サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2019 年 10 月～12 月]

2020 年 1 月 31 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、2019 年 12 月末時点の運用体制、2019 年 10 月～12 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

2019 年 10 月～12 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 249 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）。

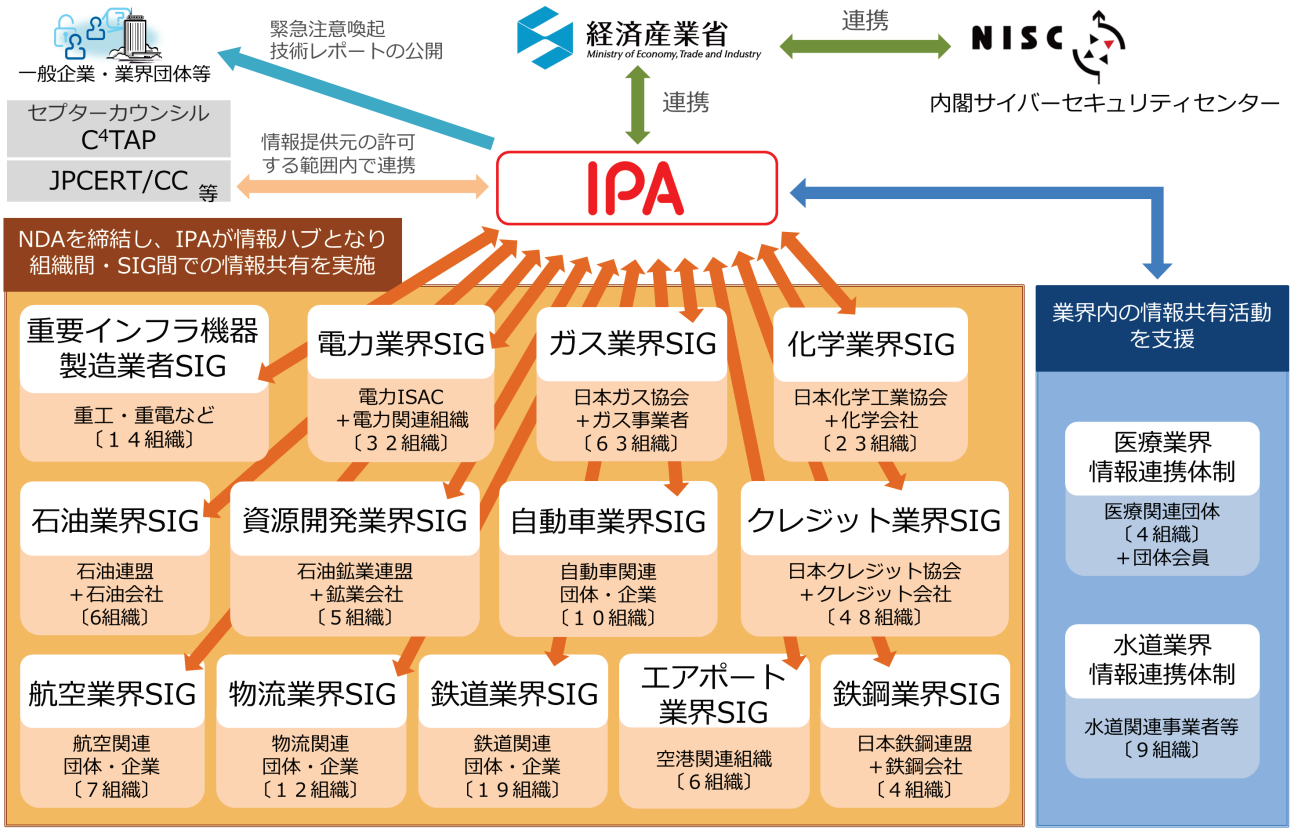

図 1 J-CSIP の体制図

[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（2019 年 10 月～12 月）

2019 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 249 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	2019 年			
		1 月～3 月	4 月～6 月	7 月～9 月	**10 月～12 月**
1	IPA への情報提供件数	238 件	424 件	235 件	**1,042 件**
2	参加組織への情報共有実施件数※1	48 件	54 件	75 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 **22 件**を含む。

本四半期は情報提供件数が **1,042 件**であり、うち標的型攻撃メールとみなした情報は **47 件**であった。提供された情報の主なものとして、Emotet への感染を狙うウイルスメールがおよそ 7 割を占めている。これについては、5 章で詳しく述べるが、Emotet への感染を狙うウイルスメールについては、国内で大規模にばらまかれていることを確認している。また、本四半期では Emotet への感染を狙うウイルスメール以外にも、日本語のばらまき型と考えられるメールで、Emotet とは異なるウイルスへの感染を狙うメールも複数観測している。

このほか、次に挙げる情報提供があり、一部情報共有を行った。

- 38 件のビジネスメール詐欺について情報提供があった。IPA で追加調査したところ、複数の国内外の組織に向け、連続した攻撃が行われたと思われる痕跡について確認できた事例もあった。これらについては 3 章で詳しく述べる。

- 2017 年 10 月から注視している、プラント関連事業者を狙う一連の攻撃において、初めて日本語の攻撃メールを観測した。この一連の攻撃は、プラント等の設備や部品のサプライヤーに対し、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールであり、短期間で多岐にわたる文面のバリエーションを確認している。現時点では、攻撃者の目的が知財の窃取にある（産業スパイ活動）のか、あるいはビジネスメール詐欺（BEC）[3]のような詐欺行為の準備段階のものかは不明だが、ある程度特定の組織へ執拗に攻撃が繰り返されていることから、標的型攻撃の一種とみなして取り扱っている。詳しくは 4 章で述べる。

[3] Business E-mail Compromise （ビーイーシー）
【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（続報） （IPA）
https://www.ipa.go.jp/security/announce/201808-bec.html

- 2018 年 11 月に正規のウェブサイトに酷似した偽のウェブサイトが設置され、そのウェブサイトを利用した詐欺の事例について情報提供を受け、監視を続けていた。この偽サイトが、2019 年 9 月に停止した（アクセス不能となった）ことを確認した。本件について、発覚に至る経緯と、実施した対応内容等を共有した。これについては、6 章で述べる。

- 本四半期に限らず、不審なメールとしてフィッシングメールが情報提供されることがあるが、本四半期では、インフルエンザを題材としたフィッシングメールが送信されたという攻撃を確認した。これについては、7 章で述べる。

- 解凍ソフトの種類によって、解凍されるファイルが変わるように細工された不正な ZIP ファイルを使った攻撃の事例を確認した。文面は英語ではあるが、日本の組織でも着信したことを確認しており、今後も別の攻撃で使われる可能性もあるものと考えている。これについては、8 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	自組織を騙るウイルスメールが取引先に送られた。	1 件
2	標的型攻撃の訓練メールが着信した。	1 件
3	フィッシングメールに記載されたフィッシングサイトの URL へアクセスしてしまった。	1 件
4	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。	16 件
5	組織内のセキュリティ製品において、検知数が大幅に増加している傾向にある。	1 件

項番 1 は、自組織を騙るウイルスメールが取引先の企業へ送信されてしまったという情報提供である。攻撃者によって、自組織が騙られ、メールが送付されてしまうというケースは特にめずらしい事象ではないが、実際に問い合わせがあった場合の対応手段等は日ごろから整備しておくとよいであろう。

項番 2 は、不審なメールとして IPA へ情報提供があったものだが、確認の結果、自組織内の標的型攻撃の訓練メールだと分かったものである。組織内の情報システムやセキュリティの運用をアウトソースしているケースもあると思うが、自組織内で行う標的型攻撃の訓練については、予期しないことも起こり得る。アウトソース先も含めて、事前に情報システムの関係者で訓練の計画を共有しておく必要があろう。

項番 3 については、不審なメールの本文に書かれている URL リンクをクリックしてしまったという情報提供・相談である。調査したところ、このメールはフィッシングサイトへの誘導を目的とするものであったため、フィッシングサイト上で ID やパスワードの入力を行わなければ直接的な被害を受けるものではなかった。ただし、不審メールの本文中の URL をクリックすることでウイルスに感染してしまうという攻撃もあるため、安易にこのような操作はしないように注意するべきである。

項番 4 は、組織内の PC から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、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]等にだま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。

項番 5 は、組織内のセキュリティ製品（ゲートウェイ、メール、エンドポイント等）が検知する数が最近大幅に増加しているという相談であった。確認したところ、Emotet への感染を狙う攻撃メール等大規模なばらまき型メールや、項番 4 の情報提供と同様の不審サイトへのアクセスの検知の増加が、当該組織においても観測されていたと思われるものであった。セキュリティ製品のログ等においては、必ずしも「Emotet」のような明確なウイルス名で検知されて記録されるとは限らないため、日々の運用の難しさが従前からの課題である。

[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 月に IPA より注意喚起を行ったが、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。

本四半期は、J-CSIP の参加組織から 32 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 30 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。また、J-CSIP の参加組織外からも 6 件のビジネスメール詐欺の情報提供があった。これら合計 38 件のうち、事例情報として公開許可の得られた 5 件の事例について表 3 に示す。なお、いずれの事例においても、すべて英文のメールであった。

本章では、このうち更に 3 件の事例を詳しく説明する。

表 3 ビジネスメール詐欺の事例概要

項番	情報提供日		事例概要	被害の有無	備考
1.	2019 年	9 月 4 日	2019 年 8 月、日本国内の企業(支払側)に対して、攻撃者が海外の取引先企業(請求側)になりすまして、偽の口座へ振り込みを要求するメールを送りつけるビジネスメール詐欺が試みられた。 ・ 取引先企業から本物の請求書(PDF ファイル)が届いた 5 日後に「振込口座変更のお知らせ」という内容の英語のメールで、振込先口座と日付を修正した請求書(PDF ファイル)が攻撃者から送られてきた。 ・ 本件では、攻撃者とメールのやりとりは行ったものの、不審に思った担当者が電話で取引先に確認し、なりすましが発覚したため、金銭的な被害は無かった。メール盗聴の原因究明のため、PC とネットワーク関連のログ等を確認したが、特段不審なアクセス等の形跡は確認できなかった。	なし	-
2.		10 月 21 日	2019 年 10 月、日本国内企業(支払側)と、海外取引先企業(請求側)との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	本書:事例 1
3.		10 月 24 日	2019 年 8 月と、2019 年 10 月、日本国内企業の別の国内グループ会社の経営層になりすました攻撃者から、それぞれの企業の海外関連企業の担当者に対しビジネスメール詐欺が試みられた。	なし	本書:事例 3
4.		12 月 4 日	2019 年 11 月、日本国内の企業(A 社)の欧州子会社(B 社)の担当者に対して、A 社の CEO にな	なし	-

