特定業界を執拗に狙う攻撃キャンペーンの分析

～2015 年秋から 2016 年春に見られた攻撃事例～

サイバーレスキュー隊（J-CRAT（ジェイ・クラート））分析レポート 2015

独立行政法人情報処理推進機構
セキュリティセンター

目次

1. はじめに

IPA の発行する『サイバーレスキュー隊（J-CRAT[1]）の分析レポート』は、標的型サイバー攻撃に対する対策支援を元に、短中期的な視点から着目すべき事象を分析し、広く提供するものである。

2015 年上半期は年金機構を始めとする十件以上のインシデントが、報道により明らかになった。その後 2015 年 9 月初頭まで毎月コンスタントに標的型攻撃が確認されていた。しかし、10 月以降 J-CRAT では目立った攻撃は確認されなかった。このため、同年 9 月 25 日（金）に行われた、中国の習近平国家主席と米国のオバマ大統領の米ホワイトハウスでの首脳会談[2]の効果かとも考えられた。

しかし 2015 年 11 月に 1 通の標的型攻撃メールが確認された後、12 月から 2016 年 3 月にかけて、執拗な攻撃が見られ始めた。

このため、J-CRAT ではメールの受信組織や不正利用されたメールのアカウント利用者から、積極的にメールやログの情報提供依頼を行い、137 通のメール情報を入手した。これらの一連の攻撃では、以下の特徴が見られた。

１．同一の業界や組織に対し、執拗に攻撃を行っている
２．企業のアカウントを乗っ取り、踏み台にして送る
３．本文の特徴が似ている（「ご高覧」の文言の頻繁な利用）
４．メールの送信に使われた IP アドレスは 2 パターンである
５．全メールに、パスワード付きの ZIP で圧縮されたウイルスが添付されている
６．全メールに、添付されたウイルスの挙動[3]が同一である

攻撃対象は特定業界 A を中心に、それに関連する業界を狙ったものも見られた。本レポートではこの攻撃の集合体をキャンペーンと呼び、このキャンペーンに使われた攻撃メール情報 137 通と、ウイルス、各種ログ情報を整理し、攻撃手口や実態を明らかにする。

IPA に相談をお寄せ頂き、情報を提供してくださった組織、IPA からの依頼により情報を提供していただいた組織に感謝いたします。また、本レポート作成にあたっては攻撃者の分析と今後の対応に備えることを主眼にしており、個別組織名等は全て伏せています。

[1] Cyber Rescue and Advice Team against targeted attack of Japan
[2] 共同記者会見にて「両国政府は，サイバー空間で知的財産を窃取したり，故意にこれを支援したりしないことで合意した」などの発言があった。
http://www.moj.go.jp/psia/201509naigai.html
[3] ウイルスは、一定期間無料で利用できる環境へ接続し、次に感染させるウイルスの情報をダウンロードする挙動が見られた。

2. 標的型攻撃メールの分析とレスキュー活動

2.1. 最初の情報提供と分析の開始

サイバーレスキュー隊へ 2 通の標的型攻撃メールに関する情報提供が行われた。メールの概要は以下の通りである。

表 2.1-1 提供情報（1 通目）　　< >：個別名称置換

着信日時	2015 年 12 月 15 日（火）　17：XX （日本時間）
実際の送信者	<フリーメール で取得したアカウント>
送信者の詐称	<受信組織に実在する個人名>
件名	<制度（応募要項等）>について
本文の概要	件名に関する簡易の説明が書かれており、詳細は添付を見るように促されている。
添付ファイル形式	パスワード付き zip （解凍後は、実行ファイル×2、PDF ファイル×1）

表 2.1-2 提供情報（2 通目）

着信日時	2015 年 12 月 16 日（水）　17：YY （日本時間）
実際の送付者	<実在する企業>
差出人の詐称	<実際の送付者と同一>
件名	参加申し込み
本文の概要	件名に関して、作業が完了した旨を伝え、詳細は添付を見るよう促されている。
添付ファイル形式	パスワード付き zip （解凍後は、実行ファイル×2、PDF ファイル×1）

提供された 2 通の攻撃メールは、差出人やメールのテーマが異なり、一見大きな関連性が無いように見えた。しかし、メールヘッダに記録されているメールの配送経路や送信環境、添付ファイルを調査したところ、以下の共通点が確認できた。

- メールの送信元 IP アドレス
- 添付ファイルの中身
- ウイルスの特徴

なお、2 通目のメール送付者は実在する企業のアカウントが不正利用されているものであったため、攻撃の連鎖を追った。

2.2. 標的型攻撃メールの分析と連鎖の追跡

本節では、本キャンペーンに関して行った、J-CRAT の調査・活動例を説明する。

2.2.1. 類似の攻撃メールのあぶり出し

攻撃者はターゲット組織に所属する複数の人物に対し、攻撃メールを送るケースがよく見られる。そのため、たとえ一人の受信者が標的型攻撃メールの不審点に気がつき、ウイルスに感染しなかったとしても、別の受信者が開いてしまい、密かに感染が広がっているケースがある。このため、差出人アドレス、件名、本文キーワード、添付ファイル名をキーにして、同様の類似メールが無いかを確認し（下図③）、並行して、ウイルスの通信先でネットワーク機器をフィルタリング・検知することで類似のウイルスへの感染を把握・予防する必要がある。

今回、情報提供者に調査依頼をし、複数の類似メールを検出、J-CRAT に提供いただいた（下図④、⑤）[4]。

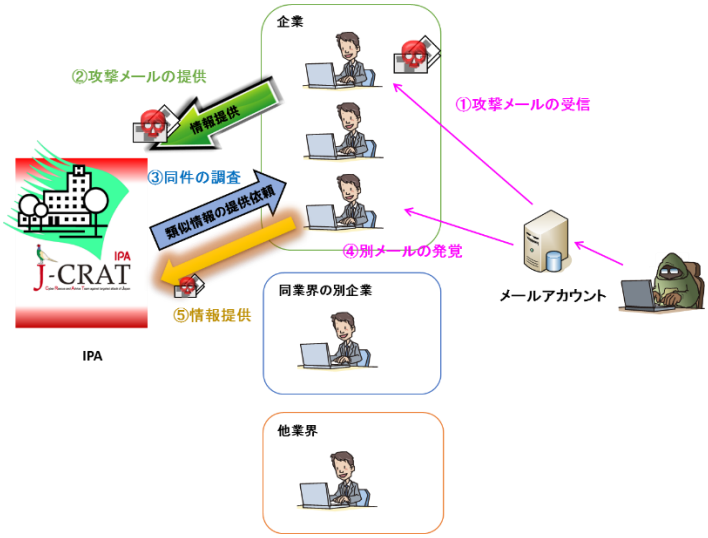


図 2.2-1 フィードバック情報の活用

[4] 自組織のメールを検索できる機能を持つことが重要である。

2.2.2. 標的型攻撃メールの連鎖を追跡

標的型攻撃メールの詐称方法には、フリーメールアドレスを取得し、組織名などを詐称するケースと、アカウントを乗っ取るケースなどがある。今回のケースでは、プロバイダや企業のメールサーバを乗っ取ったものが 9 割以上であったが、フリーメールで似たようなアドレスを取得し攻撃が行われたものも確認された（3.3.1 節参照）。

標的型攻撃メールの踏み台となっていたメールアカウントを突き止め、その組織の協力を得て調査を行ったところ、標的型攻撃メールが実際に送付された組織を把握することができた（①）。これにより、送付された組織に対して、標的型攻撃メールの分析情報を通知することができ、着弾、開封状況のヒアリング、既に添付ファイルを開いてしまっていた場合の検知方法と遮断方法を伝え、インシデント初動処置を支援した（下図②、③）。

