제18차 IMDRF-DITTA 합동 온라인 워크숍 주요내용

❑ 회의개요

○ **일　시** : 2020.09.21.(화), 20:00~23:00

○ **목　적** : 사이버보안(Cybersecurity)

❑ 주요 내용

○ IMDRF-DITTA ‘사이버보안’ 주제의 공동워크숍

1. IMDRF 사이버보안 실무그룹

- 현재까지의 업무 진행 내용

  · 사이버보안 가이던스 올 초에 발간하였으며, 의료기기 전주기(시판 전/후)에 해당하는 내용임

  · 의료기기 사이버보안의 일반적인 원칙과 모범사례에 대한 기본적인 개념과 고려사항을 제공하여 글로벌 규제 통합을 촉진시키기 위한 목적으로 개발되었으며 소프트웨어 탑재된 의료기기, 소프트웨어 단독 의료기기(SaMD)가 사이버보안 범위에 해당됨

  · 공개의견 수렴 및 반영하여 발간

  · [공개의견 수렴 내용]

  (1) 용어를 일관성있게 사용

  (2) 이해당사자의 역할과 책임을 명확히 함

  (3) 사이버 보안의 범위 수정도 함

  (4) 정의(definition) 명확화 위해 추가, 삭제, 수정함

  (5) 사이버보안 위험 관리 vs 안전성 위험 관리

- 레거시 디바이스 관련하여 의견 수렴한 내용을 바탕으로 내용을 일부 수정하고 명확히 함
  - 레거시 디바이스는 현재의 사이버보안 위협에 취약한 기기를 의미하며, device age(기기의 연식)는 레거시 디바이스로 결정짓는 sole determinant 아님
  - 연식이 오래되었다고 해도 앞으로의 사이버보안 위협으로부터 보호받을 수 있는 능력이 있는 기기는 레거시 아님
- 레거시 디바이스 구상 체계
  - 개발에서 시판 이후 성능저하(end of life date)까지 사이버보안으로부터 보호를 받을 수 있으며 제조자는 end of life 이후에는 제한된 지원을 제공한다는 것에 대한 공지를 이용자에게 정확히 할 필요가 있으며, 지원 종료 시점부터 legacy로 구분함. 이 구상 체계는 아직 실현된 것은 아니며 현재 구상 중임

2. 캐나다의 사이버보안 관련 규제

- 사이버보안 명칭의 규정은 따로 없으며 시판전/후 규제를 적용
- Health Canda에 2018년 Digital Health Division 설치하여 의료기기 소프트웨어, 인공지능 적용된 의료기기, 사이버보안 능력 강화 가능한 기기 등을 규제함
- 사이버보안 능력을 키우고 잘 규제하기위해 산업계, 정부 등의 이해당사자 대상으로 ‘18년 이후 사이버보안 인식 캠페인 실행하였으며, 이 캠페인을 통해 PAN Canadian Government Council 설치하게 되었으며 설비, 비즈니스, 의료기기 등 분야에 걸친 사이버보안 문제 해결을 하고 있음
- Health Canada는 또한 Advisory Committee를 소집하여 회의 개최를 하며 참여 위원들은 Health Canada에 과학적, 임상적 증거를 제공하며, 의료기기 사이버보안 관련 위원회를 통해 산업계와의 비공개 회의를 개최하여 좋은 의견을 들을 수 있었음

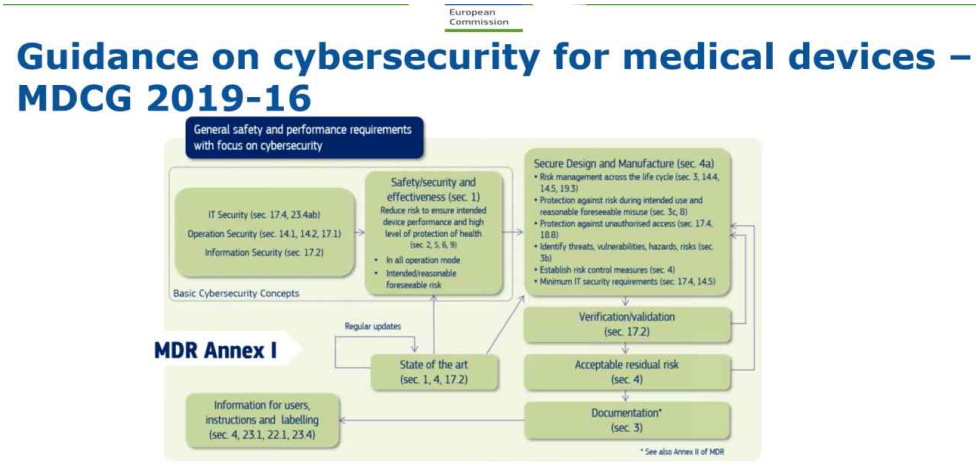
- 2019년 6월, Premarket Requirement 가이드라인을 발간하였으며 의료기기 시판전 평가 시, 위험통제(Risk Control)를 평가요소에 넣는 것이 이 가이드라인의 핵심 내용임. Risk Control에는 Design, Risk Management, Risk Control이 포함됨
- Health Canada는 안전성에는 해를 주지 않으면서 보안은 최대로 강화할 수 있는 것을 목표로 하고 있으며 이를 위해 planning과 사이버 보안 문제 대응에 대한 지속적 모니터링을 평가함. (예: Usability)

