令和7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

立入検査研修
医療機関向けコース
前編

一般社団法人ソフトウェア協会

目次

前編

後編

医療機関におけるサイバーセキュリティ対策チェックリストの準備について

「医療機関等におけるサイバーセキュリティ対策チェックリスト」について

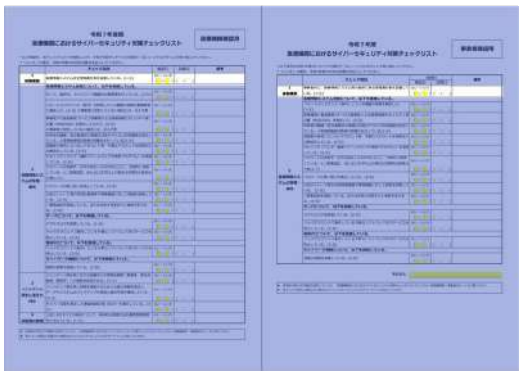
- 本コースではチェックリストの各項目についての説明を行います。
- チェックリストの概要、立入検査の進め方については
  令和7年度　**立入検査研修　準備コース**　をご確認ください。
  → e-learningで公開

【注意】 現物確認を求める文書等

マニュアルでも示されている通り、以下の文書は立入検査時に現物確認できるよう準備してください。

- 機器台帳　（２-①）
- インシデント発生時の連絡体制図　（３-①）
- 事業継続計画（BCP）　（３-③）
- 運用管理規程の規程類　（４）

規程等の文書整備は、多くの確認項目において実施されている根拠として求めるもの。

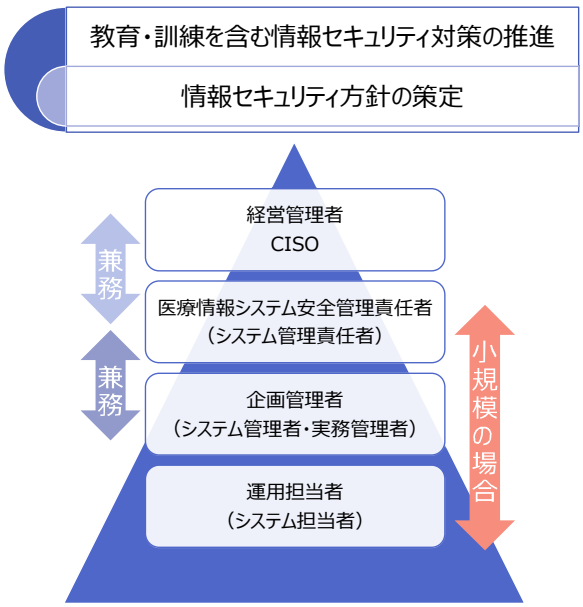


【医療機関等確認用・事業者確認用】

1 体制構築

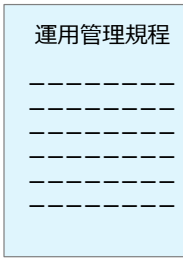
医療情報システム安全管理責任者を設置している。(1-①)

医療情報システム安全管理責任者を設置している。(1-①)

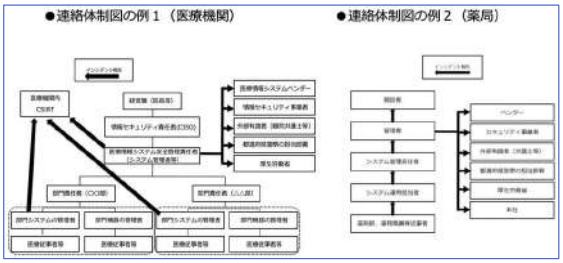


準備、対応のポイント

- 運用管理規程等の文書に医療情報システム安全管理責任者の設置、役割を明示してください。
- 組織図や体制表などで任命された方を明確にしてください。



役割の定義



責任者の明確化、組織内での認知

医療情報システム安全管理責任者を設置している。(1-①)

どのような人が適任か？

●CISO

●企画管理者（システム部門長等）による兼務の場合、経営層による後ろ盾、支援あること。役割を遂行するための裁量が規程などで明示されている。

責任者がシステムに関する知識を持っていない場合は？

●責任者自身がセキュリティ研修等を活用して知識、判断力を向上させる　（本事業で提供されている研修を活用してください）

●前提知識を有する職員を任命し、権限を委譲する

●前提知識を有する職員や外部専門家を補佐として配置し、責任者が判断の責任を負う

外部の事業者を責任者にしても良いか？

●外部の事業者に組織としての責任を移転することはできません

●診療報酬、診療録管理体制加算の施設基準では『専任』の医療情報システム安全管理責任者を配置することとしているため、責任者は常勤の職員であることが望ましいと考えられます

