サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 10 月～12 月]

2024 年 2 月 29 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 12 月末時点の運用体制と、2023 年 10 月～12 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、4 章では本四半期で把握・分析した特徴的な攻撃事例について解説する。

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）。

近年のサイバー空間における厳しい情勢を踏まえ、IPA は、2023 年度からの第五期中期計画[3]において、「サイバー攻撃情報の収集能力と分析機能の強化を通じて『サイバー状況把握力』の強化を図り、これによって、精度の高い脅威評価と多面的なサイバーセキュリティに関する課題解決提案を行い、もって国家の安全保障・経済安全保障の確保に貢献する」方針を掲げている。J-CSIP においても、この方針を踏まえて、参加組織や関係機関等との情報共有・連携をさらに強化し、APT をはじめとしたサイバー攻撃に関する情報の収集・分析・発信をより一層充実させていくとともに、本レポートの記載内容についても、本方針を踏まえ充実を図っていく。

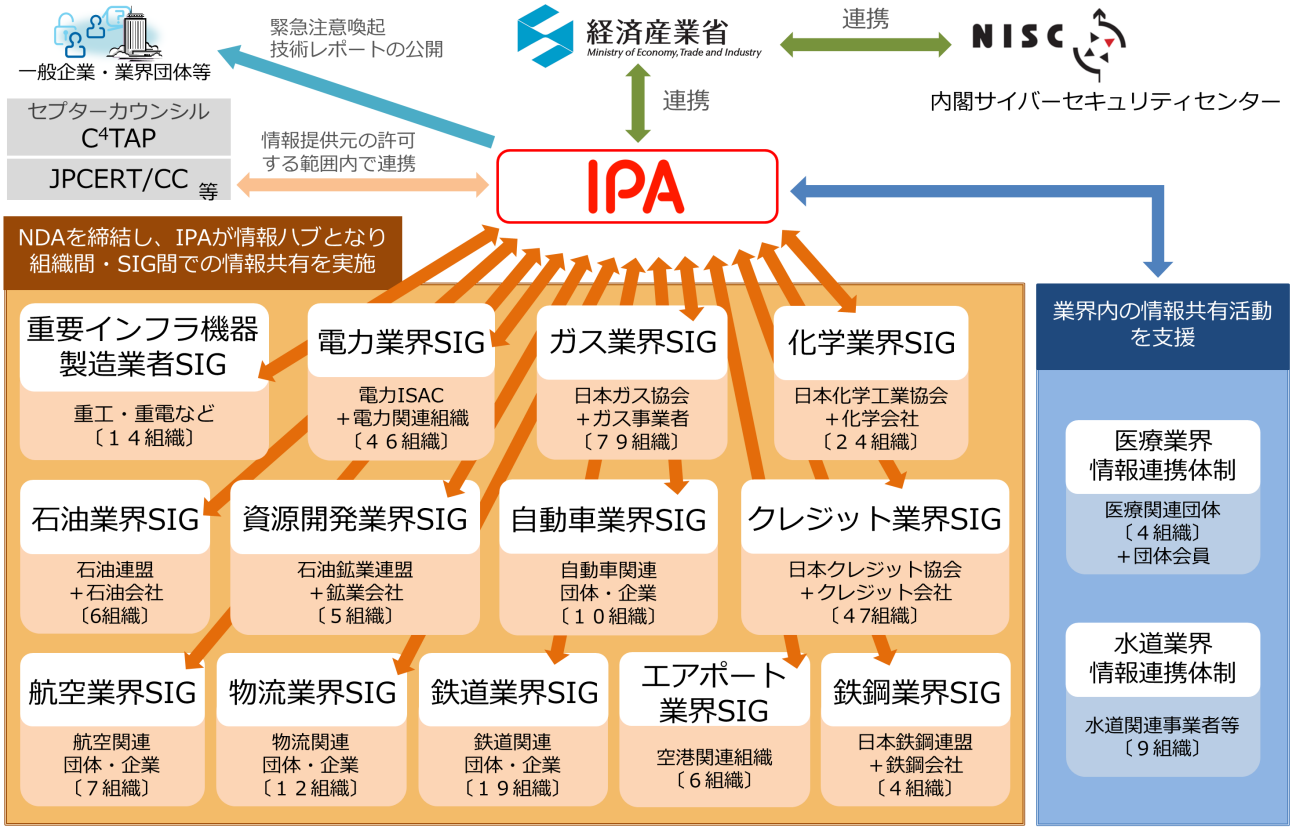

図 1 J-CSIP の体制図

[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。
[3] 独立行政法人情報処理推進機構（IPA）「第五期中期計画」
https://www.ipa.go.jp/about/disclosure/ps6vr7000000h6ln-att/5thplan.pdf

2　運用状況（2023 年 10 月～12 月）

2023 年 10 月～12 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 節で参加組織から提供された情報を報告する。

2.1 情報提供・情報共有の実施件数

2023 年 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 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	2023 年			
		1 月～3 月	4 月～6 月	7 月～9 月	**10 月～12 月**
1	参加組織から IPA への情報提供件数	59 件	26 件	24 件	**27 件**
2	IPA から参加組織への情報共有実施件数※1	22 件	23 件	22 件	**15 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 **9 件**を含む。

本四半期は情報提供件数が **27 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 **1 件**であった。

2.2 IPA が収集し参加組織へ共有した情報

IPA では、公開情報を含め独自に APT 等のサイバー攻撃に関する情報を収集し、必要に応じてこれらの情報を J-CSIP 参加組織へ情報共有するといった活動を行っている。

2023 年は、VPN 装置やオンラインストレージ等のインターネット境界に設置された装置に対するサイバー攻撃（ネットワーク貫通型攻撃 [4]）が問題となっており、その一部は、国家の支援を受けた APT 攻撃グループの関与が疑われている。Trend Micro 社が Earth Kasha（別名：MirrorFace）と呼称する攻撃者グループによる、日本の政府機関やハイテク関連団体などを標的とした攻撃キャンペーンでは、「Array AG」、「FortiOS SSL VPN」などの VPN 装置や、オンラインストレージサービスの「Proself」に関する脆弱性が悪用されたとみられている [5]。また、Mandiant 社が UNC4841 と名付けた攻撃者グループは、メールゲートウェイ製品である「Barracuda Email Security Gateway（Barracuda ESG）」のゼロデイ脆弱性を悪用し、情報窃取等

[4] 独立行政法人情報処理推進機構（IPA）「インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～」
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html

[5] Trend Micro「Spot the Difference: An Analysis of the New LODEINFO Campaign by Earth Kasha」
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf

の活動を行っていたものとみられている[6]。前四半期には、J-CSIP 参加組織においても Array Networks 社および Citrix Systems 社の VPN 装置の脆弱性を悪用した攻撃の痕跡が確認されており[7]、J-CSIP 参加組織を含む重要インフラを担う組織においても、ネットワーク貫通型攻撃の脅威にさらされているとみられる。

こうした状況を踏まえ、本四半期中も、ネットワーク貫通型攻撃に悪用される恐れがある脆弱性について、J-CSIP 参加組織に対し次の 2 件の注意喚起を行った。

- Proself 等のオンラインストレージの脆弱性に関する注意喚起　（2023 年 10 月）
- Barracuda 社製品 Email Security Gateway Appliance（ESG）の脆弱性に関する注意喚起（2023 年 12 月）

