宇陀市立病院コンピューターウイルス感染事案に関する「報告書」

令和２年２月２８日

宇陀市

目次

はじめに（市長から患者・市民の皆様へ）

平成３０年１０月１６日、宇陀市立病院において、コンピューターウイルスに感染し、電子カルテを含む医療情報システムが使用できない状況となりました。同年１０月１８日にシステムは復旧したものの、一部の患者カルテ情報が暗号化され、診療記録等の参照ができない状況が継続し、宇陀市立病院をご利用の患者様・市民の皆様をはじめ多くの病院関係者の皆様に多大なご迷惑をお掛けしましたことを、心からお詫び申し上げます。

本件事案は、事の重大性から、厚生労働省及び奈良県による宇陀市立病院への立入調査を受け、その結果、原因分析、被害状況の実態把握、再発防止策等の報告等を行うように奈良県より行政指導を受けました。

それを受けて、宇陀市全体として取り組むために、平成３１年１月に市長を本部長とする「市立病院コンピューターウイルス感染事案対策本部」を設置し、必要な対策を講じてまいりました。

さらに、本件事案が医療業界の情報セキュリティ関係者から注視されていることも踏まえ、平成３１年３月に事案の審議をいただくため、第三者委員会として「市立病院コンピューターウイルス感染事案有識者会議」を設置しました。
有識者５名の委員の皆様により、平成３１年３月より９月までに全５回の開催で、原因分析、再発防止に向けた精力的な議論を重ねられ、提言書をいただいたところです。

委員の皆様におかれましては、専門的な見地から、本質的な課題のご指摘と貴重なご助言、適切なご指導をいただきましたことに対し、心から感謝申し上げる次第です。

宇陀市・宇陀市立病院では、この提言を厳粛に受け止め、これまでの実態や改善策、今後の継続的な対応計画について、市民や関係者の皆様に正確な情報提供を行うため、本報告書を取りまとめ公表いたします。

私たち職員は、この教訓を真摯に受け止め、患者様をはじめ、宇陀市立病院をご利用いただくすべての皆様が安全で安心して受診・療養生活を送っていただけるように、ガバナンスの改革を進めてまいります。

令和２年２月
宇陀市長　　髙　見　省　次

１．事案発生の概況

平成３０年１０月１６日に、宇陀市立病院の医療情報システムの中核である、電子カルテシステムがウイルスに感染し、電子カルテシステムの利用が不可能となりました。

システムデータが暗号化[1]されたこと、バックアップが正しく取得されていなかったことから、システムを停止し、電子カルテシステム他、影響のあったシステムの再構築を行ったため、１０月１８日までの丸二日間、電子カルテシステムを全面停止しました。

なお、システム停止期間中は紙カルテにより診療を継続しました。

事案発生日以降の約１ヶ月間の経過は以下のとおりです。

平成 30 年 10 月 16 日（火）

午前 5 時 40 分頃　職員が、電子カルテシステムが使用出来ない状況であることに気づき、システムベンダー[2]に連絡しました。

午前 8 時頃　システムベンダーの担当者が確認したところ、サーバ画面にウイルス感染を示すメッセージの表示を確認したため、システムを全面停止し、ネットワークからの物理的遮断（コンピューターの LAN ケーブルを抜く）を行いました。

経営幹部（病院長・副院長・看護部長・事務局長）が復旧作業に時間を要すると判断し、紙カルテ及び伝票運用による診療を行うことを決定しました。

午後 5 時 30 分　システムベンダーの担当者より経営幹部に電子カルテシステム障害に関する状況報告がありました。

病院長が部門システムベンダー各社にウイルスチェック等の対応を指示し、リモート・オンサイトでチェックしました。

病院長は、システムベンダーから、再セットアップによる復旧見込みが約２日間を要するとの報告を受け、安全を確認して復旧するとともに、証拠保全するようにシステムベンダーに指示しました。

また、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ことがシステムベンダーからの報告により判明しました。

---

1 データが参照できない状態になる。

2売り主、売り手。また、販売会社。特にＯＡ機器、ソフトウエアなどの販売納入業者。システムの開発会社をさすこともある。

午後 7 時 30 分　病院長が、システムベンダーに対し、早急にウイルス感染経路や影響範囲を調査するよう指示しました。
経営幹部がシステムベンダーと協議して調査方法を決めました。

平成 30 年 10 月 17 日（水）

午前 8 時　システムベンダーから経営幹部に対して、「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」との報告がありました。

午後 0 時　部門システムベンダー各社によるウイルスチェックの終了及びウイルス除去は終了したとの報告が経営幹部にありました。

午後 6 時 30 分　経営幹部の判断で、電子カルテ再稼働については、翌日朝 7 時の状況により決定することとしました。

午後 8 時 30 分　ネットワークモニタリング監視のため、経営幹部の指示により、システムベンダーが監視センサーを設置しました。

平成 30 年 10 月 18 日（木）

午前 7 時　システムベンダーより経営幹部に「サーバ[3]、クライアントパソコンを個別にウイルス除去し、再セットアップが完了しました。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、安全確認を行うとともに再発防止のために最新のウイルス対策ソフトをインストールしました。また、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が確認できた」との報告があり、電子カルテシステムの運用を再開しました。

午前 8 時　病院長がシステムベンダーにウイルス対策、バックアップの再確認及び感染対策を万全にするように指示しました。

午後 6 時　システムベンダーより経営幹部に事故後経過報告がありました。

平成 30 年 10 月 19 日（金）

午前 8 時 40 分　病院長、事務局長が市長に、電子カルテシステムの障害発生、初期対応の経過報告を行い、今後の対応について協議を行いました。

午後 0 時 20 分　近畿厚生局及び奈良県地域医療連携課に、ウイルス感染により電子カルテシステムに障害が発生し初期対応を行った後、18 日から再稼働したことを報告しました。

[3] コンピューターネットワークにおいて、他のコンピューター（クライアント）からの求めに応じて何らかの情報処理サービス（ファイルの提供等）を行うコンピューター・ソフトウェアのこと

午後0時30分　病院全職員に対して、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を行いました。（１回目）

午後4時　セキュリティ対策ベンダー、システムベンダー、病院事務局が感染経過調査の聞き取りを行いました。

平成30年10月22日（月）

午後3時　事務局長から議会に対して、ウイルス感染により電子カルテシステムに障害が発生し初期対応を行った後、18日から再稼働したことの報告を行い、併せて、報道発表の予定について報告しました。

午後5時　病院全職員に対して、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を行いました。（２回目）

平成30年10月23日（火）

午後2時　セキュリティ対策ベンダーから経営幹部に対して、監視センサーにより通信を監視しているＬＡＮにおいては、外部への不正通信及び感染拡散は確認されなかった中間報告を受けました。
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の報告がありました。

午後4時　報道機関に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）をしました。
本事件による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しました。

平成30年10月24日（水）

午後5時　宇陀市議会全員協議会にて、事務局からウイルス感染の発生、経緯及び初期対応についての報告を行いました。

平成30年10月30日（火）

午前10時　厚生労働省と奈良県による立入調査を受けました。

平成30年11月6日（火）

午後1時　奈良県より以下のとおり、宇陀市立病院長に対する行政指導を受けました。

・原因分析、被害状況の実態把握、再発防止策等について最終報告をとりまとめること。
・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。

