

スマートフォンや情報通信サービスでの トラブル概説とセキュリティ対策

2017年11月20日

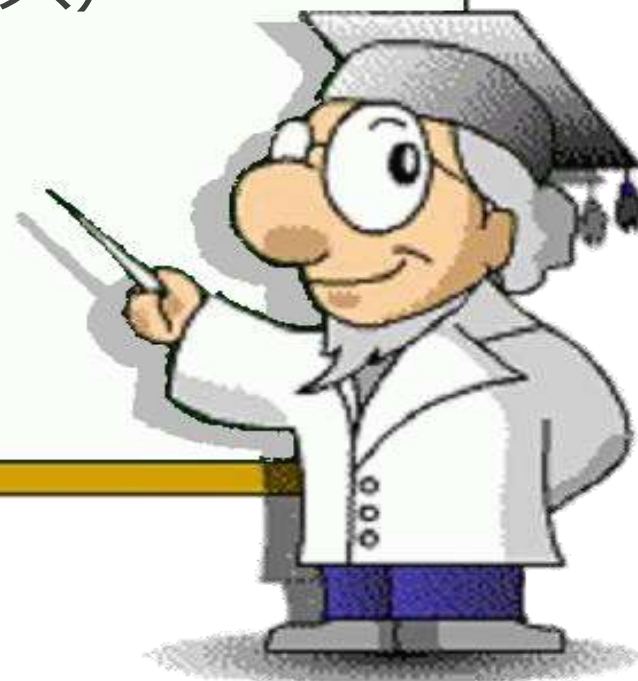
2017年12月 4日

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

中島 尚樹

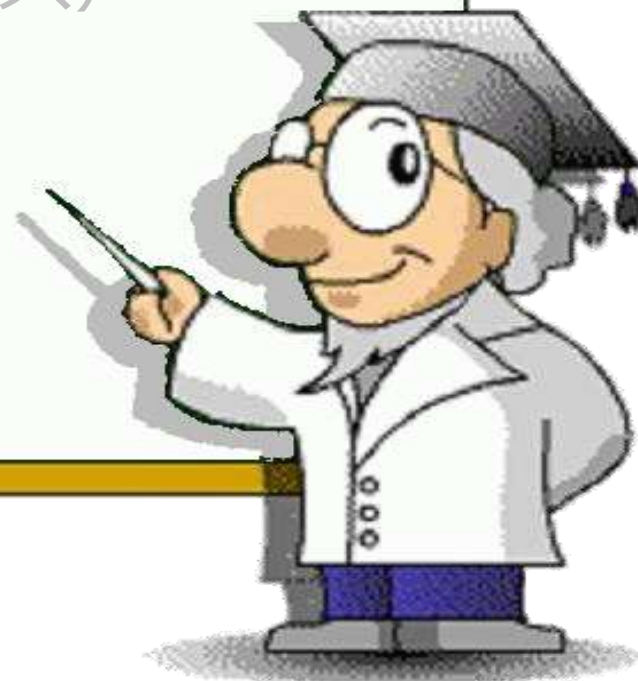
目次

- 1.情報セキュリティ安心相談窓口について
- 2.スマートフォンを狙った手口
- 3.詐欺、騙し系の手口
- 4.パソコンを狙うランサムウェア（ウイルス）



目次

1. 情報セキュリティ安心相談窓口について
2. スマートフォンを狙った手口
3. 詐欺、騙し系の手口
4. パソコンを狙うランサムウェア（ウイルス）



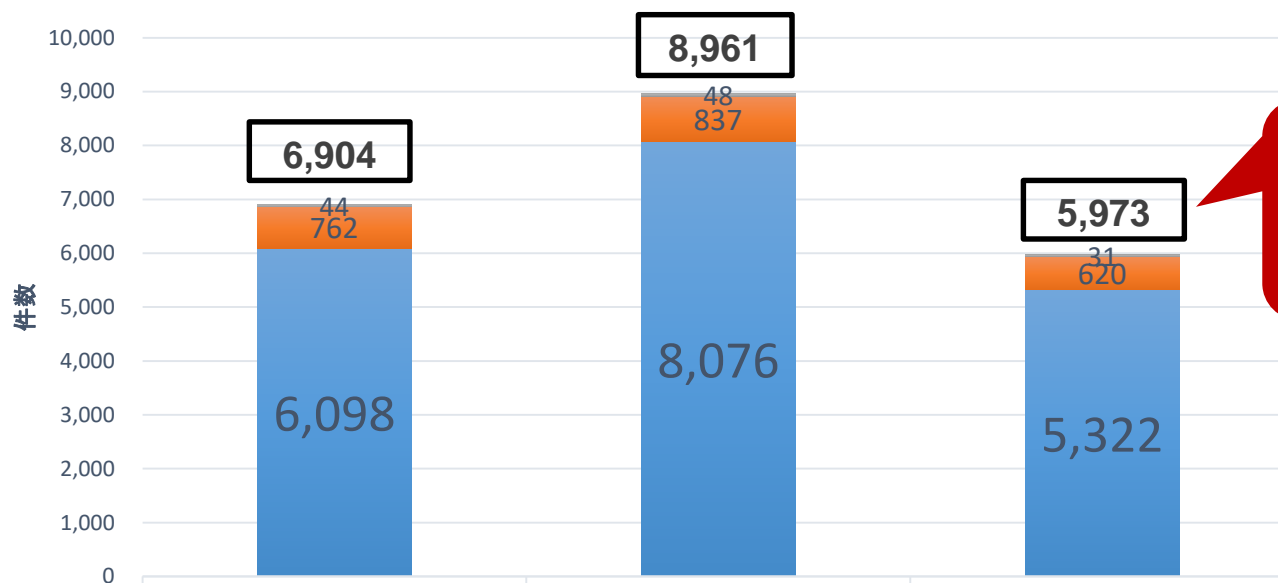
情報セキュリティ安心相談窓口とはIPA



- 安心相談窓口ポータルサイト
<https://www.ipa.go.jp/security/anshin/index.html>

- IPA(独立行政法人情報処理推進機構)が国民に向けて開設している、ウイルス（マルウェア）および不正アクセスに関する技術的なご相談を受け付ける窓口。
- 相談者のほとんどは、パソコンやインターネットを普通に利用している一般ユーザ。
- コンピュータウイルスの届出受付の付随業務として1990年に相談対応業務を開始。

相談件数推移

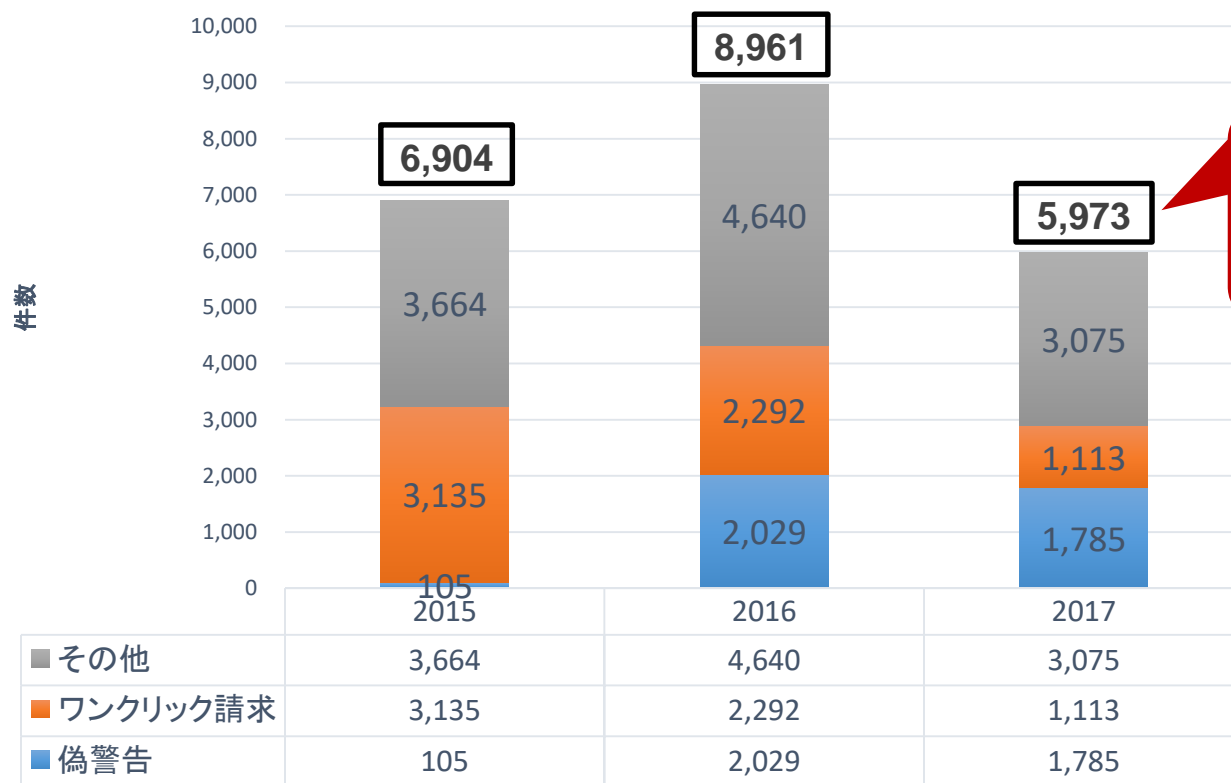


1月~9月分
の実績

	2015	2016	2017
■ FAX・その他	44	48	31
■ 電子メール	762	837	620
■ 電話	6,098	8,076	5,322

- 2017年は1月~9月の件数。
- 実際に相談員が対応を行った件数。
- 2016年は前年と比べて約2,000件増加となっているが、その増加分の大半を後述する『偽警告』の相談が占めている。

相談内容内訳件数



- 2017年は1月～9月の件数。
- 2016年より『偽警告』の相談が急増。2017年も継続傾向。
- 『偽警告』『ワンクリック請求』の2つの相談が多くを占める。
- その他は『偽対策ソフト』や、『不正ログイン』など多種多様な相談内容。

目次

1. 情報セキュリティ安心相談窓口について
2. スマートフォンを狙った手口
3. 詐欺、騙し系の手口
4. パソコンを狙うランサムウェア（ウイルス）



不正アプリのお話

(自分で入れちゃう話)

SNSやメールで不正アプリサイトへ誘導する事例 (2012年9月) ※Androidの事例

Subject:スマホの電池切れを解消！便利アプリを紹介[APP マグ]

Date:2012/09/24 11:30

To:●●@i●.jp

今回はアプリを紹介します。

□ 電池バッテリー改善アプリ

<http://●.net/●/◆◆.html>

スマホの電池切れを解消する、画期的なアプリが出ました。
このアプリを入れるだけで、朝充電して帰宅まで充電が不要になりました。
有料版や無料版を数多く試してきましたが、
今のところこのアプリが「ベスト」です。
バージョンアップの期間中だけ、無料でダウンロードが可能です。
今すぐ試してみてください！

□ 安心スキャン

<http://●.net/●/▼.html>

一番最初に入れたいウイルス対策アプリ。
軽い動作と、常に最新のウイルス対策パターンをダウンロードします。
無料でさくっとスキャン出来るのは魅力的。
定期的に行えば安心ですね♪

