

遠隔医療モデル参考書
-オンライン診療版-
改訂版

別 添

令和6年5月

総 務 省

目次

1	オンライン診療の基礎知識	1
1.1	遠隔医療とは	1
1.1.1	医療従事者と患者間での遠隔医療	1
1.1.2	医療従事者間での遠隔医療	2
1.2	オンライン診療とは	3
2	法的・規制的な基礎知識	4
2.1	オンライン診療指針の遵守	4
2.2	遵守する法令等	20
2.3	関係団体による各種手引き	20
3	技術とインフラに関する基礎知識	21
3.1	オンライン診療システムの概要	21
3.1.1	システム構成	21
3.1.2	機能構成	22
3.1.3	ハードウェア・ネットワーク構成	23
3.2	オンライン診療システムの構築パターン	24
3.2.1	前提条件	24
3.2.2	費用の目安	25
3.3	サイバーセキュリティ	26
3.3.1	セキュリティに関する課題	26
3.3.2	セキュリティ事案	26
3.3.3	参照すべき指針と医療機関が実施すべき具体的な対応	27
3.3.4	サイバーセキュリティに関連する各種情報	32
4	用語の解説	34
4.1	五十音順	34
4.2	アルファベット順	35

1 オンライン診療の基礎知識

1.1 遠隔医療とは

遠隔医療とは、情報通信機器を活用した健康増進、医療に関する行為であり、どの関係者（医療従事者、介護関係者、患者等）との情報の伝達・提供・共有を行うかによって、大きく次の2つに分類・整理されます。

1.1.1 医療従事者と患者間での遠隔医療

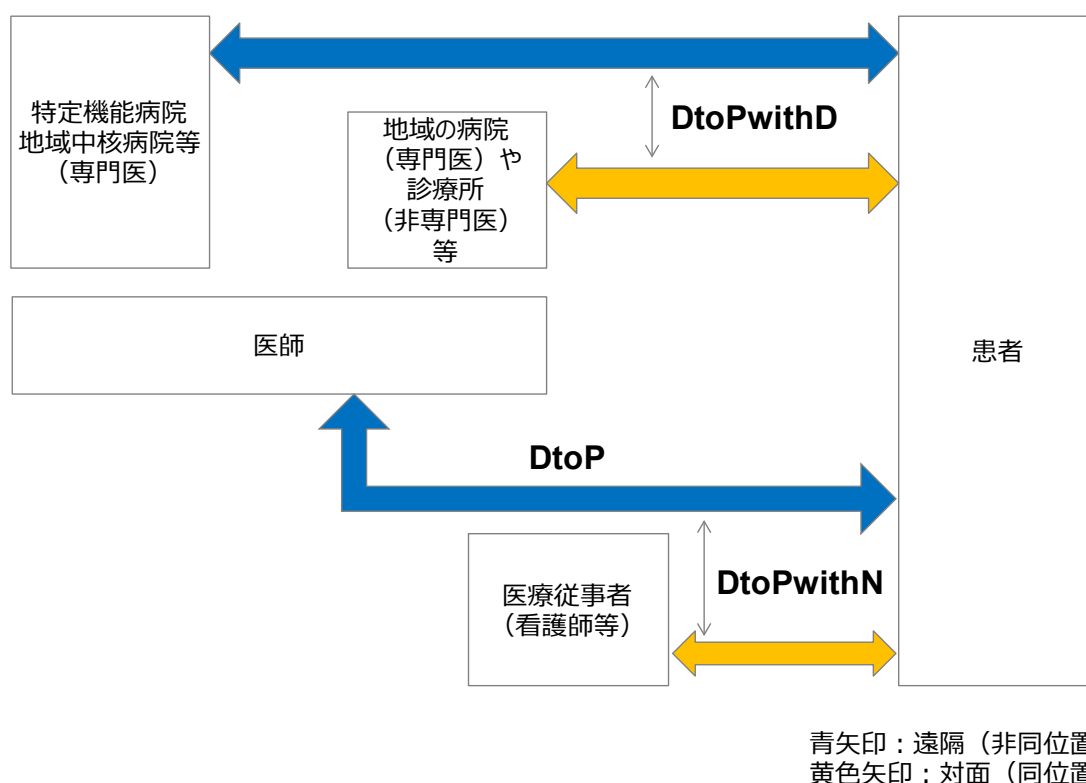


図1-1 医療従事者と患者間での遠隔医療の実施イメージ

医療従事者と患者間での遠隔医療の代表的なモデルに、医師と患者間の DtoP (Doctor to Patient) でオンライン診療を実施するモデルがあります。例えば、テレビ電話を通して医師が在宅患者を診療するなど、遠隔地の患者に対し直接医師が伝送されてくる映像やバイタルデータを通じて診療や健康維持・向上のための助言を行うモデルなどがあります。また、内容面では、医療行為と、健康増進、介護・見守り、指導・教育など直接的な医療行為にならないものと分けられます。オンライン診療以外に医学的な判断を含むものとして、オンライン受診勧奨、医学的判断を伴わないものは遠隔健康医療相談と位置付けられています。医療従事者と患者間での遠隔医療として、医療従事者（例えば看護師等）が患者の日々のバイタルデータを遠隔でモニタリングし、患者の健康状態を管理したり、健康指導したりする遠隔モニタリングもあります。

オンライン診療のその他の形態として、患者が主治医等の医師という場合に行うオンライン診療である D to P with D (Doctor to Patient with Doctor)モデルや患者が看護師等という場合のオンライン診療である D to P with N(Doctor to Patient with Nurse) のモデルがあります。D to P with N は、患者の同意の下、オンライン診療時に、患者は看護師等が側にいる状態で診療を受け、医師は診療の補助行為を看護師等に指示することで、予測された範囲内における治療行為や予測されていない新たな症状等に対する検査が看護師等を介して可能となるモデルになります。

1.1.2 医療従事者間での遠隔医療

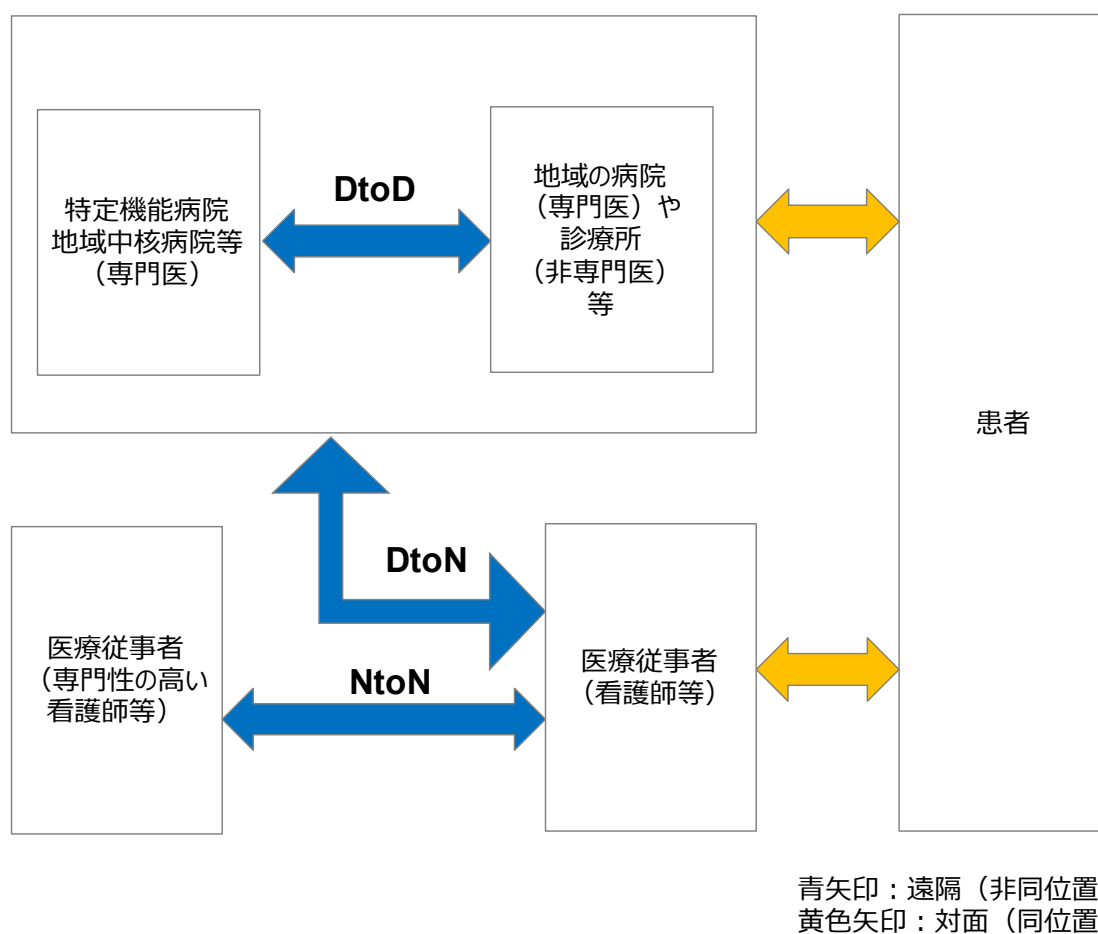


図1－2 医療従事者間での遠隔医療の実施イメージ

医療従事者間での遠隔医療として代表的なモデルは、DtoD (Doctor to Doctor) と呼ばれる医師と医師の間で遠隔医療を実施するモデルです。例えば、へき地の診療所の医師が中核病院の専門医に診療上の相談をしたり、外科医が大学病院の病理医に検体データを送って病理診断を依頼したりするような、医師間で診療支援等を行うモデルが含まれます。

