▧ 원 저 ▧

의료기관의 정보보안 수준 측정을 위한 평가모형 개발

안 선 주*, 권 순 만**†
동의의료원 의료정보실*, 서울대학교 대학원 보건정책관리학과**

<Abstract>

A Development of the Model for Evaluating the Security of Information Systems in Health Care Organizations

Sun Ju Ahn*, Soon Man Kwon**†
Dong Eui Medical Center, Graduate School of Public Health, Seoul National University***

The purpose of this study is to develop a framework for evaluating security levels in hospitals. We classify security indicators into administrative, technical and physical safeguards. The security evaluation model for hospital information systems was applied to three general hospitals. The analysis of the results showed a low security level in information systems. In particular, requirements for administrative and physical safeguards were very low. Hospitals need strict security policies more than other organizations because their information systems contain patients' highly confidential data. The evaluation model developed in this study can be used for guidelines and as a checklist for hospitals. The security evaluation in hospital informational systems needs to be an essential element of hospital evaluation.

Key Words : Information security, Hospitals, Information system, Confidentiality

† 교신저자 : 권순만(02-740-8875, kwons@snu.ac.kr)

Ⅰ. 서 론

의료분야 정보화가 추진되면서 정보보안이 중요한 과제로 대두되고 있다. 의료기관 정보의 대부분은 진료정보로서, 법률상 비밀이 유지되어야 하는 개인정보이나 우리나라 병원들은 타 업종에 비해 정보보호를 위한 투자나 활동이 극히 저조하며(한국정보보호진흥원, 2001), OCS, EMR 등의 의료정보시스템을 도입하는 병·의원이 늘면서 환자들의 개인정보 유출사례가 빈발, 대책마련이 시급하다는 지적이 일고 있다(http://www.dailymedi.com, 2004). 그러나 국내에서는 병원정보보안에 관한 지침이나 가이드라인이 제정된 바 없고 병원 대상 주요 평가에서도 정보보안 항목은 제외되어 있다. 따라서 본 연구에서는 국내 의료기관의 정보보안 현황파악을 위한 평가모형을 개발하는 것이 목적이다. 기존 문헌에서 정보보안 지표를 파악한 후 그 중요도와 우선순위에 따라 평가모형을 개발하되 평가항목의 중요도에 따라 배점을 부여하였다. 마지막으로 병원 정보보안 수준 향상을 위한 제언과 평가지표 활용방안을 제시하였다.

Ⅱ. 연구방법

1. 정보보안 지표 선정방법

정보보안 지표를 도출하기 위해 비교·검토한 자료는 총 10개이며 이 중 ISO17799, HIPAA, MEDIS-DC의 가이드라인, GPCG의 체크리스트를 중심적으로 활용하였다(표 1).

평가지표 개발단계를 요약하면 다음과 같다. 먼저 1단계에서 광범위한 문헌고찰을 시도하여 보안에 관한 국제표준 및 가이드라인에서 공통적이면서도 필수적인 평가항목을 발췌하였다. 2단계에서는 선정된 지표에 대한 측정가능성 및 실행가능성에 대한 자문을 전문가에게 의뢰하였으며 3단계에서 평가 항목 간 배점을 포함하는 평가모형을 개발하였다. 4단계에서는 개발된 모형을 이용해 3개 의료기관에 시범 적용하여 평가하였다.

<표 1> 정보보안 관련 표준 및 가이드라인

	제 정 기 구	종 류	특징 및 내용
1	ISO17799(BS 7799) International Standards Organization	국제 표준	관리적, 기술적, 물리적 보안요구사항
2	HIPAA Health Insurance and Portability and Accountability Act of 1996	미국 법률	의료정보의 안전한 보관·활용에 관한 법률로 병원이 준수해야 할 프라이버시보호 및 보안사항 제시
3	JCAHO Joint Commission on Accreditation of Healthcare Organization	미국 병원신임평가 기구	관리적, 인적, 기술적, 물리적 보안영역에 대한 평가
4	BMA British Medical Association, Clinical System Security Interim Guidelines	영국 의학협회 가이드라인	컴퓨터의 물리적 보안 사항과 암호화 방안 제시
5	MEDIS-DC The Medical Information System Development Center	일본 전자기록 연구기구	전자기록의 보안에 관한 사항을 관리적 측면에서 제시
6	GPCG General Practice Computing Group, Computer Security Check-list	호주 개원의 체크리스트	기술적 보안에 필요한 핵심사항을 체크리스트로 제시
7	AMC Academic Medical Center's Guidelines	미국의 가이드라인	HIPAA를 병원에서 어떻게 준수할 것인가에 대한 구체적 내용 제시
8	HL7 Health Level 7의 EHR보안	미국의 표준화기구	EHR시대의 보안요구사항
9	한국보건산업진흥원의 EMR보안인증항목	전자의무기록 보안인증항목	전자의무기록시행병원의 보안인증 평가 항목
10	국내 정보보안 관련 법률	한국의 관련법률	전자서명법, 의료법

