JPCERT CC®

標的型攻撃対策手法に関する調査報告書

有限責任中間法人 JPCERT コーディネーションセンター

2008 年 8 月 7 日

JPCERT CC®

序

近年、インターネット上で観測されるセキュリティインシデントの中で、特にその脅威が取りざたされているのが、標的型攻撃（Targeted Attack）である。標的型攻撃はその名のとおり、特定組織に攻撃の対象を限定する。従来のような不特定多数に対して無差別に攻撃を行う手法とは異なり、外部からその攻撃の試み及び被害の実態を窺い知ることが難しいのが特徴である。そこで、JPCERT コーディネーションセンター（以下「JPCERT/CC」という。）では、国内企業を対象にアンケート調査を行い、2007 年 3 月、標的型攻撃に関する実情を報告書にまとめた。その結果、6.4%の企業等が過去 1 年間に標的型攻撃を受けたことがある[1]という結果が得られた。国内においても、標的型攻撃の脅威が過去数年の間に増加していることが明らかとなったわけである。

このような背景を踏まえ、JPCERT/CC では、標的型攻撃の実態を公開文献と国内組織へのヒアリングによって調査し、その内容に即した効果的な対策手法を報告書としてまとめることとした。

本報告書が、企業/組織における標的型攻撃対策を検討する際の手助けとなれば幸いである。

なお本報告書の作成にあたってヒアリングに快くご協力いただいた各企業、組織に対しこの場を借りて御礼を申し上げたい。

2008 年 8 月
有限責任中間法人 JPCERT コーディネーションセンター

[1] JPCERT/CC 『標的型攻撃についての調査』
http://www.jpcert.or.jp/research/2007/targeted_attack.pdf

JPCERT CC®

目次

1. はじめに

本章では本標的型攻撃対策報告書の目的、適用範囲など本報告書に関する概要を記す。

1.1. 本報告書の想定読者と目的

本報告書は、企業等のシステム管理者及びセキュリティ管理者などの技術者を対象に、1)標的型攻撃の実態についての理解を助けること 及び 2)標的型攻撃の具体的対策手法を紹介すること 3)対策手法の 1 つである「予防接種」について紹介することを目的としている。

「予防接種」については倫理的な懸念からセキュリティ対策として企業において実施された例がすくない。そのため本文書では具体的な実施手段も含めて説明を試みる。

1.2. 用語解説

本報告書で扱う用語の意味を以下に示す

標的型攻撃

情報セキュリティ上の攻撃で、無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的としたもの。特定の組織あるいはグループに特化した工夫が行われることもある。

標的型メール攻撃

標的型攻撃の一種。特定の受信者に対してウイルス付きのメールを送ること。この場合、件名や文面も受信者にカスタマイズされている。海外では”Targeted Trojan Attack”などと呼ばれる。

スピアフィッシング

標的型攻撃の一種。特定の個人、小規模な集団に対してフィッシングを行うこと。具体的には以下のようなケースがこれにあたる。
特定の企業の社員を対象に、その企業独自の年金管理サイトのパスワード入力を迫るフィッシング

企業の CEO、CFO のみを対象に個人情報を入力するよう迫るフィッシング

2. 標的型攻撃の現状

本章では調査の結果から近年の標的型攻撃の現状を解説し、既存の標的型攻撃対策の攻撃の問題を考える。

2.1. 標的型攻撃の現状

公開文献での調査、並びに国内のセキュリティベンダー、企業、官公庁へのヒアリングから浮かび上がる近年の標的型攻撃の現状は、以下の通りにまとめることができる。

標的型メール攻撃が多い
確認されている攻撃の多くにおいては、メールの文面や添付ファイルの名前が各組織を狙ったものにカスタマイズされている。そのカスタマイズのレベル(巧妙度)は、攻撃によりまちまちである。対してスピアフィッシングその他の標的型攻撃は数が少ない、もしくは攻撃が認知されていないため、本調査では実際にインシデントが発生したという情報を得られなかった。

攻撃対象となりやすいのは政府関連組織や特定の製造業などである
ただし、JPCERT/CC のヒアリング調査は全業種に対して行ったものではなく、また、そもそも標的型攻撃を受けたことに企業が気づいていないケースもあり得ると考えられる。

攻撃に使用される添付ファイルはビジネスアプリが多い
PDF ファイル、MS Office 文書(Word, Excel, PowerPoint)、JustSystems 一太郎文書など、企業などが業務で必要とするいわゆるビジネスアプリケーションの脆弱性が利用されることが多い。

ウイルス対策ソフトで検知不可能なケースもある
標的型メール攻撃に添付されたファイルが最新のウイルス検知ソフトで検知されなかったというケースがあった。さらに、いわゆる「ゼロデイ」脆弱性が攻撃の対象となるケースもある

添付ファイルを開いてしまった場合、情報漏洩が起こる
PC 上で動作するソフトウェアの脆弱性が密かに攻略され、キーロガーやバックドアが稼働し、特定のサーバに対して PC 上で取得した情報を送信しようと

する。

2.2. 対策の問題点

標的型メール攻撃は、対象のユーザや組織について個別化され、特徴づけられたものであるため、多様性が大きい。そのためユーザ自身が個々の攻撃に対して正しく対応できるようになる必要がある。

多くのケースにおいて、標的型攻撃は特定組織の極少数を狙うものであった。被害拡大を防ぐためにも、少数名が攻撃を受けたという事実を速やかに組織内に展開する情報網が必要である。またその情報を国内の同業種の他企業と迅速に共有することができれば、国内での標的型攻撃対策に大いに資すると思われる。

3. 技術的な対策および緩和方策

技術的な対策の不備ばかりでなく、組織内のユーザの心理的盲点をも狙う標的型攻撃の被害を緩和するためには、3 つの側面からの複合的な対策を実施することが望まれる。

1. 攻撃を察知するのを助ける技術的対策
   より巧妙になる攻撃をユーザが判別するための判断材料を提供する技術的な対策を導入する必要がある。たとえば、従来であればウイルス検知ソフトやネットワーク境界に設置されたファイアウォールで攻撃を検知、遮断することが可能であったが、標的型攻撃に対してはそれだけでは不十分である。より高い精度で標的型攻撃を検知する手法を考えたい。
2. 被害を最小範囲に留める仕組み
   攻撃を察知する技術的対策を徹底しても、一定の割合で悪意のある添付ファイルを開いてしまうユーザがいることが予想される。従ってファイル開封/マルウェア実行による被害を限定的にするために正しい対応をとる必要がある。
3. ユーザ教育
   ユーザー人一人が攻撃に気づき、危険を避け、情報を組織内に報告・共有するためには 1)怪しいメールの見分け方、2)そのようなメールを受け取った際に取るべき対応について事前に組織内に周知しておく必要がある。

