Initiative for Cyber Security Information sharing Partnership of Japan

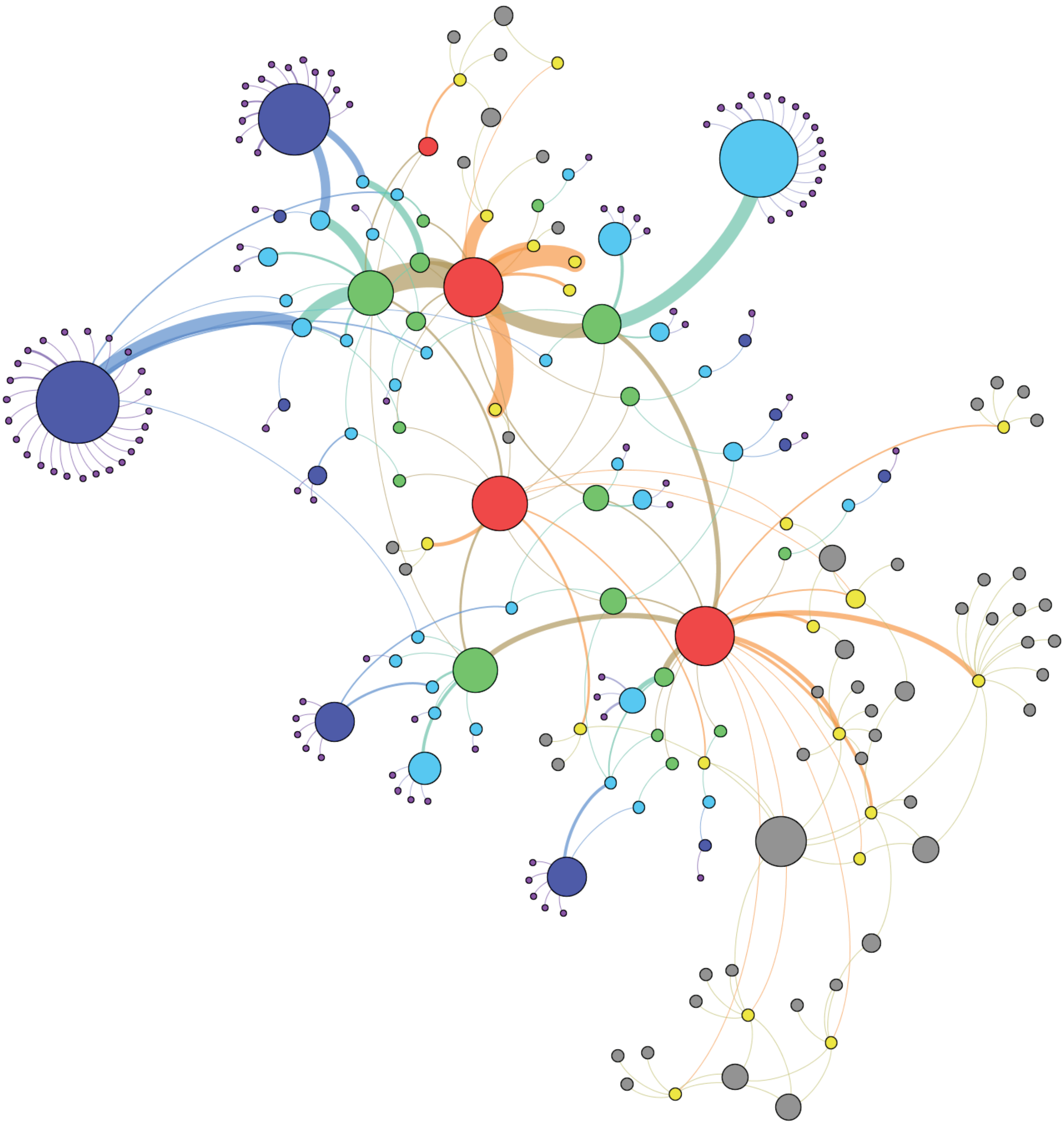
サイバー情報共有イニシアティブ（J-CSIP）

2014 年度 活動レポート　別冊

# 国内組織を狙う執拗な攻撃者「X」の分析

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

このページは空白です。



この図は、J-CSIP で確認された、攻撃者「X」によるものと推定した 114 通の攻撃メールから得られた情報とその関連をグラフで表したものである。色の付いた円(ノード)はそれぞれ、紫:メール受信日、青:メール送信元 IP アドレス、水色:From メールアドレス、緑:メールの騙しの手口、赤:添付されていたウイルスの種別、黄:C&C サーバ、灰色:C&C サーバの IP アドレスを示し、線(エッジ)はノード間の関連を示している。

# 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　別冊
# 国内組織を狙う執拗な攻撃者「X」の分析

## 目次



## 添付資料

・添付資料　「X」による攻撃メール一覧

# 1　はじめに

J-CSIP は、2012 年 4 月からサイバー攻撃に関する情報共有の実運用を開始し、2015 年 4 月より 4 年目の運用に入った。この 3 年間の活動で、不審メールなど、参加組織から IPA への情報提供件数は 1,257 件となり、そのうち、IPA が**標的型攻撃メール**とみなしたものは **939 件**にのぼる。

本書において、標的型攻撃メールとは、情報窃取などを目的として特定の組織に送られるウイルスメールを指し、添付ファイルや罠の URL リンクを開かせるための件名や本文の細工、セキュリティソフトで検知しにくいウイルスの使用といった特徴を持つ。標的型攻撃メールを送りつけてくる攻撃者の第一目的は組織内ネットワークへの侵入のための**踏み台（裏口、橋頭堡）を築くこと**であり、添付されているファイルは、ほとんどの場合、遠隔操作ウイルス（パソコンを外部から遠隔操作する機能を持ったウイルス〔RAT、Remote Access Trojan〕）の一種である。パソコンが遠隔操作ウイルスに感染すると、攻撃者は、**そのパソコンから情報を窃取したり、踏み台として悪用し、組織内の別のパソコンやサーバへと侵入の拡大を試みる。**

これらの標的型攻撃メールや添付されたウイルスの情報を集約し、横断的に分析していくことで、複数の攻撃について、**同一の攻撃者（または攻撃グループ）による一連の攻撃行為であろうと推定できる**ことがある。そして、その一連の攻撃行為について、**攻撃手口がどのようなものか、時とともにどのように変化しているか**といったことも明らかになってくる。J-CSIP の「2013 年度活動レポート」では、その一例として、「やり取り型」の攻撃を行う攻撃者について、その巧妙な攻撃手口や、攻撃者が“学習”していること、そして国内組織が次々と狙われた実態を明らかにした。

同様の横断的な分析により、いくつかの攻撃者像が浮かび上がっている中、本書では、**特に執拗な攻撃者の一つ**について、その一連の攻撃手口や実態を、事例とともに解説する。また、これを通じ、改めて情報共有活動の有効性を示したい。

ここでは仮に、**この一連の攻撃を行っている攻撃者を「X」**と呼ぶ。

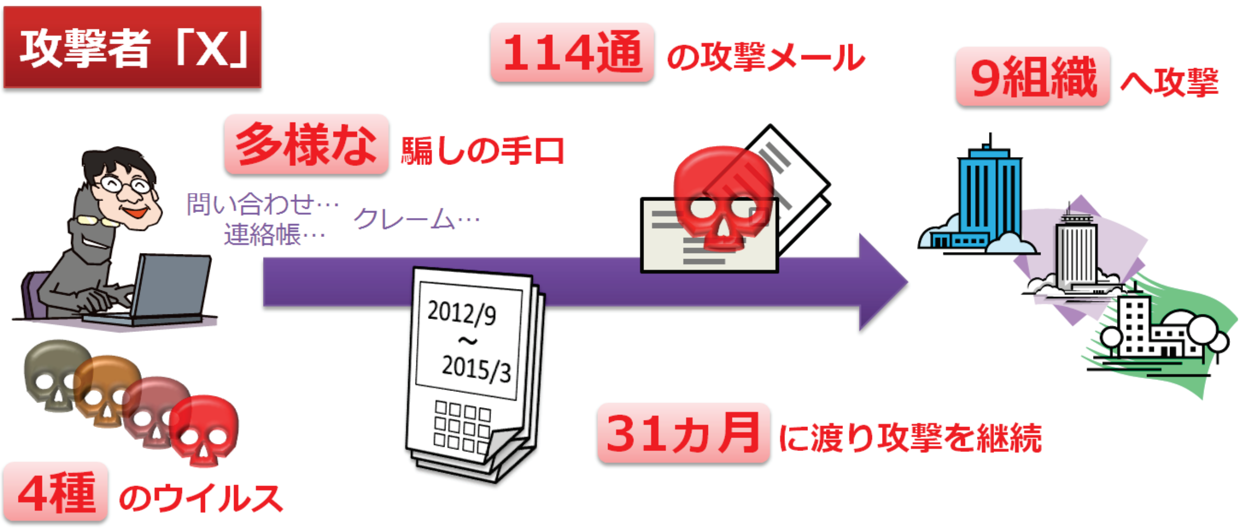



**図 1　攻撃者「X」**

本書では「X」によるものと推定した標的型攻撃メール、**114 通**を取り上げて分析を行う。**多様な**騙しの手口で、**4 種**のウイルスが添付されたこれらの攻撃メールは、J-CSIP 内の **2 つの SIG、9 つの参加組織**において、**31 ヵ月間**に渡り確認されている（図 1　攻撃者「X」）。

## 攻撃者「X」の抽出

J-CSIP は、重要インフラ機器製造業者（重工・重電）をはじめとし、電力・ガス・化学・石油・資源開発の各分野の、国内の重要インフラ/重要産業関連組織により構成されている。そして、秘密保持契約のもと、各組織への攻撃に使われた検体（標的型攻撃メールそのもの）について、極力、生の（未加工の）状態で IPA へ提供いただき、参加組織相互の情報共有を行っている。

このため、提供され、IPA で集約している情報からは、次のような**攻撃の痕跡**を得ることができる。

- メールの件名や本文の文面などの騙しの手口
- メールの送信元 IP アドレス、From メールアドレス
- メールが着信した組織、着信した日時
- 添付ファイルの情報、添付ファイルによって感染させられるウイルスの構造、特徴
- ウイルスが不正な通信を行う先（C&C サーバ[1]）のホスト名、およびその IP アドレス

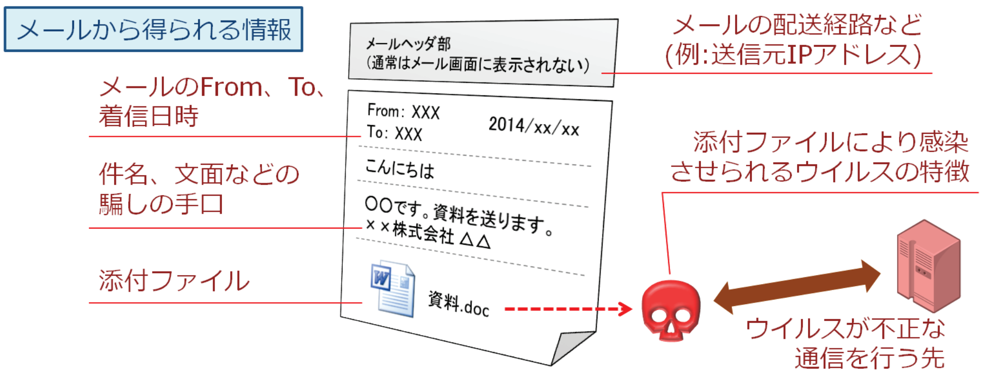



**図 2 メールから得られる情報**

これらの痕跡について相互の関連性を分析することで、**939 通の攻撃メールの情報の中から、同一の攻撃者によるものであろうと推定できた 114 通分（12%）の攻撃メールを抽出した**。「騙しの手口のみ」、「ウイルスの特徴のみ」といった個別の観点では、攻撃間の関係が十分に分からないことがあるが、そのようなケースも含め、本分析では、複数の観点から関連性の確認を行っている。

114 通という件数は、実に J-CSIP で確認してきた全攻撃メールの一割を超える量だが、決して無作為にばら撒かれているものではない。手を替え品を替えつつ長期に渡り確認されてきた攻撃メールは、何らかの共通点によって互いに結びついている。**「X」は、特にその「執拗さ」において、国内組織を狙う攻撃者として注意を要する者**であることに間違いない。

本書では、まず導入として、異なる騙しの手口による 4 件の攻撃メールの事例を紹介する（2 章）。続く 3 章では、2 章で紹介したものを含む 114 通の攻撃メールについて、その関連性を導き出すためのいくつかのアプローチを示しつつ、これらが同一の攻撃者による一連の攻撃であろうと推定した根拠を述べる。

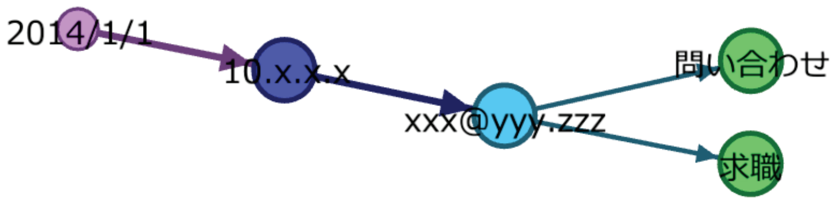
4 章では、攻撃メールとウイルスの着信時期や件数に着目して分析を行う。そして、5 章では、改めて攻撃者「X」による特徴的な攻撃メールの事例を個別に見ながら、この攻撃者の具体的な攻撃手口とともに、考えうる対策を紹介する。

[1] C&C サーバ： Command and Control サーバの略。指令サーバと呼ぶこともある。

## 有向グラフについて

本書では、情報同士の関連性を図示する際、「有向グラフ」を用いている。

本書の有向グラフでは、標的型攻撃メールから得られた個々の情報を「ノード」（節点）と呼び、色の付いた円で表現する。ノードの色は、情報の種類を示す。ノード間に関連性がある場合、矢印でノードを結びつける。この矢印（辺）を「エッジ」と呼ぶ。




上図の例では、「2014 年 1 月 1 日」に、IP アドレス「10.x.x.x」から、メールアドレス「xxx@yyy.zzz」を使ったメールが送信されたことを示している。また、メールアドレス「xxx@yyy.zzz」からのメールは、「問い合わせ」と「求職」を装った 2 種類が確認されたことを示している。円の大きさはそのノードに向かう矢印の多さに従い、矢印の太さは同一の関連性の多さ（例えば、同一の IP アドレスから同一のメールアドレスを使った多数のメールが送信された場合など）に従っている。ノードの位置（配置）、エッジの長さは意味を持たない。

本書で使用しているグラフについて、共通の凡例を次に示す。


**凡例（ノードの色と情報の種類）**

## 2 攻撃メールの事例

本章では、本書で取り上げる標的型攻撃メールがどのようなものかの説明として、4 件の事例を紹介する。

### 2.1 事例 1 - 2012 年 11 月 - 調査事項

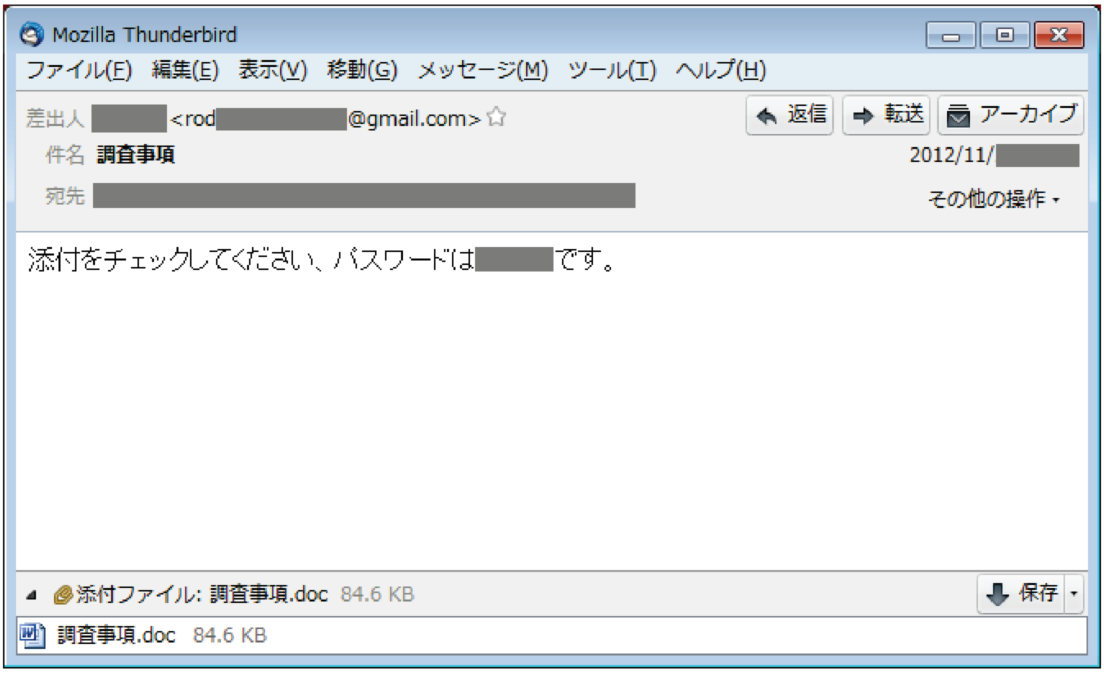



**図 3 事例 1 のメール**

**2012 年 11 月**、J-CSIP の参加組織へ不審なメールが着信した(「図 3 事例 1 のメール」)。メールはフリーメールから送信されており、「調査事項」と称する簡素な内容であった。

このメールの添付ファイル「調査事項.doc」は、Word の文書ファイルで、メールの本文にある通り、Word の機能でパスワードによる閲覧制限が設定されていた。ファイルを開き、メール本文中に書かれたパスワードを入力すると、それらしい文書の内容が表示されるが、**<u>これと同時に</u>**、このファイルに施された細工によって、Microsoft 社製品の脆弱性が悪用され、**<u>パソコンにウイルスを感染させようとする動作が行われる</u>**。

