정 보 보 호 학 회 지
제26권 제4호, 2016. 8

분야별 정보보호 경영시스템 인증 동향

박 태 완*, 오 경 희**

요 약

올 6월 약 4년간의 표준화 활동의 결과로 ISO/IEC 27009 “ISO/IEC 27001의 분야별 응용 – 요구사항”이 국제 표준으로 발표되었다. 이 표준은 ISO/IEC 27001을 어떤 특정 분야에 적용하고자 할 때 필요한 요구사항을 정의한 것으로서, 분야별 정보보호 경영체계 인증제도의 국제적 상호 인정의 기반을 마련하기 위한 것이다.

본 논문에서는 이 표준의 개발 배경, 내용과 의미, 그리고 관련 현황을 소개하고 국내 정보보호 경영시스템 전문가들의 대응 방향을 제시한다.

Ⅰ. 서 론

ISO/IEC JTC 1 SC 27에서는 다양한 분야별 표준이 개발되고 있다. 2014년에는 “퍼블릭 클라우드에서의 개인식별정보 보호를 위한 정보보호통제 실무지침” 27018[1], 2015년에는 클라우드의 정보보호를 위한 27017[2]이 각각 제정되었다. 2016년에는 통신분야 정보보호 경영을 위한 27011[3]이 개정되었으며, 현재 에너지 분야를 위한 27019[4], 개인정보보호를 위한 29151[5] 등이 개발 중에 있다. 이러한 표준들은 ISO/IEC 27002 “정보보호 경영을 위한 실무지침(Code of practice for information security management)”[6]에 기초하여 개발되었다.

한편 ISO/IEC 27001은 Annex A를 참조하도록 되어 있고 이 Annex A는 27002에서 정의한 통제 및 통제 목표를 나열하고 있다. 이에 따라 27002 뿐만 아니라 위에서 설명한 분야별 표준들을 참조하여 정보보호 경영시스템 인증제도를 운영할 수 있도록 하기 위하여 ISO/IEC 27009 “ISO/IEC 27001의 분야별 응용 – 요구사항(Sector-specific application of ISO/IEC 27001 – Requirements)”[7] 개발이 개시되었고. 지난 2016년 6월 15일, 약 4년간의 표준화 활동의 결과로 ISO/IEC 27009 국제표준(International Standard)으로 통과되었다.

ISO/IEC 27009는 향후 정보보호 경영시스템 시장에 매우 중대한 영향을 끼칠 수 있는 중요한 표준이다. 그러나 그 내용은 매우 단순하기 때문에 이에 대한 배경지식이 없는 상태에서 표준만 접할 경우 이해하기 어려운 측면이 있다.

ISO/IEC 27001[8]을 활용하여 특정 분야(산업, 서비스)에 적용한다는 것은 분야별 정보보호 경영시스템에 대한 인증제도를 운영하는 것을 의미한다. 특정 분야의 정보보호 경영시스템에 대한 인증 제도를 운영하고 그것을 ISO/IEC 27001에 기초한 분야별 정보보호 경영시스템 인증으로 국제적으로 상호인정 받기 위해서는 먼저 해당 경영시스템에 대한 표준을 이 표준 문서에서 요구하는 대로 작성해야만 한다는 것이다.

본 논문에서는 이 표준의 개발 배경, 표준의 내용과 의미, 그리고 관련 ISO 표준 개발 현황을 소개한다. 또한 관련 국제 동향을 설명하고 우리의 적절한 대응 방향을 제시한다.

Ⅱ. 개발 배경

2.1. 경영체계와 인증제도

경영시스템(Management System)이란 조직이 정책과 목표 그리고 그 목표를 달성하기 위한 프로세스를 수립하기 위해 필요한, 밀접한 관련을 갖거나 서로 영향을 미치는 요소들의 집합[9]이다. 이러한 요소에는 조직

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (정보보안 경영전문가 자격기준 국제 표준화)
* 시큐리티 인사이드 전문위원, ISO/IEC 27009 에디터, ** TCA 서비스 대표 (khoh@tcaservices.kr), ISO/IEC 27011 에디터

의 구조, 역할 및 책임, 계획, 운영 등이 포함된다. 즉, 기업을 영위하면서 부딪치게 되는 다양한 분야(예; 품질, 환경, 정보보호 등)를 보다 체계적이고, 효과적으로 관리하기 위한 방법론으로서 경영시스템 혹은 관리체계를 수립하게 된다.

