개인정보보호를 위한 정보시스템 보안감사 방법에 관한 연구

이 동 녁* · 박 정 선*
*명지대학교 산업경영공학과

A Study on the Information System Security Audit Method for Personal Information Protection

Dong-Nyuk Lee* · Jeong-Sun Park*
*Dept. of Industrial Engineering, Myong Ji University

Abstract

To give a solution to solve personal information problems issued in this study, the domestic and overseas cases about information security management system including an authentication technique are analyzed. To preserve the outflow of personal information, which is such a major issue all over the world, a new security audit check list is also proposed.

We hope this study to help information system developers construct and operate confidential information systems through the three steps: Analysis of risk factors that expose personal information, Proposal to solve the problem, Verification of audit checking items.

Keywords : Personal Information, Security Audit, Information Protection

1. 서 론

하루가 다르게 변해 가는 인터넷과 정보통신 인프라의 발전은 지난날 오프라인에서 처리하던 대부분의 정보를 온라인에서 처리할 수 있도록 변화시키고 있으며, 정치, 경제, 사회, 문화, 교육 등 대부분의 분야에 큰 영향을 미치고 있다. 이와 함께 최근 모바일의 급속한 성장을 통해 시간과 장소의 제약을 받지 않고 필요로 하는 정보를 얻을 수 있는 정보화의 변화는 우리의 일상생활에 많은 편리함을 제공해 주고 있다.

우리나라 인터넷 이용자 수는 2000년 1,940만 명에서 2009년 2574만 명으로 증가하였으며, 보급률은 2009년 기준으로 세계에서 가장 높은 수준인 72%에 달하고, 2011년에는 77.3%까지 증가할 것이라고 예상하고 있다.

세계 최고수준의 인터넷 이용환경을 바탕으로 인터넷에 기반한 금융거래 및 전자상거래 규모가 급증하게 되었지만, 이를 악용한 정보화 역기능으로 정보유출, 불법정보의 유통, 인터넷상의 사기, 해킹 등을 이용한 사이버테러 등이 나타나고 있다.

정보화 역기능 피해현황을 살펴보면 2008년 한 해 동안 컴퓨터, 웜, 트로이잔 피해를 경험한 사업체는 41.4%로 추정하고 있으며, 개인의 경우 해킹 피해 경험률은 2007년 15.4%에서 2008년 18.8%로 증가하였다.

특히 여기에서 주목할 만한 점은 인터넷 이용자들이 가장 우려하는 역기능 조사 결과 '개인정보 및 프라이버시 침해'인 것으로 나타났다. 이러한 결과는 정보화 사회에서 개인정보가 상업적 가치를 지니게 되어 개인정보의 유출 및 오·남용 사례가 급증하였으며, 유출된 개인정보는 개인의 프라이버시 침해는 물론 명의도용, 보이스피싱 등을 통해 제2의 피해까지 발생시킬 수 있다는 점 때문인 것으로 나타났다.

† 교신저자: 박정선, 경기도 용인시 처인구 남동 명지대학교 공학관 507호
M · P: 019-208-6453, E-mail: jspark@mju.ac.kr
2010년 10월 20일 접수; 2010년 12월 1일 수정본 접수; 2010년 12월 3일 게재확정

대부분의 개인정보 유출사고는 사용자 부주의 보다는 기업의 개인정보 관리소홀 및 정보시스템의 보안취약점을 통해 나타나고 있으며, 유출된 개인정보는 개인의 프라이버시 침해는 물론 상업적 이용으로 경제적 손실까지 입힐 우려가 있어 사회적 문제로 대두되고 있는 상황이다.

따라서 본 논문에서는 정보시스템 운영시 개인정보가 유출될 수 있는 위험을 분석하여 해결방안을 제시하고, 그에 따른 감사 점검항목을 도출하여 안심하고 온라인 서비스를 이용할 수 있는 신뢰기반의 정보시스템 구축 및 운영에 도움을 주고자 한다.

