スマートフォンアプリケーションに求められるセキュリティ対策

2012年10月26日

株式会社ブロードバンドセキュリティ

Copyright©2012 BroadBand Security, Inc.

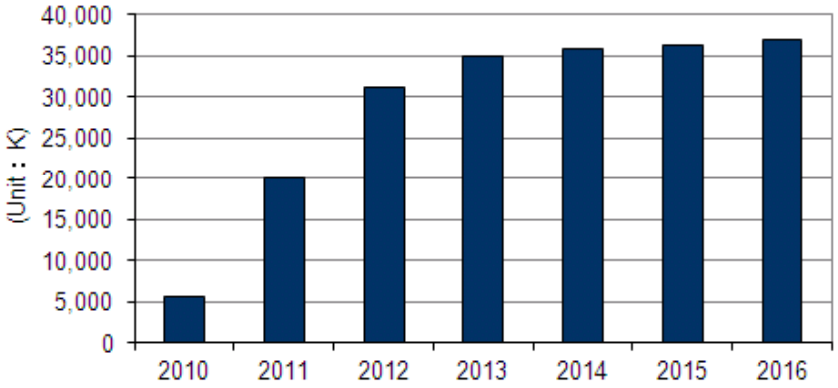
スマートフォン/タブレット端末を取り巻く現状

BBSec

スマートフォン/タブレット端末 ～普及率およびネット利用の増加～

スマートフォンの普及率は急速に増加

【国内におけるスマートフォン普及率予測】



（出典：IDC Japan）

海外と比較すると、日本におけるシェアはまだまだだが各キャリアから次々と新機種・新製品が発表されており今後さらに普及率は増加する見込み。

2012年第2四半期に
世界中で販売された
スマートフォンは**1億5,400万台**
（IDC調べ）

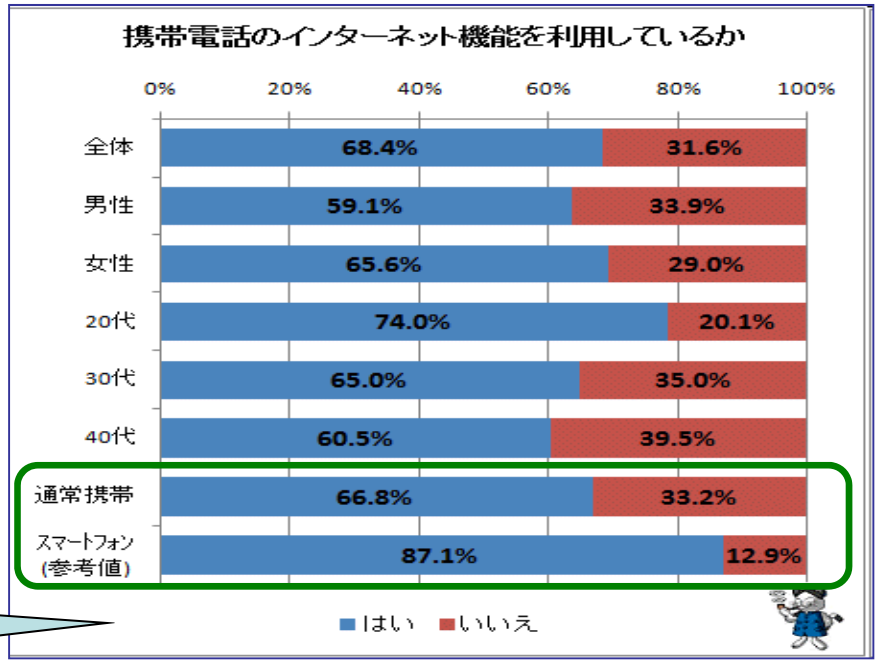
2016年には世界で11億6,000万台普及すると予測されている。

（出典：アイシェア）

【スマートフォンによるインターネット利用】

スマートフォンユーザのインターネット利用率は
携帯電話ユーザより高い

携帯電話ユーザの
約1.3倍

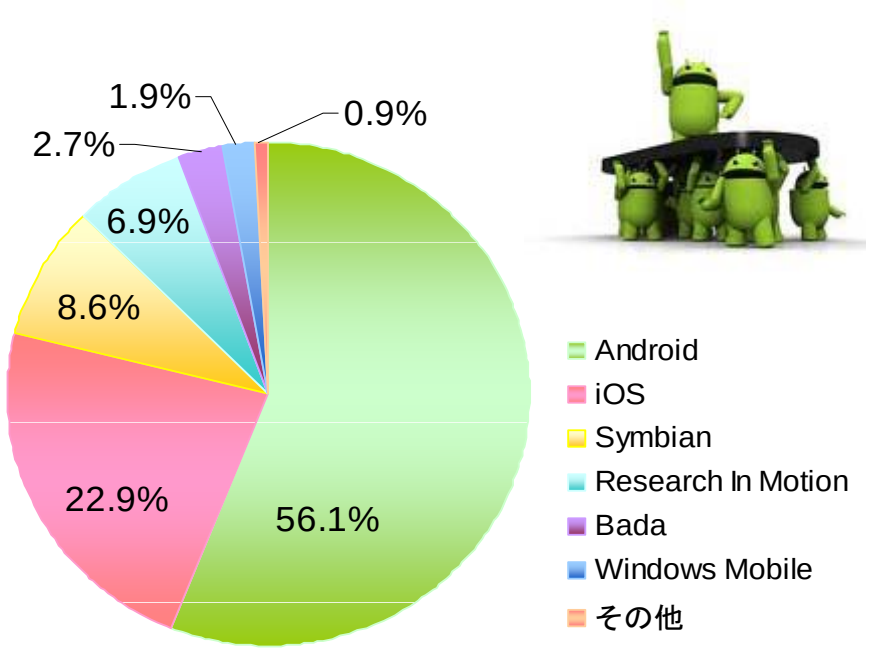


Copyright©BroadBand Security, Inc.

