ITU-T SG17 프라이버시 보안 국제표준화 연구

오흥룡
한국정보통신기술협회
hroh@tta.or.kr

A Study on the international standardization for privacy security in ITU-T SG17

Oh Heung-Ryong
Telecommunications Technology Association(TTA)

요 약

본 논문은 정보통신 보안 국제표준을 개발하고 있는 ITU-T SG17 연구반 내에 프라이버시 보안 국제표준을 분석하고자 한다. 프라이버시 보안은 사용자의 민감한 정보(개인정보)와 밀접하게 관련되어 있으며, 규제적 측면에서 보호와 기술적 측면에서 보호가 함께 만족될 때, 안전한 제도가 만들어질 수 있다. 본 논문에서 프라이버시 보호의 기술적 측면에서 논의되고 있는 국제표준을 분석한다.

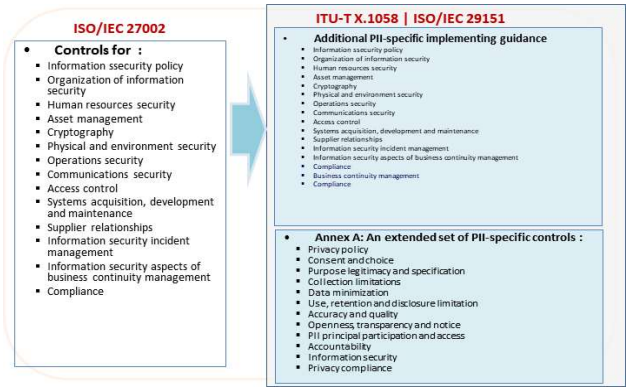
Ⅰ. 서 론

정보통신 국제표준을 다루고 있는 ITU-T SG17은 총 14개의 연구과제(Question)로 구성되어 있으며, 프라이버시 이슈를 다루고 있는 그룹은 Q3(보안관리), Q7(응용서비스보안), Q10(ID관리 및 메커니즘) 그룹에서 각 연구범위에 맞게 국제표준을 개발하고 있다. 본 논문에서 3개의 그룹에 개발되었거나 개발 중에 있는 프라이버시 보안 국제표준에 대해 분석한다.

Ⅱ. 본론

2.1 연구과제 3(보안관리)

연구과제 3에서는 정보보호관리체계(ISMS) 국제표준(ISO/IEC 27000 시리즈)을 근거로 네트워크 운영자 관점에의 보안통제, 보안지침 표준을 개발하고 있다. 특히, 중소기업이나 개발도상국 등 보안 운영 환경이 열악한 조직을 위한 국제표준 및 구현 지침을 개발하고 있다. Q3에서의 프라이버시 보안은 2017.4월에 제정된 ITU-T X.1058(개인식별정보를 보호하기 위한 구현 지침) 국제표준이다[2]. 이 국제표준은 ISO/IEC JTC1/SC27/WG5 공동표준(ISO/IEC 29151)으로 개발되었다.

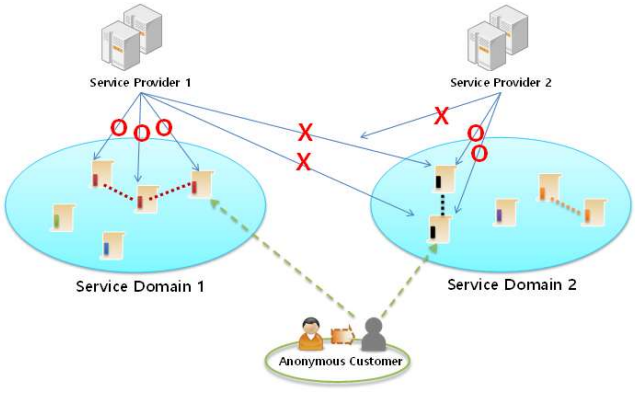


(그림 1) ITU-T X.1058 국제표준 주요 내용

X.1058 국제표준은 (그림 1)와 같이 ISO/IEC 27002 국제표준에서 제시하고 있는 보안통제 항목을 개인식별정보 보호에 구현하기 위한 지침을 정의하였으며, 개인식별정보 보호측면에서 보안통제 항목을 총 12가지로 추가 확대 정의하였다.

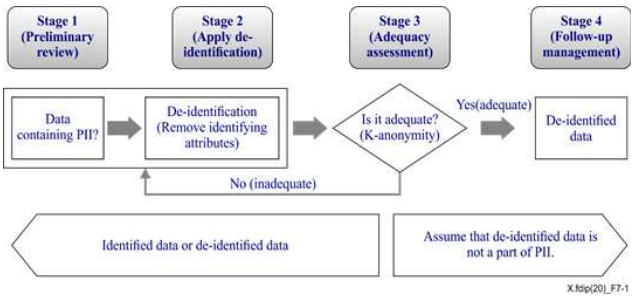
2.2 연구과제 7(응용서비스보안)

연구과제 7에서는 다양한 응용서비스 보안을 다루고 있다. 즉, 서버와 단말 간 통신구조, 단말과 단말 간 통신구조, 웹서비스, 응용보안 프로토콜, 안전한 인증기술들을 주로 담당하고 있다. Q7에서의 프라버이시 보안은 2016.6월에 제정된 ITU-T X.1155(전자서비스를 위한 부분 연결 가능한 익명인증 가이드라인) 국제표준이다[3]. 본 국제표준은 사용자가 다수의 쇼핑몰을 이용할 경우, 각각 쇼핑몰 사이트에 회원정보를 가입하지 않고도 물건을 구매할 수 있게 해주며, 사용자가 구매한 제품에 대한 소비자 취향 등의 프라이버시 보호를 가능하게 해 준다. 한편, 쇼핑몰 운영자 입장에서는 사용자의 익명성이 보호되지만, 쇼핑 취향에 대한 정보를 통해 홍보 활동도 가능하게 해주는 익명인증 기술이다. X.1155 국제표준에서 제시하고 있는 부분 연결 가능한 익명인증 개념은 (그림 2)와 같다.



