令和6年度情報セキュリティ研修会

2024/11/23

情報セキュリティシニアコンサルタント　中島 明彦

アジェンダ

Ⅰ　開会

Ⅱ　研修会

（講演）国保組合及び調剤薬局における業務運用リスクと情報セキュリティ対策について

Ⅲ　質疑応答

＜事前質問＞

1　バックアップは、１日に何回位取られてますか？

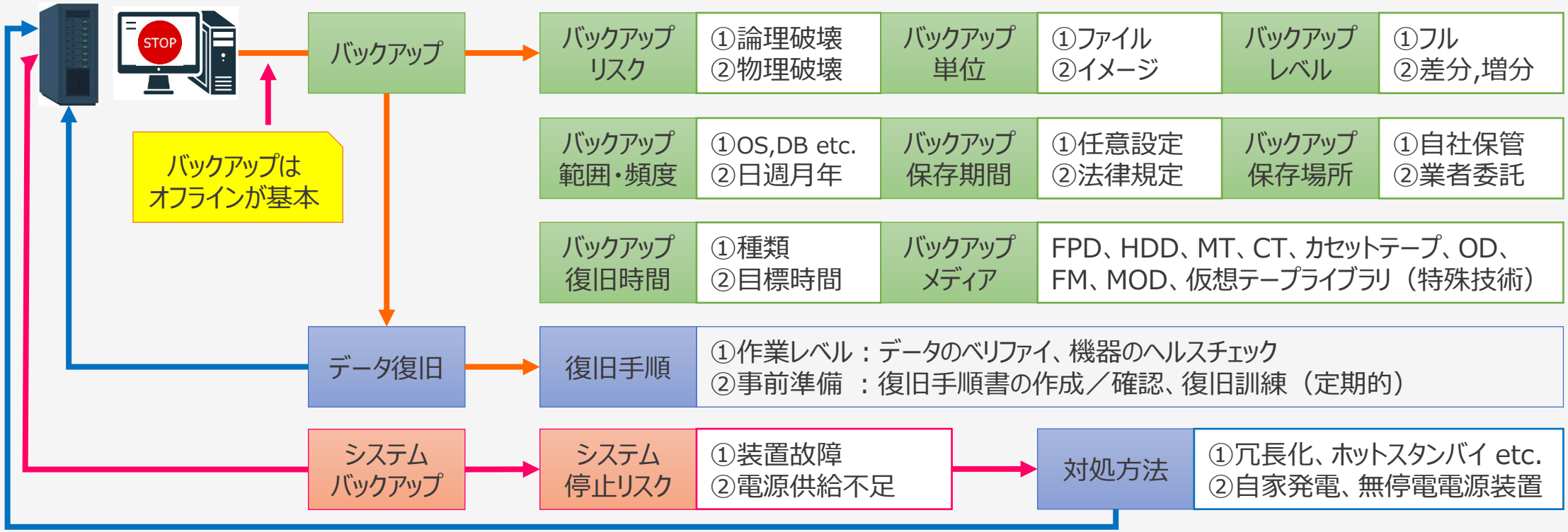
2　立入検査時対応について
小規模の個人薬局において、サイバーセキュリティ対策チェックリストは「薬局確認用」だけでよいと思うが、今後の対応として、事業者との契約は必要か？

Ⅳ　閉会

質疑応答

1．バックアップは、1 日に何回位取られてますか？

　バックアップ（英: backup）とは、コンピュータシステムで主にデータやシステムの状態を複製し、問題発生時の復旧（リストア）に備えることです。



質疑応答

２．立入検査の対応

① 事前に連絡が入る
⇒〇年〇月〇日に立入検査をしますので準備しておいてくださいと連絡が来る

② 厚生労働省の役人が来る
⇒通常２人が多い

③ 薬局の誰に質問されるかを想定しておく
⇒薬局の職員に質問されることを想定し、職員全員にサイバー対策チェックリスト対策の内容を理解させる

④ 何を質問するのか、何を見るのか？
⇒チェックリストや連絡表を見に来るのではなく、サーバーセキュリティ対策ができているかを現場確認する
※本日の話を必ず職員に周知徹底し、各薬局での情報セキュリティ対策を具体的に始めてください。

医療情報システムの安全管理に関するガイドライン　第6.0版（令和5年5月）に記載された「情報セキュリティ対策基準」に基づき質問と現場確認を実施する

サーバーセキュリティインシデントが発生したら

３．サイバーセキュリティが発生したら
　　情報セキュリティインシデントが　・・・　発生した？　発生したかも？　のレベルで「速報」として連絡する所は・・・

サイバーセキュリティ対策通信
大阪府警察本部サイバーセキュリティ対策課

電話番号：06－6943－1234

※　各薬局のサイバーセキュリティ体制連絡体制図の外部関係機関の連絡先一覧表に記入し、まず一報を入れましょう。

「医療情報システムの安全管理に関するガイドライン第6.0版」の主な改正ポイント（チェックリスト確認の事前準備）
（https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html）

医療情報システムの安全管理に関するガイドライン　第6.0版（令和5年5月）

第２ 改定の概要

１．全体構成の見直し

本文を、概説編、経営管理編、企画管理編及びシステム運用編に分け各編で想定する読者に求められる遵守事項及びその考え方を示すとともに、**Q&A 等において現状で選択可能な具体的な技術にも言及**するなど、構成の見直しを行う。

２．外部委託、外部サービスの利用に関する整理

クラウドサービスの特徴を踏まえたリスクや、対策の考え方を整理するとともに、**医療機関等のシステム類型別に責任分界の考え方等を整理**する。

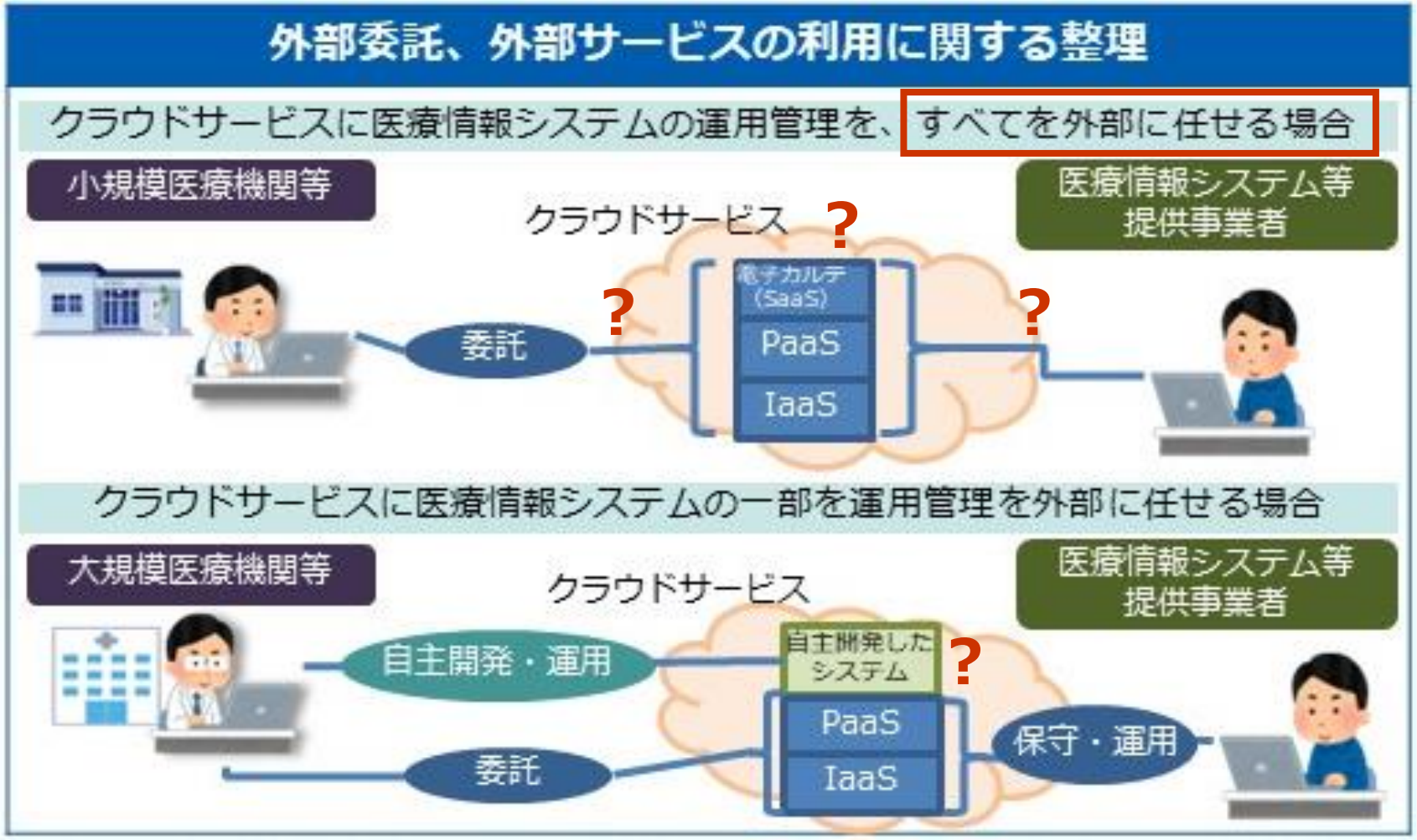
３．情報セキュリティに関する考え方の整理

ネットワークの安全性の考え方や認証のあり方を踏まえて、ゼロトラスト思考に則した対策の考え方を示すほか、サイ　バー攻撃を含む非常時に対する具体的な対応について整理する。

