サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2014 年 1 月～3 月]

2014 年 4 月 25 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 1 月～3 月の運用状況は以下の通り。

本四半期、化学業界 SIG へ新たに 1 組織が参加した。これにより、化学業界 SIG の組織数は 8 組織となり、J-CSIP 全体での参加組織数は 46 組織となった。

1 実施件数

2014 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、その情報をもとにするなどして 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 46 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	（2013 年 10 月～12 月）	（2013 年 7 月～9 月）	（2013 年 4 月～6 月）
1	IPA への情報提供件数	**95 件**	（121 件）	（95 件）	（74 件）
2	参加組織への情報共有実施件数	**40 件**※1	（51 件）	（34 件）	（55 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場合や、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 J-CSIP 外から入手した情報で、J-CSIP 参加組織へ情報共有を行ったもの 4 件を含む。

また、2013 年度一年間の実施件数の合計を表 2 に示す。

表 2 2013 年度一年間の実施件数

項番	項目	件数 （昨年比）	（2012 年度）
1	IPA への情報提供件数	**385 件 （157%）**	（246 件）
2	参加組織への情報共有実施件数	**180 件 （113%）**	（160 件）
3	（参考） 提供された情報のうち、標的型攻撃メールと見なして統計対象とした件数	**233 件 （116%）**	（201 件）

- 各月や四半期ごとの情報提供等の数に波はあったが、通年で見た場合は、全体的な件数は一割強の増加となった。なお、参加組織の数は 2012 年度末時点で 39 組織、2013 年度末時点で 46 組織である。
- 情報提供件数については昨年度に比べ 1.5 倍以上の増加となった。不審なメールが実際にどのような脅威なのか、見た目だけでは判断が難しい。分析の上、結果的には広く無差別にばら撒かれたウイルスメールであろうと判断するものも多かったが、標的型攻撃メールか否か判断のつかないものについても、参加組織からは積極的な情報提供が行われるようになっている。IPA は全ての内容を確認し、見解を返答するとともに、情報を蓄積して活動に役立てている。

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

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 1 月～3 月に提供された情報 95 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 57 件である（2013 年 4 月～6 月は 64 件、7 月～9 月は 61 件、10 月～12 月は 51 件であった）。
- メール送信元や不正接続先に使用される IP アドレスは、これまで通り、アジア諸地域とアメリカに所属するものが多く観測されている（図 1、図 2）。なお、攻撃メールの送信元メールアドレスは、7 割以上がフリーメールサービスのものであり、ウェブメールを使用して送信された形跡が見られた。
- メール種別割合では、添付ファイルを開かせることによりウイルス感染を狙うものが多数を占めた（図 3）。メールデータが部分的にしか入手できず「不明」となっている 18%についても、そのほとんどに悪意のある添付ファイルが付いていたと思われる。
- 添付ファイルは、本四半期ではほぼ全てが実行ファイルかショートカット（LNK）ファイルであり（図 4）、利用者の錯誤を狙って開かせる（ダブルクリックさせる）ためのアイコン偽装などの仕掛けが施されていた。これらのファイルを開いてしまうリスクを低減するため、利用者への改めての注意喚起や、システム上の工夫（例えば、実行可能なファイルの拡張子が添付ファイル中に存在した場合、メールサーバで破棄・保留したり、メール本文中に警告を埋め込む等）を行うことが望ましい。

