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

第 6 班：大原和人，木村正典，角鹿誠真，長谷川大輔
アドバイザ教員：古川　宏

1. 背景・目的

近年，日本では携帯電話の売り上げが頭打ちとなる一方で，スマートフォンの売り上げは上昇傾向にある．スマートフォンとは「ソフト開発のための情報が提供されている OS を搭載した携帯電話」であり，PC と同様に Web 閲覧や word・excel の編集といった機能を有する[1]．しかし，PC と同等のデータを扱っているため，スマートフォンの利用の際には PC と同様にウィルスや情報漏えいなどのリスクがある．実際に韓国ではスマートフォンでウィルス被害が発生しており[2]，更に，公衆無線 LAN の脆弱性が報告されている[3]．そのため，多様な通信方法もち，常時ネットワークに接続しているといった特徴を持つスマートフォンは，今後被害が増大していくことが予想されている[4]．

しかし，まだ被害の件数が少ないため，スマートフォンのセキュリティ対策は PC ほどの考慮がされていない．

そのため，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となる．

そこで本研究では，スマートフォン，ならびに比較対象として PC，携帯電話を対象とし，ユーザがオンライン機能・サービスを利用する際のリスクと，対策を行うことによるリスクの軽減をセキュリティ対策マップの作成によって可視化する．そして作成したマップを用いてユーザにリスクを適切に理解してもらうことを目的とする．

2. 研究の流れ

図 1 に本研究の流れを示す．

はじめに，スマートフォン，PC，携帯電話のオンライン機能・サービスの利用における被害とその対策について把握するため文献による調査を行った．さらに，スマートフォンのセキュリティ対策についてより詳細な情報を得るために共立情報通信株式会社が主催したスマートフォンのセキュリティ対策セミナーに参加した．また，専門的な意見を聞くためにコンピュータウィルス・不正アクセス・脆弱性に関し情報収集・提供を行っている独立行政法人情報処理推進機構（IPA）へのヒアリングを行った．

次に，調査した被害のリスクと対策の効果を把握するためにリスクの定性的評価を行った．

最後に，評価結果からスマートフォン，PC，携帯電話のリスクをセキュリティ対策マップとして可視化した．そしてセキュリティ対策マップについて検証し，マップの妥当性について検討を行った．

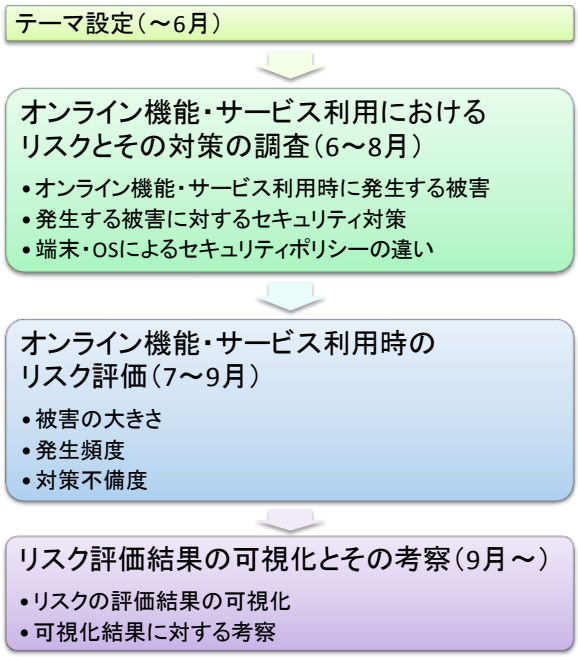


図 1 ：研究の流れ

3. 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

本章では，まず対象とする端末・OS 及び機能・サービスについて述べる．そして，オンライン機能・サービス利用におけるリスクを算出するため，どのような被害・対策が存在するかについて調査を行った結果と，IPA へのヒアリングから得られた各端末・OS のセキュリティポリシーの違いについて示す．

