2022.6.20

第9回医療サイバーセキュリティ協議会

「PACS障害における臨床現場での経験と対応」

市立東大阪医療センター　医療技術局　倉橋達人

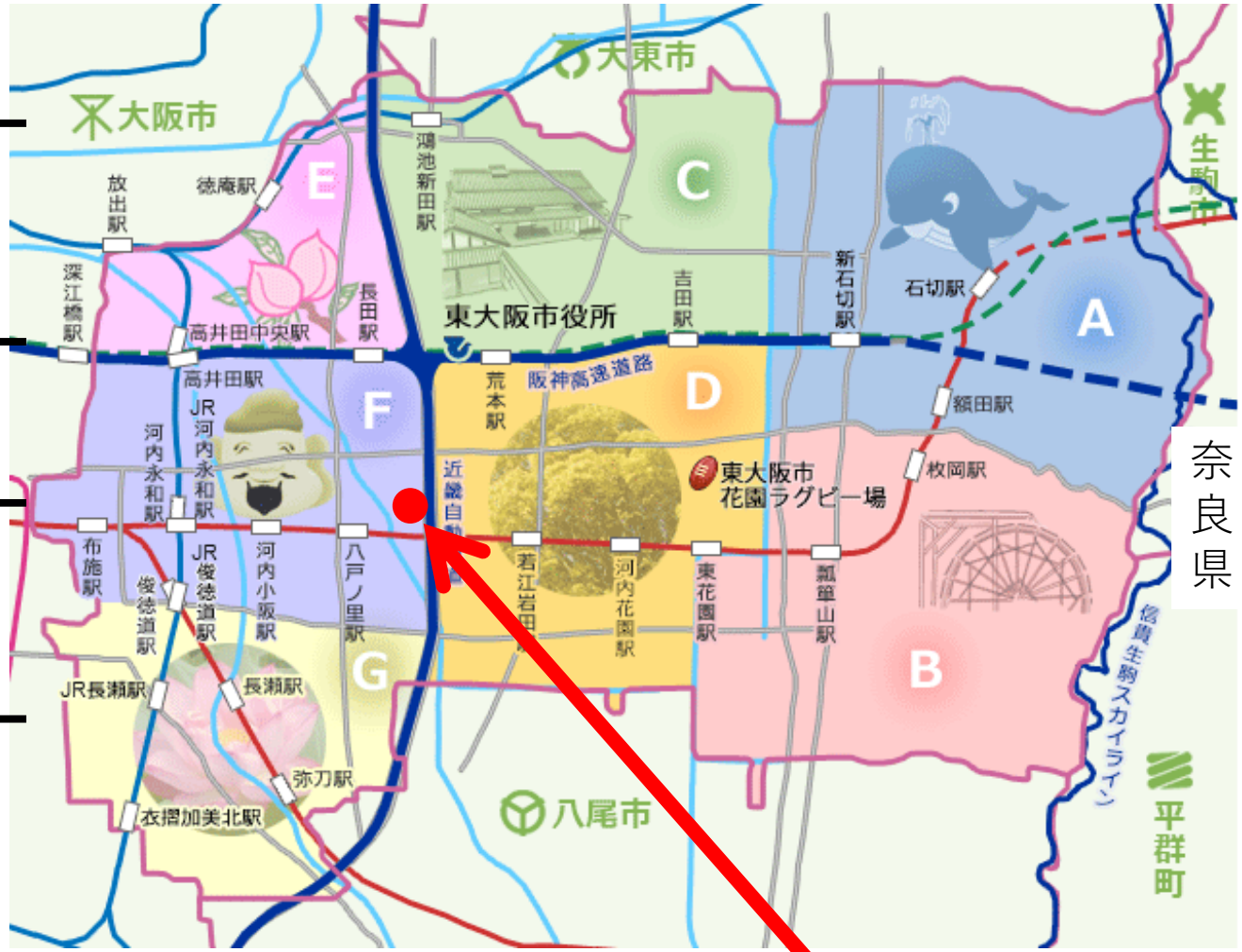
モノづくり・ラグビーのまち

東大阪市

東大阪市の位置

東大阪市は、河内平野のほぼ中央部に位置し、西は大阪市と、南は八尾市と、北は大東市と接し、東は生駒山系で奈良県と境を接する、面積61.81ｋｍ2、人口約51万人の都市です。

梅田←
本町←
なんば←
天王寺←



病院概要

●中河内二次医療圏
（大阪府東大阪市，八尾市，柏原市；82万人）
※地域がん診療連携拠点病院
※災害拠点病院
※大阪府新型コロナウイルス感染症重点医療機関
及び診療・検査医療機関

◆患者数及び病床数など（令和3年度）
・診療科 36科　　・延外来患者数 234,971人
・病床数 520床　　・延入院患者数 141,649人
・平均在院日数 9.1日

