サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2020 年 1 月～3 月]

2020 年 4 月 30 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、2020 年 3 月末時点の運用体制、2020 年 1 月～3 月の運用状況を報告する。1 章、2 章は全体状況を、3 章は 2019 年度の活動状況、4 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

2020 年 1 月～3 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）。

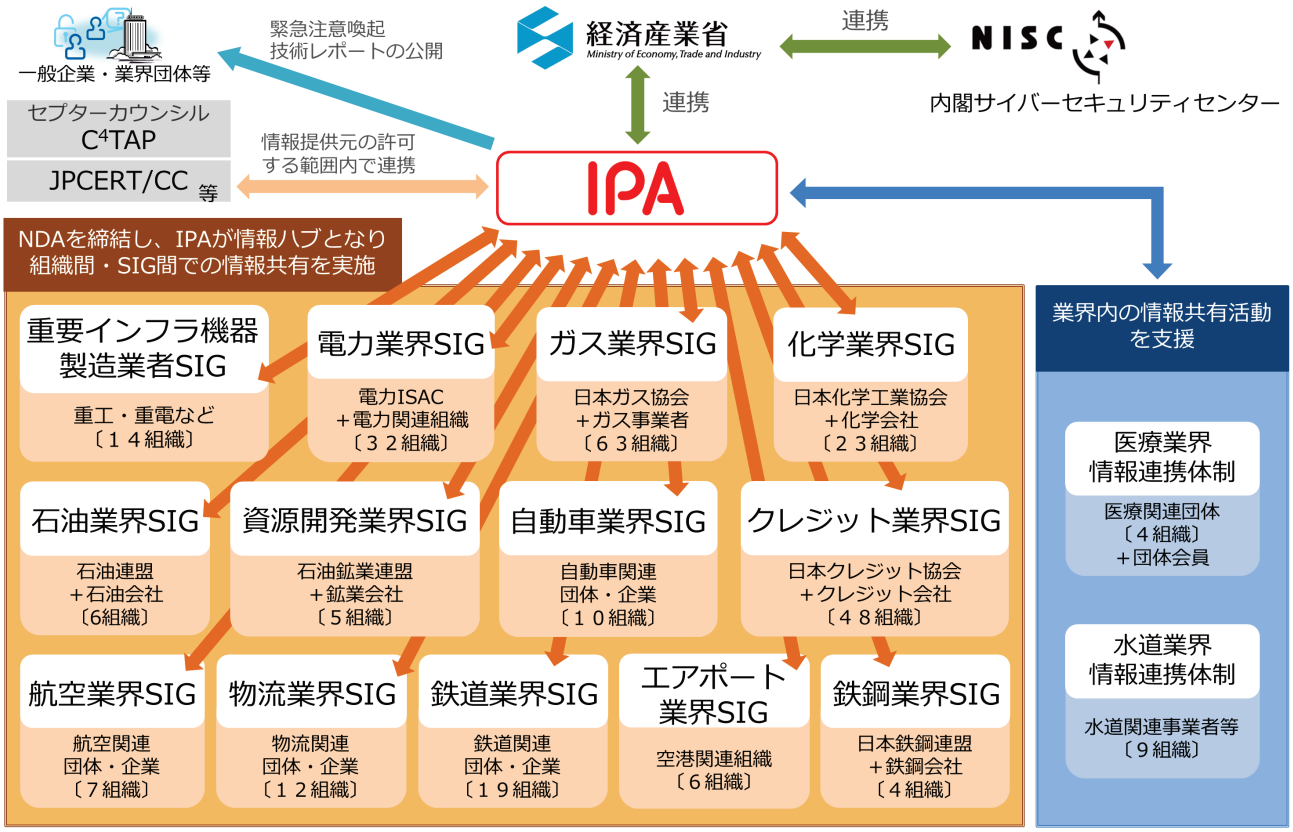

図 1 J-CSIP の体制図

[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（2020 年 1 月～3 月）

2020 年 1 月～3 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（3 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			2020 年
		4 月～6 月	7 月～9 月	10 月～12 月	1 月～3 月
1	IPA への情報提供件数	424 件	235 件	1,042 件	**602 件**
2	参加組織への情報共有実施件数※1	54 件	75 件	40 件	**56 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 **37 件**を含む。

本四半期は情報提供件数が **602 件**であり、うち標的型攻撃メールとみなした情報は **166 件**であった。提供された情報の主なものとして、実在するある日本の企業を騙ったウイルスメールが多数着信したという情報提供がおよそ 2 割を占めている（下記、相談・報告事例の項番 1）。

また、前四半期で多数観測されていた Emotet への感染を狙うウイルスメールについて、2020 年 2 月上旬頃までは観測されていたが、以降情報提供はなかった。なお、2020 年 1 月末には、新型コロナウイルス感染症（COVID-19）を題材とした Emotet への感染を狙うウイルスメールが一時的に観測され、IPA から情報を公開[3]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。

- 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 4 章で詳しく述べる。

- オープンソースのペネトレーションツールを悪用した攻撃について情報提供があった。この時悪用されたツールは、攻撃者によって特定の時間にのみ不正通信を行うように細工されていた。これについては、5 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、国内組織の海外関係企業のメールアカウントを攻撃者が乗っ取り、複数の組織へ Office 365 等のアカウント情報を詐取するためのフィシングメールが送られたという事例を確認した。これについては、6 章で述べる。

[3] 「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

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	実在する日本の企業を騙るウイルスメールが着信した。	2 件
2	問い合わせフォームが悪用され、大量のメールが着信した。	1 件
3	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。	9 件

項番 1 は、実在する日本のある企業を騙るウイルスメールが着信したという情報提供である。悪意のある者によって、実在する組織が騙られ、攻撃メールが送られてくるというケースは特にめずらしい事象ではない。ただ、この例では数百通が着信したとも報告されており、そういった事象が自組織で実際に発生し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、情報提供元とは別の正規の企業のウェブ上の問い合わせフォームを攻撃者に悪用され、その自動応答メールが大量に着信したという情報提供であった。これが単なる嫌がらせであるのか定かではないが、攻撃者は、問い合わせ元（連絡先）として、被害組織のメールアドレスをフォームに入力した（それを大量に投稿した）ということである。このような場合、メールを受信する側での対策は難しいが、同様の手口で自社の問い合わせフォームを悪用されてしまう可能性を考慮し、短時間に一定回数以上の入力があった場合にはアクセス制限を設けるといった対策を検討してもよいと考えられる。

項番 3 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。

[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　今年度の状況

3.1 今年度の取り扱い件数と年度ごとの推移状況

J-CSIP における取り扱い件数（情報提供件数、標的型攻撃と見なした件数、情報共有件数）と参加組織数について、今年度（2019 年度）の合計と、J-CSIP を運用開始した 2012 年度から 2018 年度までの推移状況を次に示す（表 3、図 2）。

表 3 年間の取り扱い件数と参加組織数

項目	IPA への 情報提供件数	標的型攻撃メールと 見なした件数	参加組織への 情報共有実施件数	参加組織数
2012 年度	246	201	160	5 業界 39 組織
2013 年度	385	233	180	5 業界 46 組織
2014 年度	626	505	195	6 業界 59 組織
2015 年度	1,092	97	133	7 業界 72 組織
2016 年度	2,505	177	96	7 業界 86 組織
2017 年度	3,456	274	242	11 業界 228 組織
2018 年度	2,020	213	195	13 業界 249 組織 ＋ 2 情報連携体制 13 組織
2019 年度	2,303	401	225	13 業界 249 組織 ＋ 2 情報連携体制 13 組織

