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]

2018 年 7 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、2018 年 6 月末時点の運用体制、2018 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

2018 年 4 月～6 月期（以下、本四半期）は、新たに医療業界での「情報連携体制」の運用開始、電力業界 SIG で参加組織の増加があり、全体では 2018 年 3 月末の 11 業界 228 組織の体制から、11 業界 229 組織[2]＋1 情報連携体制（4 団体およびその会員約 5,500 組織）の体制となった（図 1）。

- 2018 年 4 月、電力業界 SIG に新たな参加組織があり、30 組織から 31 組織となった。
- 2018 年 5 月、新たに「医療業界 情報連携体制」を運用開始した。

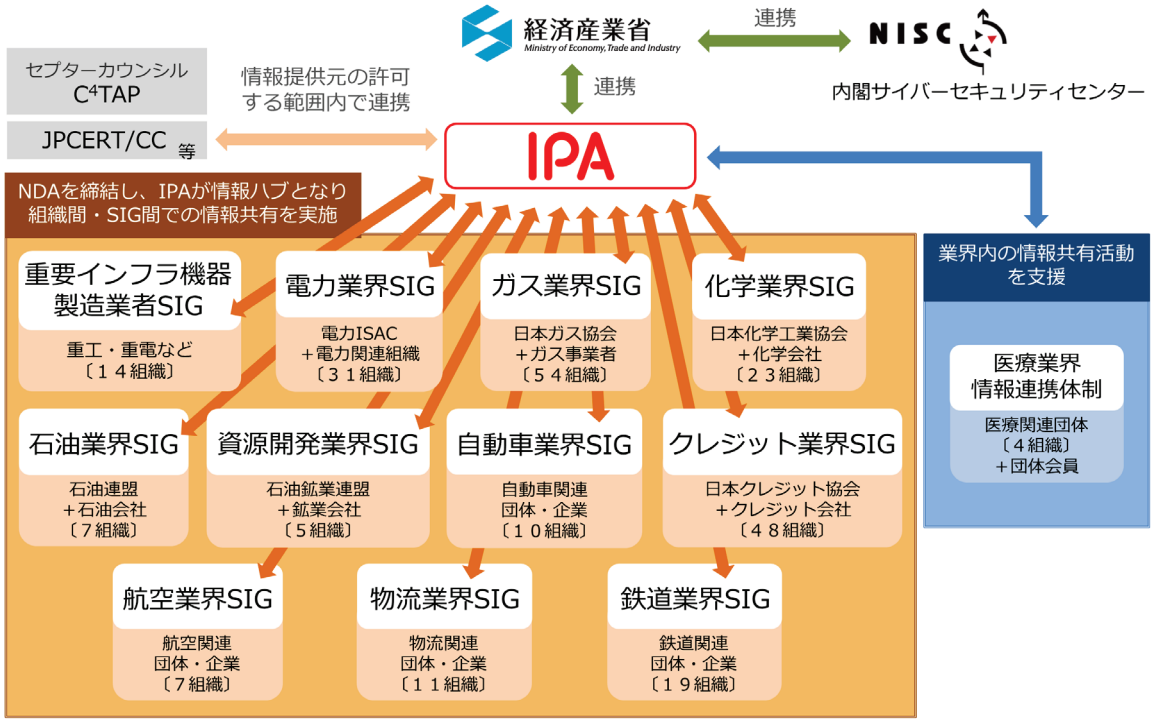

図 1 J-CSIP の体制図

「情報連携体制」について

2018 年 5 月より、J-CSIP における新たな情報共有の実現形態として、運用ルール等を必要最小限としつつ、より多数の組織間での情報共有活動を支援可能とする、「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り、各業界団体が活動に参加する会員組織のとりまとめとして IPA と連携を行う。また、秘密保持は、NDA ではなく規約への合意に基づくこととしている。

本四半期、医療業界における情報連携体制を運用開始し、当該体制は、医療関連 4 団体およびその会員（医療機関等約 5,500 施設）が参加する活動となっている。

[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（2018 年 4 月～6 月）

2018 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、11 の SIG、全 229 参加組織と、1 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	2017 年		2018 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	57 件	1,930 件	256 件	**191 件**
2	参加組織への情報共有実施件数※1	17 件	123 件	76 件	**49 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 **191 件**であり、うち標的型攻撃メールとみなした情報は **43 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約 8 割（34 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、6 章で改めて述べる。

さらに、本四半期でもビジネスメール詐欺が試みられたという事例を引き続き観測した。詳しくは 7 章で述べる。ビジネスメール詐欺は、2017 年 12 月に国内企業での大規模な被害事例が報道され、また、2018 年の IPA の 10 大脅威（組織編）[4]でも第 3 位にランクインしている。更に 2018 年 7 月 4 日には、日本国内で数千万円規模のビジネスメール詐欺に関与した疑いにより 4 人が逮捕される [5]等、差し迫った脅威となっており、ますます注意が必要な状況にある。

この他、本四半期には、国内組織を狙ったと思われる標的型攻撃の情報を IPA で入手し、その手口を分析した。一部の標的型攻撃については、J-CSIP 参加組織より提供を受けたものもある。これについては、3 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 （IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

[4] 情報セキュリティ 10 大脅威 2018 （IPA）
https://www.ipa.go.jp/security/vuln/10threats2018.html

[5] ビジネスメール詐欺 7000 万円送金させた容疑で逮捕 （毎日新聞）
https://mainichi.jp/articles/20180705/k00/00m/040/013000c

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、本四半期に確認した Office 365 のアカウント情報を狙ったメールには、宛先組織のドメイン名の一部をメールの本文内で使うといった手口や、特定の組織を狙う攻撃もみられた。これについては、4 章で述べる。

また、本四半期では Drupal[6]の脆弱性を悪用した攻撃を観測した。本件の脆弱性に限らず、脆弱性の公開から攻撃発生までの期間は短くなっている傾向にあり、修正プログラムの適用までの間に、いかにして攻撃を防ぐのかという観点も検討が必要である。これについては、5 章で述べる。

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	自組織を騙るばらまき型メールが取引先に対して送られた。	2 件
2	自組織外で実施している標的型攻撃メール訓練のメールが送られてきた。	2 件
3	Cisco Smart Install Client を悪用した攻撃を確認した。	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。	5 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、特に、項番 1 のように、自組織が詐称されて攻撃メールをばらまかれるという事態は、いつ発生するか分からない。外部組織からの問い合わせ等に適切かつ迅速に対応できるよう、対応方針や対応手順を定めておくべきである。例えば、情報収集・状況把握の体制の整備、対応窓口の設置、自組織のウェブサイトでの注意喚起の公開等が考えられる。

