サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2021 年 10 月～12 月]

2022 年 1 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 12 月末時点の運用体制、2021 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

2021 年 10 月～12 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）の体制となっている（図 1）。

- 2021 年 11 月、化学業界 SIG 内での加入に伴い、参加組織数が 23 組織から 24 組織となった。
- 2021 年 12 月、ガス業界 SIG 内での退会に伴い、参加組織数が 63 組織から 62 組織となった。

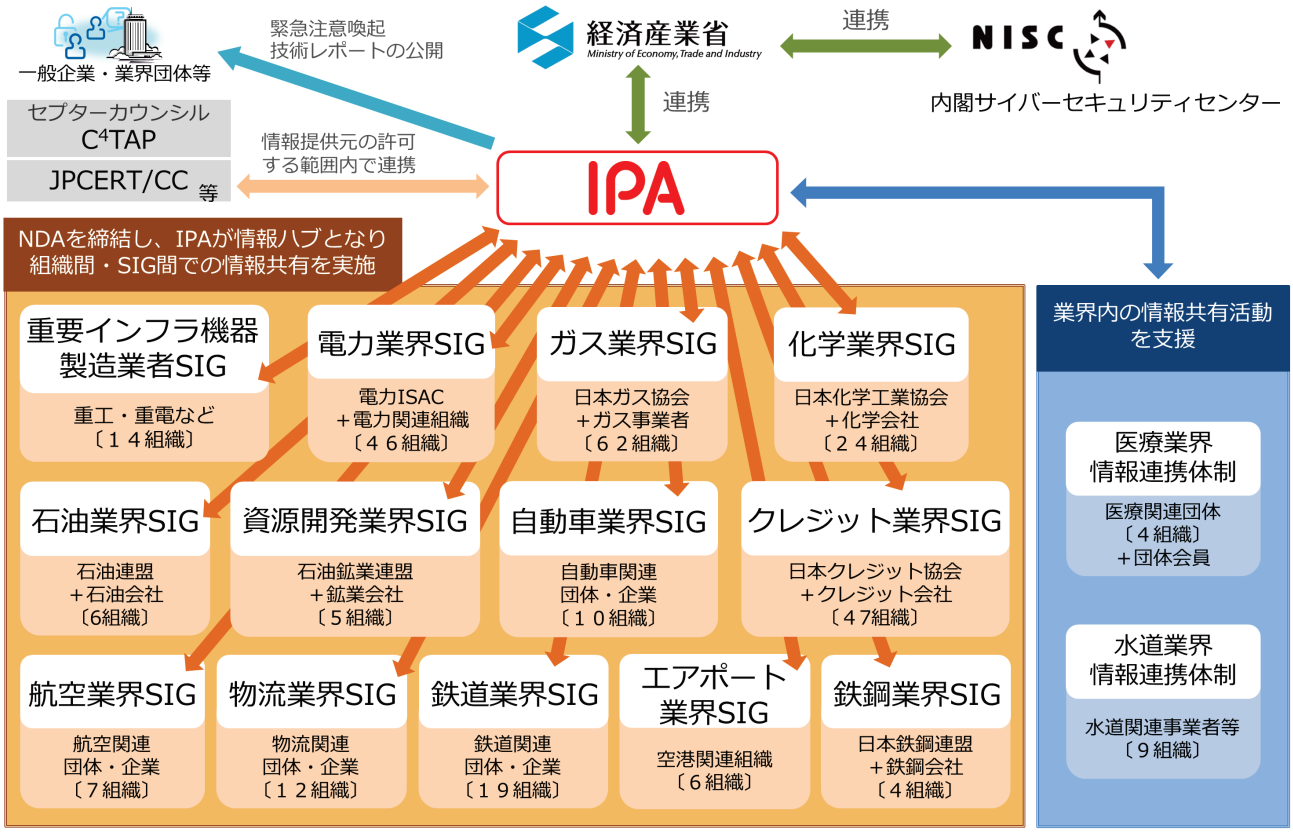


図 1 J-CSIP の体制図

[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 10 月～12 月）

2021 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 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	2021 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	410 件	369 件	346 件	**77 件**
2	参加組織への情報共有実施件数※1	25 件	40 件	21 件	**28 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 **21 件**を含む。

本四半期は情報提供件数が **77 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 **5 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。この中には取引先を詐称するもの（タイプ 1）と、経営層を詐称するもの（タイプ 2）があった。これらについて 3 章で述べる。

- 日本企業の海外関連会社から送られてきたと考えられ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。メールの添付ファイルを開くと、偽のログイン画面が表示されるが、その際に攻撃対象の企業のロゴを表示するような仕掛けがあった。これについて 4 章で述べる。

- 参加組織において、導入しているセキュリティ製品によって検知したウイルスメールやフィッシングメールについて情報提供があった。特段巧妙な攻撃ではないが、日常組織へ着信する攻撃メールについても J-CSIP で取り扱っている。これについて 5 章で述べる。

- 本四半期、Emotet への感染を企図した攻撃メールが公開情報上で観測された。IPA でそれらの情報をまとめ、共有したところ、J-CSIP の参加組織内でも観測された。これについて 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	海外の関連企業にて、Microsoft Exchange Server の脆弱性を悪用した攻撃を受けた。	1 件
2	Apache Log4j の脆弱性におけるバージョン 1 系の深刻度についての相談。	1 件
3	ランサムウェア被害を受けた組織から情報漏洩の可能性があると連絡を受けた際に、自組織内でどのような対応をするかの相談。	1 件
4	約 1 時間の間に 900 通ほどのフィッシングメールを受信した。	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。	1 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、サーバ内に設置された不正なファイル（ウェブシェル等）の実行を EDR 製品によって検知したと情報提供を受けたものである。なお、本攻撃では当該企業のネットワーク内へ侵入後、PowerShell スクリプトをダウンロードして実行しようとしたとの痕跡も確認している。情報提供元組織によると、事前に脆弱性のパッチ適用について周知していたが、当該企業の判断でパッチ適用が遅れていたとのことであった。本脆弱性については、継続して J-CSIP 内でも悪用の痕跡が確認されているため、パッチが未適用の場合は早急な適用の検討をしてほしい。

