フルリゾルバ bowline における KeyTrap 対策

2025年11月26日

株式会社インターネットイニシアティブ
技術研究所
日比野 啓

自己紹介

- 日比野 啓
- 所属: IIJ技術研究所

- 以前 - 50万ID規模の ISP で Radius 認証サーバーバックエンドシステムの構築
  - アーキテクチャ設計
  - Radius サーバー実装
  - 検証、導入支援
- 2022 - DNS の研究開発として、フルリゾルバ　bowline を実装

DNS フルリゾルバ bowline

bowline(もやい結び) という DNSフルリゾルバを実装しています

- DoT / DoH2 / DoH3 / DoQ
- DNSSEC 検証
  - DS (委任の信頼チェーン検証) / RRSIG (署名検証)
    - **KeyTrap 対策 (今回の話)**
  - NSEC / NSEC3 (不在証明)
- 各種拡張機能

- STM(Software Transactional Memory) と軽量スレッドによる並列処理
  - Haskell で実装
- 優先度付きキューによるキャッシュ

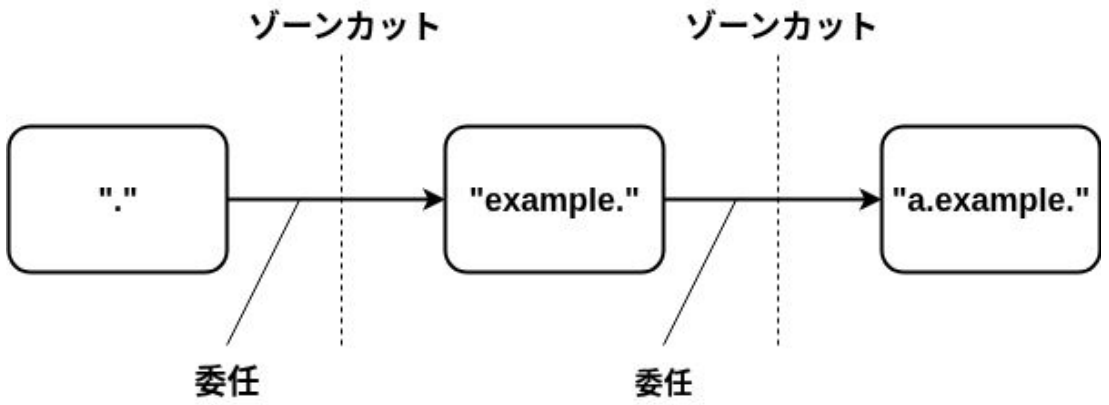
DNS ツールチェインの整理と部品化

KeyTrap とは

- KeyTrap: DNSSEC の検証操作を多数、実行させることで CPU 資源を枯渇させる攻撃
  - HashTrap: DS のハッシュの照合の回数
    - e.g. 1357 DSs * 1357 keys
  - KeySigTrap: RRSet の署名の検証の回数
    - e.g. 589 keys * 519 sigs

KeyTrap とは

- KeyTrap: DNSSEC の検証操作を多数、実行させることで CPU 資源を枯渇させる攻撃
  - HashTrap: DS のハッシュの照合の回数
    - e.g. 1357 DSs * 1357 keys
  - KeySigTrap: RRSet の署名の検証の回数
    - e.g. 589 keys * 519 sigs



KeyTrap とは

- KeyTrap: DNSSEC の検証操作を多数、実行させることで CPU 資源を枯渇させる攻撃
  - HashTrap: DS のハッシュの照合の回数
    - e.g. 1357 DSs * 1357 keys
  - KeySigTrap: RRSet の署名の検証の回数
    - e.g. 589 keys * 519 sigs

