評価観点別の質問表

評価の観点	大項目	中項目	評価対象
役割分担が明確なシステム構成をとりやすいか	システム構成	ポンチ図に相当するサーバ機能を開発なしに そろえられるか? (IA, RA, リポジトリ、申請受付サーバ、利用者管理 サーバ)	システム構成要素
		ポンチ図に相当するRA用ツールを開発なしに そろえられるか? (RA管理インタフェース、RAA申請インタフェース、RA 申請インタフェース)	各種RA用インタフェース
	オペレータの権限設定	RAAはRAのみの証明書申請ができるように 設定できるか?	RAサーバ or 申請受付サーバ
		RAはEEのみの証明書申請ができるように設定できる	RAサーバ or 申請受付サーバ
		RAAはRAのみの証明書失効ができるように 設定にできるか?	RAサーバ or IA(CA)サーバ
		RAは自分が申請したEEのみの証明書失効が できるように設定できるか?	RAサーバ or IA(CA)サーバ
		RAによるEE証明書申請数について上限を設定できるか?	申請受付サーバ?
		EEの鍵対のバックアップをとる場合、バックアップデータ へアクセスできるオペレータを指定できるか?	RAサーバ or IA(CA)サーバ
		複数名のRAO, RAAの認証が完了しないと証明書発行ができないように設定できるか?	RAサーバ
		CAサーバ、RAサーバのログ閲覧のみができる インタフェースの提供と設定ができるか?	RAサーバ or IA(CA)サーバ
	オペレータのアクセス	RAOからRAサーバへのアクセス制限方法としてユーザ	RAサーバ
		RAAから申請受付サーバへのアクセス制限方法として	申請受付サーバ
		RAから申請受付サーバへのアクセス制限方法として ユーザ認証以外の方法をサポートしているか?	申請受付サーバ
オペレータ以外からの不正アクセス対策が 充実しているか?	サーバ管理権限の設定	CAOを複数人とし、複数人集まらないとIA(CA)サーバの 設定を変えられないようにできるか?	IA(CA)サーバ
		RAOを複数人とし、複数人集まらないとRAサーバの 設定を変えられないようにできるか?	RAサーバ
		RAAを複数人とし、複数人集まらないと申請受付サーバ	申請受付サーバ
		?	利用者管理サーバ
		?	リポジトリ
	サーバ間の通信保護	IA(CA)サーバとRAサーバ間の通信保護を考慮した プロトコルが採用されているか?	IA(CA)サーバ、RAサーバ
		RAサーバと申請受付サーバ間の通信保護を考慮した プロトコルが採用されているか?	RAサーバ、申請受付サーバ
	不正アクセス対策の前提となる機能	JPNIC認証局の設備である、IA(CA)サーバ、RAサーバ、 リポジトリへの不正アクセスを防ぐための機能がある	IA(CA)サーバ、RAサーバ、 リポジトリ
		IP事業者の設備である、申請受付サーバ、利用者管理 サーバへの不正アクセスを防ぐための機能があるか?	申請受付サーバ、 利用者管理サーバ
	サーバ管理ログ	RAサーバの作業記録に、RAO, RAA, RAの区別があるか?	RAサーバ
		申請受付サーバの作業記録に、RAA, RAの区別があるか?	利用者管理サーバ
		IA(CA)サーバの作業記録をCAOにメールで送る機能が	IA(CA)サーバ
		RAサーバの作業記録をRAOにメールで送る機能があるか?	RAサーバ
		申請受付サーバの作業記録をRAAにメールで送る機能	申請受付サーバ
RA(ISP)にとって導入しやすいか?	インタフェース導入	RA申請インタフェースの動作プラットフォームは、Windows	RA申請インタフェース
		RA申請インタフェースの動作プラットフォームは、UNIXに	RA申請インタフェース
		RA申請インタフェースの動作プラットフォームは、Macに	RA申請インタフェース
	インタフェースの使いやすさ	RA申請インタフェースのカスタマイズが 簡単にできるか?	RA申請インタフェース
事業部にとって導入しやすいか?	インタフェース導入	RAA申請インタフェースの動作プラットフォームは、Windows xxに対応しているか?	RAA申請インタフェース
		RAA申請インタフェースの動作プラットフォームは、UNIXに対応しているか?	RAA申請インタフェース
		RAA申請インタフェースの動作プラットフォームは、Macに対応しているか?	RAA申請インタフェース

