

Dive セキュリティチェックシート

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」の項目に沿って、Dive のサービスレベルとセキュリティへの取り組みをまとめたものです。
2026年10月31日時点 エピソテック株式会社

可用性

No.	項目	Dive の回答
1	サービス時間	24時間365日です。(計画停止除く)
2	計画停止予定通知	有 実施 5 営業日前までに、公式WEBサイト (https://help.divedx.com/) で通知します。
3	サービス提供終了時の事前通知	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	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	過去1年間の実績値は99.9%です。 社内の稼働目標は月間99.9%以上 (計画停止を除く) としています。詳しくはヘルプセンターの「サービスレベルの目標」(https://help.divedx.com/hc/ja/articles/5762381180702) をご覧ください。
6	ディザスタリカバリ	有 サーバーは Google Cloud 上の異なる物理的な場所 (ゾーン) に複数配置して冗長化しています。 データベースのバックアップとアップロードされたファイルは毎日、別のリージョン (大阪) へ複製し、東京リージョン全体の被災にも備えています。
7	重大障害時の代替手段	有 バックアップと、別のリージョン (大阪) への毎日の複製から復旧します。最大で約1日前の時点まで復旧でき、復旧は弊社が行います。 お客様でも、手順書の出力や動画のダウンロードでデータを保全できます。
8	代替措置で提供するデータ形式	有 手順書を PDF・Excel・Word・PowerPoint で、動画を MP4 で出力できます (出力できる形式はプランにより異なります) 。
9	アップグレード方針	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) 依存ライブラリの脆弱性は、週次の自動検査と常時のアラートで把握し、重要度に応じた期限を決めて更新しています。

信頼性

No.	項目	Dive の回答
10	平均復旧時間(MTTR)	平均値としては公開しておりません。
11	目標復旧時間(RTO)	障害は常時監視し、担当者へ即時に通知され、速やかに復旧に着手します。目標復旧時間の数値保証は設けていません。
12	障害発生件数	回数としては公開しておりませんが、個別の障害情報はヘルプセンターで公開しています。 https://help.divedx.com/hc/ja/sections/4948508049438

No.	項目	Dive の回答
13	システム監視基準	有 外形監視（5分間隔）、サーバー処理のエラー、定期処理の失敗・未実行、バックアップの失敗などを常時監視しています。
14	障害通知プロセス	有 異常は弊社担当者へチャットとメールで即時に通知されます。 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（ https://help.divedx.com/ ）、SNSで行います。
15	障害通知時間	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	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	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	有 監査ログ（ログインの成功・失敗、アカウントのロック、IP アドレス制限によるログインの拒否とログアウト、ユーザー・権限・セキュリティ設定の変更、外部共有など。日時・ユーザー・IP アドレスを含む）を、オーナー権限の方が管理画面から CSV で出力できます（全プラン）。

性能

No.	項目	Dive の回答
19	応答時間	公開しておりません。
20	遅延	公開しておりません。
21	バッチ処理時間	公開しておりません。

拡張性

No.	項目	Dive の回答
22	カスタマイズ性	有 外部出力時のフォーマットカスタマイズなど、都度ご要望を確認のうえ、検討します。
23	外部接続性	有 シングルサインオン（SAML 2.0・Microsoft Entra ID）、アカウントの自動連携（SCIM 2.0）、手順書の検索 API、AI との接続（MCP）、Microsoft 365・Google ドライブとの連携に対応しています。
24	同時接続利用者数	無
25	提供リソースの上限	無 ただし、動画は1本あたり60分までアップロードできます。

サポート

No.	項目	Dive の回答
26	サービス提供時間帯(障害対応)	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)	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

