サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2022 年 1 月～3 月]

2022 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

サイバー情報共有イニシアティブ（J-CSIP）[1]について、2022 年 3 月末時点の運用体制、2022 年 1 月～3 月の運用状況を報告する。1 章、2 章は全体状況を、3 章は 2021 年度の活動状況、4 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

2022 年 1 月～3 月期（以下、本四半期）は、次の通り参加組織の変更があり、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）。

- 2022 年 3 月、ガス業界 SIG 内での追加に伴い、参加組織数が 62 組織から 79 組織となった。

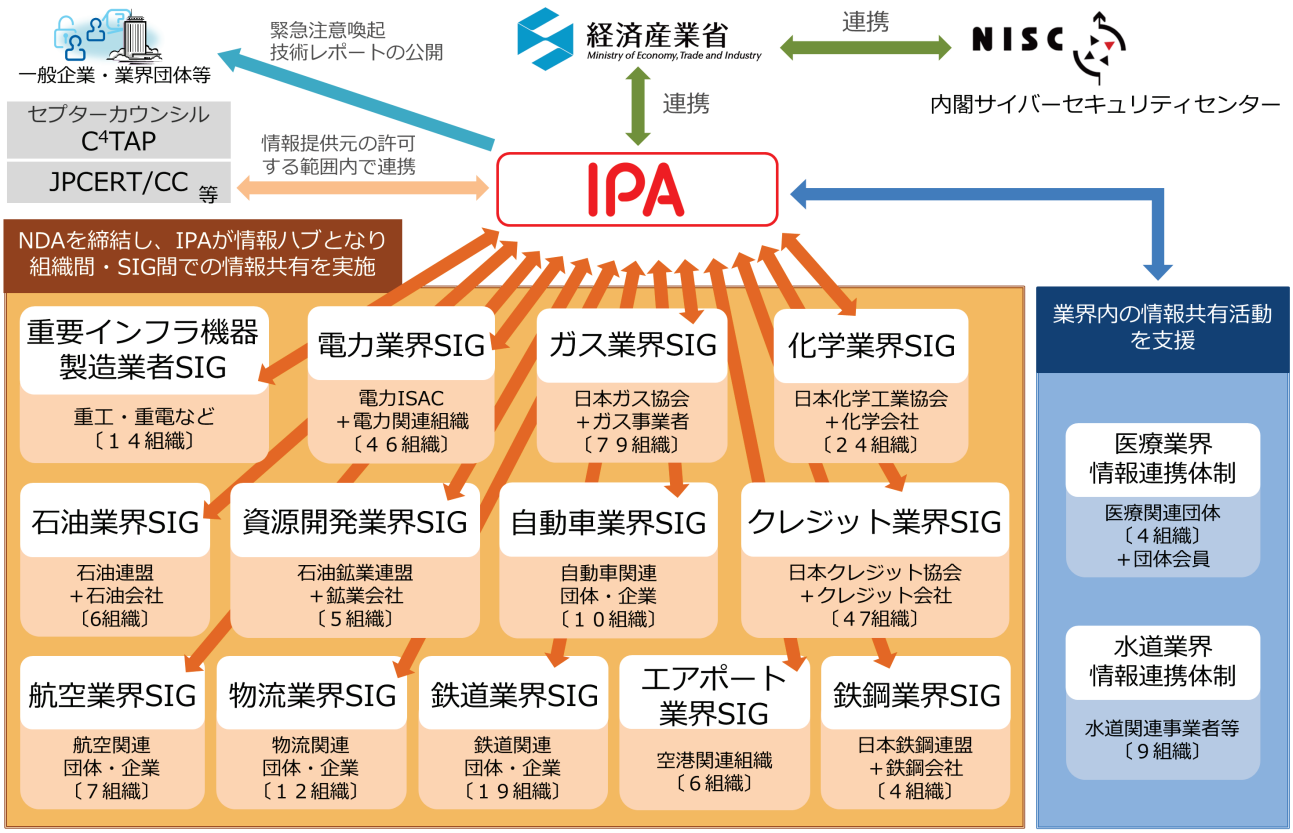

図 1 J-CSIP の体制図

[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（2022 年 1 月～3 月）

2022 年 1 月～3 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（3 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	2021 年			2022 年
		4 月～6 月	7 月～9 月	10 月～12 月	**1 月～3 月**
1	IPA への情報提供件数	369 件	346 件	77 件	**51 件**
2	参加組織への情報共有実施件数※1	40 件	21 件	28 件	**29 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 **20 件**を含む。

本四半期は情報提供件数が **51 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 **12 件**であった。

この他、次にあげるような情報提供があり、一部情報共有を行った。

- ビジネスメール詐欺が試みられたという情報提供が複数あった。この中には取引先を詐称するもの（タイプ 1）と、経営層を詐称するもの（タイプ 2）があった。さらに、J-CSIP 参加組織外の国内企業からビジネスメール詐欺が試みられたという相談もあった。これらについて 4 章で述べる。

- 参加組織の経営者を騙る FAX 文書を受信したという情報提供があった。具体的な文書の内容や攻撃手口について 5 章で述べる。

- 社外から持ち込まれた USB メモリをパソコンに接続したところ、不審な通信を検知したという情報提供があった。IPA で確認したところ、USB メモリ内にはウイルス感染を目的とするファイルがあった。情報提供元組織での対応経緯を含め 6 章で述べる。

- 参加組織にて、商材等を登録している BtoB サービスを経由した問い合わせがあり、問い合わせに対して返信したところ、フィッシングメールが送付されてきたという事例の情報提供があった。これについては 7 章で述べる。

- 本四半期も、前四半期から継続して、Emotet への感染を企図した攻撃メールが確認された。J-CSIP の参加組織内でも攻撃メールの着信が観測された。その中には、パスワード付き ZIP ファイルが添付された攻撃メールを着信した後に、パスワードを通知するメールが着信したという情報提供があった。IPA で確認したところ、攻撃者が 2 通に分けて攻撃を行った**ものではなく**、送信元組織で利用していた**メールシステムによって 2 通となっていた**ことが分かった。これについて 8 章で述べる。

このほか、情報提供に加え、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	標的型攻撃と考えられる不正アクセス被害を受けた	1 件
2	自組織に類似するドメイン宛のメール送信を検知するシステムを社内に導入したところ、複数の類似ドメイン宛のメールを検知した	1 件
3	セキュリティソフトによって正規のファイルや正規の通信と思われるものが検知された	4 件
4	組織内から送られてきたメールの添付ファイルがウイルスであると警告するメッセージが表示された	1 件
5	組織内からウェブシェルをダウンロードする通信を検知した	1 件

項番 1 は、J-CSIP の参加組織が不正アクセスを受け、組織内ネットワークに侵入されたと情報提供を受けたものである。その攻撃手口から、標的型攻撃であると判断している。提供された情報の一部について、J-CSIP 内で情報共有を行った。

項番 2 は、自組織に類似したドメイン宛のメール送信を検知・遮断する仕組みを社内で導入したところ、複数の類似ドメイン宛のメールを検知したと情報提供を受けたものである。これらは、いずれも社内の送信者による誤入力等によるものであった。しかし、検知した類似ドメインには MX レコードが設定されているものもあり、メール送信を遮断しなかった場合、情報漏洩に至る可能性があった。

ビジネスメール詐欺やフィッシングメール等で、攻撃者が企業の類似ドメインを取得し攻撃を行うこともあるため、自組織に類似したドメインの調査・メールを検知する仕組みを採ることは、未然に攻撃や情報漏洩を防ぐ意味でも有用といえる。