４．新技術、制度・規格の変更への対応

オンライン資格確認の導入に必要な**ネットワーク機器等の安全管理措置等**について整理する。

① 医療情報システムの安全管理に関するガイドラインの主な改正ポイント

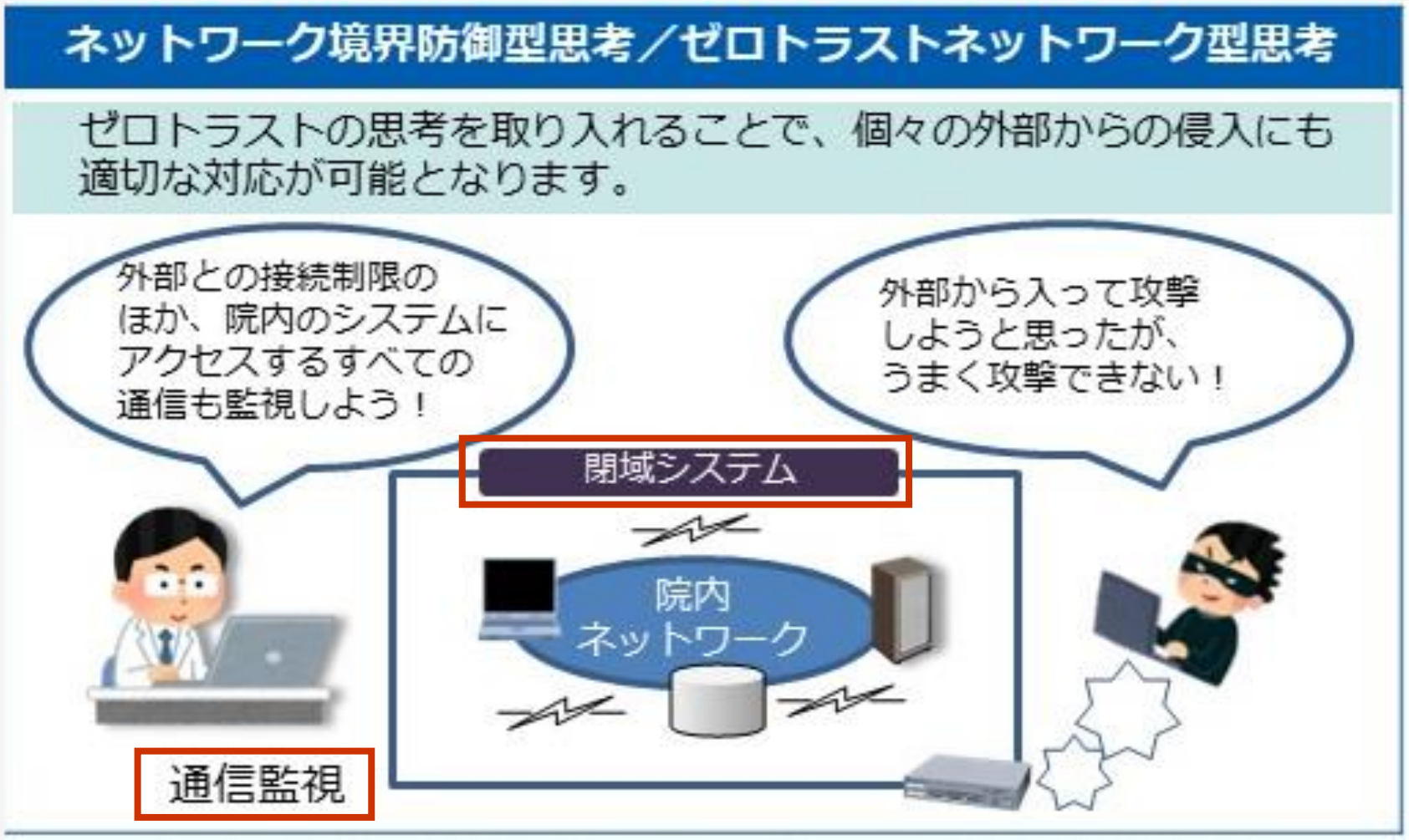


① クラウドサービスの特徴を踏まえたリスクや対策の考え方を整理する。

② 医療機関等のシステム類型別に責任分界の考え方等を整理する。

「クラウド」とは、インターネット経由でのWebサービス利用をする環境の総称です。クラウドサービスの種類は①SaaS ②PaaS ③IaaSの3種類に分類されます。

