■本資料のご利用にあたって（詳細は「利用条件」をご覧ください）

本資料には、著作権の制限に応じて次のようなマークを付しています。
本資料をご利用する際には、その定めるところに従ってください。

＊：著作権が第三者に帰属する著作物であり、利用にあたっては、この第三者より直接承諾を得る必要があります。

CC：著作権が第三者に帰属する第三者の著作物であるが、クリエイティブ・コモンズのライセンスのもとで利用できます。

：パブリックドメインであり、著作権の制限なく利用できます。

なし：上記のマークが付されていない場合は、著作権が東京大学及び東京大学の教員等に帰属します。無償で、非営利的かつ教育的な目的に限って、次の形で利用することを許諾します。

Ⅰ　複製及び複製物の頒布、譲渡、貸与
Ⅱ　上映
Ⅲ　インターネット配信等の公衆送信
Ⅳ　翻訳、編集、その他の変更
Ⅴ　本資料をもとに作成された二次的著作物についてのⅠからⅣ

ご利用にあたっては、次のどちらかのクレジットを明記してください。

東京大学　Todai OCW　工学倫理講演会
Copyright 2013,　独立行政法人　情報処理推進機構

The University of Tokyo / Todai OCW　Lectures on Engineering Ethics
Copyright 2013, Information-technology Promotion Agency, Japan

IPA

Information-technology Promotion Agency, Japan

ネットワークの脅威と情報セキュリティ
～ウイルス等ネットワークの脅威の変遷と対策～

2013年6月6日

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　主任研究員　小門寿明

Copyright © 2013 独立行政法人　情報処理推進機構

内　容

- コンピュータウイルス
  - ・ウイルスとは、感染経路
- 愉快犯から実害を与える脅威へ
  - ・スパイウェアとは、キーロガーとは
  - ・フィッシング(Phishing)とは、銀行の第二認証情報（乱数表の番号）の詐取
  - ・ボットとは、ボットネットワーク
  - ・遠隔操作ウイルス［感染］、［遠隔操作］
  - ・ワンクリック請求、偽セキュリティ対策ソフト
  - ・スマートフォンの情報流出、スマートフォンの不正なアプリ例
- 不正アクセス
  - ・不正アクセスとは、不正アクセスの事例
- セキュリティ対策
  - ・感染防止対策(ウイルス、スパイウェア)
  - ・フィッシング対策
  - ・スマートフォンのセキュリティ対策
  - ・ファイルのダウンロード時の注意、怪しいファイルの見分け方
  - ・パスワード設定、管理

Copyright © 2013 独立行政法人　情報処理推進機構

コンピュータウイルス

Copyright © 2013 独立行政法人 情報処理推進機構

ウイルスとは

- コンピュータに対して、数々の悪さをする不正プログラム
  - 自己伝染機能
  - 潜伏機能
  - 発病機能

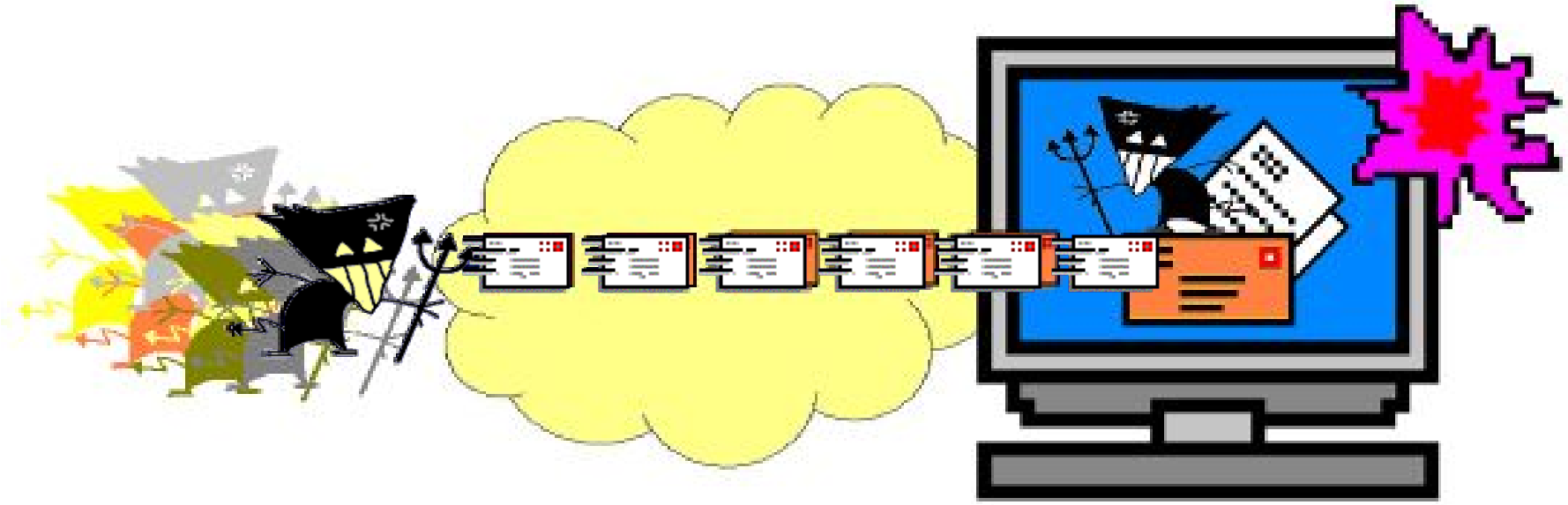
＊ 画像：（独）情報処理推進機構（IPA）

☆ 最近では、広い意味で、スパイウェアやボットなどもウイルスと呼んでいます。

Copyright © 2013 独立行政法人 情報処理推進機構

メールから感染

Information-technology Promotion Agency, Japan



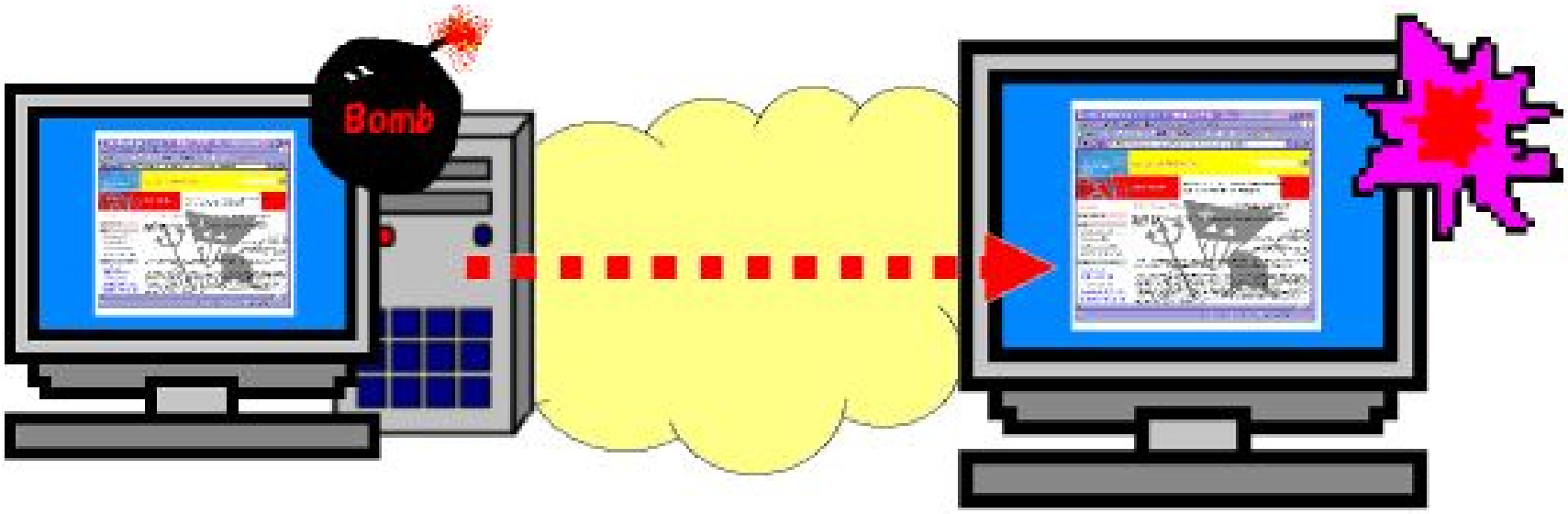
＊ 画像：（独）情報処理推進機構（IPA）

- ウイルスメールの開封やプレビューにより**添付ファイルが自動的に実行**して感染
- ファイルの拡張子やファイルのアイコン等の偽装をして添付ファイルを開かせることにより感染

Copyright © 2013 独立行政法人　情報処理推進機構

Webサイトの閲覧から感染

Information-technology Promotion Agency, Japan



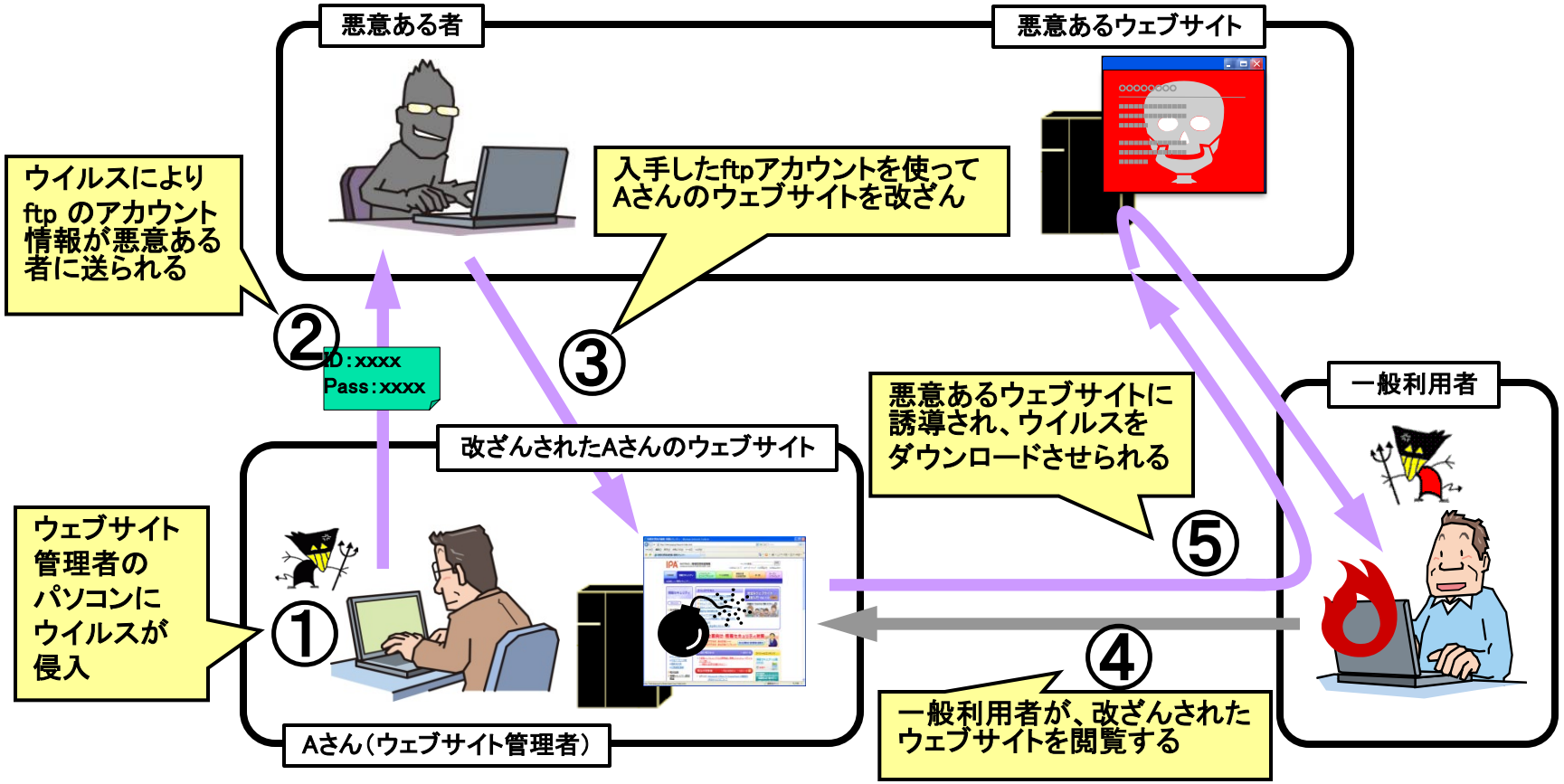
＊ 画像：(独)情報処理推進機構(IPA)

- ウイルスが仕掛けられたWebサイトの閲覧による感染
- ウイルスメールを見ただけで強制的にウイルスが仕掛けられたWebサイトにアクセスさせられて感染

Copyright © 2013 独立行政法人 情報処理推進機構

ウイルス感染の新たな手口(ガンブラー)

Information-technology Promotion Agency, Japan



・悪意ある者が、FTPアクセスにより、改ざんウェブページをアップロード
・悪意あるウェブサイトには、Adobe製品の脆弱性を突くウイルスが・・

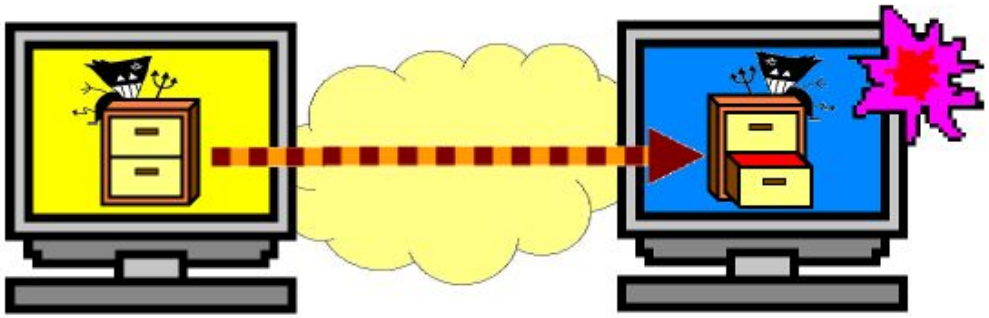
＊ 画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ファイルのやり取りによる感染

