目次

情報流

アプリケーション提供における情報流

開発フェーズにおける情報流

本番環境だけではなく開発環境や試験環境を含め、アプリケーション上の情報の処理に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
開発保守要員が	対象事業者DCの開発拠点の	開発保守端末で	開発・試験環境のプログラム・環境情報・ログ・テストデータ等を	作成・閲覧・操作する
		遠隔診療サーバ(開発環境)で		
		フロントサーバ(開発環境)で		
		ログサーバ(開発環境)で		
		遠隔診療運営管理サーバ(開発環境)で		
		オブジェクトストレッジサーバ(開発環境)で		閲覧する
運営管理者が		運営管理端末やモバイル端末で		作成・閲覧・操作する
QA担当者が				
開発保守要員が	対象事業者DCの本番拠点の	開発保守端末で	本番環境のプログラム・環境情報・ログ等を	閲覧・操作する
		遠隔診療サーバ(本番環境)で		
		フロントサーバ(本番環境)で		
		ログサーバ(本番環境)で		
		遠隔診療運営管理サーバ(本番環境)で		
		オブジェクトストレッジサーバ(本番環境)で		閲覧する
運営管理者が		運営管理端末やモバイル端末で	本番環境のデータ等を	閲覧・操作する
QA担当者が			本番環境のテストデータ等を	

運用フェーズにおける情報流

実際の業務におけるアプリケーションの活用に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
患者が	インターネット接続が可能な場所の	モバイルフォーン・タブレットで	患者情報・診療情報・病院情報・医療スタッフ情報(医者、クリニック管理者、スタッフ)等を ※ 診療情報	作成・閲覧・操作する
運営管理者が	対象サービスの本番拠点の	運営管理端末やモバイル端末で	予約・問診・決済・明細書・領収書・診断結果（対象医療情報）等	
Clinic Admin、医師、スタッフが	診察室の	医事端末で		

契約終了フェーズにおける情報流

開発フェーズと運用フェーズにおいてアプリケーション上に保存される情報の廃棄や移管等の処理に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
開発保守要員が	対象事業者DCの開発拠点の	オブジェクトストレッジサーバ(開発環境)で	保存されているテストデータ及びアプリケーション関連の情報・履歴データ等を	保管・移管・破棄する
	対象事業者DCの本番拠点の	遠隔診療サーバ(本番環境)で	患者情報・診療情報・病院情報・医者情報等のデータを	
		フロントサーバ(本番環境)で		
		遠隔診療運営管理サーバ(本番環境)で		
		オブジェクトストレッジサーバ(本番環境)で		
		ログサーバ(本番環境)で	保存・作成されているログ・履歴データ等を	

プラットフォーム提供における情報流

開発フェーズにおける情報流

開発フェーズと運用フェーズにおいてアプリケーション上に保存される情報の廃棄や移管等の処理に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
開発保守要員が	対象事業者DCの開発拠点の	開発保守端末で	開発環境のアプリケーション提供に係る情報・データ等を	作成・閲覧・操作する
		遠隔診療サーバ(開発環境)で		
		フロントサーバ(開発環境)で		
		ログサーバ(開発環境)で		
		遠隔診療運営管理サーバ(開発環境)で		
		オブジェクトストレッジサーバ(開発環境)で		
	対象事業者DCの本番拠点の	開発保守端末で	本番環境のアプリケーション提供に係る情報・データ等を	
		遠隔診療サーバ(本番環境)で		
		フロントサーバ(本番環境)で		
		ログサーバ(本番環境)で		
		遠隔診療運営管理サーバ(本番環境)で		
		オブジェクトストレッジサーバ(本番環境)で		

運用フェーズにおける情報流

プラットフォームが提供する機能の利用に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
患者が	ネットワークが可能な所の	モバイル端末で	アプリケーション提供に係る情報・データ等を	操作・処理する
運営管理者が	対象事業者DCの本番拠点の	運営管理端末で		閲覧・操作・設定・処理する
Clinic Admin, 医師、スタッフが	診察室の	医事端末で		閲覧・操作・処理する
開発保守要員が	対象事業者DCの本番拠点の	遠隔診療サーバ(本番環境)で		処理・保存する
		フロントサーバ(本番環境)で		
		ログサーバ(本番環境)で		
		遠隔診療運営管理サーバ(本番環境)で		
		オブジェクトストレッジサーバ(本番環境)で		
		ストーレッジ装備で		保管する

契約終了フェーズにおける情報流

プラットフォーム上に保存される情報の廃棄や移管等の処理に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
開発保守要員が	対象事業者DCの開発拠点の	オブジェクトストレッジサーバ(開発環境)で	開発環境のアプリケーション提供に係る情報・データ等を	移管・保管・破棄する
	対象事業者DCの本番拠点の	遠隔診療サーバ(本番環境)で	本番環境のアプリケーション提供に係る情報・データ等を	
		フロントサーバ(本番環境)で		
		遠隔診療運営管理サーバ(本番環境)で		
		ログサーバ(本番環境)で		
		オブジェクトストレッジサーバ(本番環境)で		

インフラ提供における情報流

開発フェーズにおける情報流

開発フェーズと運用フェーズにおいてアプリケーション上に保存される情報の廃棄や移管等の処理に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
インフラ開発担当者が	対象サービスの開発・試験拠点の	開発用端末で	開発・試験DCのPhysical Serverの設定情報等を	作成・閲覧・操作する
	対象サービスの開発・試験DCの	開発用Physical Serverで		
	対象サービスの開発・試験拠点の	開発用端末で	本番DCのProduction Physical Server の設定情報等を	
			本番DCのPrivate Zone Physical Serverの設定情報等を	
			本番DCのObject Strorage Serverの設定情報等を	
			本番DCのService Firefallの設定情報等を	
			本番DCのApplication Firefallの設定情報等を	
			本番DCのInfra Firewallの設定情報等を	
			本番DCのDC NATの設定情報を	
	対象サービスの本番DCの	本番DCのProduction Physical Serverで	本番DCのProduction Physical Serverの設定情報等を	
		本番DCのPrivate Zone Physical Serverで	本番DCのPrivate Zone Physical Serverの設定情報等を	
		本番DCのObject Strorage Serverで	本番DCのObject Strorage Serverの設定情報等を	
		本番DCのService Firefallで	本番DCのService Firefallの設定情報等を	
		本番DCのApplication Firefallで	本番DCのApplication Firefallの設定情報等を	
		本番DCのInfra Firewallで	本番DCのInfra Firewallの設定情報等を	
		本番DCのVPN終端装置で	本番DCのVPN終端装置の設定情報等を	
		本番DCのDC NATで	本番DCのDC NATの設定情報を	

運用フェーズにおける情報流

インフラが提供する機能の利用に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
通信事業者が	本番DCと医療機関の間の	VPN用ネットワークで	暗号化したアプリケーション提供に係る情報・データ等を	転送する
-	本番DCの	Production Physical Server 上で	アプリケーション提供に係る情報・データ等を	処理する
		Private Zone Physical Server 上で	アプリケーション提供に係る情報・データ等を	処理する
		Object Storage Server で	アプリケーション提供に係る情報・データ等を	保存する
		Service Firewallで	暗号化したアプリケーション提供に係る情報・データ等を	転送する
			アプリケーション提供に関係のない情報・データ等を	遮断する
		Application Firewallで	暗号化したアプリケーション提供に係る情報・データ等を	転送する
			アプリケーション提供に関係のない情報・データ等を	遮断する
		Infra Firewall で	アプリケーション提供に関係のない情報・データ等を	遮断する
		PrivateZone内のネットワーク機器で	暗号化したアプリケーション提供に係る情報・データ等が	転送される
		PrivateZone内と外のネットワーク機器で	暗号化したアプリケーション提供に関わる情報・データ等が	転送される
		DC NAT で	アプリケーション提供に係る情報・データ等が	転送される
	医療機関内の	無線LANまたは有線LAN上の機器で	アプリケーション提供に係る情報・データ等が	転送される

契約終了フェーズにおける情報流

インフラ上に保存される情報の廃棄や移管等の処理に着目

Who(誰が)	Where(どこの/どこを)	Which(どの機器で/どの媒体で)	What(何を/何が)	How(どうするか/どうされるか)
インフラ運用・保守担当が	対象サービスの開発・試験DCの	Development Physical Serverで	開発・試験DCのDevelopment Physical Serverの設定情報等を	破棄もしくは移管する
	対象サービスの開発・試験拠点の	開発用端末で	本番DCのProduction Physical Serverの設定情報等を	
			本番DCのPrivate Zone Physical Serverの設定情報等を	
			本番DCのObject Storage Serverの設定情報等を	
			本番DCのService Firewallの設定情報等を	
			本番DCのApplication Firewallの設定情報等を	
			本番DCのInfra Firewallの設定情報等を	
			本番DCのVPN終端装置の設定情報等を	

情報流の分類表

提供形態	フェーズ	情報流		分類
		ID	内容	
アプリケーション	開発	AD01	開発・試験環境のプログラム・環境情報・ログ・テストデータ等を作成・閲覧・操作する	開発テストデータ
		AD02	開発環境情報・ログデータ等を閲覧する	開発テストデータ
		AD03	本番環境のプログラム・環境情報・ログ等を閲覧・操作する	アプリケーションの設定情報(本番環境情報)
		AD04	本番環境のデータ等を閲覧・操作する	サービス情報（個人情報を含む可能性あり）
		AD05	本番環境のテストデータ等を閲覧・操作する	本番テストデータ
	運営	AO01	患者情報・診療情報・病院情報・医療スタッフ情報(医者、クリニック管理者、スタッフ)等を作成・閲覧・操作する ※ 診療情報 予約・問診・決済・明細書・領収書等	患者情報 診療情報 医療スタッフ情報 医療施設情報
		AO04	患者情報を閲覧する	患者情報 診療情報
	契約終了	AC01	保存されているテストデータ及びアプリケーション関連の情報・履歴データ等を保管・移管・破棄する	開発テストデータ
		AC02	患者情報・診療情報・病院情報・医者情報等のデータを保管・移管・破棄する	患者情報 診療情報 医療スタッフ情報 医療施設情報
		AC03	保存・作成されているログ・履歴データ等を保管・移管・破棄す	ログ情報
プラットフォーム	開発	PD01	開発環境のアプリケーション提供に係る情報・データ等を作成・閲覧・操作する	プラットフォーム上の開発アプリケーション提供に係る情報(開発環境のテストデータ)
		PD02	本番環境のアプリケーション提供に係る情報・データ等を作成・閲覧・操作する	プラットフォーム上の本番アプリケーション提供に係る情報(個人情報を含む可能性あり)
	運営	PO01	アプリケーション提供に係る情報・データ等を閲覧・設定・操作・処理・保存する	プラットフォーム上の本番アプリケーション提供に係る情報(個人情報を含む可能性あり)
	契約終了	PC01	開発環境のアプリケーション提供に係る情報・データ等を移管・保管・破棄する	プラットフォーム上の開発アプリケーション提供に係る情報(開発環境のテストデータ)
		PC02	本番環境のアプリケーション提供に係る情報・データ等を移管・保管・破棄する	プラットフォーム上の本番アプリケーション提供に係る情報(個人情報を含む可能性あり)
インフラ	開発	ID01	開発・試験DCのPhysical Serverの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(開発環境)
		ID02	本番DCのProduction Physical Server の設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)
		ID03	本番DCのPrivate Zone Physical Serverの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)
		ID04	本番DCのObject Strorage Serverの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)
		ID05	本番DCのService Firefallの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)
		ID06	本番DCのApplication Firefallの設定情報等を作成・閲覧・操作す	インフラ機器の設定情報(本番環境)
		ID07	本番DCのInfra Firewallの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)
		ID08	本番DCのDC NATの設定情報を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)
	運営	IO01	暗号化したサービス提供に係る情報・データ等を転送する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)
		IO02	サービス提供に係る情報・データ等を処理する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)
		IO03	サービス提供に係る情報・データ等を保存する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)
		IO04	暗号化したサービス提供に係る情報・データ等が転送される	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)
		IO05	サービス提供に関係のない情報・データ等を遮断する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)
	契約終了	IC01	開発・試験DCのDevelopment Physical Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(開発環境)
		IC02	本番DCのProduction Physical Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)
		IC03	本番DCのPrivate Zone Physical Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)
		IC04	本番DCのObject Storage Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)
		IC05	本番DCのService Firewallの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)
		IC06	本番DCのApplication Firewallの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)
		IC07	本番DCのInfra Firewallの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)
		IC08	本番DCのVPN終端装置の設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)