項番	情報提供日		事例概要	被害の有無	備考
			りすました攻撃者から、偽のメールを送り付けるビジネスメール詐欺が試みられた。極秘の企業買収案件という名目の偽メールであった。 本件は、B 社の担当者と攻撃者の間でメールのやり取りを行ったものの、B 社の担当者がやり取りしているメールの内容を不審に思い、B 社の CEO を通じて A 社の CEO へ確認をしたところ、偽のメールであると発覚した。		
5.		12 月 12 日	2019 年 11 月、日本国内企業の海外関連会社（請求側）と、海外取引先企業（支払側）との取引において、攻撃者が請求側企業の担当者になりすますビジネスメール詐欺が試みられた。	なし	本書:事例 2

3.1 事例 1 国内組織を狙った攻撃

本事例は、2019 年 10 月、J-CSIP の参加組織の国内企業（A 社：支払側）と、その海外取引先企業（B 社：請求側）との間で取引を行っている中で、攻撃者が B 社の担当者になりすまし、「財務監査により銀行口座が使用できなくなったため、代理の口座に送金する必要がある」という理由で偽の口座への振り込みを要求するメールが送られたものである。

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、支払側である A 社の担当者が不審な点に気づいた。また、**攻撃者がミスをした**と思われるが、請求側の B 社担当者もなりすましメールが発生したことを認識することができ、A 社の担当者へすぐに連絡したため、金銭的な被害には至らなかった。

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) 財務監査を理由に偽の口座への変更を装う
(2) 詐称用ドメインの取得と悪用
(3) メール引用部分の改変

（1） 財務監査を理由に偽の口座への変更を装う

本事例では、A 社（国内企業）と、その取引先である B 社（海外取引先）との間で、取引に関するメールのやりとりを行っていた。このメールのやりとりの中で、A 社担当者から、B 社担当者へ 2019 年 10 月 18 日に支払を行う旨を伝えていた。支払にかかるタイミングを見計らい、攻撃者は「財務監査で口座が使用できない」という理由で、偽の口座への送金を要求するメールを送り付けてきた。攻撃者は、何らかの方法でメールのやりとりを盗聴していたものと考えられる。

攻撃者から A 社担当者へ送られてきたメールは 2 通あった。1 通目のメールは、同報先（CC）のメールアドレスに、B 社担当者のメールアドレスが設定されていた。本来であれば A 社担当者にのみ偽のメールを送り付けるのがビジネスメール詐欺の常套手段であるが、この偽メールは同報（CC）により B 社の担当者にも着信している。これは、**攻撃者がミスをした**ものと推測している。

2 通目のメールは、1 通目のメールを引用しつつ、約 15 分後に送られた。2 通目のメールでは、同報先のメールアドレスだけでなく、メールの引用部分にある 1 通目のメール内容からも、B 社担当者のメールアドレスが削除されていた。恐らく、攻撃者は、1 通目のメールを送った後に、同報先に B 社担当者を設定してしまったことに気づき、この 2 通目のメールを送ることで隠蔽工作を図ったものと考えられる。

このやり取りの中で、A 社の担当者は差出人のメールアドレスが不審なものであると気づき、また、1 通目の偽メールを受信した B 社の担当者から、A 社の担当者へ、なりすましメールが送られた旨の連絡があったことで、事案が発覚した。

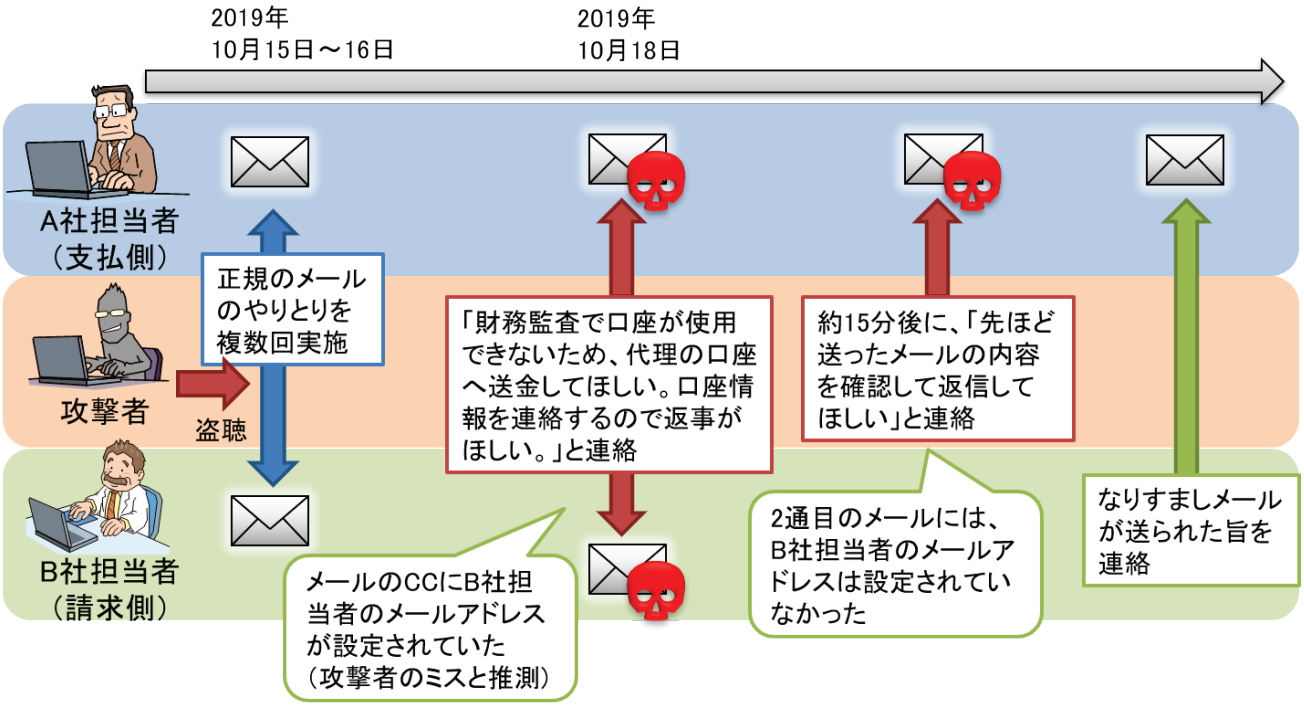

図 2 事例 1 攻撃者とのやりとり

（2） 詐称用ドメインの取得と悪用

攻撃者は B 社の正規ドメインに似通った「詐称用ドメイン」を新規に取得していた。詐称用ドメインは、次の例に示すように、正規のドメイン名を 1 文字変更したものであった。

【本物のメールアドレス】 alice @ b-company . com
【偽物のメールアドレス】 alice @ b-compeny . com （「a」を「e」に 1 文字変更）

※実際に悪用されたものとは異なる。

また、本事例の詐称用ドメインは、ドメインの登録情報（whois 情報）から、なりすましメールを送信する”**約 2 時間前**”に取得されていた。不正な目的で自組織の類似ドメインが新たに取得されていないかを定期的にチェックしている企業があるが、そのような対策を回避しようとしているものと考えられる。あるいは、メールの盗聴を続けながら、詐欺を仕掛けられそうなタイミングで、状況に応じてドメインを適宜取得するという、柔軟かつ素早い行動をとっている可能性もある。

（3） メールの引用部分の改変

攻撃者は、A 社の担当者へ向けて 2 通目のメールを送った際、1 通目のメールを引用する形でメールを送信していた。この時、（1）で説明した通り、引用されていた 1 通目のメールのヘッダ部分にある同報先（CC）のメールアドレスから、B 社担当者のメールアドレスを削除していた。

メールの引用部分を改変することで、それまでのやり取りについて、偽のメールであることを気付かせないように細工する点も、ビジネスメール詐欺でよく見られる手口である。

3.2 事例 2 海外グループ企業を狙った攻撃

本事例は、2019 年 11 月、情報提供元企業（J-CSIP 参加組織）の海外子会社（A 社：請求側）と、同企業の別の海外子会社（B 社：支払側）との間で取引を行っている中で、攻撃者が A 社の担当者になりすまし、B 社へ偽の振込先を記載した書類を送り付けてきたものである。すなわち、**同じグループ企業間であっても、ビジネスメール詐欺が試みられる可能性がある**ことを示す事例である。

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、支払側である B 社の経理担当者が不審な点に気づき、A 社の担当者へ直接電話による確認を行ったことで、偽のメールであることが判明し、金銭的な被害には至らなかった。

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) 支払にかかるタイミングで偽の口座への変更を装う
(2) A 社担当者のメールアカウントの悪用
(3) 詐称用ドメインの取得と悪用
(4) 正規の書類フォーマットの悪用

（1） 支払にかかるタイミングで偽の口座への変更を装う

A 社と、その取引先である B 社との間で、取引に関するメールのやりとりを行っていた。このとき、なんらかの方法で攻撃者は A 社のメールアカウントの情報を窃取し、メールのやりとりを盗聴していたものと考えられる。支払にかかるタイミングを見計らい、攻撃者は「従来の口座が使用できなくなる」という理由で偽の口座への送金を要求するメールを送り付けてきた。

攻撃者から送られてきたメールを受信した B 社の担当者は、B 社の経理担当者へメールを転送し、以降は B 社経理担当者と攻撃者の間で、メールのやりとりが行われた。B 社経理担当者は、攻撃者に騙され、支払の期限を連絡しつつ、新しい口座情報を連絡してほしいという旨のメールを攻撃者へ返信した。そして、約 9 時間後、攻撃者から偽の銀行口座情報が書かれた書類（書類には、「従来の銀行口座は、税務監査の最中であるため使用できない」と記載されていた）と、A 社の偽の子会社の法人設立証明書が添付されたメールが送られてきた。

このやり取りの中で、B 社経理担当者はメールの内容を不審と感じ、A 社の担当者へ電話で確認を行ったことで事案が発覚した。

事案発覚後、A 社ではすぐに A 社担当者を含め、全社員に対してメールアカウントのパスワード変更を指示した。その後の調査で、A 社担当者のメールアカウントが何者かにより乗っ取られていた形跡があることが判明した。