Information-technology Promotion Agency, Japan

・Webサイトなどからダウンロードしたフリーソフト(無償プログラム)やシェアウェア(有償プログラム)にウイルスが仕掛けられており、そのプログラムファイルをインストールすることにより感染
・ファイル交換(P2P※)ソフト、IM※(インスタントメッセンジャ) サービス等により入手したファイルによる感染



＊ 画像：(独)情報処理推進機構(IPA)

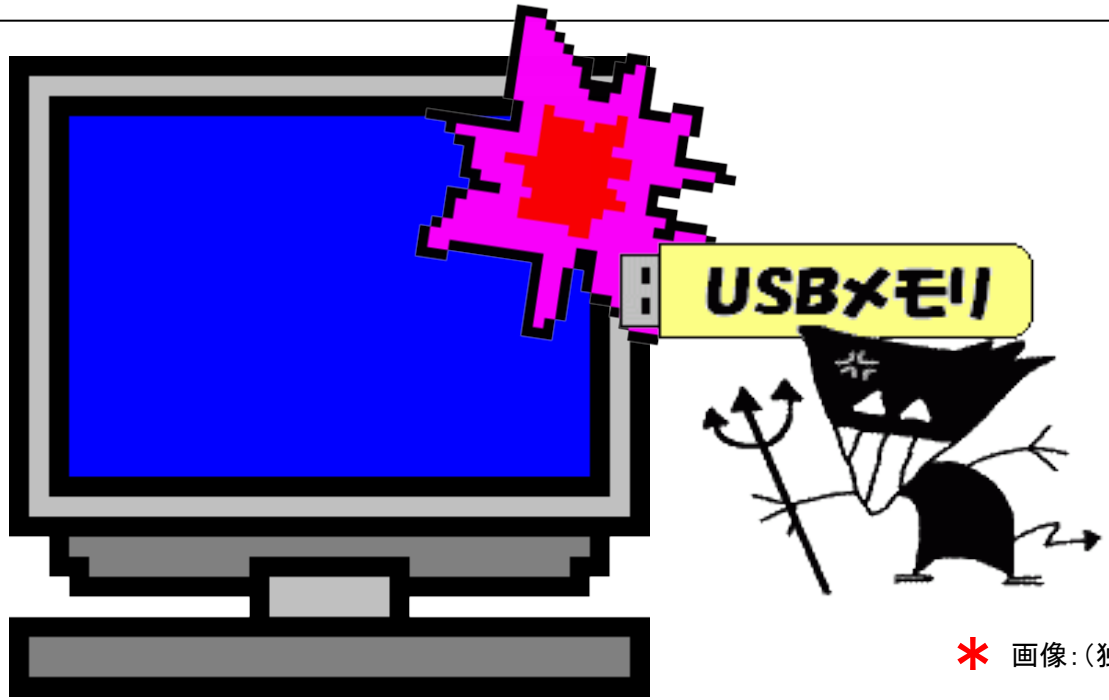
代表的ウイルス：Antinny、Exponny　等

・コンピュータがネットワークに接続されていなくても、CDやUSBメモリなどの電子媒体からファイルをやり取りすることにより感染

Copyright © 2013 独立行政法人　情報処理推進機構

電子媒体からの感染

- 外部接続の電子媒体をパソコンに接続すると媒体に格納されたウイルスが自動的に実行される問題が発生しています

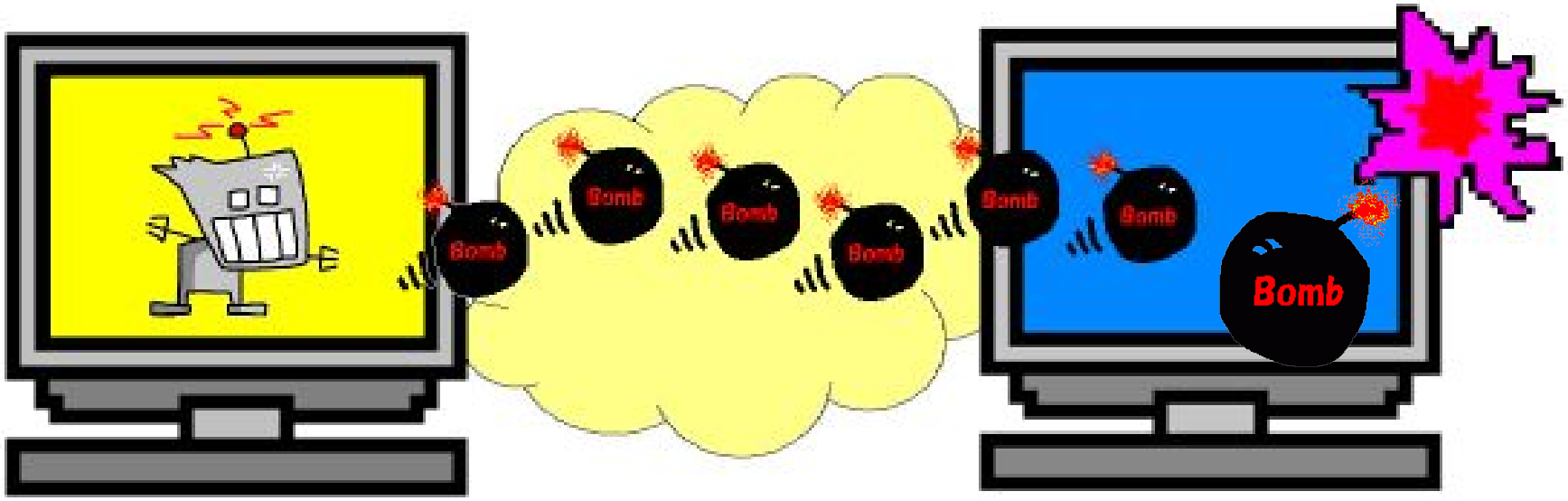


＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ネットワークに繋いでの感染

Information-technology Promotion Agency, Japan



＊ 画像：（独）情報処理推進機構（IPA）

- **悪意のある利用者**や**サイト**から、ネットワークを介してコンピュータの**ぜい弱性（セキュリテホール）**をついた侵入によるウイルス感染

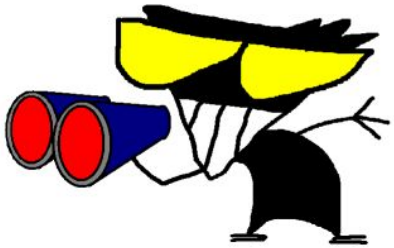
Copyright © 2013 独立行政法人　情報処理推進機構

愉快犯から実害を与える脅威へ

Copyright © 2013 独立行政法人 情報処理推進機構

スパイウェアとは

- 利用者や管理者の意図に反してインストールされ、利用者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等。



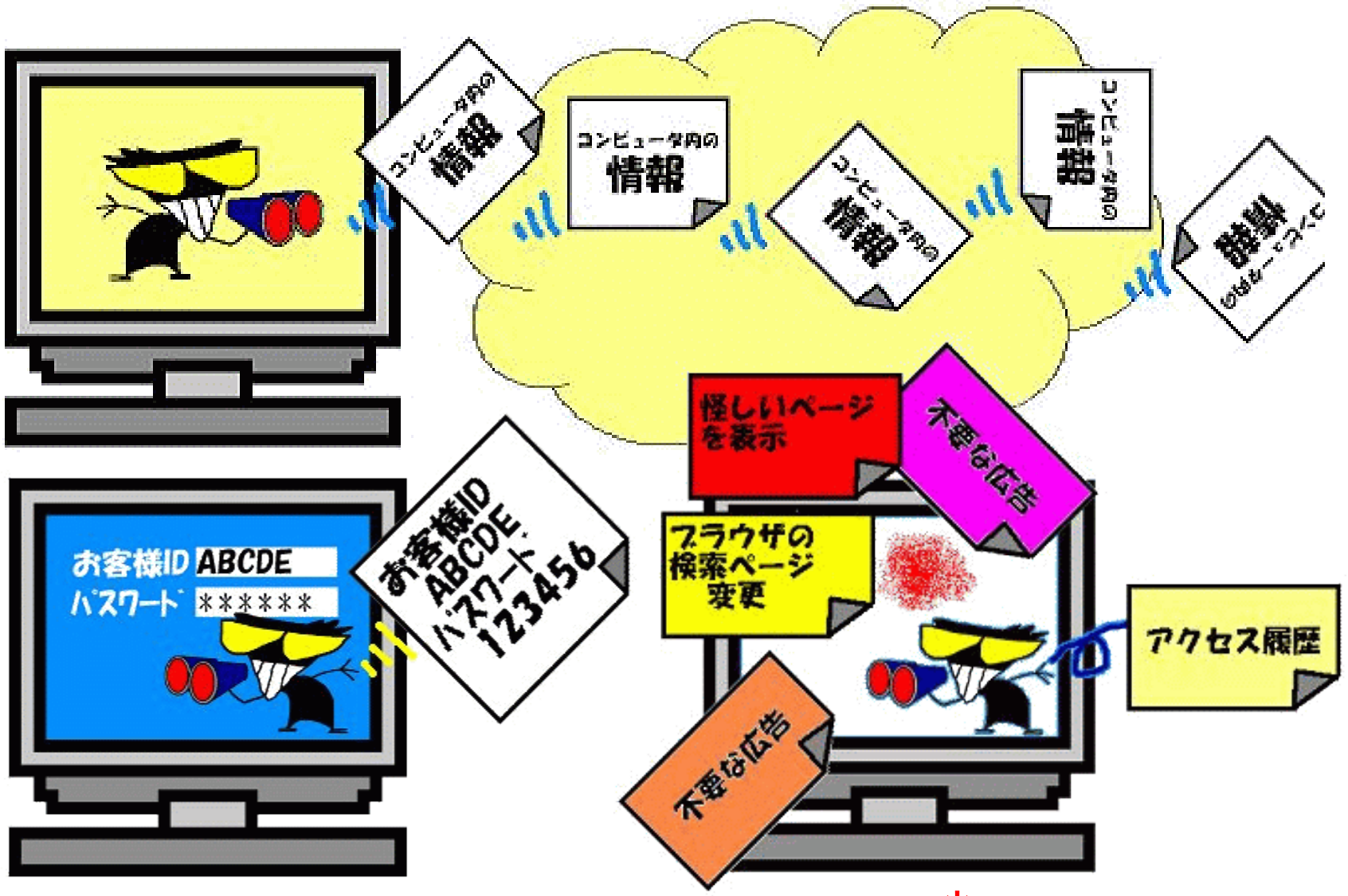
スパイウェアは、収集した情報をファイルに保存したり、外部へ自動的に送信したりするなどの機能を併せ持つものが多く見られます。

＊画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

スパイウェアのイメージ

Information-technology Promotion Agency, Japan



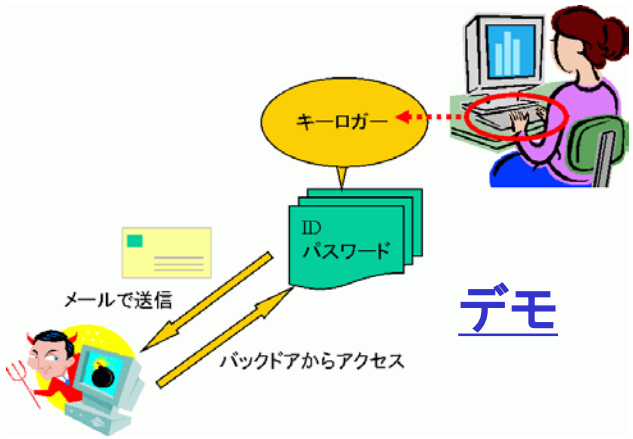
＊ 画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

スパイウェアの代表例「キーロガー」

Information-technology Promotion Agency, Japan

- WindowsなどのOSに入り込み、キー入力やマウス操作などを監視
  - 表向きは起動しているように見えない。
  - タスクマネージャのプロセス画面には表示される場合がある(表示されないものもある)。
  - レジストリ※を書き換えて、起動時に自動的に実行される。
- 盗聴した情報はファイルに保存
  - しばらくの間、情報を収集した後にファイルを回収
- あるいはネットワーク経由で送信
  - 悪意ある人がリモートで収集



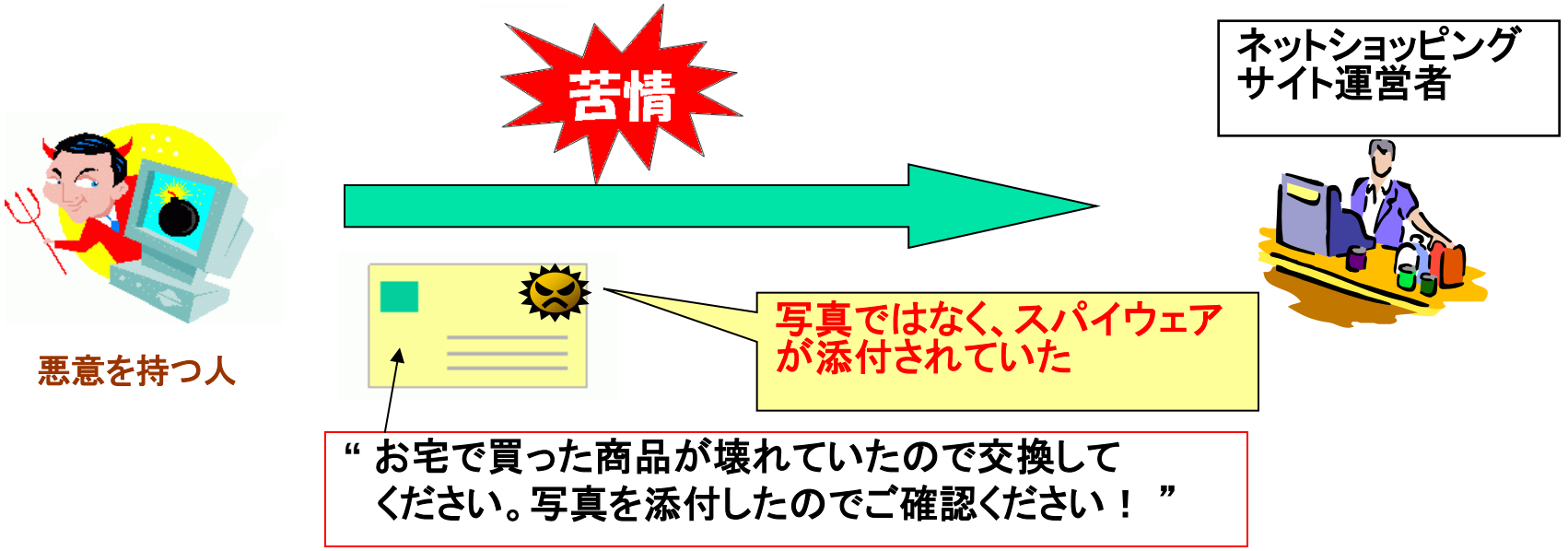
デモ

＊ 画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

キーロガーによるID/パスワード盗難(事例)
ネット銀行での不正送金被害

ネット銀行の不正引き出し、スパイウエアが原因
オンラインショップの経営者へ商品の返品交換を要求する苦情メールが届いた。メールに添付されていた商品の写真を開いたが、写真は存在しなかった。→　添付ファイルをクリックした際、本人が気づかないうちに、キーロガーと呼ばれるスパイウエアがインストールされた。 このキーロガーは、ネット銀行などへのアクセスを監視し、口座番号や暗証番号を犯人に送信。犯人は、盗んだ情報を悪用して不正に引き出した。



