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-

2014年度 JSSEC名古屋セミナー資料

ALSI

スマートフォン＆タブレット
安全＆快適を実現するセキュリティの考え方

-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から-

2014年10月24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
セキュリティ事業部IAM製品企画課グループマネージャー
松下綾子

もくじ

1. はじめに
2. スマートフォンのしくみ
3. セキュリティの視点と管理のポイント
4. まとめ

1．はじめに

JSSEC利用ガイドラインと基本方針

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
・情報セキュリティの考え方以前の、スマートフォンの特性に焦点

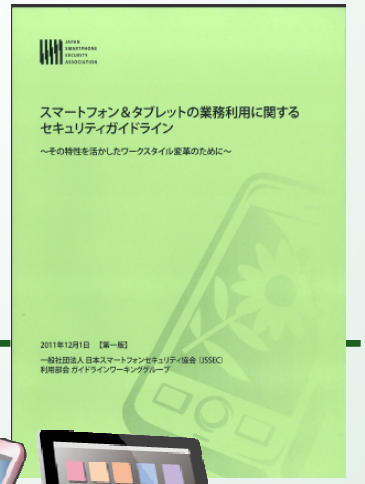
企業、官公庁など多くの皆様に活用していただいています。

総務省 MIC Ministry of Internal Affairs and Communications

NISC 内閣官房情報セキュリティセンター National Information Security Center

FISC 金融情報システムセンター The Center for Financial Industry Information Systems

警視庁 Metropolitan Police Department



両方合わせて
「スマートフォン」

スマートフォン

タブレット

http://www.jssec.org/report/20140417.html

ALSIのJSSEC参画の立場

グループ・関連企業

社内システム運用

社会貢献

セキュリティ
ソリューション
企画、販売

事業ドメイン

・製造・流通ソリューション事業
・セキュリティソリューション事業
・ファームウェアソリューション事業

インターセーフシリーズ InterSafe

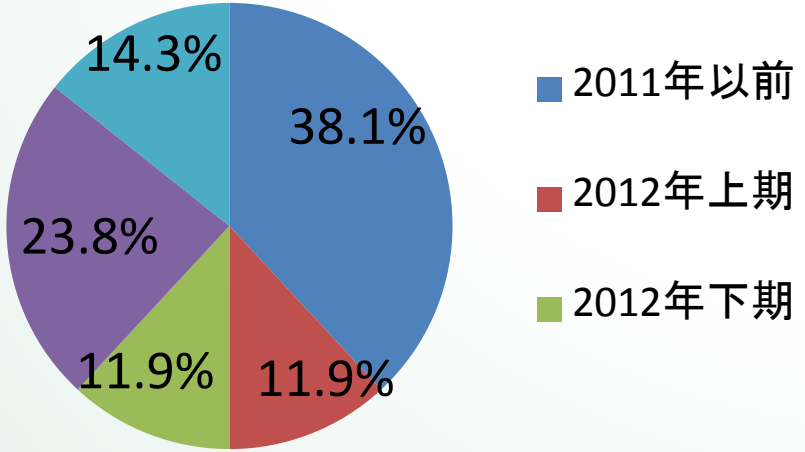
主なセキュリティ製品群

・InterSafeWebFilterなどのIAMシリーズ
・IRMなどのILP(情報漏洩対策）シリーズ
・携帯キャリア様向けWebフィルタ提供！
・スマートデバイス向け
　トータルセキュリティ（VPN,MDM,フィルタ等）
etc

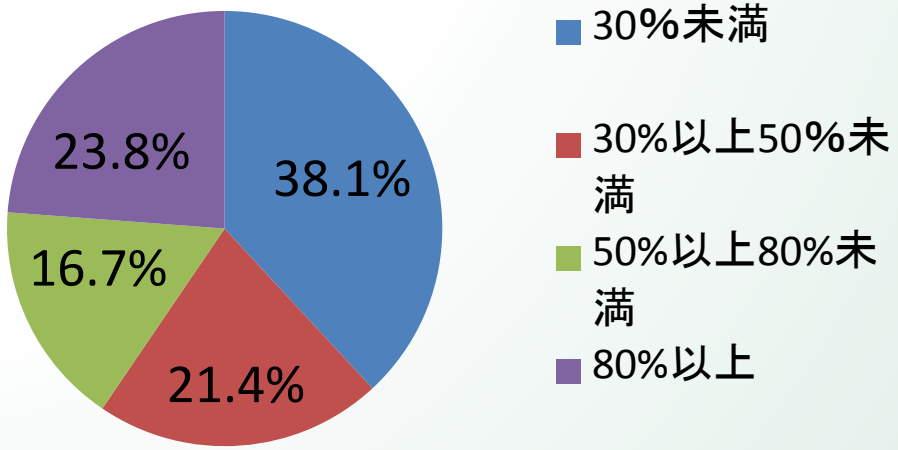
プロローグ　～JSSEC 調査資料から

「第二回スマートフォン企業利用実態調査　レポート」本調査2014年１月
http://www.jssec.org/dl/ResearchReport2014_v1.pdf

Q.導入を始めた時期はいつごろでしょうか。
(n=42)



Q.全社員の役何割の方に現在スマートフォンが配布されていますか。(n=42)



