宇陀市監査委員告示第　８　号

# 令和元年度随時監査（ＩＣＴ監査）結果報告書の提出について

地方自治法(昭和２２年法律第６７号)第１９９条第２項及び第５項の規定に基づき、令和元年度随時監査（ＩＣＴ監査）を実施したので、その結果を同条第９項の規定により別紙のとおり公表する。

令和２年３月２５日

宇陀市監査委員　籠　谷　順　司

宇陀市監査委員　西　岡　宏　泰

１　監査の種別

地方自治法（昭和２２年法律第６７号）第１９９条第２項及び第５項の規定による随時監査

２　監査の対象

対象事業　　宇陀市立病院電子カルテシステムウィルス感染後の対応

３　監査の期間及び対象

令和元年１２月１８日から令和２年３月２５日まで

調査実施日：令和２年１月２９日

４　監査の方法

監査の実施に必要な資料の提出を求め、事案発覚後の医療情報システムの信頼回復への寄与、医療情報システムの構築・運用・維持管理の妥当性、事案発覚後の業務委託費用の投資効果について、関係書類を調査するとともに、担当課職員から聴取を実施した。

なお、実施にあたっては、公益社団法人大阪技術振興協会とのＩＣＴ監査に係る技術調査業務委託契約に基づき、技術士１名の派遣を求め実施した。

５　監査の結果

技術士の技術調査結果に基づき、概ね適正であると判断できた。しかし、今回の発生事案は、守るべきセキュリティに対するルール違反からウィルス感染し、重大な事案発生につながってしまったものである。

また、コンピューターウィルスは日々進化しており、宇陀市における他の情報システムにおいても感染しないとは限らない。宇陀市立病院のみならず、十分な安全対策と維持管理体制を整えていただきたい。

なお、調査結果の概要は、技術士から報告された調査結果報告書のとおりである。

# 宇　陀　市

令和元年度

# 宇陀市情報セキュリティ調査報告書

令和２年３月４日

公益社団法人　大阪技術振興協会

技術士（総合技術監理/電気電子部門）　弓削　靖

調 査 実 施 日：　令和２年１月 29 日（水）

調　査　場　所：　宇陀市立病院会議室

事 業 担 当 課：

| | | | |
|---|---|---|---|
| 宇陀市立病院 | 医務課 | 荒木　正好 | 課長 |
| | 経営企画課 | 橋野　誠 | 課長 |
| | 情報システム管理室 | 中西　一昭 | 室長 |
| | 事務局 | 合田　憲二 | 次長 |

調 査 立 会 者：

| | | | |
|---|---|---|---|
| 宇陀市監査委員会 | | 籠谷　順司 | 代表監査委員 |
| | 事務局 | 藤原　秀一 | 局長 |
| | | 藤本　進 | |

調　査　対　象：宇陀市立病院電子カルテシステムウィルス感染後の対応

# 目　次

## 1.　調査担当者

### 1.1　調査機関

公益社団法人　大阪技術振興協会
理事長　亀尾　恭司
住所：〒550-0004　大阪市西区靭本町 1-8-4
大阪科学技術センタービル 504 号室
電話番号：(06)6444-4798

### 1.2　担当技術士

弓削　靖　　(総合技術監理/電気電子部門)　　登録番号：52032 号

## 2.　調査概要

### 2.1　調査対象

宇陀市立病院電子カルテシステム(以降、「EC システム」と記載) ウィルス感染後の対応

### 2.2　調査対象の概要

市立病院が保有する全ての情報（カルテ、レントゲンなどの画像データ、検査結果、会計情報、調剤情報）を施設内のサーバで管理し、必要な時に必要な情報を閲覧できるようにするため、電子カルテシステム(EC システム)導入が計画された。平成 29 年度にプロポーザル方式により導入業者が決定され、平成 30 年 9 月に導入が完了した。同年 10 月 1 日より運用が開始されたが、10 月 16 日にウィルス感染が発覚した。その後、初期対応が実施され、2 日後の 10 月 18 日には外部ネットワークとは遮断された状態ながら EC システムは復旧した。その後もコンサルタント会社やセキュリティベンダーなどにより原因の分析、復旧作業等が実施された。また、市では対策協議会が発足し、専門家による有識者会議が新たに立ち上げられて､外部の視点で様々な検討が加えられ､提言書がまとめられた。その提言書を受け、宇陀市で報告書が取りまとめられ、令和元年 9 月 1 日に発行された。

### 2.3　調査目的

前項に記載した EC システムウィルス感染に関する一連の対応内容を確認し、次の観点から調査を実施する。

- 一連の対応の妥当性 1 (医療情報システム信頼性回復への寄与)
- 一連の対応の妥当性 2 (投資効果)
- 医療情報システムの構築、運用、維持管理の妥当性

## 3.　調査対象に関する情報収集

### 3.1　宇陀市立病院電子カルテシステム導入経緯

宇陀市立病院の一世代前の医療情報システムは平成 21 年度に更新稼動した。平成 29 年時には稼働以来 8 年経過しており、保守サポートの期限切れが近く、機能・運用が近年の病院運用にそぐわない部分が目立ってきていた。これらを解消するため、新しい医療情報システム導入計画が立てられた。

新しい医療情報システム構築の際に次の方針が掲げられた。

①旧システムはオーダリングシステム[1]中心で稼動しており、地域医療の中核病院として業務の効率化や情報の共有化を図るため、電子カルテシステム(EC システム)[2]を導入すること。

②その他の部門システムを含めた病院全体の業務システムの見直しや統合及び、業務の電子化を進め、国の求める地域包括ケアシステムの地域中核病院として、良質な地域医療包括ケアを継続するために必要な病院経営システムを構築できること。

