情報セキュリティハンドブック Ver 1.0

令和　7年　2月　1日

一般社団法人大阪市阿倍野区薬剤師会

目　次

セキュリティ対策自己宣言

セキュリティ対策自己宣言

1－1　組織の基本ルール

1.1.　OSとソフトウェアのアップデート

1.1.1. OSのアップデート

① パソコンのOSは、Windows Updateの自動更新機能を有効にして、最新の更新プログラムをインストールした状態にする。
② 業務に利用するスマートフォンのOSは、以下の内容を参考に手動で更新する。
- ☛ Android端末の場合：端末毎の情報を常に調べて必要に応じて対応する（MDM利用）。
- ☛ Apple　端末の場合：Apple端末（Wi-Fiを利用）でiOSアップデートを行う。

注）アップデート後は、元のバージョンに戻せないので事前にデータのバックアップを取得する。

1.1.2. ソフトウェアのアップデート

① Windowsの更新時に他のMicrosoft製品の更新プログラムも入手しインストールした状態にする。
② Adobe Flash Player、Adobe　Reader はアップデートを自動に設定する。
③ 業務でスマートフォンを使う場合は、スマートフォンのOS、ウイルス対策ソフトもアップデートする。アップデートの方法が分からない人は、メーカー又は安全管理責任者に確認する。

1.2.　ウイルス対策ソフトの導入

① 業務で利用するパソコン等には、以下のウイルス対策ソフトを導入し定義ファイルを随時更新する。
② 持ち出し用のノートPCは、利用時に必ず定義ファイルの更新をする。
- ☛ パソコン　　：○○○○ウイルス対策ソフト（定義ファイル更新方法　自動）
- ☛ タブレット端末：○○○○ウイルス対策ソフト（定義ファイル更新方法　自動又は手動）

1.3.　パスワードの管理

① ログインパスワードは、仮のパスワードのまま使用せず、最初のログインの時に必ず変更する。
② 自己の管理するID・パスワードは、他人に利用させない。
③ ログインや個人情報などの重要な情報が含まれる電子ファイル（Excelやword等）に使うパスワードは以下の内容に従って設定し利用する。

◎必須	×禁止
８文字以上の文字数で構成されている。 ※推奨は、12文字以上	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない。
アルファベットの大文字と小文字、数字や@、%、&などの記号を組み合わせる。	同じ文字・数字を連ねただけにしない。
ＩＤ・パスワードの使い回しをしない。	他者に見えるところに記さない/教えない。

1－2　組織の基本ルール

1.4.　パソコンや電磁的記録媒体の管理

① 業務で利用するパソコンや電磁的記録媒体（USB、CD-R、MO等）は、盗難防止のため以下のルールに従って管理する。
- ☛ 業務で利用するパソコンは、物理的対策として、セキュリティワイヤー等で固定する。
- ☛ 電磁的記録媒体（USB、CD-R、MO等）は、使用時以外の場合、施錠管理ができるロッカー等に施錠保管する。

注）電磁的記録媒体は、情報が保存される必要がなくなった時点で、必ず削除する。

1.5.　アクセス制御

① 業務で利用する情報システムや機器（パソコンやファイルサーバー等）は、アクセス権限のない従業員等が利用できないように制限する（Adminとguestの設定）。
② 複数名が共有して利用する情報システムや機器（パソコンやファイルサーバー等）は、情報の重要度に応じて利用できるユーザーを限定する（利用者のアクセス制限）。

機器名	アクセス制御の方法	アクセス許可対象者
ファイルサーバー	NAS（ネットワークHDD）	管理(Admin)／一般(guest)
複合機	アクセス権限設定機能	管理(Admin)／一般(guest)
無線ルーター	パスワード／暗号化	管理(Admin)／一般(guest)

1.6.　情報セキュリティに対する注意

① 安全管理責任者は毎週月曜日に以下のサイトを参照し、薬局で利用するIT製品やサービスに関わる重要なセキュリティ情報、緊急情報などが公表された時には、速やかに理事長に報告し、電子メールで、その対策を全従業員に通知する。
② 通知を受けた従業員は、速やかに対策を理解し実行する。