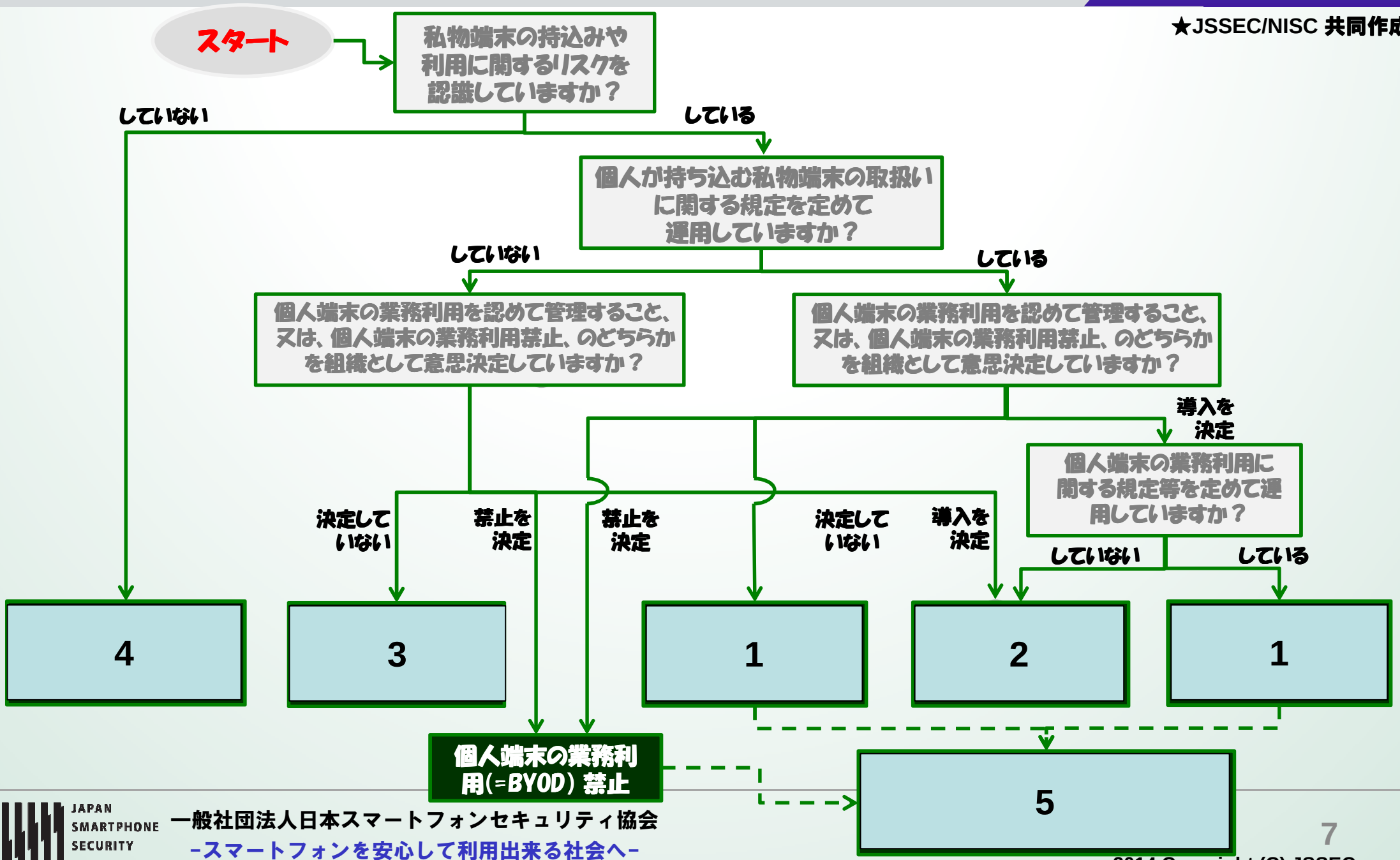
Q.スマートフォンの導入で得られた効果があった場合は、具体的に教えてください。
A.半数以上が「仕事の効率化」

<内訳>・ メールなどによるコミュニケーションの向上で外出時でも意思決定ができ仕事の滞留が減った
・ 社外から社内のリソースを確認でくる
・ PC の代用としてオフィス系処理など作業ができる

<少数の回答>・ モチベーションが上がった
・ ペーパーレス化促進
Etc.

「社内状況把握してますか。」
～まずはチェックしてみましょう。

★JSSEC/NISC 共同作成



2. スマートフォンのしくみ

スマートフォンとは？

それはモバイルＰＣ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	携帯電話	PC	スマートフォン
OSの 管理者権限	解放されていない	解放	解放されていない （例外あり）
ネットワーク セキュリティ	キャリアで対応	利用者自身で対策	利用者自身で対策
機能の実装	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	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	キャリアが提供	利用者が各種方法で導入	マーケットが提供

特性からみたリスクの考察①

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。 ・ **操作痕跡を残さない**

特性からみたリスクの考察②

脅威	解説(リスク)	対策　または　要件
誤操作 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。	・ 誤操作のみならず、**悪意を持ったサイトも存在するため**慎重な操作を喚起する。（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易い）
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。

特性からみたリスクの考察③

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要（Android)

例）

順位	合計 980	利用率	Android Permission	説明
1	882	90.0%	INTERNET	インターネットへのアクセス
4	567	57.9%	READ_PHONE_STATE	電話番号やSIM情報の読み取り

スマートフォンとうまくつきあうために

当たり前と思わず、違いを意識する

常に電源ON＋Net　　いつも一緒　　自分流も簡単

インターネットが
手帳になった。
しかも
隣人の分も！

コミュニケーションの活性化

意思決定の迅速化

生産性向上

データはどこに？　**保存場所や同期範囲は認識していますか？**
アプリケーションが問題になってる？
不正アプリとは？信頼できるマーケットって？

従業員・利用者も、みんなが分かってる？

トラブルの例(1)

意図しない情報発信

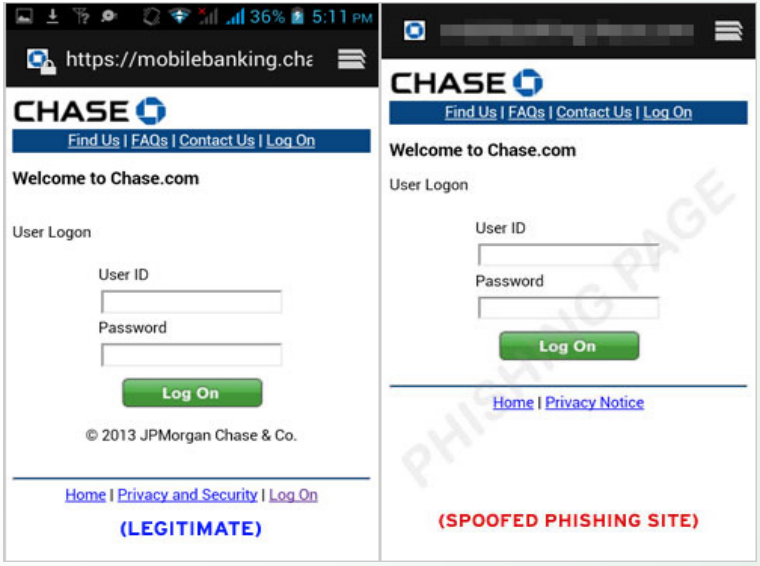
■問題アプリを実行すると下記を外部サーバに送信。**送信事実には気付かない。**
- 端末の電話番号
- Android ID
- 所有者の名前
- 連絡先にある人物の名前とメアド

■**「Simeji」**は下記項目をサーバへ送信。
- 変換確定文字列
- デバイス名
- アプリパッケージ名
- UUID
- Simejiのバージョン

架空請求

■アダルト動画アプリと偽り**架空にコンテンツ料金を請求。**被害総額は2000万円以上
(支払人数 約200人／インストール人数 9000人)

