새로운 gTLD 프로그램
설명서

악의적 행위의 완화

발행일: 2009.10.3

배경 - 새로운 gTLD 프로그램

ICANN이 인터넷의 주소 지정 시스템 조정에 목적을 두고 다수의 이해 당사자가 참여하는 비영리 조직으로 10년 전에 창설된 이래로 미국 및 기타 정부들의 인정을 받은 ICANN의 기초 원칙 중 하나는 도메인 이름 시장에서의 경쟁을 촉진하는 한편 인터넷 보안 및 안정성을 보장하는 것이었다. 일반 최상위 도메인(gTLDs)의 확장은 현재 21 개의 gTLD로 대변되는 인터넷 주소 지정 시스템에 대한 더욱 많은 혁신, 선택 및 변화를 고려하게 될 것이다

새로운 gTLD 도입 결정은 정부, 개인, 시민 사회, 비즈니스 및 지적 재산권 선거구, 및 기술 커뮤니티와 같은 광범위한 이해 당사자들로 대변되는 글로벌 인터넷 커뮤니티의 모든 선거구와 구체적이며 긴 협의 과정을 거쳐 이루어졌다.

그 외에 ICANN 정부 자문위원회 (GAC), 대표자 자문 위원회 (ALAC), 국가 코드명 지원 기구 (ccNSO), 및 보안 및 안정성 자문위원회 (SSAC)도 함께 기여하였다

이러한 협의 과정의 결과 새로운 gTLD의 도입에 관한 정책이 마련되었으며 본 정책은 2007년에 일반 명칭 지원 조직 (GNSO)에서 완성하고 2008년 6월에 ICANN 이사회에서 채택하였다. 프로그램은 2010년에 시작될 전망이다.

본 설명서는 현재 초안 형태로 신청인 지침에 제시된 요건 및 과정의 이해와 관련하여 글로벌 인터넷 커뮤니티를 지원하기 위해 ICANN이 발행한 일련의 문서들 중 일부분이다.

2008년 말 이래, ICANN 직원들은 신청인 지침 초안 및 보조 문서에 관한 일련의 공공적 의견 포럼을 통해 인터넷 커뮤니티와 프로그램 개발 과정을 공유하여 왔다.

현재까지, 중요한 프로그램 자료에 관한 협의가 250 여일 간 지속되었다. 수집되는 의견들은 계속 신중한 평가를 거쳐 프로그램의 지속적 보완과 신청인 지침의 최종 버전 개발에 유용하게 쓰여지고 있다.

새로운 gTLD 프로그램에 관한 최근 정보, 일정표 및 활동에 대해서는 http://www.icann.org/en/topics/new-gtld-program.htm.을 참조하기 바란다

단 본 설명서는 하나의 논의를 위한 초안에 불과하다는 점에 유의하기 바란다. 그러므로 프로그램은 앞으로도 협의 및 개정될 수 있으므로 잠재적 신청인들은 새로운 gTLD 프로그램 제안 세부 사항 중 어떤 부분도 이를 확정적인 것으로 간주해서는 안 된다.

본 설명서의 핵심 사항 요약

ICANN 은 잠재적인 악의성 행위를 완화하기 위해 모든 레지스트리에 요구되는 하기와 같은 새로운 gTLD 레지스트리 계약에 특정 조치를 추가하는 안에 대한 의견을 구하고 있다

악의적 행위에 대한 연구 기간 중 ICANN 은 피싱 방지 실무 그룹 (APWG), 레지스트리 인터넷 안전 그룹 (RISG), 보안 및 안정성 자문위원회 (SSAC), 컴퓨터 비상 대응 팀 (CERTs) 및 금융 및 인터넷 보안 위원회 회원을 포함한 다수의 외부 소스에 협조를 요청하여 이들의 의견을 수렴하였다.

이들 당사자는 여러 잠재적인 악의적 행위 이슈들을 제시하였으며 ICANN 은 새로운 gTLD 레지스트리 계약에서 이들 이슈의 해결 또는 완화 방법을 강구하도록 하였다. 이들 권고 대책은 등록인들을 위한 전반적 보안 및 안정성 그리고 이러한 새로운 gTLD 구역의 모든 사용자에 의한 신뢰에 미칠 이익을 증진하고자 하는 것을 목적으로 한다.

시드니 회의에서 신청인 지침 초안 버전 2에 대해서 제시된 의견 그리고 동 회의 이후 협의 과정에서 제시된 의견에서는 악의적 행위를 완화하기 위한 대책 및 제어 장치가 새로운 gTLD를 위한 기초 레지스트리 계약 안에 필수 요건으로 명시되어야 한다고 권고하였다. 다음은 이들 권고안 준비 과정에서 고려된 내용과 이어진 과정의 요약이다.

권고안은 다음의 9 개 분야에서 악의적 행위의 위험성을 구체적으로 완화하는 방법을 제시한다.

1. 검증된 레지스트리 운영자
2. DNSSEC 전개를 위한 시연 계획
3. 와일드 카딩 금지
4. 네임 서버 엔트리가 구역에서 삭제될 경우 오펀 글루(Orphan Glue)기록의 삭제
5. 집중형 (thick) Whois 기록의 필요성
6. 구역-파일 접속 집중화
7. 레지스트리 레벨 오남용 담당자 및 절차 문서화

8. 신속 등록 보안 요청 참여 과정
9. 상위 보안 영역 확인에 대한 프레임워크 초안

아울러 우리는 이들 대책이 새로운 gTLD로 야기되는 악의적 행위의 증대 위험을 완화시키는데 크게 기여할 것으로 생각한다. 이러한 이슈에 관한 정책 작업 및 악의적 행위 완화를 위한 조치는 계속될 것이다. ICANN은 또한 보안 산업 및 ICANN 커뮤니티 내 회원 들을 결합하여 실무 그룹을 구성함으로써 솔루션을 개발하고 제안된 완화 대책을 실시하도록 할 수 있다.

