IPA Better Life with IT

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

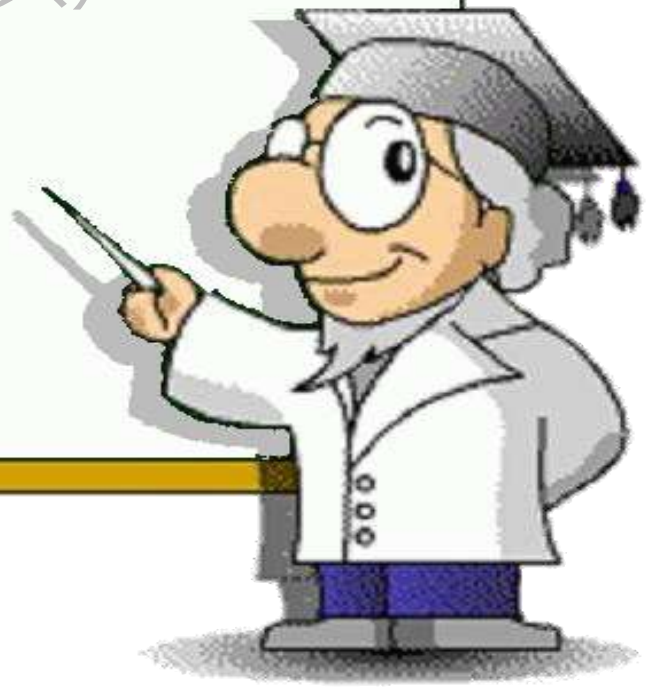
独立行政法人情報処理推進機構
技術本部　セキュリティセンター
中島　尚樹

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.ﾊﾟ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.ﾊﾟｿｺﾝを狙うﾗﾝｻﾑｳｪｱ（ウイルス）

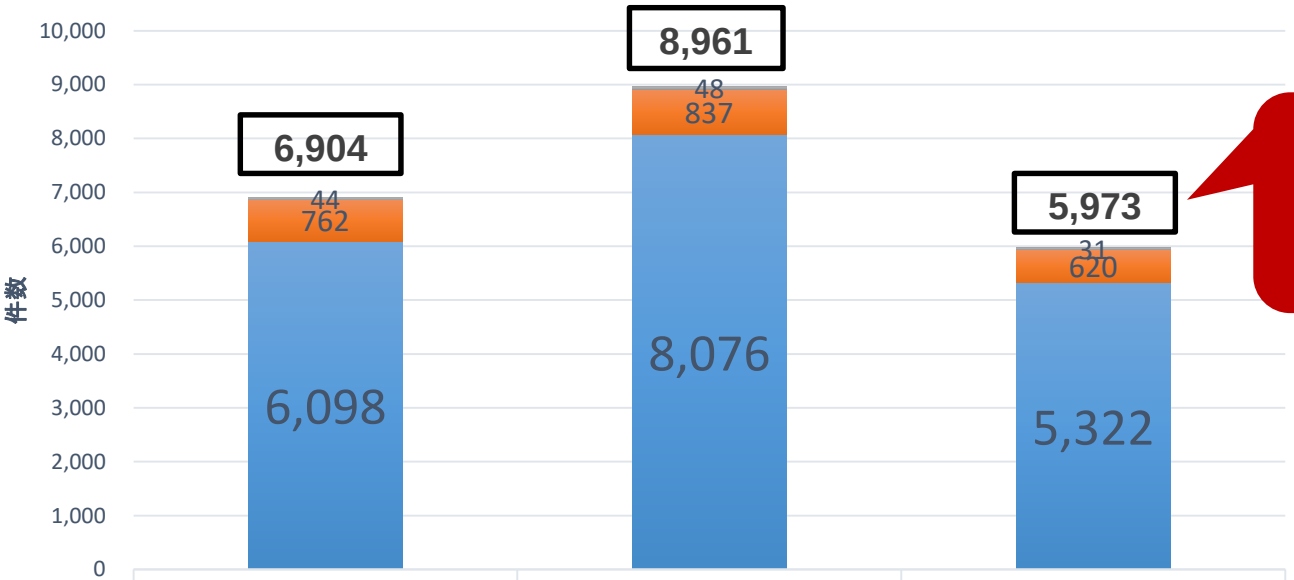


情報セキュリティ安心相談窓口とは

- 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。

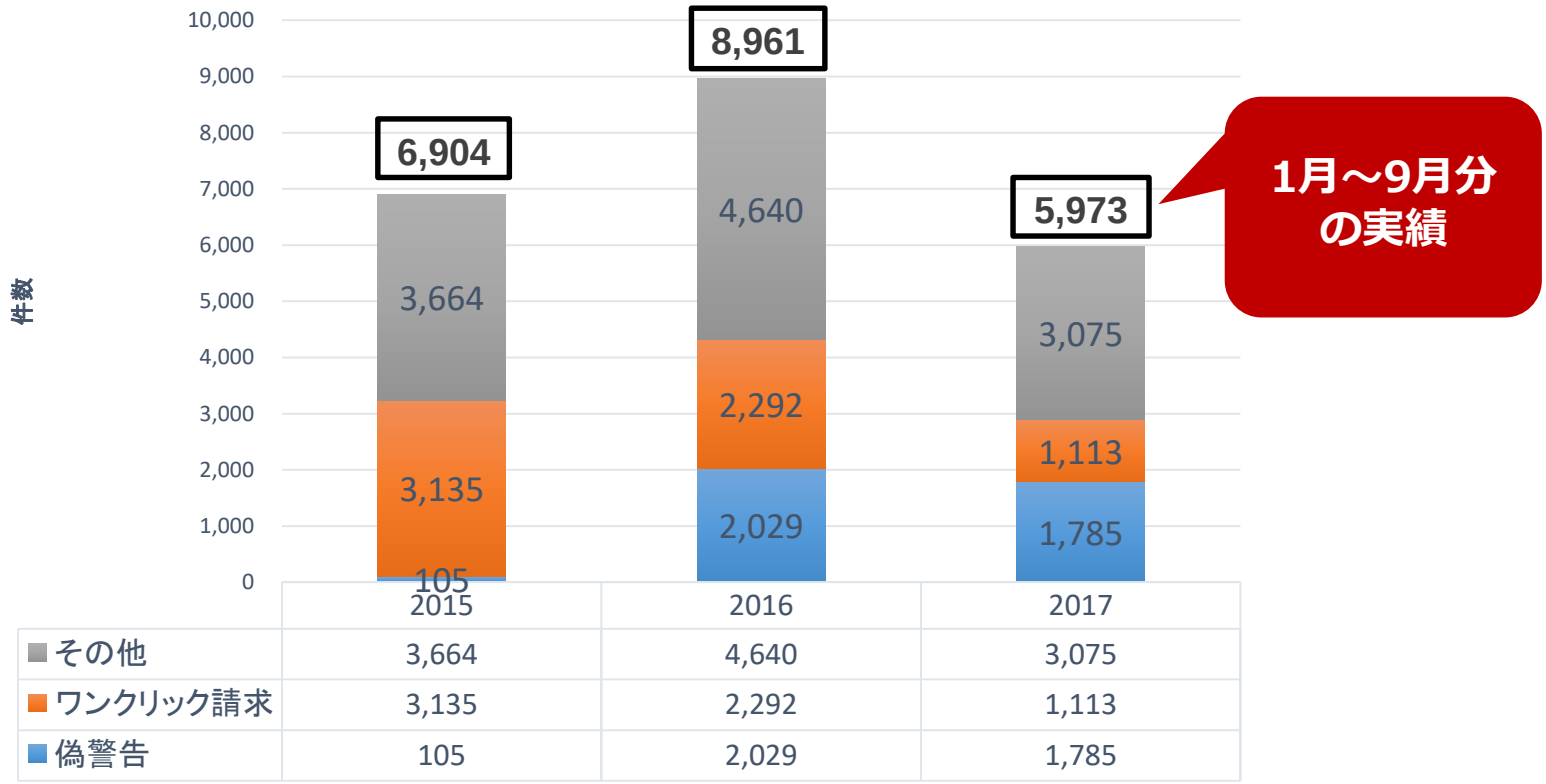
相談件数推移



	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



	2015	2016	2017
その他	3,664	4,640	3,075
ワンクリック請求	3,135	2,292	1,113
偽警告	105	2,029	1,785

