.jprs ドメイン名における DNSSEC 運用ステートメント（.jprs DPS）

1. はじめに

本文書、すなわち「.jprsドメイン名における DNSSEC 運用ステートメント(.jprs DPS)」(以下「.jprs DPS」という)は、株式会社日本レジストリサービス(以下「JPRS」という)が、.jprs ドメイン名における DNSSEC 運用の考え方等について記述したものである。

1.1. 概要

JPRS は、.jprsドメイン名における DNSSEC(*1)運用についての情報を提供するため、.jprs DPS を公開する。
.jprs DPS は、.jprsドメイン名における DNSSEC サービス(以下「.jprs DNSSEC サービス」という)の安全性や運用の考え方、方式、手順等を網羅的に検討する目的から、IETF Domain Name System Operations Working Group で検討された DPS フレームワーク(*2)を用いて記述されている。.jprs DPS の章立ては以下の通りである。

1. はじめに
2. 情報公開
3. DNSSEC 運用における要件
4. 施設、管理および運用コントロール
5. 技術的なセキュリティコントロール
6. ゾーン署名
7. 準拠性監査
8. 法的事項

---

*1: DNSSEC(DNS Security Extensions)は、DNS 問い合わせへの応答に公開鍵暗号方式による署名を付加することで、応答の出自(正当な発信元であること)・完全性(改ざんのないこと)を問い合わせ側で検証可能にする仕組みである。DNSSEC の基本仕様は以下の標準プロトコル(RFC: Request for Comments)により規定されており、DNS プロトコルに対して DS、DNSKEY、RRSIG、NSEC 等の追加リソースレコードを定義している。

- RFC 4033
  DNS Security Introduction and Requirements
  https://www.ietf.org/rfc/rfc4033.txt

- RFC 4034
  Resource Records for the DNS Security Extensions
  https://www.ietf.org/rfc/rfc4034.txt

- RFC 4035
  Protocol Modifications for the DNS Security Extensions
  https://www.ietf.org/rfc/rfc4035.txt

*2: DPS（DNSSEC Practice Statement）は、DNSSEC 運用者が、その運用の考え方、方式、手順等を記述する文書である。DPS のフレームワークについては、以下の RFC 文書に記されている。

- RFC 6841
  A Framework for DNSSEC Policies and DNSSEC Practice Statements
  https://www.ietf.org/rfc/rfc6841.txt

1.2. 文書名とバージョン

文書名　　：.jprs ドメイン名における DNSSEC 運用ステートメント（.jprs DPS）
バージョン：1.6
公開日　　：2022/10/25
実施日　　：2022/10/25

1.3. コミュニティと適用性

.jprs DNSSEC サービスにおける関係者とその役割を説明する。

1.3.1. レジストリ

.jprs ドメイン名のレジストリは JPRS である。レジストリは、.jprs ドメイン名の登録管理と jprs ゾーンの DNS 運用を行う。.jprs DNSSEC サービスにおいて、レジストリは、jprs ゾーンの署名鍵（KSK、ZSK）（*3）を生成し、jprs ゾーンに署名を行う。更に、ルートゾーンに DS リソースレコードを登録することで、ルートゾーンのトラストアンカー（*4）を基点に jprs ゾーンのリソースレコードの出自・完全性を検証できるようにする。

---

*3: 署名鍵は、署名に用いる公開鍵と秘密鍵（私有鍵）のペアである。KSK は鍵署名鍵（Key Signing Key）、ZSK はゾーン署名鍵（Zone Signing Key）である。

*4: トラストアンカーは、署名検証を行うリゾルバが DNSSEC の信頼の連鎖（Chain of Trust）を構築するために基点として使用する KSK 相当の情報である。

1.3.2. レジストラ

レジストラは、.jprs ドメイン名登録申請等の取次に関する契約をレジストリと締結した者である。レジストラは、1.3.3 項に示す登録者または登録しようとしている者からの.jprs ドメイン名および DS リソースレコードについての各種申請をレジストリに取り次ぐ。

