標的型攻撃メールの事例と対策
メールがもたらす脅威

KIS Security株式会社

（2023年3月）

目次

本資料は、3つのパートに分けて説明しています。

１. 標的型攻撃メールについて

２. 標的型攻撃メールの事例

３. 標的型攻撃メールのメールの見分け方

1. 標的型攻撃メールについて

メールが利用されるサイバーセキュリティ攻撃

KIS SECURITY

✓ フィッシング攻撃

フィッシング詐欺とは、金融機関などの有名企業を詐称したメールを送り付け、本文のURLをクリックさせることで偽サイトに誘導し、不正にIDとパスワードなどを詐取する詐欺行為のこと。本物とそっくりのフィッシングサイトに誘導し、認証情報や個人情報などを入力させ詐取する方法がとられることが多い。

✓ スパムメール攻撃

スパムとは、受信者の意図とは関係なく、大量に配信されるメッセージのこと。スパムで配信されるメッセージの内容は、商品の勧誘販売・出会い系・アダルト系を中心に、注文書・請求書や宅配便の再配達などを騙るものなど、不特定多数に対し大量に送信される。

✓ マルウェアによる攻撃

マルウェア（malware）とは、悪意のある（malicious）ソフトウェア（software）を合わせた造語で、感染対象に対して有害な作用をもたらすことを目的に作成されたソフトウェアの総称である。マルウェアによる攻撃は、メールに含まれる添付ファイルやリンクを通じて、受信者のコンピュータに感染し、ネットワークに接続された他のコンピュータにも感染することがある。また、感染したコンピュータには、バックドアやスパイウェアなどの悪意のあるプログラムがインストールされることがある。

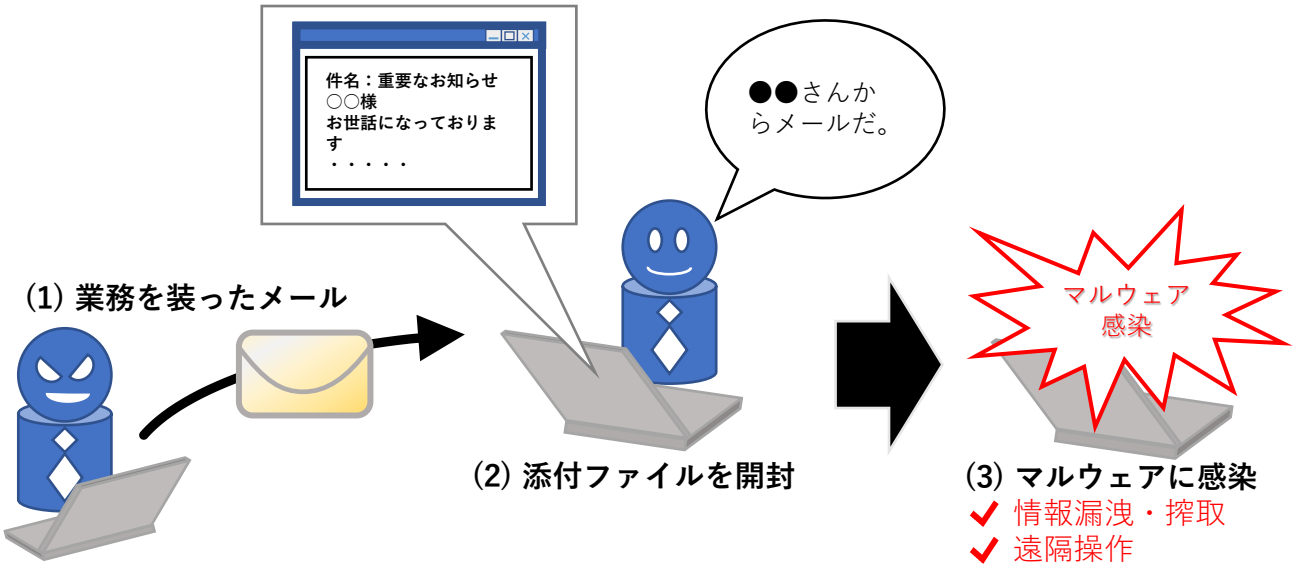
✓ 標的型攻撃メール

標的型攻撃メール攻撃とは、不特定多数の対象にばらまかれる通常の迷惑メールとは異なり、対象の組織から重要な情報を盗むことなどを目的として、組織の担当者が業務に関係するメールだと信じて開封してしまうように巧妙に作り込まれたウイルス付きのメールのことです。また、メールに記載のURLや添付ファイルから悪意あるWebサイトへ誘導し、マルウェアに感染させる場合もある。

標的型攻撃メールとは

攻撃者はメールの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し、マルウェア感染の仕掛けが施された添付ファイルを開かせたり、本文に記載されたマルウェア感染の仕掛けが施されたサイトへのリンクをクリックさせる。

- ✓ 受信者をだます為に、業務でよく使われるメールの件名やメール本文、添付ファイルの形式や署名をまねて送られてくる
- ✓ 慌ててうっかりミスを誘うために「緊急」「重要」など目にひく文言を使って添付ファイルを開封させようとする



