DM5-04-111

スマートフォン・タブレット端末の使用手順

雛形

（官支給品編）

2012 年 4 月

内閣官房情報セキュリティセンター

１．本書の位置づけ

本書は、府省庁内外でスマートフォン及びタブレットを利用する場合の手順を作成する場合の雛形であり、記載すべき事項を、文書構成例の枠組みの中に盛り込んだものである。

２．本雛型の使用方法

本雛型書において想定する前提

本雛形は、以下を前提として記述している。

・行政業務の遂行において、府省庁外でスマートフォンやタブレットを使用している。

・ソフトウェア製品等は次のものを使用している。なお、機器は特定していない。

OS：Apple®　iOS、google®　android、Microsoft® Windows mobile
Research In Motion®　BlackBerry

インストールソフトウエア：

① ファイル暗号化ソフト
② ＶＰＮクライアント
③ ウイルス対策ソフト
④ 管理ツール(Mobile Device Management)

対象とする OS、使用する環境が上記と異なる場合や機器が実装する機能にあわせ、適宜、修正、追加又は削除する必要がある。

３．手直しポイント

「政府機関の情報セキュリティ対策のための統一管理基準」及び「政府機関の情報セキュリティ対策のための統一技術基準」（NISD-K304-111 及び NISD-K305-111）に基づき策定された省庁基準に準拠したスマートフォン及びタブレット関連の使用手順を作成する手順は、大別して、新規で作成するものと既存の文書を修正するものとがあるが、どちらの場合でも以下の事項を踏まえて作業を行う必要がある。

① 使用環境（使用する OS やアプリ等）やその前提（使用者へ管理者権限を付与しているか否か等）に応じて内容を変更する。
② 利用目的、用途及び扱う情報資産に応じて必要な管理策を決定する。（スマートフォン及びタブレットは端末の特性上、多様な利用形態があり、求められる管理策やセキュリティ水準が異なることに留意する）
③ 手順書中に明記される設定数値（パスワード文字数、容量等）については、府省庁内の定めに合わせる。
④ 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。

雛形に情報セキュリティ対策の観点以外の一般的な記述について不足がある場合には、適宜補う。

４．引用

各府省庁においてスマートフォン及びタブレット端末の使用手順を作成する際には、本手順に加えて、必要に応じて以下の情報を参考にしてもよい。

日本スマートフォンセキュリティフォーラム（JSSEC）
『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』
http://www.jssec.org/dl/guidelines2011_v1.0.pdf
※上記ガイドライン　付録 A に対策の推奨レベルが記載されている。

改訂履歴

改訂日	改訂理由
2012/4/26	初版

目次

1　本手順書の目的

行政事務を遂行するに当たっては、府省庁内外において相互連絡や情報処理を実施する必要が生ずる場合がある。この際、事務を遂行する環境や使用するネットワーク等、府省庁内においてPCから府省庁内ネットワークに接続する場合と比較して物理的な安全対策を講じることが困難になることが多い。

また、府省庁外での相互連絡や事務遂行に当たっては、情報システムセキュリティ管理者等の目が行き届かないことも多いため、府省庁外でのセキュリティの維持に関しては行政事務従事者各個人の行動や意識等への依存度が高くなる。

本書は、上記の状況を考慮し、府省庁内外におけるスマートフォン及びタブレットの使用に関する使用手順を提供することを目的とする。

なお、本書は、技術変化・進歩及び法制度の変更に対応し、常に意味あるものにするために、情報システムセキュリティ管理者の指導の下で見直しを行う必要がある。

2　本手順書の対象者

本書は、行政事務の遂行に当たり府省庁内外において官支給のスマートフォン及びタブレットを使用するすべての行政事務従事者と、官支給のスマートフォン及びタブレットを管理する情報システムセキュリティ責任者並びに情報システムセキュリティ管理者を対象とする。

※行政事務従事者とは、政府職員及びそれぞれの府省庁の指揮命令に服している者のうち、それぞれの府省庁の管理対象である情報及び情報システムを取り扱う者をいう。

3　本手順書の目的

官支給スマートフォン及びタブレットを使用する際には、全ての行政事務従事者は情報システムセキュリティ責任者又は情報システムセキュリティ管理者によって決められた方法及び認められた方法を遵守すること。

なお、情報システムセキュリティ管理者は、安全性と利便性の双方を考慮した上で、府省庁外におけるスマートフォン及びタブレットの接続や機能等に係る使用範囲を設定すること。

3.1 使用対象者

(1) 業務の都合等の理由により申請した者のうち、情報システムセキュリティ責任者（又は大臣官房情報システム課）がその必要性を許可した中央合同庁舎△号館在籍の○○省職員に限る。

(2) 申請をする者は、直前 1 年以内に情報セキュリティ対策の教育を受講した職員に限る。

3.2 使用端末

(1) 行政事務従事者が所属する府省庁から支給されたスマートフォン及びタブレット（以下、貸与端末）に限る。

(2) 貸与端末には、以下のものを含む。

- スマートフォンもしくはタブレット本体
- スマートフォンもしくはタブレット用充電器
- SIM カード（タブレット端末のうち、3G 回線を使用しない場合は対象外）
- 端末が利用する電子記録媒体

【手順書作成者への補足説明】

端末によっては、アプリケーションやデータの保存領域として microSD カード等の電子記録媒体の利用が必要となる場合がある。記録媒体に保存されたデータに対する暗号化、利用終了時のデータ消去、及び電子記録媒体の紛失や盗難もあわせて留意する必要がある。

3.3 使用機能

スマートフォン及びタブレットにおいて使用できるのは、以下の機能のみとする。また、機能に対しての管理事項及び遵守事項を各項目に示す。

3.3.1 電話

3G 回線や VoIP アプリケーション等により、府省庁内外ユーザと通話を行う機能

3.3.2 電子メール

府省庁内外のユーザと電子メールを送受信する機能

3.3.3 スケジュール

端末内もしくは府省庁内の掲示板等の機能により、使用者個人のスケジュールの備忘もしくは府省庁内におけるスケジュール情報の調整及び共有を行う機能

3.3.4　ブラウザ

インターネットに接続することにより、ホームページを閲覧等する機能

3.3.5　省内イントラネット（電子掲示板等）

VPN 接続により http://www.****.go.jp にアクセスし、情報の閲覧等を行う機能

＊ 貸出端末においては、標準ブラウザのホームページに設定されている。

3.3.6　組織契約の SaaS/ASP サービス

省内外が契約した外部の SaaS/ASP サービスベンダが提供するネットワーク上のサービスを使用する機能

3.3.7　アプリケーション

スマートフォン及びタブレット端末に対し、既存機能の利便性の向上や新規機能の付与を目的として提供されるプログラムであり、単体もしくは外部のサービスとの連携で機能を提供するもの

