.jp DNSSECキーセレモニー
作業手順書

第1回用

2010年10月4日（月）実施

株式会社日本レジストリサービス

JPRS
JAPAN REGISTRY SERVICES

■ jp DNSSEC キーセレモニー 実施体制

No.	役割	担当者	作業内容
	統括責任者	JPRS 田中正則	jp DNSSECキーセレモニーの責任者
	進行管理	JPRS 高嶋隆一 JPRS 野口昇二	jp DNSSECキーセレモニーの司会進行を行う
A	鍵管理運用者1	JPRS 舩戸正和	鍵生成・削除の主担当者として操作を行う
B	鍵管理運用者2	JPRS 春名光一	鍵生成・削除の副担当者として操作内容を確認する
C	金庫鍵管理者1	JPRS 舩戸正和	金庫鍵1による金庫の開錠・施錠を行う
D	金庫鍵管理者2	JPRS 白岩一光	金庫鍵2による金庫の開錠・施錠を行う
E	作業立会者1	(株)インターネットイニシアティブ 松崎吉伸	一連の作業が手順書の内容どおり正しく行われていることを確認する
F	作業立会者2	NTTコミュニケーションズ(株) 図師稔	一連の作業が手順書に定められた担当者により、定められた手順で行われていることを確認する

■ 作業手順書中の用語

TEB

Tamper Evident Bagの略。シリアル番号つきの封印できる袋。
前回の保存時から未開封であることを担保することができる。

■詳細作業手順書の作成

本手順書は公開を前提とする。
本手順書とは別に、詳細作業手順書を作成するが、その内容には公開に適さない情報を含むため、
詳細作業手順書については非公開とする。

凡例: ■: 作業担当として実行(操作)を行う
□: 作業担当として正しい操作が行われている事の確認を行う
C1: 作業が定められた内容で正しく行われている事の確認を行う
C2: 作業が正しい権限を持つ担当者により決められた手順で行われている事の確認を行う
●: 操作対象の物品

No		手順	アクター														
			A	B	C	D	E	F	①	②	③	④	⑤	⑥	⑦		
			鍵管理運用者1	鍵管理運用者2	金庫鍵管理者1	金庫鍵管理者2	作業立会者1	作業立会者2	KSK管理用記憶媒体	ZSK管理用記憶媒体	KSK/ZSK操作用PC	金庫	.jpゾーン署名サーバ	.jpゾーン署名サーバ格納用記憶媒体	TEB		
0	金庫鍵搬送～作業場所への集合																
	0.01	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥.jpゾーン署名サーバ格納用記憶媒体の封印、および番号の記録 【初回および物品交換時のみ】	■	■					●	●	●			●	●		
	0.02	金庫鍵1の取り出し			■												
	0.03	金庫鍵1のデータセンタ搬送			■												
	0.04	金庫鍵2の取り出し				■											
	0.05	金庫鍵2のデータセンタ搬送				■											
	0.06	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥.jpゾーン署名サーバ格納用記憶媒体、⑦TEBのデータセンタ搬送 【初回および物品交換時のみ】	■	■					●	●	●			●	●		
	0.07	データセンタ入館	■	■	■	■	■	■									
	0.08	ケージ開錠			■		C1	C2									
	0.09	金庫の状態の記録					■	□				●					
	0.10	TEBとシリアルの記録					■	□	●	●	●			●	●		
	0.11	時計の時刻あわせ	■	■			■	□									
1	金庫の開放																
	1.01	金庫鍵1による開錠			■		C1	C2				●					
	1.02	金庫鍵2による開錠				■	C1	C2				●					
	1.03	金庫の開放					■	□				●					
	1.04	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥.jpゾーン署名サーバ格納用記憶媒体 が封印されている事の確認					■	□	●	●	●			●	●		

凡例: ■: 作業担当として実行(操作)を行う
□: 作業担当として正しい操作が行われている事の確認を行う
C1: 作業が定められた内容で正しく行われている事の確認を行う
C2: 作業が正しい権限を持つ担当者により決められた手順で行われている事の確認を行う
●: 操作対象の物品