No.	項目	Dive の回答
28	バックアップの方法	有 データベースは毎日1回、自動でバックアップし、約90日分（最長98日）を保管しています。データベースのバックアップとアップロードされたファイルは毎日、別のリージョン（大阪）へ複製しています。復旧は弊社が行い、バックアップデータへのアクセスは限られた担当者の方に制限しています。 データは Google Cloud に保存しています（ファイルは東京リージョン、データベースはシンガポールリージョン、複製は大阪リージョン）。
29	バックアップデータを取得するタイミング（RPO）	データベースは毎日1回、日本時間の15時台に自動取得しています（取得時刻はクラウド基盤側の仕様により指定できません）。 アップロードされたファイルは毎日1回、大阪の保管先へ複製しています。
30	バックアップデータの保存期間	データベースのバックアップは約90日分（最長98日）を保管しています。 削除・上書きされたファイルは、複製先に90日間保管しています。
31	データ消去の要件	有 有償プランの終了後もフリープランとしてご利用を続けられ、その間データは保持されます。ご利用を終了される場合は、30日間の保管期間を経てデータを削除します（ご希望があれば期間を待たずに削除します）。削除は本番環境と大阪の複製の両方が対象で、データベースのバックアップは保存期間（最長98日）の経過で自動的に消去されます。ご要望に応じて、弊社代表者名の削除完了報告書を発行します。 解約前に、手順書の出力や動画のダウンロードでデータをお手元に保全できます。
32	バックアップ世代数	データベースは約90世代（毎日1回・最長98日）を保管しています。 ファイルは日ごとの世代ではなく、ファイルごとの版で90日間保管しています。
33	データ保護のための暗号化要件	有 通信は HTTPS（TLS）で暗号化しています。Web アプリと動画・画像の配信（app.divedx.com、cdn.divedx.com）は TLS 1.2 / 1.3 のみを受け付けます。 データベース、ファイル、バックアップは、Google Cloud の機能により AES-256 で常時暗号化して保管しています。パスワードは認証基盤でソルト付きハッシュ（scrypt）として保管し、平文では保持しません。
34	マルチテナントストレージにおけるキー管理要件	有 暗号鍵の生成・保管・定期的な更新は基盤事業者（Google Cloud）が行い、弊社の担当者も鍵そのものには触れられない仕組みです。 データは契約ごとのチーム単位で区分し、データベースの読み書きは、ログインした利用者の所属チームと権限をルールで確かめたうえで許可しています。
35	データ漏えい・破壊時の補償/保険	無 データ漏えい・破壊時の損害賠償保険には加入しておりませんが、利用規約に基づき責任範囲を定めています（損害賠償の上限は直近12ヶ月間の利用料金総額、逸失利益等は対象外）。 お客様のデータ保護に最大限の注意を払います。

No.	項目	Dive の回答
36	解約時のデータポータビリティ	有 解約前に、手順書の出力（PDF・Excel・Word・PowerPoint）や動画（MP4）のダウンロードで、データをお手元に保全できます（出力できる形式はプランにより異なります）。 ご利用を終了される場合は、30日間の保管期間を経て、本番環境と大阪の複製からデータを削除します。ご要望に応じて、削除完了報告書を発行します。
37	預託データの整合性検証作業	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	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。アップロードできるファイルは、種類ごとに形式を限定しています。

