

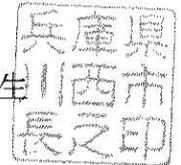
諮 問 第 53 号

平成29年2月1日

川西市個人情報保護審議会

会長 井上典之様

川西市長 大塩民生



電子計算機の結合による個人情報の提供に関する意見について（諮問）

川西市個人情報保護条例第13条第2項の規定に基づき審議会の意見を聴くことについて、下記のとおり諮問します。

記

電子計算機の結合による個人情報の提供について

健康診査におけるCT検査業務に係る電子計算機の結合による個人情報の結合について

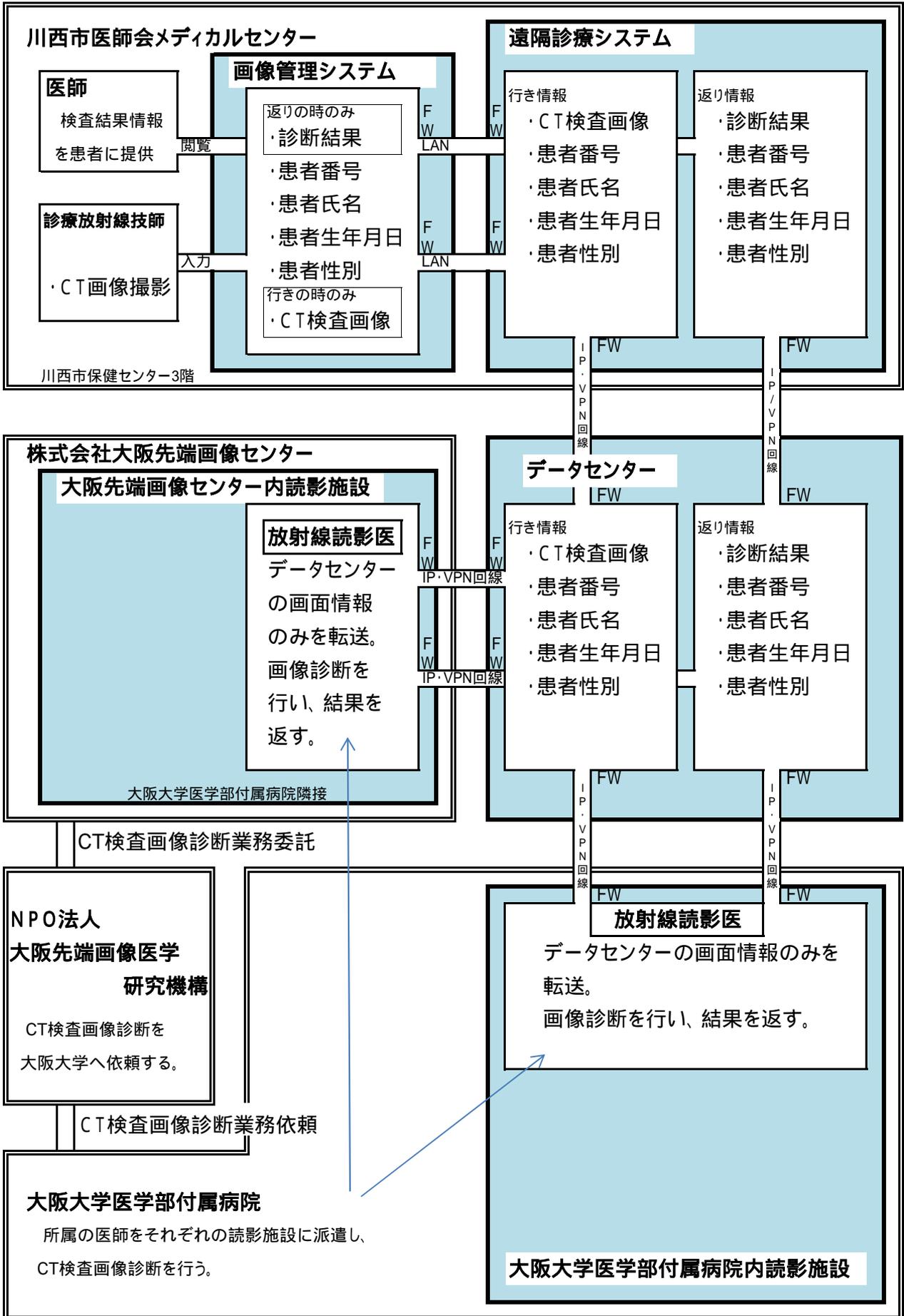
[別紙]

