解　説

DNSSEC 解説

―DNS におけるセキュリティ拡張の導入―

三田村健史　佐藤新太

((株)日本レジストリサービス(JPRS))

DNS と DNSSEC

■ DNS の役割

インターネットは，いまや社会基盤を支える重要なものになっている．特に DNS（Domain Name System）は，Web アクセスや電子メールの利用などインターネットにおけるドメイン名利用サービスの急速な拡大の中，インターネットにとって欠かせない重要な基盤技術の 1 つとなっている．

しかし，DNS に対するより効率的な攻撃手法の発見がここ数年で問題となっており，DNS の管理者にとって，問題の所在と影響について知っておくことが必要となっている．

DNS とは

DNS の基本的な役割は，「IP アドレスとドメイン名の対応付け」である．DNS には，この役割を実現するために基本となる構成要素が 2 つある．1 つは対応付けの問合せを行う「リゾルバ」であり，もう 1 つは，その問合せに返信する「DNS サーバ」であり，この一連の処理を「名前解決」と呼ぶ．

図 -1 を用いて名前解決の仕組みを説明する．図 -1 の例では，ブラウザから http://www.example.jp/ と入力され名前解決を要求されたリゾルバ（スタブリゾルバ）は，PC に登録されていたキャッシュ DNS サーバと呼ばれる DNS サーバに問合せを行う（図中の①）．キャッシュ DNS サーバでは，問合せに対する答えを知らない場合，自らのリゾルバ（フルサービスリゾルバ）を呼び出し，権威 DNS サーバと呼ばれる DNS サーバに問合せを行う（図中の②～⑦）．まずキャッシュ DNS サーバは，ルート・サーバと呼ばれる DNS サーバに www.example.jp の IP アドレスを問い合わせ(②)，.jp ドメインの DNS サーバのありか（IP アドレス）を得る（③）．次に，.jp