- 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。

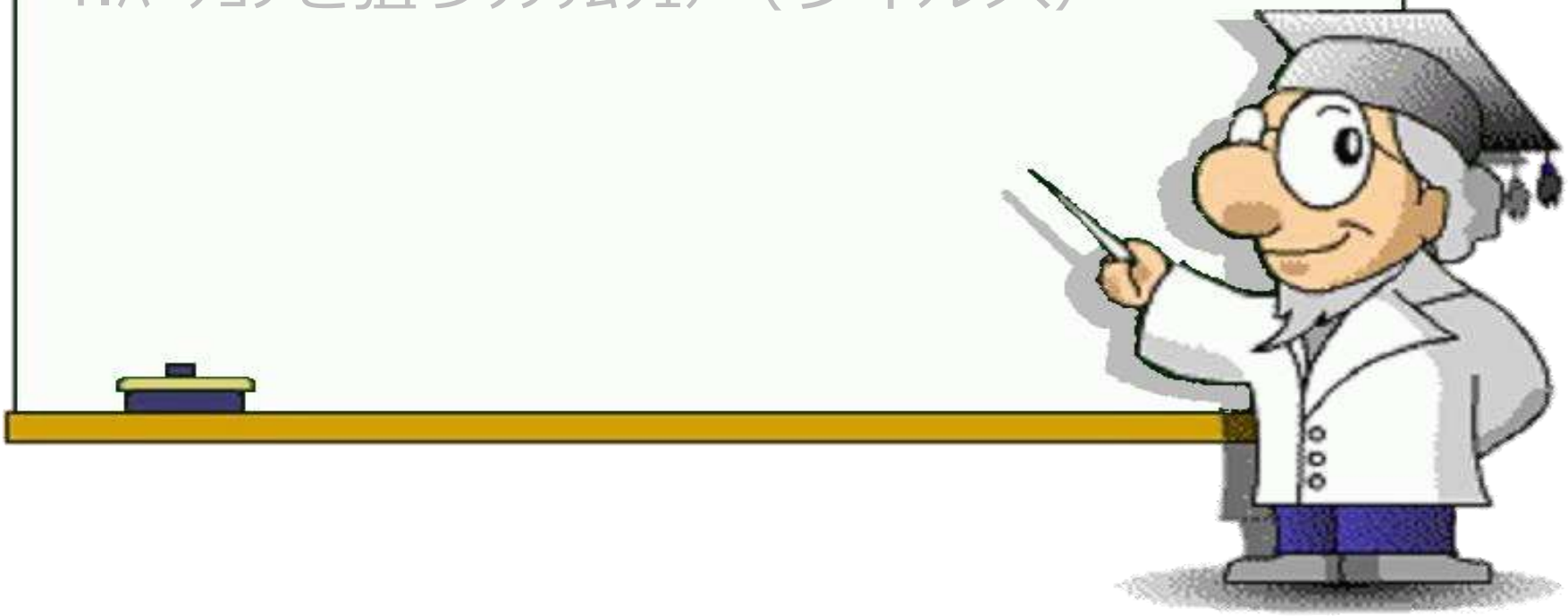
目次

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.ﾊﾟｿｺﾝを狙うﾗﾝｻﾑｳｪｱ（ウイルス）



スマートフォンを狙った手口

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。
今すぐ試してみて下さい！

□　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。
定期的に実行すれば安心ですね♪

* ==========* AI
◆編集・発行：便利アプリを紹介！APPマグ
◇配信停止・配信先の変更　http://●.net/●/
◆Copyright(C) 2011-2012, APPSマグ
◇本メールマガジンの著作権はAPPSマグに帰属します。,
　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！

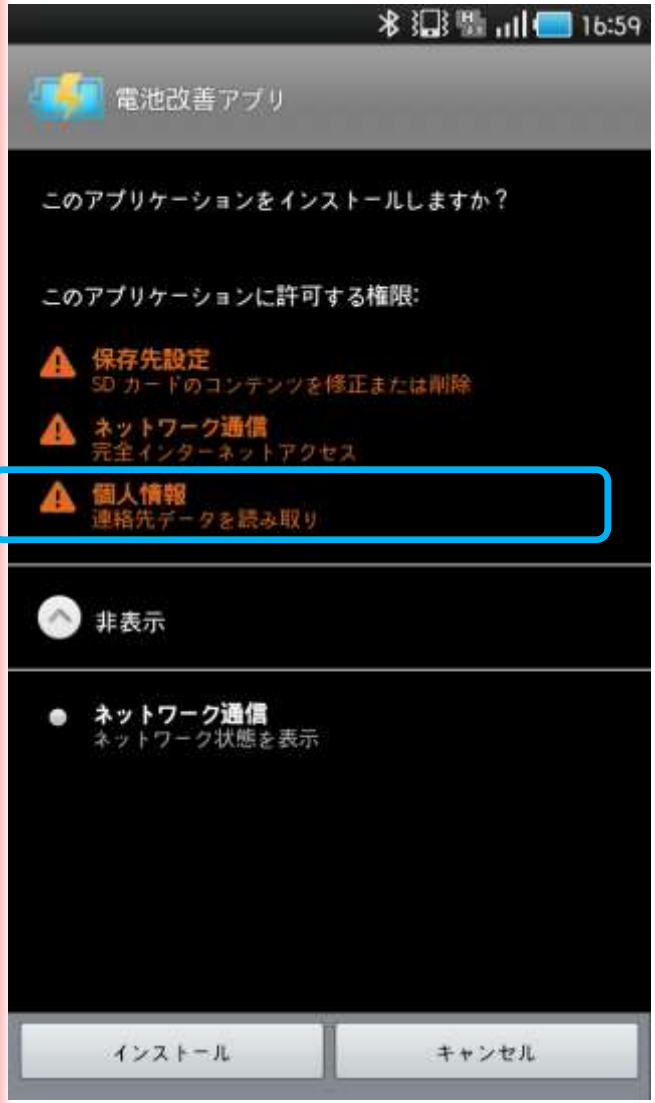
Facebookの某コミュニティに投稿されていた、不正アプリサイトへのリンクを含んだ投稿

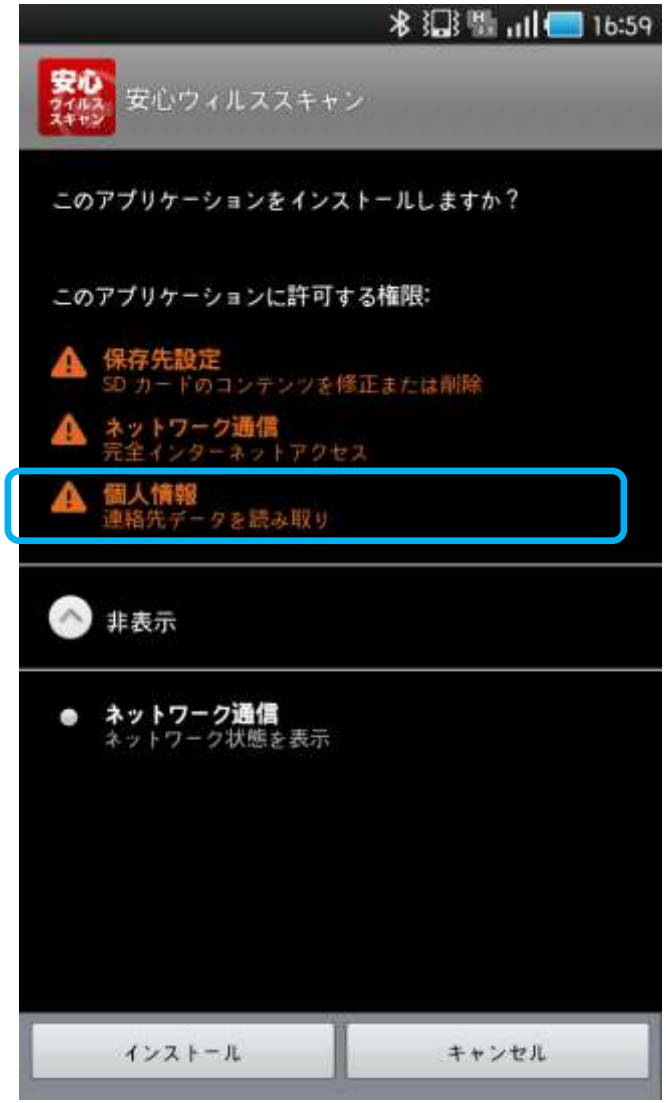
SNSやメールで不正アプリサイトへ誘導する事例（2012年9月） ※Androidの事例

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

アプリ初起動時、
権限初使用時

Android OSのバージョンによって表示のタイミングが異なる

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)

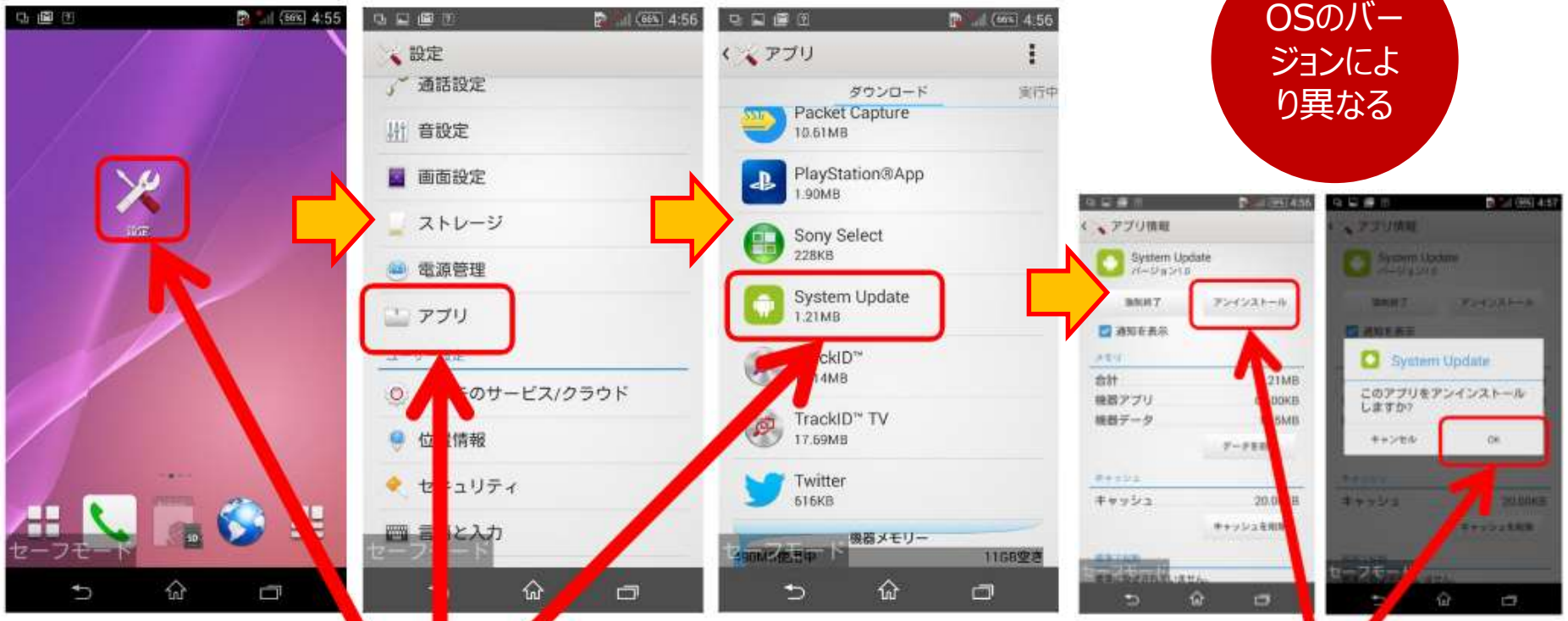
※Android端末での例

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



「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

管理

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

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！

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。同種のものは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！

