Information-technology
Promotion
Agency, Japan

プレスリリース

2014 年 5 月 30 日
独立行政法人情報処理推進機構

問い合わせ等のフリをして送りつけられる「やり取り型」攻撃メールが国内の複数組織の窓口へ同時並行的に送信されていたことを確認

― サイバー情報共有イニシアティブ（J-CSIP[*1]）2013 年度　活動レポート ―

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、標的型攻撃の防御に向けた産業界との情報共有の枠組みである「サイバー情報共有イニシアティブ」（J-CSIP）において、参加組織から得られた情報の集積・共有を通じ、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）の実態を明らかにし、2013 年度（2013 年 4 月～2014 年 3 月）の活動レポートとして公開しました。同レポートでは、情報共有の運用状況に加えて、2013 年度に扱った標的型メールの分析も行っています。
URL：https://www.ipa.go.jp/security/J-CSIP/

IPA では、国内組織を狙った標的型攻撃の深刻な被害が 2011 年に表面化したことを受けて発足した J-CSIP 等[*2]、標的型サイバー攻撃に対する活動を通じ、巧妙な「やりとり型」攻撃が 2012 年以降引き続き発生していることを確認しています。「やり取り型」攻撃とは、一般の問い合わせを装った無害な「偵察メール」の後、ウイルス付きのメールが送られてくるという、標的型攻撃の手口の一つです。今回のレポートでは、この脅威に対する周知を図り、国内組織における対策に役立てるため、具体的な事例を基に解説しました。

レポートでは、J-CSIP および IPA の相談窓口に情報提供された 15 件の事例より、同一と思われる攻撃者から複数の国内組織に対して同時並行的に行われた「やり取り型」攻撃の実態を明らかにしています。このような手口の一端を把握できたのは、個別の攻撃事例や単一の組織からの情報にとどまらず、複数組織からの情報を集約・共有するという J-CSIP の運用があってのことです。

（1）「やりとり型」攻撃の事例

1) 複数の組織の様々な問い合わせ窓口に対して、“製品に関する問い合わせ”“窓口の確認”といった「偵察メール」が送りつけられていた。また、短期間（約 2 週間）で 5 つの組織へ次々と攻撃が仕掛けられていたり、4 分間で異なる 3 つの窓口に並行して「偵察メール」が送信されたりしたケースもあった。

2) 「偵察メール」に対して組織から回答を行った場合、攻撃者から 11 分～15 分など短時間で「ウイルス付きメール」が返信されてきていた。

3) 攻撃者から送付された添付ファイル（ウイルスを圧縮したファイル）が解凍できなかったため、組織より“開封できない”旨を回答したところ、13 分後に“使用している解凍ソフトをたずねる”攻撃者からの返信があった。（表 1　#4-4～#4-7）
その後、使用している解凍ソフトについて回答すると、51 分後に、そのソフトで解凍可能なファイルが再送されてきた。（表 1　#4-8、#4-9）

[*1] J-CSIP：Initiative for **C**yber **S**ecurity **I**nformation Sharing **P**artnership of **J**apan。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。
[*2] J-CSIP と同時期に、一般の組織・企業向けの「標的型サイバー攻撃　特別相談窓口」も運用を開始している。

（2）「やりとり型」攻撃の考察

1) 各組織が設けている外部向け窓口は、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ことを攻撃者は理解していると考えられる。

2) 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宛先は一組織あたり一ヶ所と少数に絞るなど、慎重に行動している。また、数ヵ月の期間をおいて、同じ組織へ攻撃を繰り返すこともある。

3) 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。

4) 攻撃者は日本語で会話し、話題に合った形で仕掛けをした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、攻撃を通して学習し、更に巧妙化することもある。

表１　ある「やり取り型」攻撃事例のメールの流れ

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。**

（3） J-CSIP の 2013 年度の運用状況

2013 年度は新たに 7 組織が参画し、全体で 5 業界 46 組織となりました。また、IPA は参加組織から 385 件（前年比 157%）の不審なメール等の情報提供を受け、180 件（前年比 113%）の情報共有を実施するなど、順調に運用を拡大しています。

一年間を通じた情報共有の統計結果から、次の傾向が見られました。

1) 標的型攻撃で用いられたウイルスの不正接続先（パソコンを遠隔操作するための指令サーバ等）の地域別割合において、**日本は 2012 年度は 7%であったが、2013 年度はその 4 倍の 28%を占めた。**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、**不正通信の「不審さ」に気付かれにくいよう、攻撃が悪質化した可能性がある**（図 1）。

2) 攻撃メールの添付ファイルとして、**2012 年度はマイクロソフト社の「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」や「ショートカット（LNK）ファイル」が観測され、**攻撃手口が次々と変化している**ことが分かった。

3) 攻撃メールの送信元は 86%がフリーメールを悪用しており、**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、攻撃を回避することができた状況であった**（図 2）。

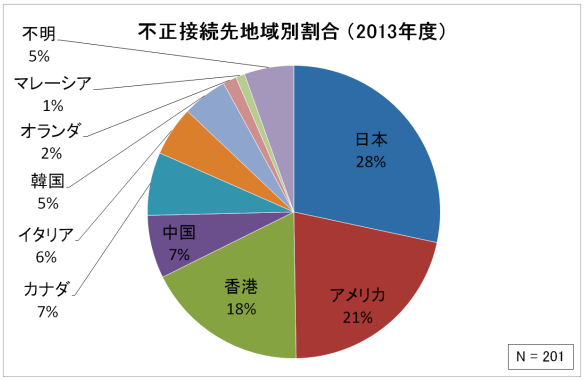

図 1

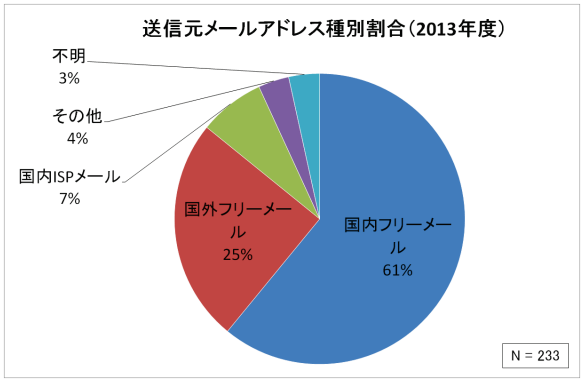

図 2

IPA は J-CSIP の活動を拡大し、標的型攻撃に関する情報の集約・分析とその共有を続け、国内の重要組織における防衛力の向上に取り組んでいきます。

■ 本件に関するお問い合わせ先
IPA 技術本部　セキュリティセンター　松坂／栗栖
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: isec-info@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部 広報グループ　横山／白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp