『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』補足資料

BYOD の現状と特性

～あなたの組織はどのパターンですか～

2012 年 10 月 26 日

日本スマートフォンセキュリティ協会（JSSEC）
利用部会 ガイドラインワーキンググループ
BYOD タスクフォース

文書管理番号 JSSEC-USFG-BY-GL20121026-2

目 次

1. はじめに

1.1. 本資料の位置づけと目的

本資料は、組織が個人所有のスマートフォンを業務で利用許可する BYOD の導入を検討する際、もしくは導入後に実状を改めて考察するための基礎資料です。

ワークスタイルの変革などをテーマに、スマートフォンを業務で本格的に利用しようという動向の中で BYOD の関心が高まっていますが、利用状況のパターンや定義の捉え方は様々です。そこで、現状を整理し共通の認識に立った上で、BYOD 導入時に留意する点について解説しています。

本資料は、BYOD の促進や禁止を促すものではなく、客観的な視点で事実を考察するものです。

なお、本資料では、日本スマートフォンセキュリティ協会（JSSEC）発行の「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」（以下、利用ガイドライン）と同様、「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。また、考察の対象は「スマートフォン」であり、PC は含んでおりません。

1.2. 考察範囲

本資料は、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た際、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）のみを考察対象範囲としています。

利用ガイドラインでは、「BYOD」を以下のように分類しています。

表 1　利用ガイドラインに記載されている対象範囲

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、利用ガイドラインでは言及していない範囲です。

2. 利用状況と定義

2.1. 利用状況のパターン

BYOD の捉え方は、個人によって異なっています。そのため、BYOD の導入検討にあたり焦点が合わず、具体的な検討に入れない事例も見受けられます。

本章では､BYOD と捉えられている個人所有のスマートフォンの業務利用状況を考察し､分類しています。各々の分類項目によっていくつかのパターンが見えてきますが、ここでは、下記の５パターンとします。

表２　個人所有スマートフォンの業務利用における利用状況のパターン

パターン (*2) / 分類項目 (*1)	舵取り型	踏み出し型	なし崩し型	知らん振り型	忍び型
所有形態	個人所有				
利用目的	業務利用と個人利用の併用				
利用場所	問わない				
管理者のリスク認識	あり	あり	あり	なし	「舵取り型」と「BYOD 禁止」の場合に存在
導入の意向	あり	あり	決めていない	考えていない	
導入の意思決定	あり	あり	なし	なし	
規定	あり	なし	なし	なし	
規定に基づく許可	あり	なし	なし	なし	

※「BYOD 禁止」とは、BYOD の導入を組織として禁止している状態です。

*1（分類項目）

■利用場所　　：業務をどこで行うか。
■管理者のリスク認識：脅威やリスクを多少なりとも認識しているか否か。
■導入の意向　　：導入する意向があるか否か。
■導入の意思決定　：導入するという意思決定をしたか否か。
■規定　　：規定（利用規定、管理規定、経理規定等）を明文化しているか否か。
■規定に基づく許可　：規定に則り、申請／承認を経て業務での利用を認めているか否か。

*2（パターン）

■舵取り型　：規定が整備され、利用申請と承認のしくみがある状態。管理者と利用者は、個人所有のスマートフォンで利用可能な業務範囲について合意している。組織毎のセキュリティポリシーに応じて、実施する対策には幅がある。場合によっては、未承認の個人所有のスマートフォンを業務利用されている可能性がある（忍び型の発生)。

■踏み出し型　：規定はないが、個人所有のスマートフォンを業務利用する意志があり、実際に利用している状態。効果や利便性を優先しているがリスク認識が不十分である可能性がある。

■なし崩し型　：ある程度のリスク認識はあるが、導入に関する意思決定をしないまま利用者側が先走って利用している状態。

■知らん振り型　：管理者は関与していないように見える状態。組織としても管理者としても、責任を放棄している可能性がある。

■忍び型　：個人所有のスマートフォンを隠れて業務で利用している状態。個人所有のスマートフォンの業務利用を禁止している中での利用、および「舵取り型」でも許可を受けていないスマートフォンの利用、が該当する。

