IPA Technical Watch

IPA Better Life with IT

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」

IPA 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

本書の標的型攻撃メールの例では、実際の標的型攻撃メールをイメージできるように、架空の組織名や個人名などの名称を記載している。それらはすべて仮名であり、同一もしくは類似の組織名や個人名などの名称が万が一実在しても、本書の記載内容とは無関係である。

1. はじめに

特定の組織や人から機密情報を窃取する「標的型サイバー攻撃」が深刻な脅威となっているが、その中でも「標的型攻撃メール」が依然として猛威を振るっている[1]。

標的型攻撃メールは、不特定多数に大量に送られるウイルスメールとは異なり、特定の組織や人にしか送られないため、セキュリティソフトの定義ファイルに登録される前に標的とするメール受信者まで届いてしまう。そのため、受信者がセキュリティソフトを利用していても、被害を防ぐことが難しい。

また、メール受信者が不審をいだかないように様々な騙しのテクニックが駆使されているため、メール受信者は本物のメールと勘違いしてしまい、ウイルス感染の仕掛けが施された添付ファイルを開いたり、本文に記載されたウイルス感染の仕掛けが施されたサイトへのリンクをクリックしたりしてしまう可能性が高い。

添付ファイルの開封や本文のリンク先にアクセスすると、遠隔操作ウイルス（RAT：Remote Access Trojan／Remote Administration Tool）に感染し、新たなウイルスの感染、組織システム内へのウイルス拡散、情報収集、機密情報の外部への漏えい、システムの破壊といった大きな被害へ発展することになる。

標的型攻撃メールについては、国内でも 2005 年頃から報道されるようになったが、特に 2011 年 9 月に大手重工の被害が報道されてからは、多数のメディアで取り上げられるようになり、ここ数年は実際のメールが報道されることも多くなったため、目にする機会は増えたともいえよう。このような標的型攻撃メールは、大手企業や官公庁だけでなく、それらの組織と関係のある業界団体や中小企業に対して行われることにも留意が必要である。加えて、プライベートで利用しているメールアドレスを一時的に業務メールで使用している、またはしていた場合には、プライベートのメール利用環境でも不審なメールに注意する必要がある。

本書は、標的型攻撃メールの具体的な例を示すことで、メール受信者が標的型攻撃メールに気づくためのノウハウを培い、標的型攻撃メールによる被害が低減されることを目的としている。

なお、標的型攻撃についての一般的な説明は、IPA から多数の資料を公開しており、それらは「5. 参考資料」に示す。

---

[1] サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））の運用状況のレポートを参照（https://www.ipa.go.jp/security/J-CSIP/index.html）

1.1. 本書の対象読者

- 業務で電子メールを利用する人（プライベートのメールアドレスやフリーメールも含む）
- 組織でセキュリティ教育に携わっている人（教材としての活用）

1.2. 注意事項

標的型攻撃メールの騙しのテクニックは日々進化しており、本書で説明する着眼点で全ての標的型攻撃メールを見抜けるとは限らない。そのため、OS や各種ソフトウェアのアップデート、セキュリティソフトを最新の状態に保つといった基本的なセキュリティ対策も合わせて実施する必要がある。

受信したメールを不審に感じた場合には、「メール文面を見た」「リンクをクリックした」「添付ファイルを開いてしまったかもしれない」など些細な点も含め、組織で定められている運用ルールに従い、組織内の情報集約窓口に速やかに相談・連絡することが重要である。

一方、情報システム担当部門は、利用者が不審なメールに気づいた際の情報集約の体制、及び運用ルールを整備するとともに組織内に周知し、迅速に情報の集約が行える体制を整える必要がある。さらに、これまでは攻撃の初期侵入を防止（入口対策）する事を前提としてシステム設定が行われていたが、利用者が標的型攻撃メールを見抜けずにウイルスに感染してしまうなどの入口対策が突破され内部に侵入されることを前提とした上で、「侵害拡大防止」、及び「監視強化」を目的としたシステム設計（内部対策）も講じていく必要がある。IPA では、その様な考えに基づいたシステム設計ガイドを公開している[2]ので、参考にしていただきたい。

なお、組織の情報セキュリティ対策として、組織内の情報セキュリティ問題を専門に扱うインシデント対応チームである CSIRT（Computer Security Incident Response Team）の設置が注目されている。CSIRT については、一般社団法人 JPCERT コーディネーションセンターより構築を支援する資料などが公開されている[3]ので参照いただきたい。

加えて、標的型攻撃メールを受信した際や標的型サイバー攻撃の被害に遭われた際には、他の組織における被害の予防と拡大防止のために IPA などの標的型サイバー攻撃の対応の支援を行っている機関へ相談や情報提供いただきたい。

---

[2] https://www.ipa.go.jp/security/vuln/newattack.html
[3] CSIRT マテリアル：https://www.jpcert.or.jp/csirt_material/

2. 標的型攻撃メールの見分け方

本章では、標的型攻撃メールの例を示し、見分けるためのポイントを説明する。

加えて、日本語の文面ではないが、請求書や送付状などを装いボットウイルスや偽セキュリティソフト、ランサムウェアの感染を目的とするメールや、ID やパスワードなどの入力を要求するフィッシングメールも存在しており、結果的に標的型攻撃メールと同じ被害が生じる可能性もあるため、その例も合わせて掲載している。

標的型攻撃メールには、受信者が不審をいだかないように、高度な騙しのテクニックが用いられる。そのため、本書の例に類似した本物のメールやその逆に本書の例に類似しない巧妙な標的型攻撃メールも存在することを理解した上で参考にしていただきたい。

2.1. 標的型攻撃メールと注意する時の着眼点

表 2-1 は、IPA に情報提供があった標的型攻撃メールや公開情報から得た知見を基に標的型攻撃メールの特徴をまとめたものである。

これらの特徴に複数合致するメールを受信した場合は、標的型攻撃メールの可能性があるため、注意して対応する必要がある。対応方法については、「3. 標的型攻撃メールへの対応」を参照いただきたい。

表 2-1　標的型攻撃メールの着眼点

(ア)メールのテーマ	① 知らない人からのメールだが、メール本文の URL や添付ファイルを開かざるを得ない内容 (例 1) 新聞社や出版社からの取材申込や講演依頼 (例 2) 就職活動に関する問い合わせや履歴書送付 (例 3) 製品やサービスに関する問い合わせ、クレーム (例 4) アンケート調査
	② 心当たりのないメールだが、興味をそそられる内容 (例 1) 議事録、演説原稿などの内部文書送付 (例 2) VIP 訪問に関する情報
	③ これまで届いたことがない公的機関からのお知らせ (例 1) 情報セキュリティに関する注意喚起 (例 2) インフルエンザ等の感染症流行情報 (例 3) 災害情報
	④ 組織全体への案内

	(例 1) 人事情報 (例 2) 新年度の事業方針 (例 3) 資料の再送、差替え
	⑤ 心当たりのない、決裁や配送通知 (英文の場合が多い) (例 1) 航空券の予約確認 (例 2) 荷物の配達通知
	⑥ ID やパスワードなどの入力を要求するメール (例 1) メールボックスの容量オーバーの警告 (例 2) 銀行からの登録情報確認
(イ)差出人のメールアドレス	① フリーメールアドレスから送信されている
	② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
(ウ)メールの本文	① 日本語の言い回しが不自然である
	② 日本語では使用されない漢字（繁体字、簡体字）が使われている
	③ 実在する名称を一部に含む URL が記載されている
	④ 表示されている URL（アンカーテキスト）と実際のリンク先の URL が異なる（HTML メールの場合）
	⑤ 署名の内容が誤っている (例 1) 組織名や電話番号が実在しない (例 2) 電話番号が FAX 番号として記載されている
(エ)添付ファイル	① ファイルが添付されている
	② 実行形式ファイル(exe / scr / cpl など)が添付されている
	③ ショートカットファイル(lnk など)が添付されている
	④ アイコンが偽装されている (例 1) 実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
	⑤ ファイル拡張子が偽装されている (例 1) 二重拡張子となっている (例 2) ファイル拡張子の前に大量の空白文字が挿入されている (例 3) ファイル名に RLO[4]が使用されている