* =====* AI

◆編集・発行:便利アプリを紹介！APPマガ

◇配信停止・配信先の変更 <http://●.net/●/>

◆Copyright(C) 2011-2012, APPSマガ

◇本メールマガジンの著作権はAPPSマガに帰属します。
記事の無断転載は堅くお断りします

メール本文内のリンクをタッチすると、不正アプリサイトに飛ばされる！

Facebookの某コミュニティに投稿されていた、不正アプリサイトへのリンクを含んだ投稿



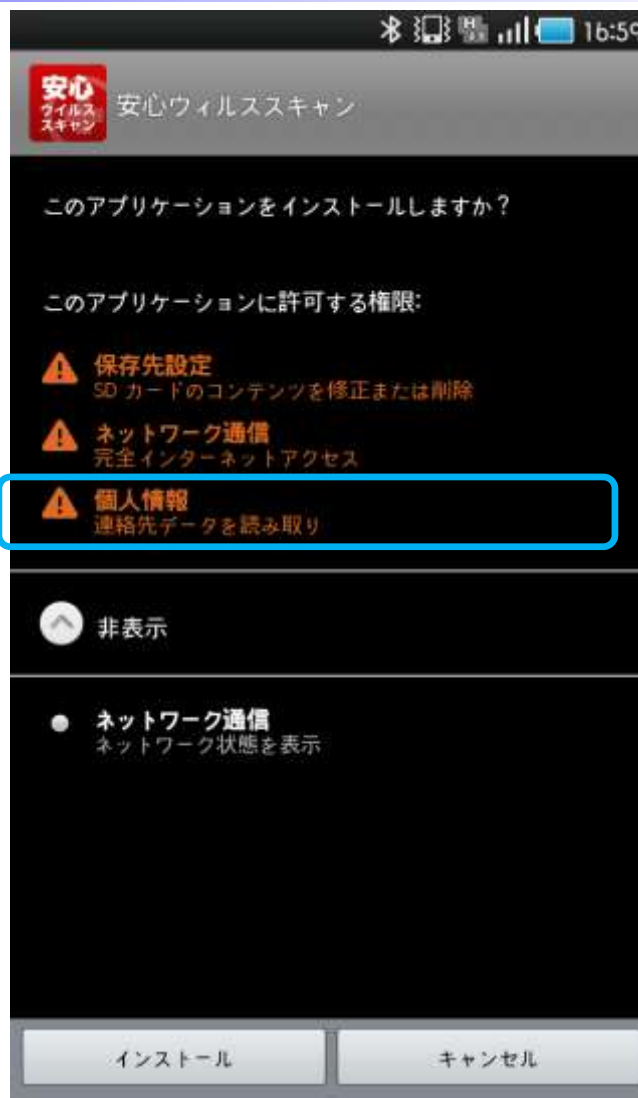
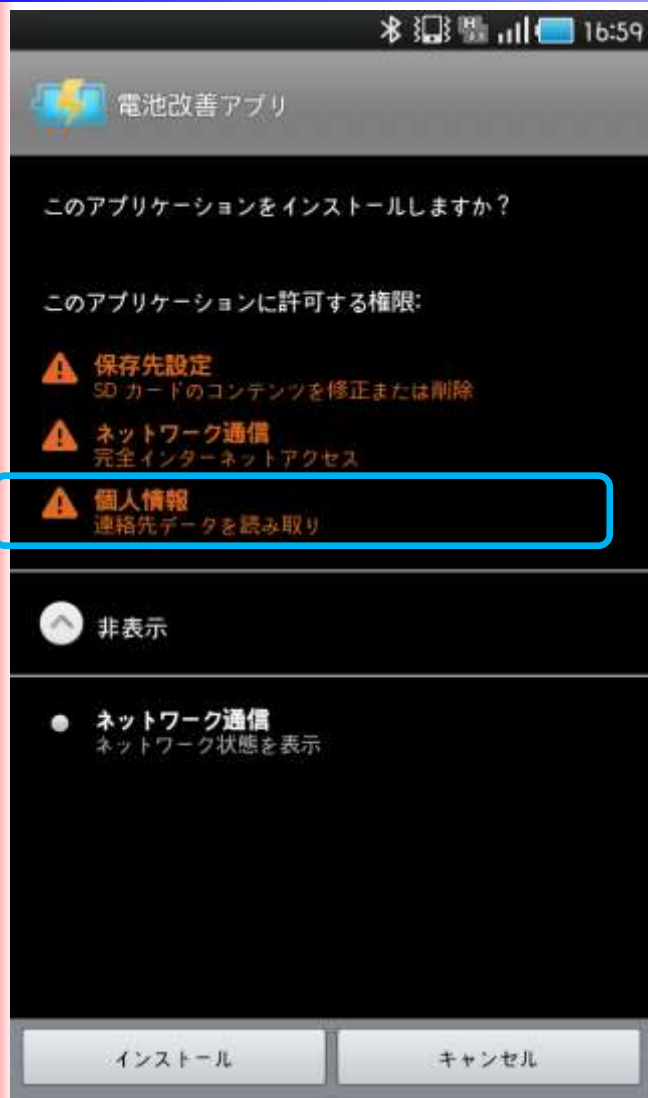
SNSやメールで不正アプリサイト へ誘導する事例 (2012年9月) ※Androidの事例



ウェブブラウザ
の画面

似ているが、
公式マーケット
(Google Play)
ではナイ！！

SNSやメールで不正アプリサイト へ誘導する事例 (2012年9月) ※Androidの事例



「連絡先データを読み取り」の許可を求めてくる！

※権限の許可を求められるタイミングは、Androidのバージョンによって異なる。

提供元不明のアプリ

※Androidの事例



普段は
「提供元不明のアプリ」
は【オフ】に！

オフにしておけば、間違っても不正アプリサイトからインストールすることは無くなる。

- 設定方法

設定⇒セキュリティ⇒提供元不明のアプリ

Androidアプリが権限を要求してくる 場面例



インストール時

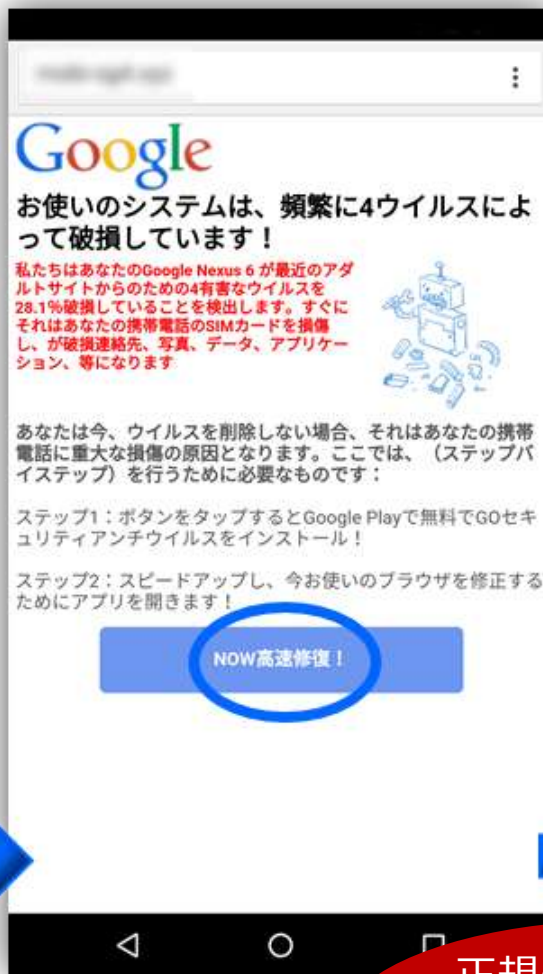
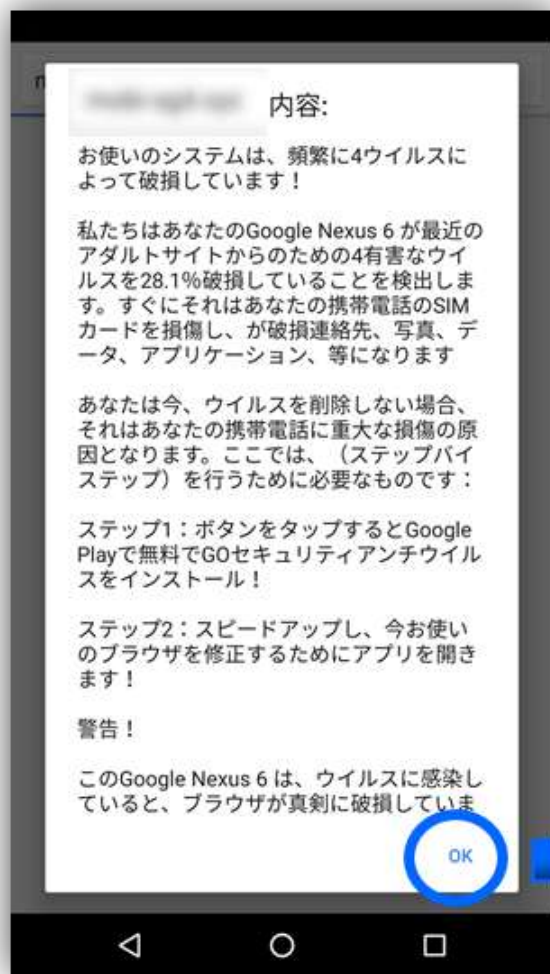
Android OSのバージョンによって表示のタイミングが異なる



アプリ初起動時、
権限初使用時

ウイルス感染警告

→正規アプリマーケット誘導 (2016年6月頃)



正規のアプリマーケットに誘導 (Google Play)

※Android端末での例

日本語表示に対応したAndroid版 ランサムウェア (2016年3月) ※Androidの事例

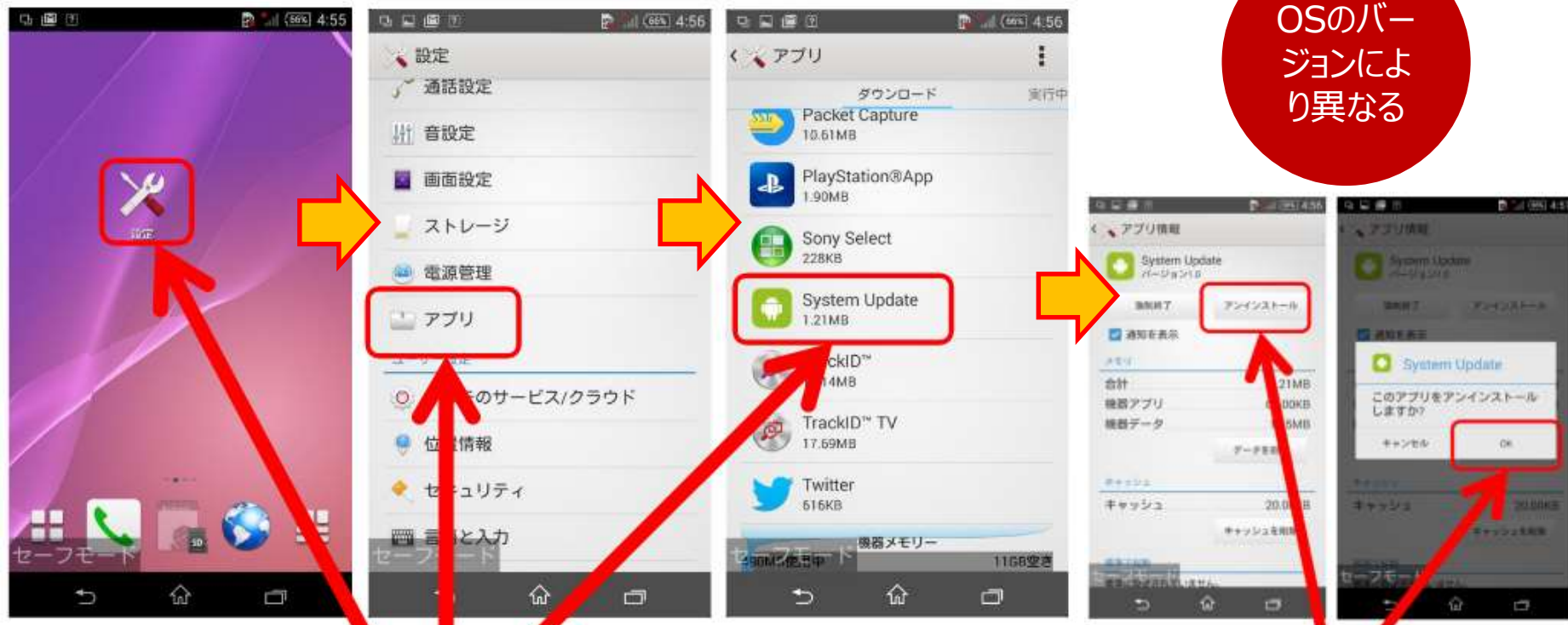


日本語"身代金"要求メッセージ



"罰金"支払指示表示

Androidランサムウェアへの対処法 IPA



「セーフモード」で起動し、アプリを削除すれば解決

詳しくは愛知県警の資料参照：

https://www.pref.aichi.jp/police/anzen/cyber/1news/documents/capture_1.pdf

https://www.pref.aichi.jp/police/anzen/cyber/1news/documents/uninstall_1.pdf

マーケットへのウイルスアプリの混入 **IPA**



管理



マーケットA

不正なアプリケーションを削除したり、事前審査を行うなど、管理されているマーケット

ウイルスなどの不正なアプリケーションが混入しやすい



マーケットB

管理が不十分、あるいは海賊版などを扱っているマーケット

アプリ悪用のお話

(誰かに入れられちゃう話)

