KINDNSって親切？

2022年11月29日(火)

DNSOPS.JP幹事会 米谷嘉朗

そもそもKINDNSって何？

https://kindns.org

- **KINDNS** Stands for **K**nowledge-Sharing and **I**nstantiating **N**orms for **D**NS and **N**aming **S**ecurity.
- It’s a program supported by ICANN to develop and promote a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.

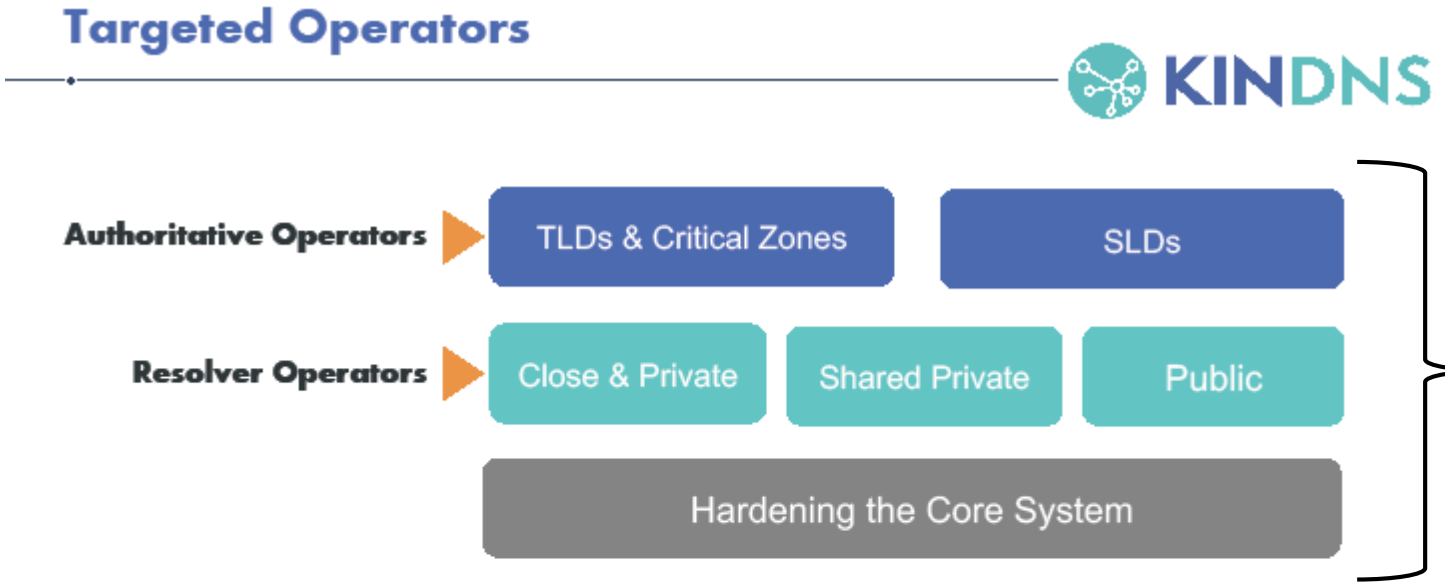
- KINDNSは知識共有と、DNSと名前の安全に関する規定の例示を表す言葉である
- 実態はICANNが支援するプログラムで、DNSセキュリティのベストプラクティスのうち、最も重要な運用に関するベストプラクティスや具体例に特化したフレームワークを開発・促進する場である

結局何をやってるの？

- DNS運用者向けのガイドラインを作成・公開しています
  - https://kindns.org/guidelines/
- DNS運用者が自分の運用を自己評価可能なチェックサイトを提供しています
  - https://kindns.org/self-assessment/

本日は前者の紹介をします
（後者は面白そうだと感じたら試してみてください）

DNS運用者向けガイドライン構成



出展：ICANN75 DNSSEC and Security Workshopプレゼン資料

- 権威サーバ運用者
  - ***TLDと重要ゾーン***
  - ***一般登録者ゾーン***
- リゾルバ運用者
  - ***非公開・組織内***
  - ***限定共有***
  - ***公開***
- ***基幹システム***