서문

10년 전 ICANN이 인터넷의 주소 지정 시스템 조정에 목적을 두고 다수의 이해 당사자가 참여하는 비영리 기구로 창립된 이래 많은 국가 정부 및 기타 이해 당사자들이 인정하는 그 설립 기본 원칙 중 하나는 도메인-이름 시장에서 경쟁을 촉진하는 한편 인터넷 보안 및 안정성을 보장하는 것이었다. 향후 이 기구의 확장과 함께 인터넷의 주소 지정 시스템을 위한 개혁, 선택 및 적극적 변화가 야기될 것이다. 15억 인터넷 사용자를 보유한 지구 상에서 다양화, 선택 및 경쟁은 글로벌 네트워크의 지속적인 성공 및 확장의 열쇠가 된다.

이들 새로운 gTLD 신청 라운드들의 도입 결정은 글로벌 인터넷 커뮤니티의 모든 선거구와 상세하고 긴 협의 과정을 거쳐 이루어졌다. 광범위한 이해 당사자—정부, 개인, 시민 사회, 비즈니스 및 지적 재산권 선거구 및 기술 커뮤니티— 대표들은 18 개월이 넘게 논의를 진행하였다.

2007년 10월, 일반적 명칭 지원 기구(GNSO)— ICANN 에서 글로벌 인터넷 정책을 조정하는 그룹 중 하나—는 새로운 gTLD 및 승인된 일단의 권고안에 대한 정책 개발 작업을 완료하였다

본 정책 개발 과정의 정점은 바로 2008년 6월 파리 ICANN 회의에서의 커뮤니티 개발 정책을 채택하기 위하여 ICANN 이사회가 내린 결정이었다. 정책 과정 및 산물에 대한 개요는 http://gnso.icann.org/issues/새-gtlds/ 에서 확인할 수 있다.

본 설명서는 신청인 지침으로도 알려져 있는 제안 요청서 (RFP) 에 대한 인터넷 커뮤니티의 이해를 돕기 위해 ICANN 이 발행하는 설명서 역할을 할 일련의 문서 중 하나이다. 신청인 지침 및 이들 문서들에 대한 여론을 수집하는 기간 동안 상세한 검토 및 이들 아이디어에 대한 개정이 이루어질 것이며 이 의견들은 신청인 지침 작성 과정 중 문서 개정에 활용될 것이다.

본 설명서는 하나의 논의용 초안이라는 점에 유의하기 바란다. 그러므로 프로그램이 앞으로 협의 및 개정될 수 있으므로 잠재적 신청인들은 새로운 gTLD 프로그램의 제안 세부 사항 중 어떤 부분도 확정된 것으로 받아들여서는 안 된다.

악의적 행위 문제에 관한 커뮤니티 의견

ICANN은 IDN TLD를 포함한 새로운 TLD 위임을 위해 TLD 공간의 확장을 제안하는 성명에 대응하여 다수의 영역을 망라하는 수많은 여론을 수집하였다

여러 당사자들에 의해 확인된 문제점 중 하나는 새로운 gTLD로 야기될 수 있는 악의적 행동의 증대 가능성이었다. 본 문제를 해결하기 위해 ICANN 은 악의적 행동에 대응하여

전문가로부터 그리고 현존 gTLD 내에서 악의적 행동에 영향 받은 이해 당사자들로부터 의견을 구했다.

신청인 지침 초안의 초기 버전 1 및 2에 수용된 내용들은 신청인 지침 초안 버전 3에 명시되고 있는 권고안의 개발에 중요한 일차적 소스 역할을 하고 있다.

본 문제점에 관한 두 번째 소스는 악의적 행위 유형에 관해 SSAC 가 발행한 보고서들, 그 중에서도 특히 SAC038: 등록 대행업체 악용 담당 창구 (pdf) 및 SAC040: 착취 또는 오용에 대한 도메인 등록 서비스 보호 대책 (pdf)이다.

이들 보고서 및 SAC가 실시한 기타 연구에서는 레지스트리 및 등록인을 위한 최선의 보안 관행에 관한 지침을 제시하고 있으며, 최선의 보안 관행에 따라 신청인 지침 초안 및 새로운 gTLD 레지스트리 계약의 개정 제안이 유도되었다.

세 번째 소스는 피싱 및 이메일 스푸핑 (spoofing) 문제 증가로 야기되고 있는 신분 도용 및 사기 제거에 초점을 두고 있는 업계 내 조직인 피싱 방지 실무 그룹(APWG) 이 작성한 보고서 초안이다. 이 보고서는 APWG 구성원 전체를 대표하는 90여 회원이 가입되어 있는 APWG의 인터넷 정책 위원회 (IPC)에 의해 조정되었다.

주지할 것은 gTLD 및 ccTLD 레지스트리 그리고 등록 대행업체, 인터넷 서비스 제공자, 지적 재산권 소유자 그리고 보안 및 금융기관 등을 망라하는 수많은 ICANN 이해 당사자들이 모두 APWG 및 APWG IPC 회원들이라는 점이다. http://www.antiphishing.org/sponsors.html 참조.

