◆本チェックシートは、株式会社アジャイルウェアが提供する有償のクラウドサービス「Lycheeクラウド」について、そのセキュリティ対策を記載したものです。(2023年6月27日現在)
◆株式会社アジャイルウェアは、下記認証登録範囲の情報セキュリティマネジメントシステムについて「ISO/IEC27001:2013(JIS Q 27001:2014)」の要求事項に適合し、
認証登録番号「IS708853」を保有しています。
・パッケージソフトウェア及びWebアプリケーションの企画、開発、導入支援、運用、保守
・仮想サーバーの設計、構築、運用、保守
・システム開発に関する研修サービス
・業務システムの企画、開発、運用、保守
◆本チェックシートの項目は、以下を基に作成したものです。
経済産業省 - クラウドサービスレベルのチェックリスト 2010年8月版
(https://warp.da.ndl.go.jp/collections/content/info:ndljp/pid/8658576/www.meti.go.jp/press/20100816001/20100816001-4.pdf)

No.	種別	サービスレベル項目例	規定内容	測定単位	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)	時間帯	24時間365日 (計画停止／定期保守を除く)
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	[専有サーバーオプション:あり] 事前に弊社サポート用問合せ管理システムまたはメールで通知 [専有サーバーオプション:なし] 事前通知なし ・Redmineのバージョンアップ 原則平日の夜間(20:00～)もしくは、土日祝の休日昼間に実施 ・Lychee Redmineプラグインのバージョンアップ 平日22時以降、弊社の任意のタイミングで実施
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	30日前までにメールで通知
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	なし
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(%)	サービスとしてはSLAなし。 サーバー稼働率についてはAWSのSLAを参照ください。 ただし、専有サーバーオプションありの場合はサーバー構成に依存します。
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	なし
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	データベースにアクセス可能な場合は、データベースのダンプデータの提供は可能です。 ストレージにアクセス可能な場合は、日次で取得しているバックアップデータの提供は可能です。
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)	データベースのSQLファイルとして提供。 Redmine上の添付ファイルはZIPファイルとして提供。
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	[専有サーバーオプション:あり] 事前通知の上、原則毎月バージョンアップを実施。 [専有サーバーオプション:なし] 事前通知なし ・Redmineのバージョンアップ 原則平日の夜間(20:00～)もしくは、土日祝の休日昼間に実施 ・Lychee Redmineプラグインのバージョンアップ 平日22時以降、弊社の任意のタイミングで実施
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)	時間	弊社営業時間内での対応となります
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	時間	12時間以内
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	回	0回／0回
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)の設定に基づく監視	有無	サービス、ネットワークの死活監視 パフォーマンス監視 [専有サーバーオプション:あり] 上記に加え、ディスク残容量監視
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)	有無	有:以下のいずれかの方法で通知 - 弊社サポート用問合せ管理システムを利用して窓口のご担当者様に通知 - 指定された緊急連絡先へのメール通知
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	時間	サポートサービス提供時間内に検出した場合1時間以内に通知
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	時間(分)	3分
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	時間	なし
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)	有無	ログの提供は原則行っておりません。 アプリケーションの操作ログは利用者自身でご取得いただけますが、記載内容等についてのサポートはございません。 [専有サーバーオプション:あり] 上記に加え、監査等の目的でログの提供が必要な場合、別途有償での対応は可能です。
19	性能	応答時間	処理の応答時間	時間(秒)	規定なし(利用する機能による)
20		遅延	処理の応答時間の遅延継続時間	時間(分)	規定なし(利用する機能による)
21		バッチ処理時間	バッチ処理(一括処理)の応答時間	時間(分)	規定なし(利用する機能による)
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	有無	[専有サーバーオプション:あり] Redmineの仕様に準ずる [専有サーバーオプション:なし] なし

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）	有無	Rest API（Redmineの仕様に準ずる）
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	有無（制約条件）	[専有サーバーオプション:あり] サーバー性能に準拠（ベストエフォート） [専有サーバーオプション:なし] ベストエフォート
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	処理能力	契約内容に準ずる
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	時間帯	弊社営業日10時～17時（電話・メール・弊社サポート用問合せ管理システム）
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	時間帯	弊社営業日10時～17時（電話・メール・弊社サポート用問合せ管理システム）
No.	**種別**	**サービスレベル項目例**	**規定内容**	**測定単位**	**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	有無／内容	毎日定時に取得。データベースは7世代分のスナップショットを保持。 添付ファイルは1世代分を保持。 サーバー障害発生時のロールバックを目的とするため、利用者へのデータ提供は原則行いません。
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	時間	毎朝4時まで。
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	時間	AWS S3を使用しています。 契約期間内はバックアップデータを保持。 ログについては、6ヶ月分保持。
31		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	解約時に全データをインスタンスごと消去。 データベースダンプおよび添付ファイルの提供が可能。
32		バックアップ世代数	保証する世代数	世代数	データベースは7世代分。 添付ファイルは1世代分。
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、暗号化要件の有無	有無	ストレージの暗号化を実施
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	有無／内容	[専有サーバーオプション:あり] シングルテナント型のため対象外 [専有サーバーオプション:なし] 無 ストレージキーはアプリケーションサーバーにて一括管理。 ただし、アップロードされたデータおよびデータベースはテナント毎に分離。
35		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	損害賠償保険加入なし。
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、外部への漏えいの懸念のない状態が構築できていること	有無／内容	Lycheeクラウド利用規定第11条（契約終了後の処理）に定義。
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ること	有無	なし
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	有無	Redmineの仕様に準ずる
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）が取得されていること	有無	2019年6月にISMS認証を取得。
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ること	有無／実施状況	年1回、第三者によるアプリケーションの脆弱性診断を実施
41		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	あり。 顧客情報並びに付随情報などを最重要情報と定め、適切な保管場所・保管方法を規定し、実施している。
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	有無	TLS1.2 ※SSL3.0以下は使用不可
43		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	なし
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	有無	[専有サーバーオプション:あり] シングルテナント型のため対象外 [専有サーバーオプション:なし] あり。 データベースを物理的に分離し、データベース利用ユーザも別々に管理している。
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	あり。 利用者データへアクセス可能な人数は必要最小限とし、職務範囲に応じた権限のみ付与する。

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	なし。 別途有償にて対応可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	随時
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	なし。 AWS RDSのスナップショット、AWS S3を使用しており、二次媒体には記録していません。
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るか	把握状況	データ保存地はAWSの東京リージョンです。 各種法制度の下におけるデータ取扱いおよび利用に関する制約条件を把握しています。