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 ～

1.0 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

2013 年 3 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が大幅に進んでいる。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、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、利用者の利便性は劇的に向上した。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縮まりつつある。
スマートフォンは PC と比較して、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。また、ユーザー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。
その一方で、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。さらに組織にとって最も重大なセキュリティリスクの一つである情報漏えいが、PC 並の能力と極めて高いモビリティを同時に実現したスマートフォンの特長ゆえ潜在的に発生しやすくなっているとも考えられる。
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
  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、ユーザー個々のセキュリティリテラシーを上げ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組織の責任と、ユーザーリテラシーの境界線を明確化し、組織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。

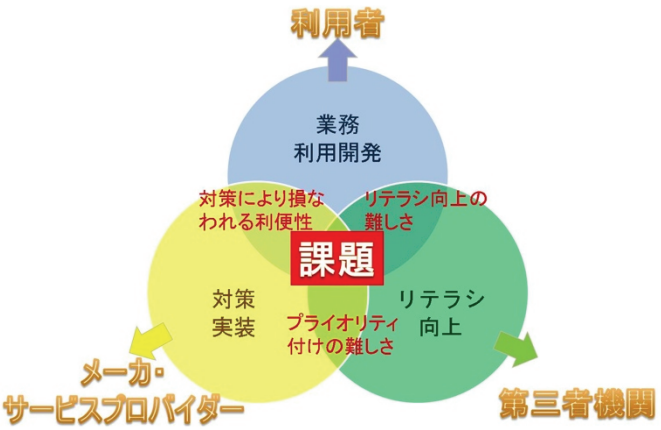
本ガイドラインの利用のしかた

スマートフォンの位置づけ

このガイドラインでは、組織内の業務においてスマートフォンを安全に利用することを検討する際に必要な情報を掲載するよう努力した。我々の前提として、スマートフォンの普及において、個人所有のものが組織による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組織内統制が利かないと予測されると考えた。そのため、今までのような私物と支給物としての機器の区別はスマートフォンに適用することは困難であると考え、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、これまで一般の組織が目指すセキュリティポリシー(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、本来、組織がスマートフォンに期待する生産性の向上や機動力、携帯性を著しく損なう可能性がある。

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である。



[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、組織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。従って、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、課題を解決する必要がある。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、すべてのリスクを等しく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いる。スマートフォンはその携帯性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。リテラシを教育やルール、ドキュメントなどで向上させようとしてもその効果は限定的であるため、タイムリーなリスクの顕在化と、組織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。

ゆえに、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。

本文書が提示する課題に関する注意点
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組み込ま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

このガイドラインは、2011 年 4 月にリリースした「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」の内容を踏襲しながら、ネットワーク技術や認証技術、運用面を追記し、より現場での安全なスマートフォン利用に役立てられるよう配慮した。これから導入を検討する、または導入したがより安全かつ快適に利用できるよう改善させる責任者や担当者の方々の参考として頂きたい。

1. スマートフォンとはどのようなものか

1.1 スマートフォンのセキュリティを考える

スマートフォンは、その形態から「携帯電話の高機能版」という考え方と、「電話機能を持つ小型化したパソコン」という考え方があり、これはどちらが正しいというものではない。しかし、これから組織内にスマートフォンを導入するという状況となった場合には、スマートフォンを「小型のパソコン」として取り扱うべきである。なぜならば、組織内のネットワークは様々な理由から十分に保護されなければならず、そのためには最悪を想定し、スマートフォンを「脆弱なデバイス」であるという認識のもとにネットワークの設計・管理・運用が必要となるからにほかならない。

組織内部にスマートフォンを導入するにあたって考慮すべきは、まず、BYOD(Bring Your Own Device)を認めるかどうかである。

スマートフォンは、その特性上、個人持ちの携帯電話として購入され利用されることが多い。このような状況では、電話帳のような個人的な情報が大量に登録されていることが想定される。その上で、電子メールやウェブアクセスの記録、様々なアプリケーションの導入など、個人が利用しやすいように成長していく。

このような特性を考えれば、携帯電話のように「業務用として組織が支給する」というモデルはうまくいかなくなる可能性が高い。まず、スマートフォンにおける情報の同期において、組織のシステムだけを利用する方式では、そのスマートフォンの利便性を大いに損なうことが挙げられる。また、すでにスマートフォンを持っている利用者にとって、スマートフォンの使い分けを行うことは、利用者の利便性を大きく制限することとなる。なぜならばスマートフォンは携帯電話の何倍もの情報を扱うため、端末間で情報の同期が取れないとうことは、端末の使い分けを状況に応じて強いることになるからである。

ゆえに、すでにスマートフォンを持っているユーザーに対して2台目以降のスマートフォンを配布したとすると、「組織支給のスマートフォンに業務外の情報を大量に投入する」もしくは、「個人持ちのスマートフォンに業務情報を投入する」という状況が発生することは容易に想像できる。もちろん規定などで縛ることは可能であるが、その規定が有名無実になったり、規定のためにスマートフォンの業務利用が阻害されたりしては、意味がない。さらにセキュリティ面で苦慮すべき事柄として、Android 端末、iOS 端末で脆弱性が発見される度に対策された最新 OS へ更新できない旧端末が、導入一定期間後には必ず存在してしまう現実がある。ここで該当端末を利用機能を限定するなどして使用を継続するか、新型機へ機種変更するかシステム管理者の判断が必要となる。

