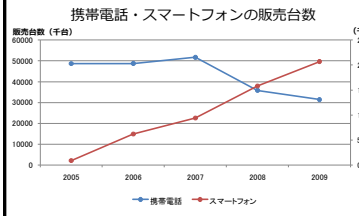
ユーザによるセキュリティ対策のための スマートフォン利用リスクの可視化

グループ演習６班　最終報告会
201020654　大原和人
201020672　長谷川大輔
201020667　角鹿誠真
201020659　木村正典
アドバイザ教員　古川宏

背景・スマートフォン販売台数の増加



- 近年,日本の携帯電話の販売台数が頭打ち
  - 販売推奨金の廃止による端末料金の値上げ
  - 日本の携帯電話保有率　96．3%（2009年3月）
- その一方,スマートフォンの販売台数が増えている

2

スマートフォンとは

- スマートフォンの定義
  - 「ソフト開発のための情報が提供されている OSを搭載した情報端末」
- スマートフォンの魅力を感じる点（ケータイ白書2010より）
  - パソコン用Webサイトの閲覧
  - 無線LAN
  - タッチパネル
  - Word・Excelの閲覧・編集
  - PCとの同期機能
  - アプリケーションやソフトのインストール

3

スマートフォン・セキュリティ被害例

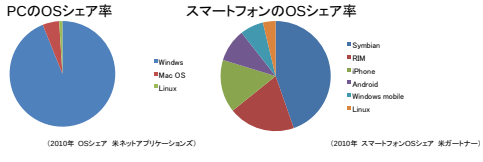
- ウィルス被害（2010/04　韓国）
  - ゲームのアプリダウンロードから感染
  - 使用者が気づかない内に国際電話に接続
  - 韓国国内で155件の被害例
- iPhone,iPadに危険な脆弱性（2010/08）

今後，被害が増大していくことが予想され、
スマートフォンのセキュリティについて考慮する必要性

4

スマートフォンのセキュリティ対策について

- 多様なOS・・画一的な対策が難しい



- CPU・メモリの制限・・常駐プログラムの負担が大きい
  →利便性とセキュリティ対策のトレードオフ
- 被害の件数が少ない
  - セキュリティ対策に対する需要が少ない

セキュリティ対策はPCほど充実していない

5

本研究の目的

ユーザはスマートフォンの利用におけるリスクを理解し
リスクを回避するための適切な対策を知ることが重要

オンライン機能・サービスを利用する際の
セキュリティリスクとその対策効果の可視化

スマートフォン，ならびに PC・携帯電話の
・オンライン機能・サービスの利用におけるリスク
・対策を行うことによるリスクの軽減
を表すセキュリティ対策マップの作成

スマートフォンにはどんなリスクがあり
どのような対策を行えばいいかを明示する

6

研究フロー

テーマ設定（～6月）

オンライン機能・サービス利用におけるリスクとその対策の調査（6～8月）
- オンライン機能・サービス利用時に発生する被害
- 発生する被害に対するセキュリティ対策
- 端末・OSによるセキュリティポリシーの違い

オンライン機能・サービス利用時のリスク評価（7～9月）
- 被害の大きさ
- 発生頻度
- 対策不備度

リスク評価結果の可視化とその考察（9月～）
- リスクの評価結果の可視化
- 可視化結果に対する考察

7

テーマ設定（～6月）

オンライン機能・サービス利用におけるリスクとその対策の調査（6～8月）
- オンライン機能・サービス利用時に発生する被害
- 発生する被害に対するセキュリティ対策
- 端末・OSによるセキュリティポリシーの違い

オンライン機能・サービス利用時のリスク評価（7～9月）
- 被害の大きさ
- 発生頻度
- 対策不備度

リスク評価結果の可視化とその考察（9月～）
- リスクの評価結果の可視化
- 可視化結果に対する考察

8

調査方法

① 文献・インターネットを利用した調査

② スマートフォンセキュリティ対策セミナーへの参加

協立共同通信（株） スマートフォン＆クラウド情報活用フェア
日時：7/9（金） 14：40～15：40

→スマートフォンのセキュリティ対策について把握

③ 情報処理推進機構(IPA)へのヒアリング調査

協力：加賀谷様 永安様 山北様
日時：8/17（火） 14：00～15：30

→セキュリティ対策の専門的な意見を伺う

・オンライン機能・サービス利用時に発生する被害
・発生する被害に対するセキュリティ対策
・携帯・OSによるセキュリティポリシーの違い

9

調査を行う端末・OS

- 現在日本で広く普及しているOSを採用
- PC，携帯電話はスマートフォンの比較対象として調査

調査を行う端末・OS

- スマートフォン
  - iPhone, Android, Windows Mobile, BlackBerry
- PC
  - Windows7
- 一般的な携帯電話

