PHONE APPLI PEOPLE セキュリティチェックシート

2023年8月8日版

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　2010年8月発行）に基づき、株式会社PHONE APPLIの提供するPHONE APPLI PEOPLE（適用となる利用規約：https://phoneappli.net/product/agreement/renraku/）のセキュリティについてまとめたものです。
他社が提供する同名のサービスは本資料の対象外となりますので、ご注意ください。
また、オプションサービスも本資料の対象外となりますので、再委託先が発生するオプションサービスを申し込まれる場合は、必要に応じて別途お問合せください。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）
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	時間帯	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）	有無	【有】 1週間前までにステータスサイト（https://status.phoneappli.net/）およびメールにて通知いたします。
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】 事前通知の詳細なタイミングは定めておりませんが、コーポレートWebサイト（https://phoneappli.net/）およびメールにて事前に通知いたします。
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】 現時点で予定はありません。
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% なお、目標値となりますので、未達時の補償はありません。
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	有無	【有】 バックアップデータは災害対策を考慮し、サービス環境とは異なるリージョン（国内）に保管しております。
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	【無】 代替手段はご用意しておりませんが、早期復旧を目的としたサービス基盤の冗長化、復旧手順の整備を行っております。 なお、お客様が復旧に向けて事前に準備できる手段として、サービス時間内に利用者にて各種データをTSV（タブ区切り）形式ファイルでエクスポートする機能をご用意しております。当該エクスポートデータを利用者の責任において保管することで重大障害時の代替手段とすることが可能です。 エクスポート可能なデータおよびエクスポート手順はサービス管理者ガイド（https://status.phoneappli.net/guide/）をご確認ください。
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）	【無】 公開しておりません。 ただし、上記TSVファイルを利用することで、お客様にて、代替となる連絡先データベースの復旧は可能となります。
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】 機能・インターフェイスの変更を伴うソフトウェアのバージョンアップ、および各種メンテナンス作業は、計画メンテナンスにて行うものとし、1週間前までにメール配信およびWebサイト掲載により通知します。
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	4時間
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。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）
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】 サービス基盤の死活・リソース監視およびサービス正常性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】 10分以上故障状態が継続した場合は、サポート提供時間帯にステータスサイト（https://status.phoneappli.net/）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	サポート提供時間帯に、速やかに通知いたします。
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）	5分 故障発生時・異常値検知時の当社サービス運用担当者への通知は20分以内としております。
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	個別のご報告はしておりませんが、ステータスサイト（https://status.phoneappli.net/）にて稼働状況を公開しております。
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】 管理者権限を付与されているユーザにてアクションログ（ユーザ操作ログ）を取得することが可能です。 ログ詳細はサービス管理者ガイド（https://status.phoneappli.net/guide/）をご確認ください。
19	性能	応答時間	処理の応答時間	時間（秒）	ベストエフォートとなります。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	ベストエフォートとなります。
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）	ベストエフォートとなります。
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】 一部、項目の表示・非表示設定が可能です。
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】 PHONE APPLI APIを公開しております。 （https://note.com/pa_api/n/n8262e9ed4c83）
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	処理能力	上限はありません。
サポート					
26	サポート	サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	受付：24時間365日となります。（メール／お問い合わせフォーム） 対応時間：平日9:00～17:00となります。（年末年始・土日・祝祭日を除く） 対応時間外のお問合せは翌営業日以降の対応となります。また、お問合せ内容によっては回答までお時間をいただく場合がございます。
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	受付：24時間365日となります。（メール／お問い合わせフォーム） 対応時間：平日9:00～17:00となります。（年末年始・土日・祝祭日を除く） 対応時間外のお問合せは翌営業日以降の対応となります。また、お問合せ内容によっては回答までお時間をいただく場合がございます。
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	有無／内容	【有】 夜間処理による日次バックアップを実施しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）
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0時
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	7日間
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】 サービス利用契約終了後1ヶ月以内に、お客様のテナントごと論理削除する方法でデータ消去いたします。
32		バックアップ世代数	保証する世代数	世代数	7世代
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】 FIPS 140-2に準拠した256ビットAES暗号化を使ったハードディスクレベルでの暗号化を実施しております。
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】 テナントごとにユニークな識別子を付与し論理的に分離することで、他利用者からのアクセスを制限しております。
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】 データ漏えいが当社の故意・重過失による場合には、利用規約に定められた範囲で賠償いたします。 個人情報漏えいに備えた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】 サービス利用契約終了時は、お客様のテナントごと論理削除する方法でデータ消去いたします。 ご要望があれば、当社にて消去証明書を発行することが可能です。
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	【無】 サービスの性質上、データの整合性はお客様にてご確認ください。
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】 各種入力フォームでバリデーションチェックをしております。
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】 ISMS認証（ISO/IEC27001）、クラウドセキュリティ認証（ISO/IEC27017）およびプライバシーマーク（JISQ15001）を取得しております。
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】 第三者機関による第三者機関によるWebアプリケーション脆弱性診断およびプラットフォーム診断を年1回実施しております。
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】 本番環境へのアクセス権限の付与は、サービス運用担当の従業者に限定しております。 また、IPアドレス制限によりアクセス可能な経路を限定しております。
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】 TLS1.2にて通信を暗号化しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定（記入欄）
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】 テナントごとにユニークな識別子を付与し論理的に分離しております。
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】 本番環境へのアクセス権限の付与は、サービス運用担当の従業者に限定しております。 また、IPアドレス制限によりアクセス可能な経路を限定しております。
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	アクションログ（ユーザ操作ログ）をサービス上で90日間保存しております。ログは権限を持つユーザにてダウンロードが可能です。 ログの詳細は管理者ガイド （https://status.phoneappli.net/guide/）をご参照ください。 その余の協力については、セキュリティインシデント発生時に別途ご相談ください。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	サービス運用端末につき、ファイルアクセスおよび電子メール受信時に常時スキャンするよう設定をしております。
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	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得しております。
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	データ保存地は日本国内となります。 適用となる各種法令を把握しております。