2. 이론적 고찰

2.1 개인정보

일반적으로 개인정보의 의미는 '생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보' 혹은 '생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아 볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보'(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제6호)를 말하며, 이러한 개인정보 등과 사실에 관한 자료로서 특정 개인에게만 한정되어 당해 개인을 알아 볼 수 있는 자료와 자료 자체로는 개인적인 특성을 직접 찾을 수 없는 전자와 결합하였을 때, 그 내용이 구체적으로 드러나는 개인관련 자료라고 할 수 있다.

이와 같이 개인정보는 개인의 인격주체성이 현출될 수 있는 일체의 정보만을 의미하므로, 개인과 관련된 모든 자료를 개인정보로 볼 수는 없다. 즉, 개인과 관련된 모든 자료가 아니라 본인의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 당사자인 정보주체의 안녕과 이해관계에 영향을 미칠 수 있는 개인을 식별할 수 있는 정보를 개인정보라고 할 수 있다.

위와 같은 내용들을 종합하여 개인정보의 개념을 종합해 보면 생존하는 자연인의 내면적 사실, 신체나 재산상의 특질, 사회적 지위나 손상에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체를 일컫는 것으로 정의할 수 있다.

2.2 정보시스템 보안감사

감사(auditing)는 특정조직의 자원처리와 보안이 정해진 규정에 따라 올바르게 수행되는가를 조사하는 제3자의 독립된 활동이며 정보시스템 감사는 정보시스템의 활용기술과 운영을 감사대상으로 한다.

정보시스템 보안감사는 정보시스템의 취약요소를 종합적으로 점검, 평가하여 관계자에게 조언, 권고함으로써 보안측면의 피해를 최소화하는 등 건전한 시스템을 도모하고자 하는 특징을 보인다.

조직의 모든 활동은 나름대로 그 목적을 가지고 있는데, 조직의 경영 목적을 달성할 수 있는 방향으로 수행된다. 따라서 정보시스템에 관련된 활동들도 다른 경영활동과 마찬가지로 조직의 경영목적을 달성할 수 있는 방향으로 수행되어야 한다.

2.3 정보시스템 보안 관리체계와 관련된 각종 기준

2.3.1 BS7799

BS7799란 영국표준협회 (British Standards Institution)에서 정보보호 관리를 위해 1995년에 제정된 표준규격이다. 기업이 고객 정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 두고 있으며, BT, HSBC, Marks and Spencer, Shell International, Unilever 등 주요 업체와 더불어 영국의 상무성 주관으로 "정보보안관리 실무 규범 (A Code of Practice for Information Security Management)"이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 개발되었으며, 조직에서 활용할 수 있는 보안 표준의 기반이 되도록 고안되었다.

다른 보안관리 표준 지침들이 IT를 대상으로 보안 기술의 상세까지 규정하고 있는데 비해, BS7799는 관리시스템에 대한 보편적, 포괄적인 가이드, 기준을 나타내고 있으며, IT 자산을 전자매체로 한정하지 않고 종이 매체 등 여러 가지 정보자산을 보안의 대상으로 규정하고 있다. 조직에 대해서 획일적인 요구사항을 부과하는 것이 아니라, 각각 조직이 위험 분석을 수행한 후 이를 기초로 하여 보안 관리를 실시할 것을 요구하고 있다.

2.3.2 ISO 27001

ISO 27001은 정보보안 관리체계 인증규격(Specification for Information Security Management)으로 2005년에 BS7799의 Part2에서 국제표준으로 전환되었다. 정보보안 관리체계(Information Security Management System)의 수립, 설계, 운영, 감시, 검토, 유지 및 개선을 규정하기 위해 제정되었으며, ISO 27001을 획득하였다는 것은 그 조직이 정보보안 관리체계를 수립하여 제3의 인증기

관으로부터 정보보안 관리의 적합성과 실행상태를 평가받아 그 결과를 신뢰할 수 있다는 것을 의미한다.

