標的型メール攻撃の注意喚起

2016 年 7 月 20 日
東京電機大学シーサート
（TDU-CSIRT）

平素より情報セキュリティ対策にご協力を頂きまして、誠にありがとうございます。昨今、「標的型メール攻撃」の脅威が叫ばれているため、以下のとおり注意を喚起します。

覚えて欲しい３項目

A) 標的型メール攻撃は今も流行しており、あなたも危険です。
B) 標的型メール攻撃では、メールの添付ファイルを開かせるなどして不正プログラムに感染させ、あなたの PC を乗っ取ろうとします。
C) 標的型メール攻撃を防ぐためには、メール受信者が不審なメールをそれと見抜く必要があります。

実際に不審メールの添付ファイルを開いたら！

- 上司に報告するとともに、以下の組織に速やかに連絡してください。

TDU-CSIRT
E-Mail：tdu-csirt@csirt.dendai.ac.jp

不審に思ったメールを受信したら、メールごと削除するか、無視してください。安易に添付ファイルの開封、URL リンクのクリックを行わないようにしてください。

実際に不審なメールの添付ファイルを開いたり、URL リンクをクリックしてしまった場合は、上司に報告するとともに、TDU-CSIRT（E-Mail：tdu-csirt@csirt.dendai.ac.jp）に速やかに連絡してください。

(1) 標的型メール攻撃の背景

標的型メール攻撃については、国内では 2005 年頃より攻撃の発生が知られておりますが、実際の被害発生などによって更に広く報道されております。

標的型メール攻撃は「特定少数を狙う」・「換金可能な情報を狙う」もので、情報処理推進機構（以降 IPA と記載）から公開されている「2014 年度 情報セキュリティ 10 大脅威」(2014 年 3 月)[i]の中で 1 位となるなど、危険性が広く周知されてきています。狙われる情報は、一般には、クレジットカード番号・オンライン銀行のパスワードや、防衛・公安・産業上の機密情報などがあります。

(2) 標的型メール攻撃の手口

標的型メール攻撃では、特定少数のメール受信者に宛てて攻撃メールを送りつけるところから攻撃が始まります。攻撃メールには受信者の興味を惹く話題(時事問題や社内連絡を装うもの等)を巧みに利用して、添付ファイルを開くように誘導します。

受信者が添付ファイルを開くと、その添付ファイルに仕込まれたマルウェア(悪意のあるプログラム)が起動するケースや、添付ファイル中の埋め込まれたスクリプトコードに従い C&C サーバ※からマルウェアをダウンロードするケースにより、あなたの PC から様々な情報を盗むなどの悪事を働きます（感染①)。あるいは、マルウェアに感染した PC を攻撃基盤として、他の PC へと感染が広まることもあります（感染②、感染③)。

