

スマートフォン法人利用のための セキュリティの考え方とBYODの考察

2012年11月21日

**JSSEC 日本スマートフォンセキュリティ協会
利用部会 利用ガイドラインWGリーダー**

ALSI アルプスシステムインテグレーション株式会社
営業統括部 特販プロジェクト グループマネージャー

松下綾子

もくじ

1. はじめに
2. セキュリティのポイント
3. 管理のポイントとBYODの心得
4. おわりに

1. はじめに

利用部会 利用ガイドラインWG活動報告

『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』リリース報告

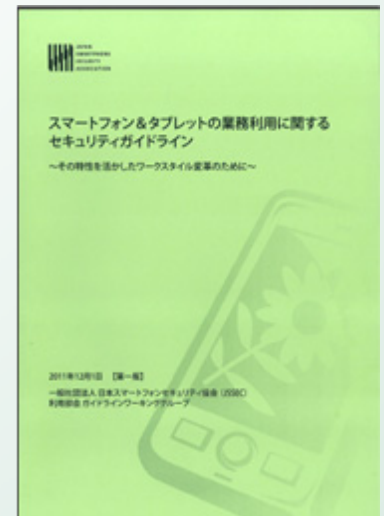
■現在の発行資料一覧 ※【β版】【第1版】は掲載終了

1. 【第1版 英語版】：2012年 3月30日
2. 【BYOD基礎資料】：2012年10月26日
3. 【第一版+BYOD資料収録版】：同上

多くのご意見ご協力
ありがとうございました

■ガイドラインタスクフォース（+WGの皆さん）

- 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）
メンバー相原 弘明（株式会社ネットマークス）
浅井 奈津樹（アイ・ティー・シーネットワーク株式会社）
片岡 進一郎（凸版印刷株式会社）
北村 裕司（サイバートラスト株式会社）
後藤 悦夫（トヨタ自動車株式会社）
高橋 竜平（NTTコミュニケーションズ株式会社）
西原 敏夫（シスコシステムズ合同会社）
牧野 俊雄（株式会社ネクストジェン）
松本 照吾（株式会社インフォセック）（氏名五十音順）



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/導入決定者の皆様に「気付いて」いただき、将来の判断基準となるよう構成しています。
- ・ 情報セキュリティの考え方の前に、注目したいスマートフォンの特性に焦点を当てています。

「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

新環境への身支度～変革が求められる時代

■ スマートフォン→モバイルデバイスの役割



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！

2. セキュリティのポイント

その前に～現状把握

■ 組織では何が起きているのか？

P Cへの対策を中心としたセキュリティは
きっちり実施してきた、はず。

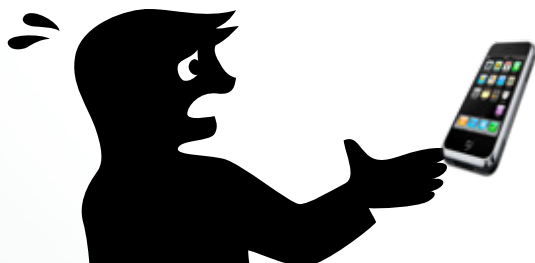
- ①社内でのP C利用時は、発信規制されている。
(メール、We b、USBメモリ、その他デバイスいろいろ)
- ②P Cを持ち出す際は申請が必要で、個人のものは持ち込めない。
- ③携帯電話でさえ、カメラの規制など行ってきた。

**ガチガチなはずなのに、
もしかしてスマートフォン使われている…？
スマートフォンには、期待と不安が！**

重複セキュリティではなく必要なセキュリティを！

■ 漠然とした不安。新しい手口の脅威

不安払拭のために利用目的をよく考えましょう



- ④ データはどこに？ 保存場所が、よく分からない！
- ④ アプリケーションDL？ マーケットの信頼性って？
- ④ マルウェアって？ ウイルス感染方法がPCと違う？
- ④ アプリケーションが問題になってる？ 不正アプリって？

