資料8－3

モバイル環境におけるMalware等の調査

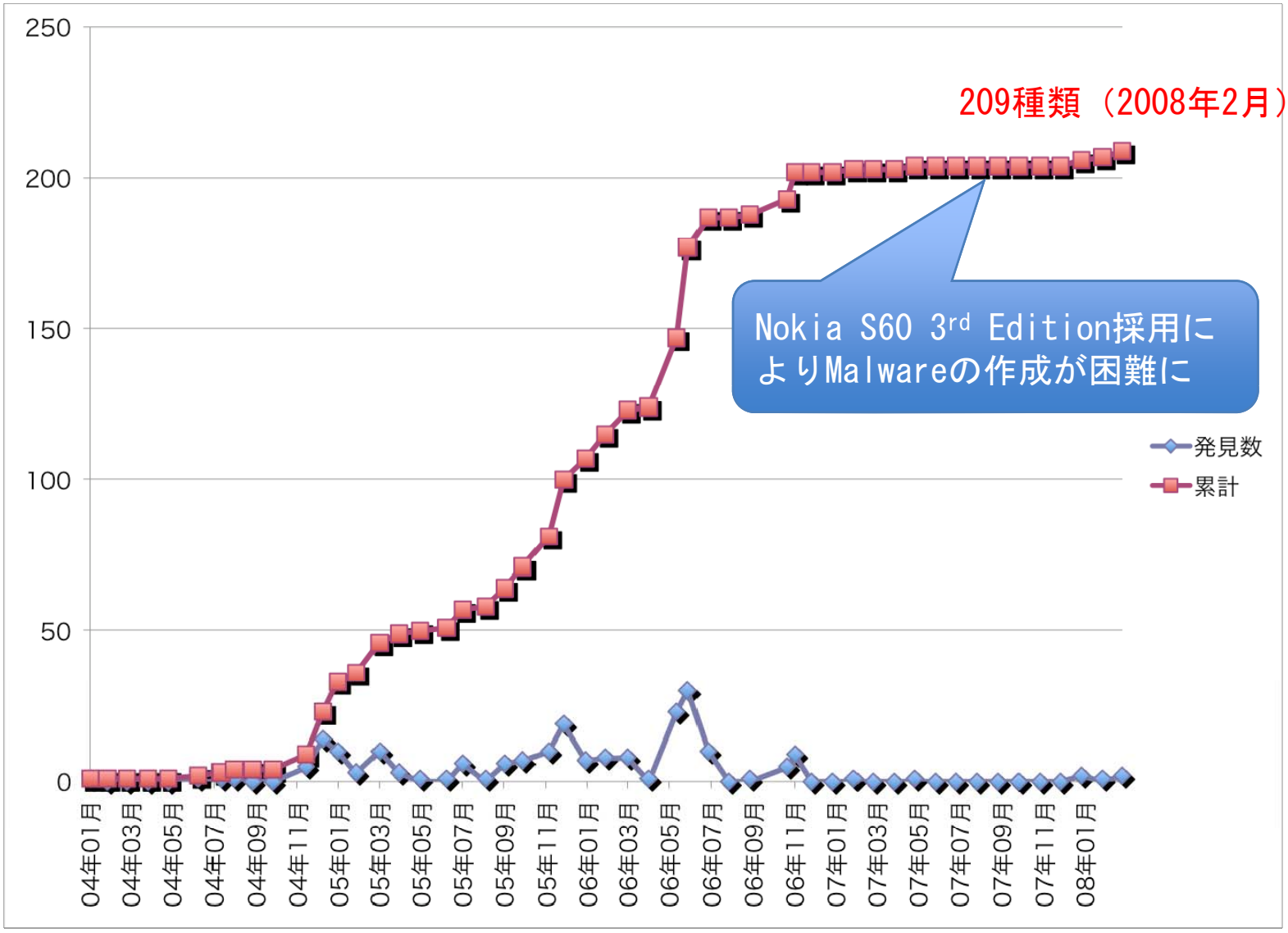
株式会社セキュアブレイン

2008年5月23日

目的と調査概要

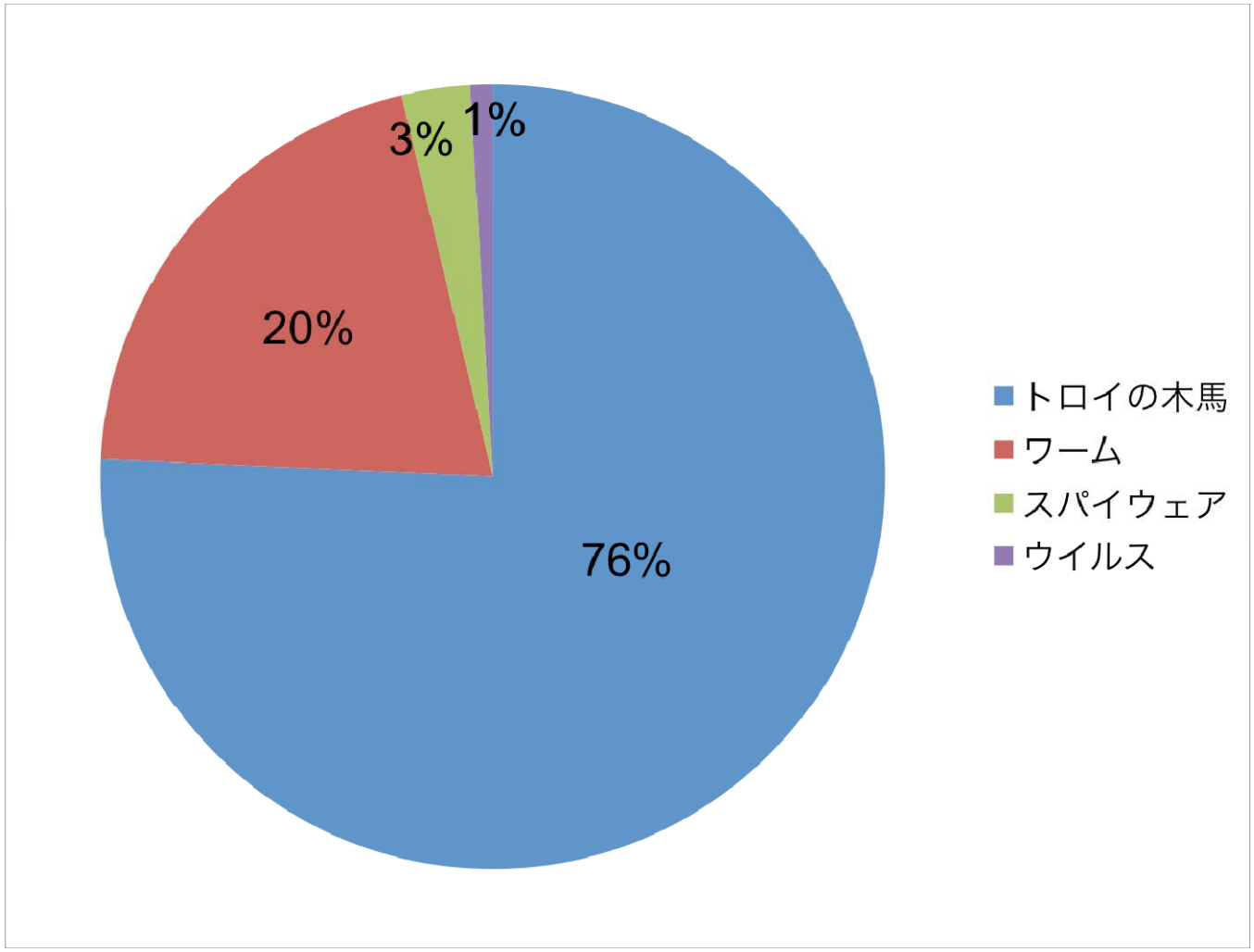
- 目的
  - 現状および近い将来における携帯電話やスマートフォンにおけるモバイル環境に関して、Malware等の情報セキュリティの現状の脅威や今後発生する可能性のある脅威を把握・検討するとともに、Malwareの収集方法および対策について調査研究する
- 調査概要
  - 携帯電話とスマートフォンのハードウェア及びソフトウェアの構造調査を細部まで調査することにより、悪意のあるプログラムを作ることの可能性やその脆弱性に関して検討する
  - 公開されているアプリケーション開発用のAPIやスクリプトの調査を行う
  - モバイルMalwareの収集方法と対策について検討する

