Strap セキュリティホワイトペーパー

Ver 3.4　2024/7

このドキュメントについて

このドキュメントはStrapをご利用いただく上でのセキュリティについて、2024年7月22日時点の概要を簡易的に記したものです。

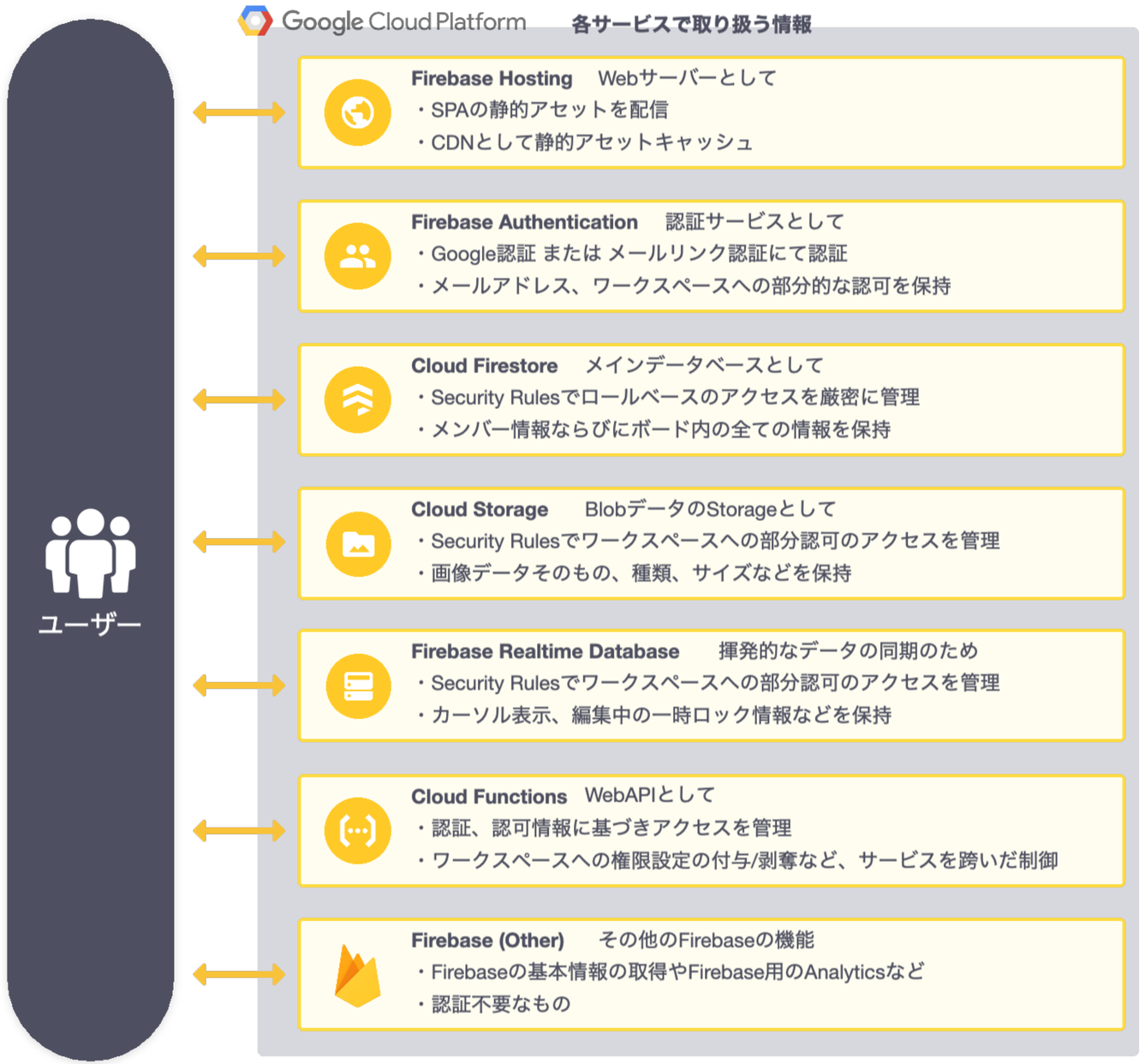
導入にあたり、より詳細な情報が必要な場合はお問い合わせください。

お問い合わせ先:　strap-support@goodpatch.com

その他の事項についてはStrapの利用規約およびプライバシーポリシーに定めるとおりとします。

システムセキュリティ／動作基盤

Strapの動作基盤は全て
マネージドサービスである
Google Cloud Platformの
Firebaseの各種サービスで
動作しており、右図のよう
な構成となっております。



