

EventRegist クラウドサービス セキュリティチェックリスト

総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン(第3版)」準拠

サービス名	EventRegist (イベントレジスト)
提供事業者	イベントレジスト株式会社
サービスURL	https://eventregist.com/
サービス種別	SaaS (イベント登録・管理プラットフォーム)
基準文書	総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン(第3版)」(2021年9月)
対象範囲	Ⅱ.共通編 + Ⅲ.SaaS編 (Ⅳ.PaaS/IaaS編・Ⅴ.IoT編は対象外)
作成日	2026年5月28日
作成者	イベントレジスト株式会社

■ 回答区分の凡例

○	対応している / 実装済み
△	一部対応 / 条件付き対応 / 計画中
×	未対応
—	本サービスでは対象外

■ レベルの凡例 (ガイドライン上の位置づけ)

基本	ガイドラインで「基本」とされる要求事項
推奨	ガイドラインで「推奨」(ベストプラクティス) とされる要求事項

■ 本書の位置づけ

本書は、お客様のセキュリティ評価を支援する目的で、総務省ガイドライン(第3版)の章構成に沿ってEventRegistの対応状況を整理したものです。確認項目はガイドラインの管理策タイトルに基づき、当社で要約しています。個別の機微な実装詳細はNDA締結後に開示します。
本書記載内容は2026年5月時点のものであり、継続的な改善により変更される場合があります。

項番	レベル	大項目	中項目	小項目	確認項目	回答	補足説明
II.1.1.1	基本	II.1 情報セキュリティへの組織的取組の基本方針	II.1.1 組織の基本的な方針を定めた文書	方針の作成・承認・配布	情報セキュリティに関する基本方針・役割・責任を定めた文書を作成し、経営陣の承認を経て組織内に配布しているか	○	情報セキュリティ基本方針を策定し、経営層の承認のもと社内へ周知。ISMS認証取得に伴い文書化体制を整備。
II.1.1.2	基本	II.1 情報セキュリティへの組織的取組の基本方針	II.1.1 組織の基本的な方針を定めた文書	方針の変更	基本方針を定期的またはサービス提供に関わる重大な変更時に見直す体制があるか	○	ISMS運用の枠組みで定期レビューを実施。組織・業務・法的・技術環境の変化に応じて改定。
II.1.1.3	推奨	II.1 情報セキュリティへの組織的取組の基本方針	II.1.1 組織の基本的な方針を定めた文書	文書保護	セキュリティ方針文書を不正開示・改変から保護しているか	○	文書管理ポリシーに基づき、アクセス権限を限定して保管。
II.2.1.1	基本	II.2 情報セキュリティのための組織	II.2.1 内部組織	情報セキュリティ責任者	組織全体の情報セキュリティに責任を持つ責任者を任命し、必要なリソース支援を行っているか	○	情報セキュリティ責任者を任命。ISMS体制の下、経営層の支援を受けて運用。
II.2.1.2	基本	II.2 情報セキュリティのための組織	II.2.1 内部組織	システム一覧	保有・提供するシステム・アプリケーション・クラウドサービスの一覧を作成し責任者を定めているか	○	サービス基盤・利用クラウドサービスの一覧を維持。各システムに管理責任者を割当。
II.2.1.3	基本	II.2 情報セキュリティのための組織	II.2.1 内部組織	相反する職務と責任の分離	相反する職務・責任範囲を分離し、単独で資産にアクセス・修正できない仕組みがあるか	○	開発・運用・承認の役割分離を実施。本番リリースはPRレビュー+承認者によるデプロイ承認制。
II.2.1.4	推奨	II.2 情報セキュリティのための組織	II.2.1 内部組織	リスク管理戦略	組織全体の包括的なリスク管理戦略を策定し、定期見直しを行っているか	○	ISMSの枠組みで情報資産のリスクアセスメントを年次実施。
II.2.1.5	推奨	II.2 情報セキュリティのための組織	II.2.1 内部組織	テスト、トレーニング及びモニタリング	情報セキュリティのテスト・トレーニング・モニタリングを実施しているか	○	従業員向け教育・訓練、脆弱性診断、ログモニタリングを定期実施。
II.2.1.6	推奨	II.2 情報セキュリティのための組織	II.2.1 内部組織	組織内苦情管理	組織内の情報セキュリティに関する苦情を管理する仕組みがあるか	○	内部通報・相談窓口を設置。
