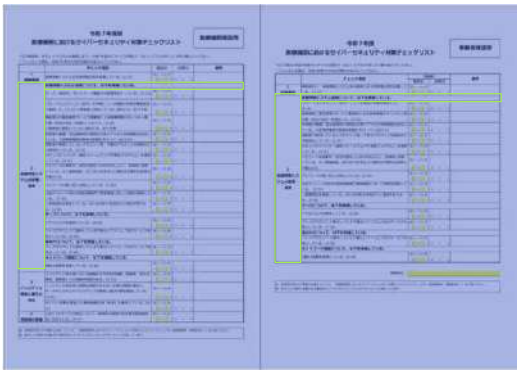
令和7年度医療情報セキュリティ研修
及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業

立入検査研修
医療機関向けコース
後編

一般社団法人ソフトウェア協会

目次



【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）

USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。（2-⑨）

USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。（2-⑨） 追加

マニュアルの解説要約

USBストレージ等の外部接続機器はマルウェア感染拡大を防ぐため接続制限が必要です。

業務で使用する場合は、機器の限定やウイルススキャン、管理規程の整備が求められます。

事業者は接続制限の実施状況やシステム機能について医療機関に情報提供する必要があります。

準備、対応のポイント

- 外部記憶媒体を使用する場合の基本ルールを規程に定めましょう。
- 関係者への周知、教育を行いましょう。

- 許可の無い機器の接続を防止し、許可された機器のみに接続を制限する仕組みを整備してください。

- 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。

USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。(2-⑨)

利用者対象のルールによる制限（運用管理規程等＋教育）

システムによる規制-端末毎の外部デバイス制限

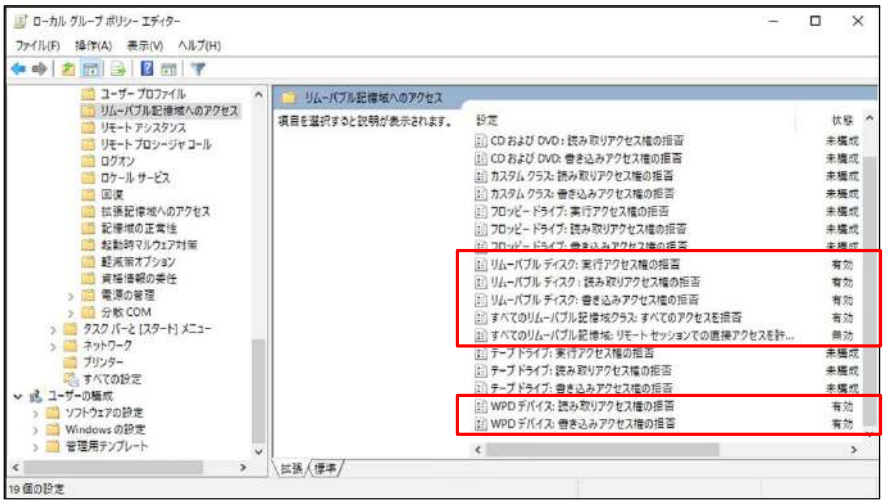
システムによる規制-USBメモリ個体番号による接続可否制御

Windows標準機能で可能

種類	例
USBメモリ	フラッシュメモリ型USBスティック
外付けHDD（ハードディスク）	USB接続の外付けハードディスク
外付けSSD	ポータブルSSD
SDカード・microSDカード	各種メモリカード

デバイス制御ソフト
or
セキュリティ対策ソフト、
資産管理ソフト

USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。(2-⑨)



[ローカルコンピューターポリシー]>[コンピューターの構成]>[管理用テンプレート]>[システム]>[リムーバブル記憶域へのアクセス]

Windowsローカルグループポリシーの例
-タスクバーの検索ボックスで「gpedit.msc」と入力、「Enter」押下し、ローカルグループポリシーエディターを起動

