サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2016 年 10 月～12 月]

2017 年 1 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、2016 年 10 月～12 月の運用状況は以下の通り。

1 実施件数

2016 年 10 月～12 月に、J-CSIP 参加組織から IPA に対し、標的型攻撃メールと思われる不審なメール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（7 つの SIG、全 87 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			
		1 月～3 月	4 月～6 月	7 月～9 月	**10 月～12 月**
1	IPA への情報提供件数	177 件	1,818 件	218 件	**396 件**
2	参加組織への情報共有実施件数	39 件	33 件	32 件	**22 件**※1

※1 同等の攻撃メール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と判断して情報共有対象としない場合等があるため、情報提供件数と情報共有実施件数には差が生じる。また、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 **2 件**を含む。

本四半期は情報提供件数が **396 件**であり、うち標的型攻撃メールとみなした情報は **19 件**であった。前四半期は 123 件と多くの標的型攻撃メールを観測したが、長期的には 2015 年 4 月から標的型攻撃メールの件数は四半期あたり 20～30 件程度の状況が続いている。

その他の情報提供の主なものは、英語のばらまき型メールが 296 件、日本語のばらまき型メールが 50 件と、大部分をばらまき型メールが占めている。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窃取を行うウイルスやランサムウェア[2]に感染させられることを確認している。日本語のばらまき型メールの件名・本文は、一見して不自然だと見抜きにくいものも増えてきており、引き続き注意を要する状況である。

前四半期に多数観測された、攻撃者「X」（J-CSIP 2014 年度の活動レポート[3]を参照）との関連性が見られる標的型攻撃メールについては、本四半期では 10 月～11 月に数件観測されるにとどまった。

本四半期の標的型攻撃メールについては、次に挙げるような特徴があった。

---

[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] IPA テクニカルウォッチ「ランサムウェアの脅威と対策」
https://www.ipa.go.jp/security/technicalwatch/20170123.html

[3] サイバー情報共有イニシアティブ（J-CSIP） 2014 年度 活動レポート レポート別冊 （IPA）
https://www.ipa.go.jp/files/000046019.pdf

- 会話を行った後でウイルスメールを送りつける、「やり取り型」攻撃を観測した。
  J-CSIP 2013 年度の活動レポート[4]で示した手口と大きく変わるものではないが、このような攻撃手口が継続して使用されているという事実を問い合わせ窓口の担当者をはじめとする職員等が認識していない場合、騙されて添付ファイル(ウイルス)を開いてしまう可能性がある。引き続き、組織内での警戒が必要である。
- Windows PowerShell によるスクリプトが埋め込まれたショートカット(lnk)ファイルが圧縮ファイルに格納されている攻撃を複数観測した。ショートカットファイルを悪用する手口は珍しくないが、拡張子が表示されない点など、継続して注意が必要な攻撃手口である。
  また、これらショートカットファイルの不正接続先(更なるウイルスのダウンロード先)は複数の標的型攻撃メールにおいて同一であったが、アクセスするタイミングによってダウンロードされるウイルスが変化したことを確認した。攻撃者は、不正接続先であるマシンを「攻撃インフラ」として継続して使い回しつつ、個別の攻撃や標的に合わせて複数のウイルスを使い分けていることが推察される。
- 不正な「コード署名」が行われた同種のウイルスを複数観測した。コード署名とは、ソフトウェアが改ざんされていないこと、開発元組織が実在することを証明するための仕組みである。今回、ウイルスのコード署名に使用されていた証明書は、認証局によって正しく発行されたものであり、漏えい等により攻撃者の手に渡って悪用されたものと思われる。
  コード署名されたファイルは、認証局によって開発元組織の実在が証明されており、「安全である可能性が高いファイル」という認識で扱われることがある。攻撃者はこの考え方を逆手にとり、ウイルスに不正な署名を施した可能性がある。
- 1 通のメールに 2 つのファイルが添付されており、どちらを開いてもウイルスに感染させられるという手口の攻撃メールを観測した。2 つの添付ファイルは、それぞれファイル名が異なり、拡張子とアイコンを偽装して Excel 文書ファイルと PDF 文書ファイルに見せかけた実行ファイルであった。

情報提供以外では、「毎日 100 通を超えるばらまき型メールが着信している」といった相談も寄せられた。着信しているメールに添付されたファイルは zip 形式の圧縮ファイル内に wsf ファイル、js ファイル、vbs ファイルが格納されていた。このようなウイルスメールに対しては、メールサーバ等において、圧縮ファイル内に存在するファイル名をチェックし、その拡張子がこれら実行ファイル相当の場合は、添付ファイルを隔離するといった対策が有効である。

