スマートデバイス利用規程

1.0版

スマートデバイス利用規程

１　趣旨 3
２　対象者 3
３　対象システム 3
４　遵守事項 3
４．１　スマートデバイスのセキュリティ対策 3
４．１．１　スマートデバイスの使用 3
４．１．２　スマートデバイスに導入するソフトウェア 3
４．１．３　スマートデバイスの他者への利用の制限 3
４．１．４　スマートデバイスでの情報の取り扱い 4
４．１．５　社外持ち出し時の注意事項 4
４．１．６　スマートデバイスの利用者の変更 4
４．１．７　スマートデバイスの改造 5
４．２ マルウェア対策 5
４．２．１　マルウェア対策ソフトの利用 5
４．２．２　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の防止 5
４．２．４　マルウェアに感染した場合、または感染したと疑われる場合 5
４．３　アプリケーション利用におけるセキュリティ対策 6
４．３．１　利用アプリケーションの制限 6
４．４　外部サービス利用におけるセキュリティ対策 6
４．４．１　クラウドサービスの利用 6
４．４．２　SNS サービスの利用 6
４．５　スマートデバイスの取り扱いに関するセキュリティ対策 6
４．５．１　スマートデバイスの修理 6
４．５．２　外付け媒体の制限 6
４．５．３　スマートデバイスと媒体の廃棄 7
４．６　ネットワークの利用 7
４．６．１　社内ネットワークの利用 7
４．６．２　社外ネットワークの利用 7
５　運用確認事項 7
６　例外事項 7
７　罰則事項 7
８　公開事項 8
９　改訂 8

スマートデバイス利用規程

１　趣旨

本規程は、スマートデバイスの利用に伴う、情報の漏えい、改ざん、破壊を防止することを目的とする。

２　対象者

当社の従業員等で業務にスマートデバイスを利用する全ての者。

３　対象システム

当社より支給・貸与されたスマートデバイス（スマートフォン、タブレット)。

４　遵守事項

４．１　スマートデバイスのセキュリティ対策

４．１．１　スマートデバイスの使用

(A.6.2.1)

当社の業務に利用するスマートデバイスは、以下のものでなければならない。

（１）当社が支給・貸与するスマートデバイス

４．１．２　スマートデバイスに導入するソフトウェア

(A.6.2.1　A.12.6.2)

（１）『システム管理規程』で規定されたソフトウェアを導入すること。支給・貸与するスマートデバイスには、それ以外のソフトウェアを導入してはならない。

（２）（１）にて指定したソフトウェア以外で、業務上やむを得ず導入しなければならないソフトウェアは、情報セキュリティ担当者に申請し、許可を得なければならない。

（３）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うえで使用すること。

４．１．３　スマートデバイスの他者への利用の制限

(A8.3.1　A9.2.4　A.9.3.1　A9.4.2　A9.4.3)

（１）利用者は、スマートデバイスのロック機能（パスワード、生体認証など）を有効にし、第三者が無断でスマートデバイスを利用できないようにしなければならない。

（２）ロック機能はシステム管理者が定めた通りに使用し、ロック解除方法が第三者に漏れないようにしなければならない。

（３）社外持出用のスマートデバイスでは、盗難・紛失時の対策として、スマートデバイス本体のロック以外に、外部記憶媒体を利用するときは暗号化などの対策を行わなければならない。

４．１．４　スマートデバイスでの情報の取り扱い

(A.6.2.1)

（１）スマートデバイスで機密情報を取り扱う場合には、情報セキュリティ担当者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。

（２）機密情報取り扱い後には、不必要となった情報を削除し、いつまでも保持してはならない。

４．１．５　社外持ち出し時の注意事項

(A.6.2.1　A.6.2.2　A8.3.1　A8.3.3　A.11.2.6)

（１）スマートデバイスを社外へ持ち出す際には、所定の手続きを行い、情報セキュリティ担当者の許可を得なければならない。

（２）移動時の交通機関や人混みでは、盗難に遭わないよう、適切にスマートデバイスを所持しなければならない。また、紛失対策（ストラップによる固定等）を施さなければならない。

（３）社外でスマートデバイスを使用する際には、盗み見に注意し安全な場所で利用しなければならない。やむを得ず周辺に他者がいる状態で利用する場合には、覗き見防止対策を施すこと（視野角コントロールフィルムや本体に搭載されている同等機能を有効にする）。

（４）紛失防止のため、スマートデバイスは常に手元に置き、放置しないようにすること。

（５）紛失に気付いた場合は、『セキュリティインシデント報告・対応規程』に基づき速やかに対応しなければならない。

４．１．６　スマートデバイスの利用者の変更

(A.9.2.6)