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。

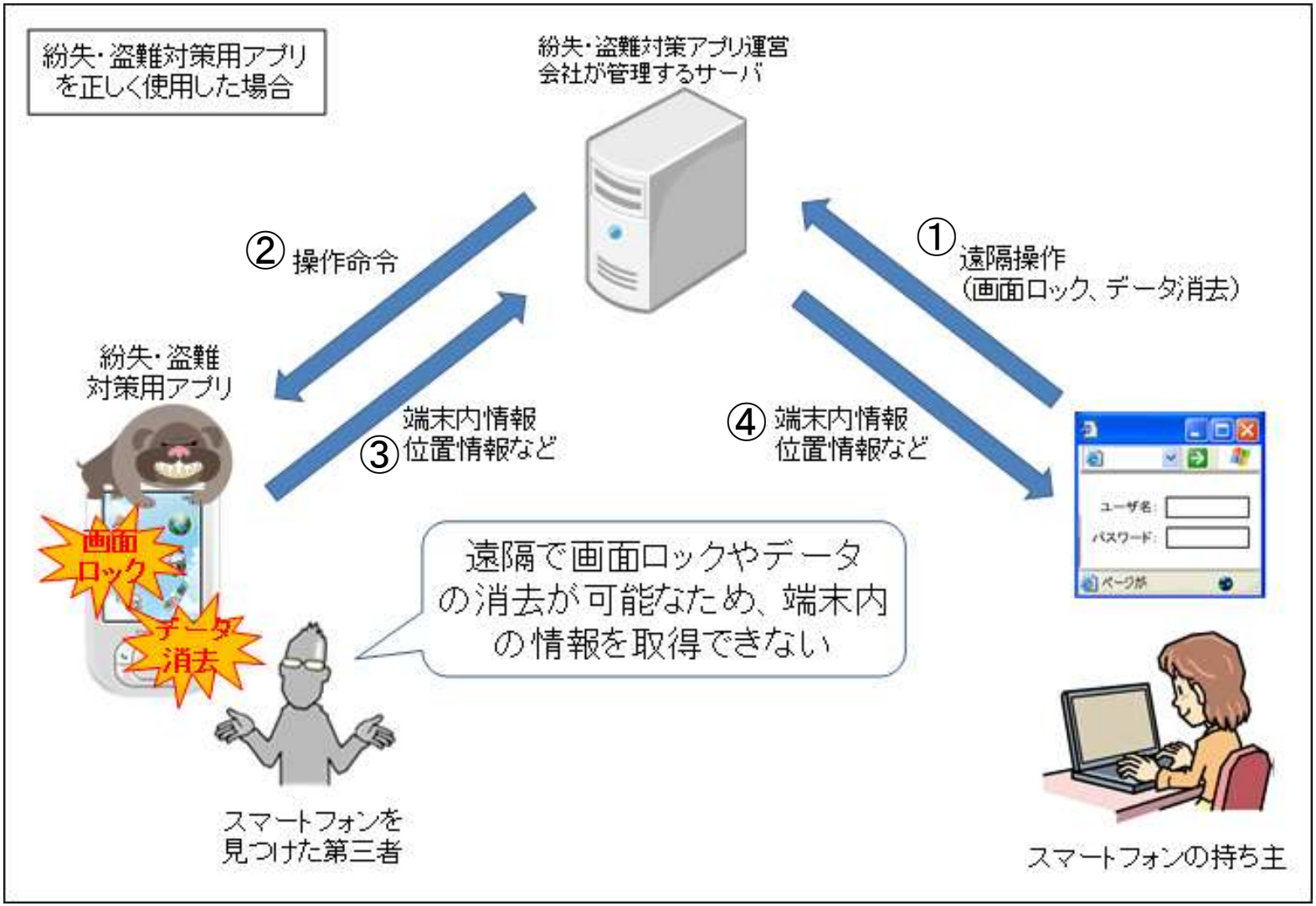
使用されたのは「ＴｒａｃｋＶｉｅｗ」というアプリで、音や動きに反応して撮影を始め、別のスマホでその動画が見られる。本来、自宅に残したペットを確認するためなどに使う。

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。

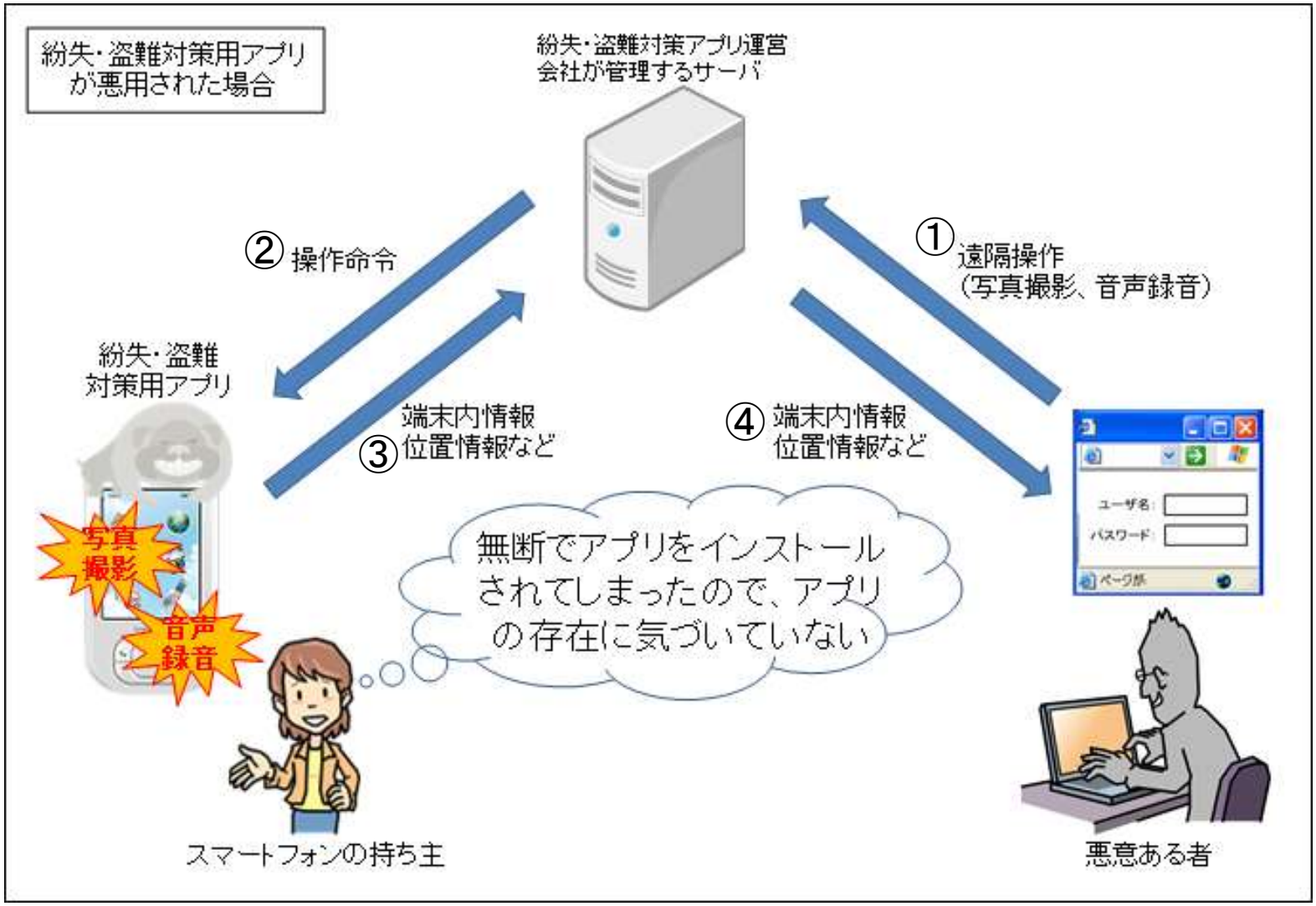
高梨容疑者は、女子大生が勤務中に部屋に侵入し、古いスマホを盗んでいたという。スマホが充電されていることを不審に思い、県警に相談。容疑者が映った動画がスマホに残っていたため発覚した。

