デジタル庁
Digital Agency
デジタル
推進委員

第3回パソコン研修会
基本から学ぶ
情報セキュリティと個人レベルのセキュリティ対策

2022年12月20日（火）
K-unet 石垣 英明

情報セキュリティとは

「情報の機密性、完全性および可用性を維持すること」をいう

見えない脅威とその対策

―個人レベルのセキュリティ対策―

最近のウイルスは経済的利益を狙ったものが多い。

感染の兆候が目に見えず、脅威がみえにくい特徴がある。

※ウィルス、スパイウェア、ボット、フィッシング詐欺、ワンクリック請求、ランサムウェア等

適切な対策で情報を守る

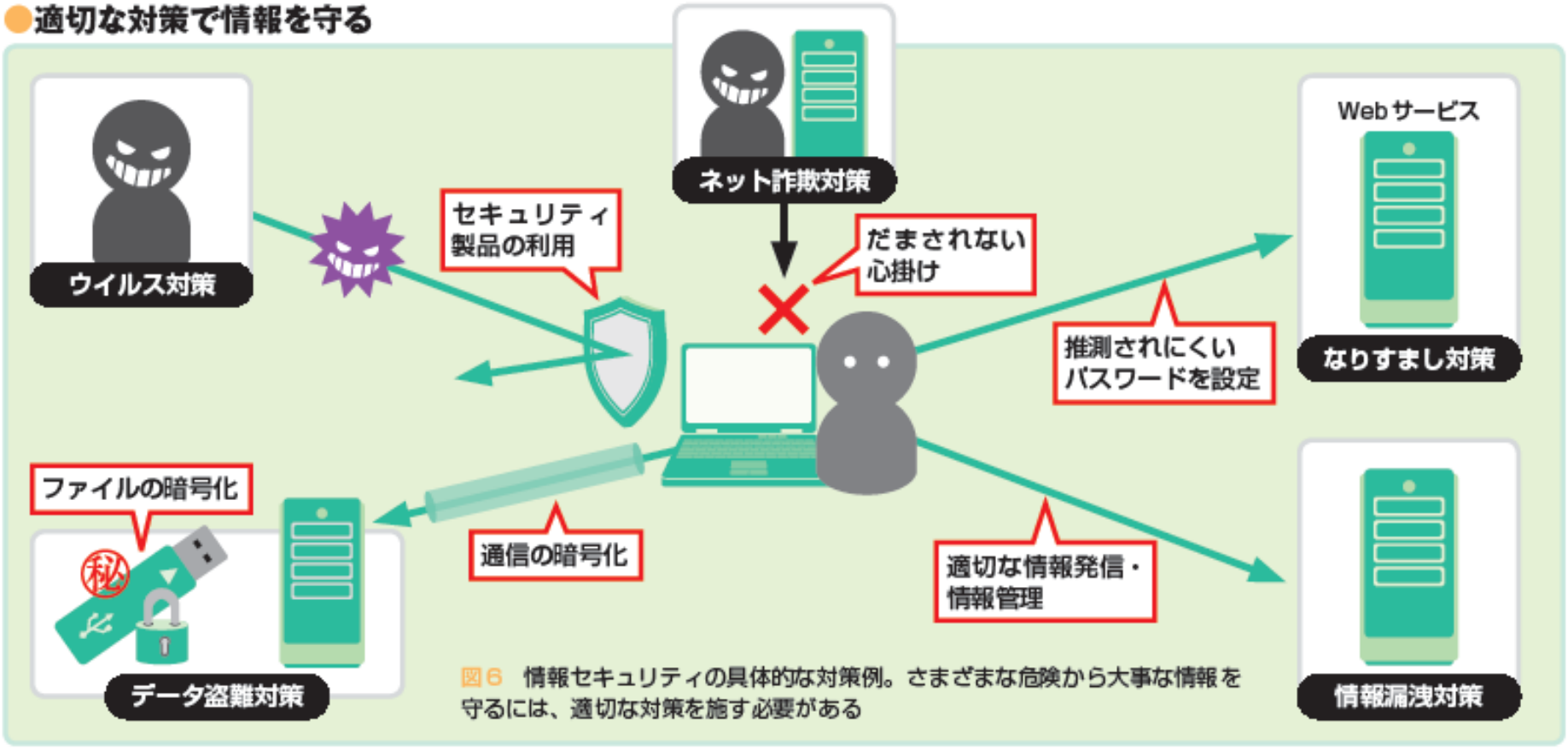


図6　情報セキュリティの具体的な対策例。さまざまな危険から大事な情報を守るには、適切な対策を施す必要がある

●ウイルスからはさまざまな被害を受ける

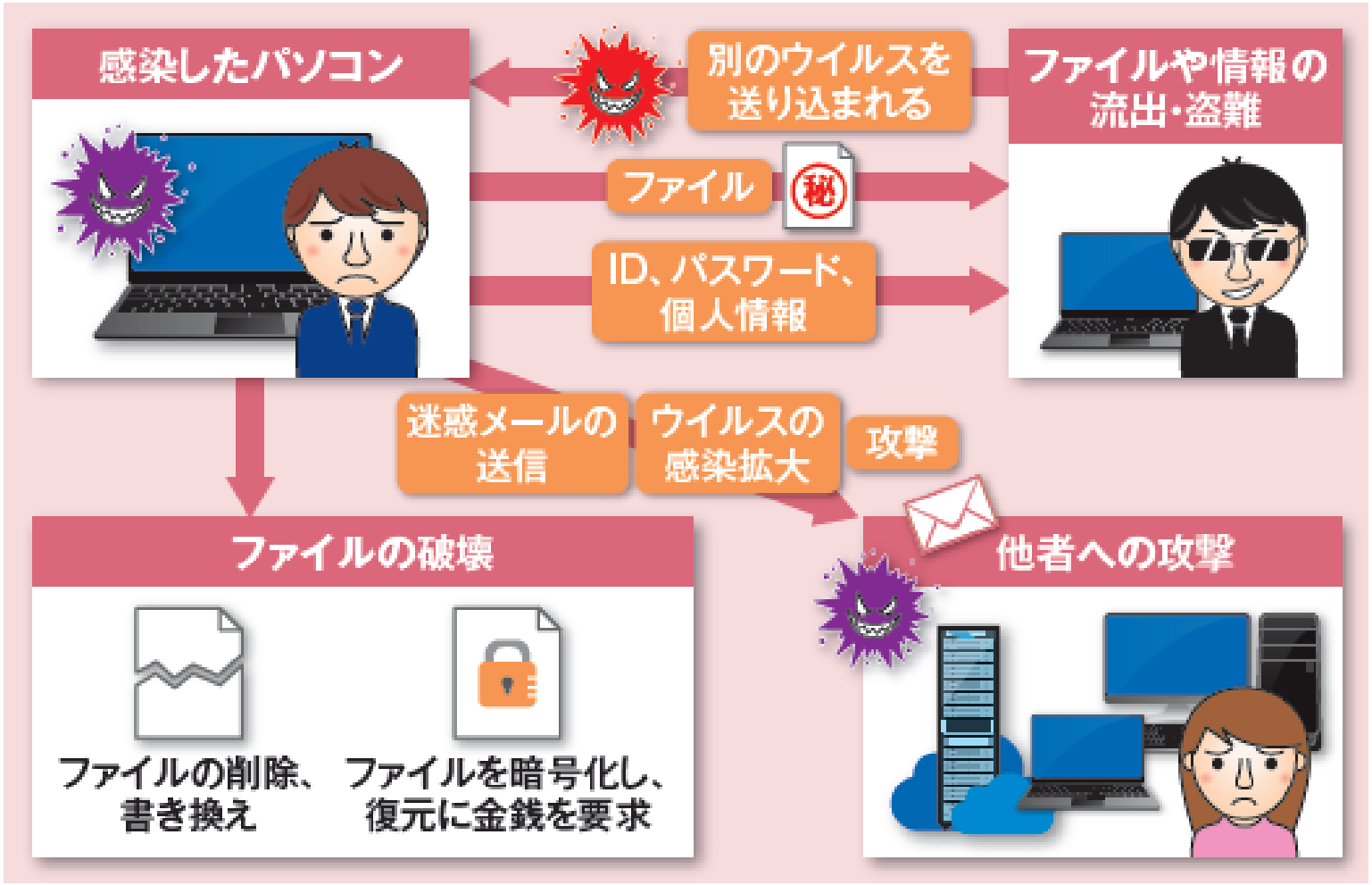


図 1　ウイルスの被害は多岐にわたる。パスワードなどが悪用されて別の被害につながる場合もある。また、自分が被害を受けるだけでなく、他者を攻撃する悪事に加担させられてしまう場合もある

インターネットの安全性や信頼性を脅かす事例

- １．盗み読み
- ２．なりすまし
- ３．不正アクセス
- ４．情報の改ざん・窃盗
- ５．踏み台にした不正アクセス
- ６．サービス不能攻撃
- ７．コンピューター・ウイルス（マルウェア）
- ８．ネット上での詐欺
- ９．迷惑メール
- １０．不適切コンテンツ
- １１．身代金を要求するランサムウェア

