サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2020 年 10 月～12 月]

2021 年 1 月 28 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 12 月末時点の運用体制、2020 年 10 月～12 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 10 月～12 月期（以下、本四半期）は、参加組織の増減はなく、全体で 13 業界 263 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）。

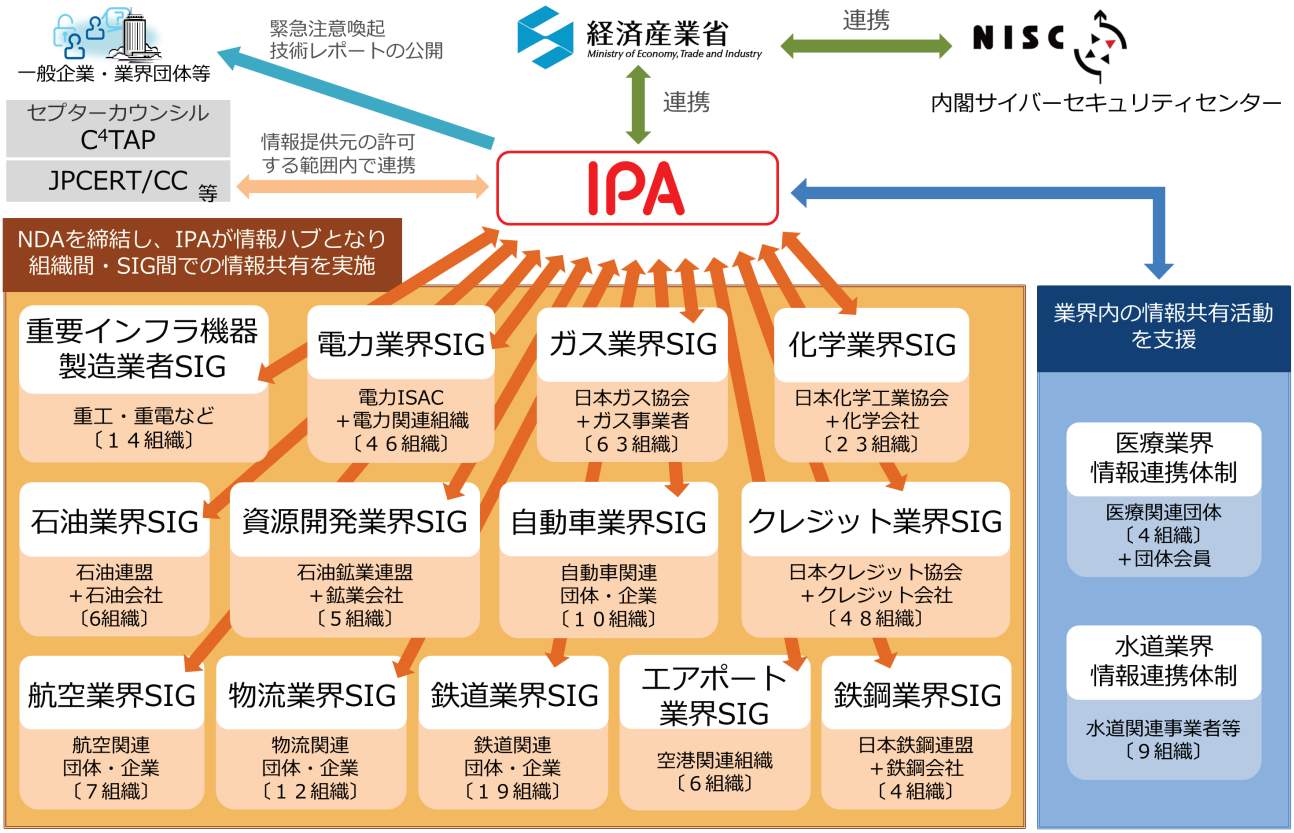

図　1 J-CSIP の体制図

[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現れている。ここでは延べ数としている。

2　実施件数（2020 年 10 月～12 月）

2020 年 10 月～12 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（12 月末時点、13 の SIG、全 263 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	2020 年			
		1 月～3 月	4 月～6 月	7 月～9 月	**10 月～12 月**
1	IPA への情報提供件数	602 件	325 件	4,988 件	**479 件**
2	参加組織への情報共有実施件数※1	56 件	55 件	29 件	**38 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 **16 件**を含む。

本四半期は情報提供件数が **479 件**であり、うち標的型攻撃メールとみなした情報は **16 件**であった。提供された情報の主なものとして、架空の組織を騙る、コロナ禍に乗じた日本語の不審メールについての情報提供が 4 割あった。類似のメールが複数の組織で確認されているものの、着信日や着信通数にはばらつきが見られた。これについては、5 章で述べる。

このほか、次のような情報提供があり、一部情報共有も行った。

- 取引先とのやり取りに割り込んでくるタイプや、企業の CEO になりすますタイプのビジネスメール詐欺の情報提供があった。また、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もあった。これらについては、3 章で述べる。

- 国内組織で運用中の VPN 装置に対する、脆弱性の悪用を企図した通信を検知したという情報提供があった。この脆弱性は、Cisco 社の VPN 装置に対して、認証されていないユーザが不正に機密ファイルを読み取ることができる可能性があるというもので、悪用するためのコード（PoC）も公開されている状態であった。これについては、4 章で述べる。

- 遠隔操作ウイルス（RAT）が添付された日本語の攻撃メールについて情報提供があった。メール本文は比較的簡素ではあるが、日本語に不自然な点が少ないものであった。本件について情報共有を行ったところ、複数の組織で類似したメールが確認された。これについては、6 章で述べる。

- Zoom のミーティングへの招待メールを装ったフィッシングメールが着信したとの情報提供があった。メールの内容は簡単な英語で書かれており、本文中の URL リンクをクリックすることでフィッシングサイトへアクセスさせられると考えられるものであった。これについては、7 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	社内のマシンから標的型攻撃に関係する可能性があるウイルスが発見された。	1 件
2	Emotet、IcedID への感染を目的とした攻撃メールの添付ファイルを開いてしまった。	3 件
3	Open Bug Bounty から、自組織サイトの脆弱性を発見したという報告があった。	1 件
4	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。	5 件

項番 1 は、海外拠点のマシンから不審な通信が発生していることを検知し、その通信を行っているウイルス検体について情報提供を受けたものである。IPA でウイルス検体を解析したところ、標的型攻撃に関係する可能性があるウイルスであった。これについては、J-CSIP 内で情報共有を行っている。

項番 2 は、Emotet や IcedID への感染を目的とした攻撃メールが組織内へ着信し、受信者が添付ファイルを開いてしまったという情報提供である。これらのメールの添付ファイルはパスワード付きの zip ファイルであったため、メールの配送経路上のセキュリティ製品の検知・検疫をすり抜けて着信したものと推測される。また、メールはいずれも日本語であり比較的不審であると気づきにくいメールであった。

情報提供元の組織ではいずれも zip ファイルを解凍し、格納されている Word 文書ファイルを開いてしまったが、マクロの有効化は実施していなかったため、ウイルス感染の被害には遭ってはいなかった。少しでも不審と思われる内容のメールや、Office 文書ファイルの場合、安易にマクロ機能を有効化しないよう徹底することが重要である。Emotet については IPA からも注意喚起 [4]を行っており、そちらも参考としていただきたい。

項番 3 は、Open Bug Bounty[5]（以降、OBB）という海外の脆弱性の報奨金プラットフォームから、自組織の運営するウェブサイトに脆弱性があるということが通知されたというものである。OBB は、ウェブアプリケーションに関するものなど、セキュリティリサーチャーが発見した脆弱性について、報告・調整・開示などを一定のルールの下で進めるための仕組みとなっている。報告を受けた組織は、発見者への報奨金の支払いや感謝の意を示すことが推奨されている。

