６都薬情発第２９号
令和６年８月２６日

各地区薬剤師会　担当役員 殿

公益社団法人 東京都薬剤師会
副会長　一 瀬　信 介

サイバーインシデント発生時の事業継続計画（BCP）の薬局向け雛形について
（都薬版BCP雛形の周知依頼）

平素より本会会務に格別のご理解、ご協力を賜り、厚く御礼申し上げます。

医療機関等に対するサイバー攻撃は近年増加傾向にあることから、令和５年４月には、改正薬機法施行規則が施行され、薬局の管理者が遵守すべき事項として、薬局の管理者はその薬局のサイバーセキュリティの確保について必要な措置を講じることが追加されました。

今般、サイバーセキュリティの確保については、厚生労働省より示されたサイバーセキュリティ対策チェックリスト及び、サイバーセキュリティ対策チェックリストマニュアルの項目に「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」が記載され、各薬局においても令和６年度中に本BCPを策定することが求められています。

当該 BCP は個人での作成は些か困難であることから、令和６年８月２３日付け事務連絡にて、日本薬剤師会から本BCPを策定する際に活用できるサイバーインシデント発生時の事業継続計画(BCP)の薬局向け雛形(日薬版)を作成した旨お知らせしたところですが、この度、本会においてもサイバーインシデント発生時の事業継続計画(BCP)の薬局向け雛形(都薬版)を作成し、都薬HP（会員用ページ）に公開しましたのでお知らせいたします。

つきましては、自局の状況に合わせた編集をしていただき、薬局での事業継続計画(BCP)策定にご活用いただきますよう、貴会会員にご周知の程お願い申し上げます。

【サイバーインシデント発生時のBCP 薬局向け雛形（都薬版）】
都薬HP＞地域への貢献に向けて＞薬局BCP
https://www.toyaku.or.jp/contribution/member/community/bcp.html

○○薬局

サイバーインシデント発生時の事業継続計画（BCP）

雛形

年　　月　　日　策定

本 BCP では、サイバーインシデントによる大規模なシステム障害が発生しても、重要な事業を中断させない、または中断しても可能な限り短い時間で復旧させるための方針、体制、手順等を示す。

公益社団法人 東京都薬剤師会 薬事委員会 2024 年 8 月作成

目次

第１章　総則

1.1　事業継続計画を策定する目的と必要性

【記載例】

〇〇薬局（以下、当薬局）は、サイバーインシデントによる大規模なシステムが発生した際、基幹となる事業の停止に追いこまれるケースが想定される。この場合、医療・顧客サービス等の基幹事業機能の停止、患者個人情報の漏えい、経済的な損失が生じ、ひいては事業からの撤退を余儀なくされることになりかねない。サイバーインシデントが発生したときに、薬局に対して問われるのは、その薬局が危機に直面した時であったとしても事業を遂行（継続）するという社会的使命を果たせるかどうかである。これは、マニュアル化という次元で解決できる問題ではなく、危機に直面したときの「薬局経営のあり方」そのものなのである。

薬局は、自身の被害の局限化という観点に留まらず、コンプライアンスの確保や社会的責任という観点から対策を講じなければならない。経営者は、個々の事業形態・特性などを考えた上で、企業存続の生命線である「事業継続」を死守するための行動計画である「事業継続計画（Business Continuity Plan：BCP)」を構築することが望まれる。

本計画は、薬局がサイバー攻撃を受けた場合を含むサイバーインシデントを想定し、大規模なシステム障害が発生した際に、当薬局が行う業務等に関して優先順位等を定めるとともに、業務遂行のために、必要な事項を定めるものである。

当薬局では、有事発生時の対応行動を迅速化するためのＢＣＰを策定し、訓練を通した継続的改善の繰り返しにより、有事における対応力をより一層強化し、社会全体の安心安全の実現のために活動していく。

【作成のポイント】

「事業継続計画を策定する目的と必要性」では、事業継続の必要性について経営者からのメッセージを記載します。

例

- 薬局内の情報システム設備の災害対策の充実
- 個人情報漏洩時の対応・対策の明確化

※サイバーインシデント：主にインターネットやネットワークを介した攻撃や不正アクセスなど、外部からの脅威による問題を指します。例えば、マルウェア感染や DDoS 攻撃などが含まれます。

1.2　基本方針

【記載例】
当薬局は、個人情報の保護と薬剤師・薬局サービスの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。
①　安全かつ持続的な薬剤師・薬局サービスの提供を実現する
②　サイバーインシデントに対する脅威からの被害から事業を保護する
③　リスクマネジメント対策としてサイバーセキュリティを確保する
④　平時、非常時を通じて事業継続に関する説明責任を果たす
⑤　被害後、医療安全を担保しつつ、迅速かつ合理的な薬局機能の復旧を行う
⑥　〇〇〇〇

1.3　対象範囲

【記載例】
対象とする医療情報システムは以下の通り。
①　電子調剤録（電子薬歴）システム
②　会計システム（レセコン）
③　調剤機器システム（錠剤・散剤・水剤・薬袋発行など）
④　薬剤監査支援システム
⑤　電子お薬手帳システム
⑥　オンライン服薬指導システム
⑦　〇〇〇〇

1.4　想定する事象～備えるべき脅威と被害想定～

1.4.1　想定する事象

本 BCP で想定される事象において、薬局業務に影響するものを以下に挙げる。なお、自然災害、大規模停電等による電源喪失などの計画は別に定めるものとする。
【記載例】
①　調剤情報など電子調剤録・レセコンの確認・参照不能
②　調剤情報など電子調剤録・レセコンへの入力不能
③　電子お薬手帳システムの操作不能・誤作動
④　オンライン服薬指導システムの操作不能・誤作動
⑤　その他情報機器・調剤機器等の操作不能・誤作動
⑥　職員・患者等の個人情報の漏えい・拡散
⑦　〇〇〇〇〇〇

1.4.2　備えるべき脅威

当薬局に影響を及ぼす可能性のあるITリスク（脅威）としては以下のものがある。

【記載例】**【備えるべき脅威】**

No	ITリスク	感染経路	被害
1	身代金要求型 ウイルス (ランサムウェア)	下記の No２，３以外にウェブサイト閲覧で感染する。	パソコン、サーバのファイルが全て暗号化され、読めなくなる。ファイルを元に戻すために金銭を要求されるが、支払っても元に戻らない場合もある。
2	メール添付型 ウイルス (エモテット)	メールの添付ファイルを開く、または本文中のURL(リンク先)を開くと感染する。	個人情報(連絡先、メールアドレス等)、企業秘密(ID、パスワード等)の外部漏えい。加えて、取引先等へウイルス付きのメール(過去の送受信メールを利用し偽のメールだと気付かない)を勝手に送信する。そのため、多くの企業で感染が発生する。
3	ネットワーク機器への脆弱性攻撃	会社のネットワーク機器の脆弱性を狙って攻撃する。	会社のネットワークの信頼性向上のために導入したネットワーク機器のソフトウェアの脆弱性を利用し、会社のネットワークに侵入し、情報漏えい等を行う。
4	パソコン等への 脆弱性攻撃	パソコン、スマートフォン等の脆弱性を狙って攻撃する。	ソフトウェアの脆弱性を利用し、外部からパソコンやスマートフォンが攻撃され、情報の窃取や破壊が行われる。
5	フィッシング詐欺 メール	もっともらしい電子メールで偽のサイトに誘導する。	偽サイトでユーザーID、パスワード、クレジットカード番号等の個人情報をだまし取り、本人になりすまし、商品を購入したりする。
6	分散型サービス妨害（DDoS攻撃）	サーバまたはネットワークを偽のインターネットトラフィックで氾濫させ、ユーザーがアクセスできないようにする。	業務を中断させるサイバーインシデントである。
	○○○○○○	○○○○○○	○○○○○○

【新たな脅威となったＩＴリスク】

2023(令和 5)年 3 月に、内閣府がＢＣＰのガイドラインを約２年ぶりに改定し、情報セキュリティが強化されました。その背景には、新型コロナウイルス感染症により、在宅勤務（テレワーク）が急速 に普及した半面、IT リスク(脅威)への備えが不足しており、大企業のみならず中小企業でも情報事故が多発し、サプライチェーンに大きな影響を与えたことがあります。 さらに、近年、金銭要求型のサイバー攻撃も増えています。独立行政法人情報処理推進機構の報告では、2021 年度、企業から寄せられたウイルス感染の報告件数は、前年度の約２倍となりました。この感染で実際に被害があった事案のうち、６割がランサムウェアという身代金要求型ウイルスです。

【作成のポイント】

●個人情報保護法

個人情報保護法において「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報をいいます。個人情報保護法は、全ての事業者が対象になっており、企業として行う個人情報の収集・保管・活用について、規定されています。また個人情報が漏えいした場合の届け出や対処法についても言及しており、薬局は組織として個人情報を取り扱っているので、個人情報保護法について、今一度、確認してみてください。

●情報セキュリティ

企業の規模に関係なくサイバーインシデントに遭うリスクがあることを認識し、普段からサイバーインシデントの被害等について、知見を持つことが重要です。

1.4.3　情報セキュリティ被害想定

【記載例】【情報セキュリティ被害想定】

カテゴリ	予想される被害	被害を大きくする要因（脆弱性）
経営者	情報セキュリティのリスクを理解せず、準備していないために、サイバー攻撃等を受ける。	保守期限が切れた OS（例えば、Windows XP,7,8 等）やアプリケーションを使用しており、容易にサイバー攻撃等を受ける。
	従業員教育が不十分なため、サイバーインシデント等に気づかず被害が拡大。	会社のパソコンに情報セキュリティの低い私物のスマホや USB メモリーの接続を許容。
従業員	不審なメールの添付ファイルやリンクを開いたりすることで、パソコン等がウイルスに感染。	アンチ・ウイルス・ソフト（ワクチン・ソフト）を導入していないため、ウイルスに容易に感染。
	フィッシング詐欺を理解しておらず、怪しいサイトにクレジットカードの情報等を入力し、被害にあう。	早期にカード会社や銀行に連絡しなかったため、補償が受けられないケースがある。
機器	パソコン、スマホ、ネットワーク機器の脆弱性に適宜、対応していないため、脆弱性を狙われ、サイバー攻撃を受ける。	パソコン、スマートフォン、ネットワーク機器の ID やパスワードが容易に類推できるものになっており、容易にサイバー攻撃を受ける。
	パソコンが暗号化され、使えなくなった際に予備のパソコンがなく、業務継続が困難。	予備パソコンの環境設定が行われておらず、業務を短時間で復旧できない。
情報	サイバーインシデントにより重要な情報が暗号化され、業務が停止。	重要な情報をバックアップしてあったが、 ハードディスクが常時ネットワークに接続されており、バックアップも暗号化される。また、最近のサイバーインシデントではクラウド上のバックアップ情報も暗号化されるケースもある。 個人情報の流出については、個人情報保護委員会に届けずに放置すると、刑事上の罰則(6 ヶ月以下の懲役又は 30 万円以下の罰金)、及び民事上の損害賠償が請求される可能性がある。
その他	○○○○	○○○○

【作成のポイント】

●サイバーインシデントから中小企業を守るサービスとして、独立行政法人情報処理推進機構(IPA)が行っている 「サイバーセキュリティお助け隊」があります。
https://www.ipa.go.jp/security/otasuketai-pr/

第２章　体制整備

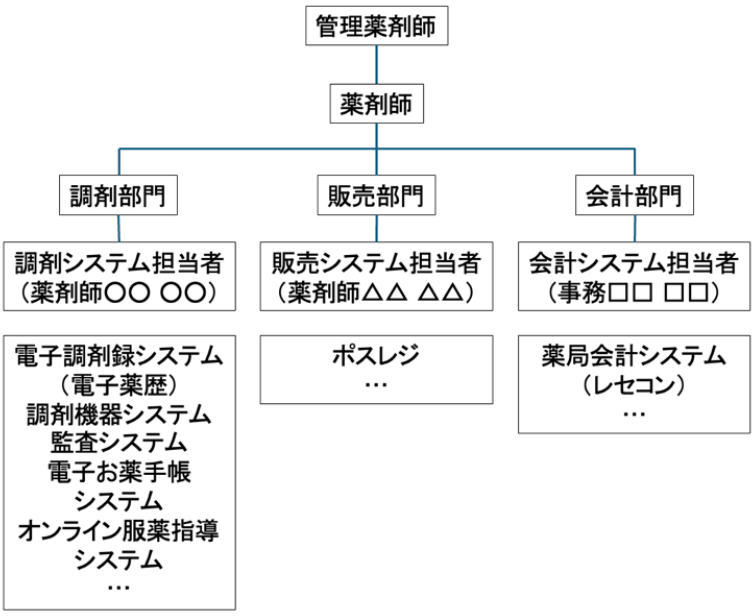
2.1　情報機器等の把握と適切な管理

2.1.1　医療情報システム安全管理責任者

○○○○（役職名）を、医療情報システム安全管理責任者として定める。
△△△△（役職名）を当薬局におけるサイバーセキュリティに関する最高責任者とする。
（医療機関の規模・組織等によっては上記が兼務することも想定される。）

2.1.2　組織体制図

薬剤師・薬局サービスの継続及び医療情報システムの復旧を目的としたサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。