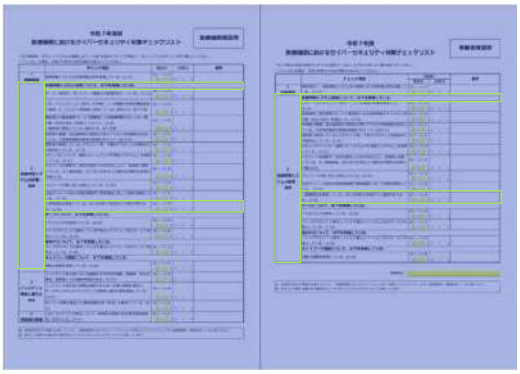
Windowsドメインポリシーの例
-ドメインコントローラにてタスクバーの検索ボックスで「gpmc.msc」と入力して起動

➡ USBストレージ等のアクセス制御

➡ Windows Portable Device* のアクセス制御

注意
- メモリ個別の制御ではなく一律の制限
- 個別の接続可否は機能を備えたソフトが必要

＊ Windows Portable Device ：スマートフォン、デジタルカメラ、音楽プレーヤー等のポータブルデバイス



【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）

二要素認証を実装している。
または令和９年度までに実装予定である。(2-⑩)

二要素認証を実装している。または令和９年度までに実装予定である。(2-⑩)

追加

マニュアルの解説要約

令和9年度に稼働予定の医療情報システムには、二要素認証または同等の対応が求められます。

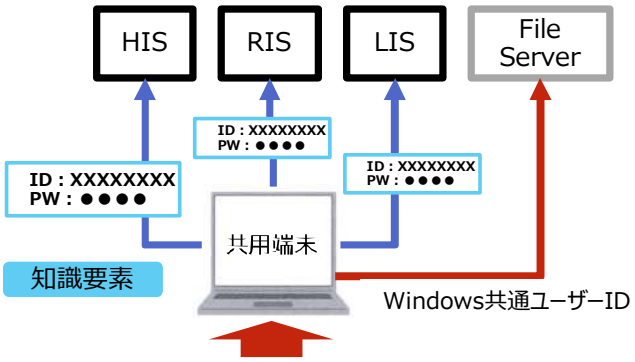
導入には費用がかかるため、計画的な更新が推奨されます。

準備、対応のポイント

- 現行システムで採用できていない場合は、一般的に安全とされるパスワードや、マニュアルで示される強固なパスワードを適用してください。
- 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、認証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。

二要素認証を実装している。
または令和９年度までに実装予定である。(2-⑩)

共用端末とシステム個別認証

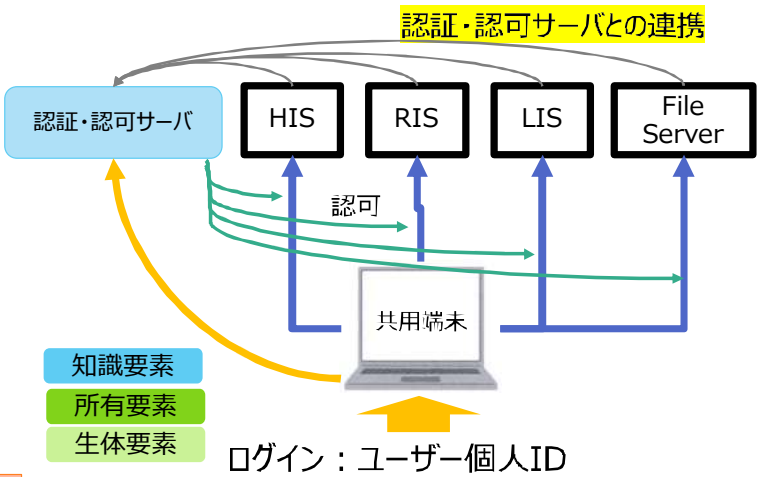


ログイン：共通ユーザーID
認証：なし（自動ログイン）

まずは「安全なパスワード」の使用を徹底

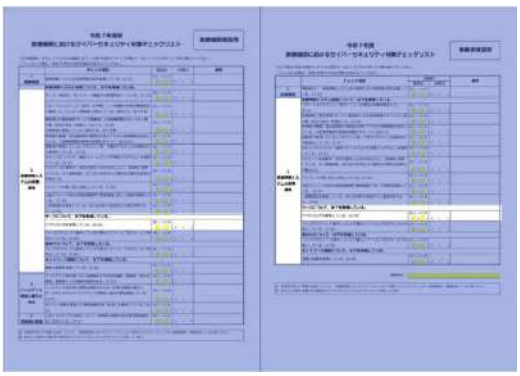
個別に二要素認証を導入するのは非効率

端末ログインでの二要素認証とシステム連携



ログイン：ユーザー個人ID
認証：二要素認証

端末における個人認証と、システム利用認可を連携、統合する環境により、利用者の効率とセキュリティを両立



【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（サーバ）

アクセスログを管理している。(2-⑪)