項番 2 は、標的型攻撃メールの疑いありとして IPA へ提供された不審メールを調査したところ、当該組織外で実施していた標的型攻撃メール訓練のメールが着信したというものであった。今回の 2 件では特段の問題とはなっていないが、標的型攻撃メール訓練を実施する場合、必要十分な範囲で対象となる組織の情報システム部門等へ事前連絡をしておくべきであろう。

項番 3 については、ネットワーク機器の脆弱性を悪用する攻撃であり、事象の発生前にベンダ等から攻撃の増加について注意喚起がなされていた。本件に限らず、自組織が使用している機器や製品の脆弱性情報を適宜入手し、対応を行う必要がある。

また、項番 4 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、これらはいずれも、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[7]等に騙されないように従業員への教育を行うことが重要である。

---

[6] Drupal（ドルーパル）は、オープンソースの CMS（コンテンツマネジメントシステム）。
https://www.drupal.org/

[7] 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　国内組織を狙う標的型攻撃

本四半期、IPA は、国内組織を狙う標的型攻撃に使用されたと思われる悪意のあるメールやウイルスに感染させるための細工が施されたファイルを複数確認した（表 3）。これらが実際に攻撃に使用されたか否かについては確証のないものもあるが、一部は、J-CSIP の参加組織内でも同件のメールやファイルが見つかっている。本章では、これらの攻撃手口を説明する。

今後も国内組織への攻撃が継続して行われる可能性があり、また、これらのファイルはメールの配送経路等で検知・検疫できるとは限らない。これらの攻撃手口を各利用者に認識していただくとともに、被害に遭わないよう注意していただきたい。

表 3 標的型攻撃で使われたと思われる悪意のあるファイル

項番	ファイル名	ファイル形式・特徴
1	●●概要.csv	細工が施された CSV ファイル
2	平成 30 年●●報告書 docx　　.exe	Word 文書ファイルのアイコンに偽装した実行ファイル
3	領収証.doc	マクロが含まれる Word 文書ファイル
4	●●ご案内 2.doc.docm	マクロが含まれる Word 文書ファイル
5	●●概況.ppsx	脆弱性を悪用する PowerPoint スライドショーファイル

※ファイル名の一部は「●」でマスクしている。

※項番 2 は、ファイル名の拡張子を偽装するため、docx と exe の間には複数の空白文字が埋め込まれている。

攻撃の手口

表 3 で挙げた悪意のあるファイルによる攻撃では、次のような手口が使われている。

- アイコンと拡張子の偽装 （項番 2）
- マクロの有効化操作の誘導 （項番 3, 4）
- CSV ファイルの悪用 （項番 1）
- PowerPoint スライドショーファイルによる脆弱性の悪用 （項番 5）

アイコンと拡張子の偽装

項番 2 は、Microsoft Word 文書のアイコンに偽装し、拡張子を「.docx」に見えるよう偽装した実行形式のファイルであった。このファイルを開くと、ウイルスに感染させられてしまう。これまでにも確認されている、利用者を騙してファイルを開かせる手口である。

マクロの有効化操作の誘導

攻撃者が作成した悪意のある Word 文書ファイルを開くと、文書ファイル内に仕掛けられているコードを実行させるため、マクロ機能を有効にさせるよう誘導する操作指示が日本語で書かれている（図 2、図 3）。

ここで、攻撃者の操作指示に従ってしまい、Microsoft Word のウインドウ上段部分にある黄色いセキュリティの警告バーにある「編集を有効にする」あるいは「コンテンツの有効化」といったボタンをクリックすると、文書ファイル内に仕掛けられているコードの実行を許すことになり、ウイルスに感染させられてしまう。