平成 30 年 11 月 13 日（火）

午後 3 時 30 分　セキュリティ対策ベンダーからの最終報告がありました。

・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。

・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。

２．ウイルス感染の影響

電子カルテシステムのデータファイルが暗号化されたことで、患者カルテの参照ができなくなり、医療情報システム全体に影響が及びました。

なお、暗号化された電子カルテデータは、平成３１年３月に復元に成功したことにより、現在は全ての電子カルテデータが参照できる状態になっています。

本件事案における被害は、本件事案発生月の診療報酬請求に影響が及び、福祉医療費助成制度等に基づく償還に遅れが生じました。

また、電子カルテシステムの復旧を優先する一方、システムログ[4]の保全を行わないままシステムの再セットアップを行ったことで、正確な原因究明ができない状況になりました。その結果、個人情報の漏洩の有無について、明確に否定することは不可能な状況であります。

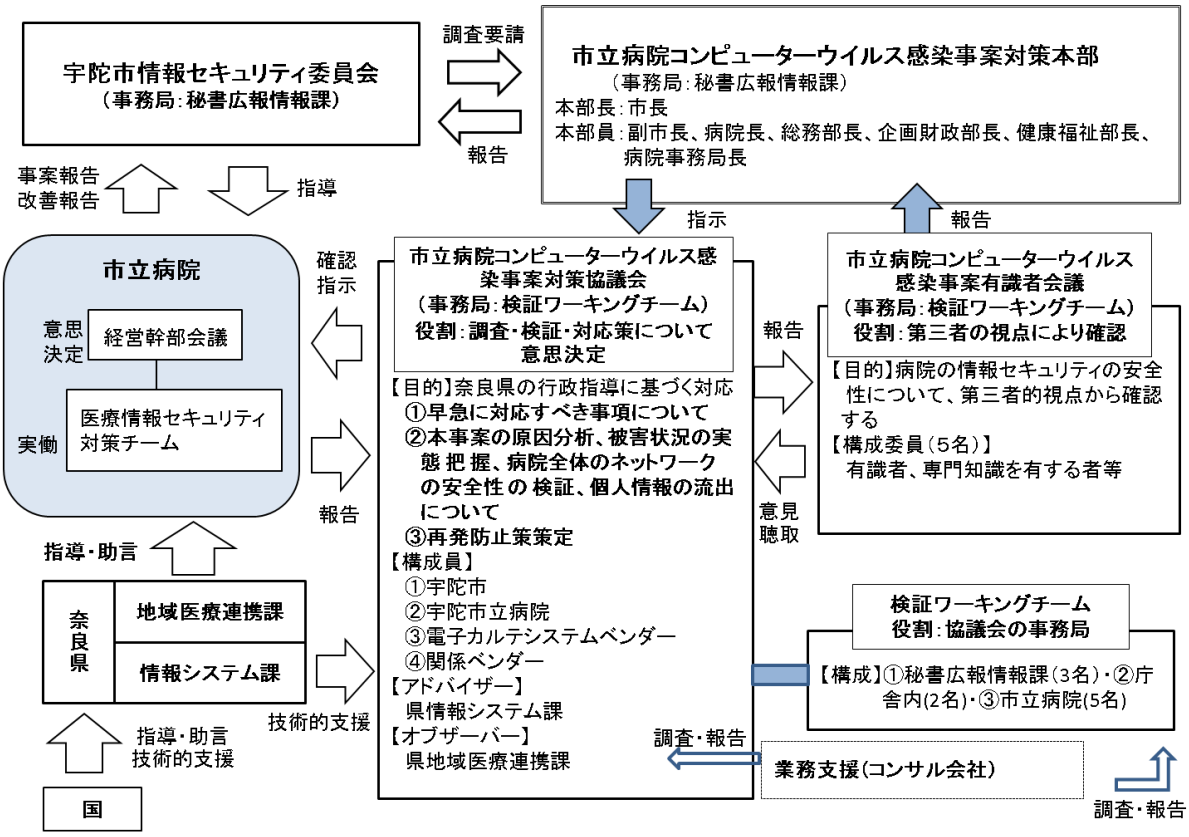
なお、現時点において個人情報の漏洩あるいは悪用されたとの被害報告はありません。

[4] コンピューターやソフトウエアが、その起動や停止、設定変更、処理した情報や通信に関する内容、処理結果、エラーの有無内容等を自動的に時系列で記録したもの。

３．事案発生後の対応

市立病院コンピューターウイルス感染事案対策の体制

本件事案の解決に向けて、平成３１年１月２１日、市長を本部長とした「市立病院コンピューターウイルス感染事案対策本部」を設置するとともに、「対策協議会」及び「検証ワーキングチーム」を立ち上げ、宇陀市全体の取り組み体制としました。



【宇陀市情報セキュリティ委員会】

宇陀市が保有する情報資産の機密性、完全性及び可用性を維持するため、宇陀市が実施する情報セキュリティ対策を推進する全庁的な組織体制として平成１９年４月に設置。

組織体制：最高情報統括責任者：宇陀市副市長

統括情報セキュリティ責任者：宇陀市総務部長

【市立病院コンピューターウイルス感染事案対策本部】

本件事案解決の意思決定の場となる対策本部。

役職	部　局
本部長	宇陀市長
副本部長	宇陀市副市長
本部員	宇陀市立病院長
本部員	宇陀市総務部長
本部員	宇陀市企画財政部長
本部員	宇陀市健康福祉部長
本部員	宇陀市立病院事務局長

【市立病院コンピューターウイルス感染事案対策協議会】

本事案の原因分析、被害状況の実態把握、病院全体のネットワークの安全性の検証、再発防止策策定を議論する組織。

目的　奈良県の行政指導に基づく対応について協議

① 早急に対応すべき事項の検討

② 本事案の原因分析、被害状況の実態把握、病院全体のネットワークの安全性の検証、個人情報の流出の確認

③再発防止策策定

構成員　・宇陀市（情報システム担当）

・宇陀市立病院

・奈良県総務部情報システム課（アドバイザー）

・奈良県地域医療連携課（オブザーバー）

・電子カルテシステムベンダー

【市立病院コンピューターウイルス感染事案検証ワーキングチーム】

目的　「有識者会議」「対策本部」「対策協議会」の事務局

構成　宇陀市及び宇陀市立病院

４．市立病院コンピューターウイルス感染事案有識者会議

本件事案を受けて、原因調査及び分析、再発防止策の検討を行うため、市立病院コンピューターウイルス感染事案有識者会議（以下「有識者会議」という。）を設置しました。

職　名	氏　名	所　属
会長	上原　哲太郎	立命館大学 情報理工学部教授
委員 （会長代理）	玉本　哲郎	奈良県立医科大学付属病院 医療情報部部長
委員	山口　雅和	ＩＳＡＣＡ大阪支部　理事 NPO 法人　情報システム監査普及機構　理事 日々創発　代表
委員	加藤　久和	宇陀地区医師会会長 一般社団法人宇陀地域医療・介護連携ネットワーク運営協議会　代表理事
委員	下村　敏博	奈良まほろば法律事務所 弁護士

（１）有識者会議における議論の内容

５回の有識者会議での議論

①本件事案の発生・対応経緯の確認と今後の検討に関する方向性の確認について

②調査結果、原因分析及び再発防止策の確認について

③運用管理規程の整備状況について

④提言書の内容の確認 について

⑤再発防止策を含む報告書の確認について

（２）本件事案の調査内容

本件事案の原因調査を事案発生直後の平成 30 年 10 月と、平成 31 年 3 月にセキュリティ対策ベンダーに委託しました。

調査内容

①電子カルテシステムのサーバ及び管理端末の調査

・実施日：平成 30 年 10 月 17 日（水）

②ネットワーク監視機器による不正通信の監視

・実施日：平成 30 年 10 月 17 日（水）～10 月 31 日（水）

③サーバ全台の詳細調査（ヒアリング及び調査を実施、併せて実機の設定値確認）

・実施日：平成 31 年 3 月 11 日（月）10:00～3 月 13 日（水）21:00

④ネットワーク監視装置による不正通信の監視（上記の調査と並行して不正通信監視を実施）

・実施日：平成 31 年 3 月 11 日（月）10:00～3 月 13 日（水）21:00

・過去 1 か月分（平成 31 年 2 月 10 日～）のシステムログを含めた調査を実施しました。

調査結果 1

☆ウイルスの種類

①の調査によりウイルスの種類は、ランサムウエアであることが判明しました。

ランサムウエア（GandCrab）

（GandCrab は、2018 年 1 月に存在が発見されました。感染したファイルを暗号化し参照できなくなるコンピューターウイルス。
英文で「あなたのファイルは暗号化されました」「ファイルはすべて取り戻せます」とのメッセージと共に、復元のための解除代金が要求されます。）

※本件事案で、電子カルテシステムのデータファイルが暗号化されましたが、復元のための解除代金の要求には応じていません。

☆感染範囲

①の調査により、電子カルテを含む診療部門システムサーバ 4 台、診療部門端末 2 台、ウイルス対策サーバ 1 台、看護部門サーバ 1 台が感染していることが判明しました。

これらのサーバ、端末は、本来、外部のネットワークに接続していないはずでした。

☆ウイルスの残存

②から④の調査により、現時点では病院内のネットワークに未知のウイルスが存在していないことが確認できました。概要は、以下のとおりです。

［ネットワーク］

ネットワーク監視装置のログ確認を行いましたが、病院情報システム系（ＨＩＳ系）において未知のマルウエア[5]に関連する危険度の高い不正通信は確認されませんでした。

［サーバ］

全台について詳細調査を実施し、不正プログラムが存在しないことを確認しました。

[5]不正・有害な動作を行う意図で作成された悪意のあるソフトウエアの総称。何らかの不正な命令を実行したり、外部への通信を行ったりする。

［端末機］

ウイルス対策ソフトによる最新のパターンファイル[6]での全ファイル検索を実施した結果を元に、検知ログを確認し、不正な検知が無いことを確認しました。

☆感染経路の特定

感染した機器が初期化され、証拠保全がなされなかったため、感染経路の特定はできませんでした。

調査結果２

☆関係者への聞き取り調査

本件事案発生後の病院職員及び電子カルテシステムベンダーへの聞き取り調査では、どこからも原因となり得る操作、行為は確認できませんでした。

① 病院職員への聞き取り（医務課から事案発生時の当直職員への聞き取り）

第１回：平成３０年１１月１日～５日

第２回：平成３１年４月１日～２日

② システムベンダーへの聞き取り（医務課とセキュリティ対策ベンダーからシステムベンダー関係者への聞き取り）

第１回：平成３０年１０月１８日

第２回：平成３０年１０月１９日

第３回：平成３１年４月１０日

☆マトリクス[7]分析

本件事案においては、管理端末のシステムログが残っておらず、正確な原因の特定が出来なかったため、有識者会議では考えられる状況を可能な限り想定した上で対策を検討いただきました。具体的には、それらの状況に対する対策を総合的に整理し、重点対応すべきリスクを確認するために、運用的対策をリスクコントロールの観点からマトリクス検証を行いました。

マトリクス検証により、管理体制の見直しの必要性と技術的対応の不足が判明したため、それらの対策をシステム運用管理規程に反映させて、同様の事案に対し必要な対策をすべてシステム運用管理規程に記載しました。

---

6 ウイルスを感知するために、各ウイルスの特徴をまとめたデーターベース。過去に登場したウイルスに関する情報が登録されている。

7 あるテーマについて細かく内容を掘り下げていく際に、関連する情報を縦軸と横軸に分類することで、それらの相関関係やポジショニングを捉えることができる。

（3）有識者会議の見解

有識者会議での本件事案の調査・分析の検証において、本件事案を誘発した原因として、提言にあるように基本的なルールを守らなかった結果、外部と接続されないはずの医療情報システムが外部と接続された状況になり、ウイルスの侵入・感染に至った可能性が高いとの指摘がありました。

また、システム復旧を優先する一方、証拠保全を行わないまま医療情報システムの再セットアップが行われたことで、正確な原因究明ができない状況になった点については、事案発生時の初期対応が不適切であり、証拠保全の観点が欠落していたとの指摘がありました。

院内のネットワークにおいてもウイルス攻撃を許したシステム的な予防対策が不十分であったこともウイルス感染の要因でもあるとしています。

有識者会議は、本件事案の調査結果とこれまでの議論を踏まえ、事案の発生原因を以下のように結論づけています。

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[8]に問題があったこと。

（4）提言書の内容

５回の有識者会議の議論の中で、今後、本件事案と同様の事態が発生しないように、発生経緯の確認と具体的な対策案について協議をいただきました。

その総括として、有識者会議より宇陀市・宇陀市立病院に対し、再発防止に係る対策・改善を行うように次に掲げる３つの提言がありました。

提言１

医療情報システム運用管理規程の見直し、遵守徹底、等のガバナンスの強化

① 今回の事案を誘発した原因として、「医療情報システムのネットワークには、私物のパソコンやネットワーク機器を接続しない」、という基本的なルールを守らず、私物のパソコンもしくは Wi-Fi ルータを持込接続した可能性が考えられる。この病院職員もしくは委託業者等による「ルール違反」により、外

[8]組織や社会に関与するメンバーが主体的に関与を行う意思決定、合意形成のシステムのこと。

部と接続されないはずの医療情報システムが外部と接続された状況になり、結果的に、医療情報システムへの侵入・コンピューターウイルスへの感染に至った可能性が高いと推測される。

一方で、本件事案発生後の内部聞き取り調査では、どこからもその「ルール違反」の原因となり得る報告が行われていない。このことは、総じて宇陀市・宇陀市立病院としての情報セキュリティに対するガバナンスが機能していなかった可能性を表している。

ガバナンスを機能させるには、医療情報システム運用に責任ある立場の職員は、業者任せにならない運用を行い、システム利用者の資質向上に努める必要がある。また、監督的立場にある職員は、リスクに正しく対応する職場風土を作っていくことが求められる。加えて、システム利用者は、ルール遵守はもとよりインシデント発生時には正しい対処が求められる。

② 本件事案発生当時、システム復旧を優先する一方、システムログの保全が行われないままシステムの再セットアップが行われたことで、正確な原因究明ができない状況になった点については、事案発生時の初期対応が不適切であり、証拠保全の観点が欠落していたといえる。コンピューターウイルス感染時対策は、自然災害発生と同様に、災害発生時の対策（BCP）として見直すとともに、定期的な訓練・教育も行うべきである。

③ これらのガバナンスや対応・訓練・教育の根拠とすべき、医療情報システムに関する宇陀市立病院の運用管理規程は、本件事案発生時においても存在していたが、今回の事案を防ぐために必要な内容が不足、もしくは十分に適用されていなかった状況が認められた。当会議での検討を通して、新たに見直された運用管理規程に記載されている内容については、早急にその実効性を担保する対策を取り、継続的にその実施状況を見直す体制を組むことが必要と考えられる。

④ これらの対策・対応の実施状況については、宇陀市・宇陀市立病院による、定期的な内部監査の実施を求めるとともに、内部監査での検証不足を補う意味でも、宇陀市以外の外部機関による外部セキュリティ監査も定期的に受ける事を推奨する。

提言２

医療情報システムのみならず、院内情報システム全体への技術的対策の強化

① 一例として、本件事案発生時に、私物の Wi-Fi ルータ等を通して、院内のネットワークと外部インターネットが接続可能な状況になっていた、電子カルテ端末のリモートデスクトップ操作が常時許可された状態になっていた、といったシステム的な予防対策が不十分であった可能性のうち、早急に対策が必要な内容への対応は完了したとの報告を受けている。

② 今後は、短期的に行える対策の継続はもちろんであるが、追加のシステム導入などによる中長期的な対策などを含め、より多面的な技術的対策を行うことが必要である。

③ 中長期的な対応が必要な事項については、費用対効果を鑑みながらの対応となるが、自治体病院の特性上、すぐに対応ができない事項がある場合も考えられるため、いつまでに、どのような形で実施するといった、具体的な計画を示すべきである。

提言３

市民に向け、本件事案及び対策についての報告書の作成・公表

① 本提言を踏まえ、宇陀市・宇陀市立病院としての対策状況・今後の対策方針を整理し、市民に向けて公表すべきである。

② 前述のとおり本件事案発生当日のログが残っていないため、個人情報の流出があったか否かの断定が行えない状況にある中、実際に個人情報の漏えい・悪用の被害報告はないが、住民感情として不安を抱かせたことは間違いないため、正確な報告が必要である。

③ サイバーセキュリティの世界では日々新たな脅威が発生しており、セキュリティ対策はそれに対応した継続的な対応が必要である。その上で、既知の問題への対策は、すべて行った（行っている）と市民に伝え続けることは重要である。

５．有識者会議の提言を受けた再発防止策について

今後は事案を二度と発生させないため、有識者会議からの提言に沿って、詳細については後述しますが、ガバナンスの強化、システム的対応の観点から再発防止策を策定しました。

ガバナンスの強化の観点からは、①組織の見直し、②緊急時における対応の見直し、③職員研修・訓練、④運用管理規程と運用管理体制の見直しを行いました。

また、システム的対応の観点からは、有識者会議で求められた対策について、①短期的対策、②中長期的対策に分けて、対策を既に図り、もしくは今後図っていくことにしています。

特に組織の見直しについては、本件事案は、ガバナンスが不十分であったとの指摘を有識者会議から受けたことを踏まえ、宇陀市立病院が取り扱う医療情報資産を適切に管理し、医療情報システムの安全対策を総合的に推進するため、「情報システム管理委員会」を設置するとともに、病院事務局内に「情報システム管理室」を設置し、専門職員を配置します。

重要なことは、これらの対策が個別に行われるのではなく、規程の見直し、周知・教育・実施、実施状況の自己（相互）点検、監査による外部評価の４つが有機的に結合し、継続的に情報システム管理委員会で協議し、改善を図っていくというサイクルを情報セキュリティに係る「組織の認識」として定着させていくことが必要であると考えています。

また、サイバーセキュリティの世界では、日々新たな脅威が発生しており、管理体制の人的対応だけでは、未知の攻撃に対しても安全と言い切れるものではありません。システム的対策はそれに対応した継続的な取り組みが必要であり、より多面的な安全対策として、中長期的なシステム対応を講じていきます。

提言１の対応

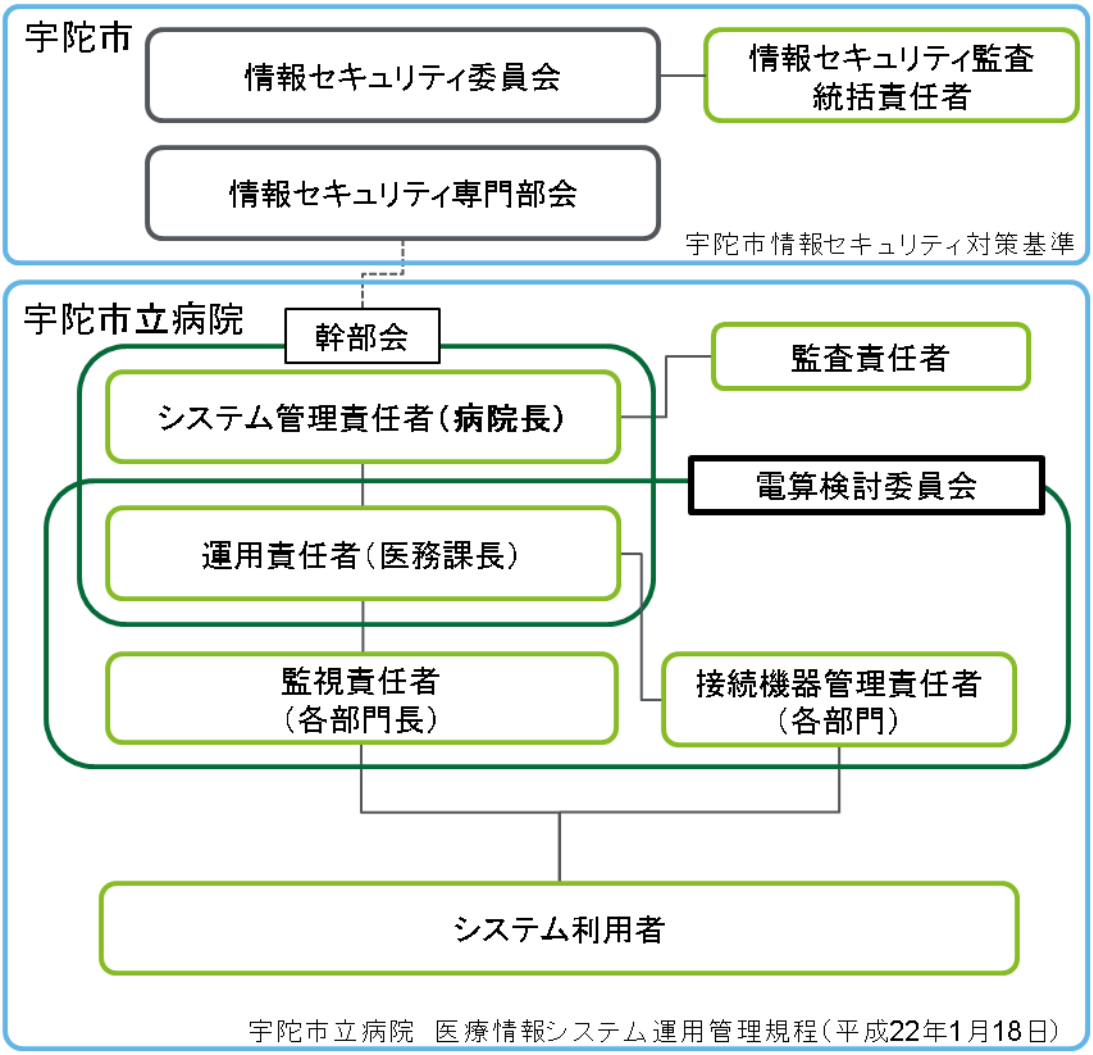
（１）医療情報システム運用管理規程の見直し、遵守徹底等のガバナンスの強化

①組織の見直し

◆セキュリティ管理体制の見直し

従来の管理規程・体制では、今回発生したようなインシデントへの具体的な対応を想定できていなかったため、医療情報システム責任者の明確化、専門職員の配置、宇陀市・市立病院幹部も関与する体制に見直しました。

