電子カルテの安全な導入と運用
―宇陀市立病院事件を事例に

応用

黒田知宏 | 京都大学医学部附属病院

事件の概要と予想される原因

宇陀市立病院は 2018 年 10 月 1 日に病院情報システム（HIS：Hospital Information System）を導入し，紙カルテから電子カルテへの移行を果たしたが，その直後の 10 月 16 日に電子カルテ本体がランサムウェア（GandCrab）に感染して 2 日間停止した．

同事件の調査は外部セキュリティ対策ベンダによって 2018 年 11 月と 2019 年 3 月の 2 回にわたって，また，2019 年 3 月から 9 月にわたって 5 回の会合を含む調査が外部有識者によって行われた．宇陀市は外部有識者会議の提言を受けて対策等を実施し，2020 年 2 月 28 日，全 31 ページに及ぶ「報告書」を発出した☆1．なお，残念なことに，報告書が出される直前の 2 月 2 日，この問題の対応にあたった同市職員が飛び降り自殺をしている☆2．

同報告書は，システムログなどの証拠保全が行われることなく，復旧時に管理端末が初期化されてしまっているので正確なことは分からないものの，「ルール違反」で HIS 系の LAN にモバイルルータなどの機器を通じて外部インターネットと接続された情報機器が接続され，外部から侵入を許してしまったと考えられるとしている．また，同報告書に書かれた今後の「技術的対策」の中で，リモートデスクトップ（RDP）の接続が攻撃に悪用されたとしていることから，RDP がさまざまなサーバに設定されていた上に，その設定がきわめて甘かったのであろうと想像される．加えて同報告書によると，同市は有識者会議から技術的問題と同時に，「病院のガバナンスに問題があった」との指摘を強く受けており，今後の対策を論ずる後段においてもガバナンス強化のための取り組みに一定の紙幅が割かれている．詳細は報告書自身に譲るが，示された 6 項目の対策は，きわめて一般的かつ基本的な事項でしかない．裏を返せば，何もなされてなかったことが透けて見える．

このように，導入ベンダ側は適切な技術的対策を施していないばかりか，外部回線と接続してはならないというきわめて基本的なルールを守ることもセキュリティインシデント対応の基本であるログの保全もできず，病院・市側は基本的なガバナンスがなっていなかったようである．端的に言うならば「揃いも揃ってみんなだめ」だったのであろう．

同事件は特別だったのか

筆者は大学病院の情報システム担当者として，20 年近く HIS の導入や管理に携わってきた．筆者の実体験や業界関係者の間で共有された事例に照らしてみたとき，宇陀市民病院事件をとりまく「揃いも揃ってみんなだめ」な状況は決して特別ではなく，むしろきわめてありがちな状況に思われる．外部有識者会議が設置されることなく業界関係者だけで事件調査が行われていたならば，「運が悪かったねぇ」で済まされてしまっていたかもしれない．

同事件は HIS の導入初期段階で発生している．この時期は，一般的に導入事業者から病院に運用が完

☆1 http://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/houkokusyo.pdf
☆2 http://www.naraseikei-np.com/news200302_002.html

全に引き渡されるより前であり，導入事業者の多くが調整や改修のためにHISに通常運用では用いない機器を接続していることが多く，管理が不安定になりがちである．ガバナンスの観点から見れば，主たる導入事業者が一義的な管理責任を負うことになるが，きわめて多くのサブシステムから構成されるHISの場合，その全てにきちんと目を配ることはそう容易ではない．加えて，近年保険財政が厳しい中，HISの導入・運用コストの低減が国会で取り上げられるほど目の敵にされ，導入コストを下げるために分割調達，すなわち，個別サブシステムごとの個別契約が行われることが増えてきており，ベンダごとの責任範囲が明確でないことも多い．聞くところによると，本事案でも分割調達がなされており，電子カルテベンダ，ソフトウェア導入SIer，ネットワーク導入SIerなどの責任範囲が不明確だったようである．