前述の通り、これらの脆弱性を悪用した攻撃には、国家の支援を受けた APT グループが関与しているとの情報もあることから、J-CSIP 参加組織に対して、脆弱性対応や侵害痕跡確認等の対応を促している。その一環として、サイバーレスキュー隊（J-CRAT）[8]が独自に把握している、攻撃に使われた IP アドレス等の情報を J-CSIP 参加組織に共有した。

2024 年に入ってからも、「FortiOS SSL VPN」や「Ivanti Connect Secure」といった VPN 装置において、悪用を確認、または悪用が懸念される脆弱性が見つかっており[9] [10]、今後もネットワーク貫通型の攻撃に警戒が必要である。各組織においては、VPN 装置等のネットワーク境界に設置された製品と脆弱性に関する最新の動向を把握し、脆弱性が発見された場合は、速やかに修正プログラムや緩和策の適用等の対策を実施いただきたい。また、既に脆弱性を悪用した攻撃が観測されているといった情報がある場合は、製品ベンダやセキュリティ機関等が発信している情報をもとに不正アクセスの有無を確認してほしい。その結果、装置に対する不正なファイルの設置や組織内部への侵害が疑われる場合は、影響範囲や被害状況の確認を行うことを勧める。

---

[6] Mandiant「中国との関連が疑われる攻撃的、かつ高度なスキルを持つ攻撃者が Barracuda ESG のゼロデイ脆弱性（CVE-2023-2868）を悪用」
https://www.mandiant.jp/resources/blog/barracuda-esg-exploited-globally

[7] 独立行政法人情報処理推進機構（IPA）「サイバー情報共有イニシアティブ（J-CSIP） 運用状況[2023 年 7 月～9 月]」
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf

[8] 独立行政法人情報処理推進機構(IPA)「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について」
https://www.ipa.go.jp/security/j-crat/about.html

[9] 独立行政法人情報処理推進機構（IPA）「Fortinet 製 FortiOS SSL VPN の脆弱性対策について(CVE-2024-21762)」
https://www.ipa.go.jp/security/security-alert/2023/alert20240209.html

[10] 独立行政法人情報処理推進機構（IPA）「Ivanti Connect Secure（旧 Pulse Connect Secure）および Ivanti Policy Secure Gateways の脆弱性対策について(CVE-2023-46805 等)」
https://www.ipa.go.jp/security/security-alert/2023/20240111.html

2.3 参加組織から IPA へ提供された情報

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。

- 日本企業を装ったドメインからの不審メールを受信したという情報提供があった。この不審メールには、日本企業から送信されたと見せかける偽装がされており、添付ファイルを開かせようとする内容が記載されていた。受信者に添付ファイルを開かせることで、ウイルスに感染させる目的があったとみられている。詳細については、3 章で述べる。

- FAX 受信の通知メッセージを装ったフィッシングメールを受信したという情報提供があった。このフィッシングメールには、セキュリティ対策を回避するため手法が複数使われており、情報提供元のメールセキュリティ製品によるフィルタリングをすり抜けて、数十件が従業員の手元まで届いてしまっていた。詳細については、4 章で述べる。

- Microsoft Outlook の RSS[11]フィードフォルダを悪用した詐欺メールについて情報提供があった。これは、情報提供元の海外関係会社の従業員あてに、人事部長を騙った金銭の詐取を目的とする詐欺メールが着信したことから発覚したものである。なりすまされた送信者（人事部長）に確認したところ、当人の気付かないうちに詐欺メールが送信されていたことが判明した。調査の結果、送信元のアカウントに設定していた Microsoft 365 の多要素認証が何らかの方法で突破され Web 版の Outlook に不正ログインされたことが判明した。さらにメールの仕分けルールが不正に作成されており、このルールは詐欺メールに対する返信メールを受信した場合、RSS フィードフォルダに移動し（図 2 -①）、開封済みにする（図 2 -②）というものであった。
  RSS フィードフォルダは、Outlook に標準で用意されているフォルダであり、Outlook で RSS を利用しない場合、その中身を確認する可能性はほとんどないといえる。攻撃者には、このことを悪用して詐欺メールの送信元となっていることを隠蔽する目的があったとみられている[12]。また、メールの仕分けルールは、一度設定すると再度確認を行うことが少ないと想定され、不正なルールが設定されていても気付くことは難しいといえる。
  攻撃者が多要素認証を突破した方法は不明であるが、その一例として、認証済みのセッション情報を盗むフィッシング攻撃が確認されている[13]。多要素認証を設定していた場合でも、バイパスされる可能性があること念頭におき、従業員へのセキュリティ教育や不審なログインがないかの確認を行うといった対策が重要である。なお、本件のような信頼できる送信元からのメールであっても、不審な点があった場合には、電話等メール以外の信頼できる方法で送信者や関係者に事実確認を取ることを勧める。

---

[11] ウェブサイト（ニュースサイトやブログなど）の更新情報を配信する仕組み。
RSS によって配信される情報のことを「RSS フィード」と呼び、購読したい RSS フィードを Outlook に登録することで、RSS フィードフォルダに RSS フィードが配信される。

[12] Palo Alto Networks「Behind the Curtains of a Vendor Email Compromise (VEC) Attack」
https://www.paloaltonetworks.com/blog/security-operations/behind-the-curtains-of-a-vendor-email-compromise-vec-attack/

[13] Microsoft「From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud」
https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

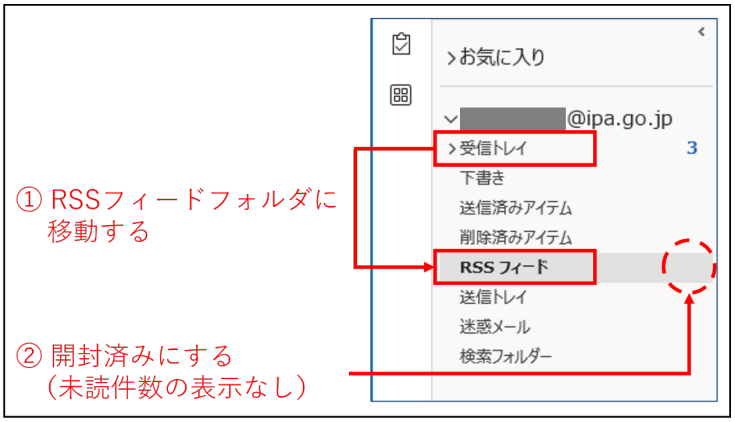

図 2 仕分けルールによる詐欺メールの隠蔽（イメージ図）

- 外部サイトの閲覧中にポップアップ通知による偽のセキュリティ警告が表示されたという情報提供があった。情報提供元によると、当該サイトで表示された偽のセキュリティ警告には、ヘルプデスクへの連絡（図 3）や、ウイルスの削除、ブラウザ拡張機能のインストールを促すものがあったという。IPA にて当該サイトを調査したところ、Web プッシュ通知 [14]を悪用し、偽のセキュリティ警告を表示させることで、別の不審サイトへ誘導するというものであった。
  偽のセキュリティ警告や不審サイトの指示に従ってしまうと、サポート料金と称した金銭の詐取や、不正なソフトウェアのインストール、ウイルス感染等の被害に遭う可能性が考えられる [15]。組織のパソコンにおいて、外部サイトの閲覧中に不審なセキュリティ警告が表示された際には、決して指示には従わず、すぐに上司やシステム管理者に報告してほしい [16]。また、ブラウザでの通知を安易に許可しないことに加え、従業員へのセキュリティ教育、報告プロセスの策定・周知を行うといった対策が有効である。

