サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2016 年 4 月～6 月]

2016 年 7 月 29 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 4 月～6 月の運用状況は以下の通り。

1　実施件数

2016 年 4 月～6 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 72 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	件数	（2016 年 1 月～3 月）	（2015 年 10 月～12 月）	（2015 年 7 月～9 月）
1	IPA への情報提供件数	**1818 件**	（177 件）	（723 件）	（88 件）
2	参加組織への情報共有実施件数	**33 件**※1	（39 件）	（34 件）	（33 件）

※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 **14 件**を含む。

本四半期の情報提供件数は **1818 件**、そのうち、**1584 件**が日本語のばらまき型メールの情報提供であった。日本語のばらまき型メールとは、件名や本文に日本語が使われ、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る。メールの題材や文章は時間と共に変化を続けており、受信者に添付ファイルを開かせようと巧妙化している。添付ファイルを開いた場合、ランサムウェアやオンラインバンキングの情報窃取を行うウイルスに感染するであろうことを確認している。これらのメールは前四半期に引き続き J-CSIP 内においても多数観測しており、これらについては「標的型攻撃メール」とは見なしていないが、危険なウイルスメールではあるため、情報共有を行っている。

本四半期の 1818 件の情報提供のうち、標的型攻撃メールとみなした情報は **35 件**であった。これらのメールには、次に挙げるような注意を要する特徴が見られた。

- 本四半期で確認した zip 形式の圧縮ファイルでは、zip ファイルの中に「パスワードが設定された rar 形式の圧縮ファイル」と、「解凍パスワードが記載されたテキストファイル」が入っているものを複数観測した。これは、おそらく人の手でなければ解凍作業ができず、メールの配送経路上でのマシンによるウイルス検査等を避けるため、攻撃者が更に工夫を凝らした結果と思われる。
- 有名なオンラインストレージサービスに似通ったドメイン名を使った URL リンクがメール本文に記載されており、その URL リンクにアクセスさせようとする攻撃を確認した。
- 添付ファイル種別割合（図 4）における「Office 文書ファイル」は、マクロ機能を悪用するものであった。この文書ファイルでは、本文中に「ぼかし」効果を施した画像ファイルが挿入されており、「（画像ファイルの）内容を確認したい場合は、マクロ機能を有効にすること」といった指示が添えられていた。文書

[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/

の内容を確認しようと、この指示に従ってマクロ機能を有効化してしまうと、ウイルスに感染させられてしまう。マクロ機能の悪用は以前から多く見られるが、この手口では、基本的には何らかの方法で利用者にマクロを有効化するボタンをクリックさせる必要があり、攻撃者はそのための工夫を重ねていることが分かる。

- 35 件のうち、33 件のメールにおいて日本国内のドメインの、フリーメールサービスのメールアドレスが使用されていた。

2 日本語ばらまき型メールの傾向

2015 年 10 月頃から国内で多く観測されている日本語のばらまき型メールについて、前述の通り、本四半期も引き続き J-CSIP では多数観測している。これらのメールはいずれも着信した業界等に偏りは見られず、広く無差別に送信されているようであった。

本四半期では、ヤマト運輸[2]や日本郵便[3]からの配達通知を装ったメールがあった。これらのメールにはそれぞれの事業者から送られている本物のメールと同様の件名が使用されているものもあるため、騙されて添付ファイルを開かないよう注意が必要である。また、「残高」、「ご確認お願い致します。」、「状況一覧表」、「製造依頼」のように短い件名、簡潔な本文で特に違和感のない日本語を使ったメールも多数観測した。

添付ファイルは圧縮された実行形式ファイルであることがほとんどだが、ファイル名に「doc」、「xlsx」、「pdf」などの文字列を付け加え、実行形式ファイルであることに気付かれないよう細工が施されている。

参考として、本四半期に提供された情報の中から、2 種類の日本語のばらまき型メールについて、その傾向を表 2 に示す。

表 2 日本語のばらまき型メールの例

件名	「残高」	「ご確認お願い致します。」
情報提供件数	263 件	258 件
送信元メールアドレス	262 種類（重複したメール 1 件）	256 種類（重複したメール 2 件）
送信先（着信）メールアドレス	263 種類（重複なし）	258 種類（重複なし）
添付ファイル名	263 種類（重複なし）	258 種類（重複なし）
着信日時	252 種類（重複したメール 11 件）	251 種類（重複したメール 7 件）

表 2 の 2 種類のメールについて、それぞれメールの件名は全て同じだが、送信元メールアドレス、送信先（着信）メールアドレス、添付ファイル名がほぼ全て異なっている。

送信元として使われたメールアドレスは、「【日本人の姓】_【日本人の名】@【ISP 等の名前】.jp」、「【日本人の姓】@【英数文字列】.【ISP 等の名前】.jp」のようなメールアドレスを多数確認している。これらが実在するメールアドレスであるかは不明だが、少なくとも攻撃者が大量の「日本人が使いそうなメールアドレス」のリストを持っているか、日本人が使いそうなメールアドレスを大量に自動生成することが可能であることを示している。これにより、受信者が不審であると見破りにくくなるとともに、特定の送信元メールアドレスや添付ファイル名をブロック（受信拒否）するといった対策が難しくなっていると思われる。

