PQ DNSSEC遊び

Kazunori Fujiwara
fujiwara@jprs.co.jp
株式会社日本レジストリサービス (JPRS)

(2026年6月のdnsops.jp summer dayにて)

簡易なDNSSEC

- 原則2035年までに耐量子暗号への移行が求められている
  - アメリカ政府: 国立標準技術研究所 (NIST)
  - 日本政府: 内閣官房国家サイバー統括室(NCO)

- 耐量子暗号への移行は、標準が決まり、ツールがそろってから検討
  - 2035年までに移行することだけが決まっている状態
    → 2034年に実施すればいい

Copyright © 2026 Japan Registry Services Co., Ltd.

(2026年6月のdnsops.jp summer dayにて)

JPRS

耐量子暗号への移行を焦らない理由

- DNSSECは署名のみで暗号化しないため、データを蓄積してあとで暗号解読する攻撃の対象外
- まだ署名アルゴリズムが決まっていない (つまり実装がない)
  - NISTが方針を決め、IETFで標準化して、実装が出そろうまで 5年でできる気がしない
  - なにかあったらNIST, IETF, 開発者があわてるので、それからでよい
- つまり、期限の2034年に行えばよい

Copyright © 2026 Japan Registry Services Co., Ltd.

転向

- 焦らない、という発表をしましたが、最近PQ-DNSSEC業界に変化があったので、ふつーPQに転向しました

- しばらくは、「ふつーMLDSA44」で

Copyright © 2026 Japan Registry Services Co., Ltd.

PQC DNSSEC その後

- IETF 126 (2026/7) にて PQ-DNSSEC side meeting 開催
  - 今後は表 (dnsop WGなど) で標準化を進める
  - NISTのアルゴリズム標準化の完了を待たず、標準化されたもので進める
- 2026/10/2 dnsop WG interim meeting: PQ-DNSSEC
  - 2026/8にML-DSA-44にアルゴリズム18が割り当てられたことが報告
    - https://www.iana.org/assignments/dns-sec-alg-numbers
  - Cloudflare 1.1.1.1 にてML-DSA-44のDNSSEC validation実験開始
  - NIST PQC algorithmのステータスの報告など

Copyright © 2026 Japan Registry Services Co., Ltd.

ML-DSA-44 アルゴリズム18

- draft-westerbaan-dnssec-mldsa-04
  - Module-Lattice Digital Signature Algorithm for DNSSEC
  - ML-DSA-44は2024年にNIST発行のFIPS-204で規定
  - 公開鍵のサイズは1312バイト、署名のサイズは2420バイト
  - DNSSECプロトコルの変更は必要なく、アルゴリズム追加のみ
  - 署名、検証のCPU利用量はRSA, ECDSAと大差なし
  - ニーモニック: MLDSA44
  - 現在のdraftでは、署名、検証、実装ともにMAY
- DNSSEC Algorithm Numberは、提案(draftとかメール)により、Expert Reviewを経て割り当てられる

Copyright © 2026 Japan Registry Services Co., Ltd.

その他の案

- FN_DSA_512
  - Falcon 512と呼ばれていた案、署名サイズが666バイトなので有力だが、標準化が停止していた。
  - 9月末ごろに標準化再開、FIPS-206 として標準化される見込み
  - 公開鍵サイズは897バイトなので、DNSKEY応答は1500バイトを超える
- SLH-DSA in MTL mode
  - Verisignが提案、patentを持っていてライセンスもするらしい
  - SLH-DSAはFIPS 205で標準化済
  - RRSIGをMerkle Treeにいれ、各RRSIGには小さいハッシュのみ、頂点には途中のものを含めた完全なものをいれるので巨大という仕組みのようである (理解できていない)

Copyright © 2026 Japan Registry Services Co., Ltd.

現在の実装状況

- BIND 9
  - 2026/11/3 GitLab main branch: Add support for the ML-DSA-44
- Verisignによる実装
  - https://github.com/verisign/{mtl-mode-ldns,MTL,mtl-mode-nsd,mtl-mode-unbound}
  - 多くのPQアルゴリズムに対応 (configureオプションで指定)
- PQCライブラリ liboqs
  - https://openquantumsafe.org/liboqs/
  - FN_DSA(Falcon)など、NISTで選定中のものも入ってる
  - FreeBSD: pkg install liboqs
  - Debianではunstableにのみ存在
  - ML-DSAはOpenSSLに入っているのでliboqs不要
- OpenSSL 3.5以降: ML-DSA-44 対応済

Copyright © 2026 Japan Registry Services Co., Ltd.

