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）
2013 年度 活動レポート
～「やり取り型」攻撃に関する分析情報の共有事例 ～

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）

2013 年度 活動レポート

～ 「やり取り型」攻撃に関する分析情報の共有事例 ～

目次

添付資料

サイバー情報共有イニシアティブ（J-CSIP）

2013 年度 活動レポート

～「やり取り型」攻撃に関する分析情報の共有事例 ～

2014 年 5 月 30 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、2013 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。
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。 IPA の「『標的型メール攻撃』対策に向けたシステム設計ガイド」[2]では、この攻撃手口の全体像と、対策ポイントを紹介している。
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] 「『標的型メール攻撃』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　2013 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 2 年間の情報共有活動を続け、2014 年 4 月からは 3 年目の運用に入った。情報共有活動は、参加組織による情報提供をはじめとする積極的な関与なくしては成立せず、ここに深く謝意を示したい。

本書では、J-CSIP の 2013 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 2013 年度の活動成果の概要は次の通りである。

- 参加組織が **7 組織追加**となり、**5 つの業界**、**46 組織**での情報共有体制となった。
- **180 件**の情報共有を実施した（前年度の情報共有件数は 160 件）。
- 内閣官房情報セキュリティセンター（NISC）が事務局を務めるセプターカウンシルとの情報連携の運用を開始した。

2012 年度に引き続き、2013 年度は標的型攻撃メールに関する情報共有を継続的に行った。各参加組織から IPA へ日々情報提供が行われており、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開催しており、事例を掘り下げての分析、攻撃間の相関の分析、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等を行っている。

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。4 章では、「やり取り型」攻撃に関する分析情報を共有した具体的な事例紹介を通し、情報共有活動の有効性について示す。

なお、J-CSIP の活動に関連し、経済産業省の所管 10 独法が参加する「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）」において、IPA は、J-CSIP の運用知見をもとに、J-CSIP 同様の情報共有体制の事務局を担うことになった。本件については、本書のまとめとともに、参考情報として 5 章に示す。

[3] 2012 年度の活動状況については、次の文書で報告している。
「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）
https://www.ipa.go.jp/files/000028304.pdf

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 については、「2012 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[4]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 5 月現在	5 業界 46 参加組織にて情報共有体制を運用中

セプターカウンシル「C4TAP」との相互情報連携開始（2013 年 6 月）

2013 年 6 月より、内閣官房情報セキュリティセンター（NISC）が事務局を務めるセプターカウンシル [5]における標的型攻撃に関する情報共有体制、通称「C4TAP」[6]（Ceptoar Councils Capability for Cyber Targeted Attack Protection、シータップ）との間で、相互の参加組織（情報提供元）の許可に基づき、情報を連携する運用を開始した。

セプターカウンシルには業種分野別の 16 のセプターが参加 [7]しており、C4TAP には、その中から約 350 組織（運用開始時点）が参加している。C4TAP との相互情報連携を開始したことにより、J-CSIP に参加していない業種分野の組織・企業と標的型攻撃に関する情報の授受が可能となった。

参加組織の拡充（2013 年 6 月～7 月、2014 年 2 月）

2013 年度は、ガス業界 SIG に 6 組織、化学業界 SIG に 1 組織、J-CSIP へ新たに参加することとなり、J-CSIP は 5 業界 46 参加組織の情報共有体制となった。IPA は、既存の参加組織の活動状況の紹介等を通じ、引き続き参加組織の拡充を計っていく予定である。

---

[4] SIG：Special Interest Group の略。J-CSIP では、同業界の組織で構成する情報共有のグループを指す。

[5] 「重要インフラの情報セキュリティ対策に関する取組み」（NISC） 参照。
http://www.nisc.go.jp/active/infra/torikumi.html

[6] 「標的型攻撃に関する情報共有体制（C4TAP）」（NISC） 参照。
http://www.nisc.go.jp/active/infra/pdf/cc_kyouyuu2.pdf

[7] 「セプターカウンシル総会第6回会合の開催について（セプターカウンシルの概要）」（NISC） 参照。
http://www.nisc.go.jp/active/infra/pdf/cc_dai6.pdf

1.4 情報共有体制 全体図

2014 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。

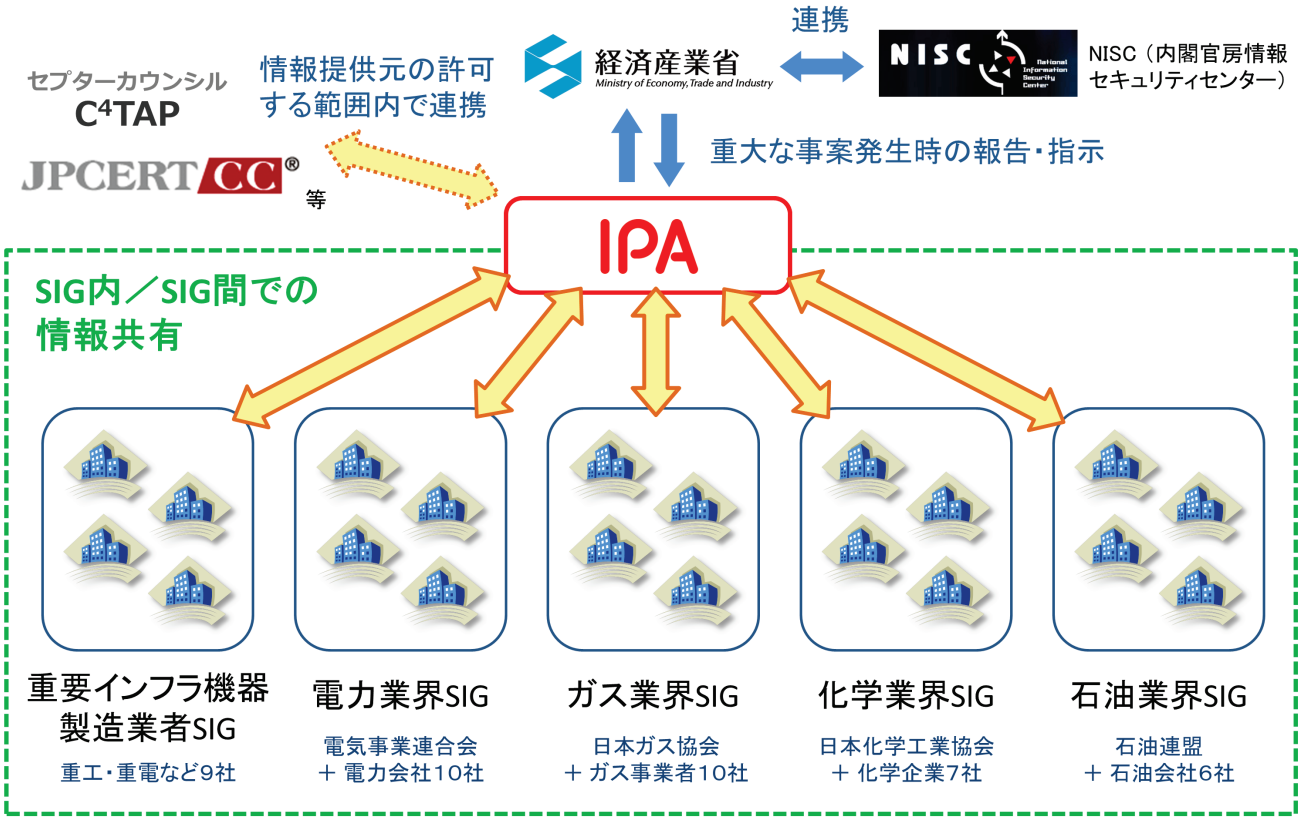


図 1 J-CSIP 情報共有体制 全体図

「2012 年度 活動レポート」でも述べている通り、J-CSIP は次の体制で運用を行っている。

- 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、業種ごとのグループである「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「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（内閣官房情報セキュリティセンター）との連携を行う。

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（2013 年度合計）」および「表 3 実施件数（2013 年度・四半期ごと）」に示す。数値は 5 つの SIG、全 46 参加組織での合算である。

表 2 実施件数（2013 年度合計）

項番	項目	件数	（前年比）	（2012 年度）
1	IPA への情報提供件数※1	**385 件**	**（157%）**	（246 件）
2	参加組織への情報共有実施件数※2	**180 件**	**（113%）**	（160 件）
3	標的型攻撃メールと見なした件数※3	**233 件**	**（116%）**	（201 件）

表 3 実施件数（2013 年度・四半期ごと）

項番	項目	2013 年 4 月～6 月	2013 年 7 月～9 月	2013 年 10 月～12 月	2014 年 1 月～3 月
1	IPA への情報提供件数※1	74 件	95 件	121 件	95 件
2	参加組織への情報共有実施件数※2	55 件	34 件	51 件	40 件
3	標的型攻撃メールと見なした件数※3	64 件	61 件	51 件	57 件

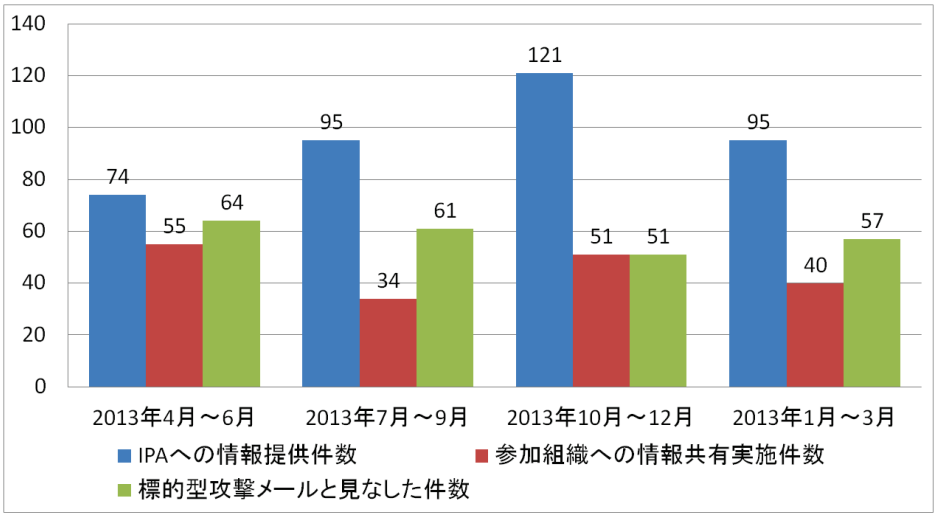


図 2 実施件数（2013 年度・四半期ごと）グラフ

※1 不審なメールの他、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。また、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 年度全体で 37 件）を含む。

※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。

実施件数については、次の傾向が見られた。

- 各月や四半期ごとの情報提供等の数に波はあったが、通年で見た場合は、全体的な件数は一割強の増加となった。なお、参加組織の数は 2012 年度末時点で 39 組織、2013 年度末時点で 46 組織である。
- 情報提供件数については前年度に比べ 1.5 倍以上の増加となった。分析の結果、広く無差別にばら撒かれたウイルスメールであろうと判断するものも多かったが、標的型攻撃メールか否か判断のつかないものについても、参加組織からはより積極的な情報提供が行われるようになっている。不審なメールが実際にどのような脅威なのか、見た目だけでは判断が難しい。IPA は、各参加組織で判断のつかないものについても情報提供を呼びかけており、提供された情報については、全ての内容を確認し、見解を返答するとともに、情報を蓄積して活動に役立てている。