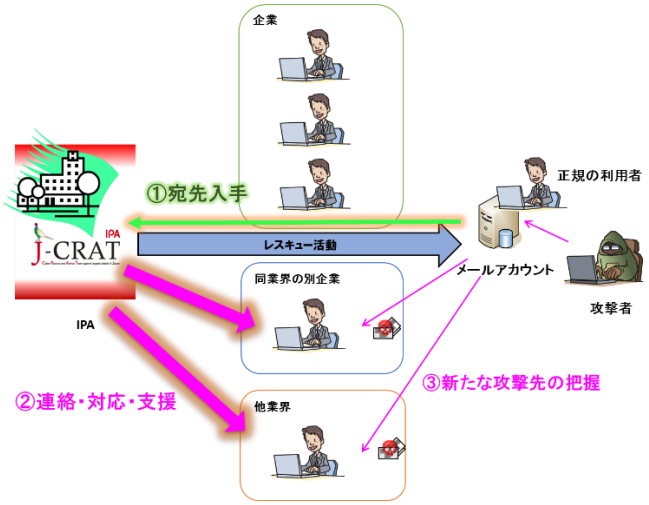


図 2.2-2 踏み台組織の調査

2.2.3. 被攻撃組織の攻撃履歴を分析

標的とされた組織の攻撃履歴や、新たに送られてくる攻撃を分析した。攻撃者は踏み台のメールアカウントやメール文面、ウイルスを変えて攻撃を継続してきた（①）。

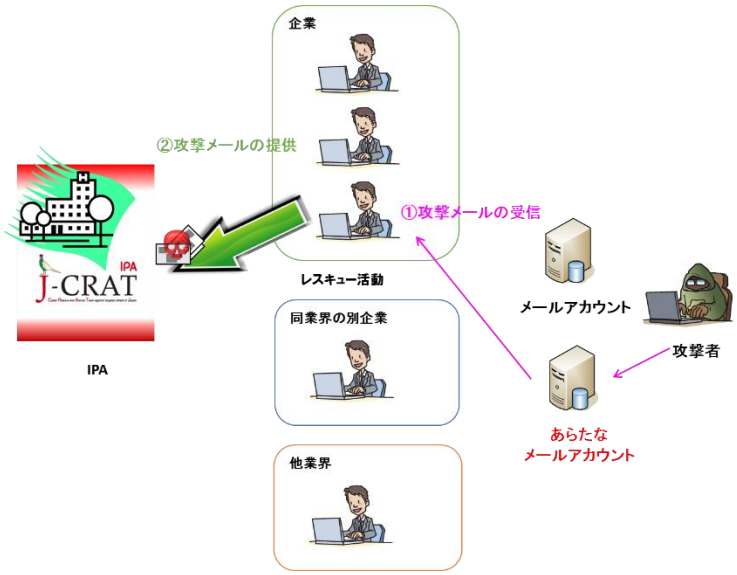


図 2.2-3 同一組織への長期的な攻撃の把握

このように、同様の攻撃メールの着信組織や、感染している組織が無いか、また、踏み台となったアカウントの調査を行うことで、44 組織から合計 137 通の関連すると思われるメールを入手した。

次章ではその分析の詳細結果について説明する。

3. 標的型攻撃メールに基づく分析

J-CRAT では、最初に報告のあった 2015 年 12 月から 2016 年 3 月までに情報提供を受けたものを調査した。この結果、実際の攻撃は 2015 年 11 月から 5 ヶ月間にわたり、44 組織宛に、137 通の標的型攻撃メールが送られていたことが判明した。これらを分析すると、同一の攻撃者の関与、特定の攻撃手法、インフラの使用というキャンペーンの特徴が明らかになった。

3.1. 本キャンペーンにおける標的型攻撃メールの時系列推移

137 通のメールの送信日について月ごとの通数、日ごとの通数を「図 3.1-1 攻撃メール通数：月別統計」「図 3.1-2 攻撃メール通数：日別統計」に示す。5 ヶ月におよぶ攻撃であったが、攻撃のピークは 12 月の後半から 1 月までの 1 ヶ月半である。

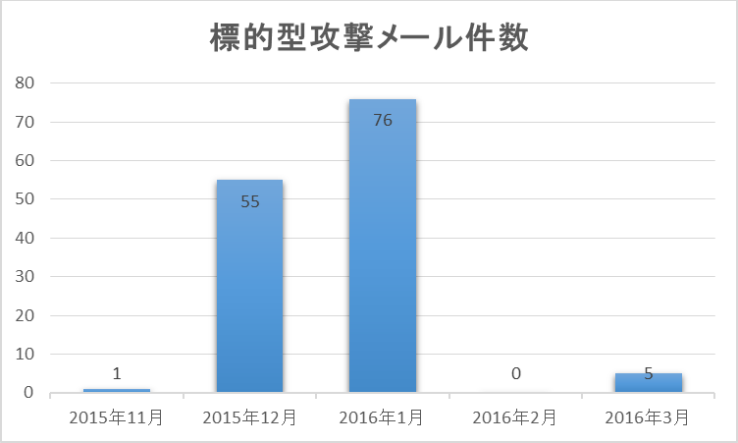


図 3.1-1 攻撃メール通数：月別統計

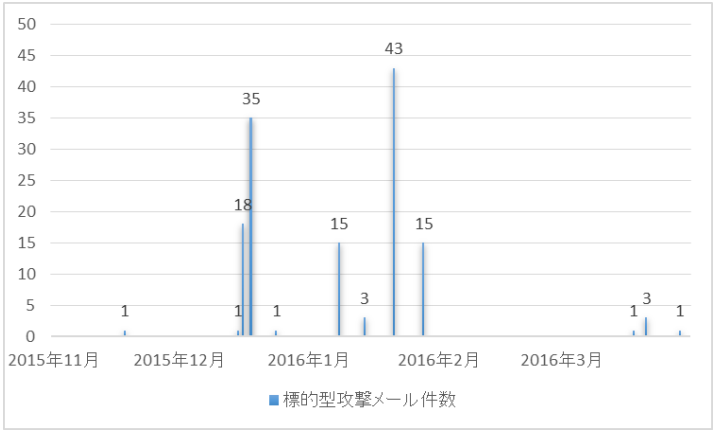


図 3.1-2 攻撃メール通数：日別統計

3.2. 一連の攻撃（Op:Operation）の定義と分類および相関

J-CRAT ではこの 137 通の標的型攻撃メールに内在している攻撃者の挙動に関わる痕跡を分析するため、攻撃メール群の分類を行った。分類に当たっては、攻撃メールを以下の定義で分類し、同じ特徴で紐付けられるものをオペレーション（Operation）として整理した：

一連の攻撃（Operation、以下 Op.と略記）の定義

・標的型攻撃メールの差出人、件名、本文、添付ファイルのすべてが同一

・メールの送信間隔に 1 時間以上の開きが無い

この定義に依ると、本キャンペーンの 137 通の標的型攻撃メールは、16 のオペレーションに分類された。さらに、攻撃に用いられた、メール送信元 IP アドレス、ウイルスの不正通信先、攻撃メールの宛先組織に着目してオペレーション間の関連を分析した結果を「図 3.2-1 オペレーション毎の共通点と相関」に示す。

