資料31

情報公開･個人情報保護審議会　諮問・報告事項

件名	新型コロナウイルス感染者等情報把握･管理支援システム（ＨＥＲ－ＳＹＳ）に係る外部結合について（変更）

内容は別紙のとおり

条例の根拠

【報告】
　◇第 17 条第 1 項第 2 号（法令等に基づく外部電子計算機との結合）

（担当部課：健康部保健予防課）

事業の概要

事業名	新型コロナウイルス感染者等情報把握・管理支援システム（ＨＥＲ－ＳＹＳ）について
担当課	保健予防課
目　的	感染症の予防及び感染症の患者に対する医療に関する法律（以下、「感染症法」という。）に基づく積極的疫学調査において、新型コロナウイルス感染者等情報把握・管理支援システム（以下、「ＨＥＲ－ＳＹＳ」という。）を利用することで、広域的に行政及び医療機関等の情報を共有し、その事務の簡略化及び感染症予防に係る政策立案の迅速化を図る。
対象者	新型コロナウイルス感染症患者
事業内容	１　概要 区では、新型コロナウイルス感染拡大防止の観点から、全国一律で運用されているＨＥＲ－ＳＹＳを活用して、新規感染者の情報管理等を行ってきた（令和２年度第４回情報公開・個人情報保護審議会了承済）。 この度、ＨＥＲ－ＳＹＳとの外部結合について、感染症法等に基づき、以下の変更を行ったこと、また行うことを報告する。 ２　変更点 （１）情報項目の追加 令和３年１月から７月にかけて、ＨＥＲ－ＳＹＳにおいて管理される新規感染者情報に「新型コロナウイルスワクチン接種歴」や「変異株ＰＣＲ／ゲノム解析結果」等の情報項目が追加された。 （２）医療機関等（健康フォローアップ機関）へのＩＤ付与の実施 自宅療養者に対する健康フォローアップ（定期的な体温や酸素飽和度の確認など）をより迅速に行うため、区から医療機関等（健康フォローアップ機関）へ、ＨＥＲ－ＳＹＳにアクセスするためのＩＤを付与する。 ＩＤ付与を行うことで、医療機関等（健康フォローアップ機関）は、ＨＥＲ－ＳＹＳを活用して、担当する感染者の健康情報を確認することができるようになり、今まで以上に切れ目のない対応を行っていくことが可能となる。 ３　対象者数 約５００名を想定 ＨＥＲ－ＳＹＳに係る個人情報の流れは、資料３１―１のとおり

別紙（電子計算機の外部結合関係）

◇法令等に基づく外部との結合（第17条第1項第2号関係）・・・報告事項

件名　新型コロナウイルス感染者等情報把握・管理支援システム（HER－SYS）に係る外部結合について（変更）

※太字ゴシック（下線）が、令和２年度第４回本審議会了承済の内容からの変更箇所

保有課（担当課）	保健予防課
登録業務の名称	新型コロナウイルス感染者等情報把握・管理支援システム（ＨＥＲ－ＳＹＳ）の外部結合について
結合される情報項目（だれの、どのような項目か）	対象者：新型コロナウイルス感染症患者 情報項目：**資料３１―２のとおり** **※情報項目を追加した。** **※医療機関等（健康フォローアップ機関）へ、ＨＥＲ－ＳＹＳにアクセスするためのＩＤ付与を行う。**
結合の相手方	国（厚生労働省）
結合する理由	新型コロナウイルス感染拡大防止の観点から、効率的に患者等に関する情報を収集し、地域の関係者あるいは必要に応じて地域外の関係者の間での情報共有が必要である。広域的に、正確な情報を共有するために、各々の情報について当該システムを介して外部結合する必要があるため。
結合の形態	利用端末からインターネットを経由して、クラウドの上に構築された、当該システムにアクセスすることで利用する。（ただし、データのダウンロードについては、ＬGWAN回線を利用する。）
結合の開始時期と期間	令和２年８月３日から（以降も、同様の外部結合を行う。） **（医療機関等（健康フォローアップ機関）へのＩＤ付与は、本審議会了承日以降に実施する。）**
情報保護対策	【ＨＥＲ－ＳＹＳにおけるセキュリティ対策】 セキュリティ対策について、国より、以下の情報保護対策を行っていることを確認した。 １　運用上の対策 （１）個人情報保護 「個人情報保護法」を遵守し、「政府機関等の情報セキュリティ対策のための統一基準」及び「IPA（独立行政法人　情報処理推進機構）のガイドライン」に準ずることとし、準拠性を第三者機関により確認している。 （２）システム運用事業者にかかる体制 情報セキュリティ管理者を設置し、セキュリティ対策に係る事務を統括 （３）情報セキュリティに対する教育 システム運用事業者は、情報セキュリティに関する社内教育を実施 （４）入退室管理 データ保管場所について、施設の周辺、建物の内部等、それぞれでセキュリティ保護が用意されており、建物内への不法侵入等を防止 ２　システム上の対策 （１）ユーザ認証（ユーザ ID、パスワード、ワンタイムパスワード） （２）ウェブアプリケーションファイアウォールの設置 （３）クラウドのマネージドサービスを活用した、DDoS 対策、ログ管理等 （４）通信データ・DB 暗号化

	（5）セキュリティ・稼働監視を行い、異常等に瞬時に自動対処を行うプログラム適用 （6）アクセス制御（ユーザ登録されていない者のアクセス不可・役割ごとのアクセス制限） （7）ウイルス対策 （8）サーバ監視・サーバの脆弱性検査 【区におけるセキュリティ対策】 1　運用上の対策 （1）「新宿区個人情報保護条例」及び「新宿区情報セキュリティポリシー」の遵守 （2）区によるユーザ情報の管理（職員、医療機関、感染者等の情報を台帳で管理） （3）以下の運用により、二段階認証を行う。 ア　携帯電話の場合 ①　サイトにアクセスし、ユーザ ID とパスワードを入力する。 ②　あらかじめ登録した携帯電話番号あてにショートメール（ＳＭＳ）で認証コード（6桁の数字）が送られる。 ③　認証コードを入力することで、ログインが完了する。 イ　固定電話の場合 ①　サイトにアクセスし、ユーザ ID とパスワードを入力する。 ②　あらかじめ登録した固定電話番号あてに、電話（音声ガイダンス）がかかってくる。 ③　固定電話の「＃」ボタンを押すことで、自動的に認証され、ログインが完了する。 2　システム上の対策 （1）ユーザ認証（ユーザ ID、パスワード、認証コード、電話認証） （2）不正侵入検知システム（IDS）、不正侵入防止システム（IPS）の設置 （3）Web 脆弱性攻撃防止(WAF) （4）標的型攻撃対策 （5）ふるまい検知・通報･遮断･通信制御(特定通信のみ許可) （6）対象者データ（エクセル）へのアクセス制御及びパスワード設定 **（7）医療機関等（健康フォローアップ機関）へのＩＤ付与にあたっては、感染者ごとにＩＤを付与し、担当する医療機関等（健康フォローアップ機関（当該機関のグループの事業者含む））のみが、当該感染者情報を閲覧・入力できるようにする。** **（8）医療機関等（健康フォローアップ機関）へのＩＤ付与にあたっては、パスワード付きのメールにて行い、１件ずつ送付する。**