セキュリティ

No.	項目	Dive の回答
39	公的認証取得の要件	有 ISO/IEC 27001:2022（ISMS）の認証を取得しています（認証番号 GIJP-1469-IC、2024年11月取得、有効期限 2027年11月）。認証範囲に本サービスを含み、年1回の維持審査を受けています（直近は2026年10月）。
40	アプリケーションに関する第三者評価	有 クラウドサービスのセキュリティ評価サービス「Assured」の評価を受けています（2026年10月に回答を更新）。あわせて ISO/IEC 27001:2022（ISMS）認証を取得しています。 アプリケーションの診断は自社で継続的に実施しています。 ・週次（毎週月曜）の自動検査：ソースコードの静的解析（OWASP Top 10 等の規則）、依存ライブラリの脆弱性、秘密情報の混入 ・依存ライブラリの脆弱性アラートを常時有効化し、重要度に応じた期限を決めて対処
41	情報取扱い環境	有 本番環境は Google Cloud と Vercel のフルマネージドサービスで構成し、サーバーへの直接のログインや接続口は公開していません。 クラウド基盤の管理画面へのアクセスは、IAM による権限制御で業務上必要な担当者に限定し、2段階認証と16時間ごとの再認証を必須としています。運用用の操作は、認証アプリによる2段階認証でログインした場合だけ実行できるよう強制しています。
42	通信の暗号化レベル	有 HTTPS（TLS）で暗号化しています。Web アプリと動画・画像の配信（app.divedx.com、cdn.divedx.com）は TLS 1.2／1.3 のみを受け付けます（SSL、TLS 1.0／1.1 は受け付けません）。
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	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	有 データは契約ごとのチーム単位で区分して管理し、データベースの読み書きは、ログインした利用者の所属チームと権限をルールで確かめたくうえで許可しています。動画・画像などのファイルも、そのチームのメンバーと、メンバーが発行した外部共有の URL を開いた人にだけ配信しています。 チームのメンバー・権限・契約の変更は、権限を確かめるサーバーだけが行います。

No.	項目	Dive の回答
45	情報取扱者の制限	有 役割（オーナー・チーム管理者・グループ管理者・作成ユーザー・閲覧ユーザー・ゲスト）とグループの単位で、フォルダごとの閲覧・編集の範囲と使える機能を設定できます。手順書の本文と一覧のフォルダごとの閲覧範囲と、手順書の作成・編集を作成ユーザー以上に限ることは、データベースのセキュリティールとサーバーで強制しています。 接続元の IP アドレスによる制限も設定できます（全プラン）。 弊社がお客様のデータにアクセスするのは、サポートのご依頼があった場合と、障害の防止・対応でやむを得ない場合に限りです（利用規約第10条）。
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は個人ごとに発行して管理しています。 アプリケーションの監査ログはご利用期間中、ログインの記録・データベースへのアクセスの記録・管理操作などのセキュリティ調査用の監査ログは400日間、そのほかのクラウド基盤のログは90日間保存しており、必要に応じて検索・抽出してご提供します。
47	ウイルススキャン	本番システムはサーバーOSを自社で保有しないフルマネージド構成のため、基盤事業者（Google Cloud・Vercel）による保護・パッチ適用に依拠しています。アップロードできるファイルは、種類ごとに形式を限定しています。 開発・運用端末にはマルウェア対策ソフトを導入し、リアルタイム保護を有効化、定義ファイルを自動更新しています。 あわせて、ソースコードおよび依存ライブラリへの不正なコード混入を、開発パイプライン上で週次スキャンにより検査しています。
48	二次記憶媒体の安全性対策	有 外部記憶媒体は、情報セキュリティ管理規程（7.10 記憶媒体・8.13 情報のバックアップ）に基づき、システム管理者が承認した媒体（暗号化した SSD）を、開発データの月1回のバックアップにだけ利用しています。
49	データの外部保存方針	把握しております。データは Google Cloud のデータセンターに保管しています。動画・画像などのファイルは日本（東京リージョン）、データベースはシンガポール、ログインに使う認証情報は米国（Google の認証基盤の仕様）、災害に備えた複製は日本（大阪リージョン）です。任意の機能（映像通話・AR の位置合わせ）を使う場合は、それぞれのサービスでも処理します。 個人情報保護法に基づく安全管理措置を講じ、委託先（Google Cloud 等）を監督しています。
50	ログの種類	有 クラウド基盤：管理操作、データベース・ファイルへのアクセス、認証、権限のない要求の拒否などの監査ログ、サーバー処理のログ、WAF が遮断した要求の記録 アプリケーション：監査ログ（ログインの成功・失敗、アカウントのロック、IP アドレス制限によるログインの拒否とログアウト、ユーザー・権限・セキュリティ設定の変更、外部共有、契約の変更 等） 保存期間：アプリケーションの監査ログはご利用期間中、セキュリティ調査用の監査ログは400日間、そのほかのクラウド基盤のログは90日間です。
51	WAFについて	有 アプリケーション配信基盤の WAF（Web Application Firewall）を導入しています。既知の探索行為（CMS・管理ツール・設定ファイル等への不正アクセス試行）、ディレクトリトラバース、OS上のファイルへの参照試行、オープンリダイレクトを遮断しています。遮断した要求の記録は400日間保管しています。 また、認証系エンドポイントにレートリミットを設定し、同一の接続元からの短時間の大量アクセスを遮断しています。 加えて、プラットフォーム層で DDoS 緩和が常時稼働しています。
52	IDSについて	無 サーバーOSや仮想マシンを自社で保有しないフルマネージド構成のため、ネットワーク型IDSは適用対象外です。 代替として、アプリケーション配信基盤（Vercel）の標準の DDoS 対策と WAF で不正な通信を自動で検知・遮断し、その記録を400日間保管しています。認証・操作・管理操作のログはクラウド基盤のログ基盤で収集し、異常の検知に利用しています。

