フォームズ株式会社（2021年01月時点）

クラウドサービスレベルのチェックリスト（経産省 2010年8月発行「クラウドサービスレベルのチェックリスト」より）

No.	種別	サービスレベル項目	サービスレベル内容	回答の単位	備考	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	計画停止時間は提供者が個々に設定	24時間365日です。（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	有無		【有】５営業日前にメール／ホームページで通知
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	有無		【有】6ヶ月前にメール／ホームページで通知
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	サービス提供企業が倒産等した場合にもサービスを継続できるように、プログラムを第三者に預託していることが望ましい	【無】データがダウンロードできる機能を提供します。
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	稼働率（%）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討 ※「計画サービス時間」は、サービス提供時間と計画停止時間の両方を含む	99.9%以上
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	データセンタ構成、復旧までのプロセス／時間、費用負担についても明示されていることが望ましい また、適用する業務の重要性に応じた「ディザスタリカバリ」のレベルにより設定内容は変わる	【有】１日以内に復旧を行います。
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】バックアップデータよりシステムを再現できるようにしております。
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）	データ保護の観点からは、クラウド・コンピューティング・サービス提供者だけでなく利用者側でもバックアップを実施しておくことが望ましい。また、システムの信頼性、サービス継続性の観点からは、サービス提供者は十分に対策を行っていると考えられるが、トラブル時に備えて、預託データのダウンロード	【有】CSVファイルのダウンロードが可能です。
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	頻度、事前通知方法、履歴管理／公開、利用者の負担についても明示されていることが望ましい	【有】バージョンアップやセキュリティパッチの適用は随時行っています。
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	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	当サービスの独自アプリケーションに起因する障害：２時間以内 当社が契約するインフラサービス（AWS等）に起
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	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	当サービスの独自アプリケーションに起因する障害：２時間以内 当社が契約するインフラサービス（AWS等）に起
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	回	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	１時間以上の影響した障害：２回
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	詳細な監視項目は提供者が個々に設定	【有】システム監視
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	初期対応後の経過報告の方法・タイミングについても明示されていることが望ましい	【有】原則メールで連絡します。
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	営業時間内／外で異なる設定を行う場合がある	２時間以内
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）	営業時間内／外で異なる設定を行う場合がある	１０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	報告内容／タイミング／方法は提供者が個々に設定	ホームページ上で公開
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	提供内容／方法は提供者が個々に設定	【有】アクセスログ、操作ログ ただし、ログデータの提出には合理的な理由が必要です。

クラウドサービスレベルのチェックリスト（経産省 2010年8月発行「クラウドサービスレベルのチェックリスト」より）

No.	種別	サービスレベル項目	サービスレベル内容	回答の単位	備考	回答
19	性能	応答時間	処理の応答時間	時間（秒）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	1秒以内
20		遅延	処理の応答時間の遅延継続時間	時間（分）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	1分以内
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	該当なし