悪用が試みられる脆弱性は、このメール着信から半年ほど前に修正プログラムが提供された「CVE-2012-0158」[2]であった。Windows Update を行っていれば、攻撃(ウイルス感染)は失敗に終わる。

脆弱性の悪用が成功した場合、本書では「X Type1」と呼ぶ、パソコンを遠隔操作するウイルスの一種に感染させられてしまう。

[2] 「Microsoft Office 等の脆弱性について(MS12-027)(CVE-2012-0158)」(IPA)
https://www.ipa.go.jp/security/ciadr/vul/20120411-Windows.html

## 2.2 事例 2 - 2013 年 3 月 - 求職

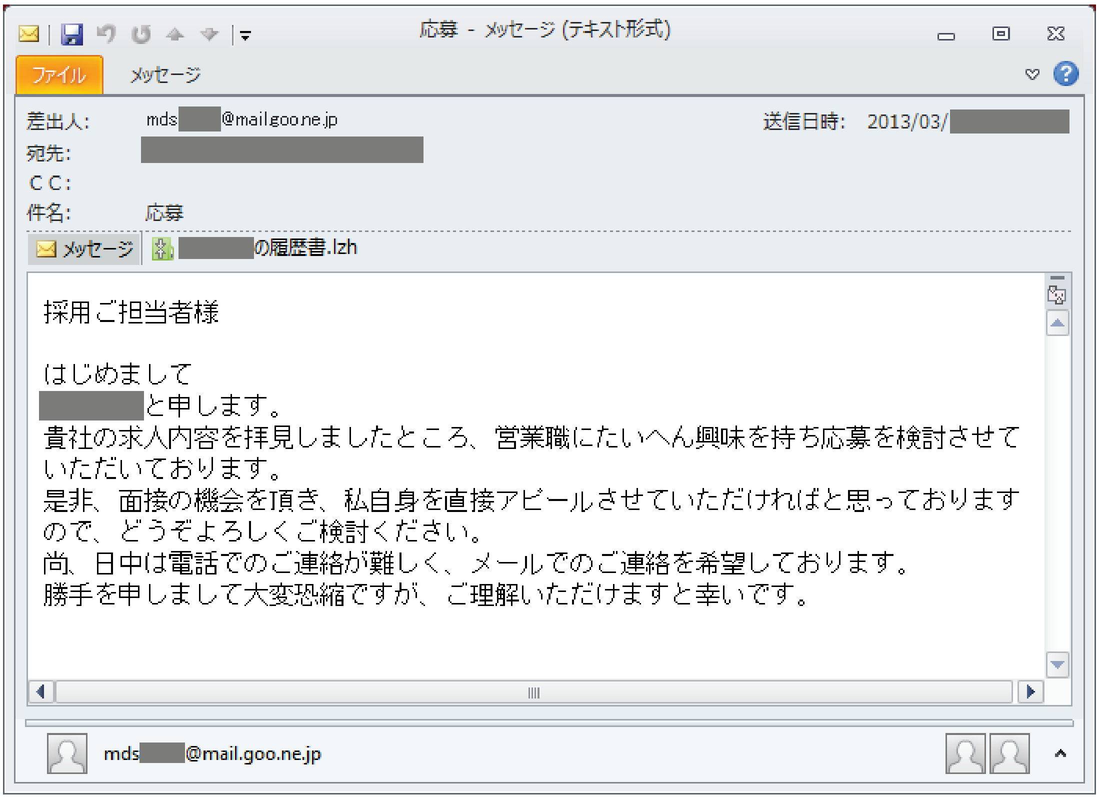



**図 4 事例 2 のメール**

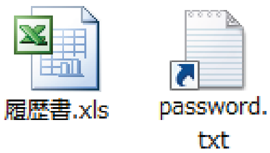



**図 5 事例 2 の添付ファイル(解凍後)**

「図 4 事例 2 のメール」は **2013 年 3 月**の事例である。

国内のフリーメールサービスを使い、「応募」という件名で、求職を装う本文とともに、履歴書と称するファイルが添付されていた。メールには全体的に不審だと気付けるような点が少なく、人事・採用の担当者は添付ファイルを開いてしまう可能性があるだろう。また、本文の「電話でのご連絡が難しく」というくだりは、電話による本人確認(本物のメールであるかの確認)を避けたものと思われる。

添付ファイルは、主に日本で使用されている「LZH 形式」で圧縮されていた。圧縮ファイルを解凍すると、「図 5 事例 2 の添付ファイル(解凍後)」のファイルが得られる。

このうち、「履歴書.xls」は、Excel の機能でパスワードによる閲覧制限が設定された Excel 文書ファイルだが、事例 1 とは異なり、**無害である(ウイルスではない)**。同梱のテキストファイルに偽装した「password.txt」が、実際は「ショートカット(LNK)ファイル」であり、**こちらが罠である**。このファイルを開いてしまうと、事例 1 と同じ「X Type1」と呼ぶウイルスの一種に感染させられてしまう。

このウイルス感染の罠の手口は、J-CSIP で確認している多数の攻撃の中でも、珍しいものであった。

## 2.3 事例 3 - 2014 年 7 月 - 連絡帳

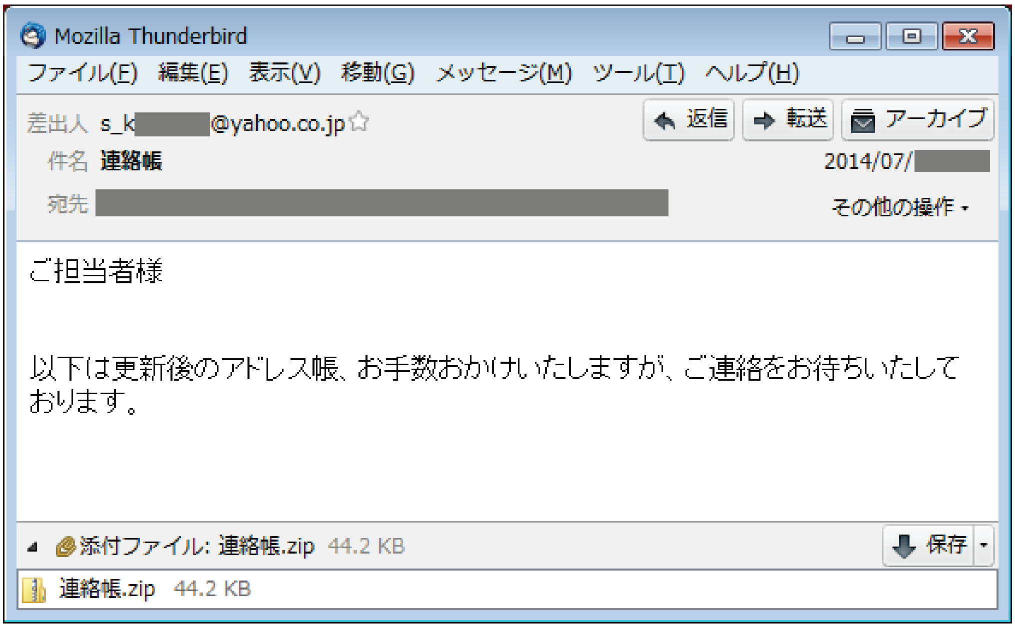



**図 6 事例 3 のメール**


**図 7 事例 3 の添付ファイル(解凍後)**

この「図 6 事例 3 のメール」は、多数確認されている「連絡帳」または「アドレス帳」の送付を装う攻撃メールのうち、**2014 年 7 月**の事例である。このメールも国内のフリーメールサービスを使って送信されている。

添付ファイルは ZIP 形式で圧縮されており、解凍すると「図 7 事例 3 の添付ファイル(解凍後)」のファイルが得られる。このファイルは、**アイコンを Excel 文書ファイルに偽装した実行ファイル**(拡張子「.exe」)であり、ダブルクリックしてファイルを開くと、ウイルスに感染させられてしまう。

アイコンの偽装は、標的型攻撃に限らず、よく悪用される騙しの手口の一つである。この「連絡帳」で使われているアイコンは本物と全く見分けがつかないため、ファイルの拡張子を表示しない設定としていたり、ファイルを開く前にその種類を確認する習慣がなかったりすると、被害に遭ってしまう可能性が高い。

このファイルによって感染させられてしまうウイルスは、事例 1 と 2 とは異なる「X Type4」と呼ぶものの一種である。ウイルスの種類について、詳しくは後述する。

## 2.4 事例 4 - 2014 年 7 月 - 研究に関する問い合わせ

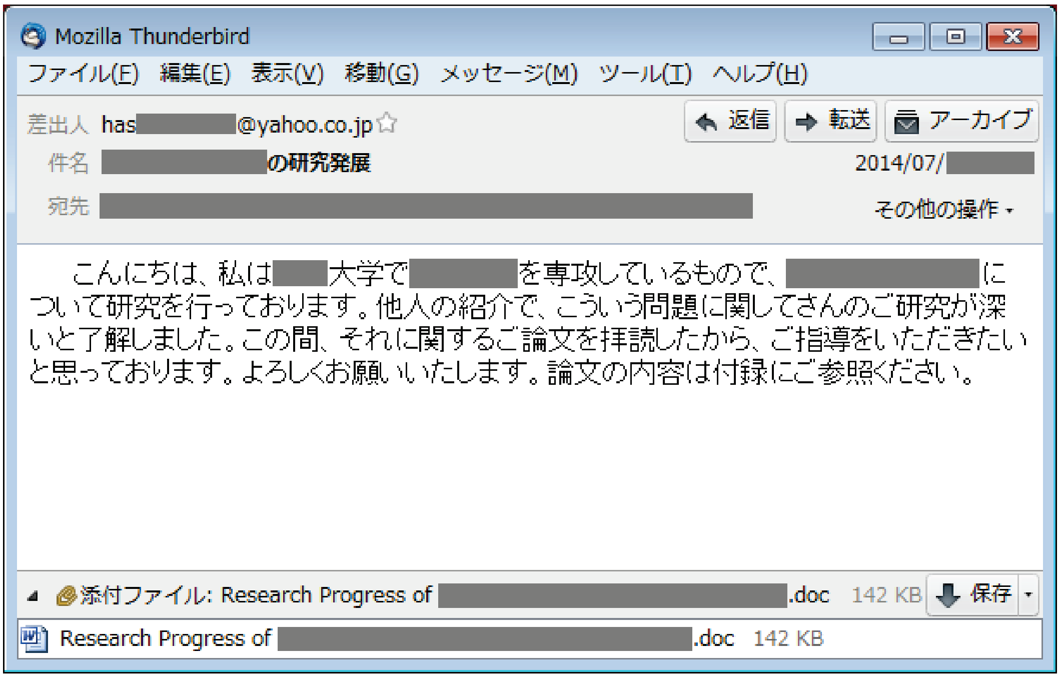



**図 8 事例 4 のメール**

事例 3 と同じく**2014 年 7 月**に確認された攻撃メールを「図 8 事例 4 のメール」に示す。

メールの着信時期は近いのだが、送信元メールアドレス、メールの内容、添付ファイルの形式など、前ページの事例 3 とは全てが異なっている。このメールでは、国内の大学の学生を装い、ある研究テーマについて論文を見ていただきたいと添付ファイルを開くよう促している。日本語の言葉遣いには不自然な点が見られるが、この研究テーマに興味がある人物が本メールを受信した場合は、多少不審だと思っても、添付ファイルを開いてしまう可能性があるだろう。

添付ファイル「Research Progress of ….doc」は、Word の文書ファイルで、Microsoft 社製品の脆弱性を悪用するものであった。悪用が試みられる脆弱性は、事例 1 と同じ「CVE-2012-0158」である。修正プログラムの公開から 2 年以上経っており、2012 年以降 Windows Update を全く実施していないようなパソコンでなければ、攻撃(ウイルス感染)は成功しない。この攻撃者が、なぜこのような(攻撃の成功の見込みが薄い)古い脆弱性を悪用しようと試みているのかは不明である。

脆弱性の悪用が成功した場合、事例 3 と同様、「X Type4」と呼ぶウイルスの一種に感染させられてしまう。

## 2.5 事例の整理

本章では、それぞれ、着信時期だけでなく、メールの題材や添付ファイルの形式が様々に異なる 4 件の事例を紹介した。各事例の特徴点を改めて整理したものを「図 9 4 つの事例の整理」に示す [3]。

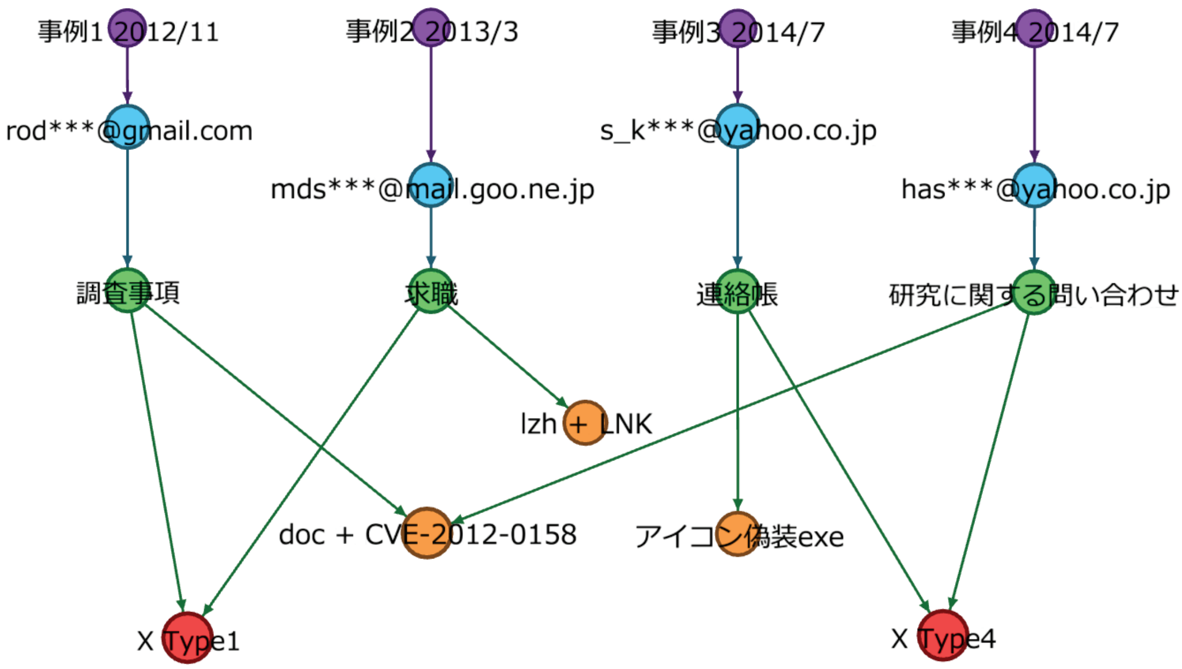



**図 9 4 つの事例の整理**

この 4 件の表面的な部分だけを見ても、関連性はほとんど見いだせない。フリーメールを使っている点は 4 件で共通しているが、これは近年の標的型攻撃メール全般で見られる特徴である。また、事例 1 と事例 4 では、添付された Word 文書ファイルが悪用する脆弱性が同一であるが、この「CVE-2012-0158」は、標的型攻撃に限らず、ウイルスを感染させる手口として広く悪用されているもので、これだけで関連性を判断することも、また難しい。

