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

レ	ルートゾーンからの「信頼の連鎖」がつながっていること
レ	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)

	権威DNSサーバ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※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
	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
	DNSプロバイダ移転に対応していること (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)
	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※

	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
	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
	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
	レジストラ移転に対応していること (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)
	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)

	ルートゾーンからの「信頼の連鎖」がつながっていること
	権威DNSサーバのチェックリストに適合していること
	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
	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
	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

	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

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)*

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

レ	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
レ	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/>

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

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

権威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	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
	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
レ	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

レ	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
レ	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

レ	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
レ	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

レ	*dig +norec +tcp ターゲットドメイン名 @権威DNSサーバ* で応答が返ること

DOに対応していることの確認

レ	*dig +norec +dnssec ターゲットドメイン名 @権威DNSサーバ* 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

レ	*dig +norec +bufsize=4096 +dnssec ターゲットドメイン名 @権威DNSサーバ* 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

レ	*dig +norec +nodnssec ターゲットドメイン名 @権威DNSサーバ* でDNSSEC対応のリソースレコードが返らないこと

凡例

レ	該当する
	該当しない