] >

→ 氏名からローカル部への変換規則が実際のA社のものと異なる

図 4 攻撃者によるメールアドレスの偽装

差出人の表示名が偽装された場合、図 5 に示すように、受信者側の環境次第では、実際の差出人のメールアドレスが表示されないことから、表示された人物が実際の差出人であると騙されてしまう恐れがある。

図 5 アドレス帳での差出人の表示例

なお、IPA で確認した本件と類似の攻撃メールでは、メールの返信先(Reply-To)に、差出人(From)と異なるメールアドレス(攻撃者のものと思われる)が設定されていた。本件の攻撃メールにおいても、同様の手口で返信先に攻撃者のメールアドレスが設定されていた可能性があるが、情報提供の範囲外のため不明である。

攻撃者からの電話

A 社会長を詐称したメールの後、当日中に、A 社専務になりすました攻撃者から、「A 社会長からメールで連絡した件のフォローアップをしている」と称した電話が B 社社長に着信した。このとき、発信元電話番号は A 社の代表番号に偽装されていた。会話内容（言語含む）については、情報提供の範囲外であり詳細不明ながら、何らかの理由で B 社社長が電話の相手は A 社専務でないことに気付き、その旨を攻撃者に伝えたところ、電話を一方的に切られたとのことである。

この電話では、攻撃者は A 社専務の声を模倣していたとのことであった。昨今では、ディープフェイクで生成した音声を詐欺に悪用するという公開情報もあるため、本件でも同様の手口が用いられていた可能性が考えられる。

その後の対応

以降、攻撃者からのコンタクトは確認されず、金銭的な被害には至らなかった。B 社社長はその後、関係者に本件の報告を行うことで攻撃事案を周知したとのことであった。

本事例のまとめ

本件は、メールと電話を併用したものであり、更に発信者番号の偽装や本人の声の模倣といった複数の騙しの手口が用いられていた。幸いにも、標的とされた B 社社長が電話の相手を偽物と気付いたことで、金銭的な被害には至らなかったが、今後も同様の手口には注意が必要と考えられる。

これまでも J-CSIP の運用状況レポートで度々紹介してきたとおり、BEC では標的を騙すために様々な手法が駆使される。メールや電話の内容に少しでも不審な点があれば、信頼できる方法で入手した連絡先に折り返しの電話で事実確認を行うことを徹底していただきたい。また、関係者を騙る不審な電話を受けた際には、本人しか知らない質問をする等、電話の相手が確かに本人であるかの確認を行っていただきたい。

3.2 偽造文書を使い海外取引先を狙った攻撃

本事例は、2023 年 5 月、J-CSIP の参加組織（以下、A 社）の海外取引先（以下、B 社）の経理担当者に対し、A 社の担当者になりすました攻撃者から、取引における支払先銀行口座の変更を依頼する偽のメールが着信したものである。

偽のメールには、A 社担当者が B 社経理担当者に送付した正規メールの内容が流用されていたほか、A 社と口座変更先の銀行、それぞれが発行した正規の文書のように見せかけた偽造文書が添付されていた。攻撃者はある程度の期間、何らかの方法で正規メールを盗み見ていたと思われる。

本件では、攻撃者からの偽のメールを受信したＢ社経理担当者が当該メールを不審に思い、Ａ社担当者に問い合わせたところ、詐欺であることが発覚したため、金銭的な被害は発生しなかった。

