Dive セキュリティチェックシート

2025 年 7 月 22 日時点

2024 年 5 月 19 日時点経済産業省が公開している「クラウドサービスレベルのチェックリスト」に基づき、Dive のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目	規定内容	測定単位	Dive
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 日です。(計画停止除く)
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 実施 5 営業日前までに、担当者へのメール通知、及び、公式 WEB サイト（https://www.episotech.com/）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 現時点でサービス終了予定はありませんが、終了 3ヶ月前までに公式 WEB サイトにて事前に通知します。
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 現時点でサービス終了予定はありません。データの預託も未定です。
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)	稼働率 (%)	過去一年間)の実績値は 99.9%でした。
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	有無	有 サーバは、異なる物理的な場所（Availability Zone）に複数配置し冗長化して運用しています。データセンター（GCP）です。
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 即時復旧が可能なように、データセンターの冗長化、及びバックアップの世代管理を行っております。
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)	無 ただし、今後 PDF でエクスポートができるよう実装を検討しています。
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 機能追加などは随時行っております。事前告知は原則行わず、リリース後に公式 WEB サイト等で報告します。（軽微な場合は、この限りではありません）

Dive セキュリティチェックシート

2025 年 7 月 22 日時点

2024 年 5 月 19 日時点経済産業省が公開している「クラウドサービスレベルのチェックリスト」に基づき、Dive のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目	規定内容	測定単位	Dive
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	回数としては公開しておりませんが、個別の障害情報は公式 WEB サイトで公開をします。 https://www.episotech.com/
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 パフォーマンス監視、リソース監視、アプリケーションエラー監視、死活監視を常時実施しております。
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 メールにて弊社担当者に通知されます。 お客様への通知は必要に応じてサービス内、公式 WEB サイト、SNS で行います。 「Dive 障害運用マニュアル（社内用）」にて運用。※非公開
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即時行われます。 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)	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	定期的なサービス提供状況報告は行っていません。
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 Web アプリから、アカウントの利用履歴、監査ログ機能をご利用ください。

Dive セキュリティチェックシート

2025 年 7 月 22 日時点

2024 年 5 月 19 日時点経済産業省が公開している「クラウドサービスレベルのチェックリスト」に基づき、Dive のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目	規定内容	測定単位	Dive
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	有 外部出力機能など、都度ご要望の確認うえ、検討します。
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 Immersal サービスとの API 連携、Microsoft アカウントでのシングルサインオンが可能です。
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)	無 ただし、同じアカウントでスマホアプリに同時にアクセスできるのは 1 人まで。
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	無 ただし、動画のアップロードの 1 回あたりの上限は 1GB です。
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	24 時間 365 日となります。（メール・お問い合わせフォーム）
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	月～金曜日 10：00 ～ 17：00（年末年始、祝日等は除く）となります。*日本時間
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 過去 90 日間のデータを復元できるよう、1 日 1 回以上のバックアップを行っております。バックアップデータへのアクセスは、限られた一部の担当者のみに制限されています。 データはデータセンター（GCP）に保存。
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	毎日 13 時頃に取得します。＊日本時間
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	バックアップデータの保存期間は最大で 90 日間となります。
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 サービス解約時に無料プランを利用しない場合、直ちにデータを削除します。また、サービス解約前に作成データを保存できるよう動画ダウンロード、手順書 PDF 出力機能を備えています。
32		バックアップ世代数	保証する世代数	世代数	90 世代を保管しています。

Dive セキュリティチェックシート

2025 年 7 月 22 日時点

2024 年 5 月 19 日時点経済産業省が公開している「クラウドサービスレベルのチェックリスト」に基づき、Dive のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目	規定内容	測定単位	Dive
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 HTTPS 通信にて暗号化しています。データベース・ファイルともに暗号化しております。 また、パスワードなどの機微な情報はアプリケーションレベルでも暗号化しています。
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 お客様の契約チームごとに、論理的に分離されたデータ領域で管理しています。
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	無 損害賠償保険には加入しておりませんが、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 サービス解約時に直ちにデータを削除します。また、サービス解約前に作成データを保存できるよう動画ダウンロード、手順書 PDF 出力を今後実装予定です。
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	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。

Dive セキュリティチェックシート

2025 年 7 月 22 日時点

2024 年 5 月 19 日時点経済産業省が公開している「クラウドサービスレベルのチェックリスト」に基づき、Dive のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目	規定内容	測定単位	Dive
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 ISO/IEC270001: 2022（ISMS）を 2024 年 11 月に取得済
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 ただし、今後有外部のセキュリティ専門会社によるアプリケーション脆弱性検査、クラウド診断を定期的に実施する事を計画しております。
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担当者のみに明確に制限しております。また、ファイアーウォールで弊社環境からのみアクセスできるように制限しております。
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 HTTPS で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 お客様の契約チームごとに、論理的に分離されたデータ領域で管理しています。
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担当者のみに制限されています。
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います。アクセスログは無期限で保存しています。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	Palo Alto Networks のテクノロジーを使用して構築されている GCP の Cloud IDS（クラウド侵入検知システム）によりリアルタイムに監視しています。
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 二次記憶媒体の利用を禁止しています。

Dive セキュリティチェックシート

2025 年 7 月 22 日時点

2024 年 5 月 19 日時点経済産業省が公開している「クラウドサービスレベルのチェックリスト」に基づき、Dive のセキュリティについてまとめたものです。

No.	種別	サービスレベル項目	規定内容	測定単位	Dive
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	把握しております。
50		ログの種類	取得しているログの種類について	有無	有 GCP：操作ログ、アクセスログ OS：システムログ、認証ログ、監査ログ ログミドルウェア：実行ログ、アクセスログ、エラーログアプリケーション：エラーログ、操作ログ
51		WAF について	WAF を導入しているか	有無	有 DDoS 攻撃などを防ぐ施策をしています。
52		IDS について	IDS（不正侵入検知システム）は機能しているか	有無	有 Palo Alto Networks のテクノロジーを使用して構築されている GCP の Cloud IDS（クラウド侵入検知システム）で監視しています。
53		セキュリティパッチについて	セキュリティパッチ適用はどのぐらいの周期で実施されているか	頻度	GCP の Firebase サービスにより、定期的に実施されています。
54		セッションについて	セッションタイムアウトの時間は何分か	頻度	360 分（6 時間）です。 ログイン画面の「自動ログインする」チェックが OFF の場合、6 時間アクセスがないとログアウト状態になります。