IPA Technical Watch

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

～だましのテクニック事例4件の紹介と標的型攻撃メールの分析・対策～

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

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

～だましのテクニック事例 4 件の紹介と標的型攻撃メールの分析・対策～

目次

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

～だましのテクニック事例 4 件の紹介と標的型攻撃メールの分析・対策～

2011年10月3日
IPA（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

1. はじめに

インターネットの普及に伴い、葉書や封書のような紙による情報の伝達手段が、電子メールにおき替わってきている。ビジネスにおける取引先や社内との連絡だけでなく、ダイレクトメールと呼ばれる広告の媒体としても電子メールが活用されるようになり、知らない組織から電子メールが届くことも多くなった。

こうした中で、コンピュータウイルスと呼ばれる不正なプログラムを他人のコンピュータに感染させて情報を盗んだり、業務を妨害したりする悪意のある人たちも、攻撃手法のひとつとして電子メールを利用している。

電子メールを利用して他人のコンピュータにウイルスを感染させる、いわゆるウイルスメール攻撃は、当初は不特定多数にウイルスを感染させる手段として使われており、添付の実行形式ファイルを開かせるという形態がとられていた。

ウイルスメール対策としては、市販のウイルス対策ソフトを導入し、Windows Updateをきちんと実施し、不審なメールは開かないという対応で、ほとんど被害に遭うことはなかった。

ところが、特定の相手を狙い、送信者の詐称やタイトル、本文、添付ファイル名等の巧妙な記述内容によって、添付ファイルを開かせたり記載URLをクリックさせる「標的型攻撃メール」が出現してきた。

2005年10月に、ある実在の官公庁職員を詐称して複数の官公庁職員宛てに送られたウイルスメールが確認されて以来、標的型攻撃メールが徐々に増え、大きな脅威となってきている。最近では、2011年3月に発生した東日本大震災や福島原子力発電所の事故を題材としたウイルスメールが多数確認されている。

また、その添付ファイルとして、PDFファイルやMS Word、Excel、一太郎のような業務でよく利用するアプリケーションで作成した文書データファイルにウイルスを埋め込んだ例が増えており、ウイルス対策ソフトでも検知されないという事例も多く報告されている。

昨今、企業の機密情報や個人情報が窃取される不正アクセス被害が多発しているが、その攻撃手段として、標的型攻撃メールが利用されているという事例も確認されている。

このような状況に対して、IPAは、2008年9月に「不審メール110番」という相談窓口を設置し、標的型攻撃メールに関する相談に応じるとともに、国内における標的型攻撃メールの検体を収集して、その特徴を分析し、啓発活動を行ってきた。

また、ウイルス対策ソフトを開発・販売している企業や、情報セキュリティサービスを提供している情報セキュリティオペレーション事業者と連携し、標的型攻撃メールの被害を少なくするための活動を行っている。

本レポートでは、標的型攻撃メールにおいてメール受信者をだますためにどのようなテクニックが使われているか、標的型攻撃メールの被害に遭わないためにどのような対策をする必要があるか、万一不審なメールを受け取った場合どのように対応したらよいかを、一般の方にも分かりやすく説明している。

2．ウイルスメールについて

電子メールを永く利用していると、仕事のメールや個人的な知人からのメールの他に、欲しくもない広告メールや、利用したことのないサービスに対する利用料の請求メール、英語や中国語など外国語で何が書いてあるか判らないメールなど、色々なメールが届くようになる。

それらのメールの中には、コンピュータにウイルスを感染させようとする、いわゆる「ウイルスメール」も混ざっている。

ウイルスメールには、不特定多数にウイルスメールを送り、メールの添付ファイルを開くことによりコンピュータウイルスに感染したパソコンから更にウイルスメールを送ることで感染を拡大する、「マスメール型ウイルスメール」と、情報窃取を目的として特定の組織だけに送られる、「標的型攻撃メール」と呼ばれるウイルスメールがある。

図 1 は、経済産業省の告示[1]に基づき、IPA に報告された国内のウイルス届出件数の推移である。2005 年をピークに、ウイルス届出件数は、減ってきているが、以下で述べるように、ウイルスを蔓延させるウイルスメールの目的と手段が異なってきているためであり、情報窃取などの深刻な脅威は逆に増大していると考えるべきである。

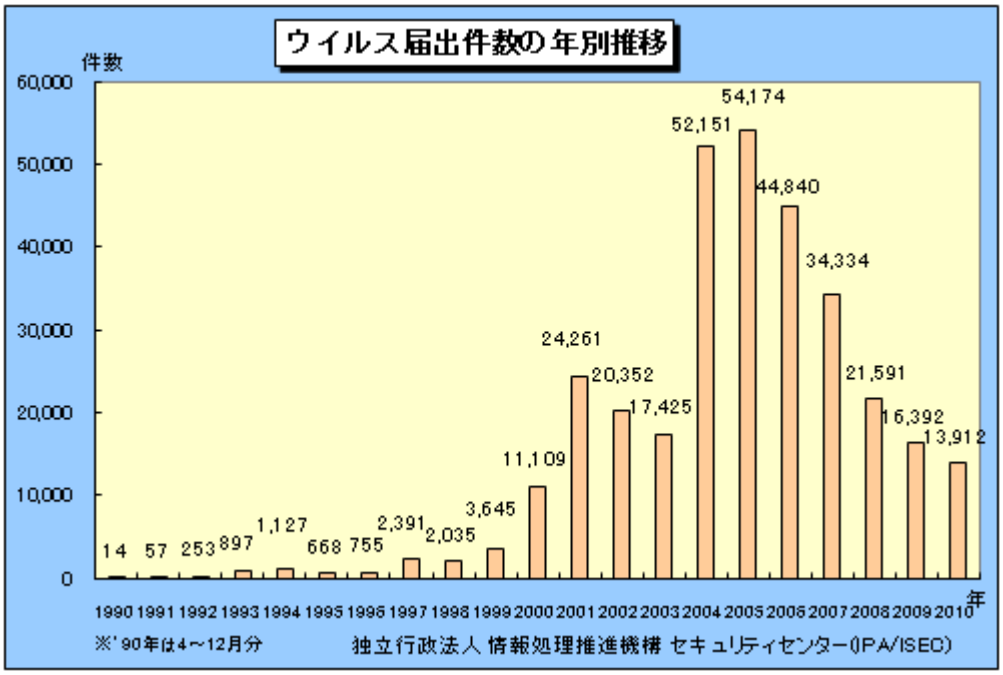


図 1．ウイルス届出件数の年別推移

[1] コンピュータウイルス対策基準（通商産業省告示第 139 号 平成 2 年 4 月 10 日制定）

(1) マスメール型ウイルスメール

1999 年に電子メールの添付ファイルによって感染するウイルス Melissa（メリッサ）が出現後、次々とウイルスメールが作られ、届出件数のほとんどをウイルスメールの検知件数が占めている。

特に、2004 年に出現したマスメール型ウイルス Mydoom（マイドゥーム）や Netsky（ネットスカイ）等によって、届出件数は 2004 年、2005 年と急伸し、現在でも届出件数の上位を占めている。図 2 に、最近のウイルス種別毎の届出件数を示す。

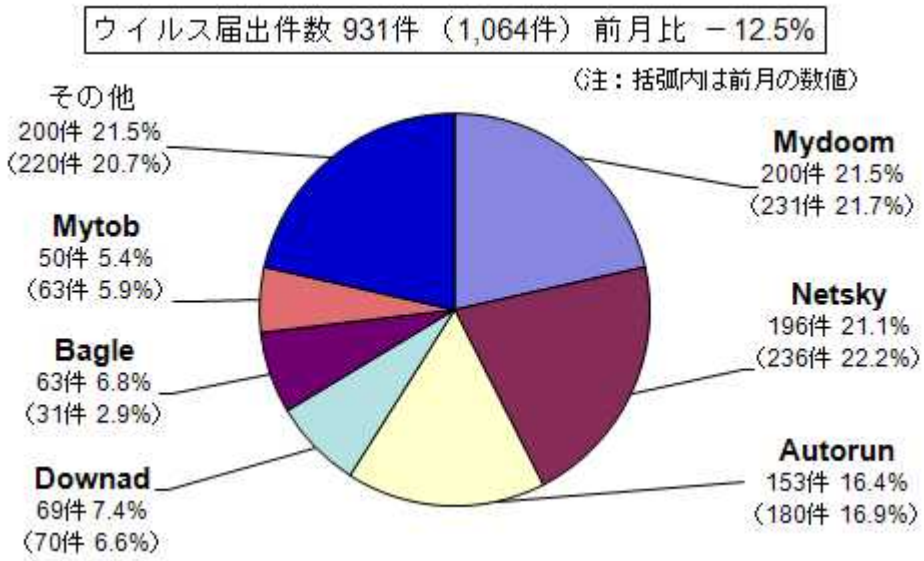


図 2．ウイルス届出件数（2011 年 8 月度）

多くのマスメール型のウイルスメールは、感染したコンピュータ上に記録されているアドレス帳やメール、ウェブの閲覧記録などからメールアドレスを収集し、そのアドレス宛てに自身をメール送信するため、ねずみ算的にウイルスメールが拡散することになる。