APWG의 IPC는 gTLD의 계획적 확장이야말로 인터넷 범죄 공간에 잠재적 영향을 미치는 하나의 중요한 사건이라고 보고 있다. APWG IPC 보고서는 새로운 gTLD의 개시 기간 중 APWG 의 IPC 가 주목할 필요가 있다고 느끼고 있는 수많은 악의적 행위 문제와 관련하여 ICANN에 종합적이며 건설적인 의견을 제시하고 있다

네 번째 소스는 인터넷 신분 도용, 특히 피싱 및 맬웨어 배포 퇴치를 위해 제휴하고 있는 책임 있는 인터넷 관련 기구들의 글로벌 그룹인 레지스트리 인터넷 안전 그룹 (RISG)에서 제시하였다. RISG 보고서 (pdf)는 레지스트리의 수적 증가에 의해 야기될 수 있는 여러 문제점 들을 열거하고 있다

다섯 번째로 악의적 행위에 관하여 수집된 소스는 은행 및 금융 커뮤니티에서 수집된 일련의 의견이다. BITS 사기 완화 프로그램, 미국 금융업 협회, 금융서비스 정보 공유 및 분석 센터 (***FS-ISAC***) 그리고 금융 서비스 기술 컨소시엄 (FSTC) 등을 비롯한 일단의 업계 협회에서는 이들의 전문 지식을 지원하였다

네트워크 및 민감한 데이터의 확보에 관한 이들의 독특한 관점과 경험을 바탕으로 본

커뮤니티에서는 사용자 신뢰를 증대하고 악의적 공격에 의한 타협의 위험성을 완화하기 위해 안정된 비즈니스 관행 채택을 포함하여 레지스트리가 실시해야 할 조치 들에 대한 특정의 가치 있는 권고안을 제시하였다

새 gTLD 내의 악의적 행위 완화 대책에 관한 여섯 번째 소스는 구현 권고안 팀(IRT)에서 실시한 연구 보고였다. ICANN은 새 gTLDs의 구축에서 해결해야 할 별도의 큰 문제점으로 상표권 보호 및 악의적 오남용에 대한 가능성을 지적한 반면 이러한 우려를 해결하기 위해 제안된 교정적 접근들에는 하나의 중대한 교차점이 존재한다

IRT 연구 결과는 2009년 5월 29일에 발표된 "우리의 연구를 소개하는 IRT의 공개 서한" 에 요약되어 있다. IRT 는 새로운 gTLD의 실시로 상표권 보유자들이 직면한 잠재적 위험성의 해결책을 구하고자 하는 커뮤니티의 요청에 따라 2009년 3월 6일 개최된 ICANN 이사회 결의안(link) 에 의거하여 ICANN 지적재산권 선거구에서 조직하였다. IRT 팀이 작성한 보고서 (pdf) 는 8개 회원 및 2 개 임시회원의 경험 및 지리적 다양성을 반영하고 있다.

그 외의 소스는 인터넷 보안 최초 대응자 커뮤니티의 회원들에 의존한다. 미주, 아시아, 유럽 및 오세아니아 전 지역에 걸쳐 산재한 180개 회사, 정부 단체, 대학 및 기타 기구의 컴퓨터 및 네트워크 비상 대응 팀들로 구성되어 사이버 범죄 퇴치를 위한 전세계의 노력에 일조하고 있는 국제 침해 사고 대응 팀 협의회 (FIRST)와 같은 기구들 소속 회원들이 가치 있는 조언을 제공하였다

다양한 법 집행 기관의 회원들도 중요한 문제점의 정의 및 레지스트리 운영 변경 제안으로 지원을 하였고, 이는 인터넷 기반 범죄 퇴치에 일조하게 될 것이다.

앞에서 인용된 소스들 외에도 ICANN은 시드니, 뉴욕, 런던, 홍콩 및 아부 다비에서 개최된 공청회 참석자들의 의견을 참고하였다. 이러한 공청회에는 악의적 행위 가능성을 완화하는 문제 및 새로운 gTLD에 전적으로 초점을 맞춘 세션들이 포함되었다.

ICANN 은 새로운 gTLD에서의 악의적 행위를 해결하기 위한 잠재적 솔루션을 구하는 전용 icann.org 웹사이트 상에 wiki 를 유지하고 있다. 상기에 언급된 보고서는 이 wiki 에 게재되어 있으며 일반에게 참여 및 의견 표명 기회가 제공되었다.

확인된 주요 이슈

잠재적인 악의적 행위에 관한 다수의 문제점이 ICANN 과정에서 다양한 범위의 참가자들에 의해 제기되었다. 문제점 중 많은 것들이 독특하고 복잡한 기술적 취약점을 노정함으로써 다양한 제어 와 고려가 필요하지만, 이들은 다음과 같은 핵심 주제 영역들로 요약될 수 있다.

A. 악의적 행위자들이 레지스트리를 운영하지 않을 것을 어떻게 보장할

것인가?

소스들의 의견에서는 ICANN이 레지스트리의 수가 확장됨으로써 신뢰할 수 없는 운영자나 범죄자가 커뮤니티에 들어오도록 하여 악의적 행위를 발생시킬 수 있는 위험성을 완화시킬 조치를 취해야 한다고 요구하고 있다

B. 레지스트리 정보의 무결성 및 실용성을 어떻게 보장할 것인가?

도메인 이름 등록과 도메인 이름 해결 서비스의 질을 개선하여 소스들이 악의적 행위의 기회를 제한하도록 ICANN은 신규 gTLD의 생성을 권장하고 있다.

C. 확인된 오남용을 퇴치하기 위한 더 효과적인 노력은 어떻게 보장하는가?

악의적 행위가 이미 존재함으로써 모든 TLD 들에 영향을 줄 것을 전제로, 소스들의 의견은 새로이 구축되는 TLD 내에서 현재 진행중인 사이버 범죄 및 DNS와 도메인 등록 시스템 오남용을 완화하기 위해 활용 가능한 공정 및 도구를 개선할 것을 요청하고 있다.

