J-CSIP
Initiative for Cyber Security
Information sharing Partnership of Japan

サイバー情報共有イニシアティブ（J-CSIP）
2012 年度 活動レポート

IPA 独立行政法人情報処理推進機構
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）

2012 年度 活動レポート

目次

サイバー情報共有イニシアティブ（J-CSIP）

2012 年度 活動レポート

2013 年 4 月 17 日
IPA（独立行政法人 情報処理推進機構）
セキュリティセンター

本書の要旨

本レポートでは、IPA（独立行政法人情報処理推進機構）が運営しているサイバー情報共有イニシアティブ[1]（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan、ジェイシップ）について、設立経緯等を含め、2012 年度の活動の概要および成果について報告する。

本書の用語

用語	説明
サイバー攻撃	本書では、不正アクセス、DoS／DDoS（サービス拒否）攻撃、標的型サイバー攻撃を含む、インターネット等を経由して行われる攻撃全般を指している。
標的型サイバー攻撃	本書では、ごく少数の対象または多数だが特定の範囲のみに対して、情報窃取等を目的として行われるサイバー攻撃を指している。IPAの「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」[2]では、これらの攻撃への対策を紹介している。
ウイルス	コンピュータウイルス。マシンの遠隔操作を可能にする遠隔操作ウイルスやボットウイルス、情報窃取を主目的とするスパイウェア、悪意のあるプログラム全般を指すマルウェアといった様々な分類（用語）があるが、本書では、これらを総称してウイルスと呼んでいる。
標的型攻撃メール	本書では、情報窃取等を目的として特定の組織に送られるウイルスメールを標的型攻撃メールと呼んでおり、メールの受信者に関係がありそうな送信者の詐称、添付ファイル等を開かせるための件名や本文の細工、ウイルス対策ソフトで検知しにくいウイルスの使用といった特徴がある。 ある不審なメールについて、それが標的型攻撃メールなのか、広くばら撒かれたウイルス付きスパムメールなのかを明確に区別することは難しく、また、基準も存在しないため、様々な要素から総合的に判断することになる。

1 サイバー情報共有イニシアティブ （IPA）
http://www.ipa.go.jp/security/J-CSIP/index.html
2 「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を公開 （IPA）
http://www.ipa.go.jp/security/vuln/newattack.html

1　J-CSIP の概要

1.1 発足の背景

サイバー攻撃による知的財産やライフラインを狙った事案や機密情報漏洩が海外を中心に多発し、ITの安全確保によって守るべき対象が、経済活動や国民生活に直接かかわる分野へ質的に変化している。こうした背景のもとに、2010 年 12 月より、経済産業省にて有識者参画のもと「サイバーセキュリティと経済 研究会」[3]が開催された。

この研究会の中間とりまとめ [4]における主要な結論および提言として「標的型サイバー攻撃への対応」が挙げられ、その有効な対策の一つに、組織間の情報共有の必要性が議論された。また、研究会の中間とりまとめと同時期、2011 年には日本国内でも標的型サイバー攻撃に起因すると考えられる事案が複数件発生した。

これらの状況を受け、経済産業省要請のもと、2011 年 10 月 25 日、日本の基幹産業を担う重要インフラ機器製造業者 9 社（重工・重電等）の関係者が集まり、経済産業大臣より、セキュリティ対策の強化を改めて求めると共に、標的型サイバー攻撃への対抗施策として、官民連携による情報共有体制である「サイバー情報共有イニシアティブ（J-CSIP）」が発足した。

情報共有の重要性

サイバー攻撃への効果的な対策を行うためには、自組織に対し存在する脅威、および、実際の攻撃に関する事例の情報が重要となる。一方、標的型サイバー攻撃と呼ばれる、ごく少数または多数だが特定された範囲のみに対して水面下で行われる攻撃については、そもそも攻撃の存在の認知・検知が難しい。そして、攻撃を受けた組織で認知できた内容についても、その情報が組織外へ共有される機会が少ない、または共有することが難しいため、実態の把握すら困難である。

「サイバーセキュリティと経済 研究会」では、次に挙げるような、情報共有における複数の課題をクリアするため、政府機関が先陣を切って進めるべきという意見があった。

- 情報提供元や機微情報の匿名処理、スキームの検討が必要。
- 秘密情報を扱うクローズドな中での実効的な情報共有のコミュニティの作成が必要。

また、特定業種を狙うような標的型サイバー攻撃については、同業種の組織間での情報共有が効果的であるが、それらの組織は、時に市場においては競合関係にもある。

サイバー攻撃と対策は非対称的（防御側よりも攻撃側が有利）であり、対抗施策の一つとして、被攻撃側での情報共有が重要であるという共通認識のもと、J-CSIP では、各参加組織における様々な制約を相互に認めながらも、情報共有の活動を行っている。

---

[3] サイバーセキュリティと経済 研究会 （経済産業省）
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#cyber_security

[4] サイバーセキュリティと経済 研究会中間とりまとめの公表について （経済産業省）
http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/report01.html

1.2 取り組みの目的

J-CSIP は、公的機関である IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組みである。

具体的には、IPAと各参加組織（あるいは参加組織を束ねる業界団体）間で締結したNDA[5]のもと、参加組織およびそのグループ企業において検知されたサイバー攻撃等の情報をIPAに集約。情報提供元に関する情報や機微情報の匿名化を行い、IPAによる分析情報を付加した上で、情報提供元の承認を得て共有可能な情報とし、参加組織間での情報共有を行っている（図 1）。