スマートフォン/タブレット端末 ～OSシェア～

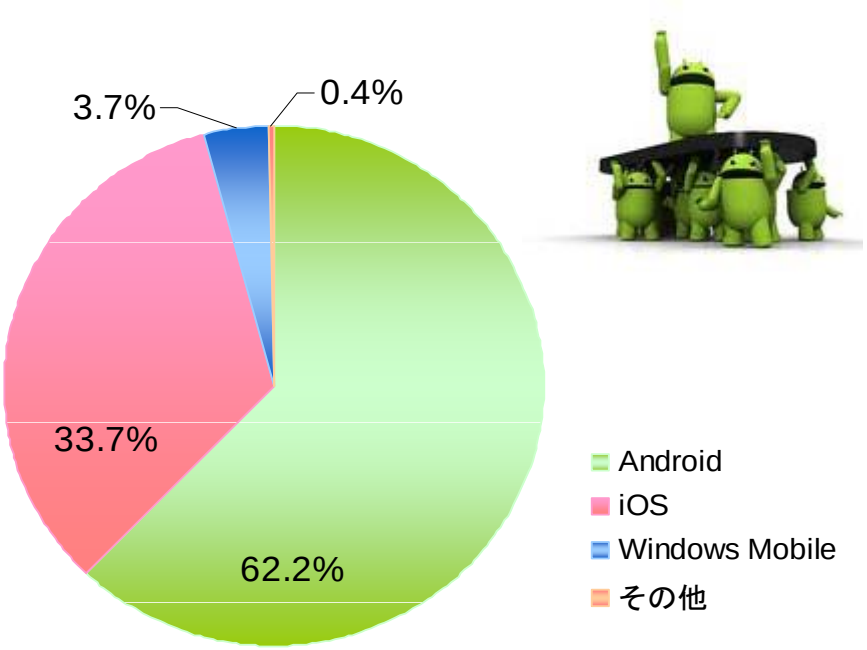
スマートフォンのOS別普及率

【世界スマートフォンOS別出荷台数シェア（2012年第1四半期）】



（出典：Gartner, Inc.）

【国内スマートフォンOS別出荷台数シェア（2012年第1四半期）】

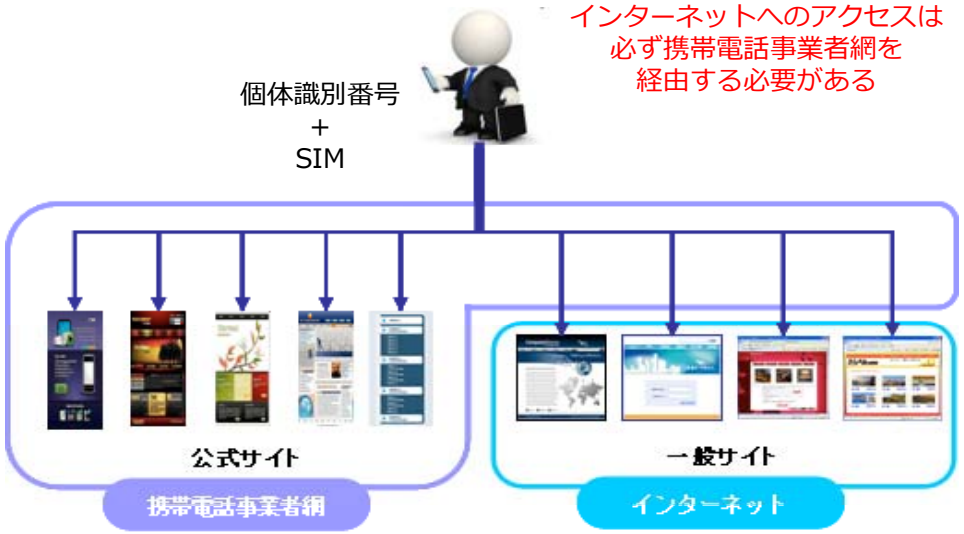


（出典：comScore, Inc.）

Copyright©BroadBand Security, Inc.

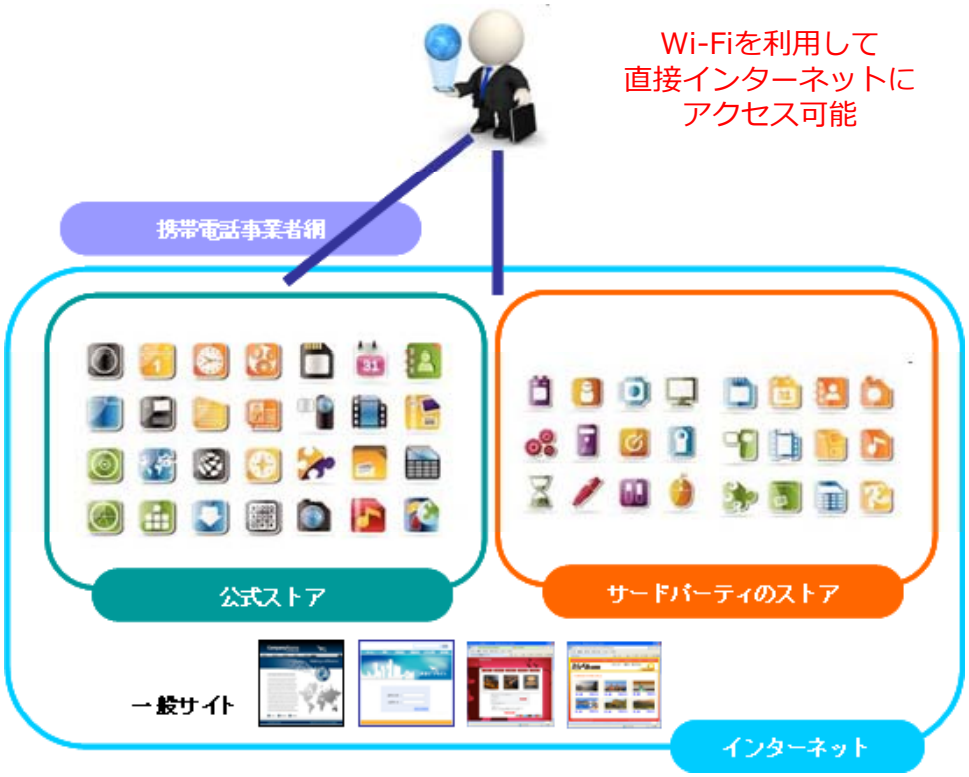
スマートフォン/タブレット端末 ～フィーチャーフォンとの比較～

【フィーチャーフォン】



独自仕様によって特化していることから、
マルウェア等の感染リスクは低い

【スマートフォン】



マルウェア等感染リスクはPCと同様、
セキュリティ課題は多い

Copyright©BroadBand Security, Inc.

スマートフォン/タブレット端末に対する脅威

スマートフォン/タブレット端末 ～アプリ配布～

悪質なAPP
ダウンロード

外部の悪意ある者

悪質な
APP配付

・マルウェア混入

APPマーケット

・星の数ほどのコンテンツの
管理は難しい
・書類審査のみで登録

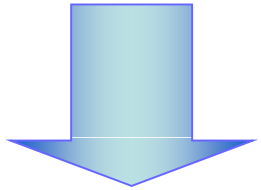
悪質なAPP
ダウンロード

・端末情報
ID/PW
TEL
アドレス
メール

・端末裏取り
サーバ認証する
ID/PWを取得される
（2回目から保存されている
情報を利用する）

なりすまし
リモートで何でもできる

ダウンロード



バンキングアンドロイドなど

配付

アプリ配付
・責任＝（製造責任・提供責任）
・パッチ
・セキュリティ
・保守（動作）

コンテンツ事業者

Copyright©BroadBand Security, Inc.

