

## 情報詐取を目的として特定の組織に送られる不審なメールの相談窓口

### 「不審メール 110 番」を設置

独立行政法人情報処理推進機構(略称:IPA、理事長:西垣 浩司)は、最近増加している「情報詐取を目的として特定の組織に送られる不審なメール」、いわゆる標的型攻撃メールを受信した組織が情報詐取などの実被害に遭わないよう、相談窓口「不審メール 110 番」を9月29日に設置しました。

「不審メール 110 番」では、不審なメールを受信した組織や、送信元をかたられた組織が、どのような対応をすべきかなどの相談を受け付けます。また、標的型攻撃メール対策を推進するため、受信した不審なメールに関する情報の積極的な提供を呼びかけています。

IPAは、「不審メール 110 番」に提供された不審なメールの情報を分析し、ユーザへの注意喚起や対策方法の公表、セキュリティ対策ソフトベンダへのウイルス情報の提供のほか、ウイルス感染に利用されたソフトウェア製品の脆弱性情報についての早期警戒パートナーシップとの連携などを通じ、標的型攻撃メール対策を推進していきます。

### ■「不審メール 110 番」で受け付けた不審なメールの取り扱い

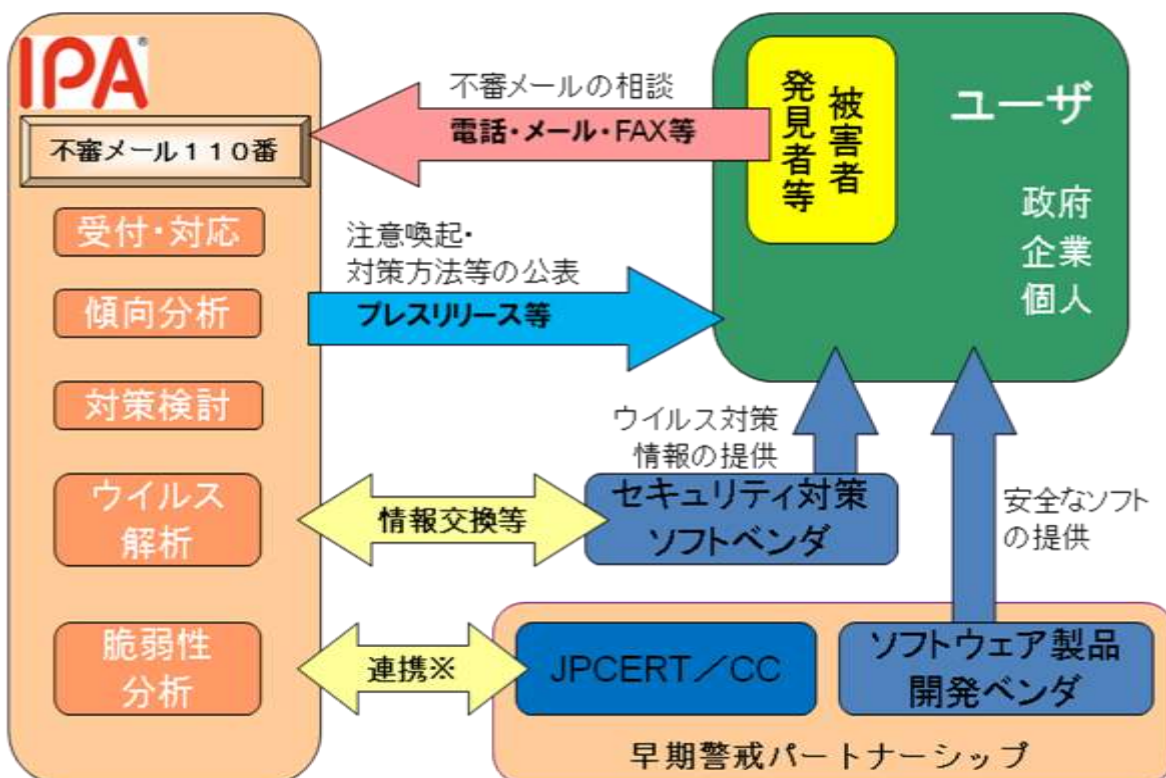


図1. 情報詐取を目的として特定の組織に送られる不審なメールの取扱いイメージ<sup>1</sup>

<sup>1</sup>必要に応じて情報システムの脆弱性対策の取り組み(早期警戒パートナーシップ)を活用

## ■不審なメールに関する情報提供のお願い

- ・不審なメール<sup>2</sup>を受信した組織は、まず送信者の組織に問合せ、正規のメールであるかを確認します。正規のメールでないことが確認された場合は、「不審メール 110 番」に連絡してください。
- ・「不審メール 110 番」が、当該不審メールを調査する必要があると判断した場合は、相談窓口の担当者が専用メールアドレスを個別に連絡しますので、不審なメールを添付し送信してください。

## ■「不審メール 110 番」窓口

### (1) 電話による相談窓口

TEL: 03-5978-7509

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

### (2) 電子メールまたはファクシミリによる相談窓口

E-mail: [fushin110@ipa.go.jp](mailto:fushin110@ipa.go.jp)