3.3.8　デバイス機能

端末の筐体に付随したハードウェア等が提供する機能

① カメラ：静止画もしくは動画を撮影し、保存する機能
② マイク：音声を録音し、保存する機能
③ 位置情報：使用者の位置情報を記録し、必要に応じて外部に公開する機能
④ 各種近距離通信機能：無線機能を使用し、近～中距離でデータの送受信を行う機能　※Bluetooth、赤外線通信、NFC 等が該当
⑤ ワンセグ：移動体向けの地上デジタル放送を受信する機能
⑥ 可搬媒体：データの可搬媒体として使用する機能

3.3.9　ファイルの使用

省内イントラネットにアクセスすることにより、イントラネット上にあるファイルの使用を行う機能

3.3.10　ファイルの作成

アプリケーションの機能によりファイルを作成する機能

※3.3.7 アプリケーションを参照のこと

3.3.11　ファイルの暗号化

貸出端末にインストールされているファイル暗号化ソフト等によりファイルを暗号化する機能

3.3.12　テザリング

端末が無線通信のルーター機能を実装することにより、他の端末による外部ネットワークの接続を行う機能

※テザリングを利用する場合、貸与端末がテザリングを行い、貸与端末以外にネットワークを提供する場合と、他の端末のテザリング機能を利用することで貸与端末がネットワークを利用する場合が存在する。

3.4 ネットワークへの接続

省庁内外へのネットワークに対する接続に際し、以下の接続形態が存在する。

① 3G 回線によるネットワーク接続
　電気通信事業者が提供する携帯電話の通信網に接続する。

② 無線 LAN（Wi-Fi）によるネットワーク接続
　省庁や事業者が提供するサービスに接続する。

③ その他無線機能による接続
　端末に実装された短距離無線通信により端末間の通信等を行う。

4　情報システムセキュリティ責任者及び情報システムセキュリティ管理者が実施すべき事項

4.1 基本設定の定義

以下の事項に対して、府省庁にて標準とする設定条件を定めること。

① 使用する端末の機種と OS
② ウイルス対策
③ 使用を許可するアプリケーション
④ バックアップの方式
⑤ 管理ツール(Mobile Device Management)
⑥ 暗号化機能

【手順書作成者への補足説明】

公開されたアプリケーションを使用する場合、アプリケーションの仕様変更等により必要な機能の使用が制限される、また、アプリケーションを経由して意図せず外部に情報が漏えいするリスクが存在する。

公開されたアプリケーションを使用する際には、使用開始前及びアプリケーションの仕様変更時にアプリケーションの挙動を調査した上でリスクを把握すること。

また、特に要機密情報を扱う場合には、専用に設計されたアプリケーションを使用することが望ましい。

ウイルス対策に関しては、OS の特性により重要度が異なる。利用の対象となる OS がマーケット及び OS の特性により、ウイルス対策の必要が低いとされる場合は、特段の対策は求めないが、OS に対する脆弱性の情報を適宜入手し、必要な場合は対策を行うことが望ましい。

また、管理ツール、暗号化機能は、利用する端末、OS、ソフトウェア等により提供される機能や範囲、暗号強度が異なるため、組織の要件にあわせて選択することが望ましい。

4.2 基本設定の定義

4.2.1 端末設定の基本方針

(1) 端末が搭載している機能及びアプリケーションを特定すること。

(2) 貸与する端末には、以下の機能を実装もしくは設定すること。

① 端末内及び外部記憶媒体のファイルデータ暗号化

② リモートワイプ（遠隔からのデータ消去機能）

③ アプリケーションの導入制限

④ 府省庁内ネットワーク接続時の端末認証及び使用者認証

⑤ 府省庁内ネットワーク接続時の経路暗号化

⑥ 不要な機能の停止

(3) 端末のセキュリティロックを設定すること。

(4) ウイルス等の対策を行うこと。必要な場合はアプリケーションをインストールし、必要な設定を行うこと。

(5) 原則、可搬媒体としての使用を認めないこと。

(6) カメラ機能が不要な場合は、機能を停止させるか、もしくはセキュリティシール等を行政事務従事者に配布し、貼付させる。

(7) 電子メールの送受信に対し暗号化、大容量ファイルの送受信手段及び機密情報の閲覧手段を設けること。

(8) メールの送受信記録を省庁内に保管すること。

(9) 各アプリケーションがアクセスする内部情報を確認し、不要な内部データへのアクセスを防ぐこと。
(10)監視対象情報を定めること。

【手順書作成者への補足説明】

上記の要件は利用する端末、OS、暗号化ソフトウェア等により提供される機能や範囲が異なるため、組織の要件にあわせて選択することが望ましい。端末固有の機能でセキュリティ機能が実装されない場合は、利用するネットワークにおける管理策を踏まえて総合的に対策を実施すること。

4.2.2 通話機能に対する設定

(1) VoIP の使用を許可する場合は、通信経路を暗号化すること。
(2) IP 電話による内線電話網を構築する場合は、IP PBX サーバの機器やサービスを正しく設定すること。また、IP PBX サーバにパスワードを設定する等、周囲の環境のセキュリティを強化すること。

【手順書作成者への補足説明】

IP 電話アプリケーションによっては、端末を構内の内線電話網用の端末として利用することが可能となるものがある。

一方でネットワーク上の盗聴や不正アクセスを考慮し、経路の暗号化等を実装する必要がある。暗号化を含めた VoIP の仕様は、提供される VoIP アプリケーションの仕様及び機器の設定による。

4.2.3 電子メール機能に対する設定

(1) メールの本文を暗号化する対策を講じること。
(2) 電子メールにファイルを添付する場合は、暗号化すること。
(3) メールサーバにデータを残す運用とし、原本を保存すること。

【手順書作成者への補足説明】

端末における電子メールアプリケーションの使用に際しては、メールデータの保管場所（端末やクラウドサービス等）や保管されたメールデータの暗号化に留意すること。メールデータが端末上に保管されていない場合でも、常時ネットワークに接続しているスマートフォン及びタブレットの場合、端末の認証機能を解除された場合、容易にメールデータにアクセスすることが可能となる。特に機密度の高い情報を扱う場合は、電子メールアプリケーション使用時に認証を要求する等、多段の認証を実装することが望ましい。

