

HER-SYS はなにが問題だったか — 先行導入, 本導入, 改修提案を 振り返って —



日野麻美 | 港区総務部情報政策課,
みなと保健所保健予防課兼務

みなと保健所に兼務発令

本稿では、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: Health Center Real-time Information-sharing System）の導入経緯を振り返り HER-SYS は何が問題であったかを解説します。すでに多くの記事が公開され経緯は広く知られていますが、ゼロトラストネットワークモデル上で大量の要配慮個人情報扱う大規模システムの初のケースであったことにも起因しているように思います。それについても本稿の最後に触れたいと思います。

経緯を振り返るにあたり、システム化対象業務を押さえて考えるため、保健所の感染症対策業務の概要を説明します。

2020年4月20日、みなと保健所への兼務辞令を受け、新型コロナウイルス感染者の発生届対応や医療費の公費負担事務（コロナの入院費用は医療保険と税金でまかなわれ、患者さんの個人負担はありません）に従事することになりました。

感染症法とは人権を守る法律

感染症の予防および感染症の患者に対する医療に関する法律（感染症法）の前文の一節には「我が国においては、過去にハンセン病、後天性免疫不全症候群等の感染症の患者等に対するいわれのない差別や偏見が存在したという事実を重く受け止め、これを教訓として

今後に生かすことが必要である。このような感染症をめぐる状況の変化や感染症の患者等が置かれてきた状況を踏まえ、感染症の患者等の人権を尊重しつつ、これらの者に対する良質かつ適切な医療の提供を確保し、感染症に迅速かつ適確に対応することが求められている」との記述があり、着任時の簡単な研修の中で保健所長と感染症対策担当の課長補佐からこう言われました。

「感染症対策は、過去の経験を活かし、人権尊重が重要な柱となっています。積極的疫学調査は、感染者との信頼関係に基づいて行われるものです」

着任前、感染者の個人情報取り扱いを整理して、庁内周知するために感染症法や公衆衛生入門書を読み込んでいたこと、研修で得た「人権擁護」と「信頼」というキーワードが、後に HER-SYS の適法性やリスク対策を判断する上での基準、大きな武器となりました。

発生届を起点とした事務の概要

感染症法第12条に基づき、新型コロナウイルスの感染者と診断した医師は「新型コロナウイルス感染者発生届（コロナ発生届）」に記入して、最寄りの保健所に届出します。コロナ発生届は診断時点の患者さんの居所である医療機関所在地の保健所に届くもので、住民登録地の保健所に出されるものではありません。発生届記載の患者さんの住所は、医療機関に申し出たもので、住民登録地が分からない方や違う方もいます。また、診断後に入院せずに帰った患者さんは、帰った場所の最寄り保

健所に移管し、発生届を転送しています。

届出された、または移管された発生届をもとに、保健所の医師、保健師の医療職チームは、入院調整や健康観察を行うとともに、感染症法第15条に基づく積極的疫学調査（注：今後の感染拡大防止を目的として、感染者と濃厚接触者に対して行動歴や家族状況、勤務状況等の聞き取り調査）を行います。事務職チームは、就労制限や入院勧告書を作成して療養費申請書と一緒に本人に送付し、個人番号（マイナンバー）利用事務である公費負担事務、入院医療機関への支払事務を行います。

4月中に事務改善を完了

港区では、10名を超える職員兼務発令と併せて、ICT（情報通信技術）を活用した数々の事務改善で、保健所職員の負担軽減を進めていきました。

4月30日には自宅療養中の感染者や濃厚接触者の健康観察のために、みなと保健所長が考案して独自開発した健康観察アプリ（図-1）がリリースされました。保健師が朝晩2回電話をかけていた確認がなくなり、発熱など発症の兆候があれば保健所にアラートメールが届き、手書きしていた健康観察記録もシステムからダウンロードできるようになりました。後にHER-SYSにも健康観察機能がリリースされましたが、区の健康観察アプリ開発事業者に「再委託で構築したのか」と問い合わせたほど、そっくりなインターフェースでした。