項番 2 は、Apache Log4j の脆弱性に対して組織として脆弱性対策を進めているが、バージョン 1 系への影響の詳細について相談したいというものであった。相談元組織ではバージョン 2 系への対応を進めている中でバージョン 1 系についても 2 系と同様のレベルで対策を行っていく必要があるのかを危惧していた。
Apache Log4j の 1 系はすでに End Of Life を迎えており、さらに同脆弱性による影響があることが開発者のサイトで確認されている。脆弱性の対応については、開発元のサイトを確認しつつ、組織内で導入しているバージョンに影響がないか、また可能な限り最新のバージョンへのアップデート等も検討してほしい。

項番 3 は、ある関連組織にてランサムウェアによる被害を受けたと連絡があり、組織内での対応について相談したいというものであった。相談元組織では、当該被害組織と関係があり連絡を受けたが、当該連絡の中では情報漏洩の可能性は低く、情報漏洩があったとしてもメールアドレスだけであろうということであった。これについて、何らか対応が必要ではないかと心配しての相談である。残念ながら、ランサムウェアをはじめ、サイバー攻撃によって情報が漏洩した場合には、組織として対応できることは限られる。攻撃者や悪意のある者の手にその情報が渡ったという前提で、対応を検討するといったこととなろう。

項番 4 は、J-CSIP 参加組織のグループ企業宛に、約 1 時間の間に同じ内容のフィッシングメールが 900 通程受信したと情報提供を受けたものである。なお、メールは組織のセキュリティソフトにて検疫されており、実被害はなかったとのことである。このフィッシングメールは Microsoft 365 のアカウント情報詐取を企図したものであった。Microsoft 365 のアカウント情報を狙ったフィッシングメールは多数観測しており、J-CSIP の運用状況レポートでも度々紹介している。このような攻撃は、騙された利用者のアカウントを通じ、企業・組織内の情報等が侵害される可能性をもたらす脅威であり、注意が必要である。フィッシング詐欺への対策は、二要素認証の導入のほか、利用者一人ひとりが、騙されないよう手口を知ることが重要である。

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あり、同様の情報提供・相談が継続している。調査の結果、ウェブでの検索中に悪意のある仕掛けのあるページを開いたものであった。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 3 件のビジネスメール詐欺について情報提供を受けた。これらのうちタイプ 1（取引先との請求書の偽装）は 1 件、タイプ 2（経営者等へのなりすまし）は 2 件であった。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相談があった。

本章では、開示許可の得られた 3 つの事例について詳しく説明する。

3.1 経営者を騙る日本語の攻撃

本事例は、2021 年 10 月、J-CSIP の参加組織の複数の役員に対し、同社の代表取締役になりすました攻撃者から、約 2 時間の間に 17 通の偽のメールが送られたと情報提供があったものである。

この手口は、IPA が 2017 年 4 月に公開した注意喚起レポートで紹介しているビジネスメール詐欺の 5 つのタイプのうち、「タイプ 2:経営者等へのなりすまし」に該当する。

本事例で、攻撃者から送られたメールを図 2 に示す。

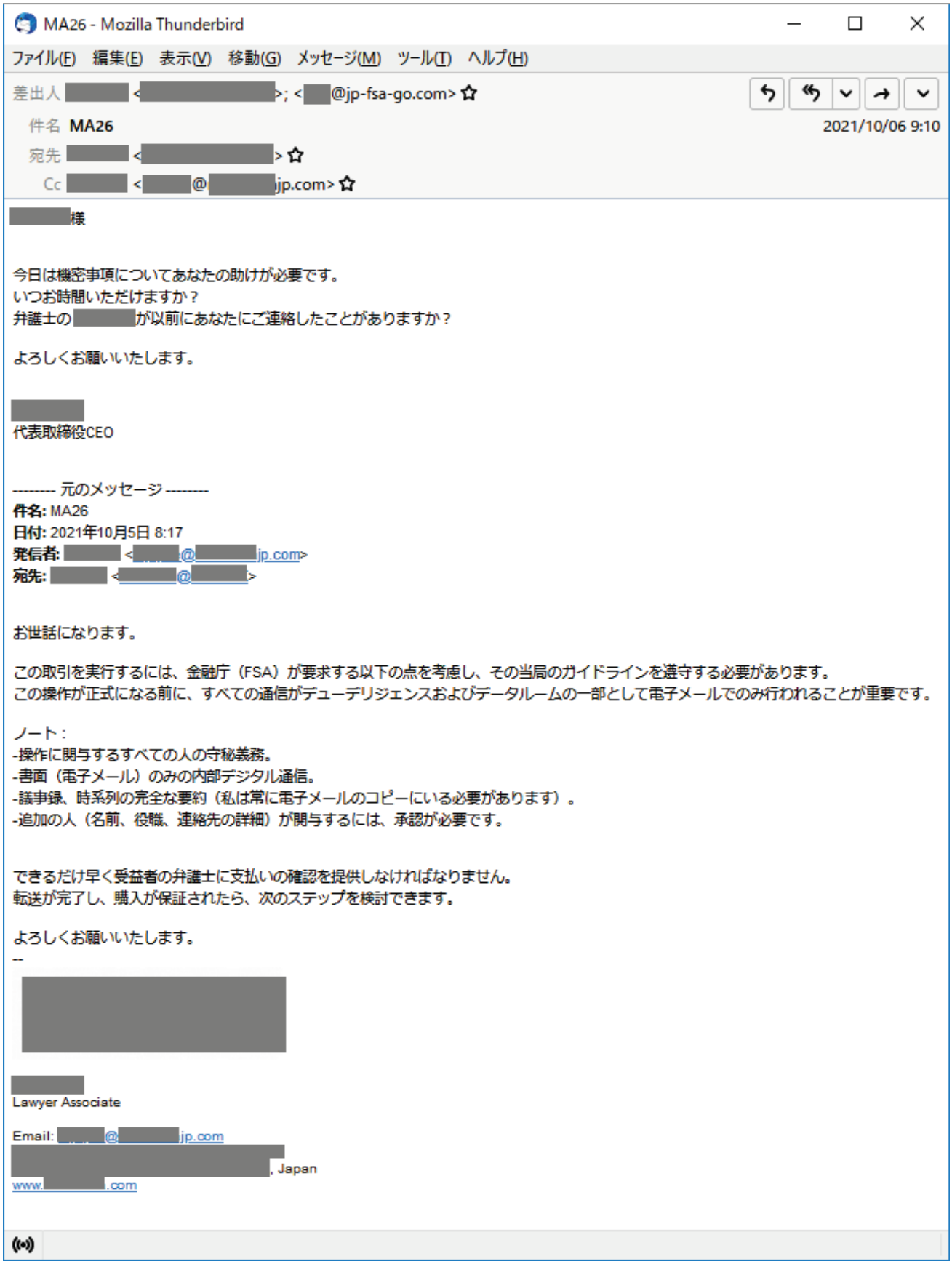
攻撃者から送られた偽のメールは日本語であり、機密事項について助けが必要だという内容で、返信を依頼するようなものであった。メールの下部には実在する日本の弁護士事務所の弁護士から連絡があったように見せかける偽の内容が記載されていた。

