資料 1-2
改訂版（事務局案）

「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

(3) 通信環境（情報セキュリティ・プライバシー・利用端末）

考え方

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及び汎用サービス等を適切に選択・使用するために、個人情報及びプライバシーの保護に最大限配慮するとともに、使用するシステムに伴うリスク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。

※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
※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）医師が行うべき対策

医師は、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。医師は、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）共通事項

・オンライン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を示し、それに伴うセキュリティリスク等と対策および責任の所在について患者に説明し、合意を得ること。
・OS やソフトウェア等を適宜アップデートするとともに、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こと。
・汎用サービスを用いる場合は、医師のなりすまし防止のために顔写真付きの身分証を患者の求めに応じて示すこと（医師資格証を使用するのが望ましい。）。
・オンライン診療システムを用いる場合は、求めに応じて患者がいつでも医師の本人確認ができるようにすること。

・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いか確認すること。
・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。
・チャット機能やファイルの送付などを患者側に利用させる場合には、医師側（所属病院等の医療従事者、スタッフ等を含む）から、セキュリティリスクを勘案したうえで、チャット機能やファイルの送付などが可能な場合とその方法についてあらかじめ患者側に指示を行うこと。
・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。
・患者が入力した Personal Health Record(以下、PHR)をオンライン診療システム等を通じて診察に活用する際には、当該 PHR を管理する事業者との間で当該 PHR の安全管理に関する事項を確認すること。

１－２）医師が汎用サービスを用いる場合に特に留意すべき事項

医師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。

・医師側から患者側につなげることを徹底すること（第三者がオンライン診療に参加することを防ぐため。）。
・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。
・オンライン診療システムを用いる場合と異なり、個別の汎用サービスに内在するリスクを理解し、必要な対策を行う責任が専ら医師に発生するという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。
・汎用サービスがアドレスリストなど端末内の他のデータと連結しない設定とすること。

１－３）医師が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を用いる場合

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

ムを用いる時は、１－１）に加えて下記の事項を実施すること。

・医師は、オンライン診療システムにおいては、チャット機能やダウンロード機能を用いるリスクを踏まえて、原則使用しないこと（使用するシステム上、リスクが無害化されている場合を除く。）。
（オンライン診療システムにおいては、システム提供事業者がこれらの機能の使用に関して提供する情報を踏まえて利用を行う。）
・医師個人所有端末の業務利用（BYOD）については、原則禁止とすること。

２）オンライン診療システム事業者が行うべき対策

※医療機関の医療情報管理責任者は、下記を踏まえて、所属する医師が行うべきセキュリティリスク対策を講じること。

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、下記の項目を満たすセキュリティ面で安全な状態を保つこと。また、オンライン診療システム事業者は、平易で理解しやすい形で、患者および医師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、医師・患者双方のセキュリティ対策の内容、患者への影響等について、医師に対して説明すること（分かりやすい説明資料等を作成し医師に提示することが望ましい。）。

２－１）共通事項

・医師に対して、医師が負う情報漏洩・不正アクセス等のセキュリティリスクを明確に説明すること。
・オンライン診療システムの中に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。
・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。（＊）
・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（＊）（２－２）に該当する場合を除く。）。
・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(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を講じること(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ため、患者が医師の本人確認を行えるように、顔写真と医籍番号を常に確認できる状態とすること(例えば、JPKI を活用した認証や端末へのクライアント証明書の導入、ID/パスワードの設定、HPKI カード等)。(＊)
・アクセスログの保全措置(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促す機能。(＊)
・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(TLS1.2)を実施すること。(＊)
・特定の施設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。(＊)
・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。(＊)
・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すること。

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

オンライン診療システムが、医療情報システムを扱う端末で使用され、オンライン診療を行うことで、医療情報システムに影響を及ぼす可能性がある場合、２－１)に加えて医療情報安全管理関連ガイドラインを遵守すること。特に留意すべき点を例示として下記に示す。

・法的保存義務のある医療情報を保存するサーバーを国内法の執行が及ぶ場所に設置すること。(＊)
・医師(医療機関の医療情報管理責任者)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うこと。
・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。(＊)

また、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。第三者機関の認証としては以下のようなものが考えられる。

（例）プライバシーマーク（JIS Q15001）、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会の CS マークや ISMS クラウドセキュリティ認証（ISO27017）の取得　等

３）患者に実施を求めるべき内容

医師はオンライン診療を活用する際は、診療計画を作成時に患者にして、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）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。
・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、第三者に参加させないこと。
・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（医師が判断の上、患者に通知した場合に限る）

・原則、医師側が求めない限り、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。

３－３）対面診療の例外として初診でオンライン診療を用いる場合

・患者は、少なくとも一種類以上の顔写真付きの身分証明書を含む、二種類以上の身分証明書を用いて本人証明をすることが望ましいこと。