サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2022 年 4 月～6 月]

2022 年 7 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、2022 年 6 月末時点の運用体制、2022 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

2022 年 4 月～6 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 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）。

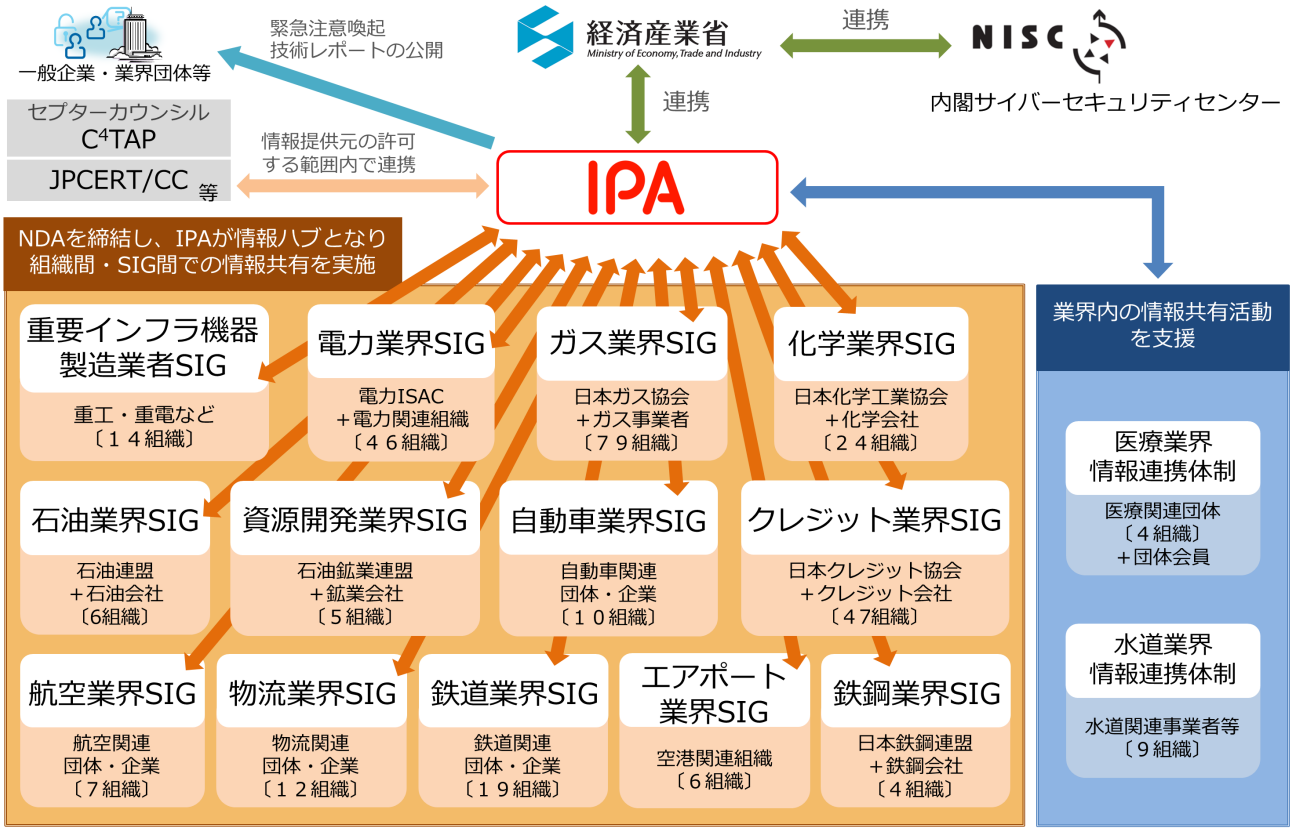

図 1 J-CSIP の体制図

[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 4 月～6 月）

2022 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 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	
		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	346 件	77 件	51 件	**134 件**
2	参加組織への情報共有実施件数※1	21 件	28 件	29 件	**35 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 **30 件**を含む。

本四半期は情報提供件数が **134 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 **4 件**であった。

このほか、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あった。この事例では攻撃者がメールアカウントを乗っ取った上で、取引先に対し偽のメールを送り付けていた。これについて 3 章で述べる。

- 参加組織の役員を騙り、組織内の複数のメールアカウントに対し、フィッシングメールを送り付けられたという攻撃に関する情報提供があった。メールに添付された PDF ファイルやフィッシングサイトには、攻撃対象の企業のロゴが使われており、当該組織を明確に狙ったものであった。これについて 4 章で述べる。

- 参加組織に対して行われた不正アクセスに関する情報を共有したところ、別の参加組織で不正接続先からのアクセス痕跡が発見された。これについて 5 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	ランサムウェアと思われるウイルスを発見し、関連情報についての相談を受けた。	2 件
2	特定の場所でのみ公開しているメールアドレスが大量のバウンスメールを受信した。	1 件
3	従業員が過去のメールを探している中で、ウイルスへの感染を企図した攻撃メールの添付ファイルを開封してしまった。	1 件
4	Emotet への感染を企図した攻撃メールを受信した。	6 件