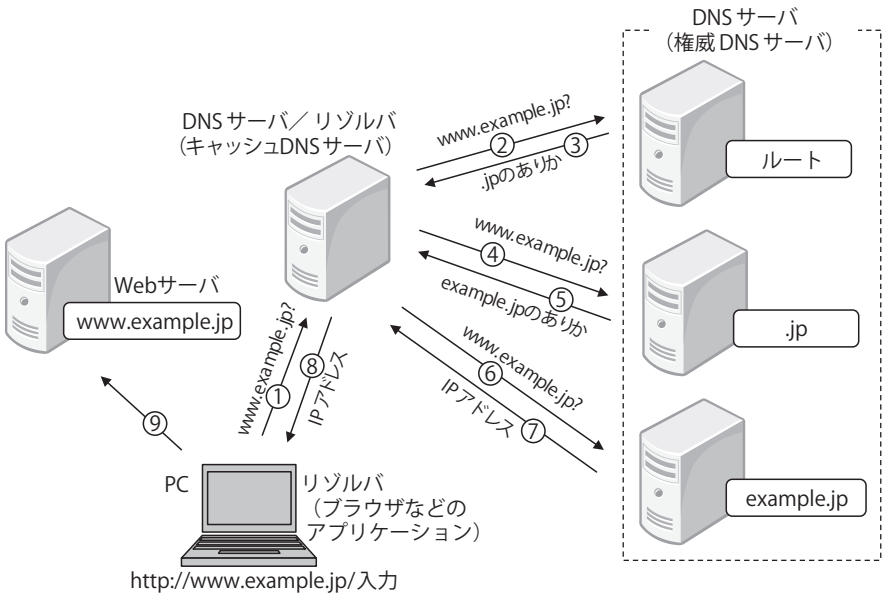

図 -1　名前解決の仕組み

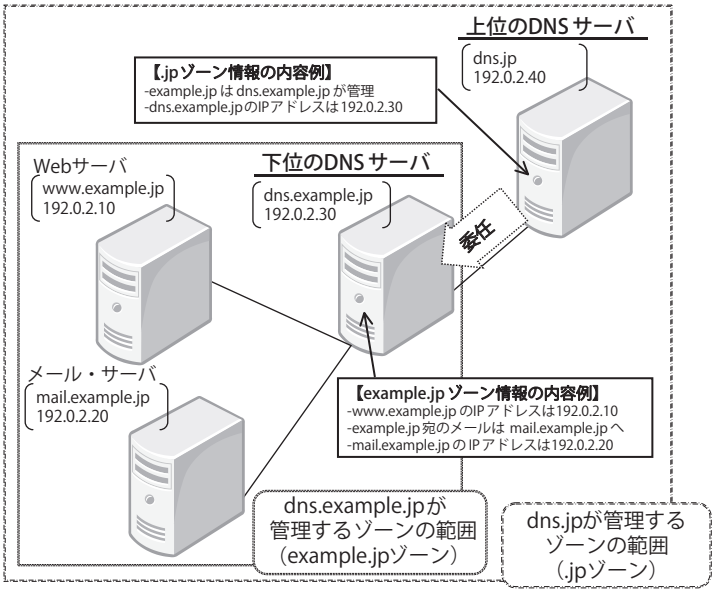

図 -2　ゾーンと委任

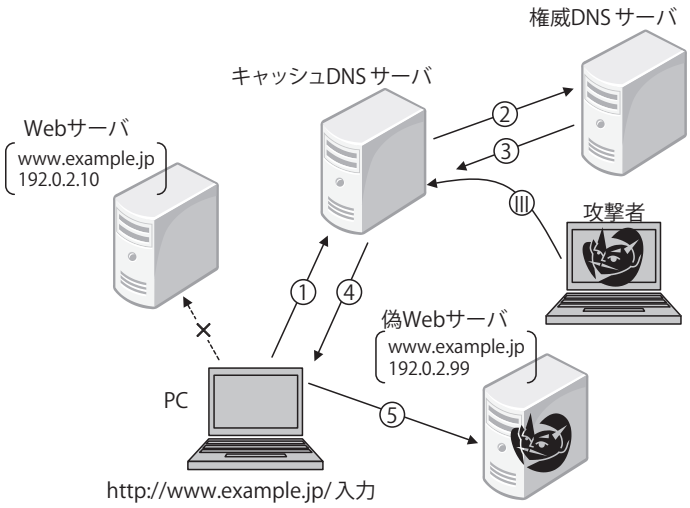

図 -3　DNS キャッシュポイズニングの仕組み

ドメインの DNS サーバに www.example.jp の IP アドレスを問い合わせ（④），example.jp の DNS サーバのありかを得る（⑤）．example.jp の DNS サーバは，www.example.jp の問合せに対し（⑥），IP アドレスをキャッシュ DNS サーバに返信する（⑦）．キャッシュ DNS サーバは，この答えを PC に送り返し，名前解決は終了する（図中の⑧）．PC は，入手した www.example.jp の IP アドレスを用いて Web サーバにアクセスする（図中の⑨）．

ゾーンと委任

図 -1 に示したように，DNS サーバは複数存在する．各々の権威 DNS サーバが管理するドメイン名空間の範囲を「ゾーン」と呼び，DNS サーバ間でサブドメイン名の管理を任せることを「委任」と呼ぶ．**図 -2** を用い，その仕組みを説明する．図 -2 では，.jp というドメイン名空間（以下，.jp ゾーン），その配下に example.jp というドメイン名空間（以下，example.jp ゾーン），さらにそのサブドメイン名として www.example.jp という Web サーバ，mail.example.jp というメール・サーバがある構成例を示している．この例では，DNS サーバである dns.jp（IP アドレス : 192.0.2.40）が .jp ゾーンを管理し，その下位の DNS サーバである dns.example.jp（IP アドレス : 192.0.2.30）に example.jp ゾーンの管理を「委任」している．

■ DNSSEC の役割

DNSSEC 導入の背景

DNSSEC（DNS SECurity extension）とは，DNS にセキュリティ強化を行う 1 機能である．これが注目されるようになったのは，「DNS キャッシュポイズニング」と呼ばれる攻撃手法の成功率が飛躍的に上がったことが理由の 1 つにある．**図 -3** を用いて「DNS キャッシュポイズニング」の仕組みを説明する．www.example.jp の Web サーバにアクセスする場合の一般的な名前解決の流れは，①→②→③→④である．この名前解決の流れにおいて攻撃者は，キャッシュ DNS サーバが権威 DNS サーバからの応答である③を受け取る前に，権威 DNS サーバの IP アド