👉 独立行政法人情報処理推進機構（略称：IPA）重要なセキュリティ情報
https://www.ipa.go.jp/security/
👉 JVN （Japan Vulnerability Notes 脆弱性対策情報ポータルサイト）
https://jvn.jp/
👉 一般社団法人 JPCERT コーディネーションセンター
（略称：JPCERT/CC 技術的な立場における日本の窓口CSIRT）
https://www.jpcert.or.jp/

2－1　仕事中のルール

2.1.　電子メールの利用

① 業務で利用するメールは、プロバイダーメール（NTTやOCN等）を必ず利用する。
② フリーメールはウイルス感染力が非常に強いので業務に利用してはいけない。
　☛ フリーメール（Google、Yahoo!等）は、セキュリティの信頼度が低く、情報漏洩に繋がる可能性があり、また受信拒否や迷惑メール設定により大切な連絡が送信できていなかったり、受け取れなかったりすることがある。その他、メール遅延、データ消滅インターネット環境の不可欠等、様々なデメリットがあることから業務での利用してはいけません。

2.2.　電子メールの送信

2.2.1. 電子メールの誤送信対策

① 電子メールを送信する前は、宛先や宛先アドレスが間違っていないか、再度確認してから送信する。

2.2.2. 電子メールの情報漏えい対策

① 複数の外部の人に対して、同時に同じメールを送信する場合は、「TO」に対処となる相手のアドレスを入力し、「BCC」に複数相手のアドレスを指定し、アドレス情報の漏えいを防がなければならない。
　☛ 「CC」を使用して、複数の外部の人に送信した場合、受信者は他のすべての受信者のメールアドレスがわかってしまいます。「CC」を使用する場合は、すべての受信者に、他のすべての宛先及び宛先アドレスを開示する必要があるときに限定する必要があります。
② 重要な情報又は個人情報を送信する場合は、メールの本文に記入せず、以下の方法で送信する。
　☛ 重要な情報又は個人情報は、Excelやword等の電子ファイルに記載し、パスワード設定又は、暗号化したうえでメールに添付して送信する。
　☛ パスワードは先方と予め決めておく、又は携帯電話のショートメッセージサービス（SMS）で知らせるなど、パスワードが他者に傍受されないようにする。

	ウイルスメール	フィッシングメール	スパムメール	標的型メール
イメージ				
分類	コンピューターウイルスの感染を目的とした迷惑メール	金銭や個人情報収集を目的とした迷惑メール	大量に送信される迷惑メール	特定の対象者に何らかの目的をもって送信される迷惑メール

2－2　仕事中のルール

2.2.3. 電子メールの標的型攻撃対策

① 標的型攻撃メールによるウイルス感染を防止するため、以下の内容に十分に注意し、チェックポイントが複数合致する場合は安易に添付ファイルを開いたり、リンクを参照しないでください。

チェックポイント

☛ メールのテーマ（件名・見出し）

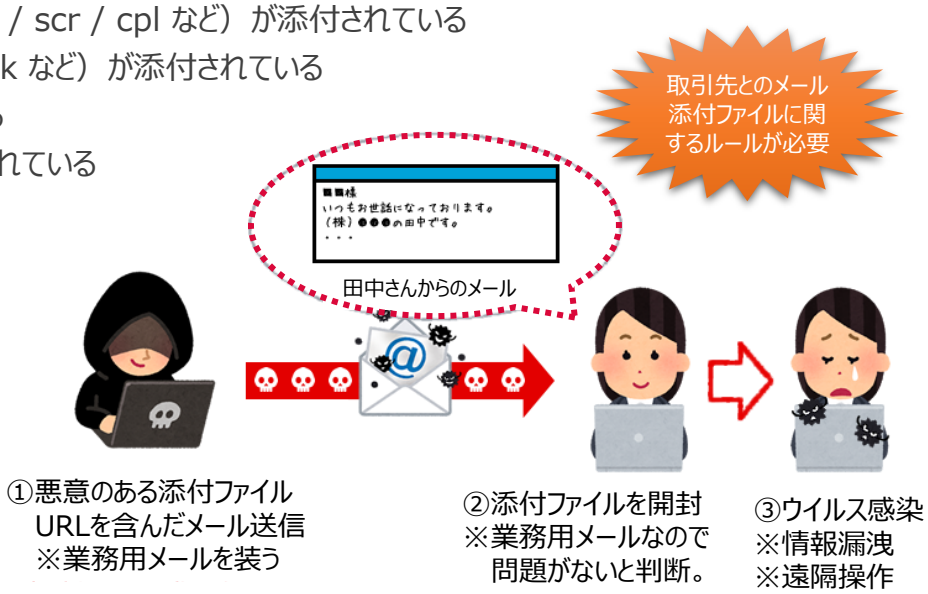
- ✓ 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容
- ✓ 心当たりのないメールだが、興味をそそられる内容
- ✓ これまで届いたことがない公的機関からのお知らせ
- ✓ 組織全体への案内
- ✓ 心当たりのない決済や配送通知 （英文の場合が多い）
- ✓ ID やパスワードなどの入力を要求するメール

