サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2020 年 4 月～6 月]

2020 年 7 月 30 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、2020 年 6 月末時点の運用体制、2020 年 4 月～6 月の運用状況を報告する。1 章、2 章は全体状況を、3 章以降は本四半期で把握、分析した特徴的な攻撃事例や動向等を併せて解説する。

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/

1　運用体制

2020 年 4 月～6 月期（以下、本四半期）は、次の通り参加組織の増加があり、全体では 2020 年 3 月末の 13 業界 249 組織＋2 情報連携体制から、13 業界 259 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）の体制となった。（図 1）。

- 2020 年 4 月、電力業界 SIG に新たな参加組織があり、32 組織から 42 組織となった。

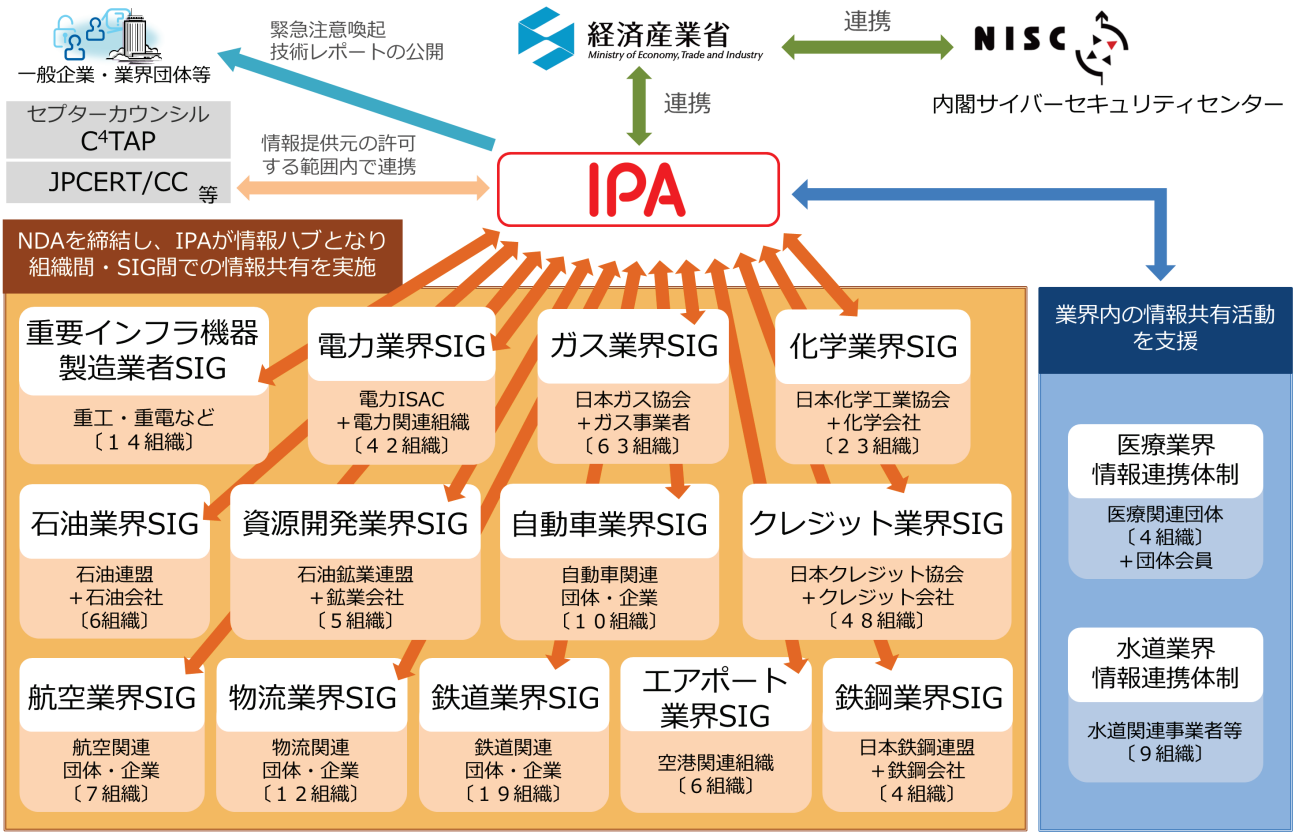

図 1 J-CSIP の体制図

[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現れている。ここでは延べ数としている。

2　実施件数（2020 年 4 月～6 月）

2020 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 259 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	2019 年		2020 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	235 件	1,042 件	602 件	**325 件**
2	参加組織への情報共有実施件数※1	75 件	40 件	56 件	**55 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 **38 件**を含む。

本四半期は情報提供件数が **325 件**であり、うち標的型攻撃メールとみなした情報は **87 件**であった。提供された情報の主なものとして、複数組織へ継続して行われた CEO を詐称する一連の攻撃や、2020 年 4 月に公開したビジネスメール詐欺第三報[3]にある、「日本語化」された CEO 詐欺の攻撃についての情報提供がおよそ 2 割を占めている。この他にも取引先とのやり取りに攻撃者が割り込んでくるタイプの事例についても情報提供があり、本四半期に標的型攻撃メールと見なした情報は、いずれもビジネスメール詐欺に関するものであった。これらについては、3 章で述べる。

また、前四半期まで観測されていたプラント関連事業者を狙う一連の攻撃について、本四半期では観測されなかった。一時的に攻撃が停止しているだけであるのか、攻撃そのものが終わったのかは不明である。これについては、6 章で述べる。

このほか、次に挙げる情報提供があり、一部情報共有を行った。

- 外部公開しているサーバに暗号資産の採掘を行うプログラム（コインマイナー）が不正に設置されたという情報提供があった。攻撃者は当該サーバへ不正アクセスしたのち、VPN 経由で通信可能な組織内の端末に対して総当たり攻撃による侵入を試み、侵入に成功した端末でもコインマイナーが不正に動作させられた。これについては、4 章で述べる。

- 本四半期、多数の日本企業や組織の偽サイト（当該組織の正規のものとは異なるドメインで、当該組織のウェブページの内容が表示されるサイト）が存在するという情報が出回った。本件について、ある参加組織から、自組織の偽サイトの存在を確認したという情報提供があった。当該組織では、偽サイトの停止手続きを行ったとのことであった。これについては、5 章で述べる。

[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（第三報）（IPA）
https://www.ipa.go.jp/security/announce/2020-bec.html

情報提供に付随して、IPA へ次のような相談・報告事例があった（表 2）。

表 2 相談・報告事例

項番	相談・報告内容	件数
1	実在する日本の企業を騙るウイルスメールが着信した。	1 件
2	Office 365 のアカウント情報を狙うフィッシングメールが着信した。	14 件
3	組織内から外部の不審サイトに不正通信を行っていることを検知した。	4 件

項番 1 は、実在する日本のある企業を騙るウイルスメールが着信したという情報提供である。悪意のある者によって、実在する組織が騙られ、攻撃メールが送られてくるというケースは特にめずらしい事象ではない。ただ、この例では日本語の件名・本文のメールであり、組織内へ 1 通のみ着信したと報告されている。メールに添付されているウイルスの種類や、メールの特徴から、現時点では本件を標的型攻撃とは見なしてはいないが、広範囲にばらまかれたメールでもないと考えられ、引き続き注視していくこととした。

項番 2 は、Office 365 のアカウント情報を狙うフィッシングメールが着信したという情報提供である。これまでも Office 365 のアカウント情報を狙うフィッシングメールは観測されており、J-CSIP の運用状況レポートで度々紹介している。本四半期では、一つの組織で 700 通のフィッシングメールが着信したという情報提供もあった。騙された利用者のアカウントを通じ、企業・組織内の情報等が侵害される可能性をもたらす脅威であり、注意が必要である。フィッシング詐欺への対策は、二要素認証の導入のほか、利用者一人ひとりが、騙されないよう手口を知ることが重要である。

項番 3 は、組織内の PC から不審サイトへのアクセスをセキュリティ機器で検知したというもので、URL 等はそれぞれ異なるが、同様の情報提供・相談が継続している。調査の結果、いずれも、ウェブ閲覧中に不正な広告があるページを開いたものや、何らかの理由で詐欺サイトのような悪意のあるウェブサイトへ誘導されたものであった。意図的に不審なサイトを閲覧せずとも、通常業務の中でこのようなことは発生しうるため、攻撃の被害に遭わないよう、OS やブラウザ等のソフトウェアの脆弱性を解消するとともに、不審サイト・詐欺サイト・偽警告 [4]等に騙されないようにするといった従業員への教育を継続的に実施すべきであろう。

[4] 被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20170411.html

3 ビジネスメール詐欺（BEC）の事例

本四半期においても、引き続き J-CSIP の参加組織に対してビジネスメール詐欺が試みられた事実を把握した。ビジネスメール詐欺については、2017 年 4 月と2018 年 8 月、そして 2020 年 4 月の 3 回にわたりIPAより注意喚起を行ったが、その後も継続して事例や実被害を確認しており、今後も注意が必要な状況である。

ビジネスメール詐欺の被害に遭わないようにするため、ビジネス関係者全体で、この脅威を認識し、手口を理解するとともに、不審なメールやなりすましメールへ警戒する必要がある。社内ルールを整備し、組織全体で被害を防止するという体制も必要であろう。また、社内だけではなく、取引先や銀行等、ステークホルダ全体でビジネスメール詐欺の被害防止に向けた対策が進むことが望ましい。

本四半期は、J-CSIP の参加組織から 69 件のビジネスメール詐欺について情報提供を受けた。これらのうち、3 件はタイプ 1（取引先へのなりすまし）の攻撃で、残りの 66 件は、タイプ 2（経営者等へのなりすまし）であった。さらに、J-CSIP 外の一般企業・組織からも 8 件のビジネスメール詐欺の情報提供があった。

本章では、開示許可の得られたタイプ 1 の 3 件の事例と、タイプ 2 の 1 件の事例について詳しく説明する（表 3）。また、2019 年 10 月～12 月期から継続して観測していた「複数組織へ行われた CEO を詐称する一連の攻撃」や、2020 年 4 月の注意喚起レポートに掲載した、「日本語化」された CEO 詐欺の攻撃について、本四半期でも継続して確認されたため、あわせて説明する。

表 3 ビジネスメール詐欺の事例概要

項番	情報提供日		事例概要	被害の有無	備考
1.	2019 年	12 月 23 日	2019 年 10 月、日本国内企業（支払側）と、海外グループ企業（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	**あり**	本書:事例 1
2.	2020 年	4 月 24 日	2020 年 4 月、日本国内企業（支払側）と、海外取引先企業（請求側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	本書:事例 2
3.		5 月 11 日	2020 年 5 月、日本国内企業の海外グループ企業（請求側）と、海外取引先企業（支払側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	本書:事例 3
4.		5 月 19 日	2020 年 4 月、日本国内企業の CEO になりすました攻撃者が、海外グループ企業の CEO に対してビジネスメール詐欺を試みた。	なし	本書:事例 4

3.1 事例 1 国内企業を狙った攻撃

本事例は、2019 年 10 月、J-CSIP の参加組織（A 社：支払側）と、A 社の海外グループ企業（B 社：請求側）との間で取引を行っている中、B 社の担当者になりすました攻撃者から、偽の口座への送金を要求するメールが送られたものである。

この手口は、IPA が 2017 年 4 月に公開した注意喚起レポートで紹介しているビジネスメール詐欺の 5 つのタイプのうち、「タイプ 1：取引先との請求書の偽装」に該当する。

この事例では、偽の口座への送金にまで至ったため、金銭的な被害が発生した。

今回の事例でやりとりされたメールはすべて英文であった。

本事例では、詐欺の過程において、次の手口が使われた。

(1) 偽の口座への送金を連絡する

(2) 偽のメールアドレスの使用

(1) 偽の口座への送金を連絡する

本事例は、A 社（国内企業）と、その取引先である B 社（A 社の海外グループ企業）との間で、取引に関するメールのやり取りを行っている中で発生した。

2019 年 9 月から 10 月にかけて、正規の A 社と B 社とのやりとりで、「B 社から A 社へ支払われた前払い金」の払い戻し処理に関するやり取りが複数回あった。そのやりとりの中で、A 社から B 社へ、送金予定日が 11 月 22 日であることが通知され、B 社からは、送金先となる B 社の口座情報が、A 社側に提示されていた。

その後、2019 年 10 月 21 日、A 社担当者から B 社担当者へ、「口座情報に問題が無いことが確認できたため、払い戻し手続きを進める」という旨の正規のメールを送信した後、攻撃者から、別の口座への送金を依頼するメールが送られた（図 2）。すなわち、B 社側が送金処理を待つのみとなったタイミングで偽のメールが送られており、攻撃者は何らかの方法でメールのやりとりを盗聴していたものと考えられる。

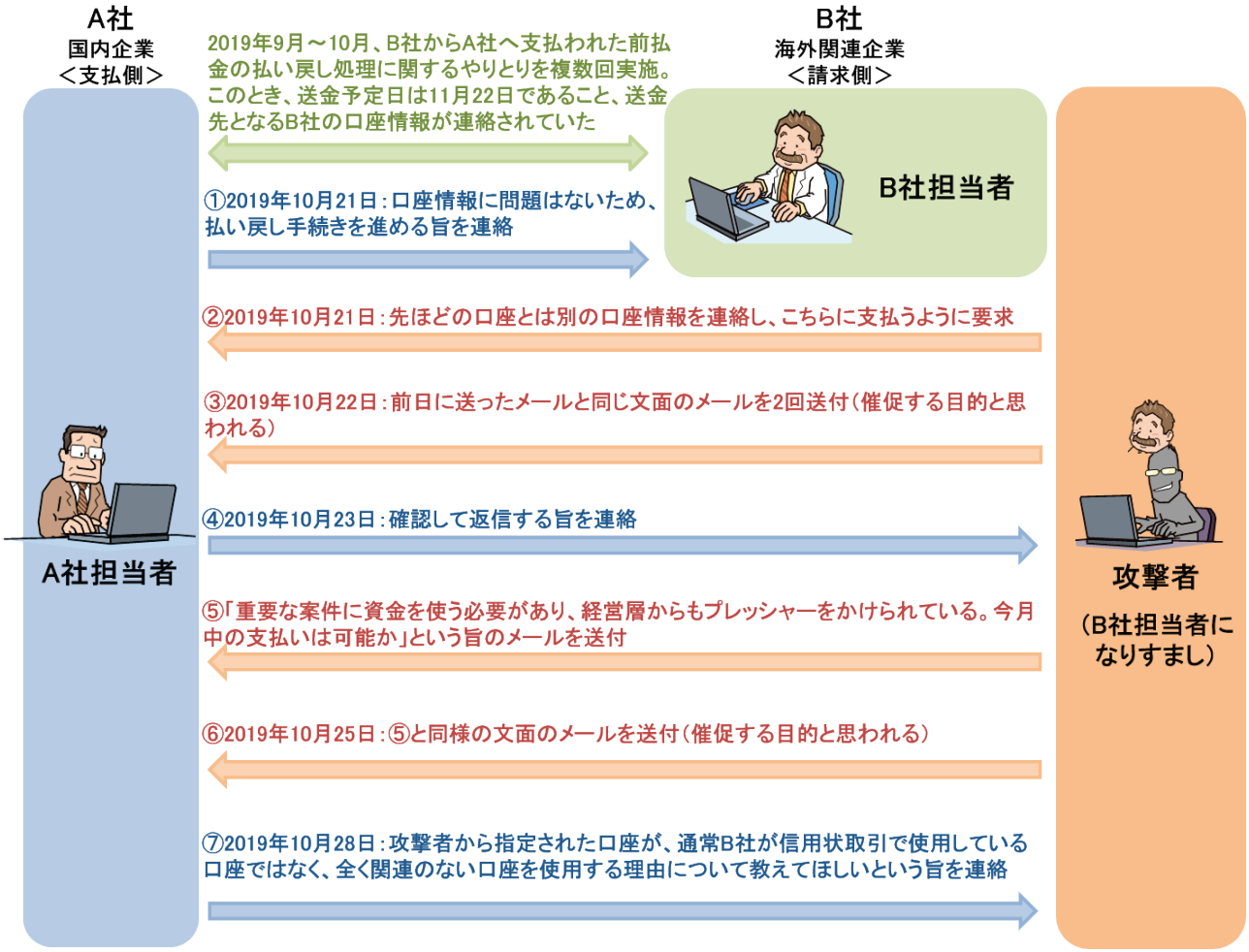

図 2 事例 1 攻撃者とのやりとり（前半）

口座の変更についてＡ社担当者はいくつか質問をしたが、攻撃者は様々な理由を挙げ、担当者を騙し通すことに成功している。

更に、攻撃者は 11 月 22 日であった送金予定日を早めることを要求し、その日付として 11 月上旬を指定してきた（図 3）。このことから、攻撃者はＡ社とＢ社間の払い戻し処理に関するやり取りを監視しており、事情を全て把握していたものと思われる。