以降では、各項の具体的な内容について紹介する。

3.1. 攻撃を察知する技術的な対策

3.1.1. 送信ドメイン認証

標的型攻撃のメールでは送信者の詐称が行われる場合が多い。送信ドメイン認証は受信側のメールサーバでメールの送信ドメインを検証することで送信者の詐称を見抜くことを容易にする技術である。標的型攻撃の成立を難しくする緩和策としての性格を持つと言える。SPF/Sender ID、DKIM の方式がある。

SPF/Sender ID

SPF（Sender Policy Framework）は、送信ドメイン認証に利用される技術

手法のひとつであり、送信元の IP アドレスの確認に基づく手法である。SPF は IETF の Network Working Group において検討され、SPF Version 1 の仕様は RFC4408 に示されている 。

送信側はメールを送信するサーバを示す情報（SPF レコード）としてメールサーバのドメインと送信 IP アドレスの関連を DNS サーバ上に公開する。受信側では、SMTP 接続中に得られる送信側ドメイン情報と DNS サーバ上の SPF レコードとの整合性をチェックし、そのメールが正当なメールサーバから送信されたものかを判別する。

メールを送信するサーバを示す情報（SPF レコード）としてメールサーバのドメインと送信 IP アドレスの関連を DNS サーバ上に公開する。受信側では、メールのエンベロープに書かれた From アドレスから得られるメール送信者ドメインと DNS サーバ上の SPF レコードとの整合性をチェックし、そのメールが正当なメールサーバから送信されたものかを判別する。

公開された SPF レコードを確認することで、そのメールサーバから送信されたと自称するメールに関して送信元を詐称しているか否かを判別することができる。

送信側における SPF への対応は、DNS サーバ上で SPF レコードを公開するだけで対応可能である。主要な DNS サーバは改変無しに SPF レコードが記述できることもあって、対応は比較的容易と言える。携帯電話各会社やウェブメールを持つ大手ポータルサイト等のドメインにおいても既に実装されている。

WIDE プロジェクトによる調査 によれば、2008 年 3 月の時点で.jp ドメインにおける SPF への対応率は 18.7%と示されている。

SPF に実効性を持たせるためには、受信側において実際に検証を行うことが重要である。SPF 対応ドメインからのメールを優先的に受信する等の対処も ISP 事業者において行われ始めている。

DKIM

DKIM（DomainKeys Identified Mail）は、送信ドメイン認証に利用される技術手法のひとつであり、送信されるメールの電子署名の確認に基づく手法である。DKIM の仕様は RFC4871 に示されている。

DKIM においては、あらかじめ公開鍵を DNS に設置し、ドメイン情報が含まれるメールヘッダに電子署名を付与して送信する。メールを受け取ったサーバでは、ドメイン情報を基に DNS に問合せを行い、公開鍵を取得して署名を検証する。検証にパスした場合には正しい送信者とみなしてメールを受け取る。

DKIM の元となった送信ドメイン認証の手法には米 Yahoo!社が提案した DomainKeys(RFC4870)があり、現在 Yahoo!、Gmail などのフリーメールサービ

スでも利用されている。DKIM では更に送信ドメイン側で署名検証に失敗したメールを破棄して良い、というステートメントを公開することが可能となる Author Domain Signing Practices (ADSP)などについても、仕様が検討されている。

WIDE プロジェクトにおける調査によれば 2008 年 3 月の時点で.jp ドメインにおける DKIM/DomainKeys への対応率は 0.27%と示されている。

3.1.2. メッセージ署名

メッセージへの署名はメールの出所を確認可能とする。送信時に署名を付け、受信時にメッセージの発信者を確かめることを習慣づければ、送信者詐称による被害を抑止する効果が期待できる。メールのメッセージに署名を施す技術としては S/MIME、PGP が知られている。

S/MIME

S/MIME とは、電子メールのセキュリティを向上させるための技術のひとつであり、デジタル署名によるメールの作成者の検証と本文の改ざん検知、メッセージの暗号化によるデータの秘匿性向上を可能とする。

S/MIME は、メールの送受信者におけるエンドツーエンドのセキュリティを提供するものであるが、送受信者が利用可能な PKI 環境の存在が活用の前提となる。送信者は S/MIME を利用するために、信頼できる電子認証局から発行された電子証明書を、事前に所有している必要がある。S/MIME の信頼性は証明書を発行した認証局の信頼性に依存しており、不特定多数との信頼性の高いメール送受信を行ないたい場合に向いている。

S/MIME は IETF において、RFC3850、RFC3851、RFC3852 として標準化されている。

PGP

PGP は暗号化／デジタル署名のアプリケーションとして開発されたものである。オープンソースのソフトウェアとして普及したが、商用利用について制限があるため、オープンな仕様として Open PGP が提示され、有名な実装として GnuPG（GNU Privacy Guard）が開発されている。

公開鍵暗号方式を利用する上では、メッセージの正当な送信者の公開鍵を信頼できるような仕組みを作る必要があるが、PGP においては、PKI のような中心となる第三者機関を持つ構造ではなく「信頼の輪」という利用者の相互扶助

的な構造を基本としている。
PGP のオープンな仕様である OpenPGP は IETF より RFC2440[2]に示されている。この仕様に準拠した実装としては例えば GnuPG が有名である。

一般的に普及が難しいメッセージ署名であるが、標的型攻撃を防ぐという観点から今後その重要性は増すと思われる。特に顧客など不特定多数へのメール送信を行う企業においては、自社を騙った標的型攻撃だけでなく、スパムメールやフィッシング対策としてもメッセージ署名の導入を検討すべきである。

3.1.3. メールサーバでの添付ファイルの制限

2.1 「標的型攻撃の現状」で述べたとおり標的型メール攻撃で用いられる添付ファイルの拡張子つまり脆弱性を狙われるアプリケーションの種類は限定されている。従ってメールサーバでこれらの特定の種類の添付ファイルを受信した際に添付ファイルだけを削除するという対応が考えられる。例えば、2007 年度には Microsoft Access 形式(拡張子が mdb のファイル)が標的型攻撃に用いられた。多くの企業においては、通常、メールで mdb ファイルをやり取りする必要は少ない。つまり、事前に外部から受け入れるメール添付ファイルを制限するという方法が有効と思われる。

3.1.4. OFFICE 2007 を利用する

Microsoft Office はビジネスユーザへの普及度が高く、従って標的型攻撃に利用される可能性の高いアプリケーションの 1 つである。
OFFICE 2007 では、標準の文書ファイルフォーマットとして OpenXML フォーマットが採用された。このフォーマットでは Office 2003 及びそれ以前のバージョンで用いられていた独自バイナリ形式のファイルフォーマットと比較すると攻撃コードをドキュメント中に埋め込むことが難しくなっている。

