クラウドサービスレベルのチェックリスト

改訂日：２０１７年８月２２日（火）

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ウィ・キャンの回答
アプリケーション運用							
1	利用性	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／定期保守を除く）	計画停止時間は提供者が個々に設定	システム停止時間は、以下の通りです。 日曜日～金曜日：０４：００～０４：３０ 土曜日　　：０２：００～０６：００
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	30日前にメール／ホームページで通知		有: 実施７日前までに、弊社から書面で通知させて頂きます。 SymphonyAtwo利用契約書の第５条に記載させて頂いています。
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	15ヶ月前にメール／ホームページで通知		有： SymphonyAtwo利用契約書に、利用終了日を明記致します。 利用終了日の６ヶ月前に、弊社からメールにて通知させて頂きます。
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	第三者へのプログラムの預託を実施	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	有： SymphonyAtwoのプログラムは、財団法人ソフトウェア情報センターに著作権登録しています。 不測の事態に陥ったときに、ユーザ様の使用継続がより実現しやすくなる「ソフトウェア・エスクロウ」制度があります。
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（%）	99.9%以上（基幹業務） 99%以上（基幹業務以外）	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。	2014年1月1日(水)～2014年12月31日(水)の稼働率は、 99.898%でした。 2015年1月1日(木)～2015年12月31日(木)の稼働率は、 99.917%でした。 2016年4月1日(金)～2017年3月31日(金)の稼働率は、 99.734%でした。
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	遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システム切替時間は半日～1日	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： 障害発生時は、弊社の「SymphonyAtwo障害発生時対応マニアル」に則り、障害対策本部を立ち上げ、迅速に対応致します。
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	バックアップデータの取得が可能なホームページを用意		有： 障害発生時の復旧方式として、サーバ機の二重化を行っています。切替作業を行い、迅速に業務再開が行える構成を取っています。 復旧時間は、基本的に最大３０分です。
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）	CSVあるいはExcelファイル	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が可能かどうかを確認することが望ましい	有： ＣＳＶ又はＰＤＦにて出力が可能です。
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	年2回の定期バージョンアップを実施	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： 日々04:00～04:30にジョブメンテナンスを実施し、実施した内容は『メンテ情報』に記載しています。
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	1時間以内（基幹業務） 12時間以内（上記以外）	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	業務時間内：システム障害：３０分以内 バグ改修　：２４時間以内 業務時間外：システム障害：３時間以内 バグ改修　：翌業務開始時刻から２４時間以内
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	3時間後 3日後	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	業務時間内：システム障害：３０分以内 バグ改修　：２４時間以内 業務時間外：システム障害：３時間以内 バグ改修　：翌業務開始時刻から２４時間以内

クラウドサービスレベルのチェックリスト

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ウィ・キャンの回答
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	1回以内（基幹業務） 3回以内（上記以外）	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	2014年1月1日(水)～2017年03月31日(金)の障害発生件数（＝対応に長時間（1日以上）要したSymphonyAtwoの障害）は、『０』件です。
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	ハードウェア／ネットワーク／パフォーマンス監視	詳細な監視項目は提供者が個々に設定	有： 弊社にて、月～金（祝日除く）の１０：００、１１：００、１６：００にサーバの負荷状態の監視を行い、弊社内全スタッフに報告メールを発信しています。
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	指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知	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： ①株式会社ビットアイル様のデータセンター、 「SymphonyAtwoセンター」にサーバを設置しています。 ②富士通様（富士通サポートデスク様）とハード保守契約をして、リモート通報サービスを受けています。 万が一、機器に障害が発生した場合、富士通様のハード保守センターに自動通報（メール発信）されます。 障害内容の把握／交換部品の手配／保守員の手配を一貫して請け負って頂いています。 ③上記通知は、弊社システム責任者にも届きます。 弊社システム責任者が状況掌握の上、ユーザ様への影響の度合い等を判断の上、必要に応じてユーザ様へメール及びＦＡＸにて通知を致します。
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	15分以内（基幹業務） 2時間以内（上記以外）	営業時間内／外で異なる設定を行う場合がある	障害発生から１５分以内（弊社の営業時間外は３時間以内）に、ユーザ様へ通知を致します。
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	時間（分）	1分以内（基幹業務） 15分（上記以外）	営業時間内／外で異なる設定を行う場合がある	時間を設定していません。
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	月に一度ホームページ上で公開	報告内容／タイミング／方法は提供者が個々に設定	定期的なサービス提供状況報告は行っていません。重大な障害発生の際などに、ユーザ様へメール又は文書で報告を行っています。
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）	時間	セキュリティ（不正アクセス）ログ／バックアップ取得結果ログを利用者の要望に応じて提供	提供内容／方法は提供者が個々に設定	システムへのアクセスログ（＝ジョブ起動履歴）、操作ログ（予約カルテ登録・変更履歴）は、ユーザ様環境にてリアルタイムに確認して頂けます。
19	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3秒以内	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	登録：１秒以内 検索：１秒以内 集計：３０秒以内
20		遅延	処理の応答時間の遅延継続時間	時間（分）	データセンタ内の応答時間が3秒以上となる遅延の継続時間が1時間以内	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	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します。
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）	4時間以下	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	SymphonyAtwoはリアルタイム処理のみです。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	有無	利用画面上の項目配置変更や新規項目の追加が設定画面より可能		有： 画面上の一部項目において、ユーザ様の設定で名称や配置の変更が可能です。 機能開発を伴うカスタマイズの際には、「機能情報確定書」を取り交わし、仕様等の条件を認識統一しています。
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（プログラム機能を外部から利用するための手続き）を公開	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	有： 現状外部システムとしてコンビニ決済、カード決済が対応しています。外部のシステム会社にご了解を頂ければ、その他も対応致します。また標準機能にて、各種集計・財務諸表のＣＳＶ出力機能を備えています。
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）	50ユーザ（保証型）	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： ご契約頂いたライセンス数の同時接続を保証致します。
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	1TB40,000ページビュー		ディスク容量の上限／ページビューの上限はありません。