ウイルスメールの脅威の増大に伴い、ウイルスの被害に遭わないための対策として、ウイルス対策ソフトの導入や、Windows Update に代表されるオペレーティングシステムの脆弱性対策が定着してきている。

(2) 標的型攻撃メール

特定の相手を狙い、送信者の詐称やタイトルや本文の巧妙な記述内容によって、添付ファイルを開かせたり記載 URL をクリックさせる「標的型攻撃メール」が出現してきた。

2005 年 10 月に、ある実在の官公庁職員を詐称して複数の官公庁職員宛てに送られた標的型攻撃メールが確認されて以来、標的型攻撃メールが徐々に増え、大きな脅威となってきている。最近では、2011 年 3 月に発生した東日本大震災や福島原子力発電所の事故を題材とした標的型攻撃メールが多数確認されている。

また、その添付ファイルとして、PDF ファイルや MS Word、Excel、一太郎のような業務でよく利用するアプリケーションで作成した文書データファイルにウイルスを埋め込んだ事例が増えており、ウイルス対策ソフトでも検知されないという事例も多く見受けられる。

昨今、企業の機密情報や個人情報が窃取される不正アクセス被害が多発しているが、その攻撃手段として、標的型攻撃メールが利用されているという事例も確認されている。

表 1 は、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と、IPA に届出・相談のあった標的型攻撃メールの主な事例を示している。

表 1．標的型攻撃メールの事例（報道、届出・相談など）

2005/10 [報道]	**実在の外務省職員を詐称**して**ウイルスを埋め込んだ MS Word ファイル**が添付された標的型攻撃メールが複数の**官公庁に届いた**。
2006/5 [届出]	官公庁を詐称してウイルスを埋め込んだ MS Word ファイルが添付された標的型攻撃メールが**民間大手企業に届いた**。
2006/5[届出]	**新聞社を詐称**してウイルスを埋め込んだ MS Word ファイルが添付された標的型攻撃メールが民間大手企業に届いた。
2006/8 [届出]	**ウイルスを埋め込んだ一太郎ファイル**が添付された標的型攻撃メールが届いた。
2006/10[届出]	**実行形式のウイルス**が添付された標的型攻撃メールが届いた。
2007/4[報道]	一太郎の**未修正の脆弱性を悪用**したウイルスメールが届いた。(**ゼロデイ攻撃**)
2007/6[報道]	**日本語環境の圧縮解凍ソフトの未修正の脆弱性**を悪用したウイルスメールが届いた。(ゼロデイ攻撃)
2007/9[報道]	**首相をかたる**標的型攻撃メールが届いた。
2007/10[報道]	ウイルスを埋め込んだ **PDF ファイル**が添付された標的型攻撃メールが届いた。
2008/4 [相談]	**政府関係機関（IPA）を詐称して**ウイルスを埋め込んだ PDF ファイルが添付された標的型攻撃メールが官公庁に届いた。
2008/11[届出]	**標的型攻撃メールに関する組織内の注意喚起メールを加工して、多数の従業員に**標的型攻撃メールが届いた。
2009/5[届出]	**新型インフルエンザ関連情報に見せかけた**標的型攻撃メールが届いた。
2009/7[届出]	**添付ファイルがついていない**標的型攻撃メールが届いた。
2010/12[報道]	**有名アーティストのマネージャ宛てに送られた**標的型攻撃メールによっ

	て未公開楽曲が窃取された。
2011/3[報道]	**RSA の SecureID の情報窃取**は標的型攻撃メールによって行われた。
2011/3-4[届出]	**東日本大震災や福島原発事故関連情報に見せかけた**標的型攻撃メールが多数届いた。
2011/7[届出]	**おれおれ詐欺を模倣した**標的型攻撃メールによって情報流出した。
2011/9[報道]	マイクロソフトの**ヘルプファイルを使う標的型攻撃メール**が発見された。
2011/9[届出]	ネットバンキングの ID とパスワード情報を盗む**ウイルスが付いたフィッシングメール**が届いた。
2011/9[報道]	**防衛関連企業の複数箇所の拠点で、数十台のパソコンやサーバ**にウイルスが感染していた。標的型攻撃メールの可能性がある。
2011/9[報道]	**Mac OSX を標的として**ウイルスが埋め込まれた PDF ファイルのウイルスが確認された。

3．標的型攻撃メールの特徴

不特定多数に送られて次々と感染拡大するマスメール型ウイルスメールと標的型攻撃メールの比較を表 2 に示す。全てがこのように区分できるわけではないが、大枠の特徴と傾向を表している。

表 2.　マスメール型ウイルスメールと標的型攻撃メールの比較

特徴の比較（傾向）	攻撃者の目的	感染数	検体収集	言語	件名	本文	送信者	添付ファイル	感染後のPCの症状
マスメール型ウイルスメール	・社会騒乱 ・多数のPCを操りたい	多い	容易	主に英語	一般的な用件	・一般 ・勧誘 ・指示：添付ファイルを開封等	・個人名 ・不明組織	実行形式	・重い ・PCダウン
標的型攻撃メール	・特定の組織の情報窃取 ・システムの妨害	**少ない**	**困難**	**日本語**	**自分に関係ありそうな用件**	**・関心事 ・用件の説明が適切**	**(詐称) ・官公庁 ・大企業**	**文書形式**	**特に変わらず**

標的型攻撃メールの目的は、特定の組織の情報を窃取することなので、無関係な組織に送られる可能性は低い。

ウイルス対策ソフトの多くは、世の中に発現しているウイルスを収集し、そのウイルスの情報を登録することで、ウイルスを検知しており、裏を返すと、ウイルス情報を登録するまでは、ウイルスを検知することが困難である。

従って、ウイルス対策ソフトを開発・販売している情報セキュリティ企業がウイルス検体を入手するチャンスの少ない標的型攻撃メールの場合、ウイルス対策ソフトで検知できる可能性は低いことになる。

ウイルス対策ソフトで検知できなくても、メール受信者が、そのメールを不審に思い、添付ファイルを開かなければ、ウイルスに感染する可能性はほとんどない。

しかしながら、信頼できそうな組織から、自分に関係ありそうな表題や内容の日本語のメールが送られており、添付ファイルも文書ファイルなので、ウイルスメールと気付かずに開いてしまう可能性が高くなる。

しかも、添付ファイルを開いてウイルスに感染しても、パソコン等に特に異常な症状が現れないケースが多く、感染に気付かずに使い続け、長期間に渡ってウイルスが活動し、組織内の他のパソコンやサーバ等に感染を拡大したり、情報窃取等の被害を及ぼすことになる。

4. メール受信者をだますテクニック

標的型攻撃メールは、メール受信者をだます色々なテクニック（ソーシャルエンジニアリング）を駆使している。

どのようなだましのテクニックが使われているかを、実際の事例で紹介する。ただし、だましのテクニックを紹介して啓発すると新たなだましのテクニックを使うという攻撃側と防御側のいたちごっこの面はあるが、つけいる手口の本質は変わらないので、6 章の対策と併せて従業員教育の参考にしてください。

4.1. ウェブ等で公表されている情報を加工して使用した事例

標的型攻撃メールの特徴として、**『ウェブ等で公開されている情報をメール本文にコピーしたり、ウェブに掲載された PDF の報告書を加工してウイルスを埋め込んだりする』**事例が多い。

図 3 は、2008 年 4 月に、IPA をかたって政府関係組織に送られたメールである。

メール本文や PDF ファイルは、2008 年 3 月に IPA のウェブに公開した報告書のプレスリリースの情報を利用しているため、メール受信者をだます次の条件を満たしている。

① メールの受信者が興味を持つと思われる件名
② 送信者のメールアドレスが信頼できそうな組織のアドレス
③ 件名に関わる本文
④ 本文の内容に合った添付ファイル名
⑤ 添付ファイルがワープロ文書や PDF ファイルなど
⑥ ②に対応した組織名や個人名などを含む署名