特定した脅威の一覧

ID	脅威	
	項目	詳細
T01	不正な閲覧・操作	正当な権限を持たない者（組織の内外を問わない）が、医療情報、認証情報等を盗み見る。または、医療情報システム等に関連する端末等を不適切に操作する。
T02	ネットワーク上の盗聴・なりすまし	ネットワーク上を流れるデータの盗聴等により、認証情報等を入手する。または、入手した認証情報等を用いて正当な権限を持つ者になりすます。
T03	高度サイバー攻撃	標的型メール等によって医療情報システム等や関連する端末等をマルウェアに感染させる。
T04	情報の窃取・漏洩	物理的あるいは電子的方法を用いて、医療情報等を盗み出す。または、故意/過失に依らず、医療情報等を不適切に組織外へ流出させる。
T05	情報の改竄・破壊	故意/過失に依らず、医療情報等を物理的あるいは電子的に不正に書き換える、もしくは破壊する。
T06	医療情報システム等の停止	悪意を持った者による攻撃、あるいは過失による設定ミスや誤操作等により、医療情報システム等が停止する。
T07	技術的脆弱性の混入	故意/過失に依らず、OS やミドルウェア・アプリケーション等のソフトウェアの脆弱性や、IoT 機器やルータ等のネットワーク機器の脆弱性が医療情報システム等に混入する。
T08	機器や記憶媒体の持ち出し時の紛失・盗難	医療情報システム等に関連する機器や記憶媒体を業務上の理由で施設等の外へ持ち出す際、機器や記憶媒体を誤って紛失する、あるいは第三者に盗難される。
T09	施設への物理的侵入	正当な権限を持たない者（組織の内外を問わない）が、執務エリアやデータセンター等、医療情報システム等に関連する機器や記憶媒体が設置されている施設に侵入する。
T10	災害等	自然災害や社会インフラの損失等により、医療情報システム等に関連する機器や端末等が物理的に破損する等して、医療情報システム等の提供に支障をきたす。
T11	人的資源不足	サービスに必要な人材を確保できず、医療情報システム等の提供や運用等に支障をきたす。
T12	法令違反	医療情報システム等の提供に係る法律・ガイドライン、当局指針等に違反する。

リスクレベルの判定基準

発生頻度×深刻度

			深刻度				
			5	4	3	2	1
			深刻(Severe)	重要(Major)	中程度(Moderate)	限定的(Minor)	軽微(Negligible)
発生頻度	5	非常に高い(Frequent)	High	High	Moderate	Middle	Low
	4	高い(Probable)	High	Moderate	Moderate	Middle	Low
	3	偶発的(Occasional)	High	Moderate	Middle	Middle	Low
	2	低い(Remote)	Moderate	Moderate	Middle	Low	Low
	1	非常に低い(Improbable)	Moderate	Middle	Low	Low	Low

リスクレベル一覧

リスクレベル		
発生頻度×深刻度		
レベル	内容	対応要否
High	重大リスク→経営に重大な影響を及ぼすため、直ちに何らかの改善策を講ずる、もしくはリスクを受け入れる必要がある	Yes
Moderate	管理対象リスク→経営に重大な影響を及ぼす可能性があるため、改善策を講ずる必要がある	Yes
Middle	監視対象リスク→直ちに経営に重大な影響を及ぼす可能性は低いが、定期的にモニタリングする必要がある	No
Low	軽微リスク→経営に及ぼす影響は少ないため、リスクの存在を認識しておく	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
アプリケーション	開発	AD01	開発・試験環境のプログラム・環境情報・ログ・テストデータ等を作成・閲覧・操作する	開発テストデータ	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AD02	開発環境情報・ログデータ等を閲覧する	開発テストデータ	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスす	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AD03	本番環境のプログラム・環境情報・ログ等を閲覧・操作する	アプリケーションの設定情報(本番環境情報)	T01	不正な閲覧・操作	開発保守端末で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	開発保守端末で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	開発保守端末で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	開発保守端末で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	開発保守端末で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	開発保守端末で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AD04	本番環境のデータ等を閲覧・操作する	サービス情報（個人情報を含む可能性あり）	T01	不正な閲覧・操作	開発保守端末で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	開発保守端末で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	開発保守端末で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	開発保守端末で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	開発保守端末で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスす	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	開発保守端末で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AD05	本番環境のテストデータ等を閲覧・操作する	本番テストデータ	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスす	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
	運営	AO01	患者情報・診療情報・病院情報・医療スタッフ情報(医者、クリニック管理者、スタッフ)等を作成・閲覧・操作する ※ 診療情報 予約・問診・決済・明細書・領収書等	患者情報 診療情報 医療スタッフ情報 医療施設情報	T01	不正な閲覧・操作	運営管理端末やモバイル端末で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	運営管理端末やモバイル端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T03	高度サイバー攻撃	運営管理端末やモバイル端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	運営管理端末やモバイル端末で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	運営管理端末やモバイル端末で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	運営管理端末やモバイル端末で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ					
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ	深刻度	発生頻度	リスクレベル	対応要否
					T07	技術的脆弱性の混入	運営管理端末やモバイル端末で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できない。	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	運営管理端末やモバイル端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	運営管理端末やモバイル端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T10	災害等	運営管理端末やモバイル端末で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	運営管理端末やモバイル端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	5	3	High	Yes
					T12	法令違反	運営管理端末やモバイル端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AO04	患者情報を閲覧する	患者情報 診療情報	T01	不正な閲覧・操作	運営管理端末やモバイル端末で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	運営管理端末やモバイル端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	運営管理端末やモバイル端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	運営管理端末やモバイル端末で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	運営管理端末やモバイル端末で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	運営管理端末やモバイル端末で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	運営管理端末やモバイル端末で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	運営管理端末やモバイル端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	運営管理端末やモバイル端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	運営管理端末やモバイル端末で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	運営管理端末やモバイル端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	運営管理端末やモバイル端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
	契約終了	AC01	保存されているテストデータ及びアプリケーション関連の情報・履歴データ等を保管・移管・破棄	開発テストデータ	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	ファーマシーサーバ(開発環境)で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	ファーマシーサーバ(開発環境)で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	ファーマシーサーバ(開発環境)で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	ファーマシーサーバ(開発環境)で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-
					T11	人的資源不足	ファーマシーサーバ(開発環境)で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	ファーマシーサーバ(開発環境)で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AC02	患者情報・診療情報・病院情報・医者情報等のデータを保管・移管・破棄する	患者情報 診療情報 医療スタッフ情報 医療施設情報	T01	不正な閲覧・操作	フロントサーバ(本番環境)で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	フロントサーバ(本番環境)で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	フロントサーバ(本番環境)で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	フロントサーバ(本番環境)で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	フロントサーバ(本番環境)で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	フロントサーバ(本番環境)で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	フロントサーバ(本番環境)で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	フロントサーバ(本番環境)で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	フロントサーバ(本番環境)で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	フロントサーバ(本番環境)で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	フロントサーバ(本番環境)で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	フロントサーバ(本番環境)で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		AC03	保存・作成されているログ・履歴データ等を保管・移管・破棄する	ログ情報	T01	不正な閲覧・操作	ログサーバ(本番環境)で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	ログサーバ(本番環境)で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	ログサーバ(本番環境)で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	ログサーバ(本番環境)で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	ログサーバ(本番環境)で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	ログサーバ(本番環境)で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	ログサーバ(本番環境)で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	ログサーバ(本番環境)で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	ログサーバ(本番環境)で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	ログサーバ(本番環境)で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	ログサーバ(本番環境)で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	ログサーバ(本番環境)で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
プラットフォーム	開発	PD01	開発環境のアプリケーション提供に係る情報・データ等を作成・閲覧・操作する	プラットフォーム上の開発アプリケーション提供に係る情報(開発環境のテストデータ)	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		PD02	本番環境のアプリケーション提供に係る情報・データ等を作成・閲覧・操作する	プラットフォーム上の本番アプリケーション提供に係る情報(個人情報を含む可能性あり)	T01	不正な閲覧・操作	開発保守端末で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	開発保守端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発保守端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	開発保守端末で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T05	情報の改竄・破壊	開発保守端末で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	開発保守端末で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	開発保守端末で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発保守端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発保守端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T10	災害等	開発保守端末で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	開発保守端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発保守端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
	運営	PO01	アプリケーション提供に係る情報・データ等を閲覧・設定・操作・処理・保存する	プラットフォーム上の本番アプリケーション提供に係る情報(個人情報を含む可能性あり)	T01	不正な閲覧・操作	運営管理端末で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	運営管理端末で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	運営管理端末で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T04	情報の窃取・漏洩	運営管理端末で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	運営管理端末で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	運営管理端末で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	運営管理端末で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	運営管理端末で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T09	施設への物理的侵入	運営管理端末で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	運営管理端末で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	運営管理端末で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	運営管理端末で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
	契約終了	PC01	開発環境のアプリケーション提供に係る情報・データ等を移管・保管・破棄する	プラットフォーム上の開発アプリケーション提供に係る情報(開発環境のテストデータ)	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	ファーマシーサーバ(開発環境)で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T03	高度サイバー攻撃	ファーマシーサーバ(開発環境)で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	ファーマシーサーバ(開発環境)で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	ファーマシーサーバ(開発環境)で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-
					T11	人的資源不足	ファーマシーサーバ(開発環境)で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	ファーマシーサーバ(開発環境)で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		PC02	本番環境のアプリケーション提供に係る情報・データ等を移管・保管・破棄する	プラットフォーム上の本番アプリケーション提供に係る情報(個人情報を含む可能性あり)	T01	不正な閲覧・操作	遠隔診療サーバ(本番環境)で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	遠隔診療サーバ(本番環境)で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	遠隔診療サーバ(本番環境)で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	遠隔診療サーバ(本番環境)で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	遠隔診療サーバ(本番環境)で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	遠隔診療サーバ(本番環境)で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	遠隔診療サーバ(本番環境)で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	遠隔診療サーバ(本番環境)で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	遠隔診療サーバ(本番環境)で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	遠隔診療サーバ(本番環境)で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	遠隔診療サーバ(本番環境)で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	遠隔診療サーバ(本番環境)で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
インフラ	開発	ID01	開発・試験DCのPhysical Serverの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(開発環境)	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	開発用Physical Serverで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発用Physical Serverで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発用Physical Serverで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発用Physical Serverで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-
					T11	人的資源不足	開発用Physical Serverで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	開発用Physical Serverで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		ID02	本番DCのProduction Physical Server の設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのProduction Physical Serverで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	本番DCのProduction Physical Serverで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのProduction Physical Serverで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのProduction Physical Serverで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのProduction Physical Serverで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのProduction Physical Serverで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	本番DCのProduction Physical Serverで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのProduction Physical Serverで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのProduction Physical Serverで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのProduction Physical Serverで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	本番DCのProduction Physical Serverで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのProduction Physical Serverで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		ID03	本番DCのPrivate Zone Physical Serverの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのPrivate Zone Physical Serverで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのPrivate Zone Physical Serverで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのPrivate Zone Physical Serverで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのPrivate Zone Physical Serverで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T05	情報の改竄・破壊	本番DCのPrivate Zone Physical Serverで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのPrivate Zone Physical Serverで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのPrivate Zone Physical Serverで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのPrivate Zone Physical Serverで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのPrivate Zone Physical Serverで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T10	災害等	本番DCのPrivate Zone Physical Serverで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのPrivate Zone Physical Serverで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのPrivate Zone Physical Serverで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		ID04	本番DCのObject Strorage Serverの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのObject Strorage Serverで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのObject Strorage Serverで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのObject Strorage Serverで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T04	情報の窃取・漏洩	本番DCのObject Strorage Serverで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのObject Strorage Serverで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのObject Strorage Serverで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのObject Strorage Serverで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのObject Strorage Serverで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T09	施設への物理的侵入	本番DCのObject Strorage Serverで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのObject Strorage Serverで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのObject Strorage Serverで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのObject Strorage Serverで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		ID05	本番DCのService Firefallの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのService Firefallで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのService Firefallで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのService Firefallで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T04	情報の窃取・漏洩	本番DCのService Firefallで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのService Firefallで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのService Firefallで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのService Firefallで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのService Firefallで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのService Firefallで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T10	災害等	本番DCのService Firefallで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのService Firefallで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのService Firefallで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		ID06	本番DCのApplication Firefallの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのApplication Firewallの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのApplication Firewallの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのApplication Firewallの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのApplication Firewallの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのApplication Firewallの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのApplication Firewallの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ					
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ	深刻度	発生頻度	リスクレベル	対応要否
					T07	技術的脆弱性の混入	本番DCのApplication Firewallの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのApplication Firewallの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのApplication Firewallの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのApplication Firewallの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのApplication Firewallの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのApplication Firewallの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		ID07	本番DCのInfra Firewallの設定情報等を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのInfra Firewallの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのInfra Firewallの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのInfra Firewallの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのInfra Firewallの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのInfra Firewallの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのInfra Firewallの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	本番DCのInfra Firewallの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのInfra Firewallの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのInfra Firewallの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのInfra Firewallの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのInfra Firewallの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのInfra Firewallの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		ID08	本番DCのDC NATの設定情報を作成・閲覧・操作する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのDC NATで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのDC NATで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのDC NATで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのDC NATで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのDC NATで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのDC NATで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	本番DCのDC NATで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのDC NATで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのDC NATで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのDC NATで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのDC NATで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのDC NATで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
	運営	IO01	暗号化したサービス提供に係る情報・データ等を転送する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)	T01	不正な閲覧・操作	VPN用ネットワークで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	VPN用ネットワークで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	VPN用ネットワークで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	VPN用ネットワークで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	VPN用ネットワークで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	VPN用ネットワークで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	VPN用ネットワークで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	VPN用ネットワークで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	VPN用ネットワークで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	VPN用ネットワークで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	VPN用ネットワークで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	VPN用ネットワークで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		IO02	サービス提供に係る情報・データ等を処理する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)	T01	不正な閲覧・操作	Production Physical Server上で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	Production Physical Server上で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	Production Physical Server上で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	Production Physical Server上で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	Production Physical Server上で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	Production Physical Server上で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	Production Physical Server上で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	Production Physical Server上で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	Production Physical Server上で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	Production Physical Server上で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	Production Physical Server上で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	Production Physical Server上で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		IO03	サービス提供に係る情報・データ等を保存する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)	T01	不正な閲覧・操作	Object Storage Server で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	Object Storage Server で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	Object Storage Server で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	Object Storage Server で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	Object Storage Server で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	Object Storage Server で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	Object Storage Server で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	Object Storage Server で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	Object Storage Server で	R09	許可された者以外が機器や媒体に直接アクセスす	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	Object Storage Server で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	Object Storage Server で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	Object Storage Server で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		IO04	暗号化したサービス提供に係る情報・データ等が転送される	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)	T01	不正な閲覧・操作	VPN用ネットワークで	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	VPN用ネットワークで	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	VPN用ネットワークで	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	VPN用ネットワークで	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	VPN用ネットワークで	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	VPN用ネットワークで	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	VPN用ネットワークで	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	VPN用ネットワークで	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	VPN用ネットワークで	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	VPN用ネットワークで	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	VPN用ネットワークで	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	VPN用ネットワークで	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
		IO05	サービス提供に関係のない情報・データ等を遮断する	インフラ上のアプリケーション提供に係る情報(個人・医療情報を含む可能性あり)	T01	不正な閲覧・操作	Private Zone Physical Server 上で	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	Private Zone Physical Server 上で	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	Private Zone Physical Server 上で	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	Private Zone Physical Server 上で	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	Private Zone Physical Server 上で	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	Private Zone Physical Server 上で	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	Private Zone Physical Server 上で	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	Private Zone Physical Server 上で	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	Private Zone Physical Server 上で	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	Private Zone Physical Server 上で	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	Private Zone Physical Server 上で	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	Private Zone Physical Server 上で	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
	契約終了	IC01	開発・試験DCのDevelopment Physical Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(開発環境)	T01	不正な閲覧・操作	-	-	-	-	-	-	-
					T02	ネットワーク上の盗聴・なりすまし	開発・試験DCのDevelopment Physical Serverの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	開発・試験DCのDevelopment Physical Serverの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	-	-	-	-	-	-	-
					T05	情報の改竄・破壊	-	-	-	-	-	-	-
					T06	医療情報システム等の停止	-	-	-	-	-	-	-
					T07	技術的脆弱性の混入	-	-	-	-	-	-	-
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	開発・試験DCのDevelopment Physical Serverの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	開発・試験DCのDevelopment Physical Serverの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	-	-	-	-	-	-	-

