スマートフォンの安全な利活用のすすめ

～ スマートフォン利用ガイドライン ～

β 版

スマートフォン活用セキュリティガイドライン策定 WG

2011 年 4 月

目　次

はじめに

近年、スマートフォンをはじめとした携帯電話端末の高機能化・オープン化が進んでいる。通話機能を主体とした従来の携帯電話に、さまざまな付加機能が搭載され、膨大な数のアプリケーションが利用可能となり、また加えて、いわゆるクラウドサービスとの連携が可能となったことで、利便性が劇的に向上した。従来 PC 向けとして開発された OS がスマートフォンのプラットフォームとして採用されるようになってきた結果、スマートフォンで実現できることと、PC で実現できることの差は急速に埋まりつつある。

PCと比較して、スマートフォンは圧倒的な携帯性（モビリティ）を有していることから、PC で実現できなかったことを補完するデバイスとしてその地位を確立しつつある。それゆえに、既に多数の組織において、スマートフォンの業務利用が決定、あるいは検討されている他、ユーザが個人所有のスマートフォンを組織内に持ち込み、使用する機会は今後ますます増加すると考えられる。

一方で、機器の開発サイクルの短縮化により、脆弱性が潜在したまま出荷され、これを悪用されることにより、望ましくない使われ方をされる、あるいは事故が起こるといった事例が発生している。また、PC に搭載される OS の脆弱性が、スマートフォンにも影響を及ぼす状況が生じている。

このため、スマートフォンをビジネスに利用しようとする場合、従来の携帯電話とは異なる脅威を想定し、組織の情報セキュリティ対策を見直す必要がある。

一般に、スマートフォンを対象としたセキュリティ管理策の検討において、多くの組織は以下の問題に直面している。

- PC に適用される従来型のセキュリティ管理策を、そのままスマートフォンに適用することは困難な場合があること
  例） 操作ログの採取、ウイルス対策ソフトウェアの導入、セキュリティパッチの
  タイムリーな適用 等
- セキュリティ管理策で、スマートフォンを利用することのメリットを損なう

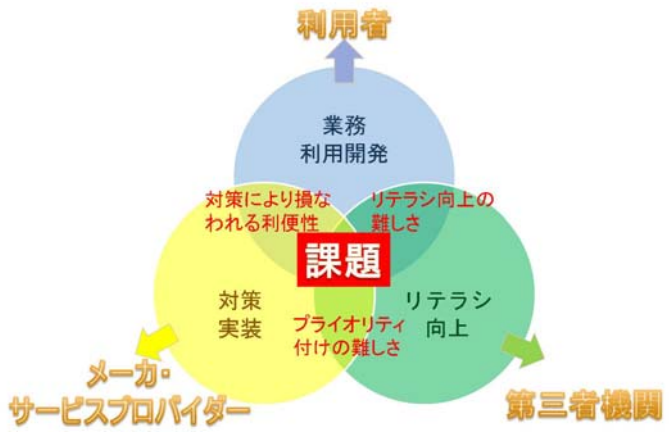
スマートフォンの普及が、組織の情報セキュリティマネジメントに及ぼす最も重大な影響は、ユーザ個々のセキュリティリテラシーへの依存度を高めざるを得ないことである。

以上を鑑み、本書では、スマートフォンの安全な利活用を促進するため、スマートフォンの現状の課題を整理し、スマートフォンの利用における企業の責任と、ユーザーリテラシーの境界線を明確化し、社内外でのさまざまな利用局面において、実施すべきセキュリティ対策を紹介する。

本ガイドラインの利用のしかた

スマートフォンの位置づけ

このガイドラインでは、スマートフォンを企業の業務において、安全に利用することを検討する際に必要な情報を可能な限り掲載するよう努力した。また、スマートフォン普及においては、個人所有のものが企業導入よりも先行した背景から、個人所有スマートフォンの業務持ち込みを禁止しても、社内統制が利かないと予測される。そのため、個人が所有するスマートフォンを業務に利用するケースを想定している。このような状況で、これまで一般の企業が目指すセキュリティポリシ(情報資産の洗い出しから情報資産の機密度定義、それに見合った課題と対策)をそのまま当てはめようとすると、本体企業がスマートフォンに期待する生産性の向上や機動力、携帯性を著しくそこなう結果がみえてくる。



スマートフォン発展の3要素

スマートフォンに限らず、情報システムを有効にかつ安全に利用するには、次の3つの要素においてバランスがとれていることが重要。

[業務利用開発] 新しい技術やプロダクトを積極的に業務に利用する意識や活動であり、これを牽引するのが利用者となる。スマートフォンの有効活用により、生産性向上、機動力、コスト削減などが後押しする。

[対策実装] 新しい技術やプロダクトを安全に利用するためのインフラや基盤サービスであり、これを牽引するのがメーカーやサービスプロバイダの役目となる。

[リテラシ向上] 第三者として業界の有識者(フォーラムなど)が[業務利用開発] や[対策実装]をそれぞれ後押しするような情報を開示し、業界発展のための啓発をしてゆく位置づけ。

スマートフォン発展の課題

この 3 つの要素のバランスには、以下の 3 つの課題がある。

[スマートフォン発展課題1： 対策により損なわれる利便性]

利用者が業務利用開発を進めても、企業の過度な対策や適切でない対策により、期待されていた利便性を損なう場合が多い。メーカーやサービスプロバイダが、利便性を損なうことなくスマートフォンを利用できるような仕組みやサービス、プロダクトの改善をすることで、課題を解決する。また、利用者も利用開発の意識を高く維持することは非常に重要となる。

[スマートフォン発展課題2： 対策プライオリティ付けの難しさ]
第三者機関がリテラシ向上のためにリスクを可視化しても、すべてのリスクを低減させることは困難である。対策の有効性や投資効果などを適切にとらえ、優先順位をつけ、タイムリーに対策実装することが重要となる。

[スマートフォン発展課題3： リテラシ向上の難しさ]
スマートフォンに限らず、PC においてもリスクの多様化や変化スピードが速まることで、システムでの対策が困難となり、情報セキュリティのリテラシが叫ばれる状況となってきた。スマートフォンはそのモビリティとパーソナライズにより、さらに個人のリテラシが重要となるのは必至である。リテラシは教育やルール、ドキュメントなどでは向上させにくいため、タイムリーなリスクの顕在化と、企業がそれらの最新情報を常に取り入れ、周知徹底し、リテラシの向上に努めることが課題となる。

故に、ガイドラインに掲載する様々な視点からの利用者課題をもとに、自社の IT 環境、利用シーン、扱う情報を精査しながら、優先すべき対策、受容すべきリスクを的確に見極める必要がある。

ガイドラインが提示する課題の注意点
このガイドラインには、スマートフォンの特徴を活かしながら、既存の情報システムにどのように巻き取られるべきかを基本に記述している。そのため、一般的な情報システムセキュリティで実施するべき対策に関連する記述も含まざるを得ないが、可能な限りスマートフォンに関連する内容に絞って記述するため、以下のような課題や対策は含まない。