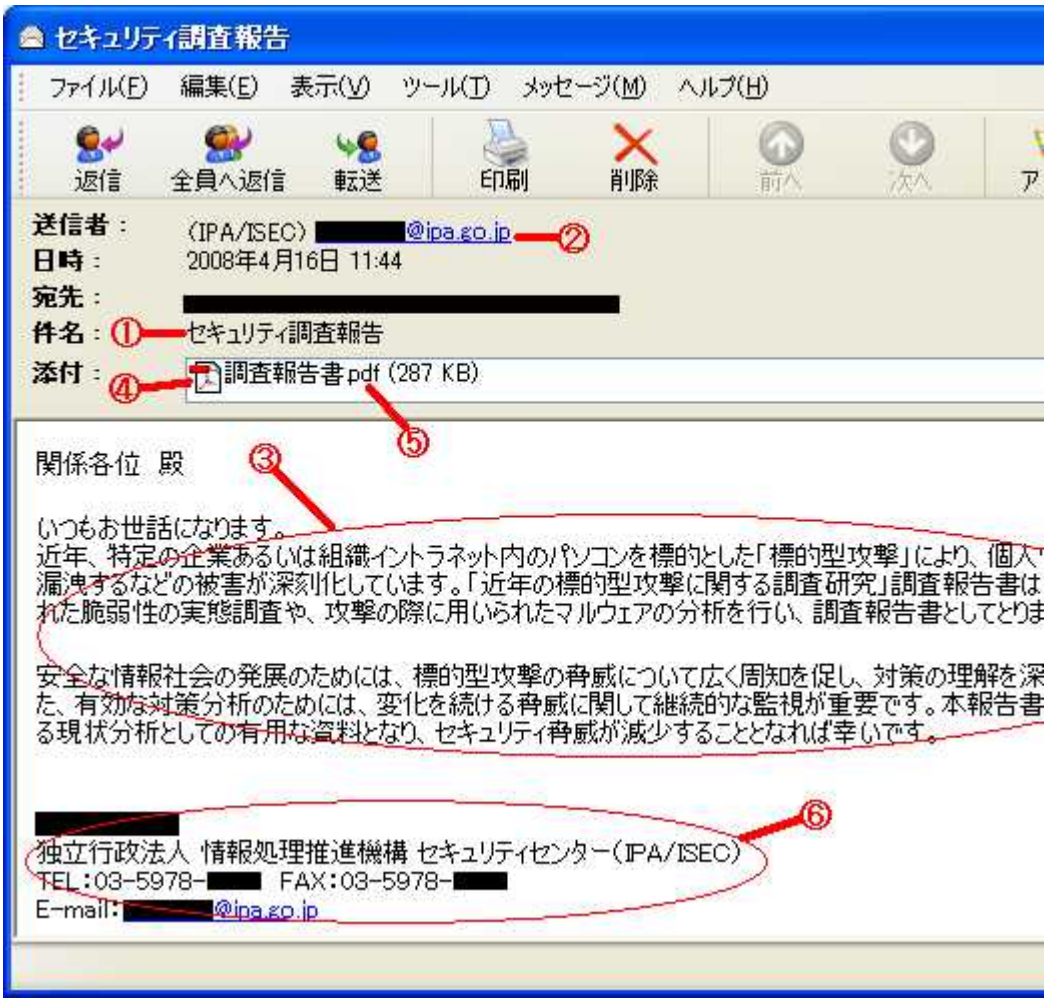


図 3．2008 年 4 月 16 日に、IPA をかたって政府関係組織に送られたメール例

このメールの受信者が IPA のことをよく知っていれば、有用な情報を送ってくれたと勘違いしてメールの添付ファイルを開いてしまうかもしれない。

あるいは、IPA のことを余り知らない人でも、ウェブ検索で IPA を確認すると、セキュリティ対策を推進している政府関係組織なので、正しいメールと信用してしまう可能性も高い。

しかしながら、冷静に考えると、今まで IPA からこのような情報を直接メールで送ってきたことはなかったことに気づくはずである。

このように標的型攻撃メールは、『**一見正しいメールの特徴をもつが、普段メールをやりとりしていない人から届き、なぜ自分宛てに送ってきたか心当たりがない**』場合が多い。

つまり、添付ファイル付きのメールを送ってきた理由がわからない場合には、送信者に電話等で問い合わせることで、正規のメールかどうかを判断することが必要となる。

このメールに添付されていた PDF ファイルは、2008 年 2 月 7 日に修正プログラムが提供されていた Adobe Reader と Acrobat の脆弱性を悪用していたので、最新版の Adobe Reader や Acrobat を使用していればウイルス感染の被害には遭わないで済む。

4.2. 組織内の業務連絡メールを加工して使用した事例

2008 年 11 月に、組織内の業務連絡メールを加工してウイルス付きの PDF ファイルを添付した標的型攻撃メールに関する届出があった。その攻撃のフローは以下のとおりである。

① 最初に、官公庁や公的機関を詐称して、実行形式のウイルスを添付した標的型攻撃メールが 2 通届いた。

② 不審なメールと判断した受信者はメールの添付ファイルを開かず、被害に遭わなかった。

③ 管理部門が添付ファイルを調べると、キーロガー機能を持つウイルス[2]と判明した。

④ 管理部門より、①の標的型攻撃メールに関する注意喚起をテキスト本文のみのメールで、海外拠点を含めた幹部職員約 150 名に送った。

⑤ 約 2 時間後に、④の注意喚起メールを加工して、ウイルスを埋め込んだ PDF ファイルを添付した標的型攻撃メールが同じ 150 名に届いた。

⑥ 正規の注意喚起メールと信じた約 10 名の受信者が添付ファイルを開いてしまった。

初めの 2 通の標的型攻撃メールに対しては、標的型攻撃メールの見分け方のひとつである、『**一見正しいメールの特徴をもつが、普段メールをやりとりしていない人から届き、なぜ自分宛てに送ってきたか心当たりがない不審なメールに注意する**』という対策で被害を回避できたが、⑤の標的型攻撃メールの場合、社内で注意喚起を発信する正規の部門名、担当者名を詐称し、メールタイトルや本文も正規の注意喚起を元にしているので不審な点は全くなく、添付ファイル開いてしまう可能性は非常に高くなる。

この事例では、組織内に限定した業務連絡メールを加工していることから、少なくとも 1 人以上の職員のメールがすでに窃取されていたと考えられる。標的型メール攻撃は、数カ月から数年続いている場合が多く、このインシデント以前に、すでに標的型攻撃メールの被害に遭っていた職員がいた可能性がある。

---

[2] キーボードの操作を記録することで、ID やパスワードなどの情報を窃取するウイルス。

⑤のメールに添付されていたPDFファイルは、2008年2月7日に修正プログラムが提供されていたAdobe ReaderとAcrobat の脆弱性を悪用していたので、最新版のAdobe Reader やAcrobat を使用していればウイルス感染の被害には遭わないで済む。

4.3. 添付ファイルのないウイルスメールの事例

ほとんどの標的型攻撃メールには、実行形式ファイルやPDFファイル、MS Wordなどの添付ファイルがついているが、添付ファイルがついていなければ安全という訳ではない。

図4は、2009年7月に、IPAをかたって民間企業と官公庁に送られたメールである。

メール本文はHTMLで記述されており、①の部分に、不正な仕掛けをしたサイトへのリンクが記述されている。

メールソフトによっては、マウスカーソルをリンクされた箇所に乗せることによって、②のように、リンク先が表示されることがあるが、明らかにIPAと無関係なサイトのURLにリンクされている。

