HISPRO レセプト・オンライン請求用チェックシート項目集

項番			分類		要件	確認項目
大分類	中分類	小分類	大分類	中分類		
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、契約者と確認していること
		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、契約者と確認していること
		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、契約者と確認していること
		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
		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
	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）
		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）
	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
	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
		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
		3			障害時の対策の明確化	
	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
		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
		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
		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
2						
2	1	1	サービス拠点	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
		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
		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
	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
		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
		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
		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
	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
		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
		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
		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
	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

項番			分類		要件	確認項目
大分類	中分類	小分類	大分類	中分類		
	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。
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
		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
		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
		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）
		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
	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）
		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
		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
		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
		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
		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
	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
	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での通信モード	適切な通信モードを採用していること
		2			IKEでの暗号化アルゴリズム	安全性を認められた暗号化アルゴリズムを採用していること
		3			IKEでの認証	安全性を認められた認証アルゴリズムを採用していること
		4			IKEでの鍵長	安全性を認められた鍵長(DHグループ)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
		6				RSAデジタル証明書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
		7			セッション毎の共通鍵の自動決定	暗号鍵の有効な時間を設定するため、Life Type、Life Durationを有限の値で設定してある。拠点間の機器の設定値にズレがある場合は、Life Durationの低い値にリキーのタイミングを合わせること
		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
		9				適切なセキュリティプロトコルを採用していること
		10				安全性を認められた暗号化アルゴリズム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認証アルゴリズムを採用していること
		12				安全性を認められた鍵長(DHグループ)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
		14			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
		15			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
		16			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
		17				（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
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
		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