社会医療法人有隣会 東大阪病院 2022 vol.97

地域連携だより

腎臓・透析専門医が3名となり
９月より腎不全外来も３名体制で行います。

4月より透析科に三上医師が入職し3名体制で診療を行っております。専門医による腎不全外来を通し、保存期腎不全から透析導入・維持透析迄一貫した治療を行います。今後も地域の先生方と連携をより一層深め、地域の健康を守る為　診療体制を充実させて参ります。ご協力の程よろしくお願い致します。

腎臓内科（透析）透析センター長代行

梅田　優（うめだ まさる）

- ■日本透析医学会専門医・指導医
- ■日本腎臓学会専門医
- ■日本泌尿器科学会専門医
- ■医学博士
- ■身体障害者福祉法第15条指定医

腎臓内科（透析）部長

飯田　剛嗣（いいだ たけし）

- ■日本透析医学会専門医・指導医
- ■日本腎臓学会専門医・指導医
- ■日本泌尿器科学会専門医・指導医
- ■日本内科学会認定内科医
- ■身体障害者福祉法第15条指定医

腎臓内科（透析）

三上　典子（みかみ のりこ）

- ■日本透析医学会透析専門医
- ■日本内科学会総合内科専門医
- ■身体障害者福祉法第15条指定医
- ■日本抗加齢医学会専門医

《 腎不全外来 》・・・９月より腎不全外来は週3回となります。

	月曜日	火曜日	水曜日	木曜日	金曜日	土曜日
14:00～17:00	三上医師	梅田医師	—	—	飯田医師	—

《腎不全外来》は完全予約制とさせていただいております。大変ご迷惑をおかけしますが、ご理解とご協力の程よろしくお願い致します。

【対象患者さん】

・クレアチニン値3.0以上の方

クレアチニン値3.0以上で腎臓の残存機能が20%を下回ってきますので、上昇スピードが速くなります。経過を診ながら、透析に向けて準備を行って参りたいと思っております。

☆腎不全外来についてのご相談やご予約は地域医療連携室迄お電話ください。

腎臓あるいは透析に関する事がございましたら、お気軽にご相談ください。
地域の先生方との併診体制で患者さんの健康をバックアップさせていただきます。

東大阪病院 **地域医療連携室**　【 月曜日～金曜日 8:30~19:30 】　【 土曜日8:30~17:00 】

直通TEL 06-6932-0369　直通FAX 06-6932-0086

～病院システム部システム課 より～

クリニックで可能なランサムウェア対策について

システム課
課長 吉岡伸能

いつもお世話になっております。

東大阪病院 病院システム部システム課課長の吉岡です。

ニュース・新聞記事などでご存知かと思いますが、医療機関を狙ったサイバー攻撃（ランサムウェア感染）が発生し、医療システムが停止し診療ができなくなるという、深刻な事態が発生しています。

ランサムウェアとは、身代金要求型不正プログラムとも呼ばれるコンピュータウィルスで、感染したコンピュータをロックしたり、ファイルを暗号化して使用不能とし、元に戻すことを引き換えに「身代金」を要求するというものです。近年では「身代金を支払わなければ情報を暴露する」といった二重脅迫型もあります。

<クリニックでできる対策>

このようなサイバー攻撃に対してクリニックでできる対策を5点挙げてみました。

(1)電子カルテネットワークとInternetネットワークの切り離し

基本的に電子カルテとInternet利用PCのそれぞれのネットワークは切り離しておくのが安全です。ウィルス等の脅威はInternetを経由して侵入してくるためです。

(2)パソコンの感染対策

Internet利用PCには必ずアンチウィルスソフトを導入し、定義を最新に保つ必要があります。また電子カルテでもクラウド型の場合はInternetに接続するため、同様にアンチウィルスソフトの導入が必要です。

(3)外部媒体利用時の感染対策

外部からの持込みデータや、Internetからダウンロードしたデータを格納したUSBメモリ等の媒体については、利用前にウィルスチェックを行い、安全を確認してから利用すべきです。

(4)電子カルテベンダのリモート保守の確認

最近のベンダの保守は、遠隔からVPN接続してリモート保守を行うケースが増えています。ところがそのリモート回線の脆弱性を突いてランサムウェアが侵入する危険性があるため、接続機器の脆弱性対処（アップデート）を実施しているか、また医療情報システム安全管理ガイドラインに則り構築しているか、ベンダに確認が必要と考えます。

(5)電子カルテのデータのバックアップ

対策としてオフラインでの保存が推奨されます。ランサムウェアはネットワークを経由してバックアップ装置にも感染し、データを暗号化するからです。対象はシステム、診療データ、医事データ、画像イメージがあり、それらをどのような媒体で何世代取得すべきかなど、ベンダに構築を提案してもらい決めるのが良いでしょう。

サイバー攻撃の対策を全て取ることはコスト的にも難しく、システムベンダと相談しながら、対応範囲と優先順位を決めて対応する必要があると考えます。まずはできるところから対策し、脅威に備えるのが肝要ではないでしょうか。