サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2018 年 1 月～3 月]

2018 年 4 月 25 日
IPA（独立行政法人情報処理推進機構）
技術本部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 3 月末時点の運用体制、2018 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 章では 2012 年度から 2017 年度までの年度毎推移状況と 2017 年度の動向等を、4 章以降は本四半期で把握、分析した特徴的な攻撃事例や、通年での動向等を併せて解説する。

目次

1 運用体制 2
2 実施件数（2018 年 1 月～3 月） 3
3 年度毎推移状況 5
4 国内組織を狙う標的型攻撃 7
5 プラント関連事業者を狙う一連の攻撃 （続報） 10
5.1 攻撃の観測状況 10
5.2 攻撃メールの例と特徴 10
5.3 まとめ 13
6 ビジネスメール詐欺（BEC） 国内組織への攻撃を引き続き確認 14
6.1 海外のカンファレンス事務局担当者を詐称する攻撃 14
6.2 海外関連企業の CEO を詐称する攻撃 17
6.3 まとめ 19
7 SLK ファイルを悪用した攻撃の手口 20

[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 1 月～3 月期（以下、本四半期）は、次の通り参加組織の増加があり、全体では 2017 年 12 月末の 11 業界 227 組織の体制から、11 業界 228 組織 [2]の体制となった（図 1）。

- 2018 年 3 月、航空業界 SIG に新たな参加組織があり、6 組織から 7 組織となった。

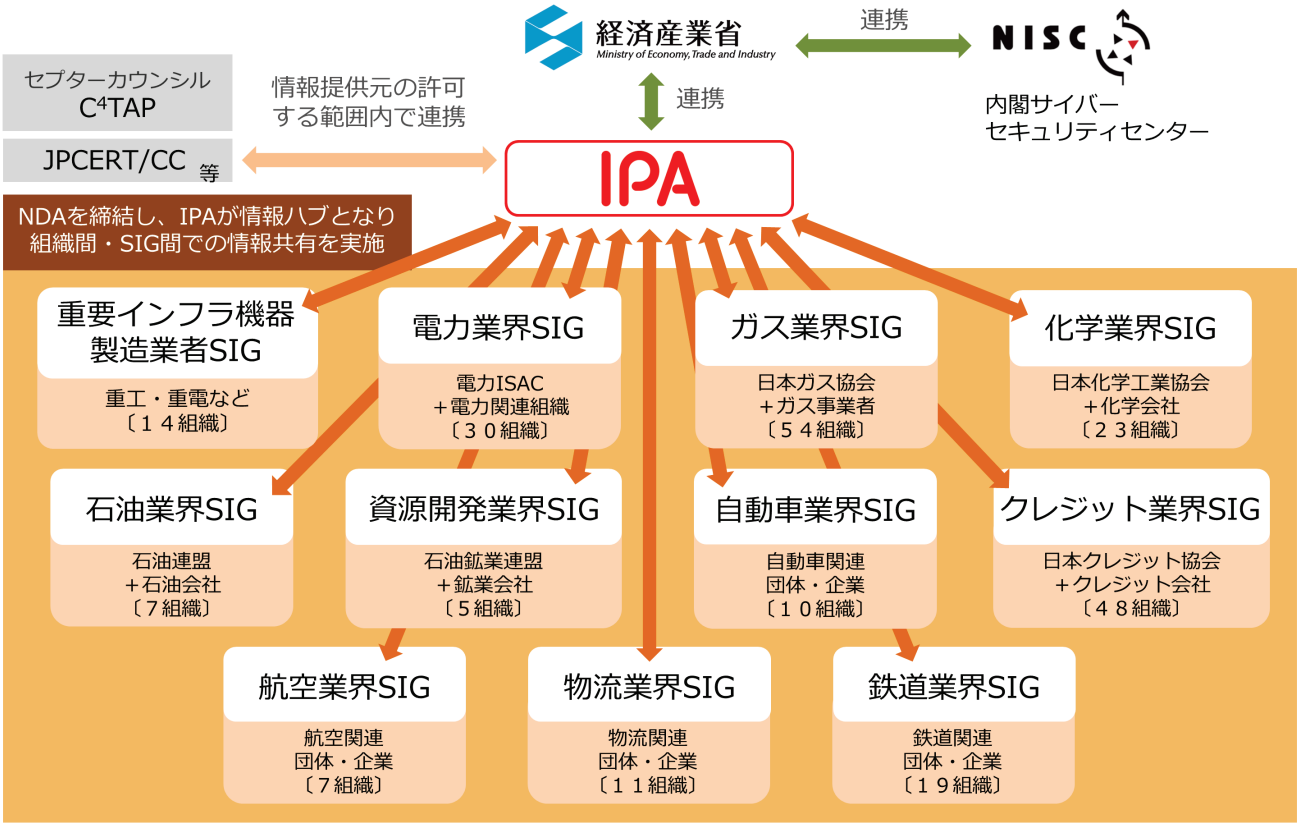

図 1 J-CSIP の体制図

[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（2018 年 1 月～3 月）

2018 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、11 の SIG、全 228 参加組織での合算）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
		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	1,213 件	57 件	1,930 件	**256 件**
2	参加組織への情報共有実施件数※1	26 件	17 件	123 件	**76 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 **17 件**を含む。

本四半期は情報提供件数が **256 件**であり、うち標的型攻撃メールとみなした情報は **101 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大部分を占めている。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）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、5 章で改めて述べる。なお、本四半期に標的型攻撃メールとみなした 101 件のうち、80 件が本件に該当する。

さらに、本四半期でもビジネスメール詐欺（BEC）が試みられたという事例も引き続き観測した。ビジネスメール詐欺（BEC）の事例については 6 章で改めて述べるが、2017 年 12 月に国内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おり、今後も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 で入手して、その手口を分析している。これについては、4 章で改めて述べる。

---

[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

また、本四半期、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	組織内の実在する人物を騙るフィッシングメールが取引先に送られた。	1 件
2	実在する外部組織の従業員を騙るフィッシングメールが送られてきた。	1 件
3	企業の公開ウェブサイトにある問い合わせフォームに対して大量の投稿を行う攻撃を受けた。	2 件
4	自組織を騙る偽サイトを発見した。	2 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 3 の「企業の公開ウェブサイトにある問い合わせフォームに対する大量の投稿を行う」攻撃は、前四半期から継続して相談・報告を受けている。これについては、同一 IP アドレスからの投稿回数に制限を設けるといった対策が必要である。

項番 1 と 2 のフィッシングメールは、クレジットカード番号等を狙う単純な金銭目的のものではなく、Office 365 等のアカウント情報を狙った攻撃であった。組織内の機密情報の窃取等に悪用できる情報として継続して狙われている可能性があり、注意が必要である。

