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]

2021 年 4 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、2021 年 3 月末時点の運用体制、2021 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 2020 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

2021 年 1 月～3 月期（以下、本四半期）は、次の通り参加組織の変更があり、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）の体制となった（図 1）。

- 2021 年 3 月、クレジット業界 SIG 内での退会に伴い、参加組織が 48 組織から 47 組織となった。

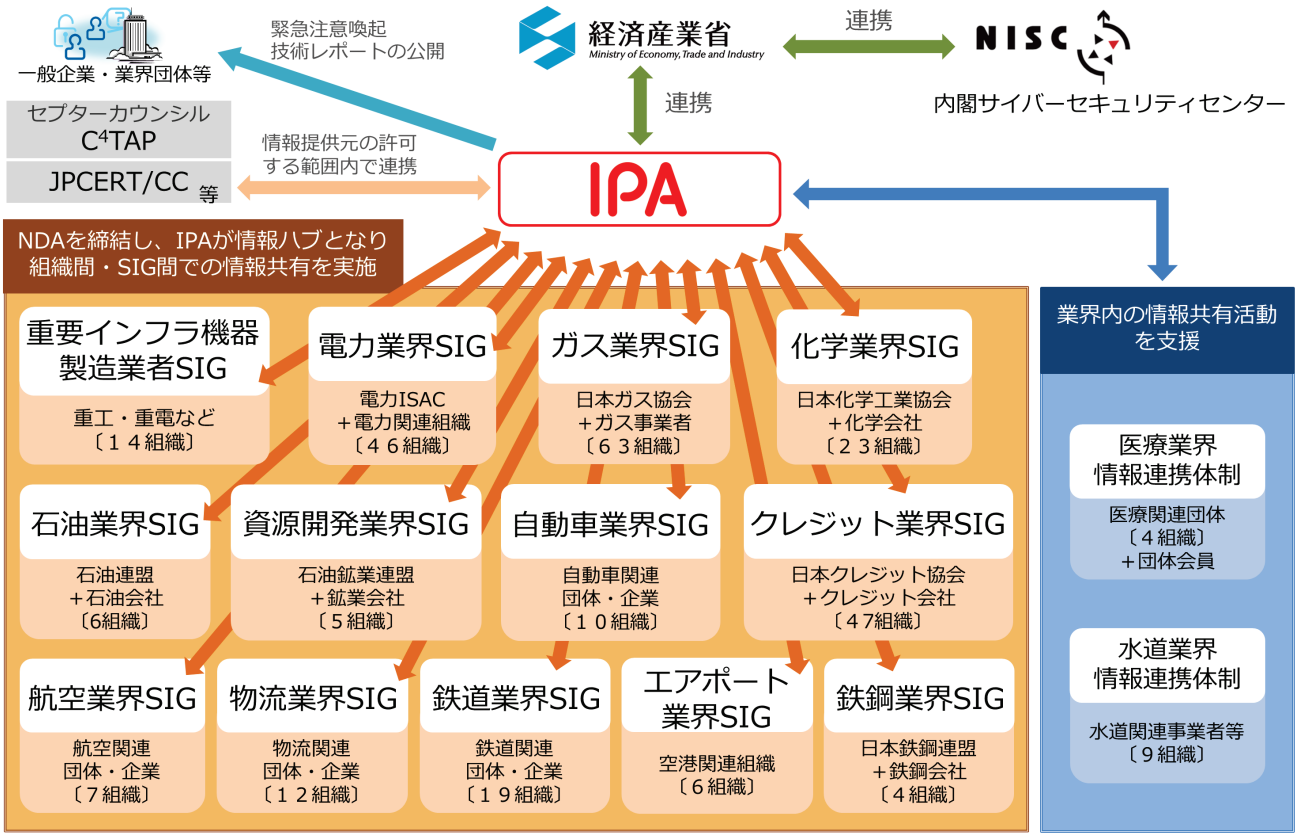


図 1 J-CSIP の体制図

[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 1 月～3 月）

2021 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 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
		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	325 件	4,988 件	479 件	**410 件**
2	参加組織への情報共有実施件数※1	55 件	29 件	38 件	**25 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 **18 件**を含む。

本四半期は情報提供件数が **410 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 **13 件**であった。提供された情報の主なものとして、2021 年 1 月に Emotet への感染を狙った攻撃メールについて 50 件以上の情報提供があった。なお、1 月末の Europol 等によるテイクダウン [3]以降は Emotet に関する情報の提供や観測は無くなっている。

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。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が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。

- 参加組織が契約しているクラウドサービスに対する不正アクセスが行われたという情報提供があった。具体的な攻撃の手口の他、不正アクセス元の IP アドレスについて、情報共有を行った。これについては 5 章で述べる。

- Microsoft Exchange Server の新たな脆弱性の悪用の痕跡を確認したという情報提供があった。当該組織のグループ会社 3 社で観測されたが、実被害はなかったとのことであった。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やある程度広くばらまかれたと思われる攻撃メールが情報提供されることがある。本四半期で観測された特徴的なメールについて、7 章で述べる。

[3] World's most dangerous malware EMOTET disrupted through global action （Europol）
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

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	実在する日本の銀行から身に覚えのないメールを受信した。	1 件
2	偽のセクストーションメールを受信した。	2 件
3	テレワーク中の職員が偽警告サイト閲覧時に攻撃者の指示に従ってしまい、遠隔アシスタントツールをインストールしてしまった。	1 件
4	短時間の間に不審メールが大量に着信した。	1 件
5	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。	6 件

項番 1 は、実在する日本の銀行から、支払い通知のような身に覚えのないメールを複数受信し、添付ファイルの開封をしてしまったという相談であった。本物のメールのように考えられたが、不審と判断した理由も妥当であったため、当該銀行への確認を勧めるとともに、念のため J-CSIP 内に情報共有を行った。その後、過去に同銀行より類似の本物のメールを受信したことがあるという他組織からの情報提供が複数あり、また、最終的には当該情報提供元においても本物のメールであることが確認できたとのことであった。本物か攻撃かすぐに判断の難しいようなメールは、その送信元への直接の確認が確実ではあるが、状況により情報共有も並行して実施することもある。

項番 2 は、偽のセクストーションメールを受信したという情報提供である。個人のプライベートな情報（弱み）を入手し、友人・知人に情報をばらまくと脅す内容で、実際には嘘のメールであった。個人を狙う詐欺の一種ではあるが、企業・組織のメールアドレスにもこのようなメールが多く着信している。当該メール自体は無視してよいものであるものの、今後もばらまかれ続ける可能性がある。

項番 3 は、偽警告に関する相談である。テレワーク中の職員が PC の操作中、Microsoft を装った偽の警告画面（偽警告サイト）が表示された。職員は画面に表示された電話番号に電話をし、電話口での指示に従ってしまい、遠隔アシスタントツールをインストールしてしまった。職員は電話の途中で不審と思い終話したため、金銭的な被害はなかった。当該職員はテレワークをしており、偽の警告画面とともに警告音が鳴ったため、パニック状態になり画面に表示されている電話番号に電話をしてしまったとのことであった。社内環境で同様の事象が発生した場合、すぐに周囲やシステム管理部門への相談等ができた可能性があるが、在宅勤務により連絡がしにくいという影響があったようである。また、自宅回線を利用していたため、ネットワークの通信ログ等による詳細な影響調査ができず、一部対応の遅れや解明しきれない箇所等が残った。コロナ禍でテレワーク等を活用している企業・組織は多いと考えるが、本件のような異常発生時の対応について、必要に応じ職員への周知や連絡体制の見直しを実施していただきたい。

項番 4 は、4 時間の間に約 9,000 件、見慣れない不審メールが着信したという相談で、メール本文中には 1 つの短縮 URL リンクのみが記載されているものであった。攻撃意図が不明であり、情報提供元では対応に困り IPA へ連絡をいただいた。IPA で確認した結果、恐らくはなんらかの詐欺を目的としたメールであろうと思われ、最終的には無視するという対処とした。通常運用している中で、質・量の面で見慣れない不審なメールを受信した場合は、標的型攻撃である可能性も考慮し、可能な範囲で調査をすべきであろう。

項番 5 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、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　今年度の状況