3.1.5. MOICE を利用する

既存の環境から OFFICE 2007 への移行が難しい場合、各端末に MOICE を導入するという方法が有効である。

---

[2] 2007 年 11 月に RFC2440 を改訂した RFC4880 が公開されている。
http://www.ietf.org/rfc/rfc4880.txt

MOICE [3]は、Office 2003 のファイルを新しい Office 2007 の Open XML フォーマットに変換する。万一、開こうとした文書が攻撃コードを含むものであった場合、MOICE がファイルの変換を完了できない、あるいはコンバーターが不正終了するため、ユーザがそのファイルが危険なものであることを認識することができる。

3.2. 被害を最小範囲に留める仕組み

3.2.1. ソフトウェアの脆弱性対策

標的型攻撃においては、特に、PC で用いられるブラウザ、メールクライアント、オフィススィート等のアプリケーションソフトウェアの脆弱性が狙われる。標的とされる組織において用いられる特定のソフトウェアの脆弱性をつく攻撃が行われた事例も報告されている。組織内で利用するアプリケーションに関する修正プログラムを積極的に適用することは標的型攻撃による被害の未然防止のために最も基本的克つ有効な対策となる。特に 2007 年に多く攻撃に利用されたことが確認されている下記アプリケーションについてはバージョン管理を徹底するべきである。

- Microsoft PowerPoint
- Microsoft Word
- Microsoft Excel
- Adobe Acrobat
- Adobe Reader
- JustSystems 一太郎

3.2.2. 通信の監視と制限

標的型攻撃により PC にインストールされるマルウェアについての解析結果によると[4]、インターネット経由で攻撃者と通信を行う機能を持つ事例が確認されている。解析結果により得られる知識に基づいたトラフィック監視を行うことができれば、攻撃者による通信を遮断し被害の発生を防止することが可能であ

[3] Microsoft Office Isolated Conversion Environment (MOICE) および Microsoft Office 向けファイル ブロック機能の公開
http://www.microsoft.com/japan/technet/security/advisory/937696.mspx
[4] 近年の標的型攻撃に関する調査研究
http://www.ipa.go.jp/security/fy19/reports/sequential/index.html

る。ただし前提となる最新のマルウェアに関する解析は高度な技術を持つ専門家を必要とするため実現は難しい。
そのため一般企業においては、PC から外部ネットワークへのアクセスをプロキシサーバ経由に限定し、さらにプロキシサーバの利用にパスワードによる認証をかけるという対策が考えられる。

3.2.3. ファイルを開くための専用マシン

標的型メール攻撃で送信されるメールは、受信者の業務や役職の情報を用いて巧妙に偽装されている。そのため、最終的に実際に添付ファイルを開いてみないと、それが攻撃なのか正規のメールであるのか判別できない場合が十分に考えられる。また、営業部門などは日常的に不特定多数からメールを受け取る場合が多く、それを開封しないと業務に支障が生ずる可能性も否定できない。

このような場合には個人情報や業務上の機密情報などが保存されていない、添付ファイル確認のための専用端末を持ち、添付ファイルの確認はその専用端末を利用することを検討するとよいであろう。

なお、VMware などの仮想テクノロジを使用して、仮想 OS 上でファイルを開くというのも、この項の応用手段として有効である。

3.2.4. 社内外との情報共有

標的型攻撃は特定組織の極少数を狙うものであることが多い。そして攻撃は同業種の他社でも同じ手口で行われることがある。そのため攻撃を受けたという事実を速やかに展開する情報網が整備されていないと、同様の手口で組織内の別の部署/セクションあるいは同業他社が被害にあうおそれがある。

このような被害を防ぐためにも、企業内に情報セキュリティインシデントに対する連絡と情報共有体制を構築する必要がある。企業内に CSIRT というセキュリティ対応組織を設けることを推奨したい。これは、世界中の様々な組織において CSIRT が情報セキュリティインシデントへの対応を目的として活動してきた長年の実績があり、その活動を通じて蓄積されたノウハウが流用可能だからである。

また JPCERT/CC は標的型攻撃手法についての調査を継続して行っており、インシデント報告[5]を受け付けている。

---

[5] JPCERT Coordination Center “インシデント報告の届け出”
http://www.jpcert.or.jp/form/

3.3. ユーザ教育

標的型メール攻撃に対しては、メールクライアントやブラウザのウィンドウにおいて脅威と対峙するユーザの判断力が、被害発生を大きく左右する要素となる。

現状のウイルス対策ソフトなどが、常に行われているマルウェアの巧妙化を後追いする性質であるため、ユーザへの意識啓発や教育に基づく被害防止への期待は以前より高まっているといえる。

3.3.1. “不審な”メールの見分け方

標的型メール攻撃においては攻撃者による偽装メールを見破ることができれば被害を未然に防ぐことが可能である。そして標的型メール攻撃を見分けるためには、事前にユーザに対して開いてはいけないメールの条件を伝える必要がある。この条件については組織の文化や業務の事情によって異なってくるため、一概に基準を設けることはできない。ここでは一般的な不審なメールの条件を列挙する。各組織の事情に応じて取捨選択して、周知していただきたい。

(1) 日頃メールのやり取りのない企業からのメール

(2) 日頃メールのやり取りのない組織幹部からのメール

(3) 無料 Web メールアカウントからのメール

(4) 件名、本文、添付ファイル名の日本語が拙い、漢字の選び方が間違っているメール

(5) 本文中に部署や電話番号を記した署名がない（ここでの署名とは電子署名ではない）メール

(6) 件名に「緊急」など、ことさらに添付ファイル開封を促すメール

(7) 日頃メールでやり取りすることの無い種類のファイルが添付されているメール

3.3.2. 予防接種

予防接種は、擬似的な標的型攻撃を組織に属する個人に対して行うことで、脅威への理解とセキュリティ意識向上を図る演習手法の一種である。ユーザに

不審なメールの特徴を教育する手法には様々な形態が考えられる。たとえば社内メーリングリストなどを使った告知、掲示板、集合研修、e ラーニングなどである。予防接種には、これらの既存の教育手法と比較すると、より個人の判断力が詳らかになるなどのメリットがある。予防接種の概要と詳細については、4 章で詳しく述べる。

4. 予防接種によるセキュリティ意識向上

既存のウイルス対策やメール・フィルタリングを潜り抜ける標的型攻撃に対しては、メールクライアントやブラウザを扱うエンドユーザの判断が、被害防止を大きく左右する要素となる。

ここでは、エンドユーザにおける脅威への理解とセキュリティ意識向上の効果的な方策として、「予防接種」という手法を、実際に実施した訓練に基づきながら、紹介する。また、小規模な組織を対象とした訓練の実施手順と留意点について解説を試みる。