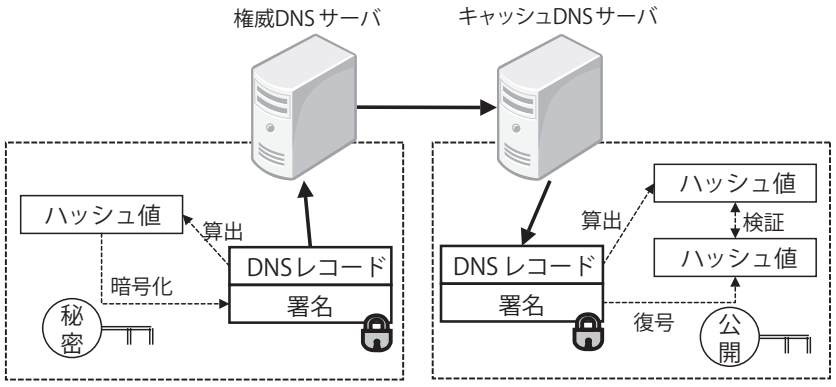

図 -4　DNSSEC における検証の仕組み

- DNS 通信の傍受(リゾルバと DNS サーバ間の通信内容を，第三者が盗み見ること)の防止
- ホモグラフィック攻撃(紛らわしい文字を用いて，本物のサイトのように見せかける攻撃)の防止
- タイポスクワッティング攻撃(URL を入力する際の打ち間違いを悪用し，偽サイトに誘導する攻撃)の防止

レスを詐称して，www.example.jp の IP アドレスが 192.0.2.99 という偽の応答Ⓘをキャッシュ DNS サーバに送りつけ，キャッシュ DNS サーバにキャッシュさせる．PC はこの偽の応答を返され，偽の Web サーバに誘導される (図中の⑤) のが DNS キャッシュポイズニングである．DNS キャッシュポイズニングに至る DNS プロトコルの脆弱性は以前から知られていたが，現実的には簡単には成功しないと考えられていた．しかし，2008 年にカミンスキーメソッドという DNS 応答を詐称する手法が発表されたことで，その危険性が飛躍的に増したことが DNSSEC 導入の背景にある．

DNSSEC とは

DNS キャッシュポイズニングが悪用しているのは，従来の DNS プロトコルの脆弱性である．DNSSEC は，DNS プロトコルのセキュリティ強化のため，次の 2 つの機能を有している．

- データの出自認証
  正しいゾーン管理者により作られたゾーン情報であることを確認する機能
- データの完全性
  ゾーン情報が，途中経路で改ざんや喪失されていないことを確認する機能

DNSSEC は，従来の DNS の仕組みを拡張する実装を行っているが，上位互換を保っている．

なお，DNSSEC では以下のようなことを目的とはしておらず，実現していない．

DNSSEC の仕組み

DNSSEC では，データの正しさを確保するため，公開鍵暗号による電子署名の仕組みを名前解決の処理に応用している．公開鍵暗号は，データの暗号化と復号に，ペアとなる鍵を用いる暗号化方式である．本方式は，鍵の作成者が秘密鍵を保持し，公開鍵を外部に公開しておくことで，安全に受信者にデータを送ることができる仕組みである．**図 -4** を用いて DNSSEC における署名検証の仕組みを説明する．権威 DNS サーバは，自らが管理するゾーン情報 (DNS レコード) からハッシュ値を算出し，秘密鍵を用いて暗号化したデータを署名として付加する．キャッシュ DNS サーバなどの受信側では，受信した DNS レコードから算出したハッシュ値と，付加された署名データを復号して求めたハッシュ値とを比較することで検証を行う．

DNSSEC では，署名に用いた鍵が正当なものであることを，DNS の階層構造に対応した形で証明している．この概念を「信頼の連鎖(Chain of Trust)」と呼んでいる．また DNSSEC で用いる鍵には 2 種類あり，1 つはゾーン署名用の鍵（ZSK : Zone Signing Key）であり，もう 1 つは信頼の連鎖を構築するための鍵(KSK : Key Signing Key)である．