3.1 対象とする端末・ＯＳ及び機能・サービス

本研究で対象としたスマートフォンの OS は現在日本で利用されている iPhone，Android，Windows Mobile，BlackBerry の 4 種類とした．ならびに比較対象として PC，携帯電話を考慮する．PC の OS は Windows7，携帯電話は日本で一般的に利用されている端末の機能のみを考慮する．

また，機能・サービスに関しては，オンライン接続が必要となるもののうち，セキュリティ被害が発生する可能性がある以下の 4 つを対象とした．

- 電子メール
- Web 閲覧
- Web ダウンロード
- オンラインショッピング・バンキング

ここで，PC での電子メール利用は Web メール利用も含

み，携帯電話での電子メールは i モードメールなどのキャリア回線を介してのメールのやりとりを指す．スマートフォンでの電子メールは PC，携帯電話両方の電子メール機能を利用することとする．

PC, スマートフォンでの Web 閲覧は PC 用の Web を閲覧することを指し，携帯電話での Web 閲覧は携帯電話用の Web を閲覧することを指す．携帯電話による PC 用の Web の閲覧は利用できる機種が限られるため，考慮していない．

Web ダウンロードは Web 上にアップロードされているアプリケーションなどを端末にダウンロードすることを指す．

オンラインショッピング・バンキングは Web 閲覧に加え，Web 上で買い物や預金などを行うことを指す．

3.2 オンライン機能・サービス利用時に発生する被害

3.1 節の機能・サービスを利用時に発生する被害は警察庁の情報[5]を参考にし，定義した．表 2 に機能・サービスごとに想定した被害とその内容を記述する．

ただし，情報漏洩などから発生するなりすましのような二次的な被害については一次被害に含まれるものとし，考慮していない．また，端末の構造上の弱点である脆弱性についても，ユーザ側で行える対策がアップデートを行うことしか存在しないため，今回は考慮していない．

表 1　オンライン機能・サービス利用時に発生する被害

(a)電子メール利用時の被害

被害	内容
フィッシング･ID 窃盗	・ 公的な機関になりすまされメールアカウントなどの ID を聞きだされる． ・ 端末の紛失・盗難によって端末内の ID データを盗まれる．
架空請求	架空請求メールが送られてくる．
スパムメール	邪魔なメールが送られてくる．
ウィルス 1	ウィルスによってデータを削除される．
ウィルス 2	ウィルスによって情報漏洩してしまう．
ウィルス 3	ウィルスによって動作が妨害される．
盗聴・盗み見	・ 通信中にメール内容を見られる． ・ 端末の紛失･盗難によってメール内容が見られる．
メール改ざん	メール内容を改ざんされる．

(b)　Web 閲覧利用時の被害

被害	内容
フィッシング･ID 窃盗	・ フィッシングサイトにより ID やパスワードを盗みとられる． ・ 端末の紛失･盗難によって端末に保存してある ID･パスワードを盗まれる．
架空請求	架空請求ページの表示．
ウィルス 1	ウィルスによってデータを削除される．
ウィルス 2	ウィルスによって情報漏洩してしまう．
ウィルス 3	ウィルスによって動作が妨害される．
盗聴	Cookie，ID，パスワード，個人情報などを盗みとられる

(c)　Web ダウンロード利用時の被害

被害	内容
フィッシング･ID 窃盗	・ フィッシングサイトにより ID やパスワードを盗みとられる． ・ 端末の紛失･盗難によって端末に保存してある ID･パスワードを盗まれる．
ウィルス 1	ウィルスによってデータを削除される．
ウィルス 2	ウィルスによって情報漏洩してしまう．
ウィルス 3	ウィルスによって動作が妨害される．
盗聴	ID，パスワード，個人情報などを盗みとられる

