インターネット10分講座

SSAD (System for Standardized Access Disclosure)とは

1 はじめに

2020年7月31日(金)、ICANN (The Internet Corporation for Assigned Names and Numbers)の分野別ドメイン名支持組織(Generic Names Supporting Organization, GNSO)内で検討が進んできた、「gTLD登録データの暫定仕様書第2フェーズ迅速ポリシー策定プロセス(the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process)」に関する、最終報告書が公開されました。

Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process
https://gnso.icann.org/en/correspondence/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

これは、2018年5月25日に欧州連合(EU)で発効となった一般データ保護規則(General Data Protection Regulation, GDPR)に準拠するためにICANN理事会が制定した、gTLD登録データに関する「暫定仕様書」に対して、後追いでGNSOにおけるポリシー策定を行うために実施された迅速ポリシー策定プロセス(Expedited Policy Development Process, EPDP)の成果です。2019年2月に提出されたフェーズ1報告書に引き続き、残項目の検討結果として公表され、議論を経て、2020年9月24日にGNSO評議会で承認されています。

暫定仕様書とEPDPに関しては、以下をご参照ください。

ICANNがEUのGDPRに準拠したgTLD登録データのための暫定仕様書を承認
https://www.nic.ad.jp/ja/topics/2018/20180521-02.html

インターネット用語1分解説(EPDPとは)
https://www.nic.ad.jp/ja/basics/terms/epdp.html

本稿では、このフェーズ2最終報告書の主な要素である、SSAD (System for Standardized Access Disclosure)の仕組みをご紹介したいと思います。SSADは、WHOISサービス(近年WHOISは「登録ディレクトリサービス」(Registration Directory Service, RDS)と呼ばれつつありますので、以下、この呼び方で統一します)で非開示となっているデータの提供を司る機構です。

2 GDPRと登録者情報開示の関係

インターネットではその黎明期から、IPアドレスやドメイン名などのインターネット資源が、誰によって保持されているかを明らかにするために、RDSと呼ばれるサービスで、インターネット資源のレジストリが資源と保持者の対応を明らかにし、開示してきました。一方でGDPRは、個人情報(個人データ)の不適切な利用を制限する規則で、個人データの利用は、データ主体の同意の下、正当な目的(legitimate interest)のために限られるとされています。インターネット資源の保有者に関する情報を、インターネットの運営のために開示しようとするのがRDS、個人情報保護のため非開示にしようとするのがGDPRと、それぞれの達成しようとしていることが正反対ということになります。

GDPRにおいては、個人データがRDS上で誰にでも提供されている状態は、正当な目的に沿っているとは考えにくいため、データの開示を、RDSの参照利用者の目的に従って制限することが必要となりました。つまり、一般的な参照利用者には、最低限の情報を開示するに留めてそれ以外の情報を非開示とするとともに、犯罪捜査、ドメイン名に関する知的財産権の紛争処理、サイバーセキュリティに関する調査など業務上必要な場合、つまり正当な目的があると認められる場合にだけ、一般に公開している以上の情報を開示する、ということです。

