2025年7月1日

経済産業省　クラウドサービスレベルのチェックリスト

https://warp.da.ndl.go.jp/info:ndljp/pid/8658576/www.meti.go.jp/press/20100816001/20100816001-4.pdf

アートメタバースランド株式会社

No.	種別	サービスレベル項目例	規程内容	対応/可否	メタバースOffice Hub設定内容
アプリケーション運用					
1	可用性	サービス停止時間	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）	○	24時間365日継続的な運用を保証します。（計画されたメンテナンス時間を除く）
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）	○	定期メンテナンスによるサービス停止の2週間前までに通知します。
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）	○	サービス終了の予定はありませんが、Office hub利用規約の第１４条に「終了の90日前までに通知」と規定しています。
4		突然のサービス提供停止時の対処	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	○	顧客データの保護機構を備え、定期的なバックアップを実施し、突発的な障害時に迅速なシステム復旧が可能です。
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）	○	100%　これまで障害による稼働停止はありません 24時間365日稼働（メンテナンス時間を除く）。
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	○	AWSを活用した災害対策の導入により、障害発生時のセキュリティ管理とシステム復旧を可能にしています。
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	○	即時復旧が困難な場合の代替策を用意できます。

8		代替処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	○	データのダウンロード機能（画像、アップロード済ファイルなど）を提供し、サービスが一時的に中断してもユーザーがデータを取得可能です。
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	○	AWS が責任を保有する OS やミドルウェア等については AWS が随時パッチを適用します。 当社が責任を保有するOffice Hubシステムについては、当社が、計画的にアップグレード・バージョン変更・パッチ適用の管理ポリシーを運用します。
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）	○	これまで障害による稼働停止はありません。 MTTR（平均修復時間）に関する明確な規定はありませんが、可能な限り迅速に復旧します。
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	－	RTO（復旧目標時間）に関する明確な規定はありませんが、可能な限り迅速に復旧します。
12		目標復旧時点(RPO)	障害発生後のサービス提供再開に対応するバックアップ世代管理の目標時間	○	RPO（復旧時点目標）を設定し、最新のバックアップデータからの復旧を保証します。 当日午前3時（JST=UTC+9）以前のデータに復旧します。
13		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	○	これまで障害による稼働停止はありません。
14		システム監査基準	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	○	システム監視、リソース監視、パフォーマンス監視を実施しています。
15		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）	○	障害対応ガイドラインで明確な障害通知プロセスを定めており、障害レベルに沿って、サービス内・当社ホームページ内・eメールで通知します。
16		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	○	常時、当社ホームページ上でOffice Hubの稼働状況を開示しています。 その他障害に関するご連絡は、障害検知後、可能な限り迅速に通知します。
17		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	○	システムの状態を常時監視し、情報の収集を行っています。
18		サービス提供状況の報告/間隔	サービス提供状況を報告する方法／時間間隔	○	常時、当社ホームページ上でOffice Hubの稼働状況を開示しています。

19		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）	○	**利用者のログデータは1ヶ月間保存しています。 ログデータの提供については個別に有料で対応可能です。（最大1年間の設定が可能です）**
20	性　能	応答時間	処理の応答時間	○	**ほぼリアルタイムで応答します。 Office Hubシステムの応答時間の保証は行っておりません。**
21		遅延	処理の応答時間の遅延継続時間	○	**ほぼ遅延はありません。 Office Hubシステムの応答時間の保証は行っておりません。**
22		バッチ処理時間	バッチ処理（一括処理）の応答時間	○	**ほぼ遅延はありません。 Office Hubシステムの応答時間の保証は行っておりません。**
23	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	○	**外部サービス（WEB会議システムやカレンダー）連携先の選択、ユーザー権限の管理、ユーザーＩＤのブロック等のカスタマイズを行うことができます。**
24		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）	○	**外部サービス（WEB会議システムやカレンダー）とＡＰＩ連携を行っています。**
25		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	○	**AWSの自動拡張機能を活用しており、同時接続ユーザー数に制限はありません。 ただし、各オフィスフロアごとには、接続定員を設定しています。**
26		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	○	**リソースに制限はありません。 ただし、設定利用枠を超えた場合、追加料金が発生します。**
サポート					
27	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	○	**eメール…24時間365日 電話…平日9:00～17:00**
28	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	○	**eメール…24時間365日 電話…平日9:00～17:00**

データ管理				
29	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	○	**バックアップ方法 … 自動フルバックアップ** **保存期間 … 30日間** **保存先 … AWS S3（東京リージョン）**
30	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	○	**毎日午前3時（JST=UTC+9）にバックアップ実施します。**
31	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	○	**データ保持期間… 30日間**
32	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	○	**Office Hub利用規約の第９条、第１１条、第１２条に定めております。**
33	バックアップ世代数	保証する世代数	○	**30日分のバックアップ（30世代分）を保持しています。**
34	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	○	**TLS による暗号化を実施しています。**
35	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	○	**AWS側のGitLab Runner上で効果的にキー管理を行っています。** **Office HubはＩＤ毎に権限設定を行い、ファイヤーウォールを厳正に管理しています。** **別途料金がかかりますが、シングルテナントストレージ管理も採用可能です。**
36	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	○	**Office Hub利用規約の第１３条、第１５条に定めております。**
37	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	○	**解約時はデータを消去する仕組みを整えています。**
38	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	○	**通信経路をTLSにより暗号化し、ユーザーが入力したデータ（テキスト、画像、アップロード済ファイルなど）の盗聴や改ざんを防ぎ、正確に他のユーザーに配信します。**

39	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	○	**想定外のデータ入力が行われないように制御する仕組みを導入しています。**
セキュリティ				
40	公的認証取得の要件	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	○	**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、利用者のデータアクセス権など、利用者データの取扱方法は、認証取得要件を満たしています。 ISMS認証の取得準備中です。**
41	アプリケーションに関する第三者評価	第三者によるウェブアプリケーション脆弱性評価実施	○	**年間を通してWeb サービス全体の診断を実施しています。 年１回、外部機関による評価を実施します。**
42	情報取扱い環境	提供者側でデータ取扱環境が適切に確保されていること	○	**情報へのアクセス権は担当ごとにアクセス範囲が決められており、オペレーションを監視しています。**
43	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	○	**TLSによるセキュリティ確保**
44	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」	－	**非上場会社で対象に当たりません。**
45	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	○	**論理的に他社データと分離し、相互に閲覧できないよう制御しています。 Office HubはＩＤ毎に権限設定を行い、ファイヤーウォールを厳正に管理しています。**
46	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	○	**アクセス権は限定された担当者ごとにアクセス範囲が決められており、オペレーションを監視しています。**
47	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	○	**ＩＤはユーザーごとに発行されており、操作ログはAWS上に30日間データ保持されます。**
48	ウイルススキャン	ウイルススキャンの頻度	○	**AWS側に実装されている機能に加え、SonarQubeを使用したソースコードスキャンを実施しています。**

49	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	○	**AWS上に自動バックアップを行なっており、許可された権限者のみアクセス可能です。セカンダリのセキュアストレージは使用していません。**
50	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	○	**各地域のデータ保存および処理に関する法規制を遵守しています。**