サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2021 年 4 月～6 月]

2021 年 7 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、2021 年 6 月末時点の運用体制、2021 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

2021 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 262 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）。

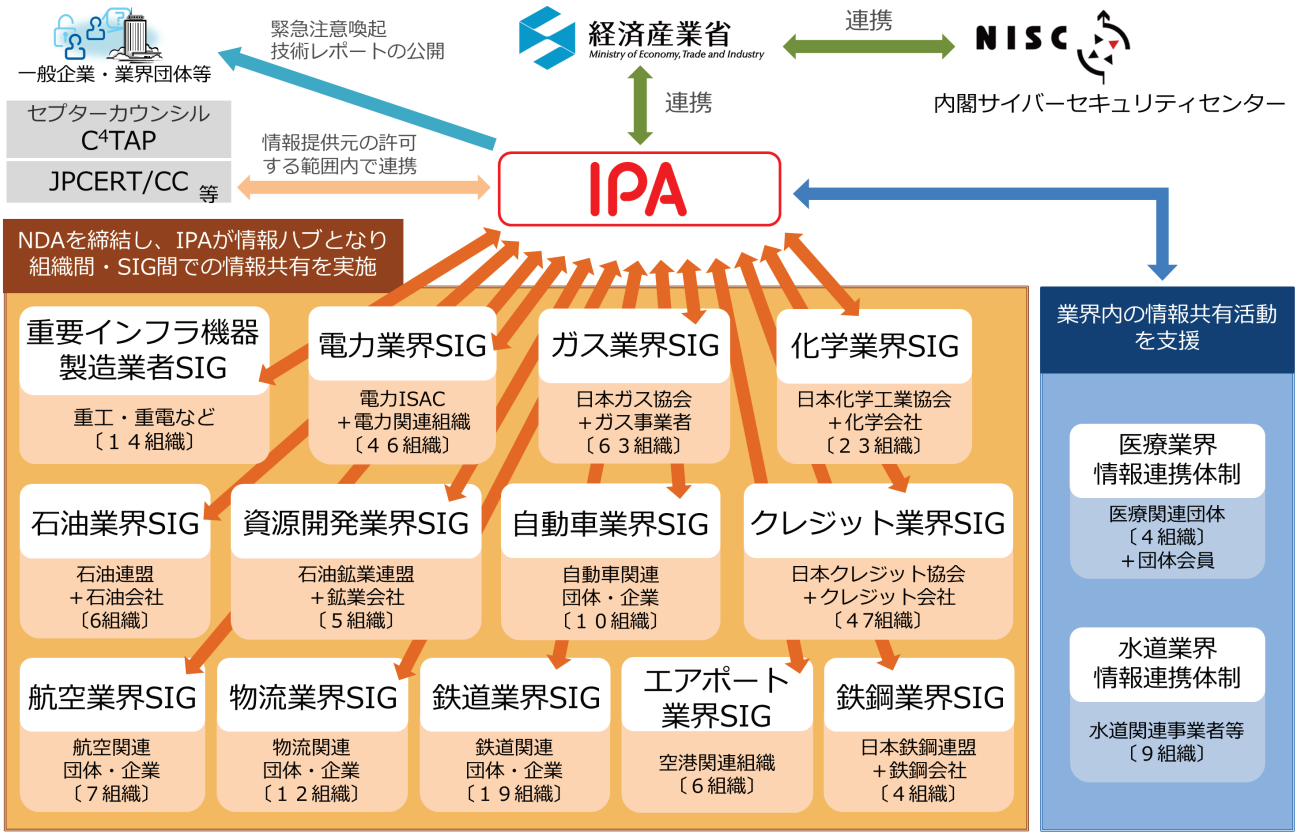

図 1 J-CSIP の体制図

[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（2021 年 4 月～6 月）

2021 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 262 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		2021 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	4,988 件	479 件	410 件	**369 件**
2	参加組織への情報共有実施件数※1	29 件	38 件	25 件	**40 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 **27 件**を含む。

本四半期は情報提供件数が **369 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 **15 件**であった。

この他、次に挙げる情報提供があり、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複数の情報提供があった。中には国内外の複数の組織に向け、連続した攻撃が行われたと思われる痕跡が確認された事例もあった。これらについては 3 章で述べる。

- 参加組織の海外グループ企業のウェブサイトに設置された問い合わせフォームに対して、実在する攻撃グループを騙った脅迫文が投稿されたという情報提供があった。当該組織では実際に脅迫文に記載されていたような攻撃の痕跡はなかった。具体的な脅迫文の内容も含め、詳細を 4 章で述べる。

- 工場内に設置したラベルプリンタのファームウェアアップデート作業時に意図しない通信を検知したという事例の情報提供があった。これについては 5 章で述べる。

- 参加組織の国内関連企業において、PowerPoint アドインファイル（拡張子 .ppam）が添付された不審なメールが着信したとの情報提供があった。IPA で確認したところ、最終的にウイルス感染を企図した攻撃メールであることが分かった。これについては 6 章で述べる。

- 本四半期に限らず、IPA では攻撃に関係しそうなメールやウイルス等の検体を公開情報から情報収集している。本四半期では攻撃に関係する可能性のある不審なファイルを複数入手した。これらについて 7 章で述べる。

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	フィッシングメールと思われるメールの本文中の URL リンクをクリックし、アクセス先でメールアドレスとパスワードを入力してしまった。	1 件
2	特定のキーワードをウェブ検索した際に、不審なスクリプトファイルがダウンロードされ、不正な通信が発生した。	2 件
3	海外のグループ企業にて、Microsoft Exchange Server の脆弱性を悪用した攻撃を受けた。	1 件
4	古い脆弱性の名称で検知される不審メールを受信した。	1 件
5	脅威インテリジェンスサービスから自社への攻撃のインジケータ情報を受領し、対応を行った。	1 件
6	ばらまき型メールを受信した。	3 件
7	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。	7 件

項番 1 は、従業員 2 名がフィッシングメールと思われるメールを開き、本文中の URL リンクをクリックし、アクセス先のウェブサイトでメールアドレスとパスワードを入力してしまったため、当該アクセス先の調査をしてほしいという相談を受けたものである。IPA で調査をしたところ、URL リンク先は Microsoft を騙る偽のサイト（フィッシングサイト）であった。当該サイトからはウイルス感染に繋がる動作はなかったが、恐らくは入力してしまったメールアドレスとパスワードは詐取されたと考えられる。このような場合は、早急にメールアカウントのパスワードを変更するとともに、組織内で同様の事象が他に発生していないか確認し、不審なメールの URL リンクを容易にクリックしないこと、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ことを周知徹底していただきたい。フィッシング対策についてはフィッシング対策協議会のページも参考となる [3]。

