資料３－５

スマートフォン等の業務利用における
情報セキュリティ対策の実施手順策定手引書

2015 年　5 月 21 日
内閣サイバーセキュリティセンター

改訂日	改訂理由	備考
2015/ 5/21	初版	

目　次

1. 総則

1.1 本書の目的・位置付け

本書は、スマートフォン等を府省庁の業務に利用する場合に関して、「政府機関の情報セキュリティ対策のための統一基準」（以下「政府機関統一基準」という。）に準拠した情報セキュリティ対策の実施手順を定める際の、要件の策定の考え方や対策例等を整理したものである。

本書においては、スマートフォン等の利用形態として、モバイル端末として庁舎外で利用する形態を前提としている。また、府省庁が支給する端末の利用を基本としながら、職員の私物端末を公務に利用する場合についても考慮している。

なお、政府機関統一基準の遵守事項及び「府省庁対策基準策定のためのガイドライン」の基本対策事項と本書の規定内容の関係について別紙１に示すので、実施手順策定の際に参考にされたい。

1.2 本書が対象とする者

本書が対象とする者は、以下のとおりである。

- スマートフォン等を業務利用する組織において安全管理措置に係る手順を策定する統括情報セキュリティ責任者及びその命を受けて実施手順の策定業務に携わる行政事務従事者。
- スマートフォン等の安全管理措置の実施状況を管理する責任者（情報セキュリティ責任者、課室情報セキュリティ責任者）及びその命を受けて管理業務に携わる行政事務従事者。
- スマートフォン等の接続先となる情報システム（例えば、府省庁 LAN）の情報システムセキュリティ責任者及びその命を受けて管理業務に携わる行政事務従事者。

1.3 本書の使い方

府省庁においてスマートフォン等の業務利用を検討する際の留意事項を以下に示す。また、検討の流れを概念的に示したものを図１－１に示す。

- 業務形態等の検討に入る前に、まず２章に示すスマートフォン等の特性とリスクについて理解し、その上で自府省庁の業務利用形態について、３章に示す例を参考に方向性を整理する。さらに、４章に示す内容に従い、府省庁における業務利用の目的及び適用範囲を暫定的に定める。この時点で、職員の私物端末を適用範囲に含めるかどうかについても、併せて整理する。
- 次に、２章に示すスマートフォン等の特性、組織や取り扱う情報の特性、利用形態等を考慮してリスク評価を行い、その結果を踏まえて、自府省庁におけるスマートフォン等の業務利用形態及び適用範囲を見直す。
- 最後に、５章に示す内容に従い、情報セキュリティ対策の要件を定める。また、６章

に示す要件の策定例を参考に、実施手順を策定する。

・ 業務利用開始後も、業務利用において生じた課題、問題、その他の改善すべき点等を踏まえて、適宜リスクを再評価し、実施手順の見直しを行う。

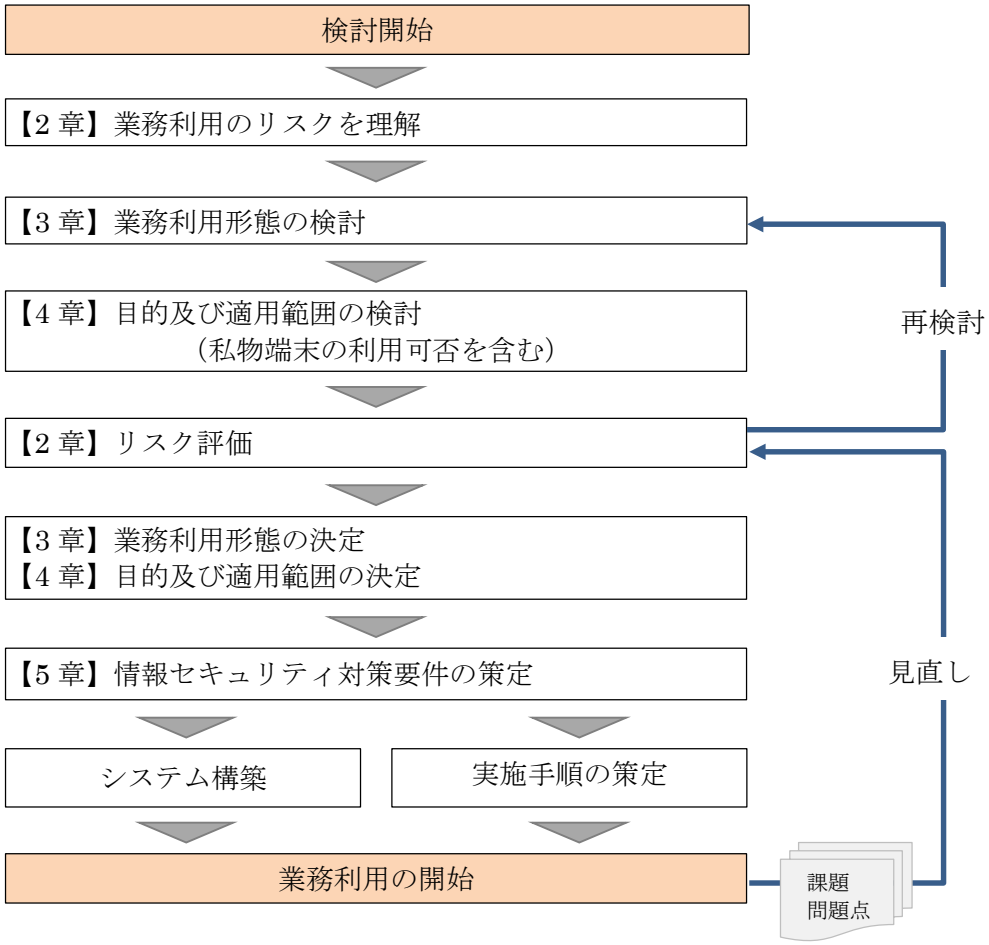

図１－１　業務利用検討の流れ

なお、本書は、庁舎外でスマートフォン等を業務利用する場合を前提に記述しているが、府省庁の会議室等の庁舎内に利用場所を限定した上でスマートフォン等を業務利用する場合における情報セキュリティ対策の要件策定に適用可能な事項も多いので、その場合も、必要に応じて参考とされたい。

1.4 用語の定義

本書において特別に使用する用語について、以下のとおり定義する。その他の用語については、政府機関統一基準の用語を使用する。

○ スマートフォン等

「スマートフォン等」とは、iOS、Android その他のスマートフォン対応 OS がインストールされた端末であって、主としてタッチパネル上のソフトウェアキーボードの操作により入力を行い、インターネット上のサイトからアプリをダウンロードすること等により、利用機能を取捨選択する使い方をする端末をいう。

スマートフォン等は、画面の大きさや電話機能の有無で区別されることが多く、画面サイズがおおむね 7 インチ以下で電話機能を有するものをスマートフォン、それ以外のものをタブレットという場合が多いが、市場において一様に定義されていないことから、本書においては、スマートフォンとタブレット端末を区別せずに、「スマートフォン等」として一括して取り扱うものとする。また、「端末」と表記しているものについては、特に断りのない限りはスマートフォン等の端末のみを指すものとする。

なお、スマートフォン等には、通信事業者の回線サービス及び無線 LAN を利用可能なモデルと、無線 LAN のみ利用可能なモデルが存在するが、本書では双方を対象としている。

○ アプリ

アプリケーションプログラム、アプリケーションのうち、特定の目的のためにスマートフォン等の OS 上にインストールされるソフトウェアであって、単体で機能を提供するもの又はネットワーク上に設置されたサーバと連携して機能を提供するものをいう。アプリの例としては、SNS や地図情報を利用するためのもの、電子メールを利用するためのもの、不正プログラム対策を行うためのもの等がある。

なお、スマートフォン等は、複数のアプリがインストールされて使われることが一般的であるが、本書においては、特に断りのない限り、それらのアプリを総称したものを指すものとする。

○ 業務用アプリ

スマートフォン等にインストールされるアプリのうち、府省庁の業務を実行するために、スマートフォンにインストールされるアプリを総称したものをいう。

○ 府省庁 LAN

府省庁 LAN とは、職員が日常業務で使用するために整備された府省庁内のローカルエリアネットワークであって、特に断りのない限り、各府省庁が個別に整備しているも

の（複数の府省庁で共同利用しているものを含む）を指す。

○ 府省庁 LAN 端末

府省庁 LAN の構成要素の一つであって、LAN ケーブル等により府省庁 LAN に接続されており、府省庁の職員が文書の作成や電子メールの送受信を行うなどの日常的な行政事務を遂行するために利用される端末をいう。特に断りのない限り、府省庁の執務室に配備されている PC を指すものとし、出張等の際に利用するモバイル専用の PC は除くものとする。

2. スマートフォン等の特性と業務利用におけるリスク

組織としてスマートフォン等の業務利用について意思決定する際は、スマートフォン等の特性や業務利用によって生じる脅威と業務上取り扱う情報や組織の特性に応じたリスクを総合的に評価した上で、スマートフォン等の業務利用形態を定め、運用開始時からリスク評価の結果に基づいた情報セキュリティ対策が適切に講じられるようにする必要がある。

2.1 スマートフォン等の特性

① PC と携帯電話双方の特徴を併せ持ち、電話、電子メール、ウェブサイト閲覧、文書の作成保存、画像や映像の記録等の様々な機能が利用可能である。

② OS の開発サイクルが短い。デバイスごとにソフトウェアの実装やベンダサポート（OS のアップデートを含む）が異なる。セキュリティ対策も発展途上である。

③ 様々な主体が開発したアプリが利用可能であり、インターネット上で運営されているスマートフォン等用のアプリマーケット（以下「アプリマーケット」という。）からアプリをダウンロードして利用する。

④ アプリがネットワーク上のクラウドサーバ等と接続して動作する場合が多く、基本的にネットワークに常時接続して利用される。

⑤ 携帯性に優れ、様々な場所に持ち運ばれる。

⑥ フリック入力等、タッチパネル操作による特有のユーザインタフェースを持つ。

⑦ 端末内のアドレス帳、画像や映像、通話履歴やメール送受信履歴等のプライバシーに関わる情報等がアプリ等に取得され、クラウド上に大量に保存される。

⑧ Bluetooth、NFC 等の近距離通信機能を持ち、データ送受信等に利用される。

2.2 スマートフォン等の特性及び業務利用における脅威

スマートフォン等の特性に対応する脅威、脆弱性、リスクの関係を表２－１に例示する。業務利用における脅威を認識し、脅威に対抗するための対策を適切に講ずるとともに、リスクを増大させる要因や脆弱性が発生又は拡大しないようにするための対策も必要である。

また、安全管理措置の実施水準は、職員個々の行動や意識等にも依存する場合があることから、特に、組織の管理下に完全に置くことができない私物のスマートフォン等を業務利用する場合は、表２－１に例示する私物端末特有の脆弱性を考慮した上で、利用の可否を判断することが重要である。

