#	ご質問	回答
1	・説明責任としてアクセスログの保管期間に基準はありますか？ ・セキュリティ対策に要する標準的な費用は？（事業規模の平均や売り上げにたいする割合等）	医療情報のアクセスログの保管期間については、法律で明確に定められた基準はありません。しかし、医療情報システムの安全管理に関するガイドラインでは、アクセスログは「医療機関の情報セキュリティポリシーに基づき、適切な期間保存すること」とされています。また、IPAの調査によると、医療機関の約半数がアクセスログを1年以上保存していることが分かっています。アクセスログの保存期間は、データ容量やサイバー攻撃のリスクなどを考慮して、各医療機関で適切に判断する必要があります。 https://warp.da.ndl.go.jp/info:ndljp/pid/11440710/www.ipa.go.jp/files/000052999.pdf 病院でのセキュリティ対策に要する標準的な費用は、病床規模やIT予算の割合によって異なります。一般的には、収益の2%程度をIT予算にかけ、そのうちセキュリティ対策に15%以上を投資するという目安があるようです。 これらの費用はあくまで目安であり、実際には病院のIT環境やセキュリティリスク、対策の内容や範囲などによって変動する可能性があります。また、セキュリティ対策は一度行えば終わりというものではなく、定期的な見直しや更新が必要です。セキュリティ対策の費用は、医療機関の経営にとって大きな負担となることが予想されますが、医療情報の漏洩やシステムの停止などの被害を防ぐためには、必要不可欠な投資と言えるでしょう。
2	各制御をする必要がある旨については理解できました。実際に制御を行うにあたり、管理方法の具体案等も説明頂けると理解しやすいのではないかと感じました。当院でも運用上の確認も れ・効率化が図れる運用があれば検討できると思いましたので、参考案がありましたらご教授頂けると幸いです。	アクセス制御を効果的に実施するためには、以下のようなポイントがあります。 - アクセス制御の方針や基準を明確に定めること。医療情報システムの安全管理に関するガイドラインでは、医療機関の情報セキュリティポリシーに基づき、アクセス制御の方針や基準を策定し、運用することが求められています。アクセス制御の方針や基準には、アクセスするユーザーや役割、情報の分類やレベル、アクセスの種類や権限、アクセスログの保存期間や管理方法などが含まれます。 - アクセス制御の設定や変更を適切に管理すること。アクセス制御の設定や変更は、責任者や承認者の承認を得た上で、正確に行う必要があります。また、設定や変更の内容や理由、日時や担当者などを記録し、定期的に見直しや監査を行うことが望ましいです。 - アクセス制御の効果や問題点を評価すること。アクセス制御の効果や問題点を評価するためには、アクセスログの分析やレビューが有効です。アクセスログとは、誰がいつどの情報にどのようにアクセスしたかを記録したものです。アクセスログを分析やレビューすることで、アクセス制御の適切性や効果、不正なアクセスや情報漏洩の兆候などを把握することができます。 以上のように、アクセス制御は、方針や基準の策定、設定や変更の管理、効果や問題点の評価という3つのステップで実施することができます。これらのステップを遵守することで、医療情報の安全管理を向上させることができると考えられます。
3	現在運用中の環境で多要素認証などを除くセキュリティ対策、ゼロ・トラストを意識した環境構築の例を具体的にご教示いただけますと幸いです。	ゼロトラストを意識した環境構築の例について、以下にいくつか紹介します。 - デバイスのアクセス制御：デバイスは、ネットワークやリソースにアクセスする前に、常に認証と検証を受ける必要があります。デバイスの状態やパッチレベル、セキュリティポリシーの適用などを確認し、信頼できるデバイスのみにアクセスを許可します。また、デバイスには最小限の権限を付与し、不要なサービスやポートを無効化します。 - ユーザーのアクセス制御：ユーザーは、ネットワークやリソースにアクセスする前に、常に認証と検証を受ける必要があります。