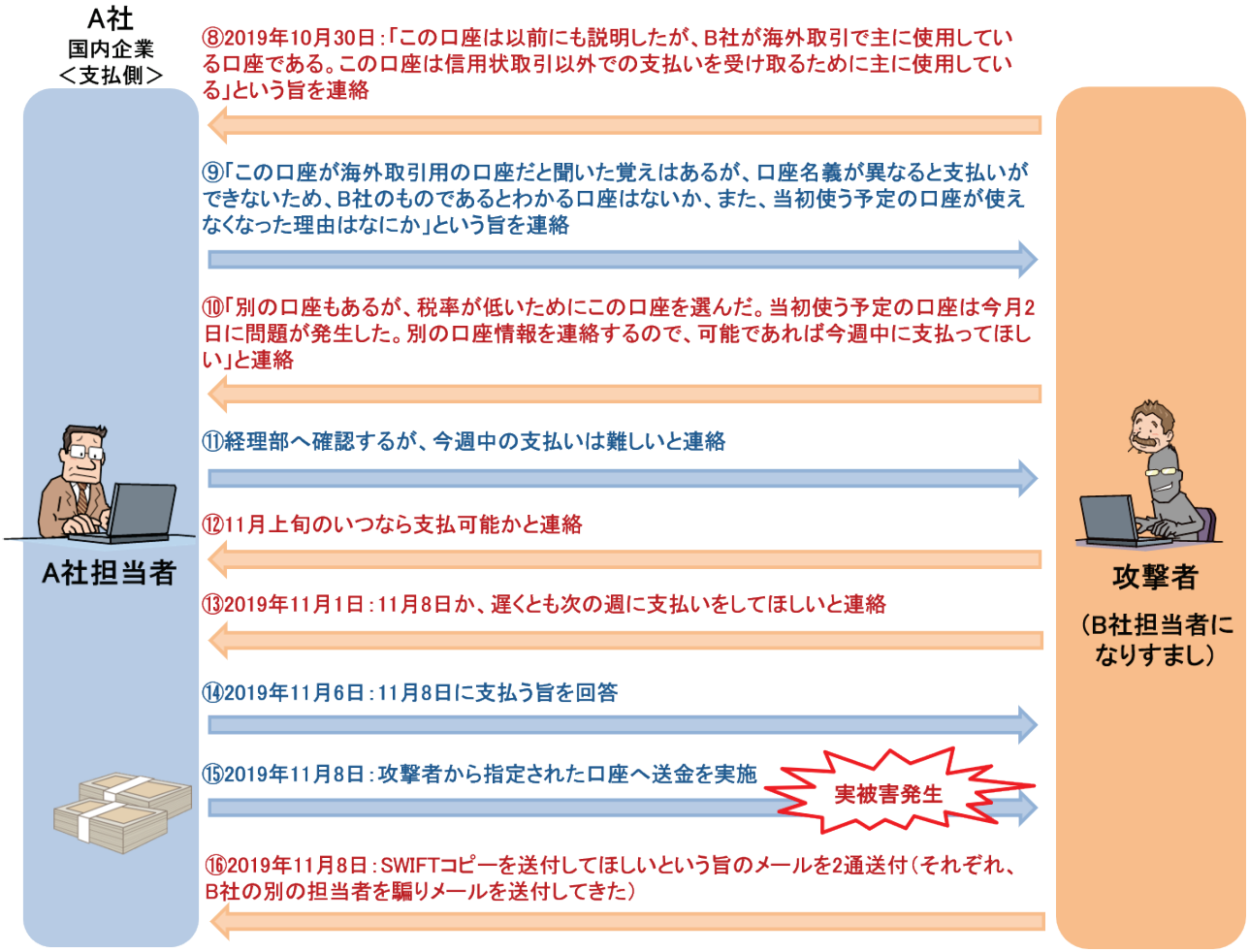

図 3 事例 1 攻撃者とのやりとり（後半）

（2） 偽のメールアドレスの使用

攻撃者は、B 社担当者になりすまして、A 社担当者へなりすましメールを送る際にメールの差出人（From ヘッダ）と、返信先（Reply-To ヘッダ）と、不達通知先（Return-Path ヘッダ）、および同報先（Cc）を次のように設定し、細工していた。

From ヘッダ： B 社担当者の氏名 〈B 社担当者の本物のメールアドレス〉
Reply-To ヘッダ： B 社担当者の氏名 〈攻撃者のメールアドレス〉
Return-Path ヘッダ： B 社とは関係のないメールアドレス
Ccヘッダ： B 社担当者の氏名 〈B 社とは関係のないメールアドレス〉
A 社担当者の氏名 〈A 社担当者の本物メールアドレス〉

この手口により、次の効果を狙ったものと考えられる。

- 差出人（From）を本物のＢ社担当者のメールアドレスに設定することで、本物のメールに見せかけつつ、メールへ返信しようとすると、返信先（Reply-To）に書かれたメールアドレスが宛先として設定されるため、正しい宛先への返信に思わせようとしている。
- メールが何らかの原因で配送エラーとなった時に、B 社宛にエラー通知が届かないようにするため、Return-Path ヘッダに、B 社とは別のメールアドレスを設定することで、詐欺の発覚を防ぐように細工している。
- 同報されているメールアドレスを改変することで、A 社担当者にとっては、自分以外の多くの関係者が宛先に入っているように見える（衆人環視の中でのやりとりに見える）が、実際には A 社のみに送られており、騙されていることに気づきにくい。また、B 社側の関係者にとっては、この偽メールが届かないため、詐欺が行われていることに気づけない。

3.2 事例 2 国内企業を狙った攻撃

本事例は、2020 年 4 月、J-CSIP の参加組織（A 社：支払側）と、その海外取引先企業（B 社：請求側）との間で取引を行っている中、B 社の担当者になりすました攻撃者から、偽の口座への振込先の変更を要求するメールが送られたものである。

この手口は、IPA が 2017 年 4 月に公開した注意喚起レポートで紹介しているビジネスメール詐欺の 5 つのタイプのうち、「タイプ 1：取引先との請求書の偽装」に該当する。

この事例では、A 社の担当者が急な振込先変更の指示がメールで届いたことを不審に思い、B 社の担当者へ電話による確認を行ったため、金銭的な被害には至らなかった。

今回の事例でやりとりされたメールはすべて英文であった。

本事例では、詐欺の過程において、次の手口が使われた。

(1) 偽の口座への振込先変更依頼
(2) 詐称用ドメインの取得と悪用
(3) メールの配送・開封通知設定

(1) 偽の口座への振込先変更依頼

本事例は、A 社（国内企業）と、その取引先である B 社（海外取引先）との間で、2019 年 12 月から 2020 年 4 月の期間において、取引に関するメールのやり取りを行っている中で発生した。

2020 年 4 月 22 日、B 社担当者から A 社担当者へ、「B 社の銀行口座で技術的な問題が発生したため、香港の代替口座へ変更したい」という旨の振込先の変更を依頼するメール（図 4）が送り付けられた。この時の攻撃者からのメールは、それまで A 社と B 社でやり取りしていたメールの内容を引用し、返信する形となっていた。このため、攻撃者は何らかの方法でメールのやりとりを盗聴していたものと考えられる。

さらに、2020 年 4 月 23 日にも、4 月 22 日に送られたメールと同一の内容のメールが、攻撃者から A 社担当者へ送り付けられた。

これら 2 通のメールには、口座情報が記載された正規の請求書など 4 つのファイルが添付されており、それらのファイルは改ざんされていなかった。攻撃者の意図は不明であるが、本物の情報（取引に関する正規の各種文書）と、偽の情報（偽の口座への変更）を同時に送ることで、偽メールであることのカモフラージュを試みた可能性が考えられる。

この攻撃者からのメールに対し、A 社の担当者は、急な口座変更の指示がメールで届いたことを不審に思い、B 社担当者へ電話による確認を行ったところ、偽のメールであることが発覚した。

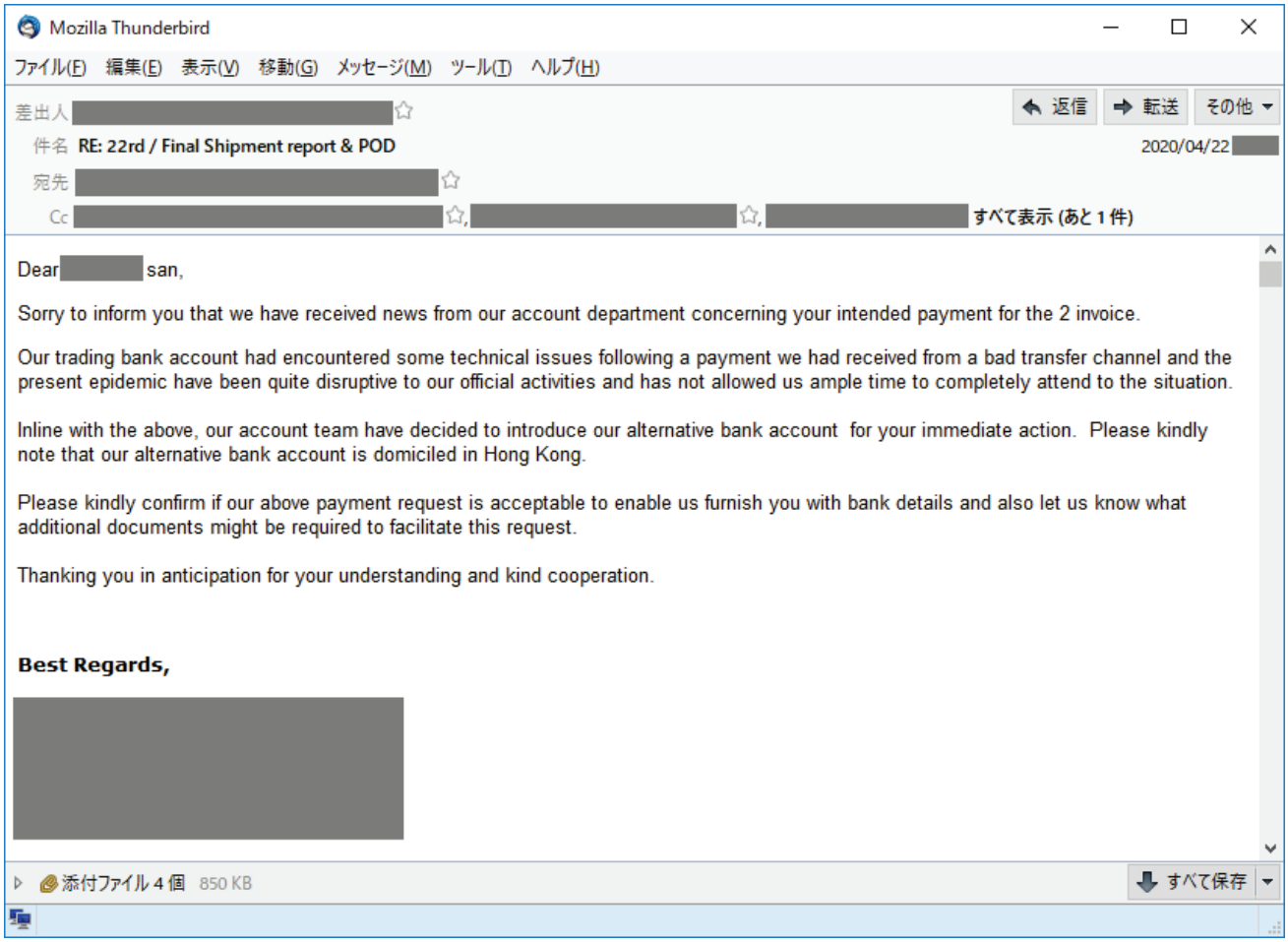

図 4 事例 2 攻撃者からのメール

(2) 詐称用ドメインの取得と悪用

攻撃者は差出人(From)と同報先(Cc)に記載されていた、B 社および、B 社グループ企業の正規のドメインに似通った「詐称用ドメイン」を、攻撃メールを送る当日(2020 年 4 月 22 日)に新規に取得していた。詐称用ドメインは、次の例に示すようなものであった。