情報セキュリティの10大脅威

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等の ニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる スマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
インターネット上のサービスからの 個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬ IT 基盤の障害に伴う業務停止
インターネット上のサービスへの 不正ログイン	10	不注意による情報漏えい等の被害

000096899.pdf (ipa.go.jp)

セキュリティ10大脅威

ウイルスの脅威

- 「ウィルス」とは、ユーザが知らない間に、Webページやメールを介してパソコンに侵入し、パソコン内のデータを破壊したり、ほかのコンピュータに増殖したりする機能を持つ悪意のあるプログラムの総称。

機能	説明
発病機能	プログラムやデータの破壊、コンピュータに異常な動作をさせたりする機能
自己伝染機能	自分自身をほかのコンピュータにコピーして伝染する機能
潜伏機能	特定の時刻や一定時間、処理回数などの条件が整うと発病する機能

ウィルスの侵入経路

- **メールからの感染**

  最近のウィルス感染の多くはメールによるものです。ウィルスがメールの添付ファイルとして送られ、そのファイルを開くことで感染してしまうケースがある。また、HTMLメールを画面に表示するだけで感染するものもある。

- **USBメモリなどの移動媒体からの感染**

  ウィルス感染しているファイルを含むUSBメモリなどを組織内に持ち込むことで感染してしまうケースがある。

- **悪意のあるWebページを閲覧して感染**

  インターネット上のWebページを閲覧しただけでウィルスに感染してしまうケースがある

- **インターネット上からダウンロードしたファイルからの感染**

  インターネット上に公開されているファイルの中には、悪意のあるものが作成したウィルスプログラムが含まれている場合があります。このファイルをダウンロードして感染してしまうケースがある。

- **インターネットに接続しただけで感染**

  OSなどのプログラムに欠陥がある場合、インターネットに接続しただけで感染してしまうケースがある。

ウイルスの種類

種類	説明
フィルム感染型	拡張子がcomやexeなどの実行型ファイルに感染して制御を奪い、感染、増殖するウィルス
ワーム型	ネットワークを通じて他のコンピュータに伝染することを目的としたウィルスです。ほかのプログラムに寄生せずに自動的に増殖する。
トロイの木馬型	無害を装い利用者にインストールさせ、データを盗んだり削除したりすることを目的としたウィルス。基本的にほかのコンピュータには増殖しない。
マクロ型	Micirosoft社のOffice製品に感染するウィルスです。コンピュータの種類やOSの種類には依存しない。
ボット型	コンピュータを外部から操り、特定のコンピュータを攻撃するためのプログラム。ボットに感染したコンピュータ同士は、ボットネットワークを形成し、攻撃者からの命令によって、ボットネットワーク内のコンピューターが一斉に特定のコンピュータに攻撃をしかける。

スパイウェア

スパイウェアとは、ユーザの知らないうちにコンピュータにインストールされて、ユーザの個人情報やアクセス履歴などの情報を収集するプログラムのこと。収集した情報は、スパイウェアの作成者などに送信されるようになっている。

スパイウェアは、ほかのソフトウェアに添付されていることが多く、そのソフトウェアをインストールすることによって、同時インストールされる。

ソフトウェアのインストール時に表示されるソフトウェアの使用許諾契約などに「このソフトウェアは、ユーザーの使用状況などを確認するような仕組みを持っています」といった文面でスパイウェアについて説明されていることがありますが、使用許諾契約をじっくり読むユーザは少なく、スパイウェアの存在に気付かないままインストールしている。

国民のための情報セキュリティサイト

知らぬ間に大量の広告メールを発信者に・・・　犯人はBOT！あなたのPCも攻撃の踏み台になるかもしれない。

- 感染したパソコンをまるでロボットを操るようにリモートコントロールしてしまうから、たちの悪いことこの上ない。感染したパソコンを集めて「botnet(ボットネット）」をつくり、他のコンピュータシステムを攻撃するなど、その脅威は高まっているから要注意。

どうやって感染？メールやセキュリティホール、Webサイトからのダウンロード、共有フォルダに不正侵入など感染経路はさまざま

ウイルス感染した！？

●いつの間にか見知らぬファイルが作成されている
●送信した覚えのないメールが送信されている
●OSやソフトウェアが頻繁に異常停止する
●Webページが自動的に開く
●パソコンの動作が遅くなった
●操作していないのにハードディスクのアクセスがよくある
●操作していないのにルータのアクセスランプが頻繁に点滅している
●パソコン起動時にウィルス対策ソフトが起動されなくなっている
●ウィルス対策ソフトの更新用Webサイトにアクセスできない
●Windows UpdateのWebサイトにアクセスできない

ウイルスに感染した時は、

（1）ウイルスを拡散しないため、インターネット接続やネットワーク接続を遮断する。

（2）セキュリティソフトで駆除

再起動の際に動作するウイルスもあるのでまずは駆除しよう。

ウィルスの予防

- セキュリテイソフトの定義ファイルを最新にすること
- セキュリティソフトは最新版にすること！
- ウィンドウズ・アップデートは速やかに適用すること
- ソフトのアップデートも定期的に実行すること

独立行政法人情報処理機構（IPA）セキュリティセンター

https://www.ipa.go.jp/security/anshin

定義ファイルとは
ウィルスを特定するための情報が記載されたファイル。このファイルにはウィルスの特徴が記されており、この特徴と一致する情報を持ったファイルをウィルスとして認識する。新種のウィルスは日々世界中で発生するため、古いウィルス定義ファイルのままだと最新のウィルスを発見することができない。最新のウィルス定義ファイルは、ウィルス対策ソフトの開発元から定期的に提供されるので、常に最新のものに更新するようにする。

ウィルス対策ソフト

機能	説明
ウィルスの侵入防止	パソコン内にウィルスが侵入することを防ぎます。メールの受信時やファイルを開く際に、ウィルスがいるかどうかを監視。
ウィルスの検出	すでにパソコン内にウィルスが侵入しているかどうかを検査する。
ウィルスの駆除	ウィルスを発見した場合、ウィルスを削除する。

ウィルス定義ファイル（パターンファイル）というものを常に最新にしておくこと！

ウイルス対策のポイントを知る（1）

●被害が拡大している「Emotet」

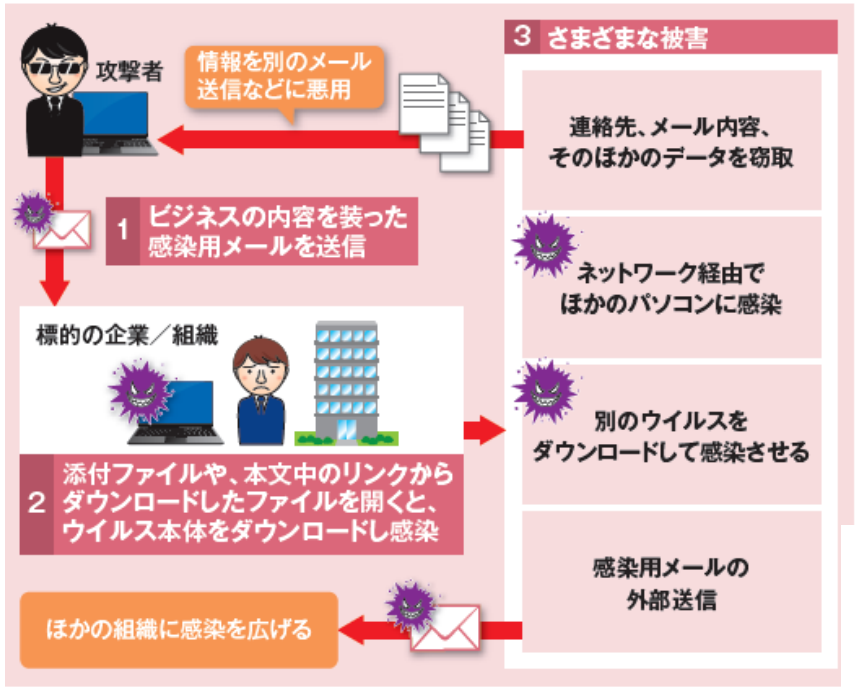


図7 「Emotet」は、主に取引先などを装ったメールを通じて感染。端末からメールやパスワードなどの情報を盗むだけでなく、さまざまな被害を与える

ウイルス対策
（１）OSのウイルス対策機能やセキュリティソフトを動作させておくこと。常時システムを監視することでウイルスを検知し、動作を止め、削除する。

●ウイルス対策の種類

パターン検知	振る舞い検知	サンドボックス
既知のウイルスのデータベースとファイルを照合する	プログラムの危険な動作を検知する	プログラムを仮想環境で実行して動作を検査する

レピュテーション（評判）検知	そのほかの対策
既知のウイルスのデータベースとファイルを照合する	ファイアウオール、Webフィルタリング、メールスキャンなど

図10 ウイルス対策は、主にパターン検知などのウイルス自体を検知する仕組みが中心となる。そこに、ファイアウオールなど複数の方式を組み合わせて、より高度なセキュリティを実現している

ウイルス対策のポイントを知る(2)

