정 보 보 호 학 회 지
제24권 제4호, 2014. 8

보안관리 표준화

오 경 희*, 박 태 완**

요 약

정보보안은 조직의 거버너스와 사회적 책임의 기본적인 구성요소의 하나다. 조직이 정보보안을 구현하고 관리하는 것은 일반적으로 기대되는 관리자의 책임이며, 많은 선진국에서는 투자자와 고객의 이익을 보호하고 안전한 거래 기반을 마련하기 위해 정보의 보안관리에 관한 다양한 법적 규제를 수립하여 강제 또는 권고하고 있다.

이러한 조직의 책임을 지원하고 최적의 실무를 제시하기 위하여 여러 국제기구에서 보안관리 표준화를 진행하고 있다. 보안관리 표준화 분야의 국제 표준화를 주도하고 있는 대표적인 표준화 기구로는 ISO와 ITU-T가 있다. 본 논문에서는 이 두 기구에서 진행되고 있는 보안관리 표준화 동향에 대한 정보를 제공하고자 한다.

Ⅰ. 서 론

정보보안 또는 정보보호란 정보의 기밀성, 무결성 및 가용성을 보존하는 것으로서 때로 인증, 책임추적성, 부인봉쇄, 신뢰성 등을 포함할 수 있다.[1] 정보보안 관리는 조직의 정보를 안전하게 관리하기 위한 조직의 노력과 관리적, 기술적, 물리적 대책들을 포함한다. Information security management는 정보보호관리, 정보보안관리, 정보보안경영 등으로 다양하게 번역되는데, 국제 표준의 최근 KS 번역본에서는 management system은 '경영 시스템'으로, information security는 '정보보안'으로 통일하여 사용하고 있다. 그러나 아직 정보보안 경영이라는 단어가 일반적으로 활용되는 상황은 아니라고 판단하여, 본 논문에서는 정보보안 관리라는 용어를 사용할 것이다.

정보보안은 조직의 거버너스와 사회적 책임의 기본적인 구성요소의 하나다. 조직이 정보보안을 구현하고 관리하는 것은 일반적으로 기대되는 사항이고 때로는 법적인 요구사항이 되기도 한다.[2]

이러한 조직의 책임을 지원하기 위하여 여러 국제 기구에서 보안관리 관련 표준화를 진행하고 있으나, 관리 분야의 표준은 주로 ISO/IEC JTC 1/SC 27/WG 1과 ITU-T SG 17 WG1 Q3에서 진행하고 있다. 본 논문에서는 이들 기구에서 개발 중인 관리 관련 표준화 현황을 간단히 소개하고, 특히 현안이 되고 있는 ISO/IEC 27009, 27011, 27021 표준의 현황을 설명한다.

Ⅱ. 정보보안 관련 국제 표준화 기구 현황

2.1. ITU-T SG 17 WG1 Question 3

ITU-T에서 보안관리 표준을 담당하고 있는 과제 그룹은 Study Group 17의 Working Party 1에 속한 Question 3이다. 축약하여 Q3/17 또는 Q3로도 불리는 이 그룹은 통신 정보보안 관리(Telecommunication information security management)를 다루고 있다.

통신 조직에 있어 정보와 지원 프로세스, 통신 시설, 네트워크 및 전송 매체는 중요한 업무 자산이다. 정보보안 관리는 통신 조직이 이들 업무 자산을 적절하게 관리하고 업무 활동을 정확하게 지속하기 위해 필수적인 사항이다.[3]

이러한 이유로 ITU-T는 통신 조직을 위한 정보보안 관리 지침을 제공하기 위하여 X.1051을 개발하였으며, 이를 기반으로 하여 거버넌스, 관리 프레임워크, 위험, 사고 및 자산의 관리를 위한 상세하고 구체적인 권고들을 개발하고 있다. 또한 클라우드 컴퓨팅, IPv4에서 IPv6로의 전환, 개인식별정보 등의 관리와 같은 새로운 전세계적 대책의 관리에 관련된 사항들 역시 Q3의 연

* TCA서비스 대표
** 한국뷰로베리타스 인증원 ISO27001 선임심사원

구 범위에 포함하여 고려하고 있다.

이 과정에서 ITU-T의 관련 기술 과제 그룹 뿐만 아니라 ISO/IEC JTC1의 여러 부문과 긴밀하게 협력하면서 X.gpim|ISO/IEC 29151, X.1051|ISO/IEC 27011 등을 공동 개발하고 있다. ISO/IEC의 경우 정보보안관리체계 인증 표준을 가지고 있지만, ITU-T는 인증 자체는 업무범위에서 제외하고 관리를 위한 표준만을 개발한다.