ISO 27001은 효과적인 정보보호 활동을 위해 같이 “계획(Plan)단계-실행(Do)단계-확인(Check)단계-조치(Action)단계”를 따르고 있다. 이의 목적은 보호해야 할 자산을 식별하고, 이를 누가 어떤 형태로 어디에 보관, 사용하고 있는지를 파악하고, 그 자산에 어떠한 위협과 취약성이 존재하며, 그 가능성은 얼마나 높으냐를 바탕으로 적절한 보안 대책들을 구현하는 것이다.

3. 개인정보보호를 위한 감사 접근방법

3.1 개인정보 유출방지를 위한 감사 점검항목

개인정보 유출방지를 위한 감사 점검항목은 개인정보 생명주기별 침해방법에서 도출된 위험과 개인정보보호 관련법률인 「정보통신망법」의 개인정보보호 관련 조항, 개인정보의 기술적·관리적 보호조치 기준 해설서인 '개인정보보호 핸드북'의 세부 조항, '개인정보보호 지침 해설서'를 포함하였다. 또한 유사 감사기준의 문제점을 개선하여 반영하였으며, 최근 정보시스템에서 개인정보 유출의 주된 경로로 이용되고 있는 웹 어플리케이션 강화를 위한 목적으로 OWASP Top 10(2007)을 기반으로 점검항목을 추가하였다.

각 점검항목은 개인정보 생명주기 및 점검범위에 따라 11개의 통제 분야, 92개 점검항목으로 이루어져 있으며, 각 점검항목에 대한 관련 법률과 유사 감사기준, OWASP Top 10 연관도를 포함한 상세 점검항목은 다음과 같다.

[표 3.1] 각 점검항목 별 연관도 기준

구분	내용
관련법률	- 「정보통신망법」의 개인정보보호 관련 조항 - 개인정보의 기술적·관리적 보호조치 기준 해설서인 '개인정보보호 핸드북'의 세부 조항 - 개인정보지침 해설서
유사 감사 기준	- 정보보호 관리체계 국제 표준(ISO 27001) - 한국정보보호진흥원 인증체계인 ISMS
OWASP Top 10	- OWASP Top 10 (2008년도 발표자료 기준)

[표 3.2] 감사항목1 - 개인정보보호 관리체계의 검토

구분	점검항목	유사감사기준	관련법률
개인정보 보호정책	조직 내부적으로 개인정보보호를 구체적으로 시행하기 위한 개인정책이 수립되어 있는가?	√	√
	문서화된 개인정보보호 정책은 최고경영자의 승인을 받았는가?	√	
	사내 개인정보보호 정책은 모든 임직원 및 관련자에게 공개되고 공유되고 있는가?	√	√
	조직 내 개인정보보호 정책은 정기적인 검토 또는 관련 법령의 제·개정, 보안기술의 발전 등에 따라 수시로 변경되어 공개되고 있는가?	√	
	개인정보보호 정책에 의해 정의된 정보시스템 및 보안시스템 등의 운영 절차를 문서화하고 있는가?	√	√
	개인정보에 대해 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 정의하여 문서화하고, 법규 및 규정, 요구사항 등을 검토하고 있는가?	√	√
개인정보 관리조직	개인정보보호 업무를 체계적으로 이행하기 위한 내부 조직체계가 구축되어 있는가?	√	√
	개인정보보호에 관한 업무를 총괄 관리하기 위한 개인정보보호 관리책임자가 지정되어 있는가?	√	√
	개인정보보호 업무를 이행하거나 개인정보를 이용·처리하기 위한 역할과 책임을 문서화하고, 문서화 내용에는 정칙 수립, 구현, 운영 등의 일반적인 책임과 개인정보의 보호와 활동에 대한 구체적인 책임이 포함되어 있는가?	√	√

[표 3.3] 감사항목2 - 개인정보의 수집 · 이용 · 제공

구분	점검항목	유사감사 기준	관련법률
개인정보의 이용 · 제공	수집되는 개인정보가 개인정보를 처리하는 시스템 뿐 만 아니라 타 조직이 운영하는 시스템 등과 연계되어 활용될 경우 이에 대한 통제 및 감독 절차가 마련되어 있는가?	√	√
	개인정보 처리를 위한 시스템이 다른 시스템과 연계되어 활용된다면 각각의 시스템을 연결하기 위해 주민등록번호와 같은 개인 식별도구가 활용될 경우 식별도구 사용이 개인정보 관련 법률이나 지침 · 가이드라인 등에 위반되는지를 검토하였는가?	√	