電子計算機の結合による個人情報の提供について

番号	事務の内容	電子計算機の結合による提供の必要性	提供する個人情報の内容	提供先の保護措置	提供先	所管課
14	C T 検査業務	<p>現在、川西市医師会メディカルセンターでは、検査画像について画像管理システムにより一括管理しており、C T 検査画像の読影については大学病院から医師の派遣により実施しているが、昨今の大学医局内の放射線読影医不足から派遣の打ち切りを打診されている状況である。</p> <p>そのため、放射線読影医に川西市医師会メディカルセンターまで来所いただくのではなく、C T 検査画像を大阪先端画像センターに送り、そこで放射線読影医に診断をいただくことにより、C T 検査画像の診断事務を継続して行おうとするものです。</p>	<ul style="list-style-type: none"> ・患者番号 (管理番号) ・氏名 ・生年月日 ・性別 ・川西市医師会 メディカルセン ターで撮影され たC T 検査画像 	<p>提供する情報については、次のセキュリティ措置を講じるものとする。</p> <p>厚生労働省発出の「医療情報システムの安全管理に関するガイドライン」の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に基づき、以下のとおり取り扱う。</p> <ul style="list-style-type: none"> ・川西市と結合先の委託業者との通信については、通信事業者の管理する閉域ネットワークであるIP-VPN網を利用し、接続装置間は暗号化を行う。 ・個人情報を取扱う端末については、IDとパスワードによる個人認証を実施し、取扱者を制限する。 ・個人情報を取扱う端末についてはウイルス対策ソフトを導入し、運用管理を行う。 	(株)大阪先端 画像センタ ー	健康福祉部 健幸政策室

