サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2019 年 1 月～3 月]

2019 年 4 月 25 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 3 月末時点の運用体制、2019 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 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）の体制となった（図 1）。

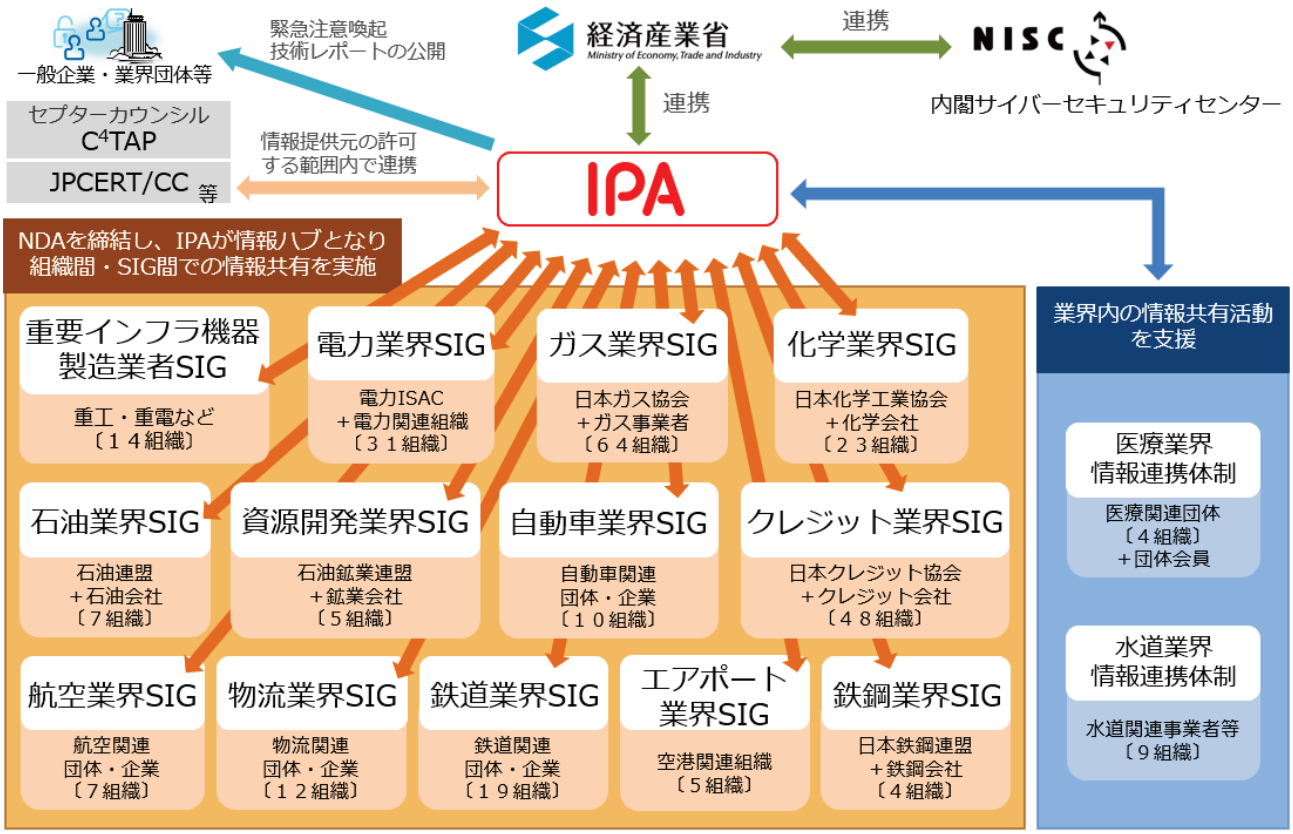

図 1 J-CSIP の体制図

[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（2019 年 1 月～3 月）

2019 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	2018 年			2019 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	191 件	519 件	1,072 件	**238 件**
2	参加組織への情報共有実施件数※1	49 件	39 件	59 件	**48 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 **15 件**を含む。

本四半期は情報提供件数が **238 件**であり、うち標的型攻撃メールとみなした情報は **47 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 9 割以上（45 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、ある程度特定の標的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。これについては、8 章で改めて述べる。

さらに、本四半期では 2018 年 10 月に行われたビジネスメール詐欺について分析を行った。詳しくは 4 章で述べるが、実際に被害を受けた事例である。同じく本四半期、2018 年 10 月に正規ウェブサイトに酷似した偽のウェブサイトが設置され、そのウェブサイトを使用した詐欺の事例について情報提供を受け、発覚に至る経緯と、実施した対応内容等を共有した。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、本四半期で確認した Office 365 のアカウント情報を狙ったメールには、正規の Microsoft サービスを悪用したフィッシングサイトの手口が見られた。これについては、6 章で述べる。

また、本四半期には、実在するグループ組織を騙るウイルスメールが、同グループ内の別の組織へ送られるという事例を確認した。文面は英語であるが、攻撃者は特定のグループ組織を狙いメール文面をカスタマイズしているものと考えられる。これについては、7 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	メールアカウントが乗っ取られ大量のフィッシングメールが送信された。	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。	4 件
3	公開ウェブサーバへ連続した探索用の不審な通信が行われた。	1 件

これらは、いずれも業務に少なからず影響が発生するものである。項番 1 は、前四半期に続いて[4]本四半期でも確認された事例であり、攻撃者によってメールアカウントが乗っ取られ、大量のフィッシングメールを送信するための踏み台にされたというものである。攻撃者によってメールアカウントが乗っ取られることがないよう、メールアカウントには複雑なパスワードを設定するとともに、二要素認証等の対策を行うことが必要であると考えられ、引き続き注意が必要である。

項番 2 については、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、継続して情報提供されている。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。通常業務の中でも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、PC 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[5]等にだまされないよう従業員への教育を行うべきである。