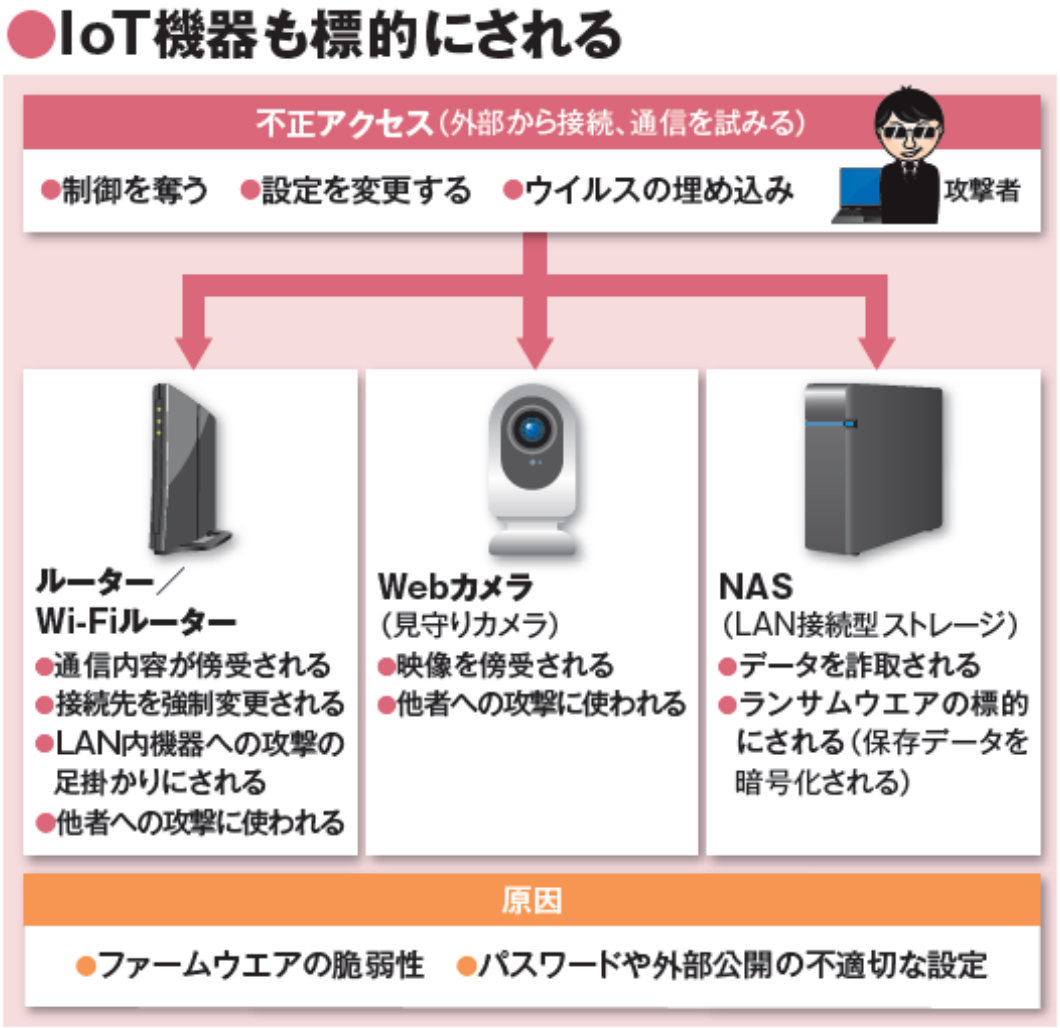


図18　通信用のルーターやWi-Fi機器、ネット接続型のカメラ、NASといったIoT機器もサイバー攻撃の対象になる。機器自体にウイルスが仕込まれ、悪用される場合もある

ウイルス対策
（２）OSやアプリなどの更新を欠かさず、できるだけ早く最新状態に保つこと。これらは、発売後にプログラムの問題点が発見されることが多い。そのなかに、ウイルスの感染や不正アクセスといった攻撃を助けてしまうものがあり。
「脆弱性」とよばれている。

インターネット上のトラブル防止

- フィッシング詐欺防止機能を活用すること
- 検索結果にも注意すること
- パスワードや個人情報を入力するときはアドレスと証明書を確認すること
- 脅迫ページが出ても慌てることなく処理

フィッシング詐欺とは
偽者のホームページに誘い込んで、重要な個人情報を盗み取る詐欺のこと。「フィッシング」とは「sophisticate」(間違っていることを正しいと仕向けて欺く)と「Fishing」(釣り)を合せた造語で、「Phishing」とつづる。

フィッシングの手口

●よくあるフィッシングの手口

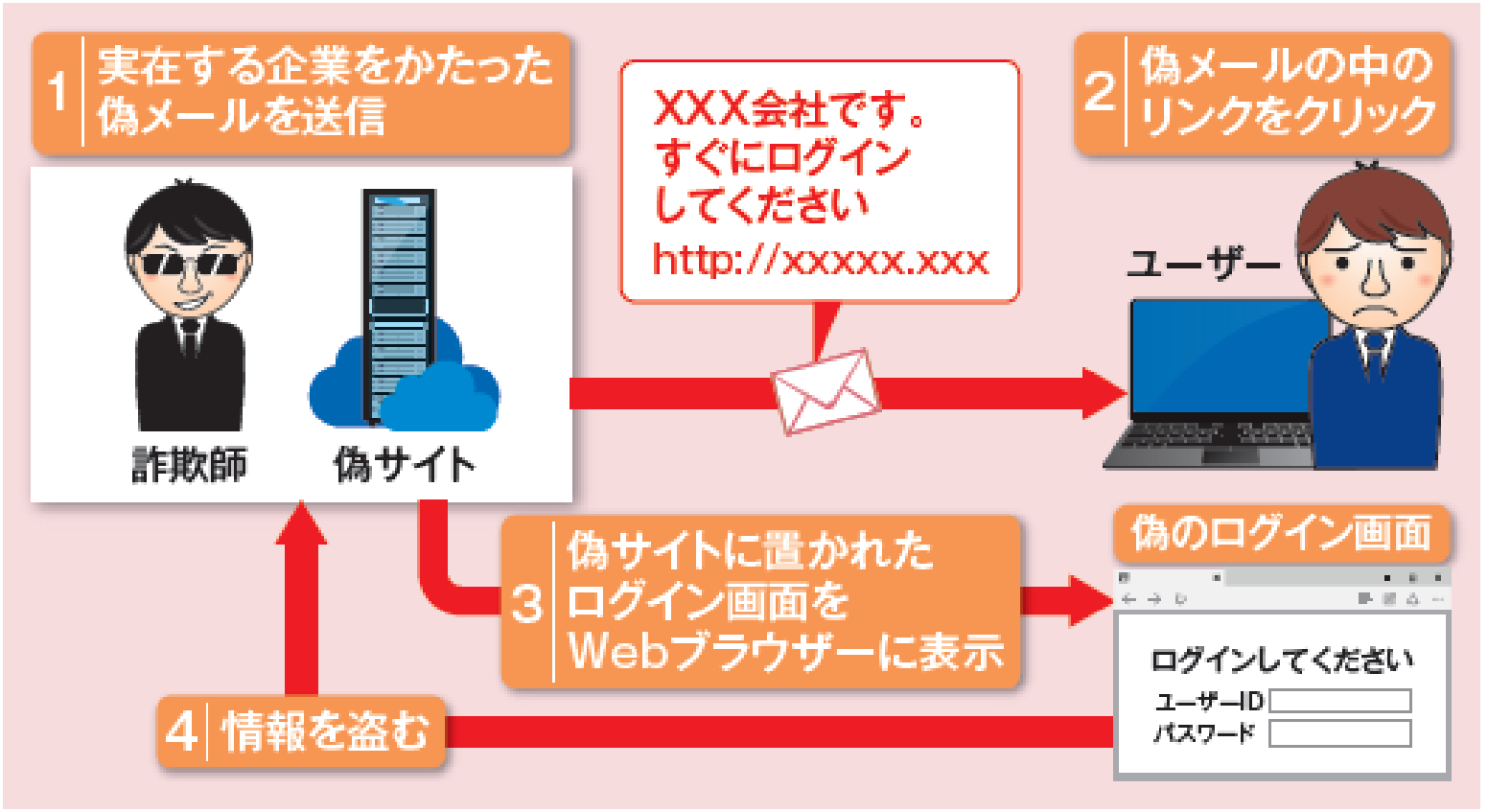
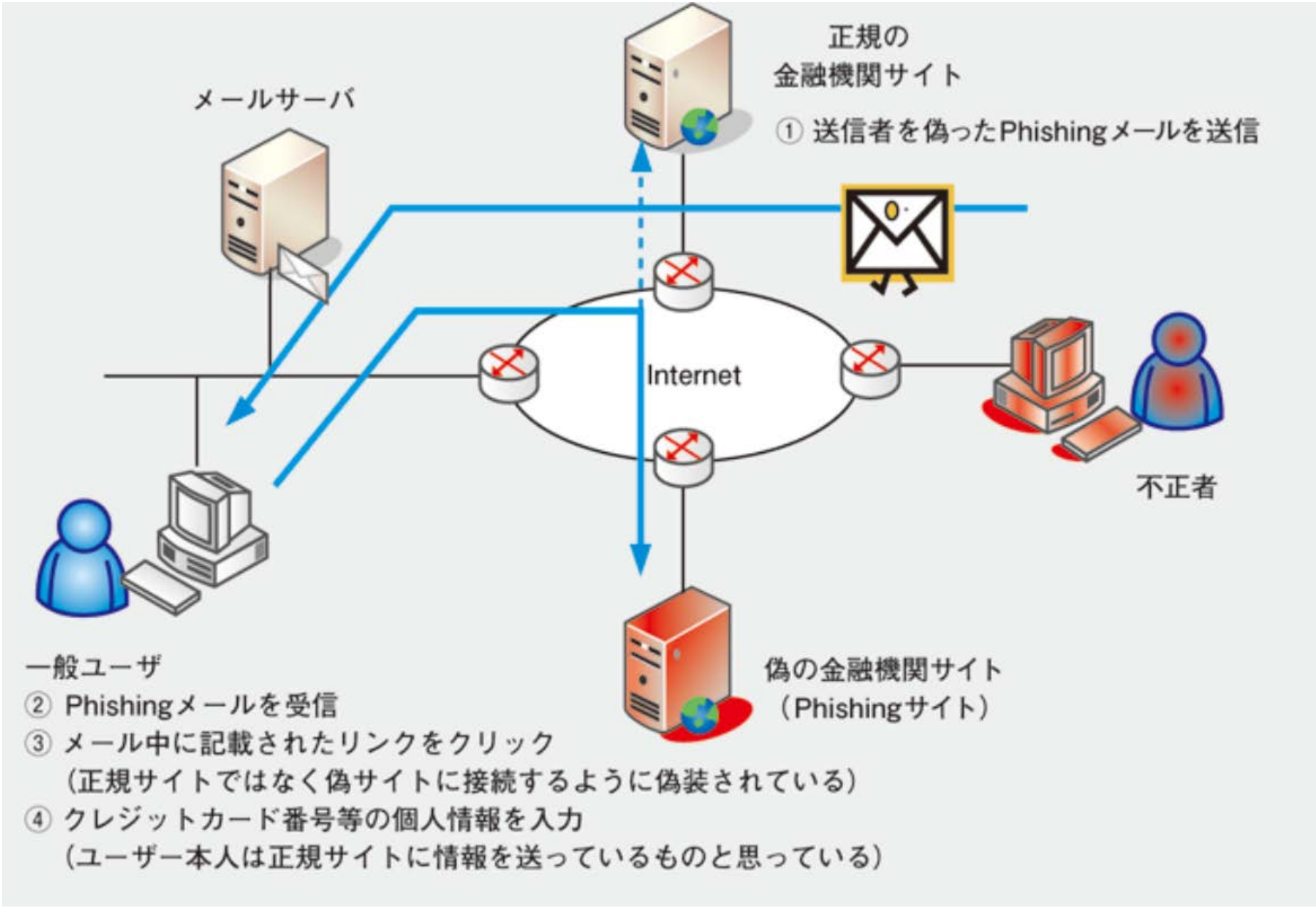
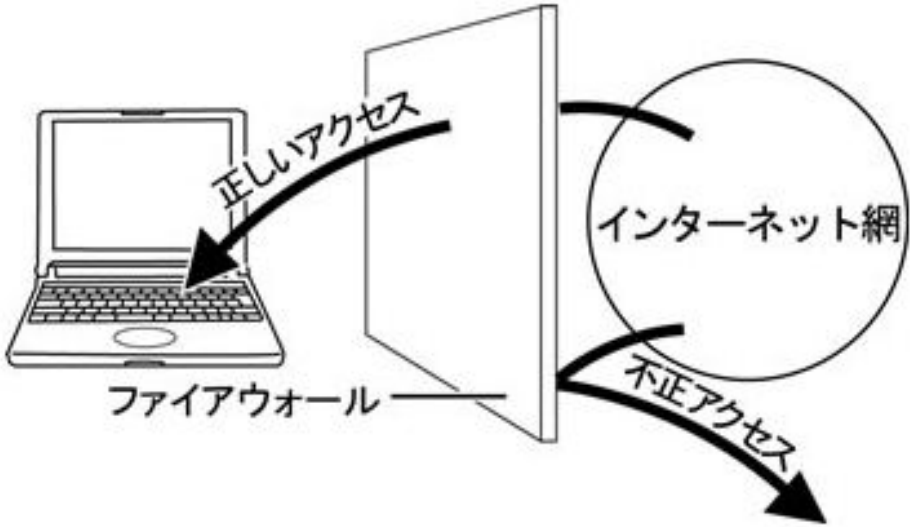


