DNS サーバ DNSSEC 導入

鍵管理チェックリスト

平成 23 年 3 月

DNSSEC ジャパン

DNSSEC サーバ DNSSEC 導入

鍵管理チェックリスト

（目次）

DNS サーバ DNSSEC 導入
鍵管理チェックリスト

1. はじめに

近年、インターネットの根幹を支える重要な仕組みであるDNSに対して、DNS応答を偽造することで引き起こされるセキュリティ上の脅威(キャッシュポイズニング)が顕在化している。

その対策として、DNS のセキュリティ拡張機能である DNSSEC の導入が急がれ、2010 年 7 月、ルートサーバに導入されたのをきっかけに、各 gTLD、ccTLD も続々と導入に向けての施策を進めている。

1.1. 目的

「DNS サーバ DNSSEC 導入鍵管理チェックリスト」(以下、「本ドキュメント」という。)は、DNS サーバへの DNSSEC 導入に伴い、鍵の作成と管理において考慮しなければならない確認事項を取りまとめ、チェックリストとして提示することで、スムーズに DNSSEC 導入ができることを目的としている。

また、本ドキュメントで対象とする「鍵」は、ZSK (Zone Signing Key)と KSK (Key Signing Key)のそれぞれ秘密鍵を想定している。

本ドキュメントが、健全な DNSSEC 運用を確保することに一助になれば、幸いである。

1.2. 注意事項

・免責事項

本ドキュメントの内容は保証されたものではない。下記 Web サイトの免責事項を確認いただいた上で、本ドキュメントを使用されたい。

http://dnssec.jp/?page_id=16

・問合せ先

本ドキュメントに関する改善点等のコメントは下記事務局までご連絡ください。

DNSSEC ジャパン事務局　＜sec@dnssec.jp＞

1.3. 想定する読者

本ドキュメントは、DNSSEC に対応する必要があるドメイン名登録者、ドメインレジストラ(JP ドメイン名の場合は指定事業者)、DNS サーバ運用者を、読者として想定している。また、本ドキュメントの完全な理解のためには、DNSSEC を含む DNS の概念について基本的な理解があることが望ましい。

DNSSEC の基本に関しては、下記の【基本情報】の各文書を参照されたい。

【基本情報】

DNSSEC の仕組みと現状
http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-DNSSEC-mechanisms-and-status.pdf

DNSSEC 導入に当たって
http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-DNSSEC-deployment.pdf

DNSSEC 関連 RFC
http://dnssec.jp/?page_id=124
RFC 4033 DNS Security Introduction and Requirements.
RFC 4034 Resource Records for the DNS Security Extensions.
RFC 4035 Protocol Modifications for the DNS Security Extensions.

1.4. 本チェックリストの位置付け

本チェックリストは、【参考情報】に示される各文書を参考としているが、あくまで現実的な運用を念頭において独自の基準に基づいて作成されたものである。また、本チェックリストで想定している安全性の水準は、ほとんどの DNSSEC 運用者にとって十分安全といえるものである。しかながら、運用者によっては、本チェックリストを満足することがコスト面から難しかったり、求められる安全性の水準を上回っていることがありうる。そのような場合、運用者は、求められる安全性と既存システムとのバランスを考慮した上で、本チェックリスト中の個々の項目に対応するか否かを各自検討されたい。

