サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2017 年 7 月～9 月]

2017 年 10 月 26 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、2017 年 9 月末時点の運用体制、2017 年 7 月～9 月の運用状況を示す。

1　運用体制

2017 年 7 月～9 月期（以下、本四半期）は、新たな SIG の発足、各 SIG での参加組織拡大があり、全体では 2017 年 6 月末の 8 業界 154 組織の体制から、11 業界 190 組織 [2]の体制となった（図 1）。

- 2017 年 7 月、化学業界 SIG に新たな参加組織があり、20 組織から 22 組織となった。
- 2017 年 9 月、新たに「航空業界 SIG」、「物流業界 SIG」、「鉄道業界 SIG」がそれぞれ発足した。
- 2017 年 9 月、クレジット業界 SIG に新たな参加組織があり、45 組織から 47 組織となった。

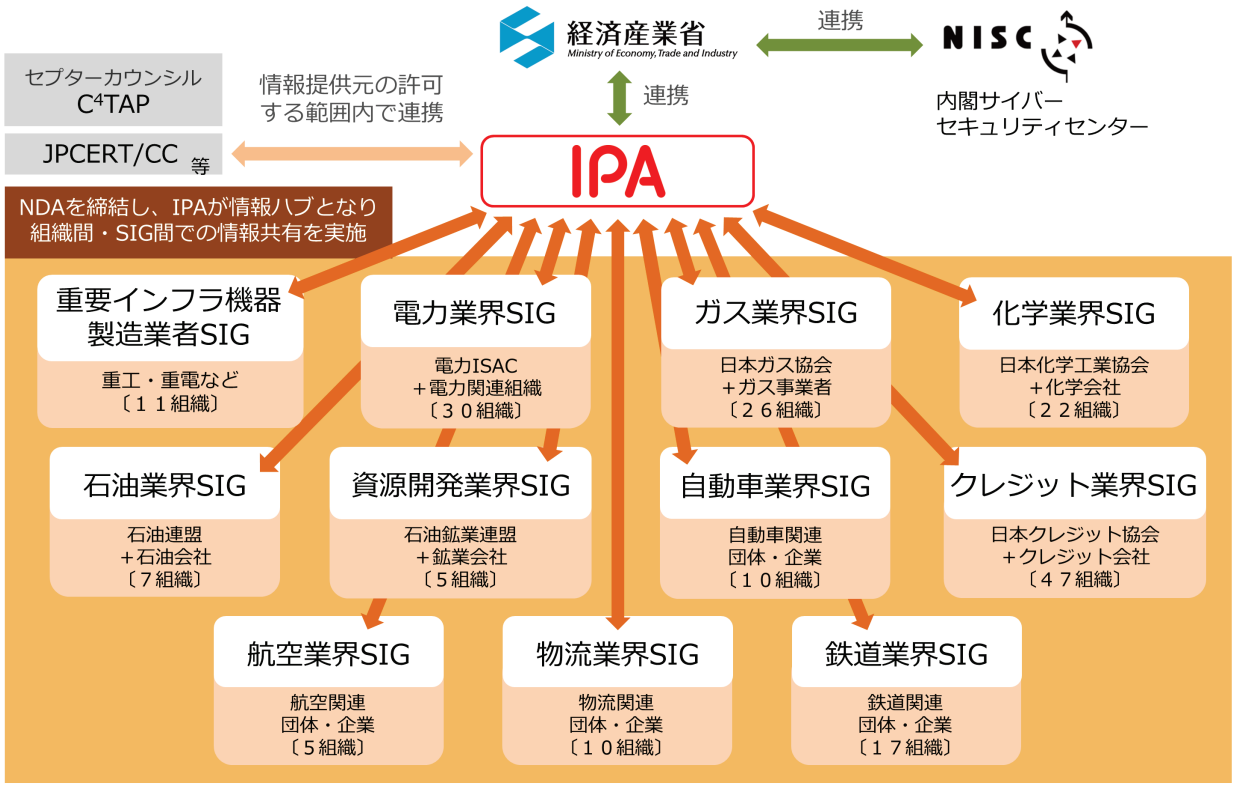

図 1 J-CSIP の体制図

---

[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/

[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（2017 年 7 月～9 月）

2017 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、11 の SIG、全 190 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	2016 年	2017 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	396 件	73 件	1,213 件	**57 件**
2	参加組織への情報共有実施件数※1	22 件	9 件	26 件	**17 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 **10 件**を含む。

本四半期は情報提供件数が **57 件**であり、うち標的型攻撃メールとみなした情報は **3 件**であった。前四半期は 6 件であったが、本四半期においても標的型攻撃メールの観測数は少ない傾向が続いた。

数は減少しているものの、日本語のばらまき型メールが前四半期に引き続き観測された。ばらまき型メールとは、国内の一般利用者を攻撃対象に、広く大量に送信されているウイルスメールであり、添付ファイルを開いた場合、オンラインバンキングの情報を窃取するウイルス等に感染させられることを確認している。日本サイバー犯罪対策センター[3]からもばらまき型メールの注意喚起情報が定期的に発信されており、多くの人の目にウイルスメールの情報が留まりやすくなっている。しかし、メールの件名や本文は一見して不自然だと判断しにくいものが増えており、標的型攻撃メールで使われるような、通常の業務で利用する件名と見間違えるようなものもあり、引き続き注意を要する状況にある。

また、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、特に本四半期は Office 365 のアカウント情報を狙ったフィッシングメールが目立った。企業や組織等で利用するクラウド型サービスのアカウント情報が狙われている可能性があり、これについては 3 章で改めて述べる。