FAX: 03-5978-7518

対応時間: 24 時間受付

## ■参考 URL

- ・情報詐取を目的として特定の組織に送られる不審なメールの相談窓口「不審メール 110 番」  
<http://www.ipa.go.jp/security/virus/fushin110.html>
- ・IPA を騙った「なりすましメール」にご注意ください  
<http://www.ipa.go.jp/security/topics/alert20080416.html>
- ・「近年の標的型攻撃に関する調査研究」調査報告書の公開について  
<http://www.ipa.go.jp/security/fy19/reports/sequential/>
- ・情報セキュリティ早期警戒パートナーシップガイドライン  
[http://www.ipa.go.jp/security/ciadr/partnership\\_guide.html](http://www.ipa.go.jp/security/ciadr/partnership_guide.html)

### ■ 本件に関するお問い合わせ先

独立行政法人 情報処理推進機構 セキュリティセンター 小門／木邑

Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: [isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp)

### ■ 報道関係からのお問い合わせ先

独立行政法人 情報処理推進機構 戦略企画部 広報グループ 横山／大海

Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: [pr-ing@ipa.go.jp](mailto:pr-ing@ipa.go.jp)

<sup>2</sup> ここでいう不審なメールとは、実在の企業名や官公庁名をかたって、特定の組織に添付ファイル付きのメールを送り、その添付ファイルを開くとその組織の情報を盗むウイルスなどに感染させられるものをいいます。不特定多数に送られるウイルスメールや広告メール、フィッシングメールは除きます。不審なメールの特徴と被害例については別紙 1 を、不審なメールが届いた場合の対応については別紙 2 をご覧ください。

