第2回システムセキュリティ管理者向け研修（Q&A）

令和5年2月2日に開催いたしました第2回システムセキュリティ管理者向け研修におけるQ＆Aについて、下記通り回答いたします。

#	質問	回答
1	(医療系の)システムによってはローカルadministrator権限が無いと動作しないとベンダに言われることがあります。レジストリキーやProgram Filesフォルダの一部アクセス権に手を入れることで解消することが多いのですが、ベンダ側の無知と怠慢を病院側に押し付けている現状だと、果たしてどこまでUsers権限で運用できるのかが疑問です。	研修に参加頂きありがとうございました。 ご指摘の点は、多くの方々から頂戴しており、疑問に思われるのもごもっともと思います。一方で、過去数年間のランサムウェアの被害を見ると、管理者権限を付与している組織が攻撃にあっています。システムの設計当時や導入当時とは、サイバー攻撃の状況が大きく変わったと言わざるを得ません。 当面、管理者権限の付与を行わざるを得ない場合は、外部からの侵入点を洗い出し、リモートデスクトップ接続の制限や、ネットワーク構成の変更、長いパスフレーズの採用などをご検討ください。 また、次期システム更新時には、管理者権限が不要なシステム導入をご検討下さい。
2	ビルトインadministratorを使わないように、とのお話ですが、別管理者アカウントを作成しても端末ごとにパスワードを変更しないと、万一乗っ取られた際、ラテラルムーブメントの餌食にならないでしょうか？	研修に参加頂きありがとうございました。 ご指摘の通りで、一台一台のビルトインAdministratorのパスワードをユニークにする必要があります。研修では触れませんでしたが、そのためのマイクロソフトからLocal Administrator Password Solution(LAPS) と呼ばれる無償ツールが提供されています。 https://msrc-blog.microsoft.com/2020/08/26/20200827_laps/ 日本語のLAPS導入ガイドが用意されていますので、是非、ご一読の上、導入のご検討をお願い致します。
3	電子署名については、オンライン接続での対応のなるのか？ローカルで構築できるのか知りたいです。	研修に参加頂きありがとうございました。 利用する電子証明書の発行元が、Comodoやデジサートなどの認証局発行の場合は、証明書が失効しているかを確認するため、インターネット接続が必要になります。従って、インターネット接続が可能な業務系のネットワークでの運用が前提になります。 一方で、Officeに付属している自己署名ツールを使用して署名が可能で、この場合、インターネット接続は不要です。以下のサイトで自己署名証明書での署名方法の解説がありますので、ご参照ください。 https://www.teijitaisya.com/vba-selfcert/
4	PowerShellの実行ポリシーをベンダに見せたいのですが、この資料はどこかからダウンロードできますか？	研修に参加頂きありがとうございました。 医療機関向けセキュリティ教育支援ポータルサイト https://mhlw-training.saj.or.jp/info-20230222/ にて公開しております。ご参考下さい。
5	ベンダーに対して様々なセキュリティ対策要件を交渉するということについて、医療機関が独自に動くことは、限界があると思います。本日のような内容を、もっと公開すべきでしょうし、全医療機関に共有すべきだと思います（本日の内容を理解できる医療施設担当者がどの程度おられるのか疑問ですが。少なくとも当院は皆無です）。同時に、ベンダーにも共有してもらえると助かります。	研修に参加頂きありがとうございました。 ご指摘の点は、2023年2月15日に開催された「医療機関におけるサイバーセキュリティ対策セミナー」において、厚生労働省から、「医療機関におけるサイバーセキュリティ対策の更なる強化策」(p3)で「①医療機関向けサイバーセキュリティ対策研修の充実 ②脆弱性が指摘されている機器の確実なアップデートの実施」が指摘されております。 https://mhlw-training.saj.or.jp/wp/wp-content/uploads/2023/02/01-mhlw.pdf 今後、厚生労働省を通じて、医療情報システムベンダー、医療機器ベンダーにも共有されると伺っております。
