DNSSEC

●権威サーバの役目：ZSK（ゾーン署名鍵）の鍵ペアを持つ。ZSK 秘密鍵でキャッシュサーバへの応答レコードに署名する。これを RRSIG (Resource Record digital SIGnature)という。

●権威サーバの上位サーバの役目：KSK（鍵署名鍵）の鍵ペアを持つ。KSK 秘密鍵で ZSK 公開鍵のハッシュ値である DS (Delegation Signer)に署名する。これを署名 DS という。

●キャッシュサーバの役目

①上位サーバから KSK 公開鍵と DS 署名をもらう。

②権威サーバから応答レコードと RRSIG と ZSK 公開鍵をもらう。

③ZKS 公開鍵の検証として、①から KSK 公開鍵で復号した DS（ZSK 公開鍵のハッシュ値）と②から ZSK 公開鍵のハッシュ値を比較して一致すれば、ZSK 公開鍵は本物である。

④応答レコードの検証として、②から ZSK 公開鍵で復号した RRSIG と応答レコードを比較して一致すれば、応答レコードは本物である。これで完了。

DNS サーバ関係

●コンテンツサーバ　＝　権威サーバ　＝　ゾーンサーバ

●【キャッシュサーバ　＝　フルサービスリゾルバ】　⇔　スタブリゾルバ

※オープンリゾルバは不特定多数から再起問い合わせを受けるサーバ

●スタブリゾルバ　→　DNS フォワーダ　→　フルサービスリゾルバ（フォワーダ）

CAA レコード（Certification Authority Authorization Record）

●DNS サーバのレコードの 1 つ。当該ドメインの証明書の発行を許可する CA を登録し、不正な証明書の発行を防ぐ。

EDNS 0（Extension DNS ver.0）

●DNS の名前解決は、UDP53 を使用しているが、512 オクテットを超えると、DNS サーバは超過分を切り捨てて、クライアントに返信するとともに、その旨をクライアントに伝える。

●クライアントは **TCP フォールバック（TCP53 による再クエリ）**を行うが、DNS サーバにとって、TCP は負荷が大きい。そこで、UDP サイズを 2 の 16 乗オクテットまで拡張した EDNS 0 を用いる。

●TCP53 は、ゾーン転送にも使用される。

nslookup = dig

●DNS サーバを指定して、DNS 要求を直接送信して、その回答を得ることができる。

●プライマリ DNS サーバに対するゾーン転送要求において、プライマリが要求元を制限していなければ、nslookup コマンドによって、攻撃対象の NW 構成を知ることができる。