② 医療情報システムの安全管理に関するガイドラインの主な改正ポイント

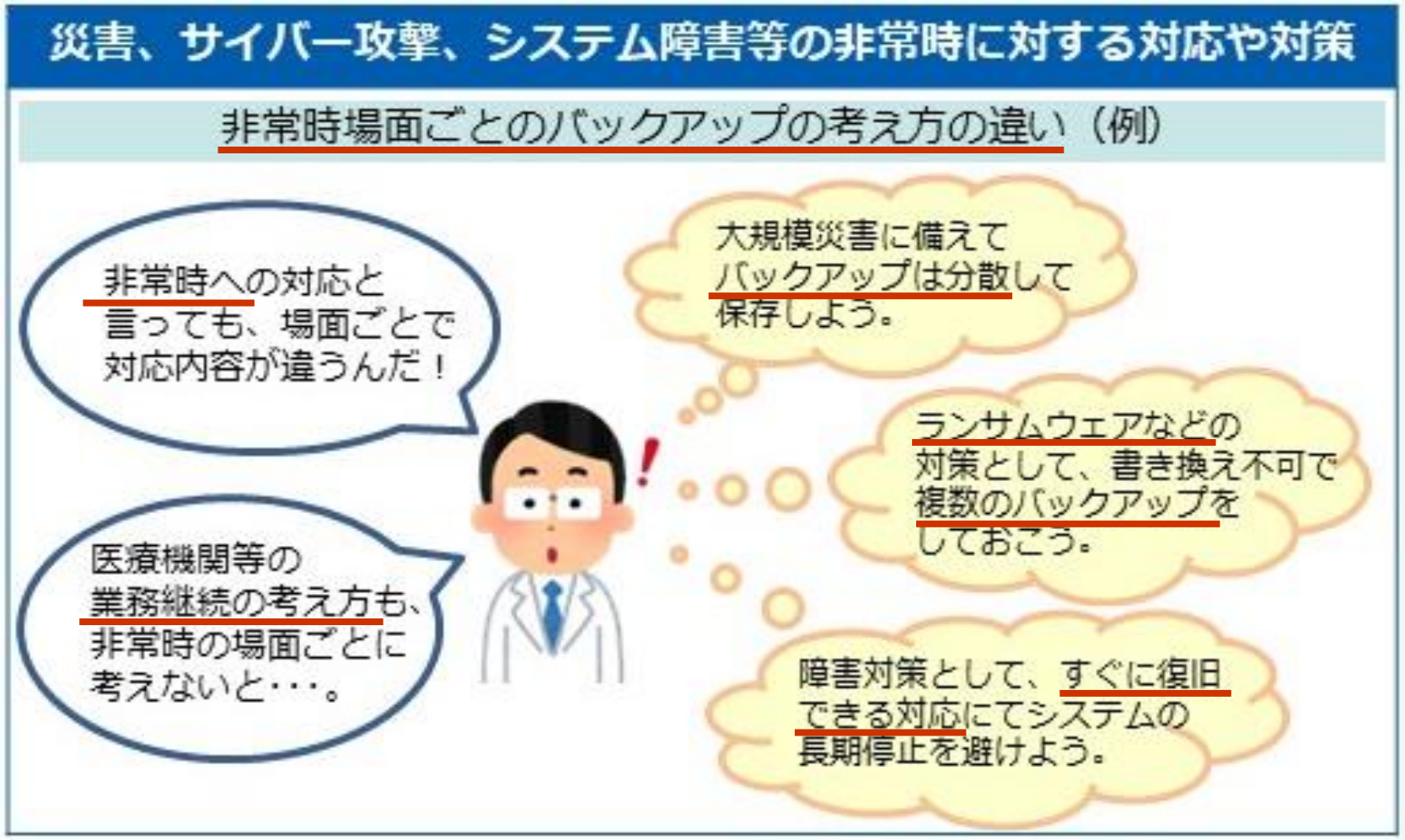


① ネットワークの安全性の考え方や認証のあり方を踏まえて、ゼロトラスト思考に則した対策の考え方を示す。

認証とは対象の正当性や真正性を確かめることです。

IT分野では相手が名乗った通りの本人であると何らかの手段により確かめる本人確認（相手認証）のことを単に認証という場合が多いです。

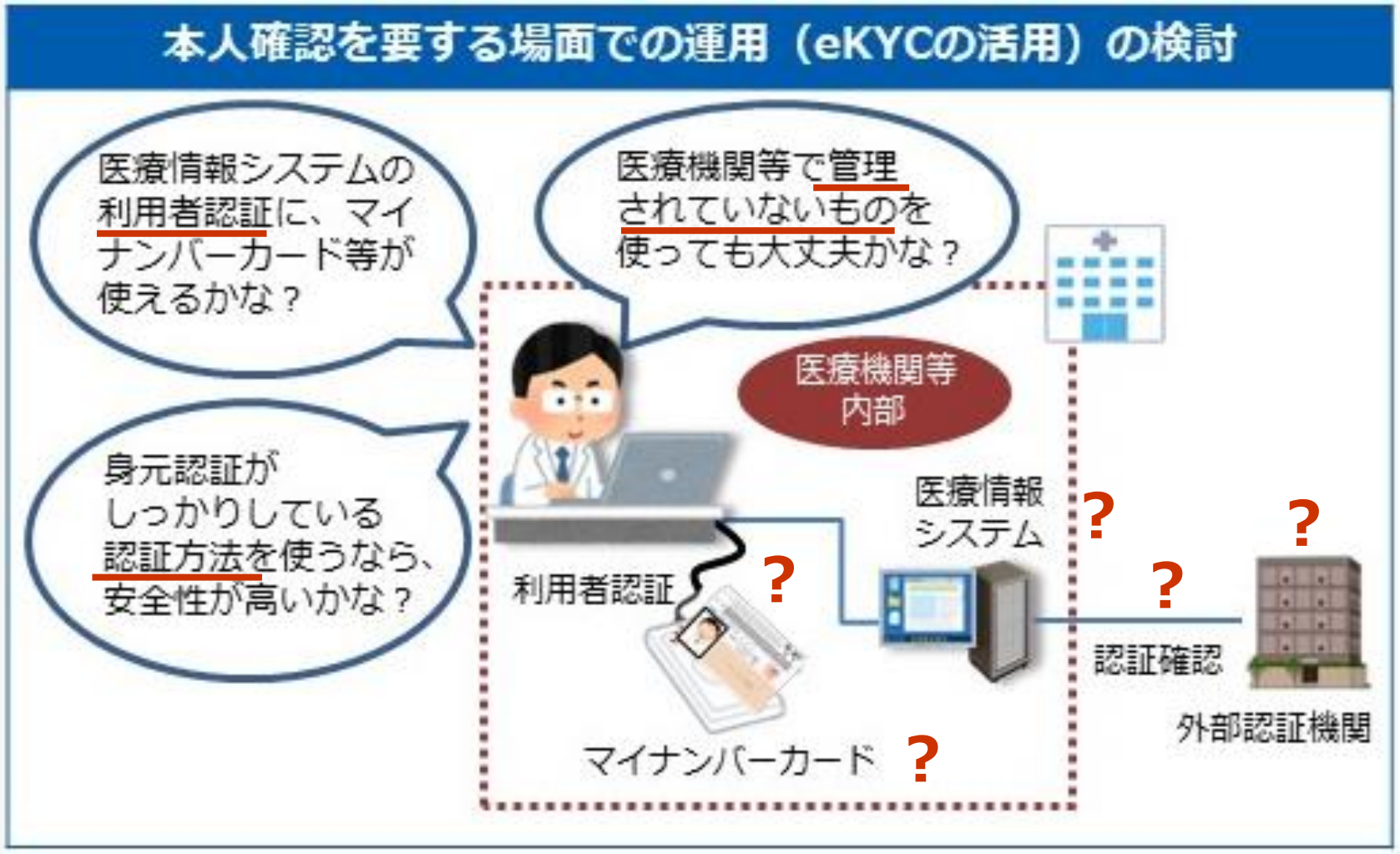
③ 医療情報システムの安全管理に関するガイドラインの主な改正ポイント



① サイバー攻撃を含む非常時に対する具体的な対応について整理する。

日本薬剤師学会のHP HOME＞薬局関連情報＞ 医療情報システムの安全管理についてに記載されているサイバーインシデント発生時の事業継続計画（BCP）薬局向け雛形（日本薬剤師会作成）を確認してください。

④ 医療情報システムの安全管理に関するガイドラインの主な改正ポイント



① オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置等について整理する。

薬局にマイナンバーカードを持参された方の資格確認とレセプト請求（12月1日まで）については、厚労省のホームページを確認下さい。
https://www.mhlw.go.jp/stf/newpage_08280.html

マイナンバーカードによるオンライン資格確認を行うことができない場合の対応について

マイナンバーカードあり

リーダーで
読み込む

確認できた

認証OK

❶

確認
できない

マイナポータルログイン

確認
できた

❷

マイナポータルからダウンロードしたPDFファイルも可

マイナポータル画面
にログインできない

マイナンバーカードなし
（保険証あり）

❸

マイナンバーカードなし
（保険証なし）

過去の受診で必要情報を把握していれば患者への口頭確認で可

❹

過去受診からも
確認できない

被保険者資格申立書
＋
マイナンバーカード

❺

※申立書の場合は支払いを
受けたのちの事後確認

患者には適切な自己負担分の支払いを求める

❶ ❷ ❸

①左記の方法で、確認した被保険者番号等を入力してレセプト請求をしてください。

※オンライン資格確認等システムから、資格情報をダウンロードしておくことで、事後的に被保険者番号等の確認が可能です。

❹ ❺

以下①-②-③の順に可能な方法を選択してレセプト請求をしてください。

① 患者からの聞き取りや過去の受診歴等から確認できた「現在」の被保険者番号を入力する。

② オンライン資格確認における「資格（無効）」画面や過去の受診歴等から確認できた「過去」の被保険者番号を入力する。

⇒資格無効の場合には喪失した「旧資格情報」で請求してください。

③ 被保険者資格申立書に記入された患者の住所・連絡先等を摘要欄に記載の上、被保険者番号等は不詳として「７」を必要な桁数分入力する。

⇒資格情報なしの場合には「不詳レセプト」として請求をしてください。

医薬品、医療機器等の品質、有効性及び安全性の確保等法律
昭和三十五年八月十日法律、第百四十五号に基づく立入検査

https://www.mhlw.go.jp/web/t_doc?dataId=81004000&dataType=0&pageNo=1

① 医薬品、医療機器等の品質、有効性及び安全性の確保等法律に基づく立入検査

薬機法（医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律）に基づく立入検査では、薬局においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。

立入検査では「薬局確認用」、「事業者確認用」の全ての項目について、**１回目の確認の日付と回答等が記入されていることを確認**します。

※このうち、３(1)の**連絡体制図は現物を確認します**。

薬局におけるサーバーセキュリティ対策チェックリストを用いて、日頃からサイバーセキュリティ対策の状況を確認することが重要です。なお、薬局は各事業者からチェックリストを回収しておきましょう。

※事業者と契約していない場合には、「薬局確認用」２(2)及び２(3)についての確認は求められません。

薬局用
チェックリスト

・確認日付
・回答記入

＋

連絡体制図

・連絡先記
・電話番号
・担当者名

＋

事業者用
チェックリスト

・確認日付
・回答記入

① 医薬品、医療機器等の品質、有効性及び安全性の確保等法律に基づく立入検査

令和６年度版薬局における**サイバーセキュリティ対策チェックリストマニュアル** ～薬局・事業者向け～は薬局におけるサイバーセキュリティ対策チェックリストをわかりやすく解説するものです。

薬局においても調剤レセプトコンピューターや電子薬歴システム等の医療情報システムが導入されており、**法令やガイドラインに基づき、適切な管理の下でこれらのシステムを利用することが求められています**。

薬局および医療情報システム・サービス事業者は、本マニュアルを参照しつつチェックリストを活用して、**日頃から実のあるサイバーセキュリティ対策を行ってください**。

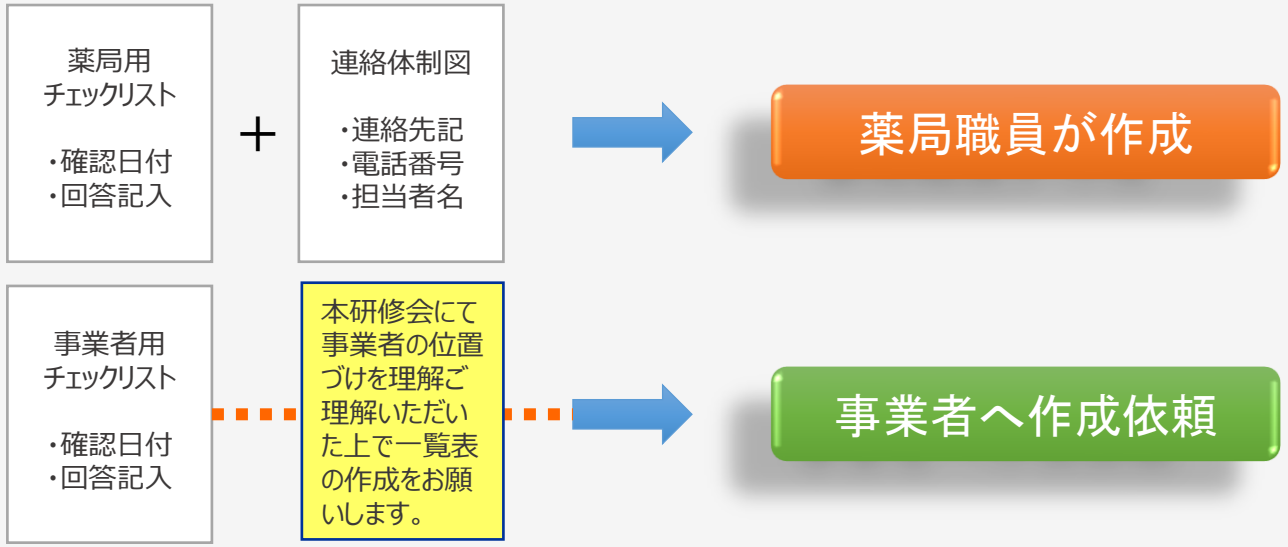
1. チェックリストの用意
2. チェックリストの記入方法
3. その他

サイバーセキュリティ対策チェックリストは、今回作るだけでなく、**毎年確実にできているか否かを確認するためのリスト**です。

1 立入検査前の準備（薬局におけるサイバーセキュリティ対策チェックリスト）

○ **チェックリストを使用するにあたり、薬局においては「薬局確認用」**、事業者においては「事業者確認用」を用いて確認してください。
※事業者と契約していない薬局においては「事業者確認用」による確認は不要です。

○ 薬局は**事業者に「事業者確認用」を送付し、対策の状況を確認するよう求めてください**。
複数の医療情報システムを利用している場合、システムを提供している事業者ごとに確認を求めてください。なお、事業者に対しても別途本取組について周知を行っていきます。

