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）
2014 年度 活動レポート

～ 国内組織を狙う執拗な攻撃者「X」の分析 ～

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）

2014 年度 活動レポート

～ 国内組織を狙う執拗な攻撃者「X」の分析 ～

目次

別冊

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

～ 国内組織を狙う執拗な攻撃者「X」の分析 ～

2015 年 5 月 27 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

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、2014 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、および標的型サイバー攻撃を含む、インターネットを経由し企業・組織等に対して行われる攻撃全般を指す。
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す。IPA では、標的型サイバー攻撃の全体像と対策ポイントについて、システム内部での攻撃プロセスの分析と内部対策をまとめた「システム設計ガイド」を公開している[2]。
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（RAT、Remote Access Trojan）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。
不正接続先	マシンに感染したウイルスが不正な通信を試みる接続先（例えば、遠隔操作ウイルスが接続する指令サーバ（C&C、Command and Control サーバ））や、標的型攻撃メールの本文に記載されたリンク先の URL 等を指す。

[1] サイバー情報共有イニシアティブ（IPA）
https://www.ipa.go.jp/security/J-CSIP/
[2] 「『高度標的型攻撃』対策に向けたシステム設計ガイド」の公開（IPA）
https://www.ipa.go.jp/security/vuln/newattack.html

1　2014 年度の J-CSIP の活動

1.1 はじめに

2011 年 10 月 25 日に J-CSIP が発足し、2012 年 4 月から情報共有の実運用を開始して以来、J-CSIP は 3 年間の情報共有活動を続けてきた。

情報共有活動は、攻撃の検知、情報の確保（メール、ウイルス、ログ等）、そして情報提供をいただくこと、また、共有された情報を得た組織においては、同等の攻撃の有無の確認等、全ての参加組織で多大な尽力をいただくことではじめて成り立つものであり、3 年目となった 2014 年度も順調かつ有意義な活動とできたことに、改めて深く謝意を示したい。

本書では、J-CSIP の 2014 年度の一年間の活動状況を報告する[3]。

1.2 活動の概要

J-CSIP における 2014 年度の活動成果の概要は次の通りである。

- 新たな SIG[4]として、**「資源開発業界 SIG」**を発足、運用を開始した（**5 組織**）。
- 既存の SIG の参加組織が **8 組織追加**となった。
  これらにより、J-CSIP は 2013 年度より **1SIG、13 組織が追加**となり、**計 6 つの SIG、59 組織**での情報共有体制となった。
- **195 件**の情報共有を実施した（前年度の情報共有件数は 180 件）。

J-CSIP では、2012～2013 年度に引き続き、2014 年度も主に標的型攻撃メールに関する情報共有を継続した。また、数は多くないが、攻撃者が使用していると思われる不審なファイル（ツール）や、不正接続先（URL や IP アドレス）の情報等についても共有を進めた。これら参加組織から IPA へ提供された情報については、IPA で匿名化や分析情報を付加した上で、概ね即日あるいは一両日中に情報共有を実施している。

また、各 SIG において必要に応じ会合を持ち、事例の紹介や、複数の攻撃情報の横断的な分析、情報共有ルールの見直し、そして各参加組織での標的型攻撃対策や情報セキュリティの取り組み状況に関する情報交換を行っている。

本書では、1.3 節で活動の沿革を示し、1.4 節で全体の体制図を示す。その後、2 章で実施件数、3 章で統計情報を示す。

J-CSIP の活動に関連し、経済産業省の所管 10 の独法および共管の 2 独法が参加[5]する「経済産業省・関係機関情報セキュリティ連絡会議（通称：独法連絡会）」についても、IPA は、J-CSIP の運用知見をもとにした情報共有体制の事務局を担っている。本件については、本書のまとめとともに、参考情報として 4 章に示す。

別冊**「国内組織を狙う執拗な攻撃者「X」の分析」**では、J-CSIP の 3 年間の活動で得られた情報を基に、横断的な分析を行った一つの成果を示す。IPA では、多数の攻撃の痕跡の繋がりから、同一の攻撃者（または攻撃グループ）が、**31 ヵ月間に渡り 9 つの国内組織へ攻撃を継続している**という推定に至った。この分析過程、攻撃者の手口について、事例の紹介とともに説明する。

---

[3] 2012 年度と 2013 年度の活動レポートは次の URL で公開している。
https://www.ipa.go.jp/security/J-CSIP/

[4] SIG：Special Interest Group の略。J-CSIP では、類似の産業分野同士が集まった情報共有のグループを指す。

[5] 独立行政法人通則法の一部改正に伴い 2015 年 4 月 1 日以降国立研究開発法人に分類される組織を含む。

1.3 活動の沿革

J-CSIP 発足からの内容を含む活動の沿革を「表 1 J-CSIP の沿革」に示す。項番 1～8 は「2012 年度活動レポート」、項番 9～11 は「2013 年度 活動レポート」で報告した内容であるため、説明は割愛する。

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」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 39 組織となる
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 6 月	セプターカウンシル「C4TAP」との相互情報連携開始
10	2013 年 6 月～7 月	ガス業界 SIG に 6 組織が新たに参加
11	2014 年 2 月	化学業界 SIG に 1 組織が新たに参加
12	2014 年 7 月～9 月	石油業界 SIG に 1 組織、化学業界 SIG に 3 組織が新たに参加
13	2014 年 10 月～12 月	化学業界 SIG に 3 組織が新たに参加
14	2015 年 3 月	化学業界 SIG に 1 組織が新たに参加 ※ 2014 年度、化学業界 SIG が J-CSIP で最大の SIG（参加組織数 15）となる
15	2015 年 3 月	資源開発業界 SIG（5 組織）を設立・運用開始、参加組織の数が 59 組織となる

「資源開発 SIG」の設立と運用開始（2015 年 3 月）

既存の「重要インフラ機器製造業者」「電力」「ガス」「化学」「石油」の業界に加え、2015 年 3 月、国内の重要産業である原油鉱業分野および天然ガス鉱業分野の 2 産業分野を擁する「資源開発 SIG」を設立・運用開始した。この SIG は、発足メンバとして石油鉱業連盟と鉱業に関する企業 4 社で構成している。

参加組織の拡充（2014 年 7 月～2015 年 3 月）

2013 年度末時点では 5 つの SIG、46 組織であった J-CSIP は、2014 年度、石油業界 SIG に 1 組織、化学業界 SIG に 7 組織が新たに参加することとなり、資源開発業界 SIG とあわせ、J-CSIP は 6 つの SIG、59 組織の情報共有体制となった。J-CSIP は、引き続き参加組織の拡充を計っていく予定である。

日本化学工業協会「情報セキュリティ対応部会」の発足（2015 年 2 月）

日本化学工業協会は、国内大手の化学関連企業とともに J-CSIP へ参画いただいているところであるが、この 2 月、「情報セキュリティ対応部会」（および「連絡会」）を発足させ、対応組織としての活動を開始した。J-CSIP の化学業界 SIG の活動は同部会の一部として位置付けられており、IPA は、今後とも化学業界の情報セキュリティの強化へ寄与していく。

1.4 情報共有体制 全体図

2015 年 5 月現在における、J-CSIP の情報共有体制の全体図を「図 1 J-CSIP 情報共有体制 全体図」に示す。J-CSIP は、次の体制で情報共有の運用を行っている。

- 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り、類似の産業分野同士が集まった情報共有のグループ「SIG」を構成し、SIG 内での情報共有に加え、情報提供元の許可に従い、SIG 間でも情報共有を行う。
- 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やセプターカウンシルの情報共有体制「C⁴TAP」と連携する。
- 重大な事案が発生した場合は、経済産業省および NISC（内閣サイバーセキュリティセンター）との連携を行う。

