ISS-P-209

名前解決時間短縮を目的としたDNSSECキャッシュに対するWebキャッシュ戦略適用の可能性

福田　修太†　　藤野　貴之††
† 近畿大学大学院システム工学研究科　　†† 近畿大学工学部電子情報工学科

1.　はじめに

近年，DNS キャッシュポイズニング攻撃のため，名前解決の信頼性が問われている．名前解決の信頼性を向上させる拡張機能として DNSSEC[1]が開発され，ドメイン登録情報にデジタル署名を施すことにより情報の信頼性を保証することが可能となった．しかし認証データを付加・検証することによって処理に時間がかかり，応答時間の遅延が発生するという問題がある．本研究の目的は，名前解決時間短縮を目的としたDNSSECキャッシュに対するWebキャッシュ戦略適用の可能性の調査である．

2.　DNSSEC

DNSSEC はデジタル署名技術を用いて，DNS 情報の出自と完全性を保証する技術である．DNSSEC キャッシュサーバは，権威サーバから受け取った情報に付加された署名を，権威サーバの公開鍵で検証し，DNS 情報の出自と正当性を検証する．キャッシュサーバは権威サーバから情報を受け取るたびに，検証処理を行う．

3.　シミュレーション

DNSSEC 環境において，キャッシュサーバでのキャッシュ管理に用いられるアルゴリズムによって，キャッシュヒット率がどのように変化するか，シミュレータにより調査を行った．クライアントがキャッシュサーバに名前解決を要求するドメインの人気が，ポアソン分布，あるいは対数正規分布と仮定した場合について調査した．キャッシュサーバは，クライアントから要求を受け取り，キャッシュに要求されたドメインの IP アドレスがすでにキャッシュされていれば，キャッシュの内容をクライアントに返答する（キャッシュヒット）．キャッシュ内に求められたデータが存在しない場合，キャッシュサーバは名前解決処理を行い，IP アドレスをキャッシュに格納する．その際キャッシュ領域に空きが無ければ，LRU または LFU のアルゴリズムに従い既存のキャッシュを破棄して，新たなキャッシュを格納する．アルゴリズム別にキャッシュ容量を変化させながら計算を行い，測定結果をグラフにまとめた．

4.　測定結果

アルゴリズム別にキャッシュ容量を変化させながら計算を行い，測定結果をグラフにまとめた．ドメインの散らばりがポアソン分布の場合の結果を図１，対数正規分布の場合の結果を図２，分布がシミュレーションの途中で変化した場合を図３に示す．求められるドメインの分布によって，LRU が有利な場合，LFU が有利な場合がある事が確認された．

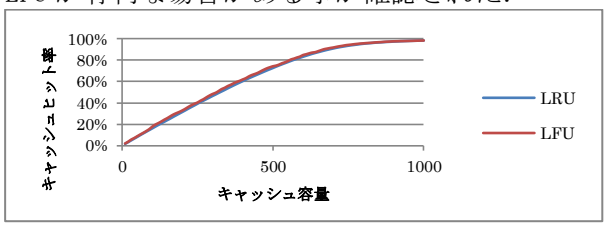

図１　ドメインの分布がポアソン分布の場合

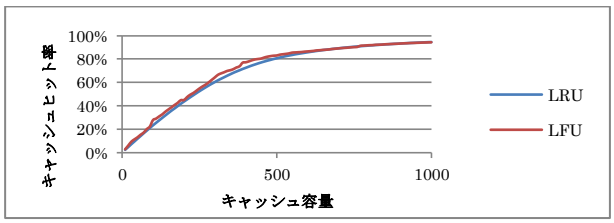

図２　ドメインの分布が対数正規分布の場合

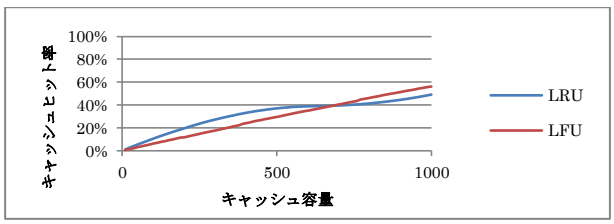

図３　ドメインの分布が途中で変化した場合

5.　まとめ

DNSSEC の導入により名前解決時間は増加するが，キャッシュサーバでのキャッシュヒット率によって，名前解決時間の短縮が見込まれる．

今後の課題として，キャッシュヒット率を向上させるために，LRU・LFU の切り替え戦略の検討や，破棄キャッシュ候補が複数存在する場合の選択方法を検討したキャッシュ管理アルゴリズムの構築などが挙げられる．

参考文献

[1] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose: “DNS Security Introduction and Requirements”, RFC4033, March 2005