Journal of The Institute of Electronics and Information Engineers Vol.53, NO.8, August 2016 http://dx.doi.org/10.5573/ieie.2016.53.8.028
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2016-53-8-4

국내 ID 연합 생성을 위한 연합 정책 개발 방안

(A Federation Policy Development Method for Generating Domestic ID Federation)

왕 기 철*

(Gicheol Wang©)

요 약

ID 연합은 사용자에게 다양한 서비스를 한번의 인증만으로 제공하고 서비스 제공자들에게는 사용자 정보의 개별적 관리 부담을 경감시켜주는 이점들을 제공한다. 이에 따라 국내에서도 연구 및 교육 공동체의 사용자들에게 솔기 없는 네트워크 연결성을 제공하고 제한 없는 연구 환경의 확장을 지원하기 위해 국내 ID 연합의 생성이 진행되고 있다. 본 논문에서는 국내 ID 연합 생성을 위한 기본 작업으로서 국외 ID 연합 정책들을 분석하고 비교한다. 또한, 국내의 환경을 고려하여 국내 ID 연합 정책에 포함되어야 할 내용들을 자세히 제시한다. 향후에 국내 ID 연합의 활성화를 위해서는 잘 만들어진 연합정책은 물론 적극적인 홍보, 다양한 서비스 발굴, 편리한 기술 및 서비스 지원체계 수립이 병행되어야 한다.

Abstract

ID federation provides users various benefits such as employing multiple services with only single authentication and mitigating management burden of service providers that individually preserve account information of users. To keep up with this international trend, efforts for making the domestic ID federation is ongoing to provide users in the domestic research and education community seamless network connectivity and to support tetherless extension of research environment. In this paper, we analyze the foreign ID federation policies and compare them as a underlying work for making the domestic ID federation. Besides, we suggest some contents that should be included in the domestic ID federation policy. To activate the coming domestic ID federation, we need to first have a well-made federation policy. Then, we need to aggressively promote the domestic ID federation, develop various and fascinating services, and build a convenient support system for technology and service.

Keywords : ID 연합, ID 관리시스템, SSO(Single Sign-On), ID 제공자, 서비스 제공자

Ⅰ. 서 론

최근 들어 인터넷 사용자들이 이용하는 서비스들은 기본적인 웹 서핑은 물론이고 이메일, 쇼핑, 온라인 예약, 사진 및 영상 공유, SNS(Social Networking Service) 처럼 매우 다양하다[1]. 각각의 서비스를 제공하는 사이트들은 사용자가 자신의 서비스에 가입하여 개인계정을 만들도록 요구하고 있으며 나중에 사용자가 같은 사이트를 방문하기 위해서는 그 계정을 접근하기 위한 ID와 비밀번호를 기억해야 한다. 따라서 사용자가 가입하는 서비스의 수가 늘어날수록 사용자가 기억해야 하는 ID와 비밀번호의 수도 늘어나서 관리의 어려움을 겪게 된다[2]. 한편, 서비스 제공자 입장에서는 한 사용자가 각각의 서비스 마다 가입한 계정정보(ID와 비밀번호)를 따로 유지한다면 이로 인한 관리비용이 증가한다. 또한, 임의의 서비스 제공 서버가 문제가 발생하면 다른 서버에 같은 사용자에 대한 계정정보가 있다 하더라도 서버간 계정정보의 공유가 불가하므로 이용가능한 서버의 계정정보를 이용하여 인증을 수행할 수 없는 비효율성이 발생한다[3].

ID 연합은 사용자에겐 단일 계정정보의 인증을 통해 다중서비스를 제공하고 서비스 제공자에겐 사용자 계정정보를 관리하는 부담을 덜어주는 기술과 표준을 이용

* 정회원, 한국전자통신연구원 위성항공ICT연구부
(Aerospace ICT Research Department, Electronics and Telecommunications Research Institute)
© Corresponding Author (E-mail : gcwang@etri.re.kr)
Received ; August 06, 2015 Revised ; January 25, 2016
Accepted ; July 26, 2016

하는 기관들의 연합체를 의미한다. ID 연합은 이미 국외에서는 WebSSO, eduroam, Moonshot 프로젝트와 같은 서비스들을 단일 계정정보로 효율적으로 이용하기 위하여 널리 사용되고 있다. 국내에서는 아직 ID 연합이 생성되지 않았으나 다중 서비스 이용자를 위한 단일 인증 기반의 접속환경 제공, 솔기 없는 네트워크 연결성 제공, 여행중 다양한 인터넷 서비스 요구 측면에서 그 수요는 매우 크다. 이에 부응하기 위해 국가 연구망인 KREONET(Korea Research Open NETwork)을 운영하는 KISTI(Korea Institute of Science and Technology Information)에서 현재 국내 ID 연합을 생성하기 위한 작업을 수행하고 있다. ID 연합이 여러 기관들의 연합체이기 때문에 이 연합을 잘 운영하기 위한 정책을 잘 설정하는 것이 매우 중요하며 KISTI에서는 현재 국내 실정과 환경에 맞는 ID 연합 정책을 개발하고 있다.

본 논문의 구조는 다음과 같다. 먼저 2장에서는 관련 연구로써 ID 연합 정책 템플릿 문서와 부록의 구조 및 내용을 분석한다. 또한, 이 문서를 기반으로 해서 만들어진 이스라엘, 칠레, 콜롬비아, 에쿠아도르의 연합 정책 문서의 구조와 내용을 분석한다. 이후에 3장은 ID 연합 정책 템플릿에서 제시하는 기본 구조를 중심으로 국외 ID 연합 정책들을 분석한다. 4장에서 국내 ID 연합정책 개발을 위해 포함되어야 하는 사항들을 제시한다. 5장에서 우리는 본 논문의 결론을 내린다.