専従：勤務時間のすべてをその業務に従事すること ＊

専任：主業務として業務時間の5割以上をその業務に充てること ＊

専ら：専従と専任の中間。業務時間の概ね8割程度の業務を行なっている ＊

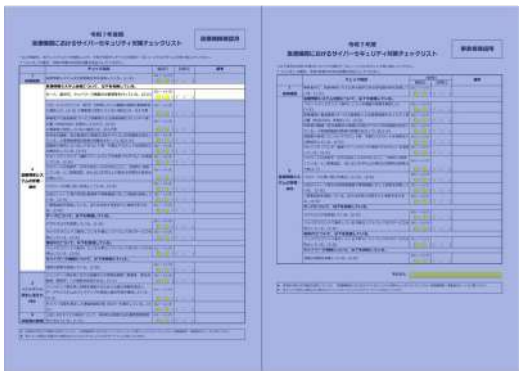
＊ 割合については施設要件の解釈を参考としています。
新規開業医のための保険診療の要点（総論）　／　東京都医師会
https://www.tokyo.med.or.jp/doctor/practicing_docs/general/03

医療情報システム安全管理責任者を設置している。(1-①)

＜事業者における医療情報システム安全管理責任者＞

顧客・施設に対しての責任者		提供製品・サービス単位（全社）
• 製品または顧客を担当する事業部門長や、導入システムのプロジェクトマネージャー等 • 導入後、保守フェーズ終了まで含めて対応できる体制	＋	• PSIRTのように、横断的に製品・サービスを管理する組織の設置が望まれる – インシデント発生時の情報集約、ハンドリング – 共通的に構成されるソフトウェアやハードウェアなどの脆弱性評価やリスクアセスメント – 他の顧客、提供先へのリスク管理情報展開

PSIRT（Product Security Incident Response Team）：
組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能です。自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的としており、国内の製品開発者においても徐々に設置が進んでいます。
https://www.jpcert.or.jp/research/psirtSF.html



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-①)

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-①)

マニュアルの解説要約

医療情報システムの機器は、所在や使用可否を台帳で管理する必要があります。

企画管理者が機器台帳を作成・更新し、利用状況を常に確認できるようにします。

経営層は定期的に報告を受け、管理状況と責任の所在を把握・監督します。

準備、対応のポイント

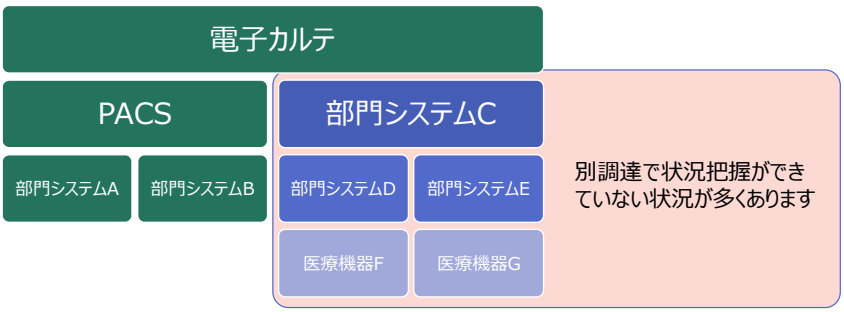
- 台帳の作成は必須です。
- **立入検査では文書現物が確認対象**です。

- 機器の追加、変更、削除があった際は台帳を随時更新してください。
- 最新情報を管理、維持するための規程、管理手順を整備してください。

- 変更時、棚卸し時など、経営層、執行部が確認、承認するフローを定型化してください。
- 承認の履歴が残るような手続きにしてください。

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-①)

調達範囲による管理情報の漏れが生じないよう注意してください



構成するすべての機器を台帳へ記載してください

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-①)

●機器台帳の例

最終更新日： 2024年7月1日
最終更新者： 鈴木一郎

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC1	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC1	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC1	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

対象機器

- PCやサーバ、ネットワーク機器など医療情報システムを構成する情報機器全般が対象です
  （職員の給与や勤怠、財務会計など組織内事務系は対象外です）
- 薬機法上の「管理医療機器」であっても、情報システムの側面を持つものは管理対象としてリスト化してください
- 買取、リース、レンタルなど、保有形態によらず、施設の環境内に設置、使用されているものはリスト化してください

台帳で管理する内容　（例）

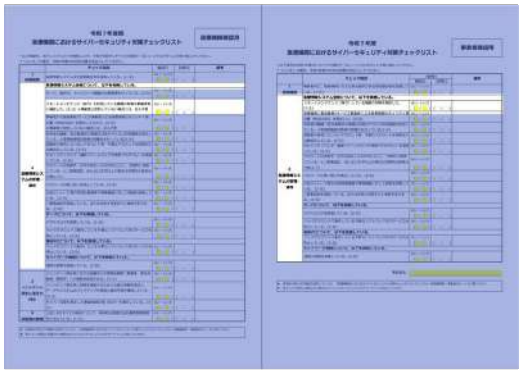
- 管理番号、機器名称
- システム名、メーカー名
- OSバージョン、ソフトウェアバージョン
- 接続ネットワーク、IPアドレス、MACアドレス
- 機器の設置場所
- 管理部門、利用者
- 状態、稼働状況
- 登録日、確認日　　等

