

2020.12 ブログ：「HER-SYS はなにが問題だったか」を読んで、の詳細
(→ <http://www.1968start.com/M/blog/index2.html#2012c>)

特別解説「HER-SYS はなにが問題だったか」を読んで

中所武司

■この本の読書のきっかけ

最新号に掲載されていた下記の特別解説は、
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 について、
利用者の視点で、問題点が具体的に指摘されている。

- ・特別解説：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
情報処理 Vol.62 No.1 pp.4-9 (2021年1月号) (2020 年10 月23 日受付)

以下の2件のブログは、本システムに関するもので、
いずれも、**システム利用者への要求分析の不足**を指摘してきたが、
本解説は、その具体的な内容が記載されている。

- ・2020.9 「感染者情報管理の新システムの問題点とは」
<http://www.1968start.com/M/blog/index2.html#2009>
(抜粋)『システムの要求仕様書が、多様なステークホルダー・**利用者の視点で**
作成されていないと思われる』
- ・2020.12 「患者急増で、感染者データ集約システムへの入力が遅延」
<http://www.1968start.com/M/blog/index2.html#2012b>
(抜粋)『本システムの最も重要なステークホルダーは、**医療機関での入力担当者**だが、
システムの要求分析段階での調査が不十分だったのではないだろうか』

■本解説からの抜粋とコメント

(注) コメントは、システム構築技術に限定

[...] と 【...】 は、本解説の大見出しと小見出し

→★の部分は、私のコメント

[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) 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
- ・本解説の著者は、本年の4/20から、みなと保健所 (東京都港区) で、
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に従事

【感染症法とは人権を守る法律】

【発生届を起点とした事務の概要】

- ・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を最寄りの保健所に届出
（発生届は、診断時点の患者の居所である医療機関所在地の保健所に提出）
（住民登録地が異なり、帰った患者の発生届は、患者の最寄りの保健所に転送）
- ・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い、
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実施
- ・事務職チームは、就労制限や入院勧告書を作成、療養費申請書と一緒に本人に送付し、
公費負担事務、入院医療機関への支払事務を実施

【4 月中に事務改善を完了】

- ・港区では、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を軽減
- ・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」経由での
個人情報（所得情報や加入医療保険情報）の照会や、住民基本台帳ネットワークでの
本人確認情報照会、住民登録地検索を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たので、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

【東京都の公表への違和感】

- ・5月に、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り、
訂正するとのお知らせあり
- ・この不整合調査の中で、重複報告ではなく、同一人の重複届出があると気づく

【違和感の正体、揺れと名寄せ】

- ・発生届事務では、診断時の居所、本人申出または保険証に記載の住所、
公費負担事務に必要な住民登録地、ホテルに滞在とか旅行中とか友人宅に同居など、
複数の住所情報を管理する必要あり
- ・管轄保健所も、発生届受理保健所、入院勧告や就労制限を行う保健所、
感染者の濃厚接触者の健康観察を行う保健所が異なる場合あり
- ・当初のHER-SYSの要件定義には、複数の住所や管轄保健所の概念がなかった。
公表される統計値が移管先で集計され、都道府県をまたいで移管すると
とりまとめる県レベルでは把握できないなどの不具合が残っている。
- ・名寄せが不完全なために重複届出を見逃すことがある
（週に何件も重複届出を発見し、取り下げている）
- ・HER-SYS では、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
マイナンバーも保有しないため、ほかの保健所に出されて見逃された重複届出がある

[わずか2 週間で先行導入]

- ・港区は、5/1にHER-SYSの先行利用自治体に応募し、5/15に試行を開始。
試行初日は、開発事業者や厚生労働省CIO 補佐官も同行

【象の耳だけのシステム】

- ・開発チームの人は、発生届が医療機関の管轄保健所に出されることを知らず、感染者の管理に必要な複数の住所情報の入力エリアがなく、移管機能もなし
- ・従来システムに比べ、入力項目が10 倍以上に増えているが、論理チェック機能がない
- ・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
- ・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での選択のため、万が一にも管轄保健所を誤選択すると、検索することが一切できなくなる
- ・現場と乖離している点をあげればきりがない
- ・ただデータを集めるためだけの仕組みとしか思えない

→★上記6項目から、利用者視点なしのシステム開発だったことは明白！

今どきのシステム開発で、利用者無視の要求仕様が作成されることは驚き！

【誰が要件定義をしたのか】

- ・このままリリースしたら、精度の低いデータの集合体で、なんの分析にも使えない
- ・入力している職員や医師の所属から、管轄保健所を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、行方不明データを避けるべき
- ・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

→★本来は、要求分析段階で利用者から聞き出すべき事柄を開発後に実施している

- ・開発メンバは、感染症法をよく知らない、厚生労働省内での応援チームで、感染症に詳しい職員に質問できるような雰囲気ではなかったとのこと

→★現場の協力が得られず、使われないシステムが開発された失敗は、1980年代の話？

- ・何も知らない人たちが要件定義をしていたので、現場と乖離した偏った内容だったが、責めることはできませんでした

→★いえいえ、システム開発者としては、責められるべき、とても恥ずかしいこと！

【収集根拠のない入力項目】

- ・感染者の氏名や住所、生年月日、性別、職業に加え、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国への報告義務として入力すべきという指示あり

- ・保健所の負担軽減のためのシステムと言いながら、入力項目と入力範囲の拡大は、旧システムの100 倍を超えて、負担は増える一方でした

→★ISOのソフトウェア製品の8項目の品質特性 {機能適合性、性能効率性、互換性、使用性、信頼性、セキュリティ、保守性、移植性} の観点でいえば、機能のみを重視し、使用性を軽んじた結果、システムの利用率が達成できなかった

[致命的な機能の欠如]

- ・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

【漏えいのおそれ案件】

- ・SE 作業のため、保健所のアカウントを作って作業して、消し忘れていたとのこと
- ・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だった

【アクセスログ点検機能がない】

- ・不正アクセスがなかったことの確認のため、厚生労働省に当該アカウントのアクセスログを求めたが、ログを開示する機能を、HER-SYS は持っていなかった
- ・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マストの機能なので、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た。
- ・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た。
- ・ログ開示機能がリリースされた9/10から、港区ではHER-SYS の試行利用を再開。10 月末のLGWAN 移行にともなって本格利用となった。

[システムへの信頼のために]

- ・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たので、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、国が資料を提示するまでは導入を判断できないと、トップ自らが明確に答えていた。

【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、人権侵害に直結する情報なので、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る。

【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る

【ゼロトラストネットワーク推進】

- ・自治体システムは、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なので、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
- ・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

→★e-Japan戦略以来、20年間に開発したが利用されない行政システムは多い。
本解説は、これからのデジタル庁の設立にかかわる人の必読書と思う！

以上