Ⅱ. 관련 연구

유럽내의 범 연구 및 교육망인 GEANT(Grand European Academic NeTwork)은 임의의 국가에서 ID 연합을 새로 생성하거나 이미 만들어진 연합정책을 수정하기 쉽도록 연합 정책의 표준모델을 만들어서 ID 연합 정책 템플릿[4]을 만들었다. ID 연합 정책 템플릿은 크게 본문과 부록으로 구성된다. ID 연합 정책의 본문은 핵심적이면서 비교적 고정적인 내용들을 포함하고 있고 유동성이 높고 기술할 내용이 많은 정책들은 부록 부분에 포함시킨다.

ID 연합 정책의 본문은 일반적으로 정의 및 용어, 서론, 운영 및 역할, 적법성, 가입 및 탈퇴, 그리고 사용조건으로 구성된다[4]. 첫 번째로 정의 및 용어는 연합에 관한 정의와 정책 안에서 지속적이면서도 일관되게 사용될 용어들의 명확한 정의를 기술해야 한다. 두 번째로 서론은 연합의 명칭, 설립 목적, 혜택 등을 기술하고 부록 리스트를 얻을 수 있는 웹사이트 등을 제시한다. 세 번째, 운영과 역할은 연합에 관련된 문제들에 대해 자문을 수행하는 운영조직의 구성 및 선출방법, 운영조직의 권한 및 책임을 설명한다. 또한 운영과 역할부분은 연합 운영자 및 연합 멤버에 대한 책임과 권한도 명시한다. 일반적으로 연합운영자는 서비스의 신뢰성 있는 운영관리를 위하여 운영에 중대한 악영향을 끼친 멤버를 서비스에서 제외시키는 권한을 가진다. 연합멤버는 그 멤버의 역할에 따라 상응하는 의무와 권리가 주어진다. 네 번째, 적법성은 연합에 가입할 수 있는 멤버의 자격조건을 명시하며 일반적으로는 교육 및 연구업무를 수행하는 기관들에게 우선적으로 멤버자격이 부여된다. 만일 연합멤버 다수의 이익을 위해 다른 성격의 기관에게 가입을 허용하려면 가입 예외 조항과 특이사항 등을 명시할 수 있다. 다섯 번째, 가입 및 탈퇴는 연합에 가입하고 탈퇴하기 위한 절차를 간략하게 설명하며, 세부절차는 부록 혹은 웹 사이트에 명시한다. 특히, 탈퇴는 멤버가 탈퇴하는 절차와 연합 운영자가 탈퇴하는 절차를 따로 분리해서 기술해야 한다. 즉, 멤버의 탈퇴는 다른 멤버에게 영향을 미치지 않지만 연합운영자가 탈퇴하는 경우에는 연합의 서비스가 아예 종료될 수도 있기 때문에 서비스 중단 유예기간과 같은 조항이 제시되어야 한다. 여섯 번째, 사용조건은 종료조건, 책임과 배상 조건, 관할구역 및 분쟁해결 조건, 연합간 연합 조건, 개정 조건 등으로 구성된다. 먼저, 종료조건은 연합정책에 불응하는 멤버에게는 수정기간을 주고 그 이후에도 변화가 없는 경우에 강제로 탈퇴시키는 조건을 의미하며 강제탈퇴 후의 공지절차 등을 명시한다. 책임과 배상 조건은 연합운영자와 멤버가 서비스의 운영관리 혹은 사용 중에 현 연합의 멤버 혹은 타 연합의 멤버에게 손해를 끼친 경우에 책임과 그 한계를 설명한 것이다. 관할구역 및 분쟁해결에 관한 조건은 연합의 멤버 간에 다툼이 발생한 경우에 이를 해결하기 위한 방법을 제시한다. 연합간 연합의 조건은 연합멤버는 연합에 가입하면 현 연합이 국외의 타 ID 연합과의 상호 서비스 제공협정을 맺는 것에 동의한다는 조건을 의미한다. 또한 이를 통해 영향을 미치는 특정 기술 프로파일들의 구조를 설명하고 연합간 연합 서비스를 통해 발생하는 문제에 대한 해결 방법들을 명시한다. 마지막으로 개정조건은 연합정책을 변경하기 위한 절차와 변경내용이 효력을 발생시키는 방법 및 공지방법을 명시한다.

ID 연합 정책의 부록 부분은 연합의 서비스별 기술 프로파일, 보증수준 프로파일, 데이터 보호 프로파일, 연합운영 사례, 운영 그리고 회비 등으로 구성된다[4]. 기술 프로파일은 연합에서 제공하는 서비스에 대한 기

술적 내용과 서비스 제공에 필요한 멤버와 연합운영자의 책임을 정의한다. 보증수준 프로파일은 ID 제공자가 사용자의 ID에 대한 확실성을 보장하는 수준을 정의한다. 데이터 보호 프로파일은 ID 제공자 혹은 서비스 제공자가 사용자의 개인정보를 다루는 경우에 개인정보의 보호 방법을 정의한다. 연합운영 사례는 연합운영자가 제공하는 서비스, 시스템, 구성 데이터의 가용성 및 무결성을 보장하기 위해 수행하는 모범 사례 등을 제시한다. 기타 부록으로는 연합 운영을 위해 거출하는 회비에 관한 규정이나 운영조직의 구성 및 운영방법 등에 관한 세부 규정들을 다루는 내용 등이 포함된다.

이스라엘의 ID 연합 정책[5]은 1장 정의와 용어에서부터 5장 가입 및 탈퇴까지의 내용을 정책 템플릿 문서의 내용과 거의 동일하게 적용하고 있다. 반면에, 6장 사용조건에서는 사용자가 연합 서비스의 이용 중에 발생한 손실에 대해서 연합운영자나 운영조직인 IUCC(Israel interUniversity Computation Center)는 면책특권을 가진다는 것을 명시하고 있다. 그러나, 연합운영자나 IUCC가 정책을 위반함으로써 발생하는 손실의 경우에는 피해자로부터 수금한 회비의 합계 금액을 최고 배상 금액으로 설정하고 있다. 이스라엘의 정책은 영어로만 지원되고 구성원으로써 ID 제공자와 서비스 제공자를 가지며, 멤버 간에 스타형의 연결구조를 가지고 별도의 부록은 없다. 이스라엘 정책이 다른 연합의 정책과 다른 특이점은 정책의 마지막 부분에 서명란을 두고 있다는 것이다. 따라서 본문에 변경이 발생하면 모든 멤버들에게 다시 서명을 받아야 하는 문제점을 가진다.

