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]

2019 年 7 月 26 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 6 月末時点の運用体制、2019 年 4 月～6 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 4 月～6 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 6 月、エアポート業界 SIG に新たな参加組織があり、5 組織から 6 組織となった。
- 2019 年 6 月、石油業界 SIG 内での組織改編に伴い、参加組織が 7 組織から 6 組織となった。

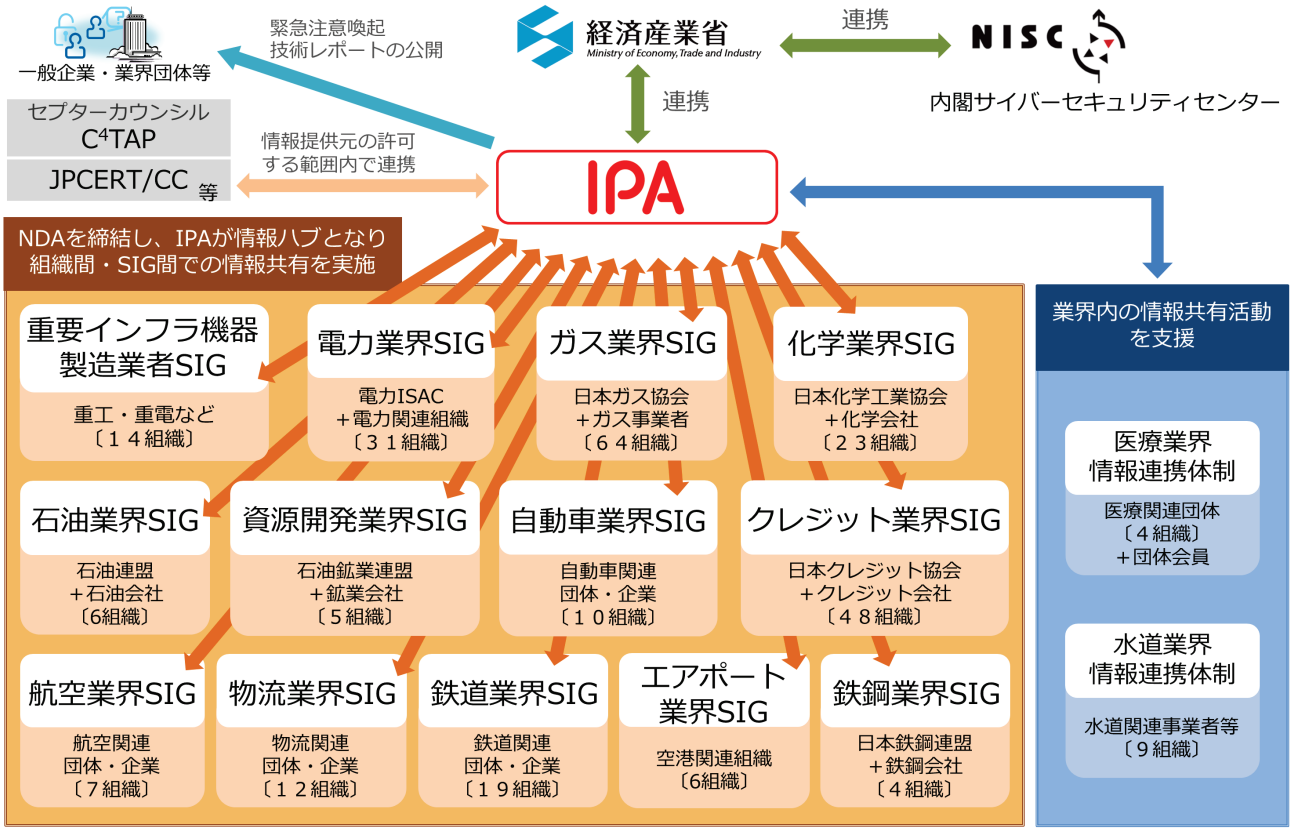

図 1 J-CSIP の体制図

[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 4 月～6 月）

2019 年 4 月～6 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（6 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	
		7 月～9 月	10 月～12 月	1 月～3 月	**4 月～6 月**
1	IPA への情報提供件数	519 件	1,072 件	238 件	**424 件**
2	参加組織への情報共有実施件数※1	39 件	59 件	48 件	**54 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 **424 件**であり、うち標的型攻撃メールとみなした情報は **75 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 7 割（52 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 4 件のビジネスメール詐欺について分析を行った。詳しくは 3 章で述べるが、実際に被害を受けた事例もある。

