サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2013 年 4 月～6 月]

2013 年 7 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、2013 年 4 月～6 月の運用状況は以下の通り。本四半期も、昨年度と同程度のペースで情報提供が行われ、IPAを経由した情報共有を実施した。

1 実施件数

2013 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	（2012 年 4 月～2013 年 3 月 1 年間の件数 [2]）
1	IPA への情報提供件数	**74 件**	（246 件）
2	参加組織への情報共有実施件数	**55 件** ※1	（160 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 件に集約して配付したり、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 5 件を含む。

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。

- 情報提供されたメール情報のうち、標的型攻撃メールとみなして統計対象としたものは 64 件である。
- 送信元地域別割合（図 1）、不正接続先地域別割合（図 2）について、2012 年度（2012 年 4 月～2013 年 3 月）と異なる偏りが見られるが、これは一時的なものであると推測する。全体の情報提供件数に対し、同一の攻撃者または攻撃グループによるものと思われる同等のメールが相対的に多数提供されたことが主な要因である。
- 攻撃には添付ファイルが使われることが多く（図 3）、また、その添付ファイルは約 8 割が実行ファイルであった（図 4）。これも一時的な偏りである可能性はあるが、攻撃者が、アプリケーションの脆弱性を狙うだけでなく、アイコンの偽装や拡張子の偽装によってメール受信者の錯誤を誘い、ウイルスに感染させる手口も依然として有効だと考えている可能性がある。
- この四半期においては、送信先メールアドレスの存在の確認等が目的と思われる「情報収集」に分類したメールも多く見られた（図 3）。

---

[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/

[2] 2012 年度（2012 年 4 月～2013 年 3 月）の件数や統計情報の詳細については、「サイバー情報共有イニシアティブ（J-CSIP）2012 年度 活動レポート」を参照のこと。
http://www.ipa.go.jp/files/000028304.pdf