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T11	人的資源不足	開発・試験DCの Development Physical Serverの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	5	3	High	Yes
					T12	法令違反	開発・試験DCの Development Physical Serverの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC02	本番DCのProduction Physical Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのProduction Physical Serverの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのProduction Physical Serverの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのProduction Physical Serverの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのProduction Physical Serverの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T05	情報の改竄・破壊	本番DCのProduction Physical Serverの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのProduction Physical Serverの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのProduction Physical Serverの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのProduction Physical Serverの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T09	施設への物理的侵入	本番DCのProduction Physical Serverの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのProduction Physical Serverの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのProduction Physical Serverの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	5	3	High	Yes
					T12	法令違反	本番DCのProduction Physical Serverの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC03	本番DCのPrivate Zone Physical Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのPrivate Zone Physical Serverの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのPrivate Zone Physical Serverの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T03	高度サイバー攻撃	本番DCのPrivate Zone Physical Serverの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのPrivate Zone Physical Serverの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのPrivate Zone Physical Serverの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのPrivate Zone Physical Serverの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのPrivate Zone Physical Serverの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのPrivate Zone Physical Serverの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのPrivate Zone Physical Serverの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのPrivate Zone Physical Serverの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのPrivate Zone Physical Serverの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	5	3	High	Yes
					T12	法令違反	本番DCのPrivate Zone Physical Serverの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC04	本番DCのObject Storage Serverの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのObject Storage Serverの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	本番DCのObject Storage Serverの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのObject Storage Serverの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのObject Storage Serverの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのObject Storage Serverの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのObject Storage Serverの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのObject Storage Serverの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのObject Storage Serverの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのObject Storage Serverの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのObject Storage Serverの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのObject Storage Serverの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのObject Storage Serverの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC05	本番DCのService Firewallの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのService Firewallの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T02	ネットワーク上の盗聴・なりすまし	本番DCのService Firewallの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのService Firewallの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのService Firewallの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのService Firewallの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのService Firewallの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのService Firewallの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのService Firewallの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのService Firewallの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのService Firewallの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのService Firewallの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのService Firewallの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC06	本番DCのApplication Firewallの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのApplication Firewallの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのApplication Firewallの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T03	高度サイバー攻撃	本番DCのApplication Firewallの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのApplication Firewallの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのApplication Firewallの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのApplication Firewallの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのApplication Firewallの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのApplication Firewallの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T09	施設への物理的侵入	本番DCのApplication Firewallの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのApplication Firewallの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのApplication Firewallの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのApplication Firewallの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC07	本番DCのInfra Firewallの設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのInfra Firewallの設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのInfra Firewallの設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのInfra Firewallの設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのInfra Firewallの設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes

リスクアセスメント結果の一覧

リスク特定										リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T05	情報の改竄・破壊	本番DCのInfra Firewallの設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのInfra Firewallの設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes
					T07	技術的脆弱性の混入	本番DCのInfra Firewallの設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのInfra Firewallの設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのInfra Firewallの設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのInfra Firewallの設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのInfra Firewallの設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T12	法令違反	本番DCのInfra Firewallの設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No
		IC08	本番DCのVPN終端装置の設定情報等を破棄もしくは移管する	インフラ機器の設定情報(本番環境)	T01	不正な閲覧・操作	本番DCのVPN終端装置の設定情報等を	R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	5	1	Moderate	Yes
								R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	4	1	Middle	No
								R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行	3	1	Low	Yes
					T02	ネットワーク上の盗聴・なりすまし	本番DCのVPN終端装置の設定情報等を	R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	5	1	Moderate	Yes
								R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	5	4	High	Yes
								R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	5	3	High	Yes
								R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	5	3	High	Yes
								R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	5	4	High	Yes
								R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装され	5	3	High	Yes
								R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読 もしくは偽装される。	5	3	High	Yes
								R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	5	3	High	Yes
								R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	5	3	High	Yes
								R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	5	3	High	Yes
					T03	高度サイバー攻撃	本番DCのVPN終端装置の設定情報等を	R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	5	1	Moderate	Yes
								R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	5	4	High	Yes
								R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	5	4	High	Yes
								R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	5	3	High	Yes
					T04	情報の窃取・漏洩	本番DCのVPN終端装置の設定情報等を	R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	5	1	Moderate	Yes
								R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	5	4	High	Yes
								R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	5	4	High	Yes
								R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	4	1	Middle	Yes
								R66	医療情報システム等提供に係る事業者 （再委託先も含む）による故意又は過失による情報漏洩が行われる。	4	1	Middle	Yes
								R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生す る。	3	2	Middle	Yes
					T05	情報の改竄・破壊	本番DCのVPN終端装置の設定情報等を	R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	2	Moderate	Yes
								R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じ る。	4	1	Middle	Yes
								R78	情報が毀損や滅失した場合にバックアッ プされたデータを用いて元の状態に復元できない。	4	2	Moderate	Yes
								R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	4	1	Middle	No
								R80	医療情報システム等を更改等により移行 する際、移行元で記録された情報が移行後に正しく読みだせない。	4	1	Middle	No
					T06	医療情報システム等の停止	本番DCのVPN終端装置の設定情報等を	R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	5	3	High	Yes