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	身に覚えの無い取引に関するメール（詐欺の一種と思われる）を受信した。	1 件
2	不審なメールに記載されている URL リンクをクリックしてしまった。	2 件
3	不審なメールの添付ファイルを開いてしまった。	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。	3 件

[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

項番 1 は、これといった具体的な内容の書かれていない「緊急の取引について話し合いたい」という主旨の英文のメールであった。添付ファイルやメール本文中の URL リンクも無く、特段の危険の無いメールではあるが、返信してしまうと詐欺が行われる類のものと思われる。このようなメールは多くばらまかれているが、本件のメールの件名には、メールの受信者の氏名が正しく書かれており、何らかの方法で攻撃者が入手した情報をもとにメールが送られてきていると考えられるものであった。

項番 2、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、添付ファイルを開いてしまったという情報提供・相談である。調査したところ、これらのメールはいずれも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、不審メールの本文中の URL のクリックや、添付ファイルを開くことでウイルスに感染させられていた可能性もあったため、安易にこのような操作を行わ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、今後もこの脅威は続くものと考えられ、注意が必要な状況である。

本四半期では、4 件のビジネスメール詐欺について確認した（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 4 件の事例は、すべて英文のメールであった。

本章では、このうち特筆すべき 2 件の事例を説明する。

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.	2018 年	12 月 5 日	2018 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、被害が生じた。	**あり**	-
2.	2019 年	4 月 8 日	2019 年 2 月、日本国内企業の国内関連企業（支払側）と、新規の海外取引先企業（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.		4 月 9 日	2019 年 4 月、日本国内企業の海外関連会社において、同社の CEO になりすました攻撃者から、同社の財務部長へ企業買収の準備と称して、国際送金をさせようとするビジネスメール詐欺が試みられた。	なし	-
4.		5 月 15 日	2019 年 3 月、日本国内企業の海外関連企業（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 2

3.1 事例 1 新規の海外取引先企業を詐称する攻撃

本事例は、2019 年 2 月、J-CSIP の参加組織の国内関連企業（A 社：支払側）と、その「新規」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、「新規に取引を開始する口座の情報を差し替える」形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、支払い側である A 社の担当者が偽のメールであると気づかなかったため、偽の口座へ振り込みを行ってしまったが、送金依頼先の日本の銀行の担当者とのやり取りの中で不審な点に気づき、海外側の経由銀行へ連絡して送金を止めることができたため、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）「口座の変更」ではなく「見積書の価格の修正」を装う
（2）偽のメールアドレスの使用
（3）Reply-To ヘッダの悪用
（4）メール引用部分の改変

（1）「口座の変更」ではなく「見積書の価格の修正」を装う

攻撃者は、A 社（国内関連企業）と、A 社の新規取引先である B 社（海外取引先）との間で、初めて行う請求と振り込みに関するやりとりに対して、割り込む形で詐欺を試みてきた（図 2）。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。

A 社によると、事後の調査において A 社側のメールが窃取されていた形跡が確認できなかったことから、「おそらく、本取引の開始前から B 社側のメールが攻撃者によって窃取されていたものと考えられる」とのことであった。