不正送金



正規サイト　フィッシングサイト

※出典：出典: トレンドマイクロ社「TrendLabs SECURITY BLOG」8月14日記事

■主にオンラインバンキング**なりすまし。**
- 政府発行の身分証明書や　Apple ID入力を促すこともある。
- 特に短縮URLは要注意！

トラブルの例(2)

不正送金被害～金融系マルウェアの猛威

http://www.ipa.go.jp/security/txt/2014/08outline.html

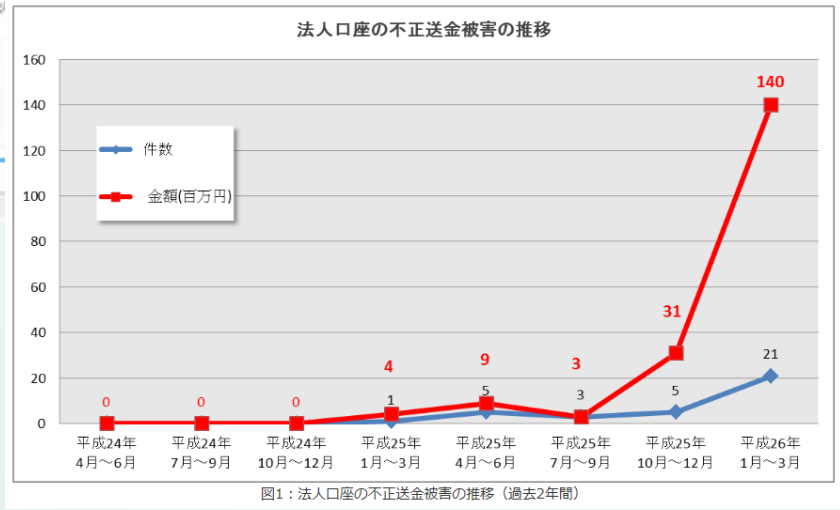
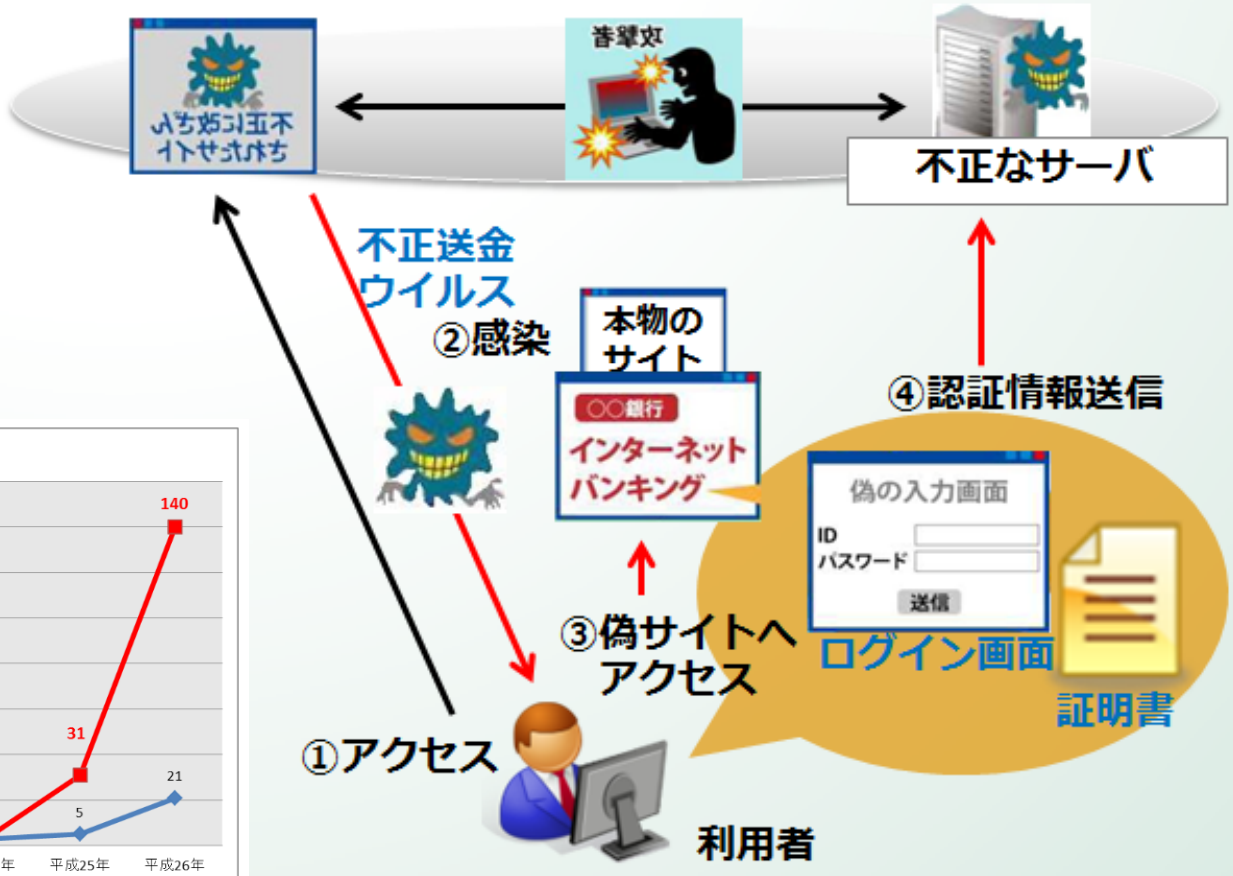


図1：法人口座の不正送金被害の推移（過去2年間）

http://www.ipa.go.jp/security/txt/2014/08outline.html



リスクのあるアプリケーションの分類

問題が発生するパターン

分類	可能性のある問題	対策例
ウィルスアプリ（悪意あるアプリ）	・ウィルスに感染したアプリを配布してしまう。	・アプリケーションの動きを確認する。 ・アンチウィルスでリリース前のアプリをスキャンする。
迷惑なアプリ	・迷惑なアプリを配布し、会社の評判を落としてしまう。	・不必要な個人情報を取得しないなど、ユーザーが迷惑に感じない仕様にする。
脆弱性のあるアプリ	・利用者が個人情報漏洩等の被害にあう。	・開発者がセキュア設計、セキュアコーディングを行う。