スマートフォンの業務利用に関しては、特に利用者の教育も必要となることが予想される。スマートフォンは、一般には携帯電話の延長ととらえられることが多く、個人使用のイメージが強いものである。したがって、業務利用されるスマートフォンには、業務情報だけで無く個人情報も大量に蓄積されることが予想される。このようなデバイスにおける情報の取り扱いは、システム管理者、利用者ともに知識や経験が不足しているのが日本における現状であろう。このような点を考慮すれば、スマートフォンの業務利用に当たっては、利用者のリテラシーの向上が必要であると考えられる。

本ガイドラインは、BYOD を推進する意図はない。しかし、スマートフォンの導入を考慮すると事実上の

BYOD 状態になってしまう可能性がある。このような状況を考慮すると、スマートフォンを収容するためのネットワークを独立させて、既存の組織内サービスネットワークを保護するような対策を講じることが必要であろうと考える。

1.2 特徴

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（無線 LA ネットワーク無線 LAN）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（組織・組織）向け構成管理機能

スマートフォンは、機能的にも、構造的にも、PC に近い特徴を有している。携帯電話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、移動中での地図・GPS の複合的な情報の参照や内蔵カメラの画像データを使ったコンテンツの作成・更新が即時に行えるなど、PC では使い勝手に難があり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。また、ウルトラブックやタブレット PC の登場により、PC とスマートフォンの境界は非常に曖昧になりつつある。

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（通信事業者回線）
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
Android	Google	Linux
iOS	Apple	Mac OS
BlackBerry	RIM	独自 OS
Windows Phone	Microsoft	Windows

※「Android」は Google Inc. の商標です。

※「iOS」は Apple Inc. の商標です。

※「Black Berry」は Research In Motion Limited の商標です。

※「Windows Phone」は Microsoft Corporation の商標です。

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。

1.2.4 スマートフォンと ID

スマートフォンは、本体のパスワードとは別に、連携したサービスの利用や管理などに ID が必要となっている。スマートフォンの管理で使用する ID は、主に以下のものがあげられる。

- Android 端末：Google アカウント
- iOS 端末：Apple ID
- Windows Phone：マイクロソフトアカウント

スマートフォンのユーザー情報は各アカウントに紐付けられ、スマートフォンの種別ごとに提供されている公式アプリケーションストアの利用はアカウントが必要となる。スマートフォンを購入・導入の際に新規にアカウントを作り端末を登録するか、既存のアカウントに端末情報を登録する。
このアカウント情報はスマートフォン本体での利用以外にも、ブラウザ経由などでアクセスすることが可能であり、スマートフォンの現在位置、電話帳、メールの閲覧、アプリケーションの導入状況の確認や新規導入、端末のデータ消去などが可能である。第三者にアカウントを窃取された場合、こうした行為が遠隔から行われる可能性があるため、アカウントには強固なパスワード使用し、管理には注意が必要である。

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。

2.2 脆弱性管理における課題

2.2.1 スマートフォンの潜在的な脆弱性とその影響

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。

導入された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。

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
  - 本来不要である情報にアクセスするようなソフトウェア
- ファームウェアの汚染(マルウェア感染など)、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を修正した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 やアプリケーション配布サイトから修正プログラムを（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。

特に対策版 OS や修正アップデートが提供される場合でも、端末メーカー、通信キャリアの提供スケジュールにより修正が間に合わずゼロデイ攻撃を受けてしまう可能性がある。脆弱性に対する脅威の危

険度、攻撃手法の容易さ、端末データと通信アカウント保護の観点から最低限の対策が完了するまで、該当端末の運用制限、一時利用停止と復帰、端末の機種変更、と判断基準を運用シナリオに含めておきたい。

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利用シーンには、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、以下のような形で組織内システム/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 または無線 LA ネットワーク無線 LAN 機能により組織内ネットワークに接続
（y） 組織内 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ネットワークの準備

2.3.2 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組織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組織内システムの利用を実現することができる可能性がある。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組織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。

2.3.3 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、故障時、紛失機内のデータにアクセスできなくするようなロック対策や、迅速な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重要となる。

2.3.4 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、例えば、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など、root 化や Jailbreak しなければアクセスできない領域があ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。

2.4 組織内ネットワークへの接続の課題

2.4.1 組織内システム/ネットワークへの影響

組織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されていた場合、汚染データを組織内ネットワークに撒き散らす可能性が高くなることとなる。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組織内のネットワークを分離する必要がある。

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、まず検討するべき要素はセキュリティ管理手法の違いである。同一のネットワークに異なる管理手法が要求される端末を接続することは、運用管理を煩雑にするばかりでなく、セキュリティ対策ソリューションの無力化やインシデントの潜在化、対策の形骸化につながることが予想される。

2.4.2 接続方式選定

以下に PC とスマートフォン、有線 LAN と無線 LAN の組合せによる接続の分離パターンをまとめた。

有線 LAN	無線 LAN	解説
PC	PC＋スマートフォン	PC とスマートフォンの同居状態であり、運用面やセキュリティ対策で様々な課題が生まれる
PC	PC とスマートフォンの分離	PC とスマートフォンの別居状態であり、無線 LAN 環境において端末識別や認証の仕組みを取り入れることが必要
PC	スマートフォン	PC とスマートフォンの独居状態であり、端末識別の必要性が低下する

なお、本ガイドラインでは、PC とスマートフォンを同一の LAN に接続することが許可される環境は推奨しない。

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、スマートフォンは組織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、紛失や盗難などの被害に遭いやすいデバイスである。したがって、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。機器を選定する際には、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）を有するかについても考慮すべきである。