6	グループポリシーを一斉に変更可能はAD参加している場合の話でしょうか？	研修に参加頂きありがとうございました。 グループポリシーのリモートからの変更は、Active Directory (AD) に参加しているコンピュータが対象となります。AD に参加していない Wordk Group のコンピュータは、ローカル グループポリシーで設定を構成し、%Systemroot%¥System32¥GroupPolicy フォルダを他のコンピュータにコピーすることで配布が可能です。但し、アカウントポリシーとローカルポリシーはsecedit /exportコマンドで内容をエクスポートし、secedit /importコマンドでそれを別マシンにインポートする必要があります。出典： https://social.technet.microsoft.com/Forums/office/ja-JP/4848cad3-d2da-4d59-92c3-05d70b848c76/adpc?forum=windowsserver2008ja
7	レセプトの取下げをオンラインで実施するのに電カルにJavaをインストールする必要があり、Javaをインストールしてよいか検討しています。セキュリティ面で気を付けることはありますか。	研修に参加頂きありがとうございました。 まず、Java に限った話ではありませんが、脆弱性情報を取得すること、脆弱性がある場合は、アップデートできる環境を用意する必要があると思います。Windows、Java、JRE(Java のクライアント側実行環境）、.Net、Office、Acrobat など、皆様がご利用の OS、実行環境、アプリケーションは、インターネットに接続してアップデートすることを前提に作られています。ですので、アップデートが難しい環境の場合は、外部接続点を保護し、脅威が持ち込まれない環境を整備し、その上で、Java の導入をするとこが必要になります。この点で、アップデートの実施による、電子カルテシステムへの影響がないかの確認が必要となります。 また、社会保険診療報酬支払基金のレセプトのオンライン請求システムに係る安全対策の規程例（保険医療機関及び保険薬局用） では、「オンライン請求システムの送信機器は、オンライン請求業務（レセプト作成業務を含む。）のみに使用する。したがって、業務に必要とするソフトウェア以外のソフトウェアはインストールしない。」となっており、電子カルテシステム端末へのレセプトオンライン請求システムの導入はこれに違反します。 専用端末の導入をベンダーとご検討ください。 なお、以下は、Oracle社のリンクです。 https://docs.oracle.com/javase/jp/7/technotes/guides/jweb/client-security.html https://www.java.com/ja/download/help/expire_date_ja.html

#	質問	回答
8	話の前提はWindows　AD導入が前提なのでしょうか？診療所ベースの話ではむつかしいかと思います	研修に参加頂きありがとうございました。 技術的な内容ですので難解なものもあったと思いますが、高額なセキュリティ機器を導入しなくても、システムで対策できることが多々あることをご理解いただければと思います。
9	・以下のような「電子カルテシステム」の場合、その利用を禁止、紙カルテに戻せ、となりますか。 OSの「標準ユーザーでの運用」に関して、「管理者権限」ユーザーでの利用を前提としている。 パスワードの文字数が１０文字までなど、短い。ユーザーのパスワードを管理者であれば見ることができるようになっている。 OSやアプリのパッチをあてること（ゼロデイ攻撃も考慮して極力速やかに動作検証を行い更新、アップデートを行う）ができない、してもらっては困る。 ・厚生労働省など国の機関による「電子カルテシステム」の認定制度（構築まで含めて）を行う（規制強化）予定はありますか。 電子カルテシステムを利用者として選択する側からすると、認定された電子カルテシステムを、認定されたベンダー（SIer）から導入するというのが分かりやすいです。	研修に参加頂きありがとうございました。 利用禁止という事ではなく、厳重に保護する必要があると思います。感染経路となるネットワークの接続先で、電子メールや Web サイトの閲覧をしない、USB メモリの厳格運用を行う事が重要と考えます。
10	Administrator権限じゃないと動かないと云う医療情報システムは我々が団結して排除すべきでしょう。望ましいのは米国のHIPAA法のように医療情報システムのセキュリティルールを法的に決めることでしょう。	研修に参加頂きありがとうございました。 ご意見ありがとうございます。
11	マルウェア対策ソフトウェアの活用のお話が出ていますが、ネットワーク分離環境下でのエンジン及びパターンファイル更新の検討がなされていないと、既に使い物にならなくなった過去のバージョンのマルウェア対策ソフトウェアに頼ることになると思います。 半年前1年前のバージョンのマルウェア対策ソフトウェアの実効性には疑問が残ります。	研修に参加頂きありがとうございました。 ご指摘通り、半年前、1年前のパターンやエンジンでは有効性が低く、攻撃が成功しやすくなると思います。運用については導入ベンダーとご相談の上、少なくとも週数回は更新処理を実施頂ければと考えます。
12	内視鏡装置等の医療機器に接続するUSBはどうチェックすればよいでしょうか。	研修に参加頂きありがとうございました。 USB メモリ等を使用するのであれば、感染リスクがあるといえます。機器の構成変更が難しい場合は、技術編2回目でご紹介した「USB メモリ、ストレージ」の厳格な運用をご参考下さい。この際、異なる2種類のウイルス対策ソフトでスキャンすることが重要と考えております。
13	リムーバブルディスクの実行アクセス権拒否のお話がありました。暗号化機能付きUSBメモリの場合、USBメモリ内に存在するexeファイルを実行しないと、復号化できないのですが、問題ありませんでしょうか？	研修に参加頂きありがとうございました。 ご指摘通り、暗号化機能付きUSBメモリやアンチウイルスソフト内蔵USBメモリのうち、内蔵しているソフトウェアを実行するタイプのものでは、実行アクセス権の設定をするとソフトウェアが動作しません。一方で、パスワードボタンを搭載したUSBメモリの場合、ソフトウェアの実行が伴わないため、実行アクセス権を停止しても問題ありません。また、暗号化機能がないUSBメモリの場合、エクスプローラーでUSBメモリを右クリックし、「BitLoker を有効にする」で暗号化した場合、実行アクセス権の影響はありませんでした。
14	医療機器ベンダーにUSBの読み取り書き込みの不許可はできないといわれました。どう対応すればよいでしょうか。	研修に参加頂きありがとうございました。 医療機器でUSBの設定に制限がある場合は、物理的にUSB機器を挿せなくするための、USBコネクタ取り付け機器があります。この場合、データの転送はネットワークに限られますので、ルーター、Firewallの設定で、特定のサーバーにのみ接続できるようなルーティングを設定してはどうでしょうか。もし、ご質問の趣旨にあっていない場合は、再度お問い合わせください。
15	ランサム攻撃側が最初にバックアップを削除するとのことですが、VSSの削除程度の認識ですが、ArcserveやBackupExec等で取得したバックアップも削除されるのでしょうか？実際にされた事例はありますでしょうか？	研修に参加頂きありがとうございました。 はい、半田病院の場合、バックアップソフトでバックアップしたデータも暗号化されています。大阪急性期・総合医療センターも同様です。個々のPCはご指摘通りVSSが削除されます。厳重な注意が必要です。
16	管理者ユーザーは標準で「Administrator」のIDが設定されていると思うのですが、あえてそれは使えなくしないといけないということでしょうか。	研修に参加頂きありがとうございました。 はじめにセミナーのご説明が分かり難くお詫び申し上げます。お伝えしたかったのは、「使えなくしない」というよりも、「使わない」ことです。Administrator を管理アカウントとして使用すると、正規の行為なのか、攻撃なのかの区別がつきにくくなるためです。ある時点から　Admonistrator を使用しないとすれば、それ以降、 Administrator でのログオン成功や失敗は、攻撃とみなすことができます。また、Administrator のパスワードを十分に長い、例えば20桁程度に設定することができれば、総当たり攻撃の可能性を限りなく低くすることが可能となります。
17	USBメモリの暗号化は、WINDOWSの標準機能のものでも有効ですか。	研修に参加頂きありがとうございました。 「Windows標準機能」とは BitLocker かと思いますが、問題ありません。