- スマートフォン利用者がアクセスするサーバの脆弱性対策
- PC と共通で利用するサービスの認証

1. スマートフォントはどのようなものか

1.1 概要

スマートフォンとは、音声通話に加え多数の機能を有する携帯電話の総称である。

近年のスマートフォンには、概ね以下のような機能が搭載されている。

分類	機能
基本機能	・通話（架電、受電） ・SMS（ショートメッセージサービス）機能 ・通話履歴管理
入出力機能	・ディスプレイ ・多機能 UI（キー入力用 UI、タッチパネル等） ・カメラ（静止画・動画撮影） ・音声録音
個人情報管理機能	・スケジュール管理 ・アドレス帳 ・パスワード管理
インターネット機能	・電子メール送受信 ・Web ブラウザ
ネットワーク接続機能	・無線（wifi）ネットワークへの接続 ・通話用回線を用いたデータ通信 ・VPN クライアント
PC 連携機能	・データ同期（スケジュール、メール、アドレス帳） ・データ保存 ・PC 用ファイル閲覧（MS Office ファイル、PDF ファイル等）
セキュリティ機能	・利用者認証（パスワード、指紋等） ・データ暗号化 ・遠隔操作（データ消去） ・ソフトウェアアップデート ・データバックアップ・リストア
拡張機能	・GPS ・マルチメディアプレーヤー ・サードパーティーアプリケーションの導入 ・電子マネー機能 ・グループ（企業・組織）向け構成管理機能

1.2 特徴

スマートフォンは、機能的にも、構造的にも、限りなくPCに近い特徴を有している。スマートフォンが従来から有する高度な携帯性に加え、PCとの機能的な差がなくなってきたことにより、PCで実現できなかったことを補完するデバイスとしてその地位を確立しつつある。

1.2.1 スマートフォンの構造

アーキテクチャこそ異なるものの、PCとスマートフォンの構造には類似点が多い。

	PC	スマートフォン
デバイス構成	・CPU ・メモリ ・ハードディスク ・入出力デバイス ・NIC	・CPU ・メモリ ・入出力デバイス ・NIC（3G/wifi）
ソフトウェア構成	・OS ・デバイスドライバ ・アプリケーション	・ファームウェア（OS・デバイスドライバ） ・アプリケーション

1.2.2 スマートフォンのプラットフォーム

PC向けに開発されたOSが、スマートフォンのファームウェアとして採用され始めている。

名称	開発元	ベースとなったOS	採用先スマートフォン
Android	Google	Linux	・Xperia（docomo） ・IS01（au）
iOS	Apple	Mac OS	・iPhone・iPad（Softbank）
Windows Mobile	Microsoft	Windows	・SC-01B（docomo）

1.2.3 アプリケーションによる機能拡張

PCと同様、さまざまなアプリケーションを導入することにより、スマートフォンの機能を拡張することができる。現在では、上記各プラットフォームとも、サードパーティー製のアプリケーションが多数登場しており、画面解像度が向上したことも相まって、スマートフォンの利便性をさらに押し上げている。

また、スマートフォンが備えるWebブラウザが、PCのWebブラウザと同等の機能、動作速度を獲得したことにより、いわゆるクラウドサービスをストレスなく利用することができる。

2. スマートフォンの利用におけるセキュリティ上の課題

2.1 デバイスの設計に起因する課題

PC と同様の機能を有するデバイスでありながら、PC ほど柔軟なコンフィグレーション機能を有していないため、PC と同等レベルのセキュリティ設定が行えない場合がある。

どこまで細かく設定できるかは、ひとえにメーカーの設計思想に依存する。

No	セキュリティ設定	PC	スマートフォン	携帯
1	認証設定（認証方式の選択、認証強度の調整）	○	○	×
2	アカウント設定（初期アカウントの停止、パスワード設定）	○	△	△
3	デバイス接続制御（外部記憶媒体、外部機器の接続制御）	○	×	×
4	不要なサービスの停止	○	△	×
5	パーソナルファイアウォール	○	×	×
6	ウイルス対策	○	△	△
7	自動アップデート	○	△	△
8	暗号化（通信及びファイルシステム）	○	△	△
9	無線 LAN セキュリティ	○	○	△
10	ログ採取	○	△	×
11	アプリケーションインストール制御	○	△	△
12	不正プログラム実行防止	○	△	×
13	レジストリ / カーネルパラメータ操作	○	×	×
14	特権制御	○	○	×
15	記憶域のデータ消去（物理フォーマット）機能	○	△	×

<凡例>

○ ・・・ 多くのスマートフォンで実装されている

△ ・・・ 一部のスマートフォンで実装されている

× ・・・ ほとんどのスマートフォンで実装されていない

2.2 脆弱性管理における課題

2.2.1 スマートフォンに潜在する脆弱性とその影響

スマートフォン上で動作するソフトウェアには、PC と同様、脆弱性が存在する可能性がある。近年のスマートフォンの開発サイクルは短縮化されており、脆弱性を作りこむ可能性が増大している。また、プラットフォームのオープン化、アプリケーションの共通化に伴い、PC 向けのプラットフォームやアプリケーションの脆弱性がスマートフォンに持ち込まれるケースも見受けられる。

スマートフォン上で動作するソフトウェアに脆弱性がある場合、脆弱性を悪用してスマートフォンの制御を奪い、メーカーやソフトウェア開発者が意図しない動作をさせることが可能となる場合がある。

なお、スマートフォンの脆弱性を悪用する不正プログラムの存在が確認されており、これらがスマートフォンへの攻撃やマルウェアに転用される可能性は十分にあるといえる。

例）

- 本来スマートフォン利用者が利用すべきでない特権の利用（root 化、Jailbreak 行為　等）
- 信頼できないソフトウェアの導入
- スマートフォンが有するセキュリティ機能の解除
- ファームウェアの汚染、破壊　等

2.2.2 脆弱性の露見から修正までのタイムラグ

一般に、ソフトウェアの脆弱性が露見した場合、ソフトウェアメーカーが脆弱性の修正プログラムをリリースし、利用者がこれを導入することで、脆弱性が修正される。

ソフトウェアメーカーが脆弱性を確認してから修正プログラムをリリースするまでの期間、及び修正プログラムのリリース後、利用者が導入するまでの期間があり、この期間が脆弱の露見から修正までのタイムラグとなる。PC と同様、スマートフォンにおいてもこのタイムラグは存在しており、タイムラグを最小限に抑えるための脆弱性管理が必要となる。

なお、スマートフォンへの修正プログラム導入手順は、スマートフォンの機器メーカーにより異なるが、概ね以下のとおりとなる。

- メーカーの HP より修正プログラムを（PC　あるいはスマートフォン上に）ダウンロードする
- 修正プログラムファイルをスマートフォン上に展開し、インストールする