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。そのほか、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	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。または、満たしていない場合、スマートフォン利用に関するルールを新たに定めているか	□
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認める場合に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・利用の可視化(可能な場合は制御)機能	□
7	「端末管理機能」 ※ログ採取機能があるスマートフォンは稀であると思われる	□
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	「端末システム制御機能（利用者によるセキュリティ設定の変更制限、認められない特権奪取など）	□

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、従来の業務 PC ネットワークに直接接続をさせるのではなく、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、当該セグメントを経由して接続させることが望ましい。これは、PC で扱う情報とスマートフォンが扱う情報に差異があるからである。このようにネットワークを分離する場合、PC 等が接続されているネットワークのセキュリティレベルが、スマートフォンを接続するネットワークよりも低い（たとえばより簡易な方法で接続できる無線 LAN 等）と、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、専用ネットワークを経由してのみ接続させる場合、接続を許可された端末を識別するために、対象端末の識別情報（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、ネットワークアクセス時の認証ログなど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の対策を考える必要がある。

無線 LAN

<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端末のステータスログ、または認証ログなど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できる仕組みがあるか。	□

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、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

No	提供形態による分類
4	スマートフォンメーカーが開発するもの
5	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
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に承認されていないもの

No	セキュリティの観点からの分類
7	アプリケーションで必要な範囲での権限を必要とするもの
8	アプリケーションで必要な範囲を越えた権限を要求するもの

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。

		1	2	3
提供形態	4	○	●	●
	5	○	●	●
	6	△	△	△

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）

上記表に関わらず 8 番に該当するアプリケーションは、少なくとも組織内での利用を制限すべきである。
加えて、アプリケーションによってはアプリケーションの利用許諾にデータの共有やアプリケーション開発者側での情報の二次利用などを明示していることがある。したがって、アプリケーションをインストールする際には、利用許諾に十分な注意を払う必要がある。

<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、何らかの対策を講じる必要がある。端末を組織から支給する場合には、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べきである。また個人端末の場合には、各個人に責任を持って対応させる必要がある。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。特に紛失時や盗難時などは可能な限り紛失端末を（リモートワイプ機能等を利用して）初期化するべきである。したがって、定期的なデータのバックアップ取得とともに、不測の事態が発生した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。（端末側にデータを残さない、またはクラウド利用を前提としている場合にはその限りではない）	□
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。特に個人端末の場合の対応に関しては十分な周知と対策の徹底が求められる。

〈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、確実性の高い手段が提供されている場合、その手段を採用することが望ましい。

※ 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無線 LAN 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、「2.3.4 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脆弱な状態になったりといった好ましくない事象が発生する。

一般に、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、不用意にリンクにあるアプリケーションの端末システムへのアクセスを許可してしまうと、意図せず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。特にソーシャル系と呼ばれるアプリケーションでは、電話帳やスケジュールの共有などが行われることもある。また、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、どのようなデータが、どこに、どのような形で保存されているのかを可能な限り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。この行為自体は違法ではない。

このような改造行為により、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、使い勝手の向上や、スマートフォン内での制限により不可能なことを実行できるようになるといったメリットを享受することができるようになる。

しかしながら、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。また、多くの場合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、システムが不安定になることや、悪意あるプログラムなどで汚染される確率が飛躍的に高まるというデメリットがある。既に、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、組織の責任問題にまで発展する可能性がある。

したがって、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だが、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、どうしても必要と言う状況でない限り、原則は禁止すべきである。

<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. サービス提供者側でのスマートフォン端末管理

4.1 スマートフォン端末管理の検討

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組織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にすべきである。

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、あらかじ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、組織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、組織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、スマートフォン専用の無線 LAN に接続させる
・無線 LAN 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 認証方式の検討

4.2.1 デバイス認証とユーザー認証

認証する対象には大きく分けてデバイスとユーザーがある。デバイスの認証はその機器を特定し認証するものであり、他の端末に移すことができない機器固有の情報を元に認証される場合が多い。一方、ユーザーの認証は操作しているユーザーを特定し認証するものであり、そのユーザーしか所有していない知識や物、生体情報などを元に行われる。
デバイス認証もユーザー認証も、主に組織内のネットワークまたはリソースへのアクセスを制御したい場合の識別方式として用いられる（例としては、社外から組織のゲートウェイに対して VPN による接続を行う際の認証、組織内の無線 AP から組織ネットワークにアクセスする際の認証、ファイルサーバなどにアクセスする際の認証、メールサービスにアクセスする際の認証などがある）。

なお、認証方式については、スマートフォンの利用にあたって新しい認証技術を必要とするわけではなく、スマートフォンの特徴（本文書 1.3 参照）を踏まえて、ユーザーの利便性および必要なセキュリティを考慮して、従来利用されてきた認証方式をうまく組み合わせていくことが望ましい。単一の認証方式のみを採用する場合、その認証情報が何らかの要因で意図しない第三者へ流出してしまった場合、組織内ネットワークへのなりすましによる不正アクセスなどのリスクが発生する。そのためアクセスするリソースの機密性に応じて、複数の認証方式を組み合わせる多要素認証を採用することも有効である。携帯性の高いスマートフォンの特性を考慮すると、ユーザー認証に加えてデバイス認証を組み合わせる形での認証強化は有効と考えられる。

4.2.2 デバイス認証の種類と特徴

デバイス認証を利用する目的としては、組織で利用を認められた端末であるかどうかを、組織ネットワークやリソースにアクセスする際に識別することである。
デバイス認証において、一般的に利用される方式には大きく以下のものがある。

