整理番号		評価対象プロダクト名	

項番			大分類	中分類	要件	確認項目	主な要素	評価基準
大分類	中分類	小分類						
1								
	1	1	サービス全体	サービス内容	サービス内容の確認	サービスの実施する内容について、サービス仕様に明記されており、サービスを利用する契約者と確認していること	契約書 サービス仕様書 サービス説明書	サービス提供に際して、サービスの内容について契約者の同意を得るために書面で明確にしていること
		2			サービス内容の法令順守	サービスの実施する内容について、法令並びに業界標準に沿ったものであることについてサービス仕様に明記されており、サービスを利用する契約者と確認していること	契約書	サービス提供に際して、仕様/規約について契約者の同意を得るために書面で明確にしていること
		3			サービス内容に関わる第三者の明確化	サービス内容に関わる第三者（サービス連携先、業務委託先）とのかかわり方(委託、第三者提供)についてサービス仕様に明記されており、サービスをりようする契約者と確認していること	契約書	サービス提供に際して契約書/利用申込書に、サービス内容に関わる第三者（サービス連携先、業務委託先）が洗い出されており、第三者とのかかわり方(委託、第三者提供)と契約内容について契約者の同意を得るために書面で明確にしていること
		4			サービスに関わる権限の管理の実施	サービスに関わる権限が適切に設定され管理されていることについて、サービス仕様に明記されており、契約者と確認していること	契約書 サービス仕様書	サービス提供に際して、役割と実施範囲について契約者の同意を得るために書面で明確にしていること
		5			サービス内容変更時の対応について明確になっている	サービス内容が変更になる際の契約者への対応について、サービス仕様に明記されており、契約者と確認していること	契約書	サービス内容が変更になる際の対応について契約者の同意を得るために書面で明確にしていること
	2	1		サービス仕様	医療機関とサービス提供機関との責任分界点の明確化	サービスにおける責任分界点および分界点からの責任範囲がサービス仕様として明記されており、サービス提供側、受益側の双方が了解していること （責任分界点は、物理的な分界点とする）	契約書 サービス仕様書 サービス説明書	サービスにおいて、契約者との責任分界点および分界点からの責任範囲について契約者の同意を得るためにサービス仕様として書面で明確にしていること
		2			（サービス提供機関において、サービスを連携させる場合） サービス連携先との責任分界点の明確化 ※主に接続提供サービス事業者とASP等のサービス提供機関において実施される	サービスにおける責任分界点および分界点からの責任範囲がサービス仕様として明記されており、サービス提供側、サービス連携先の双方が了解していることについて、契約者と確認していること （責任分界点は、物理的な分界点とする）	契約書 サービス仕様書 サービス説明書	サービスにおいて、サービス連携先との責任分界点および分界点からの責任範囲について契約者の同意を得るためにサービス仕様として書面で明確にしていること
	3	1		情報の管理	顧客情報の管理	サービス提供に際して受け取る顧客情報について適切に管理されていること	契約書	サービス提供に際して、受け取る顧客情報についての扱いについて契約者の同意を得るために書面で明確にしていること
	4	1		事業継続性	障害時の体制の明確化	システム障害や自然災害等によりサービスが停止し、業務が中断する状態が起こった際の体制が構築され、連絡先並びに責任者についてサービス仕様に明記されており、契約者と確認していること	契約書 サービス仕様書 サービス説明書	サービス提供に際して、障害発生時の連絡先並びに責任者について契約者の同意を得るために書面で明確にしていること
		2			障害時の対策方針の明確化	システム障害や自然災害等によりサービスが停止し、業務が中断する状態が起こった際の復旧・管理方針についてサービス仕様に明記されており、契約者と確認していること	契約書 サービス仕様書 サービス説明書	サービス提供に際して、障害発生時の対応方針について契約者の同意を得るために書面で明確にしていること
		3			障害時の対策の明確化	システム障害や自然災害等によりサービスが停止し、業務が中断する状態が起こった際の復旧・管理策について定められていること	事業継続対策書	サービス提供事業者として、障害時の対策について書面で明確にしていること
	5	1		運用	サービスの状態を監視する	サービスに対して必要となる監査ログが取得できること	運用仕様書 サービス仕様書	監査ログによって利用者からのサービス利用履歴が取得可能なこと 監査ログ等の取得によりトラブルシューティグができるような仕組みを整えていること