- B 社の詐称用ドメインの例(差出人と同報先)

【本物のメールアドレス】alice @ b-companys . com . cc
【偽物のメールアドレス】alice @ b-companys-cc . com
(″com″と″cc″の位置やハイフンでの置き換え)

※実際に悪用されたものとは異なる。

- B 社のグループ企業の詐称用ドメインの例(同報先)

【本物のメールアドレス】bob @ b-companysgroup . com . cc
【偽物のメールアドレス】bob @ b-cornpanysgroup -cc . com
(″m″を″r n″に置き換え、″com″と″cc″の位置やハイフンでの置き換え)

※実際に悪用されたものとは異なる。

(3) メールの配送・開封通知設定

本件の攻撃メールのヘッダには、次の項目が設定されており、攻撃メールの着信状況に応じて、攻撃者宛に通知メッセージが送信されるように細工されていた。ただし、攻撃者へ通知メッセージが送信されるかは、受信側メールサーバ等の設定によるため、実際に通知されていたかは不明である。

攻撃者は、攻撃メールの着信状況を把握することで、攻撃の成否や、次の攻撃段階へ移るタイミングを見極めようとしていたものと推測している。

- メールの配送通知先の設定

Return-Receipt-To: B 社担当者の氏名 〈攻撃者の偽メールアドレス〉

➢ 宛先のメールサーバにまでメールが配送された時、メールサーバから通知先へ、配送通知が送信される。

- メールの開封通知先の設定

Disposition-Notification-To: B 社担当者の氏名 〈攻撃者の偽メールアドレス〉

➢ 利用者がメールを開封した時、通知先へ開封通知が送信される。

3.3 事例 3 海外グループ企業を狙った攻撃

本事例は、2020 年 5 月、J-CSIP の参加組織（国内企業）の海外グループ企業（A 社：請求側）と、その海外取引先企業（B 社：支払側）との間で取引を行っている中、A 社の担当者になりすました攻撃者から、偽の口座への振込先の変更を要求するメールが送られたものである。

この手口は、IPA が 2017 年 4 月に公開した注意喚起レポートで紹介しているビジネスメール詐欺の 5 つのタイプのうち、「タイプ 1：取引先との請求書の偽装」に該当する。

この事例では、B 社の担当者が振込先口座の変更について不審に思い、A 社の担当者へ直接事実確認を行ったため、金銭的な被害には至らなかった。

今回の事例でやりとりされたメールはすべて英文であった。

本事例では、詐欺の過程において、次の手口が使われた。

(1) 新型コロナウイルス感染症（COVID-19）を話の取り掛かりとした振込先変更依頼

(2) 偽のメールアドレスの使用

(1) 新型コロナウイルス感染症（COVID-19）を話の取り掛かりとした振込先変更依頼

本事例は、A 社（国内企業の海外グループ企業）と、その取引先である B 社（海外取引先）との間で、請求書に関するメールのやりとりを行っている中で発生した。

2020 年 5 月 7 日、A 社と B 社が請求書に関する正規のメールのやりとりの中で、A 社から B 社へ正規の請求書が送付された。その後、同日中に攻撃者から、「COVID-19 の影響で、ロックダウンが行われた。支払いはいつになるのか教えてほしい」という内容のメール（図 6）が B 社宛に送り付けられた。この時の攻撃者からのメールは、それまで A 社と B 社の担当者で行われていた正規のやりとりのメールに引用返信する形となっていた。このため、攻撃者は何らかの方法でメールのやりとりを盗聴していたものと考えられる。

5 月 8 日、B 社担当者は、攻撃者から送られたメールを不審とは思わず、請求書に記載された期日通りに支払いを行う旨を攻撃者へ返信した。すると、攻撃者から「貴社の経理部門へ、支払いを保留するように伝えてほしい。現在、ロックダウンの影響によって、銀行等の業務に支障がでており、支払いの確認が困難となっている。」という旨のメール（図 7）が、B 社担当者へ送られた。その後、B 社担当者と攻撃者との間で、支払日について、数通のメールのやりとりが行われた。

最終的に、攻撃者から「メールに修正版の請求書を添付したので、支払いが遅れないよう早めに確認してほしい。支払い先は子会社の口座に変更した。」という旨のメールと、偽の請求書が添付されて送られてきた。この偽の請求書は、正規の請求書を基にして、振込先口座が改ざんされたものであった。

