# サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2019 年 7 月～9 月]

2019 年 10 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 9 月末時点の運用体制、2019 年 7 月～9 月の運用状況を報告する。1 章、2 章は全体状況を、3 章以降は本四半期で把握、分析した特徴的な攻撃事例や動向等を併せて解説する。

## 目次



[1] IPA が情報ハブ（集約点）となり、サイバー攻撃等に関する情報を参加組織間で共有する取り組み。
https://www.ipa.go.jp/security/J-CSIP/

## 1　運用体制

2019 年 7 月～9 月期（以下、本四半期）は、次の通り参加組織の増減があり、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）の体制となった（図 1）。

- 2019 年 7 月、電力業界 SIG に新たな参加組織があり、31 組織から 32 組織となった。
- 2019 年 8 月、ガス業界 SIG 内での退会に伴い、参加組織が 64 組織から 63 組織となった。

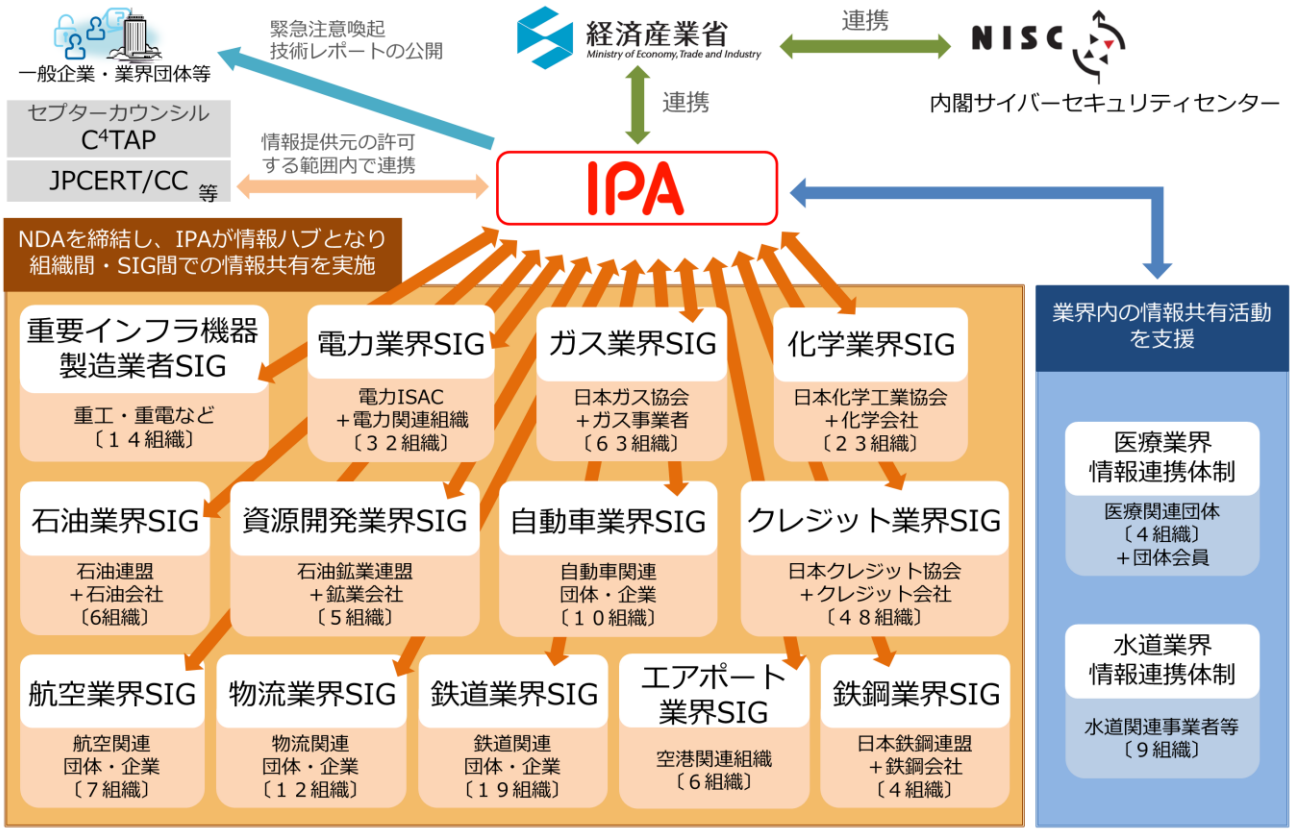


**図 1 J-CSIP の体制図**

[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（2019 年 7 月～9 月）

2019 年 7 月～9 月に、J-CSIP 参加組織から IPA に対し、サイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の情報提供が行われた件数と、それらの情報をもとに IPA から J-CSIP 参加組織へ情報共有を実施した件数（9 月末時点、13 の SIG、全 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 | 2018 年 | 2019 年 | | |
|---|---|---|---|---|---|
| | | 10 月～12 月 | 1 月～3 月 | 4 月～6 月 | **7 月～9 月** |
| 1 | IPA への情報提供件数 | 1,072 件 | 238 件 | 424 件 | **235 件** |
| 2 | 参加組織への情報共有実施件数※1 | 59 件 | 48 件 | 54 件 | **75 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 **16 件**を含む。