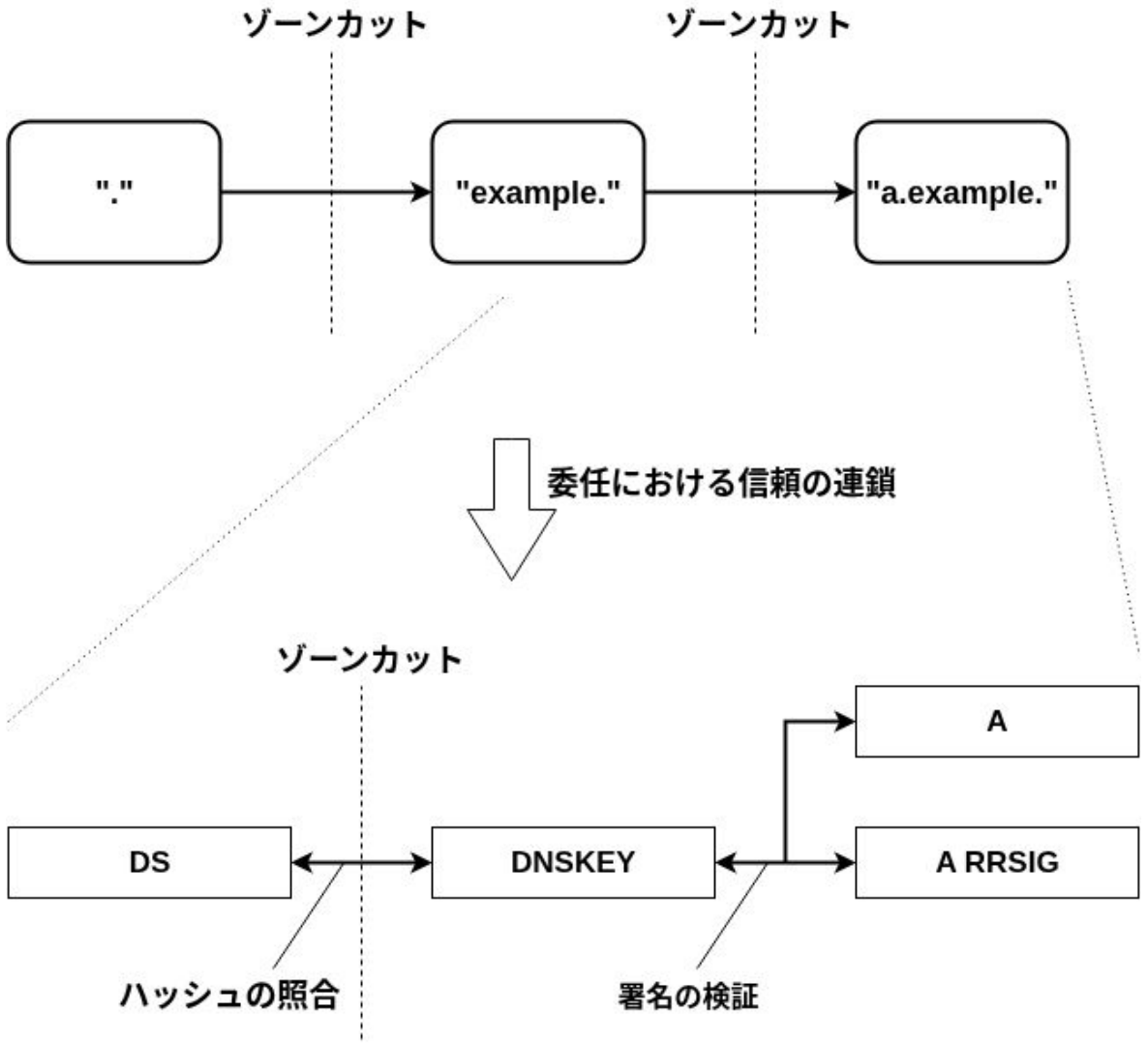
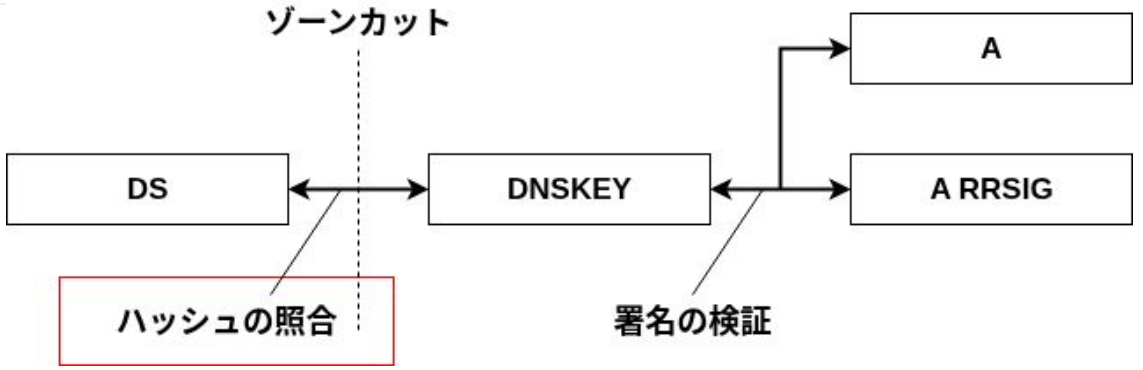


図: ゾーンカットと DNSSECの信頼の連鎖

HashTrap

- DS のハッシュの照合の回数



HashTrap

- DS のハッシュの照合の回数
  - 照合が成功する組み合わせを見つける
    - 複数のハッシュ、複数の鍵
    - 鍵 の 更 新 のときに 期 間 を 重 ねて運用できる