この情報共有によって、次のような対策に繋げ、各参加組織や業界全体において、サイバー攻撃への防御力を高めることを目的としている。

① 類似攻撃の早期検知と被害の回避
② 攻撃に対する防御の実施
③ 今後想定される攻撃への対策検討

現在、J-CSIP では、サイバー攻撃で頻繁に用いられ、かつ大きな脅威となっている、標的型攻撃メールに関する情報共有を当面の主対象として実運用を進めている。

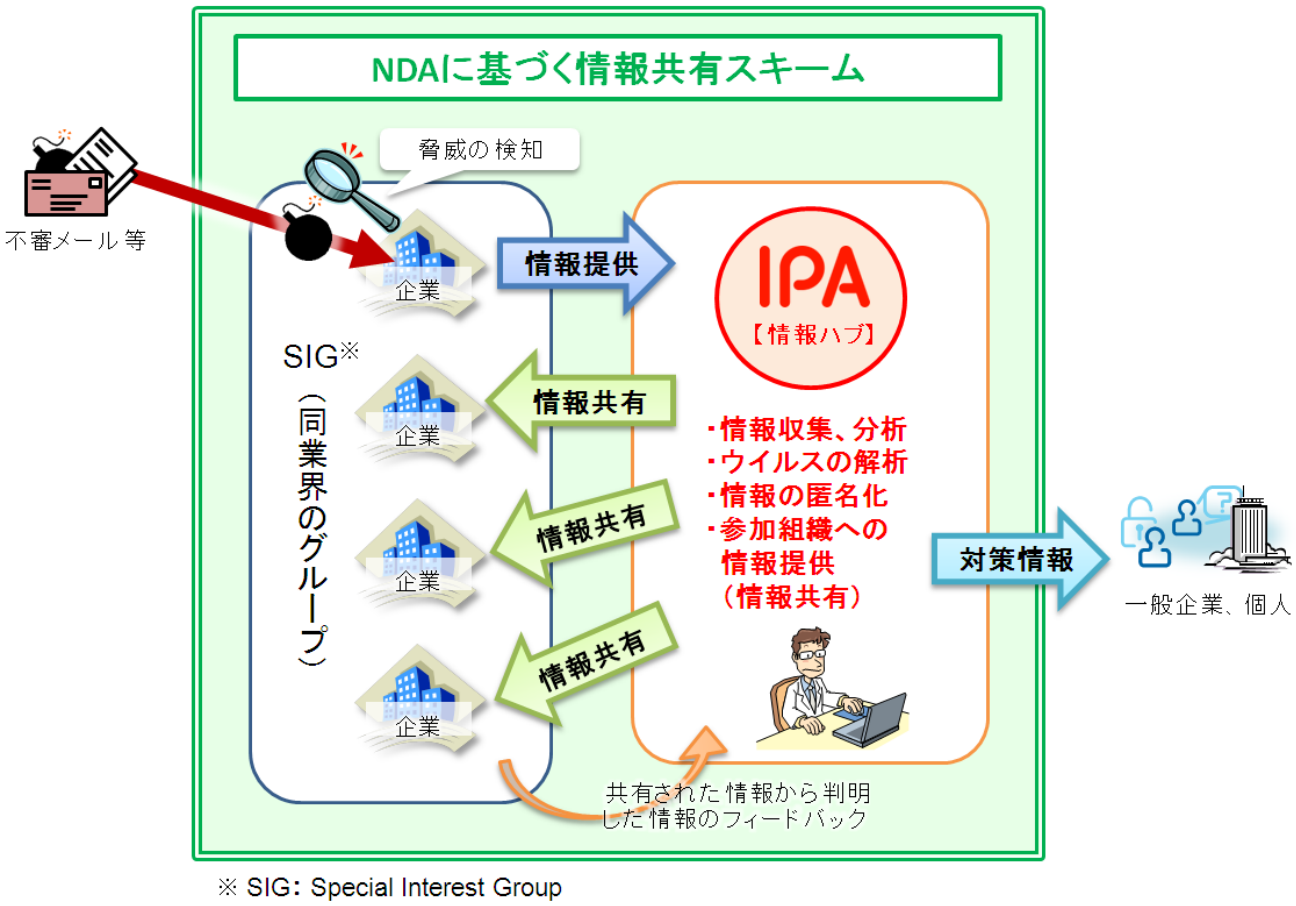

図 1　NDA に基づく J-CSIP の情報共有活動

[5] NDA：　Non-Disclosure Agreement、秘密保持契約

2　活動成果

2012 年度までの J-CSIP の活動成果は、主に次の 2 点である。

- **5 つの業界、39 組織**での情報共有体制の確立
- **160 件**の情報共有の実施（2012 年 4 月 1 日～2013 年 3 月 31 日）、および情報共有活動による定性的な効果の確認

2.1 情報共有体制の確立

J-CSIP 発足の背景を含む、J-CSIP の情報共有体制の構築と拡大の沿革を、表 1 に示す。

表 1　J-CSIP の沿革

項番	時期	内容
1	2010 年 12 月～	「サイバーセキュリティと経済　研究会」開催
2	2011 年 8 月	「サイバーセキュリティと経済　研究会」中間とりまとめ（情報共有の必要性の提言） 「標的型攻撃に関する情報共有枠組みのパイロットプロジェクト」[6]実施
3	2011 年 9 月～10 月	国内で標的型サイバー攻撃に起因すると考えられる複数の事案の報道
4	2011 年 10 月 25 日	J-CSIP 発足
5	～2012 年 3 月末まで	経済産業省、IPA、重要インフラ機器製造業者 9 社等の実務者で協議を重ね、NDA の策定、および情報共有のためのルールを整備
6	2012 年 4 月	重要インフラ機器製造業者 SIG において NDA 締結、運用開始
7	2012 年 7 月～10 月	電力業界、ガス業界、化学業界、石油業界の SIG をそれぞれ設立・運用開始、参加組織の数が 38 組織となる（その後、1 組織追加）
8	2012 年 10 月	SIG 間（業界間）の連携による情報共有の運用を導入
9	～2013 年 4 月現在	情報共有活動を実施中

J-CSIPでは、まず重要インフラ機器製造業者 9 社の集合体（SIG：Special Interest Group[7]）において、IPA と各事業者の実務者を中心に、運用開始のための準備を行った [8]。ここでの主な議題としては、次のようなものがあった。

- NDA の構成および内容の検討
- 情報共有のための手順とルールの検討
  - 情報の取扱い規則と、情報共有の流れ（運用フロー）
  - 具体的な情報の授受の手段、相互連絡窓口の設定
  - 情報の匿名化を行う基準と方式、情報提供や情報共有を行う際のフォーマットと記法
- 各社のサイバー攻撃対策状況の情報交換

---

6 「情報共有の枠組み」を構築するための実施方法やルールに関する調査検討を行ったプロジェクト。プロジェクトの一環として「サイバー情報共有のためのワークショップ」等を実施した。
http://www.jpcert.or.jp/event/CTAPP.html

7 「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。

8 経済産業省、IPA、重要インフラ機器製造業者 9 社に加え、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、一般社団法人 日本情報システム・ユーザー協会（JUAS）、株式会社ラックが協議に参画した。

これらの協議を経て、2012 年 4 月、IPA と各事業者間での NDA の締結、および情報共有のためのルール整備が完了し、J-CSIP は本格的な情報共有の運用を開始した。

続いて 2012 年 7 月から 10 月にかけ、重要インフラ機器製造業者 SIG と同等の仕組みで、電力業界、ガス業界、化学業界、石油業界の SIG をそれぞれ設立し、運用を開始した。2012 年 10 月からは、この 5 つの業界 SIG での情報共有体制に加え、SIG 間(業界間)の連携による情報共有の運用を導入した。2013 年 4 月現在、5 つの SIG 全体で、参加組織の数は 39 組織である。