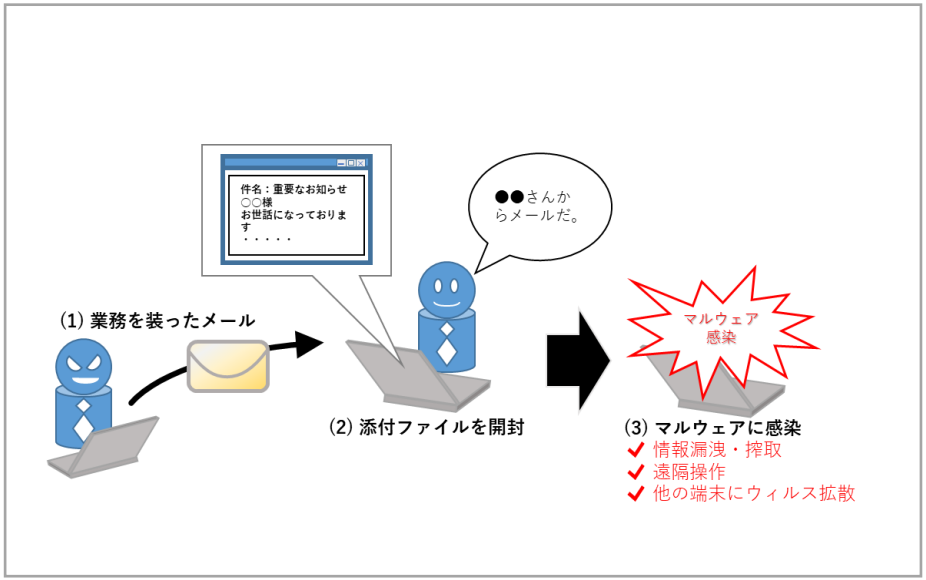
標的型攻撃メールの手口

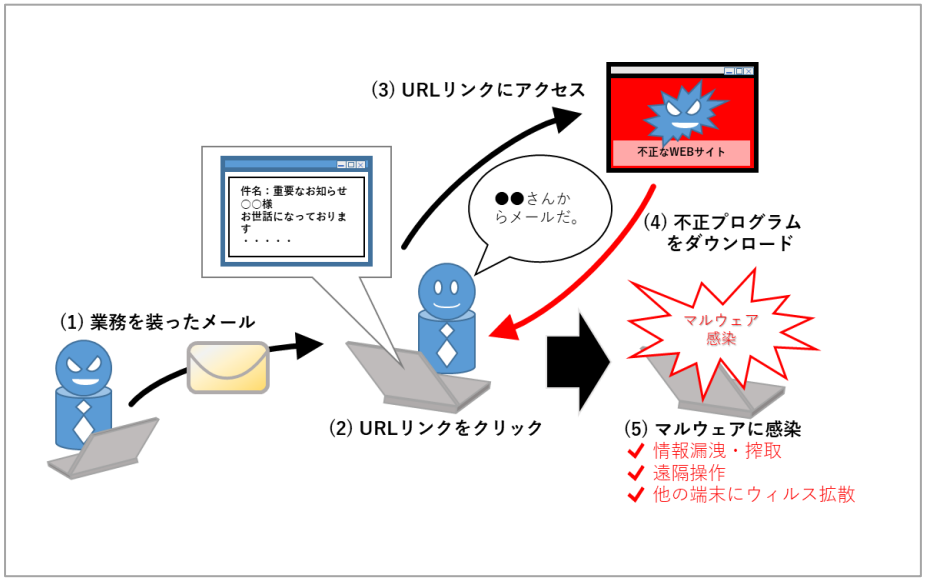
KIS SECURITY

✓ **メールによる添付ファイルの送付**
添付ファイルの拡張子を偽装し悪意あるプログラムを実行させたり、オフィスソフトのマクロ機能を使って悪意あるスクリプトを実行させてマルウェアに感染させる。

✓ **メール本文にマルウェアなどが仕込まれたWEBサイトへ誘導するURLを記載**
巧みな文章でマルウェアがダウンロードされるWEBサイトにアクセスさせ、マルウェアに感染させる。

✓ **メール本文に認証情報などを搾取するフィッシングサイトへ誘導するURLを記載**
巧みな文章でフィッシングサイトに誘導し、金融機関のWEBサイトやSaaSサービスのサイトの認証情報や個人情報を入力させ搾取する。