D. 내재적으로 오남용 가능성이 있는 TLD 에 대한 증대된 관리 프레임워크를 어떻게 제공할 것인가?

특정한 새 TLD 들은 예를 들면 전자 금융 서비스 또는 전자 투표와 같이 높은 신뢰도의 인프라를 요구하는 전자 서비스 거래와 연관될 수 있으며 도메인 이름 시스템을 사용하여 악의적 행위를 이미 일삼고 있는 범법자로부터의 보호 조치가 더욱 요구되는 (에너지 인프라나 의료 서비스를 지원하는 경우와 같이) 중요한 자산과 인프라와 연관될 수도 있다. 이 경우 소스들 의견은 ICANN 이 이러한 구역의 운영에 더욱 신뢰를 높일 수 있는 하나의 시스템을 수립할 것을 권고하고 있다

제시된 완화 대책

상기 요약된 악의적 행위 문제들을 해결하기 위해 ICANN은 새로운 gTLD 실시 계획의 일환으로 복합적 조치를 취해야 한다고 생각하고 있다

ICANN과의 계약 상 새로운 gTLD 레지스트리 측의 의무 증대 외에, 이들 새로운 레지스트리들은 등록 대행 기관들과 비즈니스 및 보안 관행에 대한 더욱 강한 기준을 협의하도록 독려 받고 있다. 특히 새로운 gTLD 레지스트리들은 등록 대행 업체 들에게 이들 구역 내에서 라벨을 등록하기 위해 악의적 행위를 감소시킬 특정의 대책을 실시하도록 요구할 수 있는 능력을 갖게 될 것이다

아울러 ICANN 은 등록 대행 업체-등록인 인터페이스에서 구현되어야 하는 완화 대책을 해결하기 위한 기존의 정책 개발 및 실무 그룹의 노력을 보완하기 위해 커뮤니티와 공조

관계를 지속해야 할 것이다

다음은 신청인 지침 안의 최근 버전에서 실시되어야 하는 완화 단계 안의 일반적 범주이다.

1. 검증된 레지스트리 운영자
2. DNSSEC 전개의 시연된 계획
3. 와일드 카딩의 금지
4. 네임 서버 엔트리가 구역에서 삭제될 경우 오펀 글루 기록의 제거
5. 집중형 WHOIS 기록에 대한 필요성
6. 구역-파일 접속 집중화
7. 레지스트리 레벨 오남용 담당자 및 절차 문서화
8. 신속 등록 보안 요청 참여 과정
9. 상위 보안 영역 확인을 위한 프레임워크 초안

문제와 완화 대책의 관계

A. 악의적 행위자들이 레지스트리를 운영하지 않을 것을 어떻게 보장할 것인가?

1. 검증된 레지스트리 운영자

B. 레지스트리 정보의 무결성 및 실용성을 어떻게 보장할 것인가?

2. DNSSEC 전개 요건
3. 와일드 카딩 금지
4. 오펀 글루 기록 제거 독려

C. 식별된 악용 행위 퇴치를 위해 어떻게 노력을 더욱 집중할 것인가?

5. 집중형 WHOIS 의 필요성
6. 구역-파일 접속 집중화
7. 레지스트리 및 등록 대행 업체 레벨 오남용 담당자 및 정책 문서화
8. 신속 레지스트리 보안 요구 과정의 가용성

D. TLD 에 대한 강화 관리 프레임워크를 어떻게 제공할 것인가?

9. 상위 보안 영역 확인 프로그램

새 레지스트리 계약으로 실시할 특정 대책

하기 대책들은 신청인 지침에 포함된 내용으로서 모든 새 레지스트리에서 요구되는 절차들을 반영하고 있다. 신청인 지침 초안 내의 언어 위치가 확인된다. 각 특정 대책에 대한 이론적 근거에 대한 간략한 내용이 또한 기술되어 있다 (이탤릭 체).

1. 검증된 레지스트리 운영자

다음은 신청자 질문 (모듈 2 부록) 내용이다

ICANN은 다음의 어떤 이유로도 신청을 기각할 수 있다

신청사 또는 임원, 파트너, 이사, 또는 매니저나 기타 관계인 또는 신청사의 15% 이상을 보유하고 있는 (또는 수익권 상으로 보유 중인) 개인이나 법인으로서

a. 과거 10 년 이내에 금융 또는 기업 지배구조 부당행위에 연루된 중 범죄 또는 경범죄로 기소되었거나 사기 또는 신용 책임 위반죄를 범한 것으로 법원의 판결을 받았거나 상기 범법 행위와 실질적으로 동등한 것으로 ICANN 이 간주할 수 있는 범법 행위 당사자

b. 과거 10 년 이내에 정부 또는 산업 규제 기구에 의해 타인의 자금에 대한 부정직 또는 오용에 연루된 행위를 범한 것으로 처벌받은 경우

c. 현재 상기 (a) 나 (b)에 명시된 유형의 기소, 판결, 결정 또는 처벌을 야기할 수 있는 사법적 또는 규제적 절차에 연루되어 있는 경우

d. 신청이 고려된 시점에 유효한, ICANN 의 자격 박탈 조치 대상에 해당되는 경우, 또는

e. 신청 시점에 ICANN 에 신분 확인에 필요한 정보를 제시하지 못하는 경우

f. 다음을 포함하여, 도메인 이름 등록과 관련하여 불성실에 대한 책임을 명시한 결정 유형 또는 불성실 행위를 지속적으로 일삼는 경우

   (i) 주로 상표나 서비스 마크 보유자 또는 경쟁사에게 매도, 임대 또는 기타 양도할 목적으로 도메인 네임과 직접 관련되는 실비를 초과하는 금전적 보수를 취하기 위해 도메인 네임을 취득하는 경우, 또는

   (ii) 상표나 서비스 마크 보유자가 동일한 도메인 이름에 마크를 반영하지 못하도록

할 목적으로 도메인 이름을 등록하는 경우, 또는

(iii) 주로 경쟁사 비즈니스를 방해하기 위한 목적으로 도메인 이름을 등록하는 경우; 또는

(iv) 상업적 이익을 위하여 웹 사이트나 웹 상의 장소 또는 웹 사이트나 웹 상의 장소의 제품이나 서비스의 출처, 후원, 소속 또는 승인과 관련하여 상표나 서비스 마크에 혼동 가능성을 유발함으로써 인터넷 사용자를 웹사이트나 기타 온라인 장소로 유인하기 위해 도메인 이름을 사용하는 경우

주: 신청 과정에서는 과거의 범죄 행위 기록을 포함하여 이들 배경 점검 과정에서 수집된 정보가 고려됨

신청 과정에는 회사 및 개인 (예컨대 핵심 간부)에 대한 표준화된 철저한 배경 및 기준 점검이 포함된다. 이러한 조치는 기존의 중죄 범인, 범죄 단체 구성원 또는 악의적 기업 운영 전력이 있는 자들이 레지스트리 운영에 관여하거나 레지스트리 소유권이나 근접 제어권을 얻을 위험성을 완화해주게 된다.

