情報セキュリティ関連特記仕様書

目次

本特記仕様書は、福島県県営住宅管理システム更新業務に係る仕様書に加え、追加で求めるセキュリティ要件を記載するものである。

受注者は本書に従わなくてはならない。

第１章　アカウント関係

（１）ID 共有の禁止

利用者のアカウントの発行単位は個人とし、１利用者に付き１アカウント発行する。

なお、組織単位でのアカウントの発行やアカウントの共有は不可とする。

（２）管理者用の ID の共有禁止

上記（１）に同じ。

（３）接続の自動タイムアウト

ログインしたままの端末を放置し、担当者以外が操作することを防ぐため、一定の時間以上操作が行われていない場合において、認証機能付きのスクリーンセーバーを動作させること。

（４）パスワードの強制変更

パソコンにログインする際のパスワードは年１回以外は管理者権限がない限り変更ができない。また、仮にパスワードが漏えいしたとしても、担当者以外が継続的に操作することを防ぐため、パスワードと生体認証の２要素認証とする。

（５）パスワードの文字数制限、単語制限

管理用アカウントに推測可能なパスワードを用いることを防ぐため、管理用アカウントのパスワードの変更時に 8 文字以上でなければ、受け付けず、その旨表示し、再度、入力を求めること。

（６）サーバに保存されたパスワードの暗号化等

サーバ等に認証等の用途で保存されるパスワードについては、SHA-256 と同等以上のハッシュ、NTLMv2 と同等以上の認証手順、又は、電子政府推奨暗号リストによる暗号化等を行い、運用管理者であってもパスワードを参照・解読出来ないようにすること。

第２章　物理的対策関連

（１）サーバ多重化

サーバ故障時にあってもサービスを継続させるため、主要なサーバおよび接続機器は、多重化するものとする。なお、多重化の方法は問わないが、サービス停止後、10 分以内にサービス再開するできるものとする。

（２）データ多重化

ストレージ（ハードディスク）故障時にあってもサービスを継続させるため、主要なサーバにおけるストレージは、1 つ以上のパリティを持つ RAID 構成とする。

（３）予備電源

サーバは UPS に接続し、停電時に自動的にシャットダウンさせること。

UPS は、シャットダウンまでに必要な電力供給を行えるものとする。

（４）雷対策

上記（３）に同じ

（５）転倒防止

サーバは、必要な免震・耐震対策を備えること。

（６）盗難防止

サーバは、鍵付のラックに収納すること。

（７）断線防止、引っ掛け防止

サーバ及びネットワーク装置等の配線は、電源と通信ケーブルを分け、モールにより保護すること。

（８）火災対策

ラックは、粉末消火器を使用する際、障害にならないものを用いること。

（９）水害対策

サーバは、必要な水害対策を備えること。

(10) 埃対策

サーバは、必要な埃対策を備えること。

(11) 異常温度湿度、静電気対策

サーバの温度および湿度異常を検出できること。

(12) 漏水対策

可能な限り天井等の水道管、スプリンクラーを回避して機器を設置するとともに、サーバをラックに収納し、漏水等がサーバへ及ばないようにすること。

(13) 入室制限

限られた者のみの入室とすること。

(14) 入退室管理

入退去が分かる一覧を設けること。

(15) 定期保守

年 1 回に稼働負荷やサーバの状態を確認すること。

第３章　ネットワーク関連

（１）アクセス制御

システム稼働環境内にはファイアーウォール機を設置し、必要のない通信は拒否すること。

（２）外部のネットワークと接続時の認証方法

外部ネットワークへの通信は行わないよう遮断すること

（３）機密性の低いネットワークの使用

電子政府推奨暗号リストの暗号を用いること。

なお、電子政府推奨暗号リストの暗号を用いるように設定し、有効な証明書を使用したリモートデスクトップや ssh でもよい。

（４）プロトコル制限

上記（２）に同じ

（５）外部のネットワークと接続時の回線の選択

上記（２）に同じ

（６）外部ネットワーク由来の業務への影響

上記（２）に同じ

第４章　サイバー攻撃対策

（１）不正データの入出力の除外

「セキュリティ関連特記仕様書」のほかに「Web アプリケーションセキュリティに係る特記仕様書」を満たすこと

（２）ウィルス対策の実施

県庁内に設置する Windows 系のサーバについては、情報通信システムネットワークシステムのウィルス対策ソフト（ライセンスは取得済み）をインストールし、稼動させること。

