【資料】 アンケート調査票

【Q１～Q６】
貴院について

Q１．貴院の開設者についてお答えください。＊

- ○ 個人
- ○ 医療法人
- ○ 医師会
- ○ 国(独立行政法人、国立大学法人を含む)
- ○ 都道府県・市町村(地方独立行政法人、公立大学法人を含む)
- ○ 公的医療機関(日赤、済生会、北海道社会事業協会、厚生連)
- ○ 社会保険関係団体(船員保険会、健保組合及びその連合会、共済組合及びその連合会、国保組合)
- ○ 公益法人(医師会を除く)
- ○ 私立学校法人
- ○ 社会福祉法人
- ○ 医療生協
- ○ 会社
- ○ その他の法人

Q２．貴院の病床数についてお答えください。＊

- ○ 無床診療所　（Q３へお進みください）
- ○ 有床診療所　（Q３へお進みください）
- ○ 病院　20～99 床　（Q４へお進みください）
- ○ 病院　100～199 床　（Q４へお進みください）
- ○ 病院　200～299 床　（Q４へお進みください）
- ○ 病院　300～499 床　（Q４へお進みください）
- ○ 病院　500 床以上　（Q４へお進みください）

※Q２．の回答による

Q３．Q２にて「診療所」の項目を選択された方にお伺いします。
貴院の主な診療科をお答えください（下記から１つだけ選択してください)。＊

- ○ 内科
- ○ 外科
- ○ 整形外科
- ○ 眼科
- ○ 耳鼻咽喉科
- ○ 小児科
- ○ 皮膚科
- ○ 泌尿器科
- ○ 精神科
- ○ 産科・産婦人科
- ○ 婦人科
- ○ 脳神経外科
- ○ その他（　　）

※Q２．の回答による

Q４．Q２にて「病院」の項目を選択された方にお伺いします。
貴院の施設の種類をお答えください。＊

- ○ 一般病院
- ○ 精神科病院

Q５．院長のご年齢について年代でお答えください。＊

- ○　３０歳代以下
- ○　４０歳代
- ○　５０歳代
- ○　６０歳代
- ○　７０歳代
- ○　８０歳代以上

Q６．令和３年（2021 年）３月から、「オンライン資格確認」（マイナンバーカードの個人認証や健康保険証の記載情報を用いて、オンラインで健康保険の資格確認を可能にする仕組み）が開始されます。貴院では、このオンライン資格確認のシステムを導入する予定かお答えください。＊

- ○　令和３年３月に導入予定である
- ○　令和３年３月には導入しないが、補助金の申請期限（令和５年３月３１日）までには導入予定である
- ○　導入する予定はない
- ○　検討中
- ○　わからない・知らない

【Q７～Q９】
貴院内のネットワークについて

Q７．　貴院の情報システムについて、取り扱っている範囲、並びに院内の接続状況(他のシステムやインターネット)についても合わせてお答えください。＊

なお、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：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、電子カルテシステムと医用画像管理システムの両方にお答えください)

	貴院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	インターネットとは接続していないが、貴院内の他のシステムと接続している	貴院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	貴院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	このシステムは使っていない
医事会計システム（レセコン）	○	○	○	○	○
電子カルテシステム	○	○	○	○	○
オンライン請求システム	○	○	○	○	○
医用画像管理システム	○	○	○	○	○
オーダリングシステム	○	○	○	○	○
診療予約システム	○	○	○	○	○
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）	○	○	○	○	○
遠隔診療システム(オンライン診療システムを含む)	○	○	○	○	○
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）	○	○	○	○	○
その他 （具体的な情報システムの名称については次問(Q6)にてご回答ください）	○	○	○	○	○

※Q７．の回答による

Q８．Q７にて「その他」を選択された方にお伺いします。
その他の具体的な情報システムの名称をご記入ください。

Q９．　貴院内のすべての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。
また、その資料の更新のタイミングと共にお答えください。＊