本メールの差出人のメールアドレスには、日本の金融庁のドメインに似た偽のメールアドレスも記載されており、この偽のメールアドレスへ返信されるように細工されていた。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。

このメールについては、2018 年 8 月に公開したビジネスメール詐欺(続報)[4]のレポート事例 1 と同じ手口であり、継続して類似した攻撃が行われているものと推測している。

ビジネスメール詐欺のメールは、英語のやりとりで多く見られるものであるが、本事例は日本語で書かれた偽のメールであるため、普段英語のメールでやりとりを行わないような企業や組織であったとしても、攻撃メールが着信する可能性があり、引き続き注意が必要である。

[4] 【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


MA26 - 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 [redacted] <[redacted]>; <[redacted]@jp-fsa-go.com>

件名 MA26

2021/10/06 9:10

宛先 [redacted] <[redacted]>

Cc [redacted] <[redacted]@[redacted]jp.com>

[redacted]様

今日は機密事項についてあなたの助けが必要です。
いつお時間いただけますか？
弁護士の[redacted]が以前にあなたにご連絡したことがありますか？

よろしくお願いいたします。

[redacted]
代表取締役CEO

-------- 元のメッセージ --------
件名: MA26
日付: 2021年10月5日 8:17
発信者: [redacted] <[redacted]@[redacted]jp.com>
宛先: [redacted] <[redacted]@[redacted]>

お世話になります。

この取引を実行するには、金融庁（FSA）が要求する以下の点を考慮し、その当局のガイドラインを遵守する必要があります。
この操作が正式になる前に、すべての通信がデューデリジェンスおよびデータルームの一部として電子メールでのみ行われることが重要です。

ノート：
-操作に関与するすべての人の守秘義務。
-書面（電子メール）のみの内部デジタル通信。
-議事録、時系列の完全な要約（私は常に電子メールのコピーにいる必要があります）。
-追加の人（名前、役職、連絡先の詳細）が関与するには、承認が必要です。

できるだけ早く受益者の弁護士に支払いの確認を提供しなければなりません。
転送が完了し、購入が保証されたら、次のステップを検討できます。

よろしくお願いいたします。
--

[redacted]
Lawyer Associate

Email: [redacted]@[redacted]jp.com
[redacted], Japan
www.[redacted].com

図 2 攻撃者から送られた偽のメール

3.2 経営者を騙る英語の攻撃

本事例は、2021 年 10 月、J-CSIP の参加組織の人事部門の担当者に対し、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 3 に示す。本メールは英語であった。

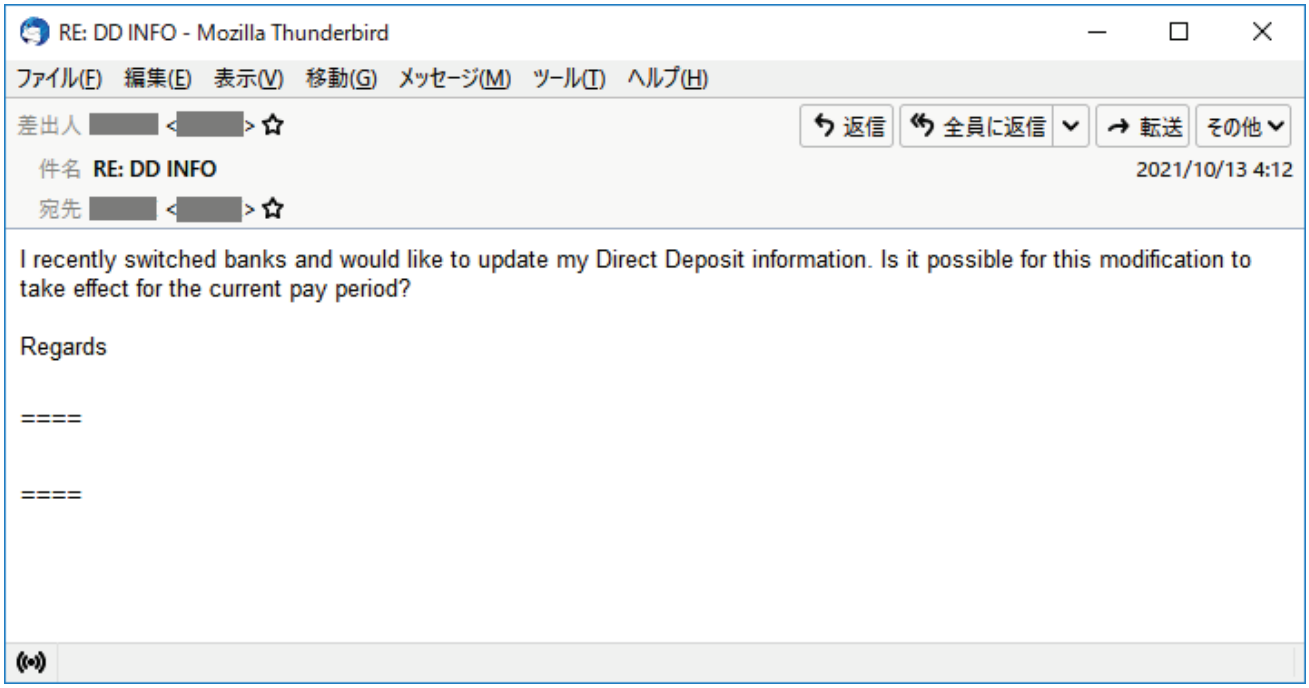


図 3 攻撃者から送られた偽のメール

攻撃者から送られた偽のメールには、給与振り込みの銀行を変更したため口座情報を更新したいといった内容が記載されていた。このような給与振込先の変更を装う攻撃手口について、近年増加傾向にあるという情報[5]が公開されており、注意が必要である。

