サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2015 年 10 月～12 月]

2016 年 1 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、2015 年 10 月～12 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（17 組織）へ新たに 1 組織が参加することとなり、J-CSIP 全体での参加組織数は 61 組織から **62 組織**となった。

1 実施件数

2015 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、それらの情報をもとに 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 62 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 7 月～9 月）	（2015 年 4 月～6 月）	（2015 年 1 月～3 月）
1	IPA への情報提供件数	**723 件**	（88 件）	（104 件）	（109 件）
2	参加組織への情報共有実施件数	**34 件**※1	（33 件）	（27 件）	（38 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 12 件を含む。

本四半期は情報提供件数が **723 件**、前期の約 8 倍と急増した。情報提供件数が増えた主な要因は次の二点である。なお、この二点による情報提供を一過性のものとして仮に差し引いた場合、残る情報提供件数は **91 件**となり、前四半期までと同程度の状況といえる。

一つ目の要因は、10 月と 12 月に、件名・本文・添付ファイル名の一部または全部に日本語が使われ、広くばらまかれたウイルス付きメール（以下、「ばらまき型メール」と呼ぶ）が大量に確認されたことである。これらに関する情報提供は **466 件**と、情報提供件数の **64%**を占めた。

二つ目の要因は、IPA で確認した結果、ウイルスとは関係のない、無害（本物のメール）あるいは広告等のスパムメールの情報であろうと見なしたものが **166 件**（情報提供数の **23%**）あったことである。J-CSIP では、参加組織において不審か否か判断に困った場合は、念のため情報提供いただくよう呼びかけている。これまでもこの種の情報提供は月に数件程度あったが、本四半期はこれが一時的に多く発生した。

最終的に、情報提供 723 件のうち、標的型攻撃メールとみなした情報は **19 件**であった。これらは次に挙げるような注意を要する特徴が見られた。

- zip 形式の添付ファイルは、本四半期で確認したものは全て暗号化されていた（圧縮パスワードが設定されていた）。これは、メールの配送経路でのウイルス検査等を避けるためと思われる。
- J-CSIP で過去に観測例がないウイルスを観測した。このウイルスは添付ファイルによって感染させられる遠隔操作ウイルスの一種であった。

[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/

また、2014 年の 3 月から 6 月に一時的に観測し、その後観測されていなかった遠隔操作ウイルスの“バージョンアップ版”が使われた事例が 1 件あった。

- Office 文書ファイルを使ってウイルスに感染させる手口として、ゼロデイ攻撃[2]ではなかったが、数ヶ月前に修正されたばかりの脆弱性を悪用するものがあった。当該脆弱性の悪用手口は、J-CSIP で過去に観測したことのないものであり、攻撃者が新たな攻撃手法を継続的に取り入れていることを示している。
- 19 件のうち、差出人(From)メールアドレスの情報が得られたものは 13 件であったが、これらにおいて全て日本国内のドメインのメールアドレスが使われていた(フリーメール 9 件、その他 4 件)。
- メールの送信元とウイルスの不正接続先、ともに日本国内の IP アドレスの件数がトップとなり、攻撃インフラ(攻撃者がサイバー攻撃に使用する基盤)が国内に築かれている様子がうかがえた。

2015 年初頭より、標的型攻撃メールを観測している件数自体は少なくなっているが、これらの点により、状況は引き続き予断を許さないと考えられる。

「ばらまき型メール」について

本四半期、国内で多く観測されていた、日本語が使われた「ばらまき型メール」を、J-CSIP においても 10 月と 12 月に大きく 2 回に分けて観測した。

10 月に観測したものは、IPA が 10 月 9 日から 10 月 30 日にかけて注意喚起を行った[3]一連のばらまき型メールであり、“特定の組織からの注文連絡”や“複合機からの自動送信”、あるいは“請求書”を装ったもので、合計 **108 件**の情報提供があった。

12 月からは、ロシアの「Rambler Mail」というサービスで取得できるメールアドレスから、“日本郵政等を騙るメール”[4]や、“負債通知”、“DHL”、“税務署から”等の件名のウイルスメールがばらまかれたことを確認しており、合計 **358 件**の情報提供があった。

これらはいずれも、着信した業界等に偏りは見られず、広く無差別に送信されているようであった。現時点、J-CSIP においては、これらを「標的型攻撃メール」とは見なしていないが、危険なウイルスメールではあるため、情報共有を行っている。その結果、多数の組織から関連情報が寄せられ、ごく一部ではあるが、「Rambler Mail」以外に、「163.com」(中国)、「YAHOO!」(アメリカ)、「Jubii」(デンマーク)といったサービスで取得できるメールアドレスからも、同じウイルスメールがばらまかれていたことが分かった。

2016 年に入ってからも、「Rambler Mail」のメールアドレスから、新たな件名や本文を使ったばらまき型メールを確認している。この傾向は今後も続くとみられ、引き続き注意が必要である。

---

[2] 脆弱性(ウイルス感染等に悪用される可能性のあるソフトウェア上の欠陥)の修正プログラムが開発者から提供(公開)される前に行われる、当該脆弱性を悪用する攻撃。

[3] 「【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意」(IPA)
https://www.ipa.go.jp/security/topics/alert271009.html

[4] 「「JAPAN POST ジャパン」や「日本郵政」等を名乗って小包の配達を装った不審メールにご注意ください」(日本郵政)
http://www.japanpost.jp/information/2015/20151214114758.html