スマートフォン活用の目的に合わせ、必要なセキュリティを
選択 するための **指標** を身につける必要があります！

スマートフォンとは？

■ それはモバイルP Cとはどう違う？

PC？ 携帯電話？

スマートフォンは新しいサービスモデル

特性	PC	携帯電話	スマートフォン
OSの 管理者権限	解放	解放されていない	解放されていない (例外あり)
ネットワーク セキュリティ	利用者自身 で対策	キャリアで 対応	利用者自身で 対策
機能の実装	すべての機能 をアプリケーション として実装	基本機能として 実装	すべての機能 をアプリケーション として実装
機能の追加	利用者が 各種方法で 導入	キャリアが 提供	マーケットが 提供

- ★一般市民は電話の後継として購入。
- ★PCに近い、高機能な電話。
- ★PCよりも直感的に操作できる。
- ★パワーポイントは作れない。
- ★長時間使うと疲れる。電池も切れる。
- ★フルブラウザとメールとSNSが得意。
- ★時間と場所を越える能力はPCより高い。
- ★

両方合わせて「スマートフォン」
としています。



今は、第三のツール
として捉える

どうしてスマートフォンを使うのか？

■ 当たり前と思わず、違いを意識する

持ち運びやすい。
いつも一緒なので備忘録に！

常に電源ON！

インターネット
が
手帳になった！

いつもネットワークが使える！

使いやすいように
自分流も簡単！

コミュニケーションの活性化

意思決定の迅速化

コスト削減

生産性向上

事業の発展

事業継続性の確保

顧客満足の上



特性からみた考察①

■ アプリケーション利用時のモデル

- アプリケーションは、マーケットからダウンロードする。
- 基本的に、各アプリケーションは他のアプリケーションに干渉できない。
- アプリケーションをダウンロードする際、利用者のアクセス許可 (Permission) が必要。～Android



特性からみた考察②

【脅威とリスクへの対策一覧】

脅威	解説(リスク)	対策 または 要件
デバイスの盗難、紛失	・ デバイスに保管された情報が漏洩する。 ・ 情報の漏洩範囲が、外部サービスに至る恐れがある	・ 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	・ 電話番号や固体識別番号等が悪用される。	・ 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	・ データが消失する。	・ 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	・ 情報が漏洩する。	・ 覗き見防止シート等を装着する。
誤認識	・ タッチパネルの反応範囲や反応速度により操作ミスを招きやすい。	・ 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）

特性からみた考察③

脅威	解説(リスク)	対策 または 要件
脆弱性	デバイスの種類が多くOSの実装にばらつきがあり、パッチを適用しにくい。	デバイスやOSの種類を絞り込む、又は統一する。
信頼できないマーケット	- アプリケーション導入時の不用意なアクセス許可によるマルウェアの感染 - アプリケーションのマルウェア化（初回のアクセス許可によるバージョンアップ時のユーザ承認すり抜け）	- 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。
利用者による改造	OSの改造（root化、Jailbreak）によるマルウェアの感染	改造を禁止する。



スマートフォンらしい利用シーンは？

■ ポイントは、データの流れと保管場所



利用シーンからの考察①

■ アドレス帳（SNSとの連動）

- 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。
- 氏名、電話番号、複数メールアドレス、SNSアカウント等、従来より多くの個人情報を含む。
- 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く、意図しない場所への保存をしてしまったり、外部サービスへ自動同期されることもある。
- **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。

アプリケーションの適切な利用と、保存先や同期設定の管理が必要

利用シーンからの考察②

■ 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。**

■ ストレージ・SNS

- スマートフォンからの利用は、その**特性のため増加**。利用時は手順の明確化が必要。
- 不用意な書き込み、不正なデータ転送、誤った情報公開、携帯性によるGPSや写真による場所特定など、脅威も高まりつつある。
- **指定サービス以外の利用禁止、ルール策定、メディアリテラシー向上策等が推奨される。**