メールタイトルや本文の内容は、IPAが2009年6月にウェブに公開した情報をコピーしており、一見して正しいメールのように見える。

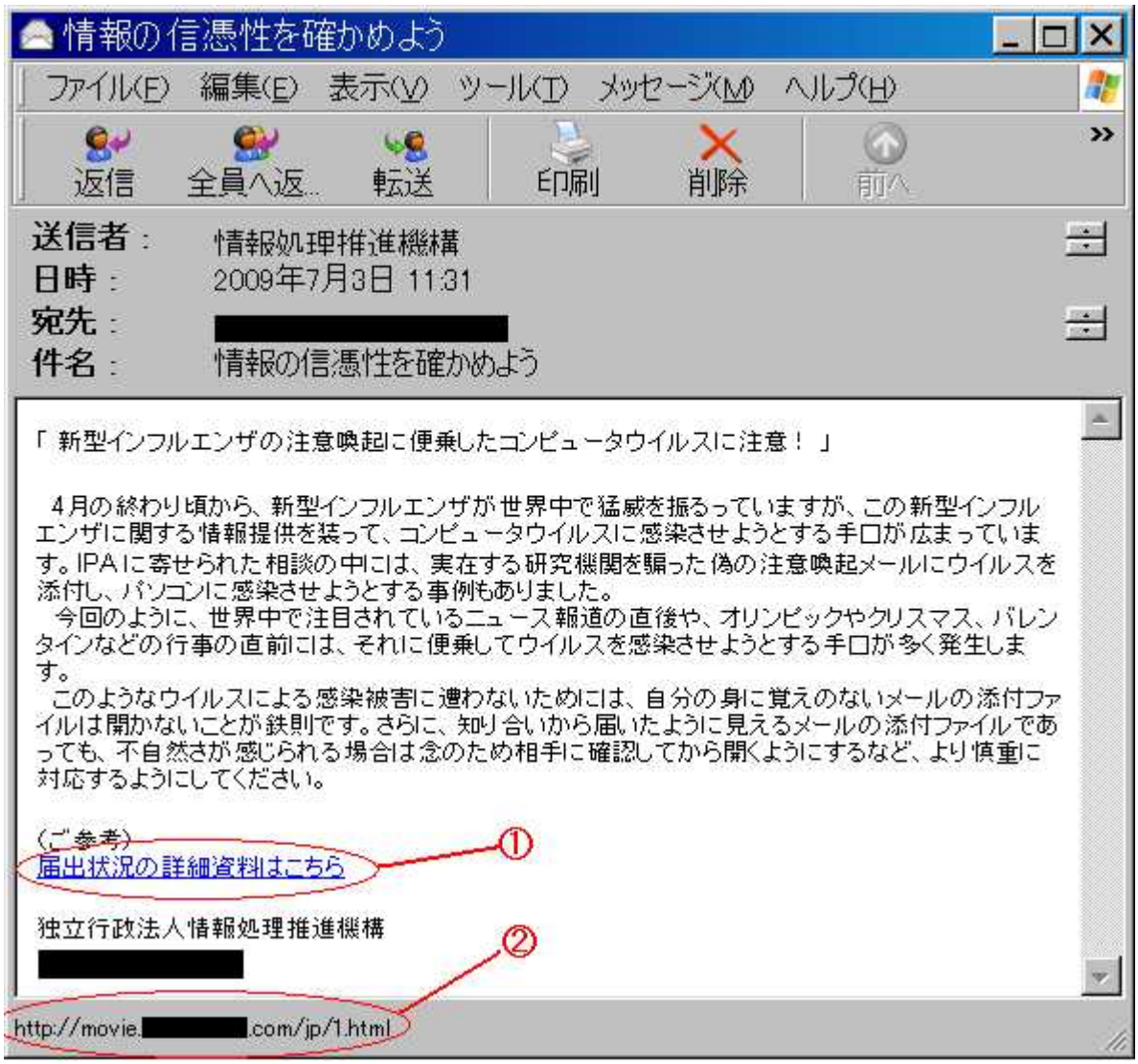


図 4．2009 年 7 月 3 日に、IPA をかたって民間企業に送られたメール例

リンク先のサイトには、2009 年 2 月 11 日に修正プログラムが提供されていた Internet Explorer の脆弱性を悪用して、ウェブサイトから不正なプログラムを自動的にダウンロードさせる仕掛けがされていた。

ウェブを参照しただけで不正なプログラムをパソコンに入れられるドライブ バイ ダウンロード攻撃は、「ガンブラー」でも使われている攻撃手法であり、標的型攻撃メールに限らず、マスメール型ウイルスメールでも使われている。

つまり、標的型攻撃メールといえども、攻撃手法は、他のサイバー攻撃で使用されている新しいテクニックをどんどん取り入れているということである。

標的型攻撃メールの見分け方のひとつである、『**添付ファイルが付いた不審なメールに注意する**』という対策を回避しようとした可能性がある。

メール本文に、不正なプログラムに感染させるウェブサイトへの誘導を記載するには、HTML メールではなく、テキストメールでも可能であるが、図 5 の例①のように、不正なサイトの

URL がそのまま見えてしまうので、異常に気付く可能性が高くなる。従って攻撃者は②③④のような HTML メールで送る場合が多いと推察する。

多くの企業が、『**HTML メールを取り扱わないポリシーで運用**』しているのは、このような背景がある。

① テキストメールで送信者のドメインと異なる URL が見える例

② HTML メールで、表示の URL では IPA の正規のサイトのように見えるが、実際には、①のような無関係なサイトへのリンクとなっている例

③ 、④ HTML メールで、具体的な URL を見せない例

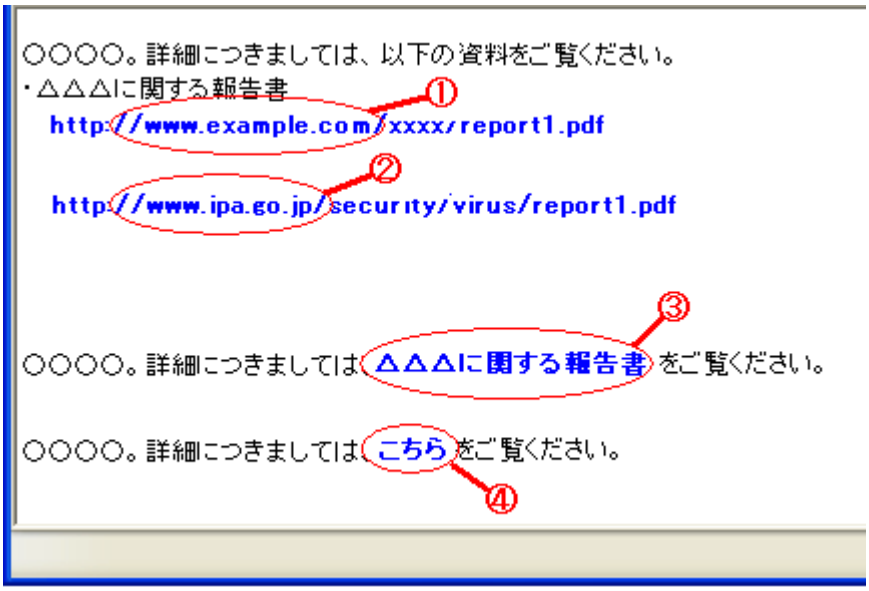


図 5．メール本文の中で、ウイルスに感染する仕掛けをしたウェブサイトに誘導する例

4.4. おれおれ詐欺を模倣した標的型攻撃メールの事例

2011 年 7 月に、おれおれ詐欺を模倣した標的型攻撃メールに関する届出があった。

最初、テキスト本文のみの日常会話的なメールが何回かやりとりされ、最後にウイルス付きの PDF ファイルが添付されたメールが届き、その PDF ファイルを開くことにより、ウイルスに感染したという事例である。

メールのやりとりは以下のようなフローであった。

① ある日、○○さん今どこに居ますかという内容のメールが届いた。

② メールの送信者に心当たりがないので、誰ですかという内容のメールを返信した。

③ すると、去年食事をしましたという内容のメールが届いた。

④ 打ち合わせ中ですという内容のメールを返信した。

⑤　後で連絡するという内容のメールが届いた。

⑥　翌朝、今忙しいですかという内容のメールが届いた。

⑦　今なら大丈夫ですという内容のメールを返信した。

⑧　再度、去年食事をしましたという内容のメールが届いた。

⑨　いつのことですかという内容のメールを返信した。

⑩　去年の○月で、一緒の時の写真を送るという内容のメールに、PDF ファイルが添付されていた。

⑪　添付ファイルを開いても写真が見えないという内容のメールを返信した。

⑫　出張なので後で連絡するという内容のメールが届き、以後メールは途絶えた。

標的型攻撃メールの見分け方のひとつである、『**心当たりの無い人からのメール**』ではあるが、最初は添付ファイルもなく、不審な URL リンクもなく、知人とするような『**日常会話的なメールのやりとりを数回繰り返すことで、メール受信者の警戒心を和らげ**』、最後に文書データファイルを開くように誘導するという新しいだましのテクニックである。

このメールに添付されていた PDF ファイルは、2011 年 4 月 15 日と 4 月 21 日に修正プログラムが提供されていた Adobe Flash Player と Adobe Reader、Acrobat の脆弱性を悪用していたので、最新版の Adobe Flash Player、Adobe Reader 及び Acrobat を使用していればウイルス感染の被害には遭わないで済む。

5．IPA に届けられた標的型攻撃メールの分析

2008 年 4 月から 2011 年 6 月までに IPA に届けられた標的型攻撃メールの分析結果を以下に示す。

(1) 標的型攻撃メールの送信先

標的型攻撃メールの標的となっている組織の内訳を図 6 に示すが、民間企業が約 1/3、独立行政法人が 1/4 となっている。官公庁が少ないが、官公庁の場合、NISC(内閣官房情報セキュリティセンター)が情報を集約しているため、IPA に相談や届出が来ないので実態を表していないと考えられる。