海外のモバイルMalware数



参考：米シマンテック社 スレットエクスプローラー

海外のモバイルMalwareの種類



参考：米シマンテック社 スレットエクスプローラー

代表的なモバイルMalware

- Cabir
  - Bluetooth経由で感染を広げるワーム
  - ファイル削除や勝手に警察などへ電話をかけたりする
- FlexiSpy
  - 2006年3月にヨーロッパで発見された携帯電話を狙った最初のスパイウェア
  - 通話やメール、SMSの履歴情報などの情報をすべて外部サーバへ転送
  - タイの企業が商用アプリケーションとして販売している
- Commwarrior
  - マルチメディアメッセージサービス（MMS）経由で感染
  - 携帯電話端末の電話帳ソフトウェアに感染し、電話帳の中からランダムに送り先のアドレスを見つけ出し、その相手に自らの複製を送りつける
- Cardtrp
  - Symbian端末のメモリカードにWindowsの実行ファイルを挿入（実行ファイルはWindows上ではシステムフォルダとして表示）
  - メモリカードのデータをPCで閲覧し、フォルダに見せかけた実行ファイルを開くとPCがワームに感染してしまう

脅威のシナリオ

- アプリ配布サイトを攻撃する
  - 携帯電話用のアプリを配布しているサイトの脆弱性を攻撃してMalwareと差し替える
  - ユーザは信頼しているサイトに登録されている正規アプリとしてMalwareをダウンロードして実行してしまう可能性がある
- トロイの木馬
  - ユーザの許可なく携帯電話内に保管されているリソースを攻撃するMalwareの可能性がある
- ワーム
  - 携帯電話やスマートフォンから携帯電話やスマートフォン、PCなどへ感染するMalware
  - メールで受け取った添付ファイルを実行すると自動的に他のメールアドレスにMalwareを添付したメールを送信する
  - Bluetoothや赤外線通信などの無線通信機能を利用して感染する可能性も考えられる
- スパイウェア
  - 携帯電話やスマートフォン内部に保管されている情報を外部へ送信する
  - 携帯電話に保存されている写真を外部へ送信する
  - 画面に表示されるイメージやメッセージの工夫によって、ユーザに個人情報を入力させる
- 個体識別情報を攻撃するMalware
  - 他人の携帯電話の個体識別情報を利用して、不正アクセスを行うMalwareの可能性が考えられる

脅威のシナリオ（続き）

- OSの脆弱性を攻撃するMalware
  - OSやミドルウェアの脆弱性を攻撃することによって本来できないはずの操作（権限のないユーザがroot権限の操作を実行できるなど）や見えるべきでない情報の取得が行える
- 基本アプリの脆弱性を攻撃するMalware
  - 基本アプリの脆弱性を攻撃することによって、本来できないはずの操作（権限のないユーザが、基本アプリが動作していた権限の操作を実行できるなど）や見えるべきでない情報の取得が行える
- 同期機能を攻撃するMalware
  - 携帯電話とPC間のデータを同期する機能を悪用して携帯電話にMalwareを送り込む
  - PC上で動作するMalwareと連携するMalwareの可能性も考えられる。例えば、携帯電話上で収集したデータを同期機能によってPC側に転送した後、PCで動作している別のスパイウェアがデータを外部に送信する
- FeliCaを攻撃するMalware
  - FeliCaのICチップの内容へアクセスする
- 物理的に携帯電話を攻撃するMalware
  - 携帯電話からメモリカードを抜き取り、保管されているアプリを書き換えて携帯電話に戻すことで、携帯電話にMalwareを送り込む