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 10 月～12 月に提供された情報 723 件のうち、標的型攻撃メールとみなした **19 件**である。

- メール送信元地域（図 1）は、前四半期と同じく「日本」が最多であり、他もアジアに集中している。また、複数の地域から同種の攻撃メールが送信された事例も観測された。攻撃者は複数の手段（乗っ取ったマシンの悪用やクラウドサービスの使用等）で攻撃メールを送信していると考えられる。
- 不正接続先地域（図 2）は、「日本」が半数を占め最多となった。国内の IP アドレスへのアクセスであっても、リスクが低いとは言えない状況が続いている。
- メールの種別（図 3）は、本四半期も「添付ファイル」が 58%と最も高い比率となった。
- 添付ファイル種別（図 4）は、実行ファイル（「実行ファイル」および「実行ファイル（RLO）」）が多く見られ、かつ、これらの実行ファイルは、ウイルス検査を避けることが目的と思われるが、全て暗号化（パスワード付き）zip 形式ファイルとしてメールに添付されていた。
  zip 形式ファイルは、パスワードが設定されていても、展開後のファイル名を確認することができる。メールサーバ等で、実行ファイルの拡張子のファイルが含まれる zip 形式ファイルについて、排除したり配送を保留する対策を行っている組織では、これらの攻撃メールのリスクを下げることができている。
- 「Office 文書ファイル」は、マクロを悪用する手口と、前述のとおり、数ヶ月前に修正されたばかりの脆弱性の悪用を伴う手口が使われていた。マクロを安易に有効化しないこと、修正プログラムを確実に適用することが、引き続き重要である。

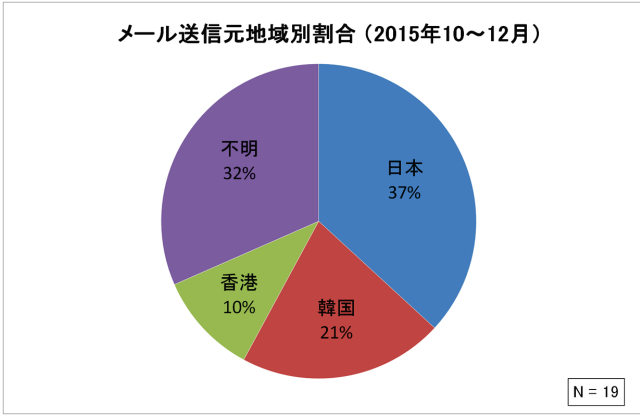

図 1　メール送信元地域別割合

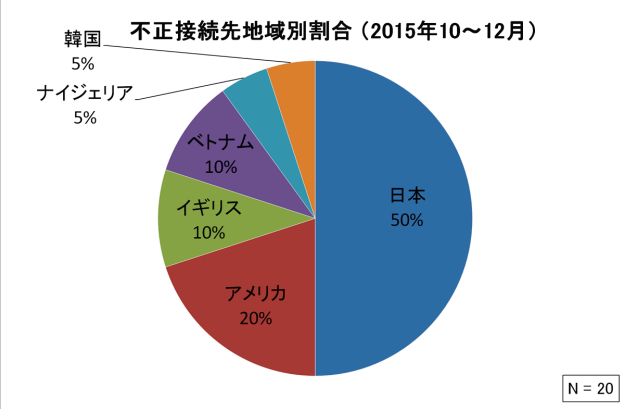

図 2　不正接続先地域別割合

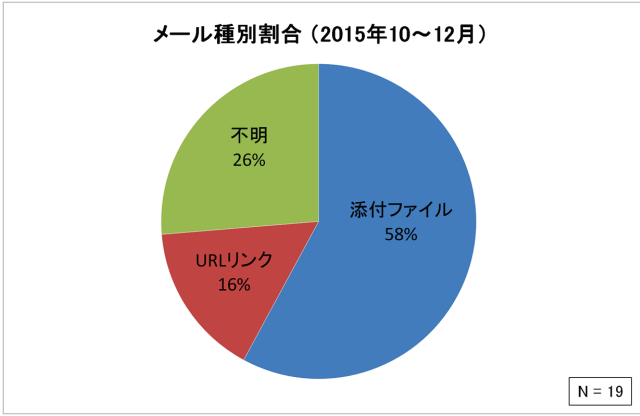

図 3　メール種別割合

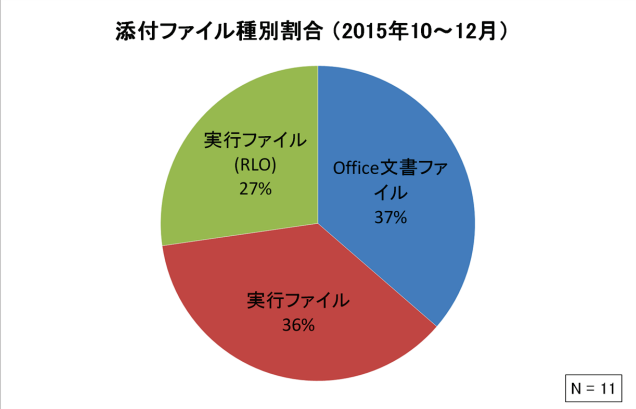

図 4　添付ファイル種別割合

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特別相談窓口」（IPA）
https://www.ipa.go.jp/security/tokubetsu/

以上