滋賀県立むれやま荘に係る指定管理者情報セキュリティ遵守事項（例）

（注）
・本書は、「指定管理者制度における施設の管理に関する基本協定書」に基づき、指定管理者が定める情報セキュリティに関する遵守事項の例を示すものである。
・【推奨】と示している事項は、規定することが望ましいものである。
・それ以外の事項は特段の理由がない限り規定すべきものである。
・上記に記載のない内容を遵守事項として追加することも差し支えない。

この遵守事項は、協定第〇条第１項に基づき、滋賀県立むれやま荘における情報セキュリティ対策を確実に行うために必要な事項を定めるものである。

第１　用語の定義

この遵守事項において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
（１）情報機器　パソコン、サーバ等の何らかの情報処理機能を持つ機器のことをいう。
（２）ネットワーク　情報機器を接続して通信するための装置および通信回線をいう。
（３）システム　情報機器、ネットワークを使用した情報処理の仕組みをいう。
（４）ウィルス等　コンピュータウィルスやその他の不正プログラムをいう。
（５）ログ　情報機器やシステムの利用状況や通信状況を記録したデータをいう。
（６）個人情報等　個人情報や滅失、き損、改ざん等により管理業務の円滑な執行に著しい支障を生じさせるおそれのある重要情報のことをいう。
（７）ソーシャルメディアサービス　インターネットを利用してユーザが情報発信し、あるいは相互に情報をやりとりする情報の伝達手段のことをいう。
（８）外部ネットワーク　インターネット等の外部と接続可能なネットワークのことをいう。

第２　管理業務で情報機器を利用する場合

１　ウィルス対策

管理業務で利用する情報機器を、ウィルス等から保護するため、次に掲げる対策を施すものとする。
（１）ウィルス等対策プログラムをインストールする。
（２）ウィルス等定義ファイルの更新の有無を確認し、ウィルス等定義ファイルを最新の

ものに保つ。
（３）ウィルス等検査機能を常時稼働させておく。
（４）定期的（週１回度程度を目安）に完全スキャンを実施する。

２　ウィルス感染時の対応

情報機器がウィルスに感染した場合またはそのおそれがある場合は、被害の拡大を防止し、被害状況の分析を円滑にするため、次に掲げる対応を行うものとする。
（１）直ちに情報機器からＬＡＮケーブルを抜く等、ネットワークからの遮断を行う（無線ＬＡＮの場合は、電源をオフにせずに通信を行わない設定へ変更をする)。
（２）画面を閉じずにそのままの状態で保持する。
（３）当該施設の県の所管課に直ちに連絡をする。

３　ソフトウェアの脆弱性対策

情報機器で利用するソフトウェアを安全な状態に保つため、次に掲げる対策を施すものとする。
（１）ソフトウェアの修正プログラム（例：Windows Update）が出た場合は、速やかに導入する。なお、システムに関する修正プログラムについては、システムに不具合が発生しないことを確認した後に導入する。
（２）サポート期限が終了したソフトウェアは使用しない。

４　バックアップの取得

情報機器に記録されたデータについては、データの滅失等の情報セキュリティ事故に備え、次に掲げる対策を施すものとする。
（１）データの重要度に応じて、取得頻度（年次、月次、週次、日次、随時）および保存期間を設定し、定期的にバックアップを取得する。
（２）独自に開発したシステムに関しては、プログラムの修正の際にプログラムのバックアップを取得する。
（３）バックアップデータは、情報機器とは別の筐体または外部記憶媒体に保存する。【推奨】

５　ユーザＩＤの管理

情報機器で利用するユーザＩＤについては、次に掲げる対策を施すものとする。
（１）ユーザＩＤの登録および登録抹消手順を定め、適切なユーザ管理を行う。
（２）利用していないユーザＩＤが放置されないよう定期的に点検し、必要に応じて登録抹消を行う（特に異動・退職者等が生じた場合)。
（３）他人にユーザＩＤを利用させない。また、複数の者で共有する場合は、共用する者以外に利用させない。