ただ、添付ファイルによって感染させられてしまうウイルスの種類については、事例 1 と 2、事例 3 と 4 で、それぞれ類似性が見られた。これは、ウイルスの特徴が似ているということであって、完全に同一のウイルスが添付されていたわけではないが、<u>**関連性を示す重要な手がかり**</u>である。

次章では、この 4 件の事例を含む 114 通の攻撃メールについて、その関連性を探っていく。

[3] 便宜上、本書の中で、このグラフでのみ「添付ファイルの種類とウイルス感染手口」として、オレンジ色のノードを使用している。

## 3　攻撃の関連性の分析

本章では、いくつかのアプローチによって、多数確認されてきた攻撃メールの関連性を横断的に分析する。

### 3.1 攻撃メールで使われた「騙しの手口」とウイルスの種別

件名、本文、添付ファイル名やアイコンに工夫を凝らし、メールの受信者の興味を惹き、詳細を確認する必要があると思わせ、添付ファイルを開かせる（あるいは URL リンクをクリックさせる）手法を、本書では**「騙しの手口」**と呼ぶ。

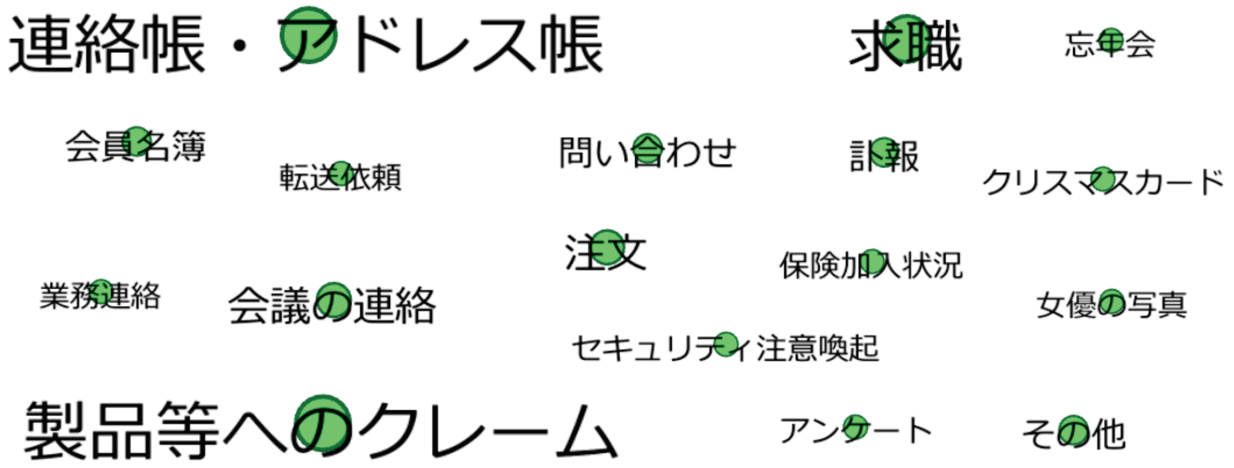



**図 10　騙しの手口**

「図 10　騙しの手口」は、本書で取り上げる攻撃メール 114 通で使われた騙しの手口について、**メールの題材をもとに 17 種に分類**した[4]ものである（円と文字の大きさは、関連する送信元メールアドレスの数に従っている）。

このうち、先の「事例 3」のような「連絡帳・アドレス帳」を題材としたメールが最も多く、計 39 通（34%）を確認している。次に、「事例 2」のような「求職」を題材としたメールが 26 通（23%）、そして「製品等へのクレーム」が 11 通（10%）と続く。文面が似たような攻撃メールが長期に渡り多数確認されたことは、本分析を行った一つのきっかけとなっている。

17 種の題材を全体的に見てみると、業務上の連絡を装ったものから、単純に受信者の興味を惹くことを目的としたようなものまで、**様々なバリエーションが存在している**ことが分かる。なお、このうち 7 種については、それぞれ 1 通の攻撃メールのみしか確認していない。攻撃者「X」は、「類似の手口で多数へ攻撃」と、「個別の手口で少数へ攻撃」を使い分けているか、もしくは、「X」の中に複数の攻撃者が存在している可能性が考えられる。

[4] 「騙しの手口」には、メールの題材だけでなく、添付ファイルを開かせるための様々な細工も要素として含まれるが、本書では題材を最も重要な要素として分類に使用している。

これらの攻撃メールに添付されていたウイルスについて、IPA ではそれぞれの特徴から「図 11 ウイルスの種別」のとおり、大きく 4 種類に分類しており、ここでは「X Type1」～「X Type4」と呼ぶことにする。


**図 11 ウイルスの種別**

このうち、「X Type1」～「X Type3」の 3 種については、ウイルスの動作や外部との不正通信のパターンに類似性が見られ、**「X Type1」をもとに、「X Type2」および「X Type3」が派生して開発された可能性が高い**と推測している。
例えば、「X Type1」～「X Type3」は、他のウイルスには見られない特徴的な方法で、自身（ウイルス）が動作している環境がインターネットにアクセスできるか否かを確認する機能を共通して持っている。それに加え、「X Type2」と「X Type3」は、自身が動作している環境が、ウイルスを解析するための装置であるかを見破る機能が追加され、また、通信電文の内容が変化した。ただ、全体的な構造は似通っている。

ところが、**「X Type4」については、他の 3 種と特徴が大きく異なる**。ウイルスを単体で分析しても、他の 3 種のウイルスとの確たる関連性は見いだせない。それでも、このウイルスを「Type4」として位置付けたのは、ウイルスの特徴ではなく、別の観点から、これが「X Type1」～「X Type3」の攻撃者によるものであろうと推定できたためである。

3.2 章と 3.3 章では、この「X Type1」～「X Type4」について、相互の関連性を見いだすための分析を試みる。更に、3.4 章では、「X Type1」～「X Type4」のウイルスが添付されていたメールについて、その送信元に関する情報に着目し、同じように関連性を見いだすための分析を行う。
3.5 章では、これらの分析で得られた推論、「ウイルスに関連性がある」であろうこと、また、それらのウイルスが添付された「メールについても関連性がある」であろうことを踏まえ、攻撃者「X」の残した痕跡の全体像を整理する。

### 3.2 ウイルスの不正接続先による関連性

最初に、ウイルスの特徴点の一つである「不正接続先」の観点で分析を行う。標的型攻撃で使われるウイルス全般に言えることだが、パソコンに感染したウイルスは、攻撃者からの遠隔操作の指令を受けるなどの目的で、外部のサーバ(攻撃者の管理下にあると思われるマシン、C&C サーバ)と通信を行うことが多く、「X Type1」~「X Type4」もその機能を持っている。

「図 12 ウイルスの不正接続先」は、本件で確認されたウイルスの不正接続先の一覧である。「X」のウイルスは通信に HTTP[5]を用いており、**<u>利用者のウェブ閲覧による通信に紛れる</u>**ようにして、不正な通信を行う。不正接続先には「www.~」というホスト名が多く、システム管理者によって通信ログを確認された場合でも、正常な通信であるかのように誤認させる目的があるのではないかと思われる。

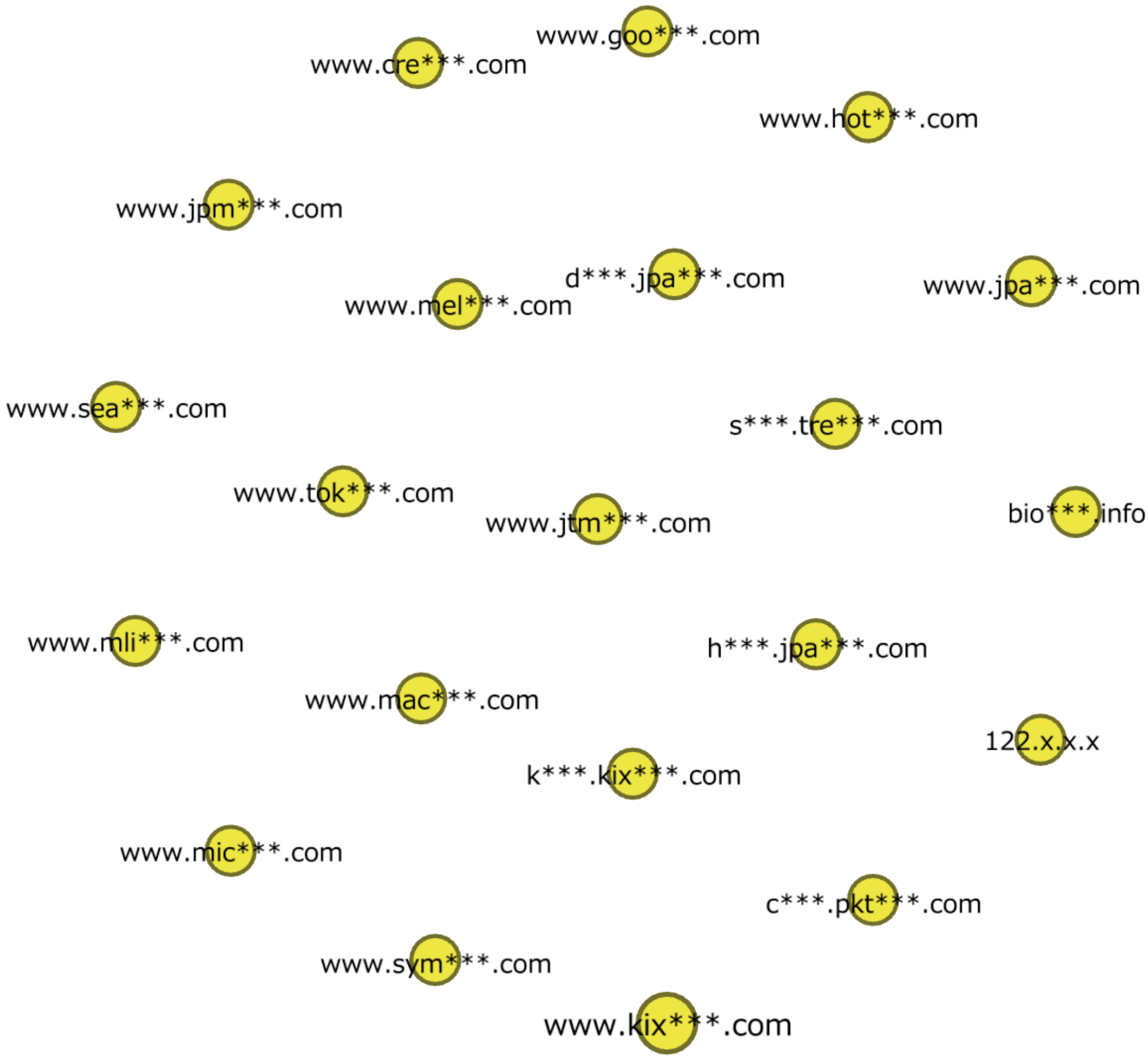



**図 12 ウイルスの不正接続先**

[5] Hypertext Transfer Protocol の略。ウェブページなどの閲覧の要求・応答に使用する通信規約(プロトコル)。

次の「図 13 ウイルスの種別と不正接続先の関連」は、これらの不正接続先（黄色のノード）について、「X Type1」～「X Type4」のどの種別のウイルス（赤のノード）が不正な通信を試みるかをグラフにしたものである。

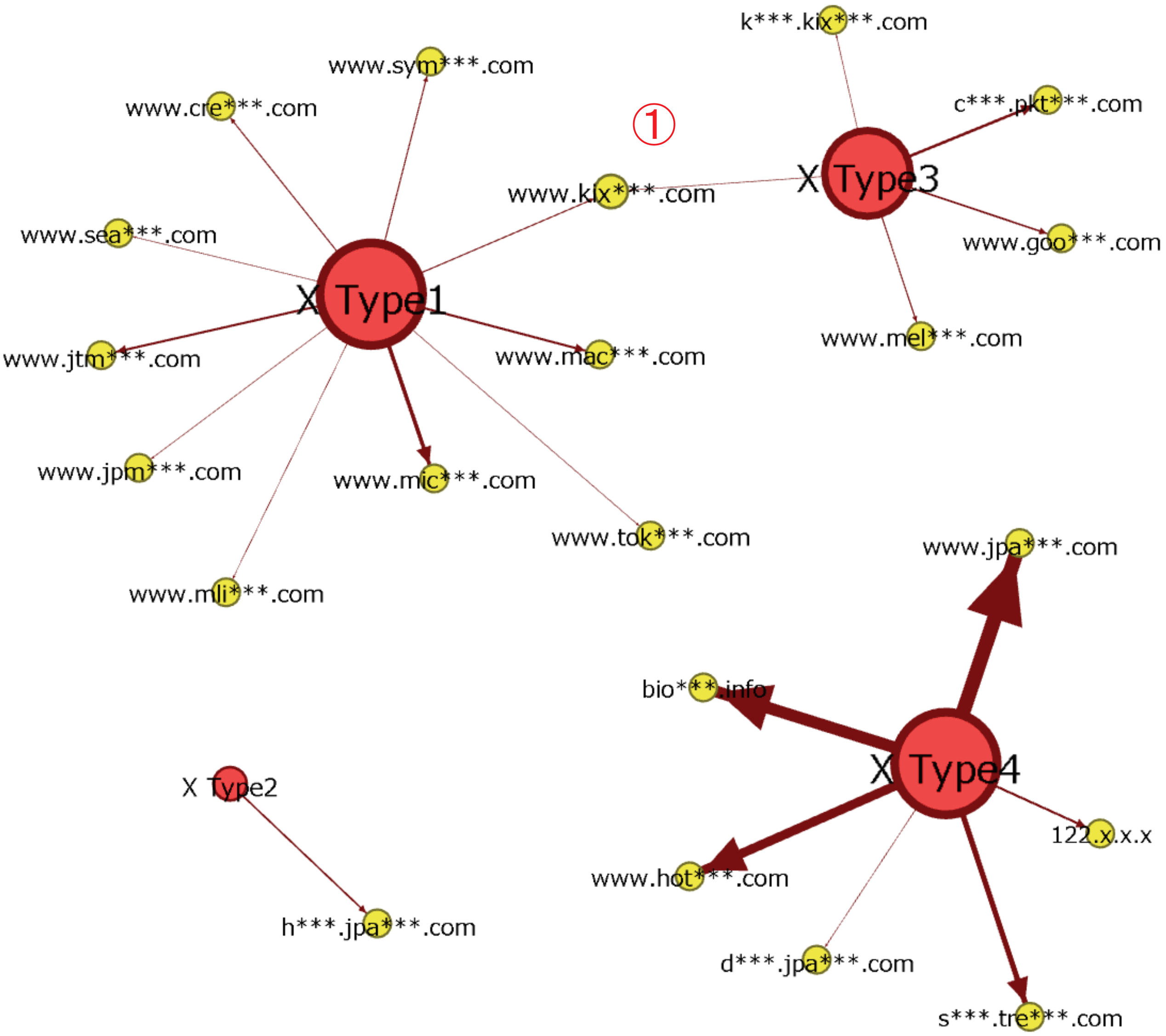



**図 13 ウイルスの種別と不正接続先の関連**

このグラフからは、次の点を読み取ることができる。

- 同じ種別（Type）であっても、不正接続先が様々に異なる亜種が存在する。また、**基本的には種別が異なると、不正接続先も異なる**。
- 唯一、**「X Type1」と「X Type3」で不正接続先が重複した**事例（「www.kix***.com」、図中①）が確認されている。これは、「X Type1」と「X Type3」が同じ攻撃者によるウイルスであることの、ひとつの根拠になりうる。
- 攻撃者は、時間とともに新たな不正接続先を用意して使っていると思われる。それでも、時期が近い攻撃では、同じ不正接続先を使い回したウイルスを多数へ送信しているケースもある（グラフの矢印の太さは、攻撃メールの多さに従っている）。

更に、それぞれの不正接続先の IP アドレス [6]の情報（灰色のノード）を追加し、その関連を分析する。「図 14 ウイルスの不正接続先とその IP アドレスの関連（1）」は、「X Type1」と「X Type3」を起点として得られるグラフである。

