

PACS에서 보안관리 평가기준 연구와 실태조사

— Research on a Valuation Standard and the Actual Condition About Security Management in PACS —

경희의료원 PACS팀¹⁾ · 광운대학교 전자공학과²⁾ · 광주보건대학 방사선과³⁾
조선대학교 원자력공학과⁴⁾ · 신홍대학 방사선과⁵⁾ · 신구대학 방사선과⁶⁾
정재호^{1,2)} · 동경래^{3,4)} · 권대철⁵⁾ · 손기경¹⁾ · 김현수⁶⁾ · 강희두¹⁾

— 국문초록 —

본 연구는 의료기관 PACS 운영 및 영상정보관리 과정에서의 개인정보보호와 보안 관리에 대한 보안평가 기준 및 보안평가에 따른 등급기준을 마련하고자 하였다. 보안평가기준과 보안평가 등급기준의 지표를 도출하기 위해 ISO17799(BS 7799), HIPPA(Health Insurance and Portability and Accountability Act of 1996), 국내 의료법 등을 참조하여 정책적 보안, 기술적 보안, 데이터관리 보안, 물리적 보안 등 4가지 항목을 대분류로 선정 후 10개의 세부 평가항목을 선정하여 점수화 하였다. 도출된 보안평가기준과 보안등급의 지표를 가지고 30곳의 의료기관에서 조사를 시행하였다. 대분류의 평가 요소 중 물리적 보안 항목의 전체 의료기관 평균 점수는 20점 만점기준 18.5점(93%)으로 가장 우수한 점수를 나타내었으며, 정책보안항목 30점 기준 18.5점(62%), 데이터관리 보안항목 20점 기준 12점(60%), 기술적 보안항목 30점 기준 17.5점(58%) 순임을 알 수 있었다. 30개 종합병원의 보안평가 점수는 평균 67점으로 4등급 수준을 나타내었다. PACS환경에서 취약한 개인정보보호 및 보안의식에 대한 관리기준 수립이 필요하다.

중심 단어 : 개인정보보호, PACS 보안평가, 평가지표

I. 서 론

오늘날 많은 의료기관이 컴퓨터를 이용하여 정보를 저장, 관리, 이용하여 업무를 수행하고 있다. 의원급 의료기관부터 초대형 의료 기관에 이르기까지 많은 의료 기관들이 각종 정보시스템을 도입하고 있으며, 또한 인터넷을 통한 의료정보의 전송 및 공유, 활용이 확산되고 있다¹⁾. 지금까지의 의료정보화는 기존 원무 중심의 의료정보 전

산화 및 전산 통합 수준으로 주로 진행되어 왔다. 하지만 오늘날과 같은 발달된 정보통신기술로 인해 의료영상정보를 전송, 관리하는 의료영상 전송시스템(Picture Archiving Communication System, PACS)과 처방전달시스템(Order Communication System, OCS), 전자의무기록(Electronic Medical Record, EMR) 등이 개발되어 의료 전반에 걸쳐 정보화가 구축되어 운용되고 있는 실정이다²⁾. 이러한 의료과학기술의 발달로 개인의 의료정보는 컴퓨터에 저장되며 사용자 편리성에 맞추어서 개발, 운영되고 있는 것이 현실이다. 따라서 엄격하게 지켜져야 할 개인의료정보는 가장 민감한 정보이고 사생활보호가 강조되어야 할 정보임에도 불구하고 보안상의 많은 문제점들을 노출하고 있다. 실제로 보안사고의 70% 이상이 내부 관련자에 의해

*접수일(2008년 9월 29일), 심사일(2008년 11월 20일), 채택일(2008년 11월 28일)

교신저자: 강희두, (130-702) 서울 동대문구 회기동 1번지
경희의료원 PACS팀
TEL : 02-958-8891, FAX : 02-958-8631
E-mail : xheedoo@hanmail.net