表２－１　スマートフォン等の業務利用における脅威と対策の例

特性	脅威	脆弱性 （リスクを増大させる要因を含む）	想定されるリスク	私物利用により増大する脆弱性	対策の例
①	PC と携帯電話双方の特徴を併せ持ち、様々な機能が利用可能。				
	ソフトウェア等の脆弱性を悪用した攻撃	多機能なため脆弱性が生じやすく、攻撃が多様化して対策が後手に回る	標的型攻撃、不正プログラム感染等により情報窃取、情報改ざん等の被害が発生する	私的に利用するサービスや機能に関する脆弱性が追加的に発生する	・不正プログラム対策ソフトウェアの導入 ・OS 及びアプリの更新 ・端末機能やサービスの利用の制限
②	OS の開発サイクルが短い。デバイスごとにソフトウェアの実装やベンダサポートが異なる。セキュリティ対策も発展途上。				
	ソフトウェア等の脆弱性を悪用した攻撃	・脆弱性対策が未実施の端末が長く使われる ・有効なセキュリティ対策ツールがリリースされず、脆弱性が放置される	・管理が脆弱な端末を介して情報窃取、情報改ざん等の被害が発生する	様々な機種が使われており、情報セキュリティ対策に係る管理が、府省庁支給端末に比べて難しくなるため、脆弱性が増大する	・端末のセキュリティ対策が不十分な状態でも一定の情報セキュリティが確保可能な業務用アプリを導入 ・利用可能な端末の機種や OS の制限又は統一 ・最新機種への変更 ・デバイス管理ツールの導入
	端末の改造により生じる脆弱性への攻撃	改造に起因して端末やソフトウェアに脆弱性が発生	改造された端末が攻撃され、情報窃取、情報改ざん等の被害が発生する	私的利用時の改造により、端末やソフトウェアの脆弱性が増大する	・改造の禁止
③	様々な主体が開発したアプリが利用可能。アプリをアプリマーケットからダウンロードして利用。				
	情報窃取等を行う不正なアプリによる攻撃	認識不足や不注意により、利用者が不正アプリをダウンロードしてしまう	・端末が不正プログラムに感染し、当該端末を介して情報窃取、情報改ざん等の被害が発生する ・センシング機能により、利用者に関する行動履歴等の様々な情報が盗取される被害が発生する	私的な利用時に不正アプリをダウンロードし、不正プログラムに感染する	・ダウンロード及び利用可能なアプリの制限 ・アプリの利用状況の定期的なモニタ ・マイク、カメラ等の不要なセンシング機能を使用不可とする
④	基本的にネットワークに常時接続して利用。				
	不正な無線 LAN アクセスポイントによる攻撃	通信回線の安全性を考慮せずに、業務を行う場所で利用可能な通信回線を無作為に選択して利用	なりすましアクセスポイントに接続する、不正プログラムに感染するなどによって、情報窃取、情報改ざん等の被害が発生する	私的な利用時に不正な無線 LAN アクセスポイントにアクセスする機会が増大する	・接続可能なネットワークの制限
	通信回線の盗聴	通信内容の秘匿性を確保せずに業務利用	通信回線上から情報窃取されるなどの被害が発生する	許可されていない通信回線に接続する	・接続可能なネットワークの制限 ・END-END で暗号化した上で通信を行う業務用アプリの導入
⑤	携帯性に優れ、様々な場所に持ち運ばれる。				
	第三者による端末の不正利	端末の放置や置き忘れ等の不十分な管理に起因する盗難・紛失	端末を入手した第三者が、端末内の情報を閲覧し情報が流出する、悪意	家族や友人への端末の貸与、旅行先や飲食店	・利用場所の制限 ・利用者の制限 ・端末ロック等の盗難・紛失

	用		のある第三者が情報窃取されるなどの被害が発生する	等で端末を利用した際の盗難・紛失等、不正利用につながる機会が増大する	・対策の徹底 ・不要な業務情報の削除 ・端末に業務情報を保存しない対策の導入
	画面ののぞき見	電車内やホテルのロビー等ののぞき見されやすい場所で業務利用	画面上に表示された情報が流出する	旅行先や飲食店等での端末利用等、のぞき見されるおそれのある機会が増大する	・のぞき見防止フィルタの導入 ・利用場所の制限
⑥ タッチパネル操作による特有のユーザインタフェースを持つ。					
	誤操作	スマホの取扱いに不慣れな利用者がメール機能等を誤操作	意図しない相手に情報が送信され情報が流出する	私的な利用時に誤操作する	・利用者の教育、注意喚起 ・タッチパネル操作に慣れていない者の業務利用の禁止
⑦ 端末内の情報がアプリ等に取得され、クラウド上に大量に保存される。					
	第三者による情報への不正アクセス	端末内の情報が自動的にクラウド上に保存され、クラウド運用者等の外部の者が不正アクセス	端末内の情報が流出するなどの被害が発生する	公私のデータが混在する	・自動保存されない領域で業務情報を取り扱うアプリの導入 ・クラウドへの自動保存機能の停止
⑧ Bluetooth、NFC 等の近距離通信機能を持ち、データ送受信等に利用される。					
	近距離無線通信による端末への攻撃	近距離無線通信を利用可能な状態のまま放置してしまい、攻撃の対象となる	不正プログラムに感染等により情報窃取されるなどの被害が発生する	近距離無線通信機能を私的に利用し、利用可能な状態のまま端末を業務利用してしまう	・近距離無線通信機能の利用禁止又は機能の停止

3. スマートフォン等の業務利用の形態

3.1 端末の配備

スマートフォン等の配備形態として想定される例を以下に示す。配備の形態ごとに端末の安全管理措置を実施する者や管理責任者が異なるため、配備形態に応じた安全管理措置の実施手順を整備し、情報セキュリティ対策が適切に講じられるようにする必要がある。

(1) 利用対象となる職員個々に端末を配備する形態

組織から、対象となる職員個々にスマートフォン等を調達、配布し、職員が当該端末を専有して利用する形態である。

安全管理措置の実施手順を適切に整備した上で職員に利用させることが重要であり、セキュリティ対策が施されている業務用アプリや端末管理ツールを導入するなどして、安全管理措置の実施に係る職員の負担を軽減させることも有効である。

(2) 組織において共用する端末を配備する形態

組織共通の端末を一定数調達し、職員が、利用の都度、借用の申請手続を行った上で端末を一定期間利用する形態である。例えば、職員の外出や出張等の際に行政事務を行うモバイル端末の一つとして、スマートフォン等を配備する場合が想定される。

組織の管理単位ごとに端末管理責任者を設置し、安全管理措置を実施することが可能になるため、管理責任者と利用者それぞれが実施すべき対策を管理手順や利用手順に定めておくことが重要である。

3.2 利用する場所

スマートフォン等を業務利用する場所を制限する場合は、あらかじめ利用手順に定め、画面ののぞき見や盗難・紛失対策等の安全管理措置が適切に講じられるようにする。

スマートフォン等を用いて庁舎外で府省庁の業務を行うことは、業務情報の要管理対策区域外への持ち出し及び要管理対策区域外での情報処理に相当するため、府省庁の情報セキュリティ関係規程において定められている情報の持ち出しに係る対策を考慮する必要がある。情報の持ち出しに係る対策は本書の対象外であるが、府省庁の情報セキュリティポリシーに従い、適切な処置が行われるよう、実施手順に含めるとよい。

また、スマートフォン等のカメラや録音機能が悪用されることが懸念されることから、機密性の高い情報を取り扱う区域へ、公用、私物を問わずスマートフォン等の持込みを禁止すること等についても考慮する必要がある。

3.3 私物端末の利用

表２－１に示す私物端末の業務利用に係るリスクへの対応方法について検討し、業務利用の要件を策定する。私物端末を業務利用する場合においても、府省庁支給の端末と同水

準の安全管理措置が実施されるよう考慮する必要がある。

私物端末の業務利用に際しては、

- 不要な機能の停止や業務用アプリのインストール等の技術的対策が府省庁支給の端末に比較して限定的になること
- ルールのみで私物端末の私的な利用までを制限することが困難であること
- 利用者の資産である端末本体や、端末内の個人所有のコンテンツ等の資産について考慮する必要があること
- 通信料金やセキュリティ対策機能の使用料金の負担について整理が必要なこと

等、解決すべき課題やリスクがあることから、組織が職員個人に対して私物の利用を強要してはならない。止むを得ず、職員の私物端末を業務利用する場合は、リスクを評価し、残存リスクを受容できる範囲での利用に限定することを考える必要がある。

【参考１】個人の判断による私物端末の利用（いわゆるシャドーIT）について

府省庁の執務室には日常的に私物端末が持ち込まれています。私物端末は、常時携帯されるものであり、また、使い慣れたものであることから、私物端末を使って業務を行なうことを利用者は便利と感じます。組織として私物端末の利用を禁止していても、禁止のルールが徹底されていない（又はルールが存在しない）と、利用者は便利さを優先して「一度くらい大丈夫だろう。」といった個人の判断で、手元にある私物端末を業務に利用してしまうことが想定されます。このような個人の判断で私物端末が使われる状態は“シャドーIT”等と呼ばれ、組織の情報セキュリティリスクを高める要因として懸念されています。

したがって、組織として情報セキュリティを適切に維持するためには、シャドーITを黙認せずに、利用を禁止するルールを定め、管理を徹底することが重要です。

なお、私物端末が頻繁に利用されているなど、業務利用上一定のニーズがあり、かつ、私物端末を利用する以外に解決方法が無い場合は、私物端末の利用を組織として認め、本書に例示するような徹底した管理の下、職員に利用させることも考えられます。

3.4 情報システムの利用形態

スマートフォン等の業務利用を判断する際には、どのような情報システムに接続して情報処理を実行するかについても考慮しておく必要がある。

例えば、

① 職員の府省庁 LAN 端末にリモートアクセスし、職員の府省庁 LAN 端末を遠隔操作することで、府省庁 LAN 端末と同等の情報処理を行う

② 府省庁 LAN に接続された情報システムにリモートアクセスし、利用を許可されたサービスを利用する

③ 府省庁 LAN や府省庁 LAN 端末にはアクセスせず、モバイル端末専用に構築された情報処理サービス（電子メールサービスやファイル共有サービス等）を利用する

等の利用形態が考えられる。

代表的なスマートフォン等の業務利用の形態を図３－１～３に、各利用形態の情報セキュリティ対策上の利点や懸念等の比較を表３－１に示す。

なお、ここで示す内容は一例であり、組織の規模や取り扱う情報の特性等を勘案した上で利用形態を決定する必要がある。

① 職員の府省庁 LAN 端末等へリモートアクセスする形態

府省庁 LAN のクライアント端末へリモートアクセスし、府省庁 LAN 端末の業務サービスを利用して情報処理を行う。仮想クライアント機能による方法やリモートデスクトップ機能を導入する方法が考えられる。

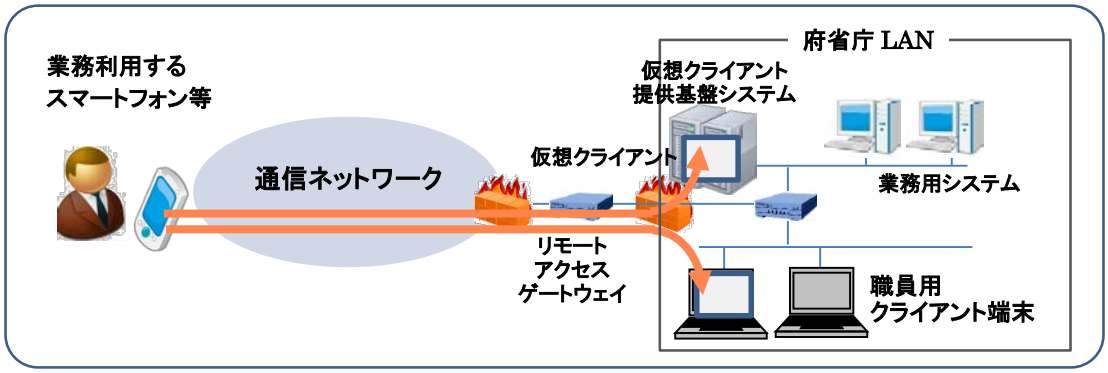

図３－１　府省庁端末等へリモートアクセスする形態

② 府省庁 LAN に接続されている情報システムへリモートアクセスする形態

スマートフォン等の利用を許可するサービスを提供している府省庁 LAN の業務用システムにリモートアクセス可能な環境を追加し、当該環境へリモートアクセスして情報処理を行う。

