第4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16日に開催いたしました第4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	インターネットに接続されていない環境で、どのようにしてリアルタイムかつ、現実的な運用でウイルス対策ソフトのエンジンやパターンを更新するのか教えて頂きたい。 (インターネット接続環境からアップデートやパターンファイルを単体でダウンロードして配信する、という作業を日に何度も土日祝日問わず毎日することが現実的にできるのか)	研修にご参加いただきありがとうございます。 多くのウイルス対策ソフトは、閉域網側とインターネット接続が可能な網側にパターン配付サーバーを設置し、USBやパーソナルファイアーウォールを設定したネットワークでパターンファイルやエンジンを更新する仕組みを持っています。導入ベンダーにご相談ください。
2	システム担当者見習いです。Windowsサーバーを触ったことがありません。業務で使用するサーバーではなく、個人でサーバーを用意して、構築や運用、保守の練習してみたいと思うのですが、なにかよい方法はありますでしょうか。レンタルサーバーなどの利用をかんがえてはいます。	研修に参加頂きありがとうございました。 レンタルサーバーを利用する際の目安としては、メモリを4GByte以上、確保すると動作がスムーズです。レンタルサーバーへの接続は、リモートデスクトップ接続で行います。この際、ご自宅のネットワークのIPアドレスが固定でないと、どこからでも接続ができてしまうため、攻撃される恐れがあります。できれば、ご自宅のIPアドレスを固定IPにして、レンタルサーバー側で指定したIPアドレス以外は接続できないように設定する必要があります。 Windows10/11 と違って、サーバーにはサーバー独自の機能が備わっています。基本的なサーバー機能として、Active Directoryユーザーとコンピュータ、DNS、DHCP、グループポリシーの管理などがあり、またWebサーバーとして機能するIISやWindows Update Service他、多数の機能が搭載されています。そのため、まず、ユーザーやコンピュータを管理するためのActive Directoryの入門書で、ある程度、機能や役割、サーバーとクライアントの関係を把握してからレンタルサーバーを申し込むのが効率的と思います。Windows Server 2008を対象とした解説BlogがASCIIで公開されています。 https://ascii.jp/serialarticles/492317/ 古いな、と思われるかもしれませんが、基本的な機能に大きな違いはありません。インターフェースのデザインが異なったり、機能強化はされていますが、基本は同じで、用語に大きな変わりはありません。イメージを掴むために、一度、ご覧になることをお勧めします。
3	攻撃ツールを利用すればイベントログの消去ができるため、イベントログのサイズ見直しだけでなく、最低限、ログ転送は必要では？	研修に参加頂きありがとうございました。 ご指摘通り、イベントログの転送は重要と思います。ただし、イベントログを消去しない攻撃もあり、基本設定としてサイズや上書きの見直しをご紹介しました。環境が許せば、Windows サーバーの転送のご設定をお勧めいたします。
4	ADのログは、Cドライブ以外のログに保存しても問題ないでしょうか？	研修に参加頂きありがとうございました。 まったく問題ありませんが、イベントログを保存するフォルダーのアクセス権の設定等が必要になります。この設定が適切でないと、攻撃者にログ消去を許す等の危険性が高まります。以下のサイトをご参照ください。（管理者権限が必要です） https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/application-management/move-event-viewer-log-files