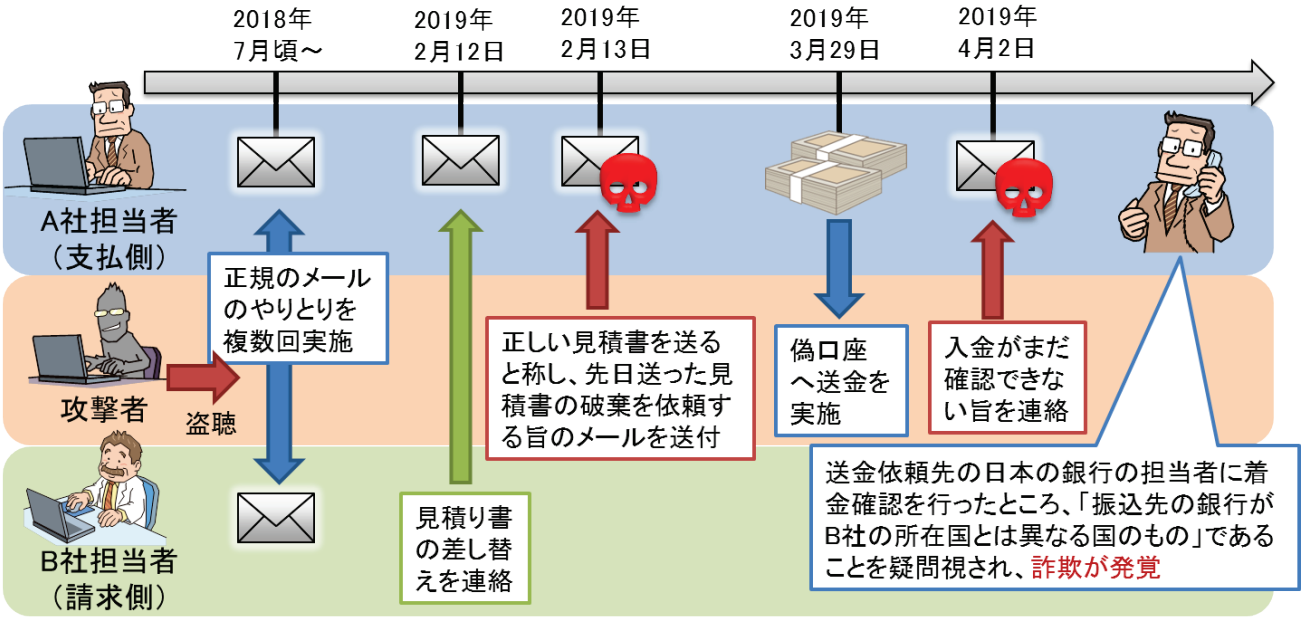

図 2 事例 1 攻撃者とのやりとり

このやりとりの中で、攻撃者は、B 社から A 社に対して本物の見積書の差し替えを連絡するメールが送られた日（2019 年 2 月 12 日）の翌日、2 月 13 日に、「正しい見積書を送る」と称し、再度見積書を差し替える形で、偽の見積書を送ってきた。そして、その偽の見積書に書かれていた支払先の口座が、偽の口座情報に改変されていた。

このビジネスメール詐欺の事例の特徴的な手口は、攻撃者は「口座の変更」とは言わず、「見積書の価格の修正」と言い、実際には口座情報を改変していたという点である。更に、攻撃者は同時に「直前に送った見積書を破棄してください」としており、本物の見積書を破棄させることで、巧妙に偽の口座への送金へ誘導している。実際に A 社へ送られた偽のメールを図 3 に示す。