諮問第 5 3 号資料

CT検査業務のシステム概要図



・LAN = Local Area Network

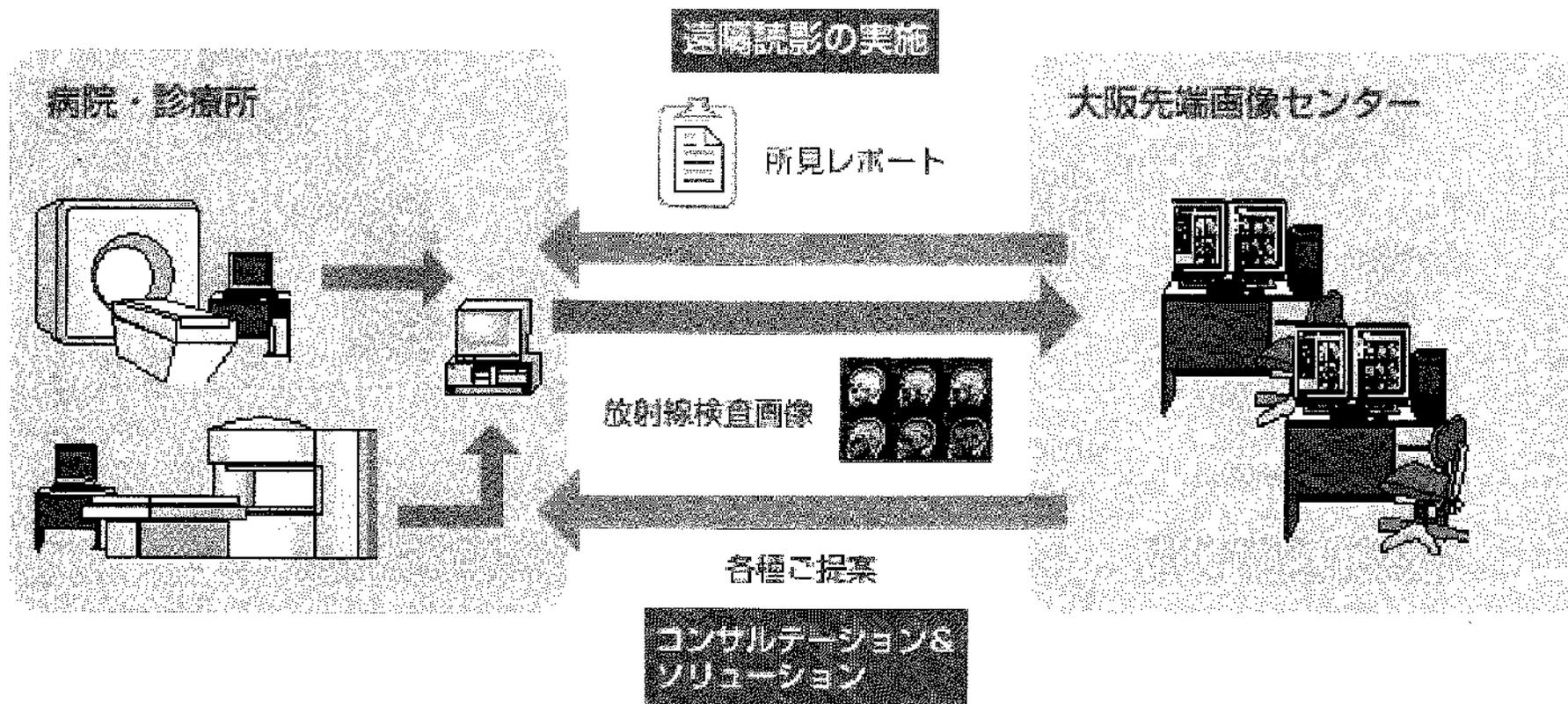
・FW = FireWall

・IP・VPN回線 = 閉域ネットワーク回線



遠隔読影の概要

- 病院や診療所から通信回線を通じて送信された各種放射線検査画像を放射線専門医が読影し、所見レポートを作成して返送する事が遠隔読影の基本です。弊社では、関連するコンサルテーションやソリューションのご提案までシームレスに提供させていただいております。



弊社遠隔読影ネットワーク概要



OAMIC遠隔読影システムは、全ての施設を高セキュリティネットワークにて接続しております。
 拠点間の通信内容は全て暗号化されております。お預かりした画像データおよび個人情報、安全に送受信、保管されます。
 ご依頼に関する管理業務や読影業務は全て仮想技術を用い、データセンター内の仮想端末にて動作します。

依頼施設 (病院等)



モダリティ (CT,MR) 依頼端末

依頼施設 (病院等)

依頼施設 (病院等)

依頼施設 (病院等)

⋮

セキュリティネットワーク

フレッツ VPN ワイド

NTT西日本が提供する、Internetに接続されて“いない”独立したネットワークです。

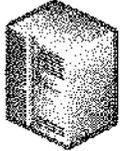
読影施設 (阪大医学部)



放射線科専門医による読影を実施する施設です。

セキュアネットワーク (VPN)

データセンター (関西・関東)



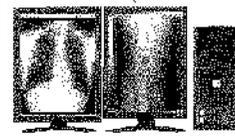
災害にも強く、セキュリティ上も強固なデータセンター内に、遠隔読影システム・画像情報サーバを格納し、運用を実施しています。

セキュアネットワーク (VPN)

大阪先端画像センター (吹田市)

受領した依頼画像の確認を実施し、内容に応じ医師をアサインします。また、セールスやシステム提供の中心的な施設です。

読影施設 (センター内)

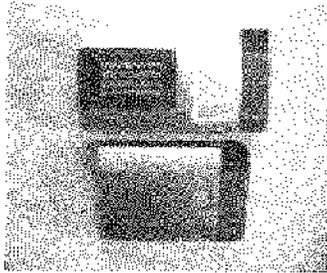


放射線科専門医による読影を実施する施設です。

弊社で行っているセキュリティ対策

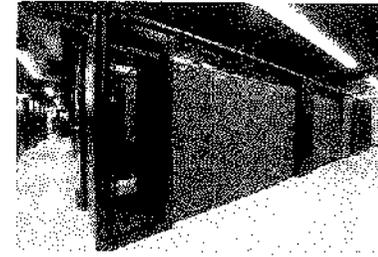


弊社では、お預かりするセンシティブな情報を保護するため、あらゆる面で対策を施しております。一例として、通信されるデータは安全なネットワーク上を、何重もデータ暗号化を行い通信を行っております。また、運用面でのセキュリティ対策にも力を入れております。



【運用上のセキュリティ対策】

- ・ICカードによる入退室制限（館内・室内）
- ・IDカードによる個人認証
- ・定期的な勉強会の実施
- ・パスワードを使用した利用者識別
（パソコン・読影依頼ソフトウェア）



“広義のセキュリティ”

【情報システムの暗号化】

- ・フレッツVPNワイド等セキュリティ回線の採用
- ・拠点設置ルータ間におけるVPN
- ・仮想技術による暗号化
- ・ウイルス対策ソフトの導入・統合管理

【データの安全保管】

- ・データセンターの利用
（厳密な入退室管理・災害対策）
- ・冗長化されたデータ保管サーバー
（機器クラッシュによるデータ損失対策）