※出典:JSSECアプリケーションWGセキュアコーディンググループ資料より抜粋

〔参考〕総務省の取り組み

総務省 MIC Ministry of Internal Affairs and Communications

プライバシーイニシアティブ（‘12年7月）/ Ⅱ(‘13年8月)

「透明性の確保」や「利用者関与の機会の確保」等の 実現を目的にリリース

『スマートフォンにおける利用者情報を取得しようとするアプリケーション提供者、情報モジュール提供者は、
個別のアプリケーションや情報収集モジュール等について、**８項目24の事項**について明記する
プライバシーポリシー等をあらかじめ作成し、利用者が容易に参照できる場所に掲示等を行うこと』

◆項目　①情報を取得するアプリケーション提供者等
の氏名又は名称
②取得される情報の項目
③取得方法
④利用目的の特定・明示
⑤通知・公表又は同意取得の方法、
利用者関与の方法
⑥外部送信・第三者提供・
情報収集モジュールの有無
⑦問合せ窓口
⑧プライバシーポリシーの変更を行う場合の手続

【図表2-2：スマートフォンにおける利用者情報の例】

区分	情報の種類	含まれる情報
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報
	クッキー技術を用いて生成された識別情報	ウェブサイトを訪問時、ウェブブラウザを通じて一時的にPCに書込み記載されたデータ等[4]
	契約者・端末固有ID	OSが生成するID（Android ID）、独自端末識別番号（UDID）、加入者識別ID（IMSI）、端末識別ID（IMEI）、MACアドレス等
第三者の情報	電話帳で管理されるデータ	氏名、電話番号、メールアドレス等
利用者の状態に関する情報 通信サービス上の行動履歴や	通信履歴	通話内容・履歴、メール内容・送受信履歴
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等
	位置情報	GPS機器によって計測される位置情報、基地局に送信される位置登録情報
	写真、動画等	スマートフォン等で撮影された[5]写真、動画

特性からみたリスクの考察④
スマートフォンらしい利用環境

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）

- 情報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、自動同期された外部サービス（無意識）など様々であり意識が必要。

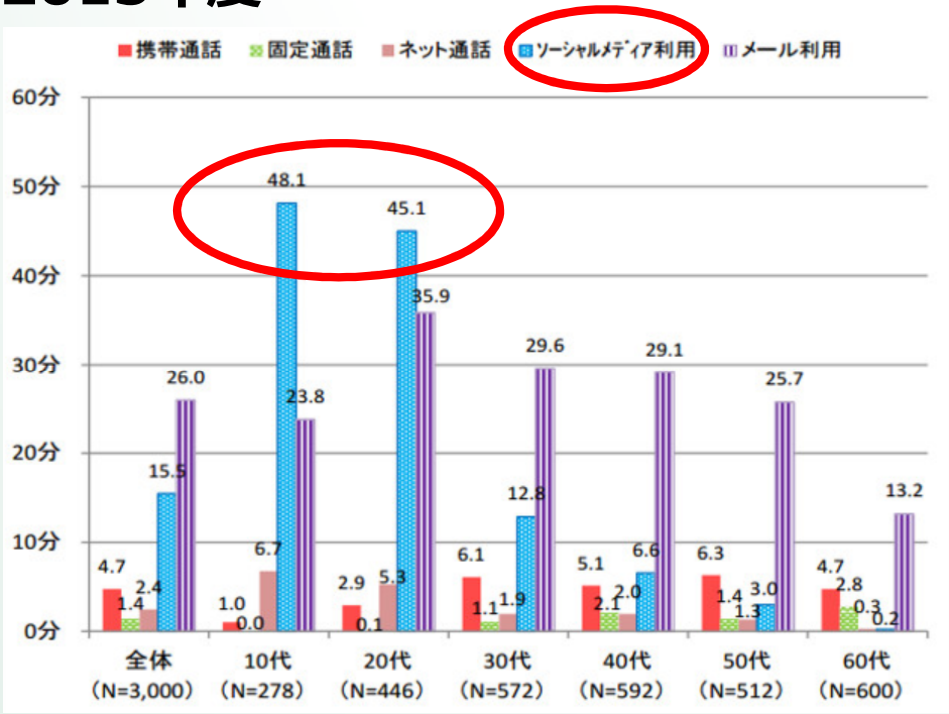
ストレージ・ＳＮＳ

- 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、利用者の拡大により被害も増加。
- 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。