◆職員数など（令和4年4月）
・職員数（嘱託等含む）1,185人
・医師･歯科医師数（専攻医含む）150人

★医療情報技師
・7名（事務職2名，看護師1名，診療放射線技師4名）

自己紹介

●診療放射線技師（1989年）
；主に核医学診療・検査に従事
（シンチグラム，SPECT，PET-CT等）
；核医学専門技師認定（2006年）

◆経歴・職歴
・和歌山（医）向陽病院（1989年4月～）
・東大阪市立中央病院（1995年5月～）
・東大阪市立総合病院（1998年5月～）
；オーダーリング導入
；電子カルテ導入（2012年5月）
；医療クオリティマネジャー修了（2014年）
；医療情報技師取得（2014年）
・市立東大阪医療センター（2016年10月）

本日の内容

●発覚から現場対応完了までの一週間（その１～その５）

●モチベーション喪失と保持

●慎重に行うべきこと

●やっておいた方が良いと思うこと

●あれから1年が経ちました

●まとめ

☆システム，ネットワークに関することは次の講演で

●発覚から現場対応完了までの一週間（その1）

2021.5.31　03:10　**『発覚』**他院紹介患者の取り込み画像のPACS閲覧不可

電カル上の「紹介情報管理システム」からは見られるのに。。。？

（月）　03:25　MRI，CR画像のPACS転送不可　→　医師は装置モニターで画像確認，診断

03:30　PACSベンダー（A社）はリモート確認不可

04:52　A社が経営企画課（経企課）に一報　→　**ウィルス感染の可能性**　→　A社が現地入り

05:35　PACSの**ウィルス感染が判明**　全サーバーのウイルスチェックを開始

PACSを物理的に病院ネットワークから遮断

05:58　放射線技師当直者から一報　→　**「大規模障害」と認知**

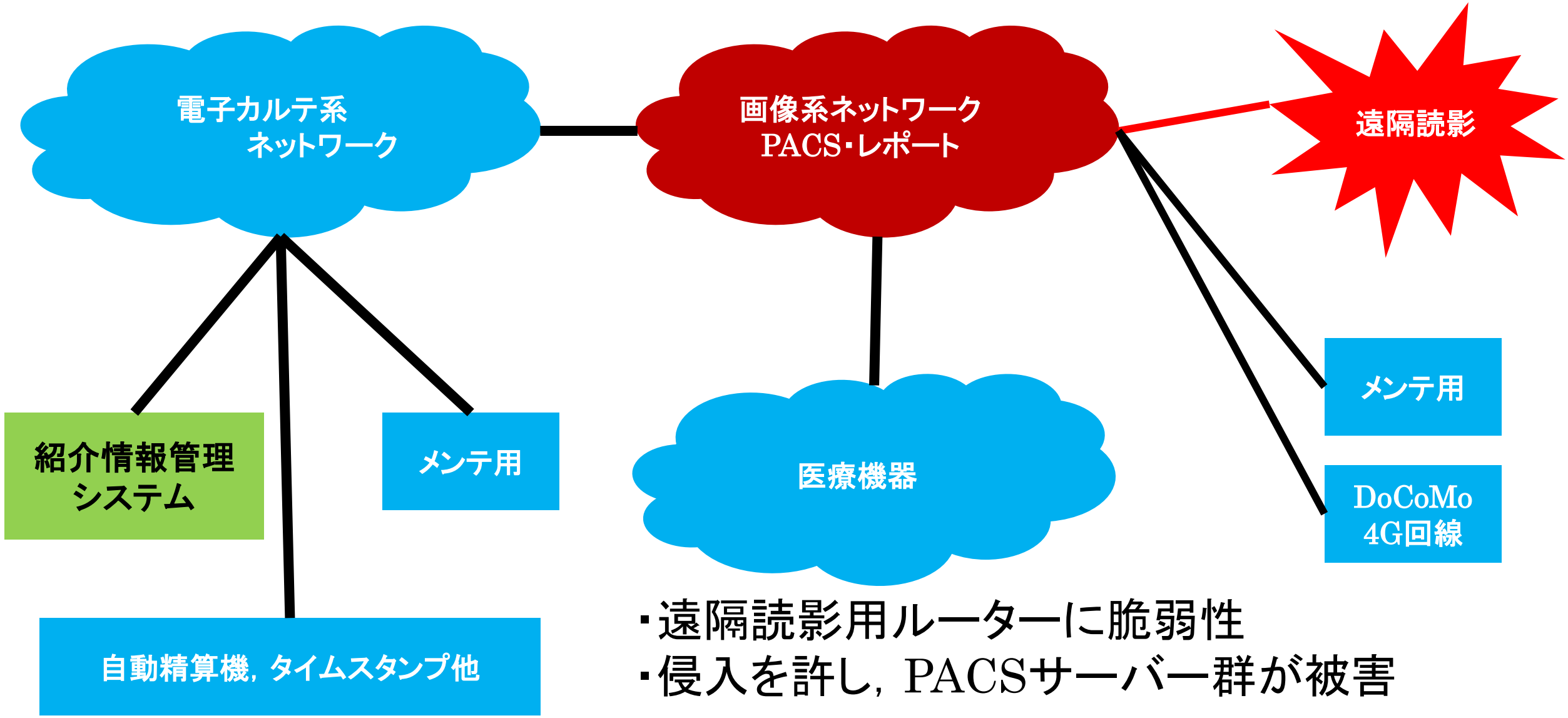
電源がOFF状態の電カル端末と画像診断装置をONにしないように指示

06:04　放射線科部長に報告．放射線技術科情報システム担当者を召集

07:10　**病院情報系の主要システム（電子カルテ等）障害はないことを共有**

07:53　職員通知院内メール【画像系サーバーPACSのダウンについて】を発出

「（第1報）5/31 AM8:00 」



・遠隔読影用ルーターに脆弱性
・侵入を許し，PACSサーバー群が被害

でも，当初はUSBやCDによる
ウィルス感染と思ってました.

