ホワイトペーパーの紹介：

- DNSSECを利用するリゾルバーのためのトラストアンカーの設定方法について 第2版
  社団法人日本ネットワークインフォメーションセンター
- DNSSECにおける鍵管理
  株式会社サリオンシステムズリサーチ
  東京エレクトロン　デバイス株式会社
- DNSサーバDNSSEC導入　鍵管理チェックリスト
  株式会社サリオンシステムズリサーチ
  東京エレクトロン　デバイス株式会社

社団法人日本ネットワークインフォメーションセンター
木村泰司

DNSSECと「鍵」

- DNSSECにおける電子署名
  - リソースレコードに電子署名
  - DNSレスポンスの署名検証（完全性チェック）
    - 改ざんされていないことを確認

  ⇒ 秘密鍵の安全性に依存
- DNSSECにおける鍵の正しさ
  - 各ゾーンの鍵が正しいものであることは、DNSのツリーに対応して担保

○リゾルバー／DNSキャッシュサーバ運用者　⇒　鍵を正しく入手

○DNSサーバ（コンテンツサーバ）運用者　⇒　秘密鍵を保護

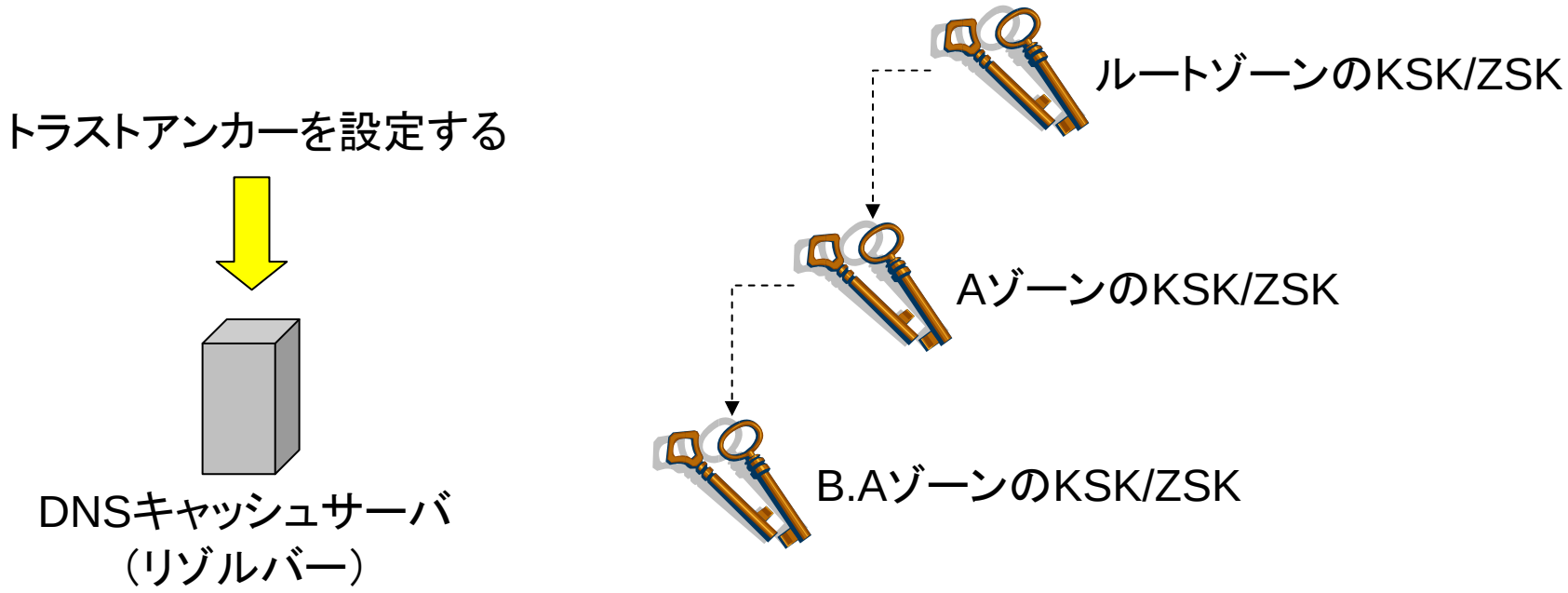
DNSSECを利用するリゾルバーのための トラストアンカーの設定方法について 第2版

（5ページ）
DNSSECを利用するDNSキャッシュサーバ（またはリゾルバー）のために、
現段階でよいと考えられる、トラストアンカーのデータを入手し確認する
方法を説明

社団法人 日本ネットワークインフォメーションセンター

トラストアンカーとは何か

- リゾルバーにおける署名検証の基点
  - ゾーンのKSK公開鍵またはそのハッシュ値



ルートゾーンのトラストアンカーデータ

- 入手元
  - https://data.iana.org/root-anchors/
- 確認方法
  - OpenPGP
  - 電子証明書を使った電子署名

確認方法（OpenPGP） 1、署名の検証

1. “DNSSEC Manager”の鍵を入手
   - （実行例）
     $ gpg –search-keys –keyserver pgp.mit.edu “DNSSEC Manager”
2. Xmlファイルとascファイル（署名データ）を入手
   - （実行例）
     $ fetch http://data.iana.org/root-anchors/root-anchors.xml
     $ fetch http://data.iana.org/root-anchors/root-anchors.asc
3. 署名を検証
   - （実行例）
     $ gpg --verify root-anchors.asc root-anchors.xml

