

# gTLD動向

## ～GDPR対応はRDAPで～

Kentaro Mori, JPRS  
<kentaro@jprs.co.jp>  
DNS Summer Day 2018

# Contents

- WHOISとは
- WHOISの問題点
- RDAPとは
- GDPRとその要求
- RDAPによるGDPR要求への対応
- 現状と今後の流れ

# WHOISとは

(as you may know)

- 各TLD (Top Level Domain) が、ドメイン名に関する以下の情報を提供するquery/responseベースのサービス
  - 登録者 (Registrant)
  - 連絡先 (Admin Contact、Tech Contact、Billing Contact)
  - 管理レジストラ (レジストリWHOISのみ)
  - ネームサーバー設定 (*i.e.* ゾーンカットのNSレコード)
  - ドメイン属性情報 (登録日、状態、*etc.*)
- 概ね2通りのI/Fがある
  - コマンドラインベース (Port 43/tcp)
  - Webベース (Port 80/tcp、Port 443/tcpなど)

# WHOISの問題点

従来よりWHOISが内包する下記のような問題点が指摘されてきた

P1	入出力の標準フォーマットがない
P2	国際化対応(ドメイン名含む)されていない
P3	ユーザー認証に基づくアクセスコントロール (“tiered access”)機能がない
P4	サーバー発見機能(Where to ask?)がない
P5	サーバー認証機能がない(Port 43/80)
P6	通信路の暗号化機能がない(Port 43/80)

VERISIGN

Your search for verisign.com returns the below results:

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

Domain Name: VERISIGN.COM  
 Registrar: CSC CORPORATE DOMAINS, INC.  
 Sponsoring Registrar IANA ID: 299  
 :

WHOIS Search Results for Domain Name: PIR.NGO

Domain ID: D175569199-LROR  
 WHOIS Server:  
 Referral URL: www.pir.org  
 Updated Date: 2016-03-11T01:32:45Z  
 Creation Date: 2015-03-10T15:22:43Z  
 Registry Expiry Date: 2017-03-10T15:22:43Z  
 Sponsoring Registrar: Public Interest Registry  
 Sponsoring Registrar IANA ID: 9998  
 :

JPRS

Domain Name: JPRS.INFO  
 Registry Domain ID: D586220-LRMS  
 Registrar WHOIS Server: whois.jp  
 Registrar URL: https://jprs.jp/registrar/  
 Updated Date: 2015-09-14T17:01:32Z  
 Creation Date: 2001-09-15T17:48:26Z  
 Registrar Registration Expiration Date: 2016-09-15T17:48:26Z  
 Registrar: Japan Registry Services Co.,Ltd.(JPRS)  
 :

※イメージです

# RDAPとは(1/3)

- Registration Data Access Protocol
  - WHOISやRDAPを総称してRDS(Registration Directory Service)という
- WHOISの問題点を解決するためにIETF/ICANNにおいて検討されてきた  
プロトコル・サービス
  - “Port 43” WHOISを置き換える目的で設計されたという位置づけ
- 以下により仕様が定義される
  - RFC 7480～7484 (プロトコル仕様 by IETF)
  - gTLD RDAP Profile (実装規定 by ICANN)  
<https://www.icann.org/resources/pages/rdap-operational-profile-2016-07-26-en>
- 余談: 黒歴史
  - IETFとICANNの連携が曖昧なままRDAP以前に設計されたプロトコルCRISP(IRIS)が、  
実サービスにおいて殆ど採用されないままお蔵入りになった経緯あり

# RDAPとは(2/3)

仕様・機能	解決する 問題点
表示項目を統一的に定義、 RESTによる入力、JSONによる出力	P1
文字コードをUTF-8に統一、表示項目にIDNを導入	P2
クライアント証明書(PKI) and/or OpenID Connect による ユーザー認証*とアクセスコントロール** (※設計中)	P3
IANAリポジトリ登録情報を元にしたサーバー発見	P4
HTTPSによる通信	P5、P6

\* Authentication(認証)はIETF、\*\* Authorization(認可)はICANNが設計

# RDAPとは(3/3)

## 〔入出力の例〕

①REST (Representational State Transfer)による入力    ②JSON (JavaScript Object Notation)による出力

(a)ドメイン名情報の検索

`https://rdap.example/rdap/  
domain/dom1.example`

情報種別の指定    検索対象ドメイン名  
(ドメイン名情報)



```
{
  "objectClassName": "domain",
  "ldhName": "dom1.example",
  "status": [ "locked", "transfer prohibited" ],
  "nameservers":
  [
```