No.	項目	Dive の回答
53	セキュリティパッチについて	サーバーの基盤（OS、ミドルウェア、ネットワーク機器）は、Google Cloud と Vercel のフルマネージドサービスで、各社が随時パッチを適用しています。 弊社のサーバー処理のコンテナは公式の Node.js イメージを土台とし、デプロイ時に作り直しています。 アプリケーションの依存ライブラリは、週次の自動検査と常時のアラートで脆弱性を把握し、重要度に応じた期限を決めて更新しています。
54	セッションについて	無操作による自動ログアウトを、チームの管理者が30分から24時間の範囲で設定できます（無効にすることもできます）。新規に開設したチームの既定値は24時間です。 あわせて、ログインからの経過時間が一定を超えた場合に、操作の有無にかかわらず再認証を要求します。この期間は1日から90日の範囲で管理者が設定でき、既定値は30日です。 認証トークンの有効期間は1時間で、利用中は自動的に更新されます。 いずれもチーム単位の設定で、管理画面のセキュリティ設定から変更します。変更履歴は監査ログに記録されます。自動ログアウトが業務の妨げになる利用者は、グループまたは個人単位で対象外に指定できます。スマートフォン・スマートグラスの Dive アプリへの適用も、チームの管理者が設定で選べます（初期状態は対象外）。

AI の取り扱い（弊社独自の項目）

No.	項目	Dive の回答
55	AIの利用有無・目的	有 Google Cloud の Vertex AI（Gemini）を利用し、動画からの字幕生成・手順の自動分割・タイトル／概要／コツ／注意事項の自動生成・口調変換・翻訳を行います（日本・東京リージョンで処理）。読み上げには Google Cloud Text-to-Speech と Microsoft Azure AI Speech を利用しています。 AI 解析を使うかは、アップロードのたびに選べます。
56	モデル学習へのデータ利用	無 弊社はお客様のデータ（動画・手順書・入力テキスト等）を AI モデルの学習・再学習に使用しません（2026年11月12日施行の利用規約 第10条第7項で明記）。 Google Cloud の規約（サービス固有規約 第18条）でも、お客様の事前の許可なく AI の学習に使わないと定められています。
57	AI処理データの保持	入力データはリクエスト処理のためにのみ使用し、学習を目的として蓄積・保持することはありません。
58	AIガバナンス	有 AI の利用は利用規約とプライバシーポリシーで定めています。AI の生成物は正確さを保証せず、確認してご利用いただくことを利用規約で定めています（2026年11月12日施行の改定で明記）。 社内では、生成 AI に機密情報を入力しないことを規定で定めています。