AES256

当チェックシートは、オフィスステーションのセキュリティについて「SaaS 対応 SLA ガイドライン」(経済産業省)に基づき回答した資料です。

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 ※計画的な停止を除く ※毎日、午前 4 時から午前 4 時 30 分は計画停止をおこなっています。
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	【無】 計画的なオフィスステーションの停止はありませんが、毎日、午前 4 時から午前 4 時 30 分はメンテナンスのため利用できません。 また、月に 1～2 回、機能リリースによる一時停止（深夜 22 時以降に 1 回につき 1～2 時間程度）を実施することがあります。 事案発生を確認次第、速やかに実施いたします。 連絡手段は、HP お知らせ、オフィスステーションお知らせなどにより通知します。
3		サービス提供終了時の事前通知	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】 現時点で終了の予定はありません。 システム内「お知らせ」にて半年程度前に通知します。
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】 現時点で終了の予定はありません。 また、プログラムやシステムの各種設定データの預託についても未定です。
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（%）	SLA では 99.9%を目標としていますが、直近の稼働率は 100%です。 毎月公開している稼働率は下記を参照ください。 https://www.officestation.jp/topics/notice/
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】 AWS 東京リージョンの複数データセンターにて冗長化構成で運用しています。 AWS 東京リージョンが利用できない場合、AWS 大阪リージョンにてサービス提供をおこないます。
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】 サーバ及びデータのバックアップを日次で取得しています。 AWS 東京リージョンの複数データセンターにて保管しているため、大規模障害時でも復旧可能です。
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】 従業員データや個人番号等は CSV 形式でお客様にてダウンロードしていただくことが可能です。 また、API の提供もおこなっています。
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	有無	【有】 随時、機能追加・不具合修正をおこなっています。 リリースの際、サービス停止が必要な場合は、事前にシステム内「お知らせ」にて通知をおこないます。
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	非公開
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	24 時間以内

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	なし
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】 サイトの死活監視、パフォーマンス監視、プログラムアラート監視、アクセス監視をおこなっています。
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】 検知の仕組みを導入し、異常を弊社担当に通知されます。 障害が発生した場合、オフィスステーション内の「お知らせ」、HPなどで通知します。
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	弊社担当者への通知確認は毎分おこなっています。 ※電話連絡は30分ごと お客様へは1時間以内を目標に通知をおこないます。
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）	毎分
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	平常運用時の定期報告はおこなっていません。 ただし、大規模障害発生時は必要に応じてシステム内「お知らせ」、Webサイト等で通知をおこないます。 （1時間ごとに情報更新）
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】 アクセスログは貴社依頼に基づき有償にて提供可能ですので、都度ご相談ください。 またオプション（有償）となりますが、従業員台帳の履歴機能を契約いただけますと、従業員台帳の変更履歴のログ取得が可能です。 ログイン履歴は管理者画面よりご確認いただけます。
19	性能	応答時間	処理の応答時間	時間（秒）	全トランザクションについて、5秒以内の応答を目標とします。 ※ファイルアップロードや帳票印刷、電子申請については対象外とします。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	非公開
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）	非公開
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】 利用者(ID)ごとに利用する機能や取り扱える個人情報の範囲の制限設定をおこなえます。 各社独自の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）	有無	【有】 APIの提供をおこなっています。 ご利用の際は営業窓口までご相談ください。