攻撃者とのやりとり

攻撃者とのやりとりの概要を図 6 に示す。

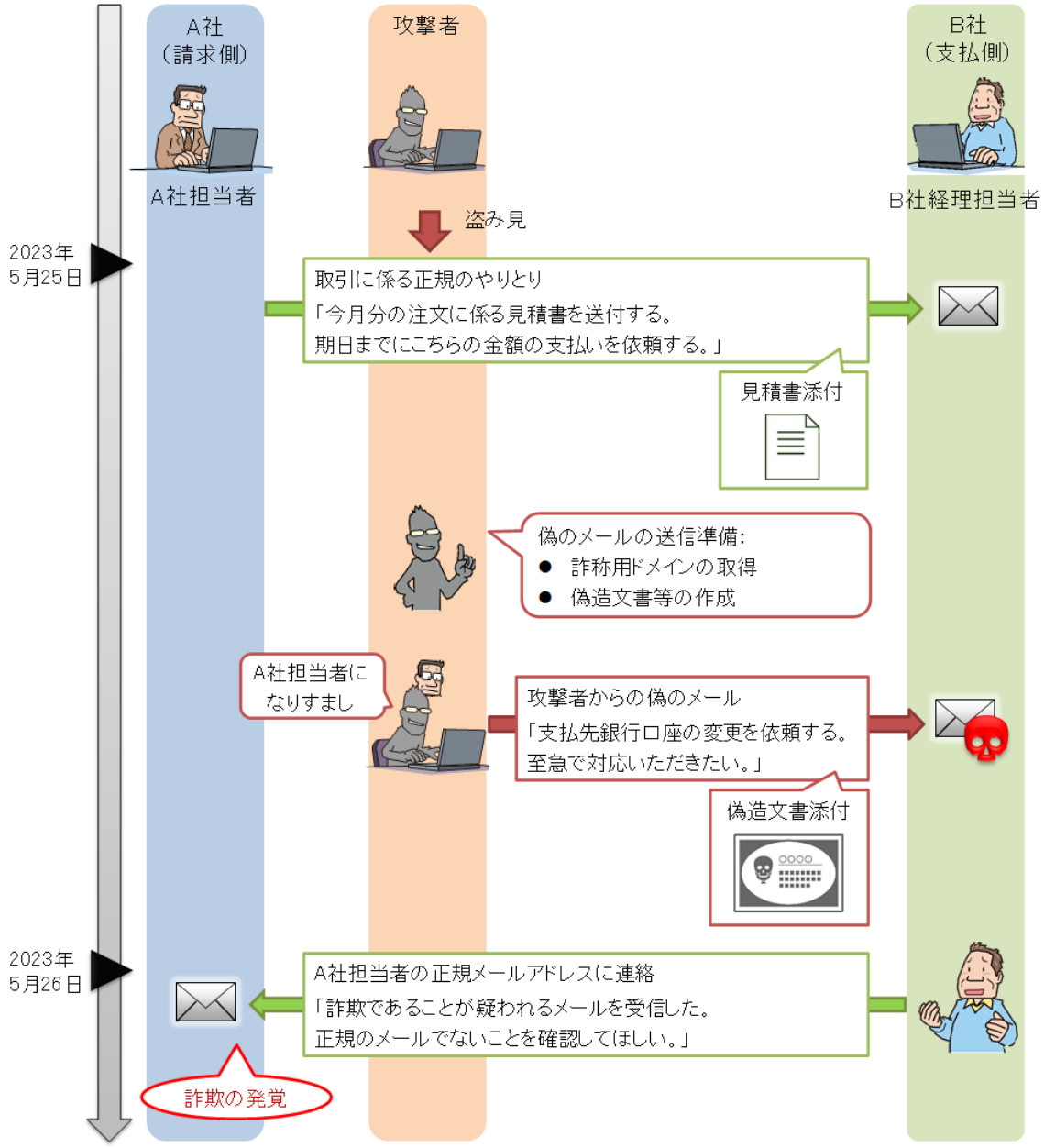

図 6 攻撃者とのやりとり(2023 年 5 月)

本件において、攻撃者が B 社経理担当者に対して試みたやりとりはメール 1 件のみであり、電話等による連絡はなかった。なお、攻撃者がなりすました A 社担当者は日本人であり、B 社経理担当者は外国人であった。

