整理番号

項番	分類	項目
1	オンライン診療システム事業者の説明責任	オンライン診療システム事業者は、オンライン診療システムが有する機能、ならびに特に医療情報システムと接続可能な機能を有するかについて、ユーザーである医師や患者に対して説明できるように文書化しておくこと。
2		オンライン診療システム事業者は、提供するオンライン診療システムの環境のハードウェア機器、ソフトウェア、ネットワークの構成図及びシステム要件、更新仕様等を説明した資料を作成すること。仮想化技術を用いオンライン診療システムに供する場合には、論理的に区分管理を行えることを保証できる措置を講じた上で説明資料を作成すること。
3		オンライン診療システム事業者は、医療機関等が患者等からの求めに対する説明責任、管理責任等に応じるために、オンライン診療システム事業者として負う責任の範囲、役割について、障害等が生じた場合の稼動を保証する範囲も含め、医療機関等に対し明確に提示できること。
4		オンライン診療システム事業者は、医師がオンライン診療システムを利用するにあたって、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。
5		オンライン診療システム事業者は、オンライン診療システムを利用するにあたって、発生するセキュリティリスクについて明確にし、ユーザーである医師や患者に対して説明できるように文書化しておくこと。
6		オンライン診療システム事業者は、オンライン診療システムを利用するにあたって、発生するプライバシーの侵害リスクについて明確にし、ユーザーである医師や患者に対して説明できるように文書化しておくこと。
7		オンライン診療システム事業者は、オンライン診療システムの利用の際に、緊急時を除き公衆無線LANへの接続を行わないことを医師や患者に説明すること。
8		オンライン診療システム事業者は、提供するオンライン診療システムの中に汎用システム及び外部サービスを組み込んだ場合においても、提供したシステム全般に対するセキュリティの責任を負うことし、ユーザーである医師や患者に対する契約の中で明記を行うこと。
9		オンライン診療システム事業者は、汎用システム及び外部サービスの安全管理策及びサービスレベルが十分であることを確認し、サービスの利用を決定、契約を行うこと。
10		オンライン診療システム事業者は、汎用システム及び外部サービスも含め、オンライン診療システムの提供状況、運用、維持について定期的に検証すること。汎用システム及び外部サービスによる状況については事前・事後報告を義務づけ、報告内容を確認すること。
11		オンライン診療システム事業者は、医師に対して十分な説明が可能となるように、提供するオンライン診療システムに関する取扱い手順書等の説明書を提供できるようにし、医師が容易にアクセスできるような環境で提供を行うこと。
12		オンライン診療システム事業者は、医師がオンライン診療システムを利用するにあたり、必要となるシステム環境（通信環境、OS、ソフトウェア、ブラウザ等）について、医師が容易にアクセスできるような環境で提供を行うこと。
13		オンライン診療システム事業者は、医師に対して利用規約等で医師が実施すべき事項を示すだけでなく、起こりうるリスク等の注意点に関して、別途医師が理解しやすいような説明を提供すること。
14	オンライン診療システムとして備えるべき事項	診療にかかる患者個人に関するデータに関して、医療情報システムと接続する場合を除き、オンライン診療システム（サーバー、端末等）に蓄積・残存を行わないこと。
15		診療に関する予約を行う際に、医師への伝達事項が存在する場合があるが、診療終了時に診療にかかる患者の情報に関しては、医療情報システム等に転記等行い、オンライン診療システムからは削除されること。
16		オンライン診療システムにおいて、患者側で第三者をビデオ通話に招待する機能を有しないこと。
17		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。

