2.「医療情報システムの安全管理に関するガイドライン」に関する取り組み

(1) 基本的な考え方

HASTOS / POST.exサービスは、健診標準フォーマットの CSVファイルに変換することを目的とするサービスであり、健診機関・医療機関等から送信された健康情報・医療情報を保存（外部保存）並びに管理することはありません。
健康情報・医療情報等を直接的に取り扱う医療機関等において、厚生労働省の「医療情報システムの安全管理に関するガイドライン第6.0版（令和5年5月）」を遵守した運用規定等が定められ、HASTOS / POST.exサービスの利用者（操作者）へのセキュリティ教育等が実施されていることをサービス提供の前提としています。

---

(2) 取り組み

1) 保守対応等に対する安全管理措置

a) 保守等

HASTOS / POST.exサービスは、日本医師会総合政策研究機構が契約する国内データセンター内に設置した物理サーバ（HASTOSサーバ）を使って運用しています。
システム保守にあたっては、作業するPC端末並びに担当者を限定し、HASTOSサーバには VPN接続によりアクセスする仕組みとしています。なお、システム管理者によって行う作業は以下に限定し、データベースの閲覧やファイル送信等は行いません。

- 不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等の更新作業
- バックアップファイルの確認と必要に応じての退避
- アクセスログの確認と必要に応じての退避
- HASTOS / POST.exサービスを提供するためのアプリケーションの保守（バージョンアップ等）
- HASTOS / POST.exサービスのダッシュボード監視（POST.ex 変換ログの監視・エラー有無の確認を含む）

セキュリティ上の理由から、ネットワーク・ハードウェア・ソフトウェアの構成詳細は公開できません。

b) 運用管理等

HASTOSサーバは、プライベート型ブロックチェーンを基盤として構築しています（パブリック型でないため、外部からは閲覧できません。）。複数台の物理サーバがそれぞれデータを保持し、リアルタイムで同期することにより、サービスの可用性と保存性を確保しています（全てのサーバが同時にダウンしない限り、HASTOS / POST.exサービスの提供を継続でき、かつデータが失われることはありません。）。
複数台の物理サーバの一部は外部ネットワークに接続していません。サイバー攻撃等の非常時には、外部から侵入できない物理サーバを使ってデータを含めて迅速に復旧します。

2) 物理的安全管理措置

a) サーバルーム等

HASTOSサーバは、日本医師会総合政策研究機構が契約する国内データセンター内に設置します。
セキュリティ上の理由から、物理サーバの設置場所は公開できません。

保守等に用いるPC端末は、事務局が業務委託するアルファインターナショナル株式会社のサーバルームの システムラック内に設 置し、施錠管理します。
なお、システムラック内に設置するPC端末には、健康情報・医療情報等は保存していません。

b) バックアップ

HASTOSサーバは、プライベート型ブロックチェーンを基盤として構築しています。複数台の物理サーバがそれぞれデータを保持し、リアルタイムで同期すること、ハッシュチェーンを使った改ざん検知と自動復旧を行うことで高い保存性と真正性を実現しています。
加えて、外部ネットワークに接続していない物理サーバを使い、HASTOS / POST.exサービスを停止することなく、定期的にデータベースを自動バックアップしています。

3）ネットワークに関する安全管理措置

オープンネットワークを使用します。セキュアなネットワーク要件を確保するため、TLS1.3 でのHTTPS接続（ネットワーク回線の暗号化）とし、クライアント証明書を利用した TLS クライアント認証を必須とします。
ネットワークを使って送受信する健康情報・医療情報は全てバイナリファイルとして扱い、ネットワーク送受信時には難読化しています。

4）認証・認可に関する安全管理措置

a）認証・認可

利用者IDとパスワードによる利用者認証を使用します。利用者IDとパスワードは、HASTOS / POST.exサービスを利用する医療機関等においてガイドラインを遵守して管理されることを前提とします。
パスワードは暗号化して管理していますので、利用者による変更後のパスワードに関する問い合わせには対応できません。パスワードの再設定は、医療機関等の担当者からシステム運営を担う健診標準フォーマット管理事務局（以下、事務局）への正式な依頼と利用者の確認手続きの後に行います。

b）アクセス権限

HASTOS / POST.exサービスを使って送受信した全てのデータは、送受信時に設定した送信機関と受信機関の利用者ID以外からの操作を受け付けない認可の仕組みが組み込まれています。加えて、データは暗号化したうえで管理しています。
ファイルを物理サーバのファイルシステムやオブジェクトストレージを使って管理することはありません。そのため、システム管理者等が閲覧する、サイバー攻撃等で外部に流出するといったことはありません。

c）データの確定

利用者IDによるアクセス権限の確認後、送受信したデータへの操作を認可する仕組みとなっています。操作の記録（証跡）は全てプライベート型ブロックチェーンに格納し、送信機関と受信機関の双方から閲覧できる仕組みとなっています。加えて、ブロックチェーンを使って操作の記録を管理することにより、証跡の改ざん耐性を高めています。
データは不要になった時点で自動的に物理削除する仕組みとなっており、削除操作の記録も送受信と同様の方法で管理しています。

d）利用者IDの作成と定期的な棚卸

HASTOS / POST.exサービスの利用申込後、健診標準フォーマットへの変換設定の完了後に利用者IDを払い出します。
利用状況を定期的に確認し、利用中止の申し出があった場合、利用者IDを「利用不可」の設定に変更します。

5）電子署名・タイムスタンプ

HASTOS / POST.exサービスの利用者による操作（証跡）には電子署名が付されます。プライベート・ブロックチェーンにタイムスタンプを付して操作記録を保存することで、監査可能性を確保します（利用者による操作のたびに電子署名とハッシュチェーンの検証を実行します。）。

6）医療機関等における利用機器・サービスに対する安全管理措置

事務局は、医療機関等に「医療情報システムの安全管理に関するガイドライン」の「システム運用編」の 安全管理措置を遵守す ることを要請します。

HASTOS / POST.exサービスは、送信機関と受信機関に 1つの利用者IDを払い出します。また、利用するPC端末（Webブラウザ）を限定することを基本としており、複数のPC端末（Webブラウザ）から操作を行った場合に確認用のダイアログが表示される仕組みとなっています。