上記の方針に基づき、平成 30 年 1 月～2 月にかけて公募型プロポーザル方式による導入業者選定が行われ、平成 30 年 3 月に導入業者が決定し、委託契約が締結された。

■導入委託業者　　株式会社医療情報システム(システムメーカー　富士通株式会社)

### 3.2　宇陀市立病院電子カルテシステム（EC システム）構成

EC システムは平成 30 年 4 月～平成 30 年 9 月の 6 ヶ月間で設計、導入が進められた。システム構成を図　3.1 に示す。なお、次の 3 システムは別途導入され、システム導入時に EC システム間相互連携が図られた。

・リハビリシステム　導入業者：タック株式会社　整備年度：平成 28 年度
・健診管理システム　導入業者：パインシステム株式会社　整備年度：平成 29 年度
・ナースコール　導入業者：株式会社ケアコム　整備年度：令和元年度

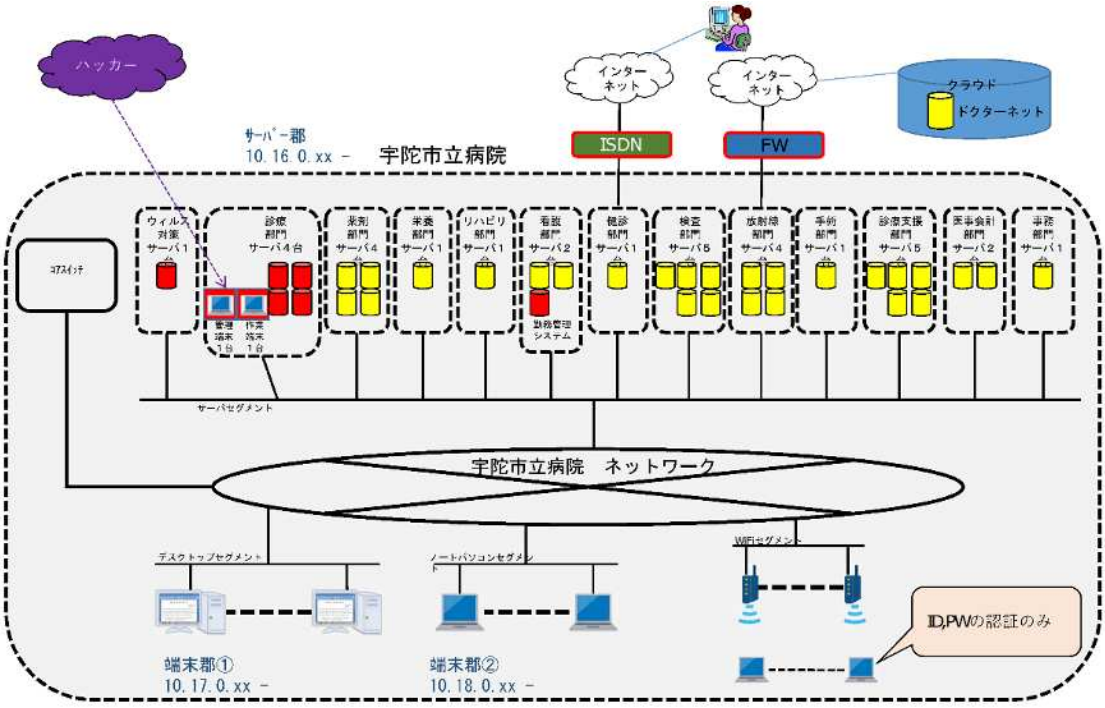



図 3.1　宇陀市立病院　EC システム、ネットワーク概略図(平成 30 年 10 月時点)

※朱塗りで示した機器が、本事案でウィルス感染した

[1] 医師や看護師が行う検査や処方などの指示（オーダー）を電子的に管理する医療情報システム
[2] 病院で医師が記録する診療記録（カルテ）を電子化し、保存・管理するシステム

### 3.3　世界中のシステムを脅かすマルウェア[3]の現状

平成 30 年 10 月 1 日に稼働開始した EC システムが同年 10 月 16 日にマルウェアの 1 つであるランサムウェア[4]に感染した。後に「GandCrab」という種類のランサムウェアであることが判明した。このランサムウェアにより EC システム内のデータファイルが暗号化され、患者カルテの参照ができなくなり、システムが機能不全に陥った。

ここで、医療情報システムのみならず、世界中のシステムに被害をもたらしているマルウェアの現状を確認する。

#### 3.3.1　マルウェアの分類

マルウェアは 2 つの英単語を合わせた造語であり、「悪意のあるソフトウェア」という意味である。

●マルウェア　Malware＝Malicious＋Software

マルウェアは広義のウィルスのことであるが、大きく 4 つに分類される。

| | |
|---|---|
| ①トロイの木馬 | 情報を搾取する。密かに潜伏する。 |
| ②ウィルス(狭義のウィルス) | ファイルなどに寄生し拡散する。 |
| ③ワーム | 自身のコピーを作って拡散する。 |
| ④暗号化/脅迫/破壊系 | 暗号化する。脅迫する。破壊する。 |

今回の感染は④の分類のものであるが、④のマルウェアはここ数年全世界で猛威を振るっている。2017 年のランサムウェア「WannaCry」による世界中の被害多発は記憶に新しいところである。