○　資料を持っており、計画的に見直しや更新を行っている
○　資料を持っており、ネットワークの追加・修正のあるタイミングで見直しや更新を行っている
○　資料を持っているが、見直しや更新は行っていない
○　資料は持っていない

【Q１０～Q１２】
貴院のサイバーセキュリティ対策への取り組み(組織体制)について

Q１０.　貴院の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ひとつ選んでお答えください。＊

- ○　専任の担当部門がある
- ○　専任の担当部門はないが、委員会等を設置している
- ○　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
- ○　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
- ○　上記のような管理体制はなく、院長が自ら管理している

Q１１.　貴院の情報システムのメンテナンス活動を現場にて行っている方についてお答えください。＊

- ○　内部スタッフ(院長含む)により実施している
- ○　外部の業者のサービスを利用して実施している
- ○　内部スタッフ(院長含む)および外部の業者のサービスにより実施している
- ○　実施していない
- ○　わからない

Q１２.　貴院では、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。＊

- ○　計画的に使えるように用意している
- ○　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
- ○　用意していない

【Q１３～Q１９】
貴院のサイバーセキュリティ対策への取り組み(運用)について

Q１３. 厚生労働省の「医療情報システムの安全管理に関するガイドライン」（最新版は【第５版】）を把握・活用しているかお答えください。＊

- ○ 活用している
- ○ 知っているが活用していない
- ○ 知らない

Q１４. サイバー攻撃を受けた際は厚生労働省 医政局 研究開発推進課 医療情報技術推進室に連絡することをご存知かお答えください。＊

- ○ 知っている
- ○ 知らない

Q１５. マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口が独立行政法人 情報処理推進機構 情報セキュリティ安心相談窓口であることをご存知かお答えください。＊

- ○ 知っている
- ○ 知らない

Q１６. 患者・受診者情報が保管されている貴院内の情報端末（ＰＣやタブレット等）の管理ルールについてお尋ねします。下記の（１）～（５）の各ルールの徹底度合いに対するご認識についてお答えください。＊

	ルールがあり、徹底されている	ルールはあるが、徹底されているかどうか、自信がない	ルールはあるが、徹底されていない	ルールはない
(1) 端末の持ち出し時のルール	○	○	○	○
(2) 外部媒体（USB メモリ等）と接続するときのルール	○	○	○	○
(3) インターネットに接続するときのルール	○	○	○	○
(4) 端末から離席するときのルール	○	○	○	○
(5) 端末を廃棄する際のルール	○	○	○	○

Q１７. ＵＳＢメモリ等の外部媒体の管理ルールについてお尋ねします。下記の（１）～（３）の各ルールの徹底度合いに対するご認識についてお答えください。＊

	ルールがあり、徹底されている	ルールはあるが、徹底されているかどうか、自信がない	ルールはあるが、徹底されていない	ルールはない

(1)持ち込み・持ち出し時のルール	○	○	○	○
(2)貴院内の PC 等と接続するときのルール	○	○	○	○
(3)廃棄する際のルール	○	○	○	○

Q１８. 下記のようなサイバーセキュリティに関わるインシデントが発生した時の明文化された対応手順やルールの有無についてお答えください。＊

	明文化された対応手順やルールあり	明文化された対応手順やルールなし
(1)貴院内のサーバや情報端末に、ウイルス感染や不正アクセスがあった場合	○	○
(2)ホームページの改ざんや乗っ取り等のハッキング被害があった場合	○	○
(3)患者・受診者の個人情報の漏えいがあった場合	○	○
(4)患者・受診者への直接の危害があった場合	○	○

Q１９. 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。＊

○ サイバーセキュリティ保険に加入しており、保険の内容も知っている
○ サイバーセキュリティ保険に加入しているが、内容はよく知らない
○ サイバーセキュリティ保険に加入していないが、検討したい
○ サイバーセキュリティ保険に加入しておらず、検討予定もない