標的型攻撃メールの攻撃の流れ

KIS SECURITY

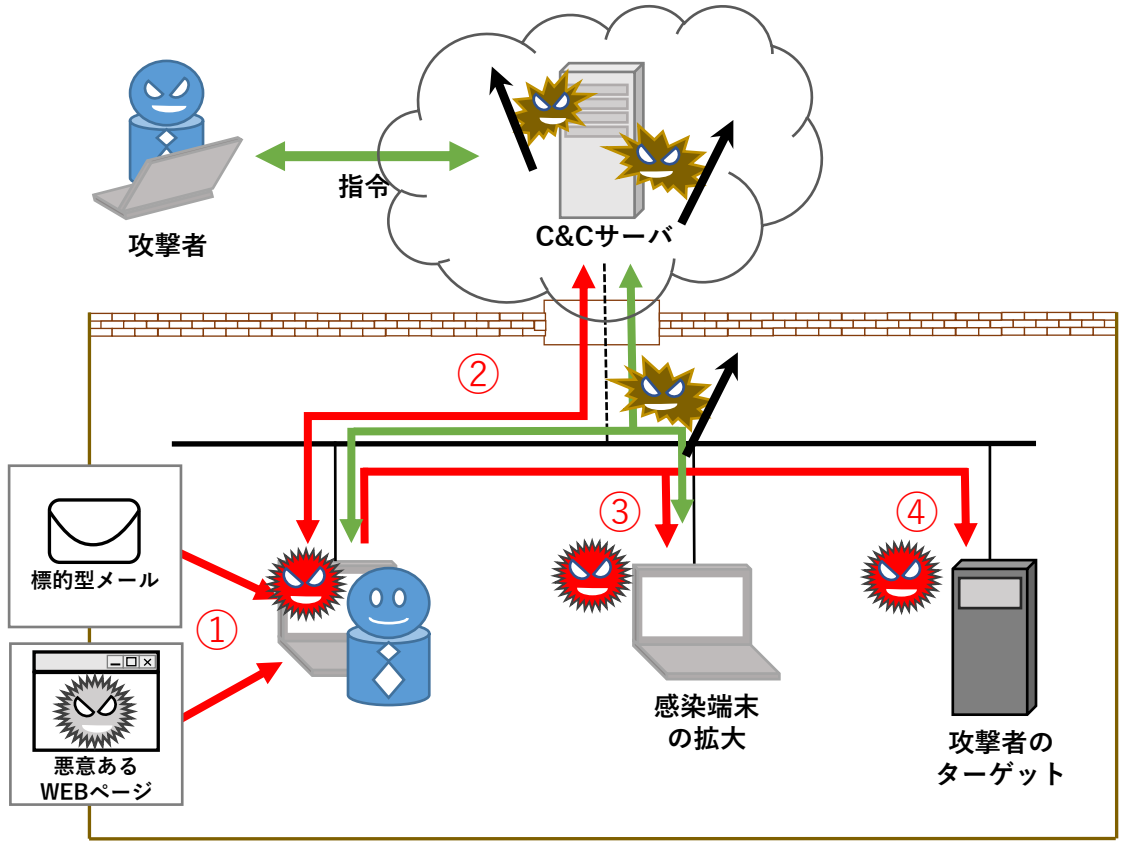
標的型攻撃メールでは次のような流れで攻撃が進行します。

① **初期潜入**
標的型メールやWEBサイト閲覧を通じてマルウェアに感染する。

② **攻撃基盤構築**
侵入したPC内でバックドアを作成し、外部のC＆Cサーバと通信を行い、新たなマルウェアをダウンロードする。

③ **システム調査**
システムに関する情報の取得や情報の在処を特定する。ネットワーク内に展開する。

④ **目的の遂行**
攻撃用のマルウェアで攻撃する。（組織の重要情報の搾取、改ざん、破壊）



感染時の被害と復旧について

KIS SECURITY

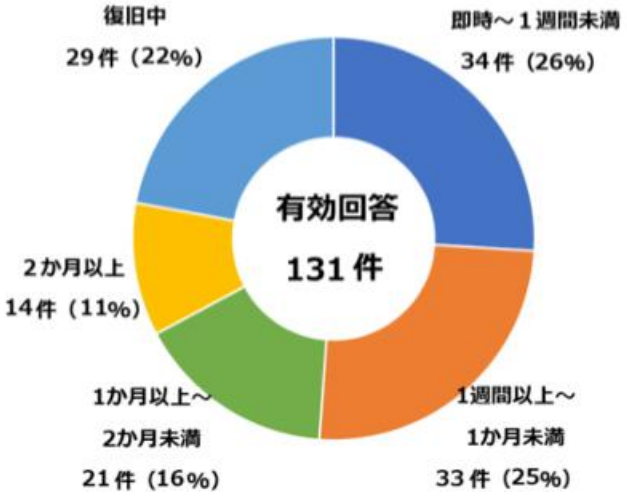
✓感染した時の被害

・機密情報の漏えい　（個人情報以外にも企業にとって重要な情報が漏えい）
・金銭の被害　（直接的な金銭の搾取だけでなく、対策にかかる費用が発生）
・社会的信用の低下　（企業イメージの低下につながり回復するまでに時間がかかる）

✓復旧に要した時間と復旧にかかる費用

標的型攻撃メールなどによるマルウェアに感染した場合の復旧に要した時間は、
1週間以上1カ月未満が多いが、2か月以上もかかるケースもある。復旧には調査費用や
システム導入、社員教育等含め1,000万以上のコストが発生する場合も多い。

<復旧に要した期間>



<復旧費用の総額>

警察庁　令和４年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

2. 標的型攻撃メールの事例

有名な標的型攻撃メールの被害事例１

KIS SECURITY

✓日本年金機構の個人情報漏洩事件（2015年）

2015年5月に、標的型攻撃メールによって、日本年金機構の職員の端末に外部からの不正アクセスされ、当機構が保有している個人情報の一部が外部に流出した。現時点で流出していると考えられるのは、約125万件です。漏洩した情報には、氏名、住所、年金番号、口座情報などが含まれていました。

厚生労働省
Ministry of Health, Labour and Welfare

本文へ ｜ お問合わせ窓口 ｜ よくある御質問 ｜ サイトマップ ｜ 国民参加の場

ホーム　検索

テーマ別に探す ｜ 報道・広報 ｜ 政策について ｜ 厚生労働省について ｜ 統計情報・白書 ｜ 所管の法令等 ｜ 申請・募集・情報公開

ホーム > 政策について > 分野別の政策一覧 > 年金 > 年金・日本年金機構関係 > 日本年金機構（厚生年金・国民年金の手続きなど） > 日本年金機構における不正アクセスによる情報流出事案について