●発覚から現場対応完了までの一週間（その１）

2021.5.31	**03:10**	他院取り込み画像の閲覧不可
（月）	03:25	MRI，CR画像のPACS転送不可 → 医師は装置モニターで画像確認，診断
	03:30	PACSベンダー（A社）はリモート確認不可
	04:52	A社が経営企画課（経企課）に一報 → **ウィルス感染の可能性** → A社が現地入り
	05:35	PACSの**ウィルス感染が判明** 全サーバーのウイルスチェックを開始
		PACSを物理的に病院ネットワークから遮断
	05:58	放射線技師当直者から一報 → **「大規模障害」と認知**
		電源がOFF状態の電カル（RIS）と画像診断装置をONにしないように指示
	06:04	放射線科部長に報告．放射線技術科情報システム担当者を召集
	07:10	**病院情報系の主要システム（電子カルテ等）障害はないことを共有**
	07:53	職員通知院内メール【画像系サーバーPACSのダウンについて】を発出
		「（第1報）5/31 AM8:00 」

●発覚から現場対応完了までの一週間（その1）

2021.5.31　03:10　他院取り込み画像の閲覧不可

（月）　04:52　A社が経営企画課（経企課）に一報　→　**ウィルス感染の可能性**

05:35　PACSの**ウィルス感染が判明**　全サーバーのウイルスチェックを開始

PACSを物理的に病院ネットワークから遮断

05:58　放射線技師当直者から一報　→　**「大規模障害」と認知**

???

ただのウイルス感染か？

先日の米石油パイプライン（2021.5.7）と同じで，

ハッカー攻撃？

もしかしたら時限的に，電カルも．．．

電源がOFF状態の電カル端末と画像診断装置をONにしないように指示

●発覚から現場対応完了までの一週間（その1）

2021.5.31　03:10　他院取り込み画像の閲覧不可

（月）　03:25　MRI，CR画像のPACS転送不可　→　医師は装置モニターで画像確認，診断

04:52　A社が経営企画課（経企課）に一報　→　**ウィルス感染の可能性**　→　A社が現地入り

05:35　PACSの**ウィルス感染が判明**　全サーバーのウイルスチェックを開始

PACSを物理的に病院ネットワークから遮断

05:58　放射線技師当直者から一報　→　**「大規模障害」と認知**

06:04　放射線科部長に報告．**放射線技術科情報システム担当者（医療情報技師）を召集**

07:10　**病院情報系の主要システム（電子カルテ等）障害はないことを共有**

Ⅰ．障害サーバーの状況と復旧・・・・事務職電算グループ

Ⅱ．院内外の広報・・・・・・・・・・・・・・・・事務職その他

Ⅲ．診療継続の方法検討・・・・・・・・・医療職

07:53　職員通知院内メール【画像系サーバーPACSのダウンについて】を発出

「（第1報）5/31 AM8:00 」

職員向け通知
（第1報）

初日AM8時

・状況報告

【画像系サーバーPACSのダウンについて】　5/31AM8:00

差出人

宛先
(2016人)

関係各位

5/31未明より画像系サーバー（PACS）の不具合が判明し、
現在改修に努めていますが、未だ復旧の目処がたたない状態です。

・放射線画像：CT、MRI、CRその他すべて
・内視鏡画像
・超音波画像

・これらの画像診断レポート

が電子カルテから参照できません。

検査そのものは施行できますが、
すぐに参照するには各検査室で閲覧するしかない状態です。

各部署で大変なご迷惑をおかけします。
申し訳ありません。
復旧に尽力しておりますので、今しばらくお待ちください。

随時ご報告します。

●発覚から現場対応完了までの一週間（その2）

2021.5.31　08:10　**予定手術をどうするか？　画像が必要な手術の出棟を一時停止**

逆紹介はどうするか？　外来受付開始

08:40　発覚時に電源OFFであった画像診断機器と画像系ネットワークを物理的遮断

この時は発覚した時（3:10）にウイルス感染したと思っていた。

後に，既に侵入されていたことがわかり，もしかすると感染していたかもしれない？

08:48　**検査受入開始**．但し，電子カルテ等でPACS閲覧不可

① 外来　；フィルム出力　② 救急室；診察医が来科し，検査室モニターで確認

③ **手術室**；　④ **逆紹介**；

⑤ **急を要さない説明は次回診察**

09:10　東大阪市市長室，東大阪市保健所に一報

09:20　**院内放送発出**

「画像診断センター、内視鏡センターの検査や過去検査の説明に影響が出る」

10:00　**「（第3報）5/31 AM10:00 」**

●発覚から現場対応完了までの一週間（その2）

2021.5.31　08:48　**検査受入開始**．但し，電子カルテ等でPACS閲覧不可

① 外来　；フィルム出力
② 救急室；診察医が来科し，検査室モニターで確認
③ **手術室**；**CT等の装置（感染不明）からCD作成**
紹介情報管理システム（電子カルテ系ネットワーク）で取込み，
ウイルスチェック．電子カルテ閲覧
④ **逆紹介**；**診療情報提供書の添付CDは作成不可，断固拒否**
相手先でウイルスチェック機能が働かなかった場合は．．．
⑤ **急を要さない説明は次回診察；**
とは言っても，明日検査できんの？説明できんの？？？