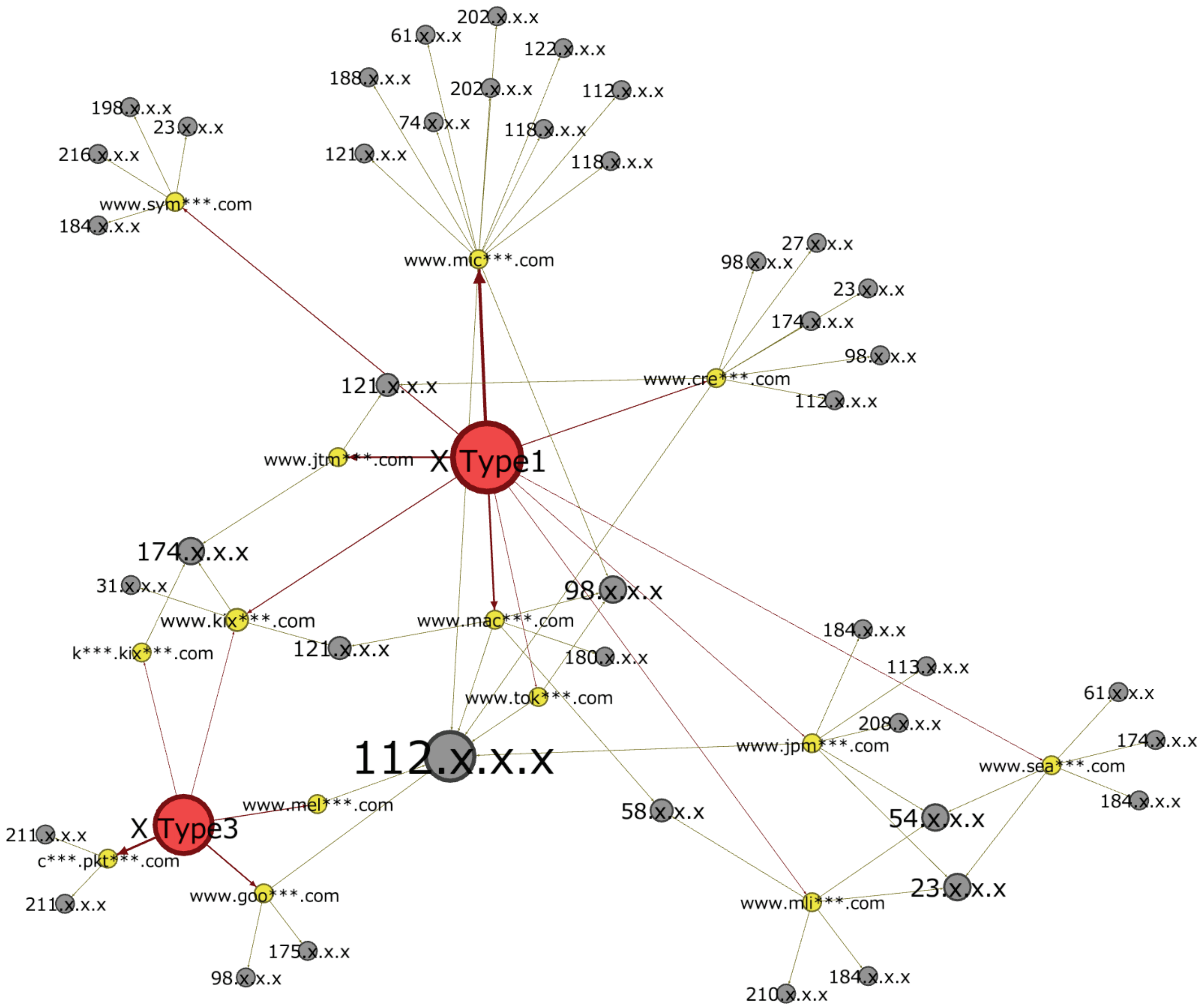



**図 14 ウイルスの不正接続先とその IP アドレスの関連（1）**

前述の通り、「X Type1」と「X Type3」では不正接続先のホスト名が重複した事例があるため、このグラフでも繋がりがあるのだが、ここでは更に多くの関係性が確認できる。「X Type1」の不正接続先同士は、共通の IP アドレスが割り振られていた時期があり、IP アドレスの情報を経由した網の目のような関係となった。これは、「X Type1」と分類しているウイルスの亜種の間にも、強い関連があるであろうことを示している。

「X Type1」と「X Type3」の間でも、不正接続先のホスト名に加えて、新たに IP アドレスの情報を経由した繋がりが数か所で現れており、「ウイルスの特徴が似ている」のみではない関連性があることが推定できる。

[6] 当該ホスト名を DNS によって名前解決して得られた IP アドレス。時間とともに変化することがあり、ここでは変化後の IP アドレス（2015 年 3 月末まで）も全て含んでいる。

次の「図 15 ウイルスの不正接続先とその IP アドレスの関連(2)」は、図 14 と同様、「X Type2」と「X Type4」を起点としたグラフである。

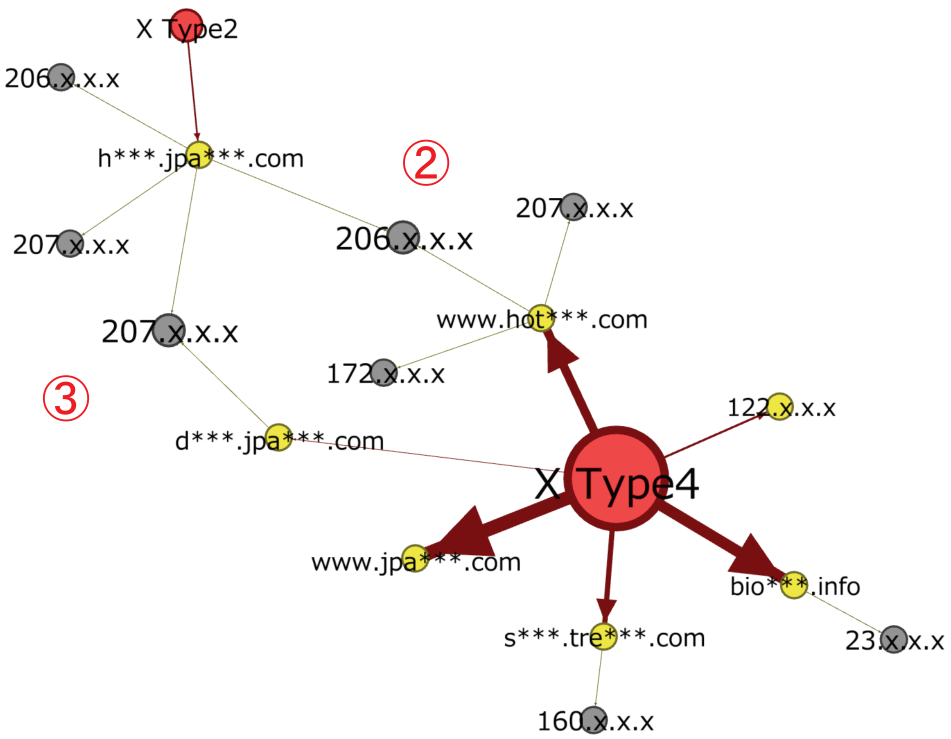



**図 15 ウイルスの不正接続先とその IP アドレスの関連(2)**

図 13 では「X Type2」と「X Type4」には接点が無かったが、不正接続先の IP アドレスの情報を追加することで、2 つの経路で繋がりが現れた(IP アドレス「206.x.x.x」〔図中②〕と「207.x.x.x」〔図中③〕を共有している)。特に、「X Type2」の攻撃メールは 3 通、不正接続先は 1 つしか確認できていなかったため、この観点で関係性が得られたことは、重要な手がかりである。

一方で、IP アドレスの情報を加えても、なお図 14 と図 15 のグラフは完全に 2 つに分かれており、**「Type1＋Type3」と「Type2＋Type4」の間は、この観点では関連性が見られない**という結果となっている。

### 「不正接続先 IP アドレスによる関連性」の注意点

本分析では、それぞれの不正接続先について、攻撃が発生した(正確には、IPA がその不正接続先の情報を入手した)時点での IP アドレスだけでなく、その後、名前解決先が変化して得られた IP アドレスも情報として使用している。これは、攻撃者が何らかの理由で C&C サーバなどを移転し、それに合わせて DNS の設定を変えたという可能性があるためである。

一方で、当該ホスト名やドメインについて、攻撃者が管理権を放棄した場合、その管理権を別の者が得て、無害な IP アドレスやウイルス感染マシン特定用の IP アドレスに振り向けられることがある(シンクホール化などと呼ばれる)。この場合は攻撃者の意図と関係なくホスト名と IP アドレスとの間で関係性が生じてしまうため、本手法による関連性の分析にはノイズが含まれる可能性がある(関連性を示す絶対的な確証にはならない)という点には、注意が必要である。

### 3.3 X Type3 と X Type4 の繋がり

次は、ある 1 つの事例から「X Type3」と「X Type4」の繋がりを示す。

この攻撃メールは **1 通**しか確認できていない。メールには、ある女優のプライベート写真と称し、ZIP 形式のファイルが添付されていた（「図 16 「女優の写真」の添付ファイル」）。


**図 16 「女優の写真」の添付ファイル**

添付ファイルを解凍すると、「図 17 「女優の写真」（解凍後）」に示す **5 つのファイル**が得られる。


**図 17 「女優の写真」（解凍後）**

このうち、一番左のファイルは、画像ファイルのようにアイコンを偽装しているが、拡張子が「.exe」となっている実行ファイルであり、**ウイルスに感染させる罠**である。残りの 4 つのファイルは無害な画像ファイルで、**「複数の無害なファイルの中に罠を 1 つだけ混ぜる」**という手口は、J-CSIP 全体においても、この攻撃者「X」でしか確認していない。「図 18 「女優の写真」（プレビュー表示）」のように、「プレビュー表示」モードにすると、罠のファイルだけはアイコンが変化しないことが分かる。


**図 18 「女優の写真」（プレビュー表示）**

この事例は攻撃の手口としても珍しいものであったが、それよりも重要な点がある。罠のファイルである「01.exe」を実行してしまった場合、そのパソコンは、**「X Type3」と「X Type4」の 2 つのウイルスに同時に感染する**のである。そして、それぞれ異なる特徴の不正通信が同時に試みられる。

このようなケースは非常に稀であり、当時はこの事例の重要性が分からなかった。しかし、全体の情報を突き合わせてみると、このメールの着信時期は、攻撃者が使用するウイルスが**「X Type1」～「X Type3」から、「X Type4」へ切り替わった時期とも一致**している。このウイルスが添付された攻撃メールは、全 114 件の攻撃を 1 つに紐づけるための、最も重要な証拠のひとつである。

## ウイルスの関連性のまとめ

ここまで示した内容をまとめると、次のとおりである。

- 「X Type1」、「X Type2」、「X Type3」は、ウイルスの動作・構造などの特徴が似ている。
- 「X Type1」と「X Type3」では、同一の不正接続先のホスト名が確認された事例があった。
- 「X Type2」と「X Type4」では、同一の不正接続先 IP アドレスが確認された事例があった。
- 1 つのウイルス（正確にはウイルスに感染させるウイルス）によって、「X Type3」と「X Type4」に同時に感染させられるものがあった。

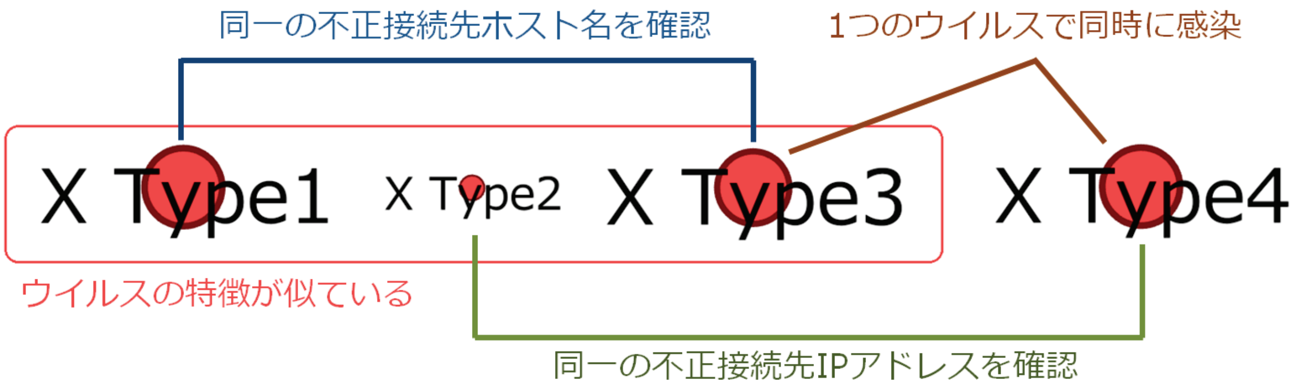



**図 19 4 種のウイルス間の関連性**

### 3.4 メールの送信元による関連性

続いて、ウイルスからは一旦離れ、**攻撃メールの送信元**に着目した分析を行う。

まず、「図 20 From メールアドレスと騙しの手口」は、攻撃者が使用した多数のメールアドレス（水色のノード）から、それぞれ、どの騙しの手口（緑のノード）を使うメールが送信されたかを示すグラフである。

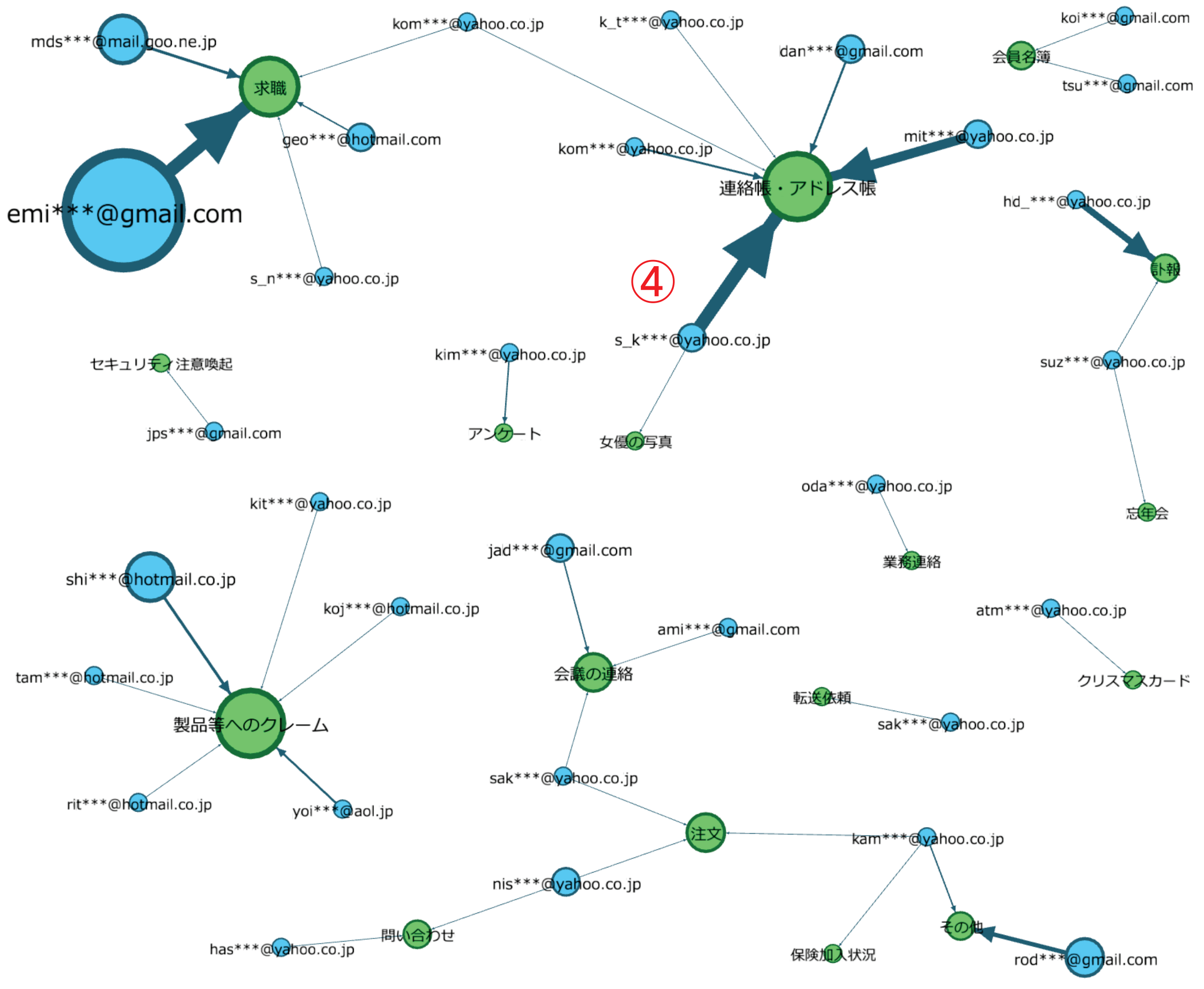



**図 20 From メールアドレスと騙しの手口**

このグラフからは、次の点を読み取ることができる。

- 攻撃者は**同じような騙しの手口を使い回しつつ**も、**メールアドレスを変えながら**攻撃を行っている。
- 数多く確認された騙しの手口がある一方、メールの件数が少なく、**メールアドレスと騙しの手口の両方を使い捨てにした**と思われるケースも複数ある。このため、グラフが全体的に分断されている。

