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]

2023 年 11 月 9 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 9 月末時点の運用体制と、2023 年 7 月～9 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。

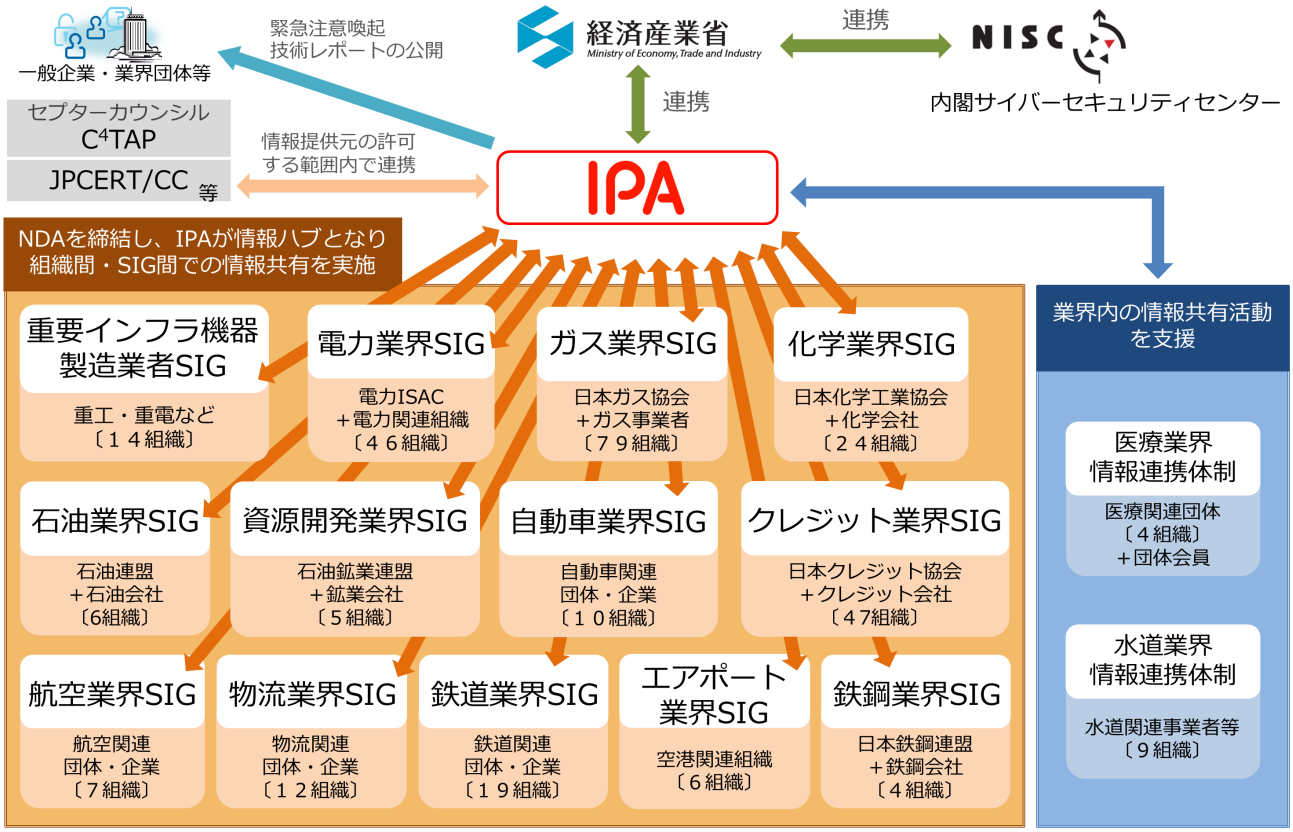

図　1 J-CSIP の体制図

---

[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 7 月～9 月）

2023 年 7 月～9 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 7 月～9 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（9 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**		
		10 月～12 月	1 月～3 月	4 月～6 月	**7 月～9 月**
1	IPA への情報提供件数	26 件	59 件	26 件	**24 件**
2	参加組織への情報共有実施件数 ※1	25 件	22 件	23 件	**22 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 **17 件**を含む。

本四半期は情報提供件数が **24 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 **5 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。

- セキュリティ製品による検知をすり抜けたフィッシングメールに関する情報提供があった。このフィッシングメールには、組織内のセキュリティ対策を回避するための手法が複数使われており、数百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、3.1 節で述べる。

- QR コードを悪用したフィッシングメールに関する情報提供があった。 このフィッシングメールには、ユーザをフィッシングサイトに誘導する QR コードが貼り付けられており、URL リンクの文字列で悪性かを判別するようなメールのセキュリティ製品を回避する目的があったと考えられる。また、この QR コードをスマートフォン等の組織の管理下にない端末で読み取らせアクセスさせることで、組織内のセキュリティ対策の回避を狙った可能性も考えられる。詳細については、3.2 節で述べる。