#### 3.3.2　マルウェアによる被害事例

科学雑誌「日経ネットワーク」記事(2020.1)には次のような被害事例の記事が紹介されている。

> 2018 年から 2019 年にかけて、米アップルや米ボーイング、ノルウェーのアルミニウムメーカーであるノルスク・ハイドロなどの大手企業がランサムウェアに感染した。海外では 2019 年だけで数百の自治体や医療機関、教育機関が被害に遭った。
>
> 国内でも日本マクドナルドやホンダといった大手企業をはじめ、神戸大学や神奈川大学などの教育機関、川崎市や町田市などの自治体がランサムウェアに感染した。これら公になっているケースは氷山の一角であり、実際はその数倍の被害が水面下で起きていると想像される。

国内の医療機関でも様々な被害が報告されている。

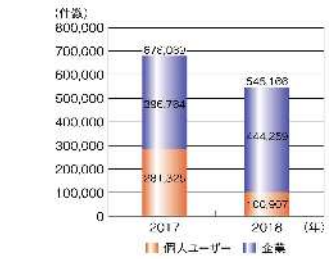
| | |
|---|---|
| 2017 年 3 月 15 日 | 岡山大学病院医療用端末 2 台のウィルス感染 |
| 2017 年 12 月 8 日 | 新潟大学歯学総合病院 PC1 台のランサムウェア感染 |
| 2019 年 6 月 3 日 | 佐世保共済病院放射線検査機器 PC5 台のウィルス感染 |
| 2020 年 1 月 17 日 | 福知山市民病院メールサーバ乗っ取りによる迷惑メール送付 |

[3] コンピュータの正常な利用を妨げたり、利用者やコンピュータに害を成す不正な動作を行うソフトウェアの総称。“malicious software”（悪意のあるソフトウェア）を縮めた略語。(コンピュータウィルス、ワーム、ランサムウェア等)

[4] 感染した PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金（ランサム」を要求する不正プログラム

右のグラフでは、マルウェアのうちのランサムウェア検出件数は 2017 年より 2018 年の方が減少したものの、減少したのは個人ユーザを狙った案件であり、企業や機関を標的とした件数は 12%増加している、という傾向を伝えている。

以上のとおり、国内のみならず、全世界で多種多様かつ非常に多くのマルウェア被害を含むセキュリティインシデントが発生しており、これらが継続発生していることがわかる。




■図 1-1-6 ランサムウェアの市場別推移
(出典:Symantec 社「インターネットセキュリティ脅威レポート第 23 号」「インターネットセキュリティ脅威レポート第 24 号」を基に IPA が作成)

出典：情報セキュリティ白書2019
独立行政法人情報処理推進機構（IPA）

### 3.4　宇陀市立病院マルウェア感染後の対応経緯

#### 3.4.1　事象発生初期対応(平成 30 年 10 月 16 日～平成 30 年 11 月 13 日)

平成 30 年 10 月 16 日にマルウェア感染が発覚した後の対応経緯を表 3.1 に示す。

表 3.1　マルウェア感染後の対応経緯（□初期対応）

T 社：有限責任監査法人トーマツ　TM 社：トレンドマイクロ(株)

| 年月日 | 曜日 | 病院 | 協議会 | 有識者会議 | 他機関 | T社 | TM社 | 対策内容 |
|---|---|---|---|---|---|---|---|---|
| 平成30年10月1日 | 月 | ● | | | | | | 電子カルテシステム運用開始 |
| 平成30年10月16日 | 火 | ● | | | | | | ウィルス感染 |
| 平成30年10月18日 | 木 | ● | | | | | | 対策後完全復旧(ローカル運用) |
| 平成30年10月19日 | 金 | ● | | | | | | 市内部での対応協議 |
| 平成30年10月19日 | 金 | | | | ● | | | 近畿厚生局、奈良県地域医療連携課への報告 |
| 平成30年10月22日 | 月 | ● | | | | | | 議会、病院全職員に対する報告 |
| 平成30年10月23日 | 火 | ● | | | | | | セキュリティ対策ベンダーからの中間報告 |
| 平成30年10月23日 | 火 | | | | ● | | | 報道機関への情報提供 |
| 平成30年10月24日 | 水 | ● | | | | | | 議会全員協議会への報告 |
| 平成30年10月30日 | 火 | | | | ● | | | 厚生労働省、奈良県による立入調査 |
| 平成30年11月6日 | 火 | | | | ● | | | 奈良県による行政指導 |
| 平成30年11月13日 | 火 | ● | | | | | | セキュリティ対策ベンダーからの最終報告 |
| 平成31年1月31日 | 木 | | | | | ● | | 監査法人T社　業務時利用資料まとめ提出 |
| 平成31年3月15日 | 金 | | | | | | ● | TM社　サービス提供中間報告書提出 |
| 平成31年3月24日 | 日 | | | ① | | | | **第1回有識者会議** |
| 平成31年3月29日 | 金 | | | | | ● | | 監査法人T社　医療情報システム運用管理規程Ver 1.1提出 |
| 平成31年4月4日 | 木 | | ② | | | | | 第2回対策協議会 |
| 平成31年4月10日 | 水 | | ③ | | | | | 第3回対策協議会 |
| 平成31年4月11日 | 木 | | | | | | ● | TM社　NWおよび端末のリスク分析結果報告書提出 |
| 平成31年4月21日 | 日 | | | ② | | | | **第2回有識者会議** |
| 平成31年4月24日 | 水 | | | | ● | | | 奈良県庁打合せ |
| 令和元年5月17日 | 金 | | ④ | | | | | 第4回対策協議会 |
| 令和元年5月29日 | 水 | | ⑤ | | | | | 第5回対策協議会 |
| 令和元年6月2日 | 日 | | | ③ | | | | **第3回有識者会議** |
| 令和元年6月30日 | 日 | | | | | ● | | 監査法人T社　業務時利用資料まとめ提出 |
| 令和元年7月11日 | 木 | | ⑥ | | | | | 第6回対策協議会 |
| 令和元年7月14日 | 日 | | | ④ | | | | **第4回有識者会議** |
| 令和元年7月31日 | 水 | | | | | | ● | TM社　サービス提供完了報告書提出 |
| 令和元年8月31日 | 土 | | | | | ● | | 監査法人T社　有識者会議提言書提出 |
| 令和元年9月1日 | 日 | | | ⑤ | | | | **第5回有識者会議** |
| 令和元年9月2日 | 月 | | | | | | ● | TM社　サービス提供完了報告書提出 |