項番 2 は、情報提供元のある従業員による、組織外へのウェブアクセスが遮断処理されたことが発端である。調査を行ったところ、数分の間隔を空けて複数回、同一の従業員の PC から不審な通信先へのアクセスが行われた痕跡を発見した。また、その直前、当該従業員が特定のキーワードでウェブ検索を実行した際、不正通信の原因と思われる不審なスクリプトファイルのダウンロードが行われていたとのことであった。ブラウザの不正な拡張機能や先読み機能が関わっていると推測したが、原因の特定には至っていない。当該情報について情報共有を行ったところ、類似の事例について 1 社から情報提供を受けた。同様に原因については不明であるとのことで、今後も監視を継続するとのことであった。

項番 3 は、J-CSIP の参加組織の海外グループ企業にて、Microsoft Exchange Server の脆弱性を悪用した攻撃を受け、サーバ内に不正なファイル（ウェブシェル等）が複数設置されたという情報提供を受けたものである。IPA で調査したところ、類似の不正ファイルが同脆弱性を悪用した攻撃で使われていたことを確認した。提供された情報や公開情報をもとに、不正ファイルのハッシュ値や不正接続先といった情報を J-CSIP 内で共有した。

[3] フィッシング対策協議会
https://www.antiphishing.jp/

項番 4 は、J-CSIP 参加組織の国内関連企業に着信したメールが、一部のセキュリティ機能にてウイルスとして検知されたという情報提供を受けたものである。このときの検知名に、CVE-2017-0199 という古い脆弱性の名称が含まれており、IPA で調査を行った。メールに添付されていた Word 文書ファイル（.docx）自体には脆弱性を悪用する細工は仕掛けられておらず、開くと不正接続先へ通信を行う。この不正接続先からは、過去に別の Word 文書ファイルがダウンロードされる状態であったことが分かっており、そのファイルに何らかの脆弱性を悪用する細工が仕掛けられていたものと推測している。このように、古い脆弱性の名称で検知された場合でも、実際の挙動は異なる（検知名が誤っている）ことがあり、検知名のみから脅威の度合いを判断しようとする場合は注意が必要である。

項番 5 は、J-CSIP の参加組織が、脅威インテリジェンスサービスからの情報として、当該組織に対して行われたとされる、ある攻撃グループからの標的型攻撃のインジケータ情報を受領したというものである。その情報からは深刻度や妥当性の判断が難しく、具体的な活用について相談があった。詳細は不明であったが、当該インジケータ情報と、その攻撃グループとの関連性については特段認められず、当該情報を起点として実施すべき対応は行ったものの、最後まで情報の妥当性の判断ができなかったようであった。脅威インテリジェンスサービスは、その情報を精査する体制を含め、活用が難しい場合がある。導入においては、慎重に検討する必要があると思われる。

項番 6 は、国内にばらまかれたウイルスメールを受信したという情報提供である。2020 年度は Emotet への感染を企図した攻撃メールが多数観測されていたところ、本四半期は Emotet とは別のウイルスへの感染を企図した攻撃メールを観測している。システム的な対策のほか、各個人においても不審なメールへの注意力を維持し、不審なメールの添付ファイルは開かないといった基本的な対策を徹底することが重要である。

項番 7 は、組織内の PC から外部の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あり、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。そのため、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 [4]等に騙されないようにするといった従業員への教育を継続的に実施すべきであろう。

[4] 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、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へ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。

本四半期は、J-CSIP の参加組織から 8 件のビジネスメール詐欺について情報提供を受けた。これらのうち、2 件はタイプ 1（取引先へのなりすまし）の攻撃で、残りの 6 件については、タイプ 2（経営者等へのなりすまし）であった。さらに、J-CSIP の参加組織外からも 5 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タイプ 1 とタイプ 2 の 2 つの事例について詳しく説明する。また、本四半期でも継続して確認された、2 つの CEO 詐欺（複数組織へ行われた CEO を詐称する一連の攻撃と、「日本語化」された CEO 詐欺の攻撃）の続報についてもまとめて説明する。

3.1 事例 1 海外取引先企業を狙った攻撃

本事例は、2021 年 4 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、偽のメールが送られたものである。

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、B 社の担当者が攻撃者の用意した偽の口座へ送金を行ってしまったため、金銭的な被害が発生した。

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 社のやりとりへ介入
（2）正規のメールアドレスに似せた偽の詐称用ドメインの悪用
（3）メールの転送設定によるメールの盗聴

（1）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。

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、2021 年 3 月 16 日に攻撃者から B 社の担当者へ偽のメールが送られた。その後、B 社と攻撃者は複数回メールのやりとりを継続したと思われるが、詳細は情報提供外のため不明である。そのやりとりの中で、B 社担当者は攻撃者が用意した偽の口座へ支払いをしてしまったため、金銭的被害が発生した。

その後、2021 年 4 月 9 日に A 社から B 社へ、請求中の支払いが無いため連絡をしたところ、B 社からは支払済みであると回答を受けたことで事案が発覚した。B 社では偽の口座への振り込みの取り消し対応を行っており、当該口座は凍結されたとのことだが、送金した資金が回収できたかは不明である。

なお、本件で攻撃者が用意した偽の口座は、同時期に本件とは別のビジネスメール詐欺と思われる詐欺行為でも悪用されていたことが判明している。攻撃者が、被害者を騙して振り込ませる口座を複数の犯罪に使い回しているであろうことは推測していたが、実際に複数の会社に対するビジネスメール詐欺が関係していたということが把握できた。

銀行や警察等と連携することで、攻撃者の口座を凍結し、別の企業等に行われているビジネスメール詐欺の被害を未然に防げる可能性があるため、攻撃者の口座が判明した際は、速やかな外部機関への連携等も検討いただきたい。

