市立奈良病院におけるシステム障害に係る報告書【概要版】

～検証結果と今後の対応～

01 原因特定

02 対応の適切性

03 再発防止の適切性

04 今後への提言

05　奈良市の今後の対応

令和8年8月31日　奈良市

はじめに　～今回の事案と専門家会議の検証について～

令和8年4月21日、市立奈良病院において情報システム障害が発生し、電子カルテをはじめとする医療情報システムの一部が使用できない状況となりました。これにより、診療や検査等に影響が生じ、病院をご利用の患者様・ご家族の皆様をはじめ、関係者の皆様に多大なご不便とご心配をお掛けしましたことを、改めてお詫び申し上げます。

発生当初はサイバー攻撃の可能性も否定できない状況であったことから、病院では安全確保を優先し、電子カルテの停止や救急受入れの一時停止などの対応を行いました。その後、厚生労働省から派遣された専門チームの支援を受けながら、病院において原因調査やシステムの安全性の確認が行われ、順次、診療機能の復旧が進められました。

本市では、本事案について、原因を明らかにするだけでなく、発生後の対応や病院が講じた再発防止策を客観的かつ専門的な立場から検証することが重要であると考え、外部有識者による専門家会議を設置しました。専門家会議では、「原因特定」「対応の適切性」「再発防止の適切性」「今後への提言」の4つの観点から検証いただきました。

その結果、本事案は、外部からのサイバー攻撃ではなく、セキュリティ監視装置※1の監視対象又は学習対象の変動により過検知が生じ、これに自動遮断が連動したことによるシステム障害であったとの見解が示されました。また、実際のサイバー攻撃への備えも含め、病院情報システム全体の安全性について意見・助言をいただき、今回確認された課題の一部は、市立奈良病院だけでなく、同様のシステムを利用する他の医療機関にも関係する可能性があることも指摘されました。

本書は、これらの検証結果を踏まえ、本事案の経過、原因、対応の評価、再発防止策及び今後の取組を取りまとめたものです。

なお、本書は、本事案の原因究明、発生後の対応の検証及び再発防止に資することを目的とするものであり、関係者の責任の有無又は所在について判断を示すものではありません。本市としては、今回の検証を一過性のものとせず、再発防止策や専門家からの提言が実際の改善につながっているかを継続的に確認し、より安全で安定した医療提供体制の確保に取り組んでまいります。

事案の発生　｜何が起きたのか

4月21日夜、セキュリティ監視装置が院内通信を異常と判定。その後、複数のシステムで警報が相次ぎ、電子カルテを含む病院情報システムに影響が広がりました。

4/21　22:15

初回異常検知

セキュリティ監視装置が、リモート保守用中継端末からの通信を異常と判定し、その通信を自動遮断※2

23:04～23:46

警報拡大・隔離

眼科システムでも異常通信を検知し、自動遮断。病院は、被害拡大を防ぐため物理的な隔離※3に着手

4/22　1:00

警報継続

生体検査システムでも異常通信を検知し、自動遮断。警報が複数の院内システムで相次いで発生

3:09～3:21

警報が連鎖

電子カルテ本番系※4・医事サーバー等にも警報が連鎖し、初回検知から約5時間で警報は計13件に。病院は電子カルテの仮想サーバー群※5をすべてネットワークから物理的に隔離