宇陀市立病院コンピュータウィルス感染事案に関する「報告書」（令和元年９月１日）(以降、「事案報告書」と記載)に基づき、初期対応内容を列記する。

**表 3.2　マルウェア感染後の初期対応経緯詳細**

UH：宇陀市立病院　SV：システムベンダー(医療情報システム)
SCV：セキュリティ対策ベンダー(トレンドマイクロ)

| | | |
|---|---|---|
| 平成 30 年<br>10 月 16 日<br>（火） | 午前 5 時 40 分頃<br>午前 8 時 00 分頃<br><br><br><br>午後 5 時 30 分<br><br><br><br><br><br>午後 7 時 30 分 | 事象確認　病院(UH)からシステムベンダー(SV)へ連絡<br>(SV)ウィルス感染確認<br>(UH)システム全面停止、ネットワークからの物理的遮断<br>(UH)紙カルテ、伝票運用による診察実施決定<br>(SV→UH)システム障害に関する状況報告<br>(UH)復旧見込み約 2 日必要と判断<br>(UH→SV)安全を確認して復旧するよう指示<br>(SV→UH)復旧に必要なバックアップデータ作成に必要な磁気テープが装填されていなかったと報告　①<br>(UH→SV)早急にウィルス感染経路や影響範囲を調査するよう指示 |
| 10 月 17 日<br>（水） | 午前 8 時 00 分<br><br>午後 0 時 00 分<br>午後 6 時 30 分<br>午後 8 時 30 分 | (SV→UH)現状では感染源の特定が出来ないのでネットワークモニタリング等での一定期間の確認が必要であると報告<br>(SV→UH)ウイルスチェックの終了及びウイルス除去終了報告<br>(UH)電子カルテ再稼働は、朝 7 時の状況により決定すると判断<br>(SV)ネットワークモニタリング監視のため、監視センサーを設置 |
| 10 月 18 日<br>（木） | 午前 7 時 00 分<br><br><br><br><br><br><br><br><br><br>午前 8 時 00 分<br><br>午後 6 時 00 分 | (SV→UH)次の 4 点を報告<br>・サーバ、クライアントパソコンを個別にウイルス除去し、再セットアップを完了<br>・各部門システムのウイルス感染状況調査と感染したウイルスの除去作業を完了させ、安全確認実施<br>・再発防止のため最新のウイルス対策ソフトをインストール<br>・監視センサーの設置及び SE の待機、データバックアップ機能の強化により安全運用を確認<br>(UH)上記報告を受け**電子カルテシステムの運用を再開**　②（外部ネットワークと接続せず病院内スタンドアロン[5]システムとして運用）<br>(UH→SV)ウイルス対策、バックアップの再確認及び感染対策を万全にするよう指示<br>(SV→UH)事故後の経過報告 |
| 10 月 19 日<br>（金） | 午前 8 時 40 分<br><br>午後 0 時 20 分<br><br>午後 0 時 30 分<br><br>午後 4 時 00 分 | (UH)市長へ電子カルテシステムの障害発生、初期対応の経過報告し、今後の対応について協議<br>(UH)近畿厚生局及び奈良県地域医療連携課へ今回の EC システムウイルス感染発生と、初期対応実施後 18 日からの再稼働を報告　③<br>(UH)病院全職員へ電子カルテシステムの障害発生に係る初期調査、経過報告及び今後の対応について説明（1 回目）<br>(SCV、SV、UH)感染経過調査の聞き取り |

[5] 機器やソフトウェア、システムなどを、他と接続せずに単独で使用すること

| | | |
|---|---|---|
| 10 月 22 日<br>（月） | 午後 3 時 00 分<br><br>午後 5 時 00 分 | (UH)EC システムウイルス感染発生と、初期対応実施後 18 日からの再稼働を報告し、併せて報道発表の予定を報告<br>(UH)病院全職員へ電子カルテシステムの障害発生に係る初期調査、経過報告及び今後の対応について説明（2 回目） |
| 10 月 23 日<br>（火） | 午後 2 時 00 分<br><br><br><br>午後 4 時 00 分 | (SV→UH)監視センサで通信を監視している LAN からは、外部への不正通信および感染拡散は確認されなかったと中間報告<br>　ウイルスにより暗号化されたデータの解読については継続して解析中と報告<br>(UH)報道機関へ宇陀市長名で電子カルテシステムの障害発生に関する情報提供（発生状況・直後の対応等）<br>　本事件によりカルテ情報の一部が参照不可となった患者 1,133 名に謝罪文書を送付 |
| 10 月 24 日<br>（水） | 午後 5 時 00 分 | (UH)宇陀市議会全員協議会にて、ウイルス感染の発生、経緯及び初期対応について報告 |
| 10 月 30 日<br>（火） | 午前 10 時 00 分 | (UH)厚生労働省と奈良県による立入調査 |
| 11 月 6 日<br>（火） | 午後 1 時 00 分 | (UH)奈良県より宇陀市立病院長に対する行政指導<br>・原因分析、被害状況の実態把握、再発防止対策について最終報告をとりまとめること<br>・個人情報の流出について再調査を行い、必要があれば患者や市民に正確な情報を伝えること |
| 11 月 13 日<br>（火） | 午後 3 時 30 分 | (SCV→UH)最終報告<br>・外部からのネットワーク経由で電子カルテの管理端末を経由して院内に侵入し、電子カルテサーバを暗号化した可能性が高い　④<br>・どのようにして端末に侵入したかは当該端末を初期化されていたため経路の追跡ができなかった　⑤ |

| | | |
|---|---|---|
| 平成 31 年<br>3 月 | | (UH)暗号化された電子カルテデータの復号化に成功し、すべての電子カルテデータが参照可能 |