まず上位ゾーンでは，下位ゾーンの KSK 公開鍵のハッシュ値から作成した DS（Delegation Signer）レコードを登録する．検証の際には，上位ゾーンの DS レコードと下位のゾーンの KSK（DNSKEY

プロダクト名			BIND	NSD	unbound
開発元			ISC	NLnet Labs	NLnet Labs
機能	権威サーバ機能		○	○	N/A
	キャッシュサーバ機能		○	N/A	○
	署名	鍵管理・全署名	○	N/A	N/A
		全自動署名／差分署名	○	N/A	N/A
		RFC 5011（署名側）	○	N/A	N/A
		RFC 5011（検証側）	○	N/A	N/A
	署名情報の提供	ツール	○（dig）	N/A	○（drill）
	署名検証	検証機能	○	N/A	○
		permissive モード	N/A	N/A	○

（2011 年 5 月現在）

表 -1　DNS ソフトウェア比較☆1

gTLD	時期	ccTLD	時期
.org	2010 年 6 月	.se	2007 年 2 月
.biz	2010 年 6 月	.jp	2011 年 1 月
.edu	2010 年 8 月	.de	2011 年 5 月
.info	2010 年 9 月	.uk	2010 年 3 月
.asia	2010 年 11 月	.eu	2010 年 6 月
.net	2010 年 12 月	.to	未対応
.com	2011 年 3 月	.tv	未対応

（2011 年 5 月現在）

表 -2　主な TLD の DNSSEC 導入状況

: DNS Public Key レコード）を検証することで，信頼の連鎖を実現している．信頼の連鎖を実現する起点を「トラストアンカー」と呼んでいる．通常の DNSSEC 運用ではトラストアンカーとして，ルート・サーバの KSK 公開鍵，または DS レコードを事前にキャッシュ DNS サーバに設定しておく．

DNSSEC の実現では，権威 DNS サーバやキャッシュ DNS サーバでの DNSSEC 対応はもちろん，信頼の連鎖を実現するためには，上位から下位まですべての権威 DNS サーバが DNSSEC に対応する必要がある．また，公開鍵の登録を行うため，ドメイン名のレジストリやレジストラなどの各事業者でも DNSSEC の対応が必要となる．

また DNSSEC では，セキュリティ強度を維持するため，権威 DNS サーバでは，ZSK/KSK の生成，ゾーンの再署名，上位への DS レコードの登録・更新などの作業，キャッシュ DNS サーバでは，トラストアンカーの更新などの定期的な作業が必要になる．

☆1 【表 -1 の用語説明】
鍵管理：スマート署名（Smart Signing）とも呼ばれる ZSK/KSK の運用を補助する仕組み．
全自動署名機能：ソフトウェアでゾーン署名，鍵更新を行う仕組み．
RFC 5011：トラストアンカーの自動更新を行うプロトコルで，キャッシュ DNS サーバの運用を軽減することができる仕組み．
permissive モード：検証失敗時にも名前解決失敗（SERVFAIL）にならない仕組み．

DNSSEC 実装の現状

■ソフトウェアでの実装

表 -1 に代表的な DNS ソフトウェアの DNSSEC 機能の実装状況を示す．いずれのソフトウェアも最新版においては基本的な機能について対応済みである．一部，運用サポート機能については差異がある．なお，単独ツールとして，OpenDNSSEC，LDNS などがあり，署名に必要ないくつかのプロセスの自動化などを行う．これらは BIND や NSD などと組み合わせて利用することが可能であり，鍵管理，全自動署名などの機能を有している．

■ルート /TLD での実装

ルート・サーバおよび，TLD（Top Level Domain）での DNSSEC 対応状況について説明する．まず，ルート・サーバであるが，2010 年 7 月に対応済みである．次に，TLD の DNSSEC 対応状況であるが，本稿執筆時点（2011 年 5 月）の主な TLD の導入状況について**表 -2** に示す．2010 年から 2011 年にかけて導入が本格化しており，全ドメイン数における署名可能ドメイン数の割合は，gTLD（Generic TLD）で 98% 強，ccTLD（Country Code TLD）で 40% 強である（2011 年 5 月）．

