神奈川県マイＭＥ-ＢＹＯカルテ
セキュリティポリシー

平成２９年４月１日

神奈川県

目次

1　総則

1.1 目的

本セキュリティポリシーは、神奈川県が「神奈川県健康・医療情報プラットフォーム」及び「神奈川県マイＭＥ－ＢＹＯカルテ」の実証又は試行を行うにあたり、本システムの運用と管理の安全にかかわる基本事項を規定し、本システムの安全かつ適正な管理を図ることを目的として定める。

1.2 適用範囲

本セキュリティポリシーは、本システムの運用と管理に係る事項に適用する。

2　定義

次に掲げる用語の意義は、以下の各号に定めるところによる。

(1)神奈川県健康・医療情報プラットフォーム

「神奈川県健康・医療情報プラットフォーム」(以下、「本システム」という。)とは、神奈川県が構築・運営する、個人の健康・医療情報等を保存・管理するデータベースをいう。

(2)マイＭＥ-ＢＹＯカルテ

「マイＭＥ-ＢＹＯカルテ」とは、神奈川県が提供する、本システムに個人個人利用者が登録・提供した健康・医療情報等を利活用するサービスをいう。

(3)サービス事業者

「サービス事業者」とは、神奈川県の実証事業の委託を受けた者で、本システムの利用申請をし、神奈川県がその申請を承諾した者をいう。

(4)運営事務局

「運営事務局」とは、実証事業の広報活動、個人利用者の募集や、個人利用者の登録、問い合わせ対応といった運営業務を行う組織をいう。

(5)記録媒体

「記録媒体」とは、データを記録するための媒体をいう。例えば、磁気テープ、フロッピーディスク、ハードディスク、USB メモリ、CD-R、DVD-R などをいう。

3　管理体制

3.1 責任者の選任と管理体制

(1)事業管理者

本システム統括責任者をこれに充てる。

(2)事業実施責任者

事業管理者が選任する者を、事業実施責任者に充てる。

事業実施責任者は、正副の任命を妨げない。

本事業の運営が円滑に執り行われるよう各種調整業務を行う。

(3)運用管理責任者

事業管理者が選任する者を、運用管理責任者に充てる。

運用管理責任者は正副の任命を妨げない。

本事業の円滑な推進を目的として、本システムの運用管理業務に責任を持つ。

(4)システム運用管理者

運用管理責任者が選任する者を、システム運用管理者に充てる。

本システムの運用が適切に行われるように、運用管理業務を行う。

3.2 運営事務局の設置

(1)運営事務局は、以下のサービス事業者個人利用者向けのサポート業務を行う。

①個人利用者の登録

②本システムの利用に関する問い合わせへの対応

③よくある質問事例集の作成

(2)運営事務局のサービス事業者、個人利用者向けサポート日と時間は、以下のとおりとする。

８：30～17：15(土日祝日除く平日)

