令和6年度医療情報セキュリティ研修 及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業　（一般社団法人ソフトウェア協会）

【立入検査研修】 医療機関向けコース　後編

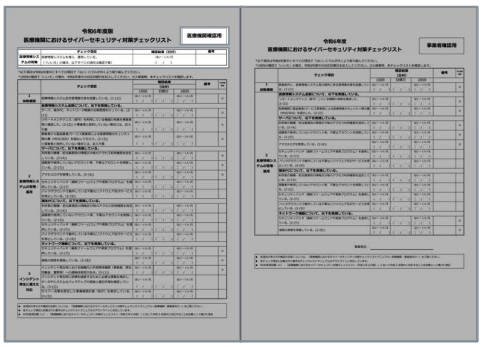
BC Signpost株式会社
松山 征嗣

立入検査研修
目次

医療機関向け　後編

主に技術的なもの

- 2．医療情報システムの管理・運用
  - サーバおよび端末PC
  - ネットワーク



医療情報システムの有無

復習

医療情報システムの有無

医療情報システムを導入、運用している。

医療情報とは？	医療情報システムとは？
•医療に関する患者情報（個人識別情報）を含む情報。	•医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般 サーバ、端末PC（≒エンドポイント,医療機器）、ネットワーク機器等を含む。

システムの例

- レセコン
- 電子カルテ
- オーダリングシステム

マニュアルにも例示

- 調剤システム、臨床検査システム等、各種部門システム
- PDI作成装置、インポート装置
- 各種撮影装置、検査装置（※）
- レポートシステム、遠隔画像診断システム

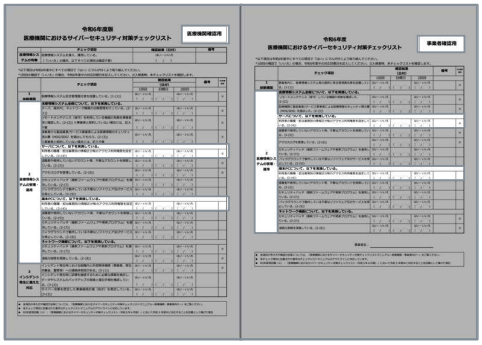
医療情報が発生するもの
医療情報を参照するもの

- オンライン資格確認端末
- 医事会計システム
- 予約システム
- 受付機・精算機
- 受付案内表示システム

患者の個人情報、
患者個人識別情報に紐づくもの

- これらシステムを構成する機器およびそこで動作するソフトウェアは全て安全管理の対象です
- インターネットへの接続の有無は関係ありません
- 製品化されたシステムではなく、内製したシステムや、汎用のソフトウェアなどを使用して医療情報を扱う業務を行っている場合も対象となります
  - PC
  - サーバ
  - ストレージ
  - テープ装置、外部ディスク装置
  - タブレット、携帯端末
  - モニター
  - ネットワーク機器（ファイアウォール、スイッチ、ルータ、VPNルータ　等）

※薬機法上の「管理医療機器」であっても、サーバや他の端末等と連携して動作する情報システムの側面を持つものは対象として考える必要があります



サーバ　端末PC

2． 医療情報システムの管理・運用

利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))

【端末PCについて、令和６年度より通常確認へ移行】

準備コースより再掲

2. 医療情報システムの管理・運用

利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))

誰が、どの情報に、どんなことができるかを決めるルール

目的

- 誰がどの情報を操作したか、責任の所在を明確にする（真正性）
- 重要な情報に、関係のない人がアクセスしてしまうのを防ぐ（機密性）
- 不正な操作を防ぎ、システムやデータの安全性を確保する（完全性）

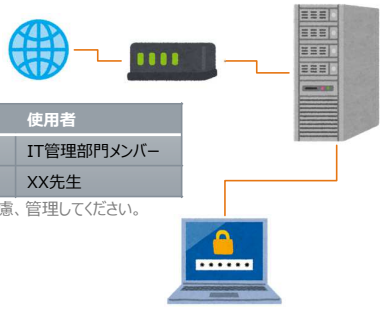
医療情報は診療を進める上で不可欠なものとなりますが、プライバシーとして保護する必要性もあります。
業務上、関係のない閲覧に起因する問題（情報漏洩など）も発生しています。

電子カルテをイメージした例	記事入力	病名	検査結果	処方オーダ
 システム管理者	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 医師	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 看護師	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	△ 閲覧のみ
 医事事務員	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	× 閲覧不可

2． 医療情報システムの管理・運用

利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))

