医師会共同使用施設（病院、健診・検査センター）運営実態調査

サイバーセキュリティ編　調査票

本調査は、日本医師会総合政策研究機構（日医総研）の調査研究として、全国の医師会共同利用施設を対象に実施しております。
ご多用のところ大変恐縮ですが、調査へのご協力のほど何卒よろしくお願い申し上げます。

サイバーセキュリティ編　調査票　目　次

Ｓ１　医療情報システムの利用状況

Ｑ１－１（医療情報システムの利用状況）

医療情報システムの利用状況、ならびに内外との接続状況（他のシステムやインターネット）について、お答えください。

※ひとつのシステムに複数の機能がある場合は、その機能に該当するシステムすべてに対してお答えください。例えば、電子カルテシステムが医用画像管理システムを兼ねている場合は、（２）と（５）の両方にお答えください。

※ここでのインターネット接続とは、インターネットに直接つないでいる状態を意味し、インターネットＶＰＮ（インターネット上に仮想的な専用ネットワークを構築する技術）を使っている場合は含みません。

（１）　医事会計システム（レセコン）
（２）　電子カルテシステム
（３）　オンライン資格確認システム
（４）　オンライン請求システム
（５）　医用画像管理システム
（６）　オーダリングシステム・オーダリング連携システム
（７）　診療予約システム
（８）　健康診断システム（健診・人間ドック等の受診者管理システム）
（９）　遠隔診療システム（オンライン診療システムを含む）
（10）　地域医療連携システム（医療連携、医療・介護連携のシステム）
（11）　検査機器連携・データ収集システム（生理検査システム、検体検査システム（LIS）等）
（12）　検査報告書作成・出力システム（検査結果の報告・結果出力・配信のシステム）

※上記（１）～（12）の選択肢は、すべて以下となります。
a. 施設内の他のシステムやインターネットとの接続はしていない
b. インターネットとは接続していないが、施設内の他のシステムと接続している
c. 施設内の他のシステムとは接続していないが、インターネットと接続している
d. 施設内の他のシステムとインターネットの両方に接続している
e. このシステムは使っていない

Ｑ１―２（データのバックアップ）

※Q1-1 で（１）レセコン、（２）電カル、（５）医用画像管理システムを使っているとお答えした方にお尋ねします。

使っている医療情報システムのデータ・バックアップ方法についてお答えください。以下の選択肢から、あてはまるものをすべて選んでください。（複数選択可）　*※(1)、(2)、(5)それぞれについてお答えください（下方に入力表があります）。*

【オンプレミス（内部設置型）】

a.　サーバのミラーリング運用

b.　NAS（Network Attached Storage）

c.　外付け HDD や RAID ストレージ

d.　テープ装置（LTO など）

【オフサイト（外部保存型）】

e.　クラウドストレージ（IaaS 型・SaaS 型）

f.　専用のバックアップセンター（データ保管サービス会社等）

g.　他施設への遠隔バックアップ（系列病院・連携機関等）

h.　物理媒体（HDD・テープ等）の施設外での保管

i.　上記以外の方法（　　自由記載、100 字、任意　　）

j.　バックアップは取っていない

※それぞれのデータ・バックアップ方法について、上記選択肢からお答えください。

（１）レセコン	
（２）電カル	
（５）医用画像管理システム	

Ｓ２　システム管理の人員・組織体制

Ｑ２－１（情報システムの管理体制）

情報システムの管理体制について、もっともよくあてはまるものを以下の選択肢からひとつ選んでお答えください。

a. 専任の担当部門がある
b. 専任の担当部門はないが、委員会等を設置している
c. 専任の担当部門や委員会等はないが、専任の担当者がいる
d. 専任の担当部門、委員会等や専任の担当者はいないが、兼務の担当者がいる
e. 上記のような管理体制はない

Ｑ２－２（保守・メンテナンス契約の状況）

システムベンダー等と締結している情報システムの保守・メンテナンス契約におけるサイバーセキュリティ対策に関する責任分界点について、もっともよくあてはまるものを以下の選択肢からひとつ選んでお答えください。

a. 責任分界点について記載があり、保守・メンテナンス契約料金に含まれている
b. 責任分界点について記載はあるが、保守・メンテナンス契約料金には含まれていない
c. 責任分界点について記載はないが、システムベンダー等との話し合いはされている
d. 責任分界点について記載はなく、システムベンダー等との話し合いもされていない

※厚生労働省のガイドラインでは、医療機関とネットワークを介したサービスを提供する事業者やネットワークを提供する通信事業者（システムベンダー等）との間でサイバーセキュリティ対策に関し予め可能な限りの事態を想定し、両者間の責任の分担（責任分界点）について明記しておくこととされています。

Ｑ２－２①

※Q2-2 で c. または d. とお答えの方にお尋ねします。

責任分界点について保守・メンテナンス契約上の記載がない理由について、もっともよくあてはまるものを以下の選択肢からひとつ選んでお答えください。

a. 責任分界点に関する厚生労働省ガイドラインを認識していなかった
b. 責任分界点に関する厚生労働省ガイドラインは認識しているが、差し迫ったリスクを感じず後回しになっていた
c. 責任分界点に関する厚生労働省ガイドラインは認識しているが、保守・メンテナンス契約料金の問題から進んでいなかった

Ｑ２－３（サイバーセキュリティ教育の実施状況）

サイバーセキュリティ対策に関する従業員教育の実施状況についてお答えください。

a. 毎年実施している
b. 毎年ではないが、定期的に実施している
c. 不定期に実施している
d. 実施していない

Ｓ３　ＩＣＴ資産管理

Ｑ３－１（ネットワーク構成図の管理）

院内の情報システム・ネットワークを外部に説明できる資料（ネットワーク構成図）を持っていますか。その資料の更新状況と共にお答えください。

a. 資料を持っており、定期的に更新を行っている
b. 資料を持っており、システム更新のタイミング等で、不定期に更新を行っている
c. 資料を持っているが、見直しや更新は行っていない
d. 資料は持っていない
e. わからない

Ｑ３－２（情報システムのアカウント管理）

情報システムのアカウント（ＩＤ、ＰＷ、アクセス権限等）の管理状況についてお答えください。

a. 定期的にアカウントの棚卸を実施し、不要アカウントの削除やパスワード管理、アクセス権限の見直し等を行っている
b. システム更新のタイミング等で、不定期に不要アカウントの削除やパスワード管理、アクセス権限の見直し等を行っている
c. 不要アカウントの削除やパスワード管理、アクセス権限の見直し等は行っていない
d. わからない

Ｑ３－３（脆弱性情報の入手経路）

情報システムの脆弱性に関する情報をどのような経路で入手していますか。あてはまるものをすべて選んでください。（複数選択可）

a. 厚生労働省からの通知やウェブサイト
b. 内閣サイバーセキュリティセンターや警察庁からの情報
c. 医師会、病院団体からの情報提供
d. 情報セキュリティに関わる専門機関（JVN や JPCERT/CC 等）の情報
e. IPA（情報処理推進機構）のメールマガジンやウェブサイト
f. ソフトウェア・機器等のベンダーからの公式通知
g. 導入している情報システムの保守・運用業者からの情報
h. セキュリティベンダー・外部サービスによる通知・監視サービス
i. 自院の情報システム担当者が独自に収集

j. その他（　　）

k. システムの脆弱性に関する情報収集は行っていない

Ｑ３－４（ＶＰＮ機器の利用状況と脆弱性の管理）

ＶＰＮ（Virtual Private Network；仮想専用線）を利用していますか。

a. 利用している

b. 利用していない

c. わからない

Ｑ３－４①

※Q3-4 で a. とお答えの方にお尋ねします。

ＶＰＮの用途について、お答えください。（複数選択可）

a. 医師やスタッフの外勤・出張先からのアクセス用

b. 従業員の在宅勤務やリモートワーク用

c. 外部業者によるシステムの保守・メンテナンス用

d. 院内の情報システム担当者による遠隔管理用

e. その他の用途（　　）

Ｑ３－４②

※Q3-4 で. a とお答えの方にお尋ねします。

お使いのＶＰＮ機器の脆弱性への対応の状況についてお答えください。

a. 脆弱性情報を確認し、適宜対応している

b. 脆弱性情報を確認したが、対応できていない

→　対応できていない理由を教えてください（　自由記載、100 字、任意　）

c. 脆弱性情報を確認していない

Ｓ４　対策費用と保険、ＢＣＰ

Ｑ４－１（対策費用）

サイバーセキュリティ対策に関する費用を計画的に用意していますか。

a. 計画的に使えるように用意している
b. 計画的ではないが、必要に応じて使えるように用意している
c. 用意していない

Ｑ４－１①

※Q4-1 で a. または b. とお答えの方にお尋ねします。

差し支えなければ、年間のサイバーセキュリティ対策費用の予算規模をお答えください。（任意回答）

年間約（　　）万円

Ｑ４－２（サイバー保険への加入状況）

サイバーセキュリティ保険への加入状況についてお答えください。

a. サイバーセキュリティ保険に加入している
b. サイバーセキュリティ保険に加入していないが、加入を検討中である
c. サイバーセキュリティ保険に加入しておらず、加入予定もない