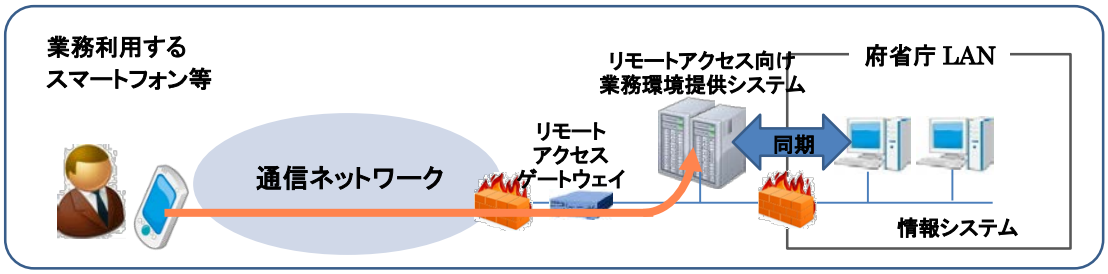

図３－２　府省庁 LAN の情報システムへリモートアクセスする形態

③ 府省庁 LAN 以外の情報処理サービスを利用する形態

府省庁 LAN は使用せず、ファイルストレージやウェブメール等の業務用サービスを別に用意し、情報処理を行う。

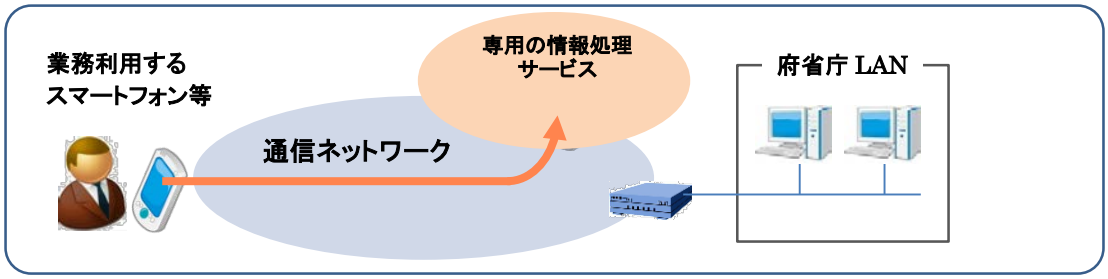

図３－３　府省庁 LAN 以外の情報処理サービスを利用する形態

表３－１　情報システムの利用形態①～③の比較

	形態①	形態②	形態③
概要	職員自身の府省庁 LAN 端末又は仮想クライアントへリモートアクセスし、府省庁 LAN 端末で提供されているサービスを利用する	府省庁 LAN のリモートアクセス専用環境を経由して情報システムへ接続し、リモートアクセス用に提供されているサービスを利用する	府省庁 LAN は使用せず、専用サービス（ファイルストレージ、ウェブメール等）を利用する
利用可能なサービスの範囲	府省庁 LAN 端末と同等の範囲	リモートアクセスによる利用環境を提供している府省庁 LAN サービスのみ	モバイル端末専用に個別に構築されたサービスのみ
情報セキュリティ対策上の利点	LAN 端末で利用できるサービスや機能を執務室外で利用できるので、無許可の業務利用が発生するリスクが小さい	府省庁 LAN サービスの利用を実現しつつ、守るべき情報を限定することも可能となる	府省庁 LAN とは独立した情報処理環境になるため、守るべき情報を限定することが可能となる
情報セキュリティ対策上の懸念	リモートアクセス先の情報システムに侵入された場合の影響範囲が府省庁 LAN 全体に及ぶ	リモートアクセス先の情報システムに侵入された場合に府省庁 LAN に一定の影響がある 利用を認めていない機能の無許可利用が発生する懸念がある	職員が複数のサービスを意識して使い分ける必要がある 利用を認めていない機能の無許可利用が発生する懸念がある
各形態の選定理由	対象とする業務が多岐にわたり、対象職員も明確に定まらない場合 （例：テレワーク）	対象とする職員や業務を限定することが可能な場合 （例：外出先からのメールやスケジュールチェック、簡易的なテレワーク）	特定のプロジェクト遂行等狭い範囲でのコミュニケーション基盤とする場合 （例：個別プロジェクトにおける外部との情報共有）

4. 目的及び適用範囲の明確化

4.1 目的の明確化

目的が曖昧なまま、闇雲にスマートフォン等や業務用アプリ等の導入を判断してしまうと、不要なコストが発生するおそれがあるばかりでなく、利用に伴うリスクが増大することになりかねない。そのため、スマートフォン等の業務利用の目的を明確化し、目的に合った業務利用の形態を定めることが重要である。

4.2 対象とする業務

スマートフォン等を利用する業務を明確化する。執務室内で府省庁 LAN 端末だけを用いて行う業務と比較して情報漏えい等の情報セキュリティインシデントが発生するリスクが高まることを想定し、組織や取り扱う情報の特性から、対象とする業務範囲の制限等について考慮する必要がある。

なお、業務の範囲を制限することが困難な場合は、スマートフォン等で取り扱うことができる情報や接続可能な情報システムを制限する方法も考えられる。

＜例＞

- 要機密情報を取り扱う業務を禁止し、それ以外を利用可能とする。
- 機密性１情報のみ取扱い可能とする。
- 府省庁の電子メールのみ利用可能とする。

4.3 利用者

組織に属する行政事務従事者全員を対象とするのか、対象とする業務や情報等に応じて対象者を限定するのかなど、利用者を選定するための条件について明確化する。以下に例を示すが、複数条件を組み合せるなども有効である。また、利用手順等への違反や端末紛失等の情報セキュリティインシデントを起こした者については、一定期間利用を停止すること等を要件に含めることも考えられる。

＜例＞

- ○○部局に属し、□□業務に従事する職員であること
- 直近の 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であること
- 課室情報セキュリティ責任者が必要と認める者

また、私物のスマートフォン等を業務利用する場合は、利用を許可する職員の条件として、例えば以下のような条件についても併せて明確化する。

- 情報セキュリティ対策の必要性を理解し、適切に安全管理措置を講ずることができる職員であって、私物端末を業務利用する際に組織から求められる要件に合意した者

5. 業務・サービスの利用要件の策定

4 章に示す内容を踏まえて、府省庁においてスマートフォン等を業務利用する際の情報セキュリティ対策に係る要件の策定例を示す。府省庁の業務や取り扱う情報の特性に応じて、適宜見直した上で要件を決定するとよい。

5.1 端末や OS の種類

利用する端末の機種や OS の種類、バージョン等の要件を定める。情報セキュリティ対策を長期的に維持するためには、可能な限り最新バージョンの OS を使用することや、脆弱性対策等のための更新版のリリースが長期に渡って確約されているなどサポート対応が明確な端末ベンダやソフトウェアベンダ等を選定することが考えられる。

また、利用する端末や OS の種類が多岐に渡ると、全ての端末において同等の情報セキュリティ対策を講ずることが困難になるほか、管理工数やコストも増大するおそれがあることから、一定程度、種類を制限することも必要である。

5.2 端末機能・サービスの要件

端末機能・サービスのうち、業務に利用するものを決定する。利用しない端末機能・サービスについては、あらかじめ機能の削除や停止等の措置を講じておくことが望ましい。端末に初期インストールされている端末機能・サービスのうち、利用しないものについて、機能の削除や停止等の措置により無効化する。表５－１に、端末機能・サービスの利用要件及び利用制限の例を示す。

なお、無効化が不可能なものについては、利用の禁止を手順として定めておく必要がある。

表５－１　端末機能・サービスの利用要件及び利用制限の例

端末機能・サービスの例	利用要件及び機能制限の考え方
音声通話	府省庁が契約する通信事業者提供の音声通話サービスのみを利用する。その他の音声通話アプリは禁止する。（5.2 節(1)に詳細を解説）
電子メール	通信事業者のメールサービスを利用又は業務用アプリを導入。受信メールフィルタリングを設定。（5.2 節(2)に詳細を解説）
ウェブブラウザ	業務用アプリを導入。ウェブサイトフィルタリングを設定。（5.2 節(3)に詳細を解説）
アドレス帳	秘匿性を確保できる専用アプリを導入した上で利用又は端末に初期インストールされているアドレス帳を利用（5.2 節(4)に詳細を解説）
近距離無線通信（無線 LAN/Bluetooth/赤外線通信等）	業務上不要であれば、利用を禁止して機能を無効化する。
撮影、録画、録音等	業務上不要であれば無効化する。カメラについては、レンズにセキュリティシールを貼付するなどして対策することも考えられる。
外部電磁的記録媒体（SD カード等）	外部電磁的記録媒体が利用可能な端末については、利用を禁止又は媒体の接続ポートを停止して機能の無効化の措置を講ずる。
GPS 測位	業務上必要な場合や、盗難・紛失時の位置検索サービス等を除き、機能を無効化する設定を行う。
クラウドへのデータバックアップ	業務利用に許可されたバックアップ機能以外は機能を無効化する。
テザリング	業務上不要であれば、利用を禁止して機能を無効化する。

主な端末機能の情報セキュリティ対策に係る要件を以下に示す。

(1) 音声通話

通信事業者が提供する音声通話サービス以外にインターネット上で運営されているスマートフォン等用のアプリマーケット（以下「アプリマーケット」という。）で提供される音声通話用アプリを利用する場合は、利用可能なアプリをあらかじめ限定することが望ましい。また、安全性が不明なものを利用者が勝手にダウンロードして業務利用しないように、当該アプリのダウンロードを禁止する（又はダウンロード不可能とする）などの措置を講じておく。

(2) 電子メール

業務利用する電子メールのアプリを限定する。電子メールの使用に際しては、メール送受信情報の保存場所（端末内部やクラウド上にあるメールボックス）や保存された情報にアクセスする際に認証を行うこと。メール送受信情報が端末上に保存されていない場合でも、一般のメールアプリやウェブメールでは、スマートフォン等に ID やパスワードを記録している場合もあり、容易にメールボックスにアクセスされてしまうことも考えられることから、特に要機密情報を取り扱う場合においては、全ての業務メールをスマートフォン等に自動転送することを禁止するとともに、専用の電子メールアプリを準備するなどして安全に電子メールが利用できるようにすることが望ましい。この方法は、私物の端末を業務に利用する場合に、業務のメールと私用のメールの混在を防止することもでき、私物端末を利用する場合の情報セキュリティ対策としても有効である。

