事業運営上開示すべき重要事項の概要[代行機関]

＊代行機関の業務を行う者は、本資料を作成し、ホームページ（自機関の Web サイトでも他のサイトでも可）に掲載すること。
＊選択肢の項目については、□を■にするか、該当する選択肢のみ残す（非該当は削除）こと。
＊ガイドラインの遵守状況については別添指定様式に記載すること。

更新情報	最終更新日	2023 年　10 月　24 日

＊下記事項に変更があった場合は速やかに変更し、掲載しているホームページを更新し、更新日を明示すること。

基本情報		
	機関名[注1)]	ホワイトヘルスケア株式会社
	所在地(住所)[注1)]	東京都中央区日本橋大伝馬町17番5号 グランド日本橋小伝馬町 2F
	電話番号[注1)]	03－4241－1905
	FAX番号	03－6661－7280
	ホームページアドレス	https://whitehealthcare.co.jp
	窓口となるメールアドレス	info_hoken@whitehealthcare.co.jp
	代行機関コード[注2)]	
	代行機関の分類[注3)]	■医療保険者サイド □健診・保健指導機関サイド（健診機関グループ） □健診・保健指導機関サイド（健診機関グループ以外）

注１）名称等は正式なもので記載する。
注２）発行した代行機関コードを記載。
注3）いずれか一つを選択。「医療保険者サイド」とは、保険者の委託を受け、機関と保険者との間に入って第三者として代行処理をする代行機関の類型。「健診・保健指導機関サイド」とは健診機関とりまとめ機関（上記「健診機関グループ」）や福利厚生代行会社（上記「健診機関グループ以外」）等によりデータや決済をとりまとめる類型

施設及び設備情報				
	従事する職員の数[注4)注5)]	専任	機関本体　0 人	協力・関係会社　人
		兼任	機関本体　5 人	協力・関係会社　人
	全職員の数[注5)]		機関本体　35 人	協力・関係会社　人
	施設数(サポート拠点数)		1 箇所（都道府県名：東京都　）	
	財務基盤に関する資料または照会先[注6)]		ホワイトヘルスケア株式会社 東京都中央区日本橋大伝馬町 17 番 5 号 グランド日本橋小伝馬町 2F TEL 03-4241-1905 FAX 03-6661-7280	
	類似業務・サービスの提供実績[注7)]		□有（内容：　） ■無	
	提供するサービス	対象	■保険者向け　■健診・保健指導機関向け	
		内容	■事務点検　■請求・支払のとりまとめ・代行 ■健診・保健指導データの受領・振分・送付 □その他（　）	
	利用者によるサービスの選択	保険者	■可（選択可能な機能：　） □否	
		健診・保健指導機関	■可（選択可能な機能：　） □否	
	ガイドラインの遵守[注8)]		□最低限のガイドラインを遵守済 ■最低限のガイドラインを遵守する予定 □最低限のガイドラインを遵守していない	

注４）当該機関のうち代行業務に従事する者のみを記載。
注５）協力会社・関係会社等がない場合は記載不要（空欄）とし、あっても従事していない場合は0（ゼロ）人と記載。
注６）貸借対照表等決算報告書の類をホームページで公開している場合はその URL 等を記載。財務情報を公開していない

場合は照会先(連絡先及び担当者名等)を明記。
注７）例として提供サービスの項を参照のこと。
注８）別添指定様式「医療情報システムの安全管理に関するガイドライン　最低限のガイドライン遵守チェックリスト」に記載すること。チェックリストにおいて全項目「実施済」の場合は「最低限のガイドラインを遵守済」、１項目以上「実施予定」がある場合は「最低限のガイドラインを遵守する予定」を選ぶこと。

情報システムに関する情報	提供開始の年月日[注9)]	2024 年　4 月 1 日	
	システムの保有	■自己導入　□借用	
	システムの運用管理	■自機関内　□全部委託　□一部委託	
	システム専用区画･施設の有無	□専用施設（機関所有）　□専用施設（委託先） □機関建物内専用区画　■特に無し	
	システム管理技術者数	機関本体　2 人	委託先　0 人
	処理可能件数(設計値)	年間　50,000 件	1 日当たり　150　件

注９）試用期間を除く。

運営に関する情報	サービス提供時間	拠点	平日 9:00-18:00(除く　土日･祝日 12/24-1/4)
		システム	平日 9:00-18:00(除く　土日･祝日 12/24-1/4)
		ヘルプデスク	平日 9:00-18:00(除く　土日･祝日 12/24-1/4)
	データ授受の方法	外部から機関へ	■オンライン(回線種別　クラウド型送受信サービス) ■オフライン(送付手段　CD-R、USB メモリ等　　)
		機関から外部へ	■オンライン(回線種別　クラウド型送受信サービス) ■オフライン(送付手段　CD-R、USB メモリ等　　)
	データ授受におけるセキュリティ対策の方法	オンライン	ファイル保管時また転送時に、 AES 256 ビット暗号化
		オフライン	盗難･紛失した場合に個人情報漏洩を防ぐための ファイル　パスワード処理を施す