また、項番 3 は、公開ウェブサーバに対して、海外の複数の IP アドレスから、スキャンの一種と思われる多数の不審な HTTP リクエストが間欠的に発生したという事例である。この事例の探索行為については、ウェブシェルと呼ばれる不正なプログラムが公開ウェブサーバに設置されているかを確認するものであった。組織としては公開ウェブサーバへの探索通信は日々多く発生しているものと考えられるが、不審な IP アドレスからの通信を禁止する等のアクセス制限を行うといった対応が必要であろう。

[4] サイバー情報共有イニシアティブ（J-CSIP）運用状況[2018 年 10 月～12 月]（IPA）
https://www.ipa.go.jp/security/J-CSIP/
[5] 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（2018 年度）の合計と、J-CSIP を運用開始した 2012 年度から 2017 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	2012 年度	2013 年度	2014 年度	2015 年度	2016 年度	2017 年度	2018 年度
IPA への情報提供件数	246 件	385 件	626 件	1,092 件	2,505 件	3,456 件	2,020 件
標的型攻撃メールと見なした件数	201 件	233 件	505 件	97 件	177 件	274 件	213 件
参加組織への情報共有実施件数	160 件	180 件	195 件	133 件	96 件	242 件	195 件
参加組織数	5 業界 39 組織	5 業界 46 組織	6 業界 59 組織	7 業界 72 組織	7 業界 86 組織	11 業界 228 組織	13 業界 249 組織 ＋ 2 情報連携体制 13 組織

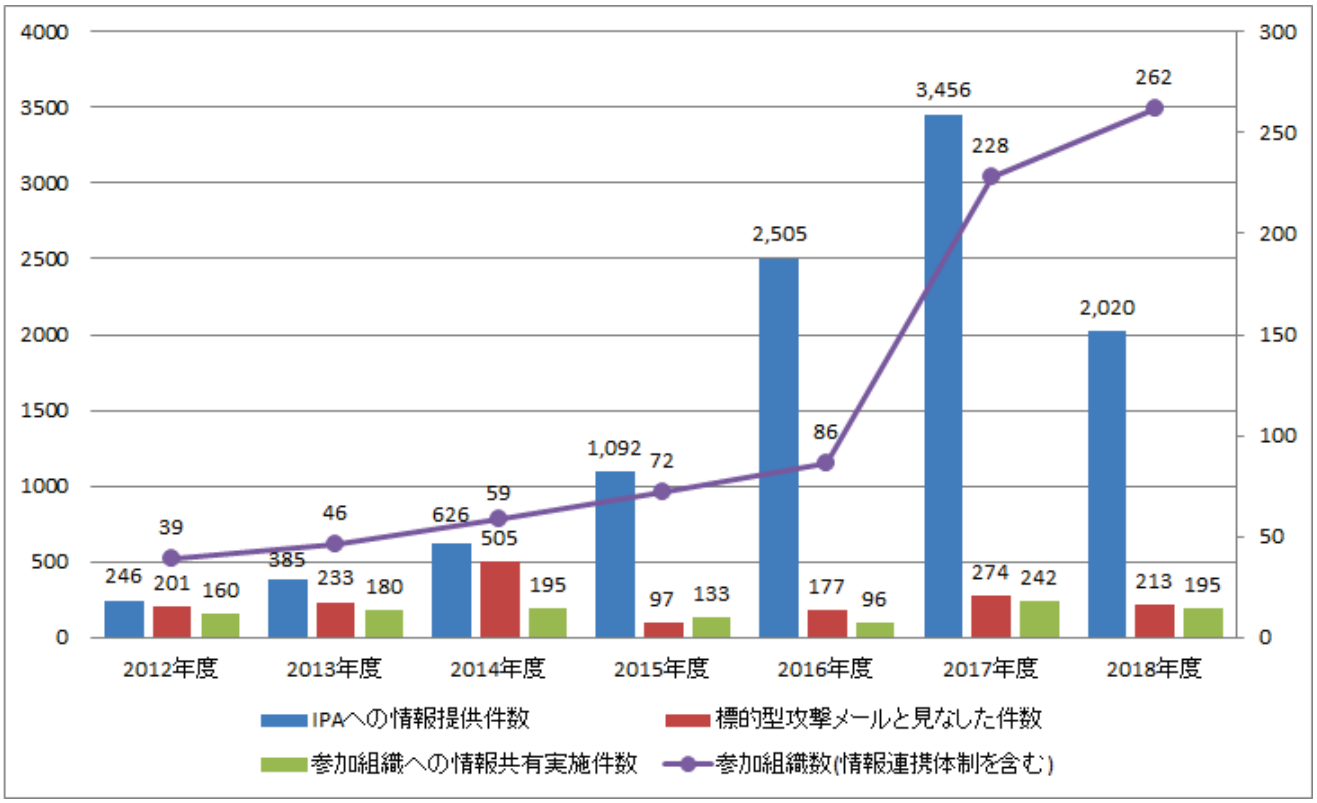

図 2 年間の取り扱い件数と参加組織数 グラフ

3.2 今年度の活動

2018 年度は、J-CSIP における新たな情報共有の実現形態として、「情報連携体制」の枠組みを開始した。IPA が情報提供を受け、必要に応じて分析・匿名化し、業界内で共有するという基本的な活動はこれまでと同等である。なお、秘密保持は、NDA ではなく規約への合意に基づくものとしている。2019 年 3 月末時点で、2 つの情報連携体制を運用している。

情報提供においては、2015 年 10 月頃から国内で多く観測されるようになった「日本語のばらまき型メール」が継続して観測されており、2018 年 8 月には IQY ファイルを悪用した日本語のばらまき型メールの提供が多くあった。この手口については、2018 年 4 月～6 月の運用状況レポート[6]に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も継続して情報提供を受けている。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。この手口については 8 章で改めて述べる。

一方、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。ただし、日本国内全体では攻撃が発生しており、国内への標的型攻撃は依然として継続している状況である。これについては、引き続き注意が必要である。