【記載例】平時の組織体制図

2.1.3　担当者の役割

【記載例】【担当者の役割】

役割	担当者	役割の概要
医療情報システム 最高責任者	役職名 〇〇 〇〇	薬剤師・薬局サービスの継続及び医療情報システムの復旧の計画策定を統括し、最終的な責任を負う。
BCP 作成責任者	役職名 〇〇 〇〇	BCP の策定と定期的な見直しを実施する。
医療情報システム 安全管理責任者	役職名 〇〇 〇〇	医療情報システムの安全管理を直接実行する。
企画管理者	役職名 〇〇 〇〇	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。
システム運用担当者	役職名 〇〇 〇〇	医療情報システムの実装・運用を担う。
部門担当者	役職名〇〇 〇〇 役職名△△ △△ 役職名□□ □□	薬剤師・薬局サービス継続の計画策定に関する各種検討作業を行う。 各部門システムの運用継続計画策定に関する各種検討作業を行う。
システムベンダー 委託先	〇〇〇社 △△△社 □□□社	医療情報システムの運用保守及び緊急時の状況に関する提供・対策を調整する。
〇〇〇〇	〇〇〇〇	〇〇〇〇

2.1.4　情報機器台帳

医療情報システム安全管理責任者は、情報機器の現況を反映した管理台帳を以下のとおり整備する。併せて、定期的に棚卸しを行い、機器の所在と稼働状況の確認を行う。

【記載例】**【情報機器台帳】**

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	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のPC１	Room1	薬剤師・事務職員・システム管理者	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	薬剤師・事務職員・システム管理者	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	薬剤師・システム管理者	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	薬剤師・システム管理者	2021/8/1	稼働	

（出典：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～ ）

URL：https://www.mhlw.go.jp/content/10808000/001253959.pdf

2.1.5　ネットワーク・システム構成図

医療情報システム安全管理責任者は、医療機関等で導入している医療情報システムの全体構成図（ネットワーク図、システム構成図等）を整備する（ネットワークの全体像が分かりやすいものを作成）。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

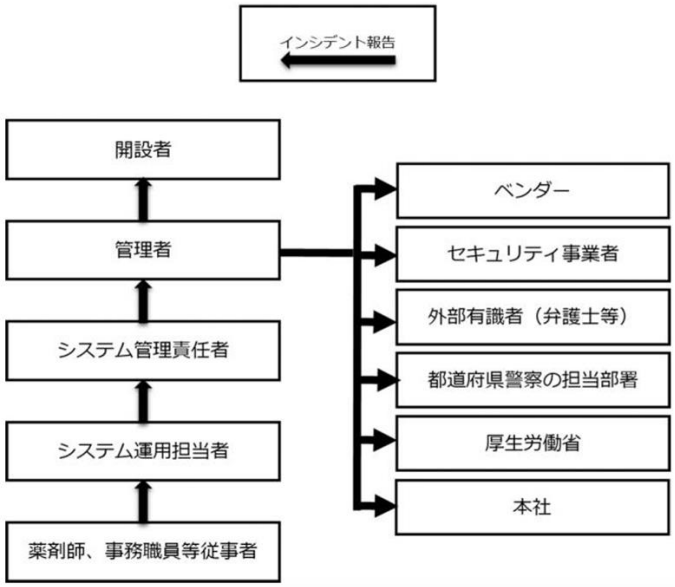
2.1.6　脆弱性に関する対策

医療情報システム安全管理責任者は、契約等で定められた責任分界をもとにサーバ、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適用を行う。万が一、適用できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器入れ替え等）について事業者等と合意した上で取り決め、実施する。

2.2　非常時に備えたサイバーセキュリティ体制

2.2.1　連絡体制図

調剤継続及び医療情報システムの復旧に資するアクションを迅速に行う目的で、サイバーセキュリティの連絡体制（連絡先、担当、メールアドレス、電話番号、連絡目的等）及び外部関係機関の連絡先を以下のとおり定める。



（出典：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～）

【記載例】**連絡体制図**

2.2.2　重要関係先連絡リスト

【記載例】【重要関係先連絡リスト】

関係先	担当	連絡先	メールアドレス
電子調剤録・薬歴	○○○社	○○-○○○○-○○○○	○○@○○○
会計システム	○○○社	○○-○○○○-○○○○	○○@○○○
お薬手帳システム	○○○社	○○-○○○○-○○○○	○○@○○○
オンライン服薬指導システム	○○○社	○○-○○○○-○○○○	○○@○○○
対策本部責任者	○○ ○○	○○-○○○○-○○○○	○○@○○○
東京都薬剤師会	総務課	03-3294-0271（代表）	
警視庁	サイバー犯罪相談窓口	03-5805-1731	
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
個人情報保護委員会		03-6457-9680（代表）	
○○○○	○○○○	○○○○	○○○○

※　厚生労働省　医療分野のサイバーセキュリティ対策について

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

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/#leak_report

2.2.3　情報収集体制

当薬局における各システムの脆弱性情報について事業者等から情報提供を定期的に受け取ることができる体制を 2.2.2 の事業者の連絡先を参考として構築する。

2.2.4　教育体制

本 BCP が迅速かつ適切に利用できるよう、年 1 回以上の教育、訓練を実施する。情報セキュリティ責任者、医療情報システム安全管理責任者は年間の教育計画に沿った訓練が適切に実施されるように監督する。訓練結果により、事前対策やサイバーインシデント発生時の対応計画等に解決すべき課題が発生した場合、課題の解決もしくは改善に向けた計画の立案をする。

2.2.5　バックアップ体制

サイバーインシデント発生時に備えた、データとシステムのバックアップの頻度、作成方法及び復旧方法について以下のとおり定める。

【記載例】**【バックアップの作成と復旧方法】**

システム	頻度	作成方法	復旧方法
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 等にデータベース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。
○○○○	○○	○○○○	○○○○

2.3　事業継続戦略

2.3.1　事業継続戦略とは

事業継続戦略とは、有事発生時に事業継続のために活動を再開するための被害の状況に合わせた複数の対応手段のことである。
有事発生時の被害は甚大な被害から軽微な被害まで様々な状況が予想される。例えば、甚大な被害が発生した場合には、単なる現状復帰だけでは再開までに多くに時間を要することとなるため、現状復帰の対応手段のみではなく、代替手段（他の場所や他の手段で再開するなど）の検討も事前に行っておくことが必要である。

2.3.2　事業継続戦略

サイバーインシデント発生時における状況に合わせた事業継続のための対応方法は以下のとおりとする。
【記載例】**【事業継続戦略】**

事業継続戦略	戦略を発動する状況
現状復旧戦略	軽微な被害で早急に再開が可能な被害の場合には、発生した被害の修復を行い早急に再開する。
代替再開戦略	甚大な被害(情報漏えい、データ改ざん)が発生した場合には、現状復旧までの間は、他店舗や他薬局に代替を依頼し、事業を継続する。
自社の代替再開戦略	ウイルスに感染していない PC の特定を行い、ベンダー（電話番号〇〇〇-〇〇〇〇-〇〇〇〇）に即座に連絡をとり、 バックアップサーバへの切替を行い、早急に業務を再開する。 ＜患者対応＞ 患者に復旧まで調剤できない旨を伝える。 その間は手書きの薬袋等で対応し、会計は後日対応とする。もしくは、復旧した後で連絡し再来局してもらう。