3.1 今年度の取り扱い件数と年度毎の推移状況

J-CSIP における取り扱い件数（情報提供件数、標的型攻撃（メール、検体等）と見なした件数、情報共有実施件数）と参加組織数について、今年度（2020 年度）の合計と、J-CSIP を運用開始した 2012 年度から 2019 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、検体等）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
2020 年度	6,202	125	147	13 業界 262 組織 ＋ 2 情報連携体制 13 組織

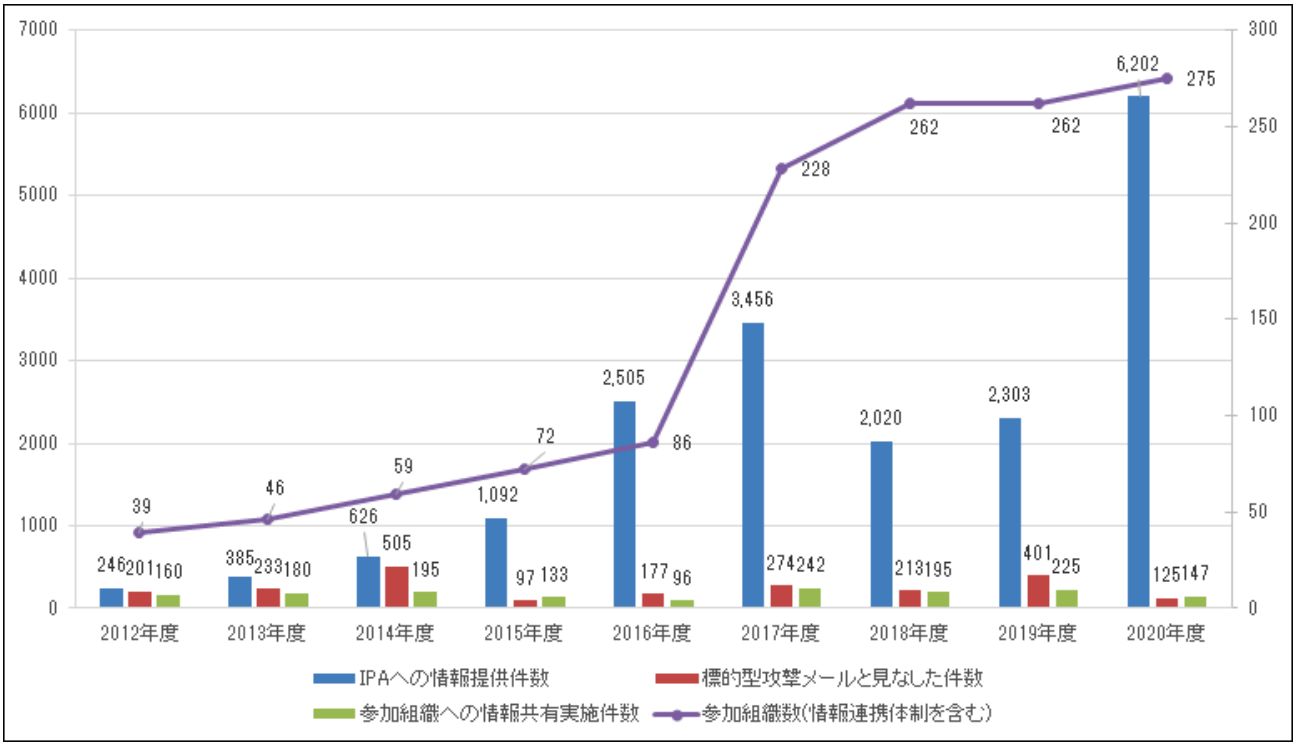


図 2 年間の取り扱い件数と参加組織数の推移

3.2 今年度の活動

2020 年度は、J-CSIP の参加組織数について、年度内での増減があり、最終的な参加組織数は 2019 年度から 13 組織増加した。

情報提供について、今年度は 6,202 件とこれまでで一番多い情報提供数となった。これは、Emotet への感染を狙った攻撃メールの情報提供が特に多かったためである。また、引き続きビジネスメール詐欺が試みられたという情報提供も続いている。これらの情報については、四半期毎の運用状況レポートの他、IPA のウェブサイトにて注意喚起 [5]を行っている。ビジネスメール詐欺では、2019 年度でも見られた国内外の多数の組織へ行われたと推測される CEO 等を騙る一連の攻撃メールについても 2020 年度で継続して観測されており、今後も引き続き注意が必要である。

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、2020 年度も引き続き確認されたが、数は減少傾向であった。2019 年 11 月に確認した日本語の攻撃メールについては、2020 年度では観測されなかった。数は減少したものの、引き続き今後の動向に注視していく。

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、2020 年度でも 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はなく、VPN 装置や Microsoft Exchange Server の脆弱性を悪用して侵入しようとした痕跡が確認されるといった情報提供があった。メール以外の侵入経路が試みられる事例や、海外拠点のマシンから標的型攻撃に関連する可能性があるウイルスが発見されたという事例も確認しており、手口を変えながら標的型攻撃が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（以降、Emotet の攻撃メール）が日本国内で多数観測された。2020 年 2 月上旬から 7 月中旬にかけて Emotet の攻撃メールが観測されない状況が続いたが、その後攻撃が再開された。攻撃の状況に関する情報は、IPA からも注意を促すためのページ [6]を公開し、随時更新を行った。また、JPCERT/CC[7]をはじめとして多数のセキュリティベンダからも情報が公開された。

J-CSIP 内では 2020 年 7 月から 9 月期において、4,730 件もの Emotet の攻撃メールの情報提供があった。Emotet の攻撃メールの件名や本文、添付ファイル等の攻撃手口は様々な種類があり、一般的なビジネス用件（請求書等）を装うものから、正規メールへの返信（Re:）や転送（Fw:）を装うものなどが確認されている。また、賞与関連や新型コロナウイルス感染症（COVID-19）等の時節に合わせた題材を使うものもあった。

2021 年 1 月、Europol が欧米各国の共同作戦により Emotet のテイクダウンを実施した [8]という発表があり、以降 Emotet の攻撃メールについては、IPA が確認している範囲では見られなくなった。

---

[5] 【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

[6] 「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

[7] 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

[8] World’s most dangerous malware EMOTET disrupted through global action （Europol）
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

その他、Emotet 以外のウイルスへの感染を企図して広くばらまかれた攻撃メールや、Microsoft 365（Office 365）等のアカウント情報を狙うフィッシング攻撃等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。

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、2020 年 4 月の 3 回にわたり 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。

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 11 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 10 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 2 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 とタイプ 2 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。

4.1 事例 1 海外グループ企業を狙った攻撃

本事例は、2021 年 1 月、J-CSIP の参加組織（A 社：国内企業）の海外グループ企業（B 社）の担当者に対し、A 社の取締役になりすました攻撃者から、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 2：経営者等へのなりすまし」に該当する。