日本年金機構における不正アクセスによる情報流出事案について

平成27年6月12日

日本年金機構に対する、外部からの不正アクセスにより、国民の皆さまの個人情報が外部に流出した件について、6月1日に日本年金機構から公表と謝罪がありました。

日本年金機構が、悪意をもった攻撃を防げなかったことは誠に遺憾です。

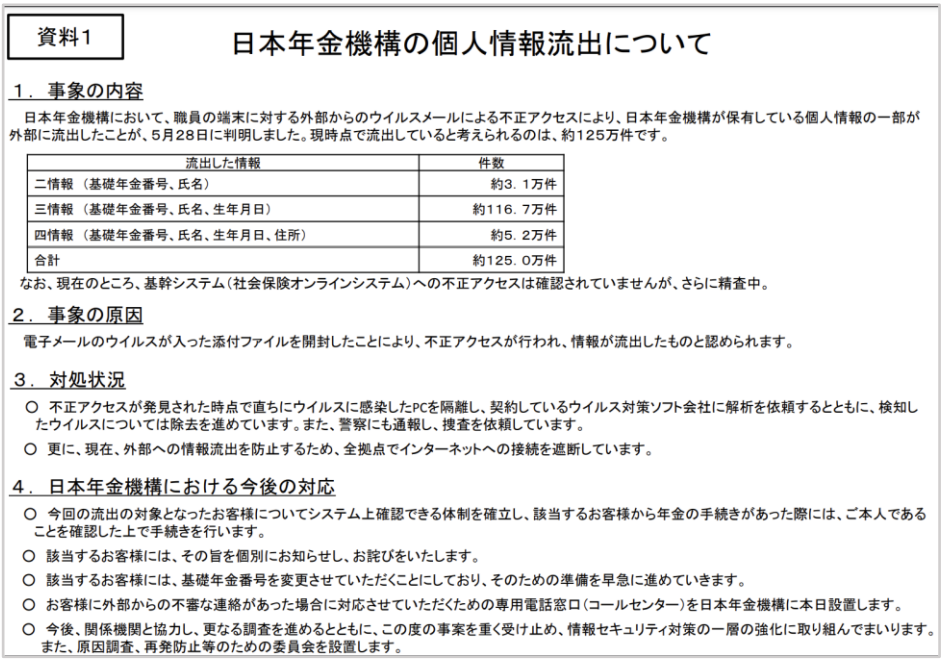
今回の事案は、日本年金機構に対する外部からのウイルスメールによる不正アクセスにより、日本年金機構が保有する個人情報の一部が外部に流出したことが、5月28日に判明したものです。現時点で流出していると考えられるのは、約125万件です。
国民の皆さま方のご心配にお答えするため、日本年金機構に専用電話窓口（コールセンター）を設置したほか、対象となった方へは日本年金機構より個別に郵送にて、このたびの事情をお知らせするとともに、お詫びをさせていただいております。
さらに、対象となった方の基礎年金番号を変更させていただき、新しい基礎年金番号を郵送でお送りいたします。

日本年金機構を監督する立場の厚生労働省としてお詫びを申し上げるとともに、今回の事案の問題点と、日本年金機構における今後の情報管理の在り方を検証するために、6月4日、第三者からなる「日本年金機構不正アクセス事案検証委員会」を厚生労働省に立ち上げました。

厚生労働省としては、今回の事案の発生原因を究明し、再発防止に向けて全力かつ可及的速やかに取り組んでまいります。

厚生労働大臣
塩崎恭久

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000152638.html



資料1

日本年金機構の個人情報流出について

1．事象の内容

日本年金機構において、職員の端末に対する外部からのウイルスメールによる不正アクセスにより、日本年金機構が保有している個人情報の一部が外部に流出したことが、5月28日に判明しました。現時点で流出していると考えられるのは、約125万件です。

流出した情報	件数
二情報（基礎年金番号、氏名）	約3．1万件
三情報（基礎年金番号、氏名、生年月日）	約116．7万件
四情報（基礎年金番号、氏名、生年月日、住所）	約5．2万件
合計	約125．0万件

なお、現在のところ、基幹システム（社会保険オンラインシステム）への不正アクセスは確認されていませんが、さらに精査中。

2．事象の原因

電子メールのウイルスが入った添付ファイルを開封したことにより、不正アクセスが行われ、情報が流出したものと認められます。

3．対処状況

○ 不正アクセスが発見された時点で直ちにウイルスに感染したPCを隔離し、契約しているウイルス対策ソフト会社に解析を依頼するとともに、検知したウイルスについては除去を進めています。また、警察にも通報し、捜査を依頼しています。
○ 更に、現在、外部への情報流出を防止するため、全拠点でインターネットへの接続を遮断しています。

4．日本年金機構における今後の対応

○ 今回の流出の対象となったお客様についてシステム上確認できる体制を確立し、該当するお客様から年金の手続きがあった際には、ご本人であることを確認した上で手続きを行います。
○ 該当するお客様には、その旨を個別にお知らせし、お詫びをいたします。
○ 該当するお客様には、基礎年金番号を変更させていただくことにしており、そのための準備を早急に進めていきます。
○ お客様に外部からの不審な連絡があった場合に対応させていただくための専用電話窓口（コールセンター）を日本年金機構に本日設置します。
○ 今後、関係機関と協力し、更なる調査を進めるとともに、この度の事案を重く受け止め、情報セキュリティ対策の一層の強化に取り組んでまいります。また、原因調査、再発防止等のための委員会を設置します。

