한국위기관리논집 제9권 제8호 2013. 08 47~66쪽

의료기관의 IT 거버넌스를 위한 병원 직원의 개인정보 관리 현황 조사연구

정혜정*, 김남현**

IT 거버넌스의 목적은 정보기술 성과가 조직의 목적과 연계되어 효익 실현에 부합하도록 하는데 있고 이를 위하여 IT 거버넌스는 위험 관리와 가치 전달이라는 두 가지 현안을 다루게 된다. 위험 관리는 조직의 목적을 달성하기 위하여 자산이 가진 취약성과 위협을 식별하고 자산의 가치를 기준으로 하여 위험을 대응할 수 있는 수준으로 감소시키기 위한 대책을 결정하는 프로세스를 말한다. 사람은 조직의 자산으로 기여하지만 조직에 피해를 입힐 수 있는 위협의 요인이자 위험을 유발하는 취약성이 될 수 있으며 이러한 취약성과 위협이 제대로 파악되지 않을 경우에 조직은 위기에 빠질 수 있다. 개인정보는 현대 조직의 최우선 자산인 동시에 정보주체의 프라이버시권 대상 인자라는 양면성을 가지고 있는데 현행 개인정보 보호 관련 법률은 고유식별정보와 민감정보의 처리를 엄격하게 제한하고 있지만 의료기관은 진료라는 본연의 목적을 달성하기 위하여 필연적으로 고유식별정보와 민감정보를 다루게 된다. 본 연구는 의료정보를 취급하는 병원 직원을 대상으로 그들의 정보 관리 현황을 조사하여 내재된 취약성을 파악하고 의료정보가 위협으로부터 안전한 상태인지 여부를 확인하고자 이행되었다. 특정 대학병원 직원들을 대상으로 구조적 설문도구를 이용하여 관련 법제도가 제시 또는 의무화한 개인정보취급자의 정보처리 조치에 준하는 패스워드 관리를 포함한 정보시스템 접근 관리와 암호화를 중심으로 자료를 수집하였다. 연구 결과 응답자의 약 70%가 사용하는 패스워드에서 취약성이 발견되었으며 1/3의 응답자는 패스워드를 타인과 공유하는 것으로 나타났다. 운영체제 접근 시 패스워드를 설정하는 응답자는 50.6%였으며 31.2%만이 자리를 비울 때 로그오프를 하는 것으로 조사되었다. 분실・도난・유출 등으로부터 보호되어야 하는 중요 정보를 개인용 저장장치에 보유하고 있는 직원은 48.5%였으며 해당 정보에 암호화 조치를 이행하고 있는 직원은 그 중 약 1/4에 그쳤다. 효과적인 위험 관리는 조직의 위험 성향에 대한 명확한 이해에서 시작된다. 연구의 한계에도 불구하고 본 연구 결과가 의료정보를 취급하는 조직들이 스스로의 취약성을 이해하고 전사적 차원의 위험 관리 전략을 수립하는데 의미 있는 자료가 될 것으로 기대한다.

주제어: 위험 관리, 취약성 진단, 접근 통제, 의료기관, 의료정보, 패스워드, 개인정보 보호

Ⅰ. 서론

* 제1저자, ** 교신저자.

위기(crisis)란 위협이 축적되어 위험 수준이 극한점에 다다른 상태를 말한다. 위험(risk)에 대한 정의는 분야에 따라 학자에 따라 다양하게 논의되어 왔는데 Yates & Stone(1992)은 위험이 잠재적 손실(potential losses), 그 손실의 의미(the significance of those losses)와 불확실성(the uncertainty of those losses)으로 구성된다고 주장하였으며 Barki, *et. al.*(1993)은 손실 발생 가능성(probability)과 그 손실의 중대성(significance) 또는 규모(magnitude)의 조합이라고 설명하였다.

국제표준기구인 ISO(International Standards Organization)는 ISO/IEC 13335-1:2004 표준에서 위험을 "위협(threat)이 자산 또는 자산 그룹의 취약성(vulnerability)을 악용하여 조직에 피해(harm)를 입힐 잠재성"이라고 규정하는데 여기서의 위협은 시스템이나 조직에 피해를 입힐 수 있는 잠재적 사고 원인을 뜻하고 취약성은 하나 이상의 위협에 의해 악용될 수 있는 자산 및 자산그룹의 결함으로 정의할 수 있다. 취약성은 그 자체로는 피해를 일으키지 않으나 위협으로 하여금 자산에 악영향을 가하도록 하는 재료로 작용하며 정보의 공개, 변조, 훼손, 파괴, 유실, 이용불능 같은 피해가 IT 시스템이나 서비스에 의해 처리되는 정보에 대한 직·간접적 공격으로부터 비롯된다.

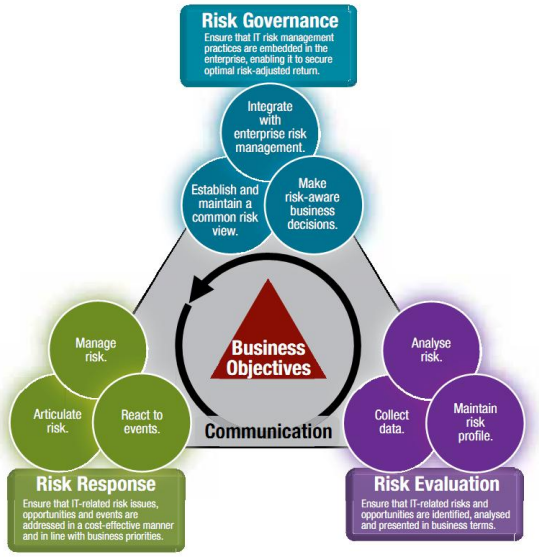
즉 그 원인이 환경적 요인이든 인적 요인이든, 의도적이든 우발적이든 간에 위협은 자산 자체에 내재하는 취약성을 악용함으로써 피해를 입힌다(ISO/IEC 13335-1:2004, 2004: 3-5). <표 1>은 ISO에서 설명하고 있는 위협의 예시이다.

<표 1> 위협의 예

인적 요인(Human)		환경적 요인(Environmental)
의도적(Deliberate)	우발적(Accidental)	
도청(Eavesdropping), 정보변조(Information modification), 시스템해킹(System hacking), 악성코드(Malicious code), 절도(Theft) 등	오류/누락(Errors & omissions), 파일삭제(File deletion), 잘못된 라우팅(Incorrect routing), 물리적 사고(Physical accidents)	지진(Earthquake), 낙뢰(Lightning), 홍수(Floods), 화재(Fire) 등

※ 자료: ISO/IEC 13335-1: 2004(2004).

위험 관리를 위해 오늘날 조직들은 IT 거버넌스(IT Governance)에 주목하고 있다. 정보시스템감사통제협회(Information System Audit & Control Association: ISACA)에 따르면 IT 거버넌스는 정보기술이 조직의 목표 달성에 기여하도록 하는 것이며 이의 핵심은 정보보호 거버넌스로 정보기술이 조직에 미치는 위험을 최소화하는 전략을 포함한다(ISACA, 2013: 135-136). ISACA는 정보기술 위험 프레임워크(The Risk IT Framework)(2009) 보고서에서 위험 프로세스 모델을 "위험 거버넌스, 위험 평가, 위험 대응"의 3개 도메인과 3개 프로세스로 구성하였는데 <그림 1>은 이 3개의 도메인 및 하위 프로세스들의 관계를 도식화한 것이다.