☆宇陀市及び市立病院の情報システムセキュリティ管理体制（見直し前）



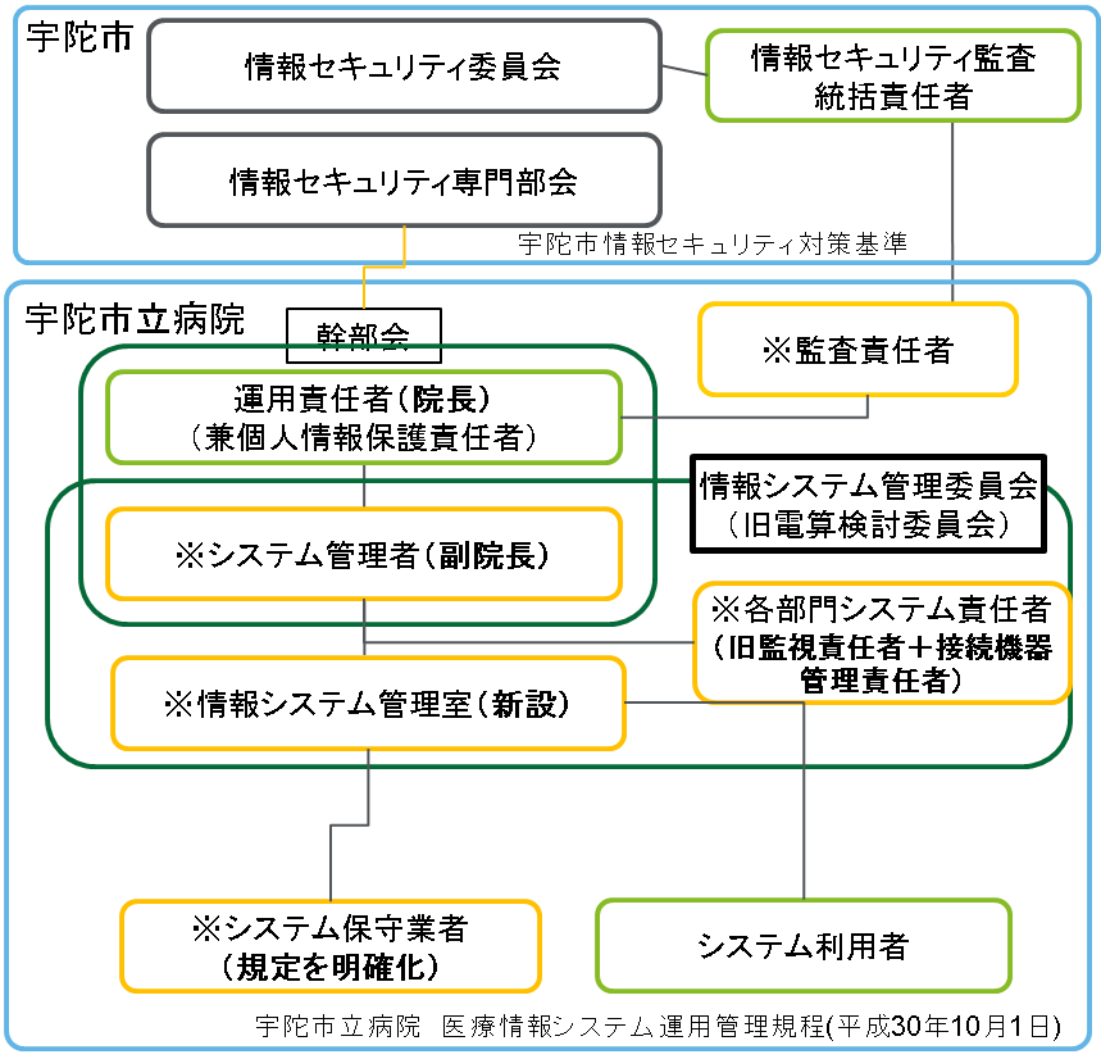
本件事案発生の要因でもある管理体制についての課題・解消方針及び対策

本件事案発生時の市・市立病院の管理体制についての課題を整理し、有識者会議での助言を踏まえて、以下のとおり解消方針を検討、対策を講じました。

NO	課題	解消方針	対策
1	市と病院の連携基準が曖昧であった	病院の基準を見直し、市の各種規程が前提にあることを明確にする	病院の運用管理規程を見直し、市の規程が前提であることを明確にした
2	電算検討委員会での検討に対する経営的責任が曖昧であった	委員会の責任者に幹部（副院長）を据え、情報システムの運用が経営課題であることを明確にする	情報システム管理委員会を設置、システム管理者に病院副院長を任命した
3	監査責任者制度が、有効に機能していなかった	監査責任者を病院職員または市担当者とすることで課題の解消を図る	運用管理規程を見直し監査体制を整備した。監査計画を策定し、定期的に外部監査、内部監査を行う体制とした
4	監視責任者・接続機器管理者の業務定義が曖昧だった	各部門の責任者・担当者が行うべき業務が具体的に定義されておらず、インシデント発生時の対応が個々人の知識・経験に依存する形になっていた。具体的な連絡ルールや対応基準を定め、インシデント発生時の対応を明確にする	監視責任者と接続機器管理責任者が分かれていたが、各部門システム責任者に統合の上、情報システム障害時対応マニュアルを策定しインシデント発生時の対応を明確にした
5	システムの問合わせに関する窓口が不明瞭だった	医務課職員が運用サポートを行っていたが、規程上の担当者ではなく、システム利用者から見た時の問い合わせ窓口や、実作業責任が曖昧であったので、運用・監視の一元化を図る	専任職員を配置の上、平成３１年４月に情報システム管理室を設置した
6	保守ベンダーへの管理・監督が不十分であった	管理規程を見直し、保守担当ベンダーへの責務やルールを明確にするとともに、契約内容についても見直しを図る	管理規程を見直し、業者委託管理規程を規定した

☆宇陀市及び市立病院の情報システムセキュリティ管理体制を見直し、予防及び初動体制の適正化を図りました。（見直し後）

（※見直した箇所）



担当・会議	責任・業務概要
運用責任者（病院長）	医療情報システムのすべてに係る最終責任者であり、各種判断・承認を行う
システム管理者（副院長）	医療情報システムの円滑な運用を目的としてシステムの導入・変更・保守にかかる管理・決定およびその結果を運用責任者・幹部会へ報告・上申を行う
幹部会	システム管理者からの報告事項・決定事項のうち、病院全体に関わる運用・管理事項について承認を行う
情報システム管理委員会	医療情報システムに関する運用・課題の検討・承認及びセキュリティ対策を行う
情報システム管理室	医療情報システムに関する日常運用の報告・作業事項についての確認・判断・承認を行うに応じて運用責任者・システム管理者への報告・上申を行う。 システムに関する日常点検・病院内からの問い合わせ・要望・課題の一次窓口・対応を実施するシステム保守ベンダーへの作業依頼・回答・報告の一次窓口・対応を実施する
システム利用者	医療情報システムを利用する全職員（非正規雇用職員を含む）
監査責任者	医療情報システムの運用・整備状況に関する監査を担当する