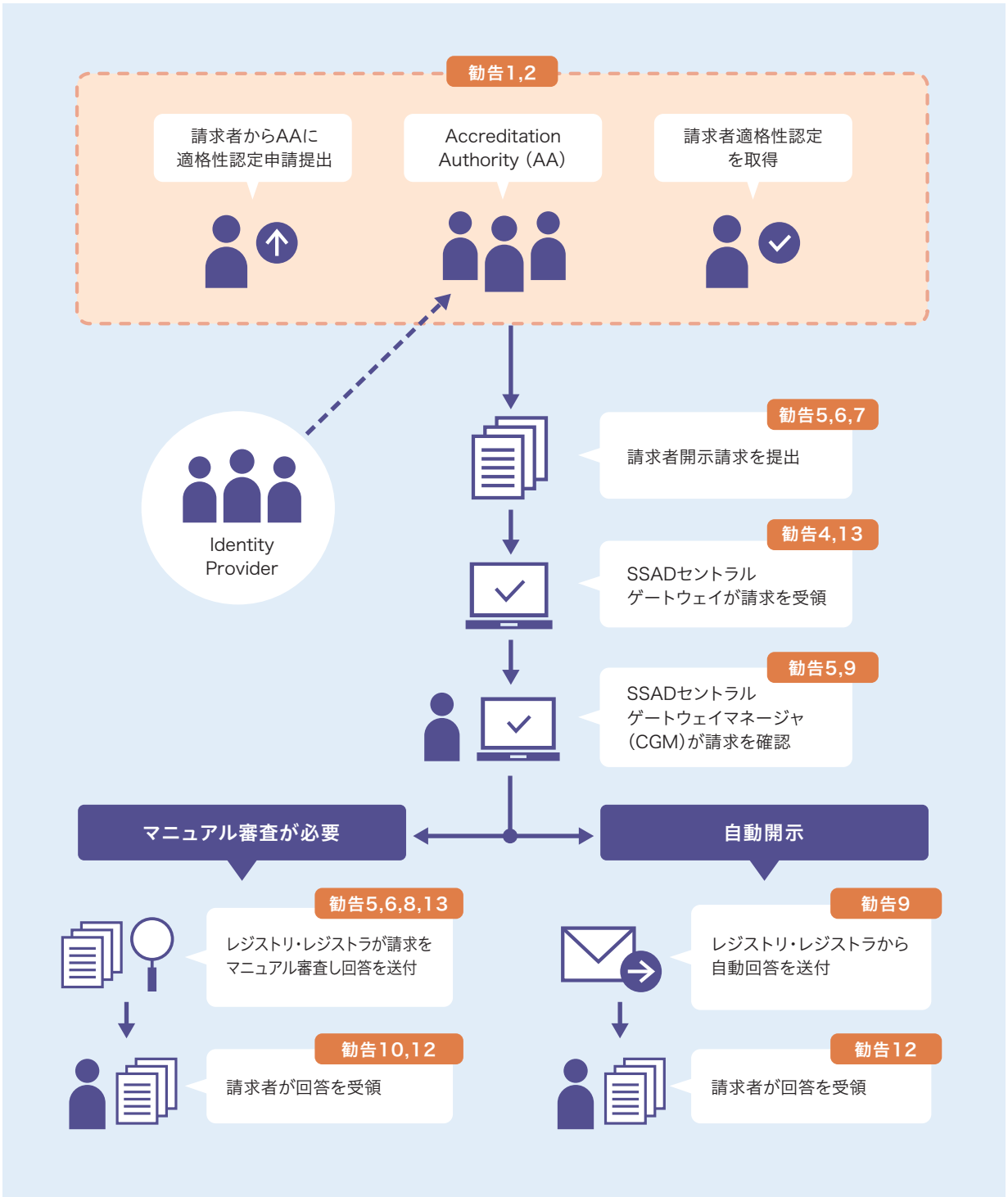
暫定仕様書では、GDPRへの迅速な準拠を第一としたため、個人

情報に当たる可能性が高い項目は非開示とした上で、レジストリに個別の開示対応を求めました。しかし、個別対応はタイムリーに処理できるものではないため、実質的に、従来であれば開示されていた情報が大幅に伏せられた状態での運用が続いています。

SSADは、RDS上で非開示となっている個人データに関して、参照利用者の資格に応じた情報開示を可能にすることで、開示を正当化するという目的があります。

3 SSADの設計

EPDPフェーズ2最終報告書では、18の勧告（recommendations）にわたってこのSSADの仕様が記述してあります。SSADの全体概要を、図に示します。



SSADによる非開示情報の開示プロセスを、順を追って見ていきます。

a) Accreditation（適格性認定）

SSADを通じて非開示情報の開示を受けるために、要求者（SSAD利用者）の本人性と利用目的の確認を行うもので、Accreditation Authority（AA）がこのプロセスを実施します。AAはICANN事務局の責任の下運営されますが、実際の運用は第三者に委託される可能性があります。また、本人性確認のために第三者のIdentity Providerの協力を得ることもできることになっています。

最終報告書の勧告1が、このプロセスを勧告しています。SSAD全体のうち、適格性の認定は重要な要素ですので、細かく見ていきます。

AAはSSAD利用者の適格性認定に関して、以下の項目を含むポリシーをあらかじめ策定して公開することとしています。（Recommendation 1.3.）

1.3.1. 適格性認定の申請はそれを求める法人・個人に広く門戸を開き、適格性認定を受けた法人・個人のみから開示請求を受け付けること。継続的利用者、一時的利用者の認定には違う条件を設け得ること
1.3.2. 法人も個人も適格性認定の対象であること。法人の信憑によりSSADを利用する個人は法人の権限による利用であることを保証すること
1.3.3. 本人性信憑（Identity Credential, IC）と署名された利用目的記述（Signed Assertion, SA）の検証、発行、継続的管理に責任を持つ単一のAAを、ICANN事務局の管理の下規定すること。AAはプライバシーポリシーを規定し、個人データの処理と取り扱いに責任を持つこと。IC, SAの検証を受け持つIdentity Providerを外部委託することができること
1.3.4. 検証されたIC, SA、申請内容から公開を決定するのは、Central Gateway Managerあるいはレジストリ・レジストラに委ねられる

ここで1.3.3.に現れるSAは、請求者によって主張される以下の内容を含むものです。（Recommendation 1.4.2.）

a） 請求の目的
b） 請求の法的根拠
c） ICによって同定された利用者が請求に関係する団体に所属すること
d） 遵法性
e） 開示されたデータの正当で遵法的な目的による利用であること
f） 保護機構および利用規約の遵守と、違反時の認定取り消しの了承
g） 不正利用防止、監査、紛争処理、苦情申立プロセスへの了承
h） 商標権、商標登録など請求者固有の主張
i） 委任状に関する表明