초래³⁾ 된다고 할 만큼 내부관련자의 업무 형태 및 보안 인식이 중요한 요소이다. 또한, 개인의료정보에 대한 침해는 명백한 헌법상 개인정보자기결정권을 침해했다고 할 수 있다⁴⁾. 의료정보의 큰 부분을 차지하는 처방전달시스템(Order Communication System, OCS)은 2002년 개정으로 의료법에 개인정보보호방안에 대하여 규정되어 있다⁵⁾. 또한, 제도적으로 충분한 보안을 하고 있고 많은 연구와 조사가 이루어지고 있다. 하지만 의료영상전송시스템(PACS)은 그 중요성에 비해 보안 및 관리체계에 대한 관련 법규⁶⁾ 및 조사가 이루어져 있지 않다. 또한 PACS 환경에서 데이터 정보 변경에 대한 변경기록 관리, 영상자료 대출(DATA CD) 신청 시 의무기록에 준하는 확인 절차 등은 보안관리 측면에서 주요한 항목임에도 불구하고 잘 지켜지지 않고 있다. 이에 본 연구에서는 정보보안에 관련된 국제적인 규격 및 권고안을 분석하여 국내 의료법에 부합하는 PACS에서의 영상정보관리부문 보안 평가 기준과 평가에 따른 등급 기준 지표 도출 연구를 시행하였다. 또한 도출된 보안평가기준과 보안평가등급의 지표를 이용하여 각급 의료기관의 영상자료 관리실태를 조사하여 의료영상정보 부문 보안 관리의 지표의 제정, 보안의식에 대한 교육 등의 기본 자료로 제공하고자 한다.

II. 연구 범위 및 방법

1. 보안평가 기준 및 보안평가 지표 도출 연구

PACS환경에서 보안 및 개인정보보호 차원의 평가 지표⁷⁾를 도출하기 위해 ISO17799(BS 7799), HIPPA (Health Insurance and Portability and Accountability Act of 1996), 국내 의료법 등을 참조하여 정책적 보안, 기술적 보안, 데이터관리 보안, 물리적 보안 등 주요한 보안항목을 대분류로 선정하였다. 대분류 항목을 기준으로 각 항목마다 구체적인 평가 요소들을 나열하여 소분류 항목으로 분류하였으며 이를 토대로 세부평가항목을 도출하였다(Table 1). 세부평가 항목에 따른 가중치 또는 점수의 근거로서의 관련 연구와 자료로부터 보증 수준 및 등급 분류 안을 도출하였으며, 최종적으로 도출된 PACS에서의 영상정보관리부문 보안 평가 기준과 평가에 따른 등급 기준 지표에 따라 보안 분류항목별 가이드라인 및 가중치 등을 제시하였다.

2. 보안관리 실태 조사 연구

도출된 보안평가기준과 보안평가등급의 지표를 가지고 의료법 제 3조 3항의 종합병원 기준에 해당하는 서울 경

Table 1. Security valuation index according to each classified list in PACS security