◆情報システム管理委員会の設置

平成３１年４月に「情報システム管理委員会」を設置し、院内の管理体制を見直しました。

【情報システム管理委員会】

（設置）宇陀市立病院が取り扱う医療情報資産を適切に管理し、医療情報システムの安全対策を総合的に推進するため、情報システム管理委員会を置く。

（所掌事項）委員会は、次に掲げる事項について協議し、又は決定する

⑴医療情報システム運用管理についての基本方針に関すること

⑵医療情報システムの安全確保及び事故等への対応に関すること

⑶その他医療情報システムに関する重要事項に関すること

（開催）毎月１回

（委員長）副院長

（委員構成）医療部から５名、医療技術部から６名、看護部から５名、事務部から８名により構成する

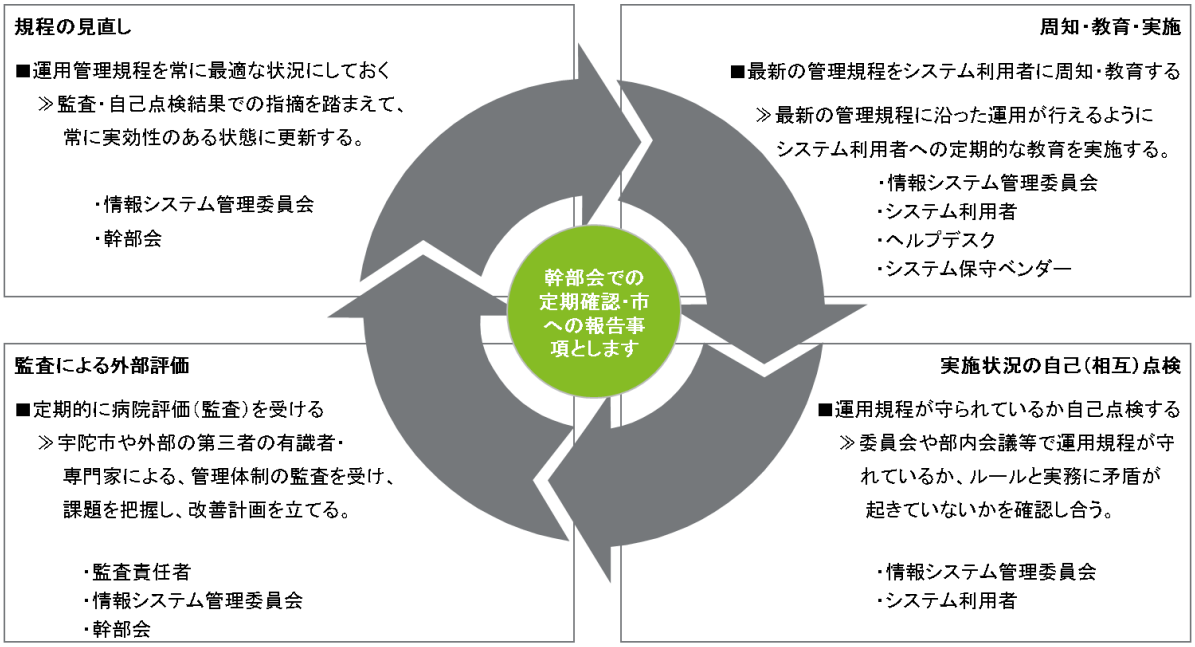
☆これまでの取り組み

平成３１年４月から５回開催し、次の内容を議論しています。

開催日	議論内容
4 月 12 日	・情報システム管理委員会規程について ・市立病院コンピューターウイルス感染事案対策の体制について ・情報システム管理室の設置について
5 月 10 日	・各種規程について（サーバー室入退出管理等）
6 月 14 日	・市立病院コンピューターウイルス感染事案の進捗状況について ・情報システム障害時対応マニュアルについて ・情報システム運用管理規程細則について
7 月 12 日	・医療情報システム運用管理規程（見直し）について ・電子カルテシステム利用宣誓書（案）について
8 月 9 日	・市立病院コンピューターウイルス感染事案の進捗状況について ・有識者会議「提言書（概要）」について ・運用管理規程の研修会について

◆運用管理体制の教育・自己点検サイクル

医療情報システムのセキュリティレベルを向上させるために、規程の見直し、周知・教育・実施、実施状況の自己（相互）点検、監査による外部評価の４つを継続的に情報システム管理委員会で協議し、改善を図ります。



運用管理体制の強化

【運用管理規程の見直し】

監査・自己点検結果での課題を踏まえて、今後のコンピューターウイルス攻撃に適切に対応できる体制の根拠となる管理規程に見直します。

【運用管理規程の周知・教育】

最新の運用管理規程に沿った運用が行えるように、各部署に規程及び緊急時対応マニュアルを設置し周知を行う。また、定期的な研修・訓練を行い、システム運用に責任のある者及びシステム利用者のセキュリティに対する資質向上を図ります。

【実施状況の自己点検】

運用管理規程の遵守状況の自己点検を行います。

【監査による外部評価】

定期的に病院評価（監査）を受けることで、課題を把握し、改善計画を立て、運用管理規程に反映させます。

②緊急時における対応の見直し

◆情報システム障害時対応マニュアル

医療情報システムの障害発生時の初期対応及び適切な対処手順である「情報システム障害時対応マニュアル」を策定しました。

【情報システム障害時対応マニュアル】

・緊急時連絡体制の見直し
・不具合の第一報から具体的な対応指示が出るまで時間がかかったことから、具体的な対応指示を出せるよう整理
・システムログの保全
・通報体制の明確化
・紙カルテ運用手順の整理
・証拠保全と運用状況の記録

◆インシデント[9]対応の見直しと定期的な訓練、教育の実施

・「情報システム障害時対応マニュアル」により緊急時連絡体制、トラブル発生時の診療体制の確保を図ります。
・定期的に研修及び訓練を実施します。
（詳細は職員研修・訓練に記載）

9 コンピューターシステムのセキュリティに脅威を及ぼし、又はその可能性のある事象。

③職員研修・訓練

病院職員の危機意識の醸成が重要で、医療情報システムの利用者全員が、常に危険にさらされているシステムを常時利用していることを十分に意識付けることが重要であり、障害発生時には即時に報告・対応できるように、セキュリティに対する正しい知識と経験を身につけます。

また、研修・訓練を通してシステム運用の管理監督の立場にある責任者の危機管理能力の向上を図ります。

◆職員研修

宇陀市立病院情報システム運用管理規程に基づき利用者に対し、定期的に情報システムの取り扱い、及びプライバシー保護に関する研修を行います。

・開催計画：５月と１２月の年２回実施予定

・令和元年度の実績

No	開催日時	研修内容
１	令和元年７月２３日	「医療情報の安全な利用」についての研修会を実施
２	令和元年８月２６日～２９日	「見直した運用管理規程」についての研修会を実施

・研修対象者：２７０人（病院全職員対象）

◆職員訓練

宇陀市立病院情報システム運用管理規程に基づき、利用者の研修に対する理解度、及び組織としての体制に不備が無いことの確認を目的として、システム障害やセキュリティインシデント等を想定した職員訓練を実施します。