システムにおいて、ユーザー管理は構成ごとに異なることが多くなります。それぞれのアカウント情報の趣旨とあわせて、混同しないよう整理、管理する必要があります。



VPNルーター　アカウント登録状況

ID名	役割	使用者
sysadmin001	システム管理者	IT管理部門メンバー
d0200123	一般利用者	XX先生

チェックリストでは明記されていませんが、できれば考慮、管理してください。

端末PC/OS　アカウント登録状況

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバ/アプリケーション　アカウント登録状況

ID名	役割	アカウント種別	使用者
systemadmin	システム管理者	管理者	IT管理部門メンバー
d0200123	医師	医師	XX先生
n0220246	看護師	看護師	YYさん

サーバ/OS　アカウント登録状況 ＊

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

一般の利用者は意識しないシステム設計/構成とされていることが多い部分ですが
システム管理、セキュリティ管理の上では
極めて重要な構成要素であることに注意してください

＊ DBサーバなどミドルウェアに関しても同様に管理が必要です。
＊ 仮想化システムやクラウドサービスの場合はサービス管理用アカウント情報を管理しておく必要があります

2． 医療情報システムの管理・運用

利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))

＜実施方法＞

誰が、どの部署が、情報にアクセスする権限があるのかを確認、設定、規程化してください

- **例示**
  - **アプリケーションでの権限レベル：役職（医師/看護師/技師/事務/システム管理者）や、部門（診療科/中央診療部門/医事/システム管理部門）など**
  - **OSでの権限種別：Windowsアカウント（管理者/標準ユーザー）**

利用者台帳などを作成し、管理してください

- **例示**
  - **Active Directoryなどの組織のシステム管理者が使用者を管理するためのシステムや技術を用いて設定する。**
  - **資産管理ツールなどを用いて管理を行う。**
  - **マニュアルにある最低限の台帳を作る。**

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可
・	・	・	・	・	・	・	・	・

※令和5年度は端末PC（エンドポイント）は参考項目でしたが
令和６年度からは通常確認項目となっています。

2． 医療情報システムの管理・運用

利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))

<ケーススタディ>

システム上、管理者や使用者を分けているが規程がない

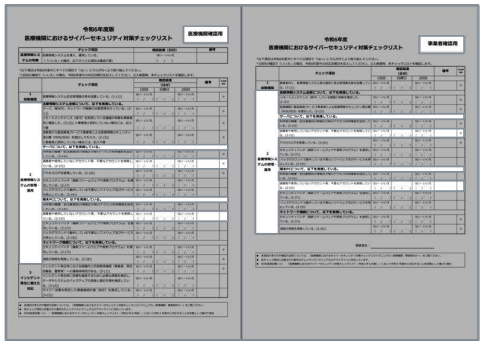
- 規程が無い場合、適切に運用できているか判断基準がない状況です。
- 誰にどのような権限を付与するのか、誰ならどの情報にアクセスすることができるのか、まずは簡易的でもいいので、規程を作成しましょう。
- ひとまずは「いいえ」を選択し、対応する期日を記載しましょう。

規程や設定はできているが、定期的な確認や棚卸、経営者への報告が行えていない

- 定期的にアクセス状況や棚卸を行うようにしましょう。最初に導入したまま見直しや対応が行えていない場合は「いいえ」を選択し、現状確認から経営者への報告・承認までを期限を決めて実施しましょう。

事業者に委託しているため、管理状況がわかりません

- 契約形態にもよりますが、基本的には医療機関が医療情報システムを使用していることに変わりはありません。自院の状況を事業者に確認し、対応状況を把握し、規程の作成やセキュリティ設定の強化などに努めましょう。



2． 医療情報システムの管理・運用

サーバ　端末PC

退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))

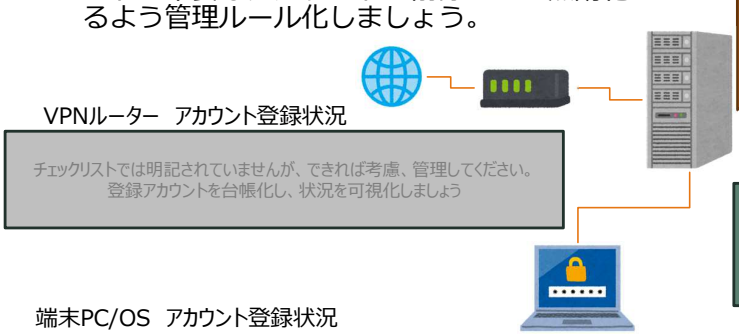
【端末PCについて、令和６年度より通常確認へ移行】

2． 医療情報システムの管理・運用

退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))