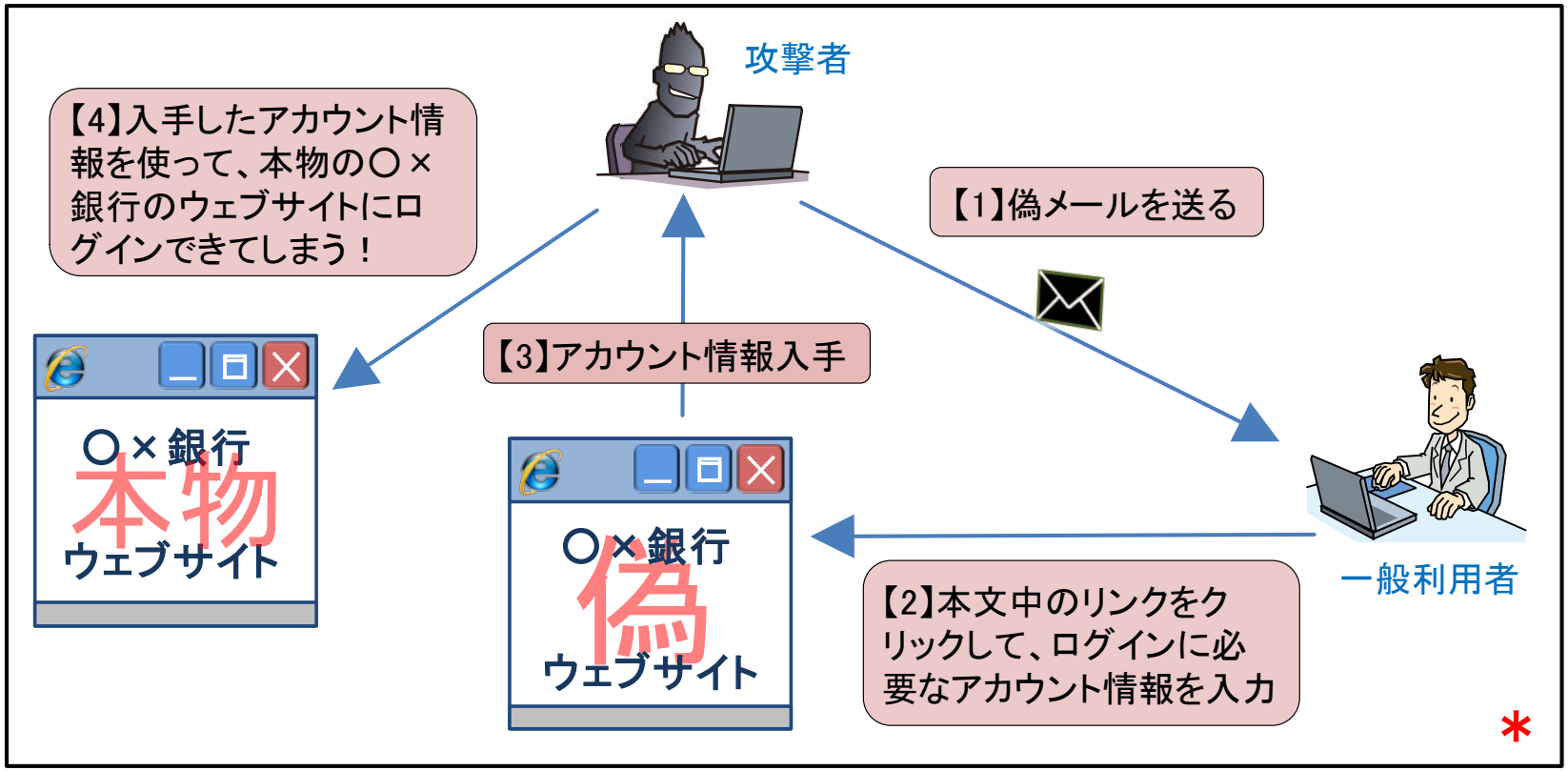
Copyright © 2013 独立行政法人　情報処理推進機構

＊ 画像:(独)情報処理推進機構(IPA)

フィッシング(Phishing)とは

Information-technology Promotion Agency, Japan

金融機関(銀行やクレジットカード会社)などを装ったメールを送り、電子メールの受信者に偽のウェブサイトにアクセスするよう仕向け、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



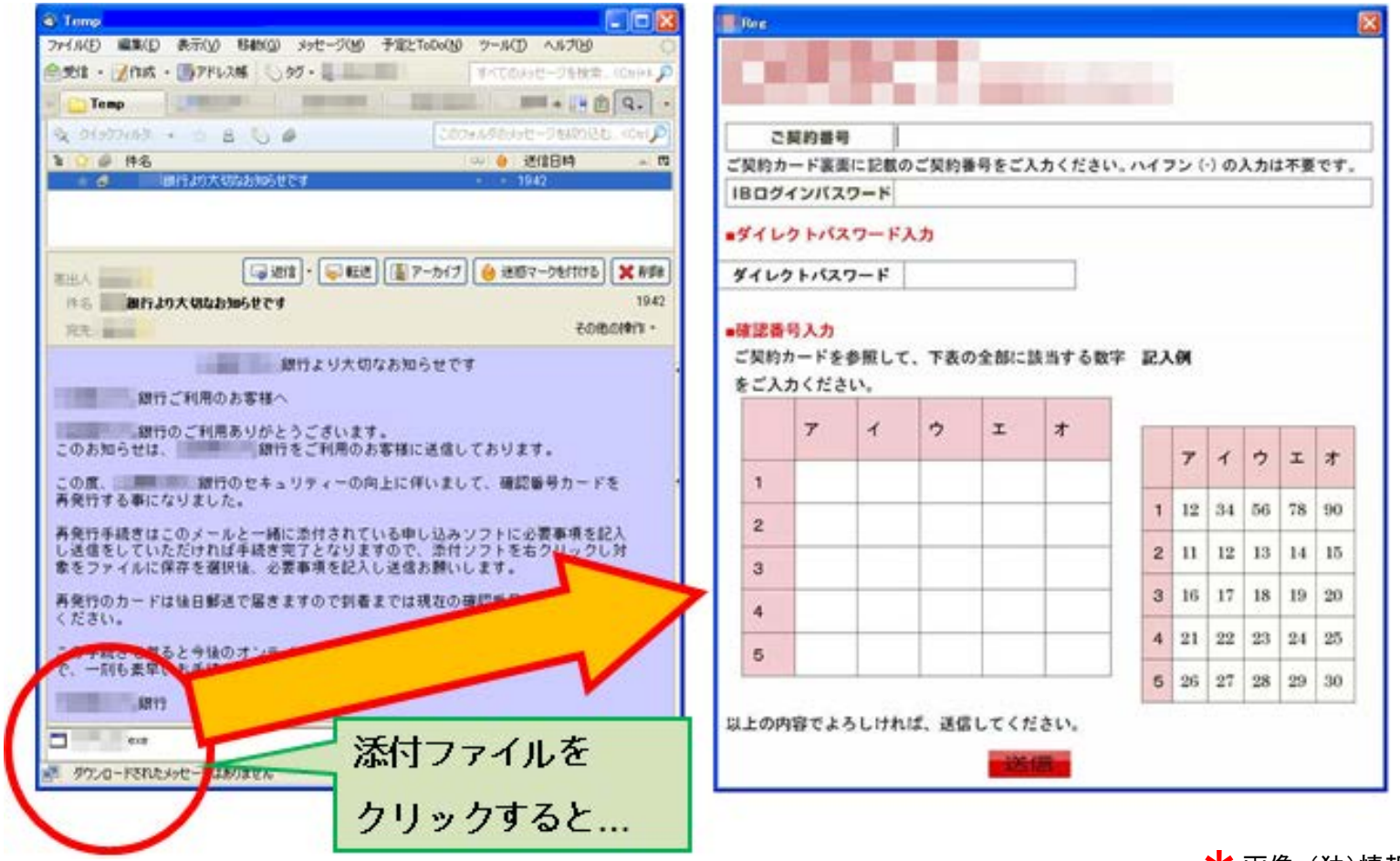
画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

銀行の第二認証情報（乱数表の番号）を詐取するフィッシング

Information-technology Promotion Agency, Japan

送信プログラム添付型の例



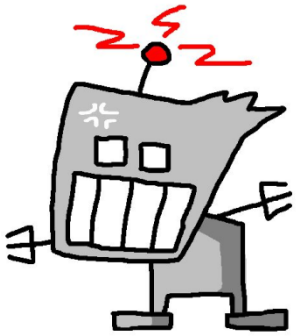
＊ 画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人 情報処理推進機構

ボットとは

- コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータをネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラム。