リスクアセスメント結果の一覧

リスク特定									リスク分析			リスク評価
提供形態	フェーズ	情報流		分類	関連する脅威		特定したリスクシナリオ			深刻度	発生頻度	リスクレベル	対応要否
		ID	内容		ID	項目	シチュエーション	リスクID	シナリオ				
					T07	技術的脆弱性の混入	本番DCのVPN終端装置の設定情報等を	R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	5	1	Moderate	Yes
								R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	5	1	Moderate	Yes
								R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	5	1	Moderate	Yes
								R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	5	1	Moderate	Yes
								R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	5	1	Moderate	Yes
								R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	1	Moderate	Yes
								R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	5	1	Moderate	Yes
								R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	5	3	High	Yes
								R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	5	3	High	Yes
								R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できな	5	4	High	Yes
								R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	5	3	High	Yes
								R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	5	3	High	Yes
								R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	5	3	High	Yes
								R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	5	4	High	Yes
								R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じ	5	2	Moderate	Yes
								R72	一般利用者の権限が高いため、任意のソ フトウェアのインストール、持込機器接 続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	5	2	Moderate	Yes
								R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等 に不具合が生じる。	4	2	Moderate	Yes
					T08	機器や記憶媒体の持ち出し時の紛失・盗難	本番DCのVPN終端装置の設定情報等を	R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	5	4	High	Yes
								R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	5	4	High	Yes
								R51	個人情報が存在するPC等の重要な機器が盗難される。	5	4	High	Yes
								R55	紛失・盗難した機器が起動され、機器を不正に利用される。	4	1	Middle	No
								R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	4	1	Middle	Yes
								R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	5	1	Moderate	Yes
								R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	5	1	Moderate	Yes
								R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	5	1	Moderate	Yes
								R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	5	1	Moderate	Yes
					T09	施設への物理的侵入	本番DCのVPN終端装置の設定情報等を	R09	許可された者以外が機器や媒体に直接アクセスする。	5	1	Moderate	Yes
								R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	5	4	High	Yes
								R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	5	4	High	Yes
								R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	5	4	High	Yes
								R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	5	4	High	Yes
								R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	5	3	High	Yes
					T10	災害等	本番DCのVPN終端装置の設定情報等を	R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	5	3	High	Yes
								R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	5	3	High	Yes
								R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	5	3	High	Yes
								R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	5	3	High	Yes
								R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	4	2	Moderate	Yes
					T11	人的資源不足	本番DCのVPN終端装置の設定情報等を	R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	5	3	High	Yes
								R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われな	5	3	High	Yes
					T12	法令違反	本番DCのVPN終端装置の設定情報等を	R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	5	1	Moderate	Yes
								R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	5	3	High	Yes
								R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	5	4	High	Yes
								R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生す	4	1	Middle	Yes
								R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	4	2	Moderate	Yes
								R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支 障が生じる。	3	1	Low	No