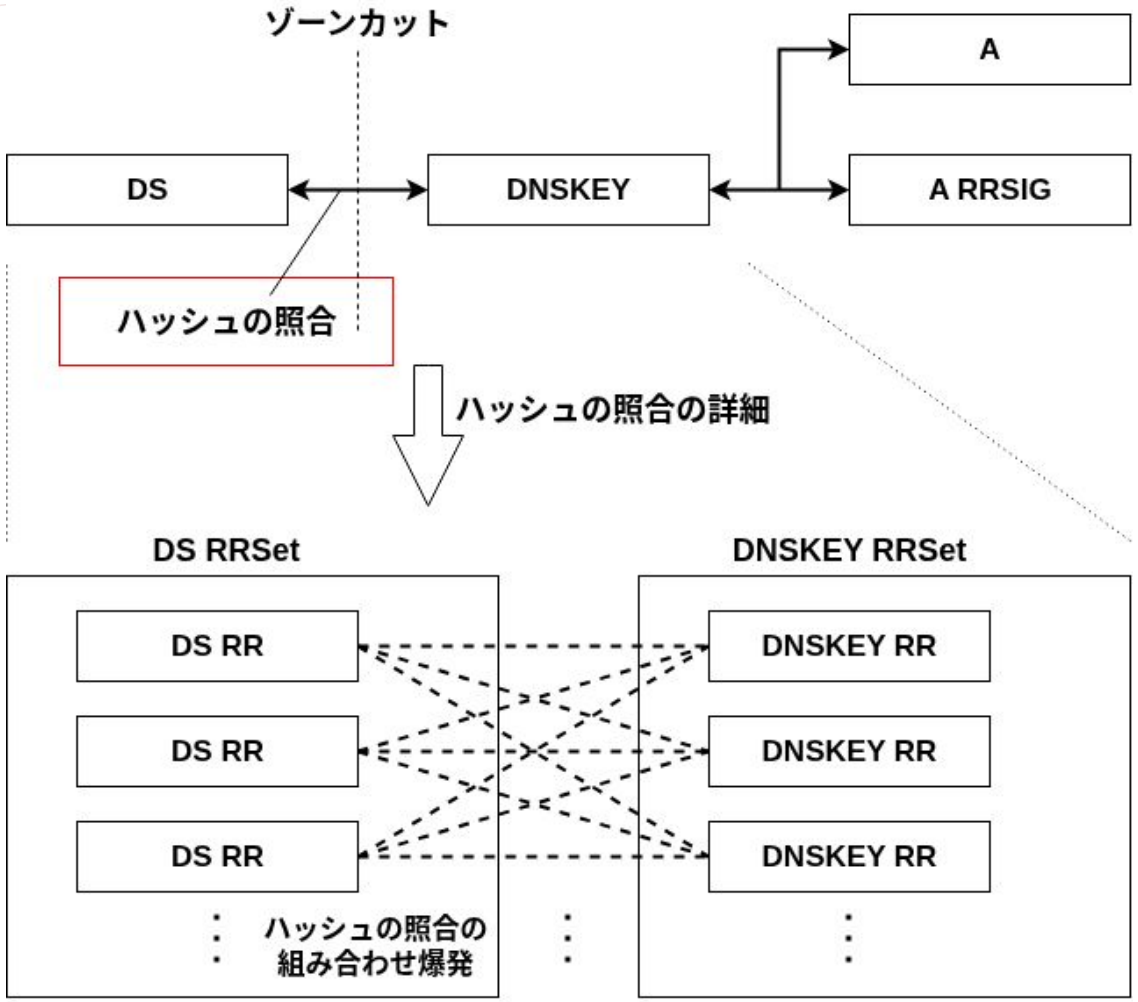
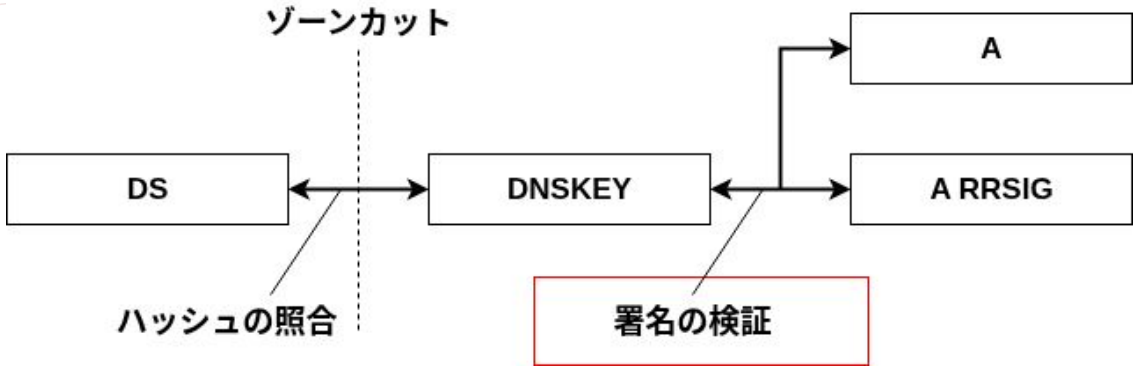


図: HashTrap の概要

KeySigTrap

- RRSet の署名の検証の回数



KeySigTrap

- RRSet の署名の検証の回数
  - 検証が成功する組み合わせを見つける
    - 複数の鍵、複数の署名
    - 鍵 の 更 新 のときに 期 間 を 重 ねて運用できる