18	LTOテープドライブのマガジンに複数のテープを挿入し、バックアップを実施する際にのみマウントして書込をしております。マウントしていないテープをオフラインバックアップと見なすことはできますでしょうか？	研修に参加頂きありがとうございました。 マウントしていないテープはオフラインバックアップとみなせます。ただし、マウント中に攻撃された場合に備えて、世代管理やライトワンスの採用等をご検討ください。
19	厚労省のシステムのガイダンス（ガイドライン）で最低限ラインに謳い、実装していない電カル・部門システムは販売・稼働不可にすればよい。システム承認は、PAMDや医療安全評価機構の仕事とすべき（個別の医療機関が行うと裁量の差がでる）	研修に参加頂きありがとうございました。 ご意見ありがとうございました。
20	大阪急性期は4日前の電子カルテのバックアップがあったそうですが、復旧には２か月かかりましたよね。おそらく、電子カルテのバックアップはあったが、連動する部門システムがなかったのではないかと推測しています。システム単体のバックアップがあったとしてもHIS全体のバックアップがなければ不十分だと思います。（じゃあどうしろと言われると答えを持ち合わせていませんが…）	研修に参加頂きありがとうございました。 ご指摘通り、部門システムはバックアップのないものもあり、全体の復旧に時間がかかりました。 完全性、真正性を担保するには、部門システムを含めた、オフラインバックアップやライトワンスのバックアップが重要と思います。

#	質問	回答
21	本日、あるベンダーと会話した際に、新規導入システムに対してセキュリティ対策ソフトを導入したい旨を伝えると「システムの動作保証はできないため、病院側で判断してください」といった話がありました。これが現実です。病院側が主導権をもって対応したとしても、ベンダーの意識を変えてもらえないのであればと思った次第です。CRYPTRECについてもなかなか理解してもらえなかったです。各医療機関が奮起するしかない現実であることもご理解いただけると幸いです。	研修に参加頂きありがとうございました。 ご指摘の状況は、十分に理解しており、大阪急性期・総合医療センターの復旧では、ウイルス対策ソフトの導入をすべてのベンダー(100社以上）に要求し、実現しております。皆様のみならず国全体がベンダーに要求し続けることで、ベンダーの意識も変わってくることを期待しております。
22	当院のベンダーはPC起動後、自動ログイン設定を行っています。PCの基本操作のユーザ特定がそもそもできませんがこのようなところは多いと思います。もちろんAdmin権限がないと業務アプリが動かない設計です。	研修に参加頂きありがとうございました。 大変恐縮ですが、ご利用のシステムと現在のサイバー攻撃の現状を考えますと、安全ではないといえます。外部からの侵入口となる VPN 装置や、リモート保守機器の脆弱性を管理すること、USB メモリの厳格な運用を図ること、電子メールやWebサイトの閲覧は HIS 系ネットワークに接続している端末では行わないこと等をご検討ください。
23	今回の資料をダウンロードできるようにしてもらいたいです。	研修に参加頂きありがとうございました。 医療機関向けセキュリティ教育支援ポータルサイト https://mhlw-training.saj.or.jp/info-20230222/ にて公開しております。ご参考下さい。
24	おそらくこの辺りのADの設計やGPOの深い話をしても理解できる電カルベンダは圧倒的に少ないのが現実です。病院側のシステム管理者がADについてベンダに教授したり、自院電カル環境のGPOの設計や構築を病院の担当者が行っているような状況です。	研修に参加頂きありがとうございました。 ご指摘の状況は多々あると実感しております。一方で、皆様のような研修にご参加下さるシステム管理者の方々を増やしていくことが、ベンダーの意識改善につながると思います。引き続き、よろしくお願い申し上げます。
