#	ご質問	回答
1	RD接続をポートを変更するという認識でよいのかを知りたい	RDPポートの変更は効果的な防御の一つですが、完全とはいえません。攻撃グループによっては、ポートをスキャンし、接続可能なRDPポートを調査する場合もあります。脆弱性対策、ウイルス対策ソフトの適用、長いパスワード、マイクロセグメントなどの多層防御の一環と捉えて頂ければと思います。
2	各サーバーのビルトインアドミニストレーターパスワードをそれぞれユニークな値に変更が必要ですが、サーバーは運用上ほとんどドメイン管理者権限を有するドメインユーザーでログオンして使っているのが大半です。ドメインユーザーのパスワードはAD内部で共通であり、この現状に対するアドバイスを頂けますと幸いです。	Administratorは周知のIDのため攻撃に悪用される最も危険なアカウントです。ドメインの場合の管理者に関する注意点は以下の通りです。 Administrator は使用しないで、yamada-admin、tanaka-admin などの管理者権限を使用したユーザーが判別できるIDを、Administratorsに登録して使用する。 Administratr のパスワードは20桁以上にしておき、ブルートフォース攻撃が不可能な状態にしておく。 定期的にSedcurity LogでAdministratorのログオンエラーがないか監査する（Event ID 4625）。この場合、院内のシステムがAdministratorを使用している場合が多々あることから、パスワード変更を行った場合は、すぐに切り戻しができるようにしておく。（エラーが発生したシステム側でのパスワードの変更が必要） 特定のAdministrators に所属するIDの使いまわしは絶対に避ける。 Administrators のメンバーの追加、削除やログオンエラーも定期的に監査する。（勤務時間外や、覚えのないログオンなど） Domain AdminsにはユーザーIを登録しない（Bulit-In Administratorの権限も取得してしまう）。 Administratorsのメンバーのパスワードが漏洩していないかを定期的に監査する → https://haveibeenpwned.com/Passwords
3	ウイルス対策としてはWindowsDefenderでも十分でしょうか	ウイルス対策ソフトの性能については、いくつかのテスト機関があり、これらの機関の評価を参照することをお勧めします。 https://www.av-comparatives.org/ https://www.av-test.org/en/antivirus/ https://selabs.uk/
その他		
1	BCPの内容が知りたかったのですが、2/5の内容なのでしょうか？	導入研修　大阪急性期・総合医療センター事例コース　第3回組織編でお届け予定です。
資料・アーカイブ		
1	手元に資料がないのですが、どこかで入手可能なのでしょうか。	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	MISTサイトには「※研修資料の事前配布はございません。」と記載がありますが、今回のスライドにはたびたび「配布資料未掲載」と表示がありました。研修資料は事前にどこかでダウンロードできたのでしょうか。 できたのならその場所を教えていただきたく、もしできなかったのなら、Zoomにログイン後など条件付きでもいいのでできるようにしてほしいです。 メモも取っていますが、資料がないと数日たって見直したいときに思い出せなかったりします。 その為現状、メモをとりつつ、画面キャプチャしつつ、聞き逃さないようにと忙しく、学習効率があまりよくありません。ご検討いただけると幸いです。	
3	講師の方が「事前にお配りした資料」と仰っていましたが、この研修シリーズで資料は一つも受け取っておりません。どこかで配布しているのでしょうか？	
4	本日のセミナー資料の入手方法を教えていただけますか？	