攻撃者から送られた偽のメールには、過去の正規メールの内容が流用されており、何らかの方法で正規メールのやりとりが盗み見られていたことが推測される。

攻撃者から送られた偽のメールの内容

攻撃者から送られた偽のメールを図 7 に示す。メールは英語で記載されていた。

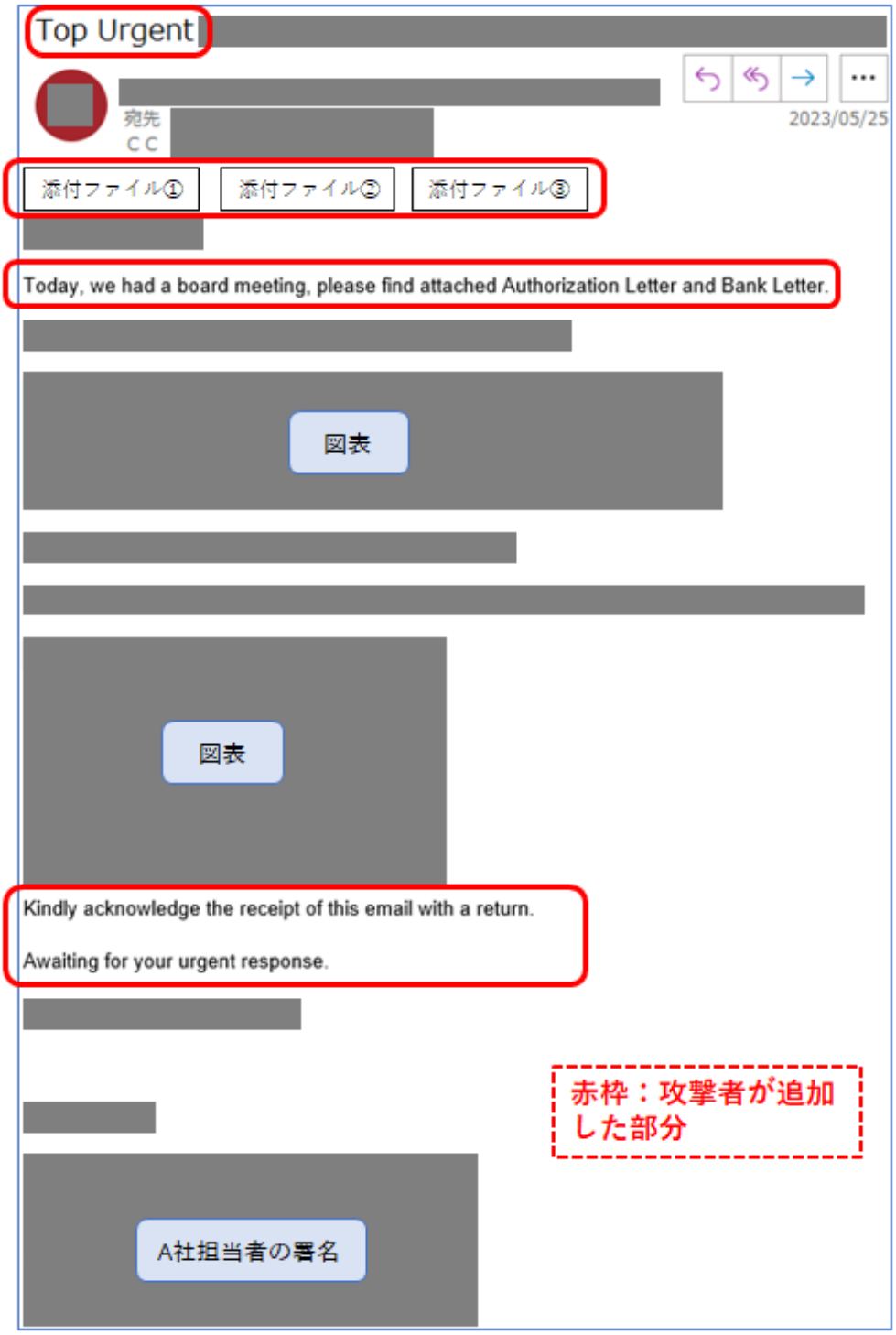

図 7 攻撃者から送られた偽のメール

攻撃者から送られた偽のメールには、当日、A 社担当者が B 社経理担当者に宛てて送信した、取引に係る正規メールの文面や図表が流用されていた。攻撃者は、メールの内容を流用しつつ、至急の対応を求める件名・本文や、添付資料の内容確認を依頼する本文を追記し送付していた。

攻撃者が偽のメールに添付した偽造文書等

偽のメールには 3 点のファイル（PDF ファイル 2 点、ZIP ファイル 1 点）が添付されており、そのうち 2 点の PDF ファイルは攻撃者によって偽造された文書であった。

- PDF ファイル（1）
  A 社による発行を装い、振込先口座の変更を依頼する偽造文書。何らかの手段で入手した A 社の正規文書を模倣して作成したことが推測されるが、実際の様式とは異なる点が複数存在していた。
- PDF ファイル（2）
  口座変更先の銀行に、A 社の口座が開設されていることを説明する偽造文書。口座変更先の銀行から、A 社からの依頼に基づいて発行されたように装っていた。
- ZIP ファイル
  PDF ファイル 1 点が格納されている、パスワードで暗号化された ZIP ファイル。拡張子は「zip」から一文字違いのものに変更されていた。格納されている PDF ファイルの内容は、解凍パスワードが不明のため確認できなかった。しかし、当該 PDF ファイルは、過去 A 社から B 社に送付した見積書のファイルと、ファイル名およびファイルサイズが一致したことから、A 社が発行した正規の見積書のファイルであった可能性が考えられる。
  A 社のメールシステムでは拡張子「zip」のファイルを添付したメールの送受信が制限されており、ZIP ファイルを添付する際には、メールシステムの制限を回避するために拡張子を変更して送受信するケースがあった。攻撃者は過去に A 社から送信された正規メールを盗み見る中で ZIP ファイルの拡張子を変更して送信しているメールを発見し、それを模倣したものと推測される。
  これは、A 社の習慣に沿うようなメールとすることで、B 社経理担当者に正規メールであると誤認させる確率を高める意図があったものと思われる。

PDF ファイル 2 点は、当該ファイルのメタデータより、偽のメールに流用された正規メールの送信から 4～5 時間後に作成したものと推測される。

PDF ファイル(1)のイメージ図を図 8 に示す。

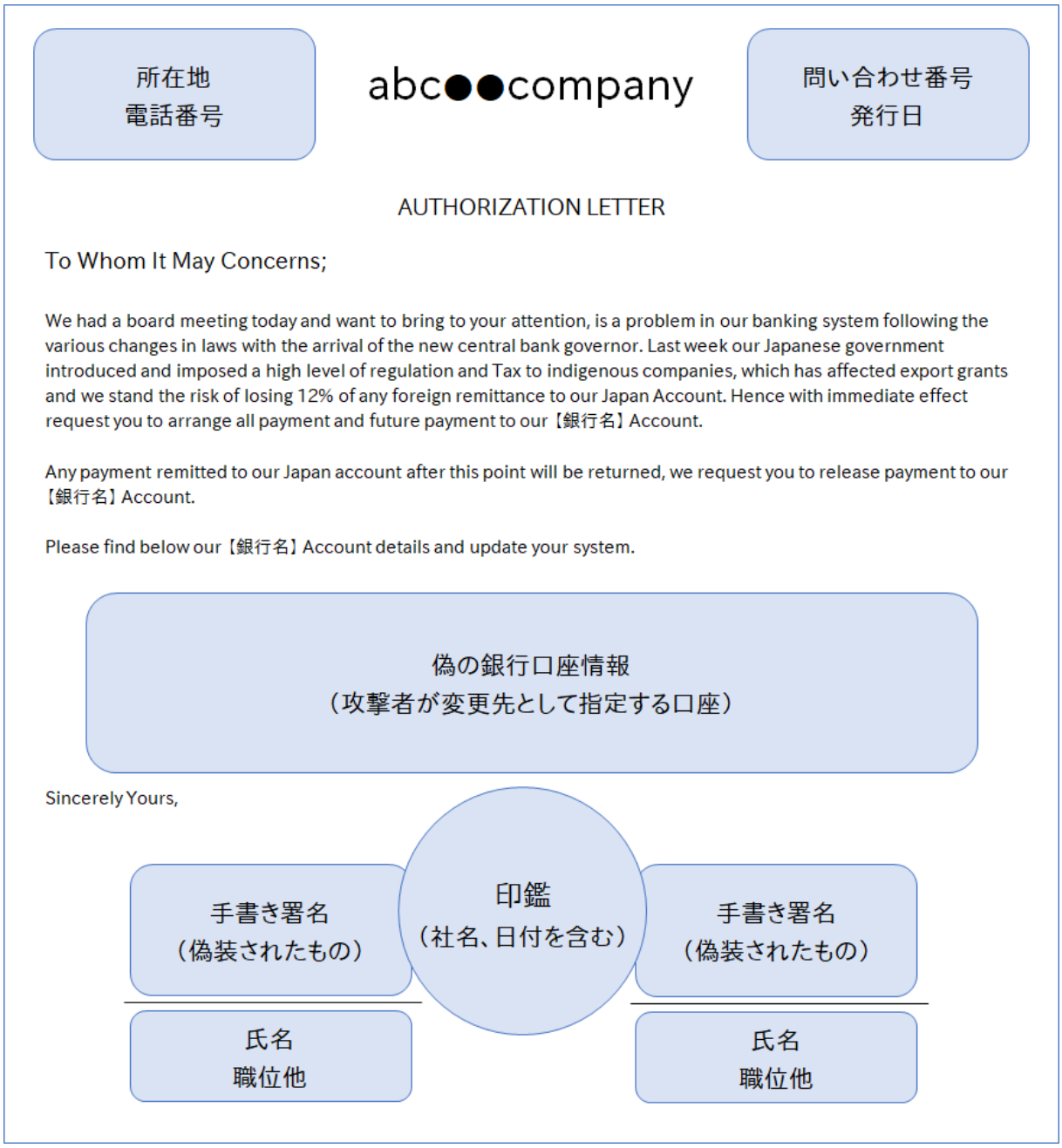

図 8 PDF ファイル(1) A 社発行を偽る偽造文書

PDF ファイル(1)、A 社発行を偽る偽造文書には、B 社経理担当者に正規の依頼であると誤認させようとする、特徴的な手口が複数用いられていた。

- 口座変更を依頼する偽の理由の記載
  偽造文書には、変更先の銀行口座の情報だけでなく、変更を依頼する偽の理由も記載されていた。攻撃者が理由として挙げた内容は次のとおり。

「新しい中央銀行総裁が着任したことで、企業に対する規制と課税を強化する法改正が行われた。その結果、海外から日本の口座への送金の際、送金額の 12%が失われる可能性がある。」

- 実在する A 社従業員の手書き署名の偽装
  偽造文書には、実際に A 社に在籍する従業員 2 名の氏名、職位、および社名が騙られており、それぞれの手書きの署名を偽装した署名が使用されていた。
  2 つの偽の署名のうち 1 つは、A 社従業員本人が実際に使用した手書きの署名を攻撃者が何らかの手段で入手して切り貼りしたものと推測している。なお、本署名箇所は、文書内の他の箇所と比較して解像度が著しく低かった。また、もう 1 つの偽の署名は本人の実際の署名ではなく、攻撃者が何らかの手段で偽造したものであった。
- A 社の社名と所在地、当日の日付の入った印鑑の押印
  偽造文書には、A 社の社名と所在地、メール送信日当日の日付が入った印鑑が押印されていた。この印鑑は実際に A 社で使用しているものとは異なるものであり、攻撃者が何らかの手段で偽造したものと推測している。

本物のメールアドレスに似せた詐称用ドメインの使用

本件の攻撃メールにおいて、差出人（From）および同報先（CC）のメールアドレスは、図 9 に示すように、A 社のメールアドレスに似せた偽のメールアドレスが使用されていた。攻撃者が同報先にも偽のメールアドレスを設定していたのは、衆人環視の状況と錯覚させる目的や、A 社関係者にメールが届かないようにすることで詐欺の発覚を避ける目的と推測される。