スマートフォン/タブレット端末 ～マルウェア増殖傾向～

【スマートフォン/タブレットPCを狙ったマルウェアの増殖推移】

（出典：McAfee. Inc.）

（出典：ABI Research）

【四半期ごとのモバイル端末向けマルウェアサンプル数推移】

- Androidを標的としたウイルスの多くが、端末のroot権限を取得し、バックドアを埋め込むタイプ（例：Geimini、Pjapps、Rootcagerなど）。
- 個人情報をはじめとした端末内の情報を奪取される危険性がある。
- ウイルス感染は、主にウイルスが混在したアプリケーションをインストールしてしまったことに起因する。
- 多くの場合、Androidマーケット以外から入手したアプリケーションにウイルスが潜んでいる。
- しかし、最近ではAndroidマーケットでもウイルスが混在したアプリケーションが確認されている（ほぼ審査がないことが原因）。

Copyright©BroadBand Security, Inc.

スマートフォン/タブレット端末の脅威まとめ

スマートフォンに対する5つの脅威

紛失・盗難	紛失・盗難に遭った端末から業務データが漏洩
不正プログラム	急増するマルウェア。感染によって情報漏洩、また、不正なリモートコントロール、不正な課金等
人為的な情報漏洩	豊富な外部インターフェースを悪用して業務データを漏洩
不正アクセス・なりすまし	不正に取得したID/パスワード/端末、及び非正規端末によって社内システムへ接続される
システム情報の漏洩	アプリから不正に端末、位置情報等が漏洩

Copyright©BroadBand Security, Inc.