本オペレーションでは以下の関連があることが確認できた。

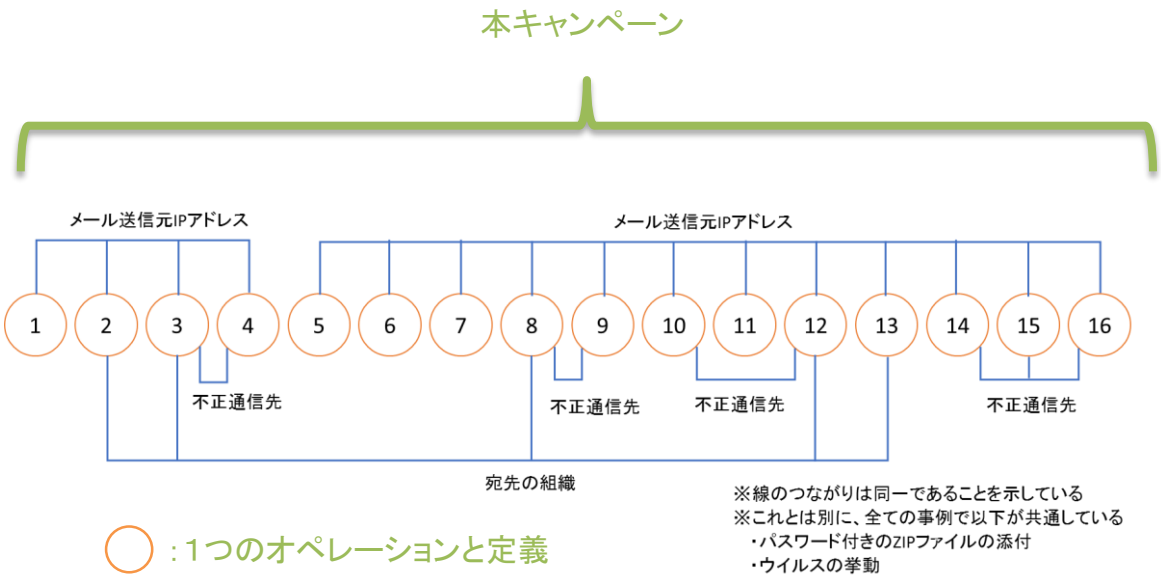


図 3.2-1 オペレーション毎の共通点と相関

このオペレーション間の関連による分析、およびキャンペーンを通した特徴は以下である。

① メールの送信元 IP アドレスは Op.1 から Op.4 までと、Op.5 から Op.16 までで同一のものとなり、同じ攻撃基盤を使い続けていることが分かる。
② 差出人のメールアドレスや、ウイルスの通信先などは、オペレーションごとに都度変えてきており、メール製品でのフィルタや、通信先のフィルタを回避する意図が読み取れる。
③ ウイルスの通信先は異なるものの、一定期間無料で利用可能な開発者向けの環境に、新たなウイルスを設置し、ダウンロードさせる仕組みとなっており、類似性が感じられる。
④ 添付ファイルは全てパスワード付きの ZIP ファイルで圧縮したものとなり、メール向けセキュリティ製品での検出回避を狙っているものと考えられる。
⑤ このほか、用いられたメールアカウント（3.3.1 項参照）や本文の特徴（3.3.3 項参照）、添付ファイルの特徴（3.3.4 項参照）に類似性がみられている。

3.3. 本キャンペーンにおける標的型攻撃メールの特徴

3.3.1. 用いられたメールアカウントの特徴

送信にフリーメールが使われることが依然多い標的型攻撃メールであるが、本キャンペーンでは企業の正規のメールアカウントを乗っ取り、不正に利用してメールを送るケースが大半であった。「図 3.3-1 メール送付手段の割合：フリーメール/アカウント乗っ取り」にメール送付方法の割合を示す。

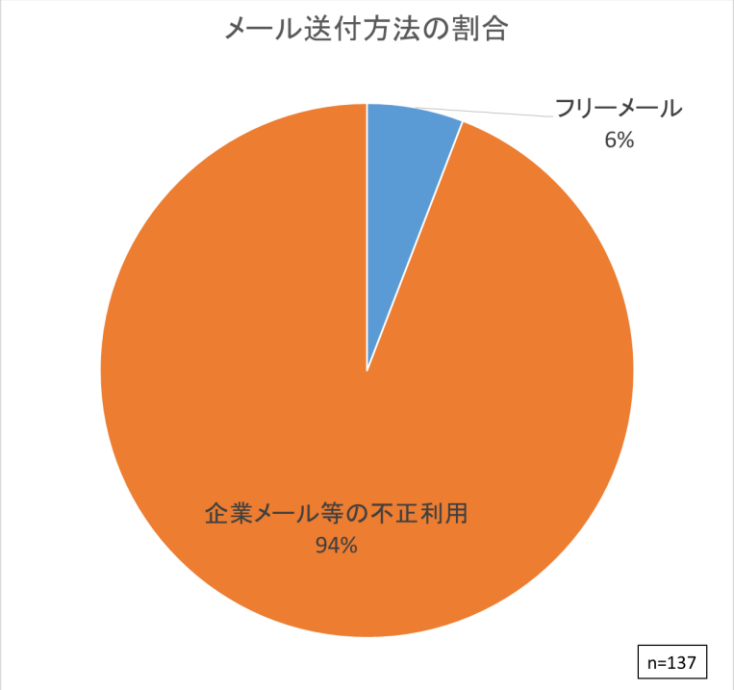


図 3.3-1 メール送付手段の割合：フリーメール/アカウント乗っ取り

本キャンペーンでは 94%のメールで企業等の正規のメールアカウントを不正に利用していることがわかった。では、攻撃者は、フリーメールと正規アカウントの不正利用によるメールをどのように使い分けていたのだろうか。着信状況を時系列でまとめたものを「図 3.3-2 メール送付手段の時系列：フリーメール/アカウント乗っ取り」に示す。

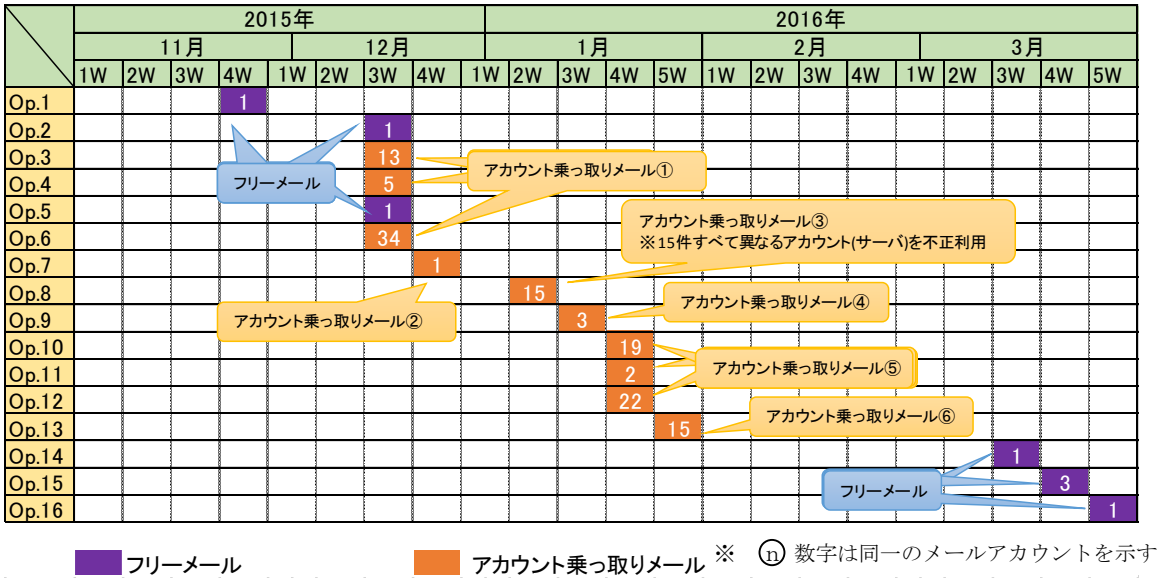
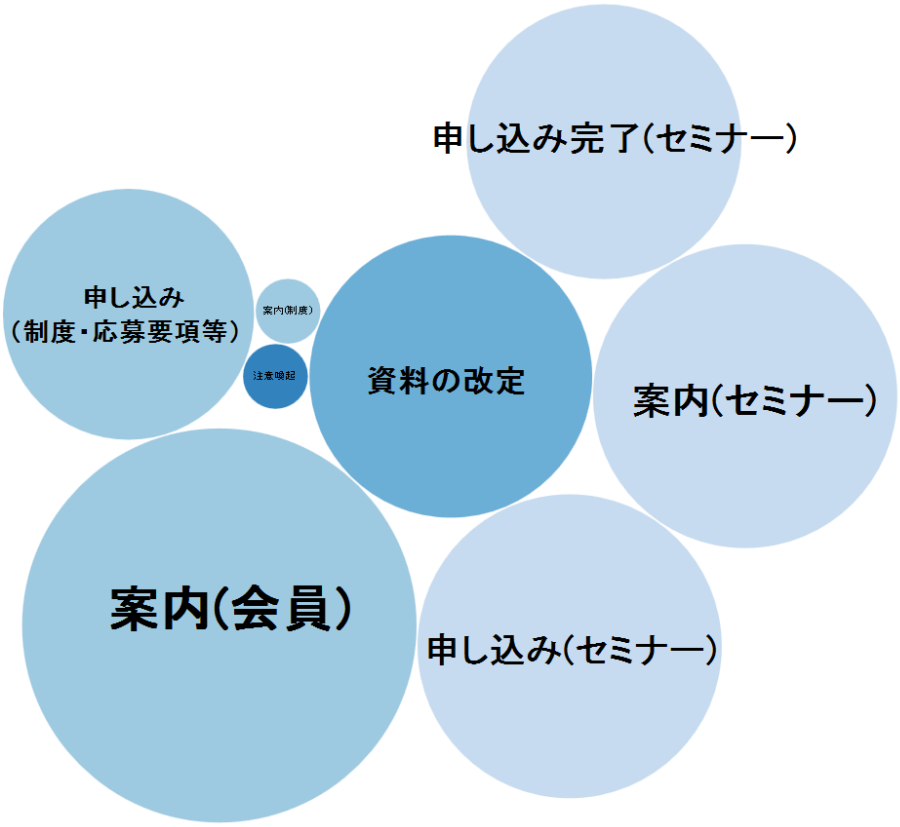