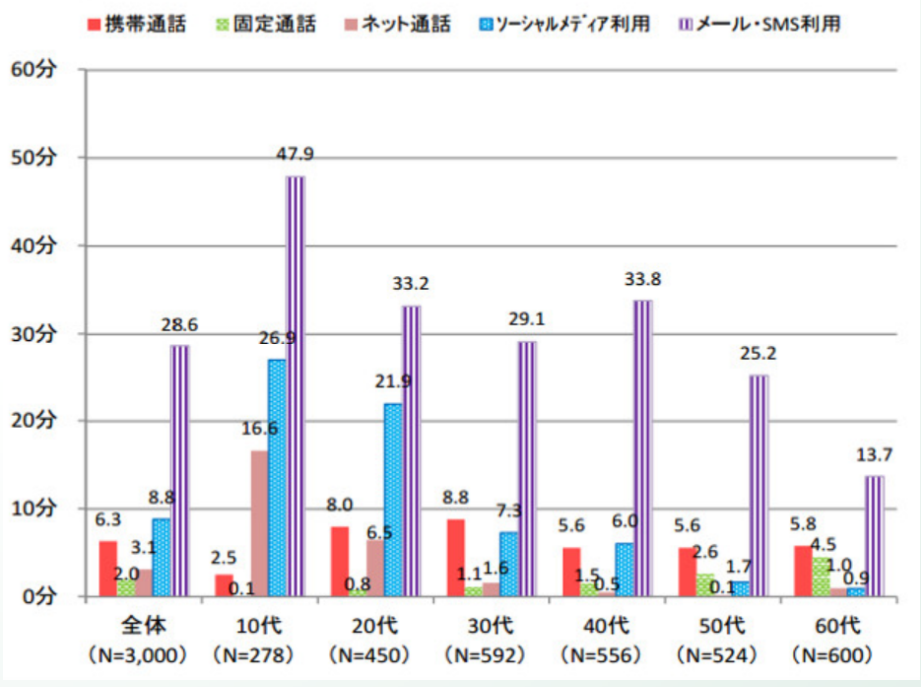
コミュニケーション系メディアの平均利用時間

デジタルネィティブ世代の増加

2013年度



2012年度



出典：総務省情報通信政策研究所
「平成25年 情報通信メディアの利用時間と情報行動に関する調査」より

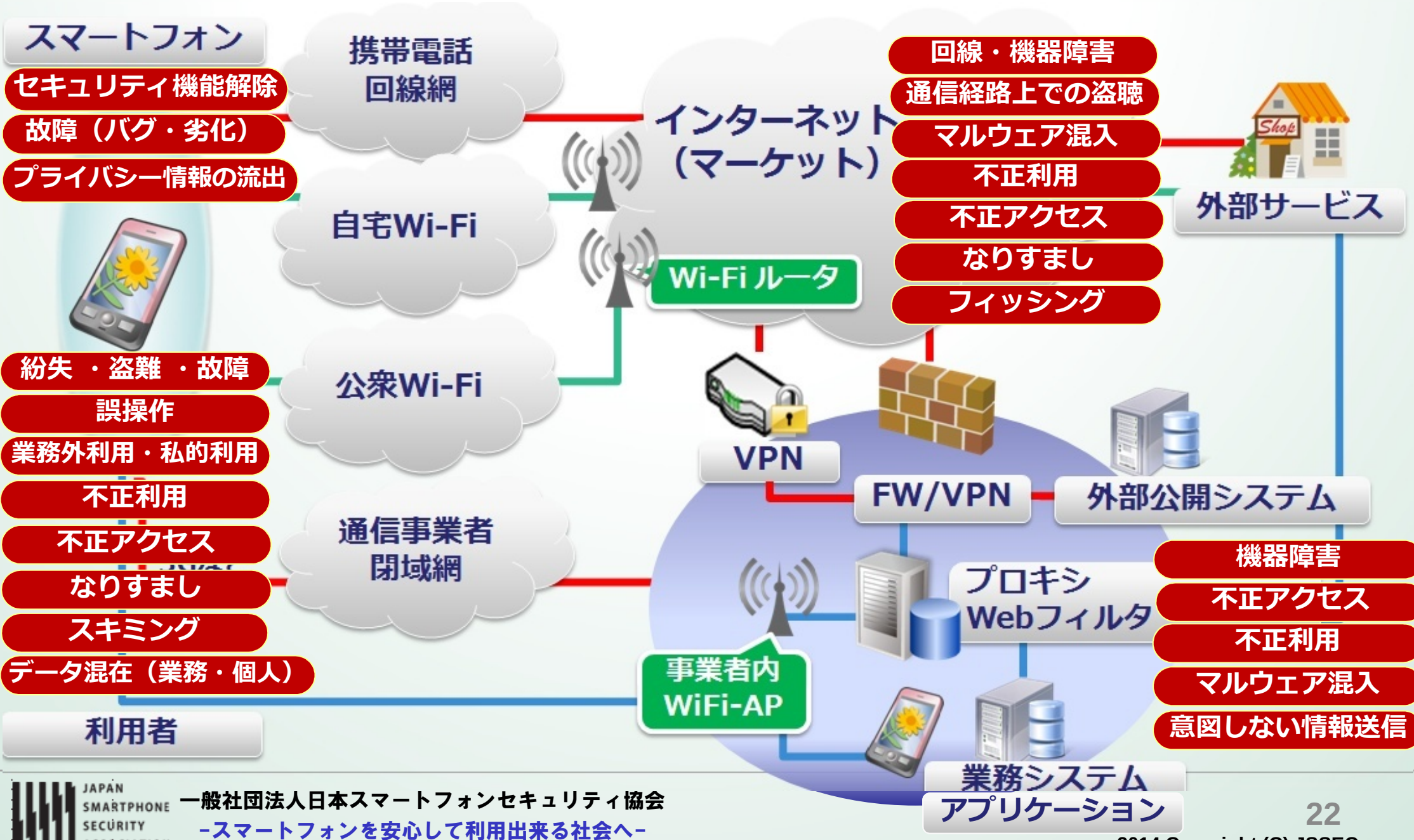
モバイルデバイス利用において
ソーシャルメディアの取り扱いは無視できない課題ですね！

～利用シーンからの考察(2)

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。
- アクセス先は社内システム・VPN・通信会社の専用線、閉域網などであり、選択が可能。
- テザリング機能により誰でもＡＰを作れる。
- 不正なＡＰ（アクセスポイント）の危険性を意識する必要あり。
- 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での対応も必要。