2. DNSSEC 전개 요구

레지스트리 운영자는 이들의 구역 파일에 서명할 서면 계획을 제시하고 운영 개시 시점에 DNSSEC를 구현하도록 요구 받게 될 것이다.

하기의 언어가 기술적 검토를 전제로 레지스트리 계약 버전 3 규격 6에 추가되었다.

"레지스트리 운영자는 도메인 이름 시스템 보안 확장("DNSSEC")을 구현하도록 한다. 계약 기간 동안 레지스트리 운영자는 RFC 4033, 4034, 4035, 4509 및 4310 과 동 승계 조항을 준수하고 RFC 4641과 동 승계 조항에 기술된 베스트 관행을 따라야 한다.

만일 레지스트리 운영자가 DNS 보안 확장 기능을 위해 해시 형태의 부재 인증 (Hashed Authenticated Denial of Existence)를 구현할 경우에는RFC 5155 및 동 승계 조항에 따라야 한다. 레지스트리 운영자는 업계 최상의 관행에 따라 확실한 방법으로 자식 도메인 이름으로부터 공개키 자료를 용인해야 한다

레지스트리는 또한 동 웹 사이트에 키 자료 보관, 자신의 키에 대한 접속 및 사용 방법 및 등록인의 신뢰성 앵커 자료를 기술한 관행 및 정책 문서 (일명 DNSSEC 정책 기술서 또는 DPS)를 게재해야 한다

전반적 보안에 대한 DNSSEC 구현의 장점은 보안 및 인터넷의 안정성이 문서화된다는 점이다. ICANN 은 2009년 안에 루트 존을 서명하게 되면 새로운 gTLD의 구축으로 DNS보안 개선을 위한 이러한 중요한 수단의 사용이 가능하게 된다.

3. 와일드 카딩 금지

SSAC의 SAC041 보고서 (ICANN 이사회가 승인한) 및 기타 의견을 개진한 기구의 보고서는 ICANN 에게 새 TLD가 DNS 재지정 및 복합적인 DNS 응답 사용을 금해야 한다고 조언하였다

광고 서비스를 하는 사이트에 관련된 맬웨어의 최근 동향을 감안할 때, 광고 사이트에 대한 도메인의 재지정은 악의적 행위 증가에 대한 가능성을 드러내고 있다.

등록인에 의해 등록되지 않은 도메인 이름의 경우 또는 등록인이 DNS 구역 파일 내 목록 등재를 위해 NS 기록과 같은 유효한 기록을 제공하지 않은 경우, 또는 이들의 상태가 DNS 내에서 이들이 게재되도록 허락하지 않는 경우, RFC 4592에 기술된 DNS 와일드 카드 리소스 기록 또는 DNS 리소스 기록 합성을 위한 다른 모든 방법이나 기술의 사용 또는 레지스트리에 의한 DNS 내 재지정 사용은 금지된다

특히 그러한 도메인 이름에 대하여 질문을 받는 경우, 권위 있는 네임 서버는 RFC 1035 및 관련 RFC 들에 명시된RCODE 3 인 “이름 오류” 응답 (일명 NXDOMAIN)을 반송해야 한다.

본 조항은 레지스트리 운영자(또는 등록 서비스 제공에 종사하는 관계인)이 데이터를 유지하거나 그러한 유지를 위해 배정하거나, 또는 그러한 유지로부터 수입을 창출하는 DNS 트리 내 모든 레벨의 모든 DNS 존 파일에 적용된다

다음의 와일드 카드 행위 금지가 레지스트리 계약 버전 3 규격 6에 추가되었다

“등록인이 등록하지 않은 도메인 이름의 경우 또는 등록인이 DNS 구역 파일 내 목록 등재를 위해 NS 기록과 같은 유효한 기록을 제공하지 않은 경우, 또는 이들의 상태가 DNS 내에서 이들이 게재되도록 허락하지 않는 경우, RFC 4592에 기술된 DNS 와일드 카드 리소스 기록 또는 DNS 리소스 기록 합성을 위한 다른 모든 방법이나 기술의 사용 또는 레지스트리에 의한 DNS 내에서의 재지정 사용은 금지된다. 그러한 도메인 명에 대하여 질문을 받는 경우, 권위 있는 네임 서버는 RFC 1035 및 관련 RFC 들에 명시된 RCODE 3 인 “이름 오류” 응답 (일명 NXDOMAIN)을 반송해야 한다

본 조항은 레지스트리 운영자(또는 등록 서비스 제공에 종사하는 관계인)가 데이터를 유지하거나 그러한 유지를 위해 배정하거나, 또는 그러한 유지로부터 수입을 창출하는 DNS 트리 내 모든 레벨의 모든 DNS 존 파일에 적용된다.”

SSAC의 SAC041 보고서 *(pdf)* 및 기타 의견을 개진한 기구의 보고서는 ICANN 에게 새 TLD가 DNS 재지정 및 복합적인 DNS 응답 사용을 금해야 한다고 조언하였다

재지정 및 복합적 응답에 내재하는 위험성은 TLD 뿐 아니라 DNS의 종속적 레벨에도

존재하고 있다. 새 레지스트리 계약 내 조항은 레지스트리 레벨에서의 이러한 문제점을 해결하기 위해 고안된 것이다

4. 오펀 글루 기록 제거의 독려

발표된 오남용 금지 정책의 일부로서, 레지스트리는 하나의 네임 서버 엔트리가 구역에서 제거되는 시점에 오펀 글루 기록을 어떻게 삭제할 것인가에 대한 내역을 제시해야 한다. 다음은 신청 지침 초안 모듈 2 신청인 질문에서 다음의 내용을 발췌한 내용이다.