  たくさんのボット感染コンピュータが集まると・・・

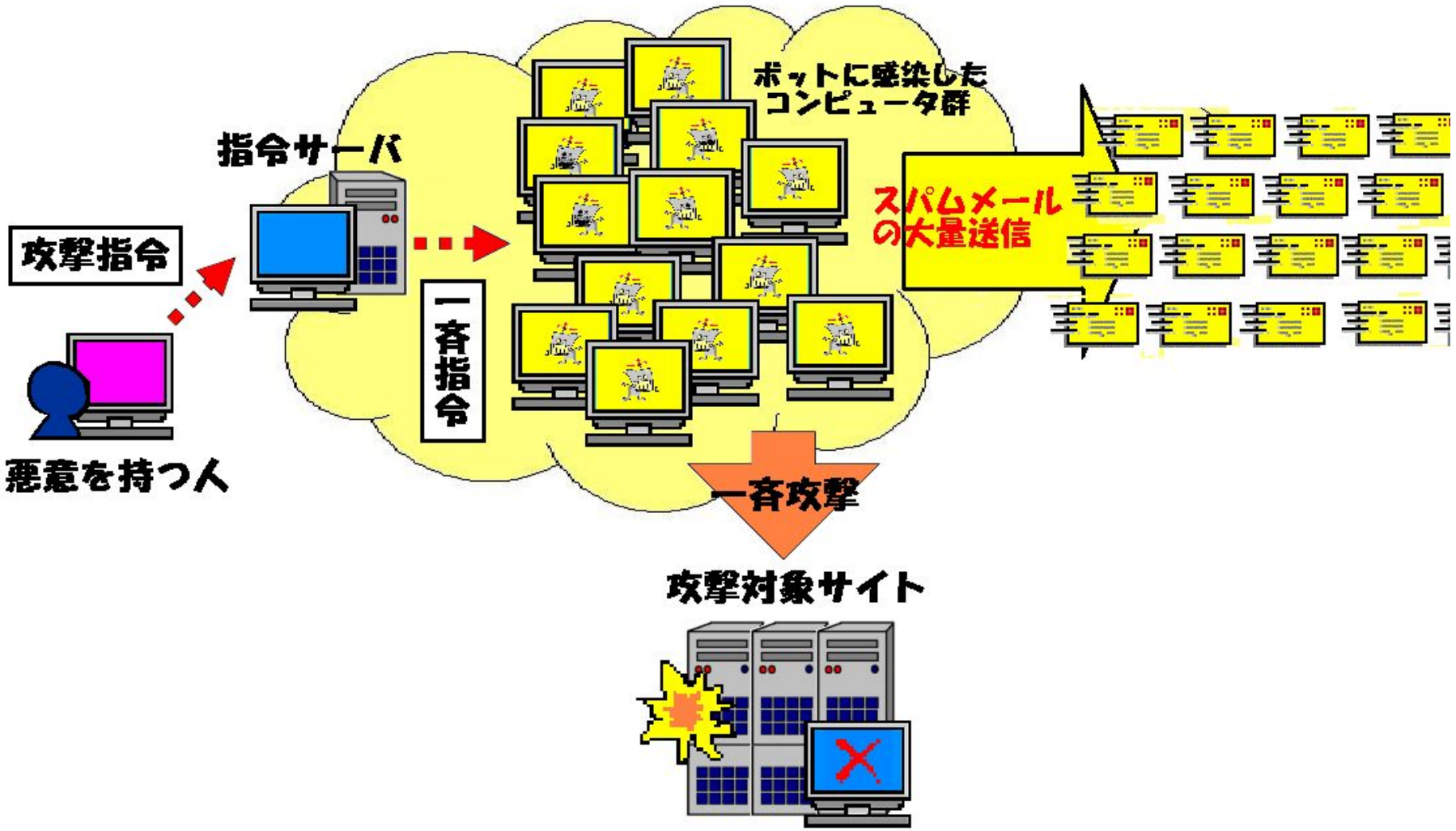


＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ボットネットワークの脅威

Information-technology Promotion Agency, Japan

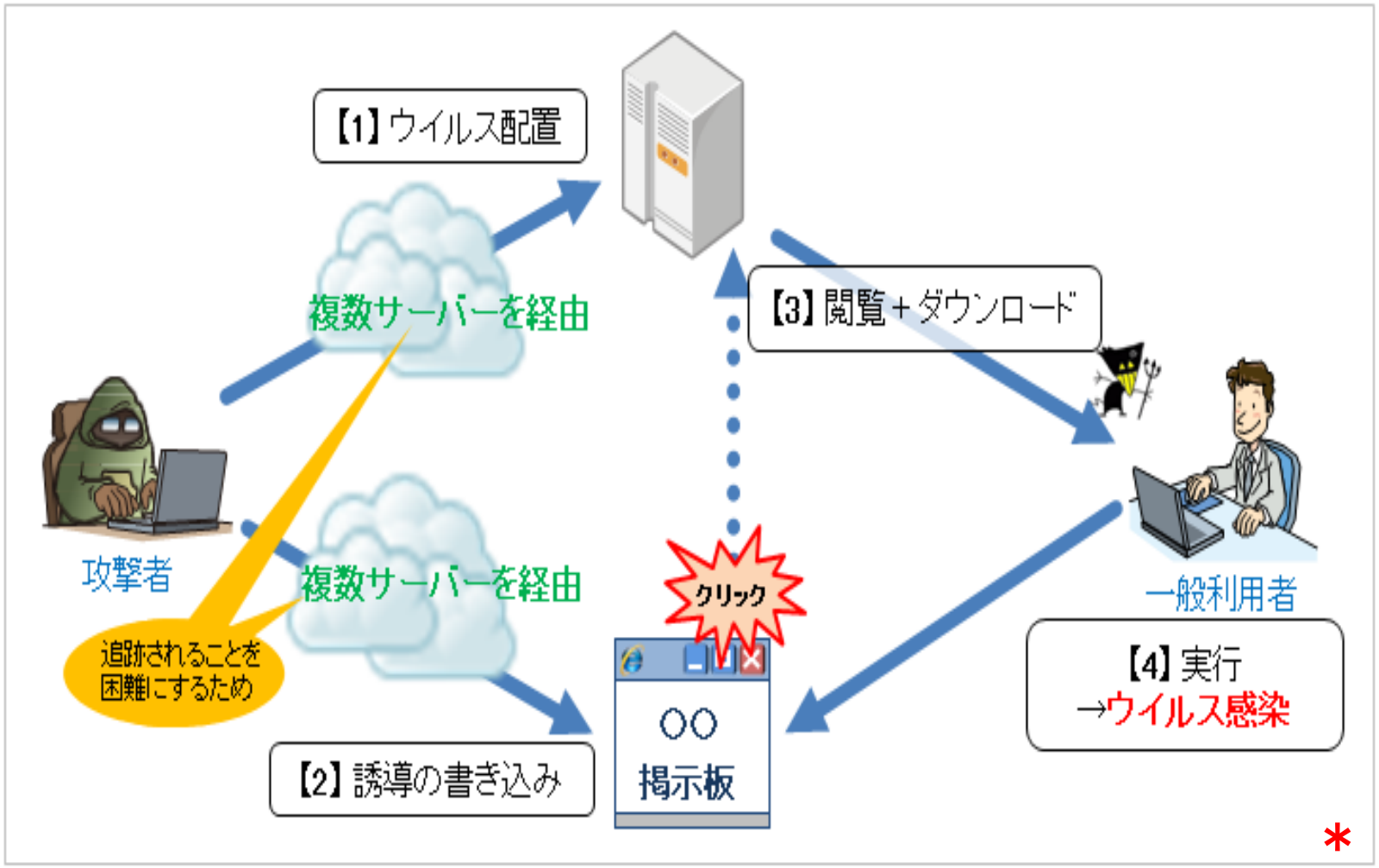


＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

遠隔操作ウイルス［感染］

Information-technology Promotion Agency, Japan

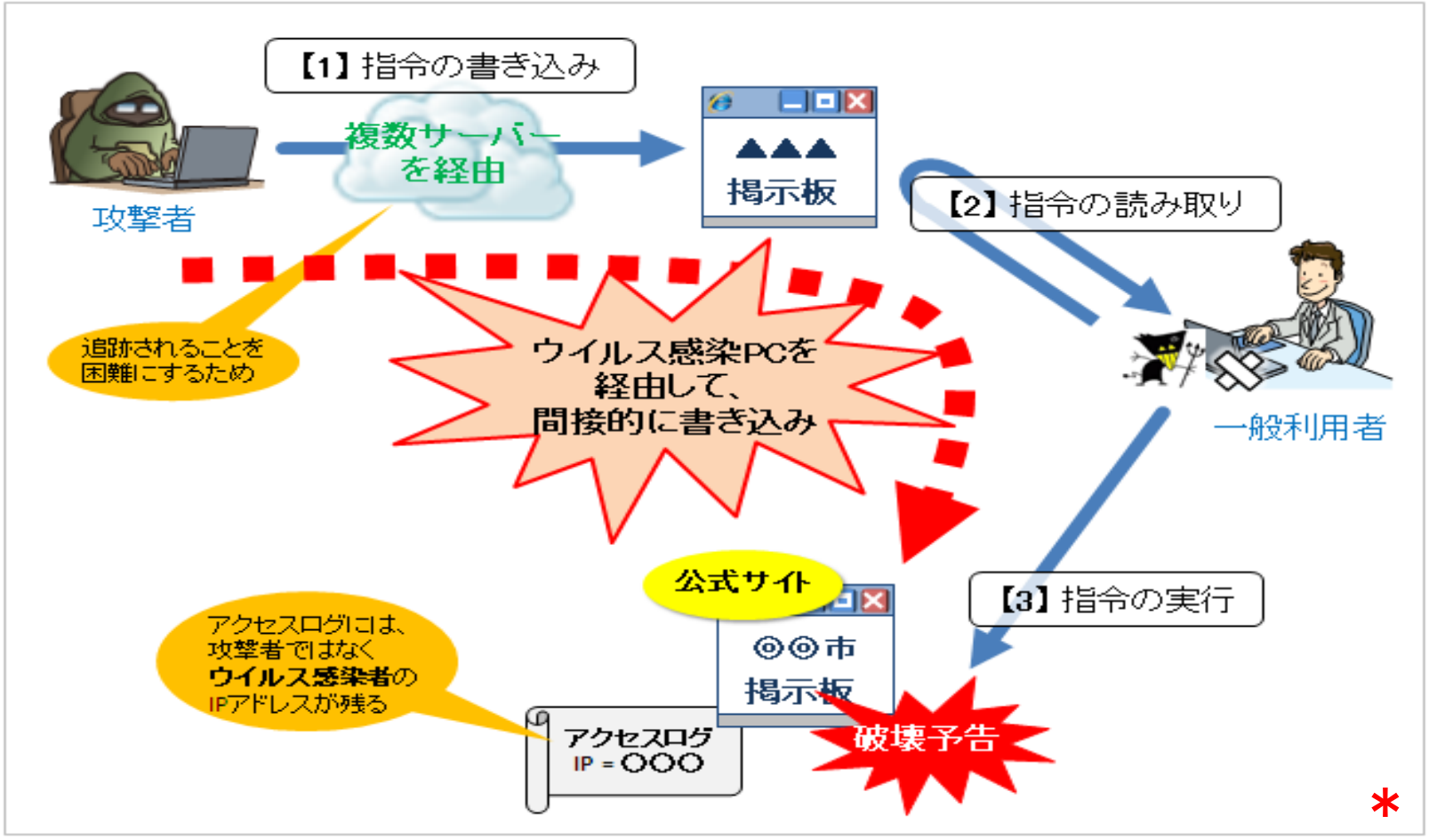


画像：（独）情報処理推進機構（IPA）

遠隔操作ウイルスに感染するまでのイメージ図

Copyright © 2013 独立行政法人　情報処理推進機構

遠隔操作ウイルス［遠隔操作］



画像：(独)情報処理推進機構(IPA)

攻撃者が遠隔操作を行うイメージ図

Copyright © 2013 独立行政法人　情報処理推進機構

ワンクリック請求・誘導事例

Information-technology Promotion Agency, Japan

＊ 画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人 情報処理推進機構

ワンクリック請求・誘導事例つづき-1

Information-technology Promotion Agency, Japan

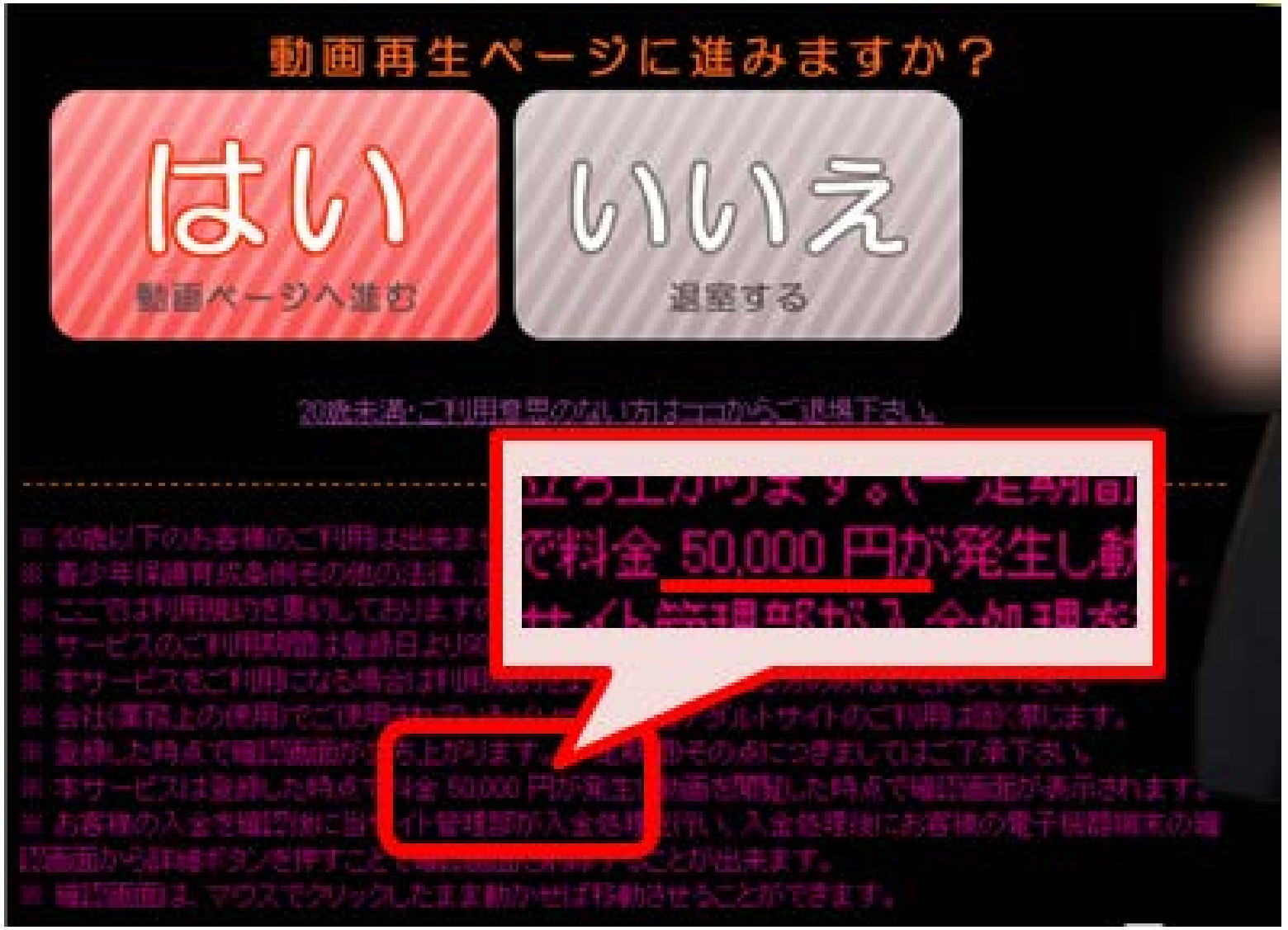
*

画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人　情報処理推進機構

ワンクリック請求・誘導事例つづき-2

Information-technology Promotion Agency, Japan



*

画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ワンクリック請求・誘導事例つづき-3

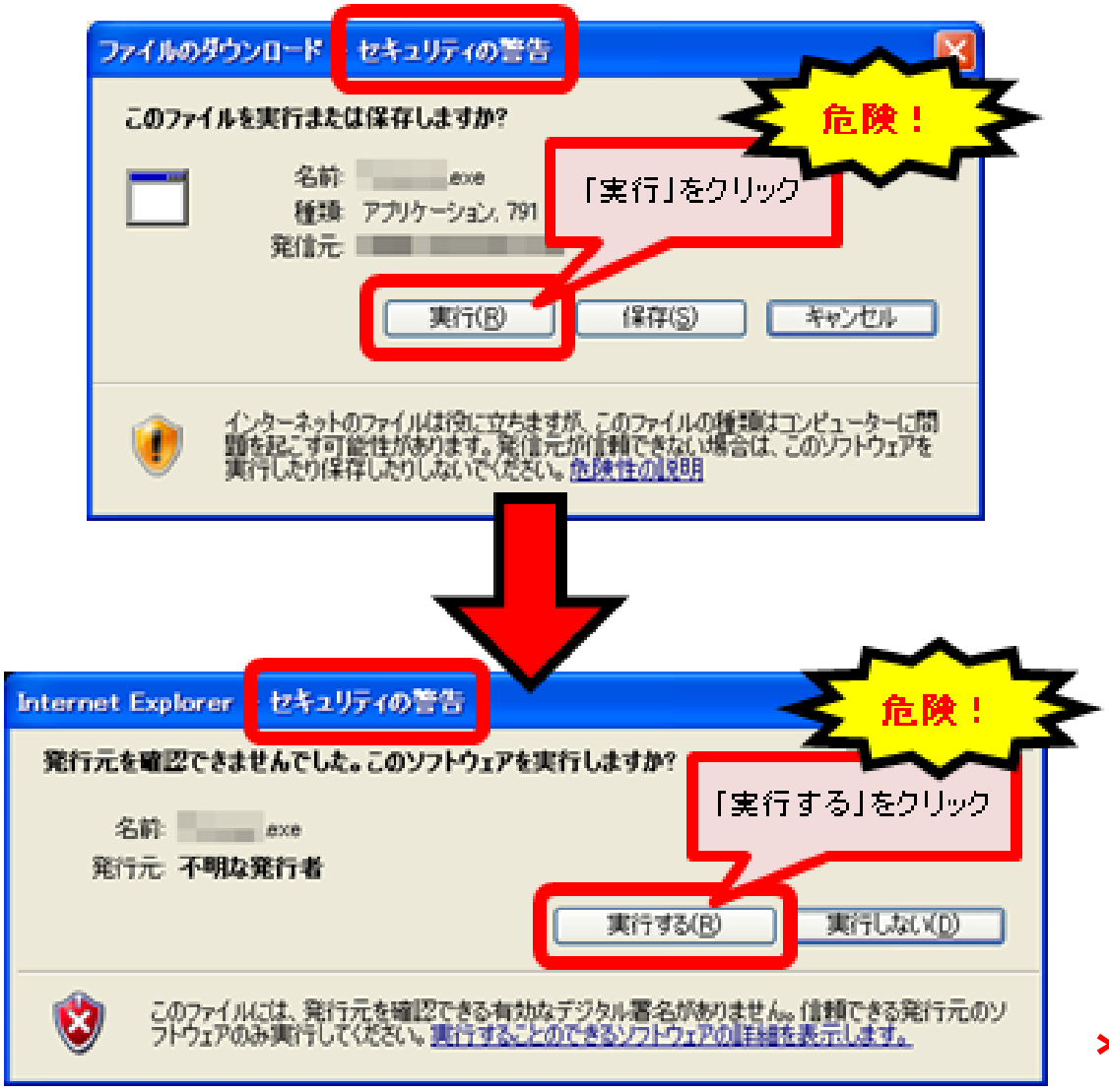
Information-technology Promotion Agency, Japan

