IPA Better Life with IT

情報セキュリティ10大脅威2017

～1章 情報セキュリティ対策の基本　スマートフォン編～

～職場に迫る脅威！　家庭に迫る脅威！？
急がば回れの心構えでセキュリティ対策を～

独立行政法人情報処理推進機構（IPA）
技術本部 セキュリティセンター
2017年4月

情報セキュリティ10大脅威 2017

- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」の投票により、
    情報システムを取巻く脅威を順位付けして解説

情報セキュリティ10大脅威 2017

- 章構成
  - 1章.情報セキュリティ対策の基本 スマートフォン編
    - スマートフォンにおけるセキュリティ対策の基本を解説
  - 2章.情報セキュリティ10大脅威 2017
    - 脅威の概要と対策について解説
    - 個人と組織の2つの立場で解説
  - 3章.注目すべき脅威や懸念
    - 知っておくべき脅威や懸念を解説

1章. 情報セキュリティ対策の基本
スマートフォン編

スマートフォン利用に伴う考慮点　その1

IPA

従来の携帯電話端末（通称、ガラケー）とスマートフォンは異なる点がある

- ウェブサイト閲覧の仕組み
  - ガラケー：機能が少ないコンパクトブラウザを利用
  - スマートフォン：PCとほぼ同じ機能のフルブラウザを利用
- アプリの機能
  - ガラケー：機能制限有
  - スマートフォン：自由度が高く高機能
- 更新プログラムの提供方針
  - ガラケー：バグに対する対策
  - スマートフォン：脆弱性に対する対策も含まれる

ガラケーと違いスマートフォンは適切なセキュリティ対策が必要

スマートフォン利用に伴う考慮点　その2

スマートフォンは使い方により、利用上の危険度が変わる

- スマートフォンのプリインストールのソフトのみ利用
  - プリインストールのアプリに対する脅威
  - スマートフォンのOSに対する脅威
    - 危険度低
- 公式マーケットやストアからアプリをインストール
  - 追加でインストールした公式マーケットのアプリに対する脅威
    - 危険度中
- 公式マーケットやストア以外からアプリをインストール
  - 非公式なアプリに対する脅威
    - 危険度高

スマートフォン利用に伴う考慮点　その2

スマートフォンは使い方により、利用上の危険度が変わる

- 危険度低：スマートフォンのプリインストールのソフトのみ利用
  - アプリケーションのバージョンアップ
  - OSのバージョンアップ
- 危険度中：公式マーケットやストアからアプリをインストール
  - アプリの機能や権限を確認
  - セキュリティソフトの導入
- 危険度高：公式マーケットやストア以外からアプリをインストール
  - 上記の使い方に加えインストールするアプリをしっかりと管理

利用方法に応じたセキュリティ対策が必要

スマートフォン利用に伴う考慮点　その3

スマートフォンならではの使い方があり、対策も存在

- ウェブサービスの利用方法
  - 個別アプリを通してウェブサービスを利用
    （ガラケーの場合はブラウザを使ってウェブサービスを利用）
    - インストールされているアプリの管理が必要
      - アプリのアップデート
- スマートフォン独自の機能が存在
  - GPS等スマートフォンに良くある機能の活用
    （ガラケーの場合は、機能が存在しない）
      - 遠隔ロック・データ消去
      - 端末位置の探索

スマートフォンならではのセキュリティ対策を活用

スマートフォン利用に伴う考慮点　その4

スマートフォンは、機種（Android端末、iPhone）や提供形態（SIMの利用の有無）が複数存在

	Android端末			iPhone	
	SIM ロック版	SIM フリー版	Android One	SIM ロック版	SIM フリー版
OS開発元	端末メーカー（Google製Androidをカスタマイズ）		Google	Apple	
OSの更新用プログラムの提供者	携帯電話通信事業者	端末メーカー	販売経路に依存		
アプリやその更新用プログラムの配布場所、審査方法	・Google Play（Google） 比較的緩やかな審査 ・各携帯電話通信事業者の公式マーケット Google Playの審査に加え、各携帯電話通信事業者の観点で選定 ・その他の配布場所 配布場所に依存			・App Store（Apple） 厳格な審査	

スマートフォンの機種や提供形態によりOS開発元や更新用プログラムの提供者、アプリの配布場所等が異なる

情報セキュリティ対策の基本　スマートフォン編

ガラケーと違いスマートフォンは、セキュリティ対策が必要

攻撃の手口	情報セキュリティ対策の基本
不正アプリ	信頼できるサイトからインストール
	アプリに許可する権限の確認
誘導（罠にはめる）	脅威や手口を知る
盗難・紛失	認証の強化・データの暗号化・バックアップ
盗聴	公衆無線LANの利用はリスクを理解
不正ログイン	パスワードを使い回さない
OS・アプリの脆弱性	OS・アプリの更新
ウイルス感染	セキュリティソフトの導入