【作成のポイント】

●「事業継続戦略」では、有事において自組織でとるべき戦略を記載します。
- 事業継続戦略は、原則として脅威ごとに変わるものではありません。
代替再開戦略が容易に検討・作成できない場合は、まずは地域や同業種・異業種との連携から検討する方法もあります。

2.3.3　優先業務の選定・実施

サイバーインシデント発生時は、被害の拡大阻止を最優先とし状況把握と対応策に努める。通常業務については、一時的に中断・縮小する。その際には、以下の優先順位を参考にする。

【記載例】**【有事において優先すべき業務】**

優先順位		業務
A:通常通り実施	1	○○○○○○
	2	○○○○○○
	3	○○○○○○
B：縮小して実施	4	○○○○○○
	5	○○○○○○
	6	○○○○○○
C：当面実施しない	7	○○○○○○
	8	○○○○○○
	9	○○○○○○

2.3.4　リスク評価・代替運用

各システムが利用できなくなった場合、その業務内容の代替手段を以下のとおり定める。また、代替運用方法については別途、システム停止時の代替運用マニュアル等にて定める。

【記載例】**【業務内容に対する代替手段】**

業務内容	システム	代替手段
調剤録・薬歴等	電子調剤録・電子薬歴システム	紙運用
薬剤調整	錠剤・散剤・水剤の分包機・分注機	手作業（コンピュータを利用しない方法）
薬袋・薬情	薬袋発行機等	手書き
会計	会計システム（レセコン）	未収扱いを検討
○○○○○○	○○○○○○	○○○○○○

2.4　情報セキュリティの事前対策実施と課題管理

赤字は『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』と同様の項目です。

実施すべき対策			担当者 所属・氏名	対応方法	予定 完了
1 体制構築	1-1	医療情報システム安全管理責任者を設置している。			
	1-2	情報セキュリティの教育・周知を行う。			
	1-3	薬局における私物品（スマホ、USB、アプリケーション）の取扱いルールを決め、徹底する。			
	1-4	個人情報保護について、正しく認識する。必要に応じて従業員にも個人情報保護を教育・周知する。			
	1-5	個人情報を業務で使用している場合は、情報管理体制を構築する。さらに、流出時の行動手順を決めておく。			
	1-6	薬局におけるサイバーセキュリティチェックリストを備えて、定期的にチェックを行っている。			
2 医療情報システムの管理・運用	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。			
	2-2	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。			
	2-3	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。			
	2-4	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。			
	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している。			
	2-6	アクセスログを管理している。			
	2-7	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。			
	2-8	接続元制限を実施している。			
	2-9	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。			

	2-10	保守期限が切れたソフト（OS 、アプリケーション）の使用を止める。			
	2-11	パソコン、スマホ、ネットワーク機器のソフトを適宜、更新する。			
	2-12	パソコン、スマホ、ネットワーク機器のパスワードは、容易に類推されないものにする。定期的にパスワードを変更する。			
	2-13	重要な情報は、適宜、バックアップを取る。バックアップを取ったハードディスクは、パソコンから取り外す。ネットワーク上のハードディスクの場合は、ネットワークから切り離す。			
	2-14	個人情報については、必要に応じてパスワード等で保護する。個人情報には、必要最低限の人のみがアクセスできるようにする。			
	2-15	個人情報を外部へ持ち出す（メールで送信する、USB メモリーを手渡す）ときは、パスワードを掛ける。			
3 インシデント発生に備えた対応	3-1	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。			
	3-2	サイバー攻撃を想定した事業継続計画（BCP）を策定し定期的に見直しを行っている。			
	3-3	できれば、予備のパソコンを用意し、業務に使えるように必要なアプリケーションを導入しておく。			

【作成のポイント】

●「情報セキュリティ の事前対策実施と課題管理 」では、情報セキュリティ事故に備えて実施すべき対策について、記載例を参考に検討の上、記載します。

-自組織に該当する対策について は、 担当者を割り振り、完了予定を記載します。

- 記載例の中で自組織に該当しない項目は除外します。

第３章　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

異常発見時の連絡経路は 2.2.1 の『連絡体制図』に、システムベンダー等への連絡先は 2.2.2『重要関係先連絡リスト』に示す通りとする。あわせて、各担当部門の連絡先は以下のように示す。なお、部門システムの管理者は連絡先が全職員に把握されるように明示して、常に最新版で管理し連絡経路が機能することを担保する。

【記載例】**【部門連絡先一覧】**

部署名	担当者	連絡先
調剤部門	○○	××-××××-××××
販売部門	○○	××-××××-××××
会計部門	○○	××-××××-××××
システム安全管理責任者	○○	××-××××-××××
システム最高責任者	○○	××-××××-××××

3.2　システム異常の検知と開設者への情報伝達

システム異常を検知した場合、あらかじめ定めた項目（発生場所、発生箇所、発生日時、連絡者、異常の内容・範囲）について担当部門に報告できるように周知する。なお、口頭による連絡後、「報告様式」を用いて記録を残す。また、職員から発出された異常において、医療情報システム安全管理責任者によりサイバーインシデントの可能性が思慮された場合、2.2.1 で作成した『連絡体制図』を基に、速やかに開設者ならびに関係各所・外部関係機関に共有し、意思決定できるように努める。

3.3　初動対応

サイバーインシデント発生後は、以下のとおり対応する。

3.3.1　原因調査

医療情報システム安全管理責任者はサイバーインシデントの原因や被害範囲の特定のために、医療情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

①　ネットワーク機器やケーブル等の調査
②　電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査
③　情報漏えいの有無に関する調査
④　メンテナンスやデータ移行等の作業に関する調査
⑤　○○○○○○

3.3.2　被害拡大防止

被害拡大防止のための対応を行う。まずは、バックアップに通ずるネットワークの遮断を行う。次に、外部の通信経路を遮断する。その上で、被害箇所から攻撃範囲および侵入経路の推定を行った上で、セグメンテーション（区分）境界において、通信を遮断して被害拡大防止を図る。

3.3.3　開設者への報告

医療情報システム安全管理責任者はサイバーインシデントについて開設者に対して、現在の被害状況を報告するとともにインシデント対応方法と患者安全を担保する運用方針案を提案する。この内容を踏まえて、開設者はシステム停止に伴う薬剤師・薬局サービスの継続方針（医薬品提供体制等の確保等）を検討し意思決定する。決定した内容は、速やかに 2.2.1 の『連絡体制図』で定める組織内ならびに外部関係機関へ周知を行う。

3.4　薬剤師・薬局サービスの継続

薬剤師・薬局サービスの継続は 2.3『事業継続戦略』のとおり実施する。
サイバーインシデント対応と薬剤師・薬局サービス継続について報告を受けた開設者は以下のとおり対応する。

① 医療情報システムの縮退運転判断
開設者は医療情報システム安全管理責任者からの提案を受け、医療情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の薬剤師・薬局サービスの継続においては、手作業による運用等、自然災害時を想定した事業継続計画（もしくはシステムダウン時マニュアル等）に則り運用する。