なお、J-CSIP では必要に応じて、情報提供元の許可のもと、情報の一部を JPCERT/CC 等の情報セキュリティ関係機関に展開し、対策の連携にも活用している。また、重大な事案が発生した場合は、経済産業省および NISC(内閣官房情報セキュリティセンター)との連携を行う体制となっている(図 2)。

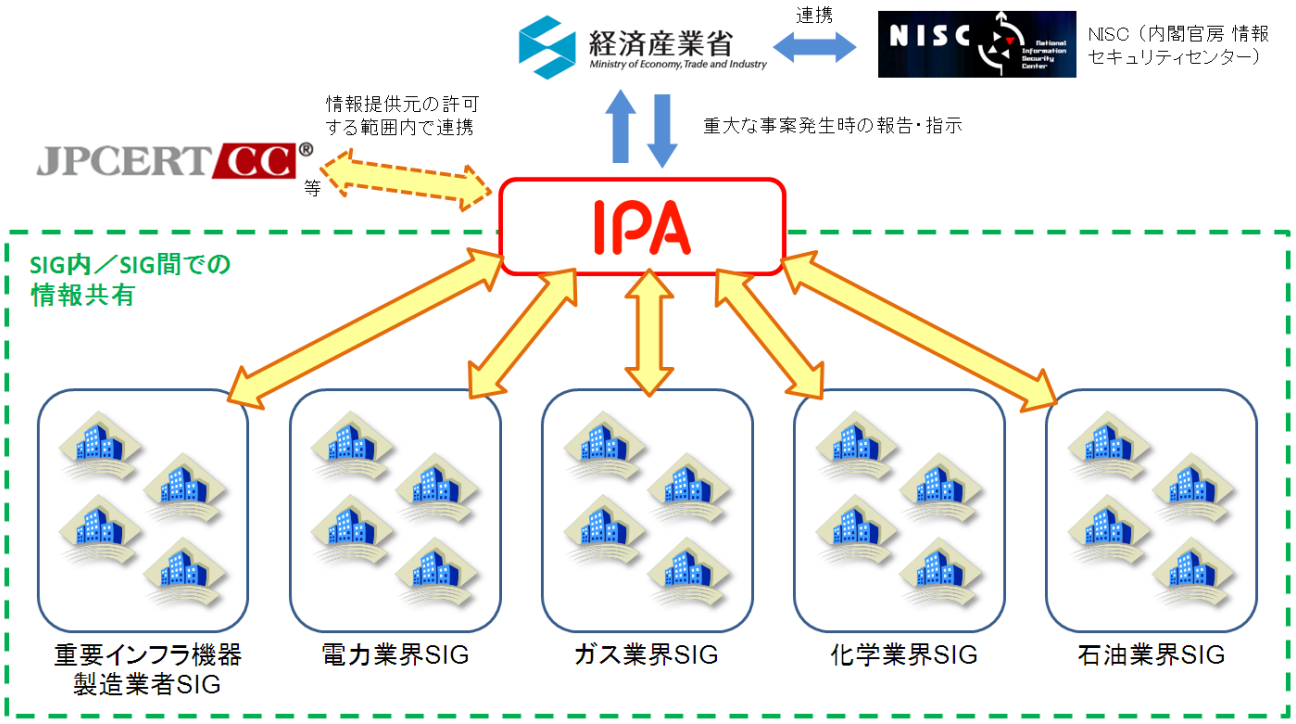

図 2　複数の SIG、関係機関を含む情報共有体制

2.2 情報共有活動の成果の概要

NDA に基づく情報共有を行う体制やルールを整備したことにより、2012 年度は 160 件の情報共有を実施するなど、多くの攻撃情報を収集、活用できたと共に、個々の攻撃の情報共有のみならず、複数の攻撃の傾向や相関を把握できるようになった。

量的な面だけでなく、同業種の異なった（市場においては競合関係にもある）組織間での情報共有という新しい試みは、攻撃の把握・防御・対策の観点で、次に挙げるような質的変革をもたらしており、J-CSIP はサイバー攻撃対策の一つとして有効な活動であることが分かった。

- これまで、事業者相互でのサイバー攻撃の状況把握は難しかったが、公的機関である IPA が情報集約点として情報共有を行うことにより、業界を狙った同一もしくは類似の攻撃が実際に行われていることが相互に把握できると共に、共同で検知・防御できるようになった。

- NDA 下での情報管理を前提としているため、情報の提供や共有する内容について迅速な判断が可能であることから、質の高い（情報の鮮度や密度が高い）情報となっており、検知と防御に有効である。

- IPA が情報共有の集約点となることで把握できた、攻撃の傾向や複数の攻撃間の相関についても、参加組織で共有できるようになった。これにより、今後想定される攻撃への対策検討へも繋がっている。

3　2012 年度の実績

3.1 実施件数および傾向

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を、表 2 に示す。

表 2　情報提供および情報共有の状況

項番	項目	件数（5 つの SIG、39 組織での合算）
1	IPA への情報提供件数	**246 件**
2	参加組織への情報共有実施件数	**160 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 件に集約して配付したり、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。

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が調査分析を行い、統計をとった結果、次のような傾向が見られた[9]。この統計情報の詳細は、別紙に示す。

- メール送信元地域は、韓国、日本、アメリカの順に多く、上位 3 つで全体の半数を占めた。
- ウイルスの不正な通信の接続先地域は、アメリカが全体の 3 割弱を占め、残りはアジア諸地域が続いた。日本が不正な通信の接続先となっていたケースも 7%確認した。
- 不審なメールの 8 割弱はウイルスと思われる添付ファイルが付いており、約 1 割は不審なウェブサイトへの URL リンクが含まれていた。
- 添付されていた悪意のあるファイルのファイル形式は、Office 文書ファイルと実行形式ファイルがほぼ同率で多く、あわせて全体の 9 割以上を占めた。

IPA は各参加組織に対し、今後とも J-CSIP への更なる情報提供を呼びかけていくと共に、IPA 自身の情報ハブとしての機能も強化していく予定である。

なお、IPAでは、2008 年から標的型攻撃メールに関する相談・情報提供の窓口を設置[10]し、民間企業・組織・公的機関や一般利用者に対して、標的型攻撃メールの情報提供を呼びかけている。参考までに、この窓口へ寄せられた標的型攻撃メールの情報は、2012 年度末時点の約 5 年間で累計 145 件となっている。これらの情報から得られた知見は「IPAテクニカルウォッチ」[11]等で公開している。

---

9 メール送信元地域やウイルスの不正接続先地域については、攻撃者が自身の身元を隠すため、他者のマシン等を踏み台として悪用している可能性を考慮する必要がある。

10 2008 年当時は「不審メール 110 番」。現在は様々な相談対応も含め「標的型サイバー攻撃の特別相談窓口」で受け付けている。
http://www.ipa.go.jp/security/tokubetsu/