3:32～6:12

診療制限を決定

病院幹部が、電子カルテの停止と救急受入れの中止を決定。その後、災害対策本部を立ち上げ、外来診療の制限を決定

発生時点では、サイバー攻撃かシステム上の問題かを直ちに判断できず、被害拡大を防ぐためのシステム隔離と、患者の安全を確保するための診療制限を実施

診療への影響と復旧　｜どのような影響があったのか

4月22日から24日にかけて、外来診療・予定手術等を一部制限。その後、安全性を確認できた端末・システムから順次再稼働しました。

診療への影響

外来予約
約1,500件のうち延期
約500件

予定手術
56件のうち延期
18件

救急受入れ
一時停止
約53時間

診療再開に向けた安全確認

4/22　14:00
厚労省支援チーム到着
病院の原因調査・安全確認を支援
総合認証サーバー等の
ログ※6分析調査を開始

①全端末・全サーバー
2種類のウイルス対策
ソフトで完全スキャン

②警報対象サーバー
ログを収集・確認し、
不審な挙動や侵害の
痕跡を調査

③外部接続機器
VPN※7装置等の
ログや設定情報の確認
外部接続部分も点検

患者情報・診療記録の改ざんや漏えい、ウイルス感染、バックドア※8設置等を示す痕跡は確認されず、再稼働へ

復旧の流れ

4/23　20:00
電子カルテ本番系再稼働
安全確認済み端末から
順次復旧

4/24　8:30
通常診療を再開
外来・入院・救急受入れを
再開。残るシステムは安全性
を確認しながら順次復旧

5/1　8:30
侵害を示す所見なし
オンライン資格確認
システム以外の
主要システム復旧

5/13　12:00
オンライン資格確認
システム復旧
すべての主要機能が復旧

専門家会議　｜何を検証したのか

専門家会議では、原因特定だけでなく、発生後の対応の適切性、病院の再発防止策、将来のサイバー攻撃への備えまでを４つの観点から検証していただきました。

01　原因特定

警報発信・通信遮断の事象につき、更新履歴・各種ログ・ヒアリング等から、何が起き、なぜ診療に影響するまでの障害に至ったのかを整理

02　対応の適切性

サイバー攻撃の可能性を否定できない中で実施した、隔離、電子カルテ停止、診療制限、復旧判断等を検証

03　再発防止の適切性

病院が講じたセキュリティ監視装置の運用見直し、接続経路・アカウント点検、次期更改の対策等の再発防止策の妥当性を確認

04　今後への提言

同種事案や実際のサイバー攻撃にも備えるため、市及び病院に対する提言を実施

専門家会議の構成

猪俣 敦夫 氏（座長）
大阪大学D3センター/教授 CISO
専門：情報セキュリティ、危機管理・組織統括

板東 直樹 氏
一般社団法人ソフトウェア協会 フェロー
専門：情報セキュリティ

北條 孝佳 氏
西村あさひ法律事務所・外国法共同事業 パートナー弁護士
専門：危機管理・企業法務

会議・ヒアリングの実施経過

6/2　第1回 専門家会議
事案説明・今後の対応方針

→ 6/30　第1回 ヒアリング
電子カルテシステム事業者

→ 7/2　第2回 ヒアリング
ネットワーク監視装置事業者

→ 7/13　第3回 ヒアリング
市立奈良病院

→ 8/31　第2回 専門家会議
報告書・概要版の確認

なぜシステム障害が起きたのか

専門家会議では、病院等による調査結果や関係者へのヒアリング、各種資料をもとに、警報や通信遮断が相次いだ原因と、その発生過程を検証しました。

何らかの要因でセキュリティ監視装置の監視状態が変化

セキュリティ監視装置の監視対象であった一部の院内通信について、過去一定期間、監視不能または通信量が低下した状態にあった可能性

セキュリティ監視装置の自動更新・再起動

（4月21日夜）セキュリティ監視装置のソフトウェアが自動更新(注①)・再起動。これを契機に、それまで十分に監視されていなかった通信が再び監視対象となった可能性

セキュリティ監視装置の監視対象が約3倍に増加

633台

⇒1,954台

学習したパターンから逸脱した通信と判定し自動遮断

従前十分に学習されていなかった院内通信が一斉に監視対象となった結果、監視装置が平常時パターンの逸脱と判定(注②)し、自動遮断が複数のシステムに拡大

｜｜｜専門家会議の検証結果｜｜｜

外部からのサイバー攻撃によるものではなく、セキュリティ監視装置の監視対象又は学習対象の変動により、従前十分に学習されていなかった院内通信が平常時パターンからの逸脱と判定され、自動遮断が連鎖したことによる障害と整理

【過去に監視状態が変化していた原因】

原因特定に必要な過去の詳細な記録（ログ）の保存期間に限りがあり、十分に確認できなかったため、一部の通信を監視できない状態になっていた原因は特定できませんでした。

（注①）：セキュリティ監視装置ソフトウェアの更新設定は、更新による影響を考慮し、導入後しばらくしてから自動から手動更新に変更していたが、令和８年４月７日にベンダーの推奨である自動更新に変更（※手動運用中、更新の必要性を認識する事象がなかったため更新の実施なし）

（注②）：セキュリティ監視装置の仕組み…ネットワーク上の通信を継続的に観測して平常時の通信パターンを学習。学習した通信パターンから大きく外れた通信に対して「異常な通信」と判定

事案への対応を専門家会議が検証

専門家会議では、事案発生後に病院や市が行った一連の対応について、当時把握できた情報や状況を踏まえ、その判断や対応が適切であったかを検証しました。

専門家会議が評価した３つの観点

01　初動・診療判断

サイバー攻撃の可能性を否定できない中、対象機器の隔離、関係事業者への照会、バックアップの保護、電子カルテの停止、救急受入れの中止等を実施しました

当時の状況を踏まえ、安全確保を優先した判断には相応の合理性があったと評価

02　病院IT担当者・体制

病院のIT担当者は、アラートの確認、関係事業者への照会、バックアップの保護、原因の切り分け、段階的な復旧等に対応しました

こうした対応を院内で一定程度自律的に行える担当者・体制が、本件対応を支えた重要な要素と評価

03　市による早期の情報発信

事案発生後、市長がSNS等を通じて早期に情報を発信しました

初動対応時に公開できる情報は限られてはいるものの、積極的に情報発信されたことは、過去の事案からの教訓が活かされており、患者や市民への迅速な情報提供につながったと評価

