

		最終更新：2026/01/09
カテゴリ	設問	回答
公開情報	情報セキュリティについて企業としての方針を定め、経営陣の承認を得ていますか。 また組織の内外へ周知していますか。	はい 組織外への周知に関しては一部プライバシーポリシーなどで出している。
第三者認証	情報セキュリティまたは個人情報保護について取得している第三者による認証や評価はありますか。	・ISO27001→GIJP-0981-IC ・プライバシーマーク→10823454
履歴	過去2年間にホームページ等で対外的に公表もしくは監督省庁や認証機関等へ報告するレベルのセキュリティインシデントがありましたか。	はい Jootoサービスにおいてはなし、 同社の運営する別サービス「PR TIMES」にて下記のセキュリティインシデントあり。  PR TIMES、不正アクセスによる情報漏えいの可能性に関するお詫びとご報告 <a href="https://prtimes.jp/main/html/rd/p/0000001531.000000112.html">https://prtimes.jp/main/html/rd/p/0000001531.000000112.html</a>
法律	契約や規約等における準拠法	日本法
法律	個人情報保護に関して対応しているもの	個人情報保護法
法律	政府、自治体又は公的機関から個人情報提供の命令又は要請等があった場合に実施すること、 している内容はありますか	・法的な根拠がある場合のみの対応 ・対応内容の記録
サービス利用者	サービスの対象者は法人のみであり、個人（個人事業主を含む）での利用は不可となっていますか。	・ISO27001→GIJP-0981-IC ・プライバシーマーク→10823454
サービスレベル	サービスレベルや責任範囲について実施していることはありますか。	・稼働目標を定めている ビジネスプラン向けにサービス品質保証（SLA）を提供。 <a href="https://www.jooto.com/sla/">https://www.jooto.com/sla/</a> 各月の99.9%以上の時間（計画的なメンテナンス時間などは除く）で 本サービスをご利用できるようにしています。  また、稼働率を提示し、万が一この品質保証を維持できなかった場合、 ご利用料金の一部を無料といたします。  ・稼働実績を開示している 毎月第5営業日までに前月の稼働率を下記ページにて提示いたします。 稼働率は外部監視システムから計測されたダウンタイムを元に計算されます。 <a href="https://www.jooto.com/sla/">https://www.jooto.com/sla/</a>  ・サービス利用者とサービス提供者間のコミュニケーション（連絡や報告）のルールや体制を定めている お知らせ及びSNSにて通知の上、重大なインシデントにおいては管理者ユーザーに対してメールにて通知
データ利用	預託データについて、定めていることはありますか。	目的外利用の禁止 プライバシーポリシー（ <a href="https://prtimes.co.jp/policy/">https://prtimes.co.jp/policy/</a> ）に準じて 機密情報の第三者開示や目的外利用はいたしません。  また、サービス利用者がサービス登録時に入力する個人情報及び請求先情報を指します。 サービス利用者等自身が作成したタスクまたはプロジェクト管理に利用される、サービス上の入力欄 に入力した情報については、利用規約第14条に記載のとおり、閲覧および開示等は原則いたしません。
データ利用	クラウドサービスで取得している情報はありますか。	当社のクラウドサービスでは、サービス提供および運用に必要な範囲で、以下の情報を取得しています。 ・利用者がサービス上に登録・入力した情報 ・サービス利用に伴い自動的に取得される情報（アクセス情報、操作履歴、エラーログ等） これらの情報は、サービス提供、運用管理、品質向上およびセキュリティ確保を目的として利用しており、目的外利用は行っていません。
データ利用	サービス利用者の個人情報に関する第三者提供をしていますか。	個人情報を第三者提供していない
データ利用	サービス利用者の個人情報をサービス提供以外の目的で利用していますか。	利用していない
データ利用	預託データを第三者提供していますか。	いいえ
データ利用	預託データをサービス提供以外の目的で利用していますか。	いいえ
データ利用	預託データの利用にあたり、契約や規約等にて利用目的として定めていることはありますか。	・サービスの提供 ・その他 お問合せ対応のため、会員登録、サービスの提供、サポート、連絡のため、 ご利用料金請求のため、マーケティングデータの調査、統計、分析のため、 新サービス、セミナー情報、メルマガの提供のため、商談、打ち合わせ、契約の履行のため