本四半期は情報提供件数が **235 件**であり、うち標的型攻撃メールとみなした情報は **113 件**であった。提供された情報の主なものとして、プラント関連事業者を狙う攻撃メールがおよそ 9 割（105 件）を占めている。これは、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。

さらに、本四半期では 5 件のビジネスメール詐欺について情報提供があった。実際に被害を受けた事例もあり、詳しくは 3 章で述べる。

また、標的型攻撃に関連すると思われる遠隔操作ウイルスの不正接続先 IP アドレスから、過去の一定期間、探索行為と考えられる不審な通信の受信を観測したという情報提供を受け、その内容を共有した。これについては、4 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、本四半期では実在する国内組織を騙り、国内の組織宛てに、Office 365 のアカウント情報の詐取を目的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、5 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

その他、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 | フリーウェアのダウンロードを行ったところ、セキュリティ製品で検知された。 | 1 件 |
| 2 | 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、オンラインソフトウェアの配布サイトより、正規の目的でフリーウェアをダウンロードした際に、セキュリティ製品がウイルスとして検知したという情報提供である。内容を調査したところ、セキュリティ製品の誤検知であったと考えられるもので、問題はないと判断した。一方、過去、広く一般的に信頼・使用されていたソフトウェアの開発元が攻撃者によって侵害され、悪意のあるソフトウェアと差し替えられていた事例が複数確認されている。このため、著名なオンラインソフトウェアの配布サイトからダウンロードしたファイルであったとしても、セキュリティ製品によってウイルス検知した場合は、安易に誤検知であると決めつけずに、対応を行うべきである。

項番 2 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行うべきであろう。

[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　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、5 件のビジネスメール詐欺について情報提供を受けた（表 3）。これらのうち、1 件は金銭的な被害を受けている。なお、これら 5 件の事例は、すべて英文のメールであった。

本章では、このうち 2 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 | 7 月 16 日 | 2019 年 1 月と、2019 年 7 月、国内企業の同一のメールアドレスに対し、当該企業と業務提携を結んでいる海外企業の担当者や CEO になりすますビジネスメール詐欺が試みられた。<br>本事例ではメールの受信者が不審であると気づくことができたため被害はなかった。なお、攻撃者は、業務提携先の海外企業のウェブサイトで公開している国内企業の情報を元に、なりすましメールを送ったものと考えられる。<br>・ 2019 年 1 月、業務提携先の海外企業の担当者になりすました攻撃者から、未払いの請求や料金、支払い期限を聞き出そうとするメールが送られた。<br>・ 2019 年 7 月、業務提携先の海外企業の CEO になりすました攻撃者から、「至急相談したいことがあり、メールでやりとりする時間はあるか」という旨のメールが送られた。 | なし | - |
| 2. | | 7 月 19 日 | 2019 年 6 月、日本国内企業の海外関係会社（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、被害が生じた。海外取引先企業（請求側）から未入金の連絡があり、事案が発覚した。<br>本事例では、次の手口により、被害に遭った支払側担当者のメールが攻撃者によって盗み見られていたと思われる状況であった。<br>・ 攻撃者が担当者の Office 365 のメールアカウントへ不正アクセスし、メールの転送設定を行っていた。<br>・ 本件の約 1 年前に、担当者がフィッシングメールを受信していたことが確認できてい | **あり** | - |

| 項番 | 情報提供日 | | 事例概要 | 被害の有無 | 備考 |
|---|---|---|---|---|---|
| | | | る。フィッシングがアカウント情報を窃取された原因であるか否かは不明。<br>・ 支払側担当者の PC に、一般に「AmmyyAdmin」と呼称される遠隔操作ツールが不正に設置されていた。PC への侵入（感染）経路や BEC との関係は不明だが、メールの転送設定が行われた形跡があり、不正な操作が行われた可能性が考えられる。 | | |
| 3. | | 7 月 30 日 | 2019 年 7 月、日本国内企業において、当該企業の CEO になりすました攻撃者から、当該企業の複数の担当者へ、ビジネスメール詐欺の試みと思われるメールが着信した。<br>本事例ではメールの受信者が不審であると気づくことができたため、返信等も行わなかった。本事例の特徴は次の通り。<br>・ 当該企業の 7 つのメールアドレスに対し、同時になりすましメールが着信した。これらのメールアドレスは、いずれもインターネット上で公開されているものであった。財務や経理にも関係なく、すでに使われていないメールアドレスも数件あった。<br>・ メールの差出人の表示名と本文中の署名に、CEO の氏名が使われていた。<br>・ メールは英文であった。<br>・ メール本文は、実在する弁護士事務所を挙げ、「弁護士事務所から連絡はあったか」というのみの内容であった。（返信した場合、詐欺が試みられるものと思われる）<br>・ 差出人のメールアドレスにはフリーメールアドレスが使われていた。 | なし | － |
| 4. | | 8 月 15 日 | 2019 年 7 月、日本国内企業（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 1 |
| 5. | | 8 月 29 日 | 2019 年 8 月、日本国内企業の CEO になりすました攻撃者から、当該企業の国内グループ企業の CEO に対し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 海外取引先を狙った攻撃

本事例は、2019 年 7 月、J-CSIP の参加組織（A 社：請求側）と、その海外取引先企業（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、偽の振り込み先を記載した請求書を送り付けてきたものである[5]。