この事例では、B 社の担当者が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。

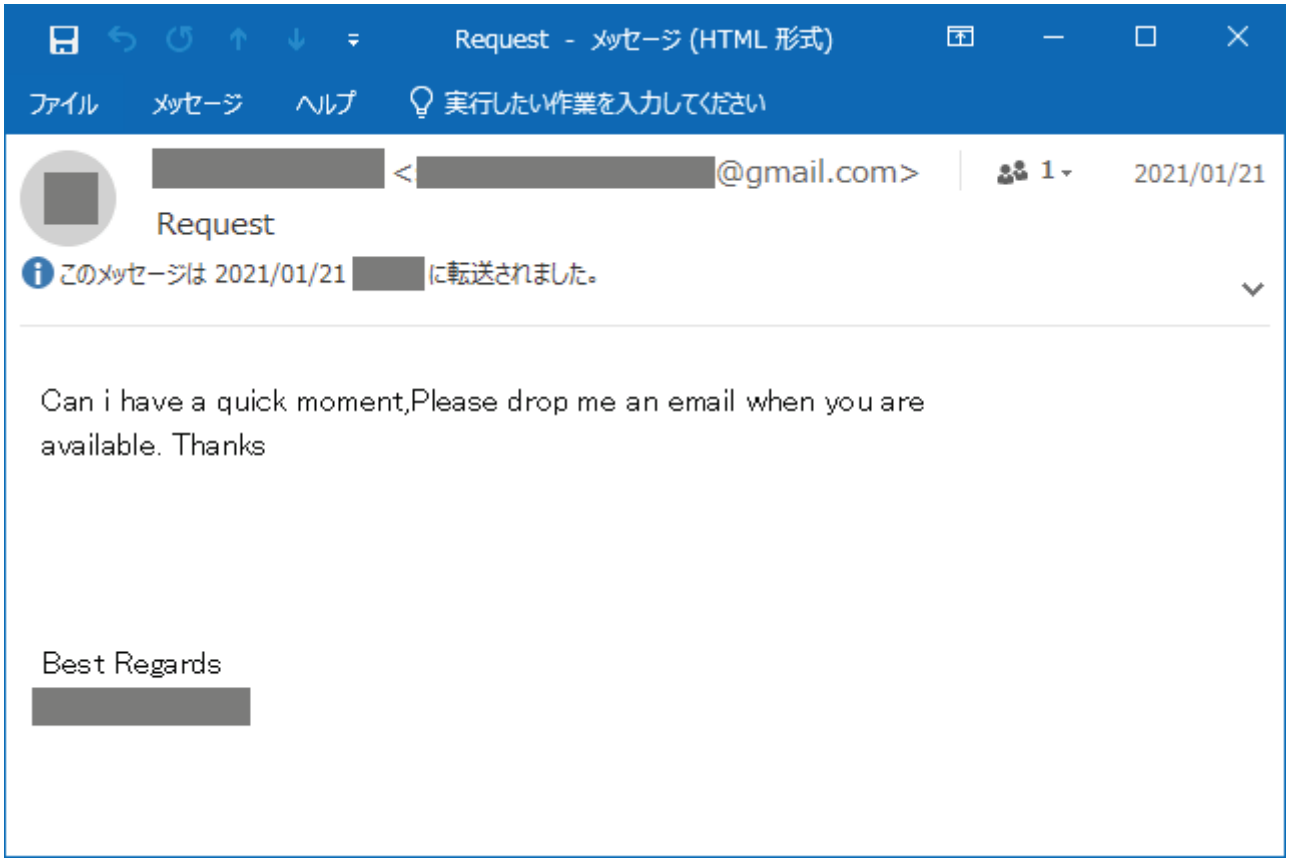


図 3 攻撃者から送られた偽のメール

攻撃者から送られてきた偽のメールは、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）のメールアドレスの表示名には A 社取締役の名前が設定されていたが、メールアドレスはフリーメールアドレスから送られていた。

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。

4.2 事例 2 国内企業を狙った攻撃

本事例は、2021 年 2 月、J-CSIP の参加組織（A 社：国内企業）の担当者に対し、取引先ではない海外の産業用機械メーカー（B 社）の担当者になりすました攻撃者から、偽の口座への支払い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」に近いが、手口としてはレベルの低いものである。

この事例では、A 社の担当者が次の理由により偽のメールの不審な点に気づき、システム管理部署に報告したことで攻撃であることが発覚したため、金銭的な被害には至らなかった。

- 普段金銭を扱うことのない部署（生産設備・土地建物を扱う部署）の担当者宛に着信した
- B 社やメールに記載されていた人物と過去にやりとりをした実績がなかった
- メールの内容に心当たりがなかった

本事例で攻撃者から送られたメールを図 4 に示す。

攻撃者から送られてきたメールは、B 社の銀行口座が使用できなくなったことと、古い口座への支払いを延期するように促す内容が書かれていた。

また、差出人（From）のメールアドレスと返信先(Reply-To)は次のように設定されていた。

差出人（From）　　：B 社担当者の名前 <B 社担当者の本物と思われるメールアドレス>
返信先（Reply-To）：B 社担当者の名前 <B 社とは別のメールアドレス>

これはメールを返信しようとした際に、差出人とは別の攻撃者のメールアドレスを宛先にしようとする典型的な手口であった。

IPA では、公開情報にて本メールの本文の内容が類似した 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。

今回は身に覚えのない企業からのメールだったため比較的容易に偽メールと気づけたが、適切な部署に適切なタイミングで届いた場合は応じてしまう場合があるので注意が必要である。

本件のように、身に覚えのない企業・組織から支払いに関する内容のメールが送られてくることもあるため、少しでも不審と思われるメールを受信した場合は、社内で相談・連絡して偽のメールであると気づけるようにしておきたい。

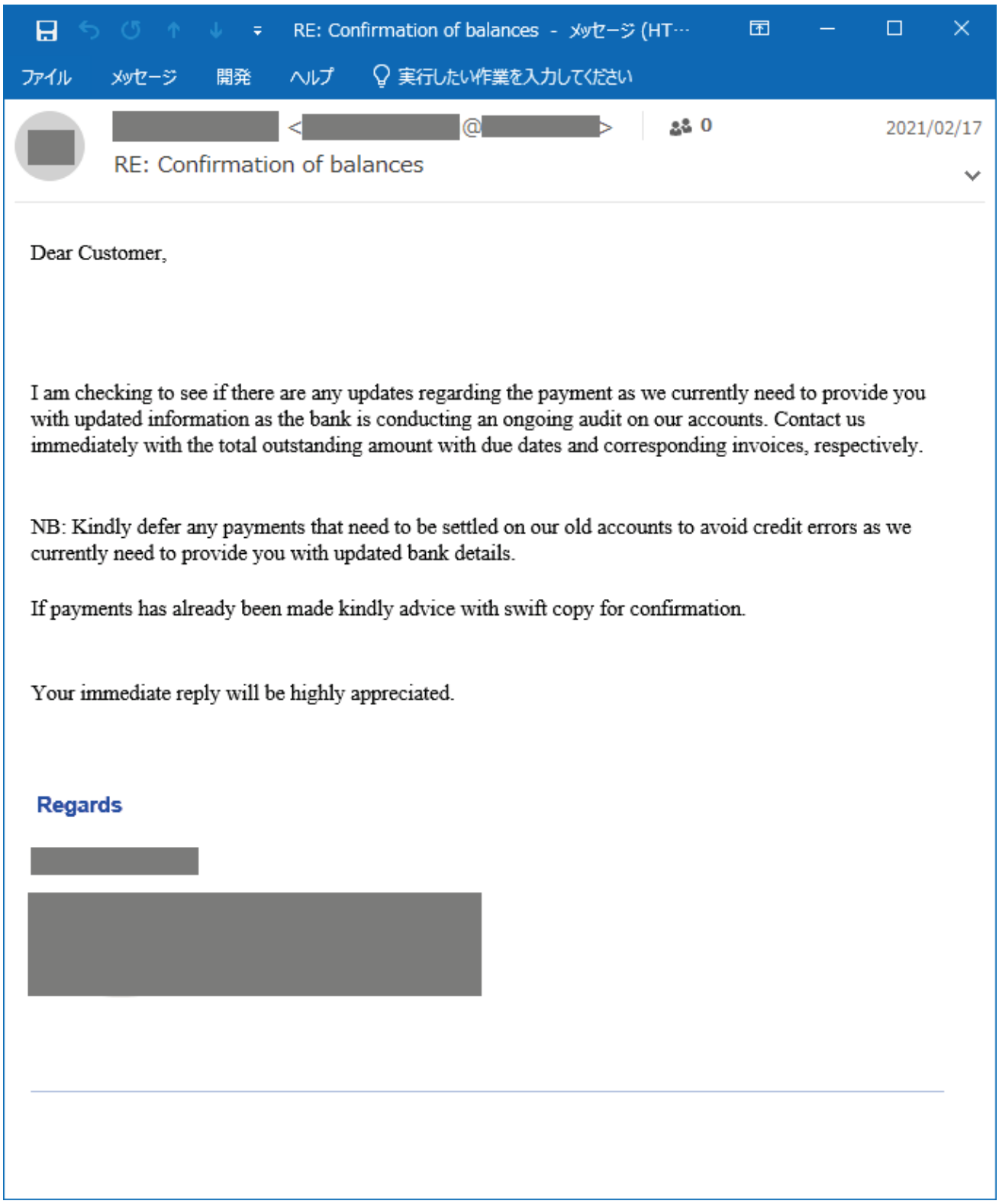


図 4 攻撃者から送られた偽のメール

4.3 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 4 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