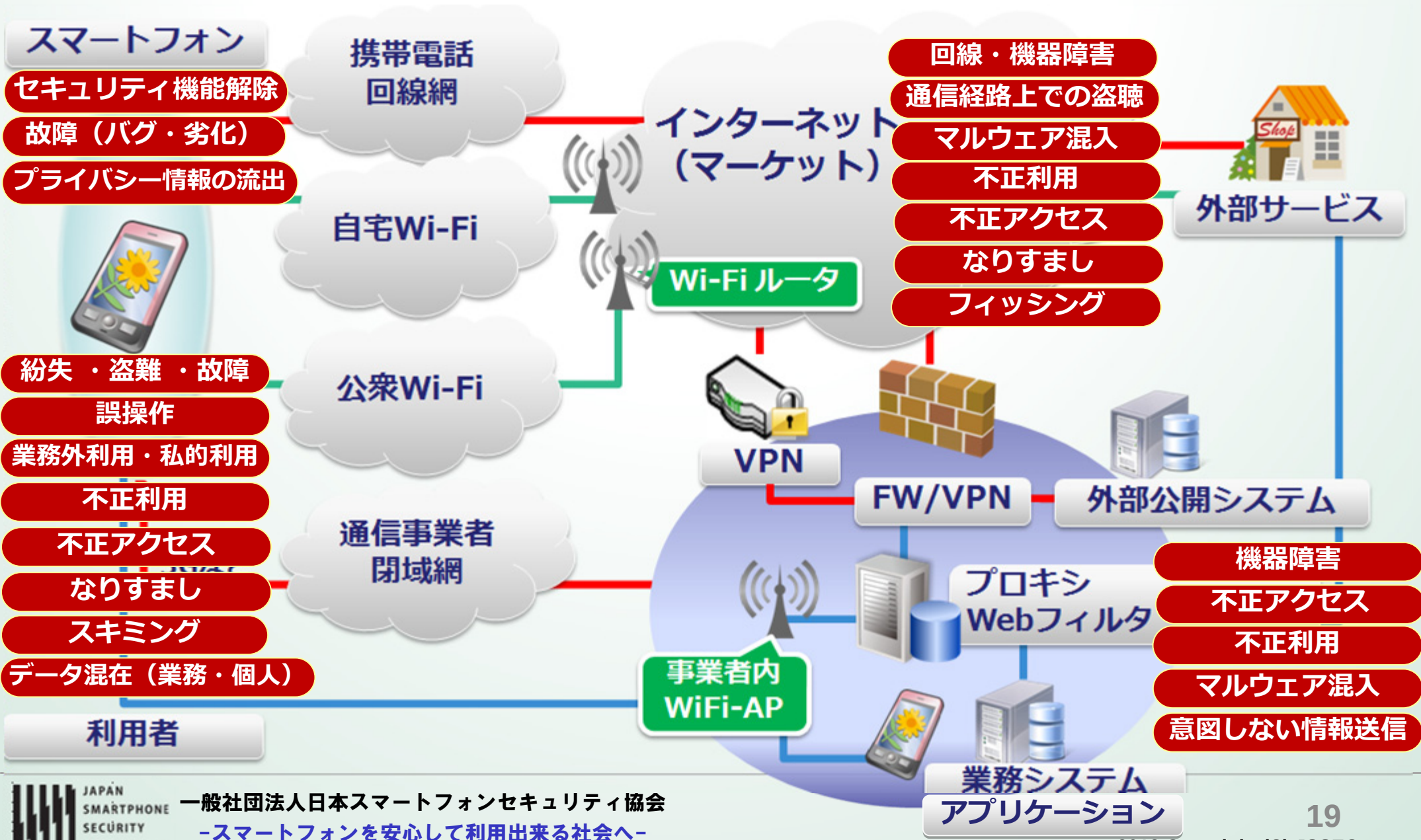
利用シーンからの考察③

■ ネットワーク

- 携帯電話回線と、Wi-Fiを利用できる。=利用者は、どこにいてもどこからでも、意識せずにスマートフォンを利用できる。
- スマートフォンからのアクセス先は、社内システム・VPN・通信会社の専用線、閉域網など多種多様。
- 最近は、公衆Wi-Fiが増加。
- 便利な分だけ危険も潜む。
- 不正なA P（アクセスポイント）もあると考えられ、予期せず情報が盗まれている可能性あり。
- テザリング機能により誰でもA Pを作れる。
- **テザリング利用は注意が必要。**
- 将来は、社内・社外という概念ではなく、常駐端末・モバイル端末という概念が強くなると考えられる。



利用可能なネットワークと 全体的な脅威の想定(イメージ)



