株式会社 XXXXXX

スマートデバイス・セキュリティポリシーサンプル第 2 版

スマートデバイス・セキュリティポリシーを以下のように規定する。私有スマートデバイスの業務使用を認められた者は、セキュリティポリシー遵守のために、リモート・ワイプを含めスマートデバイスの操作方法を習得しておく必要がある。

1. 対象機器・OS

※パターン 1：MDM を利用している場合

・当社が承認した端末、OS 以外利用しない。

・当社からの指示に基づき、バージョンアップ、パッチをあてること。

※パターン 2：MDM を利用していない場合

・当社が承認した端末、OS 以外利用しない。

・常に最新のパッチを適用すること。バージョンアップについては、当社の指示に基づき実施すること。

・リモート・ワイプ・ロックもしくは暗号化等が利用できるようにしておくこと。

2. 標準導入ソフトウェア

・私有スマートデバイスには、当社が指定する以下のソフトウェアをインストールして業務利用する。また原則としてこれらのソフトウェアは、会社より提供され、ライセンスの管理が行われる。

＜業務利用するソフトウェア一覧の記載例＞

- アンチウイルスソフトウェア（XX 社製「XXXXXX」）
- MDM クライアント（YY 社製　「YYYY」）
- 暗号化ソフト（ZZ 社製　「ZZZZZZZZ」）
- ファイル共有サービスクライアント（W 社製　「WWWWW」）
- 電子会議クライアント（Q 社製　「QQQ-QQ」）
- VDI クライアント（P 社製　「P-PPPPVer.1」）
- セキュアブラウザー（O 社製　「OO-ooo」）
- リモートアクセスサービスクライアント（N 社製　「NNN」）

・各アプリケーションは、バージョンアップ、パッチをあてること。なお、標準導入ソフトウェア以外に当社の業務でソフトウェアをインストールする場合も、同様とする。

3. リムーバブルメディア

※パターン 1：使用を禁止する場合

・原則、利用を禁止する。

※パターン 2：使用を限定的に認める場合

・リムーバルメディアを利用する場合は、当社より利用の許可を得ること。

・リムーバルメディアを利用する場合は、必ず暗号化を施すこと。ただし、暗号化のパスワードは、デバイスロックと同じものを使用しない。

・紛失した場合は、スマートデバイスと同様の対応を行うこととする。

4. 導入ソフトウェア他

・構成プロファイルを変更・削除するような私的改変を禁止する。

・私的利用のソフトウェアに関しては、スマートデバイスメーカ、OS メーカ、通信キャリアが提供するマーケットから入手したものに限る。

・当社が禁止したソフトウェアのダウンロード、インストールを行わないこととする。

※MDM を利用している場合は以下を追記

・スマートデバイスは、当社が管理する MDM に登録されて利用可能となる。

・スマートデバイスにインストールされている当社が管理する MDM を、勝手に削除してはならない。

5. データ共有の制限

・原則、当社が指定したソフトウェアまたは当社が配布したアカウントで利用できるサービス以外で、当社の情報資産・営業秘密に関して、共有（SNS による画像、データ等の共有を含む）してはならない。但し、当社が指定する以下のソフトウェア、グループウェア、カレンダーなどは、データの共有を認めるものとする。

＜データ共有を許可するソフトウェア等一覧の記載例＞

- ファイル共有サービスクライアント（W 社製　「WWWWW」）
- 電子会議クライアント（Q 社製　「QQQ-QQ」）

6. 機能制限

※パターン 1：MDM を利用している場合

・資産管理システムや MDM を、当社のルールに則り設定を行う。

※パターン 2：MDM を利用していない場合

・端末管理について、当社のルールに則り、手動と目視にて設定を行う。

（自社の管理方法に合わせて、上記「パターン１」、「パターン２」のいずれかを選択)

・当社が指定したスマートデバイス機能制限エリアでは、指定された機能を利用してはならない。（指定された機能とは、電話、写真、録音、キャリア回線での Internet 接続、Wi-Fi

での Internet 接続、Bluetooth 接続、プログラムの起動等が含まれるが、これに限らない。）

・当社が想定しているスマートデバイスの利用方法は、スマートデバイス本体の画面にて、情報の閲覧／加工である。そのため、下記の目的／方法による利用は、当社が想定するスマートデバイスの利用方法に含まないため、必要な場合は、それぞれ別途利用許可を得なければならない。

- モバイルルータとして利用（テザリング）し、社の PC など情報資産をインターネットに接続する事
- PC と接続して、データをスマートデバイスに保存する事（スマートデバイス本体をリムーバブルメディア（外部記憶媒体）として利用すること）

7. 持込制限

・当社が指定したスマートデバイス持込制限エリアに、スマートデバイスを持ち込んではならない。

8. パスワード・ID

・パスワードの強度

- スマートデバイスのパスワードは、8 文字以上（同僚、友人、家族が推測困難なパスフレーズ＜12 桁以上の長いパスワード＞を推奨）とし、文字と数字が混在する設定とする。
- 複数のサービス・アプリケーション等で、同一のパスワードを設定してはならない。
- 同じ文字・数字が連続する、数字が連続して増減する等の推測容易なものを設定してはならない。
- 同僚、友人、家族、第三者の推測が容易な生年月日や、氏名、家族やペットの名前を設定してはならない。