25	運用や設定でセキュリティレベルが上がるものはまだしも、HSMでの暗号化など相当コストがかかるものもあるように感じますが、この物価高騰の中、診療報酬が上がるわけでもなく、現実的に、経営から投資の承認がおりないものもあります。 現実的に何から始めるべきか（何が最も大事か）教えて下さい。	研修に参加頂きありがとうございました。 ランサムウェア攻撃に限って言えば、外部接続をしている機器の脆弱性管理ではないでしょうか。他のランサムウェア攻撃を受けた組織をみると、機器の脆弱性管理を行っていないという共通点が見えてきます。また、外部接続するベンダーには、接続元IPアドレス制限を求めて下さい。 さらに、初期侵入では総当たり攻撃を行うため、リモートデスクトップ接続のロックアウトが重要となります。
26	セキュリティ対策ソフトをインストールすると、介護系システムが動作しなくなりました。ベンダーに相談したところ、「特定のフォルダ、ファイルに関して、セキュリティソフトで検索対象から外してください。」と言われて設定しておりますが、これが脆弱性の一つにはなるのではないかと思うのですが、どうなのでしょうか。	研修に参加頂きありがとうございました。 特定のフォルダ、ファイルを除外設定することは、一般的にもあると思います。ただし、セキュリティ対策ソフトが誤検知するということは、ウイルスが悪用するテクノロジーを利用している可能性が高いと思われます。 防御実効性を高めるため、ウイルスが侵入してくる経路を考えてみます。 ウイルス感染の恐れがある経路は、概ねファイル共有やUSBメモリとなります。USBメモリは除外されていませんので、検出可能で問題はありません。一方で、ファイル共有が除外設定の中に入ってくる場合は感染リスクが高まりますので、接続元の侵入経路となる電子メールやWeb閲覧を制限する必要が出てきます。
27	本日ご講演いただいた内容は非常に専門的な内容であり、病院にセキュリティの専門家がいないと、ベンダとの交渉・状況確認も難しいと思います。各病院に情報処理安全確保支援士の設置を必須とさせるよう、国から働きかけていただけないでしょうか。	研修に参加頂きありがとうございました。 実際の設定変更や構成を行わずとも、Windows を初期値のままで使用するのは安全ではないということをご理解いただければと思います。
28	RDPの待ち受けポート変更の話がありましたが、nmap叩けばものの数分なので、あまり実効性に疑問がありますが(しかも変更後のポート番号も院内全端末共通。。。)	研修に参加頂きありがとうございました。 当方の環境ではすべてのポートをスキャンする場合、1台あたり2分40秒かかりました。さて、過去のランサムウェア事案をみると、初期侵入でVPN装置の脆弱性を悪用された場合は、ネットワークの構成を攻撃側が推定しやすくなりますので、効果が薄くなるかもしれません。しかし、初期侵入に手間取らせることは、攻撃側にとってリスクが高くなるため、撤退の可能性も期待できます。
29	Administratorでインストールしており、変更すると動かないソフトがあるので、変更できないといわれました。どう対応すればよいでしょうか。	研修に参加頂きありがとうございました。 ご説明申し上げました通り、Administrator で動作しているシステムにウイルスが混入すると大変危険です。USB メモリの厳格運用や、ファイル共有の共有先を限定するなど、外部からの混入する可能性の高い経路を特定して、電子メールや Web サイトの閲覧をしない、ウイルス対策ソフトの稼働などをご検討ください。次期更改では、仕様として「管理者権限が不要なこと」等をご検討ください。
30	マクロについては、行政からマクロ付エクセルで調査回答などを求められることが多くあります。医療機関もですが、行政などももっと真摯に検討していただきたいです。	研修に参加頂きありがとうございました。 ご意見ありがとうございます。
31	今回のGPO設定はドメインサーバだけでいいのですか？	研修に参加頂きありがとうございました。 ロックアウト設定などの認証強化は、Default Domain Policy と Default Domain Controllers Policy に適用頂きたいと思います。Excel などのアプリケーション関連は Default Domain Policy でよろしいと思います。
32	本日ご講演いただいた内容は専門的な内容であり、専門のSEでなければ理解はできないのではないでしょうか？どちらかといえばベンダに向けて発信すべき内容かと思います。	研修に参加頂きありがとうございました。 技術的な内容ですので難解なものもあったと思いますが、高額なセキュリティ機器を導入しなくても、システムで対策できることが多々あることをご理解いただければと思います。