なお、3.3 章で紹介した「女優の写真」は、グラフ中央（④）にある「s_k***@yahoo.co.jp」から送信された。このメールアドレスからは、グラフにあるとおり、他に「連絡帳・アドレス帳」を題材としたメールが多数（約 1 年に渡り計 18 通）送信されたことを確認している。

次の「図 21 メール送信元 IP アドレス」は、図 20 に、**それぞれのメールの送信元 IP アドレス**（攻撃者がメールを送信する際に使用したと思われるマシンの IP アドレス、青のノード）を追加したグラフである。

攻撃者は、多数のメールアドレスを用意し、そこから様々な騙しの手口を使った攻撃メールを送っているが、確認できた範囲において、**実際にはメールの送信元 IP アドレスの数はそれほど多くない**。

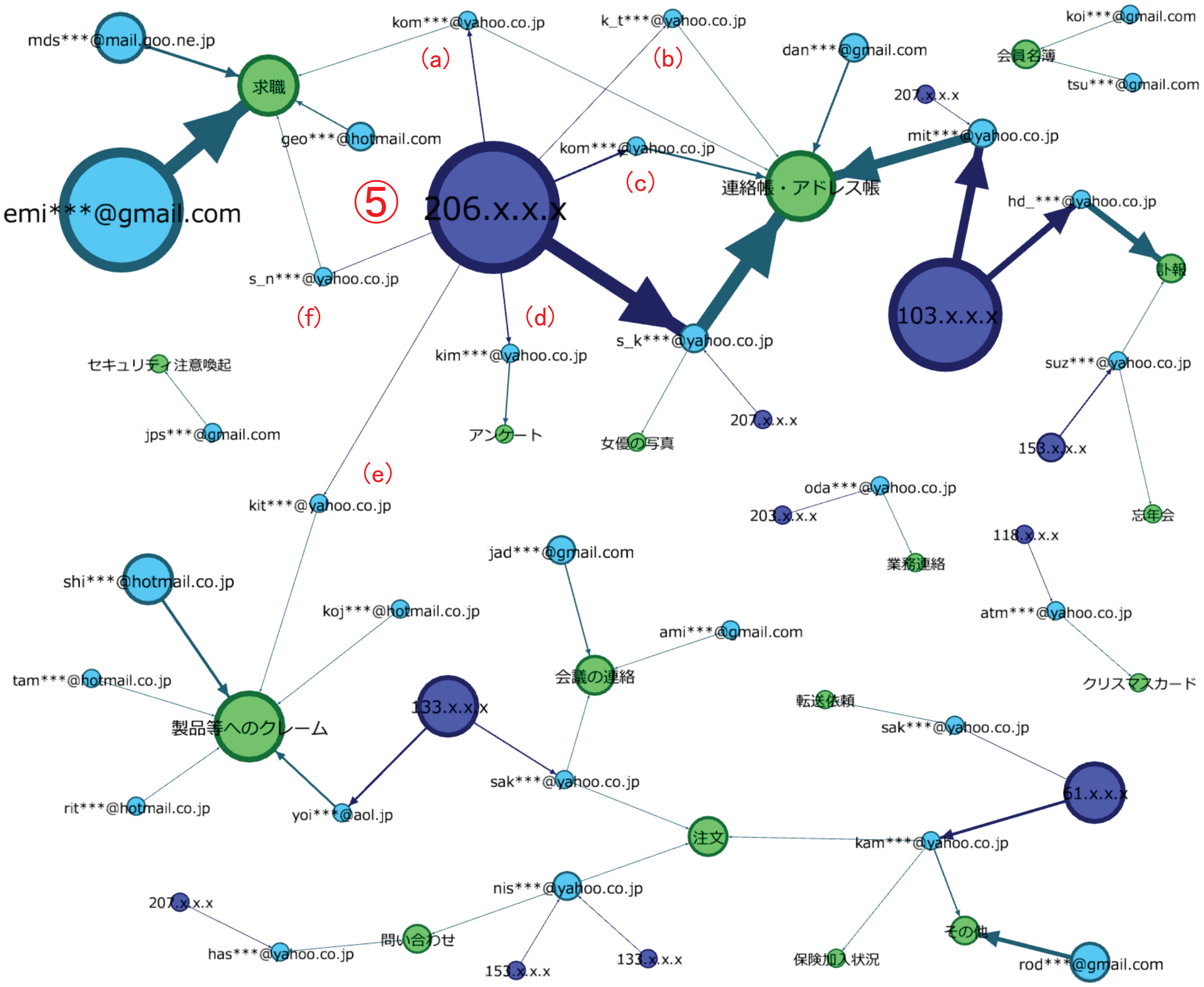



**図 21 メール送信元 IP アドレス**

例えば、先ほどの「女優の写真」の「s_k***@yahoo.co.jp」に着目すると、このメールアドレスは 2 つの送信元 IP アドレスから使われており、そのうち「206.x.x.x」（⑤、大きな青のノード）からは、**別の 6 つのメールアドレスを経由して攻撃メールが送信されている**（図中（a）～（f））。これにより、「求職」「製品等へのクレーム」「アンケート」といった他の騙しの手口とも繋がりが現れる。

一部を除き、他のノードも送信元 IP アドレスの情報によって全体が数珠繋ぎ状に接続されており、この分析の観点においても、大部分のメールについて関連性が浮かび上がっている。

「図 20 From メールアドレスと騙しの手口」の説明の際、From メールアドレス「s_k***@yahoo.co.jp」から、「女優の写真」(1 通)以外にも「連絡帳・アドレス帳」を題材としたメールが 18 通送信されたと述べた。

「図 22 「s_k***」からのメールとウイルス種別」のグラフは、「s_k***@yahoo.co.jp」から送信された「連絡帳・アドレス帳」の 18 通のメールのみを抜き出し、メール受信日(紫)[7]、メール送信元 IP アドレス(青)、From メールアドレス(水色)、ウイルスの種別(赤)、不正接続先(黄)の情報の関連性を示したものである(騙しの手口(緑)は全て「連絡帳・アドレス帳」であるため、グラフに含めていない)。

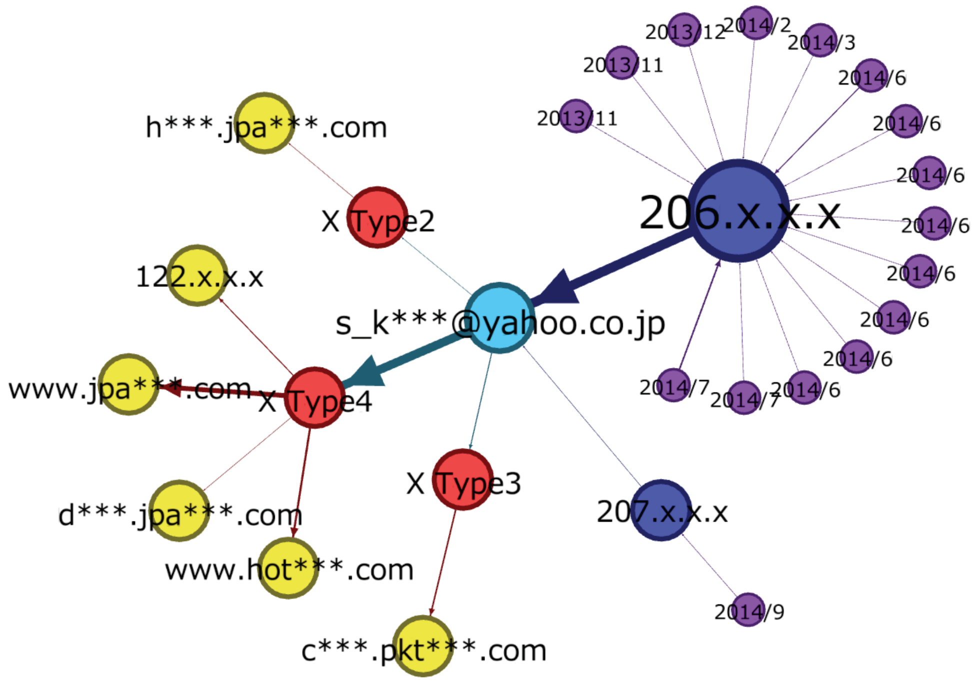



**図 22 「s_k***」からのメールとウイルス種別**

このグラフにあるとおり、「s_k***@yahoo.co.jp」という同一のメールアドレスから送られたメールで、**3 種のウイルスが添付されていた**ことが確認されている。具体的には、「X Type2」が 1 件、「X Type3」が 2 件、「X Type4」が 15 件である。この事実も、これらが一連の攻撃であることを強く示している。

また、本書では詳細を省略するが、同一の IP アドレスが「メール送信元 IP アドレス」と「不正接続先の IP アドレス」の両方で現れた事例も数件確認した。攻撃者は、メールアドレスだけでなく、攻撃に使用するマシンなども、用途を変えたり、期間を置いたりして使い回ししているものと思われる。

7 メール受信日(紫のノード)は、16 個(16 通り)となっている。すなわち、18 通のうち 2 通は、他のメールと受信日が一致しており、複数の宛先へ同報で送信されたと思われるメールである。

## 3.5 攻撃の関連性の整理

ここまで、ウイルスの観点（種別、不正接続先）、メールの送信元の観点（From メールアドレス、IP アドレス）、それぞれから関連性を検証した。これらを基に、IPA では、この 17 種の騙しの手口、添付されていた 4 種のウイルスを用いる者が、同一の攻撃者（または攻撃グループ）「X」であると推定している。

次の「図 23 騙しの手口とウイルスの種別の関連」は、攻撃メールで使われた騙しの手口と、そのメールに添付されていたウイルスの種別について、その関係をグラフにしたものである。

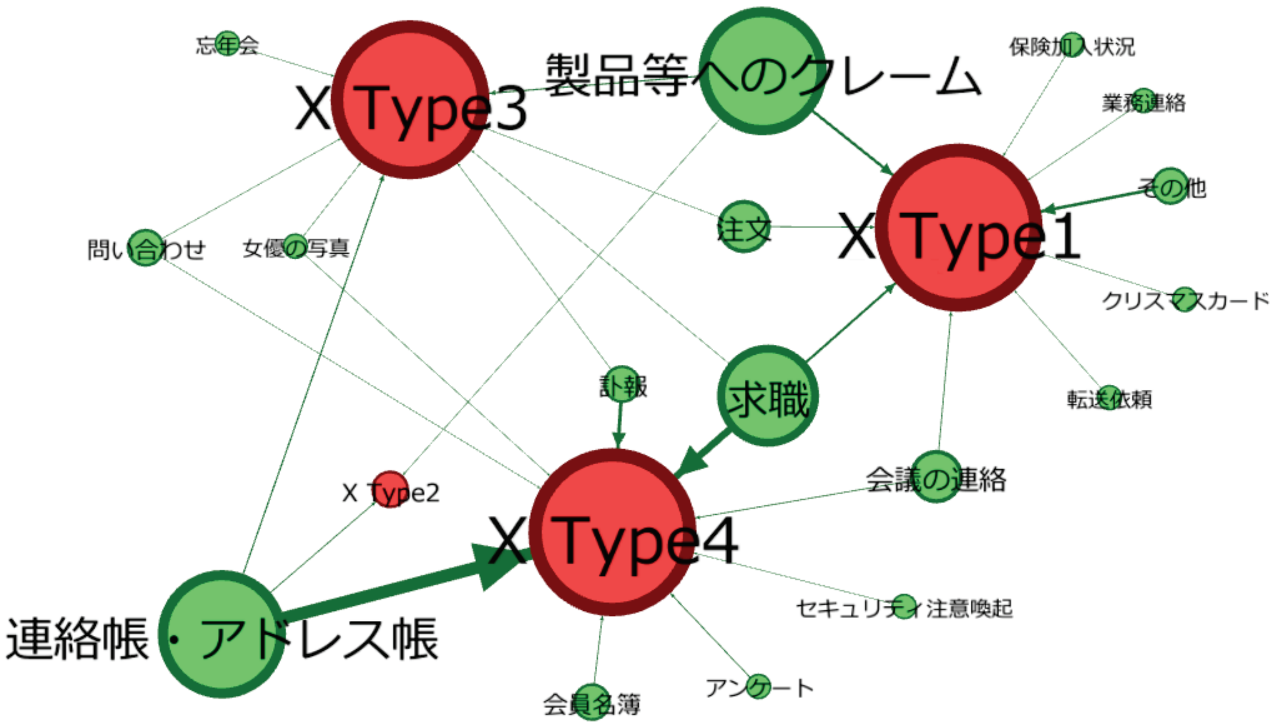



**図 23 騙しの手口とウイルスの種別の関連**

このグラフを見ると、「X Type1」～「X Type4」のウイルスが、様々な騙しの手口とともに送られており、また、時には**<u>同じ題材を使いつつ別の種別のウイルスが送られている</u>**様子が分かる。「X Type2」が添付された攻撃メールは 114 通の中で 3 通しか確認できていないが、騙しの手口は他で多く確認されているものと類似しており、この点からも、やはり「X Type2」も攻撃者「X」による一連の攻撃の一部だと考えることができるだろう。

参考として、3 章で使用した情報全てを含むグラフ「図 24 攻撃情報のグラフ全体図」を示す。表現形式が異なるが、本書の最初のページにある図も、これと同等のグラフである。

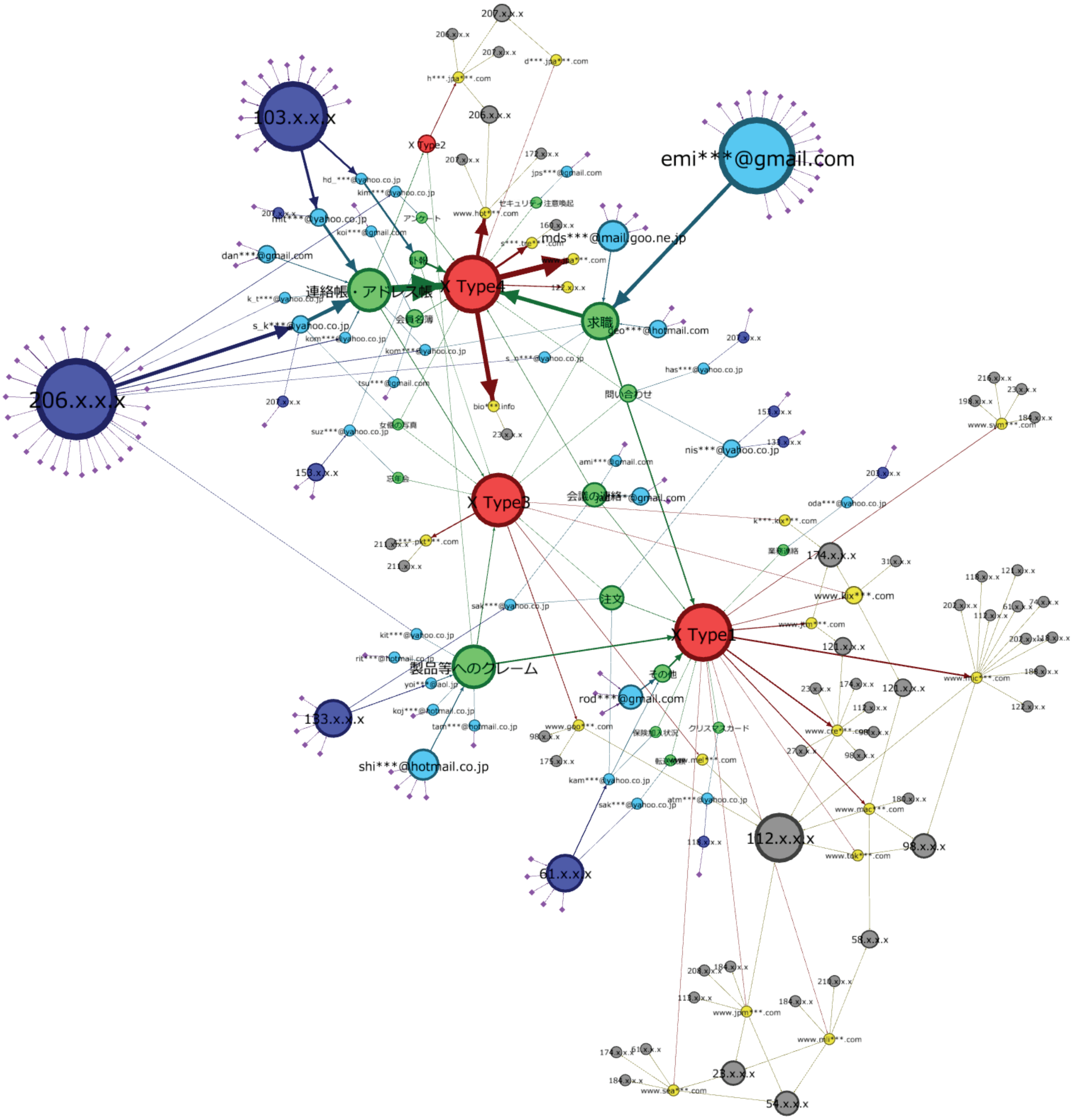



**図 24 攻撃情報のグラフ全体図**

# 4　攻撃メールの着信時期と件数

本章では、攻撃メールの着信時期と件数に着目し、攻撃の状況を俯瞰、分析する。

## 4.1 件数の統計

J-CSIP では、攻撃者「X」によるものと推定するメールについて、最初に確認した **2012 年 9 月**より、本分析を行った 2015 年 3 月までの **31 ヵ月間**に渡り、断続的に確認している。

