산업통상자원부 MINISTRY OF TRADE, INDUSTRY & ENERGY

보 도 자 료

희망의 새시대 http://www.motie.go.kr

2013년 10월 22일(화) 조간부터 보도하여 주시기 바랍니다.

문의: 정보통신표준과 박인수 과장(509-7262), 채경수 연구관(509-7264)

정보보안관리체계(ISMS) 국제표준 2.0 시대 예고

- 인천 송도에서 국제표준화기구(ISO) 정보보안기술분과 작업반(WG) 회의 개최 -

☐ 급증하는 사이버 공격에 대한 효과적인 조직적 대응 체계를 제공하는 국제표준화기구(ISO)의 정보보안관리체계(ISMS) 버전 2.0(2013년도 판)이 발표된다.

* ISMS Information Security Management System(ISO/IEC 27001(요구사항), 27002(실행지침))
** ISO International Organization for Standardization

☐ 산업통상자원부 기술표준원(원장: 성시헌)은 국제표준화기구(ISO)의 정보보안기술분과위원회(JTC 1/SC 27) 5개 워킹그룹 회의가 10월 21일부터 10월 25일까지 인천 송도컨벤시아에서 개최된다고 밝혔다.

○ 우리나라에서 세번째로 개최되는 정보보안기술분과위원회는 미국, 영국, 독일 등 34개국 200명의 표준전문가가 참여하여 조직 및 개인의 정보보호 관리체계에 대한 국제표준 안건을 처리할 예정이다.

☐ 이번 회의에서는 2005년도에 1.0 버전으로 발간된 정보보안관리체계(ISMS) ISO/IEC 27001(요구사항)과 27002(실행지침) 국제표준에 대해 지난 3여 년간의 개정 작업을 통해 '조직의 외주관리통제 및 운영 보안통제' 등을 새롭게 추가한 2.0 버전(2013년 판)을 발표하며 더욱 강화된 정보보안관리체계(ISMS) 시대를 시작하는 중요한 회의가 될 것으로 보인다.

○ 또한 암호 알고리즘의 안전성과 성능, 암호모듈 검증 및 시험평가, 침해사고 대응 및 개인정보보호 체계 등 주요 정보보안 이슈 전반에 관한 75개 국제표준 프로젝트가 진행된다.

○ 특히 우리나라는 개인정보보호, 보안 사고관리, 생체인식 기반 개인인증 및 산업별 ISMS 인증 등 7명의 국내 전문가가 각각의 프로젝트에 에디터로 참여하여 국제표준 개발을 주도하고 있다.

☐ 이번 회의에서 우리나라는 정보보안 분야의 "아동보호를 위한 연령검증" 방법 및 "암호모듈 인증절차" 등 2개의 프로젝트를 신규로 제안할 예정이다.

* 아동보호를 위한 연령검증 방법: 글로벌 기준의 위해정보 차단 및 인터넷 중독 예방효과
** 암호모듈 인증절차: 암호모듈 검증에 대한 정책 투명성 확보와 프로세스 개선으로 정보보호제품 검증업체의 시간과 비용 절감 기대

☐ 아울러, 각국 전문가가 참석하는 공식적인 워킹그룹 회의 외에도 일반인들이 참석 가능한 공개 워크숍(SC 27 & Cyber World Workshop, 10.25)이 병행될 예정이다.

○ 이번 워크숍에는 정보보안기술분과위원회(JTC 1/SC 27) 위원장 등 국내외 표준전문가가 참여하여 사이버 세상에서의 보안과 암호화 기술표준 체계에 대한 발표와 토론이 진행될 예정으로 관심있는 일반인들의 참여가 가능하다.

☐ 지식산업표준국 김정환 국장은 "더욱 확대되고 고도화 되고 있는 사이버 공격 수법이 개인 정보유출은 물론 기업 및 국가 기간전산망까지 마비시킬 정도로 영향을 미치고 있는 바, 이러한 위협으로부터 안전한 사이버 세상이 이루어 질 수 있도록 새롭게 발간된 ISO의 정보보안관리체계 2.0 확산에 주력해 나갈 것"이라고 밝혔다.

OPEN 공공누리 공공저작물 자유이용허락

이 보도자료와 관련하여 보다 자세한 내용이나 취재를 원하시면 산업통상자원부 정보통신표준과 채경수 연구관(☎ 02-509-7265)에게 연락주시기 바랍니다.