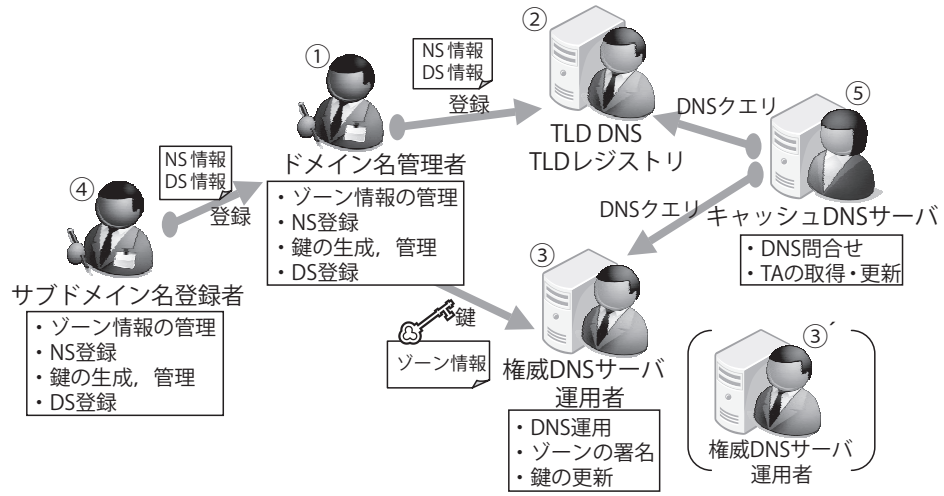

図 -5　DNSSEC 運用の関係者と実施する項目

ドメイン名管理者と運用者への影響

DNSSEC の導入はドメイン名の管理者および DNS サーバの運用者の両方の対応が必要である．**図 -5** を用いて，関係者への影響を説明する．

■ドメイン名管理での注意事項

鍵の生成と管理

これまで DNS では，ゾーン情報の変更以外にドメイン名の管理者(図中の①)が行う作業は少なかった．しかし，DNSSEC を導入する場合は，セキュリティ上の理由から，KSK と ZSK の生成と管理を定期的に実施する必要がある．

KSK の秘密鍵は，特に安全な生成と管理が必要である．ルートや TLD のように鍵生成と管理がいかに安心・安全に行われているかを第三者に対して担保する必要がある場合は，鍵運用方法の公開や，これを適切な手順で第三者の立会いのもとで行うキーセレモニーを実施することもある．

なお，生成した KSK を利用する際は，対応する DS レコードを上位のレジストリ (図中の②) に登録する必要がある．上位と下位の鍵情報に不整合が生じると，鍵の信頼の連鎖が途切れることとなり，該当するゾーンについてすべての DNSSEC 検証に失敗し，致命的な問題となる．

ZSK，KSK ともに，万が一秘密鍵の情報が漏れた場合は，速やかに新しい鍵に置き換え，古い鍵を破棄する鍵の緊急更新が必要になる．このようなトラブルが起きないように慎重に管理するのはもちろんだが，上位レジストリとの連携がいつでも実施できるようにしておくことは重要である．

DNS 運用者変更に伴う作業

権威 DNS サーバの運用は，ドメイン名管理者が DNS 運用者 (図中の③) に委託している場合があるが，委託先は必ずしも固定とは限らない．

DNSSEC 導入前であれば，新しい運用者 (図中の③´) への変更は，新しい権威 DNS サーバの運用を始め，NS 情報を変更するだけで容易に実施できた．しかし DNSSEC 導入後では，信頼の連鎖を維持しながらの変更が必要である．そのため DNS 運用者の変更の手順は，鍵の生成，管理を誰が実施しているかに依存し，複雑なプロセスが必要となる．いったん DNSSEC を解除してから対応する方法や，新旧運用者が密に協力して行う方法が考えられるが，いずれの場合も失敗しないよう細心の注意が必要である．