3　統計情報

3.1 概要

情報提供された不審なメールのうち、標的型攻撃メールと見なした **233 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、統計をとった結果、次のような傾向が見られた。

- メール送信元地域は、2012 年度と同じく、韓国、日本、アメリカの順に多く、上位 3 つで全体の半数以上を占めた。
- ウイルス等の不正な通信の接続先地域は、日本が全体の 28%を占め、1 位となった（2012 年度は 7%で 5 位であった）。2 位以降は、アメリカやアジア諸地域等が続いた。
- 不審なメールの 58%はウイルスに感染させるための悪意のある添付ファイルが付いており、16%は不審なウェブサイトへの URL リンクが含まれていた。無害な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）に関するメールも 13%観測された。
- 添付されていた悪意のあるファイルのファイル形式[8]は、実行ファイルが半数以上を占め、2012 年度には観測されていなかったショートカット（LNK）ファイルが 20%、ジャストシステム文書ファイルが 13%観測された。2012 年度に 45%を占めていた Office 文書ファイルは、8%まで減少した。
- メールの送信元メールアドレスは、国内および国外のフリーメールが合わせて 86%を占めた。そのうち、国内のフリーメールが 61%で 1 位となっており、国内外を問わずフリーメールが悪用されていることが分かった。国内 ISP（インターネットサービスプロバイダ）のメールサービスが悪用されていたケースも 7%観測された。

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。

[8] 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を行っている。

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（2013 年度）」に示す [9]。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。

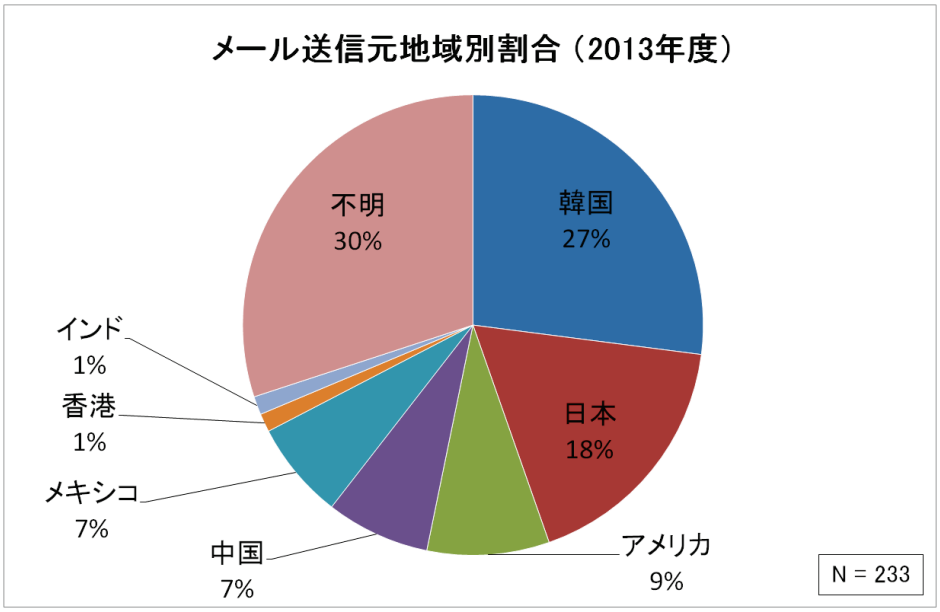


図 3 メール送信元地域別割合（2013 年度）

この統計は四半期ごとでは傾向に差がある一方、一年を通した結果では、グラフの構成が 2012 年度と近い結果となった。まず、2012 年度と同じく、1 位から 3 位は韓国、日本、アメリカの順となっており、この上位 3 つで全体の半数以上を占めた。4 位以降は、中国、メキシコ、香港、インドと続き、アメリカを除いてほとんどがアジア圏である点も 2012 年度と同様であった。7%を占めているメキシコについては、一つの案件に関して同等の複数の情報提供があったもので、観測された IP アドレスは 1 つのみであり、当該地域が広く攻撃に使われたことを示すものではない。

攻撃者が攻撃メールを送信する際は、身元を隠すため、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。しかし、2012 年度と 2013 年度で継続して近い傾向が見られることから、国内組織に対する攻撃を行っている攻撃者たちの「攻撃の際に利用（悪用）しやすい環境」という特徴情報と見ることもできそうである。

30%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。

[9] 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。

参考として、2012 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）」に示す。

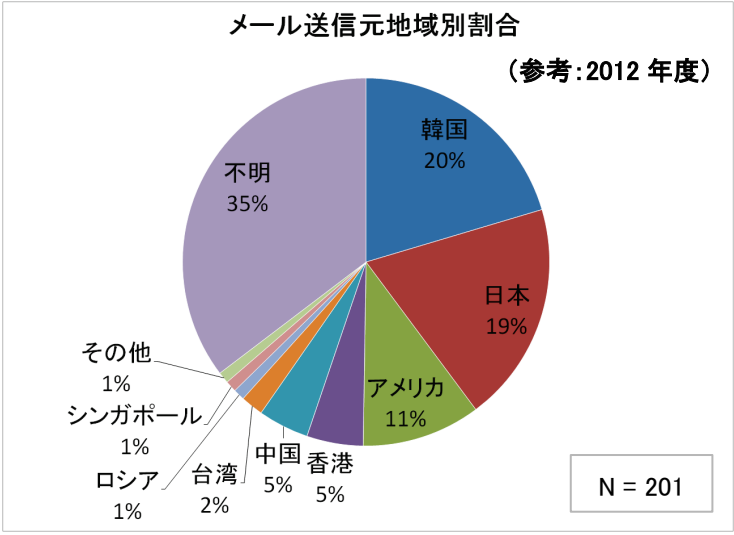


図 4 （参考）メール送信元地域別割合（2012 年度）

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（2013 年度）」に示す。観測状況は時期によってばらつきがあるが、日本国内の IP アドレスが送信元となっていたケースのみ、一年を通して継続的に同程度観測されている。これらは、国内にあるマシンを乗っ取って踏み台にしたり、通信を中継するサーバを悪用していたものと考えられる [10]。

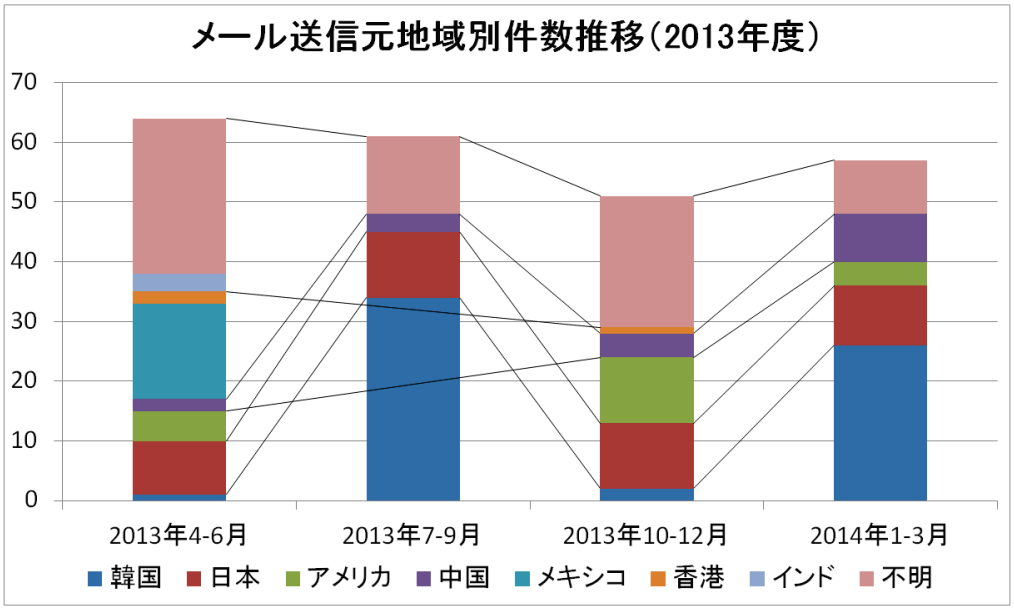


図 5 メール送信元地域別件数推移（2013 年度）

[10] 2014 年 2 月、海外からのインターネット接続を中継するサーバを運営していた会社の社長らが逮捕され、ネットバンキングの不正送金や、ウイルス付きメールの送信に利用されていたとの報道があった。
参考：中国籍の男2人を不正アクセス容疑で逮捕　警視庁と埼玉県警（MSN 産経ニュース）
http://sankei.jp.msn.com/affairs/news/140213/crm14021321280026-n1.htm

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（2013 年度）」に示す。不正接続先は、ドライブ・バイ・ダウンロード攻撃 [11]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いると考えられるサーバである。

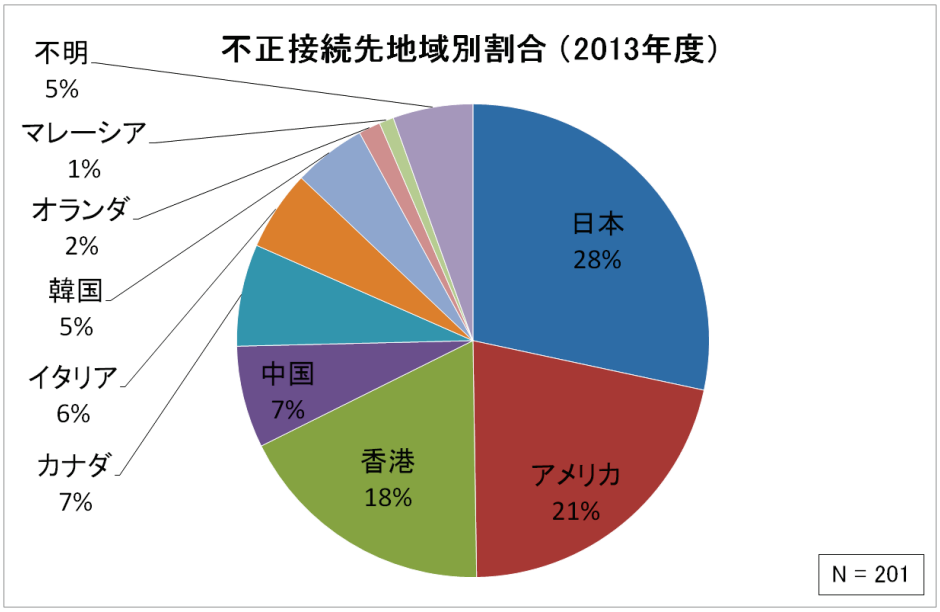


図 6 不正接続先地域別割合（2013 年度）

統計の結果、こちらも 2012 年度と同じような傾向で、アジア諸地域とアメリカで多くの割合を占めており、それに加えて他の地域が少数観測された。

顕著な傾向として、2012 年度では 7%であった日本が、2013 年度ではその 4 倍の 28%、全体で 1 位となったことが挙げられる。これは、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が複数観測されたことが要因である。攻撃者は、ウイルス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等による通信の検査に対して、不審だと見抜きにくい国内のサーバを通信先として悪用する手口へと巧妙化させた可能性がある。