システムセキュリティ／動作基盤

Firebaseのセキュリティについては以下をご確認ください。

> Firebase の全サービスは、 ISO 27001 や SOC 1 、 SOC 2 、 SOC 3 の評価プロセスを正常に完了しており、さらに一部のサービスは ISO 27017 や ISO 27018 の認証プロセスも完了しています。
>
> -- *Firebase のプライバシーとセキュリティ*

また Cloud Firestore / Cloud Storage / Firebase Realtime Database ではセキュリティルールを設定し、ワークスペース外部のユーザーからはデータを閲覧できないようにしています。

GCP全体のセキュリティについてはこちらのリンクをご参照ください。

https://cloud.google.com/security?hl=ja

システムセキュリティ／動作基盤

SLA(Service Level Agreement)について

Firebaseの各サービスでの稼働時間はSLAとしてGoogle側で設定されておりますが、StrapとしてのSLAは同一ではありません。現時点でStrapとしてのSLAは設定しておりません。稼働時間 の目安としては、GoogleのSLAにほぼ準拠する形になります。

- Service Level Agreement for Hosting and Realtime Database ｜ Firebase
- Cloud Storage for Firebase Service Level Agreement
- Firestore Service Level Agreement (SLA) ｜ Cloud Firestore
- Cloud Functions Service Level Agreement (SLA) ｜ Google Cloud

また、Google側の障害でない場合は、Strapチームはサービスを早急に復帰させるように尽力します。

システムセキュリティ／動作基盤

（参考）利用サービスとGoogleが設定しているSLAでの稼働率

- Firebase Hosting: 99.95%
- Firebase Realtime Database: 99.95%
- Firebase Authentication: 設定なし
- Cloud Firestore(Firestore Regional): 99.99%
- Cloud Functions for Firebase: 99.95%
- Cloud Storage for Firebase(Regional Storage class of Google Cloud Storage): 99.9%

主なリソースロケーションは日本国内のTokyo(asia-northeast1)となっており、ユーザーが作成するボード内のデータ（テキスト、シェイプ、画像など）は国内に保管されます。
（海外からのアクセスでは若干遅くなります。）

ただし、以下の情報については米国にも保管されます。

- 認証情報の一部、アクセスログのデータ（メールアドレス、IPアドレスなど）
- 認証時のユニークな情報（メールアドレス）
- 「Googleアカウントでログイン」を行なった場合にGoogleより提供を許可された情報（氏名・言語設定・プロフィール写真など）

システムセキュリティ／ログ記録

- Strapでは各種ログの取得を行なっています。
  - アクセスログ
  - アプリケーションのデータ更新ログ
  - ストレージへのファイルアップロードログ
  - ワークスペースへのアクセス認可ログ
  - 監査ログ

    など
- 取得したログは400日間保存されます。
- 各種ログについては 定期的に確認会を設け、確認をする体制を構築しております。
- 各種ログはGoogle Cloud Platform上のCloud Loggingで管理されており、適切なアクセス権の下で安全に保護されています。
- データ更新・閲覧等の操作ログ、およびワークスペースの認可ログを任意のタイミングで取得できる機能を有償オプションにて提供しております。

システムセキュリティ／クロックの同期

- Strapが稼働しているGoogle Cloud Platformでは、うるう秒への「ぼかし」も含めて適切に時刻の同期が行われています。
- サービス上の時刻は全てのユーザーに対して日本標準時(UTC+9)で表示しています。
- 保存するデータは世界標準時（UTC+0）で記録されており、ログを出力する際は日本標準時(UTC+9)に変換しております。