アクセスログを管理している。(2-⑪)

マニュアルの解説要約

利用者のアクセスログを記録し、定期的に確認してください。

ログは不正アクセスの追跡に役立ち、ログイン時刻・操作内容などを記録する必要があります。

不正なログ改ざんや削除を防ぐため、アクセス制限などの保護対策も求められます。

準備、対応のポイント

- 医療システム・アプリケーションのアクセスログは医療情報の真正性を裏付ける証跡となります。
- OSのイベントログ、セキュリティログでは、デスクトップログインやリモートログインの成功、失敗等、様々な履歴が残るためサイバー攻撃対策の観点で特に重要です。

- 医療情報自体の保全は法定保存年数以上または民訴時効年数以上、ログの保全も同様の期間を確保する必要があります。

- 保存先をシステム内部としている場合は、安全な外部サーバや媒体等へ定期的にバックアップしましょう。
- ログ管理サーバへ転送するシステム構成は、管理の効率化、ログデータの保護強化の対策となります。

- 運用管理規程にログの保全、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。

ログ管理が必要な機器

- 十分な容量、保存期間を確保
- それぞれの機器、システムで管理

ログの集中管理

ログ管理サーバ
（Syslog等）

- 個別に用意するとコスト高になる場合がある。
- システムと切り離しインフラ全体の機能として検討することも一案。

ログの保全・保護

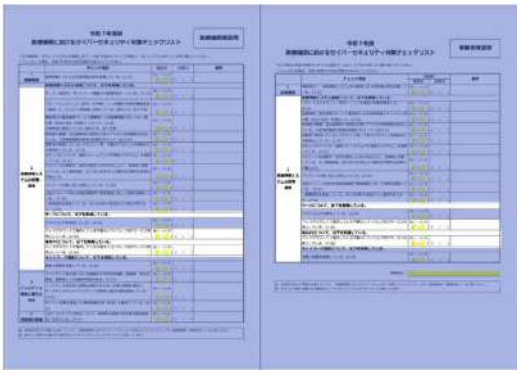
- 証拠としてのログを安全に残し、改ざんや消失を防ぐ

容量の監視

- ログが溜まりすぎてシステムに悪影響を与えるのを防ぐ

分析・可視化

- ログを整理し、問題の早期発見や改善につなげる



【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（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。(2-⑫)

【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。(2-⑫)

マニュアルの解説要約

脆弱性対策として、未使用のサービスや通信ポートは無効化しておくことが重要です。

システム運用担当者は不要なソフトやサービスの稼働状況を確認し、不要なものがあれば、企画管理者と相談して対応を講じてください。

準備、対応のポイント

- 管理対象の端末やサーバについて、プログラム一覧、稼働サービスの一覧を出力しておくようにしましょう。

- 追加やアップデートを行った際に比較確認することで不審な点はクリアにしましょう。

- 運用管理規程にシステム設定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。

【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。(2-⑫)

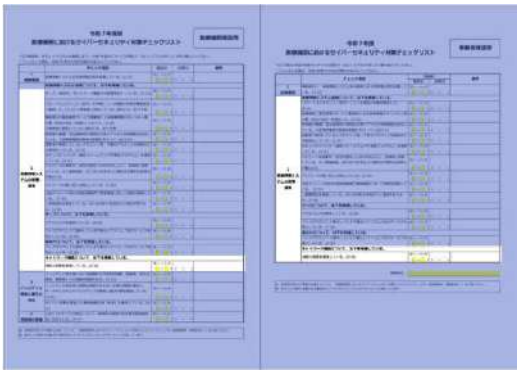
稼働しているサービス一覧を出力する方法（例）

```
PS C:¥Users¥Administrator> Get-Service | Select-Object DisplayName, Status, StartType

DisplayName                                                                  Status StartType
-----------                                                                  ------ ---------
Active Directory Web Services                                               Running Automatic
AllJoyn Router Service                                                      Stopped    Manual
Application Layer Gateway Service                                           Stopped    Manual
Application Identity                                                        Stopped    Manual
Application Information                                                     Stopped    Manual
Application Management                                                      Stopped    Manual
App Readiness                                                               Stopped    Manual
Microsoft App-V Client                                                      Stopped  Disabled
AppX Deployment Service (AppXSVC)                                           Running    Manual

～～省略～～
```