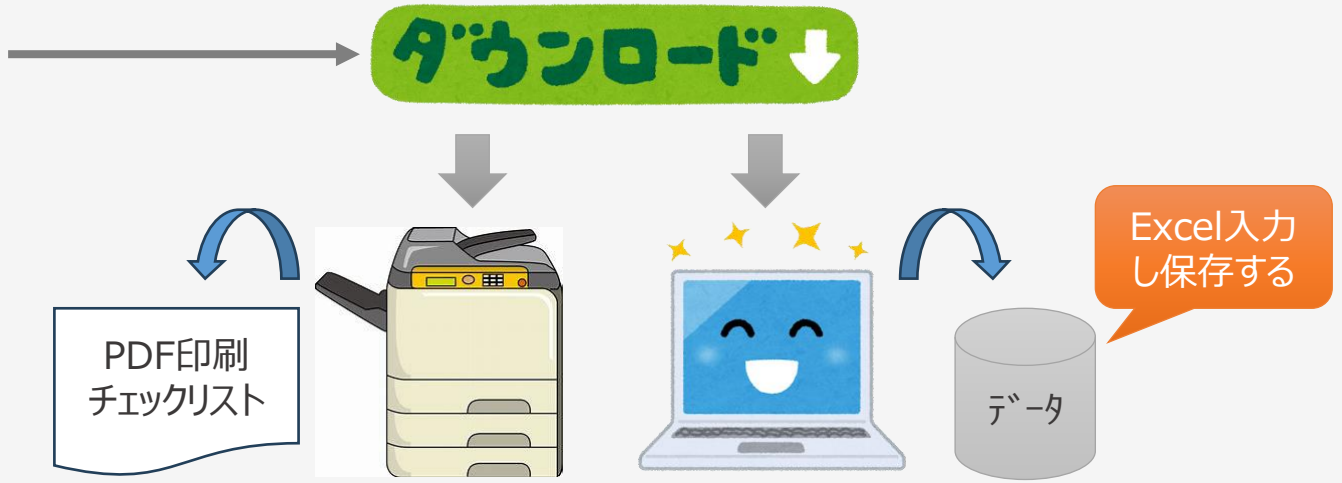


2 立入検査前の準備（薬局におけるサイバーセキュリティ対策チェックリスト）

○ 各項目の実施状況を確認し、「はい」 または 「いいえ」 にマルをつけて確認した日付を記入してください。**もし1 回目の確認で「いいえ」の場合は、対策の実施にかかる令和６年度中の「目標日」を記入**するようにしてください。チェックリストは紙媒体（PDF印刷）又は電子媒体（Excel）のどちらで使用して頂いても構いません。

○ 薬局は「薬局確認用」について**令和６年度中に全てのチェック項目で「はい」にマルがつくように事業者と連携**して取り組むようにしてください。※ 事業者と契約していない場合には、２(２)及び２(３)の記入は不要です。

○ 複数の事業者と契約している場合契約内容によっては「事業者確認用」の一部の項目の確認が不要になることもあります。「事業者確認用」には事業者名を記入する欄を設けています。**薬局は各事業者から回収してください**。



3 立入検査前の準備（薬局におけるサイバーセキュリティ対策チェックリスト）

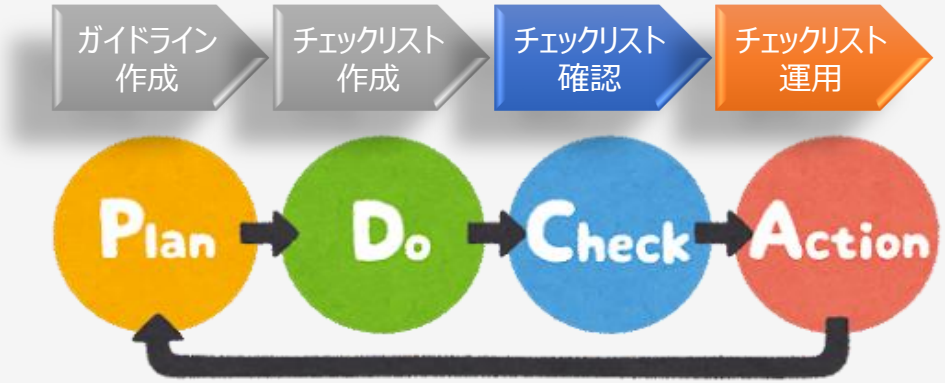
○ チェックリストの確認結果は随時参照して日頃の対策の実施に役立ててください。
⇒毎年、職員等への薬局用チェックリストに記載された項目について周知徹底を実施し記録を残してください。
✓実施記録には、必ず「実施日付」「参加者名」を記入してください。

○ 少なくとも年に１回は、チェックリストを用いた点検を実施してください。
⇒毎年、薬局用チェックリストによる自己点検を実施し、記録を残してください。
✓自己点検は誰が行うか事前に決めておいてください。
✓実施記録には、必ず「実施日付」「参加者名」を記入してください。
✓チェックリストは最新の内容か否かを厚労省HP等で必ず確認してください。

○ 薬局と直接契約関係にない事業者においては「事業者確認用」の提出は不要ですが薬局と直接契約関係がある事業者には「事業者確認用」チェックリストの提示を依頼してください。
⇒毎年、事業用チェックリストの提示を依頼してください。
✓事業者への依頼管理表を作成し、事業者名、依頼日付、受領日付、確認印などで管理してください。

4 立入検査前の職員への訓練

○ サイバーセキュリティ対策チェックリストは、医療情報システムの作成資料の内容確認と記載されたサーバーセキュリティ対策が実際にどこまでできているか確認することになります。



チェックリスト確認	チェックリストの内容を理解し具体的な対策を決める ①システム有無 ②体制 ③管理運用 ④事故対応
チェックリスト運用	決められた管理体制にてルールを守る ①教育 ②運用環境見直し ③チェックリスト見直し

○ サイバーセキュリティ対策チェックリストを完成させることが目的ではない（本末転倒）
○ サイバーセキュリティ対策が実施されているか否かを検査することが目的（真の目的：検査というより監査 ）
○ 医療情報システムの安全管理責任者はだれがいいのか？（薬局長、事務責任者、外部は在籍が必要）
○ **質問に答えるときは、口頭で記憶で答えるのではなく、台帳や資料に記載された内容で答えると心証がよい。**

・
・
・

5 立入検査のヒアリングは何を見ながら答えますか？

○事前準備として、チェックリストいがに必要なもの・・・「参考：サーバーインシデント発生時の事業継続計画」

2.1. 情報機器等の把握と適切な管理
2.1.1　医療情報システム安全管理責任者の決定
2.1.2　**平時の組織体制図**の作成、**担当者毎の役割表**の作成
2.1.3　**情報機器台帳**の作成
2.1.4　**ネットワーク・システム関連図**の作成
2.1.5　業務内容に対する**代替手段の決定**

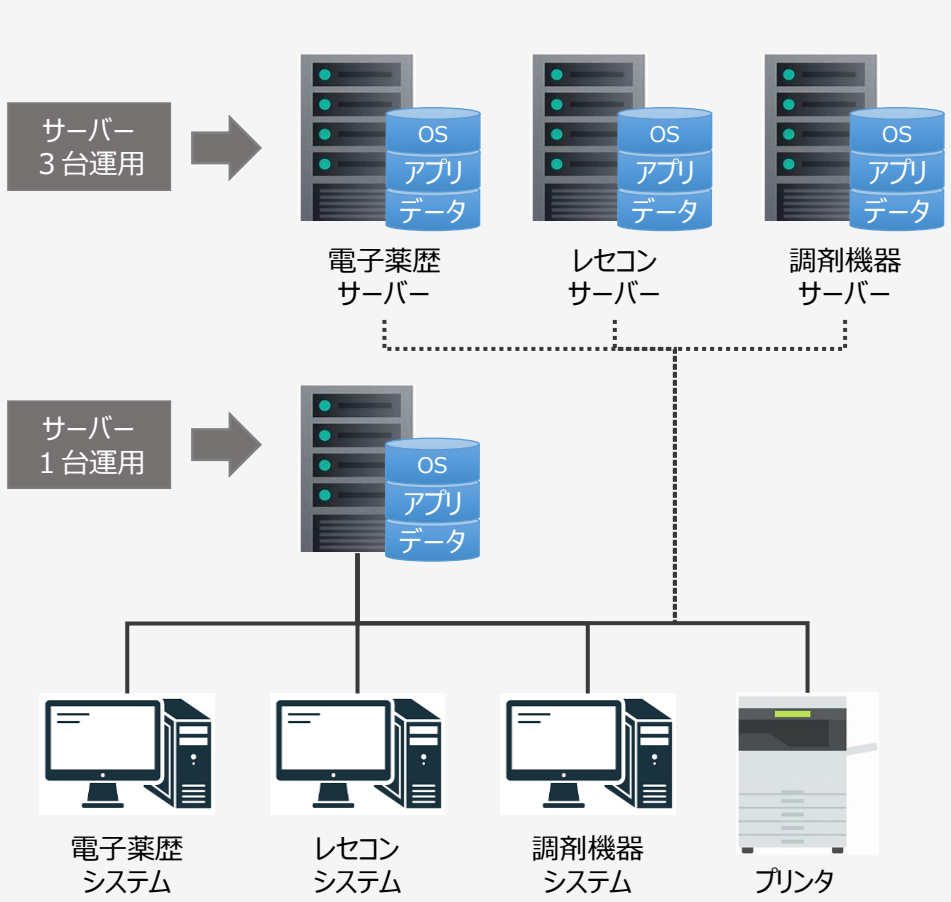
2.2. 非常時に備えたサイバーセキュリティ体制
2.2.1　**非常時の連絡体制図**の作成、**外部関係機関の連絡先**の作成
2.2.2　**事業者等の連絡先**の作成
2.2.4　**バックアップの作成と復旧方法**の決定

