일반도메인 디렉토리서비스에 관한 전문가 실무그룹(EWG)의 최종보고서: 차세대 등록정보디렉토리서비스(RDS)

본 문서의 상태

본 문서는 일반도메인 디렉토리서비스에 관한 전문가 실무그룹(EWG)의 최종보고서로 현행 WHOIS 시스템을 대체할 차세대 등록정보 디렉토리서비스(RDS)와 관련해 ICANN 이사회에 제안할 EWG 의 권고안을 포함하고 있다.

2페이지

전문가 실무그룹 최종 보고서 날짜: 2014년 6월 6일

4 페이지

I. 개요

본 문서는 일반도메인 디렉토리서비스에 관한 전문가 실무그룹(EWG)의 최종보고서로 현행 WHOIS 시스템을 대체할 차세대 등록정보 디렉토리서비스(RDS)와 관련해 ICANN 의장/CEO 및 이사회에 제안할 EWG 의 권고안을 설명하고 있다.

본 최종보고서는 15개월이 넘는 기간에 걸친 강도 높은 연구 조사 작업의 결과물로 다양한 자원활동가들로 이루어진 EWG가 수 많은 시간을 할애해 심도 깊은 조사를 실시하고, 2,600 페이지가 넘는 일반의 의견과 설문조사 응답 및 조사 결과를 검토했으며, 19차례의 공개 커뮤니티 협의에 참여하고, 35일간의 회의와 42차례의 EWG 통화, 200건이 넘는 전화회의와 외부 전문가 및 커뮤니티 회원들과의 무수한 의견 수렴을 위한 회의를 가졌다. 그리고 이 모든 수고와 노력은 다음과 같은 매우 간단한 질문에 대한 답변을 얻기 위해서였다.

현재의 WHOIS 보다 세계 인터넷 공동체에 더 나은 서비스를 제공할 대안이 있는가?

결론적으로 말하자면 '있다'이다. EWG는 모든 사용자에게 동일하게 일반도메인 등록정보 데이터(종종 정확하지도 않은)에 대한 익명의 접근을 허용하는 현행 WHOIS 모델의 폐지를 만장일치로 권고하는 바이다.

대신 EWG는 허용 가능한 특정 목적에 한해 일반도메인 등록정보를 수집, 인증 및 공개하는 차세대 RDS로 전환할 것을 권고한다.

기본적인 정보는 계속 일반 공개로 두고 나머지 정보는 신원이 확인되고 수집 및 사용 목적을 밝히고 적절한 사용을 책임지기로 동의한 인증된 요청자에 한해 접근을 허용한다.

150 페이지가 넘는 본 문서의 나머지 부분에서는 EWG가 본 권고안을 도출하기까지의 과정을 설명하고 차세대 RDS를 위한 세부적인 제안과 다음과 같은 결론을 제시한다.

- 이 사안은 매우 복잡하다.
- EWG는 이 사안을 다각도로 조사했으며 새 RDS의 실행가능성을 확인하기 위한 연구 조사를 실시했다.
- (EWG가) 제안한 RDS가 완벽한 것은 아니지만, 따로 분리해서 고려해서는 안 될 다음과 같은 상호의존적 요소들을 고려 하여 균형점을 찾고자 했다.
    - 어려운 정보 프라이버시 문제
    - 오랫동안 정보 품질과 정확성을 하락시켜 온 검증(validation) 문제

6페이지

- 접근성과 책임성 사이의 균형 문제

• RDS는 하나의 전체로 도입되어야 한다. 본 보고서에서 권고한 설계 원칙의 일부만 채택할 경우 전체 생태계에 가져올 수 있는 효과가 반감된다.

차세대 RDS를 위한 권고와 원칙들을 설명한 본 보고서는 합의를 통해 얻어진 산물이다. EWG 구성원들의 다양한 시각과 이해관계를 고려할 때 이러한 전폭적인 지지는 특기할만하다.[1]

EWG 는 본 보고서가, 일반도메인 등록정보의 사용목적과 제공을 재정의함으로써 ICANN 커뮤니티가 (일반도메인정책개발기구[GNSO]를 통해) 일반도메인 디렉토리서비스를 위한 새로운 정책 수립을 지원할 확고한 토대를 제공하고자 하는 ICANN 이사회의 방침에 부합하리라 확신한다.

또한 EWG는 본 보고서에서 설명하는 RDS가 기존에 비해 좀 더 확고한 토대, 즉 일반도메인정책개발기구(GNSO)가 개인의 프라이버시를 보호하고 향후 수 년간 전체 ICANN 생태계를 위해 정확성과 책임성 및 투명성을 향상시킬 새로운 일반도메인 등록정보 관련 정책을 개발하기 위한 바탕이 될 토대를 제공한다고 확신한다.

ICANN 이사회와 일반도메인정책개발기구(GNSO) 및 ICANN 커뮤니티가 본 보고서를 고려할 때, 다음과 같은 질문에 초점을 맞춰 줄 것을 권고한다.

• 등록정보디렉터리서비스(RDS)가 현재의 WHOIS보다 바람직한가?

• 그렇지 않다면, ICANN 커뮤니티는 현재의 WHOIS 시스템이 계속 유지되어야 하며 이 시스템이 갈수록 진화하는 세계 인터넷 환경의 요구를 충족시킬 것이라 생각하는가?

배경

EWG는 ICANN 이사회의 요청에 따라 ICANN의 CEO 파디 셰하디(Fadi Chehadé)가 조직한 실무그룹으로 현재의 WHOIS 시스템을 대체할 방안과 관련해 거의 10년 가까이 ICANN 커뮤니티 안에서 답보 상태인 문제를 해결하기 위해 조직되었다.[2]

단순히 수 많은 보고서와 연구[3]에서 제기된 WHOIS 시스템의 결함을 극복하는 수준을 넘어, EWG는 일반도메인 등록정보의 수집 및 유지 목적을 재고 및 재정의하고, 이 정보를 안전하게 지킬 방법을 고민하며, 세계 인터넷 커뮤니티의 요구에 성실히 부응하는 차세대 솔루션을 제안해야 할 임무를 부여 받았다.

---

[1] EWG 구성 및 구성원들의 전문분야는 부록 J를 참조한다.

[2] https://www.icann.org/news/announcement-2-2012-12-14-en을 참조한다.

[3] WHOIS의 단점을 제기한 보고서 목록은 부록 B를 참조한다.

EWG는 백지 상태에서 시작해 먼저 (일반도메인) 등록정보의 목적과 사용, 수집, 유지 및 제공에 관한 근본적인 가정에 질문을 던졌다. EWG는 일반도메인 디렉토리서비스에 관련된 각 이해관계자들을 고려해서 정확성과 접근성 및 프라이버시에 대한 각 집단의 요구를 조사했다. 그리고 그러한 요구를 좀 더 효과적으로 충족시키기 위해 가능한 접근방법들을 모두 고려했다.

이 과정에서 EWG는 목적에 대한 고수준 기술서(high-level statement of purpose)를 개발하고, 이것을 사용해서 보고서의 권고안과 ICANN의 사명을 조율하고 도메인네임 등록 및 유지관리를 지원하는 다음과 같은 특징을 가진 시스템을 설계했다.

- 정확하고 믿을 수 있으며 일관된 등록정보에 대한 적절한 접근성을 제공한다.
- 도메인 등록인(Registrant) 정보의 프라이버시를 보호한다.
- 도메인 소유자에게 연락하기 위한 능력을 식별하고, 확립하고, 유지하기 위한 믿을 수 있는 메커니즘을 제공한다.
- 소비자 보호, 사이버범죄 수사 및 지적재산권 보호를 비롯하여 이에 국한되지 않는 문제들을 해결하기 위한 프레임워크를 지원한다.
- 적절한 사법상의 요구를 해결하기 위한 기반구조를 제공한다.

사용자와 목적

EWG는 이해관계자들이 일반도메인 등록정보를 수집 및 저장하고 다양한 사용자에게 제공하는 기존의 그리고 잠재적인 목적을 조사하기 위해 대표적인 WHOIS 이용 사례들을 폭넓게 조사했다.

EWG는 이러한 이용 사례들과 그것을 통해 얻은 교훈 그리고 참조 자료 및 커뮤니티의 의견들을 총체적으로 고려했고 그 결과 RDS가 반드시 수용해야 할 사용자 집단 및 허용된 목적들과 함께 반드시 억제해야 할 잠재적 오용 사례들을 도출했다.

모든 도메인 소유자	일반대중
보호받는 도메인 소유자	인터넷 기술 직원
온라인 서비스 제공업체	개인 인터넷 사용자
기업 인터넷 사용자	인터넷 연구자
지적재산권 소유자	비-LEA 조사자
LEA/OpSec	범죄자

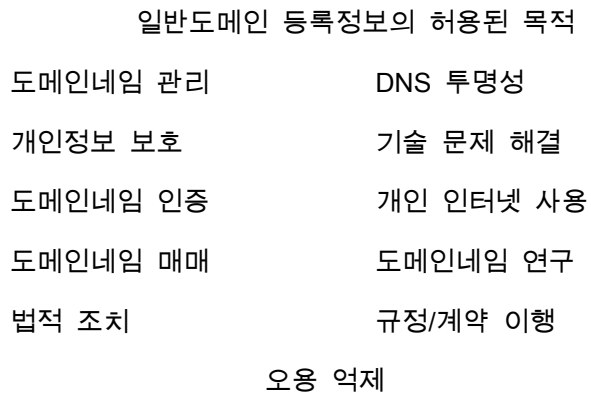
일반도메인 등록정보 사용자

8페이지

수용 또는 제지해야 할 목적

EWG가 위임 받은 임무에 따라, 이 모든 사용자들을 조사해서 기존의 그리고 앞으로 가능한 워크플로우를 식별하고 관련된 이해관계자 및 데이터를 식별했다.

도메인네임 등록정보에 대한 요구를 분석해서 의무적 데이터요소와 관련 위험, 정보보호법 및 정책과 관련한 의의를 이끌어내고 기타 본 보고서에서 탐색한 질문들을 해결하고자 했다. EWG가 권고하는 허용된 목적들이 오른쪽 그림에 요약되어 있다.



현재까지 식별된 허용된 목적 및 관련 등록정보, 연락처 및 질의 요구들이 아래에 정의되어 있으며 이를 섹션 III에서 좀 더 자세히 다룰 것이다.

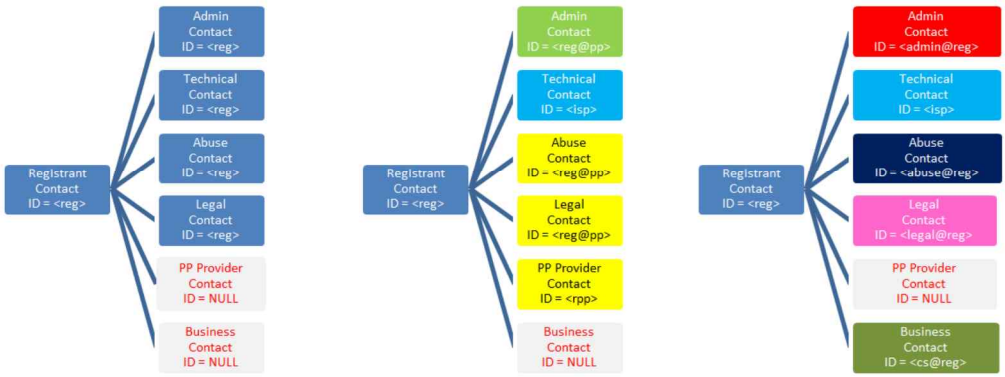
목적	관련된 활동
도메인네임 관리 (Domain Name Control)	도메인 소유자 자신의 도메인네임 생성, 관리 및 감시 활동. 도메인네임의 생성, 도메인네임 정보 업데이트, 도메인네임의 이전, 도메인네임 갱신, 도메인네임 삭제, 도메인네임 포트폴리오 관리 및 도메인 소유자 연락처 정보의 사기적 사용 탐지 등의 활동들이 포함된다.
개인 정보 보호 (Personal Data Protection)	도메인네임과 연결된 인증된 프라이버시/프록시 제공업체 또는 보안 크리덴셜 승인자(Secure Protected Credential Approver)를 확인하고 오용 신고, 신원 확인 요청 또는 달리 해당 제공업체에 연락하는 등의 활동.
기술 문제 해결 (Technical Issue Resolution)	이메일 전달 문제, DNS 분석 실패 및 웹사이트 기능 문제 등 도메인네임의 사용과 관련된 기술적 문제 해결을 위한 활동. 이 과정에서 이러한 문제 처리를 책임지는 기술 직원에게 연락할 필요가 있다.
도메인네임 인증 (Domain Name Certification)	인증 기관(CA)이 도메인네임으로 신원이 식별된 주체에게 X.509 인증서를 발급할 때, 그 주체가 도메인네임을 등록한 것인지 확인해야 한다.
개인 인터넷 사용 (Individual Internet Use)	도메인네임을 사용하는 조직의 신원을 확인해서 소비자에게 신뢰를 주거나 해당 조직에 연락해서 그들에 대한 소비자 불만이나 민원을 제기한다.

목적	관련 활동
기업 도메인네임 매매 (Business Domain Name Purchase or Sale)	도메인네임 구매 문의, 다른 도메인 소유자로부터 도메인네임 취득 및 실사 등의 활동
학술적/공익을 위한 DNS 연구 (Academic/Public-Interest DNS Research)	도메인 소유자 및 지정 연락처 정보, 도메인네임 이력과 상태 및 특정 도메인 소유자가 등록한 도메인네임 등 RDS에 공개된 도메인네임에 관한 공익적 학술 연구 활동.
법적 조치 (Legal Actions)	도메인 소유자 이름이나 주소를 다른 도메인네임이 사기적으로 사용하지 않는지 조사하고, 상표권 침해 가능성을 조사하고, 법적 조치를 취하기 전에 도메인 소유자/라이선스 보유자의 법률 대리인에게 연락하고 문제가 만족스럽게 해결되지 않을 경우 법적 조치를 취하는 등의 활동.
규정 및 계약 이행 (Regulatory and Contractual Enforcement)	온라인에서 활동하는 기업에 대한 세무 당국의 조사, UDRP 관련 조사, 계약 이행 조사 및 등록정보 매매보호 에스크로 감사 등의 활동
범죄 수사 및 DNS 오용 억제 (Criminal Investigation & DNS Abuse Mitigation)	오용 사건이 발생할 경우 수사 및 해결이 가능한 주체에게 신고하거나 오프라인 범죄 수사 중 특정 도메인네임과 연관된 실체에게 연락하는 등의 활동.
DNS 투명성 (DNS Transparency)	일반 대중에 정보를 제공하기 위한 다양한 수요를 충족시키기 위해 도메인 소유자가 공개한 등록정보를 질의하는 활동

등록 정보에 접근하는 목적을 기초로 접근을 허용하는 한편 커뮤니케이션 및 개인의 프라이버시 향상을 위해 EWG는 목적별 연락처(Purpose-Based Contacts, PBC) 체계를 위한 원칙들을 수립했다. PBC별로 구체적인 역할과 책임을 정의하고 허용 가능한 모든 접근 목적들과 매핑시켰다. 그 사례들이 아래 그림에 요약되어 있으며 3장과 4장에서 좀 더 자세히 다룰 것이다.

10 페이지

(그림)



나아가 EWG는 2013 RAA에 정의된 것부터 시작해서 등록정보의 모든 구성요소를 분석해서 본 보고서에서 권고하는 PBC 프레임워크는 물론 데이터보호법 준수를 위한 권고와도 부합하는 데이터 수집 및 공개를 위한 일단의 기본 원칙들을 이끌어냈다. 나아가 EWG는 도메인 소유자와 연락처가 좀 더 원활한 의사소통을 위해 공개 여부를 선택할 수 있는 새로운 데이터 요소들을 식별하기 위한 권고안을 제시했다. 이러한 권고안들은 섹션 IV에서 상세하게 설명하고 있으며 부록 E에 사례를 제시했다.

목적 기반 접근(Purpose-Driven Access)

EWG가 권고하는 RDS는 백지상태에서 시작해 현재 만병통치약식 WHOIS 시스템을 폐지하고 특정 목적에 한해 검증된 데이터 접근을 허용하는 시스템을 개발함으로써 프라이버시와 정확성 및 책임성을 향상시키고자 한다. EWG는 이 새로운 접근 패러다임이 다음과 같은 방식으로 일반도메인 도메인네임 등록정보의 공개와 사용에 관련된 모든 당사자들의 책임성을 증가시킬 수 있을 것이라 기대한다.

- 공개 데이터 요소에 대한 무단 접근까지 일반도메인 등록정보에 대한 모든 접근을 기록해 오용을 탐지하고 억제할 수 있도록 한다.
- 좀 더 민감한 데이터 요소의 경우 RDS 접근 신청서를 제출해서 승인을 얻은 신청자에 한해, 각 사용자와 명시한 목적에 적합한 수준에서 제한적으로 사용을 허용한다.
- 공개 및 제한적(gated) 데이터 접근 모두를 감사해서 오용을 최소화하고 부적절한 사용이 확인될 경우 각 요청자가 명시적으로 동의한 조건에 따라 제제 및 구제 조치를 취한다.

공개 및 제한적 데이터 접근에 관한 구체적인 권고안의 기초가 되는 EWG의 데이터 접근 원칙(Principles for Data Access)에 관해서는 4장에서 자세히 설명한다. 아래 그림에서 보듯이, 공개 데이터 요소의 경우 RDS에서도 별도의 인증 절차 없이 누구나 요청이 가능하다.

11페이지

(그림)
요청자 RDS 질의 모든 일반도메인 관리기관
(인증 없음, DN) RDS
RDS 응답 모든 일반도메인 검증기관
(공개 데이터에 한함)
목적에 관계없이 누구나 이용 가능한
공개 데이터만 반환한다.

제한적 데이터 요소 역시 RDS를 통해 요청이 가능하다. 그러나 먼저 요청자 인증이 이루어져야 한다. 그 후에 요청자가 명시적인 목적을 위한 데이터 요소를 요청하는 인증된 질의서를 제출해야 한다.

(그림)
1차 제한적(GATED) 질의 전에
요청자는 반드시 인증을 거쳐 요청자 ID를 얻어야 한다.

인증된 요청자 RDS 질의 모든 일반도메인 관리기관
(요청자 ID, 목적, DN) RDS
RDS 응답 모든 일반도메인 검증기관
(공개 + 제한적 데이터)

명시된 목적을 위해 이용 및 접근이 허용된
데이터에 한해 인증된 요청자에게 반환한다.

부록 E에서는 공개 및 제한적 데이터 요청에 따라 반환되는 데이터 요소, 제한적 접근이 사용자와 목적에 따라 어떻게 달라지는지 그리고 RDS 사용자 인증 기관이 어떤 식으로 제한적 접근을 허가하고 감사하는지에 대해 좀 더 자세하게 설명하고 있다.

프라이버시 및 정보 보호

EWG의 가장 큰 과제는 수집된 데이터의 정확성을 높이는 동시에 자신의 프라이버시를 지키고자 하는 도메인 소유자들을 보호할 수단을 제공하는 시스템을 어떻게 설계할 것인가 하는 것이다.

EWG는 개인정보는 정보보호법으로 보호되며 그러한 법이 없더라도 개인이 자신의 개인정보에 대한 강화된 보호수단을 추구해야 할 타당한 이유가 있음을 인정한다. 또한 일부 기업과 조직들 역시 신상품 출시를 준비할 때, 또는 소규모 기업의 경우 연락처 정보를 통해 개인 정보가 노출될 때와 같이 합법적인 목적을 위해 조직에 관한 정보를 보호하고자 한다.

그래서 EWG는 일상적으로 프라이버시 및 정보보호법을 준수하기 위한 일단의 권고안을 마련했으며 이에 관해서는 6장에서 자세히 설명할 것이다. 이러한 기본 원칙들은 다음과 같은 주제를 다루고 있다.

- RDS 생태계 내에서 합법적인 데이터 수집 및 행위자들 사이의 전달을 위한 메커니즘
- 프라이버시 및 정보보호법에 부합하고 정책으로 명문화된 표준 계약 조항
- 정보보호법 적용을 위한 “규칙 엔진(rules engine)”
- RDS 데이터 저장 장소와 사법 활동을 위한 접근과의 상관관계

정보보호법 준수를 통해 프라이버시를 지키는 동시에 RDS는 RDS 생태계 내에 다음과 같은 요소를 포함시켜 프라이버시에 대한 요구를 충족시키기 위한 원칙들도 권고했다.

- 범용 공인 프라이버시/프록시 서비스
- 위험에 노출된 사람들과 언론의 자유가 부인되거나 화자(speakers)가 기소된 경우를 위한 공인 보안 크리덴셜 서비스(Secure Protected Credentials Service)

아울러 EWG는 ICANN이 RDS 활동들에 포괄적으로 적용되는 조율된 단일 프라이버시 정책 개발을 제고하도록 권고한다.

책임성이 강화된 일관성 있고 신뢰할만한 프라이버시 및 프록시 서비스에 대한 요구를 해결하기 위해 EWG는 PBC 원칙에 프라이버시/프록시 커뮤니케이션을 포함시켰다. 또한 일반도메인정책개발기구(GNSO)의 프라이버시 및 프록시 서비스 인증 문제 실무그룹(GNSO Privacy and Proxy Services Accreditation Issues Working Group)에도 프라이버시/프록시 원칙과 프레임워크에 대한 논의를 권고했다.

그리고 등록정보로 인해 신원이 식별될 경우 위험에 노출된다는 것을 입증하는 것이 가능한 개인 및 집단의 요구를 해결하기 위해 EWG는 해당 당사자들이 보안 크리덴셜을 이용해서 등록된 도메인네임을 익명으로 신청하고 받을 수 있는 공인 보안 크리덴셜 프레임워크(Secure Protected Credential Framework)를 권고한다. 이 과정에서 위험에 노출된 실체와 등록대행자 사이에서 방패가 되어 줄 신뢰할 수 있는 증인 및 제3자가 필요하다. EWG는, ICANN이 크리덴셜을 승인(및 필요할 경우 파기)하기 위해 위험에 노출된 조직이나 개인의 주장을 검증해 줄 신뢰할만한 독립적 검토 위원회 설립을 조속히 추진할 것을 권고한다.

13페이지

데이터 품질

EWG는 도메인 소유자 정보를 현재의 WHOIS 시스템과 비교해 좀 더 강도 높게 검증할 것을 권고한다. 또한 2013 RAA를 폭넓게 이행함으로써 보강하는 수준에 그쳐서도 안 된다. 데이터 품질 개선을 위해 다음과 같은 기본적인 변화가 필요하다.

- 도메인 소유자가 제공하는 목적별 연락처 정보가 다양한 목적에 맞는 적절한 연락처로 연결될 가능성을 높이고 도메인 소유자들이 해당 연락처에 대한 정확한 정보를 제공할 유인을 제공해야 한다.
- 민감한 데이터 요소의 경우 제한적 접근을 허용함으로써 도메인 소유자가 부정확한 데이터를 제공할 유인을 줄이는 동시에 데이터의 정확성에 대한 책임감을 높일 것이다.

아울러 EWG는 서로 관련이 있으면서도 독립적인 두 가지 개선방안을 권고한다.

- 모든 일반도메인 등록정보에 대한 표준 검증 및 주기적으로 등록정보를 점검하는 동시에 수집 시에도 검증한다. 한 대안으로 여러 도메인네임을 등록할 때 다시 사용할 수 있도록 연락처 데이터 블록을 미리 검증하고 RDS 사용자들이 데이터가 언제 최종 검증되었는지 그리고 어느 수준까지 검증되었는지 확인할 수 있도록 한다.
- 사전 검증된 연락처 디렉토리(Contact Directory). 도메인네임 디렉토리와 개념적으로 분리해 도메인 소유자 또는 도메인 소유자가 도메인네임 등록과 관련된 다양한 목적을 위해 PBC로 지정한 사람 또는 조직에 연락할 때 사용되는 데이터 요소의 품질과 재사용성을 높이고 개인 정보의 오남용(사기행위)을 억제한다.

이러한 권고안에 대해 섹션 V에서 좀 더 세부적으로 설명할 것이다.

구현 모형

이러한 원칙과 권고안을 어떻게 실행으로 옮길 것인가를 생각하면서 EWG는 다양한 대안적 모형들을 심도 깊게 연구했다. 부록 F에 수록된 일단의 다면적 기준을 이용해서 모든 모형들을 평가했다. 엄격한 분석을 거친 후 EWG는 다음과 같은 결론을 내렸다.

- 현재 등록대행자 또는 등록대행자의 제휴 기관(Affiliate)는 고객들(도메인 소유자)로부터 등록 정보를 수집해 저장하는데 이 과정은 분산될 수 밖에 없다. 등록대행자 또는 제휴 기관이 계속해서 도메인 소유자로부터 등록 정보를 수집하는 동시에 검증기관(Validator)도 연락처 정보를 수집하는 방안을 제안한다.
- 모든 일반도메인에 걸쳐 등록정보를 저장하기 위한 다양한 모형들이 존재한다. EWG 는 여러 가지 가능성이 있는 모형들을 조사했고 그 중에서 가장

바람직하다고 여겨지는 두 모형을 식별했다. 이 두 모형 중에서 평가를 거쳐 한 가지를 선택할 것을 권고한다.

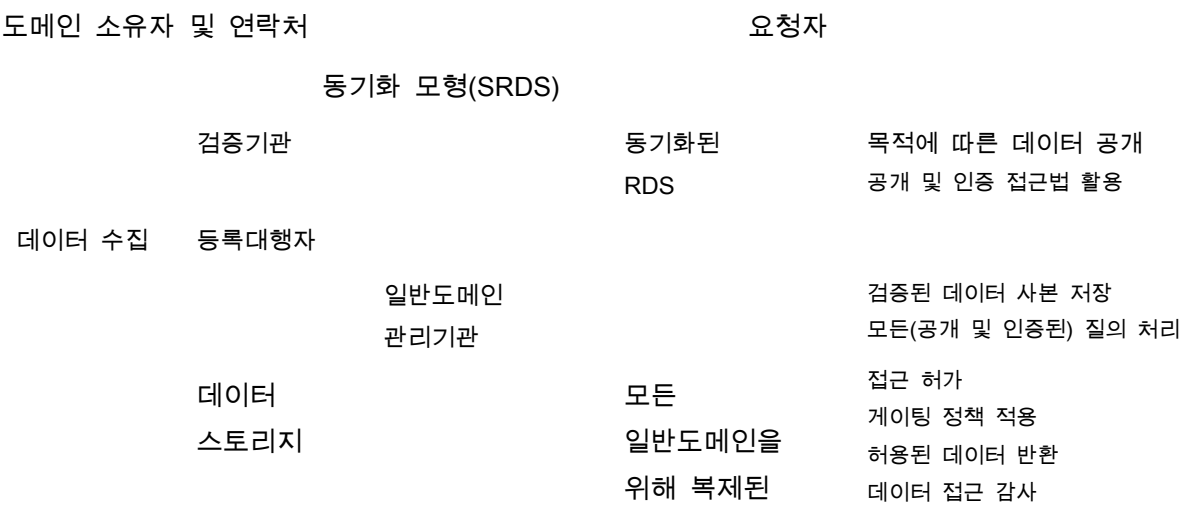
14 페이지

- 데이터 주체의 프라이버시를 보호하기 위해서, 인증절차 없는 공개 데이터 접근이든 인증을 통한 제한적 데이터 접근이든 중앙집중화된 인터페이스를 통해 적격한 요청자가 등록 정보에 접근하도록 해야 한다.
- RDS는 RDAP(등록데이터접근프로토콜, Registration Data Access Protocol) 또는 EPP(확장정보제공프로토콜, Extensible Provisioning Protocol)를 기본적인 디렉토리 접근 프로토콜로 사용해 어디든 반드시 스토리지가 있는 곳에서 등록정보를 획득해야 한다.

EWG는 여러 가지 대안적인 시스템 모형을 개발해서 시험했다. ICANN 커뮤니티가 제안한 모형을 비롯해 이들 모형에 대해서 부록 F에서 자세히 설명한다. 이 모형들은 등록 정보 복사 또는 RDS에서의 질의 방식에 있어 차이가 있다. EWG는 각 모형을 면밀히 조사해서 그러한 차이가 미치는 영향을 식별했다. 가능성 있는 모형들을 비교한 후, EWG는 현행 WHOIS 시스템을 제외한 모든 모형들이 EWG가 권고한 RDS 원칙들을 어느 정도 충족시킨다는 사실을 확인했다. 그 중에서도 EWG는 좀 더 조사해 볼만한 가장 유망한 두 모형에 초점을 맞추었다. 한 가지는 연합 모형(Federated Model)이고 다른 하나는 동기화 모형(Synchronized Model)(이전에는 “집적 모형(Aggregated Model)”으로 불렀다)이다.

분석을 위한 추가 정보를 얻기 위해 EWG는 중립적인 제3자(IBM)에게 구현 모형 비용 분석(Implementation Model Cost Analysis)을 의뢰했고 이 두 모형의 요건과 잠재적 비용을 파악했다. EWG의 심층 분석 및 IBM의 분석 보고서를 기초로 연합 모형이 전체 RDS 생태계에 더 많은 비용을 초래하는 것을 확인했기 때문에 **EWG는 최종적으로 동기화 RDS(SRDS) 모형을 권고한다.**

(그림)



동기화 데이터를 통한 데이터 접근

추가 서비스

결론

본 보고서가 매우 상세하고 복잡하며 분량이 많은 관계로 본 개요가 전체 내용을 포괄적으로 요약하지는 않는다. 따라서 독자들은 본 보고서의 본문에서 자세한 내용을 확인할 것을 권한다.

EWG는 본 보고서를 ICANN CEO 및 이사회에 전달했으며 온라인 상에 공개적으로 발표했다. 그리고 2014년 7월에 런던에서 열린 공개회의에서 다양한 일반의 의견을 수렴할 것이다. 또한 온라인회의(웨비나, Webinar)를 비롯한 여러 경로를 통해 ICANN 커뮤니티와 보고서를 논의하고 질문에 답변할 것이다. 본 보고서는 이사회가 요청한, 일반도메인 등록 정보 제공 및 해당사항이 있을 경우 계약 협상에 관한 일반도메인정책개발기구(GNSO)의 정책 개발 과정(PDP)을 진행하기 위한 기초가 될 것이다.

EWG는 본 보고서가, 일반도메인 등록정보의 목적과 제공을 재정의함으로써 ICANN 커뮤니티가 (일반도메인정책개발기구(GNSO)를 통해) 일반도메인 디렉토리서비스를 위한 새로운 정책을 수립하기 위한 확고한 토대를 제공하고자 하는 ICANN 이사회의 방침에 부합하리라 확신한다.

II. EWG의 임무, 목적 및 결과물

a. 임무

일반도메인 디렉토리서비스에 관한 전문가 실무그룹(EWG)은 ICANN 이사회의 요청에 따라 현 WHOIS 시스템을 대신할 방안과 관련해 ICANN 커뮤니티 내에서 10년 가까이 답보 상태인 문제를 해결하기 위해 ICANN의 CEO 파디 셰하디가 조직했다. 그 동안 발표된 여러 보고서와 연구[4]들이 하나같이 현 시스템의 문제점을 지적하며 새로운 솔루션을 요구했다.

EWG의 임무는 일반도메인 디렉토리서비스의 정보 수집 및 유지를 재조사 및 재정의하고, 데이터 보호 방법을 고민해서 세계 인터넷 커뮤니티의 요구에 더 잘 부응할 차세대 솔루션을 제안하는 것이다. EWG는 백지 상태에서 시작해 목적과 (일반도메인) 등록정보의 사용, 수집, 유지 및 제공 활동들의 현황을 조사하고 그러한 활동에 관한 근본적인 가정들에 의문을 제기했다. EWG는 일반도메인 디렉토리서비스에 관여하는 각 이해관계자들을 고려해 정확성, 접근성 및 프라이버시에 대한 각 집단의 요구를 조사하고 그러한 요구를 좀 더 효과적으로 충족시킬 접근방법들을 탐색했다.

b. 목적

연구 작업의 효과적인 진행을 위해 EWG는 최종적인 결론과 권고안을 검증하기 위한 기준이 될 목적에 대한 고수준의 기술서(high-level statement of purpose)를 개발했다.

세계 인터넷 고유식별체계를 조율해야 하는 ICANN의 사명을 뒷받침하고 인터넷 고유식별체계의 안정적이고 안전한 운영을 보장하기 위해 일반도메인 도메인네임에 관한 정보는 인터넷에 대한 모든 이해관계자들의 신뢰와 확신을 증진시켜야 한다.

따라서, 도메인네임 등록 및 유지 활동을 뒷받침하는 다음과 같은 시스템을 설계하는 것이 바람직하다.

- 정확하고 믿을 수 있으며 일관된 등록정보에 적절히 접근할 수 있게 한다.
- 개인정보의 프라이버시를 보호한다.
- 도메인 소유자에게 연락할 수 있는 수단을 식별하고, 확립하고, 유지하기 위한 믿을 수 있는 메커니즘을 마련한다.

[4] WHOIS의 단점을 문서화한 보고서 목록은 부록 B를 참조한다.

- 소비자 보호, 사이버범죄 수사 및 지적재산권 보호를 비롯해 여기에 국한하지 않고 도메인 소유자와 관련된 문제를 해결할 프레임워크를 지원한다.
- 적법한 사법 관련 요구를 해결하기 위한 기반구조를 제공한다.

c. 결과물

2013년 6월 24일, EWG는 최초 보고서와 자주 묻는 질문(FAQ) 및 온라인 질문지를 발표하고 ICANN 커뮤니티 내에서 최초 권고안에 관한 광범위한 의견 수렴 과정을 시작했다. 최초보고서에서 EWG는, 모든 사용자가 (종종 정확하지 않은) 일반도메인 등록정보에 익명으로 접근할 수 있도록 허용하는 현재의 WHOIS 모형은 폐기되어야 한다는 결론을 내렸다. 대신 EWG는 패러다임의 전환을 통해 일반도메인 등록정보를 허용 가능한 특정 목적을 위해서만 수집, 검증 및 공개하고 일부 데이터 요소는 그 적절한 사용에 대해 책임질 수 있는 인증된 요청자에게 접근을 허용하는 방안을 권고했다.

EWG는 WHOIS의 문제점들을 구체적으로 기술한 과거의 보고서들과 WHOIS 시스템을 사용하는 다양한 이해관계자들을 폭넓게 고려한 후에 이러한 결론에 도달했다. 식별된 각 사용자 집단을 위해 그들의 등록정보 사용 목적과 그러한 목적을 위해 필요한 개별적인 데이터 요소들을 분석했다. 이러한 분석 결과를 바탕으로 EWG는 차세대 등록정보 디렉토리서비스(RDS) 도입 과정을 이끌어 줄 원칙과 특징을 권고했다. 이러한 원칙들을 어떻게 실현할 수 있는지 설명하기 위해 EWG는 여러 가지 대안을 고려한 끝에 허용된 목적을 위해 정확한 도메인네임 등록정보를 수집 및 공개하기 위한 하나의 모형을 제안했다.

2013년 11월 11일, ICANN 커뮤니티로부터 받은 모든 의견과 피드백을 심사숙고한 끝에 EWG는 주요 문제에 관한 EWG의 생각을 내용으로 한 상태 업데이트 보고서(Status Update Report)를 발표했다. 또한 이 보고서는 커뮤니티의 요청을 반영해 최초보고서에서 개략적으로 언급한 분석에 대해서도 상당히 자세하게 다루었다.

EWG는 커뮤니티의 다양하고 폭넓은 의견들을 이용해 이들 보고서에 대한 피드백을 면밀하게 분석함으로써 실무그룹의 지속적인 작업을 위한 정보를 제공하는 동시에 EWG의 권고안을 시험하고 정교하게 다듬고자 했다. 당면한 작업이 복잡하고 차세대 RDS가 가져올 장점과 영향에 대한 확고한 이해를 다지는 것이 중요했기 때문이었다.

18페이지

EWG는 기존의 국가도메인과 상업적 데이터 검증 방식, 기존의 프라이버시/프록시 서비스 제공업체의 방식, RDS 사용자 인증이 가능한 조직에 대한 조사 그리고 RDS의 위험/편익 및 비용 분석 등 다섯 가지 부문에 대한 조사를 실시했다. 2014년 3월에 발표된 이 연구조사 결과를 이용해서 EWG의 권고안을 좀 더 정교하게 손질했다.

이 단계에서 EWG는 WHOIS에 관한 과거 연구와 기존의 그리고 미래의 일반도메인 등록정보 사용자와 그들의 사용 목적, 현재 WHOIS 시스템에 관여하는 수 많은 다양한 이해관계자들의 의견, 제안된 RDS 개선안들과 관련된 기존의 활동 및 RDS 위험, 편익 및 비용 분석 등을 면밀하게 검토했다. 이 모든 자료와 정보가 차세대 시스템에 관한 EWG의 권고안 [5] 에 반영되었으며 ICANN 이사회에 제출할 본 최종보고서에 상세히 설명되어 있다. 또한 EWG의 권고는 정책 개발 과정에서 중요한 근거 자료로 활용될 것이다.

[5] 본 보고서에서 설명하는 EWG 원칙에서 사용되는 다음과 같은 용어들은 RFC 2119의 정의를 따른다.

- 반드시 해야 한다(MUST): "반드시 해야 한다(MUST)" 또는 "요구된다(REQUIRED)" 또는 "해야 한다(SHALL)"는 해당 정의가 본 보고서의 절대적 요건임을 의미한다.
- 절대로 해서는 안 된다(MUST NOT): "절대로 해서는 안 된다(MUST NOT)" 또는 "해서는 안 된다(SHALL NOT)"는 해당 정의가 본 보고서의 절대적 금지 사항임을 의미한다.
- 해야 한다(SHOULD): "해야 한다(SHOULD)" 또는 "권장한다(RECOMMENDED)"는 특정 정황에서 특정 항목을 무시해야 할 타당한 이유가 존재할 지 모르지만 다른 경로를 선택하기 전에 전체적 의의를 반드시 이해하고 신중하게 판단해야 한다는 것을 의미한다.
- 해서는 안 된다(SHOULD NOT): "해서는 안 된다(SHOULD NOT)" 또는 "권장하지 않는다(NOT RECOMMENDED)"라는 문구는 특정 행동이 허용 가능하거나 심지어 유용한 특정 정황에서 타당한 이유가 존재할 지 모르지만 이 문구와 함께 기술된 어떤 행동을 이행하기 전에 전체적인 의의를 이해하고 그 사례를 신중하게 판단해야 한다는 것을 의미한다.