項番 3 は、セキュリティソフトにて正規と思われるファイルや通信が検知されたと情報提供を受けたもので、経緯等は異なるものの複数のケースが寄せられた。いずれの事例においても、セキュリティソフトによる過検知であったことを確認した。入手経緯やアクセス経緯等が明確ではあっても、ファイルが不正なプログラムに入れ替わっていたり、正規のアクセス先が改ざんされていたりするといった可能性を考慮し、このような警告が出た場合、無視せず調査・対応をすることが望ましい。

項番 4 は、社内から送られたメールを受信したところ、添付ファイルがウイルスであるという内容のセキュリティソフトの警告メッセージが表示されたと情報提供を受けたものである。IPA で確認したところ、添付ファイルは正規のファイルであったため、誤検知であろうと判断した。社内のメールアカウントから攻撃が行われる可能性もゼロではないため、このような場合でも調査対応する必要があると思われる。

項番 5 は、組織内の PC から不審な URL よりウェブシェルをダウンロードする通信を検知したと情報提供を受けたものである。IPA で調査した結果、あるウェブサイトが読み込む画像ファイルがウェブシェルに置き換えられており、利用者がブラウザからウェブサイトにアクセスしたため、検知されたものであった。当該ウェブサイトは、過去何らかの攻撃に関わっていたものと思われる。

ウェブシェルをダウンロードする通信は、攻撃者がウェブサーバへ侵入した後、バックドアを設置する際に発生することがある。今回は PC が通信元であったため問題は無かったが、このような通信を検知した際は、通信元のマシンをしっかりと調査する必要がある。

3　今年度の状況

3.1　今年度の取り扱い件数と年度毎の推移状況

J-CSIP における取り扱い件数（情報提供件数、標的型攻撃（メール、検体等）と見なした件数、情報共有実施件数）と参加組織数について、今年度（2021 年度）の合計と、J-CSIP を運用開始した 2012 年度から 2020 年度までの推移状況を次に示す（表 3、図 2）。

表 3 年間の取り扱い件数と参加組織数

項目	IPA への情報提供件数	標的型攻撃（メール、検体等）と見なした件数	参加組織への情報共有実施件数	参加組織数
2012 年度	246	201	160	5 業界 39 組織
2013 年度	385	233	180	5 業界 46 組織
2014 年度	626	505	195	6 業界 59 組織
2015 年度	1,092	97	133	7 業界 72 組織
2016 年度	2,505	177	96	7 業界 86 組織
2017 年度	3,456	274	242	11 業界 228 組織
2018 年度	2,020	213	195	13 業界 249 組織 ＋ 2 情報連携体制 13 組織
2019 年度	2,303	401	225	13 業界 249 組織 ＋ 2 情報連携体制 13 組織
2020 年度	6,202	125	147	13 業界 262 組織 ＋ 2 情報連携体制 13 組織
2021 年度	843	35	118	13 業界 279 組織 ＋ 2 情報連携体制 13 組織

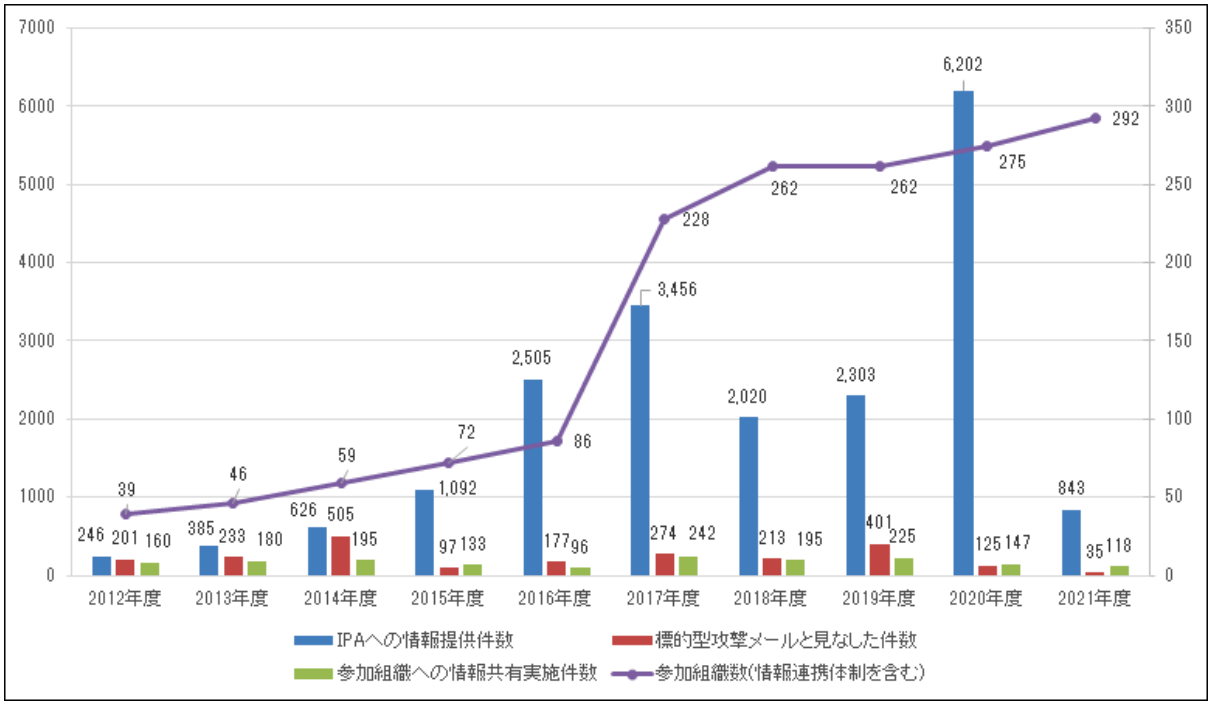

図 2 年間の取り扱い件数と参加組織数の推移

3.2 今年度の活動

2021 年度は、J-CSIP の参加組織数について、年度内での増減があり、最終的な参加組織数は 2020 年度から 17 組織増加した。

情報提供について、今年度は 843 件となった。昨年度に比べると大きく数を減らしているが、これは Emotet への感染を狙った攻撃メール等ばらまき型メールの情報提供が少なかったことと、これまで多く観測されてきた同一攻撃者と推測される CEO 等を騙る一連の攻撃メールの情報提供が少なかったためである。どちらの攻撃メールについても、J-CSIP の参加組織では継続して確認されているものの、各参加組織で導入しているメールフィルタ等のセキュリティ機能によって、利用者へ着信する前に防ぐことができているため、情報提供するまでの扱いに至っていないものと推察している。Emotet について、J-CSIP の多くの参加組織においては被害を未然に防ぐことができていると思われる。

しかしながら、ビジネスメール詐欺については 2021 年度も継続して情報提供を受けており、中には実際に金銭被害を受けたといった事例も確認している。引き続き動向に注視していく。

さらに、PowerPoint や Excel のアドインファイル、Windows のヘルプファイルを悪用した攻撃メールや、自衛隊の大規模接種センターを騙るフィッシングメール等、新たな手口を用いた不審なメールを観測しており、今後もメールを使った攻撃手口の変化には注意が必要である。

日本国内の特定の業界や組織を狙う標的型攻撃については、2021 年度でも提供件数は減少傾向にあるものの、組織内のネットワークに侵入されたという重要な事案を 2 件情報提供されており、依然として標的型攻撃自体は継続している状況であると考えられ、引き続き警戒していただきたい。

