Cloud Document

セキュリティチェックシート

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、株式会社イーツー・インフォの提供するクラウドドキュメントのセキュリティについてまとめたものです。

No.	種別	サービスレベル項目例	規程内容	
アプリケーション運用				
1	可用性	サービス停止時間	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）	24時間365日となります。（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）	実施5営業日前までにサービス画面でのお知らせおよび、下記のメンテナンス情報のページにて通知致します。 https://service.cloud-document.net/helps/information
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）	サービス利用約款に記載しています。 サービス終了3ヶ月以上前までに通知致します。
4		突然のサービス提供停止時の対処	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	お客様データ保護は常に実施していますが、突然のサービス停止時に対しては可能な範囲でシステムの復旧に努めます。 お客様データについては、お客様の責任でバックアップいただけるようお願い致します。
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）	定めておりません。
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	無停止のディザスタリカバリには対応していません。災害発生時は、定期的に取得しているバックアップをもとに環境を再構築致します。
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	代替手段は提供していません。
8		代替処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	お客様データについては、お客様の責任でバックアップいただけるようお願い致します。
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	バージョンアップやパッチの適用などのアップグレード作業は適宜実施しています。
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）	定めておりません。
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	定めておりません。
		目標復旧時点(RPO)	障害発生後のサービス提供再開に対応するバックアップ世代管理の目標時間	定めておりません。
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	件数・対応時間は公開しておりませんが、以下のURLで個別の事象は公開しています。 https://service.cloud-document.net/helps/information
13		システム監査基準	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	URL／パフォーマンス監視等を常時実施しております。
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）	障害発生後、システム上のお知らせまたはメール等、当社が適当と判断した方法にて通知 を行います。また、システム上でお知らせができない場合は、利用期間中のお客様へ、メール・電 話でご連絡いたします。
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	定めておりませんが、速やかに通知できるように努めております。
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	公開しておりませんが、短い単位で監視・データ収集を実施しています。
17		サービス提供状況の報告/間隔	サービス提供状況を報告する方法／時間間隔	個別の報告は実施しておりません。
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）	システム内部で一部のログは取得しています。お客様への提供はしておりません。
19	性能	応答時間	処理の応答時間	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	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	公開しておりません。

Cloud Document　セキュリティチェックシート

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、株式会社イーツー・インフォの提供するクラウドドキュメントのセキュリティについてまとめたものです。

No.	種別	サービスレベル項目例	規程内容	
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	機能・デザインの個別カスタマイズは承っておりません。
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）	任意の外部システムとの接続は対応しておりません。個別にご相談いただき、有償等での対応はできる可能性がございます。
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	制限はありません。
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	上限は定めておりません。
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	24時間365日受付ています。（メール・問い合わせフォーム）
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	24時間365日受付ています。（メール・問い合わせフォーム） 通常のサポート業務の対応時間は、平日9:00～17:00（祝日、年末年始等弊社休日は除く）となります。 内容を確認のうえ3営業日以内を目安にご返答いたします（調査の状況により、それ以上の時間を要する場合もございます）
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	定期的にバックアップを取得しています。また、バックアップはサービスが稼働している環境とは異なる場所に保管しています。 バックアップからの復旧はエンジニアによる手動オペレーションにより実施します。
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り、データを保証する時	具体的な時期は公開していませんが、24時間以内のデータを取得しています。
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	具体的な期間は公開していません。また、サーバー、ストレージ、データベースなど取得しているサービスにより異なります。
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	作成した帳票：最大24時間保存しています 帳票テンプレートおよび出力履歴：データ確認のため、半年程度保持しています。 データ保持が不要な場合、解約前に管理画面からテンプレートやマッピング情報の削除をお願い致します。
32		バックアップ世代数	保証する世代数	サーバー、データベースは4週（28回）分保存しています
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	データは暗号化して保存しております。パスワードに関しては復元できない形式にて保存しております。また、通信経路はTLSv1.2で暗号化しております。
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	アカウント単位でデータベースを分離して、保管しております。
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	保険には加入しておりますが、詳細は公開しておりません。
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	データの返却はございません。必要な場合、解約前にお客様ご自身でブラウザーからテンプレートファイルなどの保全をお願いします。データ消去は解約後に対応しております。
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	ファイルアップロードや画面からの更新時に整合性のチェックを実施しています。通信経路はTLSにて暗号化され、盗聴・改ざんを防いでいます。
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	データの種類に応じて、データ不整合を起こさないための適切な制限を設けております。

Cloud Document　　セキュリティチェックシート

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、株式会社イーツー・インフォの提供するクラウドドキュメントのセキュリティについてまとめたものです。

No.	種別	サービスレベル項目例	規程内容	
セキュリティ				
39	公的認証取得の要件	公的認証取得の要件	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	プライバシーマークを取得しております。 認定の詳細につきましては以下のURLよりご確認ください。 https://www.e2info.co.jp/company.html
40		アプリケーションに関する第三者評価	第三者によるウェブアプリケーション脆弱性評価実施	脆弱性診断を不定期にて実施しております。
41		情報取扱い環境	データをバックアップした媒体を保管する期限	サーバーへのアクセスを限定することでセキュリティ性を担保しております。アクセス制限では、ファイアウォールで当社社内ネットワークからのアクセスのみを許可しており、またシステム担当エンジニアのみ所有する秘密鍵の使用を必須としております。
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	TLSv1.2にて通信を暗号化しております。
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」	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	お客様ごと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	データへのアクセスは業務上必要なスタッフのみに制限しています。
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	IDは個人単位で付与しております。ログ検索にIDの情報はございませんが、IPアドレスを検索に利用することは可能です。ログは1年間保管しております。
47		ウイルススキャン	ウイルススキャンの頻度	全てのスタッフの端末にはウイルス対策ソフトが導入されており、常時スキャンが実施されております。
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	二次記憶媒体は使用せず、データセンター間でバックアップを取っております。
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	把握しております。バックアップは国内のデータセンターに保存しています。