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 [12]等という理由により、不明であった。

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。

---

[11] 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

[12] 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。

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

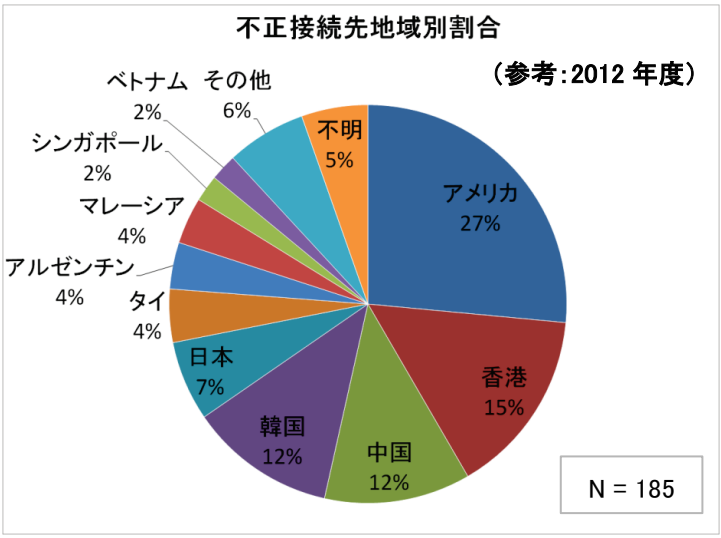


図 7 （参考）不正接続先地域別割合（2012 年度）

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（2013 年度）」に示す。日本国内のサーバが悪用されていた期間は限定的で、四半期ごとに増加と減少が見られる。日本以外では、2013 年度全体で 2 位から 4 位となっているアメリカ、香港、中国が継続して観測されており、他の地域は一時的に観測されたものであった。

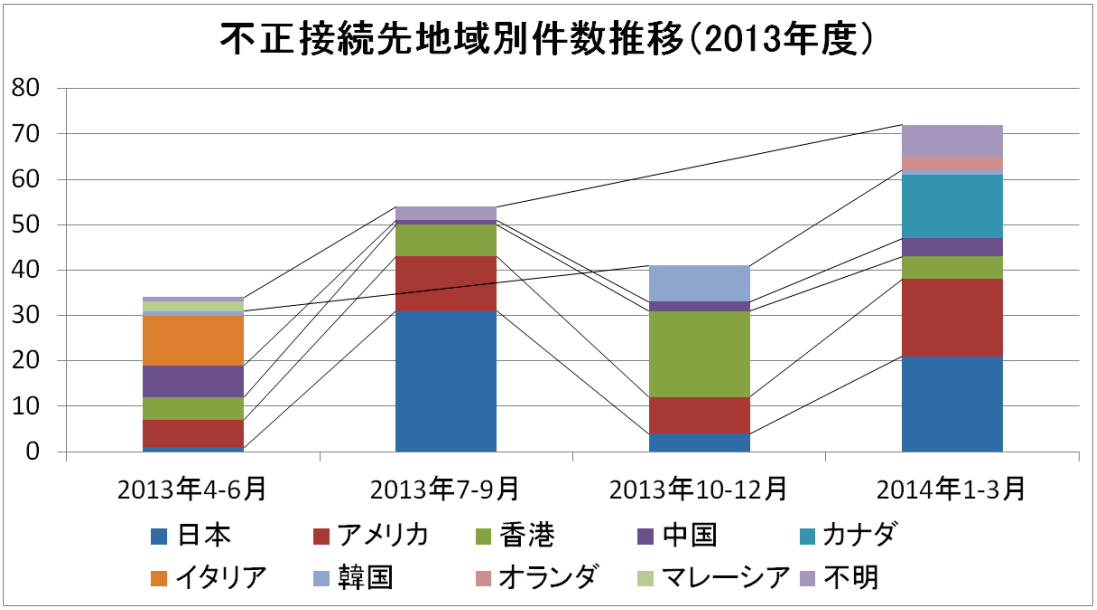


図 8 不正接続先地域別件数推移（2013 年度）

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（2013 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たり、ドライブ・バイ・ダウンロード攻撃等を行うと思われる手口。

（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。

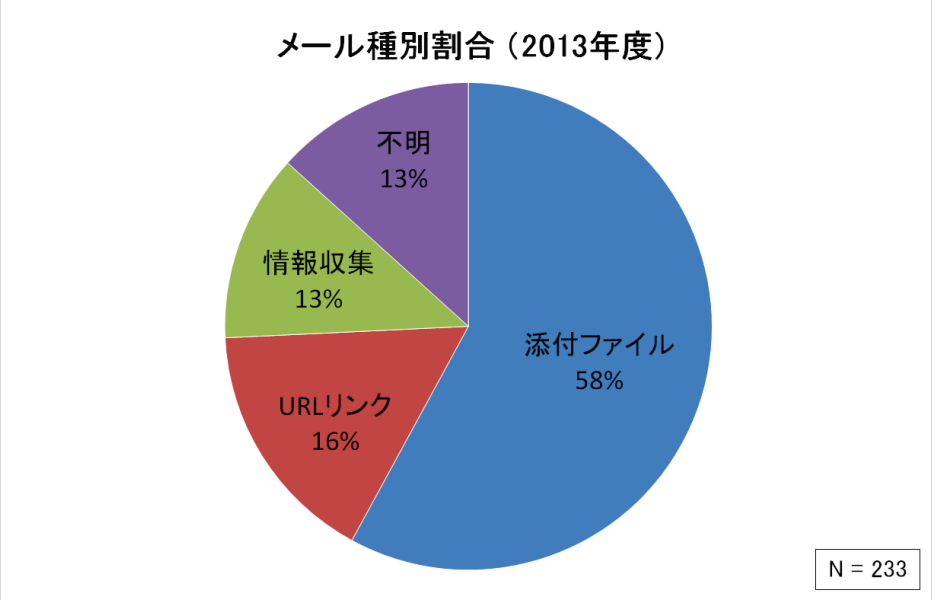


図 9 メール種別割合（2013 年度）

この分類では、「添付ファイル」が全体の 6 割弱を占め、「URL リンク」と「情報収集」がそれに続いた。添付ファイルとしてウイルスを送りつける手口が 2012 年度と同様に多いということになるが、URL リンクによるドライブ・バイ・ダウンロード攻撃を試みたと思われるものも 11%から 16%に増加しており、注意が必要である。

また、いきなり添付ファイルでウイルスを送るのではなく、無害なメールで会話を行った後にウイルスを送る「やり取り型」攻撃も、2012 年度から引き続き観測されている状況である。この攻撃手口については 4 章で詳しく述べる。

残りの「不明」は、得られた範囲の情報から、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思われるものであったが、メールや添付ファイルが検疫・削除されてしまっていたり、不審なメールが着信したと思われるログ等にとどまる情報提供であり、IPA が手口を確認できなかったものである。

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

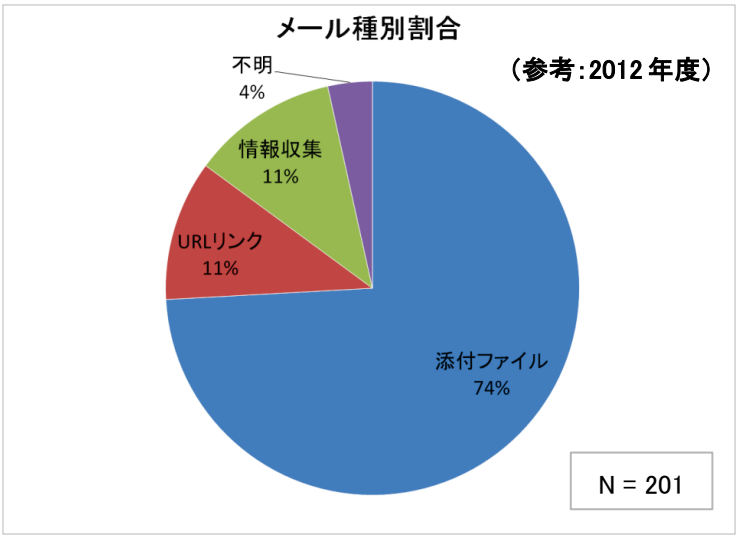


図 10 （参考）メール種別割合（2012 年度）

続いて、四半期ごとの推移を「図 11 メール種別件数推移（2013 年度）」に示す。全体としては「添付ファイル」が多数を占めている一方で、「やり取り型」攻撃に関わると思われる「情報収集」のメールが 2013 年 4-6 月に多数、また同 10-12 月に数件観測された。2013 年 7-9 月には、メールの文面は同一だが、リンク先 URL の一部が少しずつ異なる不審メールが多数観測されたため、「URL リンク」の件数が増えている。一件ずつ異なる URL をメールに埋め込むことで、攻撃者は、どのメールの受信者がリンクを開いたのかを管理・追跡しようとしていた可能性がある。