本件では、実際にリサーチャーから指摘された箇所に脆弱性があることが確認され、対応を実施することができた。そして、リサーチャーに対して報奨金を支払うことを決めたとのことであった。日本国内では、脆弱性報奨金制度の考え方はまだ広く浸透していないと思われるが、本件のように、第三者からの脆弱性の報告がありうるため、外部から連絡可能な窓口の整備や、実際に報告を受けた際の対応について検討しておくことが望ましい。

特に、見知らぬリサーチャーと連絡を取ることに対する不安や、報奨金の支払い可否について、組織内で意見が分かれる可能性がある。事前に考え方や指針を定めておくとスムーズな対応が可能であろう。

---

[4] 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて(IPA)
https://www.ipa.go.jp/security/announce/20191202.html

[5] Open Bug Bounty
https://www.openbugbounty.org/

項番 4 は、組織内のマシン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や改ざんされた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[6]等に騙されないようにするといった従業員への啓発を継続的に実施すべきと考える。

[6] 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ているが、その後も継続して事例が確認されており、今後も注意が必要である。

ビジネスメール詐欺の被害に遭わないようにするためには、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に対して警戒する必要がある。社内ルールの整備、組織全体で被害を防止するという体制作りも必要である。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を進めることが望ましい。

本四半期は、J-CSIP の参加組織から 12 件のビジネスメール詐欺について情報提供を受けた。この中で、タイプ 1（取引先へのなりすまし）は 2 件、タイプ 2（経営者等へのなりすまし）は 10 件であった。さらに、J-CSIP 外の一般企業・組織からも 11 件のビジネスメール詐欺の情報提供があった。

これら合計 23 件のうち、事例情報として公開許可の得られた 4 件の事例について表 3 に示す。なお、いずれの事例においても、すべて英文のメールであった。

本章では、表 3 の中から 2 件の事例を詳しく説明するとともに、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.	2020 年	10 月 30 日	2020 年 10 月、日本国内の企業の海外関連会社（支払側）に対して、攻撃者が海外の取引先企業（請求側）になりすまして、偽のメールを送りつけるビジネスメール詐欺が試みられた。	なし	本書:事例 1
2.		11 月 10 日	2020 年 11 月、日本国内の企業の CEO になりすました攻撃者が、同社の社員に対してビジネスメール詐欺を試みた。 偽のメールは、「年末が近づいており、債務者、未解決案件、担当者の詳細なリストが欲しいので個人的に連絡を取りたい。」といった内容が英文で書かれていた。 なお、メールの受信者は偽のメールへ返信はしておらず、金銭的な被害は発生しなかった。	なし	－
3.		11 月 11 日	2020 年 11 月、日本国内企業の海外関連会社（請求側）になりすました攻撃者が、海外の取引先企業（支払側）へ偽のメールを送り付けるビジネスメール詐欺が試みられた。	なし	本書:事例 2
4.		12 月 1 日	2020 年 11 月、日本国内の企業の CEO になりすました攻撃者が、同社の社員に対してビジネスメール詐欺を試みた。 なお、メールの受信者は偽のメールへ返信はしておらず、金銭的な被害は発生しなかった。	なし	－

3.1 事例 1 海外関連企業を狙った攻撃

本事例は、2020 年 10 月、J-CSIP の参加組織の海外関連企業（A 社：支払側）と、その海外取引先企業（B 社：請求側）の間で取引を行っている中で、攻撃者が B 社の担当者になりすまし、偽のメールを送り付けてきたものである。

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、支払側である A 社の担当者が、偽メールの差出人メールアドレスのドメイン名が偽物であることに気づくことができたため、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）A 社と B 社のやりとりへの介入
（2）詐称用ドメインの取得と悪用
（3）メール本文中の署名の改変

（1）A 社と B 社のやりとりへの介入

A 社（海外関連企業）と、B 社（海外取引先）との間で、取引に係るビジネスメールをやりとりしている中で、B 社の担当者が「発注書の支払い時期を尋ねる」目的のメールを、A 社担当者に送付した。その数時間後、攻撃者は支払の保留を要求する偽のメールを A 社担当者へ送信してきた。直前のやりとりから間を置かずに送られたことと、偽のメールには直前のメール文面が引用されていることから、攻撃者は何らかの方法でメールを盗み見ていたものと考えられる。

A 社担当者は、攻撃者から送られた偽のメールの差出人のメールアドレスのドメインが偽物であることに気づき、メールの宛先（To）を正しい B 社担当者のメールアドレスに修正したうえで、偽のメールが送られた旨を連絡した。

攻撃者から送られた偽のメールには、両社の関係者のメールアドレスも設定されていたが、同報先（CC）にあった B 社の関係者のメールアドレスもまた、偽のドメインのものに置き換えられていた。このことに気づかなかった A 社担当者は、同報先までは修正せずに送付したため、攻撃者に対しても、偽のメールに気づいたことを知らせてしまっていたことになる。

これ以降、攻撃者とのメールのやりとりはなかった。

本件では、「攻撃に気付いたことが攻撃者に知られた」ことによる問題は特に無かったようであるが、攻撃者が証拠を消したり、破壊的な行動に出たりといった可能性がありえるため、知られないように対応することが望ましい。