3.3 特筆事項

Emotet については、2021 年 1 月に EUROPOL（欧州刑事警察機構）が欧米 8 か国の法執行機関・司法当局の協力により、攻撃基盤をテイクダウン（停止）させたと報道 [3]があってからは観測されていなかったが、2021 年 11 月頃から、Emotet への感染を目的とした攻撃メールが国内で多数観測されている。J-CSIP 内でも 2021 年 11 月以降、Emotet への感染を目的とした攻撃メールについて継続して情報提供がある。

Emotet の攻撃の状況やウイルスメールに関する情報は IPA の他、JPCERT/CC をはじめ、多数のセキュリティベンダから情報が発信されている。J-CSIP 内では 2022 年 2 月には日本語で書かれた攻撃メールを確認しており、IPA でも相談件数が急増したため 2 月と 3 月に注意喚起を更新している。また、Emotet に感染しメール送信に悪用される可能性のある「.jp」ドメインのメールアドレス数は 2020 年のピーク時の約 5 倍以上に急増した [4]との情報もある。引き続き Emotet の攻撃メールはばらまかれる可能性があるため、基本的なウイルスメール対策を継続して徹底していくことが必要であろう。

その他、Microsoft365 等のアカウント情報を狙ったフィッシング攻撃も、前年度から引き続き情報提供されている。標的型攻撃に限らず、J-CSIP ではサイバー攻撃全般の情報共有を今後も進めていく予定である。

---

[3] 「World's most dangerous malware EMOTET disrupted through global action」（Europol）
https://www.europol.europa.eu/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action

[4] マルウェア Emotet の感染再拡大に関する注意喚起(JPCERT/CC)
https://www.jpcert.or.jp/at/2022/at220006.html

4　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、2020 年 4 月の 3 回にわたり IPA から注意喚起を行っているが、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、この脅威をビジネス関係者全体で認識し、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を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。また、2022 年 3 月にビジネスメール詐欺の手口と対策について、IPA で映像コンテンツを公開したため [5]、活用していただきたい。

本四半期は、J-CSIP の参加組織から 2 件のビジネスメール詐欺について情報提供を受けた。1 件はタイプ 1（取引先へのなりすまし）の攻撃で、もう 1 件はタイプ 2（経営者等へのなりすまし）であった。また、J-CSIP 参加組織外から 1 件のビジネスメール詐欺の相談があった。

本章では、開示許可の得られた事例について詳しく説明する。

[5] 映像で知る情報セキュリティ What's BEC ？ ～ビジネスメール詐欺 手口と対策 ～(IPA)
https://www.ipa.go.jp/security/keihatsu/videos/

4.1 事例の概要 ー 国内企業の海外子会社の取引先を狙った攻撃

本事例は、2021 年 5 月に、国内の企業の米国子会社（A 社：請求側）と欧州の取引先企業（B 社：支払側）との取引において、A 社の担当者になりすました攻撃者から、送金先の銀行口座の変更を依頼するメールが送られたものである。

本事例では、攻撃者からのメールを受信した B 社から A 社に対して、「最近銀行口座を変更したか」と問い合わせがあったことにより気づくことができたため、金銭的な被害は発生していない。

今回の事例で送付されたメールは、英文であった。

IPA への情報提供の経緯

A 社の親会社（C 社）から IPA へ連絡があった。米国子会社（A 社）の実在する担当者を騙り、送金先の銀行口座の変更案内を装う偽のメールが、取引先である B 社へ送られて困っており、対処方法について相談をしたいとのことであった。攻撃者から B 社へ同様のメールが 5 件以上送付されており、そのうちの 1 通のメールについて情報提供され、IPA で確認を行った。

本事例の関係者

本事例の関係者を次に示す。

表 4 本事例の関係者一覧

名前	説明
A 社	国内企業の米国子会社。請求側。
B 社	A 社と取引を行っていた欧州の企業。支払側。
C 社	A 社の親会社。本件を IPA へ情報提供した国内の企業。
攻撃者	A 社の担当者になりすまし、ビジネスメール詐欺によって B 社から金銭を詐取しようとした。

4.2　攻撃の流れ

2021 年 5 月に発生した、攻撃者からの偽の銀行口座への変更依頼に係る攻撃の流れ（図 3）を次に示す。

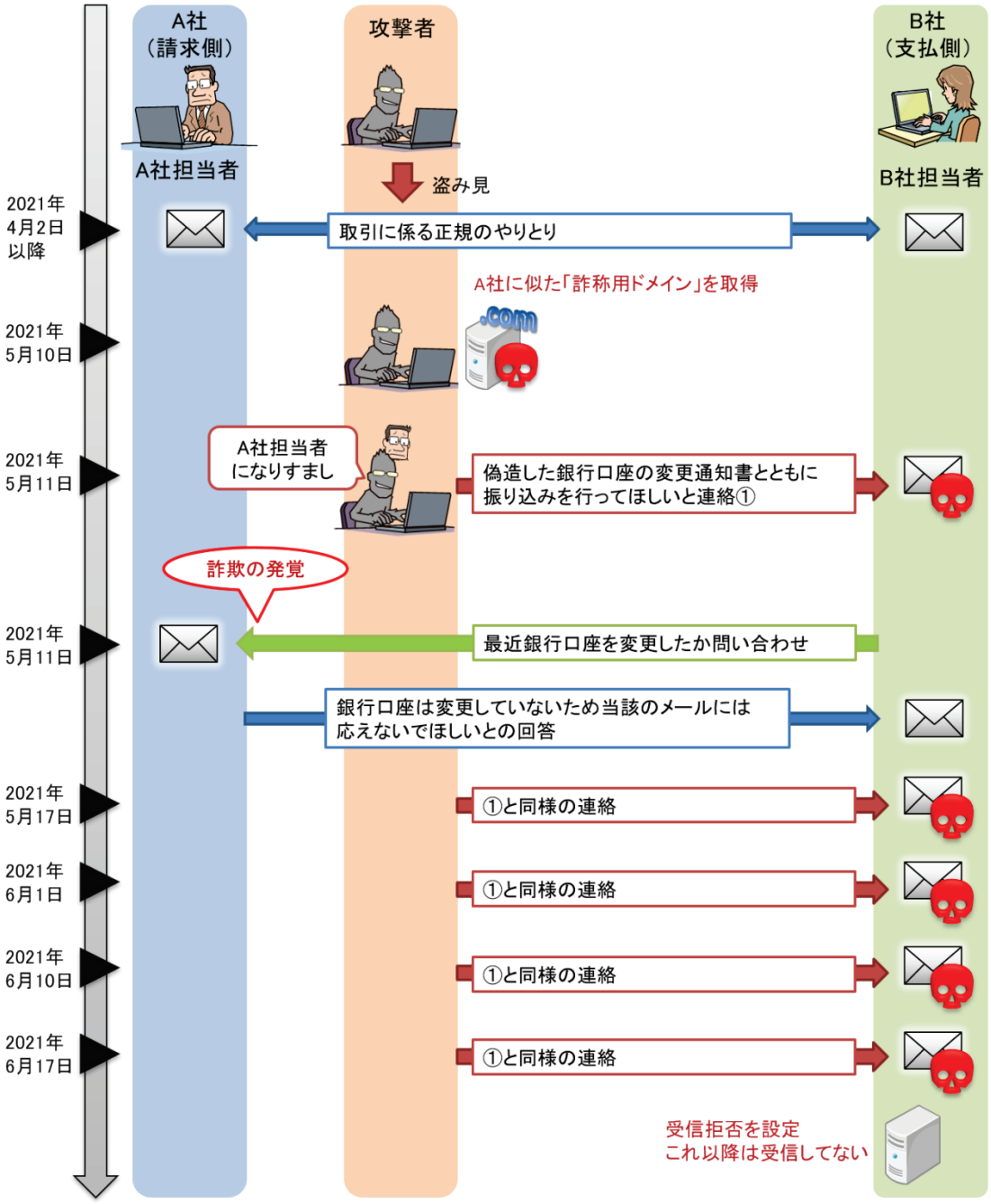

図 3 攻撃の流れ

2021 年 4 月 2 日より、A 社と B 社間で、取引や請求に関するメールのやり取りを行っていた。攻撃者は何らかの方法で、これらのメールを盗み見ていたと思われる。