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、支払い側である B 社の担当者が、不審な点に気づくことができたため、金銭的な被害には至らなかった。また、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 社間のやりとりへ介入
（2） フリーメールアドレスの悪用
（3） 同報メールアドレスの改変

### （1） A 社と B 社間のやりとりへ介入

A 社（国内企業）と、B 社（海外取引先）との間で、ビジネスメールをやりとりしていた中に、フリーメールアドレスを使って A 社担当者になりすました攻撃者が割り込み、詐欺を試みてきた。攻撃者は何らかの方法でメールを盗聴していたものと考えられる。

この事例の特筆点は、攻撃者が介入してきたタイミングである。A 社と B 社が取引に必要な書類の内容について調整していた中で、A 社が「書類を修正してすぐに送る」と B 社へ連絡した直後、A 社になりすました攻撃者が、B 社へ偽のメールを送り付けてきた。偽物であると見抜くことが非常に難しいタイミングで、攻撃が行われたことになる。

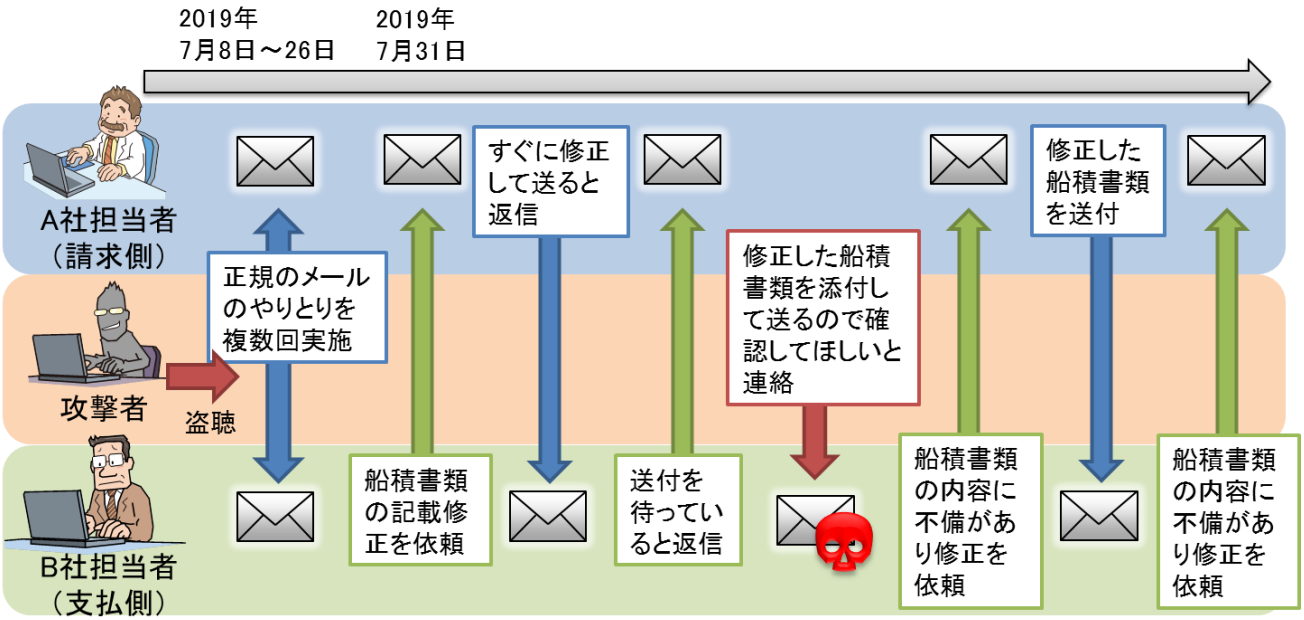


**図 2 事例 1 攻撃者とのやりとり（前半／7 月 31 日まで）**

[5] この事例は、情報提供元企業の取引先が攻撃を受けたものであったため、全ての情報が収集・提供されているわけではなく、一部推測を含む。

攻撃に係るメールのやりとり（前半）を図 2 に示す。

2019 年 7 月 8 日から 7 月 26 日まで、A 社担当者と B 社担当者は、取引に必要な船積書類に関するメールをやりとりしていた。そして、7 月 31 日、B 社担当者から A 社担当者に対して、船積書類の記載内容について修正を依頼するメールを送った。そのメールに対し、A 社担当者は数分後に「すぐに修正して送る」という旨を返信し、さらに B 社担当者は「送付を待っている」と返信した。

その直後（A 社担当者が B 社へ「すぐに修正して送る」というメールを送った約 1 時間半後にあたる）、攻撃者は B 社へ「修正した船積書類を送るので内容を確認してほしい」という旨の偽のメールを送り付けてきた。この偽メールでは、差出人（From）のメールアドレスには正規の A 社担当者のものを使い、なりすましていた。一方、同報（Cc）へ設定された A 社の他の担当者のメールアドレスが改変されていた。

