ディスカッション時にチャットに記載された質問内容です。一部は、ディスカッション時に回答しています。

1	東大阪のPACS障害ですが、感染経路の公表は難しいですか？
2	GLが出るまでの対応は？ベンダーはGLが出るまでは、しっかりしたスキームが出てきそうにありません。それまでにやられたらと心配です。
3	現在、医療情報ネットワークには電子カルテシステム(HIS)だけではなく、各部門システムのサーバ、端末が接続されております。（それらのメンテナンス回線も心配ですが）それに加えて、医療機器のコンピュータ化進み、各システムには様々な医療機器がネットワーク接続されています。その医療機器におけるメンテナンス回線、USB接続などがどうなっているのか分からない状況です。これらは、バックドアになるかと思われ、医療情報担当としては非常に恐ろし状況です。 ・　医療機器の購入・管理部門が異なっている。購入担当はコンピュータサイエンスの知識な
4	Fortinetの脆弱性に起因して認証情報が漏洩したと認識しており、もはやOSの機器アップグレードだけでなく、アップグレード前に使用していた認証情報を変更（パスワードの変更）を行う必要があるのだろうと思います。それができない場合に、まずダークウェブ等に自院の認
5	基本的に321でBACKUPしかないと思っています。
6	問題は、復旧の時間をどのように短縮するかだと思います。単純なバックアップの場合、復旧は2週間掛かると言われ頭を抱えています。V5.2は4月に出るようです。
7	緊急時を想定して、どこまでのデータをバックアップするのか、いつだれが障害を判断するのか、事業継続を如何にするのかなどを含めた意識形成が急務であると思います。保健医療福祉介護分野は、情報安全に対するインセンティブ（収入）が認めれれてない歴史が、攻撃される
8	システム内ストレージ、メディア、遠隔地へのオンラインストレージなど、多層のバックアップが望ましいことは理解できるのですが、特にランニングコストがかかるため、ガイドライン遵守のために公的支援（補助金）があると進みやすと思うのですが、、、やりたい気持ちはあ
9	ＦｏｒｔｉＮｅｔの場合はかなり前に、Ｆ社から出ていたので、現場のベンダーの責任です
10	東大坂さんの件は大変為になりました。
11	VPNの種類には通常のインターネットを利用したインターネットVPNと、通信事業者の閉域網を利用したIP-VPNがあると思うのですが、今回の事象はインターネットVPNでしょうか。通信事業者提供のIP-VPNを利用するとかなりリスクが減ると思うのですがいかがでしょうか。
12	事業継続を主眼に置く場合、「絶対」は無いので感染する可能性を想定したうえで、データとハード両面のバックアップが基本のように思います。
13	OSのセキュリティー強化という点で、バージョンアップが必要とのことですが、OSのバージョンをアップデートすると電子カルテシステムが起動しなくなるケースもあるかとおもいま
14	国が推進するマイナンバー資格確認システムについて、病院システムとの接続についてご意見

15	「事件後の事例公表」についてお伺いいたします。我々病院の情報システム管理者として、今回のような事例公表は非常にありがたいです。徳島の事例も当初からランサムウェアとして広く公表されたおかげで、我々システム管理者から病院経営者に危機感をあおって対策強化を働きかけることができました。しかしながら、攻撃を受けていながら全く情報公開がされていない事例もいくつかあるようなことをお聞きしております。事例は一つでも多くあればあるほど
16	当社の様な一般中小企業ですと、地域の商工会がセキュリティ啓蒙・注意喚起やセミナーなどの紹介をするのが一般的ですが、医療業界の場合は恐らくそういう観点で啓蒙や注意喚起を行う組織がないのが問題かなと勝手に考えていますが、松山さんがおっしゃるように医療ベン
17	システム管理部門としての職員として、必要な知識や現実に違いがあり過ぎる印象があります。日々皆様はどのように自己研鑽されているのでしょうか。教えていただければ幸いです。
18	指針を待っていても３２１のバックアップから大きく離れることは無いと聞いています。今般のランサム騒ぎで経営陣がリスクの認識を持ってくれたのが不幸中の幸いでした。ゼロトラストの観点からやられることを前提のランサム対応を検討していますが、一番問題は、電カル再起動の時間短縮です。今のところベンダーからは14日間と言われており話になりません。　何
19	もし事が起こった場合、職員、特に医師のパニックは想像を絶するものがあると予想されるのですが、いちいち対応していてはとてもやりきれません。鎮めるための効果的な文句があれば
20	報道では詳細が不明ですが、侵入された経路はSSL-VPNのように見えています。しかし、病院側が用意するリモートメンテナンスシステムは、ほぼSSL-VPNかと思いますが、なぜSSL-
21	徳島の事例だと、内部の協力者を募るようなランサムウェアが使用されているようですが、そういった事例に対する対応は何かありますでしょうか？
22	SSL-VPNは証明書をきちんと更新していればセキュリティレベルもIPSECとほとんど変わらないレベルのセキュリティですし、443ポートなので障害にも強いです。先月NTTのフィルタリング障害（キャリア障害）で顧客の病院さんのIPSEC-VPNが6時間停止した際もSSLは通信できてました。通信のオーバーヘッドが大きいのでIPSECよりは少しパフォーマンスが悪いです
23	機器のOSレベルアップ、ウイルス対策も気になります。
24	his系NWのセキュリティ管理が弱いと思いますが、ハードウェアによるNW監視システム等の
25	多数の部門システム、カルテ次第ではカルテでも複数のシステム(サーバ)が稼働している中で、医療情報として専門職種として働いている人はごく少数だと思っています。ちょっと詳しい医事課職員が兼任とはよくある話だと思います。医療業界自体がITリテラシーが低く、通常の保守管理体制、安定稼働に対する考え方や、そこに賃金や人数を投入する考え方が低いのが