III. 사용자 및 목적

a. 방법론(Methodology)

EWG는 차세대 등록정보 디렉토리서비스를 정의함에 있어 현재 부적절하다는 평가를 많이 받고 있는 WHOIS 시스템을 개선하기 위한 방안을 제안하기 보다는 “백지 상태”에서 새로운 시스템을 모색하는 접근법을 취했다. 이사회의 지시에 따라 EWG는 일반도메인 등록정보를 수집, 저장 및 다양한 사용자들에게 제공하기 위한 현재와 미래의 잠재적 목적을 조사하는 것으로 분석을 시작했다.

이 분석을 위해 EWG 구성원들은 현 WHOIS 시스템과 관련된 실제 이용 사례를 광범위하게 조사하고 각 사례를 분석해서 (i) 등록정보 접근을 원하는 사용자, (ii) 그러한 접근을 필요로 하는 이유, (iii) 그들이 필요로 하는 데이터 요소 그리고 (iv) 그러한 데이터의 사용 목적을 파악했다. 아울러 이러한 이용 사례들은 등록정보의 수집, 저장 및 제공에 관여하는 모든 이해관계자들을 식별하는 데 사용되어, 기존의 그리고 잠재적인 (등록정보의) 워크플로와 이러한 사용자 및 그들의 요구가 차세대 RDS를 통해 더욱 효과적으로 충족시키기 위한 방법들을 이해하는 데 도움이 되었다.

모든 사용 사례를 제시하기보다는 현재 WHOIS 시스템의 대표적인 사용 현황을 살펴봄으로써 다양한 사용자들과 그들의 요구 및 워크플로를 설명하는 것이 목적이다. EWG가 고려한 사용 사례 목록을 부록 C에 수록했다.

EWG는 이러한 사용 사례들과 그로부터 얻은 교훈을 전반적으로 숙고한 끝에 RDS가 반드시 수용해야 할 일단의 이해관계자 집단과 바람직한 사용 목적은 물론 새로운 시스템이 반드시 억제해야 할 잠재적 오용 사례들을 도출했다. 아울러 EWG는 이전의 WHOIS 관련 활동으로 얻은 참조 자료와 커뮤니티의 의견 및 사용 사례들을 참고해서 아래 표 1에 수록된 각 부문의 구체적인 요구를 조사했다.

사용자 및 목적	데이터 요소 요건	프라이버시 요건
	일반도메인 등록정보	
스토리지 및 데이터 에스크로 요건	접근성 및 책임성 요건	검증 및 정확성 요건

그림 1: 요구 분석

EWG는 계속해서 이러한 목적과 사용자 요구를 분석해서 각 목적에 요구되는 최소한의 데이터 요소들과 그 데이터를 접근 가능하게 만들었을 때 따르는 위험, 프라이버시법 및 정책과 관련해 지니는 의의 그리고 본 보고서에서 다룬 추가적인 질문들을 도출했다.

b. RDS 사용자와 목적

아래 그림 2는 건설적인 목적 또는 악의적 목적을 지닌 사용자들을 포함해서 기존 WHOIS 시스템 사용자들을 총체적으로 보여준다. EWG의 임무에 따라 이 모든 사용자들을 조사해서 기존의 그리고 미래에 가능한 워크플로와 그러한 과정에 관련된 이해관계자 및 데이터를 식별했다.

모든 도메인 소유자		일반 대중
보호받는 도메인 소유자		인터넷 기술 직원
온라인 서비스 제공자	일반도메인 등록정보 사용자	개별 인터넷 사용자
기업 인터넷 소유자		인터넷 연구자
지적재산권 소유자		비-LEA 조사자
LEA/OpSec		범죄자

그림 2: 사용자

본 보고서에서 “요청자(requestor)”라는 용어는 누구든 일반도메인 등록정보를 얻고자 하는 사용자를 총체적으로 지칭하기 위해 사용된다. 본 보고서에서 좀 더 상세히 설명하겠지만 EWG는 모든 사용자가 종종 정확하지 않은 일반도메인 등록정보에 익명으로 접근하도록 허용하는 현행 WHOIS 모형의 폐지를 권고한다. 대신 EWG는 특정 허용된 목적을 위해서만 일반도메인 등록정보를 수집, 검증 및 공개하고 일부 데이터 요소는 적법한 사용을 책임지는 인증된 요청자에게만 접근을 허용하는 새로운 시스템을 권고한다.

EWG는 대표적인 사용 사례들을 분석해서, 일반도메인 등록정보 접근을 원하는 사용자들의 종류와 접근 이유 및 그러한 등록정보가 어떤 목적을 위해 사용되는지를 요약한 다음의 표를 작성했다. 각 사용자와 목적 및 관련된 데이터 수요에 관해서는 섹션 III(c) 수용 또는 제재해야 할 목적(Purposes to be Accommodated or Prohibited)과 부록 D에서 자세하게 설명한다.

사용자	목적	이용 사례의 예	등록정보 접근 근거
모든 도메인 소유자 (예, 자연인, 법인, 공인 프라이버시/프록시 제공업체)	도메인네임 관리	도메인네임 등록 계정 생성	어떤 종류의 도메인 소유자든 등록대행자에 새 계정을 생성하면 도메인네임을 등록할 수 있다.
		도메인네임 데이터 수정 모니터링	현재 또는 과거에 도메인네임 등록정보가 우발적으로 또는 허가 받지 않고 수정되지 않았는지 확인할 수 있다.(WhoWas 사용)

사용자	목적	이용 사례의 예	등록정보 접근 근거
		도메인네임 포트폴리오 관리	도메인네임 포트폴리오 유지관리를 위해 모든 도메인네임 등록 정보(예, 지정된 연락처, 주소)를 업데이트한다
		도메인네임 이전 개시	도메인 소유자가 도메인네임을 다른 등록대행자로 이전한다
		도메인네임 삭제	만료된 도메인네임을 삭제한다.
		도메인네임 DNS 업데이트	도메인 소유자가 도메인네임을 위한 DNS를 변경한다
		도메인네임 갱신	도메인 소유자가 등록된 도메인네임을 변경한다
		도메인네임 연락처 검증	도메인 소유자의 등록 정보(예, 지정된 연락처, 주소)를 최초 및 지속적으
보호받는 도메인 소유자 (예, 공인 프라이버시/프록시 서비스 고객)	개인 정보 보호	프라이버시/프록시 제공업체에 연락	개인의 이름과 주소 정보에 대한 일반의 접근을 최소화하고자 하는 도메인 소유자를 위해 등록 서비스를 제공하는 공인 프라이버시 또는 프록시
		보안 크리덴셜 승인자에 연락	신뢰할 수 있는 제3자를 통해 중계되는 보안 크리덴셜을 사용해서 위협에 노출된 개인이나 집단이 사용하는 등록 서비스를 제공하는 공인 보안 크
인터넷 기술 직원 (예, DNS 관리자, 메일 관리자, 웹 관	기술 문제 해결	도메인네임 기술 직원에 연락	도메인네임과 관련된 기술적 또는 운영상의 문제(예, DNS 분석 실패, 이메일 전달 문제, 웹사이트 기능 문제) 해결을 돕는 기술 직원(개인, 역할 또
인증 기관	도메인네임 인증	도메인네임 인증서 발급	인증기관이 SSL/TLS 인증서와 묶일 도메인네임의 소유자를 식별한다
개인 인터넷 사용자 (예, 소비자)	개인 인터넷 사용자	실제 연락처	소비자가 도메인네임 소유자의 실세계 연락처 정보(예, 영업장 주소)를
		소비자 보호	소비자가 LE/OpSec 개입 없이 문제를 빠르게 해결하기 위해 도메인네임 소유자가 지정한 연락처에 연락하기 위한 기본적인 수단(예, 온라인 소매

사용자	목적	이용 사례의 예	등록정보 접근 근거
기업 인터넷 사용자 (예, 브랜드 소유자, 브로커, 에이전트)	기업 도메인네임 매매	도메인네임 중계 매매	도메인네임 구입과 관련된 실사를 한다.
		도메인네임 상표 청산	새 브랜드를 만들 때 상표 청산(위험 분석)을 위해 도메인네임 소유자의 신원을 확인한다.
		도메인네임 인수	기존에 등록된 도메인네임을 인수하기 위해 도메인 소유자와 연락한다.
		도메인네임 구입 문의	도메인네임의 가용성과 현재 도메인 소유자 및 관리자(해당하는 경우) 연락처를 확인한다.
		도메인네임 등록 이력	과거 도메인 소유자 및 WhoWas 사용 날짜를 확인하기 위해 도메인네임 등록 이력을 확인한다.
		특정 도메인 소유자의 모든 도메인네임	합병/기업분할 자산 검증의 일환으로 특정 실체가 등록한 모든 도메인네임을 확인한다.(역질의)
인터넷 연구자	학술적/공익을 위한 DNS 연구	도메인네임 등록 이력	학술적 및 공익을 위한 DNS 연구를 위해 도메인네임 등록 이력을 조사한다.(WhoWas)
		특정 연락처의 모든 도메인네임	학술적 및 공익을 위한 DNS 연구를 위해 특정 이름, 주소, 이름 서버, 등록 날짜 등으로 등록된 모든
		도메인네임 소유자나 지정 연락처 조사	도메인네임 소유자 또는 지정된 연락처를 조사할 수 있다.
지적재산권 소유자 (예, 브랜드 소유자, 상표 소유자, IP 소유자)	법적 조치	도메인네임 사용자 연락	TM/브랜드 침해나 IP 절도와 연관되어 조사 중인 도메인네임을 사용하는 당사자에게 연락한다.
		도메인 소유자 정보의 사기적 사용 방지	신원이 확인된 정보에 역질의를 사용해, 다른 도메인 소유자에게 속한 도메인네임의 합법적 정보(예, 주소)가 사기적으로 사용되지 않았는지 확인하고 대응한다.
		도메인네임 등록 이력	IP 침해 조사 중 도메인네임 등록 이력(WhoWas)을 조사한다.

24페이지

사용자	목적	이용 사례의 예	등록정보 접근 근거
		특정 도메인 소유자의 모든 도메인네임	IP 침해 조사를 위해 특정 이름이나 주소로 등록된 모든 도메인을 식별한다 (역질의)
비 LEA 조사자 (예, 세무 당국, UDRP 제공업체, ICANN 컴플라이언스)	규제 및 계약 이행	온라인 세무 조사	국가, 주, 지역 및 지방 세무 당국이 온라인 매매에 관여하는 도메인네임의 연락처를 식별한다.
		UDRP 절차	UDRP 제공업체가 도메인네임의 올바른 등록자를 확인하고, 준법 여부를 점검하고, 법적 절차 요건을 판단하고 사이버플라이트 (cyberflight)로부터 보호한다.
		RDS 생태계 계약 준수	ICANN이 계약 당사자들의 규정 위반을 감사하고 민원에 대응한다. (예, 데이터 부정확성이나 비가용성, UDRP 결정의 실행, 이전에 관한 민원, 데이터 에스크로 및 보유)
LEA/OpSec 조사자 (예, 사법기관, 사고대응팀)	범죄 수사 및 DNS 오용 억제	도메인네임 오용 수사	LEA/OpSec 인력들이, 이력 데이터 조사를 비롯해 악의적으로 등록된 것으로 주장된 도메인네임을 수사하고 증거를 수집한다.
		오프라인 범죄 활동 수사	구체적인 등록정보를 제공하고 용의자가 등록한 도메인네임을 검색함으로써 LEA/OpSec 인력들이 오프라인 범죄 활동을 효과적으로 수사하고 증거를 수집한다. (역질의).
		도메인네임 평판 서비스	평판 서비스 제공업체가 도메인네임 화이트/블랙 리스트를 분석할 수 있다.
		온라인 범죄 활동 수사	범죄 희생자나 그 변호인이 LE/OpSec의 후속적인 수사를 위해 잠재적으로 불법적인 활동에 관여한 도메인네임 소유자의 신원을 확인하도록 돕는다.
		훼손된 도메인네임 오용 신고	LEA/OpSec가 (침해된) 도메인 소유자나 지정된 오용 신고 연락처로 연락해 해당 도메인네임의 훼손을

사용자	목적	이용 사례의 예	등록정보 접근 근거
일반 대중 (예, 블로거, 매체, 정치적 활동가)	DNS 투명성	일반의 등록정보 접근	좀 더 구체적인 이용 사례에서는 달리 고려되지 않는 다양한 인터넷 사용자들이 공통적으로 원하는 대로 도메인네임의 "배후에 있는" 조직을 식별한다.
범죄 (예, 스팸, DDoS, 피싱, 신원 절도, 도메인 하이재킹 관여자)	악의적 인터넷 활동	도메인네임 탈취	도메인 소유자의 계정에 불법적으로 접근하거나 도메인네임 탈취를 위해
		악의적 도메인네임 등록	기존의/훼손된 도메인네임 등록 계정을 사용해서 새로운 이름을 등록해 사기를 비롯한 범죄 활동에
		스팸/스캠을 위한 등록정보 수집	스패머, 스캐머 및 기타 범죄자들이 악의적 사용을 위해 도메인네임

표 1. RDS 사용자 및 목적

c. 수용 또는 제재해야 할 목적

EWG 는 이용 사례 개발의 초점을 정하고 허용된 목적의 범위를 좁히기 위해서 위에서 열거한 목적들에 우선순위를 부여하고자 했다. 그러나 그 목적이 악의적이지 않은 이상 현재 WHOIS 시스템에 접근하는 일부 사용자들의 요구는 수용하고 다른 사용자들의 요구는 수용하지 않을 근거를 명확히 제시하기가 쉽지 않았다. 따라서 EWG 는 반드시 적극적으로 억제되어야 할 악의적 인터넷 활동을 제외하고 허용 가능한 것으로 식별된 모든 목적을 RDS 가 어떤 식으로든 수용할 것을 권고한다. EWG 가 권고하는 허용된 목적을 요약하면 아래와 같다.

도메인네임 관리		DNS 투명성
개인 정보 보호		기술적 문제 해결
도메인네임 인증	일반도메인 등록정보 허용된 목적	개인의 인터넷 사용
도메인네임 매매		도메인네임 연구
법적 조치		규정/계약 이행
	오용 억제	

그림 3: 허용된 목적

각 목적마다 기존의 그리고 미래에 가능한 사용 사례가 무수히 많다는 점을 유념해야 한다. EWG는 가능한 모든 사례를 식별하기보다는 일반도메인 등록정보 접근을 원하는 사용자들의 종류와 그 접근 목적을 대략적으로 파악하려는 목적으로 대표적인 샘플들을 찾고자 했다. 그러나 RDS는 반드시 앞으로 생겨날 가능성이 있는 새로운 사용자와 허용된 목적들을 수용할 수 있도록 설계되어야 한다.

EWG가 부록 C에 열거된 사용 사례들을 분석하는 동안 많은 사용자들이 요구하는 데이터 요소는 비슷하지만 목적은 서로 다르다는 것이 분명해졌다. 이러한 요구들 중 일부, 예를 들면 다음과 같은 요구는 대체로 잘 이해되고 있다.

- 도메인네임 등록 여부를 확인하는 기능
- 현재 도메인 상태를 확인하는 기능
- 도메인네임에 관해 누군가에게 연락할 수 있는 기능

그러나, 일부 요구는 매우 일반적이지만 현재의 WHOIS 시스템으로는 쉽게 충족되지 않는다. 그 예를 들자면 다음과 같다.

- 특정 실체가 등록한 모든 도메인을 확인하는 기능(일반적으로 Reverse WHOIS로 불린다)
- 도메인네임 등록 이력 정보를 확인하는 기능(일반적으로 WhoWas로 불린다)

EWG 는 이러한 공통된 요구들을 고려해서 본 보고서에서 상세하게 설명하고 있는 RDS 권고안 개발에 반영했다. 그러나 향후 새로운 요구들이 생겨날 가능성이 있기 때문에 차세대 RDS 시스템은 확장성을 염두에 두고 설계해야 한다. EWG 가 식별한 허용된 목적 그리고 관련된 등록정보, 연락처 및 질의에 대한 요구들에 관해서는 아래에서 좀 더 자세히 정의할 것이다.

목적	정의
도메인네임 관리	이 목적의 범주에는 도메인 소유자 자신의 도메인네임 생성과 관리 그리고 도메인네임 생성, 도메인네임 정보 업데이트, 도메인네임의 이전, 도메인네임의 갱신, 도메인네임 삭제, 도메인네임 포트폴리오 관리 및 도메인 소유자 연락처 정보의 사기적 사용 탐지 등의 모니터링 활동 등이 포함된다. 따라서 이 목적과 관련해 모든 도메인 소유자는 반드시 인증된 RDS 사용자여야 하고 지정 연락처 정보를 비롯해 자신의 도메인네임에 대해 RDS에 공개한 모든 공개 및 제한적 정보에 접근할 수 있다.
개인 정보 보호	이 목적의 범주에는 특정 도메인네임과 연결된 공인 프라이버시/프록시 제공업체의 확인해서 오용을 신고하고, 정보 공개(reveal)를 요청 또는 그러한 제공업체에 연락하는 등의 활동이 포함된다. 이러한 활동을 수행하기 위해 사용자는 쉽게 프라이버시/프록시 제공업체에 연락할 수 있어야 한다. 예를 들면 프라이버시/프록시 제공업체 PBC의 Abuse_URL을 따라가면 업체의 정보 공개(reveal) 과정을 설명하거나 정보 공개(reveal) 신청서 제출 페이지로 연결되어야 한다.
기술 문제 해결	이 목적의 범주에는 이메일 전송 문제, DNS 분석 실패 및 웹사이트 기능 문제 등 도메인네임 사용과 관련된 기술적 문제 해결을 위한 활동들이 포함된다. 사용자는 이러한 문제의 처리를 담당하는 기술 직원에게 연락할 수 있어야 한다. (참고: 문제의 종류에 따라 서로 다른 연락처를 지정해 두면 유용하다. 예를 들면, 이메일 문제의 경우 이메일 관리자에게 문의하게 한다.)
도메인네임 인증	이 목적의 범주에는 인증기관(CA)이 도메인네임으로 신원이 식별된 주체에게 인증서를 발급하는 활동이 포함된다. 이 활동을 위해 사용자는 해당 도메인네임이 인증서 주체에게 등록되었는지 확인할 수 있어야 한다. 그러기 위해 도메인 소유자에 관한 모든 공개 및 제한적 정보에 접근 가능해야 한다.
개인 인터넷 사용	이 목적의 범주에는 소비자 신뢰를 얻기 위해 특정 도메인네임을 사용하는 조직을 확인하거나 소비자 불만이나 민원을 제기하기 위해 그 조직에 연락하는 등의 활동이 포함된다. 그러기 위해서 사용자는 조직의 이름(바람직하게는 신원이 검증된)과 법적(우편) 주소가 필요하며 조직

	및 고객 서비스 연락처를 설명하거나 고객 서비스 문의가 가능한 페이지로 연결되는 Contact URL이 있다면 도움이 될 것이다.

28페이지

목적	정의
기업 도메인네임 매매	이 목적의 범주에는 도메인네임 구입을 문의하고, 다른 도메인 소유자로부터 도메인네임을 취득하고, 실사를 하는 등의 활동이 포함된다. 그러기 위해서 사용자는 도메인 소유자의 조직 및 이메일 주소 그리고 경우에 따라, 가령 도메인 소유자의 이름이나 연락처로 역질의(Reverse Query)를 실행해서 연관된 다른 도메인네임을 파악하기 위해 추가적인 제한 정보에 접근할 필요가 있다.
학술적/공익을 위한 DNS 연구	이 목적의 범주에는 RDS에 공개된 도메인네임과 관련된 공익을 위한 학술 연구 활동이 포함된다. 구체적으로는 도메인 소유자 및 지정 연락처에 관한 공개 정보, 도메인네임의 이력과 상태 및 특정 도메인 소유자가 등록한 도메인네임(역질의) 등을 조사한다. 그러기 위해 사용자는 RDS의 모든 공개 데이터에 접근할 수 있어야 하고 경우에 따라 익명화되어 집약된 형태의 제한적 데이터에 접근할 필요가 있다.
법적 조치	이 목적의 범주에는 도메인 소유자 이름이나 주소를 다른 도메인네임이 사기를 위해 사용하지 않았는지 조사하고, 상표권 침해는 없는지 조사하고, 법적 조치를 취하기 전에 도메인 소유자/ 라이선스권자의 법률 대리인에게 연락한 다음 문제가 만족스럽게 해결되지 않았을 경우 법적 조치를 취하는 등의 활동들이 포함된다. 그러기 위해서 사용자는 공인 프라이버시/프록시 제공업체를 거치지 않고 도메인 소유자/ 라이선스권자의 법률 대리인에게 연락을 취할 수 있어야 한다.
규제 및 계약 이행	이 목적의 범주에는 온라인에서 활동하는 기업에 대한 세무당국의 조사, UDRP 조사, 계약 준수 조사 및 등록정보 에스크로 감사 활동 등이 포함된다. 그러기 위해서 인증된 사용자는 우편주소 및 전화번호와 같이 명시된 목적을 위해 필요한 것으로 여겨지는 일부 제한적 도메인 소유자 연락처 정보 및 도메인네임 데이터 요소에 접근할 수 있어야 한다. 예를 들면 WIPO는 UDRP 분쟁해결을 위해 해당 정보에 접근할 필요가 있다.
범죄 수사 및 DNS 오용 억제	이 목적의 범주에는 오용 사건을 수사 및 해결할 능력이 있는 주체에게 그러한 오용 사건을 신고하거나 공식적인 범죄 수사가 진행되었을 때 도메인네임과 관련된 실체에게 연락하는 등의 활동들이 포함된다. 그러기 위해서 인증된 사용자(예, 사법 기관, 최초 대응자)는, 예를 들면 오용 신고 과정에 대한 설명이나 사고 신고 양식으로 연결되는 URL을 통해 관련 도메인네임을 책임지는 오용 신고 연락처(Abuse Contact)에 빠르고 정확하게 연락할 수 있어야 한다.
DNS 투명성	이 목적의 범주에는 도메인 소유자가 일반 대중을 위한 정보 제공을 중심으로 다양한 종류의 이용 사례를 충족시키기 위해 공개한 등록정보를 문의하는 활동과 관련이 있다. 그러기 위해서 사용자는

	RDS가 제공하는 공개 데이터(공개 데이터에 한함)에 쉽게 접근할 수 있어야 한다. 도메인네임 공개 등록정보가 이처럼 “잡다한(catch all)” 목적을 위해 사용될 지도 모른다는 점을 도메인 소유자에게 반드시 알려야 하며 반드시 공개 데이터로 제한되어야 한다(즉, 이 목적은 제한 데이터 접근을 허용하지 않는다).

표 2. 목적의 정의

이러한 목적들에 필요한 등록정보의 범위를, 관련 도메인네임, 필요한 정보의 종류(등록정보, 연락처 정보, 도메인네임 정보) 및 추가적으로 필요한 질의 등을 포함시켜 좀 더 요약하면 아래 표와 같다.

목적	질의 범위	필요한 연락처	필요한 도메인 소유자 정보	도메인네임 정보	기타 필요한 질의
도메인네임 관리	자체 DN	전체	공개+제한 정보	예	Reverse (자체 데이터) WhoWas (Own DN)
개인 정보 보호	PP DN*	PP	공개 정보	예	없음
기술 문제 해결	모든 DN	기술(Tech)	공개 정보	예	없음
도메인네임 인증	모든 DN	없음	공개+제한 정보	예	없음
개인 인터넷 사용	LP DN*	사업 (Business)	공개 정보	아니오	없음
기업 도메인네임 매매	모든 DN	관리 (Admin)	공개+승인된 제한 정보	예	Reverse (승인된 데이터) WhoWas (모든 DN)
학술적/공익을 위한 DNS 연구	모든 DN	전체	공개+승인된 제한 정보	예	Reverse (승인된 데이터) WhoWas (모든 DN)
법적 조치	모든 DN	법률 (Legal)	공개+승인된 제한 정보	예	Reverse (승인된 데이터) WhoWas (모든 DN)
규제 및 계약 이행	모든 DN	법률 (Legal)	공개+제한 정보	예	Reverse (모든 데이터) WhoWas (모든 DN)
범죄 수사 및 DNS 오용 억제	모든 DN	오용신고 (Abuse)	공개+제한 정보	예	Reverse (모든 데이터) WhoWas (모든 DN)
DNS 투명성	모든 DN	공개(Public)	예	없음	**DNS 투명성**

표 3. 각 목적에 필요한 등록정보의 범위

표 3에서 “승인된 제한 정보(Approved Gated Data)”는 승인된 RDS 사용자만 신청 가능한 데이터로 서비스 약관에 의해 정의되며 다음과 관련해 정의된 정책의 적용을 받는다.

- 제한된 접근에 적격한 사람
- 해당 데이터를 필요로 하는 합법적 이유
- 데이터 사용상의 제한

- 적절한 사용을 위해 요구되는 감시 활동

이처럼 “승인된 제한 데이터”가 필요한 목적들은 RDS 사용자 커뮤니티와의 논의를 통해 좀 더 심도 깊게 분석해서 어떻게 하면 책임성과 프라이버시에 대한 요구의 균형을 유지하면서 그러한 정책들을 합리적으로 정의, 이행 및 시행할 지 판단할 필요가 있다.

그러나 다음의 예들을 통해 그 대략적인 작동 방식을 설명할 수 있을 것이다.

- **학술/공익을 위한 DNS 연구**의 경우 특정 DNS 연구에 관여하는 유명 대학의 연구자가 필요한 제한적 데이터 요소와 어떻게 사용될 것인지를 열거하고, 집약된/익명화된 형태로만 결과를 발표하기로 동의하고 독립심사위원회의 감독을 받아야 한다. 승인된 RDS 사용자는 “공익을 위한 DNS 연구” 수행을 근거로 허가되었기 때문에 특정 제한적 도메인 소유자 데이터 요소에 접근하거나 역질의를 통해 그러한 데이터 요소를 질의할 자격이 주어질 것이다.

- **DN(도메인네임) 매매**를 위한 조사와 관련해 기업 사용자가 도메인네임 구입을 위한 거래에서 판매자가 보유한 도메인네임 자산에 대해 실사를 해야 하는 경우를 생각해 볼 수 있다. 인증 기구(섹션 IV(c), ‘RDS 사용자 인증’에서 정의)의 감시 및 감독 하에 이 사용자는 도메인네임을 구입한다는 사실뿐만 아니라 판매자 “X”에 관한 실사를 위해 RDS 데이터가 필요하며 실사 결과는 오직 이 특정 목적(도메인네임 매매)을 위해서만 사용될 것임을 증명해야 할 것이다. 이러한 종류의 실사를 위해 DNS 사용 승인을 받았기 때문에 승인된 RDS 사용자는 역질의를 통해 판매자 “X”와 연결된 승인된 제한 정보로 도메인네임을 검색할 자격을 얻게 될 것이다. 부록 E에서 좀 더 자세히 다룰 것이다.

- **법적 조치**와 관련한 조사의 사례로 면허가 있는 변호사가 상표권 침해 조사에 관여하는 경우를 생각해 볼 수 있다. 인증 기구(섹션 IV(c), ‘RDS 사용자 인증’에서 정의)의 감시 및 감독 하에, 이 사용자는 잠재적인 법적 조치를 위해 조사를 하고 있으며, 조사 대상 “Y”에 관한 조사를 위해 RDS 데이터가 필요하고 반환된 모든 데이터는 오직 이 목적을 위해서만 사용될 것임을 입증해야 할 것이다. 이러한 종류의 상표권 침해 조사를 위해 DNS 사용 승인을 받았기 때문에 승인된 RDS 사용자는 역질의를 통해 조사 대상 “Y”와 연결된 승인된 제한 데이터로 도메인네임을 검색할 자격을 얻을 것이다. 부록 E에서 좀 더 자세히 다룰 것이다.

이러한 목적과 관련된 데이터와 승인된 제한 정보의 역할 그리고 사용자에게 책임을 묻고 오용을 방지하기 위한 보호장치들과 관련해 부록 E, ‘제한적 및 무단 접근의 실례(Illustrations of Gated & Unauthenticated Access)’에서 좀 더 자세히 다룬다.

EWG는 RDS 사용자와 허용된 목적을 조사한 끝에 다음과 같은 목적에 기반한 등록정보 접근을 위한 기본 원칙을 수립하게 되었다.

31페이지

번호	허용된 목적 원칙
1.	ICANN는 반드시 등록정보의 목적과 허용된 용도를 설명한 사용자 친화적 정책을 한 장소에서 발표함으로써 도메인 소유자에게 데이터 수집 이유와 처리 및 사용 방식을 명확하게 알려야 한다.
2.	반드시 RDS의 허용가능/허용불가 용도를 명확하게 정의해야 한다.
3.	RDS는 반드시 다음과 관련된 사용을 포함해서 허용 가능한 것으로 정의된 목적을 지원해야 한다. • 도메인 소유자 및 특정 목적을 위해 지정된 연락처 식별 • 특정 목적을 위해 지정된 연락처와의 커뮤니케이션 • 도메인 소유자가 도메인네임에 관해 공개한 데이터의 사용 • 등록정보 중에서 특정 목적을 위해 필요한 부분 검색
4.	RDS는 반드시 새로운 사용자와 향후 새롭게 생겨날 가능성이 있는 허용된 목적을 수용할 수 있도록 설계해야 한다. • 신청 과정을 반드시 정의해야 한다. • 신청서는 반드시 정해진 기준을 근거로 심사해야 한다. • 심사를 통과한 신청서는 반드시 정책 개발 과정을 통해 결정된 다수이해관계자 심사 위원회의 평가 및 승인을 거쳐야 한다. • 승인된 신청서는 반드시 RDS 프라이버시 정책에 추가하고 정책으로 정한 바에 따라 주기적으로(예, 분기별, 연별) 이행 일정을 잡는다. 참고: 새 데이터 요소 추가를 위한 과정은 섹션 VI, '데이터 요소'를 참조한다.
5.	RDS는 반드시 적극적으로 억제해야 할 악의적 인터넷 활동을 제외하고 허용가능한 것으로 식별된 모든 목적을 *어떤 식으로든* 수용해야 한다. EWG가 권고하는 허용된 목적이 표 1, 'RDS 사용자와 목적' 그리고 그림 3, '허용된 목적'에 요약되어 있다.
6.	일반도메인 등록정보는 오직 허용된 목적을 위해서만 수집, 검증 및 공개해야 하며 일부 데이터 요소는 오직 적절한 사용을 책임질 수 있는 인증된 요청자에게만 접근을 허용해야 한다.
7.	모든 도메인 소유자는 반드시 지정된 연락처 정보를 포함해 자신의 도메인네임에 관해 RDS에 공개된 모든 공개 및 제한 정보에 접근할 수 있어야 한다.

31페이지

d. RDS에 관여하는 이해관계자

다음 표는 일반도메인 등록정보의 수집, 저장, 공개 및 사용에 관여하는 다양한 이해관계자와의 관련 목적을 요약한 것이다. 일부 이해관계자는 데이터를 제공(예, 도메인 소유자)하는 반면 다른 이해관계자들은 데이터를 수집/저장(예, 검증기관, 등록대행자, 관리기관)하거나 데이터를 공개(예, RDS 제공업체, 인증된 프라이버시/프록시 서비스 제공업체)한다. 그러나, 대부분의 이해관계자들은 데이터를 요청하는 당사자(예, 브랜드 소유자 및 그 대리인)이거나 공개된 데이터에 의해 신원이 확인되거나, 연락이 취해지거나 달리 영향을 받는 당사자(예, 도메인네임 오용 신고 연락처)이다. 아래 표는 다양한 이해관계자들 중에서도 RDS의 영향을 받을 가능성이 가장 큰 당사자들을 보여주기 위한 것이다. 그러나 등록정보가 관련된 특정 거래에서 여기서 열거하지 않은 추가적인 이해관계자가 충분히 존재할 수 있다.

이해관계자	목적
도메인네임의 오용 신고 연락처	범죄 수사 및 오용 억제
인수 회사	기업 도메인네임 매매
인수 회사의 대리인/변호인	기업 도메인네임 매매
주소 검증 서비스	도메인네임 관리
도메인 소유자의 대리인	도메인네임 관리
브랜드 소유자(Brand Holder)	규제/계약 이행
브랜드 관리 서비스 제공업체	도메인네임 관리
브랜드 소유자(Brand Owner)	기업 도메인네임 매매
인증 기관	도메인네임 인증
고소인	규제/계약 이행
웹사이트에서 상품을 구매하는 소비자	개인 인터넷 사용
웹사이트에 접근하는 인터넷 사용자	개인 인터넷 사용
도메인 중개인	기업 도메인네임 매매
도메인 구매자	기업 도메인네임 매매
사기 피해자	법적 조치
사기 피해자 대리인	법적 조치
정부 기관의 직원	규제/계약 이행
ICANN 계약관리(Compliance)	규제/계약 이행
독립심사위원회(IRB)	학술적/공익을 위한 DNS 연구
인터넷 서비스 제공업체	기술 문제 해결 범죄 수사 및 오용 억제
조사자	개인 인터넷 사용

사법 인력	범죄 수사 및 오용 억제 법적 조치
프라이버시/프록시 제공업체 연락처	개인 정보 보호 도메인네임 관리 학술적/공익을 위한 DNS 연구
기술 담당 연락처(Listed Tech Contacts)	개인 정보 보호 도메인네임 관리 학술적/공익을 위한 DNS 연구
관리담당 연락처(Listed Admin Contacts)	규제/계약 이행 도메인네임 매매 도메인네임 관리 학술적/공익을 위한 DNS 연구
법률담당 연락처(Listed Legal Contacts)	법적 조치

33페이지

	규제/계약 이행 학술적/공익을 위한 DNS 연구
사업 담당 연락처(Listed Business Contacts)	개인 인터넷 사용 도메인네임 관리 학술적/공익을 위한 DNS 연구
오용 신고 연락처(Listed Abuse Contacts)	범죄 수사 및 오용 억제 도메인네임 관리 학술적/공익을 위한 DNS 연구
온라인 서비스 제공업체	기술 문제 해결
Op/Sec 서비스 제공업체	범죄 수사 및 오용 억제
연구 후원 조직	공익을 위한 DNS 네임 연구
조사 대상 사람/실체	규제/계약 이행
프라이버시/프록시 서비스 고객	기업 도메인네임 매매 도메인네임 관리 기술 문제 해결 규제/계약 이행 개인 정보 보호
프라이버시/프록시 서비스 제공업체	범죄 수사 및 오용 억제 기업 도메인네임 매매 도메인네임 관리 공익을 위한 DNS 네임 연구 기술 문제 해결 법적 조치 개인 정보 보호 규제/계약 이행 기술 문제 해결
RDS 제공업체	모든 목적
도메인 소유자	모든 목적
도메인 소유자의 법률 담당 연락처	법적 조치 규제/계약 이행
등록대행자	기업 도메인네임 매매 도메인네임 관리 공익을 위한 DNS 네임 연구 개인 인터넷 사용 법적 조치 개인 정보 보호 규제/계약 이행 기술 문제 해결

	범죄 수사 및 오용 억제
관리기관	모든 목적
문제 신고자	기술 문제 해결
연구자	학술/공익을 위한 DNS 연구
재판매자	도메인네임 관리 범죄 수사 및 오용 억제
문제 해결자	기술 문제 해결
법적 조치/소송 대상	개인 인터넷 사용
연락처를 찾는 제3자	법적 조치 개인 정보 보호
보안 크리덴셜 승인자	개인 정보 보호
보안 크리덴셜 수령자	개인 정보 보호
UDRP 토론자	규제/계약 이행
UDRP 제공업체	규제/계약 이행

검증기관	모든 목적
오용 희생자	범죄 수사 및 오용 억제
웹 호스팅 제공업체	기술 문제 해결

표 4. 대표적인 이해관계자

e. 목적별 연락처 원칙(Purpose-Based Contact Principles)

인터넷 도메인네임의 존재와 공공 영역(public zone) 안에서 이루어지는 사용은 잠재적으로 전세계 제3자들에게 외부 효과를 발생한다. 오용 행위부터 기술 문제와 권리 침해 및 크고 작은 도메인네임 관련 문제들까지 세계 어딘가에서 제3자가 특정 도메인네임과 연결된 사람 또는 조직에 연락해야 할 합법적 이유는 수 없이 많다.

동시에 도메인 소유자들은 프라이버시를 필요로 하고 그럴 자격이 주어지기도 한다(해당 관할 지역에 따라). 그들은 구체적인 연락처 정보가 공개되길 원하지 않을 지도 모른다. 뿐만 아니라 도메인 소유자들은 제3자가 문제를 제기했을 때 예를 들어 도메인네임의 DNS 구성이나 상표권 분쟁 대응과 같은 문제를 해결할 최적의 인물이나 실체가 아닌 경우가 많다. 따라서 도메인 소유자 정보만 제공해서는 도메인네임과 관련된 문제를 해결하고자 하는 제3자를 만족시키지 못할 가능성이 높다.

다양한 성격의 잠재적 문제들은 내용에 있어서나 시기에 있어 서로 다른 대응을 필요로 하며 특정 도메인과 연관된 서로 다른 사람 및/또는 조직에 의해 논리적으로 해결되는 상황들이 종종 있다. 그러나 어떤 도메인네임이든 외부의 질의에 응답하고 그 도메인네임의 존재나 운영으로 인해 영향을 받는 외부 행위자들의 허용된 목적을 위한 연락담당자가 될 하나 이상의 정확한 공개 연락처를 반드시 제공해야 한다.

응답의 적시성(Timeliness of response)은 특정 연락처 유형에 관한 정책을 수립할 때 바람직한 목표가 될 수 있다. 그러나, 그러한 목표는 응답하는 실체가 져야 하는 부담과 비교해서 균형을 맞춰야 한다. 시스템 조작, 부적절한 요청 또는 의도적인 오버로딩 등으로 인해 그러한 연락처에 어떠한 불이익이 발생해서는 안 된다. 요청자들을 위해 특정 목적(예, 오용 문제 처리, UDRP 제소 대응)을 위한 연락처와 연결되지 못했을 때 의존할 수 있는 프로세스를 마련할 필요가 있다. 그러한 프로세스에 응하지 못할 경우 명문화된 절차를 통해 해당 연락처 및 관련 도메인네임을 정지 및/또는 삭제할 가능성도 있다. 그러나 응답의 적시성을 위한 구체적인 정책 목표는 본 보고서의 범주를 벗어나는 주제이다.