2021 年 5 月 10 日、攻撃者は A 社のドメインに似た「詐称用ドメイン」を取得した。その翌日（5 月 11 日）、A 社の担当者になりすました攻撃者から B 社へ、偽の口座へ支払いを行うように依頼するメールが送られた（図 4）。メールには、送金先銀行口座に関する、偽造された変更通知書の PDF が添付されていた。

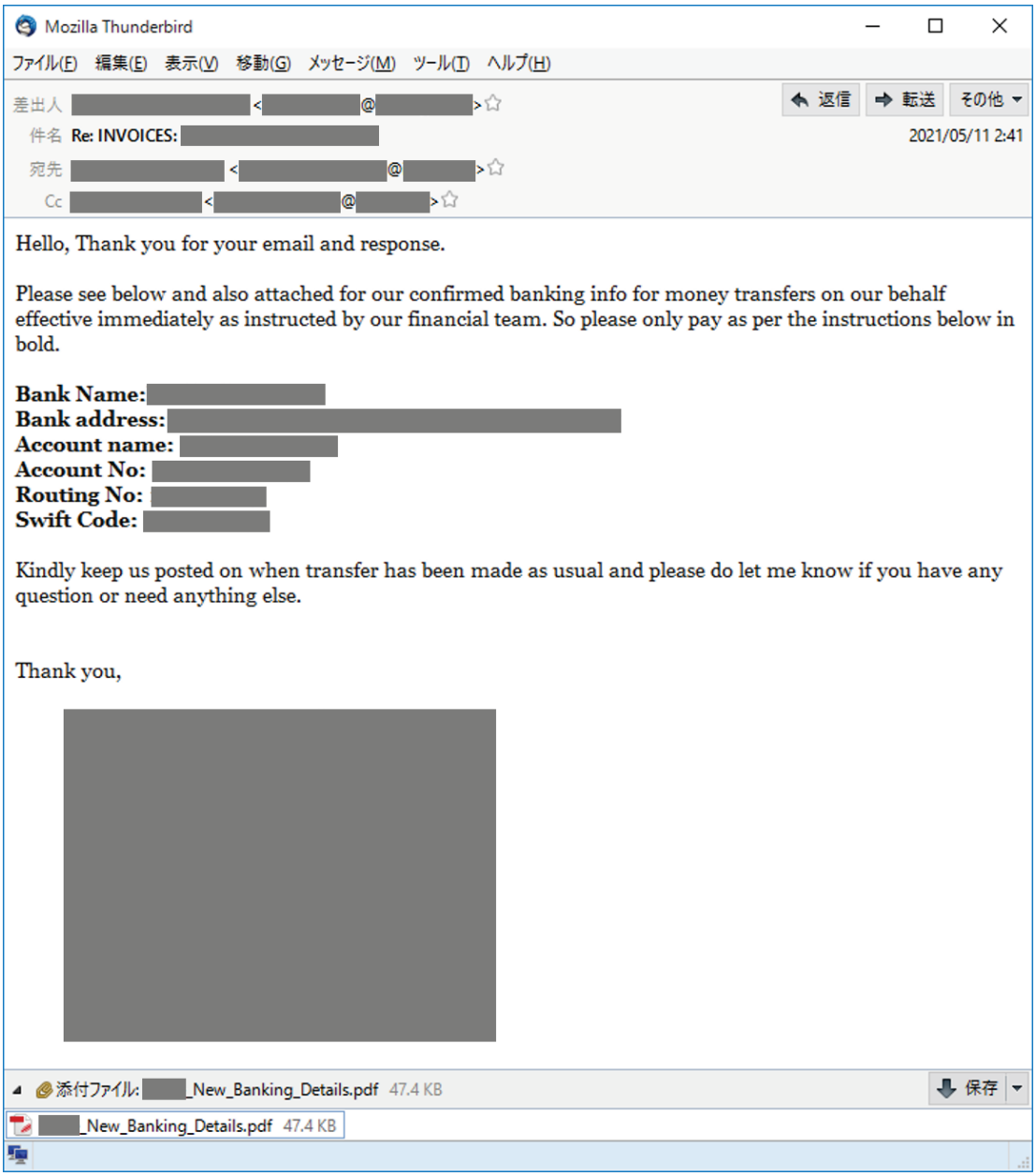

図 4 攻撃者からのメール（2021 年 5 月 11 日）

5 月 11 日、B 社から A 社にメールで「最近銀行口座を変更したか」という問合せがあり、A 社から B 社へ「銀行口座は変更していないため、当該のメールには応えないでほしい」との回答を送付した。この時点で、A 社を詐称したメールによる詐欺が試みられていることが発覚した。

参考までに、通常、A 社から取引先企業へ連絡を行うタイミングは、請求書を送付する際と、支払期限を超過した際の 2 回であり、また、取引の支払条件は NET60（商品発送または請求書発行から 60 日以内の

支払い）であった。本件について、A 社からの請求書は 4 月 2 日に送付していたため、次に連絡するならば支払期限が超過する 5 月下旬から 6 月上旬である。米国では NET30（商品発送または請求書発行から 30 日以内の支払い）が最も一般的に使用されており、攻撃者は NET30 を想定して、支払期限を超過した頃合いの 5 月 11 日に、本件詐称メールを送ってきた可能性も考えられるとのことであった。

その後も数日から数週間おきに同様の詐称メールが 5 件以上送付されており、6 月 17 日、B 社は該当の詐称メールを受信拒否設定した。本件の詐欺は未遂に終わっている。

4.3 攻撃手口

本事例では、次の攻撃手口が使われた。

- 偽の詐称用メールアドレスの使用
- 銀行口座の証明書類の偽造

これらの攻撃手口は、これまで確認されているビジネスメール詐欺でも多く使われていた手口である。

偽の詐称用メールアドレスの使用

本事例では、攻撃者はA社の担当者になりすますため、A社の正規のドメインに似通った偽の詐称用ドメインを使用していた。

【本物のメールアドレス】alice @ abcdcompany . co.jp
【偽物のメールアドレス】alice @ abcdcampany**-jp . com**
→ サブドメインに「-jp」を付け加えた、トップレベルドメインが異なるもの

※説明のための例であり、実際に悪用されたメールアドレスとは異なる。

本件で悪用された偽の詐称用ドメインは、攻撃者が最初にB社へメールを送った 2021 年 5 月 11 日の前日、5 月 10 日に取得されていた。IPA で確認したところ、この詐称用ドメインの名前解決先の IP アドレスには、他の複数の企業の偽ドメインが紐づいており、詐欺の常習者による攻撃であるものと考えられる。

銀行口座の証明書類の偽造

攻撃者から送られてきたメール（図 4）には、送金先銀行口座に関する、偽造された変更通知書のスキャン画像（図 5）が添付されていた。A 社の正規の証明書類と、今回偽造された送金先銀行口座の変更通知書では、フォーマットに多少の違いがあった。また、A 社の電話番号が偽の電話番号に変わっており、A 社のメールアドレスが削除されていたことがわかった。B 社が本物の A 社へ連絡して、詐欺が発覚することを防ぐためと思われる。