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R01	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	低減	人的・組織的対策	Yes	対象	①-1	医療情報システム等における機器及びソフトウェアの構成図を作成する。	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じることを防止するため、医療情報システム等の構成・仕様に関する医療機関等の職員への教育につきましては、医療機関等にて実施をお願い致しま	-	-	-	-	-	-
				Yes	対象	①-2	医療情報システム等のネットワーク構成図を作成する。							-
				Yes	対象	①-3	①-1、①-2で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。							-
				Yes	対象	①-4	医療情報システム等を構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。							-
				Yes	対象	①-5	①-1～①-4で策定した資料等を医療機関等の求めに応じて提出することについて、開示内容、範囲、条件等を医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R02	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	低減	人的・組織的対策	Yes	対象	②-1	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。	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じることを防止するため、医事端末の定期的なソフトウェアアップデートにつきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	②-2	変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を講じる。							-
				Yes	対象外	②-3	情報処理に供するアプリケーションについては、受託事業者自身で開発したアプリケーションを用いる。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いる。							-
				Yes	対象	②-4	ソフトウェアに不正プログラムが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。							-
				Yes	対象	②-5	業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R03	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	低減	人的・組織的対策	Yes	-	-	-	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行されることを防止するため、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	①-1	医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにする。							-
				Yes	対象	①-2	ウェブブラウザの接続するサーバを業務上必要なサーバに限定する。							-
				Yes	対象外	①-3	ウェブブラウザの設定で、認可していないサイトから、ActiveX、Javaアプレット、Flash等のプログラムコードをダウンロード及び実行することができない設定とする（管理ソフトウェアが実行されるサーバのみを認可す							-
				Yes	対象	①-4	認可したサイトからダウンロードされるコードについても不正プログラム対策ソフトウェアにより検査する。							-
				Yes	対象外	①-5	ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。							-
				Yes	対象	①-6	医療情報システム等のサーバ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。							-
				Yes	対象	①-7	医療情報システム等に用いる装置には、必要のないアプリケーション等をインストールしない。							-
				Yes	対象外	①-8	医療情報システム等に関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。							-
				Yes	対象外	①-9	医療情報システム等に関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。							-
R04	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	低減	人的・組織的対策	Yes	-	-	-	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われることを防止するため、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	最新の脅威についての情報収集に努め、導入している不正プログラム対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認する。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。							-
				Yes	対象	①-2	不正プログラム対策ソフトウェアにおいて次の設定を行う。 ・リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）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 ・電子媒体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 ・定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ・管理者以外による設定変更やアンインストールの禁止							-
				Yes	対象	①-3	一定期間、不正プログラムのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとる。							-
				Yes	対象	①-4	医療情報システム等の構築に際しては、不正プログラム等の混入が生じないようにするための手順を策定し、これに則って構築する。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
				Yes	対象	①-5	不正プログラム対策ソフトウェアのパターン定義ファイルを常に最新のものに更新する。							-
				Yes	対象	①-6	医療情報システム等の構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新の不正プログラム対策ソフトウェア等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行							-
				Yes	対象	①-7	医療情報システム等利用環境がウイルス等による攻撃を受けた場合に、医療情報システム等提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。							-
R05	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	低減	人的・組織的対策	Yes	対象	③-1	ソフトウェア開発を行う際には、運用されているソフトウェアに影響を与えない環境で行う。	-	-	-	-	-	-	-
				Yes	対象外	③-2	開発施設では不正プログラムが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には不正プログラムへの対策を行う。							-
				Yes	対象	③-3	運用施設に保存されている医療情報を開発施設及び試験施設にコピーしない。							-
				Yes	対象	③-4	運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かない。							-
				Yes	対象	③-5	情報処理に不必要なファイル等を運用システム上におかない。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R06	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	低減	人的・組織的対策	Yes	対象	①-1	医療情報を開発及び試験用データとして直接利用しない。利用する場合には、個人を識別できる情報等の削除及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用する。	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R07	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	低減	人的・組織的対策	Yes	対象	③-1	システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R08	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	低減	人的・組織的対策	Yes	対象	①-1	受託した医療情報を保守･運用を行うために閲覧するのは必要最小限とする。	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われることを防止するため、医療情報の解析や第三者提供に係る患者等への同意取得につきましては、必要に応じて医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	①-2	①-1の閲覧が必要な場合には、緊急時を除き、システム管理者の事前･事後の承認により実施する。							-
				Yes	対象	①-3	受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。							-
				Yes	対象	①-4	①-1～①-3における閲覧に係る範囲、手順等について、医療機関等と合意する。また①-2、①-3により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。							-
				Yes	対象外	①-5	受託した医療情報の解析･分析は、医療情報システム等提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。							-
				Yes	対象外	①-6	受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。							-
				Yes	対象外	①-7	受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。							-
				Yes	対象	①-8	①-7の内容を、医療情報システム等提供に係る契約に含める。							-
				Yes	対象外	①-9	医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧･取得できないように対応策を講じる。							-
				Yes	対象外	①-10	①-9により、第三者提供（閲覧）を行う場合には、閲覧･取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更･削除できる対応を行							-
				Yes	対象外	①-11	医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。							-
				Yes	対象	①-12	①-7～①-11により第三者提供及びその報告を行うための条件、範囲等について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R09	許可された者以外が機器や媒体に直接アクセスする。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	機器や媒体の設置場所等のセキュリティ境界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、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を							-
				Yes	対象	①-2	機器や媒体の設置場所については、許可された者のみが入退できるように制限する。							-
				Yes	対象	①-3	医療情報システム等を設置、医療情報を保管する部屋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、入退館及び入退室者の確実な認証を行う。							-
				Yes	対象	①-4	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。							-
				Yes	対象	①-5	有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認する。							-
				Yes	対象外	①-6	受託事業者の職員の業務に応じて執務室内に滞在できる時間を指定する。							-
				Yes	対象	①-7	機械式の認証装置で利用する認証要素としては、ハードウェアトークン又はICカード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。							-
				Yes	対象	①-8	機器や媒体の設置場所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。							-
			技術的対策	Yes	-	-	-							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R10	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	低減	人的・組織的対策	Yes	-	-	-	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見されることを防止するため、患者等による画面の覗き見防止のための医事端末のレイアウト調整につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	医療情報等が表示される端末画面等がアクセス権限の無いものが視野に入らないような対応（室内の機器レイアウト等）を行う。						-
				Yes	対象	①-2	個人情報の表示中の覗き見を予防するために、端末に覗き見対策のシートを貼る等の対策を行う。						-
			技術的対策	Yes	-	-	-							-
R11	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	低減	人的・組織的対策	Yes	-	-	-	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われることを防止するため、医療機関等の職員への内部不正防止のための教育や、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	③-1	離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐ。						-
				Yes	対象	③-2	サービスの運用･保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。						-
				Yes	対象	③-3	医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、医療機関等と合意する。						-
				Yes	対象	③-4	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、あるいは強制ログオフを行う。						-
				Yes	対象	③-5	離席の場合のクローズ処理の具体的な適用について、医療機関等と合意する。						-
R12	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	低減	人的・組織的対策	Yes	-	-	-	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われることを防止するため、パスワードの適切な管理につきましては、医療機関等にて実施をお願い致します。	推測されやすいパスワードの使用、定期的なパスワードの変更が行われないことにより、認証の突破及び不正な閲覧・操作が行われる可能性がある。	4	1	Middle	当該残存リスクについて、そのリスクレベルをふまえて、監視対象リスク（直ちに経営に重大な影響を及ぼす可能性は低いが、定期的にモニタリングする必要があるリスク）として一時的に保有し、実装が未了となっている技術的対策への継続的な対応を通じてその低減を行う。	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	④-1	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を策定し、すべてのパスワードが品質基準を満たしていることを確実とする。						医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
				Yes	対象	④-2	パスワードポリシーについて、医療機関等と合意する。						-
				Yes	対象	④-3	パスワードには有効期限の設定を行い、定期的な変更を強制する。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、サービス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ようにする。						医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
				Yes	対象	④-4	パスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。						医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
				Yes	対象外	④-5	パスワード発行時には、乱数から生成した仮の医療情報システム等へのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施する。						-
				Yes	対象外	④-6	パスワードをシステムに記憶させる自動ログオン機能を利用しないよう利用者に徹底する。						-
				Yes	対象	④-7	利用者がパスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、利用者が設定しようとする品質の低いパスワードを認めないシステムの導入等を行う。						医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
				Yes	対象	④-8	本人の識別･認証に用いる情報は、本人しか知り得ない状態に保つよう対策を行う。						-
				Yes	対象外	④-9	利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと医療情報システム等にアクセスできないにようにする。						-
				Yes	対象	④-10	初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。						-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク				残存リスクへの対応計画	
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	基本方針	LineICa8
				Yes	対象	④-11	パスワードの設定に際しては、複数の文字種（英数字･大文字･小文字･記号等）を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。							医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
				Yes	対象	④-12	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。							-
				Yes	対象	④-13	パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とする。							医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
				Yes	対象	④-14	パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とする。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入する。							医療機関が利用するシステムの認証において、二段階認証の設定を推奨することで当該リスクの低減を図る。
R13	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	低減	人的・組織的対策	Yes	-	-	-	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われることを防止するため、医事端末における適切な利用者認証の実施につきましては、医療機関等にて実施をお願い致します。	医療機関及び利用者の認証情報が窃取もしくは推察されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	4	1	Middle	当該残存リスクについて、そのリスクレベルをふまえて、監視対象リスク（直ちに経営に重大な影響を及ぼす可能性は低いが、定期的にモニタリングする必要があるリスク）として一時的に保有し、技術的対策への継続的な対応を通じてその低減を行う。	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	⑤-1	ログオン時に利用する認証要素としては、ハードウェアトークン又はICカード等の認証デバイス、暗証番号（PIN）又はパスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせた多要素認証とすることが望ましい。							多要素認証の導入については、各医療機関の環境整備状況を考慮しながら今後の導入を検討する。
				Yes	対象	⑤-2	医療情報システム等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の情報システム利用に係る認証は、多要素認証とする。							-
				Yes	対象	⑤-3	利用者の認証で採用する認証方式について、医療機関等と合意する。							-
				Yes	対象	⑤-4	利用者の認証において、ID･パスワードによる認証方式を採用している場合には、ID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン第5版の公表（平成29年5月）から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるよう							多要素認証の導入については、各医療機関の環境整備状況を考慮しながら今後の導入を検討する。
R14	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	低減	人的・組織的対策	Yes	-	-	-	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われることを防止するため、医療機関等における医事端末の操作に関するアクセス制御方針に沿った職務分掌の履行につきましては、医療機関等にて実施をお願い	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	医療情報とそれ以外の情報を区分できる措置を講じる。							-
				Yes	対象	②-2	医療情報については、情報区分に従ってアクセス制御を行えるようにする。							-
				Yes	対象	②-3	仮想化技術を用いた資源をサービスに供する場合には、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る。							-
				Yes	対象	②-4	医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、医療機関等と合意する。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R15	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	低減	人的・組織的対策	Yes	-	-	-	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できないことを防止するため、ユーザIDの共有禁止や、ユーザIDの定期的な棚卸を適じた適時・適切な改廃につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	利用者は医療情報システム等上においてユニークな利用者ごとのIDにより識別する。							-
				Yes	対象	①-2	利用者のIDを発行する際に、既存のIDとの重複を排除する仕組みを導入する。							-
				Yes	対象外	①-3	複数利用者で共用するためのグループIDの利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、利用者ごとのIDでログオンしてからグループIDに変更する仕組みを利用する。							-
				Yes	対象	①-4	利用者のIDの発行は医療情報システム等の管理に必要な最小限の人数に留める。							-
				Yes	対象	①-5	監視ログの監査時に利用者を確実に特定するため、利用者のIDは過去に使われたものを再利用しない。							-
				Yes	対象外	①-6	アクセスを許可された利用者のIDによるアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。							-
				Yes	対象	①-7	不正なアカウントの利用又は試みが行われたことを利用者自身で検出するため、利用者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。							-
				Yes	対象外	①-8	不正なアカウントの利用を防ぐため、利用者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。							-
				Yes	対象	①-9	認可されていない利用者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると当該IDが存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。							-
				Yes	対象外	①-10	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が望ましい。							-
				Yes	対象	①-11	医療情報システム等に許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知する。							-
				Yes	対象	①-12	利用者が変更あるいは退職した際には、ただちに当該作業者IDを利用停止とする。							-
				Yes	対象	①-13	不要な利用者のIDが残っていないことを定期的に確認する。							-
R16	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	特権IDの発行は必要な最小限のものに留める。							-
				Yes	対象	②-2	特権使用者に昇格可能な利用者のIDを制限する。							-
				Yes	対象	②-3	特権の使用時には作業実施内容を記録する。							-
				Yes	対象	②-4	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。							-
				Yes	対象	②-5	特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。							-
				Yes	対象	②-6	医療情報システム等の機能として可能であれば、特権IDで使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改竄、削除など不正な行為を防止することが望ましい。							-
R17	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	低減	人的・組織的対策	Yes	-	-	-	パスワードやパスワードファイルが漏洩した場合に、不正利用されることを防止するため、パスワードの適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	③-1	各利用者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護する。							-
				Yes	対象	③-2	医療情報システム等及びソフトウェアを使用する前に、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の棚卸を行い、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							-
				Yes	対象	③-3	パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管する。							-
				Yes	対象	③-4	パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用する。また、一般の作業者による閲覧を制限する。							-
				Yes	対象	③-5	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。							-
				Yes	対象	③-6	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。							-
R18	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	低減	人的・組織的対策	Yes	対象	③-1	CD-R等の廃棄手順について定める。	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じることを防止するため、医療情報システム等の提供事業者における情報の破棄手順に沿った対応が行われていることの確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	③-2	ハードディスク等の廃棄手順について定める。							-
				Yes	対象	③-3	破棄手順に、不可逆的な破壊･抹消等により元のデータを復元できなくする措置を含める。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
				Yes	対象	③-4	ハードディスク等を医療情報システム等内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認す							-
				Yes	対象	③-5	サーバ等のBIOSパスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去する。							-
				Yes	対象外	③-6	ハードディスクを機器に接続する際には、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。							-
				Yes	対象	③-7	ハードディスクの廃棄については、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、医療機関等の求めに応じ、速やかに提出できるよう整備する。							-
				Yes	対象	③-8	物理的な破壊措置については受託事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておく。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。 なお、ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式（NSA推奨方式、米国防総省準拠方式、NATO方式、グートマン方式等）も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施することが望ましい。							-
				Yes	対象	③-9	電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認する。							-
				Yes	対象	③-10	運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、医療情報システム等提供上の要否の確認を定期的に行うこと。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置(事前に破棄の基準等を告知する等）。							-
				Yes	対象	③-11	情報の破棄手順について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R19	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	低減	人的・組織的対策	Yes	対象	②-1	電子媒体は台帳を作成して管理する。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証する。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持する。	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期発見できず、被害が拡大することを防止するため、医事端末の適切な管理や、紛失・盗難発生時の医療情報システム等の提供事業者への報告につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	②-2	情報を格納する機器･媒体等については、台帳管理等を行い、定期的に所在確認を行う。							-
				Yes	対象	②-3	個人情報が保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R20	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。	低減	人的・組織的対策	Yes	対象	②-1	サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R21	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	低減	人的・組織的対策	Yes	-	-	-	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができないことを防止するため、医療情報システム等の提供事業者における取得されたログに基づく不正アクセスの監視が行われていることの確認につきましては、医療機関等にて実施をお願い致し	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	利用者の活動、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たログを作成し、一定期間保存する。							-
				Yes	対象	①-2	ログを定期的に検証して不正な行為、システムの異常等を検出する。							-
				Yes	対象	①-3	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。 ・利用者情報（利用者の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） ・ファイル及びデータへのアクセス、変更、削除記録（利用者の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） ・データベース操作記録（利用者の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）修正パッチの適用作業（利用者のID、変更されたファイル） ・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） ・システム起動、停止イベント ・ログ取得機能の開始、終了イベント外部デバイスの取り外し ・IDS・IPS等のセキュリティ装置のイベントログ ・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）							-
				Yes	対象	①-4	ログを集中させ問題の検出を一箇所で確実に行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理する。							-
				Yes	対象	①-5	運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得する。							-
				Yes	対象	①-6	システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得する。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
				Yes	対象	①-7	医療情報システム等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よるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。			-	-	-	-	-
				Yes	対象	①-8	①-7に関する情報の医療機関等への提供について、医療機関等と合意する。			-	-	-	-	-
				Yes	対象外	①-9	ログの取得機能を有しない場合には、医療機関等と合意する。			-	-	-	-	-
				Yes	対象	①-10	医療情報システム等の保守に従事する者及び管理者権限を有する者が、その業務の目的で当該医療情報システム等にアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。			-	-	-	-	-
				Yes	対象	①-11	①-10で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。			-	-	-	-	-
				Yes	対象	①-12	医療情報システム等の保守において実施した操作結果について、操作ログ等により記録し、管理する。			-	-	-	-	-
				Yes	対象	①-13	取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。			-	-	-	-	-
				Yes	対象	①-14	ログを検証するため、利用者がアクセスした医療情報等を迅速に確認できるよう、利用者のIDと、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。			-	-	-	-	-
R22	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	低減	人的・組織的対策	Yes	-	-	-	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去されることを防止するため、医療機関等の職員への内部不正及びサイバー攻撃防止のための教育につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用する。 ・ログデータにアクセスする利用者及び操作を制限する。 ・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとる。 ・ログデータに対する不正な改竄及び削除行為に対する							-
R23	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができない。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	③-1	ログを利用して正確に事故原因等を検証するため、医療情報システム等のすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておく。							-
				Yes	対象外	③-2	医療情報システム等のすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。							-
				Yes	対象	③-3	ログの時刻の信頼性を確保するために、医療情報システム等の時刻と、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又はそれよりも多い頻度で行う。							-
R24	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できない。	低減	人的・組織的対策	Yes	-	-	-	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できないことを防止するため、医療情報システム等の提供事業者においてリモートメンテナンスが適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	④-1	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、医療情報システム等への不正な侵入が生じないよう安全管理措置を講じる。							-
				Yes	対象	④-2	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。							-
				Yes	対象	④-3	サービス提供に必要な医療情報システム等の保守をリモートメンテナンスで行う場合、医療機関等と合意する。							-
R25	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	低減	人的・組織的対策	Yes	対象	②-1	情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施する。	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じることを防止するため、医療情報システム等の提供事業者において保守作業が適切に実施されていることの必要に応じた確認や、医療情報システム等の保守にあたり医療機関等において対応が必要な作業の実施につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	②-2	保守業務における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。							-
				Yes	対象	②-3	保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
				Yes	対象	②-4	②-3に定めた手順を医療機関等に示し、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、医療機関等と合意する。							-
