의료 정보 시스템 위협 요소

김 봉 회, 박 진 섭
대전대학교 컴퓨터공학과

Threats of Medical Information Systems

Bong-hoi Kim, Jin-sub Park,
Dept. of Computer Eng., Taejon Univ.

요 약

본 논문에서는 의료 정보 보호를 위한 위협요소를 제시한다. 의료 정보 시스템은 무결성, 기밀성을 기반으로 하는 접근제어가 필요하다. 본고에서는 이와 같은 요구사항을 만족시킬 수 있는 의료 정보의 특성 및 위협요소들에 대하여 조사 분석하고, 의료 정보 시스템 보안 정책 모델을 구현하기 위한 메커니즘을 제시한다.

1. 서론

외국의 경우 의료 정보 시스템이 네트워크를 통해 공유되면서 의료 정보가 개인 기밀정보(프라이버시)로 분류되어 의료정보 보호에 관한 많은 관심을 갖게 되었다. 널리 이용할 수 있는 의료정보를 만드는 것은 환자의 개인 정보 노출에 많은 위험을 내포하고 있다. 미국에서는 이 문제를 사생활침해로서 법적으로 논쟁이 되고 있다[1]. 캐나다 Ontario주에서는 모든 진료 기록에의 접근을 건강 장관에게 주려는 시도가 대중과 Ontario 의학 협회에 의해 강한 압력을 받은 후에 좌절되었다[2]. 독일에서는 개인의료정보가 탑재되는 스마트카드시스템 도입에 많은 우려를 하고 있다.

영국에서는 정부가 전국적인 건강정보 네트워크를 위임받아 사용하게 될 시스템에 필요한 많은 기준들을 세우고 있는 중이다. 기준을 설정함에 있어서 특성은 많은 양의 건강정보를 처리하게 되고 다양한 분석자료들을 만들어 관리자가 이용할 수 있게 되는 시스템에서 병원 자료의 요구가 집중화 될 것이라는 것이다. 의사들에게는 의료 정보 보안에 대한 책임이 주어진다. 아직 주 전문 조직인 영국 의학 협회(BMA)의 의사들은 정보제공을 거절해 왔고 새로운 네트워크 상에서 네트워크의 기준에 따라 환자 정보를 보호할 것으로 기대되어 진다. 또한 실제 위협과 보호 대책에 관한 많은 혼란이 있다는 것은 분명하며 신중한 요소로 분류되고 있다. 이런 문제로 BMA는 개인 건강정보에서의 위협에 대하여 연구하고, 보안정책 모델과 실습을 위한 중간 지침서를 만들고 있는 중이다.

스웨덴에서는 진료 기록의 암호화가 정보보호 당국에 의하여 위임관리 되고 있다. 그리고 노르웨이에 파급되어졌다. 많은 나라들이 의사들의 키로 서명하는 신뢰 보증 권한을 구축하고 있다[3]. 일반 보호와 의학정보의 비밀보장을 위한 유럽 표준화 그룹은 대규모 네트워크 상에서 확인된 임상데이터의 암호화를 위하여 표준 초안을 추천하였다.

캐나다에서 디지털 서명의 사용은 Ontario 건강 장관에게 보고되어 검토된 적이 있다.[4]. 건강정보 비밀에 대한 오스트리아 표준[5], 뉴질랜드 건강정보 비밀코드[6], 그리고 정부 기술 협회의 보고서는 이러한 사실

에 동의하고 있다. 그들은 위협의 이해나, 동의의 원칙, 기술적인 선택사항에 대하여 여러 다른 방법으로 검토되고 있다.

이와 같이 여러 나라에서 의료 정보의 보안을 위한 많은 노력을 하고 있지만 아직까지 설득력 있고 이해할 만한 정책 및 보안 모델은 없다. 필요성에도 불구하고 국내의 경우 의료정보보안문제는 아직 검토가 활발하지 못하다. 그러므로 본 논문에서는 의료정보에 대한 불법적인 접근, 조작 등이 발생될 경우 제반 업무에서의 혼란과 법적인 책임 등이 따르는 심각한 사태가 야기될 수 있으므로 분쟁의 원인이 될 소지가 있는 위협요소를 분석 검토함으로서 올바른 보안 정책을 수립하기 위한 참고가 되기를 기대한다.

1.1 기밀성 기반 윤리

환자들은 자신들의 동의가 없으면 의사들이 그들이 직업적 과정에서 얻게되는 어떠한 개인 정보라도 폭로하지 않게 하는 권리를 가지고 있으며 비밀을 지켜야만 하는 의무를 가진다고 정하고 있다.[7].