付録：情報セキュリティ船中八策
スマートフォン編

本資料に関する詳細な内容は

- 以下のページのPDF資料をご覧ください。

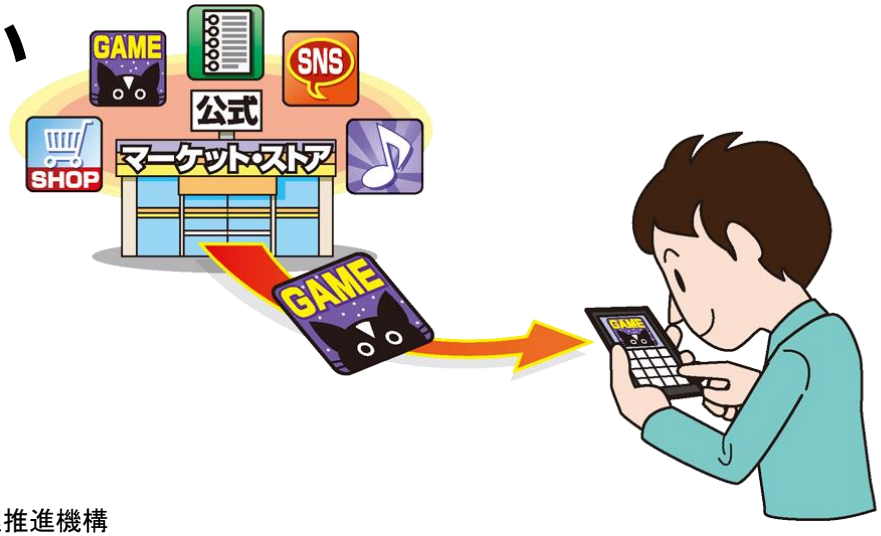
情報セキュリティ10大脅威 2017
https://www.ipa.go.jp/security/vuln/10threats2017.html

信頼できるサイトからインストール

- 不正アプリの存在に注意
- 不正アプリをインストールするとウイルスに感染する恐れ

【対策】

- アプリの公式マーケットから入手
- 信頼できるマーケット（サイト）以外からはアプリをインストールしない

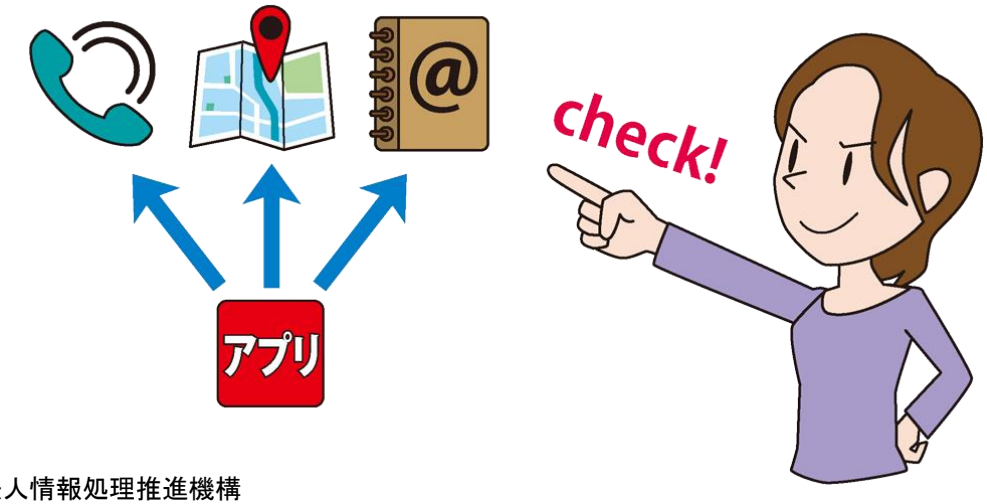


アプリに許可する権限の確認

- 不正アプリの存在に注意
- 不正アプリをインストールするとウイルスに感染する恐れ

【対策】

- アプリ起動時のアクセス権限の確認
- アプリ連携時のアクセス権限の確認も必要



脅威や手口を知る

- スマートフォンの利用者を狙った詐欺行為に注意
- スマートフォンの特性を悪用した巧妙な手口も
  - シャッター音を鳴らして撮影されたように偽装
  - 電話をかけさせようと発信ボタンを何度も表示

