ジンジャーサービス　セキュリティチェックシート

セキュリティ・チェックシート

最終更新日:2024/08/08

本チェックシートの位置づけ
・本チェックシートは、jinjer株式会社が提供する jinjerサービスについて、そのセキュリティ対策を記載したものとなります。

情報セキュリティマネジメントシステムについて
・jinjer株式会社は ISO/IEC 27001:2013 に基づく認証されたISMSおよび、プライバシーマーク（Pマーク）認証を保有しています。
ISO/IEC27001:2013 登録認証番号：IS 778939
プライバシーマーク 登録番号: 10825116

セキュリティチェック項目について
・本チェックシートの項目は、経済産業省が発行した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」
(https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf) を基本としており、項目の追加・削除および一部を弊社サービスに適用した解釈を加えて作成されています。

NO	カテゴリ		確認内容	実施有無	回答内容
1	情報セキュリティのための方針群		経営陣によって承認された情報セキュリティに関する基本方針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示する。	○	経営層に承認された情報セキュリティに関する基本方針および、従業員が遵守すべき社内規程（情報セキュリティ規則等）を定めております。
2			情報セキュリティに関する基本方針を定めた文書は、定期またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューを行う。	○	情報セキュリティマネジメントシステム（以下、「ISMS」）を構築し、情報セキュリティ保全活動を効果的に推進するために、セキュリティの基本方針を定め、その通りに実施・運用し、監査および見直しを行う仕組みを確立しています。また、経営層によって承認された関連する社内規程は、ISMSにおいて、経営者によって毎年および重大な変化が発生した場合に見直してを行っております。
3			情報セキュリティ対策、設備の認可に対する手順等を明確にし、文書化する。	○	ISMSマニュアルにて、情報セキュリティ対策（日々の活動や緊急対応、役割別PDCA）を明記しております。
4			サービスの提供に際して定めた方針及び規則を、確実に遵守していることを社内で定期的に確認する。	○	社内規程に定め、年に1回の頻度で確認を実施しております。
5			サービス利用者がサービスの導入検討を行うために必要な資料を作成し、提供すること。提供資料においては、クラウドサービスSLAなどをサービス利用検討者に明示する。	○	本チェックシートにて、ジンジャーサービス利用者に対し、クラウドドサービス利用者に対し、下記、サービスレベル目標(SLO)を公開しております。 ▼サービスレベル目標(SLO) サービス稼働率99%を目標に運用しております。 ※定期メンテナンスを除きます。 システム保守による定期メンテナンス停止時間については、ジンジャー利用規約の第21条（停止、中断、廃止）を参照。 https://hcm-jinjer.com/terms/
6			サポート窓口、苦情窓口を明確にし、外部に公開する。	○	ジンジャーを快適にご利用いただけるよう、チャットサポートを提供しております。 有人によるチャットサポートは以下の営業時間となります。 平日10:00~12:00（最終受付11:45）,13:30~17:30（最終受付17:00） ※営業時間外はチャット画面からメッセージを残すことが可能となります。 翌営業日以降にメールで回答させていただきます。 チャットbotのAI社員「MIKO-SAN」によるサポートは24時間・祝休日も含めてご利用できます。 詳細は、以下のサポートポリシーにてご確認お願いします。 https://jinjer.zendesk.com/hc/ja/articles/4403081062297