※ C&C サーバ（Command and Control server）：攻撃者の指令・命令を発行サーバ。

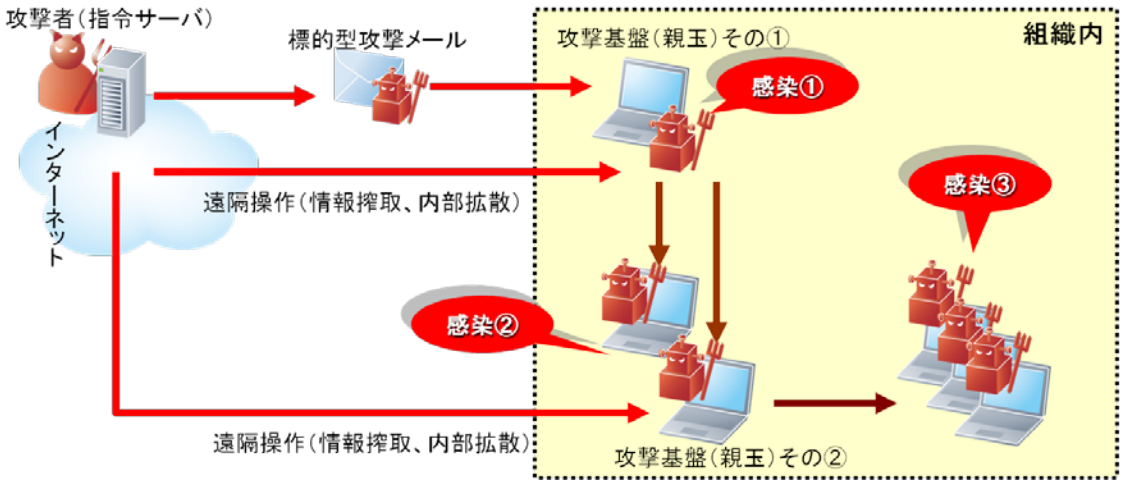

図 1　標的型メール攻撃の例

標的型メール攻撃においては、メールに添付されたファイルを開封、または本文中の URL をクリックすることで、マルウェアを外部ホームページからダウンロードして感染する傾向が多く確認されています。標的型攻撃に使用されるマルウェアはセキュリティ対策ソフトウェア等で検知されないものもあるため、ソフトウェアによる防御を過信しないことが必要です。

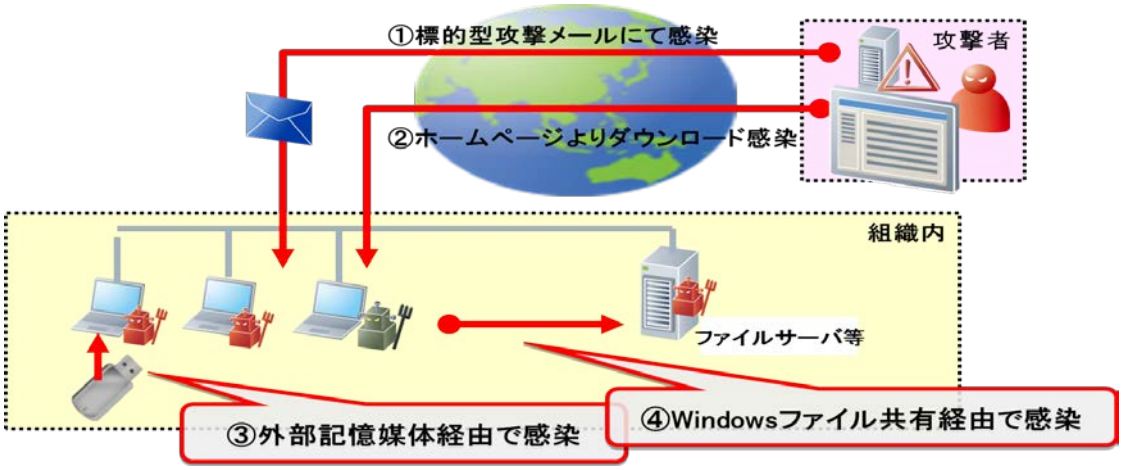

図２　マルウェアの感染経路

(3) 標的型メール攻撃の事例

一般に公開されている事例・調査としては、以下のものがあります。

IPA から公開されている「『標的型攻撃メールの分析』に関するレポート ～だましのテクニックの事例 4 件の紹介と標的型攻撃メールの分析・対策～[ii]」(2011 年 11 月)では、メール受信者をだますためのテクニックとして次の 4 パターンが紹介されています。

① ウェブ等で公表されている情報を加工して、メール本文や添付ファイルを作成した事例
② 組織内の業務連絡メールを加工して、メール本文や添付ファイルを作成した事例
③ 添付ファイルをつけずに、不正なサイトへのリンクをメール本文に記載した事例
④ 日常会話的なメールを数回繰り返して、メール受信者の警戒心を和らげた事例

IPA に届出・相談のあった標的型攻撃メールの主な事例および、最近国内で報道された標的型攻撃メールに関する代表的な報道を以下に記載します。

表 標的型攻撃メールの事例(IPA 資料、報道より抜粋)

2014/4[報道]	米国で、防衛および金融関係者を対象とする IE のゼロデイの脆弱性を悪用した標的型攻撃を確認。
2014/6[報道]	総務省、警視庁などが大手金融機関を騙るフィッシングサイトの増加について注意喚起。機密情報の窃取、不正送金の事例を確認。
2014/11[報道]	日本語文書作成ソフト「一太郎」の脆弱性を悪用してウイルスに感染させる手口が確認された。
2014/11[IPA]	「やり取り型」攻撃に対する注意喚起。 国内 5 組織で再び攻撃を確認したとして。
2014/11[報道]	国内企業宛に健康保険組合になりすまし、医療費通知を装った不審なメールが送られる。 メールに添付されたマルウェアは、Word ドキュメントを装った実行ファイル（exe）形式であった。
2015/4[報道]	国内の 2 社に対して、訃報を装った標的型攻撃メールが計数十通送られていた。

