ISSN 2093-5986(Print)
ISSN 2288-0666(Online)

The Korean Journal of Health Service Management
Vol.9 No.2 pp.23-32 June 2015
http://dx.doi.org/10.12811/kshsm.2015.9.2.023

# 의료기관 종별 웹 사이트 정보보안 관리 실태 연구

김종민[1], 류황건[2]‡
[1]고신대학교 인터넷비즈니스학과, [2]고신대학교 의료경영학과

# A Study on Information Security Management of Hospital Web Sites

Jong-Min Kim[1], Hwang-Gun Ryu[2]‡
*[1]Department of Internet Business, Kosin University,*
*[2]Department of Health Care Administration, Kosin University*

**<Abstract>**

In this paper, we evaluated web security vulnerability and privacy information management of hospital web sites which are registered at the Korea Hospital Association. Vulnerability Scanner (WVS) based on the OWASP Top 10 was used to evaluate the web security vulnerability of the web sites. And to evaluate the privacy information management, we used ten rules which were based on guidelines for protecting privacy information on web sites. From the results of the evaluation, we discovered tertiary hospitals had relatively excellent web security compared to other type of hospitals. But all the hospital types had not only high level vulnerabilities but also the other level of vulnerabilities. Additionally, 97% of the hospital web sites had a certain level of vulnerability, so a security inspection is needed to secure the web sites. We discovered a few SQL Injection and XSS vulnerabilities in the web sites of tertiary hospitals. However, these are very critical vulnerabilities, so all hospital types have to be inspected to protect their web sites against attacks from hacker. On the other hand, the inspection results of the tertiary hospitals for privacy information management had a better compliance rate than that of the other hospital types.

**Key Words : Information Security Management, Privacy Information Protection, Hospital Web Sites, Vulnerability**

‡ Corresponding author : Hwang-Gun Ryu(ryuhg@kosin.ac.kr) Department of Health Care Administration, Kosin University
• Received : Mar 23, 2015 • Revised : May 12, 2015 • Accepted : Jun 18, 2015

# Ⅰ. 서론

의료기관에서 다루는 개인정보는 크게 식별정보와 의료정보로 나누어 볼 수 있고, 식별정보는 성명, 주민등록번호, 연락처, 환자등록번호, 아이디, 비밀번호 등 환자를 식별할 수 있는 모든 개인정보를 말하며, 의료정보는 환자의 건강상태, 신체적 특징, 병력 등 의료인의 진료과정에서 생성되는 진료정보와 환자와 관련된 모든 개인정보를 말한다[1]. 이러한 개인정보는 민감한 정보이고 경제적인 가치도 클 수 있으며 유출시 개인 사생활의 침해 정도가 높고 많은 사회적 문제를 일으키게 된다[2].

미국 의료정보 관리시스템 보안기구의 통계를 보면 조사 응답자의 27%는 지난 1년 동안 최소한 1건의 정보 유출 사고를 경험했으며, 이러한 응답자는 2008년 13%에서 2010년 19%로 증가하였으며, 2012년에는 이보다 더 증가한 것으로 나타났다[3]. 한편 2011년~2012년 국내 기업에서 개인정보 유출사고에 따른 규모는 최소 2만6천 건에서 최대 3500만 건, 손실액은 최소 62억 원에서 최대 1,691억 원에 이르는 것으로 조사되었다[4].

개인정보는 정보화시대에서 보호받아야 될 중요한 자산일 뿐만 아니라, 의료기관에서 다루는 개인정보는 민감한 정보를 많이 포함하고 있기 때문에 안전한 관리가 필수적이다. 의료기관 웹 사이트에서 개인정보가 보호되기 위해서는 웹 보안에 취약성이 없어야 하고, 웹 사이트에서의 철저한 개인정보 관리가 중요하다.

웹 사이트에서 보안 취약성이 존재하게 되면 외부의 공격으로부터 개인 정보가 침해당할 수 있는 상황이 발생할 수 있으므로 정기적인 보안취약성 점검이 필수적이다. 또한 웹 사이트에서 획득되는 개인 정보의 경우 획득, 사용, 폐기에 대한 사용자 동의는 물론, 민감 개인정보의 경우 네트워크를 통한 패킷 전송 시 암호화 과정을 반드시 거쳐야 하고, 안전한 패스워드를 위해 정해진 규칙에 맞게 사용자가 설정하도록 관리하여야 한다. 한편 웹 사이트에서 개인정보 보호를 위한 가이드라인에서는 웹 사이트에서 개인정보 노출은 홈페이지 관리자, 개발자, 사용자의 개인정보 보호에 관한 의식부족에서 발생하는 경우가 많기 때문에 지속적인 교육과 점검이 필요하다고 지적하고 있다[11].