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

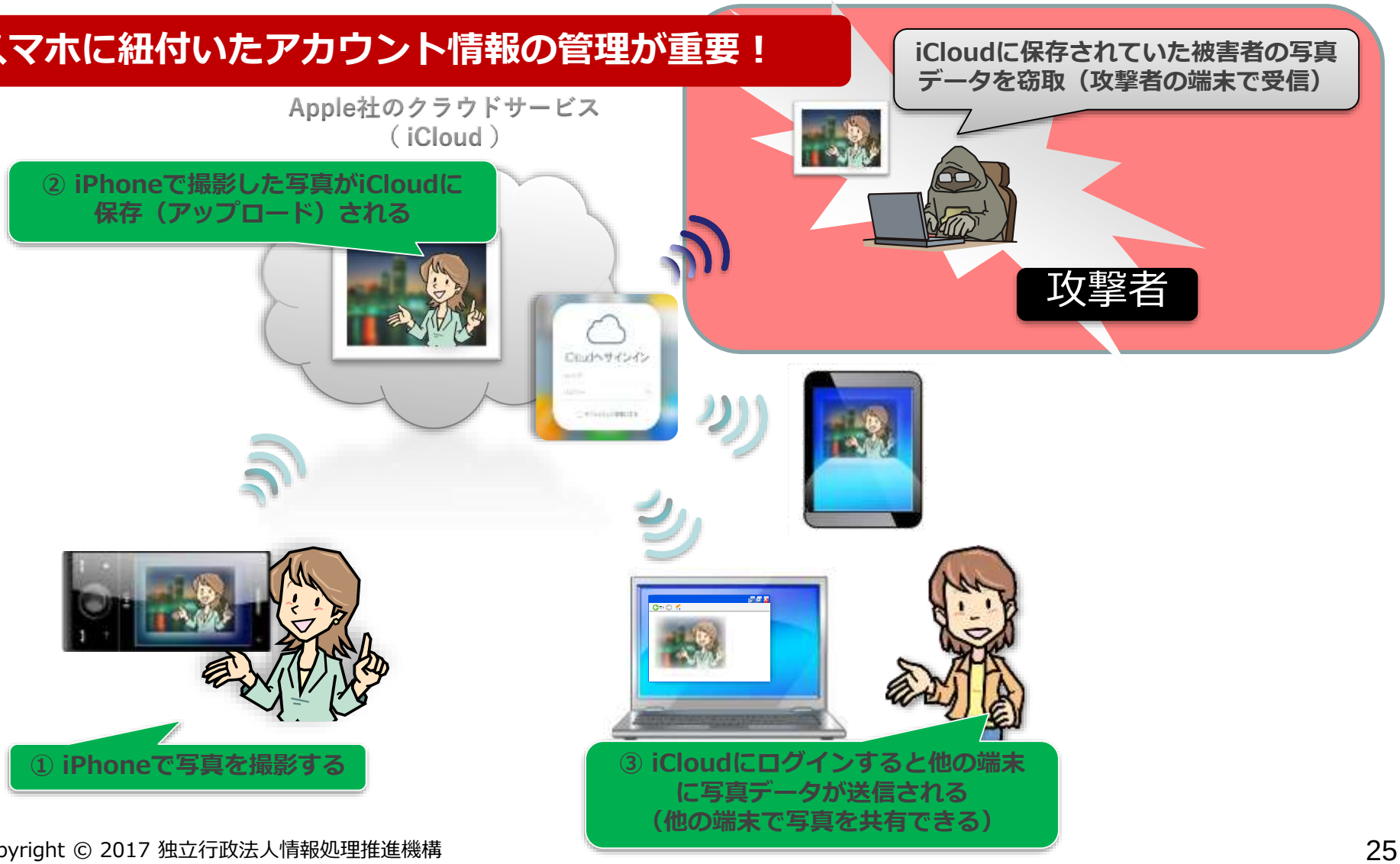
■不正アプリのインストールに注意する！

- 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か落ち着いて確認

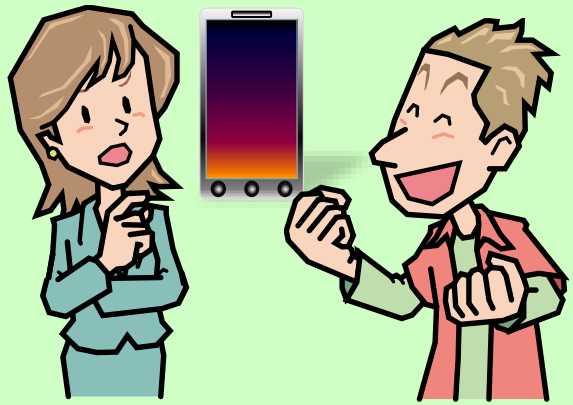
クラウド悪用のお話

クラウドに保存した情報が盗まれる！

スマホに紐付いたアカウント情報の管理が重要！



パスワードを教えてはいけません！！



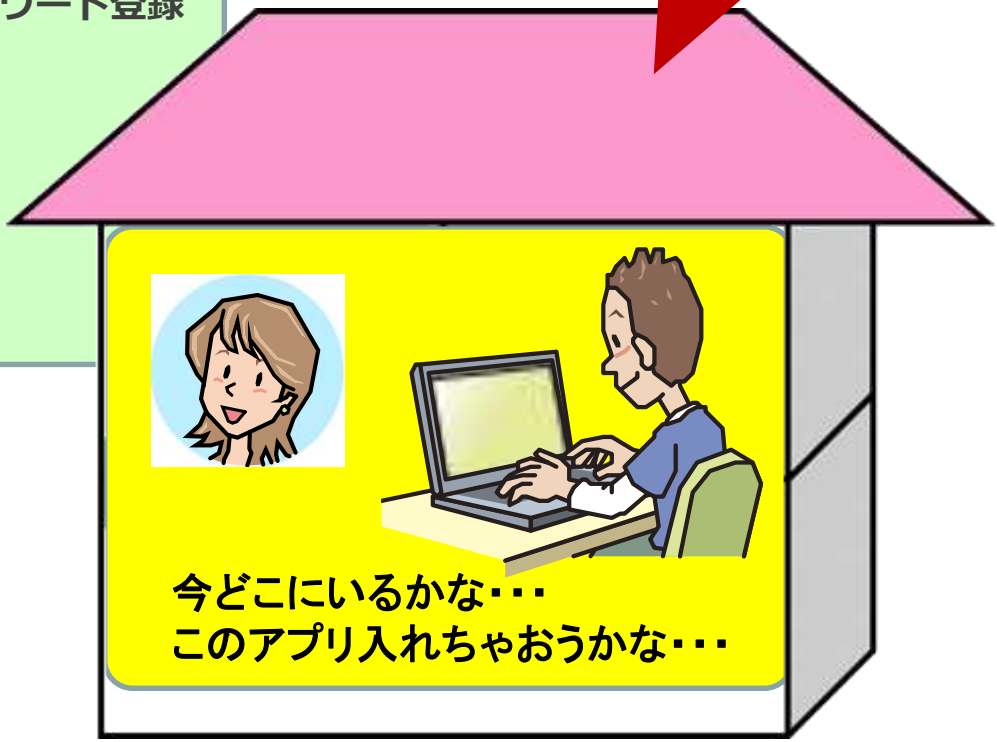
スマホよく
わかんな
～い・・

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

以下の管理に注意！！
・Googleアカウント
・Apple ID

現在地を知られる！
遠隔でアプリを入れられる！
(^ω^;)



クラウドでの不正アクセス事件！！

（2017年11月）

NHK NEWS WEB　2017年（平成29年）11月2日 木曜日　ニュースを検索

ニュース　動画　News Up　特集　スペシャルコンテン

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いた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。

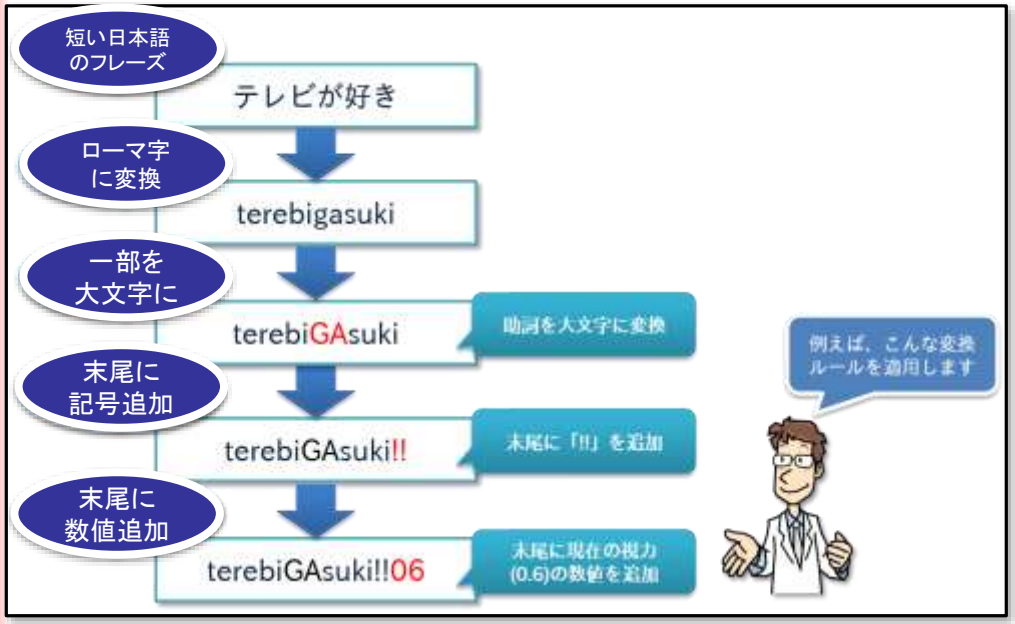
警察によりますと、ＳＮＳに公開された情報などからパスワードを割り出し、写真などを不正にのぞき見たうえ、自分のパソコンに保存していたということで、調べに対し「パスワードを破ることにやりがいを感じていた。他人のプライベート写真を見るのが楽しかった」などと供述しているということです。