図 3.3-2 メール送付手段の時系列：フリーメール/アカウント乗っ取り

単発での攻撃ではフリーメールが使われることがあるものの、乗っ取ったアカウントが使用される場合では、一斉に送信するケースがほとんどであることが明らかとなった。これは用途によって使い分けているためだと思われる。例えば使用するメールアカウントのセキュリティ対策状況を鑑み、一度に複数の宛先に送る場合は、セキュリティ対策などでブロックされないメールアカウントを用いていることなども考えられる。

3.3.2. メールのテーマの特徴

次に、本キャンペーンで使用されたメールのテーマを分類したものを「**図 3.3-3 メールのテーマ**」に示す。



※円と文字の大きさは、入手したメール通数に従っている。

図 3.3-3 メールのテーマ

入手した情報を分類したところ、13 種のテーマに分かれており案内や申し込みを含め「**セミナー（説明会や交流会含む）**」を題材としたものが最も多く、45%となった。次に、「**会員**」を題材にしたものが 27%、「**資料改定**」を題材にしたものが 13%、当事者に関連する「**制度（募集要項等）**」を題材にしたものが 11%と続いた。これらセミナーや会員というテーマは受信者の業種・業界やビジネスに特化（直結）したものであり、受信者がうっかり開封してしまうだけの信憑性を帯びていたと考えられる。他には「注意喚起」が 1%であったが確認された。なお、送付が確認されたものの、メール本文の復元ができず正確に確認できていないものが 2%（2 件）存在した。

13 種類のテーマを見てみると、業務連絡や、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は少なかった。しかし、業種・業界に特化したセミナーや会員、制度等、当

事者であれば響く内容であった。標的とする業界・業種に合わせているからこそ、テーマが絞り込まれ**バリエーションは比較的少ない**。

また、標的型攻撃メールの詐称元、または送付先のいずれかが業界団体である事から（4.2.1 参照）その間で不自然さなく受け取れるテーマに絞られているためとも、考えられる。

次に、テーマの題材と詐称された組織との関連を整理した結果を「**表 3.3-1 メールのテーマと詐称組織**」に示す。

表 3.3-1 メールのテーマと詐称組織と宛先の一覧

#	詐称・踏み台組織	宛先	テーマ
Op1	業界団体	不明	案内（セミナー）
Op2	業界団体	業界団体	案内（セミナー）
Op3	企業（製造業）	業界団体	案内（制度）
Op4	企業（製造業）	業界団体	申し込み完了（セミナー）
Op5	業界団体	企業（製造業）	案内（会員）
Op6	業界団体	企業（製造業）	案内（会員）
Op7	業界団体	企業（製造業）	注意喚起
Op8	企業（卸売業）	業界団体	申し込み（制度・応募要項等）
Op9	業界団体	業界団体	案内（セミナー）
Op10	公的機関	業界団体 個人・フリーメール	資料の改定
Op11	不明	個人・フリーメール	不明
Op12	企業（製造業）	業界団体 個人・フリーメール	申し込み（セミナー）
Op13	公的機関	業界団体	案内（セミナー）
Op14	業界団体	企業（製造業）	案内（セミナー）
Op15	業界団体	企業（製造業）	案内（会員）
Op16	公的機関	企業（製造業）	案内（セミナー）

業界団体や、公的機関を詐称しているケースはセミナーや会員に関する「案内」を題材にしているケースがほとんどであった。他には資料の改定連絡や、注意喚起も見られた。一方、企業を詐称し業界団体へ送られたケースでは、申し込みに関するものが大半であった。これらオペレーションでは、受信者にとって発信元組織と送付内容が、全く違和感を覚えないようテーマに工夫を凝らしている。

3.3.3. メール本文の特徴

メール本文中に特徴的な文言と、入力上の特徴が見られた。

（1）特定の文言：「ご高覧ください。」

16 のオペレーションのうち、本文中に「ご高覧ください。」が含まれるケースが多く見られた。事例を「図 3.3-4 本文中のキーワード（ご高覧）」に示す。

図 3.3-4 本文中のキーワード（ご高覧）

次に、137 通のメールのうち、本文に「ご高覧」が含まれていた割合を「図 3.3-5 メール本文に[ご高覧]が含まれる割合」に示す。

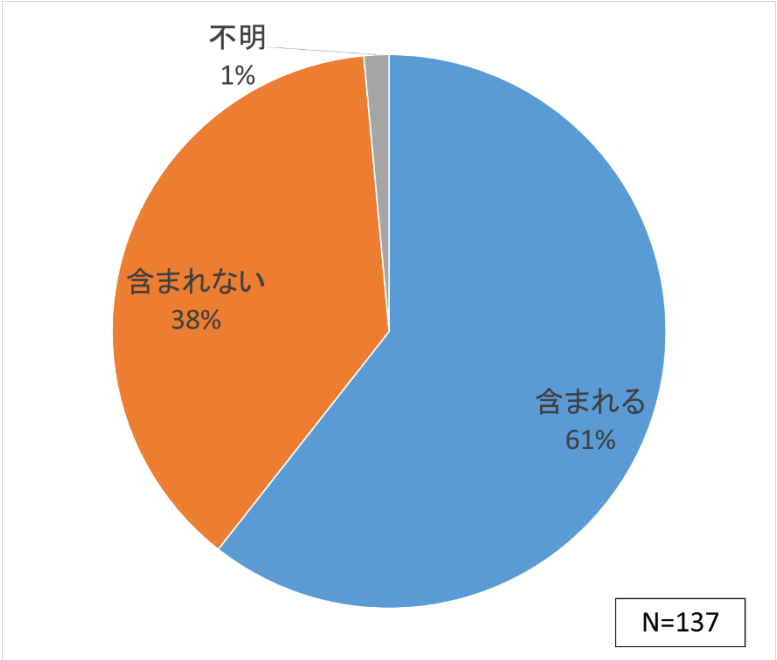


図 3.3-5 メール本文に[ご高覧]が含まれる割合

「高覧」は「見る」の非常に丁寧な尊敬語で、ビジネスでも使われる言い回しだが、本キャンペーンで共通して使われる用語が決まっているため、この部分だけ使いまわしているかと思われる。

（２）先頭行の不自然な改行

16 のオペレーションのうち、本文の先頭行に改行が含まれるケースが多く見られた。事例を以下、「図 3.3-6 メール本文先頭行の不自然な改行（例１）」「図 3.3-7 メール本文先頭行の不自然な改行（例２）」に示す。