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-①)

＜事業者の皆様へのお願い＞

納品時や構成変更時の情報提供

- システム納品時の提出物として納めている機器一覧に、必要十分な情報を記載するようご確認ください
- 医療情報を直接的に通信するもの、保存するものだけでなく、システム保守など間接的な部分で構成される周辺機器に関しても管理対象として情報提供を行なってください



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-②)

リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-②)

マニュアルの解説要約

管理が十分でない、リモート保守の経路を悪用したサイバー攻撃が多発しています。

リモートアクセス機器の設置状況、管理状況は継続的に確認する必要があります。

設置事業者、保守事業者と適宜連携して管理する必要があります。

準備、対応のポイント

- 外部からアクセスして行われる業務の有無を確認してください。
- 委託先の環境にリモートアクセス環境があるかを確認してください。

- リモートアクセス機器におけるセキュリティ設定、認証設定が安全に構成されているか確認してください。

- リモートアクセス機器の設置箇所、設置機器の情報は台帳等で管理してください。
- 最新情報を管理、維持するための規程、管理手順を整備してください。

リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-②)

リモートメンテナンスとは？

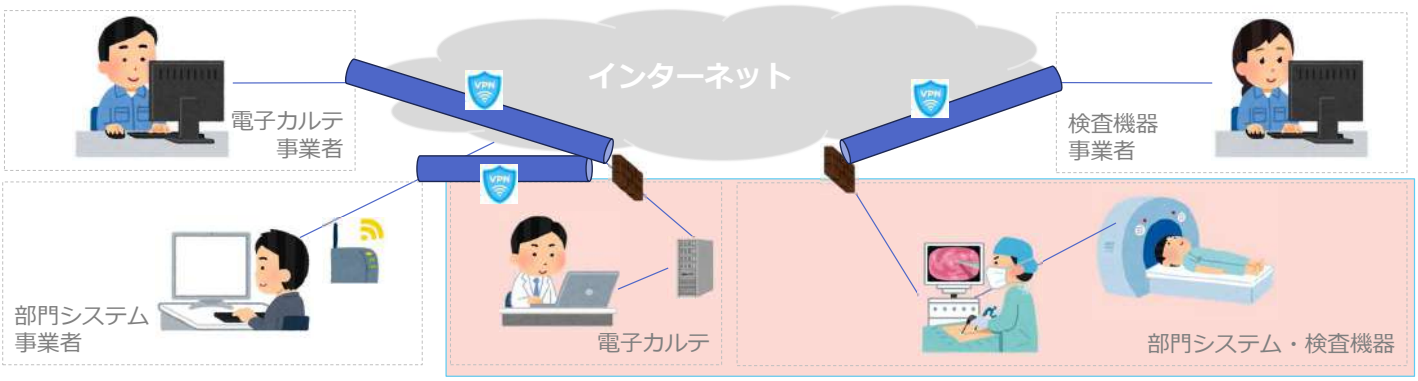
- 機器やシステムの保守や運用を行うにあたって、遠隔で医療情報システムに接続し、作業を行う仕組み全般のことです。
- 専用線相当の回線サービスや、IPSec-VPNやSSL-VPNなどインターネット間を暗号通信で繋ぐVPN接続などさまざまな接続形態があり機密性を確保した通信手段により実施されるものですが、構成や運用に不備があるとセキュリティホールになる可能性があります。

ファームウェアの更新（2-⑥に関連）

- 最新のファームウェア(アップデート)が適用されていることを確認しましょう。
- 新しいファームウェアがリリースされたときは速やかに適用されるよう調整しましょう。

認証の安全性　（2-⑦、2-⑧に関連）

- 安全なパスワードを設定しましょう。（十分な長さ、使い回しの防止など）
- 認証失敗回数によるロックアウト設定を行いましょう。

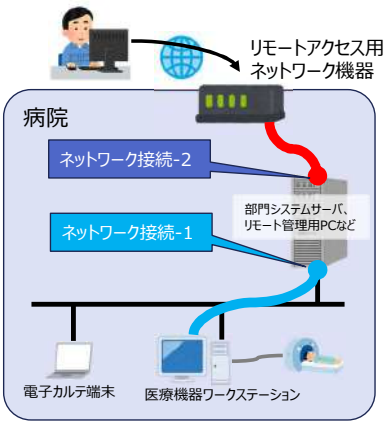


特定の人だけが通れる裏口を作るイメージです

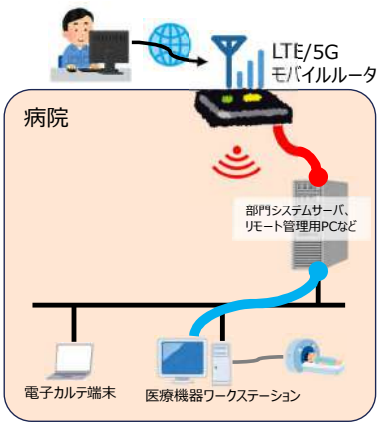
リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-②)