本四半期に確認した標的型攻撃メールは、次にあげる特徴があった。

- 2011 年頃から観測されている「やりとり型」による標的型攻撃[4]について、2014 年[5]にも事例を確認、注意喚起を行っていたが、同じ手口による攻撃が 2015 年から 2017 年にかけて、数は少ないが一部の組織へ攻撃が継続している証跡を確認した。
- 海外の関連企業の従業員のアカウントを悪用し（乗っ取り）、国内企業へ不審メールを送り付けるという攻撃を観測した。詳細は明らかではないが、攻撃者が、防御の弱いところから侵入し、そこから侵入範囲を拡大しようと試みたものである可能性が考えられる。

---

[3] 一般財団法人日本サイバー犯罪対策センター JC3
https://www.jc3.or.jp/topics/virusmail.html

[4] サイバー情報共有イニシアティブ（J-CSIP）2013 年度 活動レポート ～「やり取り型」攻撃に関する分析情報の共有事例 ～ https://www.ipa.go.jp/security/J-CSIP/

[5] 組織外部向け窓口部門の方へ：「やり取り型」攻撃に対する注意喚起 ～ 国内 5 組織で再び攻撃を確認 ～
https://www.ipa.go.jp/security/topics/alert20141121.html

3　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観測した。この攻撃は、企業等にとって大きな脅威となっていると考えられるため、ここで事例を紹介する。

フィッシングメールとは、フィッシング詐欺の典型的な手口である、本物のウェブサイトと似せて作成した偽のウェブサイト（訪問者を騙すフィッシングサイト）へ利用者を誘導させるための偽のメールである。これまで、フィッシング詐欺の代表的な狙いは、インターネットバンキング、ショッピングサイト等の利用者のアカウント情報（ID、パスワード等）や、クレジットカードの情報等、直接的に金銭の奪取を行うための情報であった。一方、インターネット上で提供されているサービスが多機能化する中で、例えば企業の業務に利用するクラウドサービスの ID とパスワードのような、利用者のサービス上の権限を奪うことが目的とみられる攻撃も見られるようになってきた。

Office 365 は Microsoft から各種の最新ツールの提供を受けるサービスであり、個人利用だけでなく、企業や学術機関、非営利団体向けのプランもある。Office 365 を契約すると、メールやスケジュール管理のデータや、Microsoft Office の Word や Excel で作成したデータを、クラウド環境を使って保存、共有することができる。すなわち、Office 365 を企業等で導入している場合、そのアカウント情報は、その組織内の機密情報にアクセスする手段となる場合がある。

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 を利用している企業等の従業員が、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。

フィッシングメールの事例

J-CSIP の参加組織内で実際に観測された、Office 365 のアカウントを狙うフィッシングメールについて、次の 3 つの手口の事例を紹介する。それぞれ、異なる方法でフィッシングサイトへ誘導させる仕組みとなっていたことを確認している。

- メールに文書ファイルのようなアイコンを埋め込み、クリックさせる手口
- メールに html ファイルを添付し、html ファイルを開かせる手口
- メール本文中にある、URL リンクをクリックさせる手口

それぞれの手口を使った 4 件のメールと、メールから誘導されるフィッシングサイトを、参考として次に示す。

メールに文書ファイルのようなアイコンを埋め込み、クリックさせる手口

この手口では、一見、メールに何らかのファイルが添付されているかのように見える（本文中でも「添付ファイルを確認して…」や「この添付ファイルには…」等と英語で書いてあり、誤認を誘っている）が、実際は、このアイコンのような画像はメール本文中に埋め込まれた URL リンクである（図 2、図 4）。

メールにある、PDF ファイルや Word 文書ファイルのアイコンに見せかけたリンクをクリックすると、文書ファイルが開くのではなく、ウェブブラウザが起動し、フィッシングサイトが開く（＝フィッシングサイトに誘導される）。フィッシングサイトは、Office 365 の ID とパスワードの入力を求めるログイン画面となっていた（図 3、図 5）。これは、文書ファイルの閲覧にログインが必要であるかのように誤認させ、ID とパスワードを入力させることで、情報を騙し取るという手口である。

