大阪急性期・総合医療センター　情報セキュリティインシデント調査報告書　概要　2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生した情報セキュリティインシデントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

◆調査結果から推定される攻撃者の手順　（調査報告書11～12頁）

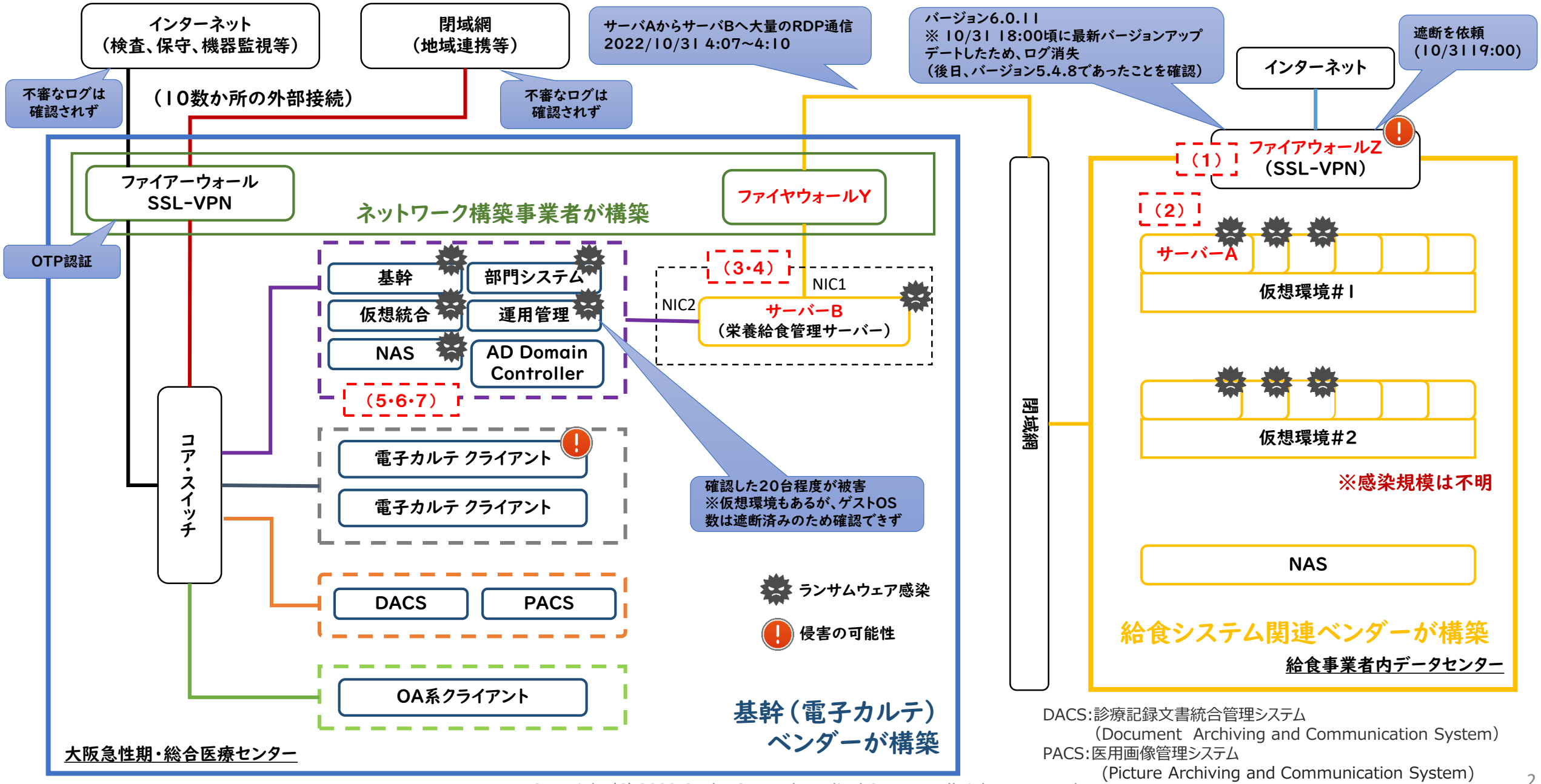
No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入（漏洩され公開されていたID・パスワード情報を用いて侵入された可能性もある）。
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため給食事業者内での攻撃拡大。
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5	他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示

◆被害状況　（調査報告書11頁、21頁、28頁、40～41頁）

No	項目	被害内容
1	電子カルテを含む総合情報システム	基幹システムサーバーの大部分がランサムウェアにより暗号化。PC端末（院内に約2,200台）も不正アクセスの痕跡あり。 ⇒全てのサーバ、端末をクリーンインストール 　基幹システムサーバ再稼働に43日間、部門システム含めた全体の診療システム復旧に73日間を要す
2	診療制限	2022年11月の診療実績　（前年同月対比）　※2022年12月は現在計算中 新入院患者数：558人（前年同月比33.3%）、延入院患者数：10,191人（前年同月比52.9%） 初診患者数　：465人（前年同月比17.9%）、延外来患者数：15,744人（前年同月比61.6%）
3	被害額	現在精査中　　調査・復旧費用で数億円以上 診療制限に伴う逸失利益として十数億円以上を見込んでいる

