정 보 보 호 학 회 지
제 25 권 제 4 호, 2015. 8

온라인 아동 보호

나 재 훈*, 이 상 우*, 나 중 찬*, 김 정 녀*, 김 태 경**

요 약

본 논문에서는 ITU-T, ISO/IEC JTC1 SC27, GSMA, 및 OECD에서 진행되고 있는 온라인 아동 및 청소년들을 보호하기 위한 국제표준화 동향을 소개하고자 한다. 현재 ITU-T SG17 및 ISO/IEC JTC1 SC27에서 온라인 아동 보호 표준과 관련하여 우리나라가 주도적인 역할을 수행하고 있으며, ITU-T SG17에서는 새로운 국제표준 제정을 위해 계속적으로 기고서를 제출하고 있다. 또한 ISO/IEC JTC1 SC27에서는 2013년 10월 송도회의에서 연령검증이 SP(Study Period) 아이템으로 선정되었으며, 2015년 4월 회의에서 Anonymous attribute assurance 제목의 SP로 진행 되고 있다. 인터넷 상에서 유해정보 차단 및 안전한 이용자 환경을 제공하기 위해서는 온라인 아동 보호 표준에 대한 국제 및 국내표준의 제정이 필요하며, 효과적인 표준의 개발을 위해서는 게임업체 및 콘텐츠 서비스를 제공하는 기업들의 참여가 필요하다.

Ⅰ. 서 론

인터넷의 확산은 아동과 청소년에게 온라인교육을 비롯하여 게임과 음악 등 문화생활과 무한한 정보에 접근할 기회를 제공하면서 삶을 풍요롭게 해주는 반면 다양한 역기능과 역효과를 동반하기도 한다. 불법 콘텐츠의 유통, 사이버폭력, 포르노, 온라인게임 중독, 온라인 사기 등 온라인 세상에서 어린이에게 노출된 위험은 점점 더 다양해지며 심각해지고 있다.

현재 국내·외에서 온라인 아동 보호에 대한 연구가 활발히 진행 중이며 정부부처와 기업체들도 온라인 아동 보호에 대해 많은 관심을 기울이고 있다. 인터넷의 발전과 확산은 아동들에게 온라인 교육, 게임, 음악 등 문화생활 제공, 다양한 정보에 대한 접근의 기회 등 여러 이익을 제공해주는 한편, 역기능과 역효과들도 함께 가져오고 있다. 불법 콘텐츠의 유통, 사이버 폭력, 포르노, 온라인 게임 중독, 온라인 사기, 사이버 상 인종차별 등 온라인 세상에서 아동이 노출되어 있는 위험은 점점 더 다양하고 심각해져 가고 있어, 이에 대한 대처가 시급히 요구되고 있다. 온라인 아동보호는 네트워크로 연결된 인터넷의 특성상, 다른 사이버 이슈와 마찬가지로 한 개별국가의 독자적 문제가 아닌 국제적 수준에서 협력하고 정책적 대응방안이 확립되어야 한다.

2013년 상반기까지 진행된 온라인 아동보호 표준과 관련된 내용은 [1,2,3]에 기술되어 있으므로 본 논문에서는 ITU-T SG17 및 ISO/IEC JTC1 SC27에서 2013년 하반기 이후 진행되고 있는 온라인 아동보호 표준과 관련된 주요 활동들에 대해서 소개하고자 한다.

Ⅱ. 본 론

2.1. ITU-T의 활동

UN의 전기통신 부문 전문기구로서 전기통신 분야의 국제표준을 개발하고 있는 ITU에서는 온라인 아동 보호를 위한 국제간의 공동관심사에 대하여 이슈분석이 3개 부분으로 나뉘어 작업이 이루어지고 있다. 하나는 2008년 11월에 결의된 GCA(Global Cybersecurity Agenda) 내의 COP(Child Online Protection) Initiative 이고, 다음은 ITU Council 산하의 CWG- COP (Council Working Group-Child Online Protectioin)이며, 2009년 결의 1306에 근거를 두고 있다. 셋째의 조직은 PP-10(2010) 결의 179에 근거하여 COP를 위한 기술적 조치에 대한 분석을 TSAG (Telecommunication