＜実施方法＞

- 2-(4) の情報を参考にし、使用していないアカウントと不要なアカウントを削除または無効化されるよう管理ルール化しましょう。



VPNルーター　アカウント登録状況

チェックリストでは明記されていませんが、できれば考慮、管理してください。
登録アカウントを台帳化し、状況を可視化しましょう

サーバ/アプリケーション　アカウント登録状況

各種サーバーアプリケーションの登録アカウントを台帳化し、
状況を可視化しましょう

サーバ/OS　アカウント登録状況

サーバのローカルアカウントや、ActiveDirectory等認証サーバへの
登録アカウントを台帳化し、状況を可視化しましょう

端末PC/OS　アカウント登録状況

端末のローカルアカウントを台帳化し、
状況を可視化しましょう

※令和5年度は端末PC（エンドポイント）は参考項目でしたが、令和６年度では通常確認項目となっています。

2． 医療情報システムの管理・運用

退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))

＜ケーススタディ＞

削除はできていないが、無効化はしている

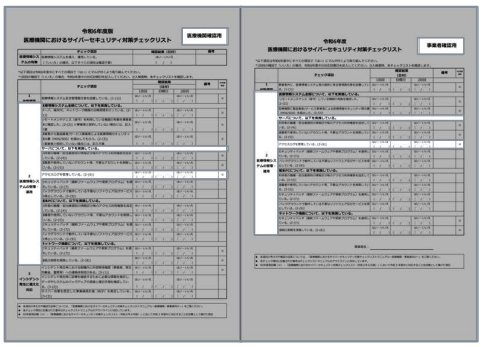
- 無効化できていれば、「はい」を選択いただいて問題ありません。

以前対応したが、最近は確認できていない

- 退職者などの組織に関係のないアカウントが有効な状態で残り続けることは健全ではありません。「いいえ」を選択し、定期的な確認及び体制確立に向けた対応を行いましょう。

退職者ではあるが、患者や業者の連絡や引継ぎの関係上、残している

- 記録保存、関連付けの維持の関係で、ID情報を残しておかなければならないような状況では「無効化」などの設定でアクセスに利用できない設定とし、離籍していることがわかるよう管理してください。
- 同じIDを再利用、共用することは適切ではありません。可能な限りIDは個人に紐づけるようにし、役割によって権限付与される仕組みが推奨されます。



サーバ

2． 医療情報システムの管理・運用

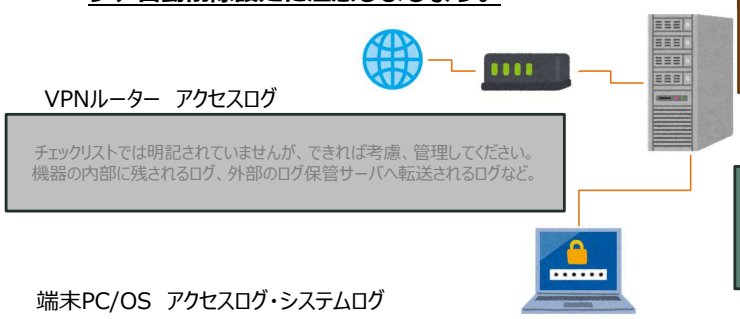
アクセスログを管理している。(2-(6))

2． 医療情報システムの管理・運用

アクセスログを管理している。(2-(6))

＜実施方法＞

- 2-(4) の情報を参考にし、各システム、サーバや機器などのアクセスログが想定の期間保存されるよう管理ルール化しましょう。**ファイル容量や期間でのローテーション、自動削除設定に注意しましょう。**



VPNルーター　アクセスログ

チェックリストでは明記されていませんが、できれば考慮、管理してください。
機器の内部に残されるログ、外部のログ保管サーバへ転送されるログなど。

端末PC/OS　アクセスログ・システムログ

チェックリストでは明記されていませんが、できれば考慮、管理してください。
Windowsのイベントログやセキュリティログ、
（もしセキュリティソフト等の機能で利用があれば）端末の操作ログなど。

サーバ/アプリケーション　アクセスログ・操作ログ

電子カルテサーバ、部門システムサーバなど。
（医療情報の真正性や、機密性、完全性のように
セキュリティに対する説明責任において不可欠な証跡となる）

サーバ/OS　アクセスログ・システムログ ＊

Windowsのイベントログや端末の操作ログ、
Active Directoryサーバ やWebサーバへの接続履歴など。

- 仮想化システムやクラウドサービスの場合も同様に管理アクセスのレビューは適宜行いましょう

2． 医療情報システムの管理・運用

アクセスログを管理している。(2-(6))