携帯電話向けアプリの柔軟性比較

アプリが操作できる項目

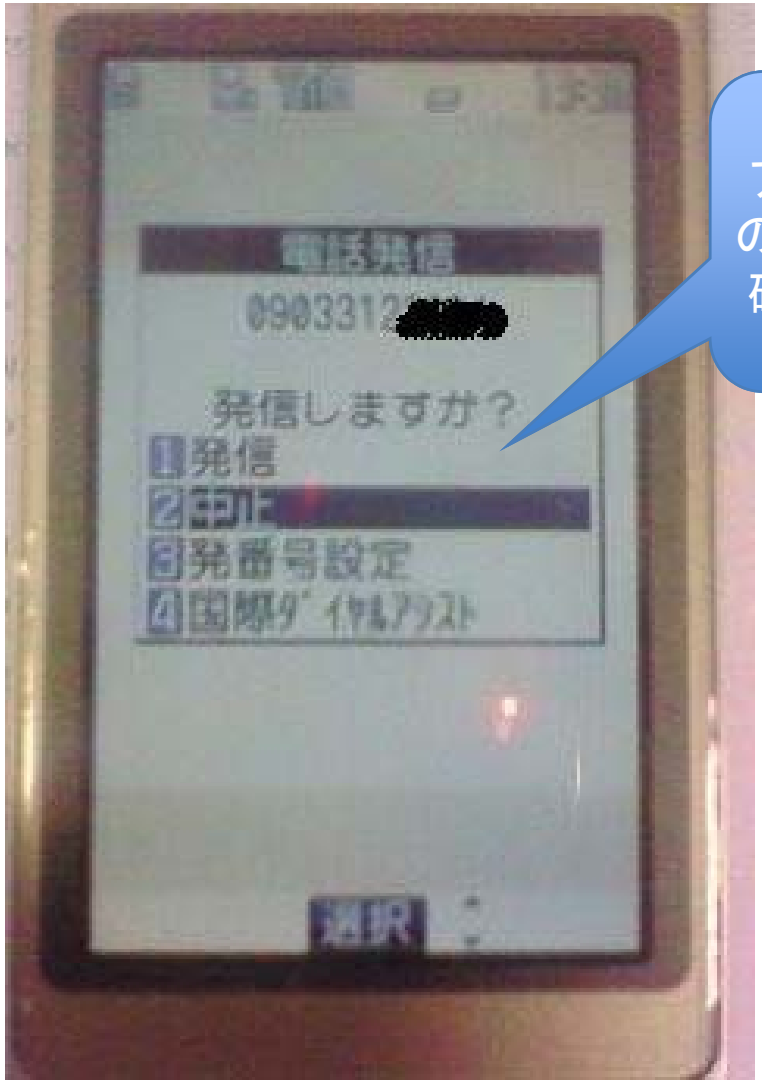
	A社	B社	C社
メールデータへのアクセス	△	×	×
画像データの読み込み	○	△	○
アドレス帳データの取得	△	○	×
HTTP(S)通信の利用	○	○	○
メールの送信	△	○	×
通話機能	○	○	○
位置情報の取得	△	△	○
通話履歴へのアクセス	△	○	×

