

## 情報セキュリティに関する特記事項

### (目的)

第1条 本仕様書は、本事業において利用するクラウドサービス（以下「本サービス」という）の導入・構築にあたり、受注者が提供すべきセキュリティ機能、および運用支援の内容を定義するものである。受注者は、本仕様書に基づき、本システムの機密性、完全性、および可用性を確保しなければならない。

### (アクセス制御に関する要件)

第2条 受注者は、不正アクセスを防止するため、以下の機能を提供し、または設定支援を行うこと。

- (1) ID・ライフサイクル管理： 識別コード（ID）の発行から廃棄に至るライフサイクルを管理できる機能を提供すること。
- (2) サービス別アクセス制御： ネットワークレベルにおいて、サービス（ポート・プロトコル）単位でアクセス制御（ファイアウォール、セキュリティグループ等）が可能であること。
- (3) 強固な認証： 特権管理者アカウントに対し、多要素認証（MFA）等の強固な認証技術を提供すること。
- (4) 認証機能の適合性： 受注者が提供する主体認証管理機能が、パスワード認証に加えて別の認証手段も可能であること。（多要素認証）
- (5) リソース・権限管理： クラウド上の保存データおよび各機能に対し、詳細な権限設定（IAM ロール等）が可能であること。
- (6) 誤操作・影響抑制： 大規模なリソース削除等、システムに多大な影響を与える操作を特定し、二重承認や操作制限等の誤操作抑制策を講じること。
- (7) 仮想マシンの保護： 仮想マシン（インスタンス）に対し、最新の OS パッチ適用、マルウェア対策、IDS/IPS 等のセキュリティ対策が実施可能な環境を提供すること。
- (8) 外部接続の管理： インターネット等から直接ログインする際の経路制限、または VPN・閉域網接続等のセキュアなアクセス手段を提供すること。
- (9) ログ管理・検証： 不正侵入や不正操作を検知・検証するため、操作ログ、アクセスログ、システムログを適切に取得・保管し、利用者側で閲覧・出力できること。

### (情報の機密性保護（暗号化）に関する要件)

第3条 受注者は、取り扱う情報の機密性を保護するため、以下の対策を講じること。

- (1) 通信および保存時の暗号化： 通信経路（TLS 等）およびクラウド内のデータ保存領域（ストレージ、データベース等）における暗号化機能を提供し、その仕様を明示すること。
- (2) 法令・規格の遵守： 採用する暗号化方式が、日本の政府情報システムのためのセキュリティ評価制度（ISMAP）や関連法令に準拠していること。

### (開発・構築時のセキュリティ要件)

第4条 受注者は、本システムの構築にあたり、以下の情報提供および管理を行うこと。

(1) セキュア開発情報の提供： 受注者の責任範囲におけるセキュアな開発手順、および利用者側でのセキュアな構築に資するベストプラクティス集を提供すること。ただし、パッケージシステムは除く。

(2) ライセンス管理： クラウド上でサードパーティ製ソフトウェアを導入する場合、受注者の提供するプラットフォーム上でのライセンス規定（BYOL 等）を明示し、抵触がないことを確認すること。

（設計・設定誤りの防止に関する要件）

第5条 受注者は、設定不備によるセキュリティ事故を防止するため、以下の支援・機能を提供すること。

(1) 設計・構築知見の提供： クラウド構成設計（アーキテクチャ設計）におけるセキュリティ上の知見や、推奨構成に関する技術支援を行うこと。ただし、パッケージシステムは除く。

(2) 設定不備の検知： クラウド設定の不備（ストレージの公開設定ミス等）を自動的に検出し、通知するツールまたは機能を提供すること。

(3) ネットワーク監視： セキュリティ要件が異なるネットワークセグメント間の通信を監視・遮断できる構成とすること。

(4) キャパシティ・性能管理： データ容量、CPU、メモリ等の稼働性能を監視し、将来の負荷予測に基づいた拡張性（スケーラビリティ）を確保すること。

(5) 可用性設計： SLA（サービス品質保証）を明示し、冗長化構成（マルチ AZ 等）による高可用性設計を支援すること。

(6) 時刻同期： ログの正確性を担保するため、クラウド環境内での NTP 等による正確な時刻同期手段を提供すること。

（ユーティリティプログラムに関する要件）

第6条 受注者が提供する運用補助ツールやユーティリティプログラムについて、その機能、権限、およびセキュリティ仕様を明示したドキュメントを提出すること。