대분류 항목별 점수	소분류	세부 평가 항목	평가점수
정책적 보안(30점)	PACS 운영업무 전담부서 유·무	PACS팀(운영 전담 부서) 구성 되어 있음	10점
	PACS 보안 정책 수립 유·무	PACS 운영 전반의 보안 정책 있음	10점
	보안 정책 및 중요성에 대한 사용자 교육 유·무	의료정보보안에 대한 관리자 및 사용자 교육 실시(1회/년이상)	10점
기술적 보안(30점)	PACS관리자, 판독자 및 일반사용자 ID관리 퇴직자 ID 관리(삭제 및 갱신 여부)	PACS 관리자 ID, password는 일정기간마다 갱신 하여 사용한다. PACS 사용자(판독자 및 일반사용자)가 퇴직 시 삭제 및 갱신 한다.	10점 5점
	시스템 미사용시 자동 로그아웃 기능 사용여부	PACS에 로그인 후 일정시간 미사용시 자동 로그아웃을 사용한다.	5점
	사용자 권한에 따른 사용권한 분류 및 관리	사용자 구분에 따른 사용권한을 분류관리한다. (특정 아이디를 공유하여 쓰지 않는다.)	10점
	PACS 데이터 대출업무 시 절차 관리	영상자료 대출(DATA CD) 신청 시 위임장, 본인확인서 등의 절차를 통해 대출업무를 진행한다.	10점
데이터 관리 보안(20점)	데이터 정보 변경 관리	데이터 정보 변경 시 일정 절차에 따른 변경과 변경기록을 남긴다.	5점
	바이러스 및 해킹 여부	바이러스에 의한 PACS 사용 불능이 없다(사용자 PC 포함)	5점
물리적 보안(20점)	데이터 백업 실시 여부(2차백업, 3차백업)	데이터 백업 시 2차 백업(5점), 3차 백업(10점)을 실시 하고 있다.	5점,10점
	전산 센터 출입 통제 여부	전산센터(PACS 서버 및 저장장치) 출입 시 본인인증 절차가 있다.	5점
	백업 센터 장소의 안전성 여부	2차 및 3차 백업 시스템은 별도 제3의 장소에 안전하게 보관한다.	5점

기지역 30곳의 의료기관에서 조사를 시행하였다.

조사기간은 2008년 7월 1일부터 8월 31일까지 2개월 동안이며 조사방법은 현장방문 조사, 우편 접수 조사, E-mail 조사 등을 시행하였다.

또한 기술적 보안 항목 중에서 ISO17799, HIPPA, GPCG에서 공통적으로 주요 하게 다루지는 사용자권한에 따른 사용권한 분류를 조사하였다. 조사 내용은 판독부분 2개, 데이터관리 부분 5개, 자료전송 및 출력 부분 2개, 조회 부분 1개를 선정하였다.

III. 결 과

1. 보안평가 기준 및 보안평가 지표 도출 연구 결과

PACS 환경에서 보안 및 개인정보보호 차원의 평가 지표를 수립하고 PACS에 대한 보안평가를 통해 보안측면에서 다양한 통제 방안을 마련하고자 하였다. ISO17799(BS 7799), HIPPA(Health Insurance and Portability and Accountability Act of 1996), 국내 의료법 등을 참조하여 세부평가 항목은 각각 점수를 부여하였으며 보안성 평가 부문에서의 측정 스케일⁸⁾은 국제공통 평가기준인 Common Criteria(CC)⁹⁾, 한국정보보호 평가기준¹⁰⁾ 등을 참조하여 보안기능의 보증수준을 6단계로 분류하여 평가

하였다. 각 항목별 점수 합계는 백점이며, 1등급(90~100점), 2등급(80~89점), 3등급(70~79점), 4등급(60~69점), 5등급(50~59점), 6등급(1~49점)으로 분류하였다. 이때 대분류 4가지의 항목별 가중치는 PACS의 보안 측면에서 중요하게 인식되는 기술적 보안과 데이터관리 보안은 각각 30%의 가중치를 부여하였고, 정책적 보안과 물리적 보안은 상대적으로 낮은 20%의 가중치를 부여하였다 (Table 2). 가중치에 대한 근거는 ISO17799(BS 7799), HIPPA, 국내 의료법, MEDIS-DC(일본 전자기록 연구기구), 호주개원의 체크리스트-GPCG(General Practice Computing Group, Computer Security Check-list) 등을 근거로 하여 각 표준기구에 공통적으로 중요하게 거론되는 항목들에 30%의 비중을 두었고 그 외의 항목에 대하여서는 20%의 비중을 두었다.