この時点では、B 社担当者は、このメールが偽物だとは気付かずに船積書類を受け取ったものの、攻撃者が送ってきた船積書類の内容に不備があり修正を依頼する旨、本物の A 社の担当者へ返信を行った（従って、そのメールには「攻撃者が送った偽メール」の内容が引用されている）。ビジネスメール詐欺では、偽メールへの返信がなりすました本人に届いて詐欺が露見しないよう、From メールアドレスや Reply-To ヘッダに細工が施されていることが多いのだが、本件の事例では、細工に失敗したか、B 社担当者が何らかの理由で、アドレス帳等から本物の A 社の担当者を正しく宛先として設定したものと思われる。

A 社担当者には、会話に噛み合わない内容のメールが着信したことになり、また、メールには送信した覚えのない内容が引用されていたため、異常に気付けた可能性はあるが、結果としては見過ごされている。

その後、A 社と B 社は互いに本物のメールアドレスでの正規のやりとりを再開し、引き続き船積書類の修正に関する調整を進めた。攻撃に係るメールのやりとり（後半）を図 3 に示す。

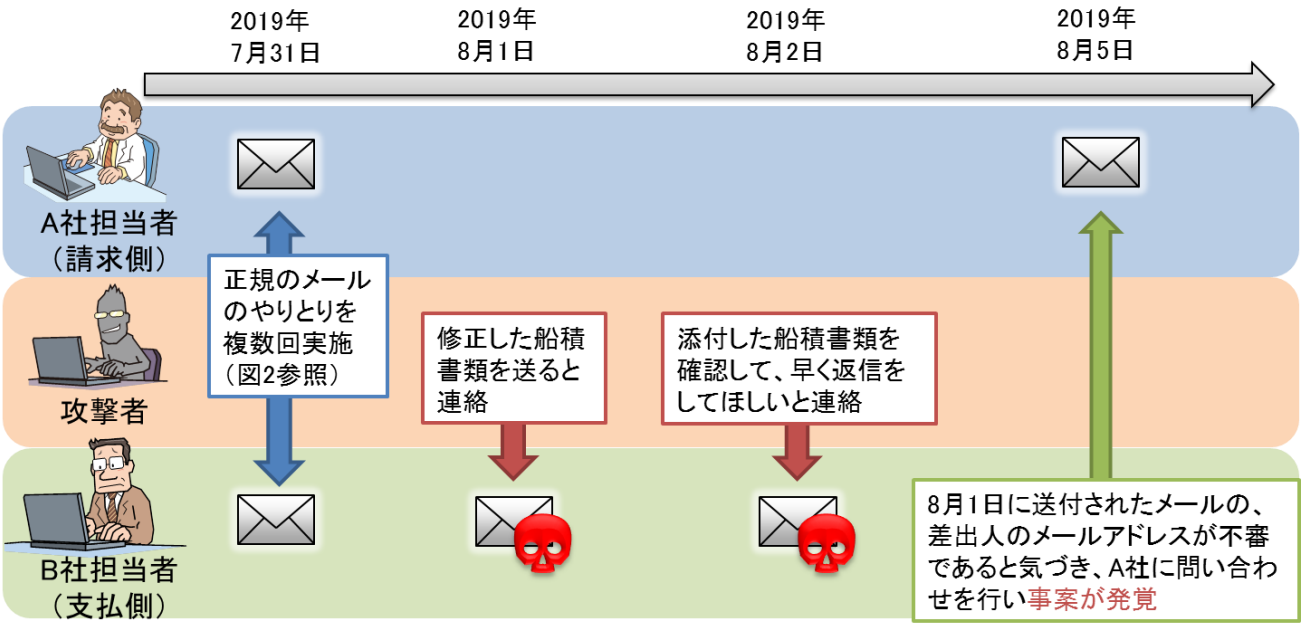


**図 3 事例 1 攻撃者とのやりとり（後半／8 月 1 日以降）**

7 月 31 日に一度攻撃に失敗している状況であるが、攻撃が発覚していないことからか、攻撃者は翌日の 8 月 1 日と、更にその翌日の 8 月 2 日にも、修正した船積書類を送るという内容で、偽の請求書が添付されたメールを 2 通、連続して B 社に送ってきた。文面には、催促するような内容も書かれていた。このときの偽メールの差出人(From)メールアドレスには、偽のメールアドレスが使われていた。

これらの偽メールに添付されていた請求書(船積書類の一部)は、過去に A 社担当者から B 社担当者宛に送付された正規の請求書の、口座情報部分を改ざんしたと思われるものであった。そのため、見た目だけでは偽物であると見破るのは難しいと思われるが、本事例で B 社が被害(攻撃者の口座への送金)へ至らなかったのは、船積書類の修正内容について合意が取れていない状態で、攻撃者が修正したという船積書類を一方的に送り付けてきたためと考えられる(攻撃者はメールを盗み見ていたが、そこまでは状況を理解していなかった可能性が高い)。

最終的には、8 月 5 日、B 社の担当者が 8 月 1 日に攻撃者から送られてきたメールの差出人(From)メールアドレスが不審であることに気づき、正規の A 社担当者に問い合わせたことで、事案が発覚した。

### (2) フリーメールアドレスの悪用

攻撃者は、B 社へなりすましメールを送る際に、A 社のメールアドレスに似通ったフリーメールアドレスを取得し、偽のメールを送ってきた。

偽のフリーメールアドレスは、次の例に示すように、メールアドレスのローカル部を、本物のメールアドレスに似せたものであった。

【本物のメールアドレス】 alice @ a-company . co . jp
【偽物のメールアドレス】 alice . a-company . jp @ freemail . com
「@」を「.」に変え、本物のメールアドレスのセカンドレベルドメイン(例では「.co」)を除いたものが使われていた。