10

調査を行うオンライン機能・サービス

セキュリティ被害が発生する可能性がある機能・サービスを調査

調査を行うオンライン機能・サービス

- 電子メール機能
  - PC：Webメール
  - スマートフォン：Webメール，キャリア回線を介すメール
  - 携帯電話：キャリア回線を介すメール
- Web閲覧機能
  - PC，スマートフォン：PC用のWeb閲覧
  - 携帯電話：携帯電話用Web閲覧
- Webダウンロード機能
  - Web上にアップロードされているアプリケーション等を端末にダウンロード
- インターネットショッピング（バンキング）サービス
  - Web閲覧機能に加え，Web上で買い物やネットバンクを利用

11

オンライン機能・サービス利用時に発生する被害

- 警察庁のデータを基に決定した．
- ウィルス被害は多岐にわたるため，3種類に分ける．
- 情報漏洩によって生じる，なりすまし等の2次的被害は，1次的被害に含まれるものとする．
- セキュリティホールから生じる被害は，ユーザの行える対策がOSのアップデートしか存在しないため本研究では対象としない．

オンライン機能・サービス利用時の被害

- **フィッシング・ID窃盗**：偽造したサイトやメールによってID等の情報を盗まれる
- **架空請求**：身に覚えのない請求をされる
- **スパムメール**：迷惑メールを受信する
- **ウィルス1**：ウィルスに感染してデータが削除される
- **ウィルス2**：ウィルスに感染して情報漏えいしてしまう
- **ウィルス3**：ウィルスに感染して動作が妨害される
- **盗聴・盗み見**：通信データを盗聴される，紛失によって端末内データを盗聴される
- **メールの改ざん**：メール内容を改ざんされる

12

発生する被害に対するセキュリティ対策

- 対策の評価を行うため，対策レベルを4つに分ける．
  - ユーザが支払うコストを考慮
- OS毎の比較を行うため，同じOSでもキャリアや機種によって独自に行われている機能・対策については対象としない．
- OS側の対策は一般に公開されているものに限る．

対策レベル	内容
OS側の対策	ユーザが使用の有無を選択出来ない機能・サービスでの対策
対策レベル1	端末購入時から標準搭載されている機能での対策
対策レベル2	端末購入時には搭載されていないが，無料で行える対策
対策レベル3	端末購入時には搭載されていないが，有料で行える対策

13

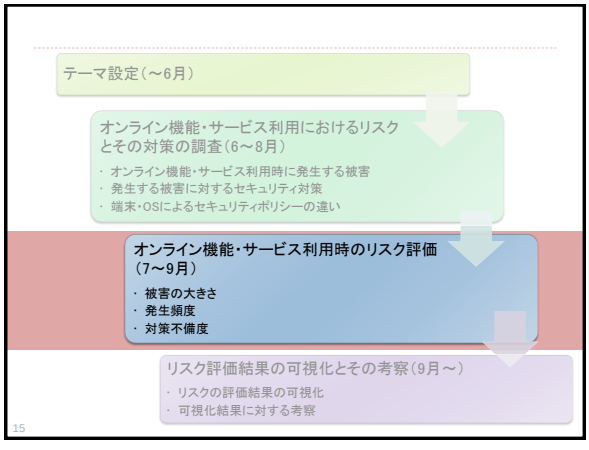
端末・OSによるセキュリティポリシーの違い

ヒアリング調査結果

セキュリティポリシー：セキュリティを確保するための方針

- PC(Windows7)
  - オープンなシステムであり，システムの自由度も高い
  - → ユーザは攻撃を受けやすく，対策も行いやすい
  - → ユーザに知識や対策意識が求められ，自ら対策を行う必要性が高い
- 携帯電話
  - クローズドなシステムであり，システムの自由度が低い
  - → ユーザは攻撃を受けにくく，対策も行いにくい
  - → ユーザに知識や対策意識が求められず，自ら対策を行う必要性が低い