4.1. 予防接種手法の概要

4.1.1. 目的

予防接種手法とは、電子メールを用いた受動型攻撃に対する、エンドユーザのセキュリティ意識の向上と組織としての対応力の向上を目的とする調査・訓練の手法で、対象者に不審メールを模した無害なメールを送付し、各対象者が適切な取扱いを行えるか否かを確認するものである。

エンドユーザに実際の脅威を模したメール（ダミーメール）を受信させ、取扱いを体験させることで、企業内ユーザを狙うメールを用いた攻撃に対する危機意識を向上させ、適切な対処方法に関する理解を促す。メールによる標的型攻撃においては、対象組織に特有の固有名詞、話題や関心事が本文や件名等に含まれ得る点に着目し、これらを考慮したダミーメールを用いる。

エンドユーザが不審なメールを受信したした際には、本来であれば、添付ファイルを開かずに破棄することや、組織内の情報セキュリティ担当者に問い合わせることが望まれる。訓練では、添付ファイルを開く等の被害に繋がりうる取り扱いを行った対象者に、取扱いについて注意を喚起し、適切な対応を理解させる

予防接種手法の実施(調査・訓練)を通じてセキュリティ関連事象に関する組織内の連絡・連携の実態を確認し、強化を図ることも可能となる。

4.1.2. 想定する脅威

実際に実施した訓練においては、脅威として、企業ユーザに宛てた標的型メ

ール攻撃を想定した。この攻撃は、通常は、電子メールの本文で社内外の関係者から受信者に送られた連絡を装い、添付ファイルを参照するように受信者を誘導する。実際の攻撃では、ユーザが PC 上で添付ファイルを開いた際にアプリケーションの脆弱性をつかれて不正なプログラムが実行される可能性がある。

予防接種訓練では、関係者からの連絡を装う内容の電子メールに、「無害な」添付ファイルをつけて送信し、メールを受信した対象者がこの添付ファイルを開いたか否かの記録を採り、開いてしまった対象者に対しては、事後、同様なメールについて適切な取扱いを行うよう促す。

4.2. 実施例

小規模な組織において予防接種手法による訓練を行う場合の手順を、以下に説明する。

4.2.1. 実施体制

今回実施した訓練においては、実施体制を以下のように想定した。

役割名		人数	解説
実施担当	連絡担当者	1～2 名	対象者の集団に所属している IT／セキュリティ担当者など。主に事前事後の調整および対象者への説明を行う。
	送信担当者	1～2 名	情報セキュリティの専門的知識を持つ者。主に実施計画、準備、訓練メール送信、結果の収集と分析を行う。
対象者		10～30 名程度	一般の職員を想定する。

4.2.2. 実施項目

訓練の効果を測定するとともに、正しい取り扱いについての理解を定着させるという観点から、訓練については、少なくとも 2 回、1 週間から 2 週間程度の間隔を置いて実施するのが望ましい。

実際に実施した訓練では、同一の対象者への訓練回数は 2 回とし、およそ 2 週間の間隔をおいて実施した。いずれも、対象者には訓練であることを伝えず、

抜き打ちでメールを送付する。
　全体手順および実施する項目を図 4-1に示す。

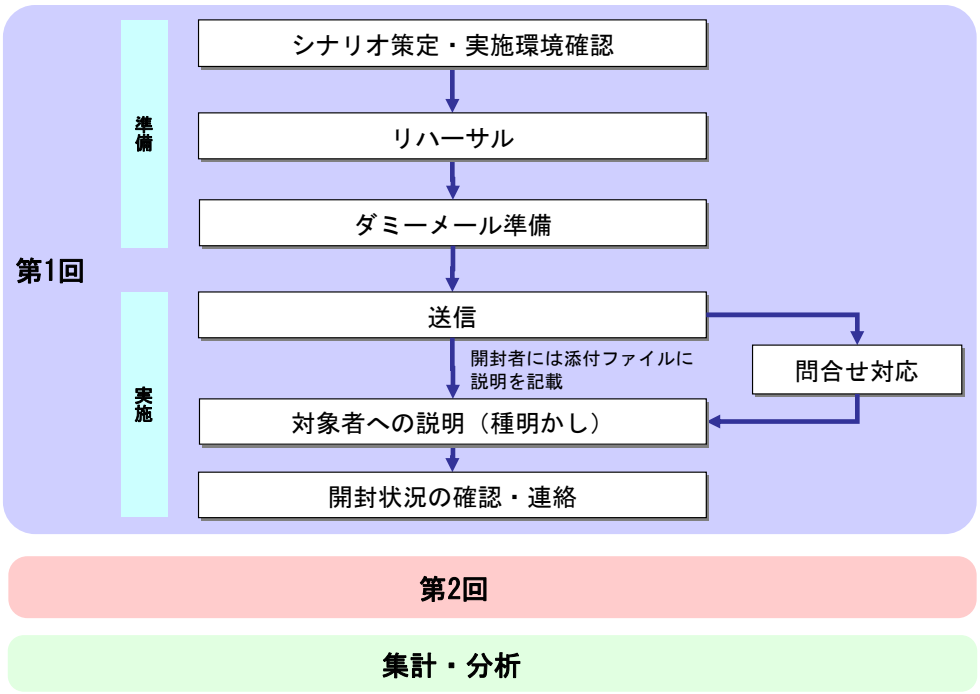


図 4-1　予防接種手法の実施フロー

4.3. ツール

　調査・訓練に用いるツール一式について、以下に説明する。

4.3.1. ダミーメール

　対象者に送付する攻撃を模したメールをダミーメールと呼ぶ。
　ダミーメールはテキスト形式のビジネスメールを装い、添付ファイルとして MS Word ファイル形式（拡張子：.doc）のファイル 1 つを付ける。
　ダミーメールを受信した対象者は、メールの送信者、メール本文、件名、添付ファイル名をもとに取り扱いに関する判断を行う。これらのダミーメールの要素の作成方針について以下に示す。

- 一読して若干の違和感を覚える程度のやや怪しげな文面を作成する。次のような気付きのポイントを幾つか含める。
  - 送信元メールアドレスが、文面の内容から通常想定されるメールアドレスとは異なったものになっている。
  - 送信元メールアドレスが、フリーメール等の初めて見るメールアドレス(見知らぬメールアドレスから来たメール)になっている。
  - 対象者のレベルにもよるが、一般ユーザを対象にする初期の訓練においては、送信元アドレスは詐称しない。

- メールのタイトルや本文中に、対象者の知識に合わせた固有名詞等をいくつか含める。

- 対象者のレベルにもよるが、実際に送られた正当なメールを元にして似せて作成したり、あるいは、対象者について詳細な情報を入手したりする等の方法でダミーメールを作り込むことは避ける。判別を極端に難しくすると、対象者の警戒心や判断力に関する現在の状況を知ることができないだけでなく、「自分には対処不能」という印象を残してしまい、訓練による意識向上の効果を期待できないからである。

