基準等遵守の確認をするためのチェックリスト

「オンライン診療基準」及び「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 8 年 4 月一部改訂）」に準拠

確認日：

確認者：

		遵守／推奨	備考
(1) オンライン診療受診施設			
ⅰ オンライン診療受診施設は、対面診療が行われる場合と同程度に、清潔かつ安全でなければならない。 ⅱ プライバシーが保たれるよう、患者が物理的に外部から隔離される空間においてオンライン診療が行わなければならない。 具体的な取組 （　　）	□	遵守	
(2) 通信環境　（情報セキュリティ・プライバシー・利用端末）			
1) オンライン診療受診施設が行うべき対策			
ⅰ オンライン診療受診施設は、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、同意を得る。	□	遵守	• オンライン診療受診施設は、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。
1-1) 基本事項			
ⅰ オンライン診療受診施設は、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（※）、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。	□	遵守	※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。
当該確認に際して、オンライン診療受診施設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。	□	遵守	
ⅱ オンライン診療システムを用いる場合は、オンライン診療受診施設は 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。 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。	□	遵守	
ⅲ オンライン診療受診施設は、必要に応じてセキュリティソフトをインストールする。	□	遵守	

			遵守／推奨	備考
	iv 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。	□	推奨	
	v 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。	□	遵守	
	vi オンライン診療受診施設の職員は、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。	□	遵守	
	1-2)オンライン診療受診施設が汎用サービスを用いる場合に特に留意すべき事項（オンライン診療受診施設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）			
	i オンライン診療受診施設又はオンライン診療受診施設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。	□	遵守	
	ii 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オンライン診療受診施設にあることを理解する。	□	遵守	• 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。
	iii 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。	□	遵守	
	２） オンライン診療システム事業者が行うべき対策 ※オンライン診療受診施設の設置者又は管理・運営責任者は、下記を踏まえて、セキュリティリスク対策を講じること。			
	i オンライン診療システムを提供する事業者は、下記を備えたオンライン診療システムを構築し、下記２－１）の項目を満たすセキュリティ面で安全な状態を保つ。	□	遵守	
	ii オンライン診療システムをオンライン診療受診施設が導入する際、事業者は、オンライン診療受診施設に対して、オンライン診療受診施設が十分に理解できるまで、オンライン診療システムのセキュリティ等（※）に関する説明を行う（分かりやすい説明資料等を作成しオンライン診療受診施設に提示することが望ましい。）。	□	遵守	※患者、医療機関及びオンライン診療受診施設がシステムを利用する際の権利、義務、情報漏洩・不正アクセス等のセキュリティリスク、患者・医療機関・オンライン診療受診施設三者のセキュリティ対策の内容、患者への影響等
	2-1）基本事項			
	i オンライン診療受診施設に対して、オンライン診療受診施設が負う情報漏洩・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。	□	遵守	
	ii 事業者はオンライン診療受診施設に対して、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。	□	遵守	
	iii オンライン診療システムの中にビデオ会議システム等の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ついて、オンライン診療受診施設に明確に説明し、合意した責任分界点の範囲において責任を負う。	□	遵守	
	iv 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オンライン診療受診施設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。	□	遵守	

			遵守／推奨	備考
	v 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	• 2－2）に該当する場合を除く。 ※第三者機関に認証されることが望ましい
	vi システムの運用保守を行うオンライン診療受診施設の職員や事業者、クラウドサービス事業者のアクセス権限を管理する（※）。	□	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。またシステム運用監督者は退職者アカウントの削除など管理外になりやすい要素を重点的に監視すること。 ※第三者機関に認証されることが望ましい
	vii 不正アクセス防止措置を講じること（IDS/IPS を設置する等）。	□	遵守	※第三者機関に認証されることが望ましい
	viii 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。 ※第三者機関に認証されることが望ましい
	ix 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を定期的に促す機能。	□	遵守	※第三者機関に認証されることが望ましい
	x 信頼性の高い機関によって発行されたサーバー証明書を用いて、通信の暗号化（TLS1.3 以上、やむを得ず 1.2 を用いる場合は十分な暗号強度とするよう留意）を実施する。	□	遵守	※第三者機関に認証されることが望ましい
	xi オンライン診療時に、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。	□	推奨	※第三者機関に認証されることが望ましい
	xii 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。	□	遵守	※第三者機関に認証されることが望ましい
	xiii 使用するドメインの不適切な移管や再利用が行われないように留意する。	□	遵守	
	2-2）システム内で診療にかかる患者個人に関するデータを蓄積・残存する場合、2-1）に加えて「医療情報安全管理関連ガイドライン」に沿った対策を行うこと。			
	i オンライン診療受診施設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。	□	遵守	
	ii 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。	□	遵守	※第三者機関に認証されることが望ましい
	iii オンライン診療システムは、上記の 2-1）及び 2-2 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 Q 15001）、ISMS（JIS Q 27001 等）、ITSMS（JIS Q 20000-1 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

		遵守／推奨	備考
			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．その他オンライン診療に関連する事項			
(1)当該施設において、オンライン診療を提供する連携医療機関等の名称等の公表			
i　オンライン診療受診施設は、患者の選択に資するため当該施設において、オンライン診療を提供する連携医療機関の名称等を公表する。	□	遵守	
(2)遠隔で施設を管理等する場合			
i　通信機器の不具合や患者急変時等に、患者・オンライン診療を行う医師/医療機関・都道府県等が連絡する連絡先を提示し、速やかに対応できる体制を確保する。 速やかに対応できる体制の確保の具体的内容 （　　）	□	遵守	
(3)法人がオンライン診療受診施設を設置する場合			
i　設置者が法人の場合は、管理・運営責任者を定める必要がある。	□	遵守	