II.2.2.1	基本	II.2 情報セキュリティのための組織	II.2.2 モバイル機器及びテレワーク	モバイル機器の利用方針	モバイル機器利用に関する方針を定めているか	○	セキュリティ管理基準にて全端末でディスク暗号化、自動ロック、紛失時の遠隔ワイプを規定。
II.2.2.2	基本	II.2 情報セキュリティのための組織	II.2.2 モバイル機器及びテレワーク	テレワーク環境での情報保護	テレワーク環境での情報保護対策を定めているか	○	VPN利用を必須化、公共Wi-Fi利用禁止。リモート環境でのアクセス制御を実施。
II.3.1.1	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	リスク対策と文書化	サプライチェーン事業者との間でリスク対策を合意し文書化しているか	○	AWS等の主要サプライヤとの契約・SLAで責任範囲を明確化。委託先には「業務委託者向けセキュリティ管理基準」を適用。
II.3.1.2	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	サービスの監視	サプライチェーン事業者のサービス提供状況を監視しているか	○	AWS等のサービス稼働状況をモニタリング。主要委託先のパフォーマンスを定期確認。
II.3.1.3	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	リスク評価とレビュー	サプライチェーンに関するリスクを定期評価・レビューしているか	○	委託先・利用クラウドサービスのリスクを年次評価。
II.3.1.4	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	関連情報の保護	サプライチェーン事業者と共有する情報を保護しているか	○	委託先との情報授受は秘密保持契約(NDA)のもと実施。
II.3.1.5	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	侵害通知	サプライチェーンで侵害が発生した際の通知体制があるか	○	委託契約上、インシデント発生時の通知義務を明示。
II.3.1.6	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	変更管理	サプライチェーンの変更管理を実施しているか	○	委託先の変更時はリスク評価を実施。
II.3.1.7	推奨	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	耐タンパー性と検出	サプライチェーンにおける改ざんに対する耐タンパー性・検出機能を備えているか	△	AWS等の利用基盤側で対策。アプリ層では署名・改ざん検知の必要性を案件ごとに評価。
II.3.1.8	推奨	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	システム又はシステムコンポーネントの検査	サプライチェーンから調達したコンポーネントの検査を実施しているか	○	OSS依存ライブラリは脆弱性スキャンで継続的にチェック。
II.3.1.9	推奨	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	システムコンポーネントの信頼性	サプライチェーンから調達するコンポーネントの信頼性を確認しているか	○	公式リポジトリ・信頼できる提供元からのみ調達。
II.3.1.10	基本	II.3 サプライチェーンに関する管理	II.3.1 サプライチェーン事業者間の合意	システムコンポーネントの廃棄	システムコンポーネントの廃棄時にデータ漏洩リスクを排除しているか	○	AWSマネージドサービスを利用しており、ストレージ廃棄はAWSの標準プロセスに従う。
II.3.2.1	基本	II.3 サプライチェーンに関する管理	II.3.2 サプライチェーン事業者の選定	選定・契約	サプライチェーン事業者の選定基準と契約手続きを定めているか	○	委託先選定時にセキュリティ要件の充足を評価し、「業務委託者向けセキュリティ管理基準」遵守を契約に含める。
II.4.1.1	基本	II.4 情報資産の管理	II.4.1 情報資産に対する責任	管理責任者	情報資産ごとに管理責任者を定めているか	○	情報資産台帳を整備し、資産ごとに管理責任者を割当。
