SpectA KY-Tool：Service Level Objective（サービスレベル目標）

V1.2
最終更新：2025/4/4

本資料は、「クラウドサービスレベルのチェックリスト」（経済産業省）に基づき、SpectA KY-Tool のセキュリティについてまとめたものです。
参考資料：https://www.meti.go.jp/policy/netsecurity/secdoc/contents/downloadfils/080121saasgl.pdf

区分	種別	サービスレベル項目	規定内容	測定単位	サービス目標（サービスレベルを保証するものではありません）
アプリケーション運	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24時間365日となります。（計画停止／定期保守を除く）
アプリケーション運	可用性	計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	実施3営業日前までにメールもしくは当Webサービス内の通知機能にて各社管理者様に通知いたします。ただし、緊急を要する保守停止の場合は実施当日にメールもしくは当Webサービス内の通知機能にて各社管理者様に通知することもあります。
アプリケーション運	可用性	サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング/方法の記述を含む）	有無	終了3か月前までにメールにて各社管理者様に通知いたします。
アプリケーション運	可用性	サービス稼働率	サービスを利用できる確率（（計画サービス時間－停止時間）÷計画サービス時間）	稼働率（%）	99%以上となります。
アプリケーション運	可用性	ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	有無	DB・ファイルストレージとも、リアルタイムバックアップが2週間分保存されています。 災害発生時はメールにて各社管理者様と協議のうえ、バックアップデータを用いた環境再構築などを実施いたします。
アプリケーション運	可用性	重大障害時の代替手段	早期復旧が不可能な場合の代替措置		バックアップデータから復旧します。外的要因により復旧ができない場合の代替措置はありません。障害の復旧を待つことになります。
アプリケーション運	可用性	代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述		-
アプリケーション運	可用性	アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	数か月に1度ほどの頻度でアップデートいたします。 アップデートに際しサービス停止を伴わない場合、事前通知は原則行わず、リリース後にメールもしくは当Webサービス内の通知機能にて各社管理者様に通知いたします。
アプリケーション運	信頼性	平均復旧時間	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間	弊社営業時間の範囲内で、ベストエフォートで対応します。
アプリケーション運	信頼性	システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	サービスの死活を常時モニタリングしています。
アプリケーション運	信頼性	障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	各社管理者様にメールで連絡いたします。
アプリケーション運	信頼性	障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	弊社営業時間の範囲内で、ベストエフォートで対応します。
アプリケーション運	信頼性	障害監視間隔	障害インシデントを収集／集計する時間間隔	時間（分）	2週間ごとにログを収集／集計しております。
アプリケーション運	信頼性	サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	サービス提供状況を報告しておりません。
アプリケーション運	信頼性	ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	ストレージ/DBへのアクセスログおよびユーザー管理ログを各社管理者様のご要望に応じて提供いたします。標準ではログの保存期間は30日間です。31日以上のログの保存期間をご希望の場合は弊社ご相談ください。 システム上で管理者権限を持つユーザーがログ出力機能を使うことでアクセスログを取得できます。
アプリケーション運	信頼性	時刻同期	クラウドサービス内での時刻同期	有無	サービス内のすべてのリソースは、Azureにより時刻同期が提供されています。
アプリケーション運	性能	オンライン応答時間	オンライン処理の応答時間	時間（秒）	データ分析およびファイルのアップロード・ダウンロードを伴わないユーザー操作に対しては、平均応答時間3秒以内を目標としています。
アプリケーション運	性能	バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	ユーザーが使用するバッチ処理の機能は本システムにはありません。
アプリケーション運	拡張性	カスタマイズ性	ユーザーによるカスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	特定項目の表示非表示の変更などが可能です。他にもご要望に応じて追加いたします。
アプリケーション運	拡張性	外部接続性	既存システムや他のSaaS 等の外部のシステムとの接続仕様（API、開発言語等）	有無	現時点ではAPIを通じた外部接続のための機能は標準版としては提供しておりませんが、ご要望に応じて追加いたします。