2014년 현재 이 그룹이 발행한 권고 및 부록으로는 X.1051, X.1052, X.1054, X.1055, X.1056, X.1057, X.Suppl.13, 및 E.409(SG 2와 공동)가 있으며, 현재 X.gpim 과 X.1051의 개정을 진행중에 있다. Q3의 라포처(Rapporteur)는 일본의 Miho Naganuma가, 부라포처(Associate rapporteur)는 한국의 오 경희가 맡고 있다.

2.2. ISO/IEC JTC1 SC 27/WG 1

ISO에서 보안 및 프라이버시 표준을 다루는 특별위원회(Sub Committee, SC는 IEC와 함께 수립한 공동기술위원회 1(Joint Technical Committee 1) 산하의 SC 27이다. 보안관리 표준은 SC 27 산하의 작업반 1(Working Group 1)이며 WG1의 의장은 영국의 Edward Humphreys가 맡고 있다. WG1에서는 일차적으로 정보보안 관리체계(ISMS) 관련 요구사항, 방법, 절차를 다루며, 이러한 관리체계에서 사용하는 보안 통제, 실무규약, 프레임워크에 관한 표준을 다룬다. 또한 관리체계를 위한 승인, 증명, 감사 요구사항 및 방법에 관한 표준을 포함한다.

WG1이 다루는 표준은 다양한 형태로 존재할 수 있는 정보의 보안에 관한 것이다. 이러한 정보에는 종이로 출력, 기록되거나, 전자적으로 저장되거나, 우편 또는 전자적 수단으로 운송되거나, 필름으로 보여지는 정보 및 대화 중의 정보를 포함한다. 또한 정보 보안 실패로 인해 발생하는 피해를 제한하기 위한 메커니즘 역시 대상이 된다.[2]

WG1은 또한 정보보안의 거버넌스 측면 및 경제적 측면을 다룬다. 프라이버시에 관한 거버넌스 및 경제적 측면은 WG5에서 다룬다는 것이 ITU-T와의 차이점이다. 그래서 ITU-T와의 공동작업은 대부분 WG 1에서 이루어지지만, X.gpim의 경우 프라이버시를 다루기 때문에 WG 5와 공동 작업을 진행하고 있다.

WG1의 표준은 크게 ISMS 관련 표준인 유형 A와 분야별 표준인 유형B의 2가지 유형으로 분류할 수 있다. ISMS 관련 표준인 유형 A에는 용어표준인 27000, 요구사항 표준인 27001, 27006, 27009가 포함되며 ISMS 관련 지침인 27002, 27003, 27004, 27005, 27007, 27008이 포함된다. 분야별 표준인 유형B에는 27010, 27011, 27013, 27014, 27015, 27016, 27017이 포함된다.[4]

Ⅲ. 주요 표준 현황

여기서는 두 표준화 기구에서 현재 진행되고 있는 표준 중 ISO/IEC 27009, ISO/IEC 27011(X.1051), ISO/IEC 27021의 현황에 대해 소개한다. ITU-T SG 17 WP1 Q3에서는 개인정보보호 표준인 X.gpim, 클라우드 관련 표준인 X.cc-control 등에도 관여하고 있으나, 이들은 일반적으로 별도의 분야로 분류되고 있어 소개를 생략한다.

3.1. ISO/IEC 27009

ISO/IEC 27009 Information technology -- Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements[5] 는 정보보호관리체계에 대한 요구사항(인증 표준)인 ISO/IEC 27001의 2013년 버전에 기초하여 개인정보, 통신, 클라우드 등의 특정 영역에서의 인증 요구사항을 설명하기 위한 표준이다. 이 표준은 새로운 인증 기준을 만드는 것이 아니라 ISO/IEC 27001:2013의 요구사항에 더하여 특정 영역에 필요한 추가 요구사항을 포함하는 방법, ISO/IEC 27001:2013의 요구사항을 상세화하는 방법, 그리고 ISO/IEC 27001:2013 부록 A에 통제 또는 통제집합을 추가하는 방법에 대해 설명한다.

이 ISO/IEC 27009가 발표되면 현재 개발이 진행되고 있는 개인정보보호, 통신, 클라우드 분야의 통제집합 표준인 ISO/IEC 29151, ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018 등을 이용한 인증이 가능해지게 되어 많은 국가들의 관심을 받고 있다.