II.4.1.2	基本	II.4 情報資産の管理	II.4.1 情報資産に対する責任	事業者間の引継ぎ	事業者変更時にデータの引継ぎ・返却・削除の手順を定めているか	○	契約終了時のデータ返却・削除手順を利用規約および個別契約で規定。
II.4.1.3	基本	II.4 情報資産の管理	II.4.1 情報資産に対する責任	バックアップ	利用者データのバックアップを適切に取得しているか	○	AWS RDSの自動バックアップ機能により日次でDBバックアップを取得。
II.4.1.4	推奨	II.4 情報資産の管理	II.4.1 情報資産に対する責任	当初目的との一致	利用者データを当初目的以外に使用していないか	○	利用者データはサービス提供目的以外で使用しない旨を利用規約・プライバシーポリシーで明示。

項番	レベル	大項目	中項目	小項目	確認項目	回答	補足説明
II.4.2.1	基本	II.4 情報資産の管理	II.4.2 情報の分類	資産目録	情報資産の目録を作成・維持しているか	○	情報資産台帳を整備し定期的に更新。
II.4.2.2	基本	II.4 情報資産の管理	II.4.2 情報の分類	データ識別	データの重要度に応じた識別・分類を行っているか	○	情報資産の機密度区分を定義し、取扱基準を適用。
II.4.2.3	基本	II.4 情報資産の管理	II.4.2 情報の分類	情報資産の取扱い	分類に応じた情報資産の取扱手順を定めているか	○	機密度区分ごとの取扱基準(保管・転送・廃棄)を規程で定義。
II.4.3.1	基本	II.4 情報資産の管理	II.4.3 情報セキュリティポリシーの遵守、点検及び監査	レビュー	情報セキュリティポリシーの遵守状況を定期レビューしているか	○	ISMS内部監査を年次実施。
II.4.3.2	基本	II.4 情報資産の管理	II.4.3 情報セキュリティポリシーの遵守、点検及び監査	点検・監査	情報セキュリティの点検・監査を実施しているか	○	ISMS外部審査(年次)、内部監査、脆弱性診断、Pマーク監査を実施。
II.4.4.1	基本	II.4 情報資産の管理	II.4.4 アクセス管理	アクセス制御方針	アクセス制御方針を定めているか	○	アクセス制御規程を整備。最小権限原則に基づき権限付与。
II.4.4.2	基本	II.4 情報資産の管理	II.4.4 アクセス管理	アクセス制御	アクセス制御を技術的に実装しているか	○	ロールベースアクセス制御(RBAC)を実装。本番環境アクセスは限定された担当者のみ。
II.4.4.3	基本	II.4 情報資産の管理	II.4.4 アクセス管理	ユーティリティプログラムの使用	システム制御を上書きできるユーティリティの使用を制限しているか	○	本番環境での特権コマンド・ユーティリティ実行を限定的に制御。
II.4.4.4	基本	II.4 情報資産の管理	II.4.4 アクセス管理	プログラムソースコードへのアクセス	ソースコードへのアクセスを制限しているか	○	ソースコードリポジトリへのアクセスは開発担当者に限定。
II.4.4.5	基本	II.4 情報資産の管理	II.4.4 アクセス管理	アクセス制御となりすまし対策	なりすまし対策(認証強化等)を実装しているか	○	管理者向けにMFAを導入。ログイン失敗時のロック機構を実装。
II.4.5.1	基本	II.4 情報資産の管理	II.4.5 構成管理	構成管理のポリシーと手順	システム構成管理のポリシーと手順を定めているか	○	IaC(コード化された構成管理)で本番構成を管理。変更手順を規程化。
II.4.5.2	推奨	II.4 情報資産の管理	II.4.5 構成管理	ベースライン構成	ベースライン構成を定めて管理しているか	○	AWS基盤の構成はIaCで定義しバージョン管理。
II.4.5.3	推奨	II.4 情報資産の管理	II.4.5 構成管理	構成変更管理	構成変更の管理プロセスを実施しているか	○	コードレビューによる変更管理。デプロイ履歴を保管。
II.4.5.4	推奨	II.4 情報資産の管理	II.4.5 構成管理	変更に対するアクセス制限	構成変更のアクセスを制限しているか	○	本番環境への変更権限は限定担当者のみ。
II.4.5.5	推奨	II.4 情報資産の管理	II.4.5 構成管理	設定項目	重要な設定項目を識別・管理しているか	○	セキュリティに関わる設定値をコード化し、レビュー対象とする。
II.4.5.6	推奨	II.4 情報資産の管理	II.4.5 構成管理	ソフトウェアの使用制限	業務端末で許可されたソフトウェアのみを使用する制限があるか	△	業務上必要なソフトウェアは指定。完全な実行制限(EDR等)は導入を検討中。