라노위츠는 웹 응용프로그램 보안취약성이 시스템의 보안에 심각한 영향이 있기 때문에 보안취약성에 적극적으로 대처해야 한다고 언급하고 있으며[5], 웹 취약성 분석을 위한 프록시 시스템을 구현하고 설계한 연구에서는 기존 웹 취약점 해결방법을 분석하고 문제점을 해결할 수 있는 취약점 해결방법을 제시하고 있다[6].

기관 웹 사이트에 대한 취약성을 연구한 논문도 있었는데, 호텔기업 웹 사이트에 대해 보안취약성을 평가하는 연구에서는 종별, 지역별 웹 사이트 취약성을 분석하였다[7]. 한편 Web Vulnerability Scanner(WVS)를 이용하여 국내 홈페이지를 대상으로 웹 취약성을 분석한 연구에서는 보안 취약점 진단을 통하여 개인정보보호를 위한 취약점 관리와 개선의 필요성에 대해 주장하였다[8].

국내 의료기관의 정보보안 수준을 측정하기 위한 연구에서는 국내 의료기관의 정보보안 현황파악을 위한 평가모형에 대해 연구하였는데, 이 연구에서는 대형병원 평가모형을 개발하는데 있어 관리적, 기술적, 물리적 보안영역으로 나누어 평가기준을 만들었으며 병상 수와 종별을 고려하여 3개의 병원을 선정한 후 시범 평가를 실시하였다[17]. 이 연구를 통해 의료기관의 전반적인 정보보안 수준을 파악하기에는 평가 대상 병원 수가 제한적이며, 지표를 평가하기 위해 설문지와 전화면담을 실시해야 하기 때문에 정보보안 수준에 대한 평가결과가 병원 관리자의 응답에 의존한다는 한계가 있다.

보안취약성을 진단하고 개인정보관리 실태를 조

사함으로써 보안 사고에 미리 대처하여 안전한 웹 사이트를 만들 수 있기 때문에 개인정보유출과 같은 사고가 발생하기 전에 관심을 가지고 보안관리 실태를 점검해야 한다. 본 연구에서는 국내 의료기관 종별 웹 사이트의 정보보안 관리 실태를 평가하고 분석하였는데, 이를 위해 병원 웹 사이트의 보안취약성과 개인정보관리 실태를 조사하였다. 주요 연구내용으로는 먼저 웹 사이트의 보안취약점 분석을 위해 취약점 점검 스캐닝 도구를 이용하여 의료기관 웹 사이트의 취약점을 분석하였다. 또한 개인정보의 관리와 보호 실태를 조사하기 위한 10개의 평가항목에 따라 웹 사이트를 직접 평가하였다. 평가항목은 개인정보의 획득 과정과 활용에 대한 동의 절차 준수 여부, 웹 사이트에서 중요 개인정보의 암호화 전송 여부, 관리자나 사용자의 홈페이지 관리 실태를 조사하기 위한 문항으로 구성하였다. 보안취약성과 개인정보관리 실태 평가를 통해 병원 웹 사이트에서의 정보보안 관리 실태의 문제점을 파악하고 개선 방안에 대해 제시하였다.

## Ⅱ. 연구방법

### 1. 평가 대상 및 기간

본 연구에서는 대한병원협회에 등록된 병원 중 상급종합병원, 종합병원, 전문병원, 병원에 대해 각각 25개의 웹 사이트를 무작위 추출로 선정하여 총 100개의 병원 웹 사이트를 평가 대상을 선정한 후 정보보안 관리 실태를 평가하였다. 평가는 2015년 1월 2일 부터 2015년 2월 27일까지 실시하였다.

### 2. 평가 방법

본 연구에서는 병원 종별 정보보안 관리 실태를 연구하기 위해 병원 웹 사이트에 대해 보안취약성과 개인정보관리 실태를 평가하였다. 보안취약성 평가와 개인정보관리 실태 평가 방법은 다음과 같다.