組織のメールアドレスではなく、プライベートなメールアドレスに届くのは、その個人が関係している組織の情報を狙っている可能性が考えられる。例えば、報道によると、レディー・ガガの未公開の楽曲を盗んだ犯人は、レディー・ガガのマネージャのプライベートなメールアドレスに標的型攻撃メールを送ったとのことである。

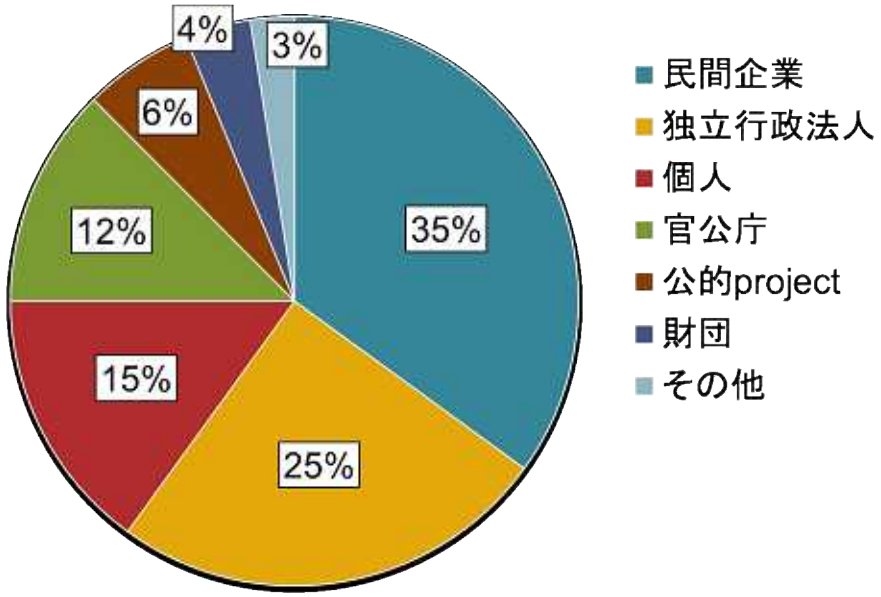


図 6．標的型攻撃メール送信先の主体の属性

(2) 標的型攻撃メールが詐称する送信元

メール受信者を信用させるために詐称するメール送信者の所属の内訳を図 7 に示すが、官公庁が約半分を占めている。2 番目に多い独立行政法人と合わせると約 2/3 が政府関係機関を詐称している。これは、政府関係機関を名乗ることで、メール受信者に安心感を持たせたり、重要な情報であると思わせることで、添付ファイルの開封行為の誘導や記載内容を信用させることを狙っていると推察される。

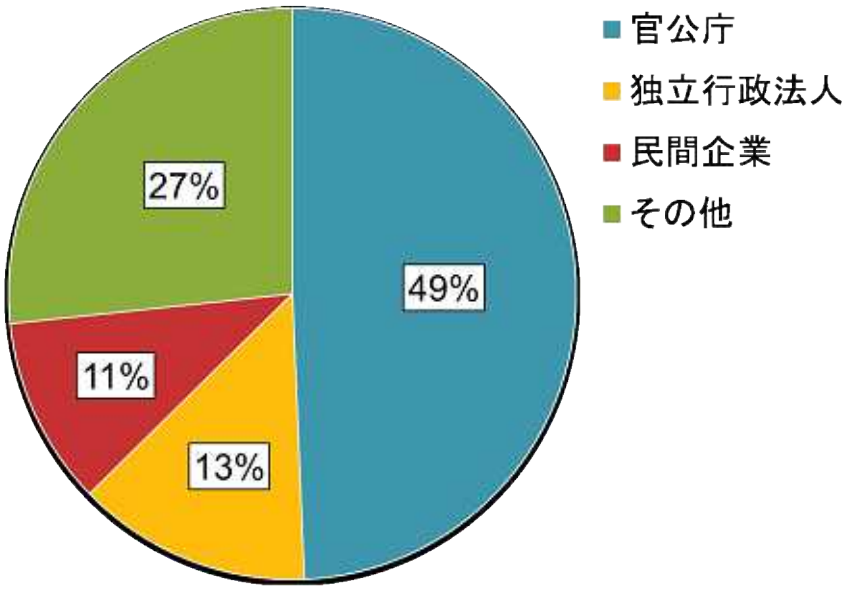


図 7．標的型攻撃メール送信者のかたる主体の属性

(3) 標的型攻撃メールの記載内容の傾向

標的型攻撃メールの記載内容を、テーマ（主題）、分野、情報レベルの３つの分類軸で傾向分析した結果を表 3-1、表 3-2、表 3-3 に示す。

表 3-1 に示す、テーマによる分類では、メール受信者が関係する、または興味を持ちそうな仕事関係のテーマが多い。「イベント」「報告書」「ニュース・注意喚起」で分類してみたが、特に目立った傾向はなかった。

表 3-2 に示す、分野による分類では、「国際」と「社会」を合わせて 7 割以上を占め、マスメール型ウイルスでよく取り上げられる「芸能」分野のメールは 0 件である。

表 3-3 に示す、情報レベルによる分類では、「組織内限定情報」「関係者限定情報」「一般公開情報」に分類したが、「関係者限定情報」に区分されるものが過半数であり、組織内でしか通用しないテーマは少ない。

これらから総じて言えることは、関心度の高いテーマ、重要な情報、特定の人に限定された情報などを装って、標的型攻撃メールが発信されていることが判る。

表 3-1．テーマによる分類

分類	割合	テーマ事例(抽象化済)
イベント	３８％	国際会議、シンポジウム、研修会、選挙、 法令改正、VIP会合日程、役員人事異動、 来訪者情報、社内ウイルス調査
報告書	３２％	外交機密文書、国際情勢、海外資源、 政府部局報告書、情報セキュリティ調査、 ウイルス・不正アクセス届出状況、 会議資料
ニュース ・ 注意喚起	３０％	東日本震災、金融情勢、国際情勢、外交情報、 政府予算、製品事故、情報セキュリティ注意喚起、 新型インフルエンザ

表 3-2．分野による分類

分類	割合	テーマ事例(抽象化済)
国際	３９％	VIP会合日程、外交機密文書、国際情勢、 国際会議、海外資源
社会	３３％	東日本震災、政府予算、新型インフルエンザ、 製品事故、情報流出事故、 情報セキュリティ注意喚起、 情報セキュリティ調査
政治	１５％	選挙、法改正、政府公表資料
経済	８％	金融情勢、経済関連法改定、経済外交、 経済成長戦略
国内	５％	法人実態調査、高官日程
芸能	０％	

表 3-3．情報レベルによる分類

分類	割合	テーマ事例(抽象化済)
関係者 限定情報	５３％	選挙、演説原稿、法令改定、外交情報、 法人実態調査、海外資源、来訪者情報、 VIP会合日程、国際会議、政府部局報告書、 情報流出事故
公開情報	３８％	東日本震災、新型インフルエンザ、 情報セキュリティ注意喚起、 情報セキュリティ調査報告、国際情勢、 シンポジウム、金融情勢、経済外交、 政府予算、製品事故、経済成長戦略
組織内限定	９％	不審メールの注意喚起、社内ウイルス調査、 組織内業務連絡、役員人事異動

(4) 標的型攻撃メール発信元の IP アドレス

図 8 は、メールヘッダに記録された IP アドレスを国別に集計したものである。分析した標的型攻撃メールは、すべて日本の組織が送信したように詐称しているが、実際の発信元は、約 1/3 が中国の管理する IP アドレスからのもので、日本国内の IP アドレスから発信したと記録されたものは 8%である。

なお、不明 35%は、メールヘッダを入手できなかったためである。

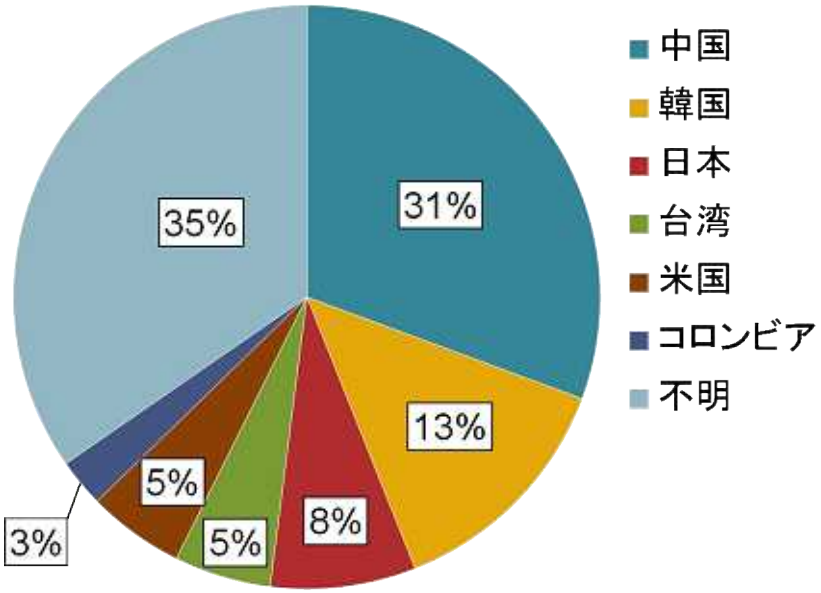


図 8．標的型攻撃メール発信 IP アドレスの国別内訳

(5) 標的型攻撃メールの（詐称している）発信ドメイン

図 9 は、詐称されたメール送信者のメールアドレスのドメインを集計したものである。官公庁を詐称した標的型攻撃メールのほとんどは、日本政府の管理するドメイン go.jp を詐称しており、全体の 1/2 を占めている。

