情報セキュリティ関連特記仕様書

本特記仕様書は、福島県が導入する「福島県河川流域総合情報システム機器賃貸借」の特記仕様書に加え、追加で求めるセキュリティ要件を記載するものである。
なお、受注者は、本書に従わなくてはならない。

1　アカウント関係

(1) ID 共有の禁止

「情報セキュリティ事案発生時に操作者を特定できるようにするため」、また、「共有しやすいように、関係者なら誰もが思いつく符丁的な安易なパスワードを利用しないため」、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。組織単位でのアカウントの発行は行わない。

(2) 管理者用の ID の共有

(1) に同じ。

(3) 管理用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、管理用の接続は、30 分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、管理用アカウントのパスワードは、前のパスワード変更から1年を過ぎた最初のログインにおいて、強制的に変更を行うこと。

(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、また、辞書にある単語、年月日などの単純なものが入力された場合は、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。

2　物理的対策関連

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、別な物理サーバによるアクティブ-コールドスタンバイ構成による冗長構成とする。

(1) 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 構成とし、さらに、ホットスペアを搭載することする。

(2) 転倒防止

サーバ及びネットワーク装置（必要な機器については列記する。）は、ラックに収納し、ラックは耐震アンカー付きとすること。

管理用ノートパソコン、監視端末は、免震ジェル又は耐震吸盤により転倒対策すること。

(3) 盗難防止

サーバ及びラック搭載のＬ２／Ｌ３スイッチ等のネットワーク装置は、鍵付のラックに収納すること。（搭載機器の詳細については、機器仕様書を参照のこと）

管理用のノートパソコン、監視端末は、セキュリティワイヤーにより固定すること。

(4) 断線防止、引っ掛け防止

サーバ及びネットワーク装置の配線は、床下配線とすること。

部屋間の配線は、既設配線収納管を利用すること。

(5) 埃対策

流総室は、特段の防塵対策がなされているわけではないが、サーバの稼働に問題があるほどではない。保守点検時、ファン付近の埃について目視でチェックし、付着しているようであれば、掃除すること。

(6) 入室制限

サーバ室への入室は、担当職員の許可を得て入室できることとする。

(7) 入退室管理

データセンターの入室は、生体認証による入退管理を実施し、状況を記録できること。

各事務所の入退に関しては、執務室職員の許可により管理する。

(8) 定期保守

サーバ及びネットワーク装置は、６ヶ月に一度、定期点検を行い、また、故障が発見された場合は、機器が設置されている場所に訪問し、修理すること。

4　ネットワーク関連

(1) アクセス制御

管理用の接続は、SSL 又は VPN により暗号化すること。なお、暗号は電子政府推奨暗号リストによる暗号化を用いること。

(2) 外部のネットワークと接続時の認証方法

情報システムの内部ネットワークへ接続にあっては、予め登録された接続元のインターネットに公開している IP アドレス以外は、接続できないようにすること。また、サーバ及びネットワーク装置へのログインには、担当者個人に配布した ID 及びパスワードにより認証を行うこと。

(3) プロトコル制限

情報システムの内部ネットワークへ接続にあっては、ファイアウォール等により、予め登録された必要なプロトコル以外は、通過させないこと。

(4) 外部のネットワークと接続時の回線の選択

情報通信ネットワークシステム(県の行政用ネットワーク)を使用しない部分は、専用線とすること。

(5) 外部ネットワーク由来の業務への影響

接続した外部ネットワークの瑕疵等により県の情報資産の漏洩、破壊、改ざん又はシステムの停止等による業務への影響が生じた場合、原因について調査を行い、再発防止の対策を行うものとする。

5　サイバー攻撃対策

(1) 不正データの入出力の除外

入出力されるデータについて、範囲及び妥当性をチェックし、不正な文字列等の入出力を除去すること。

(2) ウィルス対策の実施

サーバ(アプライアンスサーバを除く）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。なお、パターンアップデート間隔は、概ね１時間毎とする

(3) ウィルス対策ソフトのパターンアップデート間隔

(2)による。

(4) Web コンテンツ納品時の改ざんチェック
Web サーバの納品時テストにおいては、「安全なウェブサイトの作り方」改訂第6版 別冊：「ウェブ健康診断仕様」に準拠した脆弱性のチェックを行うこと。

(5) Web コンテンツ運用時の改ざんチェック
Web サーバの運用時に、情報政策課が実施する Web 脆弱性検査に参加するため、指摘事項があった場合は対応を行うこと。

(6) 脆弱性又は改ざん等のチェックの間隔
(5)による。

(7) システムの設定ファイルの改ざんチェック
システムの設定ファイルの改ざんチェックのため、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。

(8) システムの設定ファイルの改ざんチェックの間隔
(7)による。

(9) 脆弱性対応パッチ情報の取得
月に一度、システムの脆弱性対応パッチ情報の取得し、報告すること。

(10) 脆弱性対応パッチの適用
取得したシステムの脆弱性対応パッチ情報により、最低でも3か月に一度パッチを適用し、公表された脆弱性を解消すること。

(11) 脆弱性対応パッチの適用時期
(10)による。

6　障害対策
(1) データベースのバックアップ
データベースのフルバックアップを一月に一度自動で行うものとし、差分については一回／日行うものとする。

(2) データベースのバックアップの間隔
(1)による。

(3) データ領域（データベース以外)のバックアップ
データ領域（データベース以外)のバックアップについては、データ変更時、及び保守点検時にバックアップを行うこと。

(4) データ領域（データベース以外)のバックアップの間隔
(3)による。

(5) システム領域のバックアップ
運用開始時にフルバックアップを行うものとし、システム領域の変更を伴う作業を実施した場合は、差分バックアップアップを行うこととする。

(6) システム領域のバックアップの間隔
(5)による。

(7) ログのバックアップ
ログのバックアップは週に一度自動で行うものとする。その際圧縮するものとする。

(8) 死活確認
システムの死活確認は、10 分ごとに ping で行い、無反応の場合、担当にメールで警告すること。

(9) 死活確認の間隔
(8)による。

7　検出、事故対応
(1) アクセス記録の取得
サーバのログインの記録(日時、ID、IP アドレス)をログに取得すること。
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の 3 か月に一度、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
河川流域総合情報システムの NTP サーバにより継続的に時刻同期を行うこと。

８　その他の契約事項

(1) 資格の確認

事業者は、ISMS 認定、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

・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。
・責任者、作業者及び作業場所を特定し、予め提出すること。
・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。
・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。
・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。
・業務上知り得た情報は守秘すること。
・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。
・委託業務の実施内容について 6 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。