- ネットワーク機器の脆弱性を悪用した攻撃に関する情報提供があった。情報提供元によると、関連組織が公開された脆弱性情報をもとに調査を行ったところ、Array Networks 社および Citrix Systems 社の VPN 機器の脆弱性を悪用した攻撃の痕跡を確認したとのことであった。この攻撃では、攻撃者によって WebShell を不正に設置されたとのことだが、その手口は情報提供の範囲外であったため不明である。
  外部からの攻撃を受ける可能性がある IT 資産、いわゆるアタックサーフェス（攻撃対象領域）に脆弱性が残存していた場合、そこから社内ネットワークに侵入され、機密情報の窃取やデータの暗号化など様々な被害に繋がる恐れがある。組織においては、自組織のアタックサーフェスを把握および最小化することに加え、定期的に抜け漏れや脆弱性の有無を確認するなどして、適切に管理することが重要である [4]。

- ウェブサイトに対する外部からの不審なアクセスを遮断する方法について情報提供があった。
  情報提供元では、自社のウェブサイトへの攻撃対策として、WAF（Web Application Firewall）による遮断に加え、不審なアクセス元の IP アドレスやそれに紐づく AS 番号によるフィルタリングを実施していた。ただし、IP アドレスによっては正規の通信が混在するものもあり、フィルタリングしてしまうことで、それらも遮断してしまう恐れがあったため、加えて TLS 通信のパラメータである「TLS フィンガープリント」を用いてアクセス元端末を識別する遮断方法を検討し、WAF に導入したとのことであった。
  不審なアクセスを送信元 IP アドレスといった低いネットワークレイヤーで遮断することは、セキュリティ対策の観点からは望ましいものの、正規の通信も遮断してしまう恐れがある。組織においては、日ごろからウェブサイトに対する不審なアクセスを監視し、複数の遮断方法を組み合わせることや、定期的に検知やブロックのルールの見直しを行うことで、正規の通信への影響を抑えつつ攻撃を遮断することが重要である。

- 自社の類似ドメインが第三者に取得されていることを発見したとの情報提供があった。情報提供元では、対応としてメール送受信時に類似ドメインを遮断する設定や、類似ドメインとそれに紐づく IP アドレスへのウェブアクセスを制限する設定などを行った。
  自社の類似ドメインや、企業名・ブランド名を含むドメイン等が悪意を持った第三者によって取得されると、そのドメインを悪用して、自組織を騙るフィッシング攻撃やウイルスの配布、詐欺等が行われる恐れがある。組織においては、調査や外部からの報告で類似ドメインの悪用が発覚した場合には、被害の拡大を防止するため、ウェブサイトなどで注意喚起を行い周知することが望ましい。また、類似ドメインが第三者に取得された際に通知を受け取れるサービスの利用や、定期的な調査も、類似ドメインを悪用した攻撃の予兆を捉えるという観点では有効であると考える。

---

[4] 経済産業省 商務情報政策局 サイバーセキュリティ「「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」を取りまとめました」
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

- メールの開封確認の要求が設定された不審なメールに関する情報提供があった。このメールには、メールソフトの機能による開封済みメッセージの応答要求が設定されていた。受信者はこのメールを開封せず削除したが、自動で要求に応答する設定が有効になっており（図 2）、気づかないうちに未開封であることを示す応答メールを送信してしまっていた。送信者の目的は不明だが、宛先メールアドレスが実在しているか、メールアドレスの所有者が実際にメールを開封したか、応答メールのヘッダ情報から読み取れる受信者の環境等の情報を収集することが目的であった可能性が考えられる。
IPA にて公開情報を調査したところ、この開封確認機能を悪用した攻撃に関する情報は確認できなかったが、応答メールに含まれる情報を悪用されないよう、自動応答を設定した際の動作は事前に確認してほしい。確認が難しい場合には、業務上必要な場合を除き、自動応答の設定を選択しないことを勧める。