システムセキュリティ／データのバックアップ

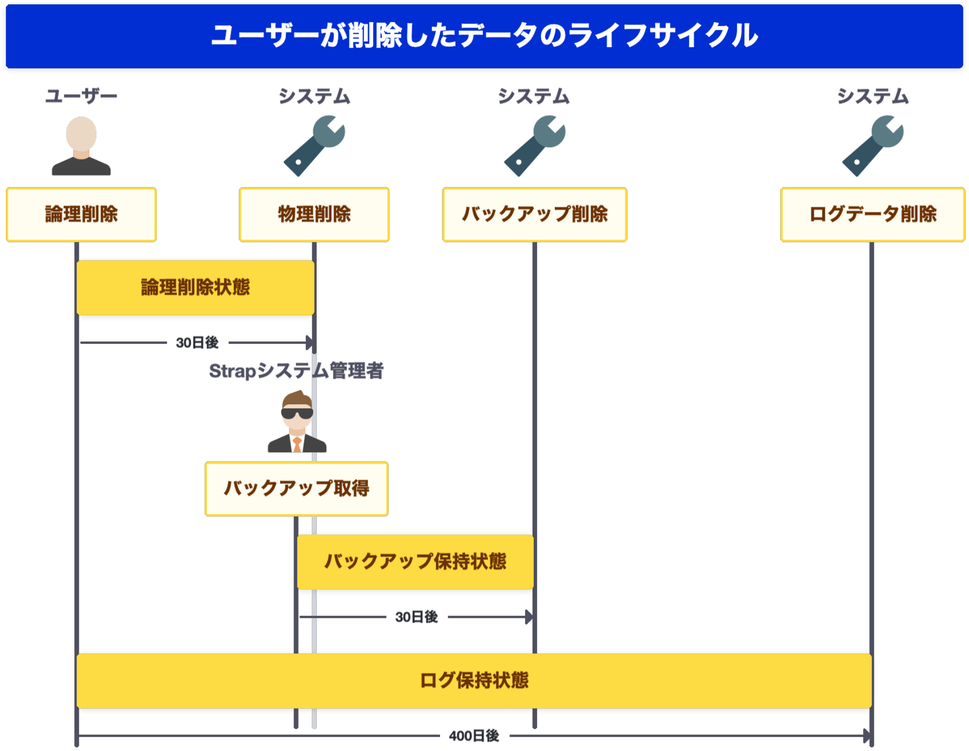
- メインのデータベースとなる Firestore については、毎日11:25頃から Multi-region でCloud Storage にバックアップを取得しており、地域的な冗長性を担保しています。
（Cloud Storageは月間可用性99.99%以上、年間耐久性99.999999999%）
- バックアップデータは暗号化され、30日間保持しています。
- リストアについても、実施方法がドキュメント化されています。
- 画像ファイルについては Cloud Storage に保管しておりますが、特にバックアップを取得しておりません。（年間耐久性99.999999999%のため）
- 上記のバックアップはシステム全体の保全等が目的であるため、ユーザーが手動でバックアップを取得することを推奨します。

PNGファイルとPPTXファイル形式で書き出しが利用可能です。操作方法はこちらのリンクをご確認ください。

- 画像の書き出し
- Microsoft Office PowerPoint ファイルの書き出し

システムセキュリティ／ユーザーが削除したデータ

- ユーザーが削除したデータは原則的にデータベース（Firestore）から全て論理削除となります。
- 論理削除後30日が経過するとデータベース（Firestore）から物理的に削除されます。
- 画像ファイルもデータベース(Firestore)からの物理削除時に同時に物理削除されます。
- 削除証明書の発行は現時点では承っておりません。
  - データの完全削除にかかる最長期間は、データが物理削除される直前にバックアップが取得された場合の約60日間です。
  - 画像ファイルはバックアップを取得していないため、データの完全削除にかかる期間は30日間です。
  - ログデータはどちらの場合も完全に削除されるまでにかかる期間は400日間です。