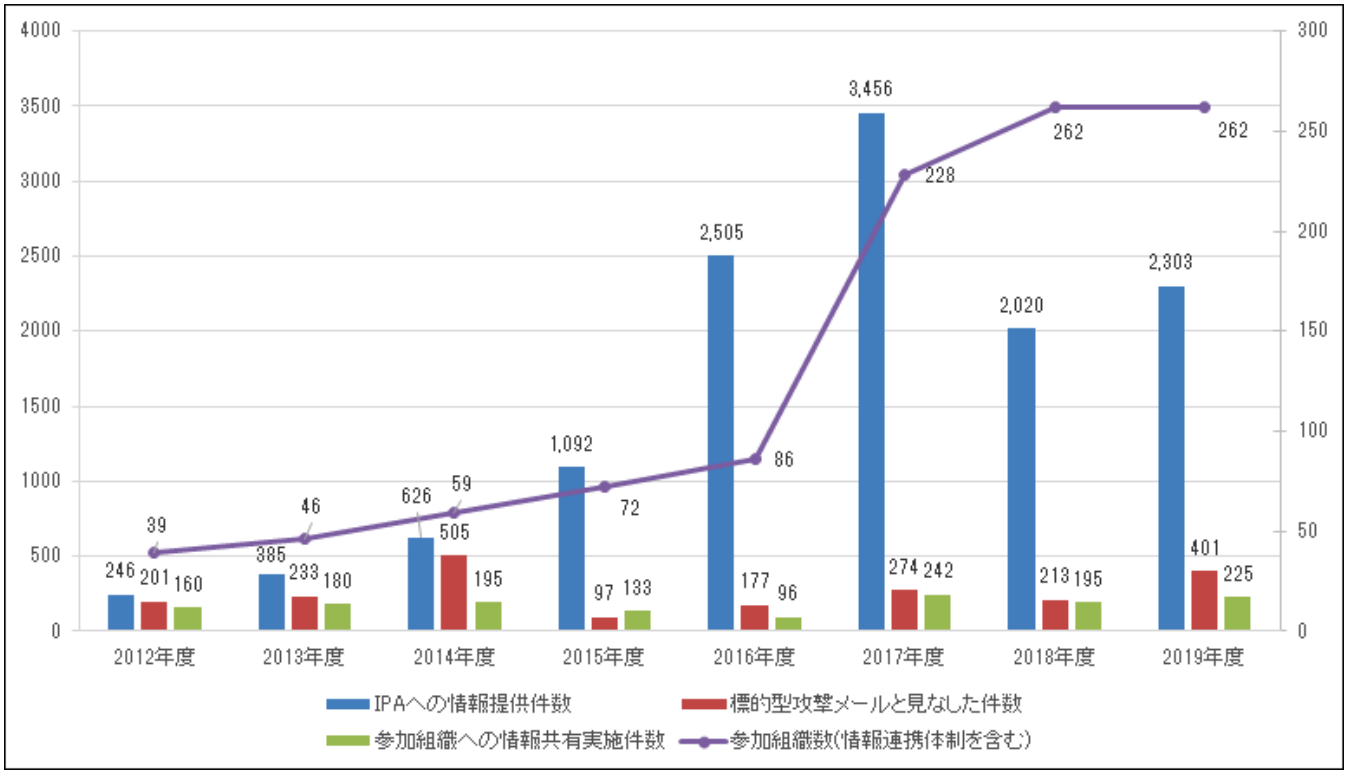

図 2 年間の取り扱い件数と参加組織数の推移

3.2 今年度の活動

2019 年度は、J-CSIP の参加組織数について、年度内での増減はあったものの、最終的な参加組織数は 2018 年度から変化はなかった。

情報提供について、特に、2018 年度から継続してビジネスメール詐欺が試みられたという情報提供が続いている。これらの中には、2019 年 7 月から国内外の多数の組織へ行われたものと推測される CEO を騙る一連の攻撃メールもある。ビジネスメール詐欺の事例については、四半期毎の運用状況レポートで詳細を記載している。

また、2017 年の 10 月頃から観測している、プラント関連事業者を狙う英文の攻撃メールについて、2019 年 11 月、日本語の攻撃メールを初観測した。一連の攻撃メールの内容は常に変化を続けており、特定の宛先に対して執拗に攻撃が行われている傾向があるため、これらのメールは標的型攻撃として取り扱っている。この一連の攻撃メールは現時点でも継続しており、今後も動向を注視していく。

2016 年度まで観測されてきたような、日本国内の特定の業界や組織を狙う標的型攻撃メールについては、J-CSIP 参加組織の中での提供件数は減少傾向にある。一方、攻撃の発端がメールであるか否かは不明だが、オープンソースのツールを悪用する標的型攻撃の事例等を確認しており、日本国内全体として見ると標的型攻撃は依然として継続している状況と考えられ、引き続き注意が必要である。

3.3 特筆事項

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日本国内で多数観測された。攻撃の状況やウイルスメールに関する情報は、JPCERT/CC[5]をはじめとして、多数のセキュリティベンダから情報が発信されている。IPA でも一般へ注意を促すため Emotet の攻撃メールや手口について解説ページを公開した。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型メールが再開し、ばらまかれる量が多くなったと考えられるタイミングから、情報提供が増加した。Emotet への感染を狙う攻撃メールの題材として、12 月頃には賞与関係を装うメールが観測され、2020 年に入ってからは、新型コロナウイルス感染症（COVID-19）に関連したものも確認された。Emotet の攻撃メールに限らず、時節に則った題材を用いる攻撃メールは多数存在する。Emotet の攻撃メールは、2020 年 2 月以降、J-CSIP 内では観測されていないが、今後この攻撃が再開することも考えられるため、基本的なウイルスメール対策を徹底することが必要であろう。

その他、単純な金銭目的とは異なる、Office 365 等のアカウント情報を狙うフィッシング攻撃も継続して情報提供されている。J-CSIP では、標的型攻撃に限らず、今後もこれらサイバー攻撃全般の情報共有を進めていく予定である。

---

[5] 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

4　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。

なお、2020 年 4 月 27 日にも、日本語の偽メールの事例や、新型コロナウイルス感染症の話題を書き出しとする事例等を含めた注意喚起を公開した[6]ため、そちらも参照していただきたい。

ビジネスメール詐欺の被害に遭わないようにするため、ビジネス関係者全体で、この脅威を認識し、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。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。

本四半期は、J-CSIP の参加組織から 35 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、1 件はタイプ 1（取引先へのなりすまし）の攻撃で、残りの 34 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 1 件のビジネスメール詐欺の情報提供があった。

本章では、開示許可の得られたタイプ 1 の事例について詳しく説明する。また、2019 年 10 月～12 月期にも観測していた、複数組織へ行われた CEO を詐称する一連の攻撃について、本四半期でも継続して確認されたため、あわせて説明する。

[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）
http://www.ipa.go.jp/security/announce/2020-bec.html

4.1 事例 1 海外グループ企業を狙った攻撃

本事例は、2020 年 1 月、J-CSIP の参加組織（国内企業）の海外グループ企業（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、B 社の担当者になりすました攻撃者から、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。

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、偽の口座への送金にまで至ったものの、A 社の担当者が詐欺に気づき、銀行へ交渉したところ、送金の取り消しを行うことができたため、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) 請求書の修正を装い偽の口座を連絡する

(2) 詐称用ドメインの取得と悪用

(1) 請求書の修正を装い偽の口座を連絡する

本事例は、A 社（国内企業の海外グループ企業）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取りを行っている中発生した。2020 年 1 月 7 日、B 社担当者から A 社担当者へ、正規の請求書のメールが送られた。その翌日（1 月 8 日）、攻撃者から、「修正版の請求書を送る」と称し、偽の口座への送金を要求するメールが A 社担当者へ送り付けられた。この時の攻撃者からのメールは、1 月 7 日に B 社担当者が送ったメールの内容を引用し、返信する形となっていた。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。

1 月 9 日、A 社担当者は、攻撃者から送られてきたメールを不審とは思わず、請求書の内容を確認。請求書の日付が誤っていたため、その旨を攻撃者へ返信した。すると、攻撃者から「入力ミスのため、修正した請求書を送る」という旨のメールが A 社担当者へ着信した。同じ日に、攻撃者は A 社にもなりすまし、B 社の担当者宛に、「仮支払日は 1 月 16 日になる予定である」という旨のメールを送っている。攻撃者は、当面の間、B 社の担当者が A 社側へ連絡を取らないように誘導し、詐欺の発覚を遅らせようとしたものと考えられる。