이 표준은 특정 분야의 추가적인 인증 요구사항이 ISO/IEC 27001:2013의 요구사항에 배치되지 않을 것을 요구하며, 기존의 요구사항을 제외시킬 수 없다.

이러한 추가적 요구사항은 ISO/IEC 27001의 요구사

항을 만족하기 위한 특정 접근방법을 포함할 수 있다. 예를 들어 관리체계 내 인력의 자격에 대한 설명을 ISO/IEC 27001의 7절에 포함할 수 있다.

특정 분야의 표준은 ISO/IEC 27001의 요구사항에 대한 해석을 제공할 수 있지만, 마찬가지로 ISO/IEC 27001의 요구사항을 무력화시키거나 ISO 9001과 같은 다른 경영시스템 표준과의 연계를 손상시켜서는 안 된다.

분야별 표준은 해당 분야에 특유한 위험을 처리할 필요가 있을 수 있다. 예를 들어 프라이버시 관련 표준은 프라이버시 원칙에 기초한 “프라이버시 위험관리”가 포함될 수 있고, 위험관리 프로세스에 대한 추가적인 또는 더 상세화된 요구사항이 있을 수 있다. 이러한 사항 역시 ISO/IEC 27001의 위험관리 프로세스에 통합되어야 한다.

또한 ISO/IEC 27001의 부록 A에 포함되는, ISO/IEC 27002 외의 추가적인 분야별 통제 목표, 통제, 구현 지침 등이 포함되어야 한다. 이를 위한 템플릿이 제안된 상태이다.

특정 분야에 대한 인증 요구사항은 많지 않을 것으로 예상되나, 분야별 통제는 많은 표준에서 개발 중에 있다. 이러한 표준들은 ISO/IEC 27002의 구조를 따르고 있었으나 ISO/IEC 27009의 활용을 위하여 표준의 명칭과 통제 번호의 표기 관례가 새롭게 제안되어 통일되고 있다. 즉, ISO/IEC 27009를 활용하기 위한 분야별 표준들의 명칭은 “ISO/IEC 27002에 기반한 ... 분야의 통제”로, 그 표준 내부의 ISO/IEC 27002에 추가되는 통제는 “TEL”, “PRV”, “CLD” 등 각 분야별 약자를 포함하는 번호 체계를 사용하도록 변경되었다.

2014년 7월 현재 현재 표준의 구조가 확정되어 1차 CD가 국가 투표를 위해 회람되고 있는 상태이며, 한국의 박 태완 대표를 비롯하여 일본의 Fuki Azetsu, ISO/IEC 27001의 에디터였던 독일의 Angelika Plate가 에디터를 맡고 있다.

3.2. ISO/IEC 27021

2012년 스웨덴 국가 대표인 Fredrik Björck가 스웨덴의 정보보호관리 전문가에 대한 인증제도 수립을 발표하고, 이에 여러 국가에서 관심을 표명함으로써 International Certification of Information Security Management Specialists에 관한 study period가 개시되었다.

이 SP는 1년간 진행되어 정보보호 전문가에 대한 기존의 국제 자격제도 및 표준 현황을 조사하고 ISO/IEC 27000 시리즈에 기초하여 정보보호관리체계를 구축, 운영하기 위한 전문가 자격제도의 필요성을 조사하였다.

SP 종료 회의에서는 정보보호관리 전문가에 대한 인증 표준의 개발 필요성에 대한 현장 투표가 이루어졌다. 신규 작업 항목 제안에 옵저버로 참석한 ISC2외에는 참여 20개국 및 ISACA까지 모두 찬성 투표를 함으로써 ISO/IEC 27021표준 번호까지 할당되었으나, 최종 ISO/IEC JTC 1 의 결의 단계에서 IEC에서 인력에 대한 신규 인증 스킴의 소유권 문제를 제기함으로써 1년간 SP가 연장되었다.

연장된 SP 과정에서는 ISO와 IEC 각각에서 인증제도를 담당하는 기구인 CASCO(Committee on conformity assessment)와 CAB(Conformity assessment body)이 참여하여, 이러한 신규 인증 제도가 만들어진다면 어떤 기구가 소유권을 가지고 인증 제도를 운영할 것인지, ISO/IEC JTC 1 SC 27/WG 1의 가능한 역할은 무엇인지에 관한 심도있는 토론이 이루어졌다.