・実施計画：年１回実施予定（１１月）

◆自己点検

研修・訓練を通じてセキュリティの周知が図れているかを情報システム管理委員会で自己点検します。

◆その他

国等が実施するセキュリティ訓練へ積極的に参加し、情報セキュリティ対策の継続的な改善を図る取り組みを行っていきます。

④運用管理規程と運用管理体制の見直し

新規程は「医療情報システムの安全管理に関するガイドライン第５版（厚生労働省)」を参考に、当院のシステムに該当する項目を整理して全面的に見直したものとしました。

☆見直した主な内容

- ・管理体制
- ・業務委託（システムの運用、保守、改造）の安全管理措置
- ・自然災害やサイバー攻撃等による非常時の対策
- ・教育と訓練
- ・電子保存のための運用管理事項

	問題点	課題（取るべき方策）	対応策
セキュリティ体制の見直し	システム管理者としての管理機能及び教育・訓練が不十分であった	システム管理者の管理機能の徹底	運用管理規程に基づき研修・訓練を通じ、管理機能の向上を図る
	医療情報システムに関する委員会が機能していなかった	委員会の規程・運用見直し	情報システム管理委員会を設置した
	規程が遵守されていなかった	遵守状況の確認、外部監査の実施	年１回の内部監査及び定期的に外部監査を実施する
	各種規程書、指示書、取扱説明書等が不足、不十分であった	各種規程書、指示書、取扱説明書の見直し	整備を行った
	最新リスクの把握がされていなかった	最新リスクの把握・対策	情報システム管理委員会にて情報共有及び周知を図る
	ヒューマンエラー（規程違反）が起こっていた可能性があった	ヒューマンエラーの防止の方策・ルール作り	運用管理規程の周知徹底及びセキュリティ研修を計画的に実施する
教育・訓練	利用者に運用規程の周知･徹底がなされていなかった	教育、訓練の充実	年２回のセキュリティ研修及び年１回の訓練を計画的に実施する
	利用者の教育･訓練が不十分であった	教育、訓練の充実	年２回のセキュリティ研修及び年１回の訓練を計画的に実施する
	運用管理規程が一目に分かりにくい	教育、訓練の充実	障害時対応マニュアルを整備した

システム的対応	外部からの侵入を防ぐことができなかった	システム上の対策の強化	システム的対策を図る
	委託業者にまかせっきりであった	委託業者管理の徹底	委託業者管理規程の整備を行った
	情報データの管理が徹底できていなかった	情報データの管理の強化	システム運用手順の整備を行った
緊急時対応	不具合の第一報から具体的な対応指示が出るまでに時間がかかった	初動の規程見直し	障害時対応マニュアルを整備し、初動体制の強化を図る
	各種のシステムログの保全が不十分なため、一部のログが消失した	初動の規程見直し、委託業者管理の徹底	運用管理規程によりシステムログ保全の徹底を図る
	国や県といった外部機関との連携が不十分なため、対策が遅れた	初動の規程見直し	障害時対応マニュアルを整備し、初動体制の強化を図る
体制	異常を感じた時の相談窓口の対応が不十分であった	通報体制の見直し	障害時対応マニュアルにより通報体制を見直した
システム	外部からの侵入がシステム障害までに発展した	水際対策、侵入対策、警告システムの構築	システム的対策を図る
緊急時における対応	今後、紙運用になれない職員が増えていく	トラブル発生時の診療体制の準備・訓練	障害時対応マニュアルを整備した訓練を計画的に実施する
	情報のバックアップがされていなかった	情報のバックアップの確認	運用管理規程細則の整備を行った
	調査着手前段階で感染端末が初期化されたため、感染源が特定できなかった	証拠保全と運用状況の記録	障害時対応マニュアルを整備したログの保存を行う

◆運用管理体制の見直し

情報セキュリティに対するガバナンスや対応、訓練、教育の根拠とすべき運用管理規程の見直しを行い、最新の運用管理規程により職員への周知・教育を行っていきます。

また、今回の事案については、運用管理規程の周知や遵守が病院職員に徹底されていなかった状況から、宇陀市・宇陀市立病院の管理体制に問題があったため、運用管理規程の見直しとともに管理体制を強化します。

⑤セキュリティ監査の見直し

宇陀市立病院情報システム内部監査規程に基づき、医療情報の安全管理が適切に運用されていることを確認するため、情報システムに関する監査を行います。
監査責任者から監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じます。

【内部監査】

監査責任者：情報セキュリティに関する知識及び経験を有する者
監査時期：毎年９月（本年度は令和２年３月に実施予定）
監査内容：以下の項目を含む監査計画書により実施

- 監査目的
- 監査テーマ
- 監査対象
- 監査体制
- 監査スケジュール
- 監査チェックシート

主な監査事項：緊急連絡体制・情報資産の管理・外部記録媒体・サーバ等の管理・情報資産の持ち出し・外部委託・ログの記録・利用者 ID の管理

【外部監査】

第三者的立場から内部監査が適正に行われているか外部監査を行います。
監査時期：令和２年に予定（以降５年に１回を計画）
外部監査者：外部監査機関に委託
監査内容：内部監査事項

提言２の対応

（２）医療情報システムのみならず、院内情報システム全体への技術的対策の強化

①短期的な対策

セキュリティ対策ベンダーによる調査結果では、理論上、外部のネットワークにつながっていないにもかかわらず、外部からの攻撃をうけた可能性が高いことが明らかになりました。感染経路については、調査をしても判明しなかったため、以下の３つの感染経路を想定しシステム的対策を講じました。

経路１：病院情報システム（ＨＩＳ）系からのインターネットアクセス

対策：私物の Wi-Fi ルータ等からのインターネット接続制限

利用者が業務のみに HIS 系端末を利用している限りにおいてはインターネットにアクセス出来ない構成となっていた一方で、私物の携帯電話でテザリング接続を行った場合と、ポータブル Wi-Fi を持ち込んだ場合においては、インターネット接続が可能な状態であったため、私物の Wi-Fi ルータ等からのインターネット接続制限を講じました。

経路２：私物パソコンからの病院情報システム（ＨＩＳ）への感染

対策：私物パソコンの病院ネットワークへの接続制限

現状 HIS 系ネットワークは固定 IP 設定が必要となる為､私物パソコンを接続するには有効な固定 IP アドレス及びゲートウェイ[10]情報等の入力が必要であり、一定の技術が必要なことから、容易に接続はできない状態です。

Wi-Fi の MAC アドレス[11]接続制御を行いましたので、無線 LAN 接続はできません。

有線接続の場合にも、ＭＡＣアドレスで接続制限できることが望ましいとの提言を受けましたが、接続制限による医療機器への影響が想定できないため、代替えの対策として IDS[12]の監視を強化し、IPS[13]による自動遮断を導入します。

ＭＡＣアドレス認証については、将来的にシステムの更新時期にネットワークの再構築を検討して取り組みます。

---

[10] ネットワークとネットワークを接続するためのハードウェアやソフトウエアのこと

[11]各ネットワークカードが持つ固有のＭＡＣアドレス（ネットワークカードや無線ＬＡＮアダプターなどに重複しない固有のＩＤとして割り振られる物理的アドレス）をアクセス制御に利用する認証方法