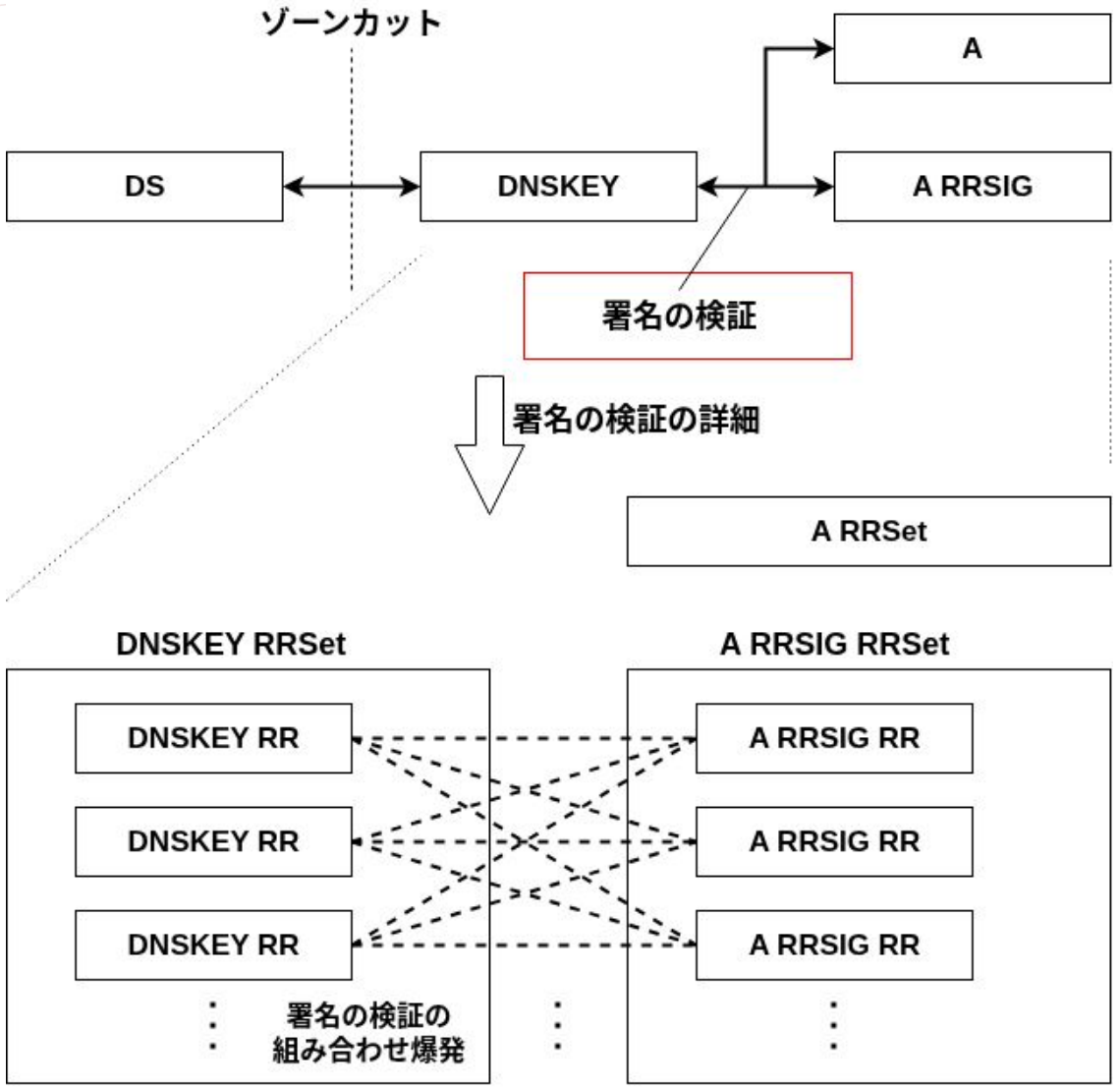


図: KeySigTrap の概要

bowline の HashTrap 対策