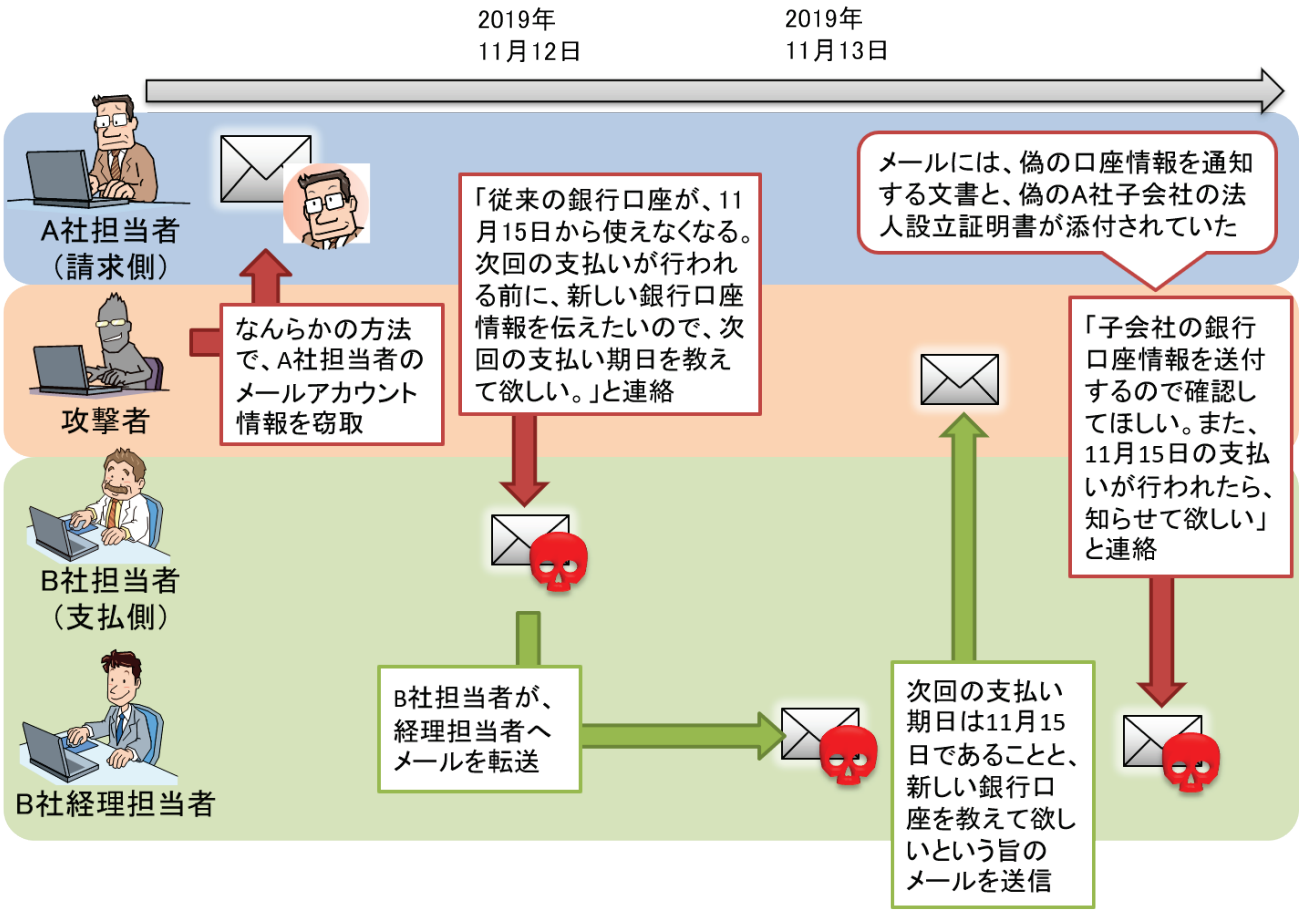

図 3 事例 2 攻撃者とのやりとり

（2） A 社担当者のメールアカウントの悪用

A 社は Office 365（Exchange Online）を使用していた。事案の発覚後、ログを確認したところ、A 社担当者が所在していない国から、A 社担当者が利用していないウェブメールサービス（Outlook Web Access）を使って、B 社へなりすましメールが送られていた。

すなわち、攻撃者は何らかの方法で窃取した A 社担当者のメールアカウント情報で、ウェブメールサービスへログインしていたことになる。この手口を使われた場合、当然ながら A 社担当者の正規のメールアドレスからメールが送られてくるため、受信者は偽のメールであると気付くことが非常に難しくなる。

また、攻撃者は、A 社担当者のメールアカウントに対して、特定期間のみ、**本件に関する送受信メールを「RSS フィード [5]」へ振り分けるルールを不正に設定していた。**攻撃者は、A 社担当者が普段はあまり注視しないフォルダに詐欺のやりとりのメールを振り分けることで、メールアカウントを乗っ取っていることに気付かれにくくさせようとしたと考えられる。

（3） 詐称用ドメインの取得と悪用

攻撃者は A 社の正規ドメインに似通った「詐称用ドメイン」を新規に取得していた。詐称用ドメインは、次の例に示すように、サブドメインの区切りのピリオドをハイフンに変更したものであった。

---

[5] 登録したウェブサイトが更新されると、更新内容が通知される機能（および、その通知が保存されるフォルダ）

【本物のメールアドレス】 alice @ subdomain . company . com
【偽物のメールアドレス】 alice @ subdomain-company . com （「.」を「-」に 1 文字変更）

※実際に悪用されたものとは異なる。

攻撃者は、この詐称用ドメインを使った偽のメールアドレスをメールの同報先（CC）に設定し、B 社へ偽のメールを送り付けていた。この手口により、A 社の関係者には実際にはこの偽メールが届いていないため、詐欺が行われていることに気付けないことになる。

また、本事例との関係は不明であるが、ドメインの登録情報（whois 情報）から、この詐称用ドメインは 2018 年 5 月に既に何者かによって取得されており、2019 年 3 月には別の攻撃で悪用された可能性を示す痕跡が確認できた。

さらに、この詐称用ドメインの取得者は、他の企業のドメインに似た偽のドメインを複数取得していた痕跡があり、ビジネスメール詐欺やその他サイバー犯罪を常習的に行っている可能性が考えられる者であることも分かった。

（4） 正規の書類フォーマットの悪用

攻撃者から送られてきたメールには、**実際に A 社が使用している書類フォーマットに則った形式で、偽の銀行口座情報が書かれた文書**が添付されていた。すなわち、攻撃者は、A 社担当者のメールアカウントを乗っ取った上で、担当者の過去のメールから A 社の正規の文書を入手し、その文書を流用して偽の銀行口座情報が書かれた文書を作成したと思われる。文書の中には、A 社と B 社の親会社のロゴや、A 社担当者とは別の、A 社の職員のサインが記されていた。

本件の事例のように、「正規のフォーマットに則って作成された偽の文書」が送られてくるというビジネスメール詐欺の事例は他にもあり、メールの受信者において、偽物であると気付くことが難しくなっている。

3.3 事例 3 複数組織へ行われた CEO を詐称する一連の攻撃

2019 年 10 月、J-CSIP の参加組織から、国内グループ会社の経営層を詐称し、当該グループ企業の海外関連企業の担当者に対し、なりすましメールが送られたという情報提供があった。この情報を J-CSIP 内で情報共有を行ったところ、複数の SIG の参加組織からも類似した攻撃の情報提供があり、合計 32 件の攻撃メールを把握した。

これらの事例を基に、IPA で J-CSIP 外の情報等を含め独自に調査を行ったところ、情報提供されたものと合わせて **62 件**の類似するメール検体を入手するに至った[6]。これらのメールは次に示す特徴が共通しており、同一の攻撃者による攻撃が、国内外の多数の組織へ行われたものと推測される状況であった。この一連の攻撃については、攻撃手口等からビジネスメール詐欺の一種であると考えている。

- メールの宛先は、国内外の複数の企業(職員等と思われるメールアドレス)である。
- 実在する CEO や弁護士等を詐称している。
  - CEO を詐称する際、ほぼ、攻撃先の各企業の実際の CEO を名乗っている。
- 攻撃者が使用したメールアドレスは様々に異なるが、命名に規則性がある。具体的には、差出人(From)や返信先(Reply-To)に、「secure」という単語と、天体(惑星・衛星等)に関する単語を組み合わせたメールアドレスが使用されている。
- 件名や本文はほぼ英文であり、日本語とスペイン語のメールは 1 件ずつ確認している。メールの内容は多数のバリエーションがある。メール本文は 5～10 行程度の簡素なもので、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る点が共通している。
  - メールへ返信すると、金銭の振り込みの要求等の詐欺が試みられるものと思われる。
- メールの着信時期は、確認できている限り、2019 年 7 月 23 日から 2020 年 1 月 16 日である。

攻撃メール(英文)の例と、IPA で確認したメールの情報の一覧を、図 4 と表 4 に示す。併せて、日本語の攻撃メール(表 4 の項番 53)の例について、図 5 に示す。

こ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、多数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、継続して国内外の組織に対して攻撃が試みられる可能性があり、今後も注意が必要である。

また、これらは冷静に考えれば不審と判断できそうなメールではあるが、J-CSIP 参加組織のいくつかの組織では、受信者が攻撃者に返信を行ってしまったとのことであった。IPA が J-CSIP 外から入手した事例では、受信者が攻撃者へ返信した結果、攻撃者からさらにメールが送付された痕跡も確認している。すなわち、このような典型的な「CEO 詐称」のメールであっても、職員が一定の確率で騙されてしまい、これを発端に、巧妙な詐欺が行われる可能性はあると考えられる。

企業・組織が相対している敵は「偽メール」ではなく、そのメールを送り付けている攻撃者(人間)であり、その攻撃者は複数の組織に対して執拗に攻撃を繰り返している。偽物だと見破ることが容易に見えるようなメールであったとしても、侮るべきではないだろう。