項番 1 や 4 のような、自組織が詐称される事態は、いつ発生するか分からない。迅速に対応できるよう、対応方針（自組織のウェブサイトで注意喚起を公開する等）や対応手順を定めておくべきである。

3　年度毎推移状況

J-CSIP を運用開始した 2012 年度から 2017 年度までの、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）と参加組織数の推移を次に示す（表 3、図 2）。2017 年度は、参加業界数と参加組織数が大幅に増加した。

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
IPA への情報提供件数	246 件	385 件	626 件	1,092 件	2,505 件	3,456 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
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
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

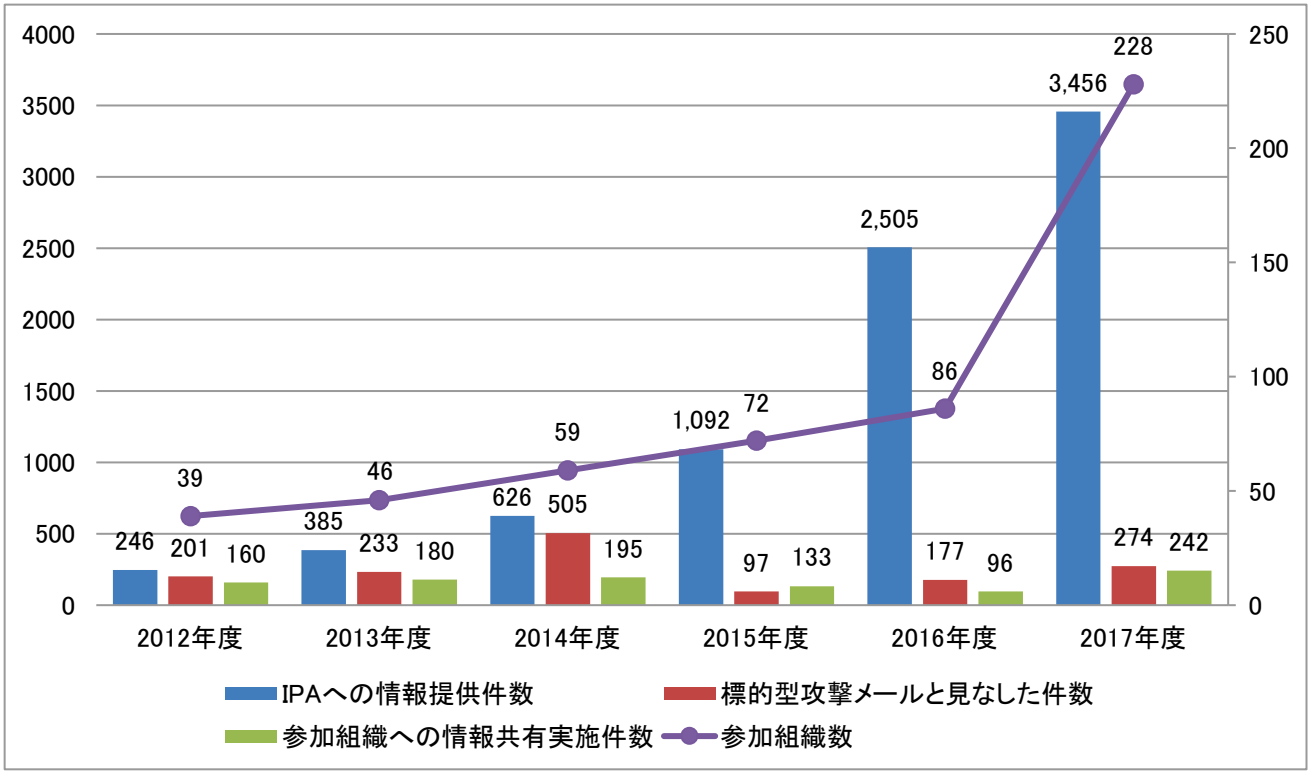

図 2 年間の取り扱い件数と参加組織数 グラフ

情報提供・情報共有の状況

2017 年度は、J-CSIP 運用開始以来、最も多くの情報提供件数となった。最大の要因は、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 2017 年度も多く発生し、それらが提供されたことである。この 1 年間、日本語のばらまき型メールでは、インターネットバンキングの情報を窃取する「DreamBot（ドリームボット）」[5]と呼ばれるウイルスやその亜種に感染させる目的のものが非常に多かった。また、文面等の攻撃手口の巧妙化も進んだ。これら事例や手口については、2017 年 10 月～12 月の運用状況レポート[6]に詳細を記載している。

もうひとつの要因は、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である。一連の攻撃メールの内容は常に変化を続けており、継続して多数の情報提供を受けている。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 5 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、IPA で入手した攻撃情報を共有したところ、同じ攻撃の痕跡（例えば同等の標的型攻撃メールの着信）が確認された事例がある。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り、引き続き注意が必要である。

特筆事項

2017 年 4 月 3 日、これまでの 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」[7]を公開した。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。レポートを公開した 2017 年 4 月以降も、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、2016 年度までに情報提供を受けた 4 件の事案に加え、2017 年度は 6 件の情報提供があり、合計 10 件を把握している。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、2017 年 5 月に世界中で感染が拡大したランサムウェアである「Wanna Cryptor」[8]の被害についても情報提供があった。また、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目立った。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。

---

[5] 国内ネットバンキングを狙う新たな脅威「DreamBot」を解析 （トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/14588

[6] サイバー情報共有イニシアティブ（J-CSIP）運用状況[2017 年 10 月～12 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 （IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

[8] Wanna Cryptor: WannaCrypt, WannaCry, WannaCryptor, Wcry 等とも呼ばれる。
（参考）世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について （IPA）
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

4 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ファイルを複数確認した（表 4）。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無いものもあるが、ウイルスに感染させるための細工が施され、悪意のあるファイルであることは確かである。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 4 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	2018 年度（平成 30 年度）●●について.doc	マクロが含まれる Word 文書ファイル
2	平成 30 年度●●計画書.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	●●アウトルック.doc	マクロが含まれる Word 文書ファイル
4	●●意見書の比較.doc	マクロが含まれる Word 文書ファイル
5	●●.csv	細工が施された CSV 形式ファイル

※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 4 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。

- ダウンロード先にクラウドストレージを悪用 （項番 2）
- マクロの有効化操作の誘導 （項番 1, 3, 4）
- CSV ファイルの悪用 （項番 5）

ダウンロード先にクラウドストレージを悪用

悪意のあるファイルをメールに添付するのではなく、メール本文中に、ダウンロード先の URL を記載し、着信者に URL をクリックさせてファイルをダウンロードさせるという手口で、クラウドストレージが悪用された。

これまでは、攻撃者が用意したと思われるサーバにウイルスが設置されている事例が多くみられたが、この手口では、広く一般に利用されているクラウドストレージの URL が記載されているだけであり、不審と判断しにくい可能性がある。

