参考資料１－２

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

～その特性を活かしたワークスタイル変革のために～

【β版】

２０１１年8月３１日

日本スマートフォンセキュリティフォーラム（JSSEC）
利用部会　ガイドラインワーキンググループ

文書管理番号 JSSEC-R-GL20110831-1

■制作■

利用部会ガイドラインワーキンググループタスクフォース

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）
	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）

■監修■

丸山 満彦 （デロイト トーマツ リスクサービス株式会社）

■発行■

日本スマートフォンセキュリティフォーラム（JSSEC）

利用部会 部会長 郷間 佳市郎（株式会社日立情報システムズ）

文書管理番号 JSSEC-R-GL20110831-1

目 次

1. はじめに

1.1. 本ガイドライン利用にあたって

スマートフォンとは、従来の携帯電話の機能に加え、高度な情報処理機能が備わった携帯デバイスです。音声通話はもちろんデータ通信、無線 LAN（以下 Wi-Fi）などの通信機能が充実し、コミュニケーション機能に優れています。また、スマートフォンとほぼ同等の機能を持ち、画面サイズの大きいタブレットと呼ばれる携帯デバイスもあります。

本ガイドラインでは、「スマートフォン」と「タブレット」を包含する言葉として「スマートフォン」を用います。

なお、本ガイドラインは 2011 年 8 月 31 日現在のβ版であり、記載された内容は今後変更の可能性があります。

1.2. 本ガイドラインの目的

現在、IT を積極的に利活用したワークスタイル変革を推進している企業が増えています。その鍵となる重要な IT デバイスとして、スマートフォンが注目を集めています。

組織としての取組みが進んでいない企業でも、個人のスマートフォンをビジネスシーンで利用している場面も散見されます。

しかしながら、スマートフォンは技術的な側面では発展段階であり、導入企業サイドにおいても情報が不足している中、本格的な業務利用においては解決しなければならない課題が多く存在するのも事実です。

本ガイドラインは、今後の日本の労働生産性の向上や事業継続性の確保、およびワークスタイル変革を実現していく中で必須になるであろうスマートフォンについて、その利用シーンという観点から企業や組織が考慮しなければならない主にセキュリティ上の脅威と対策を明確化し、安心・安全にスマートフォンを業務で利活用するための環境整備に貢献することを目的としています。

1.3. 本ガイドラインが対象とする読者

本ガイドラインは、主に以下の読者を対象としています。

(1) 企業や組織においてスマートフォンを導入する責任者・企画担当者
(2) 企業や組織においてスマートフォンを導入する際にセキュリティポリシーを策定する責任者・担当者
(3) 企業や組織においてワークスタイル変革を推進する責任者・企画担当者

1.4. 本ガイドラインが対象とする範囲

本ガイドラインが対象とする範囲は、スマートフォンの所有形態と、利用目的という観点を切り口として定めています。

法人所有の業務利用に限定せず、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）や、法人所有のスマートフォンの業務利用と個人的な利用の兼用に関しても、組織として考慮すべきポイントであるものとして対象範囲としています。

なお情報セキュリティにおいて、データの重要度による分類は一般的になりつつありますが、本ガイドラインでは利用シーンを想定しやすいように、スマートフォンの特性をもとに脅威の分析をしています。

表 1　本ガイドラインの対象範囲

利用目的 / 所有形態	業務利用のみ	業務利用と個人利用の兼用	個人利用のみ
法人所有	○	○	対象外
個人所有	対象外	○（BYOD）	対象外

※「対象外」は、本ガイドラインでは言及していない範囲です。

1.5. 本ガイドラインの構成

本ガイドライン前半の 2 章～4 章では、スマートフォンの特徴を理解して頂くため、利活用の効果や知っておくべきしくみと特性を記載しました。

後半の 5 章と 6 章は、スマートフォンのセキュリティを、「利用シーン」と「デバイスのライフサイクル」という側面で、管理者が認識しておくべき脅威と対策について説明します。

各章の「脅威と対策」は、スマートフォンと PC との違いに焦点を当てながら、多角的な可能性を考慮し、発生頻度とは関係なく網羅的に記載しています。従って、全てに対応しなければいけないということではなく、それら脅威を認識した上で、実際のスマートフォンの利用目的に照らし合わせ、必要なセキュリティを選択するための参考としてください。また、本表は基本的に、法人資産時と個人資産時、共通項として掲載していますが、「BYOD」と記載している行は、個人資産を活用する際に特有の内容です。

2. スマートフォンの利活用によるメリット

本章では、スマートフォンの利活用によるメリットを説明します。

スマートフォンは、他のデバイスと比較して、携帯性に優れている、常に電源が ON になっている、常時ネットワークに接続されているなど、コミュニケーションツールとして優れた特徴があります。また、利用者の嗜好に応じてアプリケーションを追加することで機能面での拡張性が高く、パーソナライズが容易です。

2.1. 導入のねらいと理由

スマートフォンを使った、外出先での Web サイトの閲覧やメール、スケジュールの利用頻度が高くなっています。これまでも、それらの利用シーンはネットワーク接続されたノート PC でも可能でした。しかし、その利便性とスピードを考えた際、スマートフォンは圧倒的な効果を生みます。

従って、スマートフォンを「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」などのワークスタイル変革、更には、「事業継続性の確保」、「顧客満足の向上」など、様々な目的で利用しようとする組織が増えてきました。

2.2. 活用例と効果

代表的なワークスタイル変革の事例を以下に挙げます。

◆コミュニケーションの活性化と業務効率化

外出時などの移動時間や待ち時間などに、簡単にメール対応できれば、よりタイムリーなコミュニケーションを実現できるだけでなく、隙間時間を利用した大きな業務効率向上が望めます。その結果、事務所に戻った後の電子メール処理時間を、大幅に削減することが可能になるでしょう。仮に 1 人あたり 1 日に 1 時間の削減ができた場合、月では約 20 時間（20 営業日と仮定）の削減につながります。従業員が 500 人と仮定すると、月あたり 1 万時間（1,250 営業日）分の業務効率化、コスト削減効果が見込めることになります。

◆意思決定の迅速化

出張や外出などが多い多忙な役職者は、組織の重要な意思決定や日々の様々な判断業務を抱えています。スマートフォン活用による、通話やメールでの重要事項の確認はもちろんですが、手続きとして必要な稟議決裁を行うために「いつでもどこでも」、安全に社内ネットワークへ接続して決裁できれば、組織としての意思決定を迅速化すると同時に、役職者の拘束時間を減らし柔軟に対応できるという効果も得られます。

◆ペーパレスによるコスト削減と業務効率化

コスト削減と業務効率化を目的としたペーパレス化も進んでいます。

例えば通常の組織では、マニュアルやカタログなどを紙で印刷することが定常化していますが、その改訂頻度によっては、組織に大きな業務増加やコスト負担を強いています。さらに配布時も、マニュアルなどを持ち歩く負担や、必要に迫られた際に短時間で該当文書を探す手間もあります。このような課題は、紙を電子化し、閲覧・検索媒体としてスマートフォン、主にタブレットを活用することで、大幅に改善されます。

◆外出時の移動効率化

外出時の利便性向上としては、地図および位置情報の利用も効果的です。事前に行き先を調べて印刷する必要がなくなります。

2.3. スマートフォンを取り巻く動向

スマートフォンは、以下のような社会のニーズに応えるツールとして注目されています。

◆災害時の対応や在宅勤務への活用

現在、組織においては、災害時の事業継続性の確保、電力消費削減等の社会的責任の遂行、在宅勤務などの目的を実現しようという動きがあります。ワークスタイルを変革し従業員のワークライフバランスを改善していくためのツールとして、スマートフォンが期待されています。