본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신방송연구개발사업의 일환으로 수행되었음[R166-15-1018. 온라인 청소년 보호를 위한 ID검증기술 표준개발]

* 한국전자통신연구원
** 서울신학대학교 교양학부 교수

Standardization Advisory Group) 로부터 위임받아 ITU-T SG17 내에 CG-COP (Correspondence Group on COP) 2011년 4월 회의에서 결성되었다. 두 번의 분석 결과 보고를 통하여 기술적 분석이 더 필요함이 인정되어 현재 JCA-COP를 결성하여 운영하고 있다.

결의 179 (과달라하라, 2010)에 따라, ITU는 2010년 11 월에 ITU 사무 총장과 코스타리카 전직 대통령인 로라 친칠라(Laura Chinchilla)와 함께 시작한 COP 글로벌 이니셔티브 하의 활동의 두 번째 단계에 들어갔다. 2014년 부산에서 있었던 전권회의(PP-14)에서는 결의문 179에 관련하여, ITU는 COP 이니셔티브 파트너들과 지속적으로 세계적으로 COP 활동을 시행한다는 목표를 정하였다.

ITU는 다른 국제 포럼에서 전략적 설득, 지역 포럼 및 워크샵 등의 조직을 통해 COP 문제에 대한 인식을 제고하고 있다.

2008년 11월, ITU 내에 사이버보안 등과 같이 국제적으로 공동대응 및 협력이 필요한 전략그룹 GCA 내에 COP Initiative 협력 결의를 발의하였으며, 2010년 PP-10 결의 179에 의하여 그 활동이 재조명되었다. GCA에서 COP Initiative 협력의 주요 목적은 사이버공간에서 아동들을 위협하는 요소 및 취약점을 식별하고, 위협요소들을 인지하며, 이를 최소화할 수 있는 기술적인 방법(툴)을 개발하고, COP 활동을 위한 경험 및 지식을 공유하는 것이다.

2009년 3월, COP Initiative는 COP의 활동 결과물로 아이들을 위한 가이드라인, 부모 및 교육자를 위한 가이드라인, 산업체를 위한 가이드라인, 정책 개발자를 위한 가이드라인 등 총 4종의 가이드라인을 6개국 언어로 출판해서 배포하고 있다. 또한 ITU는 2010년 10월, 제18차 전권회의(Plenipotentiary Conference)에서 결의(Resolution) 179 'COP를 위한 ITU의 역할'을 신설하여, 차기 전권회의(2014년)에 4년간의 활동결과를 보고하기로 하고, 동 활동을 극대화하고 시너지 효과를 창출하기 위하여 관련 UN기구들과 협력·조정하기로 하였다.

온라인 아동 보호를 위한 ITU 이사회 작업반(CWG-COP)에서는 2010년 3월부터 ITU 회원국 및 섹터 멤버들로부터 각 국가마다 COP를 위해 취하고 있는 기술, 정책, 가이드라인 등의 정보를 수집하여 보고서를 개발하고 있다. CWG-COP는 사이버공간에서 어린이들에 대한 위험성 및 취약성 파악, 의식(관심) 창출, 위험성을 최소화시킬 수 있는 실질적 도구의 개발, 지식과 경험 공유를 주 목적으로 하고 있다.

ITU(International Telecommunication Union)의 JCA-COP에서는 2014년 1월 회의에서 ISO/IEC JTC1 SC27에서 SP(Study Period) 중인 연령검증(Age verification)에 대해서 발표가 진행되었으며, 계속적으로 COP 관련 표준화 활동들에 대해서 다른 표준화 기관들과 협력을 진행하기로 하였다.

ITU-T SG17에서 진행하고 있는 온라인 아동 보호 관련 표준화 아이템으로는 2013년 8월에 Q7에서 우리나라에서 제안한 강화된 이용자 인증을 위한 속성 바인딩 이라는 아이템이 있다. 이 아이템의 주요 내용은 서비스 제공자에게 사용자의 여러 속성값을 이용하여 기존의 인증방식보다 향상된 인증기능과 개인정보보호 기능을 제공하여 온라인에서 청소년들에게 안전한 사이버 이용환경을 제공하는 것이다.