この文書には手書きの署名が付け加えられていたが、A 社には存在していない人物の署名とのことであった。

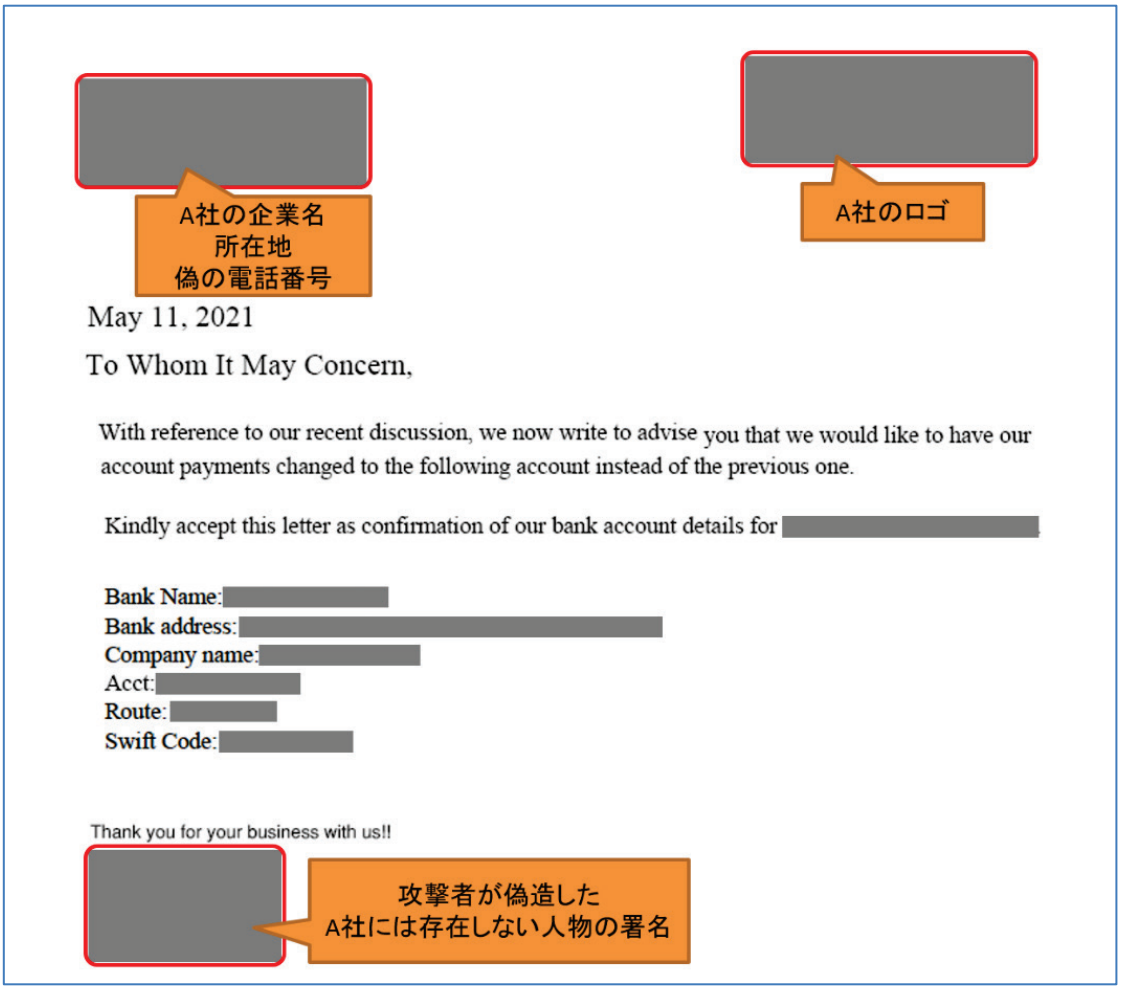

図 5 偽造された送金先銀行口座の変更通知書のスキャン画像

攻撃者は、「RAD PDF」と呼ばれる PDF の編集ツールを利用して、この偽の送金先銀行口座の変更通知書を作成していた。当該ツールはビジネスメール詐欺で使用されることが多く[6]、IPA で確認している他の事例においても同ツールが使われていたことを確認している。なお、同ツールを利用して作られているからといって、それが必ずしも悪意のある PDF ファイルというわけではない。

[6] APWG Phishing Attack Trends Report Q1 2021 Report(APWG)
https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

5　経営者を騙り詐欺を試みる文書が FAX で送られてきた事例

本四半期、J-CSIP 参加組織より、同社の経営者を名乗る不審な内容の文書が、国内外の関連会社 2 社の役員宛に FAX で送られてきたという情報提供があった。この文書内には連絡先としてメールアドレスが書かれており、このメールアドレス宛に連絡することで、金銭の詐取等の詐欺行為が試みられるものと考えられる。このため、IPA では本事例はビジネスメール詐欺に繋がる攻撃であると判断している。

また、IPA で調査する過程で、攻撃者が用意したと思われる、本事例と関連すると思われるウェブサイトの存在を確認した。

本章では、FAX で送られてきた文書（以下、詐欺文書とする）および、攻撃者が用意したと思われるウェブサイトについて説明する。

FAX で送られてきた詐欺文書

経営者を名乗り、FAX で送られてきた文書（図 6）には、ビジネス雑誌に広告記事の掲載を促す内容と、その担当者へメールで連絡するよう依頼する内容が書かれていた。本物に似せた実在しない偽の雑誌名であり、広告掲載料の名目で金銭を騙し取ることが目的と考えられる。

本事例では、FAX を受信した関連会社の役員が不審に思い、連絡を取らなかったため、この後どのように詐欺が進むのかは不明である。

IPA では、別の組織宛と思われる、本件と内容が類似する文書[7]を公開情報で発見している。攻撃者は様々な組織の経営者を騙り、複数の組織に対して攻撃を行っている可能性がある。

本件のような詐欺と思われる文書等が送られてきた際は、ビジネスメール詐欺の対策と同様の方法で対応していただきたい。すなわち、経営者や企業幹部等から身に覚えのない連絡を受けた場合や、普段と異なる方法で連絡を受けた場合は、返信・連絡を行う前に、信頼のおける方法で入手した連絡先へ事実確認を行うことが重要である。

[7] 公開情報にて確認した文書は PDF ファイルであったため、FAX で送られたかは不明である。

A社：攻撃者が送信したFAXを受信した会社(B社の関連会社)
B社：攻撃者によって経営者を騙られた会社

For the attention of: A社の会社名
Dear A社役員の氏名
I am writing to let you know that B社の会社名 is to be the subject of a major article to feature in the specialist business magazine, 実在しない雑誌名.

B社に関する説明文(B社のウェブサイト等から引用したものと思われる)

As you are one of our key suppliers, we have forwarded your name to the magazine as a company that may be interested in supporting the project by advertising your own products, skills and capabilities along side us within the pages of our article. We believe that this is an effective way to promote ourselves and increase your exposure and therefore your support for this article would be greatly appreciated. The article will also be reproduced as a brochure for independent use.

実在しない雑誌名 can supply you with all the relevant details and you can register your interest with them directly. The point of contact is Mr 人名, who is managing this project and will assist with all the arrangements. Please contact him via email at メールアドレス

All of our suppliers represent an important part of our plans for the future. I believe that both our companies will benefit from the article and the exposure that it will give us.

