セキュリティ
ホワイトペーパー

PROTO
Solution

この文書について

この文書は、ラクネコの情報セキュリティへの取り組みを紹介するものです。

ラクネコは、株式会社プロトソリューション（以下、「当社」といいます）が運営する、来訪者受付業務を効率化するためのサービスです。
ラクネコをご利用のお客様が当サービスにアポイントメントを登録すると、招待されるお客様専用の受付QRコードが自動的に発行されます。アポイントメントの当日に受付端末で受付QRコードをかざすことで、お客様が来訪されたことを知らせる通知と、来訪履歴を残すことができます。

ラクネコでは、来訪者及び受付履歴の情報を機密情報として扱い、お客様の意思に反して第三者に読み取られたり、内容を改竄されることのないように、情報セキュリティに配慮した取り組みを行います。

なお、この文書はラクネコのサービス本体について記述したものです。
他社サービスとの連携機能や一部のオプションサービスについては、この文書の記述が当てはまらない場合があります。詳細についてはご利用時にご確認ください。

目次

1. セキュリティの取り組み

1.1. 所在地と法管轄

ラクネコのサービスは株式会社プロトソリューションが提供しています。当社は日本の法人であり、本店所在地は沖縄県です。ラクネコのサービスの開発、運用は全て日本国内で行っています。

ラクネコのシステムは、Amazon Web Service（AWS）を利用して構築しており、システムが保管するデータおよびそのバックアップデータは、AWSのデータセンターに保管されています。

AWSはアメリカを本拠地とする企業ですが、日本国内にもデータセンターを所持しており、ラクネコでは東京リージョンにデータを保存しています。メール送信やPush通知の配信に海外のリージョンを利用することはありますが、データの保管はすべて国内のリージョンを利用しており、海外のサーバーにお客様のデータを保管することはありません。

また、AWSとの契約においては準拠法を日本法としています。これにより、海外法の適用によるリスクを回避しています。

1.1.1. オフィスのセキュリティ

従業員には顔写真入りの社員証とカードキーを貸与しており、業務を行うオフィスにおいて入退室管理および監視などのアクセスコントロールを行っています。

1.2. 暗号化による保護

1.2.1. 通信の暗号化

ラクネコでは、通信内容を暗号化することで、データの漏洩や改竄を防いでいます。暗号化方式としてはTLS1.2以上を使用しております。

1.2.2. データの暗号化

ラクネコでは、システムに登録されたデータを保存する際に暗号化を行い、仮にバックアップデータが窃取されたとしても情報漏洩を防ぐ対策を行っています。暗号化アルゴリズムには AES-256 を用いており、秘密鍵はAWS Key Management Service（KMS）で厳重に管理しています。

1.2.3. パスワードのハッシュ化

ラクネコの利用者のパスワードは平文では保存せず、ハッシュ化して元の形に復元することが誰にもできないようにした上で保存しています。

1.3. データのバックアップと返却・削除

お客様がサービスをご利用いただく中で登録、および生成されたデータは、ラクネコのシステム上で保管されています。原則として保管期限の制限はなく、ラクネコのサービスが続く限り、データを確認することができるようになっています。

1.3.1. サービス側でのバックアップ

ラクネコのサービス側では、お客様のデータが失われることがないよう、データのバックアップを行っています。バックアップは複数のデータセンターで冗長的に保管しており、サービスに障害が発生した場合でも、バックアップから復旧できるように備えています。
バックアップは日次で取得を行なっており、10日間保管をしています。

1.3.2. お客様側でのバックアップ

ラクネコの管理画面から、必要に応じてデータをダウンロードすることができます。これを利用することで、お客様側でバックアップを取得することが可能です。

1.3.3. 解約時のデータの扱い

お客様がラクネコを解約された場合、契約期間終了後はラクネコのご利用ができなくなります。
必要に応じて契約期間終了前にデータのダウンロードを行なってください。
また、契約期間終了後1ヶ月以内を目安にデータは削除されます。

1.4. セキュリティを向上する機能

1.4.1. 多要素認証機能

ログイン時に従来のパスワードに加えて、SMSまたは認証アプリで発行された認証コードを用いた多要素認証をご利用いただけます。
基本機能のため、オプション料金は不要です。