６　パスワードの管理

情報機器で利用するパスワードについては、次に掲げる対策を施すものとする。

（１）パスワードの発行や初期化、変更を行う手順を定める。

（２）パスワードに関する情報は厳重に管理する（パソコンの画面やキーボード等の目に付きやすい場所にパスワードが記載された付箋等を貼りつけない)。

（３）パスワードについて、数字と英文字を混在させる等、容易に推測されないものにする（１０文字以上推奨)。

（４）パスワードを、定期的（３か月推奨）に変更するものとし、古いパスワードの再使用を行わない。

（５）情報機器にパスワードを記憶させない（オートコンプリート機能は使用しない)。

７　ログの取得等

システムに関するログの取得等については、外部からの攻撃、不正行為、障害等の調査ができるよう、次に掲げる対策を施すものとする。

（１）情報機器に関するアクセス記録、稼働記録、障害記録（以下、「アクセス記録等」という。）のログを取得し、保管期間（１年以上を推奨）を定め、保管をする。

（２）情報セキュリティ事故、不正行為、障害等が生じた際に、ログの内容をチェックできる体制を整える。

（３）アクセス記録等のログを定期的に検査、分析する。【推奨】

８　盗難等防止措置

情報機器の性質や重要度等に応じて、部屋の施錠や機器の固定等の盗難防止や破損等を防止するための対策を講じるものとする。

９　ソフトウェアのライセンス管理

ソフトウェアの適正な利用を徹底するために、情報機器にインストールされたソフトウェアのライセンスを台帳等で管理するものとする。【推奨】

第３　管理業務で電子メールを利用する場合

１　電子メール送信時

インターネットを利用した電子メールを送信する際には、誤送信の防止を図るため、次に掲げる対策を施すものとする。

（１）互いに面識がない複数の宛先に電子メールを送付する場合は、送信先が非表示となるＢｃｃを使用する（Ｔｏ、Ｃｃについては同報するメールアドレスが送信先に知られてしまうため使用しない)。

（２）メールを送信する前に、宛先、送付方法（Ｔｏ、Ｃｃ、Ｂｃｃ)、添付ファイルに誤りがないか確認を行う。

（３）特に複数の宛先に同時に送信する場合は、複数名で確認を行う。【推奨】

２　電子メール閲覧

不審メールの閲覧によるウィルス感染や不正アクセスを防ぐため、電子メールの閲覧においては、次に掲げる対策を施すものとする。

（１）不審メールと思われる電子メールを受信した場合、添付ファイルを開いたり、本文のリンクをクリックしない。

（２）ＨＴＭＬメール（電子メールの本文を、ホームページのレイアウトなどに使うＨＴＭＬで記述したもの）はメールを開いただけでウィルス感染する場合もあるため、メールソフトの設定を変更し、ＨＴＭＬメールを利用できないようにする。

第４　ホームページを管理する場合

１　新規構築、再構築時

ホームページを新規構築、再構築する場合は、次に掲げる対策を施すものとする。

（１）情報処理推進機構（IPA）の「安全なウェブサイトの作り方」および別冊「安全なSQLの呼び出し方」の最新版に準拠した実装を行う。

（２）ホームページ上で個人情報等を取り扱う場合は、ＳＳＬ等による暗号化通信を実装する。

２　運用保守時

ホームページを運用保守する場合は、「第１　管理業務で情報機器を利用する場合」の対策に加え、次に掲げる対策を施すものとする。

（１）ホームページの脆弱性診断を実施し、ネットワーク機器、公開サーバおよび同サーバ上で稼働するウェブアプリケーション等の脆弱性の有無を確認する。また、受診の結果、脆弱性が検出された場合はその対処法を検討し、対策を実施する。【推奨】

第５　ソーシャルメディアサービスを利用する場合

１　ソーシャルメディアサービスのセキュリティ対策

ソーシャルメディアサービスを利用する場合は、次に掲げる対策を施すものとする。

（１）ソーシャルメディアサービスの運用ポリシーを定め、当該施設のホームページ等に掲載する。

（２）情報配信が実際に当該施設のものであることを明らかにするために、アカウントの自己記述欄等に運用組織を明示する等の方法でなりすまし対策を行う。

（３）個人情報等に該当する情報はソーシャルメディアで配信しない（ただし、当事者の了解が得られた場合は除く）。

（４）ソーシャルメディアについては、利用に際してあらかじめ当該施設の県の所管課に

報告をする。【推奨】

第６　外部ネットワーク・無線ＬＡＮを利用する場合

１　外部ネットワークを利用する場合

外部ネットワークを利用する場合は、次に掲げる対策を施すものとする。

（１）不正アクセスを防止するため、外部ネットワークの接続部分には、ファイアウォールおよびルータ等を設置し、経路制御および接続制限等を行う。

（２）外部ネットワークからの不正または大量アクセスによりサーバの利用に支障が出ないようにするため、情報機器およびネットワークの冗長化や専用の対策装置の導入、プロバイダ等が提供する対策サービスの利用など、可用性を確保するための対策を講じる。【推奨】

（３）外部ネットワークとの接続においてデータの漏えい、破壊、改ざん又はシステムダウン等の情報セキュリティの問題が認められる場合は、速やかに当該外部ネットワークとの接続を遮断する。

２　無線ＬＡＮを利用する場合

無線ＬＡＮ（ローカル・エリア・ネットワーク）を利用する場合は、次に掲げる対策を施すものとする。

（１）接続に関する認証は「IEEE802.1X(EAP)認証」もしくは「PSK 認証」を使用する。なお、「PSK 認証」を使用する場合は、 パスフレーズの文字数を２０文字以上で設定し、定期的に更新を行う。