事務手数料等[注 10)]			保険者	健診・保健指導機関
	初期費用		円	円
	経常経費	別途請求の有無	□無(健診委託費に含まれる) ■有(下記)	□無(健診委託費に含まれる) ■有(下記)
		固定費	要求仕様による	要求仕様による
		従量単価[注 11)]	要求仕様による	要求仕様による
	代行機関利用に際し必要となる設備等[注 12)]		要求仕様による	要求仕様による

注10）すべて消費税込みの金額を記載。委託機能によって費用が異なる場合はすべて記載。
注11）単位あたり（例えばデータ１件あたり）の事務手数料を記載。取扱データの内容等によって単価が異なる場合はすべて記載。
注12）保険者、健診・保健指導機関において必要となるハードウェア、ソフトウェア、ネットワーク回線等を記載。初期費用に含まれるものと、初期費用以外に各自の負担で導入しなければならないものを明記

その他	前年度の取扱件数	年間　　件	1 日当たり　　件

別添　医療情報システムの安全管理に関するガイドライン　第５版
最低限のガイドライン遵守チェックリスト

本遵守チェックリストは、平成29年５月「医療情報システムの安全管理に関するガイドライン　第５版 」の６章における「最低限のガイドライン」の遵守状況のチェックリストである。

＊代行機関の業務を実施する者は、本資料を作成しホームページ（自機関のWebサイトでも他のサイトでも可）に掲出すること。
＊選択肢の項目については、「実施済」「実施予定」より一つ選び、□を■にすること。「実施予定」を選択した場合は、実施予定時期を明記すること。

更新情報	最終更新日	2023 年　　10 月　　24 日

＊下記事項に変更があった場合は速やかに変更し、掲載しているホームページを更新し、更新日を明示すること。

組織的安全管理対策

No	チェック項目	実施済	実施予定(実施時期)
1.	情報システム運用責任者の設置及び担当者(システム管理者を含む)の限定を行っている。	■	□(　　)
2.	個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めている。	■	□(　　)
3.	情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成している。	■	□(　　)
4.	個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めている。	■	□(　　)
5.	運用管理規程等において次の内容を定めている。 (a) 理念(基本方針と管理目的の表明) (b) 医療機関等の体制 (c) 契約書・マニュアル等の文書の管理 (d) リスクに対する予防、発生時の対応の方法 (e) 機器を用いる場合は機器の管理 (f) 個人情報の記録媒体の管理(保管・授受等)の方法 (g) 患者等への説明と同意を得る方法 (h) 監査 (i) 苦情・質問の受付窓口	□	■(2024年3月31日)

物理的安全対策

No	チェック項目	実施済	実施予定(実施時期)
1.	個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠している。	■	□(　　)
2.	個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規定に基づき許可された者以外立ち入ることが出来ない対策を講じている。もしくは、同等レベルの他の取りうる手段がある	■	□(　　)
3.	個人情報の物理的保存を行っている区画への入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録している。	■	□(　　)
4.	個人情報の物理的保存を行っている区画への入退者の記録を定期的にチェックし、妥当性を確認している。	■	□(　　)
5.	個人情報が存在するPC 等の重要な機器に盗難防止用チェーンを設置している。	■	□(　　)
6.	覗き見防止の対策を実施している。	■	□(　　)

技術的安全対策

No	チェック項目	実施済	実施予定(実施時期)
1.	情報システムへのアクセスにおける利用者の識別と認証を行っている。	■	□(　　)