② 被害状況等調査（フォレンジック調査＋証拠保全）
医療情報システム安全管理責任者は、証拠保全の作業と薬剤師・薬局サービスの継続に関する作業を調整しながら両立させる。具体的には、アクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏えいの有無等の調査について医療安全を担保しつつ行う。必要に応じて医療情報システム・サービス事業者等へ協力依頼して調査を進める。なお、調査状況は随時開設者に報告する。
※フォレンジック・・・犯罪の立証のための電磁的記録の解析技術及びその手続き

③ 組織対応方針の確認と外部関係機関への報告
医療情報システム安全管理責任者の被害状況および調査結果に基づき、開設者は復旧対応方針（復旧に向けた対応、広報への対応）を決定し、その対応を関係者に指示する。また、2.2.2 で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

3.5　復旧処理

復旧計画に基づいて、以下のとおり対応する。医療情報システム安全管理責任者は医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。

- 復旧指示と復旧作業
  医療情報システム安全管理責任者は、開設者からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業(システムの再設定、再インストール、バックアップデータからの復元等)並びに検証作業を行う。必要に応じ医療情報システム・サービス事業者に対応を依頼する。あわせて、システム停止中に生じたアナログ情報についてシステムに反映させる選択肢を提示する。開設者は、アナログ情報の反映時期ならびに程度を医療安全の観点を踏まえて意思決定する。
- 結果の確認
  医療情報システム安全管理責任者は、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、開設者に報告する。開設者は診療状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第 4 章　事後対応

4.1　報告

復旧後、復旧結果と情報漏えい事実の有無等について、開設者及び組織内に報告する。不足していたと考えられる事前対策、連絡先並びに連絡内容について振り返りを行う。

4.2　再発防止

4.2.1　再発防止策検討・策定

4.1 の『報告』の後、サイバーインシデントにより発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、開設者に提案する。開設者は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。開設者は決定した再発防止策について、連絡経路を用いて全職員に周知する。

4.2.2　事業者への指示

開設者によって決定された再発防止策は、医療情報システム安全管理責任者等により、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、薬局側と誠実に議論し、計画を立てて実施する。

4.2.3　情報公開

開設者は、類似のサイバーインシデントによる被害拡大に対する警鐘を鳴らす目的、また当薬局を受診する患者への診療に関連する注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、1 次対応、患者対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。

資料編

資料１　サイバーインシデントの行動・対応の流れ

【記載例】

区分	状況	行動・対応	対策
事前準備	教育・周知	情報セキュリティの教育を実施する。	
	ソフトの更新	パソコン、スマホ、ネットワーク機器の基本ソフトを最新のものに更新する。	教育で周知
	ウイルス感染の防止	パソコン等にアンチ・ウイルス・ソフトを導入し、最新のバージョンに更新する。	教育で周知
	ネットワーク監視ツールの導入検討	ネットワーク統合脅威管理(UTMという専用の機器)の導入を検討する。	
初動対応	被災事象の発生	見慣れない画面が表示される等の事象が発生したら、速やかに管理者等へ報告する。 また、社外から通報があった場合も、同様に管理者等へ報告する。	教育で周知
	BCP発動。対策本部設置	対策本部メンバーが参集する。	BCP活用
	初動処理	異常が発生したパソコン等をネットワークから切り離す。情報漏えいのリスクがある場合は、社外とのネットワークを遮断、サービスの停止などの措置をとる。	ネットワーク構成図を整備
	調査	事実関係を調査し、情報を整理する。 必要に応じてＩＴの専門家の支援を受ける。	
	通報	個人情報の漏えいがあった場合には、個人情報保護委員会へ報告する。 (1)速報：発覚日から、３～５日以内 (2)確報(続報)：発覚日から、３０日以内 厚生労働省に連絡する：03-6812-7837	※
	報告	必要に応じて取引先、顧客等へ報告する。 東京都薬剤師会に報告する：03-3294-0271	
事業継続	被害拡大の防止	情報漏えいで発生した被害の拡大防止を図る。	
	事業復旧	バックアップ情報を利用したシステム等の復旧を行う。システム復旧に時間がかかる場合は、代替手段等で業務を継続する。	BCP活用
	事後対応	再発防止策を検討し実施する。	

※　個人情報保護委員会ホームページ「漏えい等の対応とお役立ち資料」を参照する。
https://www.ppc.go.jp/personalinfo/legal/leakAction/

資料２ 事業継続計画（Business Continuity Plan：BCP）作成の手引き

(公社)日本薬剤師会 薬剤師のための災害対策マニュアルより抜粋

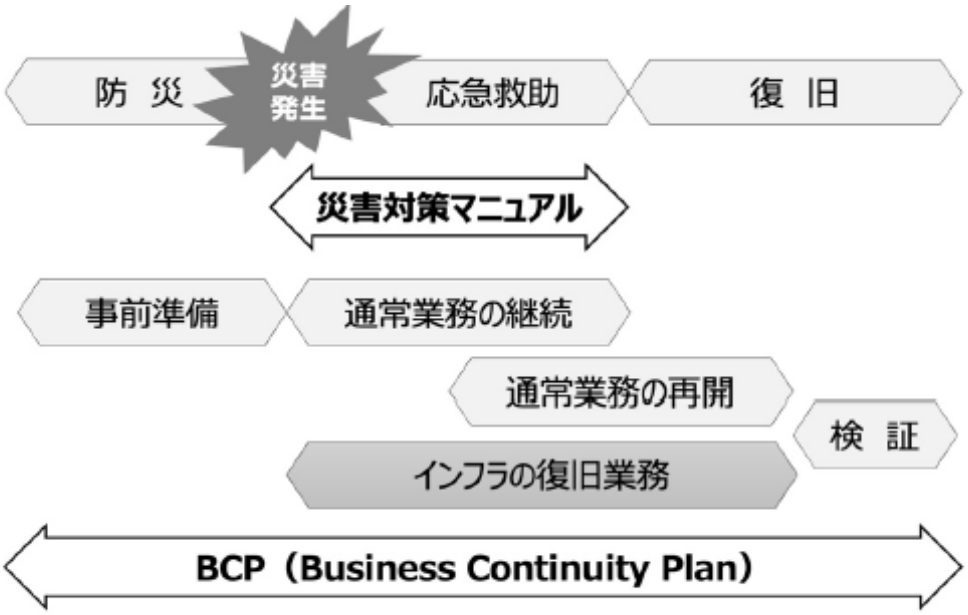
１．BCP の概念

1.1 BCP とは

事業継続計画（Business Continuity Plan: BCP）とは、企業や団体が自然災害、大火災、テロ攻撃など緊急事態に遭遇した場合に、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段などを取り決めておく計画である。医療機関は新興感染症の拡大や大規模災害が発生すると通常通りに業務を実施することが困難になるが、地域の医療を担う医療機関（病院・薬局）が医療サービスの提供を停止することは許されない。通常通りに業務を実施するには、業務を中断させないように準備するとともに、中断した場合でも優先業務の実施や速やかな業務再開のため、予め検討した方策を計画書としてまとめておくことが重要となる。