実施に先立つ準備段階において、5～6 例程度のサンプルを作成した上で、担当者間で打合せを行い、これらのうちから第 1 回および第 2 回に用いる文面の素材を選び、適宜修正を行って用いるのがよいであろう。

付録として、試行で用いたサンプル文面案を示す。

4.3.2. 添付ファイルオープン状況を記録する方法

実際に実施した訓練では、ダミーメールの添付ファイルとして MS Word 形式ファイルを用いた。ユーザが、この添付ファイルを MS Word で開くと想定する。

ファイルオープン時にはウェブサーバ上の画像を文書ウィンドウ上に表示させる。ウェブサーバでは画像へのアクセスがログとして残る。各ユーザに送付する添付ファイルにおいて、それぞれ異なる画像へのアクセスを発生させ、Web サーバに残るアクセスログから添付ファイルを開いた対象者を特定する。

概要を図 4-2に示す。

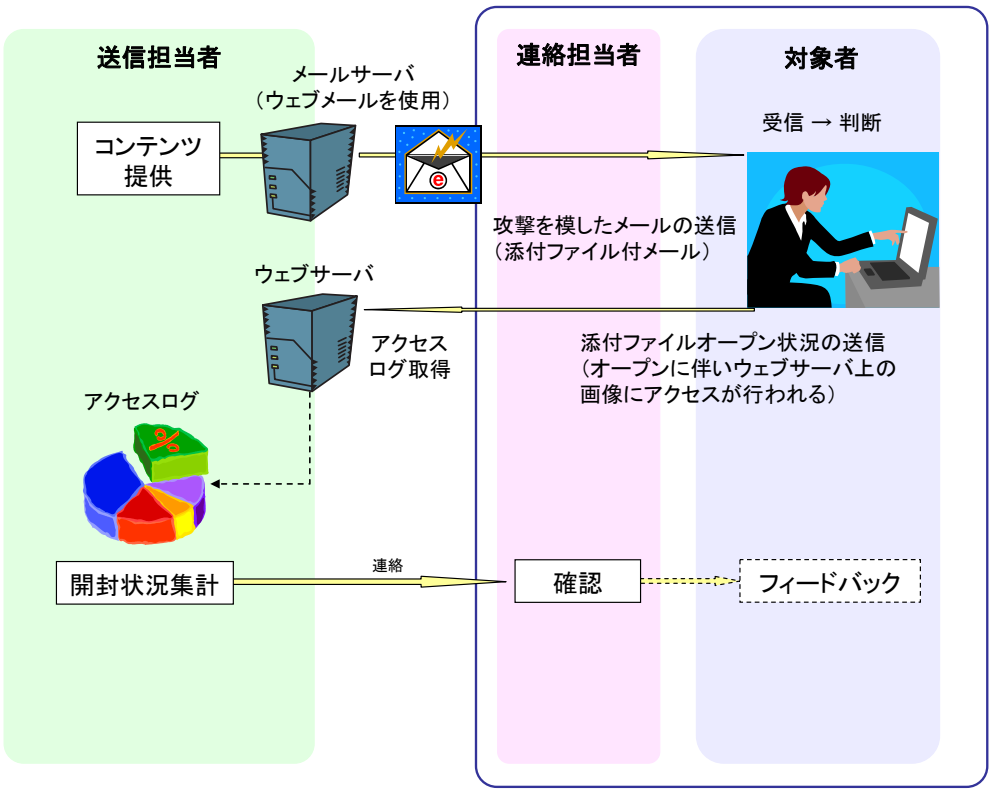


図 4-2　添付ファイルオープン状況を記録する手法

添付ファイル内のリンクは、MS Word の「図の挿入」機能を用いて、URL でウェブサーバ上の画像ファイルを指定し、リンクを作成した。

この手法にはいくつか注意すべき点がある。

対象者が添付ファイルを開いた際に、その PC からウェブサーバにアクセスできなければ添付ファイルを開いたという記録を取ることができない。例えば添付ファイルを保存後に接続を絶ち、開いた場合にはログは残らない。

また、対象者のネットワークからウェブサーバへのアクセスが制限されている場合には、ファイルオープン後にアクセスが中断されてしまい、ログが残らない可能性がある。

4.3.3. 添付ファイルの内容

ダミーメールで送る添付ファイルには 2 つの機能を持たせる。

(1) 添付ファイルのオープン状況に関するカウント

前述したように、ファイルオープン時にウェブサイトへのアクセスが生じるように、微小な画像へのリンクを埋め込む。

(2) 説明および教育

添付ファイルを開いてしまった対象者に向けて、訓練に関する説明を行うとともに、不審なメールと添付ファイルがもたらす脅威について解説を行う。訓練に関する説明項目として以下を伝える(優先して伝達すべき事項の順に示す)。

- このメールが訓練／調査を意図して､不審なメールを模して作られて送られたものであること
- 訓練／調査に関する連絡担当者の問合せ先
- 本文や件名に示された内容が架空のものであること
- 訓練／調査の結果の取り扱われ方
- 事前説明無しに送付したことについての、説明および協力依頼
- 添付ファイルに危険性が無いこと
- 添付ファイルのオープン状況について確認を行なっていること
- 脅威に関する知識（教育を意図する内容）
- 調査協力への謝意

また、教育的な内容については以下の知識を伝えることを意図する。

- 標的型のメール攻撃の概要
- 不審な添付ファイルを不用意に開くことの危険性
- 標的型のメール攻撃への対処方法（警戒心の喚起）

添付ファイルの文面の作成例を5.2に示す。

4.4. 準備

4.4.1. スケジュールの策定

同一の対象者集団に対して最大 2 回の送信を行う。2 回の送信の間にはおよそ 2 週間のインターバルをおく。第 1 回の終了後に、訓練／調査を目的とするメールである旨を対象者に通知する。第 2 回の送信を行うことについては通知

せず、これも同様に抜き打ちで実施する。
スケジュールの例を表 4-1 に示す。

表 4-1　訓練／調査スケジュール

おおよそのスケジュール（営業日でカウント）	実施項目	
第 1 日	担当者打合せ	
第 2 日～3 日	第 1 回	リハーサル・文面確認
		対象者メールアドレス受領
第 5 日～6 日		送信（訓練の実施）
		問合せ対応
		対象者への説明
第 6 日～7 日		添付ファイル開封状況の連絡
（第 8 日～9 日）	担当者打合せ	
第 10 日～11 日	第 2 回	リハーサル・文面確認
第 12 日～13 日		送信（訓練の実施）
		問合せ対応
		対象者への説明
第 13 日～14 日		添付ファイル開封状況の連絡
第 15 日	分析	
第 16 日	報告	