図2　実在の企業やサービスを装ったメールが届く。受信者が本文中のリンクをクリックすると偽のページに誘導され、そこで入力した情報が盗まれてしまう


正規の
金融機関サイト
① 送信者を偽ったPhishingメールを送信
メールサーバ
Internet
不正者
一般ユーザ
② Phishingメールを受信
③ メール中に記載されたリンクをクリック
(正規サイトではなく偽サイトに接続するように偽装されている)
④ クレジットカード番号等の個人情報を入力
(ユーザー本人は正規サイトに情報を送っているものと思っている)
偽の金融機関サイト
(Phishingサイト)

Windows ファイアウォールとは

ネットワーク(インターネットなど)経由の不正なアクセスからパソコンを守るためのセキュリティシステム(壁)のことです。
ネットワークとの間でやり取りされるデータを規制して、認められているデータ以外は通過できないようにすることで、不正なアクセスを防ぎます。
インターネットには、セキュリティ機能を設定していない無防備なパソコンをねらった悪質な攻撃もたくさん存在しています。Windows ファイアウォールは、これらの攻撃にも有効な機能です。



ファイアウォールとは、ネットワークの外部からの侵入を防ぐしくみのことで、パソコンへのデータの出入りをチェックし、許可した通信以外をブロックする機能

仕事関係者を装って偽メールを送り付けるウイルス「エモテット」

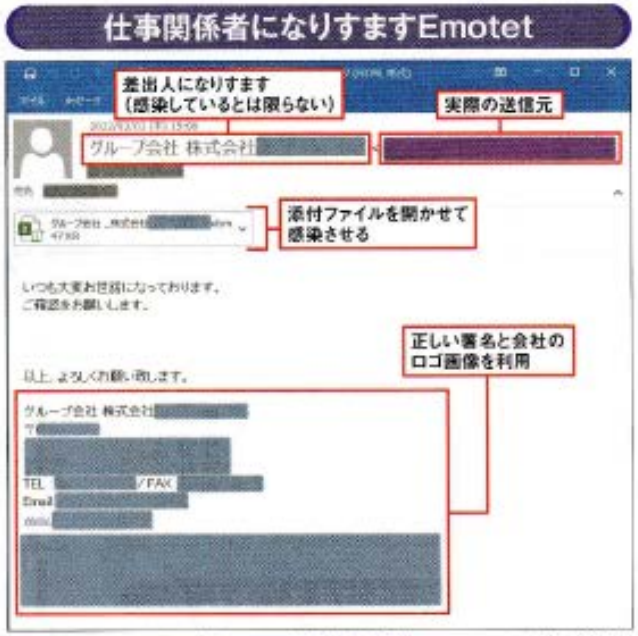


図8 Emotetによる偽メールの例（画面提供：JPCERT/CC）。差出人をなりすましたり、過去の文面を引用したりしてユーザーをだます。主にExcelやWordといったOffice文書を添付して、マクロ機能を実行させてウイルスに感染させる。文面は一例で非常に多くのパターンがある

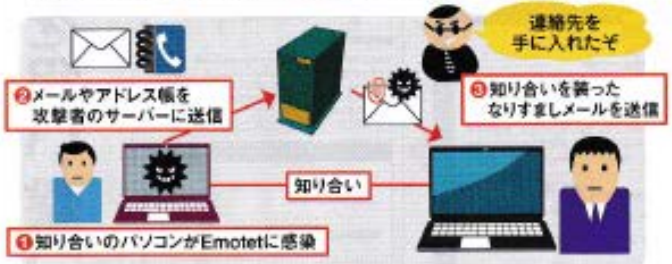


図9 Emotetに感染したパソコンから連絡先やメールの文面を盗み、それらを悪用して偽のメールをばらまく［注2］。Office文書だけでなく、パスワード付きのZIPファイルやショートカットファイル、PDFを添付したり、URLのリンク先からダウンロードさせたりするパターンもある

図10 JPCERT/CCが無償で提供している「EmoCheck」で感染の有無を確認できる。「検知されませんでした」と表示されたらひとまずは安心だ

図5 えきねっとやJR東日本をかたる偽メール。えきねっとには長期間ログインしていないユーザーを自動退会させる規約があり、それに便乗した手口だ。偽のログイン画面を経て、個人情報とクレジットカード情報を入力させる。本物そっくりのクレジットカード認証画面に遷移するなど手が込んでいる。最後に公式サイトへ移動する

差出人とURLを厳重チェック

図6 偽メールを見破るには差出人とリンク先をチェックする（左）。ただし、差出人は本物のアドレスに偽装できるため100％は信用できない。URLは必ずマウスポインターを合わせて確認する。一見、正規のURLでも実際には異なるリンクでだますので要注意だ（右）

