2021年3月9日

日医総研リサーチエッセイ　No.103

オンライン資格確認導入に係るサイバーリスクの実態に関する調査結果の分析と考察

堤信之（主任研究員）、坂口一樹（主任研究員）

目次

はじめに

2020 年 2～3 月に医療機関のサイバーセキュリティ対策の実態に関する調査を実施し、同対策に関する基本的なルールの整備状況、組織体制、予算確保等にそれぞれ問題を抱えていることを確認した[1]。同調査のサンプル数が少なかったため、今般、確認結果が医療界全体の問題といえるかどうかを検証する目的で、対象範囲を全国の診療所、病院に拡大し、対象数も大幅に増やした「医療機関の情報システムの管理体制に関する実態調査」（以下「本調査」）を行うこととした[2]。

今年度以降の数か月間にも、社会、産業界を襲うサイバーセキュリティへの脅威は世界的にますます増大し、折からの新型コロナ感染拡大により国内でもサイバー攻撃が増加している[3]。

医療界にも被害例が相次ぎ、国内では 2018 年 10 月に発生した奈良・宇陀市立病院事件[4]の他、福島・県立医科大学附属病院で 2017 年 8 月以降、院内システムがウイルスに感染して被害が出ていたことが 2020 年 12 月に公表された[5]。身近なところでは、日本医師会でも 2020 年 9 月に一部の情報端末が EMOTET に感染する事件が発生した[6]。また海外ではコンピュータウィルスに起因した患者の死亡事例すら報告された[7]。

医療界におけるサイバーリスクは、公表されたインシデントの発生事例こそ

1.坂口、堤 2020「医療機関におけるサイバーセキュリティ実態調査：パイロット調査」日医総研リサーチエッセイ No.85（2020 年 6 月 18 日）https://www.jmari.med.or.jp/research/research/wr_702.html

2.本調査は、日本医師会と公益財団法人医療機器センターとの合同で実施された。

3.日本経済新聞 2020「サイバー攻撃 コロナに便乗」（2021 年 3 月 5 日朝刊記事）
日本経済新聞 2020「身代金要求型ウイルス猛威 企業攻撃への分業体制」（2021 年 3 月 9 日朝刊記事）
カプコン 2020「不正アクセスによる情報流出に関するお知らせとお詫び【第 3 報】」（2021 年 1 月 12 日）https://www.capcom.co.jp/ir/news/html/210112.html

4.宇陀市監査委員 2019「令和元年度随時監査（ＩＣＴ監査）結果報告書の提出について」宇陀市監査委員告示第 8 号（2020 年 3 月 25 日）
https://www.city.uda.nara.jp/kansa-jimu/shisei/kansa/documents/r1-byouinn-ict.pdf

5.日本経済新聞 2020「福島の病院、サイバー被害　17 年発生　県立医大付属、公表せず　身代金ウイルス、医療機器停止　病院に攻撃海外で相次ぐ　手術延期のケースも」（2020 年 12 月 3 日朝刊記事）

6.日本医師会 2020「日本医師会事務局におけるコンピュータウイルス感染と それを発端にした関係者への不審メール発生に関するお詫びとご報告」（2020 年 9 月 8 日）
https://www.med.or.jp/people/info/doctor_info/pdf/pc20200908.pdf

7.ForbesJapan2020「史上初の身代金ウイルス攻撃による死者、ドイツの病院で発生」（2020 年 9 月 19 日）

現状ではあまり目立たないが、一旦発生した場合の被害の広がり、深刻さに鑑みれば、サイバーセキュリティ対策を、リスクマネジメント上の重要な位置づけで捉えるべきである。

一方で、医療機関の情報システムは、従来は院内で完結することが一般的であったのが、オンライン診療の他、オンライン資格確認[8]といった外部ネットワークとの接続を前提とする仕組みの登場により、環境激変の時期を迎えている。特にオンライン資格確認は 2021 年 3 月より一部医療機関での導入が開始され、いよいよ待ったなしの状況にある。これらは患者・受診者にとっての利便性の向上や、公共利益の追求を背景としたものであるが、適切なサイバーセキュリティ対策を講じなければ、サイバーリスクを飛躍的に高める結果にもつながりかねないことに留意しなければならない。

そこで、オンライン資格確認の導入が開始する 2021 年 3 月に合わせて本調査の実施時期を設定し、またインシデント発生の有無だけでなく、リスク実態を明らかにする観点から、システム環境等にも重点を置いた調査内容とした。

本調査の論点は多岐に亘るが、まずは、オンライン資格確認に焦点を当て、その導入に係るサイバーリスクの実態を分析、考察した。

8.厚生労働省「オンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）」：
https://www.mhlw.go.jp/stf/newpage_08280.html