・端末の固有識別情報

OS やデバイスが保持する固有の ID や MAC アドレスを利用することが考えられるが、組織で利用する認証システムにおいて、その ID を利用できるかをあらかじめ確認しておく必要がある。また、特に MAC アドレスなどについては、詐称が容易にできることから機密性の高い情報にアクセスする際に利用する場合には、単独での利用は望ましくない。

・電子証明書

クライアント証明書をエクスポートすることを禁止しておくことで、他のデバイスでの再利用などを防ぐことも可能であり、デバイス認証としては最も安全な方式であると考えられる。ただし、認証局の管理や電子証明書の発行、更新、廃棄などの運用について十分考慮しておく必要がある。

4.2.3 ユーザー認証の種類と特徴

ユーザー認証を利用する目的としては、組織で利用を認められたユーザーであるかどうかを、組織ネットワークやリソースにアクセスする際に識別することである。
ユーザー認証において、一般的に利用される方式には大きく以下のものがある。

・本人のみが知りえる知識

ユーザー本人のみが知りえる知識情報を認証要素として利用する方式である。一般的に良く利用されているものには以下のものがある。

- 固定 ID・パスワード（あらかじめ設定した固定文字列）
- マトリクス（あらかじめ設定したマトリクス表のパターンを都度生成し、ワンタイムパスワードを提供）

一般的に用いられている方式は固定 ID・パスワードを用いた方式である。一般的で利便性が高く広く普及しているが、フィッシングやのぞき見などに弱く、情報が流出したことにも気づきにくい。同じ ID とパスワードを使い回している場合にはさらに脅威が増大する可能性が高い。

・本人の所有物

ユーザー本人のみが保持しているものを認証要素として利用する方式である。一般的に良く利用されているものには以下のものがある。

- セキュリティトークン（定期的に変化するパスワードを生成するワンタイムパスワード）
- 生体認証

本人の所有物を利用した認証を行う場合には、多くの場合、二要素認証による認証強化を目的とすることが多いと考えられる。その観点から、スマートフォンの紛失時などのリスク・スマートフォンの携帯性の高さを考慮すると、スマートフォンにインストールするタイプのセキュリティトークンの利用には十分な考慮が必要と思われる。また、ハードウェア型セキュリティトークンの場合でも紛失時の対策なども考慮が必要であろう。
また、生体認証の利用にあたっては、生体情報（指紋、顔など）を読み取るデバイス（またはアプリケーション）が端末側で実装されている必要があるため、あらかじめ端末仕様を確認する必要がある。

ネットワーク無線 LAN

4.3 スマートフォンの運用設計

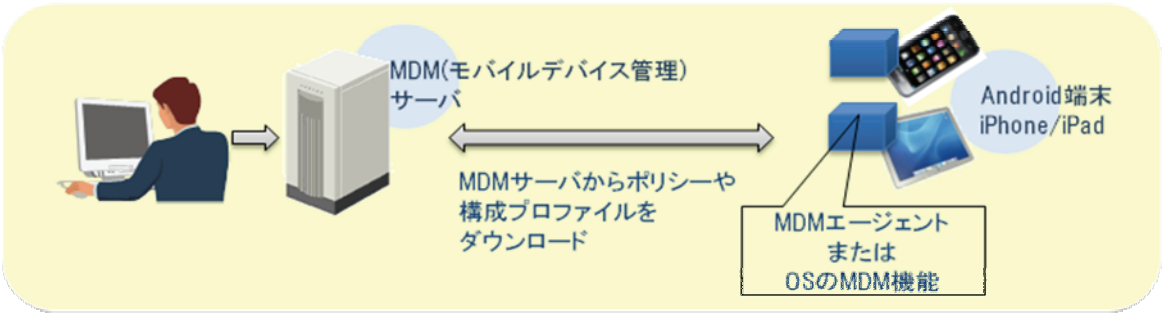
耐用年数の終了やベンダサポート終了、経年劣化、故障等によりスマートフォンを廃棄する場合、スマートフォン内に蓄積されたデータが残留している可能性がある。廃棄手段によっては、データが残留したまま再利用される恐れがある。したがって、スマートフォンの廃棄時には利用者のデータが残留しないよう注意する必要がある。

現時点では、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。記憶媒体に書き換え可能回数の上限が存在するため、制御ドライバ（プログラムのこともあればICチップ内での実装のこともある）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。

4.4 ツール選定

MDM (Mobile Device Management: 端末管理) とは

管理用アプライアンスを設置、または PC に MDM サーバアプリケーションをインストールし、端末のリモートロック，リモートワイプ，パスワードポリシーの強制，機能利用の禁止や制限，端末内の情報取得などを行う。端末側の OS の機能のみ活用するタイプと端末にエージェントアプリケーションをインストールするタイプがあり、後者に多機能な商用製品が多い。また、製品によってはアプリケーションの配信機能を持っているものもある。