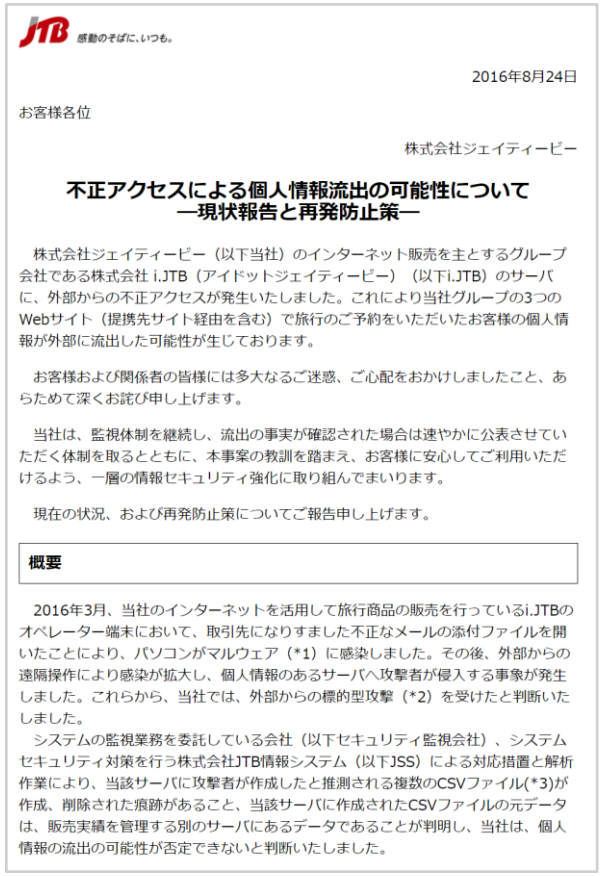
https://www.nisc.go.jp/pdf/council/cs/taisaku/ciso/dai03/03shiryou01.pdf

有名な標的型攻撃メールの被害事例２

KIS SECURITY

✓JTBの顧客情報流出事件（2016年）

2016年6月、旅行業大手JTBは、取引先を装った標的型攻撃メールによりウイルス感染したことが発端となり、顧客の個人情報の流出が発生したことを発表しました。この事件により、約679万人分の個人情報が流出した可能性があるとされている。



JTB 感動のそばに、いつも。

2016年8月24日

お客様各位

株式会社ジェイティービー

不正アクセスによる個人情報流出の可能性について
―現状報告と再発防止策―

株式会社ジェイティービー（以下当社）のインターネット販売を主とするグループ会社である株式会社 i.JTB（アイドットジェイティービー）（以下i.JTB）のサーバに、外部からの不正アクセスが発生いたしました。これにより当社グループの3つのWebサイト（提携先サイト経由を含む）で旅行のご予約をいただいたお客様の個人情報が外部に流出した可能性が生じております。

お客様および関係者の皆様には多大なるご迷惑、ご心配をおかけしましたこと、あらためて深くお詫び申し上げます。

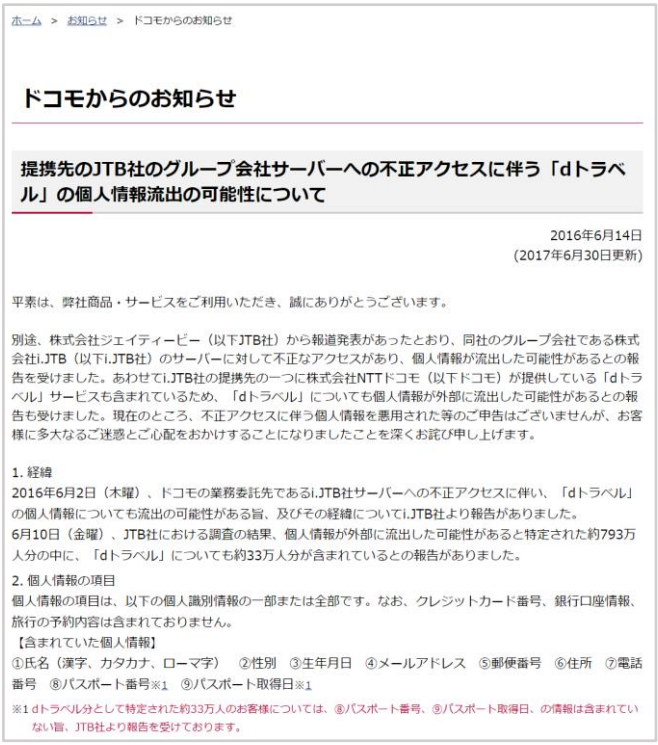
当社は、監視体制を継続し、流出の事実が確認された場合は速やかに公表させていただく体制を取るとともに、本事案の教訓を踏まえ、お客様に安心してご利用いただけるよう、一層の情報セキュリティ強化に取り組んでまいります。

現在の状況、および再発防止策についてご報告申し上げます。

概要

2016年3月、当社のインターネットを活用して旅行商品の販売を行っているi.JTBのオペレーター端末において、取引先になりすました不正なメールの添付ファイルを開いたことにより、パソコンがマルウェア（*1）に感染しました。その後、外部からの遠隔操作により感染が拡大し、個人情報のあるサーバへ攻撃者が侵入する事象が発生しました。これらから、当社では、外部からの標的型攻撃（*2）を受けたと判断いたしました。

システムの監視業務を委託している会社（以下セキュリティ監視会社）、システムセキュリティ対策を行う株式会社JTB情報システム（以下JSS）による対応措置と解析作業により、当該サーバに攻撃者が作成したと推測される複数のCSVファイル(*3)が作成、削除された痕跡があること、当該サーバに作成されたCSVファイルの元データは、販売実績を管理する別のサーバにあるデータであることが判明し、当社は、個人情報の流出の可能性が否定できないと判断いたしました。



ホーム ＞ お知らせ ＞ ドコモからのお知らせ

ドコモからのお知らせ

提携先のJTB社のグループ会社サーバーへの不正アクセスに伴う「dトラベル」の個人情報流出の可能性について

2016年6月14日
(2017年6月30日更新)