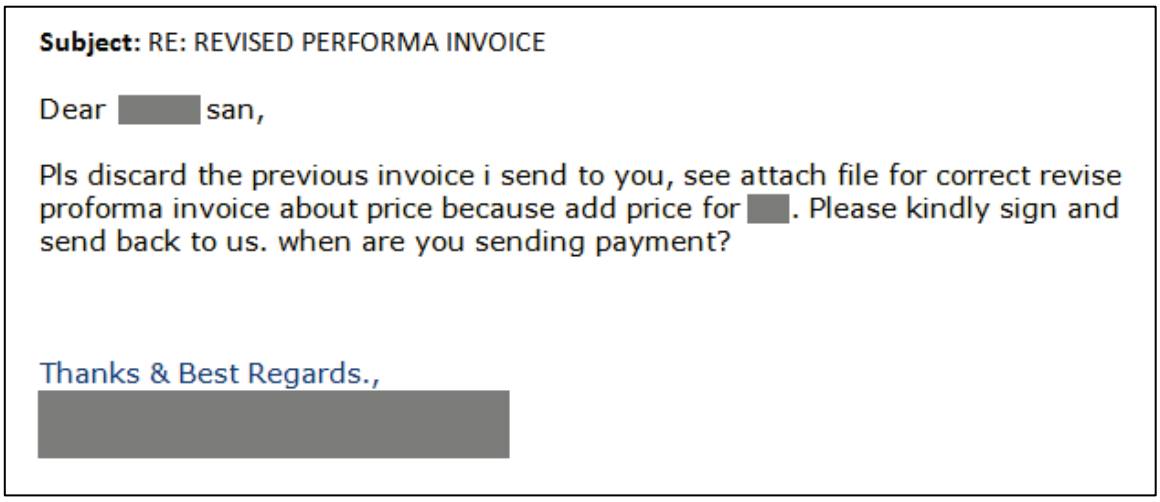

図 3 事例 1「見積書の価格の修正」を装う攻撃者からのメール

この手口によって担当者が騙された場合、経理部門等へは改変された後の偽の見積書しか渡されないという状況になりかねず、その場合、そもそも「口座が変更になった」という認識すらできないということになる。また、本件は新規の取引先であり、過去の実績を基にした確認ができないということから、本件では、送金前の経理部門による確認は行われていたものの、不審だとは気づけなかった。

IPA ではこれまで、ビジネスメール詐欺への対策として「急な振込先口座の変更等の対応を求められた場合には、事実関係を確認する」点に注意を促していたが、本件のようなケースでは、この対策を取っていても見破ることが難しい。最初の送金の時点において、信頼できる経路でのチェックが必要である。

（2） 偽のメールアドレスの使用

攻撃者は、A 社へなりすましメールを送る際に、B 社のメールアドレスに似通った「詐称用メールアドレス」を、差出人（From）へ設定していた。また、偽メールの同報先（Cc）に記載された、B 社担当者のメールアドレスも同じように改変していた。

詐称用メールアドレスは、次の例に示すように、本物のメールアドレスのローカル部の先頭から「4 文字目」のみ一文字アルファベットを改変（追加・置き換え）するものであった。改変が目立たないよう、文字列の中央部分を細工しているものと思われる。

【本物のメールアドレス】 alice @ b-company . com 【偽物のメールアドレス】 alicce @ b-company . com　（c を一文字追加） alioe @ b-company . com　（「c」を「o」に一文字変更）

※実際に悪用されたものとは異なる。

この手口により、次の効果を狙ったものと考えられる。

- 差出人（From）を詐称用メールアドレスに設定することで、本物のメールに見せかけつつ、差出人（From）宛てに返信メールが送られた場合でも、詐称されたB社の担当者にはメールが届かずエラーとなる。これは、攻撃者が詐欺の発覚を遅らせようとした細工であると考えられる。
- 同報されているメールアドレスを改変することで、A 社担当者にとっては、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 A 社担当者のみに送られており、騙されていることに気づきにくい。また、B 社側の関係者にとっては、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けない。

なお、A 社担当者がこの偽メールへ全返信を行うと、攻撃者のメールアドレス以外の宛先は（改変されたメールアドレスであるため）エラーとなる状況であり、A 社担当者は実際にエラーメールを受信していた。しかしながら、このエラーメールが本件の攻撃の兆候を示すものだとまでは、A 社担当者は気づくことができなかった。

（3） Reply-To ヘッダの悪用

攻撃者は、B 社担当者になりすまして、A 社担当者へなりすましメールを送る際、メールの返信先（Reply-To ヘッダ）に次のようなメールアドレスを設定し、細工を行っていた。

Reply-To: B 社担当者の本物の表示名 〈攻撃者のメールアドレス〉

このように細工された状態では、受信者が「返信」ボタンをクリックするなどして、そのメールへの返信メールを作成すると、メールの作成画面では、差出人（From）ではなく、Reply-To ヘッダに設定した攻撃者のメールアドレス（フリーメールサービスのものであった）が宛先となる。ただし、表示名の部分には B 社担当者の本物の名前が表示される。攻撃者は A 社担当者に対し、メールが本物であると錯覚させつつ、実際のメールのやりとりは B 社担当者本人に届かないようにして、攻撃を行っていたものと思われる。

（4） メール引用部分の改変

攻撃者は、A 社と入金確認に関するメールをやりとりする際、メールの過去のやり取り部分（引用部分）も改変していた。

メールソフトによっては、過去のメールを引用すると、メール本文以外に、差出人（From）、宛先（To）、同報先（Cc）、件名（Subject）といった、メールのヘッダ情報も併せて記載されることがあるが、攻撃者はこれらの情報を改変し、攻撃者が実際に使用しているフリーメールアドレスが過去のやりとりに含まれていないかのように見せかけていた。

