스마트의료보안 표준화 현황

한근희 _ 스마트의료보안포럼 의장,
건국대학교 정보통신대학원 정보보안학과장

1. 머리말

국내 1차, 2차, 3차 의료기관 대부분에서 정보통신기술(ICT, Information Communication Technology)을 활용하여 병원정보시스템(EMR, Electronic Medical Record), 의료영상저장전송시스템(PACS, Picture Archiving and Communication System), 처방전달시스템(OCS, Order Communication System) 등 다양한 의료정보를 가공·처리하는 컴퓨터시스템을 활용하고 있다.

의료기관에서 ICT가 적극 활용되어 의료시스템, 의료기기, 개인건강기기 등이 의료 네트워크에 연결되고, 외부 인터넷을 통해 의료 서비스가 제공됨에 따라, 사이버 위협·공격 등의 가능성이 매우 높아지고 있다. 특히 최근에는 의료기관을 대상으로 랜섬웨어 등의 공격을 통해 의료기관이 보유하고 있는 의료 정보를 망가뜨린 후(해커가 보유한 암호키로 환자 의료정보를 암호화하여 진료·치료와 관련된 정보를 알 수 없게 함) 금전을 요구하는 사례가 부쩍 늘고 있다.

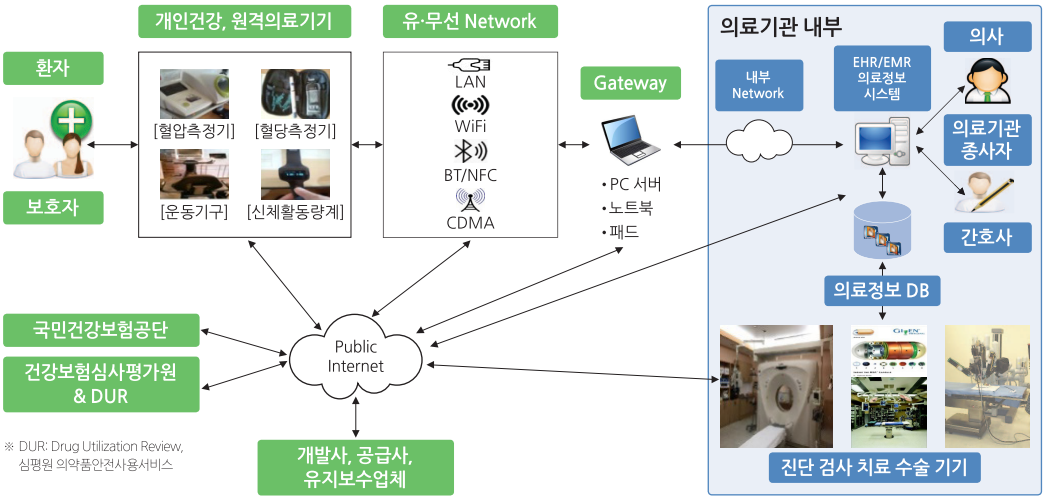
의료 관련 전체를 표현한 [그림 1]에서 화살표는 모두 취약한 부분으로, 환자부터 의료기관, 의료종사자까지 전 분야에서 취약한 접점과 요소 등을 나타내었다.

사이버보안 위협과 공격을 예방하고 대응하기 위해서 국내에서도 「정보통신망법」에 의해 모든 상급종합병원은 '정보보호 및 개인정보보호 관리체계 인증(ISMS-P)'을 의무적으로 받도록 개정·시행되고 있으며, 대형 의료기관 위주로 정보보호팀이 창설되고 있는 추세이다.