｜｜｜専門家による評価｜｜｜

事案発生当時の情報を前提とした「安全最優先の診療制限」や「病院担当者の自律的対応」、「市の迅速な情報発信」という、それぞれの局面における適切な対応を評価

病院の再発防止策を専門家会議が検証

病院は本件を受けて再発防止策を進めています。専門家会議はその方向性を妥当と評価したうえで、実際の運用で確実に機能するよう、判断基準や手順のさらなる具体化を求めるとともに、再発防止策は病院内の取組にとどまらず、関係者間の連携を含めて設計する必要があるとしています。

病院が講じている主な再発防止策

セキュリティ監視装置の運用見直し

自動更新を停止し、手動更新へ変更。更新後の通信状況を一定期間確認

外部接続経路の点検

外部から接続できる経路を精査し、不要なVPN等を閉鎖

アカウント管理の強化

保守用アカウントを棚卸し、不要なアカウントを整理

今後のシステム更改へ反映

管理者権限、保守接続、端末防御等の強化を今後のシステム更改に反映

専門家による評価と今後の課題

再発防止対策の方向性は妥当であると評価。さらに判断基準や手順等を具体化することが必要

さらに具体化すべき主な事項（※監視装置の運用に関する対策）

監視状態・アラート

監視不能状態や監視対象数の異常な増減を早期に把握し、反復するアラートは事業者への照会につなげる

更新時の確認

更新前後の監視状態・通信状況を確認・記録し、異常時の確認・承認・切戻し手順を定める

自動遮断・復旧

自動遮断は維持しつつ、監視状態や更新直後などの状況に応じた適用条件を明確化。あわせて自動遮断のみに依拠しない対策を組み合わせる

重大事案時の初動・復旧

警報発生時の確認事項をあらかじめ定め、対応手順を明確化。遮断解除の判断基準や電子カルテ等の段階的な復旧手順も具体化

初動・ログ

重大事象時に必要なログ・設定変更履歴を速やかに保全し、平時の保存範囲・期間も整理

あわせて、市・病院・関係事業者について、重大事案時の報告、役割・判断権限、連絡方法、フォローアップの方法等をあらかじめ整理することも提言されています。

本事案から得られた主な教訓 ― 他の医療機関にも参考となる5つのポイント ―

本事案には、市立奈良病院だけでなく、セキュリティ製品を利用する他の医療機関にも共通する論点があります。
専門家の意見を踏まえ、平時から確認・見直しておくことが望まれる主なポイントを整理しました。

他の医療機関にも参考になる主なポイント

自動遮断の運用を決めておく

被害拡大を防ぐ有効性と、過検知による診療への影響の双方を踏まえ、適用条件・確認手順・復旧手順を事前に整理する

監視が正常に機能しているか確認する

セキュリティ製品を導入して終わりとせず、監視状態に異常がないか継続的に確認し、必要に応じて事業者へ照会する

アップデートのルールを決める

自動・手動更新の使い分けや適用条件、更新前後の確認事項、異常時の対応・切戻し手順を整理する

必要なログを残す

重大事象が起きた際に原因を検証できるよう、必要なログや証跡の範囲・保存期間をあらかじめ整理する

診療の制限や緊急遮断を「誰が判断するか」を明確にする

重大事案に備え、診療制限やシステムの緊急遮断を伴う意思決定ルール、報告先・連絡体制、関係事業者との役割分担を平時から整理する

｜｜｜専門家からの提言｜｜｜

自動遮断機能は、サイバー攻撃による被害拡大を防ぐために有効な場合がある一方、診療への影響も考慮した運用が必要。監視状態、更新管理、ログの保全、連絡・判断体制などについて、重大事案が起きてから対応するのではなく、平時から継続的に確認・見直しておくことが重要

病院情報システム全体のセキュリティ強化に向けて

今回の障害の直接原因とは別に、実際のサイバー攻撃に備える観点から、セキュリティ監視装置は基本的な対策を整えた上で活用すべきものであるとして、今後さらに改善・強化すべき事項について、専門家から意見が示されました。