その他の場合については、ウィルス対策ソフトを導入し、随時パターンアップデートを行うこと。

（３）ウィルス対策ソフトのパターンアップデート間隔

概ね１時間毎とする。

（４）web コンテンツ納品時の改ざんチェック・運用時の改ざんチェック

該当なし

（５）脆弱性又は改ざん等のチェックの間隔

該当なし

（６）システムの設定ファイルの改ざんチェック、チェックの間隔

システムの設定ファイルの改ざんチェックのため、１年に一度、事前に保存していた設定ファイルと比較を行うこと。

（６）脆弱性対応パッチ情報の取得及び適用、適用時期

県庁内に設置する Windows 系の OS については、デジタル変革課が設置した WSUS

サーバを利用し、随時、脆弱性を解消する設定とすること。

その他の場合については、脆弱性対応パッチ情報の取得し適用するか、ネットワーク上困難な際にはこれに代わる措置を講ずること。

第５章　障害対策

（１）データベースのバックアップ、バックアップ間隔

データベース等のバックアップは、データ領域（DB 及び DB 以外を含む）、システム領域及びログについて、日次自動で行うものとする。

月初めについては、フルバックアップとし、その他は差分バックアップアップとして構わない。

なお、曜日ごとに上書きして構わない。

（２）データ領域（データベース以外)のバックアップ、バックアップの間隔

上記（１）に含む

（３）システム領域のバックアップ、バックアップの間隔

上記（１）に含む

（４）ログのバックアップ

上記（１）に含む

（５）死活確認、間隔

該当なし

第６章　検出、事故対応

（１）アクセス記録の取得

ログインの記録(日時、ID、IP アドレス)をログに取得すること。

また、Web サーバの標準のアクセス記録(combined フォーマット)をログに取得すること。

（２）ログの分析

情報システムへの不正アクセス検出のためのログの分析のため、1 年に一度、ログの中から異常なパターンを取得し、解説を付し報告すること。

（３）時刻の同期

デジタル変革課の指示する NTP サーバにより継続的に時刻同期を行うこと。

第７章　その他の契約事項

（１）資格の確認

事業者は、ISMS 認定またはプライバシーマーク認定を取得していること。

（２）外部委託における契約項目

外部委託については、契約条項に次の項目を含めること。

ア　情報セキュリティポリシー及び情報セキュリティ実施手順を遵守すること。

イ　責任者、作業者及び作業場所を特定し、予め提出すること。

ウ　別紙「SLA 関する事項」により提供されるサービスレベルを保証すること。

エ　福島県情報セキュリティポリシー及び本契約事項について従業員に対する研修を実施し、趣旨及び内容を周知すること。

オ　提供された情報の目的外利用及び受託者以外の者への提供は禁止とする。

カ　業務上知り得た情報は守秘すること。

キ　再委託を行う場合は、再委託先についても、情報セキュリティに関する契約事項を遵守させること。

ク　委託業務終了時には、すべての情報資産について、県の指示に従い、県に返還もしくは廃棄すること。

ケ　委託業務の実施内容について 1 か月に一度報告すること。
　また、緊急時については、その都度その内容について報告すること。

コ　契約条項及び情報セキュリティポリシーの遵守状況について、県は、実地検査を行うことができる。
　なお、実施にあっては、最短で 10 営業日前に通知するものとする。

サ　県は、当該業務にかかる事故等について公表できるものとする。

シ　情報セキュリティポリシーが遵守されなかった場合、損害賠償対象とし、双方の話し合いにより額を決定すること。

ス　災害時及び原子力発電所事故時においても、例外なく履行されること。

（３）クラウドの利用におけるサービスレベル

該当なし

（４）クラウドの利用における第三者提供サービス

該当なし

（５）パブリッククラウドの利用におけるデータの第三者利用

該当なし

（６）パブリッククラウドの利用にデータの削除

該当なし