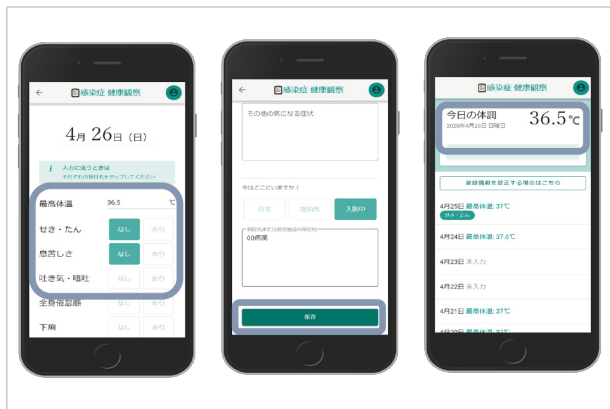


図-1 港区が独自開発した「健康観察アプリ」の画面

一方、感染症の公費負担事務は個人番号事務として、「情報提供ネットワーク」という総務大臣が設置・管理している個人番号と紐づけられた個人情報に関係機関間でやりとりするためのシステムから所得情報や加入医療保険情報の照会が認められています。同時に「住民基本台帳ネットワーク」を利用しての本人確認情報照会、住民登録地を探すことも認められた事務です。

利用できることを知らずに、他自治体や医療機関に電話照会していることに驚き、着任3日目には担当者に住基ネット統合端末や情報提供ネットワーク照会端末のアクセス権を付与し、端末を設置しました。

また、月に数件取り扱う程度だった感染症公費負担事務は、就労制限、入院勧告や延長勧告、公費負担決定通知作成、統計報告など、すべてが手作業でしたが、一緒に保健所に派遣されてきたExcel遣いの東京都職員や区職員が共同で内製した感染者管理台帳ミニシステムの稼働により、激減させることができました。後にこのミニシステムは重複しての入力作業が不要となるよう、国立および地方感染症研究所が管理する「感染症サーベイランスシステム（NESID：National Epidemiological Surveillance of Infectious Disease）」に入力した発生届情報のダウンロードCSV（Comma Separated Value）から取り込みするように改良されます。

各種帳票印刷による手作業削減から始まって、大型ディスプレイへの管内感染者情報ダッシュボード表示、性別・年代別統計分析で、リアルタイムで正確な情報把握と判断が可能となり、迅速な公表と区の施策決定に繋げることができました。

東京都の公表への違和感

5月11日と21日、保健所からの報告漏れや重複報告により公表済コロナ患者数に不整合があったため訂正するとの都知事会見がありました。23区保健所が東京都や国への報告を怠っている、FAXでの書類のやりとりが集計ミスを引き起こしている等、組織の対応能力を超えた発生届件数に起因した事務の遅れを、連携不足が原因と報道されました。

発生届が届く都度「LGWAN: Local Government Wide Area Network (総合行政ネットワーク, 都道府県・市区町村など地方自治体間を結ぶ閉域網)」に接続した区の内部情報系端末からLGWAN-ASPホスティングサービスに置かれているNESIDに入力しています。件数とNESID入力で払い出された個別IDを明記した送信票をつけて、毎晩退庁時に、都にFAXで送信しています。報告が漏れていた事実も、重複して報告した事実もありません。

この不整合調査の中で、東京都や一部自治体は、NESID統計の発生届出場所集計と異なり、移管後の管轄場所集計であること、重複報告ではなく同一人の重複届出が何件もあると気がつきました。

違和感の正体、揺れと名寄せ

発生届事務では、①診断時の居所、②本人申出または保険証に記載の住所、③公費負担事務に必要な住民登録地、④家族に感染させないためにホテルに滞在とか旅行中とか友人宅に同居など一時滞在地など、複数の住所情報を管理する必要があります。また、管轄保健所も、①発生届受理保健所、②入院勧告や就労制限を行う保健所、③感染者の濃厚接触者の健康観察を行う保健所と3つの立場があり、それぞれが異なる保健所となる場合もあります。

当初のHER-SYS要件定義には、複数の住所や管轄保健所の概念がありませんでした。管轄が移管されたことを通知する機能が実装されたのはかなりたってからのことです。公表される統計値が移管先で集計される、都道府県をまたいで移管するととりまとめの県レベルでは把握できないなど、定義の揺れでは済まされない不具合が残っています。

もう1つの問題は、名寄せが不完全なために重複届出を見逃すことがあることです。感染症公費負担は個人番号利用事務であっても、発生届出時点では番号記載はないため、名寄せ、重複届出の除外は職員の記憶に頼っています。

不安から病院を転々として検査していた方、出勤再開

のために陰性証明提出を指示されてPCR検査を受けたらまだ陽性だった方(治ったあとも体内にウイルスのかけらが残る、ずっと陽性となる方が多くいます)、週に何件もそんな方の重複届出を発見し、取り下げしています。