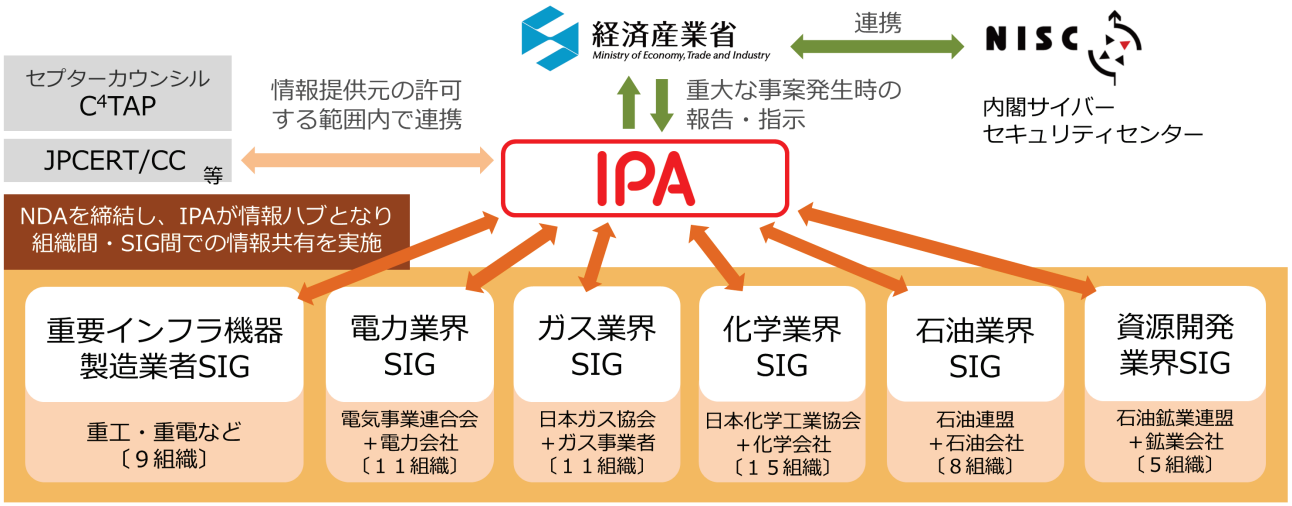


図 1 J-CSIP 情報共有体制 全体図

2　実施件数

J-CSIP での情報共有等の実施件数を「表 2　実施件数（2014 年度合計）」および「表 3　実施件数（2014 年度・四半期ごと）」に示す。数値は 6 つの SIG、全 59 参加組織での合算である。

表 2　実施件数（2014 年度合計）

項番	項目	件数	（前年比）	（2013 年度）	（2012 年度）	累計
1	IPA への情報提供件数※1	**626 件**	**（162%）**	（385 件）	（246 件）	1,257 件
2	参加組織への情報共有実施件数※2,※4	**195 件**	**（108%）**	（180 件）	（160 件）	535 件
3	標的型攻撃メールと見なした件数※3	**505 件**	**（216%）**	（233 件）	（201 件）	939 件

表 3　実施件数（2014 年度・四半期ごと）

項番	項目	2014 年 4 月～6 月	2014 年 7 月～9 月	2014 年 10 月～12 月	2015 年 1 月～3 月
1	IPA への情報提供件数※1	259 件	100 件	158 件	109 件
2	参加組織への情報共有実施件数※2	59 件	52 件	46 件	38 件
3	標的型攻撃メールと見なした件数※3	226 件	79 件	121 件	79 件

さらに、2013 年度からの四半期ごとの実施件数のグラフを「図 2　実施件数（2013～2014 年度・四半期ごと）グラフ」に示す。

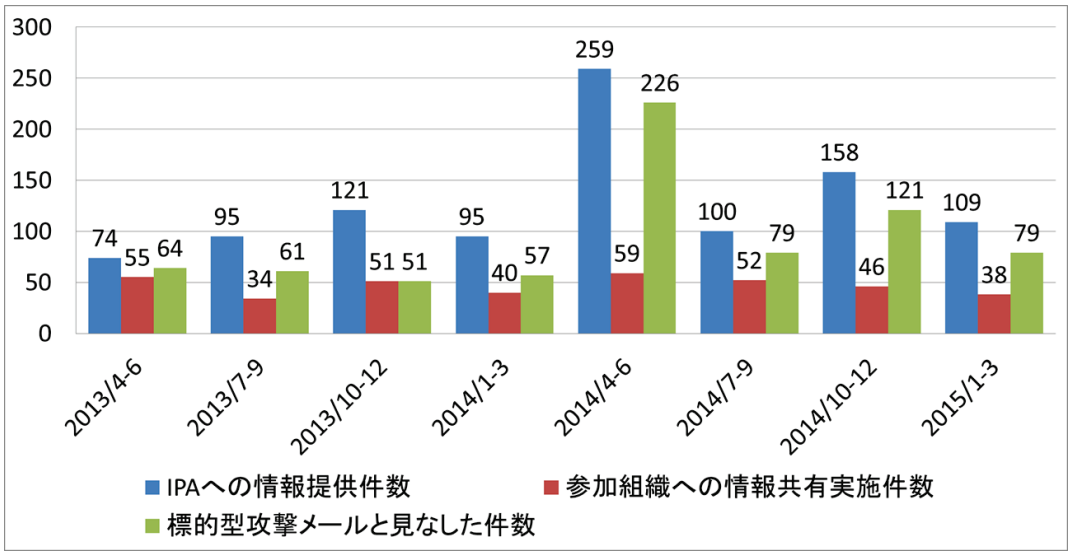


図 2　実施件数（2013～2014 年度・四半期ごと）グラフ

※1 不審なメールのほか、サーバのログや不審なファイル等の情報も件数に含む。

※2 同等の攻撃メールが複数情報提供された際に 1 件に集約して情報共有した場合や、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。

※3 情報提供されたもののうち、攻撃メールの情報であって、かつ広く無差別にばら撒かれたウイルスメール等を除外し、統計の対象とした件数。

※4 IPA が J-CSIP 外から入手した情報で、J-CSIP 参加組織へ情報共有を行った件数（2013 年度は 37 件、2014 年度は 53 件）を含む。

2012 年 4 月の情報共有の運用開始からの 3 年間で、情報提供件数の累計は 1000 件を超え、また、そのうち標的型攻撃メールと見なした件数も 900 件を超えた。平均すると、およそ 1 日 1 件の攻撃メールを観測していることになり、今後とも情報共有活動の継続が必要だと考えている。

今年度の実施件数については、次の傾向が見られた。

- 情報提供件数は、各月や四半期ごとに波はあったものの、通年では前年度より 1.6 倍の増加となった。また、標的型攻撃メールとみなした件数は、505 件と前年度より 2 倍以上の増加となった。
  特に 2014 年 4 月～6 月、いくつかの攻撃者（または攻撃グループ）により広範囲に継続して送信されたと思われる標的型攻撃メールが多数観測されたため、全体の件数を押し上げる結果となった。
- 標的型攻撃メールの観測数は、2014 年 4 月～6 月のような一過性のものを除くと、全体としては若干の増加傾向にあるように見える。ただし、時期による上下（波）が大きく、参加組織数の拡大の影響もあるため、IPA としては「攻撃は減ってはおらず、同程度で継続している」と見なしている。

3 統計情報

3.1 概要

2014 年度に情報提供された不審なメール等の情報 626 件のうち、標的型攻撃メールと見なした 505 件のメール、およびその添付ファイルやメール中の URL リンク等について、IPA が調査分析を行い、統計を行った。結果として、次のような傾向が見られた。

- メールの送信元地域の「不明」以外の割合では、日本が初めて 1 位（22%）となった（2012～2013 年度は 2 位であった）。
- 不正接続先については、アメリカとアジアの 4 地域（日本、香港、韓国、中国）が多数を占める傾向が 2012 年以降継続している（2012 年度 73%、2013 年度 79%）が、2014 年度はその割合が更に 95%へ大幅増となった。
- メールの種別について、メールの 52%はウイルスに感染させるための悪意のあるファイルが添付されていた。また、提供されたメールの情報が不完全である等の理由で「不明」としたものが 35%あるが、これらもほとんどは添付ファイルによる攻撃と推定できるものであった。
- URL リンクにより**偽の社内システムのログインサイトに誘導する攻撃（フィッシング）が見られた**。アカウント情報の窃取と、それを基にした不正アクセスが目的だと思われる。
- 添付ファイル種別では、Office 文書ファイルで**マクロ機能を悪用する攻撃**が初めて確認された。また、昨年度初めて観測されたショートカット（LNK）ファイルとジャストシステム文書ファイルは、本年度も引き続き一定の割合で確認された。なお、実行ファイルが半数を占める傾向は 2012 年度以降継続している。
- メールの送信元メールアドレスは、国内外のフリーメールが悪用される傾向が続き、合わせて 71%と高い割合を占めている。一方で、割合は多くないが、国内 ISP メール等、攻撃者が個人や組織のメールアカウントを乗っ取ったり、詐称したりして送られている攻撃メールも継続して確認している。