また、標的型メール攻撃への対策として、受信メールのフィルタリング機能を利用することも有効である。

インターネット上で提供されているフリーメールサービス等は、安全性が不明なものが多いことから、フリーメールサービスの利用は禁止することが望ましい。

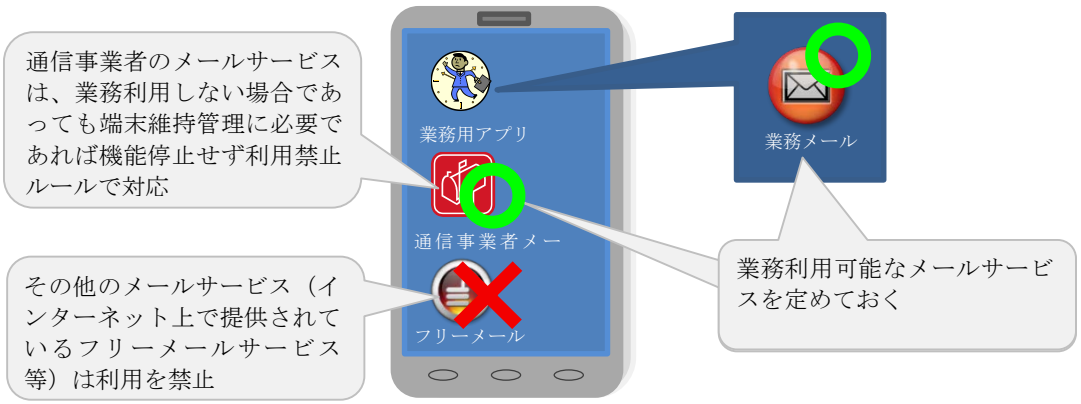

図５－１　業務用メールサービスの利用イメージ

(3) ウェブブラウザ

スマートフォン等のウェブブラウザを使用して業務を行う際に、悪意の第三者等が設置したサイトに誤ってアクセスしてしまい、ウェブブラウザの脆弱性を突かれて不正プログラムに感染する脅威が想定されることから、業務利用するウェブブラウザを限定し、ウェブブラウザのバージョンを最新化するなどして脆弱性対策を講じたり、職員が不要なウェブサイトの閲覧を行わないようルール化したりすることが必要である。また、技術的な対策としてウェブサイトフィルタリング機能が利用できる場合には、それを利用することも考えられる。

また、ブラウザのキャッシュ（ブラウザが表示したウェブページのデータを一時的に端末内のメモリに保存する機能）から要機密情報が漏えいするリスクを考慮し、一般のウェブブラウザを利用するのではなく、端末に一切の情報を残留させない専用のアプリを導入することも有効である。

このような機能を持つアプリとして、参考２に示すように、セキュアブラウザと呼ばれる製品やソリューションが流通しているのでこれらを導入することも考えられる。

【参考２】セキュアブラウザとは

一般のウェブブラウザは、閲覧したホームページのコンテンツや閲覧履歴（URL）、ログイン画面に入力した ID やパスワード、サーバとの間の通信で使用する Cookie 等の情報を、ブラウザのキャッシュに一定期間保存することにより、利用者の利便性を向上させています。

サーバ側で用意するウェブコンテンツのつくりにも依存しますが、端末側にこれらが残るような仕様となっている場合において、これらの情報は端末に残留するため、端末の盗難・紛失の際に、これらの情報が漏えいし、さらには、これらの情報を悪用されることも考えられます。ウェブブラウザの設定等により、これらを削除することも可能ですが、都度実施するルールは現実的でないので、一定のリスクが残存すると考える必要があります。

したがって、特に、要機密情報を扱う場合や組織の情報システムにリモートアクセスさせるような場合には、サーバ側で用意するウェブコンテンツのつくりも考慮し、一般のウェブブラウザを利用するのではなく、端末に一切の情報が残留しないセキュアブラウザを活用したソリューションを導入するなどしてリスクを軽減させることを考える必要があります。

セキュアブラウザやセキュアブラウザを活用したソリューションが備える機能としては、例えば以下があります。

・メール、ファイル閲覧等を画面転送等で行い、ユーザデータを端末に残さない機能
・ブラウザの終了時に閲覧に関連する情報(ブラウザのキャッシュ等)をクリアする機能
・外部出力（スクリーンショット、印刷等）の抑制機能
・SSL/TLS 等によりサーバと暗号化通信を行う機能

(4) アドレス帳

業務で使用する他の職員や業務に関係する府省庁外の者の電話番号やメールアドレス等の情報を端末に保存して管理する場合は、参考３に示すような脅威を想定し、容易に個人が特定されない登録情報（部署名や氏名のイニシャル等）を用いる、登録情報を暗号化するなどの対策を組み合わせて、厳重な管理を行う必要がある。業務用アプリを用いて、業務用アドレス帳の秘匿性を確保した上で管理する方法も有効である。

【参考３】標的にされるスマートフォン等のアドレス帳

SNS は不特定利用者のコミュニケーション活性化を目的にしており、スマートフォン等のアドレス帳情報を自動的に収集して SNS サーバへ送信し、利用者間でアドレス帳を共有するサービスも提供されています。しかしながら、プライバシーや個人情報に対する配慮が足りない事業者が提供する SNS アプリでは、初期設定状態で全 SNS 利用者に情報を公開する仕様のものも存在し、そのようなアプリをうっかり利用してしまうと、利用者の意図に反して端末内のアドレス帳情報が不特定の者に閲覧されてしまうおそれがあります。

上記の SNS の例はまだしも、スマートフォン等のアプリの中には悪質なものがあり、アドレス帳そのものを窃取することを目的とした不正なアプリが存在していることも確認されています。以下はインターネット上で報道された内容の一例です。

『スマートフォン（高機能携帯電話＝スマホ）の電話帳に登録された個人情報を抜き取るアプリ（ソフト）がインターネットで配信された事件で、警視庁サイバー犯罪対策課は 30 日、ＩＴ関連会社の元経営者ら５人を不正指令電磁的記録供用容疑で逮捕した。抜き取られた電話番号やメールアドレスなどの個人情報は約 1180 万件に上るという。アプリを巡り、大規模な個人情報流出事件が立件されるのは初めて。
（中略）グーグルの基本ソフト（ＯＳ）「アンドロイド」を搭載したスマホ用の専用サイト「グーグルプレー」上で人気ゲームなどのタイトルに「ｔｈｅ　Ｍｏｖｉｅ」などと付加した名前のアプリを約 50 種類作成し、ネット上で公開。アプリを起動した約９万人のスマホを誤作動させ、アドレス帳に登録された個人情報を不正に取得していた。』

※出典　日経新聞 web 版　2012 年 10 月 20 日記事

スマートフォン等のアプリは、個人の趣味趣向に応じて様々なものがインターネット上のアプリマーケット等に公開されており、個人のスマートフォン等には多くのアプリがダウンロードされ使用されています。私的な利用の際にうっかり不正なアプリをインストールしてしまい、業務用アドレスが含まれたアドレス帳が丸ごと窃取されてしまうなど、私物の端末を業務利用する際には、不正アプリが存在するリスクを踏まえて、守るべき情報を意識した対策を十分考慮しておくことが重要です。

5.3 業務用アプリの導入

スマートフォン等を業務利用する際に、情報処理を行うために必要となる業務用アプリとして、端末にインストールするものを決定する。アプリマーケットからダウンロードして利用する場合と専用の業務用アプリを個別に実装する場合が考えられることから、業務要件や情報システムとの接続形態等を踏まえた上でアプリの導入方法を決定する。

(1) アプリマーケットからアプリをインストールする場合

アプリマーケットからダウンロードして利用することが可能なアプリの中には、不正プログラムへ感染させて端末内の情報を窃取したり、端末を遠隔操作したりすること等を目的としたものが存在する。アプリの脆弱性対策を装うものや無料の不正プログラム対策ソフトウェアの提供を装うもの等、利用者のセキュリティ向上意識を逆手にとるものも確認されており、十分注意する必要がある。スマートフォン等を対象としたアプリマーケットも、多様な事業者が運営していることから、信頼できないアプリマーケットにより提供されているアプリは利用しないなどについても考慮が必要である。

このような背景から、業務ツールとして使用するアプリ以外は、ダウンロードを禁止として、可能であれば端末の機能によりダウンロードを不可能にするなどの対策も講ずることが望ましい。

また、業務に利用するアプリは、以下を確認した上で決定するとよい。

- アプリの利用規約
- アプリの提供元事業者（他の利用者による評価を確認することも考えられる）
- アプリのサポート対応（実績の確認が可能であれば併せて確認）
- アプリがアクセスする端末内の情報や機能等の範囲
- 初期設定の状態及び設定変更が可能な範囲
- 同時にインストール（バンドル）されるアプリの有無

上記に加えて、更新版アプリがリリースされた場合の措置方法についても利用手順に含めておくとよい。

なお、利用する OS やアプリの種類によっては、アプリが端末内の情報や機能等へアクセスすることを禁止できないものがあるので十分確認した上で利用を判断する必要がある。

(2) 専用の業務用アプリを導入する場合

スマートフォン等を業務利用する際の専用アプリとして端末にインストールするものを決定する。業務用アプリを導入することで、利用者の一括管理が可能となり、情報セキュリティ対策の面からは有効であるが、維持管理の工数やコストが必要となることから、業務や取り扱う情報の特性等に応じて導入を判断する。

専用の業務用アプリとしては、例えば以下のものが考えられる。

・ 府省庁の情報システムへのリモートアクセス（認証、経路暗号化を含む）
・ 文書作成
・ 電子メール
・ ウェブブラウザ
・ スケジュール管理
・ アドレス帳

上記の機能をパッケージ化して情報セキュリティ対策機能を強化した業務用クライアントアプリが、多くのベンダにより市場に提供されていることから、要機密情報を取り扱う場合等においては、専用のクライアント機能を提供する業務用アプリを導入し、業務用アプリ全体で情報の秘匿性を確保することにより対策を強化する方法も考えられる。

図５－２に、専用のクライアント機能を提供する業務用アプリの導入イメージを示す。

図５－２　専用のクライアント機能を提供する業務用アプリのイメージ

5.4 通信ネットワークの要件

利用可能な通信ネットワーク及び端末－サーバ間の通信経路のセキュリティ確保の方法を決定する。

(1) 通信ネットワークの制限

スマートフォン等は、基本的に通信ネットワークに接続して利用するものであることから、安全なネットワークの利用について考慮する必要がある。

通信ネットワークの選択肢としては以下が考えられる。

- 通信事業者のモバイル通信サービス
- 職員の自宅に設置されている通信事業者のブロードバンド通信サービス
- 公衆無線 LAN サービス

提供主体が不明なものや運営状況等が開示されていないものなど、安全性が不明な通信ネットワークは業務に利用すべきではないが、例えば海外出張等の際に宿泊先に設置されている公衆無線 LAN 回線等を使用せざるを得ない場合も考えられる。そのような場合は、端末－業務用システム間の通信経路に VPN 技術を用いるなどにより、END-END で通信内容の秘匿性を確保し、通信ネットワークの安全性が不明な場合であっても一定のセキュリティが確保できるよう考慮する必要がある。

なお、VPN 接続用のアプリや接続時の認証情報が外部に漏れると、府省庁 LAN や府省庁の情報システムに不正にアクセスされるおそれがあることから、利用する通信ネットワークやリモートアクセス用のアプリ、認証情報等の秘匿性を確保するための措置及び漏えいを防止するための措置をとることも重要である。