#### 1) 보안취약성 평가 방법

보안취약성 평가는 <Table 1>과 같은 OWASP Top 10(Open Web Application Security Project Top 10 Risks)[9] 위험요소를 기본으로 보안취약점을 스캐닝하는 WVS(Web Vulnerability Scanner)를 이용하여 분석하였다. OWASP Top 10은 OWASP에서 발표하는 보안위험 리스트인데 보안상 심각한 영향을 줄 수 있는 위험요소 10가지를 선정한 것이다[8]. OWASP는 웹 보안 전문가들이 자발적으로 참여해 제작된 오픈 프로젝트 그룹으로 어플리케이션 보안향상에 관심이 있는 사람이면 누구에게나 공개되어 있다[10]. 웹 취약점 스캐닝 도구는 개발사와 특징에 따라 여러 가지 도구가 개발되어 있는데[7][8], 본 연구에서는 관련 연구 [8]에서 사용한 Acunetix WVS를 이용하여 취약점을 스캐닝하였다.

<Table 1> OWASP Top 10 Risk (2013)

| OWASP Top 10 Risk (2013) | |
|---|---|
| A1 | Injection |
| A2 | Broken Authentication and Session Management |
| A3 | XSS(Cross Site Scripting) |
| A4 | Insecure Direct Object References |
| A5 | Security Misconfiguration |
| A6 | Sensitive Data Exposure |
| A7 | Missing Function Level Access Control |
| A8 | Cross Site Request Forgery(CSRF) |
| A9 | Using Known Vulnerable Components |
| A10 | Unvalidated Redirects and Forwards |

Reference : Acunetix Website Audit, OWASP Top 10 2013

WVS를 활용하여 웹 사이트의 취약성을 분석한 결과의 한 예를 <Figure 1>에 나타내었는데, 스캐닝한 해당 웹 사이트의 취약성의 위험도에 따라 <Table 2>에서 설명된 High, Medium, Low Level, 그리고 Informational alerts으로 분류하여 취약점을 나타내주기 때문에 웹 사이트의 보안취약성 상태를 일목요연하게 알 수 있게 해준다.

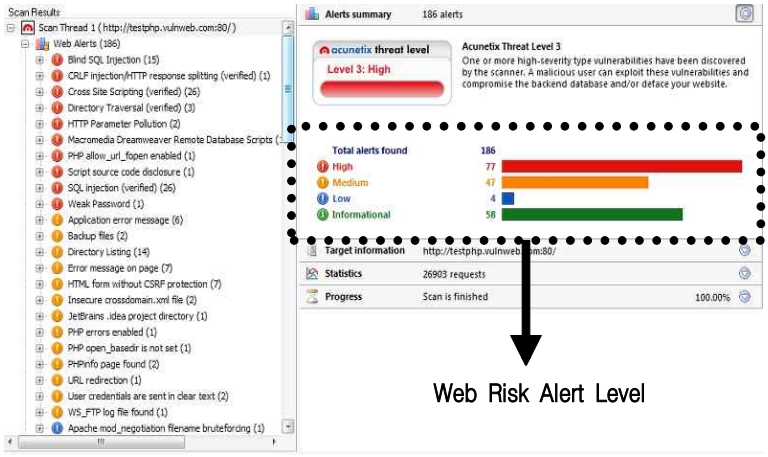
### 2) 개인정보 관리실태 평가 방법

홈페이지에서 안전한 정보보안 관리를 위해 개인정보를 어떻게 관리해야하는지에 대한 사례별 조치들이 홈페이지 개인정보 노출방지 가이드라인에 설명되어 있다[11]. 본 연구에서 병원 웹 사이트에서 개인정보 관리 실태를 평가하기 위해 가이드라인 중 웹 사이트에서 사용자가 직접 평가할 수 있는 10개의 항목들을 선별하여 <Table 3>에서와 같은 개인정보 관리실태 평가항목을 구성하였다.