"오남용 금지 및 완화: 신청인은 인터넷 사용자에게 부정적 영향을 주는 등록 및 기타 행동의 오남용을 완화하기 위한 정책 및 절차에 대한 안을 게재해야 한다.... 답변에는 신속한 중단 또는 보류 시스템, 그리고 *구역에서 제거된 네임에 대하여 오펀 글루 기록의 관리 및 삭제에 대한 대책 안*이 포함되어야 한다. "

APWG의 한 연구 보고서에서는 피싱에 사용되는 도메인의 약 3%가 "오펀 글루 서버", 즉 이전에 레지스트리로부터 제거된 도메인의 잔존 형태를 사용한 것으로 추정하고 있다. 이것은 결국 오남용자들이 범법적 도메인 등록을 지원하기 위해 사용할 수 있는 그러한 TLD 의 구역 파일 내에 잠재적인 "안전한 피난처" 네임 서버 엔트리를 제공할 수 있다

5. 집중형 WHOIS 요구

레지스트리 운영자는 레지스트리 계약 양식 버전 3 규격 4에서 규정하고 있는 집중형 WHOIS 데이터 모델을 이용하여 등록 데이터에 대한 공공 접속을 유지 제공해야 한다

"WHOIS 서비스. ICANN 이 하나의 상이한 포맷 및 프로토콜을 명시할 때 까지 레지스트리 운영자는 최소한 하기 포맷의 하기 요소에 대하여 일반 무료 질문 방식으로 접속 가능하도록 규정하고 있는 RFC 3912에 따라 포트 43 및 <whois.nic.(TLD)> 웹사이트 두 곳을 통해 입수 가능한 등록 데이터 간행 서비스를 운영하게 된다

ICANN 은 인터넷 레지스트리 정보 서비스 ("IRIS" – RFC 3981 및 관련 RFCs)를 포함하여 대안적 포맷 및 프로토콜을 명시할 권한을 가지며 그와 같이 명시함과 동시에 레지스트리 운영자는 합당하게 실행 가능하게 될 경우 즉시 그러한 대안적 명시 행위를 구현하게 된다"

ICANN는 이전의 설명서 (*pdf*)에 기술된 바와 같이 집중형 Whois 아웃풋을 제공할 것을 요구하는 새 레지스트리 계약 안에서 Whois 개정을 제안했다.

아울러 ICANN 지적 재산권 선거구에 의해 조직된 구현 권고안 팀 (IRT)의 보고서 안 (*pdf*)에서는 " IRT는 집중형 WHOIS모델에서 레지스트리 레벨의 WHOIS 정보 제공이 소비자 및 지적 재산권 소유자의 비용 효율적 보호를 위해 필수적이라고 생각한다" 라고 기술하고 있다.

집중형 WHOIS 구현은 접근 가능성 확대 및 기록 접속의 안정성 개선을 보장함으로써 악의적 행동을 완화시키는데 기여할 것이다

6. 구역-파일 접속 집중화

ICANN은 집중형 제공자를 통해 이용이 가능하도록 레지스트리가 구역 파일 데이터에 대한 접속을 허용하도록 규정할 예정이다

레지스트리 계약의 규격 4 버전의 제안서 는 (기술적 검토를 전제로) 레지스트리 운영자가 일반적으로 그러한 데이터를 커뮤니티가 사용할 수 있도록 다음과 같이 규정하고 있다

"2.2.1. 일반적 접속. 레지스트리 운영자는 ICANN 이나 동 수임자에게 지속적 기반 위에서 수시로 ICANN 이 합당하게 규정하는 방법으로 레지스트리 TLD를 위한 레지스트리에 대하여 구역 파일에 대한 일괄적 접속을 제공한다.

"2.2.2. 중앙 구역 파일 예탁소:. ICANN 이나 그 수임자가 중앙 구역 파일 예탁소를 구축하는 경우 ICANN의 요구 즉시 레지스트리 운영자는 모든 구역 파일 데이터를 ICANN 또는 ICANN 이 지정하는 동 예탁소의 제 삼의 운영자에게 제공한다. 만일 이러한 중앙 구역 파일 예탁소를 구축할 경우 ICANN은 자체적 판단에 의해 본 규격 4의 제 2.1 항의 준수를 철회하지 않을 수도 있다. [본 항목 2.2.2는 악의적 행위 완화에 관한 이전의 커뮤니티 논의 결과로서 커뮤니티 논의 목적을 위하여 기술되었다. 본 조항에 따르면 ICANN 가 지정하는 자는 적법한 목적을 위하여 책임 있는 당사자에 의해 구역 파일 데이터 접속에 대한 점검 및 감독 업무에 관하여 현재 레지스트리 운영자가 수행하고 있는 책임을 인수할 수 있다]"

현재 개별적 레지스트리에 의해 취급되고 있는 레지스트리 구역 파일 데이터 접속을 더욱 수월하게 하기 위해 ICANN (또는 본 기능을 수행하도록 ICANN 이 지정한 당사자)은 새로운 gTLD 레지스트리에서 구역 파일 데이터를 수집하여 가입자들에게 데이터에 대한 전자 접속권을 제공할 수 있을 것이다. 이에는 또한 ICANN-지정 레지스트리에 대한 구역 파일 접속을 희망하는 당사자에 대한 단일 계약을 체결함으로써 ICANN 이 현재 모델에 기초한 접속 계약을 설정하여 양도 시스템을 채택 및 지원하는 방법이 포함된다

이와 같이 중앙에서 조정이 이루어짐으로써 오남용 방지 커뮤니티에서는 새 도메인들이 각 구역 내에서 생성되는 즉시 이들에 관한 소식을 효율적으로 구할 수 있게 될 것이다.