11 IPA テクニカルウォッチ － Vol.4 と Vol.12 が標的型攻撃メールに関するレポートである。
http://www.ipa.go.jp/security/technicalwatch/

3.2 情報共有の事例

情報共有を行うことにより、同種の不審メールが複数組織に着信していたことが判明し、また、それらの情報を集約し、更なる情報共有に繋がった事例を紹介する。

ここでは、次の三段階に分けて、時系列に沿って説明を行う。

- 第一段階：不審メール情報の情報共有
- 第二段階：各組織での同種のメールの発見
- 第三段階：情報の集約分析と更なる情報共有

まず、第一段階として、不審メールの検知から、IPA を経由した情報共有の実施までの流れを図 3 に示す。

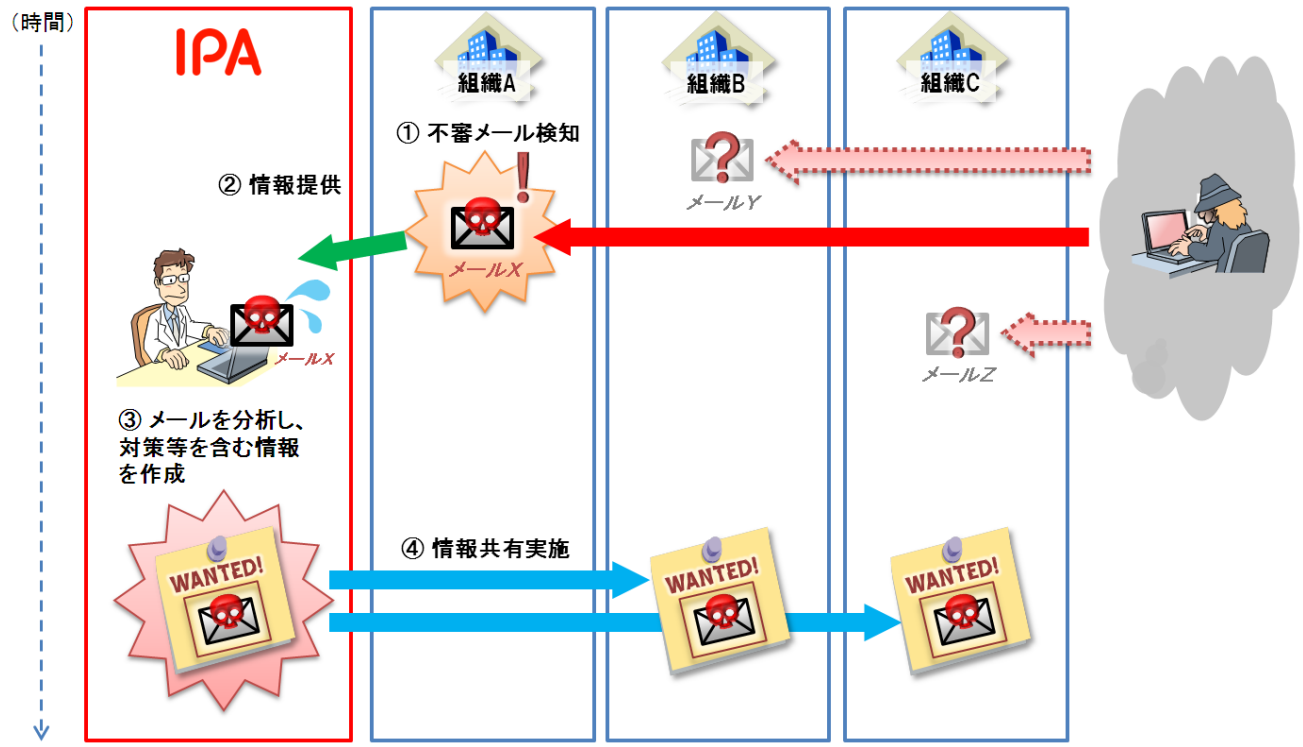

図 3　第一段階：不審メール情報の情報共有

① 不審メール検知 ～ ② 情報提供

この事例では、最初に J-CSIP 参加組織 A にて不審メールが検知された（図 3 の①）。そして、組織 A から IPA へ、当該メールが速やかに情報提供された（図 3 の②）。

この時点では、他の J-CSIP 参加組織に対して同種のメールが着信しているか否かは不明であったが、実際には着信していた。ここでは、組織 A に届き、情報提供されたメールを「メール X」、組織 B と組織 C に届いていたメールをそれぞれ「メール Y」「メール Z」とする。

③ メールを分析し、対策等を含む情報を作成 ～ ④ 情報共有実施

IPA は、情報提供された「メール X」の分析を行い、同種のメールを探し出すための情報を作成し（図 3 の③）、情報提供元である組織 A の了解を得て、J-CSIP 参加組織へ情報共有を即日実施した（図 3 の④）。