14



15

オンライン機能・サービス利用時のリスク評価手法

- リスクの定量化評価手法

リスク＝被害の大きさ×発生確率

被害の大きさ

被害	被害の対象	被害の大きさの指標
情報漏洩	情報	情報の価値
架空請求	金銭	被害額
スパム	時間	時間の価値

→ 全ての被害を同じ指標で定量評価できない

発生確率

スマートフォンは普及段階であるため，十分なデータがない

→ 発生確率を求めることができない

本研究では定性的にリスクを求めた

16

オンライン機能・サービス利用時のリスク評価手法

- 定性的評価手法
  文献[1]のリスク値算出式を参考に以下の式でリスク値を求めた

リスク値＝被害の大きさ×発生頻度×対策不備度

被害の大きさ → **被害が発生した場合**のダメージを表す。3段階で評価した。

発生頻度 → **被害が発生する頻度**を表す。3段階で評価した。

対策不備度 → **被害に対して対策が為されていない度合い**を表し，対策が為されるほど小さい値をとる。5段階で評価した。

対策の効果を細かく評価するため，対策不備度のみ5段階で評価した。

[1]日本情報処理開発協会：ISMSユーザーズガイド-JIS Q 27001：2006 (ISO/IEC 27001:2005)対応

17

被害の大きさの評価

情報に対する被害 → 損害賠償額算出式[2]の経済的損失レベルを用いて評価

経済的損失レベル	漏洩情報
3	口座番号＆暗証番号，クレジットカード番号＆カード有効期限など
2	パスポート情報，口座番号のみ，クレジットカード番号のみ，資産，所得など
1	氏名，住所，生年月日，メールアドレス，電話番号，メール内容など

情報以外に対する被害 → 情報に対する被害の中で，同等の被害の値

例：架空請求
最悪の場合は金銭への被害 → 口座番号＆暗証番号と同等

[2]日本セキュリティネットワーク協会：2006年情報セキュリティインシデントに関する調査報告書

18

発生頻度の評価

PC,携帯電話 → 年間の発生件数を基に評価

発生頻度	説明
3	発生する可能性が高い(1万件～)
2	発生する可能性が中程度(百件～数千件程度)
1	発生する可能性が低い(数件～数十件程度)

スマートフォン

将来的にはPCと同等の被害数になると考えられる → PC利用における発生頻度と同じ値

19

対策不備度の評価

セキュリティ対策評価モデル[3]の技術的な要求についての対策コアに対する評価基準を参考に評価.

対策不備度	説明
5	対策が全く為されていない
4	対策が為されているが,平均以下の対策である
3	平均的な対策が為されている
2	平均以上の対策が為されているが,まだ対策の余地もある
1	現状ではこれ以上の対策ができない

一般的にユーザはPCに関して標準搭載の対策は行っている

↓

平均的な対策が為されている

↓

PCにおける対策レベル1の対策が全て為されている

20

[3]電子商取引推進委員会；セキュリティ対策評価モデル

テーマ設定(～6月)

オンライン機能・サービス利用におけるリスクとその対策の調査(6～8月)
- オンライン機能・サービス利用時に発生する被害
- 発生する被害に対するセキュリティ対策
- 端末・OSによるセキュリティポリシーの違い

オンライン機能・サービス利用時のリスク評価(7～9月)
- 被害の大きさ
- 発生頻度
- 対策不備度

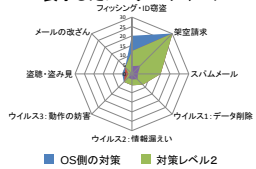
リスク評価結果の可視化とその考察(9月～)
- リスクの評価結果の可視化
- 可視化結果に対する考察

21

リスク評価結果の可視化

機能・サービス，OSごとに

対策レベルごとのリスク値を表示したレーダーチャート



対応する対策機能表

	対策	内容
OS側の対策	サンドボックス化	アプリの動作区間を区切り，ウィルスの被害を防ぐ．
	コード実行制限	コードの実行を制限し，ウィルスの被害を防ぐ．
	アプリの検証	全てのアプリに関してウィルスなどの検査
対策レベル1	デバイスロック	端末の使用を制限する．
	フィッシング警告表示	フィッシングサイトへの接続時の警告を表示する．
対策レベル2	ローカルワイプ	パスワードを一定回数連続して誤ると端末内のデータを消去する．
	悪意のあるサイトへの警告表示	悪意のあるサイトへの接続時の警告を表示する．
対策レベル3	リモートワイプ	遠隔でデータを削除する．
	遠隔ロック	遠隔操作で端末の使用を制限
	デバイス探索	紛失時に端末を発見する
	ウィルス駆除	端末内のウィルスを駆除
	ファイアウォール	外部との通信を制御

