広　報　資　料

平成 25 年 2 月 28 日

警備企画課・情報技術解析課

平成 24 年中のサイバー攻撃情勢について

1　概況

平成 24 年中も引き続き、我が国の政府機関等に対し、情報窃取を企図したとみられるサイバー攻撃（標的型メール攻撃）やウェブサイトに閲覧障害や改ざんが生じた事案（DDoS 攻撃等）が発生（攻撃の技術的特徴等は「情報技術解析平成 24 年報」参照）。

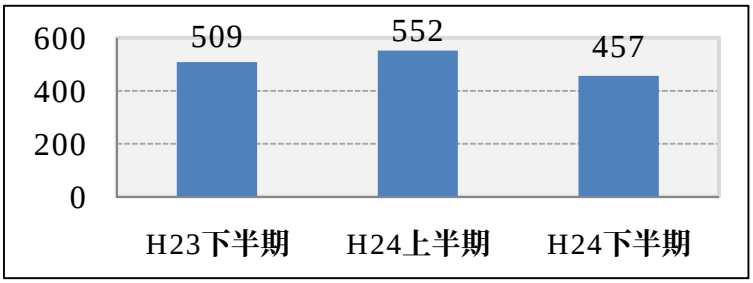
2　標的型メール攻撃

○　警察では、平成 24 年中に合計 1,009 件の標的型メールが我が国の民間事業者等に送付されていたことを把握。

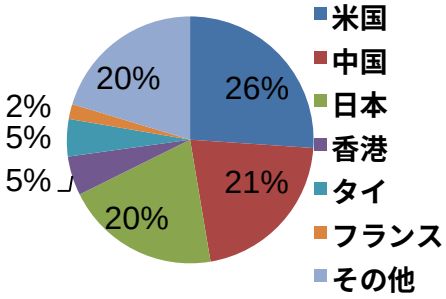
○　標的型メール攻撃に使用された不正プログラム等による通信の接続先は、約 26%が米国、約 21%が中国、約 20%が日本。

○　最初から標的型メールを送付するのではなく、不正行為に関する告発や採用希望を装うなどして、業務との関連を装った通常のメールのやりとりを何通か行い、より自然な状況を装った後に、標的型メールを送付する「やりとり型」の手口を把握。

○　政権交代や尖閣諸島等の国内外の情勢を捉えた標的型メールが複数の民間事業者等に対して送付されたことを把握。



【サイバーインテリジェンス情報共有ネットワーク等を通じて警察が把握した標的型メール攻撃の件数】



【H24 中の標的型メール攻撃に使用された不正プログラム等の接続先】

3　DDoS 攻撃等

○　国際ハッカー集団「アノニマス」によるとみられるサイバー攻撃事案（６月）や尖閣諸島をめぐる情勢等と関連したとみられるサイバー攻撃（９月）等が発生。

○　ウェブサイト改ざん事案の捜査を通じて把握した IP アドレスを分析した結果、「アノニマス事案」では約５割が欧州諸国所在のものであり、「尖閣諸島事案」では約９割が中国所在のものであった。

別　紙

平成24年中の主なサイバー攻撃事案等について

１　概況

警察では、平成23年８月に先端技術を有する事業者等と構築した「サイバーインテリジェンス情報共有ネットワーク」により、標的型メール攻撃等の情報窃取を企図したとみられるサイバー攻撃事案に係る情報を集約・分析し、注意喚起を実施しており、本ネットワーク等を通じ、平成24年中に合計1,009件（上半期：552件、下半期：457件）の標的型メール（注１）が我が国の民間事業者等に送付されていたことを把握。標的型メール攻撃に使用された不正プログラムに感染すると、コンピュータは不審な接続先に通信しようとする動作を行うが、その接続先は、約26%が米国、約21%が中国、約20%が日本であった。

本ネットワークの構成員は、約4,900の事業者等に拡大（平成25年１月１日現在）しているほか、平成24年３月からは、内閣官房情報セキュリティセンター（NISC）と連携し、政府機関に対する標的型メール攻撃に関する情報についてもネットワーク内で共有している。こうした警察からの注意喚起等により、他の事業者等に行われた標的型メール攻撃と同種の攻撃を受けていたことを確認したのは、平成24年中に770件（上半期：274件、下半期：496件）あり、被害の未然防止のための情報共有の有効性が明らかとなっている。

