

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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通知します
3		計画停止予定通知の方法	サービス停止告知はメール等、見過ごされずに確実に認識される方法で行われるか。	Yes/No	【Yes】メールにて通知します
4		計画停止予定通知の通知期間より短い期間での停止の有無	記述よりも短い告知時期でサービス全面停止を伴う緊急メンテナンスはあり得るか。	Yes/No	【Yes】セキュリティ上の理由や緊急性を要する場合に、実施します
5		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
6		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	【有】
7		サービス稼働率	サービスを利用できる確率((計画サービス時間ー停止時間)÷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
8		サービス品質保証(SLA)	SLA を満たさなかった場合のペナルティ、保証などは定めがあるか。	有無	【無】SLAの定義はありません。また、gusukuサービス利用規約 第11条 免責事項を合わせてご確認ください https://www.gusuku.io/terms-of-use
9		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
10		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
11		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】
12		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
13	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
14		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	年数回となっております。 障害情報は https://support.gusuku.io/ja-JP/support/discussions/forums/36000212349 にて、過去に遡って確認する事ができます
15		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
16		提供リソースの上限	提供リソースの上限を把握し管理しているか	Yes/No	【Yes】リソース上限は常時監視しており、必要時には順次スケールアウトします
17		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、メールにてお客様に連絡をします
18		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時間以内にお客様に連絡をします。営業時間外の場合には、出来る限り速やかに連絡をします
19		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
20		障害監視(インフラ)	事業者は障害監視しているか。 実施している場合、障害監視方法(監視内容、通知基準)・インターバルが定められ運用しているか	Yes/No	【Yes】サービス提供基盤とは別のクラウド事業者より、5分間隔で監視しています
21		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	http://status.gusuku.io/ にて確認可能です
22		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	【有】gusuku Customine Job Runner のやること「ログにメッセージを出力する」を利用することで、定期実行タスク及びkintoneのWebhookから実行時ログを出力することが可能です

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
23		システムの変更管理	クラウドサービス事業者による、クラウドサービス利用者環境のメンテナンスは、作業者と承認者を分離し、承認者が承認したメンテナンス作業のみ実施されるよう管理されているか	Yes/No	【Yes】クラウドサービスのメンテナンス時は、作業内容を予め作業者が申請し、承認者からの承認を得るプロセスとなっています
24	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
25		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
26		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 Deployit バックアップのジョブ実行時間および、gusuku CustomineのJob Runner(Webhook/定期実行タスク)についてはお客様自身が画面上にて確認いただくことが可能です
27	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	【無】個別のカスタマイズを行う事は出来ません
28		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
29		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
