サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2021 年 7 月～9 月]

2021 年 10 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、2021 年 9 月末時点の運用体制、2021 年 7 月～9 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 7 月～9 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）。

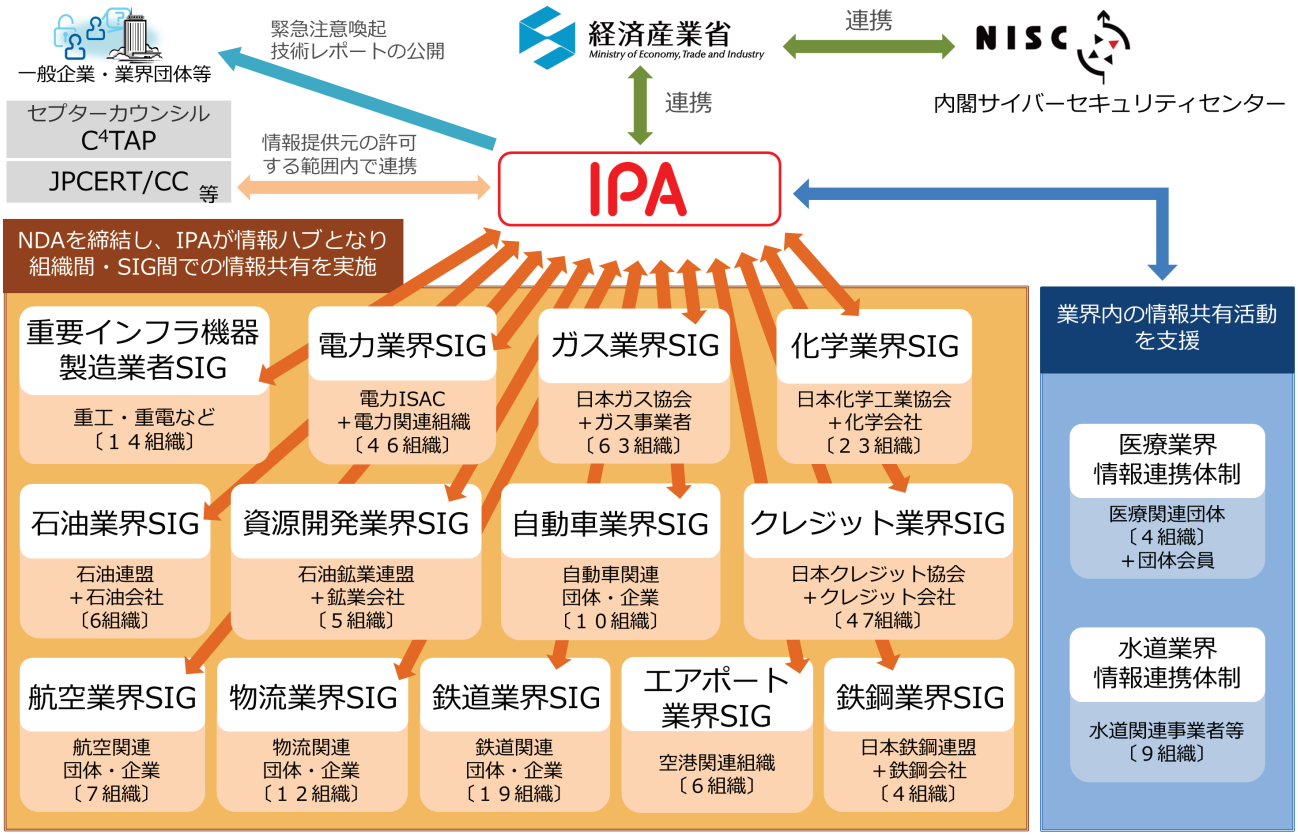

図 1 J-CSIP の体制図

[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 7 月～9 月）

2021 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 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		
		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	479 件	410 件	369 件	**346 件**
2	参加組織への情報共有実施件数※1	38 件	25 件	40 件	**21 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 **15 件**を含む。

本四半期は情報提供件数が **346 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 **3 件**であった。

次に挙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。

- 参加組織において、インターネット上の無償イラスト素材提供サイト（文書やウェブサイトに使用する画像を使用料無しの条件で配布しているサイト）からダウンロードした画像ファイルに、URL リンクが関連付けされており、最終的に不正ファイルとしてセキュリティソフトが検知したという情報提供があった。これについて 4 章で述べる。

- 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を受信したという情報提供があった。フィッシングメールとともにフィッシングサイトについて 5 章で述べる。

- Excel アドイン（.xll）ファイルを格納した圧縮ファイルが添付されたウイルスメールを受信したという情報提供があった。このメールはセキュリティソフトによる検知をすり抜けて受信者の元へ配送されたというものであった。これについては、詳細を 6 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	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
2	Google 検索をする中で発見したサイトへ訪問したところ、意図しない Onion ドメインのサイトへの通信が発生し、セキュリティソフトによって検知した。	1 件
3	ビジネスメール詐欺の疑いのあるメールを受信した。	1 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。	3 件

項番 1 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、サーバ内に複数の不正なファイル（ウェブシェル等）が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。提供された情報をもとに、不正ファイルのハッシュ値や不正接続先、不正アクセスを受けた日とその不正アクセス元となった複数の IP アドレスの情報を J-CSIP 内で共有したところ、不正アクセス元の IP アドレスの一部を、ファイヤーウォールにてブロックしていたという情報提供もあった。