本事例では、メール本文中の URL リンク先のクラウドストレージに、ZIP 形式のファイルが設置されており、この ZIP 形式のファイル内には 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（項番 2）が格納されていた。このファイルをダウンロードして開くと、ウイルスに感染させられてしまう。

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 3、図 4）。

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。

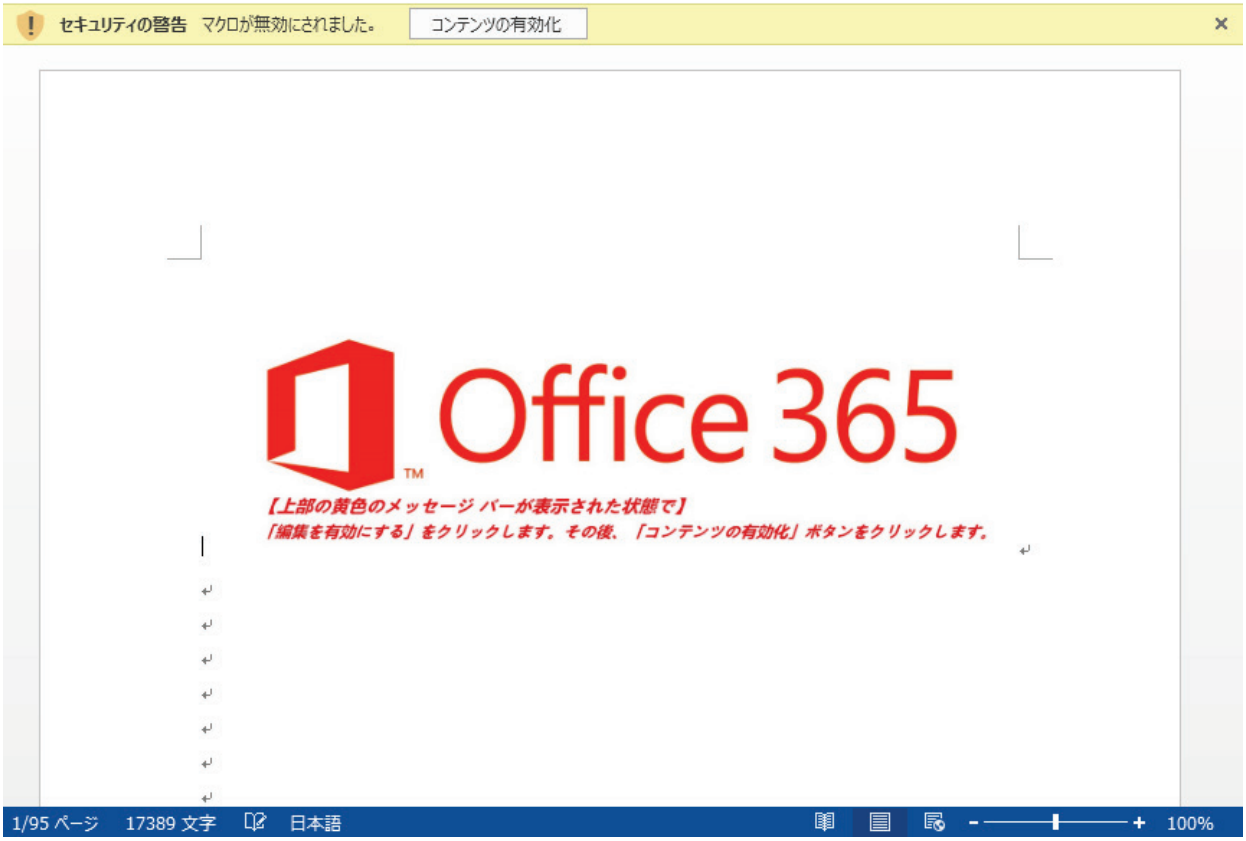

図 3 マクロの有効化操作の誘導（例 1）

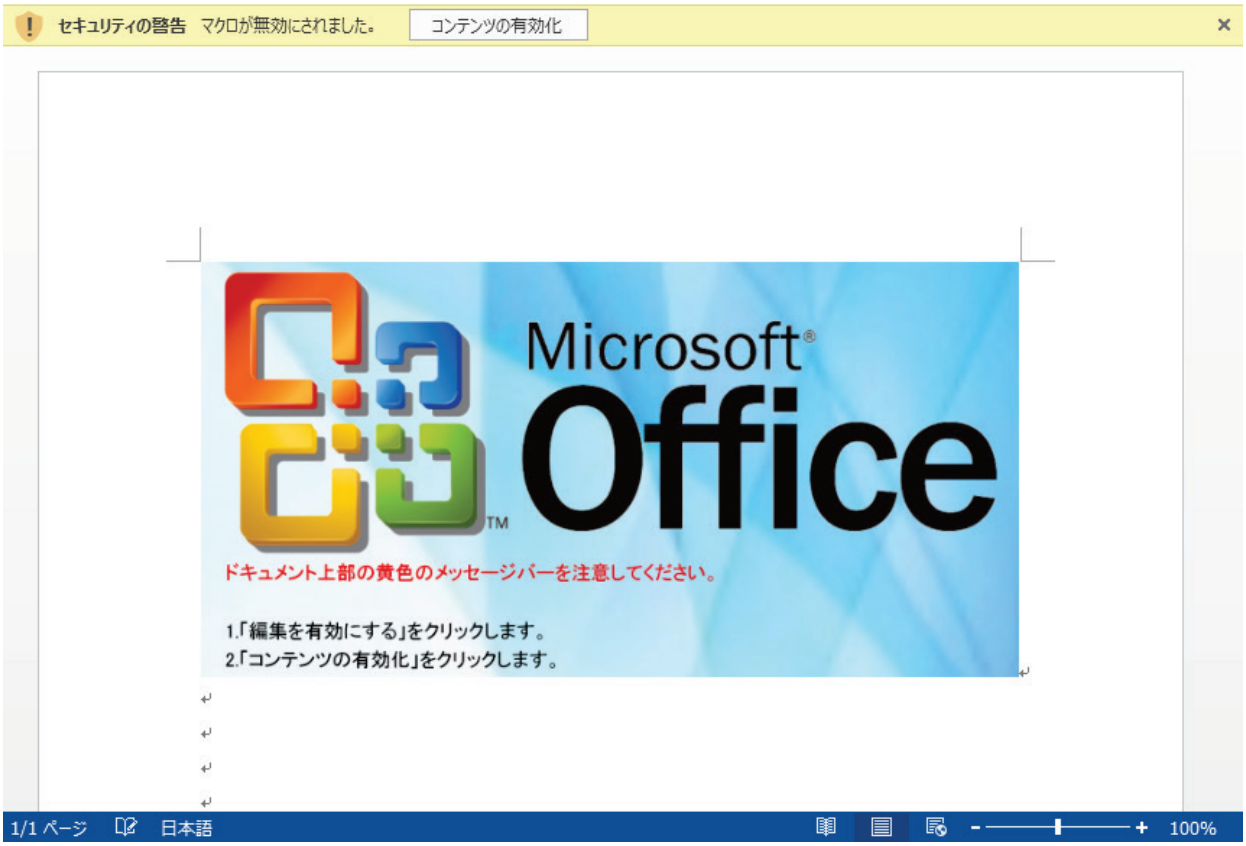

図 4 マクロの有効化操作の誘導（例 2）

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）をメールに添付し、Microsoft Excel（以下、Excel）がインストールされた環境で開かせることで、悪意のある命令が実行され、ウイルス感染を試みる攻撃を確認した。