専門家会議から改善・強化の必要性が示された主な事項

認証・権限管理の強化

管理者権限を必要な人に限定し、利用者・管理者を個別に識別できる管理へ

外部保守接続の安全性向上

病院外からの接続について、本人確認、接続経路、接続記録等をより適切に管理

侵入されても被害を広げにくい構成へ

一部の端末等に侵入された場合でも、他の端末・サーバーへ容易に広がらないよう、ネットワーク分離や通信制御を強化

旧来の技術・設定の見直しと記録の確保

セキュリティ上のリスクとなり得る旧来の機能・設定等を見直すとともに、事後検証に必要なログを確保

｜｜｜専門家会議からの指摘｜｜｜

今回の障害の再発防止だけではなく、実際のサイバー攻撃にも備え、万一侵入された場合でも被害を広げにくい「多層防御」の考え方が重要であり、認証・権限管理、外部からの接続、ネットワーク構成など、複数の対策を土台にセキュリティ監視装置による検知・遮断を組み合わせ、病院情報システム全体の安全性を高めていくことが必要

安全で安定した医療の確保に向けて

再発防止策等の実施状況を継続的に確認

専門家からの提言を踏まえ、今回の障害への直接対策に加え、病院システム全体のセキュリティ向上に向けた取組について、病院に具体的な実施計画の提出を求めた上で、その進捗・完了状況を市が定期的に確認します。
確認にあたっては、単なる書面上の自己申告にとどまらず、変更管理票や確認記録等の客観的な実施の証跡（証拠）の提出を求め、実効的な確認を行います。

1.実施計画の提出要請 ▶ **2. 対策実施の証跡確認** ▶ **3. 継続確認**

重大事案の報告体制の確立

今回の事案では、市長をトップとする市・病院間のオンライン会議を複数回開催し、情報共有を行いました。
今後は、報告の対象等を整理し、必要な情報を速やかに把握できる体制を整えます。
特に、病院の診療機能の制限や一時停止が生じるような重大事態においては、時間帯を問わず市へ即座に報告するルールを運用マニュアル等により位置付けます。

今回の検証を一過性のものとせず、病院の再発防止策や専門家からの提言が、実際の改善につながっているかを継続的に確認します。また、市と病院がそれぞれの役割を果たしながら、より安全で安定した医療提供体制の確保に取り組むとともに、今回得られた教訓について、市内医療機関への情報提供等に生かしてまいります。

さらに、医療機関等の努力だけでは解決が困難な構造的課題については、国に対して実効性のある制度改善や支援を強く求めていくこととし、具体的には、稼働中システムを安全に維持するための「システムベンダー側へのセキュリティ更新義務化」、設定変更や動作確認に伴う「検証費用への財政支援」などについて国へ要望してまいります。

【参考】

用語解説

※１「セキュリティ監視装置」：院内ネットワークの通信を監視し、異常を検知する装置

※２「自動遮断」：セキュリティ監視装置が異常と判定した通信を自動的に止める機能
病院では、自動遮断機能を有効にして運用していました

※３「物理的な隔離」：ネットワーク配線を抜くなどして物理的に切り離すこと

※４「電子カルテ本番系」：実際の診療で通常使用する電子カルテシステム。診療記録の参照や入力・更新など、通常の電子カルテ業務に使用

※５「仮想サーバー群」：電子カルテを構成する複数のサーバー群。今回の事案では、被害拡大を防ぐため、これらをネットワークから物理的に切り離しました

※６「ログ」：システムへのアクセス、通信、操作などの記録

※７「 VPN 」：院外から院内システムへ接続する際などに用いる安全な通信経路をつくる仕組み

※８「バックドア」：攻撃者が後から不正に侵入するために設ける通常とは別の侵入口

病院の医療を支える情報システムについて

現在の病院は、電子カルテや検査システムなど、多くの異なるメーカーの機器がネットワークで繋がり、お互いにデータをやり取りして日々の診療を支えています。国が進める医療のデジタル化（医療DX）に伴い外部との接続も急激に増えており、ネットワークは今や医療の重要なライフラインとなっています。

一方、病院システムは多くのメーカーの機器が複雑に絡み合っているため、安全性を保つための日々の更新（アップデート）であっても、他のシステムが誤作動を起こさないかどうかの安全テストや調整をその都度行う必要があります。

これには莫大な費用と時間がかかる上、勝手にシステムを触るとメーカーの動作保証が受けられなくなるリスクもあります。個別病院の限られた予算や人手だけで、システムを常に最新の安全な状態に保ち続けることは、全国のどの病院にとっても極めて困難なのが実態です。

こうした中でも、医療機関には診療を継続しながら安全性を確保していくことが求められます。

今後は個々の取組に加え、国による技術面・財政面からの実効性ある支援が期待されます。