項番 2 は、情報提供元のある従業員が、Google 検索をする中で発見したサイトへアクセスし、当該ページに表示された URL リンク先へアクセスしたところ、意図しない Onion ドメインのサイトへのアクセスが発生し、組織内のセキュリティ製品によって検知されたというものである。このときアクセスさせられる Onion ドメインのサイトは著作権侵害にもつながる可能性のある学術系の雑誌等の共有サービスであり、そのログイン画面が表示された。通常、Onion ドメインへのアクセスには、Tor ブラウザ等が必要であり、一般的な企業における業務で本件のようなサイトへのアクセスが行われることは少ないと考えられる。Onion ドメインへのアクセスに対する制限やポリシー等は適切に運用することが望ましい。

項番 3 は、J-CSIP の参加組織において、ビジネスメール詐欺の疑いのある不審なメールが着信したので、調査をしてほしいと情報提供されたものである。情報提供元の組織では、送付された先が正しい担当者宛ではなかったために不審と感じたとのことであったが、IPA で調査したところ、特にビジネスメール詐欺を示すような特徴は見られなかった。このため、情報提供元の組織にてメールの送信元へ正規のメールであるかを確認したところ、正規のメールであることが確認された。ビジネスメール詐欺に限らず、些細な不審さから攻撃に気付ける可能性があるため、普段のメールと違和感があれば、放置せず確認することが重要であろう。

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 [3]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。

[3] 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 2 件のビジネスメール詐欺について情報提供を受けた。これらはいずれも、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 3 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。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 海外関連企業を狙った攻撃

本事例は、2021 年 8 月、J-CSIP の参加組織の海外関連企業（A 社）の担当者に対し、同社の役員になりすました攻撃者から、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。

本事例で、攻撃者から送られたメールを図 2 に示す。なおメールはドイツ語で記載されていた。

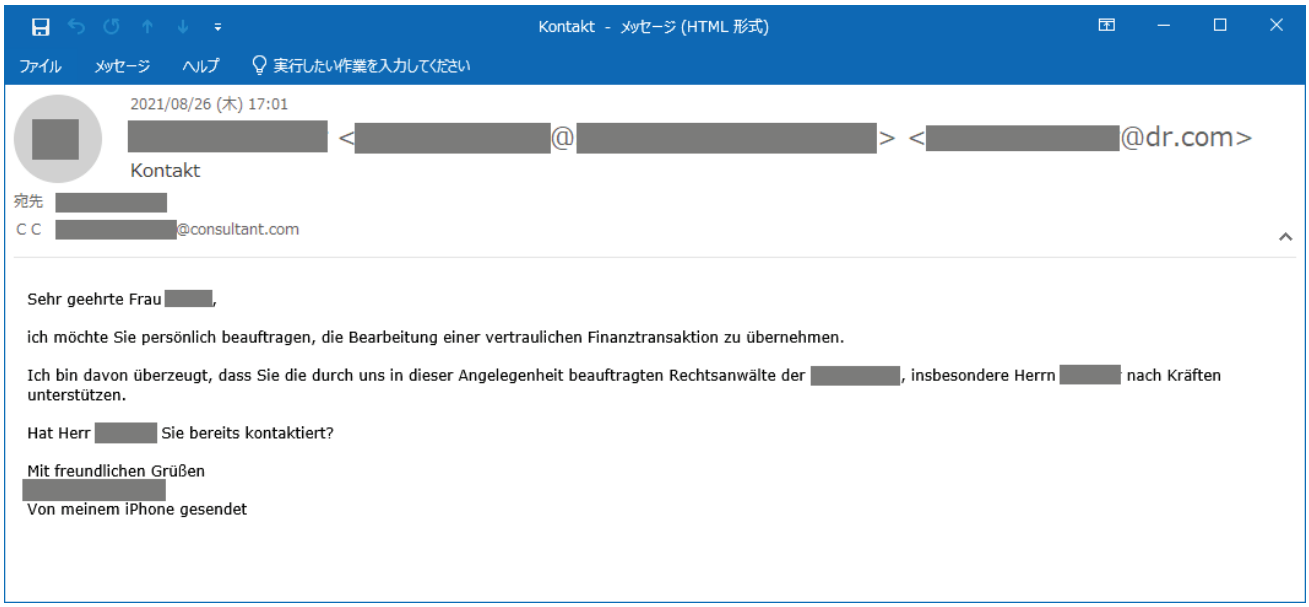

図 2 攻撃者から送られた偽のメール

攻撃者から送られた偽のメールは、機密性の高い金融取引を個人的に依頼したいという簡素な内容で、実在する弁護士事務所の弁護士へ連絡を取ってほしいという内容であった。差出人（From）の表示名には A 社役員の名前とメールアドレスが設定されていたが、実際にはフリーメールアドレスから送られていた。このフリーメールアドレスは、海外の「Mail.com[4]」というサービスで取得されたものであった。このサービスで取得可能なドメインの中には、過去ビジネスメール詐欺で使われたことのあるフリーメールドメインも存在している。