攻撃にかかるメールのやりとり（前半）を図 3 に示す。

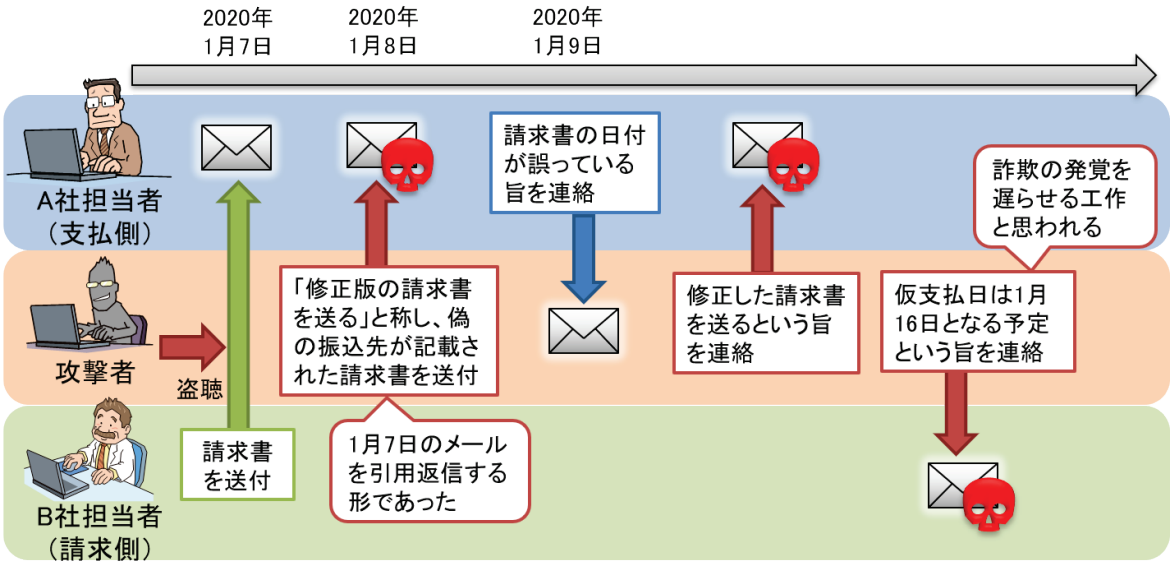

図 3 事例 1 攻撃者とのやりとり（前半／2020 年 1 月 7 日～1 月 9 日まで）

1 月 13 日、A 社担当者から攻撃者へ、請求書の口座が修正前後で異なっていることを指摘する旨のメールを送ったところ、攻撃者から「修正版の請求書が正しい」という回答があった。その後、A 社担当者は、攻撃者の指定した偽の口座への送金を行った。ビジネスメール詐欺では、本件のように、請求書等に記載された口座情報が、攻撃者によって改変されている手口が多くみられる。A 社担当者は、請求書の口座情報が異なっていることに気づいたこのタイミングで、不審だと見抜けた可能性はあるが、結果として偽のメールであると気づくことはできなかった。

1 月 15 日、攻撃者から A 社担当者へ、「支払伝票を送付してほしい」というメールが着信したため、A 社担当者は攻撃者へ、支払伝票を送付している。

1 月 16 日、本物の B 社担当者から A 社の担当者へ、支払い状況を問い合わせるメールが着信した。本物の B 社からの連絡がこの日となったのは、攻撃者が送った「仮支払日は 1 月 16 日」という偽メールによる時間稼ぎが成功したものとみられる。その後、支払い状況を確認するやり取りの中で、偽のメールが送られていることに気づき、送金先の口座が偽物であるということが発覚した。

その後、A 社は速やかに銀行へ送金の取り消し依頼を実施。銀行の担当者が、送金先の銀行と交渉を行った結果、送金の取り消しを行うことができたため、金銭的な被害には至らなかった。

攻撃にかかるメールのやりとり（後半）を図 4 に示す。

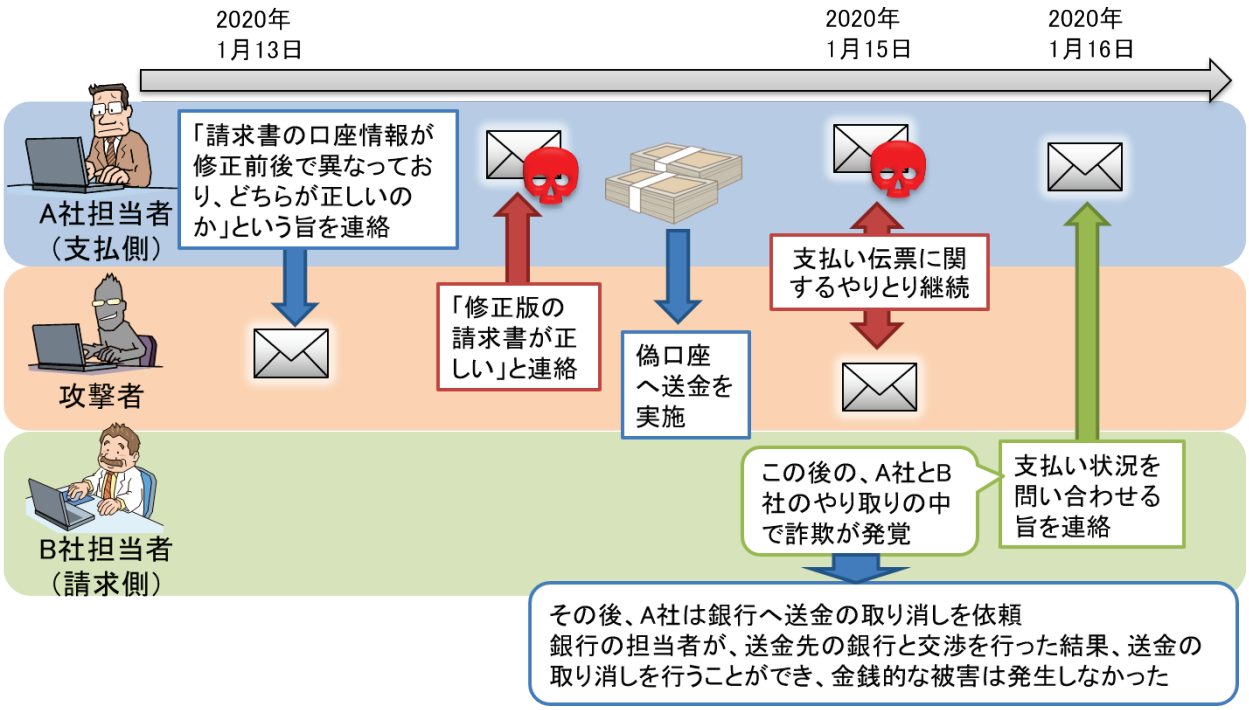

図 4 事例 1 攻撃者とのやりとり（後半／2020 年 1 月 13 日～16 日まで）

（2） 詐称用ドメインの取得と悪用

攻撃者は A 社と B 社の正規の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。

- A 社の詐称用ドメインの例（B 社へ送られたメールで使われたドメインの例）

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

※実際に悪用されたものとは異なる。

- B 社の詐称用ドメインの例（A 社へ送られたメールで使われたドメインの例）

【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。

4.2 事例 2 複数組織へ行われた CEO を詐称する一連の攻撃（続報）

2019 年 10 月以降、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たなりすましメールについて、前四半期と同様、継続して情報提供があった。また、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新たに **46** 件（前四半期は 62 件）の類似するメール検体を入手するに至った [7]。

これらのメールは次に示す点が共通しており、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る。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おり、「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」の 2.3 章 事例 3 も、この一連の攻撃の一部である。

- 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。
  - 2020 年 3 月 26 日に着信したメールのみ、「secure」という単語は使われていなかったが、その他の特徴は一致していた。また、このメール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として使用していた [8]。
- これまで確認した一連の攻撃メールの件名や本文はほぼ英文であり、日本語のメールは 2 件 [9]、スペイン語のメールは 1 件確認している。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 3 月 26 日である。

本四半期に IPA で確認したメールの情報の一覧を、表 4 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、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。

---

[7] 本事例については、本レポート執筆時点である 2020 年 4 月 6 日までの情報で記載している。

[8] 本件のメールについては「ビジネスメール詐欺「BEC」に関する事例と注意喚起（第三報）」で紹介している。
http://www.ipa.go.jp/security/announce/2020-bec.html

[9] 日本語のメールについては、表 4 の項番 23 と、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]に記載しているメール例の 2 件である。

表 4 事例 2 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.	化学工業	2019/9/13	LIAISING WITH EXTERNAL LEGAL COUNSEL	secure-jupiter-server@secure-smtp-host.cc
2.	化学工業	2019/9/13	LIAISING WITH EXTERNAL LEGAL COUNSEL	secure-jupiter-server@secure-smtp-host.cc
3.	化学工業	2019/9/13	LIAISING WITH EXTERNAL LEGAL COUNSEL	secure-jupiter-server@secure-smtp-host.cc
4.	化学工業	2019/9/13	LIAISING WITH EXTERNAL LEGAL COUNSEL	secure-jupiter-server@secure-smtp-host.cc
5.	化学工業	2019/9/13	LIAISING WITH EXTERNAL LEGAL COUNSEL	secure-jupiter-server@secure-smtp-host.cc
6.	化学工業	2019/9/13	Liaising with external legal counsel	不明
7.	化学工業	2019/10/16	Follow-up: Liaise with external legal counsel	secure-venus-server@secure-mail-server.cc
8.	化学工業	2019/10/16	Follow-up: Liaise with external legal counsel	secure-venus-server@secure-mail-server.cc
9.	化学工業	2019/10/22	Follow-up: Liaise with external legal counsel	secure-mercury@secure-mx-host.cc
10.	化学工業	2019/10/22	Follow-up: Liaise with external legal counsel	secure-mercury@secure-mx-host.cc
11.	化学工業	2019/10/22	Follow-up: Liaise with external legal counsel	secure-mercury@secure-mx-host.cc
12.	電気機械器具製造業	2019/10/30	Working with legal counsel	不明
13.	化学工業	2019/11/14	Follow-up: Liaise with external legal counsel	secure-server-saturn@secure-mail-host.cc
14.	化学工業	2019/11/14	Follow-up: Liaise with external legal counsel	smtp-nexus@secure-mail-server.cc
15.	化学工業	2019/11/14	Follow-up: Liaise with external legal counsel	smtp-nexus@secure-mail-server.cc
16.	化学工業	2019/11/14	Follow-up: Liaise with external legal counsel	smtp-nexus@secure-mail-server.cc
17.	化学工業	2019/11/14	Liaise with external legal counsel (Follow-up)	smtp-venus@secure-mail-server.cc
18.	化学工業	2019/11/26	Liaise with external legal counsel	secure-nexus@secure-email-provider.cc
19.	製造業	2019/11/27	Liaise with external legal counsel	secure-venus@secure-server-smtp.cc
20.	輸送用機械器具製造業	2019/12/5	Matter with legal firm	secure-janus@eu-1-host-protection.cc
21.	化学工業	2019/12/9	Matter with external legal firm	secure-mercury@smtp-secure-gateway.cc
22.	産業用電気機械器具製造業	2019/12/9	Matter with legal firm	不明