칠레의 ID 연합 정책[6]은 1장 정의와 용어에서부터 6장 사용조건 까지 정책 템플릿 문서의 구조를 그대로 따르고 있다. 특이한 점은 3장 관리와 역할에서 단순히 연합멤버로서의 의무와 권리만 명시하고, ID 제공자와 서비스제공자로서의 의무와 권리는 각각 WebSSO ID 제공자 기관 부록[6]과 WebSSO 서비스 제공자 부록[7]에서 따로 명시하고 있다. 칠레의 ID 연합 정책에서 6장 사용조건은 다른 나라들에 비해 굉장히 간략하게 기술이 되어 있는데 이는 책임과 배상에 대한 문제와 분쟁 발생시 문제 해결 절차에 대한 내용이 빠져 있기 때문이다. 칠레의 연합 정책은 영어로만 지원되고 ID 제공자와 서비스 제공자를 가지며, 멤버간 연결 구조는 알려져 있지 않다. 또한, 칠레의 연합정책은 eduroam 서비스 부록을 가진다.

콜롬비아의 ID 연합 정책[7]은 ID 연합 정책은 1장 정의와 용어에서부터 6장 사용조건 까지 정책 템플릿 문서의 구조를 그대로 따르고 있다. 내용면에서, 콜롬비아의 ID 연합 정책은 2장 소개에서 5장 가입절차 까지는 정책 템플릿 문서의 권고조항 들을 대부분 채택해서 이용하고 있다. 반면에, 6장에서 콜롬비아의 연합정책은 칠레의 경우와는 다르게 연합구성원의 책임과 배상, 관할구역 및 분쟁해결 절차 등을 다루고 있다. 그러나 칠레의 ID 연합 정책은 이스라엘과는 다르게 면책사유에 해당되지 않는 피해유발의 경우에 최고 배상금액에 대한 조건제시 문구가 없다. 즉, 단순히 면책사유가 아닌 피해유발에 대해 책임을 물을 수 있다라는 정도로만 명시하고 있다. 콜롬비아의 연합 정책은 영어로만 지원되고 구성원으로써 ID 제공자와 서비스 제공자를 가지며, 따로 부록을 가지지는 않는다.

에쿠아도르의 ID 연합 정책[9]도 1장 정의와 용어에서부터 6장 사용조건 까지 정책 템플릿 문서의 구조를 그대로 따르고 있다. 또한 내용면에서 보면 에쿠아도르의 연합 정책은 2장 소개에서 5장 가입절차까지 정책 템플릿 문서의 예문들을 거의 동일하게 적용하였다. 반면에 에쿠아도르의 연합정책은 칠레의 경우처럼 책임과 배상 문제 및 분쟁 발생시 문제해결 절차를 다루지 않는다. 에쿠아도르의 연합 정책은 영어와 스페인어를 동시에 지원하고, ID 제공자와 서비스 제공자를 구성원으로 가지며, 멤버간 연결 구조는 알려져 있지 않다. 에쿠아도르의 연합 정책의 특이한 점은 연합 멤버에 대한 메타데이터를 등록하는 방법과 절차 등을 기술한 메타데이터 등록 사례문[10] 부록을 제공한다는 것이다.

Ⅲ. 국외 ID 연합 정책 분석

KISTI에서는 국내 연구 및 교육공동체에 속한 사용자들이 한번의 인증으로 국내 어디서나 필요한 서비스에 접근하고 서비스 제공자들에게는 사용자의 계정정보를 개별적으로 수집, 보관, 저장, 처리하는 노력으로부터 해방되도록 국내 ID 연합 생성을 추진하고 있다. 이에 따라 KISTI는 유럽내 범 교육 및 연구망인 GEANT과 접촉하여 국내 ID 연합 생성을 위한 도움을 요청하였고 GEANT으로부터 ID 연합 정책 템플릿[4]과 4개국(이스라엘, 칠레, 콜롬비아, 에쿠아도르)의 ID 연합 정책 문서들[5~11]을 수신하였다. 현재, KISTI는 이 문서들과 15개 국가의 연합정책을 비교 및 분석한 사이트[12]를 기본 자료로 이용하여 국내 ID 연합 정책을 개발하고 있다. 이 장에서 우리는 위에서 언급한 19개국의 ID 연합 정책 문서들을 분석하여 그 결과를 비교함으로써 국내

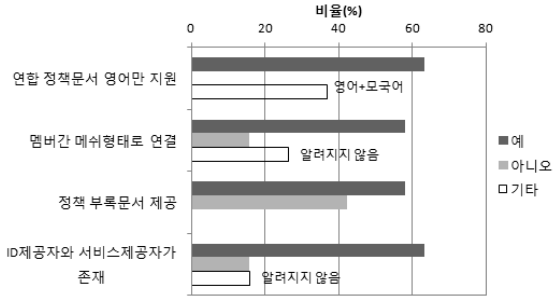

그림 1. 국외 ID 연합들의 기본구조 비교
Fig. 1. Comparison of Foreign ID Federation Architectures.

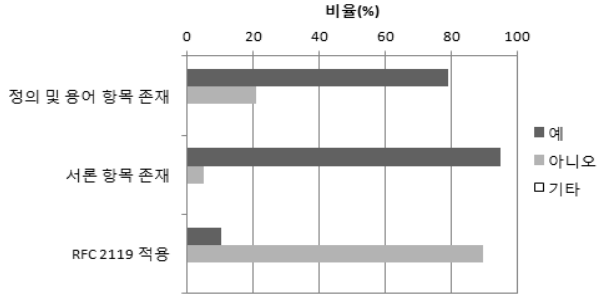

그림 2. 국외 ID 연합 정책들의 정의와 용어 비교
Fig. 2. Comparison of Definition and Terms among Foreign ID Federation Policies.