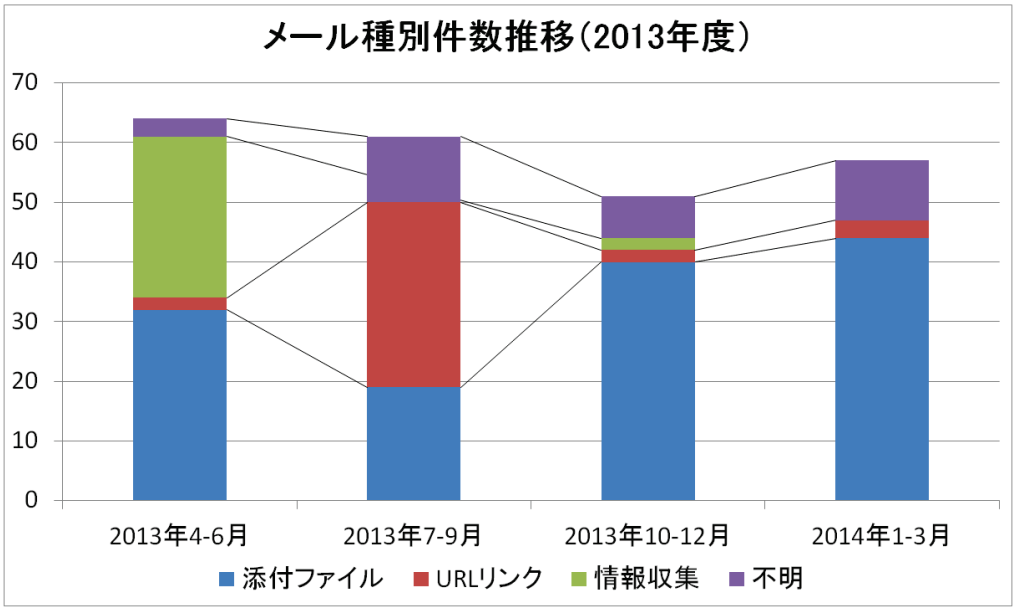


図 11 メール種別件数推移（2013 年度）

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（2013 年度）」に示す。

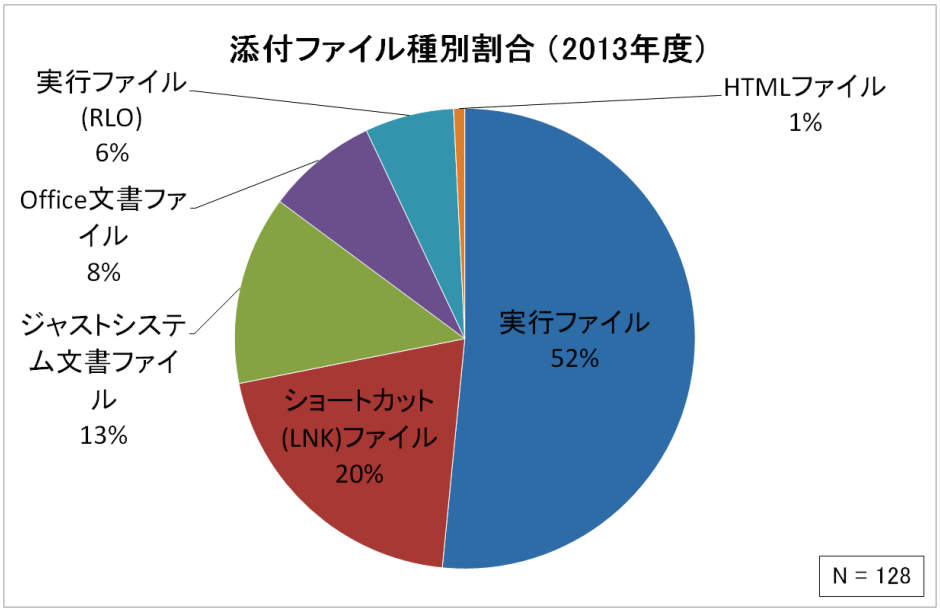


図 12 添付ファイル種別割合（2013 年度）

2012 年度は「Office 文書ファイル」が 45%を占めていたが、2013 年度は 8%まで減少した。一方で、2012 年度には観測されなかった「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）が 13%を占めた。攻撃者は、その時々により、悪用しやすい（修正プログラムが適用されている可能性が低い）脆弱性を狙っている。また、国外の組織ではあまり使われていないソフトウェアが狙われたことからも、日本国内の組織を標的とした攻撃活動が行われていることは明らかである。

更に、2012 年度には観測されなかった「ショートカット（LNK）ファイル」も、全体の 2 割を占める結果となった。Windows OS の仕様として、ショートカットファイルにはスクリプトコード（任意の簡易的なプログラム）を含めることができ、ファイルのアイコンの見た目や拡張子を偽装することができる。こうして細工されたファイルを開いた場合、実行ファイルを開いた時と同様、ウイルスに感染させられてしまう。J-CSIP 外で確認したショートカットファイルを悪用する手口については、別途「IPA テクニカルウォッチ」[13]で詳しく紹介しているが、J-CSIP 内でも同様の手口のものが観測されていた。

これらを除くと、添付ファイル全体の半数以上は実行ファイルであり、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[14]を使って拡張子を偽装する等、受信者の油断を誘ってファイルを開かせ、ウイルスに感染させようとしているものであった。ジャストシステム文書ファイル等の新しい脆弱性を悪用する攻撃手口が使われる一方で、実行ファイルが占める割合は 2012 年度よりも増加している。利用者に対し、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ろう。

---

[13]「標的型攻撃メールの傾向と事例分析 ＜2013 年＞」（IPA）
https://www.ipa.go.jp/security/technicalwatch/20140130.html

[14] 「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

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

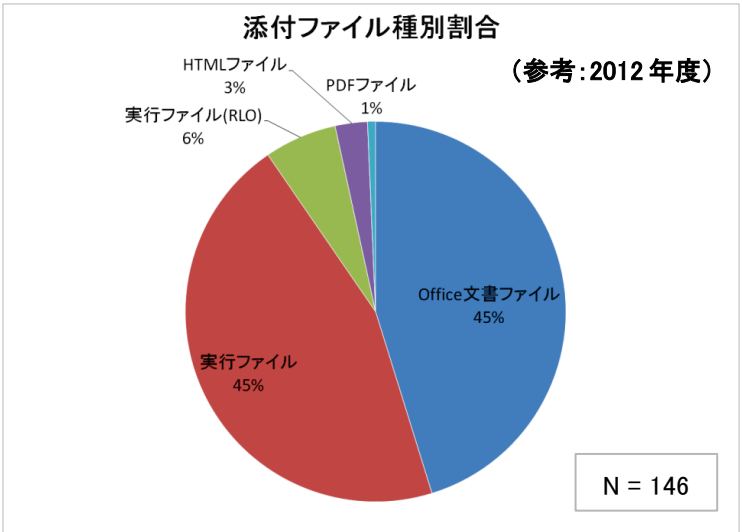


図 13 （参考）添付ファイル種別割合（2012 年度）

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（2013 年度）」に示す。2013 年 10-12 月は、ジャストシステム社の「一太郎」の脆弱性 CVE-2013-5990 が公開された[15]時期であり、この時、当該脆弱性を悪用するファイルが集中して観測された。2013 年 7-9 月は件数が少なくなっているが、この時期は前章に示した通り、URL リンクの攻撃メールが多数観測されている。全体の傾向としては、時とともに、攻撃手口が次々と変化していることが分かる。

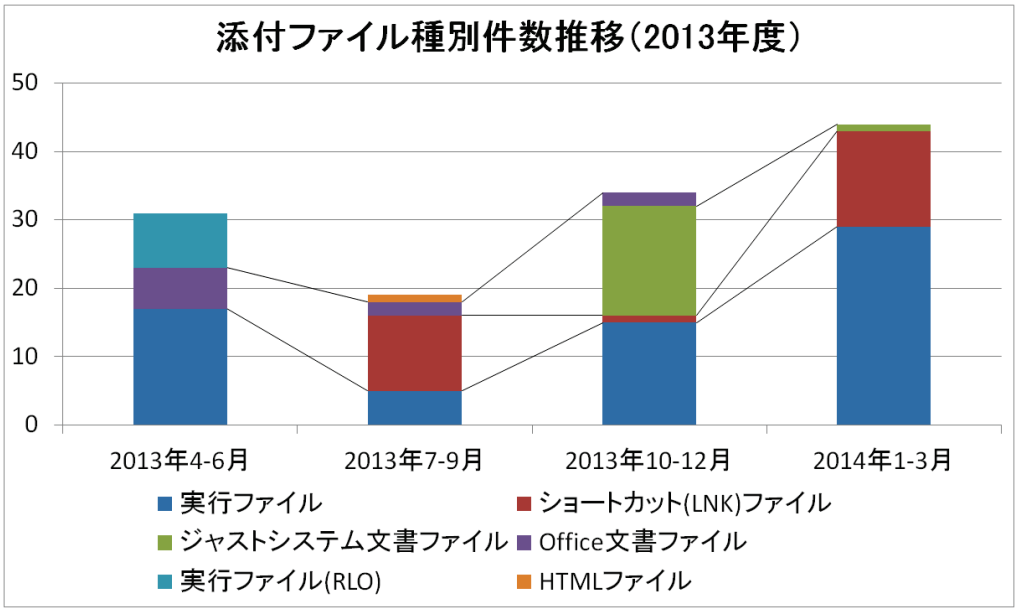


図 14 添付ファイル種別件数推移（2013 年度）

[15] 「「一太郎」シリーズにおいて任意のコードが実行される脆弱性対策について(JVN#44999463)」（IPA）
https://www.ipa.go.jp/security/ciadr/vul/20131112-jvn.html

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 233 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（2013 年度）」に示す。

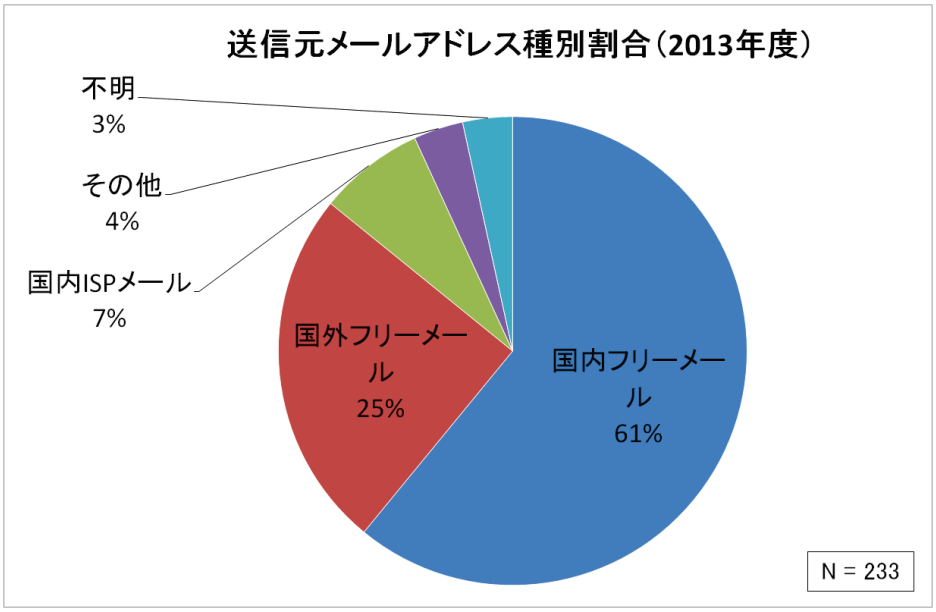


図 15 送信元メールアドレス種別割合（2013 年度）

「国内フリーメール」「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 86%を占めた。2013 年度は、その中でもメールアドレスに「.jp」が付く国内フリーメール[16]が多く観測されており、これは、攻撃者がメール受信者の警戒心を低下させ、攻撃の成功率を高めようとしているためではないかと思われる。

また、この統計の結果は、フリーメールの添付ファイルや URL リンクを開きさえしなければ、86%の攻撃を回避できたことを示している。フリーメールへの対応として、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、注意を促すといった施策を行うことが望ましい。

送信元メールアドレスとして「国内 ISP メール」も 7%観測された。これらのメールアドレスは国内の 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もので、実際のメール配送経路も当該 ISP のメールサーバが使われていた形跡があった。攻撃者は、メール送受信を行うために一般利用者のパソコンを乗っ取ったり、メール用の ID やパスワードを窃取するなどした上で、本物の利用者になりすまして攻撃メールを送信していた可能性がある。

なお、「その他」はフリーメールではないメールアドレスで、例えば企業や組織のメールアドレスを詐称していたケースである。残りの「不明」は、情報提供内容が不完全であったため、送信元メールアドレスが確認できなかったものである。

[16] 例えば Google 社の「Gmail」（メールアドレスの形式は「～@gmail.com」）は日本国内へのサービスを行っており、利用者も多いが、ここでは「国外フリーメール」に分類している。

前述の統計情報のうち、「国内フリーメール」と「国内 ISP メール」に限定し（233 件のうち 159 件）、四半期ごとの件数推移を示したグラフを「図 16 国内メールサービス 送信元メールアドレス件数推移（2013 年度）」に示す。