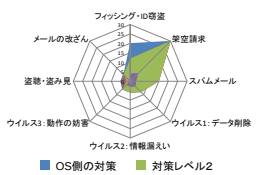
セキュリティ対策マップ

- ユーザが現状のリスクを知り，適切な対策をとる

22

セキュリティ対策マップの使用方法

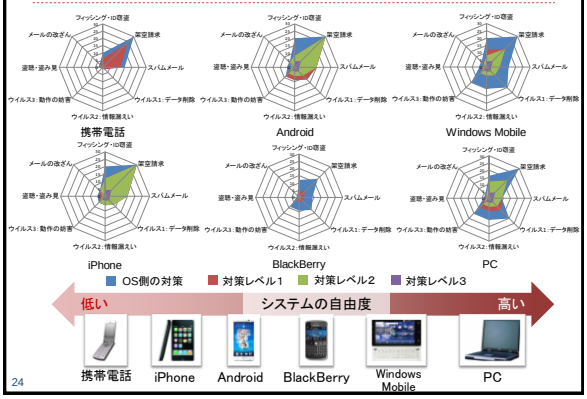
① 使用する機能・サービス及び端末・OSを選ぶ
② 現在行っている対策から現在の対策レベルを決定する
③ 現在のリスクの大きさを確認する
④ 対策の必要性を感じれば，対策表を参照しセキュリティ対策を行う



	対策	内容
OS側の対策	サンドボックス化	アプリの動作区間を区切り，ウィルスの被害を防ぐ．
	コード実行制限	コードの実行を制限し，ウィルスの被害を防ぐ．
	アプリの検証	全てのアプリに関してウィルスなどの検査
対策レベル1	デバイスロック	端末の使用を制限する．
	フィッシング警告表示	フィッシングサイトへの接続時の警告を表示する．
対策レベル2	ローカルワイプ	パスワードを一定回数連続して誤ると端末内のデータを消去する．
	悪意のあるサイトへの警告表示	悪意のあるサイトへの接続時の警告を表示する．
対策レベル3	リモートワイプ	遠隔でデータを削除する．
	遠隔ロック	遠隔操作で端末の使用を制限
	デバイス探索	紛失時に端末を発見する
	ウィルス駆除	端末内のウィルスを駆除
	ファイアウォール	外部との通信を制御

23

電子メール利用時のリスクとその軽減

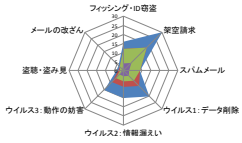


24

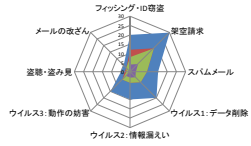
可視化結果に対する考察

オープンなシステム→PC，Windows Mobile

- OS側の対策の時点でリスクが大きいものがある
  →ユーザが対策を行うことによってリスクが小さくなる
- 対策レベル3（有償）の対策まで行えば，全ての被害のリスクを小さくできる



PCの電子メール利用時のリスク



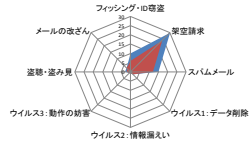
Windows Mobileの電子メール利用時のリスク

25

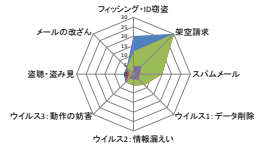
可視化結果に対する考察

クローズドなシステム→携帯電話，iPhone

- OS側の対策の時点でリスクが小さい
  →ユーザが行える対策は少ない
- 架空請求のリスクが大きい
  →ユーザ自身が気を付ける必要がある



携帯電話の電子メール利用時のリスク



iPhoneの電子メール利用時のリスク

26

可視化結果に対する考察

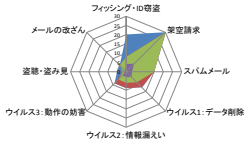
中間的なシステム→Android，BlackBerry

Android

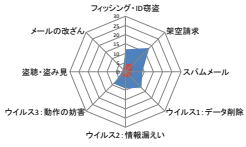
- リスクも中間のような分布となっている

BlackBerry

- 通信情報がサーバを経由することにより，安全性が保障される
- 対策レベル1（標準搭載）の対策を行えば十分といえる
- 無償，有償の対策はほぼ存在しない



Androidの電子メール利用時のリスク



BlackBerryの電子メール利用時のリスク

27

まとめ

- 作成したマップからリスクの大きさ，セキュリティ対策によりリスクが小さくなる様子が確認できる
  →ユーザが現状のリスクを理解し，適切な対策行動をとるための支援材料
- 作成したマップは，調査によって得られた端末・OSによるセキュリティーポリシーの違いと一致した
  →作成したマップの妥当性

28

今後の課題

- マップの有効性の確認
  - スマートフォンユーザにリスクの理解度，セキュリティ意識についてのアンケート
  - マップを見る前後でのユーザのリスク理解，セキュリティ意識の変化
- 対策と利便性の考慮
- キャリア側の対策，アーキテクチャの違いについて
- 完成したマップについて専門家の意見をいただく

29

ご清聴ありがとうございました

30