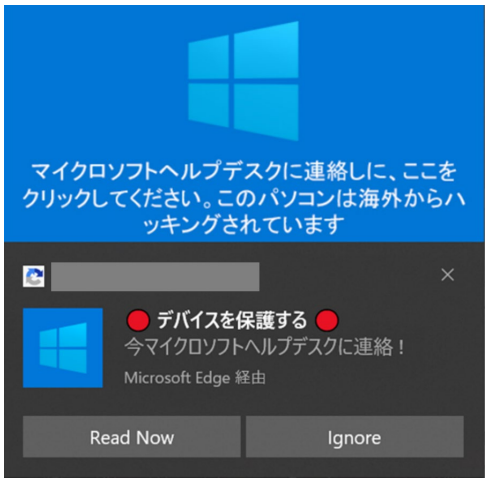

図 3 ヘルプデスクへの連絡を促す偽のセキュリティ警告（例）

---

[14] 通知を許可した利用者に対し、ウェブブラウザを経由してプッシュ通知を送信する機能。
[15] 独立行政法人情報処理推進機構（IPA）「偽のセキュリティ警告に表示された番号に電話をかけないで」
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html
[16] 独立行政法人情報処理推進機構（IPA）「会社や組織のパソコンにセキュリティ警告が出たら、管理者に連絡！」
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230711.html

- 自社の広告メールへの返信を装った不審メールを受信したという情報提供があった。このメールは、情報提供元の関連会社に着信したものであり、同関連会社が過去に配信した広告メールを引用する形で返信を装い、添付ファイルの開封を促すものであった。添付されている PDF ファイルを開くと、不鮮明な文章の手前に「Adobe Acrobat Reader」のダウンロードを促すメッセージが描かれた、1 つの画像で構成されたページが表示された（図 4）。この画像をクリックすると不正接続先から ZIP ファイルがダウンロードされる仕組みになっていた。攻撃者は、過去に配信されていた正規の広告メールを何らかの方法で入手し、それを悪用して返信を装ったものとみられる。また、IPA にて公開情報を調査したところ、類似のメールや添付ファイルを複数確認したことから、同様の手口で攻撃が広く行われている可能性が高い。

  ばらまき型の攻撃メールは、メールセキュリティ製品によるフィルタリングに加え、従業員一人ひとりが不審メールに注意することが重要である。一見正規のものに見えるメールであっても、少しでも不自然な点があれば添付ファイルは開かないことが望ましい。また、従業員が添付ファイルを開いてしまった場合に備え、URL フィルタリング製品やウイルス対策ソフト、エンドポイントセキュリティ対策製品（EDR）を導入し、常に最新の状態にしておくことも重要といえる。

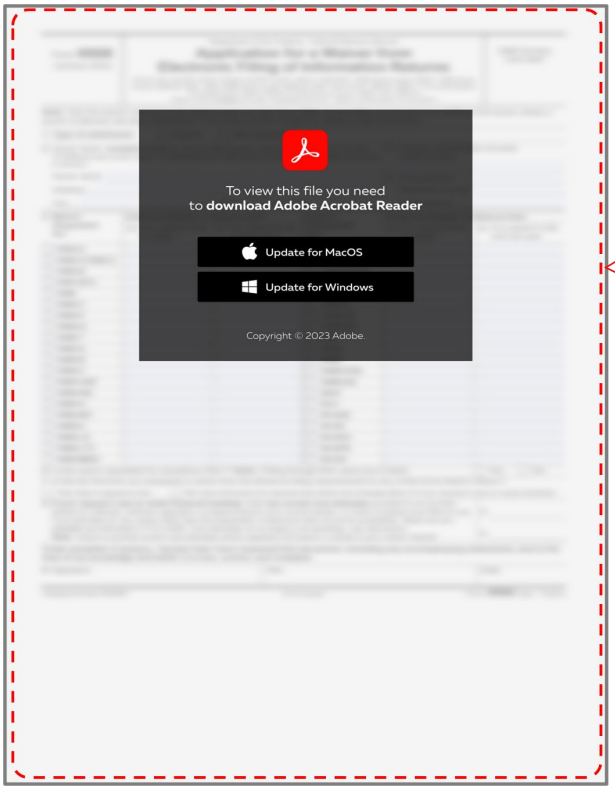

図 4 添付ファイルを開くと表示されるページ

3　日本企業からの問い合わせを装ったばらまき型の攻撃メール

本事例は、J-CSIP の参加組織（以下、A 社）に、日本企業を装った不審なメールが届いたというものである。IPA にてメールおよび添付ファイルを調査したところ、本メールは、日本企業からの製品に関する問い合わせを装い添付ファイルを開かせることで、最終的に遠隔操作ウイルス（RAT）に感染させることを企図したばらまき型の攻撃メールであるとみられる。

本章では、A 社に着信した不審メールの特徴と添付されていたウイルスの挙動、調査の過程で発見した類似検体について説明する。

3.1 不審メールの特徴

A 社が受信した不審メールの差出人/宛先や本文の署名には、日本企業から送信されたと見せかける偽装がされていた。また、本文には「添付ファイルに記載した貴社製品の詳細情報が欲しい」という内容が記載されており、受信者に添付ファイルを開かせようとするものであった。この不審メールの特徴を次に示す。

（1） 差出人（From ヘッダ）/宛先（To ヘッダ）

メールの差出人（From ヘッダ）および宛先（To ヘッダ）を、図 5 に示す。差出人（From ヘッダ）の表示名には、日本人名（ローマ字）が設定されており、メール本文の署名に記載されている人名と同じであった。メールアドレスのローカル部には、「import（輸入）」が使われており、貿易関連の業務用アカウントを連想させるものであった。また、ドメイン部には、「日本のある地域名」と「jp.com」をつなげたものを使っており、送信元の組織がこの日本の地域に存在することを連想させるものであった。なお、IPA で調査したところ、当該ドメインを使用する実在の組織は確認できなかった。

宛先（To ヘッダ）の表示名には、A 社とは無関係なメールアドレスが設定されており、ドメイン部には日本の企業名もしくは個人名を思わせるものが含まれていた。また、実際のメールアドレスは差出人（From ヘッダ）と同じメールアドレスとなっていた。なお、宛先（To ヘッダ）には、A 社のメールアドレスが設定されていないことから、A 社には Bcc にて送信されたと考えられる。また、攻撃者が Bcc を使い、A 社を含む不特定多数あての同報メールとして送付した可能性もある。