平素は、弊社商品・サービスをご利用いただき、誠にありがとうございます。

別途、株式会社ジェイティービー（以下JTB社）から報道発表があったとおり、同社のグループ会社である株式会社i.JTB（以下i.JTB社）のサーバーに対して不正なアクセスがあり、個人情報が流出した可能性があるとの報告を受けました。あわせてi.JTB社の提携先の一つに株式会社NTTドコモ（以下ドコモ）が提供している「dトラベル」サービスも含まれているため、「dトラベル」についても個人情報が外部に流出した可能性があるとの報告も受けました。現在のところ、不正アクセスに伴う個人情報を悪用された等のご申告はございませんが、お客様に多大なるご迷惑とご心配をおかけすることになりましたことを深くお詫び申し上げます。

1. 経緯
2016年6月2日（木曜）、ドコモの業務委託先であるi.JTB社サーバーへの不正アクセスに伴い、「dトラベル」の個人情報についても流出の可能性がある旨、及びその経緯についてi.JTB社より報告がありました。
6月10日（金曜）、JTB社における調査の結果、個人情報が外部に流出した可能性があると特定された約793万人分の中に、「dトラベル」についても約33万人分が含まれているとの報告がありました。

2. 個人情報の項目
個人情報の項目は、以下の個人識別情報の一部または全部です。なお、クレジットカード番号、銀行口座情報、旅行の予約内容は含まれておりません。
【含まれていた個人情報】
①氏名（漢字、カタカナ、ローマ字） ②性別 ③生年月日 ④メールアドレス ⑤郵便番号 ⑥住所 ⑦電話番号 ⑧パスポート番号※1 ⑨パスポート取得日※1

※1 dトラベル分として特定された約33万人のお客様については、⑧パスポート番号、⑨パスポート取得日、の情報は含まれていない旨、JTB社より報告を受けております。

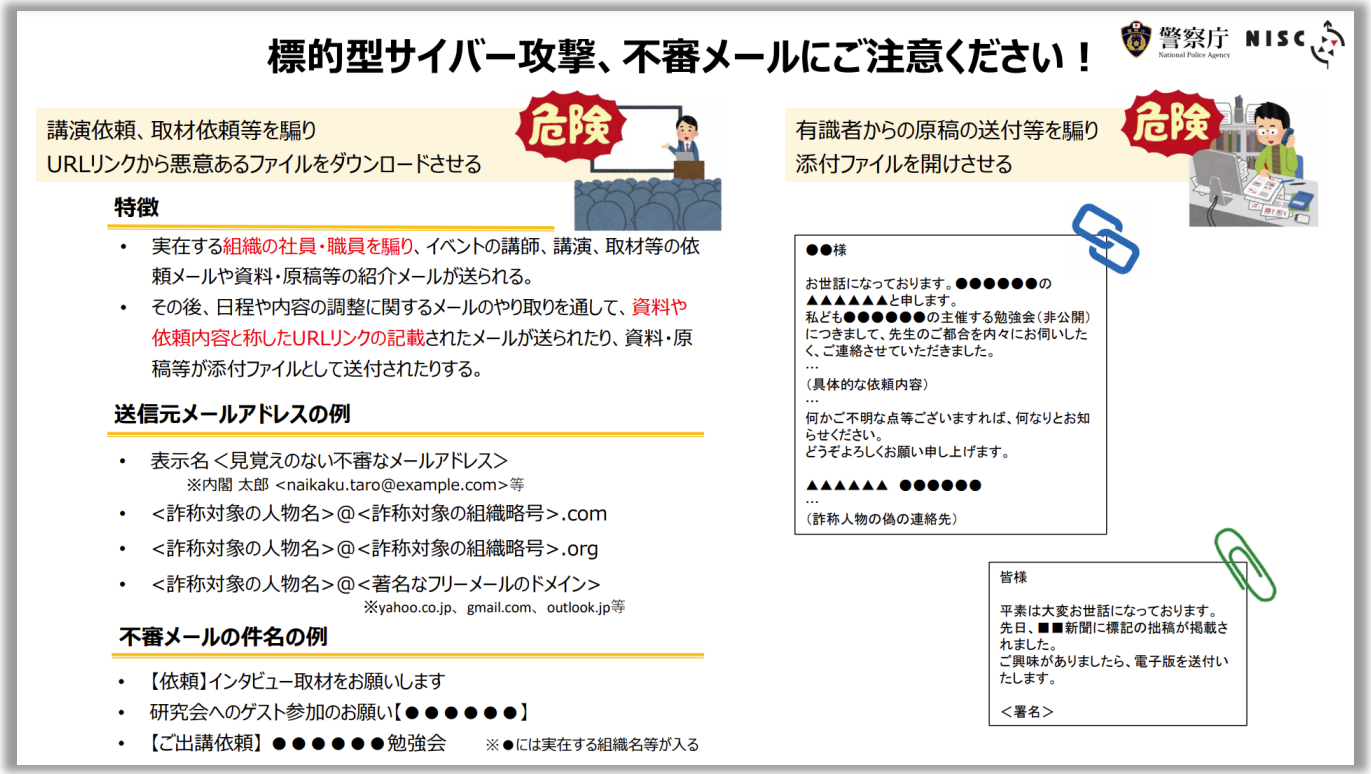
https://www.docomo.ne.jp/info/notice/page/160614_00_m.html

最近の標的型攻撃メールの事案１

KIS SECURITY

✓NISCと警察庁が「学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）」を公開（2022年11月）

この注意喚起では、実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の送付を装った標的型攻撃メールが送信されていることが報告された。