SNSに公開された情報などからパスワードを割り出し

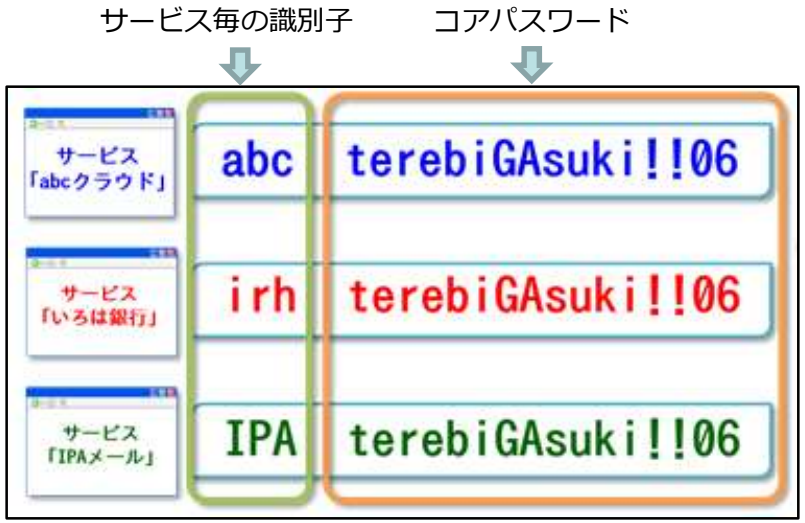
安全なパスワードの作成

「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

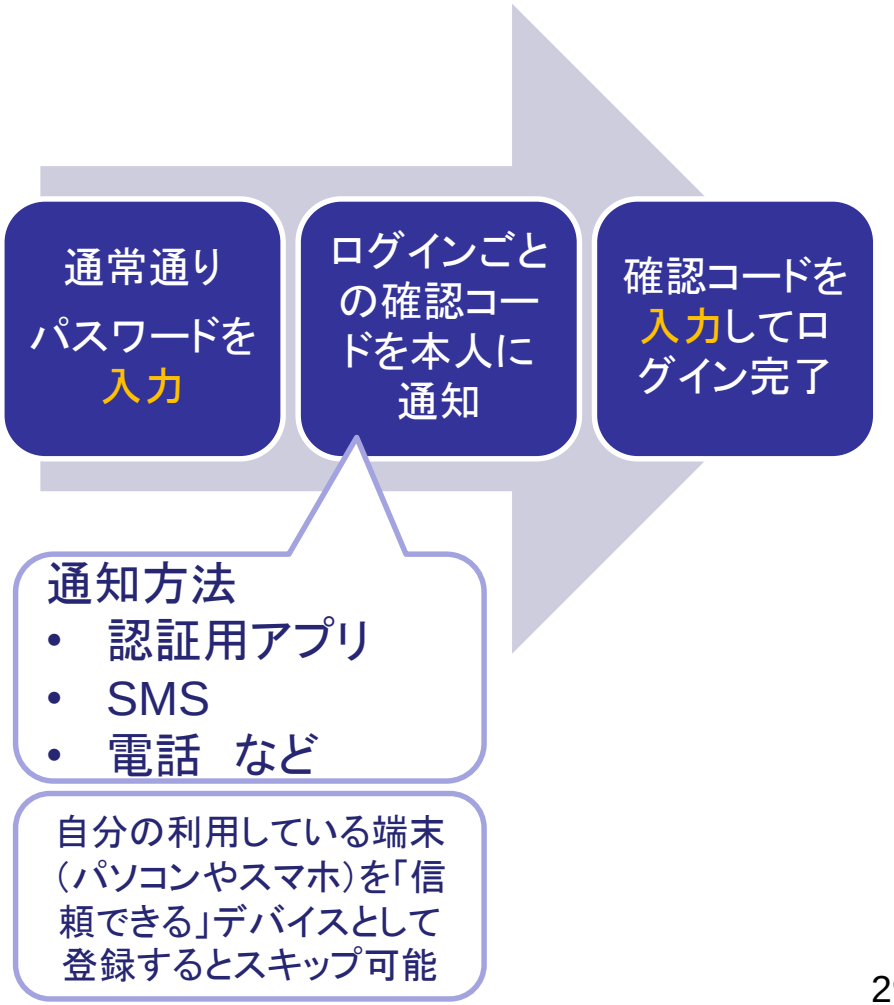


2.サービス毎に異なるパスワードの作成



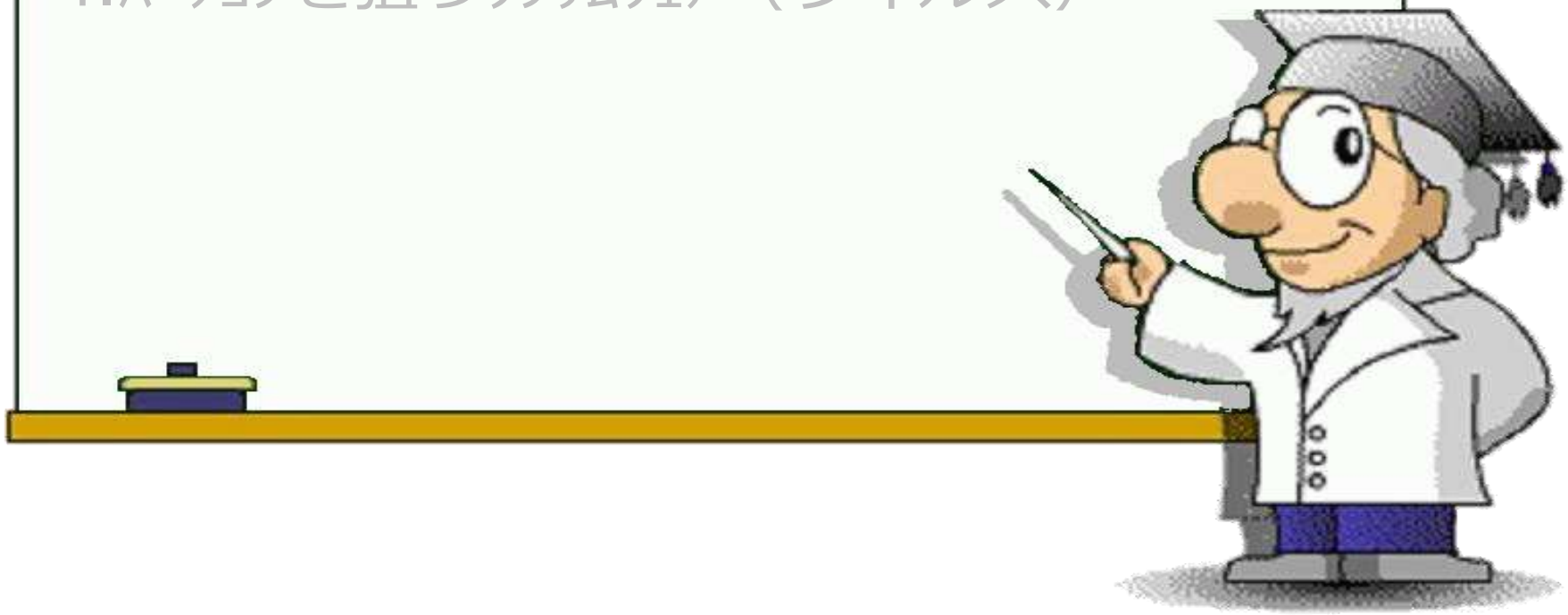
二段階認証（万が一、パスワードを破られても）

- 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.ﾊﾟ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