5	windowsのログはかなり容量を使用する為、どの程度のサイズを確保してよいか試行錯誤しています。現状、定期的にタスクスケジューラでコマンドを実行して外部媒体に出力してます。特にファイル共有サーバはログの発生件数がかなり多く、長期確保するログを絞りこみたいと考えています。特に重点的に抽出すべきものを教え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。 まず、イベントビューワーの[Windows ログ]配下のApplication、セキュリティ、システム、Setupは必須です。次にインシデントを想定して重要と考えられるのが、[アプリケーションとサービスログ]>[Microsoft]>[Windows]配下のWindows PowerShell もしくは Microsoft-Windows-PowerShell/Operational Microsoft-Windows-DeviceSetupManager/Admin Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational Microsoft-Windows-TerminalServices-LocalSessionManager/Operational Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational Microsoft-Windows-TerminalServices-RDPClient/Operational (TERMINALServices-ClientActiveXCore) Microsoft-Windows-Windows Defender/Operational Microsoft-Windows-WinRM/Operational (Windows Remote Management) などが重要です。また、グループポリシーの[監査ポリシーの詳細な設定]を設定する必要があります。以下のサイトをご参考下さい。 https://www.softwareisac.jp/ipa/index.php?%E3%83%BBL1+%E7%9B%A3%E6%9F%BB%E3%83%9D%E3%83%AA%E3%82%B7%E3%83%BC%E3%81%AE%E8%A9%B3%E7%B4%B0%E3%81%AA%E6%A7%8B%E6%88%90

#	質問	回答
6	そもそもAD導入していないときはどうするのだろうか？ AD前提となっているのはどうなのだろうか？	研修に参加頂きありがとうございました。 まず、Windowsのセキュリティ機能は、Active Directory(AD)の配下にある・ないに関わらず、ほぼ同等です。AD は、グループポリシーを使ってセキュリティ設定をリモートで適用させる機能を持っていますが、WorkGroupでもポリシーファイルをそれぞれにコピーすることで同等のことを実現できます。以下のサイトをご参考下さい。 https://social.technet.microsoft.com/Forums/ja-JP/f4e3f22b-6859-4509-a428-df04047692ab/windows10?forum=win10itprogeneralJP
7	ログの設定については理解できたが、対象の全マシンのログを人間が目視でチェックするのか？フィルタで絞り込むとしても、手動で毎日チェックが継続できるとは思えない。タスクスケジューラでPowerShellスクリプトなどを回して、ログ検査から異常通知までを自動化する方法など、もう少し現実的な方法を教えて欲しい。	研修に参加頂きありがとうございました。 まず、Active Directory環境であるならば、ドメインコントローラーのセキュリティログの監視で、相当の分析が可能です。クライアントのログオン失敗も、ドメインコントローラーに記録されますので、日常的にはイベントビューワーでログオン失敗(4625)等を絞り込むだけでもよろしいかと思います。 一方で、異常のレベルにもよりますが、複合的なログ監査には、PowerShellではなく、専用ツールであるLogPaserのご利用が適していると思います。 https://www.microsoft.com/ja-jp/download/details.aspx?id=24659 https://codezine.jp/article/detail/540 https://atmarkit.itmedia.co.jp/ait/articles/0610/27/news140.html 詳細な使用方法については、今後、ホームページ等で公開していきたいと思います。
8	そもそも端末内にデータを置いていること自体、論外では？ ※端末が盗難されたらそれだけでインシデント	研修に参加頂きありがとうございました。 システムの特性によって、端末にデータを置くケースもあり、一概にはいえない部分もあるかと思います。しかし、端末盗難は重要なご指摘かと思います。データを端末に保存する際は、Windows標準搭載のBitLockerなどのディスク暗号化機能や、漏洩に備えて個人情報の暗号化などもご検討頂ければと思います。