また、同報先（CC）には、弁護士のメールアドレスを騙った偽のメールアドレスが設定されており、あたかも弁護士も同報されているかのように見せかけていた。このメールアドレスのドメインは、公開情報を確認したところ、別の詐欺メールでも悪用されているという情報を確認している。

比較的簡単な内容の偽メールではあるが、騙されないよう注意が必要であろう。

[4] Mail.com
https://www.mail.com/consentpage

3.2 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
2021 年 7 月～9 月	2	2

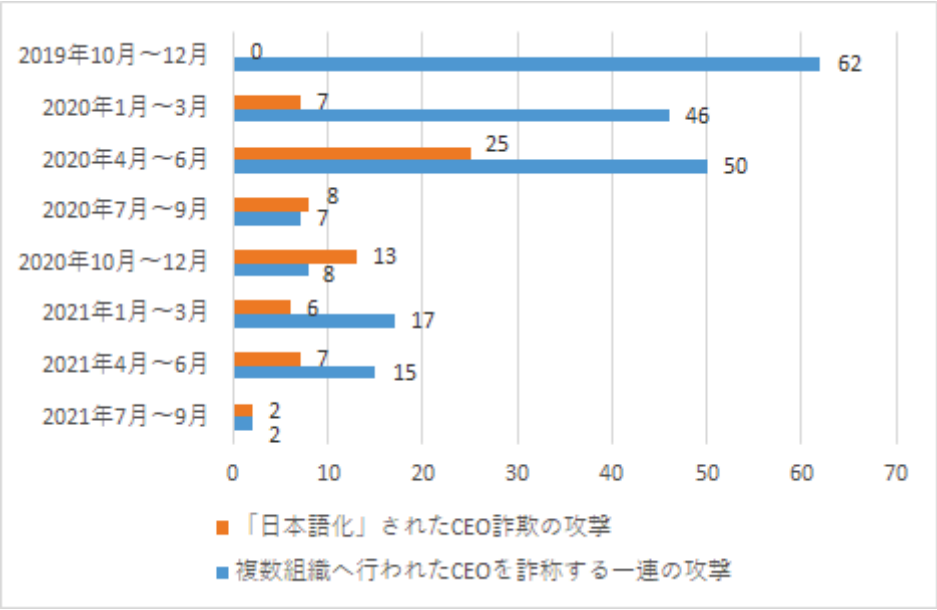

図 3 これまで入手したメール件数の推移

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[5]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。

[5] 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）[6]」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。

[6]【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　外部から入手した URL リンク付きの画像ファイルがセキュリティ製品で検知された事例

本四半期、外部から入手した画像ファイルに URL リンク情報が関連付けされており、セキュリティソフトによって検知されたという情報提供があった。本章では発見に至る経緯を含め説明する。

発見の経緯

2021 年 8 月 2 日、J-CSIP の参加組織から、インターネット上の無償イラスト素材提供サイトからダウンロードした画像ファイルについて情報提供があった。イラストをダウンロードして作成した PowerPoint 資料を PDF ファイルにした際、経緯は不明だが、当該画像ファイルに URL リンクの情報が関連付けされており、当該 URL リンクをセキュリティソフトが不審とみなし検知したとのことであった。当該画像ファイルは 2017 年頃にダウンロードされたもので、情報提供元の組織では、繰り返し組織内で利用しているものであった。事案発生後は、当該画像ファイルは削除し、今後の利用もしないように職員へ連絡した。

IPA でダウンロード元となった無償イラスト素材提供サイトを調査したが、2021 年 8 月時点で当該イラスト画像のファイルは存在していなかった。また、関連付けされた URL リンク先についても調査したが、2021 年 8 月時点で当該 URL 先も存在しておらず、本件が何らか悪意のあるものであったのか、利用者による操作の過程でたまたま URL リンクが関連付けされ、検知されてしまったのかは不明である。当該 URL が元々悪意のあるウェブサイトであったのか、改ざん等により検知の対象となったのかも不明である。

情報提供元の組織では被害等はなかったとのことであった。

ダウンロードした画像

情報提供元がダウンロードしたという画像[7]について図 4 に示す。

当該画像ファイルには、URL リンク情報が関連付けされており、マウスカーソルを合わせることによって、関連付けされた URL リンクが表示される。

本事例のように、無償のイラスト素材提供サイト等、外部から入手したファイルを利用する際は、信用できるサイトであるか注意するとともに、ダウンロードした画像を PowerPoint 等へ貼り付ける等の操作をした時、画像ファイルに URL 情報が関連付けられている場合、それを除去した方が安全であろう。

図 4 ダウンロードした画像と埋め込まれた URL リンク

[7] この画像については、作成者による著作権等を考慮し、一部モザイク処理を行っている。

5　自衛隊大規模接種センターを騙るフィッシング

本四半期、自衛隊の大規模接種センターを騙ったフィッシングメールが着信したという情報提供があった。本章では、実際に攻撃に使われたフィッシングメールを踏まえ説明する。

攻撃者から送られてきたフィッシングメールは日本語で書かれており、自衛隊の大規模接種センターでのワクチン接種のための予約案内を装うものであった（図 5）。このメールの本文中にある URL リンク（青字部分）はいずれも同一であり、クリックすると、フィッシングサイト（図 6）へ誘導される。