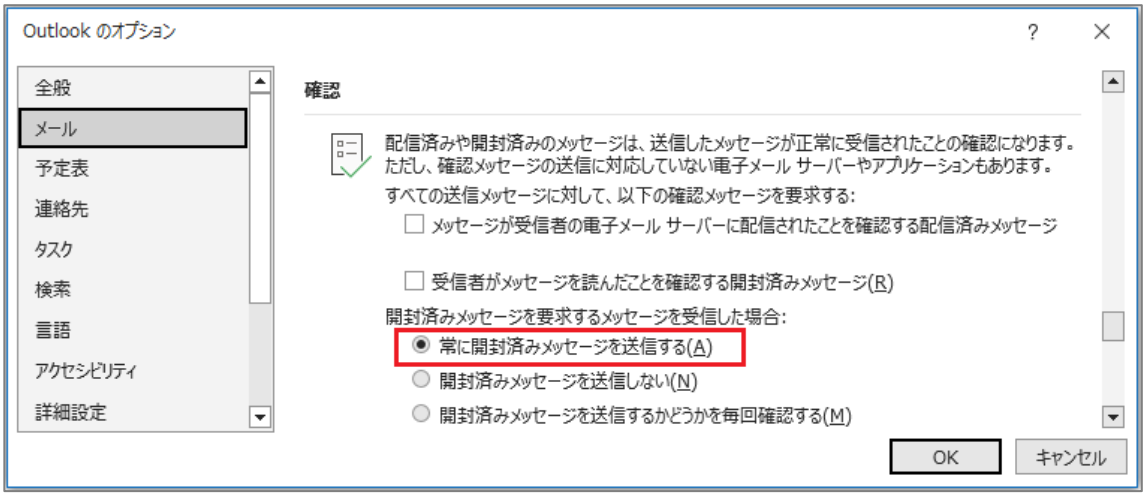

図 2 開封確認に自動で応答する設定（Microsoft Outlook の場合）

3　巧妙な手法が組み合わされたフィッシング攻撃の事例

本四半期では、J-CSIP 参加組織から複数のフィッシングメールに関する情報提供があった。これらのメールを使ったフィッシング攻撃では、セキュリティ製品による検知を回避するための巧妙な手法が組み合わされていた。

フィッシング攻撃により認証情報が詐取されてしまうと、組織への標的型攻撃や侵入型ランサムウェア攻撃、ビジネスメール詐欺（BEC）等、様々な攻撃に悪用される恐れがある。また、近年ではダークウェブ等でフィッシング攻撃に必要なツールやインフラを提供する「PhaaS（Phishing as a Service）」の存在も確認されている [5]。これにより、今後、フィッシング攻撃のノウハウがない攻撃者の参入が増え、巧妙なフィッシング攻撃も拡大することが見込まれ、フィッシング対策の重要性は増していくと考えられる。

本章では、J-CSIP 参加組織から情報提供があったフィッシングメールのうち 2 件を取り上げ、各メールで用いられたセキュリティ製品による検知を回避するための手法について詳しく説明する。

3.1 複数の手法でセキュリティ製品の回避を試みるフィッシング攻撃

本事例は、J-CSIP の参加組織(以下、A 社)において、Microsoft アカウントの認証情報の詐取を目的としたフィッシングメール数百件がセキュリティ製品による検知をすり抜け、従業員まで届いたというものである。当該メールを受信した従業員のうち、約 2%がメール文中の URL リンクをクリックしてしまったが、A 社で導入していたアクセス先の URL を評価するセキュリティ製品がアクセスを遮断したため、被害は発生しなかった。

IPA で調査したところ、本事例のフィッシング攻撃には、次に示す特徴的な手法が使われていた。

（1）本文に大量の空行を挿入する手法
（2）セキュリティ製品に通常のメールのやり取りと誤認させる手法
（3）オープンリダイレクトの脆弱性があるサイトを経由する手法
（4）フィッシングサイトに CAPTCHA 認証を使う手法

次の項より、それぞれの手法について、詳細を記載する。

---

[5] GROUP-IB 「W3LL oiled machine: Group-IB uncovers covert BEC phishing empire targeting Microsoft 365 - report」
https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