[표 3.4] 감사항목3 - 외부인의 개인정보 처리

구분	점검항목	유사감사 기준	관련법률
외부인의 개인정보 처리	정보시스템 운영 계획에 개인정보 처리의 외부 위탁에 관한 사항이 명시적으로 규정되어 있는가?	√	√
	수탁업체 또는 협력업체 등에서 접근할 수 있는 개인정보의 범위가 명확하게 정의되고 문서화되어 있는가?	√	√
	위탁업체, 협력업체, 서비스제공업체 등 개인정보를 위탁하거나, 개인정보 처리 시스템을 이용하는 외부조직과 계약시 개인정보보호와 관련한 관리 · 통제 사항의 절차 및 책임 등을 계약서상에 명시하고 있는가?	√	√
	위탁 처리되는 개인정보가 안전하게 관리될 수 있도록 위탁 업무의 범위 내에서 수탁업체에 대한 적절한 관리 · 통제시스템이 구축되어 있는가?	√	√
	위탁업체 및 기타 치부조직들의 시스템 접근 및 활동에 대한 기록을 남기고, 주기적으로 검토하고 있는가?	√	√
	외부위탁 업체가 개인정보 처리에 있어 계약서 및 보안 요구사항 이행 여부에 대한 감사 및 점검을 주기적으로 실시하는가?	√	√

[표 3.5] 감사항목4 - 개인정보 보유 및 파기

구분	점검항목	유사감사 기준	관련법률
개인정보 보유 및 파기	수집되는 개인정보의 저장 및 보유기간이 관련 법령 및 내부 규정에 따라 적절하게 책정되었는가?	√	√
	개인정보의 파기 절차 수립 시 관련 법령 및 내부규정에 의하여 보유기간 종료 후 당해 개인정보를 파기토록 시스템이 설계되어 있는가?	√	√
	서비스 이용계약 해지 등 개인정보의 수집목적이 달성된 경우 개인정보 처리 시스템을 포함하여 당해 개인정보를 제공받은 제3자에 대해서도 개인정보를 파기토록 하는 등의 조치를 취하고 있는가?	√	√
	개인정보를 담고 있는 저장 매체 폐기시 이를 물리적으로 파기하거나 완전히 삭제 후 복구 불가능 여부에 대하여 점검하고 있는가?	√	√

[표 3.6] 감사항목5 - 접근통제

구분	점검항목	유사감사 기준	관련법률
접근통제 대책	개인정보의 수집, 전송, 저장 및 처리와 접근에 대한 보안 절차와 정보시스템의 네트워크 접근 통제의 방법, 범위 등을 문서화하고 있는가?	√	√
	정보시스템에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하고 있는가?	√	√
사용자 접근관리	인터넷 망과 접속시 침입차단시스템을 통해 접근통제를 수행하고, 침입탐지시스템 등을 활용하여 접근을 모니터링 하고 있는가?	√	√
사용자 접근관리	개인정보를 처리하고 있는 데이터베이스의 접근권한을 서비스 제공에 필요한 최소의 인원으로 제한하고 있는가?		√
	해지고객 DB에 보유하는 개인정보에 대한 접관권한을 최소한의 인원으로 제한하는가?	√	√
	네트워크를 통해 시스템을 관리하는 경우 내부의 특정 터미널에서만 접속할 수 있도록 제한하고, 외부 네트워크를 통하여 시스템 관리시 사용자 인증, 암호 등 접근통제 기능을 설정하고 있는가?	√	
	정보시스템 및 서비스 접속시 사용자 인증 식별을 위한 개별 ID를 사용하고 있는가?	√	√
	사용자 패스워드의 생성규칙을 포함하고 있는 관리절차를 수립하여 이행하고 있는가? (내부 임직원 및 서비스 이용자)	√	√
	정보시스템에 대한 접근을 관리하기 위해서 정기적으로 접근 권한에 대하여 점검을 하고 있는가?	√	√
접근통제 영역	개인정보를 저장하고 있는 시스템은 공개된 시스템과 같은 일반 환경과 분리되어 있는가? (서버 분리)	√	√
	개발, 테스트, 운영, 사용자 환경을 네트워크상 에서 분리하고 있는가?	√	