No	手順	アクター													
		A	B	C	D	E	F	①	②	③	④	⑤	⑥	⑦
		鍵管理運用者1	鍵管理運用者2	金庫鍵管理者1	金庫鍵管理者2	作業立会者1	作業立会者2	KSK管理用記憶媒体	ZSK管理用記憶媒体	KSK/ZSK操作用PC	金庫	.jpゾーン署名サーバ	.jpゾーン署名サーバ格納用記憶媒体	TEB
2	データ初期化、システム運用者個別鍵の生成【初回のみ】													
	2.01	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥jpゾーン署名サーバ格納用記憶媒体 の封印の解除				■	□	●	●	●			●	●
	2.02	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥jpゾーン署名サーバ格納用記憶媒体 の配置				■	□	●	●	●			●	
	2.03	操作用PCの起動	■	□		C1	C2			●				
	2.04	②ZSK管理用記憶媒体 のデータ初期化	■	□		C1	C2		●	●				
	2.05	⑥jpゾーン署名サーバ格納用記憶媒体 のデータ初期化	■	□		C1	C2			●			●	
	2.06	②ZSK管理用記憶媒体 東京(正)の③KSK/ZSK操作用PCへの挿入	■	□		C1	C2		●	●				
	2.07	鍵管理運用者用認証情報の生成 (鍵管理運用者全員分)	■	■		C1	C2		●	●				
	2.08	認証情報の鍵管理アプリケーションへの反映	■	□		C1	C2		●	●				
3	KSK管理用記憶媒体の初期設定【初回のみ】													
	3.01	①KSK管理用記憶媒体 の初期化	■	□		C1	C2	●		●				
	3.02	操作用アプリケーションの起動と複数人認証	■	□		C1	C2			●				
	3.03	①KSK管理用記憶媒体操作用認証情報 の生成と①KSK管理用記憶媒体 への記録	■	□		C1	C2	●		●				
	3.04	操作アプリケーションの終了	■	□		C1	C2	●		●				
4	KSK鍵ペアの生成													
	4.01	操作用アプリケーションの起動	■	□		C1	C2			●				
	4.02	KSK鍵ペアの生成	■	■		C1	C2		●	●				
	4.03	KSK鍵ペアが正しく生成された事の確認	■	□		C1	C2		●	●				
	4.04	KSK秘密鍵の①KSK管理用記憶媒体 への格納	■	□		C1	C2	●		●				
	4.05	操作用アプリケーションの終了	■	□		C1	C2			●				
	4.06	KSKの確認コマンドの実行	■	□		C1	C2			●				
	4.07	KSKの確認	■	■		C1	C2		●	●				
5	DSの生成													
	5.01	操作用アプリケーションの起動	■	□		C1	C2			●				
	5.02	DSの生成	■	■		C1	C2		●	●				
	5.03	②ZSK管理用記憶媒体 内でのDSのコピー	■	□		C1	C2		●	●				
	5.04	DSが正しく生成された事の確認	■	□		C1	C2		●	●				

凡例: ■: 作業担当として実行(操作)を行う
□: 作業担当として正しい操作が行われている事の確認を行う
C1: 作業が定められた内容で正しく行われている事の確認を行う
C2: 作業が正しい権限を持つ担当者により決められた手順で行われている事の確認を行う
●: 操作対象の物品

No	手順	アクター														
		A	B	C	D	E	F	①	②	③	④	⑤	⑥	⑦		
		鍵管理運用者1	鍵管理運用者2	金庫鍵管理者1	金庫鍵管理者2	作業立会者1	作業立会者2	KSK管理用記憶媒体	ZSK管理用記憶媒体	KSK/ZSK操作用PC	金庫	.jpゾーン署名サーバ	.jpゾーン署名サーバ格納用記憶媒体	TEB		
6	ZSK鍵ペアの生成															
	6.01	【ZSK1つ目】操作用アプリケーションの起動	■	□			C1	C2			●					
	6.02	【ZSK1つ目】ZSK鍵ペアの生成	■	■			C1	C2		●	●					
	6.03	【ZSK2つ目】操作用アプリケーションの起動【初回のみ】	■	□			C1	C2			●					
	6.04	【ZSK2つ目】ZSK鍵ペアの生成【初回のみ】	■	■			C1	C2		●	●					
	6.05	ZSK確認コマンドの実行	■	□			C1	C2			●					
	6.06	ZSK鍵ペアが正しく生成された事の確認	■	□			C1	C2		●	●					
7	ZSK鍵ペアの署名															
	7.01	操作用アプリケーションの起動	■	□			C1	C2			●					
	7.02	操作用アプリケーション上で、複数人認証を実施	■	■			C1	C2		●	●					
	7.03	KSK秘密鍵によるZSK公開鍵への署名生成	■	□			C1	C2	●		●					
	7.04	②ZSK管理用記憶媒体 内での署名済公開鍵、ZSK公開鍵、ZSK秘密鍵のコピー	■	□			C1	C2		●	●					
	7.05	ZSK公開鍵への署名が正しく生成された事の確認 署名済みZSK公開鍵(RRSIG,DNSKEY)が含まれたファイルが正しく生成された事の確認	■	□			C1	C2	●	●	●					
	7.06	⑥.jpゾーン署名サーバ格納用記憶媒体 東京(正)の③KSK/ZSK操作用PC への挿入	■	□			C1	C2			●			●		
	7.07	署名済みZSK公開鍵、対応するZSK秘密鍵、DSの⑥.jpゾーン署名サーバ格納用記憶媒体 への格納	■	□			C1	C2			●			●		
	7.08	署名済みZSK公開鍵、対応するZSK秘密鍵、DSが正しく⑥.jpゾーン署名サーバ格納用記憶媒体 へ格納された事の確認	■	□			C1	C2			●			●		
	7.09	⑥.jpゾーン署名サーバ格納用記憶媒体 東京(正)の③KSK/ZSK操作用PC からの抜去	■	□			C1	C2			●			●		