HER-SYSではマイナンバーも、名寄せが可能な正確な4情報(氏名、生年月日、住民登録地、性別)も保有しないため、ほかの保健所に出されて見逃された重複届出が相当数入った状態であると考えられます。重複データをクレンジングできる体制も機能も、現時点では存在しません。

わずか2週間で先行導入

港区は5月1日にHER-SYS先行利用自治体に応募し、5月15日にはNESIDからのデータ移行を受けて、試行を開始しました。試行初日の夜には、開発事業者や厚生労働省CIO補佐官も同行しての説明がありました。

象の耳だけのシステム

初めてHER-SYSの画面を見ながら話を聞くうちに何より驚いたのは、開発チームが誰一人として、発生届が出されるのは医療機関の管轄保健所という定義を知らなかったことです(図-2、図-3、図-4)。感染者の管理では複数の住所情報を管理するということも、管轄の定義を知らない人たちが作っていますから、当初は移管機能もなく、各種住所を入れるフレームもありません。



図-2 HER-SYS ログイン画面

NESIDと比較して入力する項目が10倍以上も増えていること、入院勧告や就労制限などのマイナンバー事務を支援する機能が一切ないこと、入力項目の論理チェックがまったくないこと、現場と乖離している点をあげればきりがありません。特に、発生届出先の管轄保健所は全国400を超える保健所のプルダウンから逐次選ばなくてはならず、万が一にも管轄保健所を誤選択すると、入力したデータがどこの管轄として登録されたか分からなくなり、検索することが一切できなくなるのでした。群盲象を評す、ということわざがありますが、ただデータを集めるためだけの仕組みとしか思えないHER-SYSは、まるで象の耳だけを触っていた人が作ったシステムだと感じました。

誰が要件定義をしたのか

このままりリースしてはいけない。これでは精度の低いデータの集合体になり、なんの分析にも使えない。せめて、入力している職員や医師の所属から管轄保健所は自動設定してほしい、発生届が出たら通知が届くようにしてほしい、と、行方不明データを避ける方法を考えました。説明に来ていた厚生労働省の方に改善してほしいことを山のように並べて訴えたと、ほっとした表情をされたのを思い出します。開発していたメンバ自体が、感染症法をよく知らない、厚生労働省内での応援チームだったそうで、感染症に詳しい職員の多くは倒れていたり、質問できるような雰囲気にはなかったそうです。何も知らない人たちが

The screenshot shows the HER-SYS web interface. At the top, there's a navigation bar with the logo and 'Sign out' button. Below that, a header indicates the date and time (2020/11/19 13:50) and the user's role (みなと保健所 日野 雅美). The main content area is titled '発生届' (Incident Report) and includes a red warning message: '発生届の提出は、感染症法第12条に基づく義務です。必要な事項を入力の上、速やかに提出して下さい。' (The submission of the incident report is a legal obligation under Article 12 of the Infectious Disease Act. Please enter the necessary information and submit it as soon as possible.)

The form contains several sections:

- 医師の氏名** (Physician's Name): A text input field.
- 従事する病院・診療所の名称** (Name of Hospital/Clinic): A dropdown menu with '外米徳園を推奨' (Recommendation for Saimitokujo) and '外米徳園を推奨' (Recommendation for Saimitokujo) buttons.
- 上記病院・診療所の所在地** (Address of Hospital/Clinic): A dropdown menu.
- 電話番号** (Phone Number): A text input field.
- 1 診断(検査)した者(死体)の種類** (Type of Patient/Body): A dropdown menu.
- 2 当該者氏名** (Patient Name), **3 性別** (Gender), **4 生年月日** (Date of Birth), **5 診断時の年齢** (Age at Diagnosis), **6 当該者職業** (Occupation): A row of input fields.
- 7 当該者住所** (Patient Address): A section with dropdowns for '都道府県' (Prefecture), '市区町村' (City/Town/Village), and '住所1' (Address 1), and text inputs for '住所2' (Address 2) and '電話' (Phone).
- 8 当該者所在地** (Location of Patient): A section with dropdowns for '都道府県' (Prefecture), '市区町村' (City/Town/Village), and '住所1' (Address 1), and text inputs for '住所2' (Address 2) and '電話' (Phone).