HSM

- Thales HSM Luna はML-DSA対応と書かれている
  - 詳細は ML-DSA Thales HSM で検索してください

Copyright © 2026 Japan Registry Services Co., Ltd.

Install: 準備とMTL library

- /usr /usr/local を汚したくないので prefix=/opt/pqc とする
- autoconf, automake, libtool, liboqs を入れておく
  - liboqsが/usr/local にあるときはconfigureにCFLAGS, LDFLAGS 必須
- MTL
  - git clone https://github.com/verisign/MTL
  - cd MTL
  - autoreconf -i
  - ./configure CFLAGS=-I/usr/local/include ¥
    LDFLAGS=-L/usr/local/lib -prefix=$prefix
  - make; make install

Copyright © 2026 Japan Registry Services Co., Ltd.

Install: mtl-mode-ldns

- git clone https://github.com/verisign/mtl-mode-ldns
- cd mtl-mode-ldns/src

need to Patch configure.ac

-AC_SEARCH_LIBS([OQS_SIG_new], [oqs], ,[AC_MSG_ERROR(an acceptable version of liboqs was not found)])

+AC_SEARCH_LIBS([OQS_SIG_new], [oqs], ,[AC_MSG_ERROR(an acceptable version of liboqs was not found)], -lssl -lcrypto)

- autoreconf -i; libtoolize -i;

./configure CFLAGS="-I$prefix/include -I/usr/local/include" ¥
LDFLAGS="-L$prefix/lib -L/usr/local/lib" --prefix=$prefix ¥
--enable-pqc-algo-fl-dsa --enable-pqc-algo-ml-dsa ¥
--enable-pqc-algo-slh-dsa-sha2 --enable-pqc-algo-slh-dsa-shake ¥
--enable-pqc-algo-mayo-1 --enable-pqc-algo-mayo-2 --enable-pqc-algo-snova ¥
--enable-pqc-algo-mtl --with-examples --with-drill

- make; make install

Copyright © 2026 Japan Registry Services Co., Ltd.

Install: BIND 9

- BIND 9 だけで遊ぶとか、MTL遊ばないならこれだけでよい

- git clone https://gitlab.isc.org/isc-projects/bind9
- cd bind9
- meson setup --prefix=/opt/bind9 ../work
- meson compile ../work
- cd ../work; meson install

- 依存パッケージとかldconfigとか権限は略
- これで /opt/bind9/bin/dnssec-keygen -a MLDSA44 可能
- dnssec-signzone も MLDSA44 対応
- OpenSSL 3.5以降が必要 (いまどき標準で入ってる)

Copyright © 2026 Japan Registry Services Co., Ltd.

実験

- xeon2.dnslab.jp: prefix=/opt/pqc にverisign版ldnsと普通のNSDを用意
  - MLDSA44だけならBIND 9 でもよい
- 127.0.0.1 で BIND 9 resolverを動作
- /opt/pqc/etc/nsd/ にゾーンファイルを用意
- https://github.com/kfujiwara/dnsseczonetool を使用
- mldsa44.dnslab.jp slhdsasha2mtl.dnslab.jp slhdsashakemtl.dnslab.jp ゾーンを用意
  - それぞれ、アルゴリズム ML_DSA_44, SLH-DSA-SHA2-128s-MTL-SHA2-128, SLH-DSA-SHAKE-128s-MTL-SHAKE-128 で鍵生成、署名
- ゾーンファイル:

```
$TTL 3600
@  IN      SOA     xeon2.dnslab.jp. root.dnslab.jp. 1 10800 1800 36000 900
       IN      NS      xeon2.dnslab.jp.
       IN      A       203.178.129.45
a    TXT     "a“
_dmarc      TXT     "v=DMARC1;p=reject"
```

Copyright © 2026 Japan Registry Services Co., Ltd.

dnsseczonetool.conf

MASTERDIR="/opt/pqc/etc/nsd"
keygen="/opt/pqc/bin/ldns-keygen"
signzone="/opt/pqc/bin/ldns-signzone"
dsfromkey="/opt/pqc/bin/ldns-key2ds -n“
KSK_PARAM_mldsa44_dnslab_jp="-a ML_DSA_44 -k"
KSK_PARAM_slhdsasha2mtl_dnslab_jp="-a SLH-DSA-SHA2-128s-MTL-SHA2-128 -k"
KSK_PARAM_slhdsashakemtl_dnslab_jp="-a SLH-DSA-SHAKE-128s-MTL-SHAKE-128 -k "
SIGN_PARAM="-u "
KSK_ONLY="YES“

簡単にするためにKSKのみ、ZSKも使用するとDNSKEY RRSetがもっと太る

Copyright © 2026 Japan Registry Services Co., Ltd.