Ｑ４－３（ＢＣＰの策定状況）

システム障害やサイバー攻撃を想定した事業継続計画（BCP; Business Continuity Plan）の策定状況についてお答えください・

a. 策定している
b. 策定していない

Ｓ５　行政および日本医師会の取り組みの活用や認知の状況

Ｑ５－１（厚生労働省の取り組みの活用状況） *※(1)～(4)のすべてについて下記 a. ～c. でお答えください。*

以下の厚生労働省の取り組みや資料の活用状況をお答えください。

（１）医療情報システムの安全管理に関するガイドライン（最新は【第 6.0 版】）

（２）医療機関等におけるサイバーセキュリティ対策チェックリスト（最新は令和 7 年 5 月版）

（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

（４）医療機関向けセキュリティ教育支援ポータルサイト（MIST）

Ｑ５－２（日本医師会の取り組みの活用状況） *※(1)～(5)のすべてについて下記 a. ～c. でお答えください。*

当会の取り組み（日本医師会サイバーセキュリティ支援制度）の活用状況をお答えください。

（１）日本医師会サイバーセキュリティ相談窓口「サイ窓」

（２）セキュリティ対策強化に向けた無料情報サイト（Tokio Cyber Port）

（３）日本医師会サイバー攻撃一時支援金・個人情報漏えい一時支援金制度

（４）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の実践ガイドおよび動画

（５）　日本医師会セキュリティガイドライン相談窓口

※上記 Q5-1 と 5-2 の選択肢は、すべて以下となります。

a. 活用している

b. 知っているが、活用していない

c. 知らない

Ｑ５－３（公的な連絡・相談窓口の認知状況） *※(1)～(3)のすべてについて下記 a. ～b. でお答えください。*

医療機関のサイバーセキュリティに関わる以下の公的な連絡・相談窓口のご認識についてお答えください。

（１）医療機関等がサイバー攻撃を受けた場合の厚生労働省の連絡先（医政局特定医薬品開発支援・医療情報担当参事官室）＊

（２）企業組織向けサイバーセキュリティ相談窓口（IPA セキュリティセンター）

（３）サイバー事案に関する通報等のオンライン受付窓口（警察庁サイバー警察局）

※上記の選択肢は、すべて以下となります。

a. 知っている

b. 知らない

Ｓ６　インシデント・アクシデントの経験

Ｑ６－１（情報セキュリティに関わるインシデント・アクシデントの経験）

過去３年間において、以下のような経験がありましたか。経験がある事象をすべてお答えください。（複数選択可）

a. 経験なし
b. 院内のサーバがウイルス感染した
c. 院内の端末（PC やタブレット端末）がウイルス感染した
d. 従業員が業務用端末から、ルールに違反してインターネットにアクセスした
e. 従業員が業務用のＰＣや端末から、フィッシング（詐欺）サイトにアクセスさせられた
f. 貴院のホームページが改ざん・乗っ取りされた
g. 患者・受診者の個人情報にアクセスできる端末が、なりすましメール（迷惑メールなど）を受信した
h. 患者・受診者の個人情報が漏えいした
i. 従業員の個人情報が漏えいした
j. 院内のシステムに外部からの不正ログインがあった
k. 業務用のＰＣ・スマートフォン・タブレット等の紛失・盗難があった
l. USB メモリ等の外部媒体の紛失・盗難があった
m. 患者・受診者の個人情報が含まれるメールの誤送信があった
n. 患者・受診者の個人情報が含まれる FAX の誤送信があった
o. 情報システムや医療機器等へのサイバー攻撃により患者に直接の危害があった
p. その他（　　自由記載、任意　　）

Ｑ６－１①

※Q6-1 で b. または c. とお答えの方にお尋ねします。

感染したウイルスはランサムウェアですか。

a. ランサムウェアである
b. ランサムウェア以外のウイルス
　→　感染したウイルスの種類や名称がわかれば教えてください
　（　　自由記載、任意　　）
c. わからない

Ｑ６－１②

※Q6-1 で b. または c. とお答えの方にお尋ねします。

ウイルス感染被害に関して、日医総研からの匿名インタビュー調査にご協力いただけますでしょうか。秘密厳守。結果は、政策提言や学術報告等の公益目的のみに使用します。ご協力いただける場合は、ご担当者のメールアドレスをご記入ください。（　　自由記載、半角英数字、任意　　）

Ｓ７　今後求められる政策支援

Ｑ７―１（行政や医師会への期待）

医療ＤＸが進む一方で医療現場のサイバーセキュリティを確保するにあたって、国や自治体の行政、日本医師会や都道府県・群市区医師会には、どのようなサポートを期待しますか。

- 国政や自治体行政に望むこと（　　自由記載、300 字、任意　　）

- 日本医師会や都道府県・群市区医師会に望むこと（　　自由記載、300 字、任意　　）