◆クラウドサービスとの親和性

クラウドサービスは、組織の IT 関連の遊休資産を削減し、IT 資産をオフバランス化することにより経営の効率化を実現すると共に、「いつでもどこからでも」、必要な IT 資産を活用できる環境を提供します。それを最大限に活用するデバイスとして、クラウドと組み合わせたスマートフォンの利用が進んでいます。

◆個人所有のスマートフォン活用

スマートフォン自体の所有形態についても、従来とは違う動きが顕著になりました。法人資産以外のスマートフォン、すなわち個人のスマートフォンに対しても、業務での利用を許可する組織が現れてきました（BYOD）。これには、経費節減や効率化、緊急対応、2 台持ちに対する負担軽減など様々な背景が考えられますが、今後、新たに注目される動きと言えます。

現在、組織を取り巻く環境は、グローバル化、知的社会の進展と共に非常に競争の激しい、変化に富んだ不確実性の高いものとなっています。スマートフォンの活用によって、個人のビジネススタイルが柔軟になり、良いアイデアが生まれ、信頼や人間関係が深まり、個人の能力も高まることで、組織としての競争力や生産性も向上することが期待できます。

このような効果をワークスタイル変革に繋げてみましょう。

「さぁ、スマートフォンしましょう！」

3. スマートフォンのしくみと概要

本章では、スマートフォンのしくみと概要について解説します。

3.1. デバイスの特徴と OS の種類

スマートフォンは、従来の携帯電話や PC と比べてハードウェア面で違いがあります。携帯電話と比べると、液晶が大画面で、ソフトウェアキーボードが主体となっているという特徴を持ち、また、PC に比べると、薄型軽量であるという特徴を持っています。

スマートフォンの機種や、OS の種類も様々であり、利用者がその目的によって最適なものを選択する必要があります。

以下は、日本の市場で提供されているスマートフォンの主な OS の種類一覧と、デバイスを含めた特徴です。

表 2　OS と特徴

OS の種類	OS 提供元	特徴
iOS(iPhone/iPad)	Apple Inc.	OS、デバイス、アプリケーションマーケット全て垂直統合型で展開。iPhone/iPad 上でのみ稼動し、最新バージョンの適用が容易。
Android	Google	OS、デバイス、アプリケーションマーケット全て水平分業型で展開。デバイスの選択肢が豊富。オープンソースの OS であり、基本的には、各デバイスメーカーが独自に開発したデバイスにカスタマイズして搭載。OS バージョンが同一でも機種依存がある。
BlackBerry OS	Research In Motion（以下 RIM）	OS、デバイス、アプリケーションマーケットを、基本的には垂直統合型で展開。高次のセキュリティ機能を BES/BIS サーバで提供。現在は BlackBerry 上でのみ稼動。主要機種に QWERTY キーを搭載。
Windows Phone 7	Microsoft（以下 MS）	OS、デバイスは水平分業型で展開。デバイスの選択可。既存 Microsoft 資産と連携できる設計。METRO UI と Exchange 等による管理機能搭載。

3.2. アプリケーションとその入手形態

従来の携帯電話と違い、スマートフォンでは電話をかける場合も、ひとつのアプリケーションとして起動する必要があります。その意味では、電話、メール、スケジュールなどスマートフォンで利用する機能は、全てアプリケーションであると考えられます。

アプリケーションには、デバイスの出荷時に予め提供されているものと、利用者がマーケットからダウンロードして利用するものがあります。

マーケットは、各 OS 提供元、または通信事業者やデバイスメーカーなどが提供しています。マーケットからダウンロードする場合、マーケットによっては審査されていないケースがあるため、悪意のあるアプリケーションによって重要なデータが漏洩する危険性があります。そのためダウンロード時には、マーケットやアプリケーションの信頼性を確認するなど、注意が必要です。(5.9 節「アプリケーションを利用する」を参照)

さらに、スマートフォンはネットワークに常時接続されていることから、マーケットにいつでもどこからでもアクセスすることが可能であり、PC などに比べ格段にアプリケーションの入手が容易であることを意識しておく必要があります。

なお、企業や団体などが独自に開発したアプリケーションを活用することもできますが、その際は、開発者が配布方法を決定できます。この場合、他者の著作権を侵害しないよう注意が必要です。

表 3　マーケットと特徴

提供元	マーケット	マーケットの特徴
iPhone/iPad	「App Store」	Apple 社が審査した他社のアプリケーションを登録。アプリケーションの配布や使用時には Apple 社と契約し、Apple 社が発行する証明書が必要。App Store から配布、課金。
Android	①Google 「Android マーケット」②各通信事業者等の運営するマーケット	① Google 社は審査せず、その活用は利用者裁量。 ② 通信事業者等が、それぞれの基準で登録。 配布・課金モデルあり。
BlackBerry	「App World 」	RIM 社が審査した他社のアプリケーションを登録。 App World から配布、課金。
Windows Phone	「Marketplace」	MS 社が審査した他社のアプリケーションを登録。 Marketplace から配布、課金。

3.3. 通信形態とネットワーク

スマートフォンは、音声通話とデータ通信（パケット通信）を利用できます。アクセスするネットワークとしては、携帯電話回線、Wi-Fi 等を利用することができます。それぞれ、帯域やカバーされているエリアに違いがあります。

なお、スマートフォンが持つ Wi-Fi ルータの機能を用い、携帯電話回線を通じてインターネットに接続することをテザリングと呼びます。テザリングは組織からインターネットへの出口＝アクセスポイントを増やすということになるため、利用には注意が必要です。

表 4　回線の種類と接続方法

ネットワーク	特徴	利用可能な接続先
携帯電話回線	・音声とデータ通信が可能 ・カバーされているエリアが広い ・速度は Wi-Fi に比べ遅い ・接続認証は通信事業者対応	・通信事業者の通信基地局（データ／音声)
Wi-Fi	・データ通信のみ ・カバーされているエリアが限定的である ・速度は携帯電話回線に比べ速い ・接続認証は独自(個人かサービス提供業者)に対応	・公衆 Wi-Fi(ホテル、ホットスポットなど) ・Wi-Fi ルータ ・家庭内 Wi-Fi ・社内ネットワーク(Wi-Fi) ・テザリング（他のスマートフォンを利用）

これらのネットワークから「①社内ネットワークへアクセスする」、「②組織契約の SaaS/ASP にアクセスする」、というアクセス先の違いに応じて脅威とそれに対する対策を考える必要があります。

また、上記以外にも「Bluetooth を利用する」、「赤外線通信を利用する」など近距離データ通信についても、その脅威と対策を考える必要があります。詳細は、5 章の各項目をご参照ください。

4. スマートフォンの特性と留意点

本章では、スマートフォン特有の性質がもたらす脅威について解説します。

4.1. 特性

スマートフォンは、コミュニケーションツールとしての機能が豊富に搭載されています。また、それを補助するための各種機能も充実しています。そのため、以下のような特性があります。

表 5　スマートフォンの特性一覧

特性	従来の携帯電話	スマートフォン	PC
携帯性	◎	◎	△
ネットワークの接続性	○	◎	△
利便性	○	◎	○
機能性、処理能力	△	○	◎
拡張性	×	○	◎
柔軟性、パーソナライズ	×	◎	○

4.2. 特性から見る脅威

表 5 のように、スマートフォンは携帯性が高いことから、盗難や紛失の脅威を考慮する必要があります。デバイス本体についてだけでなく、SIM カードが抜き取られる恐れもあります。