7. 레지스트리 및 등록 대행 업체 레벨의 오남용 담당 창구 및 정책의 문서화

레지스트리 운영자는 TLD 내의 모든 도메인에 대한 단일 오남용 담당 창구를 제공해야 한다.

이러한 오남용 담당 창구는 다른 레지스트리, 등록 대행 업체, 법 집행기구 및 오남용 금지 커뮤니티의 인정된 회원 등의 인정된 당사자로부터 수집되는 오남용 불만 사항 들을 해결하고 이에 대한 시의 적절한 대응책을 제시할 책임을 갖는다. 레지스트리는 또한 오남용 퇴치를 위한 이들의 정책을 설명해야 한다

레지스트리 운영자는 이들이 서비스를 위하여 계약을 체결하는 모든 등록 대행 업체에게 오남용 담당 연락처를 제공하라고 요구할 수 있다. 이러한 조치는 SSAC 보고서 SAC038 (pdf) 권고안과 일관성을 이루고 있다. 레지스트리는 또한 등록 대행 업체에게 레지스트리 오남용 정책과 일관된 오남용 정책에 대한 문서를 작성할 것을 요구할 수 있다. 두 레벨에서 정책들은 다음과 같은 방법으로 절차를 진행하게 된다.

1. 상호 오남용, 피싱, 고의적 맬웨어 배포 또는 불법적이거나 기만적 행동에 연루된 것으로 확인된 도메인 중단 조치
2. 재판매업자 또는 이들의 통제 하에 있는 서비스에 대한 기타 유통업자에 관련된 문제 해결
3. 악의적 행위에 관련된 오펀 글루 기록 제거
4. 오남용 담당 창구 및 동 연락처와의 소통이 어떻게 이루어질 것인가에 대한 확인

본 문제점을 해결하기 위해 레지스트리 계약 버전 3 규격 6에 다음과 같은 조항이 추가되었다

“레지스트리 운영자는 유효한 이 메일 및 우편 주소를 포함한 정확한 연락처 그리고 TLD 내의 악의적 행위에 관련한 조회를 취급하기 위한 주요 연락처를 웹사이트에 게시해야 하며, 연락처가 변경될 경우 ICANN 에게 그러한 변경 사항을 즉시 통지해야 한다.”

또한 다음은 신청 지침 초안버전 3 에 기술된 모듈 2 질문 발췌문이다.

“…각 레지스트리 운영자는 재판매업자가 연루된 경우를 포함하여 기록의 모든 등록 대행 업체를 통해 TLD 에 등록된 모든 이름에 관한 오남용 불만에 대하여 신속 대응 및 시의 적절한 응답을 제공해야 하는 문제들을 해결할 책임이 있는 단일 오남용 연락처를 정하여 이를 웹사이트에 게시해야 한다.”

본격적인 규모의 새 레지스트리가 구현되기 위해서는 도메인 등록 과정에서 새롭고 잘 정의된 제어 장치와 정의된 역할이 아마 대규모로 필요할 것이다. 레지스트리 및 등록 대행 업체 양 레벨에서의 오남용 담당 연락처 및 정책은 새 운영자의 추가와 함께 지속적인 악의적 행위를 퇴치하기 위한 향후 노력의 기본적인 단계가 될 것이다

8. 신속한 레지스트리 보안 요구 과정의 가용성

ICANN 은 gTLD 가 처한 현재의 또는 임박한 보안 상황을 ICANN 에게 알리고 보안 우려를 완화 또는 제거하기 위해 레지스트리가 취해야 할 또는 이미 취한 조치에 대한 계약적 포기를 요청하도록 레지스트리에 대한 과정을 규정하기 위해 Conficker 웜 대응에서 얻은 교훈에 기초하여 gTLD 레지스트리, 등록 대행 업체 및 보안 전문가들과 협의하여 하나의 추가적 절차를 개발하였다 (http://www.icann.org/en/announcements/announcement-01oct09-en.htm 참조)

보안 상황은 다음 중 하나 또는 복수로서 정의된다.

a. DNS 의 제도적 보안, 안정성 및 복원성을 위협하는 척도 및 심도의 악의적 DNS 관련 행위

b. 레지스트리 데이터의 잠재적 또는 실제적인 비합법적 공개, 교체, 삽입 또는 파괴, 또는 모든 적용 가능한 기준에 의거하여 사용되는 시스템에 의한 인터넷 상의 비합법적인 정보나 리소스에 대한 접속 또는 공개

c. ICANN의 gTLD 레지스트리 지속성 계획(pdf).에 정의된, 단수 또는 복수의gTLD 레지스트리의 중요한 기능의 일시적 또는 장기적 오류를 야기할 수 있거나 그러한 가능성이 있는 잠재적 또는 실제적인 바람직하지 않은 결과 (pdf).

ERSR은 레지스트리에 의한 즉각적 조치 및 ICANN으로부터의 신속한 응답 (24~48 시간 이내)을 요구하는 사건을 전담한다. 본 과정은 레지스트리 서비스 평가 정책(RSEP)을 통해 해야 하는 요청을 대체하기 위한 것은 아니다 (링크)..