凡例: ■: 作業担当として実行(操作)を行う
□: 作業担当として正しい操作が行われている事の確認を行う
C1: 作業が定められた内容で正しく行われている事の確認を行う
C2: 作業が正しい権限を持つ担当者により決められた手順で行われている事の確認を行う
●: 操作対象の物品

No	手順	アクター														
		A	B	C	D	E	F	①	②	③	④	⑤	⑥	⑦		
		鍵管理運用者1	鍵管理運用者2	金庫鍵管理者1	金庫鍵管理者2	作業立会者1	作業立会者2	KSK管理用記憶媒体	ZSK管理用記憶媒体	KSK/ZSK操作用PC	金庫	.jpゾーン署名サーバ	.jpゾーン署名サーバ格納用記憶媒体	TEB		
8	署名済みZSK公開鍵の.jpゾーン署名サーバへの格納															
	8.01	【1台目】⑤.jpゾーン署名サーバ(正)へのコンソールによるログイン	■	□			C1	C2					●			
	8.02	【1台目】⑤.jpゾーン署名サーバ(正)へに⑥.jpゾーン署名サーバ格納用記憶媒体 東京(正)を挿入する	■	□			C1	C2					●	●		
	8.03	【1台目】⑥.jpゾーン署名サーバ格納用記憶媒体 から⑤.jpゾーン署名サーバ(正)の所定のフォルダへの署名済みZSK公開鍵、ZSK秘密鍵情報の格納	■	□			C1	C2					●	●		
	8.04	【1台目】⑥.jpゾーン署名サーバ格納用記憶媒体 から⑤.jpゾーン署名サーバ(正)の所定のフォルダへのDSの格納	■	□			C1	C2					●	●		
	8.05	【1台目】.jpゾーン署名サーバ格納用記憶媒体 から⑤.jpゾーン署名サーバ(正)の所定のフォルダに署名済みZSK公開鍵、ZSK秘密鍵情報が正しく格納された事の確認	■	□			C1	C2					●			
	8.06	【2台目】⑤.jpゾーン署名サーバ(副)へのコンソールによるログイン	■	□			C1	C2					●			
	8.07	【2台目】⑥.jpゾーン署名サーバ格納用記憶媒体 東京(正)の⑤.jpゾーン署名サーバ(副) への挿入	■	□			C1	C2					●	●		
	8.08	【2台目】⑥.jpゾーン署名サーバ格納用記憶媒体 から⑤.jpゾーン署名サーバ(副)の所定のフォルダへの署名済みZSK公開鍵、ZSK秘密鍵情報の格納	■	□			C1	C2					●	●		
	8.09	【2台目】⑥.jpゾーン署名サーバ格納用記憶媒体 から⑤.jpゾーン署名サーバ(副)の所定のフォルダへのDSの格納	■	□			C1	C2					●	●		
	8.10	【2台目】⑥.jpゾーン署名サーバ格納用記憶媒体 から⑤.jpゾーン署名サーバ(副)の所定のフォルダに署名済みZSK公開鍵、ZSK秘密鍵情報が正しく格納された事の確認	■	□			C1	C2					●			
	8.11	【2台目】⑥.jpゾーン署名サーバ格納用記憶媒体 東京(正)の内容の消去	■	□			C1	C2					●	●		
	8.12	【2台目】⑥.jpゾーン署名サーバ格納用記憶媒体 東京(正)の⑤.jpゾーン署名サーバ(副)からの抜去	■	□			C1	C2					●	●		