加えて、落下や水没による故障も考えられます。スマートフォンは公共の場所で利用されることも多いため、覗き見も懸念されます。

また、ネットワークの接続性の向上により常時接続が実現し、外部サービスへ容易にアクセスできるようになりました。そのため、紛失等が発生した場合の情報の漏洩範囲が、デバイス内のデータのみならず、外部サービスで保持するデータにまで広がる可能性が高まっています。

さらに、パスワードや認証情報のキャッシュによる利便性の向上が、情報漏洩のリスクを高めています。

4.3. これまでの PC セキュリティとの相違

スマートフォンは黎明期であり、OS やメーカー、通信事業者などによって、機能やセキュリティ実装面における標準化が進んでいない状況と考えられます。

従って、業務デバイスとして活用する上での管理面にはまだ未成熟な側面も残っており、一律にできる対策には制限があるため、その点を考慮しつつ導入することが重要です。また、バージョンアップの速度が速く、新旧のデバイスが混在することで、さらに管理面の複雑化を招いています。

スマートフォンには、標準化の進んだ PC そのもののセキュリティを等しく適用することは難しく、デバイスそれ自体、ネットワークアクセス時、システムやサービスへのアクセス時、データの置き場所、管理面など、様々な側面からの対策を組み合わせる必要性が高いといえます。

5. 利用シーンから見る脅威と対策

本章では、スマートフォンの利用者視点から、利用シーンを想定して脅威と対策を解説しています。
本章以降では、スマートフォン本体をデバイスと記載します。
スマートフォンでは、電話機能を含めすべての機能がアプリケーションで提供されています。
利用シーンから見た脅威を考える場合、データの保存場所を認識できるかが重要です。そのため本ガイドラインの利用シーンは、保存場所が認識しやすい「メール（デバイスにデータが保存される)」、「ブラウザ（主に外部のデータにアクセスする)」などを別項目とし、その他は、「アプリケーション（どこにデータが保存されているか容易に認識できない)」を区別してまとめています。

5.1. アドレス帳を利用する

スマートフォンのアドレス帳は、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を持っています。
そのため、氏名、電話番号だけではなく、複数のメールアドレスや SNS のアカウントなど従来よりも多くの個人情報が含まれます。
アドレス帳のデータの保管場所は、デバイス、外部記憶媒体、外部サービスを任意に選択できます。さらに外部サービスでは、他者と共有するサービスがあります。

表 6　脅威と対策（アドレス帳を利用する）

脅威	解説（リスク）	対策　または　要件
誤操作 知識不足	・情報の保存場所を誤って指定した結果、意図せず情報が公開されてしまう。 （クラウド上のアドレスに同期されるケースがあるため、それが自動的に広範囲に公開されてしまう脅威がある）	・手順書(アカウント登録の手順、登録の際の注意事項、外部接続の設定方法)を作る。 ・保存場所を選択できないようにする。 ・業務専用の場所に保存する。 ・アプリケーションの動き（データ保存先、外部接続先等）を調べる。
プライベートデータの混在 【BYOD】 	・業務データとプライベートデータが混在することにより、漏洩発生時の強制消去対象にプライベートデータが含まれると、対応が複雑になる。 ・業務利用終了時のデータ消去が困難になる。	・誓約書にサインさせる。 ・業務用とプライベートのデータ保存場所を区分する。 ・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

通話する場合、大きく分けると「通信事業者の音声回線を利用した通話」、「通信事業者のデータ通信回線を利用した VoIP による通話」、「Wi-Fi を利用した VoIP による通話」の 3 つの経路があります。
スマートフォンは、内線としても利用できます。
一般的にスマートフォンの内線化は、コストの削減、場所に囚われない円滑なコミュニケーションの実現、デスクの効率的な利用など効果は高いですが、VoIP にまつわる脅威を理解し適切な対策を行うことが求められます。以下は、3 つの経路の中で特に注意が必要な「Wi-Fi を利用した VoIP による通話」を利用した場合の脅威と対策です。
なお下記の脅威と対策に加え、5.7 節「社内ネットワークを利用する」を参照してください。

表 7　脅威と対策（電話を利用する）

脅威	解説（リスク）	対策 または 要件
盗聴	・通話の内容が第三者に傍受され情報が漏洩する。	・VoIP を利用する際には、通信経路を暗号化する。
不正利用	・電話番号を不正に利用される。	・IP PBX サーバで外線転送の機能を制限する。
不正アクセス	・IP PBX サーバが踏み台となり不正侵入される。	・IP PBX サーバにパスワードをかけるなど周囲環境のセキュリティ強化を行う。デバイスを認証する。
私的利用	・業務外の通話によりコストが増加し、さらに生産性も低下する。	・手順書の中で明記する。（業務時間中の利用に対するマナー等の注意喚起） ・通話履歴を取得する。

5.3. メールを利用する

スマートフォンのメールは、複数のメールアカウントを、ひとつのデバイスで利用できます。

スマートフォンは通信事業者のデータ通信回線に常時接続されているため、例え企業ネットワークに VPN 接続して安全にメールを受信（ダウンロード）したとしても、その後通信事業者のデータ通信回線から直接メールが転送されると企業ではそれを把握することができません。

また、メールには商取引上の重要なファイルが添付されることが多々あり、それが一般的にはデバイスにダウンロードされているため、情報漏洩対策が非常に重要になります。

なお下記の脅威と対策に加え、5.7 節「社内ネットワークを利用する」または 5.8 節「組織契約の SaaS/ASP サービスを利用する」を参照してください。

表 8　脅威と対策（メールを利用する）

脅威	解説（リスク）	対策　または　要件
不正利用	・本文や添付ファイルを容易に転送でき、情報が漏れる。	・手順書を作る。（メールの利用方法などのルール） ・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。 （アプリケーションの起動など操作履歴の取得。監査証跡を残す。スクリーンキャプチャさせない）
誤操作	・誤操作による削除で情報が紛失する。 ・誤送信により情報が漏れる。	・手順書を作る。(誤送信に対する注意喚起、添付ファイル利用時の注意喚起、誤送信発生時の連絡対応) ・送信前に送信先や添付の有無を確認する。 ・ファイルの添付は禁止し、別手段で送付する。 ・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。
プライベートメールの混在【BYOD】 	・業務メールとプライベートメールが混在することにより、漏洩発生時の強制消去対象にプライベートメールが含まれると、対応が複雑になる。 ・業務利用終了時のメール消去が困難になる。	・誓約書にサインさせる。（情報漏洩等が発生した場合、強制データ消去、懲戒、賠償等の責任が発生することを明示する） ・業務用とプライベートのデータ保存場所を区分する。 ・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。

5.4. スケジュールを利用する

スマートフォンは、簡単に持ち運びができ、必要なときに予定を管理できる手帳のように利用できるため、スケジュールの利用頻度が特に高くなっています。個人のスケジュール管理に加え、組織として他者とスケジュールを共有することで、仕事の効率化に役立てることができます。

クラウド上や社内にあるスケジュールのリアルタイムな閲覧、更新が可能であり、また、利用するサービスによってはプライベートのスケジュールや仕事のスケジュールを一つのカレンダーの上で管理することも可能です。