(d)　オンラインショッピング・バンキング利用時の被害

被害	内容
フィッシング･ID 窃盗	・ オンラインショップや金融機関になりすまされ ID やパスワードを盗みとられる． ・ 端末の紛失･盗難によって端末に保存してある ID･パスワードを盗まれる．
ウィルス 1	ウィルスによってデータを削除される．
ウィルス 2	ウィルスによって情報漏洩してしまう．
ウィルス 3	ウィルスによって動作が妨害される．
盗聴	Cookie，ID，パスワード，個人情報などを盗みとられる

3.3 発生する被害に対するセキュリティ対策

セキュリティ対策は文献調査[6][7]及びスマートフォンのセキュリティ対策セミナーへの参加によって調査した．その結果を付録に示す. 今回は対策の度合いを OS 側の対策，端末標準搭載の対策（対策レベル 1），無償のセキュリティ対策（対策レベル 2），有償のセキュリティ対策（対策レベル 3）の 4 段階に分け，対策の効果の評価を行うこととした．ここで，OS 側の対策とはユーザが使用の有無を選択できない機能・サービスを指す．ただし，キャリアや機種によって独自に行われている機能・対策は考慮していない．

3.4 端末・ＯＳによるセキュリティポリシーの違い

ヒアリング調査から PC，スマートフォン，携帯電話ではそれぞれセキュリティを確保するための方針であるセキュリティポリシーが異なるということがわかった．具体的には，携帯電話はクローズドなシステムであり，システムの自由度が低くセキュリティ対策の種類が少ない．しかし，第三者が攻撃する余地が少ないため被害が発生しにくく，ユーザが対策を行う必要性は少ない．一方，PC はオープンなシステムであり，システムの自由度が高くセキュリティ対策の種類が多様である．しかし，第三者が攻撃しやすくなるため被害が発生しやすく，ユーザが自ら対策を行う必要がある．スマートフォンは中間であり，OS ごとに異なる特徴を持つ．iPhone は携帯電話に近いクローズドなシステムとなっている．一方，Windows Mobile は PC に近いオープンなシステムとなっている． Android，BlackBerry は iPhone と Windows Mobile の中間のシステムとなっている．

4. オンライン機能・サービス利用時のリスク評価手法

情報漏洩に関する被害額を定量的に算出する式として日本ネットワークセキュリティ協会の損害賠償額算出式[8]が考えられるが，本研究で対象とする被害はその対象が情

報や金銭など多様であり，全ての被害について同一の指標によってリスクの定量的評価を行うことはできない．そこで，今回は定性的評価によってリスク評価を行った．リスク値は，情報セキュリティに関するリスクの定性的評価を行った文献[9]-[12]を参考に作成した以下の式を用いて求めた．

リスク値＝被害の大きさ×発生頻度×対策不備度

以下にこれらの要素の詳細について述べる．

4.1 被害の大きさ

情報に関する被害の大きさは日本ネットワークセキュリティ協会の損害賠償額算出式[8]における経済的損失レベルを参考に被害の大きさを 3 段階で評価した．表 6 に各情報の経済的損失レベルを示す．

また，情報以外に関する被害の大きさは，情報に関する被害の中で，同等の被害だと考えられるものの値とした．例えば，架空請求は最悪の場合は金銭的な被害が発生するため，被害の大きさを口座番号が漏洩する場合の値とした．

表 2　経済的損失レベル

経済的損失レベル	漏洩情報
3	口座番号と暗証番号， クレジットカード番号と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

4.2 発生頻度

被害の発生頻度は年間の被害の発生件数[13]-[18]をもとに 3 段階で評価を行った．表 7 に発生件数と発生頻度レベルを示す．ただし，スマートフォンに関しては，まだ普及段階であり，十分な被害データがない．そのため，スマートフォンは機能が PC に近いことから，将来的に PC と同等の被害が発生すると考え，スマートフォンの発生頻度レベルは PC と同一とした．

表 3　発生頻度レベル

発生頻度レベル	発生件数
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 （100 件～数 1000 件程度）
1	発生する可能性が低い（数件～数 10 件程度）