No	チェック項目	実施済	実施予定(実施時期)
2.	本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、本人しか知り得ない状態に保つよう対策を行っている。	■	□(　　)
3.	本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意している。	■	□(　　)
4.	入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防衛策を講じている。	■	□(　　)
5.	動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意している。注 1)	■	□(　　)
6.	関係職種ごとに、アクセスできる情報の範囲を定め、そのレベルに沿ったアクセス管理を行っている。	■	□(　　)
7.	アクセスの記録及び定期的なログを確認している。注 2)	■	□(　　)
8.	アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を講じている。	■	□(　　)
9.	アクセスの記録に用いる時刻情報は信頼できるものである。注 3)	■	□(　　)
10.	システム構築時や、適切に管理されていないメディアを使用したり、外部からの情報を受け取る際にはウイルス等の不正なソフトウェアの混入がないか確認している。注 4)	■	□(　　)
11.	システム内のパスワードファイルでパスワードは必ず暗号化(不可逆)され、適切な手法で管理及び運用が行われている。注 5)	■	□(　　)
12.	利用者がパスワードを忘れたり、盗用される恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付し、本人以外が知りえない方法で再登録を実施している。	■	□(　　)
13.	システム管理者であっても、利用者のパスワードを推定できる手段を防止している。注 6)	■	□(　　)
14.	パスワードは定期的に変更し(最長でも 2 ヶ月以内 ※2 要素認証を採用している場合を除く。)、極端に短い文字列を使用していない。注 7)	■	□(　　)
15.	類推しやすいパスワードを使用せず、類似のパスワードを繰り返し使用していない。注 8)	■	□(　　)
16.	利用者以外に無線 LAN の利用を特定されないようにしている。	■	□(　　)
17.	無線 LAN を利用する場合、不正アクセスの対策を施している。	■	□(　　)
18.	無線 LAN を利用する場合、不正な情報の取得を防止している。	■	□(　　)
19.	無線 LAN を利用する場合、電波を発する機器(携帯ゲーム機等)によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合に留意している。	□	■(2024 年 3 月 31 日)
20.	無線 LAN の適用に関して、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考としている。	■	□(　　)
21.	IoT 機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規定を定めている。	□	■(2024 年 3 月 31 日)
22.	IoT 機器を利用する場合、セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等に説明し、同意を得、また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供ししている。	■	□(　　)
23.	IoT 機器を利用する場合、システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用している。	■	□(　　)
24.	IoT 機器を利用する場合、使用が終了した又は不具合のため使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じている。	■	□(　　)

注1:動作確認用データの情報管理を厳格に行い、動作確認終了後は適切に破棄を行うことを指す。
注2:アクセスの記録はすくなくとも利用者のログイン時刻および時間、ログイン中に操作した情報が特定できなることを指す。また、情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録(操作者及び操作内容)を以って代えることができる。
注3:代行機関の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と操作事実の記録として問題のない範囲の精度を保つことを指す。
注4:適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用し、常時ウイルス等の不正ソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持(例えばパターンファイルの更新の確認・維持)を行うこと。
注 5:利用者識別にICカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用規程にて定めることを以って代えることができる。
注 6:例として設定ファイルにパスワードを記載しないようにする等があげられる。
注 7:英数字、記号を混在させた8文字以上の文字列が望ましい。
注 8:類推しやすいパスワードには、自信の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。

人的安全対策(従業者に対する人的安全管理措置)

No	チェック項目	実施済	実施予定(実施時期)
1.	法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行っている。	■	□( )
2.	定期的に従業者に対し個人情報の安全管理に関する教育訓練を行っている。	■	□( )
3.	従業者の退職後の個人情報保護規程を定めている。	■	□( )

人的安全対策(事務取扱委託業者の監督及び守秘義務契約)

No	チェック項目	実施済	実施予定(実施時期)
1.	外部受託業者を採用する場合は、包括的な委託先の罰則を定めた就業規則等で裏づけられた守秘契約を締結している。	■	□( )
2.	外部受託業者を採用する場合で、保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行っている。	■	□( )
3.	外部受託業者を採用する場合は、清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行っている。	■	□( )
4.	委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件としている。	■	□( )
5.	プログラムの異常等で保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が個人情報にアクセスする場合に、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行っている。	■	□( )

情報の破棄

No	チェック項目	実施済	実施予定(実施時期)
1.	情報種別ごとに破棄の手順を定めている。[注9)]	■	□( )
2.	情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認している。	■	□( )
3.	外部保存を受託する機関に破棄を委託した場合は、委託元の医療機関等が確実に情報の破棄が行われたことを確認している。	□	■(2024年3月31日)
4.	運用管理規程において不要になった個人情報を含む媒体の廃棄を定める規程の作成を定めている。	■	□( )

注 9:手順は、破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含む必要がある。

情報システムの改造と保守

No	チェック項目	実施済	実施予定(実施時期)
1.	動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めている。	■	□( )
2.	メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、およびアクセスした場合は対象個人情報を含む作業記録を残している。注 10)	■	□( )
3.	保守要員個人の専用アカウントは外部流出等による不正使用の防止の観点から適切に管理することを求めている。	■	□( )
4.	保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えている。	■	□( )
5.	保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認している。	□	■(2024年3月31日)
6.	保守会社と守秘義務契約を締結し、これを遵守させている。	■	□( )
7.	保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむ得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認している。	□	■(2024年3月31日)
8.	リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを採取し、当該作業の終了後速やかにアクセスログの内容を医療機関等の責任者が確認している。	□	■(2024年3月31日)
9.	再委託が行われる場合は再委託先にも保守会社と同等の義務を課している。	■	□( )