(b)ホスト情報の検索

`https://rdap.example/rdap/  
nameserver/ns1.dom1.example`

情報種別の指定    検索対象ホスト名  
(ホスト情報)



```
{
  "objectClassName": "nameserver",
  "ldhName": "ns1.dom1.example",
  "ipAddresses":
  {
    "v4": [ "192.0.2.1", "192.0.2.2" ],
    .....
  }
}
```

※イメージです

# GDPRとその要求(1/2)

- 2018/5/25から、EUエリアにおける新たな個人情報保護方針となるGDPR (General Data Protection Regulation) が施行された
- 概ね以下のような方針

① EUエリアで生成・処理(データ加工、転送、表示、その他)される個人情報に適用される

- 本人の明示的な同意がない個人情報を公開してはいけない
- 違反者には罰則(制裁金を含む)が適用される
- WHOISも例外でない(EUエリアのレジストリ・レジストラのWHOISに適用される)

② EUエリア外で生成・処理される個人情報にも条件次第で適用される  
(「域外適用」という)

- EUエリア外TLDのWHOISもEUエリア所在の個人情報が含まれていれば対象となる?
- 域外適用の解釈が一定せず、事例の蓄積待ちといえる状況



# GDPRとその要求 (2/2)

- ICANNは、gTLD WHOISをGDPR準拠とするため“Temporary Specification for gTLD Registration Data”を公表、gTLDにおける準拠を義務付けた (<https://www.icann.org/en/system/files/files/advisory-statement-gtld-registration-data-specs-17may18-en.pdf>)
- Temporary Spec.の骨子

EUエリア及び域外適用されるgTLDは、WHOISの個人情報(Registrant、Admin Contact、Tech Contact)の所定項目を非公開にする

EUエリア及び域外適用されるgTLD(レジストラ)は、非公開にした個人情報のE-mailアドレスに匿名のままコンタクトできるサービスを何とかして提供する

全てのgTLDは、7月末までに公開されるgTLD RDAP Profile(改訂版)に従い、RDAPサービスを開始する(2018/12～)

# RDAPによるGDPR要求への対応

- ICANNは、インターネットの安定運用のため、WHOIS(RDS)情報は原則公開するという立場
- が、GDPRによって個人情報(ドメイン名の連絡先)を非公開とする状況が発生する



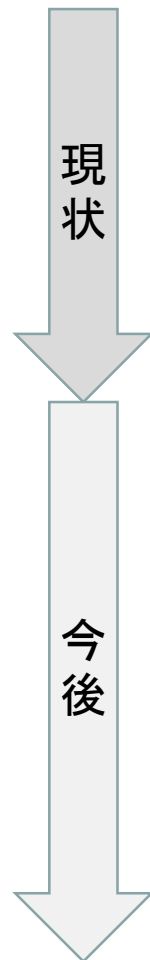
- RDAPの“tiered access”機能を用いれば、正当な権利(“legitimate interest”)を持つユーザーには、非公開にした個人情報を開示できる



- gTLD提供サービスにおいてRDAPを採用することにより、ICANNは情報公開に関するRDSとGDPRの相反する要件を両立する

# 現状と今後の流れ

時期	主体	イベント
2015/03	IETF	RDAP関連RFCの発行
2016/07/26	ICANN	gTLD RDAP Profileの公表
2018/05/18	ICANN	Temporary Spec.の公表と、gTLD(レジストリ・レジストラ)への準拠要求
2018/05/25	EU	GDPRの施行開始
2018/07/末まで	ICANN	gTLD RDAP Profile改訂版の公表
2018/12/中ごろ	gTLD	Profile改訂版に準拠したgTLD RDAPサービスの開始
(時期未定)	IETF/ICANN	“tiered access”方式(PKI and/or OpenID)の決定
(時期未定)	ICANN	“legitimate interest”を有するユーザー種別の定義(＋定義されたユーザー種別に対応するIDの定義)
(時期未定)	gTLD	RDAPにおける“tiered access”の提供開始
(時期未定)	gTLD	WHOIS(Port 43)のサービス終了



※予定は変更される可能性があります

## (まとめ)

- かねてよりWHOISの問題点が認識されてきた
- WHOISの問題点を解決するため、ICANNとIETFは、過去の失敗を糧に連携を強化しながらRDAPを設計している
- GDPR施行を機に、gTLDでは、非公開情報に対しRDAPを用いた“tiered access”を実現しようという流れになってきた
- 想定通りに推移すれば、gTLDのPort 43 WHOISは将来RDAPに置き換えられることになる

jPRS  
JAPAN REGISTRY SERVICES