

「root ipクラウド」クラウドサービスレベルのチェックリスト							2026/02/26改定 株式会社rootip	
経済産業省 「クラウドコンピューティングと日本の競争力に関する研究会」 報告書 クラウドサービスレベルのチェックリスト より								
No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	root ip設定	左記備考
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(計画停止/定期保守を除く)	計画停止時間は提供者が個々に設定	24時間365日 (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	30日前にメール/ホームページで通知		有 通常、停止の前週に当社サービス画面上部のバナーで告知。	セキュリティパッチ適用など緊急の停止を除きます
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	15ヶ月前にメール/ホームページで通知		有 1年以上前にメール／ホームページで通知(利用規約に明記)	可能であればより早い告知を行います。 なお、エクスポートはお客様自身で実施頂けます。
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	第三者へのプログラムの預託を実施	サービス提供企業が倒産等した場合にもサービスを継続できるように、プログラムを第三者に預託していることが望ましい	無 プログラムの預託は実施しておりません。	
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(%)	99.9%以上(基幹業務) 99%以上(基幹業務以外)	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討※「計画サービス時間」は、サービス提供時間と計画停止時間の両方を含む。	99%以上	
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	遠隔地のバックアップ用データセンターで保管している日次バックアップデータと予備システム切替時間は半日～1日	データセンタ構成、復旧までのプロセス/時間、費用負担についても明示されていることが望ましい また、適用する業務の重要性に応じた「ディザスタリカバリ」のレベルにより設定内容は変わる	有 物理的に離れたデータセンター(東京エリア3箇所, 大阪エリア3箇所)にデータバックアップを保存。 切り替え時間は障害レベル次第で、即時～1日程度	
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	バックアップデータの取得が可能なホームページを用意		有 バックアップから別環境にサービスを再構築して提供	
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)	CSVあるいはExcelファイル	データ保護の観点からは、クラウド・コンピューティング・サービス提供者だけでなく利用者側でもバックアップを実施しておくことが望ましい。 また、システムの信頼性、サービス継続性の観点からは、サービス提供者は十分に対策を行っていると考えられるが、トラブル時に備えて、預託データのダウンロードが可能かどうかを確認することが望ましい	有 本運用と基本的に同じサービス	オプションとして、案件情報及び添付ファイルを静的ファイルとして作成しお客様環境に定期的に保存いただくことも可能です
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	年2回の定期バージョンアップを実施	頻度、事前通知方法、履歴管理/公開、利用者の負担についても明示されていることが望ましい	クラウドサービスであり明確なバージョンおよびその更新の概念はありません(※)。適宜機能追加、バグ修正が行われます。停止を伴わないアップデートも適宜行われます。 お客様運用に影響する可能性がある場合は事前にご連絡を行います。	※内部的なソフトウェアの履歴管理は行われています
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	1時間以内(基幹業務)12時間以内(上記以外)	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討	0.33hr (実績)	障害発生時に自動で予備に切り替わる等、極力停止を避ける構成となっております。 ここ数年において障害による停止実績は1回のみで、上記実績はその値です。 休日メンテナンス時に意図せず一時的に接続できなくなってしまったもので、対策も行っております。
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	3時間後3日後	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討	障害の種類によるため明記できません。 可能な限り早い復旧を行います。	

