本書の第三者への開示はご遠慮願います

第10版 (回答日：2024年4月1日)

ChoiceRESERVE クラウドサービスレベルのチェックリスト

本資料は、経済産業省「クラウドサービスのチェックリスト」に基づき、クラウド型予約管理システム「ChoiceRESERVE」のセキュリティレベルについてまとめたものです。

尚、項目は経済産業省「クラウドサービスのチェックリスト」に加え弊社独自の項目を追加(*)しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）	備考
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）	時間帯	24時間365日	計画停止、緊急停止を除く
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）	有無	有	定期的な停止はありません。緊急時を除く計画的なメンテナンス等によるサービス停止が発生する場合は事前(2週間前を目安)に管理画面のお知らせ欄に掲載もしくはご契約者様に対しメールで通知を行います。
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）	有無	有	1ヶ月前までに管理画面のお知らせ欄に掲載もしくはご契約者様に対しメールで通知を行います。但し、サービス利用規約内の関連事項に抵触する場合はその限りではありません。
4		突然のサービス提供停止に対する対処	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	有無	無	ご契約者様自身で予約情報、会員情報を事前にダウンロードして保管頂く事は可能です。
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）	稼働率（%）	非公開	公開しておりません。尚、過去1年で長時間利用不可となる障害等は発生しておりません。
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	有無	有	バックアップデータを日次の周期で保存しています。
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	有無	有	ご契約者様自身で予約情報、会員情報を事前にダウンロードして頂く事は可能です。
8		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	有無（フ ァ イ ル形式）	有 (CSV形式)	ご契約者様自身で予約情報、会員情報を事前にダウンロードして頂く想定となります。
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	有無	有	不定期ではありますが3ヶ月を目安に機能追加をしています。
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）	時間	無	公開しておりません。
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	時間	無	公開しておりません。
12		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	回	非公開	件数の公開はしておりません。尚、障害等のお知らせは製品サイトの稼働状況ページで随時確認頂けます。
13		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	有	サービスの死活、プロセス、サーバーリソースを常時監視しています。5分毎。
14		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	有	製品サイトの稼働状況ページに状況を随時掲載します。
15		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	非公開	規定はありません。
16		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）	5分	
17		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	随時	時間間隔の規定はありませんが、製品サイトの稼働状況ページに状況を随時掲載します。
18		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	有	ご契約者様自身で管理画面の操作ログの取得が可能です。(オプションのお申込みが必要です)
19		バックアップのリストア訓練 *	バックアップのリストア訓練を実施	有無	有	
20	性能	応答時間	処理の応答時間	時間（秒）	非公開	
21		遅延	処理の応答時間の遅延継続時間	時間（分）	非公開	
22		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	非公開	
23	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	有無	有	任意のメニュー、時間帯で予約を受け付ける事が可能です。詳細は製品サイトの機能一覧ページを参照ください。
24		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）	有無	有	会員連携機能、API、Salesforceへのデータ連携機能等のご利用が可能です。その他詳細は製品サイトの機能一覧ページを参照ください。
25		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）	非公開	規定はありませんが、秒間おおよそ3以上のアクセスがあった場合に一時停止の画面が表示される場合がございます。
26		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	処理能力	規定はありません	
27	システム構成	ネットワーク・サーバー構成 *	ネットワーク・サーバー構成	有無	無	ネットワーク・サーバー構成の公開はしておりません。
28		システム構成 *	OS/開発言語等の情報	有無	有	Linux / PHP /MySQL を利用しています。バージョン等は非公開となります。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）	備考
サポート						
29	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	24時間365日	詳細は製品サイトのサポートに関するページを参照ください。 https://yoyaku-package.com/support/professional.php
30		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	24時間365日	詳細は製品サイトのサポートに関するページを参照ください。 https://yoyaku-package.com/support/professional.php
データ管理						
31	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	有 / 日次でサービス環境とは別の領域にバックアップをしています。また、復旧の訓練も実施しています。	但し、お客様のご要望による復元・バックアップデータの提供サービスはございません。
32		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点	時間	24時間以内	但し、契約においてデータの保証はしておりません。
33		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	日	31日	
34		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	有	ご契約終了後、データの削除を行います。
35		バックアップ世代数	保証する世代数	世代数	31	但し、お客様のご要望による任意の世代による復元・バックアップデータの提供サービスはございません。 また、契約上でのデータの保証はしておりません。
36		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	有無	有	個人情報を扱うページはhttps(TLSv1.2)による通信の暗号化をしています。また、データベースに保存される全てのデータは透過的暗号化がされています。
37		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	有無／内容	無	但し、ご契約ごとにデータベースは分離されています。
38		データ漏洩・破壊時の補償／保険	データ漏洩・破壊時の補償／保険の有無	有無	有	詳細はサービス利用規約を参照ください。
39		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、外部への漏洩の懸念のない状態が構築できていること	有無／内容	有 / ご契約終了後、直ちにデータの削除を行います。	データが必要な場合、契約終了前にご契約者様自身で予約情報、会員情報をダウンロードして頂く事が可能です。
40		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	有無	有	会員登録や予約登録等の操作が行われると契約者様にご利用頂く管理画面に登録されたメールアドレスにそれらの情報を自動送信する事ができ、登録データとの整合性確認が可能です。
41		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	有無	有	入力項目に合った入力制限を実装しています。
セキュリティ						
42	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	有	ISMS(ISO27001) / ISMSクラウドセキュリティ(ISO27017)
43		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	有	定期的(年1回)に脆弱性検査(webアプリケーション、プラットフォーム)をしています
44		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	有	操作者の限定、接続元の制限をしています
45		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	有	個人情報を扱うページはhttps(TLSv1.2)通信による暗号化をしています
46		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」	有無	無	
47		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	有無	有	ご契約ごとにデータベースを分離しています
48		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	有無／設定状況	有	操作者の限定、接続元の制限をしています
49		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	設定状況	ログより検索が可能です。但し、提供は原則しておりません。	
50		ウィルススキャン	ウィルススキャンの頻度	頻度	リアルタイム及び日次でのスキャン	セキュリティソフトを導入し最新の状態を維持しています。
51		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	有無	ー	二次記録媒体の使用はしておりません
52		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、国内にサーバ装置が設置され、国内法令のみが適用されているか	把握状況	把握しています	