☛ 差出人のメールアドレス

- ✓ フリーメールアドレスから送信されている
- ✓ 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なるメールの本文
- ✓ 日本語の言い回しが不自然である
- ✓ 日本語では使用されない漢字（繁体字、簡体字）が使われている
- ✓ 実在する名称を一部に含むURL が記載されている
- ✓ 表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる（HTMLメールの場合）
- ✓ 署名の内容が誤っている

☛添付ファイル

- ✓ ファイルが添付されている
- ✓ 実行形式ファイル（exe / scr / cpl など）が添付されている
- ✓ ショートカットファイル（lnk など）が添付されている
- ✓ アイコンが偽装されている
- ✓ ファイル拡張子が偽装されている



2－3　仕事中のルール

2.3.　インターネットの利用

① 業務でウェブサイト利用する場合は、以下のルールを守る。
- ☛ 不審なサイトへのアクセス及び業務用メールアドレスの登録を禁止する。
- ☛ パスワードをブラウザに絶対保存しない。

② 業務でオンラインストレージサービスを利用する場合は、以下のルールを守る。
- ☛ 業務でオンラインストレージサービスを利用する場合は、安全管理責任者の許可を得る。
- ☛ 従業員、もしくは取引先以外との業務関連情報の共有を禁止する。
- ☛ メールアドレスの登録が必要な場合は、業務用のメールアドレスを登録する。

③ 業務でSNSを利用する時は、以下のルールを守る。
- ☛ 業務の秘密情報の書き込みは行わない。
- ☛ 取引先担当者とSNS上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
- ☛ セキュリティ設定を行い、アカウントの乗っ取りやなりすましに注意する。
- ☛ 使用するスマートフォン、タブレット端末上のデータ、写真、位置情報が、予期せず公開される可能性のあることを理解し十分に注意する。

2.4.　データのバックアップ

① 重要なデータは以下に指定したNAS、HDD、クラウドに保存する。

② 重要なデータを保存したバックアップは、安全管理責任者が以下の要件に従い取得する。

機器名	対象	方法	保管媒体	頻度
サーバー、PC	ファイルのバックアップ データのバックアップ	ｺﾏﾝﾄﾞ ツール設定	NAS、HDD	毎日／月
サーバー、PC	ファイルバックアップ データのバックアップ	アプリ設定 ツール設定	クラウド	毎日／月

2.5.　クリアデスク・クリアスクリーン

① 重要書類、スマートフォン、携帯電話、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体などを業務利用しない場合は、机上に放置せず、施錠保管し、クリアデスクも徹底する。

② 離席の場合は、以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。
- ☛ スクリーンセーバー起動時間を5分以内に設定し、パスワードを設定する。
- ☛ スリープ起動時間を5分以内に設定し、解除時のパスワード保護を設定する。
- ☛ ［Windows］＋［L］キーを押してコンピュータをロックする。

③ 退室時、未使用時にはノートPC、USBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を机の引き出しに保管し、施錠する。