그리고 이렇게 효과적으로 관리하고 있다는 것을 고객이나 거래 파트너, 규제기관 등 관련 이해당사자에게 인정받기 위한 방법으로서, 신뢰할 수 있는 제3의 기관(인증기관)으로 부터 인증을 받는 인증제도가 국제적으로 운영되고 있다. 인증제도는 경영시스템에 대한 요구사항을 규정한 표준 문서에 기초하여 그 요구사항들이 준수되고 있음을 인증기관의 심사원을 통해 확인하고 인증서를 발급함으로써 이해당사자들에게 신뢰를 제공한다. 정보보호 분야에서 국제적으로 인정받고 있는 인증 제도로는 ISO/IEC 27001 표준에 기초한 인증이 있으며, 국내에는 KISA가 운영하는 정보보호관리체계 인증제도가 있다.

국제적으로 상호인정될 수 있는 인증제도를 운영하기 위해서는 그 인증에 필요한 경영시스템에 대한 요구사항들이 국제 표준으로 만들어질 필요가 있다.

2.2. 정보보호 경영시스템 인증 관련 ISO/IEC 표준

ISO/IEC 27001은 정보보호경영시스템을 수립, 구현하고, 유지하여 지속적으로 개선하기 위해 필요한 요구사항들을 정의한 국제표준이다. 여기서 “요구사항”(requirements)이란 제3자에 의한 인증 심사의 기준이 되는 항목을 의미한다.

ISO/IEC 27001 표준 문서는 “요구사항”과 “부록(Annex)” 2개의 부분으로 구성되어 있다. 요구사항에는 모든 경영시스템에 공통적으로 적용되는 공통 구조에 기초하여, 정보보호 경영시스템에 대한 요구사항들이 기술되어 있다.

서로 다른 분야의 경영시스템이 한 조직 내에서 충돌없이 효과적으로 운영되도록 하기 위해 2015년 이후에 개정된 대부분의 경영시스템은 ISO에서 이미 개발한 공통 구조와 문구를 사용하도록 요구하고 있다. 정보보호 분야만이 아니라 품질, 환경 등 타 분야의 경영시스템 요구사항 역시 동일한 구조를 따름으로써 경영진 등 관련자들의 이해를 돕고 구현 및 운영을 용이하게 하도록 지원하기 위한 것이다.

Annex는 효과적인 정보보호 활동에 필요한 14개 분야 114개의 통제항목(대응책)이 기술되어 있다. 이들 통제항목은 ISO/IEC 27002 “정보보호 경영을 위한 실무지침(Code of practice for information security management)”에서 가져온 것이다.

ISO/IEC 27002 “정보보호 경영을 위한 실무지침(Code of practice for information security management)”은 정보보호와 관련된 위험(Risk)이 발견되었을때 이 위험에 대응하기 위한 대응책들을 통제항목(control)이라는 이름으로 기술하고 있는 문서다. 즉 효과적인 정보보호 활동에 필요한 최적 실무(best practice)를 제시하고 있다.

처음 27002표준 문서가 개발될 당시에 제안된 통제항목들 중 대부분은 특정 분야나 서비스에 상관관계 없이 모두 효과적인 정보보호 활동에 공통적으로 필요한 통제항목으로 선정되어 27002에 포함, 기술되었다. 그러나 일부 통제항목들은 특정 분야나 서비스에서만 적용되거나 법, 제도적으로 특정 서비스에 한하여 효과적인 대응책으로 판단되는 것들이 있었으며, 최근 클라우드, 빅데이터, IoT등 새로운 분야가 대두되면서 이들 분야에서 필요한 통제항목들이 새로이 제시되었다.

따라서 각 분야에 필요한 통제항목들에 대한 최적 실무의 개발 요구가 발생하게 되었다. ISO에서는 각 분야별 정보보호 경영 지침을 효과적으로 관리하기 위하여 이미 27002에 기술되어 있는 통제항목에 대해서는 필요한 경우 27002의 통제에 대하여 분야별 구현 지침을 추가하고, 27002에 기술되어 있지 않지만 해당 분야에 꼭 필요한 통제항목들은 별도의 부록 A에서 기술하는 방식으로 별도의 표준 문서들을 만들기로 합의하였다. 이 결정에 의하여 통신 분야에서는 27011, 의료정보 분야에서는 27799[10], 클라우드 환경에 대해서는 27017과 27018등이 개발되었다.