Ⅲ. 연구결과

1. 평가지표

본 연구에서는 문헌고찰에서 얻은 정보보안 지표를 관리적, 기술적, 물리적 보안요소로 재분류하여 평가지표를 선정하였다(표 2). 정보보안 전문가에게 보편성과 타당성을 검증받아 선정한 지표는 병원 규모에 따른 보안역량의 차이와 전자의무기록의 도입여부를 감안하여 대형병원용과 중소병원용[1]으로, 기술적 보안 영역은 EMR 시행병원과 미 도입병원으로 구분하였다.

1) 대형병원 평가모형

관리적 보안영역은 9개 항목으로 구성되며 보안정책 2개 항목, 보안요구사정 1개 항목, 보안책임자에 관한 사항 1개 항목, 보안감사 1개 항목, 인적 보안에 관한 사항 4개 항목으로 구성하였다. 중 분류의 내용은 평가기준에 제시되고 평가기준은 다시 세부기준으로 측정되는 구조를 형성하여 실제 측정항목은 43개 항목이다(표 3).

기술적 보안은 사이버 범죄를 방지하기 위한 중요한 보안영역이며 네트워크 보안, 시스템 보안, 데이터베이스 보안, 응용 소프트웨어 보안을 포함한다. 기술적 보안은 관리적 보안 30점, 물리적 보안 20점에 비해 상대적으로 가중치가 높은 50점을 배점하였다. 기술적 보안이 상대적으로 가중치가 높은 이유는 의료기관의 정보저장, 활용의 매체가 종이에서 컴퓨터로 빠르게 이동되고 있는 현실에 근거한다. 즉, 정보를 담고 있는 매체가 컴퓨터이고, 컴퓨터에 저장된 정보는 적정수준의 보안기술이 적용되지 않을 경우 보안사고의 규모가 종이기록에 비해 훨씬 크고 심각하기 때문이다. 종이기록은 물리적 접근을 통해서만 정보취득이 가능한 반면 컴퓨터상의 정보는 보안기술이 취약할 경우 대량의 정보를 순식간에 집적, 획득할 수 있다는 특성이 있다. 따라서 정보화가 진척될수록 이에 상응하는 기술적 보안이 전제되지 않으면 어떤 조직이라도 정보를 안전하게 지킬 수 없게 될 것이다.

---

1) 대형병원과 중소병원의 정의에 관해서 합의된 개념은 없으나 통상 300병상 미만의 병원들을 지칭하기도 한다. 그러나 최근 병원의 대형화 추세로 500병상 미만을 지칭하기도 한다(이용철, 2000). 본 연구에서는 500병상 미만을 중소병원으로 규정하기로 한다.

<표 2> 제정기구별 지표 도출내용(대형병원, 전자의무기록 시행병원의 예)

대분류	중분류	평가기준	세부기준	중분류가 도출된 표준 및 가이드라인 제정기구
관리적 보안	보안정책 수립	2	12	ISO17799, AMC, JCHAO, MEDIS-DC, GPCG, KHIDI
	보안정책의 갱신	2	3	ISO17799, JCAHO, MEDIS-DC, GPCG, KHIDI
	위험 분석 및 평가	2	3	HIPAA, JCAHO
	보안책임자 지정	2	3	ISO17799, HIPAA, GPCG, MEDIS-DC
	보안감사	2	3	AMC, HIPAA, KHIDI
	보안 교육 및 훈련	2	12	ISO17799, HIPAA, AMC, JCAHO, GPCG, MEDIS-DC, KHIDI
	교육 효과 평가	1	2	
	비밀보호 서약서	1	3	ISO17799
	지침, 교육내용의 배포	1	2	MEDIS-DC
기술적 보안	정보보호시스템 적합성	1	2	ISO17799
	업데이트	1	4	GPCG
	백업	2	3	ISO17799, 의료법 시행규칙, JCAHO
	패스워드 관리	1	2	ISO17799, HIPAA, GPCG, JCAHO, KHIDI
	공인 전자서명	1	1	ISO17799, BMA
	전자서명 키 관리	1	2	ISO17799
	암호화	1	1	ISO17799, HIPAA, GPCG, JCAHO
	로그기록 감시	1	5	ISO17799, HIPAA, JCAHO
	추적 감사	1	3	HIPAA, JCAHO
	퇴직자의 권한종료	1	2	HIPAA
	접근권한 관리	2	3	ISO17799, HIPAA, GPCG, JCAHO, KHIDI
	복구절차	2	2	HIPAA, JCAHO
	비상시 운영계획	1	2	MEDIS-DC, GPCG, JCAHO, KHIDI
	운영계획의 테스트	2	3	GPCG
물리적 보안	전산센터 출입통제	1	2	HIPAA, JCAHO, KHIDI
	진료정보저장기기 보안	1	3	HIPAA, GPCG, JCAHO, KHIDI
	안정된 전원공급	1	1	GPCG
	백업센터 설치 장소	1	2	의료법 시행규칙
	시스템 별 비상계획	1	1	HIPAA
	비상계획의 테스트	1	2	HIPAA, GPCG
	유지보수내역 관리	1	1	HIPAA, GPCG
3	30	40	90	-
	본 연구에서 추가된 결과지표			KHIDI : 한국보건산업진흥원