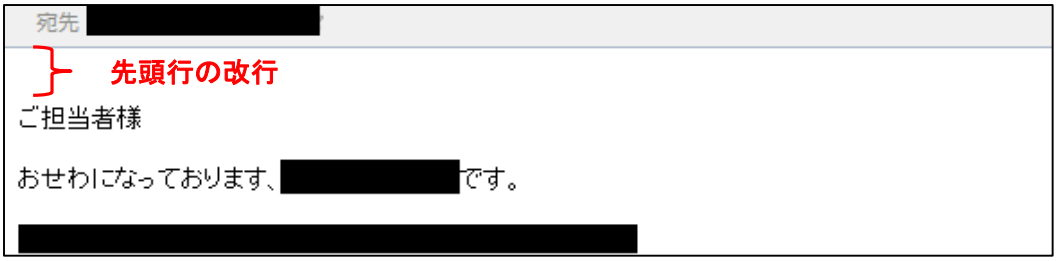


図 3.3-6 メール本文先頭行の不自然な改行（例１）

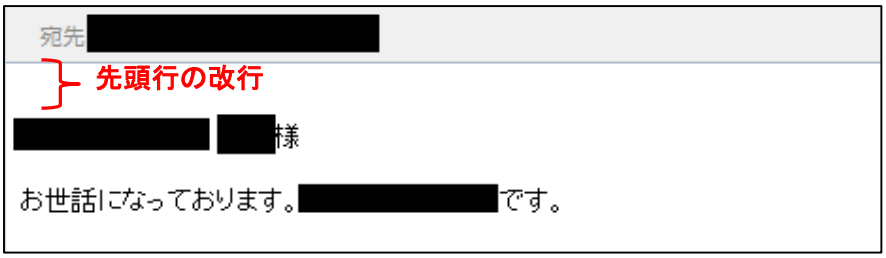


図 3.3-7 メール本文先頭行の不自然な改行（例２）

先頭行に改行が含まれていないケースを「図 3.3-8 改行がつかないケース」に示す。

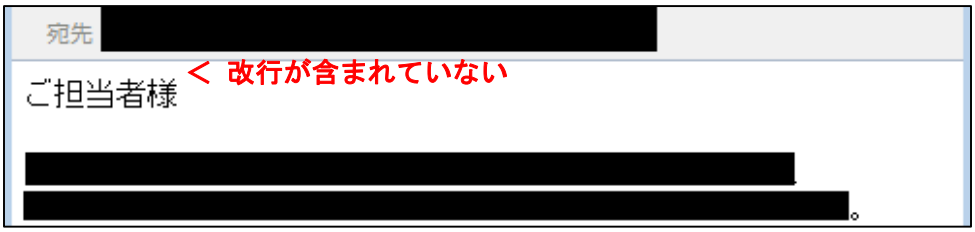


図 3.3-8 改行がつかないケース

表 3.3-2 先頭行に改行がある

#	通数
先頭行に改行あり	132
先頭行に改行なし	3
不明	2

興味深いことに、132 通（96%以上）で先頭行に改行があることが分かった。理由として、HTML 形式でメールを送る際に自動的に改行が挿入されるケースも考えられたが、本件は HTML 形式ではなく TEXT/PLAIN 形式であり、この可能性は無いと思われる。ま

た、攻撃者がメール送付用にスクリプトを作っているなどで、バグも考えられる。しかし、あるオペレーションの中で、突然改行が無いメールを送った後に次のメールからまた改行が含まれ直されているケースもあるため、本キャンペーンの攻撃者には「先頭行に改行を含めるというメール作成時の癖」がある可能性や、「日本では先頭行に改行を含めるのがビジネスマナー」と思い込んでいることも考えられる。

3.3.4. 添付ファイルの特徴

一連の標的型攻撃メールで使われた添付ファイルは、すべてパスワード付きの ZIP 形式で圧縮されており、本文に記載された「解凍パスワード」を入力し解凍することで「図 3.3-9 添付ファイルの解凍後」のファイルが得られる。

通常、拡張子を表示していない場合「exe」などの実行ファイルに気付かずに実行してしまうケースがあり、拡張子を表示するよう強く推奨しているが、本事例では**ファイル名を長くする**ことで、一目では拡張子が表示されづらくなっている。

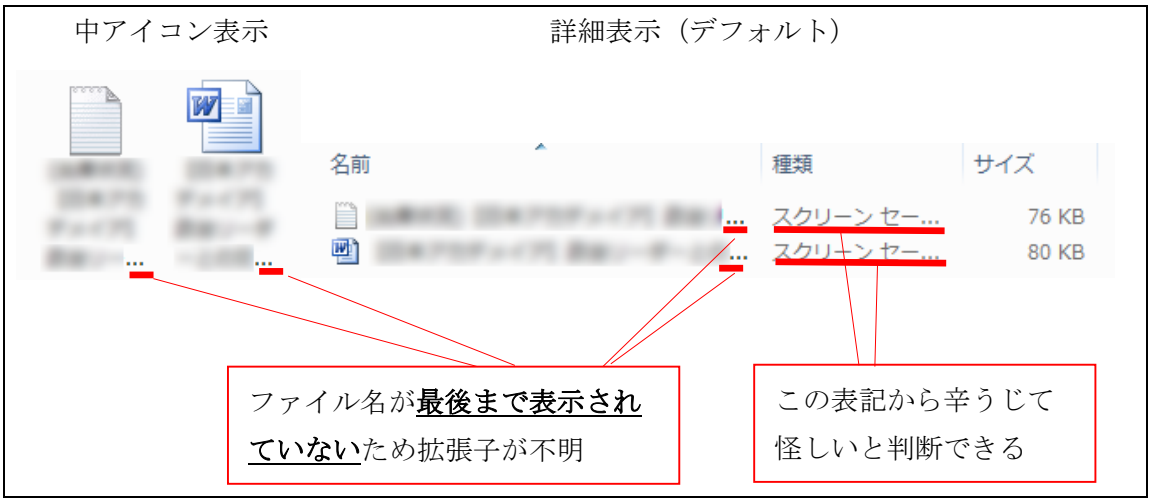


図 3.3-9 添付ファイルの解凍後

本キャンペーンで使われた圧縮ファイルを解凍した後にできるウイルスについて、ファイル名の文字数をカウントした結果を「**表 3.3-3 解凍した添付ファイルの文字数**」に示す。

表 3.3-3 解凍した添付ファイルの文字数（サンプル数 155）

最大文字数	106
最低文字数	72
平均	85.9

※半角文字を 1、全角文字を 2 としてカウント

ファイルを実行する際には、以下のように、ファイル名全てを表示させることで、拡張子を確認することが重要である。なおこの事例では Unicode 制御文字 RLO が使われているため、表示上「.txt」や「.doc」ファイルに見えるが、実際はスクリーンセーバー型の実行ファイル「.scr」である。

図 3.3-10 添付ファイルの解凍後（ファイル名全表示）

4. 攻撃者の挙動解析と攻撃目的の解明

4.1. 攻撃者の挙動解析

4.1.1. キャンペーンにおける挙動解析

各オペレーション（Op.）が行われた時間を週統計にて整理した結果を「図 4.1-1 攻撃メール件数：週統計」に示す。

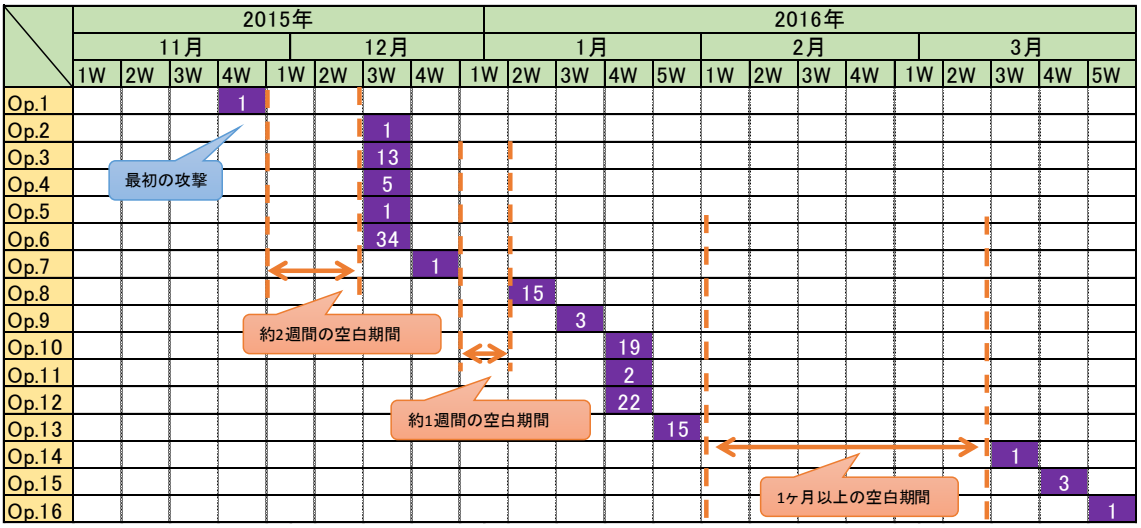


図 4.1-1 攻撃メール件数：週統計（表中の数値はメール件数を表す）

興味深いことに、12 月の第 5 週（図中、1 月の第 1 週）はメールの受信は確認されていない。（この時期はクリスマスと正月を含むが、クリスマスイブには受信があった。このため、クリスマスイブまで活動していたのではないかと考えられる。） また、2 月の 1 週から 3 月の 2 週まで 1 ヶ月以上の「空白期間」があった点も注目すべき点である。