9. 상위 보안 영역 확인 프로그램

선정된 전체 커뮤니티의 gTLD 내에서 향상된 신뢰성 니즈를 촉진하도록 ICANN 는 gTLD 검증 프로그램 프레임워크 초안을 만들었다. 현재 제안된 바와 같이 본 검증 프로그램은 완전 옵션으로 되어 있다

새로운 gTLD 신청 시 검증을 하지 않는 쪽으로 선택하더라도 이는 신청인에게 부정적 영향을 미치지 않을 뿐 아니라 평가 과정 상의 점수에도 관계가 없다. 검증 프로그램의 목적은 적절한 운영 및 보안 제어의 신청을 통해 수용 가능한 표준 및 검증되는 gTLD에서의 신뢰성을 제고하는 기준을 설정하는 것과 제어에 대한 gTLD 레지스트리 및 등록 대행 업체의 성과를 측정하는 것이다. 검증을 진행하는 방향으로 선택하는 gTLD 레지스트리는 검증된 gTLD의 마스터 목록으로 검증 가능한 “씰”, 또는 하나의 마크와 같은 공개적 디스플레이 방법을 통해 검증이 입증될 수 있다. ICANN 은 검증된 gTLD 의 마스터 목록을 유지관리 및 발행한다

검증된 gTLD 의 마스터 목록을 유지 관리하는 것 이외에, 프로그램 에서 ICANN의 역할은

프로그램 지배를 수립, 보완 및 관리하고, 커뮤니티와 협동하여 프로그램 표준 및 기준을 수립하는 것이다. 프로그램 표준 및 기준에 대한 gTLD 의 실제 평가는 독립적 개체에 의해 실시된다.

제안된 프로그램에서 검증에 도달하려면 레지스트리 운영이 하기의 원칙에 의해 일관적이어야 한다 (가이드 북 모듈 2 참조).:

a. 운영자가 효과적인 제어 장치를 운영하여 시스템의 보안성, 이용 가능성, 기밀유지성, 및 프라이버시, 그리고 중요한 레지스트리 IT 와 비즈니스 운영을 지원하는 정보 자산이 유지될 수 있도록 보장하는 것을 레지스트리가 입증할 것

b. 핵심 레지스트리 기능의 처리가 권한이 있으며 정확하고 완전하여 수립된 정책과 표준에 의해 시의 적절하게 실시될 것을 보장하기 위해 레지스트리가 효과적인 제어 장치를 유지할 뿐 아니라. 참여 개체의 신분이 확실하여 인증될 것

c. 그 등록 대행 업체에 의한 핵심 등록 대행 업체 기능의 처리가 권한이 있으며 정확하고 완전하여 수립된 정책 및 표준에 따라 시의 적절하게 실시될 것을 보장하기 위해 레지스트리가 효과적인 제어장치를 유지할 뿐 아니라. 참여 개체의 신분이 확실하여 인증될 것

검증을 획득하기 위해 필요한 공정에는 레지스트리 운영 및 부수적인 등록 대행 업체 운영에 대한 검증이 모두 포함된다

신청인이 검증 옵션을 신청하고자 할 경우, 이는 다음의 2 단계 공정을 거치게 된다

단계 I

새로운 gTLD을 위임하기 전에 신청인은 평가에 참여하게 되며 평가 대상은 다음과 같다

- 배경 정보
- 도메인 관리/중단 절차
- 오남용 담당 창구 및 응답
- 기록의 에스크로 절차

새 gTLD가 위임된 후 운영이 개시된 경우 신청인이 모든 선 승인 공정 및 제어를 실행 할 수 있도록 특정한 기간이 주어진다

단계 II

다음 단계에서는 단계 I 에서 문서화된 공정, 제어 장치 및 절차를 시험하여 이들이 계획대로 운영되는지 확인하게 된다. 만일 부적합 상태로 확인될 경우 이러한 내용은 독립적인 평가 기관에 의해 ICANN 에게 통고된다. 이 경우 레지스트리 운영자에게는 검증에 대한 신청인의 요청이 기각되기 전에 문제를 해결할 수 있는 유예 기간이 주어지게 된다. 레지스트리 운영자는 후에 검증을 재 신청할 수도 있다

새로운 gTLD 레지스트리 신청이 평가를 완료하고 TLD 가 위임될 경우 레지스트리 운영자는그 시점에 검증 신청을 결정할 수 있으며 이 경우 단일 단계에서 상기 시험을 실시하게 된다. 즉 신청인은 평가 과정을 동시에 병행하는 것이 아니라 평가 과정을 마친 후 검증을 획득하여 새로운 gTLD를 사용하는 단계를 선택할 수 있다.

검증 지원을 위해 필요한 제어 장치는 gTLD의 검증 상태를 유지할 수 있도록 정기적으로 감사를 통해 평가 받게 된다

ICANN 은 본 검증 프로그램이 레지스트리 및 등록 대행 업체 운영뿐 아니라 레지스트리, 등록 대행 업체 및 등록인 처리를 위한 관리의 정확성을 정립하기 위한 추가적 요건을 대가로 검증된 DTLD 내에서 한층 개선된 수준의 신뢰를 고려하게 될 것으로 생각하고 있다. 신뢰성 및 비용/이익 간의 균형은 검증이 추구해야 할 적절한 비즈니스 과정인 지 여부를 결정하기 위한 기반으로 사용해야 할 주요한 비즈니스 결정 사항을 형성한다

검증 프로그램은 레지스트리 운영을 위한 신뢰성에 대한 하나의 개선된 채널을 지원하기 위해 필수적인 일단의 제안된 활동에 적용된다. 프레임워크 초안의 초점은 ICANN으로부터 검증 씰을 구하기 위해 선정된 gTLD 내의 악의적 행위 가능성을 완화하기 위해 필요한 제어 장치에 초점이 맞춰져 있으며 그 범위는 레지스트리 및 등록 대행 업체 운영 레벨에서의 제어 및 활동으로 제한되며 등록인 운영까지 확장되지는 않는다.

검증 프로그램은 검증 대상 gTLD가 검증 기준을 충족하는 효과적인 운영 제어를 할 수 있도록 합당한 그러나 절대적이지는 않은 보장을 제공하는데 그 목적이 있다. 검증 기준의 수립과 함께 검증 프로그램을 통한 효용성의 정기적이며 독립적인 검토/감사는 따라서 신뢰도 수준을 한층 제고하게 될 것이다