現在6種類
（*BoldItalic*のもの）
が公開済

権威:TLDと重要ゾーン
Critical Zones & TLD Operators

1. Practice 1: Authoritative zones **MUST** be DNSSEC signed and best practices for key management **MUST** be followed.
2. Practice 2: Access to zone transfer between authoritative servers **MUST** be limited. Configure ACLs and TSIG in the DNS Authoritative software package to restrict zone transfers to secondary servers only.
3. Practice 3: Zone file integrity **MUST** be controlled to avoid unexpected modifications (malicious or accidental).
4. Practice 4: Authoritative and recursive DNS service **MUST** NOT coexist on the same DNS server. In the context of authoritative servers, this means you **MUST** disable recursive DNS resolution on servers configured to serve authoritative DNS data (if the software allows running both authoritative and recursive at the same time).
5. Practice 5: At least two distinct nameservers **MUST** be used for any given zone. Note that this is usually a requirement when registering domain names in most TLDs (gTLD, ccTLD, …).
6. Practice 6: There **MUST** be diversity in the authoritative operations to promote resilience.
7. Practice 7: Monitoring of the services, servers, and network equipment that make up your DNS infrastructure **MUST** be implemented.

1. DNSSEC署名すること
2. ゾーン転送の許可はACLとTSIGで制限すること
3. ゾーンファイルの完全性を維持すること
4. 権威サーバとリゾルバを併用しないこと
5. 少なくとも2つの異なるネームサーバを使うこと
6. 回復力のため運用者には多様性を持たせること
7. DNSインフラを稼動させているサービス、サーバ、ネットワークの監視を実施すること

権威:一般登録者ゾーン
Other SLD Operators

1. Practice 1: Authoritative zones **MUST** be DNSSEC signed and best practices for key management **MUST** be followed.
2. Practice 2: Access to zone transfer between authoritative servers **MUST** be limited. Configure ACLs and TSIG in the DNS Authoritative software package to restrict zone transfers to secondary servers only.
3. Practice 3: Zone file integrity **MUST** be controlled to avoid unexpected modifications (malicious or accidental).
4. Practice 4: Authoritative and recursive DNS service **MUST** NOT coexist on the same DNS server. In the context of authoritative servers, this means you **MUST** disable recursive DNS resolution on servers configured to serve authoritative DNS data (if the software allows running both authoritative and recursive at the same time).
5. Practice 5: At least two distinct nameservers **MUST** be used for any given zone with diversity in operational and geographical practices in mind.
6. Practice 6: Monitoring of the services, servers, and network equipment that make up your DNS infrastructure **MUST** be implemented.

1. DNSSEC署名すること
2. ゾーン転送の許可はACLとTSIGで制限すること
3. ゾーンファイルの完全性を維持すること
4. 権威サーバとリゾルバを併用しないこと
5. 運用と地域的多様性を考慮して少なくとも2つの異なるネームサーバを使うこと
6. DNSインフラを稼動させているサービス、サーバ、ネットワークの監視を実施すること

リゾルバ:非公開・組織内
Private Resolver Operators

1. Practice 1: DNSSEC validation **MUST** be enabled for recursive resolvers.
2. Practice 2: ACL statements **MUST** be used to restrict who may send recursive queries to your DNS resolvers/validators.
3. Practice 3: QNAME minimization **MUST** be enabled to mitigate leakage of domain names.
4. Practice 4: Authoritative and recursive DNS service **MUST** NOT coexist on the same DNS server.
5. Practice 5: At least two distinct servers **MUST** be used for providing recursion services.
6. Practice 6: Monitoring of the services, servers, and network equipment that make up your DNS infrastructure **MUST** be implemented.

1. DNSSEC検証すること
2. ACLで利用者を制限すること
3. QNAME minimizationを有効にすること
4. 権威サーバとリゾルバを併用しないこと
5. 少なくとも2つの異なるリゾルバを使うこと
6. DNSインフラを稼動させているサービス、サーバ、ネットワークの監視を実施すること

リゾルバ:限定共有
Shared Private Resolver Operators

1. Practice 1: DNSSEC validation **MUST** be enabled for recursive resolvers.
2. Practice 2: ACL statements **MUST** be used to restrict who may send recursive queries to your DNS resolvers/validators.
3. Practice 3: QNAME minimization **MUST** be enabled to mitigate leakage of domain names.
4. Practice 4: Authoritative and recursive DNS service **MUST** NOT coexist on the same DNS server.
5. Practice 5: Your recursion services **MUST** have resilience by using at least two distinct servers that take diversity into consideration.
6. Practice 6: Monitoring of the services, servers, and network equipment that make up your DNS infrastructure **MUST** be implemented.
7. Practice 7 (Privacy consideration): DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **SHOULD** be enabled.