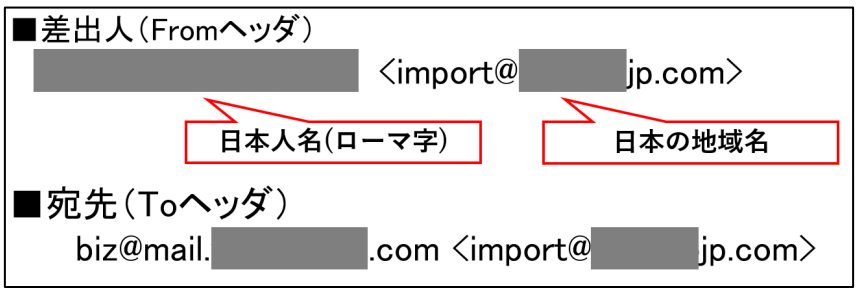

図 5 メールの差出人および宛先（イメージ図）

（2） 署名

メール本文末尾の署名は、図 6 に示すように、日本語で記載されていた。企業名は、日本語（漢字）で「〇〇輸出株式会社」と名乗っていたが、公開情報からその企業の存在を確認することはできなかった。しかしながら、署名に記載された住所には、署名とは別の企業（B 社）が存在しており、B 社の企業名と署名で名乗っていた企業名は類似していた。また、電話番号も、B 社が利用しているものであるとみられている。このことから、実在する組織に似せた社名を名乗り、その組織に関連する情報を記載することで、正規のメールを装った可能性が考えられる。

+- +-+-+-+-+-+-+-+-+

[redacted]輸出株式会社

M＆Ｉ領域　技術部

日本人名(漢字)　日本人名(ローマ字)

[redacted] - [redacted] -

〒[redacted]-[redacted] [redacted]

TEL ： [redacted]　FAX ： [redacted]

E-mail ： biz @mail.[redacted].com

図 6 メール本文の署名（イメージ図）

（3） 件名/本文

差出人や署名は日本企業を装ったものであったが、件名およびメール本文は、図 7 に示す通り、英語で記載されていた。件名は、「輸出用に購入するための情報が欲しい」というものであった。

メール本文は、宛名が「Dear Sirs」であり組織名や個人名は記載されていなかった。また、内容は A 社に限らず他の組織でも通用するような、「展示会のウェブサイトを見た。海外の顧客に輸出するための製品を貴社から探している。添付ファイルに記載したサンプル製品についてのより詳細な情報が欲しい。」といった内容であり、受信者が添付ファイルを開くよう誘導するものであった。

■件名

Information request purchase for export

■本文

Good morning

Dear Sirs,

I visited an expo website. I'm looking for the selected samples catalog for my important German partner to export from your company.

I would like to kindly ask you if you can be interested in this eventual cooperation?

If yes please kindly send me some more detailed information for the attached samples products with your best offer price and which certificates can you provide?

Have you already exported to Germany ?

I'm waiting to receive your kind reply.

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- +-+-+-+-+-+-+-+-+-+-+-+-+-+-+

(以下、署名)

図 7 メールの件名および本文（イメージ図）

3.2 添付ファイルの挙動

メールには、圧縮ファイルが添付されており、解凍すると「DBatLoader」というウイルス（ダウンローダー）が展開される。このウイルスを実行すると、最終的には「Warzone RAT」という遠隔操作ウイルス（RAT）に感染する。添付ファイルを開いて実行した際のウイルス感染までの流れを図 8 に示す。なお、IPA にて添付ファイルの動作を確認したところ、Windows10 の日本語環境では動作の途中でエラーを示すメッセージが表示されたが、英語環境ではエラーメッセージは表示されることなく動作した。日本語環境での動作は、攻撃者の意図した動作ではない可能性があり、添付されたウイルスは英語環境を想定したものであると考えられる。

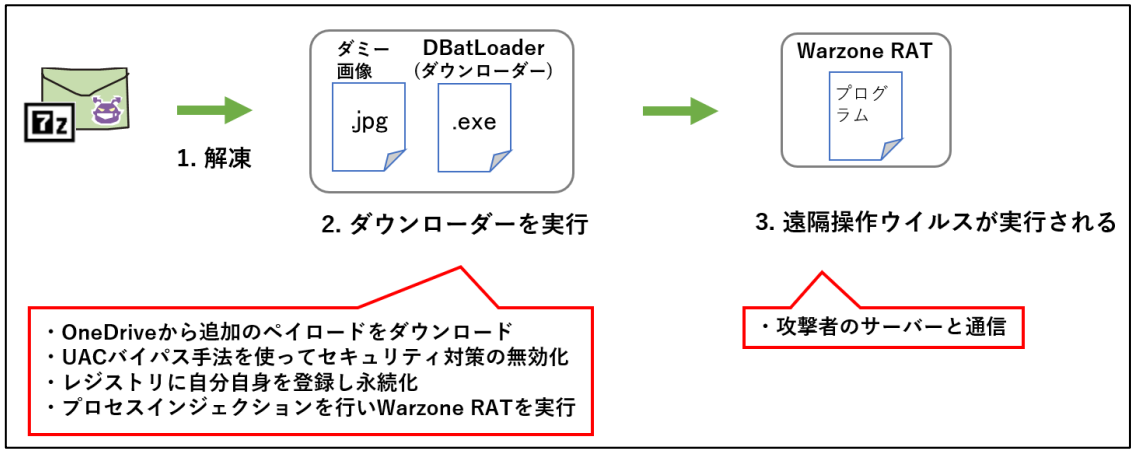

図 8 ウイルス感染までの流れ

1. 添付ファイルの解凍

メールに添付されていたファイルは、1 つの圧縮されたファイル（拡張子：.7z）である。これを解凍すると、画像ファイル（拡張子：.jpg）と実行ファイル（拡張子：.exe）が展開される（図 9）。

画像ファイルは、白い画像であり、ダミーのファイルと考えられる。実行ファイルは、Adobe Illustrator 向けの画像形式である AI ファイル（拡張子：.ai）のアイコンに似せてあった。なお、これらのファイル名は、いずれも「Order Samples 【英数字の羅列】.【拡張子】」となっていた。

この実行ファイルは、一連の動作から「DBatLoader」と呼ばれるウイルス（ダウンローダー）であると考えられる。攻撃者は、メールの受信者に対し、添付ファイルの中身がメール本文に言及のあった商品の情報であると誤認させ、添付ファイルを実行させることを狙ったものと考えられる。

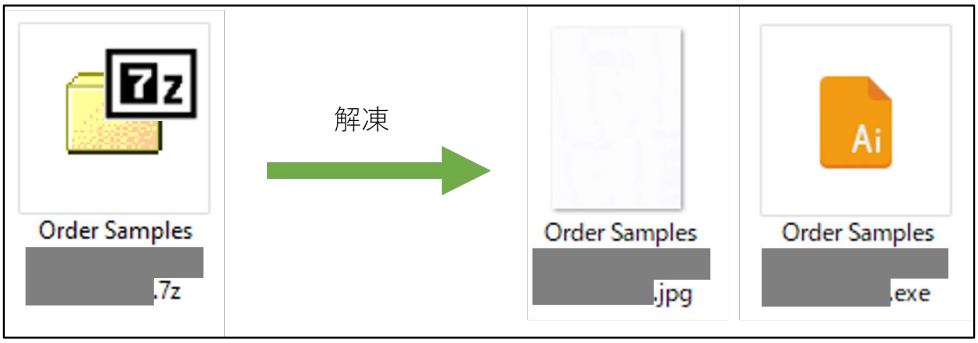

図 9 添付ファイルと解凍後のファイル

2. ダウンローダーの実行

ダウンローダーを実行すると、Microsoft OneDrive にアクセスし追加のペイロード（後続で使うファイルが含まれたデータ）をダウンロードする。このペイロードは、後続のセキュリティ対策無効化や遠隔操作ウイルス（RAT）に使われる。業務でも一般的に使用されるクラウドストレージを悪用することで、通信を遮断されることなくペイロードのダウンロードを試みるものと考えられる。