12 月の第 5 週（1 月の第 1 週）は、攻撃者は一般的に日本の組織の勤務スタイルに合わせてメールを送る傾向があることからも、「対象組織の事情に合わせた」攻撃と考えられる。

しかし、11 月の第 5 週（12 月の第 1 週）や 2 月の第 1 週から 3 月の第 2 週については、日本では長期の休み等は無く、どちらかというと攻撃者側の事情によるところが大きいとも考えられる。

4.1.2. オペレーションにおける挙動解析

乗っ取ったアカウントから連続して攻撃メールを送る際には、どの程度の送信間隔で送られていたのか、集計した結果を「**表 4.1-1 連続して送られたメールの平均送付間隔**」に示す。

表 4.1-1 連続して送られたメールの平均送付間隔

#	平均送信間隔	メール数	宛先組織数	送付開始時刻（日本時間）
Op3	0:01:13	13 件	1	17 時
Op4	0:02:23	5 件	2	23 時
Op6	0:01:06	34 件	23	12 時
Op8	0:00:34	15 件	1	16 時
Op10	0:02:11	19 件	7	9 時
Op12	0:00:55	22 件	4	15 時
Op13	0:01:31	15 件	1	0 時
合計	0:01:17	123 件		

※赤字は平均より速いペース、青字は平均より遅いペース

一番早いペースで送られていたオペレーションは Op8 の 34 秒間隔であった。これは J-CRAT で把握している本キャンペーンの中では、正月休み明けの攻撃であった。また、一番遅いペースで送られていたのは Op4 の 2 分 23 秒間隔であった。この Op4 では前述の「図 4.1-3 23 時台（日本時間）のメール送付」でも紹介しているが、2 組織に対して送っている。この、組織の変わり目のところで 5 分 49 秒と少々時間が空いたため、平均間隔が長い結果となった。次の組織のアドレスを探すのに手間取った、または深夜に新規にメールを開始することへのためらいがあったのかもしれない。いずれにせよ、メール通数や宛先の組織数では特徴的な傾向は見られなかった。また、12 時～17 時（日本時間）では平均より早いペースで送っているが、23 時、0 時、9 時（日本時間）などの深夜早朝時間帯は平均より遅いペースで送られていた。

4.1.3. 攻撃時間帯における挙動解析

メールの送信された時間ごとの通数を「図 4.1-2 攻撃メール通数：時間統計」に示す。

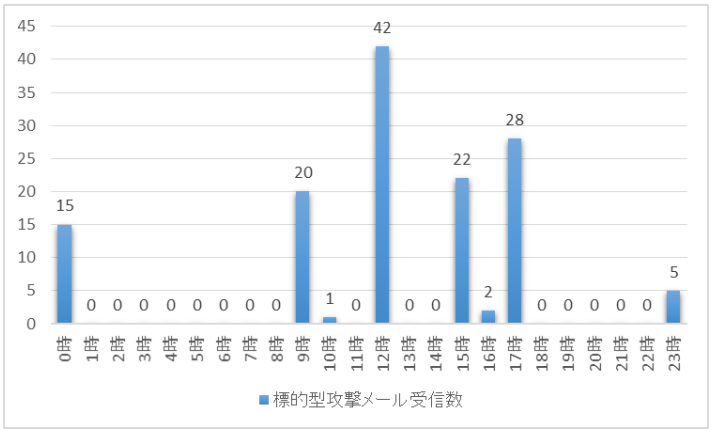


図 4.1-2 攻撃メール通数：時間統計（日本時間）

図内の時刻は、標的組織の管理するメールサーバーでメールを受け取った時間（日本時間）である。85%のメールが 9 時台から 17 時台に着信している。これは日本の組織の勤務スタイルに合わせてメールを送ることで、咄嗟に開かせることを狙っていると考えられ、「対象組織の事情に合わせた」攻撃の一環と考えられる。

その中でも 11 時台と 13 時台、14 時台は 1 通も送られていない。これは日本の組織の業務時間帯などを加味した可能性と、攻撃者の事情によるところのどちらとも考えられる。ただし、UTC＋8 を採用している国では日本時間の 13 時台、14 時台は 12 時台、13 時台となり一般的な『お昼休み』の時間と重なることが分かる。

一方で、深夜の 23 時台に 5 通、0 時台に 15 通の着信も確認されている。23 時台の 5 通については 12 月 16 日（水）に送られている（Op.4）。この概要を「図 4.1-3 23 時台（日本時間）のメール送付」に示す。

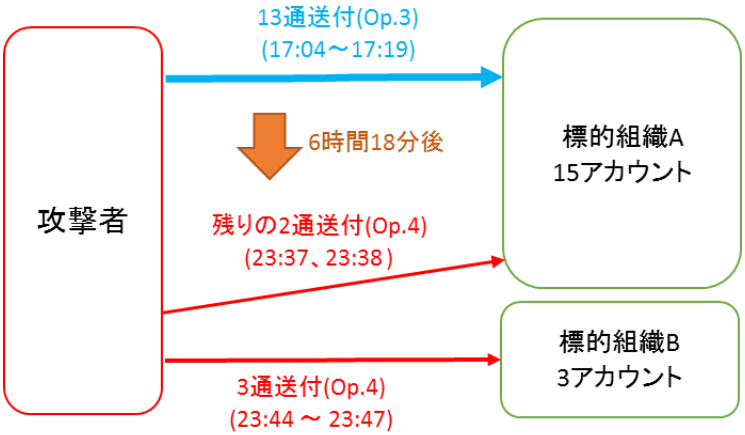


図 4.1-3 23 時台（日本時間）のメール送付（Op.3、Op.4）

攻撃者は標的組織 A の標的メールアドレスリストを 15 件保持しており、これらに対して 17 時 4 分より標的型攻撃メールを送り始めた（Op.3）。13 件目を 17 時 19 分に送り終えたがその後、次の 14 件目を 23 時 37 分に送るまで、6 時間 18 分の空白時間が発生した。これは何らかの事情や意図があったものと考えられる。攻撃者側の事情としては攻撃インフラが一時的に使えない、などのシステム的な点のほか、人的リソースの一時的欠如など、人間の事情によるものも考えられる。

17 時台に送られたメールは 28 通あるが（図 4.1-2 攻撃メール通数：時間統計（日本時間参照）、この 17 時 19 分以降に送られたケースは、フリーメールから送られた 17 時 33 分 30 秒の 1 通のみであり、それ以外はすべて 17 時 19 分以前に送られている。

次に 0 時台に 15 通送られているケースだが、これは全て、1 月 28 日（木）の 0 時 36 分から 0 時 57 分に送られている。これは前述した 2 月からの「空白期間」に入る前の最後の攻撃メールであった（Op.13）。この事例では添付ファイル解凍時にウイルスと共に保存されるデコイ（おとり）ファイルが唯一準備されていなかった事例であることからも、攻撃者側に時間的猶予が無く、慌てて送ったものとも推測される。