[4] 「Right-to-Left Override」と呼ばれる文字の表示上の並びを左右逆にする制御文字。
参考 :「ファイル名に細工を施されたウイルスに注意！」(2011 年 11 月の呼びかけ) (IPA)
https://www.ipa.go.jp/security/txt/2011/11outline.html

2.2. 標的型攻撃メールの例

本節では、標的型攻撃メールの例を用いて、不審か否かを見分けるための着眼点を示す。

以降の各ページ内の項番（例えば、【アー①】）は、「表 2-1　標的型攻撃メールの着眼点」の項番に対応する。

本書では、マイクロソフト Microsoft Outlook 2010 で表示した画面を掲載しているが、受信メールの表示形式は利用しているメールソフトにより異なる[5]ため注意いただきたい。

なお、添付ファイルに関しては、「2.3. 添付ファイルの種類」を確認いただきたい。

各例は、実際の標的型攻撃メールを基に、標的型攻撃メールの特徴を理解し易いように加工したメールである。なお、本書への掲載にあたり、実際の標的型攻撃メールにおいてフリーメールアドレスが利用されていたものについては、すべてドメイン名を「example.com」に置き換えている。

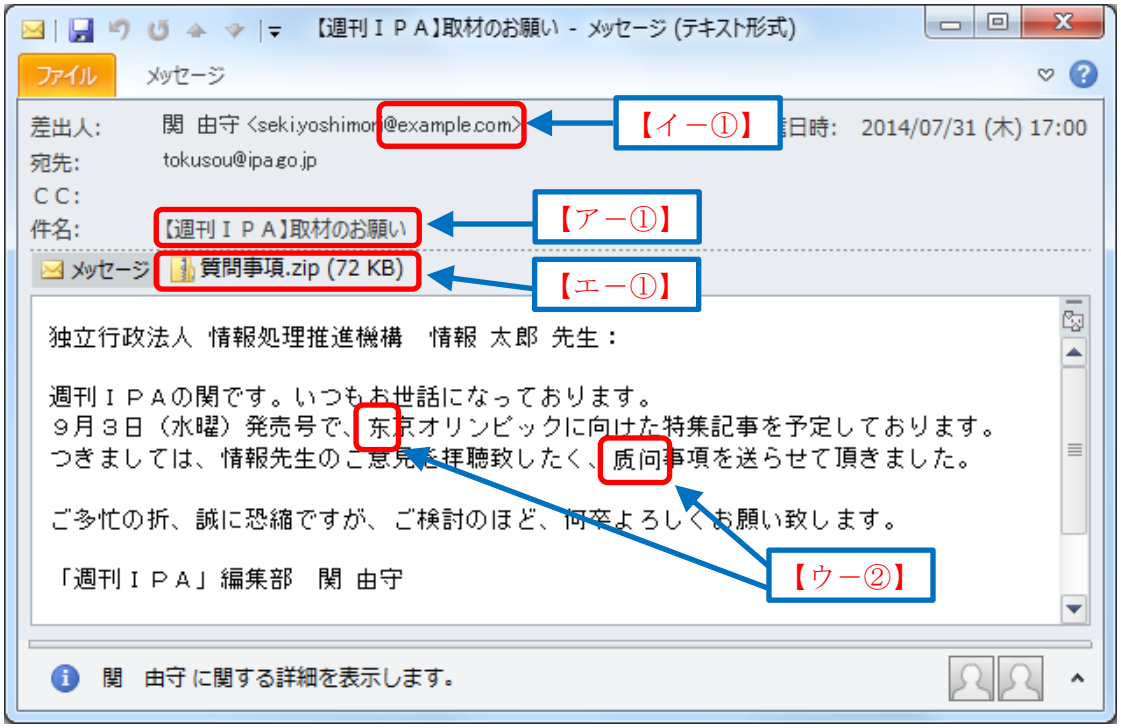
表 2-2　標的型攻撃メールの着眼点と本書の各節の対応表

節番号、及びページ番号 / 着眼点		標的型攻撃メールの例							添付ファイルの種類			
		2.2.1 P.7	2.2.2 P.8	2.2.3 P.9	2.2.4 P.10	2.2.5 P.12	2.2.6 P.13	2.2.7 P.14	2.3.1 P.16	2.3.2 P.19	2.3.3 P.19	2.3.4 P.20
(ア)	① 知らない人からのメールだが、メール本文の URL や添付ファイルを開かざるを得ない内容	●	●	●								
	② 心当たりのないメールだが、興味をそそられる内容											
	③ これまで届いたことがない公的機関からのお知らせ				●							
	④ 組織全体への案内											
	⑤ 心当たりのない決裁や配送通知					●						
	⑥ ID やパスワードなどの入力を要求するメール						●	●				
(イ)	① フリーメールアドレスから送信されている	●	●	●	●	●	●	●				
	② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる		●	●								
(ウ)	① 日本語の言い回しが不自然である							●				
	② 日本語では使用されない漢字が使われている	●										
	③ 実在する名称を一部に含む URL が記載されている				●							
	④ 表示されている URL と実際のリンク先の URL が異なる				●							
	⑤ 署名の内容が誤っている											

[5] メールソフトにより差出人の表示形式等が異なる場合がある。例えば、Mozilla Thunderbird 31.3.0 の場合、差出人の表示形式は、表示名として登録されているものが表示されるだけで、実際のメールアドレスは表示されない。

(エ)	① ファイルが添付されている	●	●	●		●			●	●	●	●
	② 実行形式ファイルが添付されている									●		
	③ ショートカットファイルが添付されている											●
	④ アイコンが偽装されている									●		●
	⑤ ファイル拡張子が偽装されている											

2.2.1. 新聞社や出版社からの取材申込のメール



出版社からの取材申し込み【ア－①】を装った標的型攻撃メールの例[6]である。

日頃から執筆活動やセミナー等の講師を行い、報道機関からの取材に対応することがある人にとって、このような取材申し込みのメールを装った標的型攻撃メールは、知らない人からのメールであっても、無視することが難しいだけでなく、本物のメールと区別することも難しい。

また、興味本位から質問内容を見てみたい、と感じ添付ファイルを開いてしまう可能性もあるだろう。

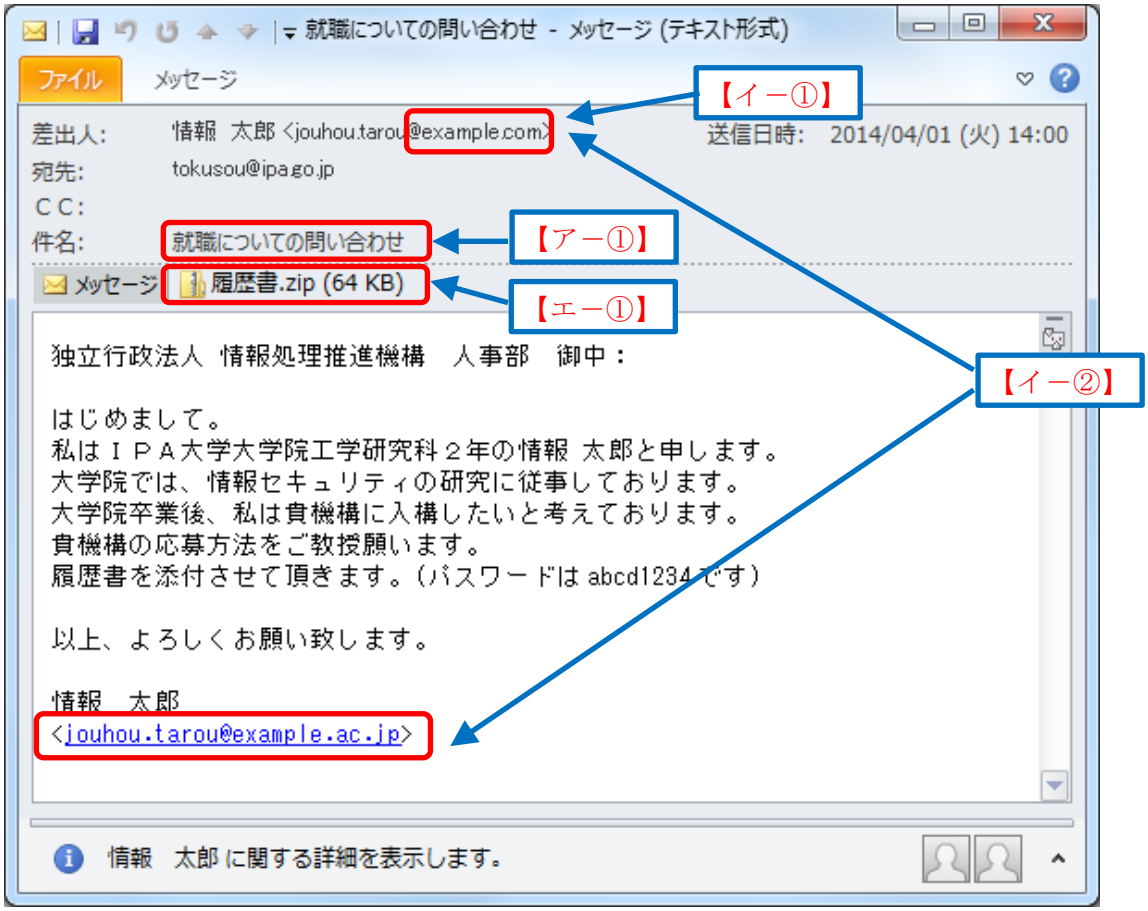
しかしながら、差出人のメールアドレスが、フリーメールアドレス（図中では@example.com）である点【イ－①】、メールの本文で日本語では使用されない漢字が使われている点【ウ－②】、zip 圧縮ファイルが添付されている点【エ－①】から、慎重に対応する必要がある。