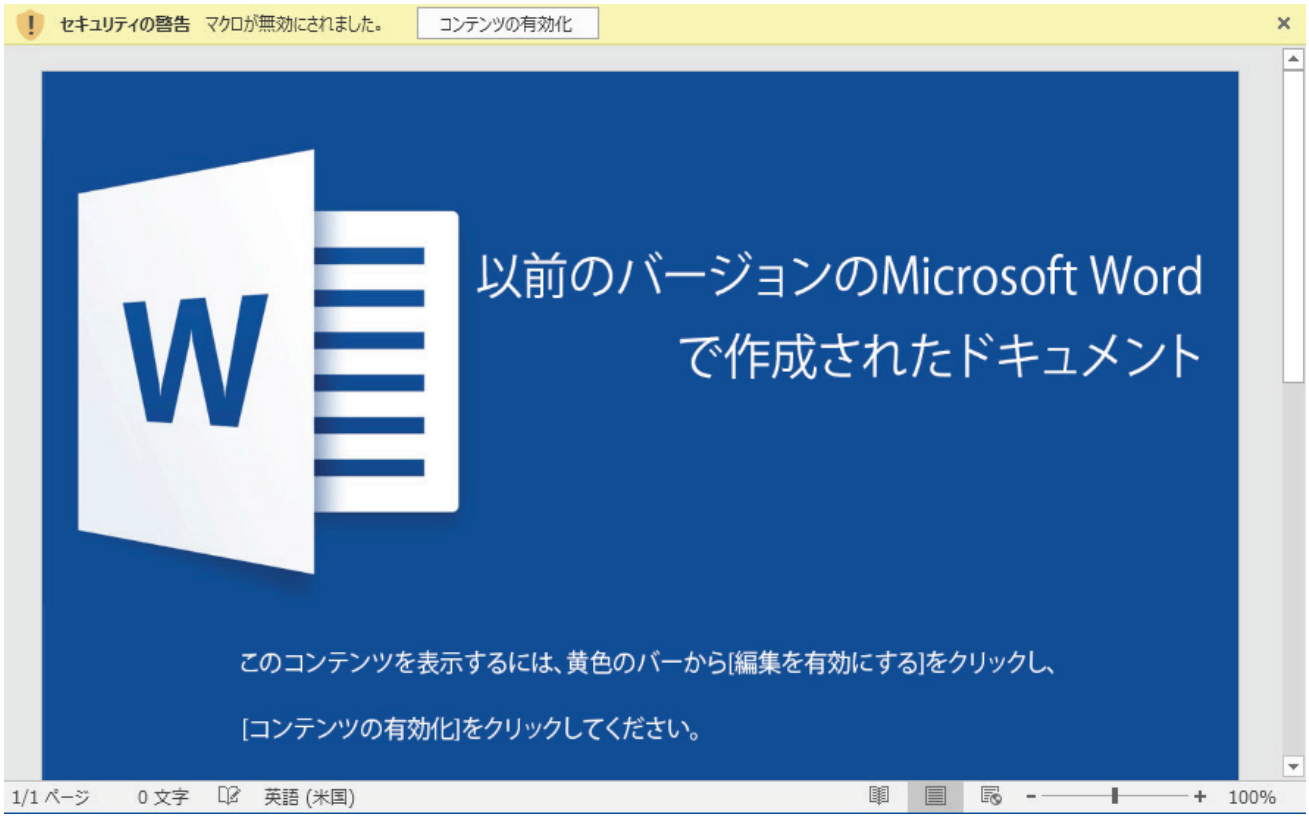

図 2 マクロ機能の有効化操作の誘導（項番 3 の事例）

図 3 マクロ機能の有効化操作の誘導（項番 4 の事例）

CSV ファイルの悪用

悪意のある CSV ファイル（拡張子「.csv」のファイル）を使って、ウイルス感染を試みる攻撃を前四半期に続いて確認した。

この攻撃手口では、細工が施された CSV ファイルを開く[8]と、悪意のある命令の実行が試みられ、図 4 の Excel の警告ウインドウが表示される。このウインドウが表示された場合、**「無効にする」を選択**すれば、攻撃を回避する（悪意のある命令の実行を止め、ウイルス感染を避ける）ことができる[9]。

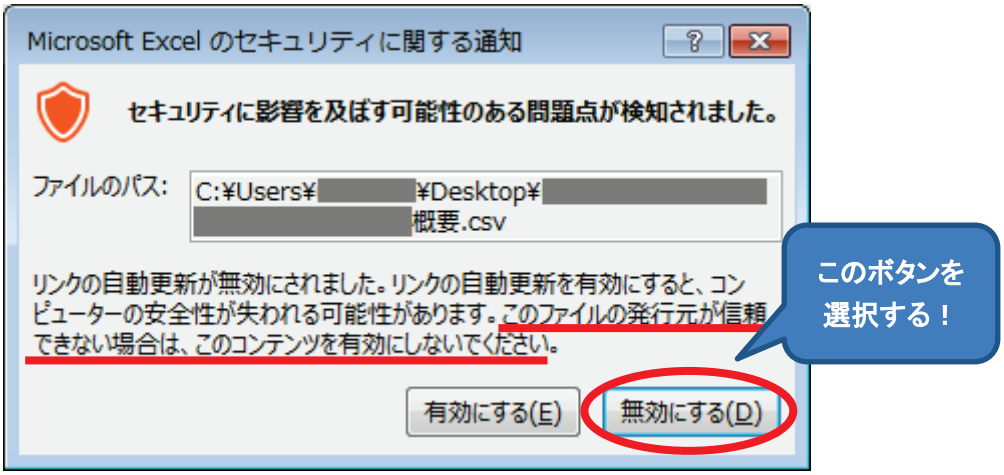

図 4 Excel で悪意のある CSV ファイルを開いた際に表示される警告ウインドウ

この CSV ファイルを悪用する攻撃手口は、脆弱性を悪用しているわけではないため、修正プログラムの適用で攻撃を防ぐことはできない。現時点では、利用者ひとりひとりが、この攻撃手口を認識し、CSV ファイルを開いたときに表示される警告ウインドウをよく確認し、正しい手順で操作する（**「無効にする」を選択する**）ことによって攻撃を回避する必要がある。

PowerPoint スライドショーファイルによる脆弱性の悪用

悪意のある PowerPoint スライドショーファイル（拡張子「.ppsx」のファイル）を格納した ZIP ファイルをメールに添付し、Microsoft PowerPoint（以下、PowerPoint）がインストールされた環境で開かせることで、脆弱性（CVE-2017-8759[10]）を悪用し、ウイルス感染を試みる攻撃を確認した（図 5）。脆弱性を解消していない環境で本ファイルを開いた場合、**悪意のある命令が自動的に実行（警告ウインドウ等は表示されない）**され、ウイルスに感染させられてしまう。

---

[8] Excel がインストールされた環境では、通常 CSV ファイルが Excel に関連付けされており、CSV ファイルをダブルクリックするなどして開いた場合、Excel が起動し、Excel 上でそのファイルが開かれる。

[9] 細工が施された CSV ファイルを「メモ帳」等のテキストエディタで開いた場合は、内容が表示されるだけで、Excel の機能を悪用した攻撃を受ける（ウイルスに感染させられる）ことはない。

[10] Microsoft .NET Framework の WSDL 処理に任意コード実行の脆弱性（JVN）
http://jvn.jp/vu/JVNVU93526380/index.html

PowerPoint スライドショーファイルは、PowerPoint のスライドショーを直接表示するファイル形式で、通常の PowerPoint ファイル（拡張子「.ppt」、「.pptx」）とは異なり、スライド編集画面が表示されない[11]ファイルである。攻撃者は、このファイル形式を使うことで、本来表示される警告ウインドウを一部回避しているものと思われる[12]。

なお、Microsoft Office の「保護ビュー」の機能が有効であると、この脆弱性の悪用が試みられることを防ぐことができる。脆弱性の解消とともに、メールに添付されている PowerPoint スライドショーファイルを開く場合、「保護ビュー」を有効な状態として開くことが望ましい。