덧붙여 개인 정보의 관리자이며 기록자인 의사들은 정보의 저장이나 전달, 수집의 과정에서 효과적으로 부적절한 노출에 대하여 방어를 해야만 한다[8]. 간호사들이나 물리치료사 약사와 같은 다른 의료인들도 유사한 강령을 가지고 있다. 결과적으로 많은 나라들이 자료 보안을 위한 법률을 가지고 있고 1998년부터 자료 보안에 있어 유럽연합 지휘부는 유럽의 나라들에게 개인 건강정보 보안을 최우선 원칙으로 환자의 동의를 얻도록 지시하고 있다.

현재 우리 나라에서는 업무 전산화와 함께 진료 기록의 전산화가 이루어지고 있고 EMR(Electronic Medical Record)의 사용이 증가하고 있다. 한국통신에서는 EDI 청구 시스템을 개발했고, 이를 바탕으로 데이터베이스를 구축하기 위한 노력을 하고 있다. 또한 정부에서는 전국민 건강카드 제도도 계획하고 있다. 이러한 것들이 모두 EMR에 포함되는 것이다. 그러나 이러한 EMR이 실용화되는데는 여러 가지 문제점이 있는데 그 중의 하나가 법적인 문제이다. 컴퓨터에 저장된 데이터의 안전성에 대한 확신이 없기 때문에 EMR의 기본이 되는 전자적 정보기록이 법적으로 인정받지 못하고 있다. 따라서 의료인이 사용을 꺼리고 있고 이에 대한 자구책으로 종이에 기록된 것을 컴퓨터에 입력하거나 컴퓨터에 저장된 기록을 다시 종이에 인쇄해서 보관하고 있는 실정이다. 따라서 이런 문제를 해결하기 위한 방법으로 전자적 정보기록이 법적으로 인정받기 위한 정책이 필요하다[17].

환자의 동의는 통보가 되어져야 되며 또한 자발적 이여야만 한다. 예를 들어, 환자들은 치료 팀의 구성원들 사이에 공유되는 정보를 인식하고 있어야만 한다.(일반적 의료 시술, 의료 담당 부서) 그리고 익명으로 되어질 수 없는 기록을 접촉하기를 원할 때에도 환자에게 통지하고 환자의 동의를 얻어야 하며 이러한 동의와 통보의 내용들은 매 5년마다 새롭게 갱신되어야만 한다[9].

1.2 의료 기밀에 대한 위협

많은 기관들이 자료의 접촉에 수 작업을 통한 기록을 보유하는 대신에 더욱 편리한 네트워크된 컴퓨터 시스템이나 집중화 된 컴퓨터시스템을 가지고 운영하고 있다. 이러한 것은 내부에 있는 사람들에 의하여 남용되는 위협을 가지고 있다. 예를 들어 대부분의 큰 은행들은 의지가 있으면 어떠한 계좌라도 접근할 수 있다. 그 결과 개인의 정보를 얻고자 하는 이들은 매수를 통하여 개인의 정보를 알아낼 수 있다[10]. 이러한 행위가 개인 정보 기관에 의하여 불법적으로 행해지고 있는 실정이다.

미 정부 기술협회에 의해 보고된 문제를 보면 정보누출 위험이 내부자의 소행이 많으며 이러한 행위는 컴퓨터 네트워크 시스템에 의한 자료 집중화에 의해 더욱 심각해지고 있다.[15]. 개인의 사생활이 파괴되고 사생활 침해에 따른 소송을 제기하는 일들이 늘어나고 있어 이에 대한 논쟁이 미 의회에서 진행되고 있다. 예를 들면,

- 주(State) 건강 위원회에서 은행가들은 암으로 진단된 환자의 모든 명단을 접촉할 수 있는데 그는 그의 고객명단과 그것을 비교 참조함에 의해 환자의 대부금을 청구하고 있다[11].
- 개인 건강정보에 대한 Harris 여론조사에 의하면 응답자 80%가 개인의 진료기록에 대하여 걱정하고 있으며 이들 중 ¼정도의 개인 건강 정보가 남용되었다는 경험을 가지고 있다고 보고하고 있다[12].
- 보험회사의 40%가 의료 정보를 채권

자나 고용인, 유통판매업자에게 고객의 허락 없이 정보를 누출하고 있다[13]. 그리고 미국의 500대 기업의 절반이 넘는 회사가 채용과 인사 업무에 진료 기록을 사용하고 있다[14].

