JAPAN SMARTPHONE SECURITY ASSOCIATION

一般社団法人日本スマートフォンセキュリティ協会

-スマートフォンを安心して利用出来る社会へ-

利用ガイドラインのリリース報告と今後の活動 について

2012年5月24日

利用部会　利用ガイドラインWGリーダー 松下綾子

(アルプスシステムインテグレーション株式会社)

アジェンダ

(1)　2011年度の活動報告
(2)　利用ガイドラインの基本方針
(3)　利用ガイドラインのポイント
(4)　2012年度の活動予定

2012 Copyright (C) JSSEC

2011年度の活動報告

利用ガイドラインのリリース報告

『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン』

【β 版】　：2011年　8月31日
【第一版】　：2011年　12月1日
【英語版】　：2012年　3月30日

http://www.jssec.org/dl/guidelines2011_v1.0.pdf

ご協力ありがとうございました。

2012 Copyright (C) JSSEC

利用ガイドラインの基本方針

目的

・スマートフォン業務活用検討者/導入決定者の皆さんに
「気付いて」いただき、将来の判断基準となるよう構成。

「こういうことがしたい」→「こういうリスクがある」→「解決するためには」

対象

・OS ：iOS、Android、 BlackBerry OS、Windows Phone 7
・スマートフォンの資産形態：
①会社資産
②個人所有 (BYOD：Bring Your Own Device)
・PCとの違い (スマートフォンらしさ) に焦点

2012 Copyright (C) JSSEC

作成経緯～ガイドライン策定プロセス

骨子となる項目の精査

- 機能面（ツール）　⇒　詰めると利用シーンに。
- 機密度、構成要素　等　（PCと同じになってしまう）
  = 情報セキュリティの観点
  - 脆弱性、脅威から　⇒　詰めると利用シーンが最初に。
  - 利用シーンから　⇒　○
  - スマートフォンらしさ　⇒　○

骨子項目の一覧表示

利用シーン　⇒脅威　⇒リスク　⇒対策　⇒要件

2012 Copyright (C) JSSEC

作成経緯～内容の詰めと確認

内容精査

- スマートフォンらしい利用シーンの側面を複数検討
- 各もくじに属する項目情報洗い出し ⇒一覧表作成
  - 実装方法の違いによるシーンの違いは、割愛
  - SNSの活用やマーケティングツールとしての利用方法は、市場背景や特性の章、またはアプリケーションの項で記載

英語化

- 「日本市場がターゲット」の明確化
- 日本語特有のニュアンス表現に一苦労
- 海外現地法人を持つユーザへアナウンス

2012 Copyright (C) JSSEC

第一版のもくじ　(2011/12/1版)

2012 Copyright (C) JSSEC

第一版のもくじ　(2011/12/1版)

5章. 利用シーンから見る脅威と対策

5.1. アドレス帳を利用する
5.2. 電話を利用する
5.3. メールを利用する
5.4. スケジュールを利用する
5.5. ブラウザを利用する
5.6. ネットワークに接続する
5.7. 社内ネットワークを利用する
5.8. 組織契約のSaaS/ASPを利用する
5.9. アプリケーションを利用する
5.10. デバイスの機能を利用する
5.11. データの可搬媒体として利用する
5.12. バックアップを取る/同期する
5.13. [参考] ｲﾝﾀｰﾈｯﾄｽﾄﾚｰｼﾞｻｰﾋﾞｽを利用する
5.14. [参考] SNSを利用する

6章. ライフサイクルから見る脅威と留意点

6.1. 計画
6.2. 導入
6.3. 運用
6.4. 廃棄

7章. おわりに

7.1. 利用目的とセキュリティのバランス
7.2. 組織のセキュリティポリシーと意思決定
7.3. 情報収集継続の必要性

8章. 用語解説・付録

・特性別 / 利用シーン別 対策チェックシート
・手順書に記載する項目の例
・誓約書に記載する項目の例
(法人所有/BYOD)