[붙임]

주요안건 개요

☐ 한국제안 기술

번호	표준번호	표준명	비고(에디터)
1	ISO/IEC 27009	섹터/서비스별 제3자 인증을 위한 27001의 사용과 적용	박태완대표 (JS시큐리티)
2	ISO/IEC 27021	정보보안관리 전문가 인증 요구사항	오경희대표 (TCA서비스)
3	ISO/IEC 18033-3	암호알고리즘: 블록 암호	이필중교수 (포항공대)
4	ISO/IEC 27035-3	침해사고 대응 및 운영지침	전상훈박사 (기재부)
5	ISO/IEC 29151	개인정보보호를 위한 지침	염흥렬교수 (순천향대)
6	ISO/IEC 29134	개인정보 영향 평가 방법론	
7	ISO/IEC 17922	바이오메트릭 하드웨어 모듈을 이용한 인증 프레임워크	전명근교수 (충북대)
8	'13 NP 제안	운영시 암호모듈 인증절차	최희봉박사 (ETRI)
9	'13 NP 제안	온라인상의 어린이를 보호하기 위한 연령 검증	나재훈박사 (ETRI)

☐ 정보보안관리체계(ISMS) 2.0 주요 내용

o 정의: 기업에 적합한 정보보안를 제공하기 위해 정책 및 조직을 수립하고 위험관리, 대책구현, 사후관리 등의 정보보안 관리과정을 통해 여러 정보보안대책들이 유기적으로 통합되어 구현, 운영되는 체계

o 주요 개정내용

- 본문에 정보보안 뿐만아니라 품질 등 앞으로 모든 경영시스템에 공통적으로 적용되어야 하는 부분에 개정

- 기술의 발달로 인한 새로운 분야를 추가하고, 통제항목들을 보다 체계적으로 단순화하여 기업들이 효과적인 정보보안 관리가 이루어질 수 있도록 개정

* 12개 통제분야 133개 통제항목 → 14개 통제분야 114개 통제항목

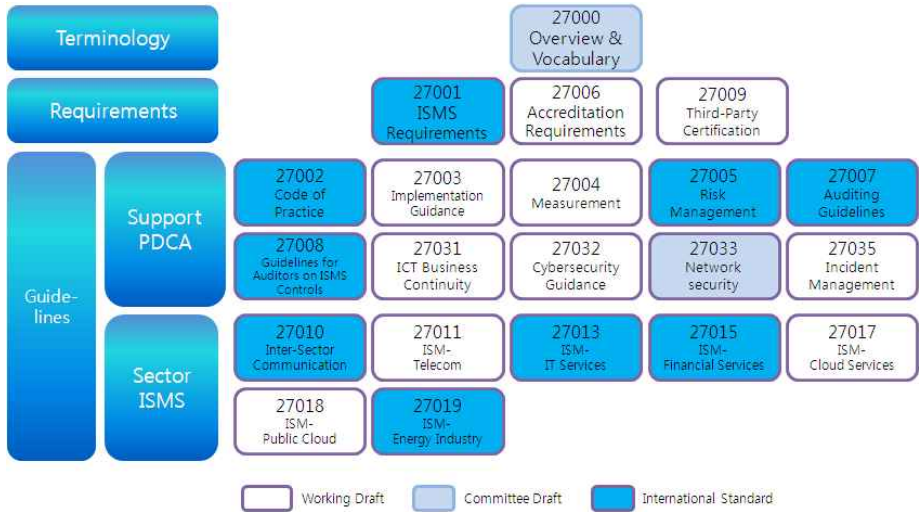
< ISMS 버전별 통제항목 비교 >

ISO/IEC 27001:2005 1.0	
통제분야	통제항목수
정보보안 정책	2
정보보안 조직	11
자산 관리	5
인적자원 보안	9
물리적 및 환경적 보안	13
통신 및 운영 관리	32
접근 통제	25
정보시스템 취득, 개발 및 유지보수	16
정보보안 사고 관리	5
업무연속성 관리	5
준수	10
합계	133

▶

ISO/IEC 27001:2013 2.0	
통제분야	통제항목수
정보보안 정책	2
정보보안 조직	7
자산 관리	10
인적자원 보안	6
물리적 및 환경적 보안	15
통신 보안	7
접근 통제	14
정보시스템 취득, 개발 및 유지보수	13
정보보안 사고 관리	7
업무연속성 관리	4
준수	8
공급자 관계	5
암호 통제	2
운영 보안	14
합계	114

< ISMS 관련 표준 체계 및 작업(안) >



[붙임]

