# サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2016 年 7 月～9 月]

2016 年 10 月 28 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、2016 年 7 月～9 月の運用状況は以下の通り。

本四半期、11 組織で構成していたガス業界 SIG へ 15 組織が新たに参加し、合計 26 組織となった。これにより、J-CSIP 全体での参加組織数は 72 組織から **87 組織**となった。

また、J-CSIP 内の一部において、STIX（脅威情報構造化記述形式）[2]の試行的な利用の取り組みを開始した。サイバー攻撃や被害の兆候を示す情報、例えば、J-CSIP で現在共有を進めている、標的型攻撃メール等の送信元メールアドレスや、ウイルスの不正接続先ホスト名、IP アドレスといった情報は、インジケータ（検知指標）と呼ばれる。STIX は、これらの情報を標準的に、かつ機械処理（自動処理）が可能な形式で表記する仕様の一つである。

## 1 実施件数

2016 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（7 つの SIG、全 87 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 | 2015 年 | **2016 年** | | |
|---|---|---|---|---|---|
| | | 10 月～12 月 | 1 月～3 月 | 4 月～6 月 | **7 月～9 月** |
| 1 | IPA への情報提供件数 | 723 件 | 177 件 | 1,818 件 | **218 件** |
| 2 | 参加組織への情報共有実施件数 | 34 件 | 39 件 | 33 件 | **32 件**※1 |

※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、広く無差別にばらま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 **4 件**を含む。

本四半期は情報提供件数が **218 件**であった。件数は前四半期と比べ大幅に減少しているが、前四半期の情報提供 1,818 件のうち、1,584 件は、一時的に提供件数が急増した「ばらまき型メール」の情報であったため、実質的な変動はさほど大きくはない。なお、本四半期においても「ばらまき型メール」の情報提供は継続しており、注意を要する状況である。

本四半期の 218 件の情報提供のうち、標的型攻撃メールとみなした情報は **123 件**であった。2015 年 4 月以降、標的型攻撃メールの提供は四半期あたり 20～30 件程度を推移していたが、本四半期はこれを大きく上回る件数となった。2012 年 4 月の J-CSIP における情報共有の運用開始以来、四半期で 100 件を超える標的型攻撃メールを観測したのは、これが 3 回目である。

---

[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/

[2] 脅威情報構造化記述形式 STIX 概説 （IPA）
https://www.ipa.go.jp/security/vuln/STIX.html

本紙の執筆時点で確認できている限り、本四半期に観測された標的型攻撃メールは、数件を除き、ほぼ全てについて、J-CSIP 2014 年度の活動レポート[3]で述べた攻撃者「X」との関連性が見られるものであった。IPA では、攻撃者「X」による攻撃が再び活発化したものか、少なくとも何らかの関係がある事象と推定している。

これら攻撃メールについては、次に挙げるような特徴があった。

- 添付された rar 形式の圧縮ファイルにパスワードが設定されており、ファイルが添付されていたメールの本文中に解凍パスワードが記載されている事例があった。
- 攻撃者のミスであるのか、理由は不明だが、同様にメールの本文中に解凍パスワードが示されていながら、パスワードが設定されていない zip 形式の圧縮ファイルが添付されていた事例があった。
- 実行形式ファイルのほか、悪意のある Office 文書ファイルが添付ファイルとして用いられることもあり、マクロ機能を悪用するものと、昨年修正された Office の脆弱性を悪用するものがあった。
  前者のマクロ機能の悪用については、以前から用いられていた攻撃手口であり、組織外からもたらされた Office 文書ファイルについて、安易にマクロ機能を有効化しないよう注意することで対応できる。
  後者については、修正プログラムにより攻撃を防ぐことができるため、Office に限らずソフトウェアを確実に最新の状態とする運用が重要である。
- 123 件のうち、**118 件**のメールについて、日本国内のドメインの、フリーメールサービスのメールアドレスが使用されていた。フリーメールは攻撃に悪用されることが多く、フリーメールからのメールを受信した場合、メールサーバにて件名や本文に警告を付与し、受信者に注意を促すといった対策を勧める。