---

[6] 本事例については、本レポート執筆時点である 2020 年 1 月 20 日までの情報で記載している。

図 4 事例 3 攻撃者から送られたメールの例

表 4 事例 3 IPA で確認している本件の攻撃メール情報の一覧

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
1.	保険業	2019/7/23	Re: Important – Urgent Discussion	secure-nexus@secure-email-host.com
2.	飲料・たばこ・飼料製造業	2019/7/31	Important – Urgent discussion	secure-nexus@secure-mail-host.com
3.	農業	2019/8/7	Follow-up discussion today	secure-net-jupiter@secure-email-server.net
4.	不動産取引業	2019/8/13	Follow-up discussion	secure-node-jupiter@secure-mail-cast.com
5.	通信業	2019/8/20	Discussion today – corporate development	secure-pluto@secure-mail-net.com
6.	輸送機械器具製造業	2019/8/26	Discussion – corporate development	secure-uranus@secure-email-server.cc
7.	情報サービス業	2019/8/29	Discussion today – corporate development	secure-neptune@secure-email-host.cc
8.	銀行業	2019/9/5	Notificación en curso	secure-mercury@secure-mail-server.cc
9.	保険業	2019/9/5	Corporate development matters	secure-uranus@secure-smtp-host.cc
10.	化学工業	2019/9/12	Liaising with external legal counsel	secure-mercury@secure-smtp-host.cc
11.	製造業	2019/9/13	Liaising with external legal counsel	secure-jupiter-server@secure-smtp-host.cc
12.	製造業	2019/9/13	Liaising with external legal counsel	secure-jupiter-server@secure-smtp-host.cc
13.	製造業	2019/9/19	Liaise With Legal Advisors	secure-saturn@secure-mail-server.cc
14.	化学工業	2019/9/23	Liaise With Legal Advisors	secure-uranus-mx@secure-mail-host.cc
15.	水運業	2019/9/25	Working with legal counsel	secure-neptune-server@secure-mail-server.cc
16.	水運業	2019/9/25	Re: Working with legal counsel	secure-neptune-server@secure-mail-server.cc
17.	製造業	2019/9/26	Working with legal counsel	smtp-tls-pluto@secure-smtp-host.cc
18.	製造業	2019/10/7	Working with legal counsel	secure-nexus@secure-mail-net.cc
19.	金融商品取引業	2019/10/10	Follow-up: Working with legal counsel	secure-mail-nexus@secure-mx-server.cc
20.	飲食料品卸売業	2019/10/10	Follow-up: Working With Legal Counsel	secure-mail-nexus@secure-mx-server.cc
21.	製造業	2019/10/10	Follow-up: Working with legal counsel	secure-mail-neptune@secure-mx-server.cc
22.	卸売業	2019/10/11	Working with legal counsel	secure-jupiter@mx-secure-email-host.cc
23.	総合工事業	2019/10/16	Follow-up: Liaise with external legal counsel	secure-pluto-mx@secure-mail-host.cc
24.	製造業	2019/10/16	Follow-up: Liaise with external legal counsel	secure-venus-server@secure-mail-server.cc
25.	輸送機械器具製造業	2019/10/22	Liaise with external legal counsel	secure-mars@secure-email-net.cc
26.	法律事務所	2019/10/23	[EXT] LIAISE WITH EXTERNAL LEGAL COUNSEL	secure-jupiter@secure-smtp-server.com
27.	製造業	2019/10/23	Liaise with external legal counsel	secure-pluto@secure-smtp-server.com

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
28.	化学工業	2019/10/23	Liaise with external legal counsel	smtp-neptune@secure-mail-server.cc
29.	銀行業	2019/10/24	LIAISING WITH EXTERNAL LEGAL COUNSEL	secure-mail-pluto@secure-mx-server.cc
30.	製造業	2019/10/28	Liaising with external legal counsel	secure-mars-mx@secure-mail-host.cc
31.	製造業	2019/10/28	Liaising with external legal counsel	secure-mars-mx@secure-mail-host.cc
32.	総合工事業	2019/10/30	Liaise with legal counsel	secure-neptune@secure-smtp-server.com
33.	金融商品取引業	2019/10/31	Liaise With External Legal Counsel	secure-neptune@secure-mx-server.cc
34.	製造業	2019/11/12	Liaise with external legal counsel	secure-neptune@secure-email-net.cc
35.	製造業	2019/11/12	Liaise With External Legal Counsel	secure-nexus@secure-smtp-gateway.cc
36.	製造業	2019/11/14	Liaise with external legal counsel (Follow-up)	smtp-venus@secure-mail-server.cc
37.	製造業	2019/11/14	Follow-up: Liaise with external legal counsel	smtp-nexus@secure-mail-server.cc
38.	製造業	2019/11/15	Follow-up: Liaise with external legal counsel	secure-server-neptune@secure-mail-host.cc
39.	建設業	2019/11/18	EXT: Liaise with external legal counsel	不明
40.	化学工業	2019/11/19	Liaise with external legal counsel	secure-mercury@secure-smtp-gateway.cc
41.	製造業	2019/11/25	Liaise with external legal counsel	secure-jupiter@secure-mail-provider.cc
42.	製造業	2019/11/25	Liaise with external legal counsel	secure-jupiter@secure-mail-provider.cc
43.	化学工業	2019/11/26	Liaise with external legal counsel	secure-nexus@secure-email-provider.cc
44.	製造業	2019/11/27	Liaise with external legal counsel	secure-venus@secure-server-smtp.cc
45.	化学工業	2019/12/3	Matter with legal firm	secure-uranus@secure-email-service.com
46.	製造業	2019/12/3	Matter with legal firm	secure-uranus@secure-email-service.com
47.	製造業	2019/12/4	Matter with legal firm	secure-nexus@smtp-secure-gateway.cc
48.	製造業	2019/12/4	Matter with legal firm	secure-host-mercury@mx-secure-email-host.cc
49.	製造業	2019/12/5	Matter with legal firm	secure-janus@eu-1-host-protection.cc
50.	製造業	2019/12/5	Matter with legal firm	secure-janus@eu-1-host-protection.cc
51.	会計事務所	2019/12/9	Matter with external legal firm	secure-mercury@smtp-secure-gateway.cc
52.	化学工業	2019/12/9	Matter with external legal firm	secure-mercury@smtp-secure-gateway.cc
53.	情報通信業	2019/12/16	法律事務所との事業	secure-mercury@secure-server-smtp.cc
54.	専門サービス業	2020/1/6	Liaise with legal firm	secure-uranus@secure-mail-provider.cc
55.	生産用機械器具製造業	2020/1/6	Assignment with legal firm	secure-nexus@secure-smtp-service.cc
56.	輸送機械器具製造業	2020/1/6	Assignment with legal firm	secure-nexus@secure-mx-gateway.cc
57.	水運業	2020/1/6	Assignment With Legal Firm	secure-nexus@secure-mx-gateway.cc
58.	製造業	2020/1/13	Matter with legal advisors	secure-jupiter@smtp-secure-service.cc
59.	卸売業	2020/1/14	Matter with legal advisors	secure-mercury@secure-mx-provider.cc
60.	金融商品取引業	2020/1/16	Corporate matter with law firm	secure-mars@smtp-secure-gateway.cc

項番	着信企業の業種	着信時期	件名	攻撃者が使用したメールアドレス
61.	製造業	2020/1/16	Resolve matter with law firm	secure-uranus@secure-mx-gateway.cc
62.	輸送用機械器具製造業	2020/1/16	Resolve matter with law firm	secure-uranus@secure-mx-gateway.cc

図 5 事例 3 日本語の攻撃メールの例 [7]

[7] 本件はマクニカネットワークス株式会社より情報提供をいただいた。

3.4 まとめ

ビジネスメール詐欺については、IPA より、2017 年 4 月と 2018 年 8 月にそれぞれ注意喚起を行っている。海外との取引のある国内企業にとっては特に重大な脅威であり、注意喚起のレポート公開後も、継続して J-CSIP 内外で情報提供を受けている状況で、実際に被害に遭ったという報告もある。

被害に遭わないようにするため、ビジネス関係者全体で、ビジネスメール詐欺という脅威を認識し、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。また、社内ルールを整備し、組織全体で被害を防止するという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。

4 プラント関連事業者を狙う一連の攻撃（続報）

2017 年 10 月以降、継続してプラント等の設備や部品のサプライヤーに対し、実在すると思われる開発プロジェクト名や事業者名を詐称し、プラントに使用する資機材の提案や見積もり等を依頼する内容の偽のメールを送り付け、添付ファイル（ウイルス）を開かせようとする攻撃を多数観測してきた。

偽のメールの内容は巧妙で、使われている英文には不審な点は少ない。プラントの設計・調達・建設に関わる企業や資機材等について一定の知識を持つものが作成したと思われ、無作為に個人を狙うような攻撃ではなく、プラント関連事業者を標的とした攻撃だと推測している。また、短期間で多岐にわたる文面のバリエーションが作られる一方で、J-CSIP 内の数組織で確認している限り、同等のメールの着信数はそれぞれ数通から数十通程度である。観測数が多くないという点でも、広く無差別にばらまかれているウイルスメールとは様相が異なっている。

現時点では、攻撃者の目的が知財の窃取にある（産業スパイ）ものか、あるいはビジネスメール詐欺（BEC）のような詐欺行為の準備段階のものかは不明である。もしくは、プラントの設計・調達・建設に関わるサプライチェーン全体を攻撃の対象としている可能性（セキュリティが比較的弱い可能性のある、下流の資機材メーカーを侵入の入口として狙っている可能性）もありうる。いずれにせよ、ある程度特定の組織へ執拗に攻撃が繰り返されていることから、標的型攻撃の一種とみなして取り扱っている。

4.1 攻撃の観測状況

これまで継続して確認してきた攻撃メールはいずれも英語のメールであったが、本四半期、初めて**日本語による攻撃メール**を確認した。この日本語版の攻撃メールについて、J-CSIP の参加組織へ共有したところ、J-CSIP 内では少なくとも 3 組織（全て異なる SIG）へ着信していることが分かった。また、着信日は 11 月上旬以降であったことを確認している。現時点では、英語版の攻撃メールのように複数のバリエーションが日々発生するような状況とはなっておらず、日本語版の攻撃メールは 1 パターンしか確認できていない。

なお、英語版の攻撃メールについては、理由は不明であるが、本四半期では減少傾向にあった。

4.2 日本語の攻撃メール

攻撃者から送られた日本語の攻撃メールを図 6 に示す。メールの件名・本文は、若干不自然ながら日本語で書かれている。また、メールの本文では、実在する日本の企業を騙り、発電所に関する、実在しないプロジェクトを掲げ、偽の見積もり依頼を装っている。

メールには 2 つの Excel ファイルが添付されており、いずれのファイルにも Microsoft Office の脆弱性（CVE-2017-11882）を悪用する仕掛けが施されていた。ファイルを Excel で開き、脆弱性の悪用に成功するとウイルスに感染させられる。なお、2 つのファイルのうち、1 つは動作が不完全であった。何らかの環境に依存しているか、攻撃者がミスした可能性がある。

また、この日本語の攻撃メールは、これまで観測してきた英語のプラント関連事業者を狙う一連の攻撃メールとの間で複数の関連性を確認できており、同一の攻撃者による攻撃であると判断している。

