第1回システムセキュリティ管理者向け研修（Q&A）

令和5年1月26日に開催いたしました第1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	実際に支払ったケースは有るのでしょうか？その際、数回要求されたのでしょうか？	研修に参加頂きありがとうございました。 米国の東海岸の燃料の45%を担っているパイプライン会社「コロニアルパイプライン」では、身代金440万ドルの支払いを行っています。 https://cloud.watch.impress.co.jp/docs/topic/special/1332396.html 調査によると、日本でランサムウエア攻撃に遭ったと回答した70組織のうち、身代金を支払ったと回答したのは11.4%（8社）あるそうです。 https://xtech.nikkei.com/atcl/nxt/column/18/00001/07178/ 別の2021年の調査では、ランサム被害にあった組織の20%が身代金の支払いに応じたと公表されています。 https://scan.netsecurity.ne.jp/article/2022/04/14/47464.html
2	ランサムウェアがファイル探索を行うときは、どのようなプロトコルを利用しているのでしょうか？SMB？	研修に参加頂きありがとうございました。 一般的にはWindowsのファイル共有プロトコルSMB（サーバーメッセージブロック）を使用しています。SMBでファイル共有されているフォルダーをリスト化し、暗号化を実行しますので、端末などで不用意にファイル共有を行っていると、その共有フォルダも暗号化されますので、注意が必要です。
3	バックアップをオンライン上の改ざん防止領域に取る事は有益でしょうか？それともやはりオフラインが必須でしょうか？	研修に参加頂きありがとうございました。 確実に改ざんされない、ということが論理的に証明できれば、オフラインバックアップは不要です。バックアップシステムを提供しているベンダーに、改ざん防止のロジックの説明を求めることが大切です。 一方で、バックアップシステムが稼働しているサーバーや仮想基盤が暗号化されると、復旧が不可能になります。 こうしたリスクを念頭に、オフラインバックアップの必要性についてご検討ください。
4	アイルランドの事例ではＥＤＲ/ＮＤＲは導入していなかったのでしょうか？	研修に参加頂きありがとうございました。 2021/5/13にアイルランド保健省(DoH)は、他の病院の状況から攻撃の可能性を予見し、EDRを急遽導入し、5/14の攻撃を免れていましたが、他の病院では、予兆に対して具体的な調査などを行わなかった、また、調査はしたが侵入元を誤って判断するなどがあり、5/14 に6病院と本部、データセンターが被害にあっています。これらでは、ウイルス対策ソフトは稼働していたものの、セグメント化されていないフラットなネットワーク構成と、管理者権限の付与などがあり広範な被害を招いた原因とされています。
5	バックアップデータの健全性について、おききします。バックアップしたデータの中に、長期潜伏型のランサムウェがいた場合、検出する手立てはありますか？バックアップデータの健全性をどのようにして検証・実現するのでしょうか？	研修に参加頂きありがとうございました。 VPN経由でネットワークに侵入した場合を考えてみます。この場合、パスワードが外部に漏れていなければ、総当たり攻撃を実施するため、Securityログにログオン失敗（EventID4625）が多数検出されます。従って、イベントログを上書き保存せずにアーカイブ設定し、過去に遡って侵害の形跡を調査することで、バックアップデータの完全性を確認することができます。また、VPN装置のSyslogを調べ、海外のIPアドレスからの接続や、過去に接続されていないIPアドレスを調査することで、最初の侵入時点を特定することが可能です。これらの証跡を確実に保管することで、健全性を検証することが可能となります。ログは定期的にBlu-rayやテープにバックアップし、改善を防ぐことが必要です。 また、長期間の潜伏があることから、バックアップはシステムの特性にあわせて、日次、週次、月次での世代管理をする必要があると思います。
6	ネットワーク監視を行うことでランサムウェアの感染を検知することはできるのでしょうか。	研修に参加頂きありがとうございました。 VPN、クラウドからの初期侵入の場合、多くはリモートデスクトップ（RDP)を使用しますので、業務で接続した以外のRDPは異常として検知することが可能です。また、SMB接続のログオンを長期間実施する場合があります。Securityログのアカウントが正常にログオンしました。（EventID 4624）のログオンタイプ 3 はSMB接続を行った際に出現します。これらから、システムのファイル共有以外の接続を除き、勤務していないIDからのSMB接続のログオン成功などで検知は可能です。LogParser などのツールを使うと効率的に調べることが可能です。 また、ネットワーク監視の場合は、サーバーやバックアップのあるセグメントへの RDPやSMBの時間外通信を監視することで検知が可能ですが、正規/非正規の通信の判定が難しいと考えられます。理想的には、ネットワーク監視とSecurityログを組み合わせて判断するのが望ましいと考えます。