※　修正プログラムの適用に際して、PC との接続を必要とするものもある。

2.3 業務利用における課題

組織におけるスマートフォンの業務利用の形態には、少なくとも以下の 3 つが考えられる。

（a） 組織としてスマートフォンの採用を決定し、従業者に配布して利用させる

（b） 個人所有のスマートフォンの業務利用を、申請により許可する

（c） 個人所有のスマートフォンを、利用者が届出無しに業務に利用する

上記いずれの形態においても、スマートフォンを業務に利用する際には、以下のような形で社内システム/ネットワークと接続し情報のやりとりを行うこととなる。

（x） VPN または wifi 機能により社内ネットワークに接続

（y） 社内 Web ポータル、スケジューラ、電子メールシステム等との接続

（z） PC あるいはサーバ上のデータをスマートフォン上に保存

以上のような利用形態を考慮した場合、以下のような課題が生じる。

2.3.1 利用許可の有無及び利用者の識別に関する課題

（a）または（b）の場合、利用者（端末）の識別のための情報（MAC アドレス、認証情報）をあらかじめ収集することが可能であり、これらの情報を元にアクセス制御を行うことができる。

しかし、（c）の場合、接続されるスマートフォンのセキュリティ機能の有無、対策状況、利用者の識別、利用状況の把握を行うことが困難となる。このため、以下のような対策が必要となる。

・未登録の機器のネットワークへの接続を防止または検知するための対策

・イントラネットの各セグメント上を流れるパケットのモニタリング

・無許可でのスマートフォンの業務利用を禁止する通達の発行

・未登録端末を収容する為の NW の準備

2.3.2 社内システム/ネットワークへの影響

社内ネットワークへのアクセスを行うスマートフォンが汚染（マルウェア感染）されていた場合、汚染データを社内ネットワークに撒き散らすこととなる。セキュリティレベルの異なるネットワークを接続する際には、ネットワークの境界を設けるべきであることから、スマートフォンを接続するためのネットワークと社内のネットワークを分離する必要がある。

2.3.3 スマートフォン上で取り扱うデータに関する課題

スマートフォンではPCと同等のデータを扱うことができるため、データの種類によって取り扱い可否を決めることや、利用制限を行うことは困難である。このため、スマートフォン上でのデータの取扱いに関して、利用者のリテラシを向上させる取り組みが必要となる。

なお、従来の携帯電話を使用して社内システムの一部にアクセスさせるソリューションも存在しており、

当該ソリューションを活用すれば端末内にデータを残さない形で社内システムの利用を実現することができる。個人利用のスマートフォンで組織のデータを利用させる場合には、上記のようなソリューションの活用により、データの完全分離を行うことも視野に入れることが望ましい。ただし、端末内にデータを残さない形で社内システムを利用しようとした場合、利便性の低下は避けられない。

2.3.4 スマートフォンの可用性に関する課題

スマートフォンを業務に利用する期間が長ければ長いほど、様々なデータがスマートフォンに蓄積されるとともに、利用者のスマートフォンへの依存度が高まることが想定される。このため、機器の故障や紛失が発生した場合、迅速に代替機への切り替え（データの回復も含む）を行えるようにしておくことが必要となる。

2.3.5 スマートフォンを廃棄する際の課題

耐用年数の終了や経年劣化、故障等に伴いスマートフォンの廃棄が発生する場合、スマートフォンに蓄積されたデータが残留している可能性がある。廃棄手段によっては、当該データが残留したまま再利用される恐れがあるため、スマートフォンの廃棄時には利用者のデータが残留しないよう注意する必要がある。

なお、スマートフォンに内蔵される記憶媒体（NAND 型フラッシュメモリ）の特性上、ソフトウェアによるデータの完全消去は困難である。これは、記憶媒体に書き換え可能回数の上限が存在することから、ドライバ側で極力書き換え回数を抑える実装がなされていることに起因している。このため、スマートフォンを廃棄する際には、物理的に破壊する等の対策が必要となる。

3. スマートフォンの安全な利用方法

3.1 IT 管理者が考慮すべき事項

3.1.1 スマートフォン導入時のセキュリティ対策

前述のとおり、スマートフォンは PC 同等の機能と高い携帯性を有するデバイスであることから、その用途や利用シーンは多岐に渡る可能性がある。したがって、スマートフォンを組織内に導入する際には、可能な限りその目的、用途、利用局面を明確化するとともに、スマートフォンの導入が業務に及ぼす影響を分析し、業務で利用する端末に求められるセキュリティ機能の充足状況を確認したうえで導入することが求められる。

また、スマートフォンは社内のみならず社外においても随時携帯して利用することが想定されることから、紛失時の対応についてあらかじめ定めておく必要がある。紛失時の対処に役立つ機能（探索機能、遠隔からのロック機能、データ消去機能、データ暗号化機能等）を有する機器の選定も有効である。

なお、個人所有のスマートフォンの業務利用を許可するかどうかに関しては、組織として明確な方針を定めるとともに、許可する場合にはその手続き（後述する識別情報の提出等）を定めておく必要がある。このほか、個人所有のスマートフォンを業務利用させる場合には、組織の機器選定基準を満たす推奨機種についての情報も周知しておくとよい。

<スマートフォン導入時のセキュリティ対策項目>

No	対策	チェック
1	スマートフォンを組織内に導入する目的、用途、利用局面、導入効果（定性的効果・定量的効果）等が明確化されているか。	□
2	スマートフォンを組織内に導入することにより生じる影響の分析を実施しているか。 （リスク分析、事業影響度分析　等）	□
3	導入候補のスマートフォン（機器）は、組織内のルールに定められたセキュリティレベルを満たしているか。	□
4	スマートフォンを紛失した場合の対応を定めているか。 （紛失時の連絡先、連絡方法、紛失した端末の処理　等）	□
5	個人所有のスマートフォンの利用可否に関する方針を定めているか。	□
6	個人所有のスマートフォンの業務利用を申請するための手続きを定めているか。	□

<参考：スマートフォンに関するセキュリティ機能確認項目（例）>

No	対策	チェック
1	暗号機能（データ暗号化、通信暗号化　等）	□
2	不正使用防止機能（利用者認証、重要データ読み出しに関する制御　等）	□
3	紛失対策機能（紛失時の探索機能、遠隔データ消去機能）	□
4	データバックアップ機能	□
5	デバイス利用制御機能（スマートフォンの搭載デバイス/外部デバイス）	□
6	アプリケーション導入・利用制御機能	□
7	ログ採取機能	□
8	ソフトウェア・ファームウェアアップデート機能（有無及び使いやすさ）	□
9	特権制御機能（利用者によるセキュリティ設定の変更防止　等）	□

