サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2017 年 4 月～6 月]

2017 年 7 月 27 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 6 月末時点の運用体制、2017 年 4 月～6 月の運用状況を示す。

1　運用体制

2017 年 4 月～6 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 2016 年度末の 7 業界 86 組織の体制から、8 業界 154 組織 [2]の体制となった（図 1）。

- 2017 年 4 月、新たに「クレジット業界 SIG」が発足した。当初 29 組織で運用を開始し、6 月末までに参加組織は 45 組織へ拡大している。
- 2017 年 6 月、電力業界 SIG で組織改編を行った。これまで 11 組織の体制であったが、電力業界における情報共有体制の強化のため 2017 年 3 月に設立された「電力 ISAC[3]」およびその会員等が J-CSIP へ参加する形態となり、電力業界 SIG は 30 組織の体制となった。
- 重要インフラ機器製造業者 SIG に新たな参加組織があり、9 組織から 11 組織となった。また、化学業界 SIG も 18 組織から 20 組織へ参加組織が拡大した。

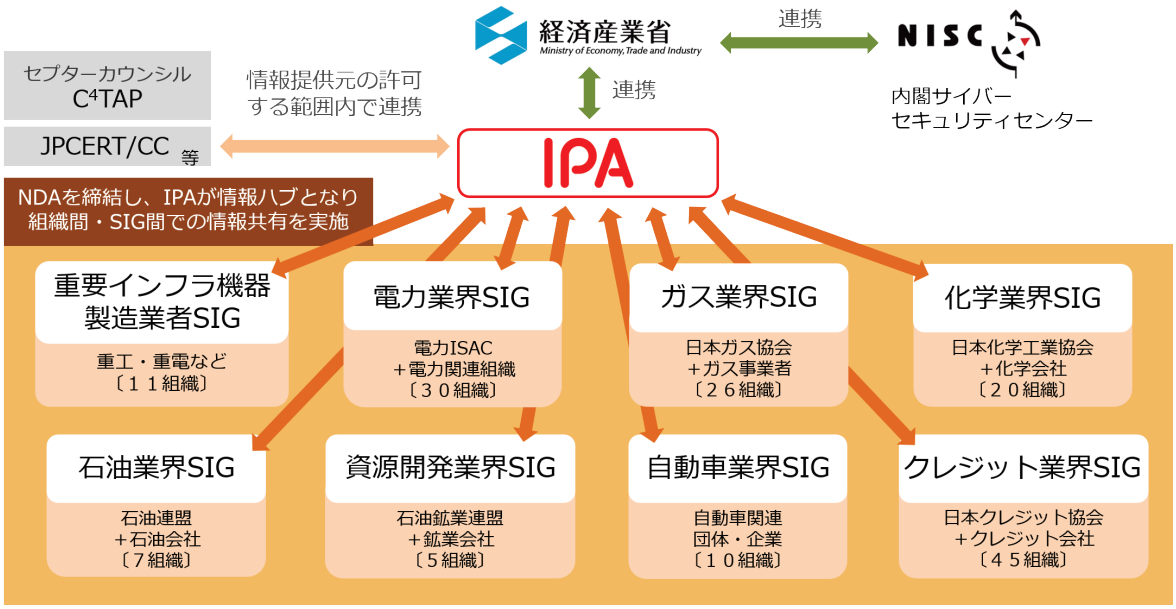

図 1 J-CSIP の体制図

---

[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。

[3] 電力 ISAC：https://www.je-isac.jp/

2　実施件数（2017 年 4 月～6 月）

2017 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、8 つの SIG、全 154 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	
		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	218 件	396 件	73 件	**1,213 件**
2	参加組織への情報共有実施件数※1	32 件	22 件	9 件	**26 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 **1,213 件**であり、うち標的型攻撃メールとみなした情報は **6 件**であった。前四半期は 0 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。

提供された情報の主なものとして、日本語のばらまき型メールが 1,171 件と大部分を占めている。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[4]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。