		2			システム障害防止のための設備管理	システム障害からの被害を最小限に抑えるため、守るべき設備要件を整え、管理を行うこと	事業継続対策書 サービス仕様書	運用マニュアル等が整備されており、守るべき設備について明記され、設備の運用管理体制が明確になっていること
		3				速やかなサービス復旧を目的とした事前対策としてバックアップを行うこと	運用仕様書 サービス仕様書	速やかなサービス復旧を目的とした事前対策としてバックアップを実施することに対して明記されており、適切な運用管理がなされていること
		4				ログ、バックアップ等について、対象、保管場所、保管期限、世代管理を定めて保管してあり、保管期限終了後は適切に削除されていること	運用仕様書 サービス仕様書	.運用規約が整備され、データ保全等についての明確に規定されていること .運用マニュアル等が整備され、ログ、バックアップ等について対象、保管場所、保管期限、世代管理についての規定がされていること 不要データの廃棄についての規約が明確であり、適切に運用されていること

整理番号		評価対象プロダクト名	

項番			大分類	中分類	要件	確認項目	主な要素	評価基準
大分類	中分類	小分類						
2								
	1	1	サービス拠点(今回は中継接続拠点のことを指す)	サービス拠点の物理セキュリティ	入館に対する制限	サービスを提供する拠点に対して、入館する際に制限が行われていること	ビル入管規程 運用仕様書	拠点の入館/作業について、明確な規約があり、入館者の履歴/作業項目が管理されていること 可搬媒体等を持込／持出については原則禁止とし、やむをえず実施する場合は、管理者の許可を取り、履歴を取るように管理されていること 作業者は個人認証を受けること
		2			領域に対する入室管理	サービス拠点内について、領域が定められており、サービス仕様に基づく権限に応じた領域内への立ち入りについて管理されていること	ビル入管規程 運用仕様書	拠点内についてエリアが定めており、立ち入る人について制限をかけ管理されていること エリアに対して立ち入りを行う際には履歴／作業項目が管理してあること 作業者は個人認証を受けること
		3			システムの設置場所	システムを設置する環境として、物理的に隔離されており、管理権限を持った者のみが扱えるようになっていること	ビル入管規程 運用仕様書	システムが設置する場所について、施錠管理されたエリアに配置してあり、管理権限を持った者により管理されていること システム機器が格納されたラックは施錠管理され、管理権限を持った者により管理されていること ラックの開錠/ラック内の機器に対する作業/ラックの施錠等についての履歴/作業項目が管理されていること 作業者は個人認証を受けること
	2	1		サービス拠点の技術セキュリティ（ネットワーク）	サービス拠点内のネットワークの構成	サービス拠点内においてサービス提供のためのネットワークとその他のネットワークについて分離していること	サービス仕様書 ネットワーク構成図	提供サービス以外のサービスに対して、ネットワークセグメントが分離されていること
		2			提供サービス毎の脅威拡散防止のための通信経路の分離	（サービス拠点で複数のサービスを提供している場合） 脅威拡散防止のため、提供サービス毎の通信経路を分離していること	サービス仕様書 ネットワーク構成図	提供サービス毎に接続分解点を明確し、ネットワークセグメントについて分離され、相互に影響を及ぼさない構成になっていること
		3			サービス拠点内でのHigh Secure Areaを接続の起点としたアクセス	High Secure Areaからの他のAreaに対するサービス拠点内部での通信を原則禁止すること やむを得ず通信を行う場合は、内部プロキシ等の機能を用い、アクセス元／先並びに通信内容について特定可能にしてあること	サービス仕様書 ネットワーク構成図	サービス拠点内では他のAreaとの通信を原則禁止すること やむを得ず通信を行う場合は、内部プロキシ等の機能を用い、アクセス元／先並びに通信内容について特定可能にしてあること
		4			サービス拠点内のHigh Secure Areaを起点とした外部への接続	High Secure Areaからの外部に対する通信を原則禁止すること やむを得ず通信を行う場合は、改ざんや侵入から守るため、外部への接続に対してセキュリティ機能を整備し、対策を実施すること また、内部プロキシ等の機能を用い、アクセス元／先並びに通信内容について特定可能にしてあること	サービス仕様書 ネットワーク構成図	High Secure Areaからの外部に対する通信を原則禁止すること やむを得ず通信を行う場合は、改ざんや侵入から守るため、外部への接続に対してセキュリティ機能を整備し、対策を実施すること また、内部プロキシ等の機能を用い、アクセス元／先並びに通信内容について特定可能にしてあること