1.3.3. 登録者

登録者は.jprs ドメイン名を登録している者である。登録者は、当該.jprs ドメイン名に DNSSEC を導入する場合、署名鍵を生成し、当該ゾーン（以下「登録者ゾーン」という）に署名を行う。登録者は、DS リソースレコードをレジストラを通じてレジストリに登録することで、登録者ゾーンのリソースレコードの出自・完全性を検証できるようにする。署名鍵の生成、登録者ゾーンへの署名、DS リソースレコードの生成は、登録者の指示により、DNS プロバイダー（権威 DNS サーバの運用サービスを行う者）が行うことがある。

1.3.4. 依拠当事者

依拠当事者（Relying Party）は、DNS プロバイダー、キャッシュ DNS サーバ運用者、インターネットユーザー等、.jprs DNSSEC サービスに関わるすべての存在である。ここで、登録者ゾーンの管理を行う DNS プロバイダーを登録者ゾーン管理者という。登録者自身が登録者ゾーン管理者であることもある。

1.3.5. 監査人

.jprs DNSSEC サービスが.jprs DPS に則って運用されているかどうか監査する者をいう。

1.3.6. 適用範囲

.jprs DPS が適用される範囲は jprs ゾーンである。登録者ゾーンにおいてはそれぞれの運用方針が適用され、.jprs DPS の適用範囲外である。DNS ユーザーは、jprs ゾーンからの DNS 応答の出自・完全性を検証できる。登録者ゾーンからの DNS 応答の出自・完全性の検証は、.jprs DPS の適用範囲外である。

1.4. .jprs DPS の作成者および更新手続

1.4.1. 作成者

株式会社日本レジストリサービス（JPRS）

1.4.2. 連絡窓口

株式会社日本レジストリサービス（JPRS）.jprs DPS 担当
電話番号：03-5215-8451
（9:00-18:00 土日祝祭日および 12 月 29 日～1 月 3 日は除く）
電子メールアドレス：info@jprs.jp

1.4.3. 更新手続

.jprs DPS については、4.2.1 項に示される DPS 管理担当者による年次の定期見直しを行うほか、適宜見直しを行い、内容の更新を行う。同項に示される DNSSEC 運営会議により更新内容の承認が行われたのち、2 章の定めに従い、更新された.jprs DPS を公開する。

2. 情報公開

2.1. .jprs DPS の公開

2.1.1. .jprs DPS の公開に関わる運用組織

.jprs DPS の公開に関わる運用組織は、レジストリである JPRS とする。

2.1.2. .jprs DPS の公開場所

.jprs DPS（日本語）

https://nic.jprs/doc/jprs-dps-ja.pdf

.jprs DPS（英語）
https://nic.jprs/doc/jprs-dps-en.pdf

2.1.3. 公開情報に関するアクセスコントロール

レジストリは、.jprs DPS に関して、読み取り専用の制御以外に特段のアクセスコントロールを行わない。

2.2. 公開鍵の公開

レジストリは、jprs ゾーンの DS リソースレコードをルートゾーンに登録することで、DNSSEC の信頼の連鎖を構築可能にする。このため、jprs ゾーンの KSK 公開鍵のトラストアンカーとしての公開は行わない。
jprs ゾーンの KSK 公開鍵と ZSK 公開鍵は、6.4 節で示されるロールオーバーの実施期間中に jprs ゾーンの DNSKEY リソースレコードへの反映を行い、公開される。

3. DNSSEC 運用における要件

3.1. ドメイン名の意味

.jprs ドメイン名の登録は、インターネット上での識別子として用いることを目的として行うもので、当社が管理する.jprs ドメイン名空間におけるドメイン名の一意性を意味し、これ以外のいかなる意味も有さない。

3.2. 登録者ゾーンに関する申請者の本人性確認

登録者ゾーンに関する申請者の本人性確認は、当該.jprs ドメイン名を管理するレジストラ（以下「管理レジストラ」という）によって行われる。レジストリは、所定のレジストラ認証手続を通じて、DS リソースレコードの登録等の申請が管理レジストラにより行われていることを確認する。