7	冒頭付近のスライドで、パブリッククラウドのIPを偽装して侵入というようなものがあったかと思いますが、MSのようなメジャーなサービス提供者であってもそのような形で乗っ取りもありうるでしょうか	研修に参加頂きありがとうございました。 どのようなクラウドサービスでも、ユーザーIDやパスワードが「推測しやすいもの」であれば侵入される可能性があります。クラウド上に公開されてパブリックIPアドレスに対して、接続元IPアドレスと接続可能なポートを制限することが重要と思います。

#	質問	回答
8	ウェブメールのみの利用下でも、エモテットに感染すると自動的にメールは送信されてしまいますか？ IP接続制限がされているため、外部からの送信は出来ない想定です	研修に参加頂きありがとうございました。 EmotetはMicrosoft のメールクライアントソフトであるOutlookや、Mozilla Thunderbird のアドレス帳を窃取することが確認されています。現時点では、Web メールのアドレス帳窃取は確認されていません。現時点で、アドレス帳窃取という意味では、Webメールは安全かもしれませんが、Emotet感染被害を軽減するということではありませんので、ご注意頂きたいと思います。
9	EDR製品の有効性はどうでしょうか？	研修に参加頂きありがとうございました。 EDR（Endopoint Detection & Redaction：端末等でのソフトウェアの振る舞いを分析し、検知・対処するソフトウェア）については、一定の効果があると考えています。一方で、侵入後の振る舞いや様々なセキュリティイベントに基づき実行阻止や通信遮断を行う事から、VPN経由でRDP接続＋総当たり攻撃のような人為的な初期侵入については、検出しない場合があり、Software ISACの検証でも未検出のケースを確認しています。また、大量の情報をコピーされ窃取されたとしても、一般的な行為とみなされると、阻止できない場合があります。 そのため、EDRが発信するログを、人間が詳細に分析することで、そうした行動の正否を判断する必要が出てきます。この場合、24/365の監視となり、相当なコストがかかります。 他方、総当たり攻撃はロックアウト設定で防げるため、次回以降、解説するWindowsやネットワークの設定を正しく行う事で、EDRがより効果的に機能するのではないかと考えております。
10	HIS系ネットワークは閉鎖されていることから、ベンダーが電子カルテ端末のWindowsバージョンのアップグレードやWindowsUpdateを実施しないのですが、これは不適切なのでしょうか？	研修に参加頂きありがとうございました。 バージョンアップやアップグレードを行っていないことが「不適切」というよりも、それだけリスクが高いということだと思います。WindowsやOffice、Chrome、Edgeなどは、インターネットに接続してアップデートすることで、脆弱性を修正することが前提です。従って、これらのアップデートが困難な場合は、それ相応の外部からの侵入を厳密に制限する必要があります。 一方で、保守用の外部接続が存在することから、完全な閉域網の維持ができない状況にあります。また、USBメモリの不適切な使用などの利用者の不手際もあり得ることから、アップデートによる脆弱性の改修は重要といえます。 ランサムウェアは近年活発になってきた脅威であり、多くのシステムは、この脅威を前提とせず設計されたものが多いと思います。新たなリスクとしてランサムウェアの感染経路を分析し、対策することが必要と考えております。次回以降も、是非、ご参加いただき、Windowsやネットワークの設定（第２回目と3回目のコンテンツ）について検討頂ければと思います。
11	NASをWAN側NWと診療系NWの間に置いて、ファイルのやり取りをしていますが、どのような対策を行えば安全な運用が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。 WAN側とは、インターネットに接続でき電子メール等の閲覧可能なネットワークという事でご回答させて頂きます。（違うようでしたら詳細をご教示下さい。） この場合、NASを介して診療系への攻撃が成立すると考えられます。特に、WAN側ネットワークのPCがウイルス感染した場合、少なくともNASのファイル共有にウイルス自身を設置して、ファイルの窃取、暗号化、改ざんなどの行為は可能です。また、診療系ネットワークからNASのファイル共有におかれたウイルスを誤って実行されてしまうと診療系への侵入が可能になるため危険です。 考えられる対策は、①NASでウイルス対策ソフトを稼働させる、②WAN側と診療側でEmotetが悪用するOfficeマクロ（VBA）の禁止、もしくは限定的使用とウイルス対策ソフトの稼働、が重要です。 この際、NASのウイルス対策ソフトと診療側のウイルス対策ソフト、WAN側のウイルス対策ソフトをそれぞれ、異なるベンダーにすると、3重のチェックとなり、ウイルス駆除の可能性が高まります。ウイルス対策ソフト各社が世界中のウイルスを同じように把握している訳ではないため、ネットワークの境界で異なるウイルス対策ソフトを稼働させるのは、有効と考えられます。 WAN側と診療側のファイル共有のアクセス制御は、必要最小限のユーザーのみアクセスできるようにして、次回以降ご説明するWindowsの設定を施して頂ければと思います。なお、NASで古いSMBv1プロトコルが稼働していないかを点検されてください。 SMBv1が稼働していると、様々な攻撃が可能となり、診療系を守ることが困難になります。