<Table 2> Web Risk Alert Level

| Risk Alert Level | Alerts category |
|---|---|
| High | the most dangerous, which put a site maximum risk for hacking and data theft |
| Medium | server misconfiguration and site-coding flaws, which facilitate server disruption and intrusion |
| Low | lack of encryption of data traffic, or directory path disclosures |
| Informational alert | the possible disclosure of an internal IP address or email address, or matching a search string found in the Google Hacking Database |

Reference : Web Vulnerability Scanner v9.5 Product Manual




<Figure 1> Example of scanning result using WVS

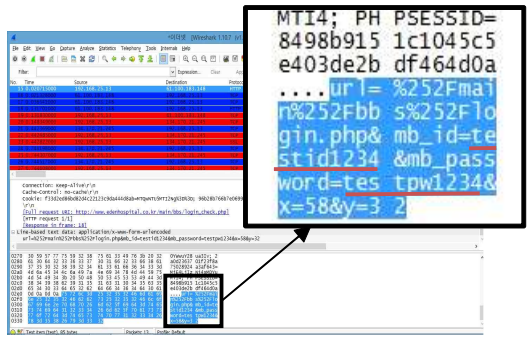
<Table 3> Evaluation items for Privacy Information Management

| Domain | Item No. | Evaluation Items |
|---|---|---|
| A. Procedure and consent for privacy Information | (1) | Consent procedure of privacy information for gathering, using, and purpose |
| | (2) | Consent procedure for giving privacy information to a third party |
| | (3) | Destruction procedure for privacy information |
| B. Security for privacy Information | (4) | Encryption of sensitive privacy information(resident registration number, phone number, name) |
| | (5) | Encryption of user id and password |
| | (6) | Secure password system |
| | (7) | Various ways(I-PIN, certificate digital signature etc.) to user authentication |
| C. Management of web site | (8) | Management for privacy information in posting |
| | (9) | Management for privacy information from external search engines. |
| | (10) | Instructions for protecting privacy information in the web sites |

개인정보 관리실태 평가항목은 크게 A, B, C 세 개의 평가영역으로 나누었다. A 영역은 개인정보 수집, 제공 그리고 파기에 관한 공지 절차의 준수에 관한 것으로[11][18], 각 절차가 사용자에게 제시되고 지켜지고 있는지를 평가하였다.

B 영역은 정보보안과 관련된 평가항목인데, 회원가입 시 전송되는 주민등록번호, 이름, 사용자 아이디와 패스워드 등 민감 개인정보를 암호화하여 전송하는지를 평가하기 위해서 <Figure 2>에서와 같이 네트워크 패킷 분석 프로그램인 와이어샤크(Wireshark)[12]을 이용하여 개인정보 전송 패킷을 조사하여 암호화 여부를 판단하였다. 안전한 비밀번호 평가에서는 비밀번호가 최소 10자리 이상의 경우는 영대문자, 영소문자, 숫자 및 특수문자 중 2종류이상으로, 최소 8자리 이상의 경우는 3종류 이상으로 구성되어 있는지를 평가한다[13]. 홈페이지 가입 시 주민등록번호를 대체할 수 있는 다른 개인인증 방법이 있는지에 대한 항목에서는 I-PIN 혹은 공인인증서, 기타 다른 대체 인증 방법의 제공여부에 대해 평가한다.

C 영역은 웹 사이트 관리에 관한 평가항목으로, 관리자와 사용자의 실수로 홈페이지에서 게시된 글에 개인정보가 포함되어 있는지 평가하고, 외부 검색엔진으로부터 검색된 자료에서 개인정보가 유출되는지의 여부를 살펴보기 위해 구글 검색엔진을 이용하여 병원 웹 사이트에서 특정 확장자를 가진 파일(.pdf, .xls, .doc, .hwp 등)을 검색한 후, 검색된 파일에서 개인정보가 존재하는지를 조사한다. 또한 홈페이지에서 사용자들이 글이나 자료를 게시할 경우 개인정보 노출에 대해 유의할 수 있도록 적절한 안내문을 홈페이지에 공지하고 있는지의 여부에 대해 평가한다.