최초의 신규 작업 항목 제안은 ISO/IEC 27006과 같은, 정보보호 전문가를 인증하기 위한 요구사항을 개발하는 것이었다. 그러나 이러한 요구사항이 실현되기 위해서는 인증기관 및 인증기관을 인정하기 위한 인정기관의 체계가 필요하며, IEC에서는 이러한 인증 스킴에 관한 문서는 본질적으로 인증기관 또는 인정기관이 개발/참조해야 하는 문서임을 주장하였다.

ISO의 적합성 평가 위원회인 CASCO 가 2012년 발령한 Directive[6] 문서에서는 표준 개발자는 “중립 원칙”에 따라 제1자(제조자 또는 공급자), 제2자(사용자 또는 구매자), 제3자(인증기관과 같은 독립 기관) 모두에게 적용될 수 있는 문서를 개발하도록 하고 있다. 이에 따르면 제3자 기관이 주로 참조하기 위한 인증스킴에 관한 문서는 SC의 개발 범위를 넘어서는 것이다.

IEC CAB은 또한 인증 스킴에는 이를 운영하기 위한 소유자가 필요한데, 이 역할을 누가 맡을 것인지가 정의될 필요를 제시하였다. IEC는 기존 보안에 관련된 인력에 대한 표준 및 인증 스킴을 보유하고 있다며 신규 인증 스킴에 대한 소유권에 관심을 보였다. 그러나 IEC가 소유권을 갖는 인력에 대한 인증 스킴은 폭발성 환경에

서의 인력 적합성 인증(“IECEx Certification of Personnel Competence for Explosive Atmospheres”)에 관한 것으로 정보보안 인력과는 일부 차이가 있는 것으로 보이는 한편, CASCO는 이미 ISMS 심사원에 대한 인증 표준을 보유하고 있지만 직접적으로 인증체계를 운영하고 있지는 않다.

어쨌든 SC 27에서는 인증 스킴에 대한 문제는 ISO/CASCO와 IEC/CAB, 또는 각 국의 인증체계의 결정사항으로 남겨 두고, 제1자, 2자, 3자가 모두 활용할 수 있는 정보보안관리 인력에 대한 국제 표준의 범위에 집중하여 하반기 SP를 진행하였다. 이에 따라 최종 신규작업항목 제안은 “정보보안관리 인력의 자격 요구사항”이라는 제목으로 이루어졌으며, SP 최종 회의에서는 ISC2를 포함한 참석자 전원 찬성으로 통과되었고, 최종 국가 투표가 진행 중에 있다.

이 표준은 정보보안관리 인력의 자격 요구사항을 명세하고 있으므로 제1자인 전문가 및 전문가 양성 교육기관에서도, 제2자인 정부기관, 보안전문회사, 보안직원을 채용하고자 하는 수요기관 등에서도, 그리고 전문가를 인증하기 위한 인증기관과 그 인증기관을 인정하는 인정기관에서 모두 활용할 수 있다.

ISO/CASCO와 IEC/CAB은 이 표준이 발행되고 관련 업계의 반응에 기초하여 스킴 개발을 결정하기로 합의했다. 이런 방식으로 인증 스킴이 개발된다면, 다양한 인증기관이 운영하는 단일 국제 인증 체계가 만들어 질 것이며, 그렇지 않은 경우 각각의 인증기관이 자신의 인증 스킴을 운영할 수도 있다.

한편 IEC/CAB은 6월 운영회의에서 신속한 적합성 수요 대응을 위한 CAB 체계를 전면 개편하고, 사이버보안 분야 적합성 평가 대응을 위한 작업그룹(WG 17)을 신설하였다. 특히 이 신규 제안 관련 적합성 평가 수요에 대해서도 WG 17에서 병행 검토하기로 결의하였다.

ISO/IEC 27021은 SP에서 라포처로 활동한 한국의 오 경희, 일본의 Yonoske Harada와 기존 라포처였던 스웨덴의 Fredrik Björck 대신 영국의 Andreas Fuchsberger가 에디터로 임명되었다. 2014년 10월부터 본격적인 작업이 이루어질 예정이며 2016년 발표를 예정하고 있다.[7]

현재 제안된 신규 표준의 구조는 초기 버전에서 포함된 인증 스킴에 관련된 부분은 모두 삭제되었으며 전문가 자격 영역에 대한 기본 틀만 제시하고 있고, 첨부로 BOK(Body of Knowledge)의 구조를 예시하고 있다.