その他、認証局の機能が充実して	アルゴリズムの設定	鍵対作成時、鍵長設定を証明書の種別ごとに変えられるか?	IA(CA)サーバ
	データベース保護	証明書データベースの保護を考慮した方式が採用されて	IA(CA)サーバ
		作業記録にディジタル署名をつけられるか?	IA(CA)サーバ、利用者管理サーバ
		作業記録にタイムスタンプをつけられるか?	IA(CA)サーバ、利用者管理サーバ
	証明書プロファイルの設定	証明書プロファイルの xxx 拡張フィールドをサポートしているか?	IA(CA)サーバ
	証明書のスムーズな発行	EE証明書をバルクで発行できるか?	IA(CA)サーバ
	ライフサイクル管理対応	CAの鍵対変更(Rekey)を想定したリンク証明書を発行する機能があるか?	IA(CA)サーバ
		EE証明書を更新(Update)する機能があるか?(同一DNの証明書発行を許容するか?)	IA(CA)サーバ
		EE証明書を更新する機能があるとき、EEから直接申請するインタフェースを開発なしに用意できるか?	IA(CA)サーバ? 申請受付サーバ?
		EEから直接申請するインタフェースがあるが不要となった	IA(CA)サーバ? 申請受付サーバ?
	トークン対応	ICカードに対応しているか?	IA(CA)サーバ? RAサーバ? RAA申請インタフェース?
		USBキーに対応しているか?	IA(CA)サーバ? RAサーバ? RAA申請インタフェース?
	CRL	CRL発行後、リポジトリへの登録が自動化できるか?	IA(CA)サーバ、リポジトリ
		CRL発行の自動化ができるか?	IA(CA)サーバ
	秘密鍵管理レベル	IA(CA)の秘密鍵をHSM内で作成して管理できるか?	IA(CA)サーバ
		IA(CA)の秘密鍵はUpdateを含め最長xx年使い続けられるか?(ソフトとしての制限ではなく、HSMとしての制限があるか?)	IA(CA)サーバ
		HSMはFIPS140-1レベル3認定であるか?	IA(CA)サーバ
		HSM管理のために複数人認証をサポートしているか?	IA(CA)サーバ
		HSM管理のために複数方式による認証をサポートしているか?(パスワード+物理トークンなど)	IA(CA)サーバ
		HSMで秘密鍵の分割バックアップをサポートしている	IA(CA)サーバ
		HSMで秘密鍵の暗号化バックアップをサポートしているか?	IA(CA)サーバ
		HSMで秘密鍵のバックアップ媒体として安全な媒体が利用可能であるか?	IA(CA)サーバ
	一般	公開鍵の重複チェック機能があるか?	IA(CA)サーバ
	管理権限		
	ログ	証明書の累計発行枚数表示機能があるか?	IA(CA)サーバ
	発行承認		
	インタフェース		
	プロトコル		

評価対象別の質問表

評価対象	大項目	中項目	その他の観点
IA(CA)サーバ	サーバ管理権限の設定	CAOを複数人とし、複数人集まらないとIA(CA)サーバの	オペレータ以外からの不正アクセス対策が充実しているか?
	サーバ管理ログ	IA(CA)サーバの作業記録をCAOにメールで送る機能が	
	アルゴリズムの設定	鍵対作成時、鍵長設定を証明書の種別ごとに変えられるか?	その他、認証局の機能の充実
	データベース保護	証明書データベースの保護を考慮した方式が採用されて	
	証明書プロファイルの設定	証明書プロファイルの拡張フィールドをサポート状況は？	
	証明書のスムーズな発行	EE証明書をバルクで発行できるか?	
	ライフサイクル管理対応	CAの鍵対変更(Rekey)を想定したリンク証明書を発行	
		EE証明書を更新(Update)する機能があるか?（同一DNの証明書発行を許容するか?）	
	CRL	CRL発行の自動化ができるか?	
	秘密鍵管理レベル	IA(CA)の秘密鍵をHSM内で作成して管理できるか?	
		IA(CA)の秘密鍵はUpdateを含め最長xx年使い続けられるか? (ソフトとしての制限ではなく、HSMとして	
		HSMはFIPS140-1レベル3認定であるか?	
		HSM管理のために複数人認証をサポートしているか?	
		HSM管理のために複数方式による認証をサポートしているか? (パスワード+物理トークンなど)	
		HSMで秘密鍵の分割バックアップをサポートしている	
		HSMで秘密鍵の暗号化バックアップをサポートしているか?	
		HSMで秘密鍵のバックアップ媒体として安全な媒体が	
	一般	公開鍵の重複チェック機能があるか?	
	ログ	証明書の累計発行枚数表示機能があるか?	
IA(CA)サーバ、リポジトリ	CRL	CRL発行後、リポジトリへの登録が自動化できるか?	その他、認証局の機能の充実
IA(CA)サーバ、利用者管理サーバ	データベース保護	作業記録にディジタル署名をつけられるか?	その他、認証局の機能の充実
		作業記録にタイムスタンプをつけられるか?	
IA(CA)サーバ、RAサーバ	サーバ間の通信保護	IA(CA)サーバとRAサーバ間の通信保護を考慮したプロトコルが採用されているか?	オペレータ以外からの不正アクセス対策が充実しているか?
IA(CA)サーバ、RAサーバ、リポジトリ	不正アクセス対策の前提となる機能	JPNIC認証局の設備である、IA(CA)サーバ、RAサーバ、リポジトリへの不正アクセスを防ぐための機能がある	オペレータ以外からの不正アクセス対策が充実しているか?
IA(CA)サーバ・RAサーバ・RAA申請インタフェース	トークン対応	ICカードに対応しているか?	その他、認証局の機能の充実
		USBキーに対応しているか?	その他、認証局の機能の充実
IA(CA)サーバ・申請受付サーバ	ライフサイクル管理対応	EE証明書を更新する機能があるとき、EEから直接申請するインタフェースを開発なしに用意できるか?	その他、認証局の機能の充実
		EEから直接申請するインタフェースがあるが不要となった	その他、認証局の機能の充実
RAA申請インタフェース	インタフェース導入	RAA申請インタフェースの動作プラットフォームは、Windows xxに対応しているか?	導入／開発のしやすさ
		RAA申請インタフェースの動作プラットフォームは、UNIXに対応しているか?	
		RAA申請インタフェースの動作プラットフォームは、Macに対応しているか?	
RAサーバ	オペレータの権限設定	複数名のRAO, RAAの認証が完了しないと証明書発行ができないように設定できるか?	役割分担が明確なシステム構成をとりやすいか
	オペレータのアクセス	RAOからRAサーバへのアクセス制限方法としてユーザ	役割分担が明確なシステム構成をとりやすいか
	サーバ管理権限の設定	RAOを複数人とし、複数人集まらないとRAサーバの設定を変えられないようにできるか?	オペレータ以外からの不正アクセス対策が充実しているか?
	サーバ管理ログ	RAサーバの作業記録に、RAO, RAA, RAの区別があるか?	
		RAサーバの作業記録をRAOにメールで送る機能があるか?	
RAサーバ or IA(CA)サーバ	オペレータの権限設定	RAAはRAのみの証明書失効ができるように設定にできるか?	役割分担が明確なシステム構成をとりやすいか
		RAは自分が申請したEEのみの証明書失効ができるように設定できるか?	
		EEの鍵対のバックアップをとる場合、バックアップデータへアクセスできるオペレータを指定できるか?	
RAサーバ or IA(CA)サーバ	オペレータの権限設定	CAサーバ、RAサーバのログ閲覧のみができるインタフェースの提供と設定ができるか?	役割分担が明確なシステム構成をとりやすいか
RAサーバ or 申請受付サーバ	オペレータの権限設定	RAAはRAのみの証明書申請ができるように設定できるか?	役割分担が明確なシステム構成をとりやすいか
		RAはEEのみの証明書申請ができるように設定できるか?	
RAサーバ、申請受付サーバ	サーバ間の通信保護	RAサーバと申請受付サーバ間の通信保護を考慮した	オペレータ以外からの不正アクセス対策が充実しているか?