また、把握した情報のうち、新たな不正プログラム等に関する情報については、ウイルス対策ソフトで検知可能となるよう、ウイルス対策ソフト提供事業者等に提供し、ITユーザ全体のセキュリティ対策の向上を図っているほか、平成24年８月以降は、不正プログラム等による通信の接続先等の情報をセキュリティ関連事業者に提供し、我が国の事業者等が不正な接続先に通信を行うことの防止を図っている。

さらに、国際ハッカー集団等が自らの主義主張を誇示する目的でサイバー攻撃を行い、我が国の政府機関等のウェブサイトに閲覧障害が生じた事案も発生している。警察では、サイバーフォースセンター等において、関連するウェブサイトやチャットページ等の観測態勢を強化し、情報収集を行っているほか、全国の都道府県警察に設置している「サイバーテロ対策協議会」等を通じ、重要インフラ事業者等に注意喚起を実施している。

警察においては、違法行為に対する捜査を行うとともに、関係省庁や外国治安情報機関等との情報交換を行うことなどにより、攻撃者及び手口に係る実態解明を推進している。

（注１）警察では、標的型メールについて、①迷惑メールと異なり、業務等に関連した内容を装うなど、一見すると正当なメールと区別がつきにくい、②市販のウイルス対策ソフトで検知できない不正プログラムに感染させようとする、との特徴があるものとしている。

２　標的型メール攻撃事案の例

※　(5)～(7)は、平成24年８月23日「サイバーインテリジェンスに係る最近の情勢（平成24年上半期）」で公表した上半期の事例を再掲したもの。

(1)「やりとり型」の標的型メール攻撃事案その１

○　最初から標的型メールを送付するのではなく、11月、まずは不正行為に関する告発を装ってウェブサイトに公開されているメールアドレスに問い合わせを行い、これに回答した担当者のメールアドレスに対し、同日、告発に関する文書の送付を装って標的型メールを送付してきたもの。

○　不正プログラムを仕込んだファイルは圧縮されてパスワードロックされており、展開（解凍）して生成される画像ファイルはRLO機能（注２）を利用してWORDファイルに偽装されていた。

○　攻撃者は、架空の日本人名でフリーメールに登録し、当該メールアドレスを利用して、一連のメールを送付していたが、当該メールアドレスから他の重要インフラ事業者等にも標的型メールが送付されていたことから、当該事業者等に注意喚起を行った。

（注２）アラビア語等に対応するため、ファイル名を右読みから左読みに変える機能で、例えばファイル名「fdp.exe」は、RLO機能により「exe.pdf」と表示されるため、実行ファイルをPDFファイルに偽装することができる。

(2)「やりとり型」の標的型メール攻撃事案その２

○　最初から標的型メールを送付するのではなく、11月、まずは採用希望者を装ってウェブサイトから問い合わせを行い、これに回答した採用担当者のメールアドレスに対し、履歴書等の送付を装って標的型メールを送付してきたもの。

○　不正プログラムを仕込んだファイルは圧縮されてパスワードロックされており、当初、パスワードが分からなかった採用担当者が送信者にパスワードを尋ねるメールを送付したところ、パスワードを教示するメールが返信されて来るなど、複数回のやりとりが行われていた。

○　採用希望者を装って標的型メールを送付する事例は他にも見られ、添付ファイルを開くと、実際の履歴書を装った文書が表示される一方で、コンピュータが不正プログラムに感染する事例も把握。

(3) 国内外の情勢を捉えた標的型メール攻撃事案その１

○　12月、政権交代のタイミングで、複数の民間事業者等に対し、内閣総理大臣就任記者会見に関するお知らせを装った標的型メールが送付されたことを把握。

○　政府機関になりすまし、内閣総理大臣就任記者会見に関する報道機関向けのプレスリリースの文章を利用して本文と添付ファイルが作成されてい

る。
○　不正プログラムを仕込んだファイルは圧縮してパスワードロックされており、パスワードは本文に記載されていた。ウイルス対策ソフトによる検知を回避する目的と推測される。
○　ただし、ファイルの圧縮にrar形式が用いられているほか、不正プログラムを仕込んだ文書ファイルにより表示される文章のフォントが中国語フォントとなっている。