ユーザーのアイデンティティや役割、アクセス要求のコンテキストなどを確認し、信頼できるユーザーのみにアクセスを許可します。また、ユーザーには最小限の権限を付与し、必要なリソースのみにアクセスできるようにします。 - ネットワークのアクセス制御：ネットワークは、ネットワーク間やネットワーク内の通信を制御する必要があります。ネットワークのセグメンテーションやマイクロセグメンテーションを行い、ネットワークの境界を細かく分割し、通信の流れを制限します。また、ネットワークの暗号化や監視を行い、通信の安全性や可視性を確保します。 - データのアクセス制御：データは、データの分類やラベリングを行い、データの重要度や機密性を明確にする必要があります。データに対するアクセス権や保護レベルを設定し、データの閲覧や編集、移動、削除などの操作を制限します。また、データの暗号化や監視を行い、データの安全性や可視性を確保します。 以上のように、ゼロトラストを意識した環境構築の例は、デバイス、ユーザー、ネットワーク、データの4つの要素に分けて考えることができます。これらの要素は、相互に連携し、補完し合うことで、より強固なセキュリティを実現します。
4	ベンダーが作成した医療系システム（電子カルテ等）の設定マニュアルでは、Windowsの標準機能で備わっているセキュリティ関係の機能をOFFにするよう記載されている項目が多いです。この設定を行わないとシステムを稼働できないのですが、このような場合のセキュリティの対策や考え方をご教示頂けますでしょうか。	残念ながら、機能を有効化していただけないと有効なセキュリティ対策を行うことは難しいと考えます。

#	ご質問	回答
5	それぞれのシステムで更新時期が違う環境でIPv4からIPv6へ移行しようとする場合、そういう状態でも移行が可能なのでしょうか？	IPv4とIPv6は互換性がないため、移行には慎重な計画と準備が必要です。移行の方法には、以下のようなものがあります。 - デュアルスタック：IPv4とIPv6の両方のプロトコルを同時にサポートする方法です。IPv4とIPv6の間の通信は、トランスレーション技術を用いて行われます。この方法は、最もシンプルで柔軟な移行方法ですが、ネットワーク機器やアプリケーションが両方のプロトコルに対応している必要があります。 - トンネリング：IPv4のネットワーク上でIPv6のパケットをカプセル化して転送する方法です。IPv4とIPv6のネットワークをつなぐトンネルを作成し、IPv6のパケットをIPv4のパケットに変換して送受信します。この方法は、IPv4のネットワークをそのまま利用できる利点がありますが、トンネルの設定や管理が複雑になる欠点があります。 - トランスレーション：IPv4とIPv6のパケットを相互に変換する方法です。IPv4とIPv6のネットワークの境界にトランスレータを設置し、ヘッダやアドレスなどの情報を変換して送受信します。この方法は、IPv4とIPv6のネットワークを透過的に接続できる利点がありますが、パケットの変換によるオーバーヘッドや機能の制限が発生する欠点があります。 これらの方法の中から、病院のシステムやネットワークの状況に合わせて最適なものを選択する必要があります。また、移行の際には、以下のような点に注意する必要があります。 - IPv6に対応したネットワーク機器やアプリケーションの導入や更新を行う - IPv6のアドレス割り当てやルーティングの設計や実装を行う - IPv6のセキュリティ対策や運用管理の体制を整える - IPv4とIPv6の相互運用性やパフォーマンスの確認や評価を行う IPv4からIPv6への移行は、一朝一夕にできるものではありません。段階的に計画を立てて実行することが重要です。