このようなメールが届いた場合は、すぐにメールに返信したり、メールに記載されている電話番号に連絡したりするのではなく、ウェブ等の当該メール以外の情報源から当該組織（この例では、「週刊 IPA」）の電話番号や問合せメールアドレスを調べ、この差出人が実在するか、このメールを送信したかなどを確認することで、標的型攻撃メールか否かを判断する必要がある。

---

6 取材申し込みを装った標的型攻撃メールは 2013 年秋に多く見受けられた。

2.2.2. 就職活動に関する問い合わせのメール



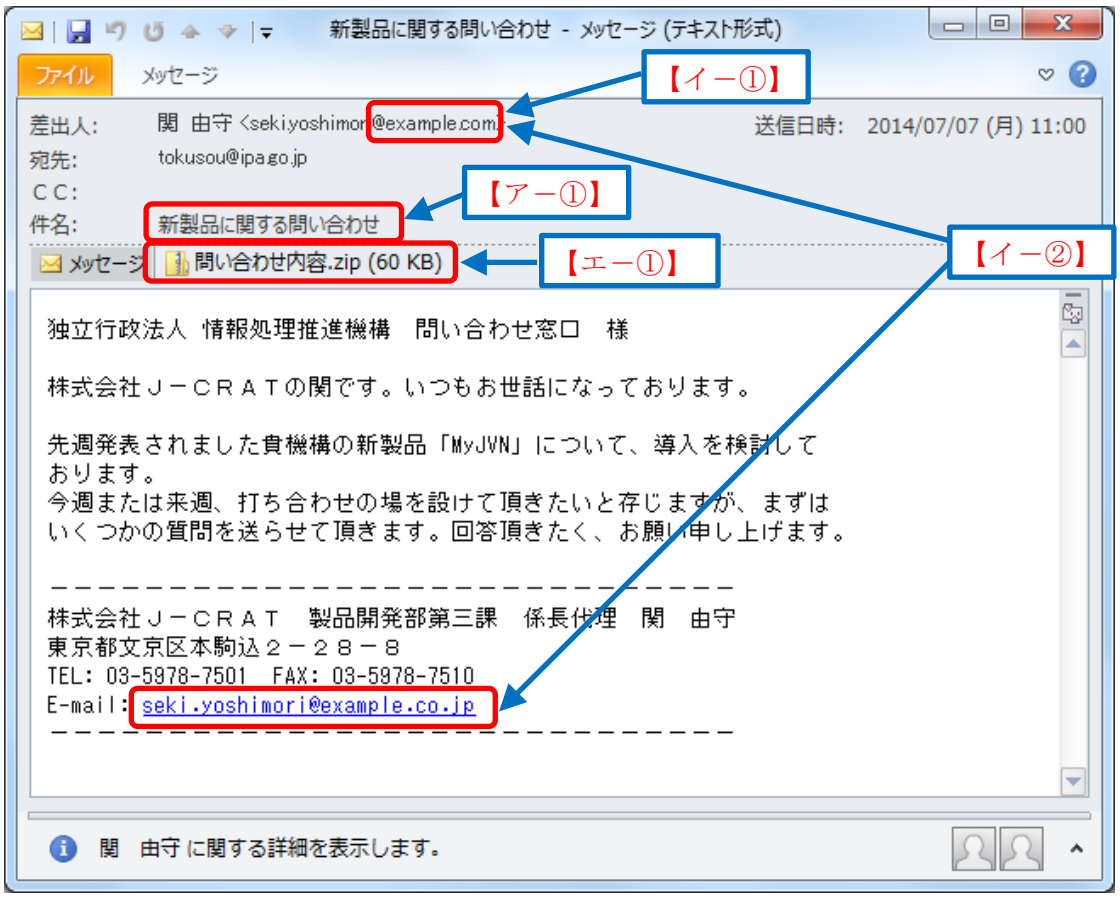
就職活動に関する学生からの問い合わせ【ア－①】を装った標的型攻撃メールの例[7]である。

学生の場合、就職活動にフリーメールアドレス（図中では@example.com）を使うこと【イ－①】は十分考えられるが、この例では、差出人のメールアドレス（フリーメールアドレス）と署名のメールアドレス（大学のメールアドレス）が一致しない点【イ－②】から、慎重に対応する必要がある。

なお、不特定の人からの問い合わせを受け付ける窓口では、就職活動に関する問い合わせのメールに限らず、フリーメールアドレスから添付ファイル付き【エ－①】のメールが届くことが十分考えられるため、常に不審なメールか否かについて判断する必要がある。

