# 2011年度版リストガイド(DNSSEC)

平成24年3月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

# 目 次

# 1　本書の位置づけ

## 1.1　本書の目的

リストガイドは、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、電子政府推奨暗号を利用する際に必要となる情報並びに推奨を示すものである。本書では、電子政府で DNSSEC を運用する際に選択すべき暗号アルゴリズムについて情報提供を行うことを目的とする。

## 1.2　対象とする利用目的

本書の想定読者は、政府機関において電子政府システムの調達を行う政府職員、ならびに、電子政府システムの構築、運用を行う情報システムの開発者および運用者を対象とする。本書で想定する利用目的は、我が国の政府機関における電子政府システムの調達、ならびに、運用において、DNSSEC 利用時の鍵生成に必要となる暗号鍵のアルゴリズムと鍵長に関する推奨事項ならびに関連する情報提供を行うことである。

## 1.3　本書の構成

## 1.4　本書の利用範囲

本書の内容は 2012 年 3 月 31 日時点の情報に基づき構成されている。従って、今後、電子政府推奨暗号の改訂や電子政府推奨暗号に係る攻撃方法の研究動向、Internet Engineering Task Force (以下、「IETF」という。) における各種 Request For Comments (以下、「RFC」という。) やその他標準規格の策定状況及び米国 National Institute of Standards and Technology の Special Publicaion (以下、「SP」という。) をはじめとする推奨文書等の改定状況等によって、本書に掲載される内容がそぐわなくなるケースが発生する可能性がある。本書を利用する際には、関連する標準規格並びに各種推奨文書等も同時に参照し、適切に判断を行うことを勧める。

# 2 定義と表記

## 2.1 定義

表 1: 用語の定義

| 用語 | 定義 |
|---|---|
| 暗号スイート | 当該プロトコルにおいて選択可能な暗号アルゴリズムの組合せ。プロトコルの仕様により異なる。 |
| 完全性 | 不当に情報が改変または消去されていないことを示す特性。データが生成、移送、蓄積されて以後、許可されていない方法で当該データが変更されていないことを示す。本文書では、ある暗号アルゴリズムにより「完全性が与えられる」という表現は、当該アルゴリズムが、不当な改変または消去を発見するために用いられることを意味する。 |

## 2.2 表記

表 2: 略語の定義

| 略語 | 定義 |
|---|---|
| IETF | Internet Engingeering Task Force |
| NIST | National Institute of Standards and Technology |
| RFC | Request For Comments |
| SP | Special Publications |

# 3 DNSSECに関する推奨

## 3.1 ネームサーバのソフトウェア・バージョンによる制約

### 3.1.1 選択できる暗号

ゾーンの署名としてDNSSECで利用できる暗号アルゴリズムはIETFのRFCによって定められている。 ゾーン署名に利用できる暗号アルゴリズムは表3の通り。なお、 本書ではDNSSECの暗号アルゴリズムをニーモニックにて表現する。

表 3: DNSSECで利用できる暗号アルゴリズム

| アルゴリズム番号 | 暗号アルゴリズム | ニーモニック | 参照先 |
|---|---|---|---|
| 1 | RSA/MD5 | RSAMD5 | RFC4034,RFC2537 |
| 2 | Diffie-Hellman | DH | RFC2539 |
| 3 | DSA/SHA1 | DSA | RFC3755, RFC2536 |
| 4 | Elliptic Curve | ECC | 具体的な記述なし |
| 5 | RSA/SHA-1 | RSASHA1 | RFC3755, RFC3110 |
| 6 | DSA-NSEC3-SHA1 | DSA-NSEC3-SHA1 | RFC5155 |
| 7 | RSASHA1-NSEC3-SHA1 | RSASHA1-NSEC3-SHA1 | RFC5155 |
| 8 | RSA/SHA-256 | RSASHA256 | RFC5702 |
| 10 | RSA/SHA-512 | RSASHA512 | RFC5702 |
| 12 | GOST R 34.10-2001 / R 34.11- 94 | ECC-GOST | RFC5933 |

ECCは現在DNSSECにおいて利用できる暗号としてRFCで規定されていない。また、 同様にしてNIST SP800-81でも推奨はしていない。 しかし、 RFC4034上では “Elliptic Curve” として予約されているアルゴリズム番号が存在する。

### 3.1.2 DNSSECにおける不在証明

DNSSECではドメイン名が存在しない場合、存在しないドメイン名が偽造されるのを防ぐために、存在しないことを証明 (不在証明) する必要がある。具体的には存在するレコード対しては署名 (RRSIG RR) を付加し、署名を検証ができる。しかし、存在しないレコードからは署名生成が行えないため「存在しないレコード」が存在しないことを検証することはできない。

そこで不在証明を行うために、 すべての存在するレコードを整列し、レコードのリスト構造を生成する。 このリスト構造から、 ある存在するレコードの次のレコードの情報に関して署名生成および署名検証を行う方式がNSEC(Next-SECure record)またはNSEC3(NSEC record version 3) 方式である。