確認方法（OpenPGP） ２、DSレコードとの比較

1. ルートゾーンのDSレコードを問い合わせ
   - （実行例）
     $ dig . dnskey | grep 257 > rootzone-dnskey
     $ dnssec-dsfromkey -2 –f rootzone-dnskey
     （DSレコードの形で出力される）
2. root-anchors.xmlに含まれるハッシュ値と比較
   - （実行例）
     $ cat root-anchors.xml
     （1の出力の中のハッシュ値と比較）

- （確認）DNSSECオプションを有効にして問い合わせ
  - （実行例）
    $ dig . ns +dnssec

日常的な運用のために

- ルートゾーンのDNSSECに関する最新情報
  - http://www.iana.org/dnssec/
- アナウンス用のメーリングリスト
  - root-dnssec-announce
    https://mm.icann.org/mailman/listinfo/root-dnssec-announce

DNSSECにおける鍵管理

（9ページ）
DNSSEC における暗号鍵の重要性と脅威である攻撃手法、そして使用される鍵の種類を説明したあと、鍵のライフサイクル各フェーズにおける考慮点と注意事項を解説

社団法人 日本ネットワークインフォメーションセンター

DNSSECにおける暗号鍵の重要性

- 秘密鍵が侵害された場合の影響
  - 正規のゾーン管理者が鍵を使用できなくなる
    - DoSになりうる。鍵をロールオーバーする必要があるが、これには時間がかかる。
  - 攻撃者がゾーン管理者になりすます
    - 虚偽のリソースレコードを作成し、下位ゾーンを捏造することが可能になる。
    - 事実上、署名のないゾーンと同じレベルに引き下げられてしまう。

DNSSECの暗号鍵に対して考えられる攻撃内容と対策

- ブルートフォース攻撃
- アルゴリズムの脆弱性をついた攻撃
- 不十分な情報エントロピーをついた攻撃
- 物理的な攻撃や盗難
- 破壊

DNSSECにおける鍵のライフサイクル

- ライフサイクル
  - 鍵生成
    - 暗号アルゴリズム、鍵長、乱数発生器
  - 保存及び保護
    - バックアップ
  - 暗号操作実行
  - 更新
  - 失効処理および廃棄

鍵の保護とアクセス

- 鍵の保護の手法
  - 鍵をサーバに保存しない。
  - 秘密鍵ファイルを保持するマシンをオフラインにする。
  - 適切な管理グループに属するユーザーのみがアクセスできるようにする。
- Hardware Security Module（HSM）
  - 鍵がハードウェアの中にのみ存在
  - 物理的保護
  - 乱数発生器

DNSサーバDNSSEC導入　鍵管理チェックリスト

（6ページ）
DNS サーバへのDNSSEC 導入に伴い、鍵の作成と管理において考慮しなければならない確認事項を取りまとめ、チェックリストとして提示

社団法人 日本ネットワークインフォメーションセンター

鍵管理チェックリスト(1)

- ZSKとKSKの秘密鍵の管理
- DNSSEC導入に伴う鍵の作成と管理における確認事項
- 6種類のチェック分野
  - 鍵の生成は、適切な方法、パラメータを用いて行わなければならない
  - 外部から鍵へ不正なアクセス(読み取り、利用、生成、更新)が行われないよう、対策が講じられていなければならない。
  - 内部から鍵へ不正なアクセスが行われないよう、対策が講じられていなければならない
  - 鍵の管理・利用は、適切な方法で行わなければならない
  - 鍵の危殆化もしくは破損時の対策および対応方法を、あらかじめ定めておかなければならない
  - 適切な運用がなされているか、定期的に監査を行わなければならない

鍵管理チェックリスト(2)

項番	確認項目	結果 OK / NG
鍵の生成は、適切な方法、パラメータを用いて行わなければならない。		
1	ZSK の鍵長は 1024 ビット以上である※1	
2	KSK の鍵長は 2048 ビット以上である	
3	署名アルゴリズムとして、RSA/SHA-256 または RSA/SHA-512 を使用している	
4	鍵の生成には、RFC 4086 または NIST SP 800-90 に準拠した乱数生成器等で発生させた安全な乱数を使用している	
5	使用している署名アルゴリズム、OS、ライブラリ等に脆弱性は見つかっていない	
外部から鍵へ不正なアクセス(読み取り、利用、生成、更新)が行われないよう、対策が講じられていなければならない		
6	外部からの不正なアクセスが行えないよう、ゾーンファイルへの署名操作および署名されるゾーンファイルのマスターコピーの保管をオフライン環境に限定するなど、対策が施されている	
内部から鍵へ不正なアクセスが行われないよう、対策が講じられていなければならない		
7	内部からの鍵へのアクセスは権限を有する管理者のみに限定するなど、対策が施されている	
8	KSK 秘密鍵は、暗号化を施したリムーバルメディア等へ保存するか、HSM 等を使用するなど、物理的に保護されている	
9	KSK の生成および利用には、複数人の立会いを必須としている	