<ケーススタディ>

アクセスログと言っても様々あるが、どのレベルで管理できていれば良いのか？

- 医療情報システムのアプリケーションへのアクセス、ログオンや認証結果、操作記録など
- Windowsのセキュリティログ（OSへのローカルログオンやリモートログオンにおける、認証結果のログ）など
- 不正なアクセスや操作が無いかログを確認し、追跡できる状況であれば、「はい」を選択して問題ありません。しかし、ログリストなどを作成し、どのようなログが取れているのかを整理し、組織としての管理体制の確立を目指しましょう。またログの保存期間についてはできる限り長く残すことを推奨します。

ログは取れているはずだが、見たことがない？

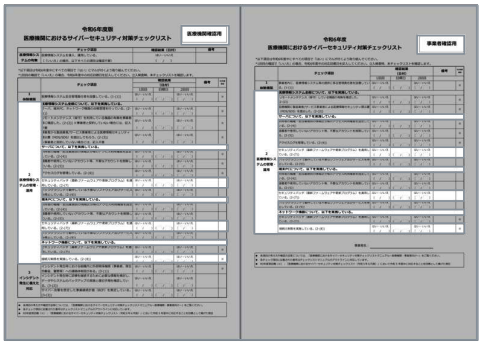
- アクセスログを管理できている状況とは言えません。適切な運用が行われているか事業者とも協議しながら確認し、何のログが取得できているのか、どのような運用状況なのかなど確認し、ログの管理体制を確立しましょう。

全てのシステムでは実施てきていない？

- 医療機関としてログが管理できる状態（＝サイバー攻撃の予兆や発生を検知できる状況）とは言えないため、その状態を目指し対応を行いましょう。

アクセスログはベンダーに依頼しないと解析できない？

- どのような契約になっているのか、ログを入手することができないのか改めて確認しましょう。万が一、ログをベンダーから取得し管理することができない場合は、どのようなログを取得し、インシデント発生時にどのような対応を行うのか。インシデントの予兆はどのように伝えてくれるのか。ログ対応に生じる費用はいくらなのかなど、事前に確認しておきましょう。



2． 医療情報システムの管理・運用

サーバ　端末PC　ネットワーク

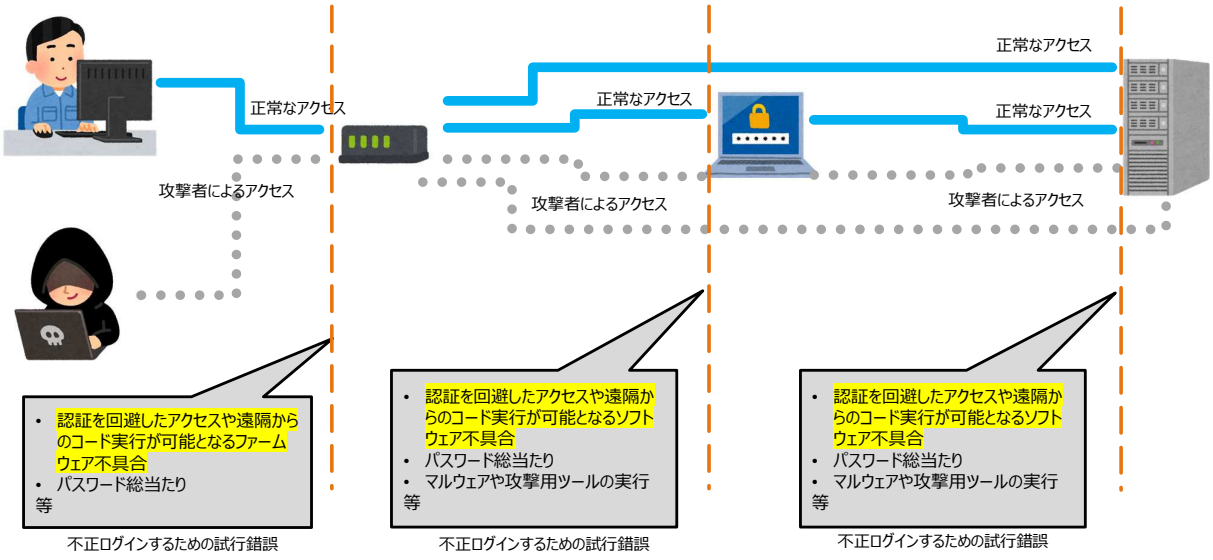
セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))