35페이지

번호	목적별 연락처 원칙
8.	등록된 모든 도메인네임을 위해 적어도 하나 이상의 목적별 연락처(PBC)를 제공해야 하며 모든 의무적 PBC를 위한 모든 의무적 데이터 요소의 집합을 공개해야 한다. PBC는 구문론적으로 정확하고 명시된 모든 허용된 목적의 요구를 충족시킬 수 있도록 실질적으로 연결 가능해야 한다.
9.	도메인네임 등록 과정에서 반드시 도메인 소유자 연락처 ID[6]를 각 목적을 위한 PBC ID 기본값으로 사용해야 한다. 도메인 소유자에게 모든 허용된 목적에 대해 반드시 공지하고 특정 또는 모든 목적을 위한 도메인 소유자의 연락처 ID를 변경하는 등 각 목적별로 다른 PBC ID를 지정할 기회를 제공해야 한다.
10.	목적별 연락처가 꼭 도메인 소유자일 필요는 없으며 도메인 소유자 정보 접근은 다른 정책에 따라 매우 제한적일지도 모른다. PBC가 반드시 사람일 필요는 없으며 여러 가지 목적을 위해 지정된 연락담당자 나타낸다는 점을 유념한다.
11.	적용 가능한 모든 목적을 위해 유효한 PBC를 제공할 때까지 도메인네임은 절대 활성화되어서는(글로벌 DNS에 올려서는) 안 된다. 지정된 목적을 위한 PBC가 유효하지 않을 경우 도메인 소유자가 새롭게 유효한 연락처를 지정할 기회를, 즉 PBC 업데이트를 공지하고 그에 합당한 시간을 제공해야 한다. 위의 9번 원칙에 따라, 각 목적을 위해 반드시 도메인 소유자의 연락처 ID를 기본 PBC ID로 사용해야 한다. 정해진 시한 내에 유효한 PBC ID를 제공하지 못할 경우 명문화된 절차에 따라 도메인네임이 정지 및/또는 삭제될 가능성도 있다. (검증 요건은 섹션 V를 참조한다.)
12	PBC ID는 모든 허용된 목적을 위해 선택적으로 제공 가능하며 허용된 목적의 요구를 충족시키기 위한 각 PBC 유형을 위해 수집 및 공개해야 할 데이터 요소를 위해 정해진 요건에 있어 차이가 있다.
13.	도메인 소유자가 지정한 연락처가 특정 도메인 등록을 위해 특정한 역할을 수행할 책임을 수용 또는 거부할 권리를 보장하기 위해 자신의 연락처 ID를 도메인네임의 PBC ID로 공개할 지 여부를 선택(옵트인/옵트 아웃)하는 과정과 정책을 개발해야 한다.

[6] 연락처 ID(Contact ID)는 검색 및 업데이트를 위한 연락처 데이터 블록과 연결된 식별자로 섹션 IV(a), '데이터 요소'와 섹션 V(d), '연락처 ID를 위한 운영 프레임워크'에서 각각 소개 및 정의하고 있다.

14.	“목적별 연락처” 제공을 위한 시스템은 반드시 유연하게 RDS에서 새로운 목적과 연락처 유형을 생성하고 공개할 수 있어야 한다.

번호	목적별 연락처 원칙
	(새 목적의 추가에 관한 자세한 사항은 섹션 III(c)을 참조한다.)

f. 목적별 연락처의 역할과 책임

그림 4와 표 1에서 알 수 있듯이 EWG는 대표적인 이용 사례들을 분석해서 일반도메인 등록정보 접근을 원하는 사용자들의 종류와 현재 그러한 데이터의 허용 가능한 사용 목적들을 식별했다. 목적에 따라 등록정보에 대한 접근성을 제공하기 위해 모든 허용된 목적을 PBC와 매핑시켰다. 예를 들면,

- TM 분쟁이나 기타 도메인네임과 관련한 법적 문제를 처리하기 위해 “법률” 담당 연락처를 지정한다. 이 PBC는 관련 목적들을 위한 연락을 위해 법적 고지서의 수신이 가능한 물리적 주소, 질문을 받기 위한 유효한 이메일 주소나 유효한 전화 또는 팩스 번호를 포함한다.
- 도메인이나 트래픽에서 포착된 오용 사건이나 기타 시간에 민감한 악의적인 인터넷 활동에 관한 문의를 처리하기 위해 “오용 신고(abuse)” 연락처의 지정이 가능하다. 관련 목적을 위한 연락을 위해 이 PBC는 반드시 불만을 접수 및 응답하기 위한 유효한 이메일 주소와 문의 접수를 위한 유효한 전화번호를 포함해야 한다. 또한 PBC는 실시간 대화를 위한 소셜 미디어 및 문자메시지 주소와 문의 접수를 위한 물리적 주소와 팩스 번호 및 오용 신고를 위한 공개 URL을 포함시켜도 된다.

또한 행정, 기술, 공인 프라이버시/프록시 제공업체 및 사업용 연락처 지정을 위한 PBC도 권장된다. 표 5는 식별된 모든 PBC 유형과 책임을 정리한 목록이다. PBC 유형에 따라 요구되는 데이터 요소들은 섹션 IV, 데이터 수집 원칙 20번을 참조한다.

아래 그림에서 보듯이 EWG는 특정 도메인네임을 위해 별도의 PBC를 제공하지 못할 경우 도메인 소유자 자신의 ID 사용을 권고한다. 예를 들면, 특정 도메인네임을 위한 법률 담당 연락처가 없을 경우 도메인 소유자에게 이해관계자들이 이 허용된 목적을 위해 연락을 취할 가능성이 있다는 점을 고지하고 해당 도메인네임과 관련해 그러한 요청을 접수하기 위한 PBC를 지정할 기회를 제공해야 한다.

도메인 소유자가 PBC를 따로 지정하지 않기로 선택할 경우, 그러한 요청은 도메인 소유자의 연락처 ID와 연관된 목적에 요구되는 정보를 사용해서 도메인 소유자에게 전송될 것이다. 도메인 소유자가 그러한 데이터 요소의 공개를 원하지 않는다면 공인 프라이버시/프록시 서비스를 이용해 도메인네임을 등록하는 것도 가능하다. 데이터 요소 원칙 및 PBC에 관한 자세한 논의는 섹션 IV를 참조한다.

		도메인 소유자 연락처 ID (의무적)			
관리 담당 연락처 ID: (의무적, 기본값 = 도메인 소유자 연락처 ID)	기술 담당 연락처 ID (의무적, 기본값 = 도메인 소유자 연락처 ID)	오용 신고 연락처 ID (의무적, 기본값 = 도메인 소유자 연락처 ID)	법률 담당 연락처 ID (의무적, 기본값 = 도메인 소유자 연락처 ID)	프라이버시/프록시(PP) 제공업체 연락처 ID (PP 등록 도메인의 경우 의무적)	사업 담당 연락처 ID (법인 등록 도메인의 경우 권장)

그림 4. RDS 연락처 유형

정책입안자는 모든 사용목적/연락처를 명문화하고 사용목적의 추가, 변경 또는 삭제를 위한 절차를 정의해야 한다.

이러한 PBC 접근법은 연락처 요구가 기본적인 도메인 소유자들을 위한 단순함을 유지하면서도 좀 더 확대된 연락처 요구를 지닌 도메인 소유자들을 위한 추가적인 세부사항을 제공한다. 이 개념을 설명하기 위해 아래에 세 가지 서로 다른, 가상이지만 전형적인 사례를 제시한다.

1.	도메인 소유자가 도메인네임의 유일한 접점으로 도메인 소유자 연락처 ID(Registrant Contact ID)를 명시적으로 지정하는 것이 가능하다. 이 경우, 모든 허용된 목적을 위한 RDS 질의는 각 목적에 따라 이 도메인 소유자 연락처 ID와 연결된 공개 또는 제한 데이터 요소들을 반환할 것이다.	**DN 레코드의 예:** Registrant Contact ID = <reg> Tech Contact ID = <reg> Admin Contact ID = <reg> Abuse Contact ID = <reg> Legal Contact ID = <reg>
2.	도메인 소유자가 공인 프라이버시 서비스(섹션 VII에서 정의)를 사용할 경우 프라이버시/프록시 제공업체 연락처 ID(즉, 프라이버시 서비스 제공업체), 기술 연락처 ID(예, 호스팅 제공업체 또는 ISP) 및 서비스 제공업체의 관리, 오용신고 및 법률 연락처 ID 등 도메인네임을 위해 여러 개의 고유 연락처 ID를 지정할 수 있다. 이 예에서, 기술 담당 연락처(Tech Contact)는 도메인네임과 관련된 모든 기술적 문제의 해결을 책임지며 공인 프라이버시/프록시 제공업체 연락처는 도메인네임과 관련된 모든 프라이버시 서비스(관리, 오용신고 및 법률 연락처로 온 메시지를 도메인 소유자에게 전달하는 등)를 책임진다.	**DN 레코드의 예:** Registrant Contact ID = <reg> PP Contact ID = <pp> Tech Contact ID = <isp> Admin Contact ID = <reg@pp> Abuse Contact ID = <reg@pp> Legal Contact ID = <reg@pp>

3.	법인으로 등록하기로 선택한 도메인 소유자의 경우 법률, 오용신고, 사업 PBC ID 등 특정 도메인네임을 위해 다수의 고유 연락처 ID를 제공하는 것도 가능하다. 이 사례에서 이러한 각각의 사용목적을 위한 RDS 질의는 해당 PBC ID와 연관된 데이터 요소를 반환함으로써 지정된 역할에 대한 책임을 수용한 사람 또는 실체와의 직접적인 접촉이 용이하다. 이 시나리오는, 대규모 조직의 경우 이러한 세부사항을 활용해 연락가능성을 높이고 연락을 하지 못하거나 엉뚱한 곳으로 연락되는 경우를 줄일 수 있어 앞으로 더욱 일반화될 것으로 예상된다.	**DN 레코드의 예:** Registrant Contact ID = <reg> Tech Contact ID = <isp> Admin Contact ID = <admin@reg> Abuse Contact ID = <abuse@reg> Legal Contact ID = <legal@reg> Business Contact ID = <cs@reg>

위의 예를 도식적으로 표현하면 다음과 같다.

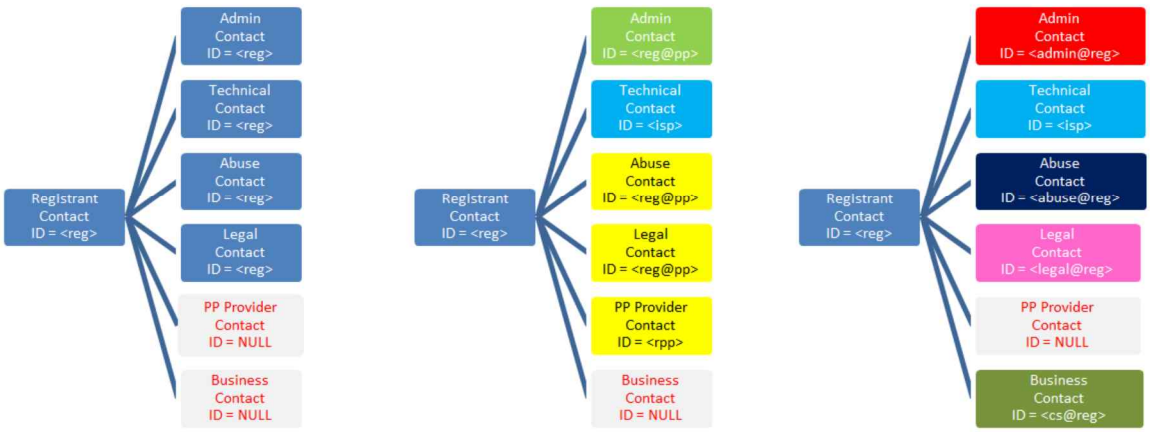


그림 5. 목적별 연락처를 사용한 DN 등록의 예

권장 PBC 목록은 섹션 IV를 그리고 각 허용된 목적 및 관련 PBC에 요구되는 데이터 요소의 전체 목록은 부록 D를 참조한다.

도메인네임에 관한 요청 접수, 그러한 요청의 평가 그리고 도메인 소유자 및 PBC 사이의 계약에 따라 요청을 승인 및/또는 도메인 소유자/라이선스권자에게 고지하는 것도 PBC의 책임이다.

각 PBC가 책임져야 할 사항을 요약하면 다음과 같다.

PBC 유형	잠재적 책임
관리 (Admin)	구입 문의와 도메인네임 이전 등 도메인네임의 취득 및 매매와 관련된 요청 처리
법률 (Legal)	도메인네임에 관한 세무 당국, UDRP 조사자, 계약 준수 조사자 및 법률 대리인의 요청 처리
기술 (Technical	도메인네임과 관련해 웹사이트 중지, DNS 문제, 메일 전송 문제 등에 관한 요청 처리
오용 신고 (Abuse)	피싱, 스팸 및 기타 유해한 인터넷 활동을 포함해 도메인네임과 관련된 DNS 오용 신고 처리.
프라이버시/프록시 (Privacy/	중계/정보공개(Relay/reveal) 요청 처리, 도메인 소유자/라이선스권자를 대신해 도메인네임 오용 민원 처리, LEA의 범죄 활동 수사 지원
비즈니스 (Business)	사업에 관한 정보 및 추가 정보를 얻기 위해 또는 고객 민원을 해결하기 위해 회사에 연락하기 위한 정보 요청 처리

표 5. 각 목적별 연락처의 잠재적 책임

추후 고려 사항: 각 PBC 유형을 위해 복수의 PBC를 지정함으로써 특정 책임자와 직접 연락도 가능하다. 예를 들어, 인터넷 활동 규모가 큰 조직의 경우, 기술적 문제들을 이메일 관리자, DNS 운영자, 웹마스터 등으로 나누어 처리하는 것이 좋을 것이다. 이러한 전문적인 담당자들이 수행하는 임무를 하나의 필드로 분류하고 공개 데이터로 제공해서 도메인 소유자가 지정한 PBC의 구체적인 사용목적을 식별한다. 현재로서는 이 정도로 복잡한 체계는 기대할 수 없겠지만 앞으로의 논의에서 배제해서는 안 된다.

g. RDS 연락처 사용 허가(RDS Contact Use Authorization)

위에서 설명했듯이, 도메인네임 소유자는 적어도 필요한 최소한의 PBC는 반드시 지정해야 한다. 그러한 연락처(담당자)는 반드시 등록된 각 도메인네임을 위해 지정된 역할에 대해 알고 있어야 하고 그러한 역할의 수행에 동의해야 한다.

40페이지

번호	목적별 연락처 사용 허가 원칙
15.	도메인네임 등록이나 도메인네임 업데이트 지연을 막기 위해 각 PBC의 승인은 반드시 확장가능한 실시간 또는 거의 실시간에 가까운 방식으로 이루어져야 한다.
16.	PBC의 무단 사용을 방지하기 위한 정책과 절차를 반드시 수립해야 한다.
17.	PBC 또는 도메인 소유자는 반드시 나중에 승인을 취소할 수 있어야 한다. (자세한 사항은 섹션 V, '검증' 부분을 참조한다.)
18.	도메인 소유자는 반드시 외부/제3자 승인 없이 스스로를 자신의 도메인네임을 위한 PBC로 손쉽게 지정할 수 있어야 한다.

예를 들면, 도메인 소유자가 PBC 연락처 ID와 이 연락처 ID를 책임지는 검증기관에 의해 즉시 그리고 자동으로 검증되는 일회용 토큰을 제공한다. 또는 연락처 승인 과정에 이메일이나 SMS 검증 시스템을 활용하는 방법도 있다.

IV. 책임성 강화

EWG가 권고하는 RDS는 백지 상태에서 시작해서 지금의 만병통치약식 WHOIS 체계를 폐지하고 대신 목적에 따라 차별적으로 검증된 데이터에 접근하게 하는 시스템을 통해 프라이버시, 정보의 정확성 및 책임성을 강화하고자 한다.

EWG는 이러한 제한적 접근 방식이 일반도메인 도메인네임 등록정보의 공개 및 사용에 관여하는 모든 당사자들의 책임성 강화에 도움이 되리라 믿는다. 먼저 RDS는 공개 데이터 요소에 대한 허가 받지 않은 접근을 비롯해 일반도메인 등록정보에 대한 모든 접근과 접근 제한을 기록해 대량 수집(bulk harvesting)하는 행위를 억제한다. 아울러 민감한 데이터 요소의 경우 제한적 접근을 통해 RDS 질의 인증을 신청해서 크리덴셜을 발급받은 요청자에 한해 이용하게 한다. 마지막으로 RDS는 공개 데이터 접근과 제한적 데이터 접근 모두를 감사해서 오용을 최소화하고 부적절한 사용에 대해서는 제재 조치를 취한다. 목적에 따라 적용되는 조건이 달라지기도 한다. 요청자가 조건을 위반할 경우 제재 조치가 적용될 것이다.

많은 ICANN 커뮤니티 구성원들이 EWG가 권고하는 제한적 접근 패러다임의 도입을 위해 완전히 익명으로 접근 가능한 WHOIS 시스템을 폐지하자는 주장에 우려를 표명했다. 일부에서는 익명의 요청자 누구에게나 모든 등록정보를 공개하자고 주장했고 또 일부에서는 등록정보를 거의 또는 완전히 비공개로 해야 한다고 주장했다. 일부에서는 허용된 목적을 위해 접근하려는 요청자를 인증하자는 발상은 지지했지만 가용 데이터 요소, 인증 절차 및 허용된 목적과 관련된 정책을 어떻게 수립하고 다듬어

갈 것인지에 대한 좀 더 구체적인 정보를 요구했다.

41페이지

이처럼 다양한 견해들을 모두 충족시킬 쉬운 해답은 없지만 이번 섹션에서는 이와 관련한 EWG의 권고를 자세히 설명하고자 한다.

a. 데이터 요소 원칙

EWG는 데이터 요소들을 범주화하기 위해 다음의 원칙들을 권고한다..

번호	데이터 요소 원칙
19.	RDS는 반드시 목적에 따른 데이터 요소의 공개를 지원해야 한다. (허용된 목적과 관련된 목적별 연락처(PBC) 목록은 섹션 III을 참조한다.)
20.	수집한 모든 데이터가 공개 정보가 되어서는 안 된다. 공개 여부는 반드시 요청자와 목적에 따라 결정되어야 한다.
21.	원활한 연락을 위해 명시적으로 공개된 PBC 정보를 비롯해 신원이 식별된 최소한의 데이터 집합에 대한 공개적 접근이 반드시 가능해야 한다.
22.	상대적으로 민감하다고 판단되는(위험영향 평가에 따라) 데이터 요소는 반드시 다음과 같이 제한적 접근을 통해 보호해야 한다. • 허용된 목적의 식별 • 요청자/목적의 공개 • 제한적 접근의 오용을 막기 위한 감사/준법
23.	반드시 명시된 목적을 위해 허용된 데이터 요소만을 공개해야 한다.(즉, 응답으로 반환하거나 역질의 및 WhoWas 질의로 검색)
24.	반드시 수집되어야 하는 유일한 데이터 요소는 적어도 하나 이상의 허용된 목적을 가진 요소들이다.
25.	각 데이터 요소는 반드시 일단의 허용된 목적과 연결되어야 한다. • 본 보고서는 허용된 사용, 허용된 목적 및 데이터 요소 요구들의 초기 집합을 식별하고 있다.(섹션 III 및 부록 D 참조). • 각 허용된 목적은 반드시 명확하게 정의된 데이터 요소 접근 및 사용 정책들과 연결할 수 있어야 한다. • 섹션 III에서 명시하듯이 반드시 허용된 목적이 추가로 제안되면 이를 논의하고, 승인될 경우 허용된 목적을 주기적으로 갱신하고, 새로운 목적을 기존의 데이터 요소들과 매핑하기 위한 지속적인 심사 과정을 정의해야 한다. • 데이터 요소가 추가로 제안되면 이를 논의하고, 필요할 경우 정의된 데이터 요소를 갱신해서 기존의 허용된 목적과 매핑하기 위한 정책 정의 과정을 반드시 마련해야 한다.

42페이지

번호	데이터 요소 원칙
26.	반드시 알려진 사용 사례(본 문서에 반영된)와 위험 평가(RDS 구현 전 완료 예정)를 기초로 수집, 저장 및 공개해야 할 최소한의 데이터 요소 목록을 결정해야 한다.
27.	모든 관리기관 및 검증기관들은 반드시 그들이 수집하고 RDS에 제공하는 데이터 요소 집합 전부를 저장해야 한다.(섹션 VII, 가능한 RDS 모형 부분을 참조한다.)

1단계: 데이터 수집

허용된 사용목적을 위해 데이터를 선택적으로 공개하려면 데이터를 먼저 수집해야 한다. 도메인네임 등록시 데이터 수집과 관련해 다음의 원칙들을 권고한다.

번호	데이터 수집 원칙
28.	섹션 VI에 제시한 상위의 법적 원칙을 지원하기 위해 등록대행자와 검증기관들은 도메인 소유자 및 목적별 연락처를 위해, 해당 관할지역의 정보보호법에 따라 데이터 수집시 미리 공개한 허용가능한 사용목적을 위한 데이터 사용에 동의할 기회를 제공해야 한다. 정책 수립시 이 원칙은 반드시 상위에 있는 이러한 법적 원칙들의 넓은 맥락 안에서 다루어야 한다.[7]
29.	기본적인 도메인 관리 요구를 위해 관리기관 및 등록대행자 그리고 도메인 소유자는 반드시 도메인네임을 등록할 때 각각 다음 데이터 요소를 의무적으로 수집 및 제공해야 한다. a. 도메인네임 b. DNS 서버 c. 도메인 등록인 이름 d. 도메인 등록인 유형 다음과 같이 도메인 등록인 이름으로 식별된 실체의 종류를 표시한다. 등록정보 요건을 적용할 때 사용한다. **미신고(Undeclared)** – 다음 옵션 중에서 어떤 것도 선택하지 않았을 때 기본값으로 적용되며 RDS에서 자연인과 유사한 방식으로 처리될 것이다. **프라이버시/프록시 제공업체** – 공인 프라이버시/프록시 제공업체를 통한 도메인네임 등록 시, 반드시 선택해야 한다. 이 옵션을 선택한 경우 PP PBC에 중계/정보공개(relay/reveal) 요청을 올리기 위해

[7] 한 명의 EWG 멤버를 제외하고 거의 만장일치로 본 내용을 지지했다.

	공인 프라이버시/프록시 제공업체의 연락처 ID 역시 반드시 제공해야 한다.

43페이지

번호	데이터 수집 원칙
	법인 – 자연인도 프록시 제공업체도 아닌 실체가 등록한 도메인네임인 경우에 선택이 가능하다. 이 옵션을 선택했을 때 소비자 문의와 불만을 처리하기 위해 지정된 Business PBC의 연락처 ID도 반드시 함께 제공해야 한다. (이 표 아래 참고를 참조한다.) **일반인** – 일반인이 등록한 도메인네임의 경우에 선택이 가능하다. 이 옵션을 선택한 경우, 프라이버시/프록시 PBC나 Business PBC 모두 정의할 필요가 없고 도메인 소유자 이름과 주소는 해당 데이터 주체의 관할권에 적용되는 정보보호법에 따라 개인 정보로 취급될 것이다. e. 도메인 소유자 연락처 ID(Registrant Contact ID) 검증 중 각 도메인 소유자 연락처에 할당된 고유 ID[이름 + 주소](연락처 ID의 자세한 정의와 어떻게 검증기관을 통해 생성되어 도메인네임 등록을 위해 사용되는지에 관해서는 섹션 V 를 참조한다.) f. 도메인 소유자 우편 주소(Registrant Postal Address) 지번, 시, 주/지방, 우편번호, 국가(해당사항이 있는 경우)와 같은 데이터 요소를 포함한다. g. 도메인 소유자 이메일 주소(Registrant Email Address) h. 도메인 소유자 전화(Registrant Phone) 다음의 데이터 요소를 포함한다: 전화번호, 내선(해당하는 경우)
30.	a. 도메인 소유자의 프라이버시를 보호하고 연락을 용이하게 하기 위해 등록대행자는 반드시 등록된 모든 도메인네임을 위한 목적별 연락처(PBC)를 수집하고 도메인 소유자는 해당 정보를 제공해야 한다. b. 도메인 소유자는 특정 허용가능한 사용목적을 위해 프라이버시/프록시의 PBC나 허가된 제3자 PBC를 지정하는 방법을 선택해도 된다(섹션 III 참조). c. 각 허용된 목적과 관련된 연락을 위해, 검증기관이 생성한 후 도메인네임과 연결시킨 PBC는 반드시 다음과 같은 최소한의 의무적 데이터 요소 요건을 충족해야 한다. Tech Contact(기술 연락처): 이메일 주소 Admin Contact(관리 연락처): 조직, 이메일 주소 Legal Contact(법률 연락처): 조직, 이메일 주소, 전화번호, 우편 주소 Abuse Contact(오용 신고 연락처): 이메일 주소, 전화번호

	Business Contact(사업 담당 연락처)[8]: 조직, 우편 주소

[8] Registrant Type = Legal Person(도메인 소유자 유형 = 법인)일 경우 연락처는 의무적이다.

44 페이지

번호	데이터 수집 원칙
	Privacy/Proxy Provider Contact(프라이버시/프록시 제공업체 연락처)[9]: 조직, 이메일 주소, Contact_URL, Abuse_URL d. 도메인 등록인이 각 허용된 목적을 위한 PBC를 지정하지 않을 경우, 그러한 PBC를 위한 기본값으로 반드시 도메인 소유자 자신의 연락처 ID를 사용해야 한다. (대신 도메인 소유자는 공인 프라이버시/프록시 서비스를 사용하거나 PBC를 지정하는 방법도 선택할 수 있다.) 도메인 소유자의 연락처 ID를 PBC ID로 사용할 경우 위에 명시한 의무적인 PBC 데이터 요소 요건을 충족시키기 위해 도메인 소유자 정보 수집 및 공개 요건이 더욱 까다로워 질 것이다.
31.	필요 이상의 데이터 수집을 피하려면, 위의 29번과 30번 원칙에서 열거하지 않고 적어도 하나 이상의 허용된 목적을 위해 사용되는, 도메인 소유자가 제공한 다른 모든 데이터는 반드시 도메인 소유자의 재량에 따라 선택적으로 수집되어야 한다. 도메인 소유자가 그렇게 선택할 경우 검증기관, 관리기관 및 등록대행자는 반드시 해당 데이터의 수집 및 저장을 허용해야 한다.
32.	인터넷 안정성을 향상시키기 위해 관리기관과 등록대행자는 RDS에 다음과 같은 의무적 데이터 요소를 반드시 제공해야 한다. a. 등록 상태 b. 클라이언트 상태(등록대행자가 설정) c. 서버 상태(관리기관이 설정) d. 등록대행자 e. 등록대행자 관할권 f. 관리기관 관할권 g. 등록 계약서 언어 h. 생성 날짜 i. 등록대행자 만료 날짜 j. 갱신 날짜 k. 등록대행자 URL l. 등록대행자 IANA 번호 m. 등록대행자 오용 신고 연락처 전화번호 n. 등록대행자 오용 신고 연락처 이메일 주소 o. 민원 제기 사이트 URL(URL of Internic Complaint Site)
33.	TLD별 데이터 요소를 위해 TLD 관리기관은 반드시 데이터 수집

[9] Registrant Type = Privacy Proxy Provider(도메인 소유자 유형 = 프라이버시/프록시 제공업체)일 경우에만 연락처가 의무적이다.

	정책(이러한 상위 원칙에 부합하는)을 수립 및 공표하고 이러한 TLD별 데이터

45페이지

번호	데이터 수집 원칙
	요소의 검증 책임을 져야 한다.
34.	검증기관, 관리기관 및 등록대행자는 내부용으로 추가적인 데이터 요소를 수집, 저장 또는 공개할 수 있으며 RDS와는 절대 공유하지 않는다.[10]

참고: EWG는 오랜 논의 끝에 **도메인네임 목적(Domain Name Purpose)**을 데이터 요소로 추가하는 것을 권고하지 않기로 했다. 대신 EWG는 이 목적과 관련된 목표를 위한 원칙들을 권고하고 스스로를 상업 활동에 관여하는 **법인**으로 식별한 도메인 소유자가 명확한 **사업 PBC(Business PBC)**를 공개하는 방안을 권고한다. 이로써 많은 상업적 인터넷 사용자들이 소비자 신뢰를 높이기 위해 좀 더 일관성 있게 데이터 요소를 공개하는 반면 도메인 등록인들이 궁극적으로 스스로 이 유형을 선택하는 결과를 가져올 것이며 Domain Name Purpose = Commercial 또는 Non- Commercial를 두고 엄격한 준수를 세계적으로 시행하기란 거의 불가능할 것이다.

2단계: 데이터 공개

수집된 데이터는 허용된 목적을 위해 선택적으로 공개할 수 있다. 정보 공개 문의를 받았을 때 지침이 될 다음과 같은 원칙들을 권고한다.

번호	데이터 공개 원칙
35.	도메인 등록인들의 프라이버시를 최대한 보호하기 위해 도메인 소유자가 제공한 데이터는 공개 접근에 수반되는 위험을 능가하는 타당한 필요성이 있는 경우가 아니라면 기본적으로 반드시 제한적으로 접근을 허용해야 한다. • 도메인 소유자는 고지에 의한 동의(informed consent)를 통해 도메인 소유자가 제공한 데이터에 대한 제한적 접근 여부를 선택할 수 있다.
36.	인터넷 안전성 강화를 위해 모든 관리기관 또는 등록대행자가 제공한 등록 정보는 허용할 수 없는 위험을 초래하지 않는 이상 반드시 항상 공개 접근을 허용해야 한다. • 도메인 소유자는 아래와 같은 기본적인 도메인 관리를 위한 경우를 제외하고 관리기관/등록대행자가 제공한 데이터에 대한 제한적 접근 여부를 선택할 수

[10] 예를 들면, 고객이 등록할 때 사용한 IP 주소, 도메인네임의 EPP 전송키 생성을 요청하기 위한 링크 및 고객의 계정과 연결된 결제 데이터 등이 있다. 내부용 데이터는 RDS에 의해 표준화되기 보다는 관리기관 및 등록대행자가 개인적으로 정의한다.

	있다.
37.	연락가능성(reachability)을 극대화하기 위해 기본적으로 모든 PBC는 반드시 공개 접근을 허용해야 한다.

46페이지

번호	데이터 수집 원칙
	• 연락처 보유자(Contact Holder)[11]는 지정된 목적을 위해 요구되는 데이터가 아니라면 어떤 PBC 데이터든 제한적 접근 여부를 선택할 수 있다.(자세한 사항은 표 5를 참조한다.)
38.	기본적인 도메인 관리 요구를 위해 다음과 같이 의무적으로 수집하고 공개해도 위험성이 낮은 도메인 소유자 제공 데이터들은 반드시 최소 공개 데이터 집합에 포함되어야 한다. a. 도메인네임(Domain Name) b. DNS 서버 c. 도메인 소유자 유형(Registrant Type) d. 도메인 소유자 연락처 IC(섹션 V에서 정의) e. 도메인 소유자 이메일 주소 f. 기술 담당 연락처 ID(Tech Contact ID) g. 관리 담당 연락처 ID(Admin Contact ID) h. 법률 담당 연락처 ID(Legal Contact ID) i. 오용 신고 연락처 ID(Abuse Contact ID) j. 프라이버시/프록시 제공업체 연락처 ID(Privacy/Proxy Provider Contact ID) (Registrant Type = Privacy/Proxy Provider인 경우에만 의무적) k. 사업 담당 연락처 ID(Business Contact ID) (Registrant Type = Legal Person인 경우에만 의무적)
39.	단순함과 연락가능성 사이의 균형을 맞추기 위해, 도메인 등록인이 의무적 PBC를 제공하지 않을 경우, 도메인 등록인의 연락처 ID가 PBC로 사용될 것이며 도메인 등록인의 데이터 요소들이 해당 도메인네임의 기술(Tech), 관리(Admin), 법률(Legal) 및 오용신고(Abuse) 연락처로 공개될 것임을 반드시 도메인 등록인에게 고지해야 한다. 도메인 등록인은 하나 이상의 제3자

[11] 섹션 Ⅲ(g), 'RDS 연락처 사용 허가'에 따라 지정된 PBC는 특정 도메인네임 등록 시 반드시 연락처 ID의 사용을 허가해야 한다. 또한 연락처 보유자(Contact Holder)는 자신의 정보를 해당 목적을 위해 공개/제한적으로 사용하는 데 동의한다. 그러나, 사전 검증된 PBC가 특정 목적에 적합한 의무적/공개 데이터 요소를 포함하지 않은 경우 도메인네임 등록 과정에서 해당 목적을 위한 PBC로 지정하지 못한다.

	PBC를 명시하거나 공인 프라이버시/프록시 서비스(이 경우 이들 서비스의 주소가 대신 제공될 것이다)를 이용해서 이러한 정보 공개를 피할 수 있다.
40.	TLD별 데이터 요소의 경우, TLD 관리기관이 데이터 공개 정책(상위의 원칙에 부합하는)을 수립 및 공표하고 제한적 TLD별 데이터 요소를 위해 허용된 목적을 식별할 책임이 있다.

데이터 요소 분류

위의 원칙들을 토대로 EWG가 권고하는 각 RDS 데이터 요소 분류에 대해 다음의 표에서 상세히 설명한다.

- 각 데이터 요소의 수집이 의무적(M) 사항인지 선택적(O) 사항인지의 여부

[1] 도메인 소유자로부터 수집하는 데이터 관련: 의무적(M)이라 함은 반드시 등록대행자/검증기관이 데이터를 요청하고 도메인 소유자는 제공해야 함을 의미하고 선택적(O)이라 함은 등록대행자/검증기관이 반드시 데이터를 요청해야 하지만 데이터 제공 여부는 도메인 소유자의 재량임을 의미한다.

[2] 목적별 연락처 보유자로부터 수집하는 데이터 관련: 의무적(M)이라 함은 등록대행자/검증기관이 반드시 데이터를 요청해야 하고 연락처 보유자는 제공해야 함을 의미하고, 선택적(O)이라 함은 등록대행자/검증기관이 반드시 데이터를 요청해야 하지만 데이터 제공 여부는 연락처 보유자의 재량임을 의미한다.

권고(R)라 함은 등록대행자/검증기관이 반드시 데이터를 요청해야 하지만 “최고(best)” 및 “우수(good)” 권고 사례를 반영하기 위해 데이터 제공 여부는 연락처 보유자의 재량임을 의미한다.[12]

[3] 관리기관 및 등록대행자가 RDS에 제공하는 데이터 관련: 의무적(M)이라 함은 관리기관/등록대행자가 반드시 데이터를 제공해야 함을 의미하고 선택적(O)이라 함은 데이터를 제공할 수도 하지 않을 수도 있음을 의미한다.

- 각 데이터 요소에 대한 접근이 공개적(P)[인증 여부에 관계없이 누구나 접근가능]인지 제한적(G)[인증된 사용자만이 허용된 목적에 한해 접근 가능]인지

[12] 다양한 PBC 데이터 요소의 공개를 위한 권장 모범 사례들은 EWG 구성원들의 실무 경험을 바탕으로 한다. 의무적 요소들은 그러한 목적을 수행하기 위한 최소한의 운영 요건을 나타낸다. 그러나, 실제로 특정 목적을 위한 의사소통 방법이 존재할 경우(예, 문제 신고를 위한 웹 양식, 기술 스텝에게 연락하기 위한 대체 이메일) 그 대안적 방법이 매우 유용하며 종종 문제 처리를 위해 선호된다. 이것은 PBC에 따라 차이가 있는데, 가령 우편주소는 법률 또는 사업 관련 연락처로는 유용하지만 오용 신고나 기술 관련 문제 해결에는 그다지 유용하지 않다. 따라서 EWG는 각 PBC 유형별로 데이터 요소에 대한 구체적인 권고안을 마련했다.

그리고 도메인 소유자가 그 기본 설정을 변경할 수 있는지 없는지 여부(Y/N).

[4] 도메인 소유자로부터 수집하는 데이터 관련:

P / N은 수집된 데이터 접근이 반드시 공개이고 숨길 수 없음을 의미한다.

P / Y는 수집된 데이터 접근의 기본값은 공개이지만 도메인 소유자가 숨길 수 있음을 의미한다.

G / Y는 수집된 데이터 접근의 기본값은 제한이지만 도메인 소유자가 고지에 의한 동의를 통해 공개로 할 수 있음을 의미한다.

[5] 관리기관 및 등록대행자가 RDS에 제공하는 데이터 관련:

P / N은 제공된 데이터 접근은 반드시 공개이고 숨길 수 없음을 의미한다.

G / N은 제공된 데이터 접근이 반드시 제한임을 의미한다. 이 범주에 속하는 데이터 요소는 존재하지 않는다.

[6] 목적별 연락처 보유자로부터 수집하는 데이터 관련:

P / N은 수집된 데이터의 접근이 반드시 공개이며 숨길 수 없음을 의미한다.

P / Y는 수집된 데이터의 접근의 기본값은 공개이지만 연락처 보유자가 숨길 수 있음을 의미한다.

특정 사용자가 접근 제한 데이터 요소에 접근 가능한가의 여부는 허용된 목적에 의해 결정된다는 점을 유념한다. 도메인 소유자가 기본적으로 접근 제한된 데이터 요소를 공개로 변경할 경우 누구나 접근이 가능하다. 도메인 소유자가 기본적으로 접근이 공개인 데이터 요소를 접근 제한으로 변경할 경우 허용된 목적에 한해 접근이 허용된다.

