BtoBプラットフォーム サービスレベルチェックシート

最終更新日：2020年9月24日

No.	種別	サービスレベル項目例	規定内容	実施内容
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）	24時間365日 計画メンテナンスを、月に1回、午前2時～4時に実施しております。
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は実施していますか。（事前通知のタイミング／方法もご記入願います）	有り 6ヶ月前にサイト上にて告知しております。
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を実施していますか。（事前通知のタイミング／方法もご記入願います）	有り 原則3ヶ月以上前にサイト上にて告知を行います。
4		突然のサービス提供停止に対する対処	突然サービスを停止するようなことになった際に、プログラムの預託等の措置はありますか。	無し プログラムの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）が十分保証されていますか。	サービスレベル目標として月間稼働率を「99.99%以上」と定めておりますが、実績値については公開しておりません。
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	有り 同一敷地内でサーバを二重化し、更に遠隔地にてデータバックアップを保管しております。大規模災害が発生した場合にはオフサイトにてバックアップの復元を行い、サービスを継続いたします。
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はありますか。	有り 障害対策サーバに切り替えを行い、サービスを継続いたします。
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	-
9		アップグレード方針	バージョンアップ／ 変更管理／ パッチ管理の方針について、頻度や事前通知方法	有り お客様に影響のある改変においては、影響度を考慮し、原則1ヶ月以上前にサイト上にて告知を行います。 バージョンアップおよび変更管理については、ISMSに準拠し、適切に運用を行っております。 セキュリティパッチに関しては、サービスへの影響を確認の上、月次で適用しております。
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）	平均復旧時間は公開しておりません。
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	目標復旧時間は公開しておりません。
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	復旧までに1日以上要した障害は発生しておりません。
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）に基づく監視項目を設定していますか。（ハードウェア/ネットワーク/パフォーマンス監視）	有り ハードウェア、ネットワーク機器の各種リソース（CPU、メモリなど）や、サイトのパフォーマンス、アプリケーションのエラーなど、常時監視を行っております。
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）	有り サイト上での通知および、障害時連絡先としてご登録いただいている宛先へメールで通知しております。
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	障害検知から１時間以内を目標に通知いたします。
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	1分間隔にて監視しております。
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	平常時においては、稼働状況の報告は行っておりません。障害発生時においては、30分毎にサービス稼働状況をサイト上で通知いたします。
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）	ログイン履歴については、管理者権限をお持ちのお客様にてサイト上より確認が可能となっております。（ログイン日時、IPアドレス、デバイス、ログイン成功・失敗）※プラットフォームIDをご利用の場合のみ また、弊社にてアクセスログ、操作ログなど各種ログを取得しておりますが、社外秘のため原則としてお客様への提供は行っておりません。
19	性能	応答時間	処理の応答時間	目標応答時間を3秒以内で設定しております。 ただし、データ量や検索条件等により目標時間を超過する場合がございます。
20		遅延	処理の応答時間の遅延継続時間	遅延継続時間の設定はしておりませんが、アクセスログからWebサイトの応答時間を収集し、遅延の監視や定期的な分析を行っております。
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	バッチによって大きく異なるため応答時間の閾値設定はしておりませんが、ログからバッチ処理の完了時間を収集し、遅延の監視や定期的な分析を行っております。
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	無し カスタマイズは原則行っておりませんが、ご要望の内容は、貴重なご意見として今後のバージョンアップの参考とさせていただきます。
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）	有り 多くのシステムとの連携実績がございます。 また、WebAPIを公開しておりますので、詳しくはホームページをご参照下さい。
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	制限なし
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	上限なし
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	・カスタマーセンター（電話） 平日 9：00～18：00 ・お問合せフォーム 24時間365日
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	・カスタマーセンター（電話） 平日 9：00～18：00 ・お問合せフォーム 24時間365日

BtoBプラットフォーム サービスレベルチェックシート

最終更新日：2020年9月24日

No.	種別	サービスレベル項目例	規定内容	実施内容
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	有り 日次にて差分バックアップを取得、月次にてフルバックアップをテープ形式で取得し、国内の遠隔地にて6か月間保管しております。 またバックアップデータへのアクセス権限は、一部のサーバ管理者のみとなっております。
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	RPOは公開しておりません。
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	6ヶ月間
31		データ消去の要件	サービス解約後の、データ消去、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	無し お客様の取引データについては、ご利用終了後においても取引先側に残す必要がございますので、サービス解約後においてもデータの消去は行っておりません。
32		バックアップ世代数	保証する世代数	7世代
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、暗号化要件はありますか。	有り データ全体を暗号化し保護しております。
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	無し 機密性を考慮したシステム設計により他社とのデータは論理的に分離しております。
35		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	無し 補償は原則行っておりません。
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、外部への漏洩の懸念のない状態が構築できていますか。	無し お客様の取引データについては、ご利用終了後においても取引先側に残す必要がございますので、サービス解約後においてもデータの消去は行っておりません。但し、アカウント情報については解約後速やかに論理削除を行っております。
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ますか。	有り 不正データを監視し、検知された場合には警告メールを送る仕組みを構築しております。
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	有り データ入力項目については、入力フォーマットのチェックや、サニタイジング処理を行っております。
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）を取得されていますか。	有り ISMS認証 ASP・SaaSの安全・信頼性に係る情報開示認定
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ますか。	有り 第三者機関による脆弱性診断を定期的に実施しております。
41		情報取扱い環境	運用者が限定されている等、提供者側でのデータ取扱環境が適切に確保されていますか。	有り 情報セキュリティ管理責任者が承認した社員のみに、データ取扱環境への接続を許可し、必要最小限の権限を付与しております。
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	有り 全画面HTTPS化し、常時SSLにて暗号化しております。暗号化強度については、電子政府推奨暗号リストに記載された暗号方式にて暗号化しております。 また、TLS1.2未満は無効としております。
43		システム監査への資料提供	システム監査時に以下の資料を提供可能ですか。 「SAS70認定」「18号監査報告書」	無し 内部統制保証報告書（SOCレポート）は作成しておりません。
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を実施していますか。	有り 機密性を考慮したシステム設計により他社とのデータは論理的に分離しております。
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おり、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ますか。	有り 弊社内においては、情報セキュリティ管理責任者が承認した社員のみ、お客様のデータへアクセス可能となっており、アクセスログ等の証跡を取得しております。
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ますか。	1人1IDを発効しており、アクセスログや操作ログなど、IDが分かる形式で各種ログを取得しております。
47		ウィルススキャン	ウィルススキャンの頻度	リアルタイム リアルタイムスキャンおよび日次でのパターンファイル更新、週次でのフルスキャンを行っております。
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おり、廃棄の際にはデータの完全な抹消を実施し、また検証していますか。 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ますか。	有り バックアップメディアは暗号化しており、機器の廃棄についてはISMS等に準拠して安全に廃棄しております。 また、外部メディアの使用についてはシステムで制限しております。
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ますか。	データ保存地は日本国内となります。