サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2015 年 1 月～3 月]

2015 年 4 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、2015 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。更に、2015 年 3 月、新たに原油鉱業分野および天然ガス鉱業分野の 2 つの産業分野を擁する SIG として「資源開発業界 SIG」（参加組織数 5 組織）が発足し、J-CSIP 全体で **6 つの SIG**、参加組織数は **59 組織**となった。

1 実施件数

2015 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 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 59 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 10 月～12 月）	（2014 年 7 月～9 月）	（2014 年 4 月～6 月）
1	IPA への情報提供件数	**109 件**	（158 件）	（100 件）	（259 件）
2	参加組織への情報共有実施件数	**38 件**※1	（46 件）	（52 件）	（59 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 17 件を含む。

本四半期は、比較的実施件数が少なく、2012 年度～2013 年度と同等レベルであった。とはいえ、注意を要する標的型攻撃メールは継続して観測されており、けして楽観できる状況というわけではない。

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。

- 2015 年 1 月～3 月に提供された情報 109 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。
- 本四半期では、**全体の 91%**の攻撃メールが**国内のフリーメールサービス**を使って送られていた。送信元メールアドレスの末尾が「.jp」であっても、そのメールの安全性を判断する材料にはならないと考えるべき状況である。
- メール送信元地域（図 1）で「不明」が 44%を占めている主な要因は、メールの送信元 IP アドレスがメールヘッダに残らないフリーメールサービスが使われたためである。
- 不正接続先地域（図 2）は、「アメリカ」と「日本」の割合が高い傾向が前四半期より続いており、この 2 つの地域のみで 97%を占める結果となった。「日本」については、国内のマシンが攻撃者により乗っ取

[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/

られるなどして悪用されているものと思われる。ウイルスによる不正な通信と、業務上発生している正常な通信を見分けることは、ますます難しくなっている。

- メールの種別（図 3）は時期による変化が大きい。前四半期で半数を占めた「URL リンク」は本四半期では 1 件も観測されず、「添付ファイル」が約半数を占める結果となった。なお、56%の「不明」のほとんどについても、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（添付ファイルそのものが入手できていないため、統計上は「不明」としている）。
- 添付ファイル種別（図 4）については、脆弱性を悪用することなくウイルスを感染させる「実行ファイル」が 87%を占めた。添付ファイルを開く前にファイルの種別を確認したり、アイコンや拡張子の偽装を見抜くことができれば、この攻撃は必ず避けることができる。攻撃の手口（ファイルの偽装の手口）について、職員一人一人への一層の注意の徹底が望ましい。

  また、13%を占める「Office 文書ファイル」では、4 件中 3 件が**マクロ機能を悪用するもの**であった。ファイルを開いた際、マクロの実行を無条件に許可する設定となっていたり、表示された警告メッセージに対してマクロ実行を許可するボタンをクリックしたりすると、ウイルスに感染させられてしまう。マクロ機能の悪用による標的型攻撃の手口は、J-CSIP では前四半期から確認されている。Office 文書ファイルを開き警告が表示された時、マクロの実行を許可しなければ、この被害は避けることができる。マクロ機能を有効にすることの危険性についても、職員一人一人への徹底が望ましい。

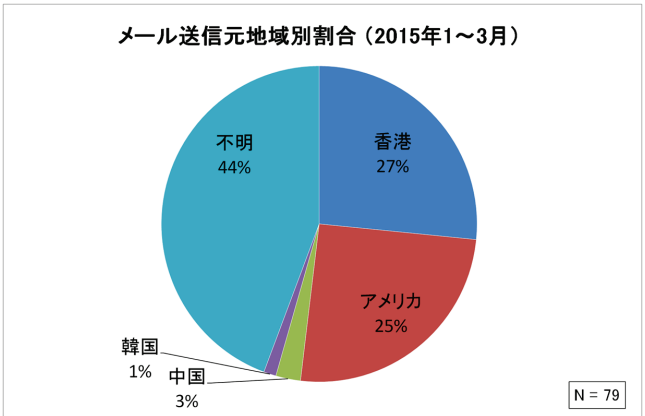

図 1　メール送信元地域別割合

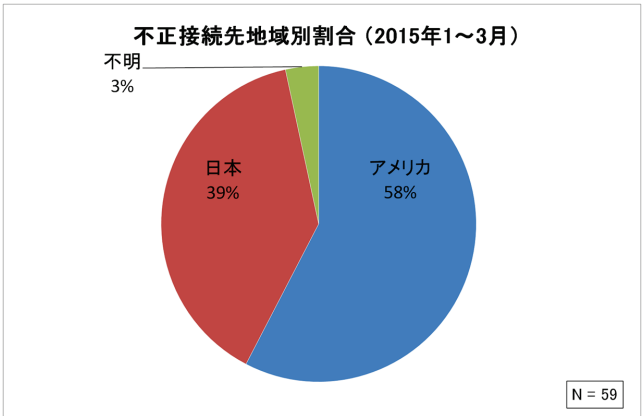

図 2　不正接続先地域別割合

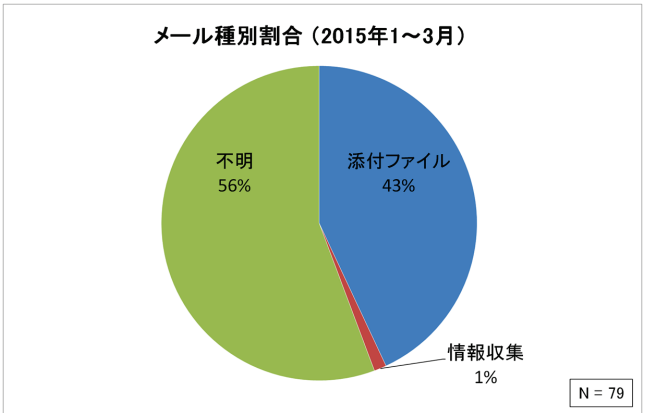

図 3　メール種別割合

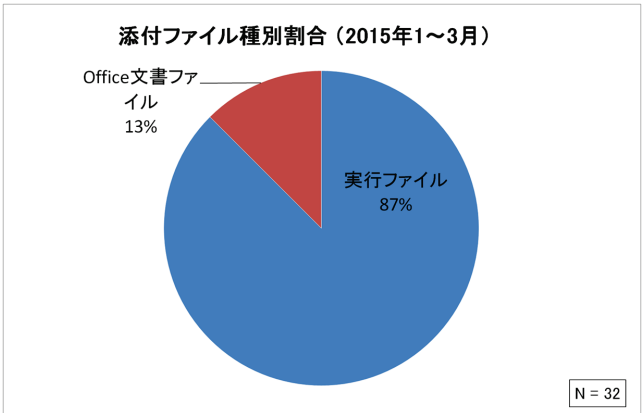

図 4　添付ファイル種別割合

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（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/

以上