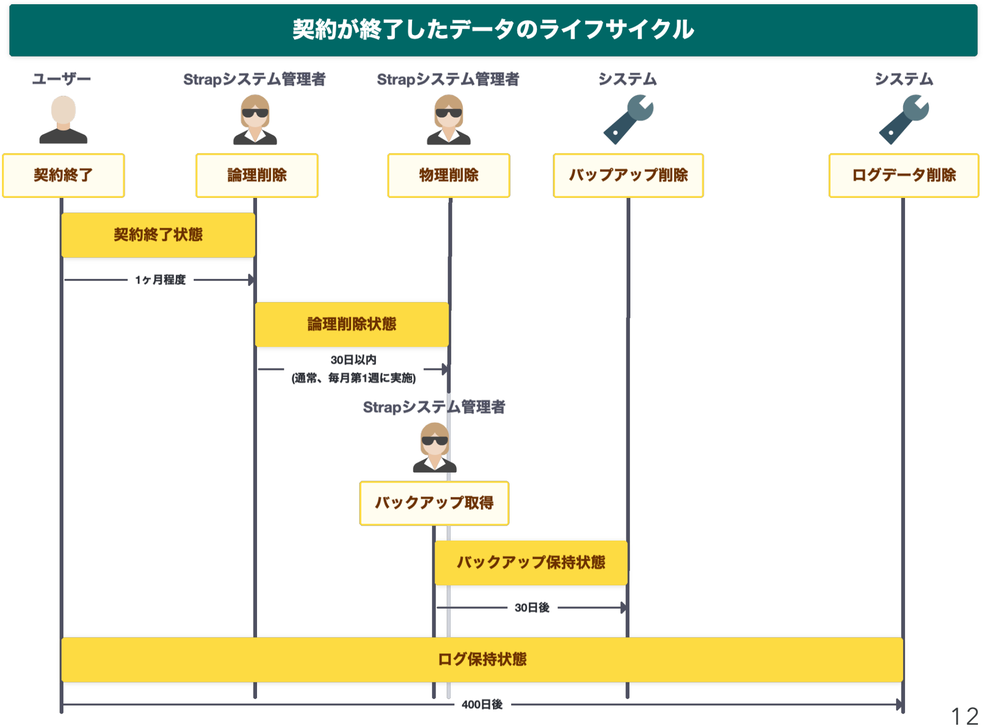


システムセキュリティ／契約終了後のデータの取り扱い

- 契約終了後１ヶ月程度の猶予期間を経て、特別な依頼がなければ、データベース上のワークスペースの論理削除およびメンバーに対する認可が削除されます。
- そこから数日〜１ヶ月以内に、論理削除されているワークスペースを対象にワークスペース内のデータと認証情報(ユーザID、メールアドレス)をデータベース上から物理削除します。

◦ データの完全削除にかかる最長期間は、データが物理削除される直前にバックアップが取得された場合の約90日間です。

◦ ログデータが完全に削除されるまでにかかる期間は400日間です。



システムセキュリティ／Firebase Authenticationの認証方式

現時点では、strap.appに対して以下の認証方式を有効にしております。

- Google認証
- メールリンク認証

パスワード認証には対応しておりません。

SAML認証など、その他の認証については、実装を検討しております。

システムセキュリティ／データの構成

Strapでは契約ごとにワークスペースが用意され、ユーザーが作成した情報はワークスペースごとに分離されます。ワークスペースの中を「スペース」という単位に分離し、スペースごとにメンバーの招待・権限管理を行えます。

以下のような構成になっており、論理的にデータは分離されます。

- ワークスペース
  - スペース
  - メンバー
  - ワークスペースの権限(Authorization)
- 認証(Authentication)
- スペース
  - ボード
    - エレメント（シェイプや画像など）
  - スペースメンバー
  - スペースの権限(Authorization)

上記の認証（前述の認証方法でのログイン）、また権限（ワークスペースの権限）に対しての管理は利用者側にて適切に行う必要があります。

システムセキュリティ／ゲスト

ワークスペースに所属していないメンバーを「ゲスト」として任意のスペースへ招待できます。

- ゲストとしてスペースに参加すると、ボードの作成や編集、閲覧ができます。
- ゲストは未参加スペースのデータにはアクセスできず、権限が付与されたスペース内のデータにのみアクセスできます。
- ゲストも個人スペースを利用することができます。
- ゲストの招待は、ワークスペースアドミンのみ可能です。
- ゲストとして招待されるユーザーも、契約プランのアカウントとしてカウントされます。