スマートフォン/タブレット端末に対する攻撃事例、起こりうる被害・影響

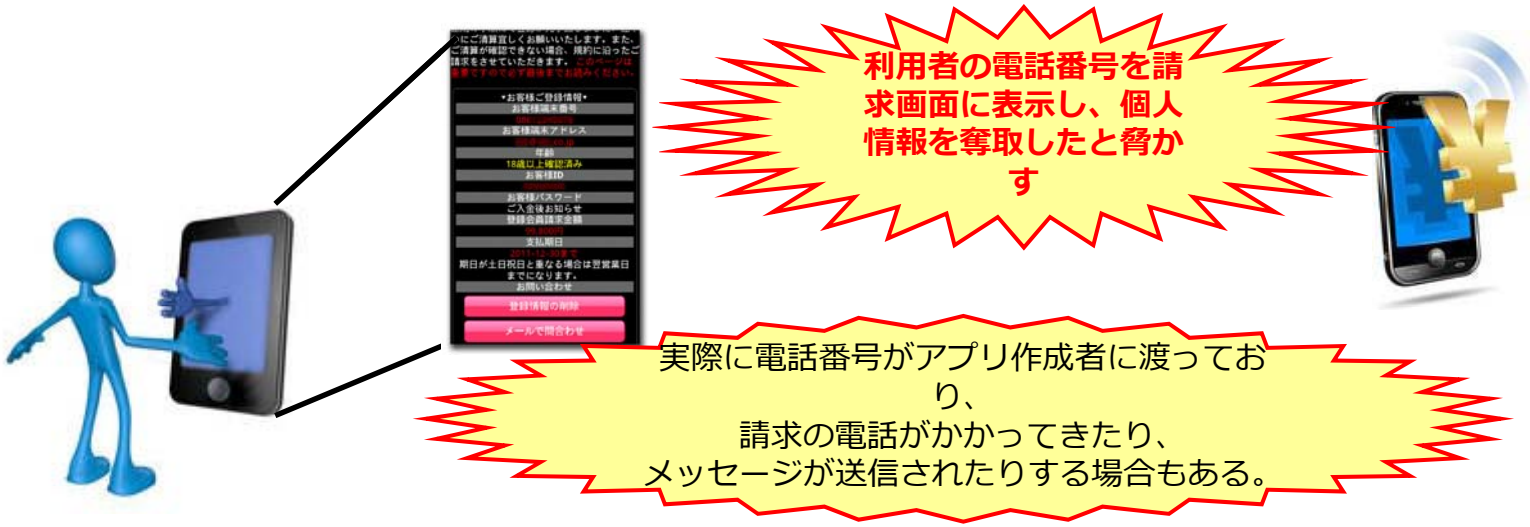
BBSec

攻撃事例１　～詐欺アプリ～

詐欺アプリ

攻撃例：

- ◆正規のバンキングアプリケーションを装い、**ユーザに金融情報を入力**させる
- ◆**人気のゲームアプリの海賊版に見せかけ**、商品やサービスの宣伝サイトへ誘導する
- ◆**いわゆる「ワンクリック」詐欺**を行い、個人情報を奪取したなどと利用者をだまし、高額請求を要求する



公式マーケットに公開された"詐欺アプリ"の例

（出典：Symantec, Inc.）

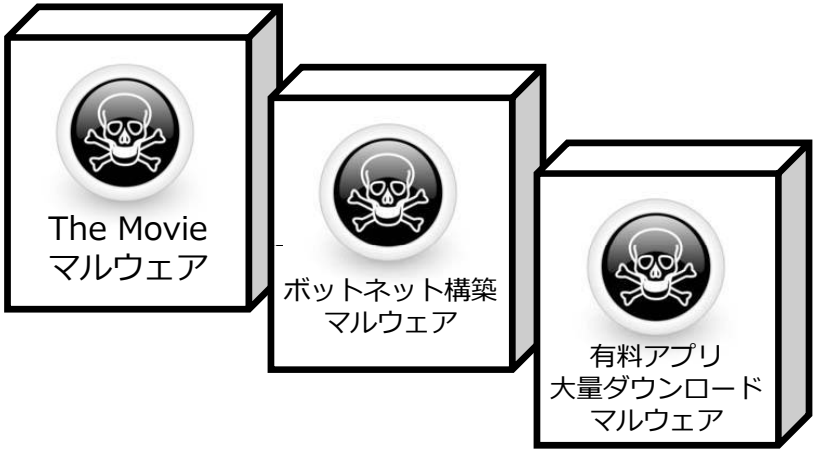
Copyright©BroadBand Security, Inc.

攻撃事例２　～マルウェア感染～

アプリからのマルウェア感染

攻撃例：

- ◆**正規のアプリにマルウェアを組み込んで“リパッケージ”**されたもので、主にゲームアプリ利用者を狙う。ボットネットに感染させることもある
- ◆OSの既知の脆弱性を悪用し、**管理者アカウント権限を取得**、デバイスを乗っ取る
- ◆**高額料金を請求する海外の拠点に電話**をかけたり、メール（ショートメッセージ）を送信したりする
- ◆**SDカードの空き容量がなくなる**まで、画像を追加し続ける



不正なダウンロードサイト、
公式アプリ配信サイト、
Facebookの友達リクエスト等、
感染場所は多種多様

Copyright©BroadBand Security, Inc.

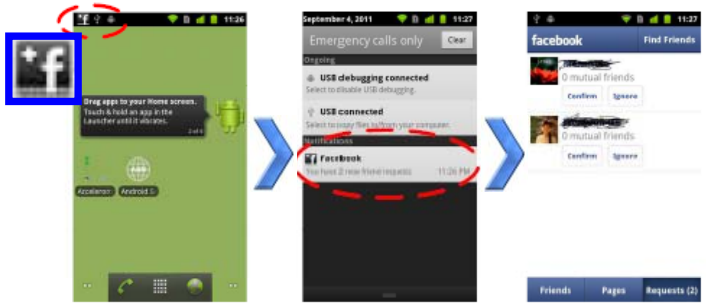
攻撃事例３　～PCの手口と同様の攻撃～

自動ダウンロードやブラウザ機能を悪用した攻撃

攻撃例：

- ◆モバイルブラウザやメールクライアントを悪用した**フィッシング詐欺攻撃**
- ◆正規サービス（**SNSサービスやモバイルキャリア）のお知らせ機能に見せかけ**、マルウェア感染や情報詐取を行う

正規のお知らせサービス



偽のお知らせサービス（フィッシング詐欺）

注意深く見ればアイコンが違うのが分かるが、通常はなかなか気付くことができない

Copyright©BroadBand Security, Inc.