2.2. BYODの定義

本資料における BYOD とは、リスクの認識をした上で、個人所有のスマートフォンの業務利用について組織として意思決定を行い、実際に業務を行うこと、と定めます。

従って、利用状況５パターンの中では「舵取り型」と「踏み出し型」が該当します。

BYOD のポイントは、個人所有のスマートフォンを業務で利用するという点です。ここで言う業務とは、組織が認めた仕事の内容であり、その範囲に当てはまらない利用については BYOD の範囲外と考えます。そのため、会社への持ち込みをしなくても個人所有のスマートフォンで業務を行えば、社内外問わず BYOD と言えます。私用のために会社に持ちこんでも、業務として利用しない場合は BYOD とは言えず、単に個人所有のスマートフォンを会社に持ってきているだけの状態です。

BYOD の望ましい姿は、リスクの認識をして、個人所有のスマートフォンの業務利用について組織として意思決定を行うと共に、利用者からの申請に基づいて利用を許可し、業務範囲を合意している状態であると考えます。従って、予め利用目的と業務範囲を明確にし、申請と承認のしくみを作っておくことが推奨されます。

このような共通認識は、BYOD 導入の検討の際には非常に重要です。同じ認識の上に立って考えることが、検討の効率と質を高めることになります。

3. 特有の環境

本章では、BYOD ゆえの特有の環境について考察します。

BYOD の利用シーンを考える際は、利用ガイドラインに記載している留意点の全体像を、基本的な情報として把握しておくことが重要です。本資料ではその部分は割愛しますが、基本的な情報を理解した上で利用者に節度ある活用を促しておくことが推奨されます。

3.1. 前提条件の変化

個人所有のスマートフォンは、既に個人によって利用が開始されています。そのスマートフォンを業務利用する場合、当然ながら利用者の意思を尊重する必要があります。

そのため、管理や統制のための強制的なアプリケーション導入や、組織側の一方的な指示が困難であることが想定されます。結果として、個人所有のスマートフォンと組織貸与のスマートフォンとでは、以下のように前提条件が変わります。

①デバイスの状態（OS のバージョン等）は、千差万別である。
②利用者が個人的に使っているアプリケーションやサービスの利用禁止は、困難である。
③資産管理（有償アプリケーションの所有や管理、紛失時のデータ削除等）には、精査が必要である。
④デバイスが最初にインターネットに接続するネットワークは、制限できないと考えられる。

詳しくは、次項の表３「管理対象と留意点」で解説します。

3.2. 管理可能な範囲の考え方

上記のような前提条件の違いにより、対象とする業務内容を考える上では、「組織側の管理可能な範囲」と「個人との合意」のバランスが重要となります。バランスのとり方は、組織のポリシーに委ねられます。

BYOD では基本的に、すべてを管理することは不可能です。すべてを管理したい場合、BYOD は推奨できません。言い換えると、BYOD ではすべてを管理する必要はなく、目的に合わせて管理対象を選択することになります。
結果として、スマートフォンの状態をコントロールすることは困難と捉えて許可できる業務範囲を設定し、その上で、BYOD 導入時に留意が必要な項目を検討してください。

例えば、アプリケーションに関係なく「情報」を管理したい場合、業務データをどこに保存させるのか、スマートフォンには保存されないようにするのか、どこ（クラウド上やスマートフォン本体、外部記憶媒体等）に保存されても良いように保護しておくのか、等が焦点になります。管理の方法は、規約による合意、監査、記憶領域の保護、データそのものの保護、システムやネットワークへのアクセス制御、等があります。
有償アプリケーション（汎用の有償アプリケーションや社内開発アプリケーション）を利用する場合は、その資産管理が必要です。有償の汎用アプリケーションを利用する場合、組織が一括購入できる場合もあれば、個人の立て替えが必要な場合もあります。

管理可能な範囲を考える上では、以下の表を参考にしてください。

表３　管理対象と留意点

対象	内容	留意点（前提条件の変化等）	利用ガイドライン参照ページ
デバイス	・組織側で把握しておくべき情報	・完全な管理は不可能であり、何を把握しておきたいのか事前に検討する。 ・個人所有のスマートフォンか組織貸与のスマートフォンかを区別する必要がある場合や、機種変更を把握したい場合は、最小限の情報を把握しておく（機種名等）。	6.3.1 節「デバイス情報を収集/監視する」