<표 3> 관리적 보안영역 (대형병원용)

중분류	평가기준	세부기준	가중치 등급	배점	점수화 방법
보안정책 수립	보안지침 및 규정의 문서화 및 내용	당해 기관의 정보 보안의 목적과 목표 직원대상 보안교육 및 훈련의 내용 정보시스템 자산 목록 및 통제사항 보안사고 발생시 대응절차(보고체계) 보안정책 위반자 징계수단과 절차 보안정책의 재검토 주기 전산관리자의 직무 분리 서버·네트워크·시스템 보안 지침 비상시 운영계획 보안감사 실시에 관한 내용 외부업체 보안협약(예:프로그램개발업체) 보안정책 준수여부에 대한 평가체제구비	Ⅰ	5	TypeⅡ
위험 분석 및 평가	보안위협 요인을 분석, 평가하고 이를 정책에 반영	정보 보안 위협요소를 분석, 공유 위협요인제거 방안 및 적용효과평가 평가된 내용을 보안정책에 반영	Ⅱ	3	TypeⅡ
보안정책의 갱신	환경, 제도, 법률을 고려한 정기적 갱신	관련 법률에 맞게 보안정책의 갱신여부 보안정책의 검토의 정기성과 갱신내용 갱신내용의 준수 여부	Ⅱ	3	TypeⅡ
보안감사	내부 혹은 외부 보안전문가에 의한 정기적인 보안 감사	보안 전문가에 의한 내·외부 감사여부 감사의 정기적 실시 여부 지적사항의 기록유무 및 개선 여부	Ⅱ	4	TypeⅢ
보안책임자 확보	보안책임자의 유무 및 책임과 권한 명시	전체 조직의 보안을 리드할 책임자 유무 책임자의 업무범위와 권한의 문서화 보안책임자의 실제 활동 내용	Ⅱ	3	TypeⅢ
직원대상 보안 훈련 및 교육 내용	진료정보 취급자에게 정보보안에 관한 정기적인 교육 및 훈련 실시	정보취급자 대상 보안교육 실시 여부 보안교육의 실시 주기 보안교육의 실시 대상의 범위 교육 내용의 정기적 갱신여부	Ⅱ	4	TypeⅡ
	정보 보안교육의 내용	진료정보비밀유지에 관한 의료법 교육 패스워드 관리 비밀번호의 주기적 갱신 윈도우/바이러스 패치 자리비울때조치(스크린세이버,자동로그오프) 보안정책 위반시 징계 정책 정보보안 사고 발생시 보고절차 부서별 정보보안 책임자 고지			
교육효과 평가	보안교육의 효과평가	교육 대상자의 교육효과 측정 방법유무 교육효과 평가에 따른 환류	Ⅱ	3	TypeⅢ
비밀보호 서약서	진료정보 취급자가 작성한 비밀보호 서약서 보유여부	진료정보를 취급하는 자의 명단확인 진료정보 취급자 명단의 정확성, 최신성 진료정보 취급자 자필 서명 서약서	Ⅲ	2	TypeⅢ
보안지침 배포	보안지침 및 교육내용을 포함한 문서의 제공여부	보안지침, 교육내용 문서로 제공 여부 직원의 소지여부 확인	Ⅱ	3	TypeⅢ
9개 항목	10개 평가기준	43개 세부기준	-	30점	-

<표 4> 기술적 보안 영역(대형병원용-EMR시행병원)