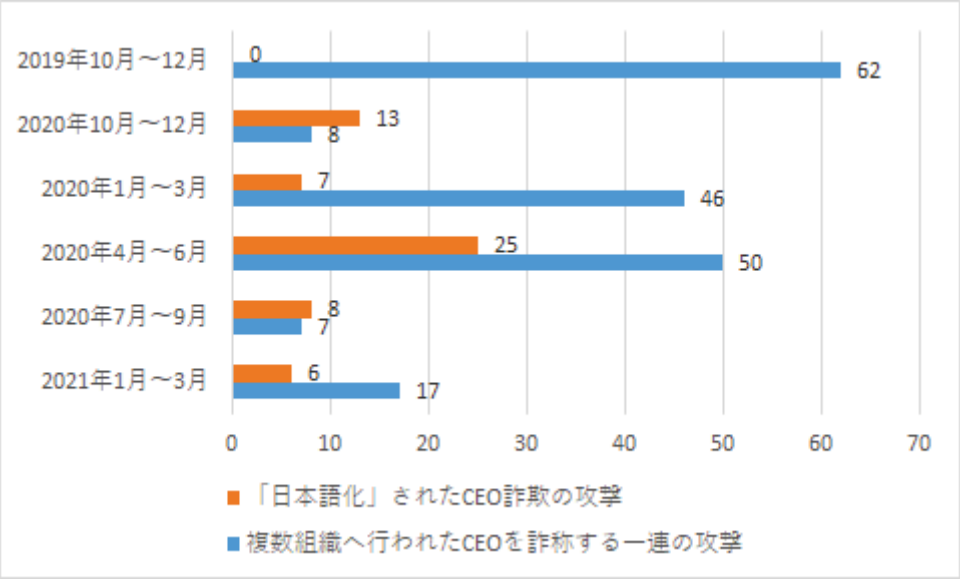


図 5 これまで入手したメール件数の推移

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、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、注意が必要である。

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[9]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 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（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 24 日以降は、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。

[9] 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」というメールサービスを使用してい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）[10]」の 2.1 章事例 1 にて、情報を公開している。

攻撃メールには、次のような特徴がある。

表 6 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。

[10]【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

5　クラウドサービスへの不正アクセス

本四半期、J-CSIP 参加組織（国内企業）が契約していた SaaS 型のクラウドサービス（以下、クラウドサービス）に対し、複数の段階を経て攻撃者が不正アクセスを行ったという情報提供があった。本件については、攻撃に使われたと思われるアクセス元の IP アドレスの他、攻撃の手口について J-CSIP 内で情報共有を行っている。

本章では攻撃の手口について、情報提供元の許可を得られた範囲で公開する。

5.1 攻撃の流れ

本事例における攻撃の全体の流れについて図 6 に示す。

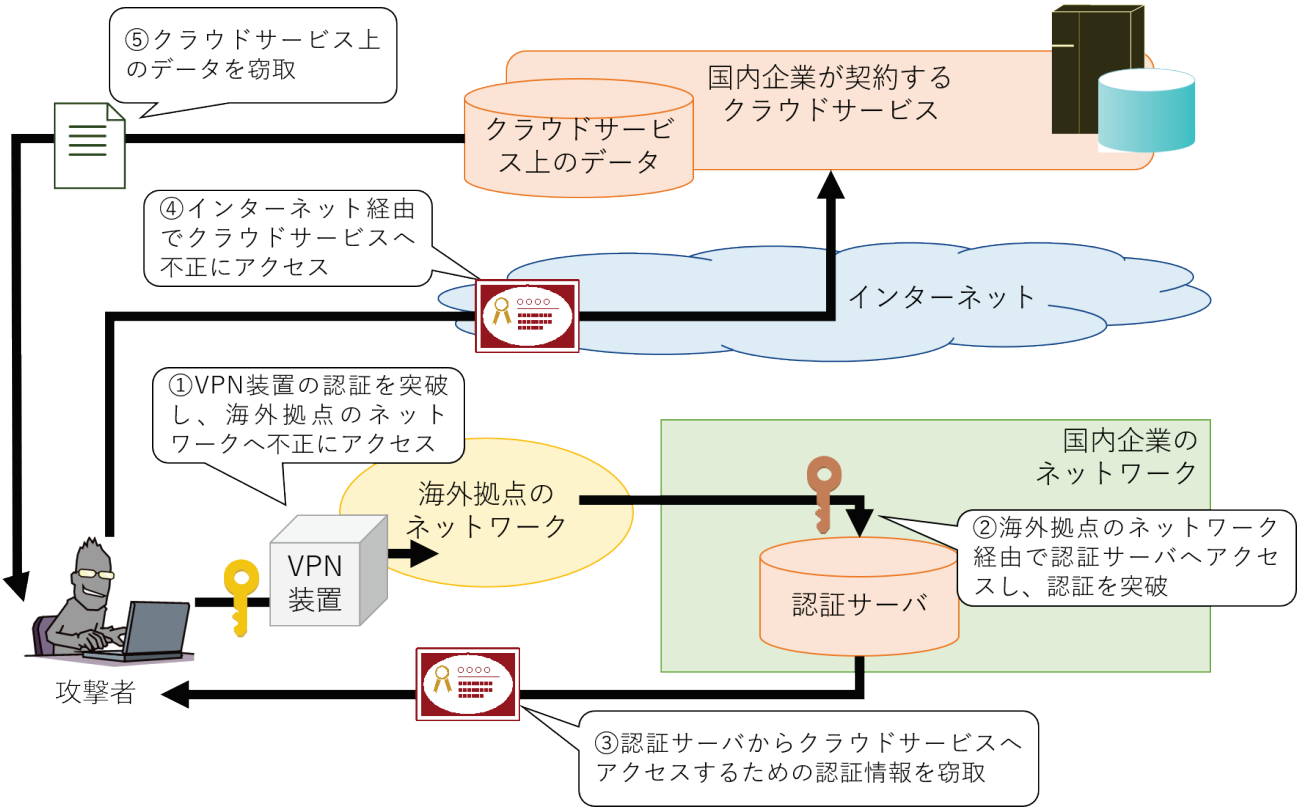


図 6 攻撃の流れ

攻撃者はまず海外拠点にあるネットワークへ不正アクセスするため、海外拠点に設置されている VPN 装置に対し、何らかの方法で入手した認証情報を使い認証を突破した（①）。海外拠点のネットワークに侵入した攻撃者は、そこから WAN で接続されている国内企業のネットワークに設置されている認証サーバに対し、何らかの方法で入手した正規の利用者の認証情報を用いて認証を突破し（②）、認証サーバからクラウドサービスへアクセスするための正規の認証情報を窃取した（③）。

窃取した認証情報を用い、攻撃者はインターネット経由でクラウドサービスへ不正にアクセスし（④）、クラウドサービス上の一部のデータを窃取した（⑤）。

5.2 不正アクセスの検知

本件では、クラウドサービスへの不正アクセスにおいて、攻撃者は組織内のネットワークを経由せず、直接インターネットからアクセスしていた。情報提供元企業はクラウドサービスへのアクセス状況を監視しており、不審な接続元からのアクセスを検知したことで発覚した。

また、クラウドサービスへの不正なアクセスは、脆弱性の悪用やウイルス等によるものではなく、利用者の正規の認証情報を使用していたため、不正アクセス元として情報提供された複数件の IP アドレスについて、本当に攻撃に使われたものか判断しかねるといったものも含まれていた。このような攻撃手口の場合、調査が難しくなることを示している。

5.3 まとめ

攻撃や侵入を完全に防ぐことは難しく、不審なアクティビティの監視（例：不審な接続元からのアクセスの監視、不審な操作の監視など）によって早期対処を図ることは、今後も重要な対策となると考えられる。

また、本件は VPN で海外拠点に侵入されたことが契機となっていると考えられる状況であった。経済産業省が 2020/12/18 に公開した注意喚起[11]においても、海外拠点から国際 VPN 等による WAN を経由した侵入について触れられている通り、類似する事例が複数確認されている。

海外拠点については、単純なセキュリティの強化による対策のみならず、様々な要因により完全なコントロールが難しいという性質を持つということに留意し、本社と海外拠点との接続やシステム統合の状態の再確認、リスクの把握、必要に応じたセキュリティ対策の見直しといった対応が、今後の課題となっていくであろう。

[11] 最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取組の強化に関する注意喚起を行います（経済産業省）
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