図7 スマホはパソコンのようにリンクを右クリックできないが、通常は長押しでURLがわかる

フィッシング詐欺（1）

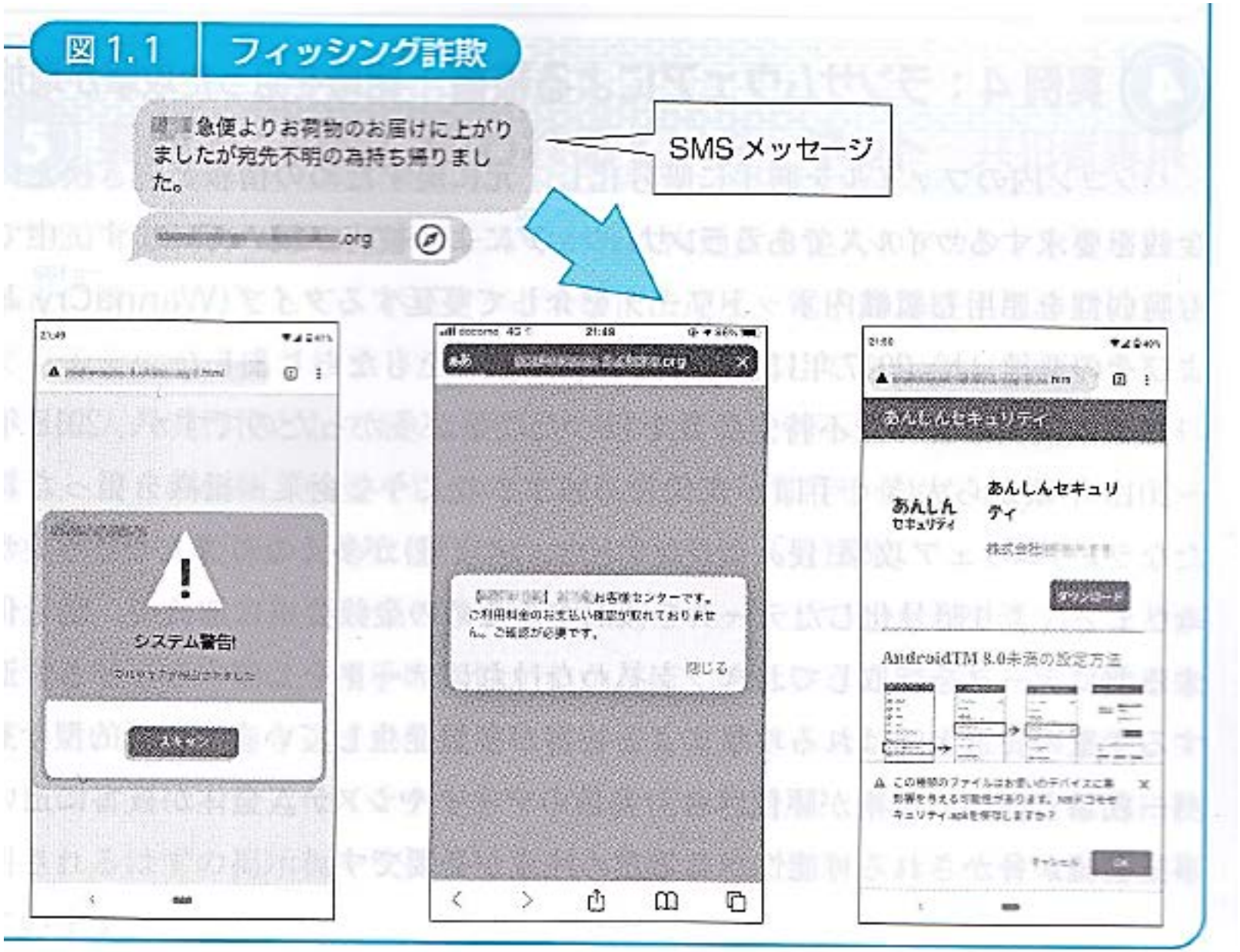
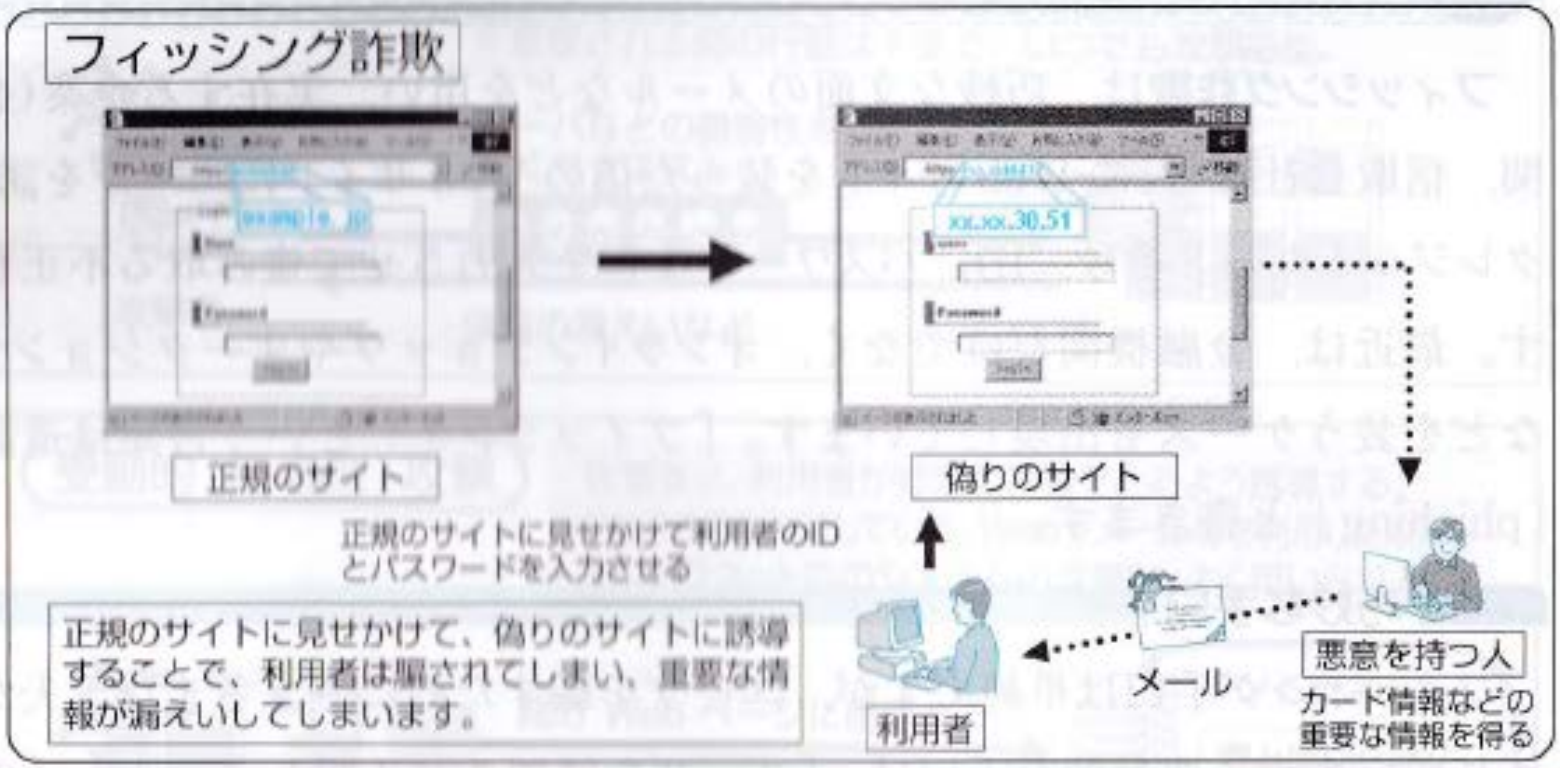


図 1.1 フィッシング詐欺
急便よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。
.org
SMS メッセージ
システム警告!
スキャン
お客様センターです。
ご利用料金のお支払い確認が取れておりません。ご確認が必要です。
閉じる
あんしんセキュリティ
あんしん
セキュリティ
あんしんセキュリティ
ダウンロード
AndroidTM 8.0未満の設定方法
Ok