ハッシュの照合の回数を減らすためのアルゴリズム

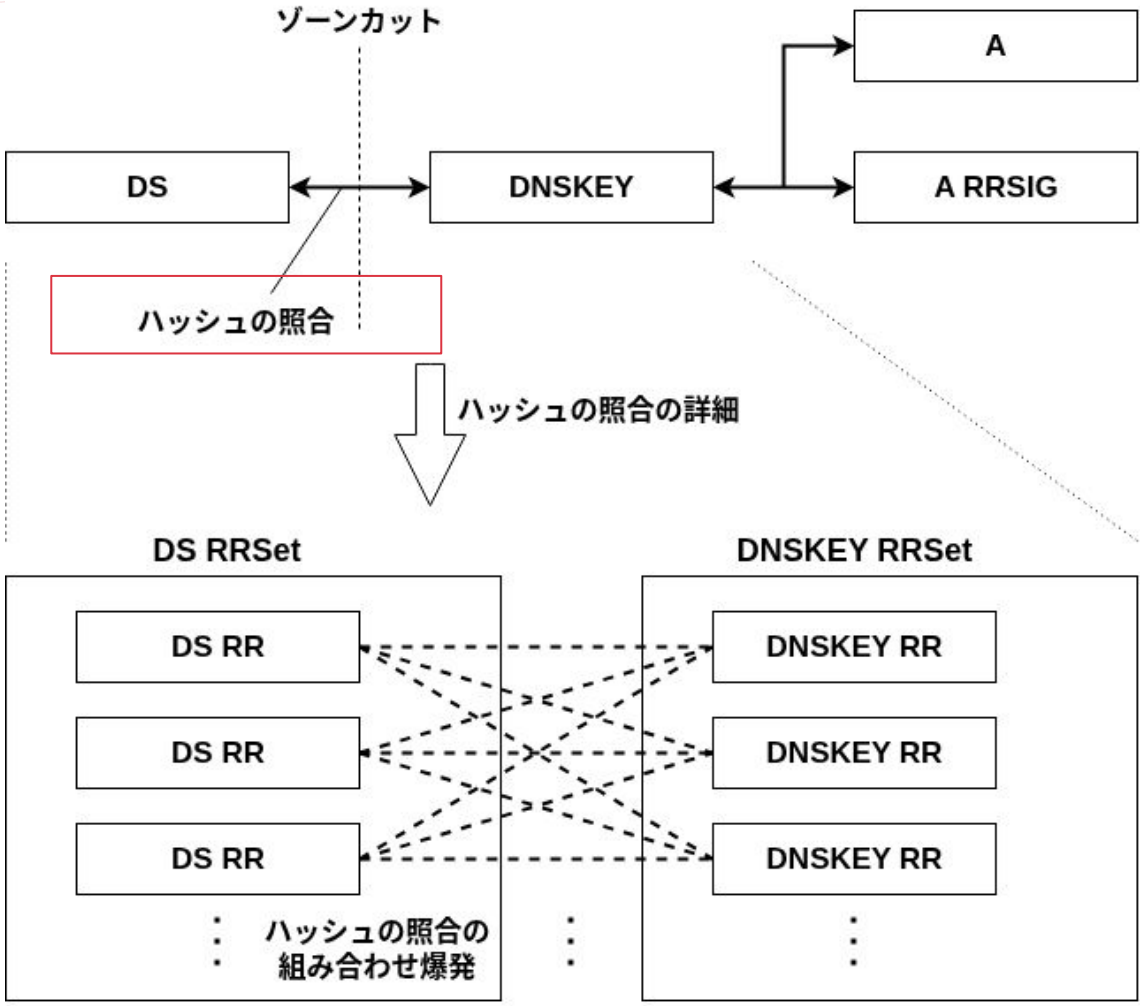
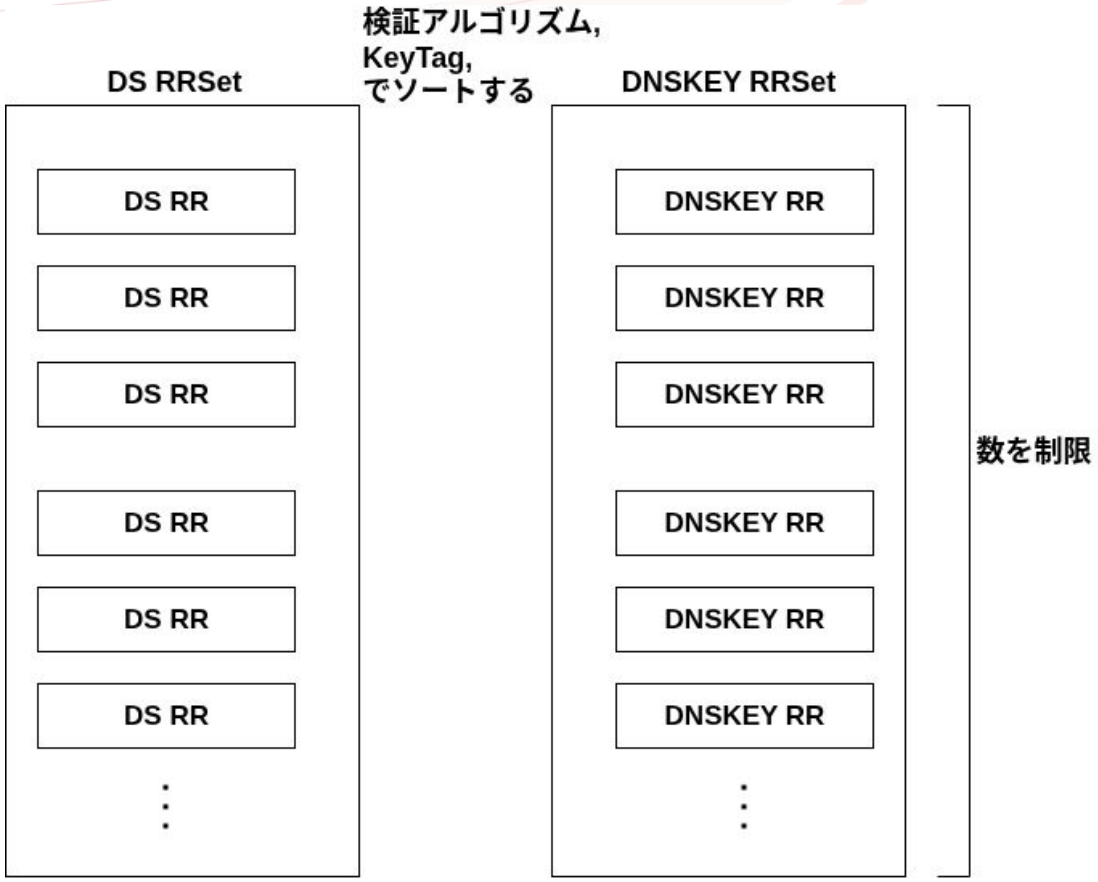