ネットワーク構成図と感染状況　（調査報告書12～13頁）

▶個人情報漏洩の可能性は極めて低い（通信ログ調査・フォレンジック調査から）
▶現在、個人情報漏洩調査を実施中



DACS:診療記録文書統合管理システム
（Document Archiving and Communication System）
PACS:医用画像管理システム
（Picture Archiving and Communication System）

技術的発生要因と再発防止策　（調査報告書18～19頁）

①外部接続（リモートメンテナンス）の管理不備

VPN機器の管理やRDP接続の運用などが適切になされていれば被害を免れた可能性がある。

No	発生原因	発生要因	再発防止策
1	サプライチェーンのVPN機器の脆弱性が放置されていた。	VPN機器やファイアウォールなど外部通信機器の保守や脆弱性管理など役割分担が曖昧だった。	機器毎に管理者と設置者が互いに保守の範囲や脆弱性管理の役割分担等について文書により確認を行う。
2	リモートデスクトップ通信(RDP)接続が常時接続となっていた。	リモート保守を許可するための基準が曖昧で、またリモート保守を行う側のセキュリティ環境の確認が不十分だった。	外部接続やリモート保守を許可する場合の基準を定めるとともに、許可申請を受ける場合には、通信元のセキュリティ環境を確認する運用を構築する。
		外部接続（リモート保守）を許可した後に、その利用状況を確認していなかった。	外部接続やリモート保守を行う場合は、相手よりその目的や時間を確認し、通信ログの確認を行い、他の不正なアクセスなどの記録が残されていないかを確認する運用を構築する。

②内部のセキュリティが脆弱

侵入を許した場合でも初期設定が適切であれば、大規模に横展開されることはなかった可能性がある。

No	横展開を許した初期設定	再発防止策
1	ユーザーすべてに管理者権限を与えていたため、攻撃者に管理者権限を利用され、ウイルス対策ソフトをアンインストールされた。	ユーザーは管理者権限のない標準ユーザーアカウントに設定。ユーザーアクセス制御を適用させ、管理者権限を要する重要な操作が意図せずに自動実行されることを防ぐ。
2	Windowsのパスワードが、サーバー、端末毎にすべて共通であり、一つのパスワードが窃取されると、他のすべてのサーバー（端末）が乗っ取り可能な状態。	Windows のパスワードを、サーバー、端末毎にすべて個別化（ユニーク化）。
3	アカウントロックアウトの設定が無く、パスワード総当たり攻撃や辞書攻撃によりパスワードを数多く試行されログオンが成功した。	アカウントロックアウトの設定を有効化。
4	電子カルテシステムサーバーにウイルス対策ソフト未設定のため、容易に侵入され、ランサムウェアを実行された（他のサーバーや端末にはウイルス対策インストール済み）。	電子カルテシステムサーバーにもウイルス対策ソフトをインストールする。

組織的発生要因と予防に向けた提案 （調査報告書15～17頁）

①ITガバナンスの欠如

No	ITガバナンスにおける主な問題点	予防に向けた提案
1	各契約単位で、保守や脆弱性管理といったセキュリティに関する責任分界点と役割が明確になっていない領域が存在した。	契約毎に、受注者と「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（総務省・経済産業省）」に基づいたサービス仕様適合開示書及びサービス・レベル合意書（SLA）により双方の責任分界点や役割を明確にし、文書化すること。
2	複数のベンダーが関与する契約において、そのプロジェクトマネジメント体制が明確になっていない状況があり、重要なセキュリティに関する事項について、関係者による十分なリスク評価が行われていないケースがあった。	合同企業体（JV）によるプロジェクトの場合（構築だけでなく保守も含む）は、受注側のプロジェクト体制を明確にさせるなど、責任の所在を明確にすること。
3	医療機器やその保守に係るセキュリティ仕様が、総合情報システムにおけるセキュリティ仕様に適合していないケースがあり、運用が共通化されていなかった。	調達が行われる場合には、病院共通のセキュリティポリシーに基づく共通仕様を作成し、共通運用となるような調達を行うこと。
4	医療情報部で調達している情報資産以外の医療機器（リモート保守用機器を含む）や建築関係の情報システムについて、一元管理されていなかった。	診療情報系のネットワークに接続されている機器やシステムはすべて情報資産としてリストアップしたうえで、安全管理上の重要度に応じて分類し、リスク分析を実施すること。
5	総合情報システムの仕様における「医療情報システムの安全管理に関するガイドライン（厚生労働省）」は第4.3版であるが、現時点では第5.2版まで更新されている。第5.2版についてベンダーを交えて組織的に検証されている状況が確認されなかった。	ガイドライン改定時には組織的に適合状況を確認し、不足している項目があれば改善に向けたPDCAサイクルを回す活動を行うこと。
6	2022年4月より診療報酬で位置づけられた医療情報システム安全管理責任者について、その役割等の組織内での認知が不十分のようであった。	医療情報システム安全管理責任者を軸としたITガバナンスを効率的効果的に運用する組織体制を構築すること。