1.5. 謝辞

本チェックリストを作成するに当たり、貴重な時間を割いてご協力いただきました以下の皆様に深く感謝いたします。

会社名(五十音順)
株式会社サリオンシステムズリサーチ
東京エレクトロン デバイス株式会社

2. チェックリスト

DNSSEC に利用される鍵の管理において、最低限確認すべき項目を以下に示す。

項番	確認項目	結果 OK / NG
鍵の生成は、適切な方法、パラメータを用いて行わなければならない。		
1	ZSK の鍵長は 1024 ビット以上である※1	
2	KSK の鍵長は 2048 ビット以上である	
3	署名アルゴリズムとして、RSA/SHA-256 または RSA/SHA-512 を使用している	
4	鍵の生成には、RFC 4086 または NIST SP 800-90 に準拠した乱数生成器等で発生させた安全な乱数を使用している	
5	使用している署名アルゴリズム、OS、ライブラリ等に脆弱性は見つかっていない	
外部から鍵へ不正なアクセス(読み取り、利用、生成、更新)が行われないよう、対策が講じられていなければならない		
6	外部からの不正なアクセスが行えないよう、ゾーンファイルへの署名操作および署名されるゾーンファイルのマスターコピーの保管をオフライン環境に限定するなど、対策が施されている	
内部から鍵へ不正なアクセスが行われないよう、対策が講じられていなければならない		
7	内部からの鍵へのアクセスは権限を有する管理者のみに限定するなど、対策が施されている	
8	KSK 秘密鍵は、暗号化を施したリムーバルメディア等へ保存するか、HSM 等を使用するなど、物理的に保護されている	
9	KSK の生成および利用には、複数人の立会いを必須としている	
鍵の管理・利用は、適切な方法で行わなければならない。		
10	複数ゾーンの署名に同一の ZSK を使用しないこと※2	
11	KSK の更新間隔は 1 年程度である	
12	ZSK の更新間隔は 1 ヶ月程度である	
13	鍵の更新手順は、「RFC 4641 bis」の「4.1 鍵のロールオーバー」に基づいている。また、更新手順は明確に文書化されている。	
鍵の危殆化もしくは破損時の対策および対応方法を、あらかじめ定めておかなければならない		
14	鍵のバックアップメディアは、元の鍵と同等またはそれ以上のセキュリティ対策を行った上で、保存性と回復手順を考慮した形で管理・保管されている	
15	鍵危殆化時の鍵更新手順をはじめとした対応手順は、「RFC 4641 bis」の「4.2 鍵の緊急ロールオーバー」に基づいている。また、更新手順は明確に文書化されている。	
適切な運用がなされているか、定期的に監査を行わなければならない		
16	鍵の管理・利用が定められた手順にしたがって行われていることを後日確認できるように、監査ログを残すなど適切な対応を行っている。また、定期的に監査を実施している。	
17	鍵の生成・更新等の各作業手順は明確に文書化され、担当者に周知されている	
18	使用している署名アルゴリズム、鍵長、OS、ライブラリ等に脆弱性が見つかっていないか、定期的に確認を行っている	

＜補足説明＞

※1 現在では、RSA の鍵長は 2048 ビット以上とすることが標準とされている。既存システムにおいて RSA 1024 ビットが使用されている場合は、性能上の問題がない限り、RSA 2048 ビットに移行することが強く推奨される。NIST(米国立標準技術研究所)の 2011 年 01 月の勧告では、1024 ビットの鍵は、2011 年からは使うべきでなく、2014 年以降は許されないとしている[9]。

※2 複数のゾーンに同一の鍵を用いて署名を行った場合、個々のゾーンに異なる鍵を用いる場合より多くの情報を攻撃者に渡すことになり、安全性が低下する。複数ゾーンに単一の鍵を用いた場合のリスクは高くはないと思われるが、可能な場合、分けるほうが望ましい。

3. 参考情報

[1] DNSSEC ジャパン(DNSSEC.jp)
http://dnssec.jp/

[2] JPRS(DNSSEC 関連情報)
http://jprs.jp/dnssec/

[3] JPNIC(DNSSEC)
http://www.nic.ad.jp/ja/newsletter/No43/0800.html

[4] RFC 4641 bis
http://jprs.jp/tech/material/id/draft-ietf-dnsop-rfc4641bis-04-ja.txt

[5] RFC 5011
http://jprs.jp/tech/material/rfc/RFC5011-ja.txt

[6] RFC 5702
http://jprs.jp/tech/material/rfc/RFC5702-ja.txt

[7] IPA 安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン(案)
http://www.ipa.go.jp/security/fy19/reports/Key_Management/documents/keymanagement_guideline.pdf

[8] IPA 暗号世代交代の現状と課題
http://www.ipa.go.jp/about/news/event/ipaforum2010/pdf/ipaforum2010_security2.pdf

[9] NIST Special Publication 800-131A
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[10] DNSSEC における鍵管理
http://dnssec.jp/wp-content/uploads/2011/04/20110317-dnssec-techwg-keymgmt.pdf

以上