こうなると，医療職はベンダーさんに強く当たるようになります．いつ直るの？と

09:10　東大阪市市長室，東大阪市保健所に一報

09:20　**院内放送発出**

「画像診断センター、内視鏡センターの検査や過去検査の説明に影響が出る」

10:00　「（第3報）5/31 AM10:00 」

職員向け通知（第3報）

初日AM10時

【画像系サーバーPACSのダウンについて】　第3報：5/31AM10:00

差出人　：
宛先　：
(2016人)

関係各位

5/31未明より画像系サーバー（PACS）の不具合が判明し、
現在改修に努めていますが、10時現在でも
未だ復旧の目処がたたない状態です。

・放射線画像：CT、MRI、CRその他すべて
・内視鏡画像
・超音波画像
・これらの画像診断レポート
が電子カルテから参照できません。
検査は開始しており、それぞれの検査装置で画像保存しています。
急がない検査は別日にしていただくことをおすすめします。
頭部CT、X線撮影に限り、本日撮影の緊急性があるものは
「フイルム」で対応しています。
また、他検査では検査室に来ていただければ閲覧できます。

本日の検査CT、MRIは時間がかかりますが、
取り込み画像閲覧画面から参照できるようにすることが可能です。（検査終了時から1時間ほどかかります）

ただ、過去画像を参照する方法は現在もありません。
未だに画像サーバーが立ち上がらない状態が続いています。

各部署で大変なご迷惑をおかけします。
申し訳ありません。

随時ご報告します。

職員向け通知
（第3報）

初日AM10時

【画像系サーバーPACSのダウンについて】　第3報：5/31AM10:00

差出人　：
宛先　：
(2016人)

関係各位

5/31未明より画像系サーバー（PACS）の不具合が判明し、
現在改修に努めていますが、10時現在でも
未だ復旧の目処がたたない状態です。

・放射線画像：CT、MRI、CRその他すべて
・内視鏡画像
・超音波画像
・これらの画像診断レポート
が電子カルテから参照できません。
検査は開始しており、それぞれの検査装置で画像保存しています。
急がない検査は別日にしていただくことをおすすめします。
頭部CT、X線撮影に限り、本日撮影の緊急性があるものは
「フイルム」で対応しています。
また、他検査では検査室に来ていただければ閲覧できます。

えっ！
まだ午前OP予定のCD
作ってるところやで！
取り込みもまだやん！

本日の検査CT、MRIは時間がかかりますが、
取り込み画像閲覧画面から参照できるようにすることが可能です。（検査終了時から1時間ほどかかります）

ただ、過去画像を参照する方法は現在もありません。
未だに画像サーバーが立ち上がらない状態が続いています。

各部署で大変なご迷惑をおかけします。
申し訳ありません。

随時ご報告します。

●発覚から現場対応完了までの一週間（その3）

2021.5.31　10:10　**理事長室召集**

理事長　;現在までの状況と復旧の目途について教えてほしい.
出席①　;A社が復旧に尽力，今日中には･･･
理事長　;明日は通常に戻せるということか？
→無理です．まだ詳細調査も始まっていません．おそらく，5/7米石油パイプラインと同じサイバー攻撃を受けたと思います．
理事長　;やっぱりそうか.
出席②　;いやいや，倉橋は･･･　（みなさん退出）

理事長　;なんでそう思う？
→アンチウイルスソフトを抜けてきた．発覚時間がAM3時．こんな大規模な障害を一つのウイルス感染で起こすとは？
理事長　;状況が判明したら，被害届を考えなあかんな.
→大阪府警どころか厚生労働省にも報告が必要かと.
理事長　;でも，なんでうちが狙われるんや？　どこに価値があるんや？
→東大（病院）＋大阪 ≒ 東大阪　ぐらいしか.

10:30　A社による詳細調査開始

11:00　「（第4報）5/31 AM11:00 」

職員向け通知
（第4報）

初日AM11時

【画像系サーバーPACSのダウンについて】　第4報：5/31AM11:00

本日日勤帯での復旧は困難な見通しです。
明日、復旧できるかどうかも不明です
非常に重大なトラブルであることが判明しています。

・放射線画像：CT、MRI、CRその他すべて
・内視鏡画像
・超音波画像
・これらの画像診断レポート
が電子カルテから参照できません。
検査は開始しており、それぞれの検査装置で画像保存しています。
急がない検査は別日にしていただくことをおすすめします。
頭部CT、X線撮影に限り、本日撮影の緊急性があるものは
「フイルム」で対応しています。
また、他検査では検査室に来ていただければ閲覧できます。
（超音波は装置でしか見れませんので、実際難しいです）
本日の検査CT、MRIを、取り込み画像閲覧画面から
参照する運用は、非常に手間と時間がかかります。
「緊急・超重要症例」に限定させてください。
現在、緊急手術などの症例に運用しています。
皆さんの譲り合いでなんとか利用可能ですので
よろしくお願いします。