(4) 国内外の情勢を捉えた標的型メール攻撃事案その２

○　10月、尖閣諸島をめぐる情勢に世論の関心が高まる中、政府機関職員になりすまし、「尖閣諸島の領有権についての基本見解」と題した標的型メールが送付されたことを把握。
○　警察では、他の複数の民間事業者等に対し、接続先や接続時のパスワードが一致する不正プログラムを使用した他の標的型メール攻撃が行われていることを把握しており、これらの標的型メール攻撃については、同一又は同じグループの攻撃者が行っていると推測される。共通する特徴は、本文や添付ファイルに政府機関との関連を装った内容が多く、政府関係の業務をしている（又は過去にしていた）民間事業者等の職員に送付されている点である。

(5) 中国地方の事業者が送付した実際のメールが利用された標的型メール攻撃事案（再掲）

○　２月、中国地方のＸ社になりすました標的型メールが「サイバーインテリジェンス情報共有ネットワーク」構成員に送付されたことを把握。本ネットワーク内に注意喚起を行うとともに、Ｘ社に係る調査を実施。
○　その結果、Ｘ社の職員が取引先に対してメールを送付した約11時間後に、当該メールの本文をほとんどそのまま引用し、Ｘ社と業務上関係する２協会・４社宛てに同様の標的型メールが送付されていたことが判明。
○　また、３月には、中国地方のＹ社になりすました標的型メールが本ネットワーク構成員に送付されたことを把握。
○　Ｙ社に係る調査を実施したところ、Ｙ社の職員がＸ社の部長に対して送付したメールを窃取され、Ｘ社と業務上関係する７社宛てにこれを利用して標的型メールが送付されていたことが判明。当該標的型メールには、添付ファイルに不正プログラムが仕込まれた上、実際のメールと同様にパスワードロックが掛けられていた。
○　両件に使用された不正プログラムに感染したコンピュータは、いずれもタイ及び米国所在の同一のIPアドレスに接続する動作を行うことから、同じ攻撃者が、Ｘ社のコンピュータを乗っ取って個人情報やメールを窃取し、これを利用して、同社が業務上関係する複数の事業者等に標的型メールを

送付していたものとみられる。

(6) 政府機関にも民間事業者等にも送付された標的型メール攻撃事案（再掲）

○　４月、内閣官房情報セキュリティセンター（NISC）を通じて得た標的型メール攻撃に関する情報を「サイバーインテリジェンス情報共有ネットワーク」の構成員に注意喚起したところ、同種の標的型メールが製造業者等６社にも送付されていたことが判明。

○　当該標的型メールは、職員採用に関する実在する調査の内容について記述されており、当該調査報告書を装った添付ファイル（PDFファイル）を開くと、調査報告書が表示される一方で、気付かない間にコンピュータは不正プログラムに感染する。

○　「サイバーインテリジェンス情報共有ネットワーク」内に、政府機関宛てに送付された標的型メール攻撃の情報を共有する有効性が明らかとなった。

(7) 多数の地方自治体等に送付された標的型メール攻撃事案（再掲）

○　４月、警察庁を含む複数の省庁に対し、政府機関職員になりすまし、「対北朝鮮措置の延長について」と題した標的型メールが送付されたことを把握。「サイバーインテリジェンス情報共有ネットワーク」を通じた注意喚起を行ったところ、同様のものが２社に送付されていたことが判明。

○　さらに、複数の地方自治体から同様の標的型メールに係る情報提供を受けたことから、全国の都道府県警察に設置された「サイバーテロ対策協議会」等の枠組みを通じ、重要インフラ事業者等にも注意喚起を行ったところ、さらに23の地方自治体及び４事業者に対しても同様の標的型メールが送付されていたことを把握。

○　地方自治体が標的となった理由は不明であるが、北朝鮮の「人工衛星」と称するミサイル発射事案に乗じた標的型メール攻撃とみられる。

３　DDoS攻撃等事案の例

※　(3)は、平成24年８月23日「サイバーインテリジェンスに係る最近の情勢（平成24年上半期)」に記載した上半期の事例を更新したもの。

(1) 国際ハッカー集団「アノニマス」によるとみられるサイバー攻撃事案

○　６月、国際ハッカー集団「アノニマス」を名乗る者が、同月20日に改正著作権法が成立したことを受け、海外のウェブサイト上で、我が国の政府機関等に対するサイバー攻撃を示唆する書き込みを行ったもの。