중분류	평가기준	세부기준	가중치 등급	배점	점수화 방법
정보보호 시스템	정보보호시스템의 적합성	기본적 정보보호시스템의 구축 여부 NW,DB,서버,PC,어플리케이션 보안	Ⅱ	4	TypeⅢ
업데이트	정보보호 제품의 종류별 최신 패치 사용 여부	정보보호제품 최신 패치 사용 여부 무작위로 선정된 의료기관내 PC와 시스템의 최신 패치 사용여부 시스템 종류별 업데이트 실시일자, 직원 홍보에 관한 문서제시	Ⅰ	5	TypeⅢ
백업	환자 진료정보에 관한 정기적 백업 수행 여부	진료정보 백업실시 여부 백업의 실시의 정기성 백업저장시스템의 네트워크 연결여부	Ⅰ	5	TypeⅢ
패스워드 관리	사용자 패스워드의 관리절차를 수립	사용자 패스워드의 관리절차 유무 PW관리책임은사용자에게 있음을 주지	Ⅱ	3	TypeⅡ
공인 전자서명	EMR시행병원의 공인전자서명적용 여부	전자의무기록의 인증 및 기밀성, 무결성, 유효성을 보호하기 위하여 적용	Ⅰ	5	TypeⅢ
공인 전자서명 키 관리	공인전자서명가입자가 개인키를 분실. 훼손.도난시 행동절차	공인인증기관에 통보 및 기존 공인증서를 폐지하고 신규 공인 인증서를 발급받아 사용하는 것의 문서화 위 내용의 교육 여부	Ⅲ	2	TypeⅡ
암호화	의료정보의 기밀성확보	암호화 도입 여부	Ⅰ	5	TypeⅢ
로그 기록 감시	환자 진료정보에 접근한 로그의 정기적 감시	로그 감시 대상 진료정보 범위 로그 감시 실시 결과 문서 불법적 로그시도 경고메시지 사용 로그 감시 기록의 보고절차 로그 감시의 정기적 실시 여부	Ⅲ	2	TypeⅡ
추적 감사	진료정보 입력, 수정, 조회, 저장주체를 규칙적으로 확인	추적 감사의 정기적 실시 여부 추적 감사 대상의 진료정보 범위 추적 감사결과에 따른 후속 조치	Ⅱ	4	TypeⅢ
퇴직자의 권한 종료	퇴직시 ID의 권한종료	퇴직자의 ID 권한 종료 실시여부 무작위 선정된 퇴직자의ID 권한 종료일-퇴직일자(시간, 일) 계산	Ⅱ	3	Type Ⅰ
접근통제 (접근권한관리)	정보 접근 권한을 사용자별, 역할별로 등급에 의해 관리	역할,사용자,진료정보별접근권한제시(Read, Write, Read only, Print 등) 역할별, 사용자별 접근승인 방법제시 역할별, 사용자별 조회기간 제시	Ⅱ	3	TypeⅡ
복구 절차	시스템 에러발생시 복구 절차 문서, 인지	에러발생시 복구 절차의 문서 전산과 직원의 복구 절차 인지 여부	Ⅱ	3	TypeⅡ
비상사태발생시 운영계획	응급상황시를 대비한 운영계획 수립 여부	응급상황 단계별 운영계획 수립 여부 진료정보 DB의 안전관리,운영계획	Ⅱ	4	TypeⅢ
비상운영계획의 테스트	수립된 계획의 정기적인 테스트 및 결과의 환류	비상운영계획의 테스트 여부 테스트의 정기적 실시 여부 테스트 결과의 환류	Ⅲ	2	TypeⅡ
14개 항목	14개 평가기준	35개 세부기준	-	50점	-

또한 기술적 보안 영역은 타 보안영역에 비해 자본투자가 요구되는 영역이다. 정보보호시스템 초기구축에는 많은 비용이 들며 이를 정기적으로 업데이트하는 것 역시 비용부담이 따른다. 이러한 이유로 인해 의료기관들이 기술적 보안장치에 대한 필요성은 절감하면서도 실제 우선 자원 투입 대상이 되지 못하고 있는 경우가 적지 않다. 그러나 필수적인 보안 장치가 결여된 정보화야 말로 가장 위험한 정보화이며 제 아무리 관리적 보안, 물리적 보안을 수행하고 있다 하더라도 기술적 보안이 담보되지 않으면 네트워크상에서 불법적 침해요인에 무방비 상태로 노출된다. 따라서 기술적 보안이야 말로 정보기술의 발전과 더불어 향후 더 강화되어야 하는 보안 분야이다.

EMR을 시행하는 대형병원에 대한 평가항목은 14개 항목이다. EMR을 도입한 병원에 대해서는 추적감사, 전자서명, 암호화 도입여부를 평가한다(표 4).

물리적 보안 영역은 전산센터를 비롯하여 의료기관내 전산기기가 놓여있는 모든 곳이 대상이다. 7개 항목으로 구성되며 세부 기준은 12개 항목으로 구성하였다(표 5).