### 3.4.2　事象発生中期対応(平成 30 年 11 月 14 日～令和元年 9 月 2 日)

平成 30 年 11 月 14 日以降の中期対応経緯を表 3.3 に示す。

表 3.3 マルウェア感染後の対応経緯（□中期対応）

| 年月日 | 曜日 | 病院 | 協議会 | 有識者会議 | 他機関 | T社 | TM社 | 対策内容 |
|---|---|---|---|---|---|---|---|---|
| 平成30年10月1日 | 月 | ● | | | | | | 電子カルテシステム運用開始 |
| 平成30年10月16日 | 火 | ● | | | | | | ウィルス感染 |
| 平成30年10月18日 | 木 | ● | | | | | | 対策後完全復旧(ローカル運用) |
| 平成30年10月19日 | 金 | ● | | | | | | 市内部での対応協議 |
| 平成30年10月19日 | 金 | | | | ● | | | 近畿厚生局、奈良県地域医療連携課への報告 |
| 平成30年10月22日 | 月 | ● | | | | | | 議会、病院全職員に対する報告 |
| 平成30年10月23日 | 火 | ● | | | | | | セキュリティ対策ベンダーからの中間報告 |
| 平成30年10月23日 | 火 | | | | ● | | | 報道機関への情報提供 |
| 平成30年10月24日 | 水 | ● | | | | | | 議会全員協議会への報告 |
| 平成30年10月30日 | 火 | | | | ● | | | 厚生労働省、奈良県による立入調査 |
| 平成30年11月6日 | 火 | | | | ● | | | 奈良県による行政指導 |
| 平成30年11月13日 | 火 | ● | | | | | | セキュリティ対策ベンダーからの最終報告 |
| 平成31年1月31日 | 木 | | | | | ● | | 監査法人T社　業務時利用資料まとめ提出 |
| 平成31年3月15日 | 金 | | | | | | ● | TM社　サービス提供中間報告書提出 |
| 平成31年3月24日 | 日 | | | ① | | | | **第1回有識者会議** |
| 平成31年3月29日 | 金 | | | | | ● | | 監査法人T社　医療情報システム運用管理規程Ver 1.1提出 |
| 平成31年4月4日 | 木 | | ② | | | | | 第2回対策協議会 |
| 平成31年4月10日 | 水 | | ③ | | | | | 第3回対策協議会 |
| 平成31年4月11日 | 木 | | | | | | ● | TM社　NWおよび端末のリスク分析結果報告書提出 |
| 平成31年4月21日 | 日 | | | ② | | | | **第2回有識者会議** |
| 平成31年4月24日 | 水 | | | | ● | | | 奈良県庁打合せ |
| 令和元年5月17日 | 金 | | ④ | | | | | 第4回対策協議会 |
| 令和元年5月29日 | 水 | | ⑤ | | | | | 第5回対策協議会 |
| 令和元年6月2日 | 日 | | | ③ | | | | **第3回有識者会議** |
| 令和元年6月30日 | 日 | | | | | ● | | 監査法人T社　業務時利用資料まとめ提出 |
| 令和元年7月11日 | 木 | | ⑥ | | | | | 第6回対策協議会 |
| 令和元年7月14日 | 日 | | | ④ | | | | **第4回有識者会議** |
| 令和元年7月31日 | 水 | | | | | | ● | TM社　サービス提供完了報告書提出 |
| 令和元年8月31日 | 土 | | | | | ● | | 監査法人T社　有識者会議提言書提出 |
| 令和元年9月1日 | 日 | | | ⑤ | | | | **第5回有識者会議** |
| 令和元年9月2日 | 月 | | | | | | ● | TM社　サービス提供完了報告書提出 |

## 4. 調査報告

### 4.1 一連の対応の妥当性１(医療情報システム信頼性回復への寄与)

#### 4.1.1 初期対応

3.4.1 項で整理した、本事案発生後の初期対応についての評価は以下のとおりである。

(注)前章までは「マルウェア」と表記してきたが、病院側から発行されたこれまでの報告書等の記載が「ウィルス」に終始しているため、本章以降では「ウィルス」と記載する。

**(1) ウィルス感染発覚後のシステム保全**

ウィルス感染発覚後、速やかに病院からシステムベンダーへ連絡され、状況確認の上、システムを全面停止し、外部ネットワークから遮断された。このことは、システムへの影響を最小限に抑え、システム保全に対して効果があるため、初期対応として評価できる。

**(2) ウィルス感染発覚後の病院運用**

医療情報システムの根幹をなすECシステムの停止を受け、止められない病院運営のため、紙カルテ、伝票運用に速やかに切り替える方針が採られたことは、初期対応として評価できる。しかし医療現場の混乱と作業量増加による職員への負担は多大なものであったと推測する。