項番 1 は、J-CSIP の参加組織からランサムウェアと思われるファイルを発見したため、当該ランサムウェアに関する情報や攻撃手口等について相談を受けたものである。ランサムウェアによる被害は国内でも複数の企業が公表している状況の中、J-CSIP でも相談や報告等を受けている。今後も継続してランサムウェアによる攻撃は行われることが予想されるため、被害を受けないよう、攻撃手口を知り、多層的な対策を講じる必要があると言える。

項番 2 は、特定の場所でのみ公開しているメールアドレスに対し、600 通ほどのバウンスメールを受信したというもので、このバウンスメールに添付されていた元のメールがセキュリティソフトにより検疫されたため、どのような攻撃であったか把握したいと相談を受けたものである。調査の結果、情報提供元の組織になりすまして送られていたフィッシングメールが、宛先不達等の理由によりバウンスメールとなって着信したものであった。フィッシングメールは情報提供元組織のメールサーバから発信されたものではなく、不正アクセス等の形跡は確認されていない。自組織を騙る不審メールやフィッシングメールが出回っていることを把握した場合、企業のサイト等で注意喚起を行うといったことも検討する必要があるだろう。

項番 3 は、情報提供元組織の従業員が業務に必要なメールを探す過程で、約 2 年前に受信したメールの添付ファイルを開いたところ、EDR にてウイルス検知したと情報提供を受けたものである。この添付ファイルは、悪意のあるマクロが仕掛けられており、ファイルを開いてマクロを有効化することで不正接続先からファイルをダウンロードして実行する動作となっていた。しかし、添付ファイル開封時点で、不正接続先にファイル等は存在していなかったため、ウイルスに感染するといった実被害には至らなかった。一度受信し、その時点では検知等がされなかったメールであったとしても、安全であるとは限らないため、不審と思われるメールを発見した場合や不審な添付ファイルを開いてしまった場合は、情報システム部門等へ報告することが望ましい。

項番 4 は、Emotet への感染を企図した攻撃メール（以下、Emotet の攻撃メール）を発見したと複数の組織から情報提供を受けたものである。Emotet の攻撃メールは本四半期においても継続して観測されており、2022 年 4 月にはショートカットファイルを悪用した新たな攻撃手法も確認されている。現在も攻撃が継続していること、今後も Emotet へ感染させるための手口の変化等が起こると思われることから、引き続き注意が必要である。

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、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、IPA からビジネスメール詐欺の手口と対策について、日本語字幕付きと、英語字幕付きの映像コンテンツを公開しているため [3]、活用していただきたい。

本四半期は、J-CSIP の参加組織から 1 件のビジネスメール詐欺について情報提供を受けた。本章ではこの事例について説明する。

3.1　取引先担当者のメールアカウントを乗っ取って行われた攻撃

本事例は、2022 年 4 月、J-CSIP 参加組織の海外関連会社（A 社：請求側）の担当者になりすました攻撃者から、海外の取引先企業（B 社：支払側）の担当者に、偽のメールが送られたというものである。

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 社担当者のメールアカウントが攻撃者によって不正に乗っ取られて偽メールの送信が行われており、このメールに B 社担当者が返信をしてしまった。しかしながら、その後に送られてきた攻撃者からの連絡内容を不審に思い、関係者へ通報を行ったため、金銭的な被害はなかった。