1.2 災害対策マニュアルとの違い

災害対応マニュアルを作成する主な目的は、「身体・生命の安全確保」と「物的被害の軽減」だが、その目的は、BCP の主な目的の大前提となっている。BCP では、災害対応マニュアルの目的に加えて、「いかに業務を継続するか」ということに主眼が置かれており、両者には共通する部分もあり密接な関係にある。



BCP（Business Continuity Plan）の概念図

2. BCP 作成

2.1 BCP 作成のポイント

BCP は、医療提供施設である病院や薬局が災害時の「ダメージの軽減」と「早期回復」を図るために作成される。BCP を作成するうえで、以下のポイントが重要である。

- □ 災害時に想定される被災状況を前提とする。
- □ 継続すべき業務を絞り込む。
- □ 継続する業務のサービスレベルの目標、中断する業務の再開目標を決定する。
- □ 目標に応じた対策を事前に検討し、実行する。
- □ 現状と目標のギャップを常に検証し、継続的に見直す。

2.2 BCP作成の進め方

BCP 作成のためのステップを以下に示す。

BCP 作成のステップと各ステップの実施概要

作成のためのステップ		内容
ステップ 1	基本方針の策定	災害時に何を優先するかを明確にし、業務継続の基本方針として定めます。BCP はここで定める基本方針に基づいて策定していきます。
ステップ 2	被害の想定	BCP 作成の前提とする被害を想定します。どのような規模の被害を前提に業務継続を検討するのか、明らかにします。
ステップ 3	業務の把握	日常的に行っている薬局業務について改めて全体像を整理するとともに、災害時に継続しなければならない業務（優先業務）を選定します。
ステップ 4	業務資源の把握	優先業務について、業務を実施するために必要なもの（業務 資源）を把握します。
ステップ 5	リスクの評価	災害時の業務資源の利用可能性について、現状の対策や先に設定した被害想定を参考に評価します。
ステップ 6	業務継続目標の設定	優先業務について、災害発生後の時間経過の中で、どのようなサービスレベルを目指すのか、業務継続の目標を設定します。
ステップ 7	対策の検討	先に設定した業務継続目標を実現するために必要となる事前対策を検討します。
ステップ 8	BCP 文書の作成	ステップ 1～7 までの検討結果、災害発生時の危機対応計画、教育訓練計画等を含めた BCP 文書を取りまとめます。

災害時の薬局業務運営の手引き(東京都福祉保健局)平成 25 年3月より

参考資料
・災害時の薬局業務継続計画〔薬局 BCP〕作成の手引き(徳島県保健福祉部薬務課)
・災害時の薬局業務運営の手引き(東京都福祉保健局)
・介護施設・事業所における自然災害発生時の業務継続ガイドライン(厚生労働省老健局)

資料３　サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

※薬局が BCP を策定する際、最低限必要な事項を網羅しているか、確認のために使用するものです。

※BCP 策定や見直しの際にご活用ください。

項番	大項目	確認項目	確認欄
1	平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）		
1-1	情報機器等の把握と適切な管理、全体構成図の作成	サーバ、端末 PC、ネットワーク機器を把握できているか。	
		ネットワーク構成図・システム構成図が整備できているか。	
		システム停止が事業継続に与える影響を把握できているか。	
		サーバ、端末 PC、ネットワーク機器の脆弱性への対応ができているか。	
1-2	非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集	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）への連絡体制図が整備できているか。	
		リスク検知のための情報収集体制が整備できているか。	
		教育訓練が実施できているか。	
		バックアップの実施と復旧手順が確認できているか。	
2	検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）		
2-1	システム異常の報告先の把握	異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。	
2-2	システム異常の検知	局内で発生した異常が局内職員によって覚知できるか。	

2-3	CSIRT/経営者によるシステム異常の覚知	局内職員から発出されたサイバー被害情報が組織を通じて速やかに CSIRT（対応者）ならびに意思決定者まで到達するか。	
3	初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。）		
3-1	原因調査（必要に応じて事業者に依頼）	原因調査のため、「ネットワーク機器やケーブル等の調査」「電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっているか。	
3-2	事業者等への連絡と作業履歴の確認	事業者等への連絡と作業履歴の確認ができるか。	
3-3	被害拡大防止	被害拡大防止に向けた対応ができるか。	
3-4	経営層への報告、経営層による確認と指示、組織内周知と対応	経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。	
3-5	被害状況等調査（フォレンジック調査＋証拠保全）と被害状況等の報告	被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。	
3-6	組織対応方針確認と外部関係機関への報告等の対応	組織対応方針を確認できるか。また、外部関係機関への報告ができるか。	
4	復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）		
4-1	経営層からの復旧指示の確認と実施	復旧指示の確認と実施ができるか。	
4-2	医療情報システム等の事業者等へ復旧対応依頼	医療情報システム等の事業者等への対応依頼ができるか。	

4-3	再設定や再インストール、バックアップデータの復旧等	再設定や再インストール、バックアップデータの復旧等ができるか。	
4-4	復旧結果の確認	復旧結果の確認ができるか。	
5	事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）		
5-1	復旧結果と情報漏えい事実の有無の報告	復旧結果と情報漏えい事実の有無、可能性について、局内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-2	再発防止策の検討・策定	再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-3	再発防止策の周知	再発防止策の周知を局内に周知する方法と体制が整備されているか。	
5-4	再発防止策の実施	再発防止策の実施が行えるか。	
5-5	事業者等への再発防止策の指示	事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。	
5-6	外部関係機関への報告と情報公開の検討	情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。 経営者と担当者により外部関係機関への報告が行えるか。	

厚生労働省 HP：【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）より抜粋

URL：https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

資料４　サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き

本手引きは、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」について、サイバー攻撃を想定した BCP 作成の一助となるよう、解説を加えたものです。貴組織において BCP を作成する際の参考として活用してください。

※ サイバー攻撃を想定した BCP 策定時の留意点

- 本手引き及び確認表は最低限必要な事項を記したものです。薬局の特性に応じて、自機関が主体となり必要な事項を整理し定めてください。
- BCP 策定には先だってリスク分析が重要となります。リスク分析は全過程において自機関だけでなく、事業者、その他の関係者の間で、情報および意見を相互に交換（リスクコミュニケーション）することが必要です。
- BCP は定期的に見直し、必要な項目を更新してください。
- 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）を含む情報を取り扱うシステムを指します。例えば、薬局のレセプト作成用コンピュータ（レセコン）、電子薬歴、オーダリングシステム等の調剤事務や調剤を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定されます。また、患者情報の通信が行われる局内・局外ネットワークも含みます。
- 薬局の規模により作成する BCP の内容も異なると想定されるため、関係団体等により示されている BCP の手引きについても適宜参照して作成してください。
- 本手引きの各項目の解説の下部には、それぞれの項目に紐づく「医療情報システムの安全管理に関するガイドライン」関連文書の該当箇所を括弧内に示しております。