II.4.5.7	推奨	II.4 情報資産の管理	II.4.5 構成管理	クラウドサービス利用者によるソフトウェアのインストール	利用者によるソフトウェアインストールを管理しているか	—	SaaSのため、利用者が本サービス基盤へソフトウェアをインストールする仕組みは持たない。
II.4.5.8	推奨	II.4 情報資産の管理	II.4.5 構成管理	情報の場所	利用者データの保管場所を明示しているか	○	原則として日本国内(AWS東京リージョン)で保管することを利用規約・FAQ等で開示。
II.5.1.1	基本	II.5 従業員に係る情報セキュリティ	II.5.1 雇用前	雇用契約	従業員との雇用契約に情報セキュリティ・守秘義務条項を含めているか	○	入社時に守秘義務契約を締結。退職後の継続義務も明示。
II.5.2.1	基本	II.5 従業員に係る情報セキュリティ	II.5.2 雇用期間中	教育・訓練	従業員に対する情報セキュリティ教育・訓練を実施しているか	○	全従業員向けに情報セキュリティ教育を定期実施。
II.5.2.2	推奨	II.5 従業員に係る情報セキュリティ	II.5.2 雇用期間中	教育のフィードバック	教育の効果測定・フィードバックを行っているか	○	理解度評価を実施し、必要に応じて追加教育を実施。
II.5.2.3	基本	II.5 従業員に係る情報セキュリティ	II.5.2 雇用期間中	契約違反	契約違反時の懲戒手続きを定めているか	○	就業規則において情報セキュリティ違反時の懲戒手続きを規定。
II.5.3.1	基本	II.5 従業員に係る情報セキュリティ	II.5.3 雇用の終了又は変更	アクセス権・資産の取扱い	退職・異動時のアクセス権削除・資産返却の手順を定めているか	○	退職・異動時の権限剥奪・端末返却手順を規程化し運用。
II.6.1.1	基本	II.6 情報セキュリティインシデントの管理	II.6.1 情報セキュリティインシデント及び低い弱性の報告	組織内報告	インシデント・脆弱性発見時の組織内報告ルールを定めているか	○	「情報セキュリティ事故対応フロー」にて検知・連絡→初期対応→回復→事後対応の手順を規定。
II.6.1.2	基本	II.6 情報セキュリティインシデントの管理	II.6.1 情報セキュリティインシデント及び低い弱性の報告	クラウドサービス事業者とクラウドサービス利用者間の報告	事業者・利用者間でのインシデント報告体制があるか	○	重大インシデント発生時は契約に基づき利用者へ通知。公開影響時は外部公表も実施。
II.6.1.3	基本	II.6 情報セキュリティインシデントの管理	II.6.1 情報セキュリティインシデント及び低い弱性の報告	インシデントの評価と分類	インシデントの重大度評価・分類を行っているか	○	事故対応フロー内でインシデントの影響度評価と分類手順を規定。

項番	レベル	大項目	中項目	小項目	確認項目	回答	補足説明
II.6.1.4	基本	II.6 情報セキュリティインシデントの管理	II.6.1 情報セキュリティインシデント及びぜい弱性の報告	フィードバック	インシデント対応の結果を組織内にフィードバックする仕組みがあるか	○	事後対応として報告書作成、再発防止策の検討・実施・周知を規格化。
II.6.1.5	基本	II.6 情報セキュリティインシデントの管理	II.6.1 情報セキュリティインシデント及びぜい弱性の報告	証拠の収集・取得	インシデント発生時の証拠保全手順を定めているか	○	事故対応フロー内でログ・関連データの保全手順を規定。
II.7.1.1	基本	II.7 コンプライアンス	II.7.1 法令と規則の遵守	関連法規と記録	サービス提供地域の関連法規を把握し、遵守記録を残しているか	○	個人情報保護法、不正アクセス禁止法、電気通信事業法等を踏まえた運用を実施。
II.7.1.2	基本	II.7 コンプライアンス	II.7.1 法令と規則の遵守	利用可否	利用者の所在地・データの種別に応じたサービス利用可否を判断する仕組みがあるか	△	一部の機能を海外からの利用を制限。
II.7.1.3	基本	II.7 コンプライアンス	II.7.1 法令と規則の遵守	ソフトウェア製品	使用するソフトウェアのライセンスを適切に管理しているか	○	OSSライセンス・商用ソフトウェアライセンスを管理。
II.7.1.4	基本	II.7 コンプライアンス	II.7.1 法令と規則の遵守	不正アクセス・流出からの保護	個人情報・利用者データを不正アクセス・流出から保護しているか	○	通信暗号化(TLS)、保管時暗号化、アクセス制御、ログ監視を多層的に実施。Pマーク認証取得。