2. 보안관리 실태 조사 연구 결과

ISO17799(BS 7799), HIPPA(Health Insurance and Portability and Accountability Act of 1996), 국내 의료법 등을 참조하여 수립된 PACS 보안 분류항목별 보안평가 지수를 적용하여 서울 및 수도권 종합병원 과 지방대도시 종합병원 30곳을 대상으로 하여 종합병원 이상의 의료 기관들의 PACS 보안 실태를 알아보았다. 분류 항목별 평가를 통해 전체 보안 평가를 측정하였으며 이를 토대로 대분류 항목별 평가결과 비교 및 사용자 권한에 따

Table 2. Basis standard guide line and weight according to each itemized security list

대분류	가중치	소분류	관련 근거 표준 가이드라인
정책적 보안	30%	PACS 운영업무 전담부서 유 무(보안관리책임자)	ISO17799, HIPPA, MEDIS-DC, GPCG
		PACS 보안정책 수립 유 무	ISO17799, MEDIS-DC, GPCG
		보안정책 및 중요성에 대한 사용자 교육 유 무	ISO17799, HIPPA, MEDIS-DC, GPCG
기술적 보안	30%	PACS관리자(Admin), 판독자 및 일반사용자 ID의 password 관리 퇴직자 ID 관리(삭제 및 갱신 여부)	ISO17799, HIPPA, GPCG
		시스템 미사용시 자동 로그아웃 기능 사용여부	ISO17799, HIPPA, GPCG
		사용자 권한에 따른 사용권한 분류 및 관리	ISO17799, HIPPA, GPCG
데이터 관리 보안	20%	PACS 데이터 대출업무 시 절차 관리	HIPPA, GPCG, 의료법 시행규칙
		데이터 정보 변경 관리	의료법 시행규칙
		바이러스 및 해킹 여부	ISO17799, HIPPA,
물리적 보안	20%	백업 센터 장소의 안전성 여부	GPCG, 의료법 시행규칙
		전산 센터 출입 통제 여부	HIPPA
		데이터 백업 실시 여부(2차백업, 3차백업)	ISO17799, 의료법시행규칙

Table 3. Security valuation result according to each detail classified list

대분류	가중치	소분류	결과
정책적 보안	30%	PACST팀(PACS 보안관리 책임자 포함) 구성 되어 있음	13 (43%)
		PACS 운영 전반의 보안 정책 있음	30 (100%)
		의료정보보안에 대한 관리자 및 사용자 교육 실시(1회/년이상)	12 (40%)
기술적 보안	30%	PACS 관리자 ID, password는 일정기간마다 갱신 하여 사용한다.	16 (53%)
		PACS 사용자(판독자 및 일반사용자)가 퇴직 시 아이디를 삭제 및 갱신 한다.	25 (83%)
		PACS에 로그인 후 일정시간 미사용시 자동 로그아웃을 사용한다.(2시간 이내)	11 (37%)
		특정 아이디나 패스워드를 공유하여 쓰지 않는다.(관리자 제외)	19 (67%)
데이터 관리 보안	20%	영상자료 대출(DATA CD) 신청 시 위임장, 본인확인서 등의 절차를 밟는다.	23 (77%)
		데이터 정보 변경 시 일정 절차에 따른 변경과 변경기록을 남긴다.	18 (60%)
		바이러스에 의한 PACS 사용 불능이 없다(사용자 PC 포함)	13 (43%)
물리적 보안	20%	데이터 백업 시 2차 백업을 실시 하고 있다.	30 (100%)
		데이터 백업 시 3차 백업을 실시 하고 있다.	21 (70%)
		전산센터(PACS 서버 및 저장장치) 출입 시 본인인증 절차가 있다.	8 (27%)
		2차 및 3차 백업 시스템은 별도 제3의 장소에 안전하게 보관한다.	2 (7%)

Table 4. PACS security valuation result of each medical institution using the deduced security valuation index