2012 Copyright (C) JSSEC

チェックシート/手順書/誓約書のイメージ

付録 A

A-1 特性別 対策チェックシート

推奨レベル：■強く推奨 □推奨

虫眼号	分類	脅威	対策 または 関係	推奨レベル
4.2	特性から見る脅威	デバイスの盗難、紛失	・デバイスをロック設定する。 ・ロック解除失敗時に強制的にデータを消去する。 ・本体および外部記憶媒体のデータ領域を暗号化する。 ・ユーザ ID やパスワードを非保存設定にする。 ・定期的にデータのバックアップをとる。	■ ■ □ □ □
		SIM カードの盗難	・通信事業者へ連絡し回線利用を停止する。	■
		水没や落下による故障	・定期的にデータのバックアップをとる。 ・落下防止用ストラップ等を装着する。 ・防水や耐衝撃性の高いデバイスを選択する。	□ □ □
		覗き見	・覗き見防止シート等を装着する。	□
		無線脆	・慎重に操作するよう注意を喚起する。 （静電容量方式を採用したパネルが多いため、静電気の影響を受けやすい）	□
		脆弱性	・デバイスや OS の種類を絞り込む、または統一する。	□
		信頼できないマーケット	・信頼できるマーケットからアプリケーションを入手する。 ・アプリケーションのインストール時に不用意にアクセス許可をしない。 ・アプリケーションに関する最新情報（不正な動き、意図しない動き、信頼できる情報等）を入手する。 （5.9 節「アプリケーションを利用する」参照）	■ □ □
		利用者による改造	・改造を禁止する。	■

A-2 利用シーン別 対策チェックシート

推奨レベル：■強く推奨 □推奨 －対象外

虫眼号	分類	脅威	対策 または 関係	推奨レベル
5.1	アドレス帳を利用する	無操作 知識不足	・手順書を作成する。（付録参照） ・アプリケーションの動き（データ保存場所、データの公開範囲等）を調べる。 ・業務専用の保存場所を決める。 ・利用者には保存場所を選択させないようにする。	－ □ □ □
		プライベートデータの保存【BYOD】	・誓約書にサインさせる。（付録参照） ・データを区分する（プライベートと業務の保存場所の区分）。 ・退職時、利用終了時には全ての業務データの保存場所に対し、データを削除したことを明示させる。	－ □ ■
5.2	電話を利用する	盗聴	・VoIP を利用する際には、通信経路を暗号化する。	□
		不正利用	・IP PBX サーバの機器やサービスを正しく設定する。	□
		不正アクセス	・IP PBX サーバにパスワードを設けるなど周囲環境のセキュリティ強化を行う。デバイスを登録する。	□
		私的利用	・手順書を作成する。（付録参照） ・通話履歴を取得する。	－ □
5.3	メールを利用する	不正利用	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・Web メールなどデバイスにデータを残さないメールを使う。 ・本文や添付ファイルを暗号化する。	－ － □ □
		無操作	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・ファイルの添付は禁止し、別手段を用意する。 ・本文や添付ファイルを暗号化する。 ・サーバにデータを残して原本を保存する。	－ － □ □ □

A-4 誓約書に記載する項目の例

A-4-1 法人所有版

推奨レベル：■強く推奨 □推奨

分類	項目	概要（ねらい）	誓約書作成上の注意事項	推奨レベル
利用目的の明示	利用目的と範囲の明確化	スマートフォンの利用目的、利用範囲などを明記し組織の定めたルールの順守を維持する。		■
管理	組織による情報収集に対する個人の承諾（情報収集、監視などを行う場合）	不正な利用防止やマルウェア感染防止などから、スマートフォンの利用状況の収集を行うことを合意する。	スマートフォンは常時携帯するため、位置情報などを取得する場合には、「プライバシーの侵害」に注意して文章を作成する。 システム的な情報収集および、管理者による情報確認、どちらも含む。	■
	組織による制御に対する個人の承諾（制御、OS のアップデートなどを行う場合）	設定変更、機能制限やデータ削除を組織として行うことを合意する。	OS やアプリケーションのアップデートは、組織が管理する。 システム的な制御および、管理者による設定変更、利用者への設定指示なども含む。	■
	バックアップデータの保護	機密情報などの保護のため、個人所有 PC へのバックアップの禁止などを合意する。		□
届け出	特定の事象が発生した場合の届け出	紛失や盗難などが発生した場合、機密情報や個人情報の保管有無や、事故の影響を確認するため、速やかに届け出ることを合意する。	組織の定めたルールに従って届け出をする。 例：「破損」「故障」「不具合」「盗難」「紛失」など	■
禁止事項	端末、OS、アプリケーションの改造	セキュリティ上の脆弱を防止するため、改造しないことを合意する。		■
	端末メーカー、通信事業者の利用規約に対する違反行為	提供元の意図に反する利用は行わないことを合意する。		□
	組織の許可しないアプリケーションの導入	マルウェアなどの侵入を防ぐため、許可されたアプリケーション以外を導入しないことを合意する。	導入して良いアプリケーション（ホワイトリスト）又は、導入してはいけないアプリケーション（ブラックリスト）などを別途定める。	□
	私的利用	コストの増加や業務生産性低下、情報漏えいなどを防ぐため、私的利用しないことを合意する。		□
	第三者への貸与、譲渡、販売	本人以外の利用を禁止することを合意する。		□
	放置または過失による情報漏えい	データを持ち歩くことや個人の発信機会が増えるため、注意を喚起する。情報漏洩時には、企業ポリシーに従い対処する。	企業情報書き込み等への制限、不用意な情報拡散及び漏洩に十分注意する旨を明記する。	□
利用の終了	端末の返却	情報の削除、端末の回収を実施することを合意する。	データのバックアップ取り扱い、返却のルールは別途手順とする。	■
誓約への違反	罰則規定	組織の定めた罰則規定の適用対象となることを明示する。		□