3.3. DS リソースレコードの登録

jprs ゾーンに登録者ゾーンの DS リソースレコードを登録することにより、登録者ゾーンの DNSSEC による検証が可能となる。DS リソースレコードの仕様は、RFC 5910 の 4.1 項の記述に従う。

- RFC 5910
  Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

https://www.ietf.org/rfc/rfc5910.txt

3.3.1. 登録可能者

レジストリは、管理レジストラからの申請に基づき、登録者ゾーンの DS リソースレコードを jprs ゾーンに登録する。管理レジストラは、登録申請において登録者の意思を確認する。

3.3.2. 登録手続

登録者は、管理レジストラに DS リソースレコードの登録を依頼する。管理レジストラは登録者の意思に基づき、レジストリ所定の手続を用いて DS リソースレコードの登録申請を行う。これを受け、レジストリは jprs ゾーンに当該 DS リソースレコードを登録する。レジストリにおける登録申請受領から jprs ゾーンへの DS リソースレコードの登録までに要する時間は.jprs DNS の更新スケジュールに準ずる。
登録者ゾーンで使用されている署名鍵に対応する DS リソースレコードが、レジストリが管理する jprs ゾーンに登録され、レジストリの署名鍵で署名されることにより、登録者ゾーンと jprs ゾーンの信頼の連鎖が構築される。

3.3.3. 緊急の登録

本文書では、規定しない。

3.4. 秘密鍵保有事実の確認

レジストリは、登録者ゾーン管理者が DS リソースレコードに対応する秘密鍵を保有することに関する、管理レジストラの確認要件を規定しない。

3.5. DS リソースレコードの削除

jprs ゾーンから登録者ゾーンの DS リソースレコードを削除することにより、登録者ゾーンの DNSSEC による検証は不可となる。

3.5.1. 削除可能者

レジストリは、管理レジストラからの申請に基づき、登録者ゾーンの DS リソースレコードを jprs ゾーンから削除する。管理レジストラは、削除申請において登録者の意思を確認する。

3.5.2. 削除手続

登録者は、管理レジストラに DS リソースレコードの削除を依頼する。管理レジストラは登録者の意思に基づき、レジストリ所定の手続を用いて DS リソースレコードの削除申請を行う。これを受け、レジストリは jprs ゾーンから当該 DS リソースレコードを削除する。レジストリにおける削除申請受領から jprs ゾーンからの DS リソースレコードの削除までに要する時間は.jprs DNS の更新スケジュールに準ずる。

3.5.3. 緊急の削除

本文書では、規定しない。

4. 施設、管理および運用コントロール

4.1. 物理的管理

4.1.1. 施設の位置と構造

レジストリは、.jprs DNSSEC サービスに関わる重要な設備・機器（以下「重要設備」という）を、水害、地震、火災、落雷その他の災害の被害を容易に受けない場所（以下「重要設備室」という）に設置する。耐震・耐火および不正侵入防止については建物構造上の対策を行う。建物の内外には、重要設備室の所在についての表示を行わない。

4.1.2. 物理的なアクセス

レジストリは、重要設備室に関して、事前に定められた本人の特定および入室権限の確認を可能とする入退室管理を行う。レジストリは、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、あらかじめ.jprs DNSSEC サービスの管理を行う者の許可を得て、入室権限者同行のうえでこの者を入室させることとする。

4.1.3. 電力と空調

レジストリは、重要設備の運用のために十分な容量の電源を確保するとともに、瞬断、停電および電圧・周波数の変動に備えた対策を講ずる。また空調設備に関して、使用する機器類に悪影響を与えないよう維持管理する。

4.1.4. 水害および地震対策

レジストリは、重要設備室に防水対策を施し、浸水による被害を最小限に抑える。また、.jprs DNSSEC サービスに関わる設備・機器を設置する建物は、耐震構造とし、機器および什器の転倒および落下を防止する対策を講ずる。