30		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、ディスク容量に上限があります
サポート					
31	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
32		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
33		インシデント発生時の連絡体制	インシデント発生時には連絡があるか	有無	【有】個社それぞれに対しての個別連絡は実施いたしますが、可能な限り速やかにすべてのユーザーに通知します
データ管理					
34	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
35		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
36		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
37		バックアップデータの提供	バックアップデータを提供する事ができるか	Yes/No	【No】
38		バックアップの保存世代数・期間の設定	バックアップの保存世代数・期間の設定は変更できるか	Yes/No	【No】
39		バックアップの遠隔保管	バックアップは遠隔保管されているか	Yes/No	【Yes】
40		バックアップの遠隔保管先	バックアップの遠隔保管先は日本国内であるか	Yes/No	【No】保管先は日本国内及び米国内となります。ただし、日本準拠法に関するAWSカスタマーアグリーメント変更契約をしています
41		データセンターの品質	サービス基盤が稼働するデータセンターはTier4相当の品質を確保しているか	Yes/No	【Yes】
42		免責事項	クラウド事業者側の過失でサービスの停止、データの喪失や情報漏洩などが発生した場合、損害賠償、損失補填について契約で定めているか	Yes/No	【Yes】gusukuサービス利用規約の第11条 免責事項をご確認ください https://www.gusuku.io/terms-of-use
43		クラウド事業者との間の責任範囲	クラウド事業者の事故責任の範囲と補償範囲が明文化されているか	Yes/No	【Yes】クラウド事業者との間の責任範囲と補償範囲は明文化されています(AWS責任共有モデル)
44		データ関連インシデント発生状況	同一事業者にてデータ漏洩やデータ消失事案が過去3年以内にないか	有無	【無】データ漏洩、データ消失事案はありません
45		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
46		削除したデータの取り扱い	削除したデータは直ちに削除されるか	Yes/No	【No】履歴機能があるため、完全にすべて削除される事はありません

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
47		データ破棄・返却	クラウドサービスの利用契約を解除した場合、利用者の作成したデータはクラウドサービス利用企業に提供可能か	Yes/No	【No】契約を解除後のデータの提供はありません
48		データ破棄証明書	クラウドサービスの利用契約を解除し、データの削除を希望した場合、利用者の作成したデータが削除された事を示すデータ廃棄証明書は発行可能か	Yes/No	【No】契約解除後メールでご案内させていただきますが、それ以外での書面発行はありません
49		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
50		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 1.2以上にて全ての通信を暗号化しています
51		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】秘匿情報はお客様ごとに異なる暗号鍵で暗号化されます
52		情報隔離	事業者の運用において、異なる利用企業間の情報隔離、障害等の影響の局所化、他の利用者の悪意ある操作への対策は実施できているか	Yes/No	【Yes】マルチテナント環境において必要な情報隔離が実施されます。ただし障害の影響は特定の利用者に局所化されない場合もあります
53		推奨される暗号化方式を用いているか	クラウドサービス上に保管されるデータ、および通信の暗号化は総務省、経済産業省等が策定したCRYPTREC暗号リスト(※)内に記載の「電子政府推奨暗号リスト」、および「推奨候補暗号リスト」に記載のものに準拠しているか ※ https://www.cryptrec.go.jp/list.html	Yes/No	【Yes】暗号化で使用するアルゴリズムは、「電子政府における調達のために参照すべき暗号のリスト」の「電子政府推奨暗号リスト」に掲載されており、準拠しています
54		セキュリティツール利用要件	サービス関連システムには情報保護やアクセス統制のためにセキュリティツールを使用しているか	有無	【有】
55		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】損害賠償保険に加入しております。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
56		ハードウェアの管理手続(パブリッククラウドのデータ消去手続き・方法)	事業者は、ハードウェアの導入、変更、及び廃棄に関する基準および管理手続を運用しているか。またパブリッククラウドを利用しサービス提供しているSaaS事業者の場合、パブリッククラウドのデータ消去手続・方法について確認済みであるか	Yes/No	【Yes】パブリッククラウドを利用しており、データの消去手続き・方法について確認済みです