의료기관	정책보안 (30)	데이터관리 보안(20)	기술적 보안(30)	물리적 보안(20)	총평가 점수	보안 등급
A	30	15	0	20	65	4
B	10	10	15	20	55	5
C	10	10	15	20	55	5
D	20	10	10	20	60	4
E	20	10	20	20	70	3
F	20	10	20	20	70	3
G	30	5	30	20	85	2
H	20	15	15	20	70	3
I	10	10	20	20	60	4
J	10	15	10	15	50	5
K	20	20	30	15	85	2
L	10	10	25	20	65	4
M	20	15	15	15	65	4
N	10	10	15	15	50	5
O	20	15	25	15	75	3
P	30	15	30	15	90	1
Q	20	10	15	15	60	4
R	20	15	15	20	70	3
S	10	20	25	20	75	3
T	20	15	20	20	75	3
U	20	10	30	20	80	2
V	20	5	25	15	65	4
W	30	15	10	20	75	3
X	20	0	10	20	50	5
Y	10	10	15	20	55	5
Z	20	15	15	20	70	3
AB	20	10	5	20	55	5
AC	20	15	5	20	60	4
AD	20	10	25	20	75	3
AE	20	10	20	20	70	3
평균	18.5 (62%)	12 (60%)	17.5 (58%)	18.5 (93%)	67	4

Table 5. classification result of usable authority according to user's authority

항목별 권한 user_level	데이터 관리				Create, Edit	판독		자료전송 및 출력		조회 Hideimage, Showimage
	Edit information	Verify, Save	Delete	Merge		1차판독	최종판독	DICOM transfer	CD출력	
Administrator	30(100%)	30(100%)	30(100%)	30(100%)	28(93.3%)	13(43%)	13(43%)	30(100%)	26(87%)	30(100%)
영상의학과전문의	3(10%)	18(60%)	3(10%)	6(20%)	6(20%)	24(80%)	30(100%)	16(53%)	4(13%)	12(40%)
영상의학과수련의	3(10%)	17(57%)	3(10%)	6(20%)	6(20%)	24(80%)	12(40%)	10(33%)	3(10%)	11(36.7%)
방사선사	16(53%)	27(90%)	21(70%)	20(66.7%)	16(53%)			22(73%)	22(73%)	20(66.7%)
일반전문의	1(3.3%)	2(6.7%)			1(3.3%)	2(6.7%)	1(3.3%)	4(13%)		7(23.3%)
일반임상수련의	1(3.3%)	2(6.7%)			1(3.3%)			4(13%)		7(23.3%)
Guest								3(10%)	2(6.7%)	3(10%)

른 사용권한 조사를 실시하였다. 평가결과는 정책적 보안 항목의 소분류 항목인 PACS 보안관리 책임자를 포함한 PACS팀이 구성된 곳은 조사대상 중 13곳(43%)의 비율이며, 조사대상의 모든 의료기관이 PACS 운영 관련 보안정책을 가지고 있다고 답하였으며, PACS관련 내부직원 보안교육(년 1회 이상)을 실시하는 곳은 12곳(40%)이었다. PACS 관리자 ID, 비밀번호를 일정기간마다 갱신하는 곳은 16곳(53%), PACS사용자가 퇴직 시 아이디를 관리하는 곳은 25곳(83%)으로서 비교적 높은 비율을 보였다. 영상자료 대출(DATA CD) 신청 시 위임장 또는 본인확인서, 신분증 등의 확인 절차를 거치는 곳은 23곳(77%)이며, 데이터 정보 변경 시 변경기록을 남기는 곳은 18곳(60%)이다. 데이터 백업 시 2차 백업은 30곳(100%), 3차 백업은 21곳(70%)의 의료 기관에서 실시하고 있다. 2차 및 3차 백업용 저장장치를 PACS서버 및 저장장치가 설치된 곳이 아닌 별도의 안전한 장소에 보관하는 곳은 2곳(7%)에 불과하였으며, 전산센터 출입 시 본인인증 절차를 거치는 곳은 8곳(27%)으로 조사되었다(Table 3). 대분류의 평가요소 중 물리적 보안 항목의 전체의료기관 평균점수는 20점 만점기준 18.5점(93%)으로 가장 우수한 점수를 나타내었으며, 정책보안항목 18.5점(62%), 데이터관리 보안항목 12점(60%), 기술적 보안항목 17.5점(58%) 순임을 알 수 있었으며, 30개 종합병원의 보안평가 점수는 평균 67점으로 4등급 수준을 나타내었다(Table 4). 사용자 권한에 따른 사용권한 분류 결과는 사용자 등급별로 사용권한에 대한 적절한 통제와 관리를 하고 있는지에 대한 조사이다. 30개의 종합병원을 대상으로 조사하였다. 데이터관리 부문에서 PACS 관리자가 영상삭제 권한을 보유한 곳이 30곳(100%), 방사선사 21곳(70%), 영상의학과 전문