この時、データがデバイス側に保管されるのか、外部サービス側に保管されるのかによって、脅威や対策が異なります。

なお下記の脅威と対策に加え、5.7 節「社内ネットワークを利用する」または 5.8 節「組織契約の SaaS/ASP サービスを利用する」を参照してください。

表 9　脅威と対策（スケジュールを利用する）

脅威	解説（リスク）	対策　または　要件
誤操作、 知識不足	・情報の公開範囲を誤って指定した結果、意図せず情報が公開されてしまう。 （クラウド上のスケジュールに同期されるケースがあるため、それが自動的に広範囲に公開されてしまう脅威がある）	・サービス毎に利用の仕組みが異なるため、アプリケーションの動き（データ保存先、外部接続先等）を調べる。 ・手順書を作る。（スケジュール登録の手順。登録の際の注意事項、例えば登録する情報を符号化など関係者以外に分かりにくくする、公開範囲の設定方法、外部接続の設定・同期方法） ・保存場所を選択できないようにする。 ・業務専用の場所に保存する。
私的利用 【BYOD】 	・業務データとプライベートデータが混在することにより、漏洩発生時の強制消去対象にプライベートデータが含まれると、対応が複雑になる。 ・業務利用終了時のデータ消去が困難になる。	・誓約書にサインさせる。（情報漏洩等が発生した場合、強制データ消去、懲戒、賠償等の責任が発生することを明示する） ・業務データを利用するサービス、アプリケーションおよびアカウントは、プライベートで利用するアプリケーションと区別して設定する。 ・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。

5.5. ブラウザを利用する

スマートフォンは、携帯電話と違いフルブラウザを利用できます。そのため、アクセスできるサイトが急増し、また、業務への活用もしやすくなりました。

PC を利用する場合は、従業員が業務とは関係ないサイトや不適切なサイトにアクセスした場合、アクセス経路上でのアクセス制御およびログ収集が可能です。

しかし、スマートフォンを利用する場合は、通信事業者のデータ通信回線を直接利用することで、管理者は、従業員による業務とは関係ないサイトや不適切なサイトへのアクセス制御およびログ収集ができません。このような状況では、セキュリティポリシーの遵守や情報漏洩対策が非常に重要になります。

なお必要に応じて、下記の脅威と対策に加え、5.7 節「社内ネットワークを利用する」または 5.8 節「組織契約の SaaS/ASP サービスを利用する」を参照してください。

表 10　脅威と対策（ブラウザを利用する）

脅威	解説（リスク）	対策　または　要件
不正利用	・キャッシュ情報により悪意を持って利用する。	・手順書を作る。（キャッシュの削除方法、ブラウザ利用上の注意喚起、ルールを作る）
盗聴	・通信の内容が第三者に傍受され情報が漏洩する。	・社内へのアクセスの場合は、HTTPS などで通信を暗号化する。
マルウェア	・デバイスをのっとられて、情報が漏洩する。 ・加害者化する可能性がある。	・マルウェア対策アプリケーションで不正コンテンツを確認し、侵入しないようにする。 ・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。
私的利用（不適切コンテンツ）	・業務外の通信によりコストが増加し、さらに生産性も低下する。 ・犯罪機会が増加する。	・手順書を作る。（利用上のマナーとルールの明示） ・企業ポリシーを作り、Web フィルタリングで制限する。 ・閲覧履歴を取得する。（【BYOD】の場合は個人のプライバシーの侵害に繋がる恐れがある）
フィッシング	・表示エリアが小さいため、不正な URL に気づかずフィッシングサイトにアクセスしてしまう。	・手順書を作る。（利用上の注意喚起 : 例えば、URL を確認する、安易に短縮 URL にアクセスしないなど） ・Web フィルタリングで保護する。

5.6. ネットワークに接続する

スマートフォンからネットワークを利用するためには、まず契約している携帯電話回線や Wi-Fi を経由し、目的となるサービスにアクセスします。

その経路とアクセス先のサービスによって、その脅威と対策を考える必要があります。

以下に、スマートフォンからネットワークへの入り口における脅威と対策を説明します。

社内 Wi-Fi ネットワークを利用する場合の脅威については、5.7 節「社内ネットワークを利用する」を参照してください。

表 11　脅威と対策（ネットワークに接続する）

ネットワークの接続先	脅威	解説（リスク）	対策　または　要件
Wi-Fi ルータテザリング(ルータ機能)	不正アクセス	・第三者に不正に利用され通信量が増加する。	・推測されにくい SSID にする。 ・できる限り暗号化強度の高い暗号化方式を利用する。 ・パスワードを複雑にする
	不正利用	・社内の PC からインターネットに直接接続し、情報を流出させる。	・社内での利用を禁止する。 ・テザリング機能が起動していないかを監視する。
公衆 Wi-Fi	盗聴	・アクセスしている内容が第三者に傍受され情報が漏れる。 ・偽装されたアクセスポイントに接続することによってパスワードなどが盗まれる。	・信頼できるサービスを利用する。 ・不明なアクセスポイントは利用しない。 ・利用可能なアクセスポイントに制限をかける。 ・パスワードなどの重要な情報については、SSL などで暗号化されているかを確認する。
携帯電話回線	通信事業者による通信規制	・通信しにくい。	・マルチコミュニケーションパスを用意しておく。(音声⇒VoIP 等)
	圏外	・通信できない。	・電波状況の良いところに移動する。 ・アクセスポイントの見直しをする。
	通信事業者の回線障害	・通信できない。	・単一通信事業者へ偏向しない。 ・Wi-Fi 接続への回避を検討しておく。 （本表、Wi-Fi ルータおよび公衆 Wi-Fi 利用時の脅威参照）
	不正利用	・業務外のデータ通信によりコストが増加し、さらに生産性も低下する。	・マナーの徹底やルールを作る。 ・社内でデータ送受信履歴を取得する。

5.7. 社内ネットワークを利用する

社内システムを利用するためには、社内ネットワークへ接続する必要があります。
社内ネットワークへのアクセス経路には、３つの方法があります。

- 社内の Wi-Fi ネットワークに直接接続
- 携帯電話回線や公衆 Wi-Fi などを使い VPN で接続
- 通信事業者が提供する専用線サービスで接続

それぞれの経路での対策が必要であるとともに、接続を許可する側においてもその対応が必要となります。

表 12　脅威と対策（社内ネットワークを利用する）

アクセス経路	脅威	解説（リスク）	対策 または 要件
社内 Wi-Fi ネットワーク	成りすまし（利用者）	・許可されていない利用者が社内ネットワークに接続する。	・ユーザ認証を行う。 ・アクセスログを取得する。 （Wi-Fi の場合、デバイス認証とユーザ認証の多段階認証が実現できないので脅威の優先度によって使い分ける。ユーザ認証の場合は無許可デバイスの持ち込みを防止することができなくなる）
	成りすまし（デバイス）	・許可されていないデバイスが社内ネットワークに接続する。	・デバイス認証を行う。 ・アクセスログを取得する。 （Wi-Fi の場合は無許可デバイスの排除を目的とすることが多いので、この場合はアクセスするシステム側でユーザ認証を行う）
	盗聴	・アクセスしている内容が第三者に傍受され情報が漏れる。	・重要なデータ通信については経路上及びデータ上で暗号化する。
	不正利用	・社内ネットワークを経由して業務外の利用を行う。	・アクセスログを取得する。
	不正アクセス	・必要でないあるいは許可されていない社内システムにアクセスし、情報を持ち出す。	・アクセスできる社内システムを制限する。（ネットワークを分離する、SSID を分ける、アクセスポイントを分ける） ・アクセスログを取得する。
VPN (携帯電話回線や公衆 Wi-Fi など)	成りすまし（利用者）	・許可されていない利用者が社内ネットワークに接続する。	・ユーザ認証を強化する。 ・アクセスログを取得する。
	成りすまし（デバイス）	・許可されていないデバイスが社内ネットワークに接続する。	・デバイス認証を行う。 ・アクセスログを取得する。
	機器障害	・ネットワーク機器の障害でサービスが停止し、業務ができない。	・冗長化する。 ・代替手段を確保する。
	脆弱性に対する攻撃	・ネットワーク機器の脆弱性を攻撃され、不正にアクセスされる。	・アクセスログを取得する。 ・機器をバージョンアップするなどして脆弱性対策を行う。
通信事業者閉域網	通信事業者による通信規制	・通信事業者の規制により通信できない、または遅延が生じる。	・利用する通信事業者を分散する。 ・公衆 Wi-Fi などのサービスを利用できる準備をしておく。
	圏外	・サービスエリア外になり通信ができない。	・サービスエリア内へ移動する。
	通信事業者の回線障害	・通信事業者側の回線障害により通信できない。	・利用する通信事業者を分散する。 ・公衆 Wi-Fi などのサービスを利用できる準備をしておく。