「root ipクラウド」クラウドサービスレベルのチェックリスト

2026/02/26改定 株式会社rootip

経済産業省 「クラウドコンピューティングと日本の競争力に関する研究会」報告書 クラウドサービスレベルのチェックリスト より

No. 種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	root ip設定	左記備考
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	1回以内(基幹業務)3回以内(上記以外)	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討	ここ数年において障害による停止実績は1回のみ	
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	ハードウェア/ネットワーク/パフォーマンス監視	詳細な監視項目は提供者が個々に設定	有 CPU負荷・メモリ使用量等を別システムにてチェックを行っております。	
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	指定された緊急連絡先にメール/電話で連絡し、併せてホームページで通知	初期対応後の経過報告の方法・タイミングについても明示されていることが望ましい	有 指定された連絡先にメールで連絡し、併せてホームページで通知	
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	15分以内(基幹業務)2時間以内(上記以外)	営業時間内/外で異なる設定を行う場合がある	特に定めておりません。可能な限り早急にご連絡いたします。	
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)	1分以内(基幹業務)15分(上記以外)	営業時間内/外で異なる設定を行う場合がある	1分以内	
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	月に一度ホームページ上で公開	報告内容/タイミング/方法は提供者が個々に設定	重大障害を除き、特に報告は行っていません。 修正/アップデート項目などはサービス画面から確認できます。	
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	セキュリティ(不正アクセス)ログ/バックアップ取得結果ログを利用者の要望に応じて提供	提供内容/方法は提供者が個々に設定	有 ユーザーのログイン履歴、案件閲覧履歴、案件編集履歴をシステムからご覧頂けます。提供期間は上限を定めておりませんが、少なくとも1年以上は確認可能といたします。 その他の内部的なログについては、SaaSシステムのため他のお客様と共通になっており、基本的にご提供できません。	インシデント発生等の場合は弊社側での解析、あるいはお客様分を抽出して提供などご相談させていただければと存じます。
19 性能	応答時間	処理の応答時間	時間(秒)	データセンタ内の平均応答時間3秒以内	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討	目標は定義しておりませんが、現状において、ほとんどの場合に3秒以内にレスポンスを返しています。	例外としてアップロード/ダウンロード処理や件数の多いエクスポート、ワードなどの差し込み、また特許庁API等外部サービス連携機能など、処理内容によっては3秒を超える可能性があります
20	遅延	処理の応答時間の遅延継続時間	時間(分)	データセンタ内の応答時間が3秒以上となる遅延の継続時間が1時間以内	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討	上記と同じ	
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)	4時間以下	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討	お客様操作に影響するバッチ処理は現状行っておりません	
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	利用画面上の項目配置変更や新規項目の追加が設定画面より可能		有 マスタの追加編集機能や、各データに追加的な備考欄を備えています。	一部機能についてはカスタマイズも請け負っておりますが、可否等はこちらでご相談させていただきます
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	API(プログラム機能を外部から利用するための手続き)を公開	APIがインターネットの標準技術で構成され、仕様が公開されており、APIの利用期限や将来の変更可能性が明記されていることが望ましい	有 APIを提供しています。 内容によってはCSVエクスポート/インポート機能での連携もご利用いただけます。	
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)	50ユーザ(保証型)	同時接続の条件(保証型かベストエフォート(最善努力)型か)、最大接続時の性能について明示されていることが望ましい	無 同時接続数の制限はありません。	1ユーザーアカウントでの同時複数ログインはできません。
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	1TB40,000ページビュー		包袋ファイル(添付ファイル)容量 1TB以上は別料金となります。 その他の制限は特にありません。	大量のロボットアクセスを除く
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(電話)	受付方法(電話/メール)や営業時間外の対応は対象業務の重大性およびサービス内容/特性/品質に応じて状況が異なる	日本時間平日の 9:00～17:30 までとし、当社が定める定休日を 除きます	