厚生労働省 HP：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）より抜粋
URL: https://www.mhlw.go.jp/content/10808000/001266631.pdf

【１．平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）】

1-1）情報機器等の把握と適切な管理、全体構成図の作成

必要に応じて医療情報システム事業者等の協力を得ながら、自薬局が保有する情報機器等の全体を網羅する医療情報システムに関する構成図（外部接続点を含むネットワーク構成図等）を作成する。

サーバ、端末 PC、ネットワーク機器を把握できているか。

局内のサーバおよび端末 PC の OS、IP アドレス、使用用途、脆弱性対応状況、ウイルス対策ソフトの稼働状況等の一覧を整備しておく。なお、各 PC にログオンする際に管理者権限でログオンする PC が分かるようにしておく。また、局内設置のすべての VPN 装置、ファイアウォール、ルータ-等の所在と、IP アドレス、使用用途等を明記した一覧を作成する。

(企画管理編：9.1、システム運用編：8.4)

ネットワーク構成図・システム構成図が整備できているか。

HIS 系、インターネット系等の局内 LAN、外部接続点（ファイアフォール、VPN、地域連携、オンライン資格確認等）のネットワーク構成が判別できるように IP アドレスおよびルーティングがわかる構成図を整備しておく。

(企画管理編：4.4、システム運用編：2.、Q&A：概 Q-６)

システム停止が事業継続に与える影響を把握できているか。

各システムが利用できなくなると、どの業務が継続できなくなるか（電子薬歴とレセコンの間で通信ができなくなる等）といった被害を想定し、代替運用の手順を作成しておく。また、代替運用サーバ、参照サーバ、バックアップデータの保持といった非常時対策状況を確認しておく。

（経営管理編：3.4、企画管理編:11）

サーバ、端末 PC、ネットワーク機器の脆弱性への対応ができているか。

サーバ、端末 PC、ネットワーク機器について、薬局が管理する機器と、事業者が管理する機器を明確化し、脆弱性情報の収集、脆弱性対応プログラムの適用基準等を定めておく。

（経営管理編：3.4.2、企画管理編：12）

1-2) 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集

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）への連絡体制図が整備できているか。

非常時の役割や手順を定め、薬局の内部や外部関係機関との緊急連絡先や情報伝達ルートを整備し関係者へ周知しておく。契約書やサービス・レベル合意書(SLA）により、非常時の責任分界点や役割分担について事業者等との明示的な合意内容を確認しておく。

（経営管理編：3.4.3、企画管理編：2.1、12.3、Q&A：企 Q-16）

リスク検知のための情報収集体制が整備できているか。

自薬局に重要な脆弱性情報が事業者から報告されるスキーム（保守契約等）を確立しておく。ファイアウォール、VPN 等外部接続点のアクセスログを定期的に確認する体制を整備しておく。

（企画管理編：12.2、システム運用編：8.2、17）

教育訓練が実施できているか。

策定した BCP が迅速かつ適切に利用できるように、教育訓練を定期的に実施する。システムが利用できなくなることを想定して、障害時マニュアルや伝票運用マニュアルを準備しておく。教育訓練の結果、必要に応じて改善計画を作成する。

（企画管理編：11.⑥）

バックアップの実施と復旧手順が確認できているか。

オフラインバックアップ等サイバー攻撃を想定したデータとシステムのバックアップの実施と復旧手順の確認をしておく。また、復旧手順においては、業務フローを意識して復旧するシステムの優先度（復旧する順序）をあらかじめ設定しておくことが望ましい。

(経営管理編：3.4.1、企画管理編：11.2、システム運用編：11)

【２．検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）】

2-1）システム異常の報告先の把握

異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。

相談窓口の一本化や体系化を組織内で行う。連絡先を局内に掲示したり、情報セキュリティマニュアルなどのわかりやすい箇所に明示する。

（経営管理編：3.4.2）

2-2）システム異常の検知

局内で発生した異常が局内職員によって覚知できるか。

発生部署、発生個所、発生日時、連絡者、異常の状態について、口頭、報告様式等を用いて正確に伝達する。

（経営管理編：3.4.3）

2-3）CSIRT/経営者によるシステム異常の覚知

局内職員から発出されたサイバー被害情報が組織を通じて速やかに CSIRT（対応者）ならびに意思決定者まで到達するか。

連絡経路を組織化し、局内のどの部署から生じたシステム障害であっても、CSIRT と経営者に必ず伝達されるように担当者を整備する。また、組織変更に応じて適宜最新化し、連絡経路が機能することを担保する。

※CSIRT（Computer Security Incident Response Team）：

コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。

【３．初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や調剤への影響を最小限にする。）】

3-1）原因調査（必要に応じて事業者に依頼）

原因調査のため、「ネットワーク機器やケーブル等の調査」、「電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっている

障害の原因としてサイバー攻撃の兆候があるか、医療情報システムのメンテナンス等の問題か、医療情報システム自体の問題か、LAN 設備やケーブルの問題か、設備の電源系統の問題か等調査を実施する。また、情報漏えいの有無を調査する。必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制にする。

3-2）事業者等への連絡と作業履歴の確認

事業者等への連絡と作業履歴の確認ができるか。

障害の前日等に医療情報システムのメンテナンスやデータ移行等の作業の有無を確認し、該当する場合は、当該作業が障害の原因であるかを確認する。

3-3）被害拡大防止

被害拡大防止に向けた対応ができるか。

3-1 による原因調査の結果、サイバー攻撃の兆候がある場合は、ネットワークの遮断により通信を遮断し感染拡大を防止する。その他、バックドアの無効化、無効にされたセキュリティ機能の復帰、攻撃された脆弱性への対応等の被害拡大防止措置を行う。必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制を整えておく。
(企画管理編：3.1.5、システム運用編：18.1)

3-4）経営層への報告、経営層による確認と指示、組織内周知

経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。

サイバー攻撃の兆候等がある場合は、経営層に報告し、対象となる医療情報システム等の使用の中止を指示する。経営層は、対応チーム設置、及び対象となる医療情報システム等の使用中止に伴う業務運用（調剤体制等）方針について検討し、必要に応じて組織内に周知し、対応を求める。（サイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性について検討する。）経営層は調剤を継続する観点で「医療施設の災害対応のための事業継続計画」も参考にしながら薬局全体の事業継続計画を策定する。対象となる医療情報システム等の異常・障害時の、調剤体制、及び医療情報システム等を代替した業務運用方法（紙の調剤録運用、参照系環境構築等）に関する対処についても定めておく。

例）○紙の調剤録運用
・紙伝票の最新化と帳票準備
・運用フローの作成と共有
○ 参照系環境構築
・サーバおよび端末 PC の構築
・プリンタ、印刷用紙、トナー準備