2－4　仕事中のルール

2.6.　重要情報の持ち出し

2.6.1. 重要情報の持ち出し許可

① 重要書類やノートPC、タブレット端末、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体を外部に持ち出す場合、必ず書面にて安全管理責任者の許可を得る。

2.6.2. 重要情報の運搬

① 重要書類やノートPC、タブレット端末、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体を、薬局外に持ち出すときには、以下のルールを徹底する。
- ☛ ノートPC又はタブレット端末に保存するデータは必要最小限にする。
- ☛ 電子媒体はケースに入れ、USBメモリはタグ、ストラップ、鈴などを付け紛失を防止する。
- ☛ 重要書類や電子媒体を持ち出す際は、必要に応じて鍵付きケースに入れる。
  ※鍵付きケースがない場合は、ひも付き封筒を利用することや、USBメモリにストラップや鈴などを付けて紛失防止対策を行う。
- ☛ ノートPCはBIOSパスワード又はWindowsログインパスワードを設定する。
- ☛ 電子データは、必ずファイル暗号化、又はUSBメモリ暗号化機能により暗号化する。

② 重要書類の携行時には以下のルールを徹底する。
- ☛ 電車内では網棚に置かない。
- ☛ 自動車内に置いたまま車外に出ない。
- ☛ 作業中離席する場合は携行する。
- ☛ 他者が画面を覗き見できない状態で使用する。

2.7.　重要情報の保管

① 退室時、未使用時にはモバイル用パソコン、USBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を机の引き出し又は所定のキャビネットに保管し、施錠する。

2.8.　入退室

① 取引先又は関係者以外が入室した場合、発見者は必ず声をかけ、用件を確認する。

② 最終退室者は以下を行う。
- ☛ 全従業員のパソコンがシャットダウンされ、プリンターなど周辺機器、暖房器具、湯沸かし器等発熱機器の電源が切られているか確認する。
- ☛ 全ての出入口の施錠を確認する。
- ☛ 退室時刻と退室者氏名を所定様式に記録する。

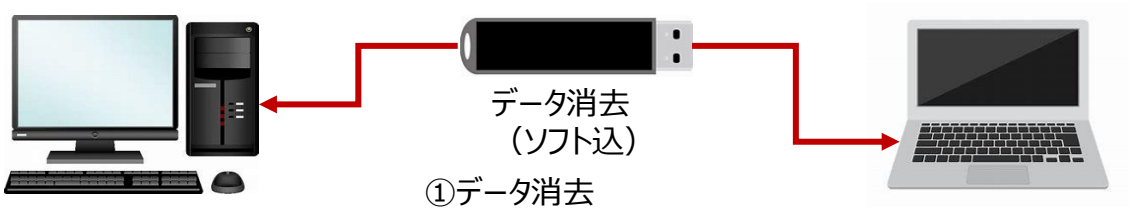
2.9.　電子媒体･書類の廃棄

① サーバー、パソコン、外付けハードディスク等の機器、CD、DVD、USBメモリ等の電子媒体、及び重要書類等の廃棄は、以下のルールに従い廃棄する。

- ☛ パソコン機器等の廃棄は、パソコン内の電子データを消去後、機器を破棄する。なお、電子データ消去及び廃棄を業者委託する場合は、消去証明書、廃棄証明書、作業写真等を取得する。
- ☛ 電子媒体又は重要書類を廃棄する場合は、書面にて安全管理責任者の許可を得る。
- ☛ 廃棄を行う者は、廃棄日時、実施者、廃棄方法等処理内容を記録する。

媒体	廃棄方法
サーバー・パソコン	• ハードディスクを取り出し鈍器等で破壊する。 • ハードディスクのデータ消去を業者に依頼し、消去証明書を取得。
外付けハードディスク	• 鈍器等で破壊する。 • ハードディスクのデータ消去を業者に依頼し、消去証明書を取得。
CD・DVDなどのディスク	• シュレッダーで細断する。 • ディスク内面にカッターでキズを入れる。
FD・USBメモリ	• 鈍器等で破壊する。
重要書類	• シュレッダー（セキュリティレベル７以上）で細断する。 • 溶解又は焼却処分を業者に依頼し、廃棄証明書を取得。

＜参考＞パソコン等のデータ消去方法



【参考】パソコン等のデータ消去及び破壊廃棄委託（SB C&S株式会社）※ｿﾌﾄﾊﾞﾝｸｸﾞﾙｰﾌﾟ

3－1　薬局の共通ルール

3.1.　私有情報機器の利用

① 私有の情報機器（パソコン、モバイル端末及び電磁的記録媒体等）は、業務に利用しない。しかし、業務上やむを得ない場合は、書面にて安全管理責任者の許可を得て利用する。

☛ 私有情報機器の業務利用を許可する場合は、私有情報機器の利用に関する運用ルールを策定する等、必要な安全管理措置を講じる。特に、サイバー攻撃による情報漏洩を防ぐためには、マルウェア対策等の技術的な安全管理措置を講ずる必要がある。

情報機器の種類	順守事項
・パソコン 自宅のパソコンで業務を行う場合も含む 	✓ 私有パソコンの薬局への無断持込みを禁止する。 ✓ 私有パソコンの業務利用を禁止する。 ✓ 私有パソコンの薬局内LANへの接続を禁止する。 ✓ 私有パソコンを利用する場合は、安全管理責任者が指定するウイルス対策ソフト、アプリケーションソフトを導入し、許可を得たうえで利用する。 ✓ 私有パソコンで業務を行った場合、業務終了後に業務用データを薬局の指定するツールで完全に消去する。 ✓ 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する。 ✓ 業務用メールアドレスで受信した電子メールを従業員の個人アドレスに転送することを禁止する。
・スマートフォン ・タブレット ・携帯電話 記憶・通信機能を備えた機器 	✓ 薬局で貸与した機器のみを利用する。 ✓ 業務での利用をすべて禁止する。 ✓ 充電など業務用パソコンへの接続を禁止する。 ✓ 私有スマホ等を利用する場合は、安全管理責任者が指定するウイルス対策ソフト、アプリケーションソフトを導入し、許可を得たうえで利用する。 ✓ 業務用データの保存を禁止する。 ✓ 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する。 ✓ 業務用メールアドレスで受信した電子メールを従業員の個人アドレスに転送することを禁止する。
・USBメモリ ・外付けHDD 記憶機能を備えた機器・媒体 	✓ 薬局でUSBメモリ等の管理台帳を作成管理する。 ✓ 薬局で管理する機器のみを利用する。 ✓ 私有物の利用を禁止する。 ✓ 私有のUSBメモリ等を利用する場合は、書面にて情報システム管理者の許可を得て利用する。 ✓ 薬局でUSBメモリ等の磁気記録媒体の利用記録を作成保存する。 ✓ 私有のUSBメモリ等を利用する場合は、業務終了後に業務用データを薬局の指定するツールで完全に消去する。

3.2.　クラウドサービスの利用

① クラウドサービスを新たな業務に利用する場合は、以下の情報を入手し、必ず書面にて安全管理責任者の許可を得たうえで利用する。

- ☛ サービス提供者が公表する情報セキュリティ方針、プライバシーポリシーなど
- ☛ サービス提供者の情報セキュリティ上の責任範囲を定めたサービス利用規約など
- ☛ サービスに予め又は、オプションで付随する情報セキュリティに関する機能やサービスについて、明記したもの
- ☛ サービス提供者が、情報セキュリティに関わる適合性評価制度の認証を取得している場合は、その証拠となるもの
- ☛ 専門家による監査を実施している場合は、その証拠となるもの

参考となる評価制度	運営組織
情報セキュリティ対策への取組み自己宣言制度	IPA
SECURITY ACTION制度	IPA
適合性評価制度	ISMAP運営委員会
ISMS適合性評価制度	JIPDEC/JAB
プライバシーマーク制度	JIPDEC
PCI DSS	クレジットカード業界セキュリティ基準
クラウドサービスの安全・信頼性に係る情報開示認定制度	ASPIC
インターネット接続安全安心マーク	同推進協議会
情報セキュリティ監査制度	経済産業省/JASA

3.3.　従業員の守秘義務

① 従業員には、薬局の就業規則で定められた守秘義務があります。規則を順守し、このハンドブックに定められたルールを守り、情報セキュリティの事故を防ぎましょう。

3.4.　事故（インシデント）が起きてしまったら

① もしも事故が起きてしまったら、以下の手順に従い、二次被害や事故の影響を最小限に止めましょう。
② 情報セキュリティ事故の定義は以下とします。

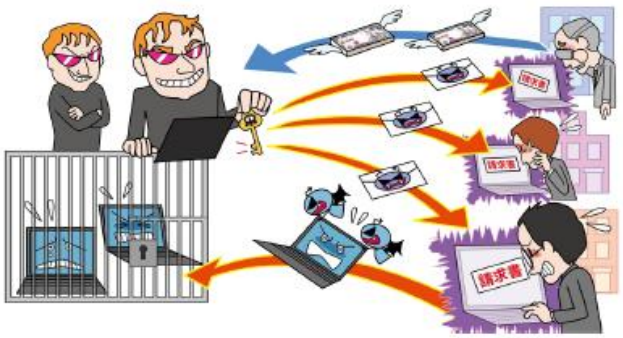
- ☛ 個人情報の「漏えい」「改ざん」の発生、又は「サーバーやパソコンが利用できない」状態になった時に、薬局の業務や患者、取引先、株主、本人（個人情報）に望ましくない影響が及びます。

3.5. 事故発生後の処理手順（サンプル）

① 事故の概要を簡単にまとめる。
↓
② 緊急時連絡網に基づき連絡する。
↓
③ 事故の内容を詳細にまとめる。
↓
④ 情報セキュリティ管理管理者の指示を待つ。
↓
⑤ 事故の対策と対応を実行する。
↓
⑥ 事故報告書を時系列にまとめる。
↓
⑦ 利害関係者へ報告する。

☛攻撃の手口
①メールから感染させる
②WEBサイトから感染させる
③ネットワーク経由で感染させる

☛被害の予防
①バックアップ（電磁的記録媒体）



1．事故の発見者は、安全管理責任者に速やかに連絡する（夜間休日を問わない）！

【緊急連絡先】
① 安全管理責任者　☛ 電話番号：〇〇〇－〇〇〇－〇〇〇〇（自宅・携帯電話含む）
② 情報システム会社　☛ 電話番号：〇〇〇－〇〇〇－〇〇〇〇（自宅・携帯電話含む）
③ 利害関係者　☛ 電話番号：〇〇〇－〇〇〇－〇〇〇〇（自宅・携帯電話含む）

2．安全管理責任者は事故の発生後以下の手順を実施する。

（１）個人情報等の漏洩が起こった場合
① 漏えいした情報の確認
② 影響範囲の全ての組織及び本人（個人情報の場合）に事実を報告
③ 影響範囲の全ての組織及び本人（個人情報の場合）に対策案を通知

（２）回線ダウン、サーバ停止、パソコン停止、ホームページの改ざん
① 原因の調査
② 影響範囲の全ての組織及び本人（個人情報の場合）に事実を報告
③ 復旧策を実施後、影響範囲の全ての組織及び本人に報告

事故対応は緊急時対応／訓練計画、連絡先一覧、組織体制図の作成を行い訓練を実施しないと対応は不可能です！

4－1　情報セキュリティマネジメントサイクル

4.1.　情報セキュリティマネジメントサイクル

4.1.1 情報セキュリティ対策（計画：Plan）

① 情報セキュリティポリシーの策定（基本方針・対策基準）
② 情報セキュリティ実施手順の策定
③ リスク分析事前評価
④ リスクへの対応・対策の検討
⑤ 運用体制とルールの策定
⑥ 運用マニュアル作成（ハンドブック）

情報セキュリティ
目標設定

4.1.2 情報セキュリティ対策（導入：Do）

① 情報セキュリティポリシーの資料配布・周知徹底
② 情報セキュリティ実施手順の資料配布・周知徹底
③ 物理的安全管理措置
④ 人的安全管理措置
⑤ 技術的安全管理措置

