CLOUD-SERVICEレベルのチェックリスト

第1.5版　2018年 3月 1日

対象サービスは　CLOUD-SLIMS、CLOUD-LMS、CLOUD-SPENCER、CLOUD-ASSORT、CLOUD-ASPITS、CLOUD-BIZBO、CLOUD-FLabor です。
項目は「クラウドサービスレベルのチェックリスト」（経済産業省）に準拠しています。

株式会社セイノー情報サービス

No.	種別	サービスレベル項目	規定内容	測定単位	回答
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日としています。 （計画停止/定期保守を除く）
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 計画停止を行う場合は、7日前を目安にWebページまたは電子メールで通知します。脆弱性対策等、緊急を要する停止については７日以内の通知になる場合があります。 定期保守に関しては、毎回の通知は行いません。
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 Webページまたは電子メールで通知します。 通知時期は定めていません。
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（サービス提供会社が倒産等した場合にもサービスを継続できるようにする措置）	有無	無 預託等の措置は行っていません。
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）	稼働率（%）	稼働率99.9%以上を目標と定義しています。
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 遠隔地にバックアップ用データを保管しています。 遠隔地の代替機の有無は選択できます。
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	無 システムが利用できない場合の代替手段は準備していません。 機器は冗長化しており、正常な機器への切替により、早期に復旧させて、システムが利用できるようにする構成としています。
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）	無 システムが利用できない場合の代替措置を未提供のため、定義していません。
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 アプリケーションのアップグレードは個別に協議の上対応します。 パッチ適用については、JPCERT、IPA等からの脆弱性情報を確認し、影響を受ける可能性のあるパッチのみ適用します。 お客様に影響がある場合は、事前に通知を行います。
10	信頼性	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	目標復旧時間　60分以内
11		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	復旧までに長時間（1日以上）要した障害は発生していません。
12		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 ハードウェア、ネットワーク、リソース(CPU、メモリ、DISK)、パフォーマンスの監視を常時行っています。
13		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 通知方法は、指定された連絡先に電子メールまたは電話となります。
14		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	60分以内の通知を目標とします。 営業時間外は、翌営業時間になる場合があります。
15		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）	10分以内の間隔で監視をしています。
16		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	定期報告は行っていません。
17		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 ログの取得は行っていますが、ログ提供は行っていません。
18	性能	応答時間	処理の応答時間	時間（秒）	データセンタ内の平均応答時間の目標値は3秒以内です。 大量データを扱う機能については、個別に協議させていただきます。
19		遅延	処理の応答時間の遅延継続時間	時間（分）	データセンタ内の平均応答時間が3秒以上となる遅延の継続時間は、30分以内が目標値です。 大量データを扱う機能については、個別に協議させていただきます。
20		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	バッチ処理時間は、データ量により変化します。
21	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 個別に協議の上、カスタマイズを行います。

CLOUD-SERVICEレベルのチェックリスト

第1.5版　2018年 3月 1日

対象サービスは　CLOUD-SLIMS、CLOUD-LMS、CLOUD-SPENCER、CLOUD-ASSORT、CLOUD-ASPITS、CLOUD-BIZBO、CLOUD-FLabor です。
項目は「クラウドサービスレベルのチェックリスト」（経済産業省）に準拠しています。

株式会社セイノー情報サービス

No.	種別	サービスレベル項目	規定内容	測定単位	回答
22		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 EDI、API　による連携ができます。
23		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）	有 お客様毎に必要に応じて設定します。
24		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	上限は設定していません。 お客様毎に必要に応じて設定します。
サポート					
25	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	電話または電子メールにて、24時間365日、受付を行います。 平日9:00-17:00以外の弊社営業時間外は、障害内容に応じて、翌営業時間での対応となる場合があります。
26		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	電話または電子メールにて、24時間365日、受付を行います。 平日9:00-17:00以外の弊社営業時間外は、翌営業時間での対応となります。
データ管理					
27	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 日次でバックアップを取得しています。 バックアップデータは、本番用サーバが設置してあるデータセンターと異なるデータセンターに保管しています。 バックアップデータへのアクセス権はシステム管理者のみに制限しています。
28		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	夜間に日次バックアップを取得しています。 バックアップ時点までの復旧となります。
29		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	日次バックアップは　次の日次バックアップを取得するまで保管されます。
30		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 サービス解約後、一定期間経過後に消去します。
31		バックアップ世代数	保証する世代数	世代数	1世代
32		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 https(TLS)による暗号化を行っています。 データベースの暗号化は行っていません。
33		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	有無	有 補償は利用規約に定める範囲となります。
34		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	有無／内容	有 サービス解約後、一定期間経過後に消去します。 提供サービスのダウンロード機能により、お客様のデータを保管していただけます。ダウンロードできないデータについては、個別に協議の上対応します。
35		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 （預託はサービス提供会社が倒産等した場合にもサービスを継続できるようにする措置）	有無	無 データの預託は行っていません。
36		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 想定外のデータ入力を検出し、不正なデータをデータベースに格納しないようにしています。
セキュリティ					
37	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認証取得 プライバシーマーク取得
38		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 ネットワークとサーバのセキュリティ診断を年1回、第三者機関により受けており、問題無いことを確認しています。 アプリケーションレベルのセキュリティ診断は受けていません。
39		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 物理的な入退室管理および、運用者の制限を行っています。
40		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 https(TLS)による暗号化を行っています。
41		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

CLOUD-SERVICEレベルのチェックリスト

第1.5版　2018年 3月 1日

対象サービスは　CLOUD-SLIMS、CLOUD-LMS、CLOUD-SPENCER、CLOUD-ASSORT、CLOUD-ASPITS、CLOUD-BIZBO、CLOUD-FLabor です。
項目は「クラウドサービスレベルのチェックリスト」（経済産業省）に準拠しています。

株式会社セイノー情報サービス

No.	種別	サービスレベル項目	規定内容	測定単位	回答
42		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 OS、データベース、アプリケーションの各レベルで、要件に合わせて、データを分離する構成にしています。
43		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	有無／設定状況	有 制限しています。 部門管理者の許可無く、データにアクセスすることはできません。
44		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	個人単位でIDを付与しており、ログに記録されています。 NTPによりサーバの時刻合わせを行っており、ログには正確な時刻が記録されています。 主要なログの保存期間は以下となります。 ・ファイアウォールログ　1年間 ・Webアクセスログ　2ヶ月間 ・アプリケーションログ　1ヶ月間 原則、ログの提供は行っていません。
45		ウイルススキャン	ウイルススキャンの頻度	頻度	ウイルススキャンはリアルタイムで行っています。 ウイルス感染リスクの低いOSに対しては除外しています。
46		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	有無	有 バックアップデータは、DISK装置に保管しており、テープ等の取り外し可能な媒体は利用していません。 DISKの廃棄時は、データを完全に抹消しています。
47		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	把握状況	把握しています。 データの保存地は日本国内です。