アプリを悪用したストーカー事件が！IPA

その1

msn 産経ニュース

監視アプリ 666回録音 逮捕の男 元交際女性の日常確認

2014.4.11 10:29 【ストーカー事件】

元交際女性のスマートフォンに、位置情報などを知ることができるアプリを取り込んだとして不正指令電磁的記録供用容疑で、広島県東広島市立中学校教諭の中川省志容疑者（43）が逮捕された事件で、女性のスマホには、遠隔操作によりスマホの周囲の音声を666回録音した形跡があることが10日、広島県警への取材で分かった。

県警によると、昨年7～8月、音声録音のほか、通話履歴を399回確認し、位置情報を35回取得した形跡があり、動画や写真の撮影、メール送信、写真データの削除をしたケースもあった。

県警は、中川容疑者が別れた後の女性の日常生活を監視する目的で、アプリを悪用したとみて調べている。

音声録音などの記録はスマホの画面に表示されない設定になっていたが、女性が昨年11月、県警に「友人と自分しか知らない内容が、画面に浮かんですぐに消えたり、フェイスブックに記憶のない書き込みがあったりする」などと相談して発覚した。

アプリは本来、紛失防止用。同種のものインターネット上で複数販売、配布されているという。

アプリを悪用したストーカー事件が！IPA

その2

産経WEST

スマホの監視アプリで女子大生を隠し撮り 疑いで会社員再逮捕 愛知県警

2017.6.8 20:20

愛知県警は8日、勤務先でアルバイトしている女子大生のスマートフォンに遠隔監視アプリを無断でインストールし、自宅の様子を隠し撮りしていたとして、不正指令電磁的記録供用とストーカー規制法違反（見張り行為など）の疑いで、住所不定、会社員、高梨真義容疑者（42）を再逮捕した。

県警によると、遠隔監視アプリでの撮影に、ストーカー規制法を適用するのは全国初という。

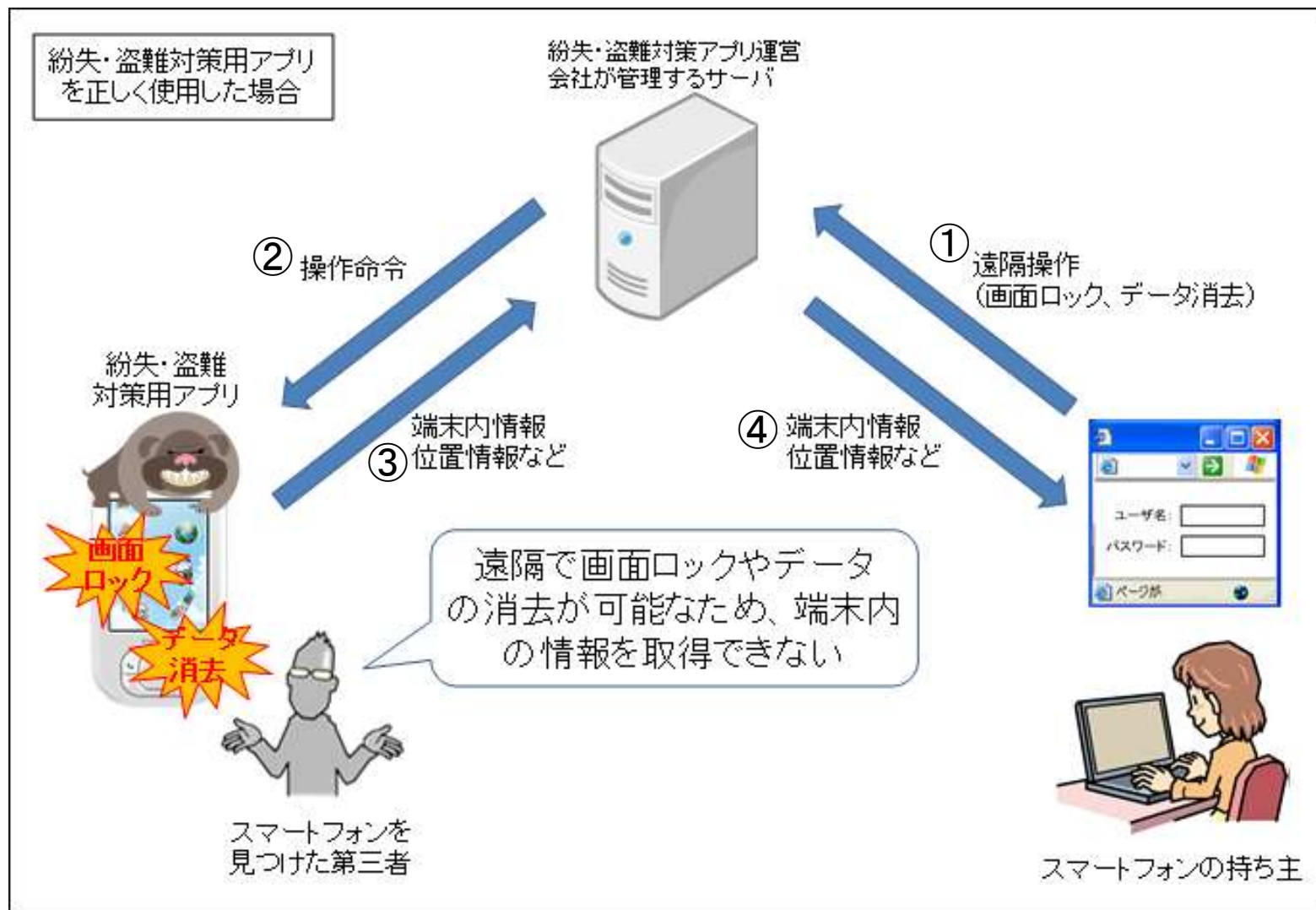
使用されたのは「Track View」というアプリで、音や動きに反応して撮影を始め、別のスマホでその動画が見られる。本来、自宅に残したペットを確認するためなどに使う。

再逮捕容疑は4月12日、同県日進市の女子大生（20）のスマホに、アプリを勝手にインストールし、5月2日に女子大生の居室に設置。6日までの間、自分のスマホで女子大生を見張った疑い。

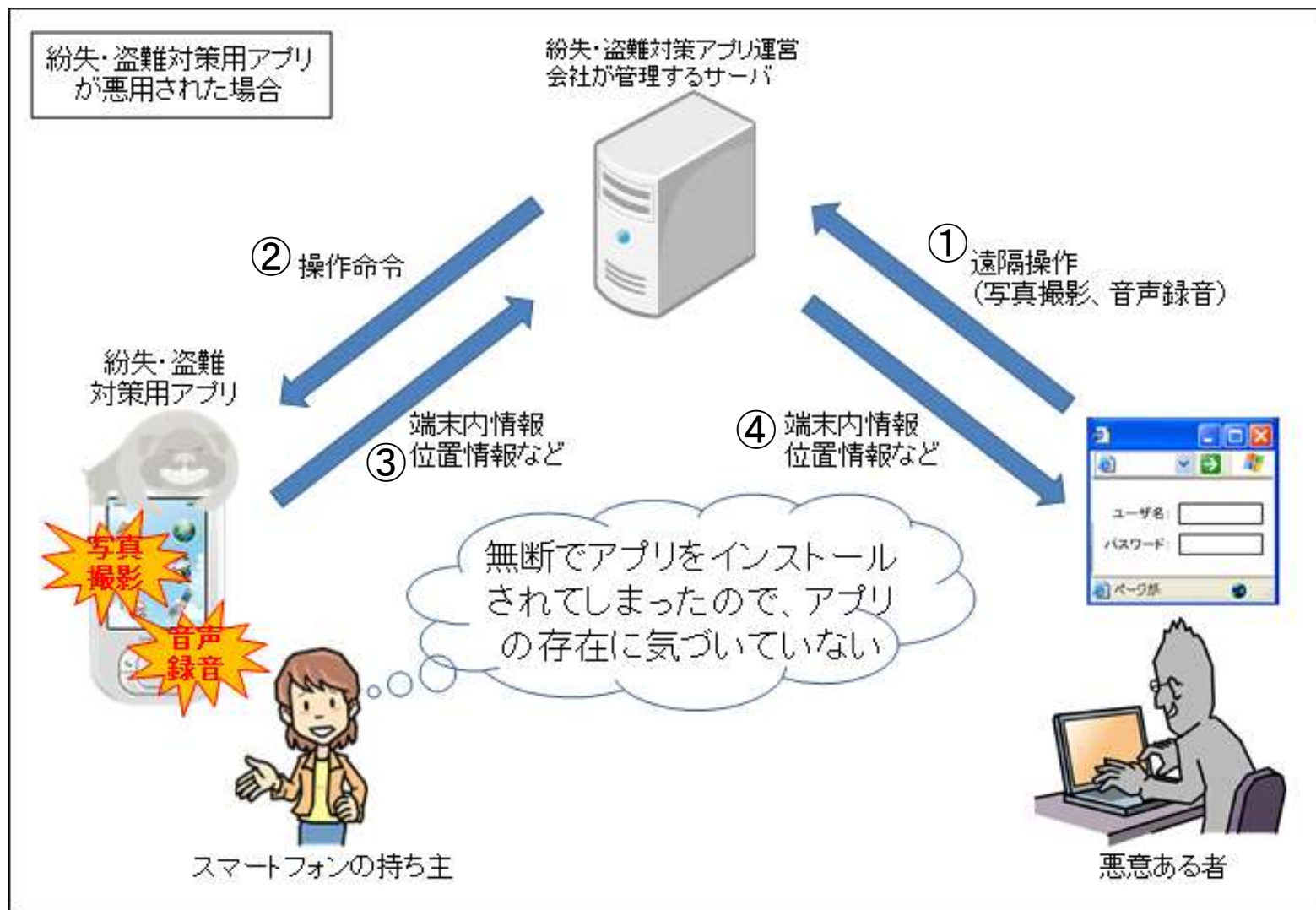
高梨容疑者は、女子大生が勤務中に部屋に侵入し、古いスマホを盗んでいたという。スマホが充電されていることを不審に思い、県警に相談。容疑者が映った動画がスマホに残っていたため発覚した。

県警が住居侵入容疑で5月9日に逮捕。スマホを盗んだとして、29日に住居侵入と窃盗容疑で再逮捕し、その後起訴された。

紛失防止用アプリの使い方（本来）



紛失防止用アプリの使い方（悪用）



スマホ不正アプリ対策

■不正アプリのインストールに注意する！

- 信頼できるアプリマーケットからインストール
- アプリに許可する権限の確認
- 端末ロックを設定
- むやみに他人に使わせない
- 身に覚えのないアプリがないか定期的に確認
- 本物のセキュリティ警告が落ち着いて確認



クラウド悪用のお話

クラウドに保存した情報が盗まれる！IPA

スマホに紐付いたアカウント情報の管理が重要！

Apple社のクラウドサービス
(iCloud)

② iPhoneで撮影した写真がiCloudに
保存 (アップロード) される



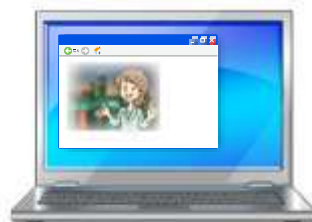
iCloudに保存されていた被害者の写真
データを窃取 (攻撃者の端末で受信)



攻撃者



① iPhoneで写真を撮影する



③ iCloudにログインすると他の端末
に写真データが送信される
(他の端末で写真を共有できる)

パスワードを教えるてはいけません！！IPA



スマホよく
わかん
ない・・・



このアプリ入れて
設定してあげる！



- ・セキュリティアプリ
- ・ID、パスワード登録
- ・各種設定

現在地を知られる！
遠隔でアプリを入れられる！
(^ω^;)

以下の管理に注意！！

- ・ Googleアカウント
- ・ Apple ID



今どこにいるかな・・・
このアプリ入れちゃおうかな・・・

クラウドでの不正アクセス事件！！

IPA

(2017年11月)