57		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
58		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おりません
59		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
60		データの入出力制御	ユーザの誤入力によるデータ漏えい、もしくはSQLインジェクション、XSS、CSRF等のWebアプリケーションの脆弱性を防止するため、システムに入出力されるデータのサニタイジング(プログラムにとって特別な意味を持つ可能性のある文字や文字列を検知して、一定の規則に従って別の表記に置き換える)が可能か	Yes/No	【Yes】システムへ入出力されるデータは脆弱性の特性をもとにサニタイジングされる仕組みを実装しています。また、年1回以上第三者のセキュリティに関する脆弱性診断を受けています
61		データの保管先	データの保管先を日本国内に限定できるか	可/不可	【不可】データセンターはAWSの日本国内および米国各地の設備を使用しています。ただし、日本準拠法に関するAWSカスタマーアグリーメント変更契約をしています
62		電子データの原本性確保	電子データの原本性確保(改竄防止・検知)の対策は実施できているか (例)時刻認証、署名(ハッシュ)、印刷データ電子化(pdf化)など	Yes/No	【No】実施されていません

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
63		kintone上のデータの取り扱い	kintone上のデータの取り扱い、「Excel/PDF出力を利用した場合」についてのデータの保管先は日本国内に限定できるか	可/不可	【不可】kintone上のデータの取り扱いにおいて、「Excel/PDF出力を利用した場合」、画面のカスタマイズから利用した場合でも、Job Runnerの場合でも、いずれも出力結果は弊社のサービス上に暗号化され保存されます。 この時、弊社サービスで使用しているデータセンターはAWSの日本国内および米国各地の設備となりますが、日本準拠法に関するAWSカスタマーアグリーメント変更契約をしています
64		削除したデータの取り扱い	削除したデータは直ちに削除されるか	可/不可	【不可】履歴機能があるため、完全にすべて削除される事はありません
65		弊社サービス上での個人情報の取り扱い	弊社が個人情報を保管する場合、当該データへのアクセス制限などのルールはあるか	Yes/No	【Yes】詳細は「gusukuのセキュリティ「kintone上のデータの取扱」についてをご確認ください」 https://support.gusuku.io/ja-JP/support/solutions/articles/36000276349
66		重要情報保存先の限定	取扱データが重要情報・最重要情報・個人情報の場合、保存先を国内拠点(バックアップや災害対策も含め)に限定可能か。また、事業者側の都合により、海外拠点に変更されることは無いか	Yes/No	【No】データセンターはAWSの日本国内および米国各地の設備を使用しています。ただし、日本準拠法に関するAWSカスタマーアグリーメント変更契約をしています
67		ストレージの運用	システム保守などの運用上の理由でストレージに利用する機器が社外に出ることはないか	Yes/No	【Yes】
68		データアクセスをするメンバの所在地	システム保守などの運用上の理由でデータアクセスをするメンバの所在地は日本国内に限定できるか	Yes/No	【Yes】
69		データ操作可能な端末へのアクセスのセキュリティ	データ操作が可能な端末へのアクセスは物理・技術セキュリティで適切に保護されているか	Yes/No	【Yes】
セキュリティ					
70	セキュリティ	公的認証取得の要件	情報処理管理に関する公的認証(ISMS)が取得されていること	有無	【有】ISO/IEC 27001:2013 (ISMS) を取得しています 登録番号 GIJP-1056-IG
71		公的認証取得の要件	情報処理管理に関する公的認証(プライバシーマーク)が取得されていること	有無	【無】取得していません
72		公的認証取得の要件	その他セキュリティに関わるマネジメントシステム認証の取得、もしくは独立した監査人による監査報告書を入手していること	有無	【無】取得・入手していません
73		電子証明書の要件	信頼できる認証局が発行する有効な証明書を利用しているか	Yes/No	【Yes】
74		セキュリティパッチ管理	事業者によるサーバー・運用管理端末へのセキュリティパッチ適用方針を定め、運用しているか	Yes/No	【Yes】各OSベンダーより一般公開されたセキュリティパッチは、即時適用しています
75		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】年に1回以上実施しています
76		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、スキャンツールなどによる脆弱性診断を定期的に行っているか	有無／実施状況	【有】年に1回以上実施しています
77		出力メッセージ管理	Webサーバーソフトのエラー表示について、攻撃者に手掛かりとなり得る不要な情報(内部挙動や製品情報等)を表示しない設定になっているか	Yes/No	【Yes】実施しており、第三者による脆弱性診断を受けています