見落とされやすい構成の例

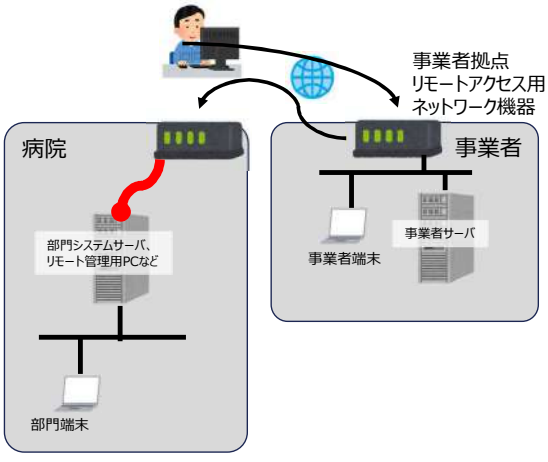
2系統のネットワーク接続、
「2枚挿し」による見落としに注意



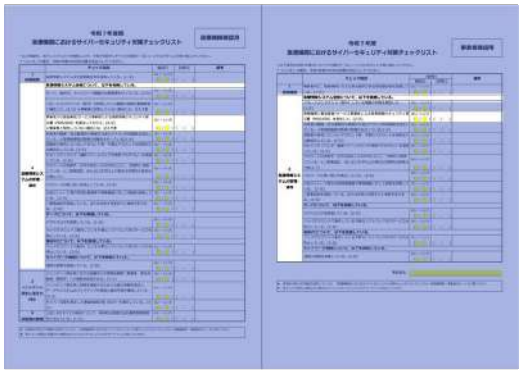
モバイルルータは回線工事が無く
見落としやすいため注意



委託事業者の拠点を経由した経路に注意
（事業者の適切な情報提供、保守が不可欠）



- **施設内に設置のものは現物を確認するとともに管理状況を確認した上で、台帳へ記載しましょう。**
- **MDS/SDSや事業者用チェックリスト等への記載を確認してください。**



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

事業者から製造業者/サービス事業者による
医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-③)

事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-③)

MDS/SDSとは

製造業者による医療情報セキュリティ開示書（Manufacturer Disclosure Statement for medical information security, MDS）、サービス事業者による医療情報セキュリティ開示書（Service provider Disclosure Statement for medical information security, SDS）を意味し、各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する標準的な記載方法を業界団体（JAHIS/JIRA）が定めたもので、厚生労働省標準規格として認定されています。

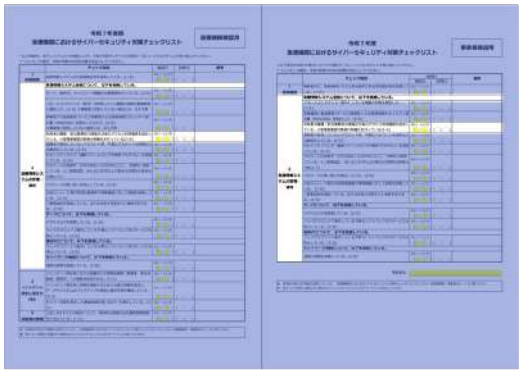
準備、対応のポイント

- 医療機器、医療情報システムが対象です。
- 調達先からMDS/SDSの提供を受けてください。（調達時点のもので良い）

- 回答内容に不足、不明点がある場合は補足情報の提供を依頼しましょう。
- 情報提供が得られた時は付属文書として保存、管理してください。

- 医療機器、医療情報システム調達の際は、納品物にMDS/SDSを含むよう提案依頼書や要求仕様書に明示するよう規程で定めておきましょう。

出典　一般社団法人保健医療福祉情報システム工業会
MDS SDS Ver.5.0チェックリスト
https://www.jahis.jp/standard/detail/id=1119



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

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。
※管理者権限対象者の明確化を行っている(2-④)

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。
※管理者権限対象者の明確化を行っている(2-④)

マニュアルの解説要約

利用者IDは台帳で一覧管理し、所属・氏名・権限等を記録します。

アプリケーション(サービス)の利用者IDだけでなく、OSの利用者IDの情報も確認してください。

利用権限は、資格や役割に応じて適切に設定し、情報のアクセス区分管理を行います。

管理者権限は最小限のユーザに限定し、サイバー攻撃による悪用を防ぎます。

準備、対応のポイント

- システムの利用者情報は台帳で管理し、定期的に確認できるようにしましょう。
- アプリケーション、サービスに対するログインIDだけでなく、OSのログインID情報も確認対象としてください。

- 自動ログイン用IDや特権ユーザーID(管理者)などは共有される対象者、範囲に注意し、確認してください。

- 運用管理規程に利用者管理、アクセス権限に関する規程を定めておきましょう。
- システム調達の際は、提案依頼書や要求仕様書に必要要件として明示するよう規程で定めておきましょう。

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。
※管理者権限対象者の明確化を行っている(2-④)