警察庁「サイバーインテリジェンスに係る最近の情勢（平成 24 上半期について)」(2012 年 8 月)[iii]によると、平成 24 年上半期の間に、我が国の民間企業等に合計約 552 件の標的型攻撃メールが送付されたとあります。

情報窃取を企図した標的型攻撃の事例として、中国地方のある事業者のネットワークが乗っ取られ、窃取した業務メールの内容を利用して添付ファイルにウイルスが仕込まれたメールを多数の企業に送付した事例が報告されています。

省庁や地方自治体に向けて、政府機関の職員を装った標的型攻撃メールが送付された事例も報告されました。

また、警察庁「平成 26 年中のサイバー空間をめぐる脅威の情勢について」(2015 年 3 月）[iv]によると、平成 26 年中に警察にて把握した標的型メール攻撃の件数が前年比約 3.5 倍の 1,723 件と大幅に攻撃件数が増加しています。平成 25 年に

は減少していた「ばらまき型」の件数が平成 26 年には再び増加しております。

攻撃メールの内容としては、英文による商品代金請求を装ったもの、健康保険組合からのメールを装ったもの、特定分野の研究会を装ったもの、などの標的型メール攻撃事例が報告されております。

(4) 標的型メール攻撃への対策

標的型メール攻撃の対策として、スパム対策や情報漏洩対策などの技術的な対策を着実に進めることも大変重要です。しかし、「特定少数を狙う」という標的型メール攻撃の性質上、技術的な対策だけで完全に被害を防ぐことは難しいと言わざるを得ない状況です。

そこで、「個々のメール受信者が不審なメールを見抜く」ことが重要となっています。攻撃者の技量やその他の状況で変化はありますが、下のリストに掲げる特徴に合致するメールは標的型メール攻撃である可能性があります。(もちろん、標的型メール攻撃ではなく通常のメールである可能性もあるため判断が難しく、対策を困難にしているところでもあります。)

IPA から公開されている「標的型攻撃メールの例と見分け方」(2015 年 1 月)[v] では、標的型攻撃メールの着眼点としても紹介されています。

不審なメールの特徴

- 差出人を信頼性の高い組織(官公庁、取引先企業、社内)に偽装している。
- 組織内の話題なのに、外部のメールアドレスから届いている。
- 受信者の興味を引く内容(社会的な事件、災害など)を装っている
- 添付ファイルまたは本文中の URL をクリックするように巧妙に誘導する本文となっている。
- 「緊急」などと急がせて、メールの内容を吟味させまいとしている。
- 差出人の署名や名乗りが無いか、曖昧である。
- 差出人の名前や組織名として、架空のものを名乗っている。
- ファイル名が文字化けしている、不自然な日本語である。
- 日本語では使用されない漢字が使われている。
- 業務に関連がありそうな内容を偽装している。
- 添付ファイルの拡張子が偽装されている。
- 表示されている URL と実際のリンク先の URL が異なる。
- 心当たりの無い決済や配送通知が届く。
- ID やパスワードなどの入力を要求するメールである。

標的型メール攻撃は特徴にあるようなポイントを組み合わせることで、巧妙に細工されている場合があり、メールを完全に見抜くことは困難です。しかしメールを処理するときに、以下のように不審なメールの特徴の有無を確認することで、不審なメールを見抜くことができる可能性が高まります。

不審なメールを見分けるポイントの例

- 差出人に心当たりがあるか。
- 組織内の連絡なのに、外部ドメインやフリーメールのアドレスから届いていないか。
- 受信者が興味を持つ内容を騙り、添付ファイルを開かせようとしていないか。
- 差出人の署名がない、名乗りが無いか曖昧ではないか。
- 添付ファイルの拡張子が偽装されていないか。