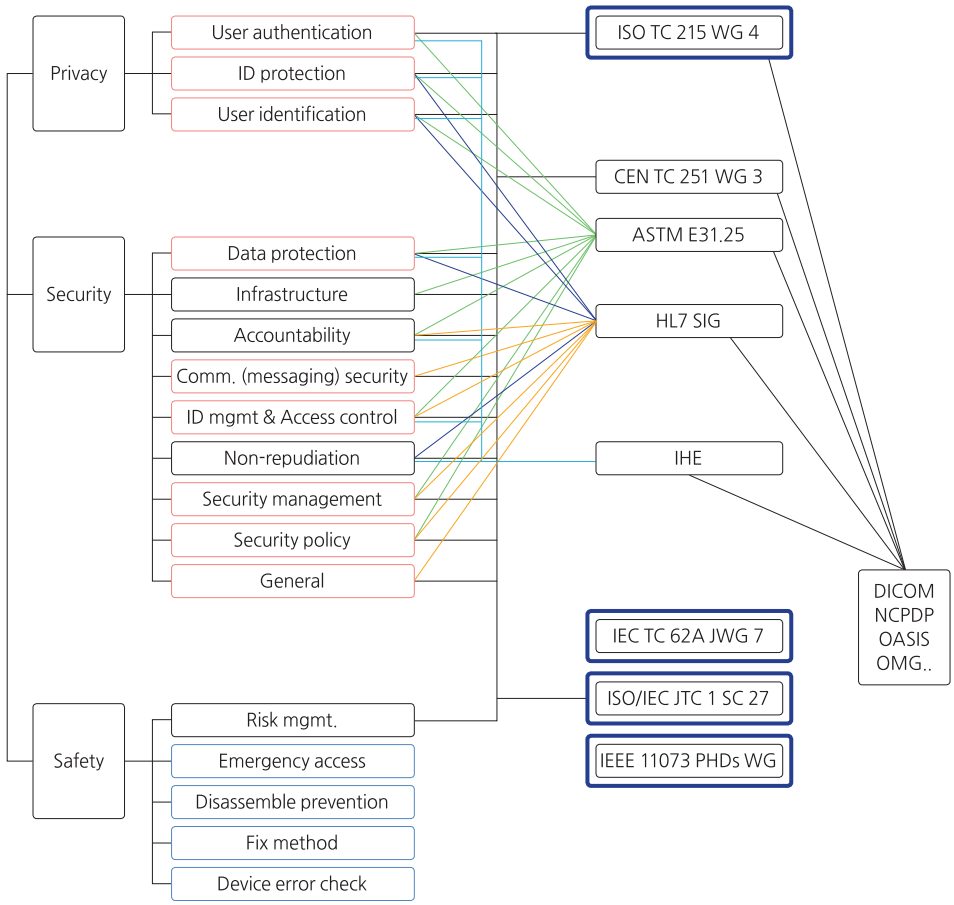
본고에서는 의료분야에서 사이버보안 위협과 공격을 예방하고 대응하기 위해서 필요한 정보보호와 개인정보보호 등에 대한 국제표준화 동향을 살펴본다.

2. 의료보안 관련 국제표준화 단체

의료 분야와 관련된 국제표준화 단체는 국제표준화기구(ISO, International Organization for Standardization), 국제전기표준회의(IEC, International Electrotechnical Commission, 미국전기전자학회(IEEE, Institute of Electrical and Electronics Engineers) 등이 있다.



[그림 1] 의료정보 수집, 저장, 이용 과정과 취약 요소



[그림 2] 의료보안 관련 국제표준기구

일반적인 정보보호와 개인정보보호는 ISO/IEC JTC 1 SC 27의 WG 1~5에서 다룬다.

2.1 ISO TC 215 WG 4

ISO TC 215 보건의료정보 기술위원회(Technical Committee 215 Health Informatics)는 의료서비스 제공기관에서 다뤄지는 다양한 의료관련 메시지를 전자적으로 공유할 수 있도록 의료정보 분야에 대한 국제적 표준을 개발하고 있다.

정보보호 관련해서 WG 4 Security, Safety and Privacy 보안 및 정보보호 작업그룹에서 〈표 1〉과 같은 표준들을 개발하였고, 일부 문서들은 한글 부합화 작업을 거쳐 국가기술표준원으로부터 국가표준(KS) 문서로 등록되어 있으며, 현재도 다양한 보안 표준들을 개발 중에 있다.

이외에도 다양한 의료보안 표준문서가 존재할 수 있으니, 관련 사이트를 면밀하게 살펴보는 것이 필요하다.