2012 Copyright (C) JSSEC

利用シーンからの考察例

アドレス帳

- 電話、メール、SNS、インスタントメッセージなどの**入り口**として利用する機能や、利用履歴を記録する機能**＝出口**を持つ。
- データの**保存場所は、デバイス、外部記憶媒体、外部サービス**を選択可能。
- 外部サービスでは、**他者と共有**するサービスあり。
- 保存場所は利用者に分かりにくい。
- **アプリケーションの動きを調べて注意を喚起することが推奨される。**
  Androidの場合、アプリケーションをマーケットからダウンロードする際に、アプリケーションが**適切なアクセス許可**を求めているかも重要。

可搬媒体

- スマートフォン本体をデータ移動媒体として利用する場合をさす。
- 機能の一面として**大容量のストレージ**である。
- 紛失時の影響度は、PC同等。
- デバイスやアプリケーションによっては、セキュリティ対策も可能だが、紛失時の対策は必須。
- 可搬媒体としての**使用は推奨しない。**

2012 Copyright (C) JSSEC

大切なポイント

1．スマートフォンの 特性 を押さえておく。

◆スマートフォンの機能は、本来すべてアプリケーション
◆パーソナライズがすごく簡単
◆携帯性、利便性、ネットワーク常時接続性、機能性、拡張性、柔軟性が高い

2．スマートフォンの サービスモデル を理解しておく。

◆個人裁量型のツール
◆OSやデバイスの提供元による違いがある
◆PCと違う点がある～できること、できないこと（機能、セキュリティ）

3．セキュリティのポイントは、三要素に相互依存する。

端末の特性

例えば
紛失や盗難
パーソナライズ
海外仕様モデル

アプリケーション の特性

例えばバージョンアップ や Permission

ネットワーク の特性

例えば 多経路の存在
テザリング

2012 Copyright (C) JSSEC

PCとも携帯電話とも違う管理スタイル

管理＝ライフサイクルのＰＤＣＡ

計画
目的を明確化する
- 社内ルールを整備する
- 利用マニュアルを整備する
- サポート体制を整備する
  (ヘルプデスクや担当設置)
- 教育を実施する

導入　PCとは手順が変わる

- 利用開始手続きを行う
- 備品を用意または装着する
- アカウントを取得する/させる
- デバイスを初期設定する
- デバイスのロック機能を有効にする
- メールアドレスを取得/設定する/させる
- アプリケーションを導入する
- デバイスを配付する

運用　先回りして考える
- デバイス情報を収集/監視する
- デバイスの機能を制御する
- OSのバージョンを管理する

廃棄　データを削除する

- デバイスの回収/廃棄、変更
- 別部署への使いまわし

PDCAをまわしましょう

2012 Copyright (C) JSSEC

まとめ～より良い活用とセキュリティを！

1．**利用目的**を明確化する
- セキュリティ範囲の特定

2．脅威と対策要件から**バランスのとれたセキュリティ**を選択する
- 無理無駄の排除
- 統一されていないOSやデバイスの状態への配慮

3．管理面では**プライバシーの侵害**に配慮し（誓約書作成等）、**ライフサイクルと既存インフラを意識**する
- 特性の理解
- 利用者への配慮、
- 既存インフラの有効活用

ワークスタイルの変革につなげましょう

「さぁ、スマートフォンしましょう！」

2012 Copyright (C) JSSEC

適切なセキュリティ確保のために

スマートフォンは
拡張性や発展性が高く利用者のモチベーションをアップします

でも！

- 黎明期でありセキュリティは完全には担保できません。
- PCのような標準化はされていません。
- 常に日進月歩であるため情報収集の継続をお願いします。

「運用でカバーする」
「利用目的を変える」
「リスクを敢えて受容する」
「今は導入しない」

…という選択も必要です。と、お伝えしています。

2012 Copyright (C) JSSEC

2012年度の活動予定

WGの活動予定とスケジュール

Step.1　～2012.5　**啓蒙活動対応中**
各種セミナー講師など

Step.2　2012.6～　**現状の課題洗い出し**
→ 例：不足部分の補足資料作成
＝6月にWG開催予定＝

Step.3　～2013. 1（？）
利用ガイドライン本編の第二版対応

2012 Copyright (C) JSSEC

ご清聴ありがとうございました。

これからもご協力よろしくお願いします！

2012 Copyright (C) JSSEC