의학정보의 무결성과 가용성은 확실한 안전과 법의학의 이유들 때문에 또한 매우 중요하다. 반면, 우편, FAX, 그리고 전화메모는 단지 컴퓨터 체계를 실패에 대한 증거의 자료일 뿐이다. 소프트웨어 버그는 연구실 보고서의 번호를 총체적으로 바꿈이 없이 다르게 할 수 있고 제거할 수도 있다. 바이러스는 이미 의료 정보를 파괴해 왔고 임상 EDI에서 표준시스템의 기능부족으로 말미암아 다른 시스템들에 의해 다른 목적으로 활용되어 위협이 증대되고 있다고 볼 수 있다.

컴퓨터 보안 메커니즘의 부재로 인하여 외부자가 내용을 조작하거나 변경하는 것이 가능하지만 대부분 보고된 의료 정보 시스템에 대한 공격은 컴퓨터의 도난으로 이루어지며 영국 일반 개업의의 11%이상이 이와 같은 경우를 당했었다. 시스템 무결성에 대한 문제는 내부자에 의해서 이루어지며 우리가 알고 있는 전형적인 경우로서 공격자들은 의료사고의 기록 변경에 의해 책임을 전가시킬 수 있다. 그리고 계약 내용들을 변경시킴으로써 사기 또는 범죄를 범할 수 있다.

그리고 무결성에 대한 공격은 기밀성의 상실에 따라 이루어진다. 만일 진료 기록이 고용 및 신용 결정의 목적에 의해 일상생활의 외부에서 광범위하게 이용된다면 이 기록들을 변경 할 동기가 될 것이다. 만일 의료정보가 건강의 치료보다 다른 목적을 위해 이용되는 시스템과 공유된다면 이와 유사한 경우가 발생할 것이다. 어떻게 전자기록이 법정증거로서 이용되기에 충분한 정도로 믿음이 있는가에 대해 걱정된다.

만일 환자들이 그들의 의료 비밀이 비밀리에 보존되어질 것이라는 믿음이 사라지면 관련된 정보를 속이게 되어 부정확한 기록으로 인하여 개별 환자에 대한 부적절한 치료가 따르게 되고 다른 환자에 대한 위험이 증가되게 될 것이다..

2. 의료 정보 시스템 위협 요소

의료 정보 시스템은 EDI와 통합 데이터베이스를 통하여 병원 내 또는 병원간 정보가 교환 또는 공유된다. 따라서 정보 교환과 공유 시에 다양한 위협요소가 존재할 수 있다. 의료 정보 시스템에서 교환되는 정보는 환자의 명부, 진료기록부, 처방전, 수술기록, 검사소견기록, 방사선 사진 및 그 소견서, 간호기록부, 조산기록부, 진단서, 사망진단서, 검안서, 적출물의 소각, 보존 및 재활용에 관한 기록부 등이 포함하는 것으로 진료에 관한 기록(의료법 시행규칙 18조)을 의미한다.

의료 정보 시스템에서의 위협요소는 전송되는 기록을 변조하는 경우, 사용자의 특권을 얻어 위장하는 경우이기 때문에 이미 알려진 위협요소들과 동일하다. 통합 데이터베이스로 운용되는 의료 정보 시스템의 경우 권한 없는 병원이 권한 있는 병원으로 위장하여 정보를 요청할 수 있다. 또한 요청된 정보가 통합 데이터베이스로 전송될 때 네트워크 상에서 위조, 변조, 도청 등의 위협요소들이 존재한다. 이러한 위협요소들은 고의적으로 혹은 사고에 의하여 발생할 수 있으며 능동적 또는 수동적일 수 있다. 의료정보시스템에서의 위협요소를 일반적인 정보시스템에서 발생할 수 있는 위협요소와 함께 의료정보 특성상 발생될 수 있는 위협요소로 분류하였다.

2.1 일반적 위협요소

의료정보 시스템은 EDI와 함께 운영되고 전자 매체를 통해서 전송되고 보관되는 과정에서 다음과 같은 위협 상황에 노출될 수 있다. 대표적인 위협요소가 <표 1>에 설명되어 있다.

2.2 의료 정보 특성에 따른 위협요소

의료 정보 시스템에 있어서는 다른 정보 시스템과는 다른 몇 가지 특수한 요소가 포함되어 있다. 따라서 위에서 설명한 위협요소들은 일반적인 정보 시스템에서 야기될 수 있는 위협요소이지만 여기서는 의료 업무 특성상 검토해야 할 위협요소들을 설명하고자 한다.

- <u>기밀 보존에 대한 인식</u> : 환자가 의료 정보의 기밀에 대한 신뢰성을 인식하지 못하면 치료와 관련된 정보의 비밀로 인하여 다른 환자에 대한 부적절한 치료의 원인이 되어 다른 환자의 위험이 증가된다.