<표 1_①> ISO 의료보안 표준문서 현황

No.	표준문서 제목
1	· ISO 27799:2016 Health informatics - Information security management in health using ISO/IEC 27002(영문) · KS X ISO 27799 보건의료정보 - 의료기관 정보보호관리체계(국문)
2	· ISO 27789:2013 Health informatics - Audit trails for electronic health records · KS X ISO 27789 보건의료정보 - 전자건강기록을 위한 감사 추적
3	· ISO 22857:2013 Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health data · KS X ISO 22857 보건의료정보 - 개인건강 정보의 국가간 교류를 위한 정보보호 안내서
4	· ISO 22600-1:2014 Health informatics - Privilege management and access control - Part 1: Overview and policy management · KS X ISO/TS 22600-1 보건의료정보 - 특권 관리 및 접근 통제 - 제1부: 개요 및 정책 관리
5	· ISO 22600-2:2014 Health informatics - Privilege management and access control - Part 2: Formal models · KS X ISO/TS 22600-2 보건의료정보 - 특권 관리 및 접근 제어 - 제2부: 형식 모델
6	· ISO 22600-3:2014 Health informatics - Privilege management and access control - Part 3: Implementations
7	· ISO/HL7 27931:2009 Data Exchange Standards - Health Level Seven Version 2.5 - An application protocol for electronic data exchange in healthcare environments · KS X ISO/HL7 27931 보건의료정보 - 자료교환 표준 - HL7 v2.5 - 보건의료환경에서의 전자자료교환을 위한 응용프로토콜
8	· ISO/TR 27809:2007 Health informatics - Measures for ensuring patient safety of health software · KS X ISO/TR 27809 보건의료정보 - 보건의료 소프트웨어의 환자 안전 보장을 위한 방안
9	· ISO/TS 25237:2017 Health informatics - Pseudonymization · KS X ISO/TS 25237 보건의료정보 - 가명화
10	· ISO/TS 25238:2007 Health informatics - Classification of safety risks from health software · KS X ISO/TS 25238 보건의료정보 - 의료 소프트웨어로 인한 안전 위험의 분류
11	· ISO/TS 13606-4:2009 Health informatics - Electronic health record communication - Part 4: Security · KS X ISO/TS 13606-4 보건의료정보 - 전자건강기록(EHR) 통신 - 제4부: 보안
12	· ISO/HL7 21731:2014 Health informatics - HL7 version 3 - Reference information model - Release 4 · KS X ISO/HL7 21731 보건의료정보 - HL7 버전 3 - 참조정보모델 - 릴리즈 4
13	· ISO/TR 21548:2010 Health informatics - Security requirements for archiving of electronic health records - Guidelines · KS X ISO/TR 21548 보건의료정보 - 전자건강기록의 보관을 위한 보안 요구사항 - 지침

<표 1_②> ISO 의료보안 표준문서 현황

No.	표준문서 제목
14	· ISO/TS 21547:2010 Health informatics - Security requirements for archiving of electronic health records - Principles · KS X ISO/TS 21547 보건의료정보 - 전자건강기록 보관을 위한 보안 요구사항 - 원칙
15	· ISO/TR 21089:2004 Health informatics - Trusted end-to-end information flows · KS X ISO/TR 21089 보건의료정보 - 신뢰성 있는 종단간 정보흐름
16	· ISO/TS 13606-4:2009 Health informatics - Electronic health record communication - Part 4: Security · KS X ISO/TS 13606-4 보건의료정보 - 전자건강기록(EHR) 통신 - 제4부: 보안
17	· ISO/TR 11633-1:2009 Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis
18	· ISO/TR 11633-2:2009 Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 2: Implementation of an information security management system (ISMS)
19	· ISO/TR 11636:2009 Health Informatics - Dynamic on-demand virtual private network for health information infrastructure
20	· ISO/TS 14441:2013 Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment
21	· ISO 17090-1:2015 Health informatics - Public key infrastructure - Part 1: Overview of digital certificate services
22	· ISO 17090-2:2015 Health informatics - Public key infrastructure - Part 2: Certificate profile
23	· ISO 17090-3:2015 Health informatics - Public key infrastructure - Part 3: Policy management of certification
24	· ISO 17090-4:2014 Health informatics - Public key infrastructure - Part 4: Digital Signatures for healthcare documents
25	· ISO 17090-5:2017 Health informatics - Public key infrastructure - Part 5: Authentication using Healthcare PKI credentials
26	· ISO/TR 17791:2013 Health informatics - Guidance on standards for enabling safety in health software
27	· ISO/TR 18638:2017 Health informatics - Guidance on health information privacy education in healthcare organizations

2.2 IEC TC 62/SC 62A JWG 7

IEC TC 62/SC 62A Common aspects of electrical equipment used in medical practice에서 시스템, 장비, 부속품, 개념, 용어, 정의 및 기호를 포함하여 의료 행위에 사용되는 전기 장비의 제조, 설치 및 적용의 일반적인 측면에 관한 국제 표준을 개발하고 있다.