78		不要機能の停止	Webサーバーソフトについて、不要なサービス機能の非稼働登録や削除処理を実施できているか	Yes/No	【Yes】実施しており、第三者による脆弱性診断を受けています
79		脆弱性に対する対策	新たに発見される脆弱性に迅速に対応するため、システムへの影響の有無を判断し、対応するための対策を実施しているか	Yes/No	【Yes】脆弱性対応について、主に以下の対策を実施しています。 - サービス提供に関わるソフトウェアのバージョンはすべて管理されており、脆弱性が報告されたバージョンに関しては速やかに更新が可能な体制が整備されています
80		脆弱性に対しての対応体制	新たに脆弱性が発見された場合、影響有無を速やかに判断し、クラウドサービス利用企業への通知・問い合わせ対応が可能な体制を備えているか	Yes/No	【Yes】新たに発見された脆弱性に対応するために、以下の体制を整備済みです。 - 深刻な影響範囲を持つ脆弱性が発見された場合、速やかにその影響範囲の有無や対策を告知する手順が整備されています
81		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】サーバー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

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
82		特権ユーザー管理	クラウドサービス基盤の運用保守に必要なユーザーのアカウントについて、多要素認証等を用いて厳格に管理されているか	Yes/No	【Yes】
83		リモートアクセスによる保守作業の特権ユーザID利用	リモートアクセスによる保守作業を行う場合、特権ユーザID(rootアカウント等)の利用を禁止しているか	Yes/No	【Yes】特権ユーザIDの利用は禁止されています
84		不正アクセス検知	クラウドサービス基盤に対して、方が一不正なアクセスがあった場合に即座に検知する仕組みが導入されており、且つ対応する手順の整備もされているか	Yes/No	【Yes】
85		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 1.2以上に全ての通信を暗号化しています
86		推奨回線	事業者側の回線について、信頼できる回線であるか	Yes/No	【Yes】一般のインターネット回線をTLSにて暗号化し使用します
87		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
88		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】秘匿情報はお客様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
89		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
90		リモートアクセスによる保守作業の接続先および経路の特定	リモートアクセスによる保守作業を行う場合、アクセス可能な接続先・接続経路を特定しているか。ファイアウォール等による接続先へのアクセスを限定しているか	Yes/No	【Yes】リモートアクセスによる保守作業を行う際の接続元IPを制限し、特定の接続経路のみに制限しています
91		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。また、ログの保存期間は1年です
92		ログの提供	ログの提供は可能か	Yes/No	【No】ログはユーザーには開示しません。ただし依頼を受けて弊社内で調査することは可能です
93		ログのバックアップ	ログのバックアップを取得しているか	Yes/No	【Yes】
94		アクティビティログの記録内容	ユーザのすべてのアクティビティログを記録しているか	Yes/No	【Yes】記録しているアクティビティログ:日時・接続元IP、ユーザ名(エラー時)、および操作内容
95		ログのユーザー閲覧可否	ログはユーザーがシステム上で閲覧可能であるか	Yes/No	【No】
96		アクティビティログの転送	アクティビティログなどを外部のログ管理システム(SIEMなど)に転送するための仕組みがあるか	Yes/No	【No】
97		ログの条件通知機能	ログが任意の条件に合致する場合、通知を受ける機能があるか	Yes/No	【No】
98		ログ分析や傾向の報告機能	クラウドサービス基盤に関わる利用者、システム管理者およびシステム保守者に関する操作ログの傾向を、定期的に報告することは可能か	Yes/No	【No】
99		ウイルススキャン	ウイルススキャンの頻度	頻度	定期的にウイルスチェックを実行しています
100		マルウェア対策の実施	マルウェアに起因する脆弱性に対して対応するために、クラウドサービス利用者環境にマルウェア対策ツールを導入し、マルウェア検知時にはシステムを隔離し駆除する運用となっていますか。また最新のマルウェア定義ファイルを適用して運用されているか	Yes/No	【Yes】サービス提供基盤および運用端末にマルウェア対策ソフトを導入しており、マルウェアを検知した場合に駆除します。また、最新のパターンファイルが定期的に適用されるようになっています
101		サーバー・端末管理	事業者の運用において、サーバー及び運用管理端末に許可されていないプログラム等のインストールを行わない仕組み(防止・検知機能)はあるか	Yes/No	【No】現時点ではありません。ただしサーバにアクセスする事が出来るのは、システム運用担当者に限定されています

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