データ利用	Cookieや位置情報、IPアドレス等のオンライン識別子の利用について、対応していることはありますか。	当社のクラウドサービスでは、サービスの提供およびセキュリティ確保を目的として、以下のオンライン識別子を利用しています。 IPアドレス： アクセス管理、不正アクセス検知、障害対応等のために利用しています。 Cookie： ログイン状態の維持や利便性向上のために利用しています。 これらの情報は、サービス提供および運用管理に必要な範囲で利用しており、目的外利用は行っていません。
データ利用	外部委託先が預託データを取り扱うことはありますか。	はい、外部委託先が業務上の目的で預託データを取り扱うことはなく、クラウド基盤（Amazon Web Services）におけるデータ保管・処理のみを委託しています。
データ利用	外部サービスの利用や外部委託等により預託データが他国に保管されることはありますか。	いいえ
データ利用	預託データが他国からアクセスされることはありますか。 （外部サービスの利用や外部委託等によるアクセスを含む）	いいえ
データ利用	日本国外に所在する第三者に対して委託のため個人情報を提供する場合、 当該第三者との間で合意していることはありますか。	日本国外へ提供していない
データ利用	外部委託先や外部サービスに個人情報が委託されることはありますか。 委託がある場合は委託先を公開していますか。	個人情報がAWS上で保管・処理されるため委託がありますが、第三者提供は行っていません。
データの所在地	サービス提供のため利用しているデータセンターのリージョンやエリア（バックアップ用途を含む）。	日本

情報セキュリティ確保のための組織体制	情報セキュリティの維持や向上、監督、それら活動全般を統制する管理上の枠組みを確立するために実施していることはありますか。	<ul style="list-style-type: none"> <li>・情報セキュリティ管理の責任者を定め、職務範囲や権限、責任について定めている</li> <li>・情報セキュリティ管理に関する関係部署や業務、機能を明らかにしている</li> <li>・情報セキュリティ体制について、通常時だけでなく有事を想定した役割や責任を定めている</li> <li>・自社で対応する箇所、外部に委託する箇所を適切に切り分け、役割と責任を明確にしている</li> </ul>
情報セキュリティ確保のための組織体制	承認されていないもしくは意図しない変更や不正利用のリスクを低減するため、組織の役割と責任に応じて情報資産へのアクセスや閲覧、修正等の権限を分離していますか。	分離しており、定期的に見直しています。
従業員に対するセキュリティ対策	従業員に対するセキュリティ対策として実施していることはありますか。	情報セキュリティおよび重要情報の取扱いに関する意識向上のため、定期的に教育を実施している 2025年2月：全社員向けセキュリティ教育およびテスト
従業員に対するセキュリティ対策	従業員および契約相手と秘密保持に関する契約を締結をしていますか。	はい
従業員に対するセキュリティ対策	従業員および契約相手との契約が終了または変更となった場合、アクセス権の変更や削除、貸与資産の返却等を実施していますか。	文書化された手続きや機能に基づき実施している
情報資産管理	情報資産の管理プロセスおよび重要度の基準を定め、管理プロセスに従い情報資産の洗い出しと評価を行い、資産一覧を作成していますか。	文書化された手続きや機能に基づき実施している
情報資産管理	契約や規約等により、サービス利用終了時のデータの取り扱いが明確になっていますか。	いいえ
情報資産管理	サービス利用終了時またはサービス利用者からの指示があった場合、預託データやサービス利用者が作成したデータを返却したり削除できますか。	削除証明書発行や削除連絡は可能、削除までは退会処理完了より30日後
情報資産管理	情報資産を消去または廃棄する場合は復旧できない状態にしていますか。	文書化された手続きや機能に基づき実施している
情報資産管理	クラウドサービスの開発、保守および運用において、私用端末を利用していますか。	利用していない
情報資産管理	持ち運び可能な外部記憶媒体を利用していますか。	いいえ
情報資産管理	持ち運び可能な外部記憶媒体の利用は禁止されていますか。	禁止されている
アクセス制御	クラウドサービスの開発、保守および運用において利用するソフトウェア、ハードウェア、ネットワーク上で取り扱われるデータについて、アクセス制御の方針やルールを定めていますか。	文書化された手続きや機能に基づき実施している