過去画像を参照する方法は現在もありません。
未だに画像サーバーが立ち上がらない状態が続いています。
（過去1週間程度で、緊急性のある症例はご相談ください）

各部署で大変なご迷惑をおかけします。
申し訳ありません。

随時ご報告します。

やっと
理解してもらえた

●発覚から現場対応完了までの一週間（その4）

2021.6.1　10:00　画像サーバー以外のウイルスチェック完了

12:00　**米国食肉加工会社にサイバー攻撃；FBIが動く（NHKお昼のニュース）**

F株式会社営業担当電話が不通（3D画像システム内のデータ転送について）

→おかしいな。。。（夜）F株式会社がサイバー攻撃を受けたことが判明

理事長；国，府，市関係機関へ報告指示

近畿厚生局に一報（画像管理加算2を返上しないといけないのか？）

23:50　仮サーバー設置完了

2021.6.2　08:30　**CT，MRI，一般撮影の自動転送開始**

09:30　**厚生労働省医政局研究開発振興課医療情報技術推進室に電話相談**

（医療情報システムの安全管理に関するガイドライン第5.1版 6.10章）

14:00　**大阪府警ハイテク犯罪対策課に訪問相談**

厚労省，府警共に

①コロナ患者を受け入れ＆治験を開始しているか？

17:00　**第1回PACSランサムウェア感染事案対策本部**

●発覚から現場対応完了までの一週間（その5）

2021.6.2　17:00　**第1回PACSランサムウェア感染事案対策本部（開催時はPACS障害対策本部）**

CT，MRI，一般撮影，内視鏡など装置に残る画像の転送開始

→本当にやっていいんですか？次に何が起こるかわかってますか？
心構えは大丈夫ですか？

放科部長；診療を止めることはできない．我々が負担を被るのは仕方ない．

→私らはなんも悪いことしてない．
それで先生が倒れたら今日はいけても明日は大丈夫なんですか？

2021.6.3　08:30　**超音波検査の自動転送開始**

→やっぱり起きてしまった。。。

「（第11報）6/3 AM8:30 」

13:30　大阪府警が来院（ログ取り）

2021.6.4　08:30　検像端末の運用再開

15:00　**「（第13報）6/4 PM15:30 」**

2021.6.7　08:30　レポートシステムの運用再開

職員向け通知
（第11報）

4日目
AM8時30分

【画像系サーバーPACSのダウンについて】　第11報：6/2AM8:30

新（仮）サーバーの運営を開始しています。
過去画像も徐々に閲覧できる画像が増えていますが、
各モダリティーからの転送業務が集中し、不安定です。
AM8時現在、すでに新サーバーの不具合が生じています。
「仮」サーバーは従来のサーバーと比較して脆弱です。
今後もサーバー停止などのトラブルのリスクが高い状態です。
本日は過去画像の転送は必要最小限とします。

放射線科からのお願い
＊読影室では、未だ通常の読影ができない状態です。
読影システムもない中、使命感から読影を続けていますが、
効率も悪く、数をこなすのは困難です。
さらに、「再読影」により、業務は逼迫しています。
（いったん読影したものをし直す作業は精神的にもやられます）

＊しばらくは、「要読影」のみの対応とさせてください。
＊まず、画像をごらんになって、どうも怪しい、
あるいは専門外の領域は必ず応えるよう努力します。
読影室３６０２まで

＊今回、画像系は類を見ない甚大な被害を被っています。
復旧と同時に原因究明も進めていますが・・・
あなたのその無造作な医療モダリティーへのUSB接続が
今回の被害の原因かもしれません。
また、かろうじて命をつないでいる電子系サーバーに
同様の被害を再発させるリスクもあります。
医療モダリティ（電子カルテその他）へのUSBへの接続は
（充電行為も含めて）厳に慎んでください。

＊今回のトラブルを耐えて診療を行っている先生方や看護師さん、
なんとか復旧できるよう努力している技師・事務系の皆さん
他、関わる皆さんのご尽力に感謝しています。

発覚4日目
6/3 AM8:30

●先の見えない状況に

●「いったん読影したものをし直す作業は精神的にもやられます」

放射線科医師は疲れがピーク

●私＆当科医療情報技師は・・
・こんな経験は
・PACSがさらになる（嬉しい！）
・FBIが来たらどうしよう？

職員向け通知
（第13報）

5日目
PM15時00分

【画像系サーバーPACSのダウンについて】　第13報：6/4　15：00

差出人　：
最終更新者：
宛先　：
(2016人)

関係各位

新（仮）サーバーの運営を開始しています。

昨日の連絡通り、以下の画像データは残存しています。
徐々にサーバに転送していますが、
下記期間の参照できない画像で急ぐものがあれば、
検査室にお問い合わせください。