<표 5> 물리적 보안영역(대형병원용)

중분류	평가기준	세부기준	가중치 등급	배점	점수화 방법
전산센터에 대한 출입통제	전산센터에 대한 접근 통제장치의 유무	물리적 통제수단 구비 여부(CCTV, 감시카메라, 사원증 Barcode 등) 주요시스템설치장소별 출입통제여부	Ⅱ	3	TypeⅢ
진료정보 저장기기 보안	전산기기로의 부적절한 접근을 차단할 수 있는가(임의의 장소 선정 평가)	병동 PC의 무방비 상태 여부 외래 PC의 무방비 상태 여부 기타장소 전산기기의 보안	Ⅱ	3	TypeⅡ
안전전원공급	전원공급을 위한 장비	시스템 전원공급을 위한 장비	Ⅱ	3	TypeⅢ
백업센터 장소	DB 백업센터의 운영위치	백업센터 운영의 위치 운영 장소의 안전성	Ⅱ	3	TypeⅡ
시스템설치장소별 비상 계획	정보시스템 설치 장소별 비상 계획	정보자산 설치 장소별 비상계획(화재, 재해 등을 대비한 수립여부	Ⅱ	3	TypeⅡ
비상계획의 테스트	수립된 비상계획의 정기적인 모의 훈련 실시	비상계획의 정기적 테스트 실시여부 테스트 결과의 반영	Ⅱ	3	TypeⅡ
유지보수 관리	장비 유지 보수 내역	유지보수 내역의 관리현황	Ⅲ	2	TypeⅢ
7개 항목	7개 평가기준	12개 세부기준	-	20점	-

2. 평가항목의 점수화 방법

평가항목의 점수화 방법은 다음과 같다(그림 1).

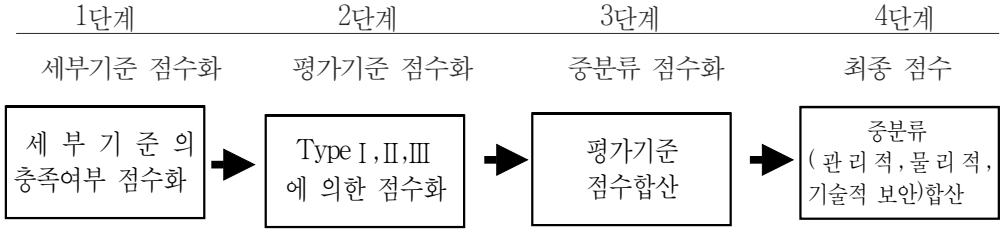

그림 1. 평가항목의 점수화 단계

평가 항목의 점수화를 위한 영역별 배점은 호주의 GPCG 가이드라인 및 체크리스트에서 전문가들이 제시한 IT Security의 중요도와 우선순위[2]와, 병원정보보안 전문가의 정보보안 우선순위에 근거하여 확정하였다. 아울러 정보보안 전문가와 함께 보안수준에 미치는 영향력과 조직의 정상적 기능에서 차지하는 중요성의 크기와 심각성에 따라 항목을 1, 2, 3급으로 분류하였다(1급: 5점, 2급: 4-3점, 3급: 2점). 가중치선정 1급 항목은 보안정책, 악성코드보안, 방화벽, 재해복구계획, 백업, 추적감사, 암호화, 공인전자서명 등이며 이 항목은 5점으로 책정하였다. 이 항목들의 특징은 병원이 전자적인 업무환경에서 정상적인 업무(환자진료)를 수행하기 위해서 필수적인 보안요소임과 동시에 정보의 안전성을 보장하기 위한 활동들이다. 2급 항목으로 '보안교육, 보안감사, 비상운영계획의 테스트'를 분류하고 4점으로, 중요도 면에서 상대적으로 낮은 요소는 3급 항목으로 분류, 2점으로 배점하였다. 2점 배점 항목은 비밀보호 서약서, 유지보수 관리 2개 항목이다(표 3, 4, 5). 세부기준의 유형별 점수화 방법은 다음과 같다(표 6).

<표 6> 세부 기준의 유형별 점수화 방법-대형병원

유형구분	정의	예
Type 1	해당 조사항목에서 제시한 정량화된 기준의 부합여부에 의한 배점	퇴직자의 ID 권한 종료까지의 기간 퇴직과 동시에 → 4점 3일 이내 → 3점 7일 이내 → 2점 14일 이내 → 1점
Type 2	세부기준의 충족율에 의해 점수 결정 100%이면 4점 80%이상 3점 60%이상 2점 40%이상 1점 40%미만이면 0점	보안교육의 내용 8개 중 4개만 충족 개수*해당항목 점수 → 8 × 4 = 32 4개 항목만 실시한 경우 4 × 4 = 16 16/32×100 = 50% 40%이상이므로 1점
Type 3	세부기준의 유, 무에 따라 평가기준의 점수 부여	전자의무기록도입병원이 암호화를 도입한 경우 5점, 미도입인 경우 0점

2) Peter Schattner, The GPCG security project-final report. ⓒ February 2004, p38

3. 평가모형을 이용한 시범평가

개발된 평가모형을 이용하여 병상 수, 종별 등을 고려하여 3개 병원을 사례연구의 대상으로 선정하고 설문지, 전화면담 등을 통하여 조사 분석하였다. A병원은 수도권 소재 대학부속병원으로서 1,000병상을 현재 운영하고 있고 EMR을 부분 시행하고 있는 병원이다. A병원은 관리적 보안은 25점, 기술적 보안 45점, 물리적 보안이 12점으로 총점은 82점이다. 평가항목 충족율은 83%, 기술적 보안이 90%, 물리적 보안이 24%이다.

