サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2014 年 7 月～9 月]

2014 年 10 月 24 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、2014 年 7 月～9 月の運用状況は以下の通り。

本四半期、石油業界 SIG（7 組織）へ新たに 1 組織が参加し、更に、化学業界 SIG（8 組織）へ新たに 3 組織が参加することとなり、J-CSIP 全体での参加組織数は **50 組織**となった。

1 実施件数

2014 年 7 月～9 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（5 つの SIG、全 50 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	（2014 年 4 月～6 月）	（2014 年 1 月～3 月）	（2013 年 10 月～12 月）
1	IPA への情報提供件数	**100 件**	（259 件）	（95 件）	（121 件）
2	参加組織への情報共有実施件数	**52 件**※1	（59 件）	（40 件）	（51 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、広く無差別にばら撒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 13 件を含む。

本四半期では、前四半期（2014 年 4 月～6 月）に比べて情報提供件数が少なくなり、前年同期（2013 年 7 月～9 月）の 95 件と同程度の 100 件となった。前四半期は一過性のものと思われる同等の攻撃メールが集中して多数観測され、本四半期はそれが沈静化したことが主な要因である。

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。

- 2014 年 7 月～9 月に提供された情報 100 件のうち、標的型攻撃メールとみなして統計対象としたものは **79 件**である。
- メール送信元地域は、67%が不明であった（図 1）。そのほとんどは、メールヘッダにメールの発信元 IP アドレスが残らないフリーメールサービスが使われたことが原因である。
  - フリーメールサービスを悪用した標的型攻撃メールは依然として多い。組織内の利用者へ、フリーメールが危険であることを十分に周知するとともに、例えば、フリーメールサービスから送られたメールについては、その件名や本文に、メールの受信者へ警告するためのメッセージをメールサーバで追加し、要注意メールであることを知らせるような仕組みが有効である。

[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。
http://www.ipa.go.jp/security/J-CSIP/

- 不正接続先として攻撃者が悪用している地域は、アジア諸地域とアメリカが多数を占める傾向が継続している（図 2）。本四半期では、中国の IP アドレスを不正接続先とする同等のマルウェアが多く観測されたことから、中国が 49%と約半数を占めた。続いて、20%が日本国内のサーバが不正接続先として悪用されたと思われるものであった。このような場合、J-CSIP 事務局は外部機関と連携し、可能な範囲でサーバの停止等の調整を行っている。
- 攻撃メールの種別は、確認できた範囲のほぼ全て（79%）が添付ファイルによるものであった（図 3）。また、添付ファイルや URL リンクがなく無害だが、攻撃に関係していると思われるメール（「情報収集」に分類している）を 1%のみ観測した。
- 添付ファイル種別は、60%が「Office 文書ファイル」であり、全て修正プログラムが公開済みの脆弱性を悪用するものであった（図 4）。修正プログラムが適用されていないパソコンが組織内に残っていないよう徹底することが重要である。また、アイコンや拡張子を偽装し、利用者の錯誤を誘ってファイルを開かせる「実行ファイル」も多い。「ショートカット（lnk）ファイル」も、技術的な違いはあるが、手口としては「実行ファイル」と同様、利用者の錯誤を誘ってファイルを開かせるものである。これらの罠に騙されることがないよう、組織内の利用者への注意を徹底すべきである。

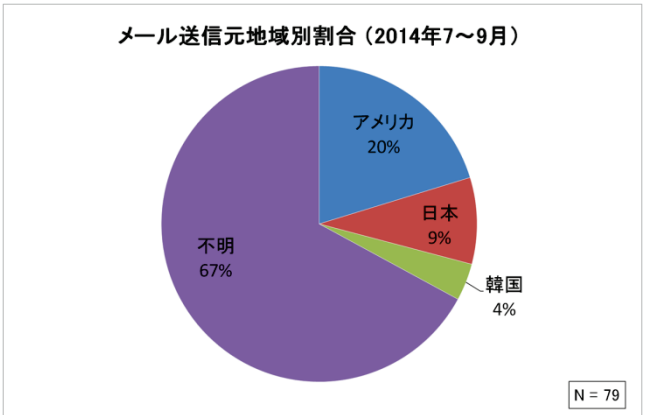

図 1　メール送信元地域別割合

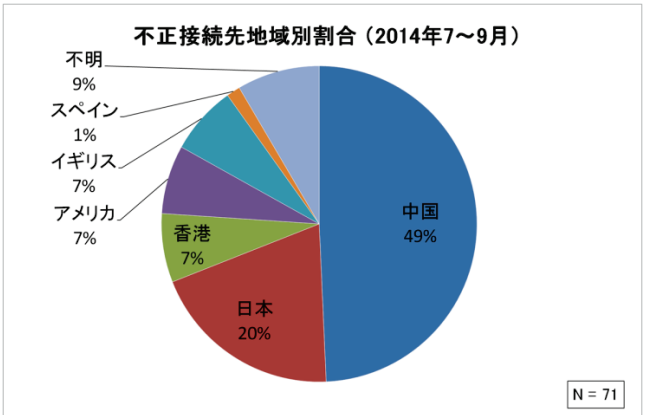

図 2　不正接続先地域別割合

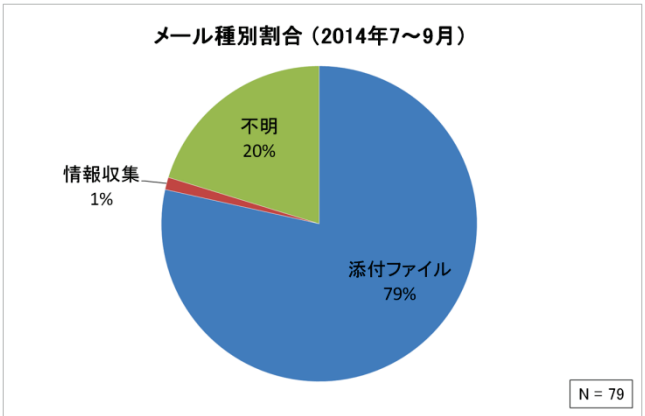

図 3　メール種別割合

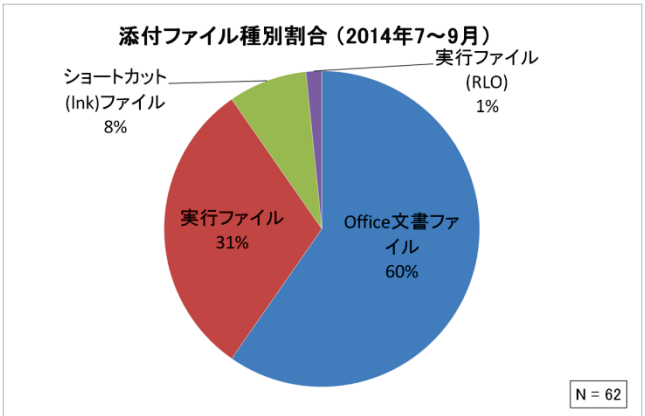

図 4　添付ファイル種別割合

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、広く無差別にばら撒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」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の特別相談窓口」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の特別相談窓口」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の特別相談窓口」（IPA）
http://www.ipa.go.jp/security/tokubetsu/

以上