

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	
<input checked="" type="checkbox"/>	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	
<input checked="" type="checkbox"/>	EDNS0に対応していること
<input checked="" type="checkbox"/>	TCP/UDPともSRCもしくはDSTのPort53宛ての packets を送受信できること
<input checked="" type="checkbox"/>	512バイトより大きいペイロードを持つ packets を送受信できること
<input checked="" type="checkbox"/>	IPフラグメント packets を送受信できること
<input checked="" type="checkbox"/>	フラグメントされる大きさのUDP packets を正しく扱えること
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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	
<input checked="" type="checkbox"/>	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	
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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	
<input checked="" type="checkbox"/>	<code>dig +tcp dnssec.jp @キャッシュDNSサーバ</code> で応答が返ること
EDNS0に対応していることの確認	
<input checked="" type="checkbox"/>	<code>dig +bufsize=4096 dnssec.jp @キャッシュDNSサーバ</code> で応答が返ること
DNSSECの検証が成功していることの確認	
<input checked="" type="checkbox"/>	<code>dig +dnssec dnssec.jp @キャッシュDNSサーバ</code> 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	
<input checked="" type="checkbox"/>	<code>dig +dnssec fail.dnssec.jp @キャッシュDNSサーバ</code> 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	
<input checked="" type="checkbox"/>	<code>dig +nodnssec dnssec.jp @キャッシュDNSサーバ</code> 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	
<input checked="" type="checkbox"/>	<code>dig +nodnssec fail.dnssec.jp @キャッシュDNSサーバ</code> 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	
<input checked="" type="checkbox"/>	<code>dig +cd fail.dnssec.jp @キャッシュDNSサーバ</code> で応答が返ること

凡例

- 該当する
- 該当しない

権威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、権威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	
<input checked="" type="checkbox"/>	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
権威DNSサーバの機能の確認	
<input checked="" type="checkbox"/>	EDNS0に対応していること
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	権威DNSサーバの機能を提供するサービスプロバイダの場合、対応しているDNSSEC機能の一覧(例:NSEC3、RSASHA512、鍵長)が公開されていること
<input checked="" type="checkbox"/>	セカンダリサーバを含めた全ての権威サーバが、必要としているDNSSEC機能をサポートしているソフトウェアを使用していること
運用方式の確認	
鍵管理方式の確認	
<input checked="" type="checkbox"/>	DNSSEC.JPの「DNSサーバDNSSEC導入鍵管理チェックリスト」に基づいて鍵管理の方式を確認していること
<input checked="" type="checkbox"/>	複数ゾーンを持つ場合、KSKをゾーン毎に個別とするか共通とするかの方針を決定していること
署名更新方式の確認	
<input checked="" type="checkbox"/>	ゾーンを更新したとき署名を更新する機構を用意していること
<input checked="" type="checkbox"/>	署名の有効期限が切れる前に再署名する機構を用意していること
動作の確認	
TCPを破棄しないことの確認	
<input checked="" type="checkbox"/>	<code>dig +norec +tcp ターゲットドメイン名 @権威DNSサーバ</code> で応答が返ること
DOに対応していることの確認	
<input checked="" type="checkbox"/>	<code>dig +norec +dnssec ターゲットドメイン名 @権威DNSサーバ</code> でDNSSEC対応のリソースレコードが返ること
EDNS0に対応していることの確認	
<input checked="" type="checkbox"/>	<code>dig +norec +bufsize=4096 +dnssec ターゲットドメイン名 @権威DNSサーバ</code> で応答が返ること
DOのない問い合わせにDNSSECの応答を返さないことの確認	
<input checked="" type="checkbox"/>	<code>dig +norec +nodnssec ターゲットドメイン名 @権威DNSサーバ</code> でDNSSEC対応のリソースレコードが返らないこと

凡例

- 該当する
- 該当しない

ドメイン名登録チェックリスト(2012年1月6日版)

このチェックリストは、ドメイン名登録者のDNSSEC情報をドメイン名登録に関係する各組織が正しく処理し、「信頼の連鎖」を構築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。

ドメイン名登録者	
<input checked="" type="checkbox"/>	ルートゾーンからの「信頼の連鎖」がつながっていること
<input checked="" type="checkbox"/>	署名されているドメイン名がロゴマークに併記されること
DNS運用者(ゾーン管理者)	
<input checked="" type="checkbox"/>	権威DNSサーバのチェックリストに適合していること
<input type="checkbox"/>	ドメイン名登録取り次ぎ事業者※を兼ねない場合は、ドメイン名登録者にDSを安全に渡す方法を持っていること
<input checked="" type="checkbox"/>	サブドメインを委任している場合は、サブドメイン名登録者のDSを安全に受け取り、ゾーンに反映する方法を持っていること
<input checked="" type="checkbox"/>	DNSプロバイダ移転に対応していること
<input checked="" type="checkbox"/>	(DNSSEC.JPの「レジストラ移転ガイドライン」の方法に準ずる業務フローを用意していること
<input checked="" type="checkbox"/>	DNSSEC対応のサービス内容を顧客に説明していること
ドメイン名登録取り次ぎ事業者※	
<input checked="" type="checkbox"/>	DNS運用者を兼ねる場合は、上記の「DNS運用者(ゾーン管理者)」に適合していること
<input checked="" type="checkbox"/>	ドメイン名登録者の指示に従ってDSをレジストリに登録・削除できること
<input checked="" type="checkbox"/>	登録を依頼されたDSをレジストリに登録する前に、そのゾーンに該当するDNSKEYがあるか確認する機構を用意していること
<input checked="" type="checkbox"/>	レジストラ移転に対応していること
<input checked="" type="checkbox"/>	(DNSSEC.JPの「レジストラ移転ガイドライン」の方法に準ずる業務フローを用意していること
<input checked="" type="checkbox"/>	DNSSEC対応のサービス内容を顧客に説明していること
レジストリ(TLD)	
<input type="checkbox"/>	ルートゾーンからの「信頼の連鎖」がつながっていること
<input type="checkbox"/>	権威DNSサーバのチェックリストに適合していること
<input type="checkbox"/>	ドメイン名登録者のDSをレジストラから安全に受け取り、ゾーンに反映する方法を持っていること
<input type="checkbox"/>	登録を依頼されたDSをゾーンに反映する前に、登録者のゾーンに該当するDNSKEYがあるか確認する機構を用意していること
<input type="checkbox"/>	DNSSEC対応のサービス内容を顧客に説明していること
サブドメイン提供者	
<input type="checkbox"/>	DNS運用者(ゾーン管理者)のチェックリストに適合していること

※ドメイン名登録取り次ぎ事業者にはリセラ、レジストラ、指定事業者が含まれる。

凡例

- 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)	
<input checked="" type="checkbox"/>	EDNS0のパケットを破棄しないこと
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	IPフラグメントパケットを破棄しないこと
<input checked="" type="checkbox"/>	UDPフラグメントパケットを破棄しないこと
<input checked="" type="checkbox"/>	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	
<input type="checkbox"/>	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
<input type="checkbox"/>	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	
<input type="checkbox"/>	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
<input type="checkbox"/>	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	
<input type="checkbox"/>	権威DNSサーバとの連携が可能なこと
<input type="checkbox"/>	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

- 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/>>

Copyright © 2012 DNSSEC.JP all rights reserved