●利用者 ID 台帳の例

No.	所属部署	姓	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

No.	利用者属性	姓	名	電話番号	ユーザ ID	説明	権限	状態
001	薬剤師	abc	def	****	abc@def	使用者	Admin	使用可
002	非常勤薬剤師	efg	hij	****	efg@hij	使用者	User	使用可
003	事務	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23 年 3 月まで）
004	非常勤事務	qrs	tuv	****	qrs@tuv	使用者	User	使用可

台帳を出力している場合は個人情報を含む機密文書として厳密に管理してください。

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

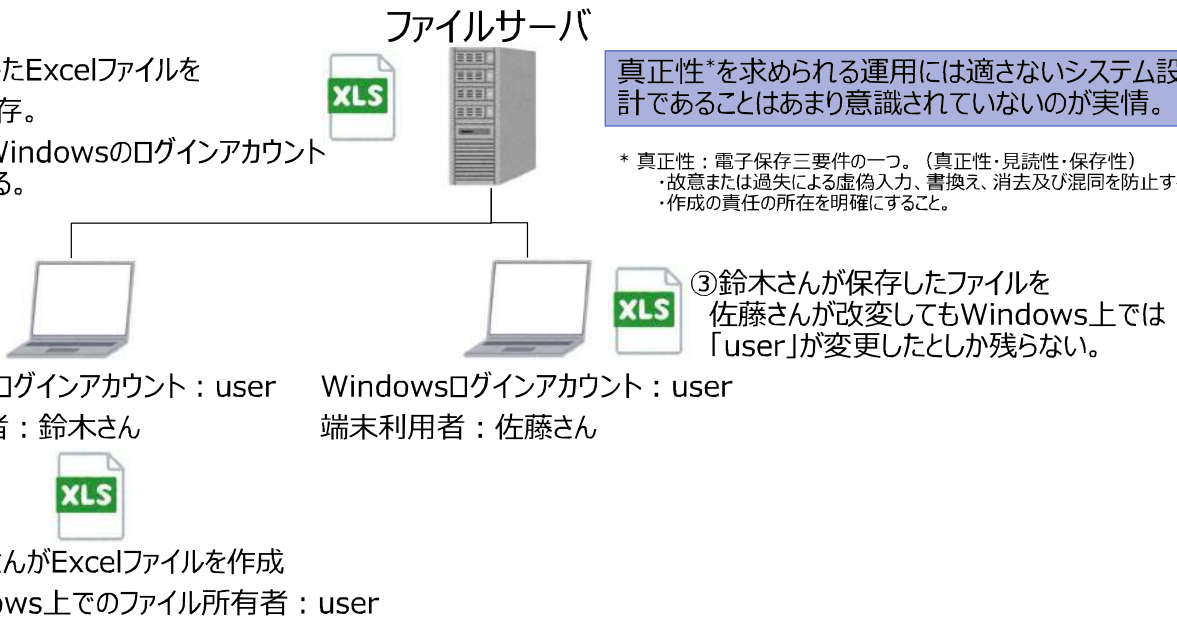
端末PC/OS　アカウント登録状況

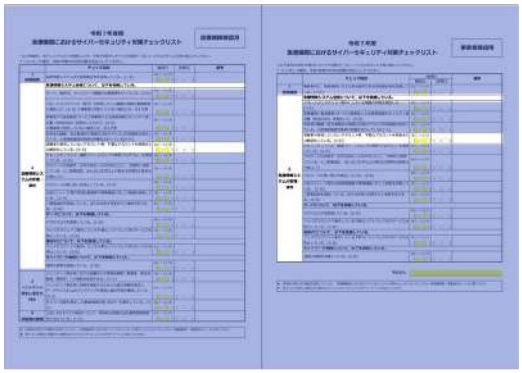
ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

各役割、権限設定において、出来ること、出来ないことを管理規程等で定義、明確化しておきましょう。

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。
※管理者権限対象者の明確化を行っている(2-④)

デスクトップのログインユーザーが共通であることの問題





【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

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または無効化している。(2-⑤)

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または無効化している。(2-⑤)

マニュアルの解説要約

退職者や長期間使用されていないIDは、不正アクセスに使用されないよう、削除または無効化する必要があります。

医療システムでは真正性維持のため、利用者IDの記録保持のため、削除ではなく無効化で対応する場合があります。

リモートアクセス機器へのログインアカウントは外部からの不正アクセスに悪用されないよう、特に注意が必要となります。

準備、対応のポイント

- システムの利用者情報は定期的に確認し、不要なIDを無効化、削除し、台帳等に記録してください。
- 利用者IDの停止や削除に関する手順を定め、運用管理を実施してください。
- 運用管理規程に利用者管理、退職等で使用しなくなるアカウント管理に関する規程を定めておきましょう。
- システム調達の際は、提案依頼書や要求仕様書に必要要件として明示するよう規程で定めておきましょう。

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または無効化している。(2-⑤)