情報セキュリティ
運用管理

4.1.3. 情報セキュリティ対策（運用：Check）

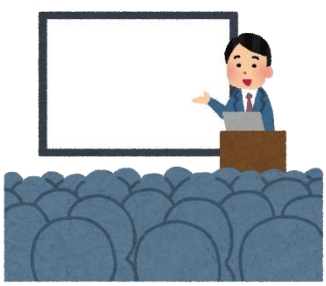
① 情報セキュリティシステムの運用監視
② 情報セキュリティポリシーの遵守状況の確認
③ インシデント発生時の教育訓練
④ 自己点検の実施
⑤ 内部監査の実施

情報セキュリティ
評価監査

4.1.4. 情報セキュリティ対策（評価見直し：Action）

① 自己点検・内部監査結果を踏まえた改善計画の作成
② 情報セキュリティ対策の評価・見直し
③ ガイドラインの評価・見直し
④ 運用体制とルールの評価・見直し
⑤ マニュアルの評価・見直し

情報セキュリティ
是正予防



面倒くさいと思わず、毎年１回以上の情報セキュリティ研修を受け、新たな脅威を学ぶことで、各々の薬局で情報システムの安心で安全な業務利用を継続しましょう。

4.2. 安全管理措置対策

情報セキュリティにおける個人情報の取扱いは、個人情報保護法第20条に記載されている「個人情報取扱事業者はその取り扱う個人データの漏えい滅失又は、き損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」という条文を根拠としています。

4.2.1. 組織的安全管理措置

安全管理について従業員の責任と権限を明確に定め、安全管理に関する規定等を整備運用し、その状況を確認する措置。

① 組織体制の整備
② 個人データの取扱いに係る規律に従った運用
③ 個人データの取扱状況を確認する手段の整備
④ 漏えい等の事案に対応する体制の整備
⑤ 取扱状況の把握及び安全管理措置の見直し

4.2.2. 人的安全管理措置

情報の漏えいを防ぐためのルールを従業員に周知し誓約させ、必要な教育を行う措置。

① 従業員への個人データの適正な取扱いを周知徹底
② 従業員への個人データの適切な教育の実施

4.2.3. 物理的安全管理措置

盗難、紛失、のぞき見等による情報漏えいを物理的に防止する措置。

① 個人データを取り扱う区域の管理
② 機器及び電子媒体等の盗難等の防止
③ 電子媒体等を持ち運ぶ場合の漏えい等の防止
④ 個人データの削除及び機器、電子媒体等の廃棄

4.2.4. 技術的安全管理措置

不正アクセス等による情報漏えい等を防止するために、情報システムへのアクセス制御、不正ソフトウェア対策、暗号化等の技術的な対策を行うこと。

① アクセス制御
② アクセス者の識別と認証
③ 外部からの不正アクセス等の防止
④ 情報システムの使用に伴う漏えい等の防止

4－3　情報セキュリティ基本方針

4.3.　情報セキュリティ基本方針（サンプル）

情報セキュリティ基本方針

○○○薬局（以下、当薬局という。）は、患者からお預かりした当薬局の情報資産を事故・災害・犯罪などの脅威から守り、患者ならびに社会の信頼に応えるべく、以下の方針に基づき当薬局で情報セキュリティに取り組みます。

１．安全管理責任者
当薬局は、安全管理責任者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

２．体制整備
当薬局は、情報セキュリティの維持及び改善のために体制を設置し、情報セキュリティ対策を当薬局の正式な規則として定めます。

３．従業員の取組み
当薬局の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

４．法令及び契約上の要求事項の遵守
当薬局は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、患者の期待に応えます。

５．違反及び事故への対応
当薬局は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日:2025年2月1日
大阪市阿倍野区薬剤師会

このハンドブックの使い方

　このハンドブックは、薬局が保有する大切な情報資産をあらゆる脅威から守っていくために必要となる、基本的な情報セキュリティ対策の概要をまとめたものです。

　機密情報の漏洩や個人情報の流出などのリスクを、薬局として可能な限り軽減するために、情報セキュリティ対策の基本ルールを導入し運用するためにご利用ください。