49페이지

관리기관/등록대행자 제공 데이터	수집 M 또는 O	공개 기본값 P 또는 G	공개 여부 변경가능성	참고 [3]수집 정의 및 [5]공개 정의 참조
등록 상태 (Registration Status)	M	P	N	
DNSSEC 위임 (DNSSEC Delegation)	O	P	N	
클라이언트 상태(등록대행자) (Client Status (Registrar))	M	P	N	등록대행자 수준에 도메인네임에 적용가능한 모든 값을 포함한다. DeleteProhibited, RenewProhibited, TransferProhibited
서비스 상태(관리기관) (Server Status (Registry))	M	P	N	RAA에 없음, 위와 유사하지만 관리기관 수준
등록대행자(Registrar)	M	P	N	
재판매자(Reseller)	O	P	N	
등록대행자 관할권 (Registrar Jurisdiction)	M	P	N	RAA에 없음
관리기관 관할권 (Registry Jurisdiction)	M	P	N	RAA에 없음
등록계약서 언어 (Reg Agreement Language)	M	P	N	RAA에 없음
생성 날짜 (Creation Date)	M	P	N	
원 등록 날짜 (Original Registration Date)	O	P	N	RAA에 없음
등록대행자 만료일 (Registrar Expiration Date)	M	P	N	
갱신 날짜 (Updated Date)	M	P	N	
등록대행자 URL (Registrar URL)	M	P	N	
등록대행자 IANA 번호 (Registrar IANA Number)	M	P	N	
등록대행자 오용신고 연락처 이메일 주소 (Registrar Abuse Contact Email Address)	M	P	N	
등록대행자 오용신고 연락처 전화번호 (Registrar Abuse Contact Phone Number)	M	P	N	
민원 제기 사이트 URL (URL of Internic Complaint Site)	M	P	N	

50페이지

도메인 소유자로부터 수집하는 도메인 소유자 데이터	수집 M 또는 O	공개 기본값 P 또는 G	공개 여부 변경가능성	참고 [3]수집 정의 및 [5]공개 정의 참조
도메인네임 (Domain Name)	**M**	**P**	**N**	
DNS 서버 (DNS Servers)	**M**	**P**	**N**	
도메인 소유자 이름 (Registrant Name)	**M**	G	Y	
도메인 소유자 유형 (Registrant Type)	**M**	**P**	**N**	
도메인 소유자 연락처 ID (Registrant Contact ID)	**M**	**P**	**N**	관리기관 도메인 소유자 ID 대체, RDS에서 검증기관이 발급
도메인 소유자 연락처 검증 상태 (Registrant Contact Validation Status)	**M**	**P**	**N**	신규, 검증기관이 제공
도메인 소유자 연락처 최종 검증 시간 (Registrant Contact Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
도메인 소유자 조직 (Registrant Organization)	O	**P**	Y	도메인 소유자 유형 = 법인 또는 프록시 제공업체일 때 수집
도메인 소유자 회사 식별자(예, 상표명, D-U-N-S) (Registrant Company Identifier (e.g., Trading Name, D-U-N-S))	O	**P**	Y	던앤브래드스트리트 같은 소스가 기업에 발급환 실제 식별자 도메인 소유자 유형 = 법인 일 때 수집 RAA에 없음
도메인 소유자 도로명 주소 (Registrant Street Address)	**M**	G	Y	
도메인 소유자 시 Registrant City	**M**	G	Y	
도메인 소유자 주 (Registrant State/Province)	O	G	Y	2013 RAA에 따라, 모든 “주 (state/Province)” 데이터 요소는 해당사항이 있을 때

				수집
도메인 소유자 우편번호 (Registrant Postal Code)	O	G	Y	2013 RAA에 따라, 모든 “우편번호 (Postal Code)” 데이터 요소는 해당사항이 있을 때 수집
도메인 소유자 국가 (Registrant Country)	**M**	G	Y	
도메인 소유자 전화+내선 (Registrant Phone + Ext)	**M**	G	Y	내선번호는 해당사항이 있을 때 수집
도메인 소유자 대체 전화 + 내선 (Registrant Alt Phone + Ext)	O	G	Y	새로운 옵션, RAA에 없음.
도메인 소유자 이메일 주소 (Registrant Email Address)	**M**	**P**	**N**	
도메인 소유자 대체 이메일 (Registrant Alt Email)	O	**P**	Y	새로운 옵션, RAA에 없음
도메인 소유자 팩스+내선 (Registrant Fax + Ext)	O	G	Y	2013 RAA에 따라, 모든 “팩스(Fax)” 및 “팩스 내선(Fax Ext)” 요소는 해당사항이 있을 때 수집

51페이지

도메인 소유자 SMS (Registrant SMS)	O	G	Y	새로운 옵션, RAA에 없음.
도메인 소유자 IM (Registrant IM)	O	G	Y	새로운 옵션, RAA에 없음.
도메인 소유자 소셜미디어 (Registrant Social Media)	O	G	Y	새로운 옵션, RAA에 없음.
도메인 소유자 대체 소셜 미디어 (Registrant Alt Social Media)	O	G	Y	새로운 옵션, RAA에 없음.
도메인 소유자 연락처 URL (Registrant Contact_URL)	O	G	Y	새로운 옵션, RAA에 없음.
도메인 소유자 오용신고 URL (Registrant Abuse_URL)	O	G	Y	새로운 옵션, RAA에 없음.

목적별 연락처 관리 담당 연락처 (Admin Contact)	**수집 M 또는 O**	**공개 기본값 P 또는 G**	**공개 여부 변경가능성**	**참고** [2]수집 정의 및 [6]공개 정의 참조
목적: DN 구입/판매, 도메인네임 관리, DNS 연구				
관리 연락처 ID (Admin Contact ID)	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	RAA에 없음
PBC 검증 상태 (PBC Validation Status)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 최종 검증 시간 (PBC Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 이름 (PBC Name)	**M**	**P**	**N**	
PBC 조직 (PBC Organization)	**M**	**P**	**N**	
PBC 도로명 주소 (PBC Street Address)	R	**P**	Y	
PBC 시 (PBC City)	R	**P**	Y	
PBC 주 (PBC State/Province)	O	**P**	Y	
PBC 우편번호 (PBC Postal Code)	O	**P**	Y	
PBC 국가 (PBC Country)	**M**	**P**	**N**	
PBC 전화+내선 (PBC Phone + Ext)	O	**P**	Y	
PBC 대체 전화 + 내선 (PBC Alt Phone + Ext)	O	**P**	Y	RAA에 없음

PBC 이메일 주소 (PBC Email Address)	**M**	**P**	**N**	
PBC 대체 이메일 주소 (PBC Alt Email Address)	O	**P**	Y	RAA에 없음
PBC 팩스 + 내선 (PBC Fax + Ext)	O	**P**	Y	
PBC SMS	O	**P**	Y	RAA에 없음
PBC IM	O	**P**	Y	RAA에 없음
PBC 소셜 미디어 (PBC Social Media)	O	**P**	Y	RAA에 없음
PBC 대체 소셜 미디어 (PBC Alt Social Media)	O	**P**	Y	RAA에 없음
PBC 연락처_URL (PBC Contact_URL)	O	**P**	Y	RAA에 없음
PBC 오용신고_URL (PBC Abuse_URL)	O	**P**	Y	RAA에 없음

52페이지

목적별 연락처 법률 담당 연락처 (Legal Contact)	수집 M/R/O	공개 기본값 P 또는 G	공개 여부 변경가능성	참고 [2]수집 정의 및 [6]공개 정의 참조
목적: 법적 조치, 규제/계약 이행, 도메인네임 관리, DNS 연구				
법률 연락처 ID (Legal Contact ID)	**M**	**P**	**N**	RAA에 없음
PBC ID	**M**	**P**	**N**	RAA에 없음
PBC 검증 상태 (PBC Validation Status)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 최종 검증 시간 (PBC Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 이름 (PBC Name)	**M**	**P**	**N**	
PBC 조직 (PBC Organization)	**M**	**P**	**N**	
PBC 도로명 주소 (PBC Street Address)	**M**	**P**	**N**	
PBC 시 (PBC City)	**M**	**P**	**N**	
PBC 주 (PBC State/Province)	O	**P**	Y	
PBC 우편번호 (PBC Postal Code)	O	**P**	Y	
PBC 국가 (PBC Country)	**M**	**P**	**N**	
PBC 전화+내선 (PBC Phone + Ext)	**M**	**P**	**N**	
PBC 대체 전화 + 내선 (PBC Alt Phone + Ext)	O	**P**	Y	Not in RAA
PBC 이메일 주소 (PBC Email Address)	**M**	**P**	**N**	
PBC 대체 이메일 주소 (PBC Alt Email Address)	O	**P**	Y	Not in RAA
PBC 팩스 + 내선 (PBC Fax + Ext)	**R**	**P**	**Y**	
PBC SMS	O	**P**	Y	Not in RAA
PBC IM	O	**P**	Y	Not in RAA
PBC 소셜 미디어 (PBC Social Media)	O	**P**	Y	Not in RAA
PBC 대체 소셜 미디어 PBC Alt Social Media	O	**P**	Y	Not in RAA
PBC 연락처_URL (PBC Contact_URL)	O	**P**	Y	Not in RAA

PBC 오용신고_URL PBC Abuse_URL	O	**P**	Y	Not in RAA

53페이지

목적별 연락처 기술 담당 연락처 (Technical Contact)	**수집 M/R/O**	**공개 기본값 P 또는 G**	**공개 여부 변경가능성**	**참고 [2]수집 정의 및 [6]공개 정의 참조**
목적: 기술 문제 해결, 도메인네임 관리, DNS 연구				
기술 연락처 ID (Technical Contact ID)	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	RAA에 없음
PBC 검증 상태 (PBC Validation Status)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 최종 검증 시간 (PBC Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 이름 (PBC Name)	R	**P**	Y	
PBC 조직 (PBC Organization)	R	**P**	Y	
PBC 도로명 주소 (PBC Street Address)	R	**P**	Y	
PBC 시 (PBC City)	R	**P**	Y	
PBC 주 (PBC State/Province)	O	**P**	Y	
PBC 우편번호 (PBC Postal Code)	O	**P**	Y	
PBC 국가 (PBC Country)	**M**	**P**	**N**	
PBC 전화+내선 (PBC Phone + Ext)	**R**	**P**	Y	
PBC 대체 전화 + 내선 (PBC Alt Phone + Ext)	**R**	**P**	Y	RAA에 없음
PBC 이메일 주소 (PBC Email Address)	**M**	**P**	**N**	
PBC 대체 이메일 주소 (PBC Alt Email Address)	**R**	**P**	Y	RAA에 없음
PBC 팩스 + 내선 PBC Fax + Ext	O	**P**	Y	
PBC SMS	**R**	**P**	Y	RAA에 없음
PBC IM	**R**	**P**	Y	RAA에 없음
PBC 소셜 미디어 (PBC Social Media)	O	**P**	Y	RAA에 없음
PBC 대체 소셜 미디어 PBC Alt Social Media	O	**P**	Y	RAA에 없음
PBC 연락처_URL (PBC Contact_URL)	**R**	**P**	Y	RAA에 없음

PBC 오용신고_URL PBC Abuse_URL	O	**P**	Y	RAA에 없음

54페이지

목적별 연락처 **오용 신고 연락처** **(Abuse Contact)**	**수집** **M/R/O**	**공개** **기본값** **P 또는 G**	**공개 여부** **변경가능성**	**참고** [2]수집 정의 및 [6]공개 정의 참조
목적: 오용 억제, 도메인네임 관리, DNS 연구				
오용 신고 연락처 ID (Abuse Contact ID)	**M**	**P**	**N**	
PBC ID	**M**	**P**	**N**	RAA에 없음
PBC 검증 상태 (PBC Validation Status)	**M**	**P**	**N**	RAA에 없음
PBC 최종 검증 시간 (PBC Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 이름 (PBC Name)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 조직 (PBC Organization)	R	**P**	Y	
PBC 도로명 주소 (PBC Street Address)	R	**P**	Y	
PBC 시 (PBC City)	R	**P**	Y	
PBC 주 (PBC State/Province)	R	**P**	Y	
PBC 우편번호 (PBC Postal Code)	O	**P**	Y	
PBC 국가 (PBC Country)	O	**P**	Y	
PBC 전화+내선 (PBC Phone + Ext)	**M**	**P**	**N**	
PBC 대체 전화 + 내선 (PBC Alt Phone + Ext)	**M**	**P**	**N**	
PBC 이메일 주소 (PBC Email Address)	O	**P**	Y	RAA에 없음
PBC 대체 이메일 주소 (PBC Alt Email Address)	**M**	**P**	**N**	
PBC 팩스 + 내선 (PBC Fax + Ext)	O	**P**	Y	RAA에 없음
PBC SMS	O	**P**	Y	
PBC IM	O	**P**	Y	RAA에 없음
PBC 소셜 미디어 (PBC Social Media)	**R**	**P**	Y	RAA에 없음
PBC 대체 소셜 미디어 (PBC Alt Social Media)	**R**	**P**	Y	RAA에 없음

PBC 연락처_URL (PBC Contact_URL)	O	**P**	Y	RAA에 없음
PBC 오용신고_URL (PBC Abuse_URL)	**R**	**P**	Y	RAA에 없음

55페이지

목적별 연락처 프라이버시/프록시(PP) 제공업체 연락처	**수집 M/R/O**	**공개 기본값 P 또는 G**	**공개 여부 변경가능 성**	**참고** [2]수집 정의 및 [6]공개 정의 참조
목적: 개인 정보 보호, 도메인네임 관리, DNS 연구				
PP 연락처 ID (PP Contact ID)	**M**	**P**	**N**	RAA에 없음
PBC ID	**M**	**P**	**N**	RAA에 없음
PBC 검증 상태 (PBC Validation Status)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 최종 검증 시간 (PBC Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 이름 (PBC Name)	**M**	**P**	**N**	
PBC 조직 (PBC Organization)	**M**	**P**	**N**	
PBC 도로명 주소 (PBC Street Address)	**M**	**P**	**N**	
PBC 시 (PBC City)	**M**	**P**	**N**	
PBC 주 (PBC State/Province)	O	**P**	Y	
PBC 우편번호 (PBC Postal Code)	O	**P**	Y	
PBC 국가 (PBC Country)	**M**	**P**	**N**	
PBC 전화+내선 (PBC Phone + Ext)	**M**	**P**	**N**	
PBC 대체 전화 + 내선 (PBC Alt Phone + Ext)	O	**P**	Y	RAA에 없음
PBC 이메일 주소 (PBC Email Address)	**M**	**P**	**N**	
PBC 대체 이메일 주소 (PBC Alt Email Address)	O	**P**	Y	RAA에 없음
PBC 팩스 + 내선 (PBC Fax + Ext)	O	**P**	Y	
PBC SMS	O	**P**	Y	RAA에 없음
PBC IM	O	**P**	Y	RAA에 없음
PBC 소셜 미디어 (PBC Social Media)	O	**P**	Y	RAA에 없음
PBC 대체 소셜 미디어 (PBC Alt Social Media)	O	**P**	Y	RAA에 없음

PBC 연락처_URL (PBC Contact_URL)	**M**	**P**	**N**	RAA에 없음
PBC 오용신고_URL (PBC Abuse_URL)	**M**	**P**	**N**	RAA에 없음

56페이지

목적별 연락처 사업 담당 연락처 (Business Contact)	**수집 M/R/O**	**공개 기본값 P 또는 G**	**공개 여부 변경가능성**	**참고 [2]수집 정의 및 [6]공개 정의 참조**
목적: 개인 인터넷 사용, 도메인네임 관리, DNS 연구				
사업 담당 연락처 (Business Contact ID)	**M**	**P**	**N**	RAA에 없음
PBC ID	**M**	**P**	**N**	RAA에 없음
PBC 검증 상태 (PBC Validation Status)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 최종 검증 시간 (PBC Last Validated Timestamp)	**M**	**P**	**N**	신규, 검증기관이 제공
PBC 이름 (PBC Name)	**M**	**P**	**N**	
PBC 조직 (PBC Organization)	**M**	**P**	**N**	
PBC 도로명 주소 (PBC Street Address)	**M**	**P**	**N**	
PBC 시 (PBC City)	**M**	**P**	**N**	
PBC 주 (PBC State/Province)	O	**P**	Y	
PBC 우편번호 (PBC Postal Code)	O	**P**	Y	
PBC 국가 (PBC Country)	**M**	**P**	**N**	
PBC 전화+내선 (PBC Phone + Ext)	R	**P**	Y	
PBC 대체 전화 + 내선 (PBC Alt Phone + Ext)	O	**P**	Y	RAA에 없음
PBC 이메일 주소 (PBC Email Address)	R	**P**	Y	
PBC 대체 이메일 주소 (PBC Alt Email Address)	O	**P**	Y	RAA에 없음
PBC 팩스 + 내선 PBC Fax + Ext	O	**P**	Y	
PBC SMS	O	**P**	Y	RAA에 없음
PBC IM	O	**P**	Y	RAA에 없음
PBC 소셜 미디어 (PBC Social Media)	O	**P**	Y	RAA에 없음

PBC 대체 소셜 미디어 (PBC Alt Social Media)	O	**P**	Y	RAA에 없음
PBC 연락처_URL (PBC Contact_URL)	**R**	**P**	**Y**	RAA에 없음
PBC 오용신고_URL PBC Abuse_URL	O	**P**	Y	RAA에 없음

또한 EWG는 이러한 목적별 분류가 실제로 정의된 목적을 위해 적절한 데이터 수집 및 공개로 이어지는지 확인하기 위해 광범위한 위험/영향 분석을 실시할 것을 재차 권고한다.

2013 RAA와의 조율과 새로운 데이터 요소

시스템의 전환과 이해를 돕기 위해서 EWG가 권고하는 데이터 요소의 명칭들을 2013 RAA에 식별된 명칭들과 비교해 가능한 일치되도록 조정했다(예를 들면, DNSSEC 위임, RDS 만료 날짜). 그러나 2013 RAA에서 연락처 데이터 요소를 위해 사용된 명칭들은 목적별 연락처에 EWG의 제안서를 반영하기에 충분하지 않다(섹션 III 참조). 이 점을 고려해서 EWG는 다음과 같이 두 시스템의 데이터 요소 명칭들을 매핑시켰다.

57페이지

RDS Admin Contact ID가 PBC일 때,

RDS PBC Name = RAA Admin Contact Name

RDS PBC Organization = RAA Admin Contact Organization

다른 RAA Admin Contact 데이터 요소의 경우도 동일하다.

RDS Technical Contact ID가 PBC일 때,

RDS PBC Name = RAA Tech Contact Name

RDS PBC Organization = RAA Tech Contact Organization

다른 RAA Tech Contact 데이터 요소의 경우도 동일하다.

참고: EWG는 RDS 포털에서 RDS 사용자들이 모든 PBC 유형의 정의에 쉽게 접근할 수 있도록 해서(예를 들면, 해당 유형 가까이 가면 정의를 표시하는 팝업창이 뜨도록 해서) 해당 PBC가 허용된 목적을 위한 문의를 처리하기 위해 공개되어 있음을 명확히 알리고 그러한 목적을 다루기 위한 연락담당자를 반드시 지정할 것을 권고한다. 도메인 소유자는 문의를 직접 받거나(도메인 소유자 ID를 PBC로 지정), 그러한 문의를 받기 위해 공인 프라이버시/프록시 제공업체를 이용하거나(PP가 그러한 데이터 요소(보통 포워딩 주소나 제공업체 주소)를 제공) 그러한 문의를 받기 위해 특정한 실체를 지정한다(예, 서비스 제공업체, 호스팅 제공업체, 법률 대리인, 고객 서비스 담당).

모든 데이터 요소가 2013RAA에 정의된 바와 동일하고 다음 요소들이 추가되었다.

등록대행자 및 관리기관 관할지역(Registrar and Registry Jurisdiction): 등록대행자 또는 관리기관이 속한 법적 관할지역. ICANN과의 계약서에 명시된 관할지역.

등록 계약 언어(Registration Agreement Language): 등록대행자와 도메인 소유자 간의 계약서에 사용된 언어.

원 등록 날짜(Original Registration Date): 해당 도메인네임이 처음 등록된 날짜.[13]

클라이언트 상태, 서버 상태(Client Status, Server Status): 2013 RAA의 클라이언트 상태값에 덧붙여 현재 이 데이터 요소들은 해당 도메인네임에 적용된 등록대행자(클라이언트)와 관리기관(서버) 상태값을 포함한다: DeleteProhibited, RenewProhibited, TransferProhibited.

도메인 소유자 회사 식별자(Registrant Company Identifier): 공개 상공인성명록(public business directory)에서 도메인 소유자에게 할당한, 영국 트레이딩 번호(UK trading

[13] 생성 날짜(creation date)와는 다르다. 생성 날짜는 도메인네임이 등록된 가장 최근 시점을 나타낸다. 이전에 도메인네임을 등록했다가 이후로 여러 차례 삭제되기도 하기 때문이다. 원 등록 날짜는 해당 도메인네임이 최초로 등록된 날짜를 가리킨다.

number), D-U-N-S 번호 또는 기타 고유한 실제 회사 식별자. RDS 밖에서 기업을 검색할 때 사용된다.

58페이지

도메인 소유자 연락처 ID(Registrant Contact ID): 해당 도메인네임의 등록자로 식별된 미리 검증된 연락처 데이터 블록에 할당된 고유 식별자. 연락처 ID와 생성 및 사용 방식에 관한 자세한 정의는 섹션 V를 참조한다. 이 ID는 RDS 내에서 연락처 데이터의 재사용 및 유지관리를 가능하게 한다. 도메인 소유자 유형 = 프라이버시/프록시 (Registrant Type = Privacy/Proxy) 일 경우, 도메인 소유자 연락처 ID가 그 공인 프라이버시/프록시 제공업체에 할당된 고유 식별자임을 유념한다

도메인 소유자/PBC 연락처 검증 상태, 도메인 소유자/PBC 연락처 최종 검증 시간 (Registrant/PBC Contact Validation Status, Registrant/PBC Contact Last Validated Timestamp): 실행된 최고 검증 수준과 가장 최근 검증 날짜. 섹션 V에서 자세하게 설명한다.

도메인 소유자/PBC SMS, IM, 소셜 미디어(Registrant/PBC SMS, IM, Social Media): SMS, 문자메시지 또는 기타 대안적 소셜 미디어 통신 수단을 통해 도메인 소유자나 PBC에 연락하기 위해 선택적으로 사용 가능한 새로운 연락 수단.

도메인 소유자/PBC 대체 이메일, 대체 전화, 대체 소셜 미디어(Registrant/PBC Alt Email, Alt Phone, Alt Social Media): 1차적 주소로 도메인 소유자나 PBC에 연락할 수 없을 때 선택적으로 사용 가능한 대안적 새 주소. 이 새로운 데이터 요소는 도메인네임 자체가 중지되었을 때 기술적 문제 해결을 위해 또는 휴대전화나 소셜 미디어로 신속하게 연락하는 등의 일반적인 요구를 해결하기 위해 추가되었다.

도메인 소유자/PBC 연락처_URL, 오용신고_URL(Registrant/PBC Contact_URL, Abuse_URL): 새로운 선택적 데이터 요소로서 연락처 또는 오용 신고 설명, 정책 또는 신고 양식을 제공해 좀 더 생산적인 커뮤니케이션을 허용하는 웹 페이지로 연결된다.

PBC 연락처 ID(PBC Contact ID): 특정 도메인네임의 PBC로 식별된 연락처의 미리 검증된 데이터 블록에 할당되는 고유명(unique handle)으로 Contact Role에 명시된 역할을 수행 한다. 도메인 소유자 연락처 ID와 PBC 연락처 ID가 서로 동일할 수도 아닐 수도 있다.

참고: RDS를 구현하기 전에 이 새로운 데이터 요소들과 관련된 전환 및 준법 문제를 반드시 고려해야 한다.

b. 데이터에 대한 미인가 접근 및 제한적 접근 원칙

EWG는 누구나 모든 정보에 완전히 익명으로 접근 가능한 현재의 방식을 폐지하고 일부 데이터는 공개 접근을 허용하고 일부 데이터는 제한적 접근을 허용하는 새로운

패러다임을 도입함으로써 등록정보 접근을 위한 새로운 접근방식을 권고한다. 이 권고를 반영한 원칙들은 아래와 같다.

번호.	데이터 접근 원칙
41.	허가 받지 않은 RDS 사용자의 경우 반드시 가장 엄격한 프라이버시 체제에 부합하는 최소한의 데이터 요소에만 접근이 가능하다.

59페이지

번호.	데이터 접근 원칙
42.	명시적으로 허용된 목적에 따라 반드시 다양한 수준의 인증된 데이터 접근을 지원해야 한다.
43.	RDS 사용자 접근 크리덴셜은 반드시 감시 가능한 인증 절차와 결부시켜야 한다. 이에 관해서는 섹션 IV(c), 'RDS 사용자 인증'에서 자세히 정의한다.
44.	접근은 반드시 비차별적으로 이루어져야 한다(즉, 동일한 목적을 가진 모든 요청자들을 위해 반드시 공평한 조건을 제공해야 한다.)
45.	오용을 억제하고 책임성을 높이기 위해, • 반드시 명시된 목적에 의거해 데이터 요소에 접근해야 한다. • 제한적 데이터 요소의 경우 반드시 허용된 목적을 주장한 인증된 요청자에 한해 접근을 허용해야 한다. • 요청자들은 반드시 이후에 인증된 데이터 접근 요청에 사용할 크리덴셜을 신청하고 받을 수 있어야 한다.
46.	반드시 제한적 접근 요청자에게 적용할 인증 체계가 수립되어야 한다. • 인증된 요청자가 데이터를 요청할 때, 반드시 요청할 때마다 매번 그 목적을 명시해야 한다. • 목적에 따라 서로 다른 조건이 적용되기도 한다. • 인증된 요청자가 조건을 위반할 경우 반드시 제재 조치가 적용되어야 한다.
47.	일반도메인 등록정보 보호 기준을 높이기 위해, 모든 RDS 질의/응답은 반드시 흔히 이용 가능한 메시지 암호화 및 인증 기법을 사용해서 데이터의 기밀성과 무결성을 보호해야 한다.
48.	허용된 목적을 가진 인증된 RDS 사용자의 요구에 대해, RDS는 반드시 특정 값에 대한 공개 및 제한 데이터 요소를 검색해서 해당 값을 참조하는 모든 도메인네임 목록을 반환하는 역질의(Reverse Query)

	서비스를 제공해야 한다..
49.	허용된 목적을 가진 인증된 RDS 사용자의 요구에 대해, RDS는 RDS에서 이용가능한 히스토리 데이터에 한해 특정 도메인네임을 위한 공개 및 제한 데이터 요소의 히스토리 스냅샷을 반환하는 후워즈(WhoWas) 서비스를 반드시 제공해야 한다.

60페이지

번호.	데이터 접근 원칙
50.	RDS 데이터 요소를 활용한 서비스를 반드시 제공해야 한다. • 제3자는 역질의와 WhoWas를 비롯해 공개 데이터 요소를 이용해서 기존의 그리고 미래의 혁신적인 서비스를 반드시 제공할 수 있어야 하고 RDS 데이터 사용 조건을 준수해야 한다. • 제3자가 제한적 데이터 요소와 관련된 혁신적인 서비스를 제공할 경우, 반드시 인증을 받고 RDS 데이터 사용 조건을 준수해야 한다.
51.	제한된 데이터 요소는 반드시 정해진 RDS 접근 방식(위에서 설명한 방법을 포함하여)에 따라 접근해야 한다. 모든 일반도메인을 위한 전체 RDS 데이터 세트(또는 단일 일반도메인을 위한 전체 관리기관 데이터 세트)은 통제되지 않은 접근을 위해 대량으로 내보내져서는 절대로 안 된다.
52.	공개는 대화형 디스플레이 및 기타 RDS 접근 방법으로 이루어지기도 한다. • 일관된 방식으로 데이터를 쉽게 찾고 접근하기 위해서 반드시 중심이 되는 접속점(예, 웹 포털)을 제공해야 한다. • 모든 요청자가 반드시 인증되지 않은 질의 방식(적어도 안전한 웹사이트를 통해)을 통해 공개 데이터에 안전하게 접근 가능해야 한다. • 반드시 인증된 요청자와 목적을 기초로 안전한 웹 및 기타 접근 방법과 포맷(예, RDAP xml 응답, SMS, 이메일)을 통해 제한 데이터에 안전하게 접근하도록 지원해야 한다. • 요청자는 RDS로부터 신뢰할만한 데이터를 필요할 때 실시간으로 반드시 얻을 수 있어야 한다.

	• RDS는 다양한 이용 사례와 허용된 목적을 위한 대규모 검색을 위해 자동화를 반드시 수용해야 한다.
53.	진정한 글로벌 시스템이 되기 위해 RDS는 반드시 등록정보를 다국어 도메인네임(IDNs)을 비롯해 다양한 언어와 스크립트 및 문자집합으로 표시할 수 있어야 한다.
54.	RDS는 일반도메인을 위해 일반도메인정책개발기구(GNSO)가 정의한 미래의 모든 음역(transliteration) 정책을 지원해야 한다.

61페이지

번호.	데이터 접근 원칙
55.	RDS는 지역 언어로 된 등록정보 데이터 요소들의 수집과 표시를 허용해야 한다.

공개 데이터 접근

아래 그림에서 보듯이 공개 데이터 요소는 인증을 받든 받지 않았든 RDS에서도 누구나 요청이 가능하다. 인증 받지 않은 공개 데이터 요청에 반환되는 데이터 요소에 대한 자세한 설명은 부록 E를 참조한다.

(그림)

<table>
<tr><td></td><td>RDS 질의
(비인증, DN)</td><td></td><td></td><td>모든
일반도메인
관리기관</td></tr>
<tr><td></td><td></td><td>포털</td><td>RDS</td><td></td></tr>
<tr><td></td><td>RDS 응답
(공개 데이터에 한함)</td><td></td><td></td><td>모든
일반도메인
검증기관</td></tr>
<tr><td>모든 요청자</td><td></td><td colspan="2" rowspan="2">목적에 관계없이 누구나
이용가능한 공개 데이터만
반환한다.</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

그림 6. RDS에서 공개 등록정보에 대한 인증 받지 않은 접근

또한 부록 I에는 관련 데이터 요소 접근을 위한 과정을 설명한 플로 차트와 이용 사례의 예가 포함되어 있다.

제한적 데이터 접근

아래 그림에서 보듯이, RDS를 통해 제한 데이터 요소도 요청이 가능하다. 그러기 위해서 요청자는 반드시 먼저 인증을 받아야 한다. 그 후에 요청자는 명시적 목적을 위해 데이터 요소를 요청하는 요청서를 제출하게 된다. 인증을 통한 제한적 데이터 요청으로 반환되는 데이터 요소에 대한 자세한 설명은 부록 E를 참조한다.

62페이지

1차 제한적(GATED) 요청에 앞서, 요청자는 반드시 인증을 받고 요청자 ID를 획득해야 한다.				
	RDS 질의 (비인증, DN)			모든 일반도메인 관리기관
	RDS 응답 (공개 데이터에 한함)	메소드	RDS	
승인된 요청자				모든 일반도메인 검증기관
	명시된 목적을 위해 인증된 요청자에게 이용 및 접근가능한 요청 데이터만 반환한다.			

그림 7. RDS를 통한 제한적 등록정보 접근

기술 규약 및 접근 방법

EWG는 현행 도메인 등록 체계에 적용된 기술 규약들(예, EPP[14])과 IETF(예, WEIRD 실무그룹)에서 개발중인 규약들이 EWG가 권고하는 설계 특징들을 지원하는지 조사했다. WEIRD 실무그룹이 개발 중인 등록정보 접근 규약(RDAP)으로 불리는 새 표준은 거의 마무리 단계이다. 이러한 규약들을 EWG가 권고하는 모형에서 채택할 경우 영향을 받는 각 당사자들의 전환 비용이 낮아질 것으로 기대된다. EWG의 분석에 따르면 EPP와 RDAP 모두, 이중 어떤 대안적 모형이 선택되든 관계없이 RDS에서 사용 가능한 것으로 나타났다. 그러나 그럴 경우 몇 가지 확장, 추가 또는 RDAP "의견(remark)"의 사용이 필요할 지도 모른다. 부록 G에서 이들 각 규약을 상세하게 평가했다.

c. RDS 사용자 인증 원칙(RDS User Accreditation Principles)

섹션 III, '목적'에서 언급했듯이 목적에 따라 제한적 데이터 요소 또는 제한적 데이터 요소 중 허가를 얻은 부분집합에 대한 접근이 필요하다. 그리고 IV(b), 46번 원칙에서 언급했듯이 제한적 데이터에 대한 접근이 필요한 목적의 경우 사용자 인증이 필요하다. 그러나 사용자 인증을 받았다고 해서 제한적 데이터에 무제한으로 접근하지는 못한다. 모든 접근은 목적을 기반으로 하며 명시된 목적에 허용된 데이터 요소만을 반환한다.

[14] EPP: 69 표준, RFC 5730 – 5734 참조

EWG는 섹션 III에서 열거한, 허용된 목적을 위해 제한적 데이터 접근을 원하는 각 RDS 사용자 집단을 위해 커뮤니티 전문가들의 도움을 받아 EWG가 식별한 등록정보의 목적과 해당 목적을 위해 반드시 접근이 필요한 데이터 요소 및 가능한 RDS 사용자 인증기구를 확인할 것을 권고한다.

많은 조직들이 RDS 사용자 인증기구가 되기 위해 ICANN과 계약을 체결할 것이다. 모든 RDS 사용자 인증기구는 반드시 일단의 공통 원칙들을 준수해야 하며 각 RDS 사용자 커뮤니티에 따라 그 구현에 있어 서로 차이가 날 수 있다. 예를 들면,

시나리오 1: 인증 기구가 인증 운영자와 다르다. 이 경우 인증 기구가 사용자를 인증하지만 제 3 자인 운영자가 인증된 사용자의 RDS 접근을 관리한다.

상표권 보유자와 같은 RDS 사용자 커뮤니티를 위해, 특정 산업 기구가 허용된 목적을 위해 제한적 데이터에 접근하려는 구성원들을 인증하는 책임을 맡는다. 이 인증 기구(Accrediting Body)는 사용자 계정 관리나 RDS 에 보내는 접근 요청서 인증에는 전혀 관여하지 않는다. 그보다 인증 기구는 특정 RDS 사용자 커뮤니티를 위해 회원가입 규칙과 서비스 조건 및 신청 및 시행 절차 등을 마련한다. 그리고 인증 기구는 제 3 자인 인증 운영업체와 계약을 체결해서 RDS 사용자 계정 생성과 관리, RDS 접근 크리덴셜 발급 및 일시적인 계정 정지 등 1 차적인 오용 사건 처리 등의 업무를 위임한다. 인증 운영업체는 단순히 특정 커뮤니티를 위해 인증 기구가 정한 RDS 접근 규칙을 이행 및 시행할 뿐이다. 계정 정지 요청이나 기타 분쟁은 인증 기구로 올려 보낸다.

시나리오 2: 인증 기구가 인증 운영자와 결합해 인증된 RDS 접근 요청을 RDS에 넘긴다.

OpSec과 같은 RDS 사용자 커뮤니티를 위해, 특정 산업 조직이 책임을 지고 기존에 다른 시스템에 대한 접근권을 구성원들에게 부여하기 위해 사용하던 (승인된) 인증 절차를 통해 구성원들을 인증한다. 이 예에서, 해당 산업 조직은 인증 기구인 동시에 인증 운영자이며 기존에 구성원들이 이미 사용하던 시스템을 활용해서 특정 목적을 위한 제한적 데이터 접근 요청을 인증한 후에 RDS로 보낸다. 이 경우, RDS 사용자는 (RDS) 조건을 준수할 책임이 있으며 산업 기구는 반드시 접근 오용, (회원 자격) 정지 등의 문제를 처리하기 위해 절차를 확립해야 한다.

64 페이지

시나리오 3: 인증 기구가 인증 운영자와 동일하며 구성원들을 대신해 RDS 접근 요청을 한다(인터폴 모형)

사법기관과 같은 RDS 사용자 커뮤니티를 위해 신뢰할 수 있는 조직이 기존에 다른 시스템에 대한 접근권을 구성원들에게 부여하기 위해 사용하던 (승인된) 인증 절차를 통해 구성원들을 인증하는 책임을 진다. 이 예에서, 해당 조직은 인증 기구인 동시에 인증 운영자이며 기존에 구성원들이 이미 사용하던 시스템을 활용해서 특정 목적을 위한 제한적 데이터 접근 요청을 인증한 후에 RDS로 대신 보낸다. 이 경우, 이 조직이 RDS 사용자로 간주되어 대리한 요청과 관련한 구성원들의 행위와 RDS 조건 준수에 대한 책임을 진다. 비록 RDS는 구체적인 사용자 활동에 대해 알지 못하지만 조직은 반드시 특정 사용자의 접근을 감시하고 오용을 탐지할 수 있는 방식으로 접근 오용이나 정지 등을 처리하기 위한 절차를 마련해야 한다.

승인된 RDS 사용자가 허용된 목적을 위해 제한된 데이터 요소에 접근하도록 허용하기 위해 EWG는 다음과 같은 RDS 사용자 인증 원칙들을 권고한다.