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

支払わない！！

電話しない！！

請求画面の消し方

■ 症状
- 画面を閉じても、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

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

■ 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

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）

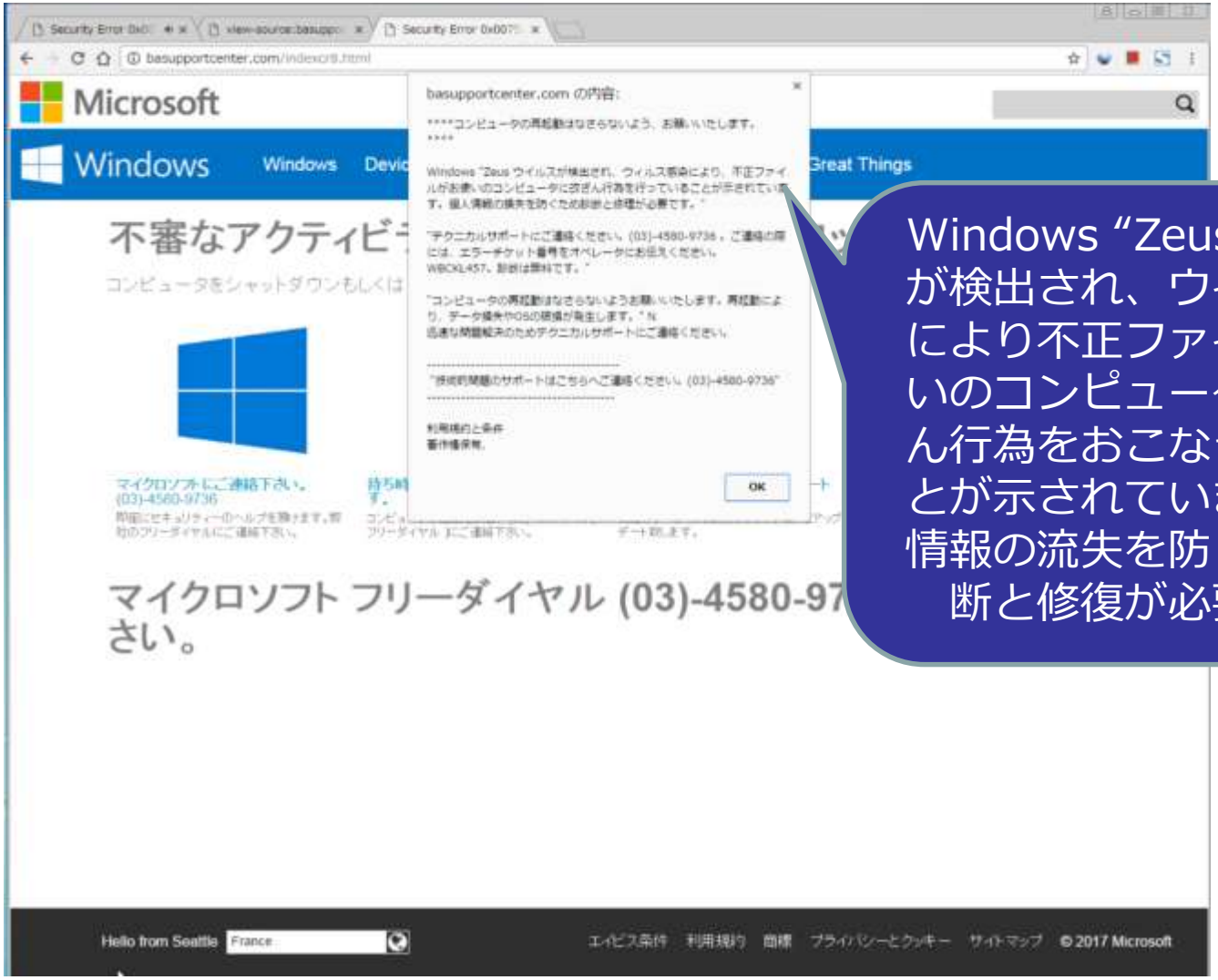
詐欺的手法の数々・・・

・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

**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**

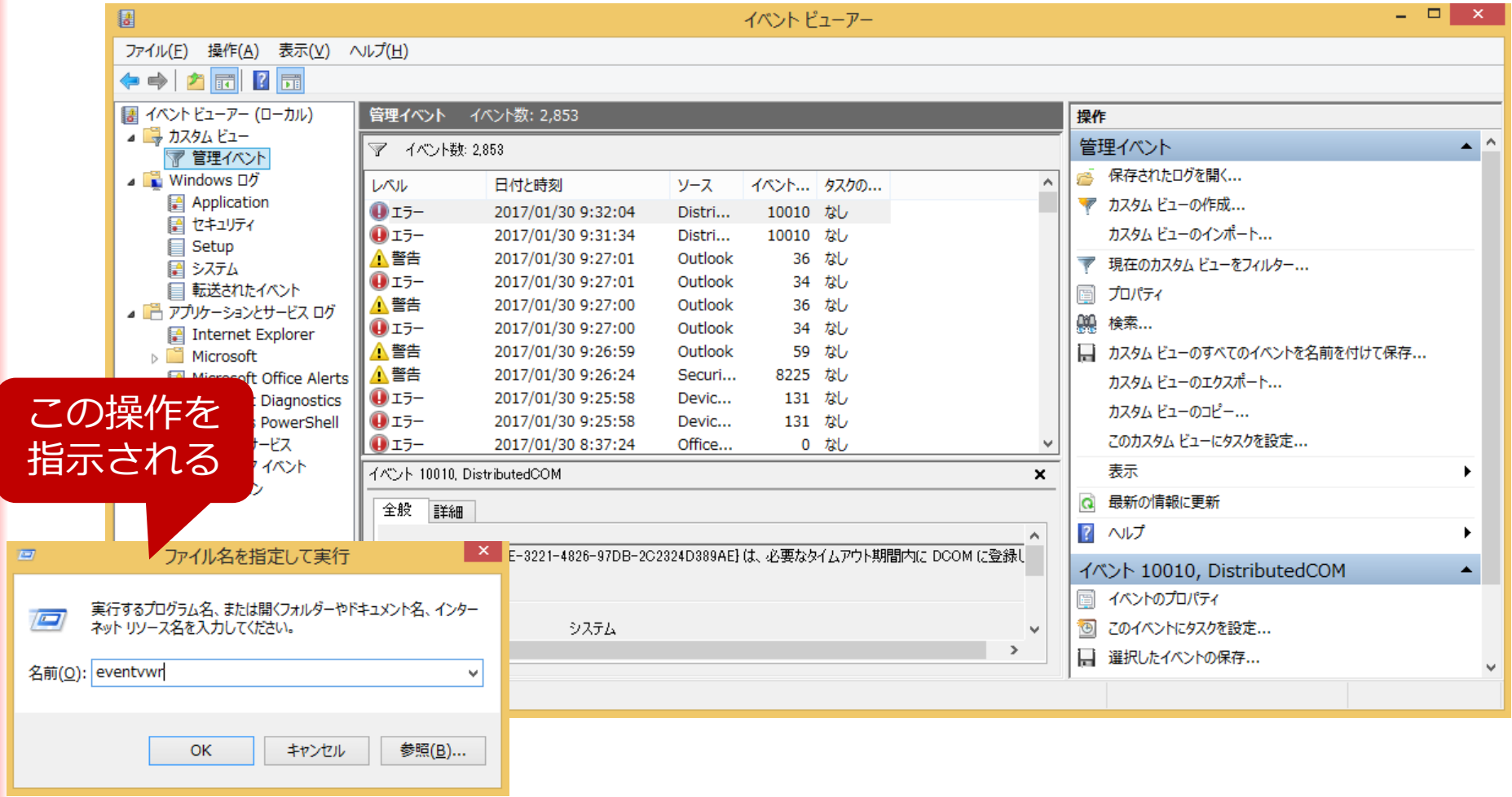
「偽警告」サイト→遠隔操作事例（2017年1月）



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ー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。