[7] 少し日本語に不自然な点があるが、真摯な熱意と共に送られる標的型攻撃メールは、2013年以降時期を問わず発生している。

2.2.3. 製品に関する問い合わせのメール



製品に関する問い合わせ【ア－①】を装った標的型攻撃メールの例[8]である。

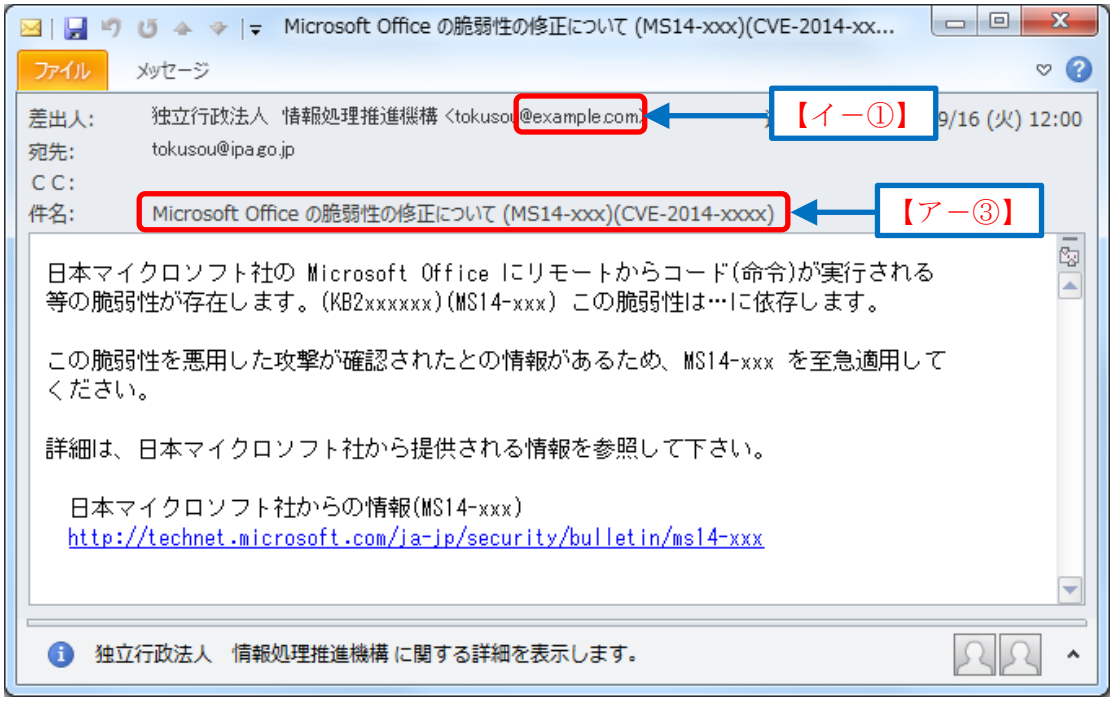
本文中に、実際の製品名やサービス名が記載されている場合が多い。

フリーメールアドレス（図中では@example.com）を利用している点【イ－①】だけでは不審と判断できないが、差出人のメールアドレスと署名のメールアドレスが異なる点【イ－②】が不審である。

また、zip 圧縮ファイルが添付されている【エ－①】ため、慎重に対応する必要がある。

[8] 本例は日本語であるが、2.2.5 「注文書送付のメール」のように外国語で届くことも考えられる。

2.2.4. セキュリティに係る注意喚起のメール

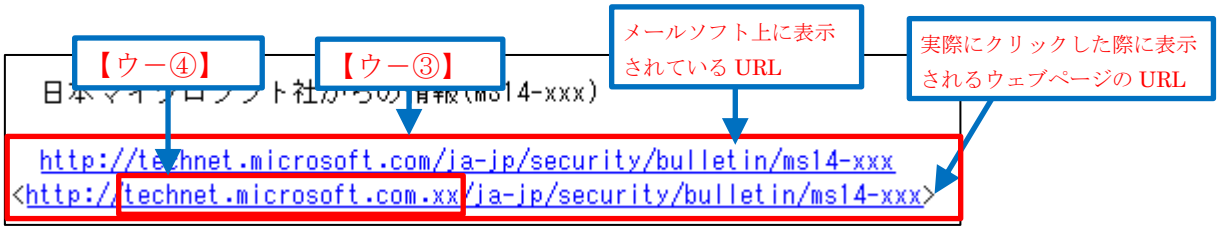


公的機関からのセキュリティに係る注意喚起【ア－③】を装った標的型攻撃メールの例[9]である。

公的機関からのメールにも関わらず、差出人のメールアドレスがフリーメールアドレス（図中では@example.com）である点【イ－①】が不審である。

また、本文の URL にも注意が必要である。本メールは、HTML メールとして送信されており、HTML メールでは表示されている URL（アンカーテキスト）と実際に URL をクリックした際に表示されるウェブページをそれぞれ設定することができる。

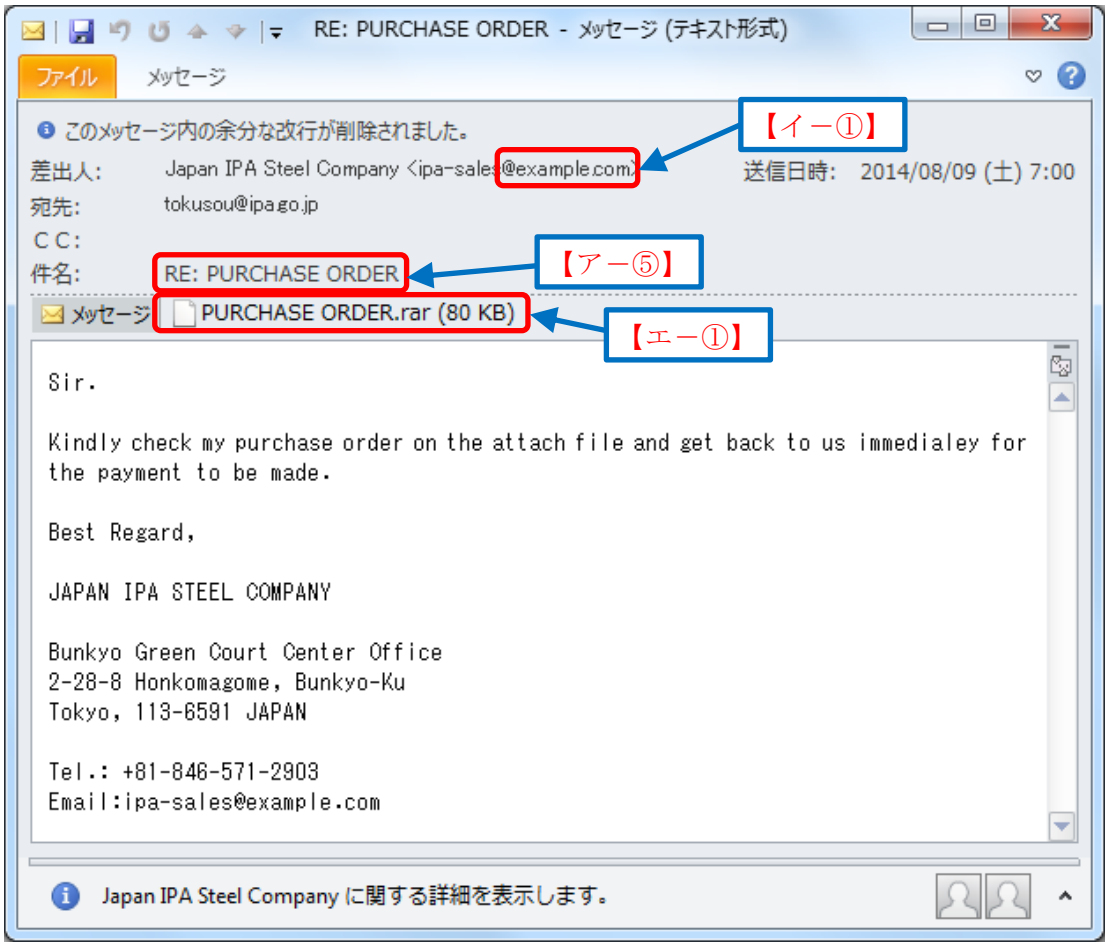
使用しているメールソフトによって操作方法は異なるが、メールの表示形式をテキスト表示にすることで実際にクリックした際に表示されるウェブページの URL を確認することができる。 Microsoft Outlook 2010 で同メールをテキスト表示にした画面を以下に示す。



9 一般にフィッシングと呼ばれる手法である。特に特定組織に送られるものを海外ではスピアフィッシングと呼ぶことが多い。フィッシングについては以下を参照。
https://www.ipa.go.jp/security/personal/protect/phishing.html

この例では、表示されている URL（http://technet.microsoft.com/・・・）と実際にクリックした際に表示されるウェブページの URL（http://technet.microsoft.com.xx/・・・）が異なる点【ウ－④】、及び実在する名称を一部に含む URL が記載されている点【ウ－③】が不審である。