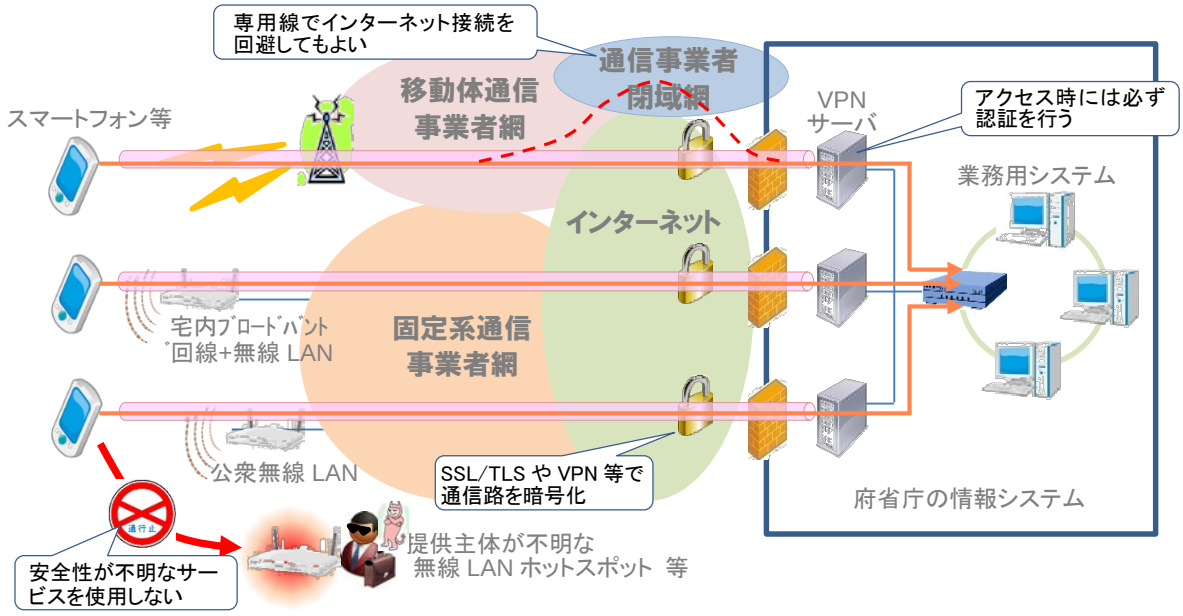

図５－３　安全な通信ネットワークの利用イメージ

【参考４】ホテルの公衆無線 LAN から機密情報が漏えい？

日本等で高級ホテルの公衆無線 LAN に接続した端末から機密情報を盗み取る被害が相次いでいるとのロシアの情報セキュリティ会社による発表がインターネットで報道されました。同社の情報では、攻撃者は、標的となる企業や研究機関等の責任者の宿泊予定をあらかじめ把握し、ホテルのシステムに侵入して標的となる端末にソフトウェア更新を装った画面を表示させ、攻撃に必要なプログラムをインストールさせて機密情報を窃取しているとのことです。

このように、公衆無線 LAN サービスの提供主体がある程度明らかであっても、当該サービスの脆弱性がサイバー攻撃の手口として悪用される場合があることを認識しておくことが大切です。リモートアクセス環境を利用者に提供する際は、“疑わしきは使わず”又は“どのようなサービスも疑ってかかる”くらいの考え方を持ち、より安全なリモートアクセス方式を利用者に提供することが必要です。

(2) 通信経路の安全性確保

以下を例とする通信経路及び端末内のデータ秘匿性確保及び業務用システムへの不正アクセスを防止するための要件について考慮する。

- 通信経路の暗号化
- VPN 接続時の端末識別又は端末認証
- 業務用システム利用時のユーザ認証
- アクセスログ等の取得及び保存

これらの機能を製品パッケージとして提供するソリューションを採用し、専用のアプリを端末に実装する方法も考えられる。図５－４に、安全な通信経路の構築例を示す。

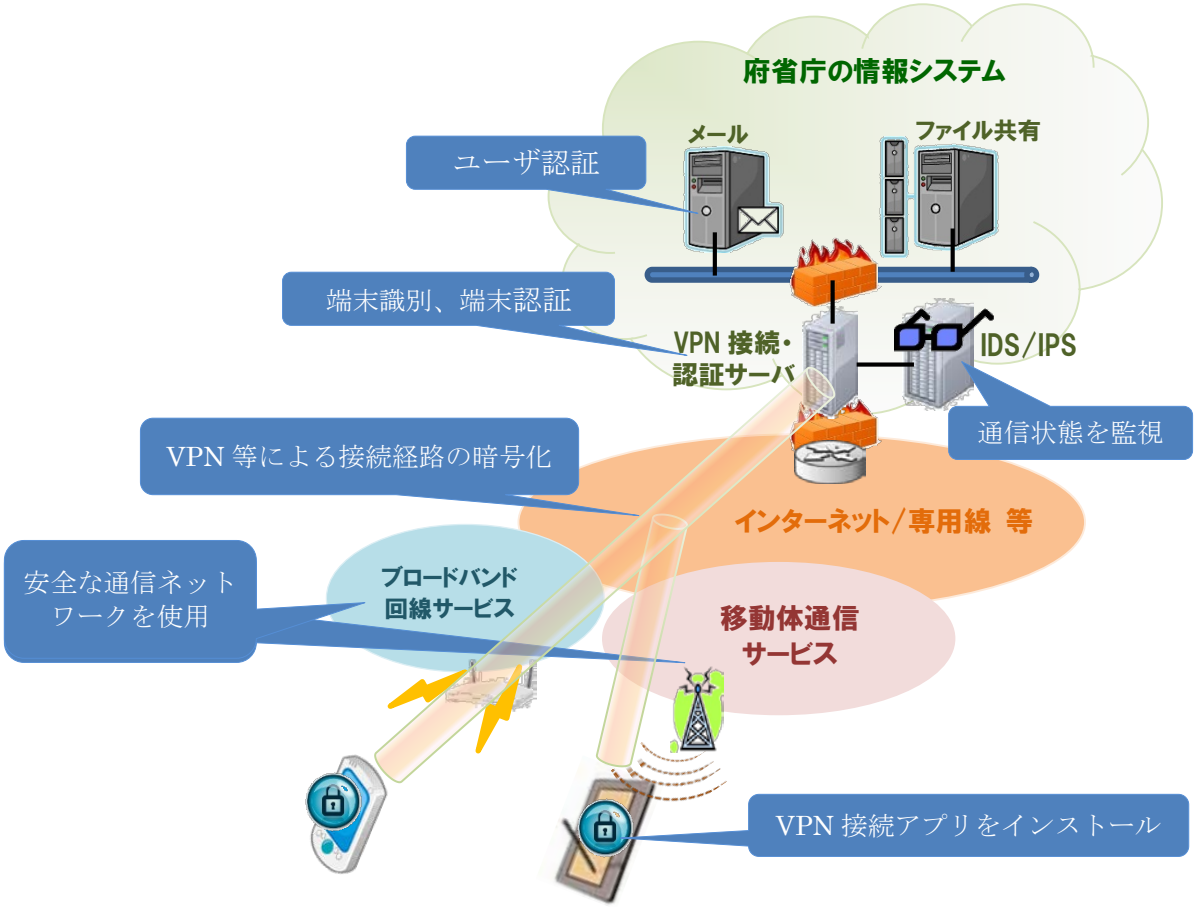

図５－４　安全な通信経路の構築例

5.5 情報セキュリティ対策要件

業務利用するスマートフォン等の情報セキュリティ対策を適切に維持するために必要なセキュリティ機能の導入要件を決定する。

(1) ソフトウェアの脆弱性対策

(2)

OS やアプリ等のソフトウェアの脆弱性を狙う外部からの攻撃の脅威に対抗するために、ソフトウェアの脆弱性対策を適切に実施することが必要である。スマートフォン等にインストールされる OS 等の汎用的なソフトウェアについては、更新版がベンダから自動的に配信される場合が多いことから、更新作業を利用者に実施させることも考えられるが、組織の特性や、配備形態、配備台数、利用者の技術習熟度等を勘案し、運用担当者が一括して実施する方法も含めて実施方法を決定する。業務用アプリを個別に導入する場合は、その更新方法をアプリ提供元のベンダとも協議して決定し、更新作業に必要な環境を準備する。また、更新版ソフトウェアについて、事前に検証機等を用いて端末機能の動作確認を行った後に、実機に適用するなどの手順を考慮することも

考えられる。

なお、脆弱性対策を実施する上では、端末ベンダやOS提供ベンダ等から提供されるソフトウェアの脆弱性等に係る情報を注視することも重要であることから、以下を例とする情報の確認を手順に含めることも考えられる。

- 脆弱性の原因
- 脆弱性による影響範囲、想定されるリスク
- 脆弱性の対処方法
- 脆弱性を悪用する不正プログラムの流通状況

(2) 不正プログラム対策

業務利用するスマートフォン等の機種に対して適用可能な不正プログラム対策ソフトウェアの中から利用するものを選定する。

不正プログラム対策ソフトウェアについては、通信事業者が提供するサービスを利用する（モバイル通信サービスを契約している端末に限る）方法、セキュリティベンダ等がスマートフォン等用にアプリマーケット等で提供しているサービスを利用する方法、業務用アプリの一つの機能として専用のものを導入する方法等が考えられる。

(3) のぞき見防止対策

第三者の画面のぞき見等による情報窃取のリスクを軽減するための対策として、以下を例とした要件を決定する。

- 操作の無い状態で一定時間経過すると自動的にスクリーンロックする端末ロック機能の設定
- のぞき見防止フィルタの画面への貼り付け
- 利用可能な場所の限定（ホテルのロビー等の公共スペースでの利用禁止等）

(4) 盗難・紛失対策

スマートフォン等の盗難・紛失対策として、端末ロック機能、リモート端末ロック機能（遠隔操作により端末ロックする機能）及びデータワイプ機能（端末のデータを削除する機能）等の要件を決定する。

端末ロック機能は、利用者個人の判断でロック設定を解除されないように、解除の禁止を要件に含める。

端末に情報を保存する場合は、データワイプ機能の対策要件も考慮する。データワイプ機能のうちリモートデータワイプ機能（遠隔操作により端末のデータを削除する機能）については、通信圏外等の通信機能が動作していない状態では有効に機能しないことから、ローカルデータワイプ機能（例えば、パスワード入力の失敗回数があらかじめ決められた閾値を超えた場合等、一定の条件と一致した場合に端末のデータを削除す

る機能）の適用についても検討し、手順を明確化するとよい。また、端末の盗難・紛失時に、利用者に代わって通信事業者のオペレータが端末の所在位置を確認したり、データワイプを実施したりするサービス等、利用者のセキュリティ対策を支援するサービスを活用することも有効である。

なお、これらの対策の中には、端末ロックが解除された状態で端末の盗難・紛失に遭った場合は無効となってしまうものもあることから、以下に示す対策を併せて実施することで、情報セキュリティリスクを軽減することが必要である。これらの対策については、府省庁対策基準策定のためのガイドラインにおいても解説していることから、参照されたい。

- 端末又は業務情報全体を暗号化する機能を設ける
- 業務情報が記録されたファイルごとに暗号化する機能を設ける
- ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する
- 仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する
- セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する