<그림 1> Risk IT Process Model

※ 자료: ISACA(2009: 15).

위험 관리(risk management)란 조직의 목적을 달성하기 위하여 자산이 가진 취약성과 위협을 식별하고 자산의 가치를 기준으로 하여 위험을 대응할 수 있는 수준으로 감소시키기 위한 대책을 결정하는 프로세스(ISACA, 2013: 157)를 말하는데 이러한 위험 관리의 첫 번째 단계는 자산을 식별하는 것이다. 자산 식별은 조직 성공의 사활이 걸려있는 위험 관리의 첫 걸음이므로 자산이 식별되지 않은 상태에서 IT 거버넌스를 구현하는 것은 불가능하다. 건물이나 하드웨어 같은 유형 자산은 물론 소프트웨어, 정보, 사람, 명성이나 이미지 같은 무형의 자산을 망라하는 조직의 자산 중에서도 정보는 현대 조직의 최우선 자산으로 꼽히며 특히 개인정보는 조직의 자산인 동시에 정보주체의 프라이버시권 대상 인자이자 공익 추구를 위한 핵심 요소로 기능하는 양면성을 가지고 있다. 국내 개인정보 보호 관련 법률은 개인을 고유하게 구별할 수 있는 고유식별정보와 정보주체의 사생활을 현저히 침해할 우려가 있는 건강에 관한 정보 등 민감정보의 처리를 엄격하게 제한하고 있다. 그러나 의료기관은 진료라는 본연의 목적을 달성하기 위하여 필연적으로 개인의 신상정보뿐 아니라 고유식별정보와 민감정보를 다루게 되는데 이러한 정보는 각종 위협에 노출되게 된다. ㈜이글루시큐리티가 2012년에 기관과 기업 보안 담당자 517명을 대상으로 진행한 설문조사 결과에 따르면 응답자의 56%가 가장 큰 위협으로 개인정보 및 내부정보 유출을 꼽았고 업무 추진 시 가장 큰 어려움으로는 보안 조직과 인력의 부족을 응답했다(전자신문, 2012).

위험 관리의 두 번째 단계는 자산과 관련된 위협과 취약성 및 이들의 발생 가능성을 평가하는 것이다. 위험을 제대로 진단하기 위해서 조직 구성원의 취약성을 파악하는 것은 매우 중요한 과정이다. 취

약성이 어떻게 관리되느냐 여부에 따라 조직의 자산인 사람이 곧 조직을 해치는 위협으로 변신할 수도 있기 때문이다. 이후의 위험 관리 프로세스에서는 식별된 위험에 따라 취약성을 수용할 수 있는 위험 수준까지 낮추기 위하여 현재의 통제를 평가하거나 새로운 통제를 설계하는 과정을 거치게 된다 (ISACA, 2013: 158-160).

본 연구는 의료정보[1]를 취급하는 병원 진료 및 진료지원부서 직원 등의 정보 관리 현황을 조사하여 조직 구성원으로서 의료업무 종사자들에게 내재된 취약성의 유무를 파악하고 의료기관의 중요한 자산이자 개인의 민감정보인 의료정보가 위협으로부터 안전한 상태인지 여부를 분석하려는 목적에서 시작하였다. 이를 위하여 본 장에서는 연구의 배경과 목적을 서술하고 두 번째 장에서는 병원 직원의 개인정보 관리 현황 조사를 위한 자료의 수집과 분석 방법을 설명하였다. 세 번째 장에서는 통계 분석을 통해 도출된 결과를 정리・해석하였으며 마지막 장에서는 연구의 결과가 의미하는 바를 요약하고 연구의 한계를 기술하였다.

Ⅱ. 연구 방법

본 연구는 의료정보를 취급하는 담당자의 개인정보 관리 현황을 조사하기 위해 병원 직원을 대상으로 설문 조사를 통하여 자료를 수집하기로 하였다.

자료 수집을 위한 설문지는 현행 개인정보 보호에 관한 기본법인 「개인정보 보호법」 제24조 제3항[2] 및 제29조와 동법 시행령 제21조 및 제30조[3]의 '개인정보 처리 시 안전성 확보 조치' 내용 중 조

---

1) 현재 국내 법제에서는 '의료정보'를 특별히 정의하고 있지 않다. 본 연구에서는 의료법 제12조에서 설명하고 있는 '의료행위'의 정의(의료인이 하는 의료・조산・간호 등 의료기술의 시행)와 개인정보 보호법 제2조의 '처리'의 정의(개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위)에 준하여 '의료행위 과정에서 처리되는 정보'를 '의료정보'라고 정의하고 '의료기관에서 의료정보를 처리하는 임직원, 파견근로자, 시간제근로자 등'을 '의료정보취급자'로 정의하기로 한다.

2) 「개인정보 보호법」 제24조(고유식별정보의 처리 제한) ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실・도난・유출・변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

3) 「개인정보 보호법」 시행령 제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립・시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장・전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조・변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

직 차원에서 전사적으로 통제되는 위험 예방 및 적발, 교정 장치와 더불어 개인정보취급자 스스로의 이행 수준 및 여부가 중대한 영향을 미치는 부분에 대해 중점을 두고 <표 2>와 같이 구성하였으며 주로 명목 척도로 측정할 수 있도록 설계하였다.

<표 2> 설문지의 구성

분류	설문 항목
인구통계학적 특성	성별 연령 직종 재직기간 컴퓨터 활용 기간(년 수)
접근 관리 현황	패스워드 개수와 생성 방법 패스워드 관리 현황 개인 컴퓨터 시스템 접근 통제 여부
암호화	기밀정보 보유 유무 암호화 여부와 방법

실증 연구를 위한 자료는 A대학병원 직원을 대상으로 <표 2>의 항목으로 구성된 구조적 설문 조사를 통해 수집하였다. 자료는 2회에 걸쳐 수집되었으며 그 중 첫 번째는 2011년 8월에 실시된 전체 교직원 개인정보 보호 교육 참석자들을 대상으로, 두 번째는 2012년 5월 전공의 대상으로 진행된 개인정보 보호 교육 참석자들로부터 수집하였다. 설문지는 교육 시작 전에 배포하여 교육 후 회수 하였으며 본인의 경험에 대해 '예', '아니오' 중 선택하거나 열거된 보기 중 해당하는 내용을 문항에 따라 1개 또는 여러 개 표기하는 형태로 구성하였다.

각 교육 마다 150부씩 총 300부의 설문지가 배포되었으며 각 111부와 127부가 회수되었고 그 중 대부분의 답변이 기재되지 않은 1부를 제외한 총 237부를 최종 유효 표본으로 정리하였다. 분석에 적합한 표본 수 확보를 위하여 성별과 연령 등 인구통계학적 특성이 부분적으로 누락된 설문 응답지를 제외하지 않고 '무응답' 자료로 표본에 포함하여 분석하였다. 선정된 표본은 통계 프로그램인 IBM SPSS Statistics 21.0을 이용하여 빈도 분석과 교차 분석을 실시하였다.