- <u>정보에 대한 안전성 인식</u> : 의료 정보에

대한 기록들이 시스템 상에서 안전하다는 확신이 없으면 의사들은 의료 정보 시스템에 구축되어 있는 정보에 대한 사용을 꺼리게 되므로 전자 기록에 대한 법적 보장이 선행되어야 한다.

종 류	내 용
내부의 적	내부자로부터 권한의 남용으로 인하여 발생되는 위협들로서 권한오용, 의도된 신뢰 활용, 특권 프로그램 오용 등이 있다.
컴퓨터 해킹	대부분 시스템을 파괴할 목적으로 공격자들로부터 발생되는 위협들로서 보호 설정 오류 활용, 스프핑과 위장, 작업 획득, 패스워드추측, 불안전한 데모 활용, 프로세스 우회, 재생 공격, 암호 해독,전송 중 감시, 전송 중 수정 등이 있다.
위장	어떤 실체가 마치 다른 실체인 것처럼 위장하는 것으로서 비인가된 이용자가 자원을 불법적으로 접근하기 위하여 제 3자가 정당한 사용자인 것처럼 위장한다.
메시지 순서변조	메시지의 일부 혹은 전부를 지연 전달시키거나 고의로 메시지의 재발급 또는 순서를 재배치한다.
정보 변조	수신자에게 전달되는 정보, 라우팅 정보 및 관리 정보를 손실되게 하거나 변조하는 것이다.
서비스 거부	객체가 자신의 기능을 수행하지 못하거나 상대방의 기능 수행을 방해하고 제공된 서비스를 거부하는 것이다.
부인	시스템 사용자가 메시지 전송, 제출, 배달 등의 행위를 실제로 하였음에도 불구하고 하지 않았다고 부인하는 것이다.
정보 누출	메시지의 전송 감시, 시스템내의 정보에 대한 비인가적 접근, 또는 위장 등에 의해서 비인가자에게 정보를 노출시키는 것이다.

<표 1> 일반적 정보 보호 위협요소

- **개인 정보의 식별** : 통계를 얻기 위한 목적으로 환자의 기록열람을 요청할 경우 관련된 환자의 모든 기록에 접근할 수 있는데 이때 개인에 대한 식별이 되지 않도록 해야 한다. 만약 개인에 대한 식별이 된다면 그것은 개인 프라이버시 침해가 되고 또한 다른 목적으로 악용될 수도 있다.
- **기록 변경에 따른 문제** : 진료기록은 어떠한 경우에도 삭제되어서는 안된다.(오진의 경우에 있어서도). 허가된 사람이 내용을 수정해야 한다면 추가사항으로 기록되야 한다.
- **동의의 원칙** : 법적으로 인정하는 경우에만 제외하고 개인에 대한 기록 접근시 반드시 환자 혹은 대리인의 동의를 얻어야 한다. 이 원칙 또한 무시되면 환자의 기록 정보에 대한 기밀이 누설되어 프라이버시 침해는 물론 다른 목적으로 악용될 수 있다.
- **정보의 보존 및 유지** : 진료 기록에 대한 보존 기간과 의무가 명확히 명시되어 유지 되도록 해야 한다. 개인에 대한 의료 정보는 성격에 따라 일정기간 유지 관리 되고 보존되어야 될 의무가 있다.
- **정보의 보고 문제** : 법으로 정해진 특정 질병의 경우 반드시 보고되어야하는 의무가 있다.

3. 의료정보시스템 정보보호서비스

안전한 의료 정보 시스템을 구현하기 위해서는 정보보호 서비스들이 요구된다. 의료 정보 시스템에서의 정보보호 서비스는 앞 절에서 정의한 다양한 정보보호 위협요소들로부터 정보를 안전하게 보호하기 위한 것이

다. 안전한 처리를 위한 필요 조건과 기술적 사항들을 포함하는 <표 2>에 나타나 있다.

종 류	내 용
기밀성	컴퓨터 시스템의 정보 및 전송 정보가 의도된 당사자만 읽을 수 있도록 하는 서비스를 말하며 위협요소로부터 전송 자료를 보호 하는 것이다.
무결성	사용자들간에 주고받는 메시지가 정확한지 또는 변경되지 않았는지를 확인하기 위하여 컴퓨터 시스템 및 전송 정보가 오직 인가된 당사자에 의해서만 수정될 수 있도록 통제하는 서비스를 말한다.
인증	정보 및 시스템 자원 사용 시 자원을 사용하려는 사용자의 신원을 확인하는 것이다.
부인 봉쇄	메시지가 성공적으로 송신되었을 때 송신자가 송신한 내용을 부인하거나 수신자가 수신된 사실에 대한 부인과 같은 잠재적인 위협요소가 존재하기 때문에 이러한 위협들을 봉쇄하기 위한 것이다.
접근제어	개방 시스템의 상호 연결에 통하여 비 인가된 자원의 사용에 대한 보호을 제공하는 것으로 특정 자원에 대한 여러 유형의 접근에 적용되거나 또는 모든 자원에 대한 접근에 적용될 수 있다.