図-3 稼働から半年近くたって改善された入力フォーム

目の前のものだけを見て、話しかけてくる人だけに聞いて、要件定義をしていたのですから、現場と乖離した偏った内容だったとしても、責めることはできませんでした。

同時に、かつての NESID のように、最初はインターネット環境から接続していてもいつかは、LGWAN 接続に移行すると信じていました。

収集根拠のない入力項目

次第に HER-SYS を導入する自治体が増える中、新型コロナウイルス感染者の氏名や住所、生年月日、性別、職業に加えて、勤務先や行き先で会った人、感染者以外の個人情報、濃厚接触者の個人情報や、PCR 検査を受けただけの人もすべて入力するように、これは感染症法第 15 条に基づく国への報告義務だ、との指示が来たのです。保健所の負担軽減のためのシステムと言いつつ、入力項目と入力範囲の拡大は、旧システム NESID の 100 倍を超えて、負担は増える一方でした。

保健所に赴任した最初の日に教えられた、感染症法における人権擁護と信頼関係。これが最も分かるのが、法の前文にもあった後天性免疫不全症候群、エイズウイルス

The screenshot shows the '届出先保健所' (Reporting Jurisdiction) dropdown menu. The menu is open, showing a list of jurisdictions. The 'みなと保健所' (Minato Health Center) is selected and highlighted in blue. The list includes various jurisdictions such as 世田谷保健所, 渋谷区保健所, 池袋保健所, etc.

図-4 担当保健所選択はいまは都道府県内プルダウンですが、当初は全国保健所から選択でした

(HIV) 検査です。検査はすべて匿名で受けられ、個人を特定できる情報は取り扱いません。特に港区は、有名人の感染者も多く存在します。要配慮個人情報を集めているシステムであればこそ、丁寧に内部監査をしよう、そう考え始めていた、7月最初の週末、その事件は起こりました。

致命的な機能の欠如

東京都全体での導入開始を前にして、入力担当職員アカウントを追加しているときでした。みなと保健所職員アカウントの中に、見知らぬ名前と異なるドメインを持つアカウントがあったのです。

漏えいのおそれ案件

慌ててスクリーンショットを撮り、HER-SYS ヘルプデスクに問い合わせたところ、即座にそのアカウントは消されました。SE 作業のため、保健所のアカウントを作って作業していたが、消し忘れていたとの回答でした。私が過去に対応してきたベンダの SE 作業は、admin 権限を用いて、複数の監督体制の下で実施されてきました。患者データの閲覧権限を持っていない厚生労働省の受託者が、特権 ID を持ち、どこの保健所アカウントも自由に作って入ることができる運用は、信じがたいものでした。

以来、これをセキュリティ事故、漏えいおそれ案件として取り扱う港区と、正当なシステム管理者としての取り扱いであって、事故ではない、とする厚生労働省のせめぎ合いが、始まったのでした。

アクセスログ点検機能がない

不正アクセスがないことを確認したいと、厚生労働省に当該アカウントのアクセスログを求めたものの、これは事故ではない、の一点張りで、ログの提供が受けられません。提供できないはずですが、ログはとっているものの、開示する機能を HER-SYS は持っていなかったのです。

たとえアジャイル開発中であろうともアクセスログ開示機能は、自己情報開示請求や不正アクセス等の点検や監

査のために ISMS (情報セキュリティマネジメントシステム) でも PMS (個人情報保護マネジメントシステム) でもマストの機能です。港区は試行利用を中止し、ログ開示を中心に、安全管理措置を強く求めてきました。

まず、情報セキュリティ対策として、技術的安全管理措置が施され、データの紛失・破壊・不正利用・不正修正・不正提供から保護されているか。これらの対応状況を判断するため、総務省が定めた「地方公共団体における情報セキュリティポリシーに関するガイドライン」との整合性の確認を求めました。

要配慮個人情報と GDPR

次に、要配慮個人情報取扱にかかる適法性の確認として、収集目的の明確化、必要最小限の項目を適法・公正な手段により収集、違法な目的外利用や外部提供はないか。法的根拠と各利用者アクセス権限を記載したファイル項目詳細表の提示を求めました。これも不完全ながらようやく提供されましたが、当初は HER-SYS のデータを使って分析する機関である感染症研究所にアカウントが払い出されていない、など、不自然な運用が見られました。