ダウンローダーは、自分自身がユーザのログイン時に自動で実行されるように、自信をレジストリに登録し、感染の永続化を図っていた。また、レジストリに登録したダウンローダーが Windows Defender により検疫されないように、Windows Defender のスキャン対象から除外する設定も行っていた。通常、Windows Defender の設定変更には管理者権限が必要であるが、Windows（OS）が信頼できると認識するフォルダを作成し、その中で悪意のあるファイルを実行することで、UAC（ユーザーアカウント制御）をバイパスしていた [17]。これにより、管理者権限を用いることなく Windows Defender の設定変更が行われていた。

3. 遠隔操作ウイルス(RAT)の実行

ダウンローダーは、正規のプロセスにプロセスインジェクションを行い、遠隔操作ウイルス （RAT）である「Warzone RAT」を実行する。このウイルスは、定期的に特定の IP アドレスに対して通信を試みる。これは C&C サーバーに接続して攻撃者からの指令を受け取るためと考えられる。

「Warzone RAT」は、マルウェアをサービスとして提供する MaaS（Malware as a Service）としてウェブサイト上で販売されているウイルスである。自分自身でウイルスを開発する技術がない攻撃者でも、MaaS として販売されているウイルスを使うことで攻撃が可能となる。本事例はそのような攻撃者により作成された攻撃メールである可能性も考えられる。

3.3 類似検体

IPA にて、本事例の差出人（From ヘッダ）をもとに公開情報を調査したところ、メール本文がロシア語や英語で記載された複数の類似検体が 2023 年 10 月初旬から送られていることを確認できた。なお、本事例の不審メールは 10 月下旬に A 社へ着信している。いくつかの類似検体を確認したところ、いずれも本事例のメールとは本文や添付ファイル名が異なるものの、受信者に添付ファイルを開かせて実行させるという点や、添付ファイルの形式・動作がほぼ同一であった。このことから、本事例のメールを含めたこれらのメールは、同一のウイルスを使ったばらまき型の攻撃メールであると推測される。確認した類似検体のうち、英語で書かれた類似検体の例を図 10 に示す。

[17] Bleeping Computer「Old Windows ‘Mock Folders’ UAC bypass used to drop malware」
https://www.bleepingcomputer.com/news/security/old-windows-mock-folders-uac-bypass-used-to-drop-malware/

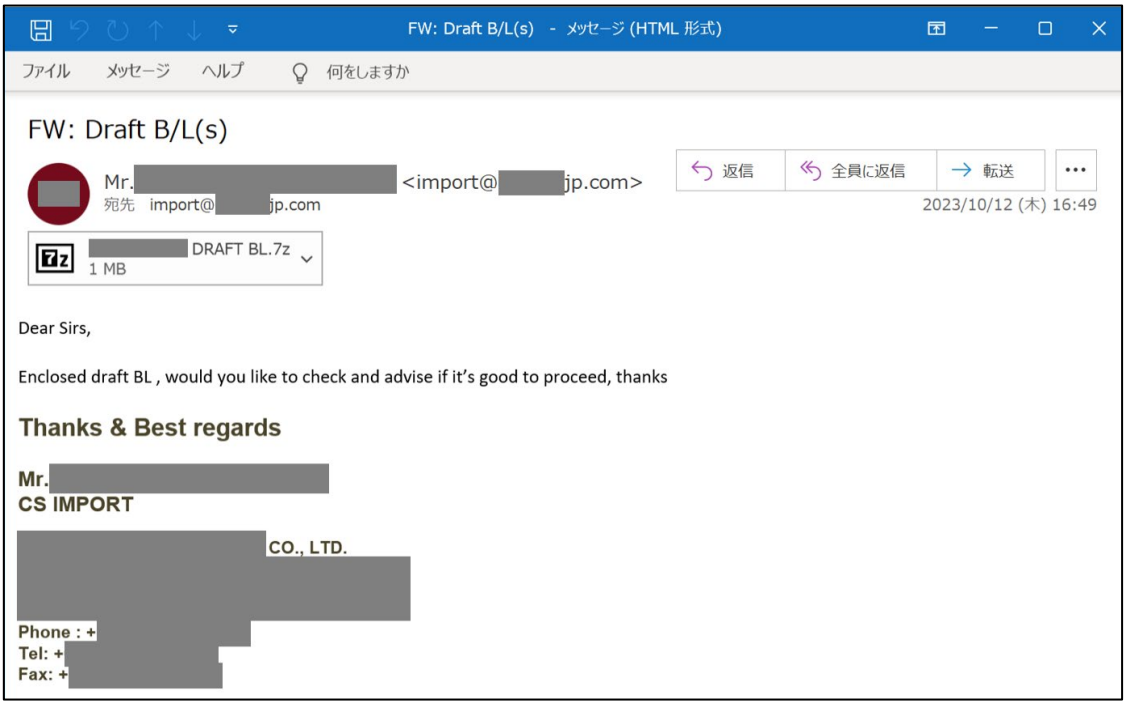

図 10 類似メールの例

3.4 まとめ

本事例では、A 社より情報提供のあった不審メールおよびその類似検体の調査により、最終的に遠隔操作ウイルス（RAT)に感染させることを企図したばらまき型の攻撃メールであることを確認した。また、今回使われた遠隔操作ウイルス（RAT）は、MaaS として販売されているウイルスであることも確認した。MaaS で販売されているウイルスを使うことは、ウイルスを開発する技術がない攻撃者でもばらまき型攻撃等への参入が容易になり、攻撃が増えることも考えられる。

ばらまき型の攻撃メールは、誰にでも通用するような内容であり、添付ファイルや URL リンクを開かせるように誘導するケースがほとんどである。また、受信者にとっては心当たりがなく、慎重に確認すると不自然な点が見られるケースが多い。本事例の不審メールも、A 社以外の組織にも通用するような内容であり、添付ファイルを開くように誘導していた。さらに、メール本文が英語でありながらも、署名には日本語が使われている等、通常のビジネスメールとしては不自然な点が見られた。

不審なメールを受信した場合には、添付ファイルや URL リンクを開かずに、組織の情報セキュリティ部門等の所定の通報先に連絡を入れる等の基本的な対応を行うことが重要である。また、報告を受けた不審メールの調査を実施し、必要に応じて組織内への注意喚起やセキュリティ対策製品のフィルタリング設定の調整等を行うことで、類似した不審メールによる被害の防止に繋げてほしい。加えて、組織の脅威となりうる攻撃情報が、公的機関等から注意喚起として出された場合にも、それらの情報を組織内に周知する等の対応を取ってほしい。