II.7.1.5	基本	II.7 コンプライアンス	II.7.1 法令と規則の遵守	暗号化	法令で要求される暗号化要件を満たしているか	○	業界標準の暗号化アルゴリズムを使用。クレジットカード情報は自社で保持せずPCI DSS準拠の決済代行を利用。
II.8.1.1	基本	II.8 ユーザサポートの責任	II.8.1 利用者への責任	責任	事業者・利用者の責任分界を明示しているか	○	利用規約・契約で責任分界を明示。SaaS責任共有モデルに基づく。
II.8.1.2	基本	II.8 ユーザサポートの責任	II.8.1 利用者への責任	SLA	SLA(サービスレベル合意)を提示しているか	×	SLAは提示していない。
II.8.1.3	基本	II.8 ユーザサポートの責任	II.8.1 利用者への責任	情報提供	利用者に対しサービス仕様・運用情報を提供しているか	○	利用規約、サービス仕様、FAQをサービスサイトで公開。
II.8.1.4	基本	II.8 ユーザサポートの責任	II.8.1 利用者への責任	クラウドサービス利用者からの苦情対応	利用者からの苦情に対応する窓口を設置しているか	○	問い合わせ窓口(メール)を設置。営業時間内に対応。
II.8.2.1	基本	II.8 ユーザサポートの責任	II.8.2 保守	システム保守ポリシーと手順	システム保守のポリシー・手順を定めているか	○	システム保守手順を整備。定期メンテナンス・緊急対応手順を文書化。
II.8.2.2	基本	II.8 ユーザサポートの責任	II.8.2 保守	保守管理	保守作業を計画的に管理しているか	○	計画メンテナンスは事前通知のうえ実施。
II.8.2.3	基本	II.8 ユーザサポートの責任	II.8.2 保守	保守ツール	保守ツールの使用を管理・制御しているか	○	保守ツールの利用は権限を付与された担当者のみが実施。
II.8.2.4	基本	II.8 ユーザサポートの責任	II.8.2 保守	リモート保守	リモート保守時のセキュリティ対策を実施しているか	○	リモートアクセスはVPN+MFA経由。アクセスログを取得。
II.8.2.5	基本	II.8 ユーザサポートの責任	II.8.2 保守	保守要員	保守要員の力量・権限を管理しているか	○	保守作業は教育を受けた限定された担当者のみが実施。
II.8.2.6	基本	II.8 ユーザサポートの責任	II.8.2 保守	保守要員による保守	保守要員による保守作業を記録・監視しているか	○	本番環境への作業はログ取得対象。
II.8.2.7	基本	II.8 ユーザサポートの責任	II.8.2 保守	タイムリーな保守	セキュリティパッチ等を適時に適用しているか	○	脆弱性情報を継続監視し、リスクに応じて適時パッチ適用。
II.9.1.1	基本	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.1 情報セキュリティの継続	情報セキュリティ継続計画の策定と実施	事業継続におけるセキュリティ継続計画を策定しているか	○	事故対応フロー内でBCPの実施判断手順を規定。
II.9.1.2	基本	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.1 情報セキュリティの継続	情報セキュリティ継続の検証、レビュー及び評価	セキュリティ継続計画を検証・レビューしているか	○	ISMS運用の中で年次レビュー。
II.9.2.1	基本	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.2 緊急時対応計画	緊急時対応計画の策定と手順	緊急時対応計画を策定しているか	○	事故対応フローを整備。重大障害時の判断・連絡・復旧手順を規定。
II.9.2.2	推奨	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.2 緊急時対応計画	緊急時対応トレーニング	緊急時対応のトレーニングを実施しているか	○	障害対応訓練を定期実施。
II.9.2.3	推奨	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.2 緊急時対応計画	緊急時対応計画のテスト	緊急時対応計画をテストしているか	○	障害復旧手順は定期的に検証。