例えば、葉書や封書のような紙媒体であっても、差出人の名前や住所に偽の情報を記載することが可能であるのと同様に、電子メールでも、送信者のメールアドレスを詐称することは容易である。

正規のメールサーバからしかメールを受け取らないように設定している組織に標的型攻撃メールを送る場合は、フリーメールを使ったり、セキュリティ対策の不十分な企業や団体のメールサーバを経由したりする手法を使うことが多い。

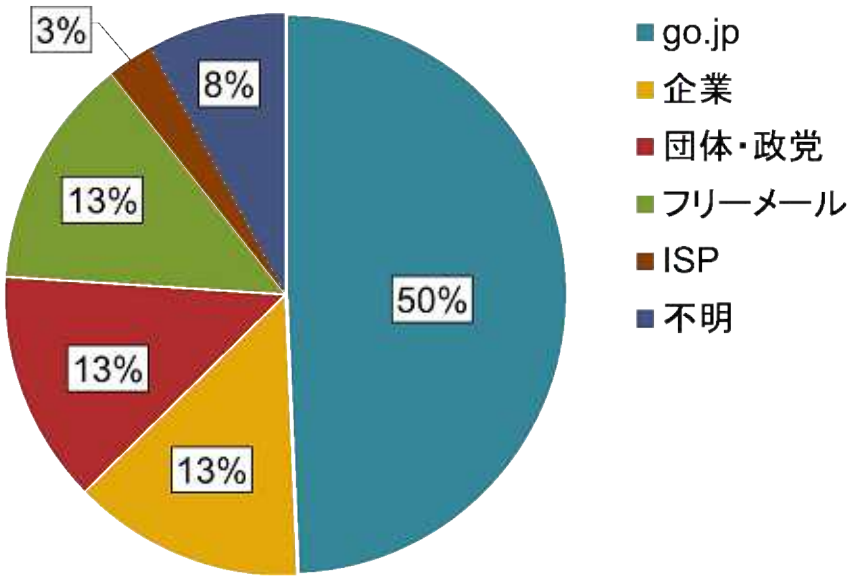


図 9.（詐称された）送信元メールアドレスのドメイン

(6) 標的型攻撃メールの添付ファイル

図 10 は、標的型攻撃メールの添付ファイルの種類を集計したものである。IPA が標的型攻撃メールの検体を収集しはじめた当初は、exe ファイルのような実行形式のウイルスを添付した事例は少なかったが、最近は exe ファイルを圧縮して添付する事例が多くなってきており、全体の 1/3 を超えている。

exe ファイルを添付する場合、アイコンを MS Word のようなアプリケーションのアイコンにしたり、ファイル識別子を「 xxx.doc.exe 」のように二重拡張子にしたり、「xxx.pdf .exe 」のように、ファイル識別子の前に空白文字を入れることで、実行形式のファイル識別子を見えにくくしたり、文字列を左右逆転して表示する手法で「 exe.xxx.doc 」のように見えるようにすることがある。

ウェブ感染型というのは、添付ファイルがなく、ドライブ バイ ダウンロード の攻撃手法で、悪意のあるウェブサイトからウイルスを感染させる手法であった。

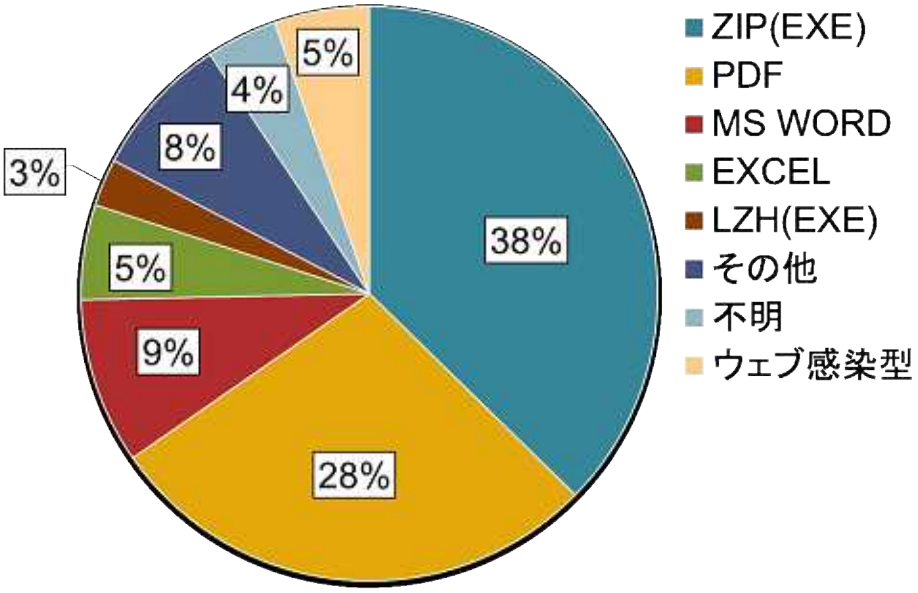


図 10．添付ファイルの種別

(7) 標的型攻撃メールで悪用された脆弱性のあったソフト

図 11 は、アプリケーションの脆弱性を悪用してウイルスに感染する仕掛けをした標的型攻撃メールを集計したものである。アドビシステムズ社のアプリケーションの脆弱性を悪用した事例が合わせて全体の約 2/3 を占めている。

Windows Update に代表される オペレーティングシステム関係の脆弱性は、多くのユーザが自動更新によって修正しているが、アプリケーションの脆弱性は修正していないユーザがまだまだ多いために、悪用される事例が多いと推察される。

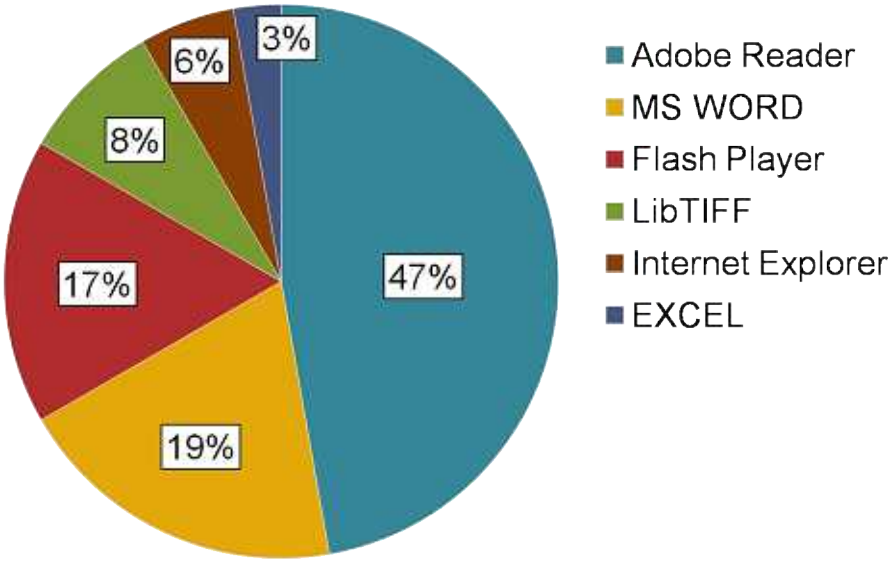


図 11．標的型攻撃に悪用された脆弱性があったソフト

6．標的型攻撃メール対策

標的型攻撃メールは、普通のウイルスメールと同様に、添付ファイルやメール本文に記載したリンクをクリックさせることで、メール受信者のパソコン等にコンピュータウイルスを感染させる攻撃である。従って、メール受信者の情報リテラシー向上や受信メールの取扱いが非常に重要となる（運用管理面での対策）。しかしながら、人間が操作するものであり、またメール受信者を信用させる様々なだましのテクニックを駆使していることから、うっかり添付ファイルを開いてしまうリスクの対策も不可欠となる（技術面での対策）。