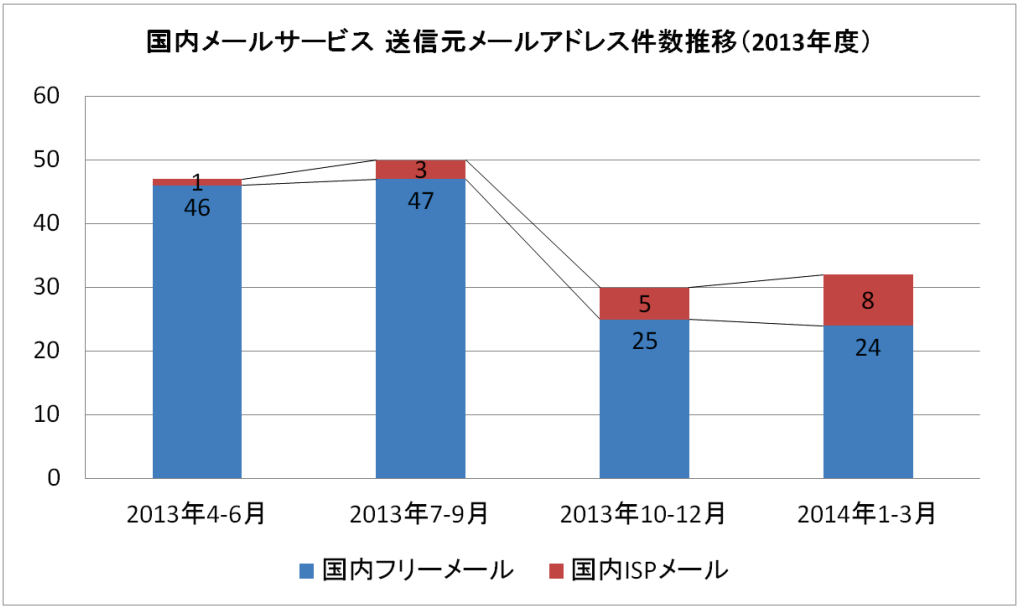


図 16 国内メールサービス 送信元メールアドレス件数推移（2013 年度）

フリーメールが警戒されるようになったのが原因か、この 2013 年度の一年間を通して、国内 ISP メールを悪用する事例が増加傾向にある。全体の数が少なく、はっきりとした傾向があるとは言い切れないが、攻撃手口の巧妙化が進んでいる兆候の可能性があり、引き続き注視していく予定である。

3.7 まとめ

2013 年度は、新しい脆弱性を悪用するジャストシステム文書ファイルや、利用者を騙す新しい手口であるショートカット（LNK）ファイルを添付する手口が観測される等、攻撃者が次々と攻撃手口を変化させている傾向が顕著に表れた。また、「2012 年度 活動レポート」では明記していなかったが、「やり取り型」の手口も継続して観測されている。

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

また、3.4 節、3.5 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。

- 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。
- 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。

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。

4　情報共有の事例 ー 「やり取り型」攻撃の分析

4.1 はじめに

本章では、メールで会話を行った後でウイルスを送りつける、いわゆる「やり取り型」の手口について、J-CSIP 内で情報の共有・集約・分析を行った事例を紹介し、この脅威について詳しく説明するとともに、情報共有の有効性について示す。

この情報共有の事例で得られた知見の概要は次の通りである。

- 個々の攻撃情報だけでなく、複数の攻撃情報を分析することで、攻撃者が複数の組織を狙ってどのような攻撃を行っているのか、その一端を把握することができた。
- 攻撃者の能力（日本語の理解、メールでの会話）や、攻撃者が複数の攻撃行為を通じて「学習」し、手口が巧妙化した形跡が確認できた。

前年度、「2012 年度 活動レポート」の 3.2 章「情報共有の事例」にて、標的型攻撃メールの発見、情報提供、情報共有、そして同種のメールが他組織で発見され、それらの情報も集約を行ったという一連の流れを紹介した。次の一文は、その際の説明の抜粋である。

> 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。

このような情報の集約と分析は現在も必要に応じて行っている。この情報が実際にどのような内容であり、また、それにより何が分かるのかという点について、今回の活動レポートでは、J-CSIP の参加組織からの了承のもと、具体的な事例によって説明する。

まず、4.2 節で、添付資料『「やり取り型」攻撃に関する分析図』の読み方について説明する。この資料は、情報集約の結果として、実際に IPA から J-CSIP の参加組織へ展開した情報の一部である（公開にあたり一部加工や削除を行っている）。

続いて 4.3 節で、分析図にあるそれぞれの案件について説明する。この際、他の案件とどのような関係にあるか、また、そこからどのようなことが分かるかといった点についても述べる。

本分析図は 2012 年に発生した攻撃を集約したものであるが、同様の「やり取り型」攻撃は 2013 年度においても継続して観測されている。この事例紹介の目的は、情報共有の有効性を説明することだけではなく、「やり取り型」の悪質で巧妙な攻撃手口について、J-CSIP 内外の組織への改めての注意喚起でもある。

「やり取り型」という手口が存在すること、また、それがどのような攻撃であるかといった情報については、IPA が 2011 年 10 月に公開したテクニカルウォッチ[17]（「おれおれ詐欺を模倣した標的型攻撃メールの事例」の紹介）や、メディアによる報道等、一部は既に公知となっているが、本事例では、同一組織の複数窓口や、複数の組織にまたがった攻撃を横断的に分析し、攻撃の関係性や攻撃者の行動を明らかにしている。

国内に対する「標的型サイバー攻撃」が現実にどのように行われているのか、その脅威への理解を助け、対策の必要性の再確認や、情報共有活動、あるいは当機構への情報提供（情報の集約）の重要性の認識に繋がることを期待している。

---

[17] 「IPA テクニカルウォッチ 『標的型攻撃メールの分析』に関するレポート」（IPA）
https://www.ipa.go.jp/about/technicalwatch/20111003.html

4.2 添付資料『「やり取り型」攻撃に関する分析図』の読み方

添付資料『「やり取り型」攻撃に関する分析図』は、J-CSIP の参加組織から提供された情報だけでなく、IPA の「標的型サイバー攻撃の特別相談窓口」[18]等で J-CSIP 外より入手した情報も含め、相互に関連していると思われる「やり取り型」攻撃に関するメールの情報を、時系列順・案件別に並べた図である。

まず全体的な構成を「図 17 分析図の構成」に示す。

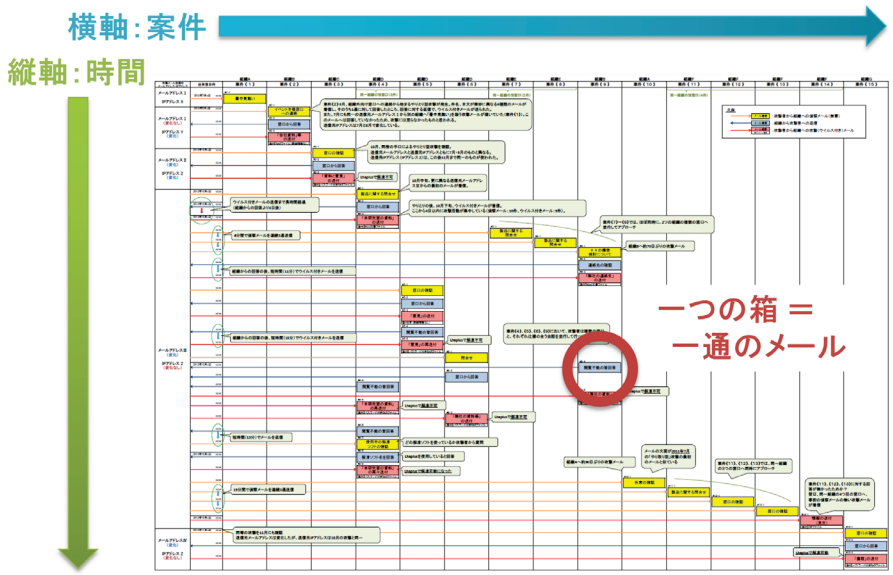


図 17 分析図の構成

分析図の縦軸は時間であり、この図で対象としている期間は 2012 年 7 月から 11 月のおよそ 4 か月間である。また、ここでは、攻撃者からの最初のアプローチのメールから始まる一連のメールのやり取りをまとめたものを、1 つの「案件」として扱っている。横軸には案件ごとに 15 の列（15 の案件）があり、各列にはその案件での攻撃の推移を示した。黄・青・赤の色を付けた箱が、それぞれ一通のメール [19]の情報であり、全体で 39 通のメールの情報が、この図に含まれている。

次に、各メールの情報（図中の箱）の凡例を示す。

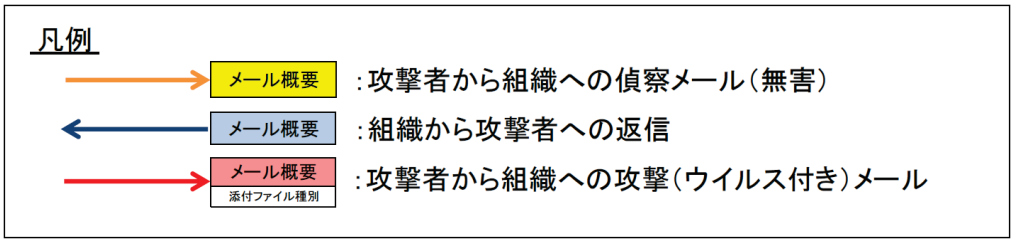


図 18 分析図の凡例

[18] 「標的型サイバー攻撃の特別相談窓口」（IPA）
https://www.ipa.go.jp/security/tokubetsu/

[19] 攻撃者が、メールを送信したのではなく、ウェブサイトの問い合わせフォーム等からアプローチを行ったと思われるケースもあるが、便宜上、メールを受け取ったものとして整理している。

黄色は、攻撃者から組織に対して送られた、添付ファイルも URL リンクもない無害なメールであり、組織へのアプローチや会話を試みるもので、ここでは「偵察メール」と呼ぶ。1 件を除き、全ての案件が、この偵察メールから始まっている。メールの内容は、窓口の確認であったり、製品等に関する問い合わせを装っているものが多い。

青色は、攻撃者からのメールを受け取った組織から、攻撃者に対して返信を行ったメールである。15 の案件のうち、7 件において、組織は何らかの返信を攻撃者に返している。

赤色は、攻撃者から組織に対して送られたメールで、添付ファイル（ウイルス）が付いていたものである。

「やり取り型」の手口では、まず偵察メールが送られてきて、組織が返信すると、そのメールアドレスへ攻撃メール（ウイルス）が送られてくる。逆に、偵察メールを受信しても、組織から返信を行わなかった場合は、そのまま攻撃者からの連絡は途絶えている。このため、分析図では、基本的に「黄→青→赤」の順でメールが並ぶか、「黄」のメールのみ（組織が返信をしなかった）となっている。