3.1.1 本文に大量の空行を挿入する手法

本事例のフィッシングメールは、図 3 に示す構成となっていた。

図 3 本事例のメールの構成イメージ

本事例で実際に受信したフィッシングメールの前半部分を、図 4 に示す。

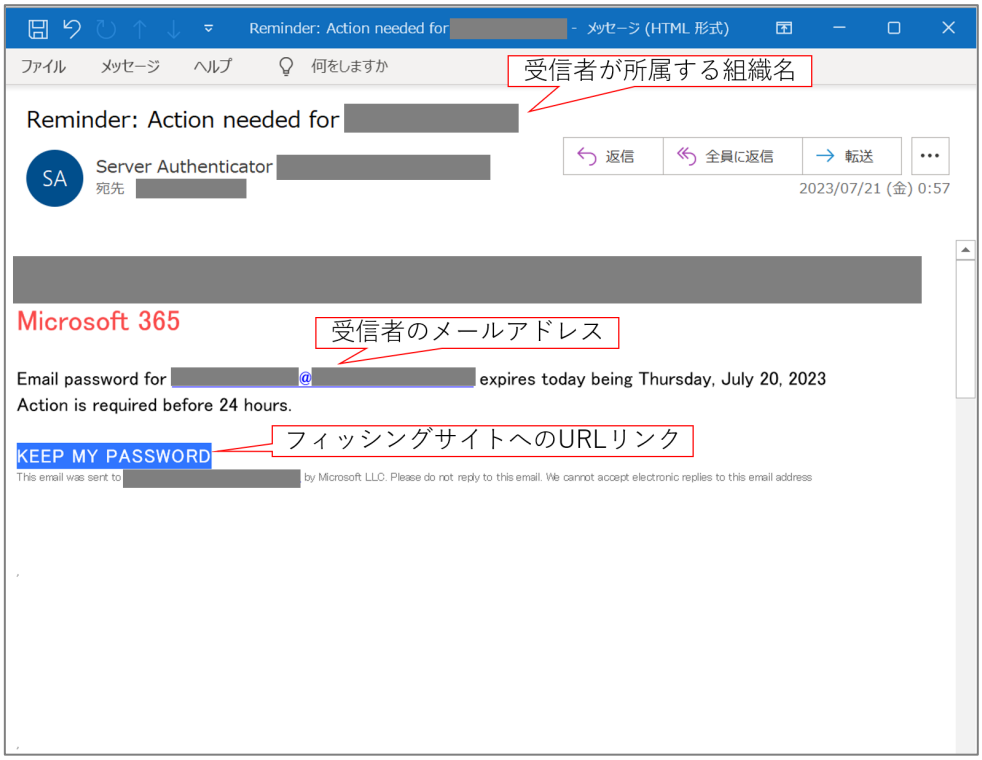

図 4 実際に送られてきたフィッシングメール（前半部分）

メール本文は、Microsoft 365 からの通知を装い、「本日パスワードの有効期限が切れるため、24 時間以内に対応が必要である」という内容で、手続きのために「KEEP MY PASSWORD」と記載されている部分(URL リンク)をクリックさせることにより、フィッシングサイトへ誘導するものであった。

また、メールの前半部分と後半部分の間にある空行によって、一見すると「KEEP MY PASSWORD」の次の行でメール本文が終了しているように見える。しかし、実際には大量の空行が挿入されており、メール本文は継続していた。この大量の空行は、受信者に対して、最初に表示させる前半部分（受信者を騙すための文章）でメール本文が終わったと誤認させ、メール後半の文章の存在に気付かせないために設けられたと考えられる。