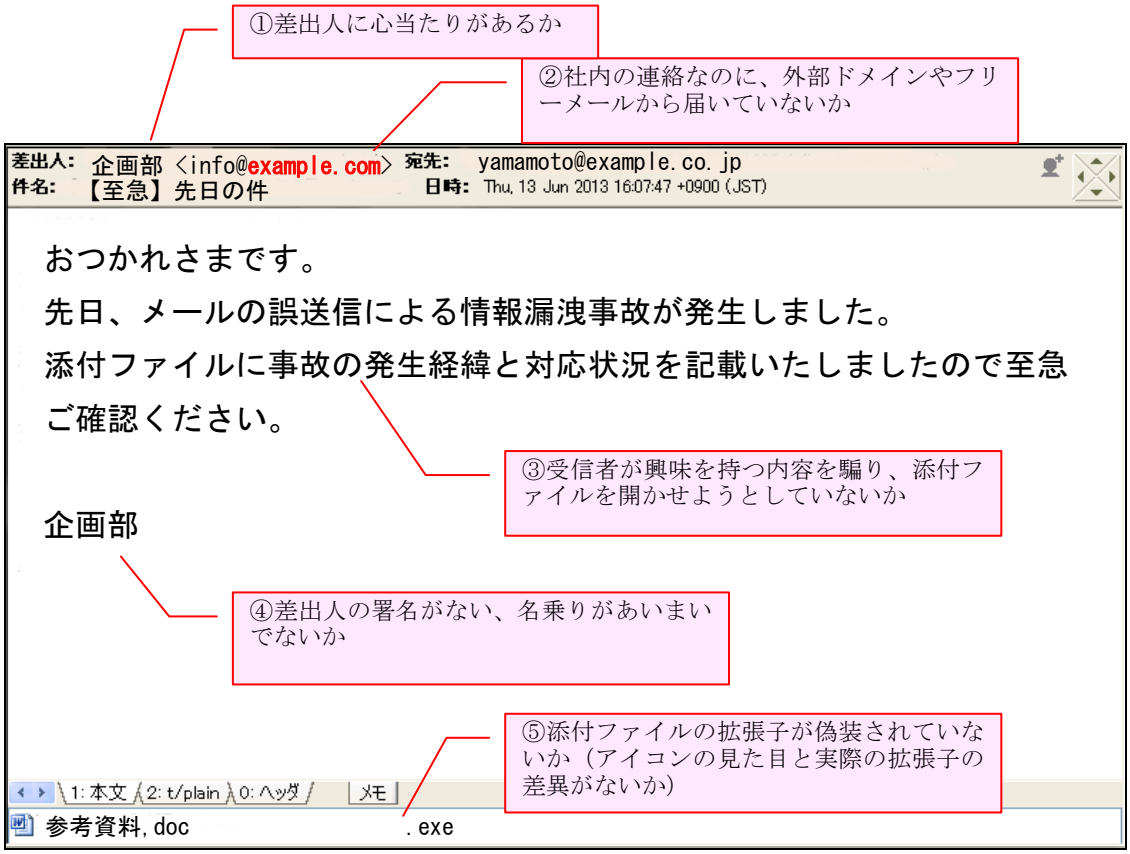

図３　標的型攻撃メールとチェック項目の例

図３に示すように、特に差出人の情報（名前やメールアドレス）をよく確認するなど、今まで以上に注意をしていただきますようお願いいたします。

---

i 2014 年版 情報セキュリティ 10 大脅威. (2014 年 3 月 31 日).

参照先: http://www.ipa.go.jp/security/vuln/10threats2014.html

ii 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. (2011 年 11 月 3 日).

参照先: http://www.ipa.go.jp/about/technicalwatch/20111003.html

iii 警察庁「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）について」. (2012 年 8 月 23 日).

参照先: http://www.npa.go.jp/keibi/index.htm

iv 警察庁「平成 26 年中のサイバー空間をめぐる脅威の情勢について」. (2015 年 3 月 12 日).

参照先: http://www.npa.go.jp/pressrelease/2015/03/20150312_03.html

v 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」. (2015 年 1 月 9 日).

参照先: http://www.ipa.go.jp/security/technicalwatch/20150109.html