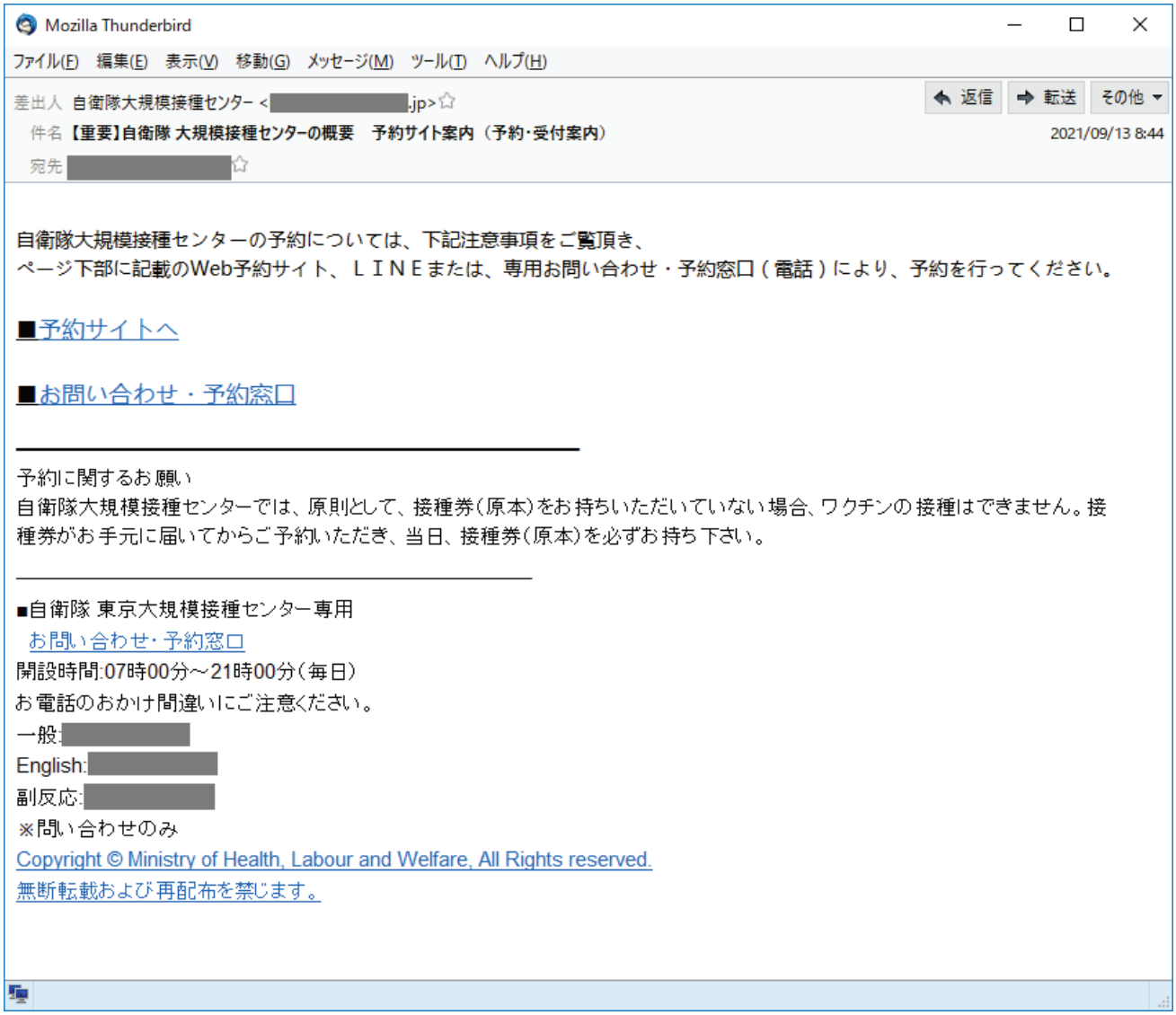

図 5 自衛隊大規模接種センターを騙るフィッシングメールの例

フィッシングサイトは、厚生労働省が公開している「コロナワクチンナビ [8]」を模した内容となっていた。

当該フィッシングサイトにある URL リンクはいずれも同じ内容であり、クリックすると個人情報を入力する画面（図 7）へ誘導される。

図 6 フィッシングサイト（アクセス時のトップ画面）

[8] コロナワクチンナビ（厚生労働省）
https://v-sys.mhlw.go.jp/flow/

さらに、個人情報を入力するページ（図 7）の下部にある、「次へ」のボタンをクリックすると、クレジットカード情報の入力をする画面（図 8）に進む。

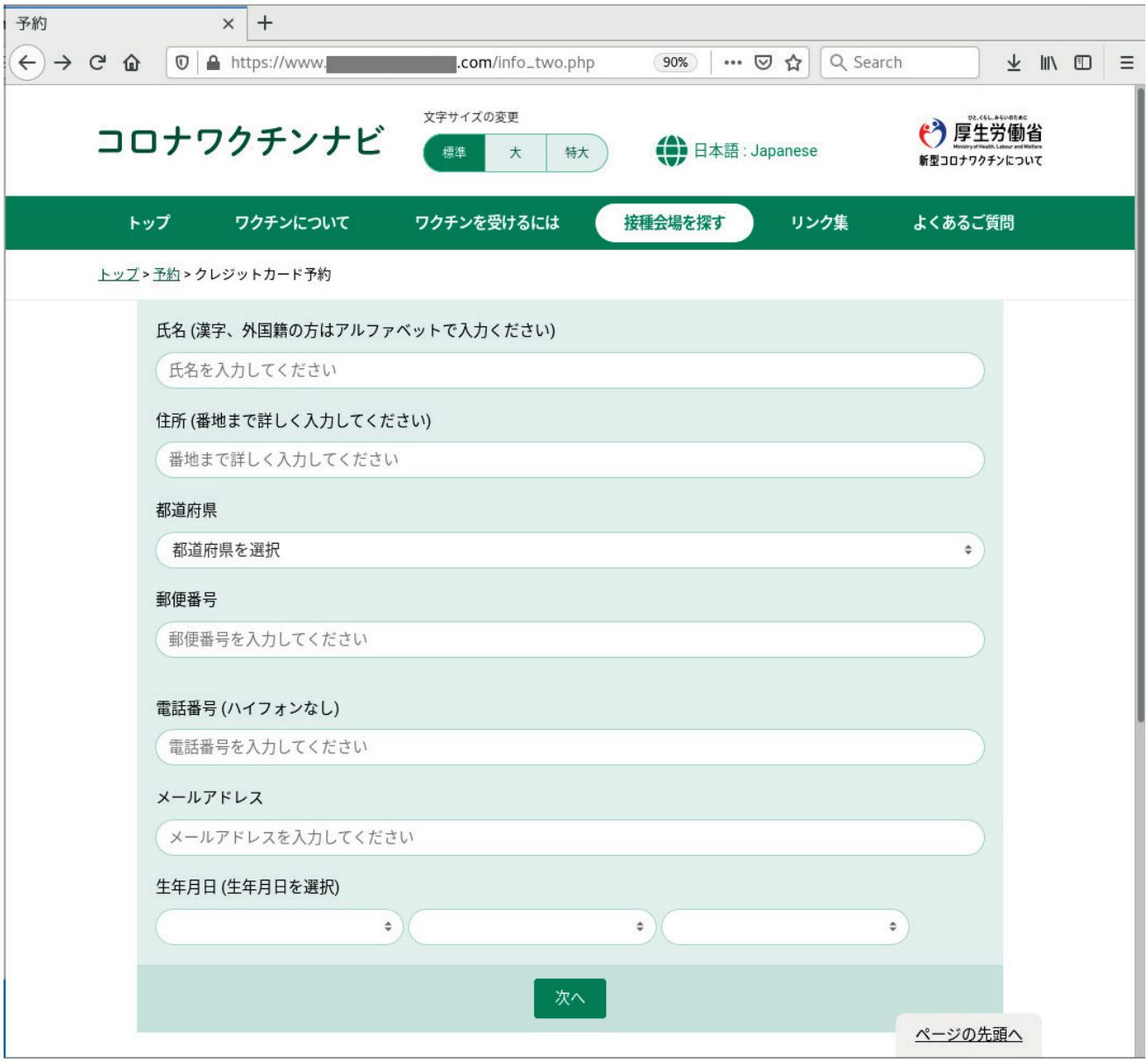

図 7 フィッシングサイト（個人情報の入力画面）