4.3 対策不備度

対策不備度は対策が為されていない度合いを示し，対策が為されるほど小さい値をとる．この値によってユーザが対策を行った場合のリスクの軽減度合いを評価した．対策不備度はセキュリティ対策評価モデル[19]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した．表 8 に対策不備度の評価基準を示す．また，対策レベルに関しては，上位のレベルの対策は下位のレベルの対策を行った状態であると考え，対策不備度の評価を行う．例えば，対策レベル 2 の場合，OS レベルの対策，対策レベル 1 の対策は行われているものとし，対策不備度の評価を行う．

ここで，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と考え，対策不備度 3 の「平均的な対策が為されている」は，「PC における対策レベル 1 の対策が全て為されている」場合とする．対策不備度 3 を基準にし，それぞれの対策の評価を行った．

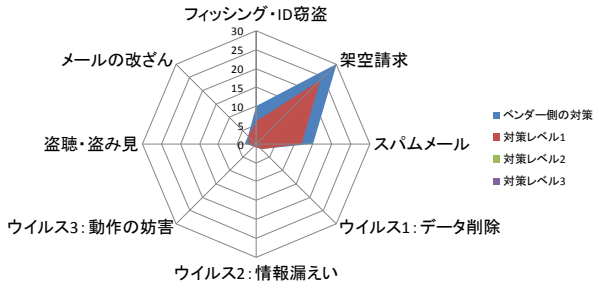
表 4　対策不備度

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，対策の余地もある
1	現状ではこれ以上の対策はできない

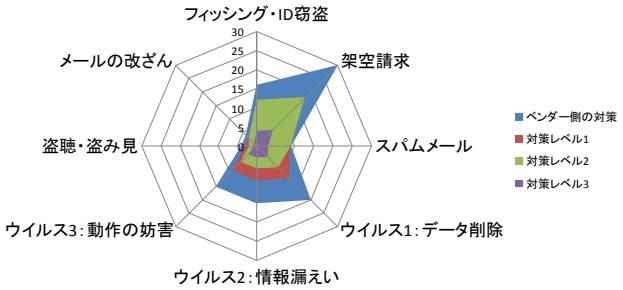
5 リスクの評価結果の可視化

3 章で解説した利用時に存在するリスクを 4 章で解説したリスク評価手法を用いてリスクを評価し，レーダーチャートを作成した．図 2 に一例として，電子メールについての結果を示す．レーダーチャートは OS ごと，機能サービスごとに作成し，対策レベルによって色分けして被害ごとのリスク値をプロットした．リスクが大きいほどプロットされる値が大きくなり，図形の面積は大きいものとなる．

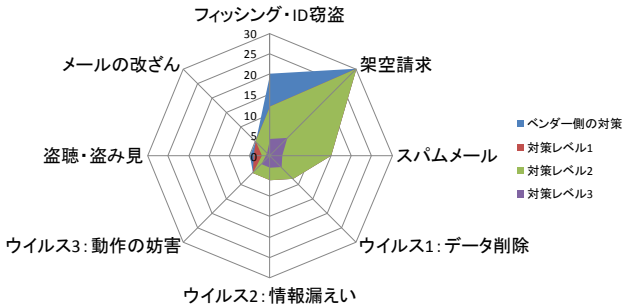
さらに，レーダーチャートと付録の対策表のセットをセキュリティ対策マップとし，ユーザが行いたい行為，使用する OS から現状のリスクを理解し，適切な対策をとるための支援材料とする．