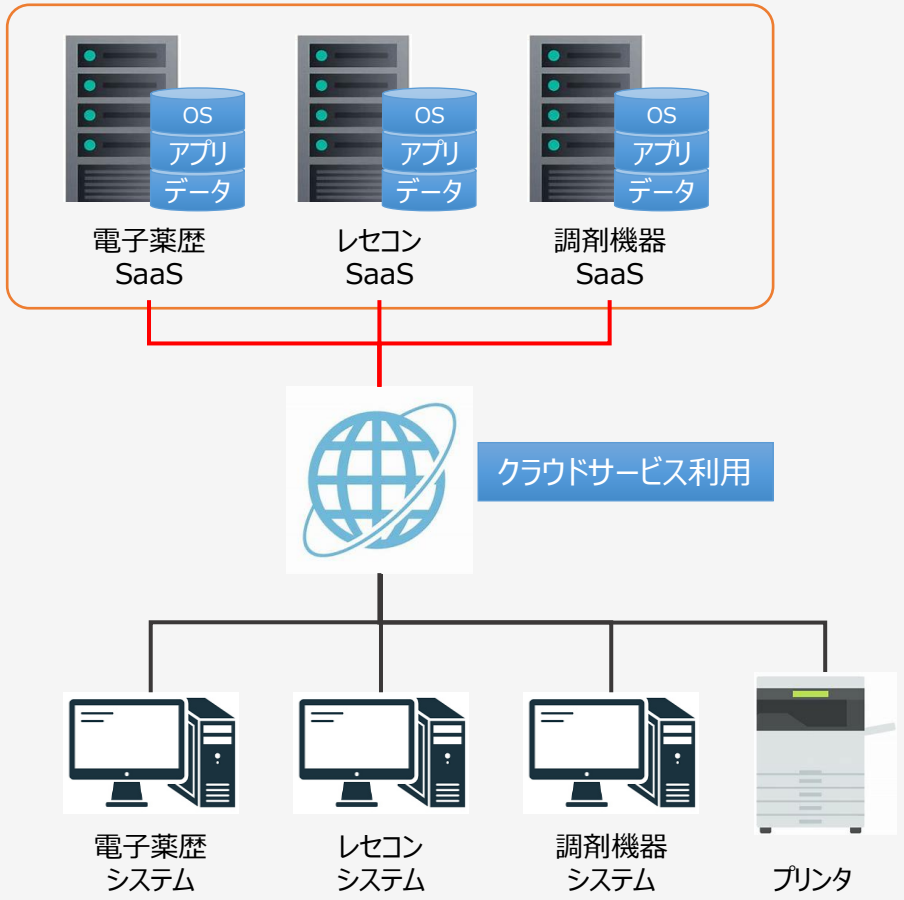
3. サイバーインシデント発生時の対応
3.1. 異常発見時の連絡先として、**部門連絡先及び事業者連絡先一覧**の作成

・
・
・

5 立入検査のヒアリングは何を見ながら答えますか？

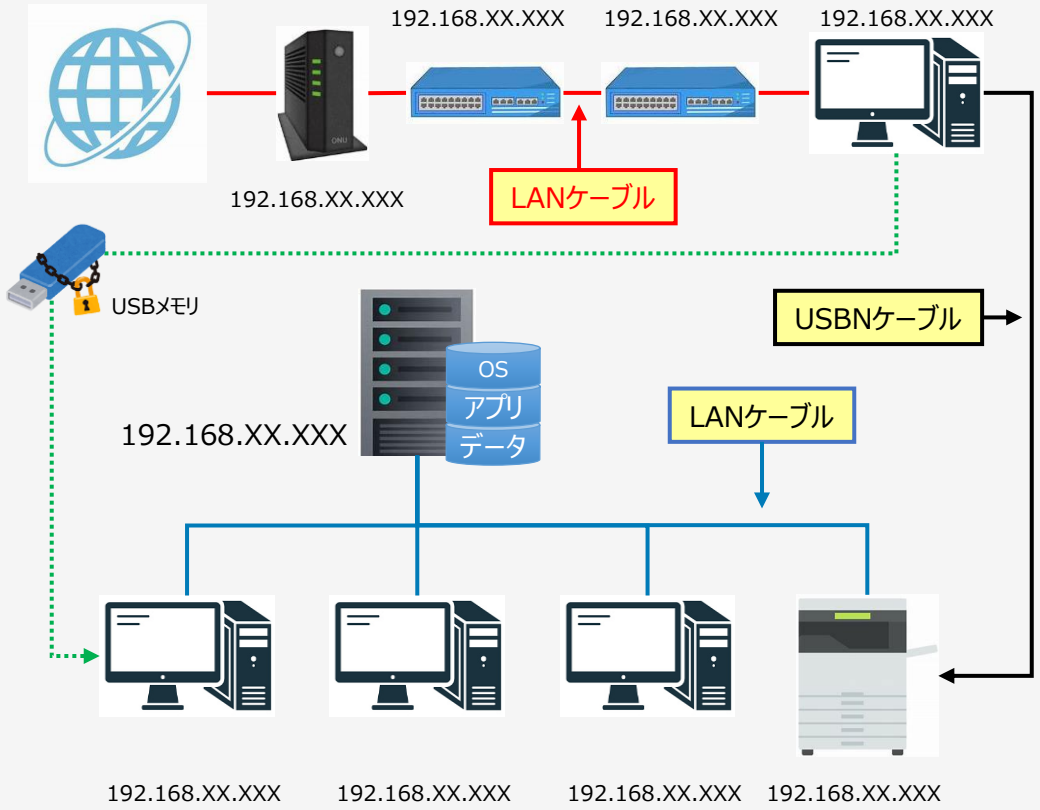
○システム構成図（オンプレミス・クラウドサービス）

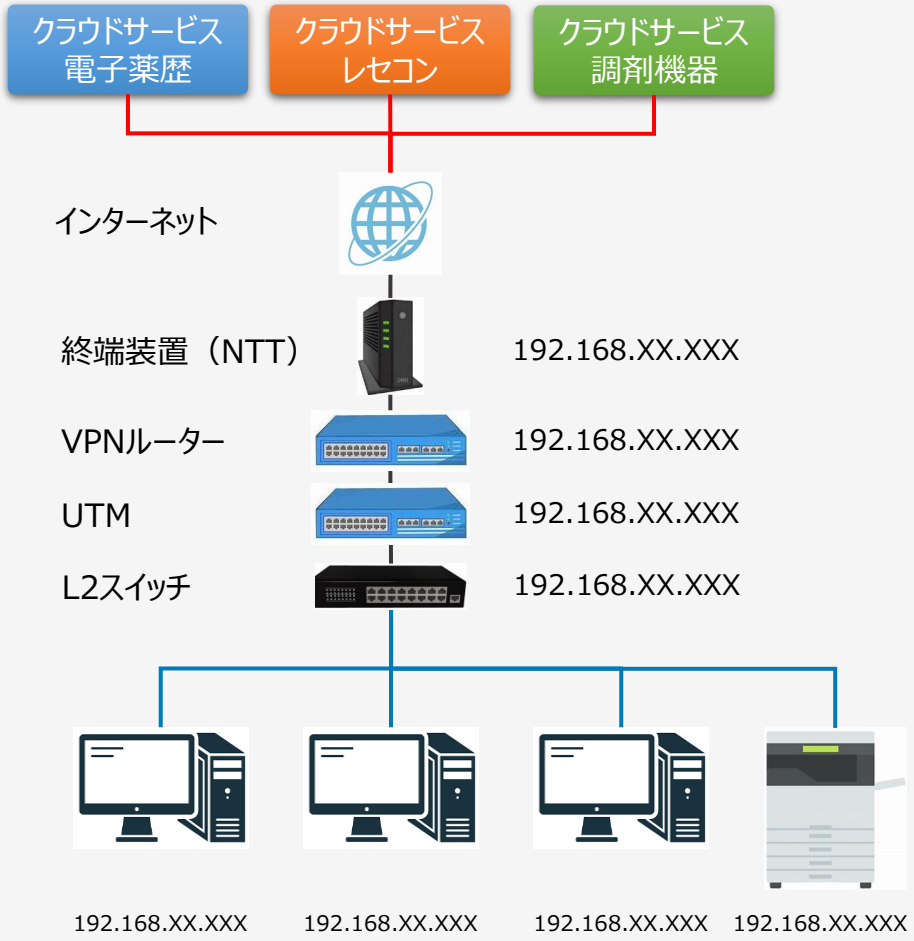




5 立入検査のヒアリングは何を見ながら答えますか？

○ネットワーク構成図（オンプレミス・クラウドサービス）





医薬局にけるサイバーセキュリティ対策チェックリストマニュアル
を見ながら「薬局確認用チェックリスト」を見直し

０．医療情報システムの有無【薬局】
▶概説編 2.3

□ 医療情報システムを導入、運用している。

本チェックリストが対象とする医療情報システムは、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を想定します（例：レセコン、電子薬歴システム等）。

これには、事業者により提供されるシステムだけでなく、薬局において自ら開発・構築されたシステムが含まれます。

本項目の「いいえ」にマルがつく場合、以下すべての項目は確認不要です。

○医療情報システム

- □ 電子調剤録（電子薬歴）システム
- □ 会計システム（レセコン）
- □ 調剤機器システム（錠剤・散剤・水剤・薬袋発行など）
- □ 薬剤監査支援システム
- □ 電子お薬手帳システム
- □ オンライン服薬指導システム
- □ ○○○○システム
- □ ○○○○システム
- □ ○○○○システム