アクセス制御	従業員やシステム管理者が預託データへアクセスすることを原則として禁止とし、アクセスする場合は、事前に承認を得たものに限定していますか。	文書化された手続きや機能に基づき実施している
アクセス制御	関連するセキュリティ対策不正アクセスや情報漏えいを防ぐため、預託データへのアクセス管理を原則禁止とし、アクセスする場合は事前に承認を必要としますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービス内のコンポーネントやデータへのアクセスを、業務上必要な従業員にのみ限定していますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービスの開発、保守および運用において、特権アカウントを割当および利用する際は、承認を必須とし必要最小限に制限していますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービスの開発、保守および運用において、特権アカウントを用いた情報資産に対するネットワークアクセスを記録し、適切な利用かどうかをモニタリングしていますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービスのコンポーネントにおいて、管理者権限や特権的ユーティリティのアクセス制限として実施していることはありますか。	<ul style="list-style-type: none"> <li>・原則、管理者権限でのログインおよびクラウドサービスへのアクセスは実施していない</li> <li>・Webサーバやアプリケーションサーバのプロセスを管理者権限以外で起動している</li> <li>・サービスやデーモン、プロトコルは必要なもののみ設定および起動をしており、不要なものは起動できないようにしている</li> </ul>
アクセス制御	プログラムソースや仕様書等のクラウドサービスに関連する情報へアクセスできる人を業務の必要性や役割に応じて資産単位で限定していますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービスのリリースもしくはローンチ作業ができる人を限定していますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービスの開発、保守および運用において、不要または一定期間使用していないアカウントを無効化あるいは削除していますか。	文書化された手続きや機能に基づき実施している
アクセス制御	クラウドサービスの開発、保守および運用において、共有アカウントを利用していますか。	いいえ
アクセス制御	共有アカウントが利用禁止であることを明文化していますか。もしくは利用する場合のルールを定めていますか。	いいえ
アクセス制御	サービス利用者のアカウントについて、実施していることおよび実施可能なことはありますか。	<ul style="list-style-type: none"> <li>・IDは各個人に発行し、利用者を特定できる仕様としている</li> <li>・接続元IPアドレスによる接続経路を制限できる エンタープライズプランにて、IPアドレスを指定して所有組織アカウントへのアクセス制限可能</li> <li>・ログイン後一定時間以内の操作がない場合に強制的にログアウトさせるため、セッションの有効期限を設けている SSO経由ログインの場合は24時間、通常アイパスによる場合は2週間</li> <li>・パスワードに最小の文字数を設定している 8文字以上</li> <li>・パスワードに英数字だけでなく、記号も使用可能である</li> <li>・パスワードはハッシュ化したものを保存している</li> <li>・パスワードは利用者自身が登録する仕様となっている</li> <li>・パスワードの再発行を行う際は本人しか知りえない情報等で本人確認をしている</li> <li>・パスワード変更URLを登録メールアドレスに送信して認証。</li> </ul>
アクセス制御	貴社従業員が利用するサービス運営のための機能や管理画面等がありますか。	はい
アクセス制御	貴社従業員が利用するサービス運営のためのアカウントについて、実施していることはありますか。	<ul style="list-style-type: none"> <li>・接続元IPアドレスによる接続経路を制限している</li> <li>・パスワードに最小の文字数を設定している 非開示</li> <li>・パスワードに英数字だけでなく、記号も使用可能である</li> <li>・脆弱なパスワードの使用を制限している</li> <li>・パスワードはハッシュ化したものを保存している</li> </ul>