以降、3.2 節から 3.6 節にて、それぞれの統計情報について詳しく述べる。各統計で母集団の数である N が異なっている理由は 3.7 節に示す。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。

3.2 メール送信元地域別割合

標的型攻撃メールと見なしたメールの送信元地域別割合を「図 3 メール送信元地域別割合（2014 年度）」に示す [6]。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。

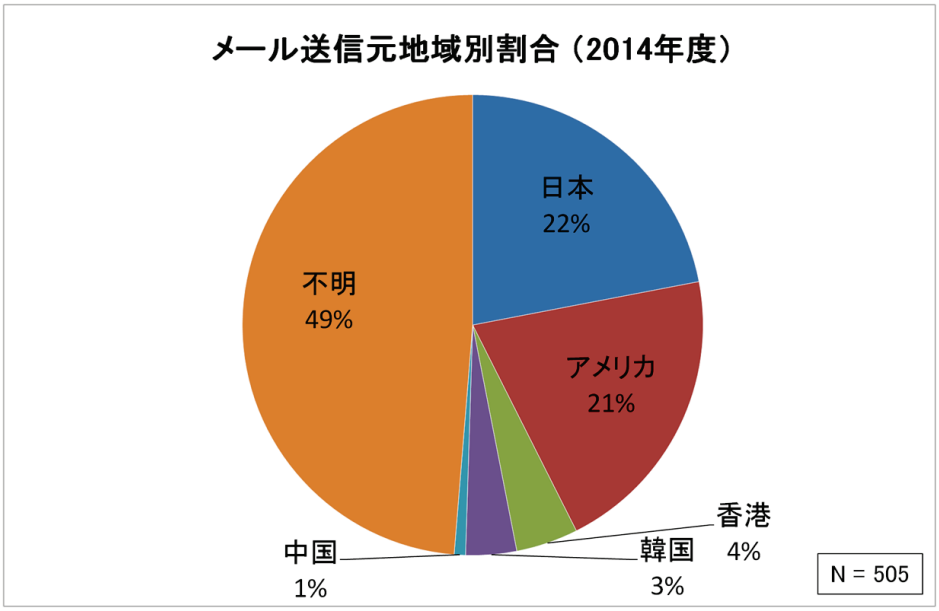


図 3 メール送信元地域別割合（2014 年度）

2014 年度は、年間を通じ、送信元地域がアジアの 4 地域（「日本」、「香港」、「韓国」、「中国」）と「アメリカ」のみが確認され、この 5 地域で全体の半数を占める結果となった。また、「日本」が初めて 1 位となっており、実際に攻撃者が国内に居る可能性もあるが、その他、攻撃者が国内のマシンを乗っ取って攻撃の踏み台に使用したり、**不正な中継（代理）サーバサービス** [7]を悪用しているものと思われる。いずれにせよ、これは**攻撃インフラ（攻撃行為に使用するマシン等の基盤）が着々と国内に築かれつつある可能性**を示しており、今後とも注意が必要な傾向である。

また、「不明」の割合が 49%（246 件）と 2012 年度および 2013 年度より増加している。この内訳は、48 件がメールのヘッダ情報が確保できてなかったもの、198 件がメールヘッダに送信元の痕跡が残っていなかったものであった。

参考として、2012 年度および 2013 年度のグラフを「図 4 （参考）メール送信元地域別割合（2012 年度、2013 年度）」に示す。

---

[6] ホスト名から得られる 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。また、攻撃者は攻撃メールを送信する際、身元を隠すために乗っ取った第三者のマシンの悪用等をしている可能性があり、この統計にある地域が攻撃者の居場所であるとは限らない。

[7] サイバー攻撃を行う際の通信の中継点として悪用できるマシンが業者によって有料で提供されていた事例があり、問題となっている。

「「中継サーバー」一斉捜索、中国人運営業者ら逮捕　警視庁などの合同捜査本部」（産経ニュース）
http://www.sankei.com/affairs/news/141119/afr1411190029-n1.html

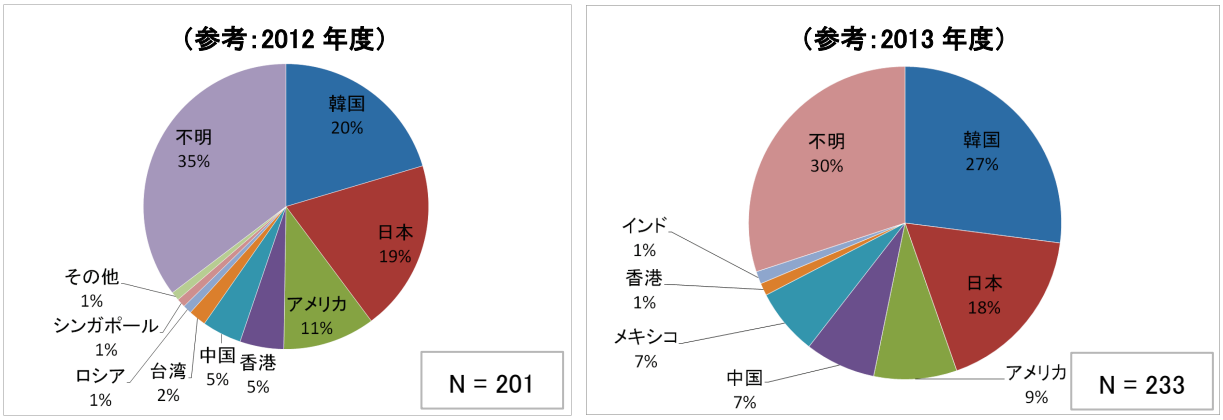


図 4 （参考）メール送信元地域別割合（2012 年度、2013 年度）

続いて、四半期ごとの推移を「図 5 メール送信元地域別件数推移（2014 年度）」に示す。送信元が「不明」のケースは、年間を通して継続的に高い割合で観測された。その他の地域の観測状況は、時期によってばらつきが見られた。

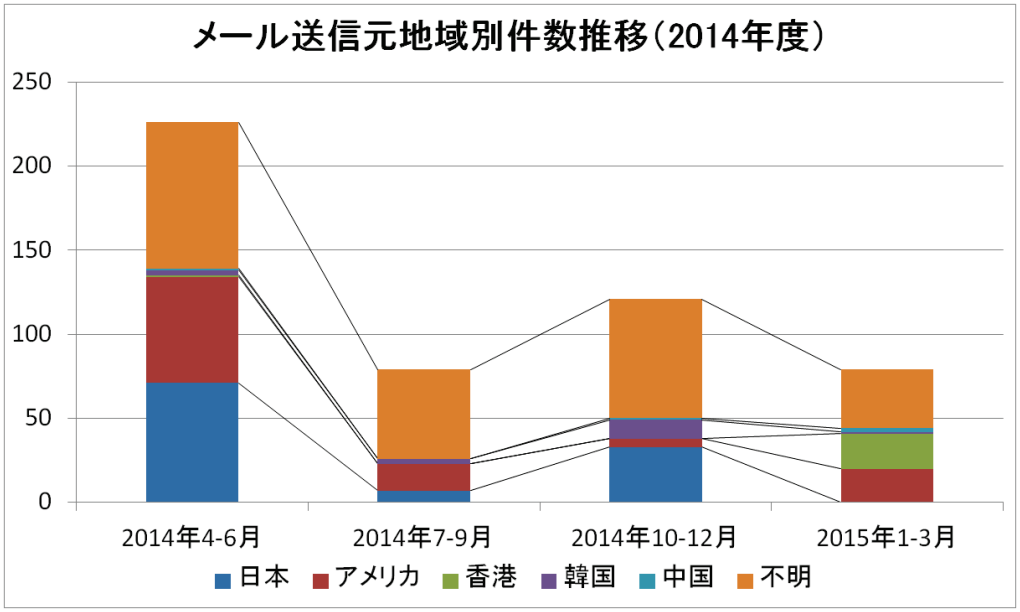


図 5 メール送信元地域別件数推移（2014 年度）

3.3 不正接続先地域別割合

標的型攻撃メールと見なしたメール等から取得したウイルス等の不正接続先の地域別割合を「図 6 不正接続先地域別割合（2014 年度）」に示す[8]。不正接続先は、ドライブ・バイ・ダウンロード攻撃[9]を行ったり、ウイルスに感染させたマシンへ更なる別のウイルスを感染させたり、マシンを遠隔操作するために使われる、攻撃者がある程度継続して管理下に置いて悪用していると考えられるサーバである。