＜ MDM ツール＞

4.4.1 端末管理ツール要件洗出し

MDM ツールで一般的に実現できる機能を以下に示す(※)。

※ 2012 年 3 月現在で代表的な機能全てをカバーしている製品は少なく、実現方式もメーカー各社により一長一短がある。

＜MDM 機能＞

分類	機能	備考	必須
端末情報管理	利用者情報	LDAP, Active Directory 連携はオプション	○
	端末種別情報	機種, OS, キャリアなど	○
	インストールアプリケーション情報	インストール済みアプリケーションの一覧表示	○
	位置情報の取得、マップ表示	マップ上の位置は GPS 情報の誤差以内の制度で表示できることが望ましい。	
	大規模構成対応・絞込み表示	大規模構成での端末一覧表示可能なこと。組織ツリー構成に合わせた表示、ポリシー別検索絞込み表示ができると良い。	
紛失・盗難・情報漏洩・対策	リモートロック	端末側で通信が遮断されている場合はロックできない。	○
	リモートワイプ	端末側で通信が遮断されている場合はワイプできない。遮断前にタイマー設定でエージェントにより自律ワイプできるのか、通信再開時にワイプされるか、など製品の仕様を確認すること。	○
	ロック解除認証の強制	パターン, PIN, パスワードによるロック解除認証を強制する。	○
	パスワードポリシーの設定	オプション。パスワードの複雑性など、より強固な認証を強制する。	
	カメラや SD カードの利用制限	端末により制限できる機種とそうでない機種があるので、あらかじめ確認する。	
不正利用対策	無線 LAN や VPN の遠隔設定	デバイス認証や VPN クライアントなど各種証明書の端末配布とインストールはオプション	
	アプリケーションの起動制限	ブラックリスト、ホワイトリスト両方でアプリケーションを指定できるのが望ましい。起動プロセスを強制終了させる場合はメモリリーク、ゾンビプロセスが生成されないことをメーカーに確認する。警告表示だけでも抑止効果がある。	
	アプリケーションの配信	ネットワーク構成、配信経路、APNS や C2DM によるプッシュメッセージを利用するか、をあらかじめ確認しておく。	
	App Store や Android マーケットの利用制限	インストール済みアプリケーションの脆弱性対策アップグレードができなくなるケースも考慮し、実施する。	
	Jailbreak の制限	iOS の Jailbreak、Android 端末の root 化を実行させない。新しい実行手法全てを網羅できなくても、ツールが公開されている代表的な手法は防止できるのが望ましい。	

初期導入にあたっては端末情報管理、紛失・盗難対策を必須機能項目とする(表中〇項目)。これらの機能は現存する MDM ツールほぼ全てで実現できていると判断してよいが、端末が通信できない環境で発生する制約(リモートワイプできないなど)については必ずメーカーに確認しておく。それ以外の項目については、組織のセキュリティポリシーもしくは端末の利用目的に従い機能が実現できているかツールの仕様を確認する。

業務システム向け端末の場合、端末機種を絞り込み、MDM ツールを使った事前検証テストを実施することが望ましい。BYOD への対応では、対応端末は実質不特定多数となるため、必須項目だけでも幅広い端末で動作確認できている MDM ツールを選定する。

4.4.2 ツール選定

前節の MDM 機能、運用環境、管理目的を考慮し、クラウド(SaaS) 型とオンプレミス型(※)から、用途に応じてツールを選定する。選定条件を表に示す。

※ 組織のイントラネットワーク内に構築するタイプ

＜提供形態＞

提供形態	特徴	用途/備考
クラウド(SaaS)型	・短期間でサービス開始可能 ・MDM 管理サーバなど新たな設備投資が不要 ・運用コストが月額費用のみ ・運用代行サービスなども利用可能 ・不要になったら、解約可能	グループウェア、メール、簡易業務など目的の端末管理に適している。
オンプレミス型	・組織イントラネットワーク内部に MDM システムを構築するため、柔軟な運用が可能 ・ID 管理システム(既存 Active Directory や LDAP)や業務システムとの連携が容易 ・端末や利用者に関する機微情報を自組織内で管理できる	既存業務システム、ID 管理システムと連携し、組織固有の業務に端末を利用するケースでの端末管理に適している。

クラウド(SaaS)型では、組織の業務システムが全てクラウド上で動作しているケースも含め、グループウェア、メールなど組織内のコミュニケーションを主体とした利用目的の端末管理に向いている。その反面、組織内の業務システムや複雑な ID 管理システムと連携させるには、MDM ツールと組織内業務システム間の安全な通信環境および連携インターフェースの整備が必須となる。現状のクラウド型 MDM ツールで組織内の重要な業務システムと連携させるにはセキュリティ上のリスクがあり、その場合はオンプレミス型のツールを用いる。

また、端末の使用目的に応じて両者を使い分ける、あるいは組み合わせる導入も今後予想される。

4.5 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(HTTPProxy 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。	□

4.5.1 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。	□

4.5.2 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。したがって、常に最新のバージョンアップやパッチ適用を行う必要がある。この点から、OS の更新が終了したスマートフォンは、その耐用年数に満たない場合でも速やかに交換することが望ましい。近年では、スマートフォンの OS やアプリケーションの更新には PC が不要になりつつある。しかし、バージョンアップに PC が必要でありながら、PC を持っていないという状況があるならば、そのユーザーには個人端末の使用を許可しないことが望ましい。

なお、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、組織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事に留意すべきである。

メーカーによっては、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、利用を許可すべきではない。
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と言わざるを得ない。そのため情報収集を欠かさない努力が必要になる。
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通常、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べきである。

※OSの更新にPCが必要な場合、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。	□

4.5.3 サーバにおける対策

管理者は、組織内の情報システム（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べきである。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組織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
（例）外部からの通信は、VPNを利用する

4.5.4 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組織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べきである。接続を許可する場合、接続設定を組織内の掲示版等、誰にでも閲覧できるような場所には公開すべきでない。

以下に、スマートフォン端末を組織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		組織内ネットワーク無線 AP に接続		組織内無線 AP 無線 LAN に非接続
		既存LANに接続	専用LANに接続	
ネットワーク帯域優先制御		困難	無線APで可	不可
アイソレーション		不可	可	不可
組織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