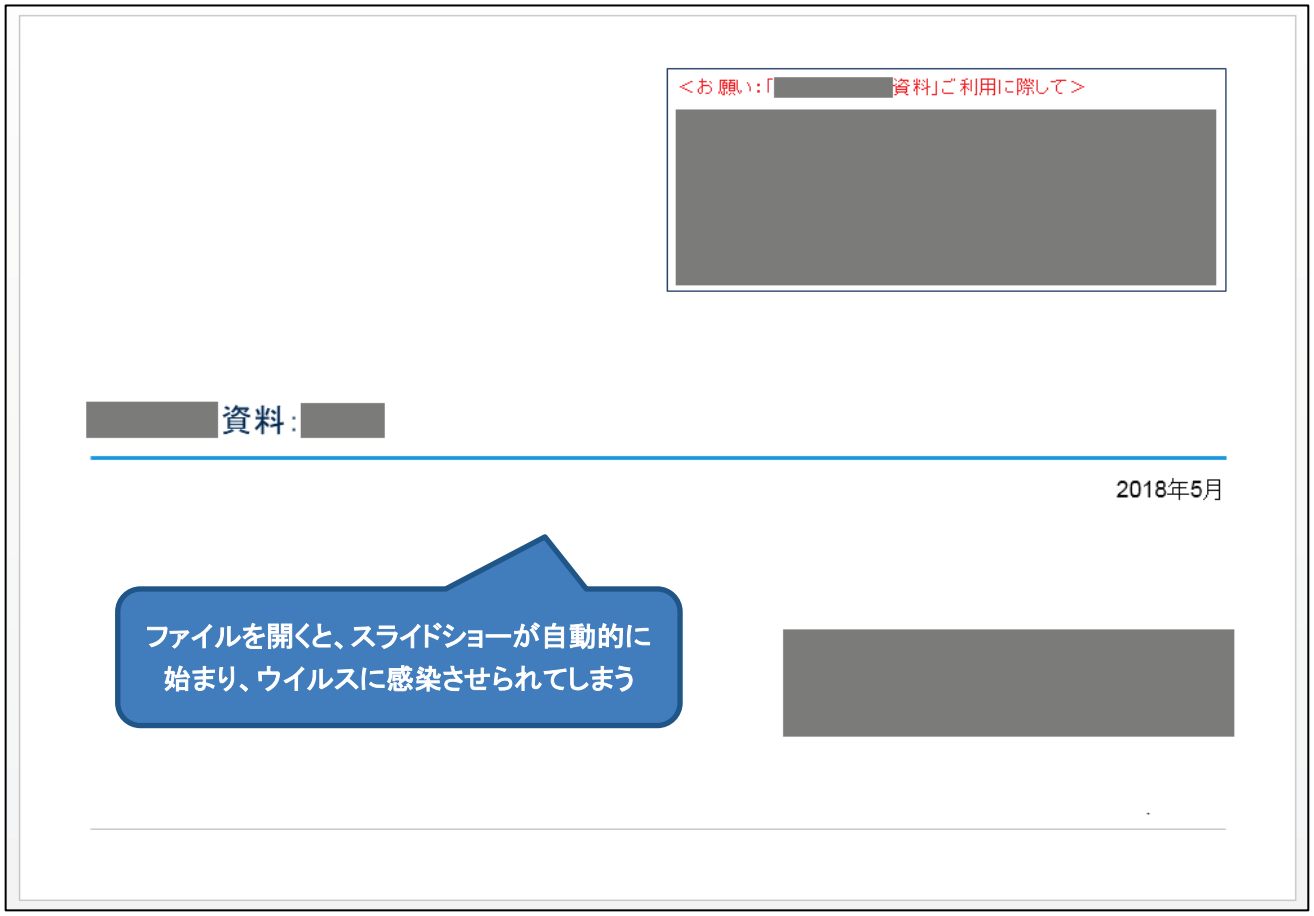

図 5 細工が施された PowerPoint スライドショーファイル

[11] PowerPoint を起動し、[ファイルを開く]から、PowerPoint スライドショーファイルを開くと、スライド編集画面が表示され、通常の PowerPoint ファイルと同じ操作が可能となる。

[12] PowerPoint ファイルの場合、ファイルを開くと警告ウインドウが表示される。

4 Office 365 のアカウント情報を狙うフィッシングメール

本四半期、Office 365 のアカウント情報を騙し取る目的のフィッシングメールを複数確認した。ここでは、特徴的な 2 つの手口を説明する。

Office 365 のアカウント情報は、攻撃者にとって魅力的な情報として狙われている可能性がある。すなわち、フィッシングによってアカウント情報を騙し取り、そこから組織内の情報（メールやクラウド上に保存したファイル等）の窃取や、奪ったメールアカウントを使った別の攻撃への悪用を企図している可能性がある。これは、深刻な標的型サイバー攻撃の準備段階（情報収集・組織内侵入の踏み台）として行われていることも考えられ、企業・組織にとって大きな被害をもたらしかねない、注意を要する脅威である。

一方で、Office 365 を導入している組織の利用者が、自身のアカウント情報の重要さや、そのアカウント情報を狙うフィッシング詐欺という攻撃が存在するということを十分に認識していないと、悪意のある者によってアカウント情報を騙し取られ、大きな被害に繋がる可能性がある。本紙で紹介する事例（攻撃手口）は一例に過ぎないが、このような攻撃があるということ、そして企業・組織内で使用している ID やパスワードを入力する際には注意が必要であることを改めて認識し、組織内でも周知していただきたい。

4.1 件名や本文に組織名が書かれたフィッシングメール

本四半期、J-CSIP の参加組織にて、宛先のメールアドレスのドメイン名の一部を組織名として抜き出して、件名や本文のところどころに使用し、本物のメールらしく細工しているフィッシングメールを複数確認した。内容は「メールの送信に失敗した」、「メールの送信が保留されている」という文面（英語）となっており、メールの本文中にある URL リンクを受信者にクリックさせることで、Office 365 のアカウント情報を詐取するためのフィッシングサイトへ誘導を試みるものであった。