제안한 아이템에 대해서 발표를 진행한 결과 다음과 같은 내용들이 논의되었다.

인터넷 상에서 유해정보 차단 및 안전한 이용자 환경을 제공하기 위해서 강화된 인증 기술에 대한 계속적인 연구와 국제적인 협력이 요구되는 것에는 모두 공감하였으나, 일부 국가에서 ID에 대한 속성 바인딩이 프라이버시 침해와 관련이 있는지 여부와 ID 관리 표준화와 중복성이 없는지에 대해서 추가적인 분석을 요청하였다.

2014년 9월 ITU-T SG17 Q7 & Q10 합동회의에서는 온라인 청소년 보호를 위한 핵심 메커니즘에 대한 분석이 있었으며 구현 가능한 메커니즘들에 대한 표준화 작업이 진행되고 있으며 그 내용은 다음과 같아.

현재까지 존재하는 속성정보 수집 모델을 분류하기 위하여 두 가지 기준이 제시된다. 하나는 속성 수집이 어디에서 이루어지는가 하는 것이고 다른 하나는 누가 전반적인 프로세스를 중재하는 가이다. 여기서 중재라 함은 수집 메커니즘을 최초 시도하는 것을 의미한다. 어디에서 수집이 이루어지는가의 기준에 의하면, 수집 메커니즘들은 SP(Service Provider)에서 수집, IdP에서 수집, 클라이언트(이용자 에이전트/브라우저)에서 수집과 같이 3개로 분류된다. 또한 수집이 이루어지는 장소에 더하여 누가 수집을 중재하느냐 하는 기준을 부가하면 SP에서는 SP 중재, IdP 중재, IdP에서는 IdP 중재, 클라이언트는 클라이언트 중재와 같이 분류할 수 있으며, 최종적으로 7종의 속성수집 메커니즘을 분류할 수 있다.

2.1.1 응용 데이터베이스 모델

이것은 가장 단순한 모델이다. SP가 로컬 식별자, 서비스에 특화된 선호도와 그룹 멤버십과 같은 이용자의 속성정보를 IdP가 제공하는 속성정보에 추가하여 저장할 수 있다. SP는 로컬 저장소에 SP가 생성한 식별자에 IdP가 제공하는 식별자와 연결하는 추가적인 속성정보를 저장하기 위한 매핑을 생성한다. 향후 이러한 로컬 속성정보는 특정서비스에 이용자가 접근 가능한지에 대한 결정을 하기 위하여 참조될 수 있다.

2.1.2 SP 중재 모델

이 모델에서, SP는 다수의 IdP로부터 한 세션의 속성정보를 수집할 수 있도록 이용자에게 허용을 한다. 이용자는 순차적으로 IdP에 의하여 인증되며, 각각의 IdP가 제공하는 속성정보가 SP에게 전달된다.

2.1.3 링킹 서비스 모델

링킹 서비스 모델은 링킹과 아이덴티티 릴레이 모델(아래 글에서 언급)의 조합형태이다. 링킹 서비스(이용자는 링킹 서비스가 제공하는 식별자를 이용)라는 특별한 형태의 SP로 구성된다. 이 식별자는 링킹표의 링킹 식별자를 이용하는 IdP들을 연결하기 위하여 사용된다. SP의 어느 특정 서비스를 접근하기 위해서, 이용자는 SP를 방문하면, 첫 번째 IdP로 전달된다. 이용자는 인증이 이루어지고, 이용자 속성을 포함하는 주장과 링킹 서비스에 대한 식별자와 링킹 서비스에 대한 참조가 SP로 회신된다. 그러면 SP는 속성정보 수집을 위하여 링킹 서비스 식별자를 링킹 서비스에게 전달하다. SP는 링킹 서비스로부터 IdP들의 리스트를 회신 받은 후, 각 IdP로부터 속성정보를 검색한다. 수집된 속성정보로부터 SP는 이용자가 서비스에 접근 가능한지를 결정한다.