2 統計情報

情報提供された不審なメールや添付ファイル等のウイルスについて、IPA の調査分析の結果得られた統計情報を、図 1 から図 4 のグラフに示す。今回の統計対象は、2016 年 10 月～12 月に提供された情報 **396 件**のうち、標的型攻撃メールとみなした **19 件**である。

- メール送信元地域(図 1)は、「アメリカ」が 42%を占めており、次いで「韓国」、「日本」の順番となっている。「アメリカ」の割合が高いのは同一の組織に同種の標的型攻撃メールが複数着信しており、それらのメールの送信元 IP アドレスが全てアメリカのものであったためである。また、前述した攻撃者「X」に関連するメールの送信元地域は全て「韓国」であった。
  「不明」は、メールの送信元 IP アドレスがメールヘッダに残らないフリーメールサービスから送信されていたものである。

---

[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
https://www.ipa.go.jp/files/000039231.pdf

- 不正接続先地域（図 2）は、「香港」が 48%を占めており、次いで「アメリカ」、「韓国」の順番となっている。「香港」の割合が高いのはメール送信元地域（図 1）のアメリカの割合が高い理由と同様で、同一の組織に同種の標的型攻撃メールが複数着信しており、これらに添付されたウイルスの不正接続先が全て同じであったためである。
- メールの種別（図 3）は 95%が「添付ファイル」となった。「不明」は、標的型攻撃メールと思われるメールが J-CSIP 参加組織で観測されたが、メールが既に削除済みで入手することができなかったものである。
- 添付ファイル種別（図 4）は、「実行ファイル」が 81%であった。これらの約半数は zip 形式の圧縮ファイルの中に実行ファイル（exe ファイル）が格納されているもので、残りはメールに実行ファイルが直接添付されていた。