7			物理的セキュリティ境界 重要な情報資産がある領域を保護するために、物理的セキュリティ境界(例えば、有人受付、カード制御による入口)を用いること。	○	重要情報がある領域について複数のデータセンタを利用したクラウドサービスを利用しております。 データセンタでは、入退室管理・エリアへのアクセス権限されており、 権限を持つ担当者のみにデータセンターへの物理的なアクセスを許可されます。 詳細の対策は以下となります。 CCTV サーバールームに物理的にアクセスできる場所は、閉回路テレビカメラ(CCTV)によって録画されています。 データセンターのエントリポイント 物理的アクセスは、建物の入り口において、サーベイランスシステム、侵入検知システム、その他の電子的システムを用いて、専門の保安要員によって厳重に管理されています。 侵入検知 データレイヤー内の場所に電子的手段による進入検出システムが設置され、セキュリティインシデントのモニタリング、検出、および適切な人員への自動的なアラート通知が行われます。
8			サーバーが設置されているデータセンターについて物理的及び環境的脅威から保護すること。	○	利用するデータセンターに関して以下の対策及び、設備仕様となっております。 立地 環境評価および地理的評価を実施します。洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所が選定されています。 電力 データセンターの電力システムは、完全に冗長化され、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源の保持 空調と温度 サーバーやその他のハードウェアの適切な運用温度を保ち、過熱を防ぎ、サーバー停止の可能性を減らすためのメカニズムを使用しています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。 火災検出と鎮火 自動火災検出システムおよび鎮火システムが設置されています。火災検出システムにおいては、ネットワーキングスペース、機械的スペース、インフラストラクチャースペース内で煙検出センサーが使用されています。また、これらのエリアは鎮火システムによっても保護されています。 漏水検出 漏水を検出するため、水があることを検出するシステムをデータセンターに備えています。水が検出された場合、それ以上の水害を防ぐために水を除去するメカニズムが備わっています。
9	運用管理	全般	サービスの提供に用いる各種アプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の運用管理の手順について文書化し、維持していくこと。	○	サービスを構成する各種アプリケーション、OS、サーバー、ネットワーク機器について、システム運用・操作手順を定め文書を作成しています。各種文書については操作方法などの変更が発生する毎に更新しております。
10			クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の変更について管理すること。またクラウドサービス利用者に影響を及ぼすものは事前に通知すること。	○	お客様影響があるものに関して以下の弊社サイトにて記載しております。 サービス運用上のお知らせ https://jinjer.zendesk.com/hc/ja/categories/360002465631 各サービスの機能アップデート https://jinjer.zendesk.com/hc/ja/categories/360002456452
11			クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	サービス構成に利用している各種アプリケーション、OS、サーバ関連の脆弱性情報について定期的に収集を行い、影響チェックを行っております。対象となった脆弱性について深刻度に合わせて適宜パッチ適応等の対応を行っております。
12			クラウドサービスの資源の利用状況について監視・調整をし、利用状況の予測に基づいて設計した容量・性能等の要求事項について文書化し、維持していくこと。	○	クラウドサービスの利用状況についてはサービスレベル目標(SLO)を定め、各種サービスレベル指標(SLI)の監視を行っております。定期的に利用状況・SLIの状態を確認・分析を行い、サーバ等の最適化(増強・増設)を実施しております。 また急激なアクセス増または月末・月初等の予めアクセス・処理増に関しては、各種サーバインスタンスの自動拡張(スケールアップ)・自動増強(スケールアウト)にて対応を行っております。
13			クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器について脆弱性診断を行うこと。また、その結果を基に対策を行うこと。	○	サービス開発・エンハンス時において、脆弱性確認を行っております。 また定期的(年一回程度の頻度)に第三者によるアプリケーションの脆弱性診断、サーバへの侵入テストを行っております。その指摘に関してはその深刻度に合わせて、即時または計画を立てて適宜対応を行っています。