ゾーンファイルのサイズ

480	mldsa44.dnslab.jp	
211840	mldsa44.dnslab.jp.signed	441倍
480	slhdsasha2mtl.dnslab.jp	
46059	slhdsasha2mtl.dnslab.jp.signed	96倍
480	slhdsashakemtl.dnslab.jp	
45746	slhdsashakemtl.dnslab.jp.signed	96倍

Copyright © 2026 Japan Registry Services Co., Ltd.

応答サイズ (MLDSA44)

- dig +norec +dnssec @xeon2.dnslab.jp mldsa44.dnslab.jp A
  - ;; ANSWER SECTION:
  - mldsa44.dnslab.jp. 3600 IN A 203.178.129.45
  - mldsa44.dnslab.jp. 3600 IN RRSIG A 18 3 3600 20261203075942 20261105075942 60297 mldsa44.dnslab.jp. 13kxODWCX44nZUpSiN…..略
  - ;; MSG SIZE rcvd: 2531
- dig +norec +dnssec @xeon2.dnslab.jp mldsa44.dnslab.jp DNSKEY
  - ;; ANSWER SECTION:
  - mldsa44.dnslab.jp. 3600 IN DNSKEY 257 3 18 JJ1FD+dC2WgoOsx…略
  - mldsa44.dnslab.jp. 3600 IN RRSIG DNSKEY 18 3 3600 20261203075942 20261105075942 60297 mldsa44.dnslab.jp. ysFqdMeI…略
  - ;; MSG SIZE rcvd: 3843

Copyright © 2026 Japan Registry Services Co., Ltd.

応答サイズ (MLDSA44 NXDOMAIN)

- dig +norec +dnssec @xeon2.dnslab.jp hoge.mldsa44.dnslab.jp A
  - ;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
  - h.mldsa44.dnslab.jp. 900 IN NSEC i.mldsa44.dnslab.jp. TXT RRSIG NSEC
  - h.mldsa44.dnslab.jp. 900 IN RRSIG NSEC (略)
  - mldsa44.dnslab.jp. 900 IN NSEC _dmarc.mldsa44.dnslab.jp. A NS SOA RRSIG NSEC DNSKEY
  - mldsa44.dnslab.jp. 900 IN RRSIG NSEC (略)
  - mldsa44.dnslab.jp. 900 IN SOA xeon2.dnslab.jp. root.dnslab.jp.
  - mldsa44.dnslab.jp. 900 IN RRSIG SOA (略)
  - ;; MSG SIZE rcvd: 7595 (SOA+NSEC*2+RRSIG*3なので2420*3以上)

Copyright © 2026 Japan Registry Services Co., Ltd.

DNSSEC検証 (1.1.1.1)

- dig +dnssec +ad @1.1.1.1 a.mldsa44.dnslab.jp TXT
  - ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
  - ;; ANSWER SECTION:
  - a.mldsa44.dnslab.jp. 3600 IN TXT "a“
  - a.mldsa44.dnslab.jp. 3600 IN RRSIG TXT 18 4 3600 20261203075942 20261105075942 60297 mldsa44.dnslab.jp. hPsT4dsduwSOcPR…略
  - ;; MSG SIZE rcvd: 2531
- dig +ad @1.1.1.1 mldsa44.dnslab.jp A
  - ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
  - ;; ANSWER SECTION:
  - mldsa44.dnslab.jp. 3600 IN A 203.178.129.45
  - ;; MSG SIZE rcvd: 62

Copyright © 2026 Japan Registry Services Co., Ltd.

DNSSEC検証 (BIND 9)

- dig +dnssec +ad @127.0.0.1 a.mldsa44.dnslab.jp TXT
  - ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
  - ;; ANSWER SECTION:
  - a.mldsa44.dnslab.jp.　3600　IN　TXT　"a“
  - a.mldsa44.dnslab.jp.　3600　IN　RRSIG　TXT 18 4 3600 20261203075942 20261105075942 60297 mldsa44.dnslab.jp. hPsT4dsduwSOcPR…略
  - ;; MSG SIZE　rcvd: 2559 ← DNS Cookie分大きい
- dig +ad @127.0.0.1 mldsa44.dnslab.jp A
  - ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
  - ;; ANSWER SECTION:
  - mldsa44.dnslab.jp.　3600　IN　A　203.178.129.45
  - ;; MSG SIZE　rcvd: 90 ← DNS Cookie分大きい

Copyright © 2026 Japan Registry Services Co., Ltd.