6 Microsoft Exchange Server の新たな脆弱性を悪用した攻撃

本四半期、Microsoft Exchange Server の新たな脆弱性[12]を悪用した攻撃を検知したという情報提供があった。当該企業ではグループ企業内で3社の攻撃の検知があったが、いずれもCVE-2021-26855の攻撃の試行が行われただけで、攻撃には失敗しており実被害はなかった。

本章では、当該脆弱性を悪用した攻撃について説明する。

発見の状況

2021 年 3 月 12 日、J-CSIP の参加組織から Microsoft Exchange Server の脆弱性である、CVE-2021-26855（別名:ProxyLogon）の攻撃の痕跡がグループ企業の 3 社で発見されたという情報提供があった。当該企業では、Microsoft 社が公開しているログ調査ツール[13]による調査を行い、当該脆弱性を悪用した攻撃の痕跡を発見した。なお、Webshell 等の悪意のあるファイルの設置、他の脆弱性の悪用による認証情報の窃取や不正なプログラムの実行等は確認されておらず、実被害はなかったとのことであった。

このとき 3 社で実施したログ調査ツールによる結果についても情報提供があった。参考として、各社の攻撃時期と攻撃で使われた User-Agent について、次に示す。

表 7 観測された攻撃時期

社名	ログ調査ツールの結果における攻撃時期
A 社	2021 年 3 月 8 日～3 月 10 日
B 社	2021 年 3 月 5 日～3 月 10 日
C 社	2021 年 3 月 3 日

表 8 観測された User-Agent

項番	User-Agent
1	Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/77.0.3865.90 Safari/537.36
3	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.81
4	CHIPs 20210303 scanner (contact asd.assist@defence.gov.au for further information)
5	ExchangeServicesClient/0.0.0.0
6	Hello-World
7	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
8	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML like Gecko) Chrome/69.0.3497.81 Safari/537.36
9	Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
10	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/60.0.3112.113 Safari/537.36

[12] HAFNIUM targeting Exchange Servers with 0-day exploits（Microsoft）
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[13] microsoft / CSS-Exchange
https://github.com/microsoft/CSS-Exchange/tree/main/Security

項番	User-Agent
11	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML　like Gecko) Chrome/74.0.3729.108 Safari/537.36
12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML　like Gecko) Chrome/77.0.3865.90 Safari/537.36
13	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML　like Gecko) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.81
14	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55
15	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
16	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML　like Gecko) Chrome/42.0.2223.0 Safari/537.36
17	Mozilla/5.0 zgrab/0.x

本脆弱性の状況

本件で確認された脆弱性は、2021 年 3 月 2 日（米国時間）に Microsoft 社から公開された Microsoft Exchange Server の複数の脆弱性の 1 つである。このうち 4 件の脆弱性については、実際の攻撃での悪用が確認されており、攻撃に成功するとサーバ上で任意のコード実行が可能となってしまう深刻なものであった。複数の攻撃者により悪用されているという点がセキュリティベンダから報告[14]されている他、本脆弱性は Microsoft 社が情報を公開する前から悪用されていた（ゼロデイ攻撃が行われていた）との情報があり、このような場合は、脆弱性の公開日から更に過去にさかのぼってログ等を調査をする必要がある。

また、本件の脆弱性についてはいくつかのセキュリティ関連機関等によってスキャンによる調査が行われていることが分かっている。本件の情報提供の中にも、攻撃であるのかセキュリティ関連機関によるスキャンであるのか不明であるが、オーストラリア政府によるスキャン行為の可能性のある User-Agent（表 8 の項番 4）が確認できる。スキャンを行う側による配慮といった点も今後の論点となりうるであろう。

なお、情報提供には攻撃元の IP アドレスとして 44 種のアドレスが存在したが、いずれも攻撃であるのかセキュリティ関連機関によるスキャンであるのかは不明であった。

脆弱性対策

本件も含め、脆弱性のあるソフトウェアに対する根本的な対策は、「修正プログラムの適用」や「脆弱性が対策されたバージョンへのアップグレード」である。本件の脆弱性では、すでにサポート切れのバージョンに対する修正プログラムの公開や、オンプレミス環境の緩和策[15]についても公開されており、重要性の高さが分かる。

本件はメールシステムに関する脆弱性であることから、業務上すぐに修正プログラムを適用することが難しい可能性があるが、攻撃者は待ってくれるわけではない。事前の脆弱性対応計画の策定、それに応じたリソースの確保等も必要である。

---

[14] Exchange servers under siege from at least 10 APT groups（ESET）
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[15] Exchange Server の脆弱性の緩和策（Microsoft）
https://msrc-blog.microsoft.com/2021/03/07/20210306_exchangeoob_mitigations/

7　本四半期で観測された特徴的なばらまき型メール

本四半期、参加組織から情報提供されたものの中にいくつか特徴的なフィッシングメールや不審メールがあった。これらのメールは、一見して不審であると見抜けるものもあるが、比較的日本語も不審な点が少なく、騙されてしまいそうなものもあった。

本章では、実際に情報提供された不審メールの例をいくつか説明する。

7.1 フィッシングメール

本四半期、情報提供されたフィッシングメールは、いくつか種類があった。それぞれの種類ごとに特徴のあるメールを示す。

Microsoft 365（Office 365）等アカウント情報の詐取を目的とするメール

本メールは Microsoft を騙り、ボイスメッセージの見逃しを装ったフィッシングメールである。添付ファイルを開くと、Microsoft 365 のログイン画面に似せたサイトが表示され、そこに ID とパスワードを入力すると詐取されるというものであった。

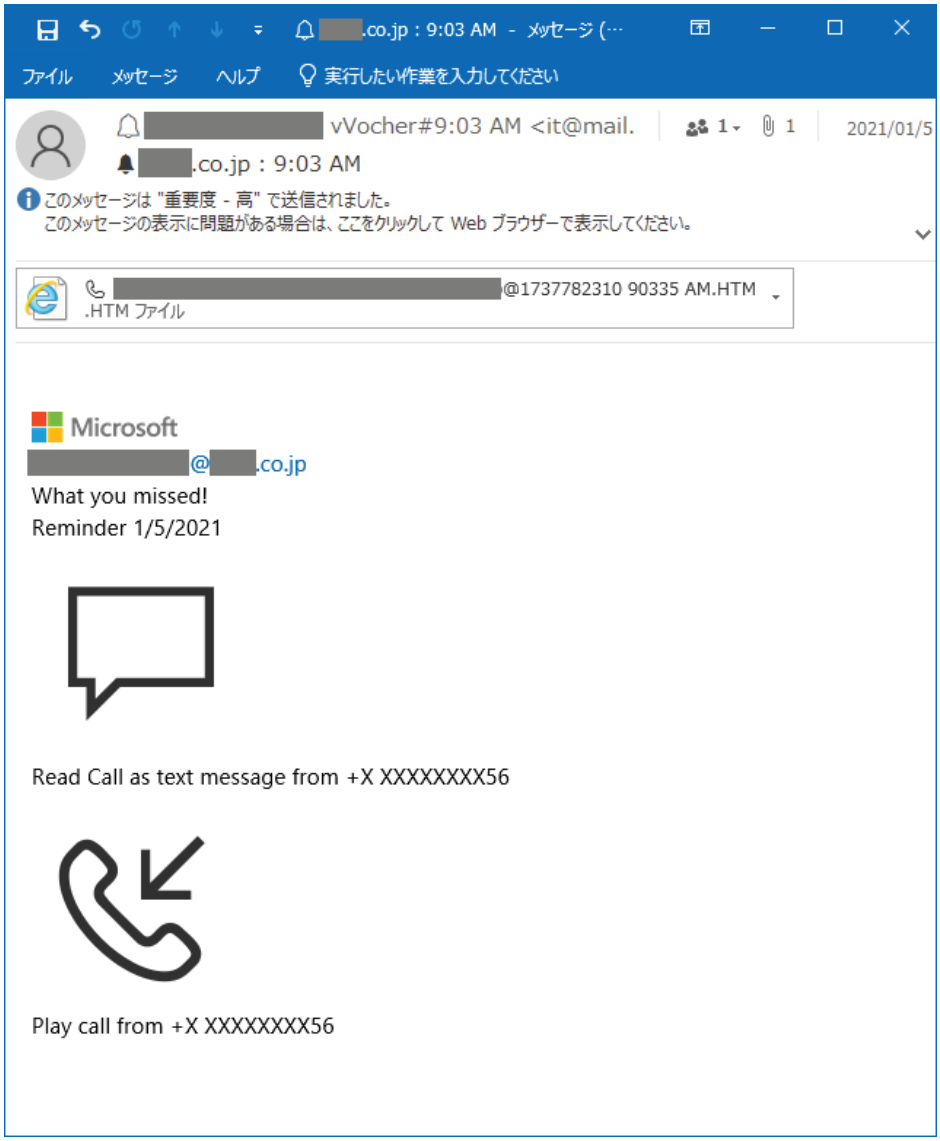


図　7 Microsoft を騙るフィッシングメール

EC サイトのアカウント情報の詐取を目的とするメール

本メールは Amazon を騙り、何者かに不正にアクセスされたと装い、登録情報の更新と称して偽のサイトへ誘導してアカウント情報を詐取するフィッシングメールである。Amazon の他、楽天等複数の EC サイトを詐称したフィッシングメールが公開情報でも多数見られる。