図: HashTrap の概要

bowline の HashTrap 対策

ハッシュの照合の回数を減らすためのアルゴリズム

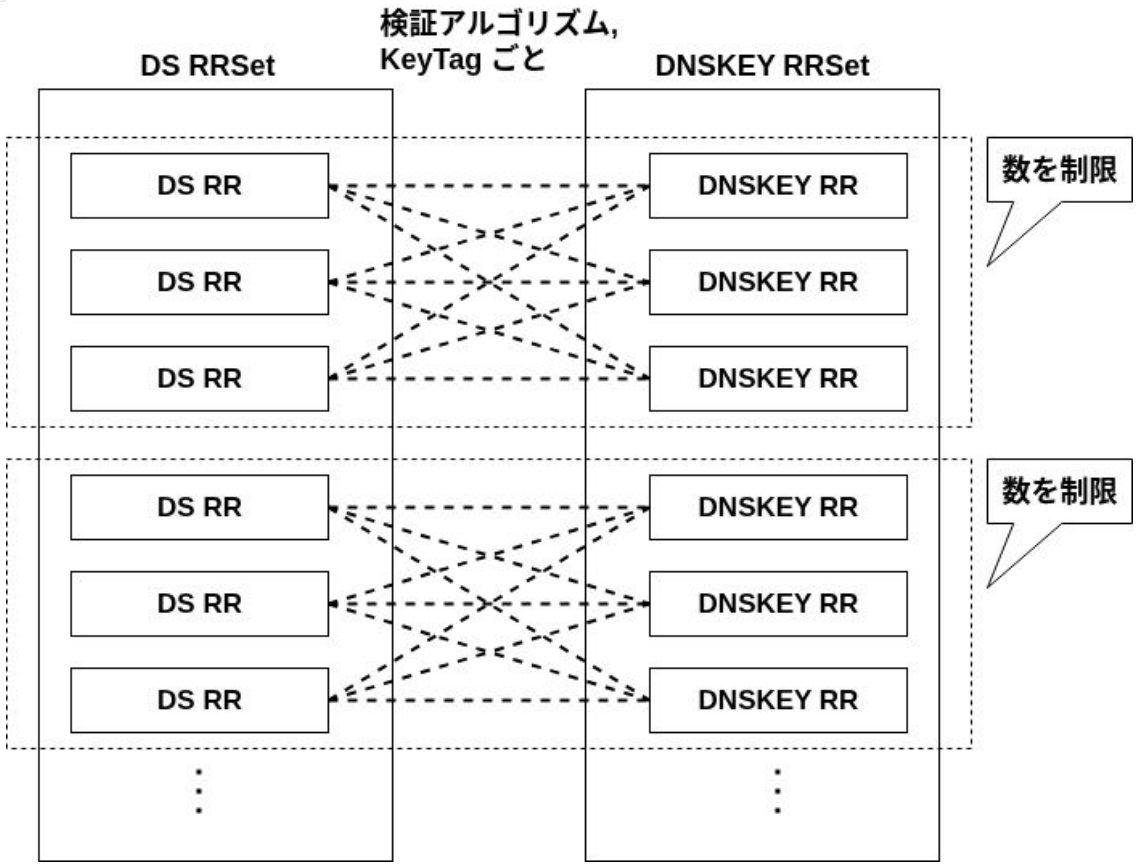
1. DS RR および DNSKEY RR の数を制限
2. DS RR および DNSKEY RR を、
   DNSKEY 検証アルゴリズム (番号)、
   KeyTag ごとにソートする
   - KeyTag (DNSKEY の checksum) が異なるなら DNSKEY が異なる



bowline の HashTrap 対策

ハッシュの照合の回数を減らすためのアルゴリズム

1. DS RR および DNSKEY RR の数を制限
2. DS RR および DNSKEY RR を、**DNSKEY 検証アルゴリズム** (番号)、**KeyTag** ごとにソートする
   - KeyTag (DNSKEY の checksum) が異なるなら DNSKEY が異なる
3. **検証アルゴリズム** 、**KeyTag** ごとにまとめる
   - 検証アルゴリズム、KeyTagが同じ場合のみ、照合が必要
4. **検証アルゴリズム** 、**KeyTag**ごとの数を制限後、ハッシュを照合する