「不明」は、調査の時点で接続先のホスト名に対応した IP アドレスが得られなかったものである。

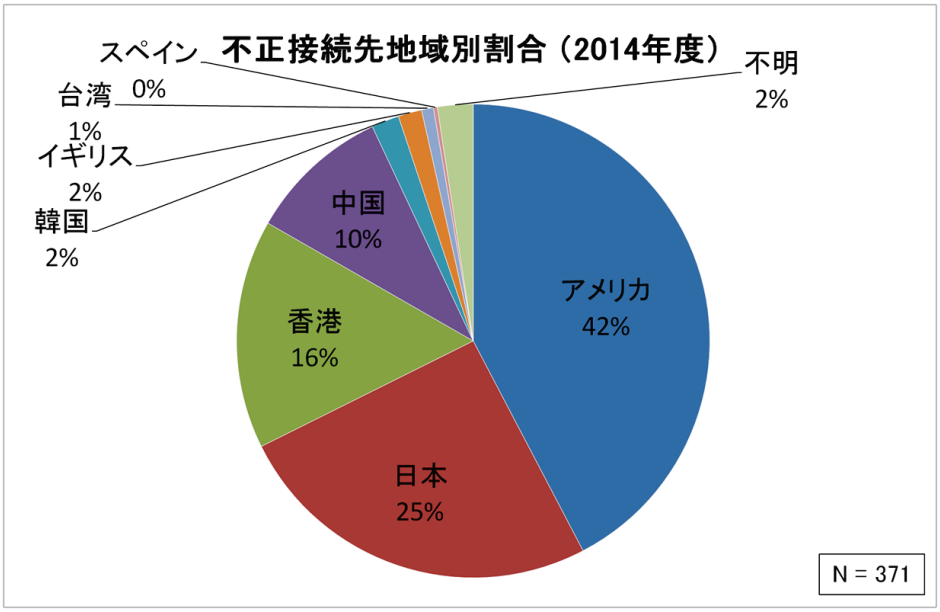


図 6 不正接続先地域別割合（2014 年度）

不正接続先の地域別割合も、メール送信元地域別割合と同様、アジアの 4 地域（「日本」、「香港」、「韓国」、「中国」）、と「アメリカ」が多数となった。これら 5 地域が占める割合は、2012 年度は 73%、2013 年度は 79%と増加してきており、2014 年度は 95%と大幅増となっている。

「日本」については、2013 年度と同様に、国内の正規のウェブサイトが攻撃者に乗っ取られ、ウイルスの不正接続先として悪用されていたと思われるケースを多く確認した。攻撃者は、ウイルスによる不正な通信が発見される可能性を低くするため、システム管理者やネットワーク監視機器等による通信の検査に対し、不審だと見抜きにくい地域のサーバを通信先として悪用しているものと考えられる。この傾向は昨年度も多く見られ、継続している。

IPA では、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・復旧等の調整（コーディネーション）を行っている。

---

[8] 「スペイン」は 1%未満であったため、グラフ上は 0%となっている。

[9] 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）
https://www.ipa.go.jp/security/txt/2010/12outline.html

参考として、2012 年度および 2013 年度のグラフを「図 7 （参考）不正接続先地域別割合（2012 年度、2013 年度）」に示す。

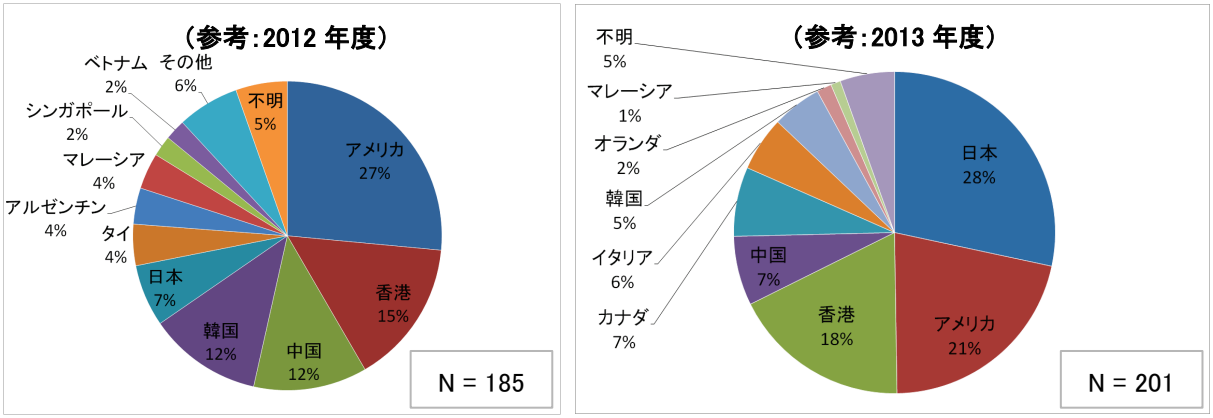


図 7 （参考）不正接続先地域別割合（2012 年度、2013 年度）

続いて、四半期ごとの推移を「図 8 不正接続先地域別件数推移（2014 年度）」に示す。「日本」は継続的に一定の割合で観測された。これらのホスト名は時期により異なっているが、ホスト名に対応する IP アドレスは同一のホスティング業者の IP アドレス帯であることが多く見られ、長期に渡り攻撃インフラとして悪用されていた可能性がある。

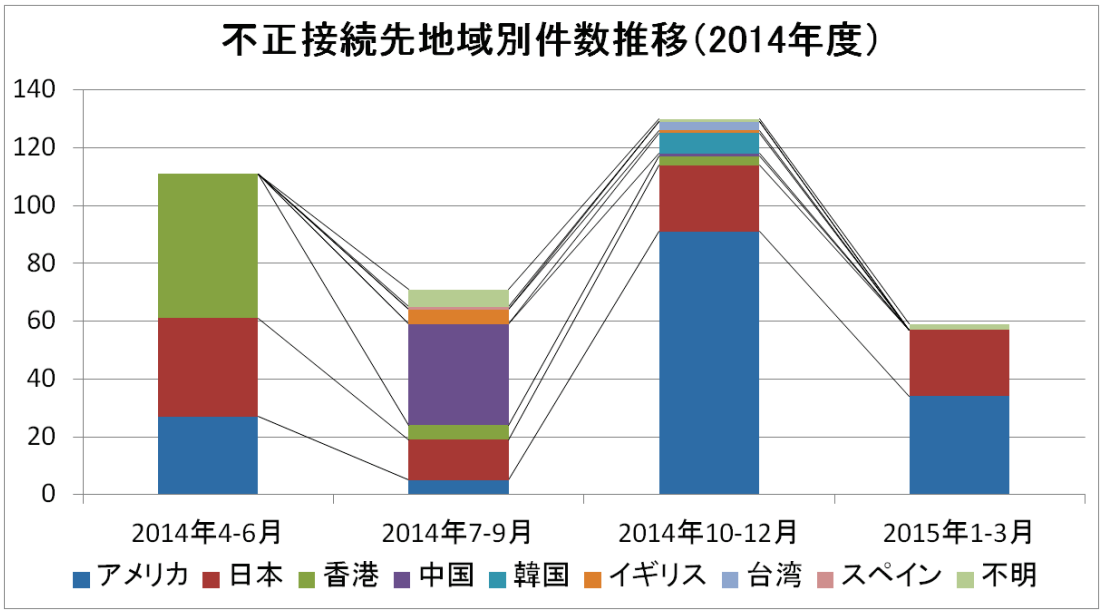


図 8 不正接続先地域別件数推移（2014 年度）

3.4 メール種別割合

標的型攻撃メールと見なしたメールで使用された攻撃手口の割合を「図 9 メール種別割合（2014 年度）」に示す。分類の意味は次の通りである。

（1） 添付ファイル

ウイルスに感染させる悪意のあるファイルをメール添付し、それを開かせようとする手口。

（2） URL リンク

メールの本文中に URL リンクを記載し、そのウェブサイトからウイルスをダウンロードさせる、もしくはドライブ・バイ・ダウンロード攻撃やフィッシング等を行う手口。

（3） 情報収集

添付ファイルや URL リンクの無い無害なメールだが、送信先メールアドレスの存在の確認や、標的型攻撃の準備段階として送信されたと考えられるもの。メールのやり取りの後で攻撃メールを送信してくる手口（「やり取り型」攻撃）に関わるメールを含む。

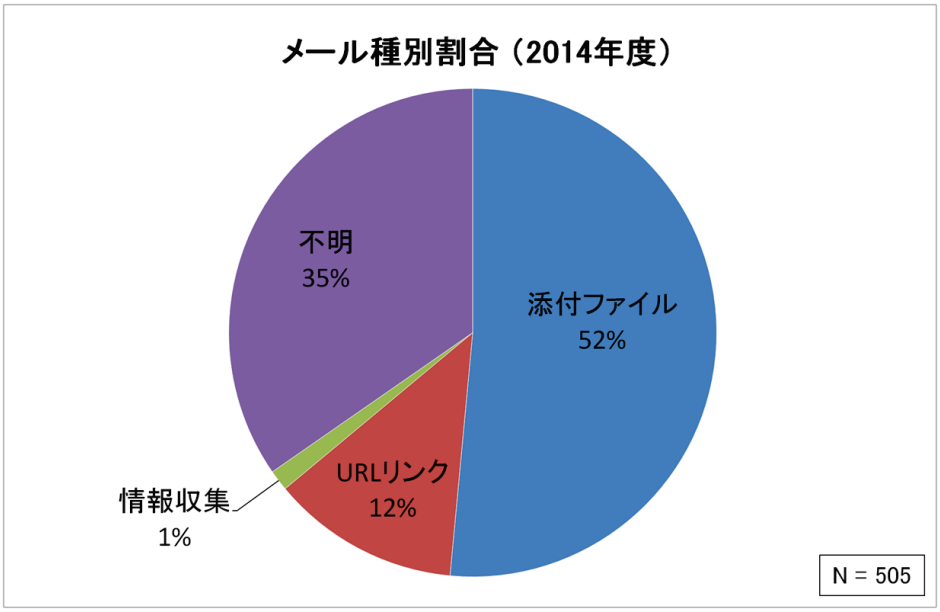


図 9 メール種別割合（2014 年度）

この統計では、2012 年度、2013 年度と同様、「添付ファイル」が半数以上を占めた。更に、2013 年度の 13%から 35%と 3 倍近く増加した「不明」についても、**実際にはそのほとんどに悪意のある添付ファイルが付いていたと推定できるものであった**[10]。

「URL リンク」は、**2013 年度と攻撃の傾向が変化した**。2013 年度はドライブ・バイ・ダウンロード攻撃を試みると思われる URL リンクが多数であったが、**2014 年度は偽の社内システムのログインサイトに誘導する攻撃**（フィッシング）が見られた。**偽のログインサイトで利用者に ID とパスワードを入力させ、それらの情報を窃取することで、不正アクセスを行う目的の攻撃**と思われる。

参考として、2012 年度および 2013 年度のグラフを「図 10 （参考）メール種別割合（2012 年度、2013 年度）」に示す。

[10] メールや添付ファイルが検疫・削除されていたといった理由で、IPA に提供された情報が断片的なもの等、添付ファイルの存在が確認できなかったものについては、この統計では「不明」としている。

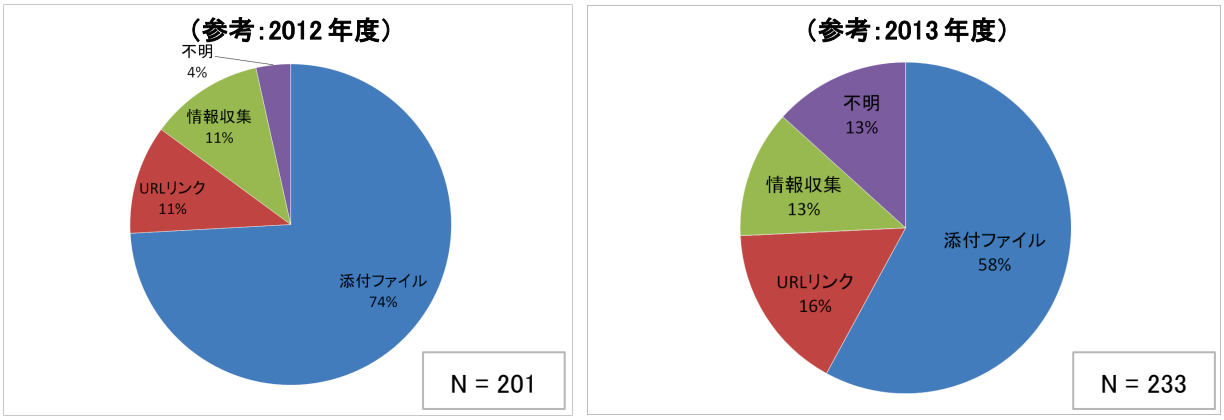


図 10 （参考）メール種別割合（2012 年度、2013 年度）

続いて、四半期ごとの推移を「図 11 メール種別件数推移（2014 年度）」に示す。

2014 年 4-6 月は複数の攻撃者（または攻撃グループ）が同時に活動したと思われ、一時的に件数が倍増した。この時期は同等の攻撃がある程度の期間継続したため、各参加組織でのセキュリティ対策や J-CSIP での情報共有による防御が進み、攻撃メールを検疫・削除できたケースが多く報告された。「不明」が多くなっているのは、防御が成功し、IPA へ提供される情報が断片的なものとなったためである（例えば、攻撃メールと思われるメールの着信は確認したが、着信拒否したり添付ファイルは検疫・削除済み、といった情報提供がこれにあたる）。

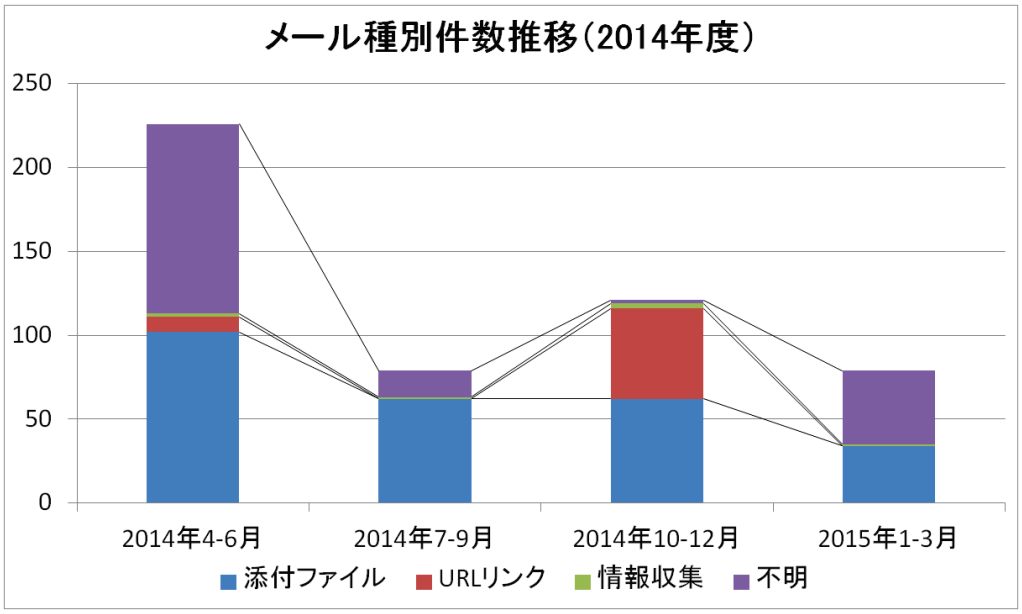


図 11 メール種別件数推移（2014 年度）

3.5 添付ファイル種別割合

3.4 節「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 12 添付ファイル種別割合（2014 年度）」に示す。