2.1.4 아이덴티티연합/링킹 모델

이 모델은 리버티 얼라이언스에서 속성 수집을 위하여 최초로 소개된 모델이다. IdP들은 이용자에게 두 개의 IdP사이에서 상호 링크를 생성할 수 있도록 허용하였다. 링크를 생성하기 위하여, 이용자는 첫 번째의 IdP를 방문하여야 하고 인증 받아야 한다. 첫 번째의 IdP는 이용자에게 다른 IdP와의 연합(Federation)을 할 것인지를 문의하며, 그렇다면 두 번째 IdP로 연합을 요청하다. 이 시점에서 두 개의 IdP 간에 랜덤별명(Random Alias)를 만들기 위하여 상호 연동한다. SP로부터 서비스 접근 동안에는, 하나의 IdP는 속성정보를 포함하는 주장을 그 랜덤별명과 함께 SP에게 제공한다. SP는 다른 IdP로부터 속성정보를 포함하는 주장을 검색하기 위하여 랜덤별명을 사용할 수 있다. 두 개의 IdP로부터의 속성정보를 조합하여, SP는 이용자가 서비스에 접근 가능한지를 결정할 수 있다.

2.1.5 아이덴티티 프록싱 모델

이 모델에서 SP는 이용자가 매우 신뢰할 수 있는 IdP를 이용하여 다수의 IdP들로부터 속성정보를 수집할 수 있도록 허용한다. 첫째로 이용자는 신뢰하는 IdP로 전달된다. 신뢰 IdP는 이후 이용자를 해당 IdP들에게 전달을 한다. 이용자는 각 IdP들로부터 인증을 받은 후에 속성정보를 포함하는 주장을 신뢰 IdP로 회신한다. 이 시점에서 신뢰 IdP는 각 주장을 검증하고, 속성정보를 검색하여 최종 속성정보를 조합한다. 신뢰 IdP는 자신이 갖고 있는 사용자 속성정보를 더 부가할 수 있으며, 이것을 다시 주장으로 만들어 SP에게 전달한다. 전달된 속성정보를 기반으로 SP는 이용자가 서비스에 접근 가능한지를 결정한다.

2.1.6 아이덴티티 릴레이 모델

본 모델은 프록싱 모델을 일반화된 케이스이다. 프록싱 모델은 SP로 하여금 신뢰 IdP하고의 강한 신뢰관계를 요구하기 때문에, 프록시 IdP가 전적으로 요구하는 신뢰를 만족시킬 수 없으면 정상적으로 작동할 수 없다. 아이덴티티 릴레이 모델은 신뢰 IdP 대신에 중도적(Relay) IdP가 사용된다. 이용자는 처음에 릴레이 IdP에게 전달이 되고, 릴레이 IdP는 이용자를 다수의 IdP들에게 전달을 한다. 이용자는 각 IdP들로부터 개별적으로 인증을 받으며, 이용자 속성정보를 포함하는 주장과 함께 릴레이 IdP로 회신된다. 릴레이 IdP는 모든 주장을 하나의 주장으로 조합하여 SP에게 전달한다. SP는 전달된 주장 안의 각 주장들을 추출하고, 검증 하여 속성정보를 검색한다. 조합된 속성정보를 기반으로 SP

는 이용자가 서비스에 접근 가능한지를 결정한다.

2.1.7 클라이언트 중재 모델

이 모델은 릴레이 모델과 유사하다. 릴레이 IdP의 기능들이 다수의 IdP들로부터의 속성정보 수집을 위한 능력을 갖는 이용자 에이전트 또는 응용으로 대체가 된다. SP는 클라이언트에게 자신이 신뢰하는 IdP들에 대한 정보를 제공한다. 클라이언트는 이용자를 이러한 IdP들에게 전달한다. 각 IdP로부터 인증을 받은 후에, 클라이언트는 모든 IdP들로부터 주장을 받으면 SP에게 조합된 주장을 제시한다. SP는 각 주장을 검증하고, 모든 속성정보를 검색하여 이용자가 서비스에 접근이 가능한지를 결정한다.

