

医療情報システムの安全管理に関するガイドライン第7.0版対応

薬局における サイバーセキュリティ対策

～患者様の信頼と薬局を守るために今すぐできる具体的アクション～

令和8年度 富山市薬剤師会 研修会 資料

明祥システム株式会社 石田 達也

ご挨拶：明祥システム株式会社について



会社概要

会社名	明祥システム株式会社
代表者	代表取締役 嶺村 和博
設立	2014年10月
所在地	〒920-0392 石川県金沢市無量寺町ハ1番地 (明祥株式会社 本社内)
関連会社	明祥株式会社 株式会社EMシステムズ

事業内容・お問い合わせ

事業内容	・調剤システム事業及びその関連事業 ・医科システム事業及びその関連事業 ・介護/福祉システム事業 ・その他の事業
------	--

お電話でのお問い合わせ

076-266-4167

FAX

076-267-9520

公式ウェブサイト

<https://mei-sys.com/>

自己紹介：石田 達也

居住地

石川県白山市（出身：富山県富山市）

経歴

株式会社EMシステムズ（勤続19年目）

2019年10月に明祥システム株式会社へ出向（現在）

趣味

A I（生成AIパスポート資格）、ドローン（二等無人航空機操縦士）
ツーリング（大型2輪）



メーカー営業の立場ではなく、薬局の皆様が明日から実践できる
具体的なサイバーセキュリティ対策をお伝えいたします

本日のアジェンダ

- 01.なぜ今、サイバーセキュリティ対策が必要なのか
- 02.なぜ医療機関が狙われるのか
- 03.「うちは小さいから(田舎だから)狙われない」の誤解
- 04.薬局を狙うサイバー攻撃の主な種類
- 05.実際に起こったサイバー攻撃とその影響①
- 06.実際に起こったサイバー攻撃とその影響②
- 07.医療情報システムの安全管理に関するガイドラインとは
- 08.第7.0版のポイント①：外部委託の推奨
- 09.第7.0版のポイント②：強固なパスワード管理
- 10.ブルートフォース攻撃（総当たり攻撃）の脅威
- 11.どうやって13桁以上のパスワードを作る？
- 12.第7.0版のポイント③：二要素認証(MFA)の義務化
- 13.二要素認証への対応に向けて
- 14.「もしも」の時の初動対応（サイバー攻撃被害発生時）
15. 同上
16. 同上
- 17.まとめ：今日から始めるサイバーセキュリティ対策
18. 同上
19. 同上
 - ・ 別資料にてサイバーセキュリティ対策チェックリストの説明
 - ・ 質疑応答（10分程度）

本日は、難しい専門用語は極力避け、
「薬局の現場で明日から何をすべきか」を具体的にお伝えします。

1.なぜ今、サイバーセキュリティ対策が必要なのか

■ 2021 年10月 オンライン資格確認の本格運用開始

■ 2022 年(令和 4年)の転換点
大阪急性期病院等のサイバー被害 による
業務停止があり全国的に 問題化。

■ 2023 年(令和 5年) 4月 法的義務化
薬機法改正により、セキュリティ確保が 義務化。

■ 2023 年6月 チェックリスト導入
「サイバーセキュリティ対策チェックリスト」
を用いた 運用開始。

令和5年度チェックリスト(初代)

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

医療機関確認用

チェック項目	確認結果 (日付)	
	1回目	2回目
1 体制確認	(1) 医療情報システム安全管理責任者を設置している。 はい/いいえ/ (/)	はい/いいえ/ (/)
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。	
	(1) サーバ、端末 PC、ネットワーク機器の点検管理を行っている。 はい/いいえ/ (/)	はい/いいえ/ (/)
	(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。 はい/いいえ/ (/)	はい/いいえ/ (/)
	(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指示書(MDS/SDS)を提出してもらった。 はい/いいえ/ (/)	はい/いいえ/ (/)
	サーバについて、以下を実施している。	
	(4) 利用者の権限・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。 はい/いいえ/ (/)	はい/いいえ/ (/)
	(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。 はい/いいえ/ (/)	はい/いいえ/ (/)
	(6) アクセスログを管理している。 はい/いいえ/ (/)	はい/いいえ/ (/)
	ネットワーク機器について、以下を実施している。	
	(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。 はい/いいえ/ (/)	はい/いいえ/ (/)
(8) 接続元制限を実施している。 はい/いいえ/ (/)	はい/いいえ/ (/)	
3 インシデント発生に備えた対応	(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)への連絡体制がある。 はい/いいえ/ (/)	

● 各項目の考え方や確認方法等については、「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マニュアル-医療機関・事業者向け」をご覧ください。
● 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

2022 年の大阪の病院での大規模なサイバー被害がきっかけ。
これまでは対応が **努力義務**とされておりましたが、
そこから薬局でもサイバーセキュリティ対策順守が **義務化**になりました。

2. なぜ医療機関が狙われるのか？

これまで「医療機関は閉じたネットワークだから安全」と言われていましたが、現在は状況が一変しています。

■オンライン資格確認等の普及

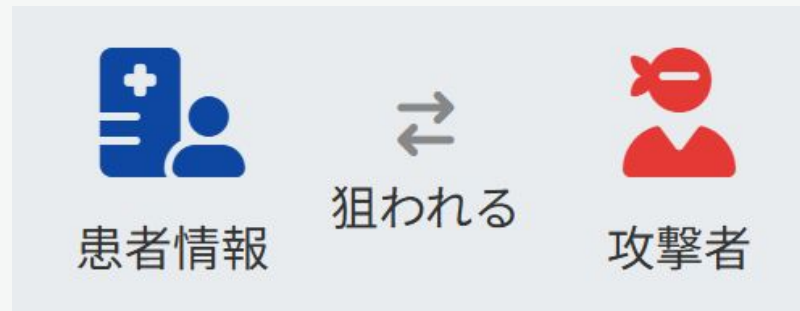
外部ネットワークとの接続が必須に。

■情報の価値が高い

患者の個人情報・病歴は、闇サイトで高値で取引される。

■人命・業務への影響が甚大

システム停止が致命的なため身代金(ランサム)を払いやすい
とされている。



3. 「うちは小さいから（田舎だから）狙われない」の誤解

サイバー空間に「小さい」「大きい」「田舎」「都会」もありません。すべての薬局が隣同士です。



現実世界の空き巣

距離と手間の壁がある

「海外や国内の遠方に住んでいる泥棒がわざわざ遠くの小さな薬局にまで、交通費や時間をかけて来ることは考えにくい」

物理的な犯罪においては、標的を選ぶ際に必ず労力やコストがかかるため**この感覚は正解**です。



サイバー攻撃の実態

自動・無差別・24時間

攻撃者はプログラムを使い、世界中の数百万もの通信口(IPアドレス)を**自動でスキャン**しています。

「特定の薬局を狙う」のではなく、24時間365日巡回し**「たまたま鍵が開いていたパソコンや機器（古いVPN等）」**を見つけて侵入するのです。



インターネットに繋がっている以上、規模や立地に関わらず世界中からの標的になります。

「うちだけは大丈夫」という思い込みを捨て、確実な戸締まり（セキュリティ対策）を行いましょう。

4. 薬局を狙うサイバー攻撃の主な種類



ランサムウェア(身代金要求型)

電子薬歴やレセコンのデータを勝手に暗号化して使用不能にし、復旧と引き換えに身代金を要求します。**医療業界で最も被害が多く、業務停止に直結**する深刻な攻撃です。



標的型攻撃メール・Emotet

実在の取引先や薬剤師会からの連絡を装ったメールを送信し、添付ファイルや不正URLを開かせます。感染すると、**個人情報の漏洩や他の端末への感染拡大**を引き起こします。



サプライチェーン攻撃

セキュリティ対策が手薄な関連企業や取引先（小規模な薬局など）を踏み台にして、本丸である**大病院やシステム会社のネットワークへ侵入**する巧妙な手口です。



不正アクセス(脆弱性・認証突破)

古いVPN機器の弱点（脆弱性）を突いたり、推測されやすい短いパスワードを総当たり攻撃（ブルートフォース）で突破し、**外部からシステムを不正に操作**します。

5. 実際のサイバー攻撃被害事例 ①

【事例】徳島県 つるぎ町立半田病院（2021年10月）

【事象】ランサムウェア感染

身代金要求型ウイルス「ランサムウェア」に感染し、電子カルテシステムが暗号化され使用不能に。

【原因】VPN装置の脆弱性

外部からリモートメンテナンス用に設置していたVPN装置の脆弱性を突かれ、ネットワーク内部へ侵入された。

【影響】長期にわたる業務停止

- 約2ヶ月間、電子カルテが完全に停止
- 新規患者の受け入れ停止
- 紙カルテでの代替運用による現場の大混乱

【復旧費用】

システム再構築等に伴う莫大なコスト

総額 約**2億円**の被害

※出典：つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議 調査報告書

6. 実際のサイバー攻撃被害事例 ②(サプライチェーン)

【事例】 サプライチェーン攻撃 大阪急性期・総合医療センター（2022年10月）

【事象】 委託業者経由でのウイルス侵入

病院のシステム自体ではなく、取引のある「給食提供事業者のネットワーク」を経由してランサムウェアが侵入。

【原因】 取引先のセキュリティの甘さ

サプライチェーン（取引先）の脆弱な部分を踏み台にされ、本丸である基幹システムがダウンし業務停止に追い込まれた。

【警鐘】 薬局に潜む重大なリスク

「薬局」も医療ネットワークの一部

地域の病院やシステム会社とネットワークで緊密に連携しているからこそ、強固な対策が求められます。

自局が「侵入口」になる危険性

セキュリティ対策が手薄な薬局が「踏み台」にされ、提携先の大病院や基幹システム全体を麻痺させてしまうリスクがあります。

※出典：大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 報告書

7.医療情報システムの安全管理に関するガイドラインとは？

厚生労働省が策定する、

医療機関が遵守すべきセキュリティのルールブックです。

時代の変化に合わせて継続的に改定されています。

最新は「第7.0版」（2026年6月公表）

サイバー攻撃の激化と、人材不足の現状を踏まえ大幅な改定が行われました。

ガイドラインへサイバーセキュリティ基本法も追加

【主な改定ポイント】

- 小規模医療機関・薬局向けの「**保守委託機関編**」を新設（外部委託の推奨）
- パスワードルールの変更**（定期変更の廃止、使い回し禁止等の徹底）
- 令和9年度（2027年度）からの**二要素認証の義務化**

8.第7.0版のポイント①：外部委託の推奨

第7.0版では、専任のシステム担当者がいない小規模な薬局等を対象とした「保守委託機関編」が新設されました。



自力での対策は限界

高度なサイバー攻撃に対し、薬局のスタッフだけでセキュリティを担保するのは不可能です。



クラウド・専門業者の活用

適切なクラウドサービスを利用しセキュリティ対策を専門事業者(ベンダー)に委託することが**推奨**されています。

9.第7.0版のポイント②：強固なパスワード管理

「パスワードの定期変更」は不要になりました

過去には「数ヶ月に一度変更する」ことが推奨されていましたが、第7.0版でこの要件が**削除**されました。

【なぜ定期変更はダメなのか？】

- ・「Password1」「Password2」のような推測されやすい規則的な変更をしがち。
- ・忘れないように付箋に書いてPCに貼るなど、本末転倒な事態を招くため。
- ・8桁程度のパスワードでは瞬時に突破される状況になったため。

現在の常識

定期変更よりも「長く複雑なパスワードを設定し、他システムと使い回さない」ことが最も重要です。

10.ブルートフォース攻撃（総当たり攻撃）の脅威

攻撃者は、特殊なプログラムを使い、考えられるパスワードの組み合わせを片っ端から入力して突破を試みます（ブルートフォース攻撃）

現在、パソコンの性能（特にグラフィックボード＝GPU）が劇的に向上しており、**短いパスワードは「数秒～数分」で解読されてしまいます。**

【表】ブルートフォース攻撃による解読に要する最大の時間（2024年基準）

桁数	数字のみ	英字(小)のみ	英(大小)+数+記号
6桁	瞬時	瞬時	瞬時
8桁	瞬時	瞬時	約 39分
10桁	瞬時	約 58分	約 5ヶ月
12桁	瞬時	約 2年	約 3万年
13桁	瞬時	約 64年	約 200万年以上



※一般的なGPUを用いた場合の理論上の解析時間（Hive Systems 2024年の調査等を参考）

最低でも「13桁以上（英大小・数字・記号混在）」を設定すれば、ブルートフォース攻撃による突破は事実上不可能と考えられます。

11.どうやって13桁以上のパスワードを作る？

「13桁の複雑なパスワードなんて覚えられない！」という方へ。

おすすめ：パスフレーズ方式（文章にする）

自分だけが分かるフレーズ(文章)をローマ字や英単語にして組み合わせます

【例】 「私は毎朝7時にコーヒーを飲む」 ⇒ **I-drinkCoffee!7am!**

※これで18桁（英大小・数字・記号入り）になります。

端末ごとのアカウントには、このような強固なパスワードを設定してください。
一定回数パスワードを間違えるとロックされる「アカウントロック機能」の設定も求められています。