攻撃事例４　～ネットワークのハッキング～

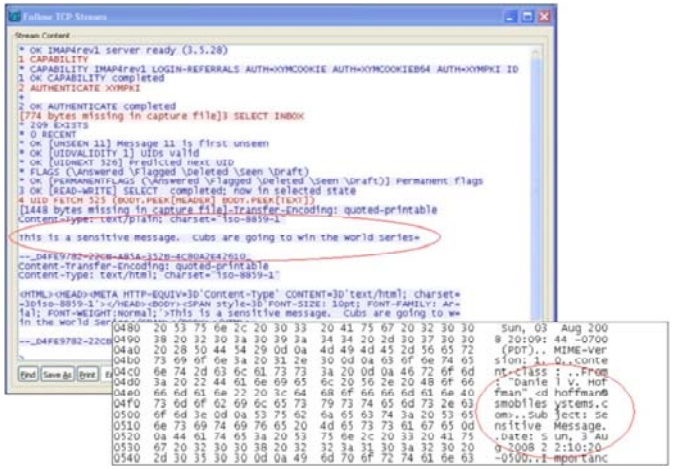
データ通信の傍受による情報の奪取

攻撃例：

- ◆Wi-Fiハッキング
- ◆3Gネットワークハッキング
- ◆中間者攻撃

セキュリティ対策が講じられていない
ネットワークに接続している端末から
情報を不正に取得

中間者攻撃



（出典：Juniper Networks）

3Gネットワークの脆弱性

◆認証／暗号鍵配送（AKA）プロトコルの脆弱性
◆「International Mobile Subscriber Identity（IMSI）：国際携帯機器加入者識別情報」送信リクエスト偽装
など

これらを悪用してスマートフォンを追跡することが可能

Copyright©BroadBand Security, Inc.

今後も進化し続ける脅威

マルウェアのさらなる劇的増加

アプリケーションが狙われる

Webブラウザ経由の自動ダウンロード型攻撃が増加

モバイルフィッシング詐欺攻撃の増加

Copyright©BroadBand Security, Inc.

スマートフォン/タブレット端末の
セキュリティ対策

BBSec

スマートフォンアプリが抱えるリスク

スマートフォンアプリはWEBアプリと比べて
下記のような独自のリスクを抱えています

1. プライバシー情報の取り扱い

スマートフォンアプリでは「**電話帳、メール、GPS**」などWEBアプリより多くのプライバシー情報を扱うことが可能になっています。

2. 端末内ファイルへのユーザ情報の保管

WEBアプリではサービス提供者が管理できるサーバ内にユーザ情報を保管していましたが、スマートフォンアプリではユーザの端末内に保管可能になっています。

サーバであればOS・サービスに適切なパッチを当てたり、Firewallやその他のセキュリティソリューションで守ったりできましたが、ユーザ端末の保護は不可能です。

3. クライアント

WEBアプリでは一般的に普及しているブラウザ（Chrome,IE,Firefox,Safari)を使ってサーバへアクセスしましたが、スマートフォンアプリでは独自開発したブラウザを使うことが多くなっています。
独自開発でコーディングしている分、脆弱性が入り込みやすいです。

Copyright©BroadBand Security, Inc.

過去に発見された脆弱性例

S●●●●の脆弱性

内容：チャット履歴や個人情報を含む端末内ファイルが他のアプリからアクセス可能な状態になっていた。
　　ユーザー名、住所、アカウント名、電話番号、連絡先などの情報を許可なく引き出せてしまうことを実証。
原因：ファイルパーミッションの設定不備
参考URL：http://www.itmedia.co.jp/enterprise/articles/1104/19/news025.html

G●●●の脆弱性

内容：端末内に保管されたユーザ情報が他のアプリからアクセスできる状態になっていた。
原因：独自開発したブラウザ（WebView)の脆弱性
参考URL：http://jvn.jp/jp/JVN99192898/

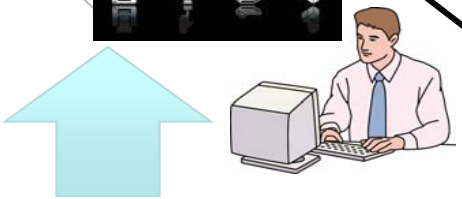
m●●●の脆弱性

内容：「友人の発言」が他のアプリからアクセスできる状態になっていた
原因：アクセス制御ができないSDカード領域への機密情報の保管
参考URL：http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-000078.html

Copyright©BroadBand Security, Inc.