102		不正な通信やソフトウェアの制御	外部からの不正侵入や情報流出に対応するために、フィルタリングソフト、ファイアウォール、IDS、IPSなどの機能による通信監視・制御がなされていますか。また不正侵入や情報流出を検知した場合に速やかにクライアントへの通知が可能か	Yes/No	【Yes】システム提供基盤上のアクティビティはすべて監視され、潜在的な脅威が検出された場合にはシステム運用担当者に通知されます。外部からの不正な侵入に対しては、ファイアウォールによる通信の監視と制御を実施しています。また、利用ユーザーに影響を及ぼすセキュリティインシデントや障害が発生した場合、または、発生の疑いがある場合には、通知を行います
103		なりすまし対策(事業者サイド)	第三者によるなりすましに関する対策は実施できているか	Yes/No	【No】現時点では提供されていません
104		ログの時刻	クラウドサービス上のシステムの時刻設定は、すべて同一になるように設定されていますか。	Yes/No	【Yes】すべてのシステムにおいて、時刻同期されています
105		アップロードされたデータへのアクセス規定	お客様がアップロードしたデータにアクセスすることはない事を利用規約等で規定しているか	Yes/No	【Yes】gusuku サービス利用規約 第10条 秘密保持 に記載の通りです https://www.gusuku.io/terms-of-use
106		お客様がアップロードしたデータに対してのアクセス可能権限の管理	お客様がアップロードしたデータにアクセス可能な権限は社内ルールに則り管理されているか	Yes/No	【Yes】
107		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
108		データセンターの入退室管理	本クラウドサービスが稼働するデータセンターは、入退室管理(施錠管理、カード貸借、入退室制限、入退室記録等)を実施しているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
109		データセンターの防災対策	本クラウドサービスが稼働するデータセンターの利用設備に対して必要な障害・防災(耐震、耐火、耐水等)対策を講じていますか。また、各設備の二重化を行っているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
110		データセンターの停電対策	本クラウドサービスが稼働するデータセンターは、外部からの給電が停止しても、1日間は代替手段(内部電源等)による自立稼働が可能であるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
111		データセンターへの情報機器の持ち込み、持ち出し制限	①本クラウドサービスが稼働するデータセンターは、記録/通信機能を持つ情報機器の持ち込み・持ち出しを禁止していますか ②サービス提供要件上、“①”の持ち込み・持ち出しを禁止していない場合、持ち込み・持ち出しの記録を行っていますか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
112		建物形態	専用区画を設けているか	Yes/No	【No】専用区画を利用してはいません。
113		耐震数値	耐震数値(震度)は十分であるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
114		耐震・免震構造	免震構造や制震構造は整備されているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
115		無停電電源	無停電電源装置(UPS)は設置されているか。設置していない場合、相当の理由があるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
116		給電ルート	別の変電所を経由した給電ルート(系統)で2ルート以上が確保されているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
117		非常用電源	非常用電源(自家発電機)は24時間以上稼働可能か	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/jp/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
118		サーバールーム内消火設備	ガス系自動消火設備はあるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
119		火災感知・報知システム	火災(煙)検知・通報システムはあるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
120		直撃雷対策	避雷針など直撃雷対策はあるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
121		誘導雷対策	誘導雷対策はあるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
122		静電気対策	静電気放電による機器・媒体破壊・データ消失・ノイズ混入対策は実施できているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
123		十分な空調設備	空調設備(床吹き上げ空調、コンピュータ専用個別空調等)および予備機等の設置はしているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
124		データセンターの入退室	データセンターの入退室記録は6か月以上保存しているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