その後、B 社の担当者が、振込先口座が変更されたことについて、A 社の担当者へ直接事実確認を行ったことで事案が発覚し、金銭的な被害には至らなかった。

攻撃にかかるメールのやりとりについて、図 5 に示す。

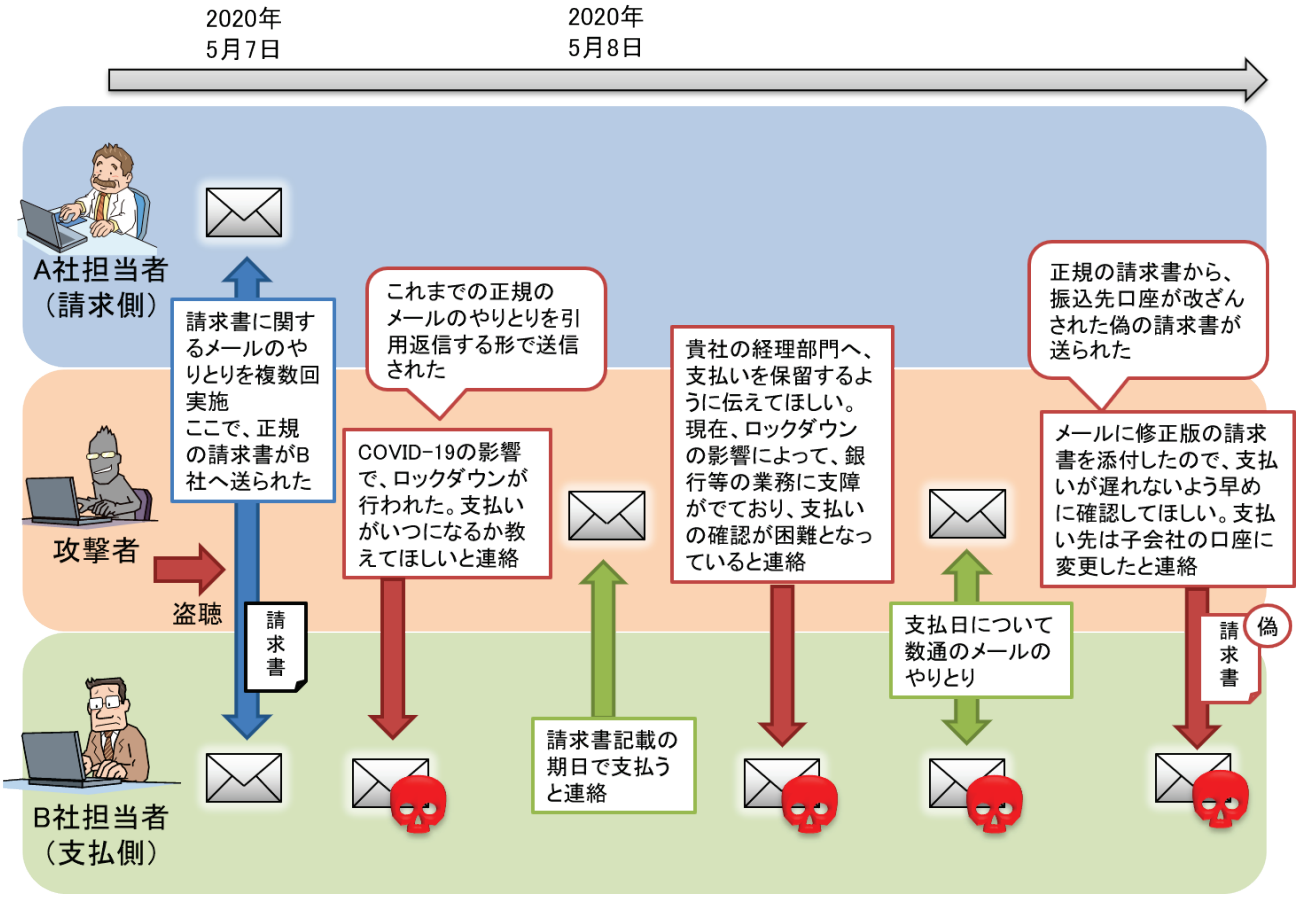

図 5 事例 3 攻撃者とのやりとり

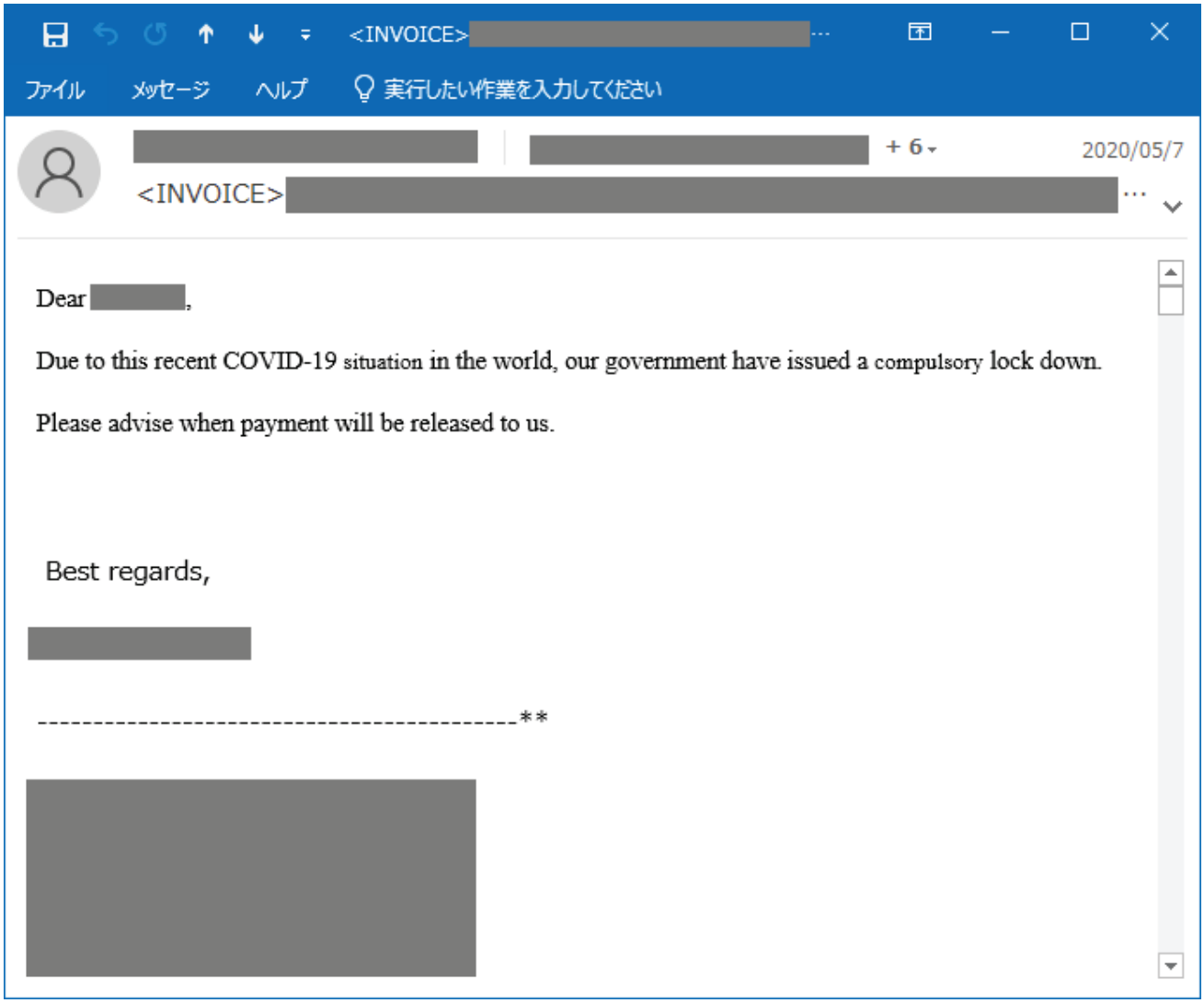

図 6 事例 3 攻撃者からのメール(1 通目)

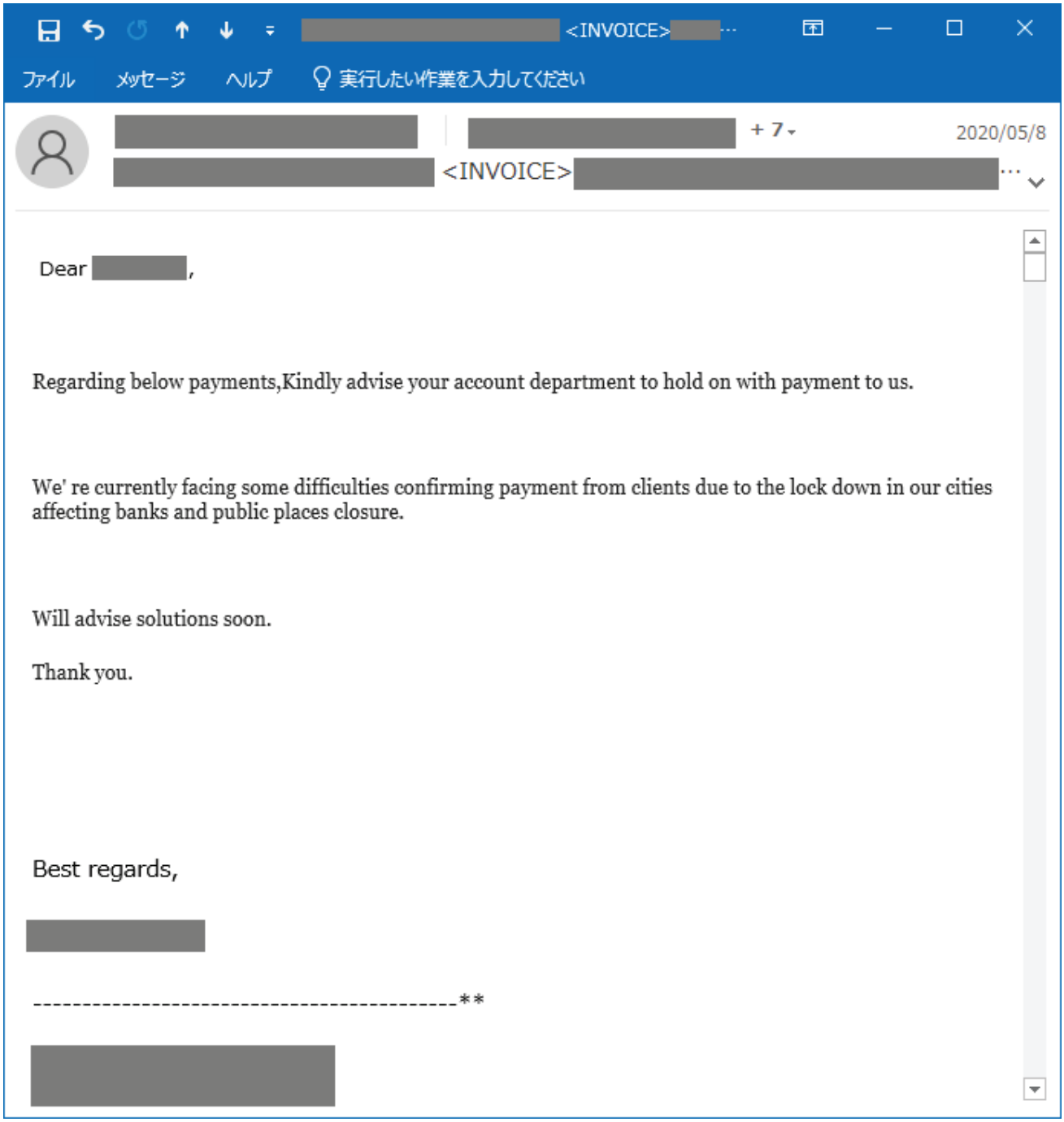

図 7 事例 3 攻撃者からのメール(2 通目)

(2) 偽のメールアドレスの使用

攻撃者は、A 社担当者になりすまして、B 社の担当者へメールを送る際に、メールの From ヘッダ（差出人）には A 社担当者の氏名と本物のメールアドレスを設定する一方で、Reply-To ヘッダ（返信先）を次のように細工していた。

- B 社へ送られたメールの Reply-To ヘッダの例

【本物】alice . eve @ company-a . com
【偽物】alice . eve . company-a @ mail . com

※実際に悪用されたものとは異なる。

Reply-To ヘッダに記載されていた攻撃者のメールアドレスは、「mail.com[5]」という、海外のサービスで無料取得できるドメインのものであった。

また、攻撃者からのなりすましメールでは、同報先（Cc）に記載された、複数の A 社の他担当者のメールアドレスも、Reply-To ヘッダと同じフリーメールアドレスのドメインのものに改変していた。