NHK NEWS WEB 2017年(平成29年)11月2日 木曜日

ニュース 動画 News Up 特集 スペシャルコンテンツ

新着 社会 気象・災害 科学・文化 政治 ビジネス 国際

複数の女性芸能人のデータのぞき見か 男を再逮捕

11月1日 15時52分

「iCloud」と呼ばれる写真などをネット上に保存するサービスに不正にアクセスしたとして逮捕された長崎県の男が、ほかにも、人気モデルなど複数の女性芸能人を含む10人のデータに不正にアクセスしていたとして、警察に再逮捕されました。

再逮捕されたのは、長崎県大村市の契約社員金子大地容疑者(31)です。

福岡県警察本部の調べによりますと、金子容疑者は、ことし1月から6月にかけて、「iCloud」と呼ばれるインターネット上に写真などのデータを保存するサービスを利用して人気モデルの益若つばささんやタレントの瑛茉ジャスミンさんなど複数の女性芸能人を含む10人のデータに不正にアクセスした疑いが持たれています。金子容疑者は先月、別の女性のデータに不正にアクセスしたとして、逮捕されていました。

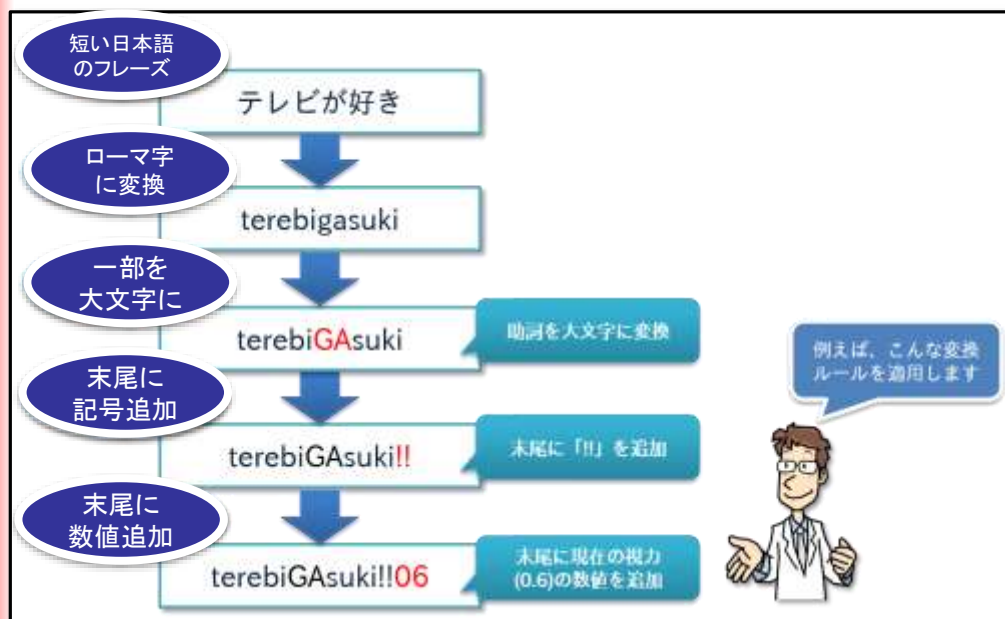
警察によりますと、SNSに公開された情報などからパスワードを割り出し、写真などを不正にのぞき見たうえ、自分のパソコンに保存していたということで、調べに対し「パスワードを破ることにやりがいを感じていた。他人のプライベート写真を見るのが楽しかった」などと供述しているということです。

SNSに公開された情報などからパスワードを割り出し

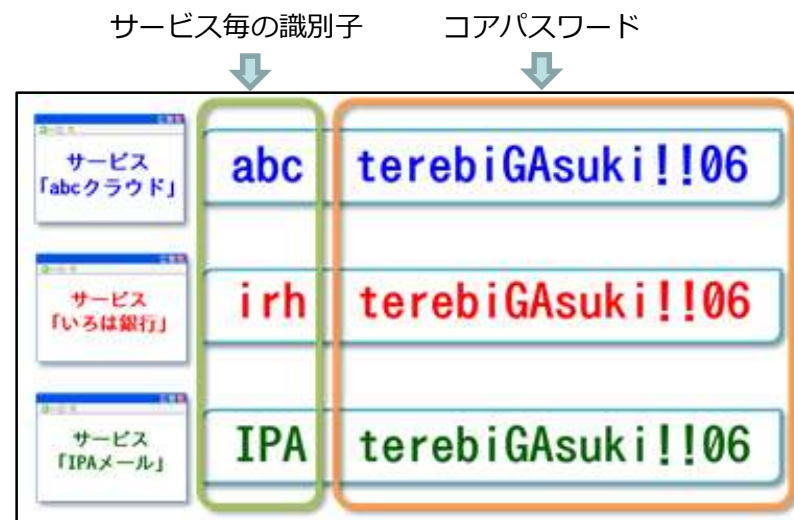
安全なパスワードの作成

- 「できるだけ長く」 : 総当り攻撃対策
- 「できるだけ複雑に」 : 辞書攻撃対策
- 「使い回さない」 : パスワードリスト攻撃対策

1. コアパスワードの作成



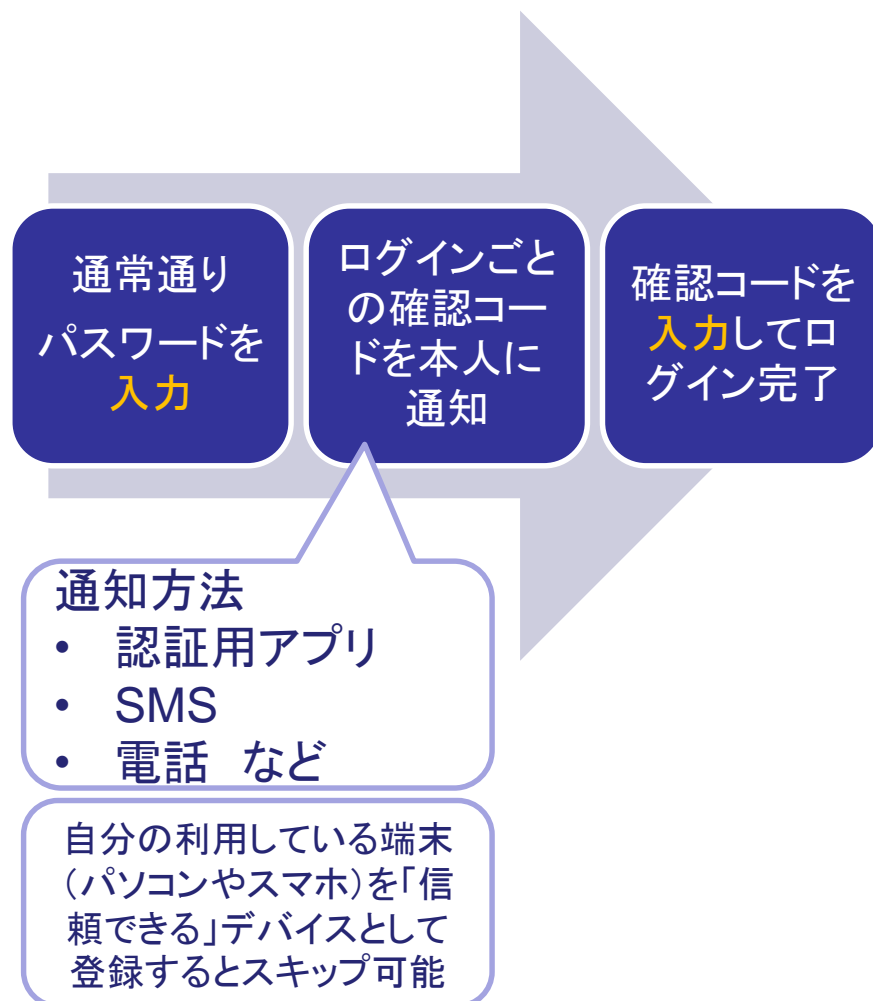
2. サービス毎に異なるパスワードの作成



二段階認証 (万が一、パスワードを破られても)

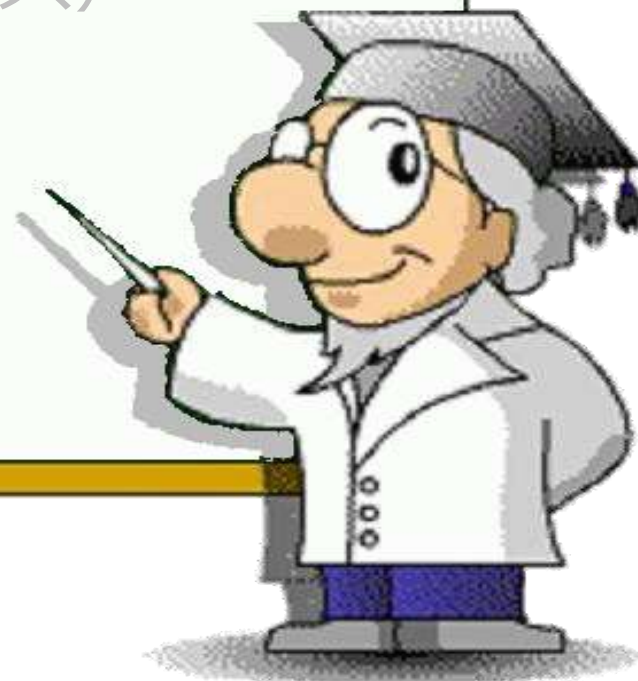
- 不正ログイン対策として、「二段階認証」の利用を推奨します。

- Googleアカウント
- Apple ID
- Microsoft アカウント
- Yahoo! JAPAN ID
- Amazon
- Facebook
- Instagram
- Twitter
- Dropbox
- Evernote etc…