本件のメールでは、差出人のメールアドレスには情報提供元の役員の正規のメールアドレスが設定されていたが、Envelope-From[6]には、攻撃者のものと思われる偽のメールアドレスが設定されていた。これによって、メールソフトでは正規の役員のメールアドレスが表示されるため、あたかも本物の相手からメールが送られてきたように細工している。

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。

---

[5] Phishing Activity Trends Reports 2nd Quarter 2021(APWG)
https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf

[6] メールの差出人にあたる。配送エラー時のエラーメールの返信先のほか、送信されたメールの返信先となる。

3.3 国内企業を狙った攻撃

本事例は、2021 年 9 月、J-CSIP 参加組織（A 社）の担当者に対し、海外の取引先企業（B 社）の担当者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 1:取引先との請求書の偽装」に該当する。

この事例では、A 社の担当者が攻撃者へメールの返信を行ってしまったものの、電話にて返信メールの着信確認を行ったため、金銭的な被害はなかった。

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) A 社と B 社のやりとりへ介入
(2) 正規のメールアドレスに似せた偽のメールアドレス

(1)A 社と B 社のやりとりへ介入

本件のやりとりの流れを図 4 に示す。

A 社（国内組織）と B 社（海外取引先）との間で、取引に係るビジネスメールをやりとりしている中で、2021 年 9 月 15 日、B 社から A 社へ正規の支払いに関するメールを送付した。その後、2021 年 9 月 17 日に攻撃者から A 社担当者へ偽のメール（図 5）が送られた。この偽のメールには、過去の A 社と B 社がやりとりを行っていた件名が使われており、メールの本文には支払先の銀行口座の変更を要求する内容が記載されていた。

このメールを受け取った A 社の担当者は不審に思い、「この内容に見覚えがあるか」という趣旨のメールを返信したが、そのメールの宛先を、攻撃者の偽のメールアドレス宛としてしまっていた。メールの返信後、さらに A 社担当者は B 社の担当者へ電話にて返信したメールが届いているか確認をしたところ、B 社担当者はメールを受け取っていないことが分かり、偽のメールアドレス宛に送っていたことにも気づいたため、詐欺であることが発覚した。

詐欺の発覚後、同日中に攻撃者から A 社の担当者へ「経理部門へ支払いを一旦停止するように指示してほしい」という内容のメール（図 6）が送られたが、偽のメールであると認識していたため、A 社担当者はメールへの返信は行わなかった。

本事例のように、不審なメールに対し、返信を行った後に、電話にて着信確認を行うといったことで偽のメールに気づける場合がある。ただし、メールに書かれている電話番号等は攻撃者によって改変されていることもあるため、必ず信頼のおける方法で入手した連絡先を使っていただきたい。

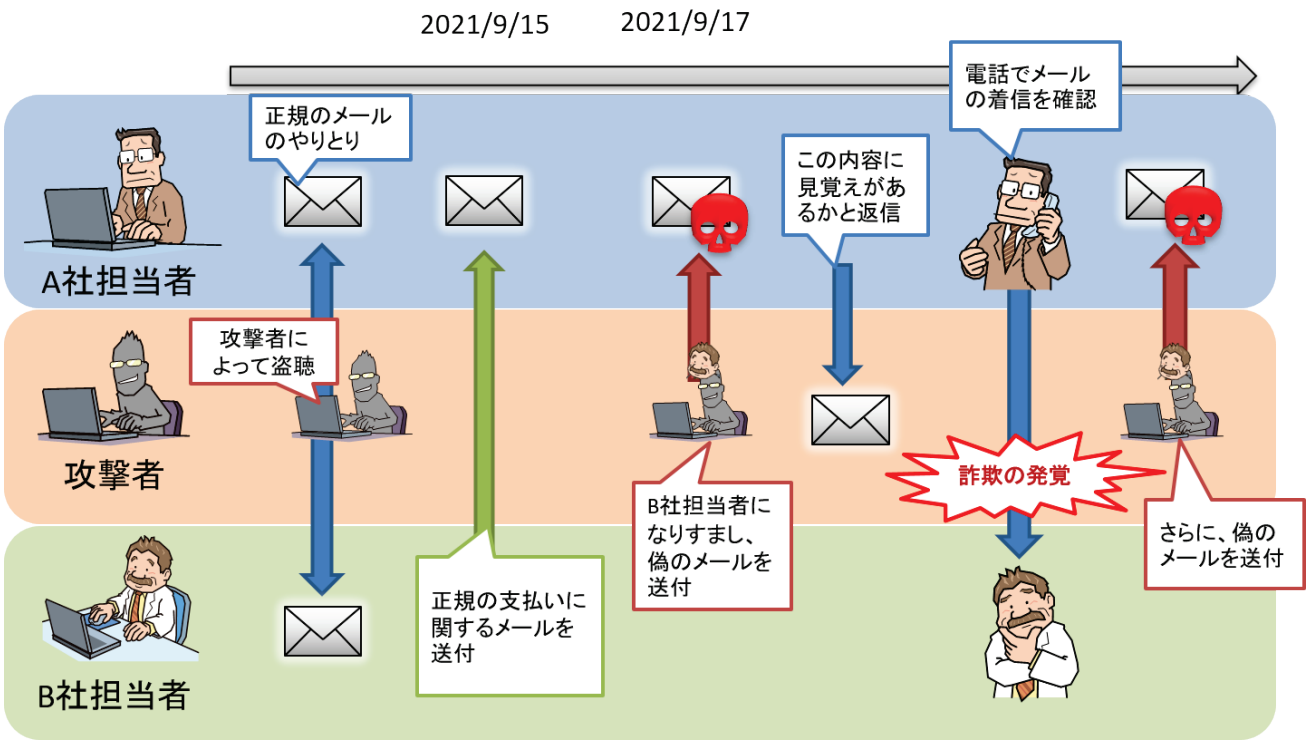


図 4 事例 3:攻撃者とのやりとり

図 5 攻撃者からのメール(1 通目)