4.1.5. 火災防止対策

レジストリは、重要設備を防火区画内に設置する。また防火区画内では電源設備や空調設備の防火措置を講じ、火災報知器および消火設備の設置を行う。

4.1.6. 媒体保管場所

レジストリは、.jprs DNSSEC サービスに関わる重要なアーカイブデータ、バックアップデータを含む記録媒体を適切な入退室管理が行われた室内の保管庫に保管する。

4.1.7. 廃棄処理

レジストリは、.jprs DNSSEC サービスに関わる秘密扱いとする情報を含む書類・記録媒体について、情報の初期化・裁断等、事前に定められた方法に従い適切に廃棄処理を行う。

4.1.8. オフサイトでのバックアップ

レジストリは、.jprs DNSSEC サービスに関わる特定の重要情報を、十分に遠隔な複数拠点に設置した重要設備室内の施錠可能な保管庫に保管する。

4.2. 手順の管理

4.2.1. 信頼される役割

.jprs DNSSEC サービスの運用に関わる役割を以下に示す。

役割名称（役割略称）

- 役割の説明

DNSSEC 運営会議（運営会議）

・ .jprs DNSSEC サービス運用の統括

・ .jprs DPS 改訂の承認

DPS 管理責任者（DPS 管理責任者）

・ DPS 管理担当者の任命

・ .jprs DPS 改訂案の確認

DPS 管理担当者（DPS 管理担当者）

・ .jprs DPS 改訂案の作成

DNSSEC 署名鍵運用責任者（署名鍵運用責任者）

・ DNSSEC 署名鍵運用担当者の任命

DNSSEC 署名鍵運用担当者（署名鍵運用担当者）

・ .jprs DNSSEC サービスに使用する KSK のアクティベーション

・ 同 KSK・ZSK の生成・廃棄

・ 同 KSK・ZSK のロールオーバー（更新）

・ 同 KSK・ZSK による jprs ゾーンへの署名作成

・ 同 KSK のルートゾーンへの登録

・ 同 KSK によるオペレーションの記録・保管

・ その他、DNSSEC 署名鍵運用責任者の指示に基づく運用

DNSSEC 金庫鍵管理責任者（金庫鍵管理責任者）

・ DNSSEC 金庫鍵管理担当者の任命

DNSSEC 金庫鍵管理担当者（金庫鍵管理担当者）

・ .jprs DNSSEC サービスに使用する KSK のアクティベーションの際の操作への立ち会い

DNSSEC キーセレモニー証跡記録責任者（証跡記録責任者）

・　DNSSEC キーセレモニー証跡記録担当者の任命

DNSSEC キーセレモニー証跡記録担当者（証跡記録担当者）

・　DNSSEC キーセレモニーの証跡記録

DNSSEC 業務監査人（監査人）

・　DNSSEC 業務監査の実施

4.2.2. それぞれのタスクに必要な人員数

署名鍵運用担当者による担当タスク遂行の際は、複数人の構成とする。KSK のアクティベーションを含むタスクを遂行する際は、これに金庫鍵管理担当者を加えた構成とする。

4.2.3. 個々の役割に対する本人性確認と認証

重要設備を操作する権限は、操作を行う人員ごとに設定される。重要設備の使用においては、操作を行う人員を認証のうえ、あらかじめ設定された操作権限が付与される。

4.2.4. 権限の分離

署名鍵運用担当者と金庫鍵管理担当者は、同一人員が任命されることはない。これにより、署名鍵運用担当者のみによる KSK のアクティベーションを不可とする。

4.3. 人員管理

4.3.1. 資格、経験および身分証明の要件

4.2.1 項に示す「信頼される役割」を担う者は、レジストリの社員またはレジストリが特に認めた者とする。

4.3.2. 背景調査手順

本文書では、規定しない。

4.3.3. トレーニング

レジストリは、4.2.1 項に示す「信頼される役割」を担う者に対するトレーニングを次のように行う。

- 4.2.1 項に示す「信頼される役割」を担う者が役割に就く前に、その運用に必要なトレーニングを実施する
- 運用手順に変更がある場合、運用手順書の必要箇所を遅滞なく変更し、その変更に関わるトレーニングを実施する