続いて、第二段階として、各組織での同種のメールの発見と報告までの流れを図 4 に示す。

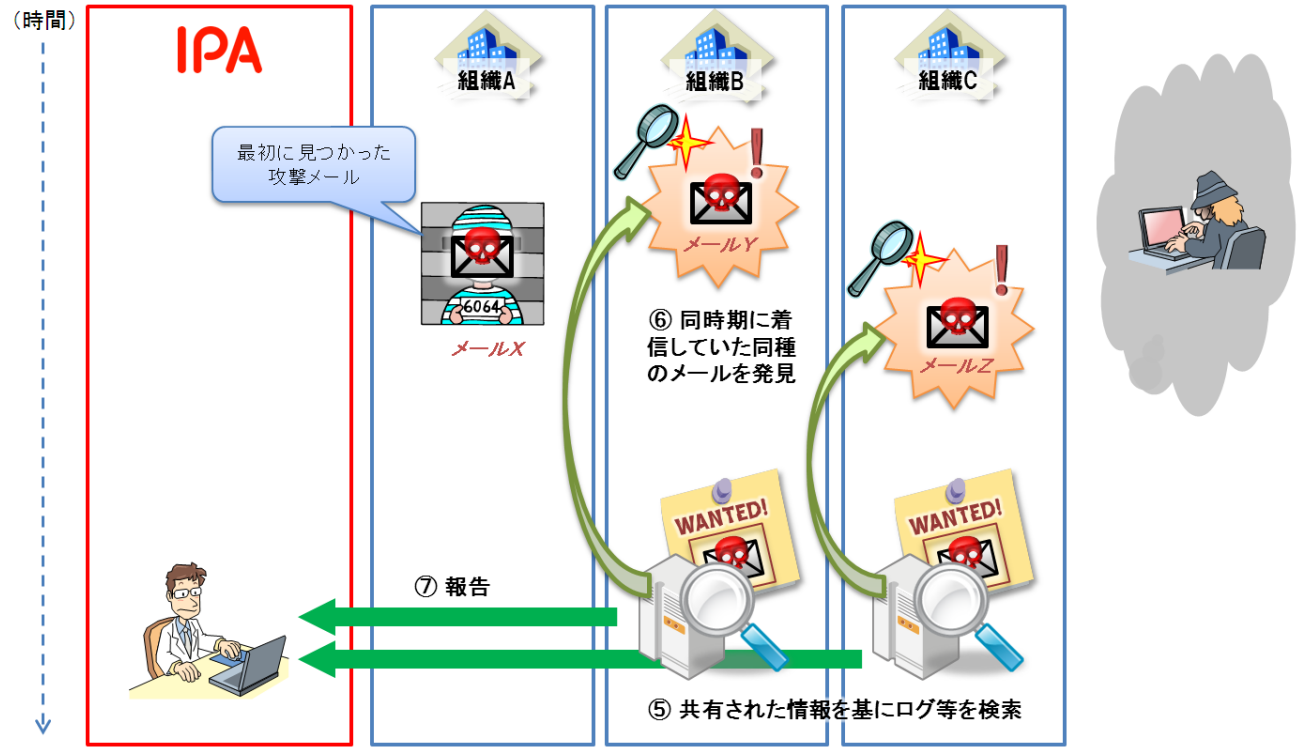

図 4　第二段階：各組織での同種のメールの発見

⑤ 共有された情報を基にログ等を検索

図 3 の④で共有された情報を基に、各参加組織は自社のメールサーバのログの検索等の調査を行った（図 4 の⑤）。

⑥ 同時期に着信していた同種のメールを発見

調査の結果、組織 B、組織 C と、他の組織においても「メール X」と同時期に着信した、同種の不審メールである「メール Y」「メール Z」が発見された（図 4 の⑥）。

⑦ 報告

J-CSIP では、共有された情報を基に判明した情報について、各参加組織から IPA へ可能な範囲での報告を求めている。このルールに従い、組織 B、組織 C から、IPA に対し、同種のメール（「メール Y」「メール Z」）の発見に関する報告がなされた（図 4 の⑦）。

第三段階として、一連の攻撃情報を集約した上での、更なる情報共有の実施までの流れを図 5 に示す。

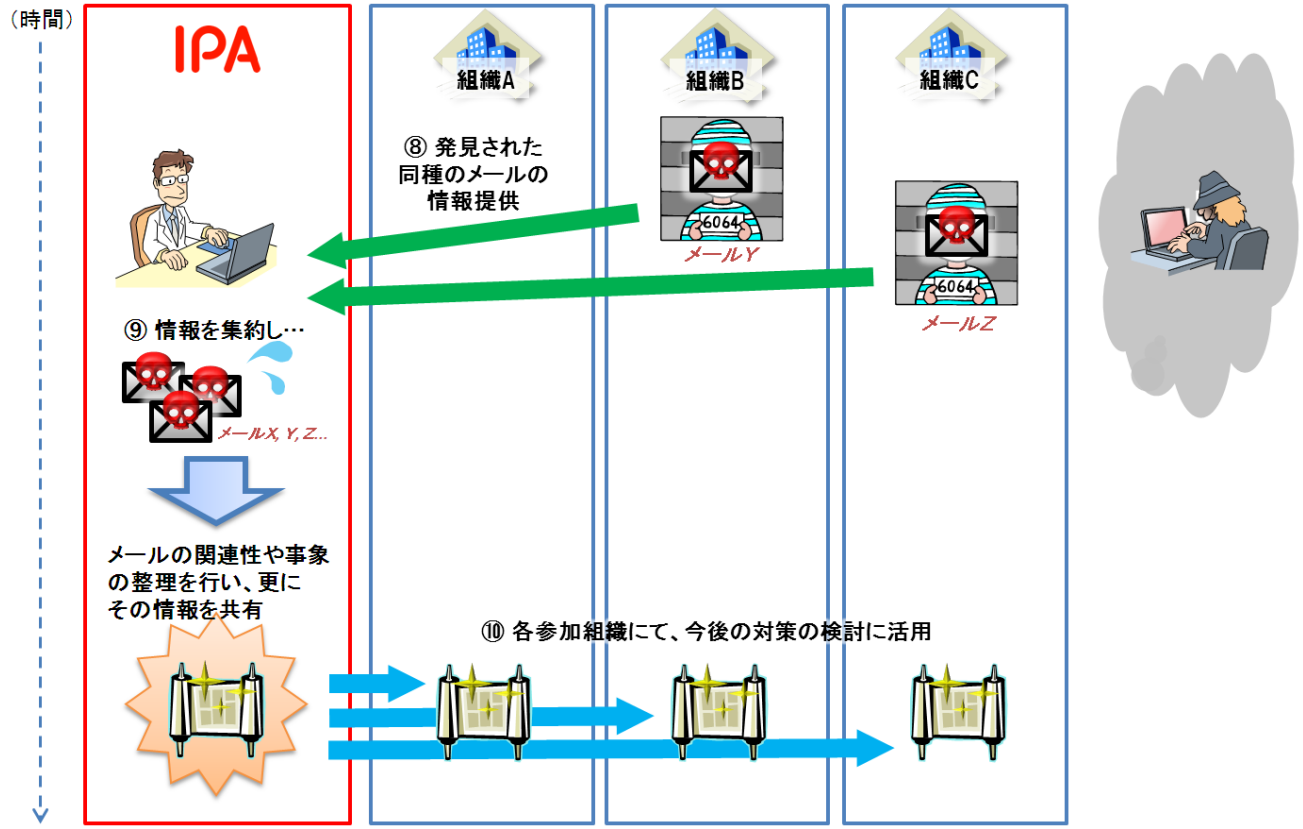

図 5　第三段階：情報の集約分析と更なる情報共有

⑧ 発見された同種のメールの情報提供

報告を受けた IPA は、これら発見されたメール X、Y、Z について、各組織に着信した日時の差や、メール同士の共通点・相違点があることに注目し、改めて、可能な限りの情報提供を呼びかけた。これにより、組織 B から「メール Y」、組織 C から「メール Z」の情報提供がなされた（図 5 の⑧）。

⑨ 情報の集約と整理、更なる情報共有 ～ ⑩ 今後の対策の検討に活用

IPA では、こうして集約した情報から、個々のメールや添付ファイル（ウイルス）について、同一である点や異なる点を抽出。一連のメールの関連性や、時系列に沿った事象の整理、攻撃手口の分析を行った上で、その情報を更に参加組織へ共有した（図 5 の⑨）。この情報は、各参加組織にて、今後の対策の検討に活用されている（図 5 の⑩）。