9	そろそろ閉域網の安全神話だけでなく、HISをインターネットに接続して、よりセキュリティを高めることについて議論をするときに来ていると思う。当法人では法人内各施設全体で数千台の電子カルテ端末や数百台のサーバがあるが、全てインターネットに接続しており、10年以上運用しているが、小さなインシデントはあれど、法人の存続に関わるような大きなセキュリティインシデントが発生したことはない。たまたま運が良かっただけ、と言えるかもしれないが、インターネットに接続していることで、OSやミドルウェアのパッチ適用の迅速化、アンチマルウェアプロダクトのエンジンやパターンファイルのリアルタイムな最新化、クラウドベースのEDRやSIEMの活用など、下手な閉域環境よりもセキュアな環境を実現していると自負している。VPN接続の存在もさることながら、外部からの画像CDの持ち込みや、外注検査会社や学会等からの外部USBメモリの接続、システムベンダからの電子カルテや部門システムの更新のためのアップデートファイルの持ち込みなど、ただインターネット以外にもマルウェアの侵入経路はいくらでも存在しているし、無くすことはできない。 StuxnetやDuquのように、完全にインターネットから遮断された環境に対してもマルウェアによるサイバー攻撃が可能なことは既に10年以上前に証明されている。 セキュリティの素人の病院職員がインターネット分離をしただけで思考停止して、何もしていない閉域環境よりも、インターネットを活用して、よりセキュアにすることを業界全体で真剣に考える時期に来ているのではないだろうか。	研修に参加頂きありがとうございました。 重要なご指摘と思います。ご指摘は今後の参考とさせていただきます。
10	現在保有するノートパソコンのほとんどは無線接続を行っています。ウィルス感染発生時において、有線であれば抜線すればいいと思いますが、無線接続の場合はどういった対処をすればいいでしょうか。特に夜間休日などに発生した場合、現場スタッフでも応急的にできる対応があれば教えていただきたい。	研修に参加頂きありがとうございました。 通常、Note PCの場合は、機内モードのスイッチもしくはファンクションキー（FNと刻印されているキー）を押しながら無線（Wi-Fi、Bluetooth等）を停止する機能がありますので、こちらを使用するとよろしいかと思います。 また、無線LAN APもしくはコントローラーの有線接続を極力集約しておき、院内LAN接続部分を抜線することも重要と考えます。 ファンクションキーの割り当てがないデスクトップ等の場合の操作方法は、以下のサイトをご参照ください。 https://support.microsoft.com/ja-jp/windows/%E6%A9%9F%E5%86%85%E3%83%A2%E3%83%BC%E3%83%89%E3%81%AE%E3%82%AA%E3%83%B3%E3%81%A8%E3%82%AA%E3%83%95%E3%82%92%E5%88%87%E3%82%8A%E6%9B%BF%E3%81%88%E3%82%8B-f2c2e0a1-706f-ff26-c4b2-4a37f9796df1#:~:text=%E6%A9%9F%E5%86%85%E3%83%A2%E3%83%BC%E3%83%89%E3%82%92%E5%88%A9%E7%94%A8%E3%81%99%E3%82%8B%E3%81%A8,(NFC)%20%E3%81%AA%E3%81%A9%E3%81%8C%E3%81%82%E3%82%8A%E3%81%BE%E3%81%99%E3%80%82 また、夜間等でスタッフの負担が大きいと判断される場合は、クライアントに限っては、シャットダウンもやむを得ないと考えます。

#	質問	回答
11	シャットダウンせずにネットワーク切断という部分について、有線LANは簡単に抜けても、無線LANを完全にOFFすることは、現場利用者にそれをお願いすることは難しいケースがあると思います(特にITに疎い人)。やり方を周知徹底をするにも、特に医師は頻繁に入れ替わるため、徹底は難しいです。そういう場合は、後でフォレンジックできないリスクよりも感染拡大のリスクの方が重要と思うので、クライアントに限りシャットダウン対応を取ることはよろしくないでしょうか。	研修に参加頂きありがとうございました。 クライアントに限って言えば、ご指摘の「後でフォレンジックできないリスクよりも感染拡大のリスクの方が重要」という選択肢は正しいと思います。