5.8. 組織契約の SaaS/ASP サービスを利用する

スマートフォンの利便性により、組織における SaaS/ASP の更なる利用拡大が予想されます。

組織契約の SaaS/ASP サービスを利用する場合、ID などアクセスできる権限を与えられ、インターネットに接続されていれば、社内に限らず、どこからでも PC を含むどのデバイスからでも、アクセスすることができます。従って、利便性が高い分、その脅威と対策について十分検討しておく必要があります。

なお、SaaS/ASP サービスを利用する上では、法規制やサービス障害など、SaaS/ASP サービス特有の脅威について念頭においておく必要があります。

表 13　脅威と対策（組織契約の SaaS/ASP サービスを利用する）

アクセス経路	脅威	解説（リスク）	対策 または 要件
社内 Wi-Fi ネットワーク 携帯電話回線 公衆 Wi-Fi Wi-Fi ルータ など	不正利用	・外出先などから組織契約の SaaS/ASP サービスにアクセスし情報を外部に漏洩させる。	・サービス提供側でアクセスログを取得する。 ・サービス提供側でアクセスできるネットワークに制限を設け、社内でアクセスログを取得する。
	成りすまし	・許可されていないユーザによって、サービスが利用される。	・サービス提供側でユーザ認証を強化させる。または社内の認証システムと連携させる。 ・デバイス認証を実施する。 ・アクセスログを取得する。

5.9. アプリケーションを利用する

アプリケーションをダウンロードする際、その信頼性はマーケットによって異なることを認識しておく必要があります。（詳細は 3.2 節「アプリケーションとその入手形態」を参照）

アプリケーションによっては、外部にデータを保管して利用するのか、デバイス内のデータを利用するのか利用者にとって判断するのが難しい場合もあります。アプリケーションの動きを調査し、相応の対策をとった上で利用してください。

なお、企業や団体などが独自に開発したアプリケーションを活用する場合は、アプリケーションの特性に合わせて個別の対策を検討してください。

必要に応じて、下記の脅威と対策に加え、5.7 節「社内ネットワークを利用する」または 5.8 節「組織契約の SaaS/ASP サービスを利用する」を参照してください。

表 14　脅威と対策（アプリケーションを利用する）

脅威	解説（リスク）	対策　または　要件
誤操作 知識不足	・情報の保存場所を誤って指定した結果、意図せず情報が公開されてしまう。 ・情報の保存場所を意識せず使うことで情報が漏洩する。	・手順書を作る。（保存場所への注意喚起を提示する） ・アプリケーションの動き（データ保存先、外部接続先等）を調べる。
盗聴	・通信の内容が第三者に傍受され情報が漏れる。	・社内へのアクセスの場合は、HTTPS などで通信を暗号化する。
マルウェア	・悪意のあるアプリケーションにより、不正に利用される。	・アプリケーションのインストール時にむやみにアクセス許可（Permission）をしない。 ・信頼できるマーケットから入手する。 ・指定されたアプリケーションを利用する。
私的利用	・業務中に利用する等で業務を阻害する。	・業務時の利用を制限（禁止）する。
私的利用（不適切コンテンツ）	・業務外の通信によりコストが増加し、さらに生産性も低下する。 ・犯罪機会が増加する。	・手順書を作る。（利用上のマナーとルールの明示） ・企業ポリシーを作り、フィルタリングで制限する。 ・利用履歴を取得する。
プライベートデータの混在【BYOD】 	・業務データとプライベートデータが混在することにより、漏洩発生時の強制消去対象にプライベートデータが含まれると、対応が複雑になる。 ・業務利用終了時のデータ消去が困難になる。	・手順書を作る。（利用範囲の明示） ・誓約書にサインさせる。 （情報漏洩等が発生した場合、強制データ消去、懲戒、賠償等の責任が発生することを明示する） ・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。

5.10. デバイスの機能を利用する

ここで言う「デバイスの機能」とはデバイスに備わっているハードウェア的な機能を前提とします。

デバイスの機能の中で注目すべきは、「情報を取り込む入口」となる機能、「情報を送る出口」となる機能になります。「情報を送る出口」となる機能については、これまで述べてきた「データ通信」（ソフトウェア的には「メール」、「ブラウザ」、「アプリケーション」も出口となります）で記載しているため、ここでは割愛します。

「情報を取り込む入口」となる機能の代表的なものは、「カメラ」、「マイク」です。また、これらの機能は新しい機種が発売されるたびに増える傾向があります。

5.10.1. カメラを利用する

多くのスマートフォンでは、カメラを内蔵し、静止画や動画の撮影に利用できます。撮影したデータは容易に送信可能であり、画像データの流出を避けるには、望まない撮影をいかに止めるかかが鍵となります。

表 15　脅威と対策（カメラを利用する）

脅威	解説（リスク）	対策　または　要件
不正利用	・利用を制限されたエリアでの利用及び持ち込みによって、取引先等のセキュリティルールの違反、不正な情報の漏洩につながる。	・プライバシー保護シール等を添付し、利用しない。 ・カメラ機能を無効化する。
誤操作 知識不足	・情報の保存場所を誤って指定した結果、意図せず情報が公開されてしまう。	・手順書を作る。（利用範囲の明示、機能の利用方法、データの保存場所に対する注意喚起、肖像権等への注意喚起）
誤操作	・誤ってカメラが起動してしまい、本人の意図しない撮影がなされてしまう。	・セキュリティシールを添付し、利用しない。 ・カメラ機能を無効化する。
知識不足	・安易に機能を利用することで、意図しない情報を取得してしまう。（他者の肖像権の侵害や禁止された区画での利用等）	・手順書を作る。（利用範囲の明示、機能の利用方法、データの保存場所に対する注意喚起、肖像権等への注意喚起）
フィッシング	・バーコードリーダーを利用して接続された先がフィッシングサイトであるおそれがある。	・手順書を作る。（注意喚起。例えば、バーコードの発行元が信頼できるかを確認する、接続前に表示される URL を確認する等）
マルウェア	・悪意のあるアプリケーションにより、カメラ機能が不正に利用される。	・アプリケーションのインストール時にむやみにアクセス許可をしない。 ・カメラ機能を無効化する。
撮影情報の漏洩	・スマートフォンで撮影された画像の情報として、Exif（位置情報等や機種情報等の撮影情報）が意図せずに漏洩してしまう。	・撮影画像を外部に公開する際には、Exif を削除する。 ・撮影時に位置情報機能を停止する。
プライベートデータの混在【BYOD】 	・業務データとプライベートデータが混在することにより、漏洩発生時の強制消去対象にプライベートデータが含まれると、対応が複雑になる。 ・業務利用終了時のデータ消去が困難になる。	・誓約書にサインさせる。（情報漏洩等が発生した場合、強制データ消去、懲戒、賠償等の責任が発生することを明示する） ・業務データを利用するサービス、アプリケーションおよびアカウントは、プライベートで利用するアプリケーション等と区別して設定する。 ・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。