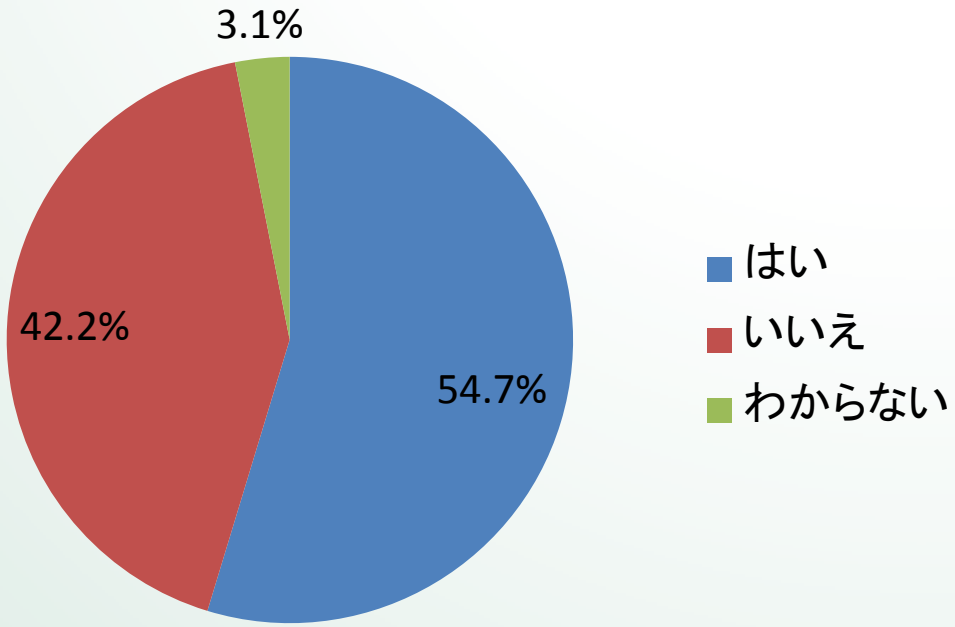
～利用可能なネットワークと脅威の想定（イメージ）



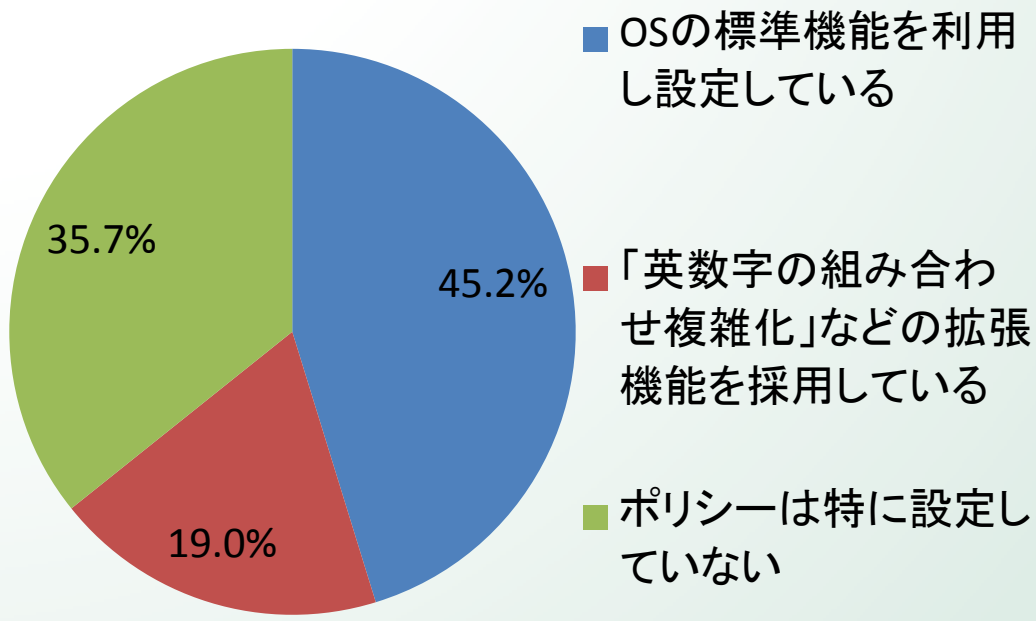
～JSSEC 調査資料から

「第二回スマートフォン企業利用実態調査　レポート」本調査2014年１月
http://www.jssec.org/dl/ResearchReport2014_v1.pdf

Q.あなたの個人用のスマートフォンには業務に関する情報が保存されていますか。（n=128)



Q. スマートフォン利用時にパスワードポリシーの設定を義務付けていますか？（*n=42)*



まとめ

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

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ＰＣとの違い

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．セキュリティの視点と管理のポイント

新しい管理スタイル

ライフサイクルのＰＤＣＡを認識する

計画
目的を明確化する
- **現状を把握する。**
- 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

- 所有形態を考える
- 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
- **セキュリティポリシーの再検討**

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

運用　先回りして考える
- 同じデバイスを使う範囲や
  数量を考えておく。
- 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**

安全な活用の一例

データの一生を考えてみる

- **MDM**（Mobile Device Management）

  端末全体を管理するためのポリシー制御やワイプ機能、アプリ導入などの機能を使った管理手法

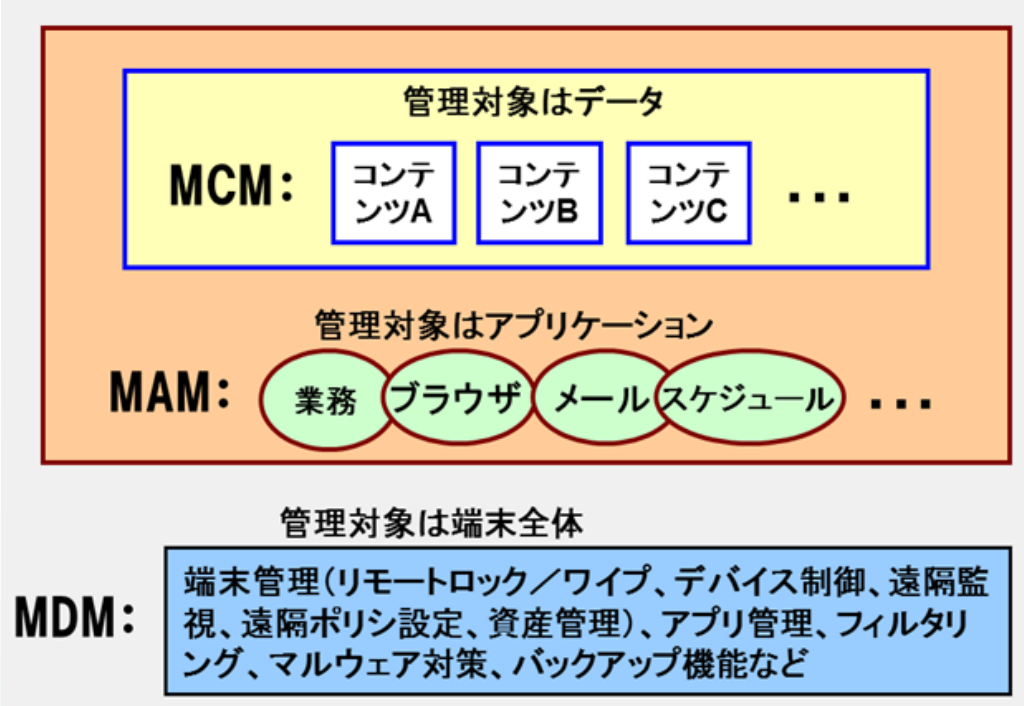
- **MAM**（Mobile Application Management）

  主にセキュリティ機能を実現するものであり、スマートフォンに導入されたアプリケーションに対し、他のアプリケーションなどから隔離させて安全に利用させることを目的とした管理手法