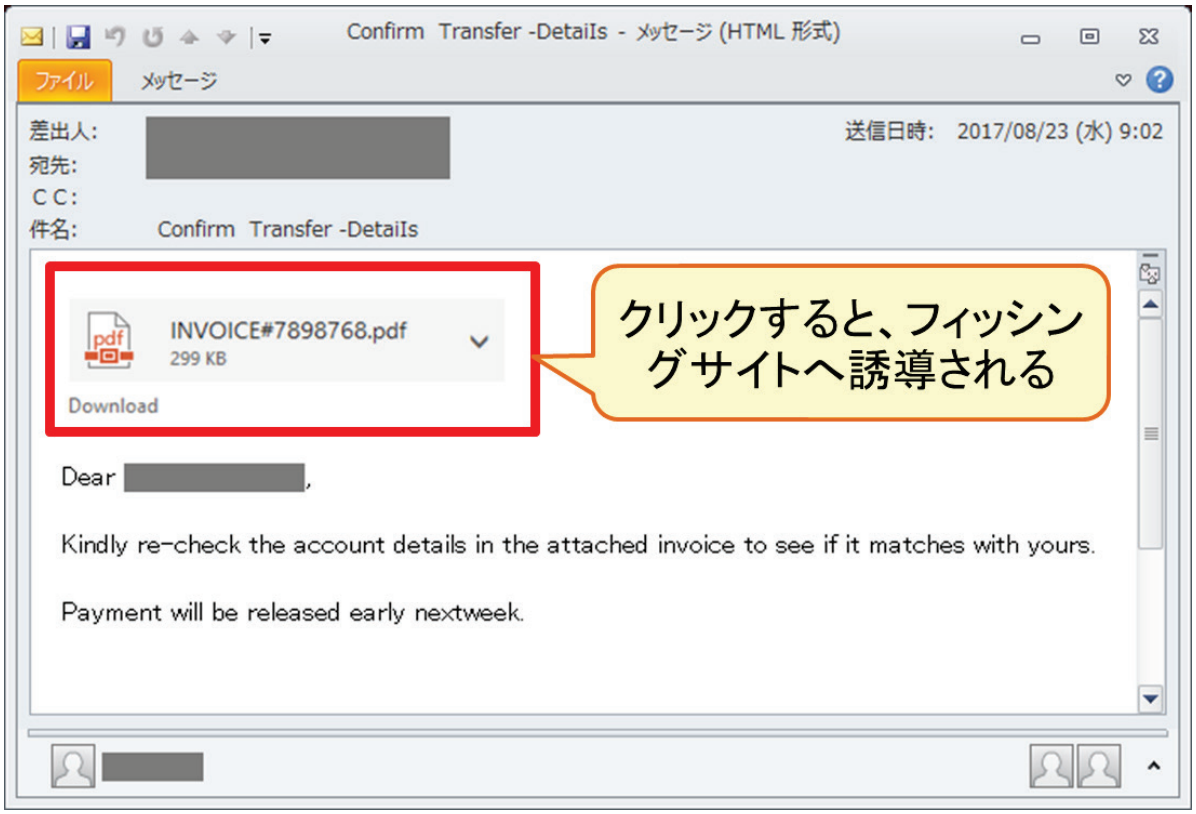

図 2 PDF ファイル風のアイコンを使ったフィッシングメール

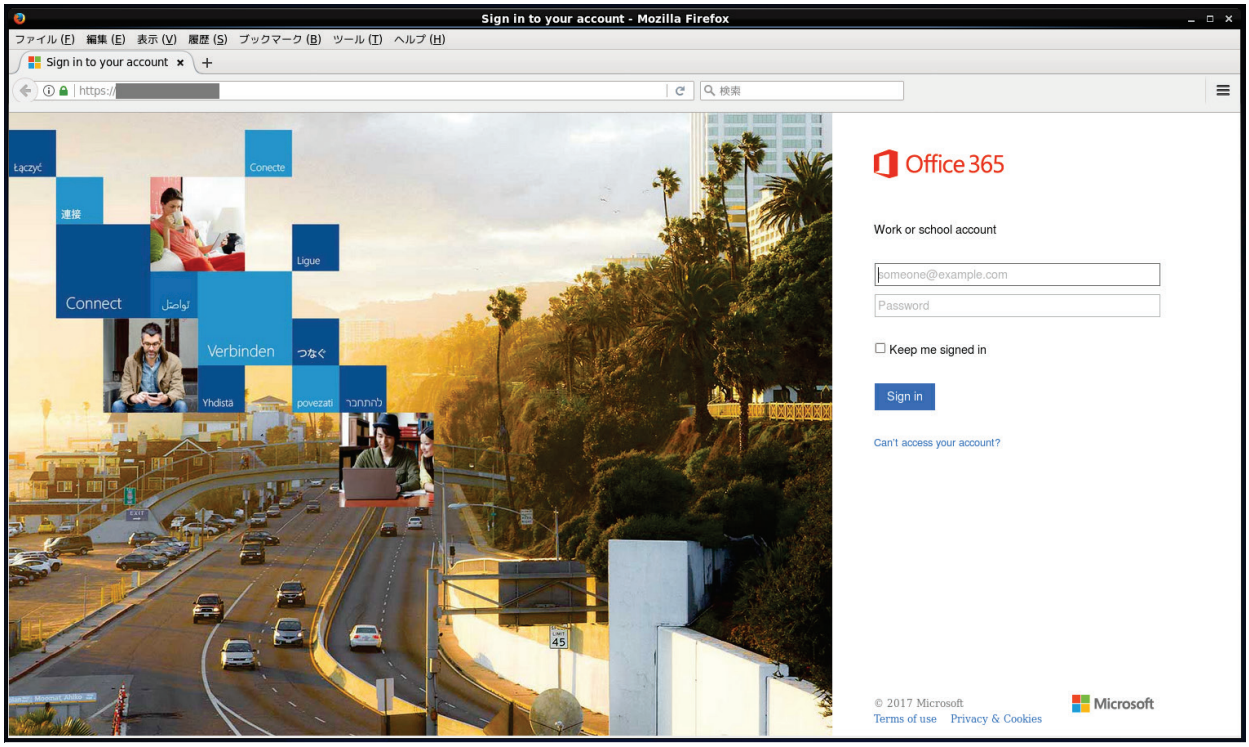

図 3 図 2 のメールから誘導されるフィッシングサイト

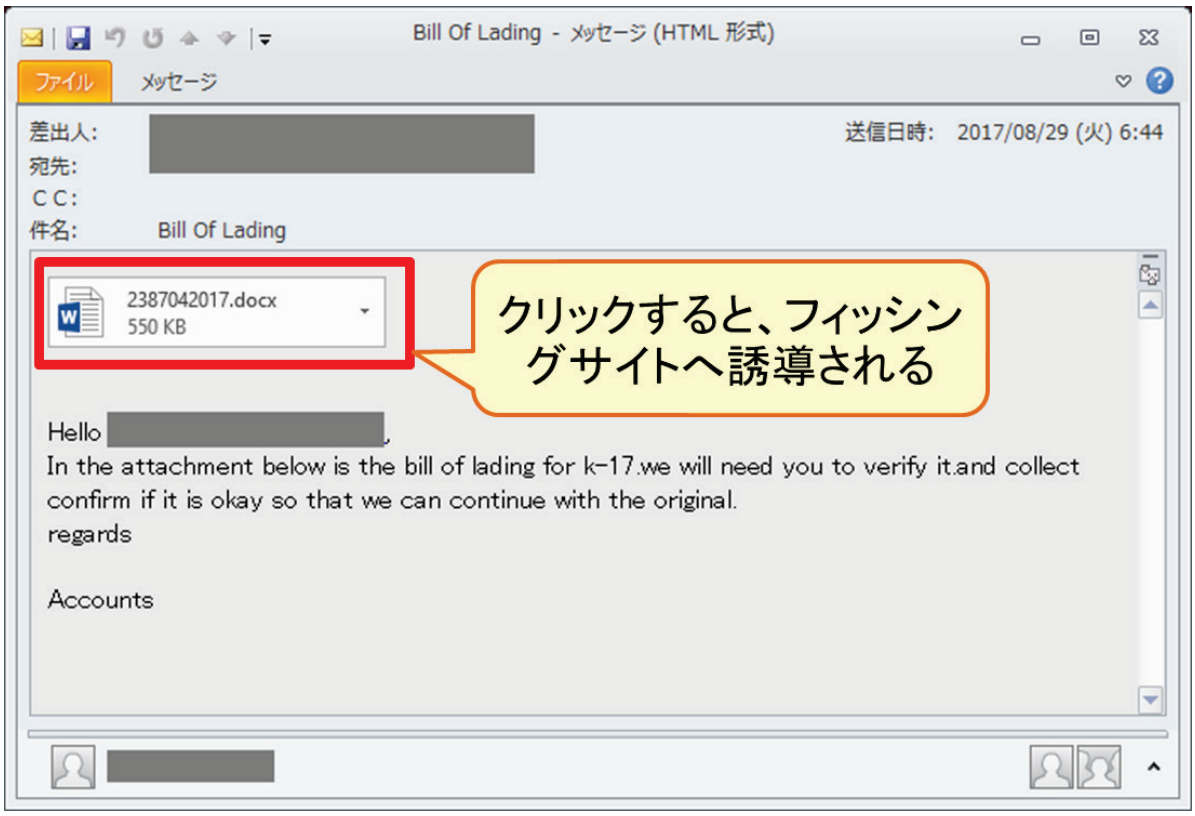

図 4 Word 文書ファイル風のアイコンを使ったフィッシングメール