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）	備考
53		適切なセキュリティパッチの適用 *	ミドルウェア等の脆弱性に対するパッチを迅速に適用しているか	有無	有	最新のパッチ情報を自動取得し必要に応じ適宜適用しています
54		セキュアコーディング *	セキュリティを考慮したプログラミングをしているか	有無	有	別紙「ウェブアプリケーションのセキュリティ実装チェックリスト」を参照ください。
55		セキュリティに関する機能 *	セキュリティに関する機能はあるか	有無	有	製品サイトのセキュリティに関する機能一覧を参照ください。 https://yoyaku-package.com/function/security/
データセンター *						
56	全般	事業者	Amazon Web Services(AWS) を利用しています。			
57		設置場所	国内にあるデータセンターを利用しています。住所等の詳細は非開示です。			
58		準拠法、司法管轄	日本			
59		取得認証/取得認定	ISO27001 / ISO27017 / ISO27018 / PCI DSS レベル 1 / その他詳細は https://aws.amazon.com/jp/compliance/programs/ を参照ください。			
60		AWS導入事例	国内の利用事例は https://aws.amazon.com/jp/solutions/case-studies-jp/ を参照ください。			
61		AWS SLA	https://aws.amazon.com/jp/legal/service-level-agreements/			
62	運用全般	安全対策基準	財団法人金融情報システムセンター FISC安全対策基準に準拠して運用をしています。			
63	ファシリティ	建物(環境)	各種災害、障害が発生しやすい地域を避けているか	はい/いいえ	はい	自然災害や火災など、環境上の脅威の可能性に対して事前の対策を講じ立地の選択をしています。
64		建物(周囲)	立地環境の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講じているか	はい/いいえ	はい	フェンス、壁、セキュリティスタッフ、監視カメラ、侵入検知システム等を用いた厳重な管理を行っています。
65		建物(構造)	耐震建築物か	はい/いいえ	はい	環境的なリスクに対する物理的な保護を備えています。
66		建物(構造)	耐火建築物か	はい/いいえ	はい	はい。また、自動火災検知および消火装置があり常時監視をしています。
67		建物(内装等)	不燃材料および防炎性能を有するものを使用しているか	はい/いいえ	はい	はい。また、第三者によるFISC安全対策基準の準拠が確認されています。
68		コンピュータ室・データ保管室 (構造・内装等)	漏水防止対策を講じているか	はい/いいえ	はい	はい。また、漏水検知デバイスにより自動ポンプを作動させて漏水を除去します。また、それらの常時監視をしています。
69		コンピュータ室・データ保管室(設備)	自動火災報知設備の設置	はい/いいえ	はい	自動火災検知および消火装置があり常時監視をしています。
70		コンピュータ室・データ保管室(設備)	出入口には出入管理設備、防犯設備を設置しているか	はい/いいえ	はい	立ち入りを許可された者に渡されたバッジにより多要素認証が実行され、事前に承認されたエリアへのアクセスのみ可能となっています。
71		電源設備	電源は複数回線で引き込んでいるか	はい/いいえ	はい	電気系統は完全な冗長設計になっています。
72		電源設備	防災、防犯設備用の予備電源を設置しているか	はい/いいえ	はい	はい。また、停電の際は無停電電源装置から特定の機能に電力が供給され、発電機から施設全体に非常用電力が供給されます。
73		空調設備	空調設備は安定的に空気調和できる措置を講じているか	はい/いいえ	はい	冗長性を持つよう設計された冷却暖房換気空調設備により管理され常時監視をしています。
74		監視制御設備	監視制御設備を設置しているか	はい/いいえ	はい	設備は 24 時間 365 日の監視を実施しています。
75	入退管理	有人監視	有人による監視はされているか	はい/いいえ	はい	入り口ゲートには警備員を配置し、監視カメラで警備員と訪問者を監視する監督者も配置されています。
76		認証	厳密な認証がされているか	はい/いいえ	はい	多要素認証が実行され、事前に承認されたエリアへのアクセスが制限されます。
77		継続的監視	継続的な監視はされているか	はい/いいえ	はい	ビデオ監視、侵入検出、およびアクセスログ監視システムを使用して継続的に監視されています。
77	点検	機器の点検	機器の保守点検は定期的にされているか	はい/いいえ	はい	マシン、ネットワーク、およびバックアップ装置に対する診断を日常的に実施しています。
78	破棄	メディアの破棄	不要になったメディアは復元できない状態で破棄しているか	はい/いいえ	はい	米国国立標準技術研究所 (NIST) が提示する手順(NIST 800-88)に則り処理を行います。

※その他、awsに関する情報は下記を参照ください。

ファシリティ関する情報： https://aws.amazon.com/jp/compliance/data-center/data-centers/

FISC安全対策基準に対する情報： https://aws.amazon.com/jp/compliance/fisc/