分割調達にありがちな責任範囲の不明確さを解消するためには，導入者側に社内SE部門を置き，強いリーダシップを発揮することが求められる．しかし，厳しい保険財政は病院にコストセンタであるSE部門を置くことを許さない．特に地方自治体の医療体制を支える自治体病院は財政的に逼迫していることが多く，SE部門が置かれていない，あるいは，置かれていたとしても，情報技術に明るくない人物1人あてがわれているだけのことが多い．国立大学病院長会議のもとには医療情報部長会議という筆者を含むSE部門長の立場にあるものが年に数回集まって議論を行う会議体があるが，「このたび，○○大学の医療情報部教授を拝命した○○です．私は○年間○○診療にあたってきましたが，コンピュータや電子カルテは素人です．一方で，当院の部門にはスタッフもおりませんので，電子カルテを1人で切り盛りせねばならず，不安でいっぱいです．これから一所懸命勉強して参りますので，皆様いろいろ教えてください」という新任挨拶をよく耳にする．国立大学病院ですらこのていたらくなのだから，地方自治体病院など推して知るべしである．

加えて，医療者の多くは業務の丸投げに慣れている．診療現場では高度技能者による分業が発達しており，医療機器は臨床工学技士が，薬剤は薬剤師が十分な調整を行ってから医師・看護師に提供される．新規導入時には，MRと呼ばれる医療機器メーカ，薬剤メーカのスタッフが病院に張り付いて手取り足取り使い方を教えてくれたりもする．当然HISも十分な調整を行ってから提供されるべきものと理解され，実際，大手病院のICU等への急性期系情報システムの導入時には「24時間導入企業のスタッフが張り付いていないとはふざけている」と憤る医療者にSEや導入企業が凍りつく場面にでくわすことも少なくない．そこに医療者不足が追い打ちをかける．地方自治体は医療者の確保に血道を上げており，三顧の礼で医療者を迎えるほかない．結果，医療者の自由を束縛するようなルールの設定などできようはずもなく，勢いガバナンスは失われてしまう．

丸投げ体質の素人を騙すのは簡単である．多くの自治体病院ではHIS調達仕様書の作成業務がコンサルタントと呼ばれる業種に丸投げされているが，自治体から相談を受けてコンサルタントを呼び，一通り話を聞いた上で，「ところでこの病院では物流管理にはどういう情報システムを導入するのですか?」と聞いたところ，真顔で「物流管理システムって何ですか?」と聞き返されたという笑えない話を，仲間の医療情報専門家から筆者が聞かされたのは一度や二度ではない．財政基盤が不安定で払いが悪いのに要求が多く，SI案件が「デスマーチ」的に増加しがちな医療分野に優秀なSEが残るはずもなく，概して担当者の技術力は高くない．こうして，情報技術に明るくない業者が丸投げ体質の素人を騙して導入された情報システムが，きわめて社会的ニーズの高いサービスの基盤として利用されることになる．ひとたびことが起これば，担当者は板挟みになり，心を病むまで追い込まれることになる．事実，電子カルテ導入のプロセスの中で心を病む例は，業者SE，病院スタッフとも後を絶たない．本件の最後に身を投げた担当者の心労はいかばかりであったかと考えると胸が痛む．

このように，宇陀市立病院の「揃いも揃ってみんな

だめ」な事例は，実はどこの医療機関でも起こり得る．いや，顕在化していないだけで，実は日々起こっているのかもしれない．保険財政が逼迫し，医療者不足が顕著な中でも，現場の医療者の献身的な努力で地域の医療体制がなんとか持ちこたえているのと同様に，現場の心ある SE やスタッフの献身的な努力でなんとか持ちこたえているというのが実情であろう．

規制はセキュリティを高めているか

社会の経済原理のメカニズムに任せて物事がなし遂げられないとき，とり得る手段は規制のみである．HIS を取り巻く規制は「ガイドライン」と「通知」の形で与えられている．