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
23.	製造業	2019/12/16	法律事務所との事業	secure-mercury@secure-server-smtp.cc
24.	輸送用機械器具製造業	2019/12/16	Matter with legal firm	不明
25.	専門サービス業	2020/1/8	Matter with law firm	secure-neptune@encrypted-network.cc
26.	電気機械器具製造業	2020/1/13	EXTERNAL: Matter with legal advisors	secure-nexus@secure-smtp-provider.cc
27.	製造業	2020/1/13	Matter to resolve with law firm	secure-jupiter@smtp-secure-service.cc
28.	製造業	2020/1/13	Matter with legal advisors	secure-jupiter@smtp-secure-service.cc
29.	製造業	2020/1/13	Matter with legal advisors	secure-jupiter@smtp-secure-service.cc
30.	製造業	2020/1/13	Matter with legal advisors	secure-jupiter@smtp-secure-service.cc
31.	化学工業	2020/1/13	Matter with legal advisors	secure-jupiter@smtp-secure-service.cc
32.	産業用電気機械器具製造業	2020/1/15	Matter with law firm	不明
33.	産業用電気機械器具製造業	2020/1/16	Corporate matter	不明
34.	化学工業	2020/2/10	Law firm matter	secure-taurus@secure-smtp-service.com
35.	その他の製造業	2020/2/11	Matter with law firm	secure-taurus@secure-mx-provider.cc
36.	化学工業	2020/2/11	Matter with law firm	secure-uranus@secure-smtp-service.com
37.	化学工業	2020/2/12	Matter with law firm	secure-taurus@secure-mx-provider.cc
38.	貨物運送取扱業	2020/2/19	[EXTERNAL] Law firm matter	secure-mercury@secure-smtp-provider.cc
39.	電気･ガス･熱供給･水道業	2020/3/2	Law firm matter	secure-nexus@secure-smtp-service.com
40.	製造業	2020/3/3	[External]Law firm matter	secure-taurus@secure-mx-host.com
41.	輸送機械器具製造業	2020/3/3	Matter with law firm	secure-uranus@secure-mx-host.com
42.	電気･ガス･熱供給･水道業	2020/3/12	Law firm matter	smtp-venus@smtp-secure-gateway.cc
43.	化学工業	2020/3/12	Law firm matter	smtp-venus@smtp-secure-gateway.cc
44.	リサイクル業	2020/3/16	Corporate matter with law firm	secure-pluto@mx-gateway-host.cc
45.	情報通信業	2020/3/18	Law firm matter	secure-neptune@mx-gateway-host.cc
46.	サービス業	2020/3/26	New corporate development initiative	host-uranus@encrypted-gateway.cc

5　オープンソースのツールを悪用した攻撃

本四半期、オープンソースのペネトレーションツールを悪用した攻撃が行われたという情報提供があった。本件で使用されたツールは、実行すると端末を遠隔操作可能にする機能があり、さらに、攻撃者によって特定の時間のみ不正接続先と通信を行うように細工されていた。攻撃者は、当該ツールを遠隔操作ウイルス（RAT）として使用したものと考えられる。

本章では、攻撃者が当該ツールを悪用し、攻撃対象の端末を遠隔操作可能な状態（ウイルス感染している状態）にするために行った攻撃手口について説明する。

なお、本章で説明する内容と類似した攻撃手口について、2020 年 4 月 24 日に LAC 社から情報が公開されているため、併せて参照いただきたい [10]。

5.1 遠隔操作ウイルスを実行する攻撃の仕組み

攻撃者は次の 3 つの手口を使い、標的とした組織内の端末へ遠隔操作ウイルスを感染させたものと推測される。

- 手口 1：MSBuild の悪用
- 手口 2：タスクスケジューラの悪用
- 手口 3：DLL サーチオーダーハイジャッキングによる不正操作

なお、手口 1 と 3 は、Windows にインストールされている PowerShell を悪用するものであるが、標準でインストールされている PowerShell（PowerShell.exe）を使用することなく、悪意のある PowerShell スクリプト（ウイルス）を実行させるテクニックが併用されていた。すなわち、本件は PowerShell を悪用する攻撃への一般的な対策である、「Windows 標準の PowerShell.exe の実行禁止」、「PowerShell.exe から端末外部へのアウトバウンド通信の禁止」といった対策を回避するものでもあった。

また、以降の説明において、「何らかの方法で」と記載している箇所があるが、それらは原因・手口が解明されていない、あるいは情報提供外となっている部分である。予めご了承いただきたい。

（1） 手口 1：MSBuild の悪用

本手口では、攻撃者によって、何らかの方法で悪意のあるコード等を含む XML ファイルが攻撃対象の端末に設置され、実行されたものと考えられる。この XML ファイルは、Windows 10 等に標準で付属されている「MSBuild.exe」というツールで解釈可能な形式（MSBuild プロジェクトファイル）であった。

本手口は、次の流れで攻撃が行われたものと考えられる。

[10] 標的型攻撃の新たな手口判明。診断ツール「PoshC2」を悪用する攻撃の流れを解説（LAC）
https://www.lac.co.jp/lacwatch/people/20200424_002177.html

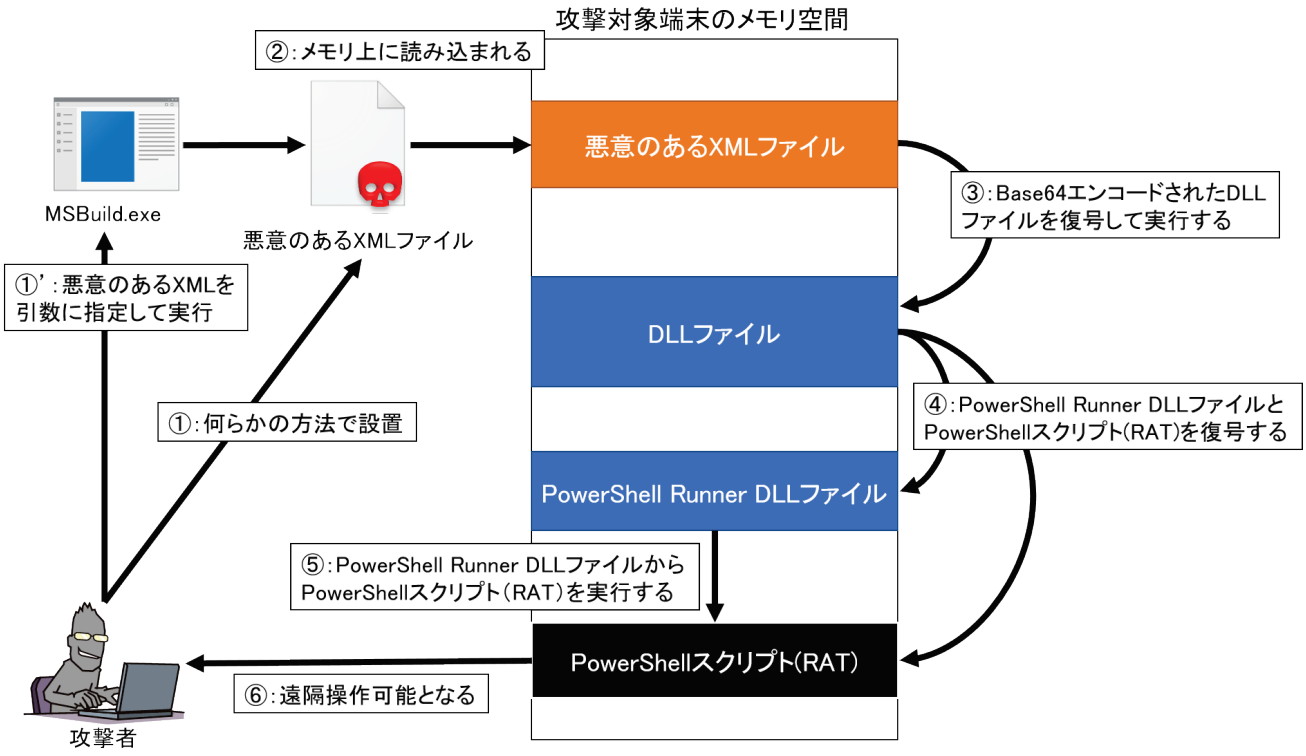

図 5 MSBuild 悪用の手口の概要図

① 攻撃者が、何らかの方法で悪意のある XML ファイルを端末上に設置するとともに、引数に当該ファイルを指定して MSBuild.exe を実行する。

② MSBuild.exe により悪意のある XML ファイルがメモリ上へ読み込まれ、ファイル内に記述された悪意のあるプログラムが実行される。これは、MSBuild.exe の仕様通りの動作である。