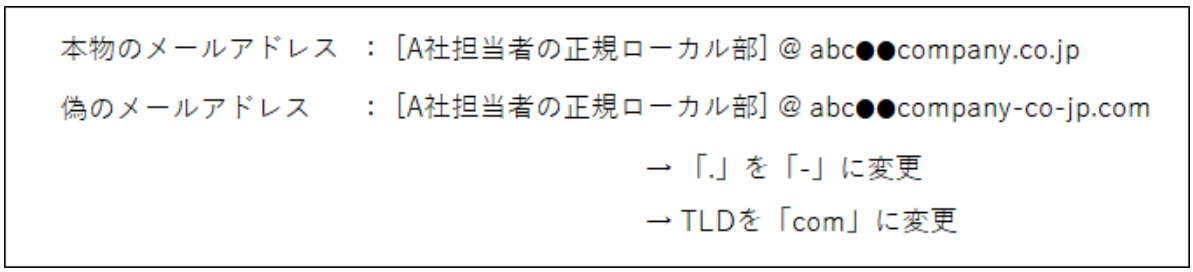

図 9 攻撃者が取得、使用した詐称用ドメイン

偽のメールアドレスのローカル部は本物のメールアドレスと同一であり、ドメイン部には A 社の正規ドメインに似せた詐称用ドメインが使用されていた。

なお、この詐称用ドメインは、偽のメールに流用された正規メールの送信から 5 時間後、偽造文書の作成とほぼ同時刻に取得されている。攻撃者は、正規メールを盗み見た後、すぐに攻撃を仕掛ける準備を始めている。

その後の対応

攻撃者から着信したメールを確認した B 社経理担当者がメールの内容を不審に思い、A 社担当者の正規のメールアドレス宛に真偽を確認する連絡を行ったことで、詐欺であることが発覚した。偽のメールには返信しておらず、また、以降に攻撃者からのコンタクトは確認されなかった。これらにより、金銭的な被害には至らなかった。なお、A 社では本件を受けて、メールの盗み見の原因の調査や関係者への聞き取り等の対応を行った。

本事例のまとめ

本件で試みられたBECは正規メールの盗み見を伴うものであり、更に偽造文書の作成といった手の込んだ手口が用いられていた。また、偽のメールの送信元として使用された詐称用ドメインは、偽のメールの送信直前に取得されていた。これには、自組織の正規ドメインと類似したドメインの取得状況を調査、セキュリティ対策に活用している組織もあることを攻撃者が意識して、そのような対策をすり抜ける意図があったものと考えられる。

詐称用ドメインを用いた偽のメールアドレスや偽造文書の使用については、J-CSIP の運用状況レポート[2022 年 1 月～3 月]で紹介した事例をはじめ、IPA では複数件を確認しており、今後も同様の手口が用いられることが推測される。

これらの対策として、偽のメールアドレスについては、メールの送信元が確かに本人のメールアドレスであるかの確認を徹底し、必要に応じて、メールのヘッダーに不審な点がないかを確認していただきたい。また、偽造文書については、文書中に少しでも違和感を覚える点（例として、いつもは宛名に個人名が明記されているのに「ご担当者様」と記載されている、手書き署名の箇所の解像度が低い、など）があれば、信頼できる連絡先に事実確認を行うことを勧める。

4　2 つの CEO 詐欺の続報

過去、J-CSIP の運用状況レポートにて報告してきた 2 つの CEO 詐欺について、本四半期においても 3.1 節で紹介した事例などの情報提供があり、また J-CSIP 外の情報等を含めた独自の調査でも、類似する複数のメール検体を引き続き入手している。

本章では、これら 2 つの CEO 詐欺について説明する。

（1） 複数組織へ行われた CEO を詐称する一連の攻撃
（2）「日本語化（多言語化）」された CEO 詐欺の攻撃

2 つの CEO 詐欺は、いずれも企業の極秘買収をテーマとして CEO や会長などの役員を騙り、偽の弁護士とやり取りさせることで多額の金銭を詐取しようとするものである。この攻撃では、国内企業だけではなく、海外企業も含めて広く攻撃が行われている。

メールの内容として、「外部の弁護士と連絡を取り、分割で支払いをしてほしい」というメールや、実在する弁護士を騙って連絡先や口座残高を聞き出そうとしたり、数千万円から 1 億円程度の支払いを求めてきたりする事例を確認している。

また、メールに加えて電話や WhatsApp 等を併用しようとする手口を 2020 年 4 月から 2023 年 5 月の間で 40 件以上観測している。

これらのメールは、特定の組織や業種のみを狙うものではなく、多くの業種に対して試みられたことも確認している。そのため、業種に関わらず、今後も継続して国内外の組織に対して広範囲で攻撃が行われる可能性があり、注意が必要である。

なお、観測し始めた 2019 年以降、2 つの CEO 詐欺の攻撃手口に大きな変化はみられていない。

これまで IPA で入手したメールの件数を次に示す。

表 2 IPA が入手したメール件数一覧

観測期間	複数組織へ行われた CEO を詐称する一連の攻撃（件）	「日本語化」された CEO 詐欺の攻撃（件）
2019 年度	108	7
2020 年度	109	52
2021 年度	19	19
2022 年度	12	31
2023 年度（4 月～6 月）	3	35