システムセキュリティ／ロール毎の操作権限

アドミン

- ワークスペース参加メンバーの招待・削除ができます。
- 各スペースメンバーの確認ができます。
- スペースやボードの作成・編集が行えます。

メンバー

- ワークスペースに新しくスペースを作成できます。
- ボードの追加・編集ができます。

ゲスト

- 特定のスペースに限定して、ボードの追加・編集ができます。

それぞれの権限でできることの詳細はこちらのリンクをご参照ください。

- ワークスペースの権限について
- スペース内の権限について

システムセキュリティ／IPアドレス制限機能

Strapのワークスペースに対して、特定のIPアドレスからのアクセスのみを許可する設定ができます。許可するIPアドレスの形式はIPv4およびIPv6、CIDR表記によるアドレス範囲指定に対応しています。
設定対応はシステムサポートにて行いますが、許可しているIPアドレスはワークスペース設定からご確認頂けます。

- IPアドレス制限機能の利用には別途オプション料金が発生します。
- ご利用を希望される際はお問い合わせ下さい。
  お問い合わせ先:　strap-support@goodpatch.com

システムセキュリティ／ボード外部公開機能

Strapで作成したボードを条件付きで外部に公開することができます。

- ワークススペースアドミンによる設定が必要です。（デフォルトはOFF）
- ボード公開が許可されているワークスペースでは各メンバーが各ボードに対して公開のON/OFF、アクセスキー発行が行えます。
- アクセスキーの更新は任意のタイミングで行うことができます。
- 公開されたボードにアクセスするためにはボードのURL・ボードのアクセスキーが必要です。
- アクセスキーを使用してボードにアクセスしたユーザには閲覧権限のみ付与され、編集を行うことはできません。また、外部公開されたボードにIPアドレス制限をかけることはできません。
- ワークスペースアドミンは外部公開されているボードを一覧で確認することができます。

システムセキュリティ／データの暗号化

保存されるデータの暗号化

Strapに保存されるデータ（データベース・バックアップ・ログを含む）に対してはGoogleによってデフォルトの暗号化が施されています。
詳細はこちらのリンクをご参照ください。

- デフォルトの保存データの暗号化

通信の暗号化

お客様の端末とシステム間のインターネット通信に対してはGoogleによって確立される接続に応じてデフォルトの保護が適用されます。たとえば、ユーザーと Google Front End（GFE）間の通信はTLSを使用して保護されます。
詳細はこちらのリンクをご参照ください。

- 転送データの暗号化

いずれの暗号化方式も総務省・経済産業省が公表した「CRYPTREC 暗号リスト」に準拠しています。

- CRYPTREC 暗号リスト

システムセキュリティ／開発

- 開発はチーム内で検討の上ドキュメント化したコーディングやスタイリングなどの各種ガイドラインに則り行なっています。
- StrapではGoogle Cloud Platformで利用している各サービスにおけるベストプラクティスを考慮した上でセキュアな設計・実装を行なっています。
- Strapチームでは本番環境へのマージ前に必ずコードレビューを行い、セキュリティの観点も含めたシステムの安全性を確認しています。
- アプリケーションを変更する場合は、本番環境と同等の検証環境で必ずテストを行い、動作に問題がないことを確認しています。

システムセキュリティ／情報のラベル付け

情報のラベル付けとして、データの名称を利用者自身で変更する機能を提供しています。

- ワークスペース名を変更する
- スペース名を変更する
- ボード名を変更する

システムセキュリティ／脆弱性診断

- Strapチームでは脆弱性に対するトリアージルールが定められており、脆弱性の影響度などを鑑みたトリアージ基準に従って対応します。
- Webアプリケーションについてはセキュリティに影響のある機能追加などのリリースごと、または年に１回以上の周期で第三者にソースコードを提出した上で脆弱性診断を行い、問題の検出および対応を行なっております。試験結果に対してはトリアージ基準に則り、随時対応を行います。
- 原則的に脆弱性診断での結果は開示しておりません。
- 開発元ベンダーのRSSやX（旧Twitter）、CERT、CISAなどの機関のRSS、GitHubのDependabot alertsなどから情報収集を行い、トリアージ基準に従って対応します。
- 利用しているサービス群の基盤部分についてはGoogleにより適切な検査が行われています。