○:全て操作可能　△:部分的に操作可能　×:操作不可

アプリの配布方法

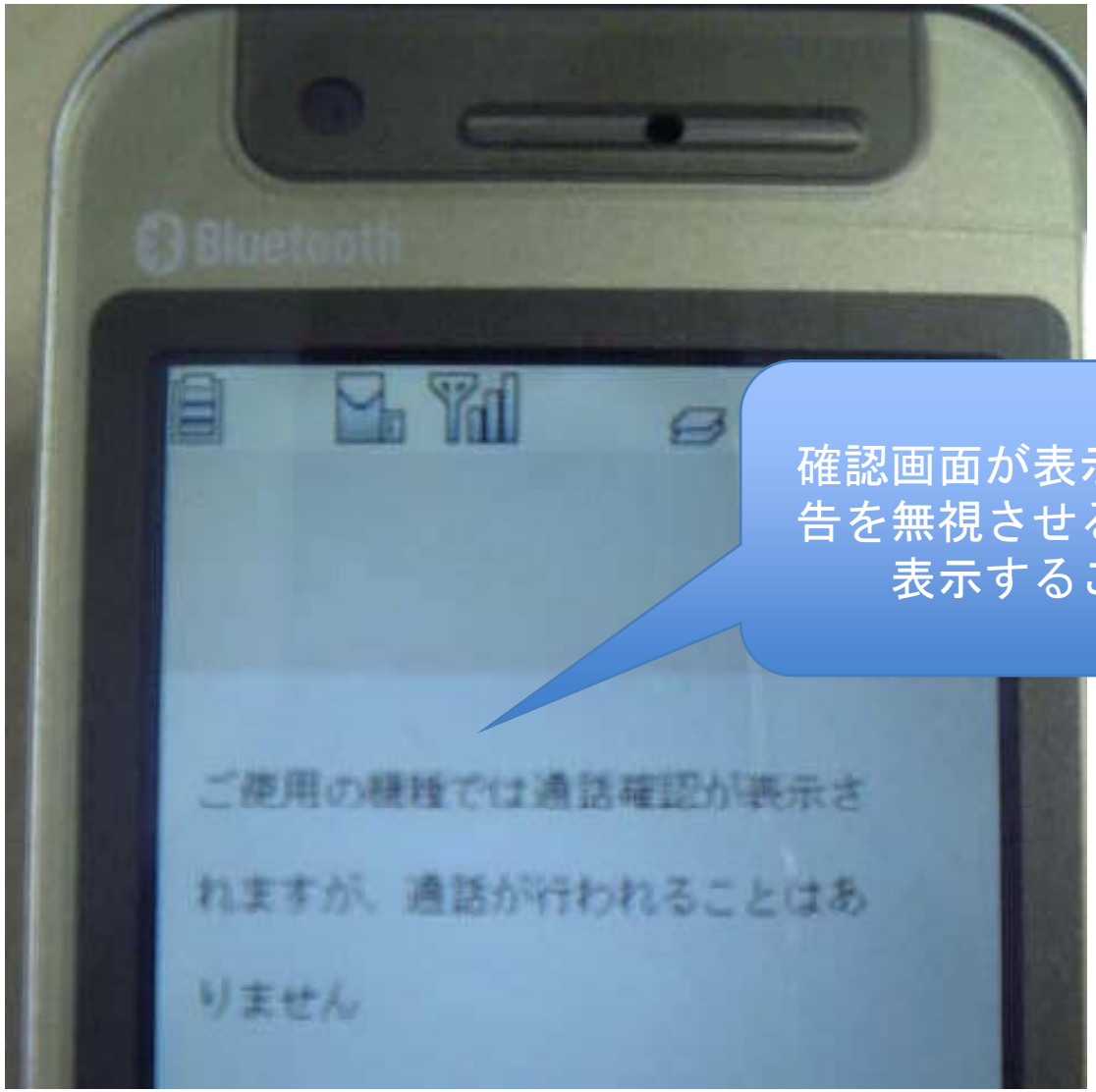
	A社	B社	C社
配布できるサイト	個人のサイト	B社のサイトのみ	C社指定のサイト

ネイティブ機能の悪用例



アプリからネイティブの機能を利用する場合、確認画面が表示される

ネイティブ機能の悪用例



スマートフォンでMalwareが作成される可能性について

- Windows Mobile 6.0はPCと同様の仕様になっている
- 基本的にPCに存在するMalwareはWindows Mobile 6.0のプラットフォームにも開発することが可能
- PC以上に個人情報を収集できるMalwareの開発が可能である
  - カメラやGPSなどのAPIが用意されている
- キャリアはプロビジョニング（デバイス製造後にセキュリティの設定を行うこと）を行うことによって事前にセキュリティポリシーを設定できるが、キャリアに任せてあるため、キャリアごとやデバイスごとにMalware対策のレベルが異なる