14		バックアップ	サービス利用者の情報、ソフトウェア及びソフトウェアの設定について定期的にバックアップを取得し、検査すること。	○	お客様のデータデータ喪失を防ぐため複数のデータセンターに論理冗長化されたストレージで運用されます。 また、システム障害や運用ミスによるデータ異常・喪失時に備え、リストア可能なバックアップデータを保持しております。 またシステム構成はコード化して管理しており、迅速な復旧が可能です。 さらに、災害時への備えとして日本国内の別地方のデータセンターにてバックアップデータを転送・保持しております。 上記の各種バックアップに関して成功可否を監視し、失敗時のリカバリを適宜行っております。
15		サーバ監視	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の稼働監視をすること。サービスの停止を検知した場合は、利用者に対して通知すること。	○	サービス稼働状況について監視をしております。 サービスの稼働状況については、以下の弊社サービスサイトにて確認が可能となります。 ■ジンジャーサービス稼働状況 https://jinjer.zendesk.com/hc/ja/articles/900002198283 またサービス停止を含むお客様影響があるもの関して以下の弊社サイトにて記載しております。 ■サービス運用上のお知らせ https://jinjer.zendesk.com/hc/ja/categories/360002465631
16			クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の障害監視をすること。障害を検知した場合は、利用者に対して通知すること。	○	サービスを構成する各種サーバ・ネットワークの状況については監視をしております。 障害が発生した場合は、弊社のお知らせサイトの障害報告にて通知します。 ■ジンジャー障害報告 https://jinjer.zendesk.com/hc/ja/sections/360007785751 また障害の影響度により 弊社サポート担当者より貴社ご担当者様へメールにてご連絡させていただきます。
17			システムの運用担当者の作業については記録すること。	○	サービスを構成するシステム運用者の作業についてはすべて記録を残しております。操作ログは改変不可能なかたちで保管されております。 また作業を実施する際には、作業内容について責任者の事前承認を得た上で、作業者とチェック者の2名体制でその作業を実行します。
18			例外処理及びセキュリティ事象を記録した監査ログを取得すること。また該当のログのアラートについては定期確認し、改竄、許可されていないアクセスがないように保護する。	○	サービスを構成する各サーバーに対する例外及びセキュリティに関連する作業について監視サービスを利用し即時でシステム管理者、運用者にアラート通知され担当者により確認しております。 また該当ログは改変不可能なかたちで保管されております。
19		クロックの同期	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器については正確な時刻源と同期させること。	○	NTPを利用して、全てのサーバー及び、ネットワーク機器等を正確な時刻源を利用し同期処理を実施しております。
20	アクセス制御	全般	クラウド基盤システムへのアクセスについては、各個人に一意な識別子にし、セキュリティに配慮したログオン手順、認証技術によって制御すること。またアクセス制御方針について文書化すること。	○	システム運用者が利用するメンテナンス用アカウントについて、個人毎にアカウントを発行しております。 また各種サーバ類へのログインは多要素認証を利用しており、これらを含めアクセス制御に関する方針・手順を社内規程に定めております。
21			クラウド基盤システムへのアクセス権限の追加・削除・変更について手順を備えること。また特権の割り当て及び利用は制限し、管理すること。	○	システム運用者が利用するメンテナンス用アカウントの登録・変更・削除、及びアクセス権の付与に関して社内規程及び手順を定めております。 アクセス権付与時においては必要最低限とし、またその利用が不要となった時点でアクセス権の変更・削除を行っております。
22			システムの運用担当者が利用するパスワードについては管理し、また良質なパスワードにすること。	○	システム運用者が利用するアカウントのパスワードについては社内規程にて強度等のポリシーを定め運用しております。
23		利用者アクセスの管理	提供するクラウドサービスにおいてアクセス制御機能を提供すること。	○	通常のユーザID、パスワードによるログイン認証に加えて、シングルサインオンを利用した認証および、IPアドレス制限を利用可能となります。
24		ネットワークの領域分割	クラウド事業者は、各クラウド利用者に割り当てたコンピューティング資源に、他のクラウド利用者や許可されていないユーザがアクセスできないように管理し、物理的な設定や移行にかかわらず、仮想環境の分離を確実にすることが望ましい。	○	ジンジャーサービスはマルチテナント構成となっております。 各企業ごとにユニークな企業IDを発行し、論理的に分離しております。
25	利用者アクセスの管理	利用者登録	提供するクラウドサービスにおいて利用者のID登録・削除機能を提供すること。	○	ジンジャーサービスは利用ユーザの登録・削除の機能を提供しております。