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	処理能力	【無】 提供リソースの制限はありません。
サポート					
26	サポート	サービス提供時間帯（障害対応）	障害対応時の問い合わせ受付業務を実施する時間帯	時間帯	方法：メール・電話 時間：10:00～12:00、13:00～16:00 （土日祝祭日、弊社休業日除く） ※電話による対応は「コールセンターオプション」をお申し込みいただいている場合に限ります。
27		サービス提供時間帯（一般問い合わせ）	一般問い合わせの受付業務を実施する時間帯	時間帯	方法：メール・電話 時間：10:00～12:00、13:00～16:00 （土日祝祭日、弊社休業日除く） ※電話による対応は「コールセンターオプション」をお申し込みいただいている場合に限ります。
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	有無/内容	毎日 AWS にてバックアップを取得しています。 ・差分バックアップ 実施：1 日 1 回 05:05～05:15 の間に実施（自動スナップショット取得） 保持期間：35 世代 ・フルバックアップ 実施：1 日 1 回 1:00 フルバックアップ取得：25:00 時点 保持期間：90 世代 サーバ設定・システムイメージ： 実施：1 日 1 回 1:00 保持期間：35 世代 アップロードファイル： 随時バックアップ 保持期間：無期限 保存場所：AWS 東京リージョン
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	当日午前 1 時ころまでに取得します。
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	35 日間（世代）保管しています。
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】 マスキング処理による論理削除を実施しています。 削除時期は以下のとおりです。 ・特定個人情報：解約日の翌日 ・個人番号以外の情報：解約日の 90 日後 ≪オフィスステーション利用規約 10 条参照≫ https://service.officestation.jp/terms_kigyou.html 原則、オフィスステーションは個人情報の委託先に該当しないため、データ返却はおこないません。 オフィスステーションに登録されたデータは利用者が自らダウンロードしていただく必要があります。
32		バックアップ世代数	保証する世代数	世代数	35 日間（世代）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】 データはすべて暗号化して保存しています。 個人番号やパスワードについては、別途個別暗号化をおこなっています。
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】 契約ごとに発行した内部キーによって論理的に分離して管理しています。

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。 利用規約に定める範囲において補償をおこないます。
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】 ご解約までにお客様自身にて必要なデータはエクスポートをお願いします。
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おこなわれていること	有無	【有】 データ入力時、送信時に検証をおこなっています。 通信の暗号化は SSL(TLS1.2)でおこなっています。
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】 データ入力時に検証をおこなっています。 不審な入力に対しては、アクセス遮断をおこないます。
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】 ISO27001（IS699609） ISO27018（PII699610）
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】 年一回、第三者機関にて Web 脆弱性診断を実施しています。 前回実施：2025 年 2 月 3 日
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セキュリティルームでのみ可能となっています。 また、セキュリティルームへの入室は一部の限られた担当者のみ許可しており、入室にはセキュリティカード及び生体認証が必要となっています。 なお、本サービスでは、「個人情報／特定個人情報」の委託先となりえません。
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】 SSL（TLS1.2,TLS1.3）認証による通信データの暗号化を実施しています。 TLS1.0/1.1 は無効化しています。
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】 セキュリティ監査が必要となる場合は個別にご相談ください。
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】 契約ごとに発行した内部キーによって論理的に分離して管理しています。

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】 原則、サービス事業者はシステムに登録された特定個人情報および個人情報へのアクセスはいたしません。 ただし、不具合やサーバートラブル、障害発生時など、データへのアクセスが必要なときのみアクセスを許容することがございます。 登録された特定個人情報および個人情報は、専用サーバーに集約し、セキュリティルーム内の専用端末のみアクセスを許可しており、セキュリティルームの運用は以下のとおりとなっています。 ・データサーバへのアクセスはセキュリティルーム内でのみ可能 ・セキュリティルームへの入室は限られた者にのみ ・セキュリティルームへの入室は作業内容の申請後、役員承認が必須 ・入室にはセキュリティカードおよび生体認証が必須 ・セキュリティルーム内は常時、監視カメラにて録画 ・セキュリティルーム内の PC では USB などの記憶媒体の利用が行えないように制御 ・セキュリティルーム内の PC では印刷が行えないように制御 ・許可されたサイトにのみアクセスできるよう制限
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、管理しています。 ※共有 ID は利用していません。 アクセスログは無期限で保存しています。 ただし、お客様でのダウンロードはおこなえません。都度ご相談ください。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	通信のたびにリアルタイムスキャンを実施しています。
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は禁止しています。
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	日本法に準拠します。