II.9.2.4	推奨	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.2 緊急時対応計画	代替処理サイト	代替処理サイトを確保しているか	○	AWSマルチAZ構成により単一AZ障害時のサービス継続を確保。
II.9.2.5	推奨	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.2 緊急時対応計画	代替処理サイトで再開	代替処理サイトでサービスを再開できるか	○	AWSマルチAZ構成によりフェイルオーバー可能。
II.9.2.6	推奨	II.9 事業継続マネジメントにおける情報セキュリティ	II.9.2 緊急時対応計画	通信サービス	通信サービスの冗長性を確保しているか	○	AWSの冗長化されたネットワーク基盤を利用。

項番	レベル	大項目	中項目	小項目	確認項目	回答	補足説明
Ⅱ.9.2.7	推奨	Ⅱ.9 事業継続マネジメントにおける情報セキュリティ	Ⅱ.9.2 緊急時対応計画	システムの復旧と再構成	システムの復旧・再構成手順があるか	○	リストア手順を文書化。IaCにより環境再構築が可能。
Ⅱ.9.2.8	推奨	Ⅱ.9 事業継続マネジメントにおける情報セキュリティ	Ⅱ.9.2 緊急時対応計画	代替通信プロトコル	代替通信プロトコルを用意しているか	△	標準プロトコル(HTTPS)で運用。リージョン障害時の代替手段は今後の検討課題。
Ⅱ.9.2.9	推奨	Ⅱ.9 事業継続マネジメントにおける情報セキュリティ	Ⅱ.9.2 緊急時対応計画	代替の情報セキュリティ対策	代替のセキュリティ対策手段を準備しているか	○	重要なセキュリティ機能は冗長化された構成で運用。
Ⅱ.10.1.1	基本	Ⅱ.10 その他	Ⅱ.10.1 暗号と認証	方針	暗号と認証に関する方針を定めているか	○	暗号化方針・認証方針を策定。業界標準アルゴリズムを採用。
Ⅱ.10.1.2	基本	Ⅱ.10 その他	Ⅱ.10.1 暗号と認証	情報提供	暗号・認証方式について利用者に情報提供しているか	○	通信はHTTPS(TLS)で暗号化することをFAQ等で明示。
Ⅱ.10.1.3	基本	Ⅱ.10 その他	Ⅱ.10.1 暗号と認証	暗号鍵の作成と管理	暗号鍵の作成・管理を適切に行っているか	○	暗号鍵はAWS KMSで管理。鍵へのアクセスは権限ベースで制御。
Ⅱ.10.2.1	基本	Ⅱ.10 その他	Ⅱ.10.2 開発プロセスにおけるセキュリティ	開発プロセスにおける情報セキュリティへの取組	開発プロセスでセキュリティを考慮しているか	○	セキュアコーディング規約、PRレビュー、定期的な脆弱性診断、ステージング環境での検証を実施。
Ⅲ.1.1.1	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	情報セキュリティ監視手順の策定	情報セキュリティ監視の手順を策定しているか	○	稼働・性能・エラー監視手順を整備。
Ⅲ.1.1.2	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	運用管理端末	運用管理端末のセキュリティ対策を実施しているか	○	運用管理端末はディスク暗号化、MFA、アンチウイルスソフト導入、アクセス制限を実施。
Ⅲ.1.1.3	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	稼働・障害監視	サービスの稼働・障害を24時間監視しているか	○	24時間有人・自動監視。異常時は担当者へアラート通知。
Ⅲ.1.1.4	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	追加報告	重大事象発生時の追加報告体制があるか	○	重大インシデント時は契約に基づき追加情報を提供。
Ⅲ.1.1.5	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	定期報告	稼働状況等を利用者へ定期報告しているか	△	個別契約・案件において定期報告に対応可能。
Ⅲ.1.1.6	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	時刻同期	システム時刻をNTP等で同期しているか	○	NTPサービスにより全システム時刻を同期。
Ⅲ.1.1.7	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	パスワード管理	パスワード管理(複雑性・有効期限等)の仕組みがあるか	○	パスワード強度要件を強制。ユーザパスワードはハッシュ化して保管。