サブドメインの委任時の扱い

ドメイン名の管理者が，さらに下位のサブドメインを別な管理者 (図中の④) に委任している場合は，そのサブドメインが DNSSEC を導入する際，DS

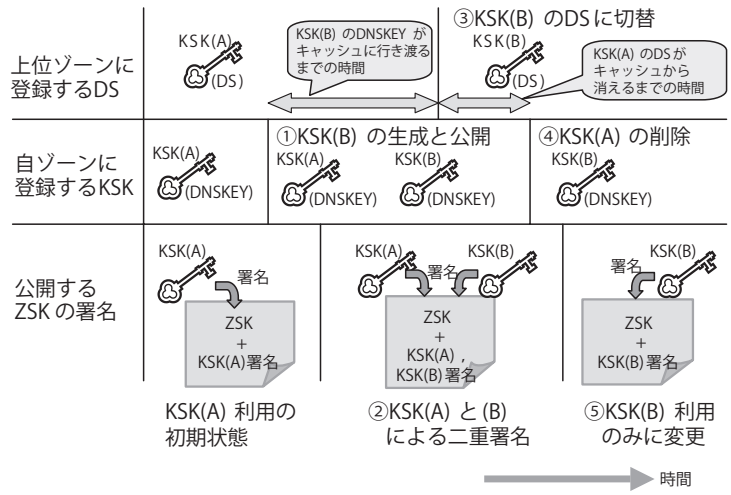

図 -6　KSK の更新の流れ（二重署名法）

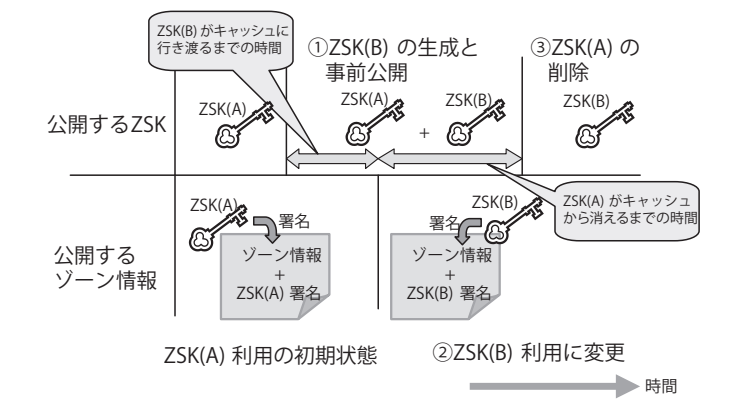

図 -7　ZSK の更新の流れ（事前公開法）

の登録受付をできるようにする必要がある．前述のとおり，これらは定期的な更新がなされるため，上位レジストリと同様の機能が必要となる．大きな会社や，大学などで，下部組織がそれぞれ独自の DNS 管理，運用を行っている場合，対応が必要である．

■権威 DNS サーバ運用の注意事項

鍵更新時の注意事項

KSK や ZSK の更新を行う際は，DNSSEC の署名の検証が継続できることが保証される手順を踏む必要がある．これには鍵の公開と削除のタイミング，上位ゾーンへの DS 登録・反映の時間，キャッシュの仕組みをあわせて考慮する必要があり，方法としては主に 2 つある．

「二重署名法（Double Signature）」は**図 -6** ①～⑤の手順のうち，②で新旧 2 つの KSK で ZSK を署名することで，いずれの KSK が使われても信頼の連鎖が維持できる．上位レジストリへの DS の更新が 1 回で済むため，KSK の更新で利用されることが多い．「事前公開法（Pre-Publish）」は**図 -7** ①～③の手順のうち①で新しく使う鍵を実際に署名に使う前から事前に公開する．ゾーン情報の署名量を増やさずに更新ができるため，ZSK の更新で利用されることが多い．いずれの方法も，キャッシュで旧情報が保持されることを考慮して作業を行う必要があり，注意が必要な点である．

