資料 1-3
現行版

「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（抄）

(3) 通信環境（情報セキュリティ・利用端末）

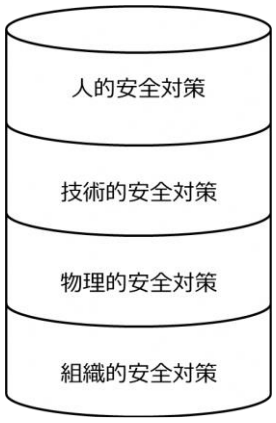
①考え方

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（汎用ビデオ電話サービス等も含む。）を適切に選択・使用するために、個人情報の保護に最大限配慮するとともに、情報セキュリティに関する対策を講じ、それらを患者・医師・オンライン診療システム提供事業者の三者で合意することが重要となる。本指針ではその整理を容易にするために、医療情報を保存しているシステムと１）接続（※）しない、２）接続する、と区分けをしたうえで、各々を利用する際に検討・考慮すべき事項を記載している。

（※） 接続とは、医療情報システムに対して、中間的なサーバーを設置して、一旦オンライン診療システムからの影響を遮断する等の対策（ネットワーク上の分離）を実施しておらず、保存されている医療情報にアクセス可能な状態を指す。

医師はオンライン診療システムを利用する際に、セキュリティリスクを十分に勘案し、患者に対して責任を負うこととなるが、オンライン診療システム提供事業者と専門性に応じた責任分担を行うことで、効果的な対策を行うよう努めること。なお、患者の行為により、セキュリティ事案や損害等が生じた場合に備えて、患者との間で責任の所在等についてあらかじめ合意しておくことが望ましい。

また、技術的安全対策のほか、人的、物理的、組織的安全対策を総合的に検討・実施する必要がある。技術的安全対策はこのうちの一要素にすぎず、他の安全対策とともに包括的な安全対策を行う必要がある。



守秘義務・罰則規定・セキュリティ教育・従事者の管理監督など

アクセス権限・利用者識別/認証・アクセスログ管理・データ/通信の暗号化脆弱性対策・ウィルス対策など

セキュリティ区画・入退室管理・盗難防止・紛失防止・施錠管理など

管理責任者・アクセス管理規定・業務委託契約・セキュリティポリシー・自己点検（監査）など

②遵守すべき事項

医師及び事業者は、次のような事項に留意すること。なお、当該事項を遵守していないシステムを使用する場合には、情報漏洩・不正アクセス等の一定のセキュリティリスクがあることを医師・患者双方が認識し、合意をした上で使用すること。

- 医師－患者関係において、医師は、オンライン診療システムを選択し利用する際に、セキュリティリスクを十分に勘案すること
- オンライン診療システム提供者（医療機関及びオンライン診療システム提供事業者を指す。以下同じ。）は、本指針に定める情報セキュリティに関するルールを厳守したシステムを構築し、常にその状態を保つこと
- 事業者は患者および医師がシステムを利用する際の権利、義務、リスク等を明示したうえで、平易で理解しやすい形で、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、説明すること（説明資料等を作成し医師に提示することが望ましい。）。

なお、医師は汎用ビデオ電話サービス等の利用にあたり、当該サービス等のセキュリティやプライバシーに関する規約等を確認し、セキュリティ対策の内容、セキュリティ事案や損害発生時の責任の所在、データ保存の有無や保存内容等について理解し、患者と合意の上で使用する必要があることに留意する。

以上を踏まえた上で、オンライン診療の情報セキュリティ対策については、次のとおり整理する。なお、本指針を踏まえた「オンライン診療における情報セキュリティ対策の例」を巻末に参考として掲載しているので必要に応じ参照されたい。

１）医療情報システムとの接続を行わないケース

本ケースでは、電子カルテシステム等の医療情報システムに、オンライン診療システム、医師側端末及び患者側端末（以下「オンライン診療システム等」という。）は接続せず、原則として、オンライン診療システム等を通じた医療情報の保存は行わない。ただし、患者の合意の下、患者端末に本人の情報を患者の自己責任で保存する場合には、この限りではない。

ｉ）患者側端末

患者側端末は、患者個人が契約するスマートフォン等による利用が想定されるが、その利用やセキュリティ対策の状況が多様であることから、患

者側端末で対策が実施されていることを前提とせず、オンライン診療システム提供者側で万全のセキュリティ対策を講じることが必要である。患者側端末では特に情報漏えい等に注意すべきであるが、患者が、自らの判断で、自らの責任において、心身の状態に関する情報を端末に自ら保存することは、本指針で禁止するものではない。ただし、患者側が、医師側の了承なくビデオ通話を録画あるいは撮影すること厳しく禁止するべきであり、オンライン診療システム提供者も配慮すべきである。