アクセス制御	クラウドサービスの開発、保守および運用において利用するインフラやデータベース、IaaS等のアカウントについて、実施していることはありますか。	<ul style="list-style-type: none"> <li>・IDは各個人に発行し、利用者を特定できる仕様としている</li> <li>・接続元IPアドレスによる接続経路を制限している</li> <li>・デバイス認証やMACアドレス制限等によりデバイスを制限している</li> <li>・パスワードに英数字だけでなく、記号も使用可能である</li> <li>・パスワードは利用者自身が登録する仕様となっている</li> <li>・パスワードの再発行を行う際は本人しか知りえない情報等で本人確認をしている</li> </ul>
暗号	情報資産を保護するため、重要度や用途に応じて暗号化方針やルールを定めていますか。	定めていて、定期的に見直している
暗号	通信に関する暗号化について実施していることはありますか。	<ul style="list-style-type: none"> <li>・サービスへのアクセス時に通信を暗号化している</li> <li>・有効期限が切れていない、信頼できる認証局が発行したサーバ証明書を利用している</li> </ul>
暗号	預託データに関する暗号化について、実施していることはありますか。	<ul style="list-style-type: none"> <li>・データベースやファイルを暗号化している</li> <li>・バックアップデータを暗号化している</li> </ul>
暗号	暗号化するためのキーやパスワードは、必要ときに限られたシステム管理者のみアクセスできるような制御をしていますか。	実施しているものの、文書化された手続きや機能は存在しない
物理及び環境的セキュリティ	データセンターの利用形態について、該当するものはありますか。	外部クラウド事業者のデータセンターを利用
物理及び環境的セキュリティ	利用しているIaaS/PaaS等の選定にあたり、データセンターの入退室管理や自然災害への対策等の物理的なセキュリティ対策を確認していますか。	はい

運用のセキュリティ	クラウドサービスの機能や仕様、サービス提供の条件、利用方法、運用方法等のサービス運営に必要な情報を定めて文書化していますか。	文書化していて、定期的に見直ししている
運用のセキュリティ	構成管理や変更管理により、システム構成やネットワーク構成、変更状況を可視化していますか。	はい
運用のセキュリティ	サービス利用者への通知について、実施していることはありますか。（実施予定のものを含む）。	<ul style="list-style-type: none"> <li>・サービスを提供する時間帯もしくはメンテナンス時間を定め、通知もしくは開示している</li> <li>・サービスは24時間稼働とし、定期メンテナンスはなく、不定期なメンテナンスは約2週間前に通知を実施</li> <li>・緊急もしくはは不定期なメンテナンスが必要な場合について、事前に通知している</li> <li>・全体メンテナンスが行われる場合には約2週間前にJootoのサイトにお知らせ掲載及びSNSにて通知する。</li> <li>・緊急時については、実施確定後速やかに通知</li> <li>・サービスの大きな変更や終了について、事前に通知している</li> <li>・利用規約準じ、3ヶ月以上前にサービス内お知らせにて掲載、SNS通知、組織アカウント管理者へメール通知</li> <li>・サービス提供に関わる障害やパフォーマンス低下等が発生した場合について、速報や追加報告（復旧予測時刻等）を実施している</li> <li>・検知後速やかにサービス内お知らせ掲載及びSNSにて通知（目標時間30分）</li> <li>・セキュリティインシデントが発生した場合は速やかに通知している</li> <li>・目標時間はセキュリティインシデント内容によるが、原則検知後速やかに</li> </ul>
運用のセキュリティ	現状だけでなく将来必要となるリソースを考慮し、キャパシティプランニングを実施していますか。	はい
運用のセキュリティ	障害や災害からあらかじめ定められた目標時間やポイントで復旧できるよう、クラウドサービスのデータやアプリケーション、環境構成情報のバックアップを取得していますか。	<p>はい</p> <p>1日1度データベースをフルバックアップし、30世代保存</p>