ISO/IEC JTC 1/SC 27 워킹그룹 회의일정

회의명	인원	10.21 (월)	10.22 (화)	10.23 (수)	10.24 (목)	10.25 (금)
WG 1(정보보안관리시스템) Plenary	**53**					
WG 1(A) 27001(정보보안관리체계 요구사항), 27002(실행지침), 27003(구현지침), 27004(효과성 측정), 27006(인정 요구사항), 27009(서비스분야별 제3자인증)	40					
WG 1(B) 27019(에너지산업 정보보안관리), 27016(정보보안 경제학), 27017(클라우드 서비스 보안지침), 27018(공공클라우드 서비스 데이터 보안지침), 27011(텔레컴 정보보안관리)	27					
WG 2(암호 및 보안 메카니즘) Plenary	**27**					
WG 2(A) 11770-3(비대칭 기법 메카니즘), 18367(암호 알고리즘 적합성 평가), 20009-2(그룹 공개키 서명 메카니즘)	30					
WG 2(B) 18033(암호알고리즘), 10118-1(해쉬함수), 18014-1(타임스탬핑 서비스), 18370(익명 디지털 서명)	15					
WG 3(보안평가기준) Plenary	**19**					
WG 3(A) 24759(암호모듈 평가요구사항), 15408(IT 보안성 평가기준), 18045(IT 보안성 평가 방법론)	22					
WG 3(B) 301104(물리적 보안 요구사항), 15443(IT보안성 보증 프레임워크), 15446(정보보호제품 사용자의 보안요구 사항)	21					
WG 4(보안 통제 및 서비스) Plenary	**44**					
WG 4(A) 27033-1(네트워크 보안 지침), 27033-2(네트워크 보안 설계 및 구현 지침), 27033-3(리스크, 설계, 기술 및 통제 이슈 참조모델)	32					
WG 4(B) 27035-1(침해사고 관리 원칙), 27035-2(침해사고 대응 계획 및 준비 지침), 27035-3(침해사고 대응 운영 지침)	31					
WG 5(ID관리 및 개인정보 보호기술) Plenary	**32**					
WG 5(A) 24760-2(ID 관리 프레임워크-참조 아키텍처 및 요구사항), 24760-3(실행지침), 29101(프라이버시 아키텍처 프레임워크), 29146(접근관리 프레임워크), 17922(바이오 하드웨어 보안 모듈의 원격바이오 인정 프레임워크)	27					
WG 5(B) 27018(공공 클라우드 컴퓨팅 서비스용 데이터 보호 관리 실행지침), 29134(프라이버시 영향 평가), 29190(프라이버시 영향 평가 모델), 29151(PII 보호용 실행지침)	27					
SC 27 HoD 회의	**70**					

[붙임]

SC 27 & 사이버 세상 워크숍

o 일시/장소 : '13.10.25(일) 14:00~18:0 / 송도 컨벤시아 1층

시 간	주요내용
14:00~14:15 (15분)	**오프닝 및 SC27 소개**
	(Walter Fumy (Chair), Marijke de Soete (Vice-Chair), Edward Humphreys (PR))
14:15~15:00 (45분)	**사이버세상에서 거버넌스, 리스크와 적합성**
	ISMS and Cyber World - Edward Humphreys (WG1 Convenor)
	Cyber Policy and Strategy in Thailand and SC27 Standards - Prinya Hom-anek(Thailand)
	Sector-Specific Certifications in Cyber World - Taewan Park (JS Security, Korea)
15:00~15:45 (45분)	**암호와 사이버 세상**
	ISO Crypto-standards and Cyber World - Takeshi Chikazawa (WG2 Convenor)
	SC27 standards for digital signatures and entity authentication mechanisms - Pil Joong Lee (Postech, Korea)
	Status and Issues of PKI Implementation: Korean Case – . Soontae Park (Korea Information Security Agency, Korea)
15:45~16:00 (15분)	Coffee Break
16:00~16:45 (45분)	**사이버세상 제품과 시스템**
	WG3 mission and standards - Naruki Kai (WG3 Vice-Convenor)
	Challenges and Needs in Testing and Evaluation of Cyber-World Products - Miguel Bañnóon (WG3 Convenor)
	Korea's Certification Scheme and Use Cases of SC27 Standards for IT Security Products Evaluation – Soohyun Lee (Wins TechNet, Korea)
16:45~17:30 (45분)	**보안 서비스와 사이버 세상**
	Security services standards - Johann Amsenga (WG4 Convenor)
	Incident Management - Geoff Clarke
	Incident Response for Cloud Computing Security – Sanghoon Jeon (Ministry of Strategy and Finance, Korea)
17:30~18:15 (45분)	**사이버 세상에서 프라이버시와 ID 관리**
	Standards for identity management and privacy - Kai Rannenberg (WG5 Convenor)
	How to use the Privacy Standards from SC 27/WG 5 - Dan Bogdanov
	Status and Issues of Information Privacy: Korean Cases of PIMS, PIA and Best Practices – Jongmin Ko (National Information Society Agency, Korea)
18:15~18:30 (15분)	**CLOSING REMARK**

[붙임]

ISO/IEC JTC 1/SC 27(정보보안기술) 개요

□ 개 요

o 설립/명칭 : 1990년 / IT Security Techniques(정보보안기술)

o 의장·간사국 : 독일(의장 Mr. W. Fumy, 간사 Ms. K. Passia)

o 참여국

- P멤버(50) : 미국, 프랑스, 영국, 독일, 캐나다, 중국, 한국, 일본 등
- O멤버(18) : 헝가리, 인도네시아, 이란, 터키, 포르투갈 등

□ 조직구성