※実際に悪用されたものとは異なる。

### (3) 同報メールアドレスの改変

正規のA社とB社間のメールでは、それぞれの社員を同報先(Cc)に設定したメールで取引に関するやりとりを行っていた。一方、攻撃者が A 社担当者になりすまして B 社の担当者へ送り付けた偽のメールでは、同報先に設定された A 社の複数の担当者のメールアドレスは、全て偽のフリーメールアドレスに改変されていた。

同報先のメールアドレスを改変することで、メール受信者にとっては、自分以外の多くの関係者が宛先に入っているように見える(衆人環視の中でのやりとりに見える)が、実際には攻撃者が狙った B 社担当者のみに送られており、メール受信者は騙されていることに気づきにくい。また、本来の同報先である A 社には、この偽メールが届かないため、詐欺が行われていることに気づくことができない。

### 3.2 事例 2 国内グループ企業を狙った攻撃

本事例は、2019 年 8 月、J-CSIP 参加組織（A 社）の CEO になりすました攻撃者が、A 社の国内グループ企業（B 社）の CEO に対して、偽のメールを送り付けたものである。攻撃者は、少なくとも A 社と B 社の関係やそれぞれの CEO について把握した上で、攻撃を行ってきている。

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 2：経営者等へのなりすまし」に該当する。

なお、本事例では、B 社側のメール受信者が、「送信元メールアドレスが通常と異なることや、英語のメールである」点を不審と感じ、メールヘッダの調査等を行ったことで、偽のメールであることが判明したため、金銭的な被害には至らなかった。