②契約に関する諸問題

契約の段階で、役割分担や責任分界点などが明示されておらず、保守の範囲や機器の管理方法が曖昧であったため、脆弱性の管理が不十分であったり、外部接続の管理が不十分であった。

【契約段階でのリスクを回避するための措置】

1）共通したセキュリティポリシーによる調達

2）契約時のガイドラインに基づく文書確認（責任分界点や役割分担の確認）

3）医療情報部門との情報共有による情報資産管理の徹底

4）複数のベンダーによる保守を含んだ契約の場合のプロジェクトマネジメント体制の確認

5）保守を含んだ契約の場合の保守方法の確認

人的発生要因　（調査報告書17頁）

「医療機関は閉域網だからセキュリティは問題ない」といった誤った閉域網神話の中で、セキュリティに関する意識が薄れていた。

⇒特に、ベンダーはシステムや機器を提供する専門家として、サイバーセキュリティの知識と経験向上に努めるべき。

⇒病院もセキュリティ意識を高く持ち、組織的にシステムや機器の導入および運用を心掛けた取り組みが必要。

調査委員会としての気付き事項と国に期待する事項　（調査報告書20～21頁）

①　地域医療への脅威からの保護

- 今回の事案はどの医療機関でも起こりうる大きなリスク
- 医療分野のネットワーク化が推進される中で、セキュリティ向上は必須課題
- 国においては、ガイドラインや法整備、財源の確保など、その役割はますます重要

②　役割と責任分界点の明確化

- ステークホルダーそれぞれの責任分界点や役割分担が非常に曖昧
- 発注者と受注者の間で「情報の非対称性」が存在する中で、ガイドラインに基づく契約時の文書による役割の明確化が必須
- 国においては、ガイドラインの運用推進および周知徹底により、情報セキュリティに係る各契約の役割や責任分界点の明確化を推進していくことが必要

③　閉域網意識の見直し

- 医療情報を扱うシステムベンダーや医療機器メーカーのセキュリティ意識は、閉域網神話から決して高いものとは言えない
- 医療分野において高度かつ複雑な様相を呈するシステム化やネットワーク化が推進される中で、医療系事業者におけるセキュリティ意識及び見識の向上は早急に必要
- 国においては、セキュリティ対策向上に資するレギュレーションの策定や整備とともに、それらを業界に浸透させていく取り組みが求められる

④　医療継続支援への更なる取り組み

- 情報システムに依存している医療においては、大規模システム障害が起こりうる状況にあるという前提で、起きた時を想定した対策が必要
- 国においては、医療機関へのサイバー攻撃を災害の一つとして捉え、その支援対策を充実させるなど、患者が安全安心に医療を受けられるよう、更なる取り組みの推進が必要

課題解決のための提言　（調査報告書65～66頁）

①　医療継続のための取り組み支援

- 自助（病院の）努力は必要性を理解した上で、国や地方公共団体は医療機関のサイバーセキュリティの継続的な向上のために、また地域医療を安定的に持続するために、以下のような支援や対応を願いたい。
  - ✓ 「財政的」「人的」「物的」、そしてスキルなどの「情報的」視点の支援
  - ✓ 厚生労働省の初動対応支援・調査事業は可能な限り継続
  - ✓ 診療録管理体制加算とは別建ての医療情報システムの管理およびセキュリティ強化やＩＴ人材の確保に係る診療報酬の評価が必要

②　セキュリティ機能の集中・集約化

- すべての医療機関でのセキュリティ責任者の設置を目指し、サイバーセキュリティに詳しい人材を仮想的にも集約し、すべての医療機関にセキュリティ支援が行えるような人材共有の枠組みが必要
- 医療機関におけるSOCを含めたセキュリティの集約を都道府県や国レベルで整備し、セキュリティの共通プラットフォーム化を検討するなど、個別医療機関のセキュリティ負荷を軽減が必要

③　脆弱なシステムや機器を生み出さないための根本的な仕組み

- 国において現状の医療機関でも適用可能な現実的かつ実践的なガイドラインの整備が必要
- 国においてシステムや機器の根本的な設計思想の転換を促す薬事法・薬機法の解釈や改正の議論が必要
- セキュリティにおける共通の考え方や枠組み、またセキュリティ運用を踏まえた現実的かつ具体的な規格が必要

④　インシデント情報等の共有の場

- 医療機関同士がセキュリティインシデントの情報共有などで連携できる枠組みについて、早期立ち上げ、運用開始が必要