3.3 考察

本紙の 1.2 章にて述べた、J-CSIP の情報共有の活動から実現しようとしている 3 点の対策の観点から、3.2 章の事例を考察する。

① 類似攻撃の早期検知と被害の回避

本事例の場合、組織 A で発見された攻撃メールを基に共有された情報によって、他の組織でも同種のメールを発見することができた。これは、情報共有による直接的な成果だと言える。

攻撃メールを漏れなく発見し、あるいは回避していくことは容易ではない。しかし、同種のメールが着信した複数の組織のうち、どこか一か所であっても発見されれば、その情報が共有されることで、全体としての防御力の向上に繋がる。

共有された情報によって類似の攻撃の発見や事前の回避（攻撃メールのブロック等）に繋がった例は本事例の他にも複数あり、情報共有が有効であると参加組織から評価されている。

② 攻撃に対する防御の実施

J-CSIP では、添付ファイル（ウイルス）によって発生する不正な通信の接続先について、情報提供元や IPA による解析で判明した場合、その情報も共有している。この情報は、プロキシサーバやファイアウォール等で外部接続先をブロックするといった対策に活用されており、共有した情報だけでは攻撃メールが発見できなかった場合や、別の新たな攻撃が発生した場合でも、同等の不正な通信を行うウイルスであれば、被害を受けずに済む。

この事例においても、IPA は提供されたウイルスの全ての不正な通信の接続先を確認し、迅速に共有すると共に、各参加組織における対策に反映されている。

③ 今後想定される攻撃への対策検討

本事例では、IPA に集約した攻撃情報について関連性や事象を整理し、更にその結果を共有している。これにより、本件に関わる一連の攻撃の相関や流れといった、攻撃手口や状況を参加組織間で把握することができた。そして、この情報は、各組織において今後どのような対策が必要か、あるいは、いかに既存の対策をより有効なものとするかといった、今後想定される攻撃への対策検討に繋がっている。これは、情報を集約していることによる、本活動の特徴的な成果と言える。

総括 ー 攻撃の認識と情報共有の重要性

本事例においては、これまでの活動で各参加組織が一通りの情報共有フローに慣れていたこと、更に、組織 A による迅速な検知と情報提供があったことにより、情報共有を非常にスムーズに行うことができた。情報共有を行うにあたり、ルール・手順や相互の窓口を事前にしっかりと定めておくこと、また、実際の情報授受を繰り返して、手順に慣れておくことが重要である。これは、組織間での情報授受だけでなく、組織内においても同じことが言える。

また、本事例の中で、「共有された情報をもとに、同種の攻撃メールの着信をメールサーバのログ等から確認したが、受信者は添付ファイルを開かずメールを削除しており、システム管理部門への報告も特にされていなかった」というケースも見られた。これは、被害を防ぐことができて問題なかったということであると共に、自組織に着信した攻撃メールを把握できていない部分があることに気付けたという意味でもあった。

一般利用者向けのウイルスメール対策としては、基本的には「不審なメールは開かず削除する」対処が一般的であり、IPA もそのように推奨している。しかし、組織として一歩進んだ対策を行っていくためには、自

組織の誰に、あるいはどの部門に、どのような攻撃メールが着信しているのかを把握することが重要になってくる。その上で、現在施している多層のセキュリティ施策がどの程度有効に機能しているのかを評価し、対策の改善に繋げていく必要があるだろう。

約一年の運用を経て参加組織へヒアリングを行ったところ、「不審なメールを確認したら即削除という指示をしていたが、システム管理部門へ届け出られるように運用を変更した」という社が複数あった。この運用は、システム管理部門にとっては負担が大きくなるが、自組織に対する攻撃の有無、また、その実態を把握する上で重要な手がかりとなる。また、そうして発見された不審メールについて、まずは自組織内の他の職員に同種のメールが着信していないかを迅速に調査できると共に、J-CSIP を通じて情報共有することで、参加組織全体での防御力の向上という、本事例のような効果に繋がっていくものである。

4 今後の取り組み

経済産業省および IPA は、この J-CSIP の活動が、標的型攻撃をはじめとするサイバー攻撃の対策へ有効なものであると考えており、同時に、参加組織からも高い評価を受けている。

IPA は、参加組織の拡大、共有する情報の拡充、全体的な効率の向上等を図りつつ、2013 年度以降もこの取り組みを継続し、標的型をはじめとするサイバー攻撃に対する組織および組織群の防衛力の向上を推進していく。

「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）
http://www.ipa.go.jp/security/tokubetsu/

別紙：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 が調査分析を行い、統計を行った結果を示す。それぞれの統計について、母集団の数である N が異なっているが、その理由は巻末に示している。また、各グラフについて、小数点以下を四捨五入しているため、合計が 100 とならない場合がある。

1. メール送信元地域別割合

J-CSIPにおいてIPAへ情報提供された不審メールのメール送信元地域別割合を図 6 に示す[12]。メール送信元とは、メールヘッダの情報から推測できる、攻撃者がメールを送信する作業を行ったと思われるIPアドレスである。

地域別割合で統計を取ると、1 位から 3 位は韓国、日本、アメリカとなっており、この上位 3 つで全体の半数を占めた。4 位以降は、香港、中国と続いている。不正なメールは、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送信されている場合がある。そのため、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が、アメリカを除くとアジア圏に集中しているのが特徴的である。

なお、情報提供されたメールの三分の一については、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要因により、送信元 IP アドレスが不明であった。