本事例で実際に攻撃者から送られてきたメールを図 4 に示す。

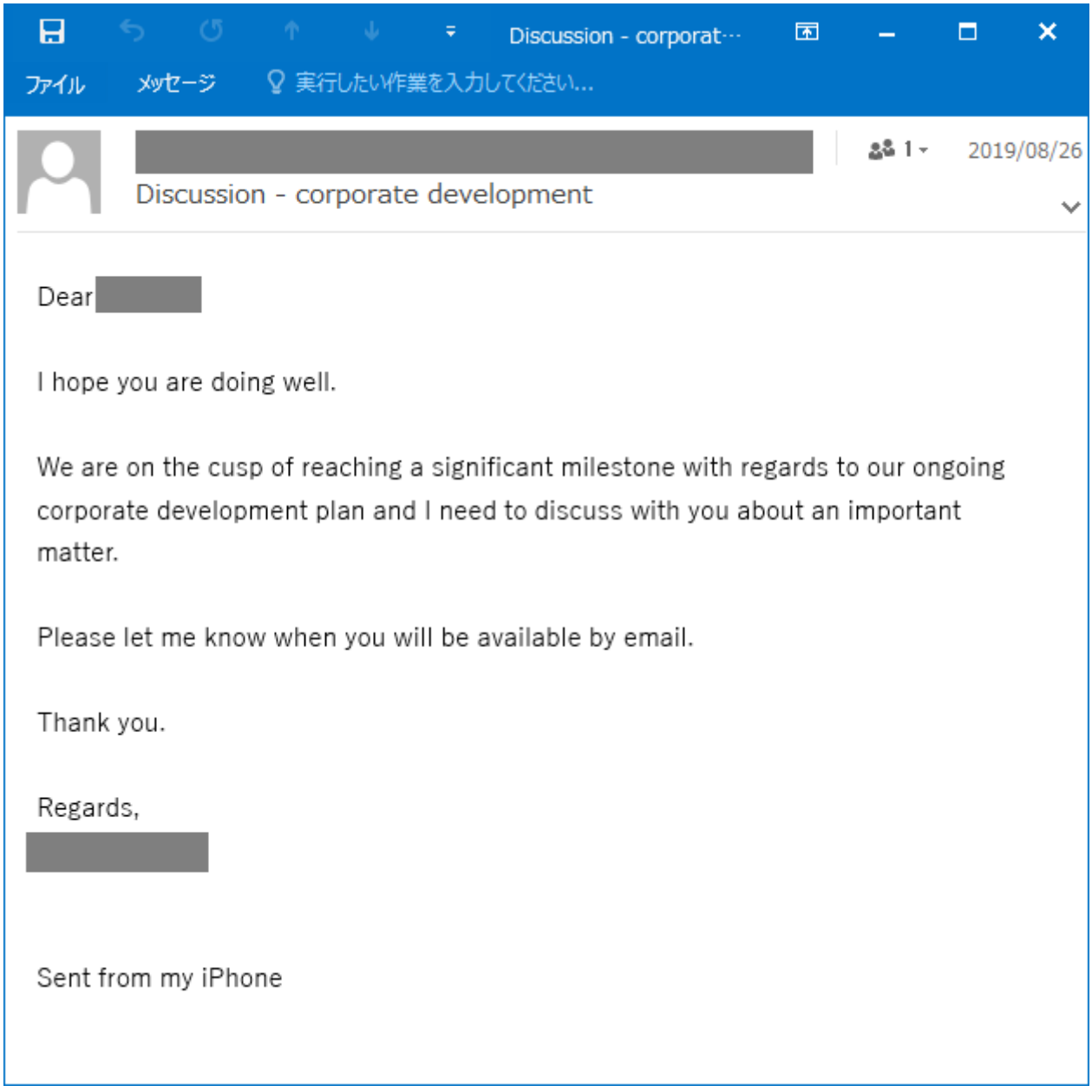


**図 4 事例 2 攻撃者から送られてきたメール**

この偽のメールでは、差出人（From）ヘッダに次のような設定が行われていた。

| From: “【A 社 CEO の名前】 – 【A 社 CEO のメールアドレス】” <攻撃者が用意した偽のメールアドレス> |
|---|

このようにすることで、受信者のメールソフト上では、本物のA社のCEOの名前とメールアドレスが表示される。これにより、偽のメールアドレスから送信されていることを気付かせにくくする狙いがあると思われる。

なお、本件の場合、From ヘッダに書かれた A 社 CEO のメールアドレスのドメインの末尾が、正規の A 社のドメインと異なるものとなっていた。攻撃者の意図は不明だが、差出人の欄に記載されたA社CEOのメールアドレスを受信者が手動で返信先へ入力してメールが返信されることを考慮したか、ミスをしたという可能性が考えられる。

## 3.3 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　探索行為と考えられる不審な通信の受信

IPA が入手した標的型攻撃に関連すると思われる遠隔操作ウイルスの情報を参加組織内へ情報共有したところ、複数の組織において、過去の一定期間、ウイルスの不正接続先（C&C サーバ）の IP アドレスから、探索行為と思われる不審な通信の受信が観測されていたことが分かった。

これらの事象が標的型攻撃と直接的に関係する動向であるのか、広く無差別な探索行為によるものかは不明である。参考までに、この事例について説明する。

### 事象発見に至る経緯

2019 年 7 月 17 日、IPA が入手した標的型攻撃に関連すると思われる遠隔操作ウイルスについて J-CSIP の参加組織へ当該情報を共有したところ、7 月 19 日、ある参加組織（以降、組織 A）より、当該遠隔操作ウイルスの不正接続先の IP アドレスから、過去一定期間の間に、探索通信と思われる通信を特定のポート宛てに受信していたという情報提供があった。

C&C サーバに対する通信ではなく、C&C サーバからの通信が観測されることは過去に例が少なく、この組織 A からの情報を 8 月 1 日に J-CSIP 参加組織へ共有したところ、翌日（8 月 2 日）に 1 つの組織（以降、組織 B）から同様の痕跡が見つかったとの情報提供があった。また、8 月 5 日にも別の参加組織（以降、組織 C）からも同様の痕跡が見つかったという情報提供があった。

### 観測された情報

3 組織から提供された情報をまとめたところ、ほぼ同時期に同一の IP アドレスから、複数回の不審な通信を受信していたことが分かった（表 4）。また、この通信はいずれも 1433 番ポート（Microsoft SQL Server の標準ポート）へ向けた通信であることが分かっている。

**表 4　組織ごとの観測期間と観測回数**

| 組織 | 観測期間 | 観測回数 |
|---|---|---|
| 組織 A | 2018/12/14～2019/2/3 | 74 |
| 組織 B | 2018/12/26～2019/2/12 | 7 |
| 組織 C | 2018/12/10～2019/2/13 | 67 |

公開情報を調査したところ、本件と同一の IP アドレスから、同じく 1433 番ポートに対して、2018 年 12 月から 2019 年 1 月の期間に探索通信があったという情報も確認している。

同一の IP アドレスを複数の悪意のある者が使用している可能性もあることから、本件の内容が何らかの標的型攻撃に直接結びつくか、あるいは無関係であるかは不明である。情報共有を実施した元々の目的は、各参加組織内から不正接続先への通信が発生していないか（ウイルス感染の兆候が無いか）の確認に資することであったが、本件は、逆に不正接続先 IP アドレスから、特定の期間、特定のポートへの探索通信があったことを、参考情報として把握・共有することとなったものである。

## 5　実在する国内企業を騙り国内組織へ送られたフィッシングメール

本四半期、実在する国内企業を騙り、国内の組織に対し、Office 365 のアカウント情報の詐取を目的としたフィッシングメールが送られたとの情報提供があった。本章では、実際に送信された攻撃メールと、誘導先の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 5）は、ボイスメールのダウンロードを装う内容が、英語と日本語で併記されていた。また、メール本文中には URL リンクが 2 か所書かれており、リンク先の URL は同一であった。URL リンクの先には、Office 365 のアカウント情報の詐取を目的としたフィッシングサイト（Office 365 のログイン画面に似たサイト）が設置されていた（図 6）[6]。

本件は、2019 年 8 月 14 日に情報提供元の組織の複数人へ着信し、8 月 16 日に IPA へ情報提供された。一見すると、無差別にばらまかれている類のフィッシングメールにも見えるが、当該組織ではメールを捨てずに確保し、調査を行っていた。そして、情報提供元の組織から、詐称された国内企業へ事実確認を行った結果、当該組織以外にも類似する攻撃メールが送られていたことが分かった。このことから、本件は日本国内の複数組織の Office 365 のアカウント情報を狙う攻撃であった可能性がある[7]。