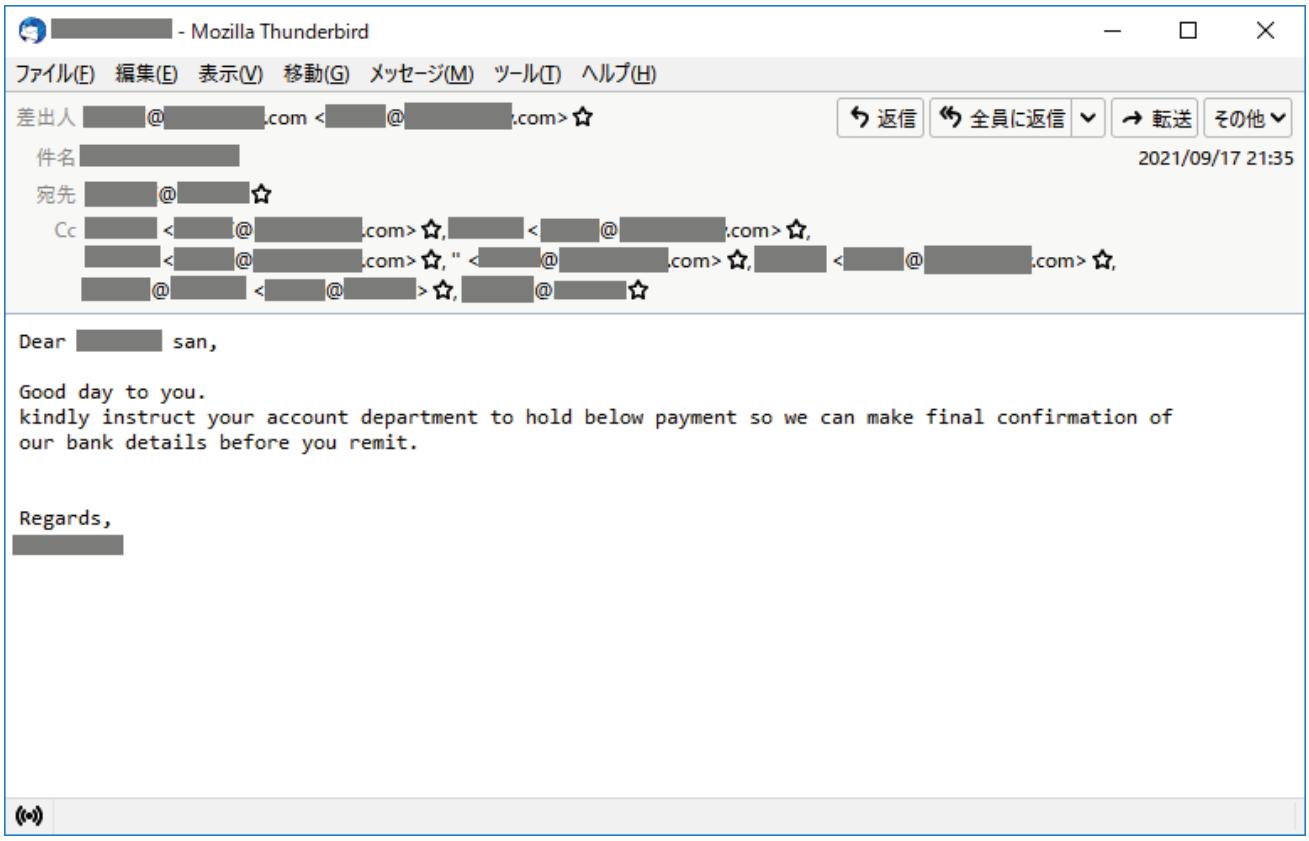


図 6 攻撃者からのメール(2 通目)

(2)正規のメールアドレスに似せた偽メールアドレス

攻撃者からA社担当者へ送られたなりすましメールでは、B社の正規のメールアドレスに似せた偽のメールアドレスが使われていた。

この偽のメールアドレスは、次の例に示すようなものであった。

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

※実際に悪用されたものとは異なる。

この偽のメールアドレスは、同報先(CC)に指定されていた、B社の関係者のメールアドレスもすべて改変されて悪用されていた。

4　日本企業の海外関連企業から送られたフィッシングメールの事例

本四半期、J-CSIP の参加組織より、国内企業の海外関連企業から送られてきたという不審なメールの情報提供があった。

当該メールを確認したところ、実在する国内企業の海外関連企業から送られてきたものであり、メールは Microsoft 365 の認証情報の詐取を企図したフィッシングメールであった。このフィッシングメールに添付されたファイルによって表示される偽のログイン画面では、受信者のメールアドレスのドメインによって企業のロゴを表示するような仕掛けがされていた。

当該メールについて J-CSIP 内で情報共有を行ったところ、他の参加組織でも同様の攻撃メールが観測されており、また公開情報でも、類似した攻撃メールを確認したため、ある程度ばらまかれているものと考えている。

本章では、当該フィッシングメールの例とともに、偽のログイン画面の攻撃手口について説明する。

攻撃メール

本件のフィッシングメールを図 7 に示す。

このメールの差出人（From）メールアドレスや、メール本文中の署名、メールの配送経路を確認したところ、実在する国内企業の海外関連企業から送られているように思われたため、当該国内企業へ IPA から確認を行った。すると、送信元となっていた海外関連企業のメールアカウントが、不正アクセスによって何者かに乗っ取られ、不正にメールがばらまかれていたということが判明した。

攻撃メール自体は巧妙なものではないが、本物のメールアカウントが乗っ取られて送られてきていることから、迷惑メールフィルタ等では対処できない可能性がある。フィッシング攻撃の手口の理解や、不審メールの添付ファイルは開かないといった基本的なセキュリティ対策を徹底していただきたい。