3.1.2 組織のネットワークにスマートフォンを接続させる際に考慮すべきこと

スマートフォンを組織内のネットワークに接続させる場合には、直接接続させるのではなく、スマートフォン専用のネットワークセグメントを用意し、当該セグメントにのみ接続させるべきである。この際、他のネットワークセグメントのセキュリティレベルが当該セグメントより低い場合（たとえばより簡易な方法で接続できる wifi ネットワークが隣接している等）、利用者による制限回避を誘発する恐れがあるので注意が必要である。

スマートフォンを専用ネットワークにのみ接続させるため、対象機器の識別情報（MAC アドレス、クライアント証明書、他の認証システムとの連携　等）をあらかじめ確認し、当該情報を入力しないと接続できないようアクセス制御（あるいは未登録機器の接続を検知する仕組みの導入）を行う必要がある。

スマートフォンの業務利用開始後は、スマートフォン専用ネットワークのトラフィックをモニタリングするとともに、不正な接続や利用がないか、機器の接続ログを定期的に確認することが求められる。

このほか、汚染されたスマートフォンの接続や、不適切な状態（たとえば root 化、Jailbreak によりセキュリティ機能が解除された状態）での利用を検出するため、当該セグメント内の端末に対して定期的にポートスキャンを行うなどの対策も検討すべきである。

<組織のネットワークにスマートフォンを接続させる際のセキュリティ対策項目>

No	対策	チェック
1	スマートフォンを接続させるネットワークセグメントは、組織内の他のネットワークセグメントと分離しているか。	□
2	スマートフォン専用セグメントと隣接する他のネットワークセグメントでは、スマートフォン専用セグメントと同等以上のセキュリティレベルが確保されているか。	□
3	スマートフォンを専用ネットワークにのみ接続させるためのアクセス制御を実施しているか。（MAC アドレス、クライアント証明書、他の認証システムとの連携　等）	□
4	スマートフォン専用ネットワークのトラフィックをモニタリングしているか。	□
5	スマートフォン専用ネットワークにおける機器の接続ログを定期的に確認しているか。	□
6	スマートフォン専用ネットワークに汚染状態あるいは不適切な状態の機器が接続されていないことを確認しているか。	□

3.1.3 スマートフォンにおけるアプリケーションの利用に関する考え方

スマートフォン上で利用できるアプリケーションは無数に存在しており、大まかに以下のように分類することができる。

No	機能的分類
1	スマートフォン内で動作が完結するもの
2	外部サービスとの連携を行うもの
3	スマートフォンにサーバ機能を付加するもの
4	特権の獲得を可能にするもの（特権制御機能を無効化するもの）

No	提供形態による分類
5	スマートフォンメーカーが開発するもの
6	サードパーティーが開発し、キャリアやスマートフォンメーカーが承認するもの
7	サードパーティーが開発し、キャリアやスマートフォンメーカーに承認されていないもの

スマートフォン上で動作するアプリケーションに関する注意事項を以下に示す。IT 管理者は下表の「△」に該当するアプリケーションの情報を収集し、組織内で利用されていないことを確認すべきである。

		機能			
		1	2	3	4
提供形態	5	○	●	●	（存在しない）
	6	○	●	●	（存在しない）
	7	△	△	△	△

注意すべき事項と対策	
○	特に注意すべき事項はない
●	意図しないデータ漏出が起こる可能性があるため、「**3.2.2 スマートフォン上で利用するデータに関する考え方**」に示した事項を理解させた上で利用させる必要がある
△	意図しないデータ漏出、誤作動、故障、汚染等の可能性があるため、利用すべきではない（但し、ブラウザから利用する Web アプリケーションについては、個別に判断が必要）

<スマートフォン上で利用できるアプリケーションに関するセキュリティ対策項目>

No	対策	チェック
1	業務で利用するスマートフォンに導入すべきでないアプリケーションを特定しているか。(ブラウザから利用する Web アプリケーションも含む)	□
2	業務で利用するスマートフォンに導入すべきでないアプリケーションが組織内で利用されていないことを確認する手段を準備しているか。 **<確認手段の例>** ・スマートフォン専用セグメントに対するスキャン ・組織内で利用されているスマートフォンに導入されているアプリケーションの確認	□
3	業務で利用するスマートフォンに導入すべきでないアプリケーションが組織内で利用されていないことを確認しているか。	□

3.1.4 スマートフォンの可用性を維持・向上させるために考慮すべき事項

業務に利用するスマートフォンの紛失や盗難、故障が発生した場合、業務に何らかの悪影響を及ぼすこととなるため、速やかに回復できるよう代用品をあらかじめ準備しておく必要がある。また、故障時のメーカーによる補償範囲、補償方法、補償時期及び内容についても、あわせて確認しておく必要がある。

このほか、スマートフォン上に保存するデータは、紛失や故障により一時的または恒久的に失われる可能性があることから、定期的にデータのバックアップを取得しておくとともに、不測自体発生時に迅速に回復するための手順を用意しておく必要がある。

<スマートフォンの可用性を維持・向上させるためのセキュリティ対策項目>

No	対策	チェック
1	スマートフォンが故障した場合に備えて、代用品を用意しているか。 （あるいは、すぐに調達できるよう代用品の選定を実施しているか）	□
2	故障時のメーカーによる補償範囲、補償方法、補償時期及び内容について確認しているか。	□
3	スマートフォン上に保存するデータのバックアップを定期的に実施しているか。	□
4	不測事態発生時に迅速に回復するための手順を用意しているか。	□

3.1.5 スマートフォンの紛失・盗難に備えた対策

業務に利用するスマートフォンの紛失が発生した場合、スマートフォンの不正利用やスマートフォンに格納したデータの漏えいが発生する可能性があるため、速やかに当該スマートフォンの保護措置を講じる必要がある。

また、スマートフォン紛失時の対応（利用者及び IT 管理者の対応）を定め、スマートフォンの利用者に周知しておく必要がある。

※　代替品の確保、回復のための措置は前項にて紹介済み。

〈スマートフォン紛失時のセキュリティ対策項目〉

No	対策	チェック
1	紛失時のスマートフォン保護手段を準備してあるか。 **<保護手段の例>** ・パスワード等による端末（または SIM）のロックの徹底 ・パスワードクラッキング対策の徹底（指定回数以内に正しいパスワードが入力されない場合、データを消去する機能等） ・紛失した端末の探索機能の有効化 ・遠隔からのデータ消去機能の有効化 ・拾得者への連絡先通知機能のテスト　等	□
2	スマートフォン紛失時の対応を定め、利用者に周知しているか。 **〈対応内容の例：利用者〉** ・紛失・盗難発生後即時所属長に連絡 ・紛失した端末の捜索 **〈対応内容の例：IT 部門〉** ・紛失・盗難にあったスマートフォンの識別情報の特定 ・当該スマートフォン保護措置を実施 ・当該スマートフォンの組織内ネットワークへの接続許可の取り消し ・当該スマートフォン利用者の ID の利用停止、パスワード変更の実施 （スマートフォンを利用してアクセスしていた全てのシステム、VPN 等）	□