3.3 特筆事項

2018 年 7 月、IPA としては初めて「日本語のビジネスメール詐欺」について、実際のメール内容の情報提供があった。この事例を含め、これまで J-CSIP 活動の中から得られた情報を整理し、レポート「ビジネスメール詐欺『BEC』に関する事例と注意喚起（続報）」[7]を 2018 年 8 月 27 日に公開した。ビジネスメール詐欺は、巧妙に細工したメールのやりとりにより、企業の経理部門等の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。レポートの公開後も、J-CSIP 参加組織からビジネスメール詐欺の事例情報が継続して提供されている。これらの情報については、J-CSIP 内で共有を行うとともに、運用状況レポートでも事例として公開している。今後もこの攻撃は続くと考えられるため、対策の徹底が必要である。

その他、単純な金銭目的ではない、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。

---

[6] サイバー情報共有イニシアティブ（J-CSIP）運用状況[2018 年 4 月～6 月]（IPA）
https://www.ipa.go.jp/security/J-CSIP/

[7] 【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

4　ビジネスメール詐欺（BEC）の事例

2018 年 10 月、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。この事例では、実際に金銭被害が発生している。今回の事例はすべて英文のメールでのやりとりであった。

4.1 事例の概要

本事例は、2018 年 10 月、参加組織の国内企業（A 社）と、その海外取引先企業（B 社）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、偽の振り込みを要求するメールがA 社に送られたものである。IPA が 2017 年 3 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くことができなかったため、金銭的な被害を受けた。

本事例では、詐欺の過程において、次の手口が使われた。

- 詐称用メールアドレスの取得と悪用
- 詐称元企業の文書様式の入手と偽造
- Reply-To ヘッダの悪用

（1） 詐称用メールアドレスの取得と悪用

攻撃者は、A 社へ攻撃メールを送る際に、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」を取得していた。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ドメインに一文字アルファベットを追加したものであった。

【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、本件の B 社を詐称するための詐称用ドメインを取得した人物は、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。これは、ドメインの登録情報（whois 情報）から、その形跡を確認している。本件の詐称用ドメインを取得した人物は、ビジネスメール詐欺や、その他サイバー犯罪を常習的に行っている攻撃者である可能性が考えられる。

(2)詐称元企業の文書様式の入手と偽造

本事例では、A社(国内企業)とB社(海外取引先)の間でビジネスメールをやりとりしていた中に、詐称用ドメインを使って B 社の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。

このやりとりの中で、攻撃者から送られた新しい銀行口座情報(偽の口座)について、A 社から攻撃者に対して、B社の口座であることの証明書の提出を要求した。これに対し、攻撃者は、A社担当者になりすまし、B 社担当者に対して社印と署名の入った文書を要求することで、証明書の偽造に必要な材料(B 社が発行する文書の様式等)を入手した。攻撃者はこれを悪用して、一見B社が発行したかのように見える偽の口座変更の文書を作成(偽造)し、A 社へ送信した。そして、A 社担当者は、偽造された書類が本物であると誤認し、偽の口座への振り込みを実施してしまった。

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。

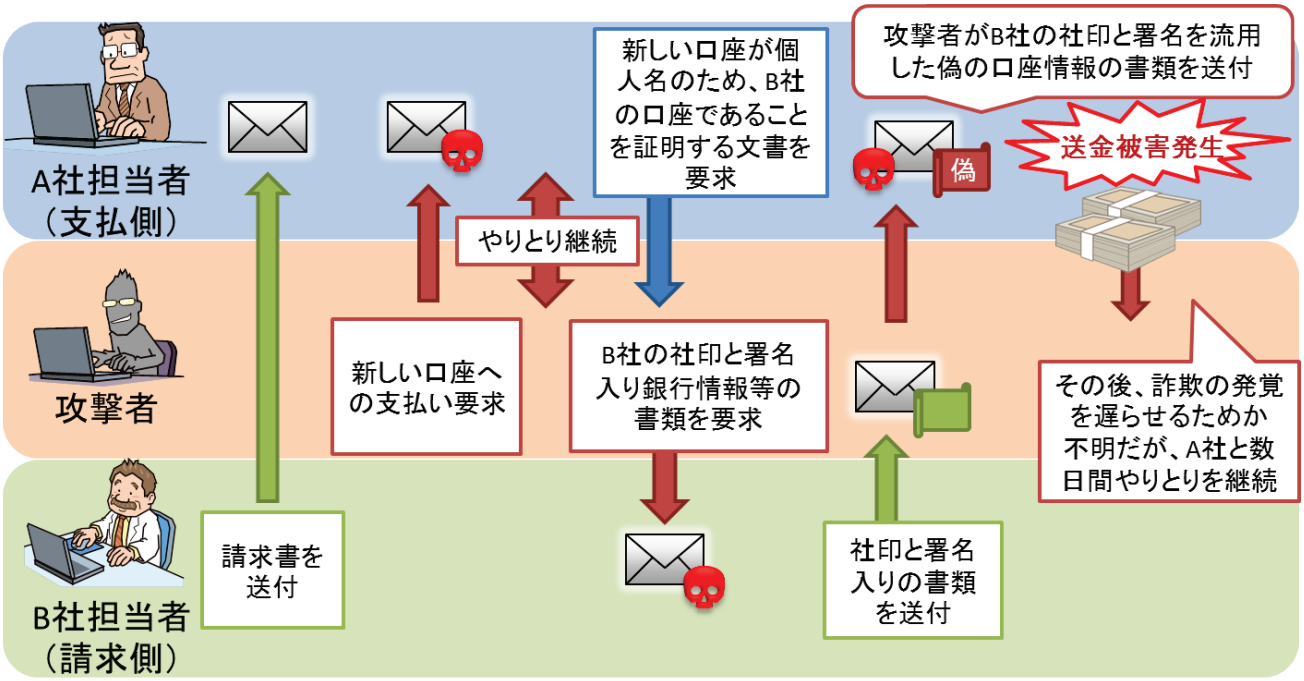

図 3 攻撃者とのやりとり

（3）Reply-To ヘッダの悪用

攻撃者は、A 社担当者になりすまして、B 社担当者へ社印と署名入りの銀行情報等の書類を要求するメールを送信する際、From ヘッダ（差出人）を本物の A 社担当者のメールアドレスに、Reply-To ヘッダ（返信先）を攻撃者のメールアドレスに設定し、細工を行っていた。