スマートフォンアプリ検査の実施

iPhone/Android
アプリケーション



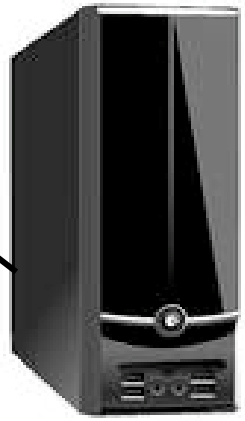
サービス提供システム/サーバ検査

・サーバ側API自体の脆弱性調査
・APIを提供するサーバプラットフォームに対する脆弱性調査

Internet

クライアントアプリケーション検査

・実機を使用したアプリ診断
・アプリソースコード分析によるより詳細な分析
・個人情報、決済情報等の重要情報取り扱いに関する調査
・アプリが不正に端末情報の送信をおこなっていないか調査
・端末に保有された情報に関するアクセス制御、暗号化等の調査



Web・APIサーバ

Copyright©BroadBand Security, Inc.

検査内容 1/3

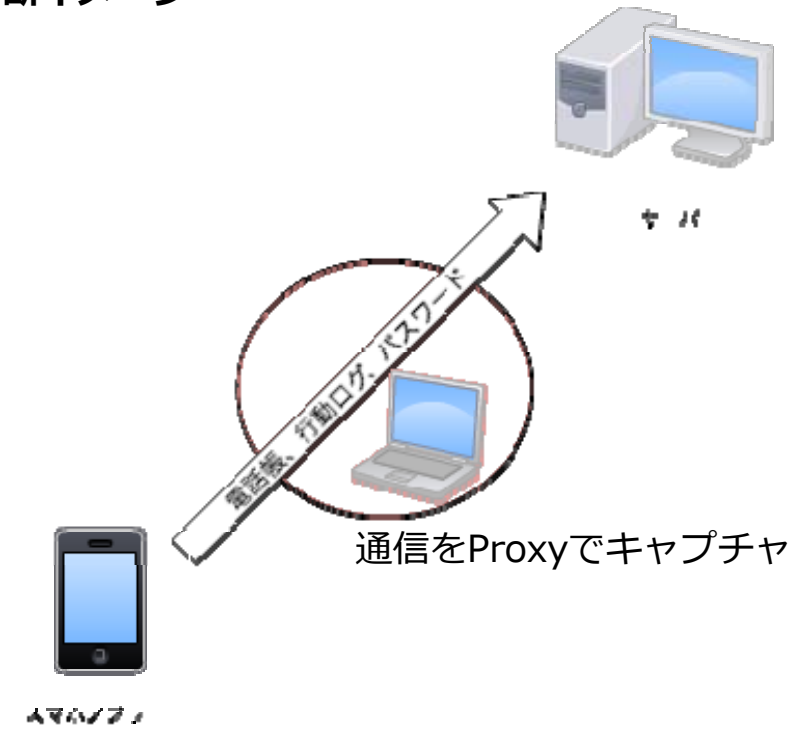
通信診断

内容：送信内容と送受信パラメータに関する脆弱性の診断を行う
手法：スマートフォンアプリの通信をProxy（PC)でキャプチャし、内容を調査する

・診断項目

不正通信の確認	外部サーバへの個人情報/機密情報の不正送信の有無を確認します。
HTTPレスポンス診断	アプリの入力となるHTTPレスポンスをキャプチャ・改竄することによってアプリの脆弱性診断を行います。
HTTPリクエスト診断（Web API診断）	サーバ側の脆弱性診断を行います。

・診断イメージ



通信をProxyでキャプチャ

検査内容 2/3

端末内データ診断

内容：端末内データに関する脆弱性の診断を行う
手法：アプリを動作させることによって生成される端末内データの内容や保持方法、設定状況を調査する

・診断項目

端末内データの不備	端末内のファイル（Database,Preference等含む）などにパスワードや個人情報などのデータを平文で保存していないことを確認します。
端末内データ改竄による不正行為	端末内データを改竄することによる不正行為（チート、残高偽装、購入履歴偽装等）の可否を確認します。
パーミッションの設定不備	重要情報を含むファイルが他アプリからアクセスできるパーミッションになっていないかを確認します。
SDカードへの機密情報の出力	他アプリからアクセス可能なSDカード内へ個人情報/機密情報を保存の有無を確認します。
ログへの機密情報の出力	ログにユーザの個人情報/機密情報の出力の有無を確認します。
コンテントプロバイダからのアクセス制御不備	個人情報/機密情報へアクセス可能なコンテントプロバイダが意図せず他のアプリから不正にアクセス可能かを確認します。

・診断イメージ

端末内の内容、設定、保持方法を調査

Copyright©BroadBand Security, Inc.