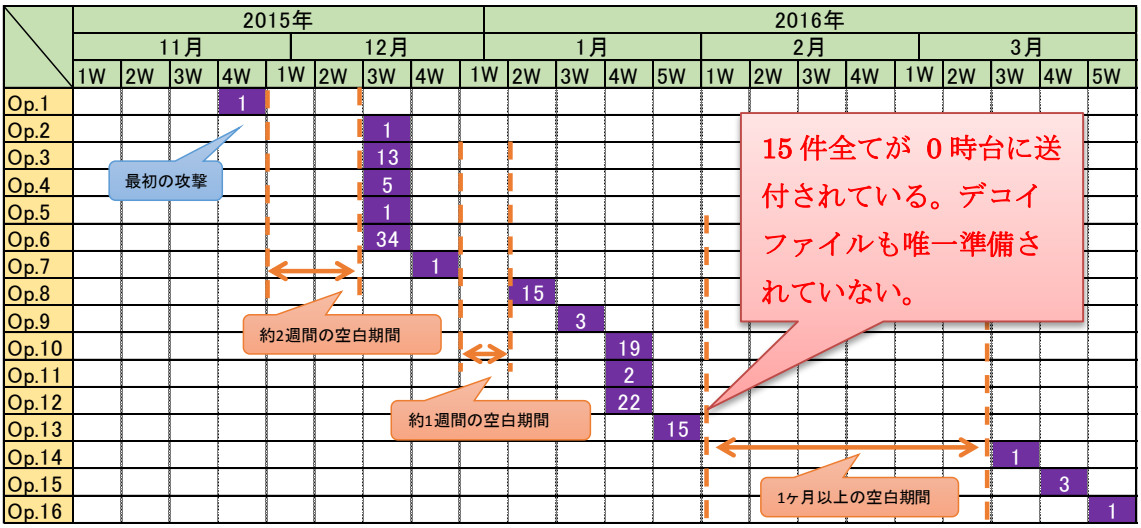


図 4.1-4 攻撃メール件数：週統計

4.2. 攻撃対象組織と攻撃目的の解明

4.2.1. 詐称・踏み台組織と攻撃対象組織の関連

次に、各 Op で標的型攻撃メールの差出人として詐称された、または踏み台とされた（本項では詐称されたに統一する）組織と狙われた組織を比較した結果を「**表 4.2-1 標的型攻撃メールの送付先**」に示す。

表 4.2-1 標的型攻撃メールの送付先

#	詐称・踏み台組織	宛先	ケース	攻撃メール数
Op1	業界団体	不明	-	1
Op2	業界団体	業界団体	ケース E	1
Op3	企業（製造業）	業界団体	ケース A	13
Op4	企業（製造業）	業界団体	ケース A	5
Op5	業界団体	企業（製造業）	ケース B	1
Op6	業界団体	企業（製造業）	ケース B	34
Op7	業界団体	企業（製造業）	ケース B	1
Op8	企業（卸売業）	業界団体	ケース A	15
Op9	業界団体	業界団体	ケース E	3
Op10	公的機関	業界団体 個人・フリーメール	ケース C	19
Op11	不明	個人・フリーメール	-	2
Op12	企業（製造業）	業界団体 個人・フリーメール	ケース A	22
Op13	公的機関	業界団体	ケース C	15
Op14	業界団体	企業（製造業）	ケース B	1
Op15	業界団体	企業（製造業）	ケース B	3
Op16	公的機関	企業（製造業）	ケース D	1

このように以下のケースに分けることができる。

- ケース A：**企業**を詐称し、**業界団体**を狙うケース（Op3,Op4,Op8,Op12）：[55 通]
- ケース B：**業界団体**を詐称し、**企業**を狙うケース（Op5,Op6,Op7,Op14,Op15）：[40 通]
- ケース C：**公的機関**を詐称し、**業界団体**を狙うケース（Op10,Op13）：[34 通]
- ケース D：**公的機関**を詐称し、**企業**を狙うケース（Op16）：[1 通]
- ケース E：**業界団体**を詐称し、**業界団体**を狙うケース（Op2 と Op9）：[4 通]

これらの結果から、企業を狙う場合は、業界団体や公的機関を詐称しており、企業を詐称する場合は業界団体を狙う傾向にあったことが分かる。これは、**実際の組織間の業務（取引）の関わりを悪用**して攻撃が行われているものと考えられる。

詐称された送付元や宛先のいずれか、または両方に業界団体が含まれている攻撃メールは、全 137 通の内の 134 通であり、このキャンペーンは標的とする産業の業界団体を軸に、仕組まれたものと見ることもできる。

4.2.2. 攻撃対象組織と目的の分析

標的型攻撃メールの送付先を整理した結果を「**表 4.2-2 標的型攻撃メール 137 通の狙っている団体の区分**」に示す。

表 4.2-2 標的型攻撃メール 137 通の狙っている団体の区分

宛先	メール件数	組織数
業界団体	86	8
企業・製造業	37	27
企業・卸売業	2	1
企業・ソフトウェア業	1	1
個人・フリーメール	9	7
不明	2	-
総計	**137**	**44**

このように「業界団体」への攻撃メールが最も多いことが分かる。本キャンペーンで標的となった業界団体は 8 つで、主に製造業に関わる業界であった。また、**一般企業を狙ったものが 40 通**あったが、そのうち **37 通**（組織数 27）**では同一の業界の**、特定の製造業を狙った攻撃であった。また、各 1 社が狙われた卸売業、ソフトウェア業においても、この製造業に深く関わる組織であった。また、業界団体（組織数 8）のほとんどが製造業に関わる組織が所属している。このことから、本キャンペーンにおいて**攻撃者は少なくとも、ある分野の製造業に狙いを絞って攻撃を行っていることが明らかとなった。**

さらに企業に対して送られたメールのうち、職種を見てみると、ある特定の部門に所属する人物、またはそれらを管理する役員クラスに送られる傾向があることがわかった。

5. まとめ

J-CRAT では、情報提供いただいた標的型攻撃メールは速やかに分析し、防御や対策に役立つ情報として適切な匿名化を行った上で関係組織に提供している。また、情報提供者の了解の下に被害が疑われる組織などに対して可能な範囲で情報提供を行い、標的型攻撃の被害低減に活用いただいている。さらに、標的型攻撃メールの送付経路としてメールの不正中継が疑われる場合は、アカウント利用者へ直接コンタクトを取り、その事実を伝える。さらに不正中継が行われたメールアカウントのログ等から送信履歴を確認することで標的型攻撃メールの送付先を解明している。解明された標的型攻撃メールの送付先組織に対しては直接コンタクトを行うことで、実際の受信の有無や感染状態を把握し、感染している場合は応急的な駆除と感染の広がり等が無いかを確認し、助言している。また、メールの送付先を把握することで攻撃者の足どりや、攻撃者の狙う業界を予測している。

このように、標的型攻撃の情報の提供と共有は各組織に対して攻撃の被害とその侵攻に対抗するため有効である、また、攻撃者や犯人の目標や意図の解明に活用することで、先回りした対策の効果も期待できる。

本報告での、標的型サイバー攻撃キャンペーンの追跡と対策および分析を通して、攻撃者の挙動や狙い（標的業界や分野）などが見えてきた。これは分析の一例に過ぎないが、この分析を通して得られた、組織が備えるべきこと、および、今後の J-CRAT 活動の展開について、以下に述べる。

5.1. 組織が備えるべきこと ～標的型サイバー攻撃に対する留意点～

（１）乗っ取られたアカウントを悪用した攻撃

標的型攻撃メールの中でも広くばらまかれるタイプのメールはフリーメールアドレスが悪用されることが多いが、背後に意図・目的があると推測される本事例では、関わりのある組織の乗っ取られたアカウントがメール送信に悪用されていたことを 3.3.1 項で解説した。従って、普段交信実績のある組織でも、メールに対して不審なところがあれば、添付ファイルの開封[5]や記載リンク先のクリックは避け、細心の注意を担当者が払うことが重要である。

（２）業務時間帯や勤務日を考慮した攻撃

5 実行ファイル形式(拡張子が「.exe」や「.scr」などのもの)のファイルを圧縮した添付ファイルや、Microsoft Office シリーズのマクロ機能を悪用するウイルスにも注意が必要である。

業務時間外に送られたメールが他のメールにまぎれてしまったり、休日中に送付された業務メールに対して警戒されることを避けるため攻撃者は、開封の可能性の高い業務時間帯に攻撃メールを発信していることを、4.1.3 項、4.1.1 項で解説した。従って、こうしたメールを受ける可能性の高い窓口や担当者の不審メールを見抜ける判断力を高めげることが、組織にとってはまず着手すべき課題である。不審メールの見分け方については J-CRAT でまとめたレポート[6]などを組織内教育等に活用されることをお薦めする。

（３）同一組織への複数の攻撃

一つのオペレーションで同一組織内の複数のメールアドレスに発信されていることを、4.1.2 項で解説した。組織においては、リテラシーの高い人がひっかからなくても、他の人がウイルスを踏んでしまえば、組織として被害は免れない。誰か一人でも不審に思ったことをシステム管理部門や組織内 CSIRT 等に報告して、組織全体への注意喚起や、組織員への類似攻撃メールの着信（着弾）を検索し、組織を守れる仕組みと体制を整備していくことが、重要である。