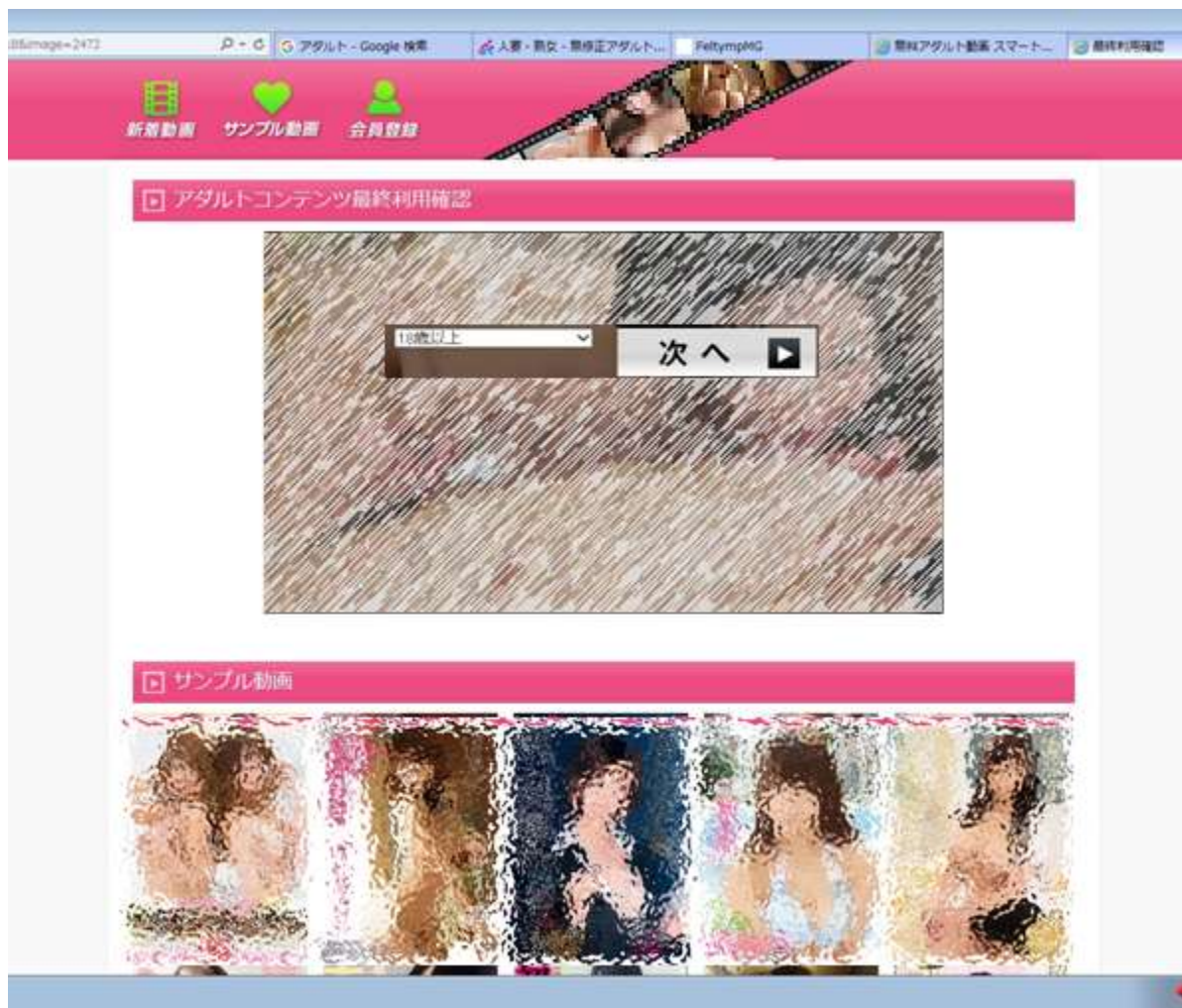


目次

- 1.情報セキュリティ安心相談窓口について
- 2.スマートフォンを狙った手口
- 3.詐欺、騙し系の手口
- 4.パソコンを狙うランサムウェア（ウイルス）



パソコン向けのワンクリ事例



パソコン向けのワンクリ事例

The screenshot shows a web browser window with a pink header. The header contains navigation links for '新着動画' (New Videos), 'サンプル動画' (Sample Videos), and '会員登録' (Member Registration). On the right side of the header, there is a support phone number '03-6328-2139' and operating hours: '平日: 1 (9:00~21:00) 日 (12:00~18:00)'. Below the header is a large black warning banner with yellow and white text: '警告!ご利用料金未払い' (Warning! Usage fee not paid) and '再生 ! 不可' (Playback ! Not possible). Below the banner, there are two red-bordered boxes: 'お客様登録ID: 12483441' and 'お支払い期限: 2016年11月17日'. Below these boxes is a small text box: 'こちらのページは過去にお客様よりご登録いただきました端末情報を基に表示されております。' (This page is displayed based on terminal information registered by you in the past). At the bottom, there are four pink buttons: 'キャンペーン料金の申請' (Apply for campaign fee), '誤作動の登録' (Register malfunction), '退会のお手続き' (Cancellation procedure), and 'クーリングオフについて' (About cooling-off).

パソコン向けのワンクリ事例

【重要】お客様登録ID
12483441

ご登録料金
59,800円

お支払い期限
2016年11月17日

◆ 誤作動で登録の方 ◆
30分以内にご連絡下さい
ご連絡頂き次第早急に対応致します

お客様総合サポート窓口 退会のお手続き

平日・土曜日 (9:00~翌3:00) 日曜日 (12:00~18:00)

☑ ご登録ありがとうございます

登録の流れ 利用規約

パソコン向けのワンクリ事例

お登録ありがとうございます

登録の流れ
誤作動を確認

利用規約
注意事項及び規約内容をご確認下さい

お客様のご登録情報

登録ID	12483441
携帯情報	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
登録日	2016年11月17日
お振込み期限	登録当日
ご利用期限	3年間

※振込期限：登録当日(翌日以降は通常料金)
※振込名義人の欄には必ずお客様ID【12483441】を入力ください。

お問い合わせ
平日・土曜日 (9:00~翌3:00)
日曜日 (12:00~18:00)

料金のご詳細

登録前の規約にある通り、本サイトのご登録については1080日間使い放題で198,000円となっております。ご利用料金は必ず3日以内にお支払い下さい。

【キャンペーン料金】 59,800円	【通常料金】 198,000円	【お振込】
------------------------------	---------------------------	-------

自宅、実家（住民票、本籍地）やご勤務先に【ご請求書】を送致します。

支払わない！！

電話しない！！

請求画面の消し方

■ 症状

- 画面を閉じて、暫くするとまた出てくる
- PCを再起動しても、また出てくる

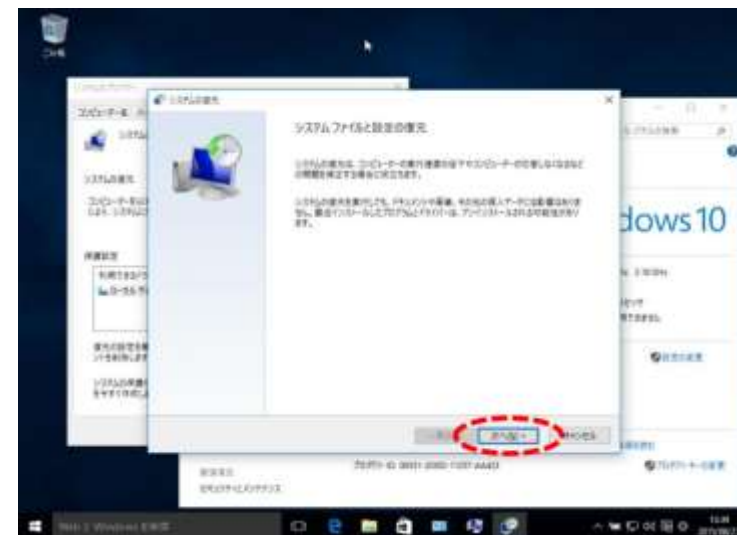
■ 消し方

- 請求画面の消し方は『システムの復元』を推奨
- システムの復元ができる条件
 1. 「システムの保護」が有効になっている
 2. アダルトサイトの請求画面表示時点より前の日時で「復元ポイント」が作成されている

システムの復元ができない場合はパソコンの初期化を推奨



請求画面を表示する
プログラムがインス
トールされている

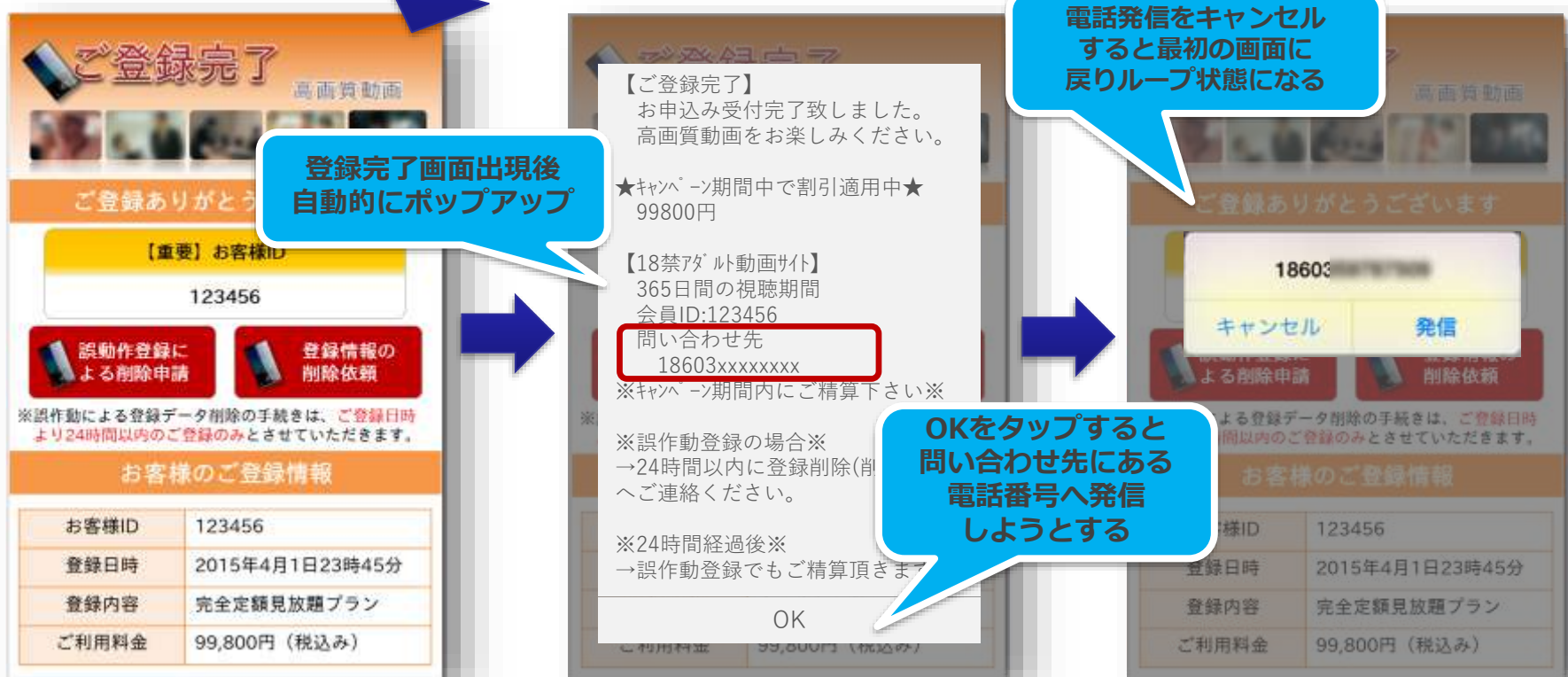


システム復元手順の画面例

詳しくは、IPA情報提供ページ
「ワンクリック請求被害への対策」
<https://www.ipa.go.jp/security/anshin/1click.html>

ワンクリック請求の新しい手口 電話を発信させる (2015年4月)

消し方：
ブラウザを閉じる



①登録完了画面出現

②登録に関する情報表示

③電話発信の確認

詐欺的手法の数々 . . .



- ・ 甘い言葉でフィッシングサイトへ誘導
- ・ セキュリティ系の脅し文句で App Storeへ誘導

ウイルスを検出したと音声で警告

音声による警告

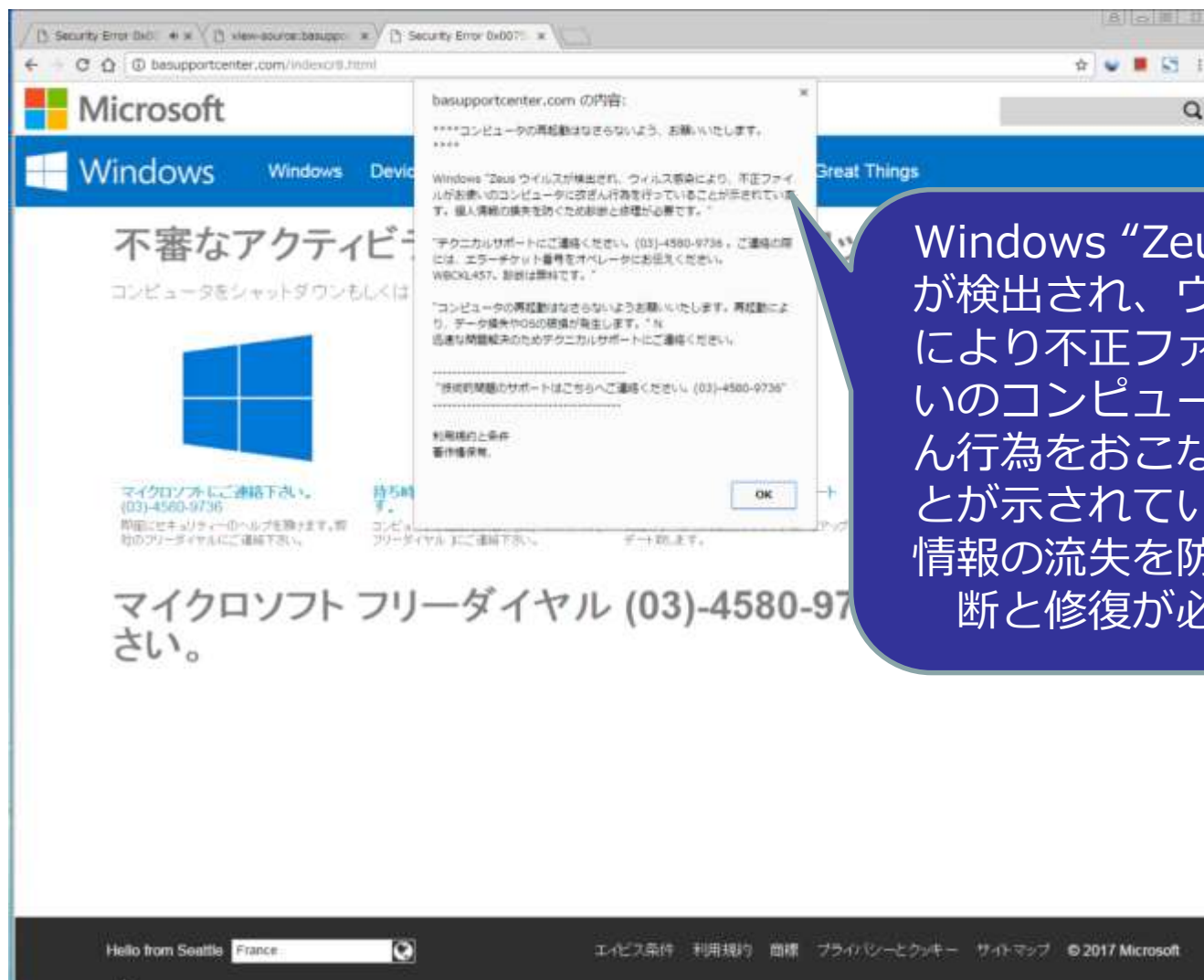
遠隔操作サポートへの
電話を促される

ウイルス感染は
困るから電話して
対応してもらおう…

電話をすると、ウイルス駆除のため
のソフトウェア購入を促される

「偽警告」 サイト→遠隔操作事例

(2017年1月)



