文書番号		モバイルPC使用基準	頁	1/9	
版　数	1		承　認	承　認	作　成
制 定 日	2019年4月1日				
改 訂 日	2019年4月1日				
実施開始日	2019年4月1日				

目次

1.本書の目的

1-1.目的

本文書は、モバイル PC の管理や遵守事項に関する基準文書である。業務で使用するモバイル PC を限定した上で使用方法を明確にすることで、社外でのモバイル PC 使用にともなう情報の漏えい、改ざん、破壊等を防止することを目的とする。

1-2.対象者

当社の従業員等で業務にモバイル PC を使用するすべての者。

2.定義

(1) 「モバイル PC」とは、社外に持ち出し可能なパソコンをいう。
(2) 「外部サービス」とは、メールやグループウェア等、社外の事業者がクラウド上で提供しているサービスをいう。
(3) 「モバイルデバイス」とは、「モバイル PC」と「スマートデバイス」の総称とする。
(4) 「スマートデバイス」とは、スマートフォンやタブレット等、パソコンと異なり、キーボードを使わず指やタッチペンにてタッチスクリーンを操作する端末をいう。
(5) 「PC」とは、社内に設置された社内 LAN パソコン（仮想 PC も含む）、モバイル PC の総称とする。
(6) 「電子媒体」とは、USB メモリ等可搬型の大容量記録媒体をいう。
(7) 「情報機器」とは、PC、モバイルデバイス、電子媒体の総称とする。
(8) 「周辺機器」とは、キーボード、マウス等、ケーブル等で情報機器に接続する機器をいう。
(9) 「当社」とは、池田糖化グループをいう。
(10) 「従業員等」とは、当社の役員及びこれに準じる者並びに従業員（嘱託、パートタイマー、アルバイト、派遣社員及び当社の関係会社からの受入者を含む。）をいう。
(11) 「ITS」とは、アイティエス システム部門をいう。

3.使用範囲

3-1.使用対象者

モバイル PC の使用対象者は、以下の条件を満たすことを必須とする。

(1) 「誓約書」を提出した者。
(2) 集合教育、または e-Learning 研修にてモバイル PC 使用に関する教育の受講を完了した者。
(3) 「IT・セキュリティに対するリテラシー」 を有する者。

3-2.対象機器

業務で会社資産の情報を取り扱うことができるモバイル PC は以下とし、私有のモバイル PC を業務に使用しないこと。

(1) ITS が使用を許可した社有のモバイル PC。

なお、使用を許可されたモバイル PC には、必ず許可されたことを示すシール等を他の従業員等から視認できる位置に貼付すること。

3-3.使用可能なソフトウェア

モバイル PC で使用が可能なソフトウェアは「使用可能なソフトウェアおよび外部サービス一覧」に記載されているソフトウェアのみとする。

なお、「使用可能なソフトウェアおよび外部サービス一覧」以外のソフトウェアで、業務上必要なソフトウェアがある場合は、「使用可能なソフトウェアおよび外部サービス一覧」に追加する必要があるため、個別に ITS に確認すること。

3-4.使用可能な外部サービス

モバイル PC で使用可能な外部サービスについては別途用意する「使用可能なソフトウェアおよび外部サービス一覧」に記載されているサービスのみとする。

なお、「使用可能なソフトウェアおよび外部サービス一覧」に記載されているサービス以外で、業務上必要な外部サービスは、個別に ITS に確認すること。

3-5.使用可能なネットワーク

モバイル PC を社内ネットワークに直接接続してはならない。

また、社外ネットワークへアクセスする場合、以下の通信手段のみ許可する。

(1) 通信事業者が提供する通信手段（4G/3G 等）
(2) 以下の Wi-Fi
    ① 社有のポータブル Wi-Fi 機器
    ② 社有のスマートフォンのテザリング
    ③ 自宅の Wi-Fi 機器、ホテルが提供するインターネット接続サービス
    ④ 拠点に据え置きする会社が用意した Wi-Fi 機器