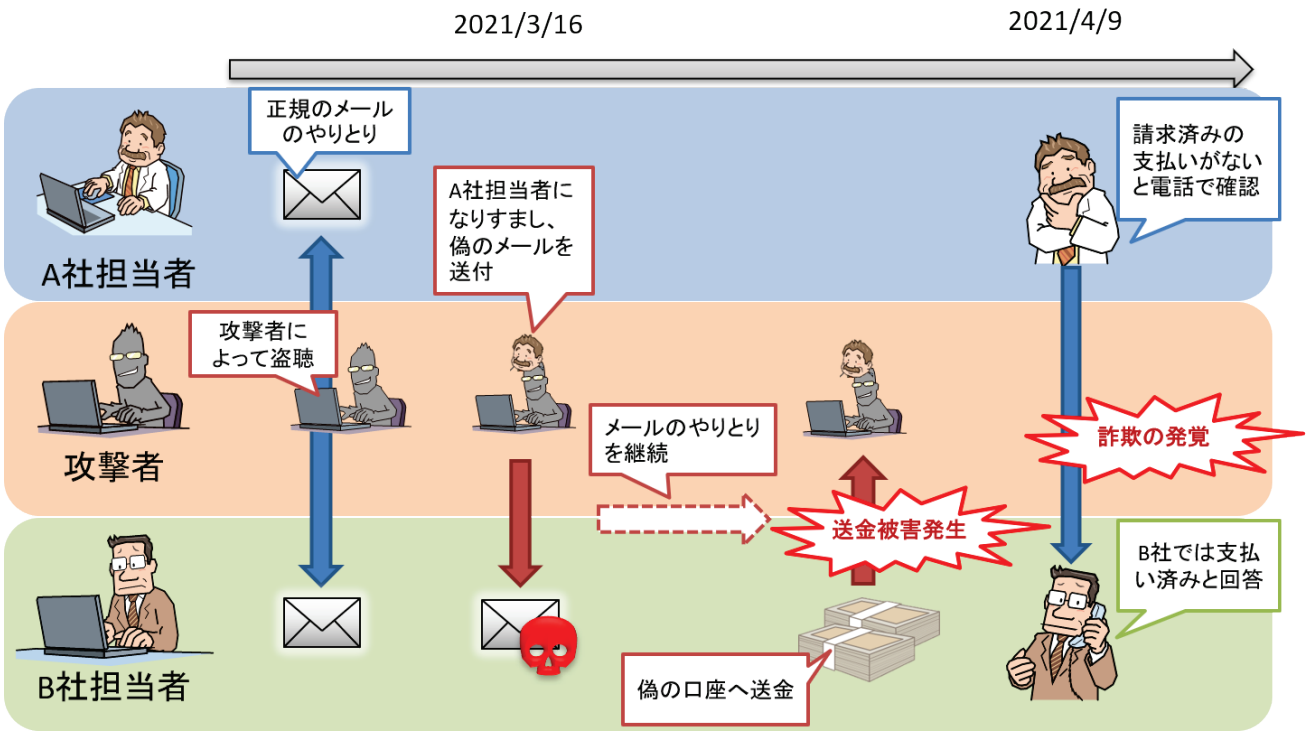

図 2 事例 1:攻撃者とのやりとり

(2)正規のメールアドレスに似せた偽の詐称用ドメインの悪用

攻撃者から B 社担当者へ送られたなりすましメールでは、A 社の正規のドメインに似通った「詐称用ドメイン」が、最初の攻撃メールが送られた当日(2021 年 3 月 16 日)に新規に取得され、悪用されていた。

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 @ abccompany-a . com
【偽物のメールアドレス】 alice @ abcccompany-a . com
(「c」を一文字追加)

※実際に悪用されたものとは異なる。

(3)メールの転送設定によるメールの盗聴

本件の事例では、攻撃者は何らかの方法で B 社の Microsoft 365 のメールアカウントへ不正アクセスし、正規の A 社の担当者から送られたメールを攻撃者の元へ転送するように設定していた。

当該設定を行うことで、攻撃者は A 社と B 社のやりとりを、B 社のメールサービスに定期的にログオンすることなく、盗み見ることが可能となっていたと思われる。

このようなメールの転送設定を悪用したメールの窃取の手口は、公開情報等、本件以外のビジネスメール詐欺でも悪用されていることを確認している。メールが窃取されていることが疑われる状況となった場合、不審なログオンの確認だけでなく、関係者のメールアカウントに身に覚えのない転送設定が施されていないか、必ず確認していただきたい。

3.2 事例 2 国内企業を狙った複数の攻撃

本事例は、2021 年 5 月、J-CSIP の参加組織の 6 名の担当者に対し、同社の役員になりすました攻撃者から、同一内容の偽のメールが送られたと情報提供があったものである。