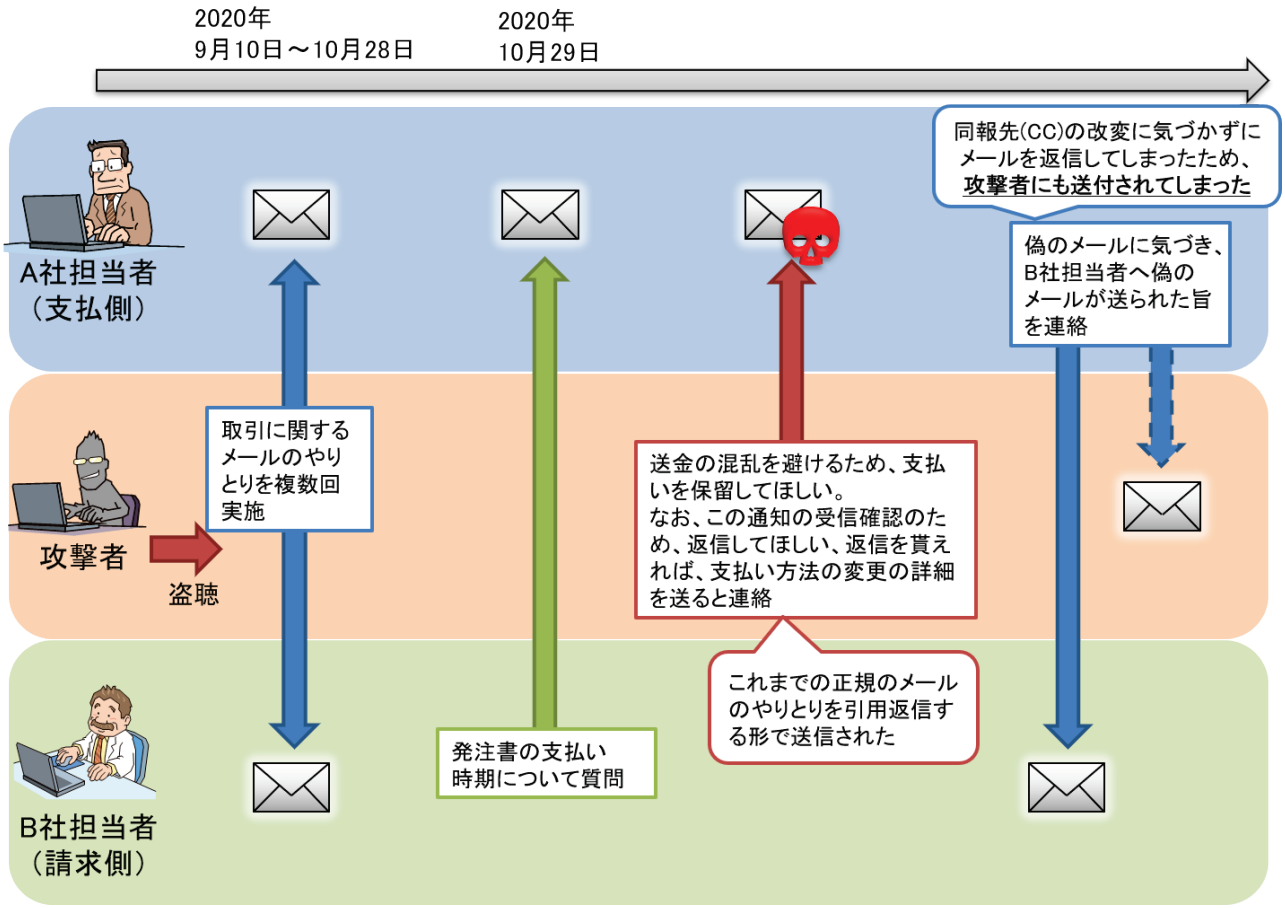

図 2 事例 1 攻撃者とのやりとり

(2)詐称用ドメインの取得と悪用

攻撃者からA社担当者へ送ったなりすましメールでは、差出人(From)と同報先(CC)に設定されていた、B社の正規のドメインに似通った「詐称用ドメイン」を、新規に取得して送り付けてきた。

詐称用ドメインは、次の例に示すようなものであった。

【本物のメールアドレス】alice @ b-company . co . jp
【偽物のメールアドレス】alice @ b-company - jp . co
(トップレベルドメインとサブドメインを入れ替え、「.」を「-」に変更)

※実際に悪用されたものとは異なる。

なお、メールの同報先には、A社とB社双方の関係者のメールアドレスが設定されていたが、なりすましメールではB社の関係者のメールアドレスのみ詐称用ドメインに改変されて、A社担当者へ送られていた。この手口により、B社の関係者には偽のメールが届かないため、詐欺が行われていることに気づかれにくくする狙いがあったものと考えられる。

(3)メール本文中の署名の改変

攻撃者からＡ社担当者に送られたなりすましメールでは、メール本文中の署名部分の一部が改変されていた。本来のＢ社担当者からのメールでは、署名に自身のメールアドレスが含まれていたが、攻撃者から送られてきたメールでは、署名からメールアドレスが削除されていた。

これは意図的な改変であることは明らかで、偽のメールアドレスを使用してＢ社担当者になりすましていることに気づかれにくくする目的があったものと考えられる。

3.2 事例 2 海外の取引先企業を狙った攻撃

本事例は、2020 年 11 月、J-CSIP の参加組織の海外関連企業（A 社：請求側）と、その海外取引先企業（B 社：支払側）との間で取引に関するやりとりを行っている中で、攻撃者が A 社の担当者になりすまし、支払日の予定について質問する偽のメールが送られたものである。

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、攻撃者から B 社担当者へ送られたメールの同報先（CC）に、A 社の共有メールアドレスが設定されており、この共有メールアドレスに騙られた A 社担当者も含まれていたことから、偽のメールが送られていることに A 社担当者が気づくことができたため、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）A 社と B 社のやりとりへの介入
（2）正規のメールアドレスに似せたフリーメールアドレスの使用

（1）A 社と B 社のやりとりへの介入

本事例では、A 社（海外関連企業）と、その取引先である B 社（海外取引先）との間で、取引に関するメールのやりとりを行っていた。このメールのやり取りの中で、支払にかかるタイミングを見計らい、2020 年 11 月 9 日、攻撃者が「支払いの予定日はいつか、今週中に決めてほしい」というメールを送り付けてきた。攻撃者は何らかの方法でメールのやりとりを盗み見ていたものと考えられる。

攻撃者から B 社に送られたメールの同報先（CC）には、A 社の共有メールアドレスが含まれていた。本来であれば B 社担当者のみに偽のメールを送り付けるのがビジネスメール詐欺の常とう手段であるのだが、この偽メールは同報（CC）により A 社にもメールが着信していた。これは、**攻撃者がミスをした**ものと推測している。

このメールが攻撃者から送られてきたものだと気づいていない B 社の担当者は、偽メールへの返信で「今週中に連絡をする」という旨のメールを返信してしまった。なお、このメールの同報先（CC）にも A 社の共有メールアドレスが設定されていたため、同様に A 社にも着信した。

この共有メールアドレスには、攻撃者がなりすましをしている最中の A 社の担当者自身も含まれていたことから、一連のメールを確認した A 社担当者が偽のメールに気づくことができ、事案が発覚した。その後、A 社では関係者に対して本事案の注意喚起を行った。