月ごとの攻撃メール着信件数を「図 25　攻撃メール件数：月統計」に示す。全体的に波があり、攻撃が無い時期もあれば、月に 20 件前後の攻撃が確認されることもあった。なお、本分析には含めていないが、IPA では、攻撃者「X」によるものと思われる攻撃メールの情報を J-CSIP 外の組織からも入手しており、この攻撃は国内組織に広く（ただし、無作為ではなく）、長期間に渡って執拗に行われていると認識している。

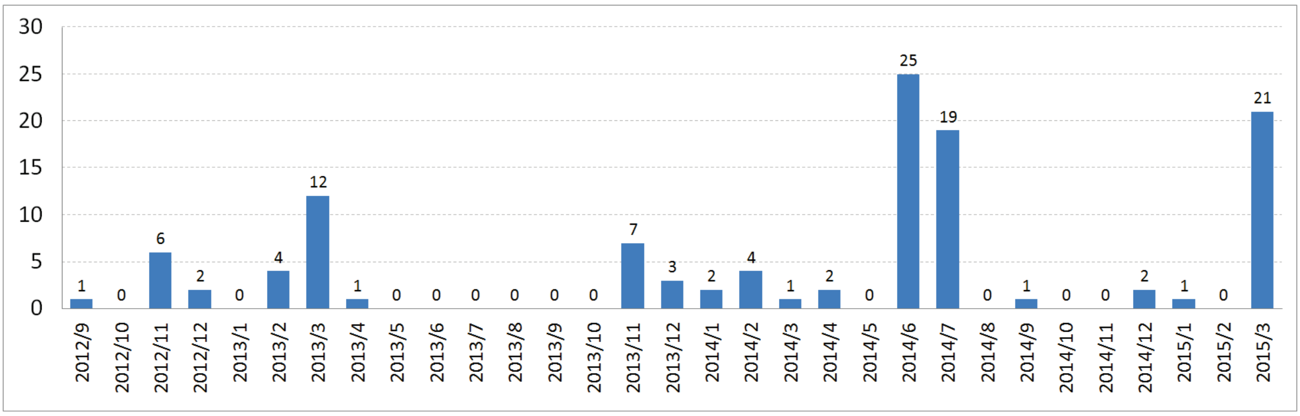



**図 25　攻撃メール件数：月統計**

更に、114 件の攻撃メールがそれぞれ日本時間の「何時に着信したか」という統計を取ると、興味深い結果となった（「図 26　攻撃メール件数：時統計」）。

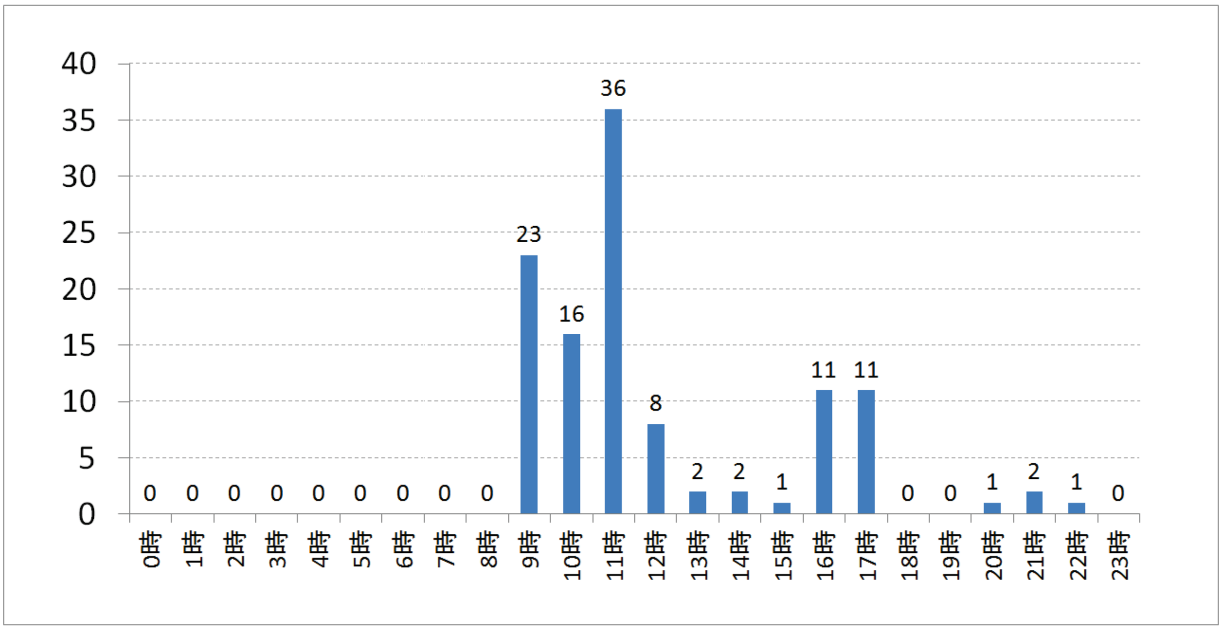



**図 26　攻撃メール件数：時統計**

J-CSIP で確認した限り、**夜の 23 時から朝の 8 時の間、1 件も攻撃が確認されていない**。また、18 時以降も稀なケースであり、朝の 9 時から夕方 17 時の間に、96%のメールが集中している。

このような結果となったのは偶然とは考えにくく、**日本の組織の一般的なオフィスアワーに合わせた標的型攻撃が行われている**ように見える [8]。特に午前中の件数が多く、攻撃者の狙いは、攻撃対象の人物が業務を忙しく処理している最中に攻撃メールを紛れ込ませて、開封の確率を高めることかもしれない。

## 4.2 ウイルスの種別と着信時期

攻撃者「X」が使用するウイルス、「X Type1」～「X Type4」の 4 種について、各種別が確認された期間と件数を「図 27 ウイルス各種別の確認件数」に示す。

| ウイルス種別 | 着信時期 | 検体数 | 2012年 | | | | 2013年 | | | | | | | | | | | | 2014年 | | | | | | | | | | | | 2015年 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 |
| X Type1 | 2012/9 ～ 2014/1 | 29 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| X Type2 | 2013/11 | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| X Type3 | 2013/11 ～ 2014/12 | 12 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| X Type4 | 2014/2 ～ 2015/3 | 71 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**図 27 ウイルス各種別の確認件数**

「X Type4」は、2014 年 6～7 月と 2015 年 3 月に多数確認されたため、全体の数が最も多くなっている。

「X Type1」～「X Type3」については、ある時期を境に確認しておらず、また、「X Type4」についても、2015 年 3 月以降、本書執筆時点（2015 年 5 月）では、着信を確認していない。とはいえ、これまで継続して攻撃が行われてきたことを考慮すると、再び攻撃が行われるのは時間の問題だと思われる。

[8] 攻撃者「X」が、攻撃を“仕事”として行っている結果と見ることもできるが、いずれにせよ推測の域をでない。

攻撃が確認されなかった空白期間なども含め、より詳しく、ウイルスの着信状況を「図 28 ウイルスの種別と着信時期」で時系列に沿って示す。こちらも、非常に興味深い結果となっている。

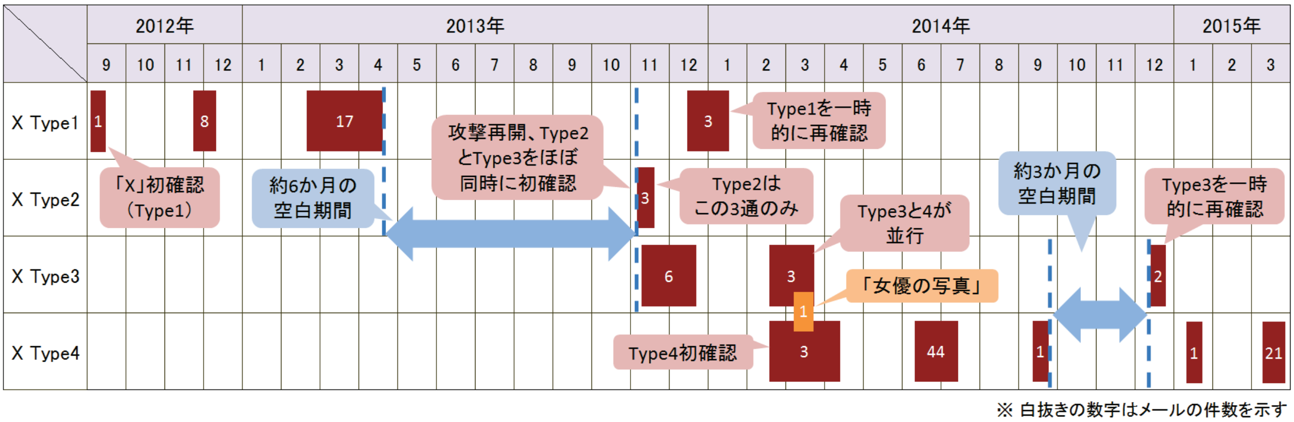



**図 28 ウイルスの種別と着信時期**

時系列とともにウイルスの種別で着信状況を追っていくと、次の点が見られる。

- 攻撃は、ある程度のまとまりで行われ、攻撃が確認されない空白期間が存在する(この期間は J-CSIP 外の組織へ攻撃が行われている可能性もある)。
- 2012 年 9 月から 2013 年 4 月まで**「X Type1」**が確認された後、約 6 ヵ月間の空白期間があった。攻撃の再開が確認されたのは 2013 年の 11 月だが、この時、ウイルスの作りが若干異なる**「X Type2」と「X Type3」が同時に現れた**。
  - 「X Type2」は、その後確認されていない。理由は不明だが、ウイルスとしては「X Type3」が残り、「X Type2」は「没」となった可能性が考えられる。
- 少しの空白期間ののち、2014 年 2 月、**「X Type4」を初めて確認**した。この時、「X Type3」も並行して確認されており、かつ、3.3 章で紹介した「女優の写真」も、この時期に行われた攻撃である。すなわち、この時期、攻撃者は「X Type3」とともに「X Type4」を並行して**試行運用していた**可能性がある。
- その後、2014 年後半からは、攻撃者は基本的に「X Type4」のみを使用している。

例外的に古い種別のウイルスが少数確認されることはあるものの、大きな流れとしては「X Type1」 → 「X Type2 / 3」 → 「X Type4」と、攻撃者「X」は**ウイルスを作り変え**、また、**攻撃を行いながら使用するウイルスの切り替えをしている**様子が伺える。今後の攻撃でもウイルスが変化していく可能性があり、攻撃者「X」の動向には引き続き注意が必要である。

# 5　攻撃者「X」の攻撃メールの手口

ここまで、攻撃者「X」が、様々な騙しの手口、多数のメールアドレスや C&C サーバ、4 種のウイルスを駆使して一連の攻撃を行っている攻撃者（または攻撃グループ）であると推定する背景を述べた。本章では、2 章や 3.3 章で紹介した事例に加え、特徴的な攻撃メールの事例を紹介しながら、この攻撃者「X」の手口と注意すべき点について述べる。

## 5.1 「連絡帳・アドレス帳」を装う手口

2.3 章で 2014 年 7 月の「連絡帳」の事例を 1 件紹介した。連絡帳やアドレス帳を送るという騙しの手口の攻撃メールは、全体で最も多く確認しており（114 通中 39 通）、具体的には図 29 に挙げるような様々なバリエーションがある。

| | |
|---|---|
| 件名 | アドレス帳のアップデート |
| 着信 | 2013/11 |
| 本文 | 同僚は、添付ファイルを送った最新の記録された通信は、アップデートしてください。 |
| 添付 | アドレス帳.rar　（解凍後：実行ファイル） |

| | |
|---|---|
| 件名 | アドレス帳 |
| 着信 | 2013/11 |
| 本文 | 最新のアドレス帳、アップデートしてください |
| 添付 | アドレス帳.rar　（解凍後：実行ファイル） |

| | |
|---|---|
| 件名 | 連絡帳 |
| 着信 | 2014/6 |
| 本文 | ご担当者様<br><br>新しいコンタクトを添付して、ダウンロードしてください。 |
| 添付 | 連絡帳.zip　（解凍後：実行ファイル） |

| | |
|---|---|
| 件名 | 連絡帳 |
| 着信 | 2015/3 |
| 本文 | ご担当者様<br><br>以下は更新後のアドレス帳、お手数おかけいたしますが、ご連絡をお待ちいたしております。 |
| 添付 | address.zip　（解凍後：Excel 文書ファイル） |

**図 29 「連絡帳・アドレス帳」のバリエーション**

本文の日本語には不自然な点が見られ、これらの個々のメールは比較的不審であると見破りやすいと思われる。

ここで注意すべきなのは、これらの事例群が示すとおり、攻撃者「X」は、メールの件名・本文・添付ファイルを**少しづつ変えながら長期間に渡って攻撃を繰り返している**点である。また、ウイルスに感染させる方法として、「アイコンを偽装した実行ファイル」を開かせようとする手口が多く確認されてきたが、最近の 2015 年 3 月の「連絡帳」の事例（図の右下）では、**Excel 文書ファイルのマクロ機能を悪用する手口を新たに取り入れている**（この手口について、詳しく次ページで述べる）。

攻撃者「X」は、使用するウイルスの作り変えだけでなく、**攻撃メールの騙しの手口やウイルス感染手口を見直し、変化・巧妙化させてくる**ということが分かる。

## マクロ機能を悪用するウイルス

悪意のあるマクロが仕掛けられた Office 文書ファイルを開くと、Word や Excel のデフォルトの設定では、マクロが無効化された旨のメッセージと、これを**有効にするためのボタン**が表示される(「図 30 セキュリティの警告表示」)。ここで、「コンテンツの有効化」ボタンをクリックし、マクロを有効にする(＝悪意のあるプログラムを動作させることを許可する)と、**ウイルスに感染させられてしまう。**

このような警告メッセージは、ウイルスが仕掛けられたファイルに限らず表示されることがあり、**マクロを有効にすることの危険性を意識せず**に、「コンテンツの有効化」ボタンをクリックしてしまう習慣のある利用者が相当数存在する可能性がある。