ITU-T SG17에서의 온라인 아동보호 표준화는 계속적으로 한국 주도로 진행되고 있으며, 이러한 표준의 개발은 미성년자의 온라인상의 안전을 향상시킬 수 있을 것이라 예상된다.

2.2. ISO/IEC JTC1 SC27

ISO/IEC JTC1 SC27에서도 온라인 아동보호를 위한 표준화 활동을 수행하고 있다. 특히 지난 2013년 10월 회의가 우리나라 송도에서 개최되었으며, 우리나라에서는 신규 SP(Study Period) 아이템으로 연령검증(Age verification)을 제안 통하여 논의가 시작되고 있으며, 2015년 4월 회의에서 제목이 수정되어 계속적으로 표준화가 진행되고 있다.

연령검증이란 서비스 제공자에게 사용자의 연령이 특정 연령 이상인지 미만인지에 대한 정보(정확한 연령값은 제공하지 않음) 및 기존의 인증방식보다 향상된 인증기능을 제공하는 표준이다. 제안된 이 표준의 특징으로는 특정 웹 브라우저나 웹 브라우저용 플러그인 없이도 사용자의 연령을 검증할 수 있는 기능구조를 제시하며, 해외에서 외국인이 우리나라의 사이트를 이용하거나 우리나라에서 내국인이 해외의 사이트를 이용할 때, 각 국의 정해진 나이 기준에 의해 능동적으로 해당 나이에 맞는 서비스를 제공하도록 되어 있다. 또한 가장 중요한 특징으로는 사용자에게 개인정보자기결정권을 제공하도록 되어 있다. 즉 사용자가 서비스 제공자가 요구하는 여러 조건들을 충족시키기 위해 자신과 관련된 여러 속성정보들 가운데 제공하고자 하는 정보들을 선택할 수 있는 기능을 제공하여 프라이버시 이슈와 관련된 문제를 해결할 수 있도록 제안하고 있다.

JTC1/SC27 WG5 회의의 논조는 아이덴티티 관리 측면에서 일반적 메카니즘이 협소한 범위인 연령검즈에만 국한 할 필요가 없으며, 속성정보를 수집하고 이것에 대한 검증은 프라이버시의 문제를 내포하고 있으니 표준화 제목을 보편적인 내용으로 확대하고 프라이버시 이슈를 해결할 수 있는 것으로 수정을 하자는 의견이 받아들여져 Anonymous attribute assurance(A3) 라는 제목으로 SP가 다시 6개월 연장되었다.

수정된 A3 SP 아이템에 대하여 대한민국, 미국, 독일, 뉴질랜드, 영국, 말레이지아등이 찬성하였으며, 일본,에스토니아등은 우려를 표현하였다. 수정변경된 A3 대한 TOR (Terms of reference)은 다음과 같다.

- SP Age Verification 보고서를 기초
- 수정된 A3 SP는 부분 익명 속성 보증에 집중
- 관련된 요구사항, 표준 및 기술모델 조사
- 다음 사항을 고려하는 use-cases를 제시
  대표적이고 주요한 산업의 기능 요구사항
  기능 요구사항을 산업 분야에 매칭하는 것과 가능한 A3 기술 모델을 기능 요구사항에 매칭
  요구사항과 기술모델과 잠재적 프로젝트에서 다루어질 수 있는 방법을 제시
- 잠재적 프로젝트가 지침이 될지 아니면 실직 표준이냐 아님 두 개년을 다 포함하는지를 언급
- 추가적인 참고자료와 관련 주제를 제시

향후 계획으로는 A3 SP에 대해 각국으로부터 기고서를 받아 SP 보고서를 다음 인도회의에서 발표할 예정이며, 신규 아이템을 제안할 예정으로 있다.

2.3 GSMA(유럽 GSM 협회)

전 세계적으로 GSM 기반의 이동통신 분야 상호운용성 확보를 위한 표준규격을 개발하고 있는 GSMA에서는 모바일 기반 온라인 서비스가 실행될 때, 아동들이 불법 콘텐츠들에 접근하지 못하게 하는 기술들에 대한 표준을 개발하고 있으며, 모바일 사용자들의 가입정보를 기준으로 부가 서비스를 이용할 때, 실제 사용자들의

연령을 검증하는 메커니즘들을 연구하고 있다. 또한 불법 콘텐츠 등록 사업자들을 제재하기 위해 국가 및 유관 기관들간 협력이 필요함을 강조하고 있다.

