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	
3．基本的な考え方					
	3．2　運用要件				
	3．2．1　運用上の留意点				
	(1)登録認定システム、カード発行者システム、サービス提供システムなどのプレーヤの登録やカード発行、カード発行後のAPダウンロードなど業務を適切に処理するシステムを構築すること。				
	(2)上記システム間および端末システム間のデータ転送を確実にかつ安全に行う、専用線や公衆回線、インターネットなどのネットワーク環境を構築すること。				
	(3)各システムの運用方針、セキュリティ方針が明確になっていること。				
	(4)システムの運用を行う運用者／操作者はシステムについて十分なスキルがあり、セキュリティ保護についても常識を持っていること。				
	(5)ICカードのOSのバージョン管理やサービスAPのバージョン管理、さらには運用システム自身のバージョン管理方法について明確にされていること。				
	(6)システムに対する保守体制、障害時対応方針が明確であること				
	3．2．2　登録審査の考え方				
	(1)カード供給者、カード発行者、サービス提供者の登録においては、組織／企業の規模や財務状況などは審査の基準とせず、実在する企業で申請情報が正しければ登録することとする。				
	(2)登録された組織／企業の名前などはWWWで公開されるため、目的以外の登録や偽りの登録は可能性が少ないと考えられる。（AP登録も同様である。）				
	(3)一方、カードおよびリーダライタについては相互運用性の観点からコンフォーマンス試験を含む認定審査を行う。				
	3．3　セキュリティ				
	3．3．1　システムセキュリティ				
	(1)オペレータ管理				
	カードを発行・運用する各団体は、適切なセキュリティポリシーを策定し、それらの個人情報に直接触れる可能性のある人物に対し、セキュリティ意識の徹底及びセキュリティ・リテラシーの向上のための教育を施す必要がある。				
	また、派遣会社、アルバイト等で要員を確保する場合、雇用の際に取り交わす契約書にも守秘義務に関する条項を盛り込む必要がある。具体的な内容は、住民基本台帳法の第30条、第42条、第44条、第48条などを参照されたい。				

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	
	(2)鍵管理				
	ICカードを発行・運用するに際しては、様々な暗号鍵(この節では単に「鍵」という)を管理する必要がある。鍵の詳細については『NICCS要件書』　に詳しいが、ここでは非対称鍵暗号方式における秘密鍵の取り扱いについて注意すべき点を記述する。				
	A. カード発行者、サービス提供者の秘密鍵				
	・秘密鍵の管理 カード発行者、サービス提供者が、登録認定機関より鍵対(秘密鍵・公開鍵)生成ツールをダウンロードし、生成する自身の鍵対において、秘密鍵については、格納するメディアの選定(セキュリティモジュールの採用など)、格納時の暗号化、格納された秘密鍵へアクセス可能な人物の制限など厳重な管理が必要となる。				
	・秘密鍵紛失時の考慮 万が一にも秘密鍵を紛失した場合にの影響を事前に調査し、対策をたてておく必要がある。				
	B. 各カードの秘密鍵				
	・鍵の生成 鍵の生成については、カード内部でカードの鍵対(秘密鍵・公開鍵)を生成する方法がセキュリティ上望ましい。				
	発行手順によってはカード内部での鍵対生成が困難な場合があること等により、外部生成してカードへ搭載することも避けられない場合の秘密鍵の取り扱いについては、ICカード外では暗号化して保管するなど、十分な注意を払う必要がある。				
	・秘密鍵の使用期限 長期に渡ってカードを使用する場合、カード発行者、サービス提供者、カード利用者いずれにも負担の少ない形での、鍵対の入れ換えについて検討しておく必要がある。				
	(3)データ管理				
	電子化された情報の管理について、カード利用者の個人情報の管理については、2002年1月に施行予定の「個人情報保護基本法」を踏まえたうえで、以下のような項目に注意するべきである。 ・データ保管設備は施錠可能か ・データ取り扱いについてルールが制定されているか ・データ(バックアップ含む)の保管管理は特定者によって行われ、定期的に保管状況が点検されているか ・管理記録が整備され、データの作成・追加・更新・廃棄について十分把握されているか ・重要なデータは暗号化され、アクセスは制限されているか				

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	
	個人情報の管理については、情報サービス産業向けのガイドラインではあるが、JISA（社団法人情報　サービス協会）の提唱する「情報サービス産業個人情報　保護ガイドライン」（第三版）が示唆に富むため、これを参照することを推奨する。				
	（4）個人情報管理				
	ICカードを発行・運用するために収集したカード利用者情報は、電子化されたものだけでなく、一次情報（「カード利用申請書」等）の管理については、電子化された情報となんら異なる点はなく、保管・管理方法について電子データと同等の注意が必要である。				
	３．３．２　障害対策				
	（1）サーバ・クライアント等				
	利用者の利便性を考えるならば、サーバは二重化しておき、障害時には待機系に切り替えて運用するなど、システムの停止時間を最小限に押さえる方策を検討すべきである。				
	（2）ネットワーク				
	（1）と同様に、回線についても障害時に備えて二重化することが望ましい。				
	各種ネットワーク機器についても二重化するか、もしくは各ベンダと適切な保守契約を締結し、障害時の迅速な対応がはかれるようにするべきである				
	（2）カードの障害対策				
	ICカード内部に格納される情報は、カードの紛失・盗難、カードの故障などの障害時に備えて、カード発行者・サービス提供者によって適切に管理されるべきである。				
	（3）ヘルプデスク				
	問合せ窓口を用意するのは他のサービスと同様に必要であり、カード発行者及びサービス提供者の義務でもある。				
	サービス利用者だけでなく、サービスを提供する現場の応対者からの問合せも考慮する必要がある。 問合せ一次窓口としては主に、 　①現場付近に設置されているサービスカウンタ 　②電話での問合せ窓口 が挙げられる。また、電子メールやWeb等による相談/対処法提供(FAQ,Q&A等)も考えられる。				
	難易度の高い問題にも対応するため、各業務の担当部署へエスカレーションするような仕組みを検討する必要がある。				
	その本部の業務担当でも対応できないようなシステム上の問題などは、そこからシステム担当へ再度エスカレーションするような流れにすべきである。				