의, 수련의는 각각 3곳(10%)의 비율로 삭제권한을 가지고 있었다. PACS 데이터의 환자고유정보를 변경할 수 있는 권한은 PACS 관리자가 30곳(100%), 방사선사 16곳(53%), 영상의학과 전문의, 수련의 각각 3곳(10%)의 비율을 보였다. PACS 데이터의 생성과 변경기능은 PACS 관리자가 28곳(93%), 방사선사 16곳(53%), 영상의학과 전문의, 수련의 6곳(20%)으로 조사되었다(Table 5).

IV. 고찰 및 결론

개인정보보호의 측면에서 적극적으로 지켜져야 할 의무이며 엄격하게 관리되어야 할 환자의 영상정보는 시스템 관리자 및 의료작업 종사자의 부주의 및 보안인식저하로 인해 심각한 상황을 초래할 수 있다. 해킹과 악의적 코드, 관리자의 부주의 등에 의한 이름(명의)이나 아이디, 비밀번호, 금융 및 신용정보 등 개인정보의 도용과 유출로 인한 피해사례들은 언론과 방송매체를 통해 매우 흔하게 보도되고 있다¹¹⁾. 따라서 의료기관내 PACS 관리자 및 사용자들의 아이디, 비밀번호의 유지 및 관리¹²⁾는 주요한 요소인데도 불구하고 기술적 보안 항목요소 중 PACS 관리자 아이디, 비밀번호의 갱신은 53%, 특정 아이디에 대한 공동사용이 33%, 일정시간 사용하지 않았을 때 로그아웃 기능은 37%만이 지키고 있어 이에 대한 보완이 필요하다. PACS 보안관리 책임자를 포함한 PACS팀이 구성된 곳은 조사기관 중 43%이었으며, PACS에 대한 보안정책은 조사기관 모두 유지하고 있는 것으로 나타났다. 데이터관리 보안 측면에서 영상자료 대출신청 시 위임장, 대출확인서, 신분증 등의 확인 절차를 통해 발급하는 곳

은 23곳(77%)으로 비교적 많은 곳에서 의무기록 발급에 준하는 절차를 밟고 있다. 물리적 보안 항목 요소에서는 2차 데이터 백업은 30곳(100%), 3차 데이터 백업은 21곳(70%)에서 백업을 실시하고 있으며 백업용 저장장치를 별도의 안전한 곳에 보관하는 곳은 2곳(7%)에 불과해 이에 대한 보완이 필요하다. 사용자 권한별 조사에서는 데이터관리 부문의 중요요소인 영상삭제 권한¹³⁾, 데이터 환자정보 변경 등은 PACS팀에서 신중히 관리하여야 함에도 영상의학과 전문의 및 수련의(삭제 : 10%, 정보변경 : 10%, 데이터생성 : 20%), 촬영실 근무 일반 방사선사(삭제 : 70%, 정보변경 : 53%, 데이터생성 : 53%)에게도 권한이 주어져 이에 대한 관리 및 보완이 필요하다. 본 연구에서는 PACS환경의 보안평가를 객관적으로 평가할 수 있는 기준을 수립하였으며 이를 근거로 종합병원의 PACS 관리 보안실태 조사를 통해 관리자 및 작업종사자의 보안 의식을 고취하는데 의의를 두고 있다. 또한, 조직의 정보관리체계가 가지고 있는 취약점을 찾아서 이를 보완할 수 있는 다양한 통제 방안들을 도입함으로써 조직의 정보에 대한 다양한 위협들에 대해 정보를 보호할 수 있다¹⁴⁾. 이러한 정보보호 체계를 효율적으로 구축하기 위해서는 체계적인 절차를 따르는 것이 바람직하며 정확하고 현실적인 평가기준이 마련되어 엄격한 관리기준이 수립되어야 할 것이다.