4　FAX 受信通知を装いセキュリティ製品の回避を図るフィッシング攻撃

本事例は、J-CSIP の参加組織（以下、A 社）にて、Microsoft アカウントの認証情報の詐取が目的とみられるフィッシングメール数十件が、セキュリティ製品による検知をすり抜けて従業員まで届いたというものである。

本章では、実際に A 社に着信したフィッシングメールを示した上で、本件のフィッシング攻撃で使われている、セキュリティ製品による検知の回避等を企図したものとみられる以下の 5 つの手法について説明する。

- 画面表示に影響しない Unicode 制御文字を挿入する手法
- 別メールから流用したとみられるメール文を挿入する手法
- 実在する組織のメールアカウントから送信する手法
- 複数種類のリダイレクトを経てフィッシングサイトに遷移させる手法
- フィッシングサイトに CAPTCHA 認証を使用する手法

はじめに、A 社に着信したフィッシングメールを、図 11 に示す。

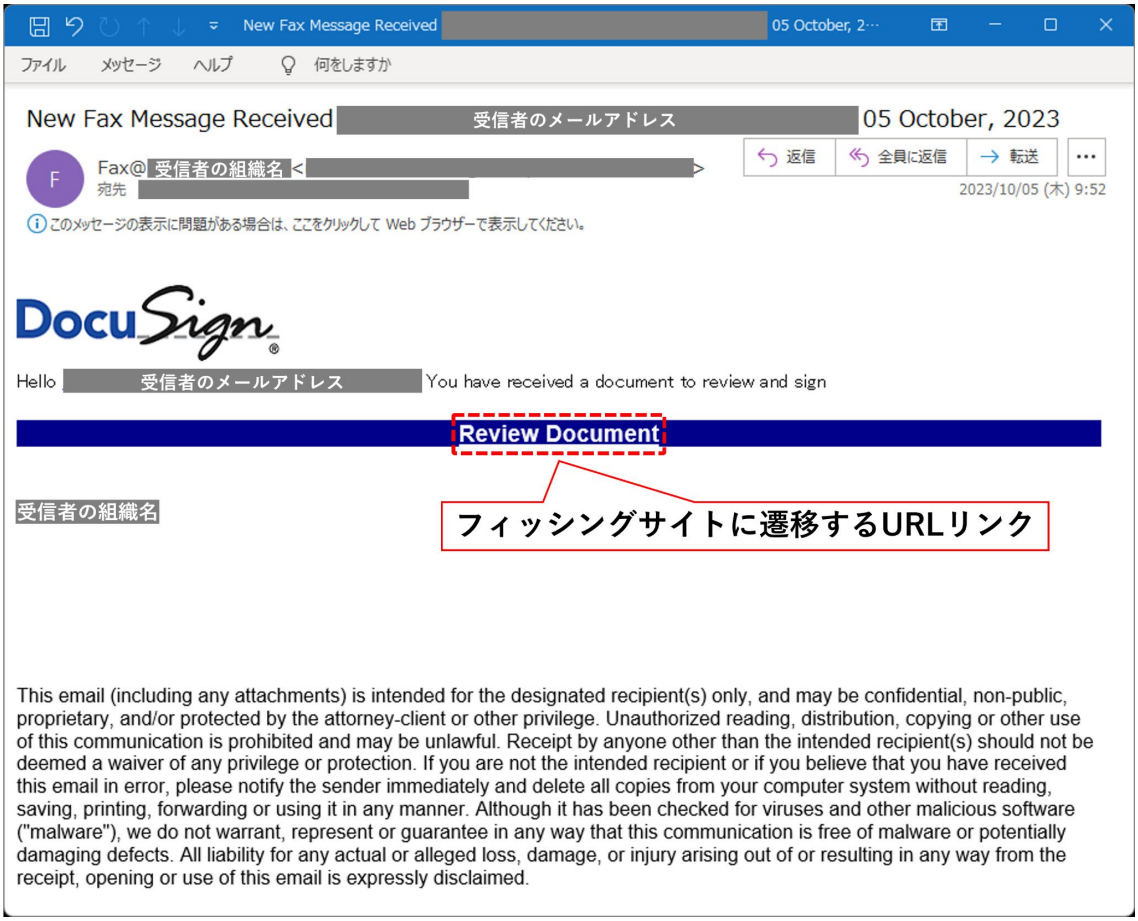

図 11 A 社に着信したフィッシングメール

このメールは、DocuSign[18]からの FAX 受信を通知するメールを装ったものであり、文書の確認とサインを促すメッセージが英語で記載されていた。また、本文中の「Review Document」と表示された箇所には、図 12 に示すフィッシングサイトに遷移する URL リンクが設定されていた。

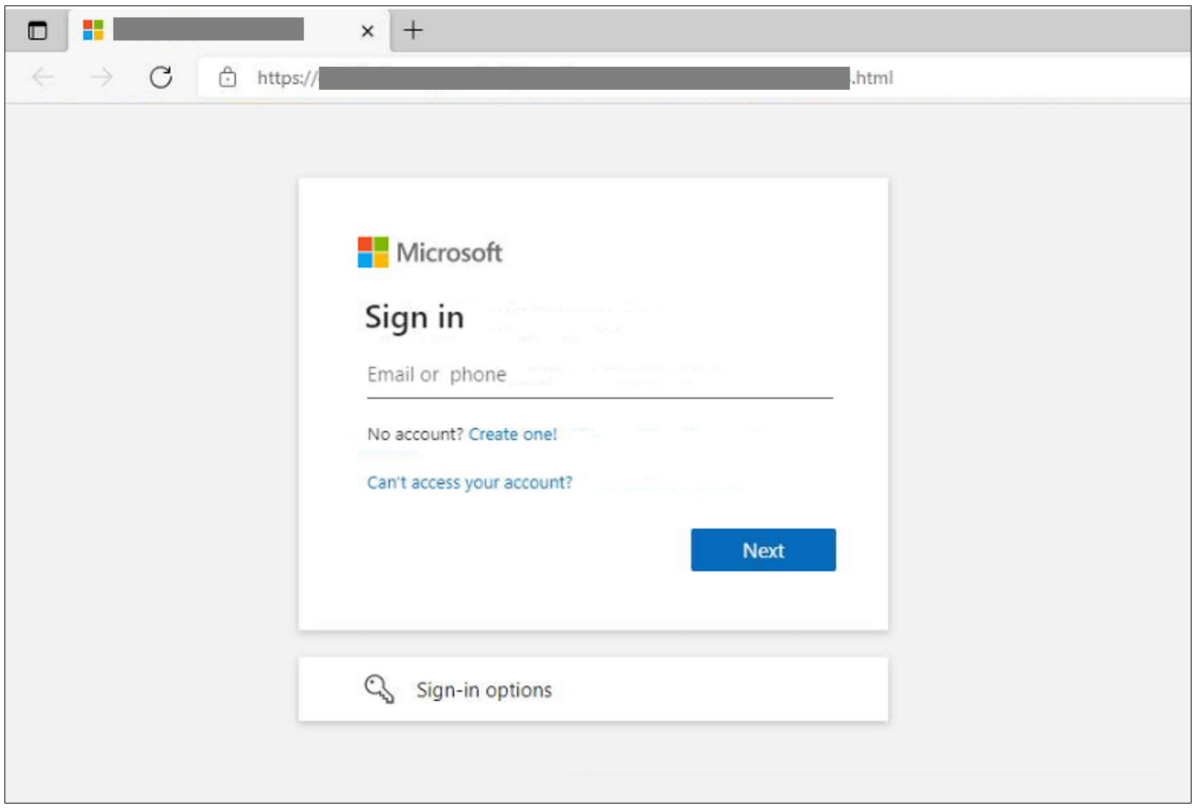

図 12 メール中の URL リンクから遷移するフィッシングサイト

フィッシングサイトに遷移すると Microsoft アカウントの入力を促す画面が表示されることから、本件は Microsoft アカウントの認証情報の詐取を企図したものであったと考えられる。