ID 연합 정책 개발에 참고하고자 하였다. 먼저, 우리는 분석한 국외 ID 연합들의 기본구조를 비교한다. 즉, 정책문서들의 사용언어, 멤버간 연결구조, 부록문서의 존재 여부, 그리고 구성멤버의 종류 등을 그림 1에서 분석한다. 그림 1에서 보는 것처럼, 사용자의 편의성을 위해 절반에 가까운 국가들이 정책문서를 영어와 모국어로 함께 제공하였다. 또한 멤버간 연결은 상호 동등한 메쉬구조로 연결되는 것이 일반적이었고 연합운영자를 허브로 하는 스타형의 연결구조는 20% 미만이었다. 또한 정책문서 본문 외에 부록 문서를 제공하는 국가도 그렇지 않은 국가에 비해 약 15% 정도 많았다. 마지막으로, 60%가 넘는 국가들이 연합 내에 ID제공자와 서비스 제공자를 모두 가지고 있었으며 둘 중 하나만 가지고 있는 연합은 20% 미만이었다.

그림 2는 정책의 서두에 나오는 정의와 용어부분에 대한 각 국의 연합 정책을 분석한 결과이다. 그림 2에서 보는 것처럼 정의와 용어항목은 약 80%의 국가들에서 제공하고 있으며 서론항목에 대해서는 90%가 넘는 국가들에서 자신의 연합을 소개하고 있었다. 그러나 RFC 2119에서 정의된 용어들은 대부분의 국가에서 적용하지 않고 있었다.

그림 3은 연합의 가입, 탈퇴, 그리고 적법성에 관한

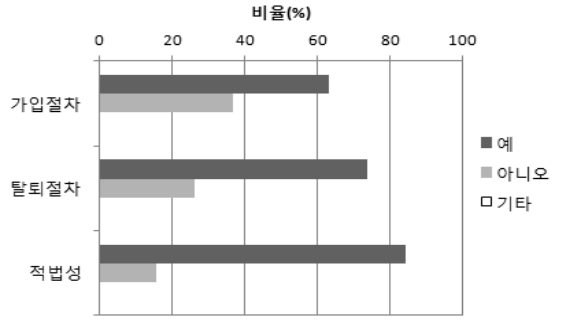

그림 3. 국외 ID 연합 정책들의 가입 및 탈퇴 비교
Fig. 3. Comparison of Join and Withdrawal among Foreign ID Federation Policies.

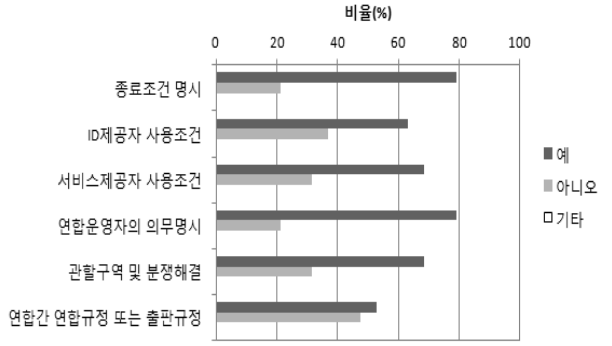

그림 4. 국외 ID 연합 정책들의 사용조건 비교
Fig. 4. Comparison of Terms of Use among Foreign ID Federation Policies.

규정을 각 국의 연합정책이 반영하는 지를 보여준다. 그림 3에서 보는 것처럼, 대부분 국가의 연합 정책에서 가입절차(60% 이상) 및 탈퇴 절차(70% 이상)를 명시하고 있다. 또한, 연합의 가입자격을 다루는 적법성에 관한 규정을 명시하고 있는 국가들도 약 85% 정도였다.

그림 4는 각국의 연합 정책에서 사용조건에 관한 규정들을 어떻게 명시하고 있는지를 보여준다. 그림 4에서 보는 것처럼, 대부분의 국외 연합들이 종료조건(79%), ID 제공자의 사용조건(63%), 서비스 제공자의 사용조건(68%), 연합운영자의 의무(79%), 그리고 관할구역 및 분쟁해결 절차(68%)를 정책에 명시하고 있다. 그러나 연합간 연합이나 멤버의 가입정보에 관한 출판 규정은 명시한 국가가 53%이고 그렇지 않은 국가가 47%로 그 차이가 크지 않았다. 특히, 유럽과 남미대륙에 있는 국가들이 연합간 연합 규정 혹은 가입정보 출판 규정을 명시하고 있었다.

그림 5는 GEANT에서 배포한 연합정책 템플릿에서는 다루고 있지 않은 내용이지만, 각 국이 연합 운영에 필요한 기타 규정들을 포함하는지 보여준다. 먼저, 로그

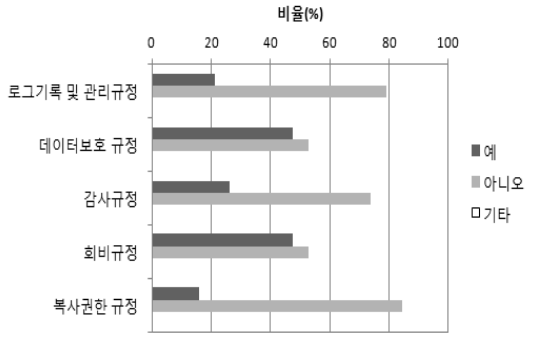

그림 5. 국외 ID 연합 정책들의 기타규정 비교
Fig. 5. Comparison of Et Cetera Rules among Foreign ID Federation Policies.