4.2.4　ブラウザ機能に対する設定

(1) 端末内にキャッシュが残らないように設定すること。
(2) Web フィルタリングの設定により各端末を保護すること。
(3) 行政事務に利用するブラウザアプリケーションを特定すること。

4.2.5　省内イントラネット（電子掲示板等）の利用に対する設定

(1) ユーザ認証を行うこと。
(2) アクセスログを取得すること。
(3) アクセス可能な掲示板や社内システムを制限すること。外部接続が可能な掲示板や社内システムは必要最低限のものとし、不要な情報の閲覧や外部からの接続を制限すること。

4.2.6　組織契約の SaaS/ASP サービスの利用に対する設定

(1) ユーザ認証を行うこと。可能であれば府省庁内の認証システムと連携させること。
(2) SaaS/ASP サービスベンダにアクセスログを取得すること。
(3) アクセス提供側がアクセス可能なネットワークは府省庁内を経由したアクセスに制限し、府省庁側からアクセスログを取得すること。
(4) 取得したアクセスログを定期的にモニタリングすること。

【手順書作成者への補足説明】

ネットワーク上のサービスを使用する場合、ブラウザ経由で使用する場合とアプリケーションを使用して接続する場合の二系統が考えられる。端末の使用に際しては、省庁内のネットワークを経由せず、使用が可能となるため、扱う情報の重要度に応じ、暗号化や二要素認証及び経路の制限を考慮することが望ましい。

4.2.7　データの格納領域の利用に対する設定

(1) 業務用のデータの格納領域を特定し、可能な限り、利用者に保存場所を選択させないようにすること。

【手順書作成者への補足説明】

アドレス帳、メールデータ、各種アプリケーションで利用するデータは、端末内、外部記憶媒体内、バックアップ用の端末内、クラウドサービスや省庁内のファイルサーバ等の端末外等、多様な場所に保管される場合がある。

特にクラウドサービス等と連携したサービスを利用する場合、公開範囲の設定不備等により、利用者の意図によらず情報漏えいが発生するリスクが存在する。

管理を行う上では、管理者が業務上利用するアプリケーションのデータの格納領域を特定し、利用者に許可の無い変更を許容しないこと、また、端末の紛失や端末の返却時に確実にデータを消去する手続きを設けることが必須となる。

4.2.8　各機能に対する設定

(1) 行政事務従事者が端末を使用する際の必要な手続き、遵守事項及び利用手順を示した手順書を作成すること。

(2) 各種機能（ブラウザ、アドレス帳、電子メール、スケジュール等）を使用する際には、定められたアプリケーションの使用を義務付けること。

(3) 電子メールにファイルを添付する場合は、ファイルを暗号化すること。

(4) 以下に示すデバイス機能は、業務上必要な場合を除いて、原則使用しないこと。

- カメラ
- マイク
- 位置情報
- 各種近距離通信機能
- ワンセグ
- テザリング

【手順書作成者への補足説明】

端末が提供する機能は、利用者の意図しない情報の開示や機能の悪用を予防するため、業務上の要件が必要な場合のみ利用を許可するものとする。

また、利用を許可する場合は、当該端末、機能及びアプリケーションに対する脆弱性情報、インシデント情報を適宜収集し、必要なセキュリティ対策を実施することが必須となる。

例えば、位置情報は地図利用時の経路案内や災害時の安否確認、端末紛失時の捜索に有効な機能である。一方、撮影された画像に位置情報が付与される等により、本人の意図によらず、外部に情報を漏えいされるリスクがある。

また、貸与端末にテザリングにより外部端末の接続を許可する場合、貸与端末がネットワーク接続の経路上に存在することで、当該端末の脆弱性に対する攻撃による情報の盗聴やネットワーク接続の中断の恐れがある。

4.2.9　通信経路の整備

(1) 各端末が府省庁内ネットワークにアクセスする場合、通信を暗号化すること。

4.3 貸与申請受付時の対応

4.3.1　申請の受付

(1) 行政事務従事者から提出された様式◇◇-1「スマートフォン及びタブレット端末貸出許可申請書」に必要事項が記入されていること、行政事務従事者が所属する課室長の承認があることを確認すること。
(2) 申請理由を確認し、申請の許可・不許可を判断すること。
(3) 申請を承認する場合は、必要な端末の貸出手配を行うこと。
(4) 行政事務従事者に貸し出す端末を特定した後に、管理台帳に必要事項（使用者氏名、所属、貸出日、使用期間、機種情報、端末情報、アプリケーション設定情報等）を記録すること。
(5) 承認可否の結果に関わらず、全ての端末貸与申請の記録を取得すること。

【手順書作成者への補足説明】

承認された試用期間中は、端末の管理は行政事務利用者の責任の下、行われる。利用期間中は包括的な端末の貸与となるため、都度の返却は求めないが、府省庁の必要に応じ、端末の利用状況の確認もしくは返却を指示することが出来る。

4.3.2　端末引き渡し時の遵守事項

(1) 手順書にて定められた必須の設定が完了していることを確認すること。
(2) 行政事務従事者に導入作業を指示する場合は手順を明示すること。
(3) 行政事務従事者から引き取り確認の署名を得ること。

4.4 貸与端末の管理

4.4.1　ネットワーク接続に対する制限

(1) 組織名や端末の機種を推測されにくい SSID を設定すること。
(2) 強度の高い暗号化方式を採用すること。
(3) ネットワーク接続時のパスワードを推測されにくい複雑なものを設定すること。もしくはより強度の高い認証方式を利用すること。
(4) 府省庁内でテザリング機能が使用されていないことを監視すること。
(5) 行政事務従事者が使用可能なアクセスポイントを明確にし、公開すること。

(6) 通信事業者による 3G 回線の通信規制が発生した場合に備えて、複数の通信経路を確保すること。
(7) 通信事業者において 3G 回線の回線障害が発生した場合に備えて、Wi-fi 接続への回避策を検討すること。

4.4.2 データのバックアップ

(1) 端末毎にバックアップを行う環境を特定すること。
(2) バックアップを行う環境においても、認証及び暗号化を行うことでセキュリティを維持すること。
(3) 情報の重要度に合わせ、バックアップの頻度を設定すること。