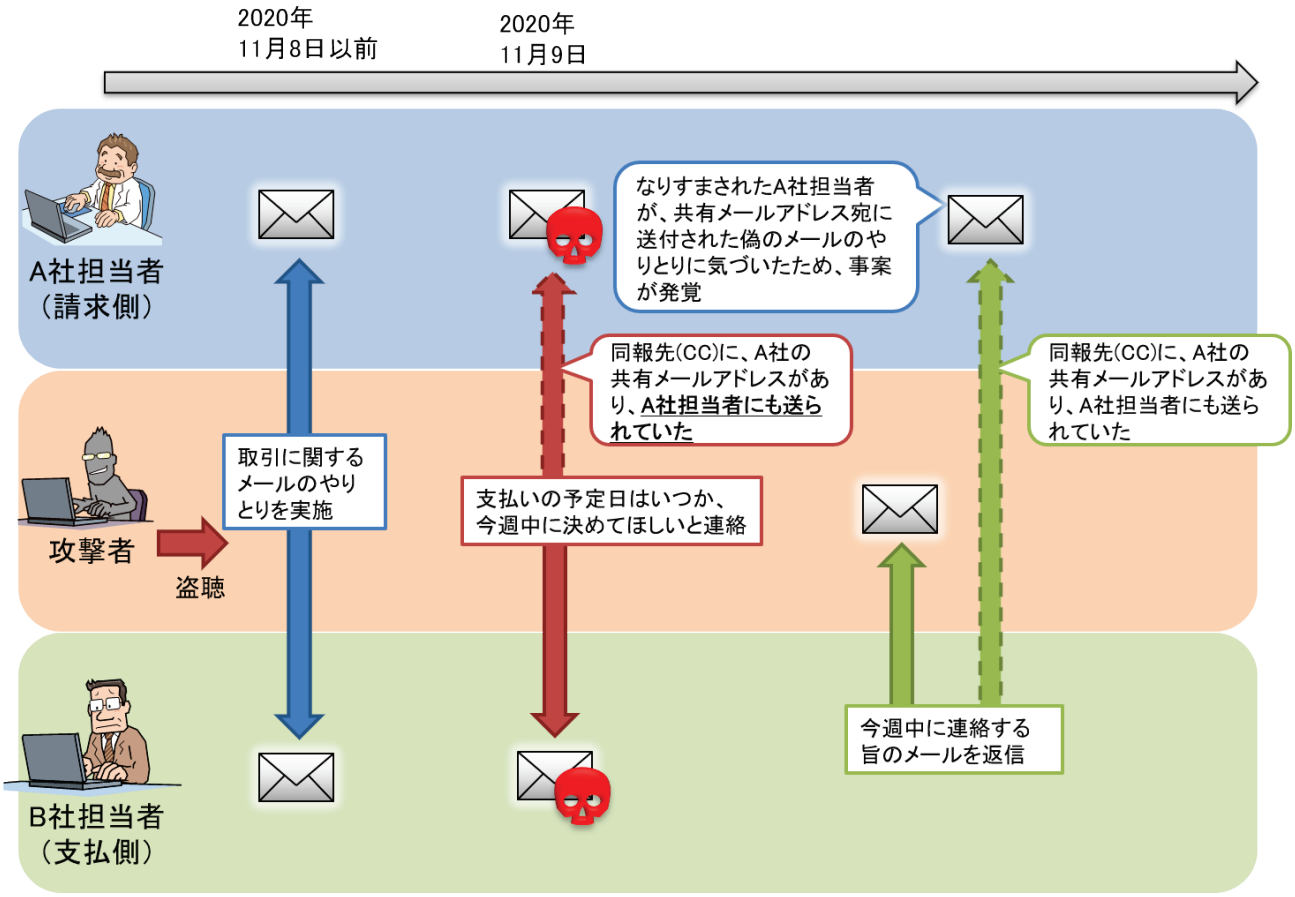

図 3 事例 2 攻撃者とのやり取り

(2)正規のメールアドレスに似せたフリーメールアドレスの使用

攻撃者は、B 社になりすましメールを送る際に、A 社のメールアドレスに似たフリーメールアドレスを取得し、その偽のメールアドレスを返信先（Reply-To ヘッダ）へ設定していた。

【本物のメールアドレス】alice @ a-company . co . jp
【偽物のメールアドレス】alice a-compeny . co . jp @ freemail . com

※実際に悪用されたものとは異なる。

なお、返信先（Reply-To ヘッダ）の表示名には、正規の A 社担当者のメールアドレスが設定されていたため、B 社担当者がメールの返信ボタンをクリックした場合、メーラでは本物のメールアドレスが表示される。

また、本件の攻撃で使われたフリーメールアドレスは、海外の「mail.com[7]」というサービスで取得されたものであった。このサービスで取得可能なフリーメールのドメインは、191 ドメインがあることが確認されており、これらの中には過去ビジネスメール詐欺で使われたことのあるフリーメールドメインが複数存在している。

[7] Mail.com
https://www.mail.com/consentpage

3.3 事例 3 複数組織へ行われた CEO を詐称する一連の攻撃（続報）

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、本四半期も継続して J-CSIP 参加組織から情報提供があった。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 **8 件**（2019 年 10 月～12 月期では 62 件、2020 年 1 月～3 月期では 46 件、2020 年 4 月～6 月期では 50 件確認、2020 年 7 月～9 月期では 7 件）の類似するメール検体を入手した [8]。

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 [9]。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（経営者、役員、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。（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」等という単語と、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多く観測されている（天体以外のケースも観測している）。
- 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 [10]、スペイン語、フランス語のメールを確認している。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 12 月 16 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 [11]が多かったが、2020 年 5 月 20 日以降のメールでは、「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」という変化があり、2020 年 11 月以降は、規制の再導入やワクチンといった文言も使うように、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」が入るものも観測されるようになった。

---

[8] 本事例については、本レポート執筆時点である 2021 年 1 月 4 日までの情報で記載している。

[9] 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/

[10] 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。

[11] 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

- 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 12 月 16 日である。

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、注意が必要である。

なお、本四半期では本件と同等のビジネスメール詐欺の観測数は大きく減少している。本件の攻撃について、攻撃者がさらに標的を絞っているのか、あるいは攻撃を観測できていないだけなのかは不明である。

表 4 事例 1 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.	建設業	2020/10/21	Project Lancelot	smtp-outbound-vulcan@secure-server-gateway.cc
2.	製造業	2020/10/22	Project Clementine	不明
3.	製造業	2020/11/18	Project Bravestar	asia-smtp-outbound-1@gateway-resolver.cc
4.	金融業, 保険業	2020/11/26	Project Pegasus	不明
5.	金融業, 保険業	2020/11/26	Project Pegasus	不明
6.	金融業, 保険業	2020/11/26	Project Pegasus	eu-smtp-outbound-apollo@intranetserver.net
7.	製造業	2020/12/10	Project Argessa	tls-us-1-outbound@intranet-server.cc
8.	製造業	2020/12/16	Project Triton	smtp-asia-1-outbound@intranet-server.cc

3.4 事例 4「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[12]。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 **13 件**（2020 年 3 月末時点では 7 件、2020 年 4 月～6 月期では 25 件確認、2020 年 7 月～9 月期では 8 件）の類似するメール検体を入手した[13]。

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。

- 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様々に異なるが、命名に規則性がある。具体的には、送信元や、返信先メールアドレス（From ヘッダや Reply-To ヘッダ）で、「board」や「board-1」、「relay」、「smtp」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。
  - メールに返信をすると、外国企業買収のため、外部の弁護士と協力して支払いを実施してほしいという旨のメールが攻撃者から送られてくる。
  - 1 通目のメールに返信をしたところ、攻撃者は実在する弁護士を騙り、連絡手段を教えてほしいといった旨のメールを送ってくることが確認されている。
- 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 12 月 15 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[14]。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。
  - 攻撃者が意図的にビーコンを仕掛けているのかは不明だが、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、これまでに複数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。

---

[12] 【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

[13] 本事例については、本レポート執筆時点である 2021 年 1 月 4 日までの情報で記載している。

[14] 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。

事例 1 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。

表 5 事例 2 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	2020/07/28	Finance M&A	board@oxs-1.host
2.	卸売業、小売業	2020/10/13	金融合併と買収につきまして	relay2@iphonemobile-outlook.com
3.	製造業	2020/10/27	金融合併と買収につきまして	relay2@secure-by-sec.com
4.	石油・石炭製品製造業	2020/10/8	金融合併と買収につきまして	smtp@iphonemobile-outlook.com
5.	製造業	2020/11/03	Liaise with external counsel	secure@ssl-365.com
6.	製造業	2020/11/13	Project Recovery	board-1@e-email.host
7.	情報通信業	2020/11/20	Finance M&A	relay3@secured-by-sec.com
8.	製造業	2020/11/3	金融合併と買収につきまして	relay2@secured-by-sec.com
9.	製造業	2020/11/3	金融合併と買収につきまして	relay2@secured-by-sec.com
10.	製造業	2020/11/3	金融合併と買収につきまして	relay2@secured-by-sec.com
11.	建設業	2020/12/07	Finance M&A	relay@secured-by-sec.com
12.	卸売業、小売業	2020/12/10	Finance M&A	relay@secured-by-sec.com
13.	卸売業、小売業	2020/12/15	Liaise with counsel	secure@365-outlook.online

4　VPN 装置の脆弱性を悪用した攻撃の検知

2020 年 12 月 15 日、国内組織で運用中の Cisco 製の VPN 装置に対して、インターネット側から設定ファイルを読み込む行為の通信を検知したという情報提供があった。本章では、悪用が試みられた脆弱性の内容とともに、対策について説明する。

本件の概要

本件は、VPN 装置の脆弱性の悪用を企図した攻撃であり、攻撃元の IP アドレスについては、過去多数のサーバに対するポートスキャン行為や、本件の脆弱性とは別の脆弱性の悪用を企図した攻撃が行われていることが、公開情報上で確認できている。

- 事象発生日：2020 年 12 月 14 日（月）
- 攻撃元 IP アドレス：5.189.162[.]164

本件の脆弱性

本件で確認された脆弱性は、Cisco 適応型セキュリティアプライアンス（ASA）ソフトウェアおよび Cisco Firepower Threat Defense（FTD）ソフトウェアのウェブインターフェイスに対し、認証されていないリモートの攻撃者が、ディレクトリトラバーサルによる攻撃を行うことで、ターゲットシステムの機密ファイルを読み取る可能性があるというものであった（CVE-2020-3452）[15]。