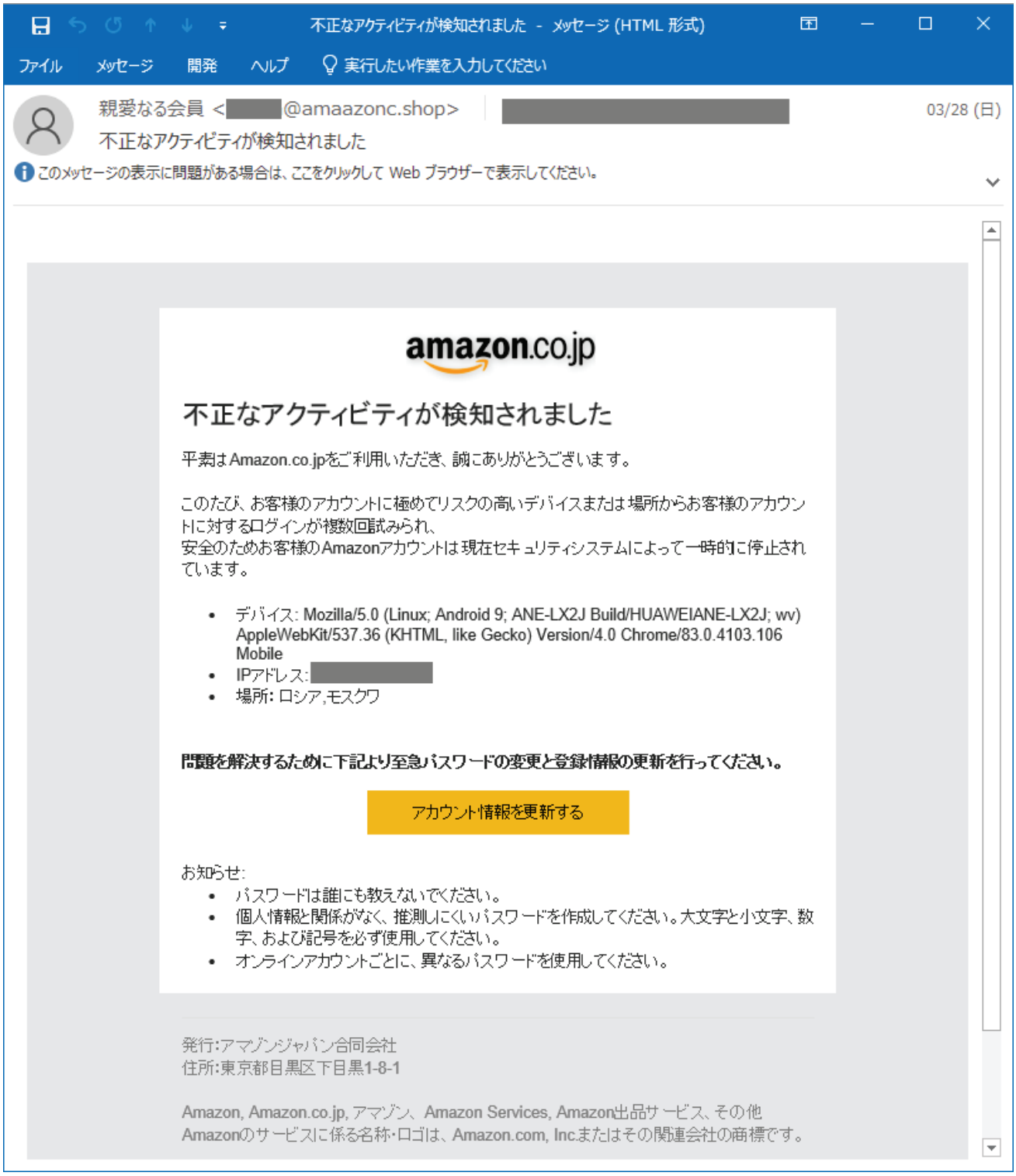


図 8 Amazon を騙るフィッシングメール

配送エラーを装いアカウント情報の詐取や金銭窃取を目的とするメール

宅配業者等からのメールを装い、配送遅延や配送手続きの情報確認のためといった理由で偽のサイトへ誘導し、アカウント情報の詐取や、クレジットカード情報等を入力させるフィッシングメールがある。

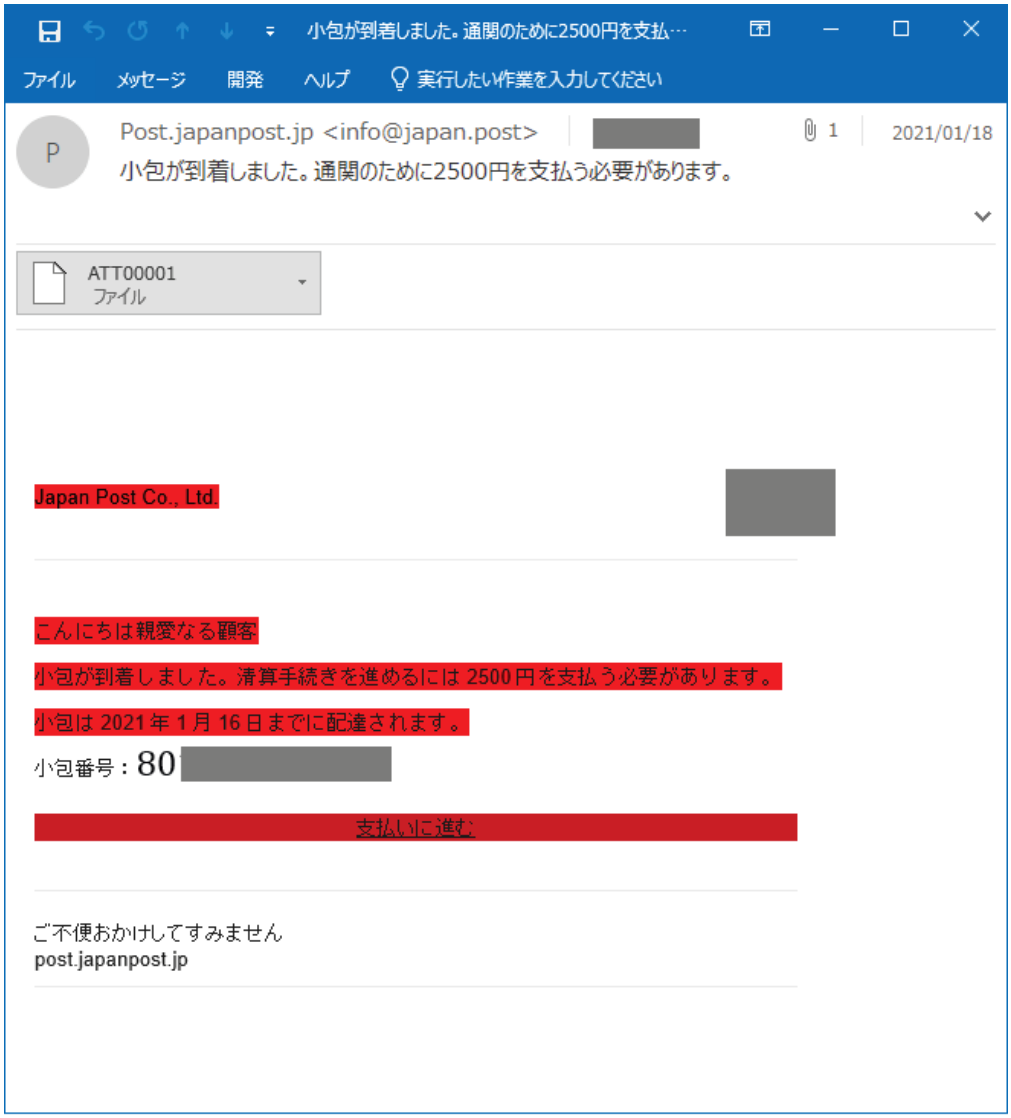
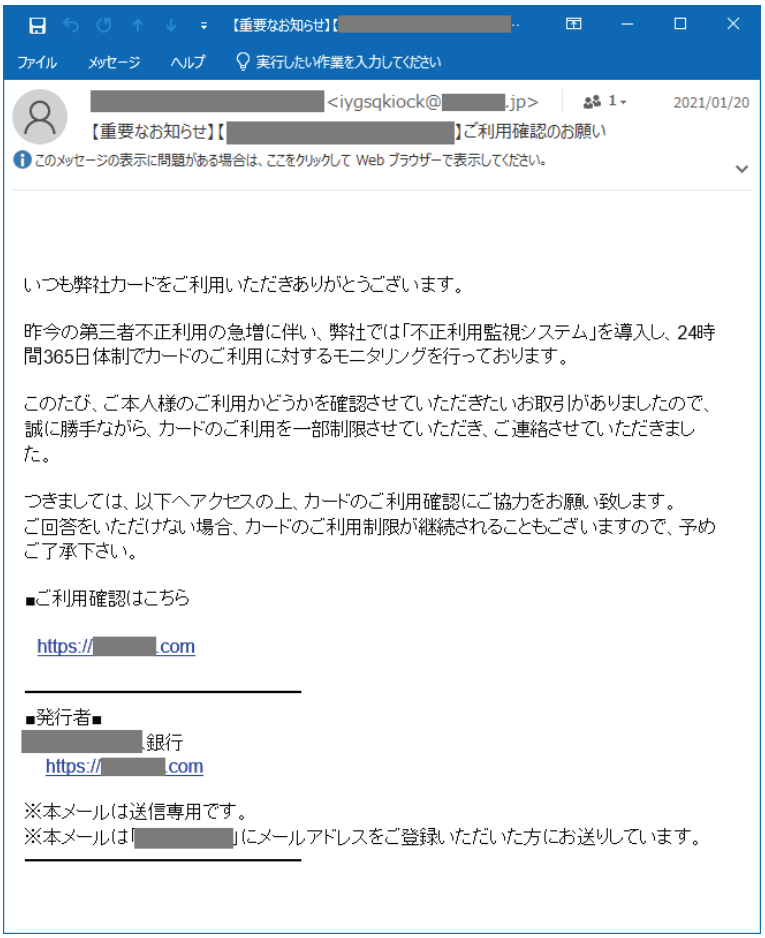