12	そもそも原因究明よりも、被蓋封じ込めや早期復旧が再優先では？	研修に参加頂きありがとうございました。 ランサムウェアでの課題は、侵入当初は人間が様々な情報を窃取したり、ネットワーク構成を調査するという点にあります。攻撃された時点で、院内LANの構成やID、パスワードなどの資格情報もすべて窃取されると考えて行動しなければなりません。バックドアやVPNソフトを設置することもあり、一旦、封じ込めに成功したように見えても、攻撃が継続していたという事例は多数あります。 従って、ネットワークの抜線をしたあとは、専門家による侵入経路の特定や、ウイルスの確保、これらの分析による再攻撃の可能性を潰す必要があります。復旧作業に入った時点で、再び攻撃されないように原因究明が必要と考えております。
13	これは大阪急性期規模の組織を想定しているのでしょうか？？	研修に参加頂きありがとうございました。今回の研修コンテンツは幅広く医療機関を想定して作成しております。ほかにも対象医療機関をわかりやすく設定する等のご指摘をいただいていますので、今後の参考とさせていただきます。
14	あまりにもやることが多すぎて実現困難に感じられます。大切だとわかっていても人手もない現状で現実味が感じられません。	研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。
15	１００床２００床規模の組織では人物金の面でかなり現実的ではないかと思いますが	研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。
16	無線LANの場合のLAN切り離し方法でITに疎い人でも対応する方法はありますか？	研修に参加頂きありがとうございました。 問10をご参照ください。
17	メール添付の不審なファイルを開いてしまった等というときはネットワークから遮断したうえでウィルス対策ソフトで	研修に参加頂きありがとうございました。 メール添付の不審なファイルを開いた場合は、LAN抜線、若しくは無線LANを停止し、ウイルス対策ソフトでの完全スキャンも手段としては有効です。但し、パターンファイルやエンジンが最新に更新されていることが前提になります。 また、そのような環境ではない場合は、USBメモリ型のウイルス検索ツールを使用し、感染していない端末でパターンとエンジンを更新して、感染端末にツールを接続し、ウイルスチェックをするという方法も考えられます。
18	無線LANの場合、機種にも寄りますが、	（下の枠に集約） 研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。
19	無線LANの場合、機種にも寄りますが、物理的なON・OFFスイッチが付いているものもあります。	
20	都度、セキュリティベンダーとの連携が提示されていますが、ほとんどの病院がそのようなベンダとは契約していない、存在を知らないと思われます。	研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。
21	続き　どのようなベンダがあるか教え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。 日本ネットワークセキュリティ協会のサイバーインシデント緊急対応企業一覧をご参考下さい。 https://www.jnsa.org/emergency_response/
22	セキュリティベンダーとは具体的に誰を指すのか。 例えばどのような会社の人でしょうか？	研修に参加頂きありがとうございました。 問25をご参考下さい。
23	メール添付の不審なファイルを開いてしまった等というときはネットワークから遮断したうえでウィルス対策ソフトでフルスキャンというのも現実的な行動ではないかと思うので、一概にフルスキャン禁止と考えていませんがそれでよいでしょうか	研修に参加頂きありがとうございました。 問23をご参考下さい。
24	セキュリティベンダとは万一の際に即日対応してくれるような契約を事前にしておくのか？	研修に参加頂きありがとうございました。 セキュリティベンダーにもよりますが、事前契約なしに24時間365日受付というベンダーもあります。日本ネットワークセキュリティ協会のサイバーインシデント緊急対応企業一覧をご参考下さい。 https://www.jnsa.org/emergency_response/
25	中小規模の病院は、専任のSEがいない現状も多くあると思います。理想論としては理解できますが、現実としては無理があります。もっと医療機関の現実を踏まえた内容と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。
26	病院職員の人的リソースの問題がたびたび上がるが、病院経営者側も、最低限、情報処理安全確保支援士か、CISSP程度のレベルの人間を相応の報酬で雇用することを真剣に考えるべき。 (しなくてもいいけど、やらないとそのうち自院がやられるだけ)	研修に参加頂きありがとうございました。