일본에서는 기 보유하고 있는 정보보안 기술사를 이 표준에 따라 국제 인증을 받고자 노력하고 있다. 일본의 자격 제도는 현재의 국제적인 인력에 대한 자격 기준이 요구하고 있는 재인증 등의 요구사항을 포함하고 있지 않아서 현재의 제도로는 국제 인증을 받을 수 없다. 이에 대응하기 위하여 일본은 SP 기간 동안 재인증을 포함하지 않는 “Qualification” 개념을 신규 자격 표준에 도입하기 위하여 노력하였으나, 여타 국가의 반대로 무산되었다. 현재 신규 표준 항목 제안서에 포함된 첨부는 이러한 일본의 끈질긴 노력으로 일본의 정보보안 기술사의 지식체계가 반영된 것이다. 현재 버전에서는 예시로 포함하였지만 일본은 지속적으로 자신들의 지식 체계를 표준 본문에 반영하기 위하여 노력할 것이며, 이에 대응하여 각 국 역시 자신들의 지식 체계를 제안할 것으로 예상된다.

우리나라의 경우에도 SIS가 변환된 정보보안 기사 자격이 존재하며, 미래창조부의 2013년 정보보호 산업 발전 종합대책에 따르면 2016년 정보보호기술사제도를 시행할 예정으로 있다. 우리나라의 자격제도 역시 일본과 유사하게 재인증을 요구하지 않고 ISO의 기본 인력 자격 기준의 요건을 만족하지 못하므로 우리의 정보보안 기사 또는 앞으로 나올 정보보안 기술사 제도 역시 국제 인증을 받지 못할 가능성이 높다. 단, 국제 자격 기준 표준을 포함하여 기술사 제도를 운영할 수는 있다.

그러나 더 효과적인 것은 우리의 지식 체계를 국제 표준에 반영하는 것이며, 좀 더 나아간다면 우리의 자격 제도가 직접적으로 국제 표준으로 인정될 수 있는 방안을 고민 하는 것이 필요할 것이다. 이를 위해서는 국내의 제도 운영 관계자가 국제 표준화에 능동적으로 참여하여 신규 제도 신설 및 운영에 반영할 필요가 있다.

3.3. ISO/IEC 27011

ISO/IEC 27011[8]은 ITU-T와 공동 개발하는 표준으로써 X.1051과 동일한 문서이다. 원래의 제목은 “Information security management guide- lines for telecommunications organizations based on ISO/IEC 27002”였으나, 앞서 ISO/IEC 27009에서 설명한 바와 같이 특정 분야의 통제 표준들의 표기 관례를 통일하면서 제목이 “Information security control guidelines

based on ISO/IEC 27002 for telecommunications organizations"로 바뀌었다.

이 표준은 기반으로 하고 있는 ISO/IEC 27002가 2013년 개정됨에 따라 개정이 결정되었다.

전체적인 구조는 변경된 ISO/IEC 27002에 기초하여 정보보호 정책에서부터 준거성에 이르기까지의 통제 구조를 따르고 있다. ISO/IEC 27002의 내용은 포함하지 않고 해당 구조에 따라 통신조직에 특유한 구현 지침과 기타 정보가 존재하는 경우 해당 통제 목적과 통제, 그리고 추가적인 통신조직을 위한 구현 지침 및 기타 정보를 제공하고 있다.

또한 부록 A에서는 통신조직을 위한 확장 통제 집합을, 부록 B에서는 추가적인 구현 지침을 제공하고 있다.

통신분야의 확장 통제 집합은 네트워크 접근통제, 물리 및 환경적 접근통제, 통신보안, 준거성 분야에서 13가지의 추가적인 통제를 제시하고 있다. 이들은 다음과 같다.

TEL.9.5.1 사용자에 의한 통신 전송자 식별 및 인증
TEL.11.1.7 통신센터의 보안
TEL.11.1.8 통신장비실 보안
TEL.11.1.9 물리적으로 분리된 운영실 보안
TEL.11.3.1 다른 전송자의 영역에 설치된 장비
TEL.11.3.2 사용자 영역에 설치된 장비
TEL.11.3.3 통신 서비스의 상호 연결
TEL.13.1.4 통신 서비스 제공의 보안관리
TEL.13.1.5 스팸 대응
TEL.13.1.6 DoS/DDoS 공격 대응
TEL.18.1.6 통신의 비밀 유지
TEL.18.1.7 비상 통신
TEL.18.1.8 비상 활동의 적법성

부록 B의 추가적인 구현 지침은 다음과 같다.