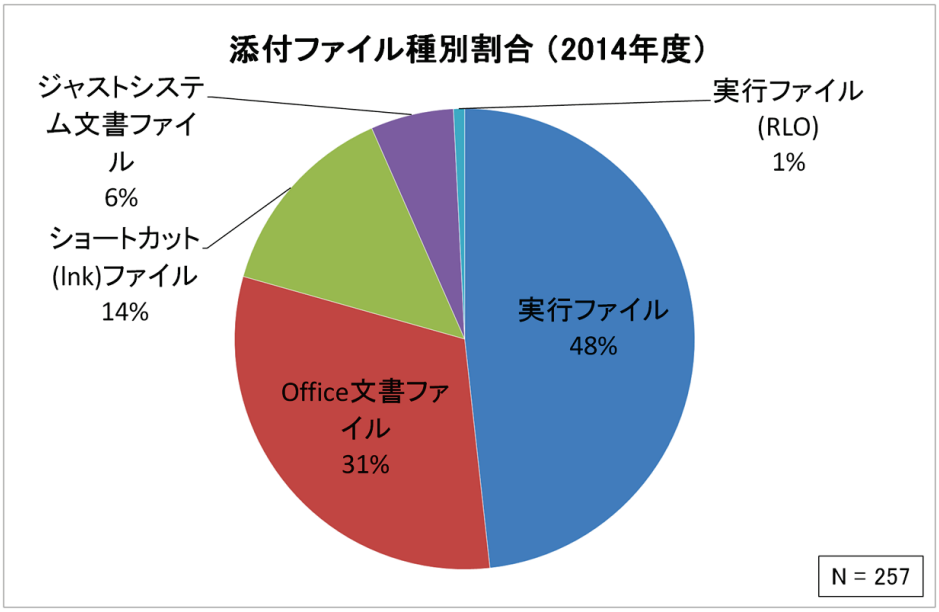


図 12 添付ファイル種別割合（2014 年度）

「実行ファイル」が半数を占める傾向は 2012 年度・2013 年度から継続している。受信者を油断させてファイルを開かせる手口として、アイコンを文書ファイル等に見せかける、二重に拡張子を付ける、RLO[11]を使って拡張子を偽装するといった手口が使われていた。この傾向は今後も続くと思われるため、利用者に対して実行ファイル（やショートカットファイル）を誤って開かないよう改めて注意を徹底するとともに、これらのファイルが添付されたメールが利用者の手元に届かないような、システム的な対策を検討すべきである。

「Office 文書ファイル」は、2013 年度の 8%から 31%に増加した。脆弱性が公開された場合、修正プログラムの迅速な適用はもとより、修正プログラムが提供されていない場合でも、Fix it 等の回避策が適用できるような組織内体制の整備が望ましい。

また、「Office 文書ファイル」では、2014 年度後半、マクロ機能を悪用する攻撃が初めて確認された。悪意のあるマクロが仕掛けられた Office 文書ファイルを開いてしまっても、マクロの実行を許可しなければ被害は生じない。利用者に対し、不用意に Office 文書ファイルのマクロの実行を許可しないように周知徹底していただきたい。

他には、「ジャストシステム文書ファイル」（一太郎や三四郎の文書ファイル）について、2013 年 11 月に修正プログラムが公開された脆弱性「CVE-2013-5990」を悪用するものが観測された。また、「ショートカット（LNK）ファイル」は、J-CSIP では 2013 年度に初めて観測した後、継続的に観測されており、攻撃手口の一つとして確立したものと思われる。

参考として 2012 年度および 2013 年度のグラフを「図 13 （参考）添付ファイル種別割合（2012 年度、2013 年度）」に示す。

[11] 「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）
https://www.ipa.go.jp/security/txt/2011/11outline.html

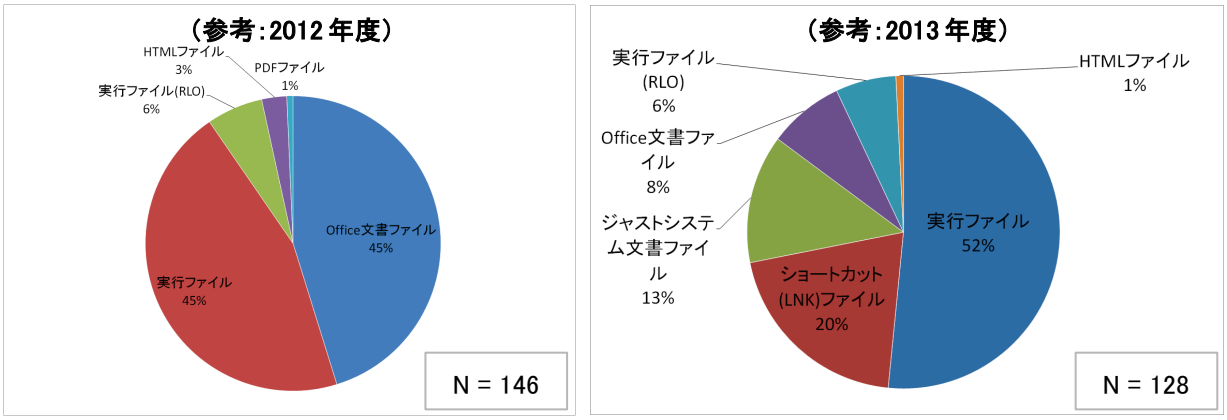


図 13 （参考）添付ファイル種別割合（2012 年度、2013 年度）

続いて、四半期ごとの推移を「図 14 添付ファイル種別件数推移（2014 年度）」に示す。

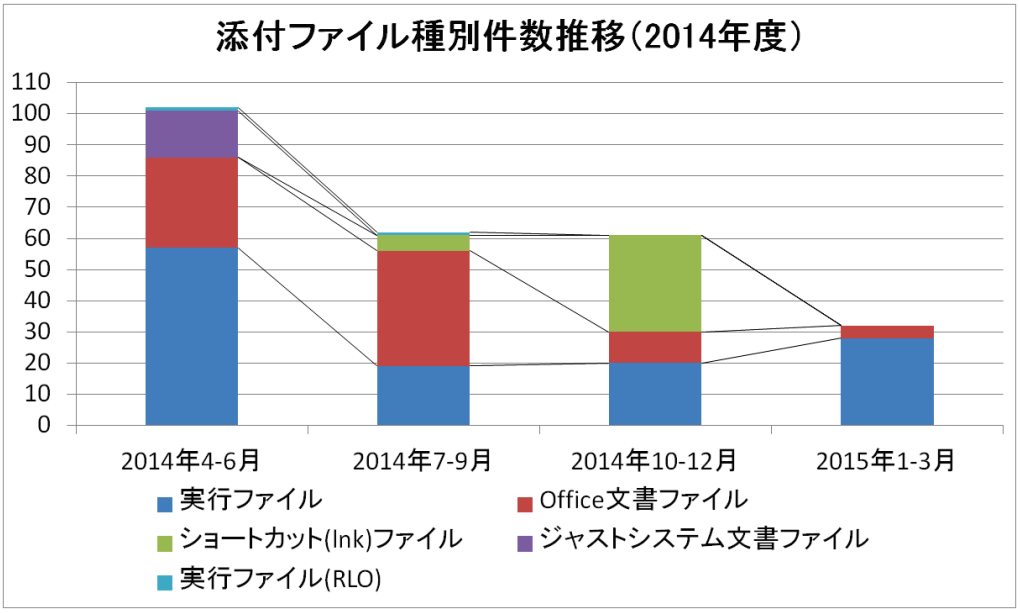


図 14 添付ファイル種別件数推移（2014 年度）

3.6 送信元メールアドレスの傾向

標的型攻撃メールと見なした 505 件のメールの送信に使われたメールアドレスの種別の割合を「図 15 送信元メールアドレス種別割合（2014 年度）」に示す。図中、「不明」は、断片的な情報の提供であったため、送信元メールアドレスが確認できなかったものである。