- 資産管理ソフト等で管理する方法を持たない場合でも、OS標準機能で確認はできる。
- システム導入の際は、導入時点のスナップショットとして実行結果の一覧を保存しておくと、後の変更時に実行した結果と比較することが可能となる。

同内容のCSV出力処理

```
> Get-Service | Select-Object DisplayName, Status, StartType | Export-Csv -Path "service_list.csv" -NoTypeInformation
```

【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（ネットワーク機器）

接続元制限を実施している。(2-⑬)

接続元制限を実施している。(2-⑬)

マニュアルの解説要約

外部ネットワーク接続は、適切な機器設定と監視が必要です。

無線LAN使用時は、適切な利用者以外のアクセス防ぐため、アクセス制限が必要です。

準備、対応のポイント

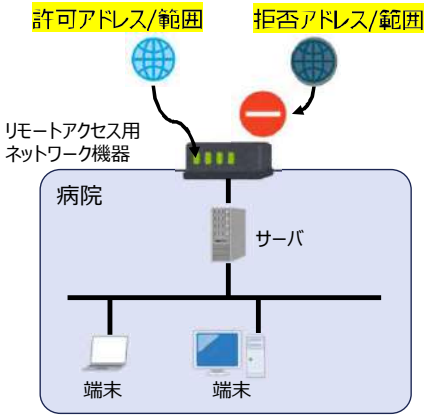
- リモートアクセス機器に接続してくる外部の接続元を固定アドレスに制限できるか。
  または、国、地域のアドレス範囲に制限できるか。

- ネットワークへの接続の際、認められた端末、機器のみに制限する仕組みがあるか。

- 運用管理規程に内外のネットワーク接続に関する規程を定めておきましょう。
- ネットワーク構築の調達の際は、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。

接続元制限を実施している。(2-⑬)

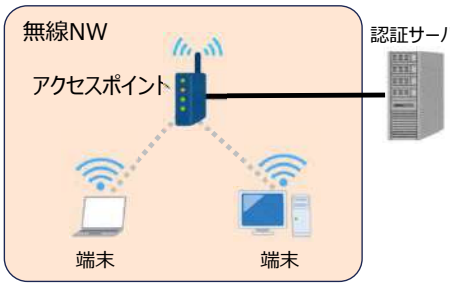
【外部】国、地域や、特定アドレスのみを接続許可する



ジオブロック：
グローバルIPアドレスは国や地域ごとにアドレス範囲が規定されている。海外からのアクセスは不要なら受け付けないようにする。

IPアドレス制限：
接続可能なグローバルIPアドレスを限定する。

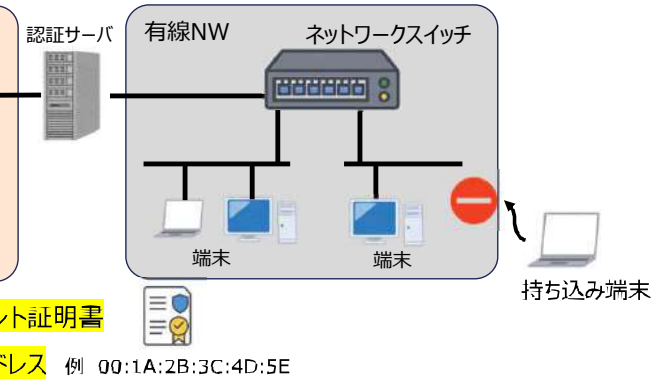
【内部】無線LANへの接続手順を強化する



WPA/WPA2/WPA3パーソナル：
SSIDとパスコードを知っていれば接続できる簡便さはあるが、認められた端末のみに制限するための識別ができていない。

WPA/WPA2/WPA3エンタープライズ：
企業や組織向けの無線LAN認証方式で、ユーザーや端末ごとにIDとパスワード（または証明書）で認証を行う。802.1X認証によりセキュリティを強固にできる。