「root ipクラウド」クラウドサービスレベルのチェックリスト

2026/02/26改定 株式会社rootip

経済産業省 「クラウドコンピューティングと日本の競争力に関する研究会」報告書 クラウドサービスレベルのチェックリスト より

No. 種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	root ip設定	左記備考
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	営業時間内(電話) (年未年始・土日・祝祭日を除く)24時間365日(メール)	受付方法(電話/メール)や営業時間外の対応は対象業務の重大性およびサービス内容/特性/品質に応じて状況が異なる	日本時間平日の 9:00～17:30 までとし、当社が定める定休日を 除きます	
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(日次で、作業前後の差分のみバックアップし、過次でフルバックアップを取る。遠隔地のデータセンタにテープ形式保管。アクセス権はシステム管理者のみに制限。復旧/利用者への公開の方法は別途規定)	保証要件を設定している場合は、具体的に明示。バックアップ内容は対象業務の重大性およびサービス内容/特性/品質に応じて状況が異なる また、クラウド・コンピューティング・サービスの民事再生、破産等によりサービス継続が出来ない場合についても明示されていることが望ましい	有 常時差分バックアップを取得。差分バックアップは3箇所以上の物理的に離れたデータセンター(東京エリア)に保存。過次バックアップは大阪エリア3箇所にも保存。 アクセス権はシステム管理者のみに制限。 データベースをお客様に直接公開することは無く、root ip側でシステムに復旧する。CSV出力する等の形でお客様にご提供は可能	
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	前日朝6時まで ただし、災害発生時は1週間前まで	データ破損、システム障害時において、どの時点のデータを最低限保証すべきか示すこと	障害発生時の5分前まで	
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	5年以上(証跡として残すべきもの、法定のもの) 3ヶ月以上(その他)	対象業務の重大性を考慮しつつサービス内容/特性/品質に応じて個々に検討する 証跡として残すべきだと思われるものとしては、アクセスログ等のセキュリティに関係するログ情報が挙げられる。法定のものとしては、帳票関係が挙げられる	データ: 2週間 アクセスログ: 3年間	データ保存期間延長はオプションにて提供 (延長分は差分ではなく1週間単位のフルバックアップとなります)
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	サービス解約後1ヶ月以内にデータおよび保管媒体を破棄	解約時には、CSVなどの一般的なフォーマットでデータ出力ができることが望ましい	契約終了後 60日以内に一切のデータを削除致します。(利用規約に明記) データ取り出しについてはCSVエクスポートが標準機能としてサービス内からお客様で実施いただけます。 包袋ファイルについては容量上一括DL機能が無いため、実費対応となります。	クラウド事業者のデータベースを使用しているため解約時の物理媒体破棄はありません。(最終的な媒体廃棄はNIST SP 800-88に従うことを確認しています)
32	バックアップ世代数	保証する世代数	世代数	3世代	ロールバックを必要と迫られた際にどの時点のバックアップデータまで遡ることが可能であるかを明確にしておくことが望ましい	常時差分バックアップのため世代の概念はありません	
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	個人情報や、業務において重要かつ暗号化せねば信頼性に欠けるデータを対象とする	有 データベースは暗号化されています	AES256を使用
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 複数のキーを使用することで、不正アクセス等の影響範囲を限定する	マルチテナントストレージの場合のキー管理の方法について、全顧客がひとつのキーを使うのか/顧客別にひとつのキーが割り当てられるのか/顧客別に複数のキーを使うのか明確にしておくことが望ましい	有 データベースはお客様ごとに論理的に分割されており、アクセス権も分離しているため、データが混合することはありません。	
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	個人情報を扱う場合には、クラウド・コンピューティング・サービス提供者との間で個人情報取り扱いに関して合意を形成して契約事項の中で責任の割り当てを行っておくべきであるが、万が一の個人情報漏えいに備える意味でサービス提供者における損害賠償保険加入の有無を確認しておくことが望ましい	無 損害賠償保険には加入していません。賠償額は「直近 1 年間の利用料金の総額」を上限とします。	

No. 種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	root ip設定	左記備考
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 返却する場合は、テープ媒体にデータを保管し、提供する消去する場合は、証明書を送付する(第三者機関発行の証明書が望ましい)	外部への漏えいをいかに防ぐ仕組みが出来ているか	データの取扱いについてはNo.31回答をご参照ください。 データを外部に開示・漏洩することはありません。	裁判所、その他の法的な権限のある官公庁の命令等を除きます。
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	入力データ、算出データ等がハードウェア/プラットフォーム/アプリケーションの問題や不正な操作により改ざんされていないこと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 開発時のチェック、またデータ作成/更新時にもデータとマスタの不整合が無いかなどをチェックしています。	
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	金額、住所、電話番号等の文字種、データ形式が制限されるフォームにおいて、想定外のデータ入力を検出し、不正なデータをデータベースに格納しないようにする仕組みを提供していること	有 数値、日付入力などはデータ形式をチェックし、異常データを入力できないようにしています。	制限外のデータは備考欄に補足を記載できます
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	ISMS認証取得プライバシーマーク取得	ITサービスマネジメントのベストプラクティスであるITILやJISQ20000、JISQ27001:2006をベースとした情報セキュリティ監査の実施等の取得状況も確認することが望ましい	有 ISMS(JIS Q 2700,ISO/IEC 27001) 認証登録番号 IR0151 プライバシーマーク 登録番号 17004395	
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 (サービス提供前に、セキュリティホールの有無等について第三者機関(又は内部機関)により検査を受け、また、検査が定期的かつ適切に行われていることを年1回、外部機関により評価を受ける。また、速やかに指摘事項に対して対策を講じる。)	セキュリティ監査、システム監査、ペネトレーションテスト等ネットワークからの攻撃に対する検証試験、ハードウェア/プラットフォーム/ウェブアプリケーションの脆弱性検査、データベースセキュリティ監査などを想定	有 第三者による診断・評価を実施しています	
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 (運用者が限定されていること)		有 ユーザーデータにアクセス可能な従業員を制限しています。 また内部システムは多要素認証を要求しています。	
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	3DES/RSA/SHA-1	SSLの場合は、SSL3.0/TLS1.0(暗号強度128ビット)以上に限定	SSL(TLS 1.2以上)で通信するようになっております	
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	有		無	
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	データ認証のアクセスコントロールについて明記		有 データベースを論理的に分割、またアクセス権もそれぞれに対して限定し、異なるユーザー間のデータが混合しないよう設計しています。	