また、医師が情報通信機器を通して、直接患者を診療していない状態で、医師が看護師等の医療従事者を遠隔で支援・指導する DtoN(Doctor to Nurse)モデルや、医師以外の医療従事者間で支援・指導を行う NtoN(Nurse to Nurse)モデルも含まれます。

■医療従事者間の遠隔医療の種類

診断支援(画像診断)	遠隔病理診断、遠隔画像診断等
診療支援	遠隔救急医療支援(脳卒中、心臓血管、災害時等) 遠隔コンサルテーション、専門的診療支援(皮膚科、眼科、ICU、周産期医療等)
指導・教育・コミュニケーション	遠隔カンファレンス、遠隔教育等

1.2 オンライン診療とは

オンライン診療とは、遠隔医療のうち、医師－患者間において、情報通信機器を通して、患者の診察及び診断を行い診断結果の伝達や処方等の診療行為を、リアルタイムで行う行為を指します。

オンライン診療は、オンライン診療指針上、①患者の日常生活の情報も得ることにより、医療の質のさらなる向上に結び付けていくこと、②医療を必要とする患者に対して、医療に対するアクセシビリティ(アクセスの容易性)を確保し、より良い医療を得られる機会を増やすこと、③患者が治療に能動的に参画することにより治療の効果を最大化することを目的として行われるべきものである、とされています。オンライン診療は、ICT を活用し、医師と患者が離れた場所でありながら、患者の状態を把握し、診療を行うものであり、患者の外来通院あるいは医師の訪問診療など、対面による診療行為と適切に組み合わせながら、これを補完するものと位置付けることができます。より効果を高めるために、訪問看護師等が患者宅を訪問して機器の取扱いや診察のサポートを行いながら医師が診断する場合もあります。



図1-3 オンライン診療の位置づけ

2 法的・規制的な基礎知識

2.1 オンライン診療指針の遵守

適切にオンライン診療を実施するに当たっては、オンライン診療指針の「最低限遵守する事項」の遵守が必須です。また、オンライン診療指針では、「推奨される事項」も記載されており、これらの事項に取り組むことが望まれます。

なお、以下の表はオンライン診療指針に位置付けられた事項を医師、患者、オンライン診療システム事業者のそれぞれが取り組むべきかを簡潔に一覧にしたものであり、オンライン診療を実施するに当たっては、必ずオンライン診療指針そのものを確認してください。

■ オンライン診療の提供に関する事項

※1： オンライン診療システム事業者

(1) 医師－患者関係／患者合意			医師	患者	システム ※1	指針内における対策例、補足等
i	医師と患者との間での合意	遵守	●	●		
ii	患者がオンライン診療を希望する旨を明示的に確認 ※オンライン受診勧奨は対象外	遵守	●			患者がオンライン診療を希望する旨を書面（電子データを含む）において署名等してもらう。
iii	実施の可否の判断	遵守	●			適切でないと判断した場合はオンライン診療を中止し、速やかに適切な対面診療に移行する。
iv	以下の事項について事前の説明 ・対面診療を組み合わせる必要があること ・オンライン診療を実施する都度、医師がオンライン診療の実施の可否を判断すること。 ・(3)「診療計画」に含まれる事項	遵守	●			緊急時にやむを得ずオンライン診療を実施する場合で

						あつて、ただちに説明等を行うことができないときは、説明可能となった時点において速やかに説明を行うことが必要
(2) 適用対象						
i	患者の心身の状態に関する有用な情報の取得	遵守	●			
ii	一般社団法人日本医学会連合が作成した「オンライン診療の初診に適さない症状」等の情報を踏まえ、オンライン診療の実施可否を適切に判断	遵守	●			
iii	原則、初診からのオンライン診療は「かかりつけの医師」が実施	遵守	●			
iv	以下のケースにおいては、初診であってもオンライン診療可能。ただし、その後対面診療を実施すること。 ・「かかりつけの医師」がオンライン診療を行っていない場合や休日夜間等で、「かかりつけの医師」がオンライン診療に対応できない場合 ・患者に「かかりつけの医師」がいない場合 ・「かかりつけの医師」がオンライン診療に対応している専門的な医療等を提供する医療機関に紹介する場合（必要な連携を行っている場合、DtoPwithD の場合を含む。）や、セカンドオピニオンのために受診する場合	例外	●			
v	診療前相談により対面受診が必要と判断した場合であつて、対面診療を行うのが他院	遵守	●			

	である場合は、診療前相談で得た情報について必要に応じて適切に情報を提供					
vi	診療前相談を実施する際、結果としてオンライン診療が行えない可能性があることや、診療前相談の費用等について医療機関のホームページ等で示すほか、あらかじめ患者に十分な周知を実施	遵守	●			
vii	原則として、急病急変患者は対面診療	遵守	●			
viii	交代でオンライン診療を行う場合は、「診療計画」に医師名を記載	遵守	●			
ix	・禁煙外来については、定期的な健康診断等が行われる等により疾病を見落とすリスクが排除されている場合であって、治療によるリスクが極めて低いものとして、患者側の利益と不利益を十分に勘案した上で、直接の対面診療を組み合わせないオンライン診療を行うことが許容され得る。 ・緊急避妊に係る診療については、対面診療が困難であると判断された場合、初診からオンライン診療を行うことは許容され得る。ただし、初診からオンライン診療を行う医師は一錠のみの院外処方を行うこととする。	例外	●			
	自身の心身の状態に関する情報の伝達に困難がある患者については、伝達できる情報が限定されるオンライン診療の適用を慎重に判断	推奨	●			
(3) 診療計画						
i	対面診療により、指針の内容を踏まえた診療計画を策定(2年間保存)	遵守	●			

ii	初診からのオンライン診療を行う場合については、診察の後にその後の方針を患者に説明	遵守	●			
iii	医師－患者間で、映像や音声等の保存の要否や保存端末等の取り決めを明確にし、双方で合意	遵守	●	●		
iv	急変に対応できる体制の整備（急変に対応できる医療機関に対して患者情報の共有を定期的に実施）	遵守	●			
i	診療計画は、文書又は電磁的記録により患者が参照できるようにする。	推奨	●			
ii	診療計画の継続に努める。	推奨	●			
(4) 本人確認						
i	原則として、医師と患者双方が身分確認書類を用いてお互いに本人であることを確認（社会通念上、本人であると認識できる状況であれば、都度本人確認を行う必要はない。）	遵守	●	●		
ii	初診でオンライン診療を実施する場合、当該患者の本人確認を実施	遵守	●			（患者）原則として、顔写真付きの身分証明書（マイナンバーカード、運転免許証、パスポート等）を提示
iii	医師本人の氏名を示す（社会通念上、当然に医師本人であると認識できる場合を除く。）	遵守	●			（医師）HPKI カード（医師資格証）、マイナンバーカード、運転免許証、パ

						スポーツ等の提示
	iv	医師が医師免許を保有していることを患者が確認できる環境を整備（社会通念上、医師であると認識できる状況であれば証明の必要はない。）	遵守	●		
(5) 薬剤処方・管理						
	i	現にオンライン診療を行っている疾患の延長とされる症状に対応するために必要な医薬品については、医師の判断により、オンライン診療による処方が可能 初診からのオンライン診療の場合及び新たな疾患に対して医薬品の処方を行う場合は、一般社団法人日本医学会連合が作成した「オンライン診療の初診での投与について十分な検討が必要な薬剤」等の関係学会が定める診療ガイドラインを参考に処方	遵守	●		
		初診の場合は、以下の処方は不可 ・麻薬及び向精神薬の処方 ・基礎疾患等の情報が把握できていない患者に対する、特に安全管理が必要な薬品（診療報酬における薬剤管理指導料の「1」の対象となる薬剤）の処方 ・基礎疾患等の情報が把握できていない患者に対する8日分以上の処方	例外	●		
	ii	現在服薬している医薬品を確認（患者は医師に対し正確な申告を行う）	遵守	●	●	
		患者に対し、かかりつけ薬剤師・薬局の下、医薬品の一元管理を行うことを求める。	推奨	●		
(6) 診察方法						

i	患者の状態について十分に必要情報が得られていると判断できない場合には、速やかにオンライン診療を中止	遵守	●			
ii	リアルタイムの視覚及び聴覚の情報を含む情報通信手段を採用する(併せて画像や文字等による情報のやり取りを活用することは良い。)	遵守	●			
iii	同時に複数の患者の診療を行ってはならない	遵守	●			
iv	医療従事者等が同席する場合は、その都度患者に説明を行い、患者の同意を得る	遵守	●			
i	開始時間及び終了時間をアクセスログとして記録するシステムであること	推奨			●	医師と患者が1対1で診療を行っていることを確認するため
ii	利用前の動作確認	推奨	●			