当該脆弱性については、事象発生時点で脆弱性を悪用するためのコード（PoC）が公開されている状態であった。

なお、情報提供元組織では、本脆弱性の悪用による被害等は確認されなかった。

脆弱性の対策

本件も含め、脆弱性のある装置やソフトウェアに対する根本的な対策は、「修正プログラムの適用」や「脆弱性が対策されたバージョンへのアップグレード」である。VPN 装置のような事業活動の基盤となる機器については、業務上すぐに修正プログラムを適用することが難しい場合があるが、攻撃者が待ってくれるわけでもない。脆弱性対応計画の策定や、それに応じたリソースの確保が必要である。

多数のセキュリティ関係機関から注意喚起がなされているところであるが、本件で試みられたような、VPN 装置の脆弱性を悪用した組織内ネットワークへの侵入の手口は、最近の標的型攻撃や、ランサムウェア攻撃 [16]の主要な手口となっている。

改めて、インターネットからアクセス可能な機器等の確実な洗い出しと、それらへ適切な脆弱性対策が行われているか確認していただきたい。

---

[15] Cisco 適応型セキュリティ アプライアンス ソフトウェアおよび Firepower Threat Defense ソフトウェアの Web サービスの読み取り専用パストラバーサルの脆弱性（Cisco）
https://www.cisco.com/c/ja_jp/support/docs/csa/2020/cisco-sa-asaftd-ro-path-KJuQhB86.html

[16] 【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について（IPA）
https://www.ipa.go.jp/security/announce/2020-ransom.html

5　架空の組織を騙るコロナ禍に乗じた日本語の不審メール

本四半期、国内の組織に対して送られた日本語の不審メールについての情報提供があった。本章では、実際に情報提供された攻撃メールの例を含め説明する。

不審メールの内容

2020 年 12 月 3 日、J-CSIP の参加組織から、日本語の不審メールが着信したという情報提供を受けた（図 4）。このメールには、添付ファイルや本文中の不審な URL リンク等もなく、メール単体で被害を及ぼすような仕掛けはなかった。差出人は架空の組織が騙られており、メールの件名や本文では「社会情勢悪化」「臨時助成制度」といった単語が使われつつ、全体的に不自然な点の少ない内容となっている、コロナ禍に乗じた不審メールであった。