【内部】有線LANへの接続制限を強化する

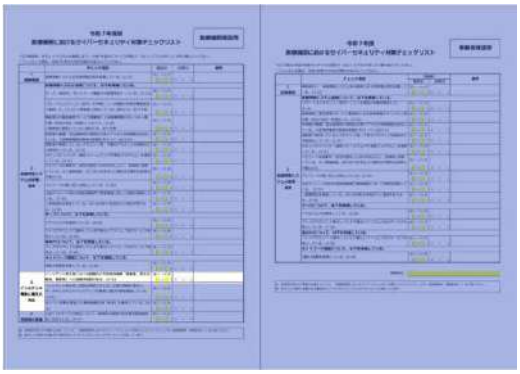


クライアント証明書

MACアドレス　例　00:1A:2B:3C:4D:5E

有線LAN：
LANケーブルを繋げばネットワークに繋がるのは簡便だが不正接続が起こりやすい。
認められた端末を識別できない。

認証スイッチ：
802.1X認証を使用する方法、独自のネットワーク管理による方法がある。



【医療機関等確認用】

3 インシデント発生に備えた対応

インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-①)

インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-①)

マニュアルの解説要約

事業者や有識者との情報共有体制の整備

緊急連絡網を含む連絡体制図の作成

準備、対応のポイント

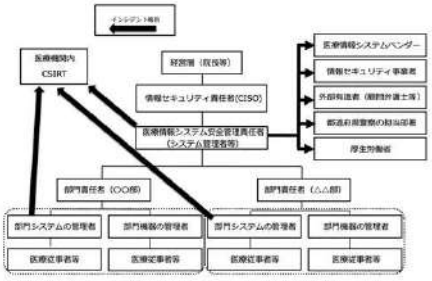
- 緊急時の連絡網、体制図を作成し、最新情報となるよう管理しましょう。

- セキュリティインシデントの際に協力要請する事業者や専門家はあらかじめ想定しておく必要があります。
- タイミングによっては対応が得られないこともあるため、可能な限り複数の協力先を想定してきましょう。

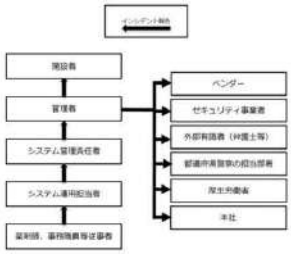
- 緊急時の体制や対応方針など、運用管理規程を定めておきましょう。

インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-①)

●連絡体制図の例１（医療機関）



●連絡体制図の例２（薬局）



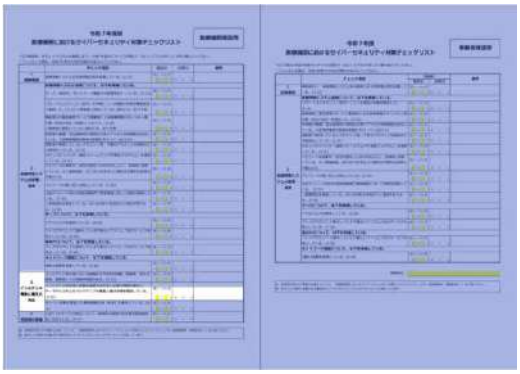
【外部連絡リスト】

No	カテゴリ	組織名	担当者名	電話番号
1	厚生労働省	医療情報担当参事官室		03-6812-7837
2	都道府県、政令市	地域医療政策部門		
3	保健所	所管保健所		
4	警察	サイバー対策課		
5	個人情報漏洩報告(疑い含む)	個人情報保護委員会	様式、申請フォーム、詳細説明等は個人情報保護委員会Webサイトへ。*	
6	システム事業者	A社		
7	システム事業者	B社		
8	近隣施設	X総合病院		
・	・	・	・	・