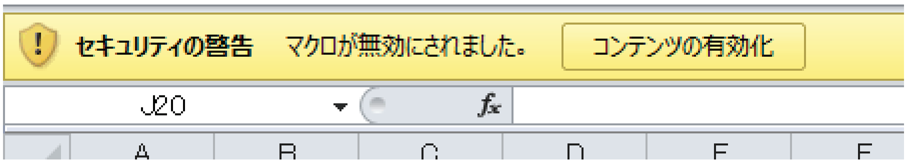



**図 30 セキュリティの警告表示**

Microsoft 社は、2014 年 12 月頃からこの手口を使ったウイルス付きのスパムメールが大量にばら撒かれているとし、注意喚起を公開した[9]。J-CSIP 内においても、インターネットバンキングに関する情報を窃取する目的と思われるウイルスに感染させる、マクロ付きの Word 文書ファイルが添付されたウイルスメールを 2014 年 11 月から複数確認してきた。

そのような中で、標的型攻撃メールにマクロの手口を応用してきた事例は、J-CSIP としては、**この攻撃者「X」による攻撃が初**であり、2014 年 12 月、「忘年会について」および「訃報」という件名のメールで攻撃が行われたことを確認した(図 31)。2015 年 3 月以降は、「連絡帳」という件名のメールでもこの手口が使用されるようになった。


**図 31 「忘年会」と「訃報」のメールの添付ファイル**

これまで、標的型攻撃メールへの利用者における対策として、「アイコン偽装や拡張子偽装に注意し、実行ファイルを開かない」、「ショートカット(LNK)ファイルを開かない」といった注意点を挙げてきたが、今後は**「マクロを自動的に有効にするような設定は行わない」**、**「外部からの不審な文書ファイルではマクロを有効化しない」**という対策も徹底する必要がある。

[9] 「Before you enable those macros…」(Microsoft 社 Malware Protection Center)
http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx

## 5.2 「求職」を装う手口

「求職」を題材としたメールは、全体で二番目に多く確認しており(114 通中 26 通)、大学の学生を騙ったもの、メールの本文が英語のものなど、いくつかパターンがある。次の「図 32 SE の求職メール」は、2.2 章の求職の事例と非常に似ているが、**同じ時期**に**別の組織**に対して送信された攻撃メールである。

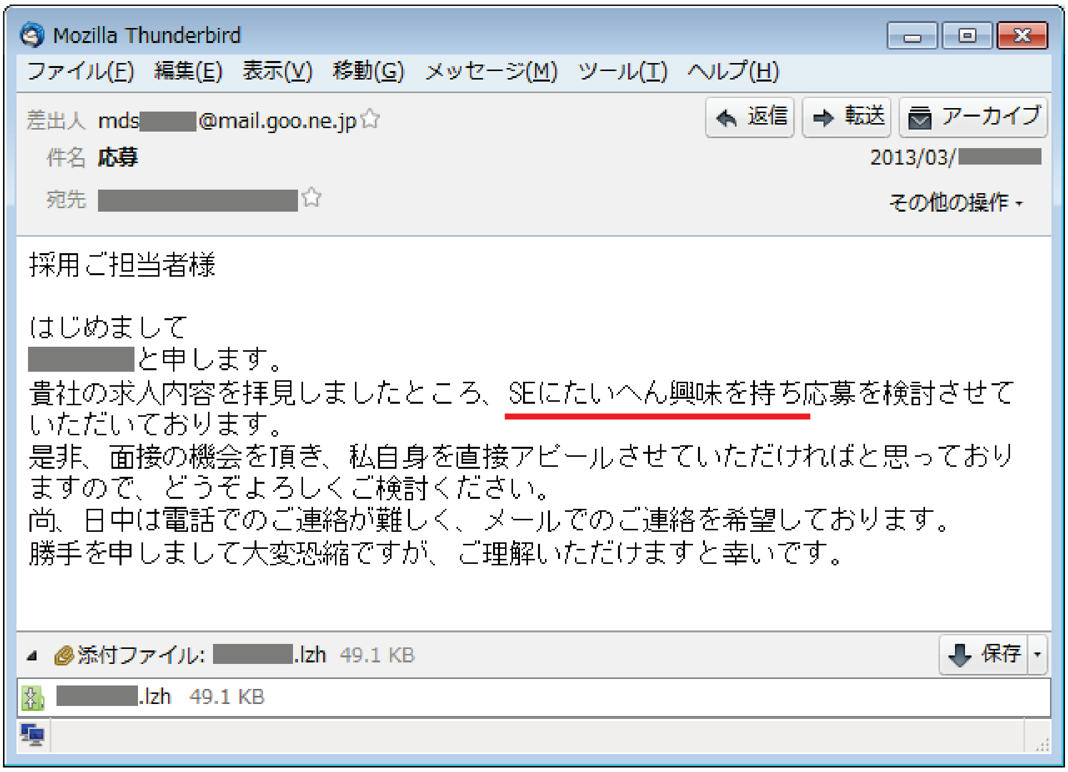



**図 32 SE の求職メール**

「図 33 2.2 章の求職メールの抜粋」に、2.2 章で紹介した事例の本文の抜粋を示す。


**図 33 2.2 章の求職メールの抜粋**

赤線で強調した部分が、この 2 つのメールの本文で唯一異なる部分である。片方は「SE」、もう片方は「営業職」となっているが、これは、それぞれのメールを受信した組織が**当時実際に募集を行っていた職種**であった。この文面のメールは、**合計 3 組織で、4 通の着信**が確認されている。

攻撃者「X」は、「連絡帳」のような汎用的な文面の攻撃メールを多数送りつける一方で、少数であるが、**標的とする組織の情報を調査し、より現実味のある騙しの文面を作る**ような攻撃も行ってくる。

### 5.3 「製品等へのクレーム」を装う手口

114 通中 11 通と、全体で三番目に多く確認している、様々な内容のクレームを装う手口を紹介する。図 34、図 35 のような、製品故障と称するメールが多い一方で、次ページの図 36 のように、**「貴社に送付した履歴書が公開されている」**といった内容で、窓口担当者が対応せざるをえないように仕向けようとした手口が確認されたこともある。

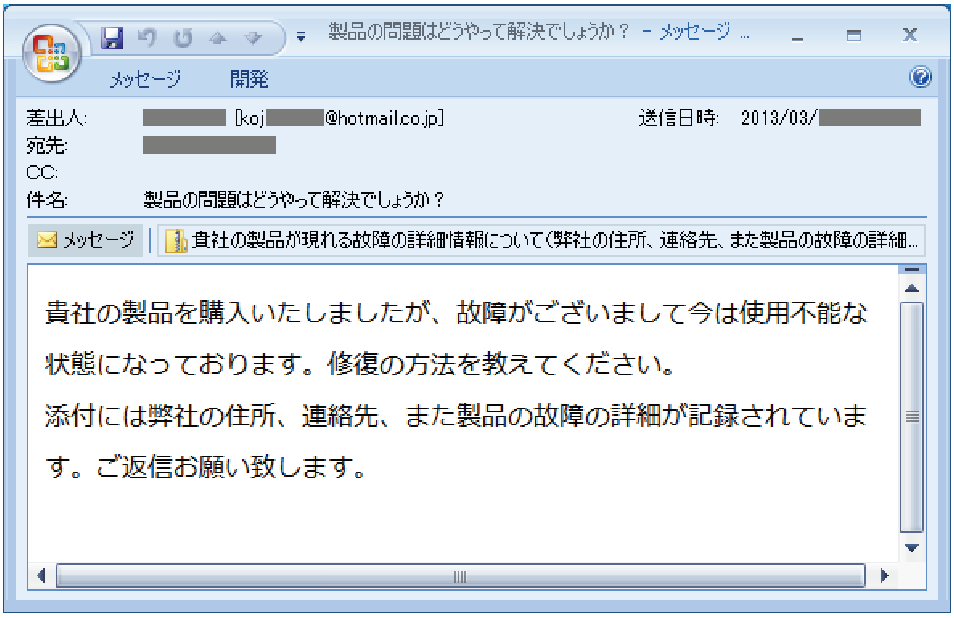



図 34 クレームを装う事例（2013 年 3 月）

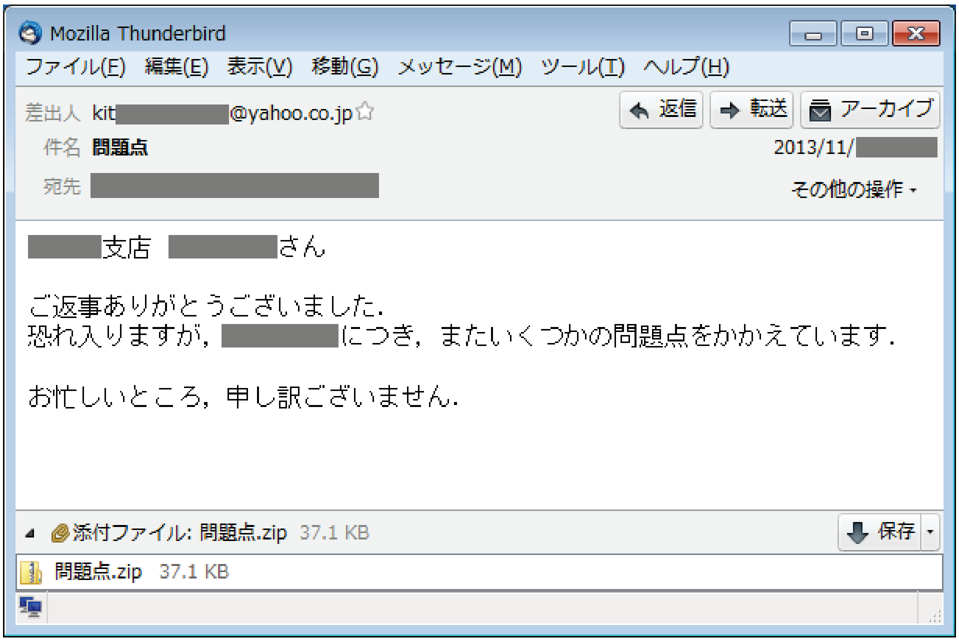



図 35 クレームを装う事例（2013 年 11 月）

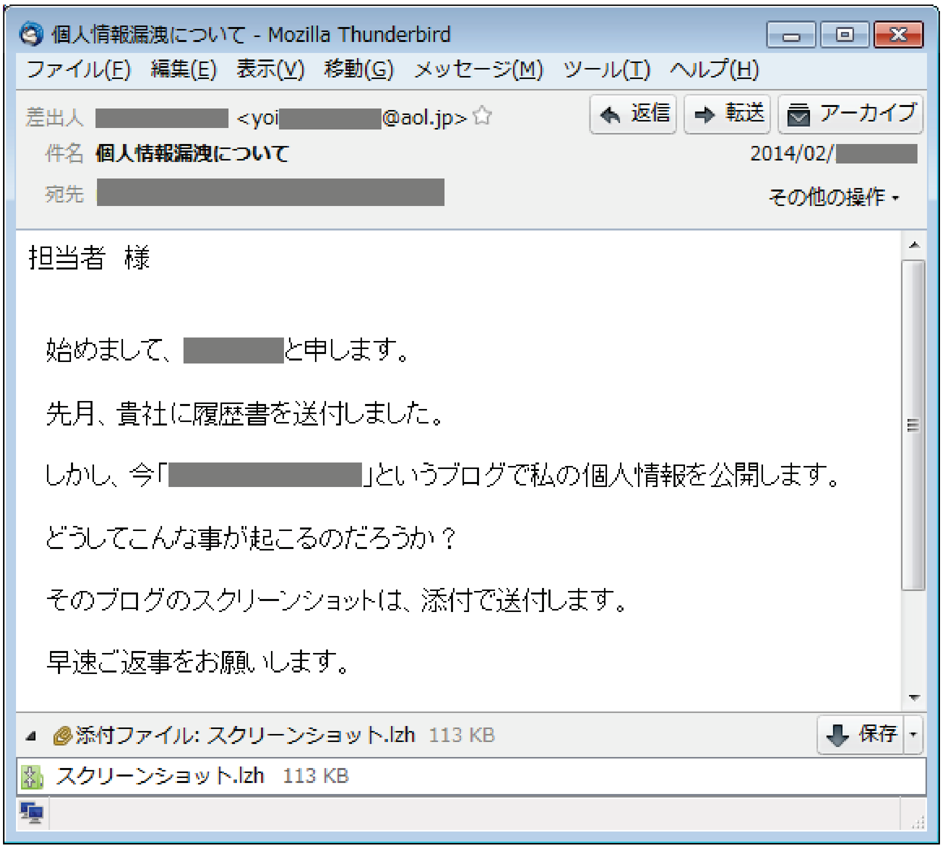



**図 36 クレームを装う事例（2014 年 2 月）**

この他、攻撃者「X」が組織の外部向け窓口を狙ったと思われる騙しの手口の題材としては、少数ながら、「注文」（3 通）や「問い合わせ」（2 通）を装うものがあった。

「求職」にも同じことが言えるが、外部向けの窓口担当者は、見知らぬ相手からのメールで、多少不審に感じたとしても、添付ファイルの内容を確認せざるをえない場合が多い。このため、不審なメールに気付いたらシステム管理部門へすぐに連絡するとともに、組織として、不審なファイルの内容を安全に確認できる環境を準備しておくことを勧める。

### 5.4 「やり取り」を伴う手口

攻撃者「X」から、「やり取り」を伴う手口による攻撃が行われた事例も数件確認している[10]。

この攻撃の事例では、「図 37 「やり取り」の経緯」に示す通り、最初に組織のウェブサイトから問い合わせ（ここでは「偵察」と呼ぶ）を行い、**組織からの返信メールを待ち、そのメールアドレスへ**ウイルスを送りつけてきた。

| 順序 | 種別 | 内容 |
|---|---|---|
| 1 | 偵察 | 攻撃者が、組織のウェブサイトの問い合わせフォームを使って問い合わせを送信。 |
| 2 | 返信 | 組織の窓口部門から、問い合わせの詳細をメール送信してほしい旨を返信。 |
| 3 | 攻撃 | 攻撃者が、「製品の故障の詳細情報」と称し、窓口へウイルス付きメールを送信。 |

**図 37 「やり取り」の経緯**

ウイルス付きメールは、具体的には次の図 38 のような内容であった。

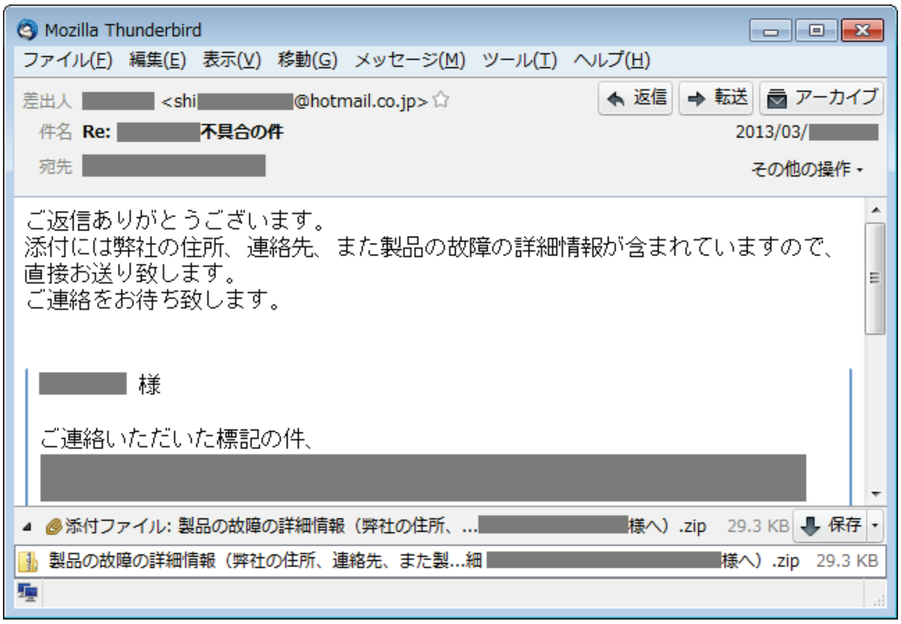



**図 38 やり取りの後で送られた攻撃メール（2013 年 3 月）**

このような形で攻撃が行われると、攻撃者にとって次のような利点（**攻撃を受ける組織側には不利な点**）が生じると考えられる。

- 一度「やり取り」のあった関係となるため、相手の警戒心を解きやすい。
- メールを授受する窓口のメールアドレスや担当者名・部署名を知ることができる。
- 担当者がある程度決まることで、メールの宛先がメーリングリストであっても、一部の担当者に攻撃対象を絞ることができる（他の担当者が攻撃メールに気付きにくくなる）。