3.1.2 セキュリティ製品に通常のメールのやり取りと誤認させる手法

フィッシングメールの後半部分には、一般的な内容のメール文章とそれに返信する文章が記載されていた。なお、これらの文章は A 社受信者とは無関係な内容であった。

実際のフィッシングメールの後半部分を図 5 に示す。

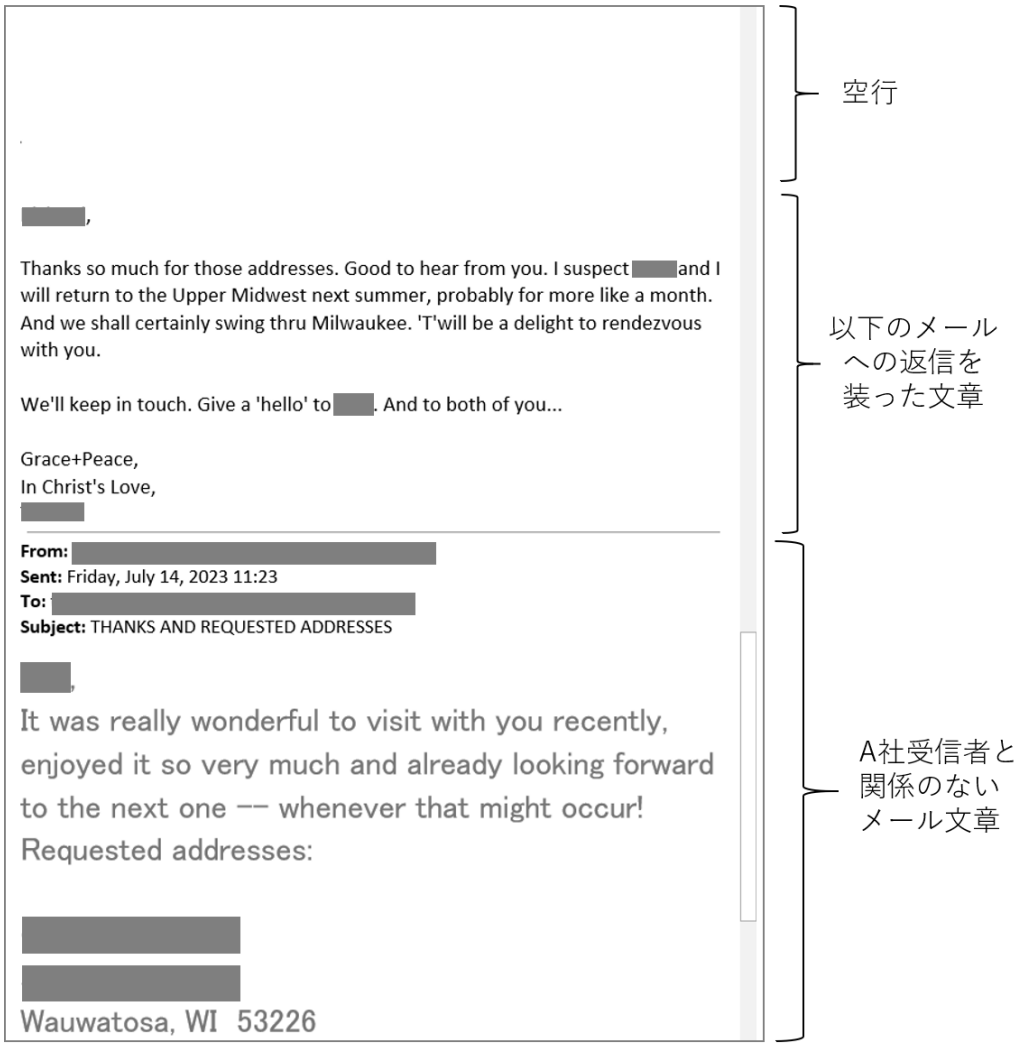

図 5 実際に送られてきたフィッシングメール（後半部分）

メールの後半部分に A 社受信者とは関係のないメール文章とそれに対する返信文章を入れることで、メールのセキュリティ製品に対して、通常のメールのやり取りと誤認させ、フィッシングメールと判定されることを回避する目的があったと推測される[6]。

なお、攻撃者が用意したこのメール文章が、攻撃者が作成した架空のものなのか、実際にやり取りされたものかは不明である。

[6] 株式会社セキュアブレイン「メールフィルタをすり抜けるフィッシングメール～攻撃者はどんな情報も悪用する！？」
https://www.securebrain.co.jp/blog/2023/0613/

3.1.3 オープンリダイレクトの脆弱性があるサイトを経由する手法

メール本文中の URL リンクは、図 6 に示す構成となっていた。

https://【正規サイトのドメイン】 / 【リダイレクトを行うパラメータ】=【フィッシングサイトのURL】
└ オープンリダイレクトの脆弱性があるサイトを悪用 ┘

図 6 オープンリダイレクトの脆弱性があるサイトを悪用する URL リンク

この URL リンクをクリックすると、オープンリダイレクトの脆弱性があるサイトにアクセスした後に、フィッシングサイトへリダイレクトされる。これは、フィッシングサイトの URL を隠し、URL リンクが正規サイトのものであると見せかけ、セキュリティ製品による検知の回避を企図したものと考えられる [7]。

3.1.4 フィッシングサイトに CAPTCHA 認証を使う手法

URL リンクをクリック後に最終的にアクセスするフィッシングサイトについて、IPA の調査時点ではアクセスすることができなかったが、A 社によるとメールが届いた時点では CAPTCHA 認証画面が表示されるサイトであったとのことだった。

そこで、IPA にて、メール本文中の URL リンク先であるオープンリダイレクトの脆弱性のあるサイトのドメインを基に公開情報を調査したところ、本事例の類似検体を見つけ、図 7 に示すような CAPTCHA 認証画面が確認できた。CAPTCHA 認証を実施すると、Microsoft アカウントのログインフォームを模したフィッシングサイトへ遷移し、パスワードの入力を求められることを確認した。本事例のメールでも、受信直後には同様の画面が表示されていたと推測される。

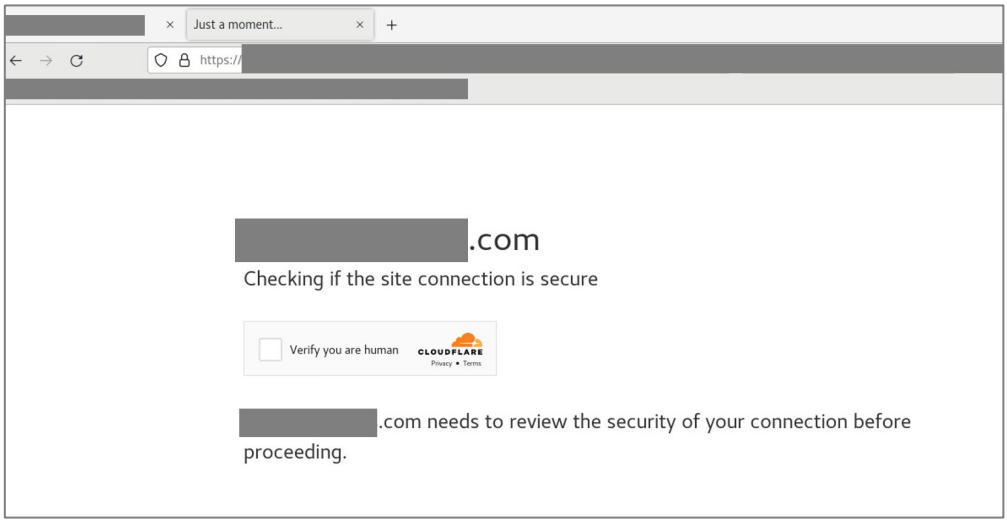

図 7 類似検体によるフィッシングサイトで表示される CAPTCHA 認証画面

CAPTCHA 認証画面の表示は、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知を回避すること

[7] 株式会社セキュアブレイン「脆弱性のある Web サイトを利用したフィッシング詐欺とは？ オープンリダイレクトを悪用したフィッシング攻撃」
https://www.securebrain.co.jp/blog/2023/0516/