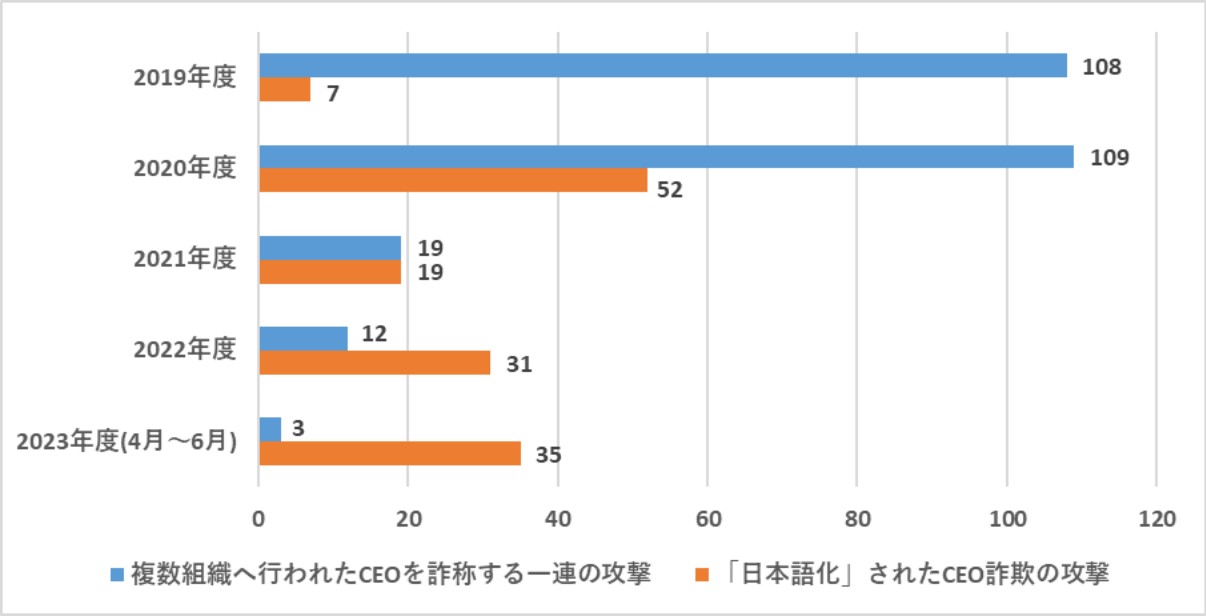

図 10 IPA が入手した年度別メール件数推移

4.1 複数組織へ行われた CEO を詐称する一連の攻撃

本攻撃は、2019 年 7 月以降継続して観測しており、国内外の複数の組織を対象として行われている痕跡を確認している。メールの件名や内容は時期ごとに変化が見られるが、メールのヘッダー情報に類似する点があり、一連の攻撃は同一の攻撃者によるものと推測している。

本攻撃に関するメールについては、米国のセキュリティベンダーが 2020 年 7 月に公開したレポート[6]においても報告されている。

IPA からの報告状況

初報は「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]」3.3 節 事例 3[7]となり、その後、J-CSIP 運用状況レポートにて続報を数回にわたって公開している。「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）[8]」の 2.3 節 事例 3 も、この一連の攻撃の一部である。

攻撃メールの特徴

攻撃メールには、次のような特徴がある。

---

[6] Cosmic Lynx: A Russian Threat Hits the BEC Scene（Agari）
https://www.agari.com/blog/cosmic-lynx-russian-bec

[7] 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/security/j-csip/ug65p9000000nkvm-att/000080133.pdf

[8] 【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（第三報）（IPA）
https://www.ipa.go.jp/archive/security/security-alert/2020/bec.html

表 3 攻撃メールの特徴

項目	特徴
メールの宛先	国内外の複数の組織（経営者、役員、職員等と思われるメールアドレス）へ送られている。
メールで騙られた人物	実在する CEO や CFO、弁護士等を詐称。CEO を詐称する場合、ほぼ、攻撃先の各企業の実際の CEO や会長を名乗っている。また、少数だが、取引先の CEO を名乗る事例も確認している。
攻撃者のメールアドレス	命名に規則性があり、差出人（From）や返信先（Reply-To）に「smtp」「relay」「secure」「server」「gateway」「outbound」「private」「trusted」「mail」「network」「encrypted」等という単語を「-」で組み合わせているものが多い。また、2020 年頃までは天体（惑星・衛星・星座等）に関する単語も組み合わせていた。
使用言語	ほぼ英語のメールだが、日本語、フランス語、スペイン語も確認している。
メール件名	2020 年頃までは「legal counsel」「law firm」「法律事務所」を含む件名を多く確認していたが、2020 年 5 月以降は件名に「Project」を含むメールを多く確認している。
メール本文	2020 年頃までは、主に数行程度で「重要な用件がある」、「計画について話がしたい」として、メールへ返信することを求める内容であった。 2020 年 3 月以降の 1 年間は、新型コロナウイルス感染症の話題を文章の書き出しにすることが多かったが、2021 年 4 月以降は、新型コロナウイルス感染症関連の文言は使われなくなった。 2020 年以降は、「外部の弁護士と連絡を取り、分割で支払いをしてほしい」というメールや、弁護士を騙って 1 億円程度を送金するよう要求するメールも確認している。