4.5.5 無線 LAN の検討

スマートフォンは、一般に「無線電話回線（携帯回線）」を用いたネットワーク接続、および「無線 LAN」を用いたネットワーク接続を行えるようになっている。
したがって、規定などによって組織内で無線 LAN の利用が禁止されている場合には、規程との整合性も含め、どのような形態でネットワーク接続を行えるようにするかを十分に検討する必要がある。スマートフォンによっては、アプリケーションのダウンロード等で、「無線 LAN」を用いることを強要するものがあるので十分な注意が必要となる。また、スマートフォンの利用者が多い場合、近隣の携帯回線の基地局数やキャパシティによっては、スマートフォンが全く利用できず、電話としても動作しなくなる（基地局が飽和する）可能性もある。この場合、スマートフォン利用者だけで無く非利用者に対しても影響を与えるので、十分な注意が必要である。以上より、スマートフォンの利用を許容する場合には、通常「無線 LAN」を用いたネットワークを準備することになると考えられる。

無線 LAN を用いたネットワーク提供を行う場合、無線 LAN ネットワークへの接続方法や利用方法などを十分に検討すべきである。以下に無線 LAN に関する検討項目を記載する。

No	対策	チェック
1	通信保護には、十分強度のある暗号方式を採用しているか。 ※2012 年 12 月現在、特に必要がない限り WPA2 を利用するべきである。	□
2	無線ネットワークのネットワーク ID(SSID)は可能な限り隠蔽しているか。	□
3	無線 LAN に接続されている各端末間の直接通信を禁止しているか。	□
4	無線 LAN に接続する端末は認証されているか。 ※認証方式には、MAC アドレス認証や 802.1x 認証などがある	□
5	無線ネットワークは、組織内 LAN と切り離されているか。 ※無線ネットワークと組織内 LAN の接続には、ファイアウォールなどを用いた通信制限をかける。 ※無線ネットワークと組織内 LAN の接続に、VPN を利用するなど。 ※無線ネットワークとインターネットの間にはファイアウォールなどを用いた通信制限をかける。	□
6	無線ネットワークから組織内あるいはインターネットへの接続点に、IPS などを用いた通信内容分析を行い、異常通信を遮断できる装置を導入する。	□
7	スマートフォンを用いた社外からの組織内リソースへのアクセスに関して、その手法を十分に検討する。 ※VPN によるアクセス、SSL を用いた Web 経由でのアクセスなどの手法を検討し、必要な対策を講じる。	□

4.6 ネットワークの運用設計

4.6.1 スマートフォン導入後のネットワーク運用

スマートフォンは、ネットワーク運用を検討する上では特殊なデバイスではない。通常のノート PC を無線 LAN に接続することとの差はほとんど無いといえる。しかし、スマートフォンの特性を考慮すると、運用上強化すべき点が幾つかある。以下にその「強化すべき点」を挙げる。

まず、スマートフォンは PC と異なり「接続」と「切断」が非常に多い。これは、PC が机の上に置き去りにされやすいのに対し、スマートフォンは離席時でも身につけていることが多いからである。従って、人間の移動に合わせ、無線 LAN 間を渡り歩くような接続形態になりやすい。また、無線 LAN が届かなくなった時に通信事業者回線に切り替わるなどの機能を持っている。これは、利便性を考慮すると非常に便利であることは確かだが、業務利用上はリスク要因となりうる。このリスクを回避するためには、業務上必要十分な範囲を無線 LAN によってカバーする必要がある。このような対応を行うことで、通信状態を十分に管理できるようになり、情報漏洩を起こしにくくすることが可能となる。例えば、組織内 LAN に対する通信事業者回

線からの直接の接続を制限し、組織内無線 LAN の接続が切れた場合に通信中のデータの再送を行わせないような運用にするなどがある。

次に、スマートフォンは PC と比較して現時点では十分に安全とは言えないという状況がある。これは、ウイルス対策や異常通信対策が十分でないことによるものである。このような状況に対応するために、組織内 LAN 側のネットワークで許可されていない端末が接続できないような対策（MAC アドレスを用いるなどの何らかの端末認証など）を行う事が望ましい。また、組織内 LAN から外部への通信に関しても十分な監視を行い、もしウイルスに感染したとしても外部に情報を漏洩させないような対策を講じることが望ましい。

このような対策は、スマートフォンが接続されるかどうかに関わらず施されるべきであるが、この種の基本的な対策を十分にかつ確実に行うことによって、スマートフォンが接続されても安全性が損なわれないようにネットワークを運用することが可能となる。

以下に、スマートフォンが接続されたネットワークの運用に関して注意すべき点を挙げる。

No	対策	チェック
1	スマートフォンが使用される可能性のあるエリアには、スマートフォンを接続するためのネットワークを準備する	□
2	定期的に「未管理の」無線 LAN 基地局が設置されていないことを確認する	□
3	スマートフォンが利用する可能性のあるサービスを、他のサービスから隔離する	□
4	スマートフォンが利用するサービスは、外部から利用できないように保護する	□
5	認証されていないスマートフォンが接続できないようにネットワークを管理する	□
6	スマートフォンが接続されるネットワークに関しては、特にその通信先を確認し、異常な通信が無いことを確認する	□
7	定期的にスマートフォンの OS の更新を実施させる	□
8	Jailbreak/Root 化された端末を接続させないよう、利用者を教育する	□

4.6.2 マルウェア感染

マルウェア感染等の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、組織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ことも考慮すべきである。