6	Windowsアップデートによるシステムへの影響度が分かりにくい。セキュリティを考えれば、常に最新化（標準化）すべきだと思うが、HISやRIS、PACSなど、複数のアプリケーションを共有で利用しているクライアントでは、Windowsアップデートを行うたびに各ベンダーに依頼して動作確認していただくことを想定しているのか見解を教えていただきたい。	Windowsアップデートによるシステムへの影響度は、システムの種類やバージョン、アップデートの内容によって異なります。一般的には、Windowsアップデートはセキュリティやパフォーマンスの向上、新しい機能の追加などを目的として行われるため、システムに有益な影響を与えると考えられます。しかし、場合によっては、互換性の問題や不具合が発生する可能性もあります。 HISやRIS、PACSなどの医療情報システムは、患者の診療や検査に関わる重要な情報を扱うため、システムの安定性や信頼性が求められます。そのため、Windowsアップデートを行う際には、システムの動作確認やバックアップを事前に行うことが推奨されます。また、各ベンダーによっては、Windowsアップデートに対応したシステムのアップデートやパッチを提供している場合もあります。その場合は、ベンダーの指示に従ってシステムの更新を行うことが必要です。 Windowsアップデートを行うたびに各ベンダーに依頼して動作確認していただくことを想定しているかどうかは、ベンダーによって異なると思われます。一部のベンダーは、Windowsアップデートの影響を事前に調査して、必要に応じて動作確認やサポートを行っている場合があります。しかし、すべてのベンダーがそうであるとは限りません。そのため、Windowsアップデートを行う前に、各ベンダーに確認することが望ましいと思います。
7	ゼロトラストというワードが昨今飛び交っていますが、ゼロトラストを推進していくのであればネットワーク分離や、USBメモリの接続を気にすることがなければ非常に便利な使い勝手になっていきます。ゼロトラストを推進する上で、必要最低限の標準構成があれば助かります。どこまですればいいか？は誰もが感じている疑問ではないのでしょうか	ゼロトラストとは、信頼できるネットワークやデバイスという概念を捨てて、すべてのアクセスやトランザクションに対して検証や監視を行うセキュリティの考え方です。ゼロトラストを推進することで、ネットワーク分離やUSBメモリの接続などの制限を緩和することができる可能性がありますが、それはゼロトラストの目的ではありません。ゼロトラストの目的は、組織のリソースやデータを保護することです。 ゼロトラストを推進する上で、必要最低限の標準構成というものはありません。ゼロトラストは、一つの製品やソリューションではなく、概念や理念の集合体です。したがって、ゼロトラストを実現するためには、組織の状況やニーズに応じて、さまざまな技術要素やソリューションを組み合わせて構築する必要があります。 ゼロトラストに用いられる技術要素には、以下のようなものがあります。 - ポリシーエンジン：アクセスポリシーを定義し、管理するコンポーネントです。アクセスポリシーは、主体（ユーザーやデバイスなど）と企業リソース（データやアプリケーションなど）の関係性や属性に基づいて作成されます。 - ポリシー実施ポイント：アクセスポリシーを適用し、実施するコンポーネントです。ネットワーク機器やエンドポイントなどが該当します。ポリシー実施ポイントは、ポリシーエンジンと連携して、アクセス要求を検証し、承認や拒否を行います。 - データソース：アクセスポリシーの作成や検証に必要な情報を提供するコンポーネントです。ディレクトリサービスやアイデンティティプロバイダー、デバイス管理ツールなどが該当します。データソースは、主体や企業リソースの属性や状態をポリシーエンジンに伝えます。 - セキュリティコントロール：アクセスポリシーに加えて、セキュリティレベルを高めるためのコンポーネントです。暗号化やマルウェア対策、侵入検知などが該当します。セキュリティコントロールは、主体や企業リソースの保護や監視を行います。 これらの技術要素を組み合わせて、ゼロトラストの考え方に基づいたセキュリティアーキテクチャを構築することが、ゼロトラストの推進になります。ゼロトラストの推進には、以下のようなポイントに注意する必要があります。 - ゼロトラストは、一朝一夕にできるものではありません。段階的に計画を立てて実行することが重要です。 - ゼロトラストは、組織のビジネスや業務に合わせてカスタマイズすることが必要です。ベストプラクティスや標準構成に頼るのではなく、自分たちの状況や目的に応じて適切な技術要素やソリューションを選択することが必要です。 - ゼロトラストは、常に改善することが必要です。アクセスポリシーやセキュリティコントロールは、主体や企業リソースの変化や脅威の状況に応じて、定期的に見直しや更新を行うことが必要です。