具体例として、次の 2 件の事例を紹介する。それぞれのメールで、件名や本文中のマスクされた部分には、攻撃対象の組織のメールアドレスのドメイン名が使われている。

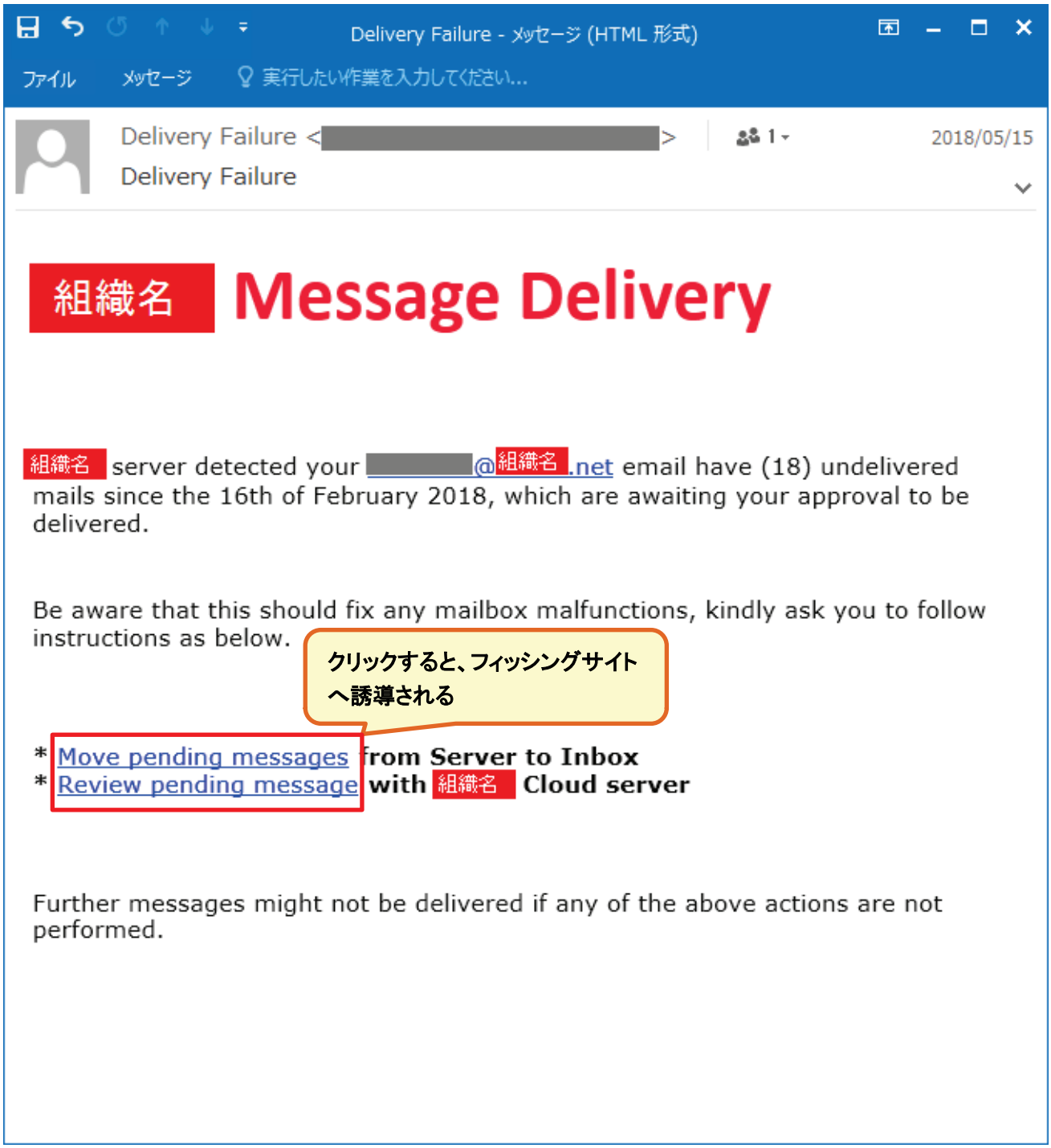

図 6 フィッシングメール事例 1

このメール（図 6）は、2018 年 2 月 16 日より 18 通のメールが未送信の状態であるため、メール本文中の URL リンク（「Move pending messages」と「Review pending message」）をクリックして対応するように促す内容が書かれている。2 つの URL リンクは、どちらも同じフィッシングサイトに誘導するものである。

図 7 フィッシングメール事例 2

このメール（図 7）は、2018 年 6 月 27 日時点で、配送保留中のメールがあり、これを解消するために、メール本文中の URL リンクを（「RELEASE TO MAILBOX」と「Review Messages」）クリックして対応するように促す内容が書かれている。2 つの URL リンクは、どちらも同じフィッシングサイトに誘導するものである。

4.2 攻撃対象組織に特化した添付ファイルとフィッシングサイト

ある組織の実在する役員を騙り、複数の従業員に対して、Office 365 のアカウントを狙うフィッシングメールが送られた事例があった。本件メールの添付ファイル（PDF ファイル）と、そのファイルから誘導される先のフィッシングサイトは、組織のロゴ画像を使うといったように攻撃対象の組織向けに特化して作成されていた。

本件のフィッシングメールには PDF ファイルが添付されており（図 8）、PDF ファイルを開くと、攻撃対象の組織名や組織のロゴ画像が記載されている。PDF ファイル中の「REVIEW」の部分が URL リンクになっており、クリックすることで、フィッシングサイトに誘導される。PDF に記載された内容は、オンライン上にある文書について、確認するように騙しており、文書の確認には認証が必要であると、思わせるように記載している。

図 8 メールに添付された PDF ファイル

PDF ファイルのリンク先のフィッシングサイト（図 9）でも、攻撃対象の組織名や組織のロゴ画像が使われている。

何らかの重要書類に見せかけた Word 文書ファイルのアイコンがあり、「File to Download」と表示されている。このアイコンをクリックすると、アカウント情報の入力を求められ、ID やパスワードを入力してしまうと、攻撃者に詐取されてしまう。

図 9 誘導されるフィッシングサイト

4.3 まとめ

Office 365 のアカウント情報を狙うフィッシング攻撃の事例を紹介した。フィッシングメールやフィッシングサイトに受信者の組織名（ドメイン名の一部）やロゴ画像が使われる等、注意すべき手口である。

また、クラウドサービスを普段から使用して文書ファイルのやりとり（保存や共有）を行っている利用者は、何らかの方法でフィッシングサイトへ誘導され、ログインのための認証情報の入力が求められても、さほど不自然と思わず入力してしまう可能性がある。攻撃者はこのような利用者の心理を利用して攻撃しているものと考えられる。

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。

具体的には、「ID やパスワードの入力が求められる画面は本物であるか、URL 等を確認する」や、「ウェブサイトを開く場合、メールに書かれたリンクからではなく、ブックマーク等信頼できる方法で開く」という対策が有効である。より詳しくは、フィッシング対策協議会 [13]のウェブサイト等も併せて参照していただきたい。

今後、悪意のある者が、「乗っ取ることで大きな権限を得られる」という理由で、より積極的に Office 365 等のアカウント情報を狙い、フィッシング攻撃を継続する可能性がある。Office 365 に限らず、クラウド型のサービスを利用している企業・組織においては、利用者がアカウント情報を騙し取られることが組織的なリスクに繋がる。従業員等に対し、アカウント情報の適切な取扱いを徹底することが重要である。

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

5 Drupal の脆弱性を悪用した攻撃

本四半期、Drupal の脆弱性（CVE-2018-7600[14]）を悪用した攻撃について、4 月から 5 月の間に 4 件の情報提供があった。本章では、それらの事例について説明する。この攻撃は、特定の組織を対象にしたものではなく、広く無差別に攻撃が行われたものと思われる。

この脆弱性は、Drupal を使用したウェブサイトに対して細工したリクエストを送信することで、ウェブサーバ上で任意のコードを実行することが可能となるものである。本件に限らず、インターネットからアクセス可能なサーバ上で稼働するソフトウェアは、脆弱性の公開から実際に攻撃が行われるまでの時間が短くなっている傾向があり、注意が必要である。