3. EU의 사이버보안 관련 규제

- EU의 의료기기 새 규정이 2017년 채택되었으며, 코로나 사태로 인해 MDR 적용은 '21년, IVDR은 '22년으로 연기됨
- 새 규정을 통해 기대하는 바
  - 소프트웨어 적용 의료기기와 소프트웨어 단독 기기를 포함한 모든 종류의 의료기기에 대한 안전성 강화 기대가 높아지고
  - 의료기기 새 분류체계, 특히 소프트웨어 의료기기에 대한 분류체계 마련
  - 시판후 감시 강화 요건 마련
  - 위험관리 요건 마련
  - 의료기기의 전주기 관리 강화 등
- IMDRF 실무그룹 활동 참여뿐만 아니라 소프트웨어 의료기기, 사이버 보안과 관련한 업무가 진행되고 있으며 전문가 그룹을 구성하여 논의하고 있음. 특히 이 전문가 그룹은 지난 몇 년간 제조업체에게 소프트웨어 의료기기의 요건, 임상평가, 의료기기의 사이버보안에 대한 가이던스 제공하고있음. EU가 이 가이던스를 발행했으며 MDCG 2019-16로 알려져있음.
  - 가이던스는 크게 새 규정의 두 가지 개정사항을 설명하고 있으며,

    ① 사이버보안에 적용가능한가 ② 개정사항에 사이버보안 관련 요건을

어떻게 설명하고 있는지, 그 요건에 부합하기위해서는 어떻게 해야 하는지를 설명하고 있음



- MDCG 2019-16의 사이버보안 관련 기본 컨셉을 설명하는 표이며, 이 프로세스는 전주기에 해당하는 것이며 계속해서 업데이트 예정
- 앞에서 설명한 개정사항의 핵심 사항을 Security risk vs Safety related risk를 통해 설명.
- 보안 관련 위험사항, 안전성 관련 위험사항이 무엇인지 설명하며, 겹치는 부분은 예를 들어, unauthorized access를 통해 security risk가 어떻게 safety related risk로 바뀌는지를 설명함
- 기기의 설계(design) 단계에서부터 사이버보안을 고려한다면 관련 문제를 쉽게 해결할 수 있으며 전주기적 접근 방식으로 접근해야 발생한 문제에 대한 적절한 대응을 할 수 있음.
- Post-market surveillance and vigilance: 의료기기에 전주기적 접근방식을 실행해야하며 특히 시판후 감시가 이루어져야함
- 사이버보안은 대형업체에게만 발생하는 것이 아니라 중소기업, 병원, 모든 관계자에게 발생 할 수 있다는 것을 인지하고 환자의 안전성을 보장하기 위해서 risk-based 접근방식을 채택해야함.