○薬局独自システム・クラウドサービス

- □ ○○○○システム
- □ ○○○○システム
- □ ○○○○システム
- □ ○○○○システム
- □ ○○○○システム

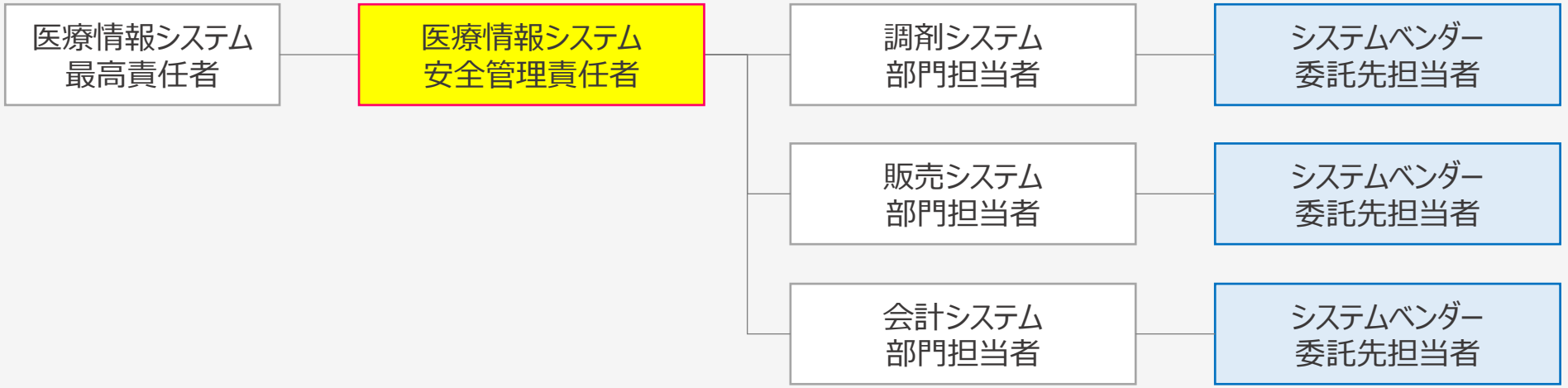
- □ ○○○○クラウドサービス
- □ ○○○○クラウドサービス
- □ ○○○○クラウドサービス

１．体制構築【薬局確認用・事業者確認用】
▶経営管理編3.1.2②／3.2

ロ（１） 医療情報システム安全管理責任者等を設置している。

薬局において、医療機関等において医療情報システムの安全管理（企画管理、システム運営） の実務を担う「企画管理者」や医療情報システムの安全管理を直接実行する「医療情報システム安全管理責任者」（以下併せて「**システム管理責任者**」という。） や、医療情報システムの実装・運用を担う「**システム運用担当者**」を設置する必要があります。

システム管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。なお、**小規模な薬局の場合には、薬局の管理者が、システム管理責任者やシステム運用担当者を兼任する場合がある**と考えられます。また、事業者においても医療情報システム等の提供に係る管理責任者を設置する必要があります。



２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶経営管理編1.2.1＜管理責任＞②　▶企画管理編9.1

ロ（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。（医療情報システム全般）

医療情報システムで用いる情報機器等の安全性を確保するために、**情報機器等の所在**と、それらの**使用可否の状態**を適切に管理する必要があります。そのため、システム管理責任者は薬局で所有する医療情報システムで用いる情報機器等について**機器台帳を作成**して管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしてください。

また薬局の開設者は**定期的に管理状況に関する報告を受け**、管理実態や責任の所在が明確になるよう、監督してください。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

※情報機器等の所在：実際の設置場所やネットワーク識別情報等を指します。
※サーバ、端末 PC、ネットワーク機器のうち、自身の**薬局で保有する医療情報システムについて台帳管理を行っていれば、「はい」にマルをつけてください。**

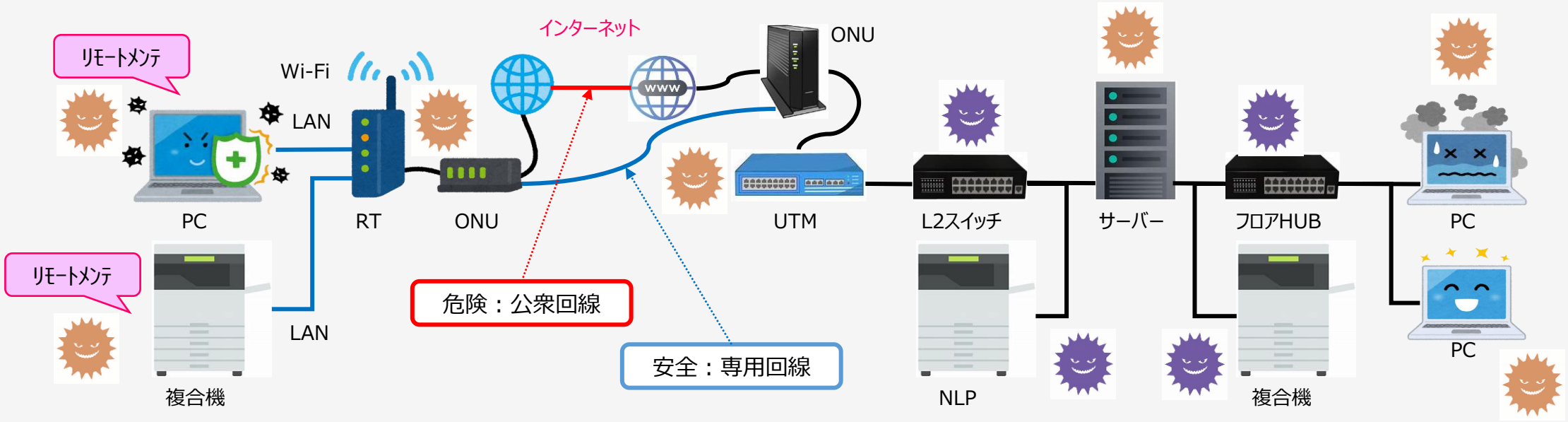
○情報機器台帳（サンプル）

管理No.	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	主な利用者属性	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1-PC1	Room1	薬剤師、職員、管理者	2024/11/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1-PC2	Room1	薬剤師、職員、管理者	2024/11/5	稼働	
003	A社	Win11	○○電子カルテ	1.5	192.168.○.○	Room1-PC3	Room1	薬剤師、職員、管理者	2024/11/10	停止	メンテナンス
004	B社	Win10	○○管理システム	5.0.1	192.168.○.○	Room2-PC1	Room2	薬剤師、管理者	2024/11/15	稼働	
005	B社	Win11	○○管理システム	6.1.2	192.168.○.○	Room2-PC2	Room2	薬剤師、管理者	2024/11/20	停止	機器故障

２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶企画管理編9.1　▶システム運用編 10.1

ロ（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に確認した。（医療情報システム全般）

リモートメンテナンス（保守）作業または保守環境に対するサイバー攻撃が想定されます。
システム運用担当者は、このようなリスクに対応するために必要な措置を講じ、システム管理責任者に報告する必要があります。そのため、システム運用担当者は、２（１）で整理した情報をもとに、**リモートメンテナンスを利用している機器の有無**を事業者に確認し、システム管理責任者へ報告してください。**なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。**

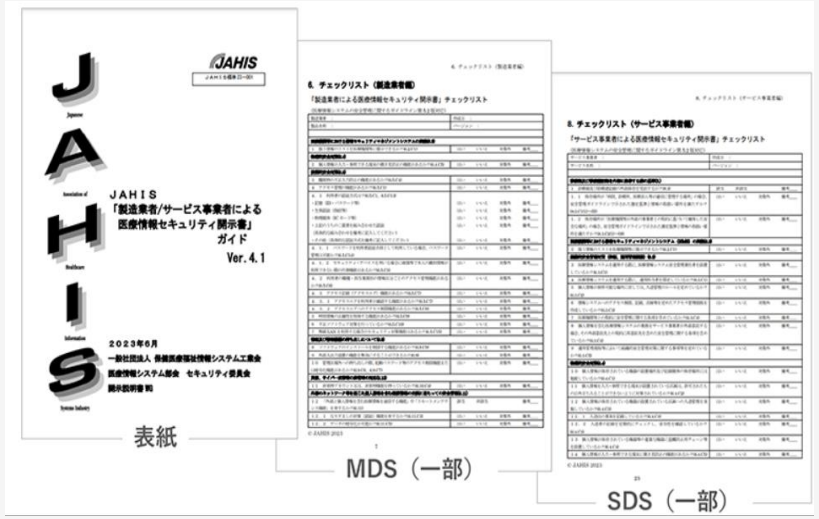


2．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶概説編 4.5

ロ（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。（医療情報システム全般）

医療情報システムのセキュリティに関するリスク評価及びリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。

システム管理責任者は事業者へ当該医療情報システムに関する MDS/SDS の有無を確認し、事業者から回収してください。**なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。**



製造業者／サービス事業者 → 委託 → JAHIS／セキュリティベンダー

「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）」とは、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説明の標準的記載方法（書式）を、一般社団法人保健医療福祉情報システム工業会（JAHIS）および一般社団法人日本画像医療システム工業（JIRA）で定めた文書です。

医療機関等で使用している情報機器・システム・サービスの「**医療情報システムの安全管理に関するガイドライン**」に対する準拠性を確認することができます。

各システムベンダーは、文書内の「MDS／SDSチェックリスト」を用いて、医療情報システム・サービス等のセキュリティ対応状況を医療機関等に開示することが求められています。

２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶企画管理編13④／13.1.3

ロ（４）利用者の属性等に応じた情報区分毎のアクセス利用権限を設定している。（サーバ、PC）

医療情報システムの利用権限は、薬局内の権限規程等に応じて、設定することが重要です。

システム管理責任者は、**情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定**してください。

利用者に付与した ID 等については、台帳を作成して一覧化することが望ましいです。なお、台帳で**管理する項目としては、①利用者属性　②氏名　③ユーザーID　④権限等等が想定**されます。