③ 実行された悪意のあるプログラムは、さらにプログラム内に Base64 エンコードされて埋め込まれている DLL ファイルを復号して実行する。
この時、復号された DLL ファイルの PE ヘッダは、一部書き替えられていた。これは、セキュリティ製品等によるウイルス検知を避けるための細工であろうと推測している。

④ 実行された DLL ファイルは、さらに内包している DLL ファイル(PowerShell Runner DLL ファイル [11])と、PowerShell スクリプト(RAT)を復号する。

⑤ DLL ファイルは、PowerShell Runner DLL ファイルを使って悪意のある PowerShell スクリプト(RAT)を実行する。

⑥ 実行された悪意のある PowerShell スクリプト(RAT)により、攻撃者による端末の遠隔操作が可能となる。

なお、本件のような MSBuild.exe を悪用する手口は、MITRE 社の ATT&CK において、「Trusted Developer Utilities」(T1127)の一部に分類されている [12]。

---

[11] ここで「PowerShell Runner DLL ファイル」と呼ぶファイルは、Windows 標準の PowerShell.exe の実行を伴わずに、任意の PowerShell スクリプトを実行する機能をもつ DLL ファイルであった。

[12] Trusted Developer Utilities(MITRE ATT&CK)
https://attack.mitre.org/techniques/T1127/

（2） 手口 2:タスクスケジューラの悪用

本手口は、タスクスケジューラの悪用により、ウイルスの感染永続化が行われたものである。

攻撃者は、何らかの方法で、タスク定義ファイル（悪意のあるタスクスケジューラのタスクを定義した XML 形式のファイル）を攻撃対象の端末に設置した。そして、このタスク定義ファイルをタスクスケジューラへインポートすることにより、不正なタスクを作成した。

不正なタスクは、タスク定義ファイルと同様、何らかの方法により端末内に別途設置された、悪性の DLL ファイルを実行するようにスケジュールされる。この悪性の DLL ファイルは、ファイルの内部に暗号化して埋め込まれた DLL ファイル（RAT 本体）を、メモリ上で動作させるものであった。

参考までに、本手口で作成される不正なタスクの設定（トリガーと操作）を次に示す。

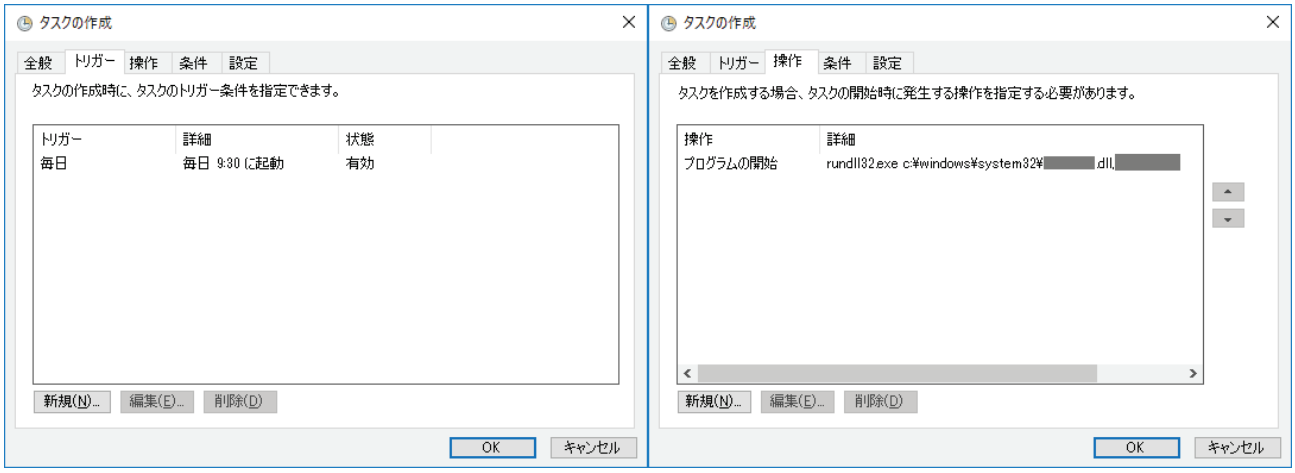

図 6 作成される不正なタスクの設定（左:トリガー、右:操作）

なお、本件のようなタスクスケジューラを悪用する手口は、MITER 社の ATT&CK において、「Scheduled Task」(T1053)に分類されている [13]。

（3） 手口 3:DLL サーチオーダーハイジャッキングよる不正操作

本手口では、攻撃者によって、何らかの方法で悪意のある「dbghelp.dll」というファイルが攻撃対象の端末に設置され、実行されたものと考えられる。このファイル名は、Windows の正規の DLL ファイルと同一であることから、攻撃者は DLL サーチオーダーハイジャッキングの手口を悪用したものと思われる。

Windows のアプリケーションの中には、DLL ファイルを読み込む際に、同一フォルダ内の DLL ファイルを優先的に読み込み使用してしまう脆弱性を持つものがある。この脆弱性を悪用し、Windows ディレクトリ配下にある正規の DLL ファイルではなく、悪意のある DLL ファイルを優先的に読み込ませ、悪性の動作を行わせる攻撃手口が DLL サーチオーダーハイジャッキングである。

なお、本件の DLL サーチオーダーハイジャッキングの手口は、MITER 社の ATT&CK において、「DLL Search Order Hijacking」（T1038）に分類されている [14]。

---

[13] Scheduled Task（MITER ATT&CK）
https://attack.mitre.org/techniques/T1053/

[14] DLL Search Order Hijacking（MITER ATT&CK）
https://attack.mitre.org/techniques/T1038/

本手口で確認された dbghelp.dll は、Windows の正規のファイルが攻撃者によって改ざんされ、悪意のある動作が追加されたものであった。この改ざんされた dbghelp.dll（以降、悪性 dbghelp.dll）は 2 種類存在し、それぞれの動作概要は次の通りであった。