<표 2> 정보 보호 서비스

4. 정보 보호 우선 순위

컴퓨터 보안을 시행하기 위한 메커니즘의 논의에는 그 시스템이 충족시켜야 하는 보안 목표와 저항해야 하는 위협을 상술한 특정 보안 정책이 들어 있어야 한다. 예컨대, 가장 자주 명시된 상위 보안 목표는 시스템이 정보의 무단 노출이나 절도를 방지하고 정보의 무단 변조를 방지하고 서비스 거부를 방지해야 한다는 것이다. 대처해야 할 전통적 위협은 허가 받지 않은 자에 의한 시스템 침입과 허가 받은 자의 무단 행위, 시스템 프로그래머와 설비 운용자의 특권 남용이다. 이 위협들은 의도적이기도 하고 우발적이기도 하다.

국방 보안 정책은 정부 내의 기밀 정보 관리를 조절하는 정책이다. 다시 말해서 모든 기밀 정보를 무단 노출이나 기밀 취급 해제로부터 지켜야 한다는 것이다. 이 정책을 시행하는데 사용되는 메커니즘에는 모든 문서에 기밀 종별 수준을 필수적으로 표시하고, 이 정보를 사용할 허가를 받은 모든 사람들의 등급에 근거하여 사용자 접속 범주를 지정하는 것이다. 지난 15-20년간, 컴퓨터에서 이 정책을 시행하는데 어떤 매커니즘을 사용해야 할지 결정하기 위해 상당한 노력이 있어왔다. 사용자 확인과 허가 등의 매커니즘, 감사 정보 생성, 접근 통제 표식과 모든 정보 객체와의 관계들은 잘 이해되고 있다. 이 정책은 그 표지 색상으로 인해 "오렌지 북"이라 불리는 국방성의 신뢰받는 컴퓨터 시스템 평가 기준(DOD)에 규정되어 있다.

의료 정보 시스템 환경에서는 노출을 방지하는 것도 중요하지만 일반적으로 자료의 무단 변경을 방지하는 것이 가장 중요하다. 특히, 자산의 관리와 회계에 관련된 상업 자료 처리에는 범죄 행위과 오류를 방지하는 것이 주된 목적이다. 이 목표는 정보의 기밀성보다는 무결성을 시행함으로써 달성할 수 있다. 이러한 이유로 우리 자신이 관심을 갖는 정책은 노출보다는 무결성을 다루는 정책이다. 이것은 국방 정보 보안정책과 대비되는 상용 정책의 특징이다.

이러한 모든 이유들 때문에 의료 시스템의 무결성과 기밀성은 분리되어 생각될 수 없고 두 단계로 고려되어야 한다. 협의적 단계로서 일반적 시술 또는 병원의 부서와 같은 하나의 시스템에 유지된 정보에 대한 위협을 걱정하여야 한다. 예로서 부정직하고 부주의한 고용인들에 의해 독단적 정보의 유출과 컴퓨터의 도난이 문제이다. 따라서 직원의

교육이나 규칙적인 보관 그리고 정기적인 감사를 통하여 조절되어질 수 있다. 즉 BMA는 [28]에 지침서를 싣고 있다.

따라서 향후 본 고에서의 주요 관심은 수많은 사람들의 진료 기록에 대한 무결성 또는 가용성 및 기밀성의 위협을 조절하기 위해 사용될 보안 정책이다. 현재의 의료 정보 시스템은 통합된 데이터베이스환경으로부터 운용되기보다는 부분적으로 병원마다 작은 시스템이 모이는 네트워크하에서 운용되고 있다. 앞으로 EDI방식으로 정보가 교환되고 공유될 경우에 더 많은 위협요소가 등장하게 되면 이에 따른 총체적 보안 대책을 수립해야 한다.

시스템의 보안성을 평가하기 위해서는 어떤 위협요소에 우선순위를 두어 보안 정책이 수립되었는지 알아야 할 필요가 있고 적절한 보안 정책이 수립된 후에야 시스템에 맞는 보안 메커니즘을 구현할 수 있다.