【Q２０～Q２１】
貴院のサイバーセキュリティ対策への取り組み(現場状況)について

Q２０.　過去３年間において、貴院では、以下のような経験がありましたか。経験があるものをすべてお答えください。＊（複数選択可）…注：調査画面上は（複数選択）と表示。以下、同じ。

□　経験がない　（Q２２へお進みください）
□　貴院内のサーバがウイルス感染した。
□　貴院内の端末（PC やタブレット端末）がウイルス感染した。
□　従業員が院内システムを使って、貴院内ルールに違反してインターネットにアクセスした。
□　従業員が貴院内のＰＣやタブレット端末から、フィッシング（詐欺）サイトにアクセスさせられた。
□　貴院のホームページが改ざん・乗っ取りされた。
□　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。
□　患者・受診者の個人情報が漏えいした。
□　従業員の個人情報が漏えいした。
□　上記以外の情報が漏えいした。
□　貴院内のシステムに外部からの不正ログインがあった。
□　業務用のノート PC・スマートフォン・タブレットの紛失・盗難があった。
□　USB メモリ等の外部媒体の紛失・盗難があった。
□　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。
□　患者・受診者の個人情報が含まれる FAX の誤送信があった。
□　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。
□　その他（　　）

※Q２０．の回答による

Q２１.　Q２０にて、いずれかの経験があると回答された方にお伺いします。
発生したインシデント情報をどのレベルまで把握し、対応できているかについてお答えください。＊

○　インシデントの原因分析と今後の対応まで整理できている
○　インシデントの原因分析まで整理できている
○　インシデントが発生したという事実まで整理できている
○　その他（　　）

【Q２２～Q２４】
貴院のサイバーセキュリティ対策への取り組み(教育)について

Q２２．サイバーセキュリティ対策に関する教育の実施状況についてお答えください。＊

- ○　半年から１年に１回程度実施している
- ○　１年から３年に１回程度実施している
- ○　３年から５年に１回程度実施している
- ○　実施していない(Q２５へお進みください)

※Q２２．の回答による

Q２３．　Q２２にて「実施している」と回答された方にお伺いします。
教育の対象者についてお答えください。＊

- ○　全職員に対して実施している
- ○　担当の部門に対して実施している
- ○　希望者に対して実施している
- ○　わからない

※Q２２．の回答による

Q２４．　Q２２にて「実施している」と回答された方にお伺いします。
貴院における教育の方法について当てはまるものをすべてお答えください。＊（複数選択可）

- □　専門家を招いての講習会を用いて実施している
- □　行政等から出されているガイドラインを用いて実施している
- □　担当部署内で作成した教材を用いて実施している
- □　専門機関の講座を用いて実施している
- □　e-learning 講座を用いて実施している
- □　市販されている教材を用いて実施している
- □　その他（　　）

【Q２５～Q２６】
貴院のサイバーセキュリティ対策への取り組み(要望)について

Q２５.　サイバーセキュリティ対策にあたって、このようなことがあればよいと思う選択肢をすべてお答えください。(複数選択可)

□　自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み
□　インシデント・アクシデント発生時の相談先
□　サイバーセキュリティ対策の体制構築を検討する際の相談先
□　サイバーセキュリティ対策を学べる場所
□　自施設内のサイバーセキュリティ対策を担う人材
□　サイバーセキュリティ対策の費用面での公的支援
□　その他（　　）

Q２６.　サイバーセキュリティ対策にあたって、最も優先度が高いと考える選択肢をひとつお答えください。

○　自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み
○　インシデント・アクシデント発生時の相談先
○　サイバーセキュリティ対策の体制構築を検討する際の相談先
○　サイバーセキュリティ対策を学べる場所
○　自施設内のサイバーセキュリティ対策を担う人材
○　サイバーセキュリティ対策の費用面での公的支援
○　その他（　　）