この手口により、次の効果を狙ったものと考えられる。

- 差出人（From）を本物の A 社担当者のメールアドレスに設定することで、本物のメールに見せかけつつ、メールへ返信しようとすると、返信先（Reply-To）に書かれたメールアドレスが宛先として設定されるため、正しい宛先への返信に思わせようとしている。
- 同報されているメールアドレスを改変することで、B 社担当者にとっては、自分以外の多くの関係者が宛先に入っているように見える（衆人環視の中でのやりとりに見える）が、実際には B 社のみに送られており、騙されていることに気づきにくい。また、A 社側の関係者にとっては、この偽メールが届かないため、詐欺が行われていることに気づけない。

[5] 2020/7/14 時点で、当該サービスでは 255 のドメインから選択してメールアドレスを取得することが可能である。

3.4 事例 4 海外グループ企業を狙った攻撃

本事例は、2020 年 4 月、J-CSIP の参加組織（A 社）の CEO になりすました攻撃者が、A 社の海外グループ企業（B 社）の CEO に対して、偽のメールを送り付けたものである。

この手口は、IPA が 2017 年 4 月に公開した注意喚起レポートで紹介している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」に該当する。

この事例では、B 社側のメール受信者が、ビジネスメール詐欺ではないかと不審に思い、B 社のシステム担当者に相談したところ、その疑いがあると判断され、メールの返信を行わなかったため、金銭的な被害には至らなかった。

今回で実際に攻撃者から送られたメールの件名、本文について、図 8 に示す。

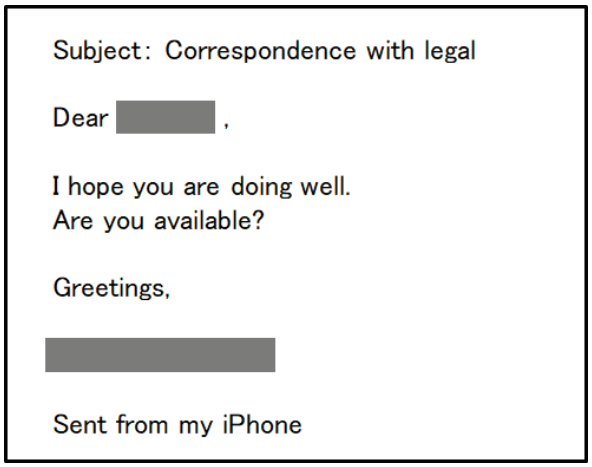

図 8 事例 4 攻撃者から送られてきたメールの件名と本文

この偽のメールでは、差出人（From）ヘッダに次のような設定が行われていた。

From: 【A 社 CEO の名前とメールアドレス】secured by [mailto:relay@365-offices.com]

このようにすることで、受信者のメールソフト上では、本物の A 社の CEO の名前とメールアドレスが表示される。これにより、偽のメールアドレスから送信されていることを気づかせにくくする狙いがあると思われる。

3.5 事例 5 複数組織へ行われた CEO を詐称する一連の攻撃（続報）

2019 年 10 月以降、J-CSIP の参加組織から、国内グループ会社の経営層を詐称したなりすましメールについて、前四半期までと同様、継続して情報提供があった。また、IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、情報提供されたものと合わせて新たに **50** 件（2019 年 10 月～12 月期では 62 件、2020 年 1 月～3 月期では 46 件確認）の類似するメール検体を入手するに至った[6]。

これらのメールは次に示す点が共通しており、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される状況である[7]。この一連の攻撃については、攻撃手口等からビジネスメール詐欺の一種であると考えており、「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」の 2.3 章 事例 3 も、この一連の攻撃の一部である。

- メールの宛先は、国内外の複数の企業（職員等と思われるメールアドレス）である。
- 実在する CEO や弁護士等を詐称している。
  - CEO を詐称する際、ほぼ、攻撃先の各企業の実際の CEO を名乗っている。
- 攻撃者が使用したメールアドレスは様々に異なるが、命名に規則性がある。具体的には、差出人（From）や返信先（Reply-To）に、「secure」という単語と、天体（惑星・衛星・星座等）に関する単語を組み合わせたメールアドレスが使用されている。
  - 2020 年 3 月 24 日に着信したメール（表 4 項番 12）のみ、天体（惑星・衛星・星座等）に関する単語は使われていなかったが、その他の特徴は一致していた。
- これまで確認した一連の攻撃メールの件名や本文はほぼ英文であり、日本語のメールは 9 件[8]、スペイン語のメールは 1 件、フランス語のメールは 1 件確認している。メールの件名・本文の内容は多数のバリエーションがある。メールへ返信すると、金銭の振り込みの要求等の詐欺が試みられるものと思われる。
  - 2019 年 7 月 23 日から 2020 年 5 月 13 日までのメールの特徴としては、メール本文は 5～10 行程度の簡素なもので、具体的な用件は書かれていないが、「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る点が共通している。
  - 2020 年 3 月 24 日以降、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して使用する攻撃メールを複数確認している。
    - 2020 年 3 月 24 日から 2020 年 5 月 12 日までのメールでは、「COVID-19 による世界的な危機の中、皆様の安全や健康を願っている」という書き出しのもの[9]が多かったが、2020 年 5 月 20 日以降のメール（図 9）では、「世界中の国々が徐々に規制を緩和していく中で、経済活動を再開していかなければならない」といったように、文章に変化が見られた。
    - 2020 年 5 月以降に観測されたメールでは、件名に「Project」が入るように変化した。
- メールの着信時期は、確認できている限り、2019 年 7 月 23 日から 2020 年 6 月 23 日である。

---

[6] 本事例については、本レポート執筆時点である 2020 年 7 月 1 日までの情報で記載している。

[7] これらメールの特徴については、米国 Agari Data 社が次の URL で公開しているレポートと同様であり、同一の攻撃者による攻撃であると推測している。
https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/

[8] 日本語のメールについては、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]にメールの例を記載している。

[9] 本件のメールについては「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」で紹介している。
http://www.ipa.go.jp/security/announce/2020-bec.html

本四半期に IPA で確認したメールの情報の一覧を、表 4 に示す。

この一連のビジネスメール詐欺は、特定の組織や業種のみを狙うものではなく、多数の業種に対して試みられたことを確認している。このため、業種に関わらず、継続して国内外の組織に対して攻撃が試みられる可能性があり、今後も注意が必要である。

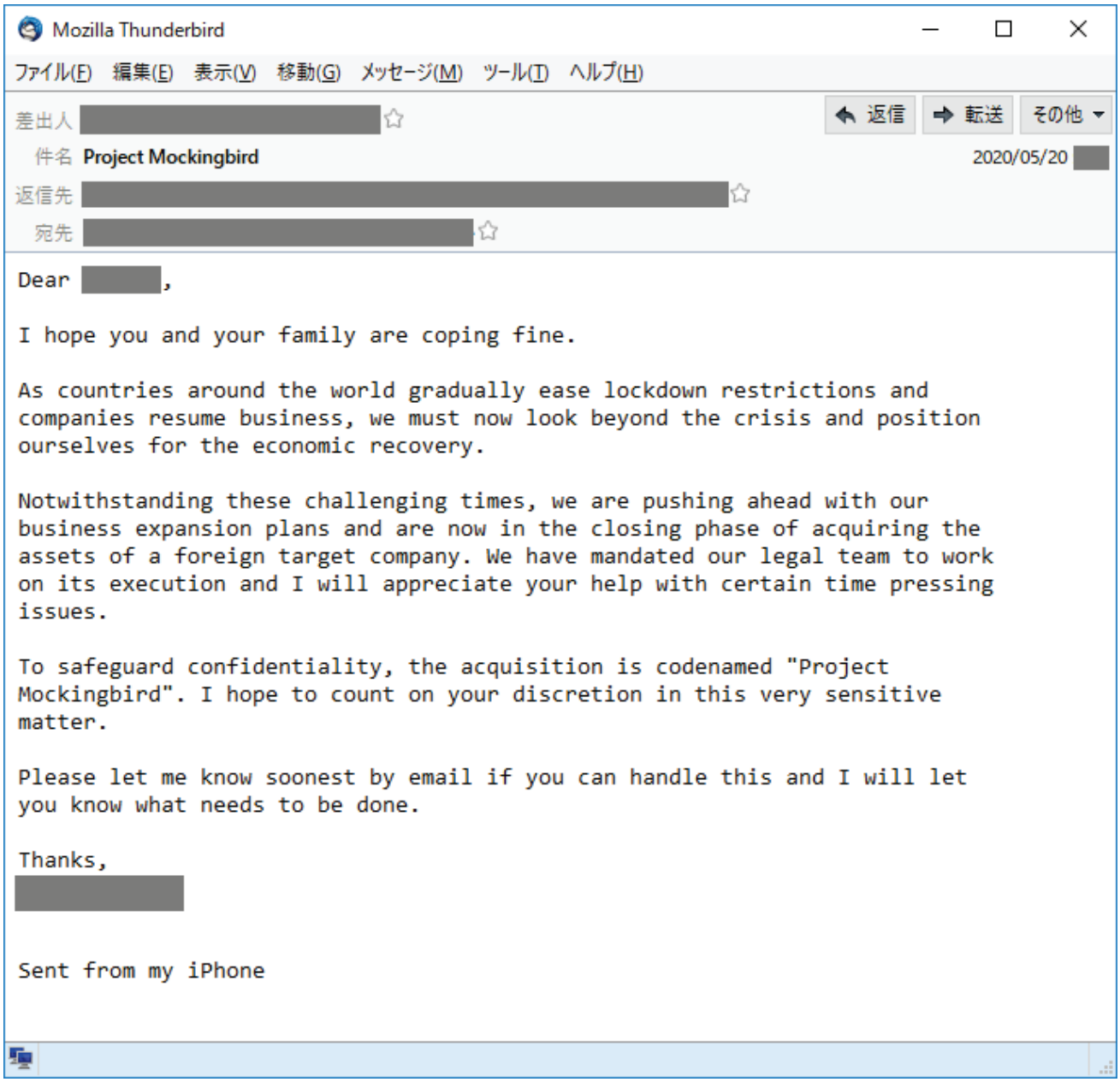

図 9 事例 5 攻撃者からのメール(2020/5/20)