検査内容 3/3

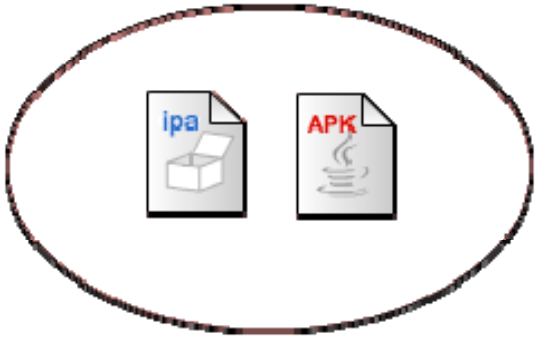
バイナリ診断

内容：アプリのロジック、ソースコードに関する脆弱性の診断を行う
手法：ディスアセンブル、リバースエンジニアリングによって得られたコードを調査する

・診断項目

耐タンパー性の確認	逆コンパイルの可否や難読化の有無等を確認します。
リバースエンジニアリングによる脆弱性解析	リバースエンジニアリングによる脆弱性の解析を行います。
ソースコードへの機密情報の出力有無	逆コンパイルしたソースコード内に暗号化キーや隠し機能、隠しURL等の情報がハードコーディングされていないかを確認します。
通信プロトコルの解析	HTTP以外のプロトコルが使われている場合は解析し、脆弱性の有無を確認します。

・診断イメージ



アプリのロジック、ソースコードを解析する

Copyright©BroadBand Security, Inc.

検査プラン

			ライトプラン1	ライトプラン2	ノーマルプラン	プラチナプラン
通信診断	不正通信の確認 ※プロトコルはhttpのみ対応	外部サーバへの個人情報/機密情報の不正送信の有無を確認します。	○	○	○	○
	HTTPレスポンス診断	アプリの入力となるHTTPレスポンスをキャプチャ・改竄することによってアプリの脆弱性診断を行います。	-	-	-	-
	HTTPリクエスト診断（Web API診断）	通常のWebアプリ診断と同様の内容です。サーバ側の脆弱性診断を行います。	-	-	-	-
実機診断	端末内データの不備	端末内のファイル（Database,Preference等含む）などにパスワードや個人情報などのデータを平文で保存していないことを確認します。	-	○	○	○
	端末内データ改竄による不正行為	端末内データを改竄することによる不正行為（チート、残高偽装、購入履歴偽装等）の可否を確認します。	-	○	○	○
	パーミッションの設定不備	重要情報を含むファイルが他アプリからアクセスできるパーミッションになっていないかを確認します。	○	○	○	○
	SDカードへの機密情報の出力	他アプリからアクセス可能なSDカード内へ個人情報/機密情報を保存の有無を確認します。	○	-	○	○
	ログへの機密情報の出力	ログにユーザの個人情報/機密情報の出力の有無を確認します。	○	-	○	○
	コンテントプロバイダからのアクセス制御不備	個人情報/機密情報へアクセス可能なコンテントプロバイダが意図せず他のアプリから不正にアクセス可能かを確認します。	-	-	○	○
バイナリ診断	耐タンパー性の確認	逆コンパイルの可否や難読化の有無等を確認します。	-	-	-	○
	リバースエンジニアリングによる脆弱性解析	リバースエンジニアリングによる脆弱性の解析を行います。	-	-	-	○
	ソースコードへの機密情報の出力有無	逆コンパイルしたソースコード内に暗号化キーや隠し機能、隠しURL等の情報がハードコーディングされていないかを確認します。	-	-	-	○
	通信プロトコルの解析	HTTP以外のプロトコルが使われている場合は解析し、脆弱性の有無を確認します。	-	-	-	○

Copyright©BroadBand Security, Inc.

本日はご清聴ありがとうございました。

【脆弱性診断、情報セキュリティに関するご相談】
株式会社ブロードバンドセキュリティ
〒160-0023 東京都新宿区西新宿8-5-1
野村不動産西新宿共同ビル 4F
URL:http://www.bbsec.co.jp/
TEL:03-5338-7425 FAX:03-5338-7435

Copyright©BroadBand Security, Inc.