レジストリは、4.2.1 項に示す「信頼される役割」を担う者に対する再トレーニングの必要性を定期的に検証する。また、必要な場合、再トレーニングを行う。

4.3.4. 仕事のローテーションの頻度と順序

本文書では、規定しない。

4.3.5. 認められていない行動に対する処罰

本文書では、規定しない。

4.3.6. 独立した契約者の要件

本文書では、規定しない。

4.3.7. 資料の開示

レジストリは、.jprs DNSSEC サービスの運用に必要な文書一式を運用人員に開示し周知する。

4.4. イベントログ記録手順

4.4.1. 記録されるイベントの種類

.jprs DNSSEC サービスに関わるシステムにおける誤操作・不正操作の検知および監査における運用の正当性の証明に必要なログ（以下「イベントログ」という）として、レジストリは次のイベントについての履歴を記録する。

- .jprs DNSSEC サービスの設備へのアクセス履歴に関する記録
- 署名鍵に関する操作の記録

+ .jprs DNSSEC サービスに使用する KSK のアクティベーション
+ 同 KSK・ZSK の生成・廃棄
+ 同 KSK・ZSK のロールオーバー
+ 同 KSK・ZSK による jprs ゾーンへの署名作成
+ 同 KSK のルートゾーンへの登録

・ イベントログの記録事実の確認

イベントの記録には、日付、時刻、イベントを発生させた主体、イベント内容を含む。

4.4.2. イベントログを処理する頻度

レジストリは、深刻なセキュリティ侵害が発生した場合等に備え、十分迅速に把握可能な頻度においてイベントログの機械的な確認処理を行う。この処理において対処すべき記録が検出された場合、適切な人員に対して即時の通知を行う。

4.4.3. イベントログを保持する期間

レジストリは、イベントログを最低 3 か月間は迅速にアクセス可能な方法により保持する。なお、イベントログは最低 3 年間保持する。

4.4.4. イベントログの保護

レジストリは、イベントログにアクセスできる者を必要な人員のみに制限し、アクセスを許可されていない者によるイベントログの閲覧、改変または削除から保護する。

4.4.5. イベントログのバックアップ手続

レジストリは、イベントログを外部記憶媒体に定期的にバックアップする。それら媒体は適切な入退室管理が行われている室内の施錠可能な保管庫に保管される。

4.4.6. イベントログ情報の取得システム

オンラインのイベントログ取得システムは.jprs DNSSEC サービスに用いるシステム（以下「.jprs DNSSEC サービスシステム」という）の一要素であり、その存在場所は.jprs DNSSEC サービスシステムと同一である。オフラインのイベントログは各々の作業担当者により記録され、レジストリ管理施設内の安全な保管庫に保管される。

4.4.7. 脆弱性評価

レジストリは、4.4.2 項に示す方針に基づき、.jprs DNSSEC サービスシステムへのセキュリティ侵害試行等の許可されない行為について確認を行うとともに、必要に応じ、システムの脆弱性分析を行う。

4.5. 危殆化と事故・災害

4.5.1. 危殆化と事故・災害への対処

レジストリは、jprs ゾーンの秘密鍵の危殆化または危殆化のおそれがある場合、署名鍵の緊急ロールオーバーを行う。事故・災害により、.jprs DNSSEC サービスが中断または停止した場合、.jprs DNSSEC サービスの速やかな再開に努める。

4.5.2. コンピューター資源の破損

レジストリは、.jprs DNSSEC サービスに関わる重要なハードウェア、ソフトウェアまたはデータが破損した場合、事前に定められた復旧計画に従い、バックアップ用のハードウェア、ソフトウェアまたはデータにより、速やかな復旧作業に努める。

4.5.3. 秘密鍵が危殆化した場合の手続

レジストリは、jprs ゾーンの KSK が危殆化した場合、次の手続を行う。

- jprs ゾーンの KSK の再生成
- jprs ゾーンの署名鍵への再生成した KSK による署名
- ルートゾーンに登録している DS リソースレコードの置き換え

jprs ゾーンの ZSK が危殆化した場合、次の手続を行う。

- jprs ゾーンの ZSK の再生成
- 再生成した ZSK を含む jprs ゾーンの署名鍵への KSK による署名
- 再生成した ZSK による jprs ゾーンへの署名