2.2.5. 注文書送付のメール



海外からの注文【ア－⑤】を装ったメールの例[10]である。

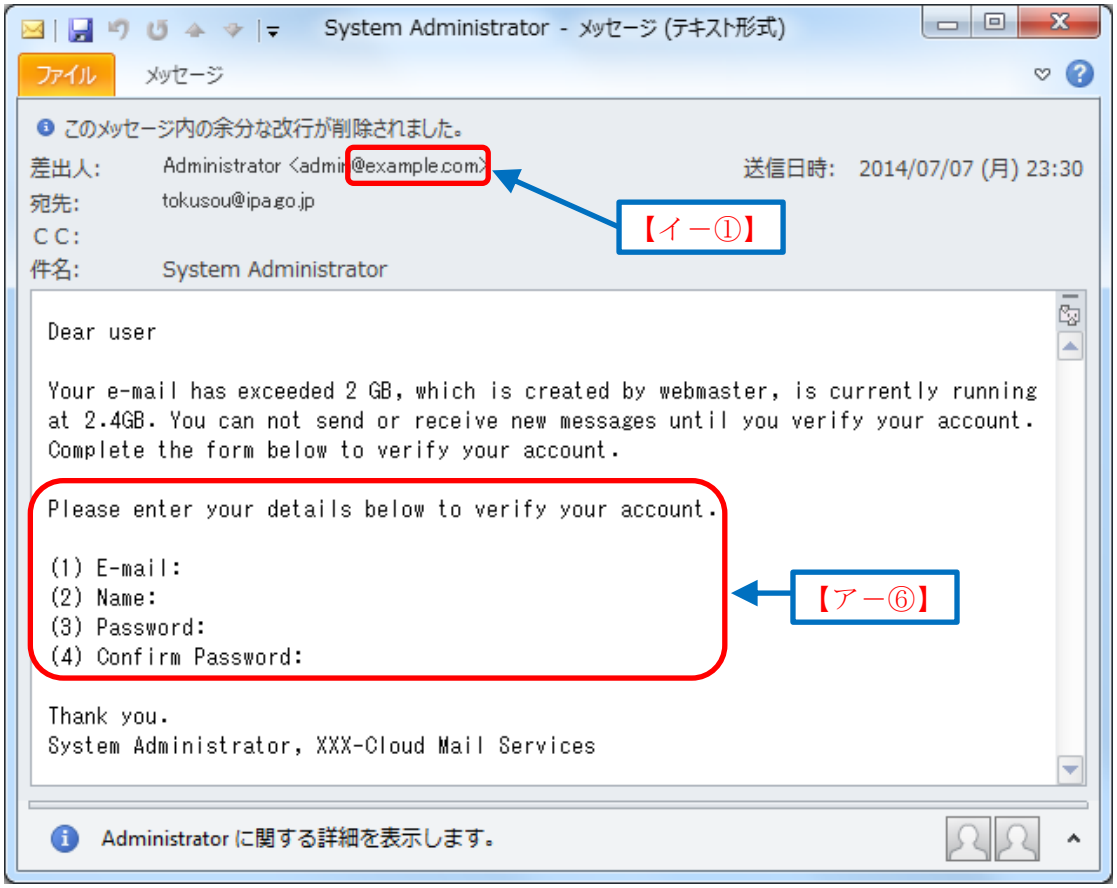
普段から海外の企業とやり取りをしている場合、本物のメールと区別することは難しい。しかしながら、突然取引のない企業からこのようなメールが届くことは考えづらいため、心当たりのない場合は、不審なメールの可能性が高いと判断し慎重に対応する必要がある。

また、差出人のメールアドレスがフリーメールアドレス（図中では@example.com）である点【イ－①】、及び国内では使われることが少ない rar 圧縮形式の添付ファイルが添付されている点【エ－①】が不審である。

なお、注文書だけではなく、請求書や送付状などの送付を装ったメールも確認されている。

[10] 他にも、Invoice、Booking、eFax、MMS、配送会社を装ったものもある。多くはボットウイルスに感染させる手口であるが、最近ではボットウイルス感染を使った標的型サイバー攻撃も海外で報道されているため、十分注意が必要である。

2.2.6. アカウント情報の入力を要求するメール（その１）



システム管理者からのアカウント情報の要求【ア－⑥】を装ったメールの例[11]である。

添付ファイルやリンクが存在しないがパスワードなどのアカウント情報をメールで返信するように要求している点【ア－⑥】、及びシステム管理者からの連絡にも関わらず差出人のメールアドレスがフリーメールアドレス（図中では@example.com）である点【イ－①】が不審である。

このようなメールが届いた場合は、安易にメールに返信せず、組織内の情報システム部門に電話等で確認するべきである。

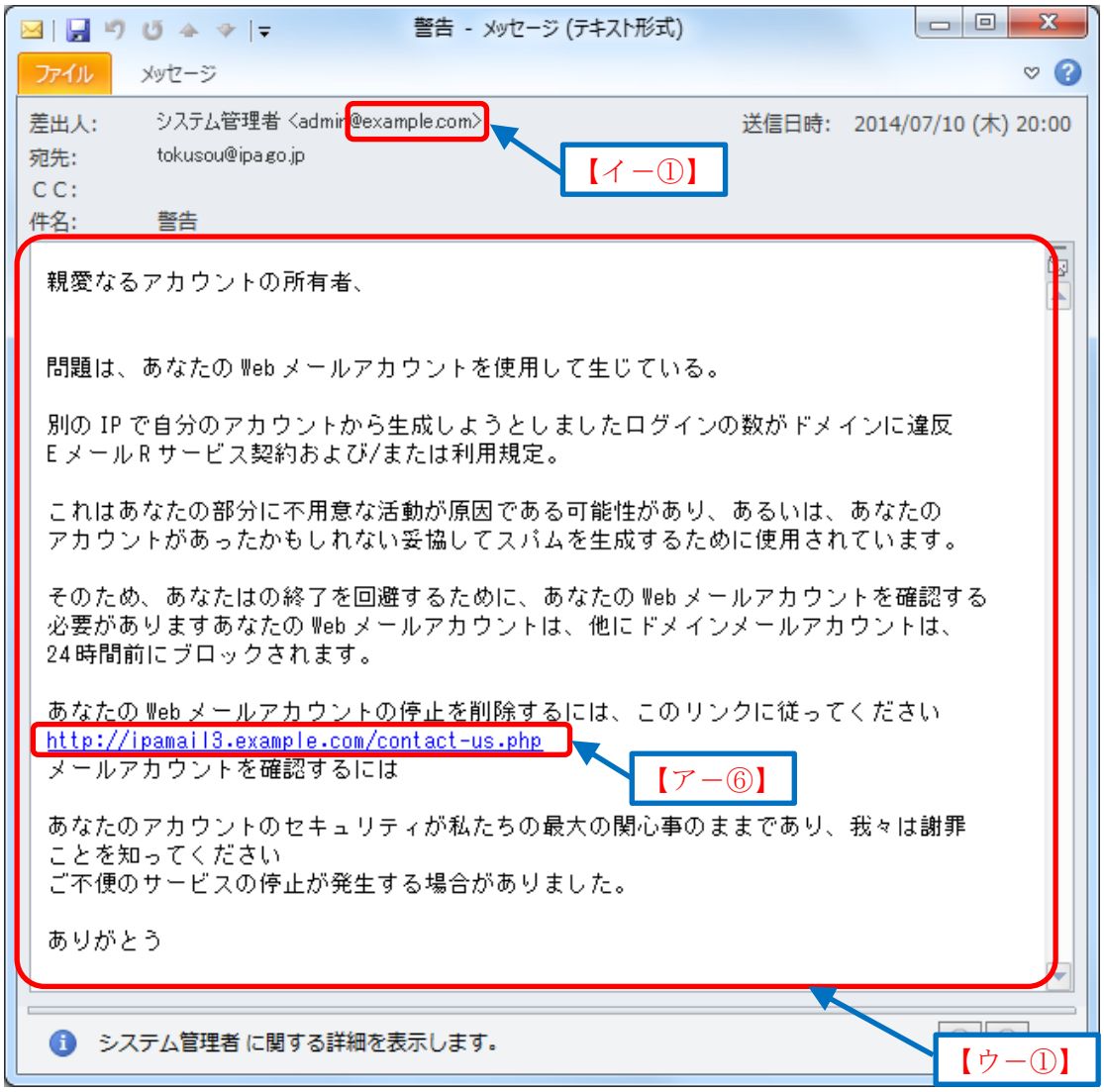
もし、このメールに返信して、自身の名前やメールアドレス、メールパスワードが攻撃者に渡ってしまうと、別の標的型攻撃メールに悪用されたり、自分宛てに標的型攻撃メールが届いたりする可能性がある。

手段は異なるが、遠隔操作ウイルスが添付された標的型攻撃メールと同様にアカウント情報を詐取することを目的とした手口である。

---

11 このようなメールに返信することは無いかもしれないが、気の緩みで思わず回答してしまう可能性もあるため注意が必要である。このようなメールは、（自動翻訳のような文面で）日本語をはじめ、複数の言語で存在している。