	・インターネット接続方法 ①Wi-Fi ルータ ②テザリング（ルータ機能） ③公衆 Wi-Fi ④携帯電話回線（データ通信回線）	・利用者の個人用途において、いつ、どこで、どのようなネットワークに接続するかは管理ができないと想定されるため、資産（業務データ等）は、必要（リスクの度合い）に応じて保護する。	5.6 節「ネットワークに接続する」
	・ハードウェアの交換	・外部記憶媒体（SD カードや SIM 等）は、交換されても確認が困難。利用する場合は、取り扱い方法やリスクについて説明をしておくことが望ましい。 ・デバイス本体の機種変更を行うと、その時点で機能が変化すると考えられるため、可能な限り把握しておくことが望ましい。	4.2 節「特性から見る脅威と対策」 4.3 節「将来における留意点」
情報	・業務データの取り扱い ①データを区分した上でデバイスに保管 ②組織が管理しているデータと同期 ③組織が管理しているデータを参照	・BYOD 終了時のデータ消去のために、プライベートと業務データの区分が重要。 ・紛失時、データ消去等を行う場合も利用者の理解を得ておくことが望ましい。 ・同じ用途の利用でも、個人用途と業務用途で別々のアプリケーションを利用すればデータは区分される。 ・必要（リスクの度合い）に応じてデータを保護する。	各項目の BYOD 欄
アプリケーション	・業務で利用させるアプリケーションの種類 ①デバイス標準搭載のアプリケーション ②マーケットから取得する無償アプリケーション ③マーケットから取得する有償アプリケーション ④社内開発アプリケーション	・管理者がアプリケーションの使い方に直接関与する必要がある場合は、社内開発アプリケーションまたは指定アプリケーションの新規導入が望ましい。 ・マーケットから取得するアプリケーションやデバイス標準のアプリケーションを利用する場合は、利用者がすでに該当するアプリケーションを個人用途として利用していないかどうか確認し、データの保管場所の分離について検討する（業務データは指定場所に保管する等）。 ・組織による一括購入ができないマーケットから取得する有償アプリケーションを利用する場合は、所有権について調査をしておく。	5.9 節「アプリケーションを利用する」
	・起動方法 ①ブラウザからの URL アクセス ②アイコンからのアプリケーション立ち上げ	・ブラウザを利用する場合、URL、アカウント情報、閲覧履歴等のキャッシュの扱いに注意する。 ・アプリケーションをアイコンから立ち上げて利用する場合、アプリケーションの動き（データ保存場所、データ公開範囲、アクセス許可情報等）を調べておく。	5.5 節「ブラウザを利用する」
	・外部サービスの運用方法（ブラウザを利用し、組織が契約した外部サービスへアクセスする場合）	・組織外の SaaS サービス利用を想定した場合、アクセス経路（通信手段）は管理ができないと想定される。 ・データ保管場所は SaaS 事業者側に依存し、クラウド上だけでなくデバイス内に同期されることもあるため、サービス内容を調べて利用可能範囲や対処方法を提示する。	5.8 節「組織契約の SaaS/ASP サービスを利用する」
マーケット	・業務で利用させるアプリケーションの入手方法	・業務用アプリケーションの入手先を指定する。 ・利用者の個人用途において、マーケットから各種アプリケーションを入手することは制限できないと想定されるため、信頼できるマーケットの利用促進や、導入してはいけないアプリケーション（ブラックリスト）の提示を行う。但し、強制はほぼ不可能。	5.9 節「アプリケーションを利用する」
組織（資産）側の接続	・資産にアクセスする手段 ①社内 Wi-Fi ②VPN(公衆 Wi-Fi、携帯電話回線等) ③通信事業者閉域網	・組織の資産が存在するシステムへのスマートフォンからのアクセス経路を調べ、必要（リスクの度合い）に応じて保護する。	5.7 節「社内ネットワークを利用する」