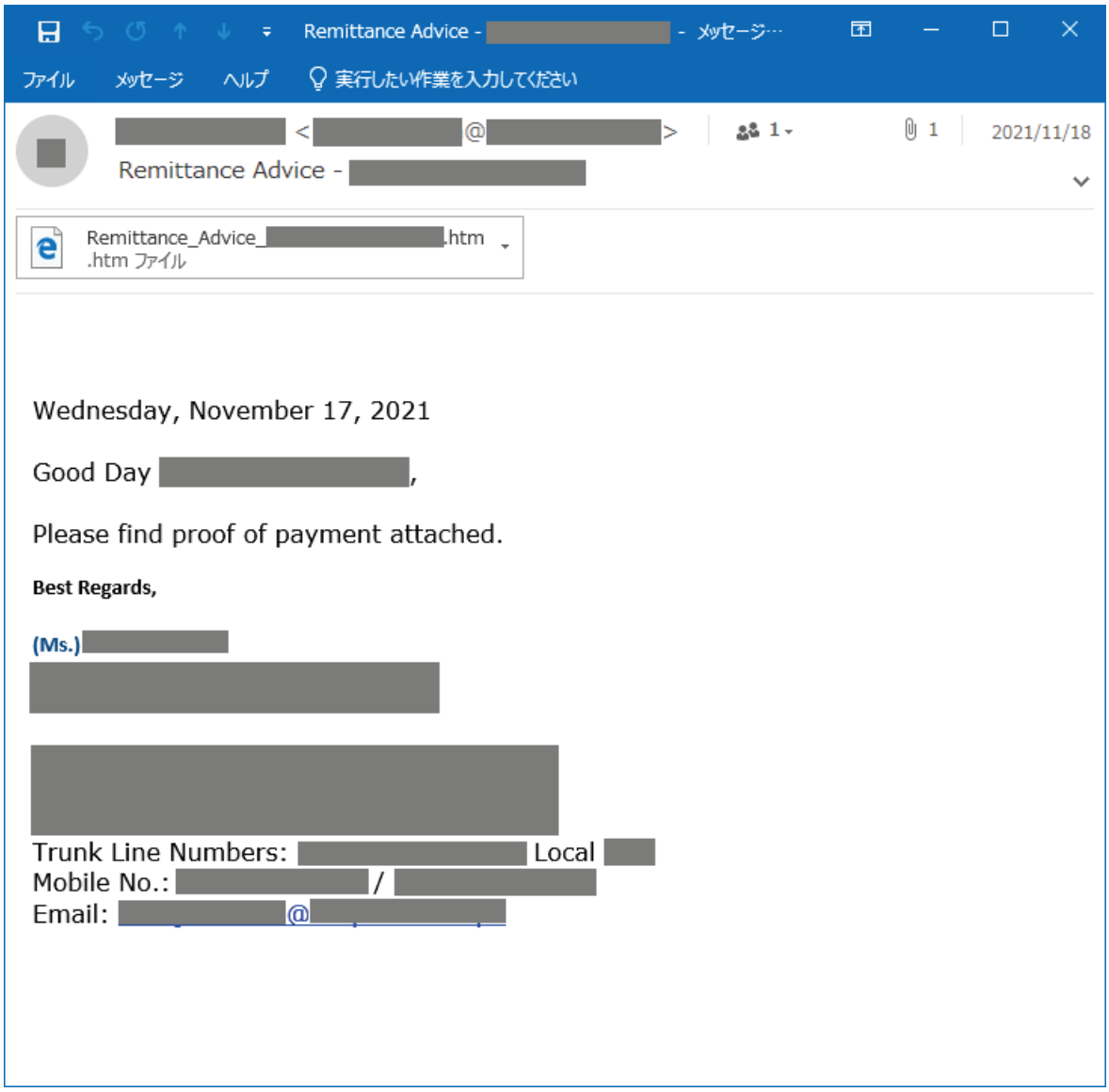


図 7 実際に送られてきたフィッシングメール

偽のログイン画面の手口

本件のフィッシングメールには HTML ファイルが添付されていた。当該ファイルを開くと、ウェブブラウザが起動して内容が表示される。HTML ファイル内に書かれた悪意のあるコードは、不正接続先から JavaScript ファイルをダウンロードして実行するようになっていた。ダウンロードされた JavaScript ファイルからは、さらに複数の JavaScript ファイルがダウンロード・実行され、最終的に Microsoft 365 の偽のログイン画面（図 8）が表示されるようになっていた。

表示された偽のログイン画面上で ID とパスワードを入力し、Next ボタンをクリックすると、攻撃者のサーバと通信を行い、メールアドレスのドメインに対応した組織のロゴや背景画像の表示を行うような仕掛けがあった。このとき、入力された ID やパスワードは攻撃者のサーバへ送付され、窃取される。