5.10.2. マイクを利用する

スマートフォンでは、マイクロフォンを内蔵しており、通話録音やボイスレコーダーとして活用できます。録音したデータは容易に送信可能であり、データの流出を避けるには、望まない録音をいかに止めるかかが鍵となります。

表 16 脅威と対策（マイクを利用する）

脅威	解説（リスク）	対策 または 要件
ルールの侵害	・利用を制限されたエリアでの利用及び持ち込みによって、取引先等のセキュリティルールの違反、不正な情報の漏洩につながる。	・持ち込み場所や利用方法を制限する。
誤操作 知識不足	・情報の保存場所を誤って指定した結果、意図せず情報が公開されてしまう。	・手順書を作る。（利用範囲の明示、機能の利用方法、データの保存場所に対する注意喚起）
マルウェア	・悪意のあるアプリケーションにより、録音機能が不正に利用される。	・アプリケーションのインストール時にむやみにアクセス許可をしない。
プライベートデータの混在【BYOD】 	・業務データとプライベートデータが混在することにより、漏洩発生時の強制消去対象にプライベートデータが含まれると、対応が複雑になる。 ・業務利用終了時のデータ消去が困難になる。	・誓約書にサインさせる。 （情報漏洩等が発生した場合、強制データ消去、懲戒、賠償等の責任が発生することを明示する） ・業務データを利用するサービス、アプリケーションおよびアカウントは、プライベートで利用するアプリケーション等と区別して設定する。 ・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。

5.10.3. 位置情報を利用する

多くのスマートフォンは、GPS 機能を備えており、自分がどこにいるかを把握できます。利用者やデバイスがどこに存在するかを確認出来ることは、非常時の安否確認や紛失デバイスの特定に有効です。

表 17 脅威と対策（位置情報を利用する）

脅威	解説（リスク）	対策 または 要件
誤操作 知識不足	・安易に機能を利用することで、意図しない情報を公開してしまう。	・手順書を作る。（利用範囲の明示、機能の利用方法、位置情報が外部に公開されることに対する注意喚起）
盗聴	・意図せず自分の位置情報を他人に知られてしまう。	・不要であれば位置情報機能を停止する。
マルウェア	・アプリケーションがスマートフォンの位置情報を収集し、不正に利用される。	・アプリケーションのインストール時にむやみにアクセス許可をしない。 ・利用許諾契約をよく読み、怪しい記載のあるアプリケーションは使わない。

5.10.4. NFC を利用する

一部のスマートフォンでは、NFC 機能※ を持っています。スマートフォンを決済や入退管理等のデバイスとして利用出来ます。

※NFC(Near Field Communication)：近距離無線通信

表 18　脅威と対策（NFC を利用する）

脅威	解説（リスク）	対策　または　要件
スキミング	・デバイス内のデータが不正に読み取られることで、情報の漏洩が発生する。	・利用しない場合はロック機能を設定する。 ・チップ部分にカバーをつける。
デバイスの故障	・デバイスの故障により機能が利用できない。（入退管理や決済など）	・手順書を作る。（故障時の代替手順の明示）
なりすまし	・不正に入手したデバイスによって本人に容易になりすましが可能となり、不正な入室や決済が発生する。	・手順書を作る。（盗難・紛失時の連絡方法、対応方法） ・ロック機能を有効にする。

5.10.5.　ワンセグを利用する

一部のスマートフォンでは、ワンセグの受信機能を持ち、テレビ番組やデータ放送を受信できます。

表 19　脅威と対策（ワンセグを利用する）

脅威	解説（リスク）	対策　または　要件
私的利用	・業務中に利用する等で業務を阻害する。	・手順書を作る。（利用範囲の明示。業務時の利用を制限する等） ・業務時の利用を禁止する。

5.10.6.　Bluetooth を利用する

Bluetooth は比較的近距離（数メートル～数十メートル）の機器間の接続に使われる規格であり、スマートフォンでは多く活用されています。あらかじめ設定（ペアリング）された機器間では、簡易に接続が可能なため、ヘッドフォンや PC との接続に利用されます。

表 20　脅威と対策（Bluetooth を利用する）

脅威	解説（リスク）	対策　または　要件
不正アクセス	・不正にデバイスに接続され、データを読み取られる。	・デバイスが接続可能な機器を限定する。 ・Bluetooth が不要であれば利用せず、無効化する。
不正利用	・利用者が組織の許可しない PC 等に接続し、デバイス上の情報を持ち出す。	・デバイスが接続可能な機器を限定する。 ・手順書を作る。（利用範囲の明示、情報の授受に対する注意喚起） ・誓約書にサインさせる。（特に BYOD の場合、漏洩時の責任等） ・Bluetooth が不要であれば利用せず、無効化する。
マルウェア	・Bluetooth 通信経路で感染するマルウェアが存在し、感染経路になりうる。	・マルウェア対策アプリケーションを導入する。 ・デバイスが接続可能な機器を限定する。 ・Bluetooth が不要であれば利用せず、無効化する。
Bluetooth の自動起動	・利用者が意図せず Bluetooth を起動し、接続を行う。 ・アプリケーション終了後も Bluetooth 自体が有効となり、他の脅威をまねく。	・ホーム画面に Bluetooth のアイコンが表示されているかどうか確認する。 ・Bluetooth を利用するアプリケーションを調べる。

5.10.7. 赤外線通信を利用する

赤外線通信は、携帯電話からも利用されている近距離（数 cm～数十 cm）の機器間の接続に使われる規格で、一部のスマートフォンで利用することができます。

用途としてはアドレス帳データの授受など、比較的短時間でデータを転送する際に利用されます。

表 21 脅威と対策（赤外線通信を利用する）

脅威	解説（リスク）	対策 または 要件
誤操作 知識不足	・意図せず情報を流出してしまう。	・手順書を作る。（利用範囲の明示、情報の授受に対する注意喚起）

5.11. データの可搬媒体として利用する

スマートフォンは、その一面として大容量の USB ストレージであるとも言えます。

この機能によりスマートフォンはデータの可搬媒体となり、大量のデータを持ち出すことが可能となりますので、紛失時の影響度は PC 同等と考える必要があります。

デバイスやアプリケーションによっては、デバイスや SD カードなど外部記憶媒体内のデータを暗号化することが可能ですが、その場合でもデバイスのロックなどの認証を抜けられた場合には、内部データの閲覧が可能となるため、紛失時の対策は必須と考えてください。

原則として、スマートフォンをデータの可搬媒体としては利用しない、ということを強く推奨します。

表 22 脅威と対策（データの可搬媒体として利用する）

脅威	解説（リスク）	対策 または 要件
盗難･紛失および故障	・盗難や紛失および故障により、持出し時に保存されたデータの消失および情報漏洩が発生する。（PC 等に比して携帯性が高いため）	・手順書を作る。（盗難・紛失時の連絡方法、対応方法、利用範囲の明示、データの保管場所に対する注意喚起。例えば、利用時には高機密のデータの保存は許可しないなど） ・代替手段（USB ストレージや企業向けのストレージサービス）を用意する。 ・本体および外部記憶媒体のデータ領域を暗号化する。
外部記憶媒体の抜き取り	・利用者が注意を怠っている間に、挿入された外部記憶媒体が抜き取られ、記録されたデータが流出する。	・手順書を作る。（外部記憶媒体の利用に対する注意喚起。例えば、組織の許可のない外部記憶媒体の利用や、組織が貸与した外部記憶媒体の抜き差しの禁止等） ・データを暗号化する。
プライベートデータの混在【BYOD】 	・業務データとプライベートデータが混在することにより、漏洩発生時の強制消去対象にプライベートデータが含まれると、対応が複雑になる。 ・業務利用終了時のデータ消去が困難になる。	・誓約書にサインさせる。（情報漏洩等が発生した場合、強制データ消去、懲戒、賠償等の責任が発生することを明示する） ・業務データを利用するサービス、アプリケーションおよびアカウントは、プライベートで利用するアプリケーション等と区別して設定する。 ・デバイス内の保存場所をプライベートデータと業務用データを分ける。 ・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。