法的に電子カルテの利用が許されたのは，1999 年 3 月 22 日，厚生労働省健康政策局発通知第 517 号，厚生労働省医薬安全局発通知第 587 号，厚生労働省保険局発通知第 82 号，「診療録等の電子媒体による保存について」，いわゆる「三局長通知」[☆3] である．三局長通知から遅れること 5 年，2005 年 4 月には，診療録を含むすべての公文書の電子保存・電子作成を認める所謂「e 文書法」が施行され，三局長通知は e 文書法厚生労働省令の補完文書である「医療情報システムの安全管理に関するガイドライン」（厚労ガイドライン）に引き継がれ，以降これに呼応する形で，経済産業省や総務省から発出されたガイドライン群とともに，いわゆる「3 省 4 ガイドライン」が形成された．厚労ガイドラインの遵守は，診療報酬点数表の中で「診療録管理体制加算」の算定要件として参照され，この加算の取得は「急性期一般入院基本料」算定の施設要件に(結果的に) なっている．すなわち，厚生労働省は入院診療報酬の保険償還のために守らねばならないルールにすることで，医療機関に同ガイドラインの遵守を迫っているわけである．

厚労ガイドラインは，本稿執筆時点で有効な版（第 5 版）[☆4] で，本文 163 ページ，付属文書 75 ページにわたる大作である．なぜこれほどまでに長いかというと，1 つ 1 つの事項について具体的対処法を事細かに書いているからにほかならない．初期のガイドラインを作成した方々の話では，「情報技術の素人である医療者が言われたとおりにすればよいように細かく記載された」米国のガイドラインを範として作成されたそうである．実際，「パスワード」1 つとっても 4 ページに渡る解説の後，悪名高い「最長でも 2 カ月以内」に定期的変更を求める項目を含めた，5 項目にわたる「最低限のガイドライン」を定めている．

事細かに細部を記載することは，一見，情報技術に精通しない医療機関の情報セキュリティを高めるように思える．しかし，実際はそうはならない．情報セキュリティは，永遠に続く攻撃者との戦いである．ガイドラインに事細かに書かれた対策は，どのような防御態勢が敷かれているかを攻撃者に知らしめる情報でもある．ひとたびそこに書かれた防御方法の弱みが明らかになれば，敵は一気に攻め込んでくることになる．加えて，強いコスト削減圧力の中で利益を守らねばならない事業者にとっては，事細かに書かれた「最低限のガイドライン」は，それさえ守れば説明責任が果たされる「防具」として機能する．結果，ガイドラインを満たす防衛力の低い手法が採用され，事業者（ベンダ）も導入者（病院）も管理者（規制当局）もそれに満足してしまうこととなる．

手法を定めたガイドラインは，決してセキュリティレベルを高めることはない．

ファンタジーでは守れない

厚労ガイドラインの根底を貫く基本的な考え方は，情報空間の分離である．これは，「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」の「B-2. 選択すべきネットワークのセキュリティの考え方」で，ネットワークの在り方を「クローズドなネットワーク」と「オープンなネットワーク」に分離し，後者に前者の倍以上の紙幅を割いて説明し，「C. 最低限のガイドライン」の 1 項目目で「選択するサービスの閉域性の範囲を事業者

☆3 https://www.mhlw.go.jp/www1/houdou/1104/h0423-1_10.html
☆4 https://www.mhlw.go.jp/stf/shingi2/0000166275.html

に確認すること.」を求め,「D. 推奨されるガイドライン」で「やむを得ず,従業者による外部からのアクセスを許可する場合は」と存在してはならないこととして外部接続を扱っていることからも見て取れる.厚生労働省のこの考え方は一貫しており,日本年金機構情報漏洩事件発覚直後の平成 27 年 6 月 17 日には「個人情報の適切な取扱に係る基幹システムのセキュリティ対策の強化について(依頼)」(図 -1)[☆5] と題した通知文書で,基幹系ネットワークと(インターネットに接続された)情報系ネットワークを物理的に切断し通信不可能な状態にすることを求め,次世代医療基盤法施行規則[☆6] 第 6 条四ニ (1) では,「外部の者との送受信の用に供する電気通信回線として,専用線を用いること.」を求めている.

しかし,外部接続をまったく持たない独立した HIS を構築することなど,土台不可能である.そもそも,オープンなネットワークへの接続が物理的に断たれていては,頻繁に提供されるセキュリティパッチを即時適用することさえできず,システムに不具合があった際に事業者からのリモートメンテナンスを受けることもできない.業者の拠点から遠く離れた地方の医療機関にとって,リモートメンテナンスの可能性を断つことは,重症患者の生命維持にかかわる情報システムの不具合発生によって即時に患者の生命が奪われることを許容することにほかならない.情報セキュリティを守るために医療安全を犠牲にすることは許されない.「規則と手順決めて 守って 見直して」[☆7] と厚生労働省自身が述べているように,規則や手順に「問題点や不都合な点が見つかったときには躊躇なく改善する」ことは,医療安全の要諦である.「守れないルールはルールが悪い」と考えねばならない.

宇陀市立病院事件は医療機関がランサムウェア被

☆5 https://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/270617-1.pdf

☆6 https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=430M60000582001

☆7 https://www.mhlw.go.jp/topics/2001/0110/tp1030-1f.html#8-4

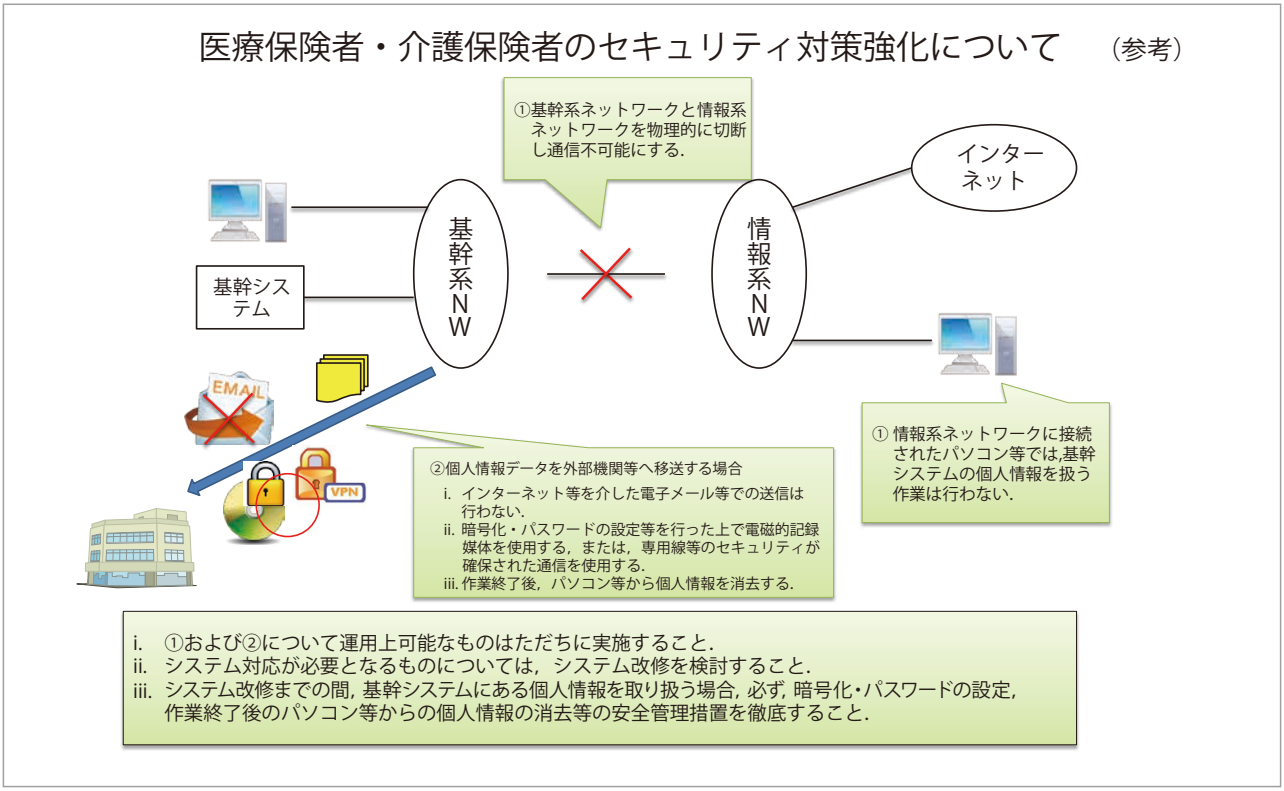

図 -1 平成 27 年 6 月通知文書参考図

害に遭った日本初の事例として，医療情報関係者の注目を集め，さまざまな情報がもたらされた．その中で，筆者を含む関係者が最もがっかりしたのは，「HISネットワークがインターネットに繋がるのが実態となっていることを踏まえて，そのための要件をガイドライン等で明確化すべき」と有識者会議の提言書に記載することを，厚生労働省が強く拒絶したという噂である．あくまでも噂にすぎないと言えば噂にすぎないが，厚生労働省のこれまでの一貫した態度からも，次世代医療基盤法関連政省令作製を支援する中で筆者が体験した関係省庁や国会議員，有識者などからの激しい圧力からも，「さもありなん」と感じさせる蓋然性はきわめて高い．医療情報関係者でこの噂を「根拠のない噂」と考える向きは１人もいないであろう．

「揃いも揃ってみんなだめ」は，宇陀市立病院関係者に限られた話ではない．規制当局である厚生労働省も含めて，「揃いも揃ってみんなだめ」なのである．

手段から目的への回帰

丸投げ体質の素人からなる現場と事細かなファンタジーからなる規制という「揃いも揃ってみんなだめ」な現実を変え，安全にHISが導入・運用されるためにはどうすればよいのだろうか．キーワードは，提言に示された「ガバナンスの強化」である．結局，導入者側が当事者意識を持って臨むほかなく，そうなるように規制をかけるほかない．