整理番号

項番	分類	項目
18		オンライン問診等、診療にかかる患者個人に関するデータを扱うシステムに関しては、医療情報安全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。
19		オンライン診療システム事業者は、オンライン診療が中断することのないようなサーバ機器、アーキテクチャを確保した上で、システムを提供すること。
20	オンライン診療システムの利用環境に対する確認	オンライン診療システムを利用する環境は、意図されない動作を行う不正プログラム等を排除するために、ウィルス対策ソフトを導入すること。
21		オンライン診療システムを利用する環境は、脆弱性への対応を可能とするために、OSのアップデート並びに利用するソフトウェアに対するアップデートを適切に実施すること。
22		オンライン診療システムを利用する際に環境をチェックし、OS並びにソフトウェアのアップデートが適切に実施されていない場合、アップデートを促す機能を備えていること。
23		オンライン診療利用時に、端末内の他のデータに意図しないアクセスができないような機能を備えることが望ましい。
24	オンライン診療システム事業者における組織的対策	オンライン診療システム事業者は、自社における個人情報保護指針、プライバシーポリシー等を医療機関等に対し明確に提示できること。
25		オンライン診療システム事業者は、情報セキュリティに関する基本方針や運用管理規程(ルール)、情報セキュリティポリシーを策定すること。
26		オンライン診療システム事業者は、プライバシーマーク認定(保健医療福祉分野)、ISMS認証、ITSMS認証、情報セキュリティ監査告書の取得、クラウドセキュリティ推進協議会CSマーク、ISMSクラウドセキュリティ認証等の公正な第三者の認証等を取得していることが望ましい。
27		オンライン診療システム事業者は、システム、組織体制、運用等に関する監査の方針、内容等について定め、定期的に監査を行い、監査実施について記録すること。
28		オンライン診療システム事業者は、個人情報保護対応策、オンライン診療システムに係る守秘義務、守秘義務に違反した場合にはペナルティが課されることを含めた利用規約や契約とすること。
29		オンライン診療システム事業者は、以下の責任者を設置し、任命・解任等のルールを策定すること。 (1)オンライン診療システムの提供についての管理責任を有する責任者 (2)医療情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者） (3)オンライン診療システムの提供に係る医療情報システムの運用に関する事務を統括する責任者
30		オンライン診療システム事業者は、下記の体制（再委託に関する情報を含む）について構築し、責任者等を含め体制図等として策定すること。 (1)情報セキュリティポリシーの遵守を担保する組織体制 (2)オンライン診療システムの提供に係る体制（保守体制、問合せ窓口、障害時保守体制、緊急時の対応体制等） (3)医療機関等の管理者からの一元化された医療機関等からの問合せ窓口ならびに受付時間帯等
31	オンライン診療システム事業者における人的対策	オンライン診療システム事業者における、雇用契約または服務規程等には従業員（委託契約員と派遣職員を含む）の守秘義務に関する内容や不正に情報を扱った場合の罰則（懲戒手続など）を含むこととし、契約時には秘密保持契約に署名を行うこと。違反した場合は適切なペナルティを課すなどの内容を服務規定に定めること。
32		オンライン診療システム事業者は、個人情報保護ポリシー及び個人情報の安全管理（退職時や契約終了以降の守秘義務も含む）に関する教育･訓練を、従業員（委託契約員と派遣職員を含む）に対して、就業開始時及び就業後の新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。

整理番号

項番	分類	項目
33		オンライン診療システム事業者は、従業員（委託契約員と派遣職員を含む）が退職した場合、管理していた個人情報及び情報資産の全てについて返却するとともに、就業中に扱った情報や知り得た情報に関する守秘義務についても服務規程等に含め、署名すること。また、システム管理者は返却確認を行うこと。
34		オンライン診療システム事業者は、従業員（委託契約員と派遣職員を含む）の退職時には、確実に職員証・名札等を回収･廃棄する、当該作業者IDを利用停止等、職員証、作業者IDの厳密な発行及び失効管理を行うこと。
35		オンライン診療システム事業者の情報管理については、従業員（委託契約員と派遣職員を含む）及び委託先に対して教育を行い、教育･訓練の実施状況や、守秘義務等への対応状況等に関する資料を用意しておくこと。
36		オンライン診療システム事業者の従業員（委託契約員と派遣職員を含む）による安全管理策違反の疑いが発生した際には、ただちにシステムへのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。
37		オンライン診療システム事業者において、委託先には自社と同等の個人情報保護方針を遵守させる守秘義務があることを確認し、委託契約を行うこと。
38	オンライン診療システム事業者における物理的対策	オンライン診療システム事業者は、オンライン診療システムに供する媒体及び機器等の設置場所等の情報セキュリティ境界について、施錠管理を行うこと。
39		オンライン診療システム事業者は、オンライン診療システムに供する媒体及び機器等を格納するキャビネット等について、施錠管理を行うこと。
40		オンライン診療システム事業者は、オンライン診療システムに供する媒体及び機器の設置場所、運用･保守端末等を設置している区域について、以下の運用管理規程(ルール)等を規定し、実施すること。 (1)設置場所、区画の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、予め届け出を行い、許可された者のみが入退できるように制限する (2)有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用する (3)設置場所、区画への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定が行う (4)職員の業務に応じて設置場所、区画に滞在できる時間を指定する (5)設置場所、区画への不明者の入退を発見するために、入退者に顔写真入りの職員証・名札等の着用を義務付け、職員で無い者を識別した際には声掛け等を行い、身分を確認する (6)職員証・名札等を紛失あるいは不正利用された疑いがあった際には、ただちに管理者に連絡する (7)設置場所、区画には、監視カメラ等を設置し、その記録を保存、状況を確認することで、不正な入退者がないことを確認する (8)設置場所、区画には、業務遂行に関係のない個人的所有物の持ち込みを制限する (9)設置場所、区画には、オンライン診療システム継続に不必要なものは置かない (10)設置場所、区画への入退状況の管理（入退記録のレビュー含む）は定期的に行う (11)設置場所、区画での作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録し、定期的に検証の上、不正な行為、システムの異常等を検出する