フィッシング詐欺（2）

図 3.13　フィッシング詐欺

金融機関（銀行やクレジット会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為



フィッシング詐欺メール

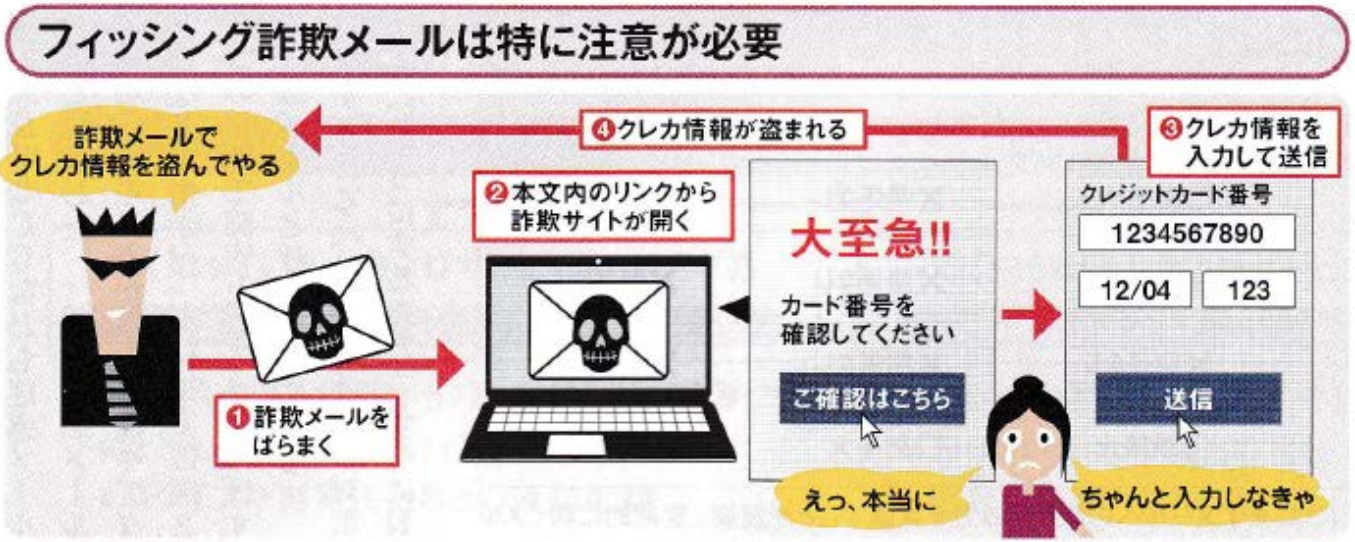


図7 フィッシング詐欺メール（詐欺メール）にだまされると金銭的な被害に遭う。メール本文内のリンクをクリックして開いた詐欺サイトでクレジットカード情報を入力すると、カードが不正に利用されてしまう（❶～❹）。古典的な手法だが被害件数はいまだに非常に多い

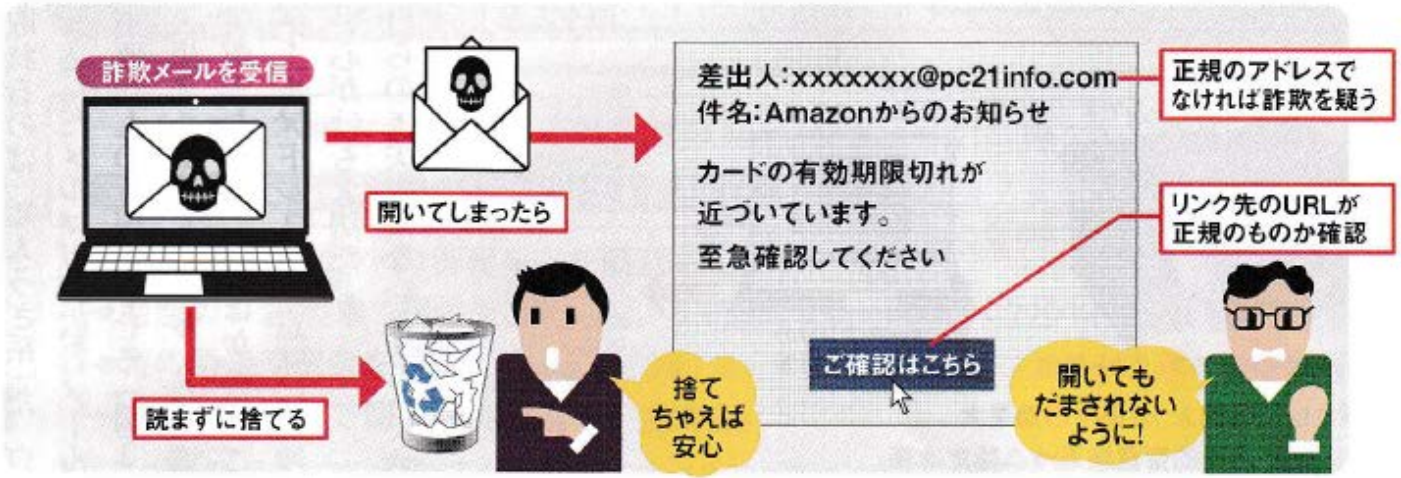


図8 詐欺メールは迷惑メールフィルターをくぐり抜けることもある。その場合は自力での対策が必要だ。明らかに怪しければ読まずに捨てるのが基本。開いてしまったときは送信者のメールアドレスやURLのリンク先を調べることで詐欺メールだと見抜ける

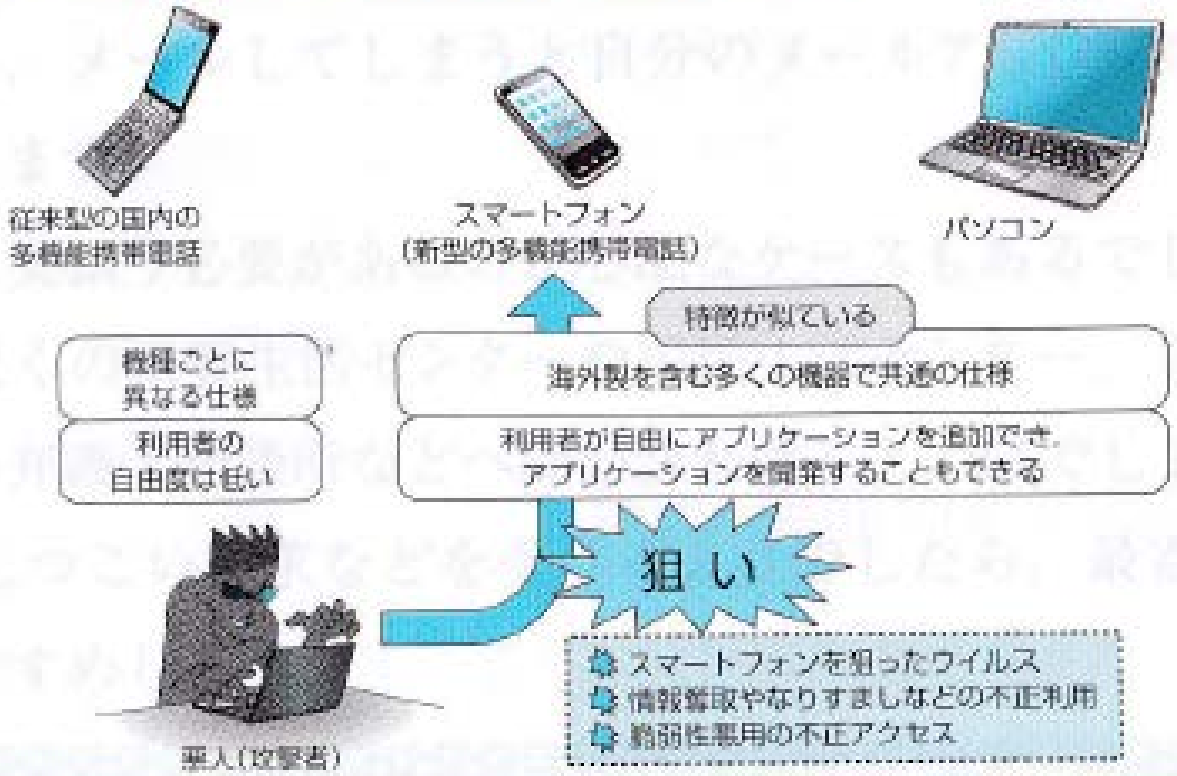
フィッシング詐欺への対策

- （1）メールの送信元（差出人）や本文内容について安易に信用しない。
- （2）リンクを安易にクリックしない。
- （3）リンク先が正規のWebサイトかどうか確認する。
- （4）SSL/TLS接続されていないWebサイトでは重要情報を入力しない。
- （5）フィッシング対策用のソフトウェアを使用する。

https://www.antiphishing.jp

スマートフォンの脅威と対策

図 3.15　スマートフォンを狙ったウイルス



スマートフォンのセキュリティ対策

- 信頼できるサイトからインストールすること
- アプリに許可する権限を確認すること
- 脅威や手口を知ること
- 認証の強化・データの暗号化・バックアップ
- 公衆無線LANの利用はリスクがあると理解
- パスワードを使い回さないこと
- OS・アプリの更新
- セキュリテイソフトの導入