## 2 J-CSIP 外への注意喚起等の実施状況

J-CSIP の活動の中で、例えば、IPA へ提供された情報から、J-CSIP 外（J-CSIP に参加していない組織）に対して、何らかの攻撃が行われた可能性を示す痕跡が得られることがある。そのような場合、可能な範囲で、当該組織等に対し注意喚起のための連絡を行っている。

本四半期は、J-CSIP 外への注意喚起に至った件数がこれまでになく多く、J-CSIP で把握したものと同等の標的型攻撃メールが着信していると考えられた **21 組織**へ、のべ **31 回**の注意喚起を行った。その結果、これらの組織に対して**合計 53 通**の標的型攻撃メールの送信が試みられたことを確認したと同時に、攻撃対象となった組織における対応を促すことができた[4]。また、注意喚起先の組織より、J-CSIP で把握していなかった攻撃メールの情報が得られ、そこから更に別の組織への注意喚起や情報共有に結びついた事例もあった。

これら 21 の組織の内訳は、製鉄・金属加工・制御機械・プラント・建設関連等、市場で高いシェアを誇る企業が 8 社、大学 7 校、研究機関等 2 組織、その他 4 組織であった。現在把握できている攻撃は氷山の一角かもしれないが、共通点として、R&D（研究開発）に積極的な国内組織が標的になっているものと見受けられ、今後とも注意が必要ではないかと思われる。

なお、IPA からの注意喚起の際、組織内に CSIRT やそれに準ずる体制があり、連絡が迅速に実施できたケースばかりではなく、本件のような連絡に対応可能と思われる部門の担当者に繋がるまでに時間を要したケースも、少なからず発生している。各組織においては、情報セキュリティに関する連絡が外部からもたらされた場合に、どの部門が窓口となるか、また、組織内の連絡経路等を定めておくことが望ましい。

---

[3] サイバー情報共有イニシアティブ（J-CSIP） 2014 年度 活動レポート レポート別冊 （IPA）
https://www.ipa.go.jp/files/000046019.pdf

[4] 攻撃者からメールの送信（攻撃）が試みられたことはメールサーバのログ等から確認できたが、当該メールアドレスが既に存在しなかったといった理由により、利用者のメール受信まで至らなかった例を含む。

## 3　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、2016 年 7 月～9 月に提供された情報 **218 件**のうち、標的型攻撃メールとみなした **123 件**である。

- メール送信元地域（図 1）は、「韓国」が 20%以上を占めており、次いで「香港」、「中国」を確認した。60%以上を占めている「不明」は、標的型攻撃メールと思われるメールの着信は確認できたが、断片的な情報しか確保できなかったため、メール送信元まで確認できなかったものである。
- 不正接続先地域（図 2）は、「アメリカ」が 80%以上を占めている。本四半期で確認したウイルスの多くが、同一の IP アドレスを不正接続先としていたことから、このような偏りが生じている。
- メール種別割合（図 3）も、メール送信元地域（図 1）と同様の理由で、「不明」の割合が 60%以上となっている。とはいえ、得られている範囲の情報から推測して、この「不明」のほとんどは、添付ファイルによる攻撃であったと思われる。
- 添付ファイル種別（図 4）は、「実行ファイル」が 80%以上であり、これらは全て、圧縮形式ファイルの中に実行ファイル（exe ファイル）が含まれているものであった。
  「Office 文書ファイル」は前述のとおり、マクロを悪用する手口と昨年修正された脆弱性の悪用を伴う手口が使われていた。

