# どっと原価3クラウドサービスレベルチェックシート

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)を基に任意で項目を追加し、株式会社 建設ドットウェブの提供する「どっと原価３」のセキュリティについてまとめたものです。

改定日：2024/11/1

| No. | 種別 | サービスレベル項目例 | 規程内容 | 対応/可否 | 内容 |
|---|---|---|---|---|---|
| **アプリケーション運用** | | | | | |
| 1 | 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） | ○ | 24時間365日（緊急/定期メンテナンスを除く） |
| 2 | | 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） | ○ | 目安として1週間前から完了まで、サービス内のポータル画面に通知用画面が表示されます。<br>また、定期メンテナンス開始20分前から、サービス起動時に警告画面が表示されます。 |
| 3 | | 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） | ○ | サービス終了3ヶ月前までに通知致します。（利用規約10条） |
| 4 | | 突然のサービス提供停止時の対処 | プログラムや、システム環境の各種設定データの預託等の措置の有無 | × | ありません。 |
| 5 | | 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） | × | 以下リンク先にて各クラウドサービスの月別稼働状況を公開しています。<br>https://www.kendweb.net/cloudstatus/ |
| 6 | | 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 | × | ありません。 |
| 7 | | 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 | × | 代替手段は提供していません。 |
| 8 | | 代替処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 | × | - |
| 9 | | 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 | ○ | 三ヶ月に1回程度の頻度でアップデートしています。アップデート1週間前にサービス内で通知します。<br>ただし、不定期で緊急アップデートを行うこともあります。 |
| 10 | 信頼性 | 平均復旧時間(MTTR) | 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） | × | 設定していません。 |
| 11 | | 目標復旧時間(RTO) | 障害発生後のサービス提供の再開に関して設定された目標時間 | × | 設定していません。 |
| 12 | | 目標復旧時点(RPO) | 障害発生後のサービス提供再開に対応するバックアップ世代管理の目標時間 | × | 設定していません。 |
| 13 | | 障害発生件数 | 1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数 | - | 過去1年間に発生した回数は1件です。/その内、対応に長時間要した回数は0件です。<br>集計期間：2023-07-01～2024-06-30 |
| 14 | | システム監査基準 | 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 | ○ | 実施しています。 |
| 15 | | 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） | ○ | ポータルサイト及び弊社ホームページを介して通知・報告いたします。 |
| 16 | | 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 | ○ | セキュリティインシデントに対しては、社内で認知してから48時間以内に報告します。 |
| 17 | | 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 | ○ | リアルタイムで収集していますが、業務時間内でのみ集計しています。 |
| 18 | | サービス提供状況の報告/間隔 | サービス提供状況を報告する方法／時間間隔 | ○ | ホームページにて稼働状況を5分毎に公開しています。<br>個別の報告はしておりません。 |
| 19 | | 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） | ○ | 利用者はサービス内でログを取得することが可能ですが、当社が管理するシステムログ等は原則提供しません。 |
| 20 | 性能 | 応答時間 | 処理の応答時間 | × | 公開しておりません。 |
| 21 | | 遅延 | 処理の応答時間の遅延継続時間 | × | 公開しておりません。 |
| 22 | | バッチ処理時間 | バッチ処理（一括処理）の応答時間 | × | 公開しておりません。 |
| 23 | | 時刻同期 | 時刻同期ができる環境か | ○ | NTPにて同期しています。 |
| 24 | 拡張性 | カスタマイズ性 | 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 | ○ | サービス内の標準機能にて項目名称などの設定が可能です。<br>有償で個別開発も対応しています。 |
| 25 | | 外部接続性 | 既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等） | ○ | 外部連携用のAPI(一部機能)を公開しています。 |
| 26 | | 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 | ○ | ライセンス数分可能です。 |
| 27 | | 提供リソースの上限 | ディスク容量の上限／ページビューの上限 | ○ | 上限は20GBです。 |
| **サポート** | | | | | |
| 27 | 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 | ○ | 障害時も一般問い合わせ体制と同様です。 |
| 28 | 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 | ○ | 電話・メールにて対応しています。<br>通常のサポート業務の対応時間は、平日9：00～17：30（祝日、年末年始等弊社休日は除く）です。 |
| **データ管理** | | | | | |
| 29 | 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 | ○ | システム全体のデータバックアップは、国内のデータセンターに保管されていますが、このデータに対してお客様がアクセスすることはできません。<br>アクセス権はシステム担当のみに制限し、復旧対象は利用規約に記載しています。<br>利用者が任意のタイミングでバックアップを取得することも可能です。 |
| 30 | バックアップデータを取得するタイミング(RPO) | | バックアップデータをとり、データを保証する時間 | ○ | 24時間 |
| 31 | 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 | ○ | お客様のサービス契約期間終了後1ヶ月後まで保管されます。 |
| 32 | 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 | ○ | サービス契約終了日から1ヶ月後以降に、弊社が定める方針に従いデータおよび保管媒体を削除します。 |
| 33 | バックアップ世代数 | | 保証する世代数 | ○ | 7世代<br>※お客様側で復旧などにご利用できるのは直近の1世代までです。以降のバックアップデータの提供は災害時などを除き原則提供は行いません。（利用規約16条） |
| 34 | データ保護のための暗号化要件 | | データを保護するにあたり、暗号化要件の有無 | × | 設定していません。 |
| 35 | マルチテナントストレージにおけるキー管理要件 | | マルチテナントストレージのキー管理要件の有無、内容 | ○ | 設定しています。 |
| 36 | データ漏えい・破壊時の補償／保険 | | データ漏えい・破壊時の補償／保険の有無 | ○ | 当社の故意重過失により、利用者自身に直接かつ現実に損害が発生した場合のみ、1年間の利用料金を限度とし損害賠償責任を負います。（利用規約26条） |
| 37 | 解約時のデータポータビリティ | | 解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること | ○ | サービス解約後にデータ削除操作を実施します。 |
| 38 | 預託データの整合性検証作業 | | データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること | × | 対応していません。 |
| 39 | 入力データ形式の制限機能 | | 入力データ形式の制限機能の有無 | ○ | 入力データ、取込データに対し、データ形式の制限があります。 |
| **セキュリティ** | | | | | |
| 40 | 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<br>（ISMS、プライバシーマーク等）が取得されていること | ○ | プライバシーマーク取得済<br>ISO27001及びISO27017取得済 |
| 41 | アプリケーションに関する第三者評価 | | 第三者によるウェブアプリケーション脆弱性評価実施 | ○ | 第三者企業の脆弱性診断を行っています。 |
| 42 | 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 | ○ | 国内のクラウドサービスにて適切に管理されています。 |