4.4.2. 事前の確認・検討

対象者には事前通知を行わず、抜き打ちで実施する。基本的に上長およびセキュリティ管理者のみに事前に訓練実施を通知する。
確認・検討を要する事項を以下に示す。

- 対象者および各担当者の所属する組織の上長の承諾を得る
- 対象者が不審なメールを受信した際の望ましい対応については、社内ポリシーや規則との整合性を考慮し、担当者間でも合意しておく。
- 実施期間中にメールのチェックができない者、届いた全メールの確認が職務上求められる者等については対象者から外すことを検討する。
- ダミーメール受信時に善意の対象者が連絡する可能性がある組織内外の相手先については、訓練実施前に連絡担当者から事前説明を行っておくとよい。

4.4.3. リハーサルの実施

対象者のメール受信およびウェブアクセスに関する環境についてチェックを行う。

確認（リハーサル）は、訓練と同様のダミーメールを作成し、担当者の 1 人に対象者と同環境（組織における標準的な PC 環境）を持つ受信者役を受け持たせて、訓練と同じように送信して行う。受信者役はメールクライアント上で受信が行えることの確認、添付ファイルの保存とオープンの確認を行う。

添付ファイルを開いた時間をもとに、担当者は、ウェブサーバ上の画像へのアクセスがログに取得されるかどうかを確認する。

リハーサルを行った際に明確化される問題の例と対処の方針を示す。

・ スパムフィルタによりメールが削除される。あるいは件名に警告メッセージが追加される。
  → 一時的にフィルタを通過するように設定を変更する（変更を依頼する）

・ 添付ファイルを開いてもウェブサーバにログが残らない
  → 以下の原因である可能性がある。
    - 添付ファイル内の画像へのリンクの作成ミス。
    - アクセス時のネットワーク接続ミス。
    - 対象者の PC からウェブサーバへのアクセスに制限がかけられている。

訓練に使用するダミーメールについて、本文、件名、送信元アドレス、添付ファイル名を連絡担当者が対象者の受信環境上で再確認し、必要であれば最終的な調整を行う。

4.4.4. ダミーメールの準備

ダミーメールは対象者ごとに全て異なるものとなるため、送付を手作業で行う際には特に注意が必要である。

添付ファイルの中の画像へのリンクが正しく作られて居ることを送信前に確認しておく。添付ファイルオープン時にブラウザのキャッシュフォルダに画像のファイルが残ることを用いて確認を行なうとよい。

メールは送信直前の状態で一時保存し、宛先アドレスと添付ファイルの添付を再確認する。

送信状況確認のため担当者に BCC を用いて写しを送るように設定する。（それらのアドレスにも誤送信が無いように確認を行なう）。

4.5. 調査／訓練の実施

4.5.1. ダミーメールの送信

あらかじめスケジュールで定めた時刻に送信担当者から対象者にダミーメールを送信する。送信は、全対象者についてほぼ同時に行う。送信時刻については、対象者の大多数が受信後にメールを確認可能な時間帯を考慮して、就業時間内の休み時間等を避けた時間帯に設定する。

送信の事実確認のために BCC でメールを連絡担当者や送信担当者に送る場合には、誤って添付ファイルをオープンしないよう事前に再確認メールを送る等して注意を促す。万が一ファイルを開いてしまった場合には、その時刻を付記して連絡させる。

送信するメールについての詳細を4.3.1に示す。

4.5.2. 連絡・相談受付と状況把握

ダミーメールを受信した対象者の中には、添付ファイルを開かずに不審メールを受信したとみなして、連絡担当者にコンタクトする可能性がある。また、添付ファイルを開いた場合には、その場合に表示される文面に記載された連絡担当者に問合せを行う可能性も高い。

連絡担当者は送信直後の状況を観察し、メールあるいは口頭で寄せられる質問に対応する。対象者からの問い合わせについては可能な限り個別に説明を行う。問い合わせてきた対象者には他の対象者が訓練／調査を続けるために、周囲に訓練である旨を明かさないよう協力を依頼する。

4.5.3. 訓練の終了と対象者全体への説明

訓練を終了するタイミングで、連絡担当者は電子メール等により、抜き打ちの訓練／調査であったことを対象者全員に説明する。必要に応じ、口頭説明等で補足する。

終了のタイミングは、対象者を近くで観察することができる連絡担当者が判断する。おおよその目安では、対象者の所属する集団内で口頭やメーリングリストを利用してダミーメールへの警戒が呼びかけられ、メールを未読の者を含めて対象者ほぼ全員が警戒心を喚起される状況に至った時点とする。

終了を通知する際の通知内容は以下を含む。

- ダミーメールの概要（送信者、件名、添付ファイル名）
- ダミーメールが訓練・調査を目的とするものであったこと
- 上長等の了解のもとで実施したこと
- 結果の取扱い
- 抜き打ち実施についての理由（調査精度向上）とお詫び
- 今回の訓練・調査が終了したこと
- 謝意および不安、不信感を与えたことへのお詫び
- ダミーメールおよび添付ファイルの削除の依頼
- 今後も不定期に同様の調査を行う可能性があること
- コメント、意見等についての依頼
- 標的型攻撃についての解説
- 不審なメールの特徴
  - 普段やり取りをしない人物からのメール
  - 添付ファイルが付いているメール
  - 見慣れないフォントが使われているメール　等
- 不審なメールを受信した際の連絡先
- 不審なメールへの対処方法（添付ファイルを開かずに削除する等）

終了後、各対象者から以下についての意見を集める。

- ダミーメールのどのような点を不審に思ったか
- ダミーメールに対してどのような対処を行ったか
- これまでどのように対処をしているか
- 訓練・周知の方法について

4.6. フォローアップ

4.6.1. 集計と分析

各回の訓練について、送信者数と添付ファイルを開いた者の数をアクセスログからカウントする。

訓練実施に必要な対象者に関する情報はメールアドレスのみであるが、傾向を掴むために年代、職種、業務分野等のいくつかの属性情報についても収集する。

ダミーメールが、ある個人にとっては特に注意を引き付け易いメールとなっている場合があるため、単純に開いた／しないという観点で評価を行っても意義が薄い点には注意が必要である。例えばダミーメールの文面にその個人が業務上興味を持つ分野への言及がある場合には添付ファイルを開いて確認しようという意識が強く働く。興味が無い分野のメールを受信した対象者とは対処を行う上での難しさが全く異なる。

全体の評価としては、1 回目および 2 回目に添付ファイルを開いた人数よりも、2 回目の訓練で改善の効果が見られたかを確認する。

また、終了後に集めた意見を基に、今後の注意喚起の際に伝えるべき情報、情報セキュリティに関する意識向上の方策について検討を行う。

4.6.2. 報告

結果は簡潔に取りまとめ、担当者から対象者および組織内関係先に報告する。報告にあわせて今後の対策を示すことが望ましい。

組織面の強化策としては、不審なメール等に気づいた場合の連絡先を（再）整備することが挙げられる。連絡先を、社内の窓口あるいは各部署内の IT 担当者等に設定し、個々人が異常に「気付く」機会を被害低減のために有効に活用することが重要である。