異動や担当変更などに注意し、最新にアップデートしましょう。

自組織内だけでなく、連絡先組織側の変更にも注意しましょう。

＊ 個人情報保護委員会　漏えい等の対応とお役立ち資料
https://www.ppc.go.jp/personalinfo/legal/leakAction/



【医療機関等確認用】

3 インシデント発生に備えた対応

インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)

インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)

マニュアルの解説要約

非常時に備え、システムやデータのバックアップと復旧手順の整備が必要です。

重要データは不正ソフトウェアの影響を防ぐため、複数方式で世代管理を行い、バックアップは手順に沿って確保します。

復旧方法はBCP(事業継続計画)等に明記し、手順を定めておく必要があります。

準備、対応のポイント

- 運用管理規程で等でデータ保全の対象となるデータ、システム停止状況における最低限の診療継続のために必要とされるデータを定義し、目的に応じたバックアップ計画を定めましょう。（現用の復旧、予備系での縮退稼働、媒体や紙への出力など）
- 重要度の高いデータは3-2-1ルールに従いオフサイトまたはオフラインへ保存する構成にしましょう。

- システム復旧手順を定め、バックアップデータからの復旧ができることを確認しましょう。
最低限はシステム導入時、可能であれば定期的に確認することを規程し、実施の確認を行いましょう。

- バックアップデータが適切に保存されているか、定期的に確認しましょう。

インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)

サイバー攻撃によって被害が及ぶ可能性の低い、離れた場所へのバックアップ

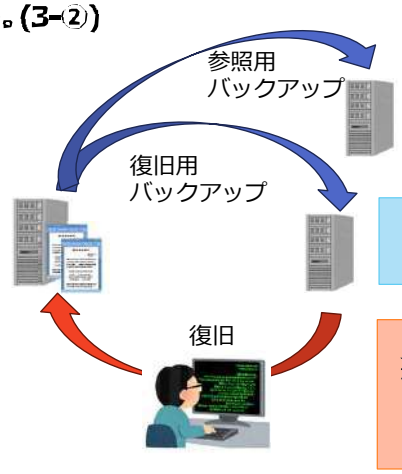
- オフライン環境
- オフサイト環境
- クラウド環境（接続方法やタイミングには注意が必要）

書き換えが困難な媒体へのバックアップ

- イミュータブルストレージ（Write Once Read Many-WORM）
- テープや一時接続のUSBストレージなどの外部媒体

システムを早期復旧するための復旧手順の確認、訓練

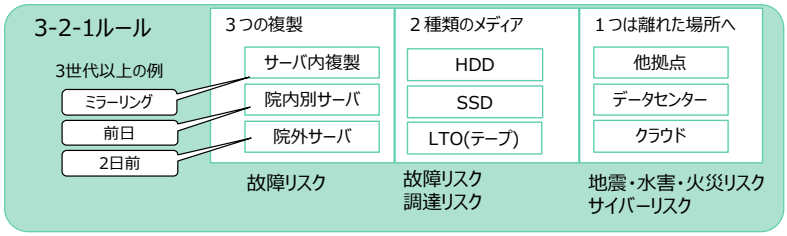
- 復旧の優先順位付けを行う
- 事業者に対応方法を確認する
- 復旧手順の文書化（有事の際に確認できる管理方法）

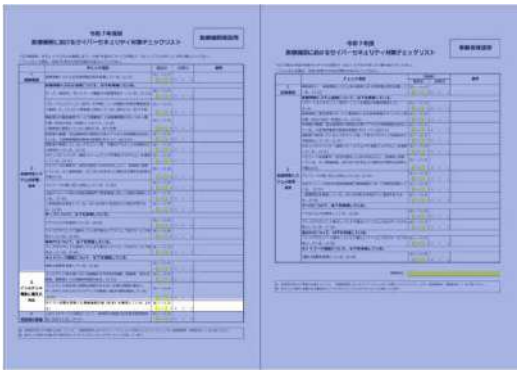


非常時参照用バックアップを準備している場合、更新確認、機能確認されているか。

対象データのバックアップは正常に保管されているか

バックアップからの復旧手順は確認されているか
・システム導入時
・定期演習、確認





【医療機関等確認用】

3 インシデント発生に備えた対応

サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-③)

サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-③)