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は、着信した業界等に偏りは見られず、広く無差別に、かつ大量に送信されていた。一方、本四半期で確認した日本語のばらまき型メールは、いくつかあるパターンのうち、ある組織においては 1 通しか着信していないものがある等、明らかに多寡がみられた。この傾向の変化が始まった時期や理由は不明だが、今後、ばらまき型のウイルスメールによる攻撃であっても、必ずしも同一組織内の不特定多数に大量に着信するという形態ではなくなっていく可能性があり、ばらまき型メールを識別しにくくなることも考えられる。

ばらまき型メールに添付されていたファイルの特徴としては、前四半期までに多くみられた「圧縮された実行形式ファイル」や、「悪意のあるマクロが仕込まれた文書ファイル」に加えて、「Microsoft Office の OLE[5]機能を悪用した文書ファイル」を確認している。この、OLE 機能を悪用する手口については、4 章で改めて述べる。

---

[4] 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

[5] Object Linking and Embedding （オーエルイー）

本四半期の標的型攻撃メールについては、次にあげる特徴を持ったものがあった。

- 1 つのファイルに 2 種類のウイルスが内包されている攻撃を観測した。ファイルを実行すると、2 種類のウイルスに感染させられる。2 種類のウイルスはそれぞれ、複数の異なる不正通信先にアクセスを行うものであった。これは、ウイルス感染後に片方のウイルスが検疫等で削除されてもよいように、攻撃の二重化（冗長化）を行っている可能性が考えられる。
- 1 通のメールに添付されているパスワード付き圧縮ファイルに、2 つのファイルが格納されている攻撃を観測した。圧縮ファイルのパスワードは、メール本文中に記載されていた。2 つのファイルはそれぞれ、実行形式のファイルと CVE-2017-0199 の脆弱性を悪用する Word 文書ファイルであり、最終的に感染させられるウイルスは同一であった。利用者の PC へウイルスを感染させるため、念入りに二通りの攻撃を試みたものである。

また、本四半期においては、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[6]についても、情報提供を受けた。Wanna Cryptor は従来型のランサムウェアと異なり、Windows OS の脆弱性を悪用し、他の PC へ感染の拡大を試みるという特徴（いわゆる「ワーム」の機能）を持つランサムウェアであった。

ワーム自体は、1990 年代後半から 2000 年代前半に複数のウイルス（ワーム）が流行し、PC やネットワークへ多大な被害をもたらすことが認識されている脅威であるが、ランサムウェアにワームの機能が組み込まれたことによって、単独の PC だけではなく、複数の PC のデータが暗号化され機能しなくなるというような、大きな被害をもたらす脅威となった。外部ネットワークとの接点として設置されているマシンの脆弱性や、外部環境から（ウイルスに感染した状態で）持ち込まれてしまう PC 等、内部ネットワークへウイルス感染が拡大してしまうというリスクについて、外部ネットワークとの境界（出入口）にあたる対策だけではなく、内部ネットワークでの感染拡大防止策等の対策を行っていく必要があると考える。

[6] 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

3　ビジネスメール詐欺（BEC[7]）　国内組織への攻撃を相次いで確認

本四半期、情報共有活動を通じて、**同一と考えられる攻撃者から、J-CSIP 内の 2 組織へビジネスメール詐欺（BEC）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、J-CSIP の複数の参加組織より被害等の報告があったことを受け、この 4 月に IPA から注意喚起を公開[8]したところであった。

2017 年 6 月 2 日、J-CSIP の参加組織のひとつ（以下、A 社）より、被害には至らなかったが、ビジネスメール詐欺が試みられた（メールは英文だった）という情報提供があった。このため、IPA は、A 社で確認された攻撃手口等の情報を整理し、6 月 6 日、J-CSIP 内で情報共有を行った。

この情報共有を行った日（6 月 6 日）、**同一と考えられる攻撃者から、別の業界（SIG）の参加組織（以下、B 社）に対しても、同じようにビジネスメール詐欺が試みられた**ことが判明し、情報提供があった。情報共有を行った**メール本文と、返信先に使われている攻撃者のメールアドレスの情報が一致**していた。