- 端末の遠隔操作を行うための Windows の設定変更を行う
- PowerShell スクリプト（RAT）を実行する

それぞれの悪性 dbghelp.dll による攻撃の流れを説明する。

（3）-1：端末の遠隔操作を行うための Windows の設定変更を行う

本手口では、次の流れで攻撃が行われたものと思われる。

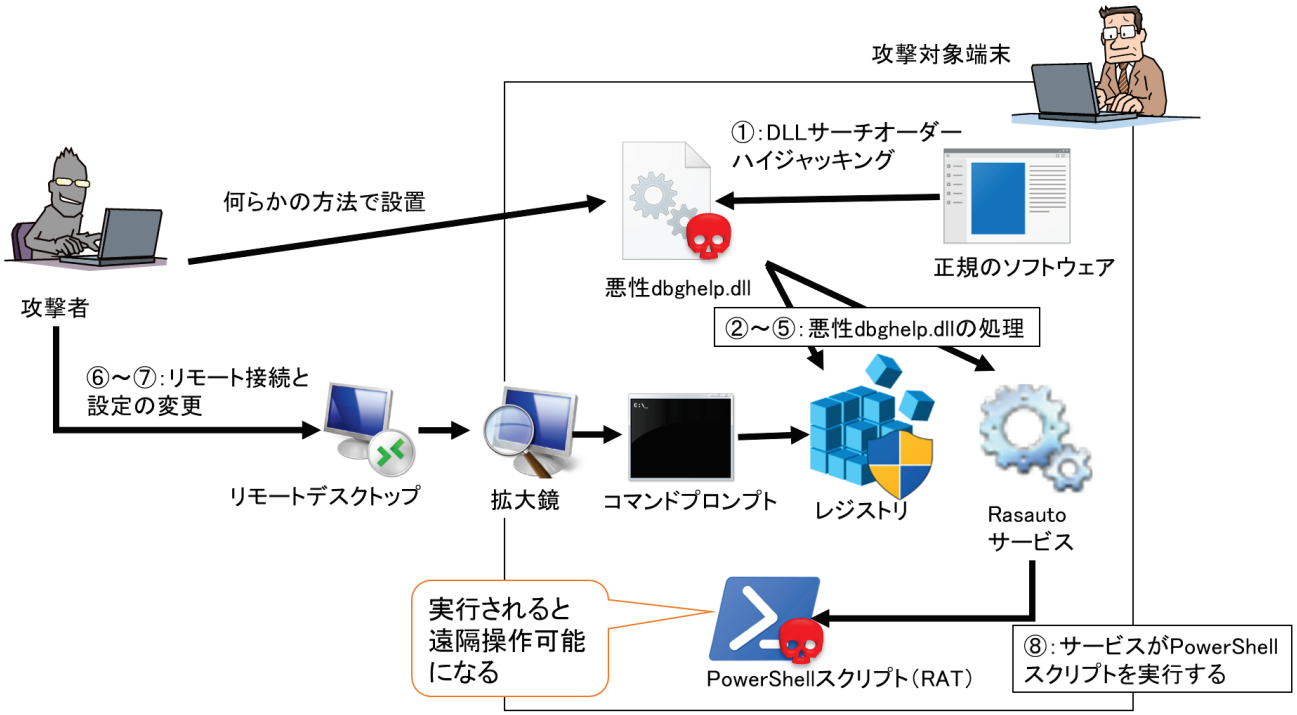

図 7 遠隔操作のための Windows の設定変更の概要図

① 何らかの方法で攻撃者によって端末上に設置された悪性 dbghelp.dll が、端末上の正規のソフトウェアの起動の際、読み込まれて実行される（DLL サーチオーダーハイジャッキング）。
この悪性 dbghelp.dll が次の②～⑤までの処理を実行する。

② ユーザ操作によって Windows の拡大鏡（magnify.exe）が起動されると、コマンドプロンプトが起動するようにレジストリを設定する（図 8）。なお、この「拡大鏡の置き換え」の攻撃手口は、MITRE ATT&CK において「Accessibility Features」（T1015）の一部に分類されている [15]。

[15] Accessibility Features (MITRE ATT&CK)
https://attack.mitre.org/techniques/T1015/

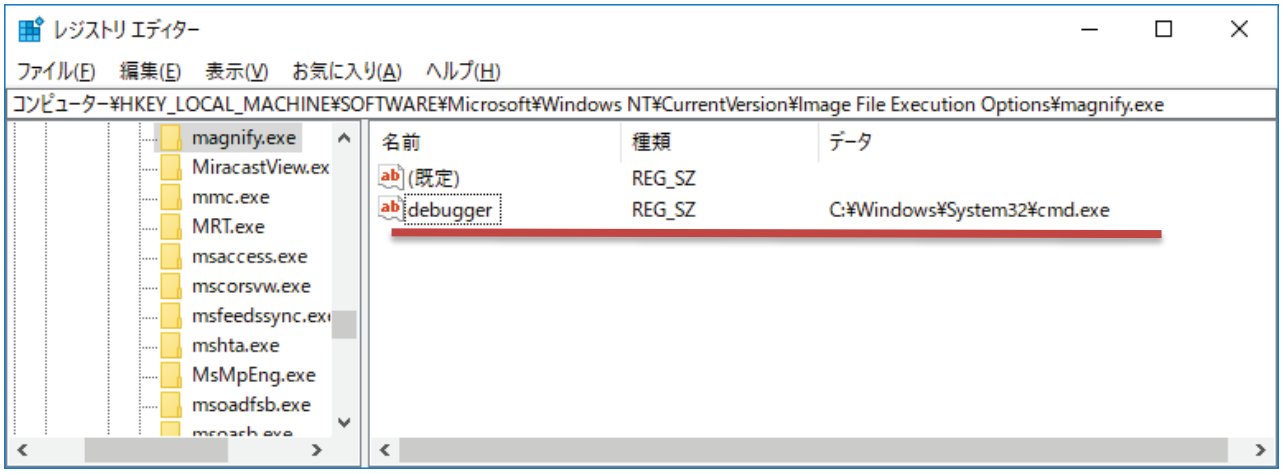

図 8 レジストリ設定（拡大鏡実行時にコマンドプロンプト起動）

③ Remote Access Auto Connection Manager サービス[16]（以降、Rasauto サービス）のアクセス制御設定を、Windows の全てのユーザ権限で操作可能な状態にする。

④ Windows のユーザを追加し、そのユーザに管理者権限を設定する。

⑤ リモートデスクトップ接続時のネットワークレベル認証を、無効にするレジストリを設定する（図 9）。これにより Active Directory に参加していないユーザからのリモートデスクトップ接続が可能となる。

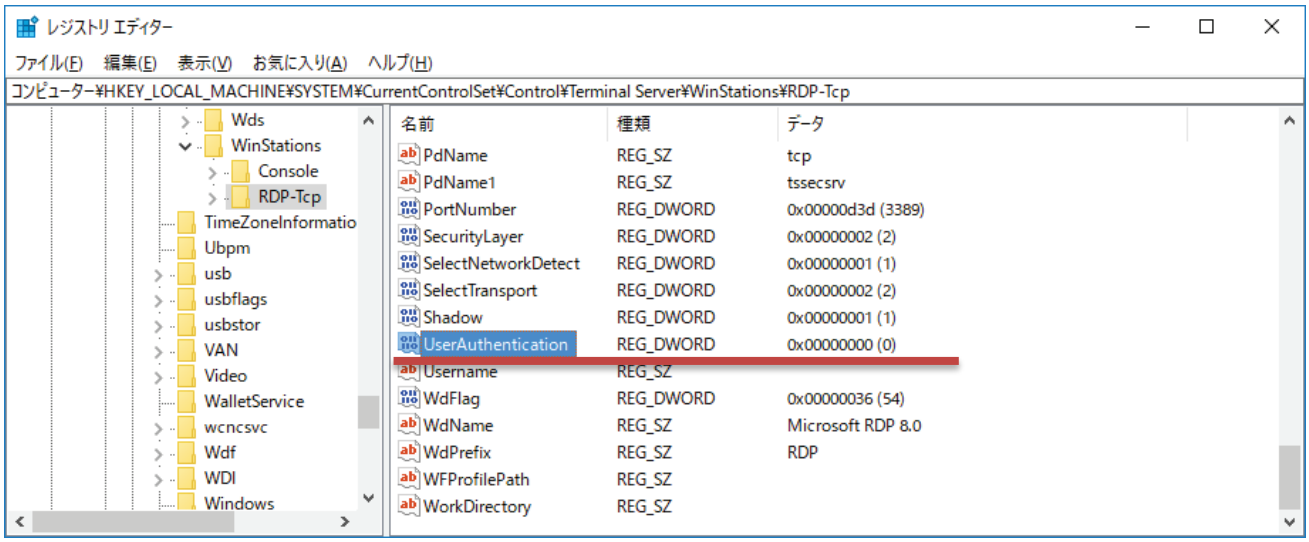

図 9 レジストリ設定（RDP-Tcp）

⑥ 攻撃者は、悪性 dbghelp.dll によって②～⑤までの設定変更が行われた端末へ、リモートデスクトップ接続を行うと、ログイン画面にて拡大鏡をショートカットキーで呼び出すことで、コマンドプロンプトを起動することができる。この状態で起動したコマンドプロンプトは Windows の System 権限で起動するため、通常のユーザ権限では操作できない操作が可能となる。

⑦ 攻撃者はコマンドプロンプト上で、Rasauto サービスのレジストリを操作し、サービス起動時に、別途何らかの方法で設置した PowerShell スクリプト（RAT）が実行されるように設定したものと思われる。

---

[16] プログラムからリモート接続の要求があった場合、リモート接続に失敗した際に VPN 等で自動的にリモート接続を確立させるサービス。

⑧ Rasauto サービス起動時に PowerShell スクリプト（RAT）が実行され、遠隔操作可能な状態となる。

（3）-2：PowerShell スクリプト（RAT）の実行

本手口では、次の流れで攻撃が行われたものと思われる。

① 何らかの方法で攻撃者によって端末上に設置された悪性 dbghelp.dll が、端末上の正規のソフトウェアの起動の際、読み込まれて実行される（DLL サーチオーダーハイジャッキング）。
② 悪性 dbghelp.dll のファイル内部に、Base64 エンコードされた状態で埋め込まれている PowerShell スクリプト（RAT）を復号する。
③ 何らかの方法で攻撃者によって改変された Windows の正規の PowerShell.exe を使い、復号した PowerShell スクリプト（RAT）を実行する。
④ 実行された PowerShell スクリプト（RAT）によって端末が遠隔操作可能になる。

5.2 併用されたその他の攻撃手法

本件で情報提供を受けた攻撃の中には、ここまで説明してきたツールとは別に、「リバースプロキシ機能をもつツール」や、「SSH クライアントに含まれているツール」といったオープンソースのツールが使われた痕跡を確認している。攻撃者はこれらのツールを悪用しつつ、リモートデスクトップ接続による端末の遠隔操作や、側方移動（ラテラルムーブメント）を行ったものと推測している。