運用のセキュリティ	バックアップから適切に復旧可能とするために実施していることはありますか。	<ul style="list-style-type: none"> <li>・バックアップが取得できていることを定期的に確認している</li> <li>・バックアップデータをクラウドサービスが設置してある場所とは物理的に離れた場所で保管している</li> </ul>
運用のセキュリティ	関連法令や規制、契約上の要求事項を満たすことができるよう、データやログの保管期間と管理要件を定め、その定めに従って管理していますか。	実施しているものの、文書化された手続きや機能は存在しない ログの箇所にもより保存期間が異なる
運用のセキュリティ	取得しているログはありますか。	<p>以下のログを最低1年以上保管しています</p> <ul style="list-style-type: none"> <li>・例外処理や誤操作によるエラー、システム障害、セキュリティインシデントに関するイベントログ</li> <li>・サービス利用者の認証ログやアクセスログ、操作ログ</li> <li>・システム管理者の認証ログやアクセスログ、操作ログ</li> </ul>
運用のセキュリティ	取得したログが不正アクセスおよび改ざんされないよう、アクセス制御や暗号化等により保護していますか。	実施しているものの、文書化された手続きや機能は存在しない
運用のセキュリティ	各コンポーネントで統一された時刻（タイムゾーン）を管理し、NTP等の仕組みによりクラウドサービスの時刻を同期させていますか。	はい
運用のセキュリティ	クラウドサービスの開発、保守および運用において利用する端末にはウイルス対策ソフトを導入し、リアルタイムスキャンや定期的なウイルススキャン、およびパターンファイルの定期的な更新が行われていますか。	はい
運用のセキュリティ	クラウドサービスの開発、保守および運用において利用する端末へインストールするソフトウェアについて、禁止したソフトウェアが利用されないよう制限やモニタリングをしていますか。	文書化された手続きや機能に基づき実施している
運用のセキュリティ	脆弱性を管理するための方針を定め、その方針に従って脆弱性に対処していますか。	文書化された手続きや機能に基づき実施している
運用のセキュリティ	脆弱性診断やペネトレーションテストについて、実施していることはありますか。	<p>ツールと手動を組み合わせたプラットフォーム診断（ネットワーク、インフラ等への詳細診断）</p> <p>定期的に実施（最終実施：2024年1月）</p>
運用のセキュリティ	OSやアプリケーション、ミドルウェア、ファームウェア等すべてのソフトウェアの脆弱性およびEOSLに関する情報を定期的に収集し、適宜パッチによる更新やソフトウェアのアップデートを行っていますか。	OS、アプリケーション、ミドルウェア等のソフトウェアについて、脆弱性およびEOSL（サポート終了）情報を定期的に収集し、必要に応じてパッチ適用やソフトウェアアップデートを実施しています。
運用のセキュリティ	クラウドサービスを構成する本番サーバに対して行なっているウイルス対策はありますか。	当社では、クラウドサービスを構成する本番サーバに対し、AWSのセキュリティ機能およびOSレベルのセキュリティ対策を活用し、マルウェアや不正プログラムの侵入防止を含むウイルス対策を実施しています。
監視	セキュリティインシデントやシステム障害を検知するために実施していることはありますか。	<ul style="list-style-type: none"> <li>・クラウドサービスおよびネットワークに対するパフォーマンス監視</li> <li>・クラウドサービスの死活や障害監視、外形監視（運用監視）</li> <li>・社内ルール違反等の挙動監視</li> <li>・操作ログ</li> <li>・内部および外部からの不正アクセスや不正利用の監視</li> <li>・ログ監視</li> <li>・サイバー攻撃の兆候監視</li> <li>・アクセスログ監視</li> <li>・不正なバケットに関する監視</li> <li>・不正なネットワークアクセスやリモートアクセスの監視</li> </ul>
監視	セキュリティインシデントを予防、もしくは被害を最小化するため、ログを効率的に分析する仕組みを導入していますか。	はい
ネットワークのセキュリティ	サーバへのリモートアクセスは制限していますか。実施していることはありますか。	特定の部署や人からのアクセスに制限している
ネットワークのセキュリティ	外部および内部からの不正アクセスを防止するためにファイアウォールを設置していますか（WAFは除く）。	設置していて、定期的に設定を見直ししている awsのSecurityGroupを利用しています。