このように細工された状態では、メールを受信して画面表示をしている時の差出人表示は、本物の A 社担当者のメールアドレスが表示され、正規のメールに見える。一方、「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、メール作成画面では、Reply-To ヘッダに設定された攻撃者のメールアドレスが宛先となる。

この手口により、攻撃者は、B 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 A 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。

4.2 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態である。

被害に遭わないようにするためには、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の注意力を高めることが重要である。また、社内ルール等を整備し、組織全体で被害を防ぐ体制作りも必要であろう。社内だけでなく、取引先に対してもビジネスメール詐欺への注意を促し、被害防止に向けて検討していただきたい。

5　自組織を騙る偽サイト設置による詐欺事例

2018 年 10 月、J-CSIP 参加組織の正規ウェブサイトに酷似した、偽のウェブサイトが設置され、そのウェブサイトを使用した詐欺が試みられたと思われる事案について情報提供があった。本章では、事案の発覚までの経緯と、実施した対応内容、及び偽のウェブサイトの特徴等について説明する。

本件の事案発覚までの経緯と対応内容

攻撃者が騙った架空の企業（X 社）の代表取締役を名乗る人物から、海外企業（B 社）の職員に対し、X 社の事業に勧誘する詐欺メールが送られた。B 社の職員は、その人物と数回のメールのやりとりを行い、その過程で、X 社のウェブサイト（国内組織の正規ウェブサイトを基に作成された偽サイト）を確認した。

その後、B 社の職員が、国内組織（A 社）へ確認のための連絡を行ったことにより、X 社が偽物であり、X 社を騙る詐欺が行われているであろうこと、また、詐欺のための偽サイトが存在することが発覚した。

偽サイトは、X 社の社名でウェブ検索すると上位に表示されるようになっており、攻撃者が X 社の存在を信じ込ませるために作成したものと考えられる状況であった。

これに対し、A 社は直接的な詐欺の被害に遭ったわけではないが、詐欺に巻き込まれた状態となり、次の対応を実施した。

- A 社と偽サイトが無関係であること等、偽サイトに関する注意喚起を公開
- ドメイン管理業者等へ、偽サイトを停止させるための調整を実施

ドメイン管理業者等への調整の結果、約 3 週間程度で偽サイトにはアクセスできない状態となった。

本事案で作成された偽サイトの特徴

偽サイトは、A 社の正規ウェブサイトのコンテンツをコピーしたもので、見た目、クリックした際の画面遷移、日本語版と英語版のページがある点など、A 社の正規ウェブサイトに酷似していた。

一方、偽サイトでは次の点が改変されていた。

- ◆ 会社の名称、社名ロゴ
  （トップページ等に表示される社名やロゴだけでなく、公開している PDF 等の文書ファイル中のロゴも、X 社のものに改変されていた）
- ◆ 代表取締役の名前、その他会社役員 1 名の名前

これらは攻撃者が意図的に改変したものと思われ、詐欺を行う上で、架空の企業の代表取締役になりすますことが目的であったと考えられる。

偽サイトを停止させるための調整

A 社は、偽サイトを停止させるため、次の機関・団体へ連絡し、ドメインやウェブサイトの停止を試みた。

- ◆ ICANN（ドメイン名等の調整団体）[8]
- ◆ 偽サイトで使われているドメイン名の管理業者（レジストラ）
- ◆ 偽サイトが稼働している IP アドレスの管理業者（ホスティング等の業者）
- ◆ FBI（米連邦捜査局）[9]

その結果、約 3 週間後に偽サイトで使われているドメイン名の管理業者（レジストラ）より、停止措置を行った旨の連絡があり、偽サイトのドメイン名の設定が無効化され、偽サイトへアクセスできなくなったことを確認した。

本事例では、偽サイトで使われているドメイン名の管理業者（レジストラ）によって停止措置が行われた。ただし、どのような調整が最も効果的であるかは、状況により異なると考えられる。同様の事案が発生した際には、上記のように、可能な範囲で関係機関・団体へ並行して調整を行うことを検討する意義はあるものと考えられる。

[8] Internet Corporation for Assigned Names and Numbers（ICANN）
https://www.icann.org/

[9] Federal Bureau of Investigation（FBI）
https://www.fbi.gov/

6　正規の Microsoft 社のサービスを悪用したフィッシング

本四半期、正規の Microsoft 社のサービスを悪用し、フィッシングサイトが構築されていた攻撃事例について情報提供があった。本章では、実際に攻撃に使われたフィッシングメールと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 4）は、「Office 365 のアカウント情報が古くなっており、サービスの利用を続けるためには、ログインしてアカウント情報の更新が必要である」という内容が英語で書かれていた。また、メール本文中には URL リンクが書かれていた。この URL リンクをクリックすると、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（図 5）へ誘導される。

このフィッシングサイトは、正規の Microsoft Azure Storage のホスティングサービス [10]を悪用して構築されていた。このため、当該ウェブサーバ（フィッシングサイト）へアクセスした場合、URL 中のホスト名が「～.windows.net」（Microsoft 社が保有するドメイン名）となっているだけでなく、SSL サーバ証明書も Microsoft 社であることを証明する正規のものであった。そのため（図 6）、フィッシングサイトであると見破ることを難しくしている。