Please see attached the second page of this letter with advert rates and magazine requirements.

Yours Sincerely

B社経営者の署名

図 6 FAX で送られてきた詐欺文書の内容

攻撃者が用意したと思われるウェブサイト

詐欺文書に記載されていた、雑誌の担当者だというメールアドレスのドメインについて IPA で調査を行ったところ、当該ドメインにウェブサイト（図 7）が存在することを確認した。

このウェブサイトは、実在するビジネス雑誌のロゴマークや URL リンクが掲載され、別のニュースサイトから盗用したと思われる記事が複数掲載されている。一見すると正規のニュースサイトのように見えるものであった。

詐欺文書の受信者が、連絡内容が本物であるか確認しようとした場合に、偽の雑誌が存在すると信じさせる目的で、攻撃者が用意したものと思われる。

図 7 攻撃者が用意したと思われるウェブサイトの画面（一部）

6　社外から持ち込まれた USB メモリから不正通信が発生した事例

社外から持ち込まれた USB メモリに悪意のあるファイルが含まれており、パソコンに接続したタイミングで不審な通信が発生し、セキュリティソフトによって検知されるという事象が複数回発生したという情報提供を受けた。

本章では、当該事案発生時に、参加組織が行った対応とともに、当該 USB メモリに含まれていた悪性ファイルの動作を説明する。

本事例の経緯と参加組織における対応

1. 参加組織にて不審な通信の発生を検知した。
2. 通信の発生元のパソコンを調査したところ、社外から持ち込まれた私物の USB メモリが接続されていたことを把握した。
3. 発生元のパソコンでは、ウイルスの感染や、以降の不正通信の発生は確認されなかった。
4. USB メモリを確認したところ、不審なファイルが存在することを確認し、当該不審な通信の発生が USB メモリに起因するものと判断し、IPA へ情報提供した。
5. IPA の見解等をもとに、USB メモリ内の不審なファイルが、いつどこから発生したのかを参加組織で調査を試みたが、私物であったこともあり、究明はできなかった。

情報提供を受け、IPA で USB メモリ内のファイルを調査したところ、攻撃用と思われる細工されたショートカットファイル及び不審なコマンドが書かれたファイル等が存在しており、USB メモリがウイルスにより汚染されていたことが判明した。

また、本事例では、参加組織にて USB メモリにあった不審なファイルについて、セキュリティベンダへ調査依頼を行ったところ、最初は「正常なファイル」と判定された。その後、IPA での判断結果を受け再度調査依頼したところ、検知対象となるよう、セキュリティベンダにて当該ファイルをウイルスとして判断するようにパターンファイルが更新された。

外部から持ち込まれた USB メモリによるセキュリティインシデントは繰り返し観測されている事例である。また、USB メモリ経由で感染を拡大するウイルスは古くから存在するが、本件のようにセキュリティソフトで検知されないものも未だに存在するようであり、組織内における USB メモリの取り扱いについてルールの整備等が必要である。

USB メモリに含まれていたウイルスファイル

USB メモリには次の 3 点のファイルおよびフォルダが含まれていた（図 8）。

- 「リムーバブル ディスク」という名前の隠しフォルダ
- 「xplw.lng」という名前の隠しファイル
- 「リムーバブル ディスク」という名前で、アイコン偽装されたショートカットファイル

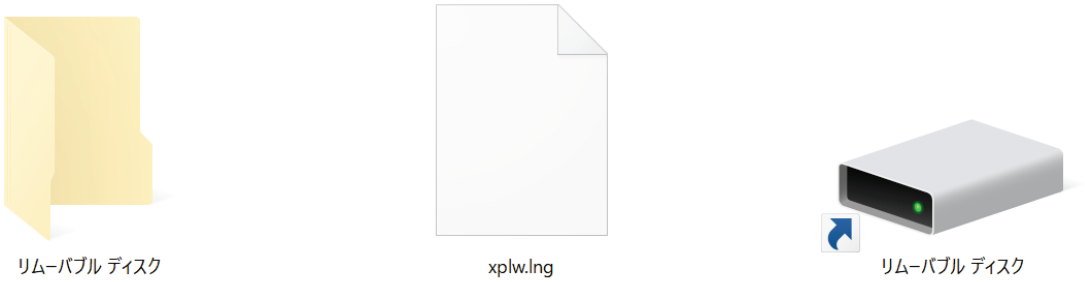

図 8 USB メモリに含まれていた 3 つのファイル

3 点のうち、2 点のファイル・フォルダは隠しファイルとして設定されており、隠しファイルを表示する設定にしていない場合、「リムーバブル ディスク」のショートカットファイルのみが表示されるようになっていた（図 9）。

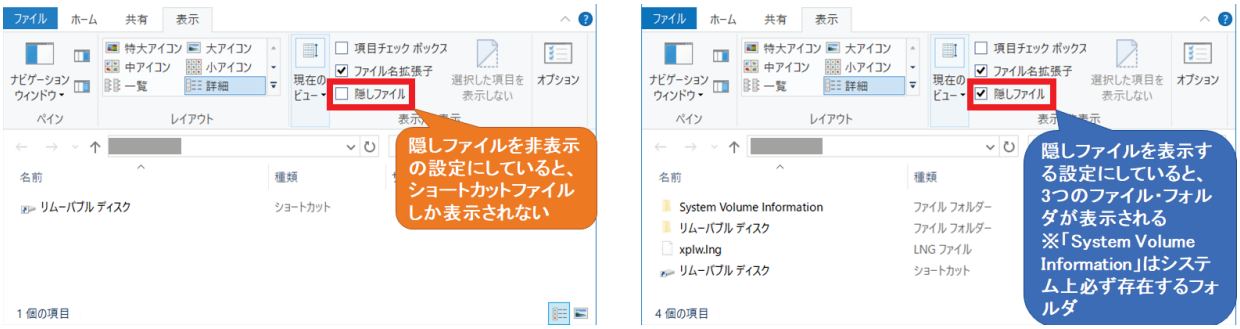

図 9 隠しファイルの表示/非表示設定による差異

参考までに、このウイルスの動作の仕組みは次の通りであった。

1. 利用者が USB メモリをパソコンに接続すると、「リムーバブル ディスク」という名称で認識される。利用者の操作か Windows の機能で、USB メモリの内容が上記 図 9 の状態で表示される。
2. 「USB メモリの中に、更にその USB メモリのアイコンが存在する」という異常な状態であるが、利用者はそれに気づかず、USB メモリのアイコン（「リムーバブル ディスク」という名前のショートカットファイル）をダブルクリックするなどして開いてしまう。
3. ショートカットファイルの中に仕込まれているスクリプトが実行される。スクリプトは、USB メモリ内にある「xplw.lng」という名前の隠しファイル内に書かれているコマンドを実行する。
4. 「xplw.lng」は、次の処理を行う。 ① 外部の不正接続先からウイルス本体ファイルをダウンロードし、パソコンへインストールする（感染させる）。 ② USB メモリ内の「リムーバブル ディスク」という名前の隠しフォルダを開き画面に表示する。
5. 利用者には、「リムーバブル ディスク」という名前の隠しフォルダが、USB メモリ直下の内容のように見える。利用者は自分のファイルをそのフォルダへ読み書きして、USB メモリを取り外す。この USB メモリを別のパソコンに接続した場合、1.～4. が再び行われ、ウイルス感染が拡大するとともに、利用者は問題なく USB メモリが使えているかのように見える。