整理番号

項番	分類	項目
41	オンライン診療システム事業者における通信回線での対策	オンライン診療システム事業者は、オンライン診療システムに関係する通信に対し、起点、終点、経路等も対象とし、適切な技術(専用線、IP-VPN、Ipsec、プロトコルを限定し高セキュリティ型で設定したTLS1.2)を使用していることを明らかにすると共に、オンライン診療システム事業者として負う責任の範囲、役割を明示できること。(例：ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関する役割等)
42		オンライン診療システム事業者は、オンライン診療が中断することのないように通信回線帯域を確保し、回線の管理、品質等に対するオンライン診療システム事業者の責任の範囲、役割等について、明示できること。
43		オンライン診療システムを利用する通信路については、最低でも信頼性の高い機関が発行したサーバー証明書を用いたTLS1.2による通信の暗号化を行うこととし、TLS の設定はサーバー/クライアントともに、IPAより公開されている「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行うこと。
44		特定施設に継続的に接続する場合の通信路については、特定施設の識別を確実なものとするために、IP-VPNやIPsec＋IKEによる接続を行うこと。 その際、下記の必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行うこと。 (1)アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐため、接続時にVPN装置間で相互に認証を行う (2)認証で電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとし、暗号鍵、ルート証明書等、安全に運用する (3)傍受、リプレイ等のリスクを最小限に抑えるために、適切な暗号技術を利用する (4)インターネット上のトラフィックがVPNチャンネルに混入しないように、インタフェース間において直接の経路を設定しない (5)複数の医師の間で情報が混同するリスクを避けるため、オンライン診療時にVPNチャンネルを構築する等の対策を実施する
45		オンライン診療システムにおいて、ソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施すること。
46		医療機関等の施設内のルータ、端末等の経路設定によりオンライン診療システムにおいてセッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃がされないよう、注意喚起を行うこと。
47		オンライン診療システム事業者は、オンライン診療システムにおいて、端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができること。
48		オンライン診療システムにおいて、ネットワーク機器及びサーバー、端末の利用していないネットワークポートへの物理的な接続を制限すること。
49		オンライン診療システムにおいて、SSL-VPNは、原則として使用しないこと。
50		オンライン診療システムにおいて、外部サービスを利用する場合は下記サービスに限定することが望ましい。 (1)外部からの稼働監視･遠隔保守 (2)セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード (3)オペレーティングシステム及び利用アプリケーションのセキュリティパッチ等のダウンロード (4)ファイアウォール、IDS／IPS などのセキュリティ機器に対する不正アクセス監視 (5)時刻同期のための時刻配信サーバー