				Yes	対象	②-5	②-3で示された手順について、医療機関等が対応すべき事項がある場合、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R26	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	低減	人的・組織的対策	Yes	対象	③-1	サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、医療情報システム等を利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼすことを防止するため、医療情報システム等の提供事業者における受託した医療情報の返却に係る対応が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	③-2	③-1の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式）、返却方法、条件については、医療機関等と合意する。また医療機関等のサービス利用開始後に、医療機関等と合意した内容を変更する場合には、③-1に準じた対応策を							-
				Yes	対象	③-3	③-2におけるデータの返却については、厚生労働省ガイドライン第5版「5情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、受託事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合があるので、その旨も合わせて、医療機関等と合意する。							-
				Yes	対象	③-4	③-1においてサービスの変更を含む医療情報システム等の一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、③-2の対応は除く）、条件等について、医療機関等と合意する。							-
				Yes	対象	③-5	医療機関等の都合により医療機関等の医療情報システム等利用が終了する場合も、③-2、③-3に示す対応策を講じる。							-
				Yes	対象	③-6	③-1～③-5についての手順等を、運用管理規程等に含める。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R27	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	低減	人的・組織的対策	Yes	-	-	-	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用されることを防止するため、医事端末の定期的なソフトウェアアップデートにつきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	③-1	提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行う。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入する。							-
				Yes	対象	③-2	アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。							-
				Yes	対象	③-3	開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。 パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的な脆弱性検査を行							-
R28	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	低減	人的・組織的対策	Yes	-	-	-	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止することを防止するため、医療情報システム等の提供事業者における障害発生時のサービス継続を目的とする対策が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施する。							-
				Yes	対象	①-2	医療情報システム等、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。							-
				Yes	対象	①-3	①-2を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、医療機関等と合意する。							-
				Yes	対象	①-4	障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、医療機関等と合意する。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R29	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	低減	人的・組織的対策	Yes	-	-	-	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できないことを防止するため、医療情報システム等の提供事業者における障害発生時のサービス継続を目的とする対策が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	①-1	医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、医療機関等と合意する。							-
				Yes	対象外	①-2	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG及びPNG等のフォーマット）で外部ファイルに出力可能とすることなどの方策を講じる。							-
				Yes	対象外	①-3	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、医療機関等と合意する。							-
				Yes	対象外	①-4	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、医療機関等と合意する。							-
				Yes	対象外	①-5	緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等）をサービスに含め、これに必要なセキュリティ等の情報提供について、医療機関等と合意する。							-
				Yes	対象	①-6	障害等が生じた場合の役割分担を明確にした上で、稼動を保証するサービスの範囲について、医療機関等と合意する。							-
R30	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	低減	人的・組織的対策	Yes	対象	①-1	情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁･物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じることを防止するため、医療情報システム等の提供事業者において受託した情報の廃棄に関する対応が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	①-2	物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については受託事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得る。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。							-
				Yes	対象	①-3	①-1で講じる措置及び資料を提供するのに必要な条件等について、医療機関等と合意する。							-
				Yes	対象	①-4	医療情報システム等提供の停止又は医療機関等における医療情報システム等利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。							-
				Yes	対象	①-5	①-4に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R31	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	低減	人的・組織的対策	Yes	対象	①-1	サイバー攻撃等により、サービスの提供に支障が生じた場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられないことを防止するため、サイバー攻撃の発生を検知した場合における医療情報システム等の提供事業者への報告につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	①-2	サイバー攻撃等により、サービスの提供に支障が生じた場合において、医療機関等が行う必要のある所管官庁への連絡･報告のために提供する資料の範囲、条件等について、医療機関と合意する。							-
				Yes	対象	①-3	医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ･ストレージ等は国内法の執行が及ぶ場所に設置する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R32	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	低減	人的・組織的対策	Yes	対象	①-1	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竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられないことを防止するため、医療情報システム等の提供事業者におけるネットワーク機器の管理に関する対応が適切に実施されていることの必要に応じた確認や、医療機関等におけるネットワーク機器の適切な管理につきましては、医療機関等にて実施をお願	-	-	-	-	-	-
				Yes	対象外	①-2	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竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。							-
				Yes	対象	①-3	ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関する受託事業者の役割分担について、医療機関等と合意する。							-
				Yes	対象	①-4	回線の管理、品質等に対する受託事業者の責任の範囲、役割等について、医療機関等と合意する。							-
				Yes	対象	①-5	通常運用時及び非常時の医療機関等と受託事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11C項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、受託事業者の負う責任の範囲、役割等について、医療機関等と合意する。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
				Yes	対象	①-6	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。							-
				Yes	対象	①-7	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。							-
				Yes	対象	①-8	サービスにより管理する医療情報を患者等の閲覧に供する場合に、受託事業者において対応すべきセキュリティ上の措置の条件、内容等について、医療機関等と合意する。							-
				Yes	対象外	①-9	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。							-
				Yes	対象外	①-10	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R33	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	低減	人的・組織的対策	Yes	-	-	-	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じることを防止するため、医療機関等におけるネットワーク機器の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	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する。							-
				Yes	対象	①-2	ルータ等のネットワーク機器は、ISO/IEC15408で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。							-
R34	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受け	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	④-1	アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとる。							-
				Yes	対象	④-2	医療情報システム等の脆弱性に関する情報は、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し、確認する。							-
R35	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	低減	人的・組織的対策	Yes	-	-	-	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受けることを防止するため、医療情報システム等の提供事業者におけるオープンネットワーク上のサービスとの接続制限が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行う。							-
				Yes	対象	①-2	セキュリティゲートウェイでは、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（接続機器類のIPアドレスをプライベートアドレスとして設定して、ファイアウォール、VPN装置等のセキュリティゲートウェイを通過しようとするトラフィックをIPアドレスベースで制御する等）。							-
				Yes	対象	①-3	医療情報システム等において、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定する。他に必要なサービスがある場合には、医療機関等の合意を得てから利用する。 ・外部からの医療情報システム等の稼動監視・遠隔保守 ・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 ・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ファイル等のダウンロード ・電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ・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 ・時刻同期のための時刻配信サーバへのアクセス ・これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等）							-
R36	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	低減	人的・組織的対策	Yes	-	-	-	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われることを防止するため、医療情報システム等の提供事業者における情報交換に関する対応が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
			技術的対策	Yes	対象	②-1	次の情報交換方法について予め合意しておく。 ・情報を電子媒体に記録して交換する際の手順 ・情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ・情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ・情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順								-
				Yes	対象	②-2	情報交換手順では搬送の形態によらず次の事項を確実にする。 ・発送者、受領者を識別し記録する。 ・発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行う。 ・交換する情報の機密レベルに関して合意する（受領側で機密レベルが低くならないようにする）。 ・交換された情報に悪意のあるコードが含まれていないことを確実とする。								-
				Yes	対象	②-3	電子的に情報を転送する際には以下の対策を実施する。 ・送信者、受信者は相互に電子的に認証を行って相手の正当性を検証する。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 ・送受信する経路は適切な方法で傍受のリスクから保護されている。 ・受信した情報について経路途中での損傷、改竄が無いことを検証する対策を講じる。 ・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施す								-
				Yes	対象	②-4	医療機関等から受託事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。								-
				Yes	対象外	②-5	②-4において、医療機関等が外部接続するサーバ等と受託事業者のサーバとの間の相互認証を行う。								-
				Yes	対象外	②-6	②-4について、受託事業者が保守業務を再委託している場合には、受託事業者と再委託先との接続では、別途なりすましを防止する策を講じる。								-
				Yes	対象	②-7	厚生労働省ガイドライン第5版6.11C項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、医療機関等と合意する。								-
R37	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	低減	人的・組織的対策	Yes	-	-	-	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われることを防止するため、医療情報システム等の提供事業者における無線LAN利用に関するセキュリティ対策が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-								-
			技術的対策	Yes	対象	④-1	医療情報を取り扱うサービスの利用に際して、医療機関等が無線LANを利用する場合に必要なセキュリティ対策について、医療情報システム等事業者の役割分担等について、医療機関等と合意する。								-
				Yes	対象	④-2	業務上、医療情報システム等に関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。								-
R38	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-								-
			技術的対策	Yes	対象	①-1	医療機関等との接続ネットワーク境界には侵入検知システム（IDS）、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行う。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。								-
				Yes	対象	①-2	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								-
				Yes	対象	①-3	侵入検知システム等が、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とする。								-
				Yes	対象	①-4	侵入検知の記録には不正アクセス等の事後処理に必要な項目が含める。								-
				Yes	対象	①-5	医療情報システム等から、不正・不審なトラフィックが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が望ま								-
				Yes	対象	①-6	侵入検知システム自身が攻撃・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が望ましい。								-
				Yes	対象外	①-7	IoT機器の利用を含むサービスを提供する場合、IoT機器による医療情報システム等へのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。								-
R39	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	低減	人的・組織的対策	Yes	-	-	-	ネットワーク経路上の通信において、直接の傍受が発生することを防止するため、医療機関等における情報伝送に用いるケーブル類の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-								-
			技術的対策	Yes	対象	①-1	ネットワークにおいて、情報の盗聴、改竄、誤った経路での通信、破壊等から保護するために必要な措置（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。								-
				Yes	対象	①-2	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）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。								-
				Yes	対象外	①-3	経路の安全性確保のため、IPsec+IKEへの対応や閉域ネットワークへの対応等及びその条件等について、医療機関等と合意する。								-
				Yes	対象外	①-4	情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。								-
				Yes	対象	①-5	暗号アルゴリズムは十分な安全性を有するものを使用する。選択基準としては電子政府推奨暗号リスト等を用いる。								-
				Yes	対象	①-6	送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。								-
				Yes	対象	①-7	サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。								-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
				Yes	対象	①-8	①-7のほか、医療機関等がメールの暗号化（S/MIME等）やファイルの暗号化への対応を求める場合には、その対応に必要な措置及び条件等について、医療機関等と合意する。							-
				Yes	対象外	①-9	VPN接続を行う場合には以下の事項に従う。 ・接続時にVPN装置間で相互に認証を行う。 ・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。 ・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、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しない。 ・複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためVPNチャンネルを医療機関等別に構築する等の対策を実施する。							-
				Yes	対象	①-10	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は、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の高い「高セキュリティ型」に準じた適切な設定を行う。							-
				Yes	対象	①-11	SSL-VPNは、原則として使用しない。							-
				Yes	対象外	①-12	サービス提供に際して、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。							-
				Yes	対象	①-13	医療機関等における利用者がソフトウェア型の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の、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、医療機関等と合意する。							-
R40	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読もしくは偽装される。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	暗号鍵が漏洩した場合に備えた対応策を策定しておく。							-
				Yes	対象外	②-2	電子署名、ネットワーク接続等に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する。							-
				Yes	対象	②-3	暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮する。							-
				Yes	対象外	②-4	医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証する。							-
				Yes	対象	②-5	暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ま							-
				Yes	対象外	②-6	暗号鍵の生成は耐タンパー性を有するICカード、USBトークンデバイスといった安全な環境で実施することが望ましい。							-
				Yes	対象外	②-7	暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。							-
				Yes	対象外	②-8	電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できるようにすることが望ましい。							-
R41	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	リモートメンテナンスにより保守を行う場合、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の安全管理措置を講じる。							-
R42	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	低減	人的・組織的対策	Yes	対象外	①-1	医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われないことを防止するため、医事端末の定期的なソフトウェアアップデートにつきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象外	①-2	受託する医療情報を格納する機器･媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行う。							-
				Yes	対象	①-3	それぞれの装置は製造元又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。							-
				Yes	対象	①-4	情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。							-
				Yes	対象	①-5	医療情報システム等について、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。							-
				Yes	対象	①-6	医療情報システム等について、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行							-
				Yes	対象	①-7	①-6においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R43	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	低減	人的・組織的対策	Yes	対象	②-1	医療情報システム等の提供における業務プロセス及び医療情報システム等の優先順位にもとづいて、医療情報処理に関する事業継続計画を策定する。	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できないことを防止するため、医療情報システム等の提供事業者における事業継続計画に基づく対応が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	②-2	策定した事業継続計画について模擬試験を含めた適切な方法でレビューする。							-
				Yes	対象	②-3	事業継続計画について定期的に見直しを行う。							-
				Yes	対象	②-4	策定される事業継続計画には次のような事項を含むことが望ましい。 ・事前準備計画 ・「非常時」判断手順 ・関係者の召集、対応本部の設置 ・機器及び作業員の縮退措置及び代替施設の手配措置 ・バックアップ施設等、代替施設への切替え措置 ・代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等） ・障害の拡大範囲に関する判断手順、基準 ・正常復帰の判断手順、基準 ・正常復帰後の医療情報システム等の点検手順（不正侵入、情報改竄、情報破損等の検出等） ・所管官庁への連絡体制、等							-
				Yes	対象	②-5	策定した事業継続計画に基づくサービス内容について、医療機関等と合意する。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R44	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	③-1	非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規定等）を講じる。							-
R45	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	低減	人的・組織的対策	Yes	-	-	-	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用されることを防止するため、医療機関等の職員への内部不正防止のための教育につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	④-1	非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、医療機関等と合意する。							-
				Yes	対象外	④-2	非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。							-
				Yes	対象外	④-3	非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。							-
				Yes	対象外	④-4	非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。							-
R46	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・医療情報が保存されるサーバ機器等への不正アクセス							-
				Yes	対象	①-2	機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。							-
				Yes	対象	①-3	サーバ等を格納するラック等について、施錠管理を行う。							-
				Yes	対象外	①-4	媒体等を格納するキャビネット等について、施錠管理を行う。							-
				Yes	対象外	①-5	電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。							-
				Yes	対象	①-6	データセンターを運営する外部事業者が、自社専有の建物と同等な安全管理策を実施する等、受託事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認する。							-
				Yes	対象	①-7	医療情報システム等の設置されるサーバラックには施錠を行い、定められた受託事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行う。							-
				Yes	対象	①-8	受託事業者が医療情報システム等の設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録する。							-
				Yes	対象	①-9	データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム等、医療情報に影響を与えないことを確認する。							-
				Yes	対象	①-10	医療情報システム等であることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしない。							-
				Yes	対象外	①-11	医療情報システム等の設置されるサーバラックの施錠装置については、ハードウェアトークン又はICカード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。							-
				Yes	対象	①-12	受託事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認する。							-
				Yes	対象	①-13	機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。							-
				Yes	対象	①-14	①-1~①-13につき、運用管理規程等に規定する。							-
			技術的対策	Yes	-	-	-							-
R47	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	低減	人的・組織的対策	Yes	-	-	-	部外者の侵入への抑止や侵入による被害範囲の特定が困難となることを防止するため、医療機関等における物理的なセキュリティ対策の実施につきましては、医療機関等にて実施をお願い致しま	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施す。 ・建物、部屋に対する不正な物理的な侵入を抑止するた							-
				Yes	対象	①-2	防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。							-
				Yes	対象	①-3	機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、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。							-
				Yes	対象	①-4	サービスの運用･保守端末等を設置している区域は監視カメラ等により適切に監視を行う。							-
			技術的対策	Yes	-	-	-							-
R48	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	低減	人的・組織的対策	Yes	-	-	-	対象事業者の職員と部外者の見分けがつかず、侵入が容易となることを防止するため、医療機関等における物理的なセキュリティ対策の実施につきましては、医療機関等にて実施をお願い致しま	-	-	-	-	-	-
			物理的対策	Yes	対象	②-1	受託事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した受託事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、受託事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておく。							-
				Yes	対象	②-2	受託事業者の職員は、受託事業者の専有する領域にて、受託事業者の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。							-
				Yes	対象	②-3	職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、受託事業者の職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行う。							-
			技術的対策	Yes	-	-	-							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R49	物理的安全対策が手薄となったバックアップ施設へ侵入される。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	医療機関等に提供する医療情報システム等の継続に必要であれば、受託する医療情報のバックアップ施設等、医療情報システム等を継続するための代替情報処理施設を設置し、それらの施設に対しても物理的安全対策を施							-
			技術的対策	Yes	-	-	-							-
R50	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機員等の持ち込みが生じる。	低減	人的・組織的対策	Yes	-	-	-	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機員等の持ち込みが生じることを防止するため、医療機関等の職員への内部不正防止のための教育や、医療機関等における物理的なセキュリティ対策の実施につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	医療情報処理施設内への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。							-
				Yes	対象	①-2	機器や媒体の設置場所には、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。							-
			技術的対策	Yes	-	-	-							-
R51	個人情報が存在するPC等の重要な機器が盗難される。	低減	人的・組織的対策	Yes	-	-	-	個人情報が存在するPC等の重要な機器が盗難されることを防止するため、医療機関等における物理的なセキュリティ対策の実施につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	対象外	①-1	個人情報が存在するPC等の重要な機器には、盗難防止用チェーン等を取り付ける。							-
			技術的対策	Yes	-	-	-							-
R52	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	低減	人的・組織的対策	Yes	-	-	-	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じることを防止するため、医療情報システム等の提供事業者における機器や媒体を物理的に保存するための施設が適切に設置されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致しま	-	-	-	-	-	-
			物理的対策	Yes	対象	①-1	機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等、及び、それに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。							-
				Yes	対象	①-2	①-1の施設を設置する建築物について、医療機関等と合意する。							-
				Yes	対象	①-3	火災発生時の消火設備が機器に損傷を与えないよう配慮する。							-
				Yes	対象外	①-4	医療情報システム等を配置する室内での喫煙、飲食を禁止する。							-
				Yes	対象	①-5	医療情報システム等を配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮する。							-
				Yes	対象	①-6	医療情報システム等を設置するサーバラックについては以下の安全管理策を実施する。 ・震災時に転倒することが無いよう確実に設置する。 ・熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されている。 ・扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。							-
			技術的対策	Yes	-	-	-							-
R53	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	低減	人的・組織的対策	Yes	-	-	-	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できないことを防止するため、医療情報システム等の提供事業者における法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存が適切に実施されていることの必要に応じた確認につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	⑤-1	取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するログ又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。							-
				Yes	対象外	⑤-2	法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、医療機関等と合意する。なお、本項におけるログの管理方法について保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。							-
R54	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	低減	人的・組織的対策	Yes	-	-	-	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われることを防止するため、医療機関等における情報伝送に用いるケーブル類の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	③-1	ネットワーク機器及びサーバ、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。							-
				Yes	対象	③-2	不正な装置を識別するため、医療情報システム等内で利用する情報処理装置を登録したリストを作成・維持する。							-
				Yes	対象	③-3	不正な情報処理装置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、脆弱性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運用する。							-
R55	紛失・盗難した機器が起動され、機器を不正に利用される。	低減	人的・組織的対策	No	-	-	-	-	-	-	-	-	-	-
			物理的対策	No	-	-	-							
			技術的対策	No	対象外	①-1	機器等については、起動パスワードの設定を行う。							
				No	対象外	①-2	起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。							
				No	対象外	①-3	医療情報システム等に関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。							