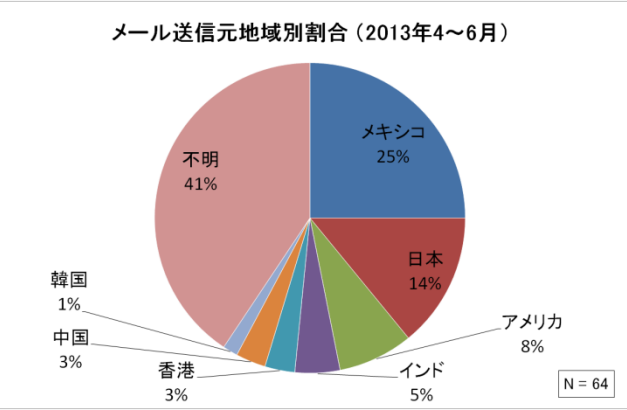


図 1　メール送信元地域別割合

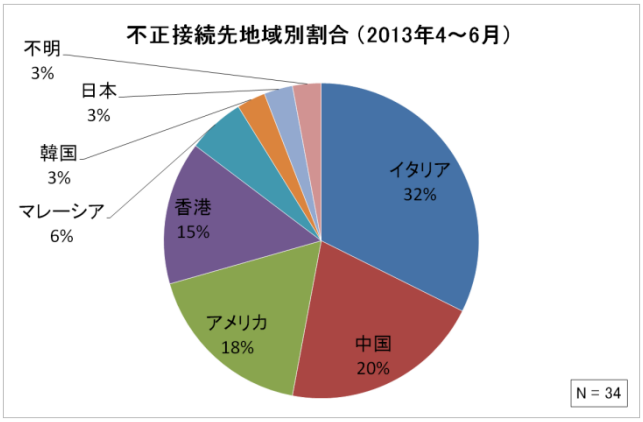


図 2　不正接続先地域別割合

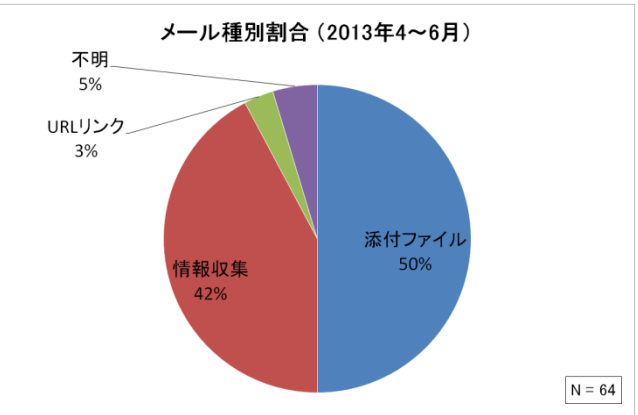


図 3　メール種別割合

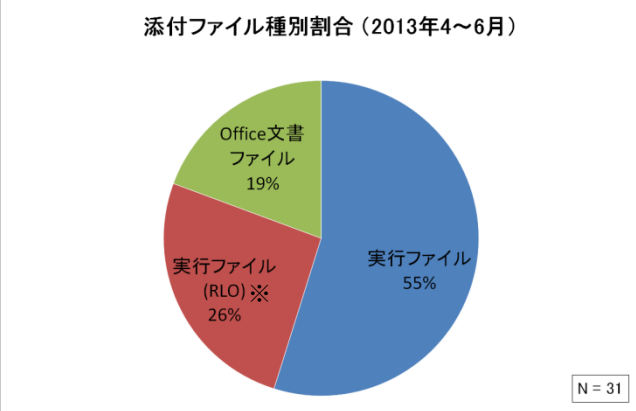


図 4　添付ファイル種別割合

※RLO：「Right-to-Left　Override」という、文字の表示上の並びを左右逆にする制御文字。RLO が悪用されファイルの拡張子の見た目が偽装されていたものを「実行ファイル（RLO）」としている。

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

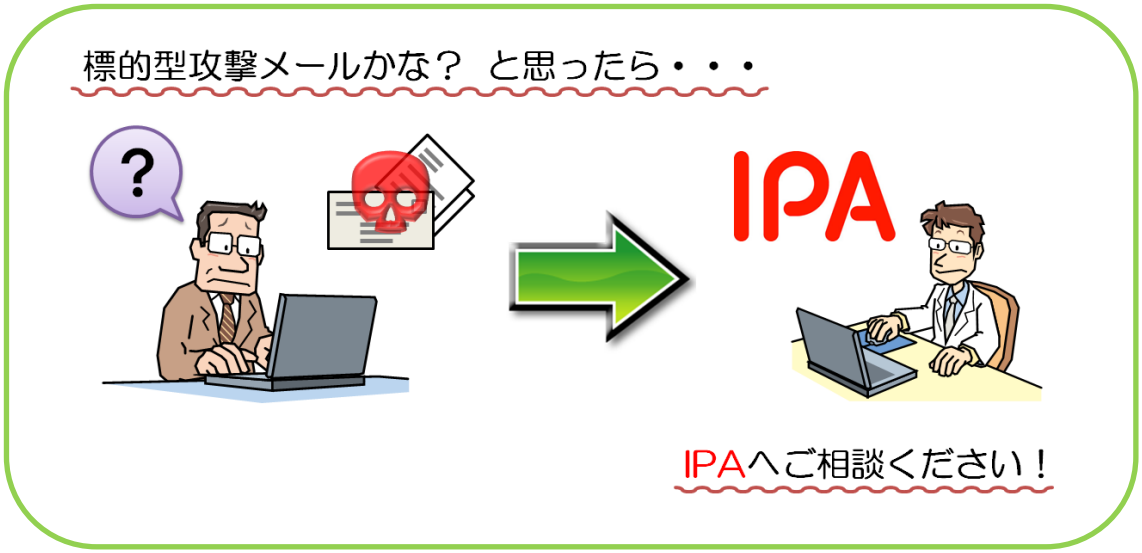
それぞれのグラフの基となっている母集団のサイズ N について、「IPA への情報提供件数」と異なっている理由を次に示す。

- 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