7　問い合わせのやり取りの中でフィッシング攻撃が試みられた事例

本四半期、J-CSIP の参加組織より、自社商材等を登録している BtoB サービスを経由して、商材についての問い合わせがあり、その問い合わせに返信したところ、フィッシングメールが送られてきたという情報提供があった。

本章では、参加組織へ届いた問い合わせやフィッシングメールと共に、攻撃の手口について説明する。

（1）問い合わせ

本件にて BtoB サービス経由で送られてきた問い合わせの内容（一部）を図 10 に示す。

お問い合わせ内容
私の電子メールに価格を記載したあなたの会社のカタログを送ってください、私はあなたの会社から購入したいです

図 10 問い合わせの内容

情報提供元組織の担当者は、「複数の商品があるため、具体的な要望等を教えてほしい」といった内容で返信を行った。

問い合わせに書かれていた会社名・住所・電話番号については実在する日本の組織のものであったが、メールアドレスについてはフリーメールアドレスが使われていた。「お問い合わせ内容」は日本語で書かれているが、文章に不自然な点が見受けられる。

（2）フィッシングメール

その後、担当者は図 11 に示すメールを受信した。このメールには、担当者からの質問に対する回答はなく、「発注書を用意した。緊急で URL リンク先にアクセスし、メールアドレスとパスワードでログインしてほしい」と要求する内容であった。担当者は、このメールの内容を不審と判断し、セキュリティ部署に報告を行った。なお、URL リンク先は「Bitbucket」という正規のサービスのウェブサイトであり、攻撃者は当該サービスを悪用したものと思われる。

本事例では、問い合わせメールに返信した 5 ヶ月後と 9 か月後の 2 回、フィッシングメールが送られてきている。なぜここまで間が空いたのかは不明である。

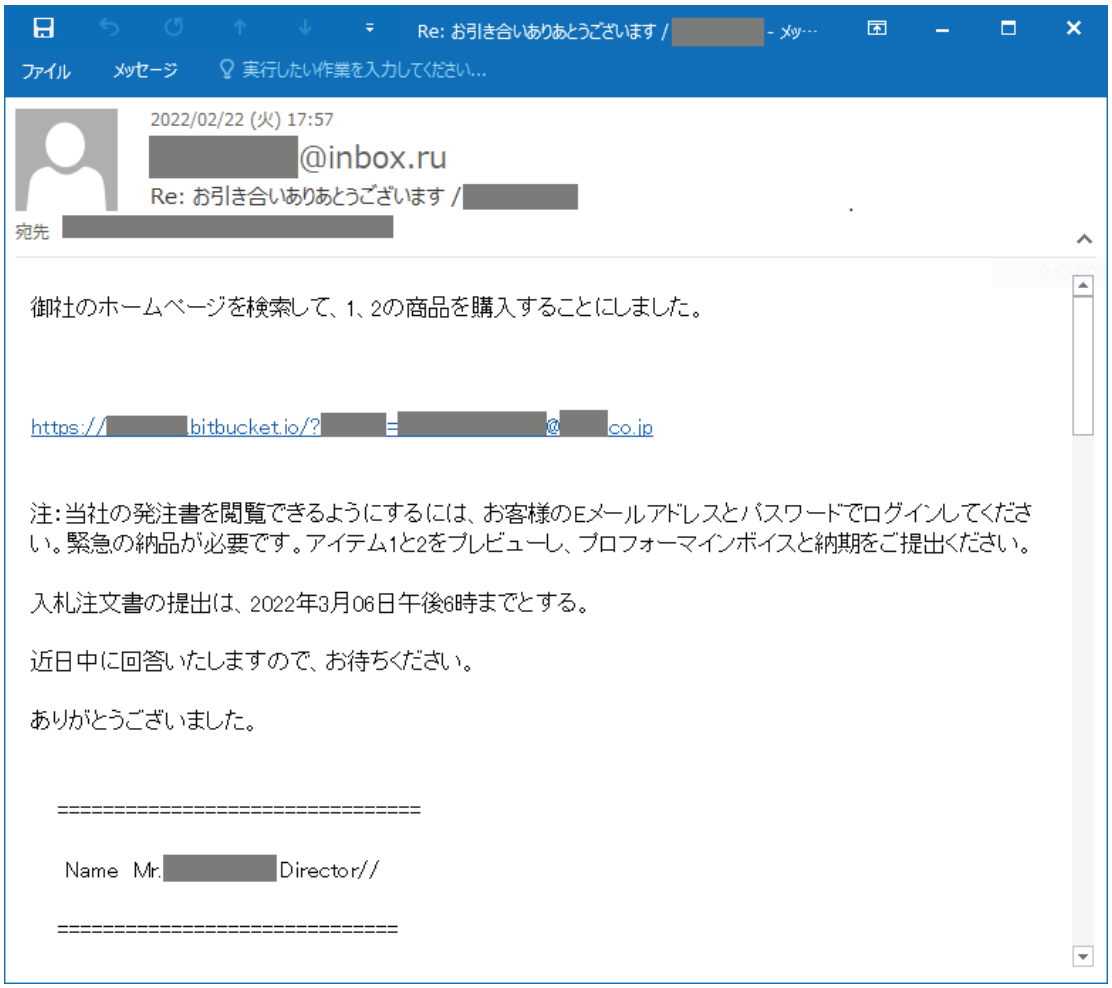

図 11 フィッシングメール

(3) フィッシングサイト

フィッシングメール内の URL リンク先にアクセスすると、Dropbox を模した偽のページが設置されており、いくつかのファイルがダウンロード可能であるかのように表示された。ファイルをダウンロードしようとページ内のアイコン等をクリックすると、ログインを要求するフォーム(図 12)が表示される。フォームは、攻撃対象(担当者)のメールアドレスがあらかじめ入力された状態となる仕組みとなっていた。このフォーム上でパスワードを入力し、「View Files File」ボタンをクリックすると、入力したパスワードが攻撃者のサーバへ送信されてしまう。

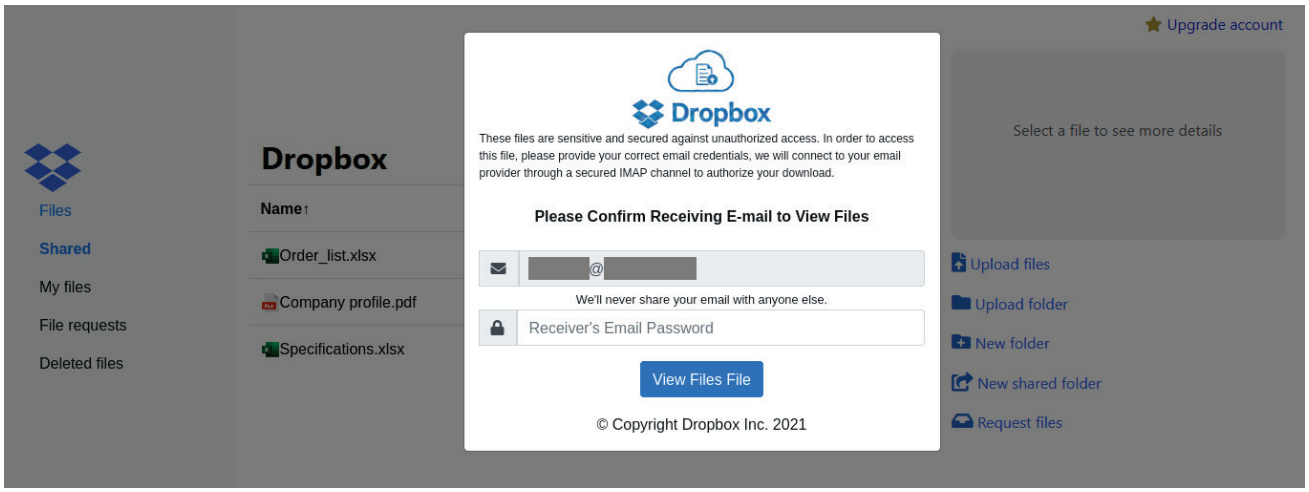

図 12 Dropbox サービスの画面を模したフィッシングサイト

この事案は、J-CSIP において 2012 年から 2014 年頃まで複数観測していた「やり取り型」と呼んでいる攻撃手口 [8]に近い。問い合わせ窓口への連絡から始まり、担当者のメールアドレスの入手やメールをやり取りした上で、攻撃を行うという手口である。企業等においては、このような攻撃手口があることをよく認識し、周知徹底しておく必要がある。