기록 및 관리에 관한 규정은 대부분의 연합(79%)에서 명시하지 않고 있어 특정 세션과 그에 관련된 사용자를 찾아내기가 어렵게 되어 있다. 반면에 데이터 보호 규정은 약 절반의 연합(47%)에서 각국의 개인정보보호법에 따라 사용자의 개인정보를 보호하도록 규정하고 있다. 임의의 연합 정책에 포함된 감사 규정은 연합멤버들이 그 연합의 정책에 순응하는지를 감사하는 권한과 비순응 시의 시정기간 및 제재조치들을 다룬다. 그림 5에서 보는 것처럼 대부분의 국가(74%)에서 이러한 감사 규정을 포함하지 않고 있다. 또한 각국의 연합 운영에 필요한 경비를 충당하기 위한 회비 거출은 약 절반의 국가(47%)에서 수행하고 있었다. 마지막으로, 오스트리아, 영국, 호주의 ID 연합만 연합정책의 복사권한에 관한 규정을 명시하고 있었다.

Ⅳ. 국내 ID 연합 정책 개발 방안

외국의 경우와 유사하게 한국 ID 연합 정책의 개발 방향은 ID 연합 템플릿 문서[4]의 기본구조를 이용하되, 국내 ID 연합 운용환경을 고려하여 내용을 가감하는 것이다. 본 장에서는 ID 연합 템플릿 문서에 포함되지 않은 내용 중에서 국내 ID 연합 정책 문서를 개발하는데 포함되거나 수정되어야 할 사항들을 제시한다.

1. 데이터 보호 프로파일 부록

국내 ID 연합 정책에서 데이터보호 프로파일은 ID 제공자와 서비스 제공자가 사용자의 개인정보를 다루는 경우에 이에 대한 보호방법, 책임, 의무 등을 명시해야 한다. ID 제공자의 경우에 소속된 사용자를 식별하기 위한 개인정보를 사용자로부터 입력받아 처리, 보관, 그리고 이용하게 된다. 이때 ID 제공자는 그 자신이 수집, 처리, 보관, 이용하는 개인정보에 대한 적법한 관리 책임이 있다. 따라서 국내 ID 연합 정책의 데이터 보호 프로파일에서는 ID 제공자의 불법적인 개인정보 취급 및 관리로 인해 임의의 사용자에게 발생하는 문제에 대해 연합운영자는 어떠한 책임도 없음을 명시해야 한다. 또한, 국내 ID 연합 정책의 데이터 보호 프로파일에서는 연합이 제공하는 모든 서비스에서 서비스 제공자는 개인정보를 수집, 처리, 보관, 이용하는 일체의 행위를 수행하지 않아야 한다는 것을 명시해야 한다. 사실, 서비스 제공자는 ID 제공자와는 다르게 서비스만을 제공하기 때문에 사용자의 개인정보를 다룰 필요가 없다. 만일, 서비스 제공자가 불법적으로 위의 행위를 수행한 경우 개인정보보호법에 의한 법적인 책임과는 별개로 연합차원의 징계 규정을 명시해야 한다. 그러나 국내 ID 연합에서 임의의 사용자가 해킹이나 침해사고와 같은 일탈행위를 수행하여 서비스 제공자 기관에 심각한 피해를 유발한 경우가 발생할 수 있다. 이 경우에는 국내 ID 연합 정책에서 ID 제공자 기관이 해당 피해 기관 담당자에게 피해 유발자에 대한 신원정보와 로그기록을 의무적으로 제공하도록 명시해야 한다.

2. eduroam 기술 프로파일 부록

임의의 ID 연합에서 eduroam 기술을 구현할 때 방문한 사용자의 인증이 완료되면 그 방문자에게 IP주소가 할당이 된다. 이때 방문자에게 할당되는 IP주소는 보통은 사설 IP 주소이지만 방문자의 패킷이 외부로 나갈때는 방문지의 WiFi망을 제어하는 컨트롤러의 주소로 변환되어 나가게 된다. 이는 IP주소 대역으로 사용권한을 할당하는 IEEE Xplore, ACM, ISI Web of Knowledge, SAGE 등과 같은 디지털 도서관 서비스에서 문제를 발생시킨다. 즉, 방문자의 입장에서는 소속기관에서는 허용되지 않은 서비스를 이용할 수 있는 이점이 있으나, 반대로 방문지의 사용자가 서비스에 가입하지 않은 기관에 방문하는 경우에는 서비스 이용이 불가한 불평등의 문제가 야기 된다. 서비스 제공자의 경우에는 서비스 미가입 기관의 사용자들이 서비스 가입기관들에 방문해서 무료로 서비스를 이용할 수 있게 되면 수입이 줄게 된다. 서비스 제공자가 이러한 불법적인 이용을 인식하게 되면 저작권 침해 문제에 대한 분쟁을 발생시킬 수 있다. Tekeni 등은 Shibboleth 구조나 VPN 터널을 이용하는 방법을 통해 해결 방안을 제시하였다[13]. 우리는 여기서 이러한 방법들을 한국의 연합 정책에 반영하기 위한 세부사항들을 제시한다.

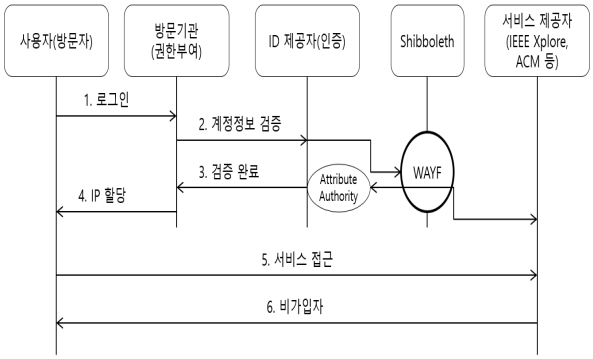

그림 6. Shibboleth를 이용한 eduroam 사용 절차
Fig. 6. Procedure for using eduroam with Shibboleth.

