ICANN の技術政策情報に関する報告

JPNIC 大谷 亘 <alt@nic.ad.jp>

2025/07/31 第 73 回 ICANN 報告会

一般社団法人 日本ネットワークインフォメーションセンター

直近半年の動向 1

- OCTO
  - OCTO-041 A Verifiable and Reproducible Random Candidate Selection Process (2025/02/25)
- RSSAC
  - RSSAC061 Guidelines for Changing IP Addresses (2025/03/27)
  - RSSAC062 Security Incident Reporting (2025/05/06)

直近半年の動向 2

- SSAC
  - SAC127 DNS Blocking Revisited (2025/05/16)
  - SAC128 SSAC Comments on Draft Governance Document for the Recognition, Maintenance, and Derecognition of RIRs (2025/06/04)
  - SAC129 SSAC Comments on GNSO Domain Name Registration Data Accuracy Concept Proposal (2025/07/07)
  - SAC130 SSAC Comments on Name Collision Guidelines in the Proposed Language for the Draft Next Round Applicant Guidebook (2025/07/22)

RSSAC062 Security Incident Reporting

RSS のセキュリティインシデント報告について

はじめに

- Root Server System（RSS）は DNS インフラの中核.
- RSSAC062 は RSS GS に対し, Criterion A.1.1.1 実装後のセキュリティインシデント報告方法を提言.
- RSOs（Root Server Operators）と RSS GS の連携強化が狙い.

セキュリティインシデント報告の目的

- RSS に影響を及ぼすセキュリティインシデント情報を **透明化**.
- 信頼性・安定性への不安を軽減し, コミュニティの **自信を醸成**.
- 既存の非公式報告から **正式プロセス** への移行を支援.

用語定義

- Availability: 情報への適時・確実なアクセス保証.
- Data Integrity: ルートゾーンデータの「正確性」保持.
- Operational Integrity: 運用プロセスや制御の適切性.
- Confidentiality: DNS ログ等の機微情報保護.
- Security Incident: RSS の可用性, 機密性, 完全性を脅かす事象.

報告対象インシデントの種類

1. Availability
    - 広域的なサービス停止や解決不能な障害.
2. Data Integrity
    - 不正確なルートゾーンデータの配信.
3. Operational Integrity
    - ミスコンフィグ, 脆弱性悪用など.
4. Confidentiality
    - 暗号鍵漏洩, 未匿名化ログ公開など.

報告の基準

- Reportable: RSS 全体に重大影響を与える事象.
- Non-Reportable: ローカル・小規模で RSS 全体影響なし.
- RSO は重大・非重大を評価し, 重大なら RSS GS へ報告義務.

報告タイミングと方法

- タイミング: 可能な限り早期に, 情報不完全でも報告可.
- 方法例:
  - メール
  - Web サイト経由フォーム
- 認証・機密保持を確保する仕組み（TLP）を推奨.

レポートに含む情報

1. 関連 RSO 名
2. インシデントのタイムライン
3. 概要（影響範囲, 原因, 対策案）
4. 詳細（TLP 指定付き, フォレンジック手順, 調整記録）
5. 今後のフォローアップ計画

RSS GS によるプロセス支援

- ガイドライン提供: テンプレート, 報告期限, 評価手順
- 調整チャネル: メーリングリスト, チャット, 電話会議
- 公開支援: `TLP:Clear` 版公開, アーカイブ公開 Web サーバ
- 改善サイクル: フィードバック基づくプロセス改良

勧告

1. RSS GS は本助言を初期要件として採用・検討.
2. 継続的改善のため, 実運用後のレビュー・更新を実施.
3. RSOs 同士, および RSS GS とのコミュニケーション体制を強化.

SAC127 DNS Blocking Revisited

DNS ブロッキングに関する再考

JPNIC Blog でも解説しています.

はじめに

- DNS ブロッキングとは, DNS クエリへの応答を改変・遮断し, 特定のドメインへのアクセスを制限する手法.
- 簡易実装が可能な一方で, **副作用や回避可能性** が存在する.

DNS ブロッキングの動機と事例

1. セキュリティ保護: マルウェア/フィッシングサイトのブロック（Reputation Blocklists）
2. 組織内アクセス制御: 学校・企業での業務外サイト制限
3. **法的・政治的理由**：検閲や裁判所命令による強制ブロック（中国の「Great Firewall」, スイス賭博サイト規制など）

原則と前提

- 有効性は限定的: VPN, DoX, パブリックリゾルバで容易に回避可能
- 副作用: overblocking, 巻き添え被害, ユーザの混乱
- Primum non nocere: 意図しない影響を最小化する実装・ポリシ策定が必須

実装手法 1: フルリゾルバでのブロッキング

- NXDOMAIN 応答: 存在しないと偽装
- リダイレクト: ブロックページへ誘導
- Silent Drop: 応答を返さない
- On the Wire Inspection: パケット受信後に偽応答生成

実装手法 2: 公式サーバでのドメイン停止

- Domain Suspension: レジストリ/レジストラによるゾーンファイルからの削除
- ServerHold/ClientHold: ステータス変更で全ユーザに影響
- 法的押収: FBI による `cracked.io` ドメイン名押収事例

検出と回避手段

- パブリックリゾルバ（Google 8.8.8.8, Cloudflare 1.1.1.1）
- VPN: 全トラフィック暗号化しブロック回避
- Tor/Snowflake: 多段ルーティングで匿名・回避
- IPFS: 分散ホスティングで耐検閲性向上

暗号化DNS（DoX）

- DoH（DNS over HTTPS）: HTTPS 上で DNS 通信
- DoT（DNS over TLS）: TLS トンネルによる暗号化
- DoQ（DNS over QUIC）: QUIC プロトコルで高速・暗号化
- ネットワーク管理者による DPI がないと検知困難

パブリックリゾルバとトレンド

- Public Resolvers の隆盛: 2024 年末で約 21％ が利用（APNIC Labs）
- DNS4EU: EU が推進するプライバシ対応パブリック DNS
- PDNS（UK NCSC）: 政府機関向け保護 DNS, 年間 810 B クエリ処理

拡張 DNS エラー（EDE）

- RFC 8914：Extended DNS Errors
- エラーコード 16 ”Censored”：意図的ブロックを明示
- 透明性向上と overblocking 抑制に寄与

勧告

1. 実装者は **ブロック技術の意味を十分理解**
2. 明確な **ポリシとレビュー体制** の構築
3. **overblocking・巻き添え被害** の最小化
4. **管轄外への影響** の排除
5. 透過性確保のため **EDE 利用**

ICANN の技術政策情報に関する報告

JPNIC 大谷 亘 <alt@nic.ad.jp>

2025/07/31 第 73 回 ICANN 報告会

一般社団法人 日本ネットワークインフォメーションセンター