#	質問	回答
27	復旧業者とのトラブルとは？	研修に参加頂きありがとうございました。 例えば、一部分だけでも復旧できたのと、全部が復旧できたのでは、大きな違いがあると思います。一部分でも復旧できたので高額な請求を行う事業者が存在しており、注意が必要です。
28	「ではどうすれば守れますか」と聞いても、ベンダ側の意識・レベルが低く、対案が出てこない。	研修に参加頂きありがとうございました。 残念ながら、一部、そのようなベンダーが存在していることは承知しておりますが、皆様方がセキュリティレベルの向上を、ベンダーに要求し続けることが重要と考えております。お困りの際は、改めてお問い合わせください。
29	事前や事後に何をするかだけでなく、何人必要だと公に発信してもらえれば、各病院もやりやすいと思います。	研修に参加頂きありがとうございました。 ご指摘は今後の参考にさせて頂きます。
30	非常に重要な講演内容であった一方、過去の回の資料や、Q&Aが未だに公開されていないのが非常に残念です。	研修にご参加いただきありがとうございます。 システム・セキュリティ管理者向け研修 e-learningのサイト(MinaSecure) よりログインしてダンロードください。 ※1：システム・セキュリティ管理者向け研修 e-learning受講申込みが未だの方は、受講申込の上、ダウンロードください。 ※2：共通研修のログインID/パスワードではダウンロードできません。 システム・セキュリティ管理者向け研修 e-learning受講申込は下記URLより申込ください。 https://www.saj.or.jp/form_agree/mist_e-learning-sys.html
31	被害に遭ったら多大なコストがかかることはもちろんで、またその対策を様々行うにはまたコストもかかることも当然です。さて、ではそのコストをどこで補填するのでしょうか。ただでさえ医療は人件費比率が高く赤字体質も多く、ベンダーも機能しない。しかし責任は医療機関がとらされる。そして赤字ではセキュリティ投資もできない。薬価は下がり続ける一方給料のボトムアップもしろと。物価高もあり電気代もうなぎ登り、しかし診療報酬は下がる。これでどうすればいいのか、厚労省としてどうお考えなのかお教え願いたいです。	研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。
32	P.58 確認用USBメモリとはどんなものでしょうか？	研修に参加頂きありがとうございました。 ご説明が不足しており申し訳ありません。ランサムウェアの場合、復旧に取り掛かる際にUSBデバイス等を接続しアプリケーションをインストールするなどがありますが、ウイルスが稼働中の場合は、接続したデバイスを暗号化されてしまうケースがあります。そのため、テキストファイルを保存したUSBメモリを用意し、被害PC/サーバーに接続し、テキストファイルが暗号化されないかを確認する必要があります。
33	中小の病院には無理です。病院から声をあげてというのは正直効果が期待できない。せめて中小の病院が使うシステムについては行政からベンダーに直接要請して担保するような方向にしてほしい。	研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。
34	LinuxやMacの対策についても教え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。 ご指摘いただいた点は今後の研修内容策定の参考とさせていただきます。
35	年度末の予算消化ではなくて、次年度も続け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。 次年度も同様の事業が計画されております。詳細が決まり次第、ご案内させて頂きます。
36	ウィルスにかかったときに補償される、損害保険はありますか？	研修に参加頂きありがとうございました。 はい、あります。以下のサイト(日本損害保険協会) をご参照ください。ウイルス被害は補償されますが、日本の損保会社はランサムウェアの身代金の支払いには応じてくれませんので、ご注意ください。
37	監査・機能評価などで、システム観点の内容が非常に薄いと感じます。もっと監査や機能評価内でのシステム観点の項目や調査に時間を割り当てていただくよう、国にも動いていただきたい。	研修に参加頂きありがとうございました。 ご指摘いただいた点は今後の研修内容策定の参考とさせていただきます。
38	ここまでの対応できる人材は医療機関ではなくベンダーで働いたほうがよいと思います	研修に参加頂きありがとうございました。ご指摘は今後の参考とさせていただきます。