RA申請インタフェース	インタフェース導入	RA申請インタフェースの動作プラットフォームは、Windows	RA(ISP)にとっての導入しやすさ
		RA申請インタフェースの動作プラットフォームは、UNIXに	
		RA申請インタフェースの動作プラットフォームは、Macに	
	インタフェースの使いやすさ	RA申請インタフェースのカスタマイズが簡単にできるか?	RA(ISP)にとっての導入しやすさ
各種RA用インタフェース	システム構成	ポンチ図に相当するRA用ツールを開発なしにそろえられるか? (RA管理インタフェース、RAA申請インタフェース、RA申請インタフェース)	役割分担が明確なシステム構成をとりやすいか
システム構成要素	システム構成	ポンチ図に相当するサーバ機能を開発なしにそろえられるか? (IA, RA, リポジトリ、申請受付サーバ、利用者管理サーバ)	役割分担が明確なシステム構成をとりやすいか
申請受付サーバ	オペレータのアクセス制限	RAAから申請受付サーバへのアクセス制限方法として	役割分担が明確なシステム構成をとりやすいか
		RAから申請受付サーバへのアクセス制限方法としてユーザ認証以外の方法をサポートしているか?	
	サーバ管理権限の設定	RAAを複数人とし、複数人集まらないと申請受付サーバ	オペレータ以外からの不正アクセス対策が充実しているか?
	サーバ管理ログ	申請受付サーバの作業記録をRAAにメールで送る機能	
申請受付サーバ、利用者管理サーバ	不正アクセス対策の前提となる機能	IP事業者の設備である、申請受付サーバ、利用者管理 サーバへの不正アクセスを防ぐための機能がある	オペレータ以外からの不正アクセス対策の充実
申請受付サーバ?	オペレータの権限設定	RAによるEE証明書申請数について上限を設定できるか?	役割分担が明確なシステム構成をとりやすいか
リポジトリ	サーバ管理権限の設定		オペレータ以外からの不正アクセス対策の充実
利用者管理サーバ	サーバ管理権限の設定		オペレータ以外からの不正アクセス対策の充実
利用者管理サーバ	サーバ管理ログ	申請受付サーバの作業記録に、RAA, RAの区別があるか?	オペレータ以外からの不正アクセス対策の充実
その他	管理権限 発行承認 インタフェース プロトコル		その他、認証局の機能の充実