Windows "Zeus"ウイルスが検出され、ウイルス感染により不正ファイルがお使いのコンピュータに改ざん行為をおこなっていることが示されています。個人情報の流失を防ぐための診断と修復が必要です。

「偽警告」 サイト→遠隔操作事例 (2017年1月)

(ファイル名を指定して実行) で「eventvwr」を実行した結果

The screenshot shows the Windows Event Viewer application. The main pane displays a list of events with the following data:

レベル	日付と時刻	ソース	イベント...	タスクの...
エラー	2017/01/30 9:32:04	Distri...	10010	なし
エラー	2017/01/30 9:31:34	Distri...	10010	なし
警告	2017/01/30 9:27:01	Outlook	36	なし
エラー	2017/01/30 9:27:01	Outlook	34	なし
警告	2017/01/30 9:27:00	Outlook	36	なし
エラー	2017/01/30 9:27:00	Outlook	34	なし
警告	2017/01/30 9:26:59	Outlook	59	なし
警告	2017/01/30 9:26:24	Securi...	8225	なし
エラー	2017/01/30 9:25:58	Devic...	131	なし
エラー	2017/01/30 9:25:58	Devic...	131	なし
エラー	2017/01/30 8:37:24	Office...	0	なし

An 'イベント 10010, DistributedCOM' dialog box is open in the foreground, titled 'ファイル名を指定して実行'. It contains the text: '実行するプログラム名、または開くフォルダーやドキュメント名、インターネット リソース名を入力してください。' and a text box with '名前(Q): eventvwr'. The dialog has 'OK', 'キャンセル', and '参照(B)...' buttons.

A red speech bubble on the left side of the image contains the text: 'この操作を指示される'.

新手の偽警告事例 (2017年3月)

パソコンが正常に操作できなくなったと錯覚させる多数の狡猾な細工

The image shows a Windows Defender notification window overlaid on a web browser displaying a support page. The notification window contains a list of items to be scanned: Facebook password, credit card info, email account password, and photos. A mouse cursor is shown moving over the notification, with a callout box highlighting this animation. Another callout box points to the notification's title bar. A third callout box points to a 'Time-limited message' box on the right side of the browser window. A fourth callout box points to a Windows Security notification in the bottom right corner. The support page in the background contains a list of items to be scanned, a phone number (03-4579-1974), and a 'Time-limited message' box.

Windows Defenderの画面

時間制限のメッセージ

マウスのポインターが移動するアニメーション

お使いのPCからウイルスとスパイウェアを検出しました。PCから盗まれている情報:

- > Facebookのパスワード
- > クレジットカード情報
- > Eメールアカウントのパスワード
- > このコンピュータに保存されている写真

我々のエンジニアがウイルスの削除方法をお教えますので、今すぐお電話ください。あなたのコンピュータが無効にならないよう、5分以内に我々にお電話ください。

サポートへの電話番号: 03-4579-1974

Windowsがお使いのコンピュータで潜在的な脅威を検出しました。

Windows Security Essentialはウイルスをブロックできませんでした。Windowsは、プライバシーを侵害したり、コンピュータに損傷を与える可能性がある潜在的な脅威を検出しました。

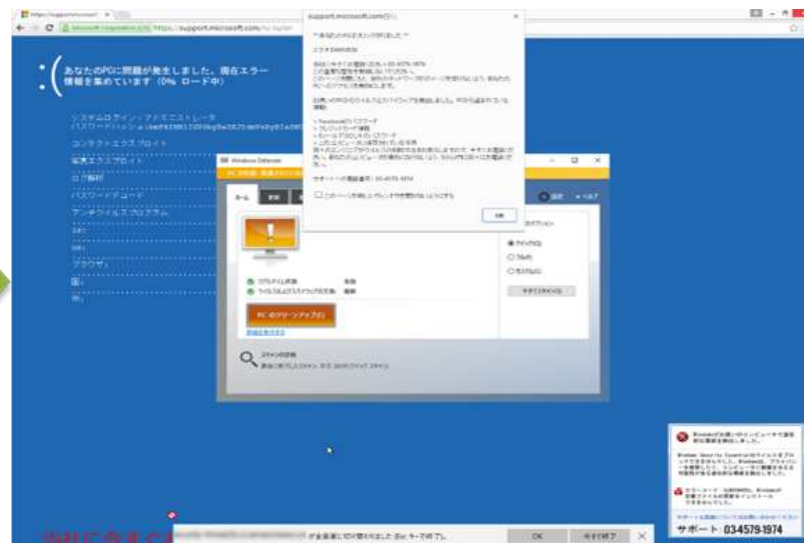
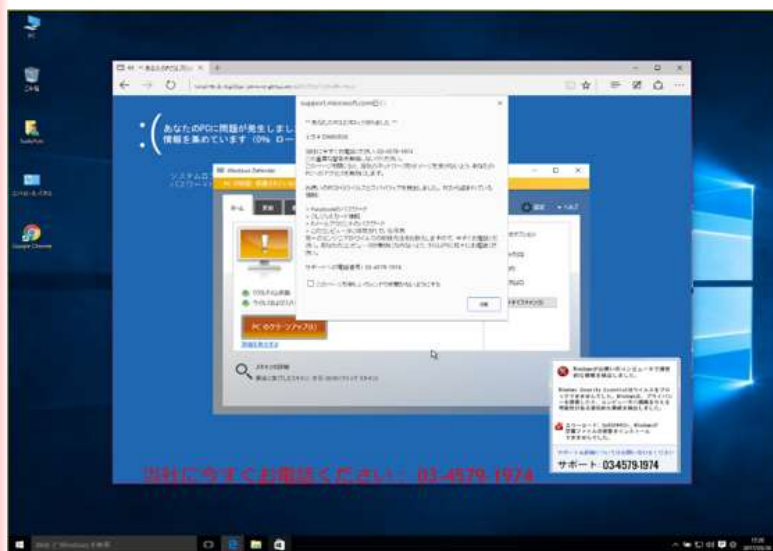
エラーコード: 0x8024402c。Windowsが定義ファイルの更新をインストールできませんでした。

サポートと詳細についてはお問い合わせください
サポート: 03-4579-1974

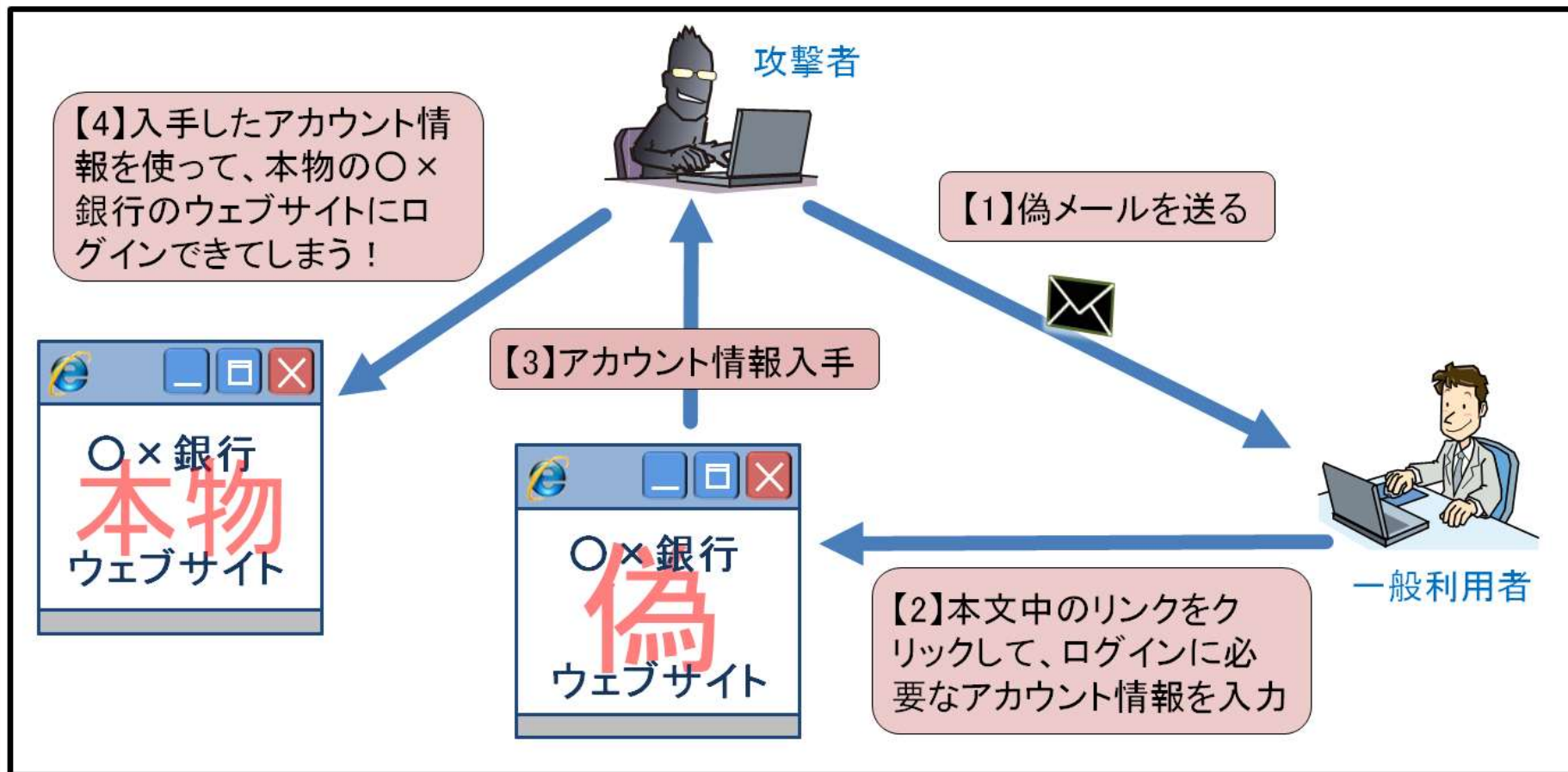
当社に今すぐお電話ください: 03-4579-1974

新手の偽警告事例 (2017年3月)

ブラウザを全画面表示にして本来のデスクトップを隠す



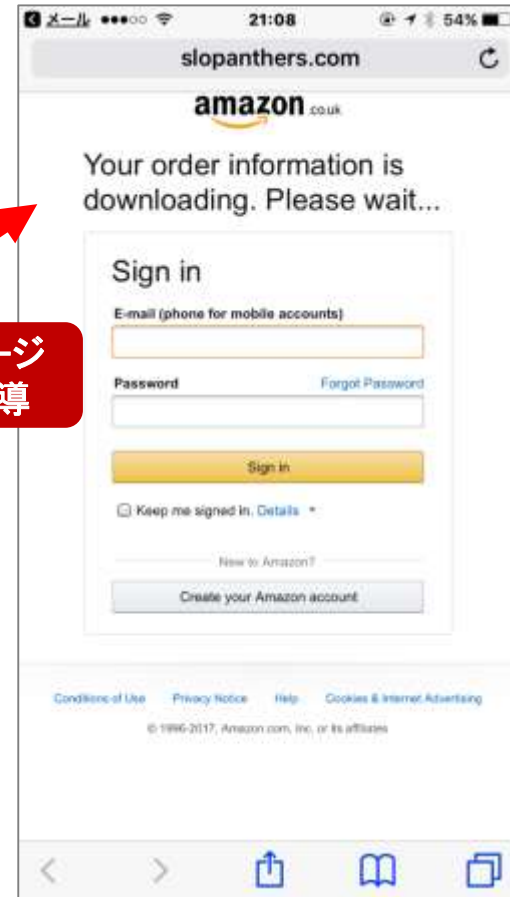
フィッシングの基本的手順



Amazonを狙ったフィッシング事例 (2017年) IPA



偽ページへ誘導



Appleを狙ったフィッシング事例

(2017年)