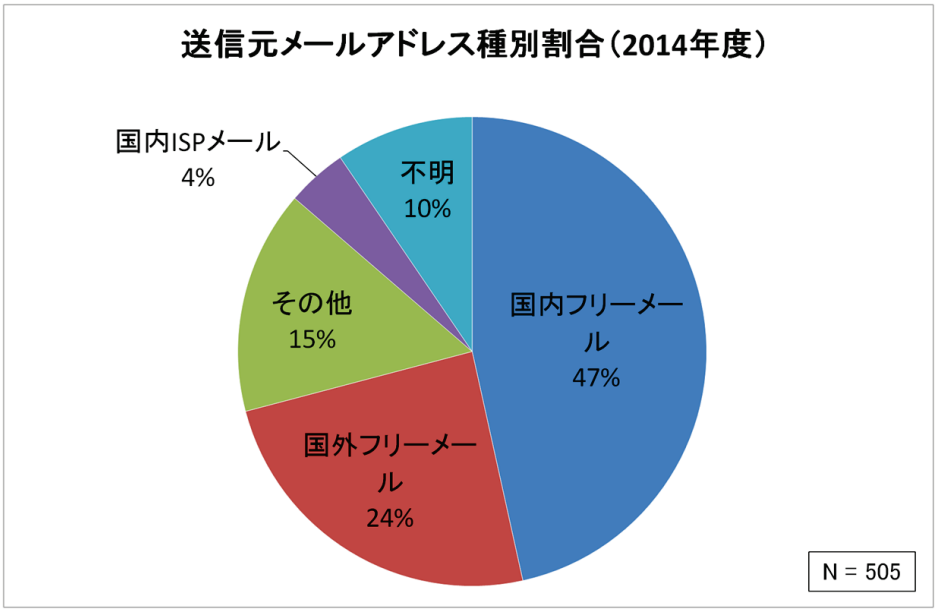


図 15 送信元メールアドレス種別割合（2014 年度）

「国内フリーメール」および「国外フリーメール」は、それぞれ主に日本国内または国外の利用者向けにサービスを行っているフリーメールのメールアドレスが使われていたもので、これらが全体の 1 位と 2 位となり、合わせて 71%と高い割合を占めた。この傾向は 2013 年度から変わっていない。業務上、フリーメールからのメールを完全に拒否したり無視することは難しいかもしれないが、これらのメールを開封するリスクが高いことに間違いはないため、例えば、次のような対策を検討していただきたい。

- メール送信元がフリーメールサービスであった際、メールシステムにて、メール件名や本文に当該メールの受信者向けの警告メッセージを付加し、注意を促す。
- フリーメールからのメールについて、特に不要と考えられる部門の利用者には届かないようにする（ホワイトリスト方式等を併用してもよい）。

4%の「国内 ISP メール」は、国内の ISP 契約に付随して利用者へ発行されていると考えられるメールアドレスで、攻撃者が当該アカウントを乗っ取る等して悪用した可能性のあるものである。また、15%の「その他」は、フリーメールでも ISP メールでもないメールアドレスで、攻撃者が企業や組織のメールアドレスを詐称、または乗っ取った上で送信したと思われる、なりすまし攻撃メールであった。

乗っ取られた正規のメールアドレスから攻撃メールが送られた場合、不審であると見破るのが一層困難になる。利用者においては、ウイルスや不正アクセス等でアカウントを乗っ取られた場合、そのメールアドレスが標的型攻撃メールの送信に悪用され、結果的に、攻撃へ加担してしまうことになる。身に覚えのないメールが自分のメールアドレスから送られたといった連絡を受けた場合は、アカウントが乗っ取られていないか、ただちに確認し、パスワードの変更等の対策を行っていただきたい。

参考として、2013 年度のグラフを「図 16 （参考）送信元メールアドレス種別割合（2013 年度）」に示す。

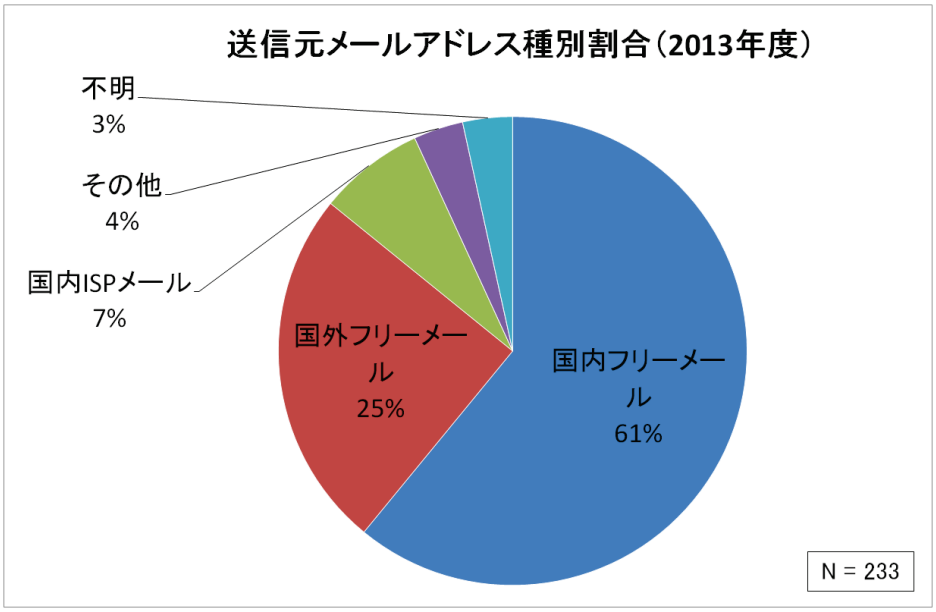


図 16 （参考）送信元メールアドレス種別割合（2013 年度）

3.7 まとめと対策

全体的な傾向は 2012 年度・2013 年度から大きな変化がないものの、国内のマシン（IP アドレス）や国内向けのフリーメールサービスが攻撃に悪用されている状況が続いており、3.2 節で述べた通り、攻撃インフラ（攻撃行為に使用するマシン等の基盤）が着々と国内に築かれつつある可能性を示している。この点については、JPCERT/CC と連携し対応を行っているところであるが、攻撃者により不正に悪用されている状態を放置しないよう、インターネットを利用している全ての利用者、各種サービス提供者、サーバ管理者の方々の協力が不可欠である。不自然な点に気付いた際、あるいは、自分の管理下にあるアカウントやマシンが不正なメールや通信に関係があると連絡を受けた場合は、サイバー攻撃に加担してしまっている可能性を考え、迅速に対応していただきたい。

また、攻撃手口では Office 文書ファイルのマクロ機能を悪用する攻撃が新たに確認された。マクロ機能は、実行ファイル、ショートカット（LNK）ファイルと同様、脆弱性を悪用せずにパソコンへウイルスを感染させることが可能であり、脆弱性対策だけでは防げない攻撃手法が増えたことになる。

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、改めて徹底することが、標的型攻撃メールの回避に重要である。

- 全てのソフトウェア（OS、各種アプリケーション）を常に最新にしておくこと
  - 最新の脆弱性の情報に注意を払うこと
  - 製造元のウェブサイトからアップデートモジュールをダウンロードして手動で適用しなければならないソフトウェアに注意すること
- 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
  - ショートカット（LNK）ファイルのような、一見危険なファイルには見えないようなものもあるため、エクスプローラでファイルの「種類」欄をよく確認すること
- 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
  - 特にフリーメールについては、国内のサービスのものであっても、十分に注意すること
  - 問い合わせ窓口等に対し無害なメールをやり取りした後で攻撃メールを送信してくる手口に注意すること
- 外部から取得した Office 文書ファイルのマクロを不用意に実行しないこと
  - メールの添付ファイルや社外ウェブサイト等外部から取得した Office 文書ファイルを開く際は、マクロを有効化しないこと
  - マクロを自動的に有効にするような設定は行わないこと

また、3.5 節、3.6 節でも示した通り、次のようなメールサーバ等でのシステム的な対策を検討すべきであろう。

- 実行ファイルやショートカットファイル等の危険な形式のファイルが添付されたメールが受信者の手元に届かないようにする
- フリーメールサービスからのメールの件名や本文に受信者向けの警告を付与する

なお、上記の対策を十分に徹底できたとしても、ある程度のウイルス感染が発生することは避けられないと思われる。仮に職員のパソコン 1 台が乗っ取られてしまっても、それを迅速に検知したり、組織内ネットワークでの攻撃者の行動を抑制し、攻撃の最終目標を達成させにくくする「内部対策」も重要であろう。