1.4.2. アクセス元IPアドレスの制限機能

ラクネコの管理画面へのログインを、特定のIPアドレスからのアクセスのみ許可する機能をご利用いただけます。
基本機能のため、オプション料金は不要です。

1.5. 情報セキュリティインシデントの取り扱いと通知

1.5.1. 報告するインシデントの範囲

インシデントのうち、利用者に明確な被害が及んだり、もしくはラクネコのサービス継続に影響を及ぼすと判断したものを「重大インシデント」と定義し、これを報告するインシデントの範囲とします。重大インシデントの例には以下のようなものがあります。

- ラクネコのサービスへの不正アクセスにより、情報流出が起きた
- 社内システムのウイルス感染により、情報流出や業務停止が起きた
- 外部からの攻撃によりラクネコのサービスが利用不可能になり、その状態が一定時間以上継続した

1.5.2. インシデントの通知手順

重大インシデントが発生した場合には、以下の手段で通知いたします。

- 管理画面のお知らせ欄にて告知いたします。
- ホームページのお知らせにて告知いたします。
- 特定のお客様に影響を及ぼしたと判断した場合、個別にSlackや電子メール等でご連絡いたします。

1.5.3. インシデント通知までの目標時間

重大インシデントが発生した場合、可及的速やかにお客様に通知いたします。影響を受けたお客様に対し、インシデントの認知から24時間以内に通知を行うことを目標としています。

2. お客様にご注意いただきたい点

2.1. サービスの利用に必要な環境

ラクネコはSaaS（Software as a Service）型のクラウドサービスです。
サービスを利用するためにはインターネットに接続できる環境と、サービスでご利用いただく機能に応じてパソコンやタブレット端末、スマートフォンが必要になります。
サービスを利用する際には、タブレット端末やスマートフォンに専用のソフトウェアをインストールする必要があります。パソコンにおいてはWebブラウザのみでご利用いただけますが、特定の機能を利用する際に追加のソフトウェアが必要になる場合があります。

推奨環境の詳細はラクネコのマニュアルページをご確認ください。
https://raku-neko.jp/manual/recommended_environment/

2.2. お客様の環境におけるセキュリティ上の注意点

ラクネコのクラウドサービス側のアプリケーション、ミドルウェア、サーバー、ネットワーク機器については、当社の責任において管理と運用を行っており、お客様にてソフトウェアのアップデートを行う必要はありません。
一方で、お客様がインターネットに接続する環境、利用される端末（パソコン、タブレット端末、スマートフォン）、Webブラウザ、電子メールアドレス等については、お客様側でご用意いただく必要があります。これらの情報セキュリティについては、お客様にて管理いただく必要があります。

お客様側の環境について、特に以下の点についてご配慮ください。

- ネットワーク環境の安全性
- 端末の盗難防止策
- 端末OSのセキュリティアップデート
- Webブラウザのセキュリティアップデート
- その他のソフトウェアのセキュリティアップデート
- 電子メールの盗聴・傍受への対策
- 電子メールへのウィルス対策

2.3. お客様のパスワードの管理

ラクネコのパスワードはご利用になるユーザー本人を識別するために大切なものです。
ユーザーご自身で、他人に漏洩しないよう適切に管理を行ってください。

2.4. ログ調査

お客様側でのインシデント調査のために、ラクネコのログ調査が必要になるケースが考えられます。お客様のご要望に応じて情報提供することは可能です。ご要望の際はお問い合わせ窓口からご連絡ください。

[付録] セキュリティチェックシート

経済産業省「クラウドサービスレベルのチェックリスト」に基づいて、
独自に項目の追加を行いラクネコ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	規定内容	測定単位	回答
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 1～2週間前にメール／Slackカスタマーサポートチャンネルにて通知します。
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 タイミングは現状定めていませんが、事前にメール／Slackカスタマーサポートチャンネル／ホームページで通知します。
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 現状実施しておりません。
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%以上です。
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 システム、及びバックアップは複数のデータセンター施設にて構成されており、冗長化を図っています。
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	無 お問い合わせに応じて、データを抽出してお渡しするなど対応可能です。
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 CSVファイル
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 月1回アップデートを実施しています。 利用者に影響のあるアップデートについては事前にメール／Slackカスタマーサポートチャンネルにて通知しております。
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	約1時間となります。