(5) ログ管理機能

スマートフォン等の業務利用環境を悪用して、要機密情報に不正アクセスされるなどの脅威に対抗するために、情報システムへのアクセス履歴等のログを確保しておく必要がある。取得するログの内容や取得する対象箇所（機器、サービス等）は、業務利用形態によって異なることから、あらかじめ監視対象のシステムや対象とする情報等を決定しておくことが重要である。

- ログの取得ポイント（端末側、サーバ側等）
- 取得するログの内容（通信の内容のほか、通信時間や通信先等）
- ログの保存期間
- ログ解析の手順

(6) 端末管理ツール（MDM：Mobile Device Management）の導入

ソフトウェアの更新、不正プログラム対策ソフトウェアの実行、端末ロックの設定等について、運用担当者が一括で実施するために、MDM を導入することが考えられる。MDM の導入によって表５－２に例示する管理業務が自動化されて、適切に実行されるほか、運用担当者の実務負担の軽減も期待されることから、管理対象となる端末数が膨大であるような場合には、MDM の導入を検討するとよい。

図５－５に MDM による端末管理のイメージを示す。

表５－２　MDM の主な機能

機能項目	機能の説明
端末ロックの遠隔制御	端末個体ごとに、遠隔制御でロック、アンロックを実施
リモートデータワイプ	端末内全データ削除、個別データ/特定フォルダ削除、業務領域のみ削除 等
暗号化	外部メモリ出力時のデータ暗号化/復号、個別データの暗号化/復号
端末機能制御	カメラ、スクリーンショット、近距離無線通信、外部メモリ出力等の機能制限
端末状態監視	端末状態の取得（OS、アプリ、改造の有無、起動中アプリ 等） 死活監視、ログ収集、位置情報取得、アラートメールの送信、管理者向け統計処理
ポリシー設定及び実行	パスワードポリシー設定、MDM ポリシー（リモートデータワイプの条件、機能制限 等）設定 メーラーや無線 LAN 接続、証明書等の端末構成の設定変更 等
資産管理	端末所有者の属性管理や端末個体情報(機種、電話番号 等）の管理 等
アプリ配信及び削除	業務用アプリの配信と自動インストール、遠隔削除
アプリ利用制限	非公認アプリのインストール制限や強制終了、アプリのアクセス許可制御 外部媒体経由のアプリインストール制御 等
MDM サーバ接続	SSL・VPN による通信路暗号化、GCM 等によるエージェント・MDM サーバ間通信路の維持 等
フィルタリング機能	ウェブフィルタ、メールフィルタ等の設定情報管理やアクセスログの収集
不正プログラム対策ソフトウェアの管理	不正プログラム対策ソフトウェアのバージョンやパターンファイルの管理、最新版への更新、スキャンログの収集、スキャン実行の要求　等
バックアップ	端末データのバックアップやリストア

※出展　CIO 補佐官等連絡会議情報セキュリティ WG BYOD 要件検討 SWG 報告書

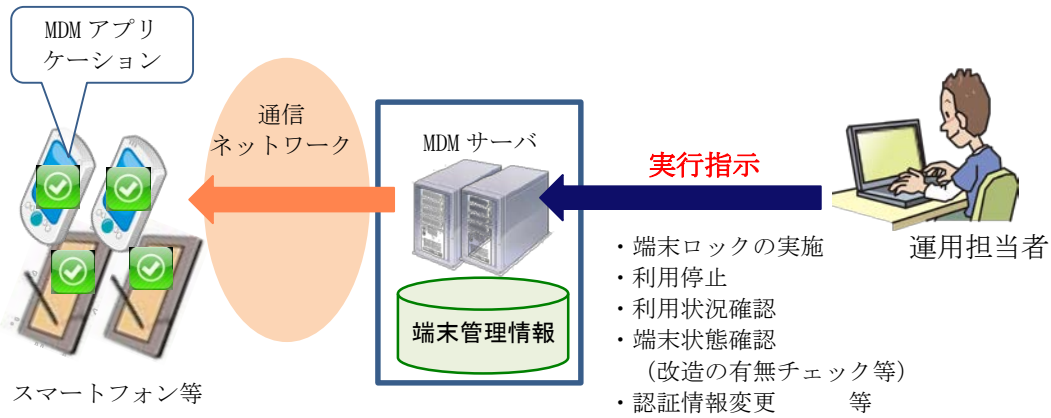

図５－５　MDM による端末管理のイメージ

なお、MDM は、端末内に保存されている情報や端末の利用状況を把握できてしまうため、利用者のプライバシーに対して一定の配慮が求められる。MDM の導入が難しい場合は、端末内の業務領域のみに限定して管理を行うことができる MAM（Mobile Application Management）の活用も検討するとよい。

図５－６に、MAM の運用イメージを示す。

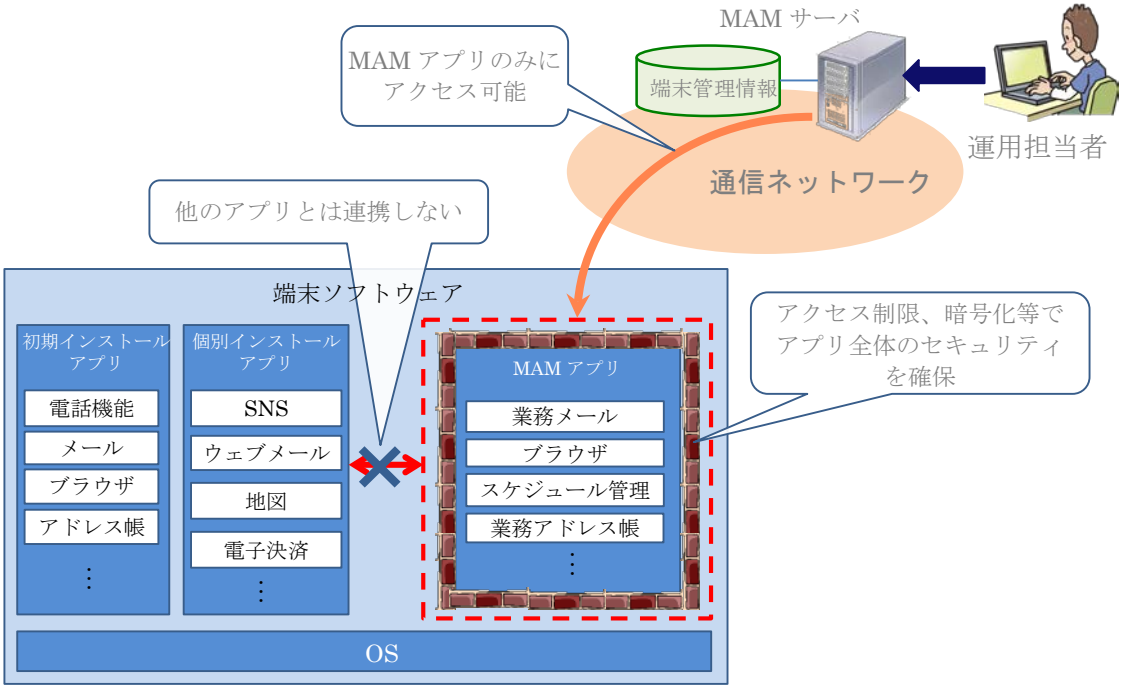

図５－６　MAM の運用イメージ

5.6 私物端末の業務利用に際して留意すべき事項

情報セキュリティ対策要件として定めた手順は、業務利用される全てのスマートフォン等において等しく実施されなければならない。１台でも手順を遵守しない端末が存在すると、当該端末の脆弱性に起因する情報セキュリティインシデントが発生することも考えられることから、私物端末であっても業務利用に関する情報セキュリティ対策要件が適切に遵守されるようにすることが重要である。

一方で、私物端末は、職員が私的な利用のために自ら費用負担して入手したものであり、府省庁支給の端末と同じ管理をすることは現実的ではない。私物端末を業務利用する際に留意すべき事項と要件の策定例を表５－３に示す。

表５－３　私物端末の業務利用する際に留意すべき事項と要件策定例

留意事項	私物端末の利用を認める場合の要件策定例	（参考）私物端末の利用を認めない場合
業務情報と私的な情報の混在の回避	・端末内の私的な情報と業務情報を混在させないよう、これらを明確に分けるための仕組みを導入する ・業務用アプリ導入又は端末に業務情報を保存させない仕組みを導入する	業務専用端末には私的な情報が存在しない
家族や友人への貸与の禁止	・私的な利用においても家族や友人が利用することを禁止することを合意した者のみに私物端末の利用を認める	利用者の限定が可能
外出先等での端末の盗難・紛失	・業務利用する際の利用場所を限定する ・私的利用時を含めて端末ロックやデータワイプ機能の設定を必須し、対策の実施について合意した者のみに私物端末の利用を認める	利用場所の限定が可能 対策の実施が前提
利用するネットワークの制限	・私的な利用時であっても安全性の確認できないサイトや通信ネットワークへの接続を禁止するなどの利用手順を策定し、合意した者のみに私物端末の利用を認める	端末機能や通信ネットワークの制限が可能
ソフトウェア更新や不正プログラム対策の実施	・ソフトウェア更新や不正プログラム対策ソフトウェアの実行を義務付け、合意したのみに私物端末の利用を認める（OS の更新により業務用アプリが正常動作しなくなる可能性について留意が必要）	対策の実施が前提
業務用アプリのインストール	・業務用アプリのインストール可能な端末を所有していて、かつインストールに合意した者のみに私物端末の利用を認める	インストールすることが前提
点検内容の明確化	・業務用アプリ、MDM や MAM により点検を自動化する ・あらかじめ点検内容を明確化し、合意した者のみに私物端末の利用を認める	業務専用端末には私的な情報が存在しないので、点検内容を明確化する必要はない

6. 実施手順の整備

スマートフォン等の業務利用に当たって、情報セキュリティ対策を適切に講じるためには、運用管理体制を明確化し、運用管理手順及び職員の利用手順を定める必要がある。

この際に、利用者の IT に関する知識水準は様々であることから、利用者に求める対策はできるだけわかり易くシンプルなものとすることが重要である。

なお、私物のスマートフォン等を業務利用する場合は、私的な利用に対する一定の配慮を行いつつも、業務利用においては厳格なルールの下で利用する手順としなければならない。

6.1 責任者の設置と運用管理体制の整備

府省庁の職員がスマートフォン等を用いて業務遂行するに当たって、端末の安全管理措置の実施状況を管理する責任者を定める。

当該責任者は、IT や情報セキュリティに係る一定の知見を有している者が当たることが望ましい。端末の配備の形態や業務利用の形態により、どのような者がその任に当たるのかは様々であるが、例えば、携帯電話として課室等の組織のまとまりごとに職員にスマートフォン等を配布する場合は、課室情報セキュリティ責任者がその任に当たり、府省庁 LAN 端末と同じように、スマートフォン等を情報システム部門が配備して運用管理を行う場合は、府省庁 LAN の情報システムセキュリティ責任者がその任に当たることが考えられる。図６－１に府省庁における運用管理体制のイメージを示す。