B병원은 700병상대의 광역시 소재 종합병원으로 EMR을 시행하지 않는 병원이다. 관리적 보안은 시행사항이 전무하여 0점 처리 되었으며 기술적 보안은 34점, 물리적 보안은 9점으로 제한적으로 보안업무를 수행하고 있는 것으로 조사되었다. 전체 평가항목 충족율은 43%이다.

C병원은 광역시에 소재하고 있고 2년 전에 OCS, PACS를 도입한(EMR은 도입 안 함) 병원으로 병상은 350병상 규모이다. 이 병원은 방화벽이 구축되어 있지 않고 보안교육도 시행하지 않고 있으나 무정전 장치와 유지보수내역은 관리하고 있다. 백업과 패스워드 관리는 시행하되 PC 사용자의 윈도우 패치와 바이러스 패치를 등한히 하고 있는 것으로 평가되었다. 이 병원의 경우 최근 2년 동안의 바이러스 피해 경험은 20회 이상이며 저장자료의 손실을 경험하였다. 이 병원의 평가점수는 기술적 보안에서 50점 만점에 31점(충족율 62%), 물리적 보안에서 8점(충족율 40%)을 얻어 종합점수 39점을 기록하였다(표 7).

<표 7> 평가모형을 이용한 3개 병원 평가

대 분 류	A병원	B병원	C병원
관리적 보안	25	0	0
기술적 보안	45	34	31
물리적 보안	12	9	8
총 계	82	43	39

평가 결과 3개병원의 점수는 각각 82, 43, 39점이었으나, 각 병원들의 점수의 50-80%는 기술적 보안에서 취득한 점수로서 관리적, 물리적 보안은 상대적으로 소홀함을 파악할 수 있었

다. 의료기관의 정보보안 활동의 우선순위는 기본적으로 전 병원을 관리대상으로 하는 보안정책의 수립과 보안교육, 정보시스템별 보안시스템 구축으로 요약될 수 있다. 기술적 부분에만 치중되었던 보안대책을 관리적, 물리적 보안과 적절히 통합하는 것은 정보화와 보안활동의 지속적인 균형유지에 필수적이라고 하겠다.

4. 개발된 평가모형의 특징

본 연구에서 개발된 평가모형의 특징은 다음과 같이 요약될 수 있다. 첫째, 기술적 보안과 더불어 지속적 보안유지를 위한 관리적 보안, 물리적 보안을 함께 다루고 있다. 또한 기존 자료에는 아예 없거나 빈약하게 제시되어 있는 전산센터의 보안활동은 물론이고 의료기관 내 모든 PC 사용자의 보안활동 실천여부와 실천정도를 평가대상에 포함하고 있다.

둘째, 평가의 영역을 의료정보가 유통되고 활용되는 범위로 확대 적용한다. 예컨대 프그로램 개발업체 및 CRM 대행업체 등 '외부업체와의 보안협약'과 EMR시행병원이 타 기관으로 자료 전송시 필수적으로 요구되는 '암호화' 등이 대표적인 것이다.

셋째, 정보화 단계와 병원 규모에 따라 평가모형의 선택이 가능하다. 기존 문헌에서는 규모에 관계없이 보안요구사항이 제시되어 있어 취사선택이 불가능하다. 본 모형에서는 전자의무기록을 도입에 따른 보안요구도의 차이를 고려하여 기술적 항목을 구분 적용하고 있다. 특히 중소병원용 평가모형은 최저수준의, 필수적인 내용들을 평가기준으로 제시하여 중소병원들이 현장에서 활용 가능하도록 하였다.

마지막으로 평가항목에 대한 점수화를 시도하였다. 기존 문헌에서는 보안활동의 우선순위에 대한 언급이 없고 단순 권고사항으로 제시되어 있어 병원현장에서 자원 제약에 따른 우선순위 결정에 어려움이 있다. 중요도에 따른 점수 차등화가 본 평가모형의 특징이다.

5. ISMS(Information Security Management System)인증과의 비교

한국정보보호진흥원에서는 정보보호인증관리체계(ISMS)를 도입하여 인증을 받기 원하는 통신서비스 제공자를 대상으로 인증을 실시하고 있다. 본 평가모형과 ISMS는 해당 조직이 체계적으로 정보보호관리 업무를 수행하고 있는가를 평가한다는 점에서는 큰 차이가 없으나 시행의 법적인 근거나 평가대상 및 특징에서 아래와 같은 차이가 있다(표 8).