整理番号

項番	分類	項目
51	オンライン診療システム事業者における外部からの攻撃への対策	オンライン診療システム事業者は、提供するオンライン診療システムの環境の脆弱性に関する情報について、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得・確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。
52		オンライン診療システム事業者は、提供するオンライン診療システムへの外部からの悪意ある侵入を防ぐために、ファイアウォール並びにIDS／IPS、WAF等を組み合わせ、不正な通信が行われないための対策を施していること。
53		オンライン診療システム事業者は、侵入検知システム等が、常に最新の攻撃･不正アクセスに対応可能なように、シグネチャ･検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。
54		オンライン診療システム事業者は、侵入検知システム等自身が攻撃･不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施すること。
55		オンライン診療システム事業者は、セキュリティゲートウェイ等において、不正なIPアドレスを持つトラフィックが通過できないように設定すること。
56		オンライン診療システム事業者は、オンライン診療システムにおけるホスティングの利用時等、ネットワーク境界にオンライン診療システム事業者による装置を設置できない場合は、オンライン診療システムを提供する個々の情報処理装置に対して、外部からの攻撃等の対策を行うこと。
57		オンライン診療システム事業者は、不正･不審なトラフィックが、提供するオンライン診療システムの環境上における内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視すること。
58		オンライン診療システム事業者は、緊急度の高い攻撃･不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定を行っていること。
59		オンライン診療システム事業者は、提供するオンライン診療システムの環境（サーバー、プラットフォーム、データベース、端末等）に対して、ウイルスやマルウェア等の混入が生じないための手順を策定し、これに則って構築すること。
60		オンライン診療システム事業者は、オンライン診療システムにおける、ウイルスやマルウェア等の対策ソフトウェアにおいて次の設定を行うこと。 (1)定義ファイル、スキャンエンジン常に最新のものにするために自動アップデート又は十分な頻度による手動での更新 (2)リアルタイムスキャン (3)リスク評価の結果として必要であれば定期的にスキャンを実施 (4)媒体及び機器へのデータ書き出し・読み込み時におけるオンデマンドスキャン (5)管理者以外による設定変更やアンインストールの禁止
61		オンライン診療システム事業者は、オンライン診療システムがウイルス等による攻撃を受けた場合に、オンライン診療システム提供に係る影響について速やかに周知し、利用者に必要な対応等を求めること。
62	オンライン診療システム事業者におけるアクセス制御	オンライン診療時に、意図しないユーザーに対しても内容が共有されることが無いように、アクセス制御を確実に行える仕組みとすること。
63		オンライン診療システムにおいて、利用者のなりすまし等を防止するための認証を行うこと。
64		オンライン診療システムにおいて、認証により利用者を特定し権限を確認し、利用者種別ごとにアクセス権限･範囲等のアクセス制御が可能な機能を含め、与えられた権限外の情報や権限外の操作画面を表示しない等の制御を行うこと。

整理番号

項番	分類	項目
65		オンライン診療システム事業者は、医療情報システムの利用者を特定し識別できるように、アカウントの発行を行うこと（利用者には、医療機関等においてサービスを利用する者のほか、医療情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含め、複数の利用者によるIDの共同利用は行わないこと。
66		オンライン診療システムにおいて、医療情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行うこと。その際、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。
67		オンライン診療システムにおいて、利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準（パスワードポリシー）を策定し、これに基づく運用を行うこと。
68		オンライン診療システムでは、患者がいつでも医師の本人確認を行うことができるように、医師の本人情報、顔写真、医籍番号、身分証等について登録を行える機能を有すること（医師の本人確認を行う方法例として、医師資格証・HPKIカードとの連携等があげられる）。
69		医師がオンライン診療システムを利用する端末を立ち上げる際は、本人確認を実施しなければならず、ID／パスワードや生体認証等の認証を実施すること。
70		医師がオンライン診療システムを利用する場合は、本人確認を実施しなければならず、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。
71		オンライン診療システム事業者は、システムの運用保守を行う作業者のアクセス権限の管理を行い、その認証については、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。
72		オンライン診療システムにおいて、パスワードには十分な安全性を満たす有効期間を設定し、定期的な変更を強制すること。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、オンライン診療システム提供側から患者等に対して定期的なパスワードの変更を要求しないこと。
73		オンライン診療システムにおいて、利用者のパスワードは、十分な強度を持ったハッシュ値での保存を行う等、暗号化して、パスワードを容易に復元できない形で情報を保管すること。また、一般の作業者による閲覧を制限すること。
74		オンライン診療システムにおいて、利用者がIDやパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行うこと。また、緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定すること。
75		オンライン診療システムにおいて、パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知すること。
76		オンライン診療システムにおいて、パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じること。
77		オンライン診療システム事業者におけるオンライン診療システムでの利用者の認証に際して、何らかの物理的な媒体･身体情報等を必要とする場合に、例外的にそれらの媒体及び機器等がなくても一時的に認証するための代替的手段･手順を事前に定め、本来の利用者の認証方法による場合とのリスクの差を最小にすること。
78		オンライン診療システムにおいて、認証に際してID及びパスワードによらない場合でも、ID及びパスワードに関する対策と同等以上の安全性を確保すること。

