サイバー情報共有イニシアティブ（J-CSIP） 運用状況
[2015 年 7 月～9 月]

2015 年 10 月 23 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 7 月～9 月の運用状況は以下の通り。

1 実施件数

2015 年 7 月～9 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 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 4 月～6 月）	（2015 年 1 月～3 月）	（2014 年 10 月～12 月）
1	IPA への情報提供件数	**88 件**	（104 件）	（109 件）	（158 件）
2	参加組織への情報共有実施件数	**33 件**※1	（27 件）	（38 件）	（46 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。

本四半期は情報提供件数が 88 件、うち標的型攻撃メールとみなした情報は **23 件**であった。件数は全体的に減少傾向にあるが、メールの文面等の騙しの手口は巧妙なものがみられ、添付ファイルについても前四半期に比べ多様な手口を観測しており（詳しくは「2 統計情報」に示す）、予断を許さない状況である。

また、本四半期は不審なウェブサイトの URL や、プロキシサーバの不審なアクセスログ等の情報提供が 88 件中 **20 件**と多くみられた。これらの情報をもとに、改ざんされ、攻撃サイトとなっていたウェブサイトの URL、ドライブバイダウンロード攻撃によって感染が試みられるウイルス、更にそのウイルスの不正接続先といった情報の共有を行い、参加組織における対策や被害の有無の迅速な確認に繋げることができた。

本四半期に観測したドライブバイダウンロード攻撃では、Adobe Flash Player の脆弱性を悪用し、標的型攻撃で使われる遠隔操作ウイルスに感染させる手口がみられた。一部は修正プログラムが公開された日の直後に攻撃サイトの存在が観測されており、暫定回避策（Flash Player の無効化等）や修正プログラムの迅速な適用を行っていなければ、被害に繋がる可能性があるものであった。また、正規のウェブサイトのバナー広告が、ウイルス感染を試みるものに差し替わっていた（**マルバタイジング**、悪意のある広告による攻撃）と思われる痕跡も一部確認した。標的型攻撃に限らず、**ブラウザやプラグインの脆弱性を悪用する攻撃は今後も悪質化が続くと考えられ**、より一層の注意が必要である。

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 7 月～9 月に提供された情報 88 件のうち、標的型攻撃メールとみなした **23 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）は、これまでと変わらずアジア地域が多く、前四半期と同じく「日本」が最多となっている。
- 不正接続先地域（図 2）について、「スーダン」が観測されたのは初めてであったが、遠隔操作ウイルスの種類としては既知（過去に確認されたもの）であった。同様に、「韓国」「日本」が不正接続先となっていた遠隔操作ウイルスも、既知のものであった。
- メールの種別（図 3）は、本四半期も「添付ファイル」が 48%と最も高い比率となった。
- 添付ファイル種別（図 4）は、前四半期が「実行ファイル」のみであったのに比較し、本四半期は多種のファイルによるウイルス感染手口を観測した。
  まず、1 位の「ショートカット（lnk）」（39%）は、ショートカットファイルに仕込むスクリプトとして、JavaScript と VBScript が使用されているものを確認。それぞれ感染させられるウイルスも異なるものであった。
  2 位の「Office 文書ファイル」（31%）では、Adobe Flash Player の脆弱性を悪用する Flash オブジェクトを Office 文書ファイルに埋め込み、ウイルス感染を試みる手口と、マクロを悪用する手口を確認した。いずれも、Office 文書ファイルを攻撃に使いながらも、Office 自体の脆弱性は悪用しない手口である。
  3 位の「実行ファイル（RLO）」は、ファイルの拡張子を偽装する仕掛けが施されたものである。
- 以上のように、本四半期は、ドライブバイダウンロード攻撃に加え、様々な種類の添付ファイルの攻撃手口を観測した。これらについては、基本的な対策、すなわち （1）修正プログラムを迅速に適用する、（2）開く前にファイル種別を確認する、（3）マクロを不用意に有効化しない、といった対策により、攻撃による被害を回避、もしくは低減することができる。改めて、基本的な対策の徹底をお願いしたい。

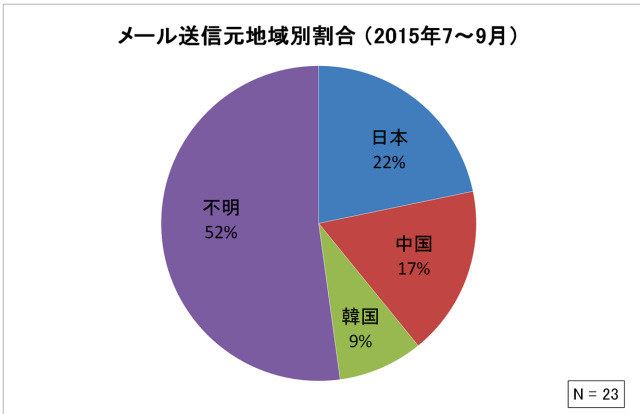

図 1　メール送信元地域別割合

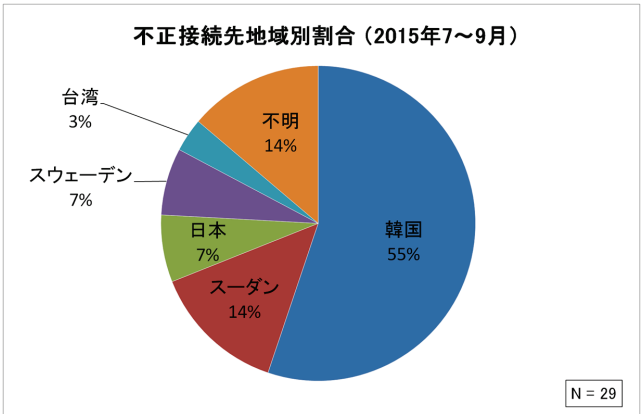

図 2　不正接続先地域別割合

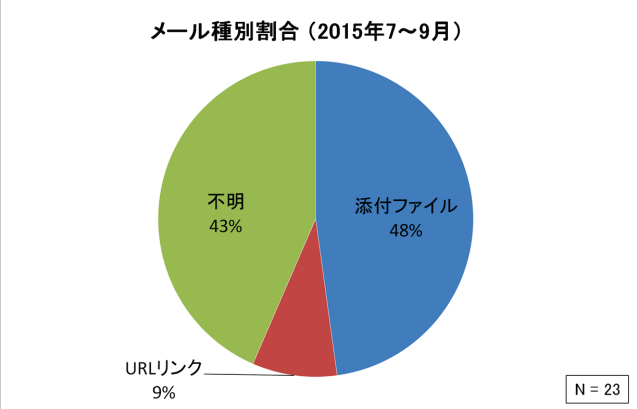

図 3　メール種別割合

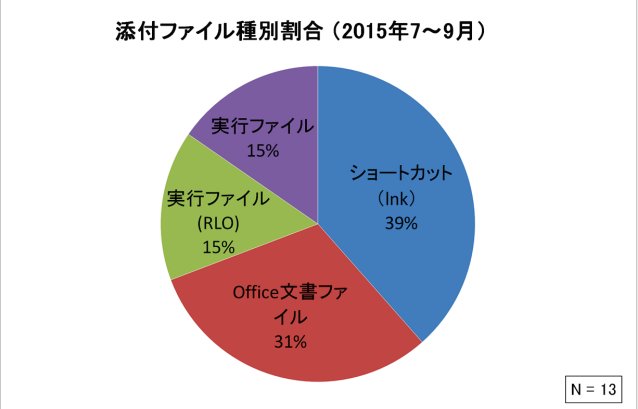

図 4　添付ファイル種別割合

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