別紙

表 1　要件表記の一例

必須要件　（一部抜粋）			
No.	入退管理システムの基本要件		
	対策要件	対策方法	
		仕様書へ記述する要件	組織における対策／運用
a03	【管理者とオペレータの設定】	a03-1.管理操作ができる機器は、保護資産や設定データへのアクセス前に管理者・オペレータを識別認証すること	■管理操作ができる機器や管理サーバでは以下の設定を行う
	保護資産や設定データへのアクセスや機器の制御をできる役割を限定すること	a03-2. 管理者がオペレータのアクセス可能な機能と情報について管理できること	・ 管理操作の前に識別認証を必須とする設定を行い、適切なアクセス制御の設定を行う ・ 不要なアカウントは削除する ・ 可能であれば個人毎に異なるユーザIDで識別する ・ 管理者は自身及びオペレータのパスワードを組織の「情報セキュリティ対策基準」に従って設定し、出荷設定値の使用は禁止する ・ 設定可能な場合、一定回数（5回程度）の連続した接続試行によるユーザIDの一定時間ロックを有効にする
		a03-3. 管理操作ができる機器は、パスワードを出荷設定値から推測困難な値へ変更すること	
		a03-4. 設定可能な機器は、一定回数（5回程度）の連続した接続試行によるユーザIDの一定時間のロック、及びパスワードの最低長（8文字以上）等パスワードの複雑さを上げる設定を行うこと	
a04	【不正アクセスの検知】	a04-1. システムを構成する機器との通信断を管理者が検知できること	■利用者が接触可能な機器の回線切断、及びケース開け（タンパ―応答）を管理者が検知できる設定とする
	システムを構成する機器への不正アクセスやなりすましを検知すること	a04-2. 制御装置、認証装置、存在する場合は鍵管理盤のケース開けを管理者が検知できること	■IP通信を行う機器のログやアラームにおいて識別認証や機器からの接続の失敗、及び／または成功を、管理者が検知できる設定を行う
		a04-3. 識別認証やシステムからの接続の失敗、及び／または成功を検知し、確認する手段を管理者に提供すること	■入退、ID追加の管理操作の記録をログに残す設定を行う
		a04-4. 入退、ID追加などの管理操作、及びセンサーからの通信の履歴を管理者に提供できること	■ログの閲覧は必要に応じてオペレータに提供する設定を行っても良いが、ログの削除や設定は管理者に限定する
		a04-5. システムの時刻は正しく設定でき、構築後に時刻データの変更やズレを管理者が検知できること	■管理者はシステムの時刻を正しく設定し、維持する