サイバーソリューションズ株式会社　セキュリティチェックシート

更新日2025年9月8日

- 本チェックシートは、サイバーソリューションズ株式会社が提供する以下のサービスについて、そのセキュリティ対策を記載したものです。
  ・CYBERMAIL Σ、MAILGATES Σ、ENTERPRISEAUDIT Σ、Cloud Mail SECURITYSUITE
- 本チェックシートの項目は、経済産業省 クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版を基に作成したものです。
- 本チェックシートは、予告なく変更することがあります。

No.	種別	サービスレベル項目	規定内容	測定単位	回答
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日となります。 （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 緊急時を除き、以下のタイミングでサポートシステムにて通知いたします。 ■停止時間 / 通知時期 ・～10分 / 2週間以上前 ・11～30分 / 3週間以上前 ・31分～ / 1ヶ月以上前
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、少なくとも2ヶ月前までに電子メール及びサービス画面上での告知によりお客様に通知いたします。
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	無 現時点で終了予定はなく、プログラムやデータの預託も未定となります。
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（%）	2024年(1月～12月)の実績値は100.00%となります。 最新の実績値はサポートシステムにてご確認いただけます。 https://cloud-sup.cybersolutions.co.jp/hc/ja (ログインが必要) なお、当社のサービス稼働率の定義は以下のとおりです。 ■月間稼働率 【各月の合計分数】から、【合計ダウンタイム分数】を減算し、【各月の合計分数】で割った数値 ■ダウンタイム 弊社監視システムにてSMTPを利用したメール送信およびHTTP・HTTPSを利用したWEBアクセスを監視し、10分以上連続して停止を検知した時間をダウンタイムとみなします。 （10分未満の断続的な停止は、ダウンタイムとして計測しません。）
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	有無	有 複数のデータセンターでサービスを提供しており、データセンターに問題が発生した場合、手動で切り替え作業を実施します。この切り替えには相当な時間を要することがあります。
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 複数のデータセンターでサービスを提供しており、データセンター間には遠隔地バックアップがあります。このバックアップデータを利用してサービス復旧を実施します。復旧まで相当な時間を要することがあります。
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 ■CYBERMAILΣ お客様の責任において事前にアカウント情報(CSV形式)・アドレス帳情報(vCard)・メールデータ(EML形式)をエクスポートすることが可能です。またAPIによるデータ取得も可能です。 ■ENTERPRISEAUDITΣ お客様の責任において事前にメールデータ(EML形式、PST形式)をエクスポート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、サポートシステムにて事前に公開しております。
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	回数としては公開しておりませんが、個別の障害情報はサポートシステムにて公開しております。
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 障害発生時は、弊社担当者が通知を受け、対応を行います。お客様へは必要に応じて、サポートシステムにて通知いたします。
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	時間	60分以内を目標に告知いたします。
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）	監視対象により異なりますが、システム停止につながる重要な監視対象は1分間隔となります。
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	サポートシステムにて確認することができます。
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	有 各サービスの管理画面より確認することができます。
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	無 利用者ごとのカスタマイズは行っておりません。
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）	有無	有 CYBERMAILΣはAPIを公開しております。 他サービス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。但し、システム影響が出る場合においては制限することがございます。
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	ご契約いただくサービスメニューよりディスク容量制限を設けております。
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	障害対応については24時間365日受付ております。 なお、夜間・休日は一次受付専用窓口(電話)での対応となります。 ・夜間・休日障害一次受付専用窓口 受付時間 夜間平日18:00 ～ 9:00 休日(土日祝・弊社休業日)
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	・サポートシステムへのお問い合わせ 受付時間 24時間365日 対応時間 営業日 9:00 ～ 18:00 ・お電話でのお問い合わせ 受付時間 営業日 9:00 ～ 18:00
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 1日1回別ロケーションのデータセンターへ遠隔地バックアップを実施し、過去7日間分を保存しております。 システム全体のバックアップのため、お客様単位での復旧はできません。
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点	時間	1日1回実施しております。
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	時間	過去7日間分を保存しております。
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	有 解約申込書記載の解約日の翌営業日に、全データの削除を実施しております。
32		バックアップ世代数	保証する世代数	世代数	過去7日間分、7世代となります。
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 蓄積データは暗号化して保存しております。
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	有無／内容	有 ストレージ単位で暗号化キーを管理しております。
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おります。
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 解約申込書記載の解約日の翌営業日に、全データの削除を実施しております。
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	有無	有 データはお客様の責任でデータ内容の確認をいただきます。 通信経路はTLSにより盗聴、改ざんを防いでおります。
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文字種や長さのチェックを行っております。
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 以下の認証を取得しております。 ・ISO/IEC27001:2022 JIS Q 27001:2023、認証番号：IS 513563 ・ISO/IEC 27017、認証番号：CLOUD 721590 ・ISO/IEC 27018、認証番号：PII 721591
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 定期的に外部ツールを用いて本番環境と全く同じアプリケーションであるステージング環境にて脆弱性チェックを行っております。
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 データへのアクセスは業務上必要な一部の技術者のみに制限しております。
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	有無	有 TLSで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」	有無	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	有 契約ドメイン毎によりデータを論理的に分離して管理しております。
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 データへのアクセスは業務上必要な一部の技術者のみに制限しております。
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	IDは個人ごとに発行して管理しております。また、セキュリティログは10年間保存しております。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	■CYBERMAIL Σ、MAILGATES Σ メール送受信時にウィルスチェックを行っております。 ■ENTERPRISEAUDIT Σ サービス仕様上、ウイルススキャンは実施しておりませんが、複数のセキュリティ対策を講じており、詳細は非公開となります。 また、オペレーション用の端末では、リアルタイムスキャンを有効化し、実施しております。

48	セキュリティ	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 二次記憶媒体を使用せず、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	把握状況	有 国内データセンターを利用しており、把握しております。