前述した検知回避等の手法について、次節以降で順に説明する。

[18] DocuSign 社が提供する電子署名サービス
https://www.docusign.com/ja-jp

4.1 画面表示に影響しない Unicode 制御文字を挿入する手法

本件の攻撃メール本文は、メーラー上で表示すると一見通常の英文のように見えるが、ソースコードを表示すると、図 13 に示すようにゼロ幅非接合子の Unicode 制御文字（U+200c）が複数個所の単語の文字列中に挿入されていた。

図 13 画面表示に影響しない Unicode 制御文字の挿入例

この文字が文字列中に挿入されてもメーラー上の表示には影響を与えないが、文字は挿入されているため、機械的な文字列検索は阻害される。攻撃者はこれを悪用し、人間がメーラー上で閲覧した際には違和感を与えずに、メールフィルタによるシグネチャ検出の回避を狙ったと推測される[19]。

[19] Alex Labs「Bypassing phishing filters with “quoted-printable” – ?utf-8?」
https://alex-labs.com/bypassing-phishing-filters-with-quoted-printable-utf-8/

4.2 別メールから流用したとみられるメール文を挿入する手法

本件の攻撃メール本文は HTML で作成されており、大きくは次の 3 つのブロックで構成されていた。1 つ目はメール受信者に URL リンクのクリックを促す騙しの文章、2 つ目はフィッシングサイトへ遷移させる URL リンク、3 つ目は「もしも本来の受信者以外が受信した場合、本メールを破棄してほしい」といった内容の定型的な免責事項であった。このうち、3 つ目のブロックについては何らか別のメールから HTML を流用して付け加えたような形跡があった。メールの HTML ソースコードのイメージを図 14 に示す。

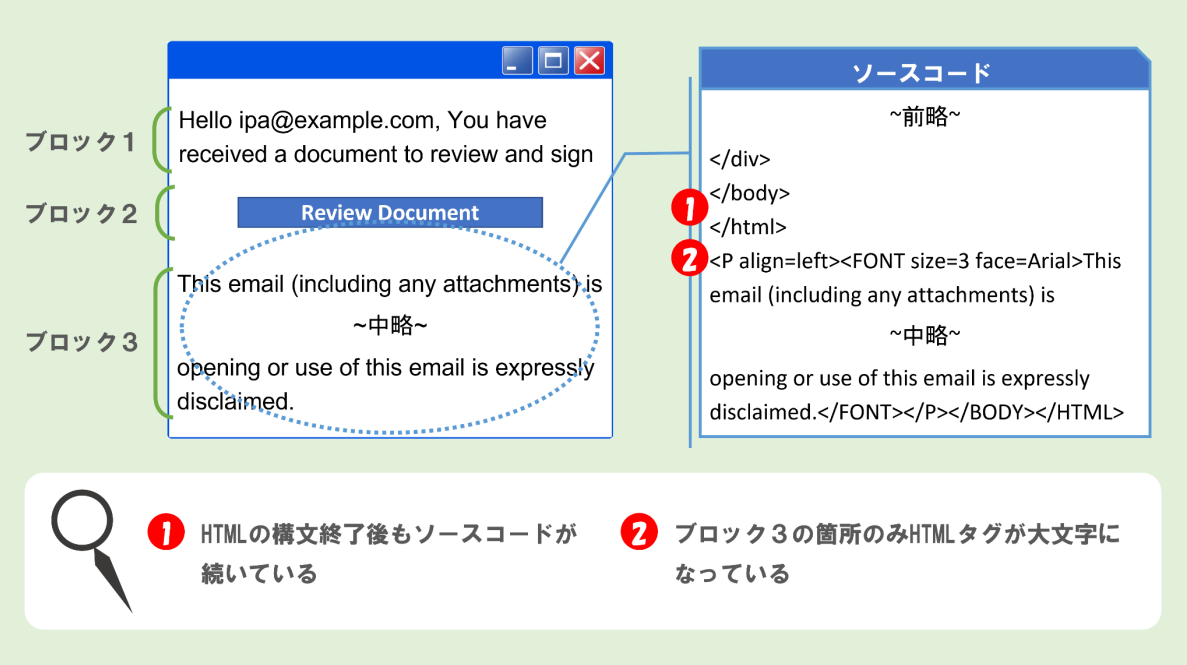

図 14 別メールからの流用とみられる HTML ソースコード

図示の通り、当該箇所からは一度 HTML の構文が終了した後もソースコードが続いていることや、HTML タグの書き方（大文字小文字）がメール末尾の免責事項部分のみ異なる表記となっていることが確認できる。このことから、攻撃者が何らか別のメールから HTML を流用して付け加えた可能性が考えられる。

これには、定型句的な文章を追記することで、メールを受信した人物にあたかも正規のメールであるかのように誤認させる狙いがあったと推測される。

4.3 実在する組織のメールアカウントから送信する手法

本メールは、メールヘッダ等の情報から、攻撃者が実在する組織のメールアカウントを何らかの方法で乗っ取った上で、当該メールアカウントから送信されたものと考えられる。

これは、攻撃者が実在する組織の正規のメールアドレスを送信元として悪用することで、フリーメール等の信頼度の低い送信元のメールを検知・検疫するメールフィルタを回避する狙いがあったと推測される。また、本件のように正規のメールアカウントを乗っ取って送信されたメールは、正規のメール配送経路を通って受信者の元に到達することから、送信ドメイン認証（SPF/DKIM/DMARC）を導入していても着信を防ぐことができない点にも注意が必要である。

4.4 複数のリダイレクトを経てフィッシングサイトに遷移させる手法

本件の攻撃は、ユーザがメール中の URL リンクをクリックするとフィッシングサイトへ遷移する仕組みであった。その遷移の過程において、ユーザ操作はメール中の URL リンクのクリック一度のみであるが、ブラウザ上ではフィッシングサイト表示前に自動で別の二つの URL を経由する仕組みとなっていた。フィッシングサイトに遷移する流れは次の通りである。