図 9 日本郵便を騙るフィッシングメール

クレジットカード情報による金銭窃取を目的とするメール

クレジットカード会社等になりすまし、何らかの理由を付けてクレジットカード情報を入力させる偽サイトへ誘導するフィッシングメールがある。このようなフィッシングメールは公開情報でも多数見られるものであり、比較的偽物であると気づきやすいと思われるが、中には偽物と分かりにくいものもある。次のメールは第三者の不正利用の疑いがあることを装い、偽のサイトへ誘導させようとしている。


【重要なお知らせ】【[redacted]
ファイル　メッセージ　ヘルプ　実行したい作業を入力してください
[redacted]<iygsqkiock@[redacted].jp>　1　2021/01/20
【重要なお知らせ】【[redacted]】ご利用確認のお願い
このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。

いつも弊社カードをご利用いただきありがとうございます。

昨今の第三者不正利用の急増に伴い、弊社では「不正利用監視システム」を導入し、24時間365日体制でカードのご利用に対するモニタリングを行っております。

このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。

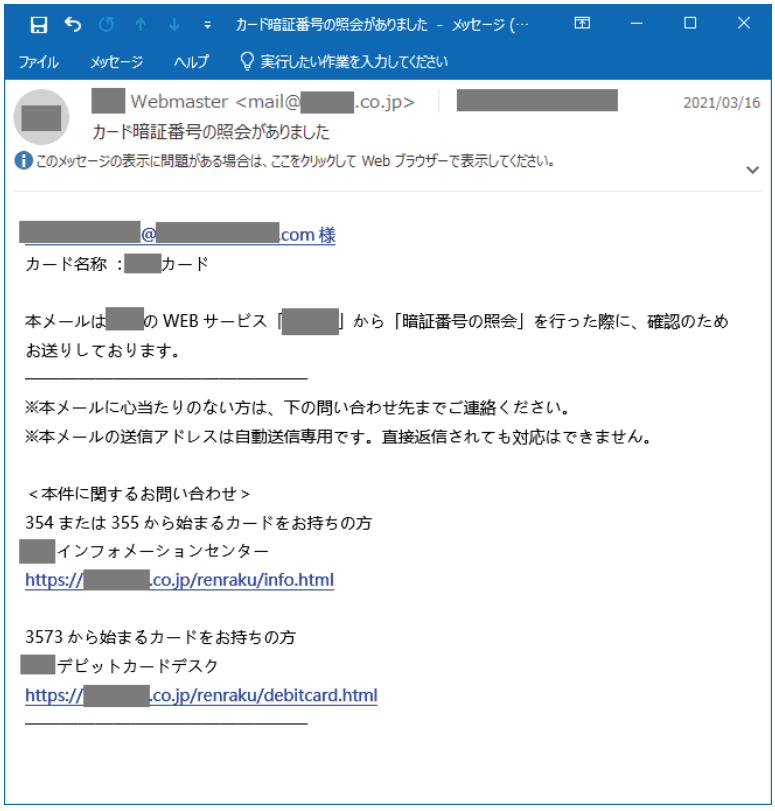
■ご利用確認はこちら

https://[redacted].com

■発行者■
[redacted]銀行
https://[redacted].com

※本メールは送信専用です。
※本メールは[redacted]にメールアドレスをご登録いただいた方にお送りしています。

図 10 銀行を騙るフィッシングメール


カード暗証番号の照会がありました - メッセージ (…
ファイル　メッセージ　ヘルプ　実行したい作業を入力してください
[redacted] Webmaster <mail@[redacted].co.jp>　[redacted]　2021/03/16
カード暗証番号の照会がありました
このメッセージの表示に問題がある場合は、ここをクリックして Web ブラウザーで表示してください。

[redacted]@[redacted].com 様
カード名称 ：[redacted]カード

本メールは[redacted]の WEB サービス「[redacted]」から「暗証番号の照会」を行った際に、確認のためお送りしております。

※本メールに心当たりのない方は、下の問い合わせ先までご連絡ください。
※本メールの送信アドレスは自動送信専用です。直接返信されても対応はできません。

＜本件に関するお問い合わせ＞
354 または 355 から始まるカードをお持ちの方
[redacted]インフォメーションセンター
https://[redacted].co.jp/renraku/info.html

3573 から始まるカードをお持ちの方
[redacted]デビットカードデスク
https://[redacted].co.jp/renraku/debitcard.html

図 11 クレジットカード会社を騙るフィッシングメール

また、このようなフィッシングメールは、本文が定型化されていることも考えられる。次の図 12 と図 13 は別のクレジットカード会社を装うフィッシングメールであるが、メール本文の内容はほぼ同一の内容が書かれている。

図 12 クレジット会社を騙るフィッシングメール

図 13 クレジット会社を騙るフィッシングメール

メールサーバの不具合を装いアカウント情報の詐取を目的とするメール

メールサーバの何らかの不具合を装い、エラー内容の確認等を装って偽のサイトへ誘導させるフィッシングメールがある。このようなメールも一般の利用者が管理者から送られてきたものと誤認してしまえば不審サイトで認証情報を入力してしまう恐れがあるだろう。