4.5.4. 災害後の事業継続能力

レジストリは、災害により.jprs DNSSEC サービスの設備が被害を受け、運用を継続できない場合は、あらかじめ構築した遠隔バックアップサイトにおいて速やかにサービスの回復に努める。

また、レジストリは、災害等により、DNSSEC キーセレモニーが通常の手順にて実施できない場合、事前に定められた緊急時の手順にて実施する。

4.6. 組織の閉鎖

レジストリの閉鎖により.jprs DNSSEC サービスの継続が不能となる場合に備え、.jprs DNSSEC サービスに必要な情報をエスクロー・エージェントに預託する。

- .jprs Registry Agreement
  https://www.icann.org/en/about/agreements/registries/jprs/

レジストリが閉鎖する場合、レジストリが規定する業務終了手続に従い、.jprs DNSSEC サービスを終了する。

5. 技術的なセキュリティコントロール

5.1. 署名鍵の生成と導入

5.1.1. 署名鍵の生成

.jprs DNSSEC サービスに用いる署名鍵は、重要設備室内に設置したオフラインのシステム環境（以下「.jprs DNSSEC サービスオフラインシステム」という）において、複数人の署名鍵運用担当者により生成される。
KSK は、.jprs DNSSEC サービスオフラインシステムに接続された暗号モジュール内部において専用のソフトウェアを用いて生成される。ZSK は、.jprs DNSSEC サービスオフラインシステムで生成され、暗号化処理を施した着脱可能なメディア（以下「暗号化メディア」という）内に格納される。

5.1.2. 公開鍵の配布

レジストリは、生成した KSK 公開鍵および ZSK 秘密鍵・公開鍵を、暗号化メディアを用いて.jprs DNSSEC サービスシステムに導入する。DNS プロトコル以外の手段を用いた KSK 公開鍵の依拠当事者への配布は行わない。

5.1.3. 署名鍵パラメータの品質管理

レジストリは、署名鍵の作成において、技術動向に照らし適切なパラメータが採用されていることを定期的に確認する。

5.1.4. 署名鍵の使用目的

レジストリは、署名鍵を.jprs DNSSEC サービスにおける署名を生成するために使用し、これ以外のいかなる用途にも使用しない。

5.2. 秘密鍵保護と暗号モジュール管理

5.2.1. 暗号モジュール標準と管理

本文書では、規定しない。

5.2.2. 複数人による秘密鍵管理

KSK 秘密鍵の操作は、複数人の署名鍵運用担当者により行う。

5.2.3. 秘密鍵のエスクロー

秘密鍵のエスクローは行わない。

5.2.4. 秘密鍵のバックアップ

署名鍵運用担当者は、KSK 秘密鍵のバックアップを暗号モジュールに複数コピー作成する。この暗号モジュールは、4.1.8 項に示されるそれぞれの重要設備室内の施錠可能な保管庫に格納される。

5.2.5. 暗号モジュール内の秘密鍵の保管

本文書では、規定しない。

5.2.6. 秘密鍵のアーカイブ

5.2.4 項に示すバックアップ以外には、使用を停止した秘密鍵のアーカイブは行わない。

5.2.7. 暗号モジュールに対する秘密鍵の導入・取り出し

暗号モジュールへの KSK 秘密鍵導入後は、これを取り出すことはできない。また、暗号モジュール内の KSK 秘密鍵使用の際は、複数人の署名鍵運用担当者による操作を必要とする。暗号化メディアに対する ZSK 秘密鍵の導入については、複数人の署名鍵運用担当者による操作を必要とする。

5.2.8. 秘密鍵のアクティベーション

KSK 秘密鍵は、金庫鍵管理担当者による立ち会いのもと、.jprs DNSSEC サービスオフラインシステムにおいて、複数人の署名鍵運用担当者によりアクティベート（活性化）される。ZSK 秘密鍵は、複数人の署名鍵運用担当者によりアクティベートされる。ZSK 秘密鍵のアクティブな状態は使用を停止するまで継続する。