類似の手口を LAC 社が情報公開[17]しているため、参考としていただきたい。

[17] オープンソースのポート転送／トンネリングツールを悪用する標的型攻撃に注意（LAC）
https://www.lac.co.jp/lacwatch/people/20200212_002127.html

6　複数の組織を狙うフィッシングメール

本四半期、J-CSIP 参加組織（A 社）より、実在する国内企業の海外グループ企業（Y 社）から、不審なメールを受信したという情報提供があった。なお、A 社が不審メールについて Y 社へ確認を行ったところ、Y 社からは、「メールアカウントが乗っ取られ、意図せず不審メールの送信が行われていた」という回答があったとのことである。

当該メールについて IPA で調査を行ったところ、メール本文中の URL リンク先からは、送信元企業（Y 社）の企業名やロゴ、送信者の名前やメールアドレス等が記載された PDF ファイルがダウンロードされた。この PDF ファイルには、URL リンクが埋め込まれており、クリックすると Office 365 等のアカウント情報を詐取するためのフィッシングサイトへアクセスさせられるものであった。

本件について調査を続けたところ、メール本文中に記載された URL 等の情報から、他の J-CSIP 参加組織も本件の攻撃対象となっている可能性があることが分かった。このため、IPA から本件の情報共有を行うと共に、対象の J-CSIP 参加組織へヒアリングを行ったところ、3 社（B 社、C 社、D 社）より、同等の攻撃メールが発見されたという情報提供があった。

本章では、本事例においてどのような攻撃が行われたのかを説明する。

（1）事例の概要

本事例は、攻撃者によって乗っ取られたアカウントから、複数の組織へ向けて Office 365 等のアカウント情報を狙うフィッシングメールが送られたものである。確認できている限り、攻撃者によってメールアカウントを乗っ取られた組織は 2 社存在し、このうち 1 社は J-CSIP 参加組織（C 社）の海外関連企業であった。また、当該フィッシングメールは多数の組織に送信されたと思われ、J-CSIP 内においても、4 つの参加組織（A 社～D 社）に着信していた。

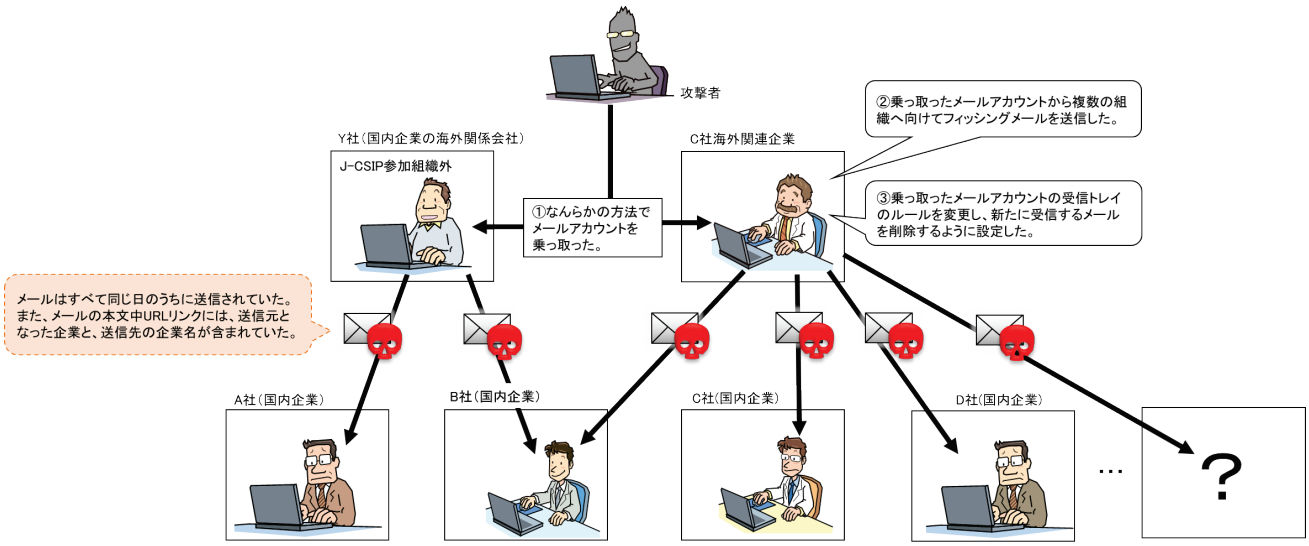

図 10　事例概要図

まず、攻撃者は何らかの方法で、フィッシングメールの送信元となった企業（Y 社および、C 社海外関連企業）のメールアカウントを乗っ取ったものと考えられる。このとき、攻撃者は乗っ取ったメールアカウントの受信トレイのルールを変更し、新たに受信するメールが削除されるように設定していた。これは、配信エラーメールや、攻撃メール送信先からの問合せといったメールを、本来のアカウントの所有者の元へ届かせないようにし、事案の発覚を遅らせる目的であったものと推測している。

その後、攻撃者は乗っ取ったアカウントから複数の組織へ向けてフィッシングメールを送信した（図 11）。このフィッシングメールには、本文中に請求書へのリンクを装う URL リンクが埋め込まれており、URL には、フィッシングメールの送信元となった企業の名前と、送信先の企業の名前が含まれていた。

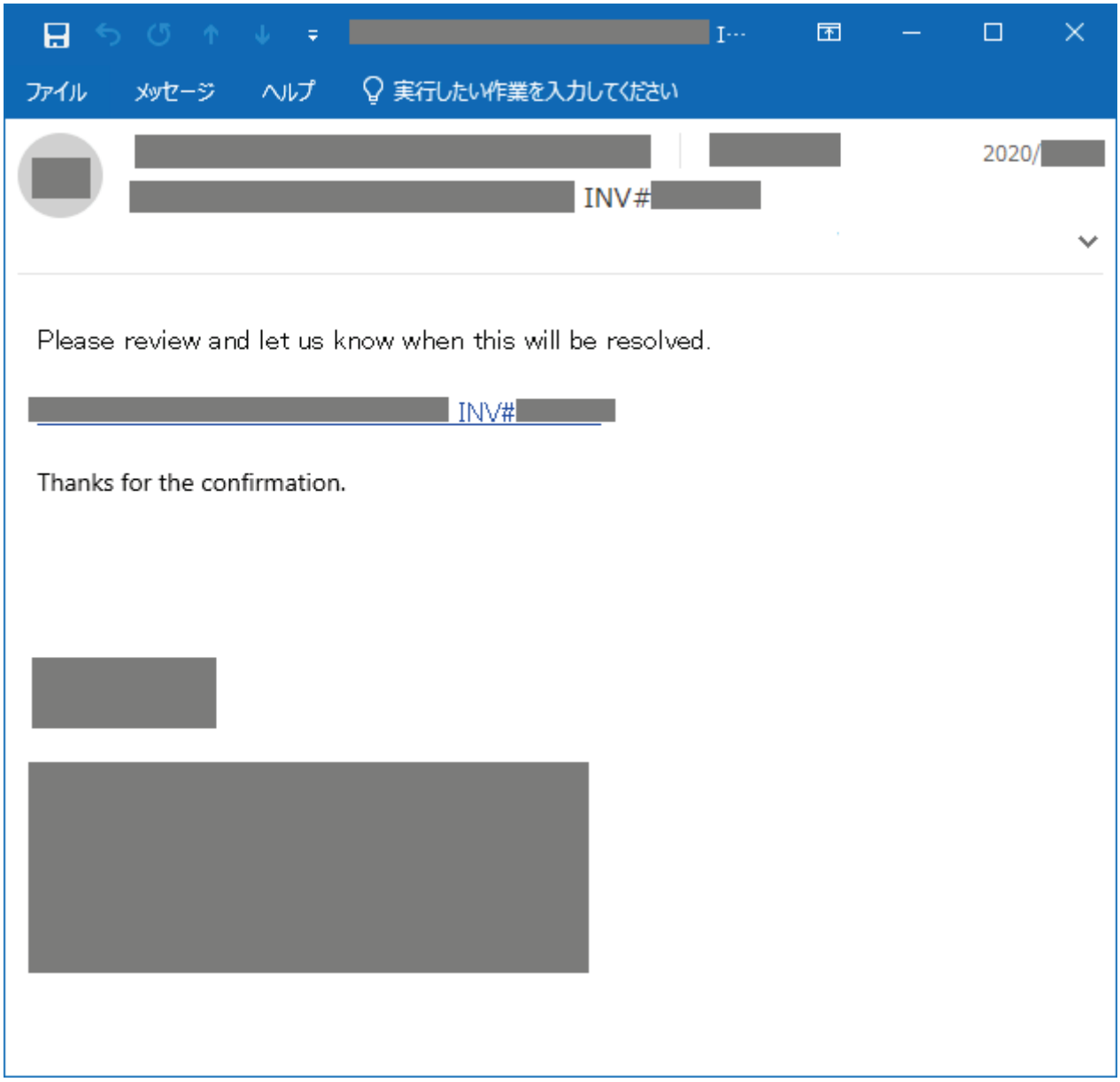

図 11 送信されたフィッシングメール

（2）攻撃に使われた手口

本事例では、メール本文中の URL リンクをクリックすると、OneDrive（Microsoft 社の正規サービスを悪用）にリダイレクトされ、そこに PDF ファイルが設置されていた。PDF ファイルには送信元となった企業のロゴや住所等のほか、攻撃者によって乗っ取られたアカウントの人物の名前やメールアドレスが記載されており、あたかも送信元企業の資料であるかのように偽装されていた。この PDF ファイルには、フィッシングサイトへの URL リンクが埋め込まれており、ドキュメントを確認するために URL リンクをクリックさせようとするものであった（図 12）。