※ 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。（通信事業者回線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。	□

4.6.3 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。通信事業者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ならば、それを利用する。

個人端末の業務利用を許可をする場合、インシデント発生時にワイプする許可を得るなど、紛失、盗難時の対応を事前に協議し、所有者に承認させることが望ましい。

・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。	□

4.6.4 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事が望ましい。これは、システムの閲覧性、操作性の改善に非常に有効である。また、スマートフォン端末から利用させる Web システムは、端末に転送するデータを十分に区分し、不要なダウンロードを制限するべきである。

※ 「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」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。 ・閲覧性、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(アプリケーション)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ー
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
- 不正プログラムを検出できること
- 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 などによる仮想専用線（VPN）機能を有していること
- 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	D
音声通話	通話（履歴）, Skype, SIP Client, Viber		○		○	
リアルタイムメッセージ交換 TV 会議	インスタントメッセンジャー		○		○	
	Skype, WebEx, Facetime				○	
非リアルタイムメッセージ交換	SMTP		○	○		
	IMAP		○	○		
	Web メール(組織内サーバ)			○		
	Web メール(SP サーバ)				○	
	Exchange		○	○		
	SMS		○			
グループウェア	スケジュール 掲示板 ワークフロー 各種 D/B 組織内 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) サイボウズ Google Apps Lotus iNotes		○	○	
		オフラインが利用できるもの Exchange (EAS) Lotus Notes Traveler	○	○	○	
		端末個別	○			
ドキュメント作成	MS-Office、 GoogleApps、カメラ		○	○	○	
閲覧	Offce View、PDF View、iBook、 Kindle、Acrobat Reader		○	○	○	
ファイル共有	Evernote、Dropbox、SugarSync、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ー等、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

以下に、その他スマートフォンを業務利用する際に考慮すべきセキュリティの課題を記載する。情報システム管理者は、以下の点においても十分に検討を行うべきである。

- 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、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発生することも考慮する。可能であれば、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、使用アプリケーションによっては、ローカルに保存し、メールで社外に送信可能となる。したがって、必要に応じて利用禁止とすることも考慮する必要がある。
- （有料、無料を問わず）公衆無線LANサービスを利用する場合、他者が共用APに接続していることを考慮しなければならない。業務アプリケーションが入った端末を利用する際には、通信の暗号化（IPsecやSSL）などを利用して安全性を確保する。
- 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。
- スマートフォンは、社外での利用も十分に考慮する必要がある。特に電車等におけるショルダーハック等、攻撃の危険性とその対策を検討するべきである。覗き見防止のために、視野角をコントロールするフィルタなどの対策を推奨する。

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利用に関する相談を受けた場合、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。

スマートフォンのセキュリティインシデントのほとんどは、マルウェアをインストールすることで発生する。またスマートフォンにおけるマルウェアの大きな特徴として、従来のPC環境におけるマルウェアのようにOSの脆弱性を利用して不正を行うタイプのものよりも、ユーザーが正当なアプリケーションと誤認してもしくは適切な権限管理を行わず、アプリケーションに不要な権限をあたえてしまうタイプのものが多いということがある。例えばアプリケーションが電話帳などの情報へのアクセスを要求しユーザーにそれを許可させ、それらの情報を正当に取得してサーバなどに送信するといった、単純なマルウェアによる被害が多数報告されている。

したがって、こういったマルウェアによる被害は、スマートフォンのシステムの脆弱性を塞いでいっても、軽減されるとは限らない。

BYODなどでアプリケーションの利用制限を実施しにくい環境も考えられるが、それぞれの利用者がマルウェアをインストールしないようにすることが、重要である。

それぞれの利用者が、自身で「動作にあたり不自然な権限を要求するアプリケーションはインストールしない」ということが可能であれば、それが対策となる。しかし一般的には、そのような対応が困難であると考えられる。このような場合は、例えば組織で利用するアプリケーションを制限する、検証が済んだアプリケーションしか利用しない、など、マルウェアをインストールしにくい何らかの行動ルールが必要になるだろう。

また、アプリケーションの権限は、アプリケーションの更新時に不要な権限が追加される場合がある点にも注意が必要となる。上記アプリケーションのインストールに関する行動ルールを設けた場合でも、検証済みのアプリケーションについて更新状況を確認し、利用権限について把握しておく等、継続的にアプリケーション管理を実施する必要があるだろう。

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。

No	対策	チェック
1	利用者がマルウェアをインストールしない行動ルールを提示しているか。	□

- 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配布サイトを周知する。
- アプリケーションをインストール/更新する際の注意事項(許諾メッセージ・アクセスできる情報の許可)を確認する。

6. サポート

6.1 情報の提供

6.1.1 スマートフォン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を必須事項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 化された端末等、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常に最新の 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その端末の使用を禁止する。

・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の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は、導入台数(利用者数)にあわせてヘルプデスクを設置し、あらかじ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べく努力すべきである。このような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。