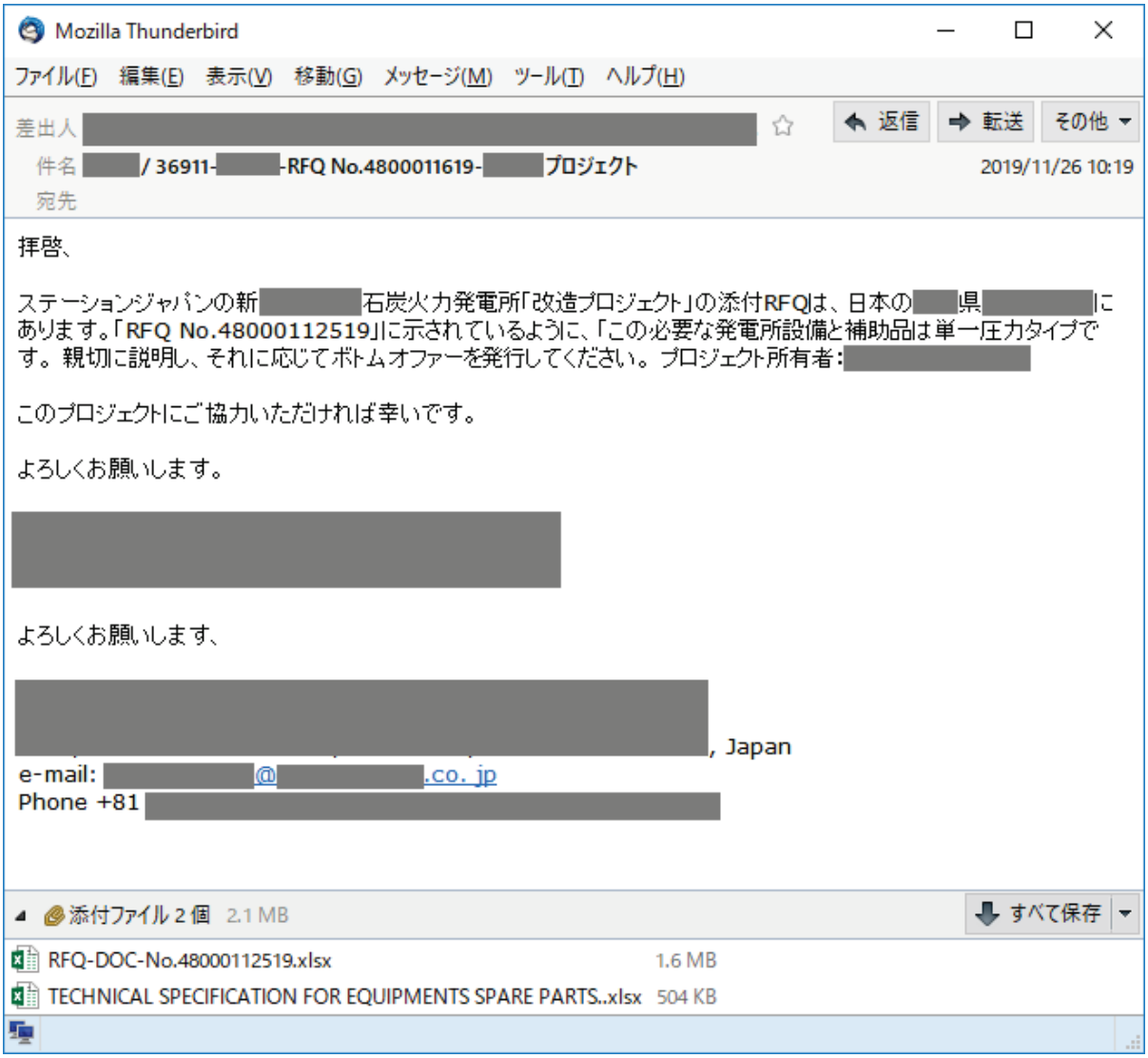

図 6 プラント関連事業者を狙う日本語の攻撃メール

4.3 まとめ

プラント関連事業者を狙う一連の攻撃について、現時点で確認できている状況を紹介した。単純な文面の提案依頼（RFP）、見積もり依頼（RFQ）、請求書等を装うウイルスメールは多種多様な事例があるが、この攻撃者は、プラントの資機材について詳細な内容の偽のメールを作成し、また、対象を絞って長期に渡り攻撃メールを送り付けてきている。攻撃対象は、無差別ではないものの、広くプラント関連事業者全般となっている可能性がある。

本四半期では攻撃メールの「日本語化」を初めて確認した。本件のような日本語の攻撃メールが、日本のプラント関連事業者、製造業等へ大量にばらまかれはじめた場合、確率は低いと考えられるが、セキュリティ製品等のすり抜け、また、ユーザによる添付ファイルの開封およびウイルスへの感染等が発生しうる。今後も引き続き、本攻撃者の動向を注視していく。

5　日本語ばらまき型メール等の動向

2015 年 10 月頃から国内で多く観測されるようになった日本語のばらまき型メールは、着信した業界等に偏りは見られず、個人・法人によらず広く無差別に、かつ継続的・大量に送信されている。日本サイバー犯罪対策センター[8]等からもばらまき型メールの注意喚起情報が定期的に発信されている。

本四半期では、Emotet と呼ばれるウイルスへの感染を狙った攻撃メールが多数観測された。他にも、Emotet とは別のウイルス感染を狙う日本語のばらまき型メールも複数観測しており、本章でこれらの攻撃メールについて説明する。

5.1 Emotet への感染を狙う攻撃メール

2019 年 9 月頃から、Emotet と呼称されるウイルスへの感染を目的とした攻撃メールが国内で多数観測されている。攻撃の状況やウイルスメールに関する情報は、JPCERT/CC[9]をはじめ、多数のセキュリティベンダ等が情報発信しており、IPA も一般へ注意を促すための解説ページを公開している [10]。

Emotet は、PC からの情報の窃取に加え、さらに他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付された文書ファイルや本文中の URL リンクを悪用する等して、継続的に感染の拡大が試みられている。

J-CSIP 内では、特に 2019 年 10 月 25 日以降、日本語による Emotet への感染を狙う攻撃メールのばらまきが再開し、かつ量が多くなったと思われたタイミングから、Emotet の情報提供が増加した。セキュリティベンダ等の情報でも国内での Emotet の攻撃の変遷について述べられているが、J-CSIP の参加組織からは次のような情報提供があり、同様の状況であった。

- 2019 年 10 月 25 日頃：正規のメールへの返信を装う手口が使われた攻撃メール
- 2019 年 11 月 12 日頃：情報提供元組織を騙った、簡単な日本語で書かれた攻撃メール
- 2019 年 11 月 28 日頃：本文中に簡単な日本語で書かれた攻撃メール
- 2019 年 11 月 29 日頃：「請求書」といった日本語の添付ファイル名が使われ、業務上開封してしまいかねないような本文の攻撃メール
- 2019 年 12 月 10 日頃から 18 日頃：本文中に不正な URL リンクを含む攻撃メール

5.2 Ursnif への感染を狙う攻撃メール

2019 年 12 月 18 日、一般に Ursnif と呼ばれるウイルスへの感染を狙う攻撃メールについて、J-CSIP 参加組織より情報提供があった。この時のメールは、Emotet の攻撃メールでも使われた、正規のメールへの返信としてウイルスを送り付けてくる手口のものであった（図 7）。

本件のメールには、パスワード付きの ZIP ファイル [11]が添付されており、添付ファイルのパスワードは本文中に記載されていた。ZIP ファイルを解凍すると、悪意のあるマクロが仕掛けられた Word 文書ファイルが得られる（図 8）。Word 文書ファイルを開き、マクロを有効化すると、不正接続先から Ursnif と呼ばれるウイル

---

[8] 一般財団法人日本サイバー犯罪対策センター（JC3）
https://www.jc3.or.jp/topics/virusmail.html

[9] マルウエア Emotet の感染に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2019/at190044.html

[10] 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（IPA）
https://www.ipa.go.jp/security/announce/20191202.html

[11] 添付ファイル名は「ATTxxxxx.zip」となっているが、これは Outlook 等、ファイル名が付いていないファイルに対して、自動的にメールソフトがつけた名前であると考えられる。