MRI　：2021.5.27以降（加えて、2021.5.21以降の一部）
パノラマ：2021.3.5以降
単純撮影：2021.2.1以降（訂正です。申し訳ありません）
CT　：2020.12.16以降
内視鏡 ：2021.5.2以降
超音波 ：2021.4.1以降の大部分

追加：
骨シンチ　：2020.9.2　以降
心筋シンチ　:2019.6.7　以降
脳血流シンチ　：2018.10.17　以降
その他　：2014.1.9　以降

発覚5日目
6/4 PM15:00

●5日目で残存データが判明

●発覚から現場対応完了までの一週間（その5）

2021.6.2　17:00　**第1回PACSランサムウェア感染事案対策本部（開催時はPACS障害対策本部）**

CT，MRI，一般撮影，内視鏡など装置に残る画像の転送開始

→本当にやっていいんですか？次に何が起こるかわかってますか？
心構えは大丈夫ですか？

放科部長；診療を止めることはできない．我々が負担を被るのは仕方ない．

→私らはなんも悪いことしてない．
それで先生が倒れたら今日はいけても明日は大丈夫なんですか？

2021.6.3　08:30　**超音波検査の自動転送開始**

「（第11報）6/3 AM8:30 」

13:30　大阪府警が来院（ログ取り）

2021.6.4　08:30　検像端末の運用再開

15:00　**「（第13報）6/4 PM15:30 」**

2021.6.7　08:30　レポートシステムの運用再開　発覚から丸一週間かかりました．

この時点で，画像診断センターが担う「検知・初動対応」と「現場対応」は完了した．

本日の内容

- 発覚から現場対応完了までの一週間（その１～その５）
- モチベーション喪失と保持
- 慎重に行うべきこと
- やっておいた方が良いと思うこと
- あれから1年が経ちました
- まとめ

●モチベーション喪失

「**喪失**」もうあかんと思ったのは，

・各種画像診断装置から診療情報提供書のCDを作成するためにウィルスチェック（有償）を大至急行うことを提案したが・・・

→**費用対効果がわからないと回答あり.**

・急を要さない説明は次回診察とは言うても・・外来診察室からTEL.

→**いつ復旧するか誰もわからない．．．**

（医師）読影は検査室モニターを確認しながら，直接電子カルテに記載した.
読影したと分かっているのに，再度読影しないといけない.

・影響は診療だけではない

→治験，学会，認定・資格，施設基準

・日常診療や復旧作業は部署や人で雲泥の差

→診療行為は可能だが画像・レポート情報はない．普段とは異なる仕事が必要.
診療放射線技師全員が携われる業務ではない（知識や端末）

●モチベーション保持

「**保持**」できたのは，

・こんな経験はしたくてもできない（不謹慎ですが）
・部下（医療情報技師2名）や経企課電算Gが同じ方向を向いていた．
　指示通り＆**臨機応変に，積極的に**行動．

・理事長はわかってくれていた．

→それでもコロナ感染や濃厚接触者としてメンバーが離脱しないか不安．

本日の内容

- 発覚から現場対応完了までの一週間（その１～その５）
- モチベーション喪失と保持
- **慎重に行うべきこと**
- やっておいた方が良いと思うこと
- あれから1年が経ちました
- まとめ

●慎重に行うべきこと

「広報」は慎重に；職員向け通知の内容によっては自らの首を絞める

・患者（院内放送）；2時間毎
・職員（電カル端末搭載のサイボウズメール）；計17報
　1日目；主に状況報告　6報
　2日目；主に**今後の予定**　3報**・・・特に慎重さが必要**
　3日目～7日目；残存データの報告など　1報/日
　22日目；最終報

・院外（ホームページ，マスコミ）

当初；お情け頂戴，皆様助けて！！！と思ってたのですが．．．

厚生労働省や大阪府警に相談後；

→**攻撃成功を広報**することで，**執拗に身代金メールが送付される．**
愉快犯，職員への脅迫・嫌がらせ

相談前はPACSランサムウェア感染事案対策本部→PACS障害・・・

本日の内容

- 発覚から現場対応完了までの一週間（その1～その5）
- モチベーション喪失と保持
- 慎重に行うべきこと
- **やっておいた方が良いと思うこと**
- あれから1年が経ちました
- まとめ

●やっておいた方が良いと思うこと

「対策」

「リモートルーターのファームウェアのアップデート」

- **誰が担っているのか？**
- 保守範囲内　or　保守範囲外

「ウィルス対策ソフト」

- PC端末　＆　サーバー

「情報セキュリティ研修」

「サイバー攻撃の情報収集」（厚労省やセキュリティベンダー）

- 対応策を速やかに実施できる環境
- **専門人材，専任担当者の配置**

【資格，知識】 厚労省通知が読解できること

日本医療情報学会（JAMI）；

上級医療情報技師，医療情報技師

日本診療放射線技師会（JART）；

医療画像情報精度管理士 **and**

【実践】

技術系； 原因を追求できるか

臨床系； 経営層を含む職員から信頼されているか

経営層に的確に状況説明できるか

診療を継続するための調整力があるか

院内外各所に適切な広報を発信できるか

●やっておいた方が良いと思うこと

「運用」

「バックアップ」

・ネットワークから切り離されている；テープ保管など

・冗長化；でも，同じ機能が複数ならコストがかかる．

今回はPACSの単独ネットワーク障害．２日間は電子カルテから閲覧不可．

→電カル系ネットワークの紹介情報管理システム画像ビュアーがOK．

別系統ネットワークで参照が可能であった．

CD経由で取り込み，手術や緊急，救急患者に対応可能であった．

手術の日程延期はゼロ．予約患者の延期は初日34名，翌日4名．

●やっておいた方が良いと思うこと

「訓練」・・どんな訓練が有効かわかりません.