125		データセンターの監視カメラ	監視カメラのデータは最低1週間以上保存しているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
126		データセンターの入退室装置	個人認証システムと連動した物理的入退出装置(ドア・柵等)はあるか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
127		データセンターの受付セキュリティ	受付・警備員は常駐しているか。常駐がない場合には監視カメラが設置され、物理的入退出装置が設置されているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
128		データセンターの入退室手順	重要な物理セキュリティ境界からの入退出を管理するための手順書は整備されているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
129		データセンターの機器の保護	重要な物理セキュリティ境界の出入口に破壊対策ドアを設置しているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
130		データセンターの施錠・鍵保管	サーバールーム及びラックの施錠・鍵管理を実施できているか	自由回答	弊社サービスはインフラとして Amazon Web Services(AWS)を採用しています。 https://aws.amazon.com/ip/compliance/fisc/ にありますとおり、AWSのデータセンターはFISC安全対策基準を満たしています
131		障害・災害発生時の対応マニュアル整備状況	障害、および災害において、システムの運用が何らかの要因で停止した場合、速やかな原因究明と復旧措置を可能にするために、障害、および災害発生時の対応のための対応マニュアルが整備されているか	Yes/No	【Yes】障害、および災害発生時の対応のための対応マニュアルを整備済みです
132		障害・災害発生時の記録管理	障害、および災害において、システムの運用が何らかの要因で停止した場合、速やかな原因究明と復旧措置を可能にするために、障害、および災害の原因と対応結果がわかるよう、記録を残しているか	Yes/No	【Yes】障害、および災害の原因と対応結果を記録しています

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
133		災害・障害対策の実施について	システム毎の災害・障害対策として、以下すべてを実施しているか (ア) データセンターへのシステム設置 (イ) データ記憶装置の二重化対応 (ウ) バックアップの遠隔地保管(DRサイトを構築している場合不要) (エ) 1週間以内の復旧を目安とした手順の整備	Yes/No	【Yes】以下すべての災害・障害対策を実施しています (ア) データセンターへのシステム設置 (イ) データ記憶装置の二重化対応 (ウ) バックアップの遠隔地保管 (エ) 1週間以内の復旧を目安とした手順の整備
134		再委託について	再委託は行っているか	Yes/No	【No】再委託は行っていない
その他					
135	情報開示	情報開示要求について	法律に基づいていない情報開示要求には応じない(応じない場合はYes)	Yes/No	【Yes】
136		法律に基づいた情報開示要求	いままで法律に基づいて情報開示を行ったことがあるか	Yes/No	【No】
137		法律に基づいた情報開示の場合の連絡の有無	法律に基づく情報開示の場合は、事前または事後に情報開示の詳細をユーザーに通知する	Yes/No	【Yes】
138	反社会的勢力との関係遮断	反社会的勢力との関係遮断	反社会的勢力等との関係遮断に関する事項について定めているか	Yes/No	【Yes】gusuku サービス利用規約 第15条 暴力団等反社会的勢力の排除 にて定めています https://www.gusuku.io/terms-of-use
139	利用者アカウントと統制	ユーザ単位のアカウント作成	ユーザ単位で個別にアカウント作成が可能である	Yes/No	【Yes】
140		ユーザ単位のアカウント作成が必要か	クラウドサービス利用者の管理者／運用者／ユーザに対して一意なアカウントを付与する必要があるか	Yes/No	【Yes】メールアドレスをアカウントとして設定いただくため、一意のアカウントを付与していただきます。 また、共用アカウントの作成・利用は禁止しています
141		ID/パスワードによるアクセス認証	システムを利用する際のユーザを特定する手段として、ID・パスワードによる認証が可能か	Yes/No	【Yes】すべてのユーザはクラウドサービスにアクセスする際にID/パスワードによる認証・特定がされるよう設計されています
142		特権/高権限アカウントでアクセス認証時の第三者承認機能	クラウドサービス利用者の管理者／運用者がシステム保守、運用行為を行う為に特権/高権限アカウントにてシステムにアクセスする場合、システムにアクセスするユーザと別のユーザが当該アクセスを承認することは可能か	Yes/No	【No】特権/高権限アカウントでのアクセス時に、第三者による承認を必要とする機能はありません
143		アカウントの作成・変更・削除	業務上の役割に応じて、クラウドサービス利用企業側で、自由にアカウントを発行することは可能か	Yes/No	【Yes】アカウントの追加手順は以下URLをご参照ください https://support.gusuku.io/ja-JP/support/solutions/articles/36000033673
