

【経済産業省】クラウドサービスレベルのチェックリスト版\_MSSV3クラウド機能

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	サービス停止時間	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日サービスを提供しています。ただし、年数回の頻度で平日夜間2時間程度メンテナンスのため、停止します。
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）	○	ホームページとMSSV3クラウド機能のお知らせ機能にて告知
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）	○	サービス利用約款に記載しています。
					サービス終了3ヶ月以上前までに通知致します。
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	○	お客様データ保護は常実施していますが、突然のサービス停止時には可能な範囲でシステムの復旧に努めます。 お客様データについては、お客様の責任でバックアップいただけるようお願いしています。
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）		公開していません。 2025年1月稼働率実績99.95%
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		無停止のディザスタリカバリには対応していません。
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。MSSV3ソフト版が同等の機能を有します。
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		単線結線図、保護協調図はDXF形式もしくはPDF、レポート機能はCSV出力が可能です。エクスポートデータはMSSV3クラウド機能専用のファイル形式となります。
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	○	製品のアップデートは年数回の頻度で実施しています。	
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）		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		RTO 最大1週間
		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	○	RPO 1日
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		過去1年間に発生した回数は0（ゼロ）件です。
13		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		システム監視基準には対応していません。
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）	○	サービス停止を伴う障害発生時は、弊社担当者が通知を受け、対応を行います。お客様へはホームページを通じて周知いたします。
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		規程はありませんが、できるだけ早く通知します。
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	○	常時監視しています。
17		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	○	サービス停止を伴う場合、弊社Webページとお知らせで通知します。

# 【経済産業省】クラウドサービスレベルのチェックリスト版\_MSSV3クラウド機能

No.	種別	サービスレベル項目例	規程内容	対応/可否	内容
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）	○	日時、操作種類、ユーザー名、会社名のお客様のご利用状況は提供可能です。
19	性能	応答時間	処理の応答時間		公開しておりません。
20		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。
21		バッチ処理時間	バッチ処理（一括処理）の応答時間		バッチ処理はありません。
22	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		カスタマイズには対応していません。
23		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）	○	外部サービスからをご利用頂けるAPIを用意しておりません。
24		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	○	同時接続利用者数の制限はございません。
25		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	○	利用可能なストレージ容量には上限がございません。将来は上限を設ける見込みです。
サポート					
26	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	○	お問い合わせフォーム・お電話にて24時間365日受付が可能です。
27	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	○	サポート受付は24時間365日、サポートWEBフォームもしくはお電話で受付いたします。
					通常のサポート業務の対応時間は、平日8：30～17：30（祝日、年末年始等弊社休日は除く）
					内容を確認のうえ2営業日以内にご返答いたします。
データ管理					
28	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、国内の同一リージョンの離れたデータセンターに日次でバックアップをしています。
29	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取り、データを保証する時	○	RPO 1日
30	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	○	3日分
31	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	○	利用するデータはお客様の責任で解約前にダウンロードいただき、解約後は即時削除いたします。当社では論理データ削除操作を実施します。物理的削除証明には対応していません。
32	バックアップ世代数		保証する世代数	○	データバックアップの保障はしていません。データはお客様責任でダウンロードしバックアップいただきます。ただし、当社ではシステム運用に必要な措置として、毎日3日分、DBの自動バックアップしています。
33	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	○	インターネット接続はSSL/TLS1.2以上により暗号化されています。
34	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	○	個別キー管理が行われています。

# 【経済産業省】クラウドサービスレベルのチェックリスト版\_MSSV3クラウド機能

No.	種別	サービスレベル項目例	規程内容	対応/可否	内容
35		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		損害賠償保険には加入していません。お客様データ管理はお客様の責任でお願いしています。
36		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	○	利用するデータはお客様の責任で解約前にダウンロードいただき、解約後は即時削除いたします。当社では論理データ削除操作を実施します。物理的削除証明には対応していません。
37		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	○	データはお客様の責任でデータ内容の確認をいただきます。
38		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	○	MSSV3クラウド機能が提供する入力形式の制限機能がございます。
セキュリティ					
39		公的認証取得の要件	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、国内の同一リージョンの離れたデータセンターに日次でバックアップを取得
40		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		第三者による脆弱性検査の実施を検討しております。
41		情報取扱い環境	データをバックアップした媒体を保管する期限	○	バックアップデータは3日間保安されます。
42		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により暗号化しています
43		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。
44		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	○	お客様ごとの個別管理キーにより、契約スペースごとに完全に分離されたデータ領域で運用しております。
45		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。
					弊社内アクセスは物理的アクセスを含めて記録され監査されています。
46		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	○	一定の期間ごとにログを取得し、記録を確認することが可能ですが、お客様は直接アクセスできません。
47		ウイルススキャン	ウイルススキャンの頻度	○	常時ウィルスチェックを行っております。

# 【経済産業省】クラウドサービスレベルのチェックリスト版\_MSSV3クラウド機能

No.	種別	サービスレベル項目例	規程内容	対応/可否	内容
48		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	○	二次記憶媒体を使用せず、データセンター間でバックアップを取っています。
49		データの外部保存方針	データ保存時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	○	【個人情報保護法】 【サイバーセキュリティに関する法律】把握しています。
その他					
50		サービス規約の有無	サービス規約が定義されているか。	○	利用規約を参照ください。
51		データの所在地	サーバー、データは日本国内にあるか	○	AWSの東京リージョンを利用しています。
52		データの再委託	各顧客データ・顧客が入力したデータ取扱いの第三者委託はあるか。	○	有り。利用規約に記載しております。
53		脆弱性対策	サーバーの脆弱性対策を遅滞なくかつ定期的に実施しているか	○	システムへの影響度を確認した後に対策を適宜実施しています。
54		情報漏洩に関しての対策、対応	人的、システムの対応はどのようなものを行っているか。対応状況は。	○	社内規定に基づく教育を実施しております
55		内部不正についての対策	従業員が利用者のデータへ不必要に、許可なくアクセスすることへの抑止力はあるか。	○	特定のアカウントでのみデータにアクセスできるよう、制限を施しています。このアカウントはデータ管理に携わる一部の社員にのみ発行されます。サーバーにてアクセスログを取得していることを周知しており、抑止力としております。
56		内部事故についての対策	データの持ち出し・紛失への対策はあるか。	○	社内規定に基づく監査を定期的の実施しております。
57		パスワードについての対策	簡単なパスワードを不許可とする仕組みがあるか	○	パスワードの強度は大文字小文字記号を含めた8文字以上となります。
58		ログイン認証についての対策	多要素認証など、パスワード以外に本人確認する手段があるか	○	ログイン時にSMSもしくはメールに通知された確認コードの入力を要求できます。
59		アカウントロック	一定回数ログインに失敗した場合に、アカウントのロックアウトが可能か。		現在はアカウントロックに対応しておりません。
60		アクセス制限	利用環境において、第三者がアクセス出来ない仕組みがあるか。（IPアドレス制限、デバイス制限等）	○	IPアドレス制限が可能です。（申し込みが必要となります）
61		アクセス権限管理	一般ユーザーのアクセス権限は管理者からのみ権限付与などの制御が可能か。	○	設定が可能です。（申し込みが必要となります）
62		管理者権限管	管理者毎のアクセス権限を設定する機能があるか。	○	設定が可能です。（申し込みが必要となります）
63		法的要求事項	OTEXが遵守する法令、国が定める指針及びその他の規範を遵守しているか。（「規範一覧表」シート参照）		社内規定に基づいた遵守確認を実施しています。