スマホに届く巧妙なメッセージにだまされるな

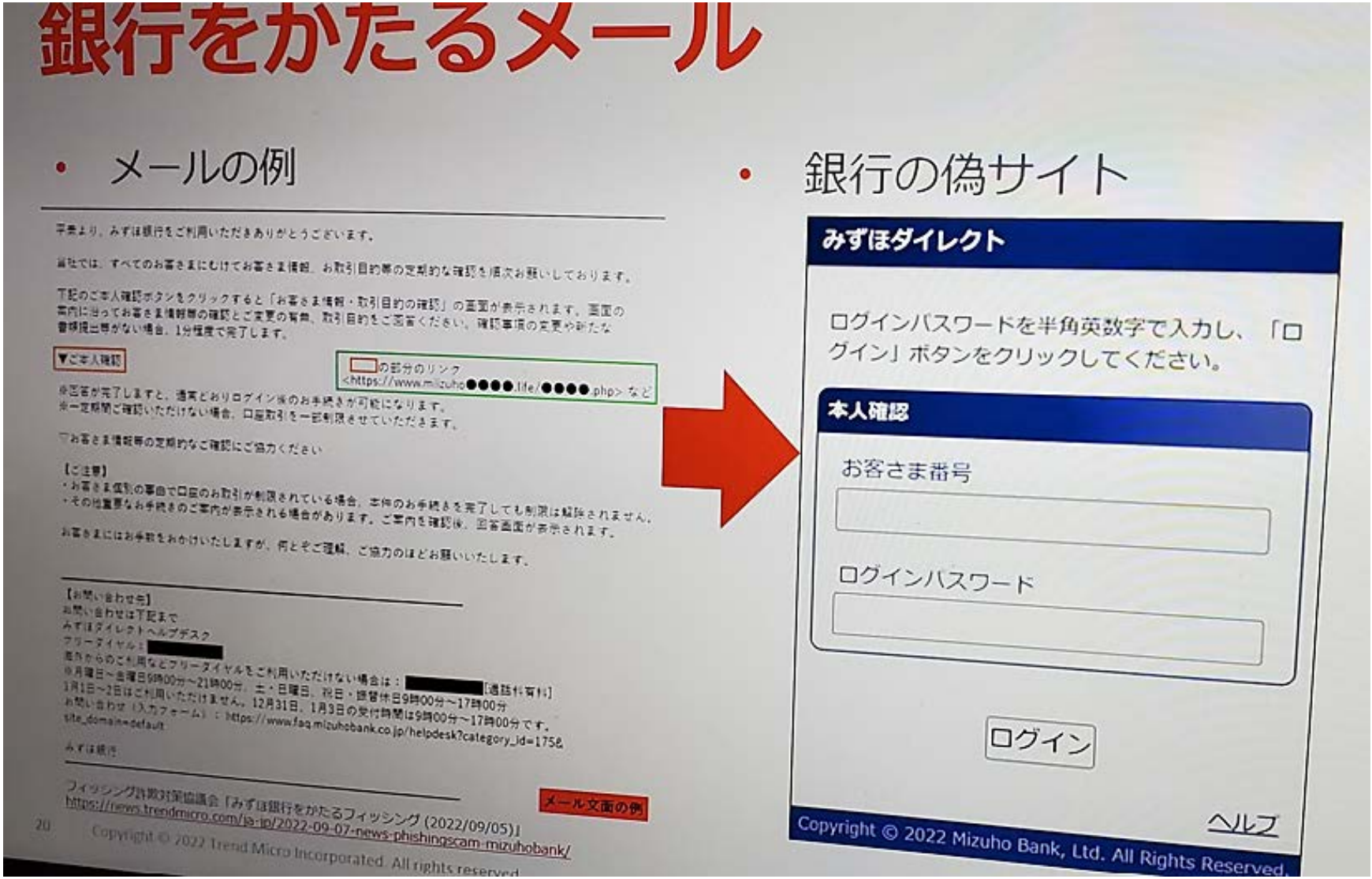
図1 SMSでスマホに届くフィッシング詐欺のうち、2018年ごろから目立ち始めたのが宅配便事業者を装った不在通知。最近増えているのが、携帯電話事業者をかたる料金未払いの通知だ。リンク先にアクセスした端末がAndroid（アンドロイド）かiPhoneかで手口を変えてくるケースもある。個人情報が漏洩したり、電子マネーを盗み取られたりする恐れがあるので要注意だ

iPhoneではアカウント情報や電子マネーを盗む

Androidには不正なアプリをインストール

LINEの「友だち」でも信用できない

銀行をかたるメール


銀行をかたるメール
• メールの例
平素より、みずほ銀行をご利用いただきありがとうございます。
当社では、すべてのお客さまにむけてお客さま情報、お取引目的等の定期的な確認を順次お願いしております。
下記のご本人確認ボタンをクリックすると「お客さま情報・取引目的の確認」の画面が表示されます。画面の案内に沿ってお客さま情報等の確認とご変更の有無、取引目的をご回答ください。確認事項の変更や新たな書類提出等がない場合、1分程度で完了します。
▼ご本人確認
の部分のリンク
<https://www.mizuho●●●●.life/●●●●.php> など
※回答が完了しますと、通常どおりログイン後のお手続きが可能になります。
※一定期間ご確認いただけない場合、口座取引を一部制限させていただきます。
□お客さま情報等の定期的なご確認にご協力ください
【ご注意】
・お客さま個別の事由で口座のお取引が制限されている場合、本件のお手続きを完了しても制限は解除されません。
・その他重要なお手続きのご案内が表示される場合があります。ご案内を確認後、回答画面が表示されます。
お客さまにはお手数をおかけいたしますが、何とぞご理解、ご協力のほどお願いいたします。
【お問い合わせ先】
お問い合わせは下記まで
みずほダイレクトヘルプデスク
フリーダイヤル：
[redacted]
[通話料有料]
※月曜日～金曜日9時00分～21時00分、土・日曜日、祝日・振替休日9時00分～17時00分
1月1日～2日はご利用いただけません。12月31日、1月3日の受付時間は9時00分～17時00分です。
お問い合わせ（入力フォーム）：https://www.faq.mizuhobank.co.jp/helpdesk?category_id=1758&site_domain=default
みずほ銀行
メール文面の例
フィッシング詐欺対策協議会『みずほ銀行をかたるフィッシング（2022/09/05）』
https://news.trendmicro.com/ja-jp/2022-09-07-news-phishingscam-mizuhobank/
20
Copyright © 2022 Trend Micro Incorporated. All rights reserved.
• 銀行の偽サイト
みずほダイレクト
ログインパスワードを半角英数字で入力し、「ログイン」ボタンをクリックしてください。
本人確認
お客さま番号
ログインパスワード
ログイン
ヘルプ
Copyright © 2022 Mizuho Bank, Ltd. All Rights Reserved.

国税庁をかたるメール

国税庁をかたるメッセージ

- メッセージの例

差押最終通知

納税確認番号:****6309

あなたの所得税（または延滞金（法律により計算した客勘 について、これまで自主的に納付されるよう催促してきま したが、まだ納付されておりません。もし最終期限までに 納付がないときは、税法のきめるところにより、不動産、自動車などの登記登録財産や給料、売掛金などの債権など の差押処分に着手致します。

滞納金合計:10628円
納付期限:2020/08/15
最終期限:2022/08/15

お支払いへ

- 国税庁の偽サイト

←不安を煽るような言葉で
クレジットカード番号の入力を
促し、情報を盗みます

フィッシング詐欺対策協議会「国税庁をかたるフィッシング (2022/08/15)」

国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意
―不審なショートメッセージやメールのURLに触れないで！―

図1：国税庁をかたる偽SMS等のURLから悪意あるサイトへ誘導される

インターネット利用中の誘導

不正アクセスとは

- 不正アクセスって何？
  - 不正アクセスとは、パソコンやシステムにアクセスする権限がないユーザーが、不正にパソコンやシステムを利用することの総称。
  - パソコンやインターネットの普及にともなって、不正アクセスによる被害が急増している。
  - 不正アクセスの手口

    他人のユーザーID,パスワードを不正に利用する

    セキュリティホールを攻撃して侵入する

不正アクセスの対策

- 不正アクセスって何？（ユーザーIDの不正使用、システムへの侵入、踏み台）
- 不正アクセスの被害（情報の破壊・改ざん、情報の盗難・漏えい、踏み台）

- 不正アクセスの対策
  - **ユーザーID・パスワードをきちんと管理すること（オートコンプリートの設定）**
  - **ファイアウォール（Windowsファイアウォールの設定）**
  - **不正アクセス禁止法**

インターネット利用上のトラブル対策

- 個人情報の取り扱い
  - 個人情報が狙われている！？(氏名、住所、電話番号、生年月日)
  - ソーシャルエンジニアリングって何？(なりすまし、トラッシング、侵入、のぞき見)
  - 移動媒体の取り扱い
- インターネット上のトラブル
  - Webページの閲覧(ワンクリック詐欺、怪しいWebページ、不当な料金請求、Cookie)
  - メールを利用するときの注意点
    - フィッシング
    - HTMLメール
    - メールの宛先指定
- ソフトウェアを使用するときの注意点
  - ファイル交換ソフト
  - スパイウェア

迷惑メールはなぜ届くのか

サーバーを攻撃して盗み出す

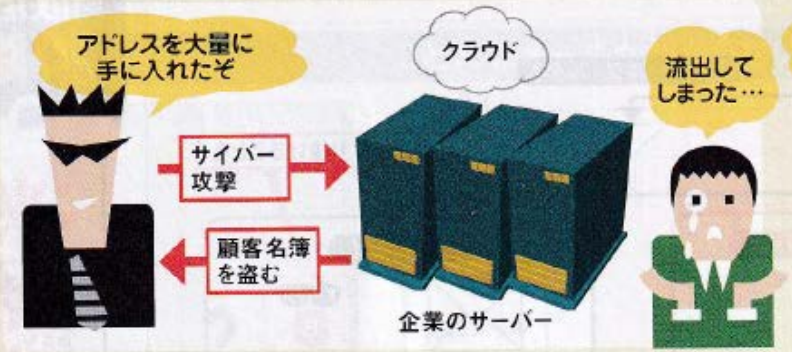


図3 会員情報を管理している企業のサーバーにサイバー攻撃を仕掛け、顧客情報を盗む手口も多い。ユーザーの落ち度の有無とは無関係に、企業が個人情報を流出させてしまうケースだ。個人情報に含まれるメールアドレスに迷惑メールが届く