■オンライン診療の提供体制に関する事項

(1) 医師の所在			医師	患者	システム	指針内における対策例、補足等
i	医師は、医療機関に所属し、その所属を明らかにする。	遵守	●			
ii	急変に対応できる体制の整備	遵守	●			
iii	不適切な場所での実施の禁止	遵守	●			
iv	患者のこれまでの情報を得られる環境での実施(緊急の場合はこの限りではない。)	遵守	●			

v	物理的に外部から隔離される空間において実施	遵守	●			
vi	ホームページや院内掲示等において、「オンライン診療の適切な実施に関する指針」を遵守した上でオンライン診療を実施している旨を公表	遵守	●			
	急変に対応できる体制を組んでいる医療機関に容易にアクセスできるよう努める。	推奨	●			
(2)患者の所在						
i	清潔かつ安全な場所で実施	遵守		●		
ii	物理的に外部から隔離される空間において実施	遵守		●		
iii	特定多数人に対してオンライン診療を提供する場合には、診療所の届出を行う。 (巡回診療、健康診断等は除く。)	遵守	●			
	患者の勤務する職場等についても許容	例外		●		
(3)患者が看護師等という場合のオンライン診療						
	診療計画及び訪問看護指示書に基づき、予測された範囲内において診療の補助行為を行う。	遵守	●			
	新たな症状の場合、診断の補助となり得る追加的な検査を指示することは可能(診断や治療は対面で実施)	例外	●			
	D to P with N のDは原則、訪問診療等を定期的に行っている医師、Nは同一医療機関の看護師等あるいは訪問看護の指示を受けた看護師等	遵守	●			
(4)患者が医師という場合のオンライン診療						

	患者の側にいる医師は、既に直接の対面診療を行っている主治医等であり、遠隔地にいる医師は、あらかじめ、主治医等の医師より十分な情報提供を受けること。	遵守	●			
	診療の責任の主体は、原則、主治医等の医師（医師間で責任分担等についてあらかじめ協議する。）	遵守	●			
1) 情報通信機器を用いた遠隔からの高度な技術を有する医師による手術等						
	遠隔地にいる医師でないと実施が困難な手術等を必要とし、かつ、患者の体力面などから当該医師の下への搬送・移動等が難しい患者を対象	遵守	●			
	手術等を実施するに当たり重大な遅延等が生じない通信環境を整備（不具合が生じた場合にも患者の側にいる主治医等の医師により手術の安全な継続が可能な体制を構築）	遵守	●			
2) 情報通信機器を用いた遠隔からの高度な専門性を有する医師による診察・診断等						
	希少性の高い疾患等、専門性の観点から近隣の医療機関では診断が困難な疾患であることや近隣の医療機関では診断が困難な疾患や遠隔地のため受診に時間がかかる患者を対象	遵守	●			
	患者の側にいる主治医等の医師と遠隔地にいる医師は、事前に診療情報提供書等を通じて連携	遵守	●			

■通信環境(情報セキュリティ・プライバシー・利用端末)に関する事項

(5) 通信環境(情報セキュリティ・利用端末)		医療機関	患者	システム	指針内における対策例
1)医療機関が行うべき対策					
オンライン診療に用いるシステムを提供する事業者による説明を受け、十分な情報セキュリティ対策が講じられていることを確認。また、責任分界点について確認し、システムの導入に当たっては、リスクを十分に理解すること。	遵守	●			
オンライン診療の際、医療情報システムに影響を及ぼす可能性があるオンライン診療システムを使用する際は、「医療情報安全管理関連ガイドライン」に沿った対策を併せて実施	遵守	●			
患者に対してオンライン診療の実施に伴うセキュリティリスクを説明し、オンライン診療に用いるシステムを利用することについての合意を得た上で、双方が合意した旨を診療録に記載し、オンライン診療を実施	遵守	●	●		
診療計画を作成する際に、患者に対して使用するオンライン診療システムに伴うセキュリティリスク等とその対策及び責任の所在について患者からの問い合わせに対応できるよう、説明文書の準備又は対応者の準備を行うこと。	遵守	●			
OS やソフトウェアのアップデートについて、事業者と協議・確認した上で実施するとともに、アップデートができない等の個別対応が必要な場合には、事業者からの説明、情報提供等を受け、必要な対応を実施すること。	遵守	●			

必要に応じてセキュリティソフトをインストールすること。	遵守	●			
オンライン診療に用いるシステムを使用する際には、多要素認証を用いるのが望ましいこと。	推奨	●		●	
患者がいつでも医師の本人確認ができるように必要な情報を掲載すること。	遵守	●			
オンライン診療システムを用いる場合は、患者がいつでも医師の本人確認ができる情報及び医療機関の問い合わせ先をオンライン診療システム上に掲載すること。	遵守	●			
オンライン診療システムが指針の要件を満たしていることを確認すること。	遵守	●			
医師がいる空間に診療に関わっていない者がいるかを示し、また、患者がいる空間に第三者がいなかったか確認する(患者がいる空間に家族等やオンライン診療支援者がいることを医師及び患者が同意している場合を除く。)	遵守	●			
意図しない第三者が当該通信に紛れ込むような三者通信(患者が医師の説明と一緒に聞いてもらうために、医師の同意なく第三者を呼び込む場合等)や患者のなりすましが起こっていないことに留意すること。	遵守	●			
患者側、医師側ともに録音、録画、撮影を同意なしに行うことがないよう確認すること。	遵守	●			
チャット機能を補助的に用いる場合には、医療機関が、セキュリティリスクとベネフィットを勘案したうえで、使用するソフトウェアやチャ	遵守	●			

ット機能の使用方法について患者側に指示を行うこと。					
患者から提示された二次元バーコードや URL 等のリンク先へのアクセス及びファイルのダウンロード等はセキュリティリスクが高いため、セキュリティリスクが限定的であることを医療機関が合理的に判断できる場合を除き、このようなアクセスやダウンロード等を行わないことが望ましい。	遵守	●			
オンライン診療を実施する医師は、オンライン診療の研修等を通じて、セキュリティリスクに関する情報を適宜アップデートすること。	遵守	●			
医療情報を取得する目的で外部の PHR 等の情報を取り扱うことが、医療情報システムに影響を与える場合は、「医療情報安全管理関連ガイドライン」に沿った対策を実施。医療情報システムに影響を与えずに当該情報を取り扱う場合には、セキュリティリスクについて医療機関と患者の間で合意を得た上で、オンライン診療を実施すること。	遵守	●		●	
1-2) 医療機関が汎用サービスを用いる場合に特に留意すべき事項					
医療機関側から患者側につなげることを徹底し、通信の管理者権限を患者に委譲しないこと。	遵守	●			
汎用サービスのセキュリティポリシーを適宜確認し、患者の問い合わせに対応できるようにすること。	遵守	●			
個別の汎用サービスに内在するセキュリティリスクを理解し、必要な対策を講じる責任は医療機関にあり、委託を受けた者が存在す	遵守	●			

る場合は、委託契約に基づき協力する責務が委託を受けた者に課されることを理解すること。					
端末立ち上げ時、パスワード認証や生体認証などを用いて操作者の認証を行うこと。	遵守	●			
2) オンライン診療システム事業者が行うべき対策					
2-1) 基本事項					
医療機関に対して、医療機関が負う情報漏洩・不正アクセス等のセキュリティリスク及びシステム障害時の診療への影響を明確に説明すること。	遵守			●	
事業者は医療機関に対して、オンライン診療のセキュリティに係る責任分界点について明確に説明し、合意した範囲において責任を負うこと。	遵守			●	
汎用サービスを組み込んだシステムにおいても、事業者はシステム全般のセキュリティリスクに対して責任を負うこと。	遵守			●	
事業者は、合意に基づき、脆弱性などのセキュリティリスク発生時には速やかに医療機関に状況や対応方法等の情報提供を行うなどの善管注意義務を適切に履行すること。	遵守			●	
オンライン診療システム等が医療情報システムに影響を及ぼし得るかを明らかにすること(※)。	遵守			●	
医療情報システム以外のシステム(端末・サーバー等)における診療にかかる患者個人に関するデータの蓄積・残存の禁止(※)	遵守			●	
システムの運用保守を行う医療機関の職員や事業者、クラウドサービス事業者におけるアクセス権限の管理(※)	遵守			●	(ID/パスワードや生体認証、ICカード等により多