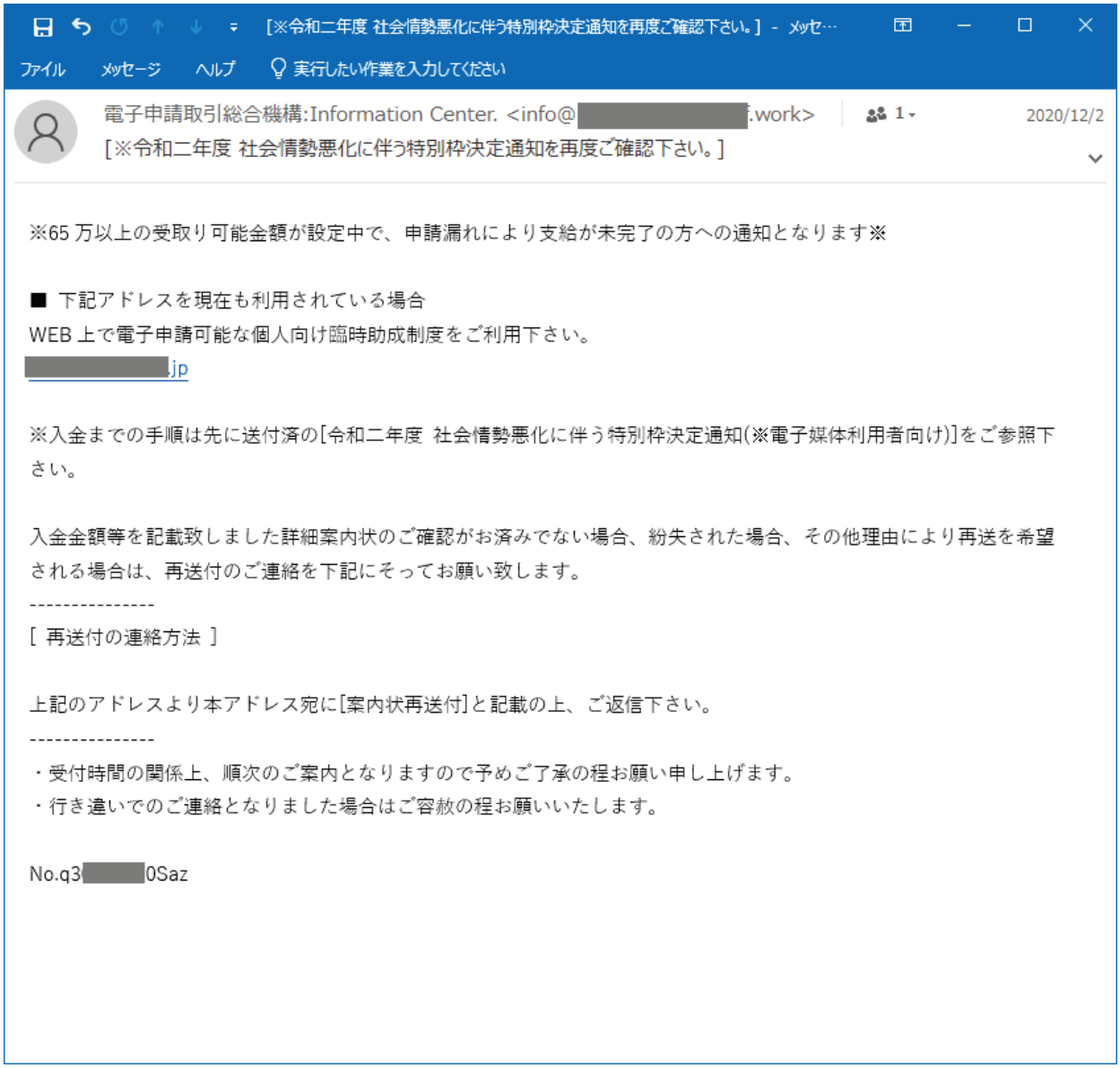

図 4 2020 年 12 月 3 日に情報提供があったメール

本件についてJ-CSIP内で情報共有したところ、いくつかの参加組織から同様の不審メールが着信しているという情報提供があった（図 5、図 6）。

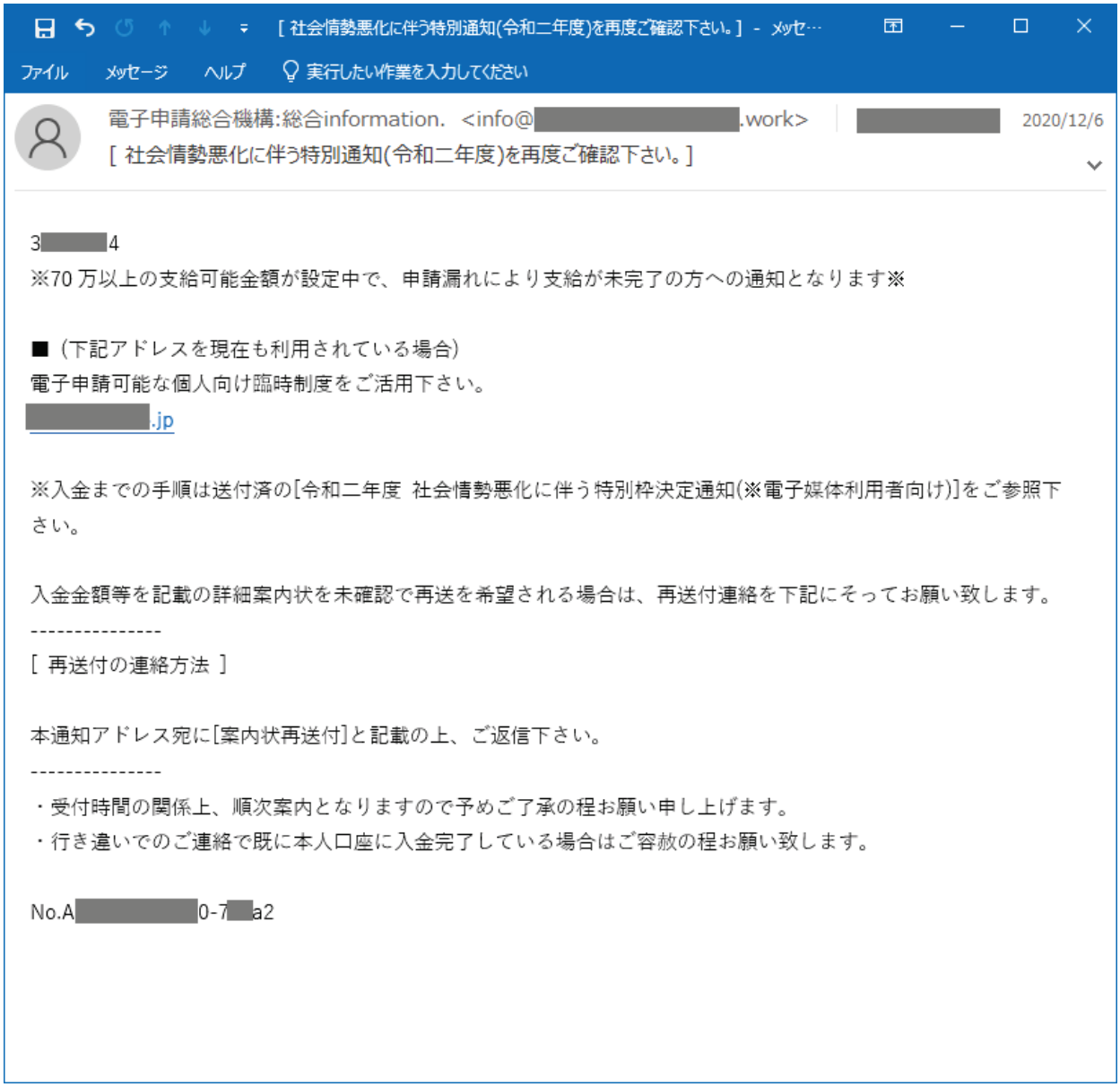

図 5 他の参加組織から情報提供された類似メール（1）

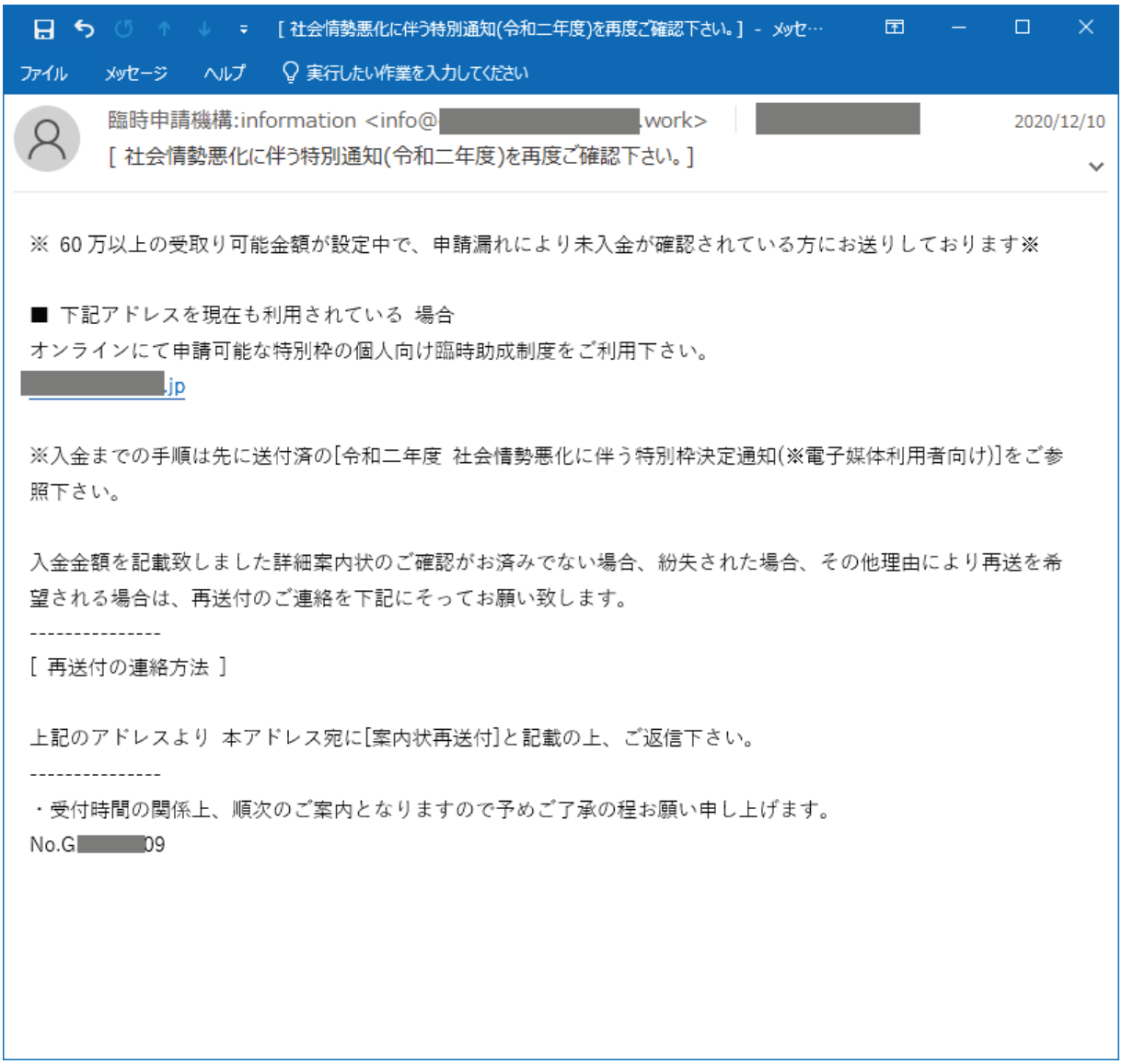

図 6 他の参加組織から情報提供された類似メール(2)

これらの情報提供から、「電子申請総合取引機構」「電子申請総合機構」「臨時申請機構」という詐称をしているパターンが確認できた。また、組織によって着信していた通数や着信日にばらつきがみられたほか、何らかの料金が未納であるといった内容と思われるものもあった。

本件に類似した不審メールについて、インターネット上では注意喚起などの情報があまり見られないものの、ある程度、広く無差別に送信されていた可能性がある。本メールの意図は何らかの詐欺ではないかと思われるが、不明である[17]。

[17] 本件の不審メールとの関連は不明であるが、総務省を騙るメールについては 10 月に注意喚起があった。
特別定額給付金の給付を騙ったメールに対する注意喚起(総務省)
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html

不審メールの特徴と着信時期

本件の不審メールは、差出人（From）メールアドレスに、次のような特徴があることが分かっている。

- 差出人（From）メールアドレス： info@【ランダムと思われる英字文字列】.work

J-CSIP 内では、最終的に合計 185 件の類似メールについて情報提供があった。件名ごとの着信件数について表 6 に示す。また、不審メールの着信日と件数の推移について図 7 に示す。