NISCと警察庁が「学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）」を公開
https://www.nisc.go.jp/pdf/press/20221130NISC_gaiyou.pdf

最近の標的型攻撃メールの事案２

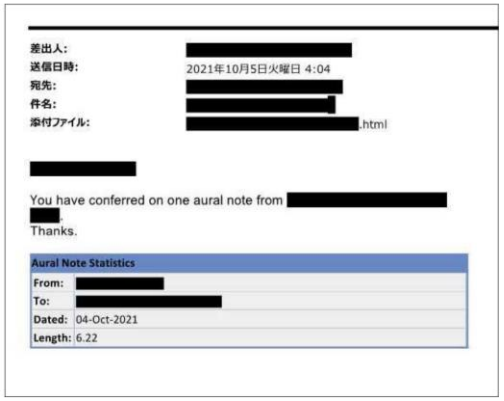
KIS SECURITY

✓機械部品関連の製造業者に対する標的型メール攻撃

新ＩＤのお知らせと称して、不正プログラムが仕掛けられたファイルをダウンロードするよう誘導する標的型メールが機械部品関連の製造業者に送信された。

✓半導体の製造業者に対する標的型メール攻撃

添付ファイルから偽のパスワード入力画面に遷移させ、業務で使用するアカウントのパスワードを入力するよう誘導する標的型メールが半導体の製造業者に送信された。



令和３年におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

3. 標的型攻撃メールの
メールの見分け方

不審なメールの気を付けるポイント

KIS SECURITY

1. タイトルや本文

- 会社の個人メールアドレスに送られてくる内容か（ECサイトやカード会社からのメール）
- メール内容に心当たりがない（自分の業務に関係ない業務のメール）
- 文字のフォントや文法や日本語が不自然
- 認証情報の入力を要求

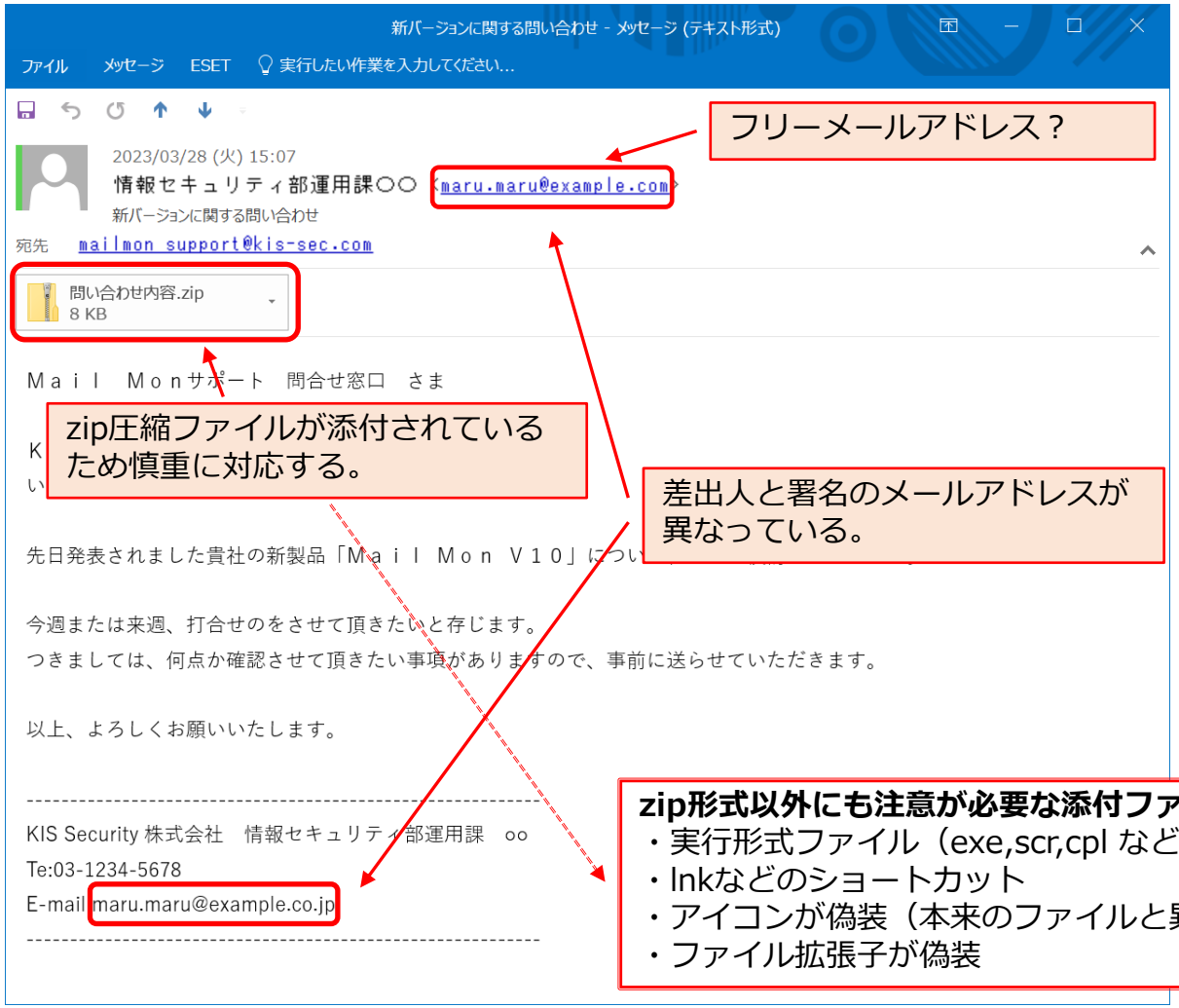
2. 送信元や送信先

- フリーメールアドレス
- 送信元のメールアドレスの表記が不自然（アルファベットが羅列）
  ※見た目の送信者アドレスは変更できるので注意が必要
- 送信先に自分以外のメールアドレスが複数ある
  ※異なるドメインのメールアドレスが羅列されている