クラウドサービスレベルのチェックリスト

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ウィ・キャンの回答
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	24時間365日（電話）	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	①サーバ保守、及びSymphonyAtwoセンターのシステムソフトウェア保守は、２４時間、３６５日の監視及びトラブル対応を行います。 ②SymphonyAtwoソフトウェアの保守、及び運用・問合せサポートの窓口は、弊社「お客様デスク」となります。 営業時間（電話受付）は以下の通りです。 平日：０９：３０～１８：３０ 土曜：０９：３０～１５：３０ 但し、１２：００～１３：００及び休日（日曜日・祝日） ・年末年始を除きます。 メール・ＦＡＸ・SymphonyAtwoお問合せシステムは、２４時間、３６５日受付しています。 ③システム停止など重大な障害発生時は、必要に応じ、上記時間帯以外でも電話問合せ対応を行います。
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	時間帯	営業時間内（電話） （年末年始・土日・祝祭日を除く） 24時間365日（メール）	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	①SymphonyAtwoソフトウェアの保守、及び運用・問合せサポートの窓口は、弊社「お客様デスク」となります。 営業時間（電話受付）は以下の通りです。 平日：０９：３０～１８：３０ 土曜：０９：３０～１５：３０ 但し、１２：００～１３：００及び休日（日曜日・祝日） ・年末年始を除きます。 ②メール・ＦＡＸ・SymphonyAtwoお問合せシステムは、２４時間、３６５日受付しています。
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	有（日次で、作業前後の差分のみバックアップし、週次でフルバックアップを取る。遠隔地のデータセンタにテープ形式保管。 アクセス権はシステム管理者のみに制限。復旧／利用者への公開の方法は別途規定）	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・サービスベンダの民事再生、破産等によりサービス継続が出来ない場合についても明示されていることが望ましい	有： ①１週間に一度データベース全体のバックアップを取得して日々は差分データのみバックアップしています。 ②顧客データ／法人データ／代理店データ／施設仕入先データにつきましては、別々のデータベースに毎日バックアップしています。誤って、顧客データを大量に消去してしまった際などに対応します。 ③バックアップデータは、別のハードディスク（SymphonyAtwoセンター内）に保管しています。 ④バックアップデータへのアクセスは、弊社システム責任者のみに限定しています。
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とり、データを保証する時点	時間	前日朝6時まで、ただし、災害発生時は1週間前まで	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	当日の午前02:00までのデータを保証致します。
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	時間	5年以上 （証跡として残すべきもの、法定のもの） 3ヶ月以上（その他）	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、帳票関係が挙げられる	①データベース全体のバックアップ保存期間は１週間です。 ②顧客データ／法人データ／代理店データ／施設仕入先データにつきましては、週１回のデータベース全体のバックアップデータ更新時に併せて更新されます。 保存期間は１日間～最大１週間です。
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	サービス解約後1ヶ月以内にデータおよび保管媒体を破棄	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： SymphonyAtwo利用契約書第１４条（データの引渡し）に沿い、解約成立後から１ヶ月経過後データを消去します。 論理的なデータ消去のみのため、保管媒体の破棄は行いません。 利用者に所有権のあるデータ（利用期間中）は、 SymphonyAtwo利用契約書第１３条（データ保管期間）に沿い、データ保管／消去を実施致します。
32		バックアップ世代数	保証する世代数	世代数	3世代	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	全体のバックアップ世代数は１世代です。 顧客データ、法人データ、代理店データ、施設仕入先データのバックアップ世代数は７世代です。