5.2.9. 秘密鍵のディアクティベーション

KSK 秘密鍵は、金庫鍵管理担当者による立ち会いのもと、署名鍵運用担当者が使用する都度ディアクティベート（不活化）される。
ZSK 秘密鍵は、5.3.2 項に定義される使用期間を上限として、複数人の署名鍵運用担当者によりディアクティベートされる。

5.2.10. 秘密鍵の消去

使用期間を過ぎた KSK 秘密鍵および ZSK 秘密鍵は、署名鍵運用担当者により、使用が不可能になるような方法で消去される。

5.3. 署名鍵管理についての補足事項

5.3.1. 署名鍵のライフサイクル

KSK のライフサイクルを以下に示す。

- KSK の生成
- KSK の jprs ゾーンおよびルートゾーンでの公開
- KSK のルートゾーンおよび jprs ゾーンからの削除
- KSK の廃棄

ZSK のライフサイクルを以下に示す。

- ZSK の生成
- ZSK の jprs ゾーンでの公開
- ZSK の有効化
- ZSK の無効化
- ZSK の jprs ゾーンからの削除
- ZSK の廃棄

5.3.2. 署名鍵の使用期間

KSK の使用期間の上限は 1 年に適切な併行運用期間を加えたものとする。ZSK の使用期間の上限は 1 か月とする。レジストリは、特に必要な場合、これらの期間を変更することがある。

5.4. アクティベーション情報

5.4.1. アクティベーション情報の生成と導入

アクティベーション情報とは、KSKをアクティベートするために使われるパスフレーズのセットをいう。署名鍵運用担当者が個々のパスフレーズを生成し、.jprs DNSSEC サービスオフラインシステムに導入する。

5.4.2. アクティベーション情報の保護

それぞれの署名鍵運用担当者は、十分安全な方法によりアクティベーション情報を保護する。

5.4.3. アクティベーション情報についての補足事項

署名鍵運用担当者は、緊急の場合に備え、アクティベーション情報の複製を作成し、タンパ証跡（耐タンパ性）のある封書に封印する。この封印を解く必要がある場合は、署名鍵運用責任者の指揮の下で行う。

5.5. コンピューターのセキュリティ管理

.jprs DNSSEC サービスシステムにおける重要なコンピューター（以下「重要コンピューター」という）では、レジ

ストリが規定する必要最小限のソフトウェアのみを稼働させることとする。重要コンピューターに対して行われた重要な操作については、イベントログが残るよう設定する。重要コンピューターにアクセスするためのすべての認証情報について、適切な管理を行う。重要コンピューターに対するリソース監視を継続的に行い、異常や不正操作を検知した際は、速やかに適切な対策を実施する。

5.6. ネットワークのセキュリティ管理

.jprs DNSSEC サービスシステムを配置するネットワークにはファイアウォールを適用し、レジストリが規定する必要最小限の通信に制限する。

5.7. タイムスタンプ

レジストリは、.jprs DNSSEC サービスオフラインシステムについて、信頼できる時刻源から時刻を取得し、時刻同期を行う。.jprs DNSSEC サービスシステムについては、NTP（ネットワークタイムプロトコル）により時刻を取得し、時刻同期を行う。これらの時刻は、4.4 節に示されるイベントログの記録時刻および RRSIG リソースレコードにおける署名有効期間の開始時刻と終了時刻として使用される。

5.8. 技術上のライフサイクル管理

5.8.1. システム開発の管理

レジストリは、.jprs DNSSEC サービスシステムの品質およびセキュリティを保つために、システム開発時における各工程の管理、導入前のシステム評価等を実施する。

5.8.2. システムのセキュリティ管理

レジストリは、.jprs DNSSEC サービスシステムのセキュリティ管理として、入退室管理、教育を含む要員管理、権限管理等の運用管理、不正侵入対策、ウイルス対策等のシステム的なセキュリティ対策を実施する。