4 件の事例を時系列に並べたものを「表 4 Drupal への攻撃事例」に示す。

表 4 Drupal への攻撃事例

日付（日本時間）	内容
2018/3/29	Drupal の脆弱性（CVE-2018-7600）の修正プログラムが公開された。
2018/4/13	Drupal の脆弱性（CVE-2018-7600）を悪用する攻撃コードが公開された。
2018/4/17	<<A 社への攻撃>> Drupal の脆弱性（CVE-2018-7600）を悪用する攻撃を受け、A 社の公開ウェブサーバに対する改ざんがあった。暫定対応として、WAF（ウェブアプリケーションファイアウォール）[15]の適用による防御の提案と検討を行った。
2018/4/20	<<B 社への攻撃>> B 社の公開ウェブサーバに対する Drupal の脆弱性（CVE-2018-7600）の悪用を試みる通信を観測した。 B 社では Drupal を使用していなかったため、これによる影響はなかった。
2018/4/22	<<C 社への攻撃>> Drupal の脆弱性（CVE-2018-7600）を悪用され、C 社の公開ウェブサーバの一部のファイルが、悪意のあるファイルに置き換えられた。C 社はウェブサーバの挙動の異変に気づき、対応と復旧を行った。C 社が本件脆弱性の修正プログラムを検証サイトでテストしている最中[16]に発生した攻撃であった。
2018/4/29	<<D 社への攻撃>> Drupal の脆弱性（CVE-2018-7600）を悪用され、D 社の公開ウェブサーバに悪意のあるスクリプトファイルがダウンロードされ、コインマイナーを設置された。D 社はサーバの CPU 負荷が上昇していることに気付き、対応と復旧を行った。 D 社は、本件脆弱性の暫定対策として、クラウド型の WAF を適用した。5/2 以降に同様の攻撃が行われたが、WAF により防御できた。

[14] 更新：Drupal の脆弱性対策について(CVE-2018-7600) （IPA）
https://www.ipa.go.jp/security/ciadr/vul/20180329-drupal.html

[15] WAF：Web Application Firewall。ウェブサイト上のアプリケーションに特化したファイアウォール。

[16] C 社によると、検証サイトでテストを行うため最低でも 2～3 週間が必要とのことであった。

これら、J-CSIP で報告を受けた事例だけでも、CVE-2018-7600 を悪用する攻撃は最速で 4 月 17 日に確認されており、これは、脆弱性が公開されてから 19 日目、攻撃コードが公開されてから 4 日目にあたる。

脆弱性の修正プログラム公開から、攻撃に使われるコードの公開、また攻撃が行われるまでの期間は短くなっている傾向にあるが、企業や組織としては修正プログラムの検証や、本番環境への修正プログラムの適用準備等、ある程度の時間を要することが考えられる。本事例では、WAF の適用による暫定対策を行った組織があり、それにより防御したという報告もあった。WAF は万能な防御ツールではないが、今回のような状況で、一定の効果が得られる可能性がある。

6　プラント関連事業者を狙う一連の攻撃（続報）

前四半期に続き、本四半期でも、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。

偽のメールの内容は巧妙で、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、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。

6.1 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 2018 年 6 月まで確認している限り、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、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。

6.2 攻撃の例と特徴

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。前四半期までの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への感染を狙うものであった。

本四半期、この傾向が変化し、最も多い攻撃手口が、メールに Microsoft Office の脆弱性（CVE-2017-11882）[17]を悪用する Word 文書ファイルを添付するものであった。また、6 月には「悪意のある Word 文書ファイルを埋め込んだ PDF ファイル」がメールに添付された手口も観測している。

なお、この攻撃者による、提案や見積もり等を依頼する偽のメールでは、その締め切り日として、メールの送信日から 1 週間から 10 日後の日付を提示してくることが多く、添付ファイルを急いで確認させようとする意図があると思われる。

---

[17] Microsoft Office 数式エディタにスタックベースのバッファオーバーフローの脆弱性（JVN）
https://jvn.jp/vu/JVNVU90967793/

「悪意のある Word 文書ファイルを埋め込んだ PDF ファイル」（図 10）の事例を次に示す。

この PDF ファイルを開くと、警告ウインドウ（図 11）が表示される。「このタイプのファイルを開くことを許可しない」のラジオボタンを選択する[18]ことでウイルスへの感染を回避することができる。そうでない場合、Word 文書ファイルが開き、脆弱性の悪用が試みられてしまう。

攻撃者がこのように PDF ファイルと Word 文書ファイルを組み合わせた形態で攻撃を行った理由は不明だが、セキュリティソフトによる検知の回避や、攻撃を繰り返す中で様々な手口を試行しているものと推測している。

