「楽楽明細　クラウドサービス」
セキュリティガイドブック

～ラクスが行っているセキュリティ対策のご説明及び
お客さまのご利用におけるセキュリティ上の注意点～

(株)ラクス　クラウド事業本部
TEL　：03-6675-3812
FAX　：0120-82-5348
Mail　：rakurakumeisai@rakus.co.jp
URL　：https://www.rakurakumeisai.jp/

20000843
JQA-IM1748

目次

■はじめに

この度は、弊社の「楽楽明細　クラウドサービス」のご導入検討を賜りまして誠にありがとうございます。

「楽楽明細　クラウドサービス」は、弊社が運用管理するサーバ機器に楽楽明細のソフトウェアをインストールし、インターネットを介してお客様にソフトウェアをご利用いただくサービスになります。

導入が簡単で、インターネットに繋がる環境さえあれば、いつでもどこでもご利用頂くことができる非常に利便性の高いサービスとなっております。

弊社では、「楽楽明細　クラウドサービス」をお客様に安心してご利用頂くために、様々なセキュリティ対策を施しております。

本書では、本書改定日時点でのセキュリティ対策内容についてご説明致しております。

■楽楽明細が機能として持つセキュリティ対策

―『ログイン ID とパスワードによるユーザ認証』

・ユーザ毎にそれぞれ異なるユーザ ID とパスワードが付与され、ログインをする際には、ユーザ ID 及びパスワードの両方が求められるようになっています。

―『IP アドレスによるアクセス制限』

・ グローバル IP アドレス単位でサーバへの HTTPS でのアクセスを制限することができるようになっており、お客さま事業所 LAN からしかアクセスできないようにすることができます。
※ 別途オプション料金が必要となります。

―『ユーザ単位での操作権限の制限』

・顧客情報を閲覧する権限やダウンロードする権限などユーザ毎に操作権限を設定及び制限できるようになっています。

―『操作履歴の記録』

・ どのユーザがいつどのような操作をしたかなどの履歴を記録する機能を実装しております。ユーザ ID や操作時刻、（アクセス元のグローバル）IP アドレスや操作内容などの記録を確認することができます。

―『暗号化通信』

・本サービスへのアクセスは、SSL/TLS を使った暗号化通信によって行うことができ、情報が暗号化されるため、安心してご利用頂くことができます

―『無操作状態での強制ログアウト』

・ユーザがログインし、何もせずに一定時間経過すると、自動的にシステムからログアウトすることが要求されるようになっています。これにより、ユーザが万一ログインしたまま席から長時間離れた場合でも第三者が不正に利用する危険性を減少させることができます。

―『パスワード変更』

・利用者は、ログイン時に入力するパスワードを簡単に変更できます。

－『マイページ２段階認証』

・マイページへのログイン時にログイン ID とパスワードによる認証に加え、確認コードを利用した２段階認証が可能になります。

※ 別途オプション料金が必要となります。

－『SSO』

・管理画面へのログイン時にログイン ID とパスワードによる認証の代わりに、SSO（シングルサインオン）でのログインが可能になります。

■楽楽明細における脆弱性診断

―『UBsecure 社 Vex(Vulnerability explorer)による脆弱性診断』

・ UBsecure 社の Web アプリケーション脆弱性検査ツール「Vex(Vulnerability explorer)」を使用して以下の検査を行い、情報漏洩・改ざん・なりすましに対して適切に対処しています。

○主な脆弱性診断項目

SQL インジェクション
OS コマンドインジェクション
クロスサイトスクリプティング
パラメータ操作
バッファオーバーフロー
セカンドオーダーアタック
クロスサイトリクエストフォージェリ（CSRF）
不要なファイルの検出
サーバの設定ミス
プロトコルの不適切な使用
エラーコード
セキュア属性のない Cookie
セッション管理に関する問題
その他既知の脆弱性

■サーバ運用・管理上のセキュリティ対策

―『管理水準の高いデータセンター』

・サーバを設置しているデータセンターは、下記のとおり、十分な災害対策や万全のセキュリティ対策が施されています。

▼データセンターの仕様

項　目		仕様内容
災　害	地震対策	・免震構造
	火災対策	・ 超高感度煙感知器 ・ N2（窒素）ガス消火設備設置
	室温対策	・冗長（N＋1）構成による空冷式空調システム
	漏水対策	・漏水検知システム設置
電　源	停電対策	・非常用自家発電設備装置の設置 ・冗長化された UPS 無停電電源装置
セキュリティ	侵入対策	・有人受付による入館者の身分証明書確認 ・生体認証及び IC カードによる入室制限

―『定期的なデータバックアップの実施』

・お客様データに関するすべてのデータのバックアップを取得しており、万が一、サーバが２台とも故障及び破損した場合でも、バックアップデータを用いてデータを復元させることができます。

―『緊急時に備えた機器の冗長化』

・サーバ機器やネットワーク機器についても、万が一の故障に備えて、冗長化しており片系の機器に障害が発生しても、サービスが停止しない環境を整備しております。

―『ネットワーク回線の冗長化』

・データセンターではバックアップ回線を用意しており、万が一、ネットワーク回線に障害が発生しても、サービスが停止しない環境を整備しております。

－『外部からの HTTP,HTTPS,SMTP 以外のプロトコルでのアクセス制限』

・ファイヤーウォールを設置し、HTTP,HTTPS,SMTP を除くプロトコルでの不正なアクセスを遮断しています。

－『ファイヤーウォールの冗長化』

・ファイヤーウォールは、万が一の障害に備えて冗長化構成となっております。

－『サービス監視』

・Web,Mail,DB といったサービスの提供に必要なプログラムが正常に応答しているかどうかの監視を常時行っており、万が一、異常が発生した場合には、運用管理責任者に警告通知が行われます。

－『ハードディスク空き容量の監視』

・サーバにおいてハードディスクの空き領域がある一定値より少なくなった場合には、運用管理責任者に警告通知が行われます。

－『ログ』

・各種サーバにおけるログを一定期間保存しており、不正なアクセスなどがあった場合には、解析を実施できるようになっております。

－『ソフトウェアの脆弱性対策』

・サーバにインストールされている各種ソフトウェアにおける脆弱性を発見・察知し、弊社がソフトウェアのアップデートが必要であると判断した場合には、動作検証を行った上でアップデートを実施致します。

－『サーバへのアクセス制限』

・サーバのメンテナンス作業は、限られた担当者が特定アクセス用端末を経由してのみ作業できるようになっており、弊社設備内からのみアクセスできる構成になっております。
作業時に必要となるアクセス用端末のログイン ID、パスワードは、厳重に管理しております。

■弊社におけるセキュリティ対策

－『プライバシーマーク認定』

・弊社では、2006 年 8 月にプライバシーマークを取得致しました。
　【認定番号】第 20000843 号

－『ISMS 認証』

・弊社では、2021 年 1 月に ISMS 認証を取得致しました。
　【認証機関】　一般財団法人　日本品質保証機構
　【認証内容】　ISO/IEC 27001:2013／JIS Q 27001:2014
　【登録証番号】JQA-IM1748

－『人的セキュリティ管理』

・すべての従業員と機密保持契約を取り交わしています。
・すべての従業員に対して定期的にコンプライアンスマニュアルを元に教育研修を行っています。

－『物理的セキュリティ管理』

・執務エリア毎に入退室のルールを策定し、外部の人間がオフィスに立ち入る際の管理を適切に実施しています。

－『パソコン及び端末管理』

・社員が利用するパソコンには、必ず Windows ログインパスワード設定を義務付けており、第三者による不正利用の防止を図っています。
・社員が利用するパソコンには、必ずウィルス対策ソフトをインストールし、ソフトウェアは確実に更新し、最新版を維持するようにしています。

－『インターネット及び E-MAIL 利用管理』

・社内パソコンからのインターネットアクセスや E メールの送受信は、すべてログを記録し、利用状況を監視・確認しています。

－『本サービスの利用管理』

・本サービスへアクセスできる社員及びアクセスできる情報は、サービスサポート担当者、設備運用業務担当者に限定した利用管理をしております。

■サービスご利用上のお願い

―『ユーザ ID、パスワードの漏洩防止』

・ユーザ ID、パスワード情報の漏洩には十分ご注意して頂くようにお願い致します。

―『パスワードの定期的な変更』

・簡単にパスワードの変更が可能ですので、定期的にパスワード変更を行うようにお願い致します。

―『転勤や退職時のユーザ ID 削除』

・転勤や退職などの事由により不必要となったユーザ ID が発生した場合には、速やかに削除するか、もしくはパスワードを変更するようにお願い致します。