<Figure 2> Example of packet transmission without encrypting of user id(testid1234) and password(testpw1234) using Wireshark program

# Ⅲ. 연구결과

## 1. 보안취약성 분석 결과

WVS를 이용하여 분석한 병원 종별, 취약점 레벨별 평가결과를 살펴보면 <Table 4>에서와 같다. High 레벨 취약점은 상급종합병원 웹 사이트 중에서 103개의 취약점이 발견되었으며, 종합병원, 전문병원, 병원의 경우는 각각 2,061개, 1,108개, 2,181개의 취약점이 발견되어 총 100개의 웹 사이트에서 총 5,453개의 High 레벨 취약점이 발견되었다. High 레벨 취약점은 해킹과 데이터 도난의 심각한 위험에 처할 수 있는 가장 위험한 항목을 분류되는 취약점[7][14]이기 때문에 반드시 점검이 필요한 상황이라고 볼 수 있다.

상급종합병원의 경우 High 레벨의 취약점이 상대적으로는 다른 규모의 병원에 비해 적은 것으로 조사되었지만 전체 취약점은 총 3,097개로 나타났으며, 종합병원, 전문병원, 병원의 경우 각각 4,894개, 3,252개, 3,671개로 나타나 병원 종별에 상관없이 취약성이 발견된 것으로 나타났다.

병원 규모에 따른 취약점 발생 빈도를 50개 등간격으로 나누어 분포를 분석한 결과를 살펴보면 <Table 5>와 같다. 상급종합병원의 경우 어떤 레벨의 취약점도 전혀 발견되지 않은 웹 사이트가 2개로 나타났으며, 취약점이 1개 이상 존재하는 웹 사이트가 23개로 나타나 보안 취약성 비율은 92%로 조사되었으며, 종합병원, 전문병원, 병원의 보안 취약성은 각각 96%, 100%, 100%로 나타났다. 전체 병원 100개의 웹사이트에 대해서는 97개의 웹 사이트에서 한 개 이상의 취약점이 발견되어 97%의 보안취약성을 나타내었으며, 거의 대부분의 병원 웹 사이트에서 보안취약성은 존재하는 것으로 분석되었다.

<Table 4> Inspection Result for Web Vulnerability

unit: N(%)

| Classification | Risk Alert Level | | | | Total |
|---|---|---|---|---|---|
| | High | Midium | Low | Informational alert | |
| Tertiary hospitals | 103( 3%) | 625(20%) | 330(11%) | 2,039(66%) | 3,097(100%) |
| General hospitals | 2,061(42%) | 1,036(21%) | 321( 7%) | 1,476(30%) | 4,894(100%) |
| Specialty hospitals | 1,108(34%) | 752(23%) | 377(12%) | 1,015(31%) | 3,252(100%) |
| Hospital | 2,181(59%) | 503(14%) | 288( 8%) | 699(19%) | 3,671(100%) |

<Table 5> Web Vulnerability

unit: N(%)

| N / Classification | none | 1~50 | 51~100 | 101~150 | 151~200 | 201~ | Total | Vulnerability percent |
|---|---|---|---|---|---|---|---|---|
| Tertiary hospital | 2(8%) | 9(36%) | 5(20%) | 1( 4%) | 2( 8%) | 6(24%) | 25(100%) | 92% |
| General hospitals | 1(4%) | 9(36%) | 2( 8%) | 3(12%) | 2( 8%) | 8(32%) | 25(100%) | 96% |
| Specialty hospital | 0(0%) | 7(28%) | 8(32%) | 2( 8%) | 3(12%) | 5(20%) | 25(100%) | 100% |
| Hospital | 0(0%) | 12(48%) | 416%) | 3(12%) | 1( 4%) | 5(20%) | 25(100%) | 100% |

WVS로 웹 사이트를 스캐닝하여 분석한 보안취약점 결과 중 SQL Injection과 XSS(Cross Site Scripting)는 심각한 정보보안 문제가 발생할 수 있는 대표적이고 오래된 보안취약점이므로 이 취약점들에 대한 병원의 대응실태를 살펴보기 위해 병원 규모별 발생 빈도를 조사하였다. SQL Injection은 조작된 질의문을 삽입하여 웹 서버의 데이터베이스 정보를 열람 또는 조작할 수 있는 취약점이며[16], XSS는 공격자가 입력이 가능한 폼(주소입력 또는 게시판 등)에 악의적인 스크립트를 삽입하여 사용자 세션을 도용하거나 악성코드를 유포할 수 있는, 비교적 쉽게 공격할 수 있는 취약점이다[16]. 전 세계 시스템 공격방법 통계에서 SQL Injection은 3위(17%), XSS는 4위(6.2%)를 차지하는 등 여전히 주의를 요하는 취약점으로 조사되었다[15].