「root ipクラウド」クラウドサービスレベルのチェックリスト

2026/02/26改定 株式会社rootip

経済産業省 「クラウドコンピューティングと日本の競争力に関する研究会」報告書 クラウドサービスレベルのチェックリスト より

No. 種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	root ip設定	左記備考
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 (利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る)	利用者組織にて規定しているアクセス制限と同等な制約が実現できるかどうかを確認すること。クラウド・コンピューティング・サービスにおけるハードウェア/プラットフォーム/アプリケーションで用意されているロール(管理者、一般ユーザ等の役割を意味する)に制約がある場合には、ユーザを既存のロールの範囲でグルーピングする等の工夫により対応できるかどうかを確認する。クラウド・コンピューティング・サービスではマルチテナントを採用しているため、他の顧客と一つのデータベースを共有する可能性があることに配慮すること	有 ユーザーデータにアクセス可能な従業員を制限しています。	
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	権限に沿ったID管理が行われていること(1人1ID発行)		一人につき1 IDで運用しており、アクセス記録にIDが付与されます。 お客様操作ログはご提供可能です。	お客様ログの提供範囲および提供方法は状況によりご相談となります。 弊社内インシデントにおける弊社内システムログはセキュリティ上ご提供はできませんが、必要に応じインシデント調査を行います。
47	ウイルススキャン	ウイルススキャンの頻度	頻度	週次		パターン更新の度に実施	
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	・権限者のみアクセス可・廃棄時には、データを完全に抹消する・暗号化、認証機能を用いる・遠地へ運ぶ際は、施錠されたトランクで運ぶこと		有 メディアは暗号化され、廃棄時には社内での一次データ抹消、その後外部業者での抹消・物理破壊を行います(NIST SP 800-88準拠)。また管理外の可搬媒体へのデータ書き出しにも制限をかけています	クラウドサービス上のストレージについても以下の管理を行っています ・暗号化 ・権限者のみアクセス可(多要素認証) ・契約終了時にデータを完全に抹消(NIST SP 800-88に準拠)
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	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		データセンターは日本国内であり、日本国法に準拠します。	