【サーバおよび端末PCについて、令和６年度より通常確認へ移行】

2． 医療情報システムの管理・運用

セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))

いずれかの段階で不正アクセスによる突破を防止できれば、最悪の事態を回避する確率は向上する



2． 医療情報システムの管理・運用

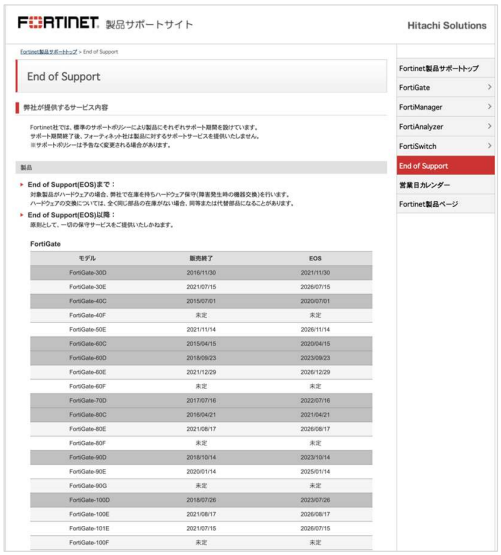
セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))

サポート期限の情報

バージョン	エディション	サポート終了日	延長サポート終了日
Windows 10 21H2	Pro, Enterprise	2023年6月13日	延長サポートなし
Windows 10 22H2	Pro, Enterprise	2025年10月14日	延長サポートなし
Windows 10 LTSC 2019	Pro, Enterprise	2024年1月9日	2029年1月9日
Windows 10 LTSB 2016	Pro, Enterprise	2021年10月12日	2026年10月13日
Windows 11 21H2	Pro, Enterprise	2023年10月10日	延長サポートなし
Windows 11 22H2	Pro, Enterprise	2024年10月8日	延長サポートなし
Windows 11 23H2	Pro, Enterprise	2025年11月11日	延長サポートなし
Windows Server 2008	Standard, Enterprise, Datacenter, Web, HPC, Storage, Small Business, Foundation	2015年1月13日	2020年1月14日
Windows Server 2008 R2	Standard, Enterprise, Datacenter, Web, HPC, Storage, Small Business, Foundation	2015年1月13日	2020年1月14日
Windows Server 2012	Standard, Datacenter, Essentials, Foundation	2018年10月9日	2023年10月10日
Windows Server 2012 R2	Standard, Datacenter, Essentials, Foundation	2018年10月9日	2023年10月10日
Windows Server 2016	Standard, Datacenter, Essentials	2022年1月11日	2027年1月12日
Windows Server 2019	Standard, Datacenter, Essentials	2024年1月9日	2029年1月9日
Windows Server 2022	Standard, Datacenter, Datacenter: Azure Edition, Essentials	サポート中	各バージョンごとに異なる

Microsoft COPILOTにて問い合わせた回答を整形

重要な点は、ライセンス期間という契約観点の問題ではなく
不具合を解消するための対応を継続していく必要があること



Fortigate製品サポート終了情報（日立ソリューションズ社HPより）
https://csps.hitachi-solutions.co.jp/fortinet/end_of_support.html

2． 医療情報システムの管理・運用

セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))

例）Microsoft社は（緊急を除き）月次での公開を予定している

2024 年のセキュリティ更新プログラムの公開予定日

	セキュリティ更新プログラム公開予定日 日本標準時間 (米国太平洋標準時間)
2024 年 1 月	2024 年 1 月 10 日 (2024 年 1 月 9 日)
2024 年 2 月	2024 年 2 月 14 日 (2024 年 2 月 13 日)
2024 年 3 月	2024 年 3 月 13 日 (2024 年 3 月 12 日)
2024 年 4 月	2024 年 4 月 10 日 (2024 年 4 月 9 日)
2024 年 5 月	2024 年 5 月 15 日 (2024 年 5 月 14 日)
2024 年 6 月	2024 年 6 月 12 日 (2024 年 6 月 11 日)
2024 年 7 月	2024 年 7 月 10 日 (2024 年 7 月 9 日)
2024 年 8 月	2024 年 8 月 14 日 (2024 年 8 月 13 日)
2024 年 9 月	2024 年 9 月 11 日 (2024 年 9 月 10 日)
2024 年 10 月	2024 年 10 月 9 日 (2024 年 10 月 8 日)
2024 年 11 月	2024 年 11 月 13 日 (2024 年 11 月 12 日)
2024 年 12 月	2024 年 12 月 11 日 (2024 年 12 月 10 日)