この細工も、これまでの手口と同じく、A 社担当者に偽のメールであると気づかせにくくする狙いがあるものと考えられる。

また、不審だと見破って調査を行う際にも、引用部分にあるメールのやりとりの経緯は信用できない前提で対応する必要がある。どこから本物と偽物（攻撃者）が入れ替わったのかを特定するためには、過去のメールも可能な限り回収し、調査する必要があるだろう。

3.2 事例 2 海外取引先を狙った攻撃

本事例は、2019 年 3 月、参加組織の海外関連企業（A 社：請求側）と、その海外取引先（B 社：支払側）の取引において、A 社の担当者になりすました攻撃者が、偽の振り込みを要求するメールを B 社に送り、金銭詐取を試みたものである。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。

また、本件の攻撃者は、詐欺の発覚を遅らせるために B 社担当者になりすまし、A 社の担当者とメールのやりとりを行ったものと推測される。

なお、本事例では、支払い側である B 社の担当者が偽のメールであると気づけず、偽の口座へ振り込みを行ってしまったが、銀行から回収できたため金銭的な被害には至らなかった。（B 社が銀行から金銭を回収できた経緯の詳細は不明）

本事例では、詐欺の過程において、次の手口が使われた。

（1） ビジネスメールの授受に割り込み、詐欺を試みる
（2） 詐称用ドメインの取得と悪用
（3） 同報メールアドレスの改変

（1） ビジネスメールの授受に割り込み、詐欺を試みる

本事例では、A 社（海外関連企業）と B 社（海外取引先企業）の間で、支払期日の異なる 3 つの請求書（以下、請求書 1～3）のやりとりを行っていた。攻撃者は、期日が最も早い請求書（請求書 1）に対する支払いが正しく完了したタイミングで、偽のメールを A 社に送り付けてきた（図 4 の 3）。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。

偽のメールには、請求書 1 の支払いに関する SWIFT メッセージ[5]が添付されていた。このタイミングが偶然であるか、意図的なものかは不明だが、結果として、メールの真偽性に注意を払われにくい内容のメールであったため、A 社担当者は偽のメールであると気づくことができなかった可能性がある。

なお、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。

また、本事例の攻撃者は A 社と B 社両方になりすまし、それぞれに偽のメールを送っていたものと思われるが、B 社側へ送られたメールについては、情報提供外のため不明である。

[5] 国際銀行間通信協会(Society for Worldwide Interbank Financial Telecommunication：SWIFT)の略称で、国際送金の際に使われる金融機関のメッセージフォーマット。