번호.	데이터 접근 원칙
56.	인증이나 승인 없이 비제한(즉, 공개) 데이터에 반드시 실시간으로 접근 가능해야 한다.
57.	RDS 데이터 접근을 위한 RDS 사용자 인증이 모든 이용 사례 및/또는 요청자를 위해 실시간으로 이루어질 필요는 없다.
58.	RDS는 반드시 RDS 사용자가 명시적 목적을 위해 제한된 데이터 요소에 접근하도록 허용하기 위해 필요한 최소한의 “인증 체계”를 적용해야 한다.[15]
59.	RDS의 모든 잠재적 사용자의 “사전 인증” 또는 크리덴셜 제공을 요구해서는 절대로 안 된다. 각 “유형”의 인증된 RDS 사용자(즉, RDS 사용자 커뮤니티)에 따라 서로 다른 요청 및 충족 과정을 수립할 수 있다.
60.	허용된 목적을 위해 데이터에 접근하고자 하는 RDS 사용자의 인증은 세 가지 방식으로 가능하다. • 인증 없음(즉, 공개 데이터에 한해 인증되지 않은 접근 가능) • 데이터를 요청하는 자/실체의 자가 인증. 사용자가 간단하게 자신의 신원과 요청하는 데이터와 요청 이유를 명시한 다음 해당 수준의 데이터에 대한 접근권을 부여 받는다. 예를 들면, 도메인네임 관리 목적을 위해 자신의 도메인네임 정보에 접근하고자 하는 도메인 소유자가 여기에 해당한다. 이 경우 그들의 자가 증명

[15] 예를 들면, 이 인증은 다중인증 선서 진술서를 요구할 필요가 없거나 대다수 유형의 데이터를 얻기 위한 “핵심(be-all-and-end-all)” 시스템 역할을 할 필요가 있다

65페이지

번호.	데이터 접근 원칙
	(self-attestation)은 도메인네임의 실제 등록 정보와 연결되어 RDS에서 해당 정보에 접근하기 위한 크리덴셜을 받을 자격이 주어진다. • 신뢰할 수 있는 제3자(즉, RDS 사용자 인증 기구, 아래 64번 원칙 참조)에 의한 인증
61.	가능한 제3자 RDS 인증 과정은 섹션 III에서 크리덴셜 발행이 필요한 것으로 식별된 각 RDS 사용자 커뮤니티에서 기존에 사용하던 인증 절차를 활용해야 한다.
62.	이러한 제3자 인증 과정은 반드시 RDS 사용자 인증 정책의 구현과 시행을 책임지는 기관(예를 들면, ICANN, 다수이해관계자 패널)에서 조사하고 주기적인 평가를 실시해야 한다.
63.	RDS 사용자 인증 기구는 반드시 ICANN 및/또는 RDS 제공업체와 서면 계약을 체결하고 서로 합의한 지침에 따라 인증 과정을 제공하고 적법 절차, 책임성, 보안, 공정한 접근 및 적용 법률 준수를 허용하는 프레임워크를 확립해야 한다.
64.	인증 기구는 다음 중 한 가지 또는 두 가지 모두 책임진다. RDS 사용자 인증 기구는 사용자 커뮤니티를 정의 및 관리한다. 구체적으로는 멤버십 기준 및 크리덴셜 제공 요건을 규정하고, 자체적인 멤버십 조건을 정의 및 시행한다. RDS 사용자 인증 운영자는 인증 기구가 사용자 계정 생성, 크리덴셜 발급, 계정 중지 및 해지, 수명주기 사용자 계정 관리 등의 기능과 분쟁 처리 및 ToC 시행과 같은 관련 절차를 제공하기 위해 사용할 플랫폼을 제공한다. 인증 기구가 두 가지 모두 책임질 수 있지만 의무 사항은 아니다.
65.	구성원들을 대신하여 RDS 정보 요청 처리에 관여하고자 하는 인증 기구는 다음 두 가지 방법을 통해 가능하다. • 인증 기구는 자체 인증 체계를 통해 구성원들 대신 RDS에 접근하며 합법적 사용을 전적으로 책임진다. 오용 발생 시 인증 기구가 모든 책임은 지지만 인증 기구를 통해 이러한 방식으로 대신 전달된 요청서는 반드시 개별 사용자 접근과 관련된 감사 및 오용 문제 해결이 가능한 방식으로 인증을 받아야 한다. • 인증 기구는 자체 인증 시스템을 통해 RDS에 접근 가능하게

	하지만 단순히 인증된 요청을 RDS에 전달하는 역할만 한다.

66페이지

번호.	데이터 접근 원칙
	이 방식의 경우, 인증 기구를 통해 전달된 요청서가 반드시 RDS 사용자를 고유하게 식별해야 하고 해당 사용자가 적절한 사용은 물론 오용 사고 발생시에도 직접 책임을 져야 한다.
66.	섹션 IV(b), 50번 원칙에서 정의하듯이 RDS는 반드시 인증된 요청자를 위해 복수의 방법을 통한 실시간 접근을 허용해야 한다. 요청서는 적절한 인증 운영자가 인증하고 인증 중 발급된 RDS 접근 크리덴셜은 반드시 정의된 모든 접근 방법과 함께 사용하기에 적합해야 한다.[16]
67.	크리덴셜 관리를 위한 우수 사례를 정의한다. 인증 기구는 반드시 우수 사례를 준수해야 한다.
68.	RDS는 반드시 인증된 접근을 위한 개별 크리덴셜을 요구해야 한다.
69.	인증된 RDS 접근은 절대로 다른 사용자에게 넘겨서는 안 된다. (즉, 인증된 RDS 사용자가 제한 데이터를 인증 범위 밖의 타인과 공유해서는 안 된다.)
70.	원래 요청된 목적의 범위를 더욱 확대해서 활용할 수 있도록 제한적 데이터의 책임감 있는 공개 과정을 마련하고 시행해야 한다.(예를 들면, 상표권 침해를 조사하는 IP 소유자가 UDRP 민원을 제기할 수 있도록 해서 범죄 행위를 수사하는 OpSec 사용자가 사법기관에 고지할 수 있도록 한다.)
71.	RDS 데이터에 접근하고자 하는 조직은 RDS 사용자 인증을 신청하고 조직 내에서 RDS를 사용하는 모든 사람이 하나의 인증으로 RDS에 접근하도록 할 수 있다.[17] 조직 내 구성원들의 인증된 접근은 해당 조직이 책임지고 관리한다. 인증된 RDS 사용자 조직의 구성원이 시스템을 오용한 경우 전체 조직을 상대로 제재 조치가 가해질 것이다.
72.	한 명의 RDS 사용자가 여러 다른 역할을 수행할 경우 목적에 따라 서로 다른 유형의 데이터에 접근하기 위해 복수의 크리덴셜을 가지는 것도 가능하다. 그러나 유용성의 측면에서 볼 때, 섹션 IV(b)에서 정의했듯이 접근할 때마다 목적을 명시하기만 한다면 한 명의 RDS 사용자에게 여러 목적에 사용 가능한 하나의 크리덴셜을 제공하는 편이 더 효과적이다.

[16] 구현하는 동안 반드시 인증 인터페이스를 정의해야 한다. 예를 들면, 일부 인증 방법의 경우, RDS가 SAML(Security Assertion Markup Language)과 같은 표준 프레임워크를 사용해서, 해당 크리덴셜을 발급한 인증 운영자가 인증할 수 있도록 한다.

[17] RDS 접근을 위해 발급된 크리덴셜의 무결성을 확인하는 것은 조직의 책임이다.

73.	반드시 감사 및 데이터 분석을 사용해서 시스템 및 접근 크리덴셜의 오용은 없는지 확인해야 한다.

67페이지

번호.	데이터 접근 원칙
74.	RDS 사용자들이 오용 혐의를 해명하고 RDS 접근 크리덴셜을 재활성화/복원하기 위한 호소(appeal) 절차를 반드시 규정해야 한다.
75.	모든 도메인 소유자가 자신이 등록한 도메인네임과 관련해 RDS에 저장된 연락처 정보를 조사하려면 반드시 크리덴셜을 받아야 한다.(섹션 III, 도메인네임 관리 목적 참조)
76.	현재의 절차를 보완하든 아니면 승인된 목적에 따라 사용자를 인증하기 위한 새롭고 혁신적인 방법을 제공하든, RDS 사용자 인증 기구를 추가하기 위한 절차를 반드시 확립해야 한다. 그러한 RDS 사용자 인증 기구는 반드시 본 문서에 열거된 원칙들에서 설명한 최소한의 요건을 충족해야 한다.

d. 책임성 강화의 이점 요약

제한적 데이터 요소에 대한 인증된 접근을 차세대 RDS의 필수 구성요소로 통합하고 좀 더 민감한 정보에 접근하는 사람들의 신원을 식별하고 데이터를 필요로 하는 목적을 명시하게 함으로써 책임성을 높일 수 있다. 구체적으로 말하자면, EWG가 권고하는 데이터 요소 및 접근 원칙들을 채택하면 다음과 같은 이점이 있다.

- 허용된 목적을 위해 등록 정보를 사용하는 실체의 책임성을 높이기 위해 목적에 따른 데이터 수집과 공개 패러다임을 확립한다.
- 관할지역에 따른 정보보호법을 준수하기 위한 지원 프레임워크를 제공한다.
- 다양한 목적을 위해 데이터에 접근하는 사람들의 책임성을 강화하기 위한 방법을 확립한다. 이로써 관할지역에 따른 정보보호/프라이버시 요건을 뒷받침하고 정확한 데이터 제공의 의무가 있는 사람들과 인증된 목적을 위해 데이터를 사용하는 사람들 사이의 균형 잡힌 책임감을 보장한다. 따라서 데이터 요청자가 연락처 정보에 대한 접근과 사용에 대해 전혀 책임지지 않는 현행 WHOIS 시스템의 근본적인 불평등성을 해결한다.
- 도메인 소유자 및 연락처를 위해 등록정보의 수집 목적에 대한 좀 더 명확한 이해를 제공하고 개인 정보의 공개적 또는 제한적 접근에 대한 차별적 통제를 가능하게 한다.
- 기본적인 공개 데이터 세트로 등록정보에 대한 보편적 요구를 충족시키지만 공개 접근이 가능한 데이터의 양을 줄이고 제한 데이터에 접근하는 사람을 인증한다.

68페이지

민감한 데이터 요소를 공개적 접근으로부터 보호함으로써 데이터 정확성이 증가하면 도메인 소유자와 PBC들이 좀 더 정확한 데이터를 공유할 가능성이 높아진다. 범죄에 사용하는 경우를 제외하고 데이터를 전체 공개로부터 보호하면 데이터 주체들이 데이터 제공에 따른 위험성이 낮아진다고 인지하기 때문에 데이터 제공으로 얻는 장점들을 위해 더 정확한 정보를 제공하게 될 것이다.

- 선택적 데이터 요소들을 새로 포함시켜 대안적 의사소통 수단을 통한 연락을 허용함으로써 전반적인 커뮤니케이션의 복구성과 효율성을 높인다.
- 중앙 포털을 통해 역질의 및 WhoWas 질의를 지원해, 허용된 목적에 한해 인증된 RDS 사용자들이 모든 일반도메인 등록정보를 검색하도록 허용한다.
- “시스템”의 전반적인 효율성 향상을 위해 접근 능력을 강화한다.
- 인증되지 않은 공개 데이터 접근과 인증을 통한 제한적 데이터 접근 모두를 제공함으로써 접근 능력, 서비스 수준 및 현재의 일반도메인 WHOIS 응답 포맷의 복잡성을 제거하고 단일 표준을 통해 자동화된 RDS 질의를 쉽게 구현할 수 있도록 한다.
- 양질의 서비스와 책임 있는 접근을 통해 생태계 전반에 분산된 여러 오용 방지책의 필요성을 없앤다.

이러한 장점들을 실현하기 위해 RDS 사용자들에게 허용된 목적과 RDS에서 검색한 데이터의 적절한 사용에 대해 교육하는 것이 무엇보다 중요할 것이다. 커뮤니티 구성원들의 RDS 접근을 인증하는 책임을 감당할 의사가 있는 인증 기구들을 물색하기란 쉽지 않은 과제일 지도 모른다. 처음에 사용자들, 특히 여러 목적을 위해 RDS을 사용하는 사용자들은 적절한 인증기구 식별에 혼란을 느낄 지도 모른다. 또한 자동화된 RDS 질의를 위해서 업데이트 도구도 필요할 것이다. 그러나 목적 기반의 접근 체계 확립을 위해 필요한 초기 투자는 RDS 사용자들이 책임감을 가지고 등록정보를 사용하는 환경을 조성하기 위한 강력한 토대가 될 것이다.

V. 데이터 품질 향상

EWG는 현재의 WHOIS 시스템이나 2013 RAA의 폭넓은 구현을 통해 현 시스템을 좀 더 강화해서 가능한 것 이상으로 훨씬 엄격한 도메인 소유자 데이터 검증을 권고한다. 먼저, 도메인 소유자가 PBC를 제공하는 경우 다양한 목적에 맞는 적절한 연락처로 연결될 가능성을 높이고 도메인 소유자들이 해당 역할과 관련해 정확한 정보를 제공할 더 많은 유인을 제공해야 한다. 둘째, 상대적으로 민감한 데이터에 대한 제한적 접근을 통해 도메인 소유자들이 부정확한 데이터를 제공할 유인을 없애고 데이터 정확성에 대한

도메인 소유자의 책임성은 향상될 것이다.

69페이지

이러한 목표를 달성하기 위해 EWG는 서로 연관성이 있으면서도 독립적인 두 가지 개선안을 권고한다.

- RDS는 모든 일반도메인 등록정보에 반드시 표준 검증을 적용해야 한다. 주기적인 점검 외에, 정보를 수집할 때도 검증이 이루어질 것이며 복수의 도메인네임 등록을 위해 재사용하기 위해 연락처 데이터 블록을 미리 검증할 수도 있다.
- RDS 생태계는 도메인네임 디렉토리와는 개념적으로 분리된 사전검증 연락처 디렉토리(Contact Directory)를 반드시 포함해서 도메인 소유자나 도메인 소유자가 다양한 도메인네임 등록 목적을 위해 PBC로 지정하는 사람이나 조직에 연락하기 위해 사용하는 데이터 요소의 품질과 재사용성을 높이고 개인 정보의 사기적 사용을 억제해야 한다.

이러한 권고와 관련된 원칙과 과정들을 아래에서 자세히 설명하고 있다. EWG는 두 개선안 모두 권고하지만 검증 강화 없이도 연락처 디렉토리 생성은 가능하며 그 반대의 경우도 마찬가지이다.

a. 데이터 정확성과 검증 원칙

다음과 같은 목적을 위해 도메인 소유자나 기타 연락처 정보의 사전 검증이 필요하다.

- 사전 검증을 활용해 새로운 도메인네임에 사용하기 전에 데이터를 점검하고 등록된 모든 데이터의 일관성을 높이기 위해 연락처 정보의 정확성을 높인다(오류나 사기를 줄인다).
- 처음 한 번 검증을 실시하고 이후로 도메인네임을 등록할 때 그 연락처 정보 블록을 재사용함으로써 도메인 소유자가 매번 새 도메인네임을 등록할 때마다 도메인 소유자나 기타 PBC 연락처 정보를 검증할 필요가 없다.(등록 절차가 간소화되고 필요한 작업이 감소한다.)
- 등록과 동시에 검증이 이루어져야 하기 때문에 도메인 등록 처리가 지연되지 않는다.

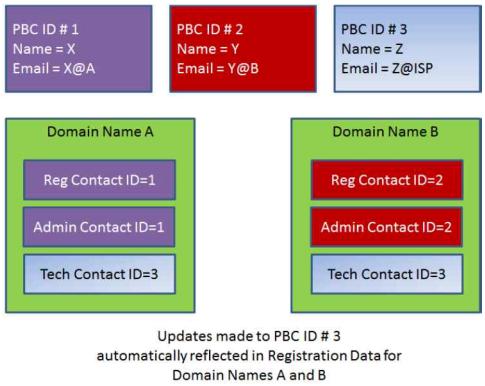
다양한 종류의 도메인 소유자들이 수 많은 도메인(종종 수백에서 수십 만개)을 등록할 때, 서비스 제공업체와 법률 대리인 및 기타 제3자들이 여러 역할(예, 기술, 과금, 법적 절차)을 수행하는 1차 연락담당자 역할을 하는 경우가 많다.

다양한 공간에 분산되어 있는 연락처 정보의 정확성과 사용의 편의성을 높이기 위해 복수의 도메인 소유자들이 그러한 연락처를 쉽게 이용할 수 있는 메커니즘을 제공할 필요가 있다. 웹 호스팅 회사를 예로 들자면, 고객들이 통제권을 가진 도메인을 위해 NOC 고유 ID를 “기술” 및 “오용 신고” 연락처로 사용할 수 있다.

70페이지

또한 그러한 실체가 새로운 주소/전화번호 또는 인수/합병으로 인한 변화를 반영하기 위해 연락처 정보를 업데이트해야 할 경우, 한 장소에서 쉽게 정보를 업데이트 하고 해당 연락처 데이터 세트(고유 식별자로 지정된)와 연결된 모든 도메인에 변동사항이 반영되도록 해야 한다.

아래 표는 목적별 연락처(PBC)를 생성하고, 고유 식별자(PBC ID)와 연결한 다음 도메인네임 등록 시 반복해서 재사용하는 패러다임에 대해 설명한다. 섹션 III에서 자세히 설명했듯이, PBC가 반드시 특정한 사람일 필요는 없으며 명백히 연락처 보유자가 생성하고 DNS 관련 목적을 위해 연락이 가능한 공표된 연락담당자를 나타낸다.



PBC ID #3을 업데이트하면 도메인네임 A와 B의 도메인 소유자 정보에 자동으로 반영된다.

번호	연락처 ID 및 관련 데이터 원칙
77.	연락처 관리는 반드시 도메인 관리와는 분리되어 이루어져야 한다. 그래야 도메인네임과 분리해서 연락처를 이동하거나 책임을 물을 수 있고 그러한 연락처에 기재된 실제 개인이나 실체에 의해 통제되도록 할 수 있다.
78.	연락처는 반드시 검증기관(Validator)를 이용해서 관리해야 한다. 검증기관은 연락처 데이터베이스를 관리하고, 검증 체제를 실행하고 연락처 및 데이터 요소(RDS를 통해 접근가능한)의 유효성 수준에 관한 정보를 보관한다.[18]
79.	도메인을 등록할 때 도메인 소유자가 지정한 연락처 ID와 연결시키고

[18] 참고: 등록대행자는 그들이 등록하는 도메인네임과 연결된 연락처에 대해 검증 서비스를 제공하는 인증된 검증기관이 될 수 있으며 그럴 가능성이 높다.

	도메인네임의 다양한 목적에 대해 그렇게 지정된 연락처의 승인을 얻을

71페이지

번호	연락처 ID 및 관련 데이터 원칙
	수 있다.
80.	그러한 연락처는 반드시 유효한 의무적 데이터 요소를 포함해야 한다. 연락처 ID가 연락처의 허가 없이 사용되지 않도록 그리고 최소 기준을 충족시키도록 보장하기 위한 절차를 관리하기 위한 정책과 감독이 필요할 것이다.
81.	연락처 정보의 변경 관리 및 사용 허가는 연락처 보유자(Contact Holder)가 통제하며 해당 연락처와 연결된 모든 도메인에 영향을 미친다. 도메인 소유자나 PBC에게 부담을 주지 않으면서 이 새로운 패러다임을 지원할 수 있는 정확하고 시기에적절한 정보 변경을 허용하는 과정과 정책이 반드시 개발되어야 한다.
82.	각 개별 연락처 데이터 블록은 반드시 검증기관과 연락처 보유자 모두를 고유하게 식별하는 연락처 ID를 가져야 한다. 이 연락처 ID를 통해 연결된 연락처 데이터의 검색과 업데이트를 실행한다. 이 연락처 ID는 반드시 RDS 데이터를 공개하는 공공 디스플레이(public display)를 통해 공표해야 한다.

b. 사전 검증 과정(Pre-validation Process)

이러한 요구를 해결하기 위해 다음과 같은 사전 검증 과정을 권고한다.

a) 각 신청자는 자신이 선택한 검증기관(예, 등록대행자, 관리기관, 인증된 제3자 연락처 관리 서비스 제공업체)를 통해 연락처 정보를 제출한다.

b) 검증기관이 구문 검증(Syntactic) 및 운영상의 검증(operational validation)(SA-058에 따라)을 실시한다.

c) **선택사항**: 검증기관이 우체국, 국가도메인 관리자, 전화회사, 세무서와 같은 실체를 활용해서 신원 검증(Identity validation)을 실시한다. *선택사항인 신원 검증 표준을 충족한 연락처는 그에 맞는 상태로 지정되어 사용자의 신뢰를 높이고 결과적으로 온라인 상거래를 활성화시킬 수 있음을 유념한다. 또한 그러한 부가가치 서비스는 그에 따른 비용이 수반될 것이며 그러한 비용은 이 부가적인 검증 수준을 요청하는 실체가 부담하게 될 것이라는 점도 참고한다.*

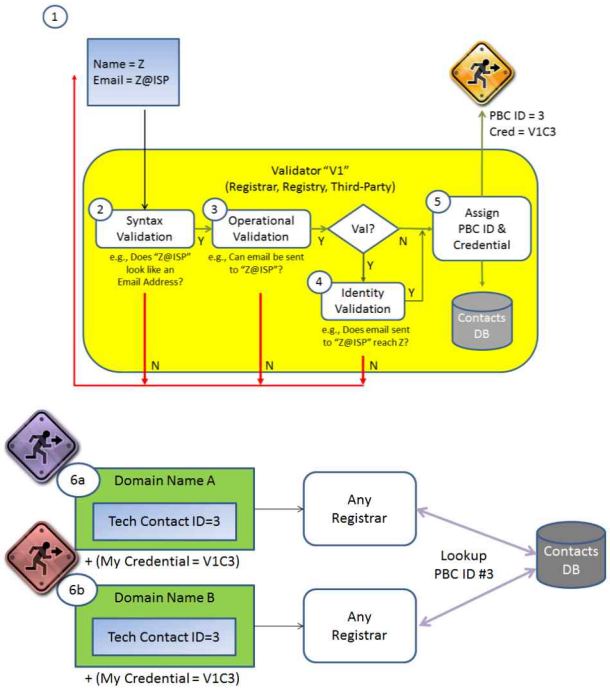
d) 구문 검증과 운영상의 검증이 성공적으로 완료되고 검증기관이 연락처 데이터 블록(연락처)에 검증기관과 연락처 모두 고유하게 식별하는 식별자를 발급하면 후속적인 검색과 업데이트가 가능해진다.

e) 검증기관은 연락처 데이터를 자체 데이터베이스로 저장하고, 크리덴셜을 발급하고 (해당사항이 있는 경우 미래의 연락처 업데이트를 위해) 고유 식별자를 신청자(이 시점부터 연락처 보유자로 알려진)에게 전달한다.

72페이지

f) 연락처 보유자(Contact Holder)는 도메인 소유자에게 이 연락처 ID를 제공하고, 도메인 소유자는 이 고유 식별자를 이용해서 등록대행자에 도메인네임을 등록하는데 이 때 연락처 ID를 목적별 연락처(즉, PBC)로 지정하면 된다. *섹션 III에서 정의했듯이, 도메인 소유자와 지정 연락처가, PBC가 각 도메인네임을 위해 수용할 목적에 동의하는지 확인하기 위한 승인 과정이 반드시 확립되어야 한다.*

g) 섹션 III(e)에 규정된 목적별 연락처 원칙에 따라 검증된 연락처 ID(Validated Contact ID)를 도메인네임의 PBC(예, 도메인 소유자, 기술, 관리, 업무, 오용 신고, 법률, 프라이버시/ 프록시 제공업체)로 지정 가능하다.



각 검증기관은 자체 연락처 데이터베이스를 유지한다는 점을 유념한다. 이 데이터를 반드시 RDS에게 제공해야 하지만 그 방식은 섹션 III에서 설명한 RDS 모형에 따라 달라진다. 예를 들어, 동기화 모형(Synchronized model)에서 연락처 데이터 추가와 업데이트는 EPP를 통해 RDS로 푸시하는 것도 가능하다. 연합 모형(Federated model)에서는 RDS가 실시간으로 RDAP를 통해 연락처 데이터를 끌어온다.

c. 정확성, 감사 및 교정 과정

지속적으로 등록정보의 정확성을 유지하고 부정확한 등록정보를 교정하기 위해 다음의 절차를 권고한다.

a) 자가 정정(Self-correction): 연락처 보유자(Contact Holder)는 검증기관을 이용해서 이전에 발급받은 크리덴셜로 자신의 데이터를 수정/갱신한다. 수정된 정보는 그 특정 연락처(고유 연락처 ID로 지정된)를 활용해서 모든 도메인으로 자동으로 흘러간다.

b) **절차 감시**: 검증기관은 자신이 관리하는 연락처 데이터 세트에 대해 주기적으로 운영상의 검증 및 선택사항인 신원 검증을 실시한다. *참고: 이러한 검증 절차가 지나치게 큰 부담이 되어서는 안되며 특정 연락처와 관련된 공개되는 상태 정보에 반영할 수 있다(예, 연락처는 2016년 1월 1일 현재 운영상 유효하다).*

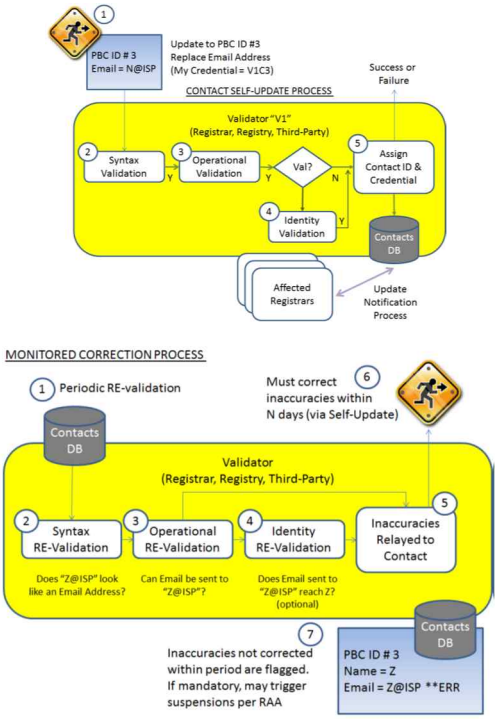
c) 검증기관은 부정확한 데이터가 탐지될 경우 연락처 보유자(Contact Holder)에게 보고하고 연락처 보유자가 부정확한 데이터를 수정하기 위한 시간(예, 14일)을 준다. 영향을 받는 도메인 소유자, 관리기관 및 등록대행자에게도 공지한다. 보고를 받은 연락처 보유자는 이전에 선택한 검증기관을 이용해서 이전에 발급받은 크리덴셜로 부정확한 데이터를 수정한다.

d) 정해진 시한이 지나도 등록정보가 수정되지 않을 경우, 해당 데이터에 부정확하다는 표시를 한다. 부정확한 것으로 표시된 데이터가 현재 이 연락처 ID를 참조하는 PBC에 있어 의무적 데이터인 경우, 연결된 도메인들은 교정 절차에 들어가고 이 과정에서 도메인 소유자에게 부정확성에 대해 고지해서 RAA가 정한 시한 내에 수정하도록 한다. 시한 내에 수정하지 않을 경우 적용 가능한 RAA에 따라 도메인 정지 또는 삭제를 비롯한 불이익을 당할 가능성도 있다.

e) 부정확한 것으로 표시된 데이터가 유효한 데이터로 교체되면 관련 도메인들에 대한 제재 조치가 풀린다.

f) ICANN 컴플라이언스에 정확성 보고서가 제출되면 검증기관에게 구문(syntactic) 및 운영상의 검증을 다시 실시하라는 고지가 갈 것이다. 재검증에 성공하면 정확성 보고서를 제출한 당사자는 상황에 따라 필요한 다른 조치를 취한다(예, UDRP 민원 제기 또는 정보제공(Reveal) 요청서 제출). 재검증에 실패할 경우, 부정확한 연락처 ID를 사용하는 모든 도메인네임의 도메인 소유자에게 반드시 고지하고 위에서 설명한 정상적인 교정 절차를 따라야 한다.

74페이지



d. 연락처 ID 운영 프레임워크

연락처 ID를 관리하고 이 ID를 등록 정보와 연결하기 위해 다음의 프레임워크를 권고한다.

a) 연락처 ID는 이동성(portability)를 보장하고 도메인네임과 필수 디렉토리 정보 사이의 확정적인 매핑을 위해 전체 검증기관들 사이에서 반드시 고유해야 한다.

b) 연락처와 검증기관 모두를 식별하는 연락처 ID는 검색 및 업데이트를 위해 반드시 별도의 연락처 정보 블록과 연결되어야 한다. 설명: 하나의 연락처 ID는 지정된 도메인네임 연락처와의 커뮤니케이션에 이용 가능한 하나의 연락처 데이터 집합과 매핑된다. 이 요건을 충족시키지 않는 정보는 운영상의 측면에서 쓸모가 없다.

c) 연락처 ID는 반드시 공인 검증기관(Validator)가 발급해야 한다. 어떤 실체든 신청을 통해 검증기관이 될 수 있으며 현재 등록대행자의 검증에 사용되는 것과 유사한 기준을 충족해야 한다. 등록대행자, 관리기관 및 제3자 검증 서비스 제공업체 모두 검증기관이 될 자격이 있다. 근거: 검증기관은 연락처 데이터베이스 생성에 꼭 필요한 일종의 기능이다. 검증 수준은 연락처에 따라 차이가 있지만 검증기관들 간에 도메인 소유자 및 지정 연락처에 대한 책임성과 정확성을 보장하기 위해 검증 과정을 조율할 필요가 있다.

d) 도메인 소유자나 지정 PBC가 도메인네임과 연결되려면 반드시 연락처 ID를 획득해야 한다.

e) 하나의 연락처 ID를 하나 또는 다수의 도메인을 위한 복수의 역할을 위해 지정할 수 있다. 예를 들면, 특정 PBC ID를 한 도메인을 위한 도메인 소유자 ID로, 동시에 다른 도메인을 위한 기술 및 오용신고 연락처로 사용하는 것이 가능하다.

f) 연락처는 도메인 등록 과정에서는 물론 언제든지 생성 및 수정이 가능하다.

e. 검증기관과의 상호작용

EWG는 검증기관과 연락처 보유자(즉, 성공적으로 재사용이 가능한 검증된 연락처 데이터 블록을 생성한 당사자) 사이의 상호작용을 위해 다음의 원칙들을 권고한다.

번호.	연락처 보유자 및 검증기관 사이의 상호작용 원칙
83.	연락처 보유자는 특정 연락처 ID를 위한 검증기관을 선택하는 것이 가능하다.[19]
84.	연락처 ID의 관리와 관련된 감독 및 책임성 정책을 반드시 개발해야 한다.
85.	연락처 보유자는 반드시 발급 검증기관을 통해 연락처 ID와 연결된 연락처 정보를 수정할 수 있어야 한다.
86.	검증기관들은 반드시 연락처 보유자 인증을 사용해서 특정 연락처 ID와 연결된 연락처 정보의 부단 수정을 억제해야 한다.
87.	검증기관은 기본적인 PIN 인증부터 이중 인증(two-factor authentication)까지 다양한 수준의 연락처 보유자 인증을 제공할 수 있다. 연락처 보유자는 반드시 사용의 편의성, 보안, 비용 및 기타 논리적인 사업 요인들과 연관된

[19] 88번 원칙에 따라 연락처 ID는 검증기관과 연락처 보유자 모두를 식별해야 한다. 이것은 검증기관들 사이에서 연락처 ID 이동을 가능하게 하는 방식으로 구현되어야 한다.

	비용/편익 제안을 기초로 서비스 제공업체를 선택하는 것이 가능해야 한다.

76페이지

번호.	연락처 보유자 및 검증기관 사이의 상호작용 원칙
88.	검증기관은 반드시 평판 관리를 위해 전세계에서 활용가능한 방식으로 인증에 관한 정책을 발표해야 한다. 이로써 열거된 연락처 정보의 정확성과 정보에 대한 책임성이 향상될 것이다.
89.	검증기관은 반드시 연락처 보유자의 모국어로 제출된 연락처 정보를 검증할 수 있어야 한다. 이로써 모국어 데이터의 정확성을 향상시키고 도메인네임 등록 시스템을 다국어 환경으로 확장시킬 수 있어야 한다. 예를 들면, 도메인 소유자는 자신의 직원들에게 익숙하지 않은 언어로 된 데이터를 검증하기 위해 값비싼 도구에 투자하지 않더라도 다양한 지역에서 검증기관과 협력해 수많은 도메인 소유자 및 지정 연락처를 위해 확장된 검증 서비스를 제공할 수 있다.

f. 연락처 검증 원칙

연락처 데이터는 SAC 058에 따라 세 가지 수준의 검증, 즉 구문(syntactic) 검증, 운영상(operational) 검증 그리고 신원(identity) 검증이 가능하다.

번호.	연락처 검증 원칙
90.	특정 연락처 ID와 연결된 모든 연락처 데이터 요소들은 반드시 구문 검증을 해야 한다. 구문 검증은 기본적인 검증 수준으로 반드시 업계에 종사하는 어떤 실체라도 실행 가능해야 한다.
91.	특정 목적을 위한 연락처 ID와 연결된 모든 의무적 연락처 데이터 요소에 대해 해당 연락처 ID를 해당 목적을 위한 도메인네임 등록 정보에 포함시키기 전에 반드시 운영상의[20] 검증을 해야 한다.
92.	연락처 보유자는 자의에 따라 선택사항인 더 높은 수준의 검증(예, 선택사항인 신원 검증)을 실시할 수 있으며 관련된 비용을 부담하는 대신 인지된 이점(예, 신원이 검증된 실체가 등록한 도메인네임에 대한 소비자 신뢰도 증가) [21]을 얻는다.
93.	선택사항인 신원 검증을 위해 비용이 수반될 경우, 경제적 여건이 좋지 않은 연락처 보유자가 선택사항인 신원 검증을 실시할 수 있는 저비용

[20] 운영상의 검증 및 기존의 국가도메인 관행에 관해서는 SAC 058과 *국가도메인 WHOIS 데이터 확인/검증 설문조사 결과 요약*을 참조한다.

[21] 예를 들면, 선택사항인 신원 검증은 별도로 비용을 청구하는 애드온으로 또는 high-volume 고객들에게 제공되는 인센티브로 도메인네임 등록 패지지에 번들로 묶어 제공할 수도 있다. 그러한 검증을 제공하는 상업 서비스의 예는 *연락처 데이터 검증 및 확인 시스템에 관한 RFI*를 참조한다.

번호.	연락처 검증 원칙
	메커니즘이 필요하다.
94.	연결 관계를 유지하고 정정 절차를 허용하기 위해 연락처 ID는 “부정확” 상태를 표시한 채로 시스템에 남아 있을 수 있다.
95.	RDS 정보에 접근했을 때, 가장 최근에 검증 상태가 결정된 시간과 함께 연락처 ID의 검증 상태가 반드시 추적되고 공개되어야 한다.
96.	섹션 V(c)에서 설명한 것처럼 제3자가 연락처 ID의 검증 상태에 이의를 제기하기 위해 부정확성 신고를 할 수 있고, 이 경우 표준 수정 절차를 통해 연락처 ID가 “부정확한” 것으로 표시가 되고 해당 연락처 ID를 PBC로 사용하는 도메인네임에 추가적인 조치가 취해질 수도 있다.
97.	유효한 도메인이라면 의무적 연락처가 어떤 수정 절차도 이루어지지 않은 채 “부정확” 상태로 남아 있어서는 안 된다. 그러나 운영 계획은 다른 곳에서 결정이 가능하다.
98.	교차 필드(cross-field) 검증이 적용 가능한 경우, 연락처 ID와 연결된 모든 연락처 데이터 요소에 대해 최소 수준의 교차 필드 검증을 반드시 체크해야 한다. (예, 물리적 주소)
99.	데이터가 선언된 수준에서 정확한 지 확인하기 위해 검증기관은 반드시 연락처 데이터를 주기적으로 재검증해야 한다.
100.	연락처 보유자가 선택사항인 데이터 요소를 제공할 경우, 해당 데이터 요소에 대해 최소한 구문 검증을 반드시 실시해야 한다. 선택사항인 데이터 요소의 경우 연락처가 요청하거나 관련된 비용을 지불하지 않는 한 구문 검증 이상의 검증은 이루어지지 않을 것이다.
101.	운영상의 검증 또는 (선택사항인) 신원 검증이 가능한 데이터 요소에 대해 구문 검증을 넘어서는 수준의 검증을 실시한 경우 반드시 검증기관이 기록해서 보관해야 한다. 예를 들면, 이메일, 전화번호 및 주소 같은 요소들은 운영상의 검증이 가능한 반면 이름이나 조직명은 운영상의 검증은 불가능하지만 선택사항인 신원 검증은 가능하다.
102.	또한 검증기관은 각 연락처 ID가 달성한 전체적인 검증 상태를 결정하고 하나의 RDS 데이터 요소로 공표해야 한다. 예를 들면, 운영상 검증이 가능한 모든 의무적 데이터 요소가 검증을 통과할 경우, 해당 연락처의 전체 검증 상태는 “운영상 검증됨”이 될 것이다.

78 페이지

번호.	연락처 검증 원칙
	신원 검증이 가능한 모든 의무적 데이터 요소가 이 선택사항인 검증을 통과할 경우 해당 연락처의 전체 검증 상태는 "신원 검증됨"으로 업그레이드 될 것이다. 정확성을 높이고 효율적 의사소통을 위해 반드시 RDS 사용자들이 이 전체 검증 상태를 연락처별로 하나의 새로운 통합 데이터 요소로서 이용할 수 있어야 한다.[22]
103.	또한 검증을 실시한 모든 데이터 요소에 대해 검증기관은 반드시 해당 검증을 실행한 시간을 기록하고 보관해야 한다.
104.	검증기관은 반드시 가장 최근에 전체 연락처 ID의 전체 검증 상태가 변경된 시간을 결정하고 연락처별로 새로운 RDS 데이터 요소로 공개할 수 있어야 한다.

g. 고유 연락처 데이터 능력(Unique Contact Data Capability)

위장, 명예 훼손 및 오용을 막기 위해서 연락처 보유자는 자신의 연락처 데이터가 고유하고 연락처 보유자라 주장하는 다른 사람에 의해 절대 사용되지 못하도록 지정할 수 있다.

a) 고유 데이터에는 특히, 이메일 주소와 전화번호를 비롯해 많은 연락처 데이터 요소들이 포함된다. 주소와 이름의 경우 고유성을 보장하기가 어렵거나 불가능하다.

b) 연락처 보유자가 고유성 지정을 요청할 경우, 반드시 다른 검증기관들이 요청된 연락처 데이터 세트를 연락처 보유자의 데이터 세트와 비교할 수 있는 메커니즘을 제공해서 새로운 연락처 ID 신청자(또는 정보를 수정하는 기존의 연락처 보유자)가 고유하게 보호되는 데이터에 나쁜 영향을 주지 않도록 해야 한다.[23]

c) 고유한 것으로 지정된 데이터는 반드시 신원 검증을 실시해 위장 및 "서비스 부인"과 같은 유형의 공격(합법적 연락처가 자신의 진실한 데이터를 사용할 수 없는)을 방지해야 한다.

---

[22] EWG는 각 개별 연락처 데이터 요소의 개별 검증 상태를 알리기 위한 RDS 데이터 요소를 공개하는 것도 고려했다(예, PBC 이메일 주소 상태 = 운영상 검증됨, PBC 네임 상태 = 신원 검증됨). 이처럼 세밀하게 검증 상태를 공개해야 할 경우 프로토콜, 데이터 요소 및 클라이언트 응용프로그램/GUI를 크게 변경해야 하고 따라서 현재로서는 권고하지 않는다. 그러나 좀 더 연구해 볼 가치가 있다.

[23] 이 고유성 점검은 동기화 모형에서는 비교적 쉽게 실행하는 것이 가능하지만 연합 RDS 모형에서는 좀 더 실행이 까다로울지도 모른다.

h. 데이터 품질 원칙의 주요 이점 요약(Summary of Data Quality Key Benefits)

연락처 ID 관리 및 검증 시스템을 차세대 RDS 시스템의 필수적인 일부로 채택한다면 도메인 소유자들이 RDS에 허위 데이터를 삽입하기 어렵게 되고 사기 및 신원 오용 사고가 줄어 데이터 품질이 향상될 것이다. EWG가 권고하는 데이터 정확성 및 검증 원칙들을 채택할 경우 얻을 수 있는 이점들을 구체적으로 말하자면 다음과 같다.