大切なポイント

1. スマートフォンの**特性**を押さえておく必要がある。

- ◆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**



2. スマートフォンの**サービスモデル**を押さえておく。

- ◆**個人裁量型**のツール
- ◆OSやデバイス毎の違いやP Cとの違い～できること、できないこと。

3. セキュリティのポイントは、**三要素に相互依存**する。

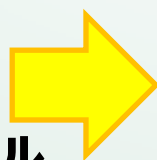
- ◆スマートフォンの利用シーンに潜む脅威は、複雑に絡み合って存在する。



電話



スケジュール



端末の特性

アプリケーション
の特性

ネットワーク
の特性

3. 管理のポイントとBYODの心得

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 P D C A

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



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

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

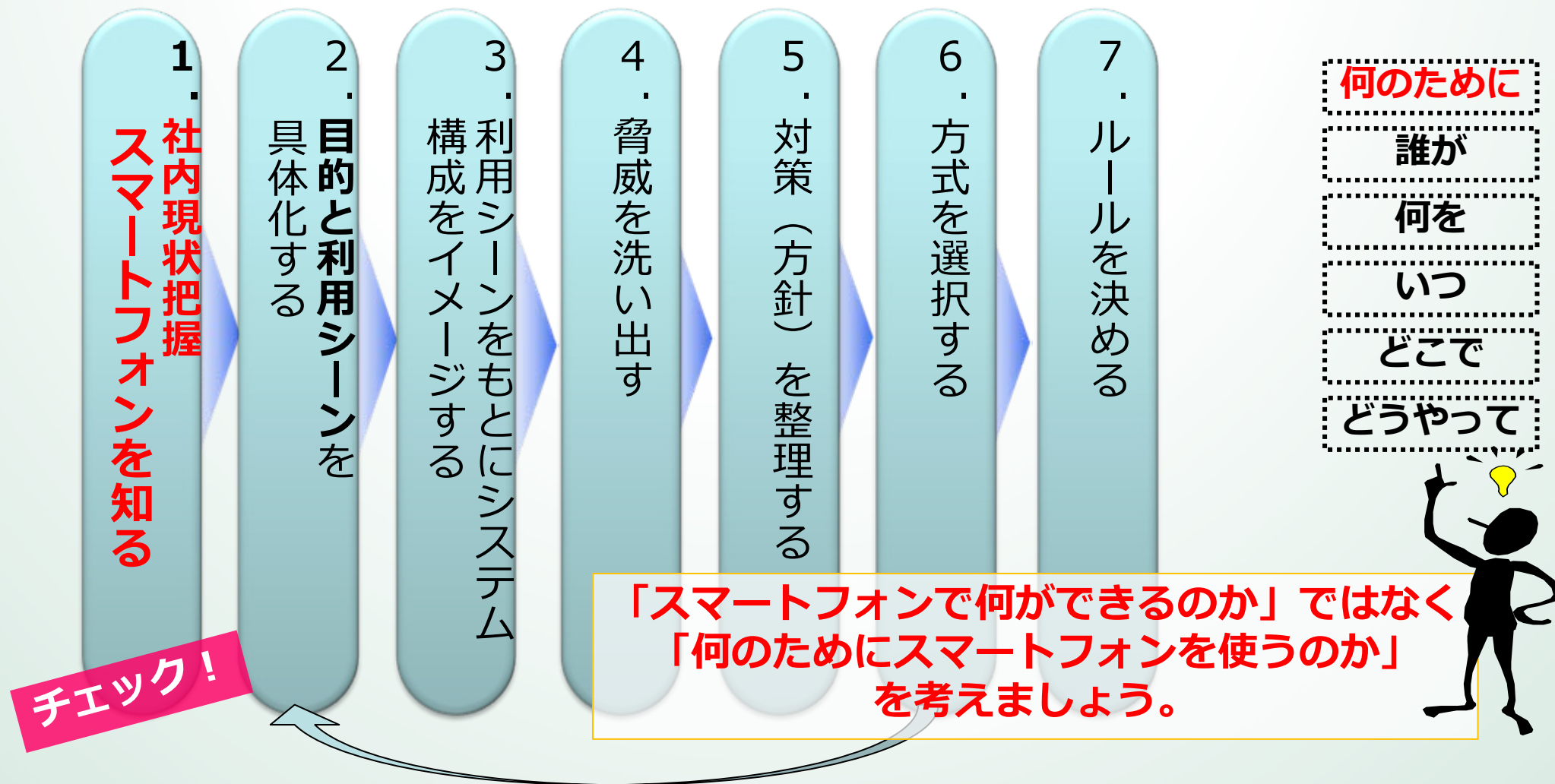


運用 先回りして考える

- ・ 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

「計画」段階での留意事項

■ 検討ステップ



この頃よく聞く「BYOD」って？

「BYOD」「私物解禁」とは、
個人所有のスマートフォンを
業務で利用許可する利用形態。

(BYOD : Bring Your Own Device)

※JSSECの立場は、賛成反対ではなく、
そのような方法があるという提示です。



NO!! ...
でも本当は興味がある。



利用者と管理者の
「思いの一致」が不可欠

効率化と費用の低減

モバイルファースト時代への対応

人の行動や発想の可能性への機会

使い慣れた端末を使いたい

いつでも災害時に備えたい

管理者

利用者

個人所有スマートフォンの 業務利用パターン

BYOD

■ 一般に「BYOD」と捉えられている状況の考察

パターン 分類項目	舵取り型	踏み出し型	なし崩し型	知らん振り型	忍び型
所有形態			個人所有		
利用目的			業務利用と個人利用の併用		
利用場所			問わない		
管理者のリスク認識	あり	あり	あり	なし	「舵取り型」と 「BYOD禁止」 の場合に存在
導入の意向	あり	あり	決めていない	考えていない	
導入の意思決定	あり	あり	なし	なし	
規定	あり	なし	なし	なし	
規定に基づく許可	あり	なし	なし	なし	