B.1 사이버 공격에 대한 네트워크 보안 수단
  a) 네트워크 설비의 보호
  b) 송신자 가장에 대한 방어수단
  c) 통신 서비스 사용자의 주의 환기
B.2 네트워크 정체에 대한 보안 수단
  a) 네트워크 정체를 감지하고 제한하는 메커니즘
  b) 정체를 유발할 수 있는 정보의 사전 수집
  c) 처리량의 임시 개선 수단
  d) 비상 통신의 식별 및 우선 처리
  e) 오작동을 유발할 수 있는 정보의 사전 수집

이 표준은 현재까지 27002에서 신규로 도입된 통제에 관한 검토가 완료된 상황이며, 2014년 4월 ISO 회의에서 구조를 확정하고 1차 CD에 대한 국가 투표가 진행되고 있다. 차기 ITU-T 회의에서는 통신 분야의 확장 통제 집합의 적정성을 검토할 예정이며, 2016년 완료될 예정이다.

스웨덴의 Brian O''Toole, 한국의 오 경희, 일본의 Koji Nakao가 에디터로 활동하고 있다.

Ⅳ. 결 론

지금까지 정보보안 관리 분야의 대표적인 표준화 기구인 ISO/IEC JTC 1/SC 27/WG 1과 ITU-T SG 17/WP 1/Q3의 활동 내역과 현재 진행 중인 정보보안 관리 분야의 대표적인 표준으로서 ISO/IEC 27009와 ISO/IEC 27021, ISO/IEC 27011의 현황을 살펴보았다.

보안관리 분야의 표준들은 기술적인 세부사항은 다루지 않으나 인증 시장과 직접적으로 연관되어 있어 각국의 관심과 견제가 치열한 분야이다. 기술적 정확성보다는 정치적인 요구사항의 합의가 결정적이기 때문에 더 어려운 부분이 있다.

중요 표준에 한국 대표가 에디터로 참여하고 있기는 하지만, 객관성과 중립성을 견지해야 하는 에디터의 입장에서는 자기 국가의 제안에 힘을 실어주기에 한계가 있다. 다만 관련 정보를 얻기에는 에디터의 입장이 유리하므로 일본 등 국제 표준의 중요성을 인식한 국가들은 자국이 에디터를 맡더라도 자국의 의견은 별도의 인원이 참여하여 설명하도록 하고 있다.

타 SC의 경우 회의 결정사항은 국가 별로 1표가 아니라 참석한 전문가 별 1표로 결정하는 경우도 있다고 한다. SC 27은 그런 상황까지는 아니지만, 많은 전문가들이 참여하여 여러 측면으로 지원 발언을 하게 되면 더 그 국가의 주장에 힘이 실리는 경향이 있다. 특히 원어민이 아닌 국가의 경우 언어문제를 극복하고 국가 이익을 관철하기 위해서는 다수의 전문가들의 상호 지원이 필수적이지만, 현재 WG 1의 참여 인원으로는 불가능한 상황이다.

특히 인증 시장에 큰 영향을 미치는 현안이 되는 표준에 대해서는 직간접적 이해당사자들의 의견을 수렴하기 위한 저변 확대와 국내 관련 담당 기관의 직접 참여가 절실하다.

참 고 문 헌

[1] N11903, Information technology – Security techniques – Information security management systems – Overview and vocabulary, 2nd edition, ISO, Dec. 2012.

[2] N11102_WG1_SD1_WG1_Roadmap, ISO, June 2012.

[3] http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q3.aspx

[4] Session 3-1 ISO WG1 ISMS Starndards, E. Humphreys, ETSI – ISO/IEC JTC 1/SC 27 SECURITY WORKSHOP, 26, April 2013.

[5] N13913_Text_1stCD_27009_20140610, ISO, June 2014,

[6] ISO/CASCO, Conformity assessment for standards writers : Do's and dont's, ISO, 2012.

[7] N13911, Proposal for a new work item on Competence requirements for information security management systems professionals, ISO, June, 2014.

[8] N13914, 1st CD of 27011, June, 2014.

〈저 자 소 개〉

오 경 희 (Kyeong Hee Oh)

1988년 8월 : 서강대학교 전산과 졸업
1992년 2월 : KAIST 전산과 석사
현재 : TCA서비스 대표
관심분야 : 정보보호 관리, 아키텍처, 감사

박 태 완 (Taewan Park)

1981. 울산공과대학 전자공학과 전자계산학 전공 졸업
1993. MSc in Information Security, Royal Holloway College, University of London
현재 : 한국뷰로베리타스 인증원 ISO27001 선임심사원(외주)
관심분야 : 정보보호 경영시스템