サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2016 年 1 月～3 月]

2016 年 4 月 28 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 1 月～3 月の運用状況は以下の通り。

本四半期、J-CSIP の活動へ賛同いただき、自動車業界 SIG（10 組織）が新たに参加することとなり[2]、J-CSIP 全体での参加組織数は 62 組織から **72 組織**となった。

1 実施件数

2016 年 1 月～3 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	（2015 年 10 月～12 月）	（2015 年 7 月～9 月）	（2015 年 4 月～6 月）
1	IPA への情報提供件数	**177 件**	（723 件）	（88 件）	（104 件）
2	参加組織への情報共有実施件数	**39 件**※1	（34 件）	（33 件）	（27 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 24 件を含む。

本四半期は情報提供件数が **177 件**であった。前四半期ほどではないが、引き続き、国内の利用者を攻撃対象としていると思われる「ばらまき型メール」が観測されている状況であり、これらの情報についても、共有を図っている。

177 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 **27 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。

- 前四半期と同じく、本四半期で確認した zip 形式の添付ファイルは全て暗号化されていた（圧縮パスワードが設定されていた）。これは、メールの配送経路でのウイルス検査等を避けるためと思われる。標的型攻撃において、攻撃者は防御側でどのような対策を講じているかを想定した上で攻撃を行ってきているものと考えられる。パスワード付き zip ファイルは、その典型的な手口の一つである。
- 年末年始の挨拶等を装う手口の攻撃メールを、過去の同時期（2014 年と 2015 年初頭）と同様に観測した。添付されていたウイルスも酷似したものであり、長期的に攻撃を繰り返しているものと思われる。
- メールに添付された PDF ファイル自体は無害だが、その PDF ファイルの文中に悪意のあるウェブサイトの URL リンクを記載し、誘導しようとする攻撃を確認した。メール本文中に URL リンクを記載すると、ウイルス検査や不審メール検査の対象となりえるため、これを回避しようとした可能性がある。
- 27 件のうち、差出人（From）メールアドレスの情報が得られたものは 22 件であったが、このうち 15 件で日本国内のドメインのメールアドレスが使われていた（フリーメール 11 件、その他 4 件）。

[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] 「サイバー情報共有イニシアティブ（J-CSIP）に自動車関連業界が新たに参加。正式運用を本日開始」（IPA）
https://www.ipa.go.jp/about/press/20160126.html

「ばらまき型メール」について

前四半期、国内で多く観測されていた日本語が使われた「ばらまき型メール」を、本四半期も引き続き J-CSIP において多数観測した。

2015 年 12 月に引き続き、主にロシアの「Rambler Mail」というサービスで取得できるメールアドレスから、“番号 xxxxxxxx の下での小包の配達”[3]、“日本郵政公社トラック”、“税務署から”、“DHL”、“EMS”、“負債通知”等の件名のウイルスメールが広くばらまかれたことを確認した。また、新たな手口として、ウイルスを添付ファイルとせず、オンラインストレージサービスにアップロードした上で、その URL リンクをメール本文に記載し、利用者にダウンロードさせるという手口も確認した。添付ファイルがウイルス対策ソフト等で駆除されることを避けることが目的と思われる。「ばらまき型」とはいえ、今後も手口の巧妙化が懸念される。

また、本四半期は、一連の「Rambler Mail」からのものとは異なる種と思われるウイルスが添付されている、別の「ばらまき型メール」も広く観測した。このメールは、一部、前四半期にも“フォト”、“【完成図・成績表】”などの短い日本語の件名・本文でばらまかれていたが、本四半期では“遅れましたが、添付ファイルにて送ります。よろしくお願いします。”、“お世話になります。 以上、宜しく願います。”といった、より自然な日本語が使われるようになった。

今後もばらまき型メールの攻撃手口や件名・本文がブラッシュアップされていく可能性があり、引き続き注意が必要である。

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 1 月～3 月に提供された情報 177 件のうち、標的型攻撃メールとみなした **27 件**である。

- メール送信元地域（図 1）は、「アメリカ」が最多となり、次いで「韓国」、「セルビア」「ナイジェリア」となっている。アメリカからは複数種類の標的型攻撃メールが送信されており、韓国からは同種の標的型攻撃メールが送信されていた。
- 不正接続先地域（図 2）は、「韓国」「イギリス」「日本」の 3 ヵ国で大半を占めた。また、日本国内向けのフリーメールサービスを使用して送信されていた攻撃メールの添付ファイル（ウイルス）の不正接続先は、全て日本国内の IP アドレスであった。攻撃者が物理的にどこにいるのかは不明だが、これら一部の攻撃行為は、国内のサービスやマシンを使って行われている状況である。
- メールの種別（図 3）は、「添付ファイル」がほとんど（92%）を占めた。
- 添付ファイル種別（図 4）は、「実行ファイル」が 92%という高い割合になっており、これらの多くは前述の通り暗号化（パスワード付き）zip 形式ファイルとしてメールに添付されていた。実行ファイル（の拡張子のファイル）が含まれる zip 形式のファイルについては、メールサーバ等で排除もしくは配送を保留する対策を推奨する。