144		アカウントの個別権限設定	各アカウントに対して、個別に権限を設定することは可能か	Yes/No	【Yes】gusuku Customine!においては オーナー/管理者/一般 の3段階の権限設定が可能です。各権限でできることについては以下URLをご参照ください https://support.gusuku.io/ja-JP/support/solutions/articles/36000034995
145		アカウントの権限レベル設定	アカウント管理を実施可能な権限を持つアカウントは、一般ユーザ権限と分かれており、別々に管理することが可能か(権限ロールが別でも可)	Yes/No	【Yes】
146		アカウントの作成・変更・削除	クラウドサービス利用者がアカウントを発行・変更・削除する際およびアカウントに対して権限を付与する際、作業者とは別の人間が確認・承認をすることは可能か	Yes/No	【No】オーナーと管理者権限をもつユーザーのみが他のユーザーを追加することが可能です。 ただし、追加時に第三者の承認を必要とする機能はありません
147		アカウント操作の履歴記録	クラウドサービス利用者がアカウントを発行・変更・削除する際およびアカウントに対して権限を付与する際の、確認・承認履歴の記録を1年以上保管することは可能か	Yes/No	【No】アカウントへの追加等変更の記録は保管されません
148		アカウント管理の監査証跡保存	アカウント管理にかかるすべての監査証跡ログが記録され、保存されているか	Yes/No	【Yes】
149		アカウント利用状況の確認機能	クラウドサービス利用者のアカウントと権限の棚卸を円滑に実施できるように、アカウントの利用状況を確認することは可能か	Yes/No	【Yes】gusuku共通管理画面にて、登録されているアカウントの一覧を閲覧いただくことは可能です。ただし、最終ログイン日時などその他の情報については閲覧できません。 また、一括出力の機能はありませんが、アカウントと権限画面についてはテキストとして表示されるため他アプリなどにコピー＆ペーストしていただくことは可能です

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
150		アカウント権限の確認機能	クラウドサービス利用者のアカウントと権限の棚卸を円滑に実施できるように、アカウントの権限を一覧で出力することは可能か	Yes/No	【Yes】gusuku共通管理画面にて、登録されているアカウントと権限の一覧を閲覧いただくことは可能です。 また、一括出力の機能はありませんが、アカウントと権限画面についてはテキストとして表示されるため他アプリなどにコピー＆ペーストしていただくことは可能です
151		初期パスワード設定の仕組み	初期パスワード設定のためのURLをメールで送付し、そのURLを用いて初期パスワードを設定する仕組みが存在するか	Yes/No	【Yes】
152		初期パスワードの強制変更	システムへの初回ログイン時、初期パスワードを強制変更させることは可能か	Yes/No	【Yes】システムへ初回ログインする際、強制的にパスワード変更を求める画面に遷移します
153		ユーザー登録に用いるドメインの制限	使用するメールアドレスのドメインを制限することが可能か	Yes/No	【No】
154		メールへのパスワード記載	パスワードが平文でメールに記載されることはない(ない場合はYes)	Yes/No	【No】パスワードリマインダーによる仮パスワードはメールにて通知されます
155		パスワード管理	パスワードは暗号化した上でシステム内に格納しているか	Yes/No	【Yes】パスワードは暗号化されています
156		アカウント管理の権限	アカウント管理はユーザーのアカウント権限で実施可能か	Yes/No	【Yes】
157		アカウントの一時停止	アカウントの一時停止(suspend)が可能か	Yes/No	【No】
158		アカウントグループの作成機能	アカウントグループの作成が可能か	Yes/No	【No】
159		アカウントに対しての権限設定	各アカウント及びアカウントグループに対し権限(閲覧権限や機能利用制限)を設定することが可能か	Yes/No	【Yes】
160		アカウントに対してのアクセス制限	各アカウント及びアカウントグループに対しアクセス元(IP、ドメイン)での制限が可能か	Yes/No	【Yes】契約組織全体に対してIPアドレス制限設定が可能です
161		ID・パスワードの運用管理(利用者サイド及び事業者サイド)	IDやパスワード(暗号鍵含む)の運用管理方法を規定し運用されているか	Yes/No	【Yes】パスワード取扱規定に則り運用されています
162		パスワードポリシー	パスワードポリシー(有効期限・強度等)の詳細設定が可能であるか	Yes/No	【No】ユーザーにて詳細設定することはできませんが、次のポリシーとなっています。 複雑性: 半角英大文字、半角英小文字、半角数字、その他、の4種の中から2種類以上の文字を使用 / メールアドレスと同じにすることはできない 文字数: 10文字以上 有効期限: 無期限
163		SSO/IDフェデレーション機能	SAML、OAuthなどのSSO、もしくはIDフェデレーション機能が存在するか	Yes/No	【Yes】OAuth認証が存在します
164	データ利用統制	OTP(ワンタイムパスワード)設定	OTP(ワンタイムパスワード)設定が可能か	Yes/No	【Yes】 多要素認証設定について: gusuku support をご覧ください
165		API呼び出し時の2FA認証機能	API呼び出しにユーザーデータが含まれる場合は、APIキーを単独で使わず、2FAによる認証が利用可能か	Yes/No	【No】