FAQ には以下のような内容が含まれているべきである。

・組織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

・アプリケーションに関するホワイトリスト、ブラックリスト、新規アプリケーションの利用可否についての問い合わせ

・組織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

※ 組織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

※ 組織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。	□

6.3 キッティング

スマートフォンを組織内システムで利用する場合、組織内ネットワークに接続する端末を事前に特定・管理するとともに、組織で定めたセキュリティポリシーと導入ポリシーに従った端末設定（プロファイル）を適用するべきである。
スマートフォンを利用するにあたっては、iOS 端末であれば Apple ID、Andorid 端末であれば Google アカウントなど、スマートフォンに応じた ID を利用者自身が取得する必要がある。一般に、スマートフォンのキッティングは利用者個人による設定を前提とした設計となっているが、組織として利用者に応じたプロファイルの適用を徹底していくには、設定手順書などをあらかじめ策定をして、利用者に周知する必要がある。しかしながら、導入台数が多くなる場合、手順書をベースとした利用者ごとの設定ではプロファイルの徹底を図ることは限界がある。
スマートフォンを組織から支給する場合には、端末導入時にキッティングサービスを利用することが可能な場合もあるが、利用者の私物の端末を利用することを認める場合には、MDM ツールを利用することなども検討する必要がある。MDM ツールでは OTA（Over The Air）を利用したプロファイルの配信を行うことにより、利用者によるセルフプロビジョニングを容易に行うことが可能となるとともに、プロファイルの強制を行うことも可能となる。
ただし、初期導入時のスマートフォンには無線 LA ネットワーク無線 LAN 設定が行われていないため、OTA により無線 LA ネットワーク無線 LAN 設定を含めたプロファイルを配信する場合には、**通信事業者回線**対応のスマートフォンを採用する必要があることに留意が必要である。

<スマートフォンキッティング時の考慮点>

No	対策	チェック
1	スマートフォンのキッティングの方法を決定しているか？ ・ 利用者による手順書による設定 ・ キッティングサービスの利用 ・ MDM によるセルフプロビジョニングの適用	□

あとがき

気がつけば、2011 年 4 月にβ版をリリースして一息ついたと思っていたら、瞬く間に丸 2 年も経ってしまいました。この 2 年間でスマートフォンを取り巻く環境は大きく変わってきています。各企業におけるスマートフォンの利用目的が明確になってきたことやセキュリティ対策が充実してきたことを裏付けるように、スマートフォン導入例は確実に増えています。当時、日本企業は意識しないだろうと思っていた BYOD はもはや当たり前に検討されるような風潮になりました。一方、残念ながらやはりマルウェアを含むアプリケーションは激増していますし、とうとう不正アプリケーション開発者が逮捕された、などということもありました。ある程度予測していたとはいえ、この激しい変化には驚くばかりです。

2012 年 4 月に正式版リリースに向けてこのワーキンググループを再スタートし始めた当初は、β版の章立てから大きく変えて、スマートフォン導入部門の担当者の立場を想定して企業の情報インフラ全体をも視野に入れたガイドラインにしたいと検討しはじめました。ところが次から次へと検討材料が追加されていき、ワーキンググループは破綻状態（というか私自身がボトルネック）なってしまいました。そのことで悩んでいた時期もありましたが、ワーキンググループのメンバーからは様々な助けがあり、やっとのことで今回のリリースに漕ぎ着けることができました。そして、この正式版が我々が思い描いた、導入部門担当者に向けたガイドラインになったかどうかは、読者の皆様の判断にお任せしたいと思います。
β版は、「とにかく早くリリースする」が世の役に立つと信じて出したわけですが、ある種のエクスキューズ的なところがあったのは否めません。ですから正式版の活動をはじめた当初は、β版は考えられる限り思いつくままにセキュリティ課題を連ねただけというイメージがあり、それを払拭しようとしてちょっと力んでいたかもしれません。それが、メンバーみんなの支えによってβ版の建てつけに戻しブラッシュアップするという方針に切り替え、徐々に正式版の完成が近づくにつれてあることに気づかされることになりました。「2 年の大きな変化」があったにもかかわらずガイドラインの内容としてはほぼ想定内だったのだなと。

正式版をつくる作業の過程で、情報インフラは大事だと再認識したのも大きな成果です。ワーキンググループメンバーはスマートフォンをきっかけに社内ネットワークはどうあるべきか検討したわけですが、スマートフォンに限らず新しいデバイスを社内システムに導入する際には常に重要となるテーマであります。
ただこれまでになくスマートフォンの登場がセンセーショナルだっただけで、IT インフラに携わる者はそれを肝に銘ずるべきなのだなと思います。現在では様々なスマートフォンのセキュリティに関するガイドラインがありますが、この正式版を他と区別するなら、「スマートフォンを使うには」ではなく、「スマートフォンを使うなら」という視点で書いたと云う点となるでしょう。

最後になりましたが、この正式版ガイドライン作成に携わって頂いたワーキンググループメンバーや正式版の核となったβ版作成に携わって頂いたワーキンググループメンバー、ならびに JNSA 事務局の皆様のご協力に深く感謝いたします。

加藤　智巳

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

＜正式版作成WG＞

ワーキンググループリーダー

加藤 智巳	株式会社ラック

ワーキンググループメンバー

最終執筆者

手塚 信之	SCSK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
栃沢 直樹	トレンドマイクロ株式会社
大竹 章裕	株式会社ネットマークス
小早川 知昭	ソニー株式会社
板倉 博和	株式会社日立ソリューションズ
許 先明	株式会社ラック
吉田 裕美	株式会社ラック

メンバー

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
小林 博之	クオリティソフト株式会社
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
小林 裕士	一般社団法人 JPCERTコーディネーションセンター
石田 淳一	独立行政法人情報処理推進機構
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
相原 弘明	株式会社ネットマークス
中谷 忍	株式会社日立システムズ
猪股 健一	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
岩井 弘志	マカフィー株式会社
新山 剛司	マカフィー株式会社
大野 祐一	株式会社ラック
西本 逸郎	株式会社ラック
山城 重成	株式会社ラック

（会社名 五十音順）

＜β版作成 WG＞

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）