- 개인 및 조직이 자신의 연락처 데이터가 도메인네임 생태계 어디에서 사용되든 해당 데이터를 통제하고 관리하는 능력이 향상된다.
- 범법자들이 도메인네임을 획득하기가 훨씬 어려워진다. 모든 연락처가 생성 또는 갱신될 때 최소한의 수준에서 반드시 검증을 거치기 때문이다. 검증기관 인증 요건은 운영상의 기준을 충족하지 않는 허위 또는 사기적 검증기관을 식별하고 제재할 수 있어야 한다. 한 도메인의 등록정보로 범법자가 확인될 경우, 공통의 PBC를 통해 동일 범법자가 보유한 다른 도메인들을 식별하고 범죄를 완화할 수 있다.
- 특정 도메인 소유자가 등록한 여러 개의 도메인네임에 걸쳐 좀 더 일관된 데이터를 생성한다. 특정 연락처를 위해 초기 검증 비용이 발생할 수 있지만 이동이 가능한 연락처 ID를 제공함으로써 추가 등록이 쉬워지고 향후 많은 도메인 소유자들의 유지 관리 비용이 대폭 감소한다.
- 시간이 지나면서 더 이상 유효하지 않은 연락처 정보를 탐지하고 해당 연락처 정보를 이용해서 전체 도메인 집합을 수정하는 능력이 향상된다. 검증기관이 주기적으로 검증하거나 업데이트 할 때 검증을 실시함으로써 오래되어 정확하지 않은 연락처 정보로 인한 문제를 파악하고 한 번의 변경으로 모든 업데이트 내용의 영향을 받는 모든 도메인네임에 적용할 수 있다.
- 전체 생태계의 비용과 효율성이 개선된다. 전체 등록 시스템이 좀 더 복잡해지기는 하겠지만 연락처 관리를 도메인 등록 관리와 분리함으로써 도메인에 대한 대규모 업데이트 적용을 허용하고 연락처 데이터 관리의 국지화가 가능하다.
- 서비스 제공업체들이, 목적별 연락처로 표시되는 도메인들을 위해 개별 도메인 등록정보를 일일이 수정할 필요 없이 연락처 정보를 유연하게 업데이트할 수 있다. 덕분에 많은 서비스 제공업체들이 수천, 심지어 수백만 개의 도메인네임을 손쉽게 업데이트할 수 있다.

- 선택사항인 신원 검증을 제공함으로써 등록정보 도용으로 발생하는 오용 사건이 감소한다. 선택사항인 신원 검증으로 인해 연락처 보유자에게 비용이 발생할

가능성이 있지만 유명 기업, 대규모 서비스 제공업체 또는 악의적 공격의 표적이 된 개인들이 종종 경험하는 도용(신원 절도)을 통한 오용 사고를 줄일 수 있다면 그만한 가치가 있을 것이다.

- 연락처 데이터 관리 및 검증을 도메인네임 등록/관리와 분리함으로써 데이터 주체를 그들의 데이터에 맞춰 긴밀하게 배열한다. 등록대행자 또는 관리기관 위치에 관계없이 검증기관을 데이터 보유자의 관할지역에 위치시킬 수 있기 때문에 관련 정보보호법을 좀 더 쉽게 적용할 수 있다.
- 검증기관은 연락처 보유자 및 도메인 소유자의 모국어로 서비스를 제공할 수 있어 데이터 품질과 정확성이 향상되고 따라서 검증 비용도 감소한다. 도메인 소유자는 일단의 분산된 검증기관을 통해 직접 지원하거나 검증하기가 쉽지 않은 언어로 서비스를 제공할 수 있다.

VI. 법률 및 계약 관련 고려사항

본 프로젝트를 수행하면서 EWG 는 상위에 있는 법 원칙들을 고려했다.

개인 정보는 반드시, • 합법적으로, 공정하게, 그리고 데이터 주체와 관련해 투명한 방식으로 처리되어야 하며, • 구체적이고 명확하며 합법적인 목적을 위해 수집되어야 하며 이러한 목적에 부합하지 않는 방식으로 추가적인 처리가 이루어져서는 안 되고, • 처리 목적에 적절하고, 연관성이 있으며 꼭 필요한 최소한으로 제한되어야 하며, • 명시된 목적에 맞게 정확하고 최신 상태를 유지해야 한다.
다음의 요건을 근거로 관련 관할지역에 따라 정보의 전송 및 공개를 비롯한 합법적 처리가 가능하다. • 정보 주체의 동의 • 정보 주체를 당사자로 하는 계약의 필요성 • 정보 관리자에게 적용되는 법적 의무를 준수해야 할 필요성
정보 주체의 정보 접근 권한 및 부정확한 정보를 수정할 권한을 보장해야 한다.

EWG는 RDS를 위한 최종 정책 및 이행 과정의 초안을 작성할 때 위의 원칙들과 기타 정보보호법에 따른 관련 원칙들을 고려할 것을 권고한다. 그리고 잘 알려져 있듯이 일부 관할지역에서는 프라이버시 권리가 언론의 자유 및 결사의 자유와 관련해 법인과 실체에도 확대 적용된다. EWG는 관할 지역에 따라 서로 분리되어 그리고 서로 다르게 보호되는 이 두 가지 권리를 모두 인정한다.

이러한 상황을 고려해서 EWG는 프라이버시 및 정보보호와 사법기관의 등록정보 접근을 위한 선택안들을 평가한 다음 RDS 원칙들을 마련했다. 이번 섹션에서는 이러한 EWG 권고 원칙들을 소개하고 계약 이행, 책임성 및 감사를 위한 원칙들로 뒷받침한다.

82페이지

a. 정보보호 원칙

현재 프라이버시 및 정보보호에 적용 가능한 국가 수준의 법률 문제를 해결하고자 고안된 알려진 실천방안들은 서로 일관성이 없다. 일부 법에서는 그 지배를 받는 개인이나 데이터 처리자의 관할권 밖으로 데이터를 내보낼 때, 법에서 요구하는 것과 유사하거나 그에 상당하는 수준의 정보보호를 요구한다. 1995년 유럽정보보호지침 (European data protection directive of 1995)은 지역 수준의 법이 "적당한" 것으로 판단되지 않을 경우 해당 관할권 밖으로 데이터를 전송하지 못하도록 규정하고 있다. EU 이외의 다른 많은 관할권의 경우 강력한 계약 조항을 찾았지만 어쨌든 대부분의 법에서는 개인 정보 보유자가 확실한 보호가 보장되지 않는 한 동의 없이 다른 관할권으로 데이터를 내보내거나 공개하지 못하도록 규정한다. 이 전송 지점에서 책임 문제가 발생할 수 있다. 지금까지 ICANN은 등록대행자가 데이터 에스크로를 금지하는 정보보호법의 적용을 받는다는 사실을 입증할 경우 RAA 계약에 면제 조항(waiver)을 두도록 허용함으로써 이 문제를 다루어왔다. 이것이 ICANN 생태계에서 정보보호법을 준수하고자 하는 사람들에게 위험이 될 수 있는 유일한 조항은 아니기 때문에 현 상태를 좀 더 주의 깊게 조사하자는 제안이 있었다. EWG가 이번 프로젝트를 수행함에 있어 책임성에 초점을 맞추고 이를 또 강조하기 때문에 정보보호에 대한 책임성 요건을 조사했다.

현재 개인 정보를 제공 받는 실체가 반드시 "집에 있는(at home)" 정보 주체에게 제공되는 보호 장치에 부합하는 수준의 적절한 보호를 보장해야 한다는 요건은 정보를 제공 받는 실체가 법률로 제정된 데이터 보호 수단이나 그와 유사한 적당한 보호 수단을 제공하는 관할권에 속해 있느냐 여부에 따라 **사례별로**(case-by-case) 충족되어야 할 것이다. 다시 말해, 데이터를 제공받는 실체에게 적용 가능한 법률로 적절성을 보장하든지 아니면 데이터 전송이 데이터 주체에게 적용 가능한 법 하에서 합법적으로 이루어지도록 허용하는 기타 보장 장치가 마련되어야 한다는 것을 의미한다.

정보 보호 메커니즘

현재 상황을 고려했을 때 RDS 생태계에서 개인 정보를 보호하기 위한 4가지 점증적 옵션들을 검토했다.

(0) 아무런 조치도 취하지 않는다.

(1) 법에 부합하는 일상적 데이터 수집 및 전송을 위한 메커니즘을 도입한다.

(2) ICANN 생태계 전반에 걸쳐 프라이버시 및 데이터보호 개념을 조화시켜 기본적인 데이터 보호 "토대"를 제공하고 인정받는 프라이버시 정책의 모범 사례들을 확립하기 위한 메커니즘을 도입한다.

(3) 그러한 정책을 일단의 “구속력 있는 기업 규칙”으로 제출한다.

83페이지

> **참고:** 이번 섹션에서 “RDS 생태계”란 VIII(c), ‘계약 관계 및 컴플라이언스’와 VIII(d), ‘책임성과 감사’ 섹션에 열거된 모든 행위자들을 가리킨다. 여기에는 ICANN(미국 비영리 법인), 모든 일반도메인 관리기관 및 등록대행자(각각이 다양한 국가에 기반을 둔 독립 법인으로 활동한다.) 그리고 EWG가 본 문서에서 제안하는 모든 새로운 실체, 즉 RDS 제공업체(RDS Provider), 검증기관(Validator), 보안 보호 크리덴셜 인증 기구(Secure Protected Credential Approvers), ICANN 컴플라이언스 및 기타 개인정보 취급에 관여하는 실체들을 포함한다.

옵션(0): “아무런 조치도 취하지 않는다.”

아무것도 하지 않을 경우 정보보호법을 지속적으로 위반하게 되고 도메인을 등록할 때마다 적용 법률을 결정하기 위해 조사해야 하기 때문에 복잡성의 수준이 크게 올라갈 것이다. 일부 운영자, 특히 관리기관의 입장에서 볼 때 상당한 간접비를 초래할 것이다. 등록대행자의 경우에도 도메인 소유자와 관리기관이 요구하는 보호의 적절성을 감시하기 위해 많은 비용이 소요될 지도 모른다. 또한 ICANN과 DNS의 다른 모든 이해관계자들에게도 잠재적인 법적 불확실성을 가중시킬 것이다. 일반도메인의 수적 증가와 관리기관 위치의 다양성은 적용 법률 및 관할권과 관련해 새로운 문제를 야기하는데 ICANN의 계약 체계가 도메인 소유자의 프라이버시 및 소비자 보호와 관련이 있기 때문이다. 복잡하고, 불확실하며, 일관되지 못한 관행들로 인해 ICANN은 계약 준수를 보장하고 잠재적 위험을 줄이기 위해 더 많은 노력을 기울여야 할 것이다. 이러한 과제들은 RDS 문제와는 독립적으로 존재한다. 1000개 이상의 일반도메인이 생겨날 경우 문제는 더욱 심각해진다. 무엇보다 중요한 것은 정보 주체의 보호가 일관성 있게 보장되지 않는다는 점이다. 위험은 줄이고 부담은 최소화하며 복잡성은 완화해 줄, 모든 이해관계자들의 이익에 부합하는 조화로운 프레임워크가 필요하다.

옵션(1): 법을 준수하는 일상적인 데이터 수집 및 전송을 위한 메커니즘을 도입한다.

두 번째, 관련 프라이버시 및 정보보호법을 평가하고 이해관계자들이 적용할 수 있도록 그리고 개인들이 자신의 정보가 어디에 있는지 그리고 어떤 법이 적용되는지 알 수 있도록 하나의 목록으로 법률을 제시하는 시스템을 도입하는 방안을 고려했다. 이 목록은 RDS가 다음 섹션에 정의된 “규칙 엔진”을 통해 자동으로 적용이 가능하다. 예를 들어 어떤 개인이 정보보호법이 갖춰진 국가에서 살고 있고 그 법이 국가 밖에서 그 개인으로부터 다른 당사자(이 경우 등록대행자)에게 전송되는 개인 정보에 적용된다면,

그 법이 적용될 지도 모른다. 만약 그 등록대행자가 정보보호법이 모든 개인(즉, 자국 국민뿐만 아니라)에게 적용되는 국가에 소재하고 있다면 그 법은 확실히 적용될 것이다.

84페이지

문제의 데이터 또는 우리의 목적을 위한 범위에 있는 데이터는 RDS에서 수집되는 데이터로 한정된다.[24] RDS 생태계에서 적용되는 관할권에 관한 데이터를 부호화한다면 관련 이해관계자들의 일이 훨씬 수월해지고, 도메인 소유자들의 정보보호에 대한 권리(해당사항이 있는 경우)가 보장되며, 위반 위험도 감소할 것이다. 그러나, 도메인네임 등록 업무, 관리기관 또는 ICANN과 그 준법 메커니즘에 적용되는 정보보호법이 제정되어 있지 않은 관할권에서는 이 시나리오가 개별 도메인 소유자를 거의 보호하지 못한다. 그럴 경우 프라이버시 권리에 대한 다층적 시스템이 초래되어 일부 개별 도메인 소유자는 전혀 인권을 보장받지 못하는 데 반해, 또 다른 도메인 소유자들은 사법적 감독과 함께 완벽한 인권과 소인(a cause of action)을 가지게 될 것이다.

옵션(2): RDS 생태계 전반의 정보보호 장치들을 조정해 인정 받는 프라이버시 정책 우수 사례들에 부합하는 정보보호 "기층(floor)"을 제공할 메커니즘을 도입한다.

프라이버시 보호와 관련한 허점(구현 중 추가적으로 논의)을 메우기 위한 계약 조항들을 마련할 수 있으며 이러한 조항들을 고안할 때 공통적으로 인정되는 프라이버시 보호 수단들을 고려해야 할 것이며 ICANN 프라이버시 정책의 근간을 이루게 될 것이다. 이러한 정책은 관련 조항들을 하나의 부록으로 열거하는 방식으로 간결할 수도 있다. 그럴 경우 개인의 프라이버시, 정보 보호 및 소비자 권리를 이유로 내세운 반대를 방지할만큼 충분히 높은 수준의 정보 보호를 제공함으로써 RDS 생태계를 구성하는 행위자들 사이의 자유로운 데이터 전송을 허용한다.

RDS 생태계 전반에 걸쳐 법을 준수하는 일상적인 데이터 수집과 전송을 장려하기 위한 메커니즘은 여러 가지 다른 형태를 취할 수 있지만 모두가 RDS에 적용가능한 일관된 정보보호 정책을 기반으로 할 것이다. ICANN은 대부분의 다른 정책들과 마찬가지로 계약 조항을 통해 모든 이해관계자들이 이 정책을 따르도록 할 것이다.

옵션(3): 위의 옵션 (2)를 토대로 개발된 정책을, APEC과 EU가 프라이버시/정보보호법에서 인정한 일단의 "구속력 있는 기업 규칙"으로 제안하는 것이 가능하다.

이 옵션의 경우 EU 회원국들의 목적에 부합하는 적절한 데이터 보호를 결정해 주기 때문에 유럽연합의 28개 회원국들 간의 데이터 전송이 용이해지고 데이터 보호가 RDS

[24] 일반도메인 시스템의 복잡성을 고려할 때 "규칙 엔진"이 일부 상황에서는 확실히 유용하겠지만 금융 거래 정보, 신용 카드 정보, 고객 관리 정보와 같이 RDS로 전송되지 않는 훨씬 더 민감한 데이터를 관리하는 등록대행자의 경우 반드시 일이 더 수월해지지는 않을 것이다.

생태계 전반에 걸친 데이터 흐름에 의해 결정되는 임시변통적 성격이 사라질 것이다.

이 옵션의 경우 상대적으로 많은 시간이 소요되겠지만 불이행(non-compliance)의 위험을 줄이고 더 나은 보호 수준을 제공할 것이다. 또한 프라이버시 정책에 대한 독립적인 감독이 가능해질 것이다.

번호	EWG가 고려한 정보보호 메커니즘 요약
(0)	아무런 조치도 취하지 않는다.
(1)	최소한의 솔루션으로, a) 법에 의해 적절한 프라이버시 보호가 이루어지는 데이터 전송을 식별하고 해당 목록을 공표한다. b) 데이터를 전송함에 있어 법적으로 충분히 보호받지 못하는 RDS 생태계 행위자들을 위해 계약서에 공통 규칙을 도입함으로써 준법을 하나의 간단한 유지관리 플랫폼으로 제공한다.
(2)	프라이버시 보호를 위한 표준 우수 사례들을 기초로 RDS를 위한 기본적인 ICANN 프라이버시 정책의 초안을 마련할 수 있고 RDS 생태계 전반에서 이 정책을 실행하기 위한 표준 계약 조항을 개발할 수 있다. ICANN과 데이터 전송에 관여하는 RDS 생태계의 모든 행위자 사이의 모든 계약에 이러한 표준 계약 조항을 포함시켜 행위자들 사이의 자유로운 데이터 전송을 허용하기에 충분히 높은 수준의 정보보호를 보장한다.
(3)	전체 RDS 생태계를 다국적 비영리 법인인 ICANN의 통제 하에 둠으로써 하나의 기구 안에서 세계적인 데이터 전송을 효과적으로 허용하는 것으로 입증된 구속력 있는 기업 규칙(BCR)이라는 법률 문서의 적용을 받을 수 있다. 이 경우, 전체 RDS 생태계가 준수 주체가 된다. ICANN은 정책과 계약 요건을 규정함으로써 APEC과 EU 용어를 빌자면 “데이터 컨트롤러”의 역할을 하는 것으로 보일지도 모른다.

평가:

옵션(0) 아무런 조치도 취하지 않는다. 시스템의 전반적인 복잡성이 증가하고 정확성과 책임성이 더욱 강조되고 있기 때문에 이 옵션은 수용할 수 없는 것으로 판단된다.

옵션(1) 법에 부합하는 일상적인 데이터 수집 및 전송 활동을 위한 메커니즘.

이 옵션의 경우, 관할지역에 따라 법이 다르기 때문에 좀 더 복잡하고 동적이며 생태계 내에서 이루어지는 복잡한 정보의 흐름을 고려해야 할 것이다. 앞에서도 논의했듯이, 개별 도메인 소유자가 이용하거나 의존하는 등록대행자와 검증기관, 관리기관 및 RDS 제공업체들이 모두 서로 다른 관할지역에 속해 있는 시나리오도 불가능한 것은 아니다.

옵션(2) RDS 생태계 전반에 걸쳐 정보 보호를 조율하기 위한 표준 계약 조항. 이 옵션의 경우 이해관계자, 특히 도메인 소유자, 등록대행자, 관리기관 및 ICANN에게 적용 가능 법률의 준수를 요구한다. 또한 여기에는 본 보고서에서 권고한, 검증기관, RDS 제공업체, RDS 사용자 인증 기구 등 새로운 RDS 생태계의 행위자들 역시 포함될 수 있다.

이 옵션은, 지역 수준의 정보보호법 준수를 강제하는 것 외에 APEC과 EU의 정보보호법에서 공통된 요소를 추출할 때 준법 보장에 있어 큰 기여를 할 것이다. 계약 조항을 통해 동의 조건, 접근 권리, 보유 정책 및 기타 요소들을 (예를 들면) 합법적 데이터 처리에 관한 EU 요건과 구속력 있는 기업 규칙으로 해결하기에 적절한 요소들을 포함시켜 명시할 수 있다. 이러한 표준 계약 조항은 해당 허가가 의무적인 관할지역이 아니라면 반드시 정보 보호 기구의 허가/감시를 요구하지는 않을 것이다.

옵션(3) (RDS 생태계를 위한 BCR) 이 옵션은, 지역 수준의 정보보호법 준수를 강제하는 것 외에, APEC과 EU 정보보호법에서 추출한 공통 요소들을 열거할 수 있다. 옵션(2)의 경우와 마찬가지로 계약 조항을 통해 동의 조건, 접근 권리, 보유 정책 및 기타 요소들을 (예를 들어) 합법적 데이터 처리에 관한 EU 요건과 구속력 있는 기업 규칙으로 해결하기에 적절한 요소들을 포함시켜 명시할 수 있다. 이러한 표준 계약 조항은 해당 허가가 의무적인 관할지역이 아니라면 반드시 정보 보호 기구의 허가/감시를 요구하지는 않을 것이다. 그러나, BCR은 RDS 생태계의 특수성을 고려해 조정해야 할 것이다. BCR은 ICANN이 운영하는 느슨하게 연결된 생태계보다는 전통적인 통제 구조를 가진 기업 실체에 좀 더 적합하다는 주장이 있지만 다국적 기업들의 경우 ICANN이 이해관계자들을 인증하고 관리하기 위해 사용하는 것과 동일한 종류의 계약을 통해 구속력 있는 프라이버시 규칙들을 시행하고 있는 것도 분명한 사실이다.

요컨대, "아무런 조치도 취하지 않는다"는, 특히 정확성과 책임성 향상을 위한 EWG의 권고가 받아들여진다면 사실상 대안이 될 수 없다. 옵션(1)은 법적으로 매우 복잡하고 모든 도메인 소유자들에게 평등한 권리를 제공하지 않는 반면 옵션(3)은 RDS 생태계 내에서 실질적으로 적용가능한가 하는 우려(즉, 구속력 있는 기업 규칙이 실현가능한지, 받아들여 질 것인지 그리고 책임성의 측면에서 ICANN에 어떤 의미를 가지는지)가 제기된다. *따라서, EWG는 옵션(2)를 권고한다. 즉, 표준 계약 조항을 이용한 정책을 개발함으로써 정책의 요건을 이행하기 위해 정보보호법들과의 조율을 모색하고 다양한 감사 메커니즘을 통해 이러한 프라이버시 보호수단들이 개인 정보 취급에 관여하는 모든*

RDS 생태계 행위자들 사이의 계약을 통해 강제될 수 있도록 보장한다.

정보보호 메커니즘의 구현

위에 언급한 모든 시나리오가 RDS 구현 문제, 특히 RDS 제공업체의 국지화와 관련성이 있다.

RDS가 개인 정보를 보유하게 될 경우, 그러한 데이터가 강제성 있는 정보보호 권한을 제공하는 관할지역에 위치해 있다면, 데이터 전송의 적법성과 데이터 침해에 대한 책임성과 관련된 질문들에 대한 답변을 회피하기에 용이할 것이다. 만약 RDS가 데이터 처리자와 같은 장소에 있는 상주 데이터를 보유할 경우 이는 더욱 명백해 진다. 상주 데이터가 아니지만 처리(예, 검증)를 위해 그곳으로 가져왔고 그 후에 다른 곳으로 보내졌다 하더라도 비슷한 방식으로 고려되어야 한다. EWG는 다음과 같은 세 가지 정보보호 구현 방안을 고려했다.

번호	EWG가 고려한 정보 보호 구현 방안 요약
(0)	"아무런 조치도 취하지 않는다."는 옵션은 RDS 국지화를 위한 위치를 선택하면서 적용 가능한 법적인 정보보호 수준을 고려하지 않을 경우에나 가능하다. 이 경우, 정보보호 수준이 매우 낮은 관할 지역에서 RDS 국지화가 이루어질 가능성도 존재한다.
(1)	RDS가 법적 분류 체계를 제공할 수 있다. 다시 말해, 정보 주체(즉, 도메인 소유자)에 적용 가능한 법률에 따라 데이터 요소에 표시를 하고 그에 따라 취급할 수 있다. 이러한 법적 분류를 위해 RDS는 각각의 특정한 데이터 전송에 적용 가능한 정보보호법을 적용하는 "규칙 엔진"을 구현할 수 있다. 좀 더 구체적으로 설명하자면, "규칙 엔진"은 RDS 내에서 구현 가능한 하나의 기능을 가리키며 (a)도메인 소유자, 연락처, 등록대행자, 관리기관 및 RDS 관할 지역(각각 도메인 소유자와 연락처 국가 코드, 등록대행자 및 관리기관 관할지역으로 대표되는)에 기반한 도메인네임 정보의 저장, 수집 및 처리와 (b)앞으로 정의될 ICANN의 RDS 정책에 따라 적용 관할지역의 정보보호 법률을 관리한다. 위에서 설명했듯이 이러한 규칙 엔진은 본질적으로 복잡하며 RDS가 호소할 정보보호법이 없는 관할지역에 있을 경우 시행이 어렵다.

번호	EWG가 고려한 정보 보호 구현 방안 요약
(2)	RDS 국지화는 가장 쉽고 가장 덜 복잡한 데이터 전송 기준에 따라 선택한다. 즉, 적용 가능한 국가 수준의 정보보호법이 높은 수준의 보호를 제공하는 곳으로 데이터 저장 장소를 선택하라는 의미이다.

평가:

옵션(0) "아무런 조치도 취하지 않는다."는 현 상태를 그대로 유지하며 다음과 같은 이유로 데이터 전송의 복잡성을 가중시킨다.

법적 프레임워크를 따르기 어렵거나, 사실상 거의 불가능하게 만드는 과정으로 되돌아간다.

- 등록대행자는 물론 ICANN 컴플라이언스를 비롯해 생태계의 다른 행위자들에게 과중한 행정적 및 법적 부담을 지운다.
- 지역 정보보호법 및 프라이버시 준수와 관련해 전혀 투명하지 않고 확장성도 부족하다.

옵션 (1) "엔진 규칙"을 통한 법적 구획화(legal compartmentalization)는 혁신적이긴 하지만 그 실현가능성에 있어서는 기술적 검증이 필요하다. 법적인 측면에서, 특히 그러한 시스템의 정의, 법적 승인 및 구현과 관련해 수많은 문제들이 제기될 수 있다.

옵션(2) 선택된 관할지역으로의 데이터 국지화(data localization)는 모든 데이터 이동을 위해 높은 수준의 법적 보호가 가능한 명확하면서도 간단한 솔루션이다. 그러나 이 옵션만으로는 모든 정보 주체의 지역 수준의 정보보호법 적용을 실현하기 어렵다.

옵션 (0)은 타당한 대안이 아니고 옵션(1)과 (2)는 상호 배타적이지 않기 때문에 *EWG는 정책과 표준 계약 조항을 통해 수준 높은 정보 보호를 실현할 수단으로 옵션(1)과 옵션(2) 모두를 고려할 것을 권고한다.*

정보보호 정책, 메커니즘 및 구현을 둘러싼 이 모든 대안들을 고려한 후에 EWG는 다음과 같은 원칙에 합의했다.

번호	정보 보호 원칙
105.	RDS 생태계를 이루는 행위자들 사이의 일상적인 데이터 수집 및 전송 활동이 법에 부합해 이루어지도록 하기 위한 메커니즘을 반드시 채택해야 한다.

106.	프라이버시 및 정보보호법과 조화를 이루는 표준 계약 조항을 정책으로 명문화

번호	정보 보호 원칙
	하고 개인 정보를 취급하는 모든 RDS 생태계 행위자들 사이의 계약을 통해 시행해야 한다.
107.	정보보호법 적용을 위한 정보 시스템(즉, “규칙 엔진”) 및 RDS 데이터 저장소의 국지화는 수준 높은 정보 보호 구현을 위한 두 가지 수단으로서 반드시 고려해야 한다. 이는 반드시 RDS 생태계를 위한 논리적 프라이버시 정책에서 나온 표준 계약 조항을 통해 보장해야 한다.

b. 사법 기관의 데이터 접근 원칙

정보보호의 경우와는 달리 사법기관이 정보에 접근하는 경우 정보 주체에 대한 법적 보호는 (“내보내기”가) 불가능하다. 사법기관에 의한 접근을 위해, 다음의 세 가지 옵션을 고려했다.

번호	사법적 접근과 관련해 고려한 옵션 요약
(0)	“아무런 조치도 취하지 않는다.” 사법기관의 접근은 사법기관이 해당 국가 수준에서 각 데이터 저장소에 저장된 RDS에 접근할 수 있는 권한이 있는 한 기존의 규칙을 따를 것이다. 중앙집중화된 RDS 포털에서는, RDS 포털 호스트 국가의 국가법에 따라 접근성이 부여될 것이다.
(1)	중앙 RDS 포털 수준에서, 데이터를 공개적으로 이용할 수 없고 해당 국가 법률에 따라 사법 기관이 특정한 법적 절차를 요구하지 않을 경우, RDS 시스템을 위한 접근 조건을 규정하고 다음 두 가지 방식으로 이행할 수 있다. a) 유로폴(Europol)과 인터폴(Interpol)은 해당 시스템을 구현하고 실행하기 위해 RDS와 계약을 체결하고 모든 사법적 접근을 위한 적극적인 실시간 중개자 역할을 하고 적절한 정보 보호 및 사용에 대한 책임을 진다. b) 유로폴과 인터폴은 RDS와 계약을 체결하고 사법 관련 커뮤니티를 위한 사용자 인증 기구 역할을 할 수 있다. 신청자들을 조사해서 개별 사법 기관들이 제한적 RDS 데이터에 접근하기 위해 사용하는 RDS 크리덴셜을 발급하고 적절한 정보 보호와 사용을 책임진다.

90페이지

번호	사법적 접근과 관련해 고려한 옵션 요약
(2)	또한, 상호사법공조협약(MLAT)을 통해 처리되는 기존의 쌍무적 관계에서 구체적인 요건이 존재하는 경우에도, 사법기관의 중앙 RDS 포털 접근을 허용하는 메커니즘을 확립하는 것도 가능하다. 적용 법률과 관련한 데이터의 구획화를 통해 해당 메커니즘 확립을 지원할 수 있다.

평가:

옵션(0) ("아무런 조치도 취하지 않는다.")은 사법기관을 위해 어떤 부가적인 가치도 제공하지 못한다.

옵션(2) (RDS 사용자 접근 포털 수준의 MLAT) 사법기관이 RDS를 통해 접근가능한 제한적 데이터 요소에 접근하기 위해 지금보다 더 까다로운 허가가 필요할 것으로 보이진 않는다. 따라서 옵션(2)는 더 이상 고려할 필요가 없다.

옵션(1)(인증된 RDS 사용자 접근 포털 방식)은 사법기관의 접근성을 향상시킨다. 두 가지 변형 (1a)와 (1b) 모두 기존의 구조를 토대로 하지만 변형 (1a)(실시간 중개자를 통한 구획화로 접근 인증)은 기존의 사법기관 공조 메커니즘을 토대로 하고 있어 추가적인 복잡성을 더하지는 않을 것이다. 그러나 잠재적인 개별 오용 사고를 탐지하고 해결하는 능력은 계속 보장되어야 한다.

변형 (1a)는 인터폴과 같은 잠재적인 인증 기구가 어떻게 허가된 사법기관의 접근 요청을 RDS에 전달하고 잠재적인 오용을 억제하는지 상세히 설명한 섹션 IV(c), 'RDS 사용자 인증', 시나리오 3번에서 살펴 보았다. 관련 권고사항은 'RDS 사용자 인증 원칙'을 참조한다..

또한 옵션(1)과 관련해 RDS 데이터가 저장된 관할지역의 국가 사법기관을 위한 법적 프레임워크가 RDS를 위해 확립된 프레임워크에 우선하지 않도록 보장해야 한다. 따라서 RDS 국지화의 지리적 위치가 매우 중요하다.

번호	사법적 접근 원칙
108.	RDS는 반드시 구현 모형에 관계없이 글로벌 수준에서 볼 때 사법기관을 신뢰할 수 있는 관할지역에 데이터를 저장해야 한다.

c. 준법 및 계약 관계 원칙

EWG 는 RDS 생태계를 구성하는 당사자들 간의 계약 관계와 관련해 다음의 원칙들을 권고한다.

번호	계약 관계 원칙
109.	비정부 조직이며 활동 범위가 세계적 수준인 제3자 서비스 제공업체가 RDS를 운영해야 한다.
110.	ICANN은 반드시 제3자 RDS 운영업체와 가용성, 감사 및 준법을 위한 적절한 계약을 체결해야 한다.
111.	ICANN은 반드시 검증기관, 프라이버시/프록시 서비스 제공업체, 보안 크리덴셜 인증업체 및 기타 RDS와 상호작용하는 업체들과 적절한 계약을 체결해야 한다.(섹션 III(c), 1번 원칙을 참조한다.)
112.	ICANN은 반드시 RDS를 수용하고 레거시 요건들을 없앨 수 있도록 기존의 계약(RAA, 관리기관 계약)을 수정해야 한다.
113.	RDS는 기존의 것이든 새로운 것이든 반드시 모든 일반도메인 관리기관에 적용해야 한다. 어떠한 기득권 인정이나 예외가 허용되어서는 안 된다.

d. 책임성 및 감사 원칙

EWG 는 RDS 생태계의 행위자들이 등록정보로 취한 행동에 대해 다음과 같이 책임지게 할 것을 권고한다.

번호	책임성 및 감사 원칙
114.	RDS 생태계의 모든 구성원들은 반드시 표6에 명시된 하나 이상의 요건을 책임져야 한다. a) 정확하고 신뢰할만한 등록정보를 제공한다. b) 등록정보를 오직 지정된 목적을 위해서만 사용한다. c) 수집, 저장 또는 전달된 정보의 보안을 유지한다. d) 정보를 수집할 때 유효성을 검사하거나 인증한다. e) 기존에 제공된 등록정보를 기한에 맞게 업데이트한다. f) RDS 프라이버시 정책과 이용 약관(ToU)을 시행한다. g) 등록정보 오용을 탐지한다. h) 민원을 해결하고 추적한다. i) 확립된 ToU 및 ToS 정책을 준수한다. j) 제3자 데이터 수확 및 사기적인 대량 계정 생성을 억제하기 위한 메커니즘을 확립한다.

	k) 지속적인 감사 및 교정 절차를 확립한다.

92 페이지

번호	책임성 및 감사 원칙
	다음의 이해관계자들[25]은 RDS 생태계에서 책임성 있게 역할을 수행해야 한다. a) 데이터를 구하는 RDS 사용자(USD) – 섹션 III 참조 b) 도메인 소유자 c) 등록대행자[26] d) 관리기관[27] e) 등록정보 디렉토리서비스 제공업체 f) ICANN g) 프라이버시 또는 프록시 서비스 제공업체 h) 보안 크리덴셜 인증 기구 i) 검증기관 j) RDS 사용자 인증 기구 k) 목적별 연락처 l) 에스크로 서비스 제공업체
115.	RDS는 반드시 데이터 가용성, 부적절한 데이터 사용, 데이터 무단 접근, 프라이버시 정책 위반 및 부정확한 데이터 입력에 관한 민원을 처리하기 위한 절차를 수립해야 한다. 예: 오용신고 연락처 데이터 요소 및 USD 및 도메인 소유자의 민원을 접수하기 위한 포털.
116.	RDS는 반드시 부정확한 데이터 수정을 위한 절차를 강화해야 한다. 예: 이메일 경고, 사용자/브라우저에 보이는 플래그 온 레코드(Flag on Records) 표시, ICANN 컴플라이언스의 조치 및 기타 새로운 정확성 향상 유인. (정확성 요건에 관해 섹션 V, '데이터 품질 향상' 참조)
117.	RDS는 반드시 데이터 무단 접근 문제의 해결을 위해 강화된 조치를 확립해야 한다. 예: 이메일 경고, 비율 제한(Rate Limiting), 일시적 차단(Temporary Blocking), 인증 중지, 해지 및 기타 제재 수단. (제한적 접근 요건에 관해 섹션 V, '책임성 향상' 참조)
118.	RDS는 반드시 부적절한 데이터 사용 문제의 해결을 위해 강화된 조치를 확립해야 한다. 예: 이메일 경고, 비율 제한, 일시적 차단, 인증 중지, 해지 및 기타 제재 수단. (허용된 목적에 관해 섹션 III, '사용자 및 목적' 참조)
119.	RDS는 반드시 RDS 접근 크리덴셜 오용 및 ToU 위반을 탐지하기 위한

[25] 이러한 역할과 책임은 이해관계자의 대리인 및 양수인(예, 재판매자)으로 확대된다.

[26] http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm의 정의 참조.

[27] http://new 일반도메인 s.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf 의 정의 참조.

	감사

93 페이지

번호.	책임성 및 감사 원칙
	메커니즘을 확립해야 한다. 예: 비정상적인 행동 패턴 탐지 메커니즘. (RDS 사용자 인증 요건에 관해 섹션 IV, '책임성 향상' 참조.)
120.	RDS는 반드시 지정된 목적 이외의 사용을 위한 등록정보의 오용을 탐지하기 위한 감사 메커니즘을 확립해야 한다. 예: 비정상적인 행동 패턴 탐지 메커니즘. (섹션 III, '사용자 및 목적' 참조.)
121.	RDS는 반드시 검증기관의 오용을 탐지하기 위한 감사 메커니즘을 확립해야 한다. 예: 검증기관 교육, 주기적인 무작위 데이터 샘플링 및 검사를 통해 적절한 검증 여부 확인. (섹션 V, '데이터 품질 향상' 참조.)
122.	RDS는 반드시 RDS 사용자 인증 기구의 오용을 탐지하기 위한 감사 메커니즘을 확립해야 한다. 예: 비정상적인 행동 패턴 탐지 메커니즘을 확립한다. (오용의 정의에 관해 섹션 IV, '책임성 향상' 참조.)
123.	RDS는 반드시 프라이버시/프록시 서비스 제공업체 및 보안 크리덴셜 인증 기구의 오용을 탐지하기 위한 감사 메커니즘을 확립해야 한다. 예: 비정상적인 행동 패턴 탐지 메커니즘을 확립한다. (오용의 정의는 섹션 VI, '도메인 소유자 프라이버시 향상' 참조)
124.	RDS USD는 반드시 이용약관(ToU)에서 데이터 접근, 정확한 신원의 사용과 제공 및 목적 정보에 대한 감사에 동의해야 한다.
125.	RDS는, 데이터가 적절하게 검증, 저장 및 보호되지 않을 경우 검증기관을 교정, 정지 또는 해지하기 위한 절차를 반드시 확립해야 한다. (VR 요건에 관해 섹션 V, '데이터 품질 향상' 참조.)
126.	RDS는, 조사가 적절하거나 적당하지 않을 경우 보안 크리덴셜 인증 기구를 교정, 사용 또는 계약 해지하기 위한 절차를 반드시 확립해야 한다. (요건에 관해 섹션 VIII, '도메인 소유자 프라이버시 향상' 참조)

127.	RDS는, USD가 적절하게 인증, 저장 및 보호되지 않을 경우 RDS 사용자 인증기구를 교정, 사용 중지 또는 계약 해지하기 위한 절차를 반드시 확립해야 한다. (RDS 사용자 인증기구 요건에 관해 섹션 IV, '책임성 향상' 참조.)