＊ 画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ワンクリック請求・誘導事例つづき-4

Information-technology Promotion Agency, Japan

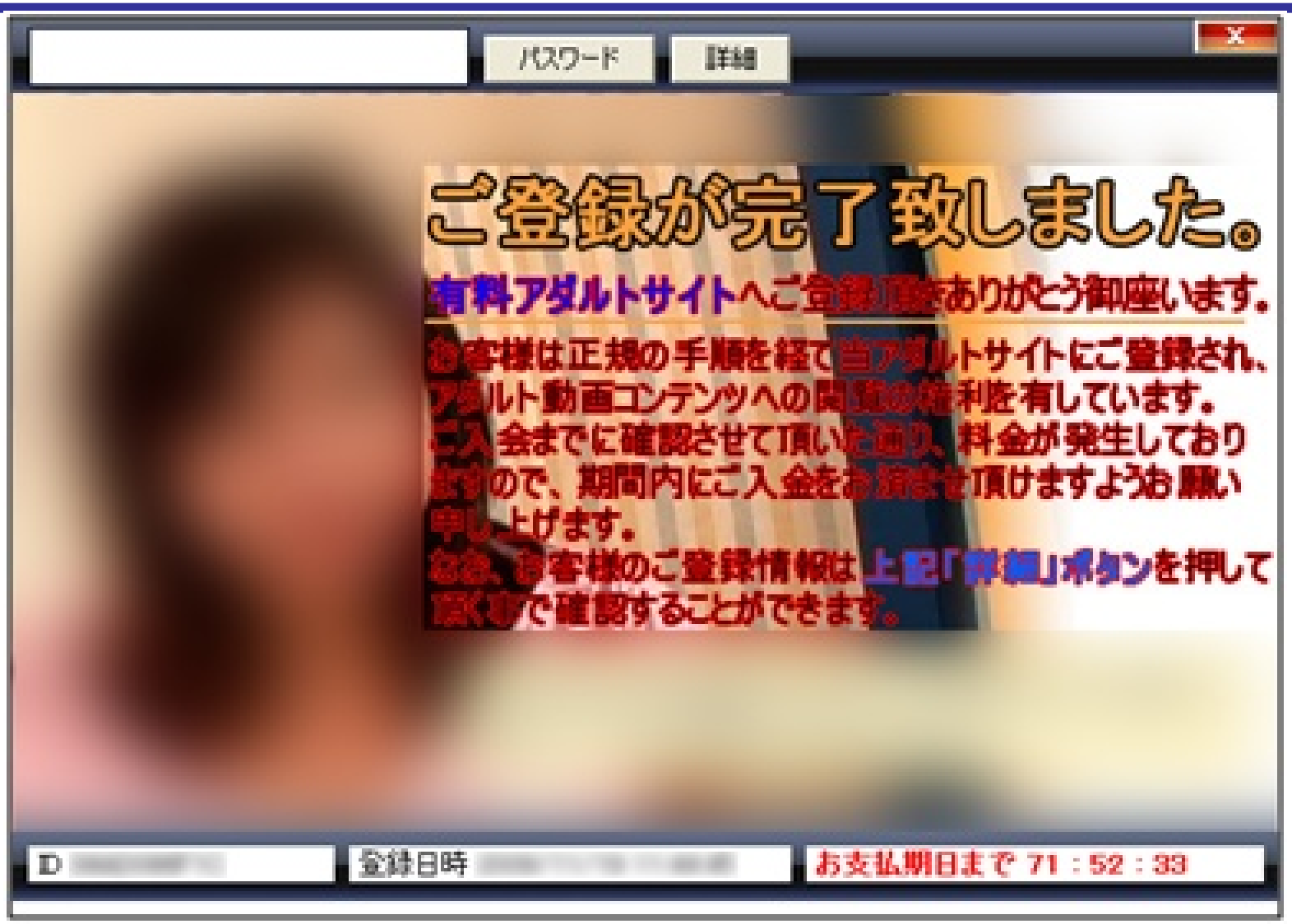


＊ 画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ワンクリック請求・誘導事例つづき–終

Information-technology Promotion Agency, Japan



*

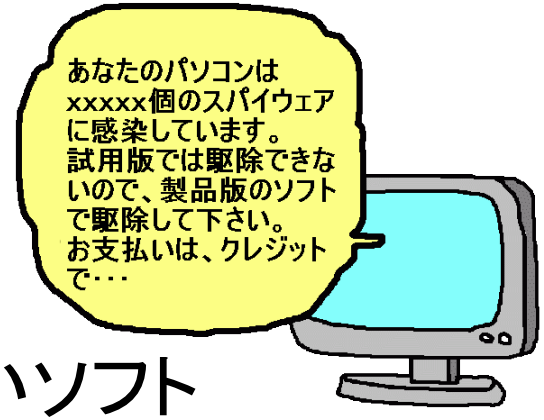
画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

偽セキュリティ対策ソフト

- 『あなたのパソコンはウイルスに感染している』と脅して、偽ウイルス対策ソフトを押し売りする
- スパムメールやIM経由、Windows Messenger経由で勧誘している
- **WinFixer,WinAntiVirusPRO**

  などが、IPAへの問い合わせが多いソフト
- 『安全なブラウザ』と称して、偽ブラウザを強制的にインストールし、アドウェアやスパイウェアをばら撒くサイトに誘導するものも出てきている



*

画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

スマートフォンの情報流出

画像:(独)情報処理推進機構(IPA)

不正なアプリが情報を流出させるイメージ図

Copyright © 2013 独立行政法人 情報処理推進機構

スマートフォンの不正なアプリ例

項番	特徴	アプリ配布場所における名称	インストール後の名称
1	有名なアプリ、ほかのスマートフォンOSで人気のアプリ名を含む	ウォーリーを探せ the Movie	ユーチューブ動画
		うまい棒をつくろう！ the Movie	youtube動画まとめ
		ギャングハウンド the Movie	グラビア動画
		スヌーピーストリート the Movie	笑える動画
		チャリ走-the Movie	ようつべ動画まとめ
		ぴよ盛り the Movie	面白動画まとめ
		メガ盛ポテト the Movie	芸能動画
		空手チョップ! The Movie	ニコニコ動画まとめ
		大盛モモ太郎 the Movie	youtube動画
		桃太郎電鉄the Movie	ようつべ動画
		魔界村騎士列伝 THE MOVIE	暇つぶし動画
		連打の達人 the Movie	ユーチューブ動画まとめ
2	個人的嗜好をくすぐる文字列を含む	FC2動画まとめ the Movie	怖い動画
		けいおん-K-ON!動画	アニメ動画
		スク水動画まとめ	美人動画
3	実用性を感じさせる文字列を含む	3D視力回復 THE MOVIE	泣ける動画

Copyright © 2013 独立行政法人　情報処理推進機構

不正なアプリが必要とする権限の例

	権限（パーミッション）名	許可した場合にどうなるか（抜粋）
1	電話発信	アプリが端末に付与されている電話番号や、端末識別番号、SIM情報などを読み取ることができます。 電話の着信状態などの情報も読み取ることができます。
2	個人情報	アプリがアドレス帳など連絡先データを読み取ることができます。
3	ネットワーク通信	アプリがインターネットなどにある外部のサーバーと自由に通信できます。

Copyright © 2013 独立行政法人　情報処理推進機構

不正なアプリの動作例

android_id（端末の識別子）と端末の電話番号を特定のサーバーへ送信する。
この送信成功後、アドレス帳に登録された名前、電話番号、Eメールアドレスを全て送信する。
さらにこれらの送信が成功後、特定のサーバーから動画を取得、再生する。

*
画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

その他の不正なアプリ例

	不正なアプリの種類	主な特徴
1	ワンクリック請求アプリ ※1	電話番号などの端末情報を外部に送信する。
2	ボット型ウイルス ※2	外部からの操作指令を受けてアドレス帳データやSMSの送信をしたり、地図やWebページを表示したりする。
3	不正発信アプリ	勝手に電話を発信する。（特定の国でのみ動作し、日本では動かない。）

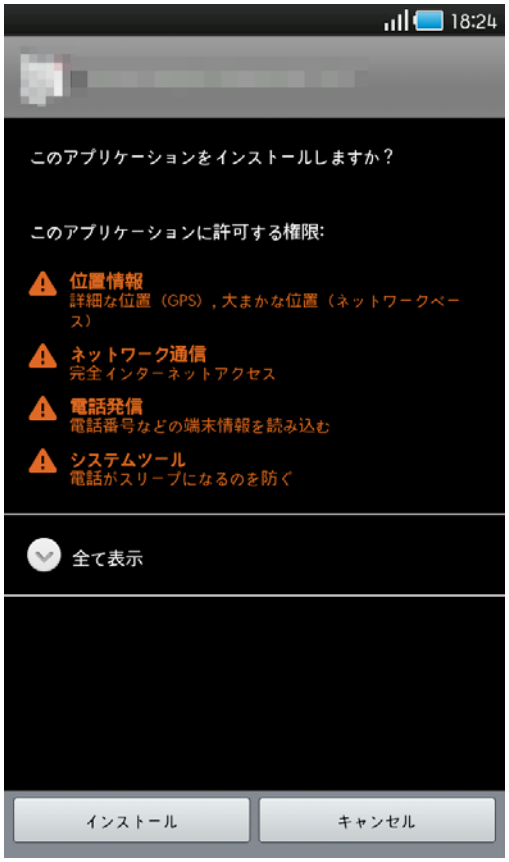
（※1 ）「 スマートフォンでもワンクリック請求に注意！ 」
http://www.ipa.go.jp/security/txt/2012/02outline.html

（※2 ）Android OSを標的としたウイルスに関する注意喚起
http://www.ipa.go.jp/security/topics/alert20110121.html