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R56	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	低減	人的・組織的対策	Yes	-	-	-	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じることを防止するため、医療機関等における物理的なセキュリティ対策の実施につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							
			技術的対策	Yes	対象	②-1	情報を格納する機器･媒体等を持ち出す場合の手順には、機器･媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。						
R57	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	低減	人的・組織的対策	Yes	-	-	-	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じることを防止するため、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	利用者が個人所有する機器による医療情報システム等利用に関する対応策について、医療機関等と合意する。なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏洩等を防止する観点から、例えば、仮想デスクトップを用いてOSレベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。						-
				Yes	対象	①-2	サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは原則禁止とする。						-
R58	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	低減	人的・組織的対策	Yes	-	-	-	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じることを防止するため、必要に応じた医事端末の作業環境に対する仮想デスクトップ等の技術導入につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するための受託事業者の役割分担等につき、医療機関等と合意する。						-
R59	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	低減	人的・組織的対策	No	-	-	-	-	-	-	-	-	-	-
			物理的対策	No	-	-	-							
			技術的対策	No	対象外	①-1	医療情報システム等においてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除する。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。						
				No	対象外	①-2	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ことが望ましい。						
R60	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	低減	人的・組織的対策	Yes	対象	①-1	医療情報システム等へのアクセス制限、記録、点検等を定めたアクセス管理規定を作成し、医療機関等の求めに応じて提出できる状態にしておく。	権限のない第三者や内部不正による不正な閲覧や操作が行われることを防止するため、患者等による画面の覗き見防止のための医事端末のレイアウト調整や、医療機関等の職員への内部不正防止のための教育につきましては、医療機関等にて実施をお願い致し	-	-	-	-	-	-
				Yes	対象	①-2	アクセス管理規定には以下の内容を含める。 ・アクセス権限、アカウント管理における登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセス ・認証及びアクセス等に対する記録の収集と保存 ・認証及びアクセス等に対する記録の定期的なレビュー ・アクセス管理の運用状況に関する定期的なレビューの実施						-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R61	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	低減	人的・組織的対策	Yes	対象	②-1	持ち出した機器を外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改竄が生じないようにするための具体的な措置（不正プログラム対策、暗号化、ファイアウォール導入等））を運用管理規程に含める。	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染することを防止するため、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R62	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	低減	人的・組織的対策	Yes	対象	④-1	受託する個人情報を運用や保守に用いる端末に原則保存しない旨、自社の運用管理規程等に定める。	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大することを防止するため、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象外	④-2	医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等又は受託事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。						-
				Yes	対象外	④-3	④-2で定める手順及び情報の提供条件について、医療機関等と合意する。						-
				Yes	対象外	④-4	持ち出した機器を再度設置するための適切な検証手順を策定する。						-
				Yes	対象外	④-5	保守点検で障害不良等が発見された際の対応作業等を行う際には受託事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにする。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出す。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択す						-
				Yes	対象外	④-6	持ち出し手順に含まれる事項には次のようなものが考えられる。 ・装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等） ・申請承認プロセス ・返却確認プロセス、等。						-
				Yes	対象外	④-7	返却時の検証手順に含まれる事項には次のようなものが考えられる。 ・装置の動作確認 ・盗聴装置等、情報の安全性を脅かす装置の有無 ・悪意のあるプログラムの検出作業 ・収められている情報の検証作業（不正な改竄等）、						-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R63	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	低減	人的・組織的対策	Yes	対象	⑤-1	サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩することを防止するため、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	⑤-2	⑤-1における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。							-
				Yes	対象	⑤-3	⑤-1で定める内容について、医療機関等と合意する。							-
				Yes	対象外	⑤-4	電子媒体について受託事業者施設外への不要な持ち出しを行わない。CD、DVD、MO等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R等）を用い、情報交換作業終了後、電子媒体を確実に廃棄処分す							-
				Yes	対象外	⑤-5	情報交換目的やバックアップ目的でMT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行う。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行う。							-
				Yes	対象外	⑤-6	全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行う。							-
				Yes	対象	⑤-7	記録媒体･記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体･記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等 （「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器･媒体等の盗難･紛失（持ち出し時の機器･媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の							-
				Yes	対象	⑤-8	⑤-7の内容に関する教育を従業員等に対して行う。							-
				Yes	対象	⑤-9	⑤-7の内容を含む運用管理規程については、再委託先に対しても遵守等を求める。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R64	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	低減	人的・組織的対策	Yes	対象	⑥-1	情報処理装置及びソフトウェアの適切な変更手順を策定する。原則、保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受ける。	-	-	-	-	-	-	-
				Yes	対象	⑥-2	機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。							-
				Yes	対象	⑥-3	機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。							-
				Yes	対象	⑥-4	医療情報システム等に係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。							-
				Yes	対象	⑥-5	変更手順に含まれる事項には次のようなものが考えられる。 ・変更についての影響が及ぶ関係者への通知プロセス ・装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等）申請承認プロセス変更試験プロセス ・変更作業に支障が発生した場合の復旧手順変更終了確認プロセス ・変更に伴う影響を監視するプロセス、等。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R65	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	低減	人的・組織的対策	Yes	対象	①-1	医療情報を操作する可能性のある受託事業者の職員全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める。派遣従業員については守秘義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われることを防止するため、医療機関等の職員への内部不正防止のための教育につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	①-2	医療情報を操作する可能性のある受託事業者の職員（派遣従業員含む）については、守秘義務に関する内容を就業規則等に含める。							-
				Yes	対象	①-3	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておく。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求める。派遣従業員については、派遣契約解除時に同等の合意書への署名を求							-
				Yes	対象	①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。							-
				Yes	対象	①-5	上記に違反した受託事業者（派遣従業員含む）の職員に対して、適切な懲戒手続きを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。定めた懲戒手続きについては各職員に周知し、理解したことの確認							-
				Yes	対象	①-6	医療情報を操作する受託事業者の職員（派遣従業員含む）に対する教育･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の提供について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R66	医療情報システム等提供に係る事業者（再委託先も含む）による故意又は過失による情報漏洩が行われる。	低減	人的・組織的対策	Yes	対象	②-1	医療情報システム等に係る情報及び受託した情報に関する守秘義務について、医療情報システム等提供に係る契約に含める。契約には、守秘義務に違反した受託事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含め	医療情報システム等の提供に係る事業者（再委託先も含む）による故意又は過失による情報漏洩が行われることを防止するため、医療機関等の職員への内部不正防止のための教育や、医療機関等におけるセキュリティインシデント防止のための教育につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	②-2	医療情報システム等の動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、守秘義務が課された要員･委託先等により動作確認を行う旨を含めた手順を定める。							-
				Yes	対象	②-3	医療情報システム等の動作確認に際し、受託した個人情報をやむを得ず使用する場合について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R67	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生する。	低減	人的・組織的対策	Yes	対象	①-1	医療情報を操作する可能性のある受託事業者の職員の全てに個人情報保護及び情報セキュリティに関する教育を行い、一定水準の理解を得た職員だけを業務に従事させる。	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生することを防止するため、医療機関等におけるセキュリティインシデント防止のための教育につきましては、医療機関等にて実施をお願い致	-	-	-	-	-	-
				Yes	対象	①-2	派遣従業員に関しては、派遣元に対し、個人情報保護及び情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行う。							-
				Yes	対象	①-3	この教育は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。							-
				Yes	対象	①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）の退職時又は契約終了時以降の守秘義務について、教育･訓練に含める。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R68	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	低減	人的・組織的対策	Yes	対象	①-1	受託事業者の職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改竄又は破壊等の行為が行われていないことを検証する。	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行うことを防止するため、医療機関等の職員への内部不正防止のための教育や、医療機関等におけるセキュリティインシデント防止のための教育につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	①-2	医療情報システム等の保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、医療機関等と合意する。							-
				Yes	対象	①-3	保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、医療機関等と合意する。							-
				Yes	対象外	①-4	医療情報システム等の保守業務を医療機関等の施設内で行う際の対応について、医療機関等と合意する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R69	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	低減	人的・組織的対策	Yes	対象	①-1	情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、合意を得る。また、当該再委託に係る契約において体制を明確にする。	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生することを防止するため、委託元である医療機関等における監督義務の履行につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
				Yes	対象	①-2	再委託先には、自社と同等の個人情報保護指針等を遵守させる。							-
				Yes	対象	①-3	再委託に係る契約に、委託業務に係る守秘義務を含める。							-
				Yes	対象	①-4	再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。							-
				Yes	対象	①-5	医療情報システム等の保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、医療機関等と合意する。							-
				Yes	対象	①-6	医療情報システム等の保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。							-
				Yes	対象	①-7	①-6の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。							-
				Yes	対象	①-8	再委託先により提供される医療情報システム等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する。							-
				Yes	対象	①-9	再委託先による医療情報システム等の実施、運用、維持について定期的に検証する。							-
				Yes	対象	①-10	再委託先による医療情報システム等の実施、運用、維持について定期的サービス実施について事前、事後報告を義務づけ、報告内容を点検確認する。							-
				Yes	対象	①-11	再委託先による医療情報システム等を実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れない。							-
				Yes	対象	①-12	医療情報システム等の実施中に再委託先が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯する。							-
				Yes	対象	①-13	再委託先による医療情報システム等の実施にともなう処理施設内への立ち入り手順に関しては、受託事業者の職員の入室、退室手順に準ずる。							-
				Yes	対象	①-14	再委託先による医療情報システム等の変更時には、引き続き安全性が維持されていることについて適切な検証を行う。							-
				Yes	対象	①-15	医療情報システム等の保守点検作業を外部事業者に委託する場合には、「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」6.8章C項の管理策を実施する。							-
				Yes	対象	①-16	外部事業者が医療情報システム等を実施する際は、受託事業者又は外部事業者の正規職員が管理している状況で作業を行うことが望ましい。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否 (Yes/No)	要求事項に対する適合判断 (対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R70	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	低減	人的・組織的対策	Yes	対象	①-1	医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別する。	-	-	-	-	-	-	-
				Yes	対象	①-2	業務プロセス間の相互関係を評価する。							-
				Yes	対象	①-3	事業を継続するための業務プロセスの優先順位を明確にする。							-
				Yes	対象	①-4	医療情報システム等に発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別する。							-
				Yes	対象	①-5	医療情報システム等に発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別する。							-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	-	-	-							-
R71	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	低減	人的・組織的対策	Yes	-	-	-	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作されることを防止するため、患者等による画面の覗き見防止のための医事端末のレイアウト調整や、医事端末の適切な管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	医療情報システム等にて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行う。							-
				Yes	対象	①-2	医療情報システム等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（複数の利用者によるIDの共同利用は行わない。ただし当該医療情報システム等が他の医療情報システム等を利用するためのID（noninteractiveID）は除く）。							-
				Yes	対象	①-3	利用者のなりすまし等を防止するための認証を行う。							-
				Yes	対象	①-4	医療情報システム等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。							-
R72	一般利用者の権限が高いため、任意のソフトウェアのインストール、持込機器接続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	低減	人的・組織的対策	Yes	-	-	-	一般利用者の権限が高いため、任意のソフトウェアのインストール、持込機器接続、持込Wi-Fiの接続等をされ、不正アクセスを誘発することを防止するため、医療機関等における医事端末の操作に関するアクセス制御方針に沿った職務分掌の履行につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	医療情報システム等の操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、閲覧、編集、削除等を防止する。							-
				Yes	対象	①-2	医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。							-
				Yes	対象	①-3	医療情報システム等の構成要素（情報処理装置、ソフトウェア）それぞれのアクセス管理に係るセキュリティ要求事項を整理する。							-
				Yes	対象	①-4	それぞれの情報にアクセスする権限を持つ利用者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行う。							-
				Yes	対象	①-5	業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定する。							-
				Yes	対象	①-6	定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。							-
				Yes	対象	①-7	予定された保守･運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。							-
				Yes	対象	①-8	システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。							-
R73	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等に不具合が生じる。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	医療情報システム等に関連する技術的脆弱性については台帳等を利用して管理する。							-
				Yes	対象	②-2	潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定する。							-
				Yes	対象外	②-3	修正パッチの適用前にパッチが改竄されていないこと及び有効性を検証する。							-
				Yes	対象外	②-4	オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システム等に対する影響を評価し、試験結果を確認してから実施する。							-
R74	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	①-1	不正な改竄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（改竄検知）を実施する。							-
				Yes	対象	①-2	不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改竄防止、検知策を実施する。							-
R75	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできな	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	①-1	医療情報システム等には、受託する医療情報を患者等ごとに管理できる機能を含める。							-