NSEC 方式では、存在するレコードすべてを整列し、 次のレコードへのリストを生成することで指定された名前が存在しないことを示す。また、 NSEC3 方式ではドメイン名をハッシュ関数でハッシュ化した文字列を Base32 でエンコードしたものを並べる。 NSEC では平文で次のドメインが示されていたことから、 悪意のある攻撃者がゾーンデータ全体を容易に入手してしまうことが可能となってしまうが、 ハッシュ化したドメイン名を並べることで、ドメイン全体の情報を開示せず、 NSEC と同様の不在証明を行うことができるのが NSEC3 である。

DNSSEC のアルゴリズム番号の 3 の DSA と 6 の DSA-NSEC3-SHA1、 また 5 の RSASHA1 と 7 の RSASHA1-NSEC3-SHA1 は、 それぞれ不在証明に NSEC 方式を利用するか、 NSEC3 方式を利用するかの違いによって便宜上使い分けるものであり、 署名方式としての差異は無い。

### 3.1.3　ネームサーバごとの制約

DNSSEC は公開鍵暗号方式を用いて、 DNS 通信における DNS レコードの出自と完全性を検証可能とする仕組である。 この機能を実現するネームサーバは複数存在している。

また、 DNSSEC は提供されているソフトウエアによって利用できる機能が異なる。さらにはネームサーバのソフトウエアの種類だけでなく、 バージョンごとに使用できる暗号アルゴリズム・暗号鍵の鍵長が異なる。 本項では代表的なネームサーバとして BIND 9、 NSD、 Unbound が利用できる暗号スイートを示す。

#### 3.1.3.1　BIND 9

BIND 9 は DNSSEC に対応する権威 DNS サーバ兼キャッシュDNS サーバであり、鍵の生成から署名まで DNNSEC 運用に必要なツール群を備えている。BIND の最新安定版である 9.8 系から 9.6 系について利用可能な暗号スイートは表 4 から表 8 のとおりである。

表 4: BIND 9.9 系と 9.8 系

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 9.9.0 | 9.8.1 | 9.8.0 |
|---|---|---|---|---|
| RSA/MD5 | 512 - 4096 bit | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | ○ | ○ | ○ |

ただし、 GOST R 34.10-2001 / R 34.11- 94 を利用する場合には OpenSSL 1.0.0 以降が必要。

表 6: BIND 9.7 系

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 9.7.4 | 9.7.3 | 9.7.2 | 9.7.1 | 9.7.0 |
|---|---|---|---|---|---|---|
| RSA/MD5 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | × | × | × | × | × |

表 8: BIND 9.6 系

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 9.6-ESV-R5-P1 |
|---|---|---|
| RSA/MD5 | 512 - 2048 bit | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ |
| RSA/SHA-256 | 512 - 2048 bit | ○ |
| RSA/SHA-512 | 512 - 2048 bit | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | × |

#### 3.1.3.2 NSD

NSD は DNSSEC に対応する権威 DNS サーバであり、利用できる暗号スイートは表 10 のとおりである。

表 10: NSD

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 3.2.9 | 3.2.8 | 3.2.7 | 3.2.6 |
|---|---|---|---|---|---|
| RSA/MD5 | 512 - 4096 bit | ○ | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | ○ | ○ | ○ | ○ |

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 3.2.5 | 3.2.4 | 3.2.3 | 3.2.2 | 3.2.1 |
|---|---|---|---|---|---|---|
| RSA/MD5 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | ○ | ○ | ○ | ○ | ○ |

ただし、 GOST R 34.10-2001 / R 34.11- 94 を利用する場合には OpenSSL 1.0.0 以降が必要。

#### 3.1.3.3 Unbound

Unbound は DNSSEC に対応するキャッシュDNS サーバであり、利用可能な暗号スイートは表 13 のとおり。

表 13: Unbound

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 1.4.13 | 1.4.12 | 1.4.11 | 1.4.10 |
|---|---|---|---|---|---|
| RSA/MD5 | 512 - 2048 bit | ○ | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | ○ | ○ | ○ | ○ |

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 1.4.9 | 1.4.8 | 1.4.7 | 1.4.6 | 1.4.5 |
|---|---|---|---|---|---|---|
| RSA/MD5 | 512 - 2048 bit | ○ | ○ | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | ○ | ○ | ○ | ○ | ○ |

| 利用できる暗号アルゴリズム | 選択可能な鍵長 | 1.4.4 | 1.4.3 | 1.4.2 | 1.4.1 | 1.4.0 |
|---|---|---|---|---|---|---|
| RSA/MD5 | 512 - 2048 bit | ○ | ○ | ○ | ○ | ○ |
| Diffie-Hellman | 128 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| DSA/SHA-1 | 512 - 1024 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-1 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-256 | 512 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| RSA/SHA-512 | 1024 - 4096 bit | ○ | ○ | ○ | ○ | ○ |
| GOST R 34.10-2001 / R 34.11- 94 | 512 bit | △ | × | × | × | × |

ただし、 Unbound 1.4.4 以降において GOST R 34.10-2001 / R 34.11- 94 を利用する場合には OpenSSL 1.0.0 以降が必要。