5. 의료 정보 보호 메커니즘

의료 정보 시스템의 사용자 인증과 접근제어를 수행하기 위해 컴퓨터 보안 메커니즘, 네트워크에서 정보의 접근 제한을 위해서 통신 보안 메커니즘, 확인되어진 환자들을 위한 충분한 잔여 정보를 보유하지 않기 위해서 연구와 검사에 사용된 기록들을 지키기 위한 통계적인 보안 메커니즘, 그리고 화재나 도둑에 의하여 기록들이 삭제되어지지 않게 지키기 위한 백업 절차와 같은 가용성 메커니즘 등이 필요하다.

5.1 컴퓨터 보안 메커니즘

의료시스템에서 컴퓨터 보안의 기본 목적은 기록이 하나의 컴퓨터에서 다른 컴퓨터로 보내어 질 때 접근제어가 다른 곳으로 정보가 새지 않게 하는 것이다. 예로, 만약 한 객체가 시스템으로 보내어져 그의 접근제어 리스트를 파괴시키거나, 동의를 수행하지 않게 되는 경우가 발생할 수 있다. 만약 깨끗한 데이터가 전화도청에 의하여 가로채어지는 일이나, 전자메일 메시지에서 임상 정보가 실수로 다른 의사나 심지어 메일링 리스트, 뉴스그룹에까지도 잘못 보내어 질 수 있다.

두 번째 컴퓨터 보안 메커니즘의 목적은 네트워크로 보내어지는 데이터의 무결성을 보호하는 것이다. 병리학 보고서와 같은 기록은 위에서 언급했던 것과 같이, 수령인에게 명백하지 않는 방법으로 갑자기 파괴되어질 수 있다. 이것은 또한 전자적인 기록들이 합법적인 목적을 위해 적당한 것인지 아닌지 여러 나라에서 논쟁이 되고 있다. 이러한 이유로, 디지털 서명이 사용되거나 다른 강력한 무결성 조사가 요구되어 지고 있다.

5.2 신뢰 구조

디지털 서명은 신뢰 구조를 갖게 한다. 예를 들면 중앙의료지원센터는 자신의 키를 가지고 사인하는 것으로 모든 의사들을 인증해야만 한다. 그리고 다른 임상 전문가들은 그들 자신을 나타낼 수 있는 신체 등에 의하여 인증될 수 있다. 이런 접근 방식은 프랑스정부에 의하여 지원되어졌다[3].

모든 이러한 선택사항 모든 것은 장점과 단점을 가지고 있으며 현재 토론의 주제가 되었다. 비록 인증이 사실상 로컬이라고 할지라도 백업 중앙 서비스가 여전히 필요하다. 그리고 이런 중앙 서비스는 자동화되어져야 한다.

여러 응용 분야에서 신뢰와 권위의 본성은 전자 신뢰구조를 반영하는 중요한 것이다[25]. 의학분야에서 권한은 계층적이며, 중앙집중화, 관료화보다 동등화하고 지역적인 경향을 보인다.

의료 시스템은 X.509나 X.9.3 등의 보안구조에 의하여 운영되어져야 한다.

5.3 접근 제어의 전파

어떤 경우에, 의료인은 키로 적당하게 인증을 획득할 수 있고, 네트워크 상에서 접근제어 리스트의 무결성은 다음과 같은 규칙집합에 의하여 수행되어질 수 있다.

- 개인의 건강 정보는 만약 그의 접근제어 리스트 상에 의료인에게 속한 것으로 확실히 믿어지는 키를 가지고 암호화 되어져있지 않다면 의료 시스템은 불안정해질 수 있다.
- 네트워크에 전송되어지는 생명이 위독한 정보는 만약 적당한 의료인에게 속한 것이라 확실히 믿어지는 키를 사용하여 서명되지 않았다면 주의를 요하여 다루어지어야만 한다.
- 위의 언급에서 적당한 신뢰는 개인적

인 접촉에 의하여나, 보증되어지거나, 다른 믿을 수 있는 여러 방법으로 인증 되어진 키의 소유권을 의미한다.

■ 해독된 정보는 환자의 이름을 포함하는 접근제어 리스트를 가진 신뢰시스템에서 저장되어져야 한다.

접근 요청은 환자의 동의를 제외하고 결코 자동적으로 허가되어져서는 안 된다. 인가는 문서가 완성될 때까지 키 도구를 제공하지 않는 일상적인 방법으로 실시될 수 있다. 이것은 웹 신뢰 접근 상에서 적어도 보증을 구축하거나 중심적인 하나의 장점이다.