GSMA는 온라인 아동 성적 학대 콘텐츠에 대한 조치로 2008년 개인이나 단체가 모바일 환경에서 아동 성적 학개의 콘텐츠의 사용을 제한 할 수 있는 모바일 얼라이언스를 시작하였다. 또한 젊은 청소년과 어린이들이 안전한 모바일 사용을 위하여 이동 전화의 아이들의 사용에 자율 규제 접근 방식을 활용한 “유럽의 프레임 워크”라는 강령을 제시하였다. 그리고 GSMA는 이동 전화를 통한 청소년들의 사용과 연령에 민감한 콘텐츠의 접근에 대한 책임 있는 관리를 위하여 참여 사업자들에게 지원과 교육 및 관련 정보를 제공하며, 사례공유와 툴킷을 제공하고 있다.
(http://www.fosigrid.org/companies/gsma)

2.4 OECD(경제협력개발기구)

OECD에서의 온라인 아동 보호에 대한 논의는 2008년 6월, ‘인터넷 경제의 미래를 위한 서울선언문’에서 본격화되었다. 서울선언문은 인터넷을 이용하는 아동에 대한 보호와 지원을 강화하기 위해 정부와 민간, 인터넷 기술 분야의 지원과 국제 협력의 중요성을 강조하였다. 이후 OECD 내 WPISP(정보보호작업반, Working Party on Information Securityand Privacy)를 주축으로 온라인 아동 보호에 대한 작업이 본격적으로 추진되었다. 2009년 4월, 일본에서 개최된 APEC(아시아·태평양경제협력체, Asia·Pacific Economic Cooperation)-OECD 공동 심포지엄에서는 아동의 안전한 온라인 활동을 위한 회원국들의 정책과 국제협력 증진방안, 그리고 모범사례가 공유되었다. 2010년 3월 개최된 OECD의 제28차 회의에서는 주로 온라인 아동 보호에 관한 정책의 접근방식에 대한 상호이해와 국제협조를 통한 온라인 아동 보호 증진방안의 필요성에 대해 논의하였으며, 2010년 12월 WPISP 제29차 정례회의를 통해 온라인 아동 보호에 관한 회원국의 정책 및 전략 비교분석과 주요 원칙을 담은 연구결과 보고서 ‘Protection of Children Online : Next Steps’를 발표했다. OECD는 온라인 아동 보호에 대한 최종 보고서인 ‘The Protecton of Children Online : Risks faced by children online and policies to protect them’를 2011년 5월 발표하였으며, 2012년 2월에 OECD Council의 Recommendation 으로 제정 되었다. 이 권고는 크게 세 파트로 구성되어 있다. 첫 번째는 온라인 환경에서 아동들이 직면하고 있는 위협요소들에 대한 분석자료이고, 두 번째는 이런 위협요소들을 정책적인 접근방법에 의해 해결하기 위한 사항들이며, 세 번째는 이런 위협요소들을 기술적인 접근방법에 의해 해결하기 위한 사항들을 제시하고 있다. 하지만 이 권고는 인터넷 이용자로서의 아동보호에 집중되어 있으며, 인터넷상의 아동 포르노, 아동 성매매에 대해서는 언급하지 않고 있다.

Ⅲ. 결 론

본 논문에서는 ITU-T SG17, ISO/IEC JTC1 SC27, GSMA, 및 OECD에서 진행되고 있는 아동 및 청소년들을 보호하기 위한 주요 활동 현황을 소개하였다.