bowline の KeySigTrap 対策

署名の検証の回数を減らすためのアルゴリズム

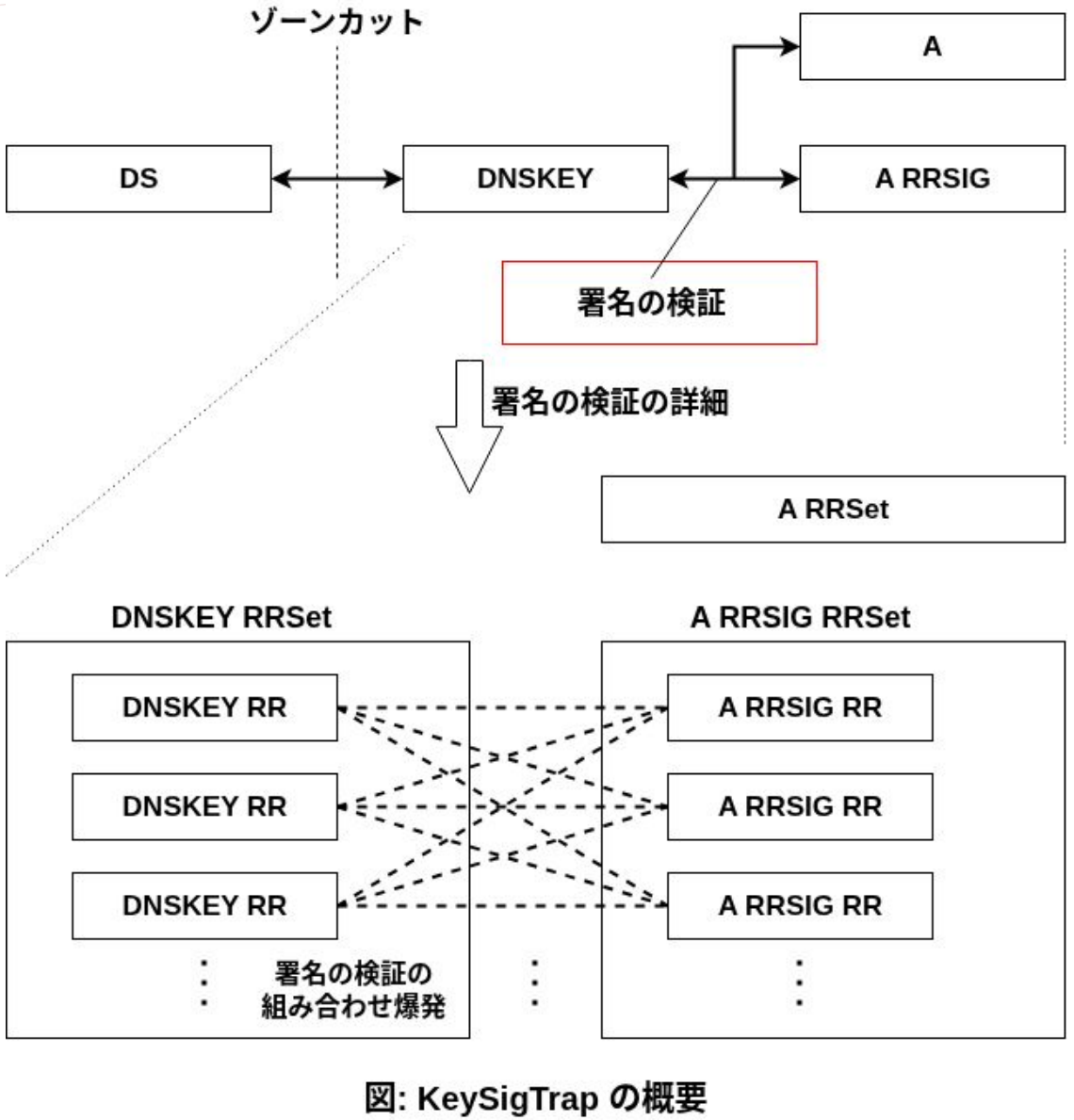
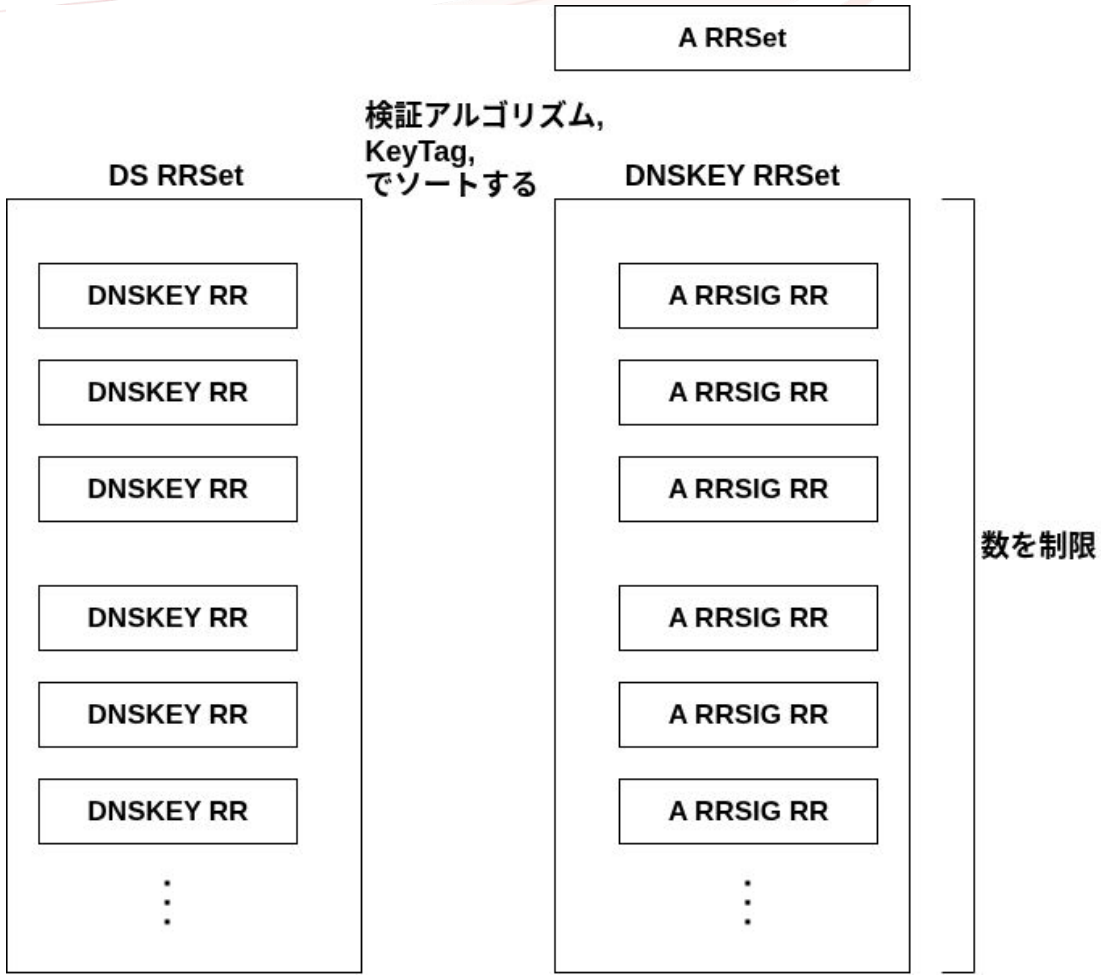


