Styleflow クラウドサービスレベルのチェックリスト

※「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。　　第 2 版：2021 年 4 月 15 日

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	Styeflow 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	24 時間 365 日（定期保守を除く） ※定期保守 毎月 1 回 3 週目の木曜日　4 時間　20:00-24:00
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 30 日前に Styleflow ログインページのメンテナンス情報と Styleflow サポートサイトで通知させていただきます。
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 サービス終了日より 3 ヶ月以上前に弊社が提供する手段で通知いたします。この 3 ヶ月間の中でやむを得ない事情がある場合は短縮することもございます。
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	無 預託等の措置は行っておりません。
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（%）	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。	対外的に保障している数値はございませんが、 実績値としましては下記の通りです。 2020 年度：　稼働率　99.99　%（2020 年 3 月現在） 2019 年度：　稼働率　100　% ※ただし、稼働率は計画停止を除いた数値となります。
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	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 Styleflow を構成する各サーバ群は、Microsoft Azure の東日本リージョンにおいて管理・運用しています。 Microsoft Azure の東日本リージョンのデータセンタ障害対策に準じます。 ・Web サーバ　・アプリケーションサーバ ・データベースサーバ

© Copyright 2021, TDC SOFT Inc. All rights reserved.

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 システムの申請データを取得可能なクライアントツールや 画面上からデータを一括取得する Excel エクスポート機能、 ワークフロー設定取得機能を準備しております。
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)	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 下記のデータ形式で提供可能となっております。 ・申請データ　CSV 形式、Excel 形式 ・各種マスタ、フォーム　CSV 形式、Excel 形式 ・ワークフロー　テキスト（Json）形式
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 年 4 回（4 月、7 月、10 月、1 月）のバージョンアップを 実施しています。 ※管理者がサービス内でバージョンアップ情報を 確認できます。 ※利用者に影響を与えかねない重大な脆弱性が確認された 場合は、早急に回避策の適用あるいはソフトウェアの アップデートを実施します。
10	信 頼 性	平均復旧時間 (RTO)	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	サービスをリリースしてから現在まで障害でサービスが 止まっていないため、平均復旧時間は定められません。 目標復旧時間は、1 日以内を目標としており、 迅速な障害復旧対応を実施する体制となっております。 ※Microsoft Azure 上のハードウェア故障が発生した 場合は 1 時間未満で自動復旧することを想定しています。
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	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	実績値としましては下記の通りです。 2020 年度：　重大障害発生数　0 回/年 2019 年度：　重大障害発生数　0 回/年
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	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 下記を監視しており、必要に応じて対策を行っております。 ・Web サイト動作の死活監視 ・仮想マシンのリソースの状況（メモリ、ディスク）

© Copyright 2021, TDC SOFT Inc. All rights reserved.

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	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 弊社は下記事象が生じた場合、事前又は緊急の場合は事後に通知いたします。 ・システムの保守点検等の作業を定期的に 又は緊急に行う場合 ・システムに故障等が生じた場合 ・停電、火災、地震、労働争議その他不可抗力により サービスの提供が困難な場合 ・その他、システムの運用上又は技術上の相当な理由が ある場合
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	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	時間は定めておりませんが、障害が発生した場合は迅速に復旧対応を行います。 ※営業時間外は翌営業時間となることがございます。
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）	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	約 5 分間隔で監視しております。
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	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	障害発生時の臨時メンテナンスに関しましては、 ログインページのメンテナンス情報とStyleflow サポートサイトに記載いたします。
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）	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	有 ・操作ログ（日時、ログレベル(INFO,ERROR など)、ユーザ ID、IP アドレス、ユーザエージェント(ブラウザや OS の情報など)、ステータス(200,400 などの HTTP ステータスコード)、メッセージ(画面名や操作内容など)) ・システムログ 通信ログやファイアウォールログの取得を取得しております。 「操作ログ」は管理者画面から参照・出力可能です。システムログについてはシステム運用のために使用するため、原則提示することは出来ません。
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 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	明確に時間を定めておりませんが、平均 3 秒程度を 目標としております。

© Copyright 2021, TDC SOFT Inc. All rights reserved.

							通信環境やデータ量によるところもございますが、 Styleflow はパブリッククラウド型のサービスとなるため、 ご利用ユーザ数に応じて適時・適切に増設しております。
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	明確に時間を定めておりませんが、 迅速に対応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）	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	処理時間はデータ量に応じて変化するため、 時間を明記することはできません。

© Copyright 2021, TDC SOFT Inc. All rights reserved.