CSV ファイルは、Comma Separated Value の略で、表などに使用する数値や文字列をカンマ記号で区切って記録した、テキスト形式のファイルである。一般的には、テキスト形式のファイルによって、ウイルスに感染させられてしまうようなことはないが、Excel がインストールされている環境では、CSV ファイルは Excel に「関連付け」されており、ダブルクリックするなどして開いた場合、Excel が起動し、その CSV ファイルが開かれる。

この攻撃手口では、細工が施された CSV ファイルを開く[9]と、悪意のある命令の実行が試みられ、図 5 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[10]。

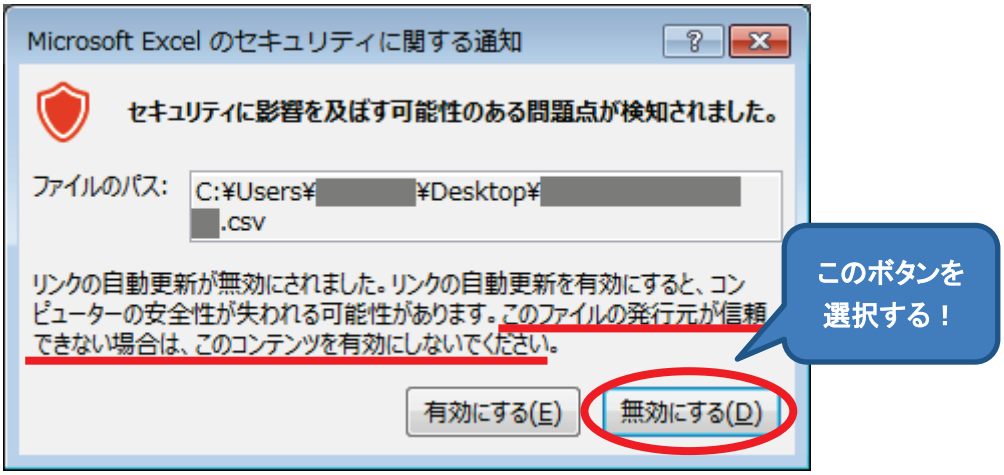

図 5 Excel で悪意のある CSV ファイルを開いた際に表示される警告ウインドウ

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。

---

[9] 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。

[10] 細工が施された CSV ファイルを「メモ帳」等で開いた場合は、内容が表示されるだけで、攻撃を受ける（ウイルスに感染させられる）ことはない。

5　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）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。

5.1 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 3 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。

また、この攻撃者は、2017 年 12 月から 2018 年 1 月の期間、Office 365 を含むメールアカウント情報の詐取を狙うフィッシング攻撃も併用していた。

現時点でも攻撃は継続している。

5.2 攻撃メールの例と特徴

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。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。

1 月には、メール本文に URL が記載され、フィッシングによりメールアカウント情報の詐取を狙う攻撃があった。3 月には、メールの添付ファイルに Microsoft Office の脆弱性（CVE-2017-11882）[11]を悪用する Word 文書ファイルを添付する攻撃もあった。

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 日後程度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。