マニュアルの解説要約

非常時の業務継続判断や対応方針の整備が必要です。

サイバー攻撃を想定したBCP（事業継続計画）の整備が必要です。

サイバー攻撃などによる障害によって、重要業務が中断しない、または中断しても短い期間で再開できるようにするための準備です。

準備、対応のポイント

- 想定される事業リスクに、サイバー攻撃によるシステム停止を含めた計画を準備しましょう。
- 対処に遅れが生じないよう、サイバー攻撃を含むBCP発動の判断基準を定め規程しましょう。

サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-③)

- 事業継続計画（Business Continuity Planning）とは？
  - 大規模災害等の発生時にも医療を継続的に提供できるようにするための計画です。
  - サイバー攻撃による被災を含めたBCPについて作成または見直す必要があります。
- 参考情報として、厚生労働省がサイバー攻撃を想定した事業継続計画（BCP）策定の確認表等を公開しています。

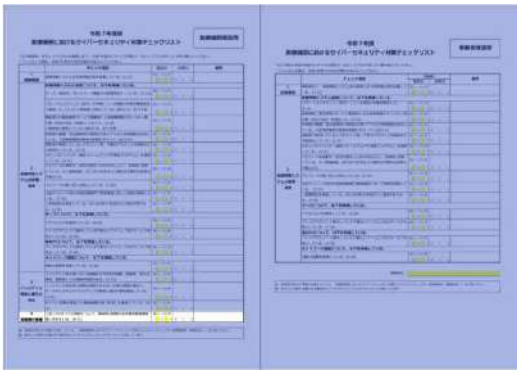
サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表のための手引き（令和６年６月）
- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表（PDF）（令和６年６月）
- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表（Excel）（令和６年６月）

- 【薬局用】サイバー攻撃を想定したBCP策定の確認表のための手引き（令和６年６月）
- 【薬局用】サイバー攻撃を想定したBCP策定の確認表（Excel）（令和６年６月）

- 医療情報システム部門等におけるBCPのひな形（PDF）（令和６年６月）
- 医療情報システム部門等におけるBCPのひな形（Word）（令和６年６月）


サイバー攻撃を想定した事業継続計画（BCP）策定の確認表



【医療機関等確認用】

4 規程類の整備

上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)

上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)

追加

マニュアルの解説要約

医療情報システムの安全管理には、明文化されたルールの策定が必要です。

機器管理、異常時対応、職員教育などを定め、管理します。

準備、対応のポイント

- 方針、規程、体制図や連絡網等の文書は職員が適宜参照できる状態になっている必要があります。（共有サーバや印刷物での保管など）
- 医療情報システム安全管理責任者が方針、規程等の策定、対策推進の責任者です。（規程文書管理も含め）
- システム管理における機器台帳等は企画管理者（システム管理者）が最新情報を管理する必要があります。

上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)

医療情報システム 運用管理規程（項目例）

章番号	見出し	チェックリスト該当項目
第1章	総則	
第2章	組織体制と責任	• 医療情報システム安全管理責任者を設置している。(1-①)
第3章	機器・資産の管理	• 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) • 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) • 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)
第4章	アカウント・アクセス権限の管理	• 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) • 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) • 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) • パスワードの使い回しを禁止している。(2-⑧) • 二要素認証を実装している。または令和９年度までに実装予定である。(2-⑩)
第5章	データ管理	• アクセスログを管理している。(2-⑪) • インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)

上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)

医療情報システム 運用管理規程（項目例）

章番号	見出し	チェックリスト該当項目
第6章	ネットワーク接続管理	• 接続元制限を実施している。(2-⑬)
第7章	外部記憶媒体の利用管理	• USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。 (2-⑨)
第8章	ソフトウェア管理と脆弱性対策	• 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) • サーバ／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。(2-⑫) • 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。(2-⑫)
第9章	保守・委託業務管理	• 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) • 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)
第10章	インシデント対応	• インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡**体制図**がある。(3-①) • インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②) • サイバー攻撃を想定した**事業継続計画（BCP）**を策定している。(3-③)
第11章	教育・訓練	• インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②) • サイバー攻撃を想定した**事業継続計画（BCP）**を策定している。(3-③)
第12章	規程の見直し、監査	

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
後編

終了