## 3.2 推奨暗号スイートと鍵長

### 3.2.1 IETF RFC と NIST SP 文書による推奨

RFC および SP では、DNSSEC の KSK(Key Signing Key:署名検証鍵) と ZSK(Zone Signing Key:ゾーン署名鍵) に対して次のような推奨が行われている。

表 17: KSK に対する推奨

| 項目 | IETF RFC | NIST SP |
|---|---|---|
| アルゴリズムごとの鍵長 | RSA/MD5 は利用可能だが非推奨である。 | SP800-57part3 において SP800-57Part1 のアルゴリズムを利用することを推奨 |
| アルゴリズムごとの鍵長の推奨 | 一般的に RFC4641 では管理するドメインの大きさによって 1024、 1300、2048 ビットを推奨している。 | SP800-57 Part3 において SP800-57 Part1 に記載されている鍵長を利用することを推奨、SP800-81 にて RSA/SHA1 または RSA/SHA256 の場合 2048bit とすることを推奨している。 |
| | RFC3110 において RSA/SHA-256 の鍵長は 512-4096bit から選択し 、RSA/SHA-512 は 1024-4096bit から選択することが記載されている。 | |
| | RFC5953 では GOST の暗号鍵長を 512bit と指定している。 | |
| 利用期間や更新に関する推奨 | RFC4641 には利用期間を 12ヶ月として 1ヶ月の鍵更新期間を設けることとされている。 | SP800-81 にて 12ヶ月での更新が推奨されている。 |

表 18: ZSK に対する推奨

| 項目 | IETF RFC | NIST SP |
|---|---|---|
| 利用するアルゴリズムに関する推奨 | RSA/MD5 は利用可能だが非推奨である。 | SP800-57part3 において SP800-57Part1 のアルゴリズムを利用することを推奨 |

| | | |
|---|---|---|
| アルゴリズムごとの鍵長の推奨 | RFC4641 では KSK よりも短い鍵長であることが推奨されている。 | SP800-57 Part3 にて RSA/SHA-1 または RSA/SHA256 の場合、1024bit として推奨している。 |
| 利用期間や更新に関する推奨 | RFC4641 には 1ヶ月での更新が妥当とされている。 | SP800-81 にて 1ヶ月から 3ヶ月での更新が推奨されている。 |

### 3.2.2 電子政府で利用する推奨暗号スイートと鍵長

電子政府で利用する DNSSEC における暗号スイートを表 19 のとおりとする。

表 19: DNSSEC における推奨暗号スイート

| アルゴリズム番号 | 暗号スイート |
|---|---|
| 2 | Diffie-Hellman |
| 3 | DSA/SHA1 |
| 5 | RSA/SHA-1 |
| 6 | DSA-NSEC3-SHA1 |
| 7 | RSASHA1-NSEC3-SHA1 |
| 8 | RSA/SHA-256 |
| 10 | RSA/SHA-512 |

DNSSEC で利用する暗号鍵の鍵長はゾーン署名鍵 (Zone Signinig Key; ZSK) と署名検証鍵 (Key Singning Key; KSK) に関して表 20 のとおりとする。

表 20: DNSSEC における推奨鍵長

| 鍵の種類 | 鍵長 |
|---|---|
| ゾーン署名鍵 (Zone Signinig Key; ZSK) | 1024 bit |
| 署名検証鍵 (Key Singning Key; KSK) | 2048 bit |

# 参考文献

[Minda2011] 民田雅人, 森下泰宏, 坂口智哉, “実践 DNS DNSSEC 時代の DNS の設定と運用”, アスキー・メディアワークス, 2011 年 5 月

[Internet Systems Consortium, BIND] Internet Systems Consortium(ISC), BIND http://www.isc.org/

[NLnet Lab. NSD, Unbound] Olaf Kolkman, DNSSEC HOWTO, a tutorial in disguise, July 4, 2009, NLnet Labs http://www.nlnetlabs.nl/publications/dnssec_howto/

[Infoblox Administrator Guide] Infoblox, “Infoblox Administrator Guide NIOS 6.1.0 for Infoblox Core Network Services Appliances”, April 22, 2011 http://ww2.infoblox.com/support/tech_lib/NIOS/NIOS_AdminGuide_6.1.0.pdf

[Secure64, Secure64 Cryptographic Module] Secure64, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1439.pdf

[RFC4034] S. Rose, “Resource Records for the DNS Security Extensions”Internet Engineering Task Force (IETF), Request for Comments, March, 2005

[RFC3755] S. Weiler, “Legacy Resolver Compatibility for Delegation Signer (DS)”, Internet Engineering Task Force (IETF), Request for Comments, May, 2004

[RFC6014] P. Hoffman, “Cryptographic Algorithm Identifier Allocation for DNSSEC”, Internet Engineering Task Force (IETF), Request for Comments, November, 2010

[SP 800-81, revision1] National Institute of Standards and Technology, “Secure Domain Name System (DNS) Deployment Guide, Recommendations of the National Institute of Standards and Technology ,”April, 2010.

発行日　2012 年 9 月 30 日第 1 版 第 1 刷
発行者
・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室、
セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN
・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（技術本部 セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN