楽dos.

一般財団法人京都工場保健会

「健康管理楽 dos.」のセキュリティ対策について

１．基本方針

「健康管理楽dos.」のクラウド提供環境および接続クライアントの通信・認証・権限・監視・データ保護・可用性を多層で実装し、法令・ガイドラインおよび弊会セキュリティポリシーに準拠した安全な運用を実施します。

２．環境について

（1）日本国内に所在するクラウド環境（Microsoft Azure 西日本リージョン）を利用したインフラを準備し、安全な運用を実施
（2）インターネットVPNおよびHTTPS暗号化通信による安全な経路確保
（3）SSL/TLS 1.3による通信データの暗号化
（4）クラウド提供環境を利用した資源の管理を行い安全に処分する手順を遵守

３．認証・アクセス制御

（1）四半期ごとのアクセス権限見直しによる権限管理の最適化
（2）個人ごとにユーザIDを作成し、必要となる権限のみを付与
（3）認証方法は、ユーザID、パスワードを使用し認証
（4）パスワードは英大文字・英小文字・数字・特殊記号の組み合わせで10文字以上。
またパスワードの入力に失敗した回数が一定回数（連続10回）を超えた場合、当該ユーザIDはロック
（5）二段階認証（認証コードを登録されたメールアドレス宛に送信）によるセキュリティ認証強化
（6）WAF(Web Application Firewall)による悪意あるHTTPリクエストの検知・遮断
（7）IDS/IPS(不正侵入検知システム)によるネットワーク上の不正アクセス検知・遮断
（8）金・土・日曜日の23:00-3:00の間に必要なセキュリティパッチを自動適用
（9）信頼性の高い認証局発行の証明書によるサーバなりすまし防止
（10）セキュリティイベントの常時監視と異常検知によるインシデント早期発見
（11）保存データおよび通信経路上のデータ暗号化によるセキュリティ強化
（12）適切なセッション（3時間）タイムアウトによる不正利用防止

４．運用監視・ログ対応

（1）システム（Azure環境、データベース）のバックアップを日次で取得し、最大1年間保存
（2）初動対応、封じ込め、根本原因分析、是正・再発防止までのプロセスを整備

（3）ログの取得・保管・開示

セキュリティインシデント調査や監査対応のため、以下のログを定期的に取得し保管します。各種ログについては、ユーザからの要請に基づき、適切な範囲で開示します

・アクセスログ（ユーザ認証、操作履歴）

・マルウェア対策ソフトのログ（検知・隔離記録）

・システムログ（サーバ稼働、エラー記録）

・ネットワークログ（通信記録、WAF/IDS/IPS検知記録）

（4）本サービスはAzureが提供するサービスを用いて時刻を同期し、日本時間（JST, UTC+0900）で管理

（5）弊会では情報セキュリティの有効性を確認するために、独立した別部門による内部監査を年 1 回実施しています。監査結果についてはユーザからの要請に基づき、適切な範囲で開示します

5．情報セキュリティ事象への対応

（1）ユーザの業務継続をサポートするため、IT のインシデントについて、優先度ごとに設定した「対応開始までの時間」および「解決目標時間」内での解決を図ります

（2）インシデント発生から解決まで計測・評価できることを前提として、以下のとおり目標設定します

優先度	優先度の定義	対応開始までの時間	解決目標時間	対応時間	状況報告	通知方法
緊急	業務全体に支障をきたす問題	10 分以内 （サービスデスク窓口時間帯） 60 分以内（上記時間帯以外）	8時間以内	24H×7Days	1 時間ごと	ログイン画面 （お知らせ欄） 弊会HP
重要	部分的に支障をきたす問題	3 時間以内	1 営業日以内	9-16×月～金	1 日ごと	ログイン画面 （お知らせ欄）
軽微	ただちに対応が必要でない問題	1 日以内	1 週間以内 （5 営業日）	9-16×月～金	1 週間ごと	ログイン画面 （お知らせ欄）

（注） 対応時間：9-16 = 9 時～16 時

優先レベルについては、インシデントが業務へ及ぼす影響や範囲をもとに決定します。

なおサービス利用者の責任者と IT サービスマネジャー間の合意によって、優先レベルを都度変更する場合があります。

（3）確認できた情報セキュリティインシデントがユーザに重大な影響を及ぼす可能性がある場合、ユーザからの要請に基づき、該当するログおよびドキュメント類を適切な範囲で開示します

6．データの処分・再利用について

（1）顧客データの保持期間と廃棄

保持期間終了後、顧客に関係する全てのデータは完全消去され復元不可能な状態とします

（2）解約の申し込みを頂いた場合は、解約希望月末日より30日以内に関係する全てのデータを削除します。ただしバックアップデータについては最長1年間保持します

（3）監査・証明については、データ消去完了後、消去証明書を発行し、年1回以上、第三者監査機関によるデータ処分プロセスの監査を実施します

（4）顧客からの要請に応じて消去証明書を提示します

７．改版履歴

版数	日付	変更内容
1	2025/8/11	初版
2	2026/2/1	クラウド環境におけるデータの処分、再利用について など追記
3	2026/4/17	リージョン表記、クロック同期、情報セキュリティ事象への対応、内部監査 など追記

本件に関します、お問合せについては、以下の宛先までご連絡ください。

問合せ先：**rakudos-support@hokenkai.jp**

Webお問合せフォーム ：**https://kyotokojohokenkai.jp/form/contact_rakudos/**