注 10:システム利用者を模して操作確認を行うための識別・認証についても同様である。

情報及び情報機器の持ち出しについて

No	チェック項目	実施済	実施予定(実施時期)
1.	リスク分析を行い、情報及び情報機器の持ち出しに関する運用管理規程を定めている。	■	□( )
2.	運用管理規程には、持ち出した情報及び情報機器の管理方法を定めている。	■	□( )
3.	情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めている。	■	□( )
4.	運用規程で定めた盗難、紛失時の対応を従業者等に周知・教育を行っている。	■	□( )
5.	医療機関等や情報の管理者は、台帳等を用いて情報が格納された可搬媒体若しくは情報機器の所在を把握している。	□	■(2024年3月31日)
6.	情報機器に対して起動パスワードを設定している。	■	□( )
7.	盗難、置き忘れの措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにしている。	■	□( )
8.	持ち出した情報機器をネットワークに接続したり、外部媒体を接続する場合は、情報端末が情報漏洩、改ざん等の対象とならない対策を施している。特にモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LANは技術的安全対策の16～20の基準を満たさないことがあるため、公衆無線LANしか利用できない環境にあり、且つ外部と個人情報を含む医療情報を交換する場合の安全管理で述べられている基準を満たした通信手段を選択することができる場合に限り認めている。	■	□( )
9.	持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールしている。	■	□( )
10.	個人保有の情報機器であっても、業務上、医療機関等の情報を持ち出して取り扱う場合、管理者は上記1～5の対策を行うとともに、管理者の責任において上記6～9と同様の要件を遵守している。	■	□( )

災害、サイバー攻撃等の非常時の対応

No	チェック項目	実施済	実施予定(実施時期)
1.	医療サービスを提供し続けるためのBCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けている。[注11)]	■	□(　　)
2.	正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意している。	■	□(　　)
3.	非常時のユーザアカウントや非常時用機能の管理手順を整備している。	■	□(　　)
4.	非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理および監査を行っている。	■	□(　　)
5.	非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更している。	■	□(　　)
6.	標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備している。	■	□(　　)
7.	サイバー攻撃で広範な地域での一部業務の停止等業務提供体制に支障が発生する場合は、所管官庁への連絡を行っている。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管省庁への連絡を行っている。	■	□(　　)

注 11:判断するための基準、手順、判断者、をあらかじめ決めていることを指す。

外部と個人情報を含む医療情報を交換する場合の安全管理

No	チェック項目	実施済	実施予定(実施時期)
1.	ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策、施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策、セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行っている。[注12)]	■	□(　　)
2.	データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認(認証)を行っている。[注13)]	□	■(2024年3月31日)
3.	施設内において、正規利用者への成りすまし、許可機器への成りすましを防ぐ対策を行っている。	■	□(　　)
4.	ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPN の間で送受信ができないように経路設定されている。[注14)]	■	□(　　)
5.	送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施している。[注15)]	■	□(　　)
6.	通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等と、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にしている。 • 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に係わる操作を開始する動作の決定 • 送信元の医療機関等がネットワークに接続できない場合の対処 • 送信先の医療機関等がネットワークに接続できなかった場合の対処 • ネットワークの経路途中が不通または著しい遅延の場合の対処 • 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 • 伝送情報の暗号化に不具合があった場合の対処 • 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 • 障害が起こった場合に障害部位を切り分ける責任 • 送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処	□	■(2024年3月31日)

No	チェック項目	実施済	実施予定(実施時期)
7.	医療機関内において次の事項において契約や運用管理規程等で定めている。 • 通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 • 患者等に対する説明責任の明確化。 • 事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。 • 交換した医療情報等に対する管理責任及び事後責任の明確化。個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。 •	□	■(2024年3月31日)
8.	リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止している。	■	□(　　)
9.	回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認している。	■	□(　　)
10.	患者に情報を閲覧させる場合、内部システムに不正な侵入等が起こらないよう対策を実施している。[注16)]	□	■(2024年3月31日)
11.	オープンなネットワークを介してHTTPSを利用した接続を行う際、IPsecを用いたVPN接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLSのプロトコルバージョンをTLS1.2のみに限定した上で、クライアント証明書を利用したTLSクライアント認証を実施している。(その際、TLSの設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行っている。)	■	□(　　)

注12:例としてIPSecとIKEを利用することによりセキュアな通信路を確保することがあげられる。

注13:採用する通信方式や運用管理規定により、採用する認証手段を決めること。また、認証手段としてはPKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用ワンタイムパスワード等の用意に解読されない方法を用いるのが望ましい。

注14:安全性が確認できる機器とは、例として、ISO15408で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が医療情報システムの安全管理に関するガイドライン第5版に適合していることを確認できるものをいう。

注15:例として、SSL/TLSの利用、S/MIMEの利用、ファイルに対する暗号化等の対策があげられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用していなければならない。

注16:システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI個人認証等の技術を用いた対策を指す。