	3	1		サービス拠点の技術セキュリティ（ネットワーク）	他拠点との接続合意がされていない通信	他拠点と接続の合意がとれている通信のみを許可し、合意の無いアクセスを禁止していること	サービス仕様書 ネットワーク構成図	他拠点と接続の合意がとれている拠点／端末同士の通信のみを許可し、合意の無いアクセスを禁止していること
		2			サービス提供を受けるユーザの認証	不正ユーザによる侵入・情報漏えいを防止するため、サービスの提供を受けるユーザの認証を実施していること	サービス仕様書 ネットワーク構成図	不正ユーザによる侵入・情報漏えいを防止するため、サービスの提供を受けるユーザの認証を実施していること
		3			他拠点またはインターネットからの不正アクセス、不正侵入、情報漏えい等の脅威への防御対策	他拠点またはインターネットへの接続境界に防御装置を設置し、不正アクセス等のサービス妨害行為から防御すること また、サービス拠点の内部ネットワークに防御装置を設置することで、外部からの不正アクセス、不正侵入等を監視し、ウィルスによる脅威を未然に防止すること	サービス仕様書 ネットワーク構成図	サービス提供の接続境界点に、適切な不正アクセス防御装置が実装されていること
		4			インターネットなどの外部からの攻撃（DoS的攻撃・不正形式パケットなど）の検知	ファイアウォール等のセキュリティ機器による対策がなされ、ポリシー設定が適切に行われているかを確認すること	サービス仕様書 ネットワーク構成図	サービス提供の接続境界点に外部からの攻撃に対し、適切な防御装置が実装されていること
	4	1		サービス拠点の技術セキュリティ（ネットワーク）（監視）	ファイアウォールやプロキシなどの外部と直接接続している装置でのロギングによるアクセス監視の実施	外部ネットワークからの接続に関して、ログを取得する仕様となっており、監査またはユーザからの提供要請に応じることが常に可能であること	運用仕様書 ネットワーク構成図	外部と直接接続されている装置ではアクセス状況を常時監視し、ログを取得できること 監査またはユーザからの要求があった場合、必要に応じて、取得したログの分析結果を提供できること
	5	1		サービス拠点の技術セキュリティ（端末、サーバ）	サービス拠点内におけるセキュリティパッチなどの更新機能の実装	サービス拠点を構成するサーバ/端末などに対しては、適切にセキュリティー更新が実施され、セキュリティホールに対する攻撃の対策が実施ていること。	運用仕様書 ネットワーク構成図	サービス拠点を構成するサーバ/端末について、必要なセキュリティーパッチを実施していること セキュリティーパッチについて、インターネットより直接ダウンロードせずに、間接的に配布すること

整理番号		評価対象プロダクト名	

項番			大分類	中分類	要件	確認項目	主な要素	評価基準
大分類	中分類	小分類						
3								
	1	1	接続サービス	サービス内容	接続先拠点との通信に関する合意	合意された内容に沿った通信の設定がされていること 通信の合意をしていない拠点との通信やアクセスができないようになっていること	サービス仕様書	合意された内容に沿った通信の設定がされていること 通信の合意をしていない拠点や端末との通信やアクセスができないようになっていること
		2			サービス内容に関する責任分界点の明確化	通信する内容に対して、暗号化などのセキュリティ対策を契約者側で対応することについてサービス仕様に明記されており、契約者と確認していること	契約書 サービス仕様書 サービス説明書	サービス仕様において、通信路に流すデータに対して暗号化を行うことについて、要求事項として契約者の同意を得るためにサービス仕様として書面で明確にしていること
		3			サービス利用に関する禁止事項の明確化	サービス利用時の禁止事項について、利用者に対して要求事項として、 サービス仕様に明記されており、契約者と確認していること	契約書 サービス仕様書 サービス説明書	サービス仕様において、サービス利用時の禁止事項について、要求事項として契約者の同意を得るためにサービス仕様として書面で明確にしていること
		4			医療機関内のセキュリティ対策の必要性の説明責任	医療機関のセキュリティを守るために終端装置の設置個所から医療機関外までのセキュリティ対策を別途行う必要があることがサービス仕様に明記されており、契約者と確認していること (終端装置とそれに接続される機器の安全管理を含む)	契約書 サービス仕様書 サービス説明書	医療機関のセキュリティを守るために終端装置の設置個所から院外までのセキュリティ対策を別途行う必要があることがサービス仕様に明記されており、契約者の同意を得ていること