[8] サイバー情報共有イニシアティブ（J-CSIP） 2013 年度 活動レポート ～「やり取り型」攻撃に関する分析情報の共有事例～ を参照。
https://www.ipa.go.jp/security/J-CSIP/

8　Emotet への感染を企図した攻撃メール

本四半期も継続して、複数の組織から Emotet への感染を企図した攻撃メールを観測したとの情報提供があった。その中には、「パスワード付き ZIP ファイルが添付された攻撃メールを着信した後に、パスワードを通知するメールが着信した」という情報提供があった。確認の結果、これは攻撃者による新たな攻撃手口ではなく、Emotet に感染した組織で使用していた、自動で添付ファイルをパスワード付き ZIP ファイルにするメールシステムの動作によるものであった（図 13）。

本レポート執筆時点では、パスワード付き ZIP ファイルが添付された Emotet の攻撃メールの場合、本文中にパスワードが記載されているものしか確認していない。一方、Emotet の攻撃メールの送信経路によっては、パスワードを通知するメールが別送で届くということがあり得るため、注意いただきたい。

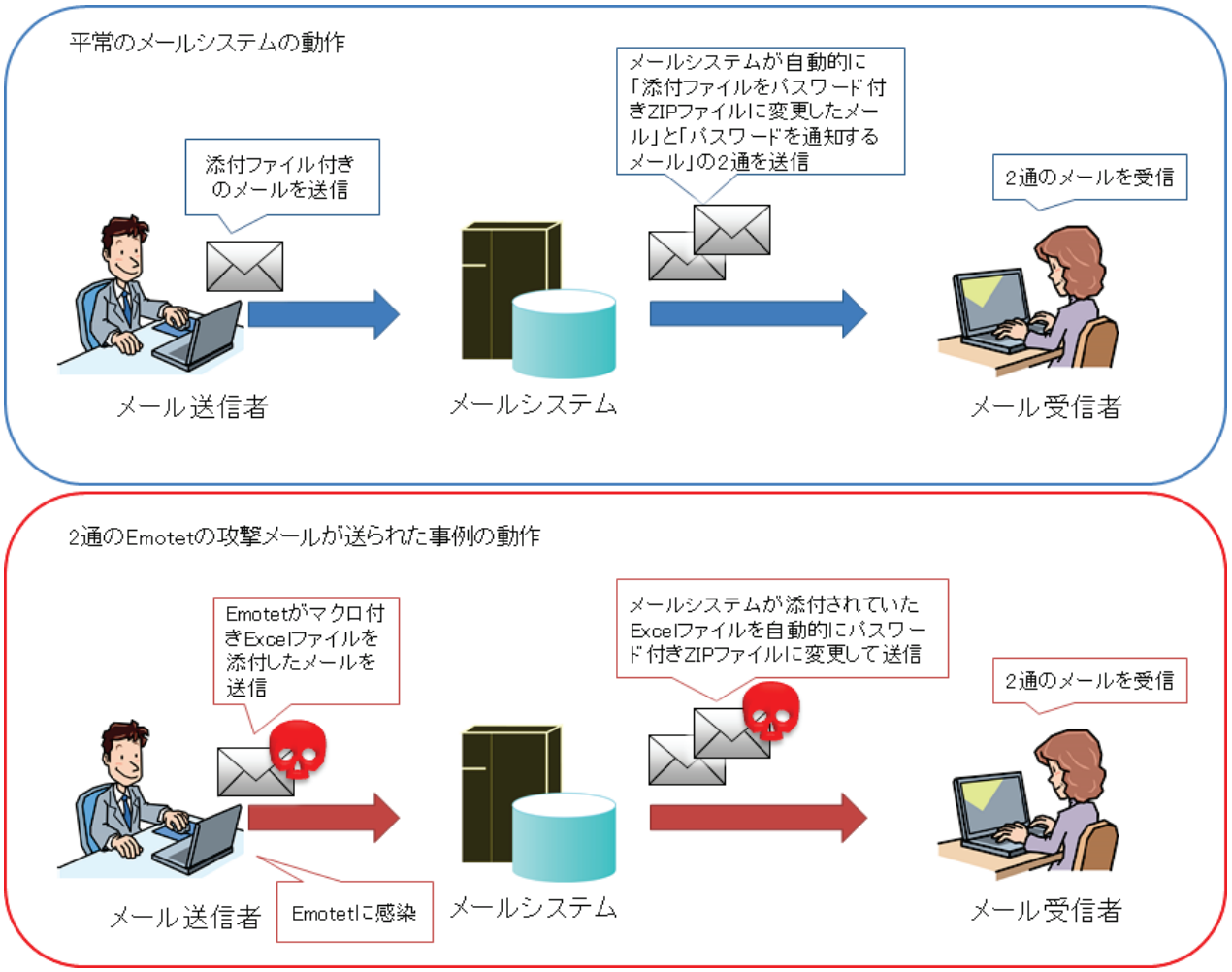

図 13 Emotet の攻撃メールが 2 通になっていた仕組みのイメージ図

IPA では、状況の変化に応じ、Emotet の攻撃メールについて継続して注意喚起のページを更新している。2022 年 3 月には、多くの国内企業・組織における Emotet への感染が報告されており、今後も引き続き注意をしていただきたい。

9　ヘルプファイルを悪用した攻撃メール

2022 年 3 月、Microsoft のコンパイルされた HTML ファイル（以降、ヘルプファイル）を悪用し、ウイルスに感染させる攻撃手口の情報を入手した [9]。

メールに添付された圧縮ファイル内に悪意のあるヘルプファイルが含まれており、ヘルプファイルを開くことでウイルスに感染することを確認している。これまでに多く確認されている Office 文書ファイルのマクロによる手口では、ファイルを開いたとしても、マクロ機能を有効化しなければ被害を防ぐことが可能だが、本攻撃手口はファイルを開くだけでウイルスに感染するため、利用者ひとりひとりにこの手口の注意点を周知するべく、参加組織へ情報共有を実施した。

この攻撃手口と注意点をまとめた一般利用者向けの資料を、本書の参考資料とした。IPA で確認できている範囲では、国内への攻撃に使用された可能性を示す情報は確認していない。しかし、今後、日本語での攻撃メールで使われるようになる可能性があること、ヘルプファイルを開くだけでウイルスに感染してしまうことから、広く周知することが重要だと考える。必要に応じ、参考資料を活用していただきたい。

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

[9] APT Attack Being Distributed as Windows Help File (*.chm) (AhnLab)
https://asec.ahnlab.com/en/32800/
Vidar Malware Launcher Concealed in Help File (Trustwave Holdings)
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/vidar-malware-launcher-concealed-in-help-file/