スがダウンロードされ、感染させられてしまう。

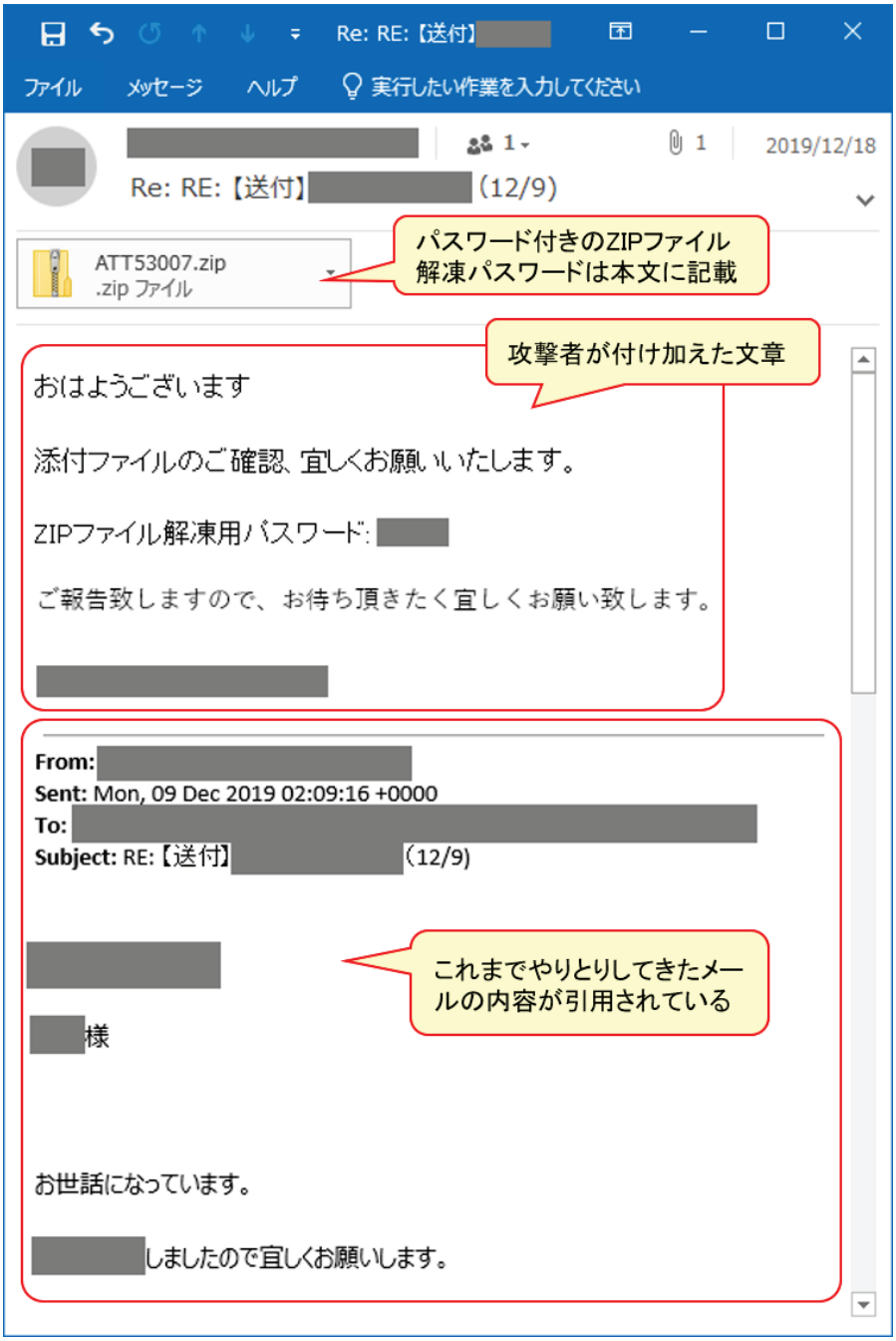

図 7 Ursnif への感染を狙う攻撃メール

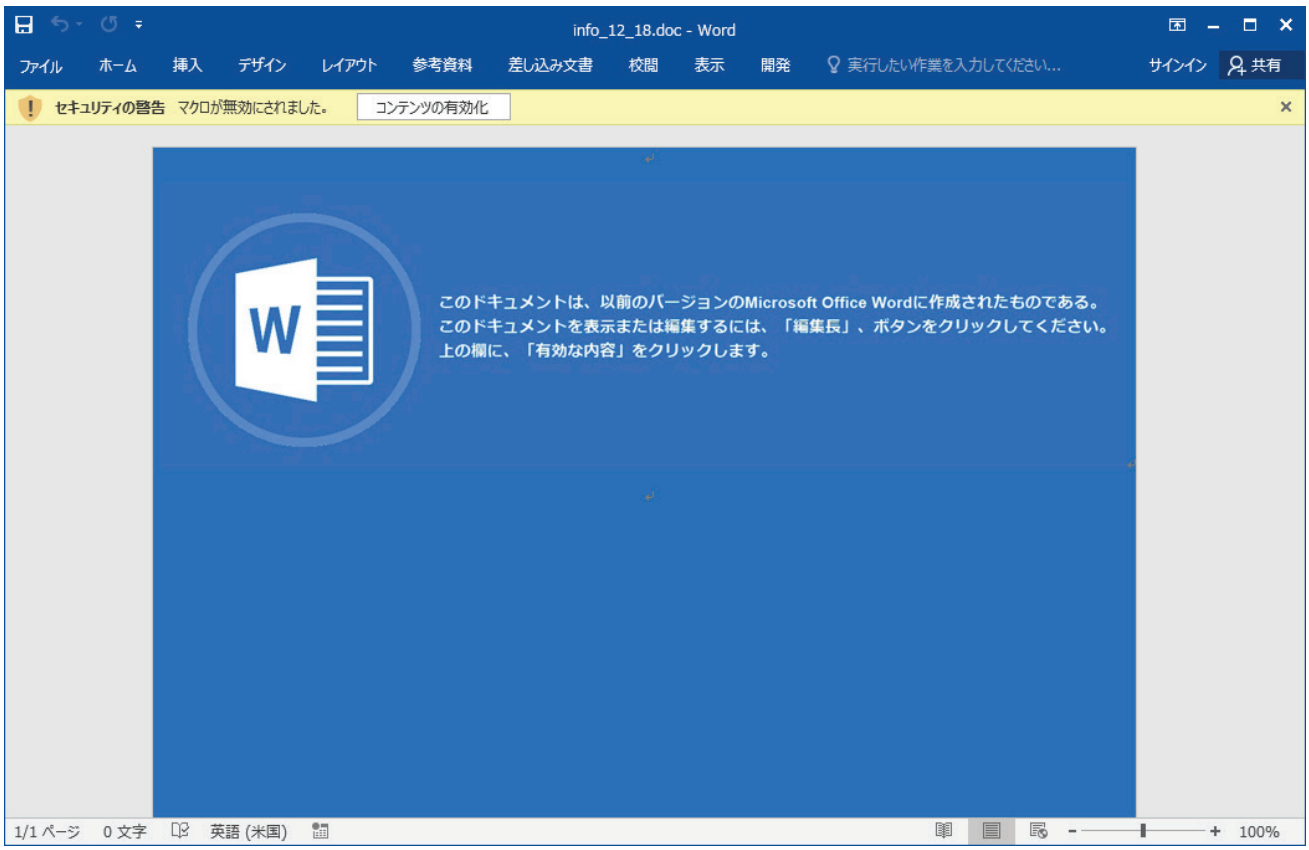

図 8 Ursnif をダウンロードするマクロを含む Word 文書ファイル

5.3 不明なウイルスへの感染を狙う攻撃メール

2019 年 12 月 3 日頃より、Emotet や Ursnif の感染を狙う攻撃メールとは別に、図 9、図 10 に示すようなウイルスメールが観測された。

メールに添付されている Excel ファイルには、悪意のあるマクロが仕掛けられており（図 11）、マクロを有効化すると、Windows のプログレスバーのような画面が表示される（図 12）。このとき、Get2 Downloader と呼ばれるウイルスが動作し、不正接続先から別のウイルスをダウンロードして感染させられるという仕組みであった。調査を実施したが、どのようなウイルスがダウンロードされるのかは不明であった。

本件について J-CSIP 内で情報共有を行ったところ、複数の組織から同様のメールが着信していたという情報提供が複数あった。数百から数千通単位で着信しているという組織もあれば、数通のみ着信があったという組織もあり、着信傾向については偏りが見られた。なお、いずれの報告についても、組織内のセキュリティ製品で検疫できており、ウイルス感染の被害はなかったとのことであった。