4. 일본의 사이버보안 관련 규제

- 의료기기 사이버공격에 따른 위험사항
- 진단 중지 또는 오진단 (예: 테스팅 또는 진단 시스템이 공격 받았을 경우)
- 치료 중단 (예: 치료기기가 공격 받았을 경우)
- 과도한 또는 불충분한 방사선 (예: 방사선 치료 시스템이 공격 받았을 경우)

=> 이러한 위험성 피하기 위해서 MHLW는 '18년 7월 발간한 가이던스를 통해 일본 의료기기 제조업체에 사이버보안 위험성을 적절히, 잘 평가하라고 요청함

- IMDRF 사이버보안 가이던스 발간된 이후 MHLW는 제조업체와 기타 이해당사자들에게 IMDRF 가이던스를 '20년 5월에 행정통보 형식으로 안내하였으며 이를 통해 의료기기 사이버보안을 강화하고 일본의 의료기기 안전을 개선할 수 있게 됨
- IMDRF 가이던스 실행 방법을 제조업체, 보건(의료)종사자들과 논의하였으며, 의료기기 사이버보안 강화하기 위해 IMDRF 가이던스 실행을 어떻게 할 것인지를 관련 이해당사자들과 향후 몇 년간 계속 논의할 계획임

5. 싱가포르의 사이버보안 관련 규제

- 시기별 사이버보안 위험 관리 규정 진행 사항
  - 2010년 이전: 의료기기 품질, 안전성, 유효성을 바탕의 의료기기 규정
  - 2014년: '14년 이전에는 사이버보안 위험은 사후관리 개념으로 관리되었으나, 의료기기 자체로도 서로 많이 연결되어있다보니 의료기기의 사이버보안의 중요성이 점차 인식되었으며 '14년 이후 규제자들은 의료기기 사이버보안 위험을 좀 더 잘 규제할 필요가 있다는 것을 전 세계적으로 인식하였으며 전주기적 접근방식을 적용할 필요가 있다는 것을 강조함

- 2016년부터 예비 규제 요건을 HSA는 시판전 등록 절차에 적용
- 소프트웨어 의료기기에 대한 규제 가이드라인을 2020년 4월에 발간
- HSA의 사이버보안 요건 및 통제(control): 전주기적 방법으로 관리하는 것이 제일 효과적임
    - 설계 시(설계 단계에서부터) 보안이 잘 되어있는지가 가장 중요함. 초기 단계에서 사이버보안이 고려되어야 함.
    - 제조사의 위험관리 과정 전주기에 걸쳐 보안 관련 사항 추적 및 관리 가능해야 함
    - 제조사에게 시판 후 관리 계획을 제출하고 사이버 보안 관리할 수 있는 시스템을 갖추도록 요구. 또한, 제조사의 시판 후 관리 의무 사항 즉, 의료기기 이상반응을 보고 및 safety correction action 실행해야 할 의무가 있음. 사이버보안의 경우에도 마찬가지임.
    - 위험 관리를 잘 한다고해도 취약성은 항상 생길 수 있기에 HSA는 시판후 감시 work flow를 실행하여 문제를 예측하고 발생 시 적극적으로 대응하고 해결하려고 함.
- 사이버보안 문제를 해결하기 위해서는 규제자, 의료기기 제조사, 의료기기 사용자, 보건기관, 문제(취약성)를 찾는 사람들 모두가 책임을 갖고 협력해야함

6. 미국의 사이버보안 관련 규제

- 미 FDA는 2013~14년 시판전 가이던스(최초판)를 발간하였으며 이는 기본 원리(원칙)의 근간이 되었음. 2018년 이후, 시판 후 가이던스를 발간.
- 의료기기의 시판전·후 가이던스 발간을 통해 의료기기의 토탈 전주기에 대한 중요성을 깨닫게 됨. 설계(design)와 소프트웨어 공급 과정이 중요하며, FDA와 제조사 모두 위험요소를 줄이는 능력도 증가했다는 사실도 알게됨.
- 2018년 시판전 가이던스 개정판을 발간했는데, 이는 '14년에 발간한 가이던스를 근간으로 하고 있지만, 가장 중요하다고 인식되는 세 가지 사항(신뢰성, 투명성, 회복성)에 초점을 맞추고 있음.

- 시판후 관리 측면에서 발생할 수 있는 문제를 해결하기 위해서는 의료기기의 전주기에 해당하는 관리를 해야함. 그러기 위해서는 공급과정의 투명성, 소프트웨어 재료, 보안 설계, 보안 관리(통제)와 관련한 조언(추천사항)이 아주 중요해짐.
- 테스트에 대한 관심 증가, threat modeling의 개념(concept) 도입
- 서로 협력하는 것이 중요. threat modeling, 워크숍, 현재 실행중인 부트캠프, 소프트웨어 구성 재료 관련 업무, 레거시 디바이스 (레거시 디바이스 관리의 현재와 미래), 취약성에 대한 문제 해결 노력의 중요성, 각기 다른 의견 차이 해결 방법 등의 노력이 필요함.