<표 8> 본 평가모형과 ISMS 비교

구 분	본 평가모형	ISMS (Information Security Management System)
의 미	의료기관의 정보자산을 보관, 활용, 전송하는 데 있어서 정보의 안전성과 신뢰성, 무결성을 확보하기 위한 기술적, 관리적, 물리적 보안수준을 측정하기 위한 평가모형	조직의 주요 정보자산을 보호하기 위해 정보보호관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리· 운영하기 위한 종합적인 체계
법적근거	의료법21조(진료기록부 등), 의료법 21조의 2(전자의무기록), 동법 시행규칙 제18의 2(전자의무기록관리,보존에 필요한 장비)	정보통신망이용촉진 및 정보보호 등에 관한 법률(제47조, 동법 시행규칙 제6조, 제10조)
평가목적	전산화된 정보(환자 진료정보) 등에 대해 해당 의료기관이 필수적 보안활동을 수행하고 있는가를 평가함으로서 병원정보화의 안정적 발전을 실현하기 위함	인증대상기관이 수립· 운영하고 있는 정보보호 관리체계가 인증심사 기준에 적합한지를 심사함으로써 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위함(권고사항)
평가대상	의료기관 (민간,공공병원,전문요양기관,보건소 등)	정보통신서비스제공자:통신사업자, 쇼핑몰, 포털 등, 정보통신서비스를 제공하기 위한 물리적 시설을 제공하는자, 그 밖에 정보통신망을 운영하는 민간사업자 : 일반 제조업 등
평가기준 (인증심사 기준)	-관리적 보안영역 -기술적 보안영역 -물리적 보안역역	-정보보호관리과정 -문서화 -정보보호대책
평가항목	- EMR(O) 대형병원-90개 세부기준 - EMR(×) 대형병원-82개 세부기준 - EMR(O) 중소병원-72개 세부기준 - EMR(×) 중소병원-56개 세부기준	-137개 통제사항
특 징	-관리적, 기술적, 물리적 부문으로 평가 -병상규모,정보화 단계별 평가모형 제시 -각 보안 영역 간 배점을 통한 차등화 -의료기관평가, 병원신임평가에 활용될 것을 목적으로 함	- 국내 실정에 적합한 정보보호관리모델제시 - 정보보호 전문기관(KISA)에 의한 인증 - 국내 최고의 전문가들에 의한 인증 심사 - 기술심사 강화를 위한 모의진단(요청시) - 정보보호 인증을 목표로 함

Ⅳ. 결론 및 제언

국내 병원의 정보화가 가속화되면서 환자 진료정보의 보안이 핵심과제로 대두되고 있다. 그러나 이러한 정보보안의 중요성에 비해 보안 분야의 연구가 활발하지 않아 병원 정보보안에 대한 지침이 제안된 바 없고, 이는 현장에서 정보보안을 어떻게 실천해야 하는지에 대한 정보부족으로 이어지고 있어 진료정보의 보호를 더욱 어렵게 만드는 요인이 되고 있다. 따라서 의료기관 정보보안에 관한 가이드라인이나 체크리스트가 시급히 마련되어야 할 필요성이 있으므로 본 연구에서는 국내 의료기관의 정보보안 수준을 평가하기 위한 평가모형을 개발하였다. 평가지표를 관리적, 기술적, 물리적 보안항목으로 구분하고 병원규모와 정보화 정도에 따라 평가항목을 차등화 하여 최종적으로 대형병원용과 중소병원용, EMR 시행병원을 위한 평가모형을 개발하였다. EMR 시행병원과 Non EMR 병원의 평가항목의 차이는 기술적 보안부문이다. 중소병원용 평가모형은 대형병원용에 비해 최소한의 보안기준을 제시하였다. 본 논문에서 개발된 평가기준은 의료기관 내에서 보안역량을 강화하기 위한 자체 평가용으로 활용할 수 있다. 나아가 평가항목을 의료기관평가, 병원신임평가 등에서 정보보안 수준을 객관적으로 측정하는 도구로 활용하여 정보보안이 더 이상 병원 업무의 우선순위에서 제외되지 않도록 지속적 관심과 환기가 필요하다. 향후 각 평가항목별 정보보안 효과에 대한 연구도 시행되어야 할 것이다.