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 2:経営者等へのなりすまし」に該当する。

この事例では、6 名のメールの受信者は偽のメールに気づいたため、金銭的な被害には至らなかった。

本事例で、攻撃者から送られたメールを図 3 に示す。なお、メールはいずれも同日のほぼ同じ時間帯（およそ 50 分の間）に送られていた。

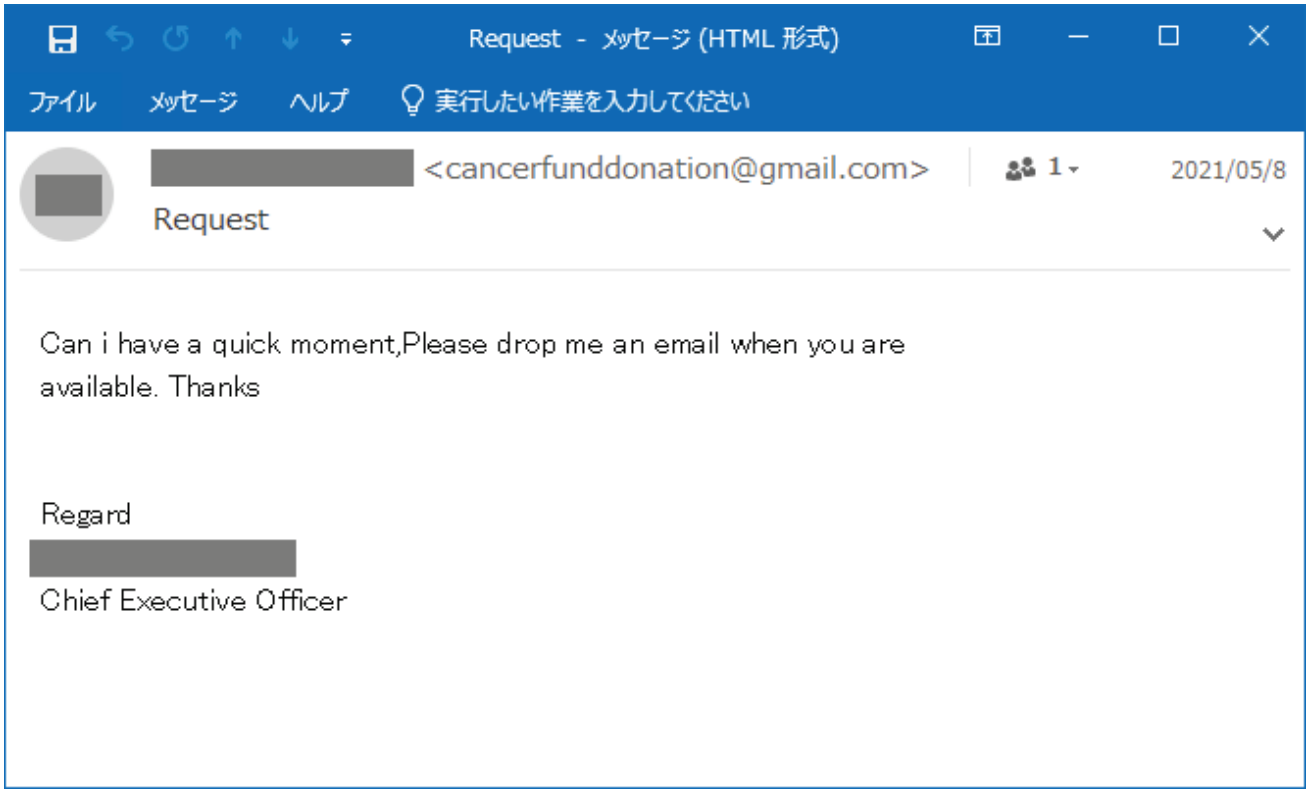

図 3 事例 2:攻撃者から送られた偽のメール

攻撃者から送られた偽のメールは、メールで連絡がほしいという簡素な内容であった。差出人（From）の表示名には A 社取締役の名前が設定されており、実際にはフリーメールアドレスから送られていた。

本件と類似したメールは 2021 年 1 月にも観測[5]しており、同一と思われる攻撃者が繰り返し攻撃を行っているものと推測している。

また、IPA では、公開情報にて本メールに類似した BEC を企図したと思われるメールを他にも確認しており、複数の企業・組織に対して同様の偽メールが送られた可能性があると推測している。簡単な内容の偽メールではあるが、注意が必要であろう。

[5] サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2021 年 1 月～3 月]（IPA）
https://www.ipa.go.jp/security/J-CSIP/

3.3 事例 3 同一攻撃者と思われる英語と日本語のメールによる攻撃

本事例は、2021 年 6 月、J-CSIP の参加組織の担当者に対し、当該組織の役員を騙る、英語と日本語のなりすましメールが送られたと情報提供があった。

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 2:経営者等へのなりすまし」に該当する。

この事例では、2 件のメールのそれぞれの受信者は偽のメールに気づいたため、金銭的な被害には至らなかった。

本事例で、攻撃者から送られたメールを図 4 と図 5 に示す。

図 4 事例 3:攻撃者から送られたメール(5 月)

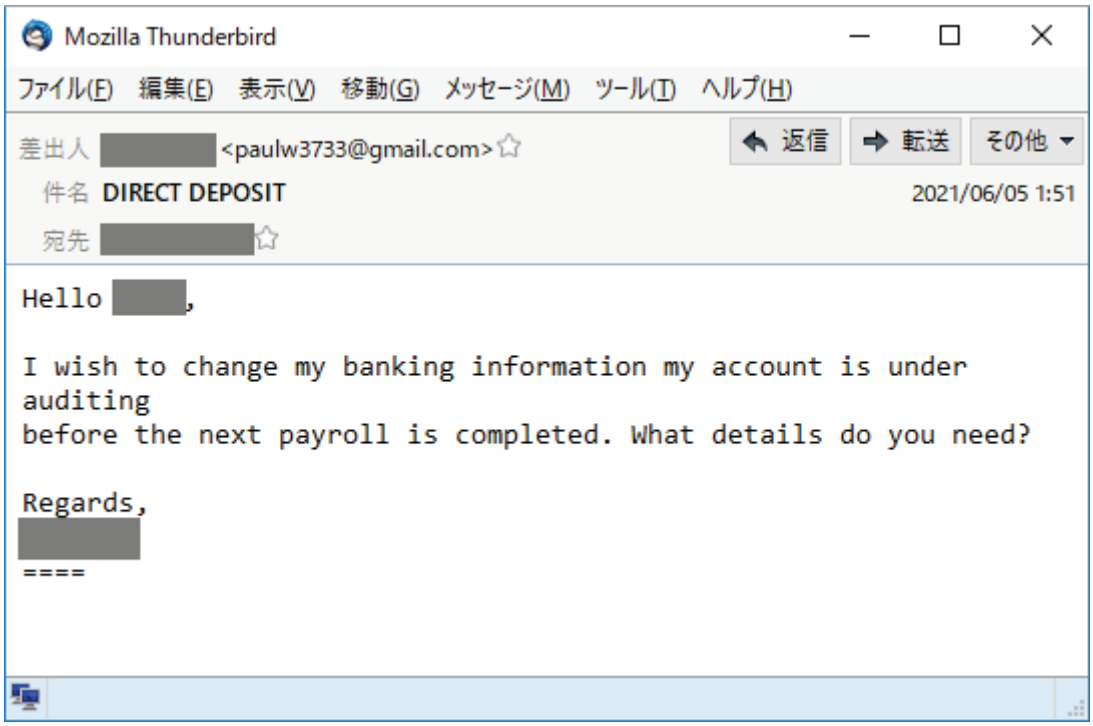

図 5 事例 3:攻撃者から送られたメール(6 月)

2 件のメールは、5 月と 6 月に当該組織の別々の担当者に対し攻撃者から送られたもので、騙られていた役員も異なっていたが、差出人のメールアドレスが同一(フリーメールアドレス)であり、本文の内容も同等であったことから、同一の攻撃者によるものと考えている。

IPA では、公開情報にて英語のメール(図 5)に類似したメールを他にも確認しており、複数の企業・組織に対して同様の BEC を企図した攻撃があったものと推測している。

日本語のメールにはまだ不自然な点が多いが、日本の企業・組織を狙う意図は明白であり、今後とも注意が必要である。

3.4 2 つの CEO 詐欺の続報

本四半期においても、次の 2 つの CEO 詐欺について継続して情報提供があった。さらに IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、複数の類似するメール検体を入手した。

本章ではこれら 2 つの CEO 詐欺について説明する。

- 複数組織へ行われた CEO を詐称する一連の攻撃
- 「日本語化」された CEO 詐欺の攻撃

本四半期を含め、四半期毎の運用状況レポートにて報告してきた 2 つの CEO 詐欺について、これまで入手したメールの件数を次に示す。

表 3 これまで入手したメール件数一覧

計測期間	複数組織へ行われた CEO を詐称する一連の攻撃（件）	「日本語化」された CEO 詐欺の攻撃（件）
2019 年 10 月～12 月	62	0
2020 年 1 月～3 月	46	7
2020 年 4 月～6 月	50	25
2020 年 7 月～9 月	7	8
2020 年 10 月～12 月	8	13
2021 年 1 月～3 月	17	6
2021 年 4 月～6 月	15	7