（２）通信内容の暗号化の方式については、「CCMP 方式 」を使用する。なお、「WEP 方式」、「TKIP 方式」については脆弱性があるため使用しない。

（３）無線ＬＡＮを利用できる場所として設定した範囲を超えて電波が漏出しないよう、電波の伝搬範囲を限定する。

（４）無線ＬＡＮのアクセスポイントの管理用パスワードを適切に設定し、定期的に更新を行う。

（５）（１）～（４）の他、総務省が作成する別添「企業等が安心して無線 LAN を導入するために」を参考に必要に応じてセキュリティ対策を講じる。【推奨】

（６）無線ＬＡＮについては、利用に際してあらかじめ当該施設の県の所管課の承認を得る。【推奨】

第７　その他一般事項

１　私物情報機器および私物外部記憶媒体の利用

私物情報機器および私物外部記憶媒体（以下「私物情報機器等」という。）については、次に掲げる事項を遵守するものとする。

（１）私物情報機器等の管理業務利用は原則行わない。やむを得ず使用する場合は、上長の許可を得る。
（２）私物情報機器等の利用を許可する際には、ウィルス対策、脆弱性対策の実施等の条件を付す。
（３）私物情報機器等の利用を許可した場合、許可する理由、期間等を台帳に記載し管理する。

２　個人情報等を含むデータ等の外部への持ち出し

個人情報等を含むデータおよび情報処理に係る帳票（以下「データ等」という。）の外部への持ち出し（電子メール含む。）については、次に掲げる事項を遵守するものとする。

（１）データ等の外部への持ち出しは原則行わない。やむを得ず持ち出す場合は、上長の許可を得る。
（２）持ち出しの許可を得る際には、帯出簿に持ち出し先、期間等を記載し、上長に報告を行う。
（３）ＥＸＣＥＬ形式のデータを外部へ持ち出す際には、別シートや非表示になっている箇所に個人情報等が入っていないか確認する。
（４）持ち出しの際には、車上荒らしや置き忘れによる紛失等が起こらないように十分に注意する。
（５）紛失等が起こった場合に備え、個人情報等を含むデータには暗号化やパスワードを施す。
（６）データ等を持ち帰った際にも、上長に報告を行う。

３　データ等の管理

データ等については、滅失、き損および情報漏えい等の防止を図るため、次に掲げる対策を施すものとする。

（１）個人情報等を含むデータを情報機器に保存する場合は、端末本体に保存せず、冗長化したファイルサーバに保存する。なお、ファイルサーバは、ウィルス感染等による侵害の拡大を防ぐため、ネットワークドライブに設定しない。【推奨】
（２）データ等をファイルサーバ以外で保存する場合は、保存用の情報機器、外部記憶媒体は、施錠保管するなど、適正な管理を行う。
（３）個人情報等を含むデータを外部記憶媒体に保存する場合は、データの名称、外部記憶媒体の種類（ＵＳＢメモリ、外付けハードディスク、ＣＤ等）、保存期間、保存場所等を記した管理台帳を作成し、保管状況を把握する。
（４）情報機器または外部記憶媒体を廃棄する場合は、データが復元できないように物理的に破壊する等の処理を行う。なお、個人情報が含まれた情報機器または外部記憶媒体を廃棄した場合は、管理台帳に廃棄日、処理内容等を記録する。

４　管理業務に従事する者への教育

管理業務に従事する者の役割および理解度等に応じた情報セキュリティに関する教育研修および訓練を定期的および随時に実施し、情報セキュリティ対策を徹底するものとする。

５　緊急時の連絡体制等

個人情報の漏えい等の情報セキュリティ事故や、不正アクセス等による侵害に対して、適切な対応が図れるよう、次に掲げる対策を施すものとする。

（１）関係者の連絡先、緊急時の対処手順をあらかじめ定めておく。

（２）情報セキュリティ事故が発生した場合もしくはそのおそれがある場合は、直ちに必要な措置を講ずる。また、不正アクセス等による侵害が発生した場合もしくはそのおそれがある場合は警察に通報する。

（３）休日に緊急時対応が想定されるシステム（県民等への情報提供や申請・予約等の休日においても利用が想定されるシステム）については、休日においても保守対応が可能となるよう、その旨を保守委託業務の契約書・仕様書に明記する。

６　ホームページ閲覧の留意事項

管理業務でホームページ閲覧を行う場合は、次に掲げる事項を遵守するものとする。

（１）ホームページ閲覧には常にウィルス感染のリスクがあるため、管理業務と関係あるホームページ閲覧であっても必要最小限の利用とする。

７　特定個人情報の取扱い

管理業務で特定個人情報（個人番号を含む個人情報をいう。）を取扱う場合は、別添「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」の「安全管理措置」に基づいた対策を施すものとする。