クラウドサービスレベルのチェックリスト（経産省 2010年8月発行「クラウドサービスレベルのチェックリスト」より）

No.	種別	サービスレベル項目	サービスレベル内容	回答の単位	備考	回答
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	有無		【有】管理画面より変更可能
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）	有無	APIがインターネットの標準技術で構成され、仕様が公開されており、APIの利用期限や将来の変更可能性が明記されていることが望ましい	【無】
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	有無 （制約条件）	同時接続の条件（保証型かベストエフォート（最善努力）型か）、最大接続時の性能について明示されていることが望ましい	【有】（目安）10秒間で200人
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	処理能力		該当なし
サポート						
26	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	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる	メール　24時間365日 電話　営業時間内
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	時間帯	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる	メール　24時間365日 電話　営業時間内
データ管理						
28	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	保証要件を設定している場合は、具体的に明示。バックアップ内容は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる また、クラウド・コンピューティング・サービスベンダの[illegible]ばデータ継続が出来ない	【有】週次でフルバックアップ（2021年1月時点）
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とり、データを保証する時点	時間	データ破損、システム障害時において、どの時点のデータを最低限保証すべきか示すこと	１日前
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間	時間	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討する 証跡として残すべきだと思われるものとしては、アクセスログ等のセキュリティに関係するログ情報が挙げられる。法定のものとしては、帳票関係が挙げら	１か月から６か月
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	有無	解約時には、CSVなどの一般的なフォーマットでデータ出力ができることが望ましい	【有】データの削除は任意のタイミングで行える。また、契約解除後365日未使用の場合、削除される。
32		バックアップ世代数	保証する世代数	世代数	ロールバックを必要と迫られた際にどの時点のバックアップデータまで遡ることが可能であるかを明確にしておくことが望ましい	３世代（ただし、当サービスの利用者の要望によるロールバックは行わない）
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	有無	個人情報や、業務において重要かつ暗号化せねば信頼性に欠けるデータを対象とする	【有】個人情報やパスワードの一部のデータのみ。
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	有無／内容	マルチテナントストレージの場合のキー管理の方法について、全顧客がひとつのキーを使うのか/顧客別にひとつのキーが割り当てられるのか/顧客別に複数のキーを使えるのか明確にしておくことが望ま	【無】
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	有無	個人情報を扱う場合には、クラウド・コンピューティング・サービス提供者との間で個人情報取り扱いに関して合意を形成して契約事項の中で責任の割り当てを行っておくべきであるが、万が一の個人情報漏えいに備える意味でサービス提供者における損害賠償保険加入の有無を確認しておくことが	【有】情報漏えい賠償責任保険に加入しています。
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	有無／内容	外部への漏えいをいかに防ぐ仕組みが出来ているか	【有】データは任意のタイミングでダウンロードできます。 データ削除証明書の発行も可能です。

クラウドサービスレベルのチェックリスト（経産省 2010年8月発行「クラウドサービスレベルのチェックリスト」より）

No.	種別	サービスレベル項目	サービスレベル内容	回答の単位	備考	回答
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	有無	入力データ、算出データ等がハードウェア/プラットフォーム/アプリケーションの問題や不正な操作により改ざんされていないこと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	【無】
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	有無	金額、住所、電話番号等の文字種、データ形式が制限されるフォームにおいて、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する仕組みを提供していること	【有】
セキュリティ						
39	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	ITサービスマネジメントのベストプラクティスであるITILやJIS Q20000、JISQ27001:2006をベースとした情報セキュリティ監査の実施等の取得状況も確認すること（望ましい）	【有】プライバシーマーク取得
40		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	セキュリティ監査、システム監査、ペネトレーションテスト等ネットワークからの攻撃に対する検証試験、ハードウェア/プラットフォーム/ウェブアプリケーションの脆弱性検査、データベースセキュリティ監査などを想定	【無】 第３者機関による、定期的な脆弱性診断は行っていない。 ただし、第３者機関の自動ツールによるアプリケーションの脆弱性検査は、新機能追加のたびに行っている。
41		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】当社の情報管理マニュアルで規定している。
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	有無	※SSL暗号化に関する基準値の記載があったが、2018年時点の基準に合わせて記載されていた内容を削除した。	【有】マイクロソフト社のサポート基準に従う。
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」	有無		【無】
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	有無		【有】アプリケーションレベルによるデータ分割
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	有無／設定状況	利用者組織にて規定しているアクセス制限と同等な制約が実現できるかどうかを確認すること。クラウド・コンピューティング・サービスにおけるハードウェア/プラットフォーム/アプリケーションで用意されているロール（管理者、一般ユーザ等の役割を意味する）に制約がある場合には、ユーザを既存のロールの範囲でグルーピングする等の工夫により対応できるかどうかを確認する。クラウド・コンピューティング・サービスではマルチテナントを採用しているた	【有】データにアクセスできる者の認証を行っている。
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	設定状況		個別のIDで管理されている。
47		ウイルススキャン	ウイルススキャンの頻度	頻度		月次
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	有無		【有】２次記憶媒体は原則使用しない規定を設けている
49		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	把握状況		当社の情報管理マニュアルで規定している。