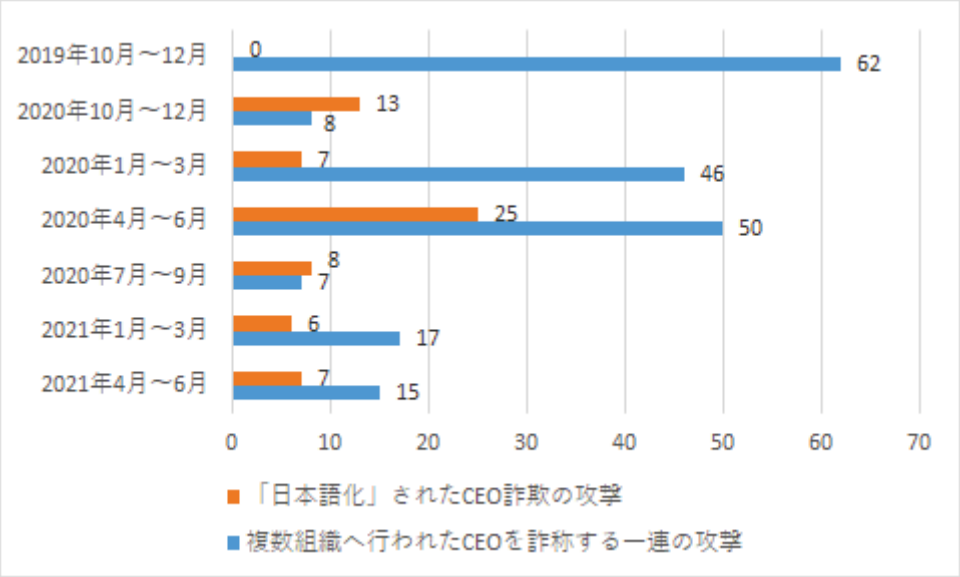

図 6 これまで入手したメール件数の推移

これら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、多く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、今後も継続して国内外の組織に対して攻撃が行われる可能性がある。

複数組織へ行われた CEO を詐称する一連の攻撃

本攻撃は、2019 年 7 月以降継続して観測しており、国内外の複数の組織を対象として行われている痕跡を確認している。メールの件名や内容は時期ごとに変化が見られるが、メールのヘッダ情報に類似する点があり、一連の攻撃は同一の攻撃者によるものと推測している。また、本攻撃メールについては米国 Agari Data 社が公開しているレポート[6]と同様の内容であることを確認している。

攻撃メールには、次のような特徴がある。

表 4 攻撃メールの特徴

項目	特徴
メールの宛先	国内外の複数の組織（経営者、役員、職員等と思われるメールアドレス）へ送られている。
メールで騙られた人物	実在する CEO や CFO、弁護士等を詐称。CEO を詐称する場合、ほぼ、攻撃先の各企業の実際の CEO を名乗っている。また、少数だが、取引先の CEO を名乗る事例も確認している。
攻撃者のメールアドレス	命名に規則性があり、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ているものが多い。また、天体以外の単語のケースも確認している。
使用言語	ほぼ英語のメールである。なお、日本語、フランス語、スペイン語も確認している。
メール件名	法律関連を装う件名を多く確認している。2020 年 5 月以降は「Project」という文言が件名として観測されるようになった。
メール本文	2019 年 7 月 23 日から 2020 年 12 月 16 日までは、数行程度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った。 2020 年 3 月以降の 1 年間は、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にすることが多くなった。なお、観測時期によって規制の緩和やワクチンといった単語も使うメールも観測している。 2021 年 4 月以降は、新型コロナウイルス感染症関連の文言は使われなくなった。

[6] Cosmic Lynx: A Russian Threat Hits the BEC Scene（Agari）
https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/

「日本語化」された CEO 詐欺の攻撃

本攻撃は、2019 年 11 月以降継続して観測しており、国内外の複数の組織を対象として行われている痕跡を確認している。メールの件名や内容は一部の変化が見られるがほぼ同じ内容のメールであり、メールのヘッダ情報や、「SendGrid」や「SMTP2GO」というメールサービスを使用する場合があるなど類似する点がある。そのため一連の攻撃は同一の攻撃者によるものと推測している。また、本攻撃については 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）[7]」の 2.1 章事例 1 にて説明している。

攻撃メールには、次のような特徴がある。

表 5 攻撃メールの特徴

項目	特徴
メールの宛先	国内外の複数の組織（CEO 等と思われるメールアドレス）へ送られている。
メールで騙られた人物	実在する CEO を騙っている。
攻撃者のメールアドレス	命名に規則性があり、差出人（From）や返信先（Reply-To）に「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を使う。
使用言語	英語と日本語を多く確認している。件名や本文に一部の違いはあるが、両言語でほぼ同様の内容が書かれたメールが確認されている。また、それ以外の言語でのメールも確認している。
メール件名	「Finance M&A」や「金融合併と買収につきまして」といった件名が多く観測されている。また、「複数組織へ行われた CEO を詐称する一連の攻撃」と同じ件名のものも確認している。（同攻撃との関連は不明）
メール本文	数行程度の簡単な文面のメールが送られてくる。内容は「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」といったものが多い。 1 通目のメールに返信をすると、「外部の弁護士と連絡を取り支払いをしてほしい」といった内容のメールや、実在する弁護士を騙って連絡先を聞き出そうとするメールが着信することを確認している。

[7]【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

4　問い合わせフォームへの脅迫文の投稿

本四半期、ウェブサイトの問い合わせフォームに、身代金を要求する脅迫文の投稿があったと情報提供があった。

本章では、実際に投稿された脅迫文の内容とともに事例を説明する。

発見の経緯

2021 年 6 月 10 日、J-CSIP の参加組織の海外グループ企業の英語の問い合わせフォームに、実在するサイバー攻撃グループを名乗る者から身代金を要求する脅迫文の投稿があった。当該脅迫文にはサーバをハッキングして機密情報を入手したという内容とともに、暗号資産（仮想通貨）を支払わなければ情報を公開すると書かれていた。このため、当該企業にて調査を行ったが、攻撃を受けた痕跡は見つからなかった。