2.2.7. アカウント情報の入力を要求するメール（その２）



日本語ではあるものの「2.2.6. アカウント情報の入力を要求するメール（その１）」と同様のシステム管理者からのアカウント情報の要求【ア－⑥】を装ったメールの例[12]である。

システム管理者からの連絡にも関わらず差出人のメールアドレスがフリーメールアドレス（図中では@example.com）である点【イ－①】、及び全体的に本文の日本語が不自然である点【ウ－①】から不審なメールである可能性が考えられる。不自然な日本語は、日本語を理解していない攻撃者が自動翻訳ソフトを利用したためと推察される。

[12] 2013 年には国内においてウェブメールのログイン画面を装った例があった。また、スマートフォンで使うアカウント情報の入力を求めるものもあるため、注意が必要である。

実際のメールでは、本文中の URL をクリックすると、実在するウェブサイトを模したアカウント情報の入力を要求する【アー⑥】ウェブサイトに接続される。場合によっては、本文中の URL をクリックし攻撃者が用意したウェブサイトに接続することで、ウイルスに感染する危険性もあるため、注意する必要がある。

2.3. 添付ファイルの種類

本節では、標的型攻撃メールで使われる添付ファイルの例を紹介する。

なお、添付ファイルを使った主な騙しのテクニックであるアイコン偽装、ファイル拡張子偽装（二重拡張子、大量の空白文字の挿入、RLO の使用）については、これまでに IPA から公開している資料[13]を参照いただきたい。

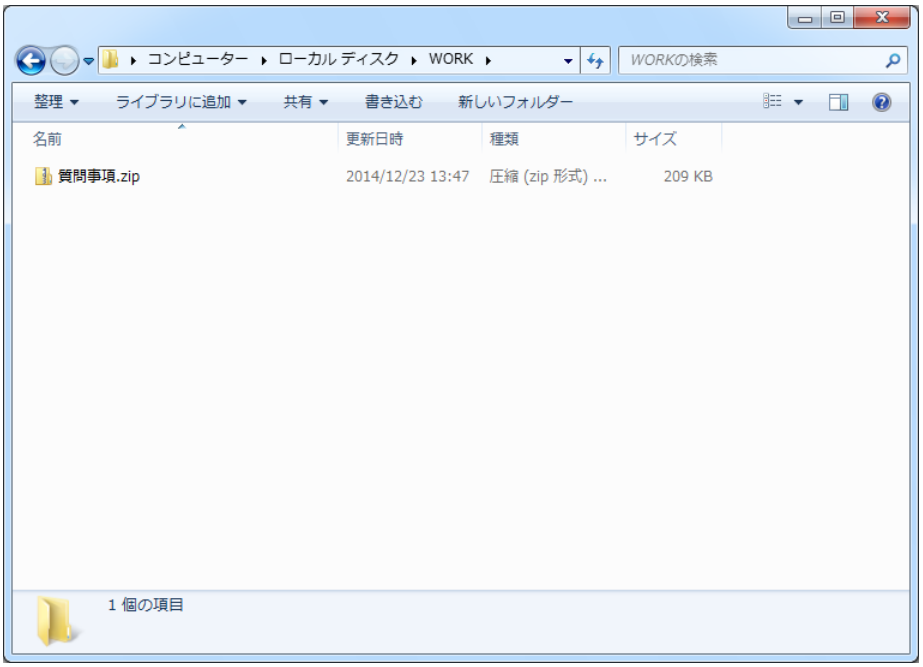
2.3.1. zip 圧縮ファイル

データを格納するためのファイル形式である。標的型攻撃メールにおいては、この zip 圧縮ファイルの中に後述の「実行形式ファイル」や「データ形式ファイル」などが格納されている場合がある。しかし、zip 圧縮ファイル自体は、一般的なメールのやり取りでも利用されているため、zip 圧縮ファイルが添付されているだけでは不審なメールとは判断できない。そのため、zip 圧縮ファイルの中にどのようなファイルが格納されているかを確認する必要がある。zip 圧縮ファイルの中身の確認方法の一例を以下に示す。

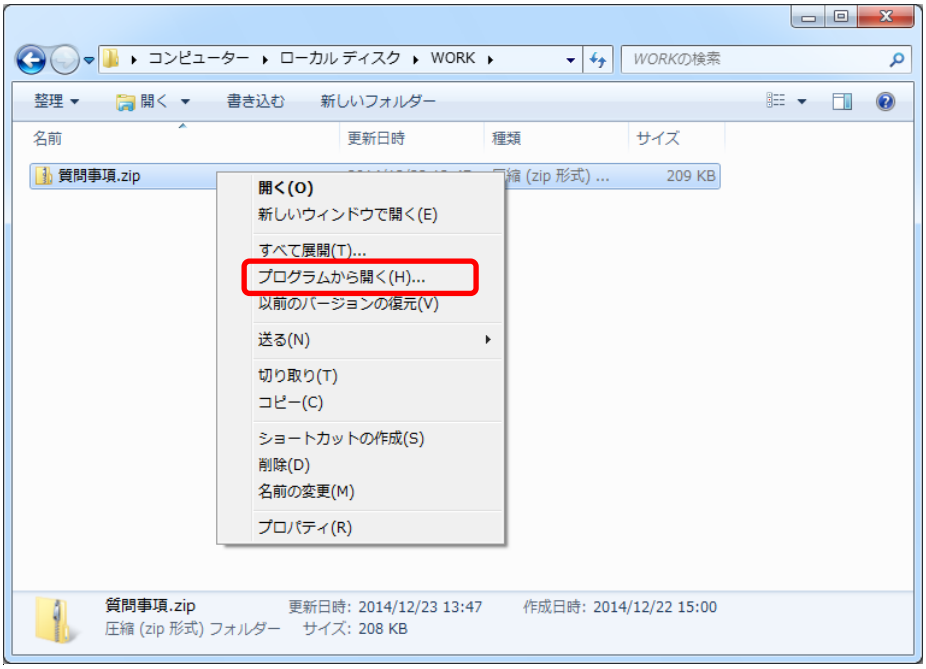
> **以下の作業では、操作ミスによりウイルス感染被害が発生する可能性があるため、興味本位などでむやみに中身を確認することはせず、不審と思えば組織で定められている運用ルールに従い、組織内の情報集約窓口に速やかに連絡・相談することが重要である。**
>
> **連絡・相談先が不明な場合は、ぜひ IPA に相談していただきたい。**

[13] 標的型攻撃メール<危険回避>対策のしおり（第 1 版）：
https://www.ipa.go.jp/security/antivirus/shiori.html

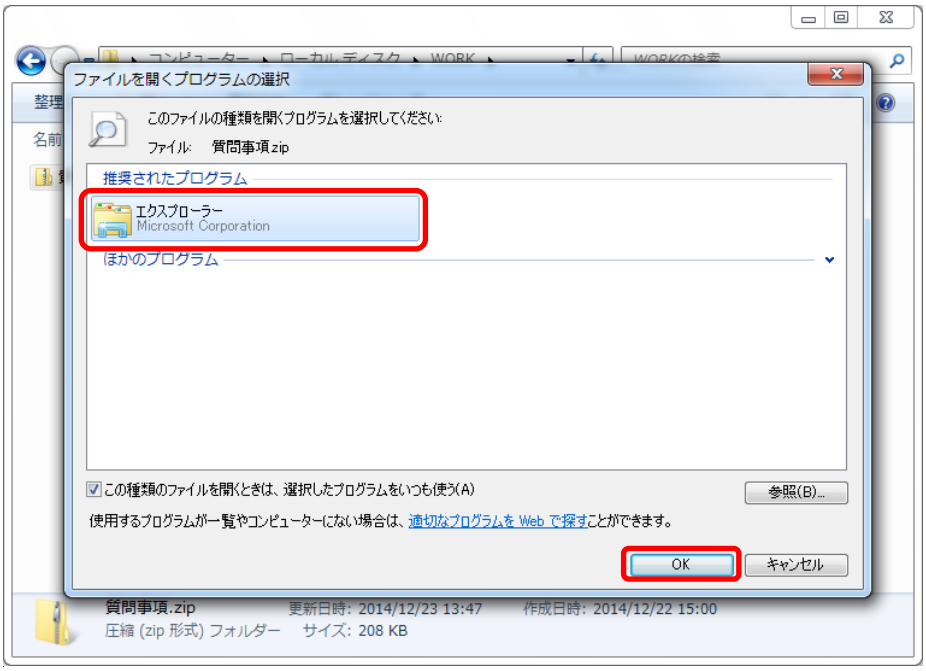
(a) 添付ファイルを任意のフォルダに保存する。ただし、この時点で、セキュリティソフトがウイルス検知の警告を表示したときは、それ以上の作業を行わない。