3.3. 利用者の意識とリテラシー

スマートフォンは既に個人所有率が高まっており、使い慣れたデバイスを業務で利用することで効率を上げたい、と考える人も少なくはありません。

そのため、個人所有のスマートフォンを安全に業務利用できるしくみを構築するか、ある一定の制限を課して運用するか、規定に則った利用を個人に委ねるか、あるいは業務での利用を禁止するか等、何らかの検討をする必要があります。

どのような場合でも組織は情報資産の保護に努める必要があり、安全性は利用者の意識に深く関係するため、BYOD を導入する際にはその特性をよく説明しておくことが重要です。結果的に、利用者のリテラシーも向上し組織も利用者も安心できる環境が実現します。

なお、個人所有のスマートフォンでは、利用者が個人的に SNS を利用することが増えているため、メディアリテラシーについての説明も添えておくことが推奨されます。

4. 管理者の心得

BYOD を検討する際は、目的を明確にしてから臨みましょう。

計画、導入時には、申請／承認／終了手続きの確立、各種規定（業務範囲や制限事項、表明保証、費用負担等）の整備と提示、リスクの洗い出しと受容範囲の想定等、組織貸与のスマートフォンとは異なったプロセスを踏む必要があります。組織貸与のスマートフォンがある場合は、その共存も念頭におきましょう。

BYOD の考え方は、災害など緊急事態の際に、一時的に個人所有のスマートフォンの利用を許可する場合にも役立ちます。

4.1. 申請／承認／終了手続き

トラブルを未然に防ぐために、業務範囲や労務管理基準、社内ルールなどの規定を明確にしておきましょう。また、BYOD として利用するスマートフォンの申請／承認、そして終了時の手続きは、利用者への意識付けのためにも大切です。

申請は、利用が許可された個人所有のスマートフォンと利用が許可されていないスマートフォンを区別する機会であると同時に、規定を提示し利用者と合意するために必要なプロセスとなります。BYOD 終了時の業務データ破棄についても、申請の段階で明確に規定し、合意しておく必要があります。

4.2. 規定における考慮点

利用が許可された個人所有のスマートフォンは、業務時間外でも利用者が望めば業務利用できる場合が多く、労働時間の管理が困難になります。また、夜間や休日でも持ち歩いていることが潜在的な前提となることから、業務外労働を強制してしまう危険性もあります。裁量労働制であってもそうでない場合も、労務管理と費用負担については業務内容に合わせて関係部門と協議しておく必要があります。

セキュリティ上の考慮点については、利用ガイドライン、および、その付録「特性別対策チェックシート」「利用シーン別対策チェックシート」「手順書に記載する項目の例」「誓約書に記載する項目の例　BYOD 版」を、合わせて参照してください。

4.3. 利用者のプライバシーへの配慮

組織が情報資産を管理し保護するように、利用者も、個人的な情報を守りたい、自分で管理をしたいと考えます。

BYOD 運用時に、利用者の個人的な情報、例えば個人の電話番号やメールアドレス、位置情報、メールの送受信履歴、インターネットの閲覧履歴、バックアップデータ等を取得する場合は、利用目的と取得範囲、管理方法を伝えましょう。これらはプライバシーに深く関わると考えられます。

組織としては、プライバシーに関わる情報の収集は極力避け、仮に利用者と合意の上で収集していたとしても、BYOD 終了時には速やかに消去するなどの配慮が必要です。

4.4. 戦略的なBYOD

BYOD 導入の目的は、効率化や費用削減、災害対策など様々で、対象機能も、電話のみの利用やコミュニケーションツールとしての導入など多様化しています。

BYOD 導入を決めた場合は、組織貸与のスマートフォンとは違う長所を活かし、ワークスタイル変革のために最大限活用しましょう。個人所有スマートフォンの方が高機能な場合もありますし、操作の教育が最小限で押さえられるかもしれません。大切に扱われることで、紛失や故障等のリスクが低下する可能性もあります。

一方、業務内容によっては、BYOD ゆえに過剰な管理やプロセスが発生する可能性があります。そのため、費用が嵩み、スマートフォンの自由度も損なわれ、結果として導入効果が現れないことも考えられます。

重要なことは、既に組織に持ち込まれている個人所有のスマートフォンは存在するということです。組織のセキュリティポリシーとの兼ね合いや費用等、様々な検討を行った上で最適な意思決定をしましょう。