III. 연구 결과[4)]

1. 인구통계학적 특성

응답자들의 인구통계학적 특성은 <표 3>과 같다. 남성과 여성이 각각 31.6%와 55.3%로 여성 비율이 높았으며 20대와 30대가 각각 38.3%, 32.5%로 전체 연령대비 약 70%를 차지했고 무응답이 각

4) 통계표 내의 수치는 반올림되었으므로 세부항목의 합이 계와 일치하지 않을 수 있음을 밝혀둔다.

10% 이상 이었다. 성별과 연령에 무응답이 많았던 이유는 번호를 선택하도록 한 다른 항목과 달리 성별과 연령을 직접 기재하도록 설문지를 설계한 데서 기인하는 것으로 판단된다.

병원 내 각자의 직종을 묻는 항목 구성은 A대학병원의 직종 분류에 따라 작성되었으며 수련직 의사가 54%로 가장 많았고 일반직 14.8%, 간호직 10.1%, 기능원과 비정규직이 각각 6.8% 순으로 조사되었다. 수련직 의사의 분포가 높은 것은 본 조사가 전 직원 대상 교육 참석자와 수련직 의사로 한정된 교육 참석자들을 대상으로 각각 시행하고 두 표본 집단을 합하여 분석하였기 때문이다. 연령과 재직기간 등 표본의 전반적인 인구통계학적 특성에 수련직 의사의 분포가 영향을 미친 것으로 파악된다. 재직기간은 5년 미만이 70% 이상이었고 이어 10년 이상 20년 미만이 15.6%, 20년 이상 A대학병원에서 근무하고 있는 의료정보취급자는 7.2%인 것으로 나타났다.

<표 3> 인구통계학적 특성

		표본 수(명)	구성비(%)
전체		237	100.0
성별	남	75	31.6
	여	131	55.3
	무응답	31	13.1
연령	20대	92	38.8
	30대	77	32.5
	40대	31	13.1
	50대	7	3.0
	무응답	30	12.7
직종	일반직	35	14.8
	간호직	24	10.1
	교수직	2	.8
	수련직	128	54.0
	조교	5	2.1
	강사	3	1.3
	기능원	16	6.8
	비정규직	16	6.8
	파견근로사원	1	.4
	기타	5	2.1
	무응답	2	.8

<표 3> 인구통계학적 특성(계속)

		표본 수(명)	구성비(%)
재직기간	1년 미만	48	20.3
	1년 이상 3년 미만	75	31.6
	3년 이상 5년 미만	52	21.9
	5년 이상 7년 미만	1	.4
	7년 이상 10년 미만	4	1.7
	10년 이상 15년 미만	19	8.0
	15년 이상 20년 미만	18	7.6
	20년 이상 25년 미만	13	5.5
	25년 이상 30년 미만	4	1.7
	무응답	3	1.3
컴퓨터 활용 기간	10년 미만	21	8.9
	10년 이상 15년 미만	90	38.0
	15년 이상 20년 미만	88	37.1
	20년 이상 25년 미만	32	13.5
	25년 이상	5	2.1
	무응답	1	.4
웹사이트 멤버십 개수	10곳 미만	44	18.6
	10곳 이상 30곳 미만	99	41.8
	30곳 이상 50곳 미만	47	19.8
	50곳 이상 70곳 미만	22	9.3
	70곳 이상 90곳 미만	6	2.5
	90곳 이상 110곳 미만	5	2.1
	110곳 이상	14	5.9

컴퓨터를 활용한 이력은 10년 이상 15년 미만(38.0%)과 15년 이상 20년 미만(37.1%)이라는 답변이 전체의 75% 이상이었고 20년 이상 컴퓨터를 사용하고 있다는 답변이 15.6%였다. 가입한 웹사이트 수를 묻는 질문에는 10곳 이상 30곳 미만이라는 응답이 41.8%로 가장 많았고 30곳 이상 50곳 미만(19.8%), 10곳 미만(18.6%)이 뒤를 이었다. 50곳 이상의 웹사이트에 가입한 직원이 19.8%이며 특히 110개 이상의 계정을 보유한 응답자도 5.9%를 차지하였다.

2. 접근 관리 현황

자산을 위험으로부터 보호하기 위하여 접근 관리는 필수적으로 이행되어야 한다. 인가된 최소한의 사람만 업무에 필요한 최소한의 정보에 접근하도록 통제가 실행되어야 하는데 접근 관리에 있어 비용 대비 가장 효과적인 수단은 패스워드이다.

행정안전부(현 안전행정부)고시 제2011 - 제43호 '개인정보의 안전성 확보조치 기준' 제5조는 개인정보처리자[5]로 하여금 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것을 명시하고 있다.

1) 패스워드[6] 생성 현황

의료정보취급자의 정보 관리 형태를 알아보기 위하여 사용하는 패스워드가 몇 개인가를 조사하였다. 패스워드 사용처는 개인 단말기 접근과 병원 내부망 접속뿐 아니라 이메일, 메신저, 커뮤니티, 학회 및 협회 멤버십 등 인터넷 서비스 이용 용도도 포함한다. <표 4>와 같이 사용하고 있는 패스워드가 3개라는 답변이 44.3%로 가장 많았고 4-5개가 30%로 그 뒤를 이었으며 1-2개의 패스워드만 사용하는 직원은 17.7%였다. 분석 결과 평균적으로 약 3.4개의 패스워드를 사용하고 있는 것인데 앞서 기술된 연구 결과 <표 3>에서 평균적으로 약 40곳에 멤버십을 보유하고 있는 점과 연계해보면 약 11개의 계정은 동일한 패스워드로 접근하고 있다는 결과를 도출할 수 있다.

<표 4> 패스워드 개수

		표본 수(명)	구성비(%)
전체		237	100.0
패스워드 개수	1개	5	2.1
	2개	37	15.6
	3개	105	44.3
	4~5개	71	30.0
	6~7개	9	3.8
	8~10개	5	2.1
	모두 다른 패스워드	5	2.1

방송통신위원회(2013)와 안전행정부(2011)의 고시 및 해설서는 안전한 패스워드 설정 원칙으로 최소 '10자리' '2종류 문자 조합' 또는 '8자리' '3종류 문자의 조합'을 제시하고 있다. 이에 응답자들이 사용하고 있는 패스워드의 안전성 분석을 위하여 수집된 패스워드 길이와 문자 조합 개수 자료를 <표 5>와 같이 교차 분석 하였다. 분석 결과 전술한 국내 개인정보 보호 관련 법제에서 제시하는 패스워드 설정 기준에 비추어 본 연구 대상자의 약 70%는 안전성이 담보되지 않은 패스워드를 사용하고 있다고 볼 수 있다.

---

5) "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다(「개인정보 보호법」 제2조 제5호, 2013).

6) "비밀번호"라는 용어가 그 정의(행정안전부(現 안전행정부)고시 제2011 - 제43호 제2조 제12호. 비밀번호란 (중략) 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다)와 사용 형태에 부합하지 않는바 본 연구자는 비밀번호를 이하 패스워드로 명명하였다.