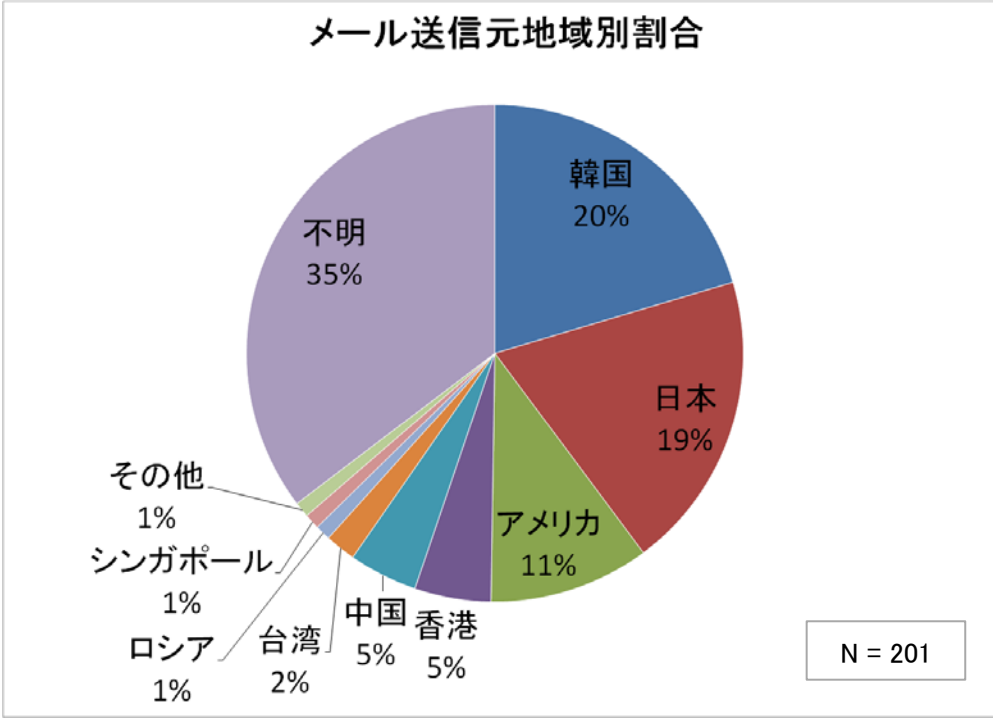

図 6　メール送信元地域別割合

[12] 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。本レポートの統計では、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。

2. 不正接続先地域別割合

同じく、情報提供されたウイルスの不正接続先の地域別割合を図 7 に示す。ここで不正接続先とは、メールの添付ファイルによって感染させられるウイルスや、メール本文に記載されたURLリンクへアクセスした際に行われるドライブ・バイ・ダウンロード攻撃 [13]によって感染させられるウイルスが不正な通信を試みる接続先を指す。

地域別割合で統計を取ると、1 位はアメリカで全体の 3 割弱を占め、2 位～5 位は香港、中国、韓国、日本と、アジア諸地域が続き、この上位 5 位で全体の 7 割を占めた。日本が不正接続先となっていたケースは 7%であった。メールの配送経路や不正接続先で国内の IP アドレスやドメイン名を確認した場合、可能な限り、情報提供元の許可のもと JPCERT/CC と連携し、当該マシンの停止・復旧等のコーディネーションを行っている。

不正接続先についても、メール送信元と同様、攻撃者が自身の身元を隠すため、第三者のサーバやパソコンを悪用している可能性がある。一方で、攻撃者は不正接続先のマシンをある程度の期間は支配下に置いておくことが必要となると考えられ、そのような環境（攻撃インフラ）を構築・維持しやすい場所として、メール送信元のグラフとは異なる偏りが生じていることも推測できる。

不正接続先の 5%については、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 [14]等という理由により、不明であった。

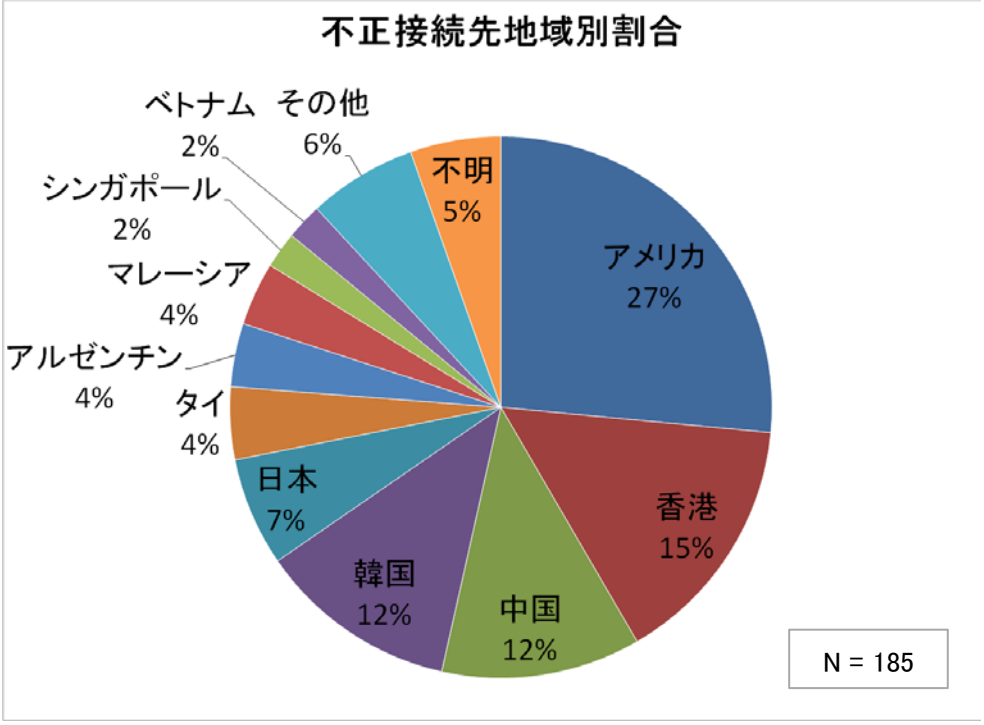

図 7　不正接続先地域別割合

---

13 ウェブサイトに仕掛けを施し、閲覧したパソコンの脆弱性を悪用してウイルスに感染させる攻撃手口。
参考：「ウェブサイトを閲覧しただけでウイルスに感染させられる"ドライブ・バイ・ダウンロード"攻撃に注意しましょう！」（2010 年 12 月の呼びかけ）　（IPA）
http://www.ipa.go.jp/security/txt/2010/12outline.html

14 通信を行う際、ホスト名を IP アドレスへ変換することを「名前解決」と呼ぶ。この時、既に情報が削除されているといった理由で、IP アドレスが得られない（名前解決できない）場合がある。

3. メール種別割合

図 8 は、それぞれのメールについて、それがどのような手口かという観点で分類したものである。

ここでは、悪意のあるファイルを添付し、それを開かせようとする「添付ファイル」、メールの本文中に URL リンクを記載し、そのウェブサイトでドライブ・バイ・ダウンロード攻撃等を行うと思われる「URL リンク」、そして、添付ファイルも URL リンクも無い、送信先メールアドレスの存在の確認等が目的と思われる「情報収集」の 3 つに分類している。

この分類では、「添付ファイル」が全体の 8 割弱を占め、「URL リンク」と「情報収集」がそれぞれ約 1 割となっている。全体としては、添付ファイルとしてウイルスを送りつける例が多いということになるが、URL リンクによるドライブ・バイ・ダウンロード攻撃にも注意が必要である。