**(3) ウィルス感染範囲の確認とウィルス除去**

発覚初日のシステムベンダーによる状況確認結果報告を受けたのち、システムベンダーへの対策指示により、ウィルス範囲の確認とウィルス除去について着々と対策が実施された。その結果、発覚2日後の朝にはスタンドアロンシステムとしての運用ながら、ECシステムの運用が再開された。(表 3.2中 ②) 2日間での運用再開は評価できるが、次の指摘ができる。

**ⅰ)磁気テープ装填がされておらず、バックアップデータが保存されていなかった**(表 3.2中 ①)

ECシステム運用開始10月1日から事象が発覚した10月16日までの約2週間という短い期間のデータであるが、それでもECシステムを直近の最新状態に復旧させるために必要かつ重要なデータである。これが保存できない状態でシステムが2週間も運用されていたということは非常に問題がある。

バックアップデータが保存されていれば、運用再開までの時間が短縮されていた可能性があるため、10月1日の正式運用開始前に実施されたECシステム最終調整・確認に手落ちがあったことを認めざるを得ない。

**ⅱ) システム復旧過程でウィルス感染端末が初期化された**(表 3.2中 ⑤)

ECシステム復旧後の信頼性評価や信頼性強化対策検討のためにも、ウィルスの感染原因、侵入経路等の分析、追跡等が非常に重要となる。しかし、システム復旧過程で当該端末が初期化されてしまったため、分析、追跡が不能となった。

このような状況を招いてしまった背景としては次の点が考えられる。

- ECシステムに関する様々なリスクが想定されていなかった。
- ECシステムに関する障害発生時の対応が想定されていなかった。
- ECシステム障害発生後の復旧過程における所定の手順が設定されていなかった。

**(4) ウィルス感染発覚後の監督官庁報告**

ウィルス感染発覚後の監督官庁報告は次の日数経過後に実施された。

■10月19日 (16日発生後3日後)　近畿厚生局、奈良県地域医療連携課 (表 3.2 中 ③)

状況把握、システム復旧と原因究明が急がれたため 3 日後となった。報告までの経過日数の良否は、EC システムを含む病院・宇陀市のセキュリティ対策基準には明記されていないため判断できない。今後速やかに設定することが必要である。いつ、誰が、何を、どこへ、どのように報告するか、5W1H を踏まえて設定しておくべきであると考える。

### 4.1.2　中期以降対応

#### (1)　事後対策、再発防止対策

3.4.2　項表　3.3 に示すように、初期対応が一段落した年明け平成 31 年 1 月以降は、事後対策、再発防止対策の動きがとられている。

■対策防止策策定等業務委託(県行政指導を受けての報告書及び有識者会議運営の支援業務)
有限責任監査法人トーマツ

■安全確認調査委託(ウィルス感染事案に関する調査・分析・システム支援業務)
トレンドマイクロ株式会社

■有識者会議(事案分析・対策協議組織)
5 名の外部有識者(委員長：上原立命館大学教授)
宇陀市・市立病院幹部
事務担当コンサルタント(上記 2 社)

これら一連の活動(有識者会議は平成 31 年 3 月～令和元年 9 月まで計 5 回開催)の結果、令和元年 9 月 1 日に「事案報告書」が取りまとめられた。「事案報告書」の内容は、次ページに示す目次のとおりである。

「事案報告書」では宇陀市長のことばから始まり、事案発生の概況、ウィルス感染の影響、事案発生後の対応、有識者会議での審議事項、見解と 3 項目の提言が示された。それを受けて各提言に対する市側の再発防止策が示された後、「宇陀市の決意」で締めくくられている。

「事案報告書」の内容は、事案発生の経緯、初期対応状況、有識者会議発足、事案発生原因分析、再発防止策策定、市民に向けての決意表明など、必要十分な内容が示されていると判断する。また、本事案は専門性が高く、非常に難解な内容ながら、「事案報告書」は市民に向けて、可能な限りわかりやすくまとめる工夫がなされていると評価できる。

上記に示した中期以降の対応は、外部の視点を入れて、事象の分析、課題抽出から再発防止策設定まで約 8 ヶ月間かけて実施されている。本事案の整理と再発防止策が設定されているため、中期以降の対応としては、必要十分な対策が実施されたものと判断する。

宇陀市立病院コンピューター―ウィルス感染事案に関する「報告書」目次(「事案報告書」目次)

目次

### 4.2　一連の対応の妥当性 2（投資効果）

#### 4.2.1　ウィルス感染の想定原因

ウィルス感染の想定原因は表 3.2 中④に記載したとおりであるが、「事案報告書」には次のようにまとめられている。

原因１

本来はインターネットに接続していない環境に、病院職員もしくは委託業者などの誰かが、何らかの「ルール違反」を犯してインターネットに接続し、何らかの方法により外部からの侵入を許してしまったこと。

原因２

医療情報システムの導入にかかる業者の管理や障害時対応の適切な運用体制が構築、運営されておらず、監督すべき病院のガバナンスに問題があったこと。

直接のウィルス感染原因は原因１に記載のとおりであり、ウィルスを EC システムに入れてしまったことである。間接的な原因が原因２に記載の内容であり、EC システム整備中にウィルスを EC システムに入れてしまう環境を作ってしまったことである。

原因１に対する対応は、緊急性と高度な専門性を要し、発注者側体制だけでは対処できない事案である。また、原因２に対する対応についても、客観性と高度な専門性を要する内容になるため、こちらも発注者側体制だけでは対処できない事案である。