（４）攻撃の検知能力の向上と情報提供および情報共有の重要性

このキャンペーンへの対応を進める中で、ある事例では、標的型攻撃メールのウイルス感染から数分後には別の攻撃ツールが仕込まれ、急速に組織内に感染を広げ、6 日以内に情報がまとめて窃取されるケースがあった。J-CRAT へ連絡があり、暫定対処と被害状況を確認した時点では既に情報が抜き取られた後であった。もう少し早く把握できていれば、情報の窃取を防げた可能性はある。このためにも早急な把握・検知は必須条件である。また、その情報の提供と、関連組織への速やかな情報共有が、業界を守っていくためには重要である。

（５）攻撃の対応を阻む証跡情報の不足

このキャンペーンへの対応を実施する中では、ログを取得していないために感染者を特定できないケースもあった。例えば、不正中継されたメールサーバーまでは特定できたものの、利用しているユーザーにたどり着けないケース、ユーザーまで把握できるがメールサーバーやサービスのログが一定時間を経て消えてしまっているケース等があった。ログを取得していないと、攻撃メールの送付先が明確に把握できないため、ユーザーに対して直接の注意喚起を行うことができない。

これまでの J-CRAT 活動状況報告[7]でも組織としてのログ取得の重要性を述べているが、自組織の被害の究明だけでなく、他への攻撃の追跡にログ取得は非常に重要である。

---

6 IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」：
http://www.ipa.go.jp/security/technicalwatch/20150109.html
7 サイバーレスキュー隊 J-CRAT：http://www.ipa.go.jp/security/J-CRAT/index.html

標的型サイバー攻撃は、日本の組織が有する知財や社会の基盤に対する大きな脅威である。その総体的な被害を極小化していくためには、痕跡を追跡する際に必要となるログ証跡取得の仕掛けは防御と同じ位重要である。インターネットが事業の基盤となった今、標的型サイバー攻撃に対抗していくことが不可欠であり、ログ証跡取得の仕掛けは、それぞれの組織の事情はあるものの、自組織、業界、ひいてはわが国全体に求められるということを、経営幹部は認識され[8]、対策が進むことを期待したい。

（６）狙う業界（事業分野）に関わる業界団体を介した攻撃

3.3.2 項で解説した標的型メールのテーマ、4.2.１項で解説した標的型メールの送信元や送信先に複数の業界団体が絡んでいた、という特徴が、このキャンペーンの分析の中で明らかになった。背後に、日本の特定の業界や事業分野を攻撃対象とする明確な意図がうかがえる。最終標的の組織に対する攻撃において、中継点が業界団体になっていることは、ある意味で日本の業界の構造をついた攻撃といえ、巧妙である。

こうした攻撃が今後も多く発生することが想定されることから、業界団体は一層のセキュリティ対策と、また、その攻撃に即応できるスキームが今後必要となってくるものと考える。

この具体的な対応案については、次節で述べる。

5.2. 今後の活動の展開 ～業界団体との連携の重要性～

攻撃者による、機密情報（知財、業界、等）の窃取や、社会システムへの妨害などが、産業や社会にとって大きな脅威である。そのいずれも、業界団体が攻撃者の狙いや足掛かりの一つになってくるものと思われる。IPA の活動では、現在標的となっている個々の組織にたいして直接のコンタクトを実施しているが、把握し切れていない組織の救済やその効果、スピードを考えると、業界団体との情報共有や連携が非常に重要と考えている。その活動スキームのイメージを図 5.2-1 に示す。以下に、2 通りの業界団体との連携のパターンを述べる。

（１） 業界団体を経由した注意喚起

攻撃者は組織の規模に関わらず、業界シェアを誇る企業や、独自技術を持つ企業を巧妙に見つけ出し、攻撃を仕掛けてくる。そしてその足がかりとして、ターゲットとする業界の業界団体を踏み台または、なりすましに利用するケースが良く見られる。このため、標的型メールから特定された業界団体に情報を提供して、業界団体傘下の会員企業へ広く注意喚起するのが一つの有効な対策となりうる（図 5.1 ③④）。

8　サイバーセキュリティ経営ガイドライン：http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

そのためには、業界団体から会員企業へ展開される情報の一つとして、セキュリティ上の注意喚起情報を含めていただき、それを展開するスキームと、それを受けとった会員企業内でその情報を活用する仕掛けの確立が重要である。

（２）攻撃対象となりえる関連業界団体への注意喚起

標的型攻撃事案の攻撃メールから直接割り出された業界団体だけでなく、標的型攻撃キャンペーンの分析を通して攻撃目標（業界や製品分野）が見えてきた段階で、関わりのある業界団体へも攻撃検知情報を共有して所属会員企業に注意喚起ができれば、攻撃者が狙う企業組織における有効な対策になるものと考えられる。実際、今回の事案では、足掛け 4 ケ月に渡り行った、レスキュー活動と連鎖の追跡は、その開始からわずか 1 ヶ月余りで攻撃者の目標分野が見えてきていた。この段階で、関連業界に情報をインプットできることは効果的な対策になったものと考えられる（図 5.2-1 ⑤⑥）。

この注意喚起情報の流れを実現するには、業界団体とのチャネルの設置だけでなく、そこから会員組織の団体窓口から情報システム部門や組織内 CSIRT に情報が流れ、対応を取れるかが重要となる。こうしたスキームの確立が、今後の課題となる。

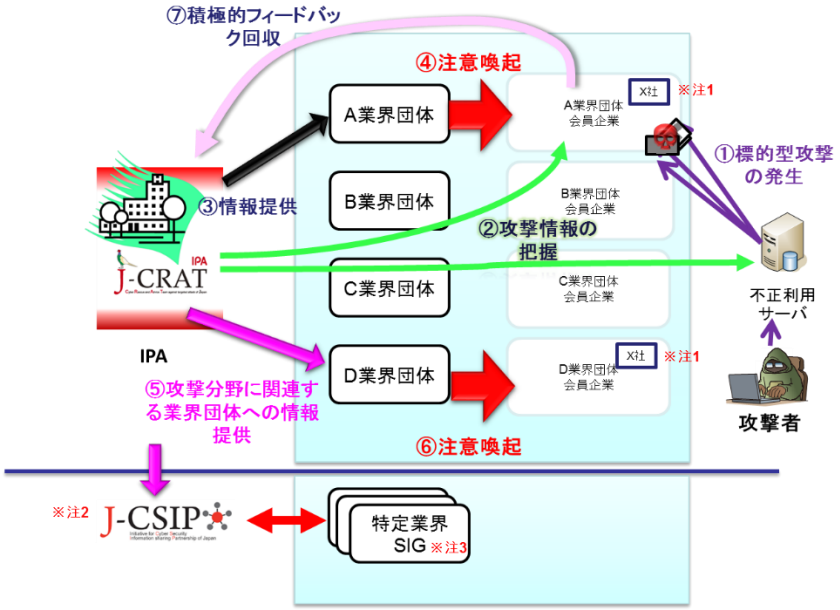


図 5.2-1 業界団体を介した注意喚起と業界団体への働きかけ

注 1）企業が展開する様々な事業分野で複数の業界団体に属していることも珍しくない。

注 2）IPA では、サイバー情報共有イニシアティブ（J-CSIP）[9]という特定業界に特化して、サイバー攻撃に関する情報共有を行う体制を運用している。この取組みでは、既に各業種の業界団体が非常に大きな役割を果たしている。J-CSIP には、2016 年 6

[9]サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan
https://www.ipa.go.jp/security/J-CSIP/

月現在、7 業界、72 組織が参加している。J-CRAT の活動を通じ、情報共有による集団的な防御体制への参画が望ましいと思われるケースについては、J-CSIP への参加も呼び掛けていく。

注 3）SIG（Special Interest Group）：類似の産業分野同士が集まったグループ

特定業界を執拗に狙う攻撃キャンペーンの分析
～2015 年秋から 2016 年春に見られた攻撃事例～
サイバーレスキュー隊（J-CRAT）分析レポート 2015

［発　　行］2016 年 6 月 29 日
［著作・制作］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
［執　筆　者］伊東宏明 青木眞夫 金野千里