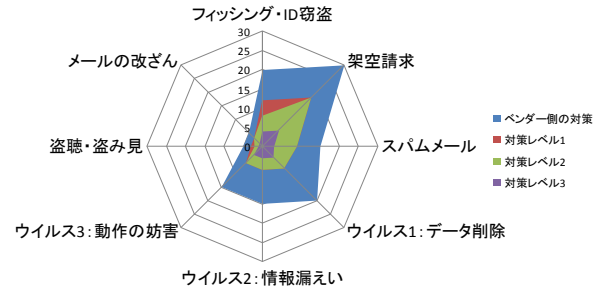
(a)携帯電話で行える対策によるリスク減少



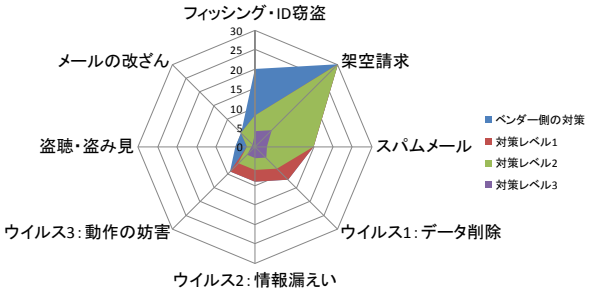
(b)PC で行える対策によるリスク減少



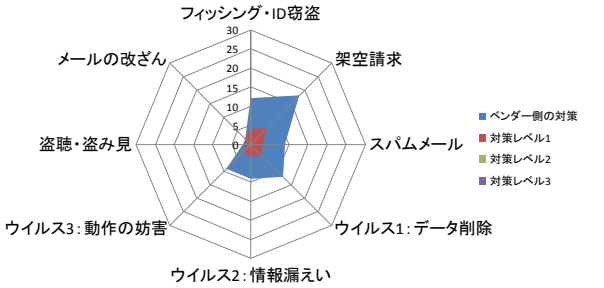
(c)iPhone で行える対策によるリスク減少



(d)Windows Mobile で行える対策によるリスク減少



(e)Android で行える対策によるリスク減少



(f)BlackBerry で行える対策によるリスク減少

図 2：電子メール利用における各端末・OS ごとのリスク

6　可視化結果に対する考察

本章では，5 章で作成したセキュリティ対策マップの結果について考察を行い，端末・OS ごとのリスクの特徴を見出した結果を示す．

6.1 携帯電話

クローズドなシステムのため，OS 側の対策の時点でリスクが小さく，そこからユーザが行える対策はほとんどない．特にウィルス被害については，OS 側の対策の時点でリスクが小さいことがわかる．フィッシングや架空請求については，リスクが大きいがユーザが行える対策はほとんどなく，ユーザ自身が気をつける必要がある．

6.2 PC

オープンなシステムのため，OS 側の対策の時点でリスクが大きいものも，ユーザが対策を行うことによってリスクが小さくなっていく．また，対策レベル 3 の対策まで行えば，全ての被害のリスクを小さくできる．

6.3 iPhone

クローズドなシステムのため，携帯電話に近い結果となった．クローズドなシステムにもかかわらず対策レベル 3 でリスクが小さくなっているのは，Apple が行っている MobileMe というサービスの影響が大きい．また，サンドボックス化が行われているため，ウィルス感染のリスクは小さい．

6.4 Windows Mobile

オープンなシステムのため，パソコンに近い結果となった．対策レベル 3 の対策まで行えば，全ての被害のリスクを小さくできる．

6.5 Android

システムは iPhone と Windows Mobile の中間くらいであるため，リスクは両者の中間のような分布になっている．また，iPhone と同じくサンドボックス化が行われているため，ウィルス被害のリスクは小さい．

6.6 BlackBerry

クローズドなシステムに近い結果となった．通信の際にサーバを経由しているため，安全性が保障されている．また，対策レベル 1 の対策を行えば十分にリスクが小さくなるため，無償，有償の対策があまり存在しない．

7 まとめ

本研究では，スマートフォン，ならびに比較対象として PC，携帯電話を対象として，ユーザがオンライン機能・サービスを利用する際に，どのようなリスクが潜んでいるか，また，それらのリスクに対してどのような対策をとることが出来るかといったことについて調査を行った．さらに，リスクの定性的評価を行い，オンライン機能・サービス利用時のリスクを可視化した．