以下では、この２つの対策について説明する。

6.1. 運用管理面での対策

(1) 従業員の情報リテラシーの向上

標的型攻撃メールのウイルスに感染しないための最初の砦は、メール受信者の適切な判断となる。そのためには、3 章、4 章、5 章で紹介した知識を従業員に周知徹底することが重要である。

少なくとも、次の知識と対応を身につけておくことが必要である。

・件名、本文、添付ファイル名などが日本語のウイルスメールも増えている。

・差出人のメールアドレスは簡単に詐称できる。

・原則として、実行形式の添付ファイルを開いてはいけない。

・ワープロ文書など実行形式でない文書データファイルから感染するウイルスもある。

・ウイルス対策ソフトを導入していても、ウイルスを 100%防げるわけではない。

・ウイルスに感染しても、目に見える異常な症状が出るとは限らない。

・脆弱性の修正プログラムが公開されたら、原則として、すぐに適用する。

なお、標的型攻撃メールを疑似体験させる「予防接種」という教育手法がある。従業員の標的型攻撃メールへの耐性確認と意識向上に効果が高いと言われている。

【参考】標的型攻撃対策手法に関する調査報告書（JPCERT/CC）

http://www.jpcert.or.jp/research/2008/inoculation_200808.pdf

(2) 標的型攻撃メールに関する情報集約と情報共有の体制整備

標的型攻撃メールは、１つの組織の複数のメールアドレス宛てに送られることがある。メーリングリストのメールアドレスに送られた場合、メーリングリストメンバ全員に当該の標的型攻撃メールが届く。

不審なメールが届いたら、開かずに削除するようにルール化している場合、気付いた人は被害に遭わないが、気付かずに添付ファイルを開いたり、メール本文のリンクをクリックしてしまう人もいるであろう。また、メールを削除してしまうと、本当に標的型攻撃メールであったのか、もし気づかずにウイルスに感染していた場合にどのような被害が発生しうるのか等を調査することもできない。

標的型攻撃メールの可能性があるメールを受信した場合に、情報システム部門に情報を集約する体制を構築すべきである。集約した情報を元に、組織内での注意喚起をしたり、同様のメールが送られている部門や人を特定し、速やかに該当者に対処方法を指示することで被害を防止もしくは極小化できる可能性が高い。

(3) 心あたりのないメールを受け取った場合の対応

一見して問題なさそうな添付ファイル付きのメールを受信したが、なぜ自分宛てに送ってきたか心当たりがない場合は、インターネット検索や電話番号案内などで送信者の連絡先を調べ、問い合わせる。その結果、当該メールを送っていないということが判明した場合は、組織内のインシデント対応部署やシステム管理者などに報告し、必要に応じて組織内に注意喚起をする。

なお、送信者の連絡先が判明しない、またはそれに時間を要する場合は先立って注意喚起を実施する必要がある。

(4) 不審なメールの添付ファイルを開く場合の対応

電子メールでの注文受付や問合せ窓口を運営している組織では、不特定多数からの添付ファイル付きのメールを受け付けざるを得ない場合がある。

標的型攻撃メールは、ネットワークを介してウイルスを感染させたり、窃取した情報を攻撃者に送ったりする。従って、ネットワークに接続していないパソコンで不審なメールの添付ファイルを開くことは有効な対策である。

万一ウイルスが仕掛けられていた場合でも、専用パソコン自体に影響がでないように、仮想 OS 上で構築・運用するというのも選択肢の一つである。また、今のところほとんど標的型攻撃の対象となっていないオペレーティングシステムである、Linux ベースで専用パソコンを構築するのも有効な対策である。

(5) 自分（や自組織）が詐称された標的型攻撃メールの連絡を受けた場合の対応

「差出人が貴方となっている添付ファイル付きメールを受け取ったが、貴方が送信したものか」との問合せを受けた場合は、心当たりがない場合には、組織内のインシデント対応部署やシステム管理者などに報告して対応を検討する。可能であれば、当該メールを転送などで入手し、送信者アドレスを詐称された単なる迷惑メールか、一般のウイルスメールか、標

的型攻撃メールかを分析する。また、当該メールを受信したという問合せが多い場合は、自組織のホームページなどで外部に注意喚起をすることも検討すべきである。

6.2. 技術面での対策

(1) ウイルス対策ソフトの適切な運用

ほとんどのウイルス対策ソフトは、既に発見されたウイルスの情報を元に、ウイルスを検知して感染を防止したり、駆除を行う。毎日数千種以上の新しいウイルスが発見されており、ウイルス定義ファイルを最新にしていないと、ウイルスを検知できない可能性がある。特に、ウイルス対策ソフトのライセンス期間を過ぎると最新のウイルス定義情報が入手できないことがあるので、注意する必要がある。

多くのウイルス対策ソフトには、常時監視する機能と、指定した時にコンピュータ内のファイルを検査するスキャン機能がついている。

①常時監視機能を用いてファイルを開く前に自動的にチェックする

②定期的にその時点での最新のウイルス定義情報を用いてコンピュータ内の全ファイルをスキャンする

の両方を行うことが重要である。

ウイルス対策ソフトはメーカーよって検知できるウイルスの種類が異なる。メールサーバで運用するウイルス対策ソフトとパソコンで運用するウイルス対策ソフトを別のウイルス対策ソフトメーカーの製品にすることで、ウイルスが検知できないリスクを低減できる。

(2) オペレーティングシステムやアプリケーションの既知の脆弱性の速やかな修正

ウイルス感染の手法として、ソフトウェアの脆弱性を悪用する場合がある。過去には、メールソフトの脆弱性を使ってメールを開かなくても添付ファイルが実行されるというウイルスもあった。近年では、PDF ファイルや MS Word、Excel、一太郎などの文書データファイル内にウイルスを埋め込んで、それらの文書データファイルを処理するアプロケーションの脆弱性を悪用してウイルスに感染させる事例も多数確認されている。

Windows Update のような、オペレーティングシステムの修正プログラムだけでなく、自分のパソコンで利用している全てのアプリケーションについて、公開されている修正プログラムを適用したり、最新版に入れ替えるということが重要である。

近年、脆弱性の修正プログラムが公開されると、その脆弱性を悪用したウイルスが短期間に作られてサイバー攻撃に使われることが多くなった。組織によっては、修正プログラムを適用して問題が発生しないことを確認するまで、修正させないポリシーを運用している所もあるが、なるべく速やかに修正プログラムを適用すべきである。

なんらかの理由で修正プログラムを自動的に適用しない設定で運用している場合は、修正プログラムが適切に適用されているかどうかを資産管理ツールなどを用いて、定期的にチェックする必要がある。

IPA では、PC で良く利用されているアプリケーションについて、最新版であるかどうかを簡単にチェックできるツールをウェブで公開しているので、活用して頂きたい。

【参考】MyJVN バージョンチェッカ（IPA）

http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

(3) 添付ファイルのファイル識別子の確認

添付ファイルのファイル識別子が exe のような実行形式ファイルであれば、原則として開くべきではない。実行形式ファイルであることを隠す手口を使っている場合があるので、ファイル形式の確認は慎重に行う必要がある。また、添付ファイルのファイル識別子が zip のような圧縮ファイルであれば、その圧縮ファイルを展開したのち、ファイル識別子を確認する必要がある。

確認の際のノウハウを以下に挙げる：

(a) 実行形式ファイルの場合、アイコンを自由に変えることができる。従って、MS Word のようなアプリケーションのアイコンであっても、ファイル識別子を必ず確認する。

(b) 登録されている拡張子を表示しない設定にしてあると、「 xxx.doc.exe 」のような二重拡張子のファイルが「 xxx.doc 」のように表示されることがあるので、すべての拡張子を表示する設定にする。

(c)「xxx.pdf　　.exe」 のように、空白文字を多数挿入されていると、一見「 xxx.pdf 」のように見えてしまうので、ファイル識別子を右端まで確認する。

(d) ファイル名の画面表示を左右逆転して表示する手法で「 cod.xxx.exe 」というファイル名を「 exe.xxx.doc 」のような文書ファイルによそおう場合があるので、添付ファイルを一旦デスクトップ等に保存して、ファイルのプロパティを確認する。

(4) メールヘッダの確認

標的型攻撃メールにおいては、メールの表題やメール送信者情報、メール本文、メール送信時刻、添付ファイル名は、メール受信者が信用するような内容で表示されるように加工してあることが多いが、メールヘッダには、実際のメール発信元 IP アドレスなど詐称することが困難な情報が多数含まれている。