数種類の違う
パターンがある



詐欺・騙し系の対策

■ ワンクリック詐欺

- 気をつけていても請求画面が出る可能性はある。
- 電話をかけない、支払わない。

■ 偽警告サイト（サポート詐欺）

- 気をつけていても請求画面が出る可能性はある。
- 警告表示が本物かどうか落ち着いて確認。
- 電話をかけない、支払わない。

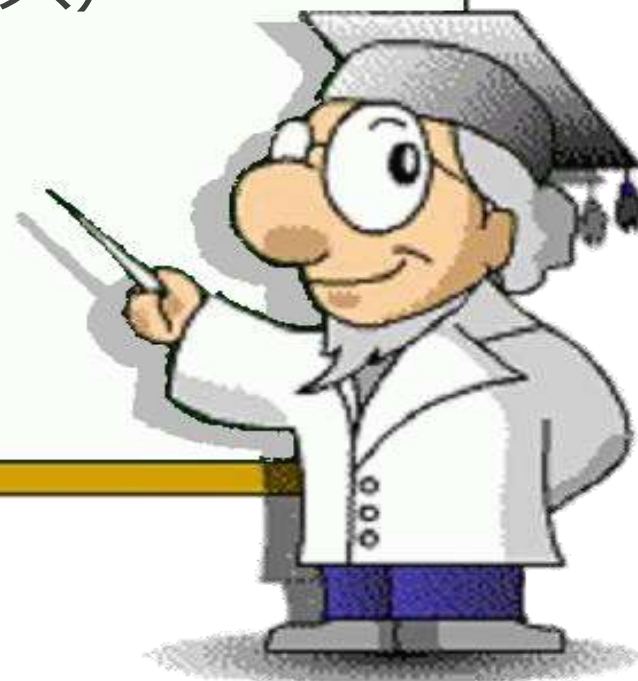
■ フィッシングメール

- メール中のリンクのクリックには十分注意する。
- 銀行やショッピングサイトなどからどのようなタイミングで、どのようなメールが届くかを事前に理解する。



目次

1. 情報セキュリティ安心相談窓口について
2. スマートフォンを狙った手口
3. 詐欺、騙し系の手口
4. パソコンを狙うランサムウェア（ウイルス）



ランサムウェアの脅威

ランサムウェアとは

2つの言葉を組み
合わせた造語

Ransom (身代金)

+

Software (ソフトウェア)



Ransomware (ランサムウェア)

ランサムウェアの脅威

ランサムウェアに感染すると・・・

パソコンの利用に制限をかけられる

- ・ ファイルを暗号化され、開けなくなる
- ・ 端末をロックされ、操作できなくなる

ファイル
暗号化型

端末ロック型

制限解除のためのメッセージが表示される

- ・ 発生した事象や復旧方法（金銭の支払いの要求）
などが記載されている

ランサムウェア感染デモ動画



<https://www.youtube.com/watch?v=duN9dYG4q3s>

<https://www.youtube.com/user/ipajp/>

IPA公式チャンネルもどうぞ

ランサムウェアの脅威

ランサムウェアに感染すると・・・

制限解除のためのメッセージは、ランサムウェアにより様々

ご注意
お客様のファイルをCryptOL0ckerウイルスによって暗号化しました

お客様の重要なファイル(ネットワーク・ディスク、USBなどのファイルを含む)画像、動画、ドキュメントなどは、当方のCryptOL0ckerウイルスによって暗号化されました。お客様のファイルをもとに戻すには、お支払いが必要となります。お支払いがない場合、ファイルは失われます。

警告: CryptOL0ckerを削除しても、暗号化されたファイルへのアクセスを復活させることはできません。

ファイル復元のお支払いはこちらをクリックしてください

よくあるご質問

Q1 私のファイルはどうなったのですか?
問題の理解
お客様の重要なファイル(画像、動画、ドキュメントなどは、当方のCryptOL0ckerウイルスによって暗号化されました。このウイルスは非常に強力な暗号化アルゴリズムRSA-2048を使用しています。RSA-2048暗号化アルゴリズムの解明は特許取得済みの鍵なしでは不可能です。

Q2 いかんして自分のファイルを取り戻せるのですか?
ファイルを取り戻す唯一の方法
お客様のファイルは使用不能、閲覧不能になっています。同じようにそれがわかります。通常の状態で復元するための唯一の方法は、当方の特許取得済みの暗号解読ソフトを使用することです。当方のウェブサイト上で、この暗号解読ソフトをお買い求めいただけます。

Illustrations: A hacker with a key, a man at a laptop with a red explosion, and three files labeled ".encrypted" with padlocks.

ランサムウェアの脅威

ランサムウェアの感染経路

ウェブサイトからの感染

- ・ 改ざんされた正規のウェブサイトを開覧することで感染
- ・ 不正広告を開覧することで感染
- ・ ダウンロードしたファイルを開くことで感染

メールからの感染

- ・ メール本文に記載されたURLからアクセスすることで感染
- ・ メール添付ファイルを開くことで感染

ネットワークからの感染

- ・ ネットワークを介して攻撃パケットを送出することで感染

ランサムウェアの脅威

ランサムウェアの感染経路

ウェブサイトからの感染

ドライブ・バイ・ダウンロード攻撃

- ・改ざんされた正規のウェブサイトを開覧することで感染
- ・不正広告を開覧することで感染
- ・ダウンロードしたファイルを開くことで感染

メールからの感染

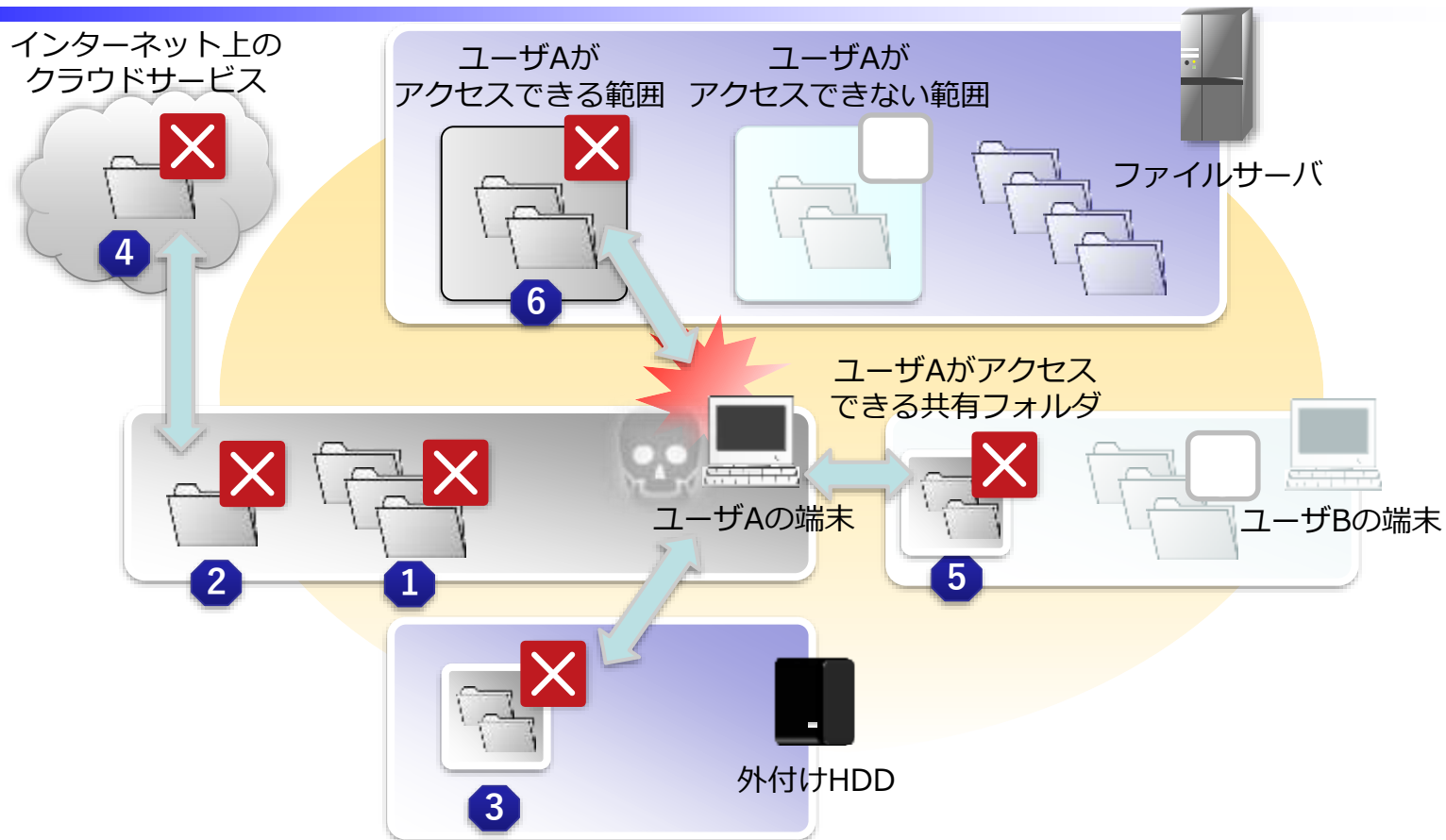
ドライブ・バイ・ダウンロード攻撃

- ・メール本文に記載されたURLからアクセスすることで感染
- ・メールの添付ファイルを開くことで感染

ネットワークからの感染

- ・ネットワークを介して攻撃パケットを送出することで感染

ランサムウェアの影響範囲

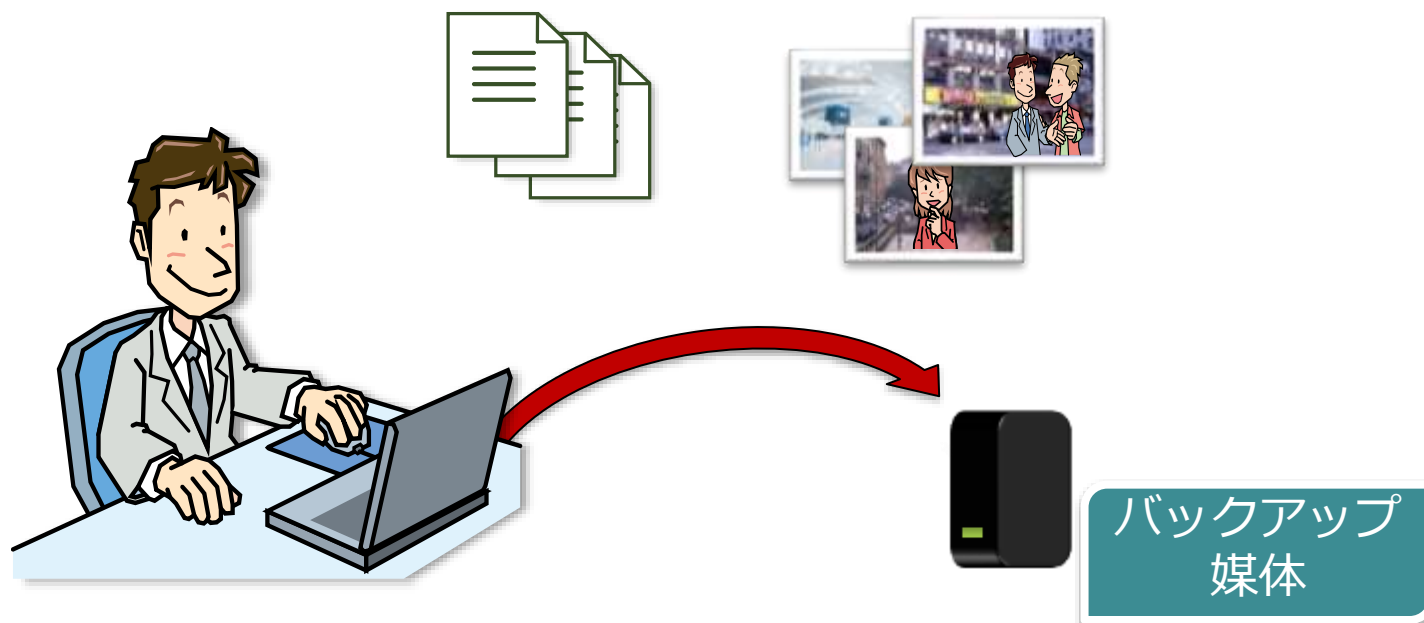


- | | |
|------------------------------------|--|
| 1 感染端末内に保存されているファイル | 4 ファイル暗号化後の同期によるクラウド内のファイル(上書き) |
| 2 感染端末内のクラウドと同期するフォルダ内のファイル | 5 感染端末と共有しているフォルダ内のファイル |
| 3 感染端末に接続されている外付けHDD内のファイル | 6 感染端末がアクセス可能な場所に保存されているファイル |