●利用者 ID 台帳の例

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

No.	利用者属性	性	名	電話番号	ユーザ ID	説明	権限	状態
001	薬剤師	abc	def	****	abc@def	使用者	Admin	使用可
002	非常勤薬剤師	efg	hij	****	efg@hij	使用者	User	使用可
003	事務	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23 年３月まで）
004	非常勤事務	qrs	tuv	****	qrs@tuv	使用者	User	使用可

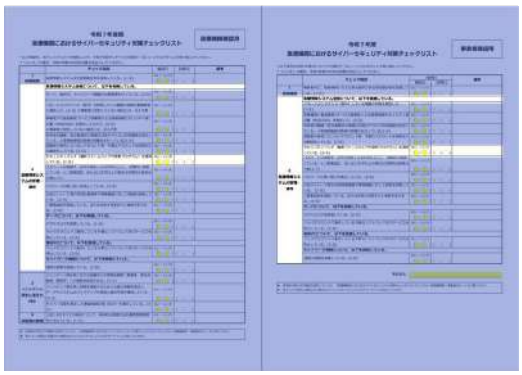
記録保存、関連付けの維持の関係で、ID情報を残しておかなければならないような状況では「無効化」などの設定でアクセスに利用できない設定とし、離籍していることがわかるよう管理してください。

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。

利用者IDの停止・無効化や、定期的な利用者IDの棚卸しを実施など、規程に定めておきましょう。

リモート保守に携わっていた職員が退職した際の注意点

個人アカウントを付与していた場合はアカウントの削除/無効化を、共用IDの場合は認証情報の更新を必ず行なってください。



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

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。(2-⑥)

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。(2-⑥)

マニュアルの解説要約

不正ソフトウェアの対策は、パターンファイル更新や脆弱性に対するセキュリティパッチ適用が重要です。

新規導入・更新時には、保守契約や運用規程を見直し、定期的なパッチ適用体制を整備します。

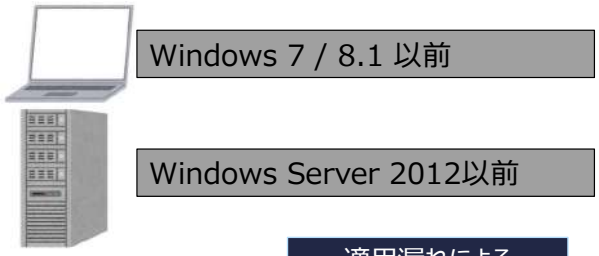
準備、対応のポイント

- OSのセキュリティパッチがリリースされた際に、重要性、影響度についてベンダーと相談、評価しましょう。
- 重要度に応じて更新計画を立てる必要があります。

- ウイルス対策などのセキュリティ対策製品を導入している場合は定義ファイル、ルールDBが公開に合わせて適宜更新されるようにしてください。

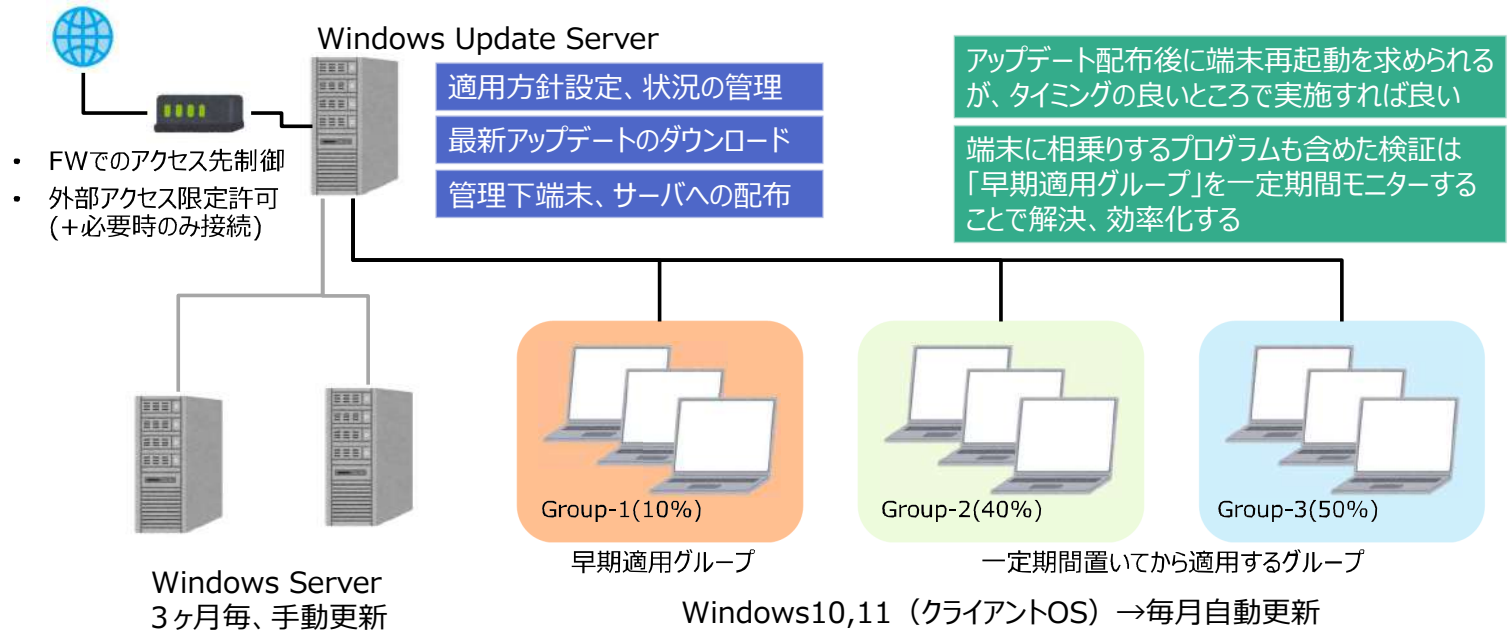
- 運用管理規程にセキュリティパッチの適用方針に関する規程を定めておきましょう。
- システム調達の際は、提案依頼書や要求仕様書に必要要件として明示するよう規程で定めておきましょう。