権威 DNS サーバのトラフィック

権威 DNS サーバで署名を行うと，応答に署名情報が付加されるため，応答パケットのサイズが大きくなり，トラフィック量が増大する．DNSSEC 検証機能を実装しているキャッシュ DNS サーバでは，検証の実施有無にかかわらず，署名情報を要求するオプション（DO : DNSSEC OK ビット）を有効にしてクエリを送出する実装が多い．そのため，権威 DNS サーバ側で署名を行うと，DNSSEC 検証の普及度合いにかかわらず，応答のパケットサイズが大きくなると考えてよい．署名情報を含めた応答は約 5 ～ 10 倍のサイズであり，受け取るクエリが多く元々 DNS のトラフィックが相当量ある場合は，トラフィック量の増大は無視できないものとなる．

■キャッシュ DNS サーバ運用の注意事項

トラストアンカーの登録

キャッシュ DNS サーバ（図 -5 中の⑤）で

DNSSEC検証を有効にするには，信頼できるトラストアンカーを運用者がキャッシュDNSサーバに登録する必要がある．トラストアンカーは，KSK更新にあわせて定期的な変更が行われるため，キャッシュDNSサーバでも定期的に更新が必要である．ただし，RFC 5011に則ったキャッシュDNSサーバの実装を用いることで，運用の手間の軽減をすることもできる．

DNSSEC検証の失敗時

実際にキャッシュDNSサーバにてDNSSEC検証を導入すると，検証の失敗に遭遇することがあるだろう．これはセキュリティ的な問題が起きている可能性をあらわす．しかしDNSSECの運用は，まだ十分に一般的になっておらず，現時点ではドメイン名管理者が事故を起こすケースが少なくない．このような事象が起き得ることを心にとめてキャッシュDNSサーバの運用を行い，経験を蓄積する必要がある．

なお，permissiveモードを利用することで，検証失敗時も該当するドメイン名にアクセスを続けることも可能だが，セキュリティのリスクを検討の上，実施してもらいたい．

使用するリソースの増加

キャッシュDNSサーバが扱うトラフィックは，DNSSEC検証の実施を行っても，権威DNSサーバ側ほどの大きな変化が現れない場合がある．これは前述のとおり，すでに署名情報を権威DNSサーバに要求している実装が多いためである．この場合，権威DNSサーバ側のDNSSEC導入有無でトラフィックが増加するため，今後多くのドメインでDNSSEC導入が進めば，それに応じてキャッシュDNSサーバの扱うトラフィックが増加することになり，今からそれを考慮しておくべきである．

一方，DNSSEC検証時にはCPUやメモリのリソースの消費が増える．これによりクエリ応答の性能の上限が低くなるため，運用者は事前にサーバのパフォーマンスの余裕を確認しておくべきである．

■ネットワーク機器運用での注意事項

パケットサイズ増大の影響

DNSサーバでDNSSECの導入を行うには，合わせてサーバ周辺のネットワークへの影響を理解し，正しく対応できることを確認する必要がある．

署名や鍵情報を扱うことで，個々の応答パケットのサイズが大きくなることに注意が必要である．DNSの応答パケットはUDPで512バイト以内が基本であるが，DNSSECではこれを超えるサイズを扱うためにEDNS0（Extension Mechanisms for DNS）という拡張を用いる．正しく実装され，設定されたネットワーク機器であれば，これに対応しており問題はないが，古いファイアウォール機器等で512バイトに制限している実装や，UDPのフラグメントに対応できないものが確認されている．正しい通信ができない場合，DNSクエリがTCPにフォールバックすることで検索時間が長くなったり，検索が不可能になる場合があり得る．

また，家庭用ルータ等はDNSのプロキシ機能を実装していることがあり，古い実装ではDNSSECに対応できない事例が見受けられる．

これらネットワーク機器に関しては，機器の情報を確認し，最新のファームウェアに更新するなどの対応が必要となる．

DNSSECの確認ツール

DNSSEC導入を行うにあたり，クライアント環境で利用できるツール等（Webサイト）を**表-3**で紹介する．これらを用いることで，設定したDNSSEC環境の動作が正しいかの確認に使ってほしい．

DNSSECの今後

DNSSECは導入が始まったばかりの技術である．DNSの運用者にとって，DNSSECの運用は決して容易なことではないが，DNSのセキュリティ向上のためには必須の技術であり，今後は，権威DNS