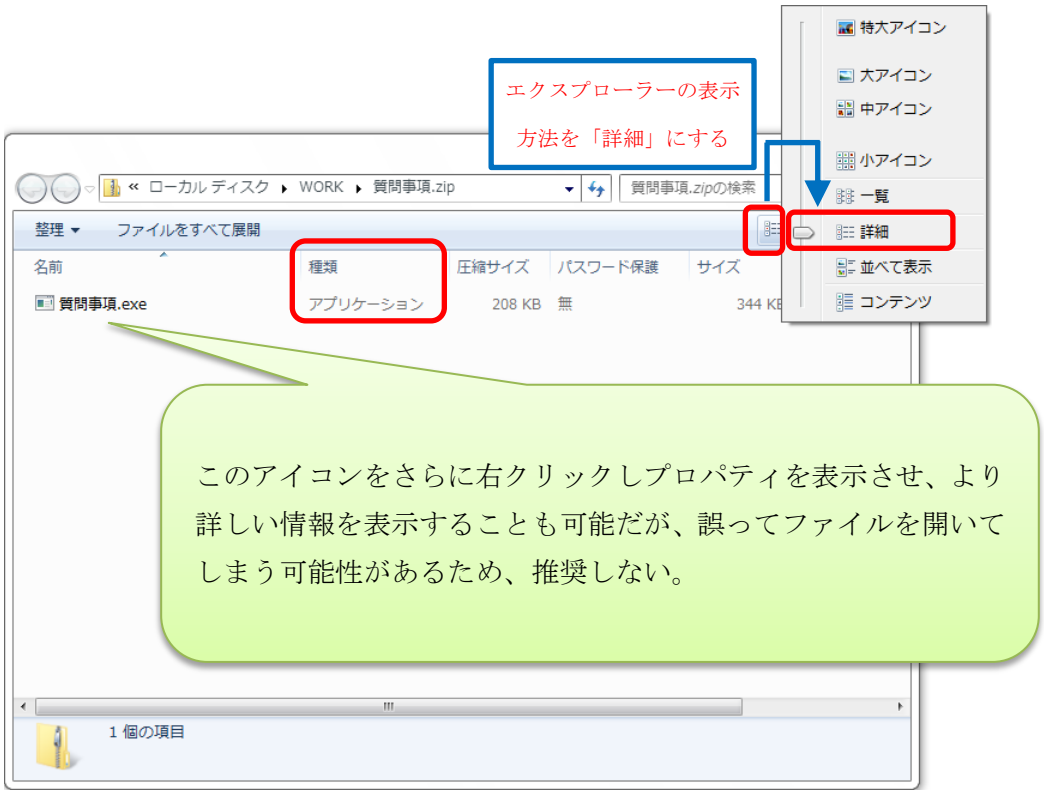
(b) zip 圧縮ファイルを右クリックして、「プログラムから開く」をクリックする。



(c) 推奨されたプログラムの「エクスプローラー」を一度クリックした後に、「OK」をクリックする。



(d) エクスプローラーの表示方法を「詳細」とすることで、ファイルの「種類」を確認できる。この例では、「アプリケーション」である。



2.3.2. 実行形式ファイル

実行形式ファイルは自由にアイコンが設定できるため、実行形式ファイルのアイコンを後述のデータ形式ファイルなどに偽装して添付した標的型攻撃メールが見受けられる。

実行形式ファイルは命令の集まりであるため、開いてしまうだけで攻撃者が事前にファイル内に記述した命令が実行され、新たなウイルスのダウンロードや遠隔操作などが行われてしまう。万一、添付ファイルが実行形式ファイルであれば、安易に開いてはいけない。実行形式ファイルを開く際には、そのファイルが本当に信頼できるのかどうかを確認し、慎重に開く必要がある。

Windows 環境を対象とした標的型攻撃メールで確認された実行形式ファイルの一例としては、拡張子が exe、scr、cpl といったものが確認されている。

メールソフトやセキュリティソフトによっては、実行形式ファイルが添付されているだけで、警告を表示したり、開けないようにしたりする機能を持つものがあるため、最近は実行形式ファイルを直接添付するメールはほとんど無くなった。

注）情報漏えい対策のために、ファイルを暗号化して実行形式ファイル（自己解凍形式）でメールに添付している場合もあるため、その際には送信元に確認する必要がある。

2.3.3. データ形式ファイル

データ形式ファイルはデータの集まりであるため、そのデータを読み込むことができるプログラムに読み込ませる必要がある。一般的に事前にデータ形式ファイルごとにどのプログラムに読み込ませるかが設定されているため、利用者はデータ形式ファイルを開くだけで、自動的にプログラムがデータ形式ファイルを読み込み起動する仕組みになっている。そのため、攻撃者は、データ形式ファイルの中にそのデータを読み込むプログラムの脆弱性を悪用するウイルスや悪意のある動作をするコマンドを埋め込んだりすることがある。

特に利用者が多い Microsoft Office 関連のファイルや PDF ファイルは、標的型攻撃メールにおいて他のデータ形式ファイルと比べてウイルスが埋め込まれることが多い。また、日本のみを標的とするためなのか、日本語のワープロソフトである一太郎のデータ形式ファイルにウイルスなどが埋め込まれることもある。

これらのデータ形式ファイルは、本物のメールのやり取りでも多用されているため、ファイルの種類だけでウイルスメールかどうかを見分けることは困難である。

データ形式ファイルを開く前には、当該データ形式ファイルを開くアプリケーションや OS のアップデートを確認するとともに、セキュリティソフトの定義ファイルを最新の状態にしてから開くことが重要である。なお、アプリケーションや OS、セキュリティソフトを最新の状態にしていても、修正プログラムが提供される前にプログラムの脆弱性が攻撃に

悪用される場合（ゼロデイ攻撃）もあるため、最新の状態のアプリケーションや OS、セキュリティソフトを使用していても絶対安全とは言い切れないことに留意する必要がある。

2.3.4. ショートカットファイル

ショートカットファイルは、実際のファイルやフォルダ、アプリケーションの場所を示すファイルであり、実体がそこになくても見掛け上はショートカットファイルを実体そのものとして扱え、ファイルへのアクセスを簡単にすることができる。

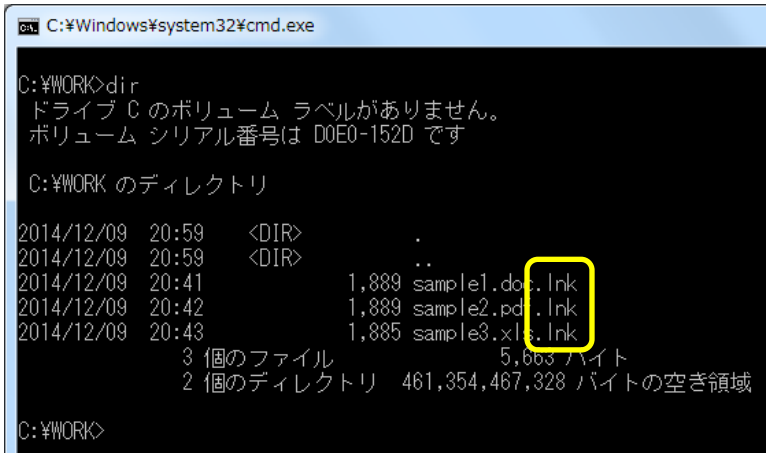
ファイル拡張子は lnk であり、その特徴として、通常の設定ではファイル拡張子が表示されない場合があり、ファイルに存在する設定値にウイルスをダウンロードする命令を記述することも可能であるため、標的型攻撃メールにおいて悪用される場合がある。