ネットワークのセキュリティ	不正なバケットを自動的に発見または遮断するためにIPSやIDSを導入していますか。	導入していて、定期的に設定を見直ししている Amazon GuardDutyにて監視
ネットワークのセキュリティ	Webアプリケーションの脆弱性を悪用した攻撃等を防止するため、WAFを導入していますか。	導入していて、定期的に設定を見直ししている AWS WAFを導入
ネットワークのセキュリティ	DDoS等のサービスの維持運用を妨害する攻撃への対策をしていますか。	はい ログ監視、キャッシュ機能など
ネットワークのセキュリティ	各サーバの用途に応じた論理的分離により境界を保護していますか。実施していることはありますか。	<ul style="list-style-type: none"> <li>・DBサーバがWebサーバと分離された構成になっており、WebサーバとDBサーバ間の通信経路が必要最低限になるようアクセスを制御している</li> <li>・DBサーバは外部から直接アクセスできないようにアクセスを制御している</li> </ul>

システムの取得、開発及び保守	クラウドサービスの開発、保守および運用において、セキュリティ対策の要求事項を明確にしていますか。	明確にしてい、定期的に見直している
システムの取得、開発及び保守	クラウドサービスの開発、保守および運用の各工程において、セキュリティや品質を確保するために実施していることはありますか。	<ul style="list-style-type: none"> <li>・機要件や非機要件、セキュリティ要件のレビュー</li> <li>・各工程における承認プロセスの整備</li> <li>・データ修正の承認プロセス、作業手順の整備</li> </ul>
システムの取得、開発及び保守	クラウドサービスの開発工程においてセキュアコーディングを行っていますか。	セキュアコーディングを実施してい、レビューもしている
システムの取得、開発及び保守	クラウドサービスの開発、保守および運用において、データの漏えいを防止するために実施していることはありますか。	<ul style="list-style-type: none"> <li>・開発環境と本番環境の分離</li> <li>・本番データについて、本番環境以外での利用禁止</li> </ul>
システムの取得、開発及び保守	アプリケーションを変更する場合は、事前にテストし変更後の影響や不具合がないか確認していますか。実施していることはありますか。	<ul style="list-style-type: none"> <li>・機要件のテスト</li> <li>・非機要件のテスト</li> </ul>
システムの取得、開発及び保守	アプリケーションを変更する場合は、事前に本番環境と同等の開発環境でテストを実施していますか。	文書化された手続きや機能に基づき実施している
システムの取得、開発及び保守	クラウドサービスのインフラやネットワークを変更する場合に実施していることはありますか。	<ul style="list-style-type: none"> <li>・機要件のテスト</li> <li>・非機要件のテスト</li> </ul>
外部委託先管理	クラウドサービスの開発、保守および運用において、外部委託先を利用していますか。	はい 機能開発や運用などの一部業務。
外部委託先管理	外部委託先の選定および管理について、方針や基準を定めていますか。	定めていて、定期的に見直している
外部委託先管理	外部委託先に対する要求事項として合意し、文書化していることはありますか。	<ul style="list-style-type: none"> <li>・セキュリティ対策 自社と同水準</li> <li>・セキュリティインシデント発生時の報告や対処</li> <li>・情報の消去</li> <li>・関連法令の遵守</li> <li>・監査権</li> <li>・機要件や非機要件</li> <li>・検収基準</li> </ul>
外部委託先管理	外部委託先との合意内容が履行されているか定期的に確認してますか。	文書化された手続きや機能に基づき実施しているものの、定期的に見直していない 契約更新時など
外部委託先管理	外部委託先を定期的に評価していますか。	文書化された手続きや機能に基づき実施してい、定期的に見直している 通常は3ヶ月ごとの更新
外部委託先管理	外部サービスやツールを利用する場合、セキュリティ水準を確認していますか。	実施しているものの、文書化された手続きや機能は存在しない 利用規約、プライバシーポリシー等が当社の規約等と照らして問題がないか等
インシデント管理	セキュリティインシデントやシステム障害に対して迅速かつ効果的に対応するために役割および責任を明確にしていますか。	明確にしてい、定期的に見直している