(3)運営事務局の場所等

名称　　：神奈川県政策局ヘルスケア・ニューフロンティア推進本部室

住所　　：神奈川県横浜市中区日本大通り１

電話　　：045-285-0196

フォームメール：http://www.pref.kanagawa.jp/cnt/f532715/p1118903.html

3.3 災害・事故対策体制

運用管理責任者は、緊急時及び災害時の連絡、復旧体制等を定め、文書化し、運用管理にかかわる関係者に周知を行う。

3.4 教育・訓練

(1)運用管理責任者は、本システムの取扱いについてマニュアルを整備し、運用管理にかかわる関係者に周知を行う。

(2)運用管理責任者は、本システムの運用にかかわる関係者に個人情報の保護に関する教育を行う。

(3)運用管理責任者は、本システムを利用するサービス事業者の責任者がその所属員に行う個人情報保護に関する教育に関し、協力の依頼があった場合に協力する。

3.5 運用管理規程などの整備

運用管理責任者は､本システムに係る運用管理規程などを整備し安全かつ円滑な運用を図る。

4　データセンター設備及び本システムの安全管理事項

4.1 データセンターの設備環境

本システムの主要な機器であるサーバ等を設置するデータセンター要件は下記を満たす。

(1)1981 年の建築基準法に規定する構造耐力等の基準に適合しており、高い耐震性を有していること。

(2)浸水・漏水対策が施されていること。

(3)2 系統以上の安定した電源供給設備を有し、冗長化された自家発電設備、非常用電源設備(UPS)を備えていること。

(4)冗長化された空調設備を有すること。

(5)建築基準法に規定する防火区画であり、消防法施行令に規定した自動火災報知器及び消火器を有していること。

(6)本システムの構成機器はデータセンター内のセキュリティ区画に設置すること。

(7)セキュリティ区画は、常に施錠され、事務室等から隔離されていること。

(8)セキュリティ区画は、作業者を監視可能な監視カメラを備え、録画できること。

(9)サーバ等の情報機器は、ラックの施錠等により許可された者以外はアクセスできない構造であること。

(10)データセンター セキュリティ ガイドブック Ver 1.0（日本データセンター協会作成）の基準に適合していること。

(11)ISO9001 品質マネジメントシステムを取得していること。

(12)ISO14001 環境マネジメントシステムを取得していること。

(13)ISO/IEC20000 IT サービスマネジメントシステムを取得していること。

(14)ISO/IEC27001 情報セキュリティマネジメントシステムを取得していること。

4.2 データセンターの入退管理

(1)データセンターへの入退室は事前に入退室者登録を行い、許可された者のみができる。

(2)入退室が許可されていない外部の者は、システム運用管理者の許可があり、入退室が許可された者の同行時のみ許可される。

(3)データセンターへの入退者は、入館許可書を着用し、入退の記録を残すこととする。

(4)本システムの主な構成機器は、データセンター内のセキュリティ区画内に設置する。

4.3 データセンター設備の保守点検

保守点検のため、本システムの利用に影響を生じる場合は、予め日程と時間を本システムの個人利用者に伝える。

4.4 データセンターにおけるシステムの運用監視

(1)安全かつ正常な稼働を維持するため、データセンターにおけるシステムの運転状態を常に監視する対策を実施し、異常な動作、不適切なアクセス等の検知に努める。

(2)データセンターにおけるシステムの運用監視は、生死監視、システムアプリケーション応答監視を行う。

(3)ファイアーウォールのアクセスログの定期的なチェックを行う。

4.5 ネットワークの管理

(1)システム運用管理者は、安全かつ正常な稼働を維持するため、ネットワークの稼働状態を常に監視する対策を実施し、異常な動作、不適切なアクセス等の検知に努める。

(2)システム運用管理者は、定期的にアクセスログの収集を行い、アクセスログを保管するよう努める。

(3)利用するネットワークは、サービス事業者では、セキュアなネットワークを利用することを強く求める。具体的には、次のとおり利用することを強く求める。

・医療機関等が発生源となる個人情報を含む医療情報であると考えられる情報を扱う接続に対しては、接続先を限定する閉域網(IP-VPN)または、「医療情報システムの安全管理に関するガイドライン　第 4.2 版　6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」で確実に安全性を確保するために必要とされている IPSec＋IKE 方式の VPN ネットワークを利用する。

・一方、個人が自身において情報を入力するなど、それ以外の情報に対しても、

一定の安全な環境を求め、情報の暗号化を行う SSL 通信を利用する。
・個人利用者においては、情報の暗号化を行う SSL 通信を利用する。

4.6 個人利用者のアクセス管理

(1)本システムへアクセスする場合は、インターネットに接続できる端末を用いる。
(2)本システムで提供される情報は、同意した個人利用者の情報のみ、本人が閲覧できる。

4.7 記録媒体の管理

(1)システム運用管理者の許可を得た場合を除き、本システムで提供される情報を CD、USB メモリ等の記録媒体への複製を禁止する。
(2)許可を得た場合において、本システムで提供される情報が格納された記録媒体を、システム運用管理者は施錠付キャビネット等に保管し、台帳に記録し、管理する。

4.8 情報の廃棄

(1)紙媒体の廃棄は、シュレッダーによる粉砕処理を行う。大量廃棄する場合は、溶融廃棄証明書を受領することで、外部業者に委託することができる。
(2)記録媒体の廃棄は、原則粉砕処理を行う。
(3)粉砕処理をしない PC 等は、再生ができない方法で情報を消去する。なお、消去証明書を受領することで、情報の消去処理を外部業者に委託することができる。
(4)情報を廃棄する場合は、システム運用管理者が立ち会いの上、廃棄・消去作業を確認する。

4.9 情報のバックアップ

(1)サーバのシステムファイル及び情報のバックアップを自動または手動で実施する。
(2)バックアップの作業に当たる者は、その作業の記録を残す。
(3)バックアップスケジュールは、日次は差分バックアップを行い週次でフルバックアップを行うこととする。その他セキュリティ上必要となるバックアップを行うこととする。

4.10 サービス事業者、個人利用者等の責務

(1)サービス事業者の責任者は、自組織内の個人利用者に本システムを正しく利用するための教育・指導をする責務がある。
(2)サービス事業者、個人利用者は、本セキュリティポリシーのほか、神奈川県の定める個人情報保護方針とその他法令等を遵守し、本システムを適正に利用しなけれ