3.1.6 スマートフォンを廃棄する際に留意すべきこと

業務に利用していたスマートフォンを廃棄する場合、スマートフォン内に蓄積されたデータを利用できないよう処理する必要がある。

なお、スマートフォン上からデータ消去操作や出荷時の設定への復元操作を実行しても、完全なデータ消去とはならない可能性があるため、物理フォーマット、破砕処理等、確実性の高い手段を採用すること。

※ 廃棄対象のスマートフォンが個人の所有物である場合でも、業務に利用していた場合には同等の対策を講じるべきである。

※ 利用者が所有するスマートフォンを機種変更した後、wifi 機能のみで当該端末を利用し続ける可能性も考えられる。このため、機種変更の届出を受けた場合には、旧機種の廃棄時に指定業者による廃棄を誓約させる等の処置が必要となる。

※ スマートフォン内に保存したデータが完全削除できない可能性については、「2.3.5 スマートフォンを廃棄する際の課題」にて紹介済み。

<スマートフォン廃棄時のセキュリティ対策項目>

No	対策	チェック
1	スマートフォン廃棄時のデータの完全消去手段を準備してあるか。 **<データ完全消去手段の例>** ・物理フォーマット機能（あるいはソフトウェア） ・破砕処理　等	□
2	利用者が、自身で所有し、且つ業務に利用していたスマートフォンの機種変更を行う場合の、申請手続きを準備しているか。 ＜申請内容の例＞ ・ 変更前の機器識別情報（メーカー・型番・OS バージョン・業務利用登録番号等） ・ 変更後の機器識別情報（メーカー・型番・OS バージョン・業務利用登録番号等） ・ 変更後も旧機種を利用し続ける場合の制約事項（廃棄時の指定業者での廃棄、現行機器と同程度の管理義務　等）	□

3.2 スマートフォン利用者が考慮すべき事項

3.2.1 スマートフォンの脆弱性対策

スマートフォンは、通話以外にも様々な機能を有しており、それらはスマートフォン上で動作するソフトウェアによって実現されている。一般的に、ソフトウェアには誤作動を引き起こす原因となるバグが潜在しており、何らかのきっかけでバグが露見した場合、スマートフォンの操作に支障をきたしたり、スマートフォン上に保存されたデータが破壊されたりといった好ましくない事象が発生する。

なお、ソフトウェアのバグは不正プログラムの開発者や攻撃者に悪用されることが多い。たとえば、普段利用している Web サイトに、スマートフォンを攻撃するための罠のリンクが仕掛けられていた場合、このリンクをクリックしただけでスマートフォンの制御を奪われ、外部から遠隔操作されたり、保存したデータを盗まれたりする可能性がある。

通常、ソフトウェアにバグの存在が確認された場合、メーカーからバグを修正するための修正プログラムが配布される。バグの影響を未然に回避するために、メーカーからバグの存在と修正プログラムの配布がアナウンスされた際には、速やかにこれを利用し、バグを解消することが必要となる。また、修正プログラムの適用方法は、スマートフォンの機種により異なるため、利用するスマートフォンのアップデート方法をあらかじめ確認しておく必要がある。

<スマートフォン利用時の脆弱性対策項目>

No	対策	チェック
1	スマートフォンのメーカーから公表される修正プログラムやアップデートに関する情報の入手方法を知っているか。	□
2	利用しているスマートフォンのアップデートあるいは修正プログラムの適用方法を知っているか。	□
3	メーカーから公表されたアップデートや修正プログラムをタイムリーに適用しているか。	□

3.2.2 スマートフォン上で利用するデータに関する考え方

近年のスマートフォンでは、さまざまな形式のデータを扱うことができる。たとえば、PDF ファイルや Microsoft Office 形式のファイル等、PC で作成したデータを閲覧あるいは編集することが可能である他、アドレス帳やスケジュール、ブックマークに登録したデータを PC や外部の Web サービスと同期させることも可能となっている。この他、メールアカウントや、よく利用する Web サイト（場合によっては組織内の情報システム）のパスワード等のデータも、パスワードリマインダ等に保存されていることがある。

スマートフォンのユーザインターフェースは PC と比較するとシンプルに作られているため、利用者はデータの保存場所を意識することなくこれらのデータをシームレスに利用できる。それゆえに、取り扱うデータが意図しない場所に、意図しない形で保存（漏出）される可能性がある。

したがって、スマートフォンで各種のデータを取り扱う場合、そのデータが、どこに、どのような形で保存されているのかを常に意識する必要がある。特に、業務資料やアドレス帳、スケジュールデータ等、万が一事故が起きた場合に組織や顧客に悪影響を及ぼす可能性のあるデータを外部の Web サービスに保存する際には、何らかの保護措置を講じた上で保存するなどの注意を払うことが求められる。また、所属する組織の情報と自身のプライベートな情報を混同しないよう注意を払うことも重要である。

<スマートフォン上でデータを扱う際の留意事項>

No	対策	チェック
1	スマートフォンで各種のデータを取り扱う場合、そのデータがどこに、どのような形で保存されているのかを意識しているか。	□
2	業務資料やアドレス帳、スケジュールデータ等、万が一事故が起きた場合に組織や顧客に悪影響を及ぼす可能性のあるデータまたはそのバックアップを外部の Web サービスに保存する際に、以下のような保護措置を講じた上で保存しているか。 **<保護措置の例>** ・業務資料やアドレス帳データについては、暗号化した上で保存する （あるいは、データ送信経路及び保存先の暗号化機能があることが確認されている外部 Web サービスを利用する） ・業務スケジュールのデータについては、顧客名を記載しない 等	□
3	所属する組織の情報と自身のプライベートな情報を混同しないよう注意を払っているか。 **<混同防止措置の例>** ・組織のメールとプライベートなメールのメールボックスを分離する ・組織のアドレス帳データとプライベートなアドレス帳データを分離する 等	□

<取扱いに留意する必要があるデータと想定される保存先の例>

No	データ項目	想定される保存先
1	PC で作成したデータ	・スマートフォン内の記憶領域 ・スマートフォン内のデータのバックアップ先（PC、オンラインストレージ等） ・メールサーバ上 ・外部の Web サービス
2	スケジュールデータ・ アドレス帳	・スマートフォン内の記憶領域 ・スマートフォン内のデータのバックアップ先（PC、オンラインストレージ等） ・外部の Web サービス
3	アカウント情報	・スマートフォン内の記憶領域（パスワードリマインダ） ・スマートフォン内のデータのバックアップ先（PC、オンラインストレージ等） ・外部の Web サービス