3.2　攻撃手口

本事例では詐欺の過程において、次の手口が使われた。

- 正規のメールアカウントを使用し A 社と B 社のやりとりへ介入
- 正規のメールアドレスに似せた偽のメールアドレスの使用

[3] 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/

(1)正規のメールアカウントを使用しA社とB社のやりとりへ介入

本件のやりとりの流れを図 2 に示す。

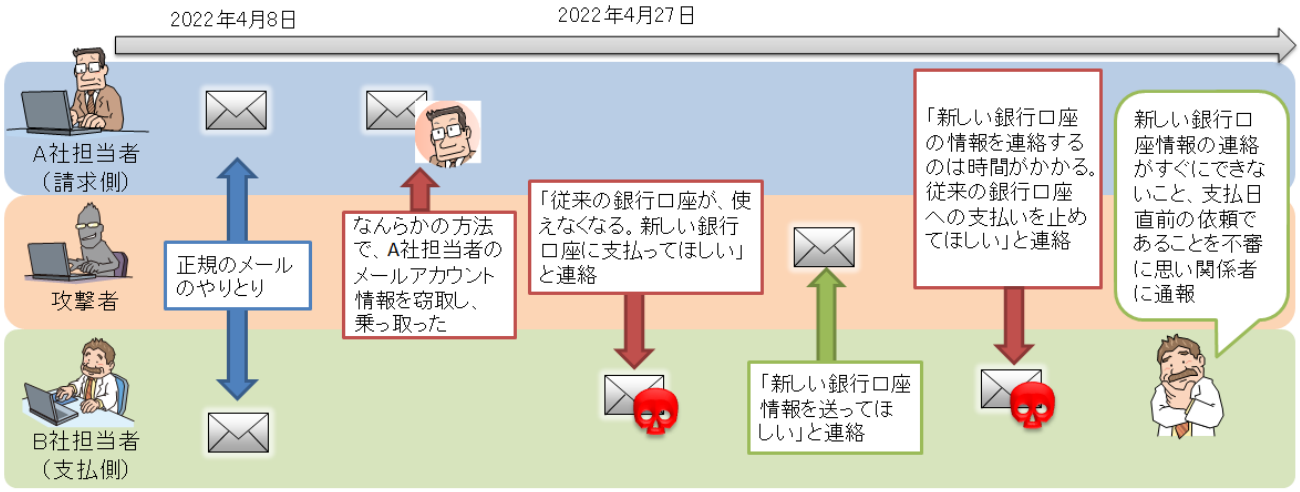

図 2 攻撃者とのやりとり

A 社とB 社との間で、取引に係るビジネスメールのやりとりをしている中で、2022 年 4 月 27 日、A 社担当者になりすました攻撃者から、現在の支払い口座が利用できなくなるという理由から、支払い先の銀行口座の変更を依頼する偽のメール（図 3）が B 社担当者へ送られた。この時、攻撃者から送られてきたメールは、何らかの方法で A 社の担当者のメールアカウントが乗っ取られた上で送付されたものであった。

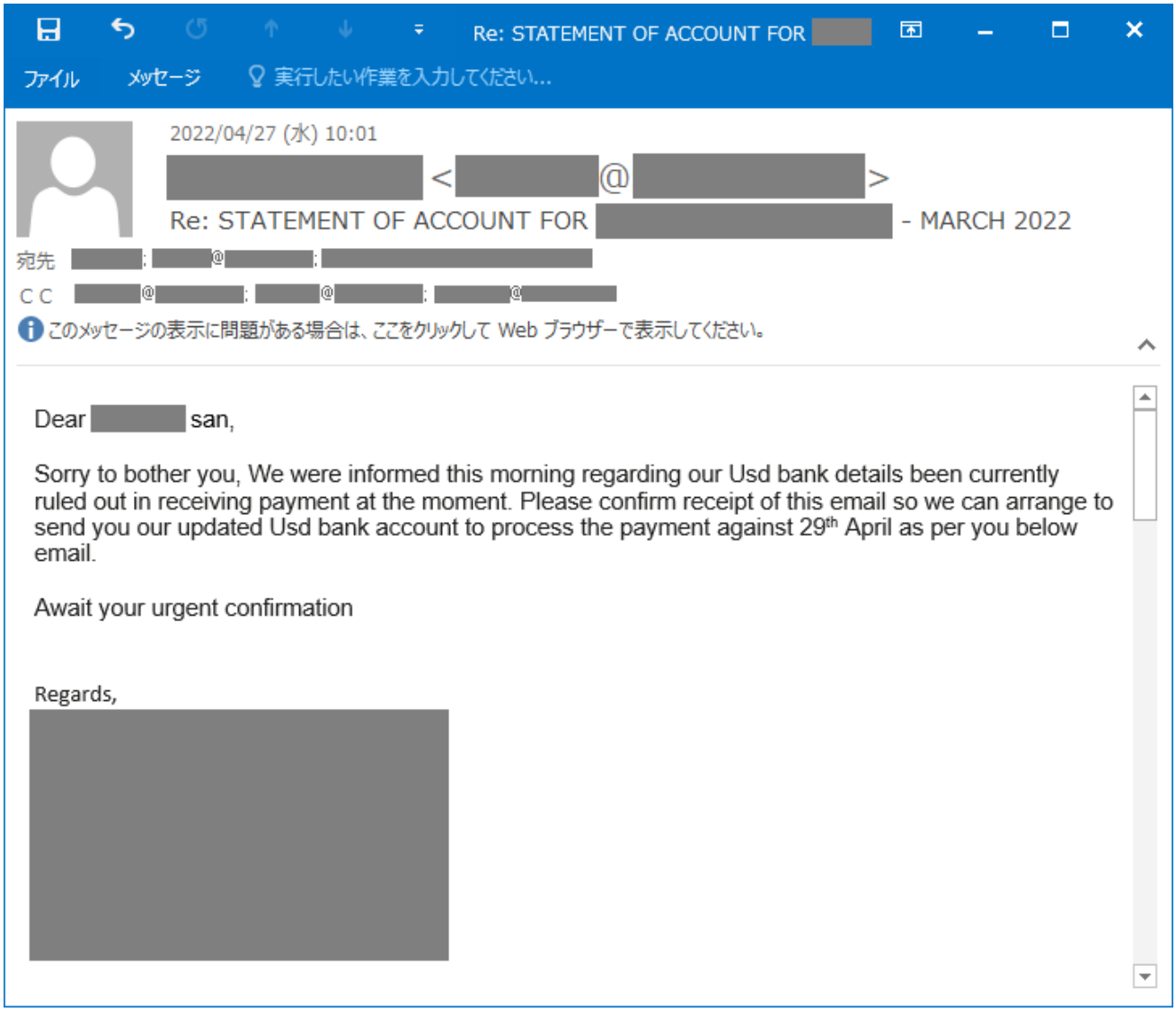

図 3 攻撃者から送られてきたメール(1 通目)

B 社担当者は、偽のメールであることに気づかず、新しい銀行口座の情報を送るように返信した。攻撃者は B 社担当者からのメールに対し、「新しい口座情報を連絡するには時間がかかるため、従来の口座への支払いを止めてほしい」といった旨の内容(図 4)を送信した。このメールを受け取った B 社担当者は、新しい銀行口座の情報がすぐに連絡されなかったことや支払日直前の急な銀行口座の変更であることを不審に思い、関係者へ通報を行ったことで、偽のメールであることが発覚した。