SQL Injection과 XSS 중 XSS가 규모에 상관없이 상대적으로 더 높은 빈도로 나타났으며, 상급종합병원에서 경우 13개의 SQL Injection이 발견되었고 다른 종별 병원에서는 상급종합병원에 비해 높은 빈도로 SQL Injection이 발생하였다. 이것은 상급종합병원에 비해 다른 규모의 병원이 상대적으로 보안취약성이 높다는 것을 나타낸다. 한편, XSS의 경우 상급종합병원에서 65개가 발견되었으며, 다른 규모의 병원보다는 상대적으로 매우 낮은 빈도로 발견되었다. 상급종합병원의 경우, SQL Injection과 XSS 보안취약점 개수는 78개로 다른 종별 병원보다 현저히 낮은 것을 볼 수 있으나, 이 취약점은 웹 사이트 보안에 치명적인 영향을 미칠 수 있는 악성 취약점이므로 발생 빈도와 상관없이 반드시 개선되어야 될 것으로 보인다. 또한 종합병원 이하 규모의 병원은 이 두 보안 취약점에 대해 심각하게 노출되어 있다고 판단되며, 이 두 취약점에 대해 시급한 점검이 필요한 것으로 나타났다.

## 2. 개인정보 관리실태 분석 결과

병원 웹 사이트에서 개인정보 관리 실태를 분석함으로써 정보보안 관리 실태를 조사하였는데, <Table 2>에 나타난 평가항목들을 이용하여 평가한 병원 종별 개인정보 관리실태 평가결과는 <Table 7>과 같다. 상급종합병원의 경우 평균 준수율이 86%를 나타내고 있으며, 종합병원, 전문병원, 병원의 경우 각각 68%, 60%, 60%의 준수율로 나타나 병원 규모가 작을수록 준수율이 떨어지는 것을 확인할 수 있다.

<Table 6> SQL Injection, XSS

| Classification / Vulnerability | Tertiary hospital | General hospital | Specialty hospital | Hospital | Total |
|---|---|---|---|---|---|
| SQL Injection | 13( 2%) | 205(38%) | 181(33%) | 147(27%) | 546(100%) |
| XSS | 65( 1%) | 1,752(37%) | 908(20%) | 2,058(43%) | 4,783(100%) |

XSS : Cross Site Scripting

<Table 7> Inspection Result for Privacy Information Management unit: %

| item / classification | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | Average compliance percent |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Tertiary hospital | 100 | 100 | 92 | 88 | 92 | 56 | 92 | 98 | 100 | 34 | 86 |
| General hospital | 100 | 76 | 100 | 64 | 56 | 4 | 50 | 92 | 100 | 28 | 68 |
| Specialty hospital | 92 | 84 | 88 | 40 | 40 | 8 | 40 | 68 | 100 | 32 | 60 |
| Hospital | 92 | 88 | 92 | 36 | 32 | 16 | 22 | 84 | 100 | 24 | 60 |
| compliance rate | 96 | 87 | 93 | 57 | 55 | 21 | 51 | 86 | 100 | 30 | - |

(1)~(10) : Evaluation Item number in <Table 3>

평가항목에 따른 병원 종별 평가 결과를 살펴보면, 상급종합병원의 경우 전반적으로 높은 준수율을 나타내고 있으나 로그인시 비밀번호 체계의 적합성 여부를 살펴보는 (6)번 항목과 웹 사이트에서의 개인정보 관리를 위한 안내문의 게시 여부를 평가하는 (10)번 항목에서 낮은 평가를 받았다.