| No. | 種別 | サービスレベル項目例 | 規程内容 | 対応/可否 | 内容 |
|---|---|---|---|---|---|
| 43 | 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 | ○ | 通信はSSL/TLSにて暗号化しています。 |
| 44 | 会計監査報告書における情報セキュリティ関連事項の確認 | | 会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨「最新のSAS70Type2監査報告書」「最新の18号監査報告書」 | × | 対応していません。 |
| 45 | マルチテナント下でのセキュリティ対策 | | 異なる利用企業間の情報隔離、障害等の影響の局所化 | ○ | テナント間は論理的に分離されております。 |
| 46 | 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利用者組織にて規定しているアクセス制限と同様な制約が実現できていること | ○ | アクセス権は限定された担当者ごとにアクセス範囲が決められています。 |
| 47 | セキュリティインシデント発生時のトレーサビリティ | | IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか | ○ | 当社が管理するシステムログ等は原則提供しません。<br>サービス内で取得できる操作ログは無期限で保存され、ログには操作日時、利用者ID、端末名が含まれます。 |
| 48 | セキュリティインシデント発生時の通知内容 | | 情報セキュリティインシデント発生時の、責任体制及び手順 | ○ | インシデント発生時はHPに以下を掲載します。<br>なお、復旧見込時間が5時間以上の場合、5時間毎に進捗を報告いたします。<br>・インシデント概要<br>・復旧見込時間<br>・復旧完了をHPにて再度報告する旨 |
| 49 | ウイルススキャン | | ウイルススキャンの頻度 | × | WAFは導入していますが、ウイルススキャンは行っていません。 |
| 50 | 二次記憶媒体の安全性対策 | | バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること | ○ | 当社では二次記憶媒体の使用を禁止しています。 |
| 51 | データの外部保存方針 | | データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか | ○ | データの保存地（日本）の各種法制度下におけるデータ取扱い及び利用に関する制約条件を把握しております。 |
| 52 | 情報取り扱い環境 | | セキュリティに配慮した開発環境が確保されていること | ○ | 事務所内は建物や部屋にセキュリティ区画を設定し、入退室管理および監視を行っています。 |
| 53 | 外部委託におけるセキュリティ事項 | | 外部組織がかかわる業務プロセスから、情報資産に対するリスクを識別し、適切な対策を実施すること | ○ | 外部委託先に対して評価を定期的に行い、開発データは適切に保護されています。 |
| 54 | 開発ソースコード管理 | | 開発プログラムはセキュリティに配慮していること | ○ | プログラムソースコードは社内コーディング規約により適切に管理されています。 |

この資料に関するお問い合わせ：infosec@kendweb.net