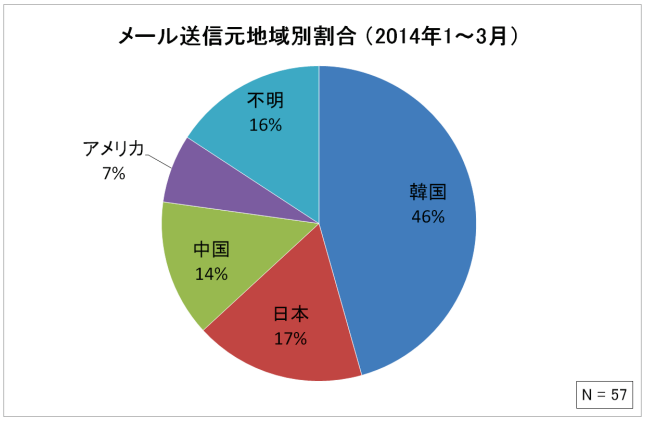


図 1　メール送信元地域別割合

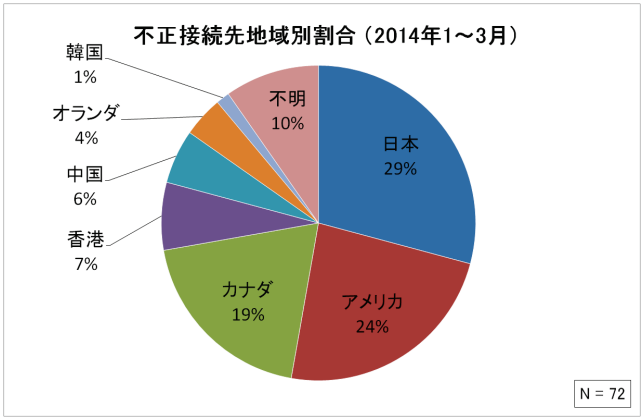


図 2　不正接続先地域別割合

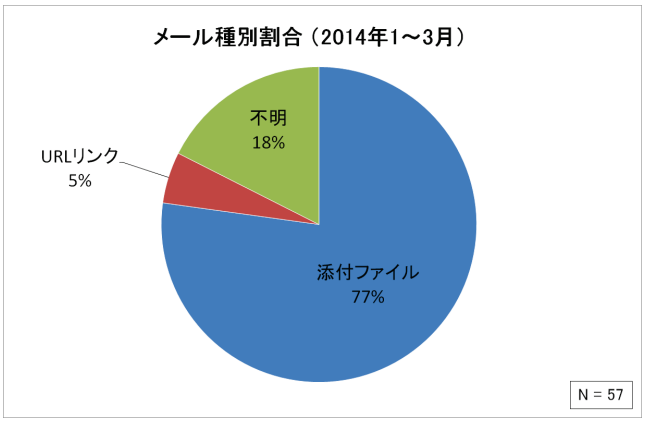


図 3　メール種別割合

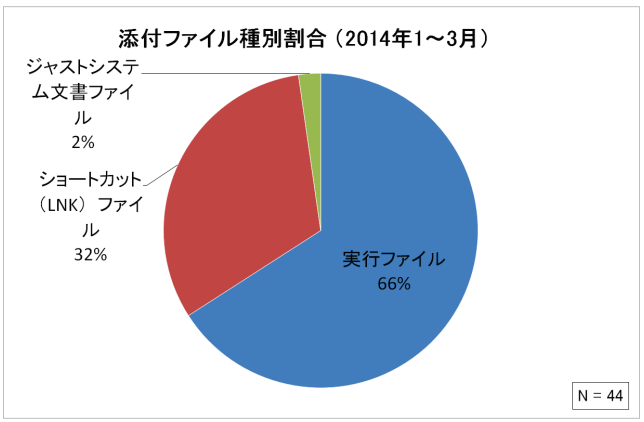


図 4　添付ファイル種別割合

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、時ととも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

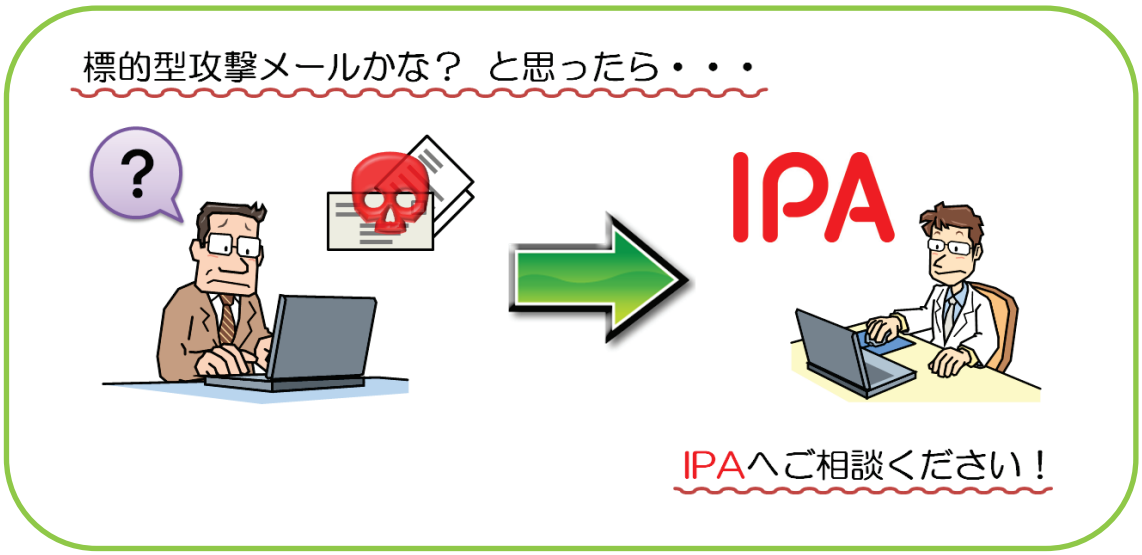
それぞれのグラフの基となっている母集団のサイズ N について、「IPA への情報提供件数」と異なっている理由を次に示す。

- 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）
https://www.ipa.go.jp/security/tokubetsu/



以上