「紙運用」

- 初診，新患なら対応可能かもしれない.
- 入院患者500人のオーダー，指示情報は全て前夜に事前印刷
- オーダー発行；依頼元，部門控，医事用の3枚綴り
- 診察記録；手書き
- 各部門；患者登録，会計情報が全て手作業
- 画像診断；フィルムとシャーカステン
- **復旧後にスキャナ**

●やっておいた方が良いと思うこと

「訓練」・・どんな訓練が有効かわかりません.

「紙運用」

- 初診，新患なら対応可能かもしれない.
- 入院患者500人のオーダー，指示情報は全て事前印刷
- オーダー発行；依頼元，部門控，医事用の3枚綴り
- 診察記録；手書き
- 各部門；患者登録，会計情報が全て手作業
- 画像診断；フィルムとシャーカステン
- 復旧後にスキャナ

こんなことはできません.

職員の半数以上は紙カルテ時代を知らない.

「障害時の問い合わせ」

- いつ復旧するか誰もわからない. こんな場合は電話はかけない.

→じゃあどうするか？

本日の内容

- 発覚から現場対応完了までの一週間（その1～その5）
- モチベーション喪失と保持
- 慎重に行うべきこと
- やっておいた方が良いと思うこと
- あれから1年が経ちました
- まとめ

●あれから1年が経ちました

6/24　**警察庁が「サイバー局」を2022.4新設**
6/28　**厚労省通知「事務連絡（注意喚起）」**
　　医療機関を標的としたランサムウェアによるサイバー攻撃について」
7/19　**ロシア系ハッカー集団のサイト閉鎖**
9/21　**ランサムウェア「REvil」の無償復号ツールが公開**
　　（BitDefender；ルーマニア）
11/4　サンプルデータで復号化ツールを検証
11/8　FBI，ユーロポールが犯人を確保，起訴．600万ドル押収．

12/9　**復号化完了**
3/ 1　**医療安全上や法的開示請求に伴う画像の出力**
　　個人要望の出力が増える

　　徐々にPACSで閲覧できる画像がふえてきた

　　現時点で，2015年1月以降の画像が閲覧可能　　完了は8月中の見込み

本日の内容

- ●発覚から現場対応完了までの一週間（その１～その５）
- ●モチベーション喪失と保持
- ●慎重に行うべきこと
- ●やっておいた方が良いと思うこと
- ●あれから1年が経ちました
- ●まとめ

●まとめ

相手はプロを超えた国家レベルのハッカー集団

いくら準備しようが突破される.

・診療（事業）を継続させるために

・医療機関は突破されても良い環境を準備すべき

→バックアップをいかに構築しておくか. **※紙運用ではない方法.**
診療への影響を最小限にするための**対策**, **運用**, **訓練**が重要.

・国や学会, 団体は柔軟な対応と金銭的支援をお願いしたい

→治験・・・・・・・「中止」　患者さんに負担. 信用低下
→学会発表・・・「取り下げ」　モチベーション低下
→認定・資格・・「更新不可」モチベーション低下
→施設基準・・・「取り下げ」　経営悪化

●まとめ

・情報公開のタイミングと対象

・模倣犯や二次被害を被る可能性がある.
→都道府県警察の対応が異なる.
→警察庁「サイバー局」の新設で指示が統一されるかもしれない.