ICによる本人確認、SAによる請求者の利用目的記述を元に、AAは以下の業務を行います。（Recommendation 1.4.）

1.4.1. 本人確認
1.4.2. SAの管理
1.4.3. ICとSAの確認とSSAD請求受諾判断の支援
1.4.4. データ保護関連法令群に準拠した基本的行動規範の規定
1.4.5. プライバシーポリシーの策定
1.4.6. 申請条件などを明確にした基本的申請手順の策定
1.4.7. 紛争処理方針の規定
1.4.8. 定期的監査の実施
1.4.9. 認定プロセス促進のための利用者グループ設置（任意）
1.4.10. 統計情報などの定期報告の作成と公開
1.4.11. 適格性認定の更新要件の確立
1.4.12. 利用者データの確認、アップデートの促進

ここまで細かく勧告の規定を見てきましたが、開示請求者の身元と主張している開示情報利用目的を明確にすることと、その業務が適正、円滑に運営されることを担保しようとしていることが分かると思います。

この他、最終報告書勧告2では、特に政府関連機関に対する適格性認定について定めており、各国政府またはその指定機関が、法執行機関、データ保護当局、消費者保護、サイバーセキュリティ関連機関などの適格性認定を行えるとしています。

開示請求者は適格性認定を受けた後、非開示情報開示請求（Disclosure Request）を提出することができます。

---

b) 開示請求

開示請求は、以下をはじめとする情報を添えて（Recommendation 3.2）、Central Gatewayと呼ばれるシステムに提出されます。

3.2.1. 対象ドメイン名
3.2.2. 請求者本人に関する情報とSA
3.2.3. 当該請求に関する請求者の法的権利、正当な目的あるいは他の法律上の権利
3.2.4. 請求が誠実に行われ開示データが目的内のみで遵法的に利用されることの確認
3.2.5. 請求されるデータ要素のリストと、それらが請求目的のために必要な理由
3.2.6. 請求種別（緊急性、優先度、機密性）

このうち優先度に関しては、三つのレベルが想定されています。(Recommendation 6)

プライオリティ1：緊急
深刻な身体被害、重要インフラへの脅威、児童搾取への脅威など

プライオリティ2：ICANN管理手続き
「統一ドメイン名紛争処理方針(Uniform Domain Name Dispute Resolution Policy, UDRP)」や「統一早期凍結(Uniform Rapid Suspension, URS)」など、ICANNとの契約あるいはポリシーによる要請に基づくもの

プライオリティ3：その他
但しフィッシング、マルウェア、詐欺などの消費者保護に関わる請求は請求者が明示することで、レジストリ・レジストラでの優先処理を可能にするべき、としている。

開示請求のハンドリングを担当するCentral Gateway Manager (CGM)は、開示請求の外形的要件(必須項目が記入されているか、など)を確認した上で、レジストリ・レジストラへの転送の準備を行うとともに、請求者に受領通知を送ります。

CGMは開示請求のハンドリングに当たって、システム監視と異常利用対応、複数請求の同時受付、履歴保持などが課せられています。

---

c) 開示請求の転送
レジストリ・レジストラにおける開示請求の処理には、自動開示処理とマニュアル処理の2通りがあります。請求が自動開示の条件に適合する場合には自動開示となり迅速に処理されますが、適合しない場合にはレジストリ・レジストラで個別の内容確認が行われます。

自動開示の条件は最終報告書の勧告9に示してありますが、法執行当局からの請求など限定的であるため、大半の開示請求はマニュアル処理になるだろうと考えられています。

---

d) レジストリ・レジストラにおける開示処理
マニュアル処理による開示可否の検討においては、請求されたデータ要素が、結果的に個人データを含まない場合など、判断が簡単なケースはあるものの、請求されたデータ要素に個人情報が含まれる場合には、登録者と請求者の利益の衡量をはじめとした検討の結果に基づく開示・非開示の判断は、レジストリ・レジストラに委ねられています。

今後

GDPRが要請する個人データの保護という問題に対して、その開示が必要な条件を目的別に明確にして、正当な目的がある場合に限って開示するという形で答えようとしているのが、このSSADです。現在GNSO評議会の議決が完了し、今後ICANN理事会で承認に向けた検討が進みます。

1,000以上に上るgTLDレジストリに対して統一的な機構を提供するために、ICANN事務局の責任下で運営されるAccreditation AuthorityとCentral Gateway Managerで開示請求を受け付け、各レジストリ・レジストラに請求を転送するという形を採っています。しかしこれによって対処されるのは、開示請求者の資格や目的の確認までであり、この開示請求を受け入れて情報を公開するべきかの判断は、レジストリ・レジストラに委ねられている状態です。自動化による効率化、迅速化にはまだまだいろいろな検討の必要があるように思われます。
報告書はGNSO評議会で承認されていますが、その一方で少数意見の表明として制度化されている少数意見表明書(Minority Report)は、GNSO内のステークホルダーグループ、部会だけでなく、諮問委員会(Advisory Committee,AC)からも寄せられています。その中では、上に述べた中央一括処理による迅速性や一貫性の欠如、この機構の構築コストに関する懸念なども目立っています。

GNSO評議会の承認を得ているという意味で、ポリシーとしては固まっているSSADですが、情報提供と情報保護の相反する二つの要請のバランスを取りながら、有効に機能するための仕組みとなっていくためには、今後の実装に向けた取り組みが非常に重要だと言えます。

(JPNIC インターネット推進部 前村昌紀／藏増明日香)