JWG 7(Joint ISO/TC 215-IEC/SC 62A WG: Application of Risk Management to Information Technology(IT) Networks Incorporating Medical Devices) 의료기기 통신 위험관리 작업그룹에서 ISO TC 215 WG 4 보안 작업그룹과 협업으로 의료기기 보안 관련해서 〈표 2〉와 같은 표준들을 개발하였고, 일부 문서들은 한글 부합화 작업을 거쳐서 국가기술표준원으로부터 국가표준(KS) 문서로 등록되어 있으며, 현재도 다양한 보안 표준들을 개발 중에 있다.

이외에도 다양한 의료기기 보안 표준문서가 존재할 수 있으니, 관련 사이트를 면밀하게 살펴보는 것이 필요하다.

<표 2_①> IEC 의료기기보안 표준문서 현황

No.	표준문서 제목
1	· ISO/IEC 13485:2016 Medical devices - Quality management systems - Requirements for regulatory purposes
2	· ISO/IEC 14971:2007 Medical devices - Application of risk management to medical devices
3	· IEC 60601-1:2018 - Medical electrical equipment - Part 1: General requirements for basic safety and essential performance · IEC 60601-1:2012 제3.1판 의료기기의 전기·기계적 안전에 관한 공통기준 및 시험방법
4	· IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety related-system
5	· IEC 61508-1: General requirements
6	· IEC 61508-2: Requirements for E/E/PE safety-related systems
7	· IEC 61508-3: Software requirements
8	· IEC 61508-4: Definitions and abbreviations
9	· IEC 61508-5: Examples of methods for the determination of safety integrity levels
10	· IEC 61508-6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
11	· IEC 61508-7: Overview of techniques and measures
12	· ISO 62304:2007 Medical device software -nSoftware life cycle processes
13	· ISO 62304-1: Scope.
14	· ISO 62304-2: Normative references.
15	· ISO 62304-3: Terms and definitions.
16	· ISO 62304-4: General requirements.
17	· ISO 62304-5: Software development process.
18	· ISO 62304-6: Software maintenance process.
19	· ISO 62304-7: Software risk management process.
20	· ISO 62304-8: Software configuration management process.
21	· ISO 62304-9: Software problem resolution process.
22	· IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities
23	· IEC/TR 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples · KS X IEC/TR 80001-2-1 의료기기가 통합된 IT네트워크에 대한 위험 관리의 적용 - 제2-1부: 단계별 의료용 IT 네트워크 위험관리 - 실제적용과 사례
24	· IEC/TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the communication of medical device security needs, risks and controls · KS X IEC/TR 80001-2-2 의료기기가 통합된 IT네트워크에 대한 위험 관리의 적용 - 제2-2부: 의료기기의 보안요구사항, 위험, 통제에 대한 공개 및 통신을 위한 지침
25	· IEC/TR 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks · KS X IEC/TR 80001-2-3 의료기기가 통합된 IT네트워크에 대한 위험 관리의 적용 - 제2-3부: 무선 네트워크에 대한 지침

<표 2_②> IEC 의료기기보안 표준문서 현황

No.	표준문서 제목
26	· IEC/TR 80001-2-4:2012 Application of risk management for IT-networks incorporating medical devices - Part 2-4: General implementation guidance for Healthcare Delivery Organizations · KS X IEC/TR 80001-2-4 의료기기가 통합된 IT네트워크에 대한 위험 관리의 적용 - 제2-4부: 적용지침 - 의료서비스 기관에 대한 일반 구현 지침
27	· IEC/TR 80001-2-5:2014 Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance for distributed alarm systems
28	· ISO/TR 80001-2-6:2014 Application of risk management for IT-networks incorporating medical devices - Part 2-6: Application guidance - Guidance for responsibility agreements
29	· ISO/TR 80001-2-7:2015 Application of risk management for IT-networks incorporating medical devices - Application guidance - Part 2-7: Guidance for healthcare delivery organizations(HDOs) on how to self-assess their conformance with IEC 80001-1
30	· IEC/TR 80001-2-8:2016 Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
31	· IEC/TR 80001-2-9:2017 Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities

<표 3> IEEE 의료기기보안 표준문서 현황

No.	표준문서 제목
1	· ISO/IEEE 11073-20601:2016/Cor 1:2016 Health informatics - Personal health device communication - Part 20601: Application profile - Optimized exchange protocol - Technical Corrigendum 1 · KS X ISO/IEEE 11073-20601 보건의료정보 - 개인건강기기 통신 - 제20601부: 응용 프로파일 - 최적화된 교환 프로토콜
2	· ISO/IEEE 11073-30200:2004/Amd 1:2015 Health informatics - Point-of-care medical device communication - Part 30200: Transport profile - Cable connected - Amendment 1 · KS X ISO 11073-30200 보건의료정보 - 현장진료용 의료기기 통신 - 제30200부: 전송 프로파일 - 연결된 케이블

2.3 IEEE PHD Cyber Security WG

IEEE 11073 series에서는 다종 다양한 의료기기들에 대한 표준을 개발하였는데, 최근 별도로 의료기기 사이버보안 작업그룹(PHD Cyber Security WG)을 구성하여 보안 표준문서를 개발 중이다.

