情報セキュリティ関係特記仕様書

目次

本特記仕様書は、福島県が導入する「電子納付システム」の福島県電子納付システム調達業務仕様書に加え、追加で求めるセキュリティ要件を記載するものであるため、受託事業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 の所属単位発行・共有禁止

すべての利用者 ID（管理者 ID を含む）は、所属単位で発行し、他所属との共有を禁止する。

（２）自動タイムアウト

自動タイムアウトを有効にすること。

（３）パスワードの保存方法

アカウントのパスワードは、サーバーには平文（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。

２　物理的対策関連

サーバー故障時にあってもサービスを継続させるため、RAID 構成、クラスタリング、バックアップサーバ等を用いて、サーバー及びデータの多重化を図ること。

３　ネットワーク関連

（１）アクセス制御

TLS 又は VPN 等を用いてアクセス制御を行うこと。

（２）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。

４　サイバー攻撃対策

（１）ウィルス対策

システムに対して適切なマルウェア対策（ウィルス対策ソフトを導入等）を講じること。

（２）改ざん及び脆弱性のチェック

脆弱性のチェック(自主検査)を年に１回以上行うこと。

５　障害対策

（１）バックアップ間隔

以下のとおり、定期的なバックアップを実施すること。

・データベース：毎日

・データ領域　：毎日

・システム領域：システムの更新、変更等の都度

（２）ログ

ログは毎日取得し、適切に保管すること。

（３）死活監視

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）等により常時監視すること。

６　検出・事故対応

（１）ログ管理

アクセスログを取得し、改ざん防止措置を講じた上で保管すること。

（２）保管期間

ログは１年以上保管すること。

（３）時刻同期

NTP サーバーにより時刻の整合性を確保すること。

７　クラウド

（１）クラウド利用要件

クラウドサービスを利用する場合は、以下の要件を満たすこと。

・ISMAP（政府情報システムのためのセキュリティ評価制度）に登録されたサービスであること

・ISO/IEC 27001 等の認証を取得していること

・SLA において可用性 99.9%以上を保証していること
・データの第三者提供を禁止していること
・データ削除時には、DoD 5220.22-M 等に準拠した完全消去を行うこと

８　委託先管理強化

（１）契約時の確認事項
・情報セキュリティポリシーを策定していること
・ISO/IEC 27001 等の認証を取得していること、または同等の管理体制を有していること
・情報資産の取扱いに関する責任者を明確にしていること

（２）業務実施中の管理事項
・インシデント発生時の報告体制を構築し、速やかに報告できる体制を整備すること
・情報資産の持ち出し・複製・廃棄に関する手順を明確にし、福島県の承認を得ること
・受託事業者の従業員に対する情報セキュリティ教育を実施すること

（３）契約終了時の対応事項
・提供された情報資産の返還または確実な廃棄（不可読化）を実施すること
・業務履行に使用した ID・パスワード等の認証情報を速やかに削除すること
・契約終了後も秘密保持義務が継続する旨を再委託先に周知徹底すること

（４）指導・監査への協力

必要と認めた場合、受託事業者は、情報セキュリティ対策状況の確認（立入調査、書面調査等）に協力しなければならない。改善を勧告した場合、受託事業者は速やかに対応し、改善結果を報告すること。