참 고 문 헌

1. 김동수 : e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향, 13:128-148, 2006
2. 김신효 : 의료정보화 및 보안 기술 표준화 동향, 한국홈네트워크산업협회, 2007
3. <http://chan.msn.co.kr/article/2008/09/08/200809081731061320.html?from=Computer>
4. 전영주 : 의료법상 의료정보 보호방안, 28:465-483, 2007
5. 길준규, 이희성 : 의료정보상 개인정보보호방안, 6:117-139, 2006
6. Liu BJ, Zhou Z, Huang HK : A HIPAA-compliant architecture for securing clinical images, Progress in Biomedical Optics and Imaging - Proceedings of SPIE, 5748:326-333, 2005
7. 안선주, 권순만 : 의료기관의 정보보안 수준 측정을 위한 평가모형 개발, 10:98-112, 2005
8. 최상수, 방영환, 최성자, 이강수 : 보안관리 및 위험 분석을 위한 분류체계, 평가기준 및 평가스케일의 조사연구, 13:38-49, 2003
9. CC. Common Criteria for information Technology Security Evaluation, Version 2.1. CCIMB-99-031, http://www.commoncriteria.org/site_index.html, 1999
10. 정보통신부고시 1998-19호 : 정보통신망 침입차단시스템 평가기준 평가지침서, 정보통신부, 1998
11. 정현백 : 디지털 프라이버시와 공공부문의 정보관리, 29:183-204, 2006
12. Myers J, Frieden TR, Bherwani KM, Henning KJ : Privacy and public health at risk : Public health confidentiality in the digital age, American Journal of Public Health, 98:793-801, 2008
13. Bushberg JT : The essential physics of medical imaging, 80-81, 2002
14. 한국정보보호학회 한국정보보호진흥원 : 정보보호 관리 및 정책, 한국정보보호학회 편, 30-32, 2002

• Abstract

Research on a Valuation Standard and the Actual Condition About Security Management in PACS

Jae-Ho Jeong^{1,2)} · Kyung-Rae Dong^{3,4)} · Dae-Cheol Kweon⁵⁾
Gi-Gyeong Son¹⁾ · Hyun-Soo Kim⁶⁾ · Hee-Doo Kang¹⁾

¹⁾*Department of PACS Team, Kyung Hee Medical Center*

²⁾*Department of Electronics, Kwang Woon University*

³⁾*Department of Radiological Technology, Gwangju Health College University*

⁴⁾*Department of Nuclear Engineering, Chosun University*

⁵⁾*Department of Radiological Technology, Shinheung College University*

⁶⁾*Department of Radiological Technology, Shingu College*

This study is to prepare an evaluation standard about personal information protection and security management of a medical institution and to build up a grade standard of evaluation in PACS environment. We built up evaluation index based on 10 detailed items in four big categories (political security, technical security, data management security and physical security) by referring to ISO17799 (BS 7799), HIPPA (Health Insurance and Portability and Accountability Act of 1996) and domestic medical law. We have investigated at the thirty places where medical facility with the extracted security criteria and security evaluation index. Average score of physical security list, one of the big categories, was 18.5/20 (93%) at all medical institutions. Political security score was 18.5/30 (62%), data management security score was 12/20 (60%) and technical security score was 17.5/30 (58%). Therefore, security evaluation score was average 67 in 30 general hospitals, which was 4th level. The results showed that it is necessary to establish evaluation and management standard about personal information protection and security consciousness which are weak in PACS environment.

Key Words : Personal information protection, PACS security valuation, Valuation index