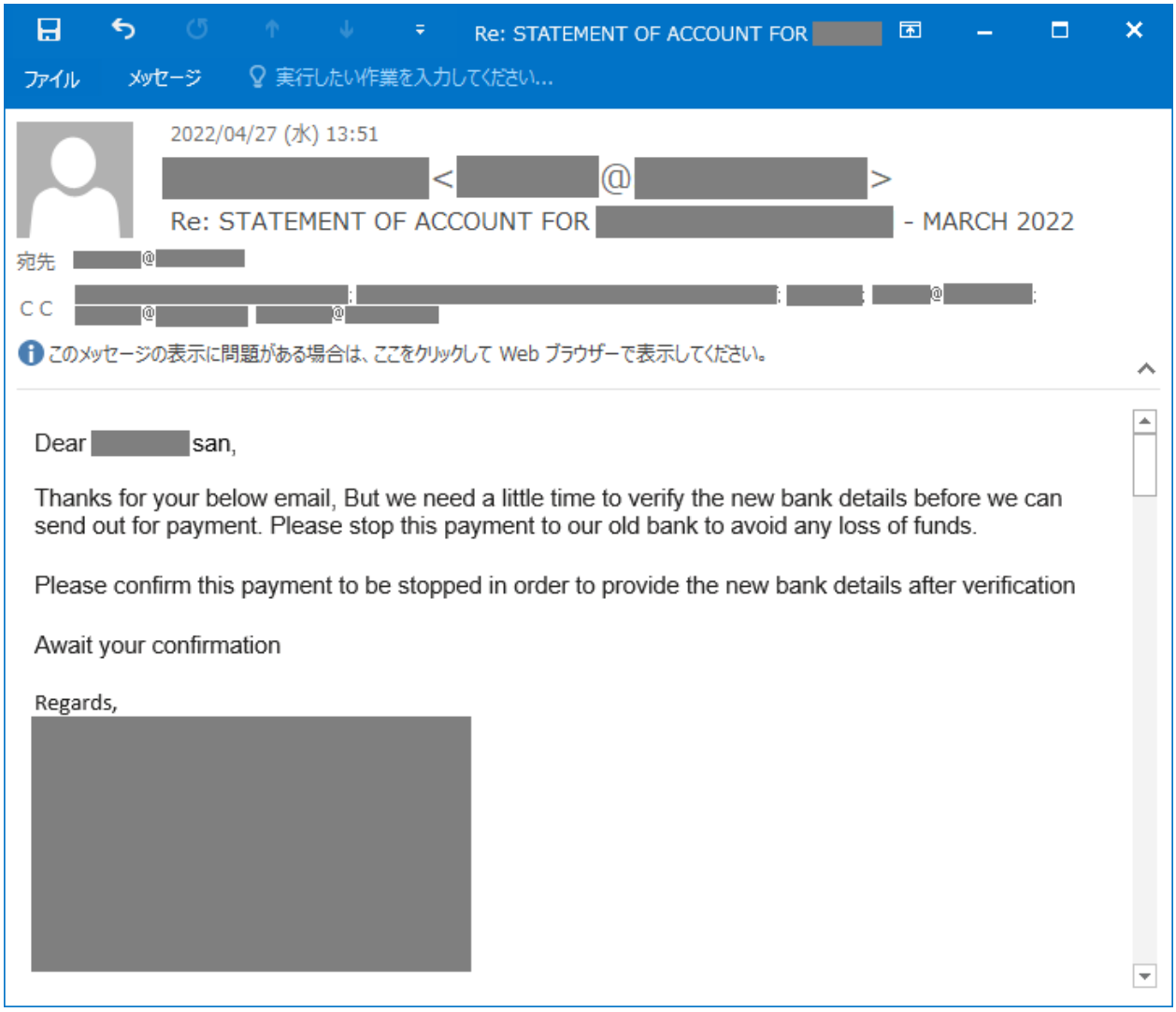

図 4 攻撃者から送られてきたメール(2 通目)

(2)正規のメールアドレスに似せた偽のメールアドレスの使用

本事例で、攻撃者は A 社担当者のメールアカウントを不正に乗っ取ってメールを送信していたため、送信元(From)のメールアドレスは正規のものであった。しかし、同報先(CC)に指定されていた、A 社関係者のメールアドレスは、正規のメールアドレスに似せた次のような偽のメールアドレス [4]が使われていた。これは、A 社関係者にメールが届き、詐欺が発覚するのを避ける目的であったと考えられる。

【本物のメールアドレス】alice @ abc.company
【偽物のメールアドレス】alice @ abc-company . com
(「.」を「-」に変更、末尾に「.com」を追加)

※実際に悪用されたものとは異なる。

[4] 偽のメールアドレスのドメインは、攻撃メールが送られる前日(2022 年 4 月 26 日)に新規に取得されていた。

4　特定の組織を狙ったフィッシングメール

本四半期、J-CSIP の参加組織（A 社）より、同社の役員を騙ったフィッシングメールが、組織内の複数のメールアカウント宛に送られてきたという情報提供があった。

当該メールを確認したところ、添付されていた PDF ファイルを起点に、正規のサービスで作成されたページを中継した後、最終的に Microsoft アカウントのログイン画面を模した偽のページに誘導されるようになっていた。この攻撃では、メールに添付された PDF ファイルや、アクセス先のページに A 社のロゴや社名等が書かれており、明確に A 社を狙った攻撃といえるものであった。