整理番号

項番	分類	項目
79		オンライン診療システムにおいて、複数要素認証が行えず、代替的手段･手順により医療情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理すること。
80		オンライン診療システムにおいて、医療情報システムのサーバー機器等への同時ログオンユーザ数（OSアカウント等）に適切な上限を設けること。
81	オンライン診療システム事業者におけるログに関する事項	オンライン診療システム事業者は、提供するオンライン診療システムの環境（サーバー、プラットフォーム、データベース、端末等）のログを取得し、保管すること。 (1)利用者の利用状況の記録（診療した事実の証跡） (2)利用者又は開発者等の活動、機器で発生したイベント、システム障害、システム使用状況等を記録したログ (3)システム運用状況の記録（システム及びサービス設定ファイル等の複製、更新及び利用時等） (4)侵入検知、例外処理、情報セキュリティ事象の記録（事後処理に必要な項目が含まれていること）
82		ログには医師が説明責任を果たすための情報（ID、時刻、時間、対象（情報主体単位）等）を含めること。
83		オンライン診療システム事業者は、ログ上の時刻の信頼性を確保するために、オンライン診療システムが提供する環境におけるハードウェア機器（サーバー、ネットワーク機器等）の時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次以上の頻度で行うこと。また、定期的に時刻が同期していることを検証すること。
84		保管したアクセスログが改ざん等されないようにオンライン診療システム事業者は、ログの定期的なレビューや検証を行い、不正な行為、提供する環境の異常等がないことを確認すること。
85		オンライン診療システム事業者は、ログ情報を不正なアクセスから適切に保護するため、保存方法について以下の管理策を適用すること。 (1)不正なアクセスを防止のため、ログデータにアクセスする作業者及び操作を制限 (2)容量超過によりログが取得できない事態を避けるため、ログサーバーの記憶容量を常時監視し、媒体及び機器への書き出し、容量の増強等の対策の実施 (3)ログデータに対する不正な改ざん及び削除行為に対して、暗号化あるいは定期的に追記不能な媒体及び機器への記録を行う等、検出･防止策の実施
86		オンライン診療システム事業者は、監査実施について記録し、当該記録の保存･管理方法を、医療機関等に対し明確に提示できること。
87		オンライン診療システムにおける監査ログに記録する事項としては次のようなものが考えられる。 (1)作業者情報（作業者ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元IPアドレス） (2)ファイル及びデータへのアクセス、変更、削除記録（作業者ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） (3)データベース操作記録（作業者ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元IPアドレス、設定変更時にはその内容） (4)セキュリティパッチの適用作業（作業者ID、変更されたファイル） 保守において実施した操作結果 (5)特権操作（特権取得者ID、特権取得の可否、利用時刻及び時間、実行作業内容） (6)システム起動、停止イベント (7)ログ取得機能の開始、終了イベント (8)外部デバイスの取り外し (9)IDS･IPS等の情報セキュリティ装置のイベントログ (10)サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）