#### 4.2.2　事案発生後の業務委託内容と費用

事案発生後の対応のために業務委託された内容と費用は表 4.1 のとおりである。

**表 4.1　事案発生後対応のための業務委託内容**

| 業務名 | 業務内容 | 業務委託先 | 期間・業務件数 | 契約金額 |
|---|---|---|---|---|
| Ⅰ．対策防止策策定等業務委託 | 県行政指導を受けての報告書及び有識者会議運営の支援業務 | 有限責任監査法人トーマツ | 平成 31 年 3 月～令和元年 8 月 3 件 | 3 件計 ¥11,880,000 |
| Ⅱ．安全確認調査委託 | ウィルス感染事案に関する調査・分析・システム支援業務 | トレンドマイクロ株式会社 | 平成 31 年 3 月～令和元年 8 月 4 件 | 4 件計 ¥25,596,000 |
| | | | 計　7 件 | ¥37,476,000 |

いずれの業務も随意契約での委託である。

業務Ⅰの委託先は、もともと EC システム導入時の「検収支援業務委託」を実施していた業者である。業務実施中に本事案が発生したため、別途内容の異なる支援業務を委託された。

また、業務Ⅱの委託先としては、何社か候補を挙げて検討していたが、業務内容や金額で折り合いがつかず、最終的に業務Ⅰ委託先の紹介により委託された。

委託金額は各委託先からの見積が採用される結果となっており、通常実施される入札手続きはとられていない。しかし前項 4.2.1　に記載した通り、緊急性と高度な専門性を要する委託であり、速やかな対応と短期間での取りまとめが必要な内容であるため、本委託は必須の委託であったと判断する。何よりも地域医療の拠点として唯一の公的医療機関の運用をいち早く正常化し、速やかにセキュリティ対策を強化する必要があったことを認識し、必要十分な費用拠出であったと認めざるを得ない。

### 4.3　医療情報システムの構築、運用、維持管理の妥当性

#### 4.3.1　医療情報システムを維持管理する上で認識しておくべき事項

近年の ICT[6]の進展により医療情報の電子化が進み、高度かつ機能性が高く、病院運営の効率化を図ることができる医療情報システムの導入は、全国どこの病院でも必須である。しかし、このシステムを取り巻く環境は 3.3　節に示したとおり、世界的にも深刻な状況であることを十分に理解しておくべきである。病院内のシステムは安全に運用されていたとしても、情報通信ネットワーク的に一歩外部に出ると、常に危険にさらされる状況なのである。

一方、システムの維持管理・正常運用、他システムとの連携(例:宇陀けあネットでの地域医療共有)のためには、情報通信ネットワークを介して外部との情報通信を行わなければならない。

医療情報システムを取り巻く環境の厳しさを認識した上で、地域医療ネットワーク等、ICT を利用した先進サービスを構築し安心・安全に利用するためには、次の対応が必要かつ重要である。

ⅰ）セキュリティポリシーの設定
ⅱ）設定したポリシーで定めたルールの厳守
ⅲ）セキュリティを確保するために必要十分なシステムの構築
ⅳ）システムの綿密な維持管理
　　(セキュリティホールを防ぐ OS やソフトウェアのアップデートなどを含む)

#### 4.3.2　医療情報システム構築の妥当性

図　4.1 に現在の EC システム、ネットワーク概略図を示す。既に医療に関わる非常に専門性の高い複雑なシステム、かつそれらを束ねる複雑なネットワークになっていることがわかる。これらを外部のサイバー攻撃[7]から守らなければならないことから、市立病院、かつ宇陀市の職員は、まず全体的にその任務の重さを再認識することが必要かつ重要である。

事案発生後の初期対応、中期対応により、当初の EC システム、ネットワーク構成（図 3.1）からセキュリティが強化されている。

ファイアウォール(FW)の導入　　：外部からの通信を監視し、不正な通信を防ぐ
RADIUS サーバの導入　　：無線 LAN に接続する端末を監視し、不正な端末の利用を防ぐ
ネットワーク監視装置の導入　　：ネットワーク内部での不正な挙動などを監視

事案発生後の分析を受け、現在の EC システム、ネットワークは非常にセキュリティ性の高いものになっていると判断する。

ここで 1 点だけ確認を必要とする事項を示す。

**ⅰ）EC システムと外部との複数接続（ドクターネットとの接続）**

外部のサイバー攻撃から EC システム、ネットワークを守るためには、できるだけ外部との接続を少なくすることが望ましい。接続数が増えると外部からの攻撃を受ける経路が増えると共に、セキュリティ対策が複数必要になり、それらのレベルに差が生じやすいためである。

図 4.1 に示すとおり正規の外部ネットワーク接続点（左上側）の他に、ドクターネットサービス利用のための別の接続点がある。(右上側)

おそらく病院側の正規ネットワークとは縁を切り、別のネットワークとしてクラウドのドクターネットと接続されているものと思われるが、接続点を一本化した場合の得失を検討し、可能であれば一本化しておくことが望ましい。

---

[6] 情報や通信に関連する科学技術の総称。特に、電気、電子、磁気、電磁波などの物理現象や法則を応用した機械や器具を用いて情報を保存、加工、伝送する技術

[7] あるコンピュータシステムやネットワーク、電子機器などに対し、正規の利用権限を持たない悪意のある第三者が不正な手段で働きかけ、機能不全や停止に追い込んだり、データの改竄や詐取、遠隔操作などを行うこと。