종합병원, 전문병원, 병원의 경우는 수집된 정보보안 평가그룹과 관련된 문항 (4)~(7)번에서 낮은 준수율을 보이고 있는데, 이들 병원의 경우 중요한 개인정보가 패킷으로 전송될 때 반드시 암호화를 해야 함에도 불구하고 암호화를 하지 않는 병원이 많았기 때문이다. 이렇게 암호화 없이 전송되는 개인정보는 유출될 수 있으므로 반드시 개선되어야 한다. 특히 로그인시 비밀번호의 체계가 보안수준에 적합한지를 평가하는 (6)번 문항의 경우 매우 낮은 준수율을 나타내었다. 이것은 비밀번호 체계를 안전한 수준으로 유지했을 때 사용자가 비밀번호 분실 시 발생하는 민원처리과 사용자의 불편을 고민하여 낮은 수준의 비밀번호 체계로도 생성가능하게 하였거나, 안전한 비밀번호를 위한 지침을 준수하지 않고 자의적인 지침으로 생성 가능하게 하였기 때문으로 판단된다. 또한 개인정보 관리를 위한 안내문의 게시 여부를 평가하는 (10)번 문항에서도 낮은 평가를 받아 개선이 필요한 것으로 판단된다. 이러한 문제가 발생하는 이유는 병원 규모가 작을수록 웹 사이트 개발 과정에서 보안 의식이 있는 전문가가 개입하지 않거나 외부업체에 웹 사이트를 개발 의뢰하는 단계에서 개인정보를 보호하기 위한 다양한 조치를 철저히 요구하지 않았기 때문으로 판단된다.

결론적으로 규모에 상관없이 개인정보를 획득하고 처리하고 활용하는 동의 여부는 잘 준수하고 있지만 웹 사이트를 통해 전송되는 개인정보의 암호화 항목에서는 병원 종별로 평가 결과가 큰 편차가 있으며 규모가 작을수록 평가가 좋지 못해 시급한 개선이 필요한 것으로 조사되었다. 한편 안전한 비밀번호 설정 원칙은 규모에 상관없이 잘 지켜지지 않고 있어 개선이 필요하다.

## Ⅳ. 고찰 및 결론

최근 정보보안에 관한 관심이 높고 이와 관련된 여러 가지 사회적인 문제가 발생하고 있다. 의료기관의 경우, 민감한 개인정보를 다루고 있기 때문에 의료기관 웹 사이트에 대한 정보보안 관리는 매우 중요한 문제이다. 의료기관 웹 사이트의 정보보안 관리 실태를 평가하기 위해 본 연구에서는 웹 보안취약점과 개인정보관리 실태에 대해 평가하였다. 보안취약점이 많을수록 웹 사이트는 외부의 공격으로부터 정보를 보호하기 어렵게 되며, 개인정보 관리실태가 부실하게 되면 웹 사이트에서 개인정보가 노출될 가능성이 높아지게 된다.

본 연구에서는 100개의 국내 의료기관 웹 사이트에 대해 정보보안 관리 실태를 평가하고 분석하였다. 보안취약점 평가에서는 상급종합병원의 경우 다른 규모의 병원보다 취약점이 상대적으로 우수한 것으로 나타났으나, 103개의 High level 취약점이 검출되어 정보보안을 위한 취약점 점검이 필요한 것으로 평가되었다. 종합병원, 전문병원, 병원의 경우 High level 취약점 뿐 만아니라 다른 레벨의 취약점도 규모와 상관없이 발견되어 안전한 웹 사이트를 위한 취약점 점검이 필요하다고 판단된다. 병원 종별 보안취약성 비율에서는 취약점이 없는 병원은 상급종합병원, 종합병원의 경우 각각 2개와 1개에 불과해 거의 대부분의 병원에서 보안취약점이 존재하는 것으로 조사되었다.

SQL Injection과 XSS의 경우 상급종합병원은 다른 규모의 병원보다 상대적으로 취약점이 작은 것으로 조사되었으나 취약점의 위험도를 고려할 때 취약점을 개선하는 노력이 필수적이라고 판단된다. 본 연구에서는 보안취약성 평가를 위해 자동회된 취약점 스캐닝 도구 사용하였는데, 자동화된 도구

의 한계점을 고려하더라도 병원 웹 사이트의 경우 규모에 상관없이 정보보안 관리를 철저히 하기 위해 보안취약성 개선을 위한 지속적인 관심과 노력이 필요하다고 판단된다.