[12] IDS：不正な通信の侵入を検知し、管理者へ通知するシステム

[13] IPS：不正な通信の侵入をブロックするシステム

経路３：リモートデスクトップ[14]接続の制限

対策：クライアントからサーバやクライアントからクライアント等へのリモートデスクトップを制限する必要があります。

本件事案ではリモートデスクトップ接続が攻撃に悪用された為、端末が踏み台になった場合にリモートデスクトップ接続が行えないことと、受信側でリモートデスクトップ接続を制限する対策を講じました。

②中長期的な対策

今回の調査の過程で、本件事案の原因とはいえないものの、間接的にあるいは潜在的にリスクとなりうる設定値や状況が確認されたため、次の事項についても今後のウイルス攻撃への中長期的対策として、順次、計画的に実施していきます。

・サポート終了ＯＳの残存（情報系は対応）
・ウイルス対策製品の一元化（対応済）
・インターネット系にURLや通過ファイルを制御する機器の導入（対応済）
・インターネット系ネットワークの管理（対応中）

提言３の対応

（３）市民に向け、本件事案及び対策についての報告書の作成、公表

本報告書は有識者会議の提言書を踏まえ、市民・患者に本件事案の調査結果、被害状況の実態及び再発防止策の対策状況、今後の対策方針を示すものです。

ウイルスがどのようにして端末に侵入したかの侵入経路は機器を初期化したことによりログが残っていないため不明で、個人情報の流出があったか否かの断定が行えない状況であり、患者様・市民の皆様をはじめ多くの病院関係者に不安を抱かせました。

令和２年２月現在、個人情報が流出したという情報はありませんが、今後も引き続き動向に注意していきます。

なお、現在被害として判明していることは、患者カルテ情報の一部が暗号化されたことによる、本件事案発生月の診療報酬請求にまで影響を及ぼし、福祉医療費助成制度等に基づく償還に遅れが生じたことです。

本件事案については、“初期対応が不適切であり、証拠保全の観点の欠落という、宇陀市立病院としての情報セキュリティに対するガバナンスが機能していなかっ

14 あるコンピューターのデスクトップ画面を、ネットワークを通じて他のコンピューターに転送して遠隔から操作すること。また、特にWindowsに搭載されているような機能（リモートデスクトップ接続）のこと

た“という有識者会議の提言を重く受け止め、今後のコンピューターウイルス攻撃に備えるため、各種の改善策及び継続的な対応計画を策定し、再発防止策を講じました。

６．まとめ　～宇陀市の決意～

このたびの事案について、セキュリティ対策ベンダーの調査を基に、有識者会議で審議いただいた結果、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等の誰かが、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が事案発生の原因として指摘されています。

何らかのルール違反については、本来はインターネットにアクセスできないシステム構成になっていましたが、私物の携帯電話やポータブルの Wi - Fi を利用した場合には、ネットワーク上の端末から外部との通信が可能な状態にあったことが確認されています。

また、事案発生後の対応について、早期復旧を最優先し、システム管理端末を初期化したことで、原因究明に至らないこととなりました。

システムの安全性を守ることは、機微な情報を多く含む患者の個人情報を守ることに他ならないことを、システムを利用する職員は勿論、委託業務従事者を含め、“してはいけない事、すべき事”を共通認識し実践を徹底していくことが、システムの安全性確保、個人情報保護のために必要なことですが、このルールが「組織の認識」として未成熟であり、遵守の管理も充分でなかったと問題提起されています。

一方、電子カルテシステムベンダーや各部門ベンダーに対し、システム構築、改修や保守作業時における情報流出防止等の安全対策の徹底が必要であり、業者としての、“してはいけない事、すべき事”が遵守されていたのか。ルール違反が起こらないよう管理する病院側の体制が充分ではありませんでした。

セキュリティ対策ベンダーの調査結果を踏まえ、有識者会議からの再発防止に向けた提言を真摯に受け止め、次の対策を講じることとしました。

先ず、宇陀市・宇陀市立病院としての情報セキュリティに対するガバナンスを機能させること、及びセキュリティ管理体制を強化・充実させることについてです。

医療情報システム運用管理規程を見直し、適切な初動対応のための情報システム障害時対応マニュアルの策定など、必要な手順書等の整備を行いました。ただし、規程の整備は、システムの安全運用のためのルールを決めたに過ぎず、これを「病院組織の認識」として全職員及び病院事業に関わる委託業務従事者等に周知し遵守を徹底していく取り組みを継続してまいります。

情報システム管理体制については、院内情報システム全般に関する管理一元化部署として事務局内に情報システム管理室を設置しました。

また、システム管理者（副院長）を委員長とした、情報システム管理委員会を設置し、院内の情報システムの管理及び情報セキュリティの管理に関し審議を行います。本委員会では、運用管理規程に沿った運用が行えるようにシステム利用者への定期的な教育を実施し、規程が守られているかの自己点検を行います。そして、定期的な監査実施による病院評価を受け、課題・指摘事項を踏まえ、より実効性のある運用管理規程に見直す自己点検サイクルを実行します。

次に、システムセキュリティに対する技術的対策についてです。
今後、宇陀市立病院において今回と同様の事案が発生しない技術的な対策はできていると判断していますが、新たなコンピューターウイルス等、情報リスクが生まれる中、未知の攻撃に対しても安全と言い切れるものではありません。従って、システムの安全性を過信することなく、同様の攻撃を受けた場合の対応方法を確立することで、安全なシステム運用を行ってまいります。

個人情報の流出につきましては、侵入経路と考えられる管理端末が初期化され操作ログ等が取れないため、個人情報の漏洩については、明確にすることができない状況です。

ただし、現在までのところ、個人情報の漏えいによる被害の報告はない事が確認できていますが、患者の皆様の不安を払拭しえない事を残念で申し訳なく思っています。

病院への信頼は、患者様の個人情報がしっかりと守られていることが大前提にあり、そのためには、医療情報システムの安全性が充分に担保され、万一障害が発生した場合でも、大事に至らず対処できる体制がとれていることが求められています。

本件事案発生の最大の要因は、病院における情報システムの安全運用に対するガバナンスが欠如していた結果、病院職員が情報システムリスクについて、正しく理解することができず、日常業務の中で運用管理規程上認められていない行為を行うことがどのような結果を招くのか正しく認識できていなかったと思慮いたします。

システム運用管理に責任を持つ立場の者は、システムの運用管理規程がどのようなリスクに対応するために設けられたものであるのかを職員に理解させることが求められます。このような取り組みを通じて、システム運用管理規程が遵守される職場環境が実現でき、ガバナンスが確保された状態が維持できると考えます。

有識者会議からのご提言を受け、再発を防止するためには、受託事業者任せにすることなく、病院が情報システムの運用に主体性をもって取り組み、管理者及び職員の資質向上に努め、セキュリティリスクに正しく対応できる組織へと生まれ変わることが何よりも重要であると重く受け止めています。

そのために、システム管理運用規程を見直し、継続的な訓練、教育により、実効性を担保する対策を取り、実施状況についての監査体制の強化を図ってまいります。

さらに、今回の教訓を生かし、市立病院にとどまらず、宇陀市全体として、情報セキュリティに関する管理体制の強化を図り、職員の意識及び組織の内部統制の改革を進めてまいります。

最後に、本件事案の課題整理や再発防止について慎重審議を賜りました有識者会議の委員各位に深く感謝を申し上げますと共に、適切な道筋をご助言ご指導頂きました厚生労働省、奈良県の関係者の皆様に心より御礼申し上げ、報告書の締めくくりとさせていただきます。