結核研究所対策支援部保健看護学科
2026.04.01

「eDOTS 飲みきるミカタ」のセキュリティ対策について

2026 年 4 月にリリースした「eDOTS 飲みきるミカタ」では、利用者の重要かつ機密性の高い服薬情報を守るため、厚生労働省のガイドラインに基づいた多層的なセキュリティ対策を講じています。

1. 信頼性の高いインフラ基盤

・国内データセンター事業者の基盤採用: 国内データセンター事業者である「さくらインターネット」の VPS（仮想専用サーバ）を採用しています。
・物理的な安全管理: 厳格な入退室管理が行われている国内データセンターにて運用されています。

2. 通信とアクセス環境の保護

・常時暗号化（SSL/TLS）: すべての通信は最新の技術を用いて暗号化されており、第三者による情報の盗聴や改ざんを防止します。
・WAF の導入: 外部からのサイバー攻撃（DDoS 攻撃等）をリアルタイムで遮断する WAF を標準装備しています。
・接続制限: 不要な通信ポートを閉じ、攻撃リスクを最小化しています。

3. アカウント管理と認証

・二要素認証機能: 二要素認証機能は実装済みであり、運用設定により有効化可能です。
・二要素認証運用: 現時点では、利用者の利用環境およびアクセシビリティに配慮し、全利用者一律の必須化は行っていません。

4. データの保全と監視体制

・多世代バックアップ: データを物理的に分離された安全なオブジェクトストレージへ定期的にバックアップし、数世代にわたって保持しています。
・24 時間 365 日のログ監視: リアルタイムログ監視システムを導入し、不審な挙動やシステムの異常を即座に検知・通知する体制を整えています。
・データアクセス管理: 個人情報および医療情報へのアクセスは、業務上必要な権限を有する担当者に限定し、アクセス状況を記録しています。
・利用終了後の取扱い: 利用終了後は、法令・契約・監査上保管が必要な情報を除き、所定の手順に従って個人を特定できる情報を削除します。