表 4 事例 5 IPA で確認している本件の攻撃メール情報の一覧

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
1.	製造業	2019/10/23	Liaise with external legal counsel	smtp-neptune@secure-mail-server.cc
2.	製造業	2020/1/16	Resolve matter with law firm	secure-uranus@secure-mx-gateway.cc
3.	製造業	2020/2/6	Accords finaux en cours	secure-pluto@fortinet-gateway.cc
4.	製造業	2020/3/9	Matter with law firm	smtp-saturn@secure-mx-provider.cc
5.	製造業	2020/3/9	Matter with law firm	smtp-saturn@secure-mx-provider.cc
6.	製造業	2020/3/9	Matter with law firm	smtp-saturn@secure-mx-provider.cc
7.	製造業	2020/3/9	Matter with law firm	smtp-saturn@secure-mx-provider.cc
8.	製造業	2020/3/17	外部法律事務所との連携	encrypted-jupiter@encrypted-mail-server.com
9.	製造業	2020/3/17	外部法律事務所との連携	encrypted-jupiter@encrypted-mail-server.com
10.	製造業	2020/3/24	外部法律事務所との連携	encrypted-sirius@encrypted-mail-server.com
11.	製造業	2020/3/24	外部法律事務所との連携	encrypted-sirius@encrypted-mail-server.com
12.	金融業, 保険業	2020/3/24	Coronavirus Sensitive Matter	ssl@secure-smtp-servers.com
13.	製造業	2020/3/30	Possible corporate action	tls-nexus@mx-secure-net.com
14.	製造業	2020/4/2	New corporate development initiative	secure-tucana@secure-smtp-service.com
15.	金融業, 保険業	2020/4/3	New corporate development project	tls-mercury@mx-secure-net.com
16.	製造業	2020/4/3	New corporate development initiative	tls-venus@mx-secure-net.com
17.	製造業	2020/4/6	Possible corporate action	-
18.	製造業	2020/4/7	New corporate development initiative	tls-uranus@mx-secure-net.com
19.	製造業	2020/4/7	New corporate development initiative	secure-jupiter@mx-gateway-host.cc
20.	製造業	2020/4/7	New corporate development initiative	secure-jupiter@mx-gateway-host.cc
21.	学術研究, 専門・技術サービス業	2020/4/16	New corporate development initiative	tls-taurus-net@mx-gateway-host.cc
22.	学術研究, 専門・技術サービス業	2020/4/20	Potential corporate transaction	tls-sirius-net@mx-gateway-host.cc
23.	情報通信業	2020/4/21	Possible corporate transaction	mx-jupiter-host@secure-email-provider.com
24.	製造業	2020/4/22	New corporate development initiative	encrypted-neptune@encrypted-mail-server.com
25.	学術研究, 専門・技術サービス業	2020/5/5	Project Indigo	gateway-atlas@encrypted-host.cc
26.	金融業, 保険業	2020/5/6	Project Daylight	gateway-pluto@mail-transport-gateway.cc
27.	情報通信業	2020/5/6	Project Ambience	tls-pluto-net@mx-gateway-host.cc
28.	製造業	2020/5/6	Project Hexagon	secure-jupiter@smtp-gateway-host.cc
29.	製造業	2020/5/6	Project Ambience	tls-pluto-net@mx-gateway-host.cc
30.	製造業	2020/5/6	Project Ambience	tls-pluto-net@mx-gateway-host.cc

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
31.	電気･ガス･熱供給･水道業	2020/5/6	Project Hexagon	secure-jupiter@smtp-gateway-host.cc
32.	製造業	2020/5/7	Project Gemini	mx-venus-host@secure-email-provider.com
33.	製造業	2020/5/7	Project Gemini	mx-venus-host@secure-email-provider.com
34.	製造業	2020/5/7	Project Gemini	mx-venus-host@secure-email-provider.com
35.	製造業	2020/5/12	Project Magnolia	tls-jupiter@fortinet-server.cc
36.	製造業	2020/5/12	Corporate matter	smtp-mercury@secure-mx-provider.cc
37.	電気･ガス･熱供給･水道業	2020/5/12	Project Magnolia	tls-jupiter@fortinet-server.cc
38.	製造業	2020/5/13	外部法律事務所との連携	smtp-jupiter@fortinet-protection.cc
39.	製造業	2020/5/13	外部法律事務所との連携	smtp-jupiter@fortinet-protection.cc
40.	製造業	2020/5/13	外部法律事務所との連携	smtp-jupiter@fortinet-protection.cc
41.	製造業	2020/5/19	Project Helium	smtp-saturn@fortinet-protection.cc
42.	製造業	2020/5/19	Project Helium	smtp-saturn@fortinet-protection.cc
43.	製造業	2020/5/19	Project Helium	smtp-saturn@fortinet-protection.cc
44.	製造業	2020/5/20	Project Mockingbird	secure-mercury@secure-mx-host.com
45.	製造業	2020/6/2	Project Evergreen	tls-jupiter@mail-transport-agent.cc
46.	製造業	2020/6/9	Project Cairo	gateway-nexus@secure-mail-gateway.cc
47.	製造業	2020/6/9	Project Cairo	gateway-nexus@secure-mail-gateway.cc
48.	製造業	2020/6/9	Project Biltmore	gateway-jupiter@encrypted-host.cc
49.	卸売業, 小売業	2020/6/18	Project Asterix	mx-venus@fortinet-protection.cc
50.	情報通信業	2020/6/23	Project Rosetta	gateway-neptune@secure-smtp-service.com

3.6 事例 6「日本語化」された CEO 詐欺の攻撃（続報）

2020 年 4 月、「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」の 2.1 章 事例 1 にて、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を公開した[10]。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った。また、IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、情報提供されたものと合わせて新たに **25** 件（2020 年 3 月末時点では 7 件確認）の類似するメール検体を入手するに至った[11]。

これらのメールは次に示す点が共通しており、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される状況である。

- 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」や「board-1」、「relay」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」や「mobile」、「server」といった単語を組み合わせたメールアドレスが使用されている。
- 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 6 月 29 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[12]。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。

本四半期に IPA で確認したメールの情報の一覧を、表 5 に示す。

この一連のビジネスメール詐欺は、これまでに 5 つの業種に対して試みられたことを確認しており、特定の組織や業種のみを狙うものではない。このため、業種に関わらず、継続して国内外の組織に対して攻撃が試みられる可能性があり、今後も注意が必要である。

事例 5 と共通して言える点として、これらは冷静に考えれば不審と判断できそうなメールに見える一方で、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、その攻撃者は複数の組織に対して執拗に攻撃を繰り返していることが明白である。偽物だと見破ることが容易に見えるようなメールであったとしても、侮るべきではないだろう。

---

[10] 【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/security/announce/2020-bec.html

[11] 本事例については、本レポート執筆時点である 2020 年 7 月 1 日までの情報で記載している。

[12] SendGrid を使用していない事例も確認しており、必ずしも本サービスを使用するというわけではない。

表 5 事例 6 IPA で確認している本件の攻撃メール情報の一覧

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
1.	製造業	2020/1/20	金融合併と買収につきまして	board@mobile81-intern.com
2.	製造業	2020/2/12	Finance M&A	board@mobile81-intern.com
3.	製造業	2020/3/3	金融合併と買収につきまして	board@intern-mobile081.com
4.	製造業	2020/3/3	金融合併と買収につきまして	board@intern-mobile081.com
5.	製造業	2020/3/25	金融合併と買収につきまして	board@intern-081mobile.com
6.	製造業	2020/3/26	金融合併と買収につきまして	board@intern-081mobile.com
7.	製造業	2020/3/30	金融合併と買収につきまして	board@intern33-mobile.com
8.	製造業	2020/3/30	金融合併と買収につきまして	board@intern-081mobile.com
9.	製造業	2020/3/30	金融合併と買収につきまして	board@intern-081mobile.com
10.	製造業	2020/3/30	金融合併と買収につきまして	board@intern-081mobile.com
11.	金融業, 保険業	2020/4/7	金融合併と買収につきまして	-
12.	金融業, 保険業	2020/4/7	金融合併と買収につきまして	-
13.	金融業, 保険業	2020/4/7	金融合併と買収につきまして	board@mobile81-intern.com
14.	製造業	2020/4/22	金融合併と買収につきまして	board@server-mobile33.com
15.	製造業	2020/4/27	Finance M&A	board@server-mobile33.com
16.	金融業, 保険業	2020/5/7	金融合併と買収につきまして	board@mobile-server33.com
17.	卸売業、小売業	2020/5/11	Finance M&A	board@intern33-mobile.com
18.	製造業	2020/5/14	Finance M&A	board@mobile-server33.com
19.	卸売業、小売業	2020/6/5	Liaise with counsel	board-1@outlook-ssl.host
20.	製造業	2020/6/8	金融合併と買収につきまして	-
21.	製造業	2020/6/9	Finance M&A	-
22.	卸売業、小売業	2020/6/22	Finance M&A	board@mobile-jp.co
23.	卸売業、小売業	2020/6/22	Liaise with counsel	board-1@dmarc-a-365.host
24.	卸売業、小売業	2020/6/23	Liaise with counsel	board-1@dmarc-a-365.host
25.	製造業	2020/6/29	金融合併と買収につきまして	relay@secure-sec-gov.com