의료기관 정보보안은 정보화시대의 성과와 성패를 결정짓는 핵심요소이다. 이러한 병원 정보보안의 중요성이 실제 현장에서 보안업무로 현실화되기 위해서는 법·제도의 정비와 보완이 필요하다. 업무수단의 전산화를 기반으로 의료정보는 병원 내·외에서 다양한 목적으로 여러 사람들에 의해 처리되고 있다. 그러나 현행 법률은 이러한 업무 처리단계에서 어떠한 보안장치가 필요한지, 단계별 보안책임은 누구에게 부여되는지에 대한 원칙이 없고 단지, 의료인의 윤리적 책임만을 강조하는 수준에 머물러 있어 현실성이 없다. 또한 전자의무기록의 보안에 관한 법률에 의하면 ‘네트워크에 연결되지 아니하는 백업저장 시스템의 설치’를 의무화하고 있으나 이를 준수하지 않는 기관도 있는 것으로 나타나 실효성에 의문이 제기된다. 따라서 정보보안에 대한 변화된 책임소재를 명시하고 정보화 수준에 따른 보안요건을 명확하게 정의하는 등의 제도보완이 필요하다.

또 병원에 산재한 개인 의료정보의 안전한 관리를 위해서는 무엇보다 정보 취급자 및 사용자의 보안인식이 선행되어야 한다. 의료기관이 환자의 정보에 대한 선량한 관리자의 책무

를 다하기 위해서는 보안업무가 일상적 업무가 되어야 한다. 또한 개인 진료정보의 생명주기 단계별로 명확한 보안원칙이 적용되어야 한다. 이러한 정보보안 문화 성숙은 의료기관이 의료 소비자의 신뢰를 얻기 위해서도 반드시 필요하다.

마지막으로 의료기관의 정보보안 활동을 리드할 정보보안 책임자의 역할이 필요하다. 병원정보화로 보안의 책임이 전산센터를 비롯하여 각 부서, 사용자에게로 이전되고 있다. 분산되고 편재하는 보안책임은 자칫 형식에 치우치거나 효과적인 보안업무의 실천을 방해하는 요소가 될 수 있다. 이러한 문제점을 해결하기 위해서는 보안업무를 총괄하고 조직전체의 정보보안활동을 리드할 정보보안 책임자를 선정하여 지속적이고 장기적으로 보안업무를 진행할 필요가 있다. 보안책임자의 리더쉽은 조직의 보안목표를 효과적으로 달성할 수 있게 하는 역할을 할 수 있을 것이다.

참 고 문 헌

곽연식, 미국의 의료정보 보안동향, 2001

김옥남, 진료정보의 등록 및 조사사업에서의 효율적인 자료수집과 개인정보보호방안, 2003

대한의사협회, 개인진료정보누출과 국민사생활보호대책 심포지엄 자료집, 2004

보건산업진흥원, 의료기관평가 결과종합방안, 2003

오향순, 국내 종합병원 병원감염관리 현황 및 평가지표와 모형개발,
서울대학교 보건대학원 박사학위 논문, 2005

이인영, 개정 의료법의 환자의 개인정보 보호규정에 관한 법리적 고찰, 한림법학포럼 제11권, 2002

정보통신부 고시 제 2005-18호, 개인정보의 기술적·관리적 보호 조치 기준, 2005

정보통신부, 정보통신망 침입차단 시스템평가기준, 2000

한국정보보호진흥원, 정보보호관리체계(ISMS) 인증제도, 2005

홍준현, 의무기록정보관리학, 고문사, 2005

KT, 보건의료정보개인프라이버시 보호기술, 2004

일본, 의무기록 전자매체 보존에 관한 법률

電子保存された診療錄情報の交換のためのデータ項目セツトの作成 報告書:The Japanese Set of Identifiers for Medical Record Information Exchange(J-MIX)

AMC, Guidelines for Academic Medical Centers on Seucurity and Privacy, 2001

American Medical Association, HIPAA Security Preparedness, 2005

British Medical Association, Clinical System Security Interim Guidelines, 1996 http://www.ftp.cl.cam.ac.uk/users/rja14/guidelines.txt

Dave Kirby, HIPAA, Security, and Privacy in Academic Medical Centers : Guidelines for Department of Health and Human Services, Health Insurance Reform: Security standards; Final Rule, 2003

Edward H. Shortliffe et al. Medical Informatics-Computer Application in Health Care and Biometics, Springer, 2001

Federal Register 68, no.34(February 20, 2003)

General Practice Computing Group, Security Self Assessment Guide for General Practitioners and Computer Security Checklist. The Department of General Practice, Monash University,2004

National Institute of Standard and Technology, Technology Administration, U.S. Department of Commerce, An Introduction to Computer Security : The NIST Handbook(Special Publication 800-12), 1999

Nick Gaunt. Security Of The Electronic Health Care Record - Professional And Ethical Implications, UK

OECD, Guidelines for the Security of Information Systems and Networks. 2002

Peter Schattner, The GPCG computer security self-assessment guide and check-list for general practitioners 1st edition, 2004