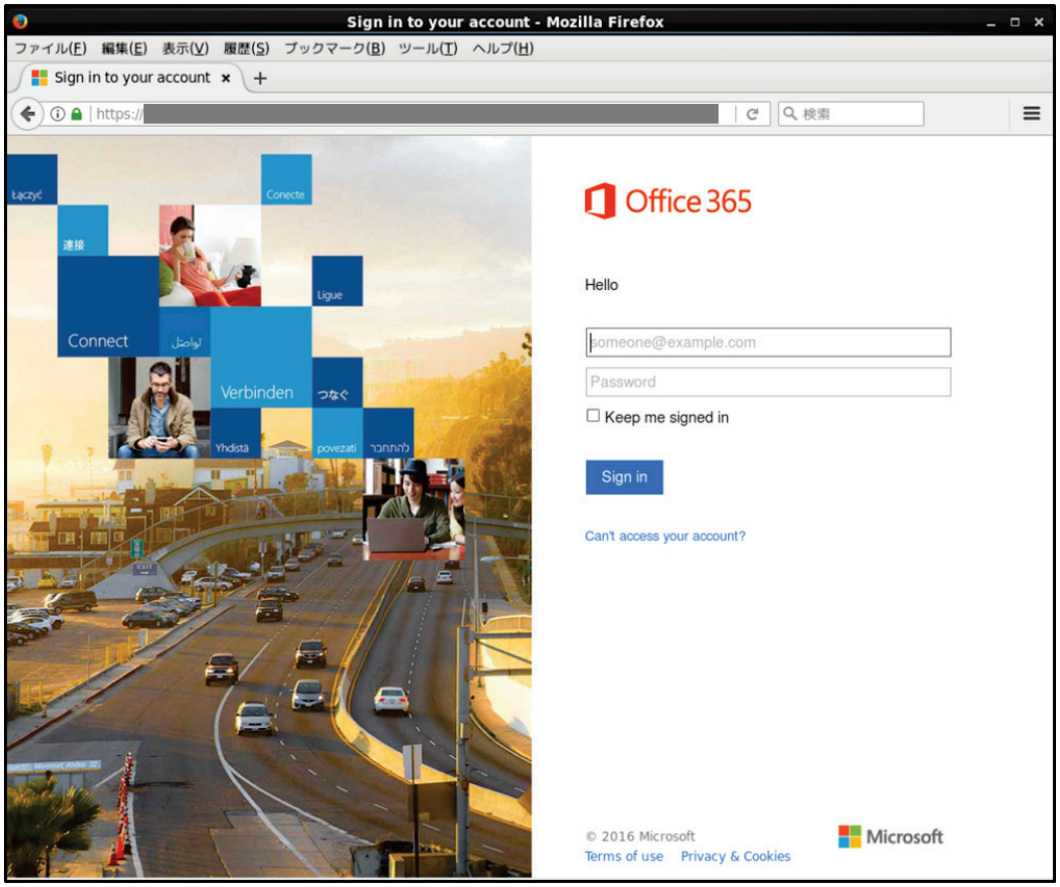

図 5 図 4 のメールから誘導されるフィッシングサイト

メールに html ファイルを添付し、html ファイルを開かせる手口

この手口では、メールに html ファイルが添付されており、メールの本文では、利用者に対し使用中のストレージ容量が逼迫しているため、"新しい設定情報"と称する何らかのファイルをダウンロードして追加容量を入手することを促している（図 6）。

このメールに添付されている html ファイルを開くと、ウェブブラウザが起動する。html ファイルには、フィッシングサイトへリダイレクトさせる命令が書かれており、自動的にフィッシングサイトが表示される（＝フィッシングサイトへ誘導される）。

フィッシングサイトは、Office 365 のパスワードの入力を求めるログイン画面となっていた[6]（図 7）。これは、何らかの設定変更にログインが必要であるかのように誤認させ、パスワードを入力させることで、情報を騙し取るという手口である。

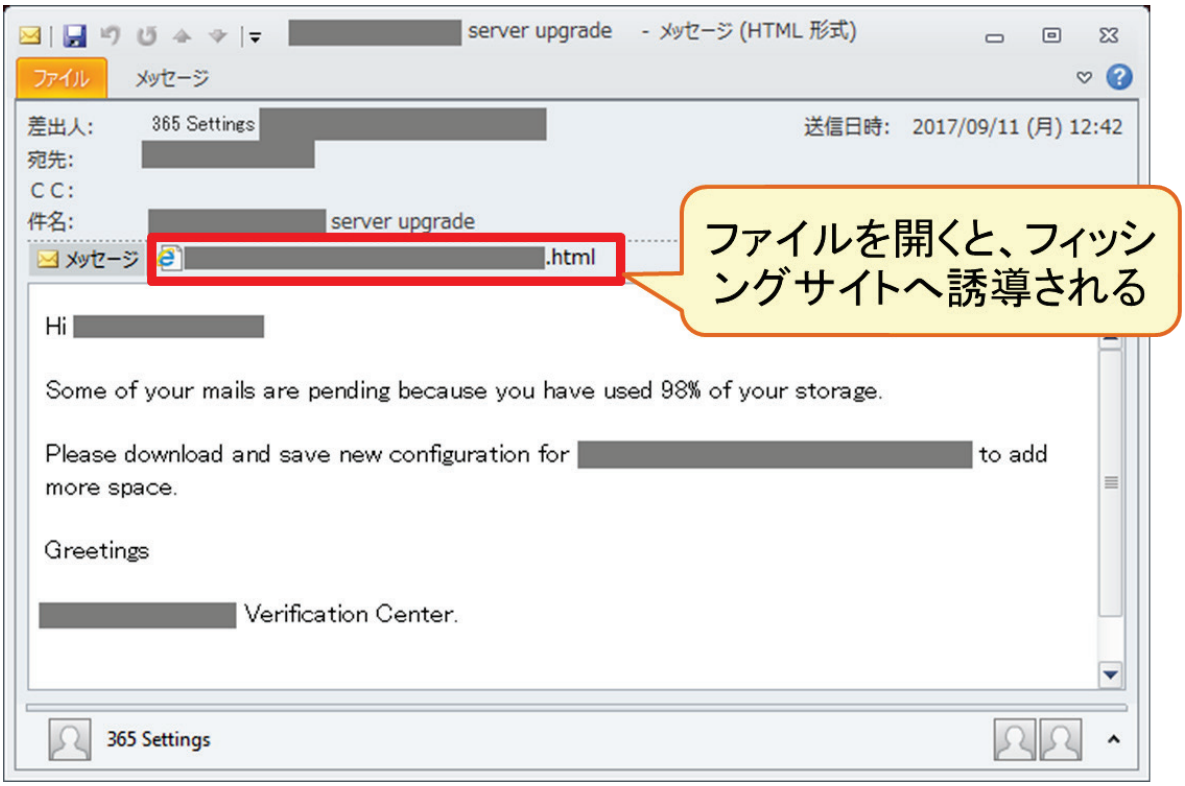

図 6 html ファイルを添付したフィッシングメール

[6] このフィッシングサイトには ID の入力欄が無いが、ID はメールアドレスが既に入力されているような状態を模擬していた。

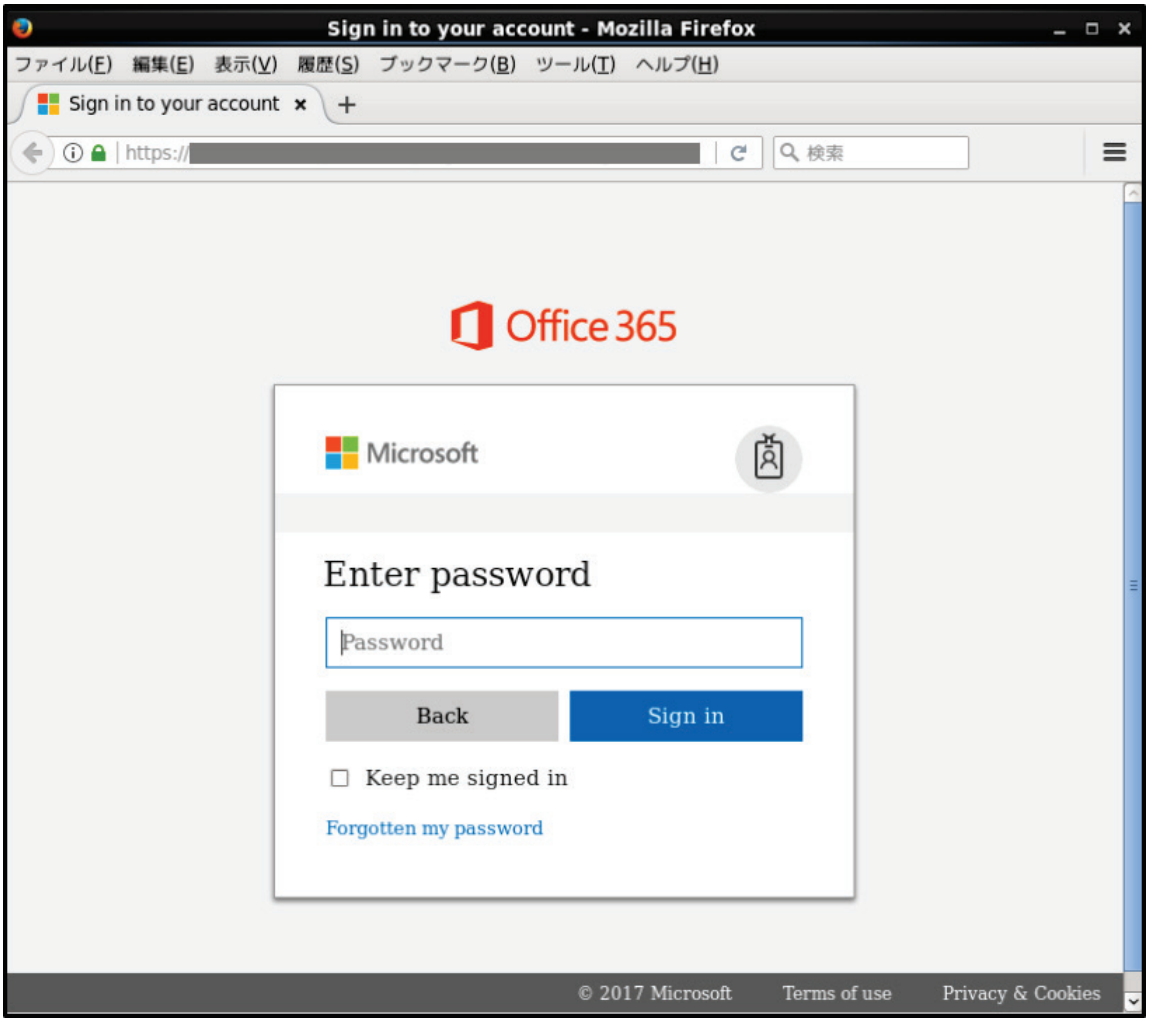

図 7 図 6 のメールに添付された html ファイルから誘導されるフィッシングサイト

メール本文中にある、URL リンクをクリックさせる手口

この手口では、配送会社を装ったメールで、メール本文中にURLリンク(″clicking here″の部分)が記載されており、配送保留にしている″重要な″小包を追跡するために、URL リンクをクリックすることを促している(図 8)。

この URL リンクをクリックすると、ウェブブラウザが起動し、フィッシングサイトが開く(=フィッシングサイトに誘導される)。フィッシングサイトは、Office 365 の ID とパスワードの入力を求めるログイン画面となっていた(図 9)。

配送保留の小包の追跡のために Office 365 のログインが求められるのは不自然ではあるが、「ログイン画面が表示された際、よく分からない場合はとりあえずログインする」ような行動を取っている場合は、騙されてしまうかもしれない。このログイン画面で ID とパスワードを入力した場合、入力した内容に関係なく、メールに書かれていた本物の配送会社のウェブサイトの画面が開く(図 10)。とはいえ、これは偽のメールであるため、当然ながら小包の配送追跡の画面等は開かない。これは、利用者に対し、騙されたことを気付かせにくくするための仕掛けだと思われる。

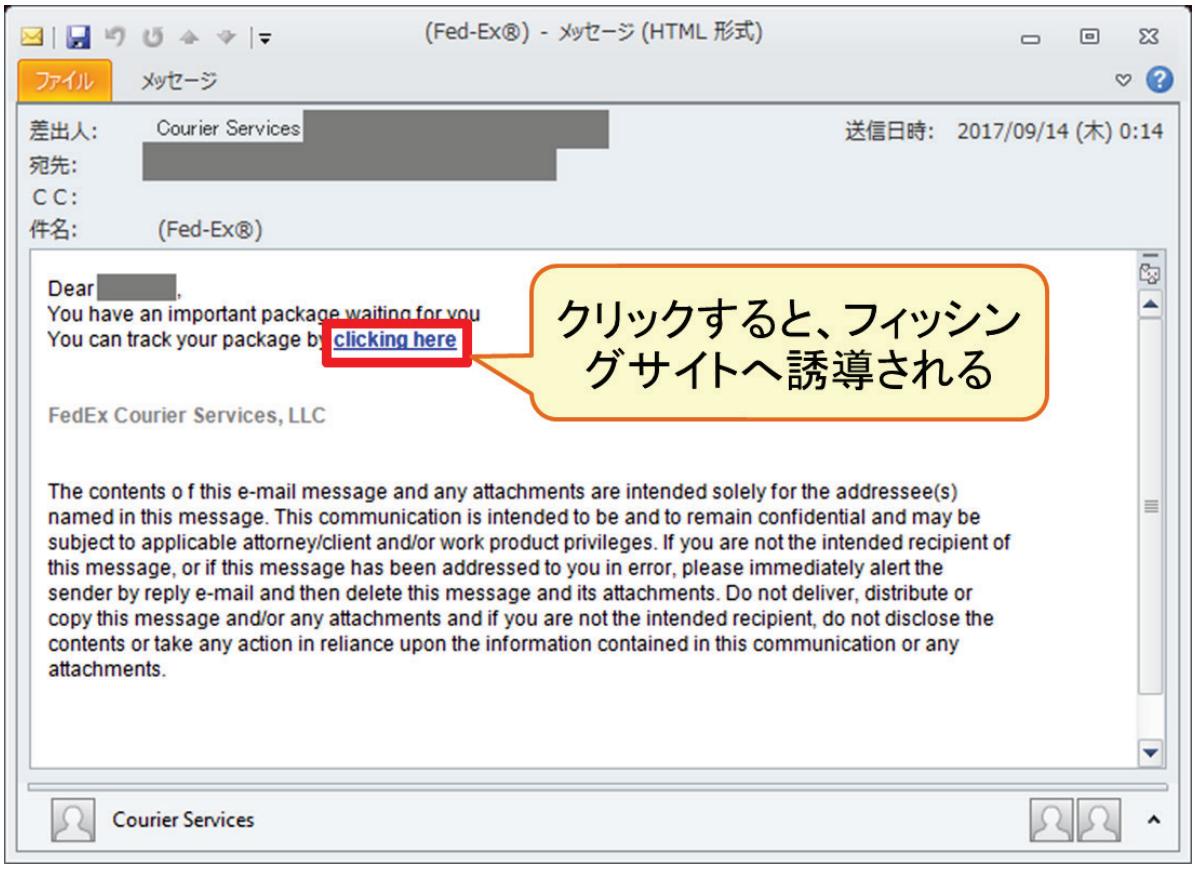

図 8 メール本文中に URL リンクがあるフィッシングメール

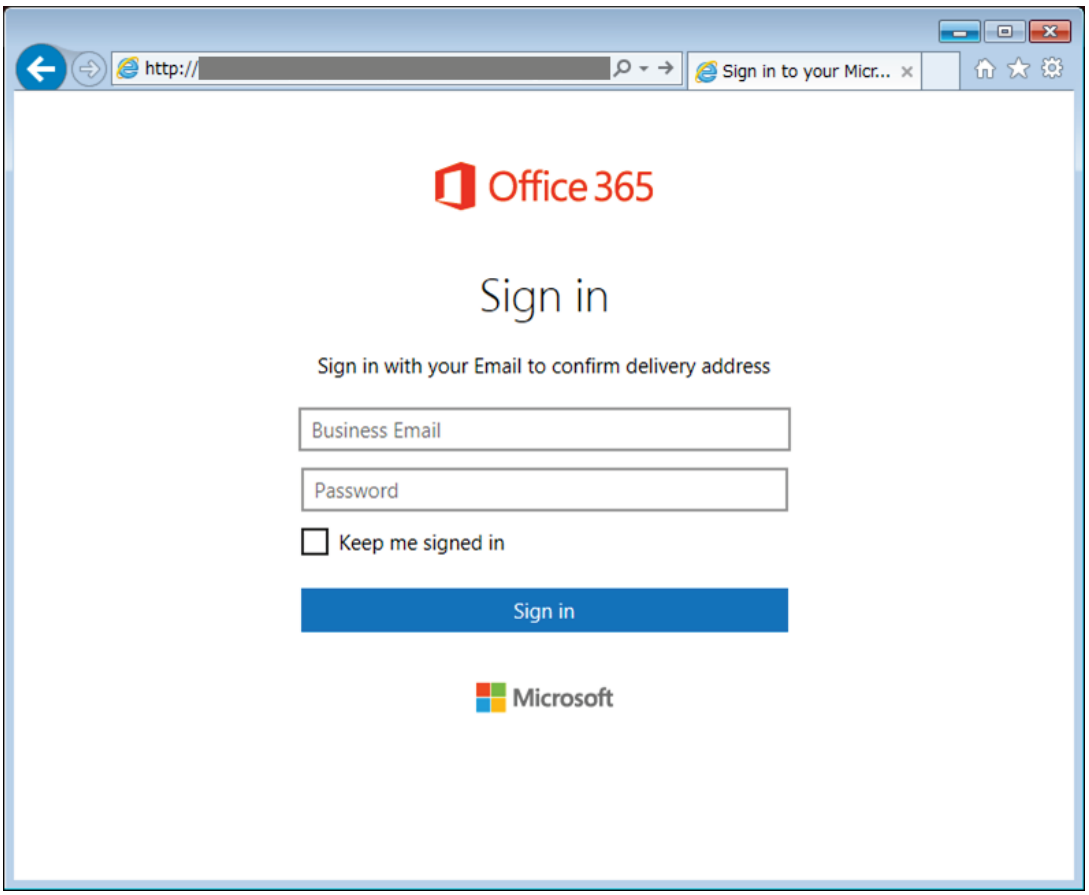

図 9 図 8 のメールから誘導されるフィッシングサイト

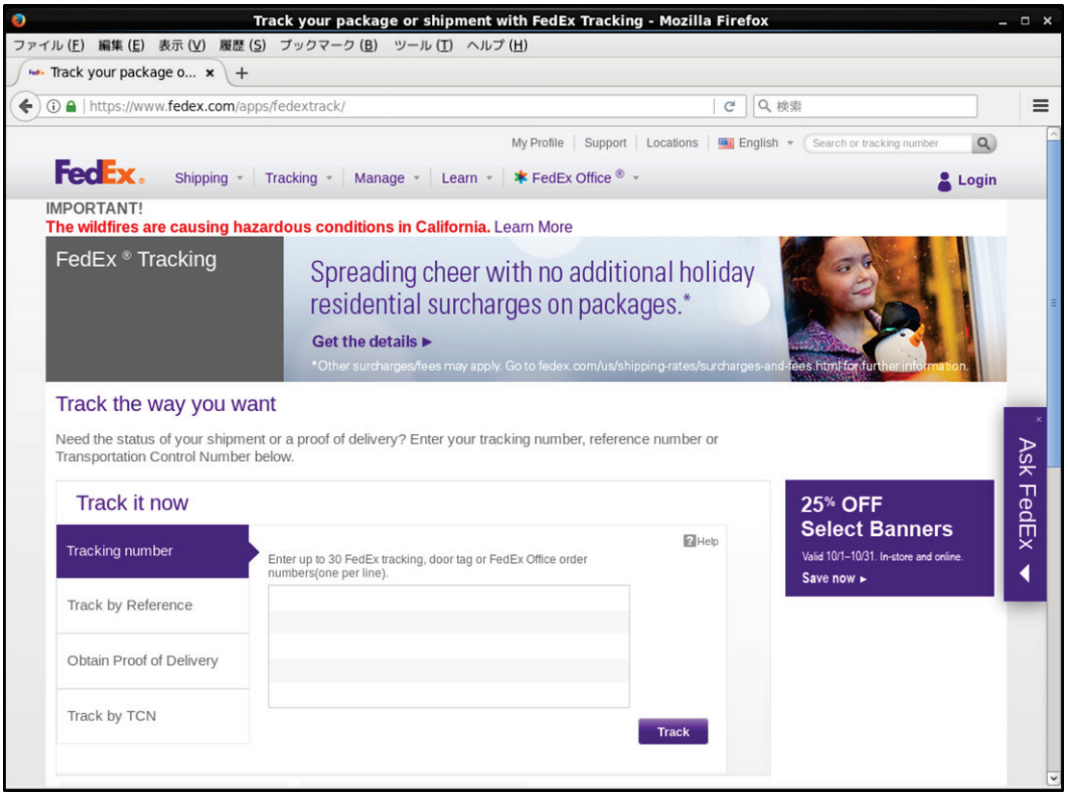

図 10 図 9 のフィッシングサイトから遷移する本物の配送会社のウェブサイト

まとめ

4 件のフィッシングメールと、フィッシングサイトへの誘導手口の事例を紹介した。

事例によりフィッシングサイトの画面は異なっているが、いずれにしても、一見して、偽物のログイン画面であると判断がしにくくなっている。また、フィッシングサイトに誘導する際、文書の閲覧のために ID やパスワードの入力が必要であるかのように見せかける騙しの手口があった。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にとっては、ウェブブラウザでアクセスした際に、ログインするための情報を入力させられるという行為は、さほど不自然な挙動と思わない可能性もあり、攻撃者はこのような心理を逆手にとっているものと考えられる。

フィッシング詐欺への対策は、このような攻撃があるということを知り、ひとりひとりが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 [7]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。

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

4　文書ファイルを悪用したフィッシング詐欺の手口

本四半期では、脆弱性の悪用とは異なる、PDF ファイルを用いるフィッシング詐欺の手口を観測した。PDF ファイルは通常のメールの添付ファイルとしてやりとりされることもあるため、実行形式ファイル等と異なり、ファイルの拡張子や形式のみから危険性を判断したり、遮断するという対応が難しい。