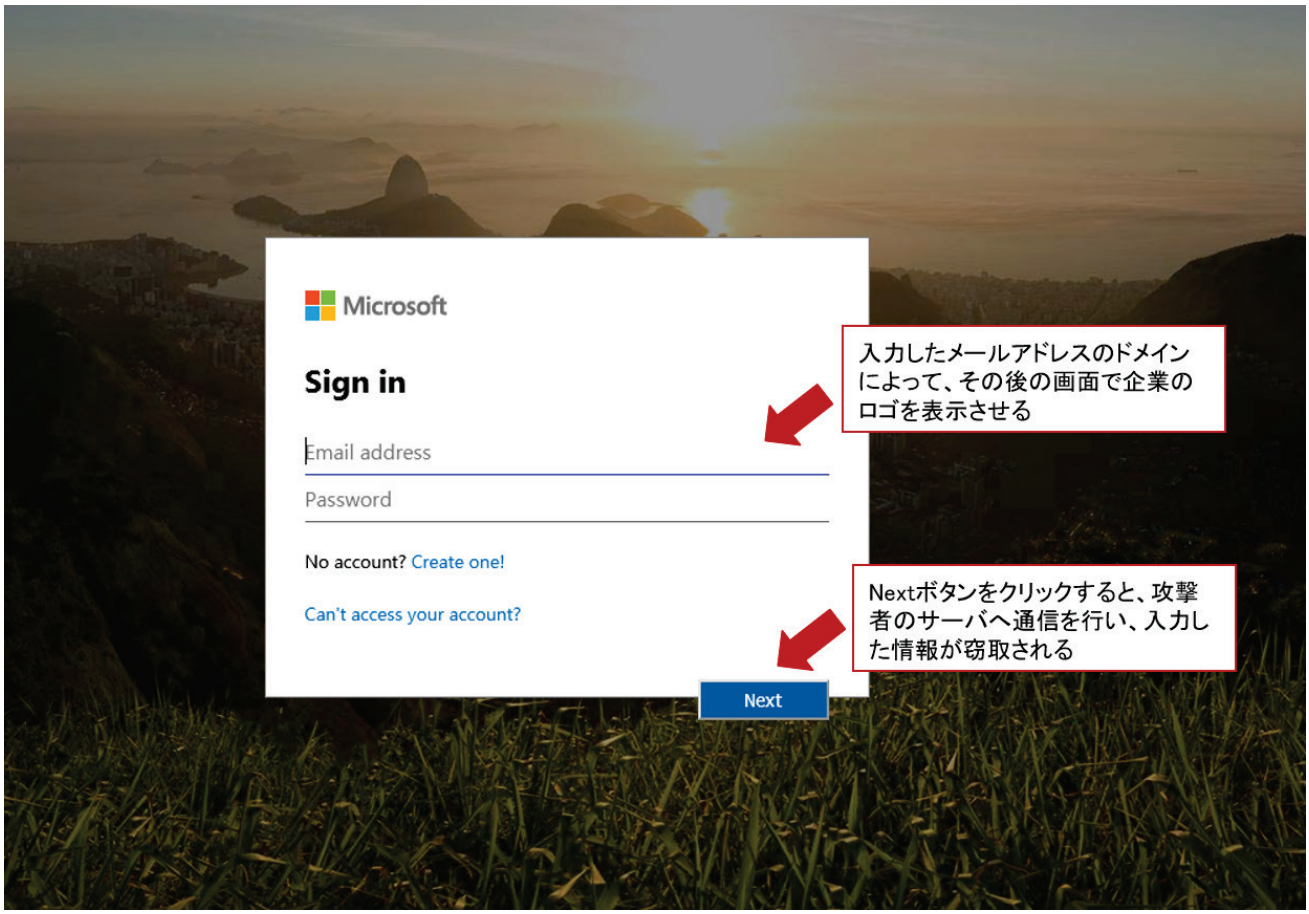


図 8 HTML ファイルを開いた際の偽のログイン画面

5　組織のセキュリティ製品で検知したウイルスメールとフィッシングメール

本四半期、J-CSIP 参加組織のセキュリティ製品で検知したというウイルスメールとフィッシングメールについて情報提供があった。

これらのメールについては、特段手口として巧妙な点等はなかったものの、企業の情報システム部門等ではこのような攻撃メールと日々対峙していることを示す例として本章では紹介する。類似したメールの他、広くばらまかれるウイルスメールやフィッシングメールに対しても注意していただきたい。

なお、J-CSIP では、本件のような比較的高度ではない攻撃メール等についても、情報共有やフィードバック等の情報収集にも努めている。

ウイルスメール

本メール（図 9）には、ISO ファイルが添付されている。この ISO ファイルをマウントすると、中にショートカット形式（.lnk の拡張子）のファイルが出力される。このショートカット形式のファイルを実行すると、Powershell コマンドが実行されるようになっていた。

本件については、Powershell コマンドの実行でエラーとなる状態であった。また、最終的に感染させられるウイルスについては不明である。

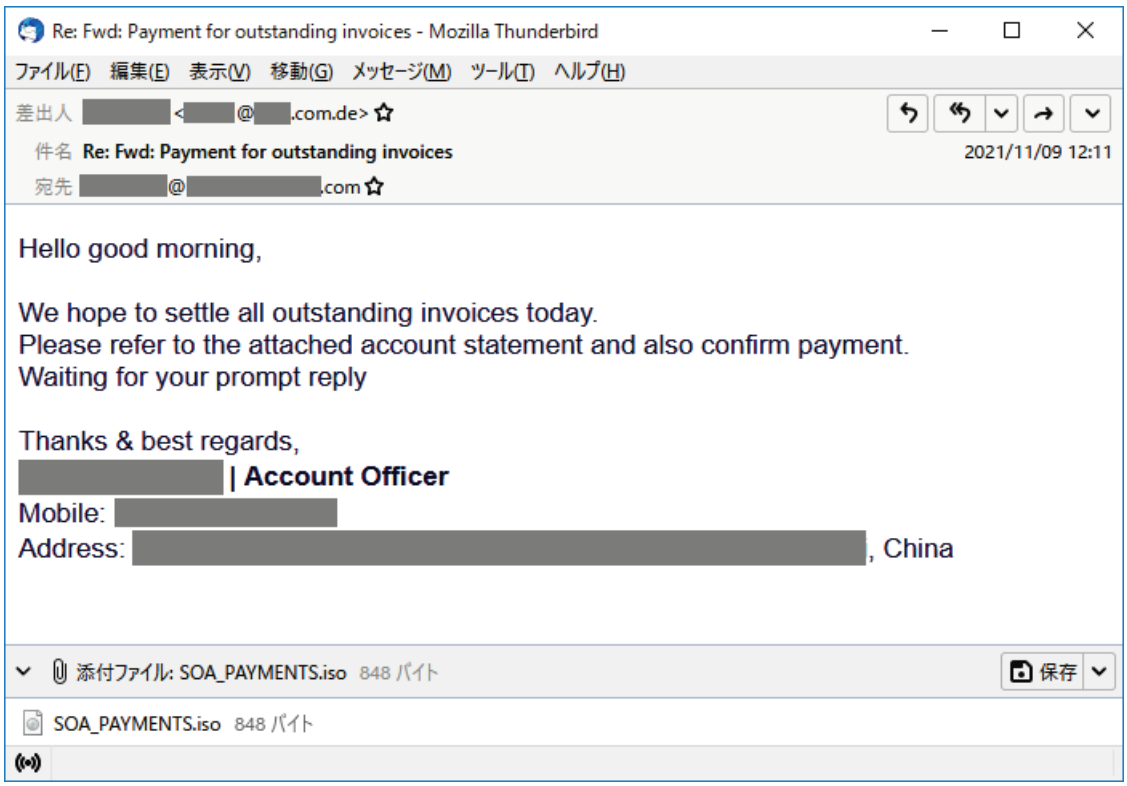


図 9 ウイルスメール

フィッシングメール

本メール（図 10）には、本文中にフィッシングサイトへの URL リンクが設定された画像（png）ファイルが貼り付けられており、本文内のいずれかの箇所をクリックするとMicrosoft 365 の偽のログイン画面が表示される仕掛けとなっていた。