  また、数は少ないが、実行ファイル以外に「PDF ファイル」を用いた攻撃も観測している。前述の通り、PDF ファイル自体は無害だが、その中に記載された URL リンクが、攻撃者の管理していると思われるウェブサイトへ誘導するものであった。

[3] 「日本郵政を騙った不審メールが急増していますのでご注意ください」（日本郵政）
http://www.japanpost.jp/information/2016/20160216115665.html

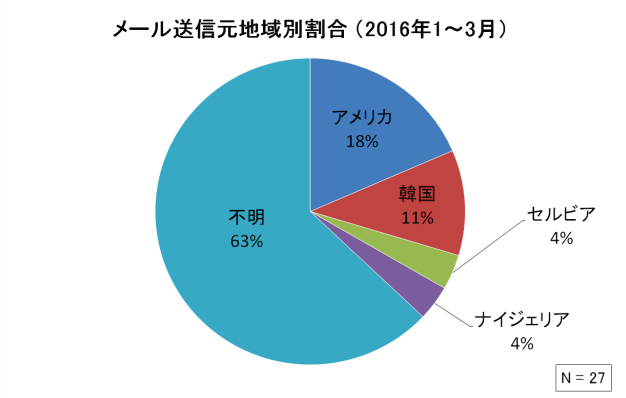

図 1　メール送信元地域別割合

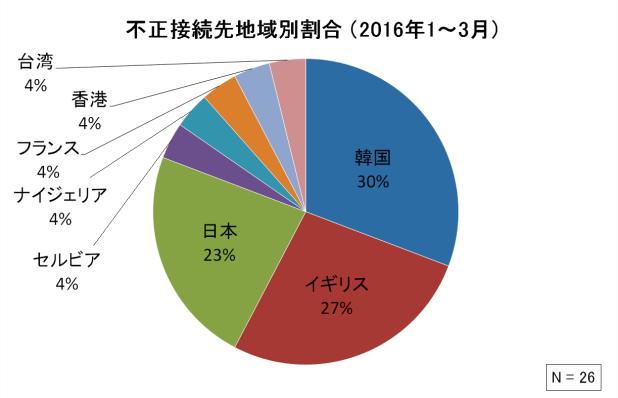

図 2　不正接続先地域別割合

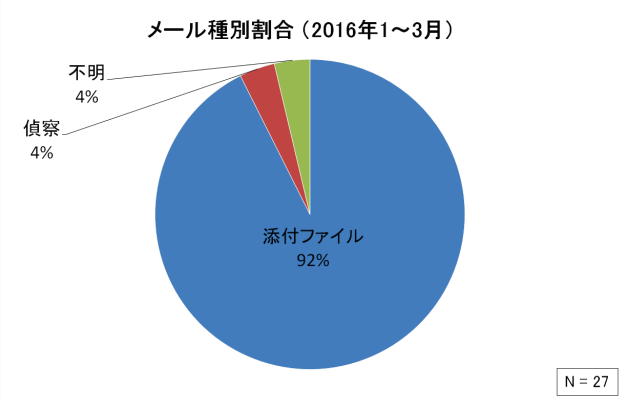

図 3　メール種別割合

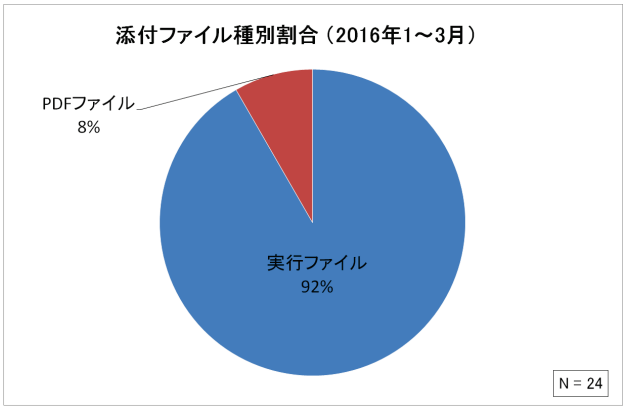

図 4　添付ファイル種別割合

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