メール中に設定された URL リンクは外部のトラッキング URL サービスのものであり [20]、アクセスすると HTTP ステータスコード 302 のレスポンスが返され、別の URL にリダイレクトされる。当該リダイレクト先の URL から返される HTTP レスポンスボディには、さらに別の URL にリダイレクトされる JavaScript のコードが含まれており、それがブラウザで読み込まれることで自動的にフィッシングサイトに遷移させられる。

メール中の URL リンククリックからフィッシングサイトに至る遷移のイメージを図 15 に示す。

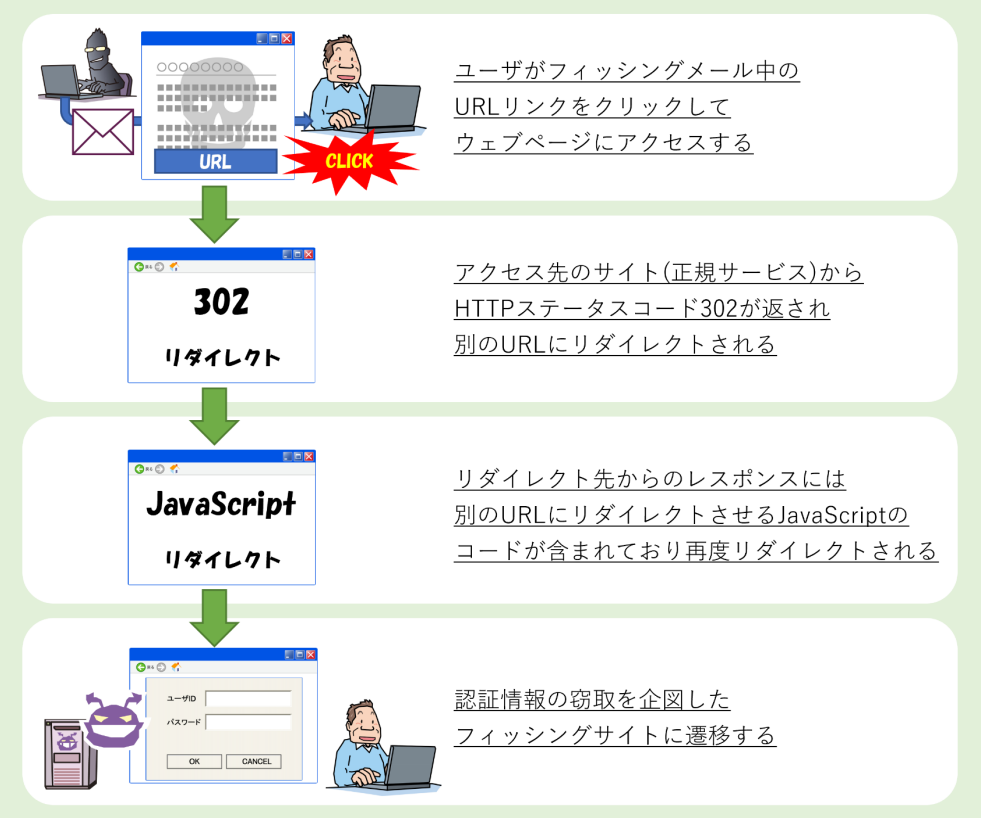

図 15 フィッシングサイトへの遷移(イメージ図)

攻撃者は、フィッシングサイトの URL を直接メール中に書くのではなく、正規サービスの URL を含む異なる方式のリダイレクトを挟んで遷移させることで、セキュリティ製品による検知を回避しようとしたものと推測される。

[20] Cofense「Zoom Phish Sent Via Constant Contact Mailer」
https://cofense.com/blog/zoom-phish-constant-contact/

4.5 フィッシングサイトに CAPTCHA 認証を使用する手法

メール中の URL リンクから最終的に遷移するフィッシングサイトは、図 16 に示す CAPTCHA 認証画面が表示されるように設定されており、チェックボックスにチェックを入れ認証を行うと図 12 のフィッシングサイトに遷移するようになっていた。

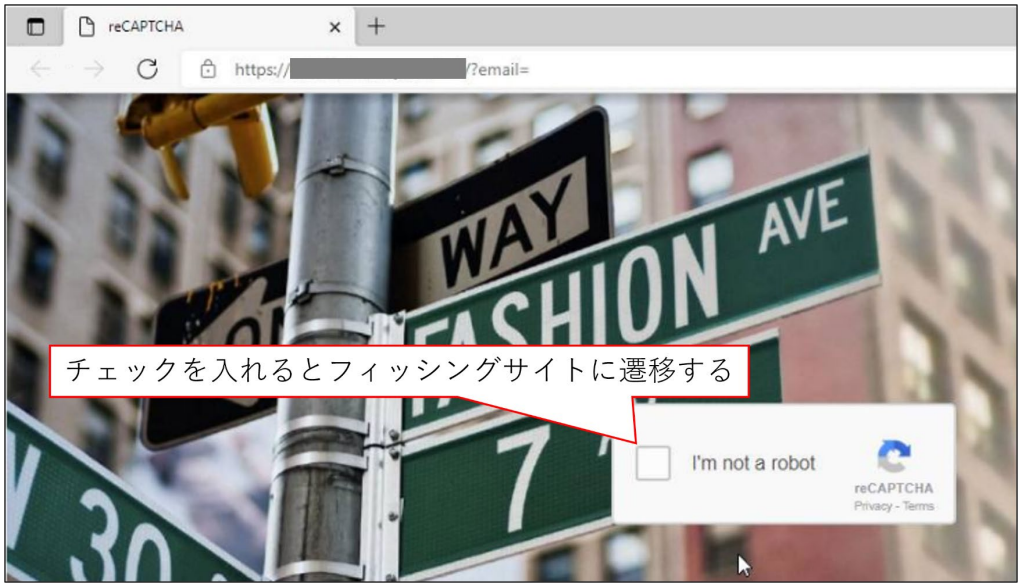

図 16 CAPTCHA 認証画面

これには、セキュリティ製品のクローリングによる悪性サイトの検出を回避する狙いがあったと推測される。

4.6 まとめ

これまでに述べた通り、本章で取り上げたフィッシング攻撃には、セキュリティ製品による検知の回避等を企図したものとみられる複数の手法が用いられており、実際に本メールを受けた組織においても検知を回避して複数の従業員の元に着信していた。

本件に類するフィッシング攻撃の対策については、「サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 7 月～9 月]」[21]の「3.3 フィッシング攻撃への対策」を参照いただきたい。

認証情報の詐取を企図したフィッシング攻撃は組織の内部ネットワークへの侵入の足掛かりとして利用される恐れもあり、そこから侵入を拡大された場合には組織に甚大な被害を及ぼすリスクもある。十分な対策を検討の上、脅威に備えていただきたい。なお、十分な技術的対策が整えられていても、本件同様に攻撃メールが検知をかいくぐり利用者の元に到達してしまう可能性もある。攻撃を防ぐためには、技術的な対策のみでなく、従業員教育のような人的な対策も組み合わせた多層防御の体制を整備することが必要不可欠である。

[21] 独立行政法人情報処理推進機構（IPA）「サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023 年 7 月～9 月]」
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf

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

また、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。標的型サイバー攻撃に関してのご相談や、提供可能な情報がありましたら、以下の窓口までご連絡ください。

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