使用にあたっては、別紙「Wi-Fi アクセスポイント使用時の留意点」に記す事項に留意すること。

4. モバイル PC の管理

4-1. 支給

4-1-1. 使用申請

(1) モバイル PC の支給を受ける者は事前に以下を提出すること。

① 「情報機器設置・支給申請書」

4-1-2. 受け取り

(1) 本基準に記載している遵守事項を遵守すること。

(2) 情報機器毎に定められた導入手順書等に従い、初期設定を行うこと。

(3) 必要に応じて、プライバシーフィルタ等の取り付けを行うこと。

4-1-3. 更新

(1) 経年劣化、修復不可能な故障、使用目的の変更等、やむを得ない理由により、モバイル PC の機種を変更する場合は、IT 推進委員等の担当者から代替機の支給または貸出を申請し、代替機到着時に使用中のモバイル PC を返却すること。

4-2. 使用時

4-2-1. パスワード設定

(1) モバイル PC のパスワードは ITS の指示に従い、各自が設定すること。

(2) モバイル PC のパスワードを第三者に開示しないこと。

(3) モバイル PC のパスワードを手帳等に記入する場合は、モバイル PC と一緒に管理（保管）しないこと。

4-2-2. 物理セキュリティ対策

(1) モバイル PC の他者への使用の制限

① 使用者は、モバイル PC のロック機能（パスコード、生体認証等）を有効にし、第三者が無断でモバイル PC を使用できないようにすること。

② ロック画面上に表示する通知などの情報は最小限にすること。

③ ロック解除方法が第三者に漏れないようにすること。

④ 一定時間未使用時に自動的に画面をロックするよう設定すること。
（推奨時間 3 分）

⑤ モバイル PC を他人に譲渡・貸与しないこと。

⑥ 離席する場合、モバイル PC を机の上等に放置しないこと。

(2) データ転送および充電

① 社有のモバイル PC に私有の情報機器・電子媒体・スマートデバイス等を接続しないこと。

② カードリーダー等､社有品であっても接続が許可されていない周辺機器を接続しないこと。

(3) 社外持ち出し時の注意事項

① ローカル（端末内に保存される領域）に不要なデータがないことを確認の上、持ち出すこと。

② 移動時の交通機関や人混みの中では、盗難に遭わないよう、適切にモバイル PC を取り扱うこと。
③ 紛失防止のため、モバイル PC は常に手元に置き、放置しないこと。
④ 社外でモバイル PC を使用する際は、盗み見に注意して安全な場所で使用すること。やむを得ず周辺に他者がいる状態で使用する場合には、壁を背にして他者から覗かれないよう配慮する、またはプライバシーフィルタを使用するなど覗き見を防止すること。
⑤ 紛失に気付いた場合は、速やかに ITS に報告すること。

(4) モバイル PC の使用者の変更
① モバイル PC の使用者を無断で変更しないこと。
② 使用者の変更が必要な場合には、いったん ITS に返却後、再度支給または貸出を受けること。

(5) モバイル PC の改造
① モバイル PC に対し、ハードウェア的な改造およびソフトウェア的な改造を行わないこと。

(6) 棚卸
① 社外への持ち出しの有無にかかわらず、年に 1 回以上の現品確認(棚卸)を行うこと。
② 棚卸期間中にモバイル PC の所在が確認できない場合、速やかに ITS に報告すること。

4-2-3. マルウェア対策

(1) モバイル PC の使用者は、モバイル PC に導入されたマルウェア対策ソフトの設定を変更せず、常駐設定にして、ファイルへのアクセスおよび電子メールの受信時には、常時スキャンできる状態で使用すること。

① 電子メールやインターネット閲覧を介してのマルウェア被害防止のため以下を遵守すること。
電子メールは、Web メールやグループウェアを使用しモバイル PC に保存しないこと。

② 送信元に心当たりがない電子メールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な電子メールの添付ファイルを開かないこと。

③ メール内に記載された URL リンクを安易にクリックしないこと。

④ マルウェアなど被害が予想されるような不審な電子メールを受信した場合は、速やかに ITS に報告すること。

⑤ インターネット閲覧時には、業務上関係のないサイトを閲覧しないこと。

(2) マルウェアに感染した場合、または感染が疑われる場合

マルウェア対策ソフトがマルウェアを検知した場合、またはマルウェアに感染、もしくは感染が疑われる場合は、以下を実行すること。

① ITS に速やかに連絡し、対応方法について指示を仰ぐこと。

② 無線通信機能（Wi-Fi、Bluetooth 等）や通信事業者が提供する通信を OFF にすること。

③ ITS の指示に従って、マルウェアを隔離あるいは駆除すること。

④ マルウェア被害の影響範囲が社外にまで至っているかを確認し、影響が確認された場合、あるいはその可能性がある場合、その事実について速やかに ITS に報告すること。