3. 添付ファイルやURL

- Zip圧縮形式の添付ファイル
- 実行形式の添付ファイル（exe,src,cpl,bat など）
- 不自然な添付ファイル（見慣れない拡張子やアイコンが表示）
- マクロ機能を有効にする必要があるオフィスソフトの添付ファイル
- 不自然なURL（HTMLで表示されるURL（アンカーテキスト）と実際のURLが異なるリンク先）

不審なメールの確認点１



zip形式以外にも注意が必要な添付ファイル
- 実行形式ファイル（exe,scr,cpl など）
- lnkなどのショートカット
- アイコンが偽装（本来のファイルと異なる）
- ファイル拡張子が偽装

point

メール内容：サポートに関する内容

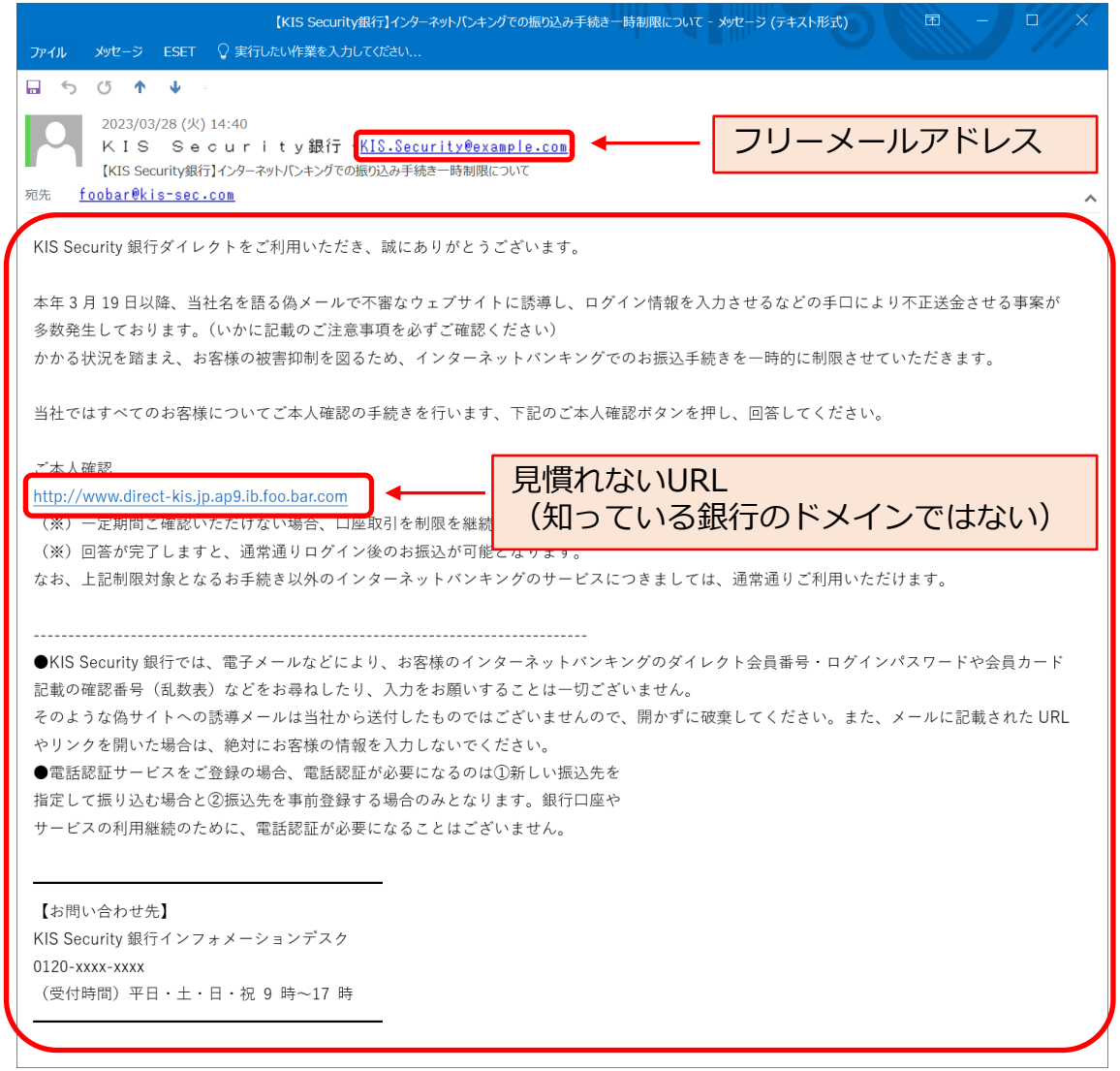
気を付けるポイント

①：メールアドレスに見覚えがない
②：差出人とメール本文の署名が異なる

↓

添付ファイルは開かない

不審なメールの確認点２



フリーメールアドレス

見慣れないURL
（知っている銀行のドメインではない）

金融機関からのメールが会社の個人メールアドレスに送られてくる？

point

メール内容：銀行からのメール

気を付けるポイント

①：メールアドレスに見覚えがない
②：見慣れないURL
③：メールの内容を疑う

↓

URLをクリックしない

KIS SECURITY

怪しいメールが届いた場合は、
上司や担当部門に相談しましょう。