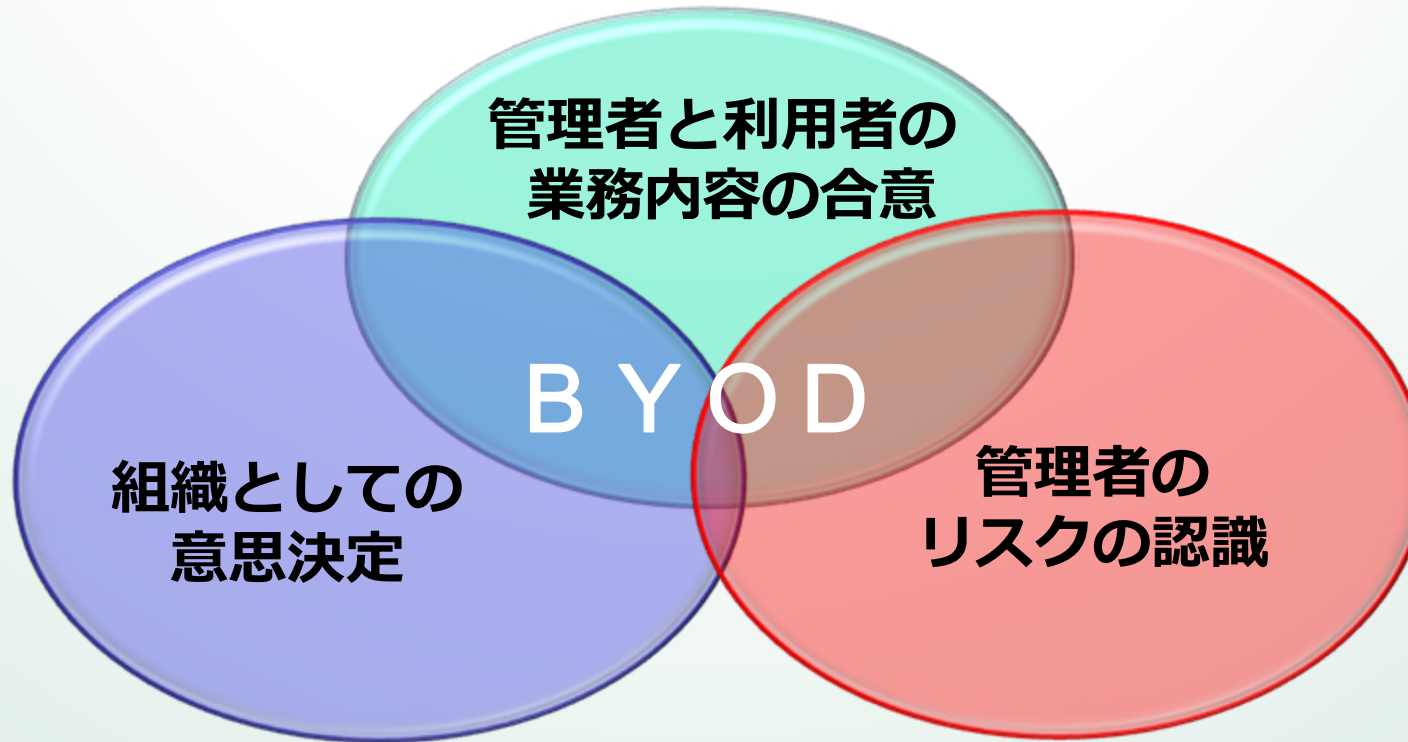
↑ 推奨BYOD

↑ ---BYOD

!!

■ BYODの定義

リスクの認識をした上で、
個人所有のスマートフォンの業務利用について
組織として意思決定を行い、実際に業務を行うこと。



■ 個人の意志の尊重

個人が利用開始していることを意識する

- ◆ デバイスの状態（OSのバージョン等）は、千差万別。
- ◆ 利用者が個人的に使っているアプリケーションやサービスの利用禁止は、困難である。
- ◆ 資産管理（有償アプリケーションの所有や管理、紛失時のデータ削除等）には、精査が必要である。
- ◆ デバイスが最初にインターネットに接続するネットワークは、制限できないと考えられる。

■ 目的の明確化とBYOD特有の管理プロセスの実行

BYODの開始と終了（期間＆業務時間）を意識する

- ◆ 申請／承認／終了手続き
利用者、管理者双方への意識付け
- ◆ 規定の策定
業務範囲、業務時間の考え方や費用負担などの検討
- ◆ 利用者のプライバシーへの配慮
終了後の個人情報消去など、プライバシー侵害の回避
- ◆ 戦略的なBYOD
BYOD導入ならきっちり導入、禁止なら禁止、の明確化

最低限、気をつけておきたいこと

■ セキュリティ～すぐに確認！

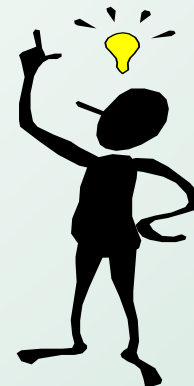
- ◆ パスワードロック
- ◆ ロック解除失敗時のローカルワイプ（データ削除）
- ◆ 紛失時の連絡先通達（企業内管理者／通信事業者）

■ 利用者教育

- ◆ 携帯電話ともPCとも違う操作性
- ◆ まずは、小さな一歩から。（慣れる）

■ PCとの違いを意識した管理

- ◆ 管轄部門同士の連携
- ◆ OSのアップデートと機能追加への配慮
- ◆ 廃棄や使いまわしなど変化のあるときの対応
- ◆ 業務利用に不要な機能が実装されたデバイスの認知



利用ガイドライン付録の チェックシート/手順書/誓約書イメージ

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 ○推奨

番号	分類	脅威	対策 または 対策	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自動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 やパスワードを暗号化して保存する。 ・定期的にデータのバックアップをとる。	■ ■ □ □ □ □ □
		RFID カードの盗難	・適宜事業場へ連絡し印刷利用を停止する。	■
		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。	□ □ □
		電磁波	・電磁波防止シート等を貼付する。	□
		断電時	・慎重に操作するよう注意を喚起する。 (充電容量方式を採用したパネルが多いため、充電電圧の影響を受けやすい)	□
		脆弱性	・デバイスやOSの脆弱性を取り込む。または統一する。	□
		保護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導入する。 ・アプリケーションのインストール時に不要な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、悪意のない動き、信頼できる情報等)を入手する。 (5.2 節「アプリケーションを利用する」参照)	■ □ □ □ □ □
		利用者による改ざり	・改ざりを防止する。	■