その他 よくあるご質問

2026/02/26改定 株式会社rootip

ご質問	root ip設定	左記備考
サービスのURLは？	お客様毎に異なるサブドメインでURLを設定いたします(***) 事務所版: https://***.rootip-cloud.net/ 企業版: https://***.rootip-enterprise.net/	
クラウド環境、データセンターは何を使用しているか？	Amazon Web Service(AWS)を利用しています。	
データセンタは日本国内か？	日本国内です	AWS 東京リージョンをメインで使用。バックアップとして大阪リージョンを使用。
データセンタの冗長化、障害対策等を行っているか？	実施しています 障害対策の実施されたAWS 東京リージョンのデータセンタを利用し、また物理的に離れた3データセンタ(アベイラビリティゾーン)を利用し冗長化を行っています。	詳細は以下をご覧ください https://aws.amazon.com/jp/compliance/data-center/data-centers/
データセンタはISMS(ISO 27001), SOC Type II, ISMAP認証を取得しているか？	取得しています	詳細は以下をご覧ください https://aws.amazon.com/jp/compliance/programs/
パスワードポリシーについて (必須文字、長さ、定期変更など)	12文字上、英数字組み合わせが必須となっています。 記号も使用可能で、使用可能文字の制限はありません。	定期的なパスワード変更については、米国国立標準技術研究所(NIST)のガイドラインおよび内閣官房 国家サイバー統括室(NCO)、総務省の方針に従い、推奨しておりません。 ご参考 NCO インターネットの安全・安心ハンドブック(第5章) https://security-portal.cyber.go.jp/guidance/handbook.html
多要素認証(2要素認証)は可能か？	可能です 基本的には必須設定となっています	
端末制限(デバイス制限)は可能か？	クライアント証明書によるデバイス制限が可能です	
ワンタイムパスワードは使用可能か？	使用可能です 全ユーザへの必須化も可能です	
接続元のIPアドレス認証は可能か	設定可能です	複数アドレス設定も可能です。 全体設定に加え、特定ユーザのみ異なるIPアドレス制限を行う事も可能です(組織外のユーザにアカウントを振り出す場合など)
シングルサインオン(SSO)に対応しているか？	対応しています 標準規格であるSAML2.0準拠の IdP (Id Provider)であればどのベンダーでもご利用いただけます	
シングルサインオン(SSO)でのログインを強制できるか？ (IP/パスワードでのログインを禁止できるか)	設定可能です	
アカウントロック機能はあるか？	ログイン失敗 5回で一定時間ロックされます。 お客様管理者での解除も可能です。	
キャパシティ不足による障害を事前回避するプロセスが構築されているか？	自動での容量増加が行われます。 (クラウドサーバーのため物理的ではなく設定上の論理的な容量が制限となります)	
バージョンアップの連絡、利用者負担はあるか？	お客様運用に影響する可能性がある場合は事前にご連絡を行います。 利用者負担はありません。	

その他 よくあるご質問

2026/02/26改定 株式会社rootip

ご質問	root ip設定	左記備考
サーバーデータの改ざん検知/防止はされているか	ファイルシステムレベルで読み取り専用(書き込み不可)の構成とし、ファイル改ざん自体ができない設計としています。	
ログの改ざん検知/防止はされているか	アプリケーションサーバーではなく外部にログを保存する仕様とし、また保存先としてはクラウド事業者(AWS)の提供する書き換え機能のないログ保存サービスを使用することで、改ざんを防止しています。	
ログの時刻は正しいか	NTPによる時刻同期を行っております。	
技術的なセキュリティ対策はどのようなことを行っているか	ファイアウォール、WAF、ランタイム監視(ふるまい検知)、ネットワーク監視(IDS)、脆弱性スキャン、書き込み禁止ファイルシステムの採用等を行っています	
DDoS対策は実施しているか	実施しています	
プライバシーポリシー、セキュリティポリシーはあるか	弊社HPに掲載しております	弊社HP https://rootip.co.jp/
AIを利用しているか、ユーザデータは学習に使用されるか	AI機能はお客様の任意で使用可能で、学習には用いません。 詳細は弊社HP AI利用ポリシーをご参照ください	弊社HP https://rootip.co.jp/
第三者への業務委託をする場合、業務委託先の管理はどうしているか？	現在、システム開発・運用等において第三者委託は行っておりませんが、第三者に委託する際は委託先に対し弊社と同等の義務を課す方針です。 (ISMS、プライバシーマークでも要求されております)	
変更管理を行っているか	実施しております	
外部の専門業者による脆弱性診断を定期的に実施しているか？	実施しております	
root ip社員からのアクセスを制限できるか？	root ipサポートからのアクセスの制限が可能で、サポートが必要な際にのみ許可する等の運用が行えます。	SaaSであるため、左記制限を行った場合もデータベース権限を持つ一部管理者からは"技術的には"アクセスが可能である事をご承知おきください。(クラウドシステムでは物理的に回避できないものと思われます)
従業員と秘密保持契約は締結しているか	締結しております	
Assuredで調査できるか	Assuredも対応しております。 Assured側へ評価をご依頼ください	