IPA の「『高度標的型攻撃』対策に向けたシステム設計ガイド」[12]や、「攻撃者に狙われる設計・運用上の弱点についてのレポート」[13]では、標的型攻撃の全体像や、講じるべき対策について論じているため、それらも参照していただきたい。

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。

- 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を除き、標的型攻撃メールと見なしたものを統計対象としているため、「メール送信元地域別割合」、「メール種別割合」、「送信元メールアドレスの傾向」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。

[12] 「『高度標的型攻撃』対策に向けたシステム設計ガイド」の公開（IPA）（再掲）
https://www.ipa.go.jp/security/vuln/newattack.html

[13] IPA テクニカルウォッチ：「攻撃者に狙われる設計・運用上の弱点についてのレポート」（IPA）
https://www.ipa.go.jp/security/technicalwatch/20140328.html

4　さいごに

本書の別冊**「国内組織を狙う執拗な攻撃者「X」の分析」**にて、J-CSIP の 3 年間の活動で得られた情報を基に、横断的な分析を行った成果を示している。こちらについても、是非参照していただきたい。

3 章の統計情報、および別冊にて詳しく述べているとおり、国内組織を狙う攻撃者は間違いなく存在し、その手口も巧妙化している。様々なシステム面での対策に加え、まずは、自組織に対してどの程度の攻撃が行われているのかの把握が必要であろう。組織内の CSIRT やシステム管理部門において、重要部門等の組織の一部からであっても、攻撃情報を集約・共有する取り組みに着手していただきたい。

また、それらの情報を IPA（J-CSIP や特別相談窓口等）に提供いただくことにより、当該情報の分析の支援だけでなく、他組織での活用とそのフィードバック情報の共有を通し、より多面的で横断的な分析に繋げることができる。

J-CSIP は、2015 年度以降も情報共有の運用を着実に行い、また、参加組織の拡大、効率の向上等を図っていくとともに、情報の集約と横断分析によって得られる情報等、共有する情報の拡充を進めていく。そして、J-CSIP 外の組織とも連携を進めながら、情報の共有と集約を通し、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。

（参考） 経済産業省・関係機関情報セキュリティ連絡会議

「経済産業省・関係機関情報セキュリティ連絡会議（通称：独法連絡会）」[14]とは、経済産業省が事務局として 2013 年 7 月に設置した、経済産業省、同省所管および共管の 12 の独立行政法人（以下、独法）等で構成する会議体である（2014 年度、経済産業省の共管独法が新たに参画するようになった）。

独法連絡会は、2013 年 6 月の情報セキュリティ対策推進会議（CISO 等連絡会議）第 10 回会合において要請 [15]された、独法におけるセキュリティ強化の一環として設置されたものであり、更に、独法連絡会の中で、J-CSIP をモデルとした標的型攻撃メール等の情報共有を行う「脅威情報共有ワーキンググループ」を 2013 年 8 月に設置した。このワーキンググループの事務局は、IPA だけではなく、経済産業省と JPCERT/CC の三者で運営を行っている。

参考として、体制図を「図 17 独法連絡会と脅威情報共有 WG 体制図（経済産業省資料抜粋）」に示す。情報共有のルールや運用フローについては、IPA が J-CSIP を運用してきた知見を活用し、円滑な立ち上げを行うことができた。2014 年度は、情報共有の実運用を開始している。

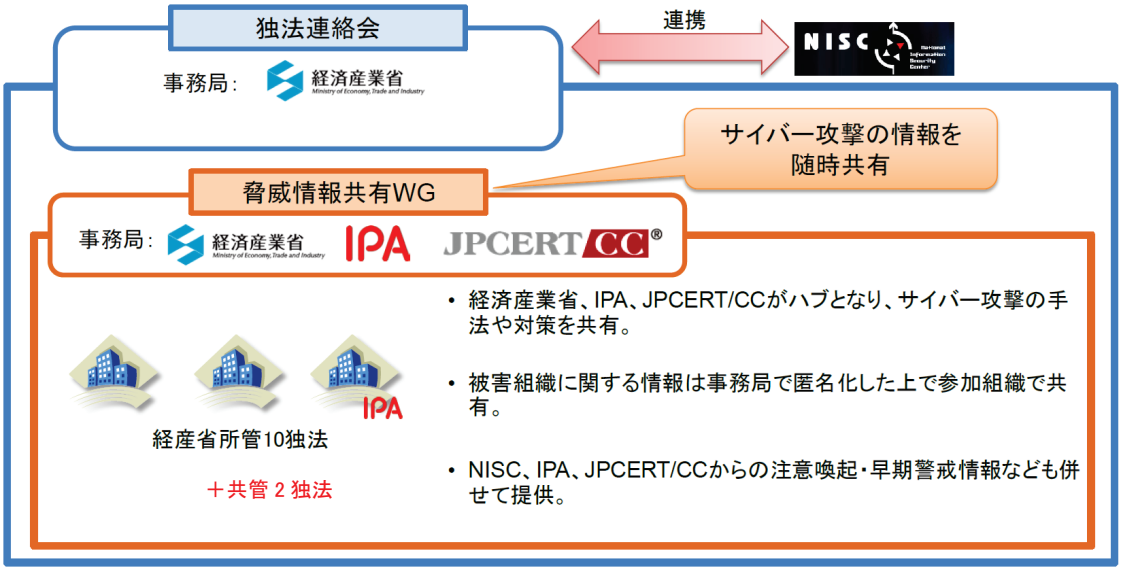


図 17 独法連絡会と脅威情報共有 WG 体制図（経済産業省資料抜粋）

※ 赤字は IPA 加筆

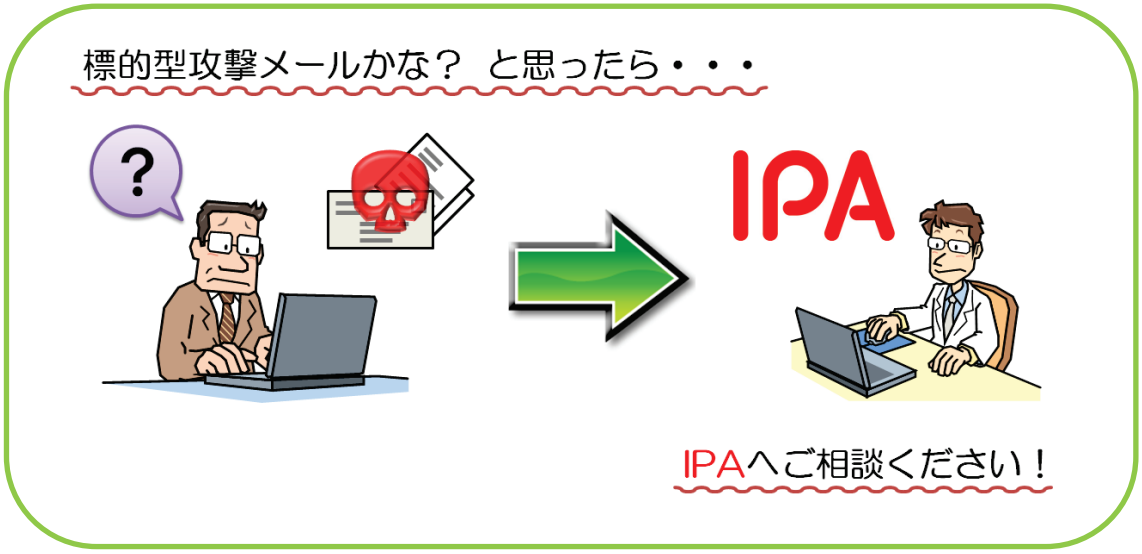
[14] 情報セキュリティ対策推進会議（CISO等連絡会議） 第16回会合（平成26年3月19日）
資料 2-2 「〔経済産業省提出資料〕経済産業省・関係機関情報セキュリティ連絡会議（独法連絡会）」
http://www.nisc.go.jp/conference/suishin/ciso/dai16/pdf/2-2.pdf

[15] 情報セキュリティ対策推進会議（CISO等連絡会議） 第10回会合（平成25年6月19日）
資料 1 「政府におけるサイバー攻撃への迅速・的確な対処について（案）」
http://www.nisc.go.jp/conference/suishin/ciso/dai10/pdf/1.pdf

「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