１．本調査及び本稿の目的と調査概要

（１）本調査及び本稿の目的

本調査は、全国の医療機関（病院・診療所）における情報システムの管理体制に関わる実態把握を目的とした。本稿では特に、オンライン資格確認導入に係るサイバーリスクに焦点を当て、システム環境やサイバーセキュリティ対策の実態を踏まえた課題を抽出し、対応策を考察した。

（２）対象と方法

①全国の医療機関名簿から無作為抽出した病院 5,000 施設、診療所 5,000 施設を対象とした。
②対象には調査画面へのアクセス方法を記載した案内状を郵送。ウェブ調査画面を通じて回答してもらった。
③調査実施期間は 2021 年 1 月 7 日～2 月 3 日であった。一部、紙媒体の返送による回答も受け付けた。

（３）回収状況と回答者属性

①回収した有効回答数は、n=2,989（回収率 30.4%、未達が 175 件）。
②主な回答者属性は、下表の通り。

		n	%
開設主体	個人	616	20.6%
	医療法人	1661	55.6%
	国公立・公的	443	14.8%
	その他の法人	269	9.0%
病床規模	無床診療所	1289	43.1%
	有床診療所	111	3.7%
	病院　20～99床	468	15.7%
	病院　100～199床	511	17.1%
	病院　200～499床	463	15.5%
	病院　500床以上	147	4.9%

		n	%
院長の年齢	３０歳代以下	25	0.8%
	４０歳代	285	9.5%
	５０歳代	790	26.4%
	６０歳代	1355	45.3%
	７０歳代	457	15.3%
	８０歳代以上	77	2.6%
回答者職位	理事長	297	9.9%
	院長	709	23.7%
	システム担当	986	33.0%
	事務長	515	17.2%
	その他	482	16.1%

２．オンライン資格確認に焦点を当てた調査結果と分析

（１）クロス集計結果

①オンライン資格確認導入意思

現状でのオンライン資格確認導入の意思を有する医療機関は必ずしも多くないことが確認された。（Q2 とのクロス集計）

ただし病床規模による差が大きく、診療所では 41.6%、病床数～199 床の病院では 55.3%、病床数 200～499 床の病院では 68.7%、500 床以上の病院では 85.7%であった（いずれも、「令和 3 年 3 月までに導入予定」と「令和 5 年 3 月 31 日までに導入予定」を合算した数値）。

表 2-1 病床規模別／オンライン資格確認導入意思

		全体	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
全体		(2989)	629 21.0	938 31.4	360 12.0	938 31.4	124 4.1
病床規模	診療所	(1400)	235 16.8	347 24.8	260 18.6	487 34.8	71 5.1
	病院　20～199床	(979)	210 21.5	331 33.8	80 8.2	323 33.0	35 3.6
	病院　200～499床	(463)	124 26.8	194 41.9	20 4.3	109 23.5	16 3.5
	病院　500床以上	(147)	60 40.8	66 44.9	0 0.0	19 12.9	2 1.4

②医療関連システムのインターネット接続環境

同システムの導入を決めている医療機関のうち、自院の医療関連システムがインターネットと接続している環境にあるところが高い割合で存在する。

しかも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ところも多い。（Q7 とのクロス集計）

2021 年 3 月導入予定の医療機関に占める割合は以下の通りであった。

a.レセコン　　：23.3%（「院内他システムと接続していないがインターネットと接続」と「他システム・インターネット両方と接続」を合算した数値)、そのうちで「他システム・インターネット両方と接続」しているところが 16.5%

b.電子カルテ　　：17.6%（同上)、そのうち同上 15.1%

c.オンライン請求：68.1%（同上)、そのうち同上 18.3%

d.画像管理　　：15.3%（同上)、そのうち同上 11.6%

e.オーダリング　：9.5%（同上)、そのうち同上 8.1%

f.診療予約　　：13.7%（同上)、そのうち同上 7.2%

g.健康診断　　：4.4%（同上)、そのうち同上 2.5%

h.遠隔診療　　：14.1%（同上)、そのうち同上 4.9%

i.地域医療連携　：23.7%（同上)、そのうち同上 12.1%

a. 医事会計システム（レセコン）

表 2-2-1

		全体	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
全体		(2989)	654	1347	368	456	164
			21.9	45.1	12.3	15.3	5.5
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	100	362	43	104	20
			15.9	57.6	6.8	16.5	3.2
	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	(938)	150	506	91	146	45
			16.0	53.9	9.7	15.6	4.8
	導入する予定はない	(360)	135	65	77	54	29
			37.5	18.1	21.4	15.0	8.1
	検討中	(938)	229	382	134	133	60
			24.4	40.7	14.3	14.2	6.4
	わからない・知らない	(124)	40	32	23	19	10
			32.3	25.8	18.5	15.3	8.1

b. 電子カルテシステム

表 2-2-2

		全体	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
全体		(2989)	205	1204	90	379	1111
			6.9	40.3	3.0	12.7	37.2
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	48	332	16	95	138
			7.6	52.8	2.5	15.1	21.9
	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	(938)	59	473	23	118	265
			6.3	50.4	2.5	12.6	28.3
	導入する予定はない	(360)	28	57	13	35	227
			7.8	15.8	3.6	9.7	63.1
	検討中	(938)	60	318	34	120	406
			6.4	33.9	3.6	12.8	43.3
	わからない・知らない	(124)	10	24	4	11	75
			8.1	19.4	3.2	8.9	60.5

c. オンライン請求システム

表 2-2-3

		全体	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
全体		(2989)	494	254	1333	488	420
			16.5	8.5	44.6	16.3	14.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	95	63	313	115	43
			15.1	10.0	49.8	18.3	6.8
	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	(938)	167	99	446	145	81
			17.8	10.6	47.5	15.5	8.6
	導入する予定はない	(360)	51	14	134	48	113
			14.2	3.9	37.2	13.3	31.4
	検討中	(938)	161	72	404	156	145
			17.2	7.7	43.1	16.6	15.5
	わからない・知らない	(124)	20	6	36	24	38
			16.1	4.8	29.0	19.4	30.6

d. 医用画像管理システム

表 2-2-4

		全体	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
全体		(2989)	471	1416	134	315	653
			15.8	47.4	4.5	10.5	21.8
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	83	380	23	73	70
			13.2	60.4	3.7	11.6	11.1
	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	(938)	128	516	45	108	141
			13.6	55.0	4.8	11.5	15.0
	導入する予定はない	(360)	71	76	15	33	165
			19.7	21.1	4.2	9.2	45.8
	検討中	(938)	162	401	43	89	243
			17.3	42.8	4.6	9.5	25.9
	わからない・知らない	(124)	27	43	8	12	34
			21.8	34.7	6.5	9.7	27.4

e. オーダリングシステム

表 2-2-5

		全体	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
全体		(2989)	129	1087	50	205	1518
			4.3	36.4	1.7	6.9	50.8
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	30	299	9	51	240
			4.8	47.5	1.4	8.1	38.2
	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	(938)	46	426	17	79	370
			4.9	45.4	1.8	8.4	39.4
	導入する予定はない	(360)	19	48	7	14	272
			5.3	13.3	1.9	3.9	75.6
	検討中	(938)	26	291	15	52	554
			2.8	31.0	1.6	5.5	59.1
	わからない・知らない	(124)	8	23	2	9	82
			6.5	18.5	1.6	7.3	66.1

f. 診療予約システム

表 2-2-6

		全体	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
全体		(2989)	140	626	169	205	1849
			4.7	20.9	5.7	6.9	61.9
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	36	184	41	45	323
			5.7	29.3	6.5	7.2	51.4
	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	(938)	39	265	47	75	512
			4.2	28.3	5.0	8.0	54.6
	導入する予定はない	(360)	21	21	16	19	283
			5.8	5.8	4.4	5.3	78.6
	検討中	(938)	38	141	61	61	637
			4.1	15.0	6.5	6.5	67.9
	わからない・知らない	(124)	6	15	4	5	94
			4.8	12.1	3.2	4.0	75.8

g. 健康診断システム

表 2-2-7

		全体	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
全体		(2989)	184	555	72	73	2105
			6.2	18.6	2.4	2.4	70.4
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	47	161	12	16	393
			7.5	25.6	1.9	2.5	62.5
	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	(938)	55	230	28	33	592
			5.9	24.5	3.0	3.5	63.1
	導入する予定はない	(360)	16	19	5	7	313
			4.4	5.3	1.4	1.9	86.9
	検討中	(938)	56	136	22	15	709
			6.0	14.5	2.3	1.6	75.6
	わからない・知らない	(124)	10	9	5	2	98
			8.1	7.3	4.0	1.6	79.0

h. 遠隔診療システム

表 2-2-8

		全体	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
全体		(2989)	68	42	174	101	2604
			2.3	1.4	5.8	3.4	87.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	18	8	58	31	514
			2.9	1.3	9.2	4.9	81.7
	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	(938)	18	22	66	36	796
			1.9	2.3	7.0	3.8	84.9
	導入する予定はない	(360)	9	2	5	4	340
			2.5	0.6	1.4	1.1	94.4
	検討中	(938)	16	10	42	28	842
			1.7	1.1	4.5	3.0	89.8
	わからない・知らない	(124)	7	0	3	2	112
			5.6	0.0	2.4	1.6	90.3

i. 地域医療連携システム

表 2-2-9

		全体	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
全体		(2989)	100	239	244	218	2188
			3.3	8.0	8.2	7.3	73.2
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	28	81	73	76	371
			4.5	12.9	11.6	12.1	59.0
	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	(938)	30	99	75	91	643
			3.2	10.6	8.0	9.7	68.6
	導入する予定はない	(360)	8	9	20	9	314
			2.2	2.5	5.6	2.5	87.2
	検討中	(938)	24	50	67	38	759
			2.6	5.3	7.1	4.1	80.9
	わからない・知らない	(124)	10	0	9	4	101
			8.1	0.0	7.3	3.2	81.5

③ネットワーク構成図の保有状況

システム導入の前提となるネットワーク構成図の保有状況が不十分という問題がある。（Q9 と Q2、Q9 と Q6 のクロス集計）

病床規模でみると、「持っていない」或いは「持っているが見直しや更新は行っていない」割合が、診療所では 80.6%、病床数～199 床の病院では 58.9%、病床数 200～499 床の病院では 32.8%、500 床以上の病院でも 17.7%であった。

2021 年 3 月オンライン資格確認導入予定のところで、「ネットワーク構成図を持っていない」が 38.2%、「持っているが見直しや更新は行っていない」が 14.0%であった。2023 年 3 月までにオンライン資格確認導入予定のところでみると、「ネットワーク構成図を持っていない」が 35.9%、「持っているが見直しや更新は行っていない」が 15.7%であった。

表 2-3-1 病床規模別／ネットワーク構成図保有状況

		全体	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
全体		(2989)	169 5.7	938 31.4	411 13.8	1471 49.2
病床規模	診療所	(1400)	43 3.1	229 16.4	141 10.1	987 70.5
	病院　20～199床	(979)	59 6.0	344 35.1	177 18.1	399 40.8
	病院　200～499床	(463)	42 9.1	269 58.1	77 16.6	75 16.2
	病院　500床以上	(147)	25 17.0	96 65.3	16 10.9	10 6.8

表 2-3-2 オンライン資格確認導入予定別／ネットワーク構成図保有状況

		全体	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
全体		(2989)	169	938	411	1471
			5.7	31.4	13.8	49.2
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	62	239	88	240
			9.9	38.0	14.0	38.2
	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	(938)	60	394	147	337
			6.4	42.0	15.7	35.9
	導入する予定はない	(360)	8	48	44	260
			2.2	13.3	12.2	72.2
	検討中	(938)	35	245	117	541
			3.7	26.1	12.5	57.7
	わからない・知らない	(124)	4	12	15	93
			3.2	9.7	12.1	75.0

④情報システムの管理体制

同システムの導入を決めている医療機関のうち、「情報システムの担当組織・担当者がおらず院長自らが管理している」「情報システムのメンテナンスが実施されていない」ところがある。

（Q10,11 とのクロス集計）

2021 年 3 月導入予定の医療機関で、「情報システムの担当組織・担当者がおらず院長自ら管理している」ところが 25.8%、「メンテナンス未実施」が 4.1%であった。

2023 年 3 月までに導入予定のところでは、「情報システムの担当組織・担当者がおらず院長自ら管理している」のが 24.8%、「メンテナンス未実施」が 6.0%であった。

表 2-4-1 情報システム管理体制

		全体	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
全体		(2989)	617	244	191	993	944
			20.6	8.2	6.4	33.2	31.6
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	169	68	34	196	162
			26.9	10.8	5.4	31.2	25.8
	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	(938)	270	88	72	275	233
			28.8	9.4	7.7	29.3	24.8
	導入する予定はない	(360)	20	14	16	131	179
			5.6	3.9	4.4	36.4	49.7
	検討中	(938)	143	68	62	343	322
			15.2	7.2	6.6	36.6	34.3
	わからない・知らない	(124)	15	6	7	48	48
			12.1	4.8	5.6	38.7	38.7

表 2-4-2 情報システムのメンテナンス活動

		全体	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
全体		(2989)	441	844	1405	237	62
			14.8	28.2	47.0	7.9	2.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	89	144	363	26	7
			14.1	22.9	57.7	4.1	1.1
	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	(938)	140	244	491	56	7
			14.9	26.0	52.3	6.0	0.7
	導入する予定はない	(360)	47	121	115	64	13
			13.1	33.6	31.9	17.8	3.6
	検討中	(938)	148	301	396	70	23
			15.8	32.1	42.2	7.5	2.5
	わからない・知らない	(124)	17	34	40	21	12
			13.7	27.4	32.3	16.9	9.7

⑤サイバーセキュリティ対策に関する予算

同システムの導入を決めている医療機関のうち、サイバーセキュリティ対策費用の予算は用意されていないところが多く存在する。（Q12 とのクロス集計）

2021 年 3 月導入予定の医療機関で、「予算が計画的に用意されている」のが 15.4%、「必要に応じて使える用意がある」のが 43.2%、「用意がない」のが 41.3%であった。

表 2-5

		全体	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
全体		(2989)	312	1240	1437
			10.4	41.5	48.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	97	272	260
			15.4	43.2	41.3
	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	(938)	104	427	407
			11.1	45.5	43.4
	導入する予定はない	(360)	24	114	222
			6.7	31.7	61.7
	検討中	(938)	79	392	467
			8.4	41.8	49.8
	わからない・知らない	(124)	8	35	81
			6.5	28.2	65.3

⑥厚労省・医療情報システム安全管理ガイドラインの認知状況

同システムの導入を決めている医療機関のうち、「厚労省・医療情報システム安全管理ガイドラインを知らない」ところが少なからずある。

（Q13 とのクロス集計）

2021 年 3 月導入予定の医療機関で、「知らない」のが 27.3%、「知っているが活用していない」のが 35.5%であった。

表 2-6

		全体	活用している	知っているが活用していない	知らない
全体		(2989)	834	982	1173
			27.9	32.9	39.2
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	234	223	172
			37.2	35.5	27.3
	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	(938)	348	304	286
			37.1	32.4	30.5
	導入する予定はない	(360)	41	93	226
			11.4	25.8	62.8
	検討中	(938)	202	335	401
			21.5	35.7	42.8
	わからない・知らない	(124)	9	27	88
			7.3	21.8	71.0

⑦サイバー攻撃時の行政連絡窓口、相談窓口の認知状況

同システムの導入を決めている医療機関のうち、大半が「サイバー攻撃を受けた際の行政連絡窓口を知らない」或いは「技術的な相談を受け付ける公的窓口を知らない」。（Q14,15 とのクロス集計）

2021 年 3 月導入予定の医療機関で、「サイバー攻撃を受けた際の行政連絡窓口を知らない」のが 63.9%、「技術的な相談を受け付ける公的窓口を知らない」のが 71.9%であった。

表 2-7-1 サイバー攻撃を受けた際の行政窓口

		全体	知っている	知らない
全体		(2989)	874	2115
			29.2	70.8
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	227	402
			36.1	63.9
	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	(938)	327	611
			34.9	65.1
	導入する予定はない	(360)	57	303
			15.8	84.2
	検討中	(938)	249	689
			26.5	73.5
	わからない・知らない	(124)	14	110
			11.3	88.7

表 2-7-2 マルウェアや不正アクセスに関する技術的な相談の受付窓口

		全体	知っている	知らない
全体		(2989)	689 23.1	2300 76.9
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	177 28.1	452 71.9
	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	(938)	276 29.4	662 70.6
	導入する予定はない	(360)	45 12.5	315 87.5
	検討中	(938)	178 19.0	760 81.0
	わからない・知らない	(124)	13 10.5	111 89.5

⑧サイバーセキュリティ対策ルール

同システムの導入を決めている医療機関のうち、「サイバーセキュリティ対策ルールがない」ところがある。（Q16,17 とのクロス集計）

2021 年 3 月導入予定の医療機関に占める割合は次の通りであった。

a.端末持ち出し　　:「ルールなし」が 18.6%
b.端末と外部媒体との接続　:同上 19.2%
c.インターネット接続　　:同上 23.2%
d.端末からの離席　　:同上 32.3%
e.端末廃棄　　:同上 25.3%
f.外部媒体持ち込み持ち出し:同上 20.3%
g.外部媒体の院内端末接続　:同上 21.0%
h.外部媒体廃棄　　:同上 35.8%

a. 端末の持ち出し時のルール

表 2-8-1

		全体	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
全体		(2989)	1650	432	91	816
			55.2	14.5	3.0	27.3
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	402	96	14	117
			63.9	15.3	2.2	18.6
	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	(938)	562	143	31	202
			59.9	15.2	3.3	21.5
	導入する予定はない	(360)	145	33	8	174
			40.3	9.2	2.2	48.3
	検討中	(938)	497	143	29	269
			53.0	15.2	3.1	28.7
	わからない・知らない	(124)	44	17	9	54
			35.5	13.7	7.3	43.5

b. 情報端末の外部媒体との接続ルール

表 2-8-2

		全体	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
全体		(2989)	1454	575	130	830
			48.6	19.2	4.3	27.8
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	347	134	27	121
			55.2	21.3	4.3	19.2
	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	(938)	498	202	41	197
			53.1	21.5	4.4	21.0
	導入する予定はない	(360)	121	44	10	185
			33.6	12.2	2.8	51.4
	検討中	(938)	443	177	43	275
			47.2	18.9	4.6	29.3
	わからない・知らない	(124)	45	18	9	52
			36.3	14.5	7.3	41.9

c. 情報端末のインターネットとの接続ルール

表 2-8-3

		全体	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
全体		(2989)	1348	524	110	1007
			45.1	17.5	3.7	33.7
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	330	123	30	146
			52.5	19.6	4.8	23.2
	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	(938)	452	180	35	271
			48.2	19.2	3.7	28.9
	導入する予定はない	(360)	117	39	10	194
			32.5	10.8	2.8	53.9
	検討中	(938)	409	160	30	339
			43.6	17.1	3.2	36.1
	わからない・知らない	(124)	40	22	5	57
			32.3	17.7	4.0	46.0

d. 端末からの離席ルール

表 2-8-4

		全体	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
全体		(2989)	686	772	302	1229
			23.0	25.8	10.1	41.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	162	194	70	203
			25.8	30.8	11.1	32.3
	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	(938)	232	289	121	296
			24.7	30.8	12.9	31.6
	導入する予定はない	(360)	67	46	19	228
			18.6	12.8	5.3	63.3
	検討中	(938)	204	220	81	433
			21.7	23.5	8.6	46.2
	わからない・知らない	(124)	21	23	11	69
			16.9	18.5	8.9	55.6

e. 端末廃棄ルール

表 2-8-5

		全体	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
全体		(2989)	1646	295	60	988
			55.1	9.9	2.0	33.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	400	62	8	159
			63.6	9.9	1.3	25.3
	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	(938)	567	98	20	253
			60.4	10.4	2.1	27.0
	導入する予定はない	(360)	143	28	7	182
			39.7	7.8	1.9	50.6
	検討中	(938)	487	92	21	338
			51.9	9.8	2.2	36.0
	わからない・知らない	(124)	49	15	4	56
			39.5	12.1	3.2	45.2

f. 外部媒体の持ち込み・持ち出しルール

表 2-8-6

		全体	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
全体		(2989)	1353	606	151	879
			45.3	20.3	5.1	29.4
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	325	145	31	128
			51.7	23.1	4.9	20.3
	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	(938)	457	209	50	222
			48.7	22.3	5.3	23.7
	導入する予定はない	(360)	121	42	12	185
			33.6	11.7	3.3	51.4
	検討中	(938)	411	188	50	289
			43.8	20.0	5.3	30.8
	わからない・知らない	(124)	39	22	8	55
			31.5	17.7	6.5	44.4

g. 外部媒体を院内の PC 等と接続するときのルール

表 2-8-7

		全体	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
全体		(2989)	1386	576	125	902
			46.4	19.3	4.2	30.2
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	340	133	24	132
			54.1	21.1	3.8	21.0
	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	(938)	480	201	40	217
			51.2	21.4	4.3	23.1
	導入する予定はない	(360)	119	40	12	189
			33.1	11.1	3.3	52.5
	検討中	(938)	408	182	40	308
			43.5	19.4	4.3	32.8
	わからない・知らない	(124)	39	20	9	56
			31.5	16.1	7.3	45.2

h. 外部媒体の廃棄ルール

表 2-8-8

		全体	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
全体		(2989)	1228	459	91	1211
			41.1	15.4	3.0	40.5
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	280	107	17	225
			44.5	17.0	2.7	35.8
	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	(938)	416	165	27	330
			44.3	17.6	2.9	35.2
	導入する予定はない	(360)	119	32	10	199
			33.1	8.9	2.8	55.3
	検討中	(938)	377	137	29	395
			40.2	14.6	3.1	42.1
	わからない・知らない	(124)	36	18	8	62
			29.0	14.5	6.5	50.0

⑨サイバーインシデント発生時の対応ルール

同システムの導入を決めている医療機関のうち、「サイバーインシデント発生時の明文化された対応ルールがない」ところが多数を占める。

（Q18 とのクロス集計）

2021 年 3 月導入予定の医療機関に占める割合は次の通りであった。

a.サーバ・情報端末へのウイルス感染　：「明文ルールなし」が 66.5%

b.ホームページ改ざん・ハッキング被害　：同上 77.3%

c.患者･受診者の個人情報漏洩　：同上 56.6%

d.患者･受診者への直接の危害　：同上 64.7%

a. サーバ・情報端末へのウイルス感染時の明文ルール

表 2-9-1

		全体	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
全体		(2989)	751 25.1	2238 74.9
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	211 33.5	418 66.5
	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	(938)	298 31.8	640 68.2
	導入する予定はない	(360)	54 15.0	306 85.0
	検討中	(938)	167 17.8	771 82.2
	わからない・知らない	(124)	21 16.9	103 83.1

b. ホームページ改ざん・ハッキング被害発生時の明文ルール

表 2-9-2

		全体	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
全体		(2989)	492 16.5	2497 83.5
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	143 22.7	486 77.3
	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	(938)	178 19.0	760 81.0
	導入する予定はない	(360)	43 11.9	317 88.1
	検討中	(938)	113 12.0	825 88.0
	わからない・知らない	(124)	15 12.1	109 87.9

c. 患者・受診者の個人情報漏えい発生時の明文ルール

表 2-9-3

		全体	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
全体		(2989)	1060 35.5	1929 64.5
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	273 43.4	356 56.6
	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	(938)	408 43.5	530 56.5
	導入する予定はない	(360)	79 21.9	281 78.1
	検討中	(938)	264 28.1	674 71.9
	わからない・知らない	(124)	36 29.0	88 71.0

d. 患者･受診者への直接の危害発生時の明文ルール

表 2-9-4

		全体	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
全体		(2989)	857 28.7	2132 71.3
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	222 35.3	407 64.7
	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	(938)	321 34.2	617 65.8
	導入する予定はない	(360)	64 17.8	296 82.2
	検討中	(938)	219 23.3	719 76.7
	わからない・知らない	(124)	31 25.0	93 75.0

⑩サイバーインシデント発生後の対応

何らかのサイバーインシデントが発生したにもかかわらず、「発生事実の整理まで」しかできていないまま、同システムの導入を決めている医療機関がある。（Q21 とのクロス集計）

2021 年 3 月導入予定の医療機関のうち、サイバーインシデントの経験があるが「発生事実の整理まで」と回答したのが 22.2%あった。

表 2-10

		全体	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
全体		(597)	348 58.3	91 15.2	142 23.8	16 2.7
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(162)	100 61.7	26 16.0	36 22.2	0 0.0
	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	(242)	155 64.0	29 12.0	48 19.8	10 4.1
	導入する予定はない	(26)	13 50.0	1 3.8	10 38.5	2 7.7
	検討中	(150)	71 47.3	33 22.0	42 28.0	4 2.7
	わからない・知らない	(17)	9 52.9	2 11.8	6 35.3	0 0.0

⑪サイバーセキュリティ対策に関する教育

同システムの導入を決めている医療機関のうち、「サイバーセキュリティ対策に関する教育が実施されていない」ところが多数を占める。

（Q22 とのクロス集計）

2021 年 3 月導入予定の医療機関のうち、「教育が実施されていない」のが 65.2%であった。

表 2-11

		全体	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
全体		(2989)	376	296	71	2246
			12.6	9.9	2.4	75.1
「オンライン資格確認」の導入予定	令和３年３月に導入予定である	(629)	132	72	15	410
			21.0	11.4	2.4	65.2
	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	(938)	156	121	30	631
			16.6	12.9	3.2	67.3
	導入する予定はない	(360)	16	14	2	328
			4.4	3.9	0.6	91.1
	検討中	(938)	65	86	22	765
			6.9	9.2	2.3	81.6
	わからない・知らない	(124)	7	3	2	112
			5.6	2.4	1.6	90.3

（２）結果の分析

現状の医療機関のシステム環境等において、セキュリティ対策を行わずに、オンライン資格確認の導入を進めることには、リスクがある。

①オンライン資格確認導入意思の実態

遅くとも令和 5 年 3 月 31 日までの導入意思が確認された医療機関は半数程度にとどまる。

②情報システムの現状とオンライン資格確認導入にあたり解決すべき課題

医療機関の情報システムの現状を分析すると、セキュリティ対策上、解決すべき各種の課題がある。

３．オンライン資格確認導入に係るサイバーリスクに関する考察

課題を踏まえ、以下の通り考察する。

①オンライン資格確認導入の意義の周知

オンライン資格確認導入の本来的な意義について、一層の周知が必要である。

日本医師会では、将来を展望すれば地域住民や患者のために活用される地域の医療・介護ネットワーク構築の入り口になるとの観点から、行政の同システム導入推進策に対して、協力している。行政としても、導入「検討中」の医療機関（31.4%）を中心に、引き続き上記趣旨を周知することが必要であろう。

②サイバーセキュリティ対策への備えの啓発と支援

同時に、サイバーリスクに関するセキュリティ対策への備えが必要であることの啓発と、そのための具体的な行政的支援が求められる。行政において、各種支援策（セミナー・研修等の啓発活動、簡易な手引書、チェックリスト作成、ネットワーク構成図作成支援等）を講じるべきである。

a. 診療所、中小規模病院対策

本調査で確認された、医療機関の病床規模による ICT リテラシーの格差（診療所＜中小規模病院＜大規模病院）を踏まえ、まずは診療所、中小規模病院を主たる対象としたサイバーリスク啓発活動に早期に着手すべきである。

b. オンライン資格確認導入予定の医療機関への対策

サイバーセキュリティ対策が脆弱なまま、オンライン資格確認を導入予定の医療機関が存在する可能性がある。このような医療機関に対する啓発及び支援策は、サイバーリスク軽減・回避の観点から緊急度が高いと考えられる。

c. オンライン資格確認導入を検討する医療機関に推奨する基本行動

オンライン資格確認導入を検討する医療機関の基本行動として、カードリーダー購入費用満額補助要件を充足するため、2021 年 3 月までに申請を行いつつ、

他方で実際の導入に当たっては、2023 年 3 月末までの猶予期間を有効に使い、サイバーリスクを認識することからはじめ、セキュリティ対策の備えを推奨すべきである。

d. ネットワーク構成図作成支援

少なくとも、最新のネットワーク構成図を保有していないとオンライン資格確認の適切な導入は困難であることに鑑み、ネットワーク構成図の整備支援に早期に着手する必要がある。

③サイバーセキュリティ対策に関する公的な資金支援の充実

医療機関におけるセキュリティ対策費用の予算措置が脆弱な実態に鑑み、サイバーセキュリティ対策に関する公的な資金面での更なる支援が必要である。

オンライン資格確認導入に際しては、カードリーダーの無償配布と資格確認端末の購入費用に加え、別途、オンライン請求との兼用回線の敷設または増強、そこから先の院内システムとの接続に要する費用及びセキュリティ対策費用、さらには導入後のメンテナンス費用の手当てが必要である。しかしながら現状の制度では、メンテナンス費用は対象外であり、導入費用やセキュリティ対策費用についても、その全てを公的補助の範囲内で賄うことは困難である。

【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（　　）

【Q２７～Q３２】
医療機器に関するサイバーセキュリティ対策の実態について

本調査で対象とするのは、サイバーセキュリティ対策が必要な医療機器です。
具体的には、通信機能・ネットワーク(Bluetooth、Wi-Fi 等)への接続や USB・CD/DVD ドライブ等のある医療機器を指します。
例えば、PACS などの医療用画像管理システムに接続される透視装置・CT・MRI 等、テレメトリー式心電計、バイタルモニタ機器、輸液ポンプ、麻酔器・モニタ機器類や人工呼吸器・透析装置といった医療機器です。

Q２７.　サイバーセキュリティ対策が必要な医療機器があることをご存知かお答えください。＊

- ○　よく知っている
- ○　知っている
- ○　あまり知らない
- ○　知らない　（Ｑ３０へお進みください）

※Q２７. の回答による

Q２８.　Ｑ２７にて「よく知っている」、「知っている」、「あまり知らない」と回答された方にお伺いします。
個別の医療機器に関するサイバーセキュリティの情報をどこから入手されているか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)

- □　医療機器のメーカ
- □　医療機器の販売業者
- □　セキュリティ会社
- □　医療情報システム会社
- □　医師会
- □　所属する病院団体
- □　行政
- □　入手していない　（Ｑ３０へお進みください）
- □　わからない　（Ｑ３０へお進みください）
- □　その他（　　）

※Q２８. の回答による

Q２９.　Ｑ２８で、いずれかから情報を入手していると回答された方にお伺いします。
入手した個別の医療機器に関するサイバーセキュリティの情報の理解度についてお答えください。＊

- ○　対策・対応の必要性の判断ができるレベルで理解している
- ○　用語は理解できているが、対策・対応の必要性の判断はできない
- ○　用語についても理解できない

Q３０. 医療機器を購入した際に、販売業者から医療機器のサイバーセキュリティに関する説明があったか、また、貴院での理解度についてお答えください。＊

- ○　説明があり、内容も十分に理解できた
- ○　説明はあったが、内容は理解できなかった
- ○　説明はなかった
- ○　わからない

Q３１. 貴院のサイバーセキュリティ対策を検討するにあたって、個々の医療機器に施されているサイバーセキュリティ対策の情報※が必要か当てはまるものすべてお答えください。＊(複数選択可)

※　医療機器内に組み込まれたセキュリティおよびプライバシー対策機能に関する標準化された情報やソフトウェアコンポーネント(部品表・構成表)の情報など。このような資料を製造業者開示説明書(MDS2)と呼びます。

□　購入検討時に必要
□　購入時に必要
□　購入後、契約更新に応じて必要
□　購入後、求めに応じて必要
□　必要ない
□　わからない

Q３２.「レガシーメディカルデバイス※」という言葉をご存知かお答えください。＊

※　レガシーメディカルデバイスとは、サイバーセキュリティ対策を検討しなければならない医療機器のうち、既に市販済みの製品であって、設計段階等においてサイバーセキュリティの検討がなされていなかった医療機器であり、当該製品単独では今後もサイバーセキュリティの脅威に対して合理的に保護できないと考えられる医療機器を指す。

○　知っている
○　知らない

【Q３３～Q３４】
ご意見、ご要望等

Q３３.　最後にサイバーセキュリティに関連するご意見、ご要望等がありますか。

Q３４.　ご回答頂いた方のお立場をお答えください。
複数兼務している場合は、メインの役職をひとつ選んでください。＊

○　理事長
○　院長
○　システム担当
○　事務長
○　その他（　　）