本メールはメールの配送経路から、正規の組織が攻撃の踏み台となって送付されてきた可能性があるものであった。

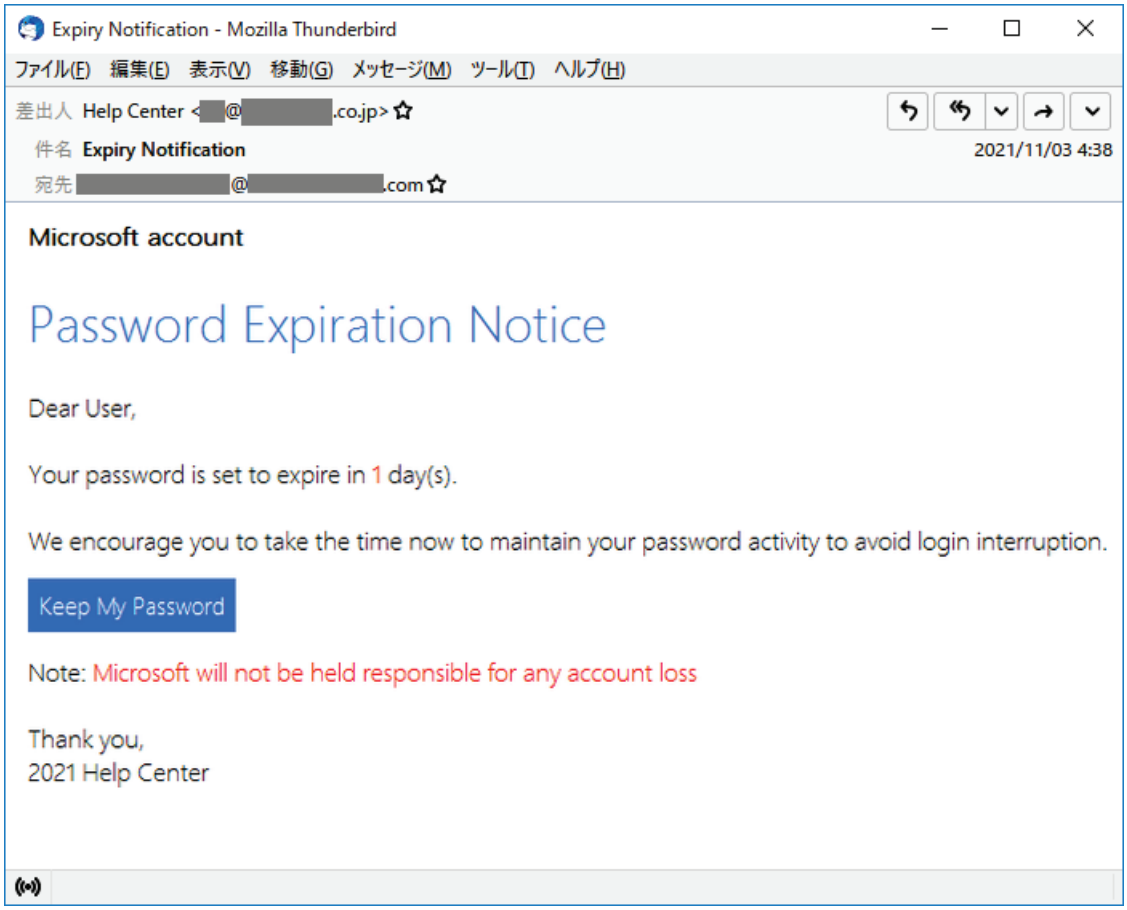


図 10 フィッシングメール

6　Emotet への感染を企図した攻撃メール

本四半期、Emotet への感染を企図した攻撃メールの活動が再開[7]したとの情報を確認し、IPA で情報を整理し、複数回に渡って参加組織へ情報共有を行ったところ、複数の組織で攻撃メールを観測したとの情報提供があった。

Emotet への感染を企図した攻撃メールについては、これまで J-CSIP 内でも多数観測しており、特定の組織・企業を狙ったものではないものの、引き続き注意を要する状況である。

また、攻撃の手口はこれまで観測されていたものと同様（悪意のあるマクロ）の手口のほか、2021 年 11 月には、メール本文中の URL リンクをクリックすると、閲覧可能な PDF 文書ファイルが存在するかのような画面のウェブサイトへ誘導するといった手口も確認している。当該サイトの画面でクリックすると PDF 文書ファイルの閲覧用を装うウイルスファイルがダウンロードされ、当該ファイルを利用者が実行することで Emotet へ感染させられる。

引き続き、不審なメールに添付されているファイルは開かない、信用できない Office 文書ファイルの場合、「編集を有効にする」、「コンテンツの有効化」といったボタンはクリックしない、不審なメールの URL リンクはクリックしないといった対応を徹底してほしい。

IPA では、2021 年の 11 月と 12 月にそれぞれ Emotet の攻撃メールについて注意喚起[8]を更新している。今後も同様の攻撃メールがばらまかれていく可能性は高く、引き続き注意していただきたい。

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

---

[7] 2021 年 1 月 27 日、EUROPOL（欧州刑事警察機構）が、欧米 8 か国の法執行機関・司法当局の協力により、Emotet の攻撃基盤をテイクダウンしたと発表があった。テイクダウン後は Emotet への感染を企図した攻撃メールは観測されていなかったが、2021 年 11 月 14 日頃に Emotet の攻撃活動が再開したとの情報を確認した。

[8] 「Emotet（エモテット）」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