本件と同様の手口は 2018 年 10 月頃から観測 [11]されており、複数の公開情報から、メールの文面やフィッシングサイトの画面には、様々なバリエーションが存在していることを確認している。また、それら事例において、攻撃者の狙いが Microsoft 社のクラウドサービス（特に Office 365）のアカウント情報であることは概ね共通していると考えられる。特に企業・組織においては、利用者のアカウントから組織内の情報等が侵害される可能性をもたらす脅威として、注意を要する攻撃である。

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、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、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る。より詳しくは、フィッシング対策協議会 [12]のウェブサイト等も併せて参照いただきたい。

---

[10] Azure Storage で静的 Web サイトの一般提供を開始（Microsoft）
https://blogs.technet.microsoft.com/mssvrpmj/2018/12/18/static-websites-on-azure-storage-now-generally-available/

[11] Phishing Attack Uses Azure Blob Storage to Impersonate Microsoft（Bleeping Computer）
https://www.bleepingcomputer.com/news/security/phishing-attack-uses-azure-blob-storage-to-impersonate-microsoft/

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

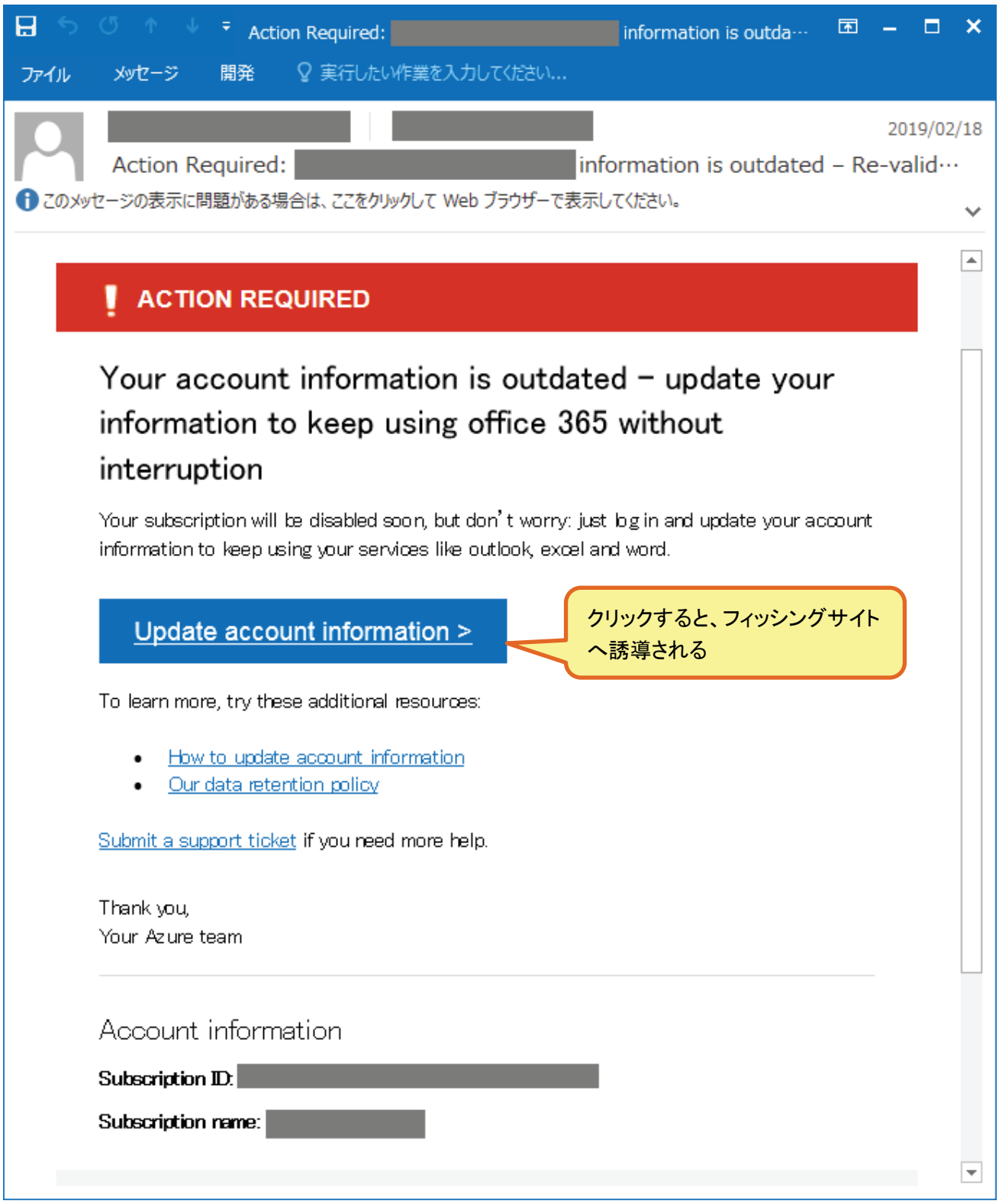

図 4 攻撃者から送信されたフィッシングメール

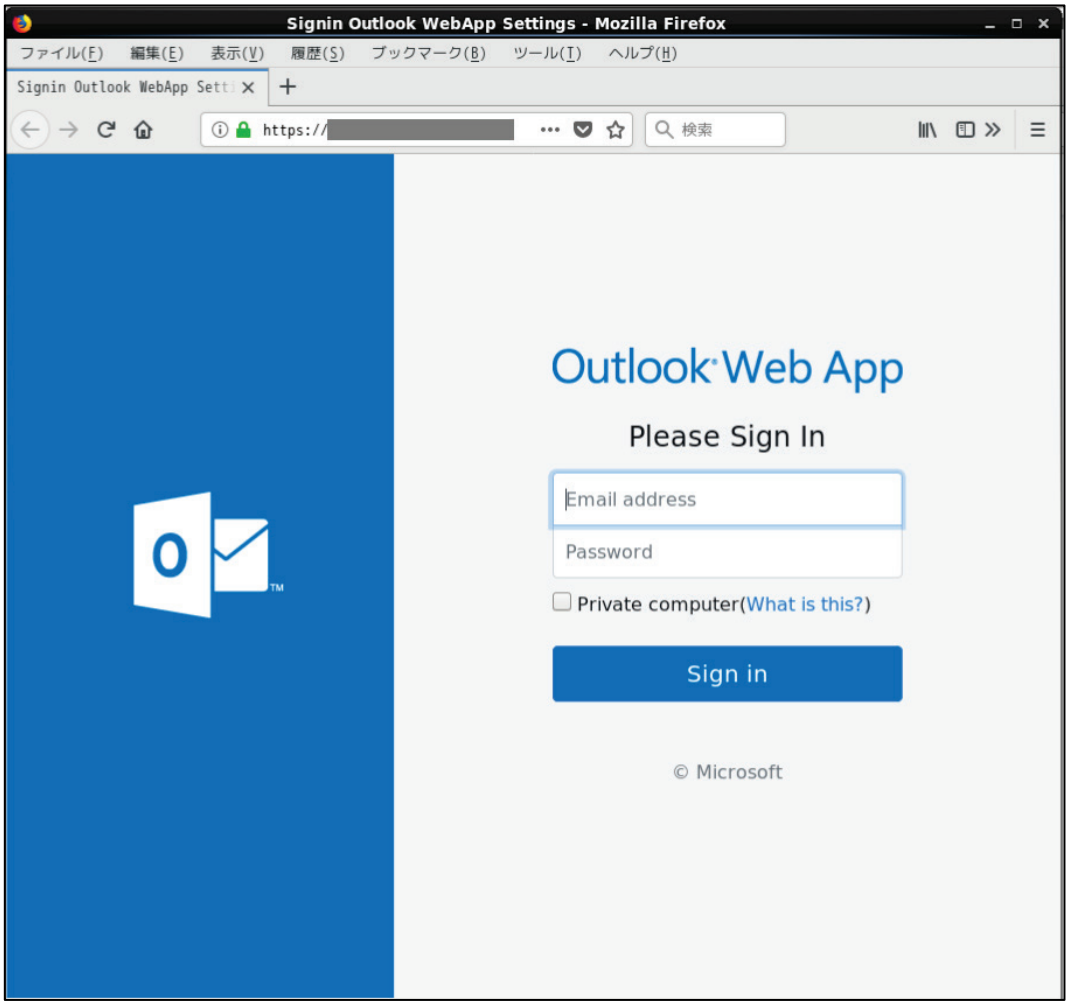

図 5 フィッシングサイトの画面

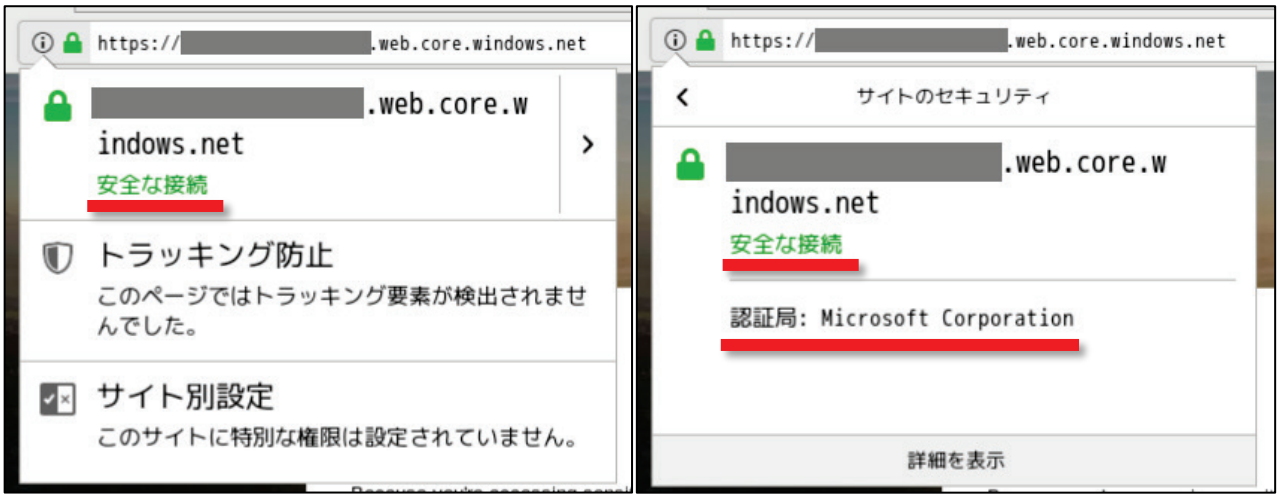

図 6 ウェブサイトの証明書の確認画面（正規の証明書）

※ 図 6 は、本事例と同様の手口が使われているウェブサイト（フィッシングサイト）を Firefox で開いた結果表示される画面において、サイトの接続の安全性について表示した例である。

7　実在する組織を騙った攻撃メール

本四半期、グループ企業内の実在する組織を騙り、同グループ内の別の組織に対し、ウイルスを感染させることを目的とした攻撃メールが送られたとの情報提供があった。本章では、送信された攻撃メールとその攻撃手口について説明する。

攻撃メール（図 7）は請求書の支払いを装う英文のメールである。この点においては、広くばらまかれているウイルスメールのように見える。しかし、本件の場合、メール本文中に実在する社員の名前や、送付先の組織名等が正しく記載されていた。また、このメールは、当該組織において 1 通（1 人）のみ着信がを確認されていた。攻撃者は無差別にウイルスメールをばらまいたのではなく、ある程度標的を定めて攻撃メールを送り付けた可能性がある。

本文中の URL リンクをクリックすると、マクロ付きの Word 文書ファイル（図 8）がダウンロードされる。この Word 文書ファイルには、「オンラインバージョンの Word で作成された文書である」と書かれている。そしてその内容を表示させるため、保護ビューの解除や、マクロの有効化の操作を行わせるよう誘導する文言が記載されている。利用者がこの偽の指示に従ってマクロを有効化してしまうと、ウイルスに感染させられてしまう。