<표 5> 패스워드 문자 조합 개수와 길이 교차표

			패스워드 문자 조합 개수				전체
			1종류	2종류	3종류	4종류	
패스워드길이	3~4자리	표본 수(명)	1	1	1	0	3
		문자 조합 개수 중 %	100.0%	0.5%	2.3%	0.0%	1.3%
	5~6자리	표본 수(명)	0	26	6	0	32
		문자 조합 개수 중 %	0.0%	14.1%	14.0%	0.0%	13.5%
	7~8자리	표본 수(명)	0	95	21	5	121
		문자 조합 개수 중 %	0.0%	51.6%	48.8%	55.6%	51.1%
	9~10자리	표본 수(명)	0	43	8	3	54
		문자 조합 개수 중 %	0.0%	23.4%	18.6%	33.3%	22.8%
	11~13자리	표본 수(명)	0	16	6	0	22
		문자 조합 개수 중 %	0.0%	8.7%	14.0%	0.0%	9.3%
	14자리 이상	표본 수(명)	0	3	1	1	5
		문자 조합 개수 중 %	0.0%	1.6%	2.3%	11.1%	2.1%
전체		표본 수(명)	1	184	43	9	237
		문자 조합 개수 중 %	100.0%	100.0%	100.0%	100.0%	100.0%

※ Pearson 카이제곱 = 86.996 df=15 p<.01

한편 연령과 패스워드 길이 간의 관계를 파악하기 위해 실행한 교차 분석에서 두 변수 간에 유의한 관계가 있음이 도출되었다(Pearson 카이제곱 유의확률 .000). 7-8자리 길이의 패스워드를 사용한다는 응답이 모든 연령에서 가장 높은 비율을 차지하였다. 주목할 만한 부분은 차 순위인데 다른 연령에서는 5-6자리 길이가 그 다음 순위인 반면 20대 응답자들에서는 9-0자리, 11-13자리라는 응답이 더 많았다. 50대의 경우 5-6자리 길이를 응답한 사람은 없었고 3-4자리와 9-10자리가 같은 비율로 조사되었으나 50대 표본의 수가 적음을 고려하면 상당한 신뢰성을 담보하기는 어려운 값이다. 자세한 결과는 <표 6>과 같다.

<표 6> 연령과 패스워드 길이 교차표

			연령					전체
			20대	30대	40대	50대	무응답	
패스워드 길이	3~4자리	표본 수(명)	0	1	0	2	0	3
		연령 중 %	0.0%	1.3%	0.0%	28.6%	0.0%	1.3%
	5~6자리	표본 수(명)	6	12	7	0	7	32
		연령 중 %	6.5%	15.6%	22.6%	0.0%	23.3%	13.5%
	7~8자리	표본 수(명)	42	44	18	3	14	121
		연령 중 %	45.7%	57.1%	58.1%	42.9%	46.7%	51.1%
	9~10자리	표본 수(명)	30	11	4	2	7	54
		연령 중 %	32.6%	14.3%	12.9%	28.6%	23.3%	22.8%
	11~13자리	표본 수(명)	12	7	1	0	2	22
		연령 중 %	13.0%	9.1%	3.2%	0.0%	6.7%	9.3%
	14자리 이상	표본 수(명)	2	2	1	0	0	5
		연령 중 %	2.2%	2.6%	3.2%	0.0%	0.0%	2.1%
전체		표본 수(명)	92	77	31	7	30	237
		연령 중 %	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

※ Pearson 카이제곱 = 65.636 df=20 p<.01

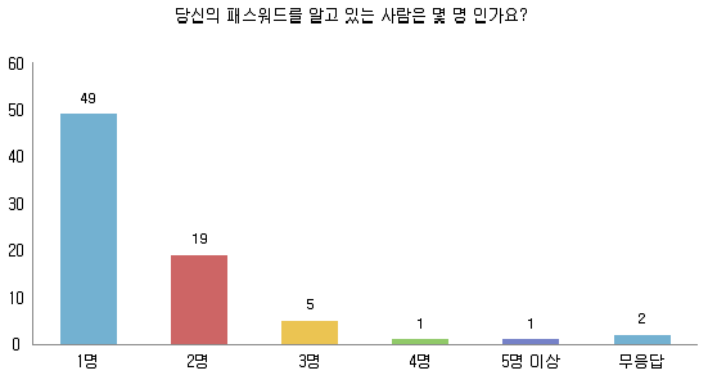
2) 패스워드 관리 현황

패스워드의 생성과 더불어 패스워드를 어떻게 관리하는가의 문제 또한 정보 자산을 보호하기 위한 접근 통제에서 주목해야 할 부분이다. 각자의 패스워드 보관 방법을 간략히 서술하도록 설문지를 구성하고 답변 내용을 <표 7>에 정리하였다. 연구 과정 전반에 걸쳐 개방형 설문에 대한 응답률이 대체로 저조한 것으로 나타났으며 이 문항 또한 예외가 아니었다. 무응답을 제외한 가장 많은 응답은 암기(32.5%)였고 모든 패스워드가 같아서 별도의 보관이 필요 없다는 답변이 14.3%로 그 다음 순위였다. 수첩에 기록(5.5%)하거나 휴대폰에 메모(2.5%)하여 보관하는 직원들이 있었고 패스워드 관리 프로그램을 이용하거나 기록한 파일을 암호화하는 방법으로 보관한다는 응답은 각각 0.8%에 그쳤다. 기타 응답으로는 주기적으로 변경한다는 내용 등이 있었다.

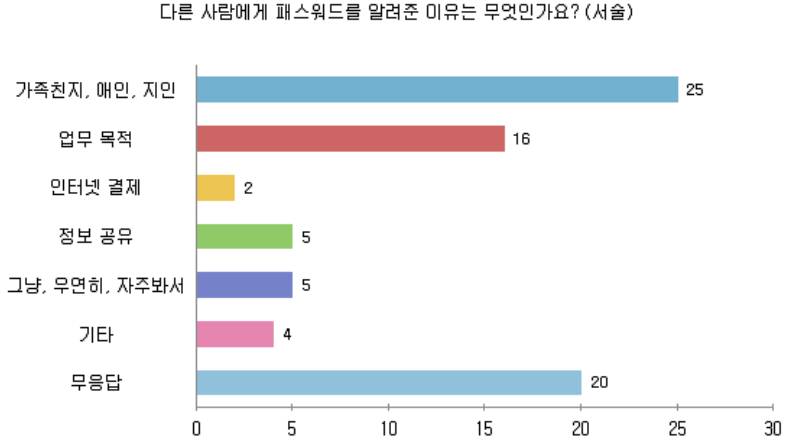
<표 7> 패스워드 관리 현황

		표본 수(명)	구성비(%)
전체		237	100.0
패스워드 보관(관리) 방법	불필요 / 모든 패스워드가 같다	34	14.3
	암기	77	32.5
	휴대폰에 메모	6	2.5
	수첩에 기록	13	5.5
	파일로 저장	2	.8
	파일에 기록하고 암호화	2	.8
	나만의 패턴	6	2.5
	패스워드 관리 프로그램 이용	2	.8
	기타	8	3.4
	무응답	87	36.7
내 패스워드 타인에게 노출 여부	예	77	32.5
	아니오	157	66.2
	무응답	3	1.3
타인 패스워드 습득 여부	예	64	27.0
	아니오	151	63.7
	무응답	22	9.3

패스워드란 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다(행정안전부(현 안전행정부)고시 제2011 - 제43호 제2조 제6호). 개인 식별 및 인증, 권한 관리에 사용되는 패스워드는 시스템에게 본인임을 증명하는 수단이자 대부분의 경우 유일한 수단이므로 타인과의 공유가 원칙적으로 금지된다. 그러나 <표 7> 및 <그림 2>와 <그림 3>에서 볼 수 있듯 상당수의 직원들이 자신의 패스워드를 타인과 공유(32.5%)하거나 타인의 패스워드를 공유(27.0%)하고 있는 것으로 조사되었으며 그 대상자는 주로 가족, 지인이거나 직장 동료였다.