システムセキュリティ／サーバーのセキュリティ対策

StrapはGoogle Cloud Platform上のマネージドサービスで動作しており、要塞化に対応した各種対策がされています。

- サービスやユーザーが信頼されていない状態を基準とするゼロ トラストセキュリティの設計
- Linux ユーザーの分離、言語・カーネルベースのサンドボックス化、ハードウェア仮想化などを用いたサービスの分離
- 不要なマシンの適切な削除および再割り当て
- 適切なマシンのみが本番環境ネットワーク上で通信できる認証情報にアクセス可能なことを保証する仕組み
- ウイルスの識別や内部トラフィックの監視による悪意のあるコンテンツを識別するマルウェア対策

詳細はこちらのリンクをご参照ください。

- Google インフラストラクチャのセキュリティ設計の概要

システムセキュリティ／各装置のセキュリティを保った処分

データが保存される装置はGoogle Cloud Platformのデータセンターにて適切に処理されます。

- Google のデータ削除パイプラインの全ステージを終えるまで安全に保存されます。
- Google のデータセンター内のすべてのストレージ機器に対し設置場所と状況、機器の取得、設置、廃棄、破壊などがバーコードと資産タグによって Google の資産データベース上でトラッキングされます。

詳しくはこちらのリンクをご参照ください。

- Google Cloud Platform におけるデータの削除

Strapのシステム管理者を含めた全ての従業員は貸与された端末を使用しており、雇用や契約の終了時にはアカウント削除、貸与端末の返却、データの初期化を速やかに行うよう文書化された手続きや機能に基づき対応しています。

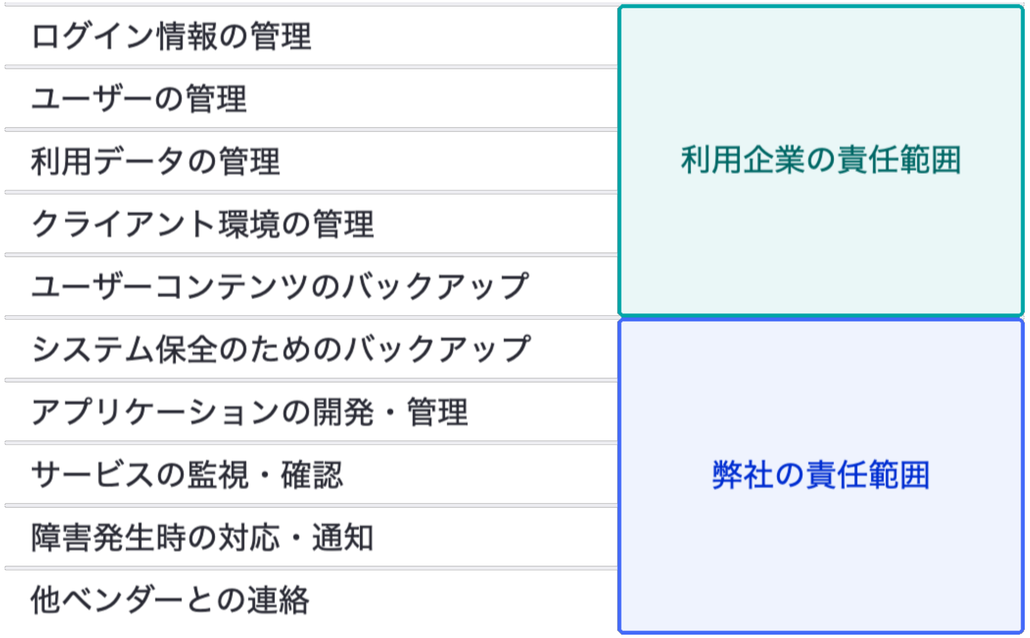
責任分界／事業者と利用者

原則として弊社の役割範囲としてはサーバー側での運用とアプリケーションの開発・管理です。

サービスの監視・確認や、障害発生時の対応・通知、他ベンダーとの連絡などが主な役割となります。

利用企業の責任範囲としましては、サービスの利用に伴うユーザーの管理、利用データの管理、クライアント環境の管理などが含まれます。

利用企業と弊社間における責任分界



責任分界／事業者とクラウドベンダー

StrapはGoogle Cloud Platform上のマネージドサービスで稼働しており、Googleとの責任分界は共有責任モデルとなっております。

Strapが利用している形態はPaaSとして分類され、Strapチームではコンテンツ、アクセスポリシー、利用方法、デプロイメント、Webアプリケーションのセキュリティを管理しています。

