

本資料は、「クラウドサービスレベルのチェックリスト」（経済産業省）に基づき、株式会社メディアスクエアが提供するSMARTCROSSのセキュリティについて記載したものです。  
お客様フォーマットのチェックシートへの回答をご希望の場合は、別途有料オプションを提供しております。詳細は営業担当までお問い合わせください。

No.	種別	サービスレベル項目	規定内容	測定単位	補足
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	【有】最低1週間前に契約者様宛にメールにて通知します。
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】現時点で終了の予定はありませんが、3か月以上前にWebサイトおよび契約者様宛にメールにて通知する予定です。
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	【有】現時点で終了予定はありませんが、データを抽出して提供するなどの対応を致します。
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 (%)	99.9%
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	【有】サーバーは複数データセンターで冗長化して運用しています。
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】日次でデータをバックアップを行い世代管理をしデータセンターに保管しています。またシステム構成はコード化して管理しており、迅速な復旧が可能です。
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)	【有】万が一に備えお客様側で管理画面よりデータをCSV形式でダウンロードすることが可能です。
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	【有】機能追加などは随時行っております。お客様への影響が大きい変更については、事前にメールなどで告知を行います。またパッチについても適宜適用を行っております。
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	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	公開しておりません。
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】死活監視、パフォーマンス監視、エラー監視を行っております。
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	【有】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メール、Webサイトで行います。
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数分以内に行われます。 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)	3分間隔です。
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	個別の報告はしていませんが必要に応じてWebサイトで行います。
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	【有】必要に応じて提供します。
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】機能、デザイン等の個別カスタマイズを承ります。
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】APIは公開しておりません。
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】同時接続利用者数の制限はございません。
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	【無】リソースの制限はございません。 但し個別に契約条項が存在する場合はそちらを優先します。

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	メール・問い合わせフォーム：24時間365日 お電話：平日10：00～18：00（12：00～13：00を除く）
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	平日10：00～18：00（12：00～13：00を除く）
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】日次でフルバックアップを取得し、データセンターに保管します。復旧方法については定められた手順に基づいて行います。バックアップデータへのアクセスは限定された管理者のみに制限されています。
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る、データを保証する時点	時間	深夜4時から2時間以内に取得(日次取得)
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	契約終了時のデータ削除後、保持バックアップ世代数(一週間)まで
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】 契約終了月の翌月の弊社指定日に全データを完全に削除します。 必要に応じてサービスの契約終了前にデータをCSV形式でダウンロードいただけます。
32		バックアップ世代数	保証する世代数	世代数	7世代を保管しています。
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】個人情報については全て暗号化しています。
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】お客様ごとに完全に分離されたデータ領域で運用しております。
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	【有】損害保険に加入しています。
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】 契約終了月の翌月の弊社指定日に全データを完全に削除します。 必要に応じてサービスの契約終了前にデータをCSV形式でダウンロードいただけます。
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】データの整合性検証を行っております。
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】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。
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】プライバシーマークを取得しています。登録番号：17001004号（2012/01取得）
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】外部セキュリティ診断会社による脆弱性診断を定期的実施しています。 (直近実施：2022/09 但しサービス毎に実施時期が多少異なりますので詳細はお問い合わせください。)
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】サーバにアクセスができるのは限定された2名のみです。
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】サービスとの通信はTLS 1.3にて暗号化しています。
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】お客様ごとに完全に分離されたデータ領域で運用しております。
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】サーバにアクセスができるのは限定された2名のみです。
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	保管しているログから調査可能です。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	サーバー：DSaaSによりリアルタイムスキャンを行っています。 PC端末：リアルタイムスキャンを有効化し随時検索しています。
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。
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ます。