を企図したものと考えられる。

3.2 QR コードを悪用したフィッシング攻撃

本事例は、J-CSIP の参加組織（以下、A 社）にて、メールアカウント情報の更新を促す不審なメールが、2023 年 7 月下旬～8 月初旬にかけて、社内の複数の従業員宛に届いたというものである。IPA で当該メールを確認したところ、本文に貼り付けられた QR コードを受信者に読み取らせることでフィッシングサイトに誘導するフィッシングメールだった。こうした QR コードを悪用したフィッシング攻撃は「Quishing（クイッシング）」などと呼ばれている [8]。

本節では、実際に A 社に着信した QR コードを悪用したフィッシングメールを示した上で、当該メールに使用されている、以下の特徴的な手法を説明する。

（1）QR コードを悪用する手法
（2）InterPlanetary File System（IPFS）を悪用する手法
（3）メールごとに異なる文字列を本文に挿入する手法

3.2.1 A 社に着信した QR コードを悪用したフィッシングメール

実際に A 社に着信した QR コードを悪用したフィッシングメールを、図 8 に示す。

[8] トレンドマイクロ株式会社「QR コードを悪用した詐欺手口と対策を解説」
https://www.trendmicro.com/ja_jp/research/22/i/hidden-scams-in-malicious-scans-how-to-use-qr-codes-safely.html
Trustwave「Think Before You Scan: The Rise of QR Codes in Phishing」
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/think-before-you-scan-the-rise-of-qr-codes-in-phishing/