図 7 攻撃メール

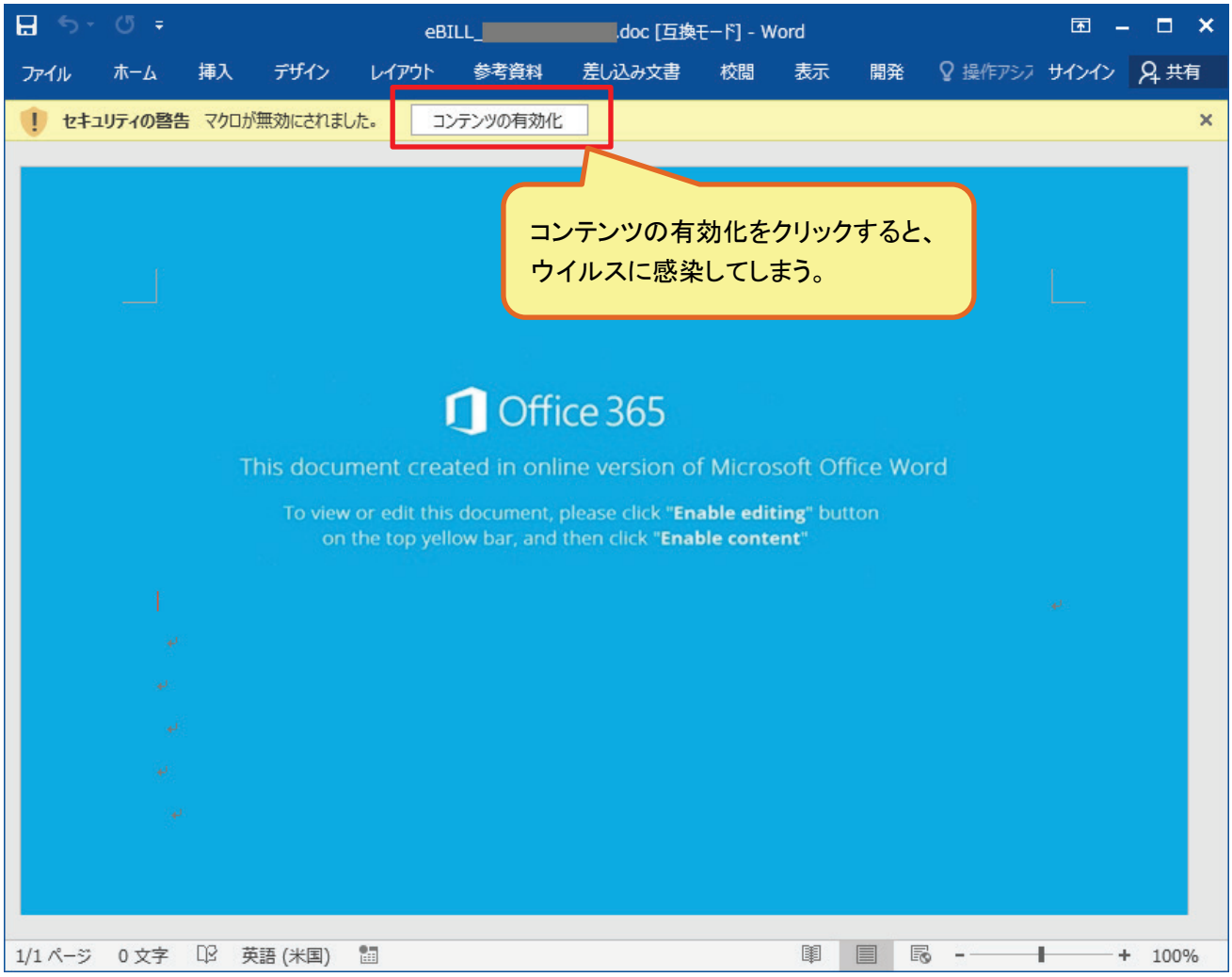

図 8 攻撃メールの URL リンク先からダウンロードされる Word 文書ファイル

請求書の送付を装った英文のウイルスメールは、業界に偏らず広く無差別にばらまかれることもあるが、本事例のように、実在する社員の名前等を使った巧妙なものも存在する。この攻撃に限らず一般的なウイルス対策（ウイルスメール対策）ではあるが、次のような対策を徹底していただきたい。

- **脆弱性の対策**
  - OS やブラウザ、Office 製品等の修正プログラムを適用し、常に最新の状態にする。

- **セキュリティソフトの最新化**
  - セキュリティソフトの定義ファイル等を常に最新の状態にする。

- **メール利用者への注意点の徹底**
  - メールに添付されているファイルや、外部からダウンロードしたファイルは、安全と判断できるもの以外は不用意に開かない。
  - ファイルを開く前に、ファイルのプロパティ等によって「ファイルの種類」を確認する。「アプリケー

ション」や「Script」等、文書ではない形式の場合は、危険を及ぼす可能性がある。

- 文書ファイルを開いた際、マクロの有効化が求められたり、警告ウインドウが表示された場合、「はい」や「OK」を不用意にクリックしない（表示された警告等の意味が分からない場合は操作を中断する）。
- メールに記載されている URL リンクには、安全と判断できるもの以外は不用意にアクセスしない。
- 少しでも不審に感じたら、組織内のシステム管理部門／セキュリティ部門／CSIRT 等へ連絡する。

8 プラント関連事業者を狙う一連の攻撃（続報）

2018 年度も、2017 年度に引き続き、プラント等の設備や部品のサプライヤーに対し、偽のメールを送り付け、添付ファイル（ウイルス）を開かせようとする攻撃を多数観測した。そのメールは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であった。