(그림 2) ITU-T X.1155 부분 연결 익명인증 개념

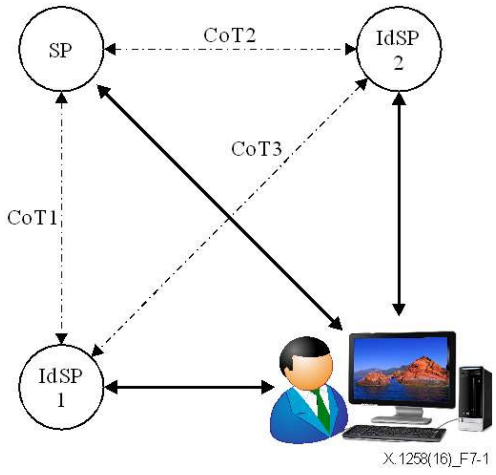
Q7에서 다른 프라이버시 보호기술은 민감한 데이터에 대한 비식별화 기술이다. 첫 번째 비식별화 국제표준은 X.1148(정보통신 서비스 사업자를 위한 비식별화 처리에 대한 프레임워크)이며, 현재 ITU-T 회원국 간에 의견수렴 중에 있어, 최종 채택은 2020.9월 SG17 국제회의에서 심의될 예정이다. 본 표준은 (그림 3)과 같이 데이터 생명주기 모델을 근거로 각 단계에서 비식별화 처리 및 고려되어야 할 보안 지침을 정의하고 있다[4]. 두 번째 비식별화 국제표준은 X.rdda(데이터 비식별화 보증수준을 위한 요구사항) 표준초안으로 공개수준의 범위, 비식별화 데이터의 적절성, 비식별화 보증에 대한 효율성을 고려해서 개발 중에 있다[5].



(그림 3) ITU-T X.1148 비식별화 프로세스

2.3 연구과제 10(ID관리 및 메커니즘)

연구과제 10에서는 ID(IDentifier) 식별자 관리 및 ID 연동 메커니즘, 이기종 IdM 시스템 간에 상호운용성에 대한 국제표준을 다루고 있다. Q10에서 프라이버시 보호기술은 2016.9월에 제정된 X.1258(속성 정보를 기반으로 향상된 개체 인증기술) 국제표준이다[6]. 본 국제표준은 쇼핑몰에서 특정 사용자들에게 할인쿠폰 등의 서비스를 제공하고자 할 때, 아주 유용하게 적용할 수 있는 국제표준이다. 즉, 쇼핑몰에서 만 18세 미만 여성에게만 할인쿠폰을 제공할 경우, 쇼핑몰 입장에서는 사용자의 나이, 성별 정보를 보유하고 있어야 모든 고객들 중에 적합한 사용자들을 구분할 수 있다. 하지만 이럴 경우, 사용자도 쇼핑몰에 민감한 개인정보를 등록해야 되고, 쇼핑몰 운영자 입장에서도 민감한 정보를 수집 및 보관해야 되는 위험이 존재하게 된다. 따라서, 쇼핑몰은 이러한 민감한 데이터를 수집하는 것 대신에 제3의 신뢰기간을 통해서 사용자의 속성 정보를 확인하는 인증구조이다. 한국에서는 통신사를 통한 사용자 인증 및 개인식별서비스와 유사한 구조이다. 따라서, 본 표준은 이런 서비스를 다양한 형태로 구축 및 운영할 수 있는 보안지침을 정의하고 있다.



(그림 4) ITU-T X.1258 속정정보 기반 인증기술 구조

Ⅲ. 결론

본 논문에서는 ITU-T SG17에서 다루고 있는 프라이버시 보안 국제표준화 동향에 대해 분석하였다. 특히 Q3(보안관리), Q7(응용서비스보안), Q10(ID관리 및 메커니즘)에서 연구하고 있는 개인식별정보 및 프라이버시 보호, 익명성 인증 기술 국제표준들에 대해 분석하였다. 정보보호 분야에서 개인정보보호 및 프라이버시 보호는 중요성이 점점 증가하고 있고, 국내외 규제가 함께 고려되어야 하는 측면에서 국제표준의 활용이 점점 증가할 것이다. 향후, 개인정보보호 산학연 전문가 및 정부 규제/정책 담당자들의 많은 참여가 필요할 것으로 예상된다.

ACKNOWLEDGMENT

본 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2017-0-00061, 국내ICT표준제개정연구).

참 고 문 헌

[1] ITU-T SG17 homepage, (https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx).

[2] ITU-T X.1058, “Code of practice for PII protection”, 2017.4.

[3] ITU-T X.1155, “Guidelines on local linkable anonymous authentication for electronic services”, 2016.6.

[4] ITU-T X.1148, “Framework of de-identification process for telecommunication service providers”, 2020.9(예정).

[5] ITU-T SG17-TD2377R2, “1st revised text for X.rdda”, 2019.9.

[6] ITU-T X.1125, “Enhanced entity authentication based on aggregated attributes”, 2016.9.