ばならない。

(3)本システムで提供される情報は、本システムの利用目的以外で、複製・公開・提供してはならない。

(4)サービス事業者、個人利用者は、情報セキュリティに十分注意するとともに接続情報を他の者に利用させてはならない。

(5)サービス事業者、個人利用者は、セキュリティを維持するため、本システムに接続する端末にウイルス対策ソフトを導入し、常に最新のウイルス定義に更新しなければならない。

4.11 接続情報の管理

(1)接続情報の交付を受けたサービス事業者の責任者、個人利用者は、接続情報を適切に管理するとともに、あらかじめ定めた一定期間で更新する。

(2)サービス事業者の責任者、個人利用者は、接続情報を紛失した時は、速やかに神奈川県に届け出て、所定の手続きをしなければならない。

4.12 接続情報の取り消し

神奈川県は、接続情報の交付を受けたサービス事業者の責任者、個人利用者が次の事項のいずれかに該当した場合は、接続情報の取り消しをすることができる。

(1)法令等に違反した時。

(2)情報の取扱いが不適切であり、指導又は警告にもかかわらず改善が認められない時。

(3)その他神奈川県が、リスクがあると判断した時。

4.13 インシデント管理

(1)事故への対応について

セキュリティ事故発生時は、直ちにシステム運用管理者に報告の上、各関連部門に連絡すること。

(2)不正アクセス被害発生時

①被害のあったデバイスをネットワークから切断する。デバイスが通信を行っていた当該サーバの電源は落とさず、システム起動した状態に保つ。また、当該サーバに対して不用意に操作は行わない。

②直ちにシステムシステム運用管理者へ状況を報告する。

③システム運用管理者より運用管理責任者へ連絡し、対処の指示を仰ぐ。

(3)ウイルス感染時

①直ちに感染したＰＣをネットワークから切断する。

②直ちにシステム運用管理者へ状況を報告する。

③システム運用管理者より運用管理責任者へ連絡し、対処の指示を仰ぐ。

④情報漏洩につながる可能性のある場合またはつながる場合は、適切な部門及び組織に連絡する。

(4)PC、記録媒体などの盗難時の対応

①最寄りの警察に盗難届けまたは遺失届を出す。

②VPN を利用していた場合は、接続情報の変更及び通信カードキャリアへのサービス停止依頼を行う。

③格納データの確認を行い、システム運用管理者に報告する。

④個人利用者に関する情報が含まれている場合は原則、事業管理者より適切な部門及び組織に連絡する。

(5)業務委託会社に起因する場合の対応

事故または事件が業務委託会社に起因する場合は、直ちにシステム運用管理者へ状況を報告し、システム運用管理者は委託契約に基づいて対応を行う。

5　情報の取扱い及び利用範囲

5.1 本システムでの情報の取扱い

(1)本システムが保存する情報は、複製情報として取り扱うものとし、情報の原本は情報を作成した者が法令に従い別途管理する。

(2)本システムが取り扱う複製情報の内容は、事業管理者、事業実施責任者、運用管理責任者、システム運用管理者、サービス事業者等において、その完全性、正確性、適用性、有用性等のいかなる面からの保証をするものではない。

5.2 本システムにおける情報の利用範囲

本システムで収集した情報を、神奈川県は、別に定める利用目的の範囲内で利用することができる。神奈川県は、本セキュリティポリシーに沿って運用する以上、個人が識別できる情報が公表されないよう努める。

6　業務委託の安全管理

6.1 委託契約における安全管理

業務を外部に委託する場合は、委託契約書に以下の措置を実施する。

(1)委託契約書には、守秘事項を含むものとし、契約先の契約署名者は代表者とする。

(2)委託契約書には、再委託先に関する事項を加える。

(3)委託契約書において、サービス提供にあたって保証する品質と事故・障害等が発生した際の補償について明確にする。

6.2 再委託の安全管理

委託先が、委託業務を外部に再委託する場合は、本セキュリティポリシーと同等の個人情報保護、安全管理に関する対策及び契約を行うものとする。また、神奈川県の求めに応じて速やかに情報管理の状況等が、委託先から提出されるものとする。

7　セキュリティポリシーの公開

本セキュリティポリシーは、本システムを利用するサービス事業者、個人利用者及び本システムの運営と構築等に係わる組織とその関係者に公開するものとする

8　セキュリティポリシーの見直し

神奈川県は、本セキュリティポリシーを、本システムを利用するサービス事業者及び個人利用者等からの苦情、緊急事態の発生、神奈川県の設置する会議、その他からの指摘等で、システムの機能、運用状況等に問題がある場合には、必要な是正の実施及び予防の実施を行うため事前の了解なく本セキュリティポリシーを見直すことがある。

9　セキュリティポリシーの施行日

本セキュリティポリシーは、平成２９年４月１日より施行する。

以上