■ Windows Updateの問題



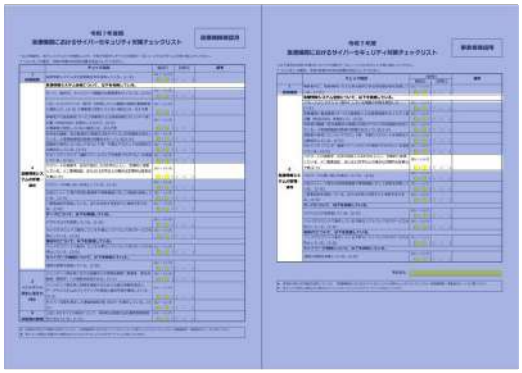
セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-⑥)

■ **Windows Updateの方針を見直していきましょう。**



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。(2-⑥)

バージョン	エディション	メインストリームサポート終了日	延長サポート終了日	備考
Windows 11 24H2	Home / Pro	2026年10月13日	–	最新バージョン
Windows 11 24H2	Enterprise / Education	2027年10月13日	–	長期サポート（1年延長）
Windows 11 23H2	Home / Pro	2025年11月11日	–	まもなく終了
Windows 11 23H2	Enterprise / Education	2026年11月10日	–	
Windows 11 22H2	Home / Pro	2024年10月8日	–	サポート終了済
Windows 11 22H2	Enterprise / Education	2025年10月14日	–	
Windows 11 Enterprise LTSC 2024	Enterprise LTSC	2029年10月9日	–	長期サポート版
Windows 10 22H2	Home / Pro / Enterprise / Education	2025年10月14日	–	サポート終了予定
Windows 10 Enterprise LTSC 2021	Enterprise LTSC	2027年1月12日	–	
Windows 10 IoT Enterprise LTSC 2021	IoT Enterprise LTSC	2027年1月13日	2032年1月13日	IoT向け、最長サポート
Windows 10 Enterprise LTSC 2019	Enterprise LTSC	2024年1月9日	2029年1月9日	延長サポート中
Windows 10 Enterprise LTSB 2016	Enterprise LTSB	2021年10月13日	2026年10月13日	まもなく終了
Windows 10 Enterprise LTSB 2015	Enterprise LTSB	2020年10月13日	2025年10月14日	まもなく終了
Windows 8.1	全エディション	2018年1月9日	2023年1月10日	サポート終了済
Windows 7	全エディション	2015年1月13日	2020年1月14日	サポート終了済
Windows Server 2022	Standard / Datacenter / Essentials / IoT / Storage	2026年10月13日	2031年10月14日	最新サーバーOS。全エディション共通
Windows Server 2019	Standard / Datacenter / Essentials	2024年1月9日	2029年1月9日	メインストリームサポート終了済、延長サポート中
Windows Server 2016	Standard / Datacenter / Essentials	2022年1月11日	2027年1月12日	延長サポート中
Windows Server 2012 R2	Standard / Datacenter / Essentials	2018年10月9日	2023年10月10日	サポート終了。ESUで最大2026年10月13日まで延長可能
Windows Server 2012	Standard / Datacenter / Essentials	2018年10月9日	2023年10月10日	サポート終了。ESUで最大2026年10月13日まで延長可能
Windows Server 2008 R2	Standard / Enterprise / Datacenter / Itanium	2015年1月13日	2020年1月14日	ESUにより最大2024年1月9日まで延長可能（Azure限定）
Windows Server 2008	Standard / Enterprise / Datacenter / Itanium	2015年1月13日	2020年1月14日	ESUにより最大2024年1月9日まで延長可能（Azure限定）



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。
※二要素認証、または13文字以上の場合は定期的な変更は不要(2-⑦)

パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要(2-⑦)