このように、攻撃者は、日本人のメールアドレスの特徴や、日常的にやり取りされるメールの件名・文面について学習を続けていることが伺える。ばらまき型メールの攻撃は、今後、より巧妙化を続け、防御しにくくなっていく可能性があり、引き続き注意が必要である。

---

[2] ヤマト運輸からの注意喚起 －「お届け予定 e メール」等を装った不審メールにご注意ください
http://www.kuronekoyamato.co.jp/info/info_160629.html

[3] 日本郵便からの注意喚起 － 日本郵便を装った不審メールにご注意ください。
http://www.post.japanpost.jp/notification/notice/2016/0607_01.html

3　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 4 月～6 月に提供された情報 **1818 件**のうち、標的型攻撃メールとみなした **35 件**である。

- メール送信元地域（図 1）は、「香港」が 80%以上を占めている。本四半期は、同一の攻撃者と思われる者からの攻撃メールが複数の J-CSIP 参加組織に着信し、情報提供があった（ただし、内容は細部が異なっている）。そのため、メール送信元地域の内訳が偏った数値となっている。
- 不正接続先地域（図 2）は、「アメリカ」が 90%以上を占めている。この数値も図 1 と同様に、同一の攻撃者から送信されたと思われる攻撃メールに添付されたウイルスの不正接続先として、同一の IP アドレスが設定されていたことからこのような数値となっている。
- メール種別割合（図 3）は、過去の傾向から大きくは変わらず、「添付ファイル」が大部分を占めた。
- 添付ファイル種別（図 4）は、「実行ファイル」が 97%という高い割合になっている。これらの多くは前述の通り、zip 形式ファイルの中にパスワード付き rar 形式ファイルが含まれており、その rar 形式ファイルの中に実行ファイル（exe ファイル）が含まれているものであった。

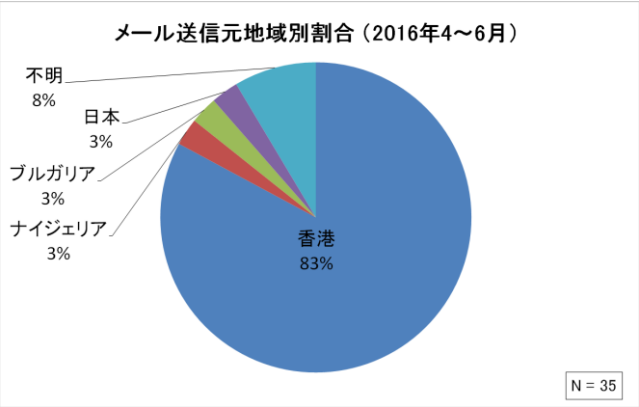

図 1　メール送信元地域別割合

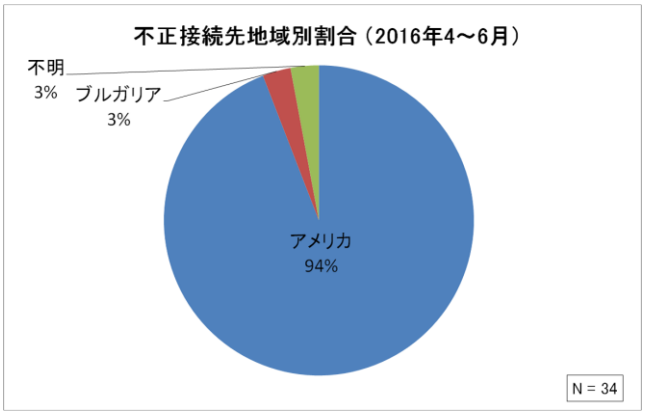

図 2　不正接続先地域別割合

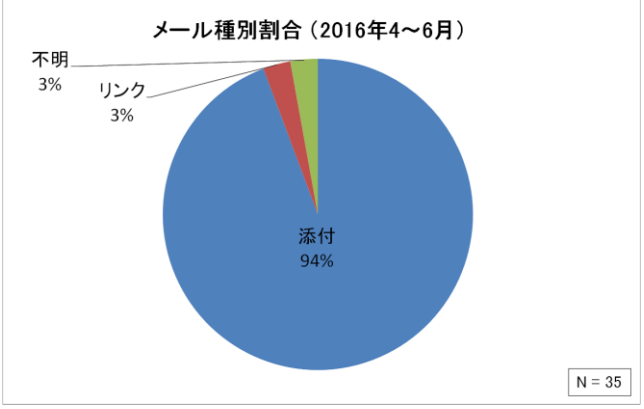

図 3　メール種別割合

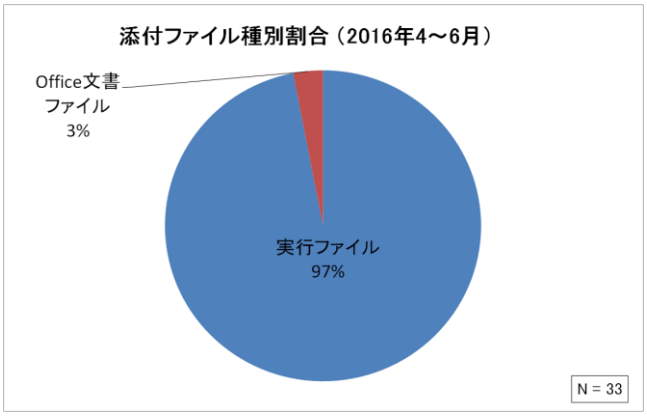

図 4　添付ファイル種別割合

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。

「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