MTL-modeの応答

- dig +norec +dnssec @xeon2.dnslab.jp slhdsasha2mtl.dnslab.jp A
  - ;; ANSWER SECTION:
  - slhdsasha2mtl.dnslab.jp. 3600 IN A 203.178.129.45
  - slhdsasha2mtl.dnslab.jp. 3600 IN RRSIG A 130 3 3600 20261203075942 20261105075942 57941 slhdsasha2mtl.dnslab.jp. AgAAish2wj2rjXau9Fbi+S674MgA0Jyr0OV4f4uJXmmGKTxcw54ANXQR hhpm35DYIgxXAAAAAAAAAqoAAAAAAAACgAAAAAAAAAK/AAZhUAr+Xa1P q19AFV3lLj+QzyFf0pa3m6HWeyp2bJHEZVGYXCkGwPo7V7tFcegcQvsn +A6Bkfy5x1ERwJvDYbxIkdU21rvkkyLje+zpBdy8B4Nak3Zg187+b8gN s7LvSE0=
  - ;; MSG SIZE rcvd: 206
- dig +norec +dnssec @xeon2.dnslab.jp slhdsasha2mtl.dnslab.jp dnskey
  - ;; ANSWER SECTION:
  - slhdsasha2mtl.dnslab.jp. 3600 IN DNSKEY 257 3 130 X4yM9VV+0jaQ3uWCfLS0RuNDGy+pef+ruxim+nNapTg= (DNSKEYは小さい)
  - slhdsasha2mtl.dnslab.jp. 3600 IN RRSIG DNSKEY 130 略 (署名は巨大)
  - ;; MSG SIZE rcvd: 8384

Copyright © 2026 Japan Registry Services Co., Ltd.

MTL-modeの応答 (2)

- dig +norec +dnssec @xeon2.dnslab.jp slhdsasha2mtl.dnslab.jp SOA
  - ;; ANSWER SECTION:
  - slhdsasha2mtl.dnslab.jp. 3600 IN SOA xeon2.dnslab.jp. root.dnslab.jp. 1793865582 10800 1800 36000 900
  - slhdsasha2mtl.dnslab.jp. 3600 IN RRSIG SOA 130 3 3600 20261203075942 20261105075942 57941 slhdsasha2mtl.dnslab.jp. AQAAish2wj2rjXa…略 (巨大)
  - ;; MSG SIZE rcvd: 8383
- dig +norec +dnssec @xeon2.dnslab.jp zz.slhdsasha2mtl.dnslab.jp A (不存在)
  - ;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49063
  - ;; AUTHORITY SECTION:
  - z.slhdsasha2mtl.dnslab.jp. 900 IN NSEC slhdsasha2mtl.dnslab.jp. TXT RRSIG NSEC
  - z.slhdsasha2mtl.dnslab.jp. 900 IN RRSIG NSEC 略(小さい)
  - slhdsasha2mtl.dnslab.jp. 900 IN NSEC _dmarc.slhdsasha2mtl.dnslab.jp. A NS SOA RRSIG NSEC DNSKEY
  - slhdsasha2mtl.dnslab.jp. 900 IN RRSIG NSEC 130 略(小さい)
  - slhdsasha2mtl.dnslab.jp. 3600 IN SOA xeon2.dnslab.jp. root.dnslab.jp. 1793865582 10800 1800 36000 900
  - slhdsasha2mtl.dnslab.jp. 3600 IN RRSIG SOA 130 3 3600 20261203075942 20261105075942 57941 slhdsasha2mtl.dnslab.jp. AQAAish2wj2rjXa…略 (巨大)
  - ;; MSG SIZE rcvd: 8894

Copyright © 2026 Japan Registry Services Co., Ltd.

まとめ

- MLDSA44 にはアルゴリズム18が割り当てられ、BIND 9 (GitLab main)とVerisign版ldns、1.1.1.1が対応済
  - 署名がすこし大きく、必ずTCPになるだけ (2420バイト以上)
    - DNSKEY応答が、公開鍵(1312バイト)+署名で3734バイト以上に
    - NXDOMAIN応答が、SOA+NSEC*3+RRSIG*3で7400バイト以上に
  - DNSSEC検証を安全にできるのはBIND 9 と1.1.1.1
  - 発表申し込み時にはBIND 9の対応がまだだったので勧めにくかったが、11/3に対応、他の実装もすぐ対応するでしょう
- Merkle Treeを使った仕組みは、通常のRRの応答サイズはUDPに入るサイズだが、SOA, DNSKEY応答は超巨大(8kから10k)
  - NXDOMAIN応答がSOAのせいで太い (SOA+NSEC*2+RRSIG*3)
  - まだアルゴリズム番号が割り当てられていないので遊べない

Copyright © 2026 Japan Registry Services Co., Ltd.