ⅱ）医師側端末

オンライン診療システム提供者は、医師側端末においては、特に不正な利用者よるアクセスや情報漏えいのリスク等を念頭におくこと。なお、医師個人が所有端末の業務利用（BYOD）を行う場合には、これらに対する対策が適切に実施されていることを定期的に確認するよう運用規則等で定めることが必要である（確認結果を監査等向けに開示可能にしておくことが望ましい。）。

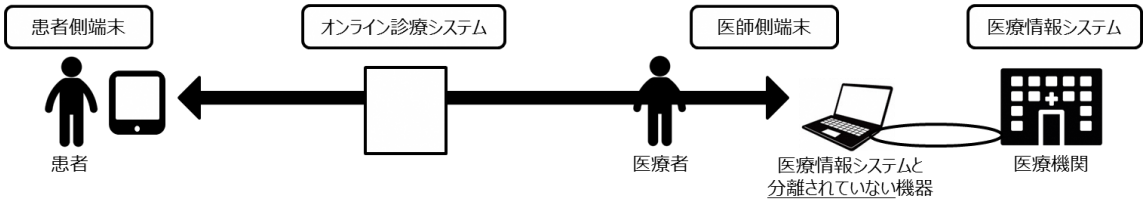
ⅲ）ネットワーク（オンライン診療を行う際のネットワークは事前に特定されているべきなのか。）

医師及び患者から適切なオンライン診療システムにアクセスされていることを担保できる状態にしていること。また、ネットワーク機器への不正アクセスを防止するため、管理者権限の設定や適切な認証、また通信の暗号化等を実施することが必要である。

なお、不特定多数の者が利用可能な公衆無線 LAN については、緊急時や他の手段がなくやむを得ない場合を除き使用しない。

２）医療情報システムと接続するケース

本ケースは、医療情報システムにオンライン診療システム等が接続する場合及びオンライン診療システム等自体に医療情報を保存する場合が該当する。一方、オンライン診療システム等と医療情報システムが「ネットワーク分離されていること」（⇨一般の医師とっては不明瞭）等により、医療情報システムがオンライン診療システム等の影響を直接受けない場合には、医療情報システムの情報を参照してオンライン診療を行っていた場合でも、１）のケースとして取り扱うことが適当である。



医療機関がオンライン診療システムと電子カルテシステム等を接続し、医師がシステム内の医療情報を確認しながら診療を実施する場合や、患者側に検査結果等を表示しながら診療を行う場合は、医療情報安全管理関連ガイドラインに沿った対策を行うことが必要である。

こうしたケースでは、例えば、

- 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
- 医師個人所有端末の業務利用（BYOD）については、原則禁止とされていること
- 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が及ぶ場所に設置すること

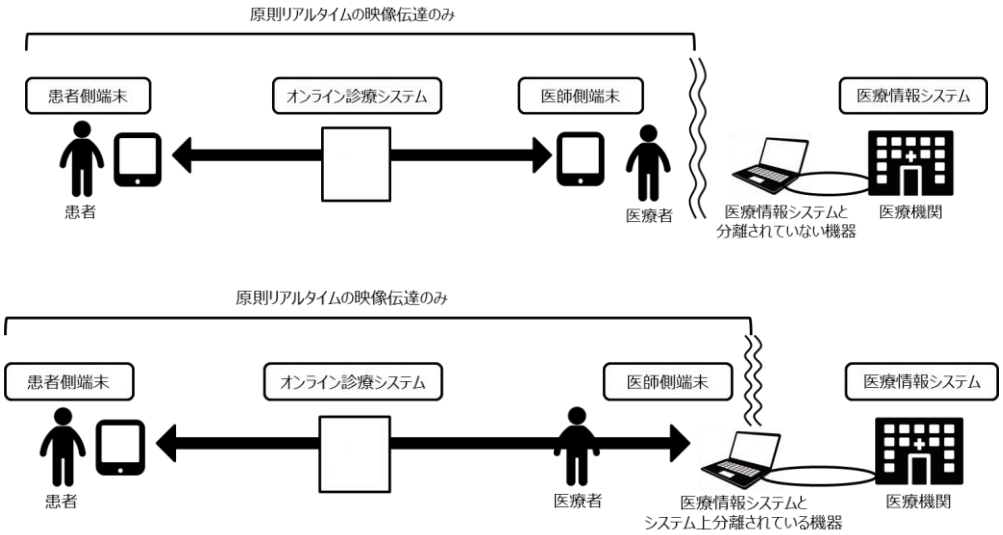
等が留意点としてあげられる。

なお、オンライン診療における患者側端末については、医療情報安全管理関連ガイドラインにおいて取扱いが明確となっていないが、患者側の端末を通じた医療情報システムへの不正アクセス等を防止する観点から、オンライン診療システムの機能として、患者側端末を医療情報システムと接続させないような措置を講ずる。この場合の患者個人所有端末の使用に当たっては、１）と同様の対策を講ずることが必要である。