短期間（1 週間）のうちに、**業種が異なる J-CSIP 内の国内企業 2 社へと連続してビジネスメール詐欺が試みられた**ということになる。

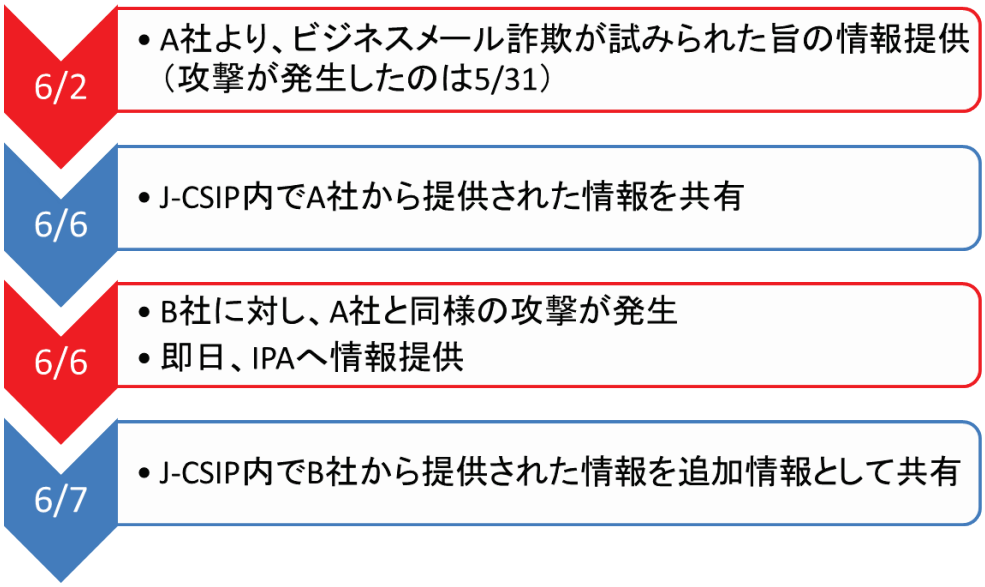

図 2 ビジネスメール詐欺の 2 件の情報提供と共有の流れ

今回確認されたビジネスメール詐欺の手口は、企業の経営者（CEO）を詐称し、財務責任者（CFO）を騙そうとするものであった。これは、IPA が公開した注意喚起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。

また、注意喚起であげた事例では、攻撃者が「メールアドレスのドメインを 1 文字変更する」、「フリーメールサービスを使ってそれらしいメールアドレスを作る」といった手口でメールの送信元を詐称していたが、今回の 2 件の事例では、**「送信元（From）メールアドレスを本物のメールアドレスに偽装し、返信先（Reply-to）メールアドレスを攻撃者のメールアドレスにする」**という手口が使われた。

---

[7] Business E-mail Compromise （ビーイーシー）

[8] 【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
https://www.ipa.go.jp/security/announce/20170403-bec.html

攻撃手口の詳細

今回の事例では、攻撃者が A 社および B 社の CEO になりすまし、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 の名前やメールアドレスを設定
- メールの返信先（Reply-To ヘッダ）には、攻撃者が取得した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に指定する（偽装する）ことができる。そして、メール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、返信メールの作成画面で、この異常に気づくことができなければ、攻撃者とメールをやりとりしてしまうことになる。

A 社の事例では、A 社と攻撃者の間で数回のメールのやりとりが行われたが、幸い、A 社側が途中で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 3）。また、その後の調査で、他の 2 名の社員へも同一の本文のメールが着信していたことが判明し、**計 3 名**へ攻撃が試みられていたことが分かった。

