私物端末の公的利用ガイドライン

国立高等専門学校機構

平成 27 年 9 月（Ver.1）

目次

１．はじめに

昨今，ノート（モバイル）パソコンをはじめ，パソコンと比べても機能的にそんしょくのないスマートフォンやタブレット（以下,「携帯型端末」と言う。）を持ち歩く人が増えています。学校内を含めて，いつでもどこでも利用可能な携帯型端末は，もはや現代人にとってなくてはならない必須ツールであるといっても過言ではなく，学校に携帯型端末を持ち込んで校内ネットワークに接続して利用したり，便利さゆえに授業等の教育や業務等で利用（以下,「公的利用」と言う）する状況も考えられます。

個人で所有している携帯型端末や自宅等に設置しているデスクトップパソコン等（以下,「私物端末」と言う。）を公的利用する形態は,「BYOD（Bring Your Own Device)」と呼ばれます。私物端末を公的利用するにあたっては，BYOD が持つ危険性とその対応策について正しく理解しておくことが不可欠です。

本ガイドラインは，学生及び教職員を対象とした，私物端末の公的利用についてのガイドラインとなり，利用する皆さんにとっての良き道しるべとなることを期待します。

なお，私物端末の公的利用の可否や情報の取扱については，各高専の規程・規則等に従って運用いただきますようお願いします。本ガイドラインは「利用を許可されている場合の留意事項」という位置づけとなり，利用を許可するものではありません。

２．私物端末の公的利用の特徴と危険性

携帯型端末は盗難や紛失の脅威を考慮する必要があります。デバイス本体だけでなく SIM カードが抜き取られる恐れもあります。落下や水没による故障や，公共の場での置き忘れ，覗き見も懸念されます。さらに，パソコンに匹敵するネットワーク接続性を持つ携帯型端末では，不正アクセスやウイルス感染といった情報セキュリティリスクも当然あります。むしろ，パスワード保存といった操作の簡略化があだとなり，情報セキュリティリスクはパソコンよりも高くなっているほどです。私物端末の利用において当たり前になっているクラウドサービスの利用も情報セキュリティリスクを高める一因となっています。個人情報や機密情報をクラウドサービスに保管することによって，情報漏洩の際の追跡範囲が学外のサービスにまで拡散する危険性もあります。

３．基本的な考え方

（１）私用と公用を混同しないように工夫する

個人情報や機密情報を誤って関係者外に送ってしまったりしないように，アドレス帳やメールフォルダ，データ保管フォルダを分けておくことが必要です。特にスマートフォンユーザでの利用が多いショートメッセージサービス（SMS 等）を利用したメールでは，パソコンメールと違ってタイトルとシグネチャ（署名）を付けずに送ることが一般的なため，相手や用件を混同する危険があります。公用でショートメッセージサービスを使うのは避けるようにしてください。

（２）不適切な機器やアプリを使用しない

改造機器や脱獄アプリなどを使用しないようにしてください。これらを使用するとメーカーからの保証やサポートを受けられなくなる上，不正アクセスやウイルス感染を受けやすくなります。また，違法コピーされたアプリや海賊版ソフトなども使用してはいけません。

（３）情報セキュリティに対する自己責任を果たす

普段から，紛失や盗難，不正アクセス，ウイルス感染に注意することが必要です。私用で使用する場合においても，放置することなく注意を持って携帯，保管してください。不正アクセス，ウイルス感染から私物端末を守るためにセキュリティ設定も最大限に設定しておくことが必要です。一つの私物端末で公用と私用を使い分ける以上，情報セキュリティに対する自己責任を果たすことが不可欠となることを認識しておかねばなりません。

（４）私用においても適切な利用を心がける

私用で私物端末を使用する場合でも，違法なコンテンツサイトや不適切なアプリの利用は避けてください。通常使用しているアプリやサイトであっても，誤送信や不適切な投稿をしないように注意してください。また，ソーシャルメディアの利用においては私用アカウントであっても不適切な投稿をしないよう注意することが必要です。常に組織に属する者としての自覚をもって適切な行動を心がけてください。

４．私物端末の公的利用上の注意点

＜設定に関すること＞

（１）ロック機能を設定する

ロックをはずさないと利用できないよう設定を行ってください。また，ログインに連続で失敗するとロックされる設定及び，一定時間放置するとロックされる設定も併せて行うようにしてください。

（２）不要な接続機能をオフにする

使用しないNFC（Near Field Communication：近距離無線通信）やBluetooth，赤外線通信をオフにするようにしてください。

（３）ユーザIDを使い分ける

私用で使用するアプリやサービスのユーザIDや連絡用メールアドレスに公用のメールアドレスを使用しないようにしてください。

（４）しっかりしたパスワードを設定する

アプリやサービスなどのログインパスワードは推測困難な英数字混在（可能であれば記号も含める）の長い文字列とし，複数のアプリやサービス間で同一のパスワードを設定しない（例えば，公用と私用のパスワードを同一にしない等）ようにしてください。

（５）私物端末上の公私データを区別する

私物端末上で写真や資料を保管する場合は，フォルダ分けするなどして公私を区分することが必要です。

（６）クラウドストレージ上の公私データを区別する

iCloudやDropBoxなどクラウドストレージ上でデータ保管する場合は，フォルダ分けするなどして公私を区分することが必要です。なお，個人情報や機密情報は，クラウドストレージ上に保管しないようにして下さい。