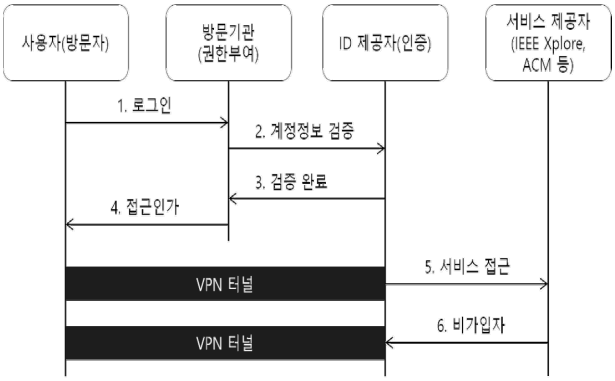

그림 7. VPN 터널을 이용한 eduroam 사용 절차
Fig. 7. Procedure for using eduroam with VPN tunnel.

그림 6은 Shibboleth를 이용한 eduroam 사용절차를 보여준다. 그림 6에서 보는 것처럼, ID 제공자가 인증요구를 받으면 인증요구를 WAYF(Whare Are You From) 데이터베이스를 통해 확인하고 인증이 성공하면 서비스 제공자는 ID제공자의 AA(Attribute Authority) 으로부터 사용자의 속성을 접근할 수 있다. 서비스 제공자는 사용자의 속성에 따라서 서비스의 가능여부를 판단하고 이에 따라 서비스 접근 여부를 결정한다. 따라서 국내 ID 연합에서 eduroam 서비스를 Shibboelth 구조를 통하여 제공하기 위해서는 국내 ID 연합 정책문서를 다음과 같이 생성하거나 변경해야 한다. 먼저, 정의 및 용어 부분에서 속성당국(Attribute Authority)의 정의를 포함해야 한다. 두 번째, 부록의 eduroam 서비스 기술 프로파일에 모든 ID 제공자와 서비스 제공자는 eduroam 서비스 제공에 있어서 Shibboleth 구조를 채택해야 한다고 명시해야 한다.

한편, Shibboleth 구조를 이용하지 않고 eudroam 서비스의 저작권 침해 및 서비스 불평등 구조를 해소하는 다른 방법은 그림 7에서처럼 사용자가 방문지에서 ID제공자에 인증을 받을 때 사용자와 ID제공자 사이에 VPN 터널을 형성하는 것이다. 먼저, 임의의 ID 제공자가 자신의 사용자로부터 인증요구를 받으면 계정정보를 검증하고 그 결과를 돌려준다. 그 결과가 성공이면 사용자와 ID 제공자는 VPN 터널을 생성한다. 이후에 사용자의 임의의 서비스로의 접근은 이 터널을 통하여 이루어지며 터널이 끝나는 곳에서는 ID 제공자의 IP주소가 할당될 것이므로, 가입되지 않은 서비스로의 접근이 자동으로 차단된다. 하지만 이 구조를 사용하려면 사용자와 ID 제공자 양쪽에서 VPN 하드웨어 혹은 소프트웨어를 설치해서 운용해야 한다. 따라서 이 구조를 사용하는 경우에 eduroam 기술 프로파일에 “ID 제공자와 그 기관 사용자는 방문지에서 인증에 성공한 후에 VPN 터널을 사용하여 eduroam 서비스를 이용하여야 한다”라는 조항을 명시해야 한다.

또 다른 대안으로는 각 기관별로 전자도서관 서비스 제공자와 사용계약을 체결하기 보다는 국내 ID 연합이 전자도서관 서비스 제공자와 사용계약을 체결하는 것이다. 이 경우에 연합에 속한 ID 제공자 기관들의 사용자들은 저작권 침해의 위험이나 불평등에 의한 불만의 염려 없이 서비스를 자유롭게 이용할 수 있다.

3. 적법성

해외의 경우에 ID 연합을 운영하는 기관들이 해당 국가의 연구망을 운영하는 기관이기에 그 연구망의 회원기관을 ID 연합의 가입자격을 가진 기관으로 정한다. 그러나 국내 ID 연합의 경우에는 연구망에 가입된 기관들 외에도 교육망이나 상용망에 가입된 기관 들이 다수 존재하기 때문에 비영리 기관을 가입자격으로 정하는 것이 외연 확대 측면에서 유리하다. 추가로 이 부분에서는 멤버로 가입하는 기관의 가능한 역할을 명시할 수 있다. 예를 들어, “본 ID 연합의 회원기관은 서비스 제공자는 물론 ID 제공자로 동작할 수 있다.”라고 명시할 수 있다. 만일 ID 연합에 유용한 서비스를 무료로 제공할 목적으로 영리 기관을 참여시키는 경우에는 이들의 활동범위를 서비스 제공자로 한정시켜야 한다. 예를 들어, “임의의 영리 기관이 자신의 서비스를 사용자들에게 무료로 제공할 목적으로 ID 연합에 가입하는 경우에는 서비스 제공자로만 동작할 수 있고 ID 제공자로서의 권리를 주장할 수 없다.”와 같은 문구가 그 역할을 수행한다. 이러한 한정 조항이 없는 경우에 서비스 제공기관의 사용자들이 연합이 제공하는 다른 서비스들을 이용할 수 있게 되며, 이에 따른 문제점 발생시 법적인 분쟁의 소지가 있다.

