

# Equipmedia セキュリティチェックシート

2024年03月22日版

本資料は、経済産業省「クラウドサービスレベルのチェックリスト」に基づき、株式会社Jストリームの提供するEquipmediaサービスのセキュリティについてまとめた資料です。

経産省 2010年8月発行 クラウドサービスレベルのチェックリスト					
No.	種別	サービスレベル項目例	規定内容	測定単位	回答
<b>アプリケーション運用</b>					
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日です。（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	【有】 原則1か月前にご連絡します。 メンテナンスでも実施5営業日前にまでメール・サービス管理画面にて通知するようにいたします。
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】 現時点で終了の予定はございませんが、サービス終了時には約半年程度前にはメール・Webサイトで通知する予定です。
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】 現時点で終了予定はなく、プログラムやデータの預託も予定はございません。
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 (%)	2023年の実績値は99.99% (※) でした。 計画停止以外でサービスが停止したインシデント情報を開示しています。 ※SLA対象項目より測定した実績値となります
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	【有】 配信用のキャッシュサーバーは複数拠点のデータセンターに分散配置しています。 コンテンツストレージデータは、バックアップを別地域のデータセンターに保管しています。
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	有無	【無】 システムはすべて冗長化されていますが、冗長化で対応できない、なんらかの重大障害時の代替手段の提供は行っていません。
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。
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】 機能追加などは随時行っております。お客様への影響が大きい変更については、事前にWebサイトやサービス内で告知を行います。
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。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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	目標復旧時間の設定はしておりますが、詳細は公開していません。
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	回数としては公開していませんが、個別の障害情報は管理画面上のおしらせやステータス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、リソース監視、サービスの正常性監視を行っております。
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。お客様への通知は必要に応じてメール、サービス管理画面上のおしらせ、ステータスページで行います。
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。 お客様への通知は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)	監視項目により異なりますが、最短1分間隔で行っています。
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	必要に応じてメール、サービス管理画面上のおしらせ、ステータスページにて行います。
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	【有】 管理画面より動画視聴ログ、操作ログを取得することが可能です。
19	性能	応答時間	処理の応答時間	時間(秒)	公開していません。
20		遅延	処理の応答時間の遅延継続時間	時間(分)	公開していません。
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)	公開していません。
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】 機能・デザインの個別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	【有】 外部サービスと連携する各種APIを公開しております。
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)	オンデマンド動画の制限はございません。 ライブの同時視聴制限はプランに応じて異なります。
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	【有】 ご利用のプランに応じて、利用可能なストレージ容量の上限があります。(有料オプションにて増設可能)

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
<b>サポート</b>					
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	24時間365日となります。(問い合わせフォームでの受付) 弊社障害検知時以外は、回答は弊社営業時間内対応となります。
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	弊社営業時間での対応となります。 回答はご質問内容によって異なりますが、概ね翌営業日中に一次回答はいたします。
<b>データ管理</b>					
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】 動画コンテンツ：ストレージ上で日次スナップショットを取得、月次で外部データセンターにバックアップを取得しています。 DBデータ：日次でバックアップを取得します。
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取り、データを保証する時点	時間	具体的な時点は公開しておりませんが、24時間以内のデータを取得しています。
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	外部データセンターでの保管データは月次で更新されます。
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】 サービス解約が確認された後に、一定期間の保持期間を経て、解約後90日以内を目標にデータの削除を実施いたします。
32		バックアップ世代数	保証する世代数	世代数	動画コンテンツ：日次スナップショットは7世代まで 月次バックアップは1世代です。 DBデータ：日次で3世代までバックアップを残します。
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】 TLSv1.2にて通信を暗号化しています。(動画データの暗号化は行っておりませんが暗号化するオプション機能は提供しています。)
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	【有】 お客様の契約スペースごとに分離されたデータ領域で運用しております。
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	【有】 データ漏洩・データ破壊時の保険は加入しており、有事の際は被害額の一部が補填される体制をとっています。
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	サービス解約時にデータは削除いたします。元データの返却は行いませんが、動画元データに関しては管理画面から再取得が可能です。
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	【有】 データ入力時に検証を行っています。通信経路はTLSにより盗聴を防いでいます。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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。
<b>セキュリティ</b>					
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】 ISO/IEC 27001, ISO/IEC 27017, プライバシーマークを取得しています。
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	【有】 年次で外部診断会社による脆弱性診断を実施しています。
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】 データへのアクセスは業務上必要な一部のシステム運用者のみに制限されています。 またアクセスするメンバーをID/PW+鍵認証とIPアドレス制限・VPNを組み合わせ制御しております。
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】 SAS70/18号監査報告は当社では行っておりません。
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】 テナントID（お客様ID）ごとにデータを論理的に分離して管理しています。
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】 データへのアクセスは業務上必要な一部のシステム運用者のみに限定されています。 またアクセスするメンバーをID/PW+鍵認証とIPアドレス制限・VPNを組み合わせ制御しております。
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	IDは個人ごとに発行して管理しており、保管ログより調査が可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	開発・運用に利用するマシンはリアルタイムスキャンを有効化し随時検索しています。 WindowsOSの配信サーバーはウイルススキャンを有効し、サーバーおよびアップロードされるコンテンツはリアルタイムスキャンが実施されています。
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】 二次記憶媒体を使用せず、データセンター間でバックアップを取っております。また運用に利用する端末では二次記憶媒体の利用を制限しています。

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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	【有】 把握しております。