#	質問	回答
12	電カルメーカ側が侵入されて、通常の保守ルートで侵入された場合、病院側では防ぎようがないように思えます。どうしたらいいでしょうか。	研修に参加頂きありがとうございました。 こうした攻撃は、サプライチェーン攻撃と呼ばれ、今、最も恐れられています。米国政府が利用している資産管理ソフトの開発現場に侵入され、正規製品に情報を外部に送信してしまうバックドアが仕掛けられた事件がありました。資産管理ソフトをインストールすると、資産管理サーバーへの通信に見せかけ、インストールされたPCの情報を外部に送信していましたが、これは10か月近く発見されず、米軍、国防総省、国務省、司法省、ホワイトハウス、NASA、民間企業など18,000社が被害にあったということです。 また、OSS（Open Source Software、ソースコードが公開され自由に使用できるソフトウェア）の中に、ウイルスを仕込むことで、OSSを組み込んで作成されたソフトウェア自身がウイルスになるというような「攻撃」も発生しています。 これらを受けて、正規のソフトウェアの汚染を防ぐ、様々な提案がされています。中でもSBOM（Software Bill of Materials、ソフトウェア部品表）を作成し、バージョンを管理することで、ウイルス混入や脆弱性の有無をチェックするようにする国際的な動きがあります。日本でも経済産業省が中心になってSBOM作成の検証事業が進んでいます。 近い将来、政府調達基準に 、SBOMが作成されているか、という項目が追加されることが予想されており、電子カルテシステムも、同様に使用しているソフトウェアの部品単位での安全性の管理が進むと期待されています。
13	電子カルテと業務用の回線を別で用意することによって被害を最小限に抑えられると考えてよろしいでしょうか。電子カルテ側ではOffice等を使用しない等。	研修に参加頂きありがとうございました。 少なくとも、電子カルテ側の端末では、①ウイルスの侵入経路となる、電子メールやWebサイトの閲覧を行わない、②ExcelやWordのマクロを有効にしない、③VPN等のネットワーク機器が設置されている場合は、脆弱性情報の入手と脆弱性保守を実施する、等の実施をお願い致します。
14	今回のQ&Aについて後日でも良いので全て回答したものは公開されますか？	研修に参加頂きありがとうございました。 事務局においてご質問内容を確認の上となりますが、原則、公開いたします。
15	USB利用は一般的にNGとされますがHIS系ネットワークからレセプトデータと抽出して介護保険のオンライン請求をするのに使用しています。ネットワークで繋げるよりは良いと思うのですがどうでしょうか。	研修に参加頂きありがとうございました。 HIS系で使用しているウイルス対策ソフトと異なるウイルス対策ソフトをインストールしたPCを1台用意し、HIS系と業務系をまたぐ際に、そのPCでウイルスチェックを行ってはどうでしょうか。異なるウイルス対策ソフトでの2重チェックとなるので、安全性が高まります。また、ウイルス対策ソフト内蔵のUSBメモリの活用も考えられます。具体的には、第2回技術編で解説していますので、ご参考ください。
16	非Windowsな専用OSで稼働するバックアップアプライアンスを利用し、 WORM(Write Once Read Many)で取得したバックアップ(スナップショット)は物理的に遮断していなくても有効と言えますでしょうか？	研修に参加頂きありがとうございました。 ランサムウェアの場合、Linux及びLinuxの仮想環境を破壊するケースがあるため、専用OSがLinux派生のものである場合、バックアップシステム全体が回復困難に陥る可能性があります。 アプライアンスのOSについて調査し、どのようなリスクがあるかを検討する必要があると思います。
17	オフラインバックアップについてはどのくらい取得するのがよいのでしょうか。世代、期間、等。ランサムウェアに入り込んでも、	研修に参加頂きありがとうございました。 標的型攻撃の場合、数年潜伏するというケースが指摘されています。一方でランサムウェアの場合は、内部の偵察が完了し次第、暗号化に移るため、数年ということは考えにくいと思います。このことから、1年くらいをめどに、月次の世代を取得し、かつ、SecurityログやSyslogもその程度は改ざんされない状態で保存して頂くことで、いつ、侵入されたかを解析できるようにしておくことが重要と思います。侵入された時点がはっきりすれば、それ以前のバックアップの真正性は確保可能となります。 また、暗号化前の改ざんは考えにくく（復号鍵を買っても被害者には意味をなさないため）、侵入から暗号化までの間のデータを精査することで真正性を確保できるのではないかと考えます。なお、精査の精度を上げるためには、部門システムのバックアップも重要となります。