通常、ショートカットファイルを添付したメールを送ることは、限定的な状況下でのみ行われると考えられるため、ショートカットファイルが添付されていた場合には、不審なメールである可能性を疑う必要がある[14]。

以下にショートカットファイルのアイコンを示す。アイコンの表示から、一見するとデータ形式ファイルのように見えるが、アイコンの左下に「矢印のマーク」があることからショートカットファイルであることが判断できる。エクスプローラーの詳細表示では、種類に「ショートカット」と表示される。もし、zip 圧縮ファイルにショートカットファイルが含まれている場合は、「2.3.1 zip 圧縮ファイル」で説明した確認方法で、同様の確認が可能である。

[14] 正当なメールの差出人が、間違えてファイル実体ではなくショートカットを添付してしまうミスも考えられる。

コマンドプロンプトでファイルのリストを表示しても、ファイル拡張子が「lnk」であることからショートカットファイルであることが確認できる。



実行形式ファイルと同様にショートカットファイルもアイコンが自由に設定できるためアイコン偽装が可能であるが、どのようなアイコンに偽装してもショートカットファイルであることを示すアイコンの左下の「矢印のマーク」が表示されるため、不審であることに気づくことができる。

3. 標的型攻撃メールへの対応

標的型攻撃メールは、標的とする組織の複数のメールアドレスに届くことが多い。そのため、標的型攻撃メールを発見した場合は、発見者が自分に届いたメールだけを削除するだけでは対応として不十分である。例えば、同じ標的型攻撃メールが 5 人に届いたとして、4 人が気づき、1 人が気づかずにウイルスに感染してしまった場合、組織としては被害が発生してしまう。つまり、標的型攻撃メールについて組織内で情報共有することが重要である。具体的には、次の対応が考えられる。

- 不審メールに気付いたメール受信者は、組織で定められている運用ルールに従い、組織内の情報集約窓口に速やかに報告する。
- 情報集約窓口に集約された情報を基に、情報システム担当部門などは、当該メールを含め類似の不審メールが他に届いていないかを、メールサーバのログなどにより調査する。
- 情報システム担当部門などは、不審メールが届いたすべての端末で、添付ファイルを開いたり、不審な URL にアクセスしたりしていないかなどを確認する。

標的型攻撃メールかどうか判らない場合や、相手の連絡先がわからず真正性が確認できない場合には、IPA では専門的知見を有する相談員が対応する「標的型サイバー攻撃の特別相談窓口」を設置しているので活用していただきたい。この他にも IPA では、ウイルス、及び不正アクセスに関する総合的な相談窓口である「情報セキュリティ安心相談窓口[15]」を設置しているので、あわせて活用いただきたい。

標的型攻撃メールは、長期間に渡り、手を変え品を変え何回も届くことが多い。そのため、組織においては、標的型攻撃メールに関する情報を入手した場合に、組織全体に対して注意喚起を行い、被害の有無を確認することが重要である。

なお、情報共有による被害の拡大と予防のために、標的型攻撃の情報収集・分析・注意喚起などを行っている IPA にも、情報提供していただきたい。

独立行政法人 情報処理推進機構（IPA）
標的型サイバー攻撃の特別相談窓口
https://www.ipa.go.jp/security/tokubetsu/

[15] 情報セキュリティ安心相談窓口：https://www.ipa.go.jp/security/anshin/

4. おわりに

2005 年 10 月に国内における標的型攻撃メールに関する報道がされてから 9 年が経つが、まだまだ広く一般には標的型攻撃メールは認知されていない。一部の大企業や官公庁を標的とした攻撃しか報道されていないことが、その要因のひとつと考えられる。しかし、一部の大企業や官公庁だけではなく、最終的な標的とする組織と関係がある中小企業や業界団体にも標的型攻撃メールは届いており、そのような組織が長期にわたりウイルスに感染していたケースも確認している。

標的型攻撃メールへの対策として、セキュリティベンダ各社から次々に製品やサービスが発表されている。しかし、攻撃者もそれに対応して攻撃手法を変化させており、システムで防ぐだけでは十分とは言えず、メール受信者が自身で不審なメールを見分けることも重要な対策のひとつと考えられる。そのため、本書では、不審なメールを見分ける着眼点を読者のノウハウとしてもらうために、標的型攻撃メールの例を基にして不審なメールを見分けるためのポイントを説明した。

標的型攻撃メールは、同じ組織の複数のメールアドレスに届く場合が多いため、一人でも気づくことができれば、他の人に届いた標的型攻撃メールも発見できる可能性が高い。そのため、不審なメールに気付いた人は、組織で定められている運用ルールに従い速やかに情報集約窓口に報告することが重要である。また、組織内に限らず組織間においても同様に、情報を共有することで複数の組織で被害の拡散防止と予防が可能なため、情報共有は標的型攻撃における重要な対策であると言える。

IPA では、標的型サイバー攻撃に関して専門的知見を有する相談員が対応する「標的型サイバー攻撃の特別相談窓口[16]」を設置し、相談を受け付けているので、不審なメールを発見した場合は、ぜひご連絡をお願いしたい。

IPA では、今後も継続して標的型サイバー攻撃に関する情報を収集・分析し、関係各機関と連携し、安心して情報システムが利用できる社会を目指す所存である。

最後に、本書が我が国の標的型サイバー攻撃の被害低減の一助になれば幸いである。

16 標的型サイバー攻撃の特別相談窓口：https://www.ipa.go.jp/security/tokubetsu/

5. 参考資料

IPA がウェブに公開している標的型攻撃メールに関する資料を以下に示す。

【標的型攻撃メール関連、及び事例分析】

① テクニカルウォッチ「標的型攻撃メールの傾向と事例分析＜2013 年＞」
https://www.ipa.go.jp/security/technicalwatch/20140130.html

② テクニカルウォッチ「フリーメールからの送信が増加傾向に：最近の標的型攻撃メールの傾向と事例分析」
https://www.ipa.go.jp/about/technicalwatch/20121030.html

③ テクニカルウォッチ「標的型攻撃メールの分析」
https://www.ipa.go.jp/about/technicalwatch/20111003.html

④ 「標的型サイバー攻撃の事例分析と対策レポート」
https://www.ipa.go.jp/about/press/20120120.html

⑤ 「東日本大震災に乗じた標的型攻撃メールによるサイバー攻撃の分析・調査報告書」
https://www.ipa.go.jp/about/press/20110929_2.html

⑥ 「標的型メール攻撃」対策に向けたシステム設計ガイド
https://www.ipa.go.jp/about/press/20130829.html

【標的型攻撃の組織への普及・啓発】

① 動画「あなたの組織が狙われている！～標的型攻撃 その脅威と対策～」
https://www.ipa.go.jp/security/keihatsu/videos/

② 対策のしおり「標的型攻撃メール＜危険回避＞対策のしおり」
https://www.ipa.go.jp/security/antivirus/shiori.html

③ 2014 年版「10 大脅威」
https://www.ipa.go.jp/security/vuln/10threats2014.html

【標的型攻撃への対策】

① テクニカルウォッチ「攻撃者に狙われる設計・運用上の弱点についてのレポート」
https://www.ipa.go.jp/security/technicalwatch/20140328.html

② 「サイバー情報共有イニシアティブ（J-CSIP）2013 年度 活動レポート」
https://www.ipa.go.jp/about/press/20140530.html

③ 講演資料「標的型サイバー攻撃の脅威と対策」
https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1.pdf
https://www.ipa.go.jp/security/event/2013/isec-semi/documents/2013videosemi_targeted_cyber_attacks_v1a.pdf

④ 講演資料「標的型攻撃／新しいタイプの攻撃の実態と対策」
https://www.ipa.go.jp/files/000024542.pdf

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」

［発　　行］2015 年 1 月 9 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］岡野 裕樹　　木邑 実　　辻 宏郷　　青木 眞夫