サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2015 年 4 月～6 月]

2015 年 7 月 31 日 （2015 年 9 月 4 日 一部改訂）
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、2015 年 4 月～6 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、化学業界 SIG（15 組織）へ新たに 2 組織が参加することとなり、J-CSIP 全体での参加組織数は 59 組織から **61 組織**となった。

1 実施件数

2015 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（6 つの SIG、全 61 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 1 月～3 月）	（2014 年 10 月～12 月）	（2014 年 7 月～9 月）
1	IPA への情報提供件数	**104 件**	（109 件）	（158 件）	（100 件）
2	参加組織への情報共有実施件数	**27 件**※1	（38 件）	（46 件）	（52 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 5 件を含む。

本四半期は、前四半期に続き、情報提供件数が 100 件程度となった。このうち、標的型攻撃メールとみなした情報は **28 件**である。

この 28 件とは別に、「.chm」形式ファイル（コンパイル済み HTML ヘルプファイル）が添付された不審メールを **30 件**確認した。これらについては、現時点では標的型攻撃メールとはみなさず、広くばら撒かれたであろうウイルスメールとして取り扱っている。メールには、ウイルスに感染させる「.chm」形式ファイル、またはそれを圧縮したファイルが添付されていた。「.chm」形式ファイルを悪用する事例は、J-CSIP では初めて確認するものであった。「.chm」形式のファイルを開いた場合、そこに仕込まれた任意のスクリプト（プログラム）が実行されてしまうため、その危険性は実行ファイルと同等である。通常の業務では授受しない形式のファイルであるため、この拡張子のファイルを受信した場合は隔離するといった対策が有効である。また、30 件のメールの中には、件名が「Amazon.co.jp」となっており、Amazon 社からの連絡のように見せかけているものもあった。ある程度広範囲に、国内の利用者を対象としてウイルス感染を試みたものと推測しており、引き続き注視していく。

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、2015 年 4 月～6 月に提供された情報 104 件のうち、標的型攻撃メールとみなした **28 件**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。
https://www.ipa.go.jp/security/J-CSIP/

- メール送信元地域（図 1）で「不明」が 78%を占める主な要因は、メールの送信元 IP アドレスがメールヘッダに残らないメールサービスが使われたためである。攻撃者が、メールに痕跡の残りにくいサービスを使うようになってきている可能性がある。
- 不正接続先地域（図 2）は、「日本」が 37%と前四半期と同じ高い割合を占める結果となり、国内のマシンが攻撃者により乗っ取られるなどして悪用されていると思われる状況が続いた。
- メールの種別（図 3）は、「添付ファイル」が 68%を占める結果となった。「不明」の 18%は、添付ファイルが付いていたが、セキュリティ製品により無害化（削除）されたと思われるものであった。このため、添付ファイルは実質 86%を占めていたことになる（添付ファイルそのものを入手・確認できていないため、統計上は「不明」としている）。
- 添付ファイル種別（図 4）は、全てが「実行ファイル」であり、これらは全て圧縮された状態（.zip、.lzh など）で添付されていた。また、メールの配送経路でのウイルス検知機能の回避が目的と思われる、「パスワード付きの圧縮ファイル」が約 6 割を占めた。パスワード付き圧縮ファイルは日常的に使用するものであるが、配送経路でのウイルスチェックが行われない状態で利用者の手元に届くため、リスクがあるということを、利用者において改めて認識いただきたい。

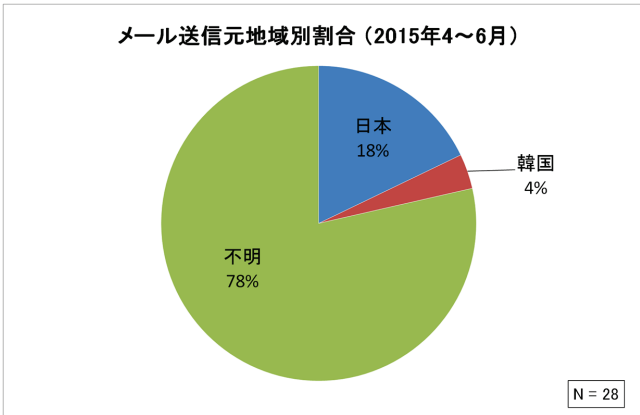

図 1　メール送信元地域別割合

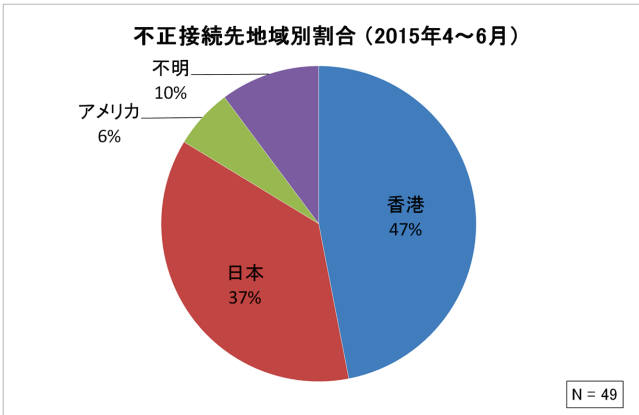

図 2　不正接続先地域別割合

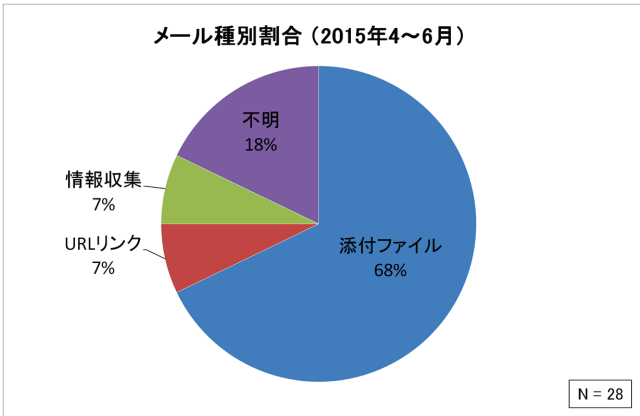

図 3　メール種別割合

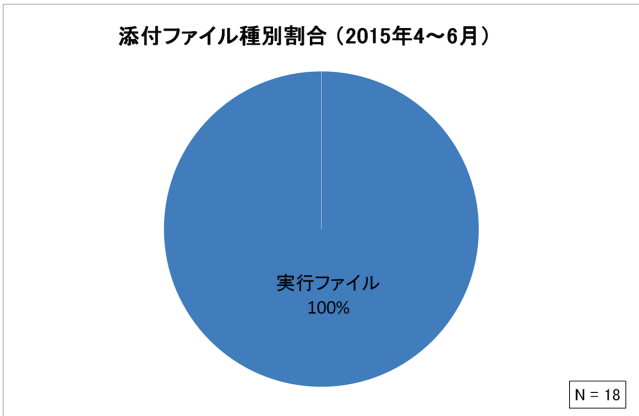

図 4　添付ファイル種別割合

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

改訂履歴

2015 年 7 月 31 日　　初版公開。
2015 年 9 月 4 日　　集計の誤りを確認したため、「表 1 情報提供および情報共有の状況」について、本四半期の「参加組織への情報共有実施件数」を 28 件から 27 件へ訂正。

以上