아동 온라인 보호는 전 세계적으로 필요성을 인지하고 있는 사이버공간상의 문제점이다. 이러한 문제를 해결하기 위하여 각국에서는 이미 자구책을 마련하여 시행하고 있다. 그러나 세계 각국의 문화적 또는 종교적인 차이로 인해 아동보호가 잘 이루어지지 않고 있으며 어떤 위해 요소가 있는지, 또 누가 책임을 지고 해결해야 하는지와 같은 기초적인 질문에 다수가 공감할 수 있는 의결에 도달하지 못하고 있는 상황이다. 일례로 한 국가에서 ‘19금’이라는 청소년 유해 판정을 받은 콘텐츠가 미국, 네덜란드, 스웨덴, 일본 등에서는 비유해 판정을 받을 수 있다. 이러한 국가간 격차는 유튜브에서도 볼 수 있는데 유튜브의 유해등급 판정은 ‘자율’ 기준으로 운영되고 있어서 각 국가의 유해성 기준이 적용되지 않고 이용자의 협의에 의해 운영되고 있다. 이러한 운영방식으로 인하여 불의의 희생자가 발생되고 있음을 인지하여야 한다.

그러므로 아동 온라인 보호는 단지 한 국가에 국한되는 것이 아니라 세계적인 문제이며 향후 기술, 표준, 정책이 조화롭게 협력하며 해결되어야 할 국제적 사안으로 인식되고 있으며 ITU-T, ISO/IEC JTC1과 같은 표준기구에서 보편적 기술적 조치로 아동보호를 위한 표준개발이 진행중에 있다. 즉 속성수집을 기반으로 보다 강화된 인증과 프라이버시를 보장하는 기술적 방편에 대하여 표준이 논의중에 있다.

참 고 문 헌

[1] 김태경, "COP 보안기술 동향", 정보보호학회지 제22권 제3호, pp.13-18, 2012년.

[2] 오흥룡, 진병문, 나재훈, 염흥열, "정보통신망에서의 온라인 아동보호(COP) 국제표준화 동향", 정보보호학회지 제22권 제3호, pp.7-12, 2012년.

[3] 나재훈, 김태경, “청소년 아동보호 표준화”, 정보보호학회지 제23권 제3호, pp.28-31, 2013년.

〈저 자 소 개〉

나 재 훈 (Jae Hoon Nah)
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 전자정보공학과 박사
1987년~현재 : 한국전자통신연구원 사이버보안연구본부 전문위원/책임연구원
2009년~현재 : ITU-T SG17 Q7 Rapporteur
2011년~2012년 : 한국정보보호학회 학회지 편집위원장
관심분야 : IPv6/MIPv6, P2P, IPTV, 웹메시업 보안

이 상 우 (Sang-Woo Lee)
정회원

1999년 2월 : 경북대학교 전자공학과 학사
2001년 2월 : 경북대학교 전자공학과 석사
2009년 2월 : 경북대학교 전자공학과 박사
2001년 1월~현재 : 한국전자통신연구원 사이버보안연구본부 선임연구원
2014년~현재 : ITU-T SG17 editor
관심분야 : 임베디드 보안, 차량통신보안, 융합보안

나 중 찬 (Jung Chan Na)
종신회원

1986년 2월 : 충남대학교 계산통계학과 학사
1989년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과 박사
1989년2월~현재 : ETRI 제어시스템보안연구실실장/책임연구원
관심분야 : 제어시스템보안, 펌웨어 보안 취약성

김 정 녀 (Jeong Nyeo Kim)
종신회원

1987년 : 전남대학교 전산통계학과 졸업
1996년 : OSF/RI 공동연구 파견 (미국)
2004년 : 충남대학교 컴퓨터 공학과 석사, 박사
2005년 : Univ. of Califoria, Irvine Post-Doc.
현재 : 한국전자통신 연구원 사이버보안시스템연구부장 책임연구원
현재 : 과학기술연합대학원대학교(UST) 정보보호공학과 교수
관심분야 : IoT보안, 모바일 보안, 시스템·네트워크 보안, 보안 OS 등

김 태 경 (KIM TAE KYUNG)
종신회원

1997년 2월 : 단국대학교 수학교육과 졸업
2001년 8월 : 성균관대학교 정보통신공학과 공학석사
2005년 8월 : 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2006년 3월~2008년 2월 : 서일대학 정보전자과 교수
2008년 3월~현재 : 서울신학대학교 교양학부 교수, 전산실장
관심분야 : 네트워크보안, USN, 클라우드컴퓨팅, COP