続いて、分析図の左上部分を抜粋し、図の構成をより詳しく説明する。

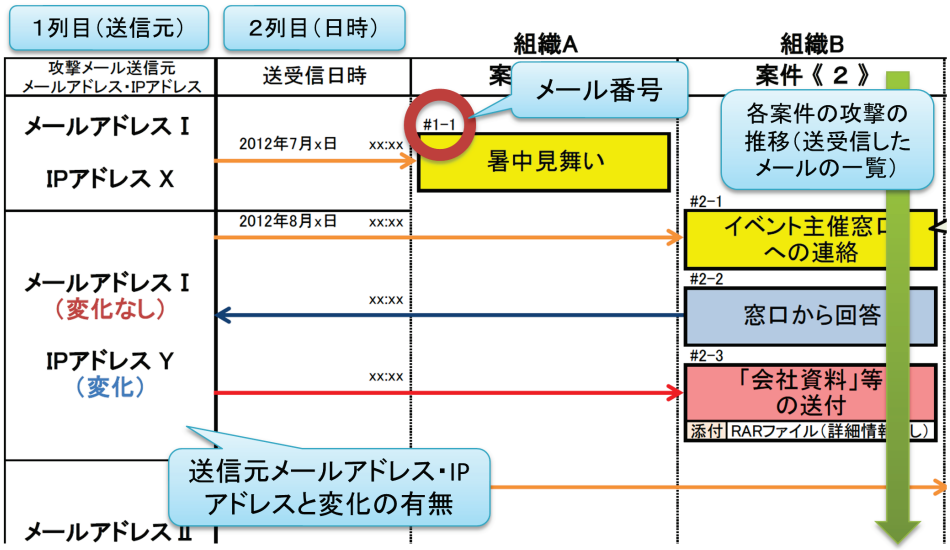


図 19 分析図の構成（左上部分抜粋）

図の左端（1 列目）は、攻撃者が使った送信元のメールアドレスと IP アドレスである。これらは時間の経過とともに、同じものが使われ続けたり、片方だけ変化したり、あるいは両方とも変化したりといったことが観測できたため、変化の有無を併せて示している。

2 列目は、メールが送受信された日時である。本分析図では基本的に年月までの情報としているが、必要な箇所は、分単位で補足説明を加えている。

3 列目からは各案件が並んでおり、攻撃メールが届いた組織、案件の番号、そして案件の中で送受信された個々のメールについて、メールの概要や添付ファイルの種別を記載している。左肩にある「#1-1」といった番号は、個々のメールに振った通し番号である。

この他、図中には、注目すべきポイントを吹き出しで説明したり、複数の攻撃が同一の組織の別窓口に対して行われたものであった場合は、その旨を示している。

4.3 分析図内の各案件の説明

引き続き、分析図に挙げた 15 の案件について説明する。全体的な流れや案件同士の相関は図の方が分かりやすいため、適宜、分析図を参照していただきたい。

案件《1》 暑中見舞い

2012 年 7 月、「＊＊さんへ」(＊＊の部分には名前が書かれていた)という件名で、暑中見舞いの内容のメールが着信した(メール#1-1)。

メールを受信した職員は返信を行わず、この案件はここで終わっている。

このメールは、この先数か月に渡って観測される「やり取り型」の攻撃の偵察メールの一部であろうことが分かったのだが、それは、案件《2》以降の情報が提供されたためである。

案件《2》 イベント主催窓口への問い合わせ

案件《1》から約 10 日後、2012 年 8 月、ある組織のイベント主催窓口に対し、件名や本文が微妙に異なる 6 種類のメールが着信した。このうち 1 通(メール#2-1)に対してメールを返信(メール#2-2)したところ、「会社資料」等と称し、不審な添付ファイル付きのメールが着信した(メール#2-3)。この添付ファイルを解析した結果、標的型攻撃でよく見られる種の実行ファイル形式のウイルスであることが分かった。

このメールを受信したのは案件《1》とは別組織であり、メールの送信元 IP アドレスは変化していたが、送信元メールアドレスは同一であった。もし案件《1》の「暑中見舞い」へ返信していたら、その後、攻撃メールが送られてきた可能性が高い。すなわち、案件《1》自体は何も問題なかった上、脅威であるのか否かも不明であったが、この案件《2》の情報より、実際には、メールを受信した職員(のメールアドレス)が、「やり取り型」の手口を使う攻撃者の攻撃先リストに載ってしまっている可能性が考えられ、当該職員においては一層の注意を払う必要があることが分かったということである(「図 20 案件《1》と《2》」参照)。そして実際に、この案件《1》の受信者へ、およそ 90 日後に再び別の偵察メールが届いている(案件《10》参照)。

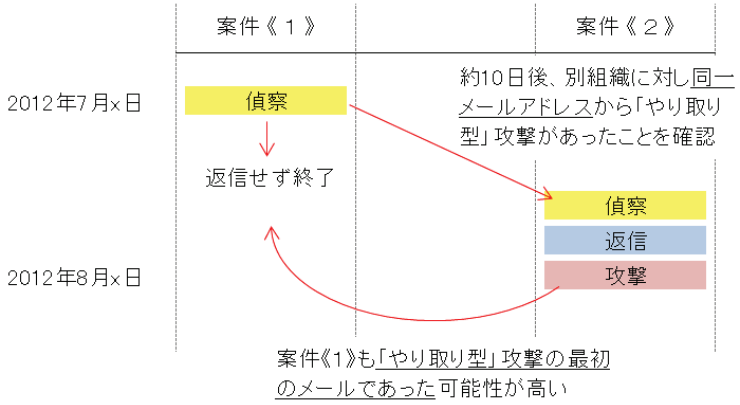


図 20 案件《1》と《2》

案件《3》 「資料と意見」の送付

案件《2》から 2 か月後、2012 年 10 月、また別の組織へ、「＊＊の質問について」という件名で、窓口の確認を行うメールが着信した(メール#3-1)。これに対し返信したところ(メール#3-2)、「資料と意見」を送付するという内容で、ウイルス付きのメールが着信した(メール#3-3)。

この案件では、送信元メールアドレスと IP アドレスの両方が変化していた。内容や手口から、案件《1》《2》と同一の攻撃者もしくは攻撃グループによるものであろうと思われるが、2 か月の間、攻撃を止めていたのか、他の組織や業界へ攻撃が続いていたのかは不明である。

添付ファイルはパスワード付きの RAR 形式 [20]の圧縮ファイルで、「Lhaplus」という解凍ソフトでは正しく**解凍することができない**ものであった。この「解凍の可・不可」については、次の案件《4》をはじめ、多数の案件と関係がある。他のツールを使って解凍すると、実行ファイル形式のウイルスが入っていた。

本件は、最初の偵察メールの着信から攻撃メールの着信まで、その日のうちに完結している。

案件《4》 製品に関する問い合わせ

案件《3》の数日後、2012 年 10 月中旬、更に別の組織へ、「＊＊関するお問い合わせについて」(＊＊の部分は製品名)という件名で、案件《3》と同じ IP アドレスから、新たな送信元メールアドレスより偵察メールが着信した。

この日から約 10 日間に渡り、本分析図に載せているだけでも、この送信元メールアドレスから 11 の攻撃(案件《4》～案件《14》)が連続して発生している。

案件《4》は、今回紹介している 15 の案件の中でも最もやり取りが長く、メールの数も多かったものである。攻撃者は、この案件《4》のやり取りをしている時期と並行して、同じ組織の別窓口や、他の組織へも攻撃を行っていた。複数の攻撃が並行している様子については、分析図を参照すると分かりやすい。

また、本件では、実に 3 回、ウイルス付きの攻撃メールが窓口へ着信している。案件《4》で送受信されたメールについて、説明とともに「表 4 案件《4》のメール一覧」に示す。

表 4 案件《4》のメール一覧

番号	種別	説明
#4-1	偵察	製品に関する問い合わせとして、最初のメールが着信した。
#4-2	返信	窓口から回答を行った。
#4-3	攻撃	「本研究室の資料」の送付と称し、Word 文書ファイル(ウイルス)が添付されたメールが届いた。
#4-4	返信	送付された文書ファイルの内容が確認できなかった旨を返信した。
#4-5	攻撃	「本研究室の資料」の再送付と称し、今度はパスワード付き RAR 圧縮ファイルが届いた。
#4-6	返信	送付されたファイルの内容が確認できなかった旨を返信した。
#4-7	偵察	**解凍ソフトは何を使用しているか**、攻撃者から質問のメールが届いた。
#4-8	返信	**「Lhaplus」という解凍ソフトを使用した**旨を返信した。
#4-9	攻撃	再度、「本研究室の資料」の再送付と称し、パスワード付き RAR 圧縮ファイルが届いた。 メール#4-5 の添付ファイルと違い、**このファイルは「Lhaplus」で解凍できるようになっていた。**

まず、メール#4-3 で送付された Word 文書ファイルは、脆弱性を悪用してパソコンへウイルスを感染させる仕組みのものであった。案件《2》および《3》では攻撃に実行ファイルを使っていたため、本件では、攻撃者は手口を変化させたことになる。

この Word 文書ファイルは、利用者が開いてしまった場合でも、その時点でソフトウェアが最新になっていれば攻撃(ウイルス感染)が失敗していた。攻撃者は、Word 文書ファイルによる攻撃が成立しないことを察したのか、メール#4-5 では、再び実行ファイルによる攻撃に切り替えている。メール#4-5 の添付ファイルは、案件《3》と同様、「Lhaplus」では解凍できない RAR 形式の圧縮ファイルであった。

その後、メール#4-7 と#4-8 のやり取りで、攻撃者は、本件メールの受信者が「Lhaplus」を使用していることを知った。最終的に、メール#4-9 で着信した RAR 形式の圧縮ファイルは、「Lhaplus」で解凍可能となった。

[20] ZIP 形式や LZH 形式のような圧縮ファイルの形式の一種(ファイルの拡張子は一般的に「.rar」)。RAR 形式のファイルを解凍するには、RAR 形式に対応した解凍ソフトを使う必要がある。「Lhaplus」は RAR 形式に対応した解凍ソフトの一つであり、特殊な場合を除き、RAR 形式ファイルを解凍することができる。

分析図には記していないが、メール#4-5（Lhaplus 解凍不可）の圧縮ファイルの内容と、メール#4-9（Lhaplus 解凍可）の圧縮ファイルの内容が、全く同じファイルであったことにも注目している。すなわち、このファイル（ウイルス）自体が解凍可・不可の問題を生じさせていたのではなく、圧縮を行う方法（ツールや作業環境）に問題があったということで、攻撃者はそのことを察知し、ウイルスには一切手を加えず、圧縮を行う方法のみを変更したことになる。「Lhaplus」を使用したという返信（メール#4-8）から、攻撃者がウイルスを別の方法で圧縮しなおして再送（メール#4-9）してくるまでの時間は、51 分間であった。攻撃者が「Lhaplus」を入手し、当該ソフトで解凍可能なようウイルスを圧縮する手順を確立するまで、1 時間もかからなかったということになるだろう[21]。

メール#4-9 より過去の攻撃に使われた RAR ファイルで、IPA で検体を確認できたもの（メール#3-3、#4-5、#5-5、#6-3、#9-5）については、全て「Lhaplus」では解凍不可で、この後の攻撃に使われた RAR ファイル（メール#15-3）は、「Lhaplus」で解凍可能であった。攻撃者は、本件を通じて「学習」したことに間違いはなさそうである。

案件《4》から 案件《9》の流れ

案件《4》から案件《9》の 6 件については、攻撃者が複数の組織に渡って順次攻撃を行った形跡が見て取れる。この流れが分かるよう、分析図から抜粋したものを「図 21 案件《4》から《9》」に示す。