166		データの一括出力機能の有無	マニュアル処理・自動処理を問わず、データを一括して抽出する機能はない(ない場合はYes)	Yes/No	【No】例えば「CSVを出力する」などでkintoneのレコードを一括して出力することが可能です。ただし元々kintone上に該当レコードに対する閲覧権限があるか、または出力結果が保存されたkintone上のレコードに対して閲覧権限があるユーザーのみ、出力結果を閲覧可能です
167		データのユーザー間共有機能の有無	ユーザーがアップロードしたデータをユーザー間で共有する機能はない(ない場合はYes)	Yes/No	【No】組織内ではデフォルトでデータが共有されます
168		データの外部ユーザーへ公開機能の有無	ユーザーがアップロードしたデータを外部ユーザーに公開する機能はない(ない場合はYes)	Yes/No	【Yes】
169		データのパブリック公開機能の有無	ユーザーがアップロードしたデータをパブリックに公開する機能はない(ない場合はYes)	Yes/No	【Yes】
170		データ抽出・公開機能の有効化無効化設定	上記「データ利用統制」種別の機能がある場合、有効化・無効化設定が可能であるか	Yes/No	【Yes】カスタマイズのアクセス権限設定にてgusukuアカウントに対して権限設定を行うことが可能です https://support.gusuku.io/ja-JP/support/solutions/articles/36000325690

gusuku セキュリティチェックシート

2024年4月11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)を基本として、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)
171		大量データ転送の検知機能の有無	ユーザ自身が検知するための条件(閾値等)を指定し、その条件に基づいて大量のデータ転送を検知する機能が存在するか	Yes/No	【No】
172	データの所有権・返却・消去	データの所有権	クラウドサービスに保存したデータの知的財産権、所有権及び利用権は利用者に帰属するか	Yes/No	【Yes】
173		データの返却	クラウドサービス利用中や契約終了時に、クラウドに保存したデータを利用者の求めに応じて返却することは可能か	Yes/No	【No】
174		データの消去(データ)	契約終了時や障害等による機器交換時にバックアップを含むデータを、再利用不可能な形で完全に削除したことを確認する手段はあるか	Yes/No	【No】
175		データの消去(アカウント)	契約終了時はクラウドサービスの利用に関わるアカウントを、再利用不可能な形で完全に削除しているか	Yes/No	【Yes】
176	責任分界点	サービスの責任分界点	クライアントからの接続について、クラウド事業者は、責任範囲(責任分界点)を明確にし、ネットワーク機器の設定、脆弱性有無、およびリソースを管理しているか	Yes/No	【Yes】責任分界点は弊社側が提供する各サービスのエンドポイントまでとさせていただきます(御社側クライアントPC・ネットワークから、一般のインターネット回線は責任範囲に含まれません)
177	管理支援機能	ダッシュボード機能	サービスの正常性を把握出来るダッシュボード機能が存在するか	Yes/No	【Yes】 gusuku.io Status's Live status をご覧ください
178		管理者支援機能	システム管理者の作業を簡素化するための支援機能(ユーザー情報のCSV連携、アクセス権の一括変更等)が存在するか	Yes/No	【No】
179	移行支援機能	移行支援	現行サービス利用終了後に他サービスへの移行を支援するサービスはあるか	Yes/No	【No】
180	通信関連	利用している通信プロトコル	クラウドサービスを利用するための通信プロトコルとして、http,https以外に必要な通信プロトコルはあるか	自由回答	https、WebSocketが必要な通信プロトコルとなります。また制限されたネットワーク環境下では、ご利用いただくにあたって特定の接続先への通信を許可する必要があります。詳しくは以下URLをご参照ください https://support.gusuku.io/ja-JP/support/solutions/articles/36000203899
181		閉域網へのネットワーク接続対応	クラウドサービスへの接続方式として、閉域網(専用線またはVPN)での接続に対応しているか	Yes/No	【No】閉域網での接続には対応しておりません
182	開発、開発体制や統制	ソフトウェアの提供事業者の開発体制	主要業務ソフトウェアは事業者(含む系列)が開発を行っているか	Yes/No	【Yes】事業者のみによって開発しています
183		管理者認証(事業者サイド)	サーバ運用側(事業者側)の管理者権限の登録・登録削除の正式な手順は定められ運用されているか	Yes/No	【Yes】定められた手順によって運用しています
184		有償カスタマイズの可否	導入に当たりソフトの変更を伴う有償のカスタマイズ(仕様変更)が可能な事項/範囲/必要な情報/今後の保守メンテ費用の配分等が明文化されているか	Yes/No	【Yes】有償のカスタマイズは行いません
185		事業者内の組織・人事変更に応じたアクセス権限の更新	事業者内の組織変更・人事異動に応じたアクセス権限の更新手順を定め、運用されているか	Yes/No	【Yes】ISMS認証取得に伴って組織変更や人事異動に伴うアクセス権限更新時の運用はルール化されており、運用されています
186		情報セキュリティの社内研修実施	情報セキュリティについて社内の研修を実施していますか	Yes/No	【Yes】研修を定期的に行い、その内容を記録しているのに加え、改善事項等について速やかに対応しています