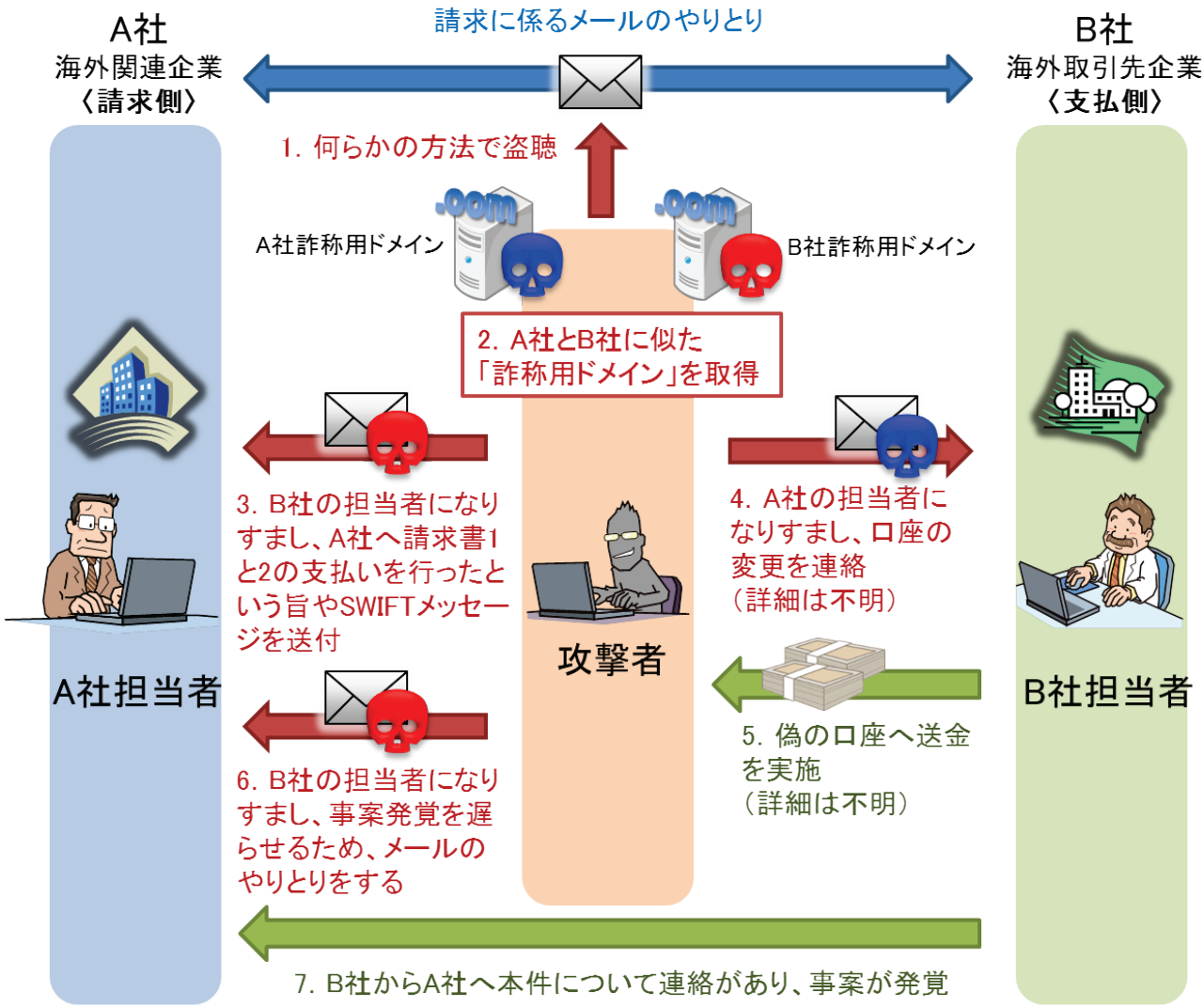

図 4 事例 2 本事例の概要図

攻撃者は、B 社とのやりとりの中で取引口座が偽の口座に変更となった旨を連絡し、それを信用した B 社は偽の口座へ送金を実施してしまった（図 4 の 4～5）。攻撃者はその後も、事案発覚を遅らせるための引き伸ばし工作と思われるメールのやりとりを A 社と行っていた（図 4 の 6）。

本事例では B 社は偽の口座へ振り込みを行ったため、当然ながら A 社は支払いを受けていない状況にあった。このため、A 社は送金の状況を B 社へ確認しようとするが、B 社になりすました攻撃者が話を合わせ、偽のメールを送り続けてきた。図 5 は、攻撃者が A 社に対して行った、引き伸ばし工作と思われるメールのやりとりである。4 月 7 日、A 社は、攻撃を見破っていたわけではないが、攻撃者のメールアドレスではなく、正規の B 社担当者へメールを送信している。これをきっかけに双方で詐欺に気づける可能性はあったが、実際には 4 月 24 日まで事案の発覚が巧妙に引き伸ばされたものと考える。

特に、図 5 の⑧では、A 社へ送金されていない状況を取り繕うため、攻撃者は「銀行へ確認中であり、送金が正しくなされていないようなので、一旦返金を受けてから再送金する」という内容で、銀行から送られてきたというメール（捏造と思われる）を引用するなど、更に長い期間の引き伸ばしを試みた形跡がある。この事例では、何らかの理由で攻撃者の手元まで金銭が届いておらず（海外の経由銀行で送金を止めていた可能性がある）、攻撃者は時間を稼ぐ必要が生じていたものと考えられる。

図 5 事例 2 攻撃者とのやりとり（引き伸ばし工作）

（2） 詐称用ドメインの取得と悪用

攻撃者は、A 社および B 社へ攻撃メールを送る際に、両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、次の例に示すようなものであった。