3.2.3 スマートフォンの不適切な利用がもたらす影響と留意事項

スマートフォンの高度な利用を可能にすることを目的として、ソフトウェア的にスマートフォンを改造するための手段（いわゆる Jailbreak／root 化）が提供されている。

具体的には、スマートフォンに搭載されるファームウェアの脆弱性を悪用し、ファームウェアの改ざんを行うことで、スマートフォンの操作者に付与された権限を昇格させる手段である。

改造行為により、スマートフォンメーカーが承認していないソフトウェアを（多くの場合無料で）利用できるようになるほか、使い勝手が向上するなどのメリットを享受することができる。

但し、改造を施した場合、当然ながらメーカーによる補償が受けられなくなるほか、スマートフォンのセキュリティ保護機能が働かなくなるため、故障や汚染等の確率が飛躍的に高まるというデメリットがある。実際、改造を施したスマートフォンにのみ感染するウイルスの存在も確認されている。改造を施したスマートフォンがウイルスに感染し、他者（知人、同僚、顧客など）のスマートフォンや他の組織に攻撃を仕掛けた場合には、組織の責任問題にまで発展する可能性がある。

業務に利用しない個人のスマートフォンの改造に関しては、自己責任で判断すべきところであるが、業務に利用するスマートフォンの改造行為は、組織や他の利用者に迷惑をかけることになるため、控えるべきである。

<スマートフォンの不適切な利用がないことの確認>

No	対策	チェック
1	改造（Jailbreak/root 化）したスマートフォンを組織内に持ち込んだり、業務に利用したりしないこと	□

4. スマートフォン端末の管理

4.1 サービス提供者側でのスマートフォン端末管理

4.1.1 スマートフォン端末の管理対象の明確化

スマートフォン端末利用者に対して社内情報システムサービスを提供するには、サービス利用ルールを定め利用者全員に周知するとともに、管理対象となる端末の識別、識別した端末と利用者との紐付け、紐付けできない端末のサービス利用停止を実施する方法を確立することが望ましい。これらは個人所有のスマートフォンにおいても同様であることが望ましい。

また、情報システムサービスを提供する側が管理対象となるスマートフォン端末を効率的に把握するため、予め利用者の所持するスマートフォン端末の利用申請を受け付けることで管理対象を明確にすることが望ましい。

4.1.2 スマートフォン端末の識別

サービス提供者は、社内システムを利用する端末を管理対象となっている端末に限定するため、社内ネットワークに接続する端末を識別する方法を確立することが望ましい。ネットワーク接続時のスマートフォン端末を識別する例として以下の方法がある。

・スマートフォンは、専用の無線ネットワークに接続する

・無線ネットワークへの接続時には、なんらかの方法（※）により識別を行う

・VPN への接続時には、端末固有の情報（※）により識別を行う

・アクセスの都度、利用者の認証を行う

※ MAC アドレス認証、クライアント証明書による認証など。

（MAC アドレスによる識別を採用する際は、MAC アドレスを偽装される可能性を考慮するべきである。）

4.1.3 不正端末の排除(不正端末を定義すること)

サービス提供者は、不正端末を発見した場合は、ネットワークから排除する方法を確立することが望ましい。

No	対策	チェック
1	個人所有のスマートフォンも含め管理対象とする端末の定義がなされているか。	□
2	管理対象となった全ての端末の識別と利用者の紐付けはされているか。	□
3	管理対象外、又は上記項目2の条件が満たされない端末に対して、サービス利用停止する方法を確立しているか。	□

4.2 サービス提供者側でのセキュリティ対策

スマートフォンは携帯電話の特性とPCの特性を併せ持っている。しがって、スマートフォンを利用する際のセキュリティ対策は、その特性上 PC に比べて様々な違いがあることを認識し対応する必要がある。特に、ログの取得が困難であったり、端末の盗難や紛失の可能性が高いにもかかわらず大容量の記憶媒体として利用できたり、PC 同様に脆弱性が存在するため、OS バージョンアップや不正プログラム（マルウェア等）対策が必須となる。また、業務に関係のないアプリケーションを利用するシチュエーションが多いことから、悪性アプリケーションの利用の可能性も高い。

4.2.1 ログの取得

スマートフォン端末のローカルでの操作ログ取得は難しいため、認証サーバや情報システム側のログを取得・管理するしくみを確立し、ログ分析を適切に行うことが望ましい。また、携帯性の高さから複数のアクセスポイントを動的に利用する特性があるため、中継ポイント(HTTP の Proxy や認証 Proxy 等)を設けてアクセス経路をコントロールしそのログを取得することも検討する。

No	対策	チェック
1	スマートフォン端末のログ解析を適切に行う仕組みがあるか。	□

4.2.2 インシデント発生時の対処と体制整備

インシデント発生時の対処を十分検討し実装するとともに、速やかに対処するための体制を整備し定期的に訓練を実施する。また、インシデント発生時の対処はスマートフォン端末の機種毎に機能や操作が異なることに留意する。特にスマートフォンは PC にくらべ盗難、紛失しやすいため、リモートロック、リモートワイプなどの対処を検討し、個人所有のスマートフォンであっても同様の対処が可能となるようオペレーションを確立しておくことが望ましい。

なお、海外勤務者にもスマートフォン利用を許可する場合には、24 時間 365 日のインシデント対応オペレーションを想定しておくことが望ましい。

No	対策	チェック
1	スマートフォンのインシデント発生時の対処を十分検討しているか。	□
2	対処を適切に実施する体制を整備し十分に訓練されているか。	□

4.2.3 スマートフォン端末の脆弱性対策

スマートフォン端末も PC と同様に OS やアプリケーションに脆弱性があるため、常に最新のバージョンアップやパッチ適用、不正プログラムのインストールをさけるための対処も必要である。そのためにソフトウェアの自動更新設定を必須とするべきである。また特に個人所有のスマートフォンにおいてバージョンアップするための PC を持っていない状況がある。この場合、使用を許可しないことが望ましい。但し、OS やソフトウェアの更新により、スマートフォンに搭載されるアプリケーションの仕様が変更され、社内システム利用時の互換性に問題が生じる可能性がある点に留意する。

マルウェア対策や不正プログラム対策において、不正プログラムの自動検出、駆除設定のしくみは PC に比べると遅れているため情報収集を欠かさない努力をする。メーカーによって、端末の初期化の手順が発表されていないか、初期化できないものも存在する。特に初期化できないものは、利用許可しないことが望ましい。

ウイルスチェッカー等の不正プログラム検知システムは一般にパターンファイルを持つことが多い。このようなパターンファイルは一般に自動的に更新するためのしくみが提供されている。従って、自動更新設定を施すことが望ましい。

※OS の更新には、PC が別途必要になる場合がある。安全が確認されている PC を用いて更新作業を行うことが重要である。また、OS 以外に導入しているアプリケーションも自動更新機能があるものは、適切な設定を行い、その機能がないアプリケーションについては、個々に更新を行う必要がある。

