『AUN（アウン）』クラウドサービスレベルのチェックリスト

※項目は「クラウドサービスレベルのチェックリスト」(経済産業省)に準拠しています。

第3版: 2024年2月22日

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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日となります（計画停止／定期保守を除く）チャットサポートは平日10:00～17:00
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】1週間前にサービス内・メール・ホームページ・SNSで通知します。
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】30日前までにサービス内・メール・ホームページで予告します。
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】現時点でサービス提供停止の予定はなく、預託等の措置は行っていません。
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（%）	2021年1月～2021年12月の実績値は99.93%です。
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	【無】サービス提供に必要なサーバ/ネットワーク機器などの設置場所は十分な災害対策が行われています。
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	【有】バックアップポリシー（世代管理、バックアップ対象、取得サイクル等）に従い、情報をバックアップしています。適切な時間内にリストアが可能です。
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）	公開しておりません。 ただし個別のAUNファイルについてはPDF形式で常時ダウンロード可能です。
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】随時、機能追加などを実施しています。お客様への影響が大きい変更は、事前にメール・ホームページで通知します。 脆弱性の情報収集、監査、ログ監視、セキュリティ診断により現状を把握し、リスク分析のうえ対策を講じています。
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	公開しておりません。
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	公開しておりません。
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	回数は公開しておりませんが、個別の障害の内容についてはホームページで公開しております。
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	【有】死活監視、パフォーマンス監視、エラー監視を行っています。
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】障害発生時は速やかに弊社担当者に通知され、対応を行います。 お客様へは必要に応じてホームページ・SNSで通知します。
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	弊社担当者への通知は数分以内に行われます。お客様への影響が大きい障害に関しては、お客様への通知を可能な限り迅速に行います。
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）	5分間隔で監視しております。
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	必要に応じてホームページ・SNSで通知します。報告内容は、発生日時・解決日時・障害原因・今後の対策等となります。
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	【無】現時点ではお客様へ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）	公開しておりません。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	公開しておりません。
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）	公開しておりません。
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】個別の企業さま向けの機能やデザインのカスタマイズは承っておりません。
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	【無】外部システムとの接続仕様はありません。
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	有無（制約条	【無】制限はありません。
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	公開しておりません。
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10:00～17:00にチャットサポートより受け付けています。
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	平日10:00～17:00にチャットサポートより受け付けています。
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】バックアップポリシー（世代管理、バックアップ対象、取得サイクル等）に従い、セキュリティ観点で必要なバックアップを、適切な方法及び形式で取得しています。

『AUN（アウン）』クラウドサービスレベルのチェックリスト

※項目は「クラウドサービスレベルのチェックリスト」(経済産業省)に準拠しています。

第3版: 2024年2月22日

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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	当社責任による万が一の障害発生時には当日夜間（時間帯と内容によっては前日夜間）へのロールバックが最短となります。
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	1週間
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	【有】弊社の定める時期に消去します。
32		バックアップ世代数	保証する世代数	世代数	7世代
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	【有】暗号化を実施しています。
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	【無】 当社システムにて管理しており、契約者側へのキー提供・契約者が認識する事象はありません。具体的な処理・構成につきましてはセキュリティ上公開してお
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	【無】保険には加入しておりますが、詳細は公開しておりません。 尚、利用規約に定められた範囲でお客様のデータ保護に最大限の注意を払っています。
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	【有】データの返却はされません。 解約後、弊社の定める時期にデータを消去します。
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	【無】データの預託は行っておりません。
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	【有】入力項目の要件に合わせて形式や長さのチェックを行っています。
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】プライバシーマークを取得しています。 登録番号:27000113
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	【無】第三者機関による診断は行っておりませんが、脆弱性に関わる情報を定期的に収集し、新たな脆弱性が発見されれば影響評価や対策検討を行っています。
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	【有】物理的なエリアの分離、入室者の制限を行っています。業務上必要な一部の開発者や担当者のみデータへのアクセスが可能です。
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	【有】TLSv1.2にて通信を暗号化しています。
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	【無】実施していません。
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	【有】ユーザ ID、パスワード、2段階認証の組み合わせでアカウント情報を管理しており、ユーザごと、 権限ごとにアクセス制御を行うことで制限しております。
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	【有】業務上必要な一部の開発者や担当者のみデータへのアクセスが可能です。
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	保管しているログから調査可能です。 セキュリティ観点で必要なログを、適切な方法及び形式で取得していますが、具体的な期間につきましては、非公開情報となります。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	全スタッフの端末にウイルス対策ソフトを導入、常時スキャンを実施しております。サービスのサーバー上ではアップロードファイルを展開・実行することはないため、ウイルス対策ソフトの導入はしておりません。
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	【有】二次記憶媒体の利用を禁止しています。バックアップはクラウドにのみ保管し、管理者のみがアクセス可能。
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	把握しております。