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	2時間を目標としております。
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	サービス全体での障害件数は12件です。 対応に長時間（1日以上）要した障害はありません。
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 ハードウェア／ネットワーク／パフォーマンスの常時監視
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 障害発生時にはメール／Slackカスタマーチャンネルにて通知します。経過・解消のご連絡も同様に通知いたします。
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	1時間以内を目安にしています。
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)	1分間隔で収集しています。
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	サービスの停止時にはメール／Slackカスタマーチャンネルにて通知します。
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 操作ログを利用者の要望に応じて提供することは可能です。
19	性能	応答時間	処理の応答時間	時間(秒)	処理や画面により差異がありますが、平均0.5秒程度となります。
20		遅延	処理の応答時間の遅延継続時間	時間(分)	処理の種類によりますが、15秒～60秒でタイムアウトとなります。
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)	無
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 設定画面より項目配置や処理フローのカスタマイズが可能です。詳細はマニュアルをご覧ください。
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	無

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 状況に合わせてスケールアップ／スケールアウトするため上限はありません。
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	状況に合わせてスケールアップ／スケールアウトするため上限はありません。
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	基本的には平日9:00～18:00となります。 受付は電話／メール／Slackカスタマーサポートチャンネルとなります。
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	基本的には平日9:00～18:00となります。 受付は電話／メール／Slackカスタマーサポートチャンネルとなります。
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 日次でのフルバックアップを実施しています。
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り、データを保証する時点	時間	0時までを保証します。
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	10日間保管します。
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 データベースの情報は1ヶ月以内を目安にに削除します。 データについてはシステム上からCSVファイルのダウンロードが可能です。
32		バックアップ世代数	保証する世代数	世代数	10世代保管します。
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。 暗号化要件有の場合は方式（ツール名）及び、鍵管理ポリシー有無を記載 ※　通信/サイトとは別、保存データベース暗号化	有無/内容	有 通信時はTLS1.2以上、データはAES-256形式で暗号化し保護されます。
34		マルチテナントストレージにおけるキー	マルチテナントストレージのキー管理	有無／ 内容	無 利用企業間でのデータ分離

		管理要件	要件の有無、内容		は実施しておらず、アプリケーションレベルで制御を行なっています。
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 データは、データ所在地の司法権、コンテキスト、法規制、契約上の制約、価値、機微性、組織にとっての重要性、第三者のための保存義務、不正な開示や誤用の防止の諸観点に基づいて、機密区分されなければならない。	有無	無 保証や保険加入はありません。
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	有無／ 内容	有 システム上からCSVファイルでデータをダウンロード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	有 TLSによって改竄検知を担保しております。
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 アプリケーションレベルで不正な入力データの無害化を実施しております。
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、プライバシーマークを取得しています。
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	無 自社内でのWebアプリケーション脆弱性テストを年1回のペースで実施しています。
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 入退室管理された執務室で取り扱い、運用者は限定されております。
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	有無	有 TLS1.2以上を使用します。

			強度		
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（共有環境）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 アプリケーションレベルで制御を行なっています。
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 一般利用者は自身に関連性があるデータのみアクセスできるよう制限されています。 （管理者は全体のデータにアクセス可）
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管理ポリシー：ID作成から廃棄に至るアカウント資格情報のライフサイクル管理がされている	設定状況	有 IDは個人ごと付与されており、ログの検索に使用可能です。 保持期間は無期限となっています。 必要に応じてログの提供は可能です。 内容により変動はありますが目安は5営業日となります。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	有 ネットワークは物理的に分離されサービス専用のものとなっています。WAFを導入し不正なアクセスをブロックする仕組みを設けています。
48		二次記憶媒体の安全性対策	バックアップに限らず、二次記憶媒体の利用を許可するケースの有無、および利用許可する場合の手続きがあること 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	有無	有 バックアップはクラウド上に保管してあり、持ち出し可能な媒体に保管することはありません。

			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		
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 データ保存地は国内で、準拠法は日本法となっています。
50		特権アカウント管理	特権アカウント付与方針・手続き・運用	有無／設定状況	特権アカウントは特定の運用者のみ利用可能で、英数字記号を含めた複雑なパスワードを用いています。
51		脆弱性修正プログラム適用	脆弱性修正プログラム適用・手続き・運用	頻度/把握状況	脆弱性の修正が含まれるセキュリティパッチが自動的に適用されるようになっております。
52		データセンター事業継続管理と運用レジリエンス	データセンター設備および環境状況の定期的安全確認	有無／管理状況	クラウドの保安上の理由により具体的な場所は非公開となっておりますが、その安全性についての情報提供が行われています。 https://aws.amazon.com/jp/compliance/data-center/controls/