（７）必要もなくアプリに機能使用や位置情報の取得を許可しない

アプリケーションのインストール時に，必要もなくアプリに機能使用や位置情報の取得を許可しないように注意することが必要です。

（８）セキュリティ対策を講じる

ＯＳやアプリのアップデートを適切に行うことや，ウイルス，スパイウェア等のマルウェアや不正なアプリが混入しないように，セキュリティ対策ソフト（アプリ）をインストールし，適切にセキュリティ設定をしてください。また，サポートが終了したＯＳやアプリは使用しないようにしてください。

（９）紛失時のロック，リモートワイプ機能を設定しておく

携帯型端末で，特に公用の個人情報や機密情報を取り扱う場合，盗難や紛失した場合に備え，端末ロックや位置追跡，リモートワイプ（遠隔操作によるデータ消去）できるように機能設定しておくことが必要です。

＜利用に関すること＞

（10）ネットワーク接続に注意する

無線スポットへの自動接続を設定しないようにしてください。また，不審な無線スポットに接続しないように注意することが必要です。テザリング（インターネット共有）を利用する場合はパスワード設定と接続台数を確認し，他人から不正アクセスされないように注意する必要があります。

（11）外部記憶媒体の紛失に注意する

アドレス帳などのデータを外部記憶媒体に保管する場合は，盗難や紛失に注意する必要があります。外部記憶媒体上の不要なデータはそのままにしておかずに確実に削除することが必要です。

（12）公用の連絡先を共有しない

アドレス帳をLINEなどでアドレス帳共有してはいけません。LINEを利用する場合は，公用のアドレス帳が共有されてしまわないように設定しておく必要があります。

（13）無料通話には注意する

公用でLINEなどの無料電話を使用しないようにしてください。パケット通信を利用した無料電話は盗聴の恐れがある上，アドレス帳共有する不特定多数によるいたずらや違法な行為を受ける可能性もあり，そのような事案が発生した場合，社会的な信用失墜につながります。

（14）メールアドレスやフォルダを使い分ける

私用メールと公用メールとでメールアドレスを変えたり，メールフォルダを区別したりするなどして混同しないように設定しておくことが必要です。

（15）カメラ使用に注意する

機密情報など学校（授業等の教育や業務等）で知り得た情報を無断でカメラ撮影や録画してはいけません。機密情報でなくても学校や外出先での出来事を勝手に撮影や録画することはプライバシー侵害や名誉毀損となる恐れがあるだけでなく，社会的な信用失墜につながります。

（16）マイク使用に注意する

機密情報など学校（授業等の教育や業務等）で知り得た情報を無断でマイク録音してはいけません。機密情報でなくても職場や学校や外出先での出来事を勝手に録音することはプライバシー侵害や名誉毀損となる恐れがあるだけでなく，社会的な信用失墜につながります。

（17）授業や業務中のワンセグやラジオ利用に注意する

授業や業務中に，ワンセグやラジオを利用してはいけません。

（18）スマートフォンを家族や他人に使わせない

授業等の教育や業務等に用いる私物端末を，家族や他人に使わせてはいけません。

＜運用に関すること＞

（19）私物端末の公的利用の許可を受ける

私物端末を公的利用する場合は，各高専の規程・規則等に従って，事前に利用許可を受ける必要があります。機種変更及び追加の場合も同じです。

（20）機種変更などによる機器廃棄時の公用データを削除する

公的利用により私物端末内に保持された情報は，すべて組織の資産であり，個人による私的な再利用は認められません。機種変更などで不要となった私物端末を廃棄する場合は，確実に公用のアドレス帳やデータを削除しなければなりません。卒業や修了時，人事異動や退職時の場合も同じです。

（21）USB 接続による充電を行わない

スマートフォンやタブレットの充電にパソコン等への USB 接続による方法をとらないようにしてください。特に自宅外でのパソコン等への USB 接続は不正アクセスとみなされる恐れがあります。また，知らないうちにデータを閲覧・窃取される危険性もあります。専用の電源アダプタを使用するなどして直接電源から充電するようにしてください。

（22）制限エリアに持ち込まない

機密エリアなど機器持込の制限エリアには，携帯型端末を持ち込んではいけません。

（23）電子証明書を管理する

教育用システムや業務用システムの利用などのために電子証明書を使用するように指示された場合，その電子証明書を無断でエクスポート（データ出力や他人へのコピー等）をしてはいけません。

（24）モバイル端末管理（MDM）を削除しない

端末管理のために，モバイル端末管理のアプリをインストールするように指示された場合は，そのアプリを削除したり止めたりしてはいけません。

（25）私物端末の公的利用の終了

異動や退職，卒業など，なんらかの要因によって私物端末の公的利用を終了することになった場合は，スマートフォンの中だけでなく利用しているクラウドサービスなど全ての関連先から公的利用上のアドレス帳やデータを確実に削除しなければなりません。パソコンやクラウドとの間で障害対策のためにバックアップや同期設定している場合は，私物端末の公的利用終了時にスマートフォンだけでなく，パソコンやクラウド上にバックアップや同期されている業務上のアドレス帳やデータも確実に削除する必要があります。