

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
第4章 管理目的と管理策の選択					
	4-2. リモートサービスにおける安全管理措置				
	4-2-1. リモートサービスにおける組織的安全管理措置				
	① 個人データの安全管理措置を講じるための組織体制の整備				
	② 個人データの安全管理措置を定める規程等の整備と規程等に従った運用 ISP 側の保守点検、バックアップ、防災対策、事業継続計画、施錠保管を明文化して責任の分界を明確にすることによって、サービス不能を防止すること。				
	③ 個人データ取扱台帳の整備				
	④ 個人データの安全管理措置の評価、見直し及び改善				
	⑤ 事故又は違反への対処 防災対策、事業継続計画によって、災害を予防し、災害による被害損失の最小化と早期回復を可能とすること				
	4-2-2. リモートサービスにおける物理的安全管理措置				
	① 入退館(室)管理の実施				
	・パーティション等により、関係者以外の立ち寄りを抑止すること				
	・入室管理により、権限の無い者の入室を阻止して画面の覗き見や不正ログインや成りすまし、紙の覗き見や持出、RSC 機器やディスクの持出を防止すること				
	② 盗難等に対する対策				
	・シュレッダ廃棄により資産を消去することによって、権限の無い者による紙の覗き見や持出を防止すること				
	・複数人管理による入室管理により権限の有る者の単独入室を防止し、RSC サービスマンによる単独入室を阻止して紙の持出を牽制すること				
	・道路とサイトの距離の確保により漏洩電磁波の受信を防止し、PHI の暴露を防止すること				
	・ログオフ時の自動消去により人的ミスを防止し、RSC サービスマンのPHI の削除忘れを防止すること				
	・クリアデスクにより無人時の資産の放置を防止し、第三者、HCF 職員、HCF ネットワーク管理者、他社一次サービスマン、一次サービスマン、HCF システム管理者による紙の覗き見や持出を防止すること				
	③ 機器・装置等の物理的な保護				
	・施錠保管により、権限の無い者による接触を阻止して媒体の持出、破壊によるサービス不能を防止すること				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	・複数人管理による施錠保管により権限の有る者の単独接触を防止し、RSC サービスマンによる単独接触を阻止して媒体やRSC 機器やディスクの持出を牽制、RSCネットワーク機器経由のPHI の暴露を防止すること。				
	・RSC 側内部経路点検により、経路上のタッピング痕跡を検出すること。				
	・シールにより、タンパリング痕跡を検出すること				
	4-2-3. リモートサービスにおける技術的安全管理措置				
	① 人データへのアクセスにおける識別と認証				
	・遠隔地からの利用者のアクセスには、認証を行うこと				
	・遠隔コンピュータシステムへの接続は、認証されること。				
	② 個人データへのアクセス制御				
	・利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること				
	③ 個人データへのアクセス権限の管理				
	・複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること				
	・パスワードの割当ては、正規の管理手続によって統制すること				
	④ 個人データのアクセスの記録				
	・情報処理設備の使用状況を監視する手順を確立すること				
	⑤ 個人データを取り扱う情報システムについての不正ソフトウェア対策				
	・悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること				
	⑥ 個人データの移送・送信時の対策				
	・データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること				
	・共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと				
	・一連の合意された標準類、手順及び方法に基づく鍵管理システムを、暗号技術の利用を支援するために用いること				
	⑦ 個人データを取り扱う情報システムの動作確認時の対策				
	・装置についての継続的な可用性及び完全性の維持を確実にするために、装置の保守を正しく実施すること				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	⑧ 個人データを取り扱う情報システムの監視				
	・極めて重要な業務情報及びソフトウェアのバックアップは、定期的を取得し、かつ検査すること				
	4-2-4. リモートサービスにおける人的安全管理措置				
	① 雇用契約時及び委託契約時における非開示契約の締結				
	・従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること				
	・組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備えていること				
	② 従業者に対する教育・訓練の実施				
	・組織の基本方針及び基準について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと。				