복호는 결코 단지 컴퓨터 보안 선택사항이 아니다. 익명은 종종 더 간단할 수 있다. 예로, 담당의사에게 검사 보고서들을 배달하기 위한 시스템은 하나의 샘플 레이블에 바코드로 표시된 일련번호를 가진 환자의 이름으로 대치해야만 한다. 그 검사 결과는 적당한 무결성 조사를 통해 깨끗한 상태로 전송되어야 한다.

5.4 효과적인 감사

기록이 서류에서 전자적 형태로 변할 때 악용이 우선적으로 고려될 수 있다.

따라서 제어를 조정하는 것은 필요하고 접근제어는 혼자서는 불충분하다. 제어를 조정하는 것은 침입자가 꼭 잡히는 감사 시스템을 포함해야만 한다. 한편, 시스템은 전자적인 기록이 적어도 교체된 서류 기록만큼 안전해야만 한다는 목표에 도달하는데 실패할 수 있다.

현재 의료 시스템에 대한 관심 있는 요소 중 하나는 인증이 신뢰받지 못하는 것이다. 군사 시스템을 만들 때 우리는 대통령이나 수상을 우리편으로 가정할 수 있다. 그리고 은행 시스템은 사기꾼을 방지하기 위해서 고위 간부에 의해서 일반적으로 설계되지 않는다.

약품은 다르다. 여러 세대들을 위해서 여러 나라에서 의료인과 환자는 개인 건강 정보를 지키려고 하는 반면에 인증기관들은 개인 건강 정보 접근을 더 늘리려고 노력해 왔다.

이것은 감사 시스템의 설계를 복잡하게 한다. 감사 단서를 가지고 있는 곳은 어디인가? 그리고 그것에 대해 동작하는 것을 믿을 것은 누구인가?

컴퓨터 시스템을 통하든지 서류 기록을 통하든지 개인 건강 정보에 대한 비인가 접근에 대한 기록된 사건은 중앙으로 통합된 통계 자료가 없다[11].

5.5 통계 보안

개인 정보와 관련된 보안 정책으로 종종 공공목적 연구나 조사 목적으로 통계자료가 발생되는 경우를 고려해야 한다.

이 주제는 인구조사의 항목에서 널리 연구되어졌다. 하지만 의학분야의 경우에는 이 문제가 더 어려워진다. 만약 침입자가 "습진을 앓고 있는 13세 그리고 15세 두 딸을 가지고 있는 35세의 여자들 모두의 데이터를 보여달라"라고 질의를 물으면, 그는 개인의 정보를 확인할 수 있을 것이다. 노르웨이의 제안은 연구자들이 전국적인 토대로 하는 것보다 지역적인 토대로 데이터를 링크할 수 있도록 받아들여야만 한다고 제한한다. 연구자들도 지역적인 등록으로 움직일 것이다.

대부분의 연구들은 큰 용량의 데이터 접근을 포함하지 않는다.

5.6 의무기록

아직까지, 대부분 전자적인 임상 기록 시스템은 서류를 기반으로 하는 습관들을 반영하고 있다. 환자가 다른 곳으로 이송되면 관련 기록도 함께 이동되어야 한다. 그러나 의무기록은 서류를 기반으로 하고 있으며 환자 지원 기록 측면보다는 의사의 필요에 대한 기록의 의미를 더 가지고 있다. 이것은 기록체제의 변화가 수반되어야함을 의미한다. 환자 중심의 기록은 응급환자의 경우에 효과를 볼 수 있을 것이다. 전자적 기록은 이에 효과적으로 대처할 수 있다. 그러나 데이터 관리에 문제가 있을 수 있다.

단일 전자적인 환자 기록 시스템의 보안 정책 복잡성의 토론을 위해선 Griew와 Currell에 제시되고 있다[22]. 이 논문에 따르면 명백하다. 단일화된 전자적인 환자 기록은 좀 더 복잡한 정책 모델을 만드는 것에 초점이 맞추어질지도 모른다.

그러나 우리는 교차해야만 하는 접근제어 리스트의 다른 객체의 꾸러미인 단일 기록을 제안한다.

6. 결론

외국의 경험에 비추어 볼 때 개인 건강 정

보에 대한 기밀성, 무결성 그리고 가용성의 위협들에 대해 많은 논란이 있어 왔다. 현재 국내에서도 지역적으로 의료정보시스템이 EDI와 함께 시험 운용되고 있다. 향후 의료 전산망의 확산과 함께 의료정보의 통합이 예상되고 있다. 따라서 많은 정보가 교환되고 공유됨에 따라 의료 정보에 대한 보안대책은 필수적으로 선행되어야 할 중요한 과제가 되었다. 그러나 아직까지 이에 대한 연구는 미흡한 실정이다. 본 논문에서는 일반 정보 시스템에서 발생될 수 있는 위협요소와 의료 정보 시스템 특성상 야기될 수 있는 여러 가지 위협요소들에 대하여 조사하고 분석하였다.