한편, 웹 사이트에서의 개인정보 관리 실태를 조사한 결과에서는 상급종합병원의 경우 준수율이 86%로 나타나 상대적으로 다른 규모의 병원보다 관리 상태가 우수한 것으로 조사되었다. 그런데 비밀번호에 대해 엄격한 보안수준의 체계를 요구하지 않고 있다는 문제가 도출되었다. 이러한 문제는 보안수준이 우수한 길고 복잡한 비밀번호를 사용하게 할 경우 나타날 수 있는 사용자의 불편을 줄여 주기 위한 편의주의로 판단된다. 종합병원, 전문병원, 병원의 개인정보 관리 실태를 살펴보면 민감한 주요 개인정보를 전송할 때 패킷을 암호화하지 않는다는 심각한 문제가 많은 병원에 있는 것으로 조사되어 시급한 개선이 필요하다. 이러한 문제가 발생하는 이유는 규모가 작을수록 웹 사이트 개발 및 운영 예산과 전문 인력 부족, 그리고 개발자의 정보보호 의식이 부족해서 발생한 것으로 보인다. 민감 개인정보의 암호화는 정보보안을 위해 필수적인 사항이므로 반드시 개선할 필요가 있다.

국내 의료기관의 정보보안 수준을 평가하기 위한 기존의 연구에서는 병원에서 종사하는 담당자의 응답에 의존하는 설문평가 방식인 반면, 본 연구에서는 의료기관 웹 사이트에서 획득되는 정보만으로 정보보안 관리 실태를 파악하였으며, 계속 발전하고 변화하는 보안 위협으로 인해 발생할 수 있는 중요 보안 취약점을 자동화된 도구로 평가하고 분석하였다는 차이점이 있다.

웹 사이트에서 정보보안 관리를 철저히 하기 위해서는 (1)웹 사이트의 개발 단계에서부터 정보보호를 위한 규정을 철저하게 준수해야하며, (2)관리자와 사용자로 인해 웹 사이트에서 개인정보가 유출될 수 있으므로 교육과 인식개선을 위한 노력이 필요하며, (3)보안취약성을 효과적으로 관리하기 위해 웹 취약성 스캐닝 도구를 이용하여 주기적으로 취약성을 점검하고 발견된 취약점을 제거하여야 한다.

## REFERENCES


1. MPIS(2014), Proceedings of Medical Center Privacy Information Security, pp.142-143.
2. Y.J. Jeon(2012), The Medical Information Protection and major Issues, J of The Korea Society of Computer and Information, Vol.17(12);251-258.
3. HIMSS(2012), 2012 HIMSS Analytics Report: Security of Patient Data, Kroll, p.11l.
4. E.S. Kang(2015), Information Security for CxO, Hanbit media, pp.60-61.
5. T. Lanowitz(2005), Now is the time for security at Application Level, Gartner Research, pp.3-7.
6. G.H. Kim(2014), Implementation and Design of Proxy System for Web vulnerability Analysis, JKIECS, Vol.9(9);1011-1018.
7. Y.K. Shin(2014), Evaluation of Vulnerabilities in the Hotel Industry's Website, J of Korean Academic Society of Hospitality Administration, Vol.23(3);123-143.
8. H.S. Jang(2012), Vulnerability Analysis using the Web Vulnerability Scanner, J. of Korea Convergence Security, Vol.12(4);71-76.
9. OWASP, http://www.owasp.org
10. J.H. Lee(2011), Study on the OWASP and WASC-oriented Web Application Security, The journal of Korea Navigation Institute, Vol.15(3);372-377.
11. MOPAS(2012), Guidelines for Protecting Privacy Information in Web Sites, Ministry of Public Administration and Security, pp.16-38l.

12. Chris Sanders(2007), Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, No Starch Press, pp.2-12.
13. KISA(2010), User Guide for Safe Password 2010-22, KISA, pp.6-8.
14. Acunetix(2014), Web Vulnerability Scanner v.9.5 Product Manual, Acunetix, pp.36-37.
15. Y.K. Seong(2013), Internet & Security Focus 2013, Korea Internet & Security Agency, pp.73-74.
16. KISA(2013), Guide for Diagnosing and Eliminating Web Vulnerabilities, KISA, pp.13-32.
17. S.J. Ahn, S.M. Kwon(2005), A Development of the Model for Evaluating the Security of Information Systems in Health Care Organizations, J. of Koean Society of Hospital Management, Vol.10(4);98-112.
18. Y.J. Jeun(2013), EMR System and Patient Medical Information Protection, The Korean Journal of Health Service Management, Vol.7(3);213-223.