表 6 件名ごとの着信件数

項番	件名	着信件数
1.	（■ WEB 契約の更新・継続について）	1
2.	[社会情勢悪化に伴う特別通知(令和二年度)を再度ご確認下さい。]	6
3.	[※令和二年度 社会情勢悪化に伴う特別枠決定通知を再度ご確認下さい。]	6
4.	[令和二年度 社会情勢悪化に伴う特別枠通知を再度ご確認下さい。]	1
5.	≪WEB 契約の更新・継続について≫	62
6.	■ WEB 契約の更新 継続について ■	13
7.	□ WEB 契約の更新/継続について □	57
8.	■情報開示手続きを経た電子告知	1
9.	※ WEB 契約の更新 継続について ※	1
10.	入会 済 番組の継続/解約の確認通知	37

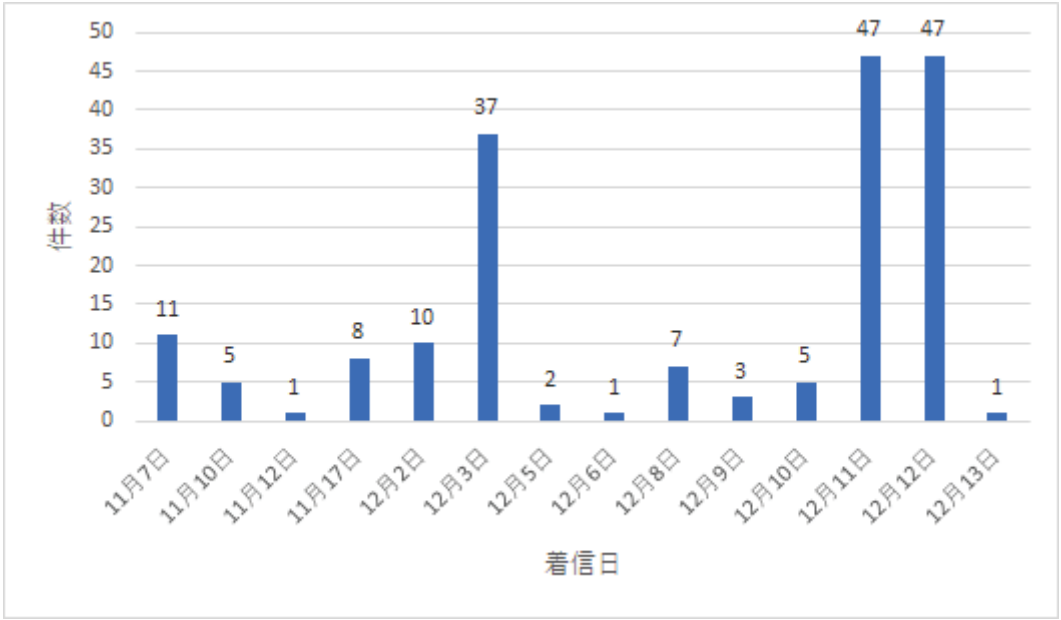

図 7 不審メールの着信日と件数の推移

今後も、コロナ禍に乗じた攻撃が懸念されるところ、継続して注意していただきたい。

6　遠隔操作ウイルスが添付された日本語の攻撃メール

2020 年 10 月と 11 月、日本語の攻撃メールについて情報提供があった。添付されていたウイルスは、これまで一部のばらまき型メールでも観測されていた遠隔操作ウイルス（RAT）であるものの、攻撃が行われた規模は不明である。本章では、この日本語のウイルスメールについて説明する。

2020 年 10 月に確認されたウイルスメール

2020 年 10 月 6 日、J-CSIP の参加組織より、日本語のウイルス付きメール（図 8）について情報提供があった。本件の攻撃メールについて情報共有したところ、別の参加組織からも同等の攻撃メールの着信が確認されたと情報提供があった。

メールの日本語は簡素ながら、不自然な点は少なかった。実在する企業の情報が署名部分に記載されており、この内容に心当たりが無くとも、本物の見積もり依頼のメールに見え、添付ファイルを開いてしまう可能性があると思われる。

メールには zip 形式の圧縮ファイルが添付されており、解凍すると実行形式（exe）のファイルが格納されている。この実行形式のファイルを開くと（実行すると）、遠隔操作ウイルスに感染させられてしまう。

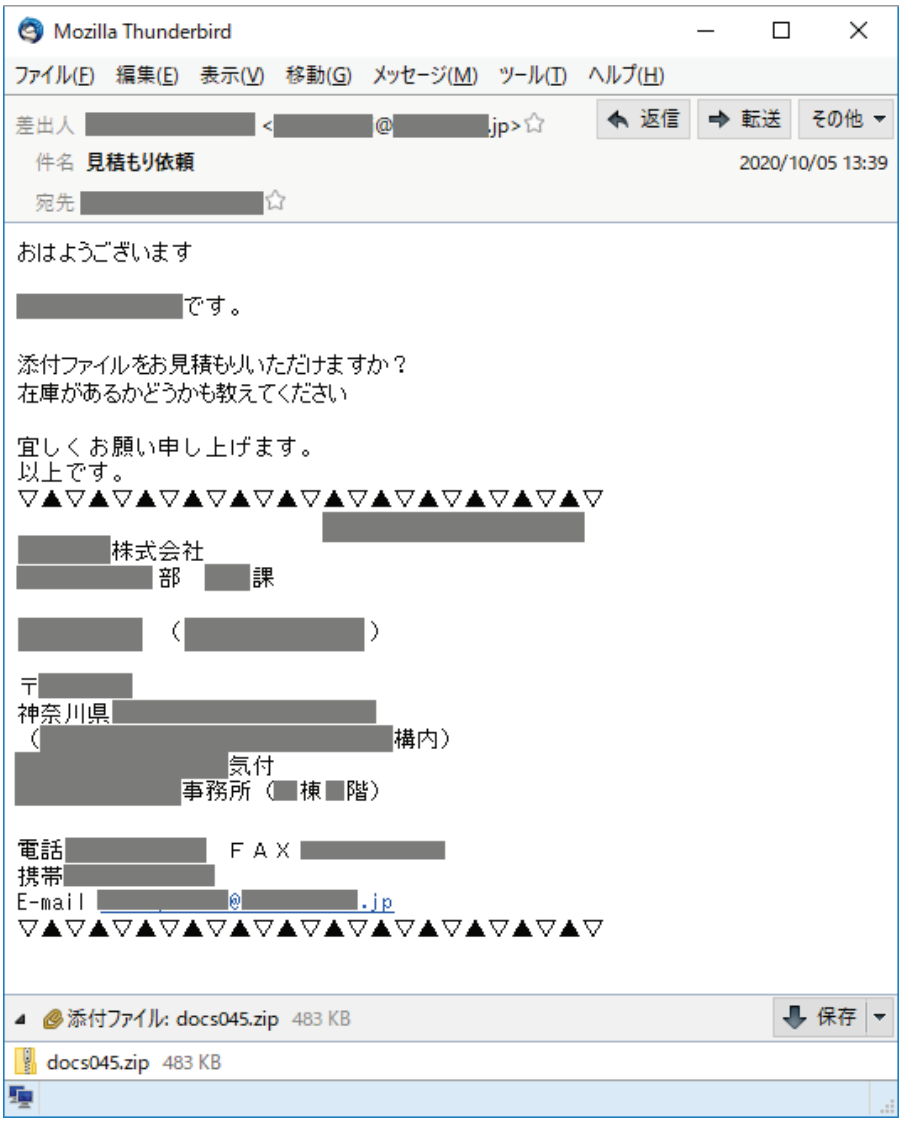

図 8 2020 年 10 月に確認されたメール

2020 年 11 月に確認されたウイルスメール

2020 年 11 月 16 日、J-CSIP の参加組織より、10 月に確認されたウイルスと同等のウイルスが添付された、別の日本語の攻撃メール（図 9）について情報提供があった。10 月のウイルスメールと比べ、更に簡素な内容であったが、同様に見積り依頼を装っていること、同等のウイルスが使われていることから、同じ攻撃者による攻撃だと考えられる。