2.3. 분야별 인증제도

정보보호 분야에는 ISO/IEC 27001 인증 뿐만 아니라 유사한 성격의 인증 제도들이 지난 10여년 동안 지속적으로 만들어져 운영되고 있다. 대표적으로 국내에서는 KISA에서 운영하는 정보보호 관리체계 인증제도, 개인정보보호 관리체계 인증제도, 클라우드 보안인증제도가 운영되고 있다. 또한 독일도 자국의 기준에 기초한

IT 정보보호 인증제도를 운영하고 있다.

또한 특정 분야 인증제도의 예로는 클라우드 분야에서는 수년전에 CSA(Cloud Security Alliance)에서 만든 기준과 ISO27001을 함께 사용하여 “STAR” 인증제도[11]가 만들어졌다. 이 STAR 인증은 중국의 클라우드 서비스 제공자에 대한 인증서 발행을 시작으로 확산되고 있다.

각 국의 법 제도 및 문화에 기초한 인증제도는 자국에 적합한 최적 실무나 해당 국법에 따른 운영 여부를 확인하기 위해 필요할 수 있다. 다만 이러한 경우 해당 국가를 넘어선 거래에서의 안전성에 대한 신뢰에 대해서는 약간의 우려가 있는 것이 현실이다. 국제적 상호 인정을 위해서는 국제 표준에 기초한 인증제도가 아무래도 좀 더 유리할 수밖에 없으며 이것이 ISO/IEC 27001 인증이 국제적인 영향을 미치는 이유가 되고 있다.

이렇게 ISO/IEC27001과 특정 산업분야의 최적 실무(예; 27011, 27017, 27018 등)를 통합하여 해당 산업 혹은 분야에서 요구하는 정보보호 활동이 효과적으로 이루어지고 있음을 인증하기 위한 제도의 필요성이 높아지고 있다. 또한 이러한 제도가 세계적으로 상호 인정되기를 바라는 요구도 증가하였다. 이러한 배경에서 ISO/IEC 27009의 개발이 개시되었다.

Ⅲ. ISO/IEC 27009: 2016

ISO/IEC 27009는 정보보호 경영시스템에 대한 요구사항(인증 표준)인 ISO/IEC 27001의 2013년 버전에 기초하여 개인정보, 통신, 클라우드 등과 같은 특정 영역에서의 정보보호 경영시스템 요구사항을 문서화 하는 방법을 기술하는 표준이다. 즉 이 표준만으로는 분야별 인증을 개시할 수 없으며, 분야별 인증에 필요한 정보보호 경영시스템 요구사항은 27009가 제시하는 규칙에 따라 별도로 만들어져야 한다.

27009는 전체가 11 페이지, 실제 내용은 9페이지에 지나지 않는 최소한의 내용만을 담고 있는 문서다. 그러나 표준 문서의 길이가 짧아도 필요한 내용들은 모두 기술되어 있다

27009는 크게 2가지 사항을 기술하고 있다. 첫번째는 ISO/IEC 27001의 요구사항 부분에 대하여 관련 분야의 요구사항을 “추가(addition)”, “정교화(refine), 또는 “해석”(interpretation) 하는 방법, 두 번째로는 기존

〔표 1〕 ISO/IEC 27009 목차

ISO/IEC 27001의 부록 A에 있는 통제항목을 “수정(modify)” 하거나 해당 산업의 통제항목을 “추가(addition)”하는 방법을 기술하고 있다.

또한 부록 A에서는 이 표준에 따라 분야별 정보보호 경영시스템 요구사항 표준을 작성할 때 사용할 수 있도록 템플릿을 제공하고, 기존 ISO/IEC 27001의 내용과 추가, 정규화, 해석 또는 수정된 내용이 분명히 구분되도록 각 항목의 특성에 따른 서식을 규정하고 있다. 이해를 돕기 위하여[표 1]에서 ISO/IEC 27009의 목차를 보였다.