12.第7.0版のポイント③：二要素認証(MFA)の義務化

パスワード（知識）だけでは、万が一漏洩した際に防げません。
そこで、別の要素を組み合わせるのが二要素認証（多要素認証）です。

知識情報

パスワード、PINコード

+

所持情報

スマホSMS、ICカード
専用アプリ

or

生体情報

指紋、顔認証
虹彩認証

【ガイドライン第7.0版の重要ポイント】

令和9年度（2027年度）から、サーバ及びクライアント端末における
「二要素認証」が義務化される予定です。

13.二要素認証への対応に向けて

令和9年度の義務化に向けて、薬局でも準備を進める必要があります。

■対象機器

レセコン、電子薬歴、オンライン資格確認端末など、患者情報を扱う端末。

■猶予措置について

令和9年4月1日時点で対応が困難なシステムについては「次期システム改修時までの猶予」が緩和措置として設定されています。

【英(大小)を含めた13桁以上のパスワード】

二要素認証を採用するまでの間については、英(大小)を含めた13桁以上のパスワードを使用することをガイドラインで求められています。

14. 「もしも」の時の初動対応（サイバー攻撃被害発生時）①

画面の異常やウイルス感染の疑いがある場合、被害拡大を防ぐための迅速な対応が必要です。

① 初動対応(隔離) - ネットワークからの切り離し

感染したPCのLANケーブルを
直ちに抜き、Wi-Fiをオフにします。



被害を他の端末や
広域サーバーへ
広げないための
最重要手順です。



電源は「切らない」



原因調査(ログの解析)のためPCの電源は切らず、
状態で放置。 (強制終了は証拠隠滅に繋がります)



身代金要求画面(ランサムウェア)
が出ても、絶対に支払い絡をしてはけません。

15. 「もしも」の時の初動対応（サイバー攻撃被害発生時）②

画面の異常やウイルス感染の疑いがある場合、被害拡大を防ぐための迅速な対応が必要です。

② 報告・連絡 - ネットワーク障害発生時の対応手順

1. システム保守業者への連絡



2. 関係機関への報告義務



個人情報漏洩の可能性がある場合は、
速やかに報告します。

3. 警察への相談



サイバー犯罪の
被害として、
管轄の警察署への
通報・相談を行います。



16. 「もしも」の時の初動対応（サイバー攻撃被害発生時）③

画面の異常やウイルス感染の疑いがある場合、被害拡大を防ぐための迅速な対応が必要です。

③ 業務継続と復旧 - BCPの発動とシステム復元



BCP(事業継続計画)
の発動

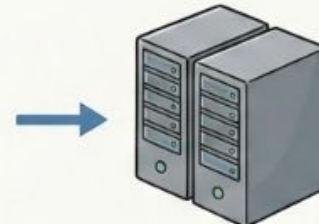


安全確認後のバックアップ復元

専門業者の指示のもと、ネットワークの安全性が確認された後、オフラインまたはクラウドに退避しておいたバックアップデータが元します。



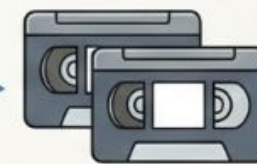
安全確認済み
ネットワーク



サーバー



クラウドバックアップ



バックアップテープ

17.まとめ：今日から始めるサイバーセキュリティ対策

日々の業務における基本的なセキュリティ対策は、大きく3つのアプローチに分類されます。

技術的対策 - システムとデータを守る

☐ OS・ソフトの
最新化



脆弱性（セキュリティの弱点）を狙う攻撃を防ぐため、常に最新のアップケータップデートを適用します。

☐ パスワードの強化
と多要素認証



二要素認証または推測されにくい13桁以上パスワードを使用します。

☐ ウイルス対策
ソフトの導入



マルウェアの侵入をシステム側で検知し、防御します。

☐ データの定期
バックアップ



ネットワークから切り離したオフラインバックアップ、または安全なクラウドバックアップに保存します。

18.まとめ：今日から始めるサイバーセキュリティ対策

日々の業務における基本的なセキュリティ対策は、大きく3つのアプローチに分類されます。

人的対策 - スタッフのリテラシー向上

☐ 不審なメール・リンク・リンクの遮断



フィッシング詐欺や標的型メールの不審な添付ファイル、URLを絶対に開かないよう徹底します。

☐ セキュリティ教育の実施



新たな手口を知るための定期的な勉強会や、訓練・研修をスタッフ全員で実施します。

☐ ルール化の徹底



業務データの持ち帰り制限やフリーWi-Fi利用時の注意点などを明文化し、遵守させます。

19.まとめ：今日から始めるサイバーセキュリティ対策

日々の業務における基本的なセキュリティ対策は、大きく3つのアプローチに分類されます。

物理的対策 - 機器や設備の保護

☐ 外部記憶媒体の管理



私物のUSBメモリなどの接続を禁止し、物理的なウイルス感染や患者データの持ち出しを防ぎます。

☐ 調剤室等の立ち入り制限



レセコンのサーバーや重要な情報があるエリアへの、患者様や部外者の立ち入りを物理的に制限します。

☐ クリアスクリーン・クリアデスク



離席時は必ずPCの画面をロックし、机上にも個人情報を含む書類を放置しない運用を徹底します。

別紙「サイバーセキュリティ対策チェックリスト」にて
それぞれの項目についてご説明いたします。

ご清聴ありがとうございました

本資料は薬局におけるサイバーセキュリティ対策の参考として作成したものです。
攻撃手法や制度/ガイドラインは日々変化しますので、最新の情報をご確認ください。