18	大阪のランサムウェアの被害やもっと具体的な復旧の流れなど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。 現在、調査委員会が立ち上がり、調査報告書を策定中とのことです。報告書の公表を待ちたいと思います。
19	急性期センターでは外部保管したLTO元に復旧したとのことですが、感染が発覚した時点で既にバックアップしていたLTO内にも感染源が仕込まれている可能性もあるのではと思うのですが、汚染されていないというのは何をもって判断したのでしょうか。 ランサムウェアに関連するファイルがないとかで判断したのでしょうか。	研修に参加頂きありがとうございました。 大阪急性期・総合医療センター様の場合、10/31の事件発生時点のバックアップは暗号化されており、使用ができませんでした。このため、不審な通信が認められなかった10/27時点での遠隔地保存されていたバックアップを精査の上、復旧に使用しています。

#	質問	回答
20	電子カルテシステムを始めとした多くの病院情報システムはローカルネットワークで構成されているため,サーバおよびクライアントの修正プログラムは導入当初から次回システム更新までそのままでことがほとんどで、これはシステム動作要件により病院側で勝手に実施できないのが現状です。なにか病院側で考えられることはあるでしょうか？あるいは内部に入られたら基本なにもできないと考え、オフラインバックアップなどの復旧できる方法を考えておくことが重要でしょうか？	研修に参加頂きありがとうございました。 セミナーでもご案内したように、ソフトウェアにはリモートコード実行、特権昇格、セキュリティ機能の回避などの脆弱性があり、修正プログラムを適用していない場合、攻撃側にとって有利な材料が豊富にあると言わざるを得ません。従って、アップデートが困難な場合は、外部からの侵入をいかに防ぐかがポイントになります。そのための、次回以降の対策のポイントをご紹介します。 ・外部接続を行っている機器の脆弱性を修正する、接続元IPアドレス制限の実施、多要素認証の実施 ・ウイルス対策ソフトを最新にして稼働させる ・ユーザーには管理者権限を与えず、標準ユーザーで運用する ・Officeマクロ（VBA）の禁止若しくは限定的運用 ・ユーザーアカウント制御の適用 ・USBメモリの厳格運用 ・管理者権限で電子メール、Web閲覧を行わない ・Windows Group Policyの適用
21	病院情報システムの特徴として、電子カルテシステムを基幹として多くの部門システムが有機的に接続している点が挙げられます。HISシステム全体としてバックアップをすることが望まれますが、実際には電子カルテシステムやサブシステムごとのバックアップにとどまっていると感じます。HISシステム全体のバックアップが取れるような製品は現在存在していますでしょうか。あるいはコールドスタンバイの環境を別に作っておくような実現方法になるのでしょうか（そのような余裕資金はありませんが…）	研修に参加頂きありがとうございました。 ご指摘のとおり、電子カルテと各部門システムごとのバックアップが通常ではないでしょうか。ただ、部門システムのバックアップが、どのような構成や世代管理されているか、導入したベンダーに依存しているケースがあり、部門ごとに異なるケースも散見されます。病院全体として、バックアップポリシーを定め、各部門も含めたオフラインバックアップの取得をお願い致します。
22	施設毎にランサムウェア対策したいのですが、予算がきびしいです。厚労省へ補助金が利用できるよう、ご提案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。 次回ご紹介するWindowsの強化設定は、一部、グループポリシー等の技術的に専門性の高いものも含まれますが、基本的にはすべて無償で実施できるものばかりであり、かつ、EDR等の高額なセキュリティ製品よりも確実な効果が期待できるものです。是非、次回もご参加いただき、内容をご理解頂ければと思います。
23	オフラインバックアップについてはどのくらい取得するのがよいのでしょうか。世代、期間等。また、バックアップに仮にランサムウェアがひそんではいるが発病していない場合、バックアップに入り込んだランサムウェアを駆除すれば、復旧として使えるものなのでしょうか？	研修に参加頂きありがとうございました。 世代、期間については、同様のご質問の回答をご参照ください。 バックアップにランサムウェアが実行されずに潜んでいて、暗号化がなされていない場合は、ほぼ、ウイルス対策ソフトで駆除が可能ですので、駆除されれば、復旧として使用可能になります。ただし、Securityログ、Syslogでの不審な行為がなかったか、多数のRDP接続の有無や、長期間に渡るSMB接続の有無、また、バックドアや市販のVPNソフトの実行形跡を調べて、バックアップ取得時点での、その他の侵害行為が無いかを調査する必要があると考えます。