・しかし，各医療機関に対策を練らせるには情報公開が必要

・医療機関の情報セキュリティ＝情報管理部門・・・は必死だが

・職員個人は？？？

・実際起きたら診療に影響＝医療安全＝職員全員

・サイバー攻撃に対応できる人材確保と組織運営

・追求　・信頼　・説明　・調整　・発信

●お願い

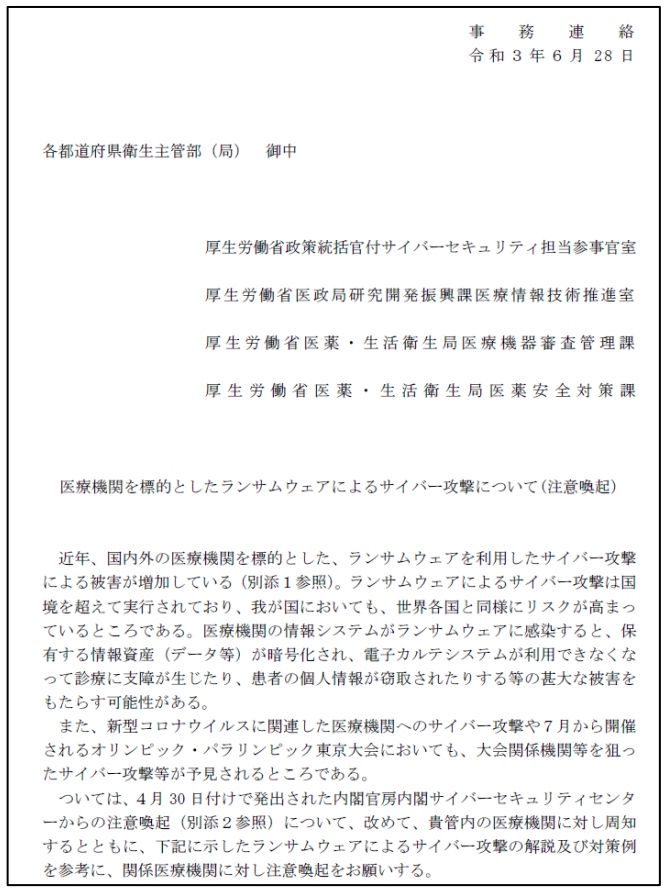
6/28　厚労省通知「事務連絡（注意喚起）」

・77頁

1 ランサムウェアについて

2 最近の攻撃の手口

3 ランサムウェア攻撃への対策（3頁のみ）



事　務　連　絡
令和３年６月28日

各都道府県衛生主管部（局）　御中

厚生労働省政策統括官付サイバーセキュリティ担当参事官室

厚生労働省医政局研究開発振興課医療情報技術推進室

厚生労働省医薬・生活衛生局医療機器審査管理課

厚生労働省医薬・生活衛生局医薬安全対策課

医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）

近年、国内外の医療機関を標的とした、ランサムウェアを利用したサイバー攻撃による被害が増加している（別添１参照）。ランサムウェアによるサイバー攻撃は国境を超えて実行されており、我が国においても、世界各国と同様にリスクが高まっているところである。医療機関の情報システムがランサムウェアに感染すると、保有する情報資産（データ等）が暗号化され、電子カルテシステムが利用できなくなって診療に支障が生じたり、患者の個人情報が窃取されたりする等の甚大な被害をもたらす可能性がある。

また、新型コロナウイルスに関連した医療機関へのサイバー攻撃や７月から開催されるオリンピック・パラリンピック東京大会においても、大会関係機関等を狙ったサイバー攻撃等が予見されるところである。

ついては、４月30日付けで発出された内閣官房内閣サイバーセキュリティセンターからの注意喚起（別添２参照）について、改めて、貴管内の医療機関に対し周知するとともに、下記に示したランサムウェアによるサイバー攻撃の解説及び対策例を参考に、関係医療機関に対し注意喚起をお願いする。

① 攻撃対象領域の最小化

インターネットからアクセス可能な、あるいは公開するサーバやネットワーク機器を最低限にするとともに、インターネット経由で利用するアプリケーションも最低限にする。さらに、それらが乗っ取られる場合を考慮し、そこからアクセス可能な範囲を限定する。

② なりすまし、不正ログイン対策

組織外からの認証・認可の対象や範囲を特定し、限定する。多要素認証等の強固な認証方式を採用するとともに、アクセスや認証のログを取得し、監視する。

③ 脆弱性対策

端末及び利用ソフトウェア、ファームウェア（ハードウェアを直接操作するソフトウェアでハードウェア内にある）等を常に最新の状態に保つ。最近は、脆弱性が公開されてから、その脆弱性を悪用する手法が出回るまでの期間が短いため、迅速に対応できるよう体制や計画を整備する。

④ ウイルス対策ソフト

ウイルス対策ソフトを導入し、定義ファイルを最新の状態に保つ。

⑤ 拠点間ネットワークのアクセス制御

ランサムウェア攻撃に限らず、複数の拠点をネットワークで接続している場合、対策の弱い拠点から侵入され、そこから侵入される事例が散見されるため、拠点間のアクセス制御を見直す。

⑥ 攻撃メール対策

攻撃メールへのセキュリティ装置等による対策や、職員の啓発や訓練を行う。

⑦ 内部対策

攻撃者による侵害を早期に検知するため、統合ログ管理、内部ネットワーク監視、コンピュータの不審な動作を監視する仕組み（製品等）を導入する。

⑧ ログの取得と保存

感染経路、他の端末、サーバへの感染拡大の有無の確認等を行うため、各種のログを取得し、一定期間（1年以上を推奨）保存する。

⑨ その他

夜間等に活動し、感染を広げるランサムウェアの被害を防止するため、使用していないパソコンの電源を切る。

●お願い

・77頁；どこが重要か？
→読みやすい，簡単な指示．この通知が有効であったなら・・・

・注意喚起では甘い．
→「する」ではなく「せよ」「しなさい」

例）
① VPNのリモートルーターのファームウェアアップデートが最新であることが判明していない場合は**アップデートせよ．**
②その指示が？？？の場合は**早急に遮断せよ．**
システムベンダーに**アップデートを依頼せよ．**
③新たに設置する場合はアップデート条項を設けて，**アップデート手順を確定させよ．**
④システムベンダーは設置したリモートルーターの状況を確認し，アップデートについて**医療機関と協議せよ．**

指示に従って対応した施設が攻撃を受けた際には，金銭的補助を用意してほしい．