Source: https://msrc.microsoft.com/blog/2023/11/securityupdatereleaseschedule2024/
https://msrc.microsoft.com/blog/2024/08/202408-security-update/

2024 年 8 月のセキュリティ更新プログラム一覧

製品ファミリ	最大深刻度	最も大きな影響	関連するサポート技術情報またはサポートの Web ページ
Windows 11 v24H2, v23H2, v22H2, v21H2	緊急	リモートでコードの実行が可能	v24H2 5041571 v23H2, v22H2 5041585 v21H2 5041592
Windows 10 v22H2	緊急	リモートでコードの実行が可能	5041580
Windows Server 2022,23H2 (Server Core installationを含む)	緊急	リモートでコードの実行が可能	Windows Server 2022, 5041160 Windows Server 23H2, 5041573
Windows Server 2019 , 2016 (Server Core installation を含む)	緊急	リモートでコードの実行が可能	Windows Server 2019 5041578 Windows Server 2016 5041773
Microsoft Office	重要	リモートでコードの実行が可能	https://learn.microsoft.com/officeupdates
Microsoft .NET	重要	情報漏えい	https://learn.microsoft.com/dotnet
Microsoft Visual Studio	重要	情報漏えい	https://learn.microsoft.com/visualstudio
Microsoft Dynamics 365	重要	なりすまし	https://learn.microsoft.com/dynamics365
Microsoft Azure	緊急	リモートでコードの実行が可能	https://learn.microsoft.com/azure

更新が容易ではない重要システムにおいては、脆弱性の深刻度や影響、変更内容の説明などを踏まえ優先度の高いものを確認する。
他の対策によるリスク低減措置の見込みの有無も考慮し、対応期日の協議を行う。

2． 医療情報システムの管理・運用

セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))

＜実施方法＞

全ての端末やシステム、機器等のソフトウェアおよびそのバージョン情報などを台帳に記録、更新してください。

サポート切れのソフトウェアを使用していないか、事業者に確認してください。

できる限り、最新のソフトウェア更新してください。
サポート期間内のソフトウェアを使用する必要があります。

管理規程を確認し、規程通りの運用が行えているか確認してください。
規程に不足がある場合は、見直しを実施してください。

※令和5年度は端末PC（エンドポイント）は参考項目でしたが、
令和６年度では通常確認項目となっています。

2． 医療情報システムの管理・運用

セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))

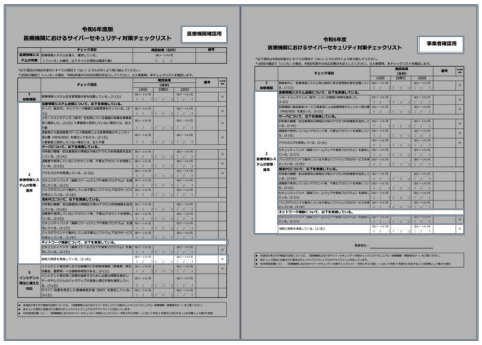
<ケーススタディ>

セキュリティパッチが適用できないといわれたら？

- なぜ適用できないかを文書での回答を求め、台帳や議事録等に理由や受容しているリスクを把握しましょう。
- 契約面での課題も考えられるので、現状の運用・保守契約がどのようになっているのか確認し、運用・保守の理解を事業者と共通認識を持つようにしましょう。
- 厚生労働省からの通達やガイドラインでは、ソフトウェア更新を行うよう促していますので、ガイドラインへの順守を含め事業者に対応を求めていきましょう。

どれくらいの頻度で更新を行っていたら適切なのか？

- ウイルス定義ファイルの更新は１日１回程度公開されていますので、可能な限り毎日更新することが望ましいです。
- Windowsアップデートは月例での公開、および緊急時は随時公開されています。
- インターネット環境であれば緊急のものは１週間以内、通常のものは1ヶ月以内程度での適用が望ましいですが、検証に時間を要する重要システムにおいては年に何度か予定しているメンテナンスのタイミングに合わせて実施し、それまでの脆弱な状況はセキュリティ対策で補うといった方法も考えられます。