インシデント管理	セキュリティインシデントやシステム障害へ対応するための体制や手順を確立していますか。	確立してい、定期的に見直している
インシデント管理	セキュリティインシデント対応や訓練、他社事例から学んだ教訓をセキュリティインシデント対応手順に取り入れて改善につなげていますか。	はい インシデントが発生した際には改善策を盛り込んだドキュメントを残しています。
事業継続マネジメントにおける情報セキュリティ	地震や火災等の災害または大規模なシステム障害に備えてリカバリ計画およびコンティンジェンシープランを策定し、定期的な訓練または見直しで実現性を確認していますか。	策定してい、定期的に見直しもしている ただし、AWSの利用リージョン（東京）の全てのDCが稼働停止する障害以上は想定されていない。
事業継続マネジメントにおける情報セキュリティ	地震や火災等の災害または大規模なシステム障害に備えて複数の拠点や地域にまたがって冗長化されたシステム構成となっていますか。	はい AWSにて物理的に離れた基地局にデータ保存
法令遵守	サービス提供者およびクラウドサービスが満たすべき関連法令や規制、契約上の要求事項を整理し、これらを満たすための取り組みを継続的に実施していますか。	はい
法令遵守	個人情報保護に関連する法令や規制上の要求に従って対応していますか。	はい
法令遵守	プライバシーポリシーを定め、サービス利用者に開示していますか。	はい <a href="https://prtimes.co.jp/policy/">https://prtimes.co.jp/policy/</a>
法令遵守	セキュリティ対策が正しく実装され意図したとおり運用されているか、関連法令や規制、契約上の要求事項を満たしているかを独立した評価部門により定期的に評価していますか。実施していることはありますか。	<ul style="list-style-type: none"> <li>・内部監査もしくは内部評価 ISO27001に準じて毎年実施 最終実施2025年7月</li> <li>・外部監査もしくは外部評価 ISO27001に準じて毎年実施 最終実施2024年12月</li> </ul>
アカウント	サービス利用者が組織内のアカウントを削除もしくは利用停止にすることができますか。	はい 組織アカウントにて管理者及びアカウント管理者権限のユーザーが、サービスページ内の組織のユーザー一覧ページにて組織アカウントの招待および削除が可能
アカウント	サービス利用者が組織内のアカウントのログイン履歴や操作ログを確認できますか。	操作ログについては、当該プロジェクトにアクセス権限を有するユーザーがプロジェクト内で確認可能ですが、アクセスログ等のシステムログについては原則として利用者への提供は行いません。
アカウント	サービス利用者が組織内のアカウント一覧を出力できますか。	いいえ 組織のメンバー以上の権限にてサービス内で一覧を確認は可能ですが、CSVによる出力は不可
ファイルアップロード	ファイルをアップロードする機能がある場合、そのファイルに対して実施していることはありますか。	<ul style="list-style-type: none"> <li>・暗号化</li> <li>・バックアップ</li> </ul>
独自ドメイン	サービス利用者がアクセスする際に利用するURLは、利用企業毎に異なりますか。 (利用企業の独自ドメインを使用可能な場合やaaa.example.comのようにサブドメインのみ異なる場合も含む)	はい 組織アカウントごとにURLが異なります
機能制限	他サービスとの連携する機能がある場合、その機能の使用可否はサービス利用者の管理者権限で設定できますか。	いいえ 一部機能についてはプロジェクトごとにプロジェクトマネージャー権限のみに制限可能だが、全てが外部連携を管理者権限で設定は不可
機能制限	預託データを公開または外部ユーザへ共有する機能がある場合、それらの機能の使用可否はサービス利用者の管理者権限で設定できますか。	該当する機能はない
API	他サービスとAPI連携していますか。該当するものはありますか。	他サービスとはAPI連携していないが、OpenAPIを公開しており、API認証及び連携は組織の管理者アカウントにて管理可能。
スマートフォンアプリ	スマホアプリが提供されている場合、スマホ経由でのデータ漏えい対策を実施していますか (スマホアプリから利用できる機能を制限している、管理者権限でスマホアプリの利用可否を設定できる等)	いいえ アプリ上での制限はないため、シングルサインオン連携を行い別途制御行う等の実装が必要
電子メール	サービス利用者が電子メールを送信する機能はありますか。	いいえ