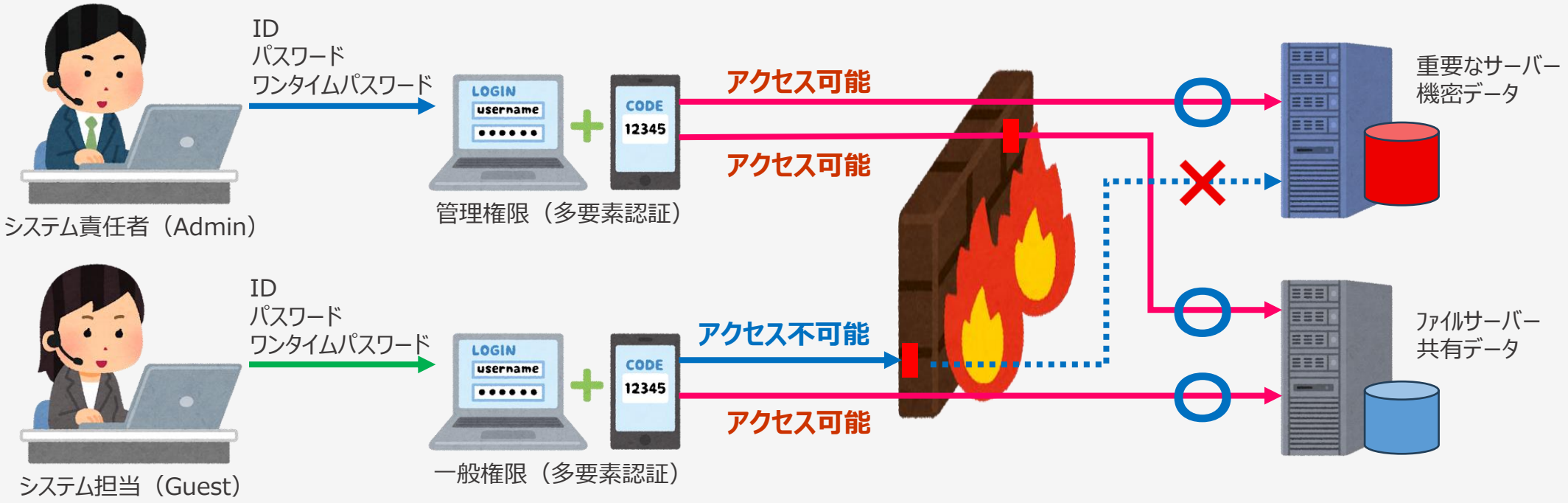
○利用者ID台帳（サンプル）

管理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	NNN	NNN	999-9999-9999	aaa@1010	使用者	Admin	使用可
002	非常勤薬剤師	NNN	NNN	999-9999-9999	bbb@1011	使用者	User	使用可
003	事務	NNN	NNN	999-9999-9999	ccc@1012	使用者／退職予定	User	使用可（2025/03迄）
004	非常勤事務	NNN	NNN	999-9999-9999	ddd@1013	使用者	User	使用可
005	パート	NNN	NNN	999-9999-9999	eee@1014	使用者／産休予定	user	使用可（2025/07迄）

２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶企画管理編 13⑦

ロ（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している。（サーバ、端末 PC）

システム管理責任者は２（４）で整理した情報を元に、**退職者や使用していないID等が含まれていないかを確認**してください。長期間使用されていない等の不要なID は不正アクセスに利用されるリスクがありますので、速やかに削除してください。**最近では、転職時に顧客に関する情報を持ちダウケースが頻繁に起こっています**。



２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶経営管理編4.2　▶企画管理編5.3　▶システム運用編 17①②

ロ（６）アクセスログを管理している。（サーバ）

医療情報システムが適切に運用されているかを確認するために、システム運用担当者は利用者のアクセスログを記録するとともに**システム管理責任者はそのログを定期的に確認**してください。

例えば不正アクセスがあった場合でも、その痕跡を発見して追跡する起点となることなどが期待されます。**アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及び操作内容が特定できるように記録**することが必要です。

※アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を併せて講じてください。

○アクセスログ（サンプル）

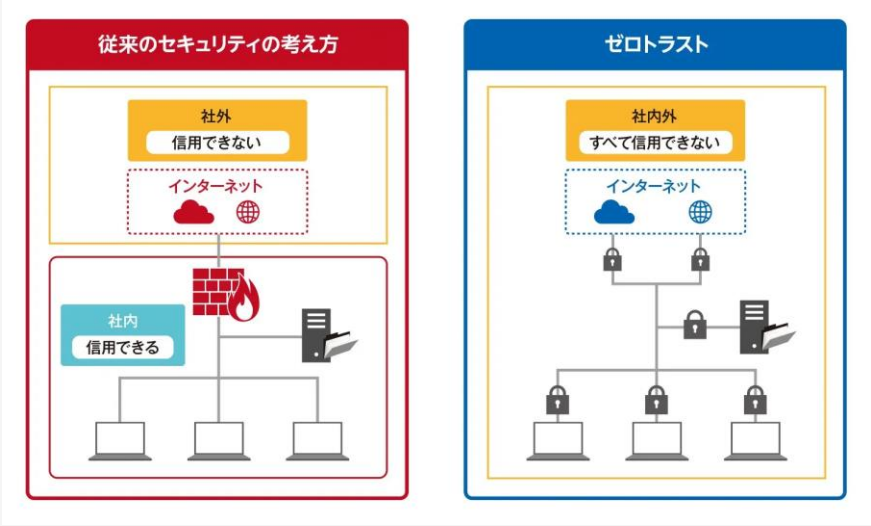
ユーザーID	利用者属性	時刻	カテゴリ	捜査情報
aaa@1010	NNN NNN	2024/11/01　08:30:00	管理メニュー	ログイン
bbb@1011	NNN NNN	2024/11/01　08:30:00	入力メニュー	起動
ccc@1012	NNN NNN	2024/11/01　08:30:00	照会メニュー／入力メニュー	起動
ddd@1013	NNN NNN	2024/11/01　08:30:00	入力メニュー	カルテ入力
eee@1014	NNN NNN	2024/11/01　17:30:00	入力メニュー	ログオフ
aaa@1010	NNN NNN	2024/11/01　13:00:00	管理メニュー	起動
ddd@1013	NNN NNN	2024/11/01　23:30:00	管理メニュー／入力メニュー／照会メニュー	ログイン／ダウンロード

２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶システム運用編　8③／8.1／8.2／13.2

ロ（７） 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。（医療情報システム全般）

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。**対策としては、不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待**できます。しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、**全ての不正ソフトウェアが検出できるわけではありません。**

※システム運用担当者が、**脆弱性が報告されているソフトウェアへのセキュリティパッチを適用**することが挙げられます。



クラウドをまとめて多要素認証（MFA）

SASE（ネットワークの機能とセキュリティの機能を一体として提供するクラウドサービス、又はその考え方・概念を表す言葉です）や Microsoft 365、Google Workspace をはじめとする様々なクラウドサービスに**デジタル証明書＋FIDO2（PWなし認証）／スマホ認証／ICカード／顔認証／パスワードによる多要素認証（MFA）**を手早く適用できます。

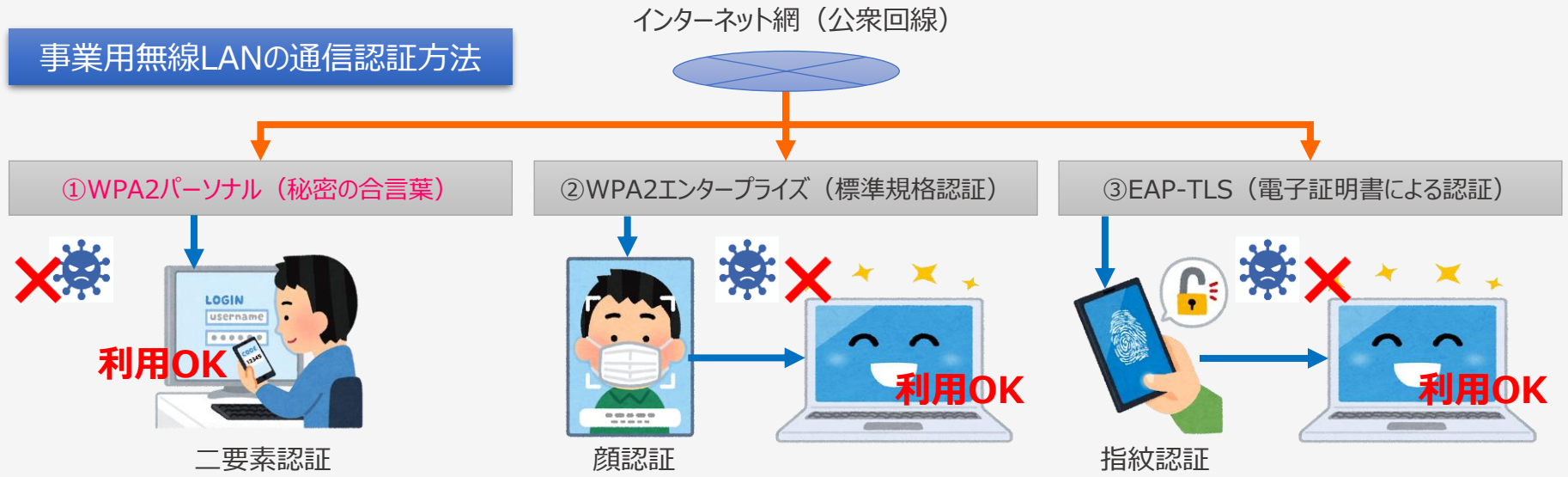
なりすましを防ぐデジタル証明書なら情報資産へのアクセスを信頼できるユーザーとデバイスに限定することができます。又、利用デバイス・時間帯・位置情報などから、**普段とは異なる不審なログイン操作を動的に検出する、リスクベース認証**も搭載しています。