4.2 「日本語化（多言語化）」された CEO 詐欺の攻撃

本攻撃は、2019 年 11 月以降継続して観測しており、メールの件名や内容は一部の変化が見られるが、いずれも M&A 案件への対応を依頼するメール内容であり、メールのヘッダー情報にも類似する点がみられる。そのため一連の攻撃は同一の攻撃者によるものと推測している。

本攻撃に関するメールについては、米国のセキュリティベンダーが 2023 年 5 月に公開したレポート[9]においても報告されている。

IPA からの報告状況

2020 年 4 月、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ビジネスメール詐欺の事例[10]を公開した。その後、J-CSIP の参加組織から、国内企業の経営層を詐称したなりすましメールについて、継続して情報提供があり、J-CSIP 運用状況レポートにて続報を数回にわたって公開している。2023 年 4 月に公開した「ビジネスメール詐欺事例集」事例 6[11]も、この一連の攻撃の一部である。

攻撃メールの特徴

攻撃メールには、次のような特徴がある。

表 4 攻撃メールの特徴

項目	特徴
メールの宛先	国内外の複数の組織（CEO 等と思われるメールアドレス）へ送られている。
メールで騙られた人物	実在する CEO や会長を騙っている。
攻撃者のメールアドレス	命名に規則性があり、差出人（From）や返信先（Reply-To）に「board」「mail」「email」「mobile」「phone」「relay」「secure」「sent」「smtp」等という単語がローカル部に使われており、ドメイン部には「board」「intern」「mobile」「phone」「server」「smtp」「ssl」といった単語を組み合わせたメールアドレスを使う。
使用言語	英語、日本語、スペイン語を多く確認している。件名や本文に一部の違いはあるが、各言語でほぼ同様の内容が書かれたメールを確認している。また、それ以外の言語（フランス語、ドイツ語　等）でのメールも確認している。
メール件名	「金融合併と買収につきまして」「Finance M&A」「M&A Project」「HQ Project」「Liaise with counsel」といった件名を多く確認している。
メール本文	「企業買収について協力してほしい」「極秘プロジェクトを手伝ってほしい」「外部の弁護士と連絡を取り支払いをしてほしい」といった内容のものが多い。実在する弁護士を騙って連絡先や口座残高を聞き出そうとするものや、数千万円から 1 億円程度の支払いを求めてくる事例も確認している。

[9] New Research from Abnormal Security Shows the Rise of Business Email Compromise Attacks Sent from Israel（Abnormal）
https://abnormalsecurity.com/about/news/israel-bec-report

[10] ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」 事例 1
https://www.ipa.go.jp/archive/files/000081866.pdf

[11] 事例 6：国内企業社長になりすまし、グループ企業役員に金銭の支払を要求した事例（IPA）
https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/case6.pdf
https://www.ipa.go.jp/security/bec/bec_cases.html

攻撃メールの一例

攻撃者から送られてくるメールには複数のパターンがあることを確認しているが、ここではスペイン語のやりとりのメールについて、一例を紹介する。なお、日本語と英語のメールについては「IPA からの報告状況」に記載の 2 つの事例を参照いただきたい。