PHD Cyber Security WG 개인건강기기 사이버보안 작업그룹에서 의료기기 정보보호 관련해서 〈표 3〉과 같은 표준을 개발하였고, 일부 문서들은 한글 부합화 작업을 거쳐서 국가기술표준원으로부터 국가표준(KS) 문서로 등록되어 있으며, 현재도 다양한 보안 표준들을 개발 중에 있다.

이외에도 다양한 의료기기보안 표준문서가 존재할 수 있으니, 관련 사이트를 면밀하게 살펴보는 것이 필요하다.

3. 맺음말

보건의료분야에서 생성되는 개인정보 및 의료정보의 경제적 가치와 의료기관 대상 사이버공격의 높은 수익성으로 인하여 DDoS 공격이나 랜섬웨어와 같

은 사이버보안 침해 사건이 꾸준한 증가세를 보이고 있다.

환자의 개인 정보, 질병 정보뿐만 아니라 유전자 정보 등과 같이 매우 민감한 정보를 클라우드 환경에서 취급한다는 점에서 이용자들의 불안감이 높은 실정이다. 이에 따라 점차 고도화·지능화되고 있는 사이버공격에 적절히 대응하고 의료정보에 대한 이용자들의 신뢰성을 확보하기 위하여 의료정보보호 체계 및 개인정보보호 대책수립의 필요성이 중요하게 제기되고 있다.

[참고문헌]

[1] 의료보안 표준, 한근희, 2018 스마트의료보안 컨퍼런스, 2018.6.29.

[2] 보건의료정보표준, 사회보장정보원, https://www.hins.or.kr/EgovPageLink.do.

[3] ISO, http://www.iso.org/

[4] IEC, http://www.iec.ch/

[5] IEEE 11073 PHD Cybersecurity WG.

[주요 용어 풀이]