筆者は，「3省4ガイドライン」を整理統合し，「3省2ガイドライン」へ集約するにあたって，受託事業者を縛る経産省と総務省の統一ガイドライン作製の一翼を担うよう依頼を受けた．改定にあたって筆者たちがこだわったのは，「手段から目的への回帰」である．事細かな手段を書くのではなく，何を達成しなければならないのかという目的を記載し，その目的を達成する方法の選択を事業者に任せ，それを医療機関に説明して合意を得る責任を事業者に負わせることを基本的な枠組みとした．事業者の説明の中には，想定されるリスクの一部を受容することや，リスクを低減するための対策を採ることを，医療機関自身に求める説明までもが含まれている．医療機関が説明を理解して合意したのでない限り，それが原因で事故が発生した場合には，事業者は責任を問われることになる．こうすることで，示された手段を盲目的に達成しようとする「手段の目的化」を行う事業者を淘汰し，目的に沿って論理的に手段を選択し，適切に説明できる事業者のみが残ることを狙うとともに，医療機関にも説明を理解し，求められた対策を実施する「当事者意識」を持たせることを狙っている．合意した対策を実施していなかった医療機関は，事故発生時の責任のすべてを自ら負わねばならなくなる．事業者のガイドラインと見せて，実は医療機関にも努力を求めているのだ．

同ガイドラインは４月６日までのパブリックコメントを経て発出される予定であり，これに続いて，医療機関を縛る厚労ガイドラインの改定が行われる予定である．厚労ガイドラインの改定を司る委員会では，「パスワードの更新頻度をさらに上げて二要素認証を採らざるを得なくなるようにするのだ」といった政策誘導的な議論がなされているとの噂も聞こえてくるが，「二要素認証」などのすでに防衛力の綻びが明るみに出つつある些末な手段へのこだわりを棄て，「情報セキュリティを高める」という目的に立ち返って議論が行われることを期待したい．根底に立ち返れば，自ら考える力を持つことを病院に求めるほかないはずだ．

事業者も医療機関も目的に立ち返って自ら考え，「知彼知己者，百戦不殆」の構えをそれぞれが採ったときにはじめて，「みんなちがって みんないい」姿が現れるのではなかろうか．

（2020年3月29日受付）

■黒田知宏　tomo@kuhp.kyoto-u.ac.jp

1994年京大・工・情報卒業，1998年奈良先端大・情報修了，博士（工学）．奈良先端大学院助手，オウル大客員教授，京大講師，阪大准教授等を経て，2013年より現職．京大病院医療情報企画部長としてHIS企画・導入・運営にあたりながら，医学研究科と情報学研究科で医療情報学に関する教育・研究に従事．医療情報学会等会員．