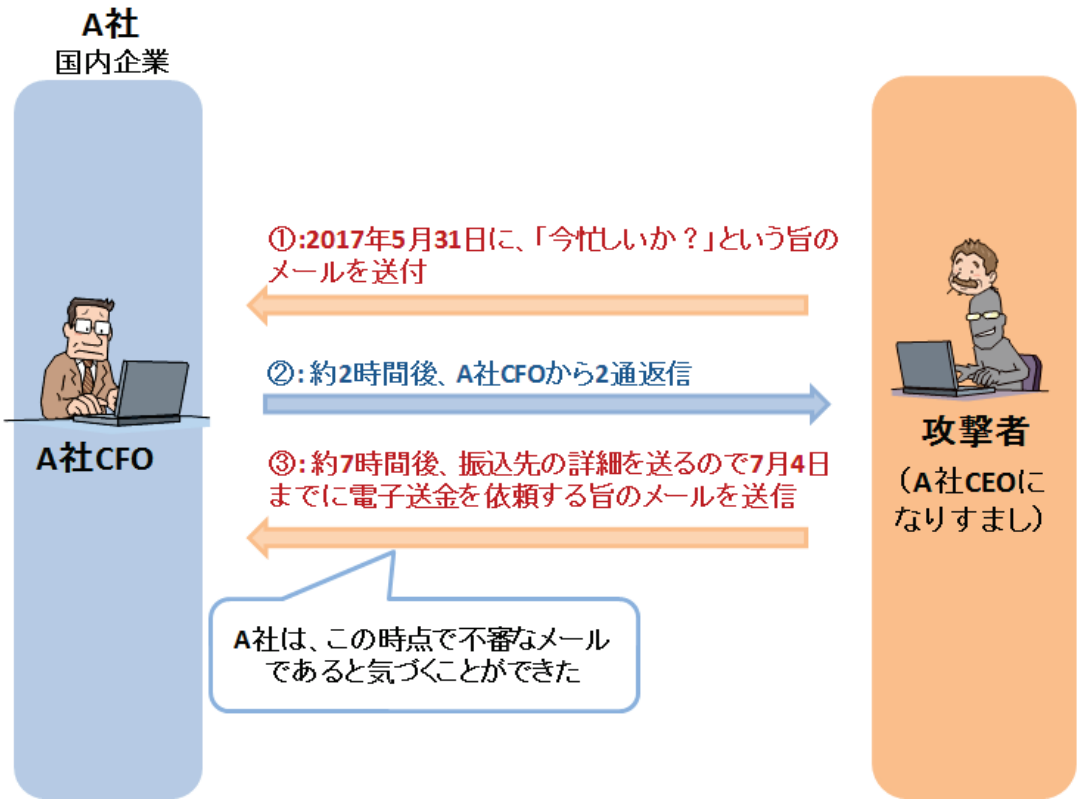

図 3 攻撃者とのやりとり（A 社の事例）

続いて、B 社において、A 社と同等の攻撃を確認したとの情報提供があった。
B 社に着信したメールは、A 社に最初に着信したものと件名は異なっていたが、**攻撃者のメールアドレスや本文の内容が同一**であり、From ヘッダと Reply-To ヘッダを使って詐称を行う手口は同様であった。

攻撃者は B 社の CEO になりすまし、B 社の現職の CFO と前任の CFO の **2 名**に対して同様のメールを送り付けていた。B 社は、攻撃者からのメールへ返信せず、被害に至らなかったが、仮に B 社が攻撃者へメールを返信していた場合、A 社と同じくビジネスメール詐欺が試みられたものと推測できる。
参考までに、B 社に対して送付された攻撃メールを図 4 に示す。