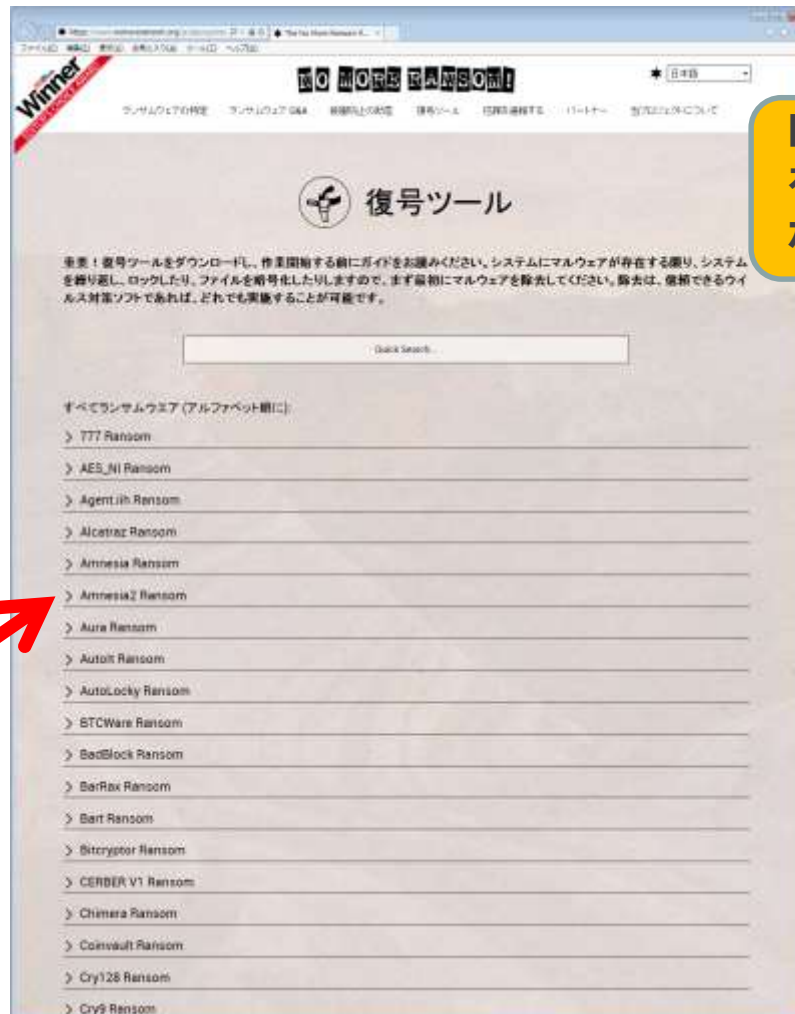
ランサムウェアの対策

定期的なバックアップを推奨

暗号化されたファイルを元通りにすることは非常に困難。
そのため、定期的なバックアップが有効！！



「No More Ransom」プロジェクト **IPA**



暗号化されたファイルを元に戻せるかもしれない復号ツールを提供

対応しているランサムウェア名

IPA
ランサムウェア
対策特設ページ
もご覧ください

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

<https://www.nomoreransom.org/ja/index.html>

セキュリティ対策の基本（パソコン）IPA

■ ウイルス対策ソフトの導入と適切な運用

- ウイルス定義ファイルを**最新に保つ**ことが必須！
- **統合型セキュリティソフト**がオススメ
(有害サイトのブロック機能やパーソナルファイアウォール機能が有効)

■ 脆弱性の解消

- OS（Windowsなど）、その他**ソフト全てを最新に**！
- こまめな**アップデート**が必須！

MyJVNバージョンチェッカをご活用ください！IPA

MyJVNバージョンチェッカ

実行 終了 全てを選択 選択をクリア 結果出力

「選択」されたソフトウェア製品を「実行」ボタンを押下後ツール下部の内容をい。

クリックするとチェック結果の表示順を切り替えることができます。

ソフトウェア製品名 ▲	チェック結果 ▲(X/O一冊)	結果詳細 ▲
<input checked="" type="checkbox"/> Adobe Flash Player (ActiveX)	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Reader	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> JRE	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Lunascape	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Adobe Flash Player (Plug-in)	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Adobe Shockwave Player	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Lhaplus	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Mozilla Firefox	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> QuickTime	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Becky! Internet Mail	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Mozilla Thunderbird	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> OpenOffice.org	— インストールされていないか、対象外のバージョンです	

チェック結果

詳細情報

表示ボタン

JRE バージョン情報詳細
あなたのPCに現在インストールされているアプリケーションの判定結果は以下の通りです

判定	インストールバージョン	最新バージョン
×	1.6.0	1.6.0_26 (2011/06/08時点)
○	1.6.0_26	1.6.0_26 (2011/06/08時点)
×	1.5.0_20	1.5.0_22 (2011/08/03時点)
○	1.5.0_22	1.5.0_22 (2011/08/03時点)

バージョンアップ方法は下記のURLを参照ください。
<http://jvndb.jvn.jp/apis/myjvn/vcchecklist.html>

Windows 10
にも対応！

IPA : MyJVN バージョンチェッカ
<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>

おまけ

情報セキュリティ10大脅威 2017



<https://www.ipa.go.jp/security/vuln/10threats2017.html>

タイトル(個人)	順位	タイトル(組織)
インターネットバンキングや クレジットカード情報の不正利用 昨年:1位	1	標的型攻撃による情報流出 昨年:1位
ランサムウェアによる被害 昨年:2位	2	ランサムウェアによる被害 昨年:7位
スマートフォンやスマートフォン アプリを狙った攻撃 昨年:3位	3	ウェブサービスからの個人情報の 窃取 昨年:3位
ウェブサービスへの不正ログイン 昨年:5位	4	サービス妨害攻撃による サービスの停止 昨年:4位
ワンクリック請求などの不当請求 昨年:4位	5	内部不正による情報漏えいと それに伴う業務停止 昨年:2位
ウェブサービスからの個人情報の 窃取 昨年:7位	6	ウェブサイトの改ざん 昨年:5位
匿名によるネット上の誹謗・中傷 昨年:6位	7	ウェブサービスへの不正ログイン 昨年:9位
情報モラル不足に伴う犯罪の 低年齢化 昨年:8位	8	IoT機器の脆弱性の顕在化 昨年:—
インターネット上のサービスを 悪用した攻撃 昨年:10位	9	攻撃のビジネス化 昨年:—
IoT機器の不適切な管理 昨年:—	10	インターネットバンキングや クレジットカード情報の不正利用 昨年:8位

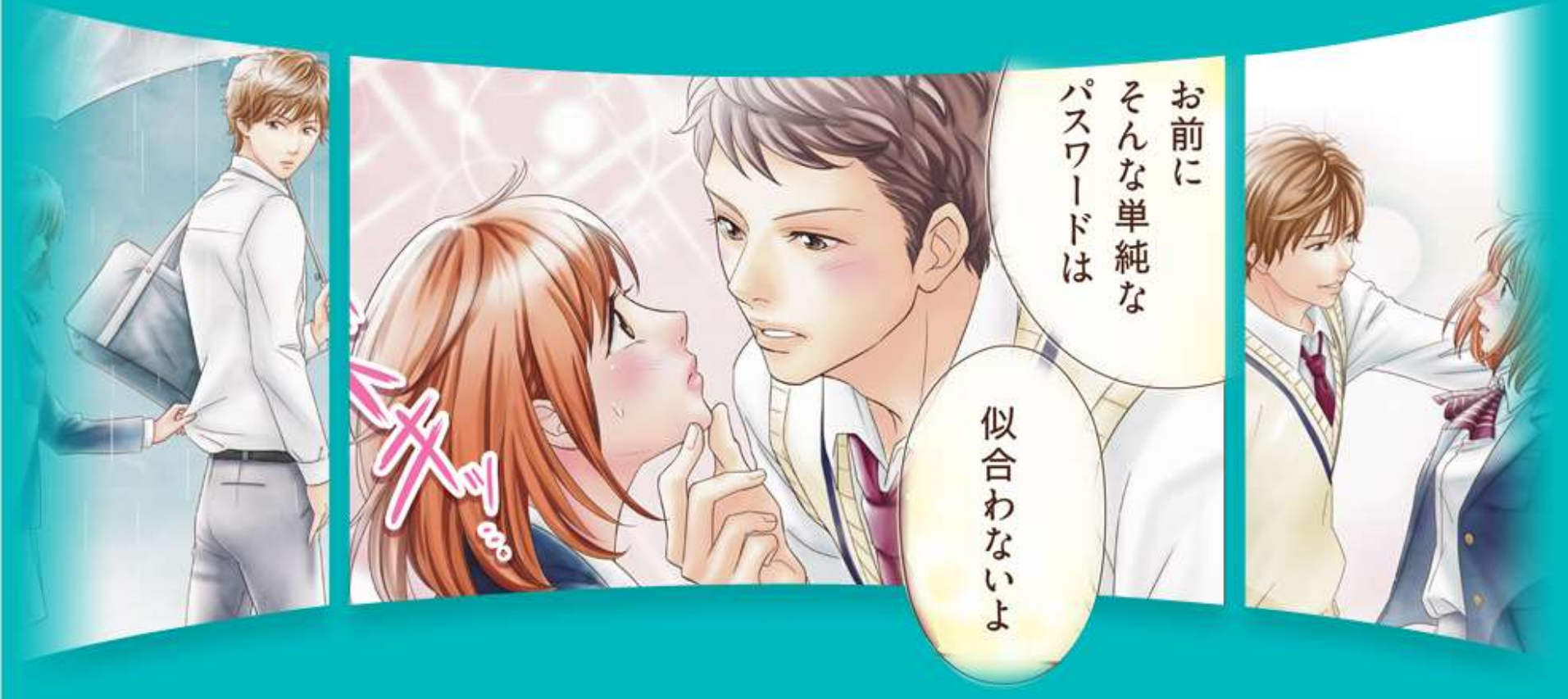
パ*ス*ワード

PASSWORD

安心してネットや
スマホを楽しむための

胸キュン♥
ラブストーリー

— もっと強くキミを守りたい —



<https://www.ipa.go.jp/security/keihatsu/munekyun-pw/>

IPA 胸キュン 検索

「iパス」は、ITを活用する すべての社会人・学生

が備えておくべきITに関する基礎的な知識が証明できる**国家試験**です。

試験の主なメリット

戦略、財務等
幅広い出題

仕事に役立つ

セキュリティ
を積極出題

セキュリティ
に強くなる

エントリー
シート等活用

就職に役立つ

上峰 亜衣
(う え み ね あ い)



パソコンを利用して受験するCBT方式なので、都合の良いときに受験可能！**お申込みはiパスWebサイトで常時受付中！**



独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

セキュリティセンター (IPA/ISEC)

<http://www.ipa.go.jp/security/>

★情報セキュリティ安心相談窓口:

TEL: 03(5978)7509 (平日10:00-12:00、13:30-17:00)

FAX : 03(5978)7518

E-mail: anshin@ipa.go.jp