2． 医療情報システムの管理・運用

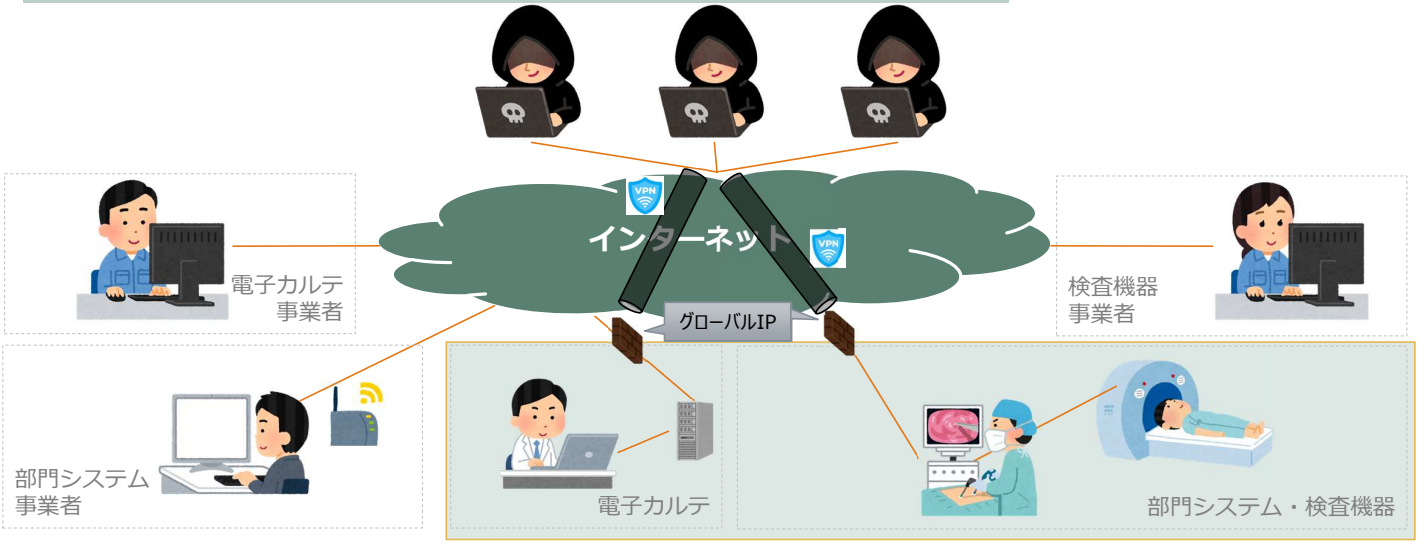
ネットワーク

接続元制限を実施している。(2-(8))

2． 医療情報システムの管理・運用

接続元制限を実施している。(2-(8))

誰でもアクセスできる状況だと、攻撃者もアクセスできてしまう…



2． 医療情報システムの管理・運用

接続元制限を実施している。(2-(8))

＜実施方法＞

ファイアウォールなどを用いて、接続できるIPアドレスを限定する。
（送信元アドレス制限）

特定の地域（国内）のアドレスからしかアクセスできないようにする。
（ジオブロック（地域制限））

無線LANや有線LAN接続におけるセキュリティ対策（接続時認証）を行う。
（MACアドレス認証,IEEE802.1x認証など）

2． 医療情報システムの管理・運用

接続元制限を実施している。(2-(8))

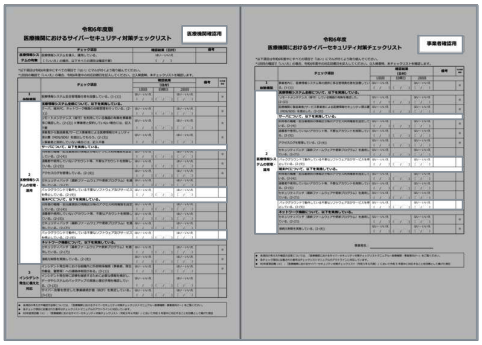
<ケーススタディ>

制限を行うのにさらに費用が必要と言われた？

- 運用・保守上の設定変更の範囲内と考えられるため、事業者と協議をしましょう。

事業者から制限されると困るといわれた？

- なぜ困るのか合理的な理由を求めましょう。安全性を十分に確保できない状態になるようであれば、別の手段を模索、検討する必要があります。



2． 医療情報システムの管理・運用

サーバ　端末PC

バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))

【サーバおよび端末PCについて、令和６年度より通常確認へ移行】

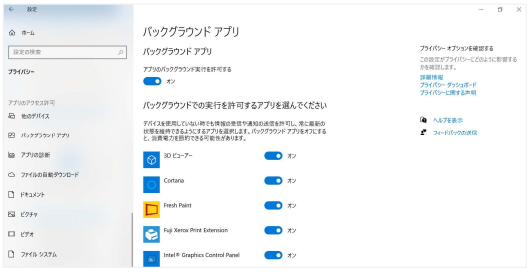
2． 医療情報システムの管理・運用

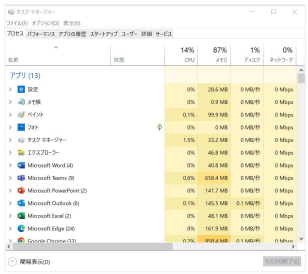
バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))

