#	ご質問	回答
1	サポート切れOSを使用している医療機器につき、使用を廃止し予算申請の上機器更新すべきと思います。 その対応がすぐには難しければ、医療機器がWindowsであれば、オーダー内容受信と画像送信の指定サーバーのみに制限すべく、医療機器のウインドウズパーソナルFireWall機能にて接続制限を行う　という形になるのでしょうか? 基本的に、装置付属のOS設定は医療機器メーカーの領域であるため、ローカル管理者のパスワードもメーカーのみが知り得ており、設定自体をメーカーに有償で依頼する形になると想定されますが、そもそも設定自体を断られる可能性もあると思われます。そのあたりを調達時に仕様書縛りで設定を義務付けるという形になるのでしょうか?	ご指摘通り、古い医療機器では、Windows パーソナルFirewallで接続先を制限することが重要です。また、医療機器ベンダーによっても対応が異なると思いますが、「医療機器のサイバーセキュリティ 導入に関する手引書 （第2版） 」では、たとえサポート終了のレガシーな機器でも、「補完的対策を含む緩和策の提供」を病院に対して行うように求められています。なお、パーソナルFirewallの設定は、軽微なもので、かつ、通信相手のIPアドレスとポートを指定するだけですので、テストや検証といった高額な費用がかかるものではないと考えられます。高額な費用の見積があった場合は、その根拠を明確にするように求めることが良いと思います。 新規調達にあたっては、調達要件に、「医療機器のサイバーセキュリティ 導入に関する手引書 （第2版） 」に準じたサイバーセキュリティに関連する情報を提供すること、病院とベンダーの責任分界点を明確化すること等を入れ、相互の役割を明確化にするとよいと思います。 https://www.mhlw.go.jp/content/11120000/001094637.pdf
2	シン・テレワークシステムでなくsoftethertではダメでしょうかおなじIPA関連だと思いますが	シン・テレワークシステムはSoftEtherを改良したものですので、差し支えありません。
3	外部からのVPN接続強化の考え方、においてこの構成では院内から病院職員がサーバにRDPできないと思うのですが、病院職員はサーバにRDPすることはないのでしょうか？ もしくは病院職員も同様にインターネットからVPN経由でアクセスするのでしょうか？	病院内でサーバーにRDP接続する際にも、この踏み台サーバーを利用するのが理想です。これは、RDPの接続元を極力少なくしたいという考え方に基づきます。一方で、ベンダーからの接続が多い場合は、踏み台サーバーが混雑することが考えられますので、この場合は、院内専用の踏み台サーバーを別途設置し、ベンダー用踏み台サーバーと院内用踏み台サーバーからのみ、RDP接続できるように各サーバーで許可してはいかがでしょうか。サーバーがRDP接続できる箇所が増えれば増えるほど、攻撃の侵入口が増えることになりますので、その点に留意いただき、構成を検討されてください。
4	検体検査を外部に委託しているのですが、委託会社本社サーバーと常時接続したいというような場合は、委託会社専用の踏み台サーバを用意すればよいのでしょうか。	ご指摘のお考え方でよろしいと思います。
5	今回紹介のあったVPNの接続について、RDPには使えるということですが、内部システムからのメール通報等にも使えますでしょうか？またNTT東日本とあるが、NTT西日本管轄のエリアでも使えるのでしょうか？	シン・テレワークシステムはRDPに特化したものですので、RDP接続先のコンピュータでの電子メール等の操作は可能ですが、それ以外の用途には使用できません。また、エリアについてですが、NTT東日本とIPAと協力して配布しているもので、管轄や地域は関係なくご使用いただけます。
6	紹介されたいたVPN接続をする際、接続元 （家庭） 側で気を付けた方がよい事はなにかありますか。	ご家庭のPCのウイルス対策ソフトのエンジン、パターンを最新のものにしてご使用ください。なお、ご家庭のPCにファイルの転送等を行う際は、個人情報の漏洩にあたらないようご配慮ください。
7	病院側でリモート環境を構築、リモート接続希望業者側に提供できれば理想ですが、リモート接続業者側も、各社独自の仕様があり、難しいとの意見をよく聞きます。 実際に運用している病院、また、この環境を提供している業者があれば、お教え頂けますでしょうか。	現在、大阪急性期・総合医療センターでは、VPN接続の統一化を図るため、シン・テレワークシステム＋踏み台サーバーの構築を行っています。一部、ベンダー指定のVPN接続も存在していますが、極力、統一するよう、各ベンダーと交渉を行っておられます。 ベンダーのリモート接続システムを使用する場合は、ネットワーク機器の脆弱性対策の実施を求め、また、接続してくる端末の脆弱性対策、ウイルス対策ソフトのエンジン、パターンファイルの最新化などを求めるとともに、いつ、誰が、何の目的で接続したのかの報告を求め、責任分界点を明確化することが重要と考えます。また、接続の都度、ベンダーに接続申請をしてもらい、病院設置のネットワーク機器の電源をオンにし、接続終了後は電源をオフにするなどで、設定ミスなどに起因する攻撃を防ぐことができます。
資料・アーカイブ		
1	具体的に推奨する対策が示されていましたので、可能でありましたら推奨対策をまとめたものを配布願いたいです。	本事業終了時（年度末頃）に、公開予定です。 公開した際には、MISTサイト（ https://mhlw-training.saj.or.jp/ ）からお知らせいたします。
2	この研修に使われているパワーポイントの資料はダウンロードできますか。	
3	資料を開示してほしい。研修時の参考URLについて特に。	
4	２年後に電子カルテの導入を検討しています。他の職員はオンプレミス型が閉鎖網なので安全と考えていますが、複数のVPN接続が常態化しており、病院側でのセキュリティ対策の必要性について十分な理解を得られているように思えません。クラウド型のほうがデータ保護的な意味では安全なのではないかと考えていますが、採用例が少なくわかりやすい説得材料になりません。選択のヒントになるようなわかりやすいヒント、資料があれば助かります。	
5	今回の説明頂いた内容に関する資料提供は可能でしょうか？	
その他		
1	RDPの踏み台サーバに関する回答を有難うございました。 しかし、零細民間病院ではSEの数も少なく、万が一の場合にベンダー頼みとなりますので 複数ベンダーの協力が不可欠です。無料のシンテレワークシステムのような仕組みを、厚労省からベンダーに強制させるなどすれば、結果的に国民の医療を守ることになると思います。	貴重なご意見、ありがとうございました。