図 12 メール本文中 URL リンクからアクセスした先にある PDF ファイル

フィッシングサイトは、OneDrive の認証画面を装っており、Office 365 かその他のメールアカウントでの認証を選択するような画面が表示される（図 13）。ここでどちらかを選択すると、偽のログイン画面（図 14）が表示され、そこで情報を入力するとアカウント情報が詐取されてしまうものであった。

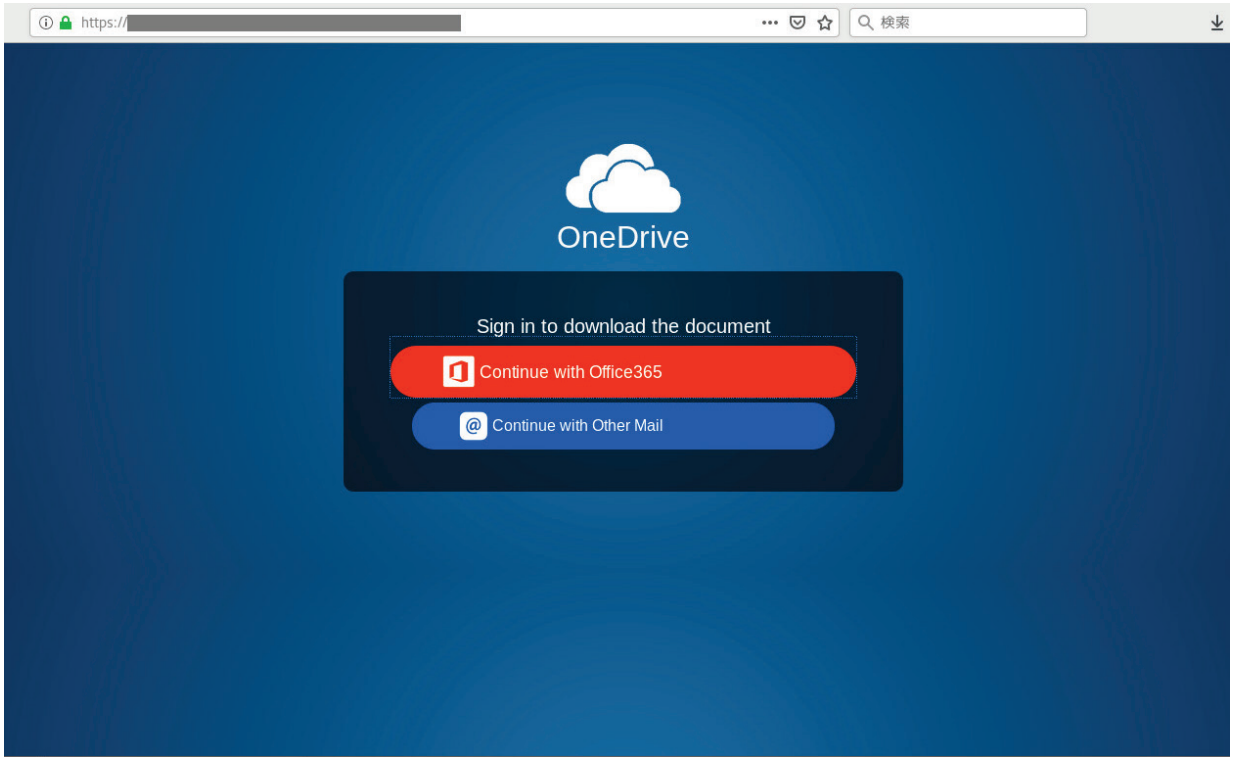

図 13 フィッシングサイト（認証選択画面）

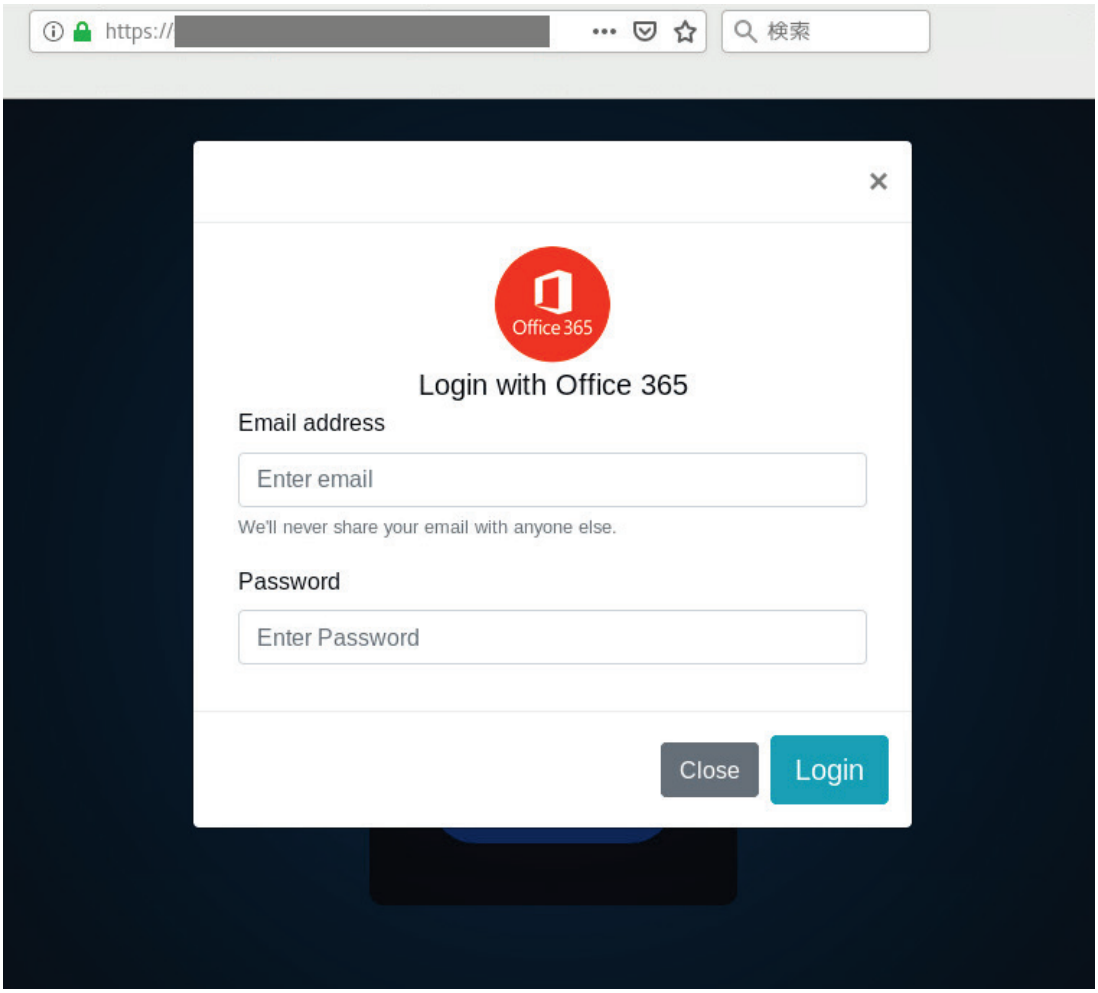

図 14 フィッシングサイト（Office 365 の偽ログイン画面）

Office 365 のアカウント情報を狙うフィッシングメールはこれまでも多数確認されてきたが、本事例は、企業を踏み台としつつ、その企業のロゴ画像等を使いながら、さらに他の複数の組織を狙って攻撃を行ってくるという手口であり、注意を要する事例であると考えられる。

フィッシング攻撃については、利用者一人ひとりが、このような手口があるということを知り、騙されないように注意し、ID やパスワード、メールアドレス等を偽のウェブサイトで入力しないことが重要である。また、組織・企業においては、利用者がアカウント情報を騙し取られることが組織的なリスクにつながることを理解し、従業員に対し、アカウント情報の適切な取り扱いを徹底することが重要である。

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