4. 책임과 배상에 관한 문제

국내 ID 연합 정책에서 책임과 배상에 관해 기술하기 위해서는 먼저 연합의 구성원간의 관계에 따라 책임을 별도로 부여하여야 한다. 각각의 관계에 대한 책임은 다음과 같다. 첫째는 연합 운영자와 운영 조직이 임의의 연합멤버에 대해 가지는 책임이다. 둘째는 임의의 연합멤버가 연합운영자와 운영 조직에 대해 가지는 책임이다. 셋째는 임의의 연합멤버가 다른 연합멤버들에 대해 가지는 책임이다. 넷째는 연합 운영자와 임의의 연합멤버가 연합간 연합을 통해 그들이 협력하는 다른 개체들에 대해 가지는 책임이다. 일반적으로 연합에서 제공하는 서비스의 사용에 의해 발생하는 손해나 손실에 대해서는 책임을 면하도록 조항을 명시해야 한다. 그러나 정책의 고의적 위반이나 서비스의 사용과 관련 없는 손실, 그리고 상위 법률에 의해 적용되는 손실 등은 손해에 대한 배상방법과 한도 등을 정해야 한다. 추가적으로 연합이 영리 기관의 연합가입을 허용하는 경우에 그 기관은 서비스 제공자로만 동작하므로 추가적인 내용의 기술이 필요하다. 예를 들어, “임의의 영리 기관이 연합에 가입하여 서비스 제공 중에 서비스 사용에 의한 유·무형의 손실에 대해 연합멤버나 연합운영자 혹은 운영 조직에 그 책임을 주장할 수 없다” 와 같은 면책조항이 필요하다. 그러나, 연합의 멤버 기관 사용자가 서비스 제공과 관련 없는 해킹이나 일탈행위로 인해 손실이나 피해를 입히는 경우에는 상위법인 정보통신기반보호법에 의해 적용을 받게 되므로 면책을 주장하기 어렵다. 이 부분은 법률자문을 받아서 손실을 유발한 사용자가 소속된 기관의 적절한 책임사항을 명시하고 법률에 저촉되지 않는 선에서 연합운영자 혹은 운영조직의 면책사항을 기술해야 한다. 만일 연합의 멤버 기관 사용자가 해킹이나 침해사고와 같은 일탈행위를 수행하여 서비스 제공자 기관에 심각한 피해를 유발한 경우에, ID 제공자 기관은 피해를 당한 서비스 제공자에게 피해 유발자에 대한 신원정보와 로그기록을 의무적으로 제공하도록 명시해야 한다.

5. 연합운영자의 탈퇴

국내 ID 연합 정책에서 연합운영자가 연합에서 탈퇴하는 경우는 두 가지로 나누어서 기술해야 한다. 먼저, 연합운영자가 자신의 권한이나 책임을 연합의 다른 멤버에게 이양하게 되는 경우이다. 이 경우에는 나머지 멤버들의 신규 연합운영자에 대한 수용의무 및 기존정책의 유효성에 관한 규정을 정책에 명시해야 한다. 또한 위의 문제로 인한 분쟁이 발생하면 이에 대한 해결방안을 정책에 명시해야 한다. 두 번째는 연합운영자가 후속 연합운영자를 찾는데 실패한 경우이다. 이 경우는 연합이 해체되는 것을 의미하므로 현 연합운영자가 일정한 유예기간 동안 서비스를 가능한 최선을 다하여 제공하고 그 이후에는 서비스를 종료하도록 명시해야 한다.

6. 복사권한 부록

국내 ID 연합 정책은 연합 정책에 대한 복사권한의 근거 문서, 접근 가능한 웹 주소, 그리고 정책사용의 라이선스 근거를 명시해야 한다. 또한, 국내 ID 연합의 로고를 개발한 경우에는 연합로고에 대한 무단 사용에 대한 금지문구와 사용허가 획득 절차 등을 연합정책의 복사권한 부록에 명시해야 한다.

7. 보상 부록

현재 ID 연합 정책 템플릿 문서의 내용에 따르면 대부분의 정책들이 규제 위주로 되어 있고 실제로 대부분의 연합정책들도 템플릿 문서의 내용을 준용하고 있는 상황이다. 그러나 ID 연합을 통해 사용자들에게 편의성을 제공하려는 기본 취지와 연합의 안정적인 운영을 위한 규제와 책임 위주의 정책이 서로 상충함으로써 신규 사용자의 ID 연합 가입에 걸림돌로 작용할 수 있다. 이를 방지하기 위해서 국내 ID 연합은 연합의 운영에 많은 공헌을 한 멤버들을 선발해서 적절한 보상을 제공하는 규정을 포함시킬 필요가 있다. 예를 들어, 가장 많은 사용자들에게 연합의 서비스를 제공한 기관, 서비스 중단 횟수가 가장 작은 기관, 사용자에게 가장 높은 평점을 받은 기관, 침해사고 발생 관련한 대응시간이 가장 빠른 기관 등에게는 회비면제, 포상, 신규 서비스 선행제공 등과 같은 보상을 제공하는 것이 필요하다. 이를 위해서는 국내 ID 연합의 정책의 보상 부록을 만들고 앞서 언급한 내용들을 명시해야 한다.

8. 보안 기술 부록

현재의 ID 연합 정책 템플릿 문서의 내용과 기존 ID 연합정책들에는 ID 연합의 운영 및 유지에 필요한 보안 기술이나 기법들을 별도로 명시하지 않고 있다. 이는 ID 연합을 운영 및 유지함으로써 특정한 보안 취약점이 발생하지는 않기 때문이다. 즉, 네트워크에 연결된 정보 시스템들이 현재 직면하고 있는 다양한 보안 위협들이 ID 연합을 구성하는 정보 시스템들에도 그대로 적용된다. 예를 들

어, SQL Injection, XSS(Cross Site Script), CSRF(Cross Site Request Forgery), 웹쉘과 같은 인증 우회 공격이 웹서버를 운영하고 있는 기관들에게 가해질 수 있으며 이에 대한 대비책들이 서버에 적용되어야 한다. 또한, 사용자가 이메일이나 메신저 혹은 P2P 프로그램을 통해 출처가 불분명한 파일을 다운로드 받다가 웜, 트로이 목마, 그리고 백도어와 같은 악성코드에 감염될 수 있다. 이러한 악성코드들은 감염된 호스트의 정보를 외부로 유출하거나 공격자에게 원격제어를 할 수 있는 핸들을 제공할 수 있기에 주기적인 탐지 및 제거활동이 수행되어야 한다.