（経営管理編：3.4、企画管理編：11）※ 資料５ リンク集参照

3-5）被害状況等調査（フォレンジック調査*＋証拠保全）と被害状況等の報告

被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。

アクセスログの分析や情報の改ざんや暗号化の有無等からサイバー攻撃の範囲、個人情報漏洩の有無等について調査し、経営層へ報告する。必要に応じて、事業者へ協力を依頼して調査を進める。自機関で証拠保全が可能か検討し、困難な場合は事業者等へ依頼する。経営層へ被害状況等を適時報告する。あらかじめ初動対応の流れについて事業者等と事前に確認しておくこと。

＊フォレンジック調査：

サイバー攻撃で消去・改竄されたデータや攻撃活動のログを取得し、攻撃対象、方法、被害範囲などを解明する調査のこと

（企画管理編：11）

3-6）組織対応方針確認と外部関係機関への報告等の対応

組織対応方針を確認できるか。

被害状況（調剤継続への影響や個人情報漏洩への有無等）に基づいた経営層による対応方針を確認し、対応する。また、被害状況について所管省庁への報告、法的措置、機密情報漏洩等の対応を確認して報告する。

（経営管理編：3.4.3）

【４．復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）】

4-1）経営層からの復旧指示の確認と実施

復旧指示の確認と実施ができるか。

復旧計画、復旧時間、費用等を踏まえて、経営層は復旧計画を指示し、情報システム担当者等は復旧計画の実施を行う。特に、ワークフローを意識してあらかじめ設定した医療情報システムの「復旧優先度」を基に復旧を行う。復旧優先度は、調剤継続を意識して定める「重要度」と異なる場合がある。

（Q&A：企 Q-42）

4-2) 医療情報システム等の事業者等へ復旧対応依頼

（医療情報システム等の）電子薬歴システム等の事業者等への対応依頼ができるか。

自機関で復旧が困難な場合、事業者等へ復旧作業を依頼する。

例）

・情報システム担当者と事業者間で、バックアップ復元手順や対応者を、平時に定めておく。

・復旧に時間を要する場合、代替として、紙の調剤録運用、参照系環境構築を検討する。

（企画管理編：11）

4-3) 再設定や再インストール、バックアップデータ復旧等

再設定や再インストール、バックアップデータの復旧等ができるか。

端末 PC/サーバ復旧手順について、情報システム担当者、事業者等と連携して事前に定め、それに基づき、再設定や再インストール、バックアップからデータ復旧等を実施する。

復旧の際、既知の脆弱性、漏洩した可能性のあるパスワード等に注意する。

（[特集] 医療機関等におけるサイバーセキュリティ:3.3 必要最小限の対策：バックアップ（システム・データ））

4-4) 復旧結果の確認

復旧結果の確認ができるか。

復旧処理について、医療情報システム等が正常に稼働することを確認する。

作業者は手順の進捗状況に合わせて経営層に報告を行い、経営層は組織方針に合わせて運用を変更する。

【5.事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）】

5-1) 復旧結果と情報漏えい事実の有無の報告

復旧結果と情報漏えい事実の有無、可能性について、局内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。

下記を、経営層に報告する（組織内への周知も行う。）。

・異常の内容、原因、被害状況、復旧工数及び費用等について

・復旧結果について

・情報漏えいの有無、範囲について

5-2）再発防止策の検討・策定

再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。

経営層や対策チームを交え、再発防止策の検討・策定を行う。

（経営管理編：1.2.2、3.4.3、企画管理編：2.1.3、3.1.5）

5-3）再発防止策の周知

再発防止策の周知を局内に周知する方法と体制が整備されているか。

確定した再発防止策を、関係者等に周知する。

5-4）再発防止策の実施

再発防止策の実施が行えるか。

定期的なチェック箇所を割り出し、日々の保守業務へのチェック箇所、実施内容、実施者の落とし込みを行う。

5-5）事業者等への再発防止策の指示

事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。

策定した再発防止策を事業者へ周知し業務への反映を指示する。指示した再発防止策が実施できているか定期的に確認する。

（企画管理編：2.1.3）

5-6）外部関係機関への報告と情報公開の検討

情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。経営者と担当者により外部関係機関への報告が行えるか。

経営層と担当者が情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できる体制を備えておく。関係省庁等外部関係機関への報告とサイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性および内容について検討し、経営層の意思決定として策定する。

(経営管理編：1.2.2)

資料５　リンク集

【雛形作成参考 URL】（2024 年 8 月参照）

- 日本薬剤師会　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 Ver.1.00（2024 年 7 月）

https://www.nichiyaku.or.jp/assets/uploads/pharmacy-info/cybersecurity03.pdf

- 岐阜県　ＢＣＰ（事業継続計画）について

https://www.pref.gifu.lg.jp/page/8320.html

- 厚生労働省　サイバー攻撃を想定した事業継続計画（BCP）策定の確認表（令和６年６月）

https://www.mhlw.go.jp/content/10808000/001261299.pdf

- 厚生労働省　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）

https://www.mhlw.go.jp/content/10808000/001266631.pdf

- 厚生労働省　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(令和６年５月)

https://www.mhlw.go.jp/content/10808000/001253958.pdf

- 厚生労働省　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～

https://www.mhlw.go.jp/content/10808000/001253959.pdf

- 厚生労働省　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）

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

- 厚生労働省　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）
[特集] 小規模医療機関等向けガイダンス

https://www.mhlw.go.jp/content/10808000/001102587.pdf

- 厚生労働省　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）
経営管理編（Governance）：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（経営管理編）（令和５年５月）

https://www.mhlw.go.jp/content/10808000/001102573.pdf

- 企画管理編（Management）：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（企画管理編）（令和５年５月）

https://www.mhlw.go.jp/content/10808000/001102575.pdf

- 経済産業省　企業における情報セキュリティガバナンスのあり方に関する研究会 報告書　参考資料　事業継続計画策定ガイドライン

https://www.meti.go.jp/policy/netsecurity/docs/secgov/2005_JigyoKeizokuKeikakuSakuteiGuideline.pdf

- 中小企業庁　中小企業BCP策定運用指針

https://www.chusho.meti.go.jp/bcp/index.html

- 総務省　国民のためのサイバーセキュリティサイト

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

- 独立行政法人情報処理推進機構（IPA）　ここからセキュリティ！情報セキュリティ・ポータルサイト　教育・学習サイト

https://www.ipa.go.jp/security/kokokara/study/company.html

- 政府広報オンライン　「個人情報保護法」をわかりやすく解説　個人情報の取り扱いルールとは？（2022年8月5日）

https://www.gov-online.go.jp/useful/article/201703/1.html

- 政府広報オンライン　マンガで学ぶ個人情報保護法　個人情報取扱い事業者が守るべきルールについて（2022 年 3 月 8 日）

https://nettv.gov-online.go.jp/prg/prg24060.html