※上記以外にも、PC のマルウェアの媒介となる恐れもあります。

5.12. バックアップを取る／同期する

スマートフォンでは、PC やクラウド等にデータのバックアップ（同期）が可能です。
そのため、セキュリティを考える上ではバックアップされたデータの管理も必要となることに注意しましょう。

表 23　脅威と対策（バックアップを取る／同期する）

脅威	解説（リスク）	対策　または　要件
誤操作 知識不足	・データ同期の方法や、データの保存場所を意識していないため、意図せずデータを上書きしたり、消失させてしまう。	・手順書を作る。（バックアップや同期およびリストアの実施方法。データの保存場所に対する注意喚起、例えば、同期先やバックアップ取得先は、貸与した業務デバイス等に限定する等） ・アプリケーションやデバイス毎に同期、バックアップの仕組みが異なるため、動きを調べる。 ・バックアップツールを配布する。
バックアップデータにおける業務データの混在 【BYOD】 	・私物 PC から業務データを含むバックアップデータが流出する恐れがある。	・誓約書にサインさせる。（情報漏洩等が発生した場合、懲戒、賠償等の責任が発生することを明示する） ・暗号化したデータでバックアップする。（私用 PC でも暗号化対象とする）

5.13. 【参考】インターネットストレージサービスを利用する

インターネットストレージサービスは、データの保管庫としての利用や、同じデータを「いつでもどこからでも」「必要な人と」利用できる便利さにより、特に個人利用を中心に利用が広がっています。
PC では、アクセスの制限（フィルタリング）や利用の監視ができますが、スマートフォンではその制御は困難です。
また、スマートフォンは通信事業者のデータ通信回線に常時接続されているため、例え企業ネットワークに VPN 接続して安全にデータを授受したとしても、その後通信事業者のデータ通信回線から直接インターネットストレージサービスに転送されると企業ではそれを把握することが困難です。そのため、組織として指定したサービス以外の業務利用は、許可しないことを強く推奨します。

5.14. 【参考】SNS を利用する

SNS やミニブログは、コミュニケーションツールとして、特に個人利用を中心に利用が広がっており、見たことや聞いたことをすぐに友人等に知らせることができるなど、スマートフォンの特性に合致しています。
また、マーケティングや、コミュニケーション活性化の手段として利用する企業も増えています。
その一方で、不注意な書き込み、誤った情報の公開、業務時間内の私的利用、携帯性による GPS や写真での場所特定など、SNS の脅威は日々高まっています。そのため、組織内でルールを策定した上で利用することを推奨します。

6. ライフサイクルから見る留意点

本章では、スマートフォンの導入計画から廃棄に至るまでのライフサイクルにおける留意点を解説します。
特に注意が必要なポイントである BYOD については、その旨を明記して解説しています。
なお本章では、災害など緊急事態の際に、一時的にスマートフォンの利用を許可する場合に考慮しておくべきポイントとしても、活用できます。

6.1. 計画

スマートフォンの導入における計画段階においては、その業務活用の目的を明確化すると共に、想定される利用シーンを特定する必要があります。その上で、5 章の「利用シーンから見る脅威と対策」を参照し、必要な対策を実施、あるいはリスクを理解した上で受容するという判断をしてください。
なお、BYOD を許可する場合には、セキュリティポリシー遵守について、利用者と事前に合意を形成することが運用時に重要になりますので、この段階で誓約書を作成しておきましょう。

6.1.1. 社内ルールを整備する

社内ルールの整備は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。利用シーンの脅威と対策を確認した上で、スマートフォンの利用範囲を決め、利用に関するルールを整備し、手順書を作成してください。
なお、不正利用やインシデント発生時のルールについては、誓約書を作成または改訂するなど、スマートフォンを想定した内容に見直しが必要です。
特に、スマートフォンの特性から、盗難、紛失に対する対応ルールの整備が重要です。

6.1.2. 利用マニュアルを整備する

利用マニュアルの整備は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。利用マニュアル作成の際、「タップ」、「フリック」、「ピンチ」などのスマートフォン特有の専門用語を利用する場合には十分な説明が必要です。また、各種設定方法は機種によって違いますので、注意してください。
なお、マニュアルはスマートフォンから閲覧することも想定して作成するのが適切と考えられます。
法人資産の時と、BYOD の時の注意点を把握して、マニュアルを作りましょう。

6.1.3. サポート体制を整備する（ヘルプデスクや担当設置）

サポート体制の整備は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。現状、利用者は、スマートフォンについて正確かつ十分な知識が不足しています。そのため導入にあたっては、サポートの体制を十分に整えておくことが非常に重要です。加えて、導入手順の簡素化やマニュアルの整備、FAQ の公開によるセルフサポートなど、計画段階から導入時のサポート負荷を削減するための検討を行うことが、スムーズな展開には必要です。
特に、営業時間外の盗難や紛失時の対応方法を、予め定めておくことが重要になります。

6.1.4. 教育を実施する

教育の実施は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。現状、利用者は、スマートフォンについて正確かつ十分な知識が不足しています。従って、導入にあたって教育を実施することは非常に重要です。教育は、本ガイドラインで解説しているスマートフォンの特性や、利用シーンにおける留意点など、利用者のセキュリティ意識を高める内容とし、定期的に実施してください。

6.2. 導入

スマートフォンの導入段階においては、利用開始手続き、各種デバイスに装着する備品などの準備からデバイスの初期設定、アカウントの設定、および利用するアプリケーションの登録など、利用者の負荷を最小

限に抑えて、効率的に展開することが重要です。
　また、大量に一括で導入する初期の導入時のみならず、定期的な小規模な導入、または紛失や故障などに対応するための随時個別の対応を想定し、作業負荷が低く、ミスのない導入を実現することが最大の課題となります。

6.2.1.　利用開始手続きを行う

　利用開始手続きは、所有形態および利用目的の違いによって異なります。しかしながら、所有形態に関わらず、業務利用の際には必要です。デバイスの管理をするために、利用者とデバイスの紐付けを行うなど台帳作成を行いましょう。
　BYOD を許可する場合、確認・承認など申請時の条件および承認手続きの整備、誓約書の合意、利用許可表示などが重要です。

6.2.2.　備品を用意または装着する

　備品を用意または装着する場合は、所有形態および利用目的の違いによって異なります。落下対策は法人資産に対して実施することを推奨します。覗き見防止対策、不正利用対策は所有形態および利用目的の違いに関わらず実施することを推奨します。

6.2.3.　アカウントを取得する/させる

　初期設定を行うためのアカウントの取得方法は、所有形態および利用目的の違いによって異なります。BYOD の場合には、利用者が既にアカウントを取得済みである場合が一般的ですので、利用時に組織に登録させることも考慮する必要があります。法人所有のデバイスのアカウントを取得する場合には、アカウントの命名規則について事前に決定しておくと運用・管理がスムーズです。

6.2.4.　デバイスを初期設定する

　デバイスの初期設定方法は、所有形態および利用目的の違いによって異なります。法人資産の場合にはキッティングを実施する場合と利用者のセルフサービスで実施する場合がありますが、BYOD の場合には利用者のセルフサービスを前提に考える必要があります。
　デバイスを初期設定する際には、セキュリティポリシーに準じて各種デバイス設定や機能制限を実施する必要がありますが、OS の違いや、同一の OS でもバージョンや機種の違いにより、デバイス設定や機能制限に制約がある場合があります。また、ほぼ全ての設定を自動化できる場合とある程度手動での設定が必要な場合があることも認識しておく必要があります。
　最後に、OS によってはセキュリティポリシーに準拠するための各種デバイス設定が利用者によって変更または削除されてしまう場合があるため、組織としての管理が必須の場合には別途対策を講じる必要があります。