---

[11] 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/

今回、事例としてメール本文中に URL があるフィッシングメール（図 6）と、そのフィッシングサイト（図 7、図 8）を次に示す。

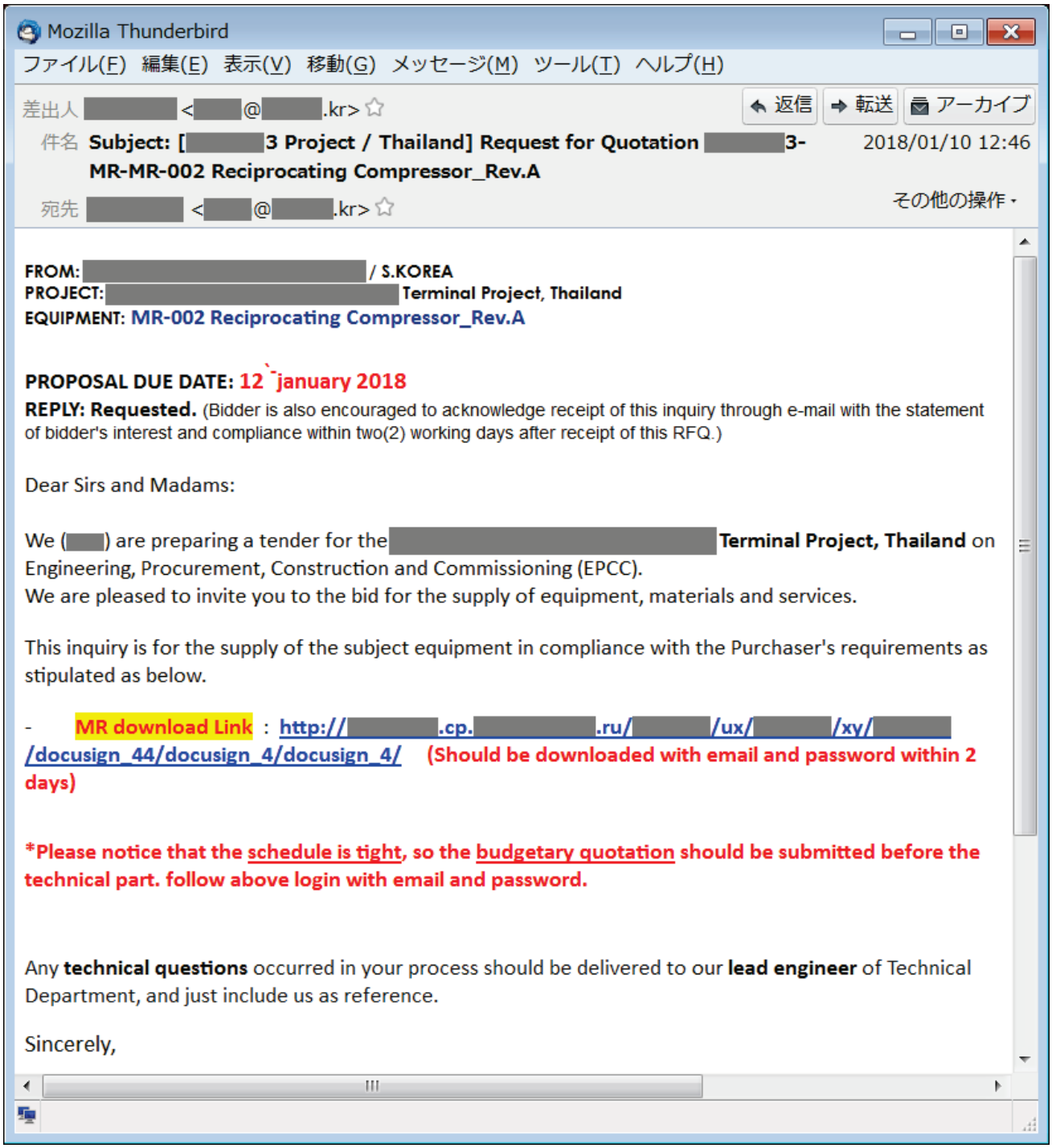

図 6 韓国のプラントエンジニアリングを提供する企業を騙る攻撃メール

このメールでは、韓国のプラントエンジニアリングを提供する企業を騙り、タイの建設プロジェクトに必要な資機材の見積もり依頼を装っている。

本文中の URL をクリックすると、次のフィッシングサイトが開く（図 7）。

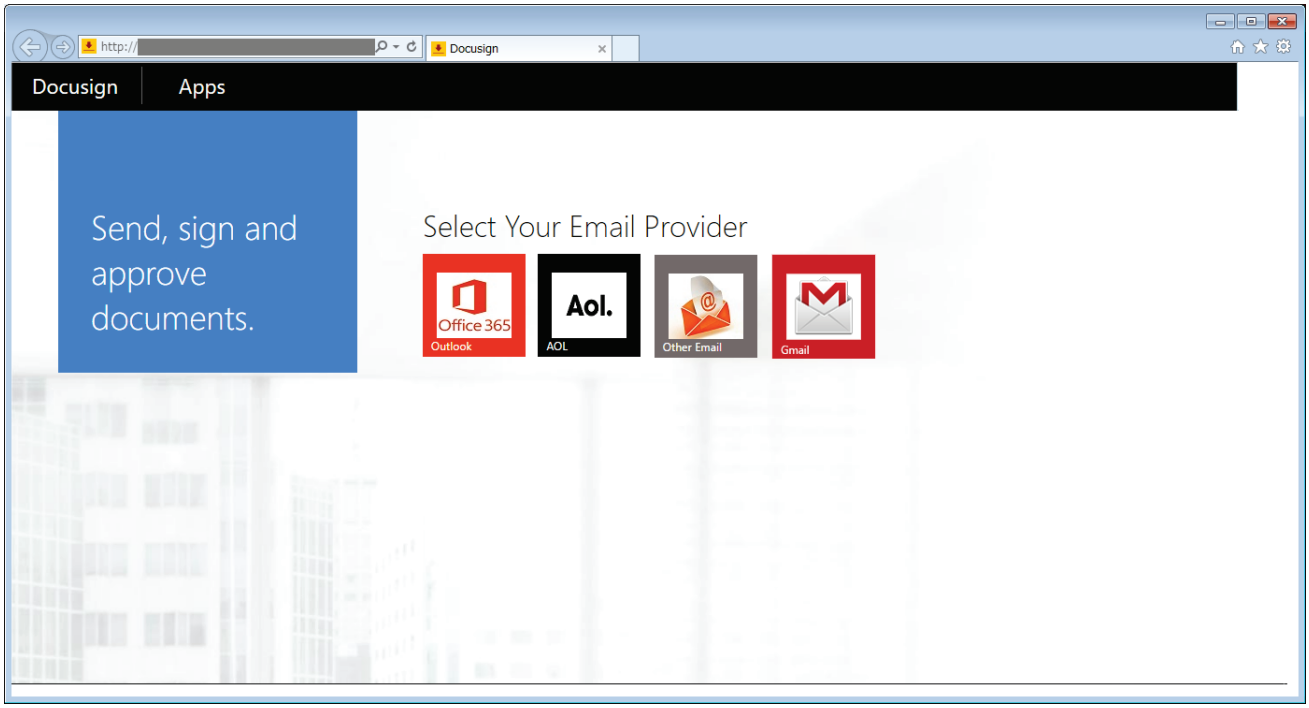

図 7 フィッシングサイト

このフィッシングサイトでは、何らかの文書ファイルを読むために認証が必要だと見せかけている。Office 365、AOL、Gmail、その他の 4 つのメールプロバイダの認証が選択できるようになっており、いずれかを選択すると、そのメールプロバイダのログイン画面を装った偽の画面が表示される。例えば Office 365 を選択した場合、図 8 の画面が表示されるが、これは偽の画面である。