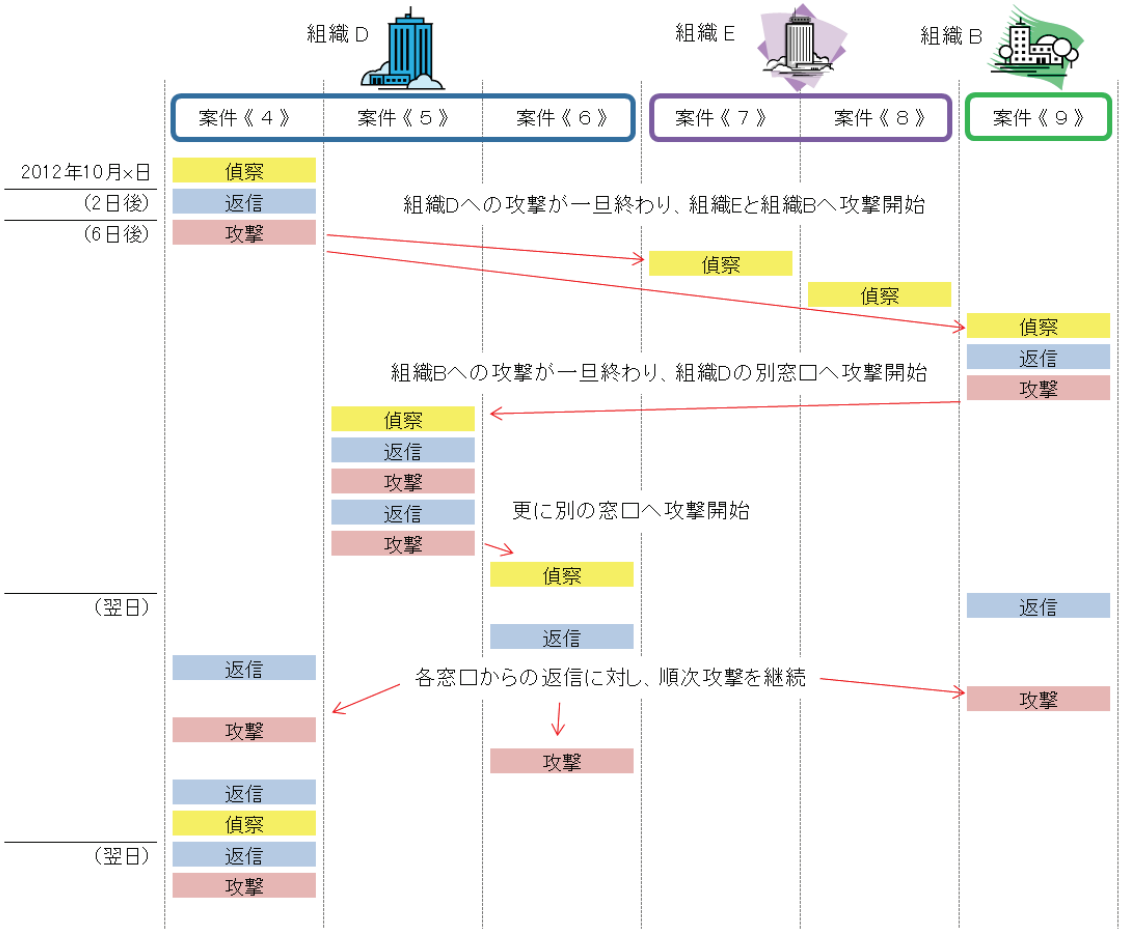


図 21 案件《4》から《9》

[21] RAR 圧縮ファイルによる攻撃が複数失敗した状況をうけ、攻撃者が、メール#4-8 受信以前に、圧縮方法の変更を試みる作業を行っていた可能性はある。

案件《5》と《6》 「意見」と「弊社の資料等」の送付

案件《5》と《6》は、案件《4》と同一組織の、別の窓口に対して行われた攻撃である。案件《4》で最初のウイルスメール（メール#4-3）を送りつけたあと、攻撃者は、更に別の 2 つの組織に対して攻撃を開始した（案件《7》～《9》）。そして、そちらがひと段落して、案件《5》と《6》の攻撃が始まっている。

案件《4》では、「本研究室の資料」と称してウイルスを送りつけてきていたが、案件《5》では「意見」を送るとし、案件《6》では「弊社の資料等」としており、対応する窓口ごとに詐称する立場や話題を変えている様子が伺えた。

また、案件《5》と《6》でも共通して、やり取りの後、最終的にはパスワード付きの RAR 形式の圧縮ファイルが送られていた（メール#5-5、#6-3）。先述の通り、この 2 つの RAR ファイルは「Lhaplus」では解凍できない。他のツールを使って解凍すると、実行ファイル形式のウイルスが入っていることが確認できた。

同一組織であっても、異なる窓口に対し、少数かつ内容も異なる手口で攻撃が行われると、不審さに気付くことは難しいと思われる。それでも、不審に感じたものについては、やはり組織内でまず情報共有を行うことができるような体制が望ましいだろう。

案件《7》と《8》 製品に関する問い合わせ

案件《4》～《6》と並行し、別の組織の 2 つの窓口に対して試みられた攻撃が案件《7》と《8》である。偵察メールの件名は「＊＊の問合わせについて」（＊＊の部分にはそれぞれ異なる製品名が書かれていた）となっており、製品に関する問い合わせを装っていた。

この組織は、いずれのメールに対しても返信を行わなかったため、この攻撃は偵察メールのみで終わっている。案件《1》と同様、この組織単体では「この不審なメールが何だったのか」を知ることができないが、情報を共有し、集約することで、次のような点を知ることができたことになる。

- これらが「やり取り型」の攻撃の偵察メールであったこと、また、本件メールが着信した窓口が再び狙われる可能性があり、今後も同様の攻撃に注意する必要があること
- 返信した場合、Word 文書ファイルか、実行ファイルを圧縮した RAR ファイルが送られたであろうこと
- 攻撃者による一連の攻撃行動の中での、自組織の相対的位置（攻撃されたタイミングが、初期・中期・後期と分けると中期にあたるということ）

これらの情報が無ければ、本メールが脅威であるのか否かの判断すら難しいだろう。案件《7》《8》のような、自組織では攻撃に至らなかったケースでも、相互の情報共有が各組織での対策検討の一助となると思われる。

案件《9》 製品に関する問い合わせ

案件《9》は、案件《7》《8》に続き、案件《2》と同じ組織の別窓口に対し、およそ 70 日ぶりに再び送られた攻撃メールである。これら案件《7》～《9》の偵察メールは、件名や文面が異なる 3 通が、わずか 4 分の間に送られている。案件《9》では、「＊＊の構想検討について」という件名で、内容は製品に関する問い合わせを装っていた（メール#9-1）。

この案件では、偵察メールに対し、窓口より問い合わせ元（攻撃者）の連絡先を確認するためのメールを返信（メール#9-2）してから、11 分後に「弊社の連絡先」の送付と称してウイルスが送られてきている（メール#9-3）。攻撃者は、ウイルス自体は事前に準備していると思われるが、メールの内容等については、妥当な会話となるよう、その場で作文していることが伺える。

メール#9-3 の添付ファイルは案件《4》と同等の、悪意のある Word 文書ファイルであった。送付された文書ファイルが閲覧できなかった旨を返信（メール#9-4）したところ、27 分後に、パスワード付きの RAR ファイルが添付された攻撃メールが送られた（メール#9-5）。先述の通り、この RAR ファイルも「Lhaplus」では解凍できないものであり、内容は実行ファイル形式のウイルスであった。

案件《10》　個人宛のメール

案件《4》～《9》が同時並行的に発生し、全てが収束したころから数時間後、同一の送信元メールアドレスから、案件《1》と同一の受信者へ、およそ 90 日ぶりに再び偵察メールが届いた（メール#10-1）。

このメールは、案件《2》～《9》のような窓口への問い合わせを装ったものではなく、「＊＊さんへ」という件名で、メールの本文は、次の内容であった。

> ＊＊さん
>
> 明日事務室にいますか？用事があります。
>
> お返事お待ちしております。
>
> ＊＊

この組織は、メールに対して返信を行わなかったため、この攻撃は偵察メールのみで終わっており、ウイルスの着信等は観測されなかった。

案件《10》と 2011 年 7 月の「やり取り型」攻撃との類似性

この案件《10》のメール本文は、更に、2011 年の「やり取り型」攻撃へ遡り、類似性が見られた。

IPA は、2011 年 10 月に公開したテクニカルウォッチ [22]において、「おれおれ詐欺を模倣した標的型攻撃メール」（やり取り型の手口）が同年 7 月に初めて観測された事例を紹介した。テクニカルウォッチの当該部分の抜粋を、「図 22　2011 年 7 月の事例（テクニカルウォッチ p.13 から抜粋）」に示す。この事例で、最初の「偵察メール」にあたるものは、下線を引いた「①」である。

> 4.4. おれおれ詐欺を模倣した標的型攻撃メールの事例
>
> 2011 年 7 月に、おれおれ詐欺を模倣した標的型攻撃メールに関する届出があった。
>
> 最初、テキスト本文のみの日常会話的なメールが何回かやりとりされ、最後にウイルス付きの PDF ファイルが添付されたメールが届き、その PDF ファイルを開くことにより、ウイルスに感染したという事例である。
>
> メールのやりとりは以下のようなフローであった。
>
> ①　ある日、○○さん今どこに居ますかという内容のメールが届いた。
>
> ②　メールの送信者に心当たりがないので、誰ですかという内容のメールを返信した。
>
> ③　すると、去年食事をしましたという内容のメールが届いた。

図 22　2011 年 7 月の事例（テクニカルウォッチ p.13 から抜粋）

上図の通り、テクニカルウォッチではメールの本文は掲載していなかったが、この時の①のメールの実際の本文は、次の内容であった。

[22] 「IPA テクニカルウォッチ 『標的型攻撃メールの分析』に関するレポート」（IPA）（再掲）
https://www.ipa.go.jp/about/technicalwatch/20111003.html

＊＊さん

今事務室にいますか？

このメールの本文は長い期間公知となっておらず [23]、実際の内容を把握していた者は、攻撃を受けた組織、その情報の提供を受けたIPAを含む一部の機関、そして、攻撃を行った者に限られていたと考えられる。文章としては非常に短いため、案件《10》と関係があると言い切ることはできないが、メールの本文と、一連の攻撃手口の類似性より、2011 年 7 月の案件と、本資料 2012 年の 15 の案件には、同一の攻撃者または攻撃グループが関わっていたのではないかと推測している。

案件《11》から 案件《14》 一組織へ連続 4 通のメール

案件《10》のメールの更に数時間後、同一の送信元メールアドレスから、ある一組織の 3 つの窓口に対し、19 分間かけて連続して偵察メールが着信した（メール#11-1、#12-1、#13-1）。件名や本文はそれぞれ異なり、「＊＊の購入について」「個人情報についてのお問い合わせ」「＊＊について」となっていた。