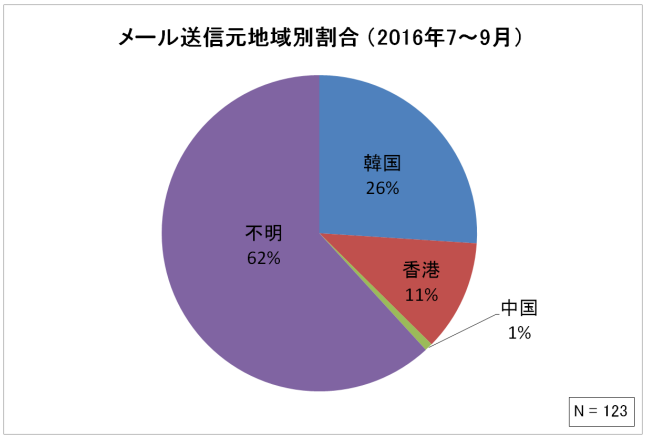


**図 1　メール送信元地域別割合**

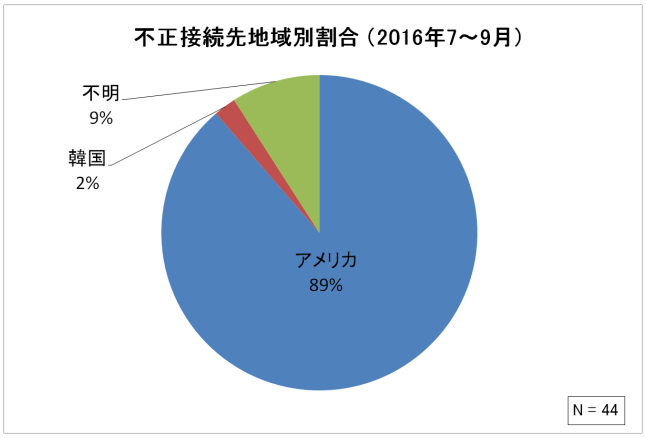


**図 2　不正接続先地域別割合**

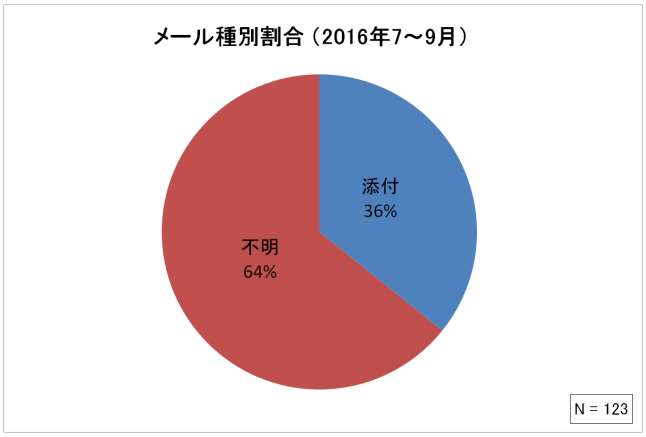


**図 3　メール種別割合**

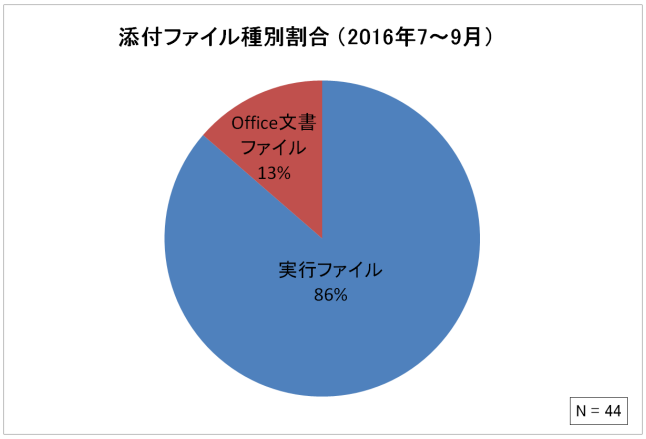


**図 4　添付ファイル種別割合**

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、広く無差別にばらま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」、「接続先不明」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