위에서 언급한 보안위협들은 국내 ID 연합의 운영 및 유지에 있어서 필수적으로 제거되고 조치되어야 한다. 만일 위의 위협들이 제거되지 않고 국내 ID 연합의 시스템들에 영향을 미친다면 국내 ID 연합에서 제공되는 서비스의 신뢰성 및 가용성은 크게 저하될 것이다. 이는 곧 국내 ID 연합의 존폐를 가르는 요소로 작용할 것이기에, 국내 ID 연합 정책의 부록에 보안기술 부분을 두어서 다루어야 한다. 먼저, 국내 ID 연합의 멤버기관은 ID 연합을 구성하는 시스템의 자체적인 보안강화 방안을 수립 및 적용하고 ID 연합 차원의 보안강화 활동에 적극적으로 동참하고 협력하는 조항을 포함시켜야 한다. 또한, 국내 ID 연합 운영자도 멤버기관의 정보시스템에 대한 보안성 향상을 위해 보안수준 점검, 주기적인 자문, 기술지원, 협력체계 수립과 같은 활동을 수행하는 조항을 포함시켜야 한다. 이는 보안 문제가 멤버기관 단독으로 해결하기에는 인력적으로나 기술적으로 어려움이 있고 보다 많은 자원과 장비를 가진 연합 운영자와 협동 대응체계를 구축함으로써 보안성을 좀 더 강화할 수 있기 때문이다.

한편, eduroam과 같은 무선랜 서비스의 경우에는 eduroam 서비스 사용자가 인증을 거친 후에 서비스 제공 기관 내의 내부망에 접속하는 것을 원천적으로 차단할 수 있는 방법을 적용해야 한다. 그렇지 않으면 eduroam 서비스 사용자에 의한 침해 사고가 발생할 수 있다. 이를 위해서는 eduroam 서비스 영역을 물리적으로 다른 망으로 분리하고 그 사이에 방화벽을 설치하여 eduroam 서비스 사용자의 내부망 접근을 차단하거나 eduroam 서비스 사용자의 접근 가능한 서비스를 웹, DNS, 이메일과 같은 필수 서비스로 제한하는 논리적 분리를 수행해야 한다. 이 내용은 국내 ID 연합의 eduroam 기술 프로파일 부록에 명시하여야 한다.

Ⅳ. 결 론

본 논문에서 우리는 국내 ID 연합을 생성하기 위한 기반 연구로써 기존에 만들어진 국외 ID 연합 정책들을 몇 가지 분류 기준에 따라 비교하고 분석하였다. 다음으로 우리는 ID 연합 템플릿 문서를 기본으로 하되 국내 운용 환경을 고려한 ID 연합정책을 개발하기 위해 필요한 요소들을 식별하여 제시하였다. 향후에 국내 ID 연합의 발전과 활성화를 위해서는 먼저 적극적인 홍보활동을 통한 국내 ID 연합의 인지도 향상이 필요하다. 둘째, 교육 및 연구기관의 활발한 가입을 위해서 다양하고 매력적인 서비스들의 발굴이 요구된다. 마지막으로 사용자들이 다양한 기술 및 서비스 지원을 받을 수 있는 국내 ID 연합 기술지원 체계가 구축되어야 한다.

REFERENCES

[1] J. Kallela, “Federated Identity Management Solutions,” Technical Report, TKK T-110.5190, 2008, www.cse.tkk.fi/en/publications/B/1/papers/Kallela_final.pdf
[2] Y. Cho, S. Jin, P. Moon, and ,“Internet ID Management System based on ID Federation: e-IDMS,” The Institute of Electronics Engineers of Korea - Telecommunications, vol. 47, no. 7, pp. 104-114, Jul. 2006.
[3] E. Birrell and F. B. Schneider, “Federated Identity Management Systems: A Privacy-Based Characterization,” IEEE Security & Privacy, 11(5), pp. 36-48, Sep.-Oct. 2013.
[4] M. Vermezovic et al., “Identity Federation Policy template document,” Ver. 0.3, Dec. 10, 2012.
[5] Z. Yoash, Y. Brauch, and A. Aliper, “IIF(IUCC Identity Federation): Identity Federation Policy,” Ver 1.2, Sep. 21, 2014.
[6] S. Jaque and A. Lara, “COFRe: Comunidad Federada REUNA: Identity Federation Rules”, Ver. 2.1, Oct. 10, 2013.
[7] S. Jaque and A. Lara, “COFRe: Comunidad Federada REUNA: WebSSO Identity Provider Organizations Appendix”, Ver 2.0, Dec. 17, 2012.
[8] S. Jaque and A. Lara, “COFRe: Comunidad Federada REUNA: WebSSO Services Provider Appendix”, Ver 2.0, Dec. 17, 2012.
[9] D. Hernan and S. Garcia, “Columbian Federation of Identity for Research and Education (ColFIRE): Identity Federation Policy,” Ver. 1.2, Aug. 29, 2014.
[10] A. Martinez, “MATE Federation Model for

Access to Technology and Education: Identity Federation Policy," Ver 0.0, Jul. 15, 2014.
[11] A. Martinez, "MATE Federation Model for Access to Technology and Education: Federation Operator Practice: Metadata Registration Practice Statement," Ver 0.0, Sep. 2, 2014.
[12] Federaton Policy Best Practice, https://wiki.refeds.org/display/FBP/Federation+Policy+Best+Practice
[13] L. Tekeni, K. Thomson, R. A. Botha, "Concerns Regarding Service Authorization by IP Address Using eduroam," in Proc. of Information Security for South Africa (ISSA 2014), pp. 1-6, Johannesburg, South Africa, Aug. 2014.

저 자 소 개

왕 기 철(정회원)
1997년 광주대학교 전자계산학과 학사 졸업.
2000년 목포대학교 전산통계학과 석사 졸업.
2005년 전북대학교 컴퓨터통계정보학과 박사 졸업.
2006년～2007년 전북대학교 박사후연구원
2008년 전남대학교 박사후연구원
2009년～2013년 한국과학기술정보연구원 선임연구원
2013년～2016년 국방과학연구소 선임연구원
2016년～현재 한국전자통신연구원 선임연구원
<주관심분야: 무선 네트워크 보안, 무인기 시스템, 무인기 시스템 보안, ID federation>