最終結果として提示したセキュリティ対策マップは，オンライン機能・サービス利用時のリスク，またそのリスクの大きさ，セキュリティ対策によってリスクが減少する様子が直観的に確認できる図となっている．さらに，スマートフォンユーザに対しては，セキュリティ対策の重要性を理解し，自分で適切な対策行動をとるための支援材料となっている．

それに加え，作成したマップは，システムのオープン，クローズドといった特徴を表しており，3.4 節で解説した端末・OS によるセキュリティポリシーの違いと一致した．このことから作成したセキュリティ対策マップの妥当性が示されたと言える．

8 今後の課題

今後の課題として，以下の点が挙げられる．

マップの効果を確認するため，スマートフォンユーザに対して，リスクに対する理解度，セキュリティ意識についてのアンケートを行い，マップを見る前後でユーザのリスク理解，セキュリティ意識がどのように変化するかを調査する必要がある．

また，今回の研究では，セキュリティ対策として OS 側の対策，端末標準搭載の対策（対策レベル 1），無償のセキュリティ対策（対策レベル 2），有償のセキュリティ対策（対策レベル 3）に絞って可視化を行った．しかし，実際にはこの他にも，キャリア側の対策，アーキテクチャの違い等が考えられる．そのため，それらの情報の調査を行い，さらに調査結果を分かりやすくユーザに提示する方法について考慮する必要がある．

他にも，セキュリティ対策と利便性はトレードオフの関係にあるため，リスクとセキュリティ対策の関係だけではなく，セキュリティ対策による利便性の低下についても調査を行い，ユーザに対し，さらに多くの情報を提示することが望ましいと考える．

参考文献

[1] 一般社団法人モバイル・コンテンツ・フォーラム；ケータイ白書 2010

[2] 東亜日報；スマートフォンの悪質ウィルス韓国で初めて被害例
http://japanese.donga.com/srv/service.php3?biid=2010042344128（最終アクセス日　2010/09/20）

[3] SMobile Systems レポート

[4] トレンドマイクロ株式会社；セキュリティ最前線 2008 年 4 月 18 日号
http://jp.trendmicro.com/imperia/md/content/jp/threat/security-headline2008/security-headline_20080418.pdf（最終アクセス日　2010/09/20）

[5] 警察庁；被害事例と対処法
http://www.npa.go.jp/cyberpolice/case/pc/index.htm（最終アクセス日　2010/09/20）

[6] Symantec 製品情報
http://www.symantec.com/ja/jp/norton/360?inid=jp_ghp_link_norton_360v4（最終アクセス日 2010/09/20）

[7] セキュリティ機能比較
http://www.symantec.com/ja/jp/norton/360?inid=jp_ghp_link_norton_360v4（最終アクセス日 2010/09/20）

[8] 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

[9] 日本情報処理開発協会；ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC27001:2005)対応

[10] 宇佐美博；リスク分析とセキュリティ対策について，日本オペレーションズリサーチ学会

[11] 千葉昌幸，松本正雄；情報資産分布を活用したセキュリティ対策実施計画モデルの提案，電子情報学会，信学技報，SWIM 2001-5

[12] 沼田雅巳；情報セキュリティ対策予算配分の意思決定～被害額算出とリスク分析

[13] IPA;情報セキュリティ白書 2010 速報版

[14] フィッシング対策協議会；月次報告書
http://www.antiphising.jp/capj-report/（最終アクセス日　2010/09/20）

[15] 警察庁；ハイテク犯罪等に係る被害状況
http://www.npa.gojp/cyber/research/h14/image/higaicyousa.pdf（最終アクセス日　2010/09/20）

[16] 日本産業協会；迷惑メールの統計
http://www.npa.gojp/cyber/research/h14/image/higaicyousa.pdf（最終アクセス日　2010/09/20）

[17] 国民生活センター；相談事例・判例
http://www.kokusen.go.jp/soudan_topics/data/kakuseikyu.html（最終アクセス日　2010/09/20）

[18] 総務省；不正アクセス行為の発生状況
http://www.soumu.go.jp/main_content/000056408.pdf（最終アクセス日　2010/09/20）