図 11 に示す 1 通目は、ある企業の役員を騙り、財務マネージャー宛に弁護士から連絡があったか尋ねるものである。

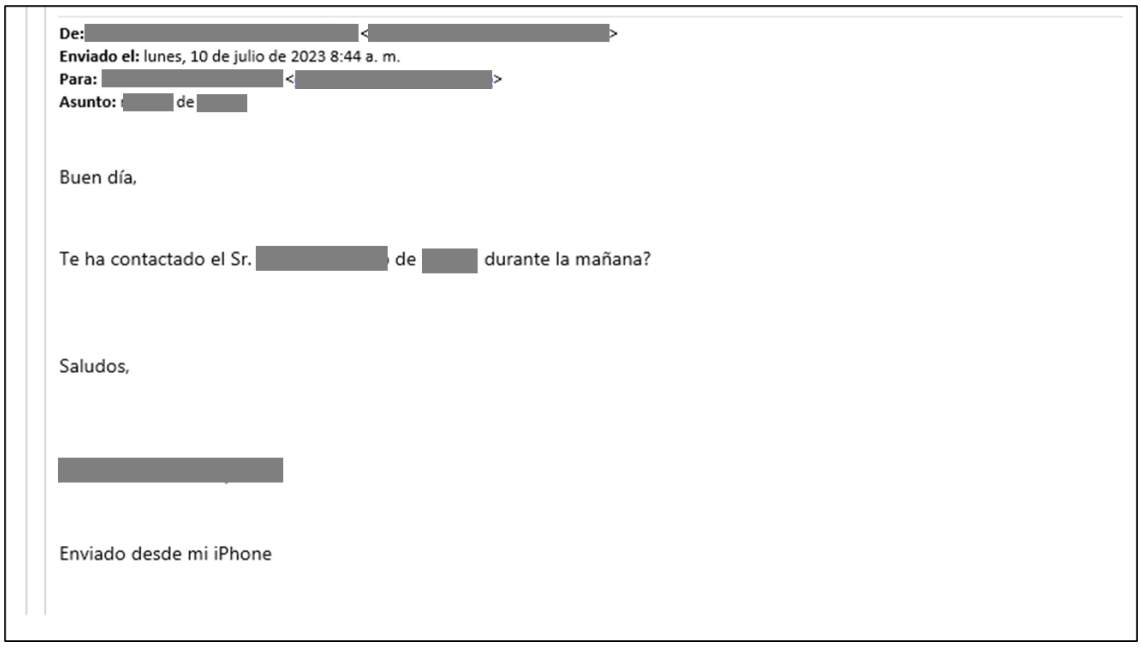

図 11 攻撃者からのメール（スペイン語） 1 通目

1 通目に「連絡はない」と返信すると、弁護士と協力して財務関連の問題に対応してほしいというメールが送られてくる（図 12）。

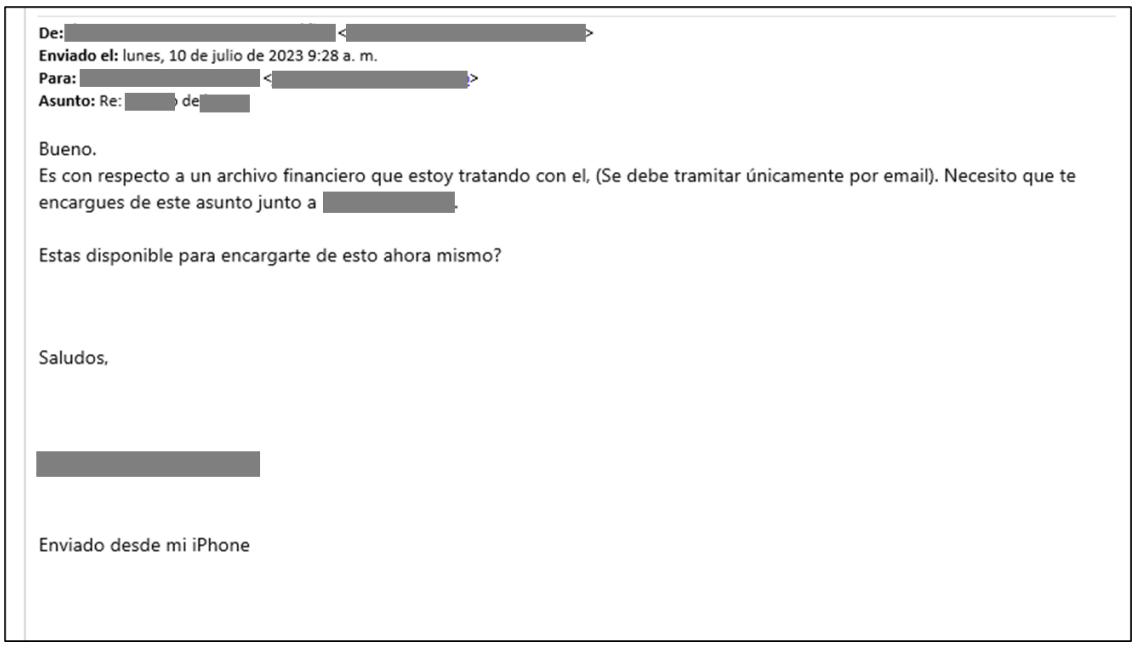

図 12 攻撃者からのメール（スペイン語） 2 通目

2 通目に「対応可能である」を返信すると、海外企業の買収に関する振込金額と弁護士の連絡先が送られてくる（図 13）。この BEC においては、782,765US ドルの振込を要求するものであった。

図 13 攻撃者からのメール（スペイン語） 3 通目

関連情報のご提供のお願い

本書で紹介した事例について、J-CSIP では関連情報を求めています。
同様の事例を確認した場合など、下記窓口へ情報提供をいただけますと幸いです。

J-CSIP 事務局 ご連絡窓口 （IPA）
jcsip-info@ipa.go.jp

ウイルス・不正アクセス届出のお願い

IPA では、国内のコンピュータウイルスの感染被害や、コンピュータ不正アクセスによる被害の届出を受け付けています。被害等の実体把握や今後の防止に役立てるため、ぜひご協力をお願いします。

コンピュータウイルス・不正アクセスに関する届出 （IPA）
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

標的型サイバー攻撃特別相談窓口

IPA の「標的型サイバー攻撃特別相談窓口」では、標的型サイバー攻撃を受けた際の相談を受け付けています。お気づきの点があれば、ご相談ください。

標的型サイバー攻撃特別相談窓口 （IPA）
https://www.ipa.go.jp/security/todokede/tokubetsu.html

以上