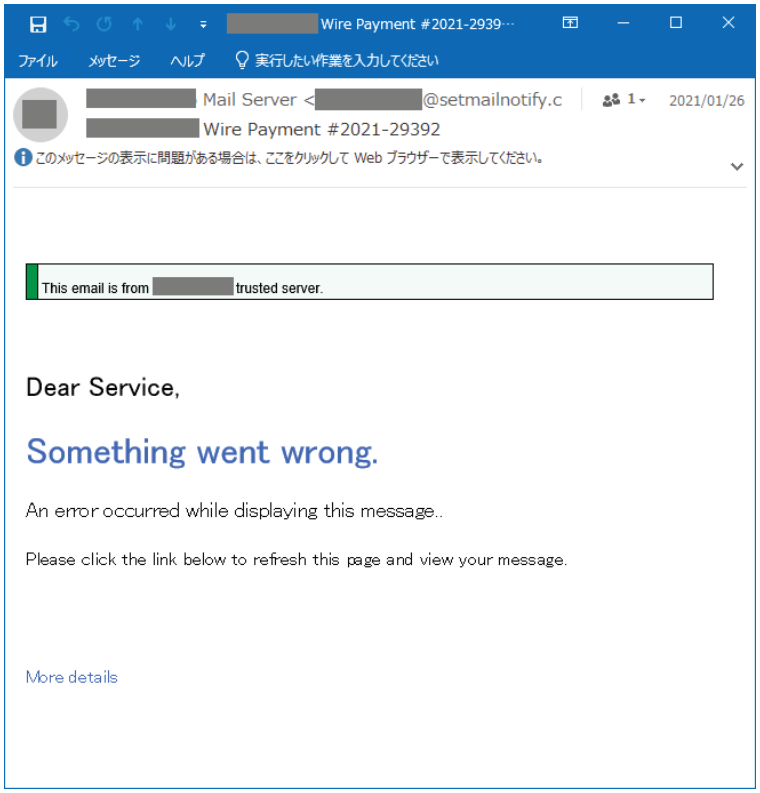


図 14 メールサーバからのエラーを装うフィッシングメール

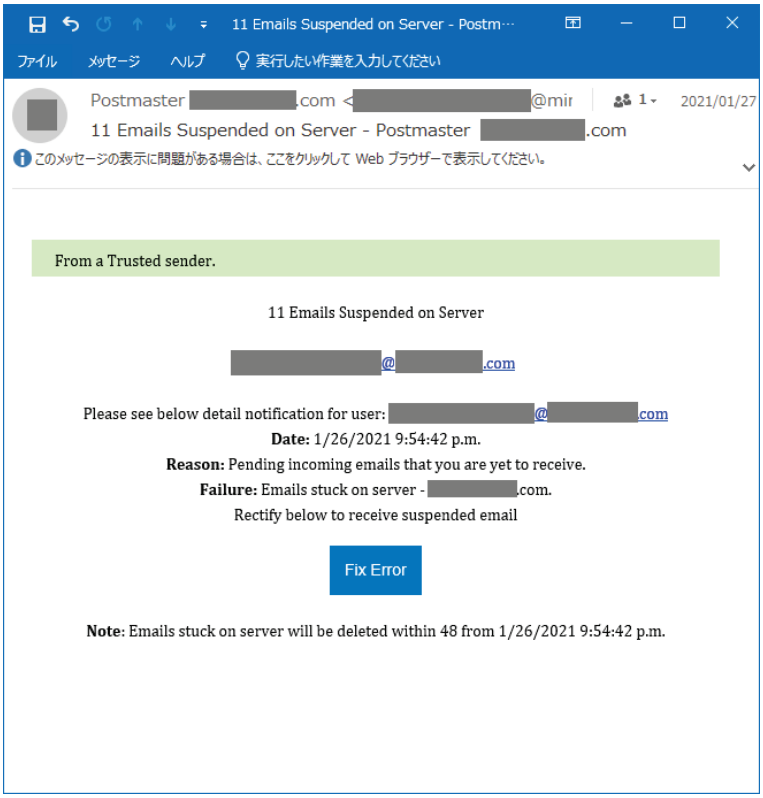


図 15 メールサーバからのエラーを装うフィッシングメール

7.2 セキュリティソフトの期限切れを装った不審メール

本メールは、Norton のサブスクリプションの期限切れ通知を装い、サブスクリプションの継続のためという理由で偽のサイトへアクセスさせようとするものである。メール本文中の URL リンク先へアクセスすると、図 17 の画面のサイトへアクセスする。このサイトではウイルスが検出されたと偽の画像が張り付けられており、画像をクリックすると別のサイトへ転送される仕組みとなっていた。IPA で調査した際には転送先のサイトへのアクセスが不可となっており、転送先でどのようなサイトが運用されていたかは不明である。

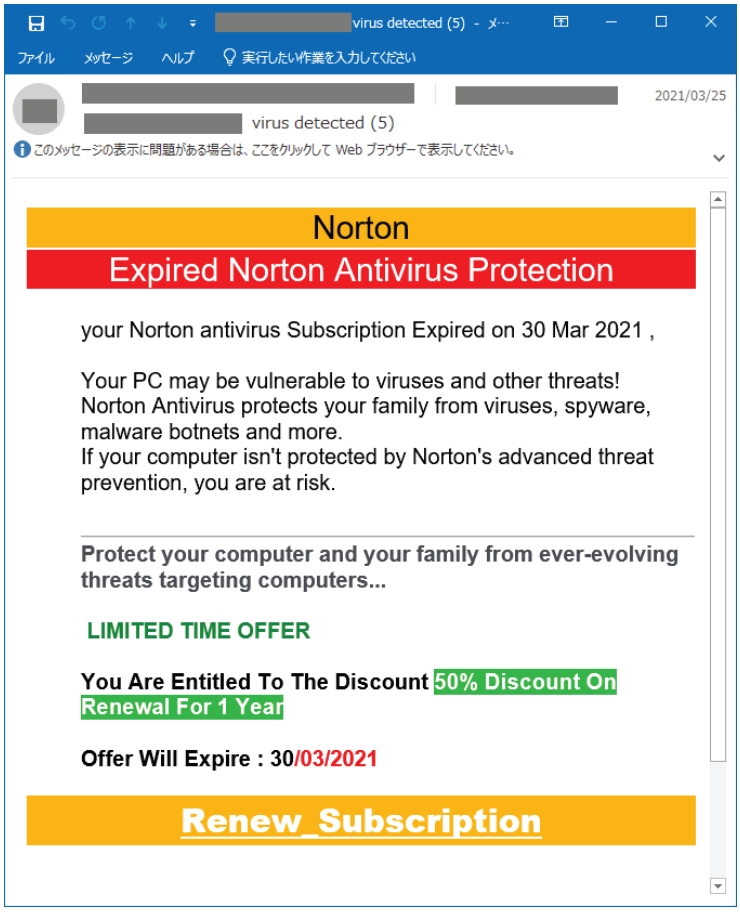


図 16 Norton のサブスクリプション期限切れを装う不審メール

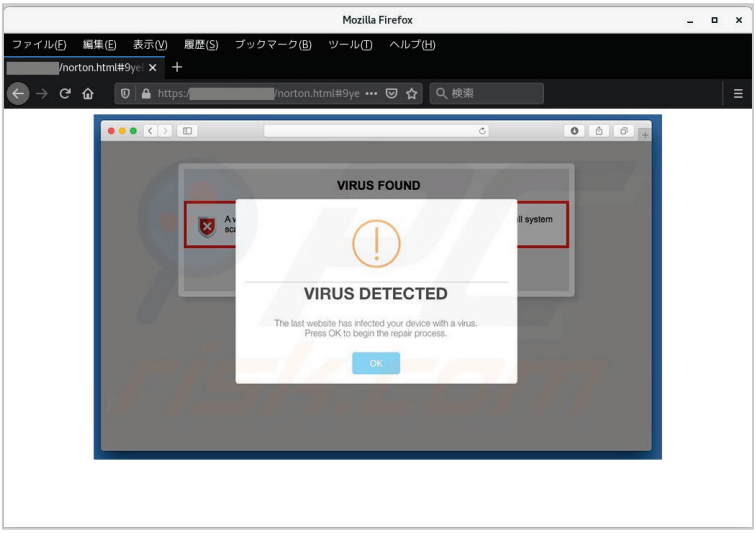


図 17 本文 URL リンク先の不審サイト

7.3 まとめ

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。より詳しくは、フィッシング対策協議会のウェブサイト[16]等も併せて参照いただきたい。

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。少しでも不審と感じたメールについては社内で相談・報告する窓口を設けておくといったことも重要である。

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

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