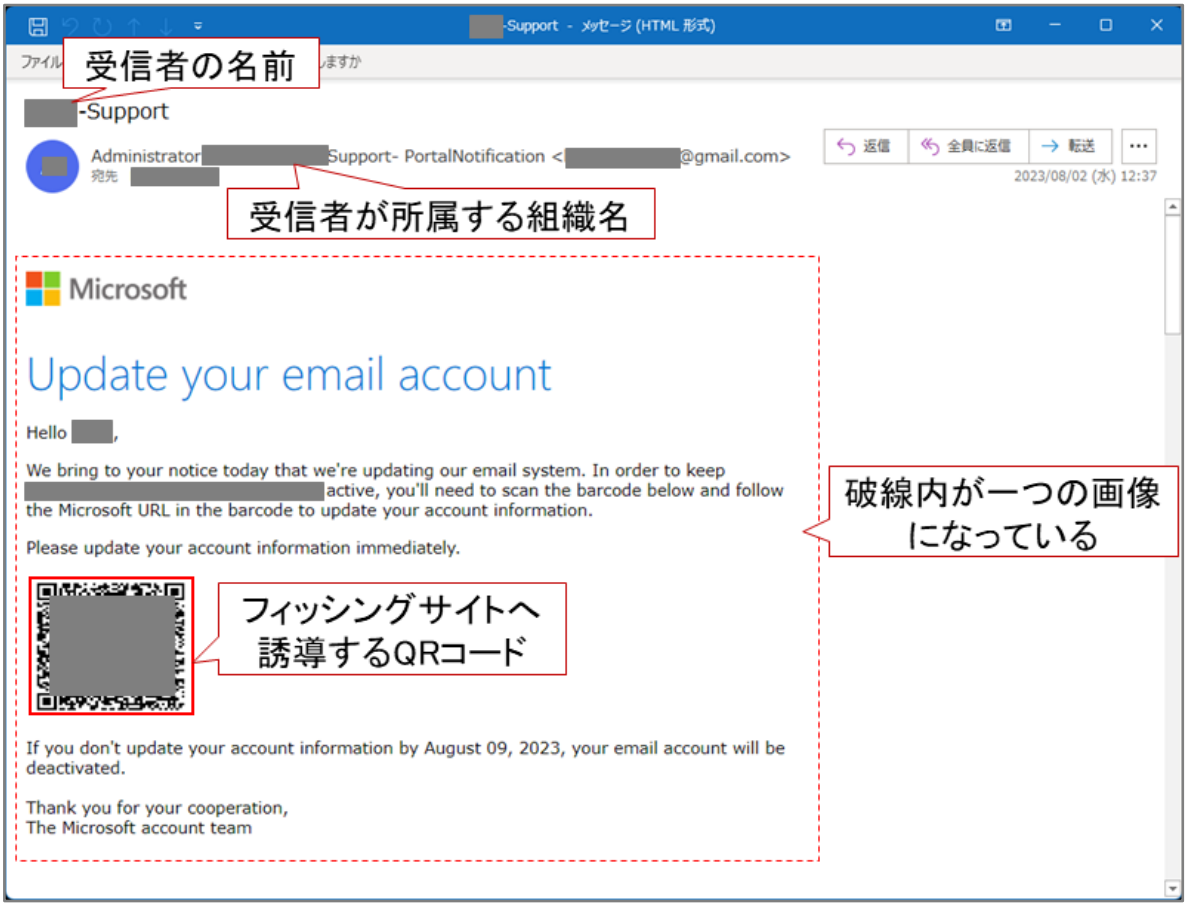

図 8　A 社に着信した QR コードを悪用したフィッシングメール（QR コードと指示の画像部分）

このフィッシングメールは、Microsoft 社からのメールアカウント情報の更新を促す通知メールに装っていた。

メールの本文部分には、QR コードと、QR コードを読み取ってメールアカウント情報を期限までに更新するように促すメッセージが書かれた一つの画像ファイルが貼り付けられていた。QR コードは、攻撃者が用意したフィッシングサイトへ誘導するための URL を変換したものだった。これを受信者がスマートフォンの QR コードリーダー（アプリ）などで読み取りアクセスすると、図 9 のような Microsoft アカウントのログインフォームを模したフィッシングサイトが表示される。

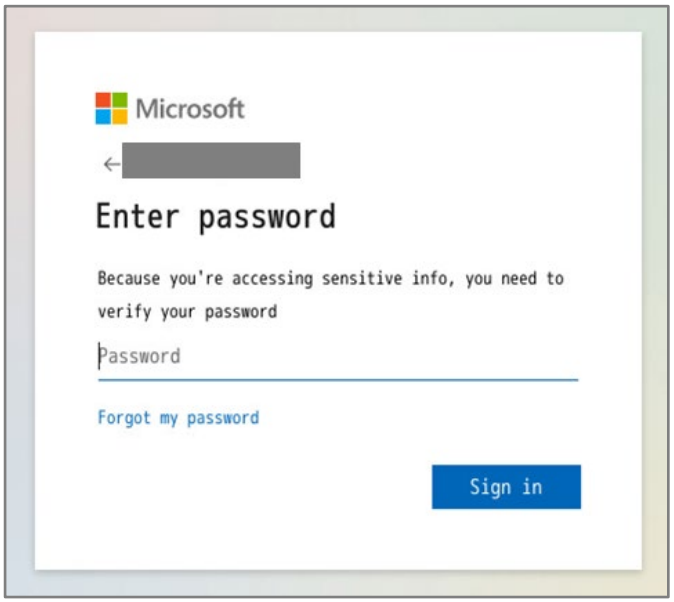

図 9 Microsoft アカウントの偽のログインフォーム

3.2.2 QR コードを悪用する手法

当該フィッシングメールでは、受信者をフィッシングサイトに誘導する手段として QR コードを悪用している。QR コードは、任意の文字列情報を 2 次元コード化したものである。フィッシングサイトの URL を QR コードに変換し、メール本文に貼り付けることで、文字列の URL を検査するようなメールのセキュリティ製品を回避する目的があったと考えられる。

また、攻撃者は、スマートフォンでフィッシングサイトにアクセスさせることで、組織内のセキュリティ対策を回避しようとしている可能性も考えられる。QR コードを読み取る際、一般的にスマートフォンの QR コードリーダー(アプリ)が使用される。受信者がスマートフォンで QR コードを読み取り、表示された URL にアクセスすると、使用環境によっては、社内ネットワークを経由せずに直接インターネットにアクセスする場合がある。このような場合、社内ネットワークに URL フィルタリングなどのセキュリティ対策を施していたとしても、その効果を得ることが難しくなる。

3.2.3 InterPlanetary File System(IPFS)を悪用する手法

当該フィッシングメールの QR コードを読み取ると、図 10 で示す URL が表示される。この URL は、「InterPlanetary File System(以下、IPFS)[9]」と呼ばれる分散型ネットワーク(以下、IPFS ネットワーク)上のデータにアクセスするためのものである。

IPFS ネットワーク上のデータは、ネットワーク上の複数のノード間で共有することができる。一度共有されたデータは削除することが難しくなるため、攻撃者はこの特性を悪用し、攻撃に関わるデータを IPFS ネットワーク上に置くことで、攻撃が妨害されないようにしたと考えられる。