（１）スマートデバイスの利用者を無断で変更してはならない。

（２）利用者の変更が必要な場合には、情報セキュリティ担当者に返却しなければならない。

４．１．７　スマートデバイスの改造

(A.6.2.1)

（１）スマートデバイスのソフトウェア的な改造（ジェイルブレイク、ルート化）を行ってはならない。

４．２ マルウェア対策

４．２．１　マルウェア対策ソフトの利用

(A.6.2.1　A.12.2.1)

（１）利用者は、スマートデバイス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、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しなければならない。

４．２．２　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の防止

(A.12.2.1)

（１）メールの受信にあたっては、スパムメールや迷惑メールを分別する機能を有効にしなければならない。

（２）送信元不明の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、不審だと思われるメールの添付ファイルは開かない、また安易にＵＲＬリンクをクリックしない。不審だと思われるメールを受信した場合は、即座に情報セキュリティ担当者に報告しなければならない。

（３）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てはならない。

４．２．４　マルウェアに感染した場合、または感染したと疑われる場合

(A.16.1.2)

マルウェア対策ソフトがマルウェアを検知した場合、またマルウェアに感染、もしくは感染が疑われる場合は、利用者は『セキュリティインシデント報告・対応規程』に基づき対応し、以下を遵守すること。

（１）利用者は、感染が疑われる症状が発生した場合には、情報セキュリティ担当者に報告し、対応方法について指示を受けなければならない。

（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にしなければならない。

（３）情報セキュリティ担当者の指示に従って、マルウェアを駆除しなければならない。

（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、情報セキュリティ担当者に報告しなければならない。

４．３　アプリケーション利用におけるセキュリティ対策

４．３．１　利用アプリケーションの制限

(A.6.2.1　A.12.6.2)

（１）情報セキュリティ担当者が許可したアプリケーションのみを使用する。

（２）アプリケーションに不要な権限を与えないように、あらかじめ設定されているアプリケーション毎の権限（電話帳や位置情報へのアクセス）を変更してはならない。

４．４　外部サービス利用におけるセキュリティ対策

４．４．１　クラウドサービスの利用

(A.13.1.2)

（１）クラウドサービスを利用する場合は、情報の重要度に応じて、情報セキュリティ担当者が許可したクラウドサービスを利用する。

４．４．２　SNS サービスの利用

(A.13.2.3)

（１）スマートデバイスで SNS サービスを利用する場合、『SNS 利用規程』を遵守する。

４．５　スマートデバイスの取り扱いに関するセキュリティ対策

４．５．１　スマートデバイスの修理

(A.11.2.7)

（１）当社にて支給・貸与されたスマートデバイスの修理を依頼する場合は、申請書を提出し、情報セキュリティ担当者を通して修理を依頼しなければならない。

（２）スマートデバイス等の修理を依頼する従業員は、機密性の高い情報が読み出し可能な状態で保管されていないことを確認した上で修理を依頼しなければならない。故障の状況により、保管されている情報の確認や保護が実施できない場合には、情報セキュリティ担当者から指定された方法にて修理を依頼しなければならない。

４．５．２　外付け媒体の制限

(A.8.3.1)

（１）スマートデバイスに外付け記憶媒体を装着する場合は、情報セキュリティ担当者に申請し許可を得なければならない。

４．５．３　スマートデバイスと媒体の廃棄

(A.8.3.2　A11.2.7)

（１）業務に使用したスマートデバイスや媒体の廃棄を行う場合は、情報セキュリティ担当者に廃棄申請を提出し、指定された方法にて廃棄処理を行わなければならない。

４．６　ネットワークの利用

４．６．１　社内ネットワークの利用

(A.9.1.2)

（１）スマートデバイスで社内ネットワークへアクセスする場合、情報セキュリティ担当者の許可を得て、定められた方法で接続しなければならない。

（２）社内と社外（通信業者の提供する通信手段）の通信切り替えに注意する。

４．６．２　社外ネットワークの利用

(A.6.2.2　A9.1.2　A13.2.1)

（１）スマートデバイスで社外ネットワークへアクセスする場合、通信業者の提供する通信手段および暗号化された通信手段を利用し、情報セキュリティ担当者が定めた方法でアクセスしなければならない。

（２）やむを得ず、無料 Wi-Fi などセキュリティが確保されているか不明なネットワークを利用する場合は、個人情報・機密情報等を扱わない通信に留めなければならない。

（３）新たな通信手段を用いる必要がある場合、情報セキュリティ担当者に申請し許可を得なければならない。

５　運用確認事項

（１）スマートデバイスを紛失していないか、手元にあることを常に確認する。

（２）ソフトウェアの最新の情報を常に把握し、脆弱性等が発見された場合、情報セキュリティ担当者の指示に従って、許可されたアプリケーションであっても一時利用停止などの措置を取る。

６　例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程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。罰則の適用については『人的管理規程』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。