令和６年 11 月

「サイバーセキュリティ対策チェックリスト」

に関するＱ＆Ａ

本 Q&A の参照箇所の使い方

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。

Q-1　事業者の医療情報システム安全管理責任者とはどのような人物を指し、求められる資格・職種などはありますか？（１-(１)）※

※サイバーセキュリティ対策チェックリストマニュアルにおける １ 体制構築の(１)を指します。

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。

Q-1　事業者の医療情報システム安全管理責任者とはどのような人物を指し、求められる資格・職種などはありますか？（1-(1)）

A：医療情報システムを担当している方の中の責任者を一般的に指します。具体的な能力や経験については、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の 32 頁（イ） 医療情報システム等の提供に係る体制 をご参照ください。
https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20230707.pdf

2 医療情報システムの管理・運用

Q-2　医療情報システムの定義は何か？（2）

A：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、電子カルテ、オーダリングシステム等）。これらには、事業者から提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムも含まれます。また、PC に医療情報を含んだ患者情報を記録したファイルを保管している場合や、管理用ソフトウェア等で医療情報を取り扱っている場合、それは医療情報システムの一部となります。

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。

Q-3　対象となる医療情報システムはインターネットにつながっているシステムだけでよいのか？（2-(1)）

A：インターネット接続有無にかかわらず、医療機関等で扱う医療情報システムはすべて対象です。

Q-4　勤怠管理システム等、医療機関等の職員の情報を扱うシステムはチェックリストの対象となるか？（2-(1)）

A：医療情報を扱わないシステムはチェックリストの対象外ですが、職員の個人情報を取り扱う場合には、個人情報保護に関する基本方針（平成 16 年４月２日閣議決定、令和４年４月１日一部変更）に基づき、適切な管理に努めてください。

Q-5　UTM（統合脅威管理：Unified Threat Management)を提供している場合、このネットワーク内にプリンタやスキャナなどもあるため、医療情報システムがどこまで対象か知りたい。（2-(1)）

A：医療情報システムに接続されており、複合機で印刷時にデータを保存する機能がある場合、プリンタやスキャナも医療情報システムとして台帳管理する必要があります。医療情報を扱わないシステムの場合は対象外です。ただし、UTM、HUB 等のネットワーク機器は医療情報システムのネットワーク接続されている場合は対象となります。

Q-6　複数のベンダーと契約して構成された医療情報システムを、医療機関等と直接契約しているＡ社が提供している。医療機関等はいずれの事業者に事業者確認用を依頼すべきか？（2-(1)）

A：直接契約を結んでいるＡ社に依頼します。

2-(2) リモートメンテナンス（保守）している機器の有無を確認した。

Q-7　代理店が商流に入るため医療機関等に直接販売していない場合、この項目の記載は必要ですか？（2-(2)）

A：はい、必要です。リモートメンテナンス（保守）を利用している全てのシステム・機器について、代理店の有無に関わらずチェックリストを提出してください。

Q-8　「契約のある事業者」とは具体的にどのような契約を指すのですか？（2-(2)）

A：チェックリストにおいて、「契約のある事業者」とは、医療機関等とリモートメンテナンス（保守）契約を結んでいる事業者を指します。

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。

Q-9　代理店として製造業者から製品を卸して販売している。保守、サポート共に製造業者が実施しており医療機関等との契約は販売のみ。MDS/SDS はどの事業者から提出すればよいか。（2-(3)）

A：造業者および保守、サポート等のサービスを提供している事業者から提出します。

Q-10　ビジネスチャットツールや SNS 等を用いて院内で患者情報（入退院履歴）を管理している。MDS/SDS を事業者に求めるべきか。（2-(3)）

A：SNS（Social Networking Service）等の Web サービスを利用して患者の医療情報を取り扱う場合、当該サービスは医療情報システムに該当し、ガイドラインの基準を満たす必要があります。特に、SNS の場合、セキュリティが十分に確保されていないサービスもあることから、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公表している「医療情報連携において、SNS を利用する際に気を付けるべき事項」を参考に、適切な対策を講じてください。
https://hispro.or.jp/open/pdf/SNS_RiyouCheckJikou_20160126.pdf