Microsoft 社のアカウント（Office 365 等）が攻撃者によって侵害されると、メールの情報のみならず、組織内の情報等が攻撃者によって窃取され、組織内や他組織への攻撃等、更なる攻撃にも繋がる可能性があるため、非常に注意が必要である。

フィッシング攻撃への対策の一つは、利用者ひとりひとりが、このような攻撃手口を知り、騙されないよう注意して、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、このようなクラウド型のサービスを利用する場合は、多要素認証の導入も一つの対策となる。フィッシング攻撃に限らず、認証情報の漏洩が大きな被害をもたらす可能性を考慮し、可能な範囲での対策を検討していただきたい。

---

[6] 情報提供を受けた 8 月 16 日時点では、URL リンク先のウェブサイトはアクセスできない状態であったが、8 月 14 日に取得されたアーカイブ情報（魚拓）が公開サービス上に存在した。このスクリーンショットは当該アーカイブ情報によるもの。

[7] 状況把握のため、本件と同様のメールを受信した組織があれば、ぜひ情報をお寄せいただきたい。

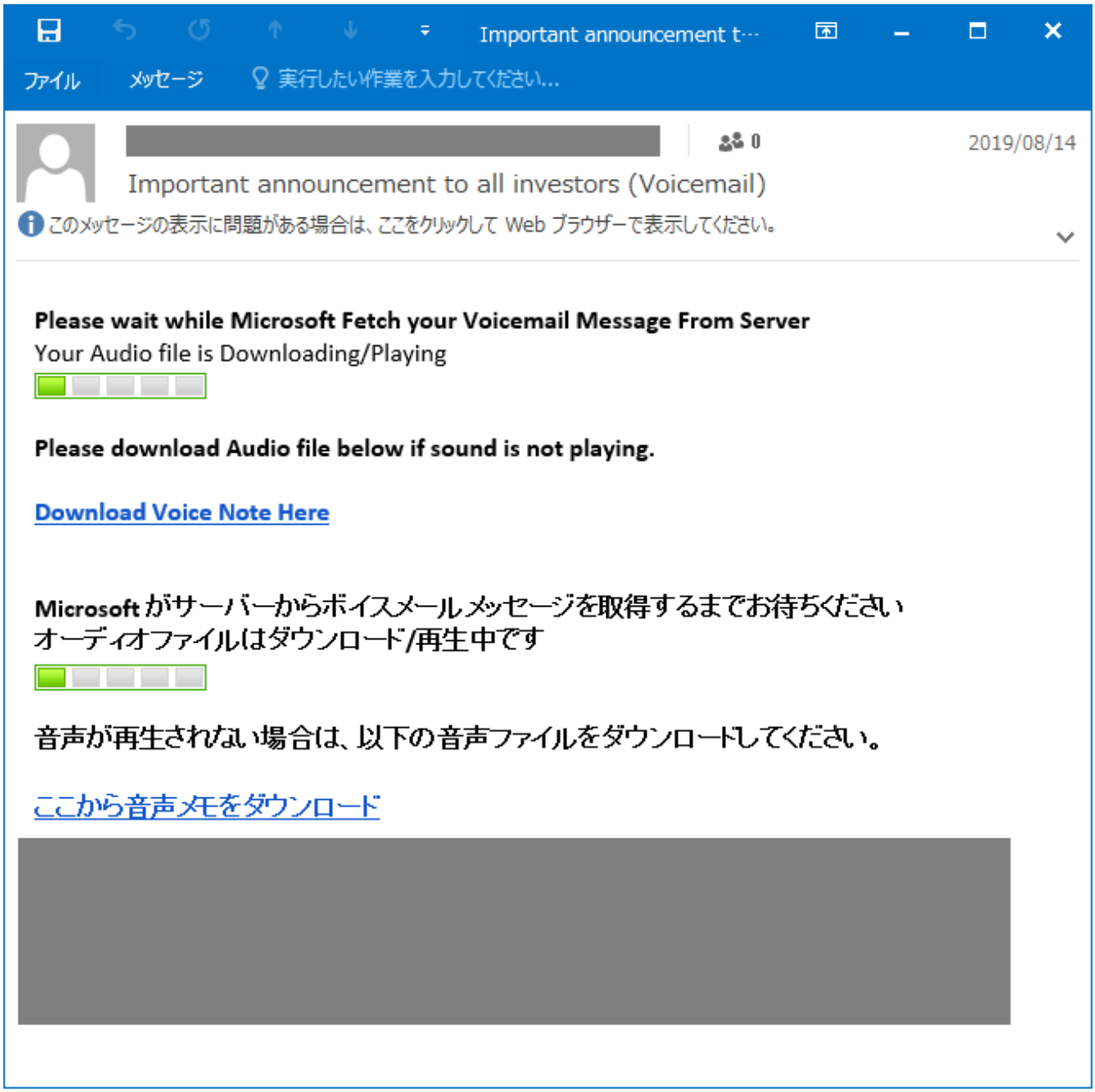


**図 5 攻撃者から送信されたフィッシングメール**

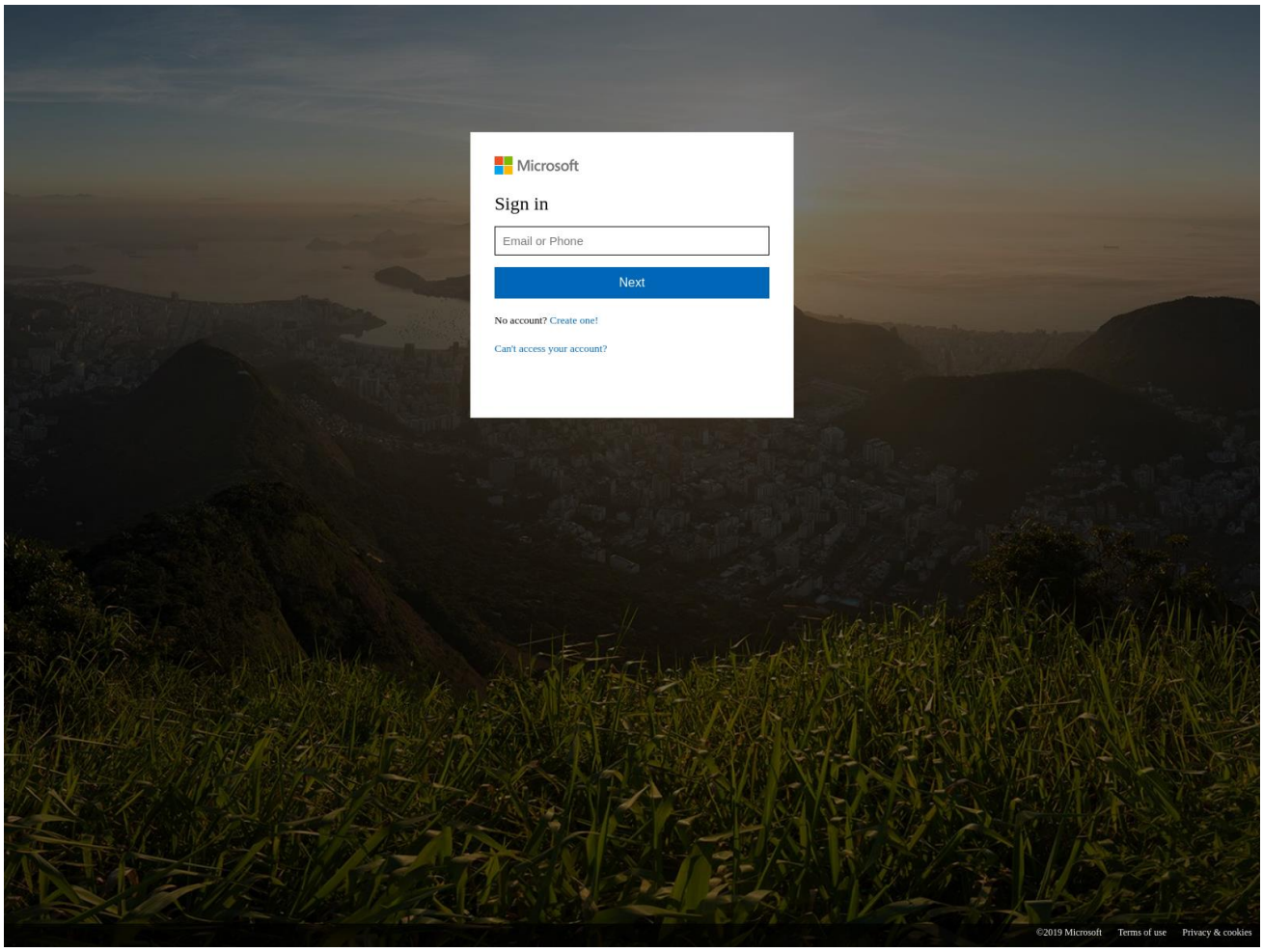