- **MCM**（Mobile Content Management）

  セキュリティ機能だけでなく、ライフサイクルを意識したコンテンツ指向の管理統制手法

JSSECにおけるMAM/MCMの概念



※出典:JSSECデバイスWG　MAM/MCM利用検討会資料より抜粋

最低限、気をつけておきたいこと①活用面

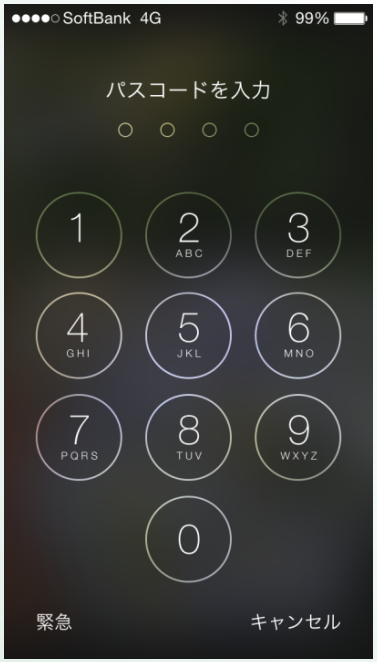
※利用ガイドライン付属のチェックシート参照

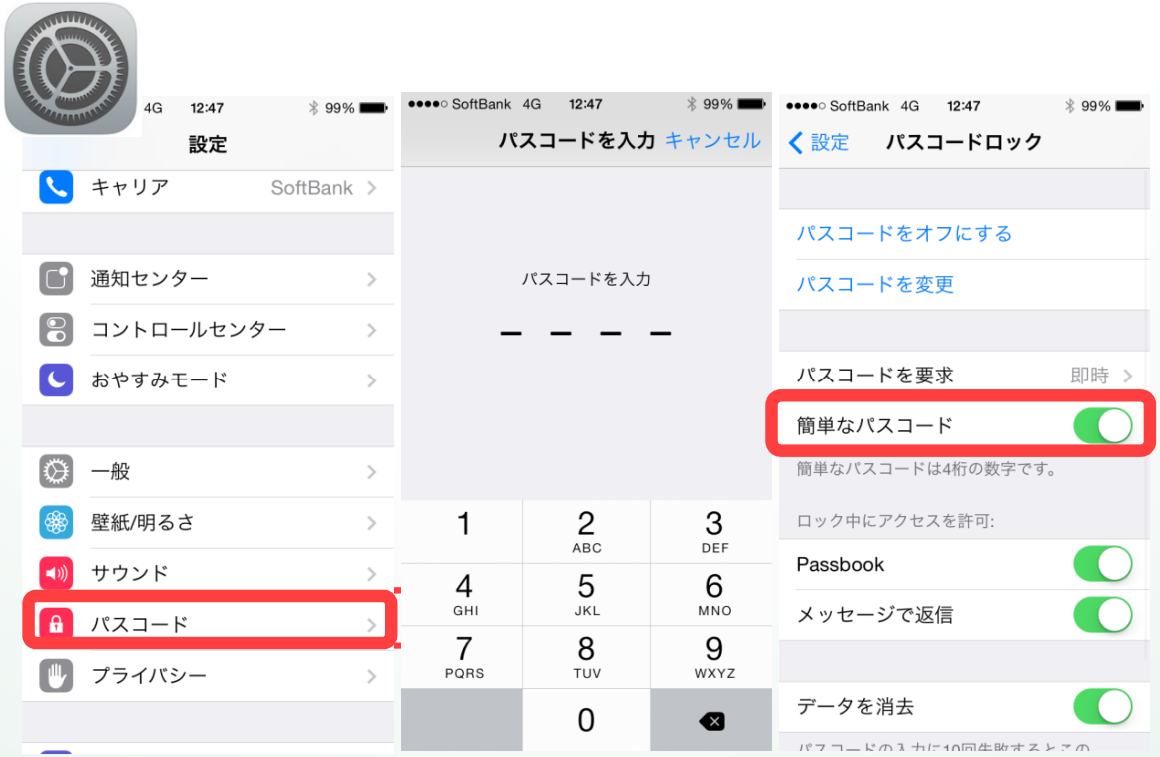
すぐ見直しましょう！

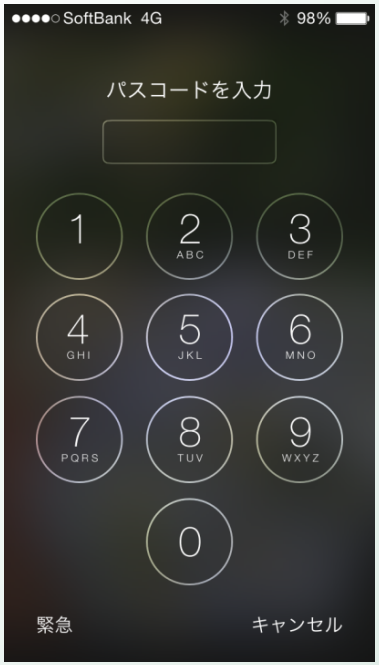
- パスワードは大切です！
  - ロック必須＋複雑化＋ロック解除失敗時のローカルワイプ
- 紛失時のルールを覚えておこう！
  - 紛失時の行動規範と連絡先の通達（企業内／通信事業者）
- マーケットは信頼できるところだけ使おう！
  - 組織の推奨したところからのみダウンロード or ホワイトリストの提供
- データの持ち歩きについて意識しよう！
  - クラウド同期の確認+利用終了データ削除＋河畔媒体としての利用禁止
- 公衆Wi-Fiはほどほどに！
  - 不明な公衆Wi-Fiの利用禁止（推奨したもののみ）＋ SSIDの複雑化
- ひと呼吸おいてからコミュニケーションしよう！
  - 普段と違うメールや短縮URLへの留意、SNS投稿時の配慮

〔参考〕パスワードロックですが・・・

ｉＰｈｏｎｅの方は、確認してみましょう。







暗号化にパスコードを利用するため、
必ず画面ロックとパスコードの設定を行いましょう！

最低限、気をつけておきたいこと②管理面

PCとの違いを意識した管理

- 管轄部門同士の連携（とくに人事部門）
- OSのアップデート時に意識すべき“機能追加”
- 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
- 利用段階に応じたシステム設計とセキュリティ