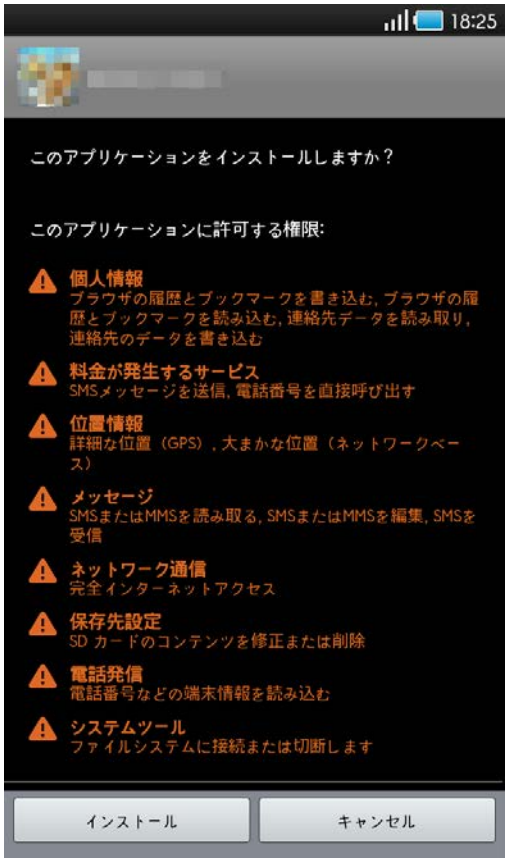
Copyright © 2013 独立行政法人 情報処理推進機構

その他の不正なアプリ例

Information-technology Promotion Agency, Japan



ワンクリック請求アプリ例



ボット型ウイルス例

不正発信アプリ例

*

画像:（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

不正アクセス

Copyright © 2013 独立行政法人 情報処理推進機構

不正アクセスとは

「コンピュータ不正アクセス対策基準」

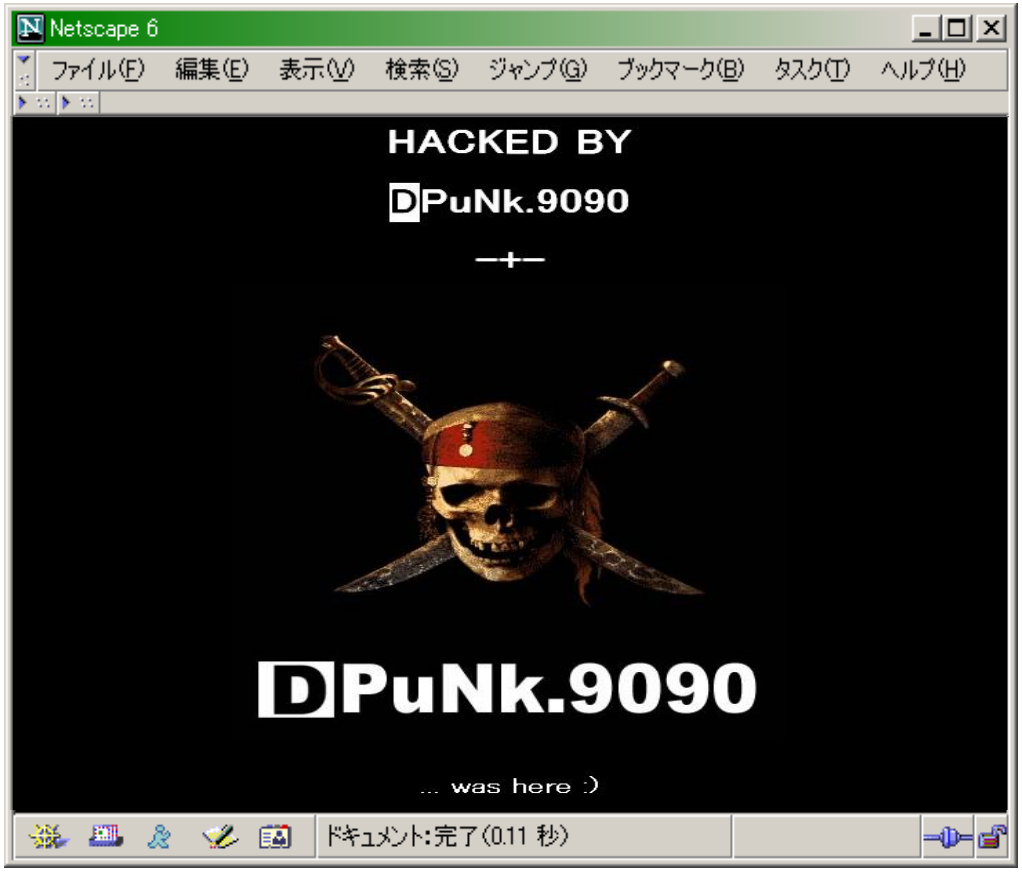
システムを利用するものが、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。　（旧通商産業省告示）

- 本人以外の人間が利用
  - **他人のIDの利用**
  - **アクセス制限が前提（管理者の責任）**
- 許可されていない資源へのアクセス
  - **資源→コンピュータや情報**

Copyright © 2013 独立行政法人　情報処理推進機構

不正アクセス被害事例－1

- 組織の内部機密情報が盗まれた
- Webページが改ざんされた



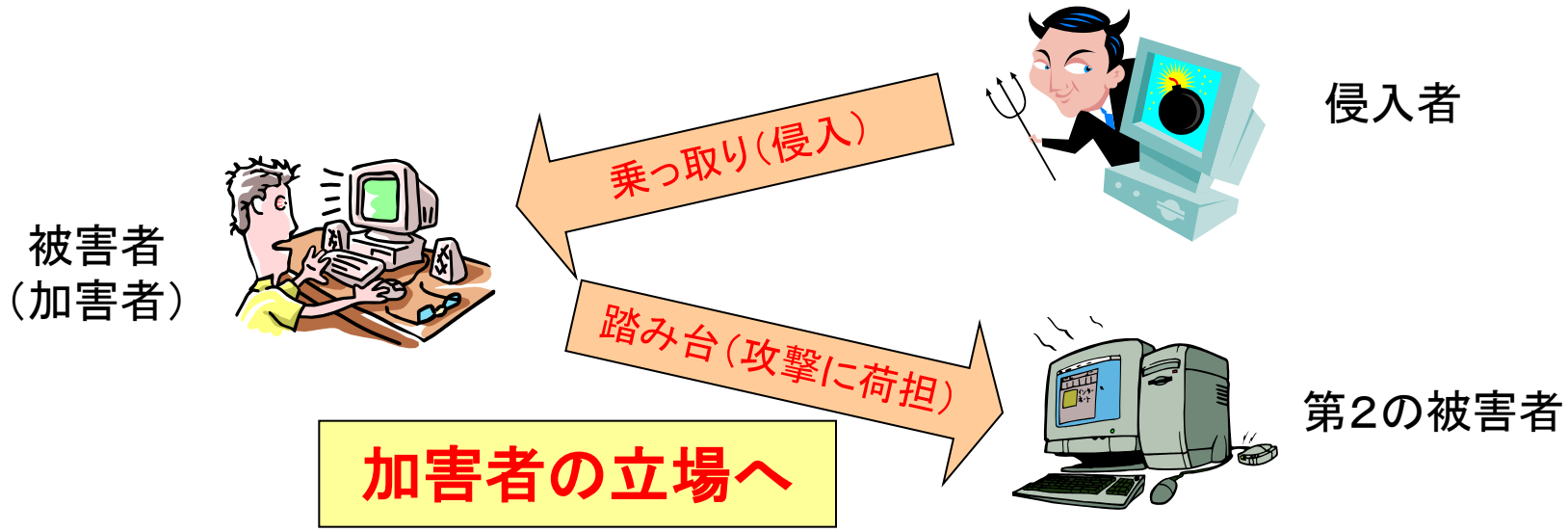
＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

不正アクセス被害事例－２

●不正プログラムの埋め込み(トロイの木馬など)

- パソコンの操作をしていないのに目の前でファイルが消えたり、ウインドウが開いたりする。
- 知らないうちにパソコンに侵入され、後日高額な国際電話料金を請求される。
- パソコンが乗っ取られて他人への攻撃に利用される。



＊ 画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人 情報処理推進機構

不正アクセス被害事例－３

●パスワード盗用

知らないうちにパスワードが盗まれる。
その結果

- オンラインショッピングで買い物をされる
- インターネットで銀行口座を操作される

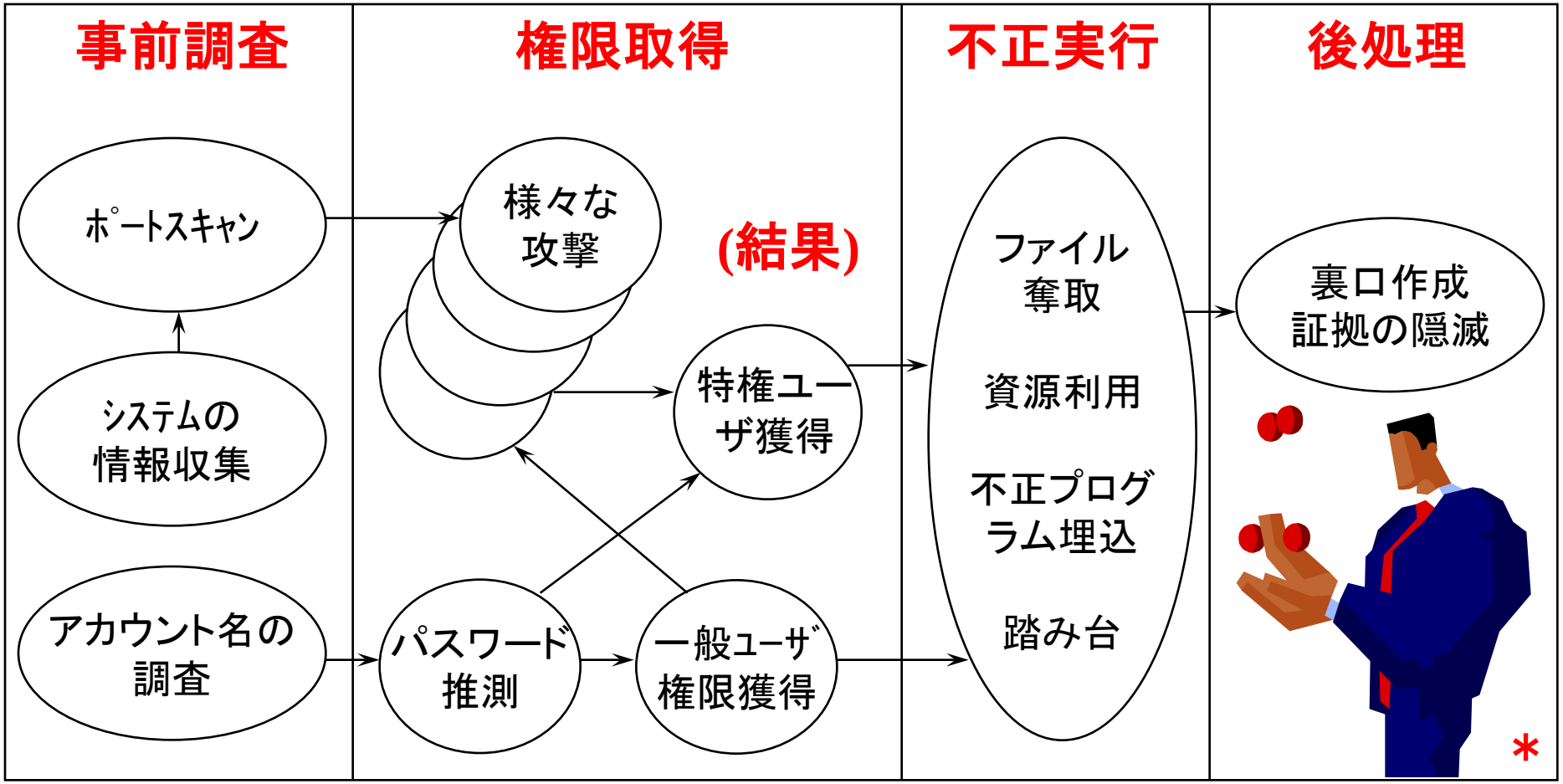
等の被害につながる。

＊ 画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

侵入行為

一般的な侵入行為の流れ



画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

セキュリティ対策

Copyright © 2013 独立行政法人 情報処理推進機構

感染防止対策

パソコンユーザのためのウイルス対策7箇条

1. 最新のウイルス定義ファイルに更新しワクチンソフトを活用すること

2. メールの添付ファイルは、開く前にウイルス検査を行うこと

3. ダウンロードしたファイルは、使用する前にウイルス検査を行うこと

4. アプリケーションのセキュリティ機能を活用すること

5. セキュリティパッチをあてること
（※ここまでが感染予防）

6. ウイルス感染の兆候を見逃さないこと
7. ウイルス感染被害からの復旧のためデータのバックアップを行うこと

Copyright © 2013 独立行政法人 情報処理推進機構

感染防止対策

**メールの添付ファイルは、
開く前にウイルス検査を行うこと**

メールの添付ファイルの取り扱い5つの心得

1. 見知らぬ相手先から届いた添付ファイル付きのメールは厳重注意する
2. 添付ファイルの見た目に惑わされない
3. 知り合いから届いたどことなく変な添付ファイル付きのメールは疑ってかかる
4. メールの本文でまかなえるようなものをテキスト形式等のファイルで添付しない
5. 各メーラー特有の添付ファイルの取り扱いに注意する

・妙なファイルは絶対開かない（触らない）

・相手先に問い合わせを行う（確認がとれない場合は削除）

Copyright © 2013 独立行政法人 情報処理推進機構

感染防止対策

セキュリティホールの解消

●セキュリティホールは命取り

・ブラウザ、メーラーのセキュリティホールは致命的な被害に遭うことがある
　メール本文を開いただけで感染
　Webサイトを見ただけで感染

・セキュリティホールは必ず埋める
　・修正プログラム（セキュリティパッチ）を適用する
　・最新のバージョンにアップデートする

Copyright © 2013 独立行政法人　情報処理推進機構

スパイウェアについて(対策)

パソコンユーザのためのスパイウェア対策 5箇条

- 1.スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新およびスパイウェア検査を行う
- 2.コンピュータを常に最新の状態にしておく
- 3.怪しいサイトや不審なメールに注意
- 4.コンピュータのセキュリティを強化する
- 5.万が一のために、必要なファイルのバックアップを取る

- 補足.自分で管理できないコンピュータでは、重要な個人情報の入力を行わない

Copyright © 2013 独立行政法人 情報処理推進機構

フィッシング対策

- メールの真偽の確認

金融機関等から来たと思われるメールでも、内容を慎重に確認してください。そもそも**カード番号や暗証番号を入力するような依頼がメールで届くことはありません**。もしそのようなメールが金融機関等から届いた場合は、送信元に電話で問い合わせたり、ウェブサイトのお知らせ欄を見たりして、その情報（メール）の真偽を確認してください。

電話で問い合わせをする時は、メール本文に記載されている連絡先ではなく、口座開設時に送付された書類を見る等、正しいと確証が持てる連絡先に電話してください。

- メール記載のリンクに注意

メール本文内にあるリンク先に不用意にアクセスしないことも重要です。当該銀行等のウェブサイトを確認する場合は、メール中のリンクからアクセスするのではなく、ブラウザの「お気に入り」や「ブックマーク」に正しいアドレスを登録しておき、常にそちらからアクセスすることをお勧めします。

Copyright © 2013 独立行政法人 情報処理推進機構

遠隔操作ウイルス ［対策］

基本的な心掛け

1　出所の不明なファイルをダウンロードしたり、ファイルを開いたりしない

2　安易にURLリンクをクリックしない

基本的対策

1　使用しているパソコンのOSやアプリケーションなどの脆弱性を解消する

2　ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保ちながら使用する

追加の対策

パーソナルファイアウォールを適切に設定して使用する

参考：証拠を保全する試み

万が一遠隔操作ウイルスに感染して、外部への攻撃に利用されてしまった場合、パソコンの利用者が嫌疑をかけられることへの対抗策として、パソコン上のプログラムの動作記録や通信記録を残しておくことで、それが証拠となることが考えられます。

Windows OSに標準に備わっている「Windowsファイアウォール」や、セキュリティ対策ソフトのログ機能などを用いることである程度の記録を取得することができます。

Copyright © 2013 独立行政法人　情報処理推進機構

ワンクリック請求対策

- 慌てないで・・・
- お金を払ってはいけません。
- 基本は無視（個人を特定する情報流出の防止）
  - 問い合わせ（メールや電話）はしない
  - ひたすら無視
- スパイウェアや請求書表示プログラムは駆除
- 内部からの情報流出を防止