本章では、フィッシングメールやフィッシングサイトの例とともに攻撃手口の詳細について説明する。

フィッシングメールと添付ファイル

同社の役員を詐称したフィッシングメールを図 5 に示す。

このメールは、ボーナスに関する内容の詳細を添付ファイルに記載したとあり、添付の PDF ファイルを開かせようとするものであった。メールの差出人（From）表示名やメールアドレスのローカル部、メール本文内の署名は、同社の役員の名前が騙られていた。なお、メールアドレスのドメイン部は、A 社のドメインに似せたものではなく、別の正規の企業のドメインに似せたものが使用されていた。

添付の PDF ファイル（図 6）には、A 社のロゴや役員の名前、サイン [5]等が書かれており、社内ポータルサイトへアクセスするように見せかけた URL リンクが埋め込まれたボタンもあった。

IPA では、別の組織宛と思われる、本事例の添付ファイルと内容が類似する PDF ファイルを公開情報にて複数入手している。このことから、攻撃者は複数の組織に対して同様の攻撃を行っていると考えられる。

[5]IPA で入手した類似検体の PDF ファイルに記載されたサインと、本件の PDF ファイルに記載されたサインは同じ見た目であった。そのため、偽のサインと推測している。

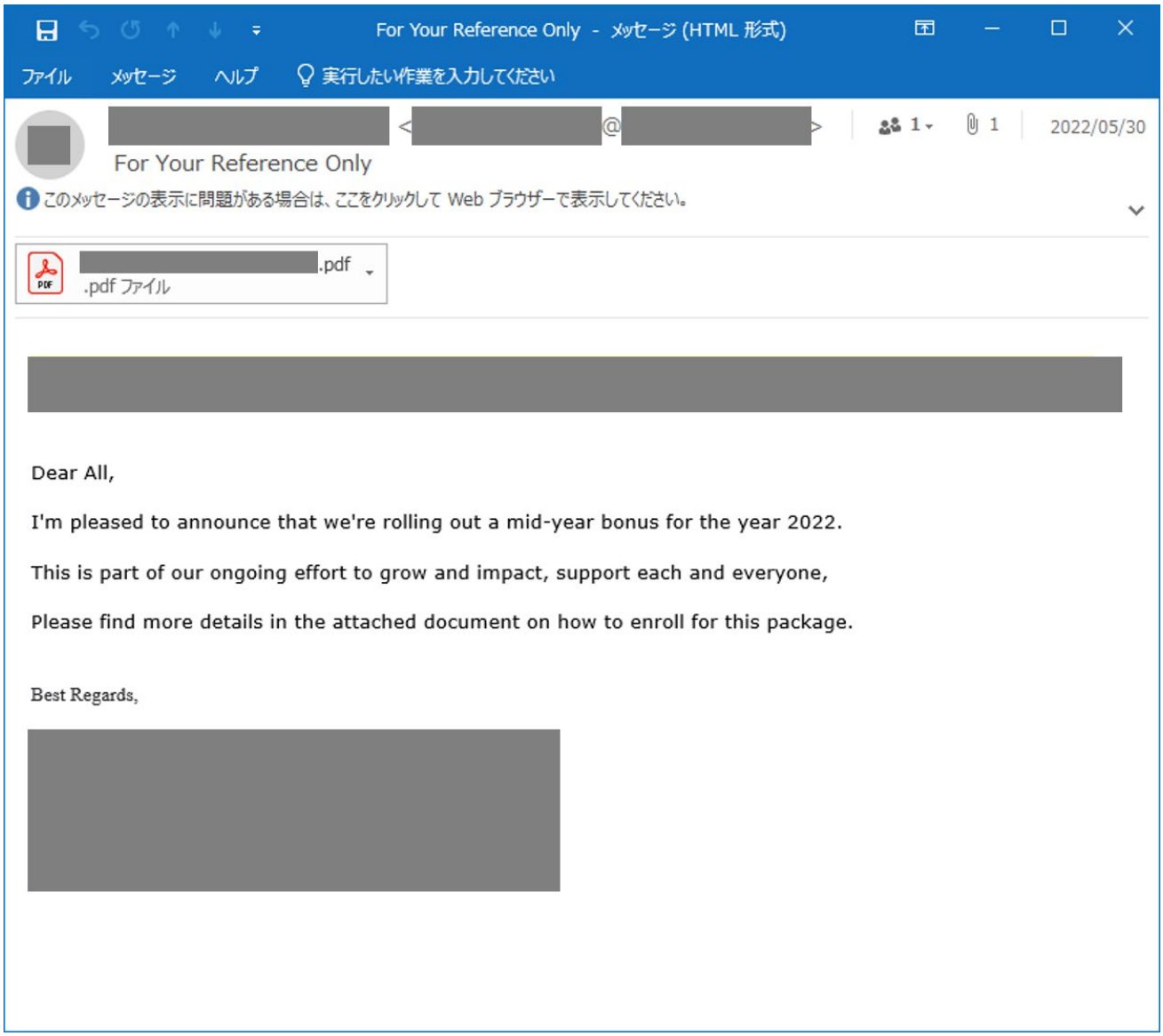

図 5 実際に送られてきたフィッシングメール

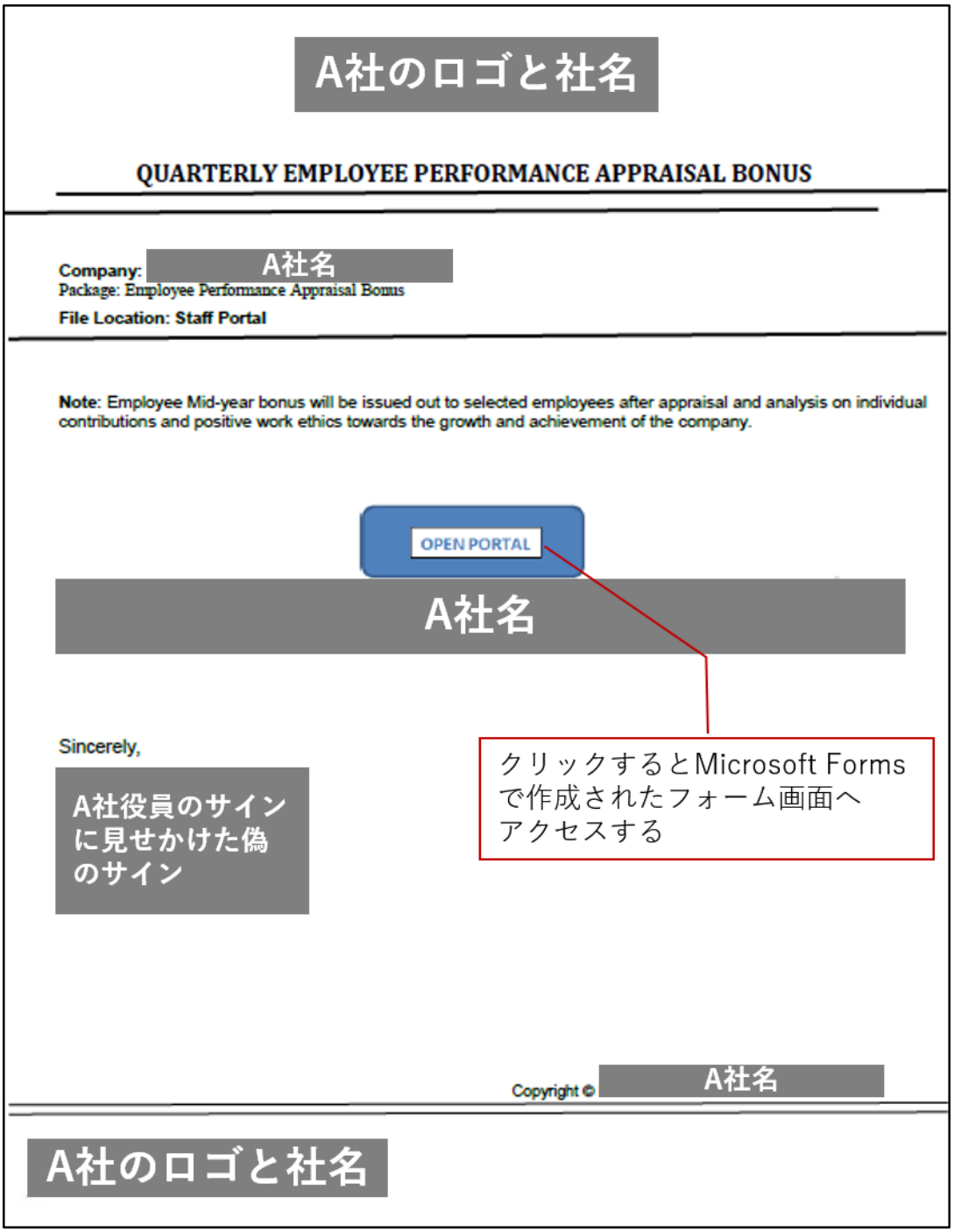

図 6 フィッシングメールに添付されていた PDF ファイル

<u>複数の正規サービスの悪用</u>

PDF ファイル内の「OPEN PORTAL」と書かれたボタンをクリックすると、ブラウザによって Microsoft Forms で作成されたフォーム画面（図 7）が開かれる。当該画面には、更に次の不正サイトへアクセスするための短縮 URL のほか、その URL にアクセスすることを促す内容が記載されており、A 社のロゴや社名、役員名なども表示されるようになっていた。

図 7 Microsoft Forms で作成された短縮 URL が記載されたウェブサイト

この短縮 URL をクリックすると、Google Sites 上に作成された Microsoft アカウントのログイン画面を模した偽の画面（図 8）に遷移する。短縮元となった URL には A 社の社名が含まれていた。また、偽のログイン画面の上部には、A 社の社名が書かれており、この画面にメールアドレスとパスワードを入力し、Next ボタンを押すと攻撃者のサーバへ入力した内容が送信される仕組みとなっていた。

攻撃者はセキュリティソフト等による検知を避ける目的で、Microsoft Forms や Google Sites といった、正規のサービスを悪用したものと考えられる。

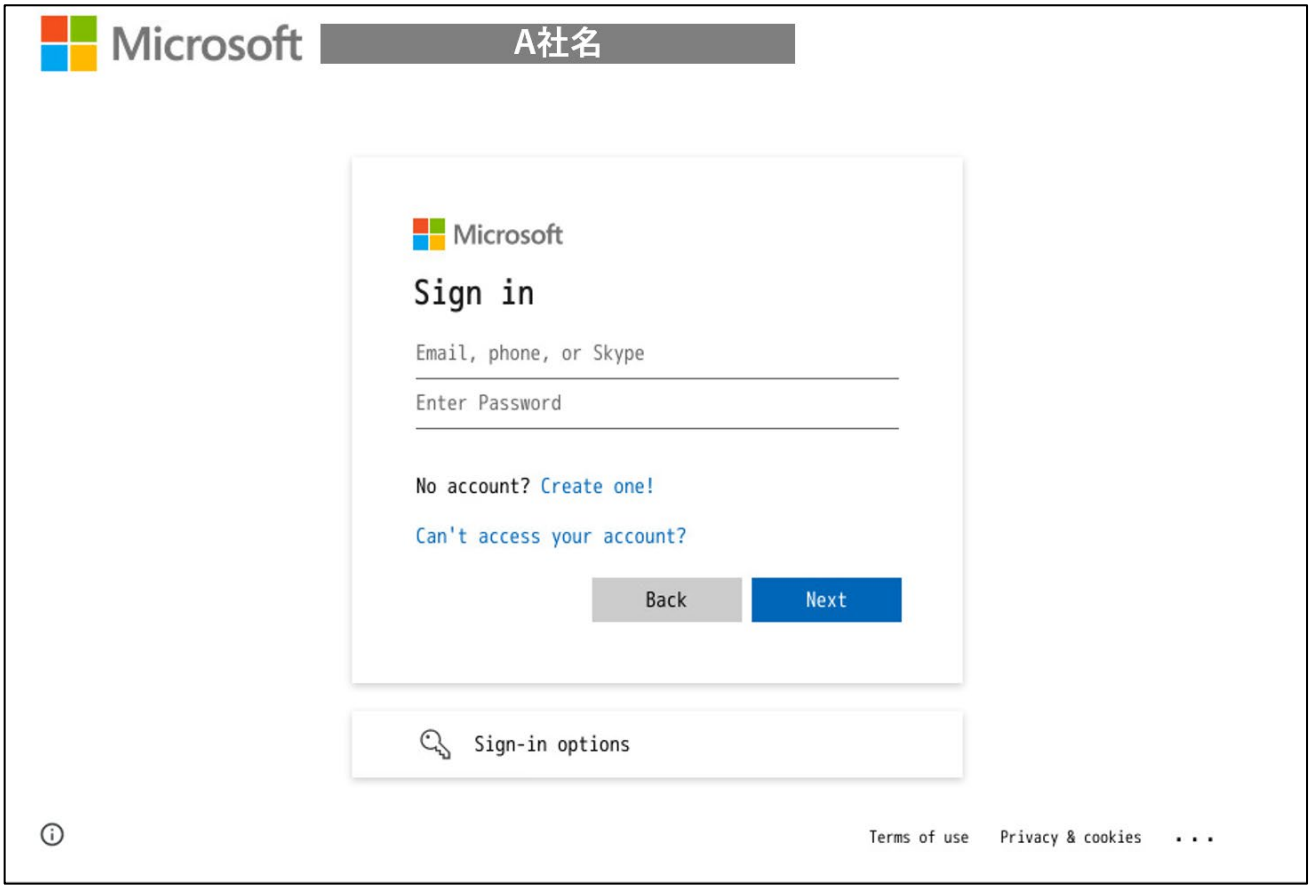

図 8 Google Sites 上に作成された偽のログイン画面

Microsoft アカウント情報を狙うフィッシングメールについては、これまでも J-CSIP の運用状況レポートで度々紹介してきている。このアカウント情報が窃取されると、組織・企業内の情報の侵害に繋がる可能性がある。フィッシング詐欺への対策は、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とともに、不審なメールの添付ファイルを開かない、URL リンクを容易にクリックしない、正規のものか判断がつかないサイトでの ID やパスワードの入力をしないといったことを徹底していただきたい。

5　情報共有活動により別組織の攻撃痕跡の発見に繋がった事例

本四半期、J-CSIP 参加組織より、不正アクセスに関する不正接続先等の情報提供があった。当該情報について、J-CSIP 参加組織へ情報共有したところ、別の参加組織 1 社においてもアクセス痕跡があったという事例である。

なお、これら 2 つの組織に行われた攻撃の痕跡が、同一の攻撃者によるものかといった関連性については観測された時期が異なるため不明である。また、別組織にて痕跡が発見された不正接続先情報は、脆弱性を悪用した攻撃で使われていた可能性があるという情報を公開情報にて確認している。

本章では J-CSIP における情報共有活動の一例としてこの事例を紹介する。

本事例の流れ

本事例の流れを、図 9 に示す。J-CSIP 参加組織（A 社）より、A 社に行われた不正アクセスに関する不正接続先情報の提供があった。この情報を J-CSIP 内へ共有したところ、別の J-CSIP 参加組織（B 社）から、不正接続先情報にあった IP アドレスからアクセスされた痕跡があったという情報提供を受けた。