---

[9] IPFS docs「What is IPFS」
https://docs.ipfs.tech/concepts/what-is-ipfs/

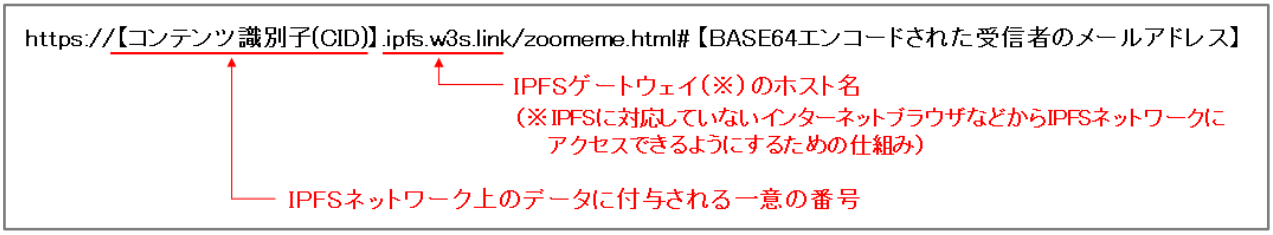

図 10　IPFS ネットワーク上のデータにアクセスするための URL

3.2.4 メールごとに異なる文字列を本文に挿入する手法

当該フィッシングメールには、前述した QR コードが貼り付けられていた以外に、スペイン語で書かれた見積依頼に関する本文が書かれていた。この本文は、図 11 のように、文中のスペース(空白)部分に英数字の文字列が挿入されており、一見しただけでは内容が読み取りづらい状態になっていた。この本文を、IPA が公開情報から入手した複数の類似メールと比較したところ、挿入された文字列を取り除いた文章は同じだったが、挿入されている文字列がメールごとに異なっていることが分かった。このことから、攻撃者はメールごとに挿入する文字列を変更し、定型的な本文にならないようにすることで、メールのセキュリティ製品の検知を回避しようとした可能性が考えられる。

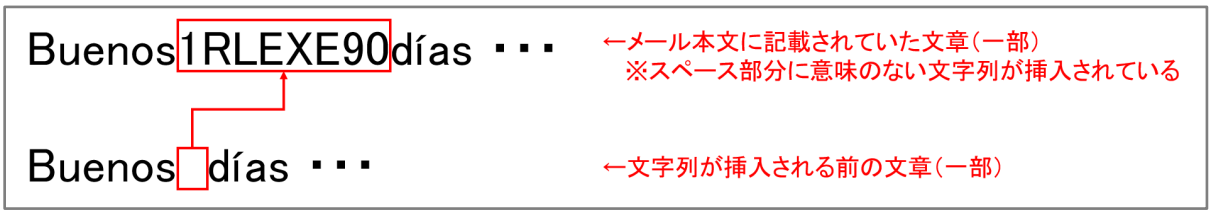

図 11　スペース(空白)部分に英数字の文字列が挿入されている本文(一部抜粋)

3.3 フィッシング攻撃への対策

3.1 節および 3.2 節で取り上げたフィッシングメールは、いずれも組織のセキュリティ製品による検知をすり抜け、複数の従業員に届いたものであった。このように、攻撃者は様々な手法を組み合わせることで、組織のセキュリティ対策を回避し、受信者から情報を騙し取ろうとする。そのため、組織においてはフィッシング攻撃の被害を受けないように、次のような複数のセキュリティ対策を組み合わせ、多層防御の仕組みを導入することが望ましい。

(1) 技術的なセキュリティ対策

[フィッシングメールを検知・ブロックするための対策]

- メールのセキュリティ製品による不審メールのフィルタリング
- 送信ドメイン認証（SPF、DKIM、DMARC）によるなりすましの検出

[フィッシングサイトへアクセスさせない対策]

- セキュリティ製品によるフィッシングサイトへのアクセス遮断
- メールのセキュリティ製品による URL リンクや添付ファイルの無害化
- フィッシング攻撃に悪用されることがあるサービス（IPFS 等）のアクセス制限
  （業務上、対象のサービスを利用しない場合）
- 業務で使用するスマートフォン等へのセキュリティ対策（URL フィルタリング 等）の導入

(2) 人的なセキュリティ対策

- 従業員への定期的なセキュリティ教育や訓練の実施
- フィッシング攻撃の新たな手口等に関する情報収集や注意喚起
- 不審なメールを受信した際の報告プロセスの策定および周知

なお、万が一、従業員が組織で利用するアカウントの認証情報（ID・パスワード）をフィッシングサイトに入力してしまった場合には、早急なパスワードの変更を行い、詐取された認証情報が悪用されないようにすることが重要である。また、従業員にパスワードの使いまわしをさせないことや多要素認証を導入することなども、認証情報が詐取された場合の被害拡大を防ぐために有効である。

フィッシング攻撃は様々なサイバー攻撃に繋がる恐れがあり、今後も増加していく可能性がある。組織においては、複数のセキュリティ対策を組み合わせる多層防御により、フィッシング攻撃の脅威に備えてほしい。

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

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