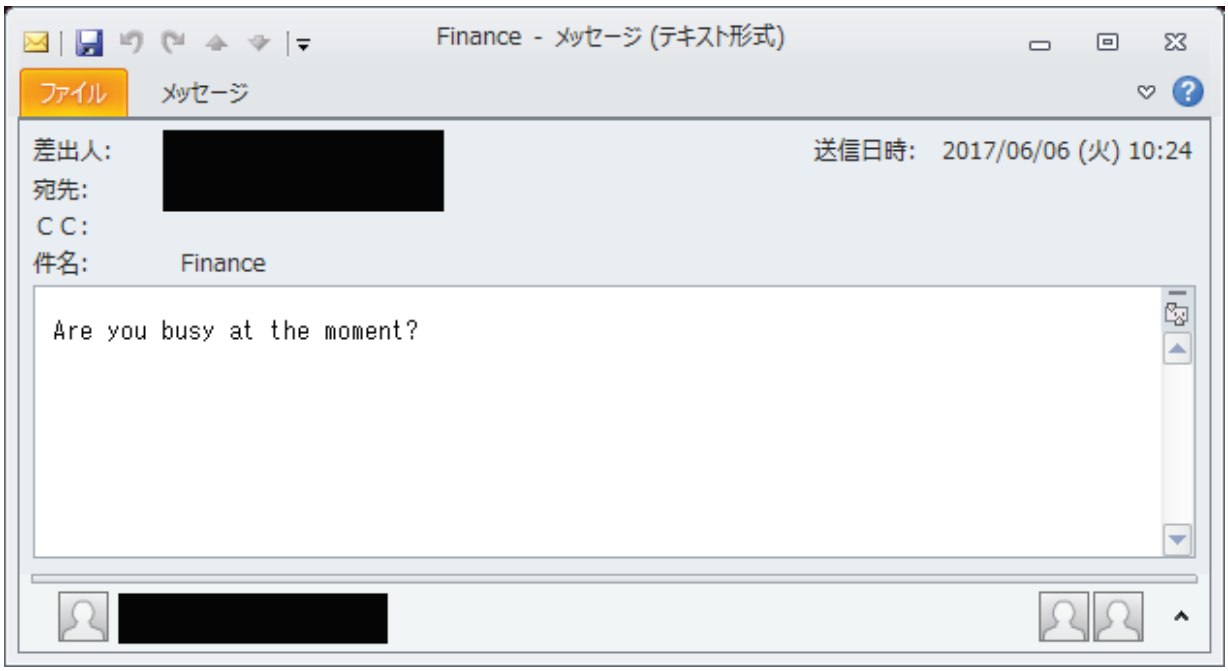

図 4 攻撃者からのメール(B 社の事例)

現在確認できている範囲の事例では、メールの内容は日本語ではないものの、ビジネスメール詐欺の標的として、日本国内の企業も狙われていることが確認できた。また、短い期間に別々の組織に対して攻撃が仕掛けられたことから、攻撃者は積極的に日本の企業を狙ってきている可能性がある。
ビジネスメール詐欺の事例と対策については、4 月に公開した注意喚起のレポートで詳細に述べている。被害に遭わないようにするためには、ビジネスメール詐欺の手口を知り、理解するとともに、不審なメール等への注意力を高めておくことが重要である。

4　文書ファイルの新たな悪用手口

本四半期では、脆弱性の悪用や、マクロ機能の悪用による攻撃とは異なる、Office・PDF 文書ファイルを用いる新たな攻撃手口を観測した。文書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、また、マクロ機能の悪用に対してはマクロを有効にしないよう徹底すること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。

これら新たな手口について、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[9]を、本紙と併せて公開した。

参考資料では、次の 3 つの攻撃手口について、特徴と対応方法について記載している。

- アイコンのような画像が埋め込まれた文書ファイル
  - 悪意のあるファイルを、OLE 機能を悪用し、Office 文書ファイル内に埋め込む手口
- Word 文書ファイルが埋め込まれた PDF ファイル
  - PDF ファイルに別のファイルを埋め込み、開かせる手口
- 細工されたスライドショー形式 PowerPoint ファイル
  - スライド内に、スライドショーの状態で動作するプログラム実行命令を埋め込む手口

いずれの手口においても、**ウイルス感染前に警告画面が表示される**が、**それぞれの攻撃手口によって表示される警告画面が異なり**、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ウイルスに感染させられてしまう。

また、これらの手口は、ばらまき型メールの添付ファイルに見られる手口ではあるが、一部は標的型攻撃にも用いられたことを確認している。このため、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

[9]【参考資料】文書ファイルの新たな悪用手口に関する注意点