26		特権管理	提供するクラウドサービスにおいて特権の割り当て及び利用制限し、管理する機能を提供すること。	○	ジンジャーサービスは利用ユーザに対して特権の割り当て等の管理する機能を提供しております。
27		パスワードの利用	提供するクラウドサービスにてパスワード管理ができるような機能を提供すること。また良質なパスワードを確実にする機能があること。	○	ジンジャーサービスは利用ユーザのログインパスワードについて以下のポリシーを設定可能となります。 ・パスワード最小文字数 ・パスワード有効期限 ・パスワード入力文字設定 パスワードについて設定できる制御につきましては以下ヘルプページに詳細を記載しております。 https://jinjer-jinji.zendesk.com/hc/ja/articles/360037557772
28		セッションのタイムアウト	一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能を提供することが望ましい。	○	セッションの有効期間を設けております。
29	ネットワークのアクセス制御		ネットワークを脅威から保護、またネットワークのセキュリティを維持するためにネットワークを適切に管理し、アクセス制御をすること。	○	セキュリティを維持するためにネットワーク構成の管理、ネットワーク機器監視を実施しております。またアクセス制御についても文書化し、管理・実施しております。
30			クラウドサービスを利用するネットワーク経路が暗号化されていることを確認すること。クラウドサービスで利用する情報がシステム上で暗号化されていること。	○	お客様のご利用端末からジンジャーサービスへのアクセスは、インターネット経由で行われ、その通信は、は全てSSL通信(TLS1.2、1.3)で暗号化しております。またサービスを利用して作成されたデータは全ては暗号化されております。
31	運用管理	媒体	記録媒体(書類、記録メディア)の保管管理については適切に行うこと。また廃棄する際には記録された情報を復元できないように安全に処分すること。また再利用の際には機密情報の漏えい等につながらないように対処すること。	○	社内規程にて、記録媒体の取扱方法(暗号化方法、保管、データの完全消去)を定め、適切に運用しております。
32	事業継続管理	事業継続計画	クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図るとともに、クラウドサービスの冗長化の状況を、クラウドサービスの利用を検討する者に明示することが望ましい。	○	ジンジャーサービスで利用する各種サーバは複数のデーターセンターを利用した冗長化構成となっています。 また大規模災害が発生した場合には別地域にある複数のデーターセンターを利用してサービス復旧が可能な構成となっております。 全てのサーバー、ネットワーク、ストレージ、データについて冗長化を実施しております。
33			事業継続計画については定期的に試験・更新すること。	○	事業継続計画書を作成し、ジンジャーサービス継続計画についての定期的(年1回の頻度)で訓練・手順の見直し等を行っております。
34		データセンタ	クラウドサービス提供に用いる機材は、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	○	ジンジャーサービスを構成するサーバ類が設置されたデータセンターでは電力システムは、完全に冗長化され、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源の保持しております。
35			クラウドサービス提供に用いる機材を設置する部屋には、火災検知・通報システム及び消火設備を用意すること。	○	ジンジャーサービスを構成するサーバ類が設置されたデータセンターでは火災検知・通報システム及び自動消火設備にて保護されております。
36	適用法令の識別		クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。	○	ジンジャーサービスで利用する各種サーバは日本国内にある複数のデーターセンターを利用して構成しております。
37			クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい。	○	当社ホームページに公開している以下の利用規約において、知的財産権について記載しております。 ■利用規約第24条（知的財産権） https://hcm-jinjer.com/terms/
38	個人データ及び個人情報の保護		個人データ及び個人情報は、関連する法令、規制、及び適用がある場合には、その要求にしたい適切に保護すること。またクラウド利用者が，データ保護及び個人情報保護に係る，国内外の法令，規則及び契約上の要求事項を識別することが望ましい。	○	当社ホームページに公開している以下の利用規約において、個人情報の取り扱いについて記載しております。 ■個人情報保護方針 https://jinjer.co.jp/privacy/
39	セキュリティ方針及び標準の順守		クラウド事業者は，独立したレビュー及び評価(例えば，内部/外部監査，認証，ぜい弱性，ペネトレーションテストなど)を定期的に実施し，情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。	○	当社担当部門による内部監査及び、ISMS認証の更新・外部審査を定期的に行っております。また、第三者機関による脆弱性診断、ペネトレーションテストを定期的に実施しております。