No	対策	チェック
1	OS やアプリケーションに対して常に最新バージョンとする仕組みがあるか。	□
2	マルウェア対策や不正プログラム対策を実施しているか。	□
3	上記項目1,2のような脆弱性対策に関する最新情報を常に収集しセキュリティ管理業務に反映しているか。	□

4.2.4 サーバにおける対策

管理者は、社内の情報システム（サーバ）へのスマートフォン端末からのアクセスを許可する際、暗号通信機能の実装を検討する。たとえば、外部のフリースポット等からスマートフォン端末を利用して社内のシステムを利用するといった用途が想定される場合は、盗聴などの対策のため、VPN の利用を強制するかサーバと端末の間の通信がすべて暗号化されるようにすることが望ましい。

（例）Web のサービスであれば SSL を実装する等

（例）外部からの通信は、VPN を利用する等。

4.2.5 ネットワークにおける対策

管理者は、スマートフォン端末を社内ネットワークに接続させる際、以下の項目を検討し問題のないことを確認する。接続を許可する場合、接続設定を会社の掲示版等、誰にでも閲覧できるような場所に公開しないことが必要である。接続に問題のある場合、例えばネットワーク帯域を消費する通信（ファイル交換、ストリーミング等）、社内ネットワークに接続させず、3G でのリモート接続のみとすることも考慮する。

以下に、スマートフォン端末を社内ネットワークに接続させる際に検討可能なコントロールについてまとめた。また、これらのコントロールはスマートフォン端末が情報システムにアクセスする際の利用者の認証方式も含めて検討することが望ましい。

コントロール		社内無線LANに接続		社内無線LANに非接続
		既存LANに接続	専用LANに接続	
NW帯域優先制御		困難	境界 S/W で可	不可
アイソレーション		不可	可	不可
社内サーバアクセスコントロール	IP/Port	不可	可	困難
	フィルタ	不可	可	困難
	プロファイル	可	可	可
社外サーバアクセスコントロール	IP/Port	可	可	—（キャリア）
	フィルタ	可	可	—（キャリア）
	プロファイル	可	可	可

4.2.6 マルウェア感染

マルウェア感染事象を速やかに発見するため、ネットワークのセキュリティ監視を実施する。発見されたマルウェア感染端末に対しては速やかにネットワークから排除し適切な処置を実施する。これには以下のようなセキュリティ監視方法がある。

・侵入検知システム（IDS）による攻撃検知

・侵入防止システム（IPS）による攻撃遮断

また、社内情報漏えいのリスクを想定し、スマートフォンから発信される社外への通信を監視するために、DLP の導入も考慮した方が望ましい。

※ スマートフォンから発信される社外への通信の検査は、データ流出経路が複数あるためその追跡が不可能なケースが多い。（3G はキャリアの協力が必須）

No	対策	チェック
1	マルウェア感染事象を発見するためにネットワークセキュリティ監視を実施しているか。	□

4.3 サービス利用者側でのセキュリティ対策

4.3.1 盗難、紛失

スマートフォンは PC と比較して、盗難や紛失などのインシデントが多いと予測されるため、その対処を十分に検討し実施する。機種およびメーカーが提供する管理ツールによりパスコードロック、リモートワイプなどが可能であるためそれを利用する。

業務利用許可をする際、インシデント発生時にワイプする許可を得るなど、事前に協議し、承認させる。

・遠隔からの端末ロック機能の有効化

・遠隔から端末内データ消去機能の有効化

・遠隔から端末の位置情報特定機能の有効化

No	対策	チェック
1	盗難/紛失対策を十分に検討し実施しているか。	□

4.3.2 Web システム画面の改修

スマートフォン端末から利用させる Web システムについては、端末からの閲覧を考慮した画面の開発を検討する（閲覧性、操作性の改善）。また、スマートフォン端末から利用させる Web システムについては、端末にデータをダウンロードする機能の利用を制限することが望ましい。

※ 「2.3.3 スマートフォン上で取り扱うデータに関する課題」にて紹介したソリューションにより、データ保護に加え、画面の最適についてもカバーできる可能性がある。

No	対策	チェック
1	Web システムはスマートフォン端末からのアクセスの利用目的を想定した開発を検討しているか。 ・閲覧製、操作性の改善 ・サーバからのデータのダウンロードの制限	□

5. スマートフォンの利用シーンとセキュリティの課題

5.1 リスクの分類とアプリケーション

スマートフォンの業務利用シーンとセキュリティの課題を明確にするために、アプリケーションで生成されたデータがどこに残るかを分類し、想定されるリスクをまとめた。その上で、一般に利用される可能性の高い、代表的なアプリケーション毎に、分類したリスクを紐付けた。

※分類 D は存在が確認されていないが、将来的に十分ありえる

分類	説明	想定リスク	対策例
A	スマートフォン自体にデータが残る	・ 紛失時にデータが盗まれる ・ マルウェアによってデータが盗まれる ・ 誤操作で消去してしまう ・ システムへの ID やパスワードが盗まれる	データの暗号化 遠隔管理機能 不正プログラム対策 ソフトウェア更新機能
B	自社で管理するシステムにデータが残る	・ ID やパスワードが漏れた場合にデータへのアクセスが可能になる ・ 自社管理システムのセキュリティ担保が難しい ・ アクセス権限管理を正しく行っていない場合に、データを見ることが可能 ・ 権限者以外がデータを閲覧取得することが可能	通信の暗号化(VPN) 通信経路指定
C	管理権限のないシステムにデータが残る	・ データの削除が適正に行われたかが不明 ・ データへのアクセス記録が確保されるか不明 ・ 問題発生時の対策が遅れがちになる ・ 問題対応が可能かどうか不明 ・ システム側がデータを見ることが可能 ・ システム監査への対応が難しい ・ 情報が漏えいした場合の責任範囲が不明確 ・ システム(アプリ)提供者の信用調査が困難	データバックアップ アプリケーション選定 ソーシャルメディアポリシ
D	どこにデータが残るか判らない	・ データへのアクセスなどを含め、全てがリスクになる	―

以下に対策例の補足をまとめる。

① データの暗号化：
- スマートフォン内に保存したデータを暗号化できること
- 暗号化、複合処理を行うための機能を搭載していること

② 遠隔管理機能
- 管理者の操作により遠隔から端末の機能をロックできること
- 管理者の操作により遠隔から端末内の全データを消去できること
- 管理者の操作により遠隔から端末の位置情報を特定できること

③ 不正プログラム対策機能
- 不正プログラムを自動で検出、駆除できること
- 不正プログラム検知のためのパターンファイルを自動更新できること
  ※ソフトウェアの追加により実現する形でもよい