94 페이지

번호	책임성 및 감사 원칙
128.	ICANN은 반드시 관리기관, 등록대행자 및 검증기관이 정확한 최신 데이터를 시기 적절하게 RDS에 제공하도록 보장하기 위한 ToS 정책을 수립해야 한다. (RIA 및 RAA에 반영될 RDS 및 관리기관 요건에 관해 섹션 VI, '법률 및 계약 관련 고려사항' 참조.)
129.	RDS는 반드시 관리기관, 등록대행자 및 검증기관에 대한 감사 절차와 관리기관/등록대행자/검증기관이 정확한 최신 데이터를 시의적절하게 제공하지 않을 경우 ICANN에 신고하기 위한 절차를 확립해야 한다. (RIA 및 RAA에 반영될 RDS 및 관리기관 요건에 관해 섹션 VI, '법률 및 계약 관련 고려사항' 참조.)
130.	RDS는 반드시 RDS가 수집하고 에스크로 서비스 제공업체에 저장한 데이터의 품질 및 무결성을 지속적으로 보장하기 위한 감사 메커니즘을 확립해야 한다. (섹션 VIII, '데이터 저장소 에스크로 및 작업기록' 참조)
131.	ICANN은 반드시 RDS 제공자의 ToC 위반을 탐지하기 위한 감사 메커니즘을 확립해야 한다. 예: 허가되지 않은 데이터 사용을 허용하고, 데이터 오용, 크리덴셜 오용 또는 검증 오용 관련 민원에 응답하지 않는다. (섹션 VI, '법률 및 계약 관련 고려사항' 참조.)
132.	ICANN은, RDS 운영업체가 계약상의 책임을 이행하지 않을 경우 RDS 운영업체를 교정, 중지 또는 해지하기 위한 절차를 반드시 확립해야 한다. 예: 가용성, 신뢰성, 프라이버시, 접근 권한 및 성과 요건. (섹션 IV, '법률 및 계약상의 고려사항' 참조.)
133.	ICANN은 반드시 RDS의 주요 목표를 달성하기 위한 연간 개선 목표를 정의하고 벤치 마킹해야 한다. (i) 데이터 품질 향상, (ii) 책임성 향상, (iii) 프라이버시 향상. RDS는 반드시 이 세가지 부문에서 비슷한 속도로 지속적인 진전이 이루어지고 있음을 증명해야 하며 다른 부문에 비해 개선 속도가 느린 부문이 있을 경우 그 원인이 되는 문제를 파악하고 교정하기 위한 절차를 마련한다.

95 페이지

아래 표는 114번 원칙을 확대해 RDS 생태계 실체들과 그들에게 적용해야 할 책임 및 감사 요건의 유형을 요약한 것이다.

적용 요건	데이터를 구하는 RDS 사용자	도메인 소유자	등록대행자	관리기관	RDS 제공업체	프라이버시/프록시 제공업체	보안 크리덴셜 인증 기구	검증기관	RDS 사용자 인증기구	목적별 연락처	에스크로 서비스 제공업체
정확하고 신뢰할만한 데이터 제공											
지정된 목적에만 사용											
정보 보안 유지											
유효성 검사/인증											
시의적절한 업데이트											
프라이버시 정책 시행											
오용 탐지											
민원 처리											
제3차 데이터 수확 제재											
감사 및 교정											

표 6: RDS 생태계 행위자들의 준수 요건

VIII. 도메인 등록인 프라이버시 향상

EWG의 핵심 과제는 수집된 데이터의 정확성을 높이는 동시에 자신의 프라이버시를 지키고자 하는 도메인 소유자들을 보호하는 시스템을 설계하는 것이다. EWG는 개인정보는 정보보호법을 통해 보호되어야 하며 해당 법이 없는 경우에도 개인이 자신의 개인정보를 좀 더 강력하게 보호하고자 하는 합당한 이유가 있다는 점을 잘 인식하고 있다. 뿐만 아니라, 일부 기업과 조직 역시, 신제품 출시를 준비하거나 소규모 기업의 경우 연락처 정보로 인해 개인 정보가 공개되는 경우처럼 타당한 목적을 위해 자신의 정보를 보호하고자 한다.

따라서, EWG는 프라이버시를 위해 다음과 같은 기본적인 원칙들을 권고한다.

번호	프라이버시 원칙
134.	정보보호법 준수를 통한 프라이버시 보호 외에 RDS 생태계는 반드시 다음과 같은 방법으로 프라이버시 요구를 충족시켜야 한다. • 일반적인 개인정보보호를 위한 공인 프라이버시/프록시 서비스 및 지역 프라이버시 법률 준수 • 위험에 노출된 개인과 언론의 자유에 대한 권리가 부인되거나 발언자가 박해 받는 경우를 위한 공인 보안 크리덴셜 서비스(Secure Protected Credentials Service)
135.	반드시 프라이버시/프록시 서비스 제공업체에 대한 인증과 공인 프라이버시/프록시 서비스 제공 및 사용에 관한 규칙을 마련해야 한다.
136.	공인 프라이버시/프록시 서비스를 통해 등록된 도메인네임을 제외한 모든 도메인 소유자는 반드시 자신이 등록한 도메인네임을 책임 져야 한다.
137.	ICANN은 반드시 아래 설명과 같이 RDS 활동을 포괄적으로 지배하는 일관성 있는 단일 프라이버시 정책 개발을 제고해야 한다.

정보보호법과 함께 기타 국가 수준의 프라이버시 법률과 헌법은 수 억 명의 인터넷 사용자들이 자신의 이름과 주소가 쉽게 그리고 즉각적으로 추적당하지 않고 온라인에서 자신의 의사를 표현할 권리를 보호한다. 이러한 프라이버시 관련 법률로는 언론과 표현의 자유를 보호하고 지도력 실행과 행사 및 국가 문화 또는 사회 운영을 비평 및

비난하는 집단, 조직, 개인 및 기업(예, 언론 매체)의 능력과 의무를 보호하는 UN 인권선언(19 조)[28]이 대표적이다.

언론 및 표현의 자유를 보호하는 프라이버시 법률은 해당 권리를 행사할 때 정부, 사회, 공동체 또는 이웃에 대해 비평적일 수 있는 의사 표현에서 조직과 집단의 이름과 주소를 분리하는 규칙이 필요함을 인정하는 경우가 많다. 해당 규칙이 존재한다면 사상의 자유시장을 활성화하고 자유로운 의사소통에 개방적인 사회의 필요성이 연설자를 박해하는 권력과 단순히 누군가가 해당 메시지의 제안자를 좋아하지 않는다는 이유만으로도 해당 메시지를 속단할 가능성에 우선할 수 있을 것이다.

또한 프라이버시 법률 및 헌법상의 권리는 결사의 자유, 종교, 민족성, 도덕성 및 공동체를 보호한다. 개인이나 조직이 인기가 없거나 소수의 견해를 표현할 때 이름이나 심지어 주소를 밝혀야 할 필요성을 없앰으로써 즉각적으로 추적을 당해서 비난을 받거나 더 심한 고충을 겪지 않도록 보호한다. 지금과 같은 정치적 동요와 반대 의견에 대한 적의가 심한 시대에 프라이버시 법률은 소수의 목소리를 옹호하고 온라인을 통해 강력하게 변화와 개혁을 촉구할 수 있는 능력을 수호한다.

본 보고서에서 프라이버시와 개인 정보 보호에 관해 언급할 때, 이는 국가마다 서로 다른 법률을 통해 서로 다른 방식으로 보호되는 이 두 가지 서로 다른 권리를 모두 인정한다는 전제하에서 이루어진 다는 점을 밝히고자 한다.

a. 공인 프라이버시 및 프록시 서비스 원칙

현재, 도메인네임을 사용하는 실체의 신원 및/또는 주소를 가리기 위해 제공되는 서비스들이 있다. 이러한 서비스는 WHOIS의 개방적 특성에 기반해 개발되었다. 다양한 종류의 서비스가 존재하지만 2013 등록대행기관 인증 계약서(RAA)에서는 이 두 가지 서비스를 다음과 같이 정의한다.

- “프라이버시 서비스”란 등록 도메인네임을 등록도메인네임 보유자로서 수혜 사용자에게 등록시키는 서비스지만 등록정보서비스(WHOIS) 또는 그에 상당하는 서비스에서 등록도메인네임 보유자의 연락처 정보 표시를 위해 P/P 제공업체가 신뢰할 수 있는 대체 연락처 정보를 제공한다.
- “프록시 서비스”란 등록도메인네임 보유자(Registered Name Holder)가 P/P 고객이 도메인네임을 사용할 수 있도록 P/P 고객에게 등록도메인네임(Registered Name) 사용을 허가하는 서비스로서 등록정보서비스(WHOIS)나 그에 상당하는 서비스 에서 P/P 고객의 연락처 정보가 아니라 등록도메인네임 보유자의 연락처

정보가 표시된다.

98 페이지

이 정의에서 “P/P 제공업체” 또는 “서비스 제공업체”는 해당 사항이 있는 경우 등록대행자와 그 제휴 기관을 포함한 프라이버시/프록시 서비스 제공업체이다. “P/P 고객”은 (P/P 제공업체가 사용하는 용어에 관계없이) 프라이버시 서비스 및 프록시 서비스의 사용권자, 고객, 수혜 사용자(beneficial user), 수혜자(beneficiary) 또는 기타 수령자(recipient)를 의미한다.

현재 프라이버시 또는 프록시 서비스는 표준화되어 있지 않다. 중간 명세서(Interim Specification)에 반영된 것처럼 2013 RAA에서 ICANN에 의한 인증이라는 개념과 기본적인 의무에 대해 소개했지만 이러한 서비스 제공업체들은 ICANN과 어떠한 계약 관계도 맺고 있지 않다. 그러나 이중 일부는 등록대행기관이기도 하고 모든 등록대행기관은 RAA의 적용을 받는데, 프록시로 등록한 도메인네임(proxy-registered domain name)에 관해 다음과 같이 명시하고 있다.[29]

> 3.7.7.3 제3자에게 도메인네임 사용을 허락하려는 등록 도메인네임 보유자 (Registered Name Holder)는 그럼에도 불구하고 기록상의 등록도메인네임 보유자이며 자신의 모든 연락처 정보를 제공하고 등록된 도메인네임과 관련해 *발생하는 모든 문제*[30]의 시기 적절한 해결에 필요한 정확한 기술 및 관리상의 연락처 정보를 제공 및 업데이트할 책임이 있다. 본 조항에 따라 등록도메인네임의 사용을 허락하는 등록도메인네임 보유자는 사용권자가 제공한 현재의 연락처 정보와 사용권자의 신원을 칠(7)일 안에 등록도메인네임 보유자를 상대로 소송 가능한 피해를 입증하는 타당한 증거를 제공하는 당사자에게 공개하지 않는 한 등록도메인네임의 불법적 사용으로 발생하는 피해에 대한 책임을 수용해야 한다.

현재 프록시 서비스를 통해 등록한 도메인에 대해 WHOIS 검색을 하면 다음과 같은 결과가 반환된다.

Domain Name: EXAMPLE-DOMAIN.COM
Created on: 31-Oct-11
Expires on: 31-Oct-13
Last Updated on: 19-Sep-12

Registrant:
Domains By Proxy, LLC
DomainsByProxy.com

Registrant Name = Proxy
Registrant Org = Proxy

---

[29] 2013 RAA는 2013년 6월 27일에 ICANN 이사회 승인을 얻었다. 3.7.7.3(여기에 인용)항은 2009년 RAA와 크게 바뀐 것은 없고 다만 7일의 기간이 더 추가되었다.

[30] 참고: EWG는 ICANN이 ”모든 문제”가 지나치게 광범위한 것은 아닌지 고려해 볼 것을 제안한다.

14747 N Northsight Blvd Suite 111, PMB 309	Registrant Address = Proxy's
Scottsdale, Arizona 85260	
United States	
Admin Contact: [same for Tech Contact]	
Private, Registration	

99 페이지

example-domain.com @domainsbyproxy.com	Email = domain@proxy
Domains By Proxy, LLC	Name = Proxy
DomainsByProxy.com	Org = Proxy
14747 N Northsight Blvd Suite 111, PMB 309	Address = Proxy's
Scottsdale, Arizona 85260	
United States	
(480) 624-2599 Fax -- (480) 624-2598	Tel/Fax = Proxy's

현재 프라이버시 서비스라 불리는 서비스를 이용해 등록된 도메인에 대해 WHOIS 검색을 하면 비슷한 결과가 반환되며 단, 등록 도메인네임(및 종종 Admin/Tech Contact Names)이 프록시 서비스 제공업체가 아닌 프라이버시 서비스 고객을 직접 식별한다는 점이 다르다.

현재 모든 프라이버시 및 프록시 서비스 제공업체들이 활용하는 표준화된 절차는 없다. 그러나 여러 가지 공통된 요구들이 존재하고, 종종 어느 정도는 충족되고 있다.

- 현 프라이버시 또는 프록시 서비스 고객에게 보통 관리/기술 연락처의 이메일 주소로 전송된 이메일을 자동으로 전달하는 방식으로 연락을 전한다. 이러한 연락 중개 서비스는 많은 업체가 제공하지만 모든 업체가 제공하지는 않는다.
- 도메인네임에 대한 민원이 제기될 경우 프록시 고객을 대신해서 사용권자의 신원 정보와 직접 연락 가능한 연락처 정보를 공개한다. 민원 처리 절차, 문서화, 대응 및 조치는 요청자와 제공업체 사이의 관계에 따라 달라진다.
- 사용권자의 신원을 밝히고 프록시 서비스 고객의 이름과 연락처 정보를 WHOIS에서 공개적으로 이용 가능하도록 조치한다.
- 요청자가 프록시 서비스 고객에게 연락할 수 없거나 프록시 서비스 제공업체가 문제를 해결하지 못할 때, 종종 등록대행기관(프록시 서비스 제공업체와 제휴 관계에 있을 수도 아닐 수도 있는)에게 의지한다.

많은 문서들이 지금의 프라이버시 및 프록시 서비스가 지닌 단점들을 입증했다.[31] 좀 더 일관성 있고 신뢰할 수 있으며 더 큰 책임성을 수용하는 프라이버시 및 프록시 서비스에 대한 도메인 소유자 및 이해관계자들의 요구를 해결하기 위해 EWG 는 다음의 원칙들을 권고한다.

[31] WHOIS와 프라이버시/프록시 서비스의 결함을 문서화한 연구와 보고서는 **부록 B**를 참조한다.

번호	공인 프라이버시/프록시 서비스 원칙
	일반
138.	ICANN은 반드시 프라이버시 및 프록시 서비스 제공업체를 인증해야 한다.[32]
139	최소한 인증 프로그램은 반드시 2013년 RAA 세부사항 설명서(RAA Specification) 에 따른 프라이버시/프록시 서비스의 의무를 계속 수행해야 한다.
	공인 프라이버시 서비스 원칙
140.	자연인과 실체는 도메인 소유자의 연락처 세부정보를 공개하지 않는 공인 프라이버시 서비스를 이용한 도메인네임 등록이 가능하다. 단, 특정한 상황(예, 서비스 조건 위반, 정보제출명령)에서는 예외로 한다.
141.	ICANN은 반드시 서비스 조건에 구체적인 조건이 포함되도록 요구해야 한다. 서비스 조건은 서비스 제공업체가 신속한 사이트 폐쇄(expedited take-downs)에 대해 고지하기 위해 노력하도록 요구한다는 조항도 포함해야 한다.
142.	공인 프라이버시 서비스는 반드시 등록대행자에게(검증기관을 통해 생성된 PBC를 이용해) 모든 의무적 목적별 연락처에 대한 정확하고 신뢰할 수 있는 정보를 제공함으로써 프라이버시 서비스 제공업체 및 도메인 소유자를 대신해 기술, 관리 및 기타 문제의 해결 권한이 있는 실체에게 연락하도록 해야 한다.
143.	공인 프라이버시 서비스는 반드시 도메인 소유자의 전달 이메일 주소 (forwarding email address)로 수신한 이메일을 도메인 소유자에게 전달해야 한다.
	공인 프록시 서비스 원칙
144.	자연인과 실체는 프록시 서비스 고객을 대신해 도메인네임을 등록하는 공인 프록시 서비스를 이용해 도메인네임을 등록할 수 있다.
145.	공인 프록시 서비스 제공업체는 반드시 등록대행기관에게(검증기관을 통해 생성한 PBC를 이용해서) 프록시 서비스 고객을 대신해서 도메인네임을 등록하도록 허가된 실체에게 연락하기 위한 고유 이메일 전달 주소를 포함해서 자신의 도메인 소유자 이름과 연락처 정보를 제공해야 한다.

[32] 일반도메인정책개발기구(GNSO)는 프라이버시/프록시 서비스 인증 정책 개발을 위한 실무그룹을 조직했다. EWG는 RDS가 PPSAI 실무그룹이 구축해 놓은 토대가 있다면 재사용할 것을 권고한다. 필요할 경우 RDS 접근 방식과 데이터 요소, 특히 P/P가 공개한 목적별 연락처를 반영해 수정한다.

146.	공인 프록시 서비스 제공업체는 등록된 도메인네임 보유자(registered name holder)로서 반드시 정확하고 믿을 수 있는 의무적 목적별 연락처 및 기타 등록정보를 제공하는 등 해당 도메인네임을 위해 도메인 소유자가 져야 할 모든 책임을 수행해야 한다.

번호	공인 프라이버시/프록시 서비스 원칙
147.	공인 프록시 서비스는 반드시 등록대행자에게(검증기관을 통해 생성된 PBC를 이용해서) 모든 의무적 목적별 연락처에 대한 정확하고 신뢰할 수 있는 정보를 제공함으로써 프록시 서비스 제공업체 및 프록시 서비스 고객을 대신해 기술, 관리 및 기타 문제의 해결 권한이 있는 실체에게 연락하도록 해야 한다.
148.	공인 프록시 서비스는 반드시 도메인 소유자의 이메일 전달 주소로 수신한 이메일을 전달해야 한다. 이에 관해서는 부록 H에서 자세히 설명한다.
149.	공인 프록시 서비스는 반드시 정보 공개(reveal) 요청에 대해 부록 H에 기술된 절차에 따라 시의적절한 방식으로 대응해야 한다.

b. 보안 크리덴셜 원칙(Secure Protected Credential Principles)

인터넷에서 익명성을 유지하고 싶은, 또는 적어도 자신의 주소와 개인 정보가 잠재적으로 위협이 될 가능성이 있는 사람들에게 공개되길 원하지 않은 개인과 집단들이 프라이버시 강화에 대한 타당한 요구를 지니고 있다는 사실은 잘 알려져 있다. 이러한 당사자들은 개인정보보호법(프라이버시보호법)이 존재하는 경우 해당 법에 따른 권리를 행사하거나 프록시 서비스를 이용하기도 한다. 그러나 안타깝게도 이러한 메커니즘들은 실질적인 위협에 노출된 사람들에게는 충분한 보안을 제공하지 못할 지도 모른다. 인터넷에서 도메인 소유자에 대한 세부정보를 얻지 못할 경우 이러한 개인이나 집단을 추적하는 사람들은 표적을 검증기관, 등록대행기관 또는 관리기관으로 바꾸고 종종 소셜 엔지니어링 기법을 이용해서 그들에게 정보를 요청하는데 이러한 기법을 탐지해 내기가 쉽지 않다.

보안 크리덴셜(secure protected credentials)을 제공하는 목적은 위협에 노출된 개인이나 집단을 위해 안전한 익명의 등록 서비스를 제공하기 위함이다. 언론의 자유를 누리고자 하는 당사자(보호받는 것으로 널리 알려져 있는) 또는 신원이 드러날 경우 자신이나 가족의 생명을 위협받는 연설가들이 여기에 속한다.

아래에 다섯 가지 예를 제시한다.

1. 종교적 소수자(Religious minorities)

전세계 많은 국가에는 상대적으로 큰 인구집단으로부터 그리고 같은 종교에

속하는 사람들로부터 위협을 받는 종교적 소수자들이 있다. 이들은 자신이 속한 집단의 구성원들에게 정보를 제공하면서도 어디에서 어떻게 활동하는지 기밀을 유지할 수 있는 웹사이트를 필요로 한다. 예를 들면, 로마에 있는 유대교 예배당은 잦은 폭탄 테러 위협 때문에 주소를 공개하지 않지만 그 장소를 아는 구성원들을 위해 예배 시간을 알린다.

2. 가정 폭력(Domestic abuse)

많은 국가가 가정 폭력을 겪었거나 공격자로부터 도망친 사람들을 위해 어떤 형태로든 신원을 바꿀 수 있는 수단을 제공한다. 또한 특정 종교 단체와 광신적 교단에서 도망친 사람들과 증인보호프로그램 중에 있는 사람들에게도 적용된다. 가정 폭력을 겪은 여성들을 위한 보호소는 인터넷에 홍보를 하고 진짜 도움이 필요한 여성들이 시설에 도착할 수 있도록 연락처와 지시사항을 안전하게 지켜야 할 필요가 있다. 신분을 바꾼 개인과 가족들은 자신이 있는 곳의 주소나 진실한 신원을 밝히지 않고 웹사이트를 개설하고 싶은 타당한 요구를 가질 지도 모른다. 여러 가지 이유로 신분을 숨기고 정부를 위해 일하는 개인들이 있으며 보통 국가 안보와 법 집행과 관련된 활동을 하는 경우가 많다. 이러한 개인들 역시 직업적으로나 사생활 측면에서도 좀 더 강화된 보호가 필요하다.

3. 정치 연설(Political Speech)

전세계 많은 국가에서 야당 또는 낙선 정치인들이 선거 후 몸을 피해야 하는 경우가 있다. 또한 이들은 자국에서 일어나는 사건이나 자신에 대한 박해와 관련해 구체적인 정보를 알릴 수 있는 웹사이트를 운영할 필요성을 느낀다. 정권을 잡은 정부는 정부 비판에 관한 증거문서가 웹사이트에 게시되면 반역이나 기타 범죄 행위를 이유로 내세워 이들의 웹사이트를 추적할 지도 모른다. 언론의 자유에 대한 권리는 국가마다 큰 차이가 있고 반역을 근거로 내세울 경우 저항하기 힘든 경우가 많기 때문에 매우 미묘하고 까다로운 사안이 아닐 수 없다. 따라서 ICANN과 공인 등록대행기관은 도메인 등록 권리에만 초점을 맞출 수 밖에 없다.

4. 인종 또는 기타 사회 집단(Ethnic or other social groups)

인종 집단은 종종 괴롭힘과 차별을 겪기 때문에 해당 집단 구성원들에게 중요한 정보를 제공하는 웹사이트를 운영하고 싶을 것이다. 예를 들어, 이러한 집단은 구성원들이 신원 노출과 보복에 대한 두려움 없이 괴롭힘을 당한 사건을 게시할 수 있는 웹사이트를 운영하고 싶을 것이다. 동성애자나 성전환자와 같은 집단 역시 해당 공동체를 위해 지극히 평범한 정보를 제공하는 웹사이트를 운영하길

원하지만 그들이 속한 국가의 제한적 법률이나 자경단원이나 증오 집단의 보복 때문에 구성원들의 신원이 노출되는 것을 꺼린다. 심지어 여성들을 위한 건강 및 영양 정보나 여성의 생식의 권리에 관한 정보 등을 제공하는 사이트 운영자를 상대로 한 보복의 사례도 있다.

103페이지

5. 적대적 환경에서 활동하는 언론인(Journalists operating in hostile territory)

적대적인 환경에서 글을 게시하는 언론인들은 자신은 물론 협력자들과 번역자 등의 신원과 주소 정보에 대한 보안과 프라이버시를 유지할 수 있는 웹사이트를 운영할 필요가 있고 운영하고 싶을 것이다.

보안 크리덴셜 기술

현재 시중에는 마이크로소프트의 유프루브(U-Prove)(http://research.microsoft.com/en-us/projects/u-prove/)와 IBM의 아이덴티티 믹서(Identity Mixer) (http://researcher.watson.ibm.com/ researcher/view_project.php?id=664)를 비롯한 다양한 보안 크리덴셜이 출시되어 있다. 보안 크리덴셜 수령자는 자신이 신뢰할 수 있는 기관으로부터 인정 및 인증을 받았으며, 특정 권리나 서비스에 대한 비용을 지불한 사실 등의 다양한 속성을 증명하면서도 개인 정보를 노출하거나 그러한 속성을 가능하게 한 거래에 대한 트레이스백(trace-back)을 제공하지 않아도 된다. 신뢰 당사자(Relying parties)는 보안 크리덴셜을 발급받은 실체가 신뢰할 수 있는 기관의 승인을 받았다는 안전한 암호화된 증거를 가지게 되며 그들이 누구인지 또는 어떻게 그 승인을 받았는지 알 필요가 없다.

이러한 기술은 위에서 설명한 위험에 노출된 실체들이 보안 크리덴셜을 이용해서 도메인네임을 등록하는 과정을 구축할 때 사용이 가능하다. 등록대행기관이나 검증기관 모두 DNS 문제의 처리를 책임지는 필수 연락처 외에는 해당 실체에 관한 정보를 알지 못한다. 따라서 합법적으로는 개인 또는 주소 정보에 대한 요청에 응답하지 못할 것이다. 확실히 기술적 적합성, 오용 및 해당 위험의 완화에 관한 우려들이 있다(아래에서 논의). 요점을 말하자면 보안 크리덴셜을 이용해 등록한 도메인네임에 대해서 등록대행기관과 관리기관이 더 이상은 취약한 개인들의 신원을 그 공격자들에게 공개해야 하는 위험과 책임을 감수하지 않아도 된다는 것이다.

운영상의 문제

그러한 서비스와 관련된 문제와 위험을 논의하기 위해서 EWG는 다음과 같은 잠재적인 상황들을 조사했다.

1. 한 정보 요청자가 합법적이라고 주장하며 제시한 목적(상표권 침해 주장,

도메인네임 매매 의사, 제품 안전성 조사 등)을 위해 위의 2, 3, 4에서 설명한 개인들의 진실한 이름이나 주소를 알아내고자 한다. 생사가 오가는 상황에서 등록대행기관은 해당 요청자가 허위 주장을 하고 있는 것은 아닌지 결정해야 하는 어려운 입장에 처하게 되고 직원들이, 특히 신분을 숨기고 있는 상황에서 사람들이 어떤

알려지지 않은 위협에 직면할 수 있는지 이해해 주리라 기대할 수 없다.

2. 한 요청자가 모종의 범죄 행위 또는 명예훼손을 이유로 내세우며 도메인네임 등록대행기관(또는 지정된 PBC 검증기관)에게 접근해 해당 도메인네임을 사용하는 웹사이트의 폐쇄를 요구한다. 이러한 상황에서, 등록대행기관 및 프록시 서비스 제공업체의 서비스 조건을 따라야 하고 그럴 경우 도메인네임 사용권자의 신원정보와 주소를 얻기 위한 정보공개 요청으로 이어질 가능성도 있다. 그러나, 보안 크리덴셜로 등록한 도메인의 경우, 정보공개 요청을 하더라도 얻어지는 것은 보안 크리덴셜을 승인한 신뢰할 수 있는 기관일 뿐이다. 신뢰할 수 있는 기관이 잠재적 DNS 오용에 대한 조사를 책임질 것이다. 일부, 범죄 행위와 같은 특정한 상황에서는 이러한 웹사이트들의 신속한 폐쇄가 허용될 가능성도 있다.

3. 정부 기관이 특정 정치 연설이 반역이나 기타 범죄적 행위의 수준에 이르렀다고 주장하는 경우에는, 관할지역의 관련 법에 따라 달라지겠지만 등록대행기관은 어쩔 수 없이 보안 크리덴셜로 등록한 도메인네임을 이용하는 웹사이트에 대해 신속한 폐쇄를 고려하지 않을 수 없을 것이다.

이러한 한계를 고려하더라도, 보안 크리덴셜은 위험에 처한 실체들에게 현재보다 훨씬 더 강력한 보안을 제공할 것이며 새로운 RDS가 데이터 정확성 및 책임성 강화를 요구할 경우 해당 서비스가 필요할 것이다. 그러기 위해서 다음과 같은 핵심적인 기능들을 개발할 필요가 있다.

1. 위험에 처한 실체가 보안 크리덴셜을 신청하기에 적격한 지 기준을 정하기 위한 프로세스. 위에 언급한 사용자의 사례와 기타 ICANN 커뮤니티가 정책 개발을 통해 적절하다고 판단하는 실체부터 시작한다.

2. 신청 양식, 필요한 증명(attestations) 및 금융 시스템 등 모든 것이 위험에 처한 실체(및 경우에 따라서는 그 증명기관)의 신원 보호에 맞춰져야 한다. 모든 익명의 시스템에서 가장 취약한 부분도 바로 이것이다.

3. 보안 크리덴셜 신청서와 이름 변경을 허가한 정부 기관, 난민 보호에 관여하는 유엔 기구, 국제언론인연합 등 신뢰할 수 있는 당사자의 증명서를 평가하고 승인하는 독립 심사위원회.

4. 신청자와 독립심사위원회 사이에서 보안 크리덴셜 신청서와 그 결과 생성된 도메인네임을 전달하는 것이 가능한 신뢰할 수 있는 당사자(위 3번에 열거).

105페이지

이 신뢰할 수 있는 당사자(이하 보안 크리덴셜 수령인(Secure Credential Recipients)이라 칭한다)는 반드시 위험에 처한 실체의 익명성에 대한 요구를 증명하고 보안 크리덴셜로 등록한 도메인네임에 의한 잠재적인 DNS 오용에 대해 책임을 져야 한다.

5. 보안 크리덴셜 승인 기구가 사용권을 부여하는 도메인네임을 등록할 때 보안 크리덴셜을 받아들일 의사가 있는 공인 프록시 서비스 제공업체와 그들이 대가를 지불 받을 금융 시스템

6. 신속한 (사이트) 폐쇄 절차 및 기타 DNS 오용 완화 방안과 관련된 정책. 잠재적인 DNS 오용과 남용을 완화하고 도메인네임을 공격으로부터 보호하도록 돕기 위한 보안 크리덴셜로 등록한 도메인네임에 대한 보안 감시 강화도 여기에 포함된다. DNS 오용을 구실로 내세우는 당사자는 위험에 처한 실체의 신청을 승인한 심사위원회에 자신들의 주장을 펼칠 것이다. 그러면 보안 크리덴션 승인 기구는 해당 오용에 대한 주장을 평가할 것이다.

아래 그림은 이 당사자들 사이의 관계와 책임 그리고 커뮤니케이션의 흐름을 보여준다.

<table>
<tr><td></td><td>위험에 처한 실체</td><td></td><td></td><td></td><td></td></tr>
<tr><td>8)SC로 등록된 도메인네임</td><td></td><td>1)SC 신청서</td><td></td><td></td><td></td></tr>
<tr><td></td><td>증명자</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>7) 2)</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>보안 크리덴셜 수령자</td><td>3)SC 신청서</td><td colspan="3">보안 크리덴셜 승인기구</td></tr>
<tr><td></td><td></td><td>6)크리덴셜 & 도메인네임</td><td>4)크리덴셜</td><td></td><td>5)도메인네임</td></tr>
<tr><td></td><td></td><td></td><td>보안 크리덴셜 발급자</td><td></td><td>프라이버시/프록시 제공업체</td></tr>
</table>

그림 8. 보안 크리덴셜 모형

106페이지

잔존 위험

보안 크리덴셜이 널리 사용되지 않는 이유는 다른 이유보다 특히 등록 및 인증 취소와 관련해 구현이 복잡하기 때문이다. 모든 당사자들이 그런 식으로 등록할 자격이 주어져야 한다는 주장이 있지만 이 서비스를 확립하고 사기 또는 범죄 목적에 잘못 사용되지 않도록 하기 위해 따르는 어려움을 고려해 볼 때, EWG는 이 접근법이 현실적으로 실행하기 어렵다고 판단했다. EWG는 제한적 사용을 위해 그리고 이 서비스를 이용하려는 실체들이 실제로 익명성에 대한 타당한 요구를 가진 후에야 보안 크리덴셜을 개발할 것을 권고한다.

또한, 일단 그러한 도메인네임이 등록되고 이것을 이용한 웹사이트가 개설되면 다양한 종류의 인터넷 트래픽 메타데이터와 콘텐츠로 인해 도메인네임 사용자의 신원이 밝혀지게 될 가능성이 있는 것도 사실이다. 그러나 이것은 오로지 도메인 등록 문제와 ICANN의 소관 범위 안에서 정의된 목적을 충족하기 위해 수집, 사용 및 공개되는 데이터에만 초점을 맞추는 ICANN 생태계의 범위를 벗어나는 주제이다. 도메인네임의 실제 사용으로 생성된 정보는 반드시 보안 크리덴셜로 등록된 도메인네임을 신청하고 사용하는 실체의 책임이 되어야 하며 이 위험을 강조하기 위한 정보를 제공하는 것이 중요할 지도 모른다. ICANN의 책임은 도메인네임 시스템 자체에서 끝이 난다.

번호	보안 크리덴셜 원칙
150.	신원이 밝혀질 경우 위험에 처할 수 있음을 증명 가능한 개인과 집단은 반드시 보안 크리덴셜을 이용해 등록된 도메인네임을 익명으로 신청하고 부여받을 수 있어야 한다. 증명자와 신뢰할 수 있는 당사자가 위험에 처한 실체와 등록대행자/검증기관 사이에서 일종의 방패 역할을 해야 한다.
151.	ICANN은 반드시 위험에 처한 조직이나 개인의 주장을 그 타당성 여부를 확인해서 크리덴셜을 승인(및 필요할 경우 폐지)할 수 있도록 독립적이고 신뢰할 수 있는 심사위원회 설립을 지원해야 한다. 그러한 조직(이하 보안 크리덴션 승인 기구(SCA)라 부른다)은 위험과 안전한 인터넷 사용에 관한 사용자 교육 등의 다른 서비스 개발에도 관여한다.
152.	ICANN은 반드시 SCA의 승인을 인정하고 그에 따라 보안 크리덴셜을 생성하는 보안 크리덴셜 발급자의 개발과 라이선싱을 지원해야 한다.
153.	보안 크리덴셜 승인기관은 반드시 발급받은 보안 크리덴셜을 사용해서 프록시 서비스 제공업체에게 도메인네임의 사용권을 정상적인 방식으로 부여해야 한다.

번호	보안 크리덴셜 원칙
	RDS에는 프록시 서비스 제공업체의 정보가 표시될 것이다. 보안 크리덴셜로 등록한 도메인네임을 이용하는 위험에 처한 실체에 관한 정보는 RDS에 전혀 알려지지 않을 것이며 익명의 또는 프록시 결제를 위한 시스템이 사용되어야 할 것이다.
154.	보안 크리덴셜을 이용해 등록한 도메인네임은 반드시 정상적인 공인 프라이버시/프록시 서비스 제공업체의 정보공개 및 폐쇄 절차를 따라야 한다. 프라이버시/프록시 고객(즉 보안 크리덴셜 승인기관)이 시기적절하게 응답하지 못하거나 DNS 오용의 증거가 있을 경우, 보안 크리덴셜로 등록한 도메인네임의 신속한 폐쇄를 초래할 가능성도 있다.
155.	보안 크리덴셜로 등록된 도메인네임은 사이버 공격의 위험에 노출되거나 위법 행위에 대한 조사가 어려워질 가능성이 있음을 고려할 때, 이러한 도메인네임에 대한 보안 감시를 강화하는 것이 위험을 완화시킬 수 있을 것으로 여겨질 수 있다.
156.	보안 크리덴셜 신청 승인 및 취소를 위한 정책과 절차를 반드시 확립해야 한다. • 승인 과정에서 증명 기관(존재할 경우)이 위험에 처한 실체의 신원과 위치가 신청서를 SCA에 제출하는 신뢰받는 보안 크리덴셜 수령자로부터 충분히 보호되어야 한다. 증명기관의 수와 신원은 RDS에서 파악이 가능하다. SCA와 직접 접촉하는 유일한 당사자는 보안 크리덴셜 수령자이다. • 취소 과정은 반드시 위험에 처한 개인의 신원과 위치에 대해 비슷한 보호장치를 허용하는 동시에 보안 크리덴셜의 서비스 조건을 이행해야 한다. SCA는 반드시 보안 크리덴셜과 관련해 주장된 DNS 오용을 조사하고 서비스 조건을 이행할 책임을 져야 한다. DNS 오용이 보안 크리덴셜 취소 사유가 될 만큼 심각할 경우 SCA는 보안 크리덴셜 수령자에게 책임을 물어야 한다.

c. 프라이버시 원칙의 주요 이점 요약

정확성과 책임성이 향상되면서 개별 시민, 특히 취약한 개인들의 보호가 더욱 중요해질 것이다. 데이터 보호, 공인 프라이버시/프록시 및 보안 크리덴셜 원칙과 메커니즘을 차세대 RDS의 필수적인 일부로 통합한다면 도메인 소유자 및 연락처의 프라이버시 향상에 도움이 될 것이다.

108페이지

EWG가 권고하는 데이터 보호 원칙들은,

- 하나로 조율된 RDS 정책을 적용하고, RDS 생태계 전반에 일관되게 구현되고 지역 법률 적용을 위한 “규칙 엔진”을 사용함으로써 좀 더 균일하게 개인 정보를 보호하고,
- 공개 및 익명으로 이용 가능한 등록정보 및 연락처 데이터는 감소시키고,
- 도메인 소유자 및 연락처 데이터를 오용으로부터 보호한다.

EWG가 권고하는 공인 프라이버시/프록시 제공업체에 관한 원칙은,

- 프라이버시/프록시 서비스 제공업체들을 위한 인증 체계를 확립함으로써 해당 서비스를 원하는 도메인 소유자들에게 명확성을 제공하고,
- 도메인네임이 공인 프라이버시/프록시 제공업체가 제공하는 서비스를 이용해서 등록된 것으로 식별되도록 요구하고,
- 등록정보 내에 프라이버시/프록시 제공업체에 연락할 방법을 명시하고,
- 제3자가 공인 프라이버시/프록시 제공업체 연락처를 허가 없이 사용하지 못하도록 방지하고,
- 공인 프라이버시/프록시 제공업체가 이메일을 도메인 소유자에게 전달하고 문의에 대응하도록 요구하며,
- 사법기관 및 기타 제3자 오용 신고자 및 정보 공개 요청자에게 좀 더 일관되고 예측 가능한 기대를 제공한다.