情報提供を受け、IPA で当該攻撃グループのリークサイトを確認したところ、その時点では当該企業に関する情報は掲載されていなかった。問い合わせフォームから連絡をしてくるという不自然な方法であること、本件と類似した事案が他でも発生していると思われる情報（当該情報の攻撃グループ名と、本件の攻撃グループ名は異なる）[8]を確認したことなどから、本件は多発しているランサムウェア攻撃に便乗した詐欺の可能性が高いと考えている。

投稿された脅迫文

参考までに、問い合わせフォームに投稿された脅迫文は次の内容であった。

> Hi, this is【攻撃グループ名】hack group.
>
> It took us a lot of time to hack your servers and access all your accounting reporting. Also, we got access to many important documents and other data that can greatly affect your reputation if we publish them. It was difficult, but luck was helped by us – one of your employees is extremely unqualified in network security issues. You could hear about us from the press – recently we held a successful attacks on the【実在する企業名】.
>
> For non-disclosure of your confidential information, we require not so much – 100 bitcoins. Think about it, these documents may be interested not only by ordinary people, but also the tax service, investors and other organizations, if they are in open access ... We are not going to wait long – you have several days.
>
> Our bitcoin wallet – bc1qcwrl3yaj8pqevj5hw【ビットコインアドレス後半部分】
> Contact us:【攻撃グループ名】@0815.ru

[8] Fake DarkSide Campaign Targets Energy and Food Sectors（TrendMicro）
https://www.trendmicro.com/en_us/research/21/f/fake-darkside-campaign-targets-energy-and-food-sectors.html

5　業務用ラベルプリンタのファームウェアアップデート時の意図しない通信の検知

本四半期、J-CSIP の参加組織より工場内に設置した機器のファームウェアアップデート作業時に、意図しない通信が発生したことを検知したという情報提供があった。本件は悪意のある通信（攻撃）ではなかったが、他組織でも使用している可能性がある機器であったため、情報共有を行った。

本章では、当該事例について説明する。

経緯と対応

1. 工場内の IT 系（OA 系）ネットワークに接続・設置した業務用ラベルプリンタについて、当該機器のメーカーのメンテナンス担当者が、ファームウェアのアップデート作業を行った。
2. 当該機器のアップデート作業の際は LAN ケーブルを抜線する手順となっていたが、担当者は本手順を行っていなかった。
3. LAN ケーブルの抜線がなかったこと、および機器の仕様（※）により、元々当該機器へ割り当てられていた固定 IP アドレスではなく、別の IP アドレスからパケットが送信され、ネットワーク上の不正機器の接続検知の仕組みにより検知された。
   ※　ファームウェアアップデートの際、設定済みの IP アドレスとは異なる IP アドレスをサブネットワーク上で自動的に割り当て、パケットを送出するという仕様であった。

本件では当該サブネットワーク上の IP アドレスの重複は発生しなかったため、通信障害等の影響はなかったが、障害に発展する可能性はあった。また、不正な通信の発生というインシデントとして、調査対応の必要が生じた。

当該企業では、本件を契機として本事象と直接関係しない点も含め次の対応を行ったとのことである。

- 通常使用していない USB ポートや LAN ポートに物理ロックを施す。
- ネットワークに接続している機器のプログラム／ファームウェアの更新作業時には、社員の立ち会いを行い、ネットワークや機器に無断で持ち込み機器を接続することのないよう注意する。
- プログラム／ファームウェアの更新作業時の LAN ケーブル抜線を確実に実施する。

補足

本事例のように、PC やサーバといった一般的に利用されている IT 機器と異なる特殊な機器は、想定外の仕様となっていることがある。また、本件は工場内とはいえ IT 系（OA 系）のネットワークで発生した事象であり、想定外の挙動であってもセキュリティ装置で検知できたとのことではあるが、工場のような拠点での資産管理、ネットワーク管理やセキュリティ対策（システム面、運用面の両方）は、本社等と比較して不十分という課題を抱えている企業は少なくないようである。

工場等については、使用している機器やネットワーク構成が多様であるため、個別の機器に依存するような問題の情報共有が即座に役立つケースは少ないと思われるが、同様の事象が発生した場合に検知・対応可能か、あるいは他組織での対策実施状況といった点で、各組織での検討材料にできる可能性がある。今後とも、特殊な機器・特殊な環境でのインシデント情報についても、情報共有が進められるようにしていく。

6 PowerPoint アドインファイルを悪用した攻撃

本四半期、国内の組織に対して、PowerPoint アドイン（拡張子 .ppam）形式[9]のファイルを悪用した不審メール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を含め説明する。

不審メールの内容

2021 年 6 月 29 日、J-CSIP の参加組織から、国内関連企業に着信したメールで PowerPoint アドインファイルが添付されており、セキュリティ製品にてウイルスと検知したと情報提供を受けた（図 7）。

本件の攻撃メールの本文には、担当者変更を装い、添付ファイルの内容で見積もりを依頼する文面が書かれていた。なお、公開情報を調査したところ、本件のメールと類似した内容のメールがあることを確認しており、ある程度の範囲にばらまかれているものと考えられる。