④ ソフトウェア更新機能
- 基本ソフトウェア（OS、ファームウェア）の更新機能を有していること
- 追加ソフトウェアの更新機能を有していること

⑤ 通信の暗号化：
- SSL 通信機能を有していること
- 端末認証のためのクライアント証明書が利用できること
- IPSec、L2TP、PPTP による仮想専用線（VPN）機能を有していること
- VPN 接続が切断された場合、自動で再接続されること
- VPN 接続状態であることが利用者にわかりやすく表示されること

⑥ 通信経路指定機能
- 全てのネットワークインターフェースにおいて、通信経路を制御できること

カテゴリ	アプリケーション		分類		
			A	B	C
音声通話	通話（履歴）		○		○
リアルタイムメッセージ交換	MS メッセンジャー				○
	ICQ				○
非リアルタイムメッセージ交換	SMTP		○	○	
	IMAP		○	○	
	Web メール(社内サーバ)			○	
	Web メール(SP サーバ)				○
	Exchange		○	○	
	SMS		○		
グループウエア	スケジュール 掲示板 ワークフロー 各種 D/B 社内 SNS 営業システム その他業務システム	オンライン専用 Exchange (OWA)		○	○
		オフラインが利用できるもの Exchange (EAS)	○		
				○	○
ドキュメント作成 閲覧 ファイル共有	MS-Office、 GoogleApps、 Evernote、 Dropbox、 Sugersynk、Springpad		○	○	○
GPS アクセス	地図検索、 現在位置確認 および経路検索 ※		○		(○)
SNS	Facebook, Twitter, Mixi, ※ソーシャルメディアポリシ等、業務情報を発信する行為に関してリテラシの問題が大きい		○		○

5.2 その他

- 基幹システム（契約・顧客管理）を利用し顧客情報を取り扱う場合は、画面ハードコピー（スクリーンショット）により情報漏えいが容易に出来ることを考慮し、構成管理ツールなどで制御する。
- PDFファイルやOffice関連ファイルも、使用アプリによっては、ローカルに保存し、メールで社外に送信可能となるため利用禁止事項とする（物理的に制限できない）。
- 公衆無線LANサービスの利用（iPhone であれば、モバイルポイントを無償で利用可能となる）において無線 LAN のアクセスポイント（有料・無料を問わず）を利用する際には、他の第三者が共用 AP に接続している危険性を考慮する。業務アプリが入った端末を利用する際には、通信の暗号化(IPSEC)などや、サーバ証明書などで安全性を考慮する。
- PC との USB 接続による記憶媒体としての利用は外部記憶媒体としての管理や情報漏えい対策の対象として検討する。
- スマートフォンの利用シーンの特性により、ショルダーハックの危険性とその対策を検討する。プライバシーフィルタ、覗き見防止フィルタなど、視野角をコントロールできる機能のフィルタを推奨する。

5.3 推奨アプリケーションの提示

利用者からアプリケーションのインストール相談を受けた場合、可能な限り検証環境において当該アプリケーションの動作検証を行い、社内システムに及ぼす影響を調査することが望ましい。
また、以下の方法により不適切なアプリケーションの排除を促す。

- アプリケーションのブラックリストを作成する。
- 信頼できるアプリケーションマーケットプレイスを周知する。
- アプリケーションをインストールする際の注意事項(許諾メッセージ・アクセスできる情報の許可)を確認する。

No	対策	チェック
1	利用者に対し、常に業務利用に適切なアプリケーションを提示しているか。	□

6. サポート

6.1 情報の提供

6.1.1 利用にあたっての注意事項の整理

パスコード設定、業務システム利用後の WEB 閲覧履歴削除など、個人所有のスマートフォンを利用する場合に最低限注意すべきことは必須としてアナウンスする。

・禁止事項

⇒ アンチウイルスソフトの停止

⇒ JailBreak、root 化等、メーカーサポート対象外となるような端末の利用

・インシデント発生時のフロー整備（4.2.2. 参照）

・バージョンアップ情報（ファーム、アプリケーション）

・情報システム管理者は最新の OS を検証する。バージョンアップできない機種に対して明確な脆弱性が確認された場合は使用を禁止させる。

・機種変更の際、リスクをもつアプリケーションを利用した場合は廃棄方法のルールを検討しておく。

No	対策	チェック
1	利用者に対し、整理された注意事項を周知徹底しているか。	□

6.2 ヘルプデスク

スマートフォン端末を業務に利用する際には、導入台数(利用者数)にあわせてヘルプデスクを設置し、予め想定されるセキュリティ事件・事故の発生を低減させることが望ましい。対応を効率化するため FAQ を構築し利用を利用者に促すことが望ましい。

・社内ネットワークの接続に関する申請や方法

・インシデントへの対応

・ホワイトリスト・ブラックリストに関する問い合わせ

・新たにインストールしたいアプリの安全性に関する相談

・会社側が許可した利用業務に対してのサポート

※ 既存のヘルプデスク業務の延長だが、導入するスマートフォン環境に依存する部分については、ヘルプデスクの教育が必要

・スマートフォン機器固有のサポート

※ 社内ヘルプデスクで対応が難しい場合があるので、メーカーのサポート情報が必要

・キッティング

※ 社内利用に適したスマートフォンにするためキッティング

No	対策	チェック
1	スマートフォン利用において、円滑で正しく安全な利用となるように促すためのヘルプデスクを設置しているか。	□

以上

JNSA 調査研究部会 スマートフォン活用セキュリティポリシーガイドライン策定ワーキンググループ

ワーキンググループリーダー

加藤 智巳	株式会社ラック

メンバー

田巻 義一	イーデザイン損害保険株式会社
田中 洋	株式会社インフォセック
鈴木 伸	NRI セキュアテクノロジーズ株式会社
西田 助宏	NRI セキュアテクノロジーズ株式会社
霜野 仁美	株式会社 NSD
竹本 哲也	株式会社 NSD
肥田 雄一朗	クオリティ株式会社
柏崎 央士	グローバルセキュリティエキスパート株式会社
清水 邦夫	グローバルセキュリティエキスパート株式会社
鹿野 恵祐	一般社団法人 JPCERT コーディネーションセンター
丸山 龍一郎	株式会社シマンテック
石田 淳一	独立行政法人情報処理推進機構
岡本 勝之	トレンドマイクロ株式会社
林 憲明	トレンドマイクロ株式会社
大津留 史郎	日本アイ・ビー・エム株式会社
渡邉 浩一郎	日本アイ・ビー・エム株式会社
安達 智雄	日本電気株式会社
柴田 浩一	日本電気株式会社
小早川 知昭	日本ベリサイン株式会社
相原 弘明	株式会社ネットマークス
中谷 忍	株式会社日立情報システムズ
板倉 博和	株式会社日立ソリューションズ
窪田 秀正	株式会社日立ソリューションズ
市橋 満	マカフィー株式会社
大野 祐一	株式会社ラック
許 先明	株式会社ラック
山城 重成	株式会社ラック
吉田 裕美	株式会社ラック

（会社名 五十音順）