**図 6 本文中の URL リンク先のフィッシングサイトの画面**

## 6　標的型攻撃に関連すると思われるウイルスの解析事例

本四半期、特定の業種・業界を狙った攻撃（標的型攻撃）で使用された可能性のあるウイルスを公開情報より入手し、解析を行った。

このウイルスは、「アイコンや拡張子の偽装」、「特定のセキュリティソフトの停止」、「特定の時間帯のみ動作を行う」、「不正接続先から、特定の応答が得られないと動作を止める」といった、ウイルス自身の存在、攻撃活動の露見、そしてウイルス解析者による解析を避けるような様々な仕掛けがあった。

参考情報として、その解析結果を本書の付録として示す。詳しくはそちらを参照いただきたい。

### 関連情報のご提供のお願い

本書で紹介した事例について、J-CSIP では関連情報を求めています。
同様の事例を確認した場合など、下記窓口へ情報提供をいただけますと幸いです。

**J-CSIP 事務局 ご連絡窓口（IPA）**
jcsip-info@ipa.go.jp

### 標的型サイバー攻撃特別相談窓口

IPA の「標的型サイバー攻撃特別相談窓口」では、標的型サイバー攻撃を受けた際の相談を受け付けています。お気づきの点があれば、ご相談ください。

**標的型サイバー攻撃特別相談窓口（IPA）**
https://www.ipa.go.jp/security/tokubetsu/

以上