レジストリの修正について

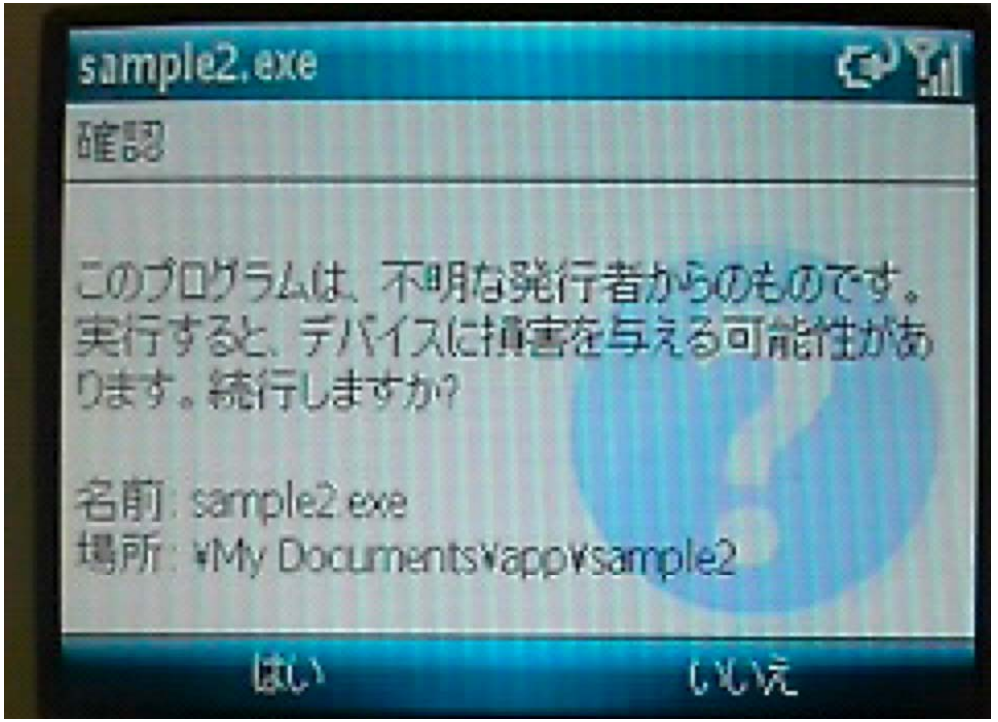
- **スマートフォンでもレジストリの修正は可能**

例えば、レジストリを修正することで内蔵カメラのシャッター音を無音のWAVファイルに変更することが可能

- 変更前
  - HKEY_・・・SnapSound=“￥Windows￥Snap.wav”
- 変更後
  - HKEY_・・・SnapSound=“￥Windows￥ShutterSound.wav”

署名なしプログラムの実行

- D社スマートフォンでは確認メッセージなしで署名されていないプログラムが実行できる
- C社スマートフォンでは確認メッセージが表示される（プログラムは実行可能）



モバイルMalware対策

- 標準セキュリティ機能
- ゲートウェイにおける対策
- ウイルス対策ソフトによる対策

標準セキュリティ機能

- A社の場合
  - アプリケーションはそのアプリケーション自身のダウンロード元であるサーバとしか通信できない
  - 電話帳などの個人情報を含んだネイティブデータへアクセスできない（キャリアの公式サイトを利用する場合は可能となることがある）
- B社の場合
  - アプリケーションはキャリアの管理下にある専用サーバ(ADS)からのみダウンロードできる仕組みになっている
  - キャリアの実施する検証にパスする必要がある
- C社の場合
  - コンテンツアグリゲータにおける制限により、ブラウザ、SDカードをフォーマットするもの、動画配信など通信大域を過大に消費するものは配布できない
  - アプリの配布基準によって使用できるAPIが制限されている
- Windows Mobile
  - セキュリティポリシーとセキュリティロール、デジタル証明書を組み合わせて、アプリケーションの制御やユーザごとのアクセスレベルの制御ができる