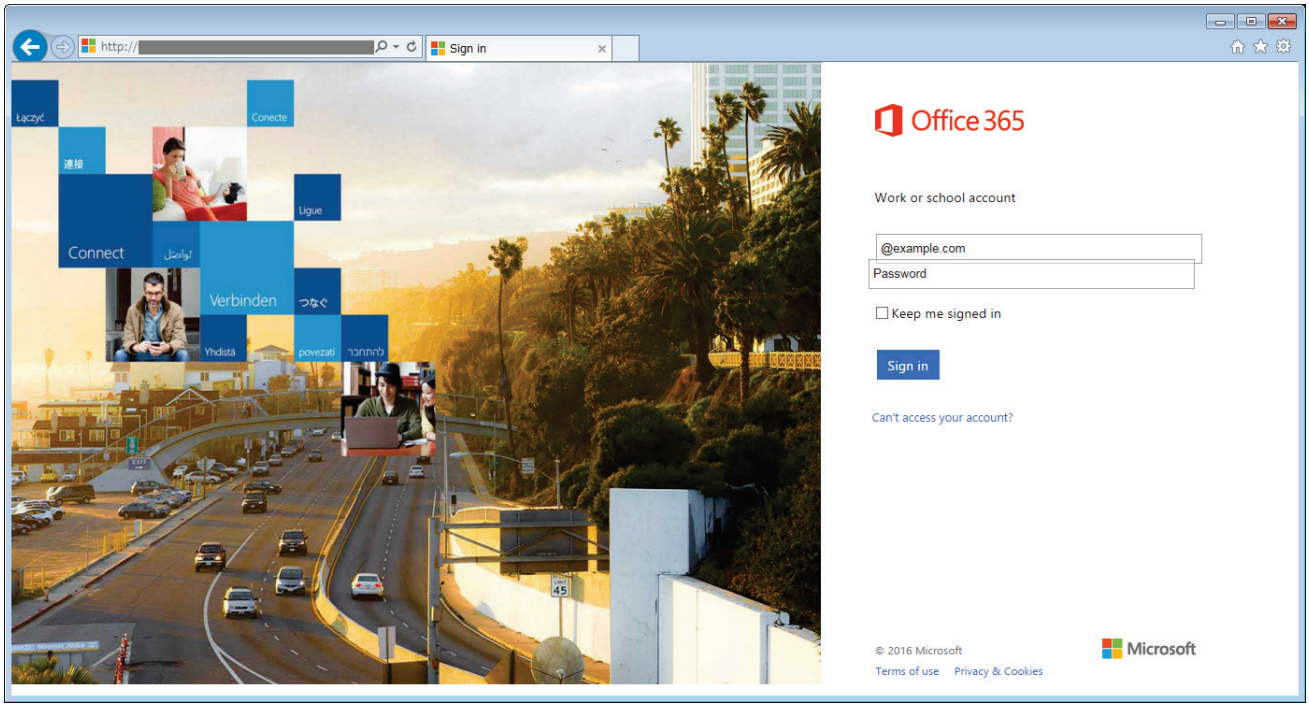

図 8 Office 365 のフィッシング画面

5.3 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ほか、フィッシングサイトへ誘導させる手口、また、比較的新しい（公開から数か月の）脆弱性を悪用する手口等の変化がみられた。

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予定である。

6　ビジネスメール詐欺（BEC） 国内組織への攻撃を引き続き確認

2018 年 2 月と 3 月、J-CSIP の参加組織に対してビジネスメール詐欺（BEC）が試みられた事実を把握した。また、初めて観測した騙しの手口として、**「決済手段の変更」**があった。ビジネスメール詐欺については、2017 年 12 月に国内での大規模な被害事例が報道されたところであり、今後もますます注意が必要な状況となっている。

今回確認された 2 件のビジネスメール詐欺の手口について、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のメールであった。

6.1 海外のカンファレンス事務局担当者を詐称する攻撃

本件で確認された事例では、国内組織（A 社）が海外のカンファレンスのブース出展に関するメールをやりとりしている中で、攻撃者が海外のカンファレンス事務局の担当者（B 氏）になりすまし、偽の口座情報を連絡して送金させようとするものであった。これは、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。

本事例において、支払側である国内組織の担当者は攻撃者の指示した偽の口座への送金を行ってしまったため、金銭的な被害が生じている。

本事例では、詐欺の過程において、次の手口が使われた。

- 正規のメールアドレスに似せた、フリーメールアドレスを詐称に使用する
- 決済手段の変更を装い、偽の振込先に誘導する
- ビジネスメールの授受に割り込み、詐欺を試みる

（1） 正規のメールアドレスに似せた、フリーメールアドレスを詐称に使用する

攻撃者は、B 氏の正規のメールアドレスと同一のローカル部[12]のフリーメールアドレスを取得し、偽のメールを送信してきた。ビジネスメール詐欺では、偽のメールを送るため、本物に似せた詐称用ドメインを取得する手口があるが、本事例ではそのような手口は使われてはいない。

【本物のメールアドレスのドメイン名】 alice . brown @ company-b . com
【偽物のメールアドレスのドメイン名】 alice . brown @ **freemail . com** ⇒ フリーメールドメイン

※実際に悪用されたものとは異なる。

なお、本事例では、偶然ではあるが、攻撃者から偽のメールが送られてくる約 1 か月前に、本物の B 氏から A 社の担当者に対してメールアドレスを変更した旨の、本物の連絡が送られていた。

このため、A 社の担当者は攻撃者とメールのやりとりを続ける中で、メールアドレスのドメイン部分が異なっていることに気付いたものの、同様のメールアドレスの変更が 1 か月前にもあったことから、それが不審であると判断することは難しい状況であった。

[12] ローカル部：メールアドレスの＠より左側の部分。

（2）決済手段の変更を装い、偽の振込先に誘導する

本事例では、決済方法としてA社からカンファレンス事務局へクレジットカードで支払いを行うこととなっていた。このとき、攻撃者は、B氏になりすましたメールの中で、「技術的な問題により、クレジットカードでの支払いを受け付けられなくなった」と理由をつけて、電子送金による振り込みを行うよう要求してきた。

これまで、ビジネスメール詐欺の手口で多く使われている「振込先口座の変更」は、実際のビジネスにおいては、そう多くは発生しないと思われ、それが不審であると気づくこともできるかと思われる。一方、クレジットカード決済は、システムのメンテナンス等により一時的に停止するといったケースが現実的に起こりえるため、それが不審であると見抜きにくく、攻撃者はその点を狙った可能性が考えられる。

ビジネスメール詐欺の対策として、急な振込先口座の変更だけでなく、急な「**決済手段の変更**」にも警戒する必要がある。

（3）ビジネスメールの授受に割り込み、詐欺を試みる

今回の事例では、2017年の夏頃からA社とB氏の間で、海外のカンファレンスブース出展に関するメールのやりとりが行われていた中で、フリーメールを使いB氏になりすました攻撃者が割り込み、詐欺を試みてきた（図 9）。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社と攻撃者の間で数回のメールのやりとりが行われ（図 10）、A社が攻撃者から送られた振込先口座に振り込みを行ってしまい、実被害を受けた。

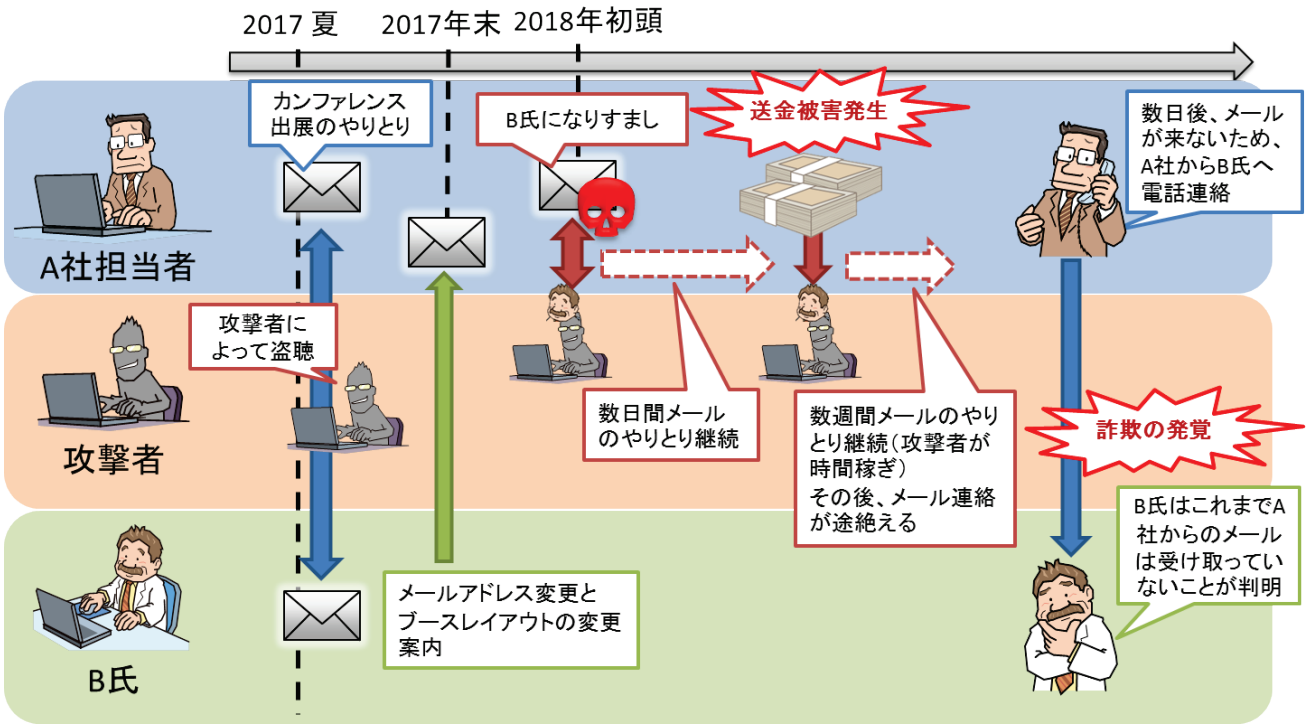

図 9 本事例の概要

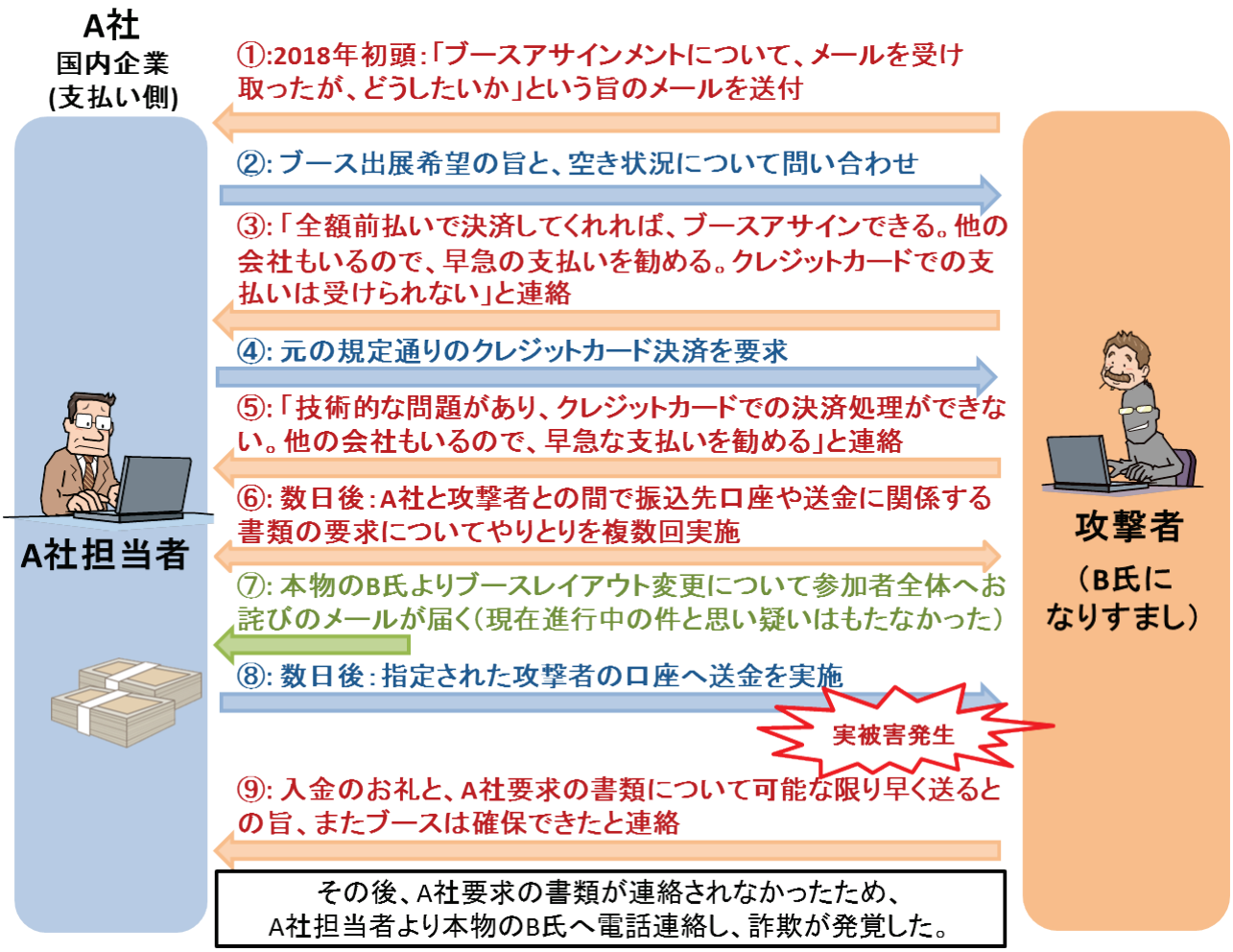

図 10 攻撃者とのやりとり

本件の攻撃者は、長い期間メールのやりとりを繰り返して、A 社よりカンファレンスのブース出展料を詐取したが、クレジットカードでの支払いが前提の金額であり、ビジネスメール詐欺でよく問題となるような、大きな金額ではなかった。しかし、本件の攻撃者は、カンファレンスのブース出展の窓口である B 氏へのなりすましに成功していることから、同時期にこのカンファレンスに出展しようとしていた他の企業からも、同じ手口で金銭の詐取を試みた可能性もある。

すなわち、1 つの組織を対象にして大きな金額を詐取するのではなく、クレジットカード決済が集中する組織とタイミングを見計らい、比較的少額ながら複数の相手を同時に騙すという手口であった可能性が考えられる。どこまで攻撃者が計画的に行ったかは不明であるが、「少額で警戒されにくい」「クレジットカード決済から口座振込へ変更」等、典型的なビジネスメール詐欺への警戒態勢や対応策をすり抜けるような手口であった。

6.2 海外関連企業の CEO を詐称する攻撃

本件で確認された事例では、国内組織の海外関連企業（C 社）において、C 社の CEO になりすました攻撃者から、偽の振り込みを要求するメールを送り付けられるというものであった。これは、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。

本事例では、支払側である C 社の支払い手続きの中で、メール受信者とは別の担当者がメールを確認したところ、不審な点に気づくことができたため、被害は発生しなかった。

攻撃の手口の詳細

本事例では、詐欺の過程において、C 社の CEO になりすました攻撃者が、次のようなメールを送信してきた。

- メールの送信元（From ヘッダ）には、本物の CEO のメールアドレスを設定
- メールの返信先（Reply-To ヘッダ）には、攻撃者のメールアドレスを設定