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	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 マスタやワークフロー、フォームなどの設定項目は、自由に追加・変更・削除等が設定画面より行えます。
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	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 一部情報へのアクセス手段として API を備えています。 API の仕様は利用者からの要求に応じて開示しています。 また、マスタや申請データに関しましては標準機能にて Excel 出力、Microsoft Azure・Gsuite から社員・組織情報の連携、Slack・Chatwork へ通知の連携ができます。
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）	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	制限無（ベストエフォート（最善努力型））
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	1TB 40,000 ページビュー		1 ドメイン（契約）に対してディスク容量は 10GB となります。 ※ストレージ追加プランにて 1 ドメイン（契約）月額 ￥1,000／10GB のストレージ上限の追加を行えます。 1 ドメイン当たりの最大ストレージ容量は 200GB です。（標準 10GB+追加 190GB）
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	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	問合せサポート時間は弊社営業日の 9:30～12:00、13:00～17:00 とします。
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	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	問合せサポート時間は弊社営業日の 9:30～12:00、13:00～17:00 とします。 ※問合せの考え方 システムに対する一般的な問合せに関しましては、ライセンス料に含まれております。固有の設定に関する問合わせにつきましては別途保守契約が必要となります。全ての問い合せは実施責任者 1 名のみが行う必要があります。受付より 3 営業日以内に回答、進捗をご報告します。ただし、最終回答を得るまでに時間を要するもの又は回答し得ないものがあります。

© Copyright 2021, TDC SOFT Inc. All rights reserved.

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、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及びサービス内容／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 バックアップは下記方法にて実施しております。 ・アプリケーションサーバのデータを日次バックアップしています。 ・バックアップデータは、Microsoft Azure ストレージアカウント内の「ローカル冗長ストレージ(*)」に作成しており、30 日間保管します。 ・データベースサーバのデータは Azure Database for MySQL のサービスにてバックアップが行われており、完全バックアップは毎週、差分バックアップは 1 日に 2 回、トランザクション ログ バックアップは 5 分ごとに行われます。これらのバックアップは 30 日間保管します。 ※同じ拠点内の 3 つのストレージノードに、トランザクションを同時に複製することにより、ストレージアカウントのすべてのデータの耐久性を確保
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	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	週次で完全バックアップ、1 日に 2 回差分バックアップ、5 分ごとにトランザクション ログ バックアップを行っており、バックアップ時点まで復旧が可能となっております。
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	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	利用者のデータに関しては 30 日間保管します。 システムのログファイルについては最低 1 年間保管しています。
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	サービス解約後 1 ヶ月以内にデータ及び保管媒体を破棄	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 サービス解約後、弊社の定める時期に廃棄するものとします。

© Copyright 2021, TDC SOFT Inc. All rights reserved.

31		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	30 世代 ※30 日前までの任意のタイミングのバックアップデータとなります。
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	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 データベースは透過的暗号化による暗号化を行っています。
33		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	無 データはテナント（ドメイン）ごとに論理的に分割されています。データにアクセスするための認証情報（ユーザ ID、パスワード）はテナントごとに分かれています。
34		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	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。
35		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）	外部への漏洩をいかに防ぐ仕組みが出来ているか	有 サービス解約後、弊社の定める時期に消去いたします。 ダウンロード機能により、事前にお客様自身でデータを保管していただけます。
36		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	無 データの預託は行っておりません。
37		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 データを入力する場合、入力チェックを行います。 想定外のデータ入力時、エラーメッセージを表示し、登録されません。

© Copyright 2021, TDC SOFT Inc. All rights reserved.

セキュリティ							
38	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 JIS Q200000 等の取得状況も確認することが望ましい	有 弊社は、下記を取得しています。 JIS Q 9001:2015(ISO 9001:2015) 登録番号 JUSE-RA-232 JIS Q 27001:2014(ISO/IEC 27001:2013) 登録番号 JUSE-IR-064 プライバシーマーク使用許諾事業者 登録番号 11820076
39		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により評価を受け、また、年 1 回、外部機関によりサービスの脆弱性に関する評価を受け、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	有 毎年、第三者機関により Web アプリケーション診断を受けており、問題がないことを確認しております。
40		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 弊社内で運用者を限定しています。
41		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 による暗号化を行っております。 定期的に脆弱な暗号化強度を使用していないか確認しております。
42		システム監査への資料提供	システム監査時に、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

© Copyright 2021, TDC SOFT Inc. All rights reserved.

43		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 ユーザ ID、ドメイン ID、パスワードの組み合わせでアカウント情報を管理しており、ドメインごと、ユーザごと、権限ごとにアクセス制御を行うことで制限しております。 また、必要に応じてテナント（ドメイン）毎に IP アドレス制限を付けることもできます。
44		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 権限グループの機能により、柔軟なアクセス制限の制約を実現することができます。 またマスタ管理者、一般ユーザ等のロールを分け、両者がアクセス可能な機能を制限しております。
45		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否か	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）		・監査ログ 弊社内の権限が付与されているユーザのみ管理を行えます。また、重要な操作やリスクのあるサインインに関しましてはログを保存しており、7 日間保管しております。 ・アプリケーションログ 基本的に 1 人 1ID 発行できる仕組みとなっており、ID を基にログ検索を行えます。 また、ログの保管期間は 1 年となっております。
46		ウイルススキャン	ウイルススキャンの頻度	頻度	週次		現状ウイルススキャンは実施しておりませんが、他の対策を複数行っております。 システムの脆弱性を無くすための対策として、ソースコードの第三者によるチェックやライブラリ、ファイル変更の監視を行っております。

© Copyright 2021, TDC SOFT Inc. All rights reserved.

47		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 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	・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 データはクラウド上にのみ保管しており、物理サーバへのアクセスに関しては Microsoft Azure に準じます。

© Copyright 2021, TDC SOFT Inc. All rights reserved.