アプリケーション運	拡張性	同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無（制約条件）	同時接続利用者数の制限はありません。ライセンス数と同数のユーザーが同時にサービスを利用可能です。
アプリケーション運	拡張性	提供リソースの上限	ディスク容量の上限	処理能力	ディスク容量の上限は標準プランでは10TBです。
サポート	-	サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	受付：24時間365日（メール）。 一次回答：弊社人員が確認後、翌営業日以内。 対応：弊社営業時間内にて実施いたします。
サポート	-	サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	受付：24時間365日（メール）。 一次回答：弊社人員が確認後、翌営業日以内。 対応：弊社営業時間内にて実施いたします。
データ管理	-	バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	DB・ファイルストレージとも、リアルタイムバックアップが2週間分保存されています。
データ管理	-	バックアップデータへのアクセス	バックアップデータへの利用者のアクセス可否	有無／内容	バックアップデータに利用者が直接アクセスすることはできません。復元等の目的でバックアップデータを利用したい場合はサポート窓口までお問い合わせください。
データ管理	-	バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	2週間です。
データ管理	-	データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	サービス解約後1ヶ月以内にデータを破棄いたします。バックアップ保持期間を過ぎたデータは、Microsoftにより完全に削除（上書き）され、復元できなくなります。 データ移行などが必要な場合、解約前にユーザー操作にて取得可能です。
データ管理	-	データの堅牢性	保存データ・バックアップデータの物理的堅牢性	有無／内容	Microsoft Azureサービスを利用しており、物理的なセキュリティ・堅牢性はそちらに依存します。 https://learn.microsoft.com/ja-jp/azure/security/fundamentals/physical-security#equipment-disposal
データ管理	-	データの暗号化	サービス内に保存されているデータの暗号化設定	有無／内容	データベースおよびファイルストレージは、バックアップデータも含めて、Microsoft Azure標準の256ビットAES暗号化が適用されます。 https://docs.microsoft.com/ja-jp/azure/mysql/concepts-security https://learn.microsoft.com/ja-jp/azure/backup/security-overview
セキュリティ	-	通信の暗号化レベル	システムとやりとりされる通信の暗号化強度。	有無	TLSv1.2となります。
セキュリティ	-	パスワードポリシー	本システムでのユーザー登録時に設定するパスワードの強度	有無／内容	8文字以上、文字種類（小文字/大文字/数字/記号）の4種類の内3種以上の使用を強制する設定となっております。
セキュリティ	-	公的認証取得の要件	JIPDEC やJQA 等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること。	有無	ISO27001（ISMS認証）取得済。
セキュリティ	-	アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること。	有無／実施状況	外部ベンダーによるWebアプリケーション脆弱性診断を、 下記基準に基づき年1回の頻度で実施いたします。 ・OWASP既定の「OWASP Top 10」、IPA既定の「安全なウェブサイトの作り方」に 含まれる脆弱性に対応する診断を実施 ・IPA情報基準適合サービスリスト(脆弱性診断サービス)記載のベンダーによる診断実施 ※2024年6月に実施。
セキュリティ	-	情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること。	有無／設定状況	弊社側で、本番環境のデータにアクセスすることが出来るのは、弊社のセキュリティ管理者の承認を得たシステム運用担当に限られ、一定期間のみアクセスできるよう制限しております。
セキュリティ	-	情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること。	有無	お客様のデータは弊社の機密情報取り扱い規程の対象となります。弊社環境外への持ち出しができないよう、セキュリティシステムやルールにより保護しております。
セキュリティ	-	マルウェア対策	本システムにおけるマルウェア対策	有無／内容	Microsoft（Defender for Cloud）により常時監視され、高リスクのインシデントは即座に弊社へ通知されます。対策エンジン等の自動更新が行われます。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/antimalware

セキュリティ	-	二次記憶媒体の安全性対策	本システムにおける二次記憶媒体使用状況と安全性対策	有無／内容	バックアップ取得・保存はAzureにより自動で行われます。USBメモリやCD等の二次記憶媒体は使用していません。