意識向上の方策としては、最近の攻撃手法に関する周知徹底を行うことが挙げられる。

4.7. 予防接種手法の試行結果に関する報告

JPCERT/CC で上記のシナリオを用いては国内の 5 組織を対象に試行訓練を実施した。各協力先における実施結果を下表に示す。

（単位：人）

協力先	対象者数	添付ファイルを開いた対象者の人数	
		第 1 回目	第 2 回目
A	15	8（53%）	—
B	27	5（19%）	3（11%）
C	26	3（12%）	0（ 0%）
D	22	6（27%）	6（27%）
E	26	2（ 8%）	5（19%）
1 回以上実施[6]	116	24（21%）	—
2 回実施	101	16（15%）	14（ 13%）

- 抜き打ちによる訓練を対象者 116 名に対して実施した。初回の演習で添付ファイルを開いた者は 24 名（21%）であった。
- 間隔をおいた 2 回の訓練は 53 名に実施した。対象者のうち添付ファイルを第 1 回の訓練で開いた者は 8 名（15%）、第 2 回に開いた者は 3 名（6%）であった。いずれの回でも開いた者は 2 名（4%）、１回目で開いた 8 名のうち 2 回目でオープンしなかった者は 5 名であった。

4.7.1. 考察

- 2 回の演習を同一の巧妙さのダミーメールで実施した組織(B 社と C 社)においてはいずれも添付ファイルのオープン率に改善が見られた。
- 協力先の組織における結果の評価を通じて、情報セキュリティに関するトラブルやインシデントが発生した際、あるいはそれらの予兆に気付いた際の連絡、情報共有の体制を確認することができた。
- 特に、平常時より情報システム担当者（あるいはセキュリティ担当者）が対象者との間で密に連絡を取っている実施事例においては、ダミーメールが受

[6] A 社においては予防接種実施回数が 1 回のみであった。そのため A 社を含む 1 回以上実施した 5 企業の結果と、A 社を含まない 2 回の予防接種を実施した 4 企業に分けて集計を行った。

信されたことに関する情報共有が迅速に行われたことが確認された。

- 技術やセキュリティに対する理解度と開封率の間に相関はなかった。ソーシャルエンジニアリングを用いた標的型攻撃メールに関しては、技術やスキルだけでは対応できないことが改めて確認できた。
- 標的型攻撃への対策として、予防接種**だけを**実施するのは無意味である。脅威や被害の実態に関するレクチャーと組み合わせて、それらの教育を補足する手段として使った場合ときに最大の効果を発揮するものと考えられる。

5. 付録

5.1. ダミーメールサンプル

例中ではアドレスを示すために questionable.sender@example.com とした。

■サンプル(1)

送信元： ●● <questionable.sender@example.com>
件名： 回覧：マスコミ取材対応方針について

携帯電話コンテンツに関するマスコミ取材への対応方針についてです。添付を参照してください。

添付ファイル名： マスコミ対応方針.doc

■サンプル(2)

送信元： ●● <questionable.sender@example.com>
件名： ご参考：●●セミナー2007 聴講者アンケート回答

各位 ●月●日の●●セミナー2007 での講演聴講者のアンケート回答をまとめたものです。

添付ファイル名： 集計結果.doc

■サンプル(3)

送信元： ●● <questionable.sender@example.com>
件名： 社内アンケートに関するご協力のお願い

各位 新規事業に関する検討の一環としてウェブメールの活用状況に関して社内アンケート調査を行います。 添付のファイルにご記入の上、●月●日(●)15 時までにご回答ください。お忙しいところ恐縮ですが、ご協力をお願いいたします。

添付ファイル名： アンケート票.doc

■サンプル(4-1)

送信元： ●● <questionable.sender@example.com>
件名： オンラインセミナー講師協力について

添付資料にあるように「最新ウェブ・テクノロジーに関するオンラインセミナー」に社内からも講師として協力します。講座内容および候補日を示しますので皆さんも検討をお願いいたします。

受講者としての参加も若干名を受け付けますので御相談ください。

以上宜しくお願い致します。

＃既に連絡を受けているようでしたら重複をお許しください。

添付ファイル名：　講師依頼（●●様）.doc

■サンプル(4-2)

送信元：　●●　<questionable.sender@example.com>

件名：　　個人情報保護セミナー参加者の募集

各位

添付資料にあるように個人情報保護関連のセミナーを数社から協力をいただいて実施することとなりました。受講希望者は御相談ください。

以上宜しくお願い致します。

＃既に連絡を受けているようでしたら重複をお許しください。

添付ファイル名：　開催概要（●●殿）.doc

■サンプル(5)

送信元：　●●　<questionable.sender@example.com>

件名：　　予算計画

皆様、

経営陣からの連絡により、来期の予算計画に関して、添付のようにまとまったとのことですので、添付ファイルを確認頂いて、●●までご連絡頂くようお願いいたします。

--
●●

添付ファイル名：　予算計画.doc

■サンプル(6)

送信元：　●●　<questionable.sender@example.com>

件名：　セキュリティについて

各位

最近の情報セキュリティに関する脅威について、良くまとまったレポートをみつけたので送ります。参考にしてください。

添付ファイル名：　ウイルス対策.doc

■サンプル(7)

送信元：　●●　<questionable.sender@example.com>

件名：　先日のテレビ番組出演について

社長の出演した番組をメールに添付しました。
参考までに、閲覧ください。

●●

添付ファイル名：　●●テレビ.doc

■サンプル(8)

送信元：　●●会計事務所　<questionable.sender@example.com>

件名：　●●事業部の監査結果

●●様、●●様

今期●●事業部の監査結果について
添付ファイルの通りご報告いたします。

添付ファイル名：　●●事業.doc

■サンプル(9)

送信元：　●●　<questionable.sender@example.com>

件名：　アンケートのご協力

某旅行代理店からの依頼で今年度の消費者の旅行動向についてのアンケート調査を実施しています。社員の皆様からも、是非アンケートにご協力いただきたいので、2，3 日の間でお手すきの際にご協力ください。旅行の時期、場所、予算、同行人数といった簡単な内容なので、数分でお答えいただけると思います。よろしくお願いいたします。●●

添付ファイル名：　旅行動向アンケート.doc

■サンプル(10)

送信元：　広報部　<questionable.sender@example.com>

件名：　新サービスについて

事業部長　各位

●●の新サービスに関するリリースをご確認ください。

広報部 ●●

添付ファイル名：　releace.doc

■サンプル(11)