		5			ロギングを行いアクセスを監視する	接続サービスとしてアクセスログを取得する仕様となっており、監査または ユーザからの提供要請に応じることが常に可能であること またユーザからの要求に応じて、ログの解析結果を提供できること	運用仕様書 サービス仕様書	通信変換拠点においてアクセスログを取得し、トラブルシューティングが可能な仕組みを有していること 終端装置においてログ機能等を用い、トラブルシューティングが可能な仕組みを有していること ユーザからの要求に応じて、監査ログの内容を要求できることが明示されていること また、ログを取得した場合、ログ内部に平文の通信内容が含まれないこと
	2	1		終端装置のセキュリティ (セキュリティを確保するための通信路を確立する装置)	終端機器の設定変更／改ざんへの対策	管理権限を持つもののみが終端装置の設定を変更可能にするために、終端装置に対する権限管理を行うこと （接続されるシステムおよび外部ネットワークからの攻撃に対する対策を含む）	サービス仕様書 終端装置仕様書 運用仕様書	管理者権限を持つもののみが設定変更可能にしてあること
		2			導入環境に対する要求事項の確認	終端装置を導入する際に、サービスとしての使用環境に対する要求事項に対して、契約者と確認していること	契約書 サービス仕様書 サービス説明書 運用仕様書	サービス仕様書に使用環境に対する要求事項(環境、運用)について契約者の同意を得るために書面で明確にしていること
		3			複数の異なる法人拠点間の不正中継に対する対策	終端装置をハブとして二つ以上の拠点を接続をする場合、保有するアプライアンスを経由して接続先拠点間で不正なアクセスや中継が行われないように経路を設定すること インシデントが発生した場合の脅威の拡散を防ぐために、サービスの同時利用を禁止していること	サービス仕様書 終端装置仕様書 ネットワーク構成図	終端装置をハブとして、他拠点への通信並びに他のサービス中継が行われないことについて、契約者の同意を得るためにサービス仕様として書面で明確にしていること
		4			終端装置のスルーモードの禁止	通常の使用状態でインターネット側と接続システムが直接接続されるないこと	サービス仕様書 終端装置仕様書 ネットワーク構成図	直接の回線が防御されていること
		5			接続サービスを利用するユーザの認証機能	不正ユーザによる侵入・情報漏えいを防止するため、サービス提供を受けているユーザを認証し、アクセスコントロールを行うこと	サービス仕様書 終端装置仕様書 ネットワーク構成図	不正ユーザによる侵入・情報漏えいを防止するため、サービス提供を受けているユーザを認証し、アクセスコントロールを行うこと
		6			通信合意に対するアクセスコントロールを行う	通信の合意をしていない拠点との通信やアクセスができないようになっていること	サービス仕様書 終端装置仕様書 ネットワーク構成図	合意された内容に沿った通信の設定がされていること 通信の合意をしていない拠点／端末との通信やアクセスができないようになっていること
	3	1		通信変換拠点内での管理	通信変換拠点内での通信	(通信変換拠点がある場合) 通信変換拠点内での終端装置から終端装置までの通信について HighSecureArea内で通信を行うこと	サービス仕様書 ネットワーク構成図	通信変換拠点内での通信がHighSecureArea内で行われていること
	4	1		接続の方式 （オープンネットワーク） ・インターネット ・情報スーパーハイウェイ等 ・複数の法人で共用している閉域網等	IKEのバージョン	現在有効なRFCに基づくIKEを採用していること	サービス仕様書 終端装置仕様書	IKEv2を利用していること
		2			IKEでの暗号アルゴリズム	安全性を認められた暗号アルゴリズムを採用していること	サービス仕様書 終端装置仕様書	AES-GCM, AES-CTR, AES-CBC, AES-CCM (128, 192, 256-bit keys)のいずれかを採用していること
		3			IKEでの整合性アルゴリズム/擬似ランダム関数	安全性を認められた整合性アルゴリズム/擬似ランダム関数を採用していること	サービス仕様書 終端装置仕様書	HMAC-SHA256以上の安全性のある方式を採用していること
		4			IKEでの鍵交換	安全性を認められたDHグループを採用していること	サービス仕様書 終端装置仕様書	DHグループとして,Group14から21,Group24,Group28から30のいずれかを採用していること
		5			IKEの認証方式	安全性を認められた認証方式を採用していること	サービス仕様書 終端装置仕様書	自動鍵配送付き事前共有鍵認証方式、デジタル証明書を用いたデジタル署名認証方式、EAP-TLSを採用していること(但し、事前共有鍵は128bit以上のエントロピーを有すること、デジタル証明書は、112ビット以上のセキュリティ強度を有すること) EAP-TTLSを用いる場合には、クライアント認証で用いる認証方式が安全性を認められた方式であることが客観的資料により示されていること