偽のメールで、使われている英文には不審な点は少なく、プラントの設計・調達・建設に関わる企業や資機材等について一定の知識を持つ者が作成したものと思われ、巧妙である。無作為に個人を狙うような攻撃ではなく、プラント関連事業者を標的とした攻撃であると推測している。また、短期間で多岐にわたる文面のバリエーションがあることを確認しているが、J-CSIP 内の数組織で確認している同等のメールの着信数はそれぞれ数通から数十通程度であり、その点でも、広く無差別にばらまかれているウイルスメールとは様相が異なっている。

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）ものか、あるいはビジネスメール詐欺（BEC）のような詐欺行為の準備段階のものかは不明である。もしくは、プラントの設計・調達・建設に関わるサプライチェーン全体を攻撃の対象としている可能性（セキュリティが比較的弱い可能性のある、下流の資機材メーカーを侵入の入口として狙っている可能性）もありうる。いずれにせよ、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。

8.1 攻撃の観測状況

本件の攻撃は、2017 年 10 月から観測しており、これらの攻撃メールの情報を継続して J-CSIP 参加組織へ情報共有を行っている。着信が確認される組織は複数あるが、ある程度限定的である。

2017 年 10 月から 2019 年 3 月までに確認している限り、これら攻撃メールは、メールの文面、メールの送信元 IP アドレス、メールの Reply-To ヘッダ、添付されているウイルスの種類や不正接続先といった要素で共通点がみられる。従って、同一の攻撃者（または攻撃グループ）による一連の攻撃であると推定している。

現時点でも攻撃は継続している。

8.2 攻撃手口の変化

本四半期においても、攻撃者は標的とする組織に対し、メールの文面等を変化させながら、執拗に攻撃メールを送り付けている。これまで、J-CSIP 内で確認している攻撃手口で最も多い攻撃手口は、実行ファイルを圧縮したファイルを添付したもので、これらは全て、PC 内の情報の窃取を目的とするウイルス（図 9 のウイルス B）への感染を狙うものであった。このウイルスを使う手口の他、この攻撃者は複数の攻撃手口を使って攻撃を行っている。

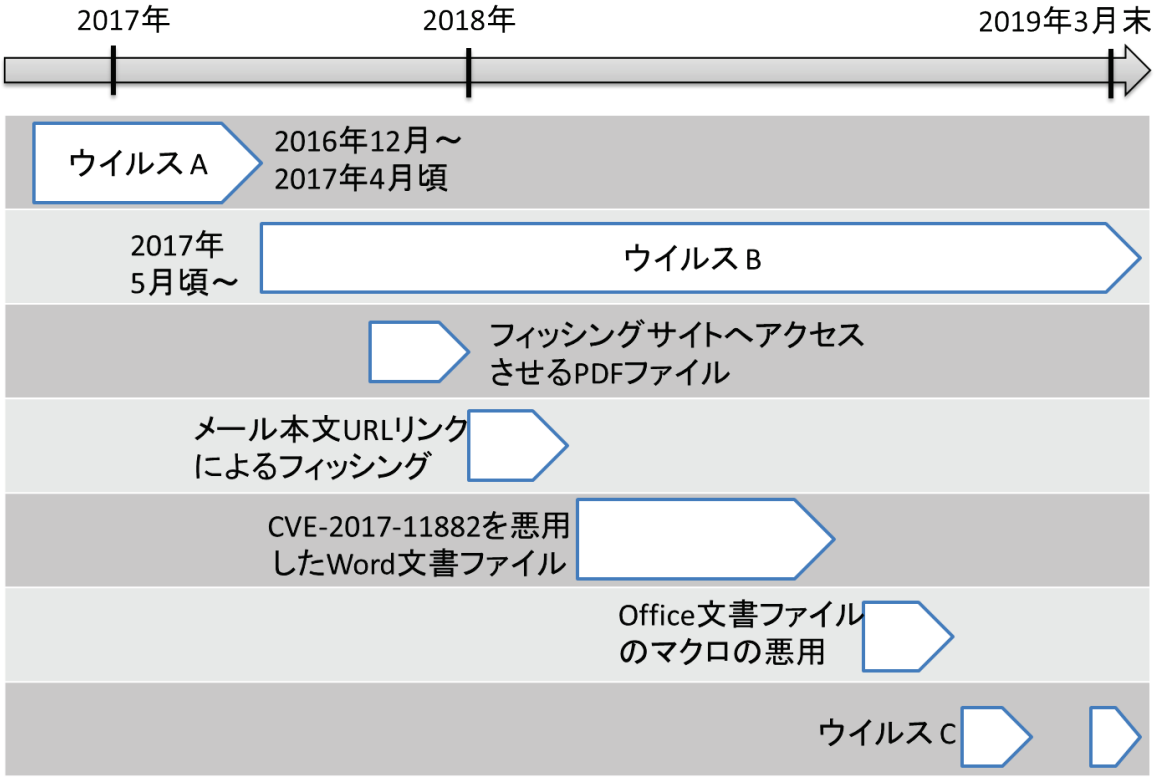

図 9 プラント関連事業者を狙う一連の攻撃手口の変化

8.3 まとめ

プラント関連事業者を狙う一連の攻撃について、現時点で確認できている状況を紹介した。単純な文面の提案依頼（RFP）、見積もり依頼（RFQ）、請求書等を装うウイルスメールは多種多様な事例があるが、この攻撃者は、プラントの資機材について詳細な内容の偽のメールを作成し、また、対象を絞って長期に渡り攻撃メールを送り付けてきている。攻撃対象は、無差別ではないものの、広くプラント関連事業者全般となっている可能性がある。

また、攻撃手口についてもウイルスを直接メールに添付して送り付ける手口の他、フィッシングサイトへ誘導する手口、Office の脆弱性を悪用する手口等がみられる。

J-CSIP には、プラントに関わる事業者が多く参加している関係上、注意を要する攻撃者であると考えており、今後も本攻撃者の動向を注視していく。

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