そして、アクセスログの照会機能でもある、自己情報開示等請求対応機能の追加構築です。自治体が管理する情報は自治体の個人情報保護条例に基づいて管理しますが、港区に多い欧州連合加盟国の感染者情報については GDPR: General Data Protection Regulation (EU 一般データ保護規則) の適用を受けます。残念ながら、自治体は GDPR の十分性認定の適用対象外ですので、万が一の場合に安全管理措置が甘いと判断されれば、制裁金リスクは避けられないと判断したためです。

ログ開示機能がリリースされた 9 月 10 日から、港区では HER-SYS の試行利用を再開しました。併せて、厚生労働省から LGWAN 接続サービスによる結合を提案されたので、10 月末の LGWAN 移行にともなって本格利用となりました。

システムへの信頼のために

まとめに、HER-SYS とのかかわりを通して、信頼されるシステム構築は、どうあるべきかを考えます。

港区には、CISO（最高情報セキュリティ責任者）制度があり、副区長がCISOと個人情報保護監査役を兼務しています。この仕組みに基づき、不正アクセスのおそれ案件として事件事故連絡票を起票し、副区長や区長にエスカレーションできました。システムの信頼性を判断できる体制が確立されているからこそ、国が資料を提示するまでは導入を判断できない、トップ自らが明確に答えました。

それは適法なものであるか

感染症にかかる要配慮個人情報とは、感染症法前文や条文中にも再三書かれているように、人権侵害に直結する情報です。その取り扱いが厳しく制限されているにもかかわらず、感染症法第15条の積極的疫学調査としてなんでも集めてよいとの解釈が見られます。感染症拡大防止のため、人の生命財産を守るためと、安直に分析情報を公開することで人権侵害が生じており、このままでは過去のハンセン病やHIVと同様に国家賠償や損害賠償請求となり得ます。

システムの導入や構築にあたっては、情報法制の視点から、情報の取り扱いが適正・適法なものであるかを点検する必要があります。そのシステムは信頼できるものなのか、人を幸せにするものなのか、と言い換えてもいいかもしれません。

PMS との整合性

感染症法の場合、通常の個人情報保護法制以上に厳しい制限や理念があります。自治体個別の個人情報保護条例との解釈の相違も顕著です。事実、ここでは要配慮個人情報という言葉を使っていますが私の勤務する港区の個人情報保護条例にはまだ要配慮個人情報の定義はありません。どこの地域であっても、同一の水準で、人権に配慮した判断ができるよう、また、地方自治体個

人情報保護法の制定やマイナンバー制度の個人情報保護委員会のように統一的に所管する機関が必要です。

参考までに、直近の民間機関向けの個人情報保護法改正では、不正アクセスでの漏えいを重要視しており、法令違反に対する法人の罰則が1億円に引き上げられるなど、強化されています。適切な安全管理措置がなければ訴訟リスクや賠償リスクが高まることを踏まえた対応が求められます。

ゼロトラストネットワーク推進

HER-SYSの正式導入を審議した港区個人情報保護運営審議会で、「パブリッククラウド上に国が構築、または自治体が共同利用するシステムにおける個人情報の取り扱いについては、国で早急に留意事項等をまとめていくべき」との意見が出ました。まずは自治体クラウドの公的監査や認定制度、自治体にお墨付きを示せる仕組みが求められます。

自治体システムについては、これまで三層分離と呼ばれるネットワークに境界を設ける物理的安全管理措置が基本と示されてきました。コロナと共存する社会としてデジタル化が進む中では、コスト面からもインターネット経由でのクラウドや共同システム利用は不可欠のものです。自治体はゼロトラストネットワークモデルへと移行し、すべての通信を信用しない運用が求められると考えます。

インターネット上のパブリッククラウドで、ここまで大量の要配慮個人情報を共同管理するシステムは、日本ではHER-SYSが初めてだったと思います。アクセスログ開示機能とアクセス権限明示の欠如は、ゼロトラストネットワークモデル上では見過ごせないことでした。

HER-SYSが信頼されるシステムとして残っていくことを、心から願っています。

(2020年10月23日受付)

日野麻美（正会員） a-hino@ichimonjiya.com

1980年：東京都職業訓練校（現職業能力開発センター）電子計算機科養成課程入学。1981年：渋谷区企画室電子計算機係に東日本自治体では初めて女性プログラマーとして配属。以来、システム部門と現場のシステム担当を歩き来し、1994年から港区。2017年港区の情報政策スペシャリストとして内部認定。