【手順書作成者への補足説明】

OS の機能等により端末内のデータをバックアップする機能が準備されている。

バックアップを行う場合は、扱う情報の重要度に合わせ、バックアップの対象、頻度及び方法を考慮することが望ましい。

4.4.3 監視

(1) 業務利用における監視対象情報を特定すること。
(2) 監視対象情報を定期的にモニタリングし、モニタリング結果を情報システムセキュリティ責任者に報告すること。
(3) 端末の使用状況を監視する担当者に対し、使用者のプライバシー情報の閲覧に対する制限を実施するとともに、閲覧ログを取得すること。

【手順書作成者への補足説明】

端末を監視する要件は扱う情報や利用目的に基づき決定する。ウイルス等の不正なプログラム導入の発見を目的とする場合、端末の不正な改造の有無、ファームウェアやプログラムのバージョン、許可のないアプリケーションの導入等を監視することが望ましい。

また、利用者の不正操作による情報の漏えい等を発見するためには、操作ログ等を取得することが要件となる。

ただし、監視により利用者のプライバシー侵害につながるおそれがあるため、収集する情報の利用を厳重に管理する必要がある。

4.4.4 更新情報の収集と展開

(1) 貸与端末のソフトウェア更新情報を入手すること。
(2) 利用しているアプリケーションの更新情報を入手すること。

(3) 端末への適用が可能だと判断でき、更新を適用する場合は、端末使用者に実施方法を通知すること。

4.5 端末返却時の対応

(1) 返却された端末本体の設定や付属品の不足有無を管理台帳と照合の上、返却の記録を残すこと。
(2) 返却された端末内の情報を完全に消去すること。
(3) 返却された端末のバックアプデータの消去要否を使用者である行政事務従事者に確認し、必要に応じて消去すること。(他端末にてデータを継続使用する場合は、この限りではない。)

5 行政事務従事者が実施すべき事項

5.1 貸与にかかる手続き

5.1.1 申請手続き

(1) 事前に所属する課室長の承認を得た上で、使用開始■日前までに、様式◇◇-1「スマートフォン及びタブレット端末貸出許可申請書」により情報システムセキュリティ責任者（又は大臣官房情報システム課）に申請すること。
(2) 申請書類には、以下の事項を漏れなく記載すること。
    ① 申請日
    ② 申請者の情報（氏名、所属、連絡先）
    ③ 申請理由
    ④ 使用目的
    ⑤ 使用期間
    ⑥ 必要な機能、希望する端末モデル等
(3) 申請書類を提出する際に、端末の貸与が必要な理由を確認できる書類（写し）を提出すること。

【手順書作成者への補足説明】

承認された使用期間中は、端末の管理は行政事務利用者の責任の下で行われる。

5.1.2　貸与端末受け取り時の遵守事項

(1) 同梱されている一覧表「スマートフォン及びタブレット端末貸出一式チェックリスト」と実際に受け取った内容物が一致していることを確認すること。
(2) 貸与端末のセキュリティロックパスワードを、初期パスワードからパスワード設定ルールに準じた任意のパスワードへ即時変更すること。
(3) 必要な機能やアプリケーションが使用可能な状態にあることを確認すること。
(4) 端末内に不明なデータ等がないことを確認すること。
(5) ウイルス対策アプリケーションの自動更新機能を設定すること。

5.2 貸与端末使用中の管理

5.2.1　端末の変更に際しての遵守事項

(1) 許可された機能及びアプリケーションのみを使用すること。
(2) OS の改造行為（管理権限の奪取等）を行わないこと。
(3) 情報システムセキュリティ責任者もしくは情報システムセキュリティ管理者から、ソフトウェアの更新等、対応の指示があった場合は、指示に従って適切に対応すること。

【手順書作成者への補足説明】

OS の不正な改造や許可のないアプリケーションの導入により、情報の漏えい、ウイルス感染リスクが高まるため、省庁の許可の無い OS、アプリケーションの導入を禁止する。

5.2.2　端末の利用に際しての遵守事項

(1) 通話を行う場合は、業務上必要な通話のみに限定すること。
(2) 行政事務の遂行の目的以外で、サイトにアクセスし、ホームページ等を閲覧しないこと。
(3) 許可のない場所でカメラ機能やマイク機能を使用しないこと。
(4) 不用意に位置情報機能を使用しないこと。
(5) 不用意に近距離通信機能を使用しないこと。
(6) 個人で別途契約しているプロバイダ、メールアドレス等を使用しないこと
(7) 原則、就業時間中にワンセグを視聴しないこと。ただし、業務上必要な場合や緊急時等の場合は、この限りではない。

【手順書作成者への補足説明】

位置情報や近距離通信機能等の端末の機能を不用意に利用可能な状態にしている場合、本人の意図によらず、情報の開示が行われる恐れがあるため、行政事務の遂行に不要な機能は原則として停止し、利用しないこと。

5.2.3　電子メール使用時の遵守事項

(1) 電子メールの送受信を行った際には、不要なメールを速やかに削除すること。
(2) 電子メールで機密性 3 情報を移送する場合には、課室情報セキュリティ責任者の許可を得ること。
(3) 電子メールで機密性 2 情報を移送する場合には、課室情報セキュリティ責任者に届け出ること。
(4) 電子メールで要機密情報を移送する場合には、ファイルの暗号化等安全確保の対策を講ずること。
(5) 許可された電子メール用アプリケーションを使用し、設定を変更しないこと。

5.2.4　ファイルの作成及び保守時の遵守事項

(1) 行政事務の遂行の目的以外でファイルを作成しないこと。
(2) 機密性、完全性、可用性に応じて格付け及び必要性がある場合には、作成した情報に取扱制限を定めること。
(3) 格付け及び取扱制限は、その情報を参照する者が認識できる方法で明示すること。
(4) スマートフォン及びタブレット端末内（SD カードを含む）にファイルを保存する場合は、許可された領域に保存すること。
(5) 原則、可搬媒体として使用しないこと。

【手順書作成者への補足説明】

安易に可搬媒体として端末を利用した場合、端末自体がウイルスに感染する、端末が PC のウイルスの媒介となる、持出しの頻度が高いため紛失が発生する可能性が高くなる等の恐れがある。

5.2.5　ネットワーク接続時の遵守事項

(1) 手順書に従って、定められた手順・範囲に従ってネットワークに接続すること。
(2) 公衆無線 LAN サービスを使用する場合 は、府省庁が許可したサービスを使用すること。

