

情報セキュリティ関連特記仕様書

目次

- 第1章 アカウント関係
- 第2章 物理的対策関連
- 第3章 ネットワーク関連
- 第4章 サイバー攻撃対策
- 第5章 障害対策
- 第6章 検出、事故対応
- 第7章 その他契約事項

本特記仕様書は、福島県が導入する「福島県立学校入学者選抜WEB出願システム構築・調達業務委託仕様書」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
ID 共有は禁止しないが ID 共有による脅威に対する回避策を行うこと。
- (2) 管理者用の ID の共有禁止
ID 共有は禁止しないが ID 共有による脅威に対する回避策を行うこと。
- (3) 管理用接続の自動タイムアウト
自動ログアウトを有効にすること。
- (4) パスワードの文字数制限、単語制限
管理用のアカウントのパスワードの最低文字数設定は有効にしないが、弱いパスワードを用いることを防ぐため運用上の回避策を行うこと。
- (5) サーバーに保存されたパスワードの暗号化等
アカウントのパスワードは、サーバには平文（元テキストのまま）又は単純な暗号化したものでは保存せず、運用管理者がそのパスワードの暗号化キーを知ることができない、十分な強度の暗号化又はハッシュ化を行い保存すること。
暗号化の詳細については、受託者と協議の上決定する。

第2章 物理的対策関連

- (1) サーバー多重化
サーバ故障時にあってもサービスを継続させるため、アクティブ-アクティブ（物理サーバ間）、アクティブ-ホットスタンバイ（物理サーバ間）、アクティブ-コールドスタンバイ（物理サーバ間）、アクティブ-アクティブ（仮想サーバ内）のいずれかにより冗長策を設けること

第3章 ネットワーク関連

- (1) アクセス制御
SSL 又は VPN を使用すること。
- (2) 外部のネットワークと接続時の認証方法
接続ネットワークの IP による認証（フィルタリング）、利用者の ID 及びパスワード認証、証明書による認証を行うこと。
- (3) 機密性の低いネットワークの使用
インターネットから Web サイトへの接続は SSL/TLS により暗号化すること。
- (4) プロトコル制限
外部のネットワークと接続時はファイアウォールにより制限すること。

第4章 サイバー攻撃対策

- (1) ウィルス対策の実施
独自にウィルス対策ソフトを導入しインターネットから自動アップデートを行うこと。
- (2) ウィルス対策ソフトのパターンアップデート間隔
概ね一日毎に行うこと。
- (3) web コンテンツ納品時の改ざんチェック
脆弱性のチェック（自主検査）を行うこと。
- (4) web コンテンツ運用時の改ざんチェック
脆弱性のチェック（自主検査）を行うこと。
- (5) 脆弱性又は改ざん等のチェックの間隔
年に1回以上行うこと。
- (6) 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をチェックすること。
- (7) システムの設定ファイルの改ざんチェックの間隔
年に1回以上行うこと。
- (8) 脆弱性対応パッチ情報の取得
脆弱性対応パッチ情報を取得すること。
- (9) 脆弱性対応パッチの適用
システムの脆弱性対応パッチの適用を行うこと。

- (10) 脆弱性対応パッチの適用時期
6ヶ月から12ヶ月未満に一度とする。

第5章 障害対策

- (1) データベースのバックアップ
3世代以上とする。
- (2) データベースのバックアップの間隔
毎日実施すること。
- (3) データ領域（データベース以外）のバックアップ
3世代以上とする。
- (4) データ領域（データベース以外）のバックアップの間隔
毎日実施すること。
- (5) システム領域のバックアップ
1世代以上とする。
- (6) システム領域のバックアップの間隔
毎日実施すること。
なお、本番環境で復旧不可能な障害が発生した場合、同じ設定を行っているステージング環境を転用可とする。
- (7) ログのバックアップ
毎日実施すること。
- (8) 死活確認
エージェントレス（TCP レベル監視）又はエージェントレス（サービスレベル監視）とする。
- (9) 死活確認の間隔
常時監視とする。

第6章 検出、事故対応

- (1) アクセス記録の取得
取得すること。
- (2) ログの分析
常時監視とする。

- (3) 時刻の同期
インターネット上の NTP サーバとする。

第7章 その他の契約事項

- (1) 資格の確認
ISMS (ISO/ICE27001)、プライバシーマークを取得していること。
- (2) 外部委託における契約項目
- | | | |
|---|-----------------------------------|-----|
| 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の遵守 | (○) |
| イ | 委託先の責任者、委託内容、作業者及び作業場所の特定 | (○) |
| ウ | 提供されるサービスレベルの保証 | (○) |
| エ | 従業員に対する教育の実施 | (○) |
| 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の禁止 | (○) |
| カ | 業務上知り得た情報の守秘義務 | (○) |
| キ | 再委託に関する制限事項の遵守 | (○) |
| ク | 委託業務終了時の情報資産の返還、廃棄等 | (○) |
| ケ | 委託業務の定期報告及び緊急時報告義務 | (○) |
| コ | 県による監査又は検査 | (○) |
| サ | 県による事故等の公表 | (○) |
| シ | 情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等) | (○) |
| ス | 可用性2以上のシステムに係る災害時及び原子力発電所事故時の対応 | (○) |
- (3) クラウドの利用におけるサービスレベル
AWS のクラウドサービスに準拠する。
- (4) クラウドの利用における第三者提供サービス
セキュリティポリシー及び契約事項の遵守を求める
- (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
AWS のクラウドサービスに準拠する。
- (6) パブリッククラウドの利用にデータの削除
完全に削除できることとする。