

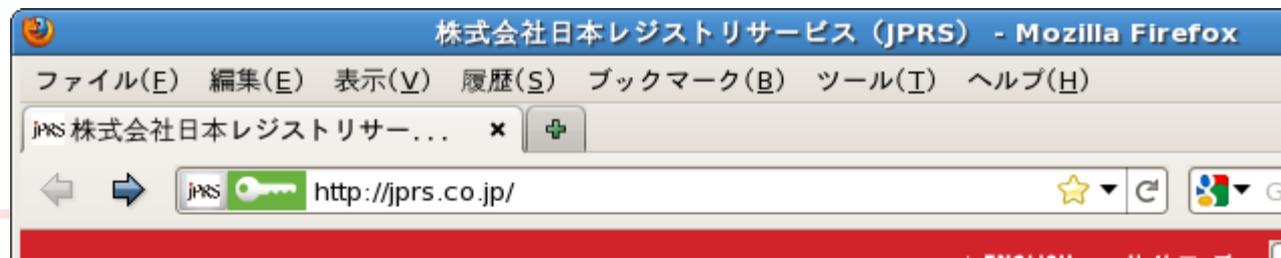
JPRS.CO.JPなどの鍵管理

- JPとの管理の違いを中心に -

野口 昇二

株式会社日本レジストリサービス

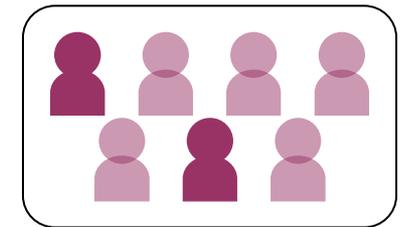
2011-07-15 JANOG28@日本橋



KSKの管理 (1/4)

1. 誰が、いつ、どこで作る?

- システム部門の社員
 - システム部門の担当者だけで作成
- 年1回、JPRSオフィス内で作成
 - オンラインのサーバー上で作成
 - 手順数は、10手順(約1時間)



KSKの管理 (2/4)

2. 秘密鍵のバックアップ方法は?
 - サーバーのストレージ上で作成するため、通常のファイルと同様にコピー

KSKの管理 (3/4)

3. 秘密鍵の保管場所は？

- 社外から直接アクセスできないサーバー
 - 権威DNSサーバーとは別のサーバに保管
 - システム部門の特定社員だけがアクセス可能
- 東京・大阪のサーバー上に保管
 - 大阪のサーバーへは、オンライン転送

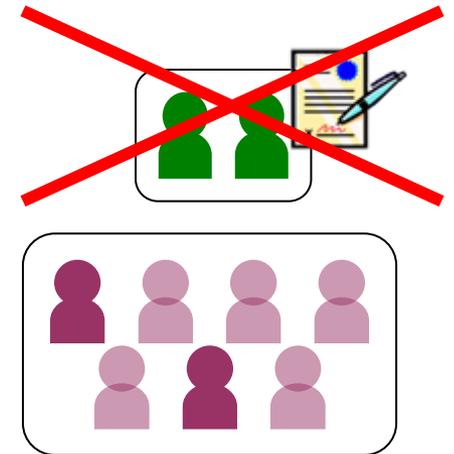
KSKの管理 (4/4)

4. 作成した署名鍵(DS)の申請は?
 - 業務部門に依頼
 - ドメイン名とNS設定・署名鍵(DS)の対応表を引き渡し
 - .jpゾーンへの反映は、15分程度

ZSKの管理 (1/4)

1. 誰が、いつ、どこで作る?

- システム部門の社員
 - システム部門の担当者だけで作成



- 4ヶ月に1回、JPRSオフィス内で作成
 - 手順数は、6手順(約1時間)
 - オンラインのサーバー上で鍵を作成

ZSKの管理 (2/4)

2. DNSKEYへの署名はどこで行われる?
 - KSKを保管しているサーバー上で実施
 - BIND 9.7のSmart Signing機能を利用
 - 署名結果(RRSIG)は、権威DNSサーバーへオンライン転送

ZSKの管理 (3/4)

3. 秘密鍵のバックアップ方法は?
 - サーバのストレージ上で作成するため、通常のファイルと同様にコピー

ZSKの管理 (4/4)

4. 秘密鍵の保管場所は?

- 社外から直接アクセスできないサーバー
 - KSKと同じサーバー
- 東京・大阪の2拠点に保管
 - 大阪のサーバーには、オンライン転送

JP と JPRS.CO.JPなどの対比

		JP	JPRS.CO.JPなど
KSK	誰が、いつ、どこで	JPRS外+JPRS、年1回、都内某所	JPRS、年1回、オフィス内
	バックアップ方法	スマートカード	ファイル複製
	保管場所	金庫	サーバー
	署名鍵(DS)の申請	rootへ	JPRSへ
ZSK	誰が、いつ、どこで	JPRS、月1回、都内某所	JPRS、4ヶ月1回、オフィス内
	DNSKEYへの署名	オフラインPC	サーバー
	バックアップ方法	暗号化USBストレージ	ファイル複製
	保管場所	金庫 + サーバー	サーバー