ISO/IEC 27001의 부록 A, ISO/IEC 27009의 부록 A, 다른 분야별 정보보호 통제 실무지침, 앞으로 만들어질 분야별 정보보호 경영시스템 요구사항 표준들의 부록 A는 그 특성이 매우 다르다. ISO/IEC 27001의 부록 A는 ISO/IEC 27002에서 나온 통제목표 및 통제의 집합이다. 앞서 언급한 현재까지 개발된 27011 등 분야별 정보보호 통제 실무지침들의 부록 A는 ISO/IEC 27002에 포함되지 않은, 해당 분야에서 필요한 새로운

〔표 2〕 ISO/IEC 27009 부록 A 목차

부록 A(정규)

ISO/IEC 27001:2013 또는 ISO/IEC 27002:2013에 관련된 분야별 표준의 개발을 위한 템플릿

A.1. 내용의 기안(Drafting instructions)

A.2. 템플릿
0. 개요
1. 범위
2. 필수적 참조
3. 용어 및 정의
4. ISO/IEC 27001에 관련된 <XX>-분야별 요구사항
   4.1 이 표준의 구조
   4.2 <XX>-분야별 요구사항
   4.3 27001 요구사항 또는 27002 통제의 확장
5. ISO/IEC 27002에 관련된 <XX>-분야별 지침

부록 <XX>-분야별 참조 통제 목표 및 통제

통제 항목들이다. 이러한 통제항목들은 기존의 27002의 통제항목과 구분하기 위하여 각 분야를 나타내는 3개 문자로 이루어진 접두사를 붙이고 통제 번호를 붙인다. 예를 들어 통신분야는 TEL.X.X.X, 클라우드는 CLD.X.X.X, 개인정보는 PRI.X.X.X 등으로 표시된다. ISO/IEC 27009의 부록 A는 분야별 정보보호 경영시스템 요구사항 표준의 템플릿이다. 이해를 돕기 위하여 [표 2]에 ISO/IEC 27009의 부록 A의 목차, 즉 분야별 정보보호 경영시스템 요구사항 표준의 목차를 보였다. 목차의 <XX> 표시는 분야 명으로 대체된다. 예를 들어 "<XX>-분야별 요구사항"은 해당 분야가 통신이라면 "<통신>-분야별 요구사항"으로 대체하라는 의미이다.

이러한 추가적 요구사항은 ISO/IEC 27001의 요구사항을 만족하기 위한 특정 접근방법을 포함할 수 있다. 예를 들면, 관리체계 내 인력의 자격의 명시가 필요한 경우 그에 대한 설명을 ISO/IEC 27001의 7절에 포함시킬 수 있다.

이 표준은 특정 분야의 추가적인 인증 요구사항이 ISO/IEC 27001:2013의 요구사항에 배치되지 않을 것을 요구하며, 기존의 요구사항을 제외시킬 수 없다. 또한 ISO 9001과 같은 다른 경영시스템 표준과의 연계를 손상시켜서는 안된다. 즉 추가, 정교화, 해석, 수정 등 어떠한 경우에도 기존의 ISO/IEC 27001의 요구사항의 수준을 낮추는 것은 금지하고 있다. 새로운 인증제도가 효과적인 정보보호에 도움이 되지 못한다거나 인증 획득이 상대적으로 용이하다는 인식이 나타나는 것은 ISO/IEC 27001에 따른 인증 제도에 부정적인 영향을 끼친다고 보고 이를 사전에 차단하기 위한 것이다.

Ⅳ. 향후 동향 및 대응 방안

ISO/IEC에서는 ISO/IEC 27009의 이러한 특성에 따라 27009 개발이 마무리되어 가는 2015년 하반기부터 "27009 활용 방안(Use case of 27009)" 사전 연구(Study period)를 개시하였다. 이 사전연구는 1) 27011에 기초한 분야별 요구사항 표준을 개발하기 위해 27009를 활용, 2) 27002에 기초한 분야별 정보보호 통제를 위한 표준을 개발하기 위해 27009를 활용, 3) 27001과 27002에 기초한 요구사항 및 통제를 포함하는 분야별 표준을 개발하기 위해 27009를 활용하는 것을 내용으로 하여 1년 기간으로 진행되고 있다.[12]

이에 대하여 독일은 보안 수준이 높은(high) PKI(public key infrastructure, 공개키 기반구조)의 인증기관을 위한 인증기준 개발 의견을 제시하였으며, ISO/IEC 27010 "분야 간 및 기관 간 통신을 위한 정보보안 관리(information security management for inter-sector and inter-organizational communications"을 27009 요구사항에 따라 응용하는 방법에 대한 문서도 제시되었다. 또한 일본에서는 ISO/IEC 27017을 기반으로한 클라우드 인증표준에 대한 필요성을 제기하였다.[13]

4월 회의에서는 이러한 요청을 검토하고, 특히 ITU-T와 공동 개발한 ISO/IEC 27011(통신)과 ISO/IEC 27017(클라우드)의 경우 ITU-T가 인증을 다루지 않으므로 ISO에서 독자적인 진행이 필요함을 확인하였다. 이 두 표준에 대한 27009 응용은 한국과 일본에서 주도적으로 참여하여 차기 회의에서 인증기준화에 관한 논의를 계속하기로 하고, 이렇게 개발된 표준의 경우 지속적 개선을 위해 SD(standing document)로 운영하는 방안에 대해 논의하였다.