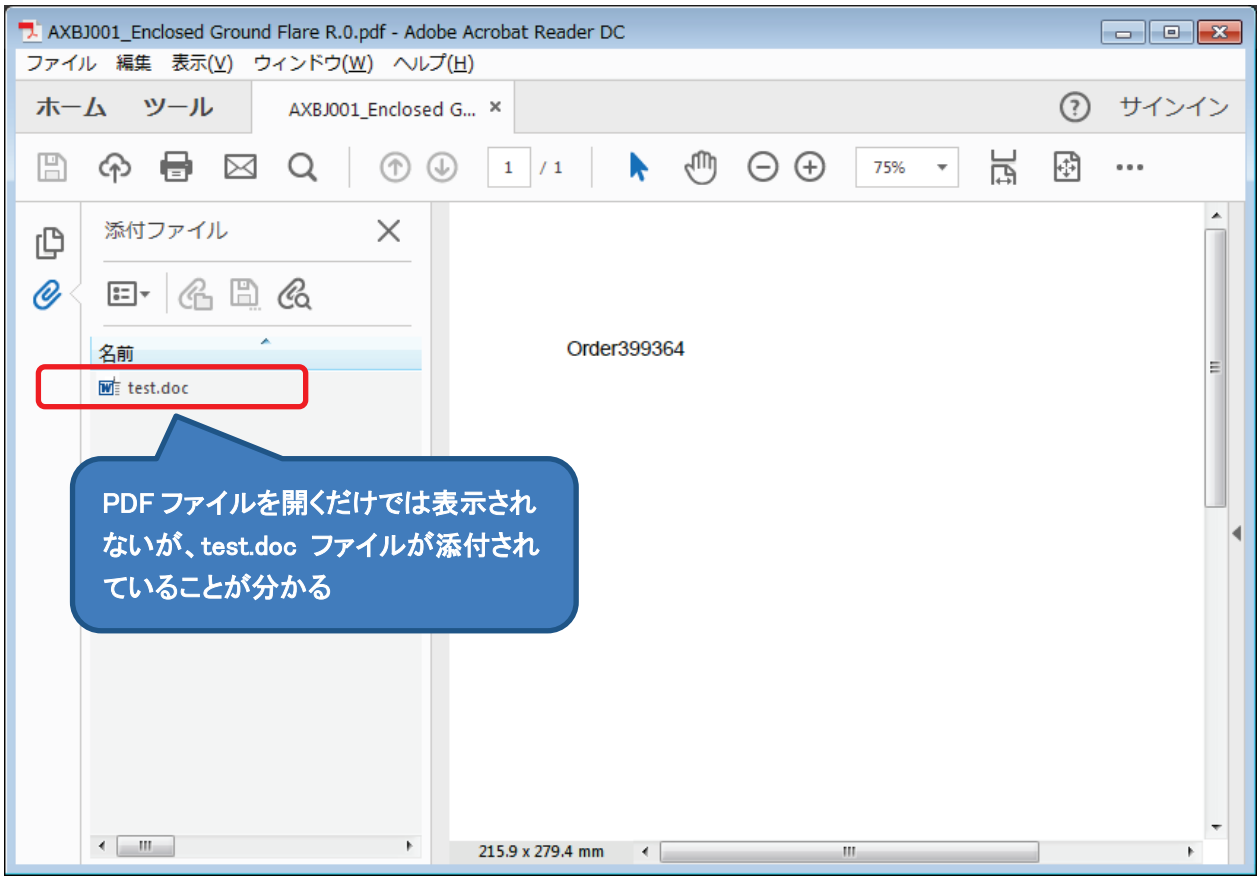

図 10 悪意のある Word 文書ファイルを埋め込んだ PDF ファイル

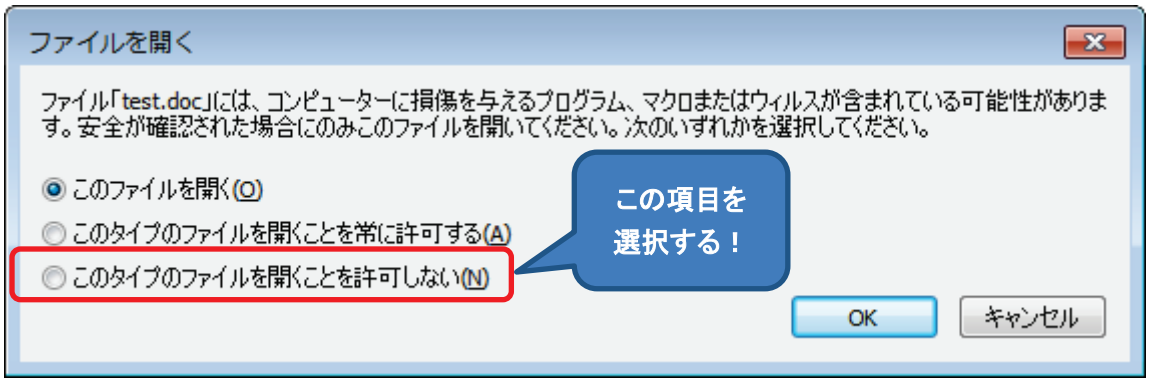

図 11 PDF ファイルを開くと表示される警告ウインドウ

[18] 本警告ウインドウは、表示されたタイミングでは「このファイルを開く」が選択されている。

6.3 まとめ

プラント関連事業者を狙う一連の攻撃について、実際の攻撃メールの事例とともに、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させる手口、Office の脆弱性を悪用する手口がみられる。

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。

7　ビジネスメール詐欺（BEC） 国内組織を騙る攻撃を確認

2018 年 5 月と 6 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。ビジネスメール詐欺については、2017 年 4 月の注意喚起以降も J-CSIP の参加組織で継続して確認しており、依然として注意が必要な状況である。

今回確認した 2 件のビジネスメール詐欺の事例と手口について、それぞれ説明する。なお、2 件の事例とも、メールはすべて英文であった。

7.1 事例 1

この事例では、参加組織の国内関連企業（A 社）と、その海外の取引先企業（B 社）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、偽の振り込みを要求するメールが B 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。

本事例においては、支払側である B 社の担当者が偽のメールであると気づくことができたため、金銭的な被害は発生していない。

偽のメールには、振込先銀行口座の変更通知書と、支払請求書の 2 つの PDF ファイルが添付されていたが、どちらの PDF ファイルの内容も正規のものであった。これでは詐欺として成立せず、こうなった理由は不明である（攻撃者が何らかのミスをしたか、別の目的があった可能性がある）。

本事例では、詐欺の過程において、次の手口が使われた。

- 詐称用ドメインの取得と悪用
- ビジネスメールの授受に割り込み、詐欺を試みる

（1） 詐称用ドメインの取得と悪用

攻撃者は、A 社のドメインに似通った「詐称用ドメイン」を、なりすましメールを送信する“前日”に取得していた。不正な目的で自組織の類似ドメインが新たに取得されていないかを定期的にチェックしている企業があるが、そのような対策を回避しようとしているものと考えられる。あるいは、詐欺がうまく進みそうな場合に、状況に応じてドメインを適宜取得するという、柔軟かつ素早い行動をとっている可能性もある。

また、本件の詐称用ドメインを取得した者は、A 社を詐称するためのドメイン以外にも、実在すると思われる企業のドメインに近い、偽のドメインを多数取得していることを確認している（ドメイン取得時のメールアドレスが同一である）。この者は、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。

なお、詐称用ドメインは、次の例に示すように、正規ドメインの 1 文字違いを使用（悪用）したものであった。

【本物のメールアドレスのドメイン名】 alice @ a-company . com
【偽物のメールアドレスのドメイン名】 alice @ a-company**s** . com　⇒ 「s」が一文字多い

※実際に悪用されたものとは異なる。

（2）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（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 A 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。

B 社の担当者は、攻撃者から送られてきた偽のメールに対して、送信元のメールアドレスのドメイン名が、A 社のドメインとは異なっていることに気づき、A 社の担当者に直接確認を行うことで、偽のメールであると見破ることができたため、被害には至らなかった。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る。