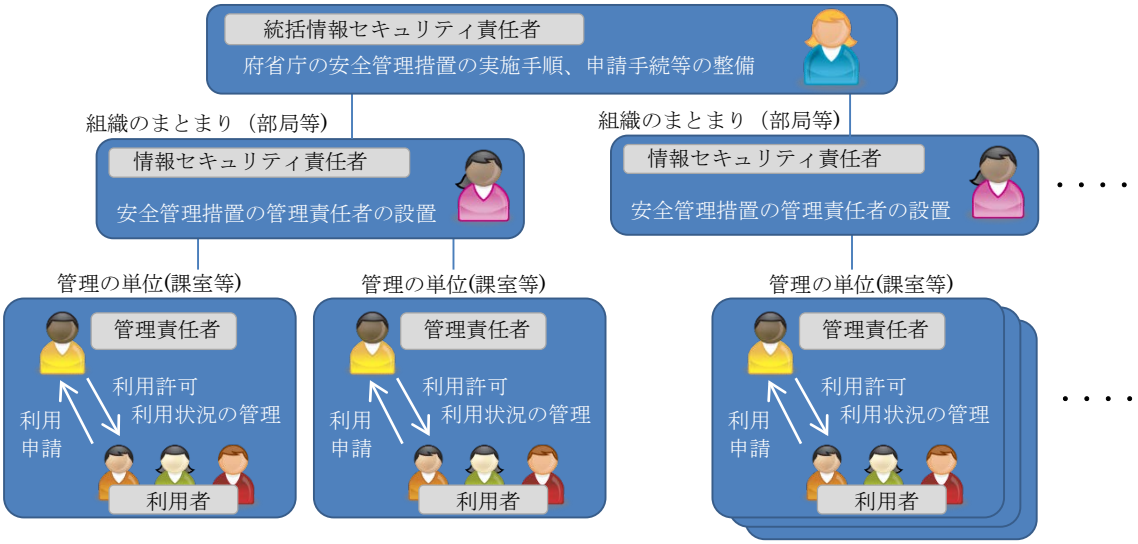

図６－１　府省庁における運用管理体制のイメージ

6.2 利用手順の整備

スマートフォン等を職員に貸与する場合の利用手順として考慮すべき事項を示す。私物端末を業務利用する場合は、府省庁支給端末のみを利用する場合と申請手続や確認事項が異なる場合があることに留意する必要がある。

(1) 利用申請書

利用申請書の記載事項の例を以下に示す。この他に必要な要件を適宜補完し、申請書及び利用手続を整備する。

- 申請日
- 申請者情報（氏名、所属、連絡先電話番号）
- 申請理由又は利用目的（可能ならば説明用の資料を添付）
- 利用対象の業務又は利用する情報
- 利用する端末
- 利用期間（最大利用期間をあらかじめ定めておくとよい）
- 主たる利用場所
- 利用形態（組織が利用形態を指定する場合は不要）

利用に当たって、安全管理措置等の利用手順を遵守することについて申請書等にチェック欄を設けて、利用者の誓約を得ることも考えられる。

なお、要機密情報の庁舎外への持ち出し等に係る申請が別途必要になることが考えられるため、本手続の際に併せて申請されるよう申請手順書等に整理しておくとよい。

(2) 端末の利用開始時の手順

利用申請が受理されるなどして、スマートフォン等の業務利用を開始する際の端末の設定手順について、端末の安全管理措置が適切に行われるように、セキュリティ対策に係る手順を含む要件をあらかじめ決定しておく。端末の設定を端末管理者が行うか、利用者自らが行うかについても明確にしておくとよい。

- 端末ロック、データワイプ機能の設定
- ソフトウェアのバージョン確認
- リモートアクセス用アプリのインストール及び初期設定
- 不正プログラム対策ソフトウェアのインストール及び初期設定
- 上記以外に業務に必要なアプリのインストール及び初期データ設定
- 不要な機能の削除又は停止に関する設定

さらに、業務用システムの利用に際して必要となる利用者の認証情報等、サーバの設定情報に関する入力手順についても併せて整備しておくとよい。

(3) 端末利用中の安全管理措置等に関する実施手順

利用申請が許可されて端末が貸与された後は、端末の安全管理措置は、利用者自身が責任をもって実施する必要があることから、以下を例とする安全管理措置の実施手順をあらかじめ整備し、利用者に適切に実施させる必要がある。

- 業務用アプリのセキュリティ機能に係る利用手順
- 端末ロック、データワイプ機能等の設定に係る手順
- 業務用アプリ、OS等のソフトウェア更新の手順
- 端末内情報の秘匿性確保に関する実施手順（端末内にデータを保存する場合）
- その他のセキュリティ対策手順（盗難・紛失対策、画面のぞき見対策等）
- 端末利用に係る禁止事項

また、利用者が遵守すべき端末の利用手順に関する注意事項を表６－１に示す。安全管理措置を利用者に適切に実施させるために、例えば以下の事項を利用条件として、利用者自身に確認させることも考えられる。

表６－１　利用者が遵守すべき端末の利用手順に関する注意事項の例

分類	職員が留意すべき事項
利用の原則	行政事務の遂行以外の目的で端末を利用しないこと
	不要不急な業務においては極力利用しないこと
	不要な情報は端末に残留させず、速やかに消去すること
	他の手段が無い場合に限り利用すること
利用手順の遵守	利用手順を遵守すること
	定められた手順以外の方法で業務を行わないこと
	手順外の処理を行う必要が生じた場合は、事前に責任者の許可又は承認を得ること
	利用を終了した場合は、速やかに手続すること
	利用中にインシデント等が発生した場合は、手順に従って管理者等へ速やかに連絡し、必要な措置を講ずること
端末管理の徹底	盗難・紛失が起こらないように、日常的に端末の管理を厳重に行うこと
	家族や知人、第三者が端末操作や画面をのぞき見する行為に注意すること
禁止事項	管理責任者の許可なく、端末の設定を変更しないこと
	安全性が確認できないアプリケーションや利用が禁止されているソフトウェアをインストールしないこと
	許可された通信回線以外に接続しないこと
	PC に接続しないこと（充電等の場合であっても NG）
	端末は家族や知人、第三者に端末を貸与しないこと

(4) 利用終了時の手順

利用申請期間が満了した場合又はスマートフォン等を用いて業務を実施する必要がなくなった場合には、利用者から利用終了手続の申請を受け付ける。その際は、端末管理部門において、返却物品の確認、台帳との照合、台帳の更新等を実施する。

また、返却された端末や端末利用に係る情報システムの設定等について、不要なデータの削除を行う。

(5) 端末の盗難・紛失時の対処手順

端末の盗難・紛失が発生した場合の対処手順についてあらかじめ整備し、全利用者に周知する。また、端末の故障時の対処手順についても規定するとよい。

対処手順に含める事項としては、以下が考えられる。

- 報告受付窓口（組織、役職名 等）
- 報告内容（盗難・紛失した場所、時間、対処状況等）
- 対処手順（端末ロック、データワイプ、通信事業者への連絡）
- 端末の所在の確認
- 関係機関、所轄警察署への連絡

なお、端末の盗難・紛失が確定していない場合であっても、そのおそれがある場合は報告するよう、手順に定め、職員にも周知しておくとよい。

(6) 私物端末の利用手順

私物のスマートフォン等を業務利用する場合においても、府省庁支給の端末と同等の情報を扱うためには、同等の情報セキュリティ水準が確保されなければならない。

5.6 節に示す私物端末の業務利用に際して留意すべき事項を参考に利用手順を考慮する必要がある。また、費用負担や利用手順の遵守以外に、表６－２に例示する内容について、利用者とあらかじめ合意しておくことが考えられる。この際に、利用条件について利用者が合意したことを示す証拠として誓約書等の文書に合意事項ごとのチェックマークにチェックし、利用者のサインを記入させるなどし、保管しておくとよい。

表６－２　私物端末の業務利用に際して、組織と職員で合意しておくべき事項

分類	項目	合意しておくべき事項	合意上の注意事項
表明保証	名義、契約者	利用する端末の契約者が職員本人であることについて合意する。	職員外の契約者を認める場合は、その条件を明確にする。
管理	業務情報の保護	業務情報の業務外利用の禁止や業務利用終了時の処理等について合意する。	業務利用時以外は、情報システムや業務情報へのアクセスを禁止することを条件とする。
	組織による情報収集に対する個人の承諾（組織として端末管理を行う場合）	不正な利用や不正プログラムへの感染等を確認するために、スマートフォン等の利用状況の収集を行うことについて合意する。	プライバシーに係る情報を含むことから、利用者の事前合意は必須。システム的な情報収集、管理者による情報確認、どちらも含む。
	組織による端末の制御に対する個人の承諾（組織として端末管理を行う場合）	設定変更、機能制限やデータ削除等の制御を組織として行うことについて合意する。	OS やアプリの推奨構成を提示する。 事故対応時の対処（プライベート情報含めてデータワイプ等）について明記しておく。
	バックアップデータの管理（端末に業務情報を保存する場合）	バックアップデータの管理を適切に行うことについて合意する。	私物端末以外へは業務情報を保管しない等の安全管理措置の実施手順を定めておく。
届出	特定の事象が発生した場合の届出	盗難・紛失等の事故が発生した場合、直ちに届出ることについて合意する。	機種変更や譲渡等の際の届出も含んだルールを組織として定めておく。
禁止事項	端末、OS、アプリの改造	改造しないことについて合意する。	－
	組織が禁止指定しているアプリの導入	マルウェア等の侵入を防ぐため、禁止指定されているアプリを導入しないことについて合意する。	導入してはいけないアプリを別途定める。
	第三者への貸与	本人以外の利用を禁止することについて合意する。	代替手段（貸与時は業務用アプリをロック等）も考慮。
	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しないことについて合意する。	技術的に排除できる場合は、合意事項に含めなくてもよい。
	故意又は過失による情報漏えい	情報漏えい時にはルールに従い対処することについて合意する。	利用者への注意喚起が目的であり、対処手順について併せて説明する。
利用の終了	業務情報、業務用アプリの削除	業務情報や業務用アプリを削除する運用を行うことについて合意する。	－
合意事項違反	合意事項違反時の措置	合意事項違反行為が発生した場合等に利用を禁止することについて合意する。	“多発した場合”等の条件にすることも考えられる。

※出展

CIO 補佐官等連絡会議情報セキュリティ WG BYOD 要件検討 SWG 報告書より抜粋（一部修正）

6.3 運用管理手順の整備

端末の安全管理措置の実施状況を管理するため、管理責任者は、端末管理手順に係る要件について、取り扱う情報や利用目的に応じたリスク対応の方針に従い定める必要がある。不正プログラムへの感染や端末の不正な改造による情報漏えい等のリスクが高い場合は、利用状況について厳しく管理することが求められるが、端末の安全管理措置の実施水準に依存せずに一定のセキュリティが確保される方式を採用しているのであれば、端末管理手順もシンプルなものになると考えられる。

(1) 運用管理手順

情報セキュリティ対策に関連する運用管理手順に含めるべき項目の例を以下に示す。

- 端末のソフトウェアバージョンの定期的な確認手順
- 更新ソフトウェアのリリースの有無の確認手順
- 利用するソフトウェア及び提供事業者に関する最新の情報の確認手順
- 業務用アプリ、OS 等のソフトウェア更新の実施手順
- 不正プログラム対策ソフトウェアの稼働状況の確認手順
- アプリケーションのインストール状態の確認手順
- 改造の有無等の確認手順
- アクセスログの取得及び管理手順
- 端末の各種設定状態の管理及び更新手順