この不正接続先の IP アドレスからアクセス痕跡があった場合、どのような影響があると考えられるのか、A 社から情報提供を受けた時点で不明であったため、B 社では当該 IP アドレスからのアクセス痕跡について、影響を図りかねていた。

そこで、IPA から A 社に対し、上記不明点について確認したところ、A 社から、「攻撃者の環境と推測している、不正アクセス元の IP アドレスである」という回答があり、IPA で調査した結果も含め B 社に連絡した。

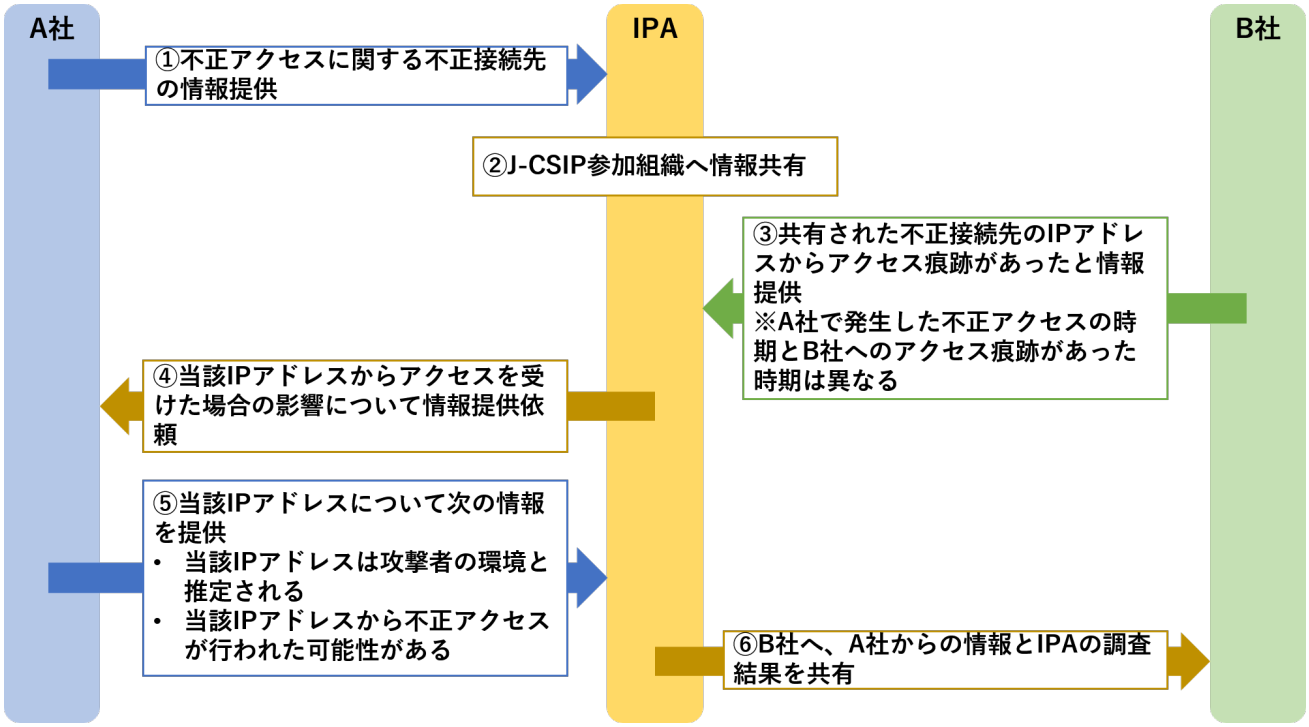

図 9 本事例の流れ

IP アドレスについて IPA にて調査したことで判明した情報

B 社でアクセス痕跡が確認された IP アドレスについて、IPA で調査したところ、B 社へアクセスした痕跡があった時期と同時期に、次の情報を公開情報より確認している。

- ウェブアプリケーションへの攻撃を行っていた IP アドレスである
- F5 ネットワークス社の BIG-IP の脆弱性を狙った攻撃に関連する IP アドレスである

また、B 社にてアクセス痕跡を発見した機器の IP アドレスを公開情報で確認したところ、BIG-IP が稼働している機器の IP アドレスであったことや、BIG-IP の脆弱性が公開された後でのアクセスであったことから、脆弱性を悪用した攻撃もしくはスキャン活動といった可能性が考えられるという状況であった。

J-CSIP では、IPA をハブとして、複数社との間で情報授受を行う場合もある。本事例のように、1 つの組織だけでは発見できないような攻撃であったとしても、情報を共有することで攻撃の痕跡を発見し、対策に繋げることができる。J-CSIP では今後も情報共有活動を通して、参加組織全体のセキュリティ向上を推進していく。

6　ショートカットファイルを悪用する攻撃の解析事例

本四半期、ショートカットファイルを悪用する攻撃手口を用いる検体を公開情報にて複数確認した。この手口は Dangerous Password という攻撃グループが使う攻撃手口に類似しており、なんらか関連性があるものと推測されるものであった。

今回確認した攻撃検体の解析結果とともに、Dangerous Password の攻撃手口を紹介し、攻撃の類似点や相違点について説明する。

参考情報として、上記内容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