詳しくは「Google セキュリティの概要 - Google Cloud のセキュリティ プロダクトとサービス」をご確認ください。

弊社とGoogle Cloud Platform間における責任分界

組織セキュリティ／組織・従業員

- 組織として、セキュリティに関する各種規程を制定し、運用しております。
- 全従業員に対して、入社時にNDAの締結、情報セキュリティ・コンプライアンス上のルールのオリエンテーション、および遵守の誓約を交わしています。また、弊社就業規則には秘密保持義務を規定した条項が設けられております。
- 社内では定期的に意識向上のための教育・啓蒙が行われております。
  また、Strapの運用に関わるメンバーについては随時セキュリティに関わる事案についての共有や、定期的にシステム操作時の注意点などの再確認を行なっています。
- 当社は、個人情報保護マネジメントシステムの第三者認証であるプライバシーマークを取得しています。
- 当社は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度における ISO27001（ISMS認証）および ISO27017（ISMSクラウドセキュリティ認証）を取得しています。

組織セキュリティ／システム管理者

- Strapに関わるメンバーは、善良な管理者の注意をもってサービス運用するよう努めます。
- Strapが稼働しているGoogle Cloud Platformにおける本番環境へのアクセスは、適切な手順で選定された限られた数名の管理者（弊社正社員）のみがアクセス可能になっており、操作は監査ログに記録されます。
- 管理者アカウントは必要な職務に応じて権限が分離されており、適切な手順での選定と、管理職以上の承認を経て、手順書に応じて権限の与奪が行われています。
- Strapチームでは月次でシステム確認会を行っており、以下の事項を確認しています。
  - 各種権限の棚卸し
  - 監査ログなどの異常値確認
  - 各種メトリクスの状況確認

    など

組織セキュリティ／開発・保守端末

社内の全端末について、EDR・MDMが導入されており、以下のようなセキュリティ管理がされています。

- ディスクの暗号化
- 端末のパスワードポリシー制御
- ウイルス対策ソフトの導入
- ネットワーク監視
- USBなどの接続検知
- リモートワイプ、ロックが可能

システム管理者を含めた社内の全ての端末に導入しているウイルス対策ソフトでは、リアルタイムの防御とパターンファイルの自動更新を行っております。

組織セキュリティ／外部委託サービス

委託先サービスの選定についてはSOC2を取得していることを前提としており、セキュリティやコンプライアンスなどを確認した上で契約締結・更新をしています。

主に以下の外部サービスを適切な管理権限を整備し利用しております。

- PaaS/IaaSとして： Google Cloud Platform [Google Cloud Japan GK]
- エラー情報の集約として： Sentry [Functional Software, Inc.]
- メール送信SaaSとして： SendGrid [Twilio SendGrid]
- カスタマーサービスとして： Zendesk [株式会社Zendesk]
- 告知として：Announcekit [AnnounceKit LLC]
- AI機能（Beta版）として：OpenAI API [OpenAI, L.L.C.]　※デフォルトではOFFになっています。

運用／変更管理

- ユーザーに影響を及ぼす計画メンテナンスやセキュリティに関わる重大な仕様変更がある場合には、利用ユーザーへのメールや公式X(@strap_app)からの事前アナウンスを実施します。
- メンテナンスなどでサービスが停止している間は画面上にアナウンスを表示し、再開後には利用ユーザーへのメールや公式X(@strap_app)などでアナウンスを行います。
- 機能の変更後に画面リロードが必要な場合にはリロード用の通知を表示します。
- 緊急メンテナンスなどは事後連絡となることがあります。

運用／インシデント発生時の対応

- 重大なセキュリティインシデントが発生した場合は、問題の検知後6時間以内を目標に関連顧客への第一報を迅速に行います。
- 当該ワークスペースが関わるインシデントの場合は必要なログを提供します。また、アドミンメンバーにメールや電話で連絡いたします。
- 全体に影響がある障害に関しては公式X(@strap_app)にてアナウンスします。
- インシデントの報告はインシデント窓口（strap-security@goodpatch.com）にご連絡をお願いいたします。
- その他Strapに関するお問い合わせや平時のサポートに関してはサポート窓口（strap-support@goodpatch.com）にご連絡をお願いいたします。