署名されたドメイン名の確認	
DNS の設定チェック（JPRS）	
http://dnscheck.jp/	DNS 設定のチェック Web．DNSSEC の鍵の状態を確認できる．
DNSviz（Sandia National Laboratories）	
http://dnsviz.net/	DNSSEC の信頼の連鎖を図で表示する．
DNSSEC Debugger（Verisign Labs.）	
http://dnssec-debugger.verisignlabs.com/	DNSSEC の信頼の連鎖が正しい状態か確認する．
キャッシュ DNS サーバの DNSSEC 対応の確認	
test.dnssec-or-not.org（Verisign Labs）	
http://test.dnssec-or-not.org/	利用中のキャッシュ DNS サーバが DNSSEC 対応かどうかを表示するサイト．
Deliberately Broken DNSSEC Validation Test Site（Comcast）	
http://www.dnssec-failed.org/	DNSSEC 検証で故意に失敗するようにしてあり，キャッシュ DNS サーバが DNSSEC 対応時はエラー表示となる．
OARC's DNS Reply Size Test Server	
https://www.dns-oarc.net/oarc/services/replysizetest/	DNS の応答が途中のネットワーク機器等で制限されていないかを確認できる仕組み．
DNSSEC に対応したアプリケーション	
DNSSEC Validator（CZ.NIC Labs）	
http://www.dnssec-validator.cz/	FireFox のアドオンとして，表示中のサイトの DNSSEC 対応と，キャッシュ DNS サーバの DNSSEC 対応の確認ができる．
ネットワーク機器の DNSSEC 対応の確認	
DNSSEC Hardware Tester（CZ.NIC）	
http://www.dnssec-tester.cz/	ネットワーク機器の DNSSEC 対応の検証ツールとその結果がある．

表 -3　DNSSEC の確認ツール

サーバやキャッシュ DNS サーバへの導入が進んでいくであろう．DNS の運用者は，DNSSEC の運用に関する知識も身につけていく必要がある．

また，日頃情報機器に多く接し，管理者とも近いであろう会員各位には，ご自身の参考に，また周囲への啓発に，本記事が役立つと幸いである．

関連情報

書籍	
実践 DNS -DNSSEC 時代の DNS の設定と運用（2011 年）	
民田雅人，森下泰宏，坂口智哉 （株）アスキー・メディアワークス ISBN: 978-4-04-870073-3	
Web ページ	
DNS 関連技術情報（JPRS） http://jprs.jp/tech/	
DNSSEC 関連情報（JPRS） http://jprs.jp/dnssec/	
DNSSEC ジャパン（DNSSEC.jp） http://dnssec.jp/	
日本 DNS オペレーターズグループ（DNSOPS.JP） http://dnsops.jp/	
TLD DNSSEC Report（ICANN） http://stats.research.icann.org/dns/tld_report/ TLD のゾーン署名の状況を確認可能	
BIND（ISC） http://www.isc.org/software/bind/	
NSD（NLnetLabs） http://www.nlnetlabs.nl/projects/nsd/	
Unbound（NLnetLabs） http://unbound.net/	
OpenDNSSEC（OpenDNSSEC） http://www.opendnssec.org/	
LDNS（NLnetLabs） http://www.nlnetlabs.nl/projects/ldns/	
主な RFC	
RFC 4033（2005）: DNS Security Introduction and Requirements	
RFC 4034（2005）: Resource Records for the DNS Security Extensions	
RFC 4035（2005）: Protocol Modifications for the DNS Security Extensions	
RFC 5011（2007）: Automated Updates of DNS Security（DNSSEC）Trust Anchors	

（2011 年 5 月 31 日受付）

三田村健史（正会員）　mitamura@jprs.co.jp
DNS およびインターネットドメイン名に関する技術企画，管理運用に従事．（株）日本レジストリサービス技術研究部長，兼システム運用部長．電子情報通信学会会員．

佐藤新太　shinta@jprs.co.jp
JP の DNS およびレジストリシステムの運用を経て，技術企画，DNS 関連研究に従事．（株）日本レジストリサービス 技術研究部．