또한 본 논문에서의 관점은 의료 시스템은 기밀성의 위협에 대한 정보 보호도 중요하지만 무결성의 위협으로부터 정보를 보호해야 한다는 점이다. 본 고에서 제시한 위협요소는 의료정보 시스템 보안 정책을 수립하기 위한 기초 자료로 활용될 수 있으며, 정보기술의 발전에 따라 추가적인 위협요소가 제기될 수 있다.

[참고문헌]

[1] "Medical Records Confidentiality Act of 1995", B Bennett, US Senate S.1360, 24th October 1995

[2] "Proposed Confidentiality Law Angers Canadians", The Lancet(16 December 1995) p 1618

[3] "Security of Health Information Systems in France: what we do will no longer be different from what we tell", FA Albert, L Duserre, Internationlj jornal of Biomedical computing v 35(supplement, 1994) pp 202-204

[4] "Health Care Information: Access and Protection", RH Smuckler, Institute for Primary Care Information, 1994

[5] "Austrian Standard 4400: Personal privacy protection in health care information systems", Standard Australia, 1995

[6] "Health Information Privacy Code 1994", Newzealand Privacy Commissioner

[7] "Good Medical Practice", General Medical Council, 178-202 Great Portland Street, London

[8] "Confidentiality, General Medical Council, 178-202 Great Portland Street, London

[9] "Medical Ethics Today - Its Practice and Philosophy", A Sommerville, BMA 1993

[10] "Your Secrets for Sale", N Luck, J Burns, The Daily Express, 16/2/94 pp 32-33

[11] "RMs need to safeguard computerised patient records to protect hospitals", Hospital Risk Management 1993 no 9 pp 129-140

[12] "Privacy and Security of Personal Information in a New Health Care System", LO Gostin, J Turek-Brezina, M Powers et al., Journal of the American Medical Association v 20(24/11/93) pp 2487-2493

[13] "Who's reading your medical records?" Consumer Reports, Oct 94 pp 628-632

[14] "Is your health history anyone's business?" McCall's Magazine 4/95 p 54, reported by M Bruce on Usenet newsgroup comp. society privacy, 22 Mar 1995

[15] "Protecting Privacy in Computerized Medical Information", Office of Technology Assessment, US Government Printing Office, 1993

[16] "Workshop on Health Care - Confidentiality: discussing current initiatives",held at the BMA on 4th April 1995

[17] "EMR의 법적, 윤리적 문제", 신동호, 대한의료정보학회, 제2권 제1호, 1996.6

[18] "Fundamentals of Computer Security Technology", E Amoroso, Prentice Hall 1994

[19] "Personal communication", WJ Caelli, July 1995

[20] "Confidentiality of medical record: the Patient's perspective", D Carman, N Britten, British Journal of General Practice v 45(Sepetember 95) pp 485-488

[21] "A Comparison of Commercial and Military Computer Security Polices", in

Proceddings of the 1987 IEEE Symposium on Security and Privacy pp 184-194

[22] "A Atrategy for Security of the Electronic Patient Record", A Griew, R Currell, IHI, Univ. of Wales, Aberystwyth, 14th March 1995

[23] " 'Sounddex' codes of surnames provide confidentiality and accuracy in a national HIV database", JY Mortimer, JA Salathiel,Communicable Disease Report v 5 no 12(10 Nov 1995) pp R183-R186

[24] "Handling confidential patient information in contracting: A Code of Practice", NHS Information Management Group EL(92)60, catalogue number 2009(c), news info 132

[25] IInstitutionell-organisatorische Gestaltung informationstechnisher Sichernfro-strukturen", A Roβnagel, Datenschutz und Datensicherung(5/95) pp 259-269

[26] "The Active Badge Location System", Roy Want, Andy Hopper, Veronica Falcao, Jonathon Gibbons, in ACM Transactions on Information System v10 no 1(January 1992) pp 91-102

[27] "A Security Policy Model for Clinical Information Systems", Ross J Anderson, univ of Cambridge

[28] "Clinical system security: interim guidelines", RJ Anderson, in British Medical Journal v 312 no 7023(13 Jan 1996) pp 109-111

[29] "의료관계 법규", 김성훈, 현문사

[30] "의무기록 관리학", 대한의무기록협회 출판부, 대한의무기록협회