- 병원 정보 시스템(HIS, Hospital Information System): 병원의 전반적인 관리 업무를 전산 시스템으로 자동화한 시스템. 병원의 인사 관리 및 급여 관리, 환자의 외래와 입·퇴원 관리, 의료 수가 관리, 급식 관리, 병원의 시설 및 의료 장비 관리 등 그 속성상 병원의 종사자를 위한 시스템이다. 따라서 사무 자동화(OA)와 아울러 경영 정보 시스템(MIS)의 구축에 필요한 여러 기법과 기술들이 적용된다.
- 의료 영상 저장 전송 시스템(PACS, Picture Archiving And Communication System): 의료 영상을 기존 필름 대신에 디지털 형태로 저장하고 통신망을 통해 의료진들에게 전송하는 장치. X선 컴퓨터 단층 촬영(CT), 자기 공명 화상법(MRI) 등의 단층 진단 시스템이나, 핵 의학 진단 시스템, 초음파 진단 시스템 등으로 촬영한 화상을 광디스크 등 대용량 파일의 데이터베이스로 저장하여 고속의 통신망을 통해 검색하고 전달받는다. 크게 영상 획득 장치(Image Acquisition System), 데이터베이스를 포함한 영상 저장 장치(Database and Storage/Archive Devices), 영상 출력 장치(Display Devices, Workstations, Printer) 및 이들을 연결해 주는 통신망(Network and Communications) 등으로 구성된다.
- 처방 전달 시스템(OCS, Ordering Communication System): 의료 기관에서 컴퓨터망을 통해 의사의 처방을 각종 진료 지원부에 전달함으로써 진료 및 처방에 소요되는 시간을 대폭 줄이고, 처방 내역을 컴퓨터에 저장해 두고 환자 진단 시에 이를 손쉽게 조회할 수 있어 진료의 질을 높일 수 있는 의료 정보 시스템이다.
- 국제 표준화 기구(ISO, International Organization for Standardization): 국제적으로 통일된 표준을 제정함으로써, 상품과 서비스의 교역을 촉진하고 과학·기술·경제 전반의 국제 협력 증진을 목적으로 하는 국제기구. 1926년에 각국의 주요 표준화 단체에 의해 결성된 ISA(International Federation of National Standardizations)의 업무를 계승하여 1947년에 설립되었다. 비조약 기구로 정부의 연합체는 아니지만, 각국을 대표하는 1개의 표준화 기관만이 의결권을 갖는 회원이고 기타 기관은 참관인(옵서버)으로 가맹하고 있다. 회원의 70% 이상이 정부 기관 또는 법률에 의해 설치된 표준화 기관이다. ISO는 창설 이래 19,500건 이상의 광범위한 분야의 국제 표준을 제정, 공표했다. 1960년에는 TC 97(컴퓨터 및 정보 처리 기술 위원회)을 설치하여 데이터 통신과 정보 처리 분야의 국제 표준화를 추진해 왔는데, 가장 대표적인 업적은 개방형 시스템 간 상호 접속(OSI) 모델의 표준이다. 국제표준화기구(ISO)는 국제전기통신연합(ITU)과 긴밀한 연락 관계를 유지하면서 전기 통신 표준화에도 참여하고 있다. 1987년에는 ISO의 TC 97과 국제전기기술위원회(IEC)의 TC 83(정보 기기)의 활동 분야가 중복되는 점을 고려하여, 이들 두 전문 위원회를 합병한 ISO/IEC JTC 1을 설치하여 정보 기술의 국제 표준화를 합동 관리하고 있다. ISO에는 JTC 1 이외에도 TC 46(정보 및 문서화), TC 68(은행 업무), TC 130(그래픽 기술), TC 184(공장 자동화 시스템) 등 정보 처리 관련 전문 위원회가 있다. ISO는 전문 위원회(TC)에서 작성한 국제 표준 원안을 ISO 회원 75% 이상의 찬성 투표로써 국제 표준(IS)으로 확정한다. 이렇게 제정된 국제 표준은 ISO 646(정보 교환용 부호), ISO 8802(LAN) 등과 같이 표기되어 공표된다. (ISO http://www.iso.org/)
- 국제 전기 표준 회의(IEC, International Electrotechnical Commission): 동의어 국제 전기 기술 위원회. 전기, 전자 및 관련 기술 분야의 비영리 국제 표준화 기관. 각국을 대표하는 표준화 기관으로 구성되어 있다. 1904년 미국 세인트루이스에서 개최된 국제 전기 회의에서 전기 기기에 관한 용어와 규격의 표준화 필요성이 제창되어 1906년 영국 런던의 회의에서 13개국이 참가하여 IEC를 발족시켰다. IEC도 국제 표준화 기구(ISO)와 마찬가지로 의결권을 갖는 회원은 1국가 1단체 또는 기관으로 국한되어 있다. 전문 분야별로 기술 위원회(TC), 분과 위원회(SC), 또는 작업 그룹(WG)을 설치하고 IEC 국제 표준(IEC Publication)을 작성, 발표하여 각국에서 국가 표준을 정할 때에 통일된 표준을 준거하도록 권고하고 있다. 1961년에는 TC 83(정보 기기) 등을 설치하여 정보 기술 분야의 표준화를 추진해 왔는데, ISO와 TC

97(컴퓨터와 정보 처리)의 활동 분야와 중복되는 점을 감안하여 ISO와 합의하여 두 TC를 합병한 ISO/IEC JTC 1을 설치하여 합동으로 정보 기술 분야의 표준화를 추진하고 있다. (http://www.iec.ch/)

- 미국 전기 전자 학회(IEEE, Institute of Electrical and Electronics Engineers): 세계 최대의 전기, 전자, 전기 통신, 컴퓨터 기술 분야의 비영리 단체. 1884년에 설립된 미국 전기 학회(AIEE, American Institute of Electrical Engineers)와 1912년에 설립된 무선 학회(IRE, nstitute of Radio Engineers)가 1963년에 IEEE로 합병하여 설립되었다. 미국뿐만 아니라 전 세계 각국의 학자와 전문 기술자 등 수십만 명이 가입하고 있는 전문가 단체이다. 주요 활동은 전기, 전자 공학, 전기 통신, 컴퓨터 공학 등의 교육과 표준화 및 기술 진보이다. IEEE 산하에는 통신 학회(IEEE Communications Society), 컴퓨터 학회(IEEE Computer Society) 등 수십 개의 분야별 학회가 있어 이들 산하 학회의 하부 기술 위원회를 통하여 주요 활동이 이루어진다. IEEE는 아이트리플이(eye-triple-ee)라고 발음한다.