CO-NECT セキュリティチェックシート

経済産業省 クラウドサービスレベルのチェックリスト準拠

◎本チェックシートは、CO-NECT株式会社が提供するサービスについて、そのセキュリティ対策を記載したものです。
◎CO-NECT株式会社は情報セキュリティマネジメントシステムについて下記認証を取得しています。
・認証基準：JIS Q 27001:2014(ISO/IEC 27001:2013)
・認証登録番号：16241624
・認証範囲：受発注システム開発、運用、カスタマーサポート
・適用宣言書：Ver.2.0
・認証機関：ビューローベリタスジャパン株式会社　システム認証事業本部(ISR018)
◎CO-NECT株式会社は「ASP・SaaSの安全・信頼性に係る情報開示認定」に認定されています。
・認定番号：0244-2102
◎本チェックシートの項目は、経済産業省クラウドサービスレベルのチェックリストを元に作成されています。

更新：2023/11/15

No.	種別	サービスレベル項目	規定内容	測定単位	回答内容
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/保守を除く)
2	可用性	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] 利用規約に記載の通り、通常計画停止の一ヶ月前までにお知らせします。 https://conct.jp/about/userpolicy
3	可用性	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] 利用規約に記載の通り、通常利用者に対し、一ヶ月前までにお知らせします。 https://conct.jp/about/userpolicy
4	可用性	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] 現状定義しておりません。
5	可用性	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(%)	直近1年の実績 99.9990 %
6	可用性	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	災害発生時のシステム復旧 [有] ・複数のデータセンターで冗長化 ・リージョンレベルでの災害が発生した場合はサービス停止
7	可用性	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] サービスが停止している期間の代替措置はありません。

8	可用性	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] サービスが停止している期間の代替措置はありません。
9	可用性	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] ・定期的な機能追加および改修のバージョンアップを実施しております。 ・利用者への影響が予見される大きな仕様変更は「お知らせ」にて事前に告知します。 ・変更内容等は「ヘルプセンター」にて公開しています。 ※サービスにて利用しているミドルウェアのバージョンアップ・セキュリティパッチ等は原則1週間以内に適用しております。
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)	時間	0分(過去1年間に発生した障害を対象) サービス全体が停止するような障害は発生しておりません。
11	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	・営業時間中に発生した障害については当日中に再開することを目標としております。 ・営業時間外に発生した障害については、障害内容によりますが翌営業日中に再開することを目標としております。
12	信頼性	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 過去1年間で、1日以内に復旧した障害件数は0件、対応に1日以上要した障害件数は0件
13	信頼性	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]
14	信頼性	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] ・サービスのエラーの監視、サーバーリソース等を監視しております。 ・エラー発生時およびサーバーリソースの閾値を超えた場合に開発担当へ通知が届きます。
15	信頼性	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	異常検出後、ネットワークの状況によりますが数分以内に弊社の開発担当へ通知が届きます。
16	信頼性	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)	・エラーについては常時監視 ・サーバーリソース(負荷)については1分または5分間隔で収集/集計
17	信頼性	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	報告方法はありません。
18	信頼性	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] 利用者に提供可能なログはありません。
19	性能	応答時間	処理の応答時間	時間(秒)	規定はありません。 (対象の機能・データ量・条件により異なります)
20	性能	遅延	処理の応答時間の遅延継続時間	時間(分)	規定はありません。
21	性能	バッチ処理時間	バッチ処理(一括処理)の応答時間	時間(分)	規定はありません。 (対象の機能・データ量・条件により異なります)
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	有無	[無] 原則カスタマイズ不可となっております。
23	拡張性	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] ・受注側の一部の機能についてはAPIを提供しており取得/更新が可能です。 ・API仕様書は公開しております。

24	拡張性	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] 制限はありません。 (サーバー負荷は監視しており、必要に応じてサーバーを増強しております)
25	拡張性	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	ページビュー数の上限は設けておりません。
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	平日10時から18時、ただし状況に応じて個別対応を実施
27	サポート	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	平日10時から18時
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	[有] DBについて ・1回/1日 S3 (AuroraDBのバックアップ) ファイルストレージについて ・S3にはバックアップという概念はありません。(複数のAZに自動コピーして保存しております)
29	データ管理	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	深夜帯にデータベース全体のスナップショットを作成しております。
30	データ管理	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	7日間 awsの機能にてバックアップ(スナップショット)を作成しております。 バックアップ頻度は1日1回、世代数は7世代
31	データ管理	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	[無] 解約してもデータは削除いたしません。
32	データ管理	バックアップ世代数	保証する世代数	世代数	サーバーのストレージ(EBS) 7世代 データベース 7世代
33	データ管理	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] サーバーのストレージ等は暗号化しております。
34	データ管理	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	[無] 顧客毎のデータはストレージ分割しておりません。(ロジックによるアクセス制御のみ)
35	データ管理	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] 弊社が賠償責任負う場合の内容については利用規約に記載があります。 https://conct.jp/about/userpolicy
36	データ管理	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] 解約時にデータの返却や削除はしておりません。
37	データ管理	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]
38	データ管理	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] 入力データ形式の制限があります。

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)が取得されていること	有無	[有] ・情報セキュリティマネジメントシステムについて下記認証を取得しております。 ・認証基準：JIS Q 27001:2014(ISO/IEC 27001:2013) ・認証登録番号：16241624 ・認証範囲：受発注システム開発、運用、カスタマーサポート ・適用宣言書：Ver.2.0 ・認証機関：ビューローベリタスジャパン株式会社　システム認証事業本部(ISR018) ・「ASP・SaaSの安全・信頼性に係る情報開示認定」に認定されております。
40	セキュリティ	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	[無] 第三者による評価/脆弱性診断等は実施しておりません。
41	セキュリティ	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] (クラウドサービスやsshの権限の文脈では)許可された従業員のみアクセス可能としております。
42	セキュリティ	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] tls1.2を採用しております。
43	セキュリティ	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]
44	セキュリティ	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	[無] SaaSのため各種サーバーリソースは分離しておりません。
45	セキュリティ	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] サービスの管理者権限、AWSのアカウント、サーバーへの接続権限などを限定しています。
46	セキュリティ	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	IDはユーザーごとに付与しております。
47	セキュリティ	ウイルススキャン	ウイルススキャンの頻度	頻度	1サーバーあたり週に1回実施
48	セキュリティ	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] バックアップはクラウド上に保持しており、持ち出し可能な外部媒体への保管は行わないようにしております。
49	セキュリティ	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	データの保存地の各種法制度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おります。