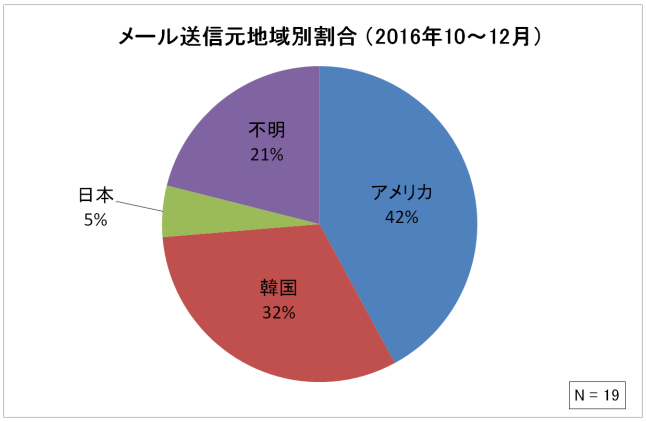

図 1 メール送信元地域別割合

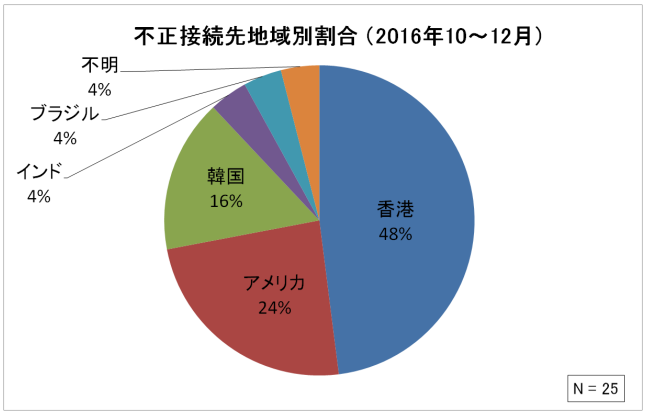

図 2 不正接続先地域別割合

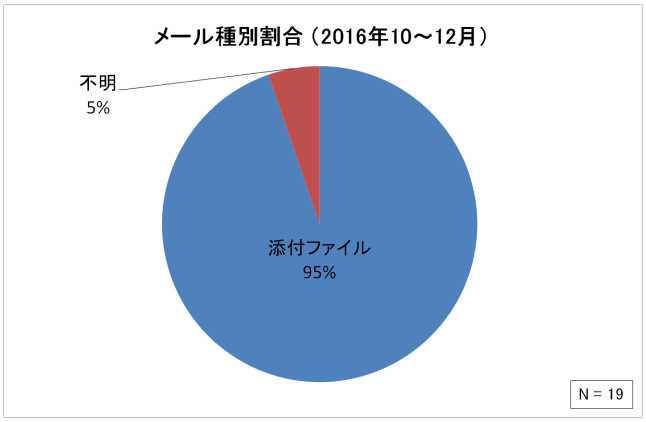

図 3 メール種別割合

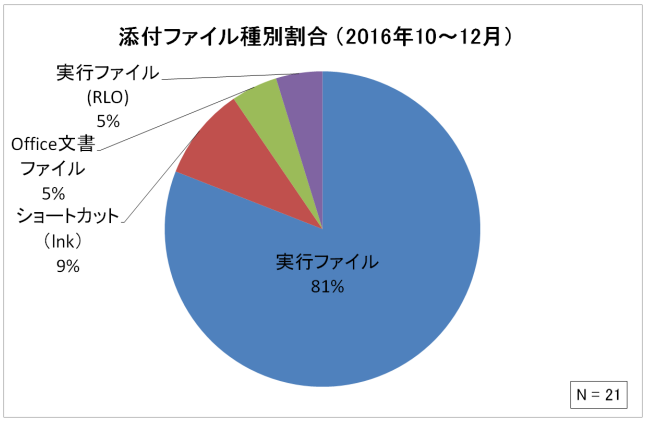

図 4 添付ファイル種別割合

注：グラフは小数点以下を四捨五入しているため、合計が 100%とならないことがある。

統計情報の補足事項

- ホスト名（FQDN）から得られる IP アドレスや、その IP アドレスが割り振られている地域は、時と共に変化する場合がある。本統計では、不審メール等の情報提供を受け、それを基に IPA が調査を行った時点で得られた情報を使用している。
- 攻撃メールの送信元や、不正接続先のマシンは、攻撃者が自身の身元を隠すため、遠隔操作ウイルスや不正アクセスによって乗っ取ったサーバやパソコン、VPN サービス等を悪用している場合がある。このため、この統計が即座に攻撃者のプロファイリングに繋がるものではない。
- 図 1 の「不明」とは、メールのヘッダ情報が確保できていない、メールヘッダに送信元の痕跡が残っていないといった理由で、送信元 IP アドレスが不明であったものである。
- 図 2 の「不明」とは、調査の時点で接続先のホスト名に対応した IP アドレスが名前解決できなかったといった理由によるものである。
- 図 3 の「不明」とは、不審なメールが着信したと思われるログ等は確認できたが、メールそのものは既に削除されていたといった理由により、メールの内容が確認できなかったものである。
- 図 4 について、添付ファイルが圧縮されたアーカイブファイル等であった場合、それを展開・復号して得られるファイルの種別で集計している。

グラフの母集団のサイズ N について

それぞれのグラフの基となっている母集団のサイズ N について、「IPA への情報提供件数」と異なっている理由を次に示す。

- 全体的に、IPA へ情報提供されたもののうち、広く無差別にばらまかれたウイルスメールと判断したもの等は統計対象から外しているため、「メール送信元地域別割合」と「メール種別割合」は、情報提供件数より数が少なくなる。
- 「添付ファイル種別割合」については、「1 通のメールに複数の添付ファイルが付いていた」、「添付ファイルがあったことは判明しているが、ウイルスとして駆除されており入手できなかった」等の場合があるため、全体の数が上下する。
- 「不正接続先の地域別割合」は、「1 つの添付ファイルから複数のウイルスが生成される」、「1 つのウイルスが複数のアドレスと通信を試みる」、「接続先不明」等の場合があるため、これもまた、他のグラフの N とは差が生じる。

J-CSIP の参加組織を募集中

J-CSIP は、約 5 年間の運用実績の中で、参加組織の方々より、情報共有が標的型攻撃対策の一つとして有効であるとの声をいただいています。この取り組みを継続するにあたり、IPA では、J-CSIP の活動主旨に賛同いただき、情報共有にご参加いただける企業・組織様を募っています[5]。

本活動は、業界ごとに SIG（Special Interest Group、情報共有を行うグループ）を形成してご参加いただくという形態であるため、とりまとめとなる業界団体様を通してご相談等をいただけるとスムーズです。また、ご関心がある場合は、業界団体様へ J-CSIP 事業のご説明に伺うことも可能です。

ご相談、問い合わせ等については、 **isec-info ＠ ipa.go.jp** までご連絡ください。

以上

[5] 参加に際しては、J-CSIP の運用上の要件との整合性を加味してご相談させていただきますので、必ずしもご期待に沿えるとは限らないことを予めご了承ください。