この組織は、3 通全てのメールに対して返信を行わなかったため、案件《11》～《13》の攻撃は偵察メールのみで終わっている。

翌日、同組織の別のメールアドレスへ、「＊＊さんへ」という件名で、メール本文は英語、添付ファイルは ZIP 形式の圧縮ファイル（解凍すると実行ファイルのウイルスが入っていた）という、偵察メールの無い攻撃メールが着信した（案件《14》）。攻撃者がこのようにした理由は計りかねるが、案件《11》～《13》に対する返信が無かったため、攻撃者が手口を切り替えた可能性がある。

案件《15》 「書類」の送付

案件《14》からしばらく経ち、2012 年 11 月、再びやり取り型の手口が観測された。この案件では、送信元メールアドレスは変化していたが、送信元 IP アドレスは 10 月の攻撃（案件《4》～《14》）と同一であり、窓口の確認、それに対する返信、そして「書類」の送付と称してパスワード付きの RAR 形式の圧縮ファイルが送られてくるという流れのものであった。

そして、この RAR ファイルは、先述のとおり、「Lhaplus」で解凍可能なものであり、内容は実行ファイル形式のウイルスであった。

[23] IPA が把握している限り、2013 年 6 月 6 日の NHK の放送が、最初に公知となった時点である。
参考：「国家の“サイバー戦争” - NHK クローズアップ現代」（NHK）
http://www.nhk.or.jp/gendai/kiroku/detail02_3360_all.html

4.4 まとめ

「やり取り型」攻撃の実態

J-CSIP 内外より情報提供された 15 の案件の具体的な事例紹介を通し、国内組織に対して行われているサイバー攻撃である「やり取り型」の標的型攻撃メールの実態を示した。この攻撃の特徴として、次のような点が分かった。

- 各組織の外部向け窓口は、業務上、問い合わせのメールへの返信や、添付ファイルの内容を確認せざるを得ないが、そのことを攻撃者は理解していると考えられ、実際に複数の組織の様々な問い合わせ窓口に対して攻撃が行われている。
- 攻撃者は、時に複数の組織に対し同時に攻撃を行いながらも、攻撃が表面化しないよう一組織あたりの宛先は少数に絞るなど、慎重に行動している。また、案件《1》と案件《10》、および案件《2》と案件《9》のように、しばらく期間をおいて、同じ組織へ攻撃を繰り返すこともある。
- 攻撃者または攻撃グループは、攻撃を仕掛けている間はメールやウイルスの送受信がすぐにできる状態を保っている様子が伺える。
- 攻撃者は日本語で会話し、話題に合った形で悪意のある添付ファイルを送る能力を持つ。状況に応じて攻撃手口を変化させることができ、また、攻撃を通して学習することで、手口が巧妙化することもある。

「やり取り型」の攻撃は、この後も観測されている。窓口部門はもちろん、このような手口をはじめとする標的型攻撃メールの脅威について、組織内に改めて周知を徹底していただきたい。なお、外部から送られた不審なファイルを開くことのリスクが高いことは当然であるが、それでも内容を確認しなければならない場合も多い。J-CSIP では、不審なファイルの内容を確認する際、仮にそれがウイルスであった場合でも悪影響を及ぼさないような特別な環境を用意することを勧めている [24]。

情報共有と集約の重要性

J-CSIP において、情報共有と集約により、個別の攻撃情報、あるいは単体の組織が持つ情報のみでは得られなかった様々な事実が分かり、また、それを共有することができた。このような情報は、標的型攻撃の脅威を把握するとともに、多くの攻撃情報の中で、自組織が受けた攻撃が相対的にどのレベルであるのかといった点も、各組織において対策を検討・実施していく上で重要であろうと考えている。

また、IPA では、J-CSIP の参加組織に限らず、「標的型サイバー攻撃の特別相談窓口」にて、一般の企業・組織からの相談や情報提供を受け付けている。情報提供いただくことで、本件のように、単独の組織では分からない「攻撃の全体像」の把握に繋がり、攻撃の検知や防御のための、より多くの情報が得られる。標的型サイバー攻撃の実態を解明し、対策を進めるためにも、ぜひ、相談や情報提供をお寄せいただきたい。

---

[24] 例えば、スタンドアロンの PC 上に仮想環境用ソフトウェアを用い、仮想マシン上に Windows OS と Office ソフト等（Linux 系 OS と Office 互換ソフト等でもよい）を導入しておき、クリーンな状態でスナップショットを取得（現在の状態を保存）しておく。その環境で不審なファイルを開き、内容を確認し、作業が終わったらクリーンな状態のスナップショットへ巻き戻す。この方法で、現状行われているような攻撃であれば、ほぼ防ぐことができる。なお、仮想環境ではなく、マシン起動のたびにクリーンな状態に OS 等が初期化される環境や、文書ファイルを自動的に無害な閲覧用の画像ファイルに変換するソフトウェア等を使う方法もある。

5　さいごに

標的型攻撃は巧妙化を続けており、システム的な対策の強化・実施とあわせて、受信者が不審だと感じたメールについては、組織内の CSIRT やシステム管理部門に届け出て、組織として確認するような対応が必要になってきている。

不審なメール等の情報を組織的に集めることによって、同様のメールの受信者が他にいるか確認したり、メールや添付ファイルの内容を分析することで、自組織が標的型攻撃を受けているのか否か、また、その攻撃がどのようなものなのか、そして、その攻撃は既存の防御策で防げるものであるのか等、実態の把握を進めることが可能となる。CSIRT やシステム管理部門の負担が大きくなるという、非常に厳しいハードルはあるが、例えば、重要情報を取り扱う部門や、不審なメールを受信しやすい対外窓口部門など、組織内の一部からであっても、攻撃情報を集約する取り組みを始めることを勧めたい。

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。

標的型攻撃メールは、攻撃者が組織内ネットワークへ侵入するための第一歩であり、もちろん、これを可能な限り防ぐことは非常に重要であるが、常に 100%防ぎ続けることもまた不可能である。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「『標的型メール攻撃』対策に向けたシステム設計ガイド」[25]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」[26]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。

2014 年度以降、J-CSIP では引き続き情報共有の運用を行うとともに、参加組織の拡大、共有する情報の拡充、効率の向上等を図っていく。また、長期的な視点においては、今回の事例のように、単独の攻撃情報の共有のみならず、複数の攻撃情報を集約して得られる「知見の共有」が、より重要になってくると考えられる。IPA では、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。

[25] 「『標的型メール攻撃』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

[26] 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

（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）」[27]とは、経済産業省が事務局として 2013 年 7 月に設置した、経済産業省および同省所管の 10 の独立行政法人（以下、独法）等で構成する会議体である。

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 [28]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」を立ち上げた。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 23 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。今後は、情報共有の実運用を行っていく予定である。

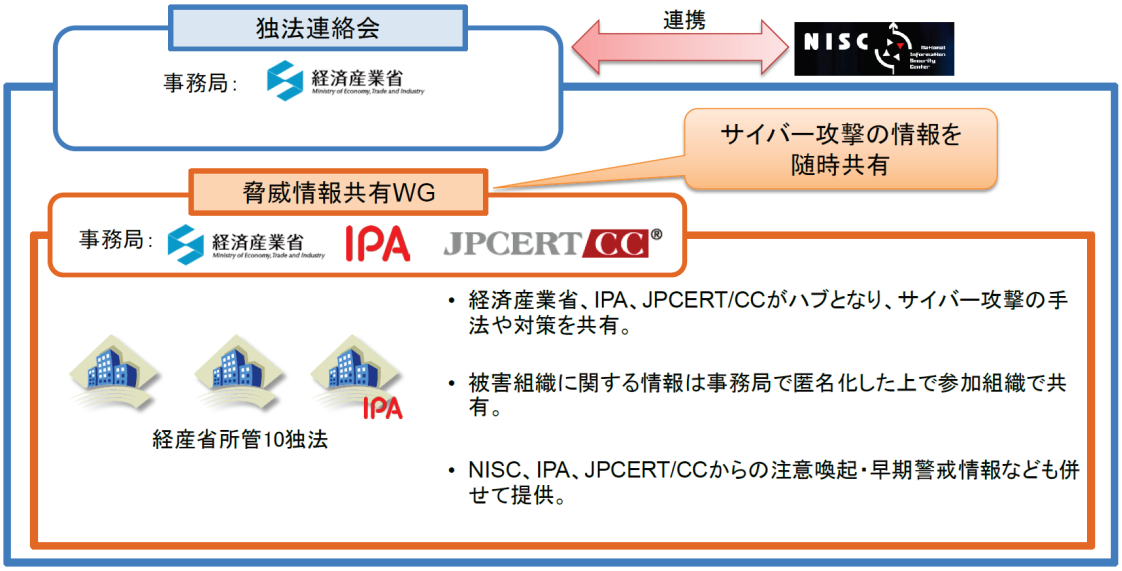


図 23 独法連絡会と脅威情報共有 WG 体制図（経済産業省資料抜粋）

---

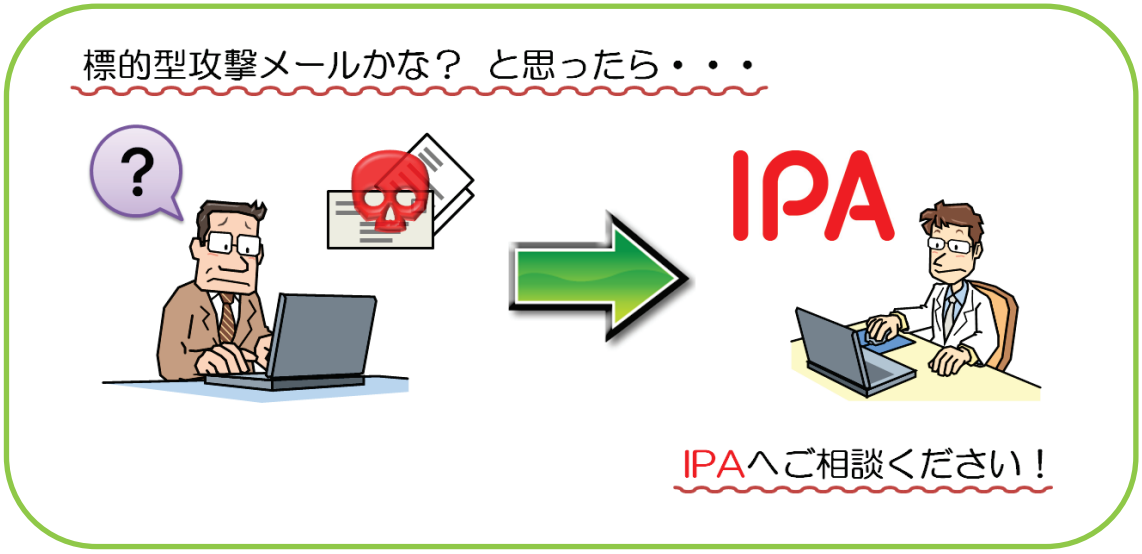
[27] 情報セキュリティ対策推進会議（CISO等連絡会議） 第16回会合（平成26年3月19日）
資料 2-2 「〔経済産業省提出資料〕経済産業省・関係機関情報セキュリティ連絡会議（独法連絡会）」
http://www.nisc.go.jp/conference/suishin/ciso/dai16/pdf/2-2.pdf

[28] 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