<그림 2> 본인 패스워드 공유 명 수



<그림 3> 본인 패스워드 공유 이유

2) PC (Personal Computer) 접근 통제 현황

접근 통제란 시스템이 담고 있는 정보를 보호하기 위하여 접근을 제한하거나 허용하는 관리 과정이다. 조직은 승인 받지 않은 접근을 적극적으로 통제함으로써 위험으로부터 자산을 보호해야 한다. 개인정보의 안전성 확보조치 기준(2011)은 개인정보처리자로 하여금 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 침입 차단 시스템(firewall) 또는 침입 방지 시스템(Intrusion Prevention System: IPS) 등을 설치·운영하도록 정하고 있다. 또한 별도의 개인정보처리시스템을 이용하지 않고 업무용 컴퓨터만 이용하여 개인정보를 처리하는 경우라면 업무용 컴퓨터의 운영체제(Operating System: OS)나 보안 프로그램 등이 제공하는 기능을 이용하여 접근 통제를 실시할 수 있다(행정안전부(現 안전행정부)고시 제2011 - 제43호 제6조). 본 연구에서는 의료 현장에서 개인정보를 취급하는 직원들의 기본적인 통제 절차 준수 여부를 확인하고자 OS 패스워드 설정, 로그오프, 컴퓨터 공유 여부

에 대해 응답하도록 문항을 설계하였다. 과반수(50.6%)가 컴퓨터 OS 접근 패스워드를 설정하고 있었으나 컴퓨터를 본인 이외 다른 사람도 이용한다는 응답 역시 과반수(53.2%)였고 자리를 비울 때 로그오프를 하는 직원은 31.2%인 것으로 조사되었다(<표 8>).

<표 8> 접근 통제 현황

		표본 수(명)	구성비(%)
전체		237	100.0
컴퓨터 OS 패스워드 설정 여부	예	120	50.6
	아니오	114	48.1
	무응답	3	1.3
컴퓨터 자리 비움 시 로그오프 여부	예	74	31.2
	아니오	157	66.2
	무응답	6	2.5
내 컴퓨터 타인 사용 여부	예	126	53.2
	아니오	108	45.6
	무응답	3	1.3

컴퓨터 OS 패스워드 설정 여부와 본인 컴퓨터의 다른 사람 사용 여부 간 관계를 알아보기 위하여 교차 분석을 실시하였다. 그 결과, <표 9>와 같이 OS 패스워드를 설정한 의료정보취급자 중 절반은 다른 사람의 OS 접근을 허용하는 것을 알 수 있었다.

<표 9> 컴퓨터 OS 패스워드 설정과 컴퓨터 타인 사용 여부 교차표

			OS 접근 패스워드 설정			전체
			예	아니오	무응답	
컴퓨터 타인 사용	예	표본 수(명)	60	66	0	126
		패스워드 설정 중 %	50.0%	57.9%	0.0%	53.2%
	아니오	표본 수(명)	60	48	0	108
		패스워드 설정 중 %	50.0%	42.1%	0.0%	45.6%
	무응답	표본 수(명)	0	0	3	3
		패스워드 설정 중 %	0.0%	0.0%	100.0%	1.3%
전체		표본 수(명)	120	114	3	237
		패스워드 설정 중 %	100.0%	100.0%	100.0%	100.0%

※ Pearson 카이제곱 = 283.485, df=4, p<.01.

<표 10>은 컴퓨터 접근 시 패스워드 설정 여부와 자리 비움 시 컴퓨터 로그오프 간의 관계를 교차 분석한 것이다. Pearson 카이제곱 유의확률이 .000으로 두 변수 간 유의한 관계가 증명되었으며 OS 패스워드를 설정하지 않는 직원들은 대체로 자리를 비울 때도 OS 로그오프를 하지 않는 것으로 나타

났다.

<표 10> 컴퓨터 OS 패스워드 설정과 자리 비움 시 로그오프 여부 교차표

			OS 접근 패스워드 설정			전체
			예	아니오	무응답	
자리 비움 시 로그오프	예	표본 수(명)	57	17	0	74
		패스워드 설정 중 %	47.5%	14.9%	0.0%	31.2%
	아니오	표본 수(명)	60	95	2	157
		패스워드 설정 중 %	50.0%	83.3%	66.7%	66.2%
	무응답	표본 수(명)	3	2	1	6
		패스워드 설정 중 %	2.5%	1.8%	33.3%	2.5%
전체		표본 수(명)	120	114	3	237
		패스워드 설정 중 %	100.0%	100.0%	100.0%	100.0%

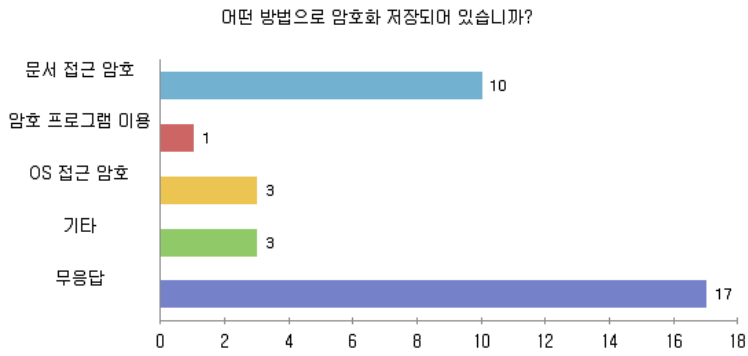
※ Pearson 카이제곱 = 42.153, df=4, p<.01.

3. 암호화

현행 개인정보 보호 관련 법제는 고유식별정보 등 개인정보를 처리하는 경우에 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 등 안전성 확보에 필요한 조치를 할 것을 규정하고 있다. 행정안전부(2011) '개인정보의 안전성 확보조치 기준' 제7조 제8항은 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장할 것을 명시하고 있고 '개인정보의 기술적·관리적 보호조치 기준'은 이용자의 개인정보를 개인용 컴퓨터(PC)에 저장할 때 암호화를 의무화하고 있다(방송통신위원회, 2013: 제6조 제4항). 연구자는 의료정보취급자들이 개인정보를 취급하는 태도를 파악하기 위하여 데스크톱, 노트북, USB 플래시 메모리 등에 비인가자의 접근이 제한되어야 하는 개인정보, 기밀정보 등 중요 데이터의 저장 유무와 해당 정보의 암호화 여부 및 그 방법을 조사하였다. <표 11>에 나타난 대로 분실·도난·유출 등으로부터 보호되어야 하는 중요 정보를 개인용 저장장치에 보유하고 있지 않다고 응답한 표본 비율은 43.0%였다. '모르겠다'고 기재하거나 답변을 작성하지 않은 표본을 포함한 잠재적 중요 정보 보유자 57.0%에 대하여 암호화 여부를 분석한 결과 25.2%만이 암호화를 실천하고 있는 것으로 분석되었다.