[19] 電子商取引推進委員会；セキュリティ対策評価モデル

付録　セキュリティ対策一覧

(a) 携帯電話

	対策	内容
OS側の対策	ネットワークアクセスセキュリティ	暗号化された通信を用いる.
	利用データ・容量制限	端末で利用するデータや容量を制限しているためウィルスに感染しにくい.
対策レベル1	デバイスロック	端末の使用を制限する.
対策レベル2なし		
対策レベル3なし		

(b) PC

	対策	内容
OS側の対策	Direct access	認証され，暗号化された通信を用いる.
対策レベル1	Windows defender	スパイウェアの侵入を防ぐ.
	ファイアウォール	外部との通信を制御
	UAC	管理者権限が必要な操作を行う際に許可を求める
	WFP	ファイアウォールの一部の機能を開発中のアプリに統合
	DNSセキュリティ拡張	受信データの真正性検証
	BitLocker	ドライブの暗号化
対策レベル2	常駐監視	ウィルスの感染を監視
	ウィルス駆除	端末内のウィルスを駆除する
	スパイウェア駆除	スパイウェア駆除する
	メールスキャン	メールと添付ファイルを検査
	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.
	悪意のあるサイト警告表示	悪意のあるサイトへの接続時の警告を表示する.
	データ実行防止	ウィルスを動作させない
対策レベル3	Xss対策	Xss攻撃を防ぐ
	リモートワイプ	遠隔でデータを削除する.
	ウィルススキャン	端末内のウィルスをスキャン
	URLフィルタリング	危険なサイトを未然にブロック
	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
	スパムメールフィルタ	スパムメールを抑制する
	バックアップ	PCと同期し，データをバックアップする.
	セキュリティキーボード	IDやパスワードを画面上のキーボードで操作することで
	キー入力暗号化	キーボードで入力した内容を暗号化して送信

(c) iPhone

	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.
	アプリの検閲	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

(d) Windows Mobile

	対策	内容
OS側の対策なし		
対策レベル1	デバイスロック	端末の使用を制限する.
	バックアップ	PCと同期し，データをバックアップする.
	ウィルススキャン	端末内のウィルスをスキャン
	ファイアウォール	外部との通信を制御
	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	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
	アプリの使用制限	アプリの端末へのアクセスを制限
	バックアップ	PCと同期し，データをバックアップする.
	データのパスワード保護	端末内のデータをパスワードによって保護
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
	スパムメールフィルタ	スパムメールを抑制する
	バックアップ	PCと同期し，データをバックアップする.

(e) Android

	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.
対策レベル1	パターンロック	端末の使用を制限する.
対策レベル2	遠隔ロック	端末紛失時に遠隔で端末をロックする.
	バックアップ	PCと同期し，データをバックアップする.
	ウィルススキャン	端末内のウィルスをスキャン
	デバイス探索	紛失時に端末を発見する
対策レベル3	リモートワイプ	遠隔でデータを削除する.
	ウィルス駆除	端末内のウィルスを駆除
	デバイス探索	紛失時に端末を発見する
	スパムメールフィルタ	スパムメールを抑制する
	ファイアウォール	外部との通信を制御
	遠隔ロック	遠隔操作で端末の使用を制限
	バックアップ	PCと同期し，データをバックアップする.

(f) BlackBerry

	対策	内容
OS側の対策	メール自動暗号化	メールを暗号化し，盗聴，改ざんを防ぐ.
	サーバ経由(BIS)	通信情報がすべて独自のサーバを経由する
対策レベル1	デバイスロック	端末の使用を制限する.
	遠隔ロック	端末紛失時に遠隔で端末をロックする.
	リモートワイプ	遠隔でデータを削除する.
	ウィルス駆除	端末内のウィルスを駆除
	スパムメールフィルタ	スパムメールを抑制する
	アプリの検閲	アプリの動作確認
	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.
対策レベル3なし		