図: KeySigTrap の概要

bowline の KeySigTrap 対策

署名の検証の回数を減らすためのアルゴリズム

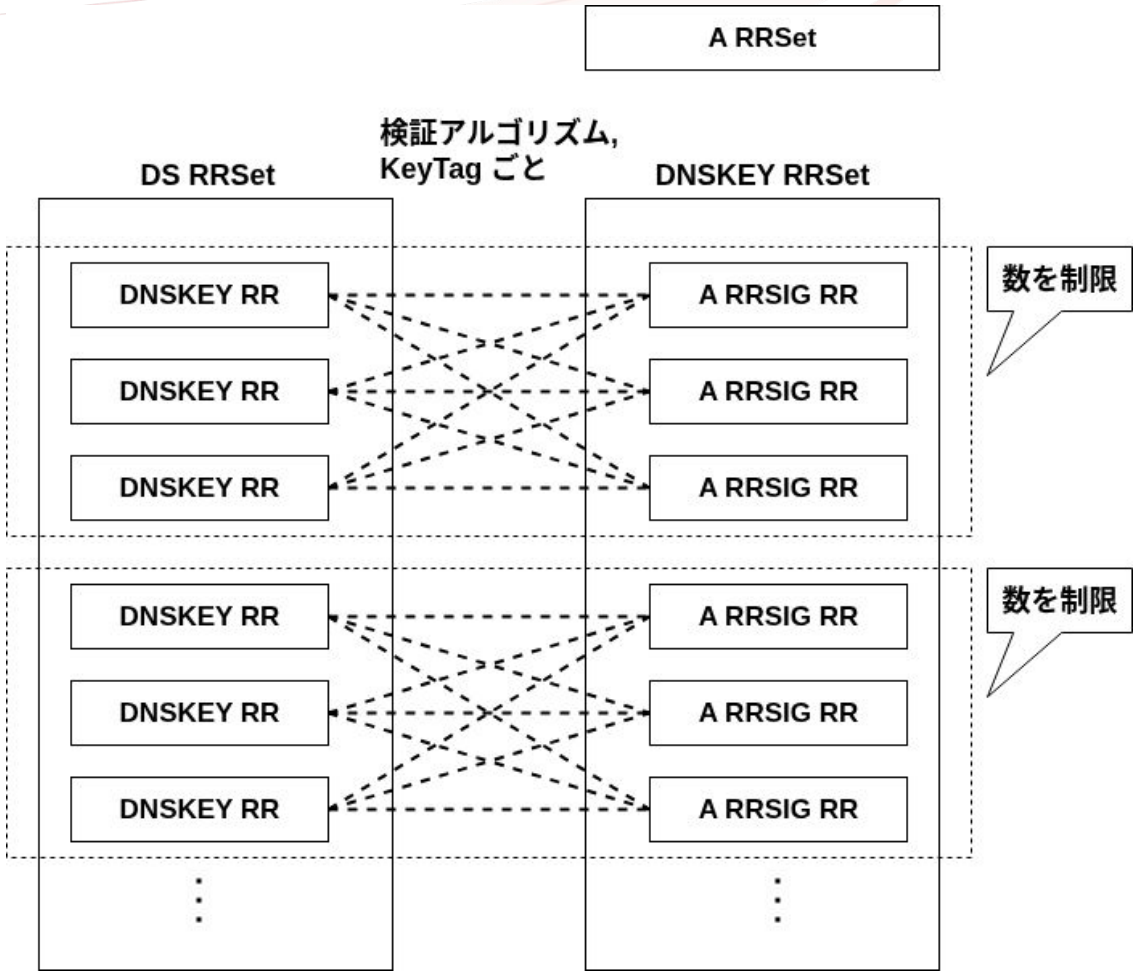
1. DNSKEY RR および RRSIG RR の数の制限
2. DNSKEY RR および RRSIG RR を、**DNSKEY 検証アルゴリズム**、**KeyTag** ごとにソートする
   - KeyTag が異なれば DNSKEY が異なる



bowline の KeySigTrap 対策

署名の検証の回数を減らすためのアルゴリズム

1. DNSKEY RR および RRSIG RR の数の制限
2. DNSKEY RR および RRSIG RR を、**DNSKEY 検証アルゴリズム**、**KeyTag** ごとにソートする
   - KeyTag が異なれば DNSKEY が異なる
3. **検証アルゴリズム**、**KeyTag** ごとにまとめる
   - 検証アルゴリズム、KeyTag が同じ場合のみ、署名検証が必要
4. **検証アルゴリズム**、**KeyTag**ごとの数を制限後、署名を検証する



HashTrap 対策と同様の制限

参考

- The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNS
  - https://www.athene-center.de/fileadmin/content/PDF/Keytrap_2401.pdf
- bowline レポジトリ https://github.com/iijlab/dnsext

bowline を試していただける方を募集中

ありがとうございました