本件の攻撃メールについても、J-CSIP 内で情報共有を行ったところ、同様に別の参加組織でも同等の攻撃メールの着信が確認された。

こちらのメールも、zip 形式の圧縮ファイルが添付されており、解凍すると Microsoft Excel のアイコンに偽装した実行形式（exe）のファイルが格納されている。この実行形式のファイルを開くと（実行すると）、遠隔操作ウイルスに感染させられてしまう。

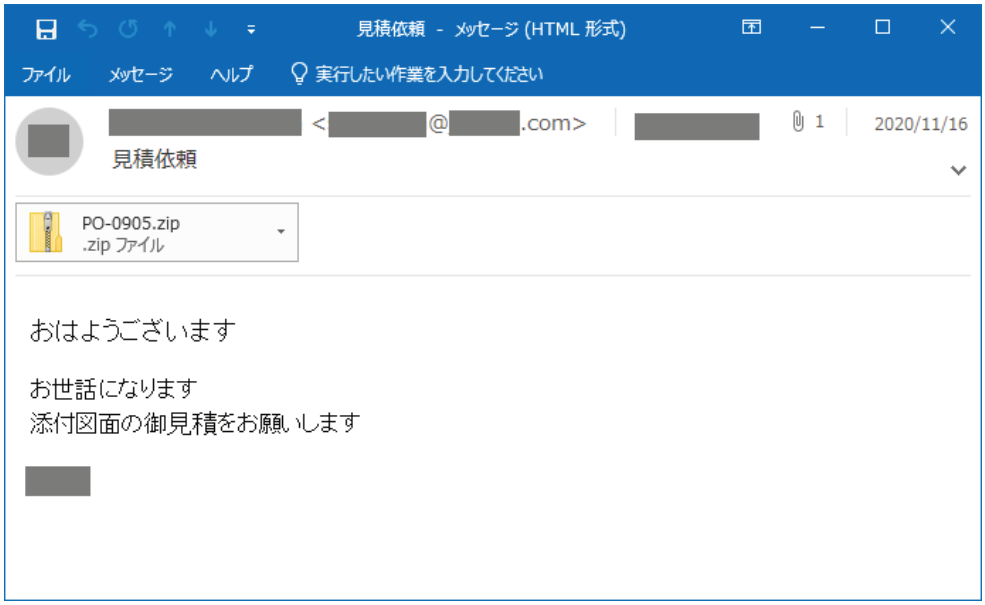

図 9 2020 年 11 月に確認されたメール

この 2 件のウイルスメールについて、現時点では数組織で着信を確認しており、一部は公開情報上にも同等のメールに関する情報がある。業界の偏りがないことから、本件は、国内企業へある程度の規模でばらまくように攻撃が行われたものと推測している。

ウイルスに感染させられてしまった場合、そのパソコン等を足掛かりとして組織内ネットワークへ侵入される可能性があり、注意が必要である。

7　Zoom ミーティングの招待メールを装うフィッシングメール

2020 年 10 月 5 日、Zoom ミーティングの招待メールを装ったフィッシングメールが着信したという情報提供があった。本章では、実際に攻撃に使われたフィッシングメールを踏まえ説明する。

攻撃者から送られたフィッシングメールは単純なもので、ミーティングのために本文中の URL リンクをクリックさせるように誘導する内容であった（図 10）。この URL をクリックすると、不正なウェブサイトへ誘導されるものと考えられる（情報提供時点で、URL リンク先にはアクセスができない状態であった）。

新型コロナウイルス感染症（COVID-19）の影響で、企業や組織でのオンライン上でのミーティングが増えてきている中、このような実在するビデオ会議システムの通知を悪用したフィッシングメールについては、今後も注意が必要であろう。

フィッシング詐欺への対策は、利用者ひとりひとりが、攻撃手口を知り、騙されないように注意し、偽のウェブサイトで情報を入力しないことが重要であり、そのためには継続的な啓発が必要である。

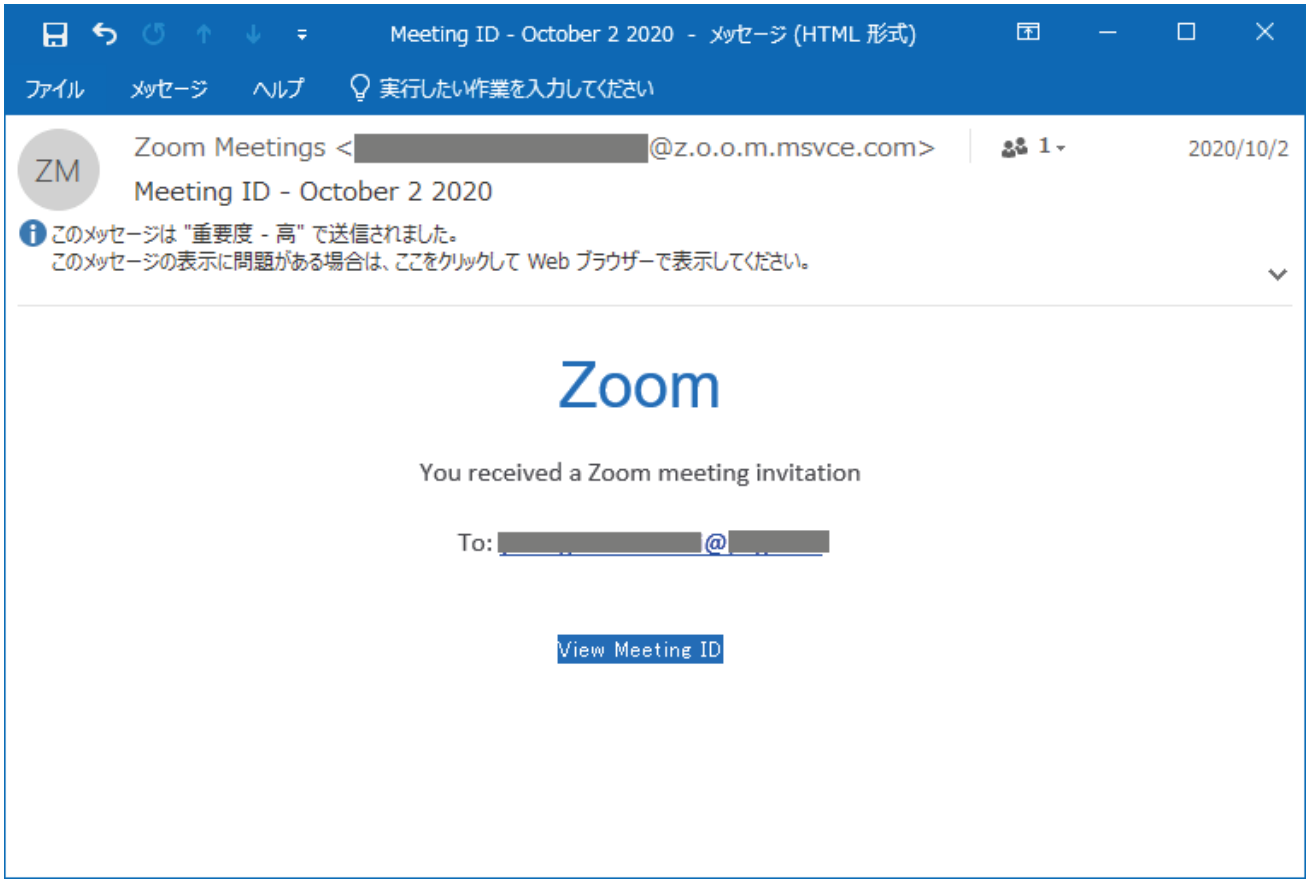

図　10 Zoom ミーティングの招待を装うフィッシングメール

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