クレジットカードの入力画面（図 8）の下部にある、「次へ」のボタンをクリックすると、正規のコロナワクチンナビのサイトへ誘導されるようになっていた。

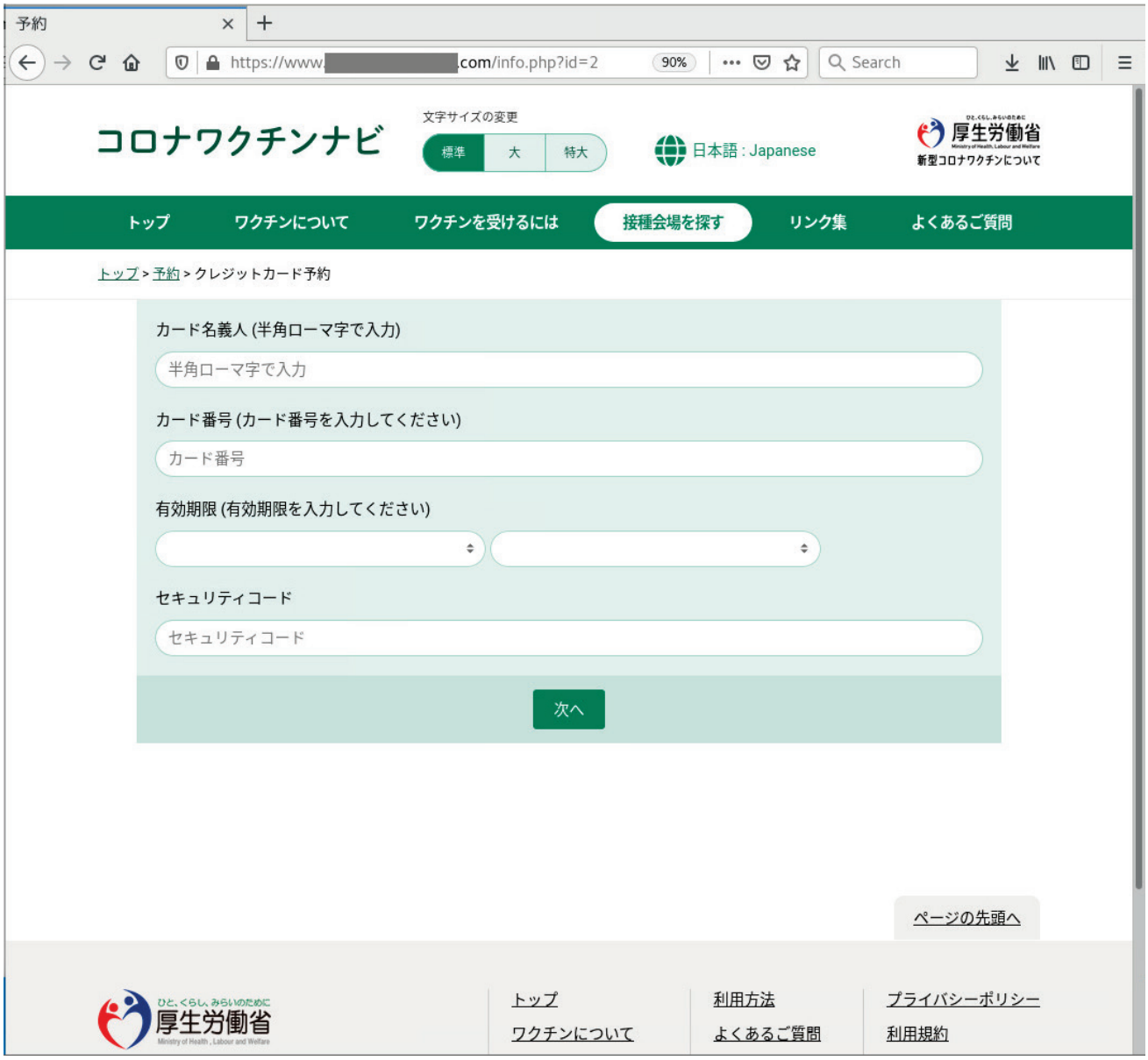

図 8 フィッシングサイト（クレジットカードの入力画面）

本件のフィッシングメールについては、フィッシング対策協議会 [9]を始め、公開情報で多数の注意喚起がなされている。

新型コロナウイルス感染症（COVID-19）のワクチン接種が進んできている中、このような題材を悪用するフィッシングメールは、今後も注意が必要であろう。

[9] 厚生労働省をかたるフィッシング（2021/08/30）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/mhlw_20210830.html

6 Excel 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、Excel アドイン（拡張子 .xll）[10]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 8 月 12 日、J-CSIP の参加組織から、約 1 時間の間に同組織の 62 のメールアドレスに対して不審メールの送付が試みられ、うち実在する 6 メールアドレスへメールが配送されたと情報提供を受けた。しかし、メール自体はメールソフトのセキュリティ機能によって検知されていたため、実際の利用者へは着信はしなかったとのことである。メールには「支払い書のコピーと請求書を添付したため、確認を願う」といった内容が英語で書かれており、RAR 形式の圧縮ファイルが添付されていた（図 9）。この RAR 形式の圧縮ファイル内には悪意のある Excel アドインファイルが格納されていたが、セキュリティソフトでの検知がされなかったとのことである。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。

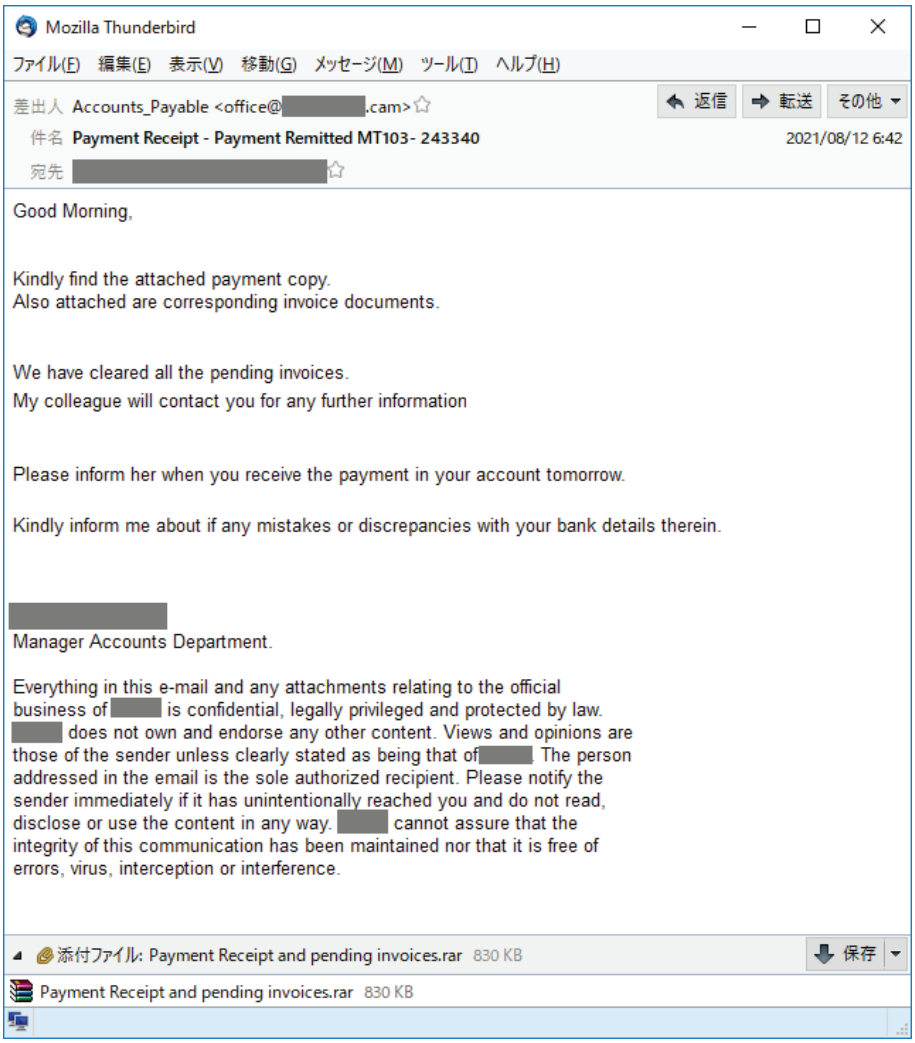

図 9 情報提供された不審メール

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

Excel アドインファイルの悪用

不審メールの添付ファイル（RAR 形式の圧縮ファイル）を解凍すると、Excel に関連付けされた、拡張子が「xll」のファイル（Excel アドインファイル）が 1 つ得られる（図 10）。

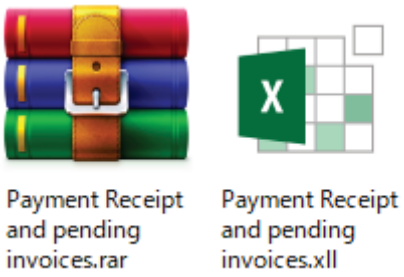

図 10 添付ファイルおよび解凍して得られる Excel アドインファイル

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 11 の Excel の警告ウインドウが表示される。利用者が、「このアドインをこのセッションに限り有効にする」を選択すると、ロシア語で書かれた請求書を装った表示用のダミー文書ファイルが表示（図 12）され、最終的に別のウイルスへ感染させられてしまう。なお、「このアドインを無効なままにする」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。

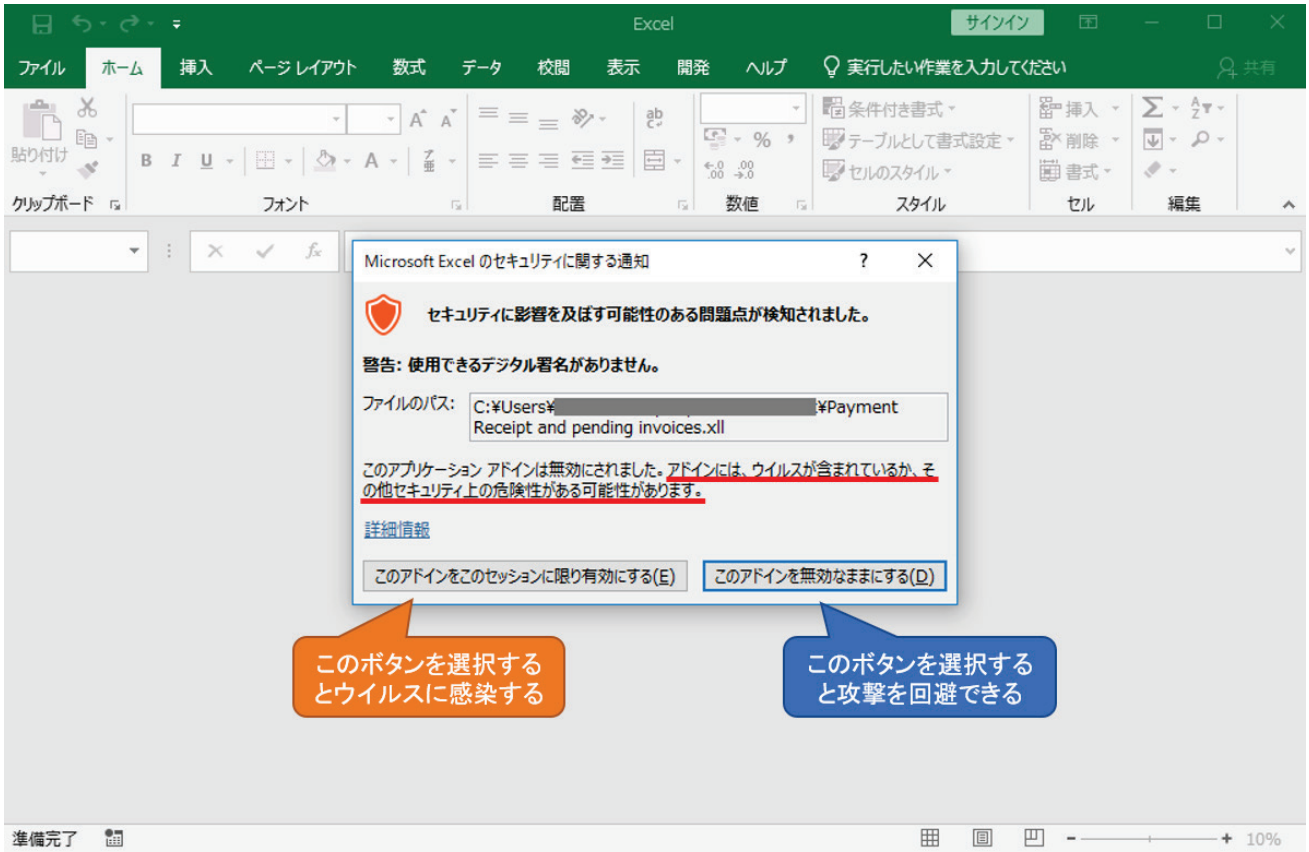

図 11 Excel で悪意のある Excel アドインファイルを開いた際に表示される警告ウインドウ

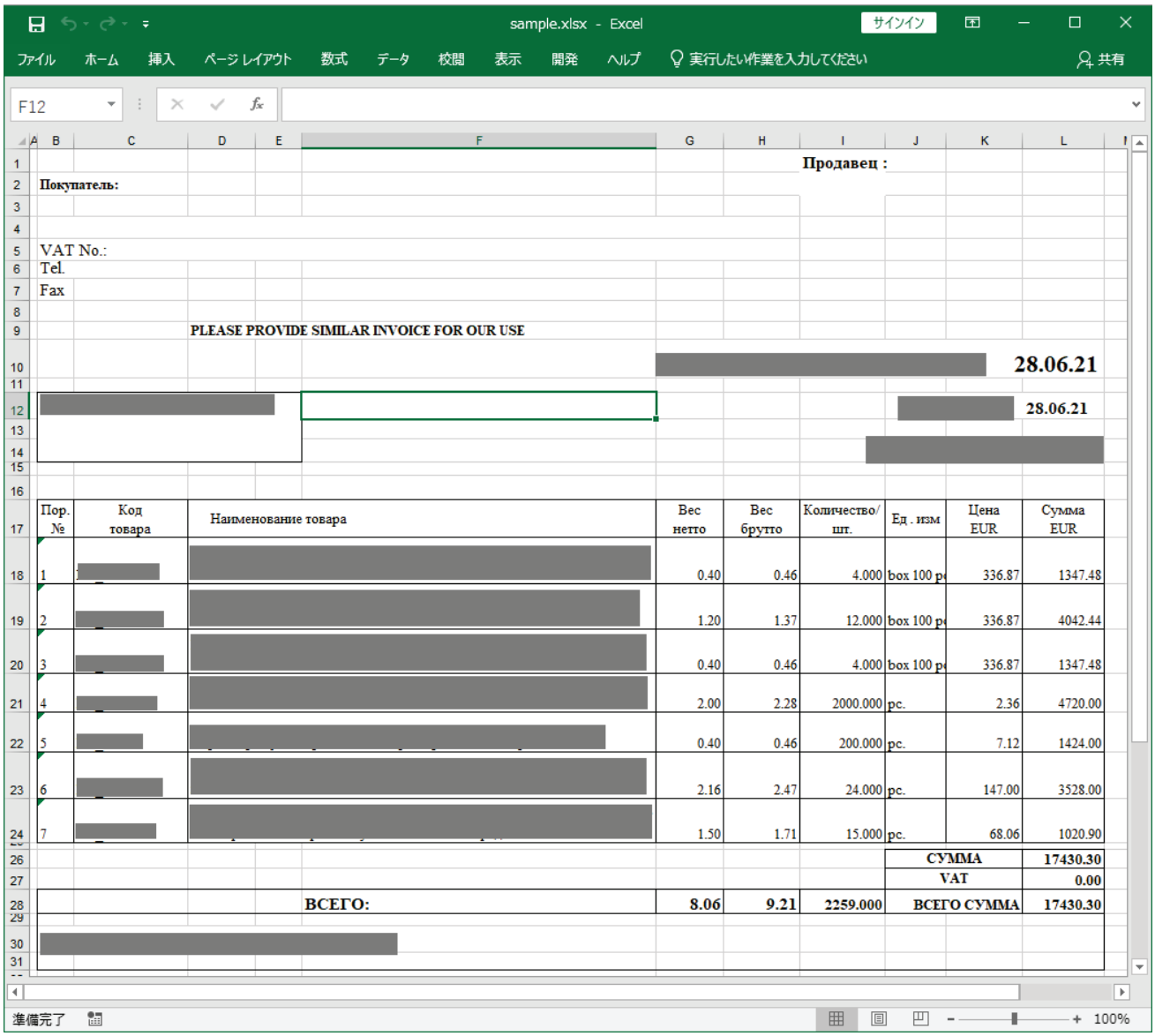

図 12 表示用のダミー文書ファイル

Excel アドインファイルの仕様を悪用するこの攻撃手口は、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「.xll」が格納された添付ファイルの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の対策としては、正しい対処（選択）が分からないダイアログウインドウが開いた時は、一旦操作をやめ、システム管理者等へ連絡できるようにすることが望ましい。

国内での観測状況とIPAでの調査

Excelアドインファイルを悪用した攻撃については、2021年9月2日に、日本医師会を騙る不審なメールがばらまかれているとして、同組織から注意喚起[11]が出されている。IPAでは、本件に加えExcelアドインファイルを悪用した攻撃について、公開情報より情報を収集して調査・解析を行った。これについては、参考情報として本紙の付録として示す。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

[11] 【注意喚起】日本医師会を騙る不審メールの流通について（日本医師会）
https://www.med.or.jp/nichiionline/article/010228.html