凡例: ■: 作業担当として実行(操作)を行う
□: 作業担当として正しい操作が行われている事の確認を行う
C1: 作業が定められた内容で正しく行われている事の確認を行う
C2: 作業が正しい権限を持つ担当者により決められた手順で行われている事の確認を行う
●: 操作対象の物品

No	手順	アクター														
		A	B	C	D	E	F	①	②	③	④	⑤	⑥	⑦		
		鍵管理運用者1	鍵管理運用者2	金庫鍵管理者1	金庫鍵管理者2	作業立会者1	作業立会者2	KSK管理用記憶媒体	ZSK管理用記憶媒体	KSK/ZSK操作用PC	金庫	.jpゾーン署名サーバ	.jpゾーン署名サーバ格納用記憶媒体	TEB		
9	ZSK鍵ペアの削除【ZSK2回目以降】【初回無し】															
	9.01	鍵確認コマンドの実行	■	□			C1	C2			●					
	9.02	操作用アプリケーション上で、複数人認証を実施と削除対象ZSKの確認	■	□			C1	C2			●					
	9.03	操作用アプリケーションの起動	■	□			C1	C2			●					
	9.04	操作用アプリケーション上で、複数人認証 (K of N) を実施	■	■			C1	C2			●					
	9.05	操作用アプリケーション上で、2世代前のZSK鍵ペアを削除の実施	■	□			C1	C2		●	●					
	9.07	⑤jpゾーン署名サーバ へのコンソールによるログイン	■	□			C1	C2					●			
	9.08	所定のフォルダの2世代前のZSK鍵ペアの削除	■	□			C1	C2					●			
10	②ZSK管理用記憶媒体 の複製【KSK生成時、もしくは認証情報変更時のみ】															
	10.01	②ZSK管理用記憶媒体 東京(正)の内容の、東京(副)、大阪(正)、大阪(副)への複製	■	□			C1	C2		●	●					
	10.02	②ZSK管理用記憶媒体 東京(正)の③KSK/ZSK操作用PC からの抜	■	□			C1	C2		●	●					
	10.03	③KSK/ZSK操作用PCの停止	■	□			C1	C2			●					

凡例: ■: 作業担当として実行(操作)を行う
□: 作業担当として正しい操作が行われている事の確認を行う
C1: 作業が定められた内容で正しく行われている事の確認を行う
C2: 作業が正しい権限を持つ担当者により決められた手順で行われている事の確認を行う
●: 操作対象の物品

No	手順	アクター													
		A	B	C	D	E	F	①	②	③	④	⑤	⑥	⑦
		鍵管理運用者1	鍵管理運用者2	金庫鍵管理者1	金庫鍵管理者2	作業立会者1	作業立会者2	KSK管理用記憶媒体	ZSK管理用記憶媒体	KSK/ZSK操作用PC	金庫	.jpゾーン署名サーバ	.jpゾーン署名サーバ格納用記憶媒体	TEB
11	金庫の施錠													
	11.01	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥jpゾーン署名サーバ格納用記憶媒体 東京分の封印					■	□	●	●	●			●	●
	11.02	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、③KSK/ZSK操作用PC、⑥jpゾーン署名サーバ格納用記憶媒体 大阪分の封印【初回のみ】					■	□	●	●	●			●	●
	11.03	①KSK管理用記憶媒体、②ZSK管理用記憶媒体、大阪分の封印【2回目以降】					■	□	●	●	●			●	●
	11.04	10.01 で作成したTEBの金庫への格納	■	■			C1	C2	●	●	●	●		●	●
	11.05	金庫鍵1による施錠			■		C1	C2				●			
	11.06	金庫鍵2による施錠				■	C1	C2				●			
	11.07	金庫の状態の確認					■	□				●			
	11.08	金庫鍵1の封印					■	□				●			
	11.09	金庫鍵2の封印					■	□				●			
12	メインサイト作業解散 金庫鍵搬送													
	12.01	ケージ施錠			■										
	12.02	データセンタ退館	■	■	■	■	■	■							
	12.03	金庫鍵1の保管場所への搬送			■										
	12.04	金庫鍵1の格納			■										
	12.05	金庫鍵2の保管場所への搬送				■									
	12.06	金庫鍵2の格納				■									
	12.07	DRサイト用TEBの搬送			■	■			●	●	●	●		●	●