パーソナルファイアウォールの導入により、不正プログラムがPC内の情報を外部に送信することを防止できる。（設定例：インターネットに接続するアプリケーションを限定する）

Copyright © 2013 独立行政法人 情報処理推進機構

IPA スマートフォンのセキュリティ対策ービデオ

Information-technology Promotion Agency, Japan

あなたのスマートフォン、ウイルスが狙っている！
ースマートフォン・タブレット型端末のセキュリティ対策ー

＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

スマートフォンのセキュリティ対策

スマートフォンを安全に使用するための六箇条

1 スマートフォンをアップデートする。

スマートフォンの取扱説明書等にしたがい、スマートフォンに搭載されているOSをアップデートする。

2 スマートフォンにおけるソフトウェア的な改造行為を行わない。

iPhoneにおけるJailBreak（脱獄）やAndroid端末におけるroot奪取行為（root化手法）などといったソフトウェア的な改造行為を行わない。

3 信頼できる場所からアプリケーション（アプリ）をインストールする。

スマートフォンで使用するアプリは、信頼できる場所からインストールする。iPhoneでは「App Store」、Android端末ではアプリの審査や不正アプリの排除を実施している場所（「Android Market」など）を推奨します。

Copyright © 2013 独立行政法人　情報処理推進機構

アプリを最新の状態に保つ（六箇条 ①）

スマートフォンの場合は、基本的に販売元（キャリアまたはメーカー）主導でOSのバージョンアップやアップデートが行われます。

Android端末の場合は、機種毎に使用されるOSのバージョンが違っていたり、販売元毎に独自機能を組み込んだりしてある場合が多いので、一律にバージョンアップやアップデートが行われるわけではありません。

アプリの更新があった場合は最新の状態にしてください。アプリの自動更新を設定することで、自動的に最新の状態にすることも可能です。

近年、スマートフォンの利用者数は増加傾向にあり、利用者数に比例するようにスマートフォンに関する脆弱性も多数報告されています※5。脆弱性を解消したアプリをいち早く利用するようにしてください。

Copyright © 2013 独立行政法人 情報処理推進機構

スマートフォンにおけるソフトウェア的な改造行為を行わない。（六箇条 ②）

スマートフォンにおける改造行為はやめましょう。

ここでの改造行為とは、いわゆるiPhoneにおけるJailbreak（脱獄）やAndroid端末におけるroot権限奪取行為（root化とも呼ばれる）などのことを指します。

改造行為を行ったスマートフォンを狙って感染するウイルスなどもあり、ウイルス感染の危険性を自ら高めてしまうことになりますので、スマートフォンの改造行為はやめましょう。

Copyright © 2013 独立行政法人　情報処理推進機構

信頼できる場所からアプリをインストールする（六箇条③）

Android端末の設定画面に「提供元不明のアプリ」という項目があります。

この項目のチェックを外しておくと、正規のアプリ・ストア（Android Market）以外で入手したアプリケーションのインストールが阻止されます（初期状態ではチェックは外れた状態になっています）。

操作を誤るなどして不正なアプリケーションをインストールしてしまわないよう、普段はこの項目のチェックを外した状態にしておくことをお勧めします。

なお、信頼できる第三者のアプリ・ストアであっても、正規のAndroid Market以外で入手したアプリケーションをインストールする際は、一時的にこの設定を変更する（チェックを入れる）必要があります。どうしてもインストールする必要がある場合は、インストール終了後、再度チェックを外すことを忘れないでください。

「提供元不明のアプリ」の設定の確認・変更手順は、こちら　⇒次のスライドを参照してください。

Copyright © 2013 独立行政法人　情報処理推進機構

信頼できる場所からアプリをインストールする（六箇条③）

Information-technology Promotion Agency, Japan

①アプリケーション一覧画面で「設定」アイコンを選択します。
※アイコンの図柄は機種により異なります。

②設定の一覧の中の「アプリケーション」を選択します。

③「提供元不明のアプリ」の設定の状態を確認、変更できます。

「提供元不明のアプリ」のインストール許可設定画面

＊画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

スマートフォンのセキュリティ対策

スマートフォンを安全に使用するための六箇条

4 Android端末では、アプリをインストールする前にアクセス許可を確認する。

アプリをインストール時に表示される「アクセス許可(*)」の一覧には必ず目を通し、不自然な点や疑問に思う点（例えば、ゲームアプリなのに個人情報へのアクセスを求めているなど）があれば、インストールを中止してください。
(*):アプリがスマートフォンの中のどの情報／機能へアクセスするか定義したもの

5 セキュリティソフトを導入する。

ウイルス対策ソフトや、危険なウェブサイトへのアクセスをブロックするソフトなど、セキュリティソフトを導入する。

6 スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

企業でスマートフォンを活用する場合、スマートフォンの利用ルール、アクセス可能な情報の範囲、スマートフォンに保存してよい情報の範囲、紛失・盗難時の対策等のポリシーを定めてください。特に端末管理（MDM：Mobile Device Management）によって、スマートフォンに搭載されているOSのアップデートの徹底やインストールできるアプリの制限等で管理者が強制できる仕組みを設けることをお勧めします。

Copyright © 2013 独立行政法人　情報処理推進機構

アプリをインストールする際に必要とされる権限（パーミッション）を確認する（六箇条 ④）

アプリをインストールするときに表示される権限（パーミッション）をよく確認してください。

例えば、動画再生や画像表示アプリなのに、電話を発信する権限を求めてくる、カメラ機能が必要なさそうなアプリなのに、写真を撮る権限を求めてくるような場合は、怪しいアプリと言えます。

Copyright © 2013 独立行政法人　情報処理推進機構

アプリをインストールする際に必要とされる権限（パーミッション）を確認する（六箇条 ④）

Information-technology Promotion Agency, Japan

Android端末の場合、アプリをインストールする際に表示される「アクセス許可」（アプリがAndroid端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通してください。

インストールしようとしているアプリケーションが、スマートフォンの中のどの情報／機能へアクセスするかという一覧。
※画面デザインは機種や状況により異なります。

「アクセス許可」の表示画面（例）

＊ 画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

アプリをインストールする際に必要とされる権限（パーミッション）を確認する（六箇条 ④）

Information-technology Promotion Agency, Japan

インストール済みアプリの権限（パーミッション）の確認方法とアンインストール方法

*

画像：（独）情報処理推進機構（IPA）

Copyright © 2013 独立行政法人　情報処理推進機構

セキュリティソフト（アプリ）を利用する（六箇条 ⑤）

パソコンと同様に、ウイルス対策は専用の対策ソフト（アプリ）を利用するのがお勧めです。

昨今では、ベンダー各社も挙（こぞ）って、スマートフォン用のセキュリティ対策ソフトを発表しています(詳細はベンダー各社の製品紹介を参照してください)。

これらのセキュリティソフトは、パソコンで培った技術を利用して、スマートフォンでも高度な対策ができるようです。それゆえ、これらのセキュリティソフトは、ウイルス対策だけでなく、それ以外のセキュリティ機能を持っている場合が多いので、スマートフォンの機種毎に対応状況を確認の上、利用することをお勧めします。

一般的に、アプリはインストールしただけでは動いていないことがほとんどです。

通常は「インストール終了」をきっかけにセキュリティソフト（アプリ）によるスキャンが始まることが多いので、対象となった当該アプリに対するセキュリティソフト（アプリ）による診断結果をよく確認してください。

場合によっては、ウイルス検知された当該アプリを自分でアンインストールすることが必要となります。

Copyright © 2013 独立行政法人 情報処理推進機構

スマートフォンを小さなパソコンと考え、パソコンと同様に管理する（六箇条 ⑥）

Information-technology Promotion Agency, Japan

●ロック（鍵）をかける

スマートフォンは、パスワードなどでロック（鍵）をかけて、他人の使用を制限することができます。機種により操作方法は異なりますが、取扱説明書をご覧いただければ簡単に操作できますので、ロックをかけるようにしてください。

●データのバックアップをとる

機種によっては、何度か入力を間違えると、スマートフォン内のデータが自動的に消去される場合もあります。普段から重要なデータはバックアップをとっておきましょう。ただし、バックアップをとる際には、スマートフォンとは別の場所（例えば、オンラインストレージやPCを通じて外部記憶媒体等）にバックアップを取ることが肝要です。

●メモリーカードなどの取り扱い

メモリーカードは、便利で、日常的に利用している方もいると思いますが、何も対策をしていないメモリーカードは、パソコン等で内容が読みだされてしまうので、十分気をつけてください。メモリーカードだけ紛失したり、ちょっと目を離したすきに盗難され、大切なデータが流出する場合もあります。

メモリーカードには重要なデータは残さないこと、また、メモリーカードで重要なデータを保存する必要がある場合は、データの「暗号化」を行うようにしてください。セキュリティソフトの中にはメモリーカードを暗号化する機能が付いているものがあり、この機能を利用すると、あなたのスマートフォンだけで読み書きができるようになります。

●紛失した場合の対応策

紛失した場合には、速やかに、購入したお店や携帯電話会社のサポート窓口に連絡して、紛失の対応策を相談しましょう。遠隔操作でスマートフォンにロックをかけられる機種であれば他人が操作できないようにしてもらえます。また、スマートフォンの位置を特定したり、中のデータを消去できる場合もあります。これらは、自分自身でもできる機種もありますので、取扱説明書をご覧いただき、事前に操作方法等を理解しておきましょう。

Copyright © 2013 独立行政法人　情報処理推進機構

ファイルのダウンロード時の注意

Information-technology Promotion Agency, Japan

●安易なダウンロードはしない

・誤ってトロイの木馬やキーロガーをダウンロードしてしまう可能性がある

●不審なサイトには近づかない

・さまざまな手法で罠が仕掛けられているので、思わぬ被害を受ける可能性がある

画像：（独）情報処理推進機構（IPA）

●警告を無視しない。入会規約などがあれば目を通す

●むやみに[OK]や[実行する]をクリックしない

●ウイルス対策ソフトなどでは検出できない場合もあるため何も検知されなくても不用意にファイルを開かない

●ファイルの見た目に騙されない

・アイコンなどは偽装されている可能性がある

Copyright © 2013 独立行政法人　情報処理推進機構

ファイル名・アイコン偽装

*

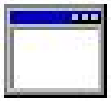
画像：(独)情報処理推進機構(IPA)

★ ここで紹介したデモはセミナー用に作成したサンプルプログラムです

Copyright © 2013 独立行政法人 情報処理推進機構

ファイル拡張子の意味

【ファイルの種類とアイコン、拡張子の対応表】

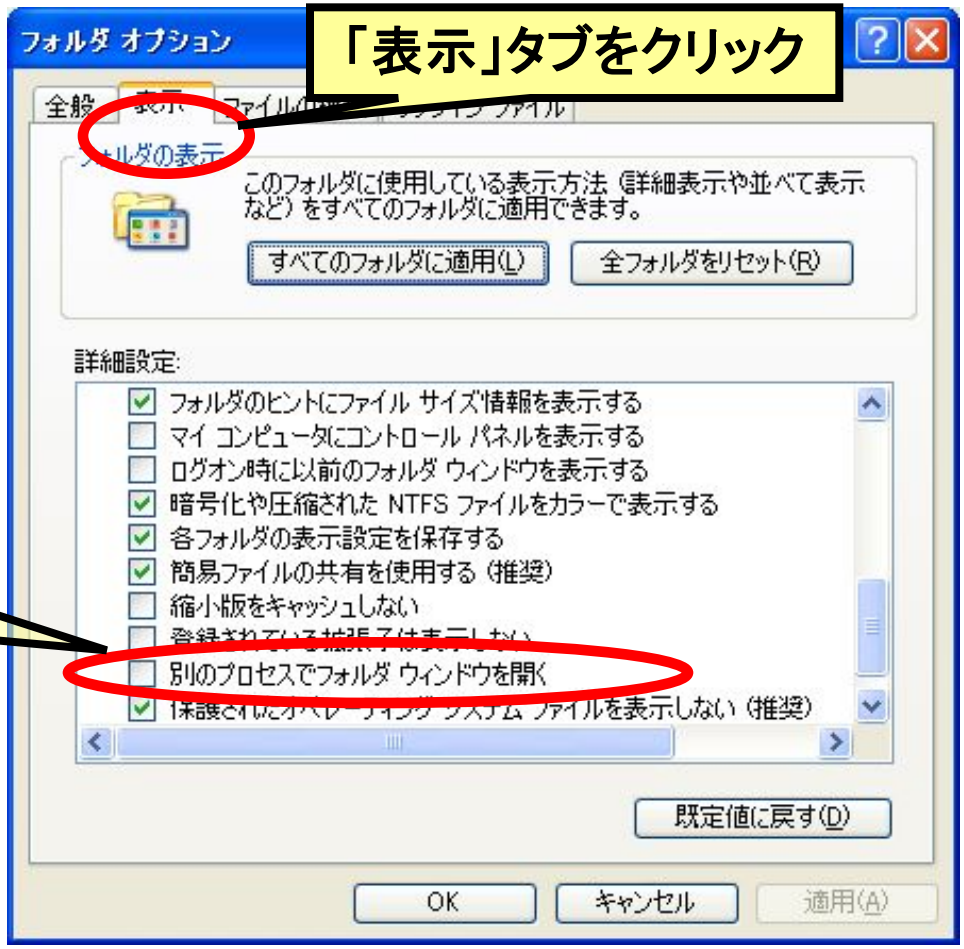
ファイルの種類	アイコン例	ファイル名＋拡張子の例
zip圧縮ファイル		圧縮ファイル.zip
画像ファイル		画像.jpg
文書ファイル		文書.doc
動画ファイル		動画.wmv 動画.mpg
テキストファイル		テキスト.txt
実行形式ファイル		実行ファイル.exe

*

画像:(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

怪しいファイルの見分け方



＊画像:(独)情報処理推進機構(IPA)

フォルダオプションを変更する

Copyright © 2013 独立行政法人 情報処理推進機構

怪しいファイルの見分け方

	ファイルの内容	「登録されている拡張子」の表示設定	
		表示しない場合	表示する場合
例１	動画ファイル	動画	動画.wmv
例２	スパイウェアの可能性あり	動画	動画.exe
例３	スパイウェアの可能性あり	動画.wmv	動画.wmv.exe