Ⅲ.1.1.8	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	クラウドサービスの変更管理	サービスの変更を管理しているか	○	コードレビュー+ステージング検証を経て本番リリース。デプロイ履歴を保管。
Ⅲ.1.1.9	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	リソース監視	システムリソースを監視しているか	○	CPU・メモリ・ストレージ・ネットワーク使用率を監視。
Ⅲ.1.1.10	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	環境分離	本番・ステージング・開発環境を分離しているか	○	AWS環境を本番・ステージング・開発で分離。データも分離。
Ⅲ.1.1.11	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	マルウェア対策	サーバ・端末のマルウェア対策を実施しているか	○	業務端末にアンチウイルスソフト導入。サーバはAWSマネージドサービス利用+最小実行環境で運用。
Ⅲ.1.1.12	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	イベントログの取得	イベントログを取得しているか	○	アプリログ、アクセスログ、システムログ、管理者操作ログを取得・集約。
Ⅲ.1.1.13	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	ログの保護	ログを改ざん・削除から保護しているか	○	ログは専用ストレージへ集約し、書込専用権限+保管期間を設定。
Ⅲ.1.1.14	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	作業記録	保守・運用作業の記録を残しているか	○	本番作業は作業記録を残す運用。
Ⅲ.1.1.15	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	ソフトウェア導入	ソフトウェア導入の手順を管理しているか	○	ソフトウェア導入はレビューを経て実施。OSSライブラリも依存管理ツールで管理。
Ⅲ.1.1.16	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.1 運用管理	技術的ぜい弱性	技術的脆弱性への対策(脆弱性管理・パッチ適用等)を実施しているか	○	外部脆弱性診断を定期実施。検出脆弱性は社内Issueで追跡・是正。OWASP Top10対策(XSS, SQLi, CSRF, 認可不備、GraphQL Introspection無効化、レート制限等)を継続実施。
Ⅲ.1.2.1	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.2 システム及び情報の完全性	原本性確保	データの原本性を確保しているか	○	DBの更新履歴・操作ログを保持。重要操作は監査ログ対象。
Ⅲ.1.2.2	推奨	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.2 システム及び情報の完全性	メモリ保護	メモリ保護対策を実装しているか	○	AWSマネージドサービスおよび最新版ランタイムを利用し、メモリ保護機構の恩恵を受ける。
Ⅲ.1.2.3	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.2 システム及び情報の完全性	セキュリティ侵害の検知	セキュリティ侵害を検知する仕組みがあるか	○	異常アクセス・エラーログ監視によりインシデント兆候を検知。

項番	レベル	大項目	中項目	小項目	確認項目	回答	補足説明
Ⅲ.1.2.4	推奨	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.2 システム及び情報の完全性	情報の更新	情報の更新が適切に管理されているか	○	データ更新は権限制御・トランザクション制御のもと実施。
Ⅲ.1.2.5	推奨	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.2 システム及び情報の完全性	代替情報源	情報の正確性を確認するための代替情報源を確保しているか	△	システムのクロスチェックの仕組みは限定的。重要処理は監査ログで照合可能。