リスク対応一覧

特定したリスクシナリオ		リスク対応策						医療機関等へ対応を求める事項	残存するリスク					
リスクID	リスクシナリオ	リスク対応の選択肢	リスク対応の観点	リスクに対する対応要否(Yes/No)	要求事項に対する適合判断(対象/対象外)	要求事項No.	要求事項の内容	医療機関等の運用管理規程に定める必要がある事項	第三者評価を踏まえた残存リスクのリスクシナリオ	深刻度	発生頻度	リスクレベル	残存リスクへの対応計画	
													基本方針	LineICa8
R76	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支障が生じる。	低減	人的・組織的対策	No	-	-	-	-	-	-	-	-	-	-
			物理的対策	No	-	-	-							-
			技術的対策	No	対象外	①-1	医療機関等が医療情報システム等を利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、医療機関等と合意する。							-
R77	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じる。	低減	人的・組織的対策	Yes	-	-	-	-	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象	②-1	診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。							-
R78	情報が毀損や滅失した場合にバックアップされたデータを用いて元の状態に復元できない。	低減	人的・組織的対策	Yes	-	-	-	情報が毀損や滅失した場合にバックアップされたデータを用いて元の状態に復元できないことを防止するため、バックアップを用いて元の状態に復元するために利用可能な資源の管理につきましては、医療機関等にて実施をお願い致します。	-	-	-	-	-	-
			物理的対策	Yes	-	-	-							-
			技術的対策	Yes	対象外	①-1	電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管する。							-
				Yes	対象外	①-2	各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。							-
				Yes	対象外	①-3	医療機関等が医療情報システム等を利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、医療機関等と合意する。							-
				Yes	対象	①-4	医療情報システム等が情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。							-
				Yes	対象外	①-5	①-4において、他の事業者が提供する医療情報システム等を利用する場合においても、同様の情報を収集して、対応する。仮想化技術による医療情報システム等を利用する場合には、受託事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。							-
				Yes	対象	①-6	①-4により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。							-
				Yes	対象	①-7	医療情報システム等に係る委託先に対しても、①-4の運用管理規程に定める管理方法への対応等を求める。							-
				Yes	対象	①-8	情報が毀損した場合、速やかに回復するための措置を講じ、その内容・手順等について、運用管理規程等に含める。							-
				Yes	対象	①-9	①-8に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。							-
				Yes	対象	①-10	①-9で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、医療機関等と合意する。							-
				Yes	対象	①-11	リスク分析結果に基づき医療情報システム等のバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。							-
				Yes	対象	①-12	取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改竄・破壊等がないことを確認する。							-
R79	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	低減	人的・組織的対策	No	-	-	-	-	-	-	-	-	-	-
			物理的対策	No	-	-	-							-
			技術的対策	No	対象外	②-1	記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。							-
				No	対象外	②-2	バックアップの記録媒体の使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。							-
				No	対象外	②-3	製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、別の媒体等に複写する。							-
				No	対象外	②-4	②-1～②-3の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。							-
				No	対象外	②-5	バックアップに係る情報の提供について、医療機関等と合意する。							-
R80	医療情報システム等を更改等により移行する際、移行元で記録された情報が移行後に正しく読みだせない。	低減	人的・組織的対策	No	-	-	-	-	-	-	-	-	-	-
			物理的対策	No	-	-	-							-
			技術的対策	No	対象外	①-1	診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。							-
				No	対象外	①-2	厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、医療機関等と合意する。							-
				No	対象外	①-3	医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を医療情報システム等に備える。							-
				No	対象外	①-4	①-3に示す機能等を備えることが困難な場合の医療情報システム等更新・移行の手順について、医療機関等と合意する。							-
				No	対象外	①-5	医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートする。							-
				No	対象外	①-6	データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。							-
				No	対象外	①-7	①-6の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行							-
				No	対象外	①-8	①-7は、他の医療情報システム等とのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、医療機関等と合意する。							-
				No	対象外	①-9	データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、見読性確保の対策を講じる。							-
				No	対象外	①-10	医療情報システム等に関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。							-
				No	対象外	①-11	他の事業者が提供する医療情報システム等を用いて、サービスを提供する場合には、他の事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他の事業者のサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、機器の劣化対策を講じる。							-
				No	対象外	①-12	医療情報システム等に係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他の事業者のサービスの変更を行う場合には、①-10、①-11を考慮して行う。							-