電子メールの仕組み上、From ヘッダは、メールを送信する側が任意の内容を指定する（偽装する）ことができる。そして、メールの受信者のメール表示画面には、この From ヘッダの内容が「送信者」として表示されるため、あたかも本物の CEO から送信されたメールのように見える。

この状態でメールに返信すると、返信メールの送り先は Reply-To ヘッダを基に設定されるため、From ヘッダに書かれた本物の CEO のメールアドレスではなく、攻撃者のメールアドレスとなる。よって、返信メール作成画面等で、この異常に気づくことができなければ、攻撃者にメールを送ってしまうこととなる。

本件の攻撃者が送信したメールの Reply-To ヘッダには、次のメールアドレスが指定されていた。

Reply-To ヘッダ：
【C 社 CEO の正規のメールアドレスのローカル部】 @ ●●ipad . com

※ドメイン部は一部伏せている。

メールアドレスのドメインが「●●ipad . com」となっているのは、受信者がメールの返信先が通常とは異なることに気づいた際に、「これは C 社の CEO が、iPad でメールを送受信しているからであろう」と受信者が錯誤することを狙ったものである可能性がある。また、メールの末尾に、iPad からの送信である旨の記載がある。

参考までに、攻撃者から送られてきたメールを図 11 に示す。

図 11 攻撃者からのメール（C 社の事例）

本事例では、図 11 のメールを起点として、図 12 に示すように、C 社の担当者と攻撃者との間でメールのやりとりが行われたが、幸い、C 社の支払い手続きの中で、メールの受信者とは別の担当者へ偽メールが転送され、別の担当者が不審であると気づくことができたため、被害には至らなかった。

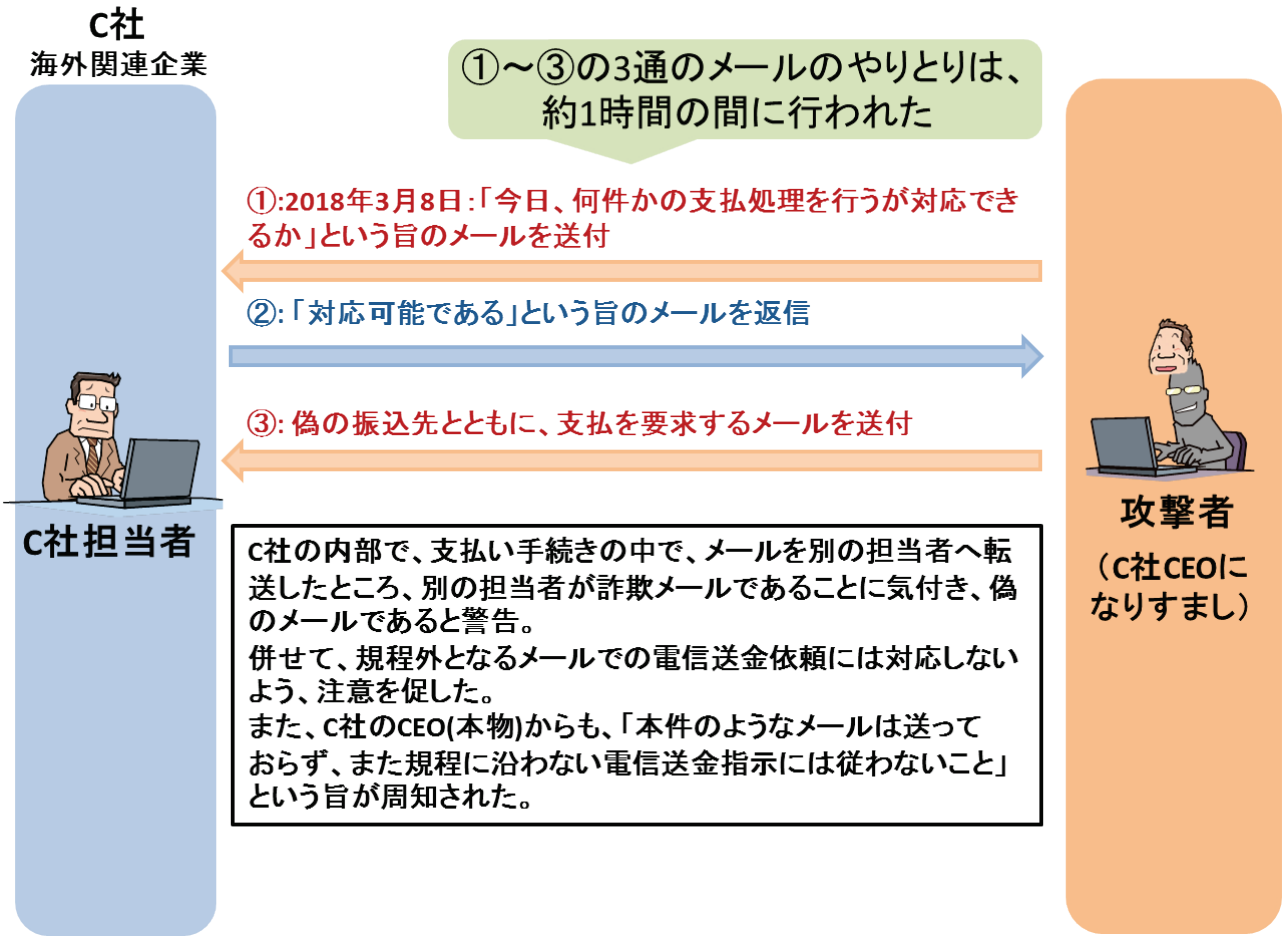

図 12 攻撃者とのやりとり（C 社の事例）

本件の攻撃者は、典型的なビジネスメール詐欺の手口で攻撃を行ってきた。しかしながら、メールのやりとりが約 1 時間の間に行われていることから、攻撃者は周到に準備した上で攻撃を行っているものと考えられる。

C 社で徹底されている通り、ビジネスメール詐欺への対策を念頭に置いた電信送金に関する社内規程を整備すること、複数の担当者が確認するといった対策が有効である。

6.3 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。

7　SLK ファイルを悪用した攻撃の手口

2018 年 2 月、脆弱性の悪用やマクロ機能の悪用とは異なる、Microsoft Excel の SLK（Symbolic Link）ファイルを用いた攻撃手口の情報を入手し、J-CSIP 内に情報共有を行った。

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、参加組織内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 [13]。

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 [14]ではあるが、攻撃の特徴、表示される警告画面、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

[13] 【参考資料】SLK ファイルを悪用した攻撃手口に関する注意点
[14] Warning! Trojan Droppers Exploiting Symbolic Link (.SLK) Files （APPRIVER）
https://blog.appriver.com/2018/02/trojan-droppers-using-symbolic-link-files/