整理番号

項番	分類	項目
88	オンライン診療システム事業者におけるシステム構築・提供時の対策	オンライン診療システムにおいて提供する環境のアプリケーションは、オンライン診療システム事業者が開発したアプリケーションを用いること。また、外部事業者が開発したアプリケーションを用いる場合、事前に安全性を十分検証した上で用いること。
89		オンライン診療システム事業者は、ソフトウェア開発を行う際に、ソフトウェア障害の影響を避けるため、以下の対策を行うこと。 (1)不正なソフトウェアの書き換えリスクを避けるため、ソフトウェアに対する改ざん防止、検知策（ソースコードレベルでの検証）を実施し、十分な試験を行うこと。 (2)アプリケーションの安全性診断は提供しているオンライン診療システムに対して直接実施せず、別途、試験環境を用意して行うこと。
90		オンライン診療システム事業者は、オンライン診療システムにおいて、不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）、環境種別（ハードウェア、プラットフォーム、アプリケーション等）による特定の脆弱性検出を含む安全性診断を行い、その結果に基づいて対策を実施すること。
91		オンライン診療システム事業者は、提供するオンライン診療システムの環境のハードウェア等に接続できる媒体及び機器の種別及びソフトウェアを限定するため、以下の対策を実施すること。 (1)管理者以外はソフトウェアやデバイスドライバのインストールやアンインストールを不可能とする (2)不要なソフトウェアやドライバがインストールされていた場合は削除する (3)不要なデバイスドライバが追加されていないことを定期的に検証する
92	オンライン診療システム事業者における運用・保守時の対策	オンライン診療システム事業者は、オンライン診療システムにおいて、定期的にバックアップを行うこと。
93		オンライン診療システム事業者は、オンライン診療システムのハードウェア機器等は製造元または供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。
94		オンライン診療システム事業者は、オンライン診療システムの保守業務を行う前に、保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。
95		オンライン診療システム事業者は、オンライン診療システムの保守業務を行う前に、セキュリティパッチ適用、設定変更等の適用前にセキュリティパッチ適用、設定変更等が改ざんされていないこと及び有効性を検証すること。
96		オンライン診療システム事業者は、オンライン診療システムの保守業務を行う際に、事前に周知すること。
97		オンライン診療システム事業者は、オンライン診療システムの保守業務を行った後、定期的なチェックを行うこと。
98		オンライン診療システム事業者は、オンライン診療システムの運用･保守端末等に対し、運用中の画面が運用者以外の者の視野に入らないよう、覗き見対策のシートを貼る等の対策を行うこと。
99		オンライン診療システム事業者は、オンライン診療システムの運用･保守端末等に、盗難防止用チェーンを設置すること。
100		オンライン診療システム事業者は、オンライン診療システムの運用･保守端末等に、クリアスクリーン等の情報漏洩防止策を講じること。
101		オンライン診療システム事業者は、オンライン診療システムにおいて、運用･保守のための作業者IDは重複がなくユニークに設定し必要最低限の発行数にしたうえで、操作実施者が特定できること。
102		オンライン診療システム事業者は、オンライン診療システムにおいて、不要な作業者IDが残っていないことを定期的に確認すること。
103		オンライン診療システム事業者は、オンライン診療システムにおいて、作業者IDのアクセス可能範囲が許可なく変更されていないことを定期的に確認すること。