運用に関する利用者教育

- 世代毎にポイントを絞った教育
- 反復学習
- デジタルネイティブ世代の活用
- 自分のデバイスと組織から支給されたデバイスの使い分け

個人所有スマートフォンの業務利用パターン

一般に「BYOD」と捉えられている状況の考察

分類項目＼パターン	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

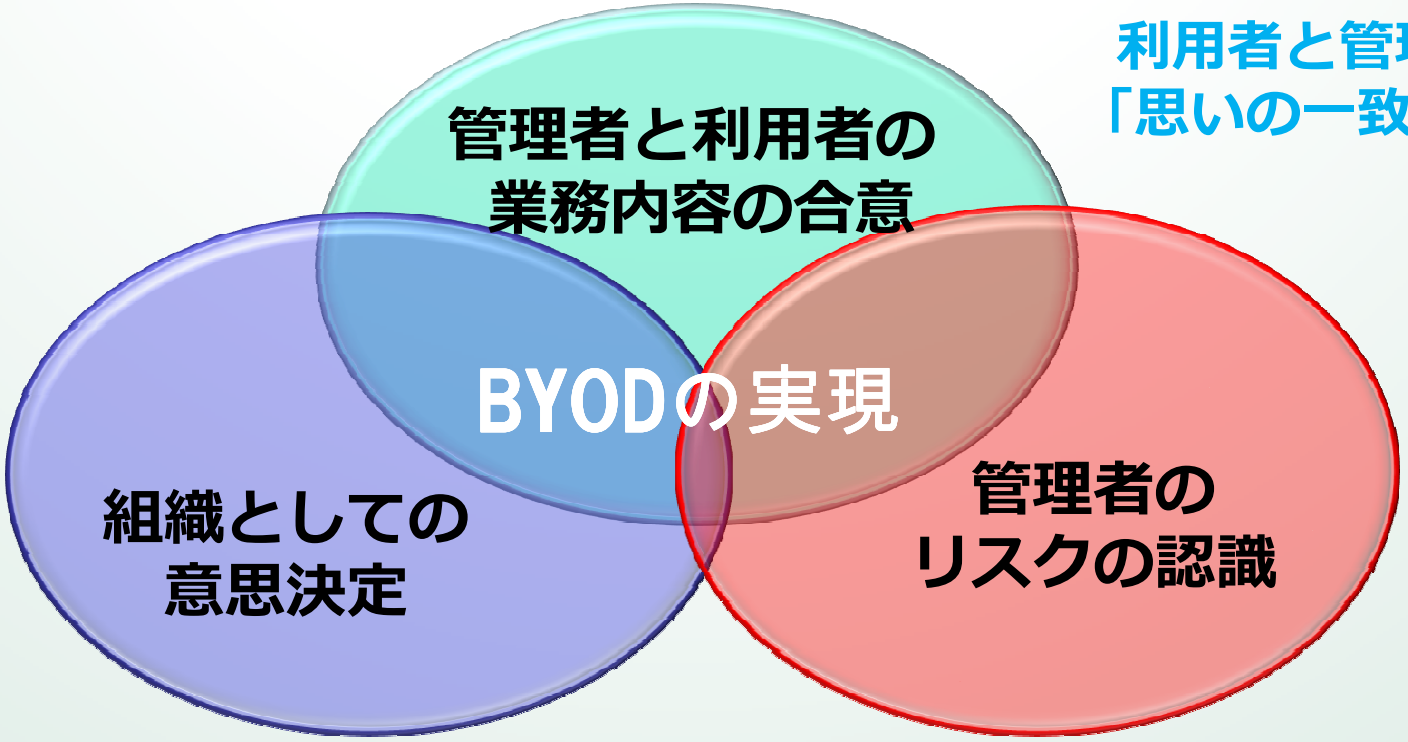
BYOD

危険！！

BYODの定義と重要な要素

BYODとは

- BYOD (Bring Your Own Device) ＝ 個人所有のスマートフォンを業務で利用許可する形態
- リスク認識をした上で、個人所有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。



利用者と管理者の「思いの一致」が不可欠

〔参考〕BYOD導入時の管理者の心得

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。

組織側の管理可能な範囲 と 個人との合意 のバランス

- 会社所有デバイスとの違いや、BYODのメリットを意識する。

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
- 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
- 戦略的なBYOD～導入するなら徹底的に。しないなら禁止を明言！

「COPE」という概念の登場

「BYOD」は、なぜ導入する？

利用者

- 同じ用途で２台もいらない
- 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

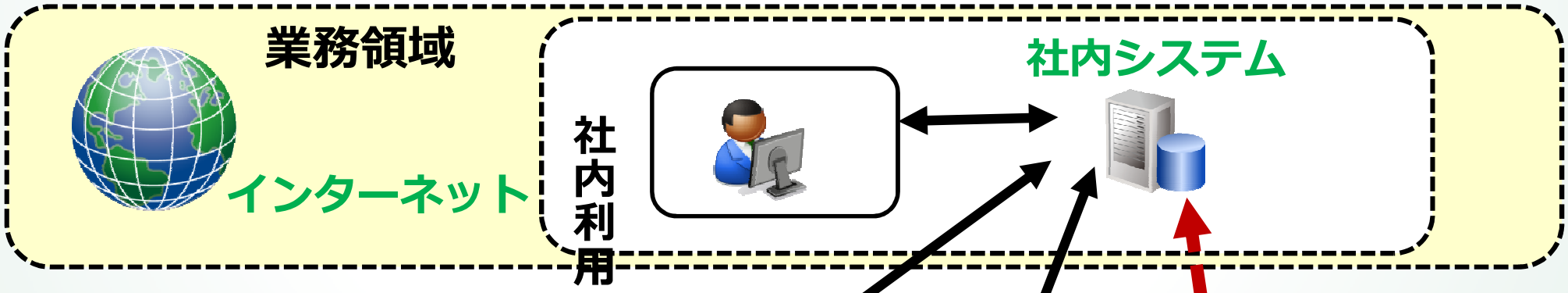
- 働き方改革への対応
- 生産性アップと費用の低減
- 人の行動や発想の可能性への機会

それならば
違うアプローチもあり？

組織から至急した端末の個人利用を認めること

＝COPE（Corporate Owned Personally Enabled）

管理者コントロールの役割



①PC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

②活用と停止

パソコン
スマートフォン

【要件例】
データ保護(アクセス権統制)
アンチウイルス・Webフィルタ
端末、アプリ管理

③禁止

(PC側機能)

スマートフォン

【要件例】
データ持出禁止
持出し申請/暗号化
WiFi/BlueTooth等ネットワーク制御

(注) 現時点では実現不可能な機能もあります。

チェックシート/手順書/誓約書のイメージ

※利用ガイドライン付属のチェックシート参照

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

虎の巻	分類	脅威	対策 または 関連	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。	□
		誤操作	・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

虎の巻	分類	脅威	対策 または 関連	推奨レベル
5.1	アドレス帳を利用する	誤操作 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混在【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。	－ － □ □
		誤操作	・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確認する。		■
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	セキュリティ上の脅威を排除するため、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	コストの増加や事務生産性低下、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。		□
	故意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。		□

4. まとめ

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

おわりに～適切なセキュリティ確保を！

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」「利用目的を変える」「リスクを敢えて受容」という視点も必要です。

ありがとうございました。

JAPAN SMARTPHONE SECURITY ASSOCIATION

さぁ、スマートフォンしましょう！
Let`s Go Beyond with Smartphones！

利用ガイドラインご意見募集中＆参加者募集中！

sec@jssec.org