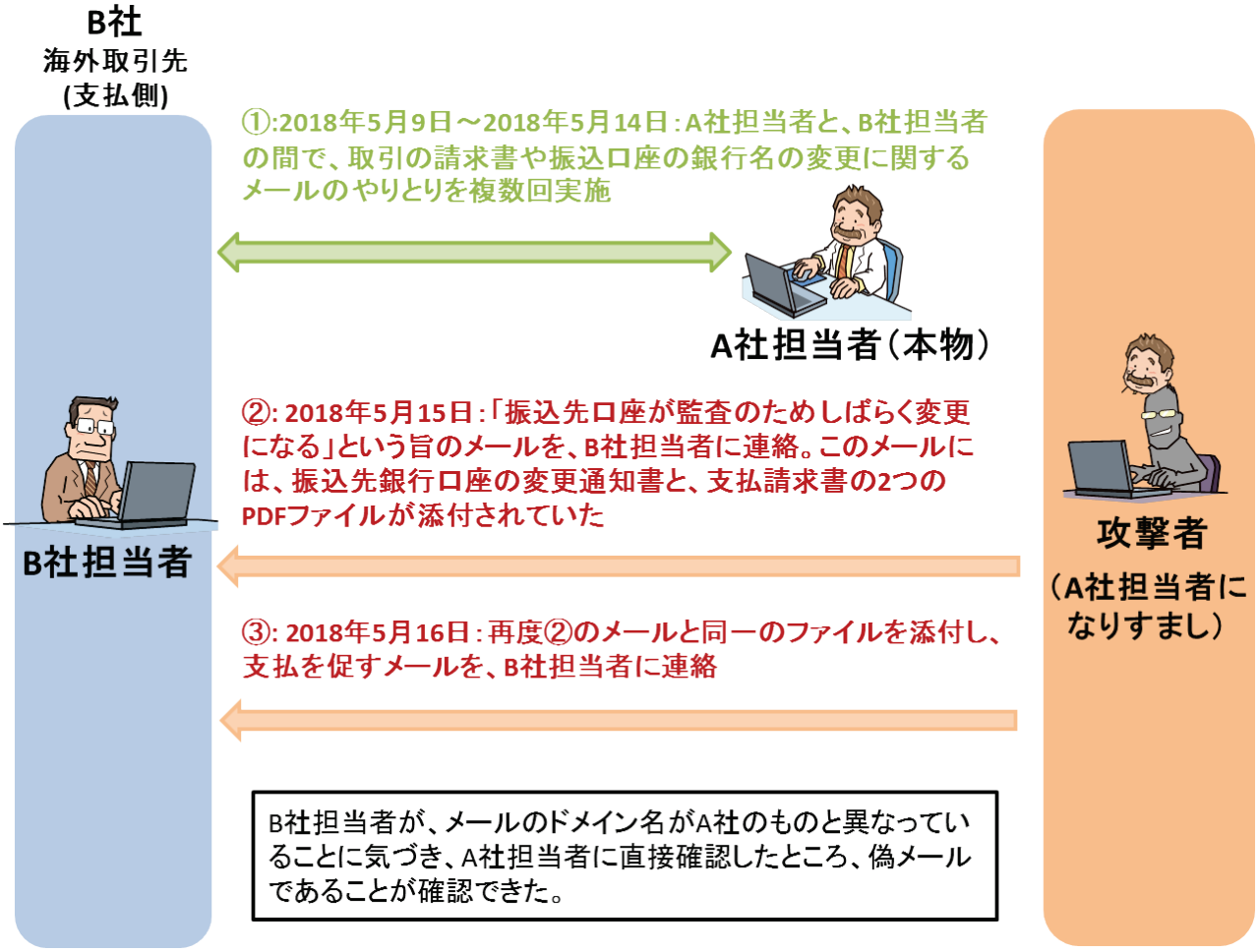

図 12 攻撃者とのやりとり

なお、今回の事例では、A 社は攻撃者によって詐称されたメールに含まれていた（同報として記載されていたメールアドレス）社員全員に対して、メールアカウントのパスワードの変更を実施し、注意を促した。

7.2 事例 2

この事例では、国内企業（C 社）と、その海外関連企業（D 社）で取引を行っている中で、攻撃者が C 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 D 社に送られたものである。このとき、C 社は請求側、D 社は支払側であった。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。

本事例において、攻撃者から D 社に送られた偽のメールには、次の内容が英文で記載されていた。

- 銀行口座の入金処理に問題が発生したため、入金が取り消されるか、遅延する恐れがある
- 問題が解決されるまで、本日以降の支払いについては振込先を変更してほしい
- 変更先の銀行口座情報 （※海外の銀行口座で、C 社とは無関係な名義となっていた）

事例 1 と同様に、攻撃者は、C 社のドメインに似通った「詐称用ドメイン」を、なりすましメールを送信する“前日”に取得していた。また、本件の詐称用ドメインを取得した者（事例 1 とは異なる）も、偽のドメインを多数取得していることを確認している。

なりすましメールの同報先（CC：）には、C 社の従業員のメールアドレスが複数設定されていたが、このメールアドレスのドメインも、詐称用ドメインに差し替えられていた。メールの同報先に「偽のメールアドレス」を設定することで、受信者に本件のメールが偽物だと気付かせにくくすることを狙ったものと考えられる。

なお、詐称用ドメインは、次の例に示すように、正規ドメインの 1 文字の位置を入れ替えたものであった。

【本物のメールアドレスのドメイン名】 alice @ a-company . com
【偽物のメールアドレスのドメイン名】 alice @ a-co**n**pa**m**y . com ⇒ 「m」と「n」が逆になっている

※実際に悪用されたものとは異なる。

7.3 まとめ

ビジネスメール詐欺のこの他の事例と対策については、2017 年 4 月の注意喚起のレポートで詳細に述べている。ビジネスメール詐欺は、特に海外と取引のある国内企業にとって、重大な脅威であり、2017 年 4 月の注意喚起レポート公開以降も継続して J-CSIP 内で情報提供を受けている。

被害に遭わないようにするため、ビジネス関係者全体で、その脅威を認識し、手口を理解するとともに、なりすましメールや不審なメール等への注意力を高めておくこと、社内ルール等による被害を防ぐ体制作りが重要である。社内だけでなく、取引先等に対しても、ビジネスメール詐欺への注意を促すことも検討していただきたい。

8　IQY ファイルを悪用した攻撃の手口

2018 年 6 月、脆弱性の悪用やマクロ機能の悪用とは異なる、Microsoft Excel の IQY（Internet Query）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だが、本攻撃手口では「保護ビュー」を有効にしている状態でもウイルスに感染させられてしまうことを確認している。

脆弱性の悪用に対しては修正プログラムの適用で、また、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、それとは異なる対策が必要であり、利用者ひとりひとりに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、国内での攻撃に使われるようになる可能性があるため、攻撃手口と注意点（表示される警告メッセージと、その場合に選択すべきボタン等）をまとめた一般利用者向けの参考資料を、本紙と併せて公開した[19]。

IPA で確認できている範囲では、海外で無差別にばらまかれたウイルスメールの添付ファイルで悪用された手口ではあるが、日本国内のドメイン宛にも同様のウイルスメールが送信された痕跡を確認している。攻撃の特徴、表示される警告ウインドウ、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。

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

[19] 【参考情報】IQY ファイルを悪用する攻撃手口に関する注意点