		6				デジタル証明書を用いたデジタル署名認証方式の場合は適切なIDペイロードタイプを採用していること	サービス仕様書 終端装置仕様書	Distingushed Name、FQDN、USER-FQDN、IPv4アドレスのいずれかを使用していること
		7			IKE SAの生存時間	暗号鍵の有効な時間を設定するため、Lifetimeを有限の値で設定してある。	サービス仕様書 終端装置仕様書	Lifetimeを24時間以内の値に設定していること

整理番号					評価対象プロダクト名			
項番			大分類	中分類	要件	確認項目	主な要素	評価基準
大分類	中分類	小分類						
		8			IPSecによる暗号化	適切な通信モードを採用していること	サービス仕様書 終端装置仕様書	トンネルモードを採用していること または、閉域網、NWで盗聴が防止できる場合はトランスポートモードも可
		9				適切なセキュリティプロトコルを採用していること	サービス仕様書 終端装置仕様書	ESPを採用していること トランスポートモードの場合はAH
		10				安全性を認められた暗号アルゴリズムを採用していること	サービス仕様書 終端装置仕様書	AES-GCM, AES-CTR, AES-CBC, AES-CCM (128, 192, 256-bit keys)のいずれかを採用していること
		11			IPSecでのメッセージ認証	安全性を認められた整合性アルゴリズムを採用していること	サービス仕様書 終端装置仕様書	HMAC-SHA256以上の安全性のある方式を採用していること
		12				安全性を認められたDHグループを採用していること	サービス仕様書 終端装置仕様書	DHグループとして,Group14から21,Group24,Group28から30のいずれかを採用していること
		13				PFS（Perfect Forward Secrecy）が有効になっていること	サービス仕様書 終端装置仕様書	PFSを有効とし、IKEで利用するDHグループと同等以上のDHグループを選択していること
		14			IPSec SA（Chiled SA）の生存時間	暗号鍵の有効な時間を設定するため、Lifetimeを有限の値で設定してある。	サービス仕様書 終端装置仕様書	Lifetimeを8時間以内の値に設定していること
		15			通信に用いる秘密鍵の管理	秘密鍵が漏洩すると盗聴される危険性があるため、秘密鍵について適切な管理を行うこと	サービス仕様書 終端装置仕様書	秘密鍵の利用環境での保持及び配送経路に対する安全性が担保されていること
		16			提供事業者の確認	(接続中継地点がある場合) 電気通信事業法に従い、電気通信事業の届出を行っている事業者であること	登録控え	通信事業者であること
		17			要求に応じたVPN接続の運用	通信の必要がないときはVPN接続を行わない機能を用い、運用を行うことについて、サービス仕様に明記しており、契約者と確認していること	運用仕様書 サービス仕様書 サービス説明書	通信の必要がないときは、VPN接続を行わない機能を実装し、運用について契約者の同意を得るために書面で明確にしていること
		18				(接続制御装置(サーバ)が別途ある場合) 接続制御装置が設置してあるサービス拠点について、本チェックリストの2.サービス拠点の基準を満たしていること	本チェックリストの2.サービス拠点の項目に準じる	接続制御装置の設置個所について、本チェックリストの2.サービス拠点の項目について全て基準を満たしている
4								
	1	1	その他	サービスの共有	(複数のサービスを運営している場合)サービスの分離	(サービス拠点で施設・資産の共有がある場合) 別途行われているサービス同士について、影響がないことについて確認していること	契約書 サービス仕様書	サービス拠点で施設・資産の共有がある場合に、サービス同士が影響を与えない方式をとっていること また、サービス同士が影響を与えないことについて、契約者の同意を得るために書面で明確にしていること
		2				(プロダクトの責任範囲に含まれる提供先(お客様環境等)の中で、施設・資産の共有がある場合) 別途行われているサービス同士について、影響がないことについて確認していること	契約書 サービス仕様書	提供先(お客様環境等)の中で施設・資産の共有がある場合に、サービス同士が影響を与えない方式をとっていること また、サービス同士が影響を与えないことについて、契約者の同意を得るために書面で明確にしていること