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 ○推奨 一対象外

番号	分類	脅威	対策 または 対策	推奨レベル
5.1	アドレス帳を利用する	新操作 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)を教える。 ・業務専用の保存場所を決める。 ・利用者には保存場所を識別できるようにする。	— □ □ □
		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。	— □ ■
		盗難	・VPNを利用する際には、通信経路を暗号化する。	□
5.2	電話を利用する	不正利用	・IP PBX サーバの権限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かけるなど脆弱性のセキュリティ強化を行う。デバイスを暗号化する。	□
		私的利用	・手順書を作成する。(付録参照) ・通知履歴を削除する。	— □
		盗難	・VPNを利用する際には、通信経路を暗号化する。	□
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。	— — □ □
		盗難	・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) ・ファイルの暗号化は禁止し、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。	— — □ □ □ □ □

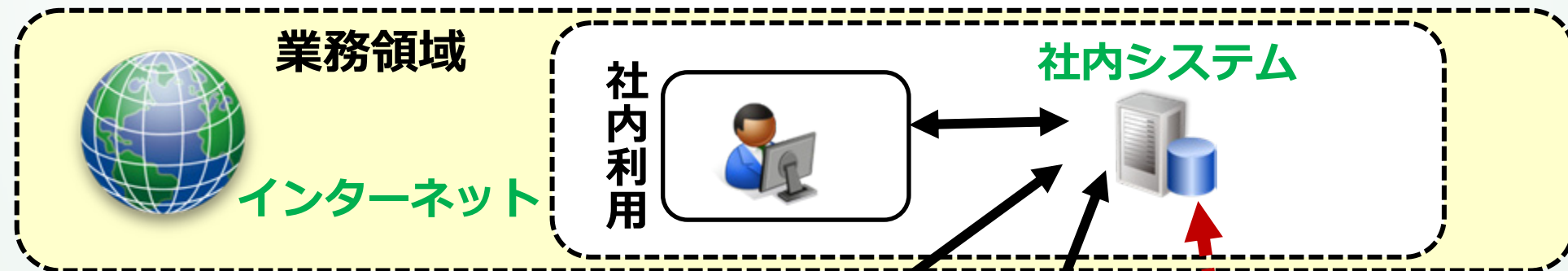
A-4 誓約書に記載する項目の例

A-4-1 法人所有版

推奨レベル：■強く推奨 □推奨 ○推奨

分類	項目	確認(わらい)	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	スマートフォンを利用目的、利用範囲などを明記し組織の定めたルールの順守を義務化する。		■
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被害防止などから、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」に該当して文書を作成する。システムの脆弱性および、管理者による情報漏洩、どちらも含む。	■
	組織による制御に対する個人の承諾(制限、OS のアップデートなどを行う場合)	設定変更、強制更新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。システムの脆弱性および、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等の保管有無や、事故の影響を確認するため、直ちに届け出を合意する。	組織の定めたルールに従って届け出をする。 例：「盗難」「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	セキュリティ上の脅威を抑制するため、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。		□
	盗難または遺失による情報漏えい	データを持ち歩くことや個人の所持機が壊れるため、注意を喚起する。情報漏洩時には、企業ポリシーに従い対応する。	企業情報等を盗み等への制限、不要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。		□

管理者コントロールの役割



① PCとの一元管理

【要件例】
ユーザ情報
コントロール
端末情報等
アプリ管理

(注) 現時点では実現不可能な機能もあります。

② 活用と停止



【要件例】
データ保護(アクセス権統制)
Webフィルタ
端末、アプリ管理

③ 禁止 (PC側機能)



【要件例】
データ持出禁止／ファイル暗号
デバイス利用／ファイル持出申請
WiFi/BlueTooth等ネットワーク制御

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

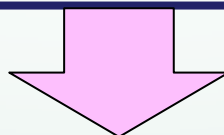
- ・セキュリティ範囲の特定

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

4. おわりに

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

- ・ PCのようなセキュリティ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。

利用ガイドライン
ご感想受付中です！

ありがとうございました。



さあ、スマートフォンしましょう！

Let`s Go Beyond with Smartphones !