## 別紙1. 不審なメールの特徴と被害例

### ■「情報詐取を目的として特定の組織に送られる不審なメール」の特徴

次のように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。

- ① メールを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

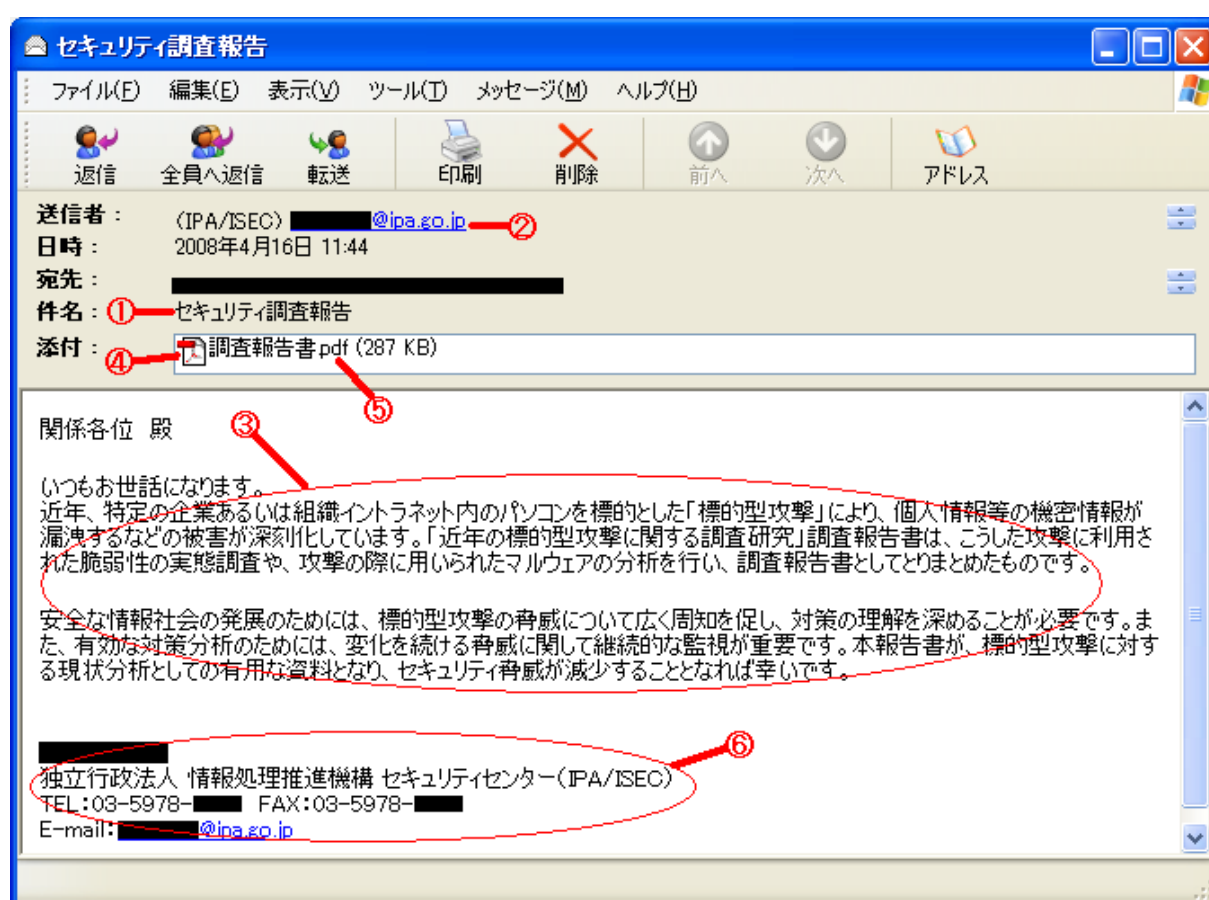


図 2. 2008 年 4 月 16 日に、IPA をかたって政府関係組織に送られたメール例

### ■不審なメールの添付ファイルを開いた場合に想定される被害例

- ・ PDF リーダやワープロソフトなど、添付ファイルを開くために必要なアプリケーションに存在する脆弱性を利用して、不正なプログラムがパソコンにダウンロードされます。
- ・ 当該パソコン内にあるファイルを外部に送られ、情報漏えいします。
- ・ キーロガー(\*1)を仕掛けられ、パソコンで入力した ID やパスワードを盗まれます。
- ・ 外部から、当該パソコンを乗っ取り、組織内のサーバに不正アクセスされます。

注(\*1) キーロガー とは、キーボードから入力された情報を記録するプログラムです。

## 別紙 2. 不審なメールが届いた場合の対応

### ■不審なメールを発見した場合の対応

(1) 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、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、問い合わせてください。その結果、そのような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してください。

(2) 自分が送信していない添付ファイル付きメールについて問合せを受けた場合は、送信者アドレスを詐称された単なる迷惑メール(\*2)や一般のウイルスメールでないか確認し、「情報詐取を目的として特定の組織に送られる不審なメール」と判断された場合は、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するとともに、必要に応じて自組織のホームページなどで外部に注意喚起してください。

【参考】IPA をかたった「なりすましメール」にご注意ください

<http://www.ipa.go.jp/security/topics/alert20080416.html>

(3) 自分が送信していない添付ファイル付きメールが、配信エラーなどで戻ってきた場合も、(2)に準じてください。

注(\*2) 単なる迷惑メールを受信した場合の情報提供先は次の通りです。

・出会い系サイトの紹介や商品売り込む広告メール

⇒ 【参考】情報提供先：日本産業協会 迷惑メール情報提供受付

<http://www.nissankyo.or.jp/spam/>

⇒ 【参考】情報提供先：データ通信協会 迷惑メールの情報提供

<http://www.dekyo.or.jp/soudan/ihan/>

・銀行などをかたって個人情報詐取するフィッシングメール

⇒ 【参考】情報提供先：フィッシング対策協議会 フィッシング事例の情報提供

<http://www.antiphishing.jp/report-phishing-mail.html>

## ■不審なメールの添付ファイルを開く場合の注意点

(1) 実在の官公庁や有名な企業などから送ってきたメールであっても、普段から添付ファイル付きのメールをやりとりしている相手でない場合は、極力添付ファイルについて送信者に問合わせて、どのような添付ファイルか確認してから開いてください。

(2) 営業部門や問合せ対応部門など、不特定者からのメールを受信せざるを得ない業務を行っている部署においては、万が一添付ファイルがウイルスであっても被害が最小限になるように、例えばインターネットに接続していない専用パソコンを使うことをお勧めします。

(3) 情報詐取を目的として特定の組織に送られる不審なメールに仕込まれるウイルスは、不特定多数に送られるウイルスメールと違い、一部のウイルス対策ソフトでしか検知されないことが多いため、添付ファイルを開く前に複数のウイルス対策ソフトで検査することが有効となります。

【参考】 VirusTotal 無料オンライン ウイルス／マルウェア スキャン

<http://www.virustotal.com/jp/>

(4) 添付ファイルがワープロ文書や PDF ファイルのようなデータファイルの場合、それらのファイルを表示するためのアプリケーションソフト（例えば、一太郎、ワード、パワーポイント、AdobeReader、画像表示ソフト、圧縮解凍ソフト、メールソフト、FlashPlayer など）の脆弱性(\*3)を利用してウイルス感染することが多いので、最新版のアプリケーションソフトを使うことが感染被害に遭わないために有効となります。

注(\*3) セキュリティ上の「脆弱性」とは、ソフトウェア製品において、ウイルスや不正アクセス等の攻撃により、その機能や性能を損なう原因となりうる安全性上の問題箇所です。ネットワーク攻撃に利用される可能性があるという点において、通常の不具合と区別されます。

## ■知っておいてもらいたいこと

ウイルス被害に遭わないためには、正しい知識を身につけることが重要です。

- ・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ある。
- ・ワープロ文書など実行形式でない添付ファイルから感染するウイルスもある。
- ・他人のメールアドレスを詐称することは簡単である。(電子署名の常用が望まれる)
- ・ウイルス対策ソフトに検知されないウイルスもある。
- ・脆弱性の修正プログラムが提供される前に、それを悪用するウイルスもある。
- ・情報を詐取するタイプのウイルスに感染した場合、画面に不審な表示がでるとか、パソコンがダウンするなどの目に見える症状は出ないことが多い。