○　当該ウェブサイトで示されたチャットページにおいて、日本へのサイバー攻撃に関するやり取りが行われ、その後、関連が疑われる被害が発生。

○　財務省や国土交通省等のウェブサイト改ざん事案では、いずれも、「大飯原発再稼働断固反対」、「WE ARE ANONYMOUS」等の内容が表示されるよう改ざんされた。また、裁判所や日本音楽著作権協会等のウェブサイトでは、アクセス集中により閲覧が一時的に困難となった。

○　ウェブサイト改ざん事案の捜査を通じて把握したIPアドレスを分析した結果、全て海外所在（約52%が欧州諸国、約22%がオーストラリア及び米国）のものであった。

(2) 尖閣諸島をめぐる情勢等と関連したとみられるサイバー攻撃事案

○　平成22年９月に尖閣諸島周辺で発生した中国漁船による公務執行妨害事件発生以降、近年、満州事変（柳条湖事件）の日である９月18日付近に我が国に対するサイバー攻撃事案が発生。平成24年は、９月11日の我が国政府による尖閣諸島国有化以降、中国各地で連日、反日デモが発生。

○　こうした情勢の中、９月、中国のハッカー集団「中国紅客連盟」の掲示板等において、攻撃対象として日本の行政機関や重要インフラ事業者等が掲示されたほか、中国の大手チャットサイト「YYチャット」等では、最大４千人が参加し、攻撃予告や攻撃ツール等に関する書き込みがなされた。

○　約300の日本の組織が攻撃対象として掲示され、そのうち、総務省統計局、政府インターネットテレビ等のウェブサイトの閲覧が一時的に困難となった。また、裁判所等のウェブサイトが、中国の国旗等の画像や尖閣諸島は中国のものである旨の文章等が表示されるよう、改ざんされた。

○　ウェブサイト改ざん事案の捜査を通じて把握したIPアドレスを分析した結果、全て海外所在（約94%が中国）のものであった。

(3) 地方自治体等が開設した「フォーム」等への大量送信事案

○　６月から７月にかけて、県庁を始めとする11府県13の重要インフラ事業者等（地方自治体８、ガス２、鉄道２、空港１）のウェブサイトに対し、大量のデータが送信されたもの。

○　ウェブサイトで問合せや意見等を受け付けるために開設している「フォ

ーム」（注３）に、空白や数字等の意味のない内容が、短時間に大量に送信されたり、当該事案と同じIPアドレスからウェブサイトに大量のアクセスが行われたりしたもの。

○　捜査を通じて把握したIPアドレスを分析した結果、全て海外所在（約50％が韓国、約42％が中国）のものであった。

○　なお、関連は不明であるが、平成25年１月にも、３つの地方自治体のウェブサイトに対し、同種の大量送信がなされる事案が発生している。

（注３）問合せや意見等を受け付けるため、ウェブサイト管理者が選定した項目のボックスに閲覧者が情報を入力・選択できるようになっているページ。例えば、意見要望フォームでは、各項目のボックスに氏名・連絡先や意見を入力し、送信ボタンを押下することにより、情報を送信することができる。

サイバー攻撃対策に関する警察の取組

サイバーインテリジェンス情報共有ネットワーク

先端技術を有する事業者等

- 全国約4,900の事業者等が参画（H23.8～）
- H24.3以降、NISC（政府機関に対する攻撃を集約）と相互に情報共有

標的型メール攻撃等の情報を提供

他の事業者等に対し注意喚起を実施

同種の攻撃を確認（770件）

サイバーテロ対策協議会

重要インフラ事業者等

- 各都道府県警察に設置
- 管内の10分野（※）の事業者が参画

サイバー攻撃に関する情報の共有

※情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

警察

民間事業者等からの情報を集約・分析

平成24年中に**1,009件の標的型メール**を把握・注意喚起

サイバーフォースセンター等における関連ウェブサイト等の観測態勢の強化

国際ハッカー集団等による サイバー攻撃を把握・注意喚起

不正プログラム対策協議会

新たな不正プログラム等の情報を提供

最新の手口等の提供

ウイルス対策ソフト提供事業者等

- 4社と設置（H23.8～）
- ウイルス対策ソフトの更新等により、ITユーザ全体のセキュリティ対策を向上

不正通信防止協議会

セキュリティ関連事業者

不正プログラム等による通信の接続先等の情報を共有

- 10社と設置（H24.8～）
- 我が国事業者等による不正な接続先への通信を防止

■ 違法行為に対する捜査・海外の治安情報機関等との情報交換 → 攻撃者及び手口等に係る実態解明を推進