＜使用してはならないパスワードの例＞

000000　123456　aaaaaa　abcdef　など

・パスワードの運用設定

- ログオンパスワードとサービス・アプリケーション等で使用するパスワードは異なるものとする。
- 個人で使用するソフトウェア・サービス（SNS やパブリッククラウド等含む）に、会社のメールアドレスを使用してはならない。

9. ロック

・スマートデバイスのログインに 5 回連続で失敗すると、アカウントがロックされる設定にする。

・スマートデバイスを 3 分間以上放置した場合はロックされ、パスワードの再入力をし

なければ利用できない設定にする。

※電子証明書を利用する場合に採用

10. 電子証明書

・当社の情報資産へアクセスする際、業務に応じ高度なセキュリティが必要と判断された場合は、当社が指定した電子証明書を指定の手順で導入しなければならない。
・電子証明書は、厳重に管理するとともに、以下の行為を禁止する。
- 許可なくスマートデバイスにインポートした電子証明書を削除してはならない。
- 電子証明書を当社が指定した以外の、他のデバイスにインポートしてはならない。
- 電子証明書を複製・保存したり、第三者に譲渡、貸与、公開、送信などをしてはならない。

11. 改造禁止

・スマートデバイスの改造（Jail Break や Root 化など）を禁止する。

12. メール・ショートメッセージ

・私有スマートデバイスにおいても、業務用メールの運用については「メール運用規定」を遵守するものとする。

13. 紛失

・紛失後は、可及的速やかに以下の手順に従わなくてはならない。リモート・ワイプを実施せずに個人的に捜索するなどし、いたずらに長時間、第三者がスマートデバイスにアクセスできる状態を維持してはならない。なお、所有者本人による対応が行われない場合、当社は強制削除等の措置を講じる。
- スマートデバイスを紛失した場合は、紛失したと思われる日時、場所、スマートデバイスの種類などを、可及的速やかに上長等に、電話、電子メール、FAX 等で届けなければならない。
- 届け出にあたっては、悪意をもった第三者によって収得されたスマートデバイスを操作した場合に発生しうる情報漏洩等の最悪の事態を想定し、予見可能な範囲で、できる限り顧客の保護、当社システム・データの保護のために適切な処置を具申しなければならない。
- 届け出後は、以下の操作、手続きを可及的速やかに実施し、その経過を、逐次、上長等に報告しなければならない。
  * リモート・ワイプの実施
  * 警察への紛失届の提出
  * リモート・ワイプ通信キャリアへの紛失届ならびに停波

* その他、必要と考えられる措置

14. データ消去

・以下の場合、データ消去もしくはリモート・ワイプを実行する。なお、社員は、データ消去もしくはリモート・ワイプを行ったことにより生じるリスクについて、すべての責任を負うものとする。

- パスワード入力に 5 回連続で失敗した場合。
- 退職や業務遂行において私有するスマートデバイスを利用する必要がなくなった場合。
- 機種変更その他の事由により私有スマートデバイス利用解除申請を提出した場合。

15. 私有データのバックアップ

・個人で所有している私有データは、適宜、自分自身で必要なバックアップを講じなければならない。（リモート・ワイプの対象は当社のデータに限られるが、私有するスマートデバイスによっては、保存された私有の個人情報や私有の個人情報資産などデバイス全体のデータが消去される可能性があるため）

・当社は、バックアップおよび復元に関する費用や、それに伴うリスクを負担しない。

16. セキュリティ対策

・ウイルス、スパイウェア等のマルウェアや不正なアプリケーションが混入しないよう、適切なセキュリティ対策を講じなければならない。

・ウイルス、スパイウェア等のマルウェアや不正なアプリケーションが混入もしくはそのおそれがある場合は、電波 OFF モードなど、ワイヤレス接続をすべて無効にした上で、可及的速やかに私有するスマートデバイスの利用を中止し、上長等に報告するとともに、取扱規程で定められた手順、もしくは上長等の指示のもと、データやプログラムの削除等、適切な処置を講じなければならない。

・上記に伴い、データ流出のおそれがある場合も同様の処置を講じなければならない。

17 データ転送

・原則、当社のデータを他のサービスへデータ転送することを禁止とする。

18. 監査

・当社による手動または MDM 等によるアプリケーション、データ、システム設定等への監査がいつでも受けられる状態にあること。

＜監査項目の例＞

- 改造（Jail Break や Root 化など）されていないこと

- 使用を認めていないソフトウェアがインストールされていないこと

19. 施行、改訂

・本規程は、情報セキュリティ委員会[1]で決議し施行する。

・当社は、必要に応じて本規程を改訂することができる。

・当社は、本条第 1 項の改訂にあたり、社員に対して改訂の周知徹底をはからなくてはならない。

以上

制定：2015 年 XX 月 XX 日

施行：2015 年 XX 月 XX 日

[1]情報セキュリティ委員会がない場合は、起案部門とする。