整理番号

項番	分類	項目
104		オンライン診療システム事業者は、オンライン診療システムにおいて、特権IDの発行は必要な最小限のものに留めることとし、使用時には実施内容を記録すること。
105		オンライン診療システム事業者は、オンライン診療システムにおいて、特権使用者に昇格可能な作業者IDを制限すること。
106		オンライン診療システム事業者は、オンライン診療システムにおいて、管理端末以外からの特権IDによる直接ログオンを禁止すること。
107		オンライン診療システム事業者は、オンライン診療システムの運用･保守端末等において、パスワードを記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。
108		オンライン診療システム事業者は、オンライン診療システムにおいて、開発用コード、開発ツール類、その他不必要なファイル等をシステム上に置かないこと。
109		オンライン診療システム事業者は、リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、オンライン診療システムへの不正な侵入が生じないよう安全管理措置を講じること。保守作業は最小限の時間に努めるため計画をたて実施すること。
110		オンライン診療システム事業者は、リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認すること。
111		オンライン診療システム事業者は、オンライン診療システムに係る媒体及び機器については、管理等に関する運用管理規程(ルール)(持ち出し手順、申請承認プロセス、返却確認プロセス、返却時検証手段、破棄時の対応)を定め、特に廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について保管すること。
112		オンライン診療システム事業者は、提供するオンライン診療システムの環境に媒体及び機器等の持ち込み機器を接続する際には、以下の対応を行うこと。 (1)持ち込み機器が再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証する (2)不正な機器がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、セキュリティパッチが適用されていること等を接続前に検査を行う仕組みを整備し運用する
113		オンライン診療システムを提供する環境は、脆弱性への対応を可能とするために、OSのアップデート並びに利用するソフトウェアに対するアップデートについて、リスク分析を行った上で必要な処置（セキュリティパッチ適用、設定変更等）を決定し、適切に実施すること。また、セキュリティパッチの適用前にセキュリティパッチが改ざんされていないこと及び有効性を検証すること。
114		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。
以下、提供する場合に実施すべき事項		
115	オンライン診療システム事業者が医師の代わりに患者への説明を行う場合	オンライン診療システム事業者は、患者に対して十分な説明が可能となるように、提供するオンライン診療システムに関する取扱い手順書等の説明書を提供できるようにし、患者が容易にアクセスできるような環境で提供を行うこと。
116		オンライン診療システム事業者は、患者がオンライン診療システムを利用するにあたり、必要となるシステム環境について、患者が容易にアクセスできるような環境で提供を行うこと。
117		オンライン診療システム事業者は、患者に対して利用規約等で患者が実施すべき事項を示すだけでなく、起こりうるリスク等の注意点に関して、別途患者が理解しやすいような説明を提供すること。
118		オンライン診療システム事業者は、患者がセキュリティリスク等と対策および責任の所在に対して、理解し、合意をしたことの証跡を取得すること。

整理番号

項番	分類	項目
119	医療情報システムと接続する場合	オンライン診療システムと医療情報システムが接続される場合、オンライン診療システム事業者は、医師や医療機関の医療情報管理責任者等に対して、接続することによる医療情報システムへの影響並びに追加的リスクに関して、十分な説明を行うこと。
120		オンライン診療システムと医療情報システムが接続される場合、オンライン診療システム事業者は、オンライン診療システムと医療情報システムとの接続点において、不正侵入防止対策等を講ずること。
121		オンライン診療システムと医療情報システムが接続される場合、オンライン診療システム事業者は、医療情報システムが医療情報安全ガイドラインに基づいて構築・運用されているか確認を行うこと。
122		オンライン診療システム事業者は、法定保存義務のある医療情報を保存する場合、サーバーを国内法の執行が及ぶ場所に設置すること。
123		オンライン診療システムと医療情報システムが接続される場合、オンライン診療システム事業者は、提供するオンライン診療システムに対して、原則医師の個人利用の端末による利用（いわゆるBYODにて）を行わないことについて、契約の中で明記を行うこと。
124	録音・録画・撮影機能を有する場合	オンライン診療システムにおいて、録音・録画・撮影を行う機能を有する場合は、プライバシー等を保護する意味でも、患者側、医師側の双方が同意した上で機能を動作させる機構を設けること。ただし、診療にかかる患者個人に関するデータの蓄積・残存は禁止されているため、診療終了後には、医療情報システムに接続し保存するか、削除する必要がある。
125		オンライン診療システムの利用する端末において、許可しない録音・録画・撮影がなされないように制御できるようにすることが望ましい。
126	ファイル送信、チャット機能を有する場合	オンライン診療システム事業者は、オンライン診療システムにおいて、ファイル送信、チャット機能の使用に関する情報を提供すること。
127		オンライン診療システムがファイル送信機能を有する場合は、医師側の許可があった際にのみ送信ができるような機能とすること。
128		オンライン診療システムがチャット機能を有する場合は、医師側の許可があった際にのみチャットできるような機能とすること。
129		オンライン診療システムがチャット機能を有する場合は、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、無効化する機能を保持すること。
130		オンライン診療システムと医療情報システムが接続される場合、ファイル送信機能、チャット機能等、患者側から影響を受けるような機能については、リスクを無害化もしくは機能の無効化を行うこと。
131	Personal Health Record(以下、PHR)と接続する場合	患者が入力したPHRとオンライン診療システムを接続し、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。
132	例外初診が行われるシステムの場合	例外的に初診が認められる疾患に対するオンライン診療システムを提供する場合、顔写真付きの身分証明書を用いた本人確認機能を有することが望ましい。