<<A 社の詐称用ドメイン>>

【本物のメールアドレス】alice @ a-company . xx
【偽物のメールアドレス】alice @ a-company-xx . com （「.」を「-」に変更し、末尾は「.com」）

※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>>

【本物のメールアドレス】bob @ b-company . com
【偽物のメールアドレス】bob @ b-comppany . com （p を一文字追加）

※実際に悪用されたものとは異なる。

なお、本事例の詐称用ドメインを取得した者は、ドメインの登録情報（whois 情報）から、このドメイン以外にも、実在すると思われる様々な企業のドメインに似た偽のドメインを多数取得していたと思われる形跡が確認できた。この者は、ビジネスメール詐欺や、その他のサイバー犯罪を常習的に行っている攻撃者（あるいは攻撃グループ）である可能性が考えられる。

（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 Cc に設定したメールで請求に関するやりとりを行っていた。一方、攻撃者が B 社担当者になりすまして A 社の担当者へ送り付けた偽のメールでは、同報先（Cc）に、B 社の複数の担当者のメールアドレスを詐称用メールアドレスに改変していた。

同報されている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メール受信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。

3.3 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少なくない。

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、本書事例では、送金に関わる銀行によりビジネスメール詐欺に気づけたという事例もあった。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　OLE 機能を悪用した文書ファイルの手口

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 文書ファイルを用いた攻撃手口の情報を入手した。

メールに添付される Office 文書ファイルによる攻撃の多くは、Microsoft Office の「保護ビュー」の機能で防御することが可能であり、本攻撃手口も「保護ビュー」を有効にしている状態ではウイルスに感染しないことを確認している。

マクロ機能の悪用に対してはマクロ機能を有効にしないように徹底することで危険を避けることが可能だが、今回確認した手口では、1 つのファイルに複数のマクロが埋め込まれており、繰り返しマクロの有効化を求める警告画面が表示されるというものであった。利用者ひとりひとりにこの手口の注意点を周知するべく、参加組織へ情報共有を実施した。

この手口について、今後、日本語での攻撃メールで使われるようになる可能性もあるため、攻撃手口と注意点をまとめた一般利用者向けの資料を、本書の参考資料とした [6]。

IPA で確認できている範囲では、英語のメールではあるが、国内への攻撃に使用されていることを確認しており、2019 年 6 月時点では、日本語のメールで攻撃が行われた可能性を示す情報は確認していない。攻撃の特徴、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だと考える。必要に応じ、参考資料を活用していただきたい。

[6]【参考情報】OLE 機能を悪用した文書ファイルの手口に関する注意点

5　オープンソースの解析ツール「Ghidra（ギドラ）」の紹介

2019 年 3 月 6 日（日本時間）、米国の国家安全保障局（NSA）より、オープンソースのリバースエンジニアリングフレームワークである「Ghidra」が公開された。

Ghidra には静的解析のための機能が含まれており、これをウイルス解析に使用する場合の長所や短所、また、広く使われている類似ツールとの比較の観点から、同様のリバースエンジニアリングツールである IDA Pro との機能的な異同の概要を確認した結果を、本書の付録とした[7]。

サイバー攻撃は、あらゆる企業・組織に対して試みられている。このような状況の中、実被害が発生したか否かに関わらず、自組織に対して試みられた攻撃について、分析し、その情報を蓄積し、更に可能ならば他組織と情報共有していくことには一定の意義があるものと考えられる。分析には様々な観点や方法があり、その一つとして、攻撃に用いられたウイルス等の不正ファイルの解析がある。

IPA セキュリティセンターでは、J-CSIP の運用をはじめとして、サイバー攻撃の情報を分析するため、必要に応じてウイルス等の解析を行っている。ウイルス解析は、一般的に、表層解析、動的解析、静的解析といった手法が用いられ、各手法に応じて様々なツールが存在する。これらの作業は、環境整備、人的資源、工数等の問題から、簡単に実践できるような性質のものではないと思われるが、一部組織の CSIRT や ISAC 等では、取り組みを進めているところもあり、Ghidra も分析に使用するツールの選択肢として検討範囲に入ってくるものであると考えている。

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

[7] 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] 付録 ～オープンソースの解析ツール「Ghidra（ギドラ）」の紹介～