6.2.5.　デバイスのロック機能を有効にする

　デバイスのロック機能の設定は、所有形態および利用目的に関わらず必要です。
　ロックの名称や機能は、デバイスや OS によって異なります。スマートフォンを利用する際は、誤入力回数を制限するなど、セキュリティポリシーに従って必ず有効化してください。

6.2.6.　メールアドレスを取得/設定する/させる

　メールアドレスの取得および設定方法は、所有形態および利用目的の違いによって異なります。BYOD の場合には、利用者が既にメールアドレスを取得済みである場合が一般的ですので、利用時に組織に登録させることも考慮する必要があります。法人所有のデバイスのメールアドレスを取得する場合には、メールアドレスの命名規則について事前に決定しておく必要があります。

6.2.7.　アプリケーションを導入する

　アプリケーションの導入方法は、所有形態および利用目的の違いによって異なります。

セキュリティ関連のアプリケーションを利用者のセルフサービスで導入する際には、アプリケーションの導入状況について、管理者が確認できることが重要です。

なお、BYOD の場合には、幅広い OS やデバイスの種類が想定されることから、利用予定のアプリケーションが対象となる OS やデバイスに対応していることを予め認識しておく必要があります。

6.2.8. デバイスを配付する

デバイスの配付は、法人資産の場合に限ります。各種デバイスの設定などを利用者によるセルフサービスで実施する場合、およびキッティングする場合のどちらについても、資産とその使用者の関係を管理することは重要です。特にキッティングしている場合には、デバイスに個人情報が登録されているため、正規の利用者にデバイスが配付されるよう注意が必要です。

6.3. 運用

スマートフォンの運用段階においては、スマートフォンを安全に業務で活用できるよう適切に管理することが重要になります。そのためには、想定されるリスクを最小限に抑えるためにデバイスが適正に利用されているか、各種デバイスに適正な設定や制限が施されているかなどを定期的に監視する必要があります。また、紛失や盗難などのインシデント発生時の対応や、OS の脆弱性に対応するバージョンアップの方法については、事前に手順を決定しておく必要があります。

6.3.1. デバイス情報を収集/監視する

デバイス情報の収集および監視は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。

スマートフォンのハードウェア情報、OS 情報、導入しているアプリケーション情報、適用している各種デバイス設定や機能制限、OS の不正改造の有無などの情報を定期的に収集し、デバイスの状態を監視することが重要です。管理者はスマートフォンの利用状況を常に把握することで、不正に利用されていないことや、OS などの脆弱性を確認することができます。

なお、OS の不正改造はスマートフォンのセキュリティを脅かす最大の脅威となりえるため、その監視および検出は非常に重要であると言えます。

最後にデバイスの位置情報を取得する場合には、利用者のプライバシーを侵害することになる可能性が高いため、取得に際しては慎重に検討する必要があると共に、紛失時を想定して位置情報を取得したい場合には、利用者に位置情報を取得する旨の合意を事前に取っておく必要があります。

6.3.2. デバイスの機能を制御する

制御は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。

スマートフォンが有する機能の制御、盗難や紛失時の遠隔からのロックやデータ消去により、管理者はスマートフォンの業務利用における安全性を常時管理する必要があります。

デバイスを制御するためには、デバイスに適用するポリシーを作成し、それを各デバイスに適用する必要があります。

現状のスマートフォンは、OS やデバイスによって様々な違いがあるため、多種多様なスマートフォンを、全て管理対象にすることは難しくなります。特に BYOD 時は注意が必要です。

加えて、OS によってはデバイス制御に SMS を利用する場合がありますが、その場合は SMS を利用できないタブレットは制御ができない場合があることも認識する必要があります。

6.3.3. OS のバージョンを管理する

OS のバージョンの管理は、所有形態および利用目的の違いに関わらず業務利用の際には必要です。特に脆弱性の修正が含まれる OS バージョンへのアップグレードは重要です。

しかし、デバイスメーカーや通信事業者の方針によって、バージョンアップすることが難しい場合があります。

そのため、管理者はスマートフォンの OS のバージョンを把握し、報告されている脅威を理解した上で技術面あるいは運用面から対策を実施する、あるいはリスクを受容するなどが求められます。

6.4. 廃棄

スマートフォンを廃棄する際は、業務で利用したデバイス本体内のデータや外部記憶媒体内のデータ、各種デバイス設定情報やアカウント情報、導入しているアプリケーションなどを確実に消去することが重要になります。

廃棄とは、故障などによる「デバイスの回収」、買い替えなどによる「デバイスの変更」、また異動などにより特定の部署に所有されているデバイスを「使いまわす」ということを想定しています。

これらのどのような場合においても必要なのは、業務利用データの消去、各種デバイス設定情報の消去、アプリケーションの削除、外部サービスの認証情報を含むキャッシュの消去です。

特に、BYOD における利用終了時には、上記のような対応が必要になります。

7. おわりに

7.1. 利用目的とセキュリティのバランス

スマートフォンを導入する目的は、組織によって様々です。一番大切なのは、利用目的とセキュリティのバランスです。目的達成のために求められるセキュリティをよく検討した上で、組織の実情に適った対策を取捨選択し、実施してください。

スマートフォンは、コミュニケーションツールとして優れた特性を持っており、それが利用者の創造力とモチベーションを支えることで期待を上回る業務改革の可能性を秘めています。それらの利用効果の発揮と、資産としての管理、そして人の管理、それぞれがうまく図れるよう、よく検討しておきましょう。

なお本ガイドラインは、脅威を網羅的に捉えています。記載している要件すべてに対処するのは難しく、また、そうしなければいけないということではありません。内容を理解してその影響度を分析し、利用目的を熟考した上で、慎重に対応してください。

7.2. 組織のセキュリティポリシーと意思決定

犯罪や事故は、組織内関係者か組織外侵入者かに関わらず、発生する可能性があります。スマートフォンのセキュリティを検討する際も、その特性による例外があるにせよ、緊急性や重要性、データの機密性など、通常のセキュリティの考慮と PDCA サイクルによる見直しが必要です。

また、その対策の実現可能性検証、既存のセキュリティポリシーとの照合/変更、PC とは違う管理・運用と教育、クラウドサービス利用時の諸外国の法律確認など、従来とは違うノウハウも必要になりますので、それらに費やせる時間や予算、そして利用者のリテラシーなど、組織として対応可能な範囲をよく検討しておく必要があります。

7.3. 情報収集継続の必要性

冒頭で述べたように、スマートフォンのセキュリティは発展段階であるため、現状では対処できない課題もあります。その課題を受容した上で運用回避するのか、課題が対象外になる利用方法を取るのか、導入そのものを先送りするのか、意思決定が必要です。さらに今後は、スマートフォンを法人所有として配付するのか、個人所有のものを業務利用(BYOD)するのかという点についても、考える価値があります。

スマートフォンを取り巻く環境は、日々進化しています。そのため、本ガイドラインが提示する特性を理解した上で、常に最新情報の収集を行い、その時点における最適かつ有効なセキュリティを実施してください。

知的生産性向上が求められる時代、変革を恐れず組織力を高めるためのツールとして、ぜひスマートフォンを活用してみましょう。本ガイドラインが、読者の皆さんの意思決定の一助となれば幸いです。