특히 관심이 많이 나타나고 있는 분야별 표준은 클라

우드 분야로서 클라우드 서비스 제공자들이 이해당사자로서 클라우드 보안인증제도 높은 관심을 보이고 있다. 또한 일본의 경우 올 8월 경 27001에 기초한 클라우드 서비스 인증제도 수립 개시를 발표한 상태[14]이며, 한국은 27001에 기반하지는 않았지만 자체 클라우드 인증제도를 수립[15]한 상황에서 그 경험을 국제 표준 개발에 반영할 수 있을 것으로 기대된다.

한편 개인정보보호 분야에서도 현재 개발 중인 PIA 표준(29134)[16]과 통제 표준 29151에 기초하여 개인정보보호 경영시스템 요구사항에 대한 표준의 제안을 한국을 중심으로 준비하고 있다.

이와 같이 27009의 활용을 통하여 27001만으로는 충분하다고 느끼지 못하는 각 산업 분야에서 분야별 인증 기준을 개발하려는 노력은 계속될 것으로 예상되며, 국제적으로 확산되고 있는 시장에서는 이러한 분야별 국제인증을 통하여 시장 점유율을 향상시키고자 하는 기업들이 경쟁적으로 인증 획득에 나설 가능성이 높다. 대표적으로 클라우드의 경우 마이크로소프트가 관련 국제표준 개발에 적극적으로 참여하고 있어 세계 최초의 국제 표준에 따른 인증 획득을 노리고 있다는 루머가 돌고 있다.

이슈가 되고 있는 이러한 분야들은 시장이 전세계적으로 형성되고 있어 이들 분야에서의 국제 인증이 개시되면 실질적으로 큰 영향을 미칠 것으로 생각된다. 향후 빅데이터나 IoT 분야의 정보보안 표준이 본격적으로 개발되면 이에 기초한 인증표준도 검토될 수 있을 것이다.

국내의 많은 전문가들이 이러한 국제 표준 개발에 적극적으로 참여하고 있으나, 그에 비해 이러한 변화에 대한 국내 산업계의 전반적인 대응은 미흡한 부분이 있는 것으로 보인다. 국내에는 이러한 표준 및 제도의 개발과 운영에 대한 노하우가 많이 쌓여 있어서 국제 표준 개발 참여의 기반으로 작용하지만, 거꾸로 이러한 국제 표준이 국내 기업의 국제적 인증 및 비즈니스 활성화 기반으로 잘 활용될 수 있는 준비가 이루어지고 있는지에 대해서는 의문점이 있다. 이는 국제표준화 활동이 참가자 개인의 노력에 의존하고 제도적 협력체계와 연결되지 못하고 있는 현실에 따른 문제점이다. 우리의 기술이 국제표준에 반영되는 것은 국제표준 요구사항의 만족 가능성을 높이긴 하지만, 국내 인증제도가 국제표준을 만족하는 것으로 인정되는 것은 또 다른 문제다. 여기에는 실질적인 기술적 내용보다는 제도 운영 기관의 정책결정이 더 크게 작용하게 된다.

인도가 미국의 콜센터나 IT outsourcing을 운영하면서 ISO/IEC 27001인증을 가장 많이 획득하는 국가가 된 사실은 잘 알려져 있다. 국내 기업들이 국제적으로 상호인증이 가능한 인증을 획득함으로써 정보가 동일한 수준으로 보호됨을 인정받는 경우 해외 비즈니스에 많은 도움이 될 것이다. 자국 내 인증제도 운영을 통해 국내 정보와 조직을 보호하는 긍정적 측면이 있는 한편 해외 시장 진출에는 명확한 한계가 존재한다. 이러한 장점을 보존하고 한계를 극복하기 위해 국제적인 동향 정보를 공유하고 국내 인증제도 이해관계자들이 모여서 상호 인정 방안을 적극적으로 검토할 수 있는 기반이 마련되어야 할 것이다.