図 9 攻撃メールの例 1

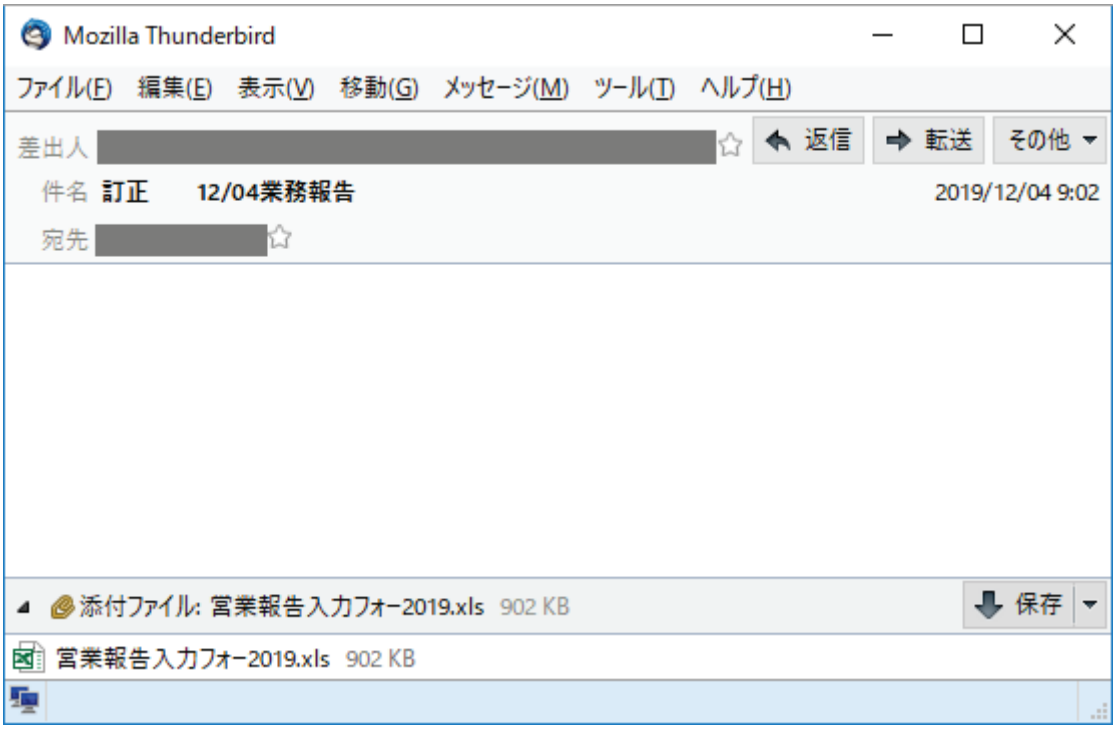

図 10 攻撃メールの例 2

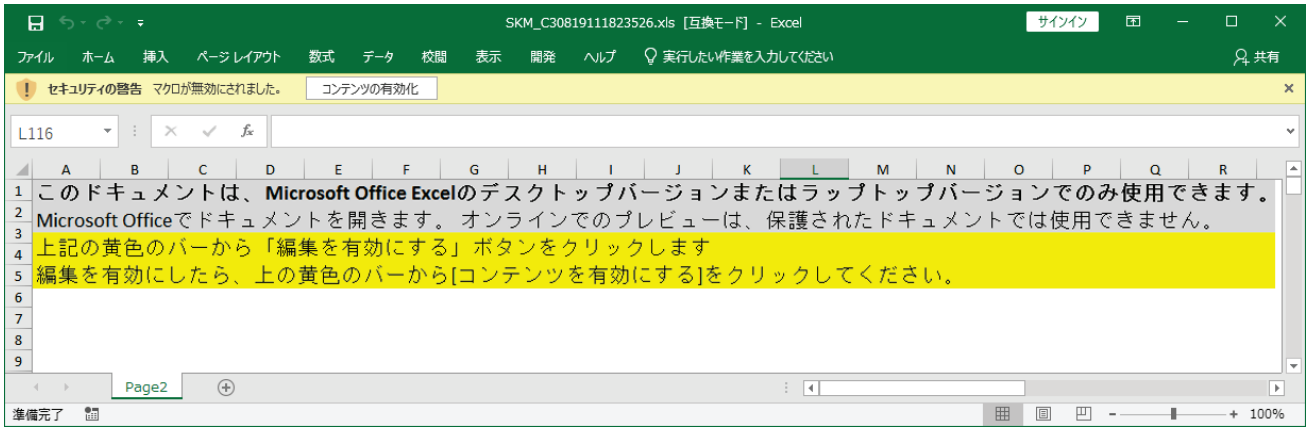

図 11 攻撃メールに添付されている Excel ファイル

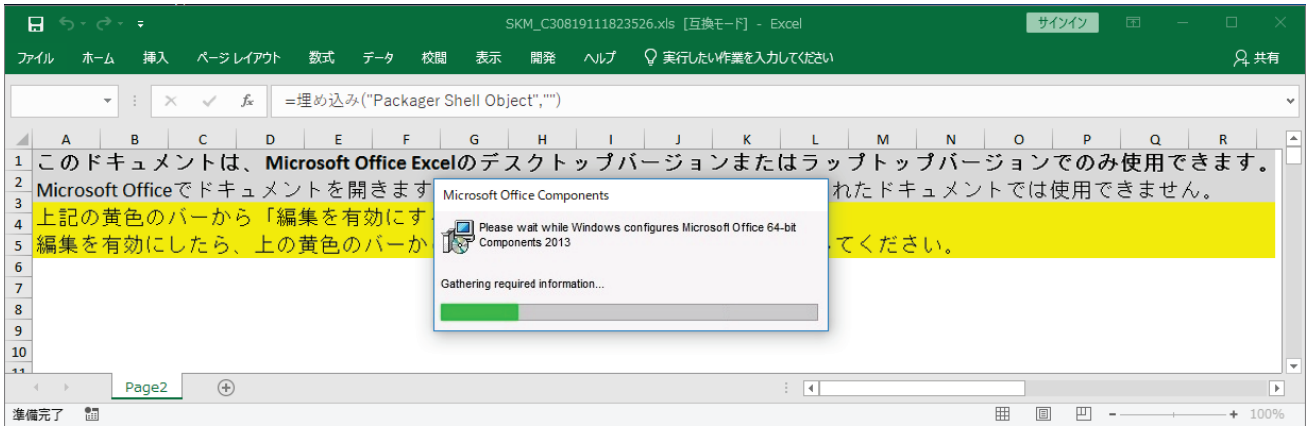

図 12 Excel ファイルのマクロを有効にした際の画面

5.4 対策

ばらまき型メールの攻撃者は、様々な手口の工夫を凝らしており、今後も今までに観測していない新たな手口で攻撃してくる可能性もある。このような攻撃をひとつの対策で防ぐことは難しく、メールフィルタリング、セキュリティソフト、メール受信者の自己防衛まで含めた総合的な対策（多層防御）を行っていくことが重要であろう。

本件の攻撃に限らず、一般的なウイルス対策（ウイルスメール対策）として、次のような対策を徹底していただきたい。

- 脆弱性の対策
  - OS やブラウザ、Office 製品等の修正プログラムを適用し、常に最新の状態にする。

- セキュリティソフトの最新化
  - セキュリティソフトの定義ファイル等を常に最新の状態にする。

- メール受信者への注意点の徹底
  - メールに添付されているファイルや、外部からダウンロードしたファイルは、安全であると判断できるもの以外は不用意に開かない。
  - ファイルを開く前に、ファイルのプロパティ等によって「ファイルの種類」を確認する。「アプリケーション」や「Script」等、文書ファイルではない形式の場合は、危険を及ぼす可能性があることに留意する。

- 文書ファイルを開いた際、マクロの有効化を求められたり、警告ウインドウが表示された場合、「はい」や「OK」といったボタンや、「編集を有効にする」や「コンテンツを有効にする」というボタンを不用意にクリックしない（表示された警告等の意味が分からない場合は操作を中断する）。
- メールに記載されている URL リンクは、安全であると判断できるもの以外は不用意にクリックしてアクセスしない。
- 少しでも不審に感じたら、組織内のシステム管理部門／セキュリティ部門／CSIRT 等へ連絡する。

無差別にばらまかれているウイルスメールといえども、詐称する組織・人、件名、文面、添付ファイル等、巧妙化が進み、一見して不審と見抜きにくくなっているものもある。システム上の対策に加え、利用者一人ひとりが注意・報告することは依然として重要であり、不審なメールが着信していることを組織内で共有できれば、組織的に被害を低減していくことができる。組織全体の問題として、攻撃の被害を避けるため、利用者からの報告を受け、同種の不審メールの着信状況を確認・対処できる体制を整えていくことが望ましい。

6　自組織を騙る偽サイト設置による詐欺事例

2018 年 11 月、J-CSIP 参加組織の正規ウェブサイトに酷似した、偽のウェブサイトが設置され、そのウェブサイトを利用した詐欺が試みられたと思われる事案について情報提供があった。その後、2019 年 9 月に偽サイトが閉鎖された。本章では、事案の発覚までの経緯と、実施した対策内容等について説明する。

本件の事案発覚までの経緯と対応内容

攻撃者は、2018 年 11 月頃、架空の企業（X 社）の社員と名乗り、海外企業（B 社）の社員に対し、何らかの詐欺と思われる勧誘行為を行った。この時、攻撃者は、X 社のウェブサイトと称して偽のサイトの URL を示し、X 社を実在する企業であると見せかけた。この X 社のウェブサイトは、国内企業 A 社の正規ウェブサイトを基に作成された、偽のサイトであった。

その後、勧誘を受けた B 社の社員が X 社へ連絡をすべく、偽のウェブサイト内に記載されていた事業所の電話番号に連絡を行ったところ、この連絡先が本物の A 社の電話番号であったため、本件偽サイトが存在すること、偽サイトを悪用した詐欺が行われている可能性があることを A 社が認識した。

これに対し、A 社は直接的な詐欺の被害に遭ったわけではないが、詐欺に巻き込まれた状態となり、次の対応を実施した。

- A 社のウェブサイトに似た偽のサイトが存在すること、またその偽サイトの特徴等に関する注意喚起を A 社のウェブサイトで公開
- ドメインやサーバの管理業者等へ、偽サイトを停止させるための調整を実施

攻撃者の意図と偽サイトの特徴

攻撃者は、X 社を実在する企業であると見せかけるため、今回の偽のウェブサイトを用意したものと考えられる。攻撃者（X 社の社員を名乗る人物）によって勧誘を受けた B 社の社員によると、次のような指示がなされていた。

- 銀行口座の情報を通知するように指示（適当な口座が無ければ、新規に口座開設するよう合わせて指示があった）
- 小切手の換金指示

攻撃者の意図は不明であるが、いわゆる資金洗浄や小切手詐欺（不正な小切手を相手に送り付け、換金させて攻撃者の口座へ入金させる手口）を目的としていた可能性が考えられる。

また、攻撃に使われた偽サイトは、A 社の正規ウェブサイトのコンテンツをコピーしたもので、全体の見た目、サイト内のリンクをクリックした際の画面遷移、日本語版と英語版のページがある点など、A 社の正規のウェブサイトに酷似していた。本件の偽サイトについては、過去、類似する事例で IPA から公開したもの [12]と同一の外観であり、同一の攻撃者によるものと考えている。

---

[12] サイバー情報共有イニシアティブ（J-CSIP）運用状況[2019 年 1 月～3 月]（IPA）
https://www.ipa.go.jp/files/000073456.pdf

偽サイトを停止させるための調整

A 社は、偽サイトを停止させるため、次の機関・団体へ連絡し、ドメインやウェブサイトの停止を試みた。

- ◆ 偽サイトで使われているドメイン名の管理業者（レジストラ）
- ◆ 偽サイトが稼働している IP アドレスの管理業者（ホスティング等の業者）

しかし、これらの管理業者等からは応答・対策の連絡が無く、長期間、偽サイトが稼働してしまうこととなった。最終的に、2019 年 9 月、偽サイトへアクセスできなくなっていることを確認した（アカウントが停止された旨の文章が表示される状態となっていた）が、偽サイトは、2018 年 11 月～2019 年 9 月 までの約 10 か月間、稼働していたことになる。

上記の管理業者等から A 社へは最後まで連絡が無かったため、偽サイトが閉鎖した理由は不明である。不正だと判断されたのではなく、単に攻撃者がアカウントを放置し、凍結された可能性等も考えられる。

本事例では、偽サイトで使われているドメイン名や IP アドレスの管理業者に連絡して、停止措置を行ったが、どのような調整が最も効果的であるかは、状況により異なるものと考えられる。同様の事案が発生した際には、上記のように、可能な範囲で関係機関・団体へ並行して調整を行うことを検討する意義はあるものと考えられる。

7　インフルエンザを題材としたフィッシングメール

本四半期、実在する国内の組織に似通った名前の組織を騙り、インフルエンザウイルスに関する偽の内容が書かれた不審なメールが国内の複数の利用者に着信している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と思われるフィッシングメールとフィッシングサイトについて説明する。

攻撃者から送信されたフィッシングメール（図 13）は、インフルエンザの無料ワクチンの提供のため、認定証を取得してほしいと騙り、フィッシングサイトへの URL をクリックさせるように誘導する内容が、日本語で書かれていた。この URL をクリックすると、不正なウェブサイトへ誘導させられる。この不正なウェブサイトは、メールの内容とは無関係の、いわゆる当選詐欺のウェブページが設置されており、利用者へ銀行口座に関する情報（銀行名、支店名、口座番号、氏名）を入力させ、詐取するものであった（図 14）。

メールの差出人表示名や本文は同一であるが、不正なウェブサイトの URL は多数のパターンが存在することを確認している。また、件名も、末尾の数字が異なる等、複数のパターンが存在することを確認している。本メールがどの程度広くばらまかれたものかは、不明である。

なお、本件のメールについては、その痕跡から、少なくとも 2019 年 3 月頃から、日本国内を対象に当選詐欺や出会い系詐欺を試みている攻撃者によるものと推定している。

フィッシング詐欺への対策は、利用者ひとりひとりが、このような攻撃手口があるということを知り、騙されないように注意し、偽のウェブサイトで情報を入力しないことが重要である。また、フィッシングメール等の不審なメールへの注意力も高めておくことが必要であろう。

Subject: 口優遇措置のおしらせ-●●-●●-

特定の地域にお住いの方だけに配信しております。

●●●●担当の●●と申します。

あなたのお住まいの地域やその近隣でインフルエンザが流行しております。

政府により「ウイルス警戒地域」に認定されました。

他の方々にも伝染してしまう病であるだけに、選ばれた地域の方は無料でワクチンを提供させて頂く事が可能です。

下記のURLより認定証を取得して頂き、お近くの医療機関へご提示してください。

【本文中のURLリンク】

図 13 フィッシングメールの内容

図 14 メールから誘導されるフィッシングサイト

8 解凍ファイルが変わる不正 ZIP ファイルを使った攻撃

本四半期、解凍するアーカイバ（圧縮・解凍ソフト）によって、解凍されるファイルが異なるという細工が施されたZIPファイルが添付された不審メールについて情報提供があった。本章では、この攻撃の手口について説明する。

攻撃者から送られてくるメール（図 15）は、現時点で英語のメールのみ確認している。このメールに添付されたZIPファイルは、**内部に2つのファイルを含んでおり、解凍時に出力されるファイルが、そのどちらか”片方のみ”となるように細工されている**（図 16）。本件の手口については、2019 年 11 月 5 日に、Trustwave 社から情報が公開されており、「Double Loaded Zip File」と呼ばれている [13]。補足情報として、当該不正ファイルについて、IPA で検証した各種アーカイバの挙動 [14]を表 5 に示す。