(a) 図 12 は、2011 年 6 月 7 日に IPA に届いた標的型攻撃メールのメールヘッダの一部である。送付されたメールを中継するメールサーバにおいて、中国の IP アドレスが見て取れる。xxxx.org [119. xxx.xxx.xxx] や xxxx.xxxx.jp (119. xxx.xxx.xxx) は国内の大手プロバイダであるにも関わらず、60.209.xxx.xxx は、中国が管理する IP アドレスである。また、メール送信時刻 08 Jun 2011 04:56:56 +0800 のタイムゾーンは、日本ではなく中国のタイ

ムゾーンであり、メールサーバが受信した時刻 7 Jun 2011 22:01:10 +0900 と比べると、7 時間 45 分程度進めていることが確認できる。

```
Received: from xxxx.org (localhost [127.0.0.1])
        by xxxx.ipa.go.jp (Spam & Virus Firewall) with ESMTP id xxxxxxxxxx
        for < xxxx@ipa.go.jp>; Tue,  7 Jun 2011 22:01:20 +0900 (JST)
Received: from xxxx.org (xxxx.org [119. xxx.xxx.xxx]) by xxxx.ipa.go.jp with ESMTP id xxxxxxxxxxxxxxx
        for < xxxx@ipa.go.jp>; Tue, 07 Jun 2011 22:01:20 +0900 (JST)
Received: from unknown (HELO user-41005cbb85.domain) (comercial@xxxx.org@60.209.xxx.xxx)
   by xxxx.xxxx.jp (119. xxx.xxx.xxx) with ESMTPA; 7 Jun 2011 22:01:10 +0900
Message-ID: <09555bb16f1754d20a3131521c3f86ae@xxxx.org>
From: <comercial@xxxx.org>
To: <xxxx@ipa.go.jp>
Subject: =?iso-2022-jp?B?MjAxMRskQkZ8S1wzMDhyJE5MXEk4GyhC?=
Date: Wed, 08 Jun 2011 04:56:56 +0800
```

図 12．標的型攻撃メールのメールヘッダ例 1

(b)図 13 は、2010 年 11 月 22 日にある個人に届いた標的型攻撃メールのメールヘッダの一部であるが、xxxx.xxxx.go.jp は日本のある官公庁のドメインであるにも関わらず、60.26.xxx.xxx は、中国が管理する IP アドレスである。

また、メール送信時刻 22 Nov 2010 10:02:19 +0800 のタイムゾーンは、日本ではなく中国のタイムゾーンであり、中国でよく利用されているメールソフト Foxmail 5.0 beta2 を使って送信していることが確認できる。

```
Received: from xxxx.xxxx.go.jp ([60.26.xxx.xxx])by mxg511.nifty.com with ESMTP id xxxxxxxxxxxxx
        for <xxxx.xxxx@nifty.com>; Mon, 22 Nov 2010 11:02:49 +0900
X-Nifty-SrcIP: [60.26.xxx.xxx]
Message-Id: <201011220202.oAM22lq3006674@mxg511.nifty.com>
Received: from CRO-EE2C1904C10[192.168.1.226] by xxxx.xxxx.go.jp
   with SMTP id 37B7040D; Mon, 22 Nov 2010 10:02:14 +0800
From: "xxxx@xxxx.xxxx.go.jp" <xxxx@xxxx.xxxx.go.jp>
Subject: RE: =?ISO-2022-JP?B?GyRCMyRKXSQrJGkkTj5wSnMhSkBtM1U0WDc4lUsbKEI=?=
To: "ｘｘｘｘ" <xxxx.xxxx@nifty.com>
Reply-To: xxxx@xxxx.xxxx.go.jp
Date: Mon, 22 Nov 2010 10:02:19 +0800
X-Mailer: Foxmail 5.0 beta2
```

図 13．標的型攻撃メールのメールヘッダ例 2

(5) 万一ウイルスに感染した場合の対策

標的型攻撃メールと見抜けなかったり、あるいは不注意や好奇心などから、メールの添付ファイルを開いてしまった場合、以下の様々な要因でウイルスに感染してしまうリスクが存在している：

・ウイルス定義ファイルがない

・脆弱性の修正がなされていない

・未知の脆弱性への攻撃である（ゼロデイ攻撃）

こうした事態が発生することも想定して、情報窃取等の重大な被害を回避するための対策が必要となる。その対策として、

①ウイルスの活動（組織内蔓延や外部通信）を阻害、抑止する　＜出口対策＞

②重要な情報の利用制限（アクセス制御）をする

③情報にアクセスされても保護するための鍵（暗号）をかける

④操作や動き（ログ証跡）を監視・分析し不審な行為を早期に発見する

などが挙げられる[3]。

この①の実現方法については、以下の資料で詳細に説明しているので参照下さい。

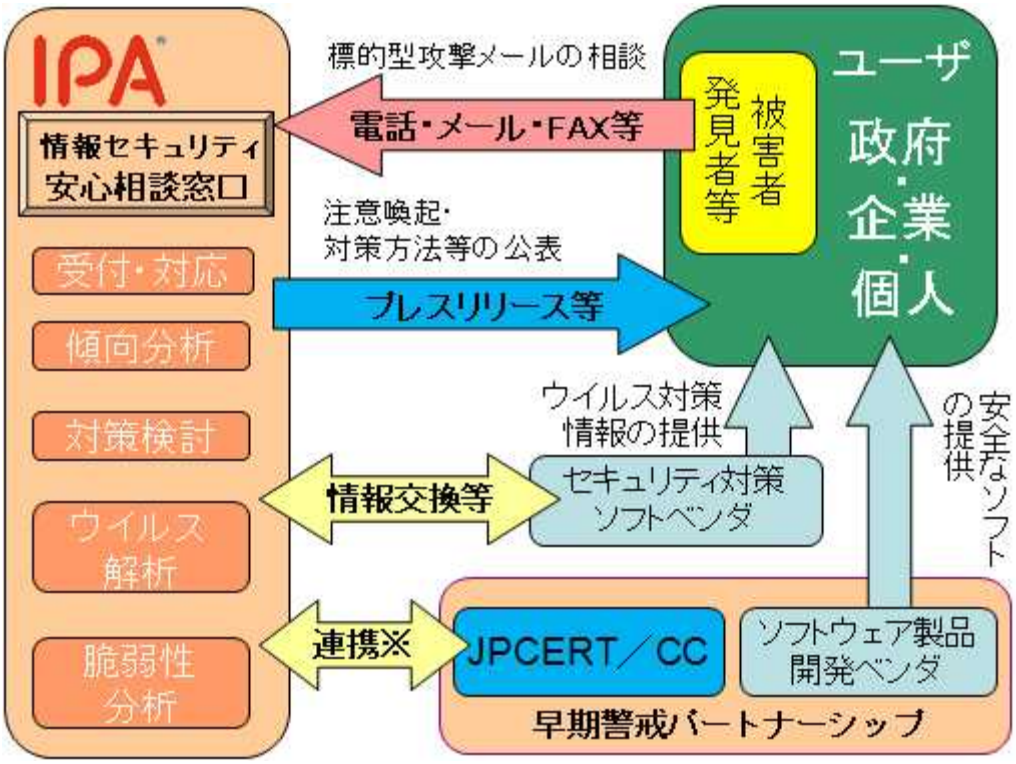
【参考】「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

http://www.ipa.go.jp/security/vuln/documents/newattack.pdf

[3] 組織の重要情報の窃取を目的としたサイバー攻撃に関する注意喚起　～組織システムのリスク把握と、日頃からのセキュリティチェックと対策の徹底を～　http://www.ipa.go.jp/about/press/20110920.html

7．標的型攻撃メールの相談及び届出

IPA の「情報セキュリティ安心相談窓口」では、不審なメールに係る相談に応じるとともに、標的型攻撃メールと判明した場合は、ウイルス検体を分析し、国内の主なセキュリティ対策ソフトメーカーにウイルス検体を提供することで、当該ウイルスをウイルス対策ソフトで検知できるようにするためのサポートを行っている。



※必要に応じて情報システムのぜい弱性対策の取り扱い（早期警戒パートナーシップ）を活用

図 14．IPA に届出・相談された標的型攻撃メールの取り扱い

情報セキュリティ安心相談窓口

(1) 電話による相談窓口

TEL：03-5978-7509

対応時間： 平日 月曜～金曜 10:00 ～ 12:00 及び 13:30 ～ 17:00

（音声ガイダンスの番号指定で「＃」を押せば、オペレータに接続する。）

(2) 電子メールまたはファクシミリによる相談窓口

対応時間： 24 時間受付けるが、回答は翌営業日以降になる場合がある。

E-mail： anshin@ipa.go.jp

FAX：03-5978-7518