<표 11> 암호화

		표본 수(명)	구성비(%)
전체		237	100.0
중요 정보 보유 여부	예	115	48.5
	아니오	102	43.0
	모름/무응답	20	8.4
암호화 여부	예	34	14.3 (유효% 25.2)
	아니오	94	39.7 (유효% 69.6)
	모름/무응답	7	3.0 (유효% 5.2)
	합계	135	57.0 (유효% 100.0)
	결측값	102	43.0



<그림 4> 암호화 방법

암호화 방법을 서술하도록 한 질문에는 50%만이 응답하였으며 그들 중 대부분은 Microsoft Office나 한컴 한글 등의 프로그램이 제공하는 문서 암호 기능을 사용하는 것으로 나타났고 별도의 암호화 소프트웨어를 사용하는 응답자는 1명 이었다(<그림 4>).

Ⅳ. 결론

본 연구는 정보기술이 조직에 미치는 위험을 최소화하고 조직의 목표를 달성할 수 있도록 지원하는 IT 거버넌스의 위험 관리에 관한 것이다. 위험 관리 프로세스에서 식별된 자산은 그 손실이 유발하는 영향력에 따라 중요도를 산정할 수 있는데 정보화 사회에서 조직의 가장 중요한 자산은 단연 정보이다. 정보 자산의 범주에 포함되는 개인정보가 제대로 관리되지 않을 경우 개인의 권리와 이익, 나아가 헌법에서 보장하고 있는 개인의 존엄과 가치 또한 침해될 우려가 있기 때문에 법률은 이를 엄중하게 보호하도록 규정하고 있다[7].

한편 의료는 사람의 생명과 건강을 다루기에 건강 증진, 질병 치료, 분만, 재활 등의 목적을 달성하기 위한 모든 의료행위에서 정확한 근거에 입각할 것을 요구받는다. 적절한 의료는 지속적인 환자에 대한 정보 수집이 있을 때 비로소 실현될 수 있는 반면 의료정보가 오·남용될 경우 개인의 사생활을 심각하게 침해할 우려가 있어 국내외 법제에서는 이를 민감정보(sensitive information)로 규정하고 각별한 처리 의무를 부과하고 있다. 이러한 딜레마 속에 제대로 된 관리를 통한 정보의 보호와 활용의 균형 및 통제가 그 어떤 분야보다도 중요하게 조명되어야 할 영역이 의료 분야다.

Ponemon Institute가 9개 국가로부터 수집한 데이터를 바탕으로 발행한 글로벌 데이터 유출 분석

7) 「개인정보 보호법」 제1조(목적) 이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다.

보고서는 2012년 발생한 데이터 유출 사고의 주요 원인이 악의적이거나 불법적인 공격(37%). 임직원의 과실(35%), 시스템의 오류(29%) 때문이라고 밝혔다. 내부직원의 과실은 주로 부주의에서 기인되었으며 악의적인 공격은 외부 공격자뿐 아니라 직원, 계약자, 파트너 등 내부인에 의한 공격이 포함된 수치로 보고되었다(Ponemon Institute, 2013: 7).

이에 본 연구는 위험 관리의 기본인 자산 식별 및 취약성 진단과 관련하여 조직에서 보호해야 할 자산인 동시에 조직을 위협하는 주된 취약 요인인 조직 내부인의 정보 관리 현황을 조사하였다. 조사 대상은 가장 민감한 정보인 의료정보를 다루는 의료 업무 종사자들로 「개인정보 보호법」에 명시된 '개인정보의 안전성 확보 조치' 기준을 반영하여 구조적 설문지를 설계하였고 A대학병원 직원을 표본 집단으로 하여 자료를 수집하여 통계 분석하였다.

도출된 주요 연구 결과가 시사하는 바를 정리하면 다음과 같다.

첫 번째로 응답자들이 보유한 패스워드가 개인정보 보호 관련 법제에서 제시 또는 의무화하고 있는 안전한 패스워드 설정 기준인 10자리 2종류 문자 조합 또는 8자리 3종류 문자의 조합에 크게 못 미치는 수준으로 응답자의 약 70%가 사용하는 패스워드에서 취약성이 발견되었다. 연구 표본이 보유하고 있는 패스워드는 평균 3.4개로 약 11개의 계정에 동일한 패스워드를 사용하고 있었고 응답자의 32.5%는 패스워드를 타인과 공유하고 있었다. 패스워드를 공유하는 이유는 가족이기 때문(32.5%)이라는 답변과 업무상 편의(20.8%) 때문이라는 답변이 대부분이었다.

정보 자산에 대한 접근 관리는 다음 세 가지 사실의 확인 위에 유지 가능하다. 식별된 정보 자산이 있어야 하고 특정 정보에 접근해야 하는 목적이 분명해야 하며 법제와 내규에 따라 조직에서 부여한 접근 승인이 있어야 한다. 접근 승인은 그가 누구인지를 확인하는 식별(identification), 그가 정당한 사용자인지 여부를 판단하는 인증(authentication), 그의 역할에 부합하는 정보에 대해 접근 권한을 부여하는 인가(authorization)의 과정으로 나눌 수 있는데 개인별 인증을 제공하는 키가 바로 패스워드다. 쉽게 해독될 수 있는 부실한 패스워드와 잘못된 패스워드 관리는 비인가된 자에게 조직의 핵심 자산을 쉽게 노출함으로써 최악의 경우 조직 경영이 불가능한 상황에까지 이르게 할 위험이 있다. 병원의 경우 생명을 다루는 곳이므로 그 어떤 조직보다도 안전성과 신뢰성이 보장되어야 한다. 의료 업무 종사자들의 잘못된 패스워드 관리는 민감정보인 의료정보의 유출・조작・훼손은 물론 의료업무 불능 사태를 초래하여 의료 시스템을 믿고 맡긴 환자의 생명을 빼앗는 결과까지도 가져올 수 있는 심각한 문제이다.

나에게 쉬운 패스워드는 공격자에게도 쉽다. 10자리 2종류 문자 조합 또는 8자리 3종류 문자의 조합이라는 고시가 2009년에 발표된 최소한의 기준임을 고려하여 의료정보취급자들은 IT 발전 속도에 따라 패스워드로서의 기능을 할 수 있는 견고한 문자열을 보유해야 할 책임이 있다. 응답자 중 20대가 다른 연령층에 비해 상대적으로 강한 패스워드를 사용하고 있는 것으로 조사된 것은 정보기술 활용 능력 또는 정보기술 접근 빈도가 높을수록 복잡한 패스워드를 설정하는 것으로 해석해볼 수 있으나 결론에 도달하려면 보다 정교한 후속연구가 필요하다. 본 연구결과에서 논의할 수 있는 부분은 연

령대가 높은 직원일수록 안전하지 않은 패스워드를 사용하는 경향이 있으므로 조직 차원에서 이러한 취약성을 인식하여 위험 관리 대책을 수립할 수 있다는 점이다. 조직은 일정 기준에 부합하지 않는 의료정보취급자의 패스워드의 생성 자체를 차단하고 올바른 패스워드 설정 방법을 안내하는 방법으로 취약성에 대한 예방 통제를 실시할 수 있다.

패스워드는 개인 유일의 소유 원칙에 준하여 관리되어야 한다. 패스워드가 공유된다면 해당 계정으로 활동한 자를 식별할 수 없어 IT 거버넌스에 있어 책임 추적성이 위태롭게 된다. 이러한 행위는 조직의 목표 달성에 이롭지 않을 뿐 아니라 패스워드를 노출한 직원 스스로 본인이 하지 않은 활동에 대하여 법적 책임의 위험을 짊어지는 행위이므로 지양해야 한다.

두 번째는 개인이 사용하는 컴퓨터 시스템의 접근 통제에 관한 것이다. 운영체제(OS) 접근 시 패스워드 설정 여부, 자리를 비울 때 로그오프 여부, 타인과의 컴퓨터 공유 여부에 대한 조사 결과 응답자의 50.6%가 OS 패스워드를 설정하고 있었으며 자리를 비울 때 로그오프를 하는 직원은 31.2%였고 53.2%는 본인 컴퓨터를 다른 사람도 사용하는 것으로 나타났다. 아울러 OS 패스워드를 설정하지 않는 직원들은 대체로 자리를 비울 때도 OS 로그오프를 하지 않고 있었다.

시스템 접근이란 컴퓨터 자원으로 작업을 할 수 있는 능력으로 파일의 생성・읽기・수정・삭제, 프로그램의 실행, 외부 접속의 사용 등을 들 수 있다. 전산화된 정보 자원에 대한 시스템 접근은 논리적 또는 물리적 수준에서 수립되며 논리적 관점에서 IT 자산은 네트워크, 운영체제, 데이터, 애플리케이션의 4개 도메인으로 묶을 수 있다. 시스템 접근 통제를 통해 사용자가 접근할 수 있는 컴퓨터 자원이 규정되며 이 때 OS 패스워드는 운영체제 수준에서의 파일 및 처리 접근 통제를 위한 최소한의 조건이 된다(ISACA, 2013: 535-536).

연구 결과 운영체제 접근을 위한 패스워드를 설정한 직원과 그렇지 않은 직원의 분포는 거의 반반이었으나 패스워드를 설정한 직원 중의 절반이 사용하는 PC는 본인뿐만 아니라 다른 사람의 접근도 허용하는 것으로 분석되어 결과적으로 응답자의 25%만이 컴퓨터 운영체제 접근을 통제하고 있었다. OS 패스워드를 설정하였고 자리를 비울 때 로그오프도 한다는 응답자는 전체의 24.1%였다. 컴퓨터 시스템이 활성화된 상태로 자리를 비웠다는 것은 누구든지 시스템을 이용할 수 있다는 것을 의미하고 이는 조직 자산의 오・남용 위험을 높이는 취약성이 된다. 조직은 이를 보완하기 위하여 네트워크에 연결된 모든 컴퓨터 OS에 접근 시 반드시 패스워드를 제출하도록 하고 일정 시간 동안 컴퓨터를 사용하지 않을 경우 자동적으로 로그온 세션이 차단되도록 통제 규칙을 마련하여 시스템 접근 통제를 실시할 수 있다. 아울러 인가받지 않은 사람의 접근을 방지하기 위하여 일회용 패스워드 토큰을 사용하도록 하거나 사용자의 신체 혹은 행동 특성을 이용한 생체인식(biometrics) 방법을 채택할 수도 있다. 보유하고 있는 자산의 민감성 정도가 클수록 접근 통제가 엄격하여야 한다는 원칙에 입각하여 의료정보의 철저한 관리가 필요하다.

세 번째는 암호화와 관련한 것으로 분실・도난・유출 등으로부터 보호되어야 하는 중요 정보를 데스크톱, 노트북, USB 플래시 메모리 등 저장장치에 보유하고 있다고 응답한 직원이 48.5%였다. '모르

겠다'고 기재하거나 답변을 작성하지 않은 표본(8.4%)을 포함한 중요 정보 보유 예상자 중 해당 정보에 암호화 조치를 이행하고 있는 직원은 25.2%였고 이들은 주로 문서 작성 프로그램이 제공하는 암호 기능을 이용하는 것으로 나타났다.

암호화는 컴퓨터 안에 저장된 데이터를 코드로 만드는 것이다. 기밀정보가 유출되더라도 읽거나 이해할 수 없다면 사용할 수 없다. 완벽한 암호화가 어렵다 하더라도 공격자가 암호를 푸는데 소요되는 비용이 기대하는 이익보다 크다면 기밀정보의 공개 위험도 줄어들게 된다. 의료기관의 개인정보 보호 활동을 규제하는 개인정보 보호법제는 업무용 컴퓨터에 고유식별정보를 저장하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장할 것을 명시하고 있다. 환자의 진료기록은 고유식별정보와 병력 등 민감정보로 구성되어 있다[8]. 업무 과정에서 지득한 의료정보의 개인 컴퓨터 저장 시에는 정당한 사유와 절차에 따라 최소한의 정보만 저장해야 하며 반드시 암호화하여 보관해야 한다. 또한 목적을 달성한 후에는 반드시 삭제・파기하여 오・남용 위험을 줄여야 한다. 조직은 중요 자산을 식별하고 그 처리에 관한 정책을 수립해야 하는데 자산에 대한 접근 기록을 유지하고 업무용 컴퓨터를 포함한 다양한 저장장치에 중요 정보가 복사・이전될 경우 승인 절차가 유지되도록 해야 하며 중요 정보에 대하여 전사적 차원의 암호화 및 모니터링 시스템을 도입할 수도 있다.

취약성은 어디에나 존재하며 그 자체로는 문제를 일으키지 않지만 고의 또는 부주의 등 인적 요인과 자연 환경적 요인 등에 의한 위협의 재료로 악용될 경우에는 조직에게 돌이킬 수 없는 손실을 가할 수 있기 때문에 위험 관리에 기반을 두어 취약성을 진단하는 과정은 매우 중요하다. 이에 의료정보를 취급하는 병원 진료 및 진료지원부서 직원의 정보 관리 현황을 조사하고 조직 구성원으로서 의료업무 종사자들에게 내재된 취약성 유무를 파악하여 의료기관의 중요한 자산이자 개인의 민감정보인 의료정보가 위협으로부터 안전한 상태인지 여부를 확인한 본 연구는 위에서 서술한 대로 연구 목적에 부합하는 의미 있는 결론을 도출하였으나 몇 가지 측면에서 한계점 또한 지니고 있다.

먼저 본 연구 대상자들은 병원 직원들이었으나 그들이 응답한 정보처리시스템의 범위는 업무 외 사적인 용도의 사용도 포함하고 있다. 패스워드를 공유하는 이유에 대한 가장 많은 답변이 가족친지 등이며 두 번째 높은 응답이 업무상 편의 때문이라는 점에서도 드러나는 부분이다. 이는 근본적으로 개인이 정보를 관리하는 행위는 그의 인식과 태도에서 비롯되는 것이므로 개인에게 내재된 취약성은 공사를 구분하지 않을 것이라는 연구자의 예상에 의해 특정한 제한점을 정하지 않고 자료를 수집한 데

8) 의료법 시행규칙 제14조(진료기록부 등의 기재 사항) 법 제22조에 따른 진료기록부・조산기록부와 간호기록부(이하 "진료기록부등"이라 한다)에는 다음 각 호의 구분에 따라 해당 사항을 한글과 한자로 적어야 한다. 다만, 질환명, 검사명, 약제명 등 의학용어는 외국어로 적을 수 있다.

1. 진료기록부

가. 진료를 받은 자의 주소・성명・주민등록번호・병력(病歷) 및 가족력(家族歷)

나. 주된 증상, 진단 결과, 진료경과 및 예견

다. 치료 내용(주사・투약・처치 등)

라. 진료 일시분(日時分)

서 기인한다. 예로 응답자들이 평균적으로 3.4개의 패스워드를 보유하고 있고 11개의 계정에 대해 동일한 패스워드를 사용하며 패스워드가 1개 또는 소수이므로 별도의 보관 방법이 없거나 암기한다는 응답으로 식별되는 취약성은 공사를 구분하지 않는 위험 상황이라는 결론에 이르게 한다. 특히 모든 시스템이 네트워크로 연결된 환경은 사실상 경계 없는 정보 관리를 가능하게 한다. 그러나 개인의 사적인 개인정보 관리 형태와 업무상 개인정보취급자로서의 정보 관리 현황의 상관관계에 대한 결론을 확인하기 위해서는 별도의 연구가 필요하므로 추후 보다 정교한 연구를 진행하고자 한다.

다음은 표본의 수와 구성 비율이 연구 결과를 일반화하기에는 한계가 있다는 점이다. 연구의 편의상 특정 대학병원만으로 한정하였으며 교직원 전체와 전공의 대상의 조사 결과를 취합하는 과정에서 전공의가 표본의 과반을 차지함으로서 직종, 연령, 재직기간 등 인구통계학적 속성 전반에 영향을 미쳤다. 아울러 성별, 연령을 포함한 서술형 항목 대부분에서 무응답 비율이 높았으나 표본 수 확보를 위하여 이를 제외하지 않고 '무응답' 상태로 분석에 포함한 부분도 언급하고자 한다. 후속 연구 시 표본의 수를 충분히 확보하고 서술형 질문을 선택형 질문으로 변형하는 등 응답률을 높일 수 있는 방법으로 자료를 수집한다면 연구의 신뢰성과 타당성을 향상시킬 수 있을 것이다.

효과적인 위험 관리는 조직의 위험 성향에 대한 명확한 이해에서 시작된다. 내부 위협이 초래하는 위험은 대부분 '사람'과 관련된 문제이므로 이를 해결할 대책도 사람 중심이어야 한다. Ponemon Institute(2013)의 보고서에서 산업별 데이터 유출에 따른 피해 분석 결과 가장 피해 규모가 큰 분야는 의료(healthcare)로 평균 대비 70%를 웃도는 수치를 기록했으며 금융, 제약, 운송 분야가 그 뒤를 따랐다. BankInfoSecurity(2013)는 Ponemon과의 인터뷰를 통해 이들 분야의 피해가 큰 이유는 다른 산업군에 비해 민감한 개인정보들을 대량 처리하고 있으며 이를 규제하는 강한 법률이 있기 때문이라고 분석했다. 이처럼 의료정보를 취급하는 사람들은 보다 엄격한 태도로 정보시스템을 이용해야 하며 조직은 구성원들의 취약성을 이해하고 이를 관리적, 물리적, 기술적 방법으로 보완해야 한다. 모든 의료기관은 조직의 자산인 동시에 정보주체에게 지대한 영향을 미치는 민감정보이자 공공 정책 수립의 근간인 개인 의료정보가 제대로 보호되고 활용될 수 있도록 지금보다 더 노력할 필요가 있다.

참고문헌

개인정보 보호법. 2013. 시행 2013. 3. 23. 법률 제11690호.
개인정보 보호법 시행령. 2013. 시행 2013. 3. 23. 대통령령 제24425호.
방송통신위원회. 2012. 고시 제2012-50호. 개인정보의 기술적·관리적 보호조치 기준.
의료법. 2013. 시행 2013. 1. 1. 법률 제10387호.
의료법 시행규칙. 2013. 시행 2013. 4. 17. 보건복지부령 제193호.
전자신문. 2012. 올 하반기 개인정보·내부정보 유출이 가장 큰 보안 위협.

한국정보보호진흥원(現 한국인터넷진흥원). 2009. 개인정보의 기술적·관리적 보호조치 기준 개정(안)의 추진방향 및 주요내용. i-PIN 정책 설명회 및 개인정보의 기술적·관리적 보호조치 기준 개정(안)공청회.

행정안전부(現 안전행정부). 2011. 고시 제2011－제43호, 개인정보의 안전성 확보조치 기준.

BankInfoSecurity. 2013. *Regulations' Impact on Data Breach Costs*. 2013. 6. 11. (accessed 2013. 6. 13)

Barki, H., S. Rivard, & J. Talbot. 1993. Toward an Assessment of Software Development Risk. *Journal of Management Information Systems*. 10(2): 203-225.

ISACA. 2013. 2013 CISA Review Manual(Korean translated). *ISACA*. USA.

ISACA. 2009. The Risk IT Framework. *ISACA*. USA.

ISO/IEC 13335-1: 2004. 2004. *Information Technology-Security Techniques-Management of Information and Communications Technology Security-Part 1: Concepts and Models for Information and Communications Technology Security Management*.

Ponemon Institute. 2013. *2013 Cost of Data Breach Study: Global Analysis*. Ponemon Institute.

Yates, J. Frank and Eric R. Stone. 1992. *The Risk Construct in Risk-Taking Behavior*. J. F. Yates. ed. Chichester, UK: John Wiley & Sons.

丁慧貞: 연세대학교에서 박사학위를 취득하고 현재 연세대학교 의과대학 연구조교수로 재직 중이다. 주요 관심분야는 미래 건강정보시스템, 건강정보의 보호관리 등이며 주요 연구로는 "서울시 중심 유비쿼터스 동북아 의료허브 구축(2010)", "글로벌 u-health 서비스 모델 개발(2012)" 등이 있다(xeno@yonsei.ac.kr).

金南鉉: 연세대학교에서 박사학위를 취득하고 현재 연세대학교 의과대학 교수로 재직중이다. 연세의료원 의료정보실장을 역임(2008-2012)하였으며 의료정보 관련 학회, 협회, 단체의 전문위원으로 활동 중이다. 주요 관심분야는 개인건강관리 지원시스템, 건강관리 디바이스 등이다(knh@yuhs.ac.kr).

투 고 일: 2013년 07월 10일
수 정 일: 2013년 08월 21일
게재확정일: 2013년 08월 25일

How Do they Manage Personal Information in Hospital?

– A Survey Study for IT Governance in Hospitals –

Hye Jeong Jeong, Nam Hyun Kim

IT governance aims at risk mitigation and business value delivery. Human resources are important assets of organization but also can be key factor of the threat and vulnerability which may harm that system. Personal information has two sides as the most valuable asset of organization and the target to be protected by the privacy law. The law strictly restricts use of personal identifiable information and sensitive information within narrow limits. To achieve the primary goal, medical treatment, healthcare organizations must deal with personal information. This study is to investigate inherent vulnerability through research survey of hospital staffs who manage information and to examine whether personal health information is safe from threat. 70% of respondents use weak password and one third of them share their password with others. 50.6% of respondents set password for access operating system and only 31.2% log out when not in use. 48.5% save confidential information in their personal storage and only one fourth execute encryption.

Key words: risk management, vulnerability assessment, access control, healthcare organization, health information, password, protect persional information