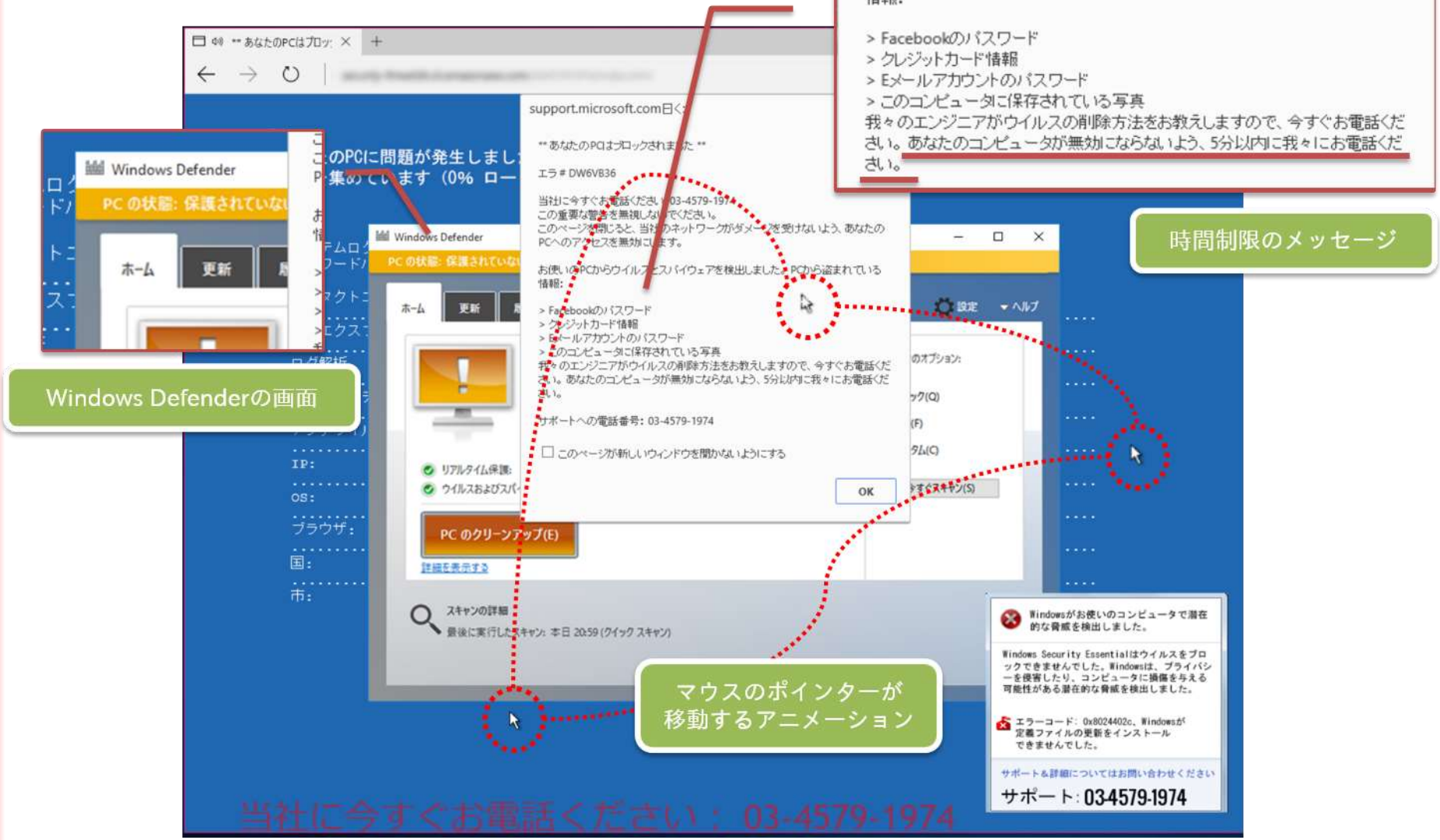
「偽警告」サイト→遠隔操作事例（2017年1月）

（ファイル名を指定して実行）で「eventvwr」を実行した結果



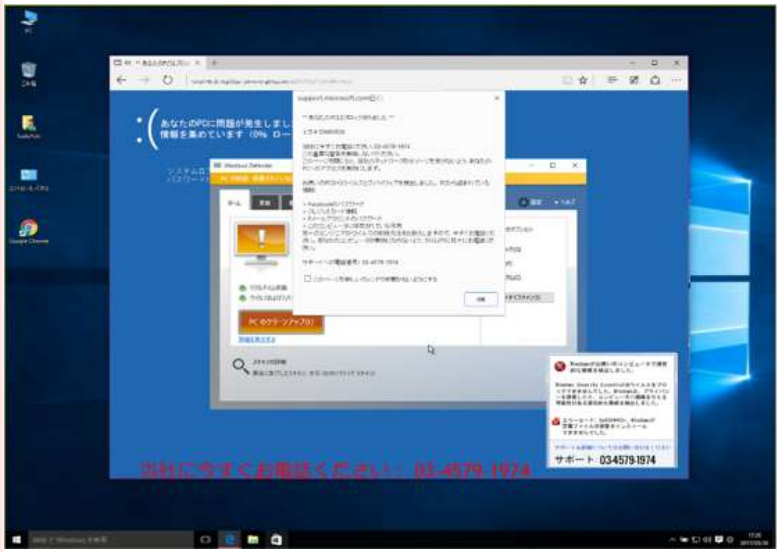
新手の偽警告事例（2017年3月）

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

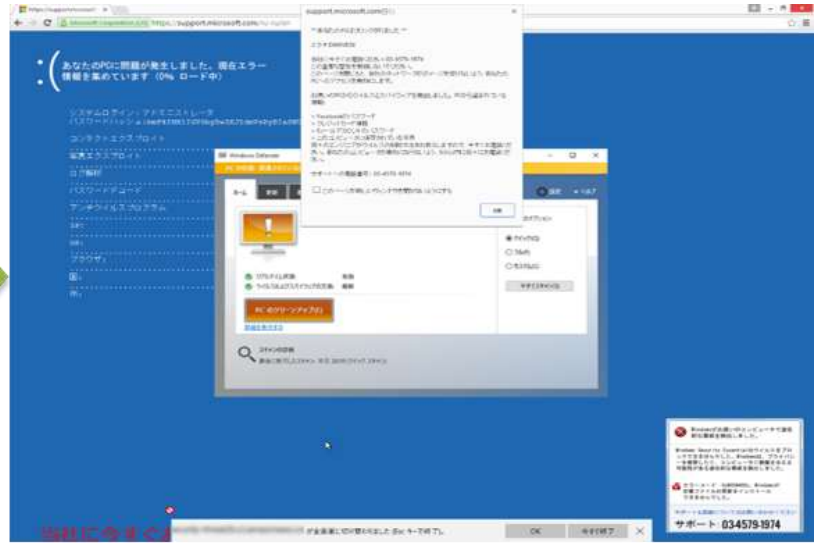


新手の偽警告事例（2017年3月）

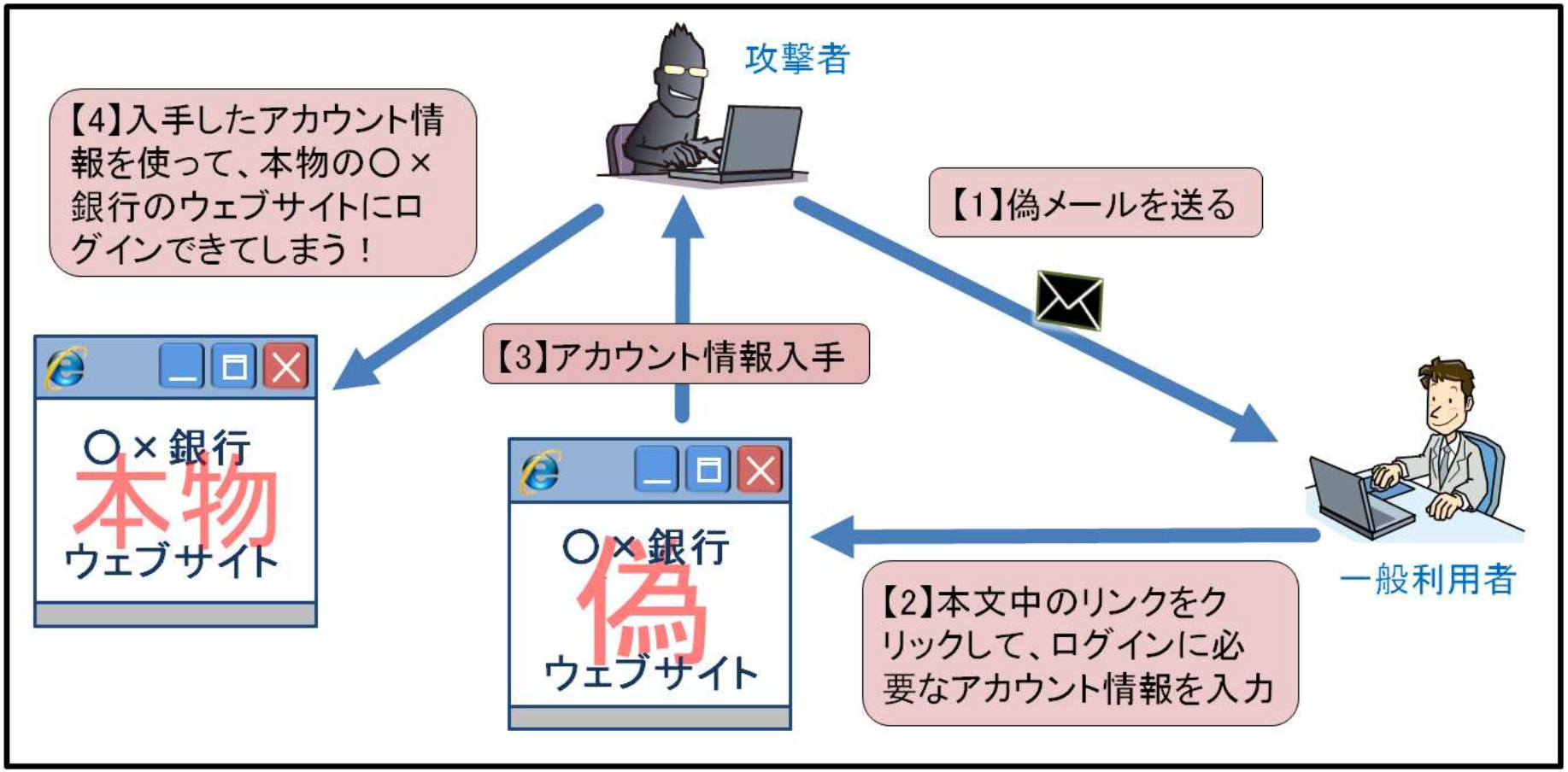
ブラウザを全画面表示にして本来のデスクトップを隠す



全画面表示

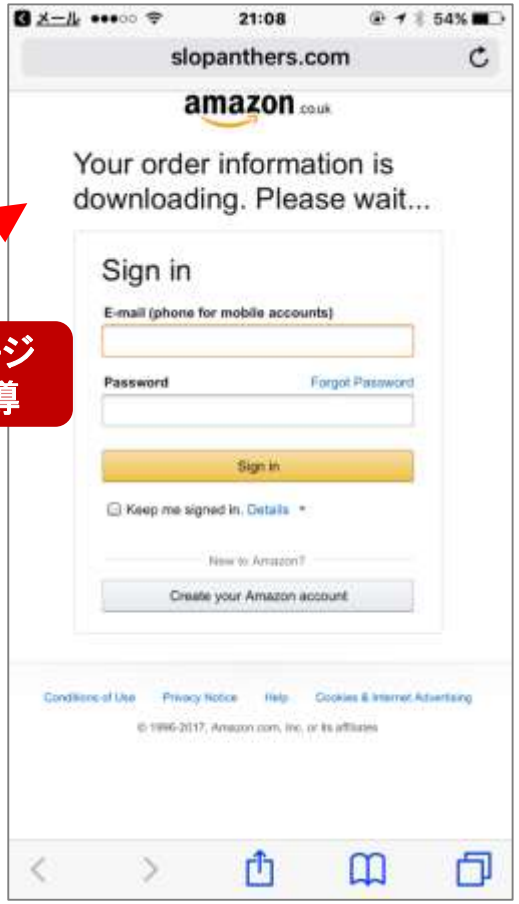


フィッシングの基本的手口



Amazonを狙ったフィッシング事例（2017年）

偽ページへ誘導



Appleを狙ったフィッシング事例（2017年）

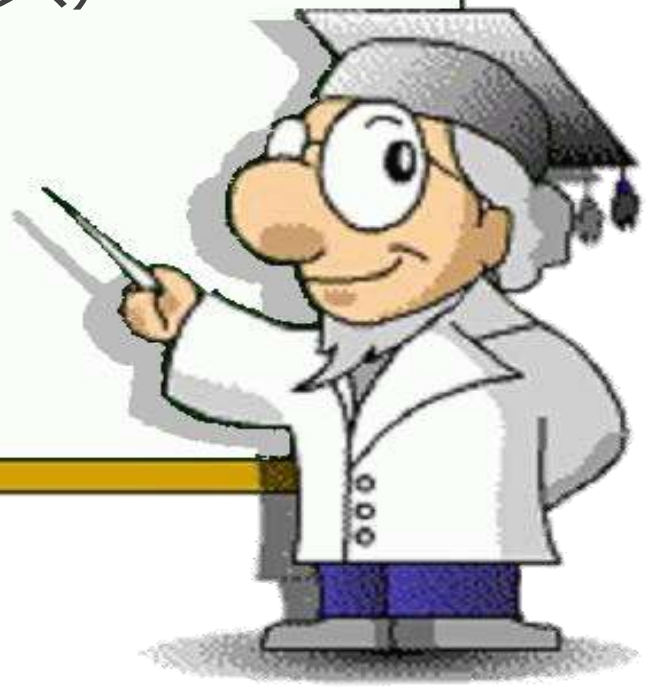
数種類の違う
パターンがある

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.ﾊﾟ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　**ファイル暗号化型**
- 端末をロックされ、操作できなくなる　**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

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閲覧することで感染
・不正広告を閲覧することで感染
・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閲覧することで感染
- 不正広告を閲覧することで感染
- ダウンロードしたファイルを開くことで感染