Ⅴ. 결 론

지금까지 ISO/IEC 27009 국제 표준을 중심으로 정보보호 경영시스템 인증에 관련된 국제 표준들과 동향을 살펴보았다.

ISO/IEC 27009는 장기간에 걸친 정보보호 경영시스템의 분야별 분화를 반영한 결과물이고 이에 따라 앞으로 국제적인 정보보호 경영시스템 시장에 큰 영향을 끼칠 것으로 예상된다. 분야별 인증 제도가 운영되기 위해서는 27009만으로는 부족하고, 분야별 요구사항 표준의 개발과 이를 이용하여 인증서를 발행하는 인증기관이 필요하다. 그러나 분야별 인증 요구사항 표준 개발의 노력들은 이미 동시 다발적으로 이루어지고 있으며 기반이 되는 표준들은 이미 개발되었거나 개발 중에 있다. 또한 기존 ISO/IEC 27001 인증기관들은 이미 만들어진 인증제도 하에서 새로운 통제항목과 구현지침에 기초한 심사 방법만 추가적으로 습득하면 되기 때문에 ISO/IEC 27009에 기초한 분야별 인증은 매우 빨리 개시되고 확산될 수 있을 것으로 예상된다.

국내 기관과 기업들도 이러한 동향을 파악하고 대응방안을 마련하여 국제 시장의 변화에 신속히 대응할 수 있는 역량을 확보하여야 할 필요가 있다.

참 고 문 헌

[1] ISO/IEC 27018:2014 Information security – Security techniques – Information security

management systems – Code of practice for Information security controls based on ISO/IEC 27002 for protection of personally identifiable information (PII) in public cloud acting as PII processors, ISO, 2014

[2] ISO/IEC 27017:2015 Information security – Security techniques – Information security management systems – Code of practice for Information security controls based on ISO/IEC 27002 for cloud services, ISO, 2015

[3] ITU-T X.1051|ISO/IEC 27011:2016 Information security – Security techniques – Information security management systems – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunication organizatons, ISO, 2016

[4] ISO/IEC TR 27019:2013 Information security – Security techniques – Information security management guidelines on ISO/IEC 27002 for process control systems specific to the energy utility industry, ISO, 2013

[5] ISO/IEC DIS 29151, Information security – Security techniques – Information security management systems – Code of practice for personally identifiable information protection, ISO, 2016

[6] ISO/IEC 27002:2013, Information security – Security techniques – Information security management systems – Code of practice for information security controls, ISO, 2013

[7] ISO/IEC 27009:2016, Information security – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements, ISO, 2016

[8] ISO/IEC 27001:2013, Information security – Security techniques – Information security management systems – Requirements, ISO, 2013

[9] ISO/IEC 27000:2016 Information security – Security techniques – Information security management systems – Overview and vocabulary, ISO, 2016

[10] ISO/IEC 27799:2016 Health informatics – Information security management in health using ISO/IEC 27002, ISO, 2016

[11] CSA Security, Trust & Assurance Registry (STAR) : Cloud Security Alliance, https://cloudsecurityalliance.org/star/

[12] Terms of reference for the study period on development use case examples for the application of ISO/IEC 27009, ISO, 2015

[13] Results of the expert CfC for the SP on the Development of Use Case Examples for the Application of ISO/IEC 27009, ISO, 2016

[14] ISMSクラウドセキュリティ認証に關する說明會資料, http://www.isms.jipdec.or.jp/seminar/cloud/shiryou20160426.html

[15] “KISA, 클라우드서비스 정보보호 수준 평가·인증한다”, 보도자료, KISA, 2016

[16] ISO/IEC DIS 29134, Information technology – Security techniques – Privacy impact assessment – Guidelines, ISO, 2016

〈저자소개〉

박 태 완 (Taewan Park)
1981년 : 울산공과대학 전자공학과 전자계산학 전공 졸업
1993년 : MSc in Information Security, Royal Holloway College, University of London
현재 : 시큐리티 인사이드 전문위원
ISO27001 선임심사원, 중앙대학교 융합보안학과 객원교수
<관심분야> 정보보호 경영시스템

오 경 희 (Kyeong Hee Oh)
1988년 8월 : 서강대학교 전산과 졸업
1992년 2월 : KAIST 전산과 석사
현재 : TCA서비스 대표, 고려사이버대학 겸임교수, ITU-T SG17 Q3 Associate rapporteur
<관심분야> 정보보안경영, 아키텍처, IT 감사, 거버넌스, 통제