

サイバー情報共有イニシアティブ(J-CSIP)¹について、2013年10月～12月の運用状況は以下の通り。

1 実施件数

2013年10月～12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45参加組織での合算)を、表1に示す。

情報提供件数が継続して増加傾向にあるが、これは主にIPAより「標的型攻撃メールであるか否か判断できないものでも情報提供を」と呼びかけているためであり、分析の結果、広く無差別にばら撒かれたウイルスメールと判断した件数も多くなっている。従って、情報共有実施件数には大きな変化は生じていない。

表1 情報提供および情報共有の状況

| 項番 | 項目 | 件数 | (2013年7月～9月) | (2013年4月～6月) |
|----|----------------|--------|--------------|--------------|
| 1 | IPAへの情報提供件数 | 121件 | (95件) | (74件) |
| 2 | 参加組織への情報共有実施件数 | 51件 ※1 | (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14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。

- 2013年10月～12月に提供された情報121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51件である(4月～6月は64件、7月～9月は61件であった)。
- メール送信元(図1)と不正接続先(図2)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ており、この傾向は従来から継続している。
- 攻撃メールの種別は、確認できた限りほとんど(78%)が添付ファイルによるものであった(図3)。
- 本四半期では、「ジャストシステム文書ファイル」(一太郎などジャストシステム社のオフィスソフトの文書ファイル)が攻撃に悪用された事例を観測し、かつ添付ファイル種別全体の約半数(47%)を占めた(図4)。本四半期中の2013年11月12日、ジャストシステム社が自社製品の脆弱性情報とアップデートモジュールを公開し、IPAからも注意喚起を行った²。これらの製品は主に日本国内で使用されており、過去にも国内組織を標的とした攻撃で観測されたことがある。脆弱性の情報は攻撃者にもすぐに知られるため、利用者においては、日頃の情報収集と迅速な修正プログラムの適用が必要である。

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/>

² 「一太郎」シリーズにおいて任意のコードが実行される脆弱性対策について(JVN#44999463) (IPA)

<https://www.ipa.go.jp/security/ciadr/vul/20131112-jvn.html>

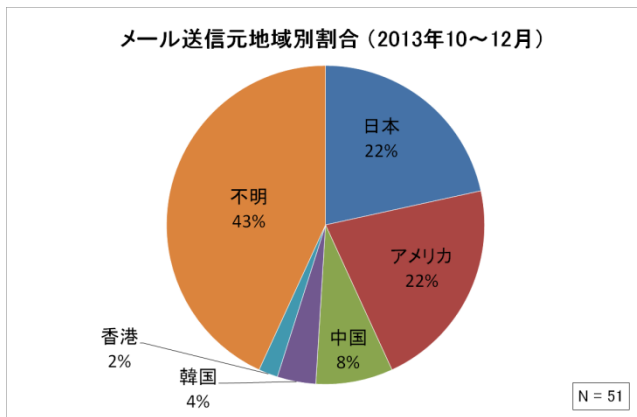


図 1 メール送信元地域別割合

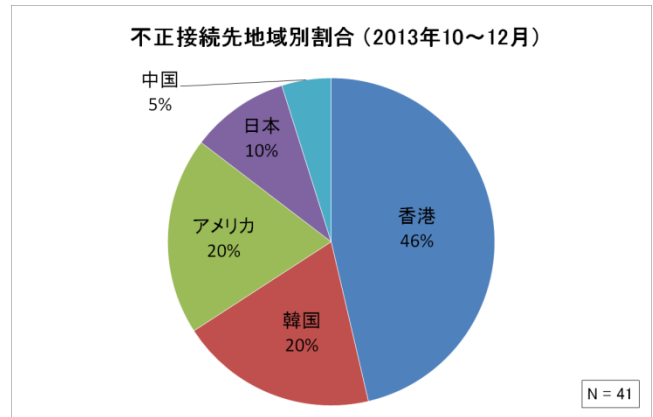


図 2 不正接続先地域別割合

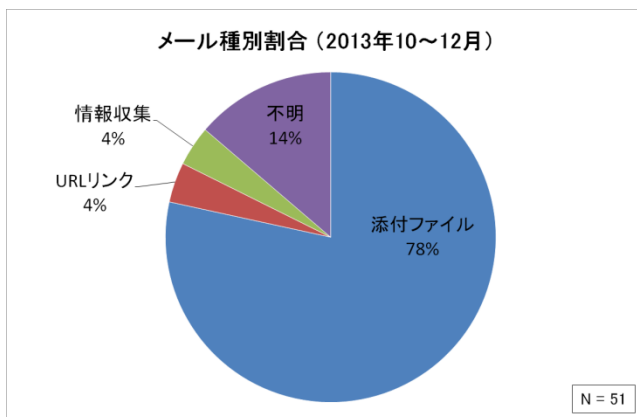


図 3 メール種別割合

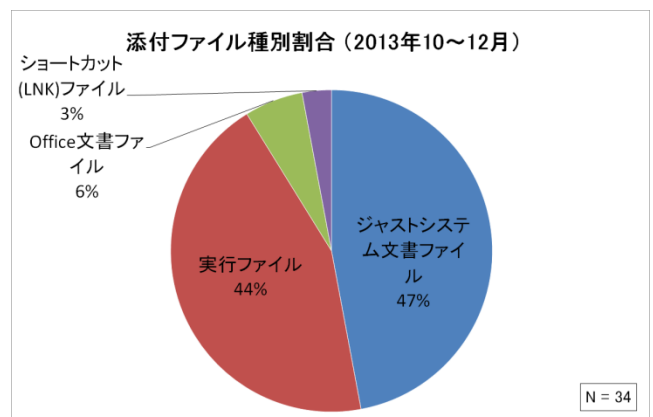


図 4 添付ファイル種別割合

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。

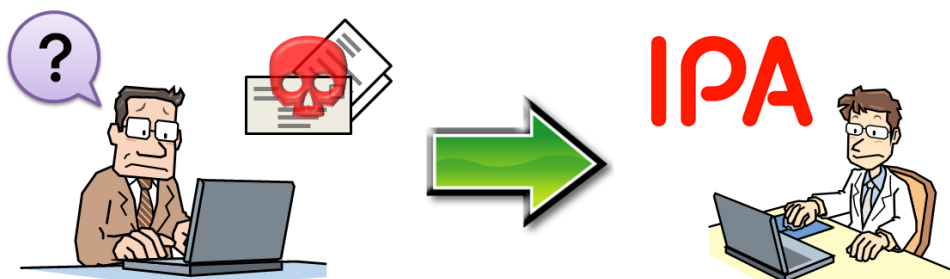
「標的型サイバー攻撃の特別相談窓口」への情報提供のお願い

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/>

標的型攻撃メールかな? と思ったら・・・



IPAへご相談ください!

以上