5.8.3. ライフサイクルのセキュリティ管理

レジストリは、.jprs DNSSEC サービスシステムの開発が規定された方法により管理されているか定期的に評価する。併せて、セキュリティに関する情報収集を行い、技術動向等を考慮したうえで、システムの評価および改善を行う。

6. ゾーン署名

6.1. 鍵長、鍵種別とアルゴリズム

jprs ゾーンで使用する署名鍵の鍵種別は、KSK と ZSK の 2 種とする。KSK では RFC 4034 で定義された SEP フラグを設定し、ZSK では SEP フラグを設定しない。
jprs ゾーンで使用する署名鍵のアルゴリズムには、標準プロトコルで定義されるものを用いる。署名鍵のアルゴリズムと鍵長は、使用期間に対して安全と考えられるものを用いる。KSK、ZSK ともにアルゴリズムを RFC 5702 で定義された RSASHA256 とし、KSK の鍵長を 2048 ビット、ZSK の鍵長を 1024 ビットとする。

6.2. 不在証明

jprs ゾーンの不在証明には、RFC 5155 で定義された NSEC3 リソースレコードを用いる方式を採用する。NSEC3 の運用においてはオプトアウト方式を採用し、ハッシュアルゴリズムは SHA-1、繰り返し回数は 0 回、ソルトは無指定とする。

6.3. 署名フォーマット

jprs ゾーンの署名には、RFC 5702 で定義された RSA/SHA-2 によるフォーマットを用いる。

6.4. 署名鍵のロールオーバー

6.4.1. ZSK のロールオーバー

jprs ゾーンでは、ZSK のロールオーバーは月次で行う。更新方式には事前公開法（Pre-Publish; RFC 6781）を用いる。

6.4.2. KSK のロールオーバー

jprs ゾーンでは、KSK のロールオーバーは年次で行う。更新方式には二重署名法（Double Signature; RFC 6781）を用いる。

6.5. 署名の有効期間と再署名頻度

jprs ゾーンでは、KSK による署名有効期間をおおむね 2 か月、ZSK による署名有効期間をおおむね 1 か月とする。KSK による再署名は 1 か月ごと、ZSK による再署名は 1 週間ごとに行う。

6.6. リソースレコードの検証

レジストリは、ゾーン公開前にすべてのリソースレコードが標準プロトコルに準拠していることを検証する。

6.7. リソースレコードの TTL

jprs ゾーンでは、DNSKEY およびこれに対する RRSIG の TTL は 86400（1 日）とする。DS およびこれに対する RRSIG の TTL は 7200（2 時間）とする。NSEC3 およびこれに対する RRSIG の TTL は jprs ゾーンのネガティブキャッシュ値と同じ 900（15 分）とする。
これらの TTL については、技術動向等に照らし、より適切と考えられる値に変更することがある。

7. 準拠性監査

.jprs DNSSEC サービスの運用にあたり、1.3.5 項に示す監査人による定期的な監査を行う。監査結果はレジストリに通達され、レジストリは必要に応じた運用改善の計画・実施を行う。

8. 法的事項

レジストリは、.jprs DPS に記述される事項に基づいては、何人に対しても法的責任は負わないものとする。
レジストリは、.jprs DNSSEC サービスの運用にあたり、日本国法およびレジストリが定める各種ルールに従う。

- .jprs ドメイン名規則
  https://nic.jprs/doc/jprs-registration-policies.pdf

更新履歴：

2014/03/19 v1.0

- 初版

2015/06/29 v1.1

- 信頼される役割の名称および説明の変更
- その他、一部表記の修正

2015/10/01 v1.2

- 資格、経験および身分証明の要件の変更
- その他、一部表記の修正

2019/08/01 v1.4

- バージョン情報の更新

2021/09/01 v1.5

- 信頼される役割の追記
- その他、一部表記の修正

2022/10/25 v1.6

- 災害等によりキーセレモニーが実施不可能な場合の対処に関する記載追加
- 不在証明として利用する NSEC3 パラメータ仕様の修正