4-2-4. データセキュリティ対策

(1) 私的利用の禁止

① 社有のモバイル PC は業務以外の目的で利用しないこと。

(2) モバイル PC での情報保管

① 重要情報や個人情報は、使用が許可された外部サービス上に保存し、モバイル PC には保存しないこと。やむを得ず、モバイル PC のローカルに重要情報や個人情報を一時的に保存する場合は、使用する必要性がなくなった時点で速やかに消去すること。

② 毎月 1 回、モバイル PC のローカルデータの確認を行い、不要な情報が保存されている場合は削除すること。

4-3. 修理・返却

4-3-1. 修理

(1) ITS が使用を許可した社有のモバイル PC の修理を依頼する場合は、IT 推進委員等の担当者を通して修理を依頼すること。

(2) モバイル PC の修理を依頼する場合は、機密性の高い情報が読み出し可能な状態で保存されていないことを確認した上で修理を依頼すること。故障の状況により、保存されている情報の確認や保護が実施できない場合には、ITS に確認し、指定された方法にて修理を依頼すること。

4-3-2. 返却

不要になったモバイル PC は、各部門で廃棄せず、ITS に返却すること。

5. ソフトウェアと外部サービス

5-1. ソフトウェア

(1) 「使用可能なソフトウェアおよび外部サービス一覧」に記載されているソフトウェアを使用したい場合は、ITS へインストールを依頼すること。

(2) 導入したソフトウェアは、各機器のアップデート方法に従って常に最新の状態にした上で使用すること。

5-2. 外部サービス

(1) 「使用可能なソフトウェアおよび外部サービス一覧」に記載されているサービス以外の外部サービスは使用しないこと。

(2) 業務で使用する情報は、「使用可能なソフトウェアおよび外部サービス一覧」に記載されているサービス以外の外部サービス以外に保存しないこと。

6. 例外事項

業務都合等により本基準の遵守事項を守れない状況が発生した場合は、ITS に報告し、例外の適用承認を受けること。

7. 罰則事項

本基準の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

改訂履歴表

版　数	制定･改訂日	実　施　日	改訂の概要 （改訂箇所、改訂内容、改訂理由等）	承 認	作 成
1	2019 年 4 月 1 日	2019 年 4 月 1 日	新規作成		

【別紙】Wi-Fi アクセスポイント使用時の留意点

(1) 原則として、社有のスマートフォンおよびポータブル Wi-Fi 機器への接続のみ使用可能とする。

(2) 自宅の Wi-Fi を使用する場合は、以下を遵守すること。

① 機器が保持しているセキュリティ機能の確認のため、使用する Wi-Fi アクセスポイントまたはルータの暗号化方式を ITS に報告後、許可を得ること。
暗号化方式が不明な場合は、機種名を報告すること。

② 適切な暗号化方式（WPA2 等）を採用すること。

③ 使用する Wi-Fi アクセスポイント、またはルータのファームウェアを最新のバージョンに更新すること。

④ MAC アドレスフィルタリングなどを施し、許可された端末以外は容易に接続できないようにすること。

(3) やむを得ず、ホテルが提供するインターネット接続サービスなどを使用する場合は、以下を遵守し、ITS が提供するリモート接続ソフトウェア以外は使用しないこと。

① 適切な暗号化方式（WPA2 等）が採用されていない場合（暗号化なし、WEP、WPA 等）は使用しないこと。

② モバイル PC の OS が使用可能なものであり、最新のバージョンであることを確認すること。

③ 不特定多数の利用者が共有しているネットワークであることを常に念頭において使用すること。

④ ホテルが使用している Wi-Fi アクセスポイント、またはルータには脆弱性が潜んでいる可能性があることを念頭において使用すること。

(4) 使用しているスマートフォンや Wi-Fi ルータのキャリアが提供しているフリーWi-Fi およびホテルで提供しているもの以外の公共施設におけるフリーWi-Fi（飲食施設、空港、機内等）は使用しないこと。