残りの「不明」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、内容が確認できなかったものである。

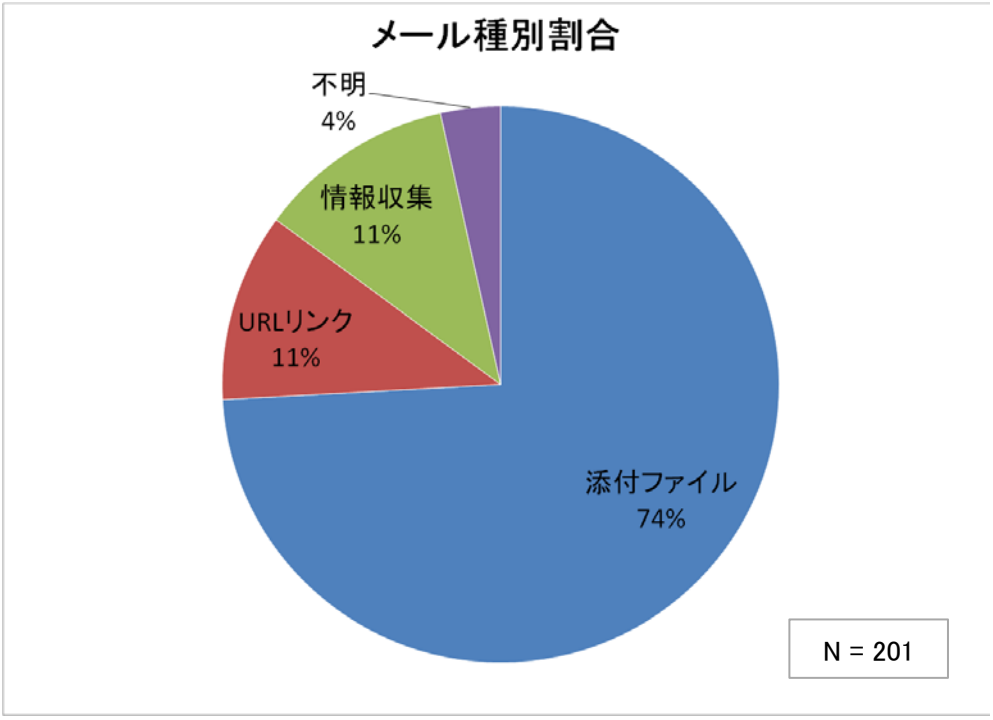

図 8　メール種別割合

4. 添付ファイル種別割合

先の「3. メール種別割合」のうち、「添付ファイル」となっていたものについて、添付されていた悪意のあるファイルの種別を図 9 に示す。

この統計では、Microsoft Word や Microsoft Excel 等の脆弱性を悪用する「Office 文書ファイル」と、拡張子が exe や scr 等である「実行ファイル」および「実行ファイル（RLO）」のみで、全体の 9 割以上を占めた。

実行ファイルについては、アイコンを文書ファイル等に偽装していることが多く、メールの受信者の錯誤を誘い、脆弱性の悪用なしでウイルスに感染させようとしていることが伺えた。「実行ファイル（RLO）」は、RLO[15]を使った拡張子偽装を施した実行ファイルである。アイコンの偽装と組み合わせ、メールの受信者を騙し、ファイルを開かせよう（実行させよう）という細工が行われることは珍しくないことが分かる。

また、統計上は「Office 文書ファイル」に含めているが、Office 文書ファイルの中に Flash オブジェクトを埋め込み、Adobe Flash Player の脆弱性を悪用するものも少数ながら確認した。

2012 年度は、Office 文書ファイル同様、Adobe Reader の脆弱性の悪用に使われる「PDF ファイル」の割合が相対的に少なかった。また、「HTML ファイル」も少数確認しており、添付されている HTML ファイルをダブルクリックしてウェブブラウザで表示すると、悪意のあるウェブサイトへ転送され、ドライブ・バイ・ダウンロード攻撃が行われる仕組みのものとなっていた。

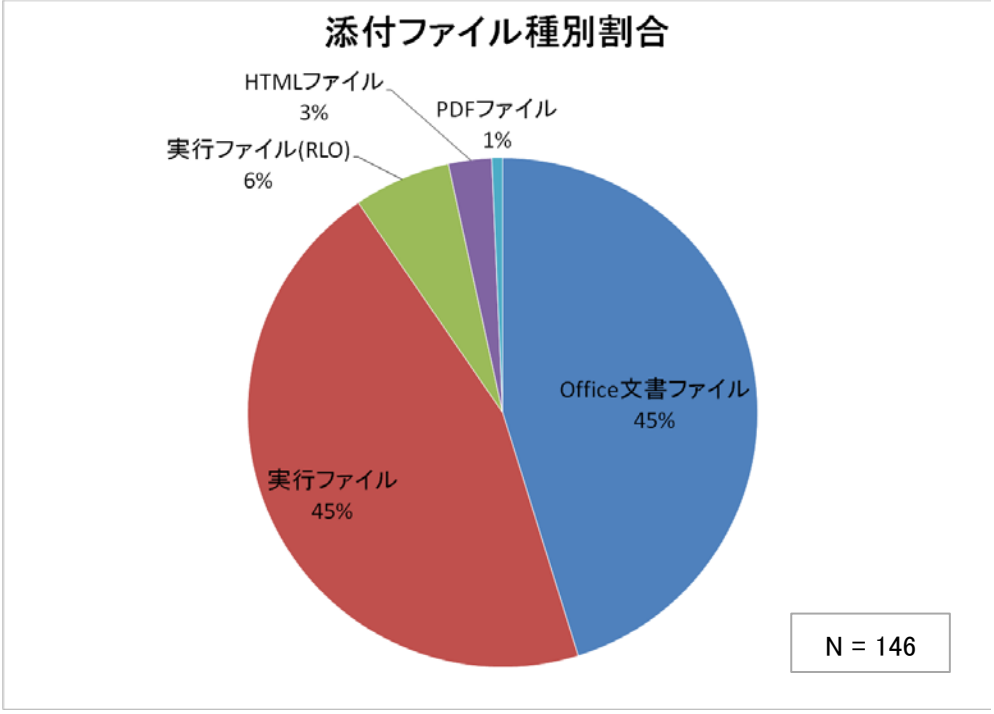

図 9　添付ファイル種別割合

15 「Right-to-Left Override」という、文字の表示上の並びを左右逆にする制御文字。
参考：「ファイル名に細工を施されたウイルスに注意！」（2011 年 11 月の呼びかけ）　（IPA）
http://www.ipa.go.jp/security/txt/2011/11outline.html

攻撃の手口が添付ファイルであるのか、URL リンクによるドライブ・バイ・ダウンロードであるのか、また、どのような添付ファイルが攻撃に使われるかといった傾向は、悪用されやすい脆弱性等と共に変化していくと思われる。一般利用者や社内で啓発活動を行うシステム管理部門においては、下記の基本的な注意点について、改めての徹底が必要であろう。

- 各種アプリケーションを常に最新にしておくこと
- 添付ファイルが実行ファイルでないかよく確認すること
- アイコンや拡張子は偽装できるという認識を持つこと
- 添付ファイルを開く際、またはメールに書かれている URL リンクを開く際は、それが罠である可能性を意識すること

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。

以上