ウイルスに感染させて盗み出す

図1 個人情報を盗む機能を持つウイルスに感染すると、パソコン内に保存された連絡先（アドレス帳）などの情報を送信されたり、遠隔操作で盗まれたりすることがある（❶～❸）。メールに仕込まれた実行ファイルやアプリなどから感染する

どこかしらでメルアドを購入している

図4 メールアドレスなどの個人情報を名簿業者やダークウェブ（匿名闇サイト）で購入しているケースもある。現状では通常のインターネット上でも普通にアドレスが販売されている

サイトに記載されたメルアドを盗む

図2 ネット上のサイトをくまなく徘徊して情報を集めるプログラムを「ロボット」あるいは「ボット」と呼ぶ。悪徳業者はこれを利用して、SNSなどに記載されたメールアドレスを自動で収集する

迷惑メール(スパム)対策

- 迷惑メールで宣伝されている物品やサービスを絶対に購入しない
- 踏み台にさせない(ボットに感染させない)
- 迷惑メールを開かない
- 迷惑メールの中のリンクをクリックしない
- アドレスを安易に登録しない
- ISPの無料対策サービスを利用する
- Webメールの「Gmail」を経由させる

＊商用目的かどうかによらず、宣伝や嫌がらせなどの目的で不特定多数に送信されるメールのこと。一般にSPAM(スパム)ともよばれる。

ネット詐欺の例

●ユーザーを狙うネット詐欺の数々

名称	手口	被害
ワンクリック詐欺	有料サイトに会員登録したと誤解させて料金を請求する	金銭
フィッシング詐欺	実在する企業をかたった偽メールで偽の Web サイトに誘導し、個人情報を入力させる	個人情報
出会い系詐欺	おとりのユーザー（サクラ）を使って、有料のサービスを利用させ続ける	金銭
情報商材詐欺	役に立たない情報を、有益な情報に見せかけて売りつける	金銭
オークション詐欺	架空の出品で落札者から金銭をだまし取ったり、出品者から商品を詐取したりする	金銭、商品
偽ソフト詐欺	ウイルスに感染したと思わせて、偽のセキュリティソフト（偽ソフト）を購入させる	金銭

表 1　ネット詐欺の例。詐欺師の目的は金銭。個人情報などを盗んだ場合も、情報を転売したり、別の詐欺に悪用したりすることで、最終的には金銭に換える

メールによる攻撃の被害にあわないための4箇条

- 第一条　怪しげなURLのリンクはクリックしない
- 第二条　怪しげなメールに返信しない
- 第三条　突然の送金指示メールは一人で判断せずに上司などに相談すること」
- 第四条　怪しげな添付ファイルは開かない（標的型メール）

複数のアカウントとパスワードを安全に管理しよう

図解

図 5.1　推測しにくいパスワードの付け方

■大文字・小文字・数字・記号をできるだけ多くの種類組み合わせる
■長いパスワード（10 文字以上）
■推測しづらく自分が忘れないパスワード（コアパスワード）
例：パスフレーズによる設計（日本語フレーズをもとに変換）

日本語フレーズ		パスワード
リンゴが好き	→	ringogasuki

■コアパスワードに，サービス毎に異なる識別子を付加
例：A銀行　→　識別子　A-GIN
　　B銀行　→　識別子　B-GIN
例：コアパスワードに識別子を付加
　　A銀行のパスワード　ringogasukiA-GIN
　　B銀行のパスワード　ringogasukiB-GIN

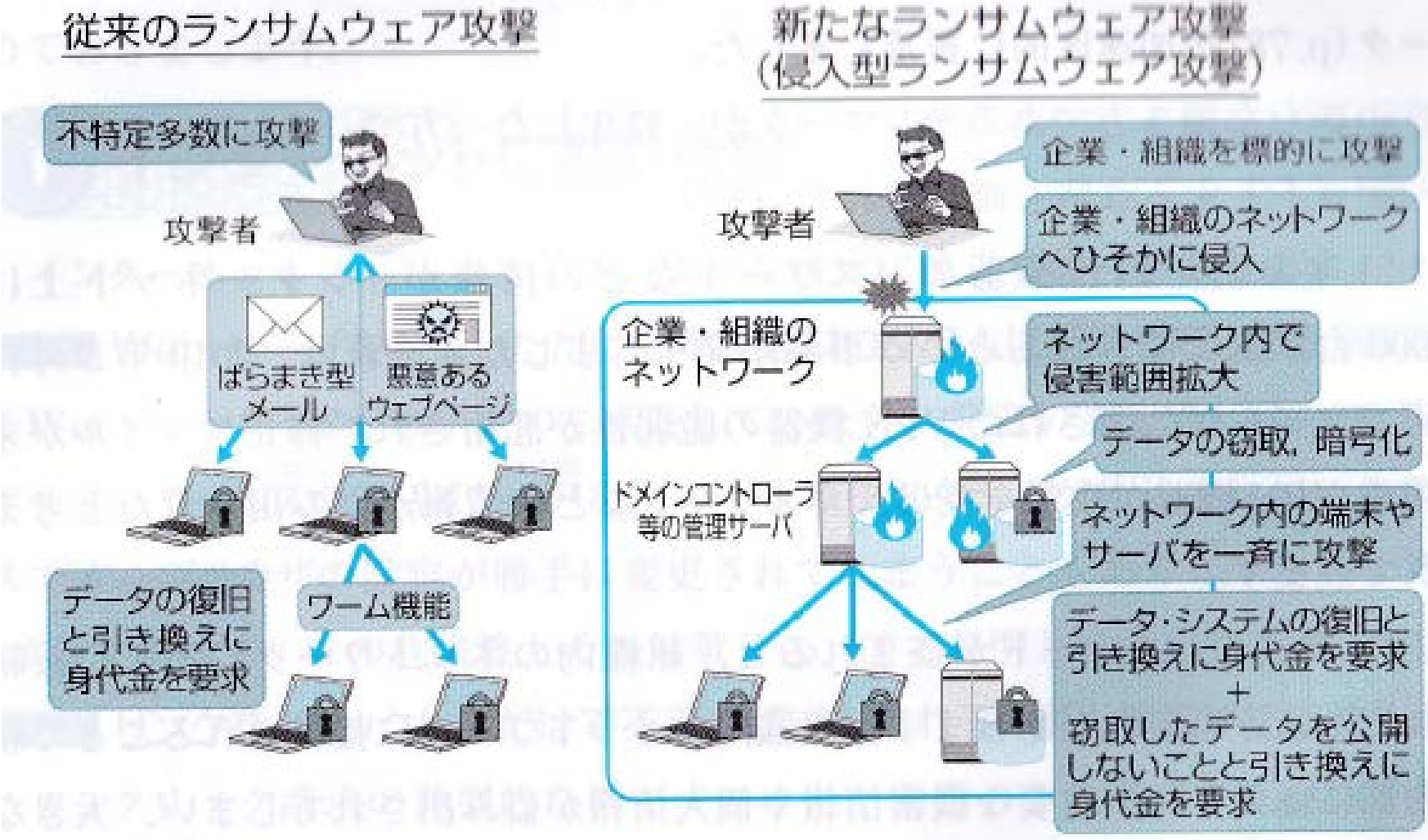
ランサムウェア

- ランサムウェアとは「Ransom(身代金）」と「Software(ソフトウェア)」を組み合わせた造語

　コンピュータに保存されている特定のファイル（オフィスドキュメントや圧縮ファイル、音楽、画像など）などに勝手に暗号化処理を行い、読み取れない状態にしたうえで画面上に金銭を要求する文書を表示。暗号化ファイルの復元が困難であるため、場合によっては組織の事業存続に致命的なダメージを与える可能性がある。

ランサムウェア

図 1.2　従来の／新たなランサムウェア攻撃の差異



スミッシング詐欺

- スマートフォンのショートメール「SMS」を利用した「フィッシング詐欺」のこと。SMSで送られてきたURLをクリックさせることで、偽のサイトに誘導し、個人情報やクレジットカード情報などを盗む詐欺のことをいう。配送業者からの不在連絡や、通販サイトからの不正ログイン検知を騙る詐欺が増えてきており、被害をSNSやYouTubeなどで警告している人も多い。
- スミッシング
- https://time-space.kddi.com/mobile/20210810/3156

スミッシング詐欺への対策法

●URLに誘導するSMSがとどいたときは、すぐにタップしない

●ドメインが正規サイトのものであるかを確認

●通知を確認する際は、できるだけSMSに記載されているURLはクリックせず、正規アプリか正規アプリからアクセスする習慣を身につける

●アプリをインストールする際は、URLからでなく、Google PlayやApp Storeなど公式アプリマーケットからインストールする習慣を身につける。

参考文献

●「IPA　情報セキュリティ読本　六訂版」
　実教出版
●シニア情報生活アドバイザースキルアップ
　研修テキスト2022年版
　　一般財団法人ニューメディア開発協会
●日経PC21　2022年12月号
　　ニセモノに騙されるな
●日経PC21 2022年4月号
　　迷惑メールはなぜ届くのか