送信元：　●●本部長 <questionable.sender@example.com>
件名：　明日の資料

各事業部門長から提出いただいた内容をベースに、来期事業について
まとめた資料です。明日の会議で検討するので、よく目を通しておい
てください。

●●

添付ファイル名：　来期の事業内容（案）.doc

■サンプル(12)

送信元：　●●室 <questionable.sender@example.com>
件名：　全社システムのアップデートについて

添付の資料を参照の上、最新のアップデートをお試しください。
新しいプログラムはコンピュータの状態を安定させ、セキュリ
ティを向上させます。

添付ファイル名：　update.doc

■サンプル(13)

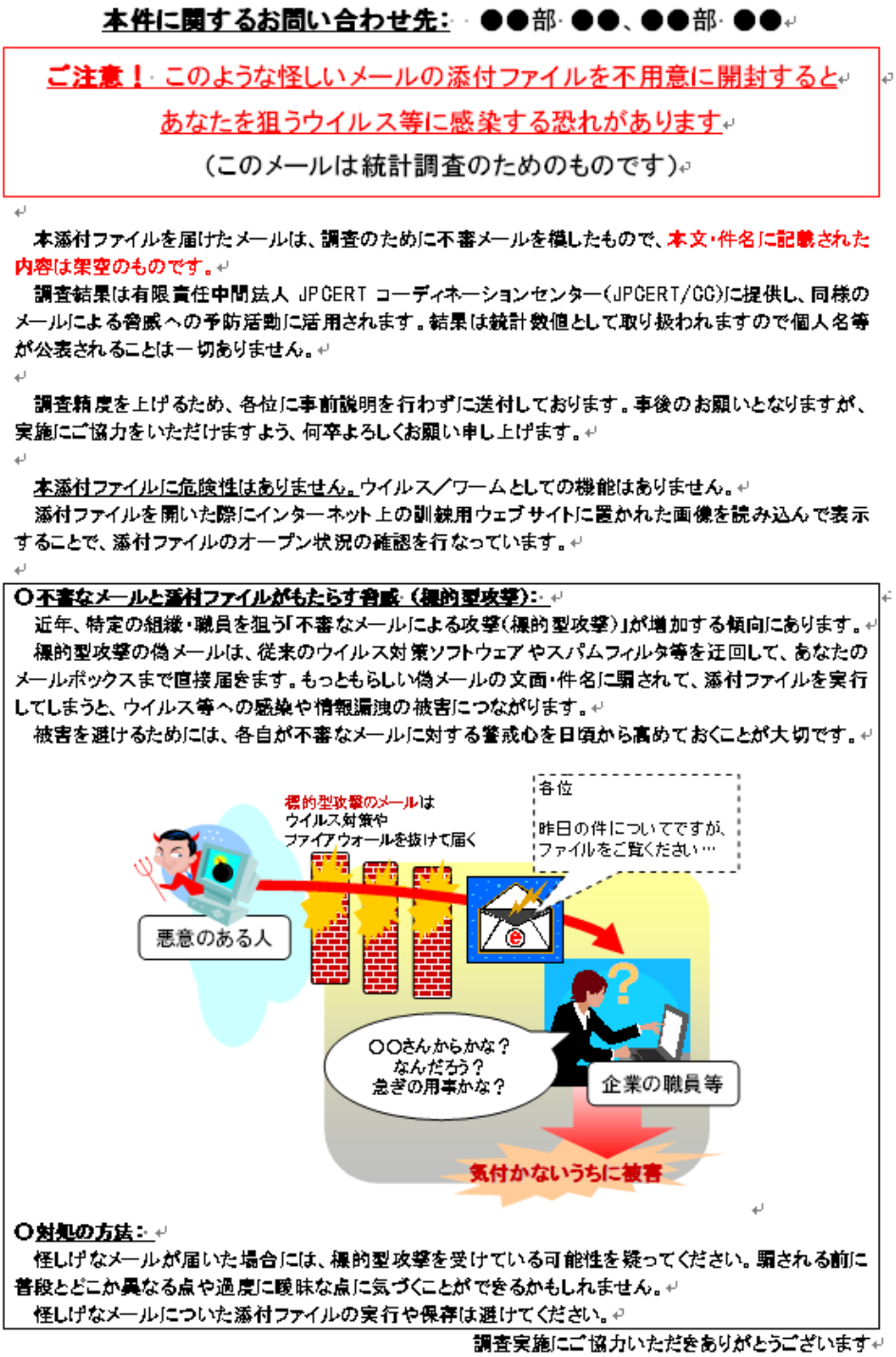
送信元：　●● <questionable.sender@example.com>
件名：　動画コンテンツ視聴アンケート

●●におけるランキングデータです。参考までに、社員に対し
てもアンケートを実施させていただきたいと思います。お手す
きの際に、添付ファイルにリンクがあげられている動画ファイ
ルを閲覧の上、評価してください。

●●

添付ファイル名：　動画コンテンツ・ランクング

5.2. 添付ファイルサンプル



本件に関するお問い合わせ先: ●●部 ●●、●●部 ●●

ご注意！ このような怪しいメールの添付ファイルを不用意に開封すると
あなたを狙うウイルス等に感染する恐れがあります
（このメールは統計調査のためのものです）

本添付ファイルを届けたメールは、調査のために不審メールを模したもので、本文・件名に記載された内容は架空のものです。
調査結果は有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）に提供し、同様のメールによる脅威への予防活動に活用されます。結果は統計数値として取り扱われますので個人名等が公表されることは一切ありません。

調査精度を上げるため、各位に事前説明を行わずに送付しております。事後のお願いとなりますが、実施にご協力をいただけますよう、何卒よろしくお願い申し上げます。

本添付ファイルに危険性はありません。ウイルス／ワームとしての機能はありません。
添付ファイルを開いた際にインターネット上の訓練用ウェブサイトに置かれた画像を読み込んで表示することで、添付ファイルのオープン状況の確認を行なっています。

○不審なメールと添付ファイルがもたらす脅威（標的型攻撃）：
近年、特定の組織・職員を狙う「不審なメールによる攻撃（標的型攻撃）」が増加する傾向にあります。
標的型攻撃の偽メールは、従来のウイルス対策ソフトウェアやスパムフィルタ等を迂回して、あなたのメールボックスまで直接届きます。もっともらしい偽メールの文面・件名に騙されて、添付ファイルを実行してしまうと、ウイルス等への感染や情報漏洩の被害につながります。
被害を避けるためには、各自が不審なメールに対する警戒心を日頃から高めておくことが大切です。

○対処の方法：
怪しげなメールが届いた場合には、標的型攻撃を受けている可能性を疑ってください。騙される前に普段とどこか異なる点や過度に曖昧な点に気づくことができるかもしれません。
怪しげなメールについた添付ファイルの実行や保存は避けてください。

調査実施にご協力いただきありがとうございます

図 5-1　ダミーメールに添付した MS Word 形式ファイルの文面（サンプル）