ゲートウェイにおける対策

- 携帯電話サービス事業者が自社のゲートウェイにモバイルMalwareに対応したゲートウェイ向けウイルス対策製品を設置して、ゲートウェイを通過するモバイルMalwareを排除する
- 利点
  - 携帯電話やスマートフォンの利用者が端末へウイルス対策ソフトを導入する必要がないので利用者への負担が少ない
  - 一定のセキュリティレベルを保つことができる
- 問題点
  - モバイルMalwareに特化したゲートウェイ向けのウイルス対策製品がない
  - Bluetooth経由で感染を広げるものは防げない

ウイルス対策ソフトによる対策

対象となる携帯電話	対策ソフト名	ベンダ
ドコモ携帯電話（FOMA 901iシリーズへ実装して出荷）	セキュリティスキャン	米マカフィー
Windows Mobile	Trend Micro ウイルスバスターモバイル セキュリティ	トレンドマイクロ
Windows Mobile	Symantec Client Security	米シマンテック
ソフトバンクスマートフォン（Symbian OS S60）	F-Secureモバイルセキュリティ	エフ・セキュア
ソフトバンク携帯電話	なし	
au携帯電話	なし	

モバイルMalwareの収集

- Webサイトからの収集
  - A社アプリとスマートフォン向けのアプリケーションはWebクローラで収集が可能
    - サイトによってはUser-AgentやIPアドレスでアクセスを制限している場合があるため工夫が必要
    - アプリをダウンロードする A社アプリを携帯に入れてサーバに送る方法がある
  - B社アプリとC社アプリは専用サーバのためインターネットからクロールすることは不可能
- Bluetoothを使った収集
  - Bluetooth機能をオンにした携帯端末で収集
  - 電車やイベント会場のように携帯端末の持ち込みと電源の投入が可能でかつ多くの人が集まる場所でなければならない
  - 他の携帯端末に感染を広げないようにする

モバイルMalwareの解析

- 解析ツールはJavaプログラム用とWindows Mobileプログラム用が必要
- Javaプログラム
  - デコンパイラ（または逆コンパイラと呼ばれる）を使用してバイトコードからソースコードを復元する
  - DJ Java Decompiler（http://www.kpdus.com/jad.html）など
  - デコンパイラによるリバースエンジニアリングを妨げるためにバイトコードを難読化するObfuscatorと呼ばれるツールがある
- Windows Mobileプログラム
  - Windows上で動作するMalwareを解析するためのツールが使用可能
  - IDA Pro（http://www.datarescue.com/）では標準でWindows Mobileのバイナリコードを解析することが可能

まとめ

- スマートフォン上で動作するMalwareが数多く存在し、すでに利用者への脅威となっている。国内でもWindows MobileをOSとして搭載したスマートフォンが増えており、今後、脅威が拡大する可能性がある
- 日本の携帯電話のMalwareは発見されていないが、高機能化してスマートフォンやPCに近づいている携帯電話にはいつMalwareが出現してもおかしくない状況である
- モバイル環境のアプリでは、モバイル機器側だけでなくWebアプリと組み合わせたサービスも多く、この組み合わせによる問題もあると考えられる
- すでにSymbian OSやWindows Mobile、iPhoneでも脆弱性が発見されている。また過去には国内の携帯電話の組み込みアプリの不具合によってデータが失われたり、許可されていないスクラッチパッドへのアクセスが可能になったりといった問題が発生している
- 今後、高度化、複雑化するモバイル環境でMalwareの問題が深刻化する可能性が高い。被害を拡大させないために引き続き調査、研究を続け、対策を講じる必要がある