クラウドサービスレベルのチェックリスト

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ウィ・キャンの回答
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	有	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： SSL3.0～TLS1.2にてデータを暗号化しています。 （保存データの暗号化は採用していません。）
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	有 複数のキーを使用することで、不正アクセス等の影響範囲を限定する	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しい	有： 本件、万全に対策を取らせて頂いています。 対策の具体性については、データベースの内部構成に関わる事である為、原則、非公開とさせて頂いています。何卒ご了承下さい。
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	有	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望ましい	無： 損害賠償保険には加入していません。
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	有 返却する場合は、テープ媒体にデータを保管し、提供する消去する場合は、証明書を送付する （第三者機関発行の証明書が望ましい）	外部への漏えいをいかに防ぐ仕組みが出来ているか	有： SymphonyAtwo利用契約書第１４条（データの引渡し）に沿い、解約成立後から１ヶ月経過後データを消去します。 SymphonyAtwo利用契約書第１０条（秘密保持義務）に沿い、データは第三者に開示・漏洩しないものとします。
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	有	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	有： データ登録各画面には、データ修正者／日時が自動で記録されます。 システムへのログイン、各ジョブ画面起動・終了履歴（作業者・日時）を閲覧できるので、正規にログインした担当者が操作したかどうかの検証を行うことが出来ます。
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	有無	有	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： 想定外のデータ入力をした場合、データ格納をしない様制限を掛けています。 想定外のデータ入力時、メッセージを表示します。
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	ISMS認証取得 プライバシーマーク取得	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JISQ20000、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が望ましい	有： ＩＳＯ２７００１認証を取得しています。
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	有 （サービス提供前に、セキュリティホールの有無等について第三者機関（又は内部機関）により検査を受け、また、検査が定期的かつ適切に行われていることを年１回、外部機関により評価を受ける。また、速やかに指摘事項に対して対策を講じる。）	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： アプリケーションに関する第三者評価は受けていません。 ウィ・キャンではＩＳＯ２７００１認証を取得し、年１回、認証機関からの監査を受け、問題なく更新出来ています。
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 （運用者が限定されていること）		有： 弊社内にて、運用者を限定しています。 指紋認証システムによる個人認証・ログイン制限を行っています。
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	有無	3DES/RSA/SHA-1	SSLの場合は、SSL3.0/TLS1.0（暗号強度128ビット）以上に限定	有： TLS1.2にてデータを暗号化しています。
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」	有無	有		無： SAS70Type2監査、18号監査を取得していません。 ウィ・キャンではＩＳＯ２７００１認証を取得し、年１回、認証機関からの監査を受け、問題なく更新出来ています。

クラウドサービスレベルのチェックリスト

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ウィ・キャンの回答
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	データ認証のアクセスコントロールについて明記		有： ログイン方式を、指紋認証システムのみとしています。不正アクセスを万全に防止致します。

クラウドサービスレベルのチェックリスト

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ウィ・キャンの回答
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	有 （利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る）	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め、他の顧客と一つのデータベースを共有する場合があることに配慮すること	有： 弊社内にてユーザ様環境にログイン出来る担当者を限定しています。またユーザ様のデータを操作する場合、操作前に「データ修正承諾書」を取り交わしさせて頂いています。 またユーザ様にて弊社担当者がログインした履歴をシステム上で閲覧する事が出来ます。 担当者名の特定については、弊社へ調査依頼頂ければ情報を開示致します。
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	設定状況	権限に沿ったID管理が行われていること（1人1ID発行）		指紋認証を採用しています。 指紋認証によって個人を特定し、ログが記録されます。 ユーザ様にてログを確認出来ます。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	週次		ノートンアンチウイルスソフトとＥＳＥＴを適用して、毎日定義ファイルの更新と毎日ウイルススキャンを実施しています。
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	・権限者のみアクセス可 ・廃棄時には、データを完全に抹消する ・暗号化、認証機能を用いる ・遠地へ運ぶ際は、施錠されたトランクで運ぶこと	有： 権限者のみアクセス可能です。 データ抽出も権限者のみ可能です。	有： ①バックアップデータは、別のハードディスク（SymphonyAtwoセンター内）に保管しています。 ②バックアップデータへのアクセスは、弊社システム責任者のみに限定しています。
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いるか	把握状況	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		データ保存地（＝SymphonyAtwoセンター所在地）は、東京都品川区です。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ます。