ドライブ・バイ・ダウンロード攻撃

メールからの感染

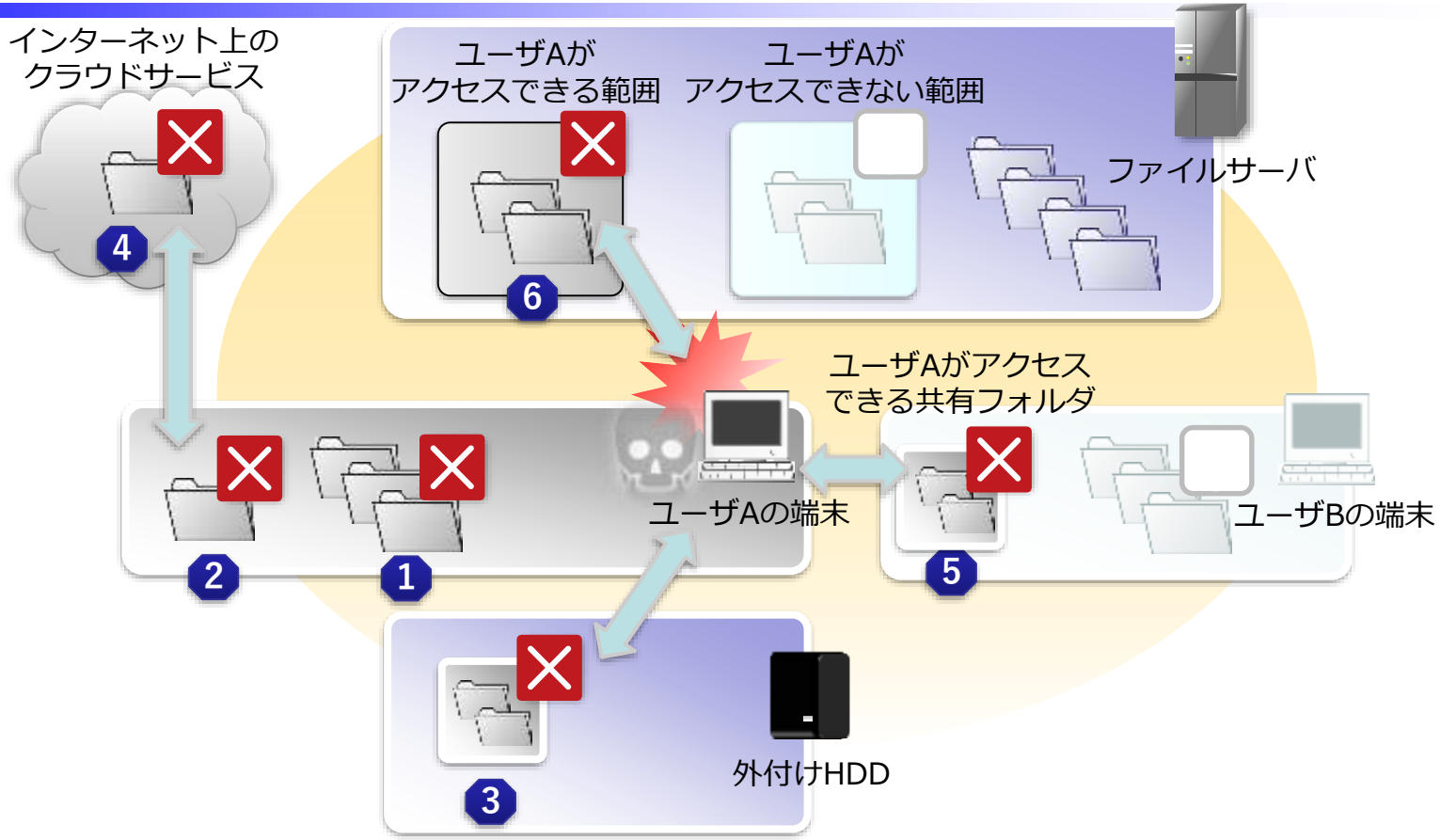
- メール本文に記載されたURLからアクセスすることで感染
- メールの添付ファイルを開くことで感染

ドライブ・バイ・ダウンロード攻撃

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

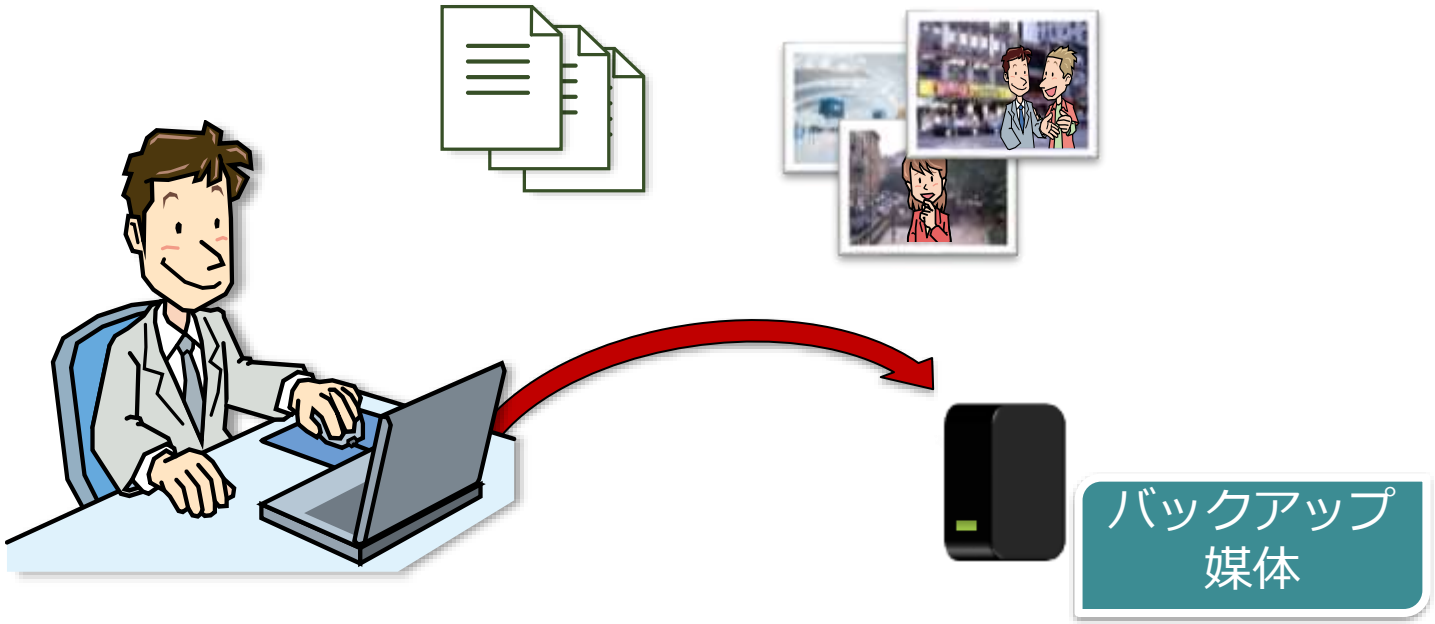


1. 感染端末内に保存されているファイル
2. 感染端末内のクラウドと同期するフォルダ内のファイル
3. 感染端末に接続されている外付けHDD内のファイル
4. ファイル暗号化後の同期によるクラウド内のファイル(上書き)
5. 感染端末と共有しているフォルダ内のファイル
6. 感染端末がアクセス可能な場所に保存されているファイル

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

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）

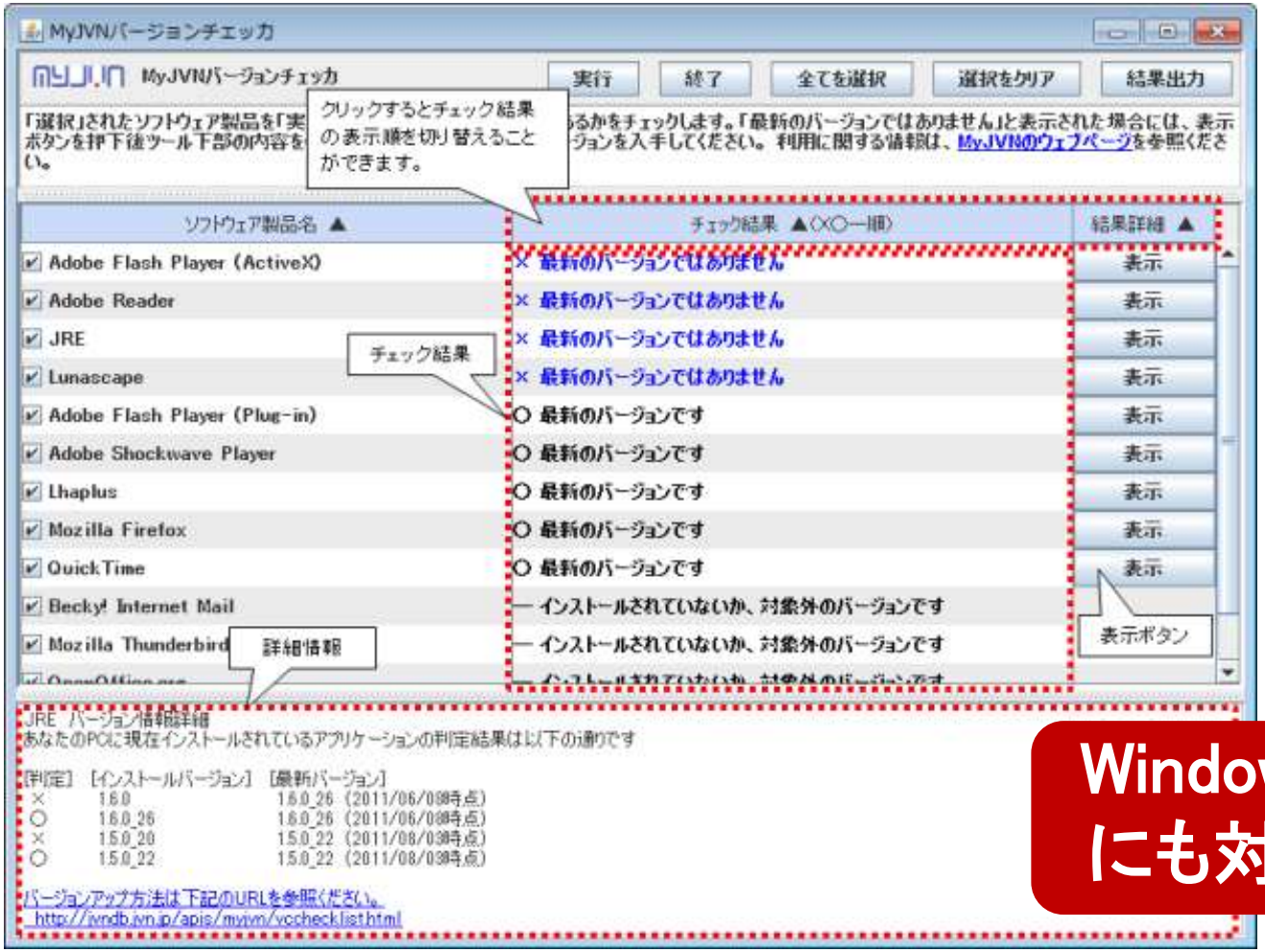
ウイルス対策ソフトの導入と適切な運用

- 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
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

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

IPA　胸キュン　検索

ITパスポート試験

IPA

「ｉパス」は、ITを利活用する

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。

公式キャラクター

上峰 亜衣（うえみね あい）

試験の主なメリット

戦略、財務等幅広い出題	セキュリティを積極出題	エントリーシート等活用
▼	▼	▼
仕事に役立つ	**セキュリティに強くなる**	**就職に役立つ**

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