【対策】

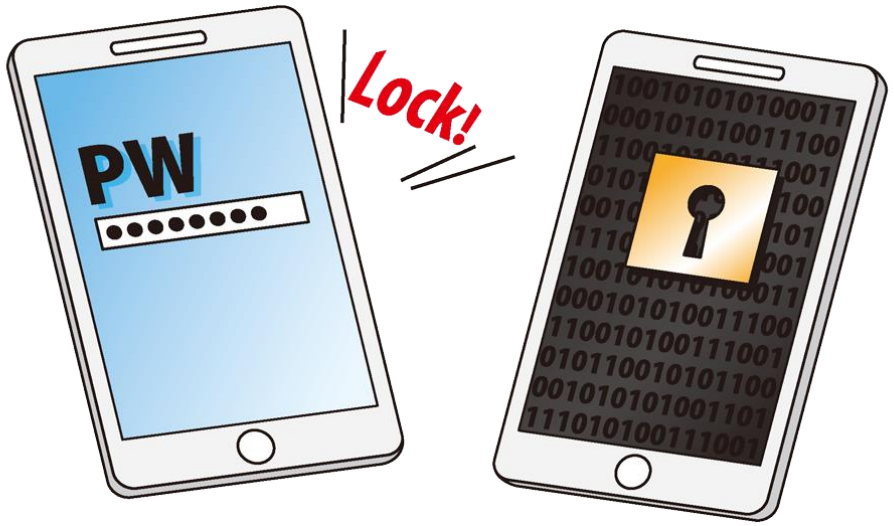
- 報道やセキュリティ関連機関の注意喚起等の情報源からセキュリティに関する脅威や犯罪の手口を情報収集