#	ご質問	回答
8	当院では電子カルテシステムで共有フォルダを使用している。基本各部署ごとフォルダの閲覧権限設定をしているが、全員が閲覧できるフォルダもある。多職種が関わる業務関係で必要不可欠であるところであるが、このような全員が閲覧できるフォルダにも細かく権限設定が必要なのか。必要である場合、どのように措置をとれば良いのか。	電子カルテシステムでの共有フォルダは、医療情報の共有や連携に便利な機能ですが、同時に個人情報の漏洩や不正利用のリスクも高める可能性があります。そのため、共有フォルダの権限設定は、必要最低限の範囲と目的に応じて行うことが重要です。 全員が閲覧できるフォルダにも細かく権限設定が必要かどうかは、フォルダに保存される情報の内容や重要度、多職種の関係性や業務の流れなどによって異なります。一般的には、以下のようなポイントに注意することが望ましいと思われます。 - フォルダに保存される情報が、患者の個人情報や医療情報を含む場合は、その情報が必要な職種や部署に限定して閲覧権限を付与すること。例えば、患者の氏名や住所、診療内容や検査結果などの情報は、個人情報保護法や医療法などの法令に基づいて適切に管理する必要があります。 - フォルダに保存される情報が、医療機関の運営や管理に関する情報を含む場合は、その情報が関係する職種や部署に限定して閲覧権限を付与すること。例えば、医療機関の方針や計画、予算や経営状況などの情報は、医療機関の利益や競争力に影響する情報であるため、慎重に取り扱う必要があります。 - フォルダに保存される情報が、医療機関の教育や研究に関する情報を含む場合は、その情報が必要な職種や部署に限定して閲覧権限を付与すること。例えば、医療機関の教育プログラムや研究成果、学会発表などの情報は、個人情報、医療機関の知的財産や評価に関わる情報であるため、適切に管理する必要があります。 以上のように、共有フォルダの権限設定は、フォルダに保存される情報の性質や目的に応じて、必要かつ適切な範囲で行うことが望ましいと思われます。ただし、権限設定を行う際には、以下のような点にも注意する必要があります。 - 権限設定は、医療機関の情報セキュリティ方針や運用管理規程などに沿って行うこと。権限設定の基準や手順、責任者などを明確にすること。 - 権限設定は、職種や部署の変更や退職などに応じて定期的に見直しや更新を行うこと。不要になった権限は速やかに削除すること。 - 権限設定は、システムのログや監査などによって記録や検証を行うこと。不正なアクセスや操作が発生した場合は、原因や対策を検討すること。
資料・アーカイブ		
1	機器トラブルでほとんど音声を聞くことができず、内容がわかりませんでした。資料の開示や講義内容の文字起こし、もしくは録画の再配布等の予定はありますか？	全オンライン研修終了後にアーカイブ配信を予定しております。 アーカイブ配信については、随時MISTサイト（https://mhlw-training.saj.or.jp/）からお知らせいたします。
2	第3回　システム・セキュリティ管理者向け研修のアーカイブを見たいのですが、URL等を教えて下さい。	
その他		
1	講師の方は情報処理安全確保支援士の方でしょうか？	いえ、情報処理安全確保支援士ではありません。
2	音声が小さくPC側で音量を最大にしてかろうじて聞こえる感じであるので、音量をもう少し出してもらえればと思います。今回で2回参加して、1回目はスマートフォンとイヤフォンで、今回はノートpcとそれぞれ環境は異なってますが、やはり音が小さいのには変わりがありませんでした。ご改善いただければと思います。	ご意見ありがとうございます。音声については事務局側で十分に確認はしておりますが、音量については調整いたします。 受講側も再度スピーカー等の設定を再確認いただけますと幸いです。