<実施方法>

Windowsの設定やタスクマネージャーなどから不要なソフトウェアが動いていないか確認し、不要なソフトウェアがあった場合は停止しましょう。

統合管理の設定でアプリ制御等を行う方法も考えられますので システム開発・運用ベンダーと相談してください。





2． 医療情報システムの管理・運用

バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))

<ケーススタディ>

不要なソフトウェアやサービスがわかりません

- どれが不要かは、環境にも依存するためにここでは言及することができません。
- 消去する内容によっては、コンピュータが動作しなくなる可能性があるため、販売店やシステムインテグレーター、メーカーへ確認してください。

おわりに

確認

証跡は必要か？

- 回答の根拠となる文書やデータを求められれば提示できるように準備しておきしましょう。

一部のシステムで実施できていない場合は？

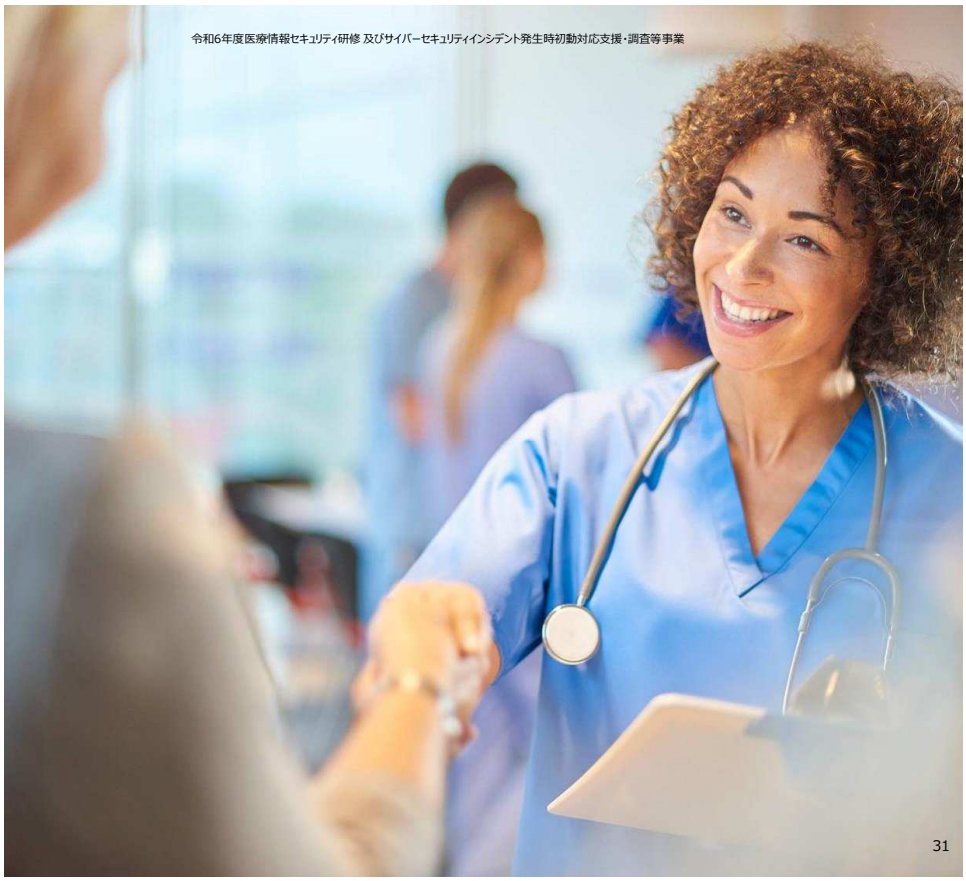
- 「はい」は、医療情報システムの範囲(後述)において、網羅的に確認ができた状態を示します。
  そのため、一部のみの対応の場合は「いいえ」を選択し、対応するため期日を記載しましょう。
- 備考欄には「いいえ」となっている理由について記載してください。

事業者から提出されてこない場合は？

- 回答が得られない理由をメールや文書などで求めてください。

立入検査研修
医療機関向け後編終了

お疲れ様でした。



ありがとうございました。