また、オンライン診療に際し、医療機関側が管理する医療機器を患者側に貸与し、医療情報システムにデータを送る場合は、医療機関内に設置された医療機器と同等とみなし、当該貸与された医療機器を含め医療情報安全管理関連ガイドラインを適用する。

（参考）オンライン診療における情報セキュリティ対策の例

１）医療情報システムとの接続を行わないケース



脅威として想定される、盗聴・情報漏えい、システム等への不正アクセス・妨害、データの改変・消失等の脅威を未然に防ぐためには、オンライン診療全体を通じたリスク分析を行い、最低限、以下のⅰ）～ⅳ）に示す技術的対策を実施する必要がある。また、物理的対策として、システムや端末の盗難防止や覗き見の防止等を図るとともに、これらの対策を実効的なものとするため、組織的対策として、システムの管理者の設定や運用管理規則の策定・適用等の取組を行い、人的対策として、医師向けの研修等を実施することが必要である。なお、オンライン診療システム提供者が電気通信事業者とならない場合においても、個人情報保護及び通信の秘密保護に最大限配慮すること。（後述の２）においても同様）

ⅰ）患者側端末

オンライン診療システム提供者は、

- オンライン診療システムへの不正アクセスを防止するため、患者側端末において適切な本人確認（認証）を実施すること（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/パスワードの設定等）
- 情報漏えいのリスクを軽減する観点から、端末内にデータを残さないことをオンライン診療システムの機能として実装すること。

また、

- 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

を併せて提供することが望ましい。

ⅱ）オンライン診療システム

オンライン診療システム提供者は、その運用に当たり、

- 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
- 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 カード等により複数要素の認証を実施することが望ましい。）
- 不正アクセス防止措置（IDS/IPS を設置することが望ましい。）
- アクセスログの保全措置（ログ監視を実施することが望ましい。）
- ウィルス対策や OS・ソフトウェアのアップデート

を実施すること。

ただし、アクセスログの保存措置について、システム等の機能として実装していない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作日時、操作者、操作内容等）を管理する方法によることも考えられる。

また、１）においては、医療機関内の他の医療情報を保存しているシステムへの侵入ができないようにネットワークを構成するものとする。また、医師側がオンライン診療システムにデータを保存する場合は、医療情報システムとして、２）に掲げる対策を講じるものとする。

ⅲ）医師側の端末

不正な利用者によるオンライン診療システムへのアクセスを防止するため、オンライン診療システム提供者は、

- 不正な利用者によるオンライン診療システムへのアクセスを防止するため、医師側の端末における適切な本人確認（認証）を実施すること（例えば、ID/パスワードの設定、HPKI を活用した認証や端末へのクライアント証明書の導入等）
- 情報漏えいのリスクを軽減する観点から端末内にデータを残さないこと

をオンライン診療システムの機能として実装すること。また、

- 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適切に促す機能

を併せて提供することが望ましい。

ⅳ）ネットワーク

医師及び患者から適切なオンライン診療システムにアクセスされていることを担保するため、オンライン診療システム提供者は、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。

また、ネットワーク機器への不正アクセスを防止するため、管理者権限の設定や適切な認証を実施すること。

なお、不特定多数の者が利用可能な公衆無線 LAN については、緊急時や他の手段がなくやむを得ない場合を除き使用しないこと。

加えて、患者がデータやテキストメッセージ等をスマートフォン等の端末を通じ医師に送り、オンライン診療で活用する場合は、ウィルスの侵入および不正アクセス防止のために IDS/IPS を設置すること等により、患者から送られてきたデータに対するファイル検疫・隔離等のウィルスチェックの徹底を図り、特にウィルス感染対策や脆弱性攻撃への対策等に留意すること。また、医師側は、情報漏洩リスクを最小限にするため、データを端末に残さないよう徹底すること。

一方、医師側のデータを患者側に転送し使用する場合には、患者とセキュリティリスクについて事前に合意を行い、責任の所在を明らかにした上で行うこと。

２）医療情報システムと接続するケース

医療機関がオンライン診療システムと電子カルテシステム等を接続し、医師がシステム内の医療情報を確認しながら診療を実施する場合や、患者側に検査結果等を表示しながら診療を行う場合は、医療情報安全管理関連ガイドラインに沿った対策を行うこと。

こうしたケースでは、例えば、

- 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
- 医師個人所有端末の業務利用（BYOD）については、原則禁止とされていること
- 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が及ぶ場所に設置すること

等が留意点としてあげられる。

なお、オンライン診療における患者側の端末については、医療情報安全管理関連ガイドラインにおいて取扱いが明確となっていないが、患者側の端末を通じた医療情報システムへの不正アクセス等を防止する観点から、オンライン診療システムの機能として、患者側端末を医療情報システムと明確に分離することを原則とする。この場合の患者個人所有端末の使用に当たっては、１）と同様の対策を講ずることが必要である。