1. DNSSEC検証すること
2. ACLで利用者を制限すること
3. QNAME minimizationを有効にすること
4. 権威サーバとリゾルバを併用しないこと
5. 回復力のため多様性を考慮し少なくとも2つの異なるリゾルバを使うこと
6. DNSインフラを稼動させているサービス、サーバ、ネットワークの監視を実施すること
7. DoTやDoHも可能な限り有効にすること

リゾルバ:公開
Public Resolver Operators

1. Practice 1: DNSSEC validation **MUST** be enabled for recursive resolvers.
2. Practice 2 (Privacy Consideration): QNAME minimization **MUST** be enabled to mitigate leakage of domain names.
3. Practice 3 (Privacy Consideration): DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **SHOULD** be enabled.
4. Practice 4: Authoritative and recursive DNS service **MUST** NOT coexist on the same DNS server.
5. Practice 5: Data collected through passive logging of DNS queries **MUST** only be retained for as long as is necessary for the sound operation of the service offered, including troubleshooting, research, and satisfying local legal requirements on data retention.
6. Practice 6: Your recursion services **MUST** have resilience by using at least two distinct servers that take diversity into consideration.
7. Practice 7: Monitoring of the services, servers, and network equipment that make up your DNS infrastructure **MUST** be implemented.

1. DNSSEC検証すること
2. QNAME minimizationを有効にすること
3. DoTやDoHも可能な限り有効にすること
4. 権威サーバとリゾルバを併用しないこと
5. DNSクエリログの収集は健全な運用に必要なものに限定し、地域の法律が許容する範囲内とすること
6. 回復力のため多様性を考慮し少なくとも2つの異なるリゾルバを使うこと
7. DNSインフラを稼動させているサービス、サーバ、ネットワークの監視を実施すること

基幹システム
Core Platform/System Hardening

1. Practice 1: ACLs **MUST** be implemented to restrict network traffic to your DNS servers.
2. Practice 2: BCP38 egress filtering **MUST** be implemented so that no network traffic can leave your network with a source IP address that is not assigned to you or your customers.
3. Practice 3: The configuration of each DNS server **MUST** be locked down.
4. Practice 4: User permissions and application access to system resources **MUST** be limited. File permissions and ownership restrictions **MUST** be set so that users and services not directly associated with management of the DNS subsystem do not have read or write access to DNS service configuration, data files, and database subsystems.
5. Practice 5: System and service configuration files **MUST** be versioned. For authoritative operators, zone files/data **MUST** also be versioned.
6. Practice 6: Access to management services (e.g., SSH, web-based configuration tools) **MUST** be restricted. All services not needed for DNS or management **MUST** be disabled or uninstalled if possible, otherwise network access to the unnecessary services **MUST** be blocked.
7. Practice 7: Access to the system console **MUST** be secured using cryptographic keys, protected with a passphrase (e.g. SSH keys) or using suitable two-factor authentication (OTP generator or token-based).
8. Practice 8: Credentials for customer access (registrants and other domain contacts) **MUST** follow sound credential management practices, including offering two-factor authentication as an option.

1. DNSサーバへのトラフィックを制限するためACLを導入すること
2. ソースIPアドレス詐称を防ぐためBCP38を導入すること
3. 権威・リゾルバともにDNSサーバ構成は厳重封鎖すること
4. ファイルオーナ・ユーザアクセス権限とシステムリソースへのアプリケーションアクセスは制限すること
5. DNSクエリログの収集は運用に必要なものに限定し、地域の法律が許容する範囲内とすること
6. 管理サービス（コンソール）へのアクセスは制限すること、DNSサービスに不要なサービスは停止するかネットワークで制限すること
7. システムコンソールへのアクセスは暗号鍵や多要素認証で保護すること
8. 顧客のアカウント情報は健全な管理原則に基づいて管理し必要に応じて多要素認証を用いること

かなりMUSTって言ってるけど…

- インターネットにおけるBCP(Best Current Practice)、BCOP(Best Current Operational Practice)を含むベストプラクティス(Best Practice)って何かを考えてみましょう
- 世の中で広く行われている慣例・慣習の最大公約数を集めた結果ではなく、多くの人が守ることで世の中がよりよくなる慣例・慣習を厳選したものです
- インターネットの安定運用を目的としています
- 守らない合理的な理由がない限りは守りましょう
  - 合理的な理由がある場合はちゃんと表明し、ベストプラクティスを変えていきましょう

KINDNSって親切？

- 現時点では、現場の運用者にはちょっと厳しいかもしれません
- 改善のために管理者を説得する素材にはなります
  - 現状とのギャップを示すことができます
- その結果、改善されればインターネットユーザにとって「親切」になります

私個人の私的解釈です

（みなさんそれぞれによい意味でKINDNSを解釈してください）