【手順書作成者への補足説明】

公衆無線 LAN の利用に際しては情報漏えい等の脅威が考えられるため、府省庁が契約している回線事業者が提供しているサービスや宿泊先等が宿泊客のみに提供しているサービス等、事業者に対する信頼を確保出来ることを前提に利用可能なサービスを限定し、利用者に提示することが望ましい。

ただし、情報漏えい等に対する対応として、府省庁への接続に関しては VPN により経路を暗号化する等の対策が必要となる。

5.2.6　ウイルスチェック

(1) 情報システムセキュリティ管理者の指示に従って、貸与端末のスキャンを実施すること。

(2) アプリケーション更新時及びフルスキャン実施時に問題が発生した場合は、通信機能を切断した上で、速やかに情報システムセキュリティ管理者に報告すること。

【手順書作成者への補足説明】

スマートフォン・タブレット端末に対するウイルスの感染経路は主にアプリケーション導入時となる。業者による審査等により、不正なプログラムが混入されたアプリケーションを発見するマーケットの仕組みを備える等、通常の利用環境ではウイルスの混入自体が困難な場合がある。利用の対象となる OS がマーケット及び OS の特性により、ウイルス対策の必要が低いとされる場合は、特段の対策は求めないが、OS に対する脆弱性の情報を適宜入手し、必要な場合は対策を行うことが望ましい。

5.2.7　アプリケーションの導入及びアップデート

アプリケーションの導入に関し、府省庁の指示がある場合には指示に従うこと。

(1) 府省庁が導入を禁止しているアプリケーションは導入を行わないこと。

(2) 行政事務に利用するアプリケーションのアップデートは、府省庁の指示に従うこと。

5.2.8　盗難・紛失・情報漏えい等への対策

(1) 手順書に定めた手段・ルールに従って、端末のセキュリティロックを設定すること。

(2) 府省庁内及び府省庁外において、要保護情報を放置したり、必要以上に複製又は配布したりしないこと。

(3) 公共交通機関等での移動時や屋外での利用時における盗難防止、置き忘れに留意し、端末を常に携帯するか、目の届くところに置くこと。

(4) 端末本体又は付属品等の紛失が判明した場合、直ちに情報システムセキュリティ管理者に紛失した状況等を報告の上、その後の対応に関する指示を受けること。
(5) ウイルスに感染したことが判明した場合、直ちに電源を切り、バッテリーパックを外した上で、情報システムセキュリティ管理者に連絡・相談し、アドレス帳登録者への連絡等も含めて指示を受けること。
(6) 「電源が入らない。」「充電できない。」「ネットワークに接続できない。」という場合は、行政事務従事者は情報システムセキュリティ管理者に問い合わせ、その後の対応の指示を受けること。
(7) 端末利用に際し、作成した情報の意図しない外部公開や情報漏えいを発見した場合、情報システムセキュリティ管理者に連絡・相談し、アドレス帳登録者への連絡等も含めて指示を受けること。

5.2.9 盗み見等に対する対策

(1) 盗み見等に対する対策
(2) 貸与端末のセキュリティロックを設定すること。
(3) セキュリティロックのパスワードを入力する際には、周囲に配慮すること
(4) 機密性の高い情報を閲覧する際には、周囲に配慮すること。

5.2.10 その他

(1) 問題があると思われる場合には、その状況を情報システムセキュリティ管理者に報告し、指示を受けること。

5.3 貸与端末の返却

(1) 「スマートフォン及びタブレット端末貸出一式チェックリスト」を用いて、貸与物が全て揃っていることを確認の上、情報システムセキュリティ責任者もしくは情報システムセキュリティ管理者に返却すること。
(2) 貸与端末を返却する際には、使用期間中に端末内に保存した各種データ（アドレス帳、電子メール、画像、メモ等）を全て削除すること。
(3) 貸与端末に設定したセキュリティロック解除用パスワードを初期パスワードに設定すること。

6 災害時の対応等

6.1 災害時の使用に向けた整備

(1) 災害時に行政事務従事者が使用可能な機能を特定すること。なお、以下の機能は緊急時に有効な機能と考えられる。

① ワンセグ

② 電子メール

③ TV 電話

④ 位置情報

⑤ ソーシャルメディア

⑥ 災害伝言版等の安否確認サービス

(2) 緊急時に使用可能な機能を行政事務従事者に教育すること。

(3) 災害時等における注意事項を行政事務従事者に教育すること。

① フィッシング

② 風評の流布

【手順書作成者への補足説明】

安否確認、情報連絡、情報収集及び在宅勤務用端末としての利用等はスマートフォン及びタブレット端末に期待される災害時の活用方法である。

緊急時に有効な機能には、通常利用時に許可を推奨しない機能も含まれる。また、通信の途絶等、利用許可の指示を伝達することが困難な状況も想定される。特定の状況下では自動的にセキュリティポリシーを緩和し上記機能の利用を許容するよう事業継続計画に定義することが望ましい。

【手順書利用者への補足説明】

災害発生時には災害伝言版等を活用し、自身の安否を家族や関係者等に連絡するとともに、ソーシャルメディア等を活用することで様々な情報を入手することが可能となる。

一方、情報の波及する速度が速いソーシャルメディアの特性により、デマや風評が急速に広がることや、混乱に乗じたウイルス等の拡散、フィッシングサイトの出現も懸念される。

利用者自身がデマやウイルス等の拡散を行わないこと、また、安易にソーシャルメディアの書き込みを経由して外部サイトへのアクセスを行わないよう留意する必要がある。

6.2 災害時の使用

発生した状況に応じ、生命の安全、業務遂行上の必要を判断した上で機能を利用すること。ただし、バッテリーの消費等を考慮し、必要最低限の利用に留めること。

【手順書作成者への補足説明】

地震等の広域災害の発生時には、必要な情報を入手するための有用な端末であり、生命の安全や情報の入手のために必要とされる機能を使用することは妨げない。

また、府省庁の指示に基づく安否確認や情報連絡、在宅勤務用の端末としての活用も期待される。

一方、停電等の事情により電源の確保が困難となることも予想されるため、予備電源を日頃から携行する、もしくは、災害時には利用する時間を定め（1時間毎に利用する等）、電源の消費を抑えること等も必要となる。

7　紛失時の対応等

(1) 端末を紛失した、もしくはその恐れがある場合、速やかに情報システムセキュリティ担当者に連絡すること。

(2) 定められた手続きにより、端末の利用を制限し、必要な場合は遠隔より端末のデータを消去すること。

(3) 利用者本人による端末内のデータ消去が行われない場合は、情報システムセキュリティ担当者が端末のデータを遠隔より消去すること。

【手順書作成者への補足説明】

紛失時のセキュリティ対策として、位置情報による端末の所在地の特定、遠隔からの端末の利用制限及びデータの遠隔消去等が挙げられる。

端末を紛失した、もしくはその恐れがある場合は、可能な限り、位置情報に基づき端末の所在を確認し、不正な利用が行われている可能性があるかを確認するとともに、必要な際には速やかに端末内のデータを消去することが望ましい。

以上

付録 A ※2011 年 12 月 1 日 JSSEC 作成「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」より引用

A-1 特性別 対策チェックシート

推奨レベル：■強く推奨　□推奨

章番号	分類	脅威	対策　または　要件	推奨レベル
4.2	特性から見る脅威	デバイスの盗難、紛失	・デバイスをロック設定する。 ・ロック解除失敗時に強制的にデータを消去する。 ・本体および外部記憶媒体のデータ領域を暗号化する。 ・ユーザ ID やパスワードを非保存設定にする。 ・定期的にデータのバックアップをとる。	■ ■ □ □ □
		SIM カードの盗難	・　通信事業者へ連絡し回線利用を停止する。	■
		水没や落下による故障	・定期的にデータのバックアップをとる。 ・落下防止用ストラップ等を装着する。 ・防水や耐衝撃性の高いデバイスを選択する。	□ □ □
		覗き見	・覗き見防止シート等を装着する。	□
		誤認識	・慎重に操作するよう注意を喚起する。 （静電容量方式を採用したパネルが多いため、静電気の影響を受けやすい）	□
		脆弱性	・デバイスや OS の種類を絞り込む、または統一する。	□
		信頼できないマーケット	・信頼できるマーケットからアプリケーションを入手する。 ・アプリケーションのインストール時に不用意にアクセス許可をしない。 ・アプリケーションに関する最新情報（不正な動き、意図しない動き、信頼できる情報等）を入手する。 （5.9 節「アプリケーションを利用する」参照）	■ □ □
		利用者による改造	・改造を禁止する。	■

A-2 利用シーン別 対策チェックシート

推奨レベル：■強く推奨　□推奨　－対象外

章番号	分類	脅威	対策　または　要件	推奨レベル
5.1	アドレス帳を利用する	誤操作 知識不足	・手順書を作成する。（付録参照） ・アプリケーションの動き（データ保存場所、データの公開範囲等）を調べる。 ・業務専用の保存場所を決める。 ・利用者には保存場所を選択させないようにする。	－ □ □ □
		プライベートデータの混在 【BYOD】	・誓約書にサインさせる。（付録参照） ・データを区分する（プライベートと業務の保存場所の区分）。 ・退職時、利用終了時には全ての業務データの保存場所に対し、データを削除したことを明示させる。	－ □ ■
5.2	電話を利用する	盗聴	・VoIP を利用する際には、通信経路を暗号化する。	□
		不正利用	・IP PBX サーバの機器やサービスを正しく設定する。	□
		不正アクセス	・IP PBX サーバにパスワードを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	・手順書を作成する。（付録参照） ・通話履歴を取得する。	－ □
5.3	メールを利用する	不正利用	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・Web メールなどデバイスにデータを残さないメールを使う。 ・本文や添付ファイルを暗号化する。	－ － □ □
		誤操作	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・ファイルの添付は禁止し、別手段を用意する。 ・本文や添付ファイルを暗号化する。 ・サーバにデータを残して原本を保存する。	－ － □ □ □
		プライベートメールの混在 【BYOD】	・誓約書にサインさせる。（付録参照） ・データを区分する（プライベートと業務のアプリケーションの使い分け等）。 ・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	誤操作、 知識不足	・手順書を作成する。（付録参照） ・アプリケーションの動き（データ保存場所、データの公開範囲等）を調べる。 ・データそのものの業務専用の基本保存場所を決める。 ・利用者には保存場所を選択させないようにする。	－ □ □ □
		私的利用 【BYOD】	・誓約書にサインさせる。（付録参照） ・データを区分する（プライベートと業務のアプリケーションの使い分け、アカウントの使い分け等） ・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	不正利用	・手順書を作成する。（付録参照） ・キャッシュを残さない。 ・Web フィルタリングで保護する。	－ □ □
		盗聴	・社内へのアクセスの場合は、通信を暗号化する。	■
		マルウェア	・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）	・手順書を作成する。（付録参照） ・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）。 ・データ（アカウント情報、閲覧履歴等）を区分する（プライベートと業務のアプリケーションの使い分け等）。	－ □ □ □
		フィッシング	・手順書を作成する。（付録参照） ・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 Wi-Fi ルータテザリング(ルータ機能)	不正アクセス	・組織名や機種を推測されにくい 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。	■ □
	ネットワークに接続する 公衆 Wi-Fi	盗聴	・信頼できるサービスを利用し、 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を制限する。	■ □
	ネットワークに接続する 携帯電話回線	通信事業者による通信規制	・通信事業者による通信規制が発生した場合を想定して、複数の通信経路を用意する。	□
		通信事業者の回線障害	・Wi-Fi 接続への回避を検討しておく。	□
		不正利用	・誓約書にサインさせる。（付録参照）	－
5.7	社内ネットワークを利用する 社内 Wi-Fi ネットワーク	なりすまし（利用者）	・ユーザ認証を行う。（Wi-Fi の場合、デバイス認証とユーザ認証は同時に利用できないので、脅威の優先度によって使い分ける。ユーザ認証のみの場合は、無許可デバイスからのアクセスを防止することができなくなる） ・アクセスログを取得する。	■ □
		なりすまし（デバイス）	・デバイス認証を行う。 （Wi-Fi の場合、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） ・アクセスログを取得する。	■ □
		盗聴	・通信を暗号化する。 ・通信の暗号化を強化する。 ・重要なデータを保護する（暗号化、パスワード等）。	■ □ □
		不正利用	・アクセスログを取得する。	□
		不正アクセス	・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等） ・アクセスログを取得する。	■ □
	社内ネットワークを利用する VPN (携帯電話回線や公衆 Wi-Fi など)	なりすまし（利用者）	・ユーザ認証を行う。 ・アクセスログを取得する。	■ □
		なりすまし（デバイス）	・デバイス認証を行う。 ・アクセスログを取得する。	■ □
		機器障害	・冗長化する。 ・代替手段を確保する。	□ □
		脆弱性に対する攻撃	・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。 ・アクセスログを取得する。	□ □

	社内ネットワークを利用する 通信事業者閉域網	通信事業者による通信規制	・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。	□ □
		通信事業者の回線障害		
5.8	組織契約の SaaS/ASP サービスを利用する 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	・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。	□ □
		なりすまし	・社内の認証システムと連携させる。 ・アクセスログを確認する。	□ □
5.9	アプリケーションを利用する	誤操作 知識不足	・手順書を作成する。（付録参照） ・アプリケーションの動き（データ保存場所、データの公開範囲等）を調べる。 ・業務専用の保存場所を決める。 ・利用者には保存場所を選択させないようにする。	－ □ □ □
		盗聴	・社内へのアクセスの場合は、通信を暗号化する。	■
		マルウェア	・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。 ・組織で許可するアプリケーションを決める。 ・アプリケーションのインストール時に不用意にアクセス許可をしない。 ・アプリケーションに関する最新情報（不正な動き、意図しない動き、信頼できる情報等）を入手する。	■ □ □ □
		私的利用	・業務時の利用を制限する。	□
		私的利用（不適切コンテンツ）	・手順書を作成する。（付録参照） ・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】	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・データを区分する（プライベートと業務で同じアプリケーションを遣う場合）。 ・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	カメラを利用する	不正利用	・セキュリティシール等を貼付し、利用しない。 ・カメラ機能を無効化する。	□ □
		誤操作、知識不足	・手順書を作成する。（付録参照）	－
		誤操作	・ セキュリティシール等を貼付し、利用しない。 ・ カメラ機能を無効化する。	□ □
		知識不足 フィッシング	・手順書を作成する。（付録参照）	－
		マルウェア	・アプリケーションのインストール時に不用意にアクセス許可をしない。 ・カメラ機能を無効化する。	□ □
		撮影情報の漏洩	・撮影時に位置情報機能を停止する。 ・撮影画像を外部に公開する際には、Exif（Information、プロパティ、属性情報）を削除する。	□ □
		プライベートデータの混在 【BYOD】	・誓約書にサインさせる。（付録参照） ・指定保存場所へ業務用データを移動する（デバイス内からの速やかな削除）。 ・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。	－ □ ■
	マイクを利用する	知識不足 誤操作、知識不足	・手順書を作成する。（付録参照）	－
		マルウェア	・アプリケーションのインストール時に不用意にアクセス許可をしない。	□

		プライベートデータの混在【BYOD】	・誓約書にサインさせる。（付録参照） ・指定保存場所へ業務用データを移動する（デバイス内からの速やかな削除）。 ・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。	－ □ ■
	位置情報を利用する	誤操作、知識不足	・手順書を作成する。（付録参照）	－
		詐取	・不要であれば位置情報機能を停止する。	□
		マルウェア	・アプリケーションのインストール時に不用意にアクセス許可をしない。	□
	NFC を利用する	スキミング	・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。	□ □
		なりすまし	・手順書を作成する。（付録参照） ・ロック機能を有効にする。	－ □
	ワンセグを利用する	私的利用	・業務時の利用を制限する。	□
	Bluetooth を利用する	マルウェア 不正アクセス	・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	・手順書を作成する。（付録参照） ・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	・Bluetooth を利用するアプリケーションを調べる。	□
	赤外線通信を利用する	誤操作 知識不足	・手順書を作成する。（付録参照）	－
5.11	データの可搬媒体として利用する	盗難・紛失および故障（外部記憶媒体）	・手順書を作成する。（付録参照） ・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	・手順書を作成する。（付録参照） ・組織から外部記憶媒体を貸与する。 ・データを暗号化する。 ・セキュリティシールを貼付する。	－ □ □ □
		プライベートデータの混在【BYOD】	・誓約書にサインさせる。（付録参照） ・利用を禁止する。 ・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。	－ ■ ■
5.12	バックアップを取る／同期する	誤操作 知識不足	・手順書を作成する。（付録参照） ・アプリケーションの動き（データ保存場所等）を調べる。 ・バックアップツールを導入する。	－ □ □
		バックアップデータにおける業務データの混在【BYOD】	・誓約書にサインさせる。（付録参照） ・私的な保存場所（私有 PC やクラウド、外部記憶媒体等）では、バックアップデータを保護する。 ・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）。	－ ■ □

A-3 手順書に記載する項目の例

章番号	利用シーン	重要ポイント
5.1	アドレス帳を利用する	・データ保存場所の選択（デバイス、クラウド、外部記憶媒体）安全性 ・データの公開範囲の指定、同期 ・【BYOD 時の追加項目】データの区分（プライベートと業務の保存場所の区分）
5.2	電話を利用する	・業務時間中の利用に対するマナー等の注意喚起
5.3	メールを利用する	・メールの転送禁止、ファイル添付、同期等のルール遵守 ・誤送信に対する注意喚起（送信前に送信先や添付の有無を確認） ・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 ・【BYOD 時の追加項目】データの区分（プライベートと業務のアプリケーションの使い分け等）
5.4	スケジュールを利用する	・データの公開範囲の指定 ・関係者以外に容易に分からないような情報の符号化（広く公開する場合） ・【BYOD 時の追加項目】データの区分（プライベートと業務のアプリケーションの使い分け、アカウントの使い分け等）
5.5	ブラウザを利用する	・ユーザ ID やパスワードの非保存設定（キャッシュ） ・インターネットアクセスに対する注意喚起(組織の許可していないサイトへのアクセス) ・正しい URL かどうかの確認、安易な短縮 URL への接続 ・【BYOD 時の追加項目】データ（アカウント情報、閲覧履歴等）の区分（プライベートと業務のアプリケーションの使い分け等）
5.6	ネットワークに接続する	・テザリングの利用制限
5.9	アプリケーションを利用する	・導入（ダウンロードとインストール）時の注意喚起（信頼できるマーケットの利用等） ・利用時の注意喚起（データの保存場所、公開時の影響範囲等） ・利用上のマナーとルールの明示(公序良俗の判断) ・【BYOD 時の追加項目】データの区分（プライベートと業務で同じアプリケーションを遣う場合）
5.10	カメラを利用する	・利用範囲の明示 ・データ保存場所の選択（デバイス、クラウド、外部記憶媒体） ・肖像権等への注意喚起 ・バーコード読み取り接続後に表示される URL の確認 ・【BYOD 時の追加項目】指定保存場所への業務用データの移動（デバイス内からの速やかな削除）
	マイクを利用する	・利用範囲の明示 ・データ保存場所の選択（デバイス、クラウド、外部記憶媒体） ・著作権等への注意喚起 ・【BYOD 時の追加項目】指定保存場所への業務用データの移動（デバイス内からの速やかな削除）
	位置情報を利用する	・利用範囲の明示 ・位置情報が外部に公開される場合があることの注意喚起 ・組織ポリシーに従った位置情報取得
	NFC を利用する	・盗難・紛失時の連絡方法、対応方法 ・故障時（入退管理や決済時に利用時）の代替手順の明示
	ワンセグを利用する	・利用範囲の明示（災害時等）
	Bluetooth を利用する	・利用範囲の明示 ・情報の授受に対する注意喚起（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）
	赤外線通信を利用する	・利用範囲の明示 ・情報の授受に対する注意喚起
5.11	可搬媒体として利用する	・利用可否の明示（利用禁止の推奨）
5.12	バックアップを取る／同期する	・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（組織が許可した同期先やバックアップ先の利用） ・【BYOD 時の追加項目】私的な保存場所（私有 PC やクラウド、外部記憶媒体等）でのバックアップデータの保護

A-4 誓約書に記載する項目の例

A-4-1 法人所有版

推奨レベル：■強く推奨　□推奨

分類	項目	解説（ねらい）	誓約書作成上の注意事項	推奨レベル
利用目的の明示	利用目的と範囲の明確化	スマートフォンの利用目的､利用範囲などを明記し組織の定めたルールの順守を確認する。		■
管理	組織による情報収集に対する個人の承諾（情報収集、監視などを行う場合）	不正な利用防止やマルウェア被害防止などから､スマートフォンの利用状況の収集を行うことを合意する。	スマートフォンは常時携帯するため、位置情報などを取得する場合には、「プライバシーの侵害」に注意して文章を作成する。 システム的な情報収集および、管理者による情報確認、どちらも含む。	■
	組織による制御に対する個人の承諾（制御、OS のアップデートなどを行う場合）	設定変更､機能制限やデータ削除を組織として行うことを合意する。	OS やアプリケーションのアップデートは、組織が管理する。 システム的な制御および、管理者による設定変更、利用者への設定指示なども含む。	■
	バックアップデータの保護	機密情報などの保護のため、個人所有 PC へのバックアップの禁止などを合意する。		□
届け出	特定の事象が発生した場合の届け出	紛失や盗難などが発生した場合､機密情報や個人情報の保管有無や､事故の影響を確認するため､直ちに届け出ることを合意する。	組織の定めたルールに従って届け出をする。 例：「破損」「故障」「不具合」「盗難」「紛失」など	■
禁止事項	端末、OS、アプリケーションの改造	セキュリティ上の脅威を抑止するため、改造しないことを合意する。		■
	端末メーカー、通信事業者の利用規約に対する違反行為	提供元の意図に反する利用は行わないことを合意する。		□
	組織の許可しないアプリケーションの導入	マルウェアなどの侵入を防ぐため､許可されたアプリケーション以外を導入しないことを合意する。	導入して良いアプリケーション（ホワイトリスト）又は、導入してはいけないアプリケーション（ブラックリスト）などを別途定める。	□
	私的利用	コストの増加や業務生産性低下､情報漏えいなどを防ぐため､私的利用しないことを合意する。		□
	第三者への貸与、譲渡、販売	本人以外の利用を禁止することを合意する。		□
	故意または過失による情報漏えい	データを持ち歩くことや個人の発信機会が増えるため、注意を喚起する。情報漏洩時には､企業ポリシーに従い対処する。	企業情報書き込み等への制限、不用意な情報拡散及び漏洩に十分注意する旨を明記する。	□
利用の終了	端末の返却	情報の削除､端末の回収を実施することを合意する。	データのバックアップ取り扱い、返却のルールは別途手順とする。	■
誓約への違反	罰則規定	組織の定めた罰則規定の適用対象となることを明示する。		□

A-4-2 BYOD 版

推奨レベル：■強く推奨　□推奨

分類	項目	解説（ねらい）	誓約書作成上の注意事項	推奨レベル
表明保証	名義、契約者	契約者が利用を許可する本人であることを表明させる。	許可条件を明確にする。	■
利用目的の明示	利用目的と範囲の明確化	スマートフォンの利用目的、利用範囲などを明記し組織の定めたルールの順守を確認する。		■
管理	組織による情報収集に対する個人の承諾（情報収集、監視などを行う場合）	不正な利用防止やマルウェア被害防止などから、スマートフォンの利用状況の収集を行うことを合意する。	スマートフォンは常時携帯するため、位置情報などを取得する場合には、プライバシーの侵害に注意して文章を作成する。 システム的な情報収集および、管理者による情報確認、どちらも含む。	□
	組織による制御に対する個人の承諾（制御、OS のアップデートなどを行う場合）	設定変更、機能制限やデータ削除を組織として行うことを合意する。	OS やアプリケーションの推奨構成を提示する。 事故対応時の対処については明記しておく。	□
	バックアップデータの保護	業務データがスマートフォン内に保存されている場合、個人所有 PC へのバックアップデータの厳格な管理を促す。		□
届け出	特定の事象が発生した場合の届け出	紛失や盗難などが発生した場合、機密情報や個人情報の保管有無や、事故の影響を確認するため、直ちに届け出ることを合意する。	組織の定めたルールに従って届け出をする。 例：「不具合」「盗難」「紛失」「修理」「機種変更」「譲渡」「販売」	■
禁止事項	端末、OS、アプリケーションの改造	セキュリティ上の脅威を抑止するため、改造しないことを合意する。		■
	組織が禁止指定しているアプリケーションの導入	マルウェアなどの侵入を防ぐため、禁止指定されているアプリケーションの導入を禁止する。	導入してはいけないアプリケーション（ブラックリスト）などを別途定める。	□
	第三者への貸与	本人以外の利用を禁止することを合意する。		□
	申請端末以外の利用	業務に利用すると表明した端末以外は利用させない。		■
	故意または過失による情報漏えい	データを持ち歩くことや個人の発信機会が増えるため、注意を喚起する。情報漏洩時には、企業ポリシーに従い対処する。	企業情報書き込み等への制限、不用意な情報拡散及び漏洩に十分注意する旨を明記する。	□
利用の終了	業務データ、アプリケーションの削除	セキュリティ上の脅威を抑止するため、業務データ、アプリケーションを削除させる。		■
誓約への違反	罰則規定	組織の定めた罰則規定の適用対象となることを明示する。		□