２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶システム運用編 13⑪

ロ（８）接続元制限を実施している。（ネットワーク）

外部ネットワークに接続する際にはネットワークや機器等を適切に選定し監視を行うことが必要です。特に、**無線LANを使用する**際は不正アクセス対策として適切な利用者以外に無線 LAN を利用されないようにすることが重要です。**システム運用担当者は、ネットワーク機器に接続出来る MAC アドレスを限定すること等、不正アクセス対策を実施**してください。

※MACアドレス認証とは、ネットワーク機器に割り当てられたMACアドレス（Media Access Control Address）を利用して、ネットワークへのアクセスを制限する手法ですが、**無線LAN認証においては全く効果がありません。**



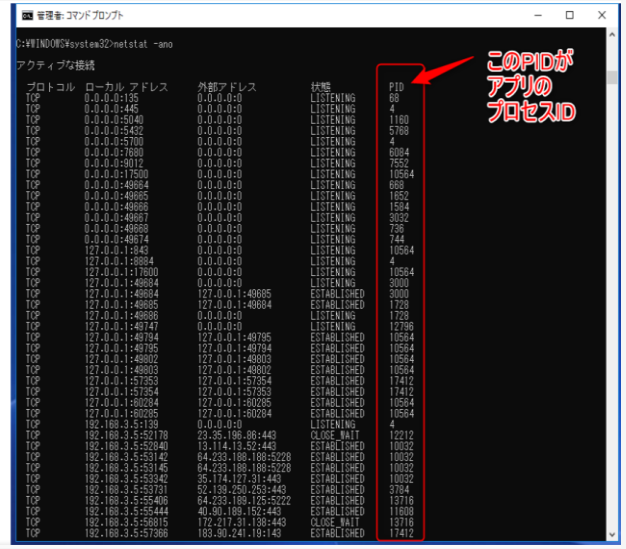
２．医療情報システムの管理・運用【薬局確認用・事業者確認用】
▶システム運用編 8.1

ロ（９）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。（サーバ、端末 PC）

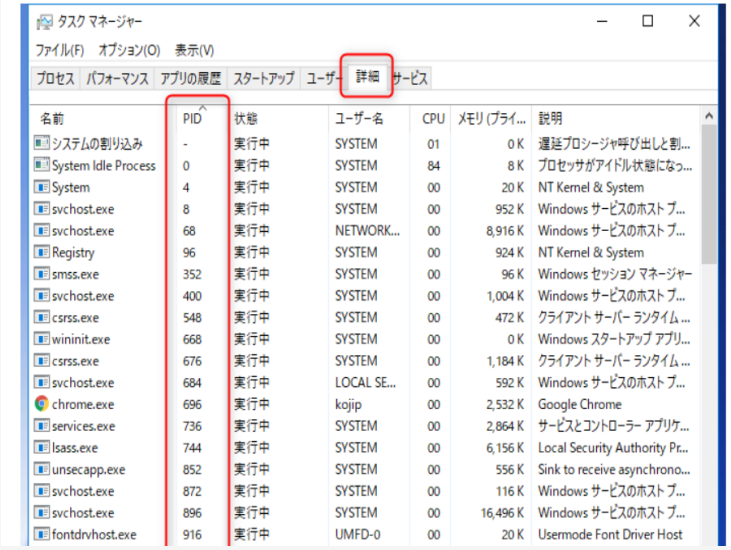
不正ソフトウェアは、電子メール、ネットワーク等の経路を利用して医療情報システム内に侵入する可能性があります。
システム側の脆弱性を低減するため、まずは**利用していないサービスや通信ポートを非活性化させることが重要**です。
システム運用担当者は、**プログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認**し、不要なものがある場合はシステム管理責任者に相談の上、対策を講じてください。

※PCのアプリケーション一覧から、デフォルト設定からアプリケーションの増減があればシステム管理者に報告し対処すること。

コマンドプロンプト
↓
①Windowsシステムツール
↓
②検索窓に「cmd」と入力
↓
③netstatと入力



デスクトップ画面
↓
①Ctrl+Alt+Delete



3．インシデント発生に備えた対応【薬局確認用】
▶経営管理編 3.4.2①／3.4.3① ▶企画管理編 12.3

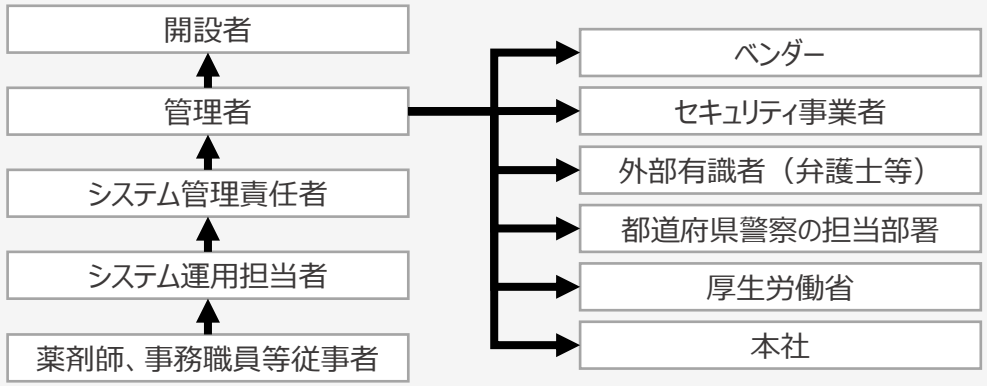
ロ（１）インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図がある。

薬局の開設者は情報セキュリティインシデント発生に備え、事業者や外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するようシステム管理責任者に指示することが重要です。システム管理責任者はサイバーインシデント発生時速やかに情報共有等が行えるよう**緊急連絡網を明示した連絡体制図を作成**して下さい。

連絡体制図には、**薬局内の連絡先や会社本部の連絡先等に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等が明示されていることが想定**されます。このような連絡体制が整備されていることで、速やかな初動対応支援が可能となり被害拡大の防止につながります。

※立入検査時は、連絡体制図が作成されていることを確認します。

○連絡体制図（サンプル）



○ステークホルダー連絡先一覧（サンプル）

外部関係機関	連絡先
厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室	03-6812-7837 igishitsu@mhlw.go.jp
事業者	99-9999-9999 aaaaaaa@bbbbco.jp
情報セキュリティ事業者	99-9999-9999 aaaaaaa@bbbbco.jp
都道府県警察の担当部署	99-9999-9999 aaaaaaa@bbbbco.jp
○○○○○○○○○○○○	99-9999-9999 aaaaaaa@bbbbco.jp

３．インシデント発生に備えた対応【薬局確認用】
▶経営管理編 3.4.1 ▶企画管理編 11.2 ▶システム運用編 11.1/12.2/18.1

ロ（２）インシデント発生時に調剤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。

稼働が損なわれた医療情報システムを速やかに復旧できるよう、情報システムやデータ等のバックアップ（オフライン）を適切に確保し、その復旧手順を整備・確認しておくことが求められます。

システム管理責任者はバックアップを確保する際、重要なファイルについては、不正ソフトウェアの混入による影響が波及しないよう複数の方式で世代管理するよう設計し、システム運用担当者は手順に従いバックアップを確保してください。

なお、復旧手順の整備については、例えば、**BCP に復旧手順を定める**などの方法が挙げられます。

（用語）世代管理：バックアップの一種で、最新データだけでなく、それ以前のデータもバックアップする方法を指します。
（補足）３世代目以降の**バックアップはオフライン（物理的あるいは論理的に書き込み不可の状態）にする等の対策が望ましいです。**

システム	頻度	作成方法（バックアップ）	復旧方法（リストア）
電子調剤録 電子薬歴	毎日	クラウドサーバにデータベースのバックアップを作成する	データベースを再構築した後に、バックアップサーバのデータを復元する。
	毎日	外付けHDD（NAS）等にデータベースファイルとシステムファイルのバックアップを作成する	システムのOSを再構築した後に、外付けHDD等のシステムファイルとデータベースのデータを復元する
○○○○○	○○	○○○○○○○○○○○○○○○○○○○○	○○○○○○○○○○○○○○○○○○○○
○○○○○	○○	○○○○○○○○○○○○○○○○○○○○	○○○○○○○○○○○○○○○○○○○○

３．インシデント発生に備えた対応【薬局確認用】
▶経営管理編 3.4.1 ▶企画管理編 11.1

ロ（３）サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。

薬局の開設者はシステム管理責任者と連携して非常時における業務継続の可否の判断基準や継続する業務選定等の意思決定プロセスを検討し、サイバー攻撃を想定したBCP等を整備することとしています。

このBCPを整備しておくことにより、万が一**サイバー攻撃を受けても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することが期待**できます。

日本薬剤師会ホームページ

↓ 薬局関連情報

↓ 薬局に備える指針、手順書等

ダウンロード
（PDF／WORD）

https://www.nichiyaku.or.jp/日本薬剤師会オフィシャルWebサイト

Ver.1.00

サイバーインシデント発生時の
事業継続計画（BCP）

○○年○○月○○日初版
○○薬局

薬局にけるサイバーセキュリティ対策チェックリストを
毎年１回以上見直してください。
機器更新、事業者変更、新しい契約・・・

2024/11/23

情報セキュリティシニアコンサルタント　中島 明彦