gusuku.io セキュリティチェックシート

2020年4月13日版

本資料は、「クラウドサービスレベルのチェックリスト」（経済産業省）に基づき、アールスリーインスティテュートの提供するgusukuのセキュリティについてまとめたものです。
独自のチェックリストへの回答をご希望の場合は、別途有料オプションを提供しております。詳細は butler@gusuku.io までお問い合わせください。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）
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	計画停止を除く、24時間365日です
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（事前通知のタイミング／方法の記述を含む）	有無	【有】実施5営業日前までにメールにてにて通知します
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	【有】終了1ヶ月前までにメールおよび公式サイトにて通知します
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	【無】現時点ではありませんが、 gusuku Deploit バックアップオプションにてバックアップされたデータは、ダウンロード可能となるよう対応を検討しています
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（%）	年間99.9%以上の実績です。ただし、本サービスの稼働率は cybozu.com の稼働率に依存します。こちらをご確認ください https://www.cybozu.com/jp/service/slo/availability.html
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】過去35日間のバックアップを行っています。災害発生時の復旧時間は1日以内です。
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】可能な限り早期復旧が可能なように、システムのおよびデータセンターの冗長化をしています。
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】現時点ではありませんが、 gusuku Deploit バックアップオプションにてバックアップされたデータは、ダウンロード可能となるよう対応を検討しています
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	【有】軽微な修正（Hotfix）は必要な時点で随時、定期的なアップデートは週1回～月1回程度の頻度でバージョンアップします。バージョンアップ後、メール/Webサイトなどで告知します
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	非公開となっております
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	年間1回以下となっております
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】サービス応答速度、ネットワーク、データベースパフォーマンスなどを常時監視しています
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】障害発生時には、メールにて顧客連絡をします
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	営業時間内には、1時間以内に顧客連絡をします。営業時間外の場合には、出来得る限り速やかに顧客連絡をします
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分間隔で監視しています
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	現時点では特にありません
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	【無】現時点では提供しておりません
18	性能	応答時間	処理の応答時間	時間（秒）	非公開となっております
19		遅延	処理の応答時間の遅延継続時間	時間（分）	非公開となっております
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）	gusuku Deploit バックアップオプションのジョブ実行時間についてはユーザー自身が画面上にて確認いただくことが可能です
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】画面上の個別カスタマイズは出来ませんが、大量データの特殊な取り扱いなどをご要望に応じてカスタマイズ可能です
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	【有】 gusuku Customine にて外部システムとの接続機能を提供しています
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）	【無】同時接続利用者数の制限はありません
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	【有】プランに応じて扱える kintoneアプリ数、バックアップオプションで利用できるディスク容量に上限が有ります（有料にて増設可能です）

No.	種別	サービスレベル項目例	規定内容	測定単位	設定(記入欄)
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	サポートサイト、メールにより24時間365日受け付けています
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	サポートサイト、メールにより24時間365日受け付けています
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】過去35日間のバックアップを行っています。災害発生時の復旧時間は1日以内です。
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	24時間以内のデータを保証しています
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	過去35日間のバックアップデータが保存されています
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	【有】フリープランがあるため、完全に全てを解約という概念は存在しませんが、お客様要望があった場合には即時対応します
31		バックアップ世代数	保証する世代数	世代数	35世代保管されています
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】データは暗号化されています。また、TLSにて全ての通信を暗号化しています
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】秘匿情報は顧客ごとに異なる暗号鍵で暗号化されます
34		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	【無】損害賠償保険には加入しておりません。有事の際には利用規約に定められた範囲で賠償する責任を負います
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	【無】基本的にすべてのデータは kintone 上にありますので、そちらを参照していただくことになります。また、現時点ではありませんが、gusuku Deploit バックアップオプションにてバックアップされたデータは、ダウンロード可能となるよう対応を検討しています
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	【無】基本的にすべてのデータは kintone 側を正として上書きされるだけになりますので、当サービスにて特別なデータ整合性検証は行っていません
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】入力項目によって長さのチェック等を行っています
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	【無】特にありません
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】実施しています
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】サーバにアクセスする事が出来るのは、システム運用担当のスタッフに限定されています。また弊社ネットワーク環境からのみアクセス可能です
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	【有】TLSにて全ての通信を暗号化しています
42		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】実施していません
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	【有】秘匿情報は顧客ごとに異なる暗号鍵で暗号化されており、各データは利用するお客様以外はアクセス出来ないよう、アクセス制限されています
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】サーバにアクセスする事が出来るのは、システム運用担当のスタッフに限定されています。また弊社ネットワーク環境からのみアクセス可能です
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、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	保管しているログから調査可能です
46		ウイルススキャン	ウイルススキャンの頻度	頻度	定期的にウィルスチェックを実行しています

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】二次記憶媒体は使用していません。異なるデータセンター間でバックアップを取っています