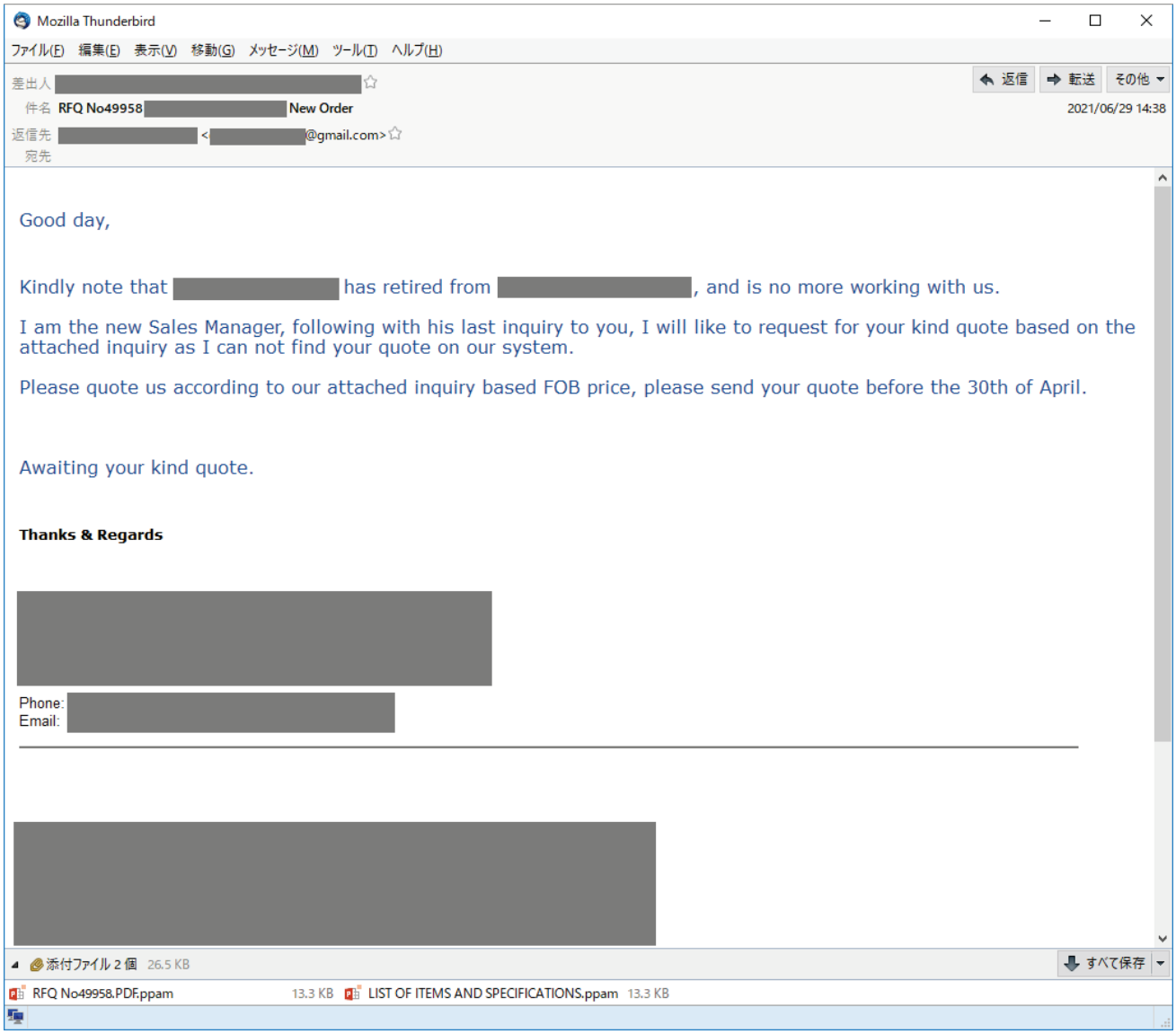

図 7 PowerPoint アドインファイルが添付された不審メール

[9] Microsoft PowerPoint でアドインを追加するために利用されるファイル形式。

PowerPoint アドイン（.ppam）ファイルの悪用

不審メールには2つのファイルが添付されていたが、ファイルのハッシュ値は同一であり、ファイル名が異なるだけで同じファイルであった。このファイルは図 8 のように PowerPoint に関連付けされたファイルとして表示されている。

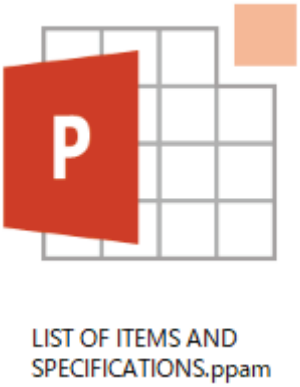

図 8 ファイルのアイコン

このファイルを開くと、悪意のある命令の実行が試みられ、図 9 の PowerPoint の警告ウインドウが表示される。このウインドウが表示された場合、「マクロを有効にする」を選択すると、最終的に別のウイルスに感染させられてしまう。なお、**「マクロを無効にする」を選択**すれば、攻撃を回避する（悪意のある命令の実行を止め、ウイルス感染を避ける）ことができる。