(2) バックアップの手順

スマートフォン等に保存されているデータのバックアップ方式を決定する。端末ベンダや通信事業者等がクラウド上にデータバックアップを行うサービスを提供しているが、業務情報をそれらのクラウド上に保存することは望ましくないことから、データバックアップの必要がある場合は、業務用のデータバックアップ環境を別途準備しておく必要がある。

バックアップの対象となるデータとしては、例えば以下が考えられる。

- 業務用のアドレス帳
- 業務用アプリ
- 業務用アプリに保存されている業務情報

（別紙１）　政府機関統一基準群と本書の主な規定内容の関係

※統一基準群の項番のうち、無印のものは遵守事項の項番を示す。
また、<基>と記されているものは、府省庁対策基準策定のためのガイドラインにおいて基本対策事項として規定されているものを示す。

本書の記載箇所 及び規定内容		統一基準 群の項番 ※	規定内容
5.1	端末や OS の種類	7.1.1(1)(c)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。 （端末の種類の選択については規定なし）
		<基> 7.1.1(1)-5	情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。 a)ソフトウェアベンダのサポート状況
5.2	端末機能・サービスの要件	7.1.1(1)(c)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。
		<基> 7.1.1(1)-5	情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。 a)ソフトウェアベンダのサポート状況 b)ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容 c)インストール時に同時にインストールされる他のソフトウェア
		8.1.1(2)(a)	情報システムセキュリティ責任者は、行政事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。
		<基> 8.1.1(2)-1	情報システムセキュリティ責任者は、府省庁外のウェブサイトについて、行政事務従事者が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。 a)ウェブサイトフィルタリング機能 b)事業者が提供するウェブサイトフィルタリングサービスの利用
		<基> 8.1.1(2)-2	情報システムセキュリティ責任者は、行政事務従事者が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。 a)受信メールに対するフィルタリング機能
5.3	業務用アプリの導入	6.1.5(1)(a)	情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。 (ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。
		6.1.5(1)(b)	情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用

			する暗号及び電子署名のアルゴリズム及び運用方法について、以下の事項を含めて定めること。
		7.1.1(1)(c)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。
		<基> 7.1.1(1)-5	情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。 d)その他、ソフトウェアの利用に伴う情報セキュリティリスク
5.4	通信回線の要件	7.3.1(1)(a)	情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。
		7.3.1(1)(b)	情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。
		7.3.1(1)(c)	情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。
		<基> 7.3.1(1)-2	情報システムセキュリティ責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、SSL（TLS）、IPsec 等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。
		7.3.1(4)(a)	情報システムセキュリティ責任者は、VPN 回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。
		<基> 7.3.1(4)-1	情報システムセキュリティ責任者は、VPN 回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。 b)通信を行う端末の識別又は認証 c)利用者の認証 d)通信内容の暗号化 e)主体認証ログの取得及び管理 f)リモートアクセスにおいて利用可能な公衆通信網の制限 g)アクセス可能な情報システムの制限
		7.3.1(5)(a)	情報システムセキュリティ責任者は、無線 LAN 技術を利用して府省庁内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。
5.5	情報セキュリティ対策要件 (1) ソフトウェアの脆弱性対策	6.2.1(1)(a)	報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。
		<基> 6.2.1(1)-1	情報システムセキュリティ責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手すること。 a)脆弱性の原因 b)影響範囲 c)対策方法 d)脆弱性を悪用する不正プログラムの流通状況

		<基> 6.2.1(1)-3	情報システムセキュリティ責任者は、構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること
		6.2.1(1)(c)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること
5.5	情報セキュリティ対策要件 (2) 不正プログラム対策	6.2.2(1)(a)	情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。
5.5	情報セキュリティ対策要件 (3) のぞき見防止対策	7.1.1(1)(a)	情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。
		<基> 7.1.1(1)-3	情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスののぞき見を防止するために、以下を例とする対策を講ずること。 a)一定時間操作が無いと自動的にスクリーンロックするよう設定する。 b)要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。
5.5	情報セキュリティ対策要件 (4) 盗難・紛失対策	7.1.1(1)(b)	情報システムセキュリティ責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。
		<基> 7.1.1(1)-4	情報システムセキュリティ責任者は、第三者により情報窃取されることを防止するために、以下を例とする、端末に保存される情報を暗号化するための機能又は利用者が端末に情報を保存できないようにするための機能を設けること。 a)端末に、ハードディスク等の電磁的記録媒体全体を暗号化する機能を設ける。 b)端末に、ファイルを暗号化する機能を設ける。 c)ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。 d)仮想クライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。 e)セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。 f)ハードディスク等電磁的記録媒体に保存されている情報を遠隔から消去する機能（遠隔データ消去機能）を設ける。
		8.2.1(1)(d)	前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。
		<基> 8.2.1(1)-3	情報システムセキュリティ責任者は、府省庁支給以外の端末により要機密情報を取り扱う府省庁の情報システムにリモートアクセスする環境を構築する場合、基盤となる情報システムにより各府省庁に提供されるリモートアクセス環境が利用可能であれば活用し、端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するために、以下を例とする対

			策を講ずること。 a)仮想クライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用の仮想クライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 b)セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。 c)ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。利用者は専用のアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
5.5	情報セキュリティ対策要件 (5) ログ管理機能の導入	6.1.4(1)(a)	情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行う必要がある場合、ログを取得すること。
		6.1.4(1)(b)	情報システムセキュリティ責任者は、情報システムにおいて、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。
		6.1.4(1)(c)	情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。
5.5	情報セキュリティ対策要件 (6) 端末管理ツール(MDM)の導入	6.2.1(1)(d)	情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。
		6.2.2(1)(c)	情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。
		<基> 6.2.2(1)-5	情報システムセキュリティ責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。 a)不正プログラム対策ソフトウェア等の導入状況 b)不正プログラム対策ソフトウェア等の定義ファイルの更新状況
		7.1.1(1)(c)	情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。
		<基> 7.1.1(1)-5	情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。 d)その他、ソフトウェアの利用に伴う情報セキュリティリスク
		8.1.1(2)(a)	情報システムセキュリティ責任者は、行政事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。
5.6	私物端末の業務利用に際して留意すべき事項	8.1.1(2)(a)	情報システムセキュリティ責任者は、行政事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。
		8.2.1(1)(b)	統括情報セキュリティ責任者は、要機密情報について府省庁支

			給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。
		8.2.1(1)(d)	前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。
6.1	責任者の設置と運用管理体制の整備	8.1.1(1)(b)	統括情報セキュリティ責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。
		<基> 8.1.1(1)-3	統括情報セキュリティ責任者は、要管理対策区域外にて行政事務従事者が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、行政事務従事者に遵守させること。 a)許可権限者の決定（情報システムセキュリティ責任者又は課室情報セキュリティ責任者が想定される。）
		8.2.1(1)(c)	情報セキュリティ責任者は、府省庁支給以外の端末による行政事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定めること。
6.2	利用手順の整備	8.1.1(1)(b)	統括情報セキュリティ責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。
		<基> 8.1.1(1)-3	統括情報セキュリティ責任者は、要管理対策区域外にて行政事務従事者が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、行政事務従事者に遵守させること。 b)利用時の許可申請手続 c)手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等） d)利用期間満了時の手続 e)許可権限者による手続内容の記録
		8.1.1(3)(a)	行政事務従事者は、行政事務の遂行以外の目的で情報システムを利用しないこと。
		8.1.1(3)(b)	行政事務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に府省庁の情報システムを接続しないこと。
		8.1.1(3)(c)	行政事務従事者は、府省庁内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。
		8.1.1(3)(d)	行政事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。
		8.1.1(3)(e)	行政事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。
		8.1.1(3)(f)	行政事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。
		8.1.1(3)(g)	行政事務従事者は、機密性３情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場

			合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。
		8.2.1(1)(a)	統括情報セキュリティ責任者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。
		<基> 8.2.1(1)-1	統括情報セキュリティ責任者は、以下を例に府省庁支給以外の端末を利用する際の許可等の手続に関する手順を整備し、行政事務従事者に周知すること。 a)以下を含む府省庁支給以外の端末利用時の申請内容 ・申請者の氏名、所属、連絡先 ・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合） ・利用する端末の機種名 ・利用目的、取り扱う情報の概要、機密性３情報の利用の有無等 ・主要な利用場所 ・利用する主要な通信回線サービス ・利用する期間 b)利用許諾条件 c)申請手順 d)利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順 e)利用期間満了時の利用終了又は利用期間更新の手続方法 f)許可権限者（遵守事項 8.2.1(1)(c)において定める、府省庁支給以外の端末の安全管理措置の実施状況を管理する責任者（以下、この項において「端末管理責任者」という。））
		8.2.1(2)(a)	行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、遵守事項 8.2.1(1)(c)で定める責任者の許可を得ること
		8.2.1(2)(b)	行政事務従事者は、要機密情報を府省庁支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。
		8.2.1(2)(c)	行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、府省庁にて定められた手続及び安全管理措置に関する規定に従うこと。
		8.2.1(2)(d)	行政事務従事者は、情報処理の目的を完了した場合は、要機密情報を府省庁支給以外の端末から消去すること。
6.3	運用管理手順の整備	7.1.1(2)(a)	情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。
		7.1.1(2)(b)	情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。
		7.1.1(3)(a)	情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。
		8.1.1(1)(a)	統括情報セキュリティ責任者は、府省庁の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。
		<基> 8.1.1(1)-1	統括情報セキュリティ責任者は、府省庁の情報システムの利用のうち、情報セキュリティに関する規定として、以下を例とする実施手順を定めること。 a)情報システムの基本的な利用のうち、情報セキュリティに関する手順 b)電子メール及びウェブの利用のうち、情報セキュリティに関する手順 c)識別コードと主体認証情報の取扱手順

			d)暗号と電子署名の利用に関する手順 e)不正プログラム感染防止の手順
		8.1.1(1)(b)	統括情報セキュリティ責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。
		<基> 8.1.1(1)-2	統括情報セキュリティ責任者は、要管理対策区域外にて情報処理を行う際の安全管理措置として、以下を例とする措置を規定し、行政事務従事者に遵守させること。 a)モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化 b)のぞき見に対する対策（のぞき見防止フィルタの利用等） c)盗難・紛失に対する対策（不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど） d)利用する場所や時間の限定 e)端末及び外部電磁的記録媒体等についての盗難・紛失が発生した際の緊急対応手順
		8.2.1(1)(b)	統括情報セキュリティ責任者は、要機密情報について府省庁支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。
		<基> 8.2.1(1)-2	統括情報セキュリティ責任者は、府省庁支給以外の端末により要機密情報を取り扱う場合は、行政事務従事者が講ずるべき安全管理措置の実施手順について、以下を例に整備すること。 a)パスワード等による端末ロックの常時設定 b)OS やアプリケーションの最新化 c)不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（府省庁として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める） d)遠隔データ消去機能の設定 e)要機密情報の暗号化等による秘匿性の確保 f)端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある） g)府省庁提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ） h)以下を例とする禁止事項の遵守 ･端末、OS、アプリケーション等の改造行為 ･安全性が確認できないアプリケーションのインストール及び利用 ･利用が禁止されているソフトウェアのインストール及び利用 ･許可されない通信回線サービスの利用（利用する回線を限定する場合） ･第三者への端末の貸与
		8.2.1(1)(d)	前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。