4　外部公開サーバへの不正アクセスによる暗号資産採掘プログラムの設置事例

本四半期、J-CSIP 参加組織より、外部公開していたサーバに、暗号資産の採掘を行うプログラム（以下、コインマイナー）が不正に設置されたという情報提供があった。

本件の事象は、同様の手口を使った攻撃事例が公開情報でも確認されており、特定の組織・企業を狙ったものではないと考えられる。本章では、参考までにこの事例について説明する。

事象発見に至る経緯

2020 年 4 月末、当該参加組織で運用している SOC（Security Operation Center）において、当該参加組織が運用している外部公開サーバが不審な通信を行い、不審なファイルをダウンロードしたことを検知した。この件について、2020 年 5 月 12 日、当該参加組織から IPA へ、不審な通信先とともに、ダウンロードされたファイルについて情報提供が行われた。

その後の調査により、本事象の原因は、クラウドサービス上にある当該参加組織が管理するサーバが、設定不備により意図せずインターネットへ公開されている状態となっていたこと、また、そのため、攻撃を受けたものであったことが分かった。

確認された攻撃の流れ

情報提供された内容から、本件の攻撃の流れは次の通りである。

1. 外部公開サーバで稼働していた PostgreSQL には、OS コマンドインジェクションの脆弱性（CVE-2019-9193）が存在していた。攻撃者は本脆弱性を悪用してサーバに不正アクセスを行った。

2. 外部公開サーバに不正アクセスした攻撃者は、外部から次のツール（Linux 用）とファイルのダウンロードを行った。この時のダウンロードに使われた不正接続先には、「tor2web[13]」のドメインのものがあった。
   - PNScan （ポートスキャンツール）
   - sshpass （SSH ログイン試行ツール）
   - パスワードリストファイル

3. 攻撃者は、外部公開サーバから VPN 経由で通信可能な組織内部の端末に対し、脆弱性の悪用の試みや、ssh ログイン試行ツールとパスワードリストファイルを用いた攻撃での侵入拡大（側方移動、Lateral Movement）を試みた。

4. 侵入に成功した端末に対しては、コインマイナーを動作させる不正操作が行われた。なお、コインマイナーはメモリ上で稼働するものであった。

なお、次の点については情報提供時点で不明であった。
- 組織内部への侵入拡大時に、攻撃者が悪用を試みた脆弱性
- コインマイナーの種別、不正接続先等

---

[13] 「tor2web」は特殊なウェブブラウザを使用せずに、インターネットから Tor ネットワークにアクセスするためのドメイン（Tor プロキシ）である。

本事例では、2 つの原因で攻撃を受け、被害に至った。1 つ目は設定の不備によって、意図せずサーバがインターネット上で公開されていたこと。2 つ目はサーバ上で動作しているシステムに脆弱性があったことである。

脆弱性対策については、修正プログラムの公開を速やかに把握し、可能な限り早く適用することが重要である。サーバの設定については、設定不備がないように心がける必要があるが、特にサーバの外部公開については、悪意のある者から不正アクセスが試みられるであろうことを念頭におき、必要な対策をしつつ慎重に行うべきであろう。

5　国内組織・企業の偽サイトの事例

2020 年 5 月 13 日、多数の日本企業や組織の偽サイト（当該組織の正規のものとは異なるドメインで、当該組織のウェブページの内容が表示されるサイト）が存在するという情報が SNS 等で出回った[14]。本件について、ある参加組織から、自組織の偽サイトの存在を確認したという情報提供があった。

仕組みとしては、当該偽サイトへのアクセス要求があった場合、その要求を正規のウェブサイトへ転送し、結果を応答する（その過程で、HTML コンテンツに含まれる正規サイトのドメイン名の文字列を偽サイトのドメイン名へ変換する）という、いわゆるリバースプロキシと思われる挙動であった。これらのサイトが作成された目的は、悪意の有無を含めて不明である[15]。

J-CSIP では、本件のような、直接的なサイバー攻撃と見なすべきか判断しかねる事案についても、情報共有やフィードバックの収集に努めている。

偽サイトの確認

この時期に情報が出回った偽サイトは一部の TLD（Top Level Domain）に集中しており、次のキーワードを Google 等の検索サイトで検索することによって確認することができた。

```
"【自組織名】" AND (site:.gq OR site:.tk OR site:.cf OR site:.ml OR site:.ga OR site:.mem OR site:.fun OR site:.review OR site:.data OR site:.yokohama OR site:.zip OR site:.country OR site:.kim OR site:.cricket OR site:.science OR site:.work OR site:.party OR site:.link)
```

偽サイトのドメインに関する停止申請

これら偽サイトは、今回の場合 Cloudflare 社のサーバを経由するように設置されていた（偽サイトのドメインの名前解決先の IP アドレスが Cloudflare 社のものであった）ため、Cloudflare 社の Abuse 窓口に当該ドメインの停止申請を行った。

この停止申請が直接的な理由であるかは不明だが、その後数日で当該偽サイトへはアクセス不能となった。

---

[14] https://twitter.com/anemone_fish/status/1260057202313670656　等

[15] 例えば、閲覧者にウイルスを感染させる仕掛け等、明らかに有害と見なせる挙動は確認できなかった。ただし、閲覧者が偽サイト上のフォームへ情報を入力した場合、その内容が第三者（偽サイト設置者）へ読み取られる可能性がある点、また、リバースプロキシ処理の過程で、ウェブサイト上に掲載されている「連絡先メールアドレス」といった文字列が偽サイトのドメインに置き換わっている点、そもそも無断で設置されている点など、看過することもできないものであった。

6 プラント関連事業者を狙う一連の攻撃（続報）

2017 年 10 月以降、継続してプラント等の設備や部品のサプライヤーに対し、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールを送り付け、添付ファイル（ウイルス）を開かせようとする攻撃を多数観測してきた。

偽のメールの内容は巧妙で、使われている英文には不審な点は少ない。プラントの設計・調達・建設に関わる企業や資機材等について一定の知識を持つものが作成したと思われ、無作為に個人を狙うような攻撃ではなく、プラント関連事業者を標的とした攻撃だと推測している。また、短期間で多岐にわたる文面のバリエーションが作られる一方で、J-CSIP 内の数組織で確認している限り、同等のメールの着信数はそれぞれ数通から数十通程度である。観測数が多くないという点でも、広く無差別にばらまかれているウイルスメールとは様相が異なっている。

現時点では、攻撃者の目的が知財の窃取にある（産業スパイ）ものか、あるいはビジネスメール詐欺（BEC）のような詐欺行為の準備段階のものかは不明である。もしくは、プラントの設計・調達・建設に関わるサプライチェーン全体を攻撃の対象としている可能性（セキュリティが比較的弱い可能性のある、下流の資機材メーカーを侵入の入口として狙っている可能性）もありうる。いずれにせよ、ある程度特定の組織へ執拗に攻撃が繰り返されていることから、標的型攻撃の一種とみなして取り扱っている。

6.1 攻撃の観測状況

これまで継続して確認してきた攻撃メールであるが、日本語のメールは、2019 年 11 月 26 日以降、英語のメールについても 2020 年 3 月 6 日に観測して以降、本四半期では同等の攻撃メールが観測されなかった。

本件の攻撃について、攻撃が一時的に停止しているのか、または本件の攻撃そのものが完全に停止したのかは不明である。

6.2 まとめ

プラント関連事業者を狙う一連の攻撃について、現時点で確認できている状況を紹介した。単純な文面の提案依頼（RFP）、見積もり依頼（RFQ）、請求書等を装うウイルスメールは多種多様な事例があるが、この攻撃者は、プラントの資機材について詳細な内容の偽のメールを作成し、また、対象を絞って長期に渡り攻撃メールを送り付けてきている。攻撃対象は、無差別ではないものの、広くプラント関連事業者全般となっている可能性がある。

本四半期では類似の攻撃メールは観測されなかったが、今後も引き続き、本攻撃者の動向を注視していく。

7　EKANS ランサムウェアの解析事例

本四半期、複数の企業でランサムウェアによるインシデントが報告され、一部のセキュリティベンダなどから関係性が指摘されている「EKANS ランサムウェア」を複数入手し、独自に解析を行った。

EKANS は Go というプログラム言語で作成されたウイルスであり、解析におけるポイントを紹介すると共に、攻撃に使われた可能性のある複数の検体について、それらの差分に注目し、説明する。

参考情報として、その解析結果を本書の付録として示す。詳しくはそちらを参照いただきたい。

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

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/tokubetsu/

以上