追加

マニュアルの解説要約

パスワードは出荷時のものから変更し、推定困難なものを設定・管理する必要があります。

サーバやネットワーク機器のパスワードも対象で、事業者の設定内容を確認・点検します。

13文字以上や二要素認証等を用いる場合は、定期変更は必須ではありませんが、使い回しは厳禁です。

準備、対応のポイント

- OS、ソフトウェア、ネットワーク機器など全てにおいて、認証にパスワードを使用する場合の基本ルールを規程に定めましょう。
- 安全なパスワードが適用されるよう、システムでのポリシー設定や、利用者への周知、教育を行いましょう。
- 運用管理規程に利用者管理、パスワードに関する規程を定めておきましょう。
- システム調達の際は、提案依頼書や要求仕様書に必要要件として明示するよう規程で定めておきましょう。

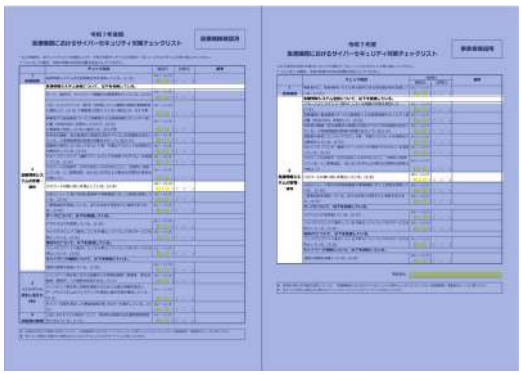
パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。
※二要素認証、または13文字以上の場合は定期的な変更は不要(2-⑦)

本チェックリストのマニュアルで示されている強固なパスワードの例

- 英数字、記号を混在させた13 文字以上の推定困難な文字列
- 英数字、記号を混在させた８文字以上の推定困難な文字列を定期的に変更させる
- 二要素以上の認証の場合、英数字、記号を混在させた８文字以上の推定困難な文字列
- 複数の機器や外部サービス等で、同一のパスワードを設定しない

システム内部連携等で使用されるアカウントでは極力長いパスワードを設定する

攻撃に悪用されるポイントとして特に重要



【医療機関等確認用・事業者確認用】

2 医療情報システムの管理・運用（医療情報システム全般）

パスワードの使い回しを禁止している。(2-⑧)

パスワードの使い回しを禁止している。(2-⑧) 追加

マニュアルの解説要約

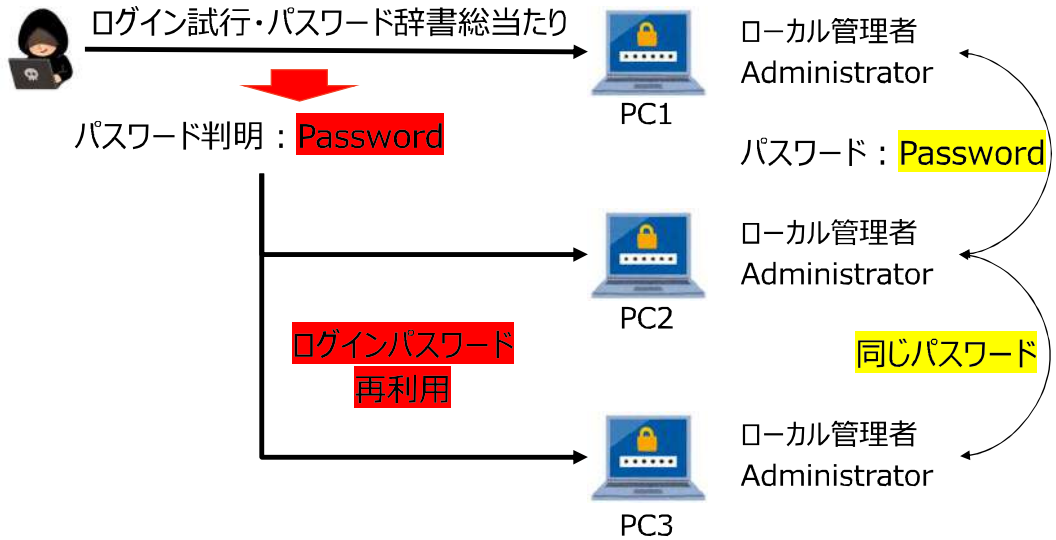
パスワードの使い回しは発覚時、漏えい時の被害拡大につながるため避ける必要があります。

事業者の導入先、保守先である医療機関内の機器で使い回しにも注意が必要です。

準備、対応のポイント

- OS、ソフトウェア、ネットワーク機器など全てにおいて、認証にパスワードを使用する場合の基本ルールを規程に定めましょう。
- 安全なパスワードが適用されるよう、システムでのポリシー設定や、利用者への周知、教育を行いましょう。
- 運用管理規程に利用者管理、パスワードに関する規程を定めておきましょう。
- システム調達の際は、提案依頼書や要求仕様書に必要要件として明示するよう規程で定めておきましょう。

パスワードの使い回しを禁止している。(2-⑧)



対策 管理者パスワードの使い回しをしないこと / ログイン連続失敗回数によるロックアウトを有効にすること

令和7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

立入検査研修
医療機関向けコース

前編終了