攻撃者「X」の問題に限らず、組織の窓口担当者は、**「やり取り」を伴う標的型攻撃メールの手口がある**ということを、よく認識しておく必要がある。

---

[10] J-CSIP 2013 年度活動レポートで説明した「やり取り型」攻撃の攻撃者とは、メールやウイルスの特徴において共通点が見られないため、「X」と異なる攻撃者だと考えている。

### 5.5 「転送依頼」を装う手口

本件は 1 通を確認したのみであるが、他では見られない手口であったため、事例として紹介する。この攻撃メールは、図 39 のような「転送お願い致します」という内容であった。

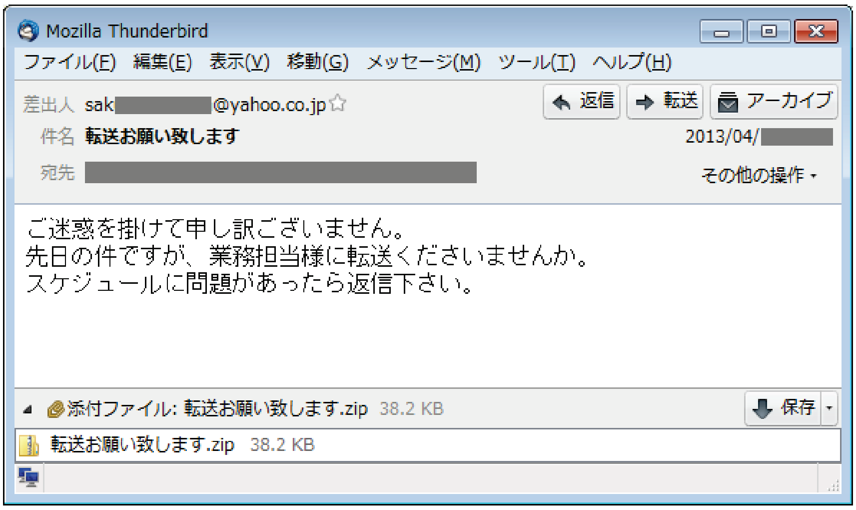



**図 39 転送依頼(2013 年 4 月)**

メールの受信者にとっては、もちろん、身に覚えのない唐突な依頼であるため、まず不審に感じるものと思われる。自身が名乗っていないだけでなく、「転送お願い致します」と言いながら、誰に転送してほしいのかも書かれていない。

一方で、メールの文面の言葉遣いには、これといって不自然な点がない。素直に内容を受け取り、「スケジュールに問題があったら返信下さい」と書かれているのだから、誰かが確認して早々に返信する必要があるのでは、と考えてしまった場合、危険である。すなわち、**誰にメールを転送すればよいのかを確認しようとして**、添付ファイルを開いてしまう可能性がある。

添付ファイルを解凍すると、図 40 のファイルが得られる(上:アイコン表示、下:ファイル名全体表示)。

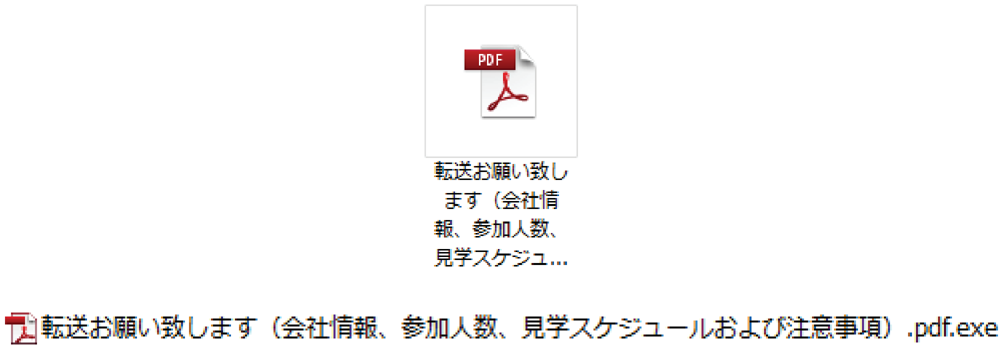



**図 40 転送依頼の添付ファイル(解凍後)**

これは**アイコンをPDF文書ファイルに偽装した実行ファイル**(拡張子「.exe」)であるが、拡張子を画面に表示する設定としていても、**ファイル名が長いため図のように「....」と省略されてしまう**。拡張子を隠す手口として、ファイル名に大量の空白を入れる手法がよく挙げられるが、この手口では、より自然に、拡張子を隠すことができているように見える。

このメールは、平日の夕方 17 時過ぎ、判断力が鈍る可能性の高い時間帯に着信した。件名、本文、添付ファイル名、解凍後の添付ファイル名、アイコン偽装…と、細工が随所に施された「騙しの手口」である。

## 6　総括

### 6.1 「X」の攻撃者像

本書では、J-CSIP で確認した攻撃情報を積み上げ、その関連性を横断的に分析し、攻撃者が残した痕跡の繋がりから、攻撃者「X」の存在と一連の攻撃活動を浮かび上がらせることを試みた。また、ウイルスの時系列での推移や、具体的な騙しの手口を紹介しながら、**この攻撃者「X」が、執拗に、様々な手口で国内組織を継続的に攻撃している様**を明らかにした。

実際には、別々の攻撃者による攻撃が 1 つに見えている可能性や、「X」の中に複数の攻撃グループが存在する可能性はあるが、少なくとも、**国内組織を執拗に狙う者の存在は明白である**。

改めて、攻撃者「X」の特徴(攻撃者像)を図 41 にまとめる。

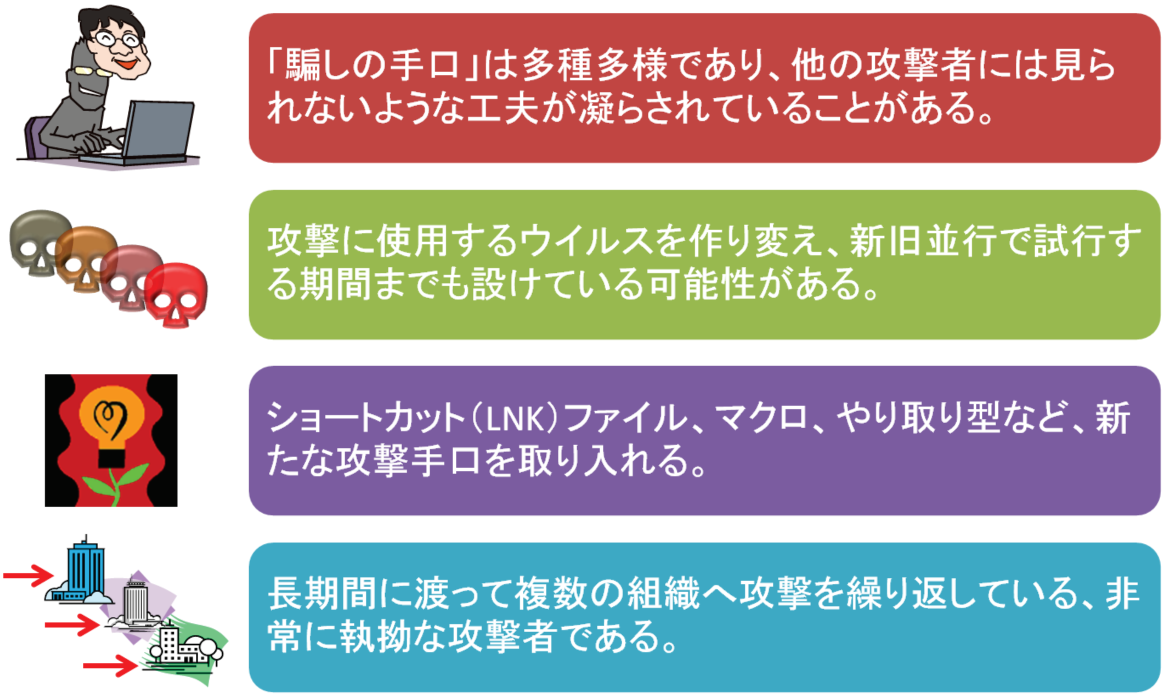



**図 41　攻撃者「X」の特徴**

サイバー攻撃に関する情報を整理する際、本書で示したような内容は、**「TTPs」**[11]の一部と位置付けることができる。**「TTPs」**とは、Tactics, Techniques and Procedures の略で、直訳すると、攻撃者の「戦術、技巧、手順(やり方)」であり、単純に「攻撃手口」とも呼んでいる。

J-CSIP では、3 年の運用を経た現在も、最も多い情報共有の対象は「標的型攻撃メール」であるが、本書の内容のような、個別の攻撃情報を積み重ねることによって見えてくる、**攻撃者の行動や攻撃手口(TTPs)**といった**「知見」のレベルの情報**についても、情報共有の対象とすべく活動を続けている。

---

[11] 米国の MITRE 社が中心に策定を行っている「脅威情報構造化記述形式(STIX)」では、このような情報を表記し、共有するための仕様を定めている。　参考:「脅威情報構造化記述形式 STIX 概説」(IPA)
https://www.ipa.go.jp/security/vuln/STIX.html

### 6.2 国内組織を狙う脅威と対策

本書で攻撃者「X」によるものとした標的型サイバー攻撃は J-CSIP の中でも全体の一部であり、国内の多数の組織が、様々な攻撃者からの標的となっているであろう状況の、氷山の一角だと思われる。

また、そもそも、**攻撃対象となっていることに気付いていない**（攻撃を検知できていない）組織も数多く存在すると考える。自組織に対して標的型サイバー攻撃が行われているのか否かを認識できなければ、対策の必要性の判断ができず、また、対策の講じようもない。不審なメールや通信の痕跡に気付いた時は、組織のシステム管理部門などに情報を集約し、それがどのような脅威であるのか、分析を行う体制を整える必要性が高まっている。そして、その情報を**組織内で共有**し、更には**他組織とも情報共有**ができれば、より望ましい。

攻撃者は、継続的に攻撃を行ってくるだけでなく、次々と新たな手口やウイルスを使用してくる。長期的な観点で、このような脅威に対抗するには、防御側も CSIRT[12]のような**組織的な対応体制**を準備し、かつ、変化に柔軟に対応できるよう、**その体制を維持**していかなければならない。

組織の個々の利用者（職員）の観点では、**自分が標的となり、組織内ネットワークへの侵入路として狙われる可能性がある**ことを、改めて認識していただきたい。本書で紹介したような「騙しの手口」のメールは、誰に、いつ届くか分からない。

メールのウイルス検知システム、侵入検知システム、パソコンのセキュリティソフトなど、サイバー攻撃に対抗するために多層の防御を施している組織であっても、油断はできない。標的型サイバー攻撃を行う攻撃者は、そういった**防御策が存在する前提**で、それらをすり抜けるよう工夫を凝らしてくる。

利用者は、自分も、このようなサイバー攻撃から組織内ネットワークや秘密情報を守る**重要な防御壁の 1 つである**と意識し、不審なメールや添付ファイルを開かないよう注意するとともに、不審なことに気付いた際は、システム管理部門へ連絡し、（個人ではなく）組織的な対応に繋げることが重要である。もちろん、IPA でも、相談を受け付けているため、相談や情報提供をお願いしたい。

また、本件 114 通の攻撃メールは、**「ソフトウェアを最新に保つ」**、**「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（実行しない）」**、**「マクロを有効にしない」**という対策を実施できれば、全て回避できるものであった。**基本的な対策が重要かつ効果的**であり、周知徹底していただければと思う。

なお、**標的型攻撃メールの訓練**（「予防接種」とも呼ばれる）も、有効な取り組みであろう。標的型攻撃メールの訓練とは、本物のウイルスは用いず、標的型攻撃メールを模したメールを職員へ送信し、開封率を確認したり、それを取りかかりに啓発・注意喚起を行う活動である。

標的型攻撃メールの訓練を行う際に重要なのは、**「開封率を下げる」ことだけを目的としていては不十分**という点である。もちろん、不審なメールを見破る目を鍛えることには意義があるが、標的型攻撃メールを受信した職員が**どのような行動を取ったか**（すなわち、組織内ルール通りの対応をしたか、そうでなかった場合、それはなぜか）、組織内の**連絡・対応フローが想定通りに機能したか**、といった点も含めた「組織全体の訓練」として、実施結果を組織内ルールや体制整備へフィードバックしていただきたい。

---

[12] Computer Security Incident Response Team の略。
参考：「What's CSIRT?」（日本コンピュータセキュリティインシデント対応チーム協議会）
http://www.nca.gr.jp/imgs/CSIRT.pdf
参考：「CSIRT マテリアル」（JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/csirt_material/

## 6.3 「内部対策」の必要性

本書で示したような標的型攻撃メールをはじめとする標的型サイバー攻撃が、執拗に、巧妙化を続けながら行われる状況下では、多層防御を施し、啓発・教育を行い、標的型攻撃メールの訓練を繰り返したとしても、**ウイルス感染をゼロにすることは不可能**だと思われる（低減することは可能で、もちろん、非常に重要である）。このため、ウイルス感染などのインシデント発生を前提としながらも、被害を最小化する（侵入後の攻撃行動を困難にする）ことに主眼を置いたシステム設計や運用体制が必要となってくる。


IPA が公開している「システム設計ガイド」[13]では、このような前提のもと、**「侵害拡大防止」**および**「監視強化」**を目的としたシステム設計について説明しており、その要点を次に示す。

- 攻撃者が心理的に“内部探索しづらい”システム設計策を施す。
- 攻撃者の内部探索活動を発見するための「トラップ（罠）」を設置する。
- システム管理者が“侵害拡大”行動（内部活動の存在）に早期に気付くようにする。

本書の範囲を超えるため、詳細については当該ガイドや、各種セキュリティベンダが提供している内部対策や情報漏えい対策の製品・サービスを参照していただきたい。

なお、「内部対策」にも関連するが、標的型サイバー攻撃などによるセキュリティインシデントが発生した際、何が起こったのか、どう対応すればよいのか、同じような事象が他でも発生していないか、また、行った対処が十分なのかといったことを判断するためには、組織内システムの様々な場所（ネットワーク機器、サーバ、パソコンなど）で記録している**ログが非常に重要**である。

現在記録しているログの対象・内容・期間が十分か、タイムスタンプが正確か、ログを遡って実際に調査分析を行う環境が整っているかといった観点で、改めて確認していただければと思う。

[13] 「『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

## 6.4 おわりに

J-CSIP における 3 年間の情報共有活動の中、2 年半以上に渡って確認されてきた攻撃者「X」について、いくつかの面から分析を行った。サイバー攻撃を行う攻撃者の具体的な脅威、個々の組織での対策の重要性のみならず、組織間での情報共有活動の有効性についても示せたものと考える。

攻撃者「X」に限らず、サイバー攻撃は今後も止まることはない。J-CSIP の情報共有活動は 4 年目に入り、IPA は、その運用を着実に継続するとともに、参加組織の拡大や、活動の質的向上を進めていく所存である。また、IPA では一般の組織向けの相談窓口として「標的型サイバー攻撃の特別相談窓口」[14]も設けているため、不審なメールなどに気付いた際は、ぜひご相談いただきたい。

最後に、本書の内容は、J-CSIP の参加組織の多大なる尽力のもと、IPA が情報提供を受け、分析が可能となったものである。参加組織の方々へ厚くお礼を申し上げるとともに、本書の内容が、国内のサイバーセキュリティの意識向上、対策、情報共有活動の活性化に繋がれば幸いである。

## 添付資料について

本書で取り上げた 114 通の全メールの一覧を、**『添付資料「X」による攻撃メール一覧』**にまとめた。この資料では、メールの着信時期、騙しの手口、着信組織と件数の分布、添付ファイル（ウイルス）のファイル形式と感染手口（下表を参照）、そしてウイルスの種別（Type1～4）を示している。

本書では説明しきれなかった事例や、攻撃手口の変遷を詳しく確認することができるため、必要に応じて参照いただきたい。

添付資料内「ファイル形式と感染手口」欄の意味

| 表記 | 意味 |
|---|---|
| ZIP / LZH / RAR | 添付ファイルが ZIP、LZH、RAR 形式で圧縮されていたことを示す。 |
| DOC / XLS | 添付ファイルが Word 文書ファイル、Excel 文書ファイルであったことを示す。 |
| EXE / LNK | 添付ファイルが実行ファイル、ショートカットファイルであったことを示す。 |
| CVE-xxxx-xxxx | Word/Excel 文書ファイルが開かれた際、悪用が試みられる脆弱性の識別子を示す。 |
| EXCEL マクロ | Excel 文書ファイルを開いた際、マクロ機能によるウイルス感染が試みられることを示す。 |

以上

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