アイコンが偽装されている！

拡張子が“exe”なので、動画ファイルではない！

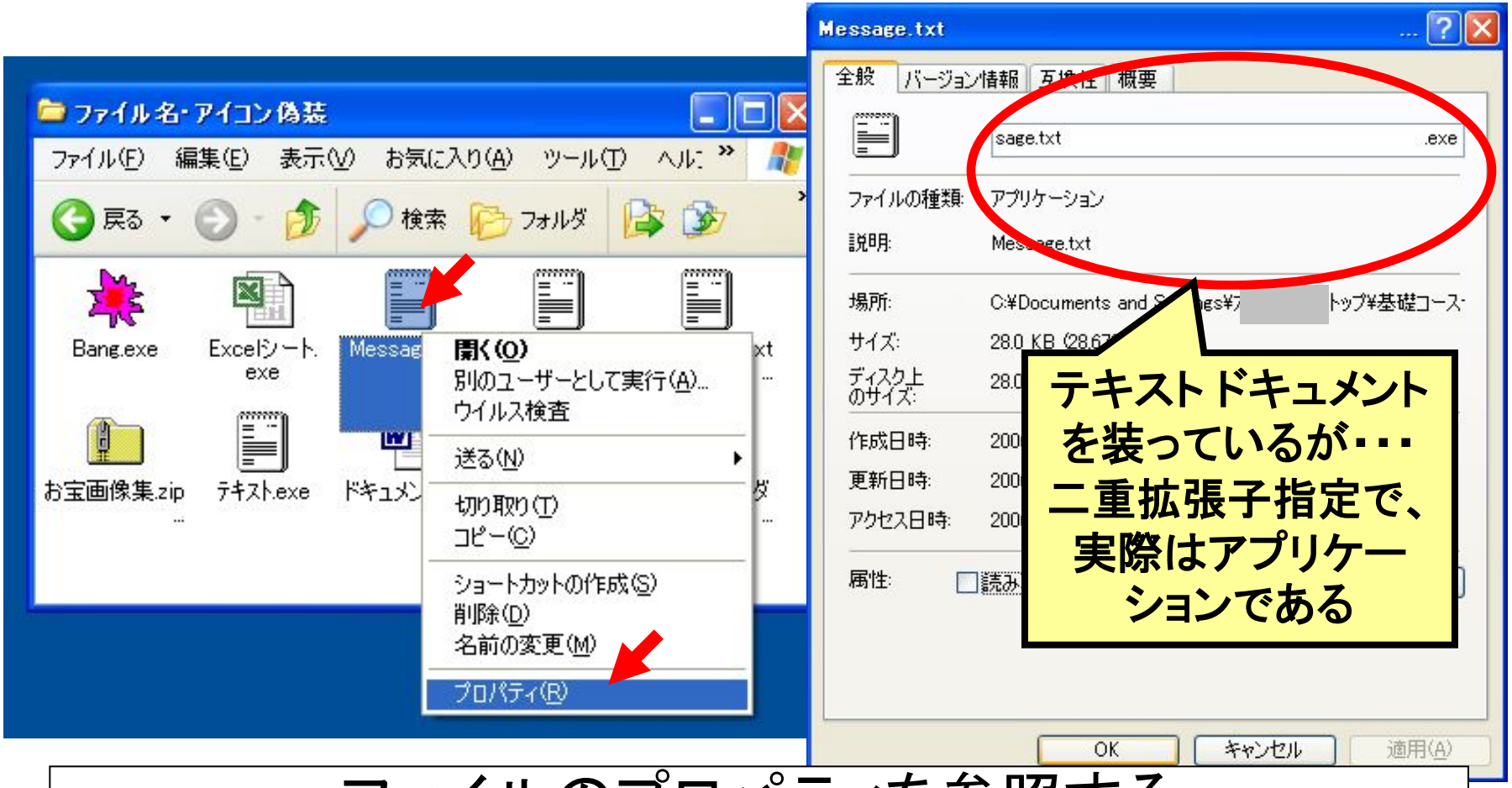
二セの拡張子に注意！

＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

怪しいファイルの見分け方

Information-technology Promotion Agency, Japan



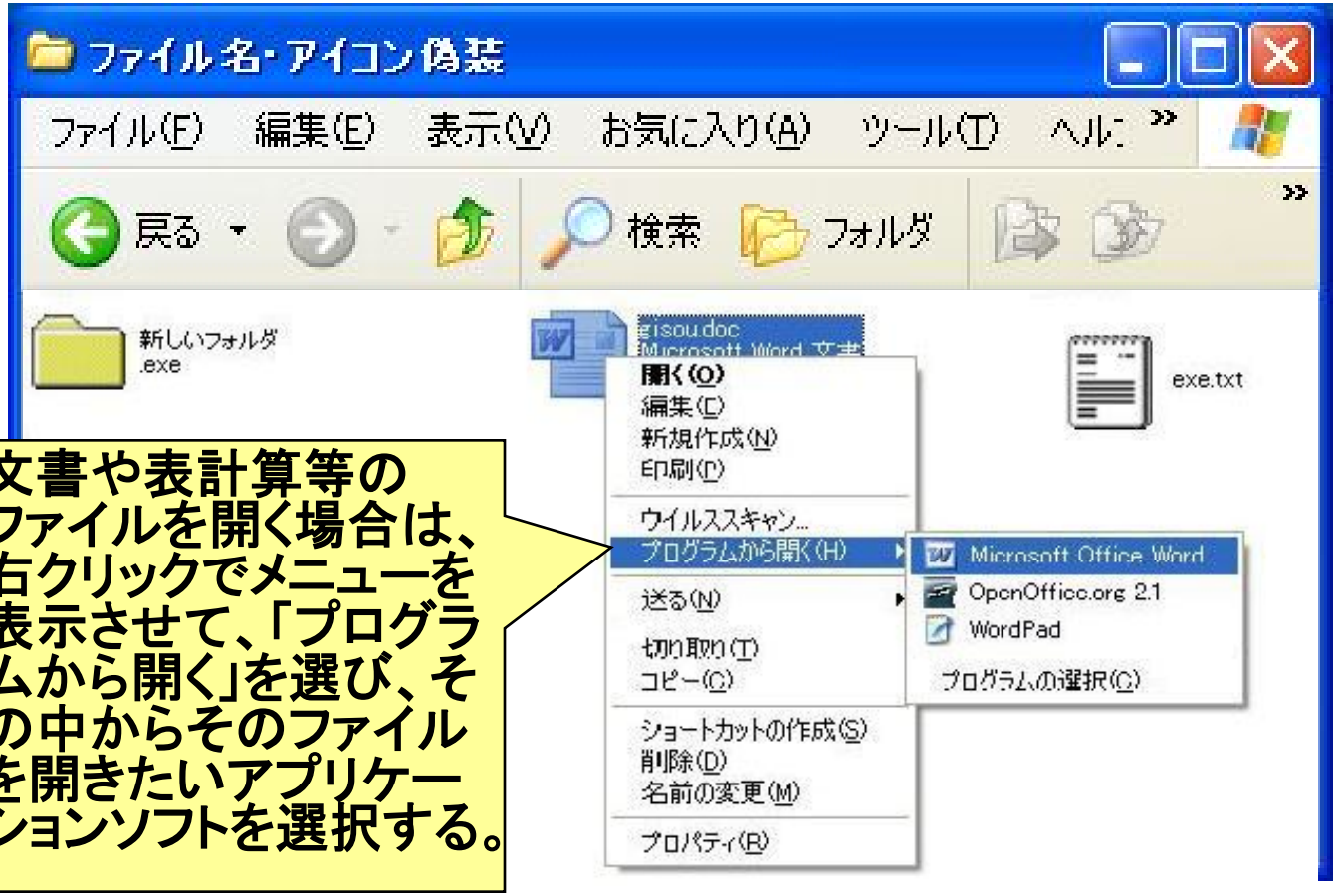
ファイルのプロパティを参照する

＊ 画像：(独)情報処理推進機構(IPA)

Copyright © 2013 独立行政法人 情報処理推進機構

ファイルの開き方

ファイルはできる限りダブルクリックで開かない。



文書や表計算等のファイルを開く場合は、右クリックでメニューを表示させて、「プログラムから開く」を選び、その中からそのファイルを開きたいアプリケーションソフトを選択する。

＊ 画像：(独)情報処理推進機構(IPA)

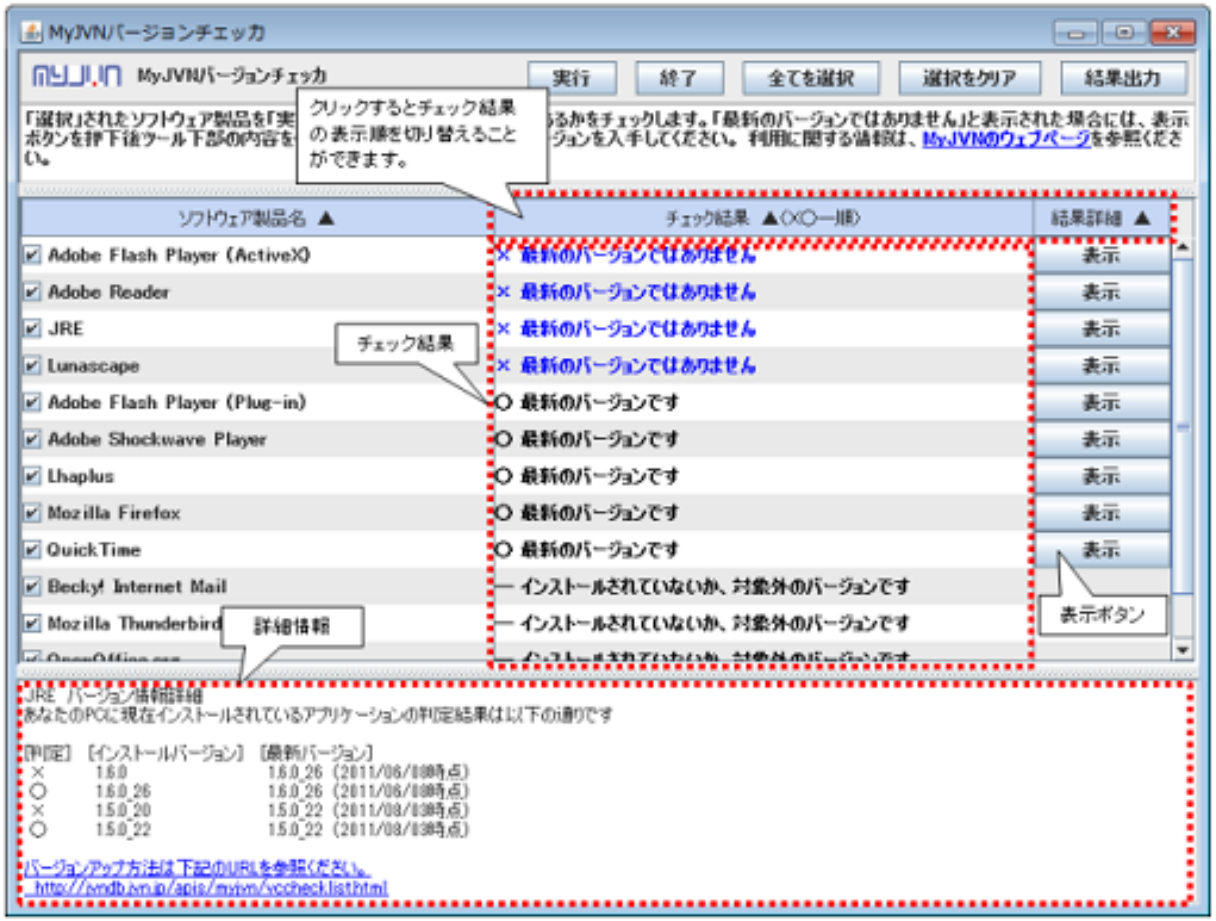
Copyright © 2013 独立行政法人 情報処理推進機構

Information-technology Promotion Agency, Japan

MyJVNバージョンチェッカ

ソフトウェアのバージョンが最新であるかを確認する

- 利用者のPCにインストールされているアプリケーションソフトウェアのバージョンが最新であるかを、簡単な操作で確認するツール
- バージョンが最新であるかどうかのチェックリストを自動で機械的に確認



*

画像：(独)情報処理推進機構(IPA)

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

Copyright © 2013 独立行政法人 情報処理推進機構

パスワード設定、管理

- 不適切なパスワード
  - 長さが不十分、辞書に載っている単語の利用、IDと同じ、自分・家族の情報、固有名詞、単純な数字や文字の並び、過去に使用したパスワードの再利用等
- 適切なパスワード
  - 大文字・小文字・数字・記号の組み合わせ、長いパスワード、推測しづらく自分が忘れないパスワード
    →例えばパスフレーズによる設計
- パスワード盗難対策
  - 定期的な変更、紙に書き留めない、マシンに保存しない、人に教えない

Copyright © 2013 独立行政法人 情報処理推進機構

パスワード設定、管理（パスフレーズ）

- パスフレーズによるパスワード設計
  - パスフレーズ

    「HARUHA　AKEBONO」

    ↓↓↓　母音を抜き記号や数字を挿入

  - 作成されたパスワード

    「HR＄HK%BN」

Copyright © 2013 独立行政法人　情報処理推進機構

基本的な対策　まとめ

- ワクチンソフトの導入・アップデート管理
- 不審なファイルは開かない
- セキュリティホールの解消
- アプリケーションの適切な設定
- ウイルス対策関連情報の収集
- 定期的なデータのバックアップ

Copyright © 2013 独立行政法人　情報処理推進機構

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

〒113-6591
東京都文京区本駒込２－２８－８
文京グリーンコートセンターオフィス１６階
URL　http://www.ipa.go.jp/security/
本講演資料及び普及啓発資料等のお問い合わせ先
セキュリティセンター　普及グループ
電子メール　isec-info@ipa.go.jp
TEL　03（5978）7508　　FAX　03（5978）7518

Copyright © 2013 独立行政法人　情報処理推進機構