					要素認証を実施することが望ましい。)
不正アクセス防止措置(※)	遵守			●	(IDS/IPS を設置する等)
不正アクセスやなりすましを防止するとともに、患者が医師の本人確認を行えるように、医師の本人証明と医師の所属医療機関の確認が常に可能な機能を備えること(※)。	遵守			●	
アクセスログの保全措置(※)	遵守			●	(ログ監査・監視を実施することが望ましい。)
端末へのウィルス対策ソフトの導入 OS・ソフトウェアのアップデートの実施を定期的に促す機能(※)	遵守			●	
信頼性の高い機関によって発行されたサーバ証明書を用いて、通信の暗号化(TLS1.2以上)を実施(※)	遵守			●	
複数の患者が同一の施設からネットワークに継続的に接続する場合には、IP-VPN や IPsec+IKE による接続を行うことが望ましいこと(※)。	推奨	●		●	
遠隔モニタリング等で蓄積された医療情報については、「医療情報安全管理関連ガイドライン」に基づいて、安全に取り扱えるシステムを確立すること(※)。	遵守			●	
使用するドメインが不適切な移管や再利用が行われないように留意	遵守			●	
2-2)医療情報システムに影響を及ぼす可能性があるシステムの場合(特に留意すべき点を例示)					

法的保存義務のある医療情報を保存するサーバを国内法の執行が及ぶ場所に設置すること(※)。	遵守			●	
医療機関に対してそれぞれの追加的リスクに関して十分な説明を行い、事故発生時の責任分界点を明らかにすること。	遵守			●	
医療情報を保存するシステムへの不正侵入防止対策等を講ずること(※)。	遵守			●	
オンライン診療システムは、上記の2-1)及び2-2)の(※)を満たしているシステムであるかどうか、第三者機関に認証されるのが望ましい。	推奨			●	第三者機関の認証としては以下のいずれかが望ましい。 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)、プライバシーマーク(JIS Q15001)、ISMS(JIS Q27001 等)、ITSMS(JIS Q20000-1 等)の認証、情報セキュリティ監査報告書の取得、クラウドセキュリティ推進協議会のCSマークやISMSクラウドセキュリティ認証(ISO27017)の取得
3) 患者に実施を求めるべき内容					
3-1) 共通事項					
使用するシステムに伴うリスクを把握すること。	遵守			●	
使用するアプリケーション、OS が適宜アップデートされることを確認すること。	遵守			●	

医師側の了解なくビデオ通話を録音、録画、撮影してはならないこと。	遵守		●		
医師のアカウント等の情報を診療に関わりのない第三者に提供してはならないこと。	遵守		●		
医師との通信中は、第三者を参加させないこと。	遵守		●		
汎用サービスを使用する際は、患者側からは発信しないこと。	遵守		●		
3-2)医療情報システムに影響を及ぼしうるケース(医療機関が判断の上、患者に通知した場合に限る)					
原則、医療機関が求めない限り、あるいは指示に反して、チャット機能の利用やファイルの送付などは行わないこと。特に外部 URL への誘導を含むチャットはセキュリティリスクが高いため行わないこと。	遵守		●		

■その他オンライン診療に関連する事項

(1)医師教育／患者教育		医師	患者	システム	指針内における対策例
医師は、オンライン診療に責任を有する者として、厚生労働省が定める研修を受講することにより、オンライン診療を実施するために必須となる知識を習得しなければならない。	遵守	●			※2020 年 4 月以降、オンライン診療を実施する医師は厚生労働省が指定する研修を受講しなければならない。
医師は、オンライン診療に責任を有する者として、医療関係団体などによる研修の受講等によりこうした知識の習得に努めるとともに、1の(1) 医師－患者関係／患者合意及	遵守	●			

び(3) 診療計画に示す事項及び情報通信機器の使用法、医療情報のセキュリティ上安全な取扱い等について、患者に対しあらかじめ説明しておくべきである。					
オンライン診療では、対面診療に比して、より患者が積極的に診療に協力する必要があることも、あらかじめ説明しておくべきである。	遵守	●			
患者は、オンライン診療には医師に伝達できる情報等に限界があることを理解し、うまく情報が伝わらない等により医師がオンライン診療の実施の中止を決めたときは、提供される医療の安全を確保する観点から、医師の判断が尊重されるべきである。	遵守		●		
(2) 質評価／フィードバック					
オンライン診療では、質評価やフィードバックの体制の整備が必要である。対面診療と同様に診療録の記載は必要であるが、対面診療における診療録記載と遜色の無いよう注意を払うべきである。	遵守	●			
診断等の基礎となる情報(診察時の動画や画像等)を保管する場合は、医療情報安全管理関連ガイドライン等に準じてセキュリティを講じるべきである。	遵守	●			

2.2 遵守する法令等

要配慮個人情報を含めた個人情報の取扱いに関しては、関係法令が制定され、また関係省庁からもガイドラインが公表されています。医療機関においては、これらを踏まえて規則類を整備し、遵守しているものと考えられます。

オンライン診療を導入する場合においても、他の情報システム(電子カルテ等)と同様、導入先医療機関の規則類を事前に確認し、それに抵触しないシステム構成・運用体制とすることが求められます。

以下に挙げるガイドラインは、オンライン診療指針に加えて、併せて確認しておく必要があります。また、各ガイドライン内において、必要な法令類を示しているものもあるため、それらの内容も確認しておく必要があります。

- ・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス(厚生労働省)
- ・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(厚生労働省)
- ・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第 1.1 版(総務省・経済産業省)¹
- ・情報通信機器を用いた精神療法を安全・適切に実施するための指針の策定に関する検討-報告書-(厚生労働省)

2.3 関係団体による各種手引き

関係団体がオンライン診療に係る標準的な手順や考え方をまとめた手引きを以下に示します。

- ・オンライン診療入門～導入の手引き～(公益社団法人日本医師会)
- ・遠隔診療実践マニュアル—在宅医療推進のために(日本遠隔医療学会編集委員会)
- ・精神科領域における遠隔(オンライン)診療のため手引書(遠隔精神科医療手引書策定タスクフォース)
- ・臨床におけるオンライン診療の手引き(日本オンライン診療研究会)

【歯科におけるオンライン診療に関する参考文献】

- ・厚生労働省 ICTを活用した歯科診療等に関する検討会(事例紹介)
<https://www.mhlw.go.jp/content/10804000/001171407.pdf>

¹ オンライン診療システム以外の医療情報システムに影響を及ぼす可能性がある場合は、「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」に沿った対策を併せて実施する必要があります。

3 技術とインフラに関する基礎知識

3.1 オンライン診療システムの概要

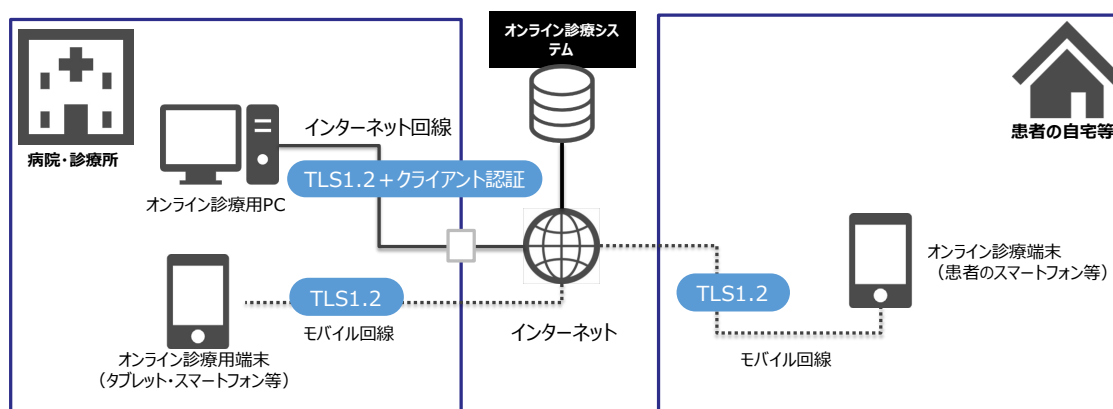
3.1.1 システム構成

オンライン診療システムは、遠隔地の医師がテレビ電話等の ICT ツールを活用して、患者の顔色や表情、動作等を確認しながら問診を行うことを可能にするシステムです。ツールとしては、さらに、テレビ電話等だけでなく、体重、血圧等のバイタルデータや問診記録等を伝送可能なシステムもあります。

なお、ネットワーク品質の確保の観点から、従来は有線ネットワークの利用が推奨されていましたが、最近では、安定した品質とセキュリティが確保されるのであれば、無線ネットワークや携帯通信網を利用することも一般的です。

どのような運用をするか検討したうえで、導入するシステムを選定します。導入システムとしては、オンライン診療システムとして提供されている有料サービスや無料で利用できる汎用サービスがあります。

ただし、オンライン診療指針において、汎用サービスを用いる場合には、医師側から患者側につなげることの徹底や汎用サービスのセキュリティポリシーを適宜確認し、必要に応じて患者に説明することなど、追加で実施することが求められている事項がありますので留意が必要です。



- ・オンライン診療システムはクラウド型での提供が一般的
- ・病院側の回線は院内の情報システムのネットワークと分離されているケースが多い

図 3-1 オンライン診療におけるシステム構成の例

3.1.2 機能構成

(1)機能体系図

オンライン診療システムの一般的な機能を以下に示します。

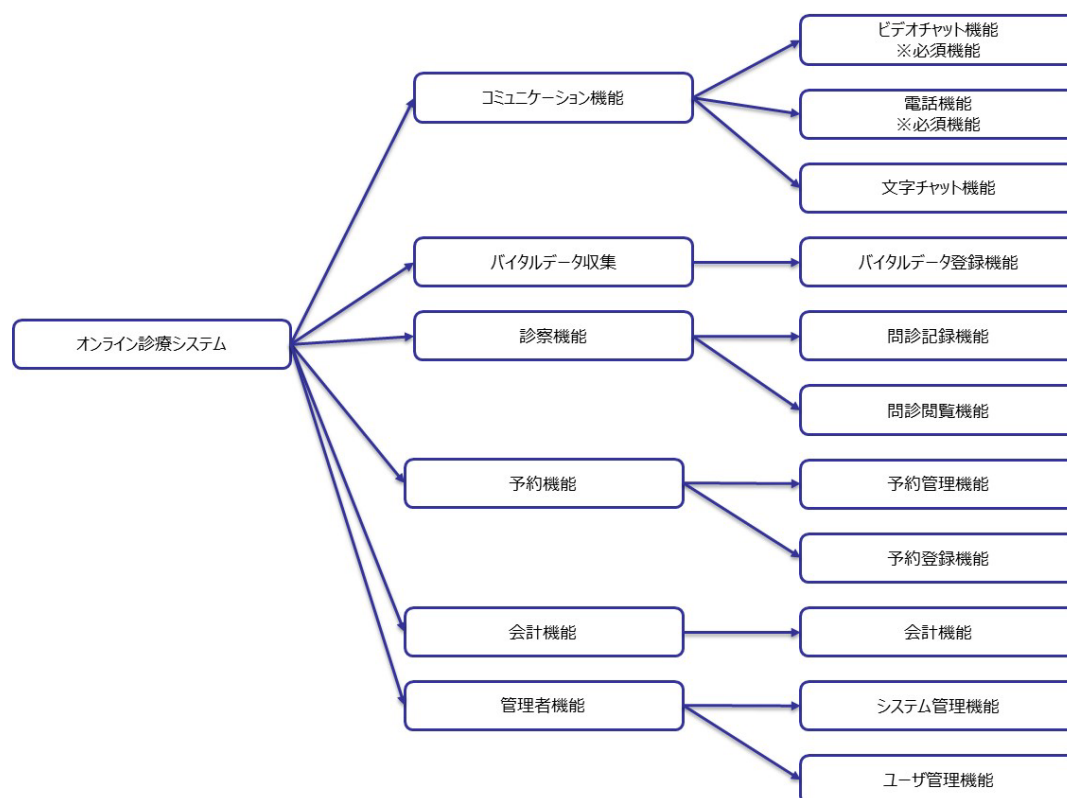


図 3-2 オンライン診療システムの一般的な機能一覧

(2)機能一覧

■機能の概要

機能		機能概要
大分類	小分類	
コミュニケーション機能	ビデオチャット機能	医師と患者を映像でつなぎ、相互に表情や顔色を確認しながら、診療を行うための機能
	電話機能	緊急時の判断等のために、医師—患者間で音声にてコミュニケーションを取るための機能
	文字チャット機能	必要に応じて文字で医師—患者間がコミュニケーションを取るための機能
バイタルデータ収集	バイタルデータ登録機能	患者が測定したバイタルデータをサーバに保管し、後で参照可能にする機能
診察機能	問診記録機能	オンライン診療の対象となる患者がオンラインで問診を受け、その結果を記録する機能
	問診閲覧機能	患者が回答した問診内容を医師用端末で表示させる機能
予約機能	予約管理機能	診察を実施する日の予約枠の設定や、予約枠を削除する等の管理を、医師側の端末で実施する機能
	予約登録機能	診察を行う日時を予約するための機能。患者や医療機関双方の利用が可能なが多い。
会計機能	会計機能	クレジットカード等の電子決済機能と連携し、実施後に精算する機能
管理者機能	システム管理機能	システム利用の実績管理を行い、セキュリティ向上と利用状況の把握のために活用する機能。またデータのバックアップを行う機能
	ユーザー管理機能	システムのセキュリティ確保のため、ユーザーアカウントの作成・削除、ユーザー権限管理の設定等を行う機能。また、組織で決定されるセキュリティポリシーに従い、システムのアクセスに関するルールを設定する機能

3.1.3 ハードウェア・ネットワーク構成

システム構成におけるハードウェア・ネットワークの構成は以下のとおりです。設置場所は医療機関と患者側の実施拠点(患者自宅や職場等)となります。PC・スマートフォンなど、導入済みの機器等で適切な性能を有するものがあれば、それを流用(他の用途と兼用)するこ

とで、導入費用を縮減することが可能です(なお、医療情報システム²に影響を及ぼす可能性のある³オンライン診療システムを使用する際は、「医療情報安全管理関連ガイドライン」に沿った対策を併せて実施する必要があります。また、汎用サービスを使用する際は、汎用サービスが医療情報システムに影響を与えない設定とする必要があります。)

■機器概要と参考仕様等

機器名	台数	説明	備考(参考仕様等)
PC 及びモニター(医療機関用)	1台/医療従事者	医師が患者とテレビ会議ができるPC とモニター(またはタブレット端末等)	既存機器の利用可。 (ただし、電子カルテ用端末とは区分するケースがほとんど。)
ビデオチャット用端末(患者用)	1台/患者	患者が医師とテレビ会議ができる端末(PC、スマートフォン、タブレット等)	既存機器の利用可。 (患者保有のスマートフォンやタブレット等を利用することが多い。オンライン診療システムが患者保有のスマートフォンやタブレット等のOS(Operation System)に対応していない場合もあり留意が必要)
インターネット回線	1回線/患者・医療機関間	オンライン診療システム(クラウドサービス等)へのアクセスのため。	既存ネットワークの利用可。 (医療機関においては、院内LANと分離されたネットワークで接続するケースが多い。)患者側は移動通信網を介してアクセスするケースが多い。

3.2 オンライン診療システムの構築パターン

3.2.1 前提条件

オンライン診療は、テレビ電話等の機能を活用して診察を行うことが基本となります。オンライン診療の主要な導入パターンとして、(i)オンライン診療専用のサービス事業者が提供する「オンライン診療システム」を活用するパターン、(ii)FaceTime や Skype などの既存の

² 医療情報システムは、医療機関のレセプト作成用コンピュータ、電子カルテ、オーダーリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も対象として想定される。また、患者情報の通信が行われる院内・院外ネットワークも含む。

³ 例えば、電子カルテを利用する端末で、オンライン診療に用いるシステムを直接起動し、オンライン診療を行うと、セキュリティ上の問題が生じた場合、当該診療に係る患者だけではなく、電子カルテデータベースやそれと連結した医事システムやレセプト作成用コンピュータ内のすべての患者の情報に影響が及ぶ可能性がある。

「汎用テレビ電話システム」を活用するパターン、(iii)新規にオンライン診療のシステムを開発するパターンの3種類が存在します。(i)及び(ii)では医師側はオンライン診療用の端末(PC・スマートフォン・タブレット等)を準備し、患者側は個人の保有するスマートフォンやタブレット等の携帯端末を使用することがほとんどです。また、医師(医療機関)側では通常のインターネット回線が整備されているものとします。

3.2.2 費用の目安

(i) オンライン診療システム

<医療機関側>

- ・ 初期費用: 端末代金+オンライン診療システム導入費用(※1)
- ・ 運用費用: オンライン診療システム利用料(※2)、通信料 (セキュリティ対策ソフト利用料などがかかる場合がある。)

<患者側>

- ・ 初期費用: なし(既に端末を保有している場合)
- ・ 運用費用: 通信料(別途オンライン診療システム利用料(※2)が患者側にも発生する場合もある。その他、セキュリティ対策ソフト利用料などがかかる場合がある。)

(※1) オンライン診療システム導入費用はおおむね 30～50 万円程度(一部、無料で提供している事業者も存在)。なお、オンライン診療専用端末と併せてオンライン診療システムを提供する場合や、オーダーメイドでオンライン診療システムを提供する場合など導入費用の負担が大きくなるケースも存在する。

(※2) 医師側のオンライン診療システム利用料はおおむね1～3万円/月程度(一部、無料で提供している事業者も存在)。患者側にオンライン診療システム利用料が発生するケースでは数百円/回程度と回数に応じた料金体系となっている事例がある。一部の医院では診療報酬を請求せず、患者から15分あたり数千円程度の費用を徴収する事例がある。

(ii) 汎用サービスシステム

<医療機関側>

- ・ 初期費用: 端末代金(病院側でオンライン診療用専用端末を準備することが望ましい。)
- ・ 運用費用: 通信料(セキュリティ対策ソフト利用料などがかかる場合がある。)

<患者側>

- ・ 初期費用: なし(既に端末を保有している場合)
- ・ 運用費用: 通信料(セキュリティ対策ソフト利用料などがかかる場合がある。)

(iii) 独自開発システム

- ・ 費用の目安は開発するシステム内容によって大きく異なる。

3.3 サイバーセキュリティ

3.3.1 セキュリティに関する課題

オンライン診療の導入と推進は、医療機関にとって重要な取り組みですが、令和5年度の総務省「医療・介護・健康データの利活用促進に関する調査研究」の調査の結果、医療機関における IT とセキュリティに関する専門知識が不足していることが課題となっている可能性が示唆されました。この専門知識の不足は、オンライン診療の安全性を確保する上で、重要な問題です。セキュリティ対策の遅れは、患者情報の漏洩やサイバー攻撃のリスクを高めるだけでなく、医療機関の信頼性にも影響を及ぼします。現在、多くの病院がこの問題に直面しており、特に中小規模の医療機関では、限られたリソースの中で最適な解決策を模索されています。このような現状を踏まえると、オンライン診療を提供するにあたり、医療機関とシステムを提供するベンダー間における責任分界点の明確化が重要です。この明確化には、データ保護、アクセス管理、システムの監視といったセキュリティ対策が含まれます。医療機関とベンダーがそれぞれの責任を正確に理解し、協力して対策を講じることが、安全で効果的なオンライン診療の提供に重要な要素となります。

3.3.2 セキュリティ事案

サイバーセキュリティ事故は、医療機関において深刻な問題を引き起こす可能性があります。以下に示す事例は、医療機関が直面する可能性のあるセキュリティリスクの一部に過ぎず、全ての事案を網羅しているわけではない点にご注意ください。また、以下に示す事例は、オンライン診療のシステムが原因で発生した事案ではありません。

1) ランサムウェア攻撃の事例

A 医療センターでは、病院の主要なシステムがランサムウェアにより暗号化され、患者の個人情報と健康記録のアクセスが遮断されました。攻撃者はデータの解放と引き換えにビットコインでの身代金支払いを要求。この攻撃により、医療機関は、電子カルテへのアクセスが不可能となり、紙ベースでの記録をせざるを得なくなりました。このことにより、医療サービスの提供に重大な遅延をもたらし、緊急手術のスケジュール調整にも影響を与えました。

本事例は、オンライン診療プラットフォームも同様の脅威にさらされる可能性があることを示しています。オンライン診療では、患者と医療提供者間のコミュニケーションや診療記録の共有が主にデジタル形式で行われるため、ランサムウェアによるシステムの暗号化は、診療予約の遅延、患者情報へのアクセス障害、診療の質の低下に影響します。これらにより、患者の健康管理に重大な影響を及ぼす可能性があります。

2) フィッシング詐欺による情報漏洩の事例

B 大学病院では、職員が巧妙なフィッシングメールに騙され、ログイン情報を盗まれる事案が発生しました。攻撃者はこの情報を利用して医療機関の内部ネットワークに侵入し、患者の診療情報、個人情報、研究データにアクセスしました。このアクシデントは、職員のサイバーセキュリティ教育の重要性と、フィッシング攻撃への警戒の必要性を浮き彫りにしています。

本事例は、オンライン診療プラットフォームを利用する職員も同様の攻撃によって、患者の重要な健康情報や個人情報漏洩するリスクがあることを示唆しています。このような情報漏洩は患者の信頼を損なうだけでなく、法的な責任や評判の損失にもつながります。

3) 内部犯によるデータ侵害の事例

C クリニックでは、内部の者によるデータ侵害が発生しました。従業員が患者の診療情報を不正に持ち出し、これを外部の第三者に販売していたことが発覚しました。この行為は、患者と医療機関間の信頼関係を根底から揺るがすものであり、医療情報の厳格な管理体制の必要性を示しています。

本事例は、オンライン診療システム内での医療情報管理の脆弱性を浮き彫りにします。オンライン診療では、患者情報のデジタル化が進んでいるため、内部の不正アクセスによる情報の不正利用や漏洩は、患者のプライバシーを危険にさらします。患者の信頼を損なうだけでなく、医療機関に対する信頼を毀損します。

これらの事例は、サイバーセキュリティが医療機関にとって極めて重要であることを示しています。ランサムウェア攻撃、フィッシングによるデータ漏洩、内部による情報の不正利用など、多岐にわたるリスクに対処するためには、包括的なセキュリティ対策と継続的なリスク管理が不可欠です。さらに、これらの事例は実際に発生したセキュリティ事故の一部に過ぎず、医療機関は常に新たな脅威に警戒し、適切な予防措置を講じる必要があることに注意してください。

3.3.3 参照すべき指針と医療機関が実施すべき具体的な対応

オンライン診療の安全な実施には、セキュリティ対策が不可欠です。本項目では、厚生労働省が提供するオンライン診療指針と、医療機関が実際に取り組んでいる具体的なセキュリティ対策を紹介します。これらの指針と実例を参照することで、オンライン診療サービスの提供と患者情報の保護をより効果的にサポートすることが期待されます。

i) オンライン診療の適切な実施に関する指針「セキュリティ該当部分」

本稿の内容は、令和5年2月時点における厚生労働省「オンライン診療の適切な実施に関する指針平成 30 年3月(令和5年3月一部改訂)」のセキュリティ該当部分を抜粋したものです。最新版は以下の URL をご確認ください。

【オンライン診療の適切な実施に関する指針】

<https://www.mhlw.go.jp/content/001126064.pdf>

(5) 通信環境(情報セキュリティ・ プライバシー・ 利用端末)

オンライン診療の実施に当たっては、利用する情報通信機器やクラウドサービスを含むオンライン診療システム(※1)及び汎用サービス(※2)等を適切に選択・使用するために、個人情報及びプライバシーの保護に配慮するとともに、使用するシステムに伴うリスク(機密情

報の漏洩や不正アクセス、データの改ざん、サービスの停止等)を踏まえた対策を講じた上で、オンライン診療を実施することが重要である。

※1 オンライン診療システムとは、オンライン診療で使用されることを念頭に作成された視覚及び聴覚を用いる情報通信機器のシステム

※2 汎用サービスとは、オンライン診療に限らず広く用いられるサービスであって、視覚及び聴覚を用いる情報通信機器のシステムを使用するもの

1) 医療機関が行うべき対策

医療機関は、オンライン診療に用いるシステムによって講じるべき対策が異なることを理解し、オンライン診療を計画する際には、患者に対してセキュリティリスクを説明し、同意を得なければならない。医療機関は、システムは適宜アップデートされ、リスクも変わり得ることなど、理解を深めるべきである。

1-1) 基本事項

- ・ 医療機関は、オンライン診療に用いるシステムを提供する事業者(以下「事業者」という。)による説明を受け(システムに関する個別の説明を受けることのみならず、事業者が提示している情報提供内容を自ら確認することを含む。)、十分な情報セキュリティ対策が講じられていることを確認すること。また、当該確認に際して、医療機関は責任分界点について確認し、システムの導入に当たっては、そのリスクを十分に理解すること。
- ・ オンライン診療の際、医療情報システム(※1)に影響を及ぼす可能性がある(※2)オンライン診療システムを使用する際は、「医療情報安全管理関連ガイドライン」に沿った対策を併せて実施すること。なお、汎用サービスを使用する際は、汎用サービスが医療情報システムに影響を与えない設定とすること。

※1 医療情報システムは、医療機関のレセプト作成用コンピュータ、電子カルテ、オーダーリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も対象として想定される。また、患者情報の通信が行われる院内・院外ネットワークも含む。

※2 例えば、電子カルテを利用する端末で、オンライン診療に用いるシステムを直接起動し、オンライン診療を行うと、セキュリティ上の問題が生じた場合、当該診療に係る患者だけではなく、電子カルテデータベースやそれと連結した医事システムやレセプト作成用コンピュータ内のすべての患者の情報に影響が及ぶ可能性がある。

- ・ 医療機関は、患者に対してオンライン診療の実施に伴うセキュリティリスクを説明し、オンライン診療に用いるシステムを利用することについての合意を得た上で、双方が合意した旨を診療録に記載し、オンライン診療を実施すること。
- ・ 「診療計画」を作成する際、患者に対して使用するオンライン診療システムに伴うセキュリティリスク等とその対策及び責任の所在について患者からの問い合わせに対応できるよう、説明文書の準備(ウェブサイト等の患者が適切にアクセスできる方法

による開示や、電磁的記録による説明文書と同等の内容のものの提供を含む。)又は対応者の準備を行うこと。

- ・ オンライン診療システムを用いる場合は、医療機関は OS やソフトウェアのアップデートについて、事業者と協議・確認した上で実施するとともに、アップデートができない等の個別対応が必要な場合には、事業者からの説明、情報提供等を受け、必要な対応を実施すること。
- ・ 医療機関は、必要に応じてセキュリティソフトをインストールすること。
- ・ オンライン診療に用いるシステムを使用する際には、多要素認証を用いるのが望ましい。
- ・ オンライン診療を実施する際は、患者がいつでも医師の本人確認及び医師の所属医療機関の確認ができるように必要な情報を準備すること。
- ・ オンライン診療システムを用いる場合は、患者がいつでも医師の本人確認ができる情報及び医療機関の問い合わせ先をオンライン診療システム上に掲載すること。
- ・ オンライン診療システムが後述の2)に記載されている要件を満たしていることを確認すること。
- ・ 医師がいる空間において診療に関わっていない者が診察情報を知覚できないこと。また、患者がいる空間に第三者がいないことを確認すること。ただし、患者がいる空間に家族等やオンライン診療支援者がいることを医師及び患者が同意している場合を除く。
- ・ 医師は、オンライン診療実施時に、意図しない第三者が当該通信に紛れ込むような三者通信(患者が医師の説明と一緒に聞いてもらうために、医師の同意なく第三者を呼び込む場合等)や患者のなりすましが起こっていないことに留意すること。
- ・ プライバシーが保たれるように、患者側、医師側ともに録音、録画、撮影を同意なしに行うことがないよう確認すること。
- ・ オンライン診療においてチャット機能を補助的に用いる場合には、医療機関が、セキュリティリスクとベネフィットを勘案したうえで、使用するソフトウェアやチャット機能の使用方法について患者側に指示を行うこと。
- ・ 医療機関や患者から、検査結果画像や患者の医療情報等を画面共有機能を用いて提示すること及び画面共有機能を用いずに画面を介して提示することは、多くの場合、後述の場合と比較して相対的にセキュリティリスクが低減されているものと考えられる。一方で、患者から提示された二次元バーコードや URL 等のリンク先へのアクセス及びファイルのダウンロード等はセキュリティリスクが高いため、セキュリティリスクが限定的であることを医療機関が合理的に判断できる場合を除き、このようなアクセスやダウンロード等は行わないことが望ましい。
- ・ オンライン診療を実施する医師は、オンライン診療の研修等を通じて、セキュリティリスクに関する情報を適宜アップデートすること。
- ・ 医療機関が、オンライン診療を実施する際に、医療情報を取得する目的で外部の PHR 等の情報を取り扱うことが、医療情報システムに影響を与える場合は、「医療情報安全管理関連ガイドライン」に沿った対策を実施しなければならない。他方で、医療機関が、医療情報システムに影響を与えずに当該情を取り扱う場合には、セキュリティリスクについて医療機関と患者の間で合意を得た上で、オンライン診療を実施すること。

1－2) 医療機関が汎用サービスを用いる場合に特に留意すべき事項

医療機関が汎用サービスを用いる場合は、1－1)に加えて下記の事項を実施すること。

- ・ 意図しない三者通信を防ぐため、医療機関から患者側につなげることを徹底し、また通信の管理者権限を患者に委譲しないこと。
- ・ 医療機関又は医療機関から委託を受けた者は、汎用サービスのセキュリティポリシーを適宜確認し、患者の問い合わせに対応できるようにすること。
- ・ 個別の汎用サービスに内在するセキュリティリスクを理解し、必要な対策を講じる責任は医療機関にあり、委託を受けた者が存在する場合は、委託契約に基づき協力する責務が委託を受けた者に課されることを理解すること。
- ・ 端末立ち上げ時、パスワード認証や生体認証などを用いて操作者の認証を行うこと。

2) オンライン診療システム事業者が行うべき対策

※本項目は事業者向けの内容となるため、本書での記載は省略します。内容を確認する際は、最新版の「オンライン診療の適切な実施に関する指針」を参照してください。

3) 患者に実施を求めるべき内容

医療機関はオンライン診療を活用する際は、「診療計画」の作成時に患者に対して、オンライン診療を行う際のセキュリティおよびプライバシーのリスクを説明し、特に下記が遵守されるようにしなければならない。また、患者側が負うべき責任があることを明示しなければならない。

3－1) 基本事項

- ・ 使用するシステムに伴うリスクを把握すること。
- ・ オンライン診療を行う際は、使用するアプリケーション、OS が適宜アップデートされることを確認すること。
- ・ 医師側の了解なくビデオ通話を録音、録画、撮影してはならないこと。
- ・ 医師のアカウント等の情報を診療に関わりのない第三者に提供してはならないこと。
- ・ 医師との通信中は、第三者を参加させないこと。
- ・ 汎用サービスを使用する際は、患者側からは発信しないこと。

3－2) 医療情報システムに影響を及ぼしうるケース(医療機関が判断の上、患者に通知した場合に限る)

- ・ 原則、医療機関が求めない限り、あるいは指示に反して、チャット機能の利用やファイルの送付などは行わないこと。特に外部 URL への誘導を含むチャットはセキュリティリスクが高いため行わないこと

ii) 医療機関の具体的な対応

令和5年の総務省「医療・介護・健康データの利活用促進に関する調査研究(令和5年度)」の調査の結果、医療機関にて実際に実施されている具体的なセキュリティ対応を以下に示します。実際のオンライン診療の運用の参考にしてください。

■ ハードウェアのセキュリティ対策

使用されているハードウェアに関しては、OS のアップデートを通じてセキュリティを確保しています。最新のセキュリティパッチや機能改善を利用し、端末の安全性を保っています。

■ ウィルス対策ソフトの使用

オンライン診療アプリケーションがインストールされた PC 等の端末にはウィルス対策ソフトを導入し、外部からのサイバー攻撃やウィルス感染対策を実施しています。

■ ウィルス定義の定期的な更新

オンライン診療に使用される PC には、ウィルス対策ソフトがインストールされており、外部からのサイバー攻撃やウィルス感染に対する予防措置が講じられています。また、ウィルス対策ソフトは定期的に更新され、最新の脅威からシステムを保護するための最新の定義ファイルが適用されています。(PC 起動時に自動で再診の情報を取得する設定としています。)

■ 個人情報の取り扱いに関する注意

シンクヘルスでは、主に血糖値や血圧などの限られた情報のみを扱っています。また、その他のツールで情報共有を行う際は、万が一の情報漏洩に備え、必要以上の情報の入力を抑える配慮を行っています。

■ プライバシー保護のための措置

プライバシー保護を目的として特定の診察室でのみ実施されています。患者情報の漏洩リスクを最小限に抑え、診療中のプライバシーを確保しています。特に、通常の診療室から物理的な距離を確保した診療室にて実施されることもあります。公民館の個室を利用し、オンライン診療のコミュニケーション内容の外部への漏洩や患者の同意を得ている支援者以外の存在を排除する対応を実施しています。これは、一般的な外来診療室で実施されている近くの診療中の音声や、ネットワークを通じて外部に漏れるリスクに配慮した対応です。なお、医療機関側の環境のみならず、患者側の診療環境がプライバシーの確保に十分な環境でない場合、オンライン診療を中止する措置が取られることもあります。

■ 物理的な接続の回避

オンライン診療に使用されるハードウェアは、院内の電子カルテシステムと物理的に隔離されており、院内の他のシステムへの不正アクセスやデータ漏洩のリスクを適切に管理されシステム間のセキュリティリスクを最小限に抑えています。オンライン診療システム以外の用途では、ブラウザを使用しない、オンライン診療で必要なツールやアプリ以外はインストールしないなどの制限を設け端末を使用されることもあります。必要時以外は電子カルテもインターネットに接続しないようにするなどの対応が来られることもあります。

■ 情報漏洩リスクの最小化

スタッフが退職する際には、パスワードを変更するなど、情報漏洩を防ぐ措置を講じています。

■セキュアなシステムの選定

ビデオ通話ツールに CLINICS、クロン等のセキュリティ対策が整備されたシステムを選定し、患者情報の安全性を確保されています。特に個人情報を多く取り扱うツールの場合は、セキュアな環境が整備されたメディカルケアステーションシステム等のソフトウェアが利用されることがあります。

3.3.4 サイバーセキュリティに関連する各種情報

医療機関がサイバーセキュリティ対策を講じるにあたり、オンライン診療指針以外に以下に示す情報を参照し対策を講じることが推奨されます。

■総務省

国民のためのサイバーセキュリティサイトを通じて、一般ユーザーから組織まで幅広い層を対象にしたサイバーセキュリティに関する情報提供を行っています。ここでは、最新の脅威情報や対策方法、緊急時の対応策などが紹介されています。

国民のためのサイバーセキュリティサイト

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

■厚生労働省

医療分野に特化したサイバーセキュリティ対策のガイドラインや情報を提供しています。医療機関におけるサイバーセキュリティ攻撃を受けた際の連絡先、個人情報等が漏洩したおそれが発生した場合の対応、情報セキュリティ管理体制の構築や、医療情報の取り扱いに関する推奨事項が詳細に記載されています。

医療分野のサイバーセキュリティ対策について

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/cyber-security.html

【医療機関等がサイバーセキュリティ攻撃を受けた際の厚生労働省連絡先】

医政局特定医薬品開発支援・医療情報担当参事官室

TEL: 03-6812-7837

MAIL: igishitsu@mhlw.go.jp

※迷惑メール防止のため、メールアドレスの一部を変えています。

「×」を「@」に置き換えてください。

【サイバー攻撃等により個人情報等が漏洩したおそれが発生した場合】

サイバー攻撃等により、患者の個人情報を含む医療情報等、個人データの漏えい（漏えいのおそれを含む）等が発生した場合は、個人情報保護委員会への報告が必要です。詳細は、個人情報保護委員会の HP を確認してください。

個人情報保護委員会「漏洩等の対応とお役立ち資料」

https://www.ppc.go.jp/personalinfo/legal/leakAction/#leak_report

■日本医師会

医療機関向けにサイバーセキュリティ支援制度を設けており、医療機関がサイバーセキュリティ対策を効果的に実施できるよう支援しています。具体的な対策方法や事例、支援内容の詳細が紹介されています。

日本医師会サイバーセキュリティ支援制度

<https://www.med.or.jp/doctor/sys/cybersecurity/001566.html>

4 用語の解説

本参考書に含まれる用語は、オンライン診療に関する一般的な理解を深めることを目的としております。これらの用語の解説については、関連する法律、規制、またはガイドラインを定める各組織・団体の正式な見解に基づくべきであり、本文書に記載された内容が最終的な定義や解釈として扱われるものではありません。また、本用語集によって他の組織・団体の見解や方針との間に齟齬が生じることを意図するものではなく、あくまで参考情報として提供されるものです。用語に関する最新の情報や詳細については、各組織あるいは団体の発表する公式な資料や通知を合わせてご参照ください。

4.1 五十音順

アクセスログ	ネットワークやコンピュータの接続や操作の履歴のこと。
インターネットVPN	インターネットは、誰でも利用できるネットワークであるが、セキュリティを強化するために、特定のシステム間だけの閉域なネットワークを実現する仕組み。VPNとは「Virtual Private Network」の略であり、専用の仮想的な回線でつないで、安全なデータ通信を実現する仕組みである。
ウィルス対策	コンピュータが正常に作動することを妨げるコンピュータウィルスの侵入を防ぐことを示す。コンピュータウィルスは機密情報などのデータを盗み出したり、データを破壊することを目的として作成された悪質なプログラムである。ウィルスの侵入を防いでくれるソフトウェアを「ウィルス対策ソフト」という。
仮想化	サーバなどのハードウェア内のリソース(CPU、メモリ、ディスク)を物理的な構成にとらわれることなく、論理的に統合や分割できる技術のこと。
クライアント認証	「機能を使うことが許された本人」であることを確認すること。クライアント、つまりサーバと接続している機械(PCやモバイル端末)が、「サービスを使うことが許された特定の機械」であることを確認して、どの固体であるかを特定する、という機能である。
クラウドサービス	クラウドとは利用者がソフトウェアを持たなくても、インターネットを通してサービスを必要な特に利用できる仕組み。利用者は、オンプレミス(サーバ設置型)のように、設備やソフトウェアを保有しないで、インターネットを介してアプリケーションを利用することができる。
サーバ	クライアント(主にパソコンやモバイル端末)からの要求に対してサービスを提供するコンピュータ、またはアプリケーションのこと。サーバにはアプリケーションやデータが保存されている。クラウドの場合はインターネット上にサーバが設置されているが、オンプレミス(サーバ設置型)は自社内にサーバが設置されている。

生体認証	個人を認証する方式の一種で、指紋や声、筆跡といった生物個体を持つ特性を利用する仕組みを指す。個人の身体の特徴等を認証として使用するため、パスワード認証のように本人が忘れてしまう懸念がないことが特徴として挙げられる。
セキュリティポリシー	セキュリティに関する基本的な方針のこと。例えば、どの情報を誰に公開するかといった運用の方針のこと。これに従い、具体的なルールを設定することで、組織全体の整合性のとれたセキュリティを確保する。
多要素認証	利用者が本人を認証する際に、複数の要素を用いて確認することを指す。例えば、IDとパスワードの入力に加えて、指紋や筆跡などの生体情報の入力を組み合わせて認証する仕組みなどが想定される。
データセンタ	コンピュータやネットワーク機器を設置する場所のこと。一般の建物に比較して、耐震性があり自家発電などの電源設備や空調設備など、コンピュータにとって最適な設置環境を提供する。
バックアップ	システム異常などによるデータの破損に備えて、データ内容を別の記憶装置やメディアに保存すること。
汎用サービス	オンライン診療に限らず広く用いられる利用料が無料のサービスであって、視覚及び聴覚を用いる情報通信機器のシステム(ビデオ会議サービス等)を使用するもの。
ベンダ	製品を提供販売する会社のこと。本参考書では、主にオンライン診療のシステムを提供販売する会社を指す。
ユーザーカウント	システムを利用する人を一般的にユーザーと呼ぶが、ユーザーカウントは、そのユーザーに与えられたシステムの利用権限のこと。ユーザーカウントは、通常、ユーザー名称やパスワードによって登録する。

4.2 アルファベット順

BYOD	「Bring Your Own Device」の略。例えば、医師が個人で所有している情報端末(パソコンやスマートフォンなど)を病院などに持ち込んで、業務で利用すること。
HPKI	保健医療福祉分野の公開鍵基盤「Healthcare Public Key Infrastructure」の略で、インターネットを介して診療関連文書のやり取りを行う際、なりすましや改ざんを防止するために、適用される電子証明書。医療現場で公的資格の確認機能を有する電子署名や電子認証を行う基盤を指す。

IDS/IPS	IDSは「Intrusion Detection System」の略。コンピュータセキュリティシステムの1つで不正侵入検知システムと呼ばれ、システムやネットワークに対して外部から不正なアクセス等があった場合に、管理者への通知を行う。これに対してIPSは「Intrusion Prevention System」の略であり、不正侵入防止システムと呼ばれ、外部から不正なアクセス等があった場合に、管理者への通知だけでなく、アクセスの侵入を遮断する等のアクションを行う仕組みである。
IPsec+IKE	IPsecは「IP Security」の略。インターネットなどのネットワーク環境で、暗号通信を行う際のプロトコル(コンピュータ同士が通信をする際の、手順や規約などの約束事のこと)の1つ。IKEは「Internet Key Exchange」の略であり、IPsecで暗号化通信を行う際に先立って暗号化に使う鍵を交換するために利用されるプロトコルを指す。
IP-VPN	インターネットと同じIPで通信するネットワークを用いるが、通信事業者が単独で構築・運用する閉域IP網であるため、セキュリティの確保や品質制御などで優れている。
JPKI	「Japanese Public Key Infrastructure」の略。公的個人認証サービスを指し、インターネットを利用して申請・届出・登録などの手続きを行ったり、ポータルサイトにログインしたりする際に用いられる本人確認の手段(電子証明書の発行)を提供するサービスである。
OS	OSとは「Operating System」の略で、パソコン本体を動かし、周辺機器やアプリケーションなどを使用できるようにする基本的なソフトウェアのこと。OSがないとパソコンを動かすことができない。OSにはWindows、Android、MacOSやiOSなどがある。
PHR	「Personal Health Record」の略。医療機関ではなく、患者個人が自分自身の医療・健康情報を収集・保存し、それを活用する仕組みのこと。
TLS1.2	TLSは「Transport Layer Security」の略であり、インターネットなどのネットワーク上でやり取りする情報を暗号化して情報の漏洩等を防ぐ仕組みである。主な機能として「通信相手の認証」「通信内容の暗号化」「通信データの改ざんの検出」の3つがある。TLS1.2は2008年に発表されたバージョンである。

【タイトル】

遠隔医療モデル参考書－オンライン診療版－ 令和5年度改訂版

【作成】

遠隔医療モデル参考書－オンライン診療版－作成事務局

【発行年月】令和6年5月

※本モデル参考書は、令和5年度 総務省事業「医療・介護・健康データの活用促進に関する調査研究」(受託:株式会社 NTT データ経営研究所)において、本事業検討会の有識者のご助言を踏まえ、令和2年に公表した「遠隔医療モデル参考書」のオンライン診療版を改訂したものです。