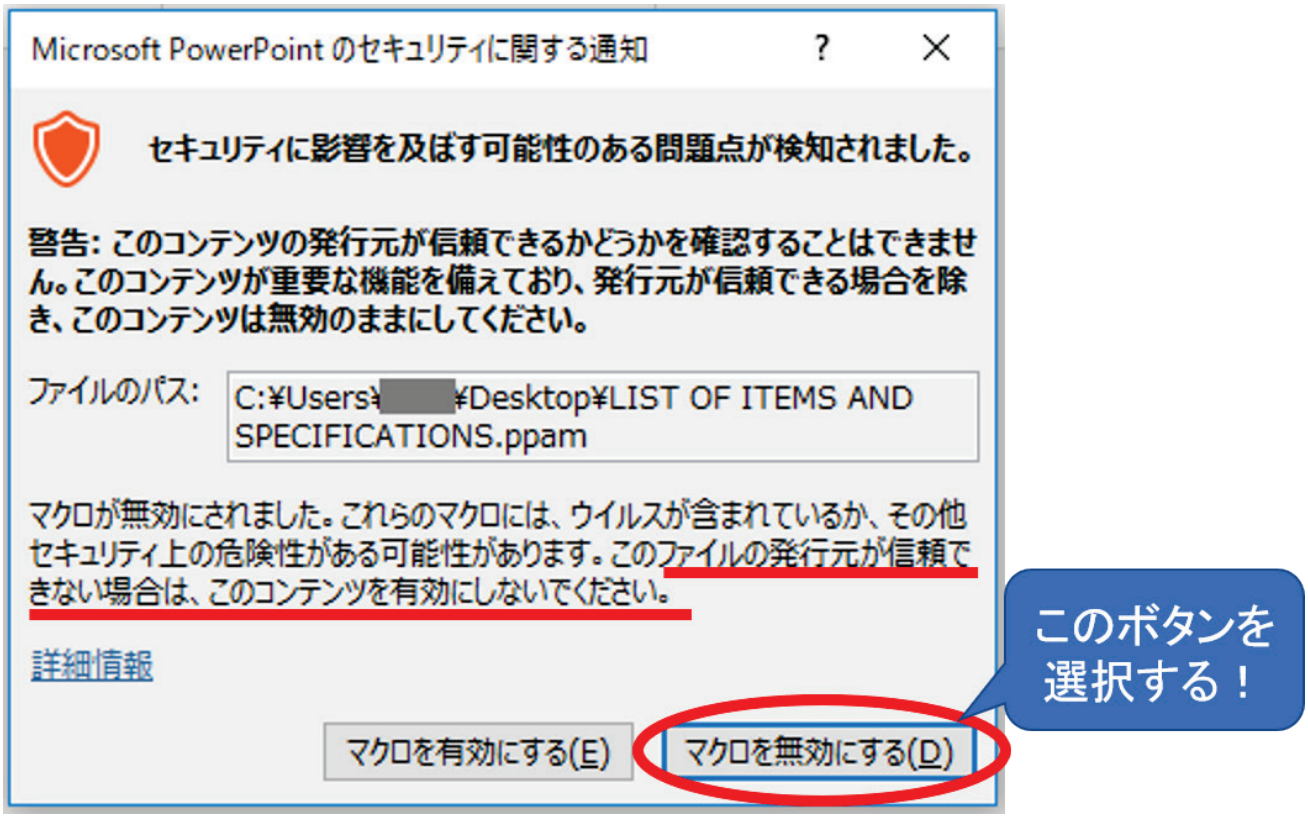

図 9 PowerPoint で悪意のある PowerPoint アドインファイルを開いた際に表示される警告ウインドウ

この PowerPoint アドインファイルを悪用する攻撃手口は、脆弱性を悪用しているわけではないため、修正プログラムの適用で攻撃を防ぐことはできない。この形式のファイルをメールで授受することは稀であろうと思われるため、対策として、拡張子「.ppam」が添付されたメールをブロックする設定を行うといった方法がありうる。また、利用者ひとりひとりが、この攻撃手口を認識し、PowerPoint アドインファイルを開いたときに表示されるウインドウをよく確認して、正しい手順で操作することで攻撃を回避できることが望ましい。

7　攻撃に関係する可能性のある不審なファイル

本四半期に限らず、IPA では公開情報を調査している中で、不審なファイルを入手し当該ファイルを分析した上で、必要に応じて参加組織へ情報共有を行うことがある。本四半期、なんらかの攻撃に関連する可能性のあるファイルを確認した。

本章では、当該ファイルについて説明する。

不審ファイルの入手に至る経緯

2021 年 6 月 1 日、ファイル名に「ASEAN-Japan」というキーワードを含む RAR 形式の圧縮ファイル（表 6 #1）を入手した。当該ファイルについて調査を行いつつ、何らかのサイバー攻撃の痕跡の可能性もあるものとして、参加組織へ情報共有した。また、その後も継続して分析をしつつ動向を監視していたところ、複数の類似する検体について入手するに至り、都度参加組織へ情報共有を行った。

なお、2021 年 6 月 2 日に、Recorded Future 社より本件に関連すると思われる情報[10]が公開されている。当該記事によると中国の関与があるとされる攻撃グループとの関連について言及はあるが、本攻撃が当該攻撃グループによるものかは断定されていない。

現時点で本件なんらかのサイバー攻撃の痕跡であるのかは不明だが、継続して監視を行っていく。

不審ファイルの一覧

IPA で入手した圧縮形式のファイルと、Windows ショートカット（.lnk）ファイルのファイル名とハッシュ値について表 6 に示す。

表 6 ファイル名とハッシュ値一覧

#	ファイル名	ハッシュ値(SHA-256)
1.	ASEAN-Japan Forum (27 May 2021).rar	542bba4019f2f5bd266036deaab509a309451ba022bbae57eeb534957dd26002
2.	Proposed Talking Points for ASEAN-Japan Summit.rar	a6057292247d928e6adcda5a48983d8702372ce195fc50ea4496f67c6ca57e26
3.	MOHS-3-covid.rar	1e629fe7c8911a9adbde2e35af4f6f9e60ee538638c82edbcbd7cce5ad2ff4ab
4.	NUG Meeting Report.rar	b9adc1433ef7c6fee4d36f73b79744ad611d51a8e039d4c384dd453e33452d0f
5.	2021-03-11.lnk	f76f1657205d7042fccfc811077bbada92c0fef735f158da35e7825da1cc6bec
6.	All-in-One_Pyidaungsu_Font.zip	ff1dcab09f24a4c314af3ee829f80127e5b54f5be2a13e812617f77d0deeef57
7.	210615_Cabinet_Meeting_Minutes.rar[11]	6a36507318893197311f6e4c5882e5988064734b3345e2ab5703b1716603751b
8.	People Defense Force.rar	1d3e2eeaec0707e531593aa9aadaee0ee7757b67de43eae924fad122e86f60a0

[10] Backdoor malware found on the Myanmar president's website, again(Recorded Future) https://therecord.media/backdoor-malware-found-on-the-myanmar-presidents-website-again/

[11] 本ファイルについては、Google Drive 上に設置されていたことも確認している。

不審ファイルの挙動

入手した圧縮形式のファイルを解凍すると、Adobe 社のアイコンを偽装した exe ファイル [12]と、Adobe 社のライブラリ名に偽装した dll ファイル [13]が出力される。この exe ファイルを実行すると、同梱された dll ファイルを読み込み、次の動作を行う。

なお、表 6 の#5 の Windows ショートカットファイルについては、実行すると発生する不正接続先が他の圧縮ファイル内の不正接続先と同一であるため、IPA では関連する検体と位置付けている。

- 次のフォルダパスへ自身をコピーする

%PUBLIC%¥Libraries¥【検体毎に異なるフォルダ名】

※作成されるフォルダは検体によって異なる。図 10 の例では「MTVUS」。

※exe ファイルは「Acrobat.exe」というファイル名にリネームしてコピーする。

図 10 コピーされるフォルダ例

- 次の場所にレジストリキーを作成し、感染を永続化させる

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run

※作成されるレジストリキー名は検体によって異なる。図 11 の例では「MTVUS」。

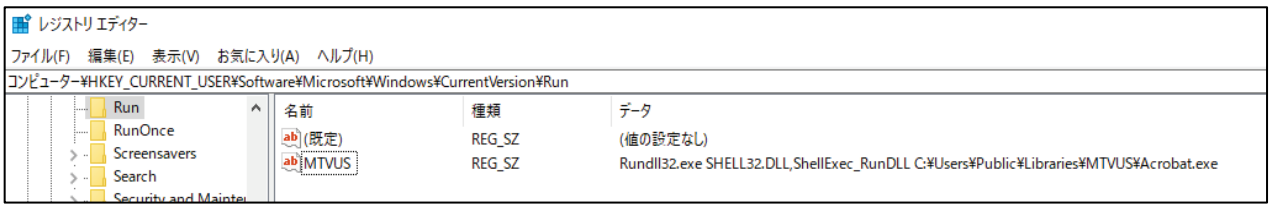

図 11 登録されるレジストリの例

- 不正接続先へ通信を行う

※不正接続先より不審なスクリプトファイルがダウンロードされることは確認しているが、
その後の具体的な挙動については不明である。

[12] 多くは圧縮形式のファイルと同名であるが、一部異なるファイル名のケースも確認している。

[13] Acrobat.dll と AcroRd32.dll の 2 パターンを確認している。

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