Q-11　チェックリストが令和５年度版から令和６年度へ改訂されたが、MDS/SDS を再度提出してもらう必要があるのか？（2-(3)）

A：MDS/SDS は対象システムの契約更新や、仕様変更などがなければ再提出の必要はありません。

2-(6) アクセスログを管理している。

Q-12　アクセスログはサーバだけでよいか？OS のアクセスログ、ソフトのアクセスログのどちらを確認すればよいか。（2-(6)）

A：チェックリストでは、サーバについてアクセスログの管理を確認しています。OS のログを管理してください。

Q-13　アクセスログは事業者に依頼しないと解析できないが、管理しているとみなして良いか。（2-(6)）

A：管理しているとみなすことができます。必要な際に確認や調査等が実施可能な体制であることが重要です。

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。

Q-14　可用性を損なうおそれがあり、サーバや端末 PC へのセキュリティパッチの適用が困難な場合、どのような対策を講じたらよいか。（2-(7)）

A：一般的に、情報システムは可用性（安全性、安定稼働）が最優先されるが、機微な情報を取り扱う医療情報システムにおいては、「既知の脆弱性を放置し、攻撃リスクを受容する」という選択肢は許容できるものではない。

このため、自組織の特性をふまえて経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施することが求められる。

例えば、医療情報システムの安定稼働への影響から、最新ファームウェアやプログラム更新などのリスク低減策の実施ができないと判断される場合には、下記①②等の対策を講じることが求められる。

① ログや通信の監視等の代替策の実施によりリスク低減を図る。

② ネットワークの分離等の代替手段を使用し、当該システムがインターネットからアクセスできないようにする。

また、USB メモリ等によるインターネットを介さない攻撃の存在を考慮すると上記のみでは十分とは言えず、端末 PC についても USB メモリの接続制限等の運用管理規定を策定することが重要となる。

加えて、医療情報システムを、今後新規導入又は更新するに際しては、保守契約の見直しや運用管理規程の変更により、セキュリティパッチを定期的に適用できる等適切な安全管理体制の構築に努めること。

Q-15　オンライン資格確認システムについて、チェックリストの対象となるのか。（2-(7)）

A：オンライン資格確認システムも対象です。

2-(8) 接続元制限を実施している。

Q-16　接続元制限の判断はどのようにすべきですか？（2-(8)）

A：接続元制限の判断は、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、システム運用編 13.ネットワークに関する安全管理措置を参照してください。

３ インシデント発生に備えた対応

Q-17　インシデント発生時の連絡体制図には必ず外部有識者（顧問弁護士など）を含める必要がありますか？（3）

A：チェックリスト対策マニュアルに記載した連絡体制図は一例ですので、外部有識者を含めることは必須ではありません。

Q-18　インシデント発生時に連絡する都道府県警の担当部署はどこですか？（3）

A：最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口に通報・相談をお願いします。

(警察のサイバー犯罪相談窓口)
https://www.npa.go.jp/bureau/cyber/soudan.html

４　その他　サイバーセキュリティ対策チェックリスト全般について

Q-19　「事業者確認用」の令和６年度中の端末 PC について、クラウドサービスを提供している場合、対象外でよいか？

A：医療機関等で利用しているクライアント PC について回答してください。

Q-20　多数のレセコンを導入しており、複数業者契約がある場合は契約している業者にそれぞれ事業者確認用を送付するのでしょうか？

A：複数契約している場合は、それぞれ事業者確認用チェックリストへの記載を依頼してください。

Q-21　開発・サーバ運用は事業者 A で、事業者 B が病院への販売、保守契約を担当している。病院との直接契約は事業者 B であるが事業者 B に問い合わせた結果、セキュリティパッチが適用されているかなどの情報が不明であった。どのように対応すればよいか？

A：事業者 B から、開発・サーバ運用を行っている事業者 A に確認するように依頼してください。