EWG가 권고하는 보안 크리덴셜 원칙은,

- 처음으로, 취약층 집단이 인터넷 상에서 자신들의 도메인을 보유함으로써 얻을 수 있는 여러 가지 이점을 누릴 수 있도록 하기 위한 절차를 확립하고,
- 언론의 자유와 집단 내 의사소통이라는 목적을 위해 인터넷 사용이 가장 필요한 사람들을 보호하는 한편 잠재적인 오용 문제의 처리 수단을 제공하고,
- 소셜 엔지니어링 기법을 통해 현재 매우 민감한 개인 정보 공개에 대한 책임을 안고 있는 검증기관 및 등록대행자의 책임을 덜어주고,
- 보안 크리덴셜을 이용해 등록한 도메인네임을 위한 추가적인 보안 수단을 제공하고,

- DNS 오용에 관여한 보안 크리덴셜로 등록한 웹사이트의 신속한 폐쇄를 요구한다.

VIII. 가능한 RDS 모형

a. 모형 설계 원칙

본 보고서에서는 EWG가 조사한 여러 가지 대안적 모형에 관해 자세히 소개하고 이러한 모형들이 어떻게 EWG가 권고하는 원칙들을 충족시킬 지에 관해서도 분석했다. 부록 F에 수록된 일단의 다면적 기준들을 이용해서 고려 대상에 포함된 모든 모형을 평가했다.

EWG가 분석을 위해 적용한 설계 원칙들은 다음과 같다.

번호	모형 설계 원칙
157.	**수집:** 현재 등록대행자 또는 등록대행자의 제휴 기관은 고객(도메인 소유자)로부터 직접 등록정보를 수집해서 저장한다. 이 과정은 본질적으로 분산되어 이루어질 수밖에 없다. 등록대행자나 등록대행자의 제휴 기관이 도메인 소유자로부터 계속 등록정보를 수집하는데 덧붙여 EWG는 검증기관이 연락처 정보를 수집하는 방안을 제안하는 바이다.
158.	**저장:** 모든 일반도메인 전반에 걸쳐 등록정보를 저장하기 위해 가능한 모형은 다양하다. EWG는 여러 가지 가능 모형들을 식별하고 가장 유망한 것으로 보이는 두 모형을 선별하고 부록 F에 수록된 평가 기준을 적용해서 한 가지 권고 모형을 선택했다.
159.	**접근:** 데이터 주체의 프라이버시 보호를 위해, 허가받지 않은 공개 데이터 접근 및 인증된 사용자의 제한적 데이터 접근을 비롯해서 반드시 중앙집중화된 인터페이스를 통해 적절한 요청자들이 전체 gTLD에 걸쳐 등록 정보에 접근할 수 있도록 해야 한다.
160.	**프로토콜**: RDS는 반드시 RDAP [33] 또는 EPP(각 인터페이스에 따라)를 저장 장소로부터 등록정보를 접근하기 위한 기본 접근 프로토콜로 사용해야 한다.

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

b. 제언 모형(고려한)

EWG가 최초 보고서에서 고려한 대안적 시스템 모형들과 ICANN 커뮤니티가 제안한 추가 모형들을 검증하기 위해 EWG는 먼저 어떤 모형들을 좀 더 심도 깊게 조사해야 할지 결정했다. 각 모형들은 등록정보가 RDS로 복사되는 방식이나 RDS를 통해 질의되는 방식을 비롯해 여러 면에서 차이가 있다. 이러한 차이점을 아래 표로 요약했으며[34] 부록 F에서 좀 더 자세히 설명했다.

가능 모형	수집	저장	복사	접근
현재의 WHOIS	RR	RR/Ry	n/a	RR/Ry
연합 모형	RR & V	RR/Ry & V	n/a	RDS
동기화 모형*	RR & V	RR/Ry & V	RDS	RDS
지역 모형	RR & V	RR/Ry & V	지역	RDS
옵트 아웃 모형	RR & V	RR/Ry & V	선택사항	RDS
우회 모형	RR & V	RR & V	RDS	RDS

* **참고:** 이전에 "집적 RDS(ARDS)"로 칭했던 모형은 이 모형이 복수의 장소에 위치하는 데이터를 일관되고 조율된 방식으로 사용하는 속성을 반영해서 "동기화 RDS(SRDS)" 모형으로 명칭이 바뀌었다. 여기서 고려한 모든 모형이 지리적으로 분산된 데이터 센터, 확고한 연결성 및 각 데이터센터의 예비성을 갖춘 기반구조를 비롯해 내고장성, 고가용성 및 부하 균형을 달성하기 위한 우수 엔지니어링 사례들을 이용해서 구현될 것이다.

c. 권고 모형

위에 제시한 가능성이 있는 시스템 모형들은 등록정보가 RDS에 복사되는 방식이나 RDS 질의 방식을 비롯해 여러 면에서 차이가 있다. EWG는 각 모형들을 면밀히 조사해서 이러한 차이가 어떻게 여러 속성에 영향을 미칠 지 결정했다. 이 가능 모형들을 비교한 후 EWG는 현행 WHOIS를 제외한 모든 모형이 EWG가 권고한 RDS 원칙들을 어느 정도 충족시키는 것을 확인했다. 그 중에서 EWG는 두 가지 가장 가능성이 높아 보이는 모형인 연합 모형(Federated Model)과 동기화 모형(Synchronized Model)(이전의 "집적 모형(Aggregated Model)")에 초점을 맞추고 좀 더 조사를 했으며

[34] 모형 요약표 약어: RR는 등록대행자, Ry는 관리기관, V는 검증기관을 가리킨다.

최종적으로 동기화 모형(SRDS)을 권고하게 되었다.

111페이지

연합 모형(차선책)

이 RDS 모형은 관리기관 및 검증기관들이 운영하는 분산된 저장소로부터 등록정보를 끌어오는데 관리기관과 검증기관들이 모두 공통된 연합 데이터 스키마를 사용한다. 데이터를 단일 저장 장소로 집적할 필요가 없으며 대신 RDS를 통하여 통합 공개/승인(허가)된 등록정보 접근 질의에 대해 모든 일반도메인 관리기관(도메인네임 데이터) 및 검증기관(연락처 세부정보)로부터 실시간으로 얻는다.

<table>
<tr><td colspan="2">도메인 등록인 및 연락처</td><td></td><td></td><td></td><td>요청자</td><td></td></tr>
<tr><td></td><td></td><td colspan="3">연합 모형(FRDS)</td><td></td><td>공개 및 허가된
접근 방법을 통한</td></tr>
<tr><td></td><td>검증기관</td><td></td><td></td><td></td><td>연합 RDS</td><td>목적별
데이터 공개</td></tr>
<tr><td>데이터 수집</td><td>등록대행자</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>데이터 저장</td><td>일반도메인
관리기관</td><td colspan="2">모든 일반도메인에
대해 실시간으로
전달된 질의를 통한
데이터 접근</td><td>검증된 데이터를 실시간으로 획득.
모든 질의(공개 및 허가된) 처리
접근 허가
게이팅 정책 적용
허용된 데이터 반환
데이터 접근 감사
추가 서비스</td></tr>
</table>

이 모형에서 FRDS는 RDAP를 통해 검증기관과 등록대행자/관리기관으로부터 데이터를 끌어온다. 이 모형과 관련된 연락처 및 등록정보의 흐름에 대해서는 부록 I(RDS 과정 흐름도)에서 자세히 설명하고 부록 E에 사례를 제시했다.

동기화 모형(SRDS)(권고 모형)

이 RDS 모형은 관리기관과 검증기관이 운영하는 분산된 저장소로부터 수신한 데이터를 거의 실시간으로 동기화된 시스템으로 복사한다. 그러면 시스템이 데이터를 모아서 RDS가 운영하는 분산형 아키텍처에 저장한다.

이 모형에서 RDS는 신뢰할 수 있는 데이터 소스이며 신뢰할 수 있는 접근성을 제공한다. 따라서 RDS는 등록대행자 및 관리기관의 업데이트 적시성에 대한 현재의 RAA 요건(및 현재의 요구)을 능가해서 충족시킬 것이다. 관리기관, 등록대행자 및 검증기관은 고객들에게 자신들이 보유한 데이터에 대한 접근을 허용하지만 제한된 데이터에 대한 모든 요청은 반드시 RDS에 질의해서 답을 얻어야 한다.

112페이지

이 모형은 이전의 WHOIS 권고 및 등록 정보 접근 장소 및 방법에 대한 소비자 혼란을 줄이자는 요청에 부응하는 동시에 등록대행자 및 관리기관 입장에서 볼 때 비용과 책임성에 대한 요건을 최소화한다.

RDS가 데이터에 대한 접근성을 제공하지만 데이터가 단일 장소에 저장되지 않고, 내고장성, 높은 가용성 및 부하 균형을 요구하는 시스템을 위한 엔지니어링 우수 사례에 따라 복수의 장소에 중복되어 저장된다. 관리기관과 검증기관은 여전히 자체적으로 데이터를 저장하지만 RDS는 이 데이터의 동기화된 사본을 사용해서 접근 요청을 좀 더 효과적으로 처리하게 될 것이다.

<table>
<tr><td colspan="2">도메인 소유자 및 연락처</td><td></td><td></td><td></td><td>요청자</td><td></td></tr>
<tr><td></td><td></td><td colspan="3">동기화 모형(SRDS)</td><td></td><td>공개 및 인증된
접근 방법을 통한</td></tr>
<tr><td></td><td>검증기관</td><td></td><td></td><td></td><td>동기화된
RDS</td><td>목적별
데이터 공개</td></tr>
<tr><td>데이터 수집</td><td>등록대행자</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>데이터 저장</td><td>일반도메인
관리기관</td><td colspan="2">모든 일반도메인에
대해 동기화된 데이터
복사를 통한 데이터
접근</td><td colspan="2">검증된 데이터 사본 저장
모든 질의(공개 및 허가된) 처리
접근 허가
게이팅 정책 적용
허용된 데이터 반환
데이터 접근 감사
추가 서비스</td></tr>
</table>

이 모형에서 검증기관과 등록대행자/관리기관은 EPP를 통해 SRDS로 데이터를 내보낸다. 이 모형에서의 연락처 및 등록정보의 흐름은 부록 I(RDS 과정 흐름도)에서 자세하게 설명했고 부록 E에 질의 사례를 제시했다. 아래에서는 부록 F에 식별한 방법을 적용해 이 두 가지 EWG가 선호하는 모형을 비교했다.

- **보안 관련 의의** – 이 두 모형 모두 보안에 미치는 영향을 기준으로 평가하면 비슷한 결과를 도출한다. 초기 보고서에서 제안한 것과 같은 집적 모형(이후 동기화 모형으로 명칭이 바뀜)은 중앙집중화된 인터페이스가 “단일 고장 지점”이 될 가능성이 있어 위험 요소가 된다는 일반 의견들이 있었지만 EWG는 그러한 위험은 현재 대규모 일반도메인 관리기관과 세계적 규모의 인터넷 웹사이트들이 안고 있는 위험과는 다르다고 판단했다.

현재의 우수 사례들을 보면, 대규모 정보기반 시스템들은 복수의 데이터센터와 백업 스토리지 및 재난복구 시스템은 물론 지리적으로 분산된 중복 구조의 기반구조를 활용해서 이러한 위험을 줄인다.

동기화 모형은 일관된 보안 구현과 정책 시행이 더욱 강화된다는 부가적인 이점을 가진다. 시스템 구성요소들을 엄격하게 운영함으로써, 한 명의 운영자가 관리하는 분산형 아키텍처의 동기화 모형은 연합 모형과 비교했을 때 명시된 보안 목표 달성을 위해 훨씬 일관된 접근법을 제공할 가능성이 크다. 그 이유는, 연합 모형의 경우 잠재적으로 수천의 관리기관과 등록대행자 및 검증기관들이 자체적인 데이터베이스를 관리할 것이고 등록대행자/관리기관/검증기관마다 전문지식이나 보안 투자 수준이 다르기 때문이기도 하다.

- **관할권 및 프라이버시 관련 우려사항 –** 관할권 및 프라이버시에 미치는 영향 측면에서 평가했을 때 두 모형 모두 비슷한 결과를 가져올 것이다. 연합 모형의 경우 데이터가 관리기관 수준에서 저장 및 제어되고 추가 사본이 다른 장소(말하자면, 전세계에 산재한 등록대행자, 검증기관 및 백업 데이터센터)에 보관된다. 동기화 모형은 관리기관과 분리된 복수의 장소에 데이터를 저장 및 관리하면서 추가 사본을 다른 장소(전세계에 산재한 등록대행자, 관리기관 및 백업 데이터센터)에 보관한다. 평가한 모든 모형들을 조사할 때, 관리기관이 연락처 데이터를 저장할 필요가 없는 “우회 모형(bypass model)을 제외한 대부분이 복수의 장소로 데이터를 전송해야 했다.

- 뿐만 아니라 동기화 모형은 지역 프라이버시 요건 준수를 위한 규칙을 좀 더 일관되게 적용할 수 있도록 허용한다. 잠재적으로 천 개가 넘을 지 모를 연합 모형 참가자들이 관리하는 것보다는 한 실체(동기화 RDS의 운영자)가 규칙을 관리하는 것이 더 쉽기 때문이다.

- **인증(Accreditation) –** 동기화 모형과 연합 모형 모두 인증 요건의 적용이 가능하다. 두 모형 모두 인증 시스템 오용자를 추적하는 것이 가능하지만 잠재적으로 참여자가 천 명이 넘는 연합 모형과 비교할 때 동기화 모형에서 한 실체가 데이터베이스를 관리할 때 훨씬 처리하기 쉬울 것이다. 또한 연합 모형을 구현하려면 추가 비용이 드는 것은 물론 일관된 시행과 감사 능력을 뒷받침하기 위해 세부적인 계약상의 의무, 서비스 수준 계약 및 ICANN 컴플라이언스에 대한 감독이 필요하다.

114페이지

- **운영(Operation) –** 동기화 모형은 운영과 관련된 부분에서 효율성을 제공하는데 이는 연합 모형으로는 얻지 못하는 부분이다. 예를 들면, 사용자 친화적인 포털을 개설해 다국어/자막으로 데이터를 표시해야 하는 경우 좀더 일관된 포맷으로 연락처 데이터를 번역 또는 음역이 가능한 동기화 모형이 훨씬 효율적이다. 연합 모형에서 이러한 일관성을 얻으려면 계약할 때 명확하게 기술된 번역/음역 표준 명세서가 필요할 것이다. 두 모형 모두 무작위 데이터 품질 감사를 실시하도록 설계하는 것이 가능하지만 동기화 모형에서 훨씬 더 쉽게 달성이 가능하다.
- 연합 모형의 경우 데이터 지연(data latency) 및 동기화와 관련한 우려가 감소한다. 표시될 데이터를 관리기관에서 직접 가져오기 때문이다. 그러나 동기화 모형의 경우 데이터를 끌어오는 과정에서 지연시간 문제가 발생하는데 검증기관과 등록대행자가(관리기관을 거쳐) 시기 적절하게 EPP를 SRDS로 업데이트하여 극복이 가능하다. (108번 준법 원칙 참조)
- **구현(Implementation) –** 연합 모형은 동기화 모형에 비해 현재의 WHOIS의 분산 모형에 좀 더 긴밀하게 맞출 수 있다. 그러나 EWG가 권고하는 강력한 기능들을 제공하기 위해 필요한 성능 요건과 검색 능력들은 현재 WHOIS가 제공하는 것보다 훨씬 더 뛰어난 사양과 성능 매트릭스를 요구할 것이다. 연합 모형의 모든 참가자들이 그들에게 기대되는 수행 수준을 보여주려면 더 뛰어난 ICANN 컴플라이언스에 대한 감독과 자원들이 필요할 것이다. 어느 모형을 채택하든 영향을 받는 당사자들은 검색 결과와 요구받은 연락처 정보를 제공하기 위해 RDS 인터페이스와 상호작용하는 소프트웨어 플랫폼을 업데이트할 필요가 있을 것이다.
- **비용(Costs) –** 동기화 모형을 채택할 경우 등록대행기관과 관리기관(및 검증기관)의 입장에서 비용 절감 효과를 기대할 수 있다. 연합 모형에서와 같이 끊임없이 RDS 인터페이스의 복잡한 질의(예, 역질의)에 응답해야 하는 운영상의 부담을 줄여주기 때문이다. 특히, 모형 비용 분석(부록 F에서 자세히 설명) 결과 다음과 같은 결론에 도달했다.

(1) 사용된 가정들을 전제로, 코어 RDS 시스템은 동기화 RDS(SRDS) 모형에서보다는 연합 RDS(FRDS) 모형에서 구현했을 때 비용면에서 약간 더 유리하다. 그러나 연합 모형은 역질의(Reverse Queries)의 숫자에 매우 민감하다. **역질의 양이 많을 경우, 연합 RDS(FRDS) 모형은 동기화 RDS(SRDS) 모형에 비해 훨씬 많인 비용이 든다**. 예를 들면, 역질의 부하가 1%가 아닌 3%가 될 경우, 연합 RDS(FRDS) 모형의 비용은 동기화 RDS(SRDS) 모형에 비해 35%나 더 증가할 것이다.

역질의 부하가 5%가 되면 전체 연합 RDS(FRDS) 비용은 약 85% 더 증가할 것으로 예상된다. 이것은 연합 RDS(FRDS) 모형의 불확실성과 위험을 상승시키는 매우 중요한 요인이다. 동기화 RDS(SRDS) 모형은 역질의 양에 상대적으로 덜 민감한 것으로 판단된다.

(2) 또한 연합 RDS(FRDS) 모형은 관리기관 운영자에게 미치는 [높은 비용] 영향으로 인해 비용 측면에서 전체 생태계에 미치는 영향도 더 크다. 연합 RDS(FRDS) 모형에서는 각 관리기관 운영자가 SLA에 의거해 역질의 및 WhoWas 히스토리 질의를 비롯해 RDS RDAP 질의에 대한 실시간 응답을 실행하고 지원해야 할 것이다. 후자의 경우, 관리기관 운영자가 히스토리 데이터도 보관해야 하기 때문에 관리기관의 입장에서 추가적인 비용 상승 요인이 된다. 이러한 추가 비용은 위에서 추정한 코어 RDS 시스템의 영향을 훨씬 넘어설 가능성도 있다.

(3) 뿐만 아니라 연합 모형은 응용프로그램 운영, 지원, 유지관리 및 시험 측면에서도 동기화 모형에 비해 더 많은 비용이 요구되는데 관리기관 운영자와의 상호작용이 훨씬 더 많을 것으로 예상되기 때문이다.

모형 비용 분석, 분석 범위 및 분석 방법 그리고 그 기초가 되는 용량(volumetrics)과 가정에 관한 자세한 사항은 부록 F와 2014년 3월에 IBM이 ICANN에 제출한 "*등록정보 디렉토리서비스(RDS) 구현 모형 비용 분석*[35]" 보고서에서 확인이 가능하다.

d. 데이터 저장, 에스크로 및 작업기록 원칙

번호	저장, 에스크로 및 작업기록을 위한 공통 요건
161.	반드시 위치, 보유, 프라이버시 및 접근 정책을 개발해야 한다.
162.	저장, 에스크로 및 작업기록 정책 및 실행을 위해 반드시 지역 및 국제 수준의 법률을 준수해야 한다.
	저장 원칙
163.	여분의 시스템을 확보하고(System Redundency) 단일 고장 지점을 제거하기 위해 데이터는 반드시 복수의 장소(즉, 검증기관, 등록대행기관, 관리기관, 에스크로 제공업체 및 RDS 제공업체)에 두어야 한다. ※ 리던던시 서비스: 한쪽의 데이터센터가 중단되면 다른 곳에서 가동되도록 하는

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

	고가용성을 제공하는 서비스
164.	데이터가 복수의 장소에 공존할 때 반드시 일관성을 유지해야 한다.
165.	등록정보디렉토리서비스(RDS)는 데이터 요소를 안전하게 보관해 허가받지 않은 공개나 이용으로 인한 위험으로부터 데이터 요소의 기밀성과 무결성을 제공해야 한다.

	보호해야 한다.
166.	트랜잭션 데이터는 반드시 무기한으로 저장해서 시간 경과에 따른 데이터 변동사항을 정확하게 기록하고 WhoWas 기능을 지원해야 하지만 적용가능한 정보보호법 준수를 위해 필요한 한도(해당하는 경우) 이상으로 오래 저장할 필요는 없다. 고아가 된(Orphaned) 연락처 정보는 법률에 따라 주기적으로(예를 들면, 연결성이 끊어진 후 1년) 정리해야 한다.
	에스크로 원칙[36]
167.	저장소의 포맷, 무결성 및 완전성을 검사하기 위해 에스크로 데이터에 대해 반드시 감사를 실시해야 한다.
168.	에스크로 및 에스크로 감사는 동기화 RDS 모형과 더 쉽게 조율이 가능하다.
169.	에스크로 데이터 자체는 반드시 암호화해서 감사자가 알 수 없도록 해야 한다.
170.	에스크로 데이터는 반드시 등록대행자 인증 계약서(Registrar Accreditation Agreement), 개별 일반도메인 관리기관 계약서 및 적용 가능한 정보보호법에서 요구하는 기간 동안 보관해야 한다. 현재로서 이 기간은 데이터를 공개하는 실체의 보증(sponsorship) 기간에 2년 추가된 기간이거나 일반도메인 관리기관 계약서에서 요구할 경우 그보다 더 길어질 가능성이 있지만 법으로 허용된 최대 기간을 넘지 않을 것이다.
	작업기록 원칙
171.	RDS 질의는 반드시 저장해서 시스템 사용 내역에 대한 기록을 제공해야 한다.
172.	분산 시스템을 표적으로 한 오용을 탐지하기 위해 작업기록을 보유해야 할 필요성이 있다.
173.	시간의 경과에 따른 데이터 요소 히스토리를 제공하기 위해 변동사항을 반드시 저장해야 한다.
174.	RDS 운영 기록에 대한 접근은 반드시 구체적인 목적이 있고 “알 필요”가 있는 신뢰할 수 있고, 인증되고, 허가된 개인과 실체로 제한해야 한다. 허가된 RDS 운영자 자신(RDS의 적절한 운영을 확인하고 고장을 해결하기 위해)과 허가된 정보보호 실체(RDS의 정보보호법 준수를 감시하기 위해)도 반드시 여기에 포함되어야 한다. (섹션 Viii(b), ‘사법기관의 접

[36] 애스크로는 신뢰받는 제3자(애스크로 제공업체)로의 암호화된 시스템 백업을 가리키며, 재난, 시스템 고장 발생 시 복구를 그 목적으로 한다. 자세한 것은 RAA를 참조한다.

	근’ 참조)

117페이지

IX. 비용과 영향

a. 비용 원칙

부록 F, ‘모형 비교를 위한 방법론’에서 보듯이 EWG는 RDS의 비용과 영향에 대해서도 고려했다. EWG는 권고한 모형의 일부 측면들이 새로운 비용을 발생시킨다는 것을 인정하지만 현재의 비효율적이고 종종 부정확한 WHOIS 시스템으로 발생하는 다른 많은 숨은 비용들이 감소할 것이라 믿는다. 권고한 RDS 모형은 새롭고 향상된 서비스를 제공하기 때문에 반드시 편익과 비용 모두를 평가해야 한다. 권고한 접근법은 정책결정자들에게 처음으로 RDS 시스템에서 등록정보를 요청하는 사람들이 시스템 운영에 효율적으로 기여할 수단을 개발할 수 있는 선택권을 제공할 것이다.

현재 WHOIS 운영 비용은 알려져 있지 않지만 WHOIS 서비스를 제공하는 관리기관 및 등록대행자는 물론 전체 생태계에 초래하는 비용을 포함한다. 등록대행자들은 WHOIS 비용을 세분할 필요가 없고 일반도메인에 대한 서비스 제공과 국가도메인에 대한 서비스 제공 비용을 구분하기 어려울 지도 모른다. 생태계의 다른 이해관계자들은 현 WHOIS 시스템의 비효율성과 결함으로 인해 비용을 발생시키는데, 가령 상표 보유자의 경우 도메인 투기꾼의 신원을 확인하기 위해 상표권 보호 회사와 상업적 WHOIS 서비스에 대해 비용을 지불한다.

EWG는 다음의 비용 원칙을 권고한다.

번호	비용 원칙
175.	공개 데이터 요소에 대한 허가받지 않은(비제한적) 접근은 반드시 무료로 제공되어야 한다.
176.	허가된 데이터 요소에 대한 사법기관의 인증된(제한적) 접근(정당한 법적 절차를 거쳐)은 특히 비용 문제를 고려해야 할 필요가 있다.
177.	RDS를 설계할 때 다른 목표를 훼손하지 않으면서도 비용 효율성과 최소화를 위해 노력해야 한다.
178.	RDS는 비용 회수 모형을 기반으로 운용되어야 한다.
179.	WHOIS에서 RDS로의 원활한 전환을 지원하고 RDS 구현에 따라 관리기관/등록대행자, 검증기관 및 RDS 사용자 인증 기구가 부담해야 할 비용을 최소화하기 위해 ICANN은 RDS 소프트웨어 개발 플랫폼을 마련하고 자금을 지원해야 한다.
180.	이러한 소프트웨어 개발 플랫폼이 다른 RDS 이용자들에게 과도한

	부담을 지워서는 안 된다.

118페이지

비용 회수 방안으로는, 사용자, 접근 데이터 요소 또는 목적에 따라 차등적인 라이선싱 비용(상업적 사용료, 파워 유저 가입비 또는 고급 접근 요금 등) 또는 관련 서비스 비용(크리덴셜 발급비 또는 사전 검증료) 부과를 들 수 있다.

또한 RDS는 관리기관과 등록대행자에게도 비용 절감 효과를 가져온다. 더 이상 이들은 공개적 접근성을 제공하거나 엄격한 서비스 수준 응답시간을 충족시켜야 할 필요가 없기 때문이다. 데이터 요청자 역시 비용 절감 효과를 기대할 수 있는데 법을 준수하지 않는 제공업체들(관리기관, 등록대행자, 검증기관 또는 공인 프라이버시/프록시 서비스 제공업체)로 인한 비효율성이 사라지기 때문이다.

b. 2013 RAA 하에서의 현 WHOIS와 비교했을 때의 이점

지금까지 부록 B에 제시한 많은 보고서와 연구들이 WHOIS의 결함을 지적해 왔다. 2013 등록대행자 인증 계약서(2013 RAA)에서 제시한 WHOIS 개선안들은 WHOIS 심사팀 권고안에 대한 ICANN 이사회 평가로 도출된 다른 개선안들과 함께 WHOIS에 대해 지적된 결함들을 다루었다.

2013 RAA에서 여러 새로운 의무, 무엇보다 정확성 향상을 위한 검증 및 확인 요건을 도입하긴 했지만 여전히 중요한 문제들이 잔존해 있다. 이러한 문제들을 아래에서 요약하고 본 보고서에서 관련 권고안이 포함된 섹션과 매핑시켰다.

2013 RAA 하에서의 WHOIS의 문제점	본 보고서의 관련 섹션
누구나 익명으로 모든 데이터 요소에 접근 가능해서 데이터 마이닝과 오용이 발생 가능하고 책임성이나 제재 능력도 취약하다.	III, ‘사용자/목적’ IV, ‘책임성 강화’ VI(d), ‘책임성과 감사’
개인 프라이버시 보호 능력 취약	VI(a), ‘정보보호’ VII, ‘도메인 소유자 프라이버시 향상’
등록정보 무결성 보장 능력 부족, 도메인 소유자가 다른 사람의 연락처와 같은 허위 연락처 정보를 쉽게 삽입하는 것이 가능하다.	V, ‘데이터 품질 향상’ V(g), ‘고유 연락처 데이터 능력’
보안 기능 결여	IV(b), ‘허가받지 않은 접근 및 제한적 접근’, IV(c), ‘RDS 사용자 인증’
감사 능력 결여	VI(d), ‘책임성 및 감사’

119페이지

2013 RAA 하에서 WHOIS의 문제점	본 보고서의 관련 섹션
	VIII(d), '데이터 저장, 에스크로 및 작업 기록'
접근 목적이 명시된 합법적 목적과 직접적인 연관관계가 없다.	III, '이용자/목적, III(e), '목적별 연락처.
일관성 없는 WHOIS 질의 인터페이스와 응답	IV(b). '허가받지 않은 접근 및 제한적 접근', VIII, 가능한 RDS 모형
다국어 등록정보 표시를 위한 지원이나 표준이 없다.	IV(b), '무단 및 제한적 데이터 접근', V(e), '검증기관과의 인터페이스'
서로 다른 데이터 프라이버시 체제 준수를 위해 서로 다른 규칙을 적용하는 능력 부족	VI(a), '정보보호'
허용할 수 없는 정확성 수준으로 인해 도메인 소유자와의 연락을 원하는 이해관계자들에게 비효율성을 초래한다.	V, '데이터 품질 향상', III(e), '목적별 연락처'
여러 도메인네임의 연락처를 업데이트하는 관리 과정이 매우 번거롭다.	V, '데이터 품질 향상', V(c), 정확성, 감사 및 교정 과정
프라이버시 및 프록시 서비스 고객의 식별 및 연락상의 어려움	III(e), '목적별 연락처, VII(a), '프라이버시/프록시 서비스', 부록 H, '전달 및 정보공개 모형'
도메인 소유자 및 그 제휴 기관에만 적용되는 2013 RAA 요건 외에 프라이버시 또는 프록시 서비스에 대한 규정이 없다.	VII(a), '프라이버시/프록시 서비스', 부록 H, '전달 및 정보공개 모형'

c. 위험영향평가

섹션 IV, '책임성 향상'에서 언급했듯이, EWG는 본 보고서에서 권고한 RDS 원칙들이 위험과 편익 사이의 올바른 균형을 유지하며 실제로 정의된 목적을 위한 적절한 데이터 수집 및 공개로 이어질 수 있을 지 확인하기 위한 광범위한 위험 평가 실시를 권고한다.

3월 14일, EWG는 도메인 소유자, 등록대행자, 관리기관 및 광범위한 범주의 개인, 기업 및 기타 현재 WHOIS 데이터를 소비하는 조직들을 비롯해 일반도메인 도메인네임

120페이지

등록정보를 제공하거나 사용하는 모든 당사자들에게 온라인 RDS 위험 설문조사에 참여해 줄 것을 요청했다. 이 설문조사를 통해 응답자들은 EWG에 WHOIS를 대신할 차세대 시스템이 그들에게 가져 올 편익과 위험에 관한 의견을 제시할 기회를 가졌다.

보고서를 마무리하기 전에 EWG는 예상하지 못했거나 불필요한 위험을 줄이려는 목적으로 이 설문조사를 통해 드러난 위험과 편익들을 조사했다. 2014년 5월 29일까지 영어로 실시한 이 설문조사를 통해 180건의 부분적인 응답과 대략 100건의 완성된 응답을 수집했다. 응답자들의 분포는 북미(68%), 유럽(35%), 아시아(20%), 남미(14%), 아프리카(11%) 그리고 오세아니아(10%) 등이었고 등록정보 제공자와 사용자의 비율은 고른 분포를 보였다. 설문조사 응답을 통해 드러난 가장 가능성과 영향력이 큰 위험과 편익은 기술, 운영, 법률 및 재무, 보안 및 프라이버시 등의 부문과 관련된 것이었다. 또한 25명 정도의 응답자들은 불가피하고 감수할만한 위험과 위험을 전환 또는 감소시킬 방법에 관한 의견을 제시했다.

이 주제에 관한 커뮤니티의 의견을 광범위하게 수렴하기 위해 EWG는 RDS 위험 설문조사를 2014년 7월까지, 영어 이외의 다른 언어로도 계속 실시하기로 했다. 설문조사 응답은 본 보고서에 대한 ICANN 이사회 검토를 위한 정보 제공과 향후 WHOIS를 RDS로 대체할 때 영향을 받게 될 모든 이해관계자를 위한 공식적인 비용, 위험 및 편익 분석 자료로 사용될 것이다.[37]

[37] ICANN의 공공 자문을 위한 DNS 위험 평가(첫 번째 반복) 참조

121페이지

X. 결론 및 향후 논의 사항

도메인네임 등록정보에 의존하는 생태계의 수 많은 이해관계자들의 시각을 고려한 끝에 EWG는 만장일치로, 사용자 누구에게나 일반도메인 등록정보에 대한 익명의 접근성을 허용하는 지금의 WHOIS 모형을 폐지하고 완전히 처음부터 새롭게 대체 시스템을 구축할 것을 권고한다.

EWG는 본 최종보고서에서 권고한 원칙들과 차세대 RDS가 지금보다 좀 더 견고한 토대를 제공하리라 믿는다. 그러한 토대가 개인의 프라이버시를 보호하고 ICANN 전체 생태계를 위해 더 큰 정확성과 책임성 그리고 투명성을 보장할 것이다. RDS는 최근에 협상을 끝낸 2013 RAA에 따른 개선안을 토대로 구축될 것이며 그보다 훨씬 뛰어난 시스템을 제공할 것이다. 이에 관해서는 섹션 IX(b)에서 좀 더 자세히 설명되어 있다.

본 최종 보고서가 매우 구체적으로 보일 수도 있으나 모든 것을 포괄하지는 못한다. 부록 A에 적었듯이 본 보고서는 이사회가 제기한 각 질문들을 다룬다. 그러나 향후 후속적인 정책 개발 과정(PDP)나 관련 구현 노력을 통해 좀 더 충실하게 다룰 필요가 있는 여러 문제들이 남아 있다.

- **RDS 사용자 커뮤니티를 위한 인증 기구와 정책.** 특정 사용자 커뮤니티가 허가된 목적을 위해 제한적 데이터에 접근하기 때문에 해당 커뮤니티의 구성원으로 누가 적격한 지 식별하기 위한 정책을 구현 단계에서 조사해야 하고 각 커뮤니티에 적합한 인증 기구와 모형들 역시 조사할 필요가 있다.
- **EPP 및 RDAP에 필요한 확장자.** 부록 G에서 자세히 설명하듯이, EWG는 RDS 요구를 뒷받침하기 위해 표준 프로토콜 사용을 권고하지만 권고된 RDS 모형과 데이터 요소를 완벽하게 지원하기 위해 필요한 특정 확장자들을 식별했다.
- **위험영향평가.** 섹션 IX에서 논했듯이 EWG는 권고한 RDS를 구현하기 전에 대규모 위험 평가 및 비용/편익 분석을 권고하며 이미 그 과정에 필요한 의견 수렴을 위한 설문 조사를 시작했다.
- **RDS 프라이버시 정책.** 섹션 VII에서 논했듯이, EWG는 프라이버시 보호에 관한 표준 우수 사례를 기초로 RDS를 위한 기본적인 ICANN 정책 초안 마련과 이 정책을 RDS 생태계 전반에 실행하기 위한 계약 조항의 개발을 권고한다.
- **연락처 데이터의 번역/음역.** 현재 이 사안과 관련해 정책 개발 과정(PDP)이 진행 중이기 때문에 EWG는 섹션 IV(b)에 제시한 원칙을 넘어서는 노력을

중복하지 않기로 하고 대신 추후에 현 PDP 결과를 조사해서 새로운 정책을 어떻게 RDS에 적용할 지 결정할 것이다.

- **프라이버시 및 프록시 서비스.** 공인 프라이버시/프록시 제공업체와 관련된 EWG 원칙들은 현재 일반도메인정책개발기구(GNSO)에서 이 주제에 관해 진행중인 작업과 함께 고려하고 현재 진행중인 PDP 결과를 RDS 구현과 조정할 필요가 있다.
- **검증기관 생태계.** 검증기관을 위한 승인 프로그램 및 전세계에 산재한 도메인 소유자 및 연락처의 연락처 세부정보를 검증하기 위한 프로세스 생성에 관해서 구현 단계에서 좀 더 탐색해 볼 필요가 있다.

RDS는 공들여 준비해서 서로 분리되어서는 안 될 상호의존적 요소들과 균형을 맞춘 타협안들을 반영한다. 이러한 타협안들은 EWG가 지금까지 해 온 작업에 관한 많은 공개의견수렴, 웨비나 및 자문을 통해 얻은 정보들을 기반으로 한다. 따라서, EWG는 이사회에서 본 최종보고서를 일반도메인정책개발기구(GNSO)에 보내 전체가 채택되도록 할 것을 촉구한다. 본 보고서의 RDS 설계 원칙들을 일부만 채택하거나 전혀 채택하지 않기로 할 경우 전체 생태계를 위해 의도했던 효용이 반감될 가능성이 있다. EWG는 구성요소들을 개별적으로 조사할 경우 과거에 WHOIS를 개선하기 위한 시도들을 통해 경험했듯이 커뮤니티 내에 의견차이와 그로 인한 교착상태가 반복되지 않을까 우려된다.

EWG는 본 최종보고서를 ICANN 의장과 이사회에 전달했고, 온라인 상에 공개적으로 게시했으며 런던에서 있을 2014년 6월 공개회의에서 다수의 세션을 개최할 예정이다. 또한 온라인회의(Webinar, 웨비나) 및 기타 보고서에 대한 논의 기회를 가지고 보고서에 관한 ICANN 커뮤니티의 질문에 답변할 것이다. 본 최종보고서는 이사회가 요청한, 일반도메인 등록정보 제공을 위한 일반도메인정책개발기구(GNSO)의 정책개발과정(PDP)과 해당사항이 있는 경우 계약 협상을 위한 토대 역할을 할 것이다. EWG는 이사회와 ICANN 커뮤니티가 다음과 같은 질문을 중심으로 본 보고서를 검토할 것을 권고한다.

- RDS가 현재의 WHOIS보다 바람직한가?
- 그렇지 않다면 ICANN 커뮤니티는 현재의 WHOIS 시스템을 계속 유지해야 하고 진화하는 인터넷의 요구를 충족시킬 수 있다는 데 동의하는가?

EWG는 본 최종보고서가 일반도메인 등록정보의 목적과 제공의 재정의를 지원하라는 ICANN 이사회의 지시를 충족시키고 ICANN 커뮤니티가 (일반도메인정책개발기구(GNSO)를 통해) 일반도메인 디렉토리서비스를 위한 새로운 글로벌 정책 수립을 위한 확고한 토대를 제공할 것이라 확신한다.