本攻撃の注意点としては、次の 2 点が考えられる。

1 点目として、本手口が使われた攻撃メールが送られた場合、メールゲートウェイで実行する検査においては、無害なファイルが含まれていると判定されるか、ZIP ファイルが壊れているかのように処理され、検知（検査）されない可能性がある。そのため、メールが利用者へ配送され、利用者の手元ではウイルスファイルが解凍されてしまう（使用しているアーカイバによる）というシナリオが考えられる。

2 点目として、この不審なZIPファイルを何らかの方法で発見したとして、システム管理部門で調査のため解凍した結果と、利用者の端末で（利用者の使用ソフトで）解凍した結果が異なる可能性がある。例えば、システム管理部門の環境では無害なファイルが出力されるが、利用者の環境ではウイルスファイルが出力されるといった状況になりうる。ZIP ファイルにこのような細工を施すことが可能であると認識していない場合、意思疎通や調査・インシデント対応に混乱が生じる可能性がある。

これらの問題は、メールの添付だけではなく、ウェブサイトからダウンロードする ZIP ファイルでも同様の状況となりうる。また、本事例では、無害な画像ファイルとウイルス [15]（exe 形式の実行ファイル）の組み合わせであったが、あえて両方とも同じ見た目の文書ファイルとし、片方のみウイルスへ感染させる細工を施すといった手口にも応用が可能である。この場合、環境により、同じ見た目で動作が異なるファイルが出力されることとなり、調査・インシデント対応に際し、より混乱が生じる可能性が高い、注意を要する攻撃となると思われる。

---

[13] Double Loaded Zip File Delivers Nanocore (Trustwave)
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/double-loaded-zip-file-delivers-nanocore/

[14] 本検証結果は、あくまでも今回検証に使用した ZIP ファイルにおける結果であり、解凍ソフトのバージョンや使用する ZIP ファイルによっては必ずしも同じ結果になるとは限らない。

[15] 本事例では、Nanocore と呼称される遠隔操作ウイルス（RAT）が出力される。

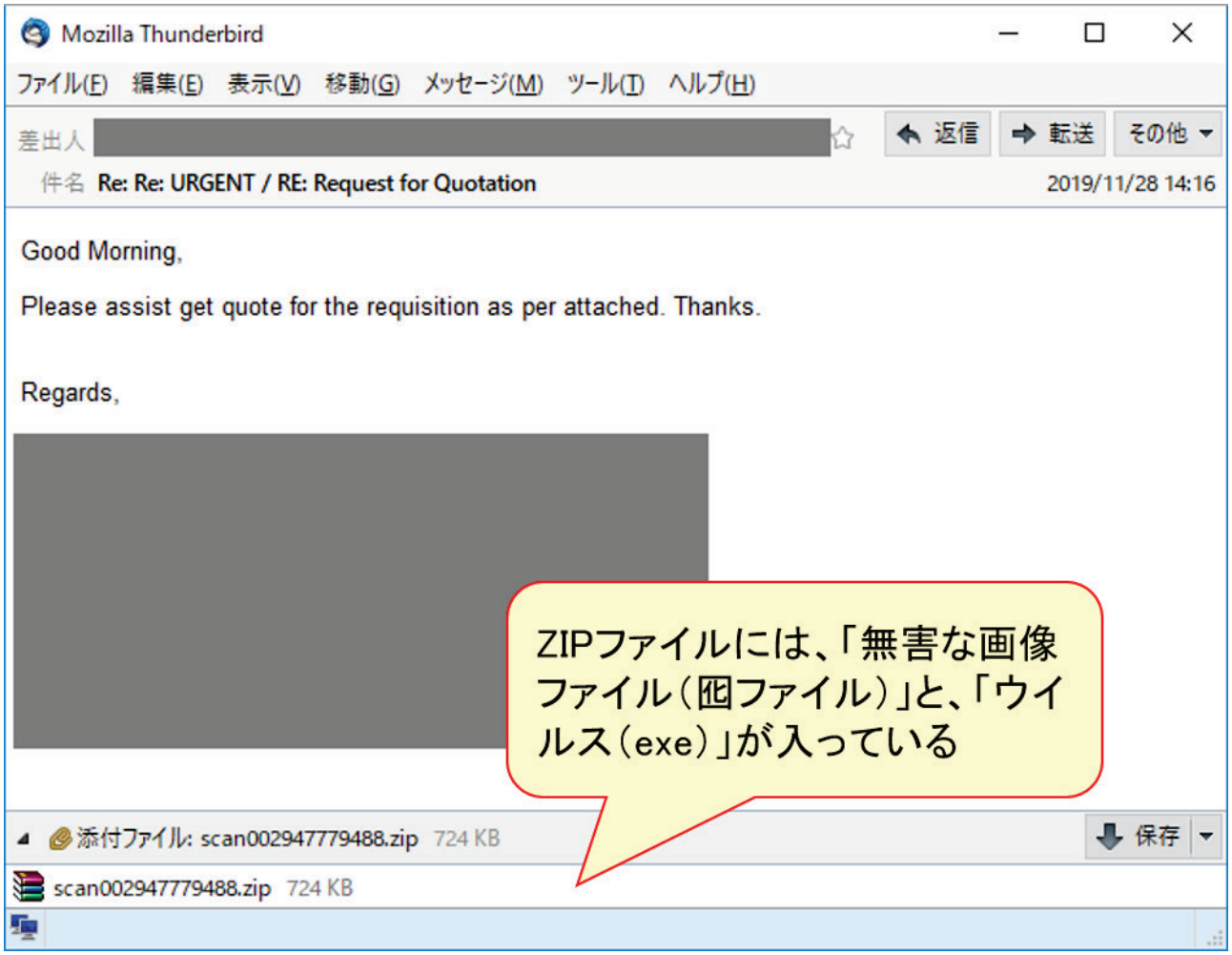
Mozilla Thunderbird
ファイル(F) 編集(E) 表示(V) 移動(G) メッセージ(M) ツール(T) ヘルプ(H)
差出人
返信
転送
その他
件名 Re: Re: URGENT / RE: Request for Quotation
2019/11/28 14:16
Good Morning,
Please assist get quote for the requisition as per attached. Thanks.
Regards,
ZIPファイルには、「無害な画像ファイル（囮ファイル）」と、「ウイルス（exe）」が入っている
添付ファイル: scan002947779488.zip 724 KB
保存
scan002947779488.zip 724 KB

図 15 攻撃メールの例

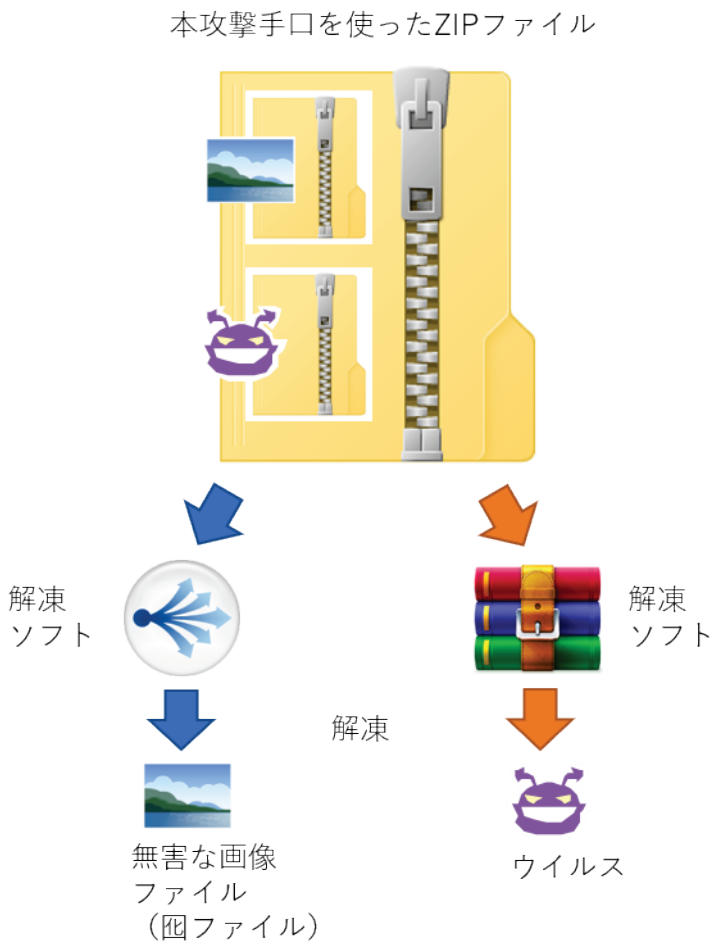

図 16 攻撃手口のイメージ

表 5 アーカイバごとの検証結果

項番	アーカイバとバージョン	エラー	出力されるファイル
1.	Windows 標準の解凍ソフトウェア(Windows 7/10)	発生	なし
2.	Lhaplus (1.74)	発生	画像ファイル
3.	WinRAR (5.71)		ウイルス
4.	WinRAR (5.80 bata3)		ウイルス
5.	7zip (9.20)		ウイルス
6.	7zip (19. 00)		画像ファイル
7.	Explzh (7.89)		なし
8.	LhaForge (1.6.7)	発生	なし
9.	+Lhaca (0.76)		ウイルス
10.	Lhaz (2.5.1)		ウイルス
11.	PeaZip (6.9.2)		画像ファイル
12.	PowerArchiver 2019 (19.00.57)		ウイルス

※ 項番 2 は、画面にエラーが表示されながらも、ファイルの解凍（出力）は行われるという動作である。

9　OLE 機能を悪用した文書ファイルの手口（続報）

2019 年 4 月、Microsoft Word の OLE（Object Linking and Embedding）機能を悪用し、悪意のあるマクロを埋め込んだ Word 文書ファイルが添付された英語の攻撃メールについて確認した。その後、2019 年 11 月、日本語のメールで本手口が使われた攻撃メールの情報を入手した。なお、IPA で確認できている範囲では、英語のメールで、国内への攻撃に使用されていることは確認できているが、日本語のメールが国内への攻撃に使用されたことを示す情報は確認していない。

本手口については、2019 年 7 月に IPA より公開[16]していたが、日本語のメールが確認されたため、本書の参考資料として更新版を公開することとした[17]。

攻撃メールや手口の特徴、ウイルス感染を防ぐため利用者が選択するべき操作について広く周知することが重要であると考える。必要に応じ、参考資料を活用していただきたい。

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

---

[16] サイバー情報共有イニシアティブ（J-CSIP）運用状況[2019 年 4 月～6 月]（IPA）
https://www.ipa.go.jp/files/000076713.pdf
[17] 【参考資料】OLE 機能を悪用した文書ファイルの手口に関する注意点（第二版）