キャッシュDNSサーバチェックリスト(2012年1月6日版)

このチェックリストは、キャッシュDNSサーバがDNSSECに関する問い合わせを正しく処理し、クライアントに適切な応答を返すことができることを確認する。利用者がDNSSEC Readyロゴマークを使用するためには、このチェックリストの中で該当する各項目に適合することが求められる。他のカテゴリーのチェックリストを参照している部分については、そのチェック結果を添付すること。

機能の確認

ネットワーク機器(ルータ、F/W・IPS・IDSなどのセキュリティ機器、負荷分散装置など)を含むシステムとしての機能の確認

- [レ] 製品チェックリストの汎用ネットワーク機器製品に対応していること

キャッシュDNSサーバの機能の確認

- [レ] EDNS0に対応していること
- [レ] TCP/UDPともSRCもしくはDSTのPort53宛てのパケットを送受信できること
- [レ] 512バイトより大きいペイロードを持つパケットを送受信できること
- [レ] IPフラグメントパケットを送受信できること
- [レ] フラグメントされる大きさのUDPパケットを正しく扱えること
- [レ] 権威DNSサーバにDO(DNSSEC OK、DNSSECの情報を要求する)ビットをつけて問い合わせ可能なこと
- [レ] クライアントからのDO、CD(Checking Disabled、DNSSEC検証を行わない)の要求を正しく解釈して取り扱えること
- [レ] DOの要求があった場合、署名検証成功時はAD(Authentic Data、DNSSEC検証の成功)ビットをつけて応答すること
- [レ] 署名検証失敗時はSERVFAILを応答すること

運用手順の確認

ルートゾーンのトラストアンカー初期導入手順の確認

- [レ] ルートゾーンのトラストアンカー導入にあたって信頼できる手順に基づいていること(参照:DNSSECジャパン「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」)

トラストアンカーの更新手順の確認

- [レ] 数年に1回の頻度で行われる予定のルートゾーンのトラストアンカー更新に対する手順が用意されていること
- [レ] 危殆化の問題から緊急でルートゾーンのトラストアンカー更新が行われる場合に備えて手順が用意されていること

動作の確認

TCPを破棄しないことの確認

- [レ] *dig +tcp dnssec.jp @キャッシュDNSサーバ* で応答が返ること

EDNS0に対応していることの確認

- [レ] *dig +bufsize=4096 dnssec.jp @キャッシュDNSサーバ* で応答が返ること

DNSSECの検証が成功していることの確認

- [レ] *dig +dnssec dnssec.jp @キャッシュDNSサーバ* でADビットがついた応答が返ること

DNSSECの検証失敗が応答されることの確認

- [レ] *dig +dnssec fail.dnssec.jp @キャッシュDNSサーバ* でSERVFAILが返ること

DOのない問い合わせにDNSSECの応答を返さないことの確認

- [レ] *dig +nodnssec dnssec.jp @キャッシュDNSサーバ* でDNSSEC対応のリソースレコードが返らないこと

DOのない問い合わせでもDNSSECの検証を行うことの確認

- [レ] *dig +nodnssec fail.dnssec.jp @キャッシュDNSサーバ* でSERVFAILが返ること

CDの付いた問い合わせでDNSSECの検証を行わないことの確認

- [レ] *dig +cd fail.dnssec.jp @キャッシュDNSサーバ* で応答が返ること

凡例

- [レ] 該当する
- [ ] 該当しない

製品チェックリスト(2012年1月6日版)

このチェックリストは、製品がDNSSECに関する問い合わせを正しく処理し、必要に応じて適切な応答を返すことができることを確認する。利用者がDNSSEC Readyロゴマークを使用するためには、このチェックリストの中で該当する各項目に適合することが求められる。他のカテゴリーのチェックリストを参照している部分については、そのチェック結果を添付すること。

汎用ネットワーク機器製品*(注)*
(ルータ、F/W・IPS・IDSなどのセキュリティ機器、負荷分散装置など)

レ	EDNS0のパケットを破棄しないこと
レ	TCP/UDPともSRCもしくはDSTのPort53宛てのパケットを破棄しないこと
レ	512バイトより大きいペイロードを持つパケットを破棄しないこと
レ	IPフラグメントパケットを破棄しないこと
レ	UDPフラグメントパケットを破棄しないこと
レ	負荷分散装置の場合はDNSSEC.JPの「DNSサーバDNSSEC導入Load Balancer機能チェックリスト」に対応できること

権威DNSサーバ製品

	DNSSEC Readyロゴの権威DNSサーバチェックリスト(「運用方式の確認」の「鍵管理方式の確認」を除く)に適合していること
	DNSSEC.JPの「DNSサーバDNSSEC導入鍵管理チェックリスト」に対応できること

キャッシュDNSサーバ製品

	DNSSEC Readyロゴのキャッシュ DNSサーバチェックリスト(「運用手順の確認」を除く)の対応が可能なこと
	トラストアンカーの設定方法および更新方法が明確になっていること

鍵管理製品

	権威DNSサーバとの連携が可能なこと
	DNSSEC.JPの「DNSサーバDNSSEC導入鍵管理チェックリスト」に対応できること

凡例

- レ 該当する
- □ 該当しない

注 以下のサイトやツール等を使用することで確認可能

- OARCのリプライサイズテスタ
  <https://www.dns-oarc.net/oarc/services/replysizetest>
- NIC.CZのDNSSEC HARDWARE TESTER
  <http://www.dnssec-tester.cz/>