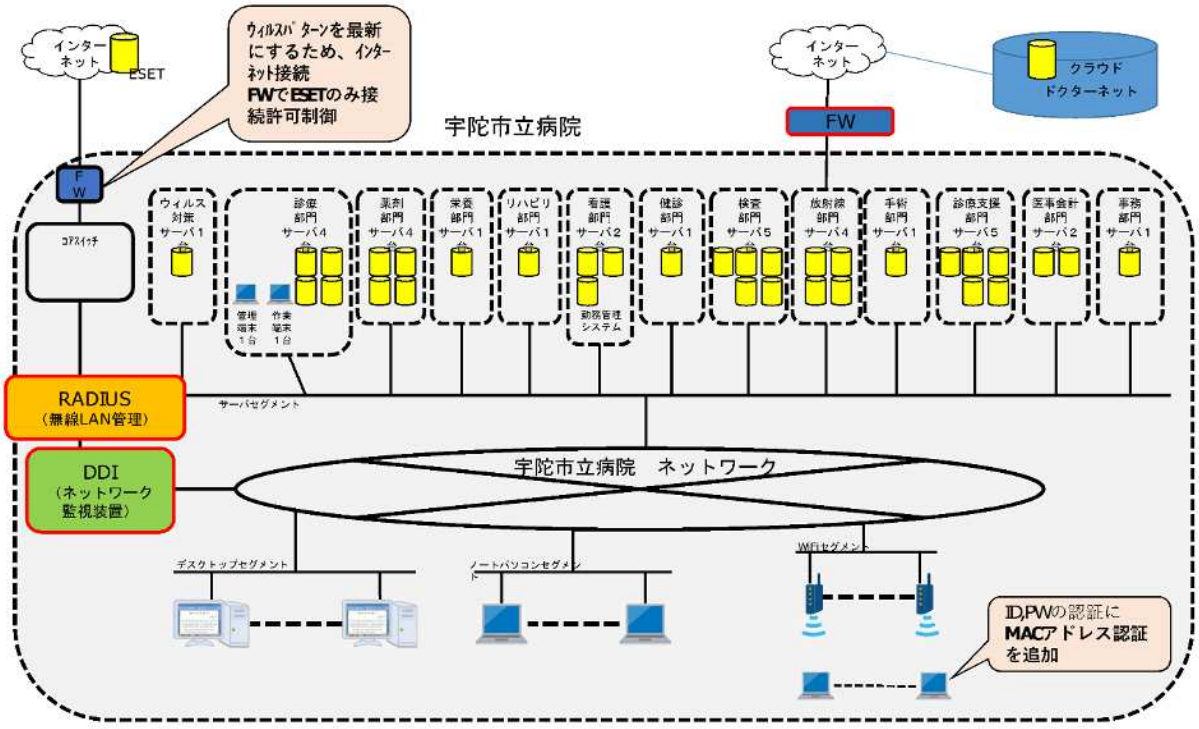



図 4.1　宇陀市立病院　EC システム、ネットワーク概略図(平成 31 年 2 月時点)

今回の事案は EC システム構築時の思わぬセキュリティホール(穴)からウィルスが入り込んでしまったことによる障害発生であったが、構築時の病院関係者、もしくは構築関係者の「ルール違反」が発端であると予想されている。今後またシステムの老朽化によって発生する再構築時には、このような「ルール違反」が発生しないよう、発注者側に専門性の高い職員を配置し、セキュリティ的に適切な監督ができる体制にしておく必要がある。

### 4.3.3　医療情報システム運用、維持管理の妥当性

前項で示したように EC システム、ネットワークのセキュリティ強化は適切に図られている。重要なのはこれらを今後適切に運用、維持管理していくことである。そのためには次の事項が重要である。

ⅰ）システムの綿密な維持管理　（4.3.1　に示した項目ⅳの再掲）
（セキュリティホールを防ぐ OS やソフトウェアのアップデートなどを含む）

ⅱ）システム維持管理者の設置、維持管理者によるセキュリティ最新状況の学習の継続
→専門技術者を登用（複数人以上が望ましい）し、最新状況を常に学習する環境におく

ⅲ）事象発生時の初期対応業者との提携
→事象発生時の迅速な初期対応のために、応援を求めることができる初期対応業者と提携し、緊急時の体制づくりをしておく

現在は一連の中期対応による「事案報告書」が取りまとめられ、再発防止策が設定されている。それにより上記ⅱ）に示したシステム維持管理者として専門技術者が 1 名登用され、病院の情報システム管理室が合計 3 名で今後の維持管理にあたる体制が確立された。

維持管理の業務とその実施体制については事案発生後に改善が図られている。しかし、外部からのサイバー攻撃は日々進化しているため、それに耐えうる継続的な学習と備えが必要であることを念頭に置き、今後も引き続き対応していく必要がある。

また、万が一同様の事象が発生した場合に速やかに対応できる体制づくりが重要であるため、今後検討しておき、いざという時のための備えを万全にしておく必要がある。

## 5. まとめ

今回発生した事案は、宇陀市立病院の医療業務を高度化、効率化させるECシステムを導入する際に守るべきセキュリティに対する「ルール違反」が発端になり、重大な事案発生につながってしまったものである。事案発生後の対応やシステムの構築、運用、維持管理について調査した結果を報告したが、地域医療にとって欠かせないものとなった非常に重要かつ複雑な医療情報システムを取り巻く環境が非常に厳しいものであること、それを守るために万全の対策を講じておくことが非常に重要であることを改めて認識し、今後ECシステムを適切に運用、かつ維持管理していく必要がある。

そのためには適切な維持管理のための体制づくりと予算措置がどうしても必要である。地方自治体の財政は必ずしも潤沢ではない環境であるが、地域医療に欠かせないシステムを運営していくための必要な措置である。よって今回不幸にも発生した事案を、逆に適切な運用のために必要な教訓であったと前向きにとらえ、今後必要十分なシステム構成、および維持管理体制を整えて、導入したECシステムを十分に利活用した地域医療活動に繋げて頂くことを希望する。