Ⅲ.1.2.6	推奨	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.2 システム及び情報の完全性	情報の断片化	情報の断片化(分散保管)対策を実施しているか	△	AWSマルチAZによる冗長化は実施。アプリ層での断片化は実装していない。
Ⅲ.1.3.1	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.3 媒体の保管と廃棄	媒体保管	記憶媒体の保管を適切に管理しているか	○	本番データの物理媒体保管はAWS側の物理セキュリティに準拠。社内では物理媒体での機密データ保管を原則行わない。
Ⅲ.1.3.2	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.3 媒体の保管と廃棄	廃棄	媒体・データの廃棄を安全に行っているか	○	AWSストレージはAWSの標準廃棄プロセスに従う。社内端末は廃棄時にディスク消去または物理破壊。
Ⅲ.1.3.3	基本	Ⅲ.1 運用における情報セキュリティ	Ⅲ.1.3 媒体の保管と廃棄	輸送	媒体の輸送時の保護対策があるか	—	本サービスは物理媒体の輸送を伴わないクラウドサービスであり、原則として該当しない。
Ⅲ.2.1.1	基本	Ⅲ.2 アプリケーション	Ⅲ.2.1 アプリケーションの情報セキュリティ対策	ウイルス対策	アプリケーションへのウイルス・マルウェア対策を実施しているか	○	ユーザアップロードファイルは適切に処理。社内端末ではアンチウイルスソフト導入。
Ⅲ.2.1.2	基本	Ⅲ.2 アプリケーション	Ⅲ.2.1 アプリケーションの情報セキュリティ対策	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワーク上のサービスのセキュリティを考慮しているか	○	全通信HTTPS化、TLS旧バージョン無効化、WAF相当の保護、レート制限を実施。
Ⅲ.2.1.3	基本	Ⅲ.2 アプリケーション	Ⅲ.2.1 アプリケーションの情報セキュリティ対策	アプリケーションサービスのトランザクションの保護	アプリケーションのトランザクションを保護しているか	○	決済処理はPCI DSS準拠の決済代行(トークン化方式)を利用。重要トランザクションはログ取得対象。
Ⅲ.2.1.4	基本	Ⅲ.2 アプリケーション	Ⅲ.2.1 アプリケーションの情報セキュリティ対策	プラットフォーム変更後のアプリケーションの技術的レビュー	プラットフォーム変更時の技術的レビューを実施しているか	○	プラットフォーム変更時はステージング環境で検証してから本番反映。
Ⅲ.2.1.5	基本	Ⅲ.2 アプリケーション	Ⅲ.2.1 アプリケーションの情報セキュリティ対策	パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更を制限しているか	○	OSS・パッケージソフトの変更管理を実施。バージョン固定+依存性更新管理。
Ⅲ.2.2.1	基本	Ⅲ.2 アプリケーション	Ⅲ.2.2 データの保護	バックアップ	データの定期バックアップを実施しているか	○	AWS RDS自動バックアップにより日次取得。
Ⅲ.2.2.2	基本	Ⅲ.2 アプリケーション	Ⅲ.2.2 データの保護	バックアップ情報の完全性	バックアップ情報の完全性を確認しているか	○	AWS提供の機能によりバックアップ完全性を担保。リストア手順を文書化。
Ⅲ.2.3.1	基本	Ⅲ.2 アプリケーション	Ⅲ.2.3 セッション管理	セッションのライフサイクル管理	セッションのライフサイクル(発行・有効期限・破棄)を管理しているか	○	セッショントークンは適切な有効期限を設定。ログアウト時に破棄。
Ⅲ.2.3.2	基本	Ⅲ.2 アプリケーション	Ⅲ.2.3 セッション管理	セッションの真正性	セッションの真正性を確保しているか	○	セッショントークンは暗号学的に安全な方式で生成。HTTPS+HttpOnly+Secure属性で保護。
Ⅲ.2.3.3	基本	Ⅲ.2 アプリケーション	Ⅲ.2.3 セッション管理	同時セッションの制御	同時セッションを制御できるか	△	標準では同時セッション数の上限は設けていない。必要に応じて個別対応。
Ⅲ.2.3.4	基本	Ⅲ.2 アプリケーション	Ⅲ.2.3 セッション管理	セッションのロック	セッションのロック・タイムアウト機能があるか	○	一定時間操作がない場合の自動ログアウトを実装。