脆弱性の悪用に対しては修正プログラムの適用で危険を避けることが可能だが、今回観測した手口では、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、国内組織への攻撃メールで実際に悪用されていることを観測しているものは一部だが、今後、国内での攻撃に使われるようになる可能性がある。このため、攻撃手口と注意点をまとめた一般利用者向けの参考資料[8]を、本紙と併せて公開した。

参考資料では、文書を共有するクラウドサービスと連携しているかのような PDF ファイルを装う攻撃手口について、特徴と対応方法について記載している。

この手口では、PDF ファイル内に仕掛けられた罠の部分をクリックすることで、ID やパスワードを騙し取るためのフィッシングサイトにアクセスさせられるが、**フィッシングサイトへのアクセス前に警告画面が表示される。**警告メッセージを理解しないまま利用者が特定の操作を行うことで、フィッシングサイトへ誘導されてしまう。

このため、攻撃の特徴、表示される警告画面、アカウントが騙し取られることを防ぐため、利用者が選択すべき操作について広く知っていただく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。

「標的型サイバー攻撃特別相談窓口」への情報提供のお願い

IPA では、一般利用者や企業・組織向けの「標的型サイバー攻撃特別相談窓口」にて、標的型攻撃メールを含む標的型サイバー攻撃全般の相談や情報提供を受け付けている。限られた対象にのみ行われる標的型サイバー攻撃に対し、その手口や実態を把握するためには、攻撃を検知した方々からの情報提供が不可欠である。ぜひ、相談や情報提供をお寄せいただきたい。

「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

[8]【参考資料】文書ファイルを悪用したフィッシング詐欺の手口に関する注意点