認証の強化・データ暗号化・バックアップ

- スマートフォンには紛失や盗難のリスクがある
- 自分の情報だけではなく友人や家族の情報も漏えいする恐れ

【対策】

- スマートフォンの認証強化
- データの暗号化
- 遠隔ロック機能の活用
- データのバックアップ

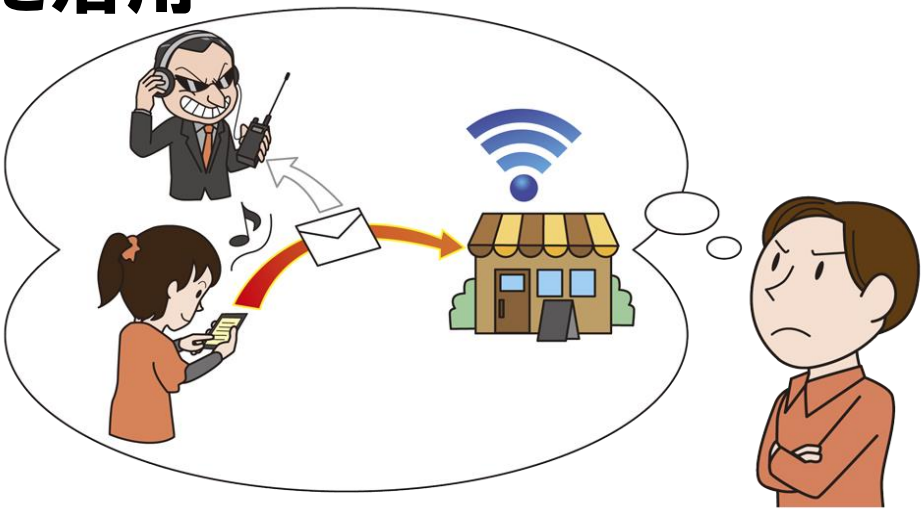


公衆無線LANの利用はリスクを理解

- 公衆無線LANの利用は盗聴のリスクあり
- 通信しているデータが漏えいする恐れ
- 悪意ある(偽の)アクセスポイントの存在にも注意

【対策】

- 通信を暗号化する仕組みを活用
  - HTTPS通信
  - VPNサービス
- 通信する情報を限定

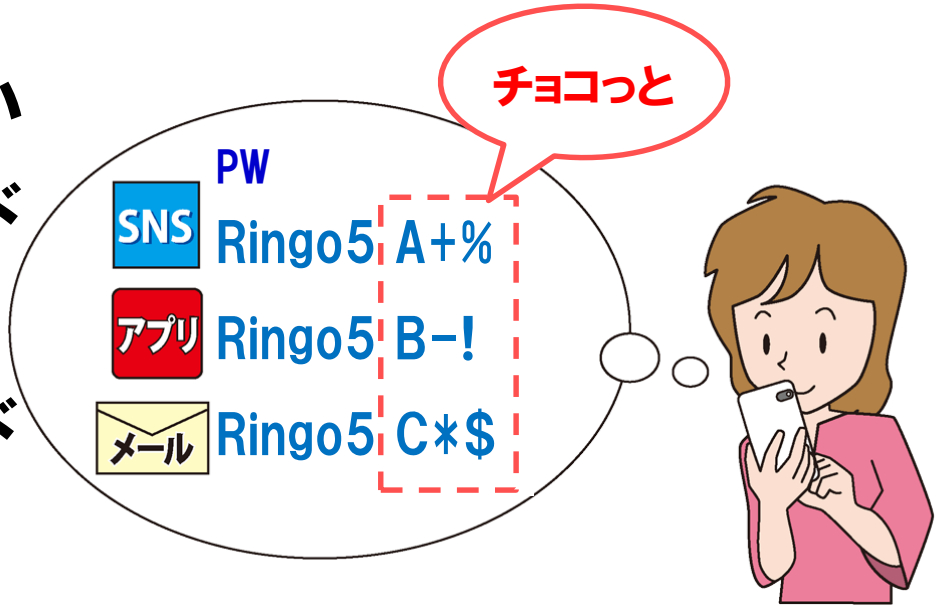


パスワードを使い回さない

- パスワードの使いまわしは危険
- 漏えいすると同じパスワードを使っている別のサービスでも不正ログインの恐れ

【対策】

- パスワードは使い回さない
- 推測されやすいパスワードは使わない
- チョコっとプラスパスワード
- 多要素認証の活用

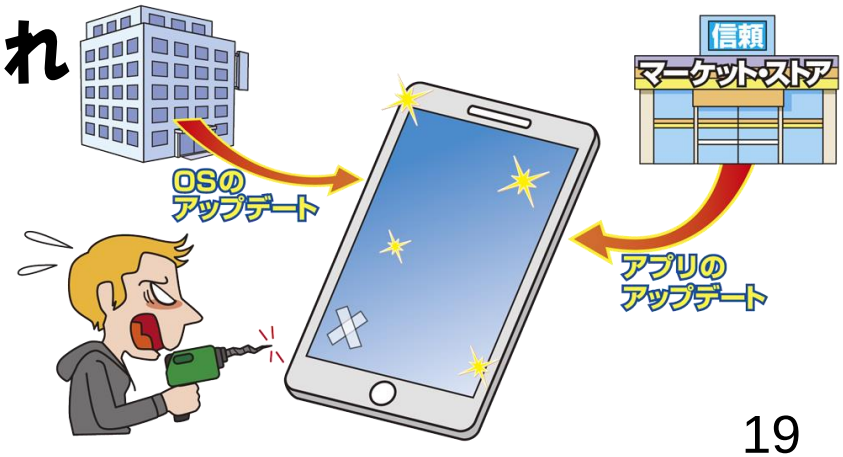


OS・アプリの更新

- スマートフォンのOSやアプリに脆弱性が存在するリスクがある
- 脆弱性を悪用されると情報窃取や遠隔操作の恐れ

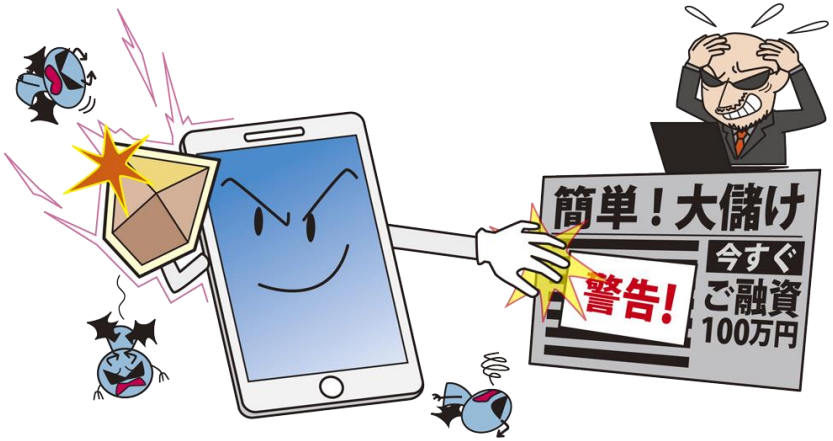
【対策】

- マイナーアップデート（セキュリティ機能の改善等）の実施
- メジャーアップデート（機能・操作性の向上等）の検討
  - アプリが動作しなくなる恐れ
  - 設定初期化の恐れ
- 更新プログラムが提供されない場合も



セキュリティソフトの導入

- 不正アプリの存在に注意
- 不正アプリをインストールするとウイルスに感染する恐れ
- 詐欺サイトにアクセスし、情報を入力することでクレジットカード情報等の機微な情報を窃取される恐れも



【対策】

- セキュリティソフトの導入
  - 不正アプリや詐欺サイトへのアクセスの抑止
- 携帯電話通信事業者から提供されるセキュリティ対策サービスの活用