[표 3.7] 감사항목6 - 운영보안

구분	점검항목	유사감사 기준	관련법률
운영보안	비활성화 된 세션은 정해진 비활성 기간(Period)후에 세션이 단절되는가?	√	
	개인정보처리시스템 및 개인정보취급자 PC에 백신을 설치하여 주기적으로 정상작동여부 확인 및 최신 소프트웨어로 갱신·점검하고 있는가?	√	√
	개인정보취급자 PC에 P2P, 공유 등의 불필요한 프로그램 설치 및 취약한 설정으로 비인가자에게 개인정보가 공개되지 않도록 통제하고 있는가?		√
	개인정보취급자 PC의 화면보호기 설정을 통해 정보처리 화면에 노출되어 있는 정보가 타인에 의해 노출되지 않도록 통제하고 있는가?	√	
	개인정보 유출방지를 위해 검색엔진을 통제하기 위한 파일이 안전하게 구현되어 있는가?		
	매체 취급 부주의로 인한 오·남용으로부터 개인정보를 보호하기 위하여 매체의 취급 및 보관에 대한 절차를 수립하여 운영하고 있는가?	√	
	웹 페이지, 게시판, 첨부파일 등을 통해 개인정보가 노출되어서는 안되며, 노출된 경우 즉시 조치를 취할 수 있는 절차를 마련하고 있는가?		
암호통제	개인정보의 민감도에 따라 암호화 조치 등 적절한 보안 체계를 마련하고 있는가? 또한 본인임을 인증하는 정보(패스워드, 생체정보 등)에 대해서는 복호화되지 않도록 단방향 암호화하여 저장하고 있는가?	√	√
	이용자가 개인정보 공개에 동의하지 않는 개인정보를 정보보호시스템에 의해 보호되는 외부 송신 또는 PC 저장 시 암호화 할 수 있는 방안을 마련하여 이행하고 있는가?	√	√
취약점 관리	사용되고 있는 정보 시스템의 기술적 취약성에 대한 최신 정보의 획득, 취약점 노출 평가 등이 이루어지고 있는가?	√	√
백업	개인정보의 파괴 및 변조에 대비한 백업 시스템을 구축하고, 사고 발생시 적시에 복구 가능하도록 관리하고 있는가?	√	
유지보수	장비 및 보안시스템의 가용성과 무결성을 위하여 장비 제공자가 지시한 명세에 따라 유지보수 등의 계획을 마련하고 이행하고 있는가? 또한 유지보수에 대한 기록을 남기고 있는가?	√	

[표 3.8] 감사항목7 - 물리적 보안

구분	점검항목	유사감사 기준	관련법률
물리적 보안	개인정보를 저장하고 있는 장비를 권한이 없는 자의 물리적 접근 및 각종 물리적 , 환경적 재난으로부터 보호하기 위한 보호구역을 정의하고 이에 따른 보안대책을 수립 · 이행하고 있는가?	√	√
	보호구역은 인가된 사람만이 접근 가능하도록 출입 통제로서 보호되고 있는가?	√	
	개인정보를 저장하고 있는 장비의 이동 또는 제거시 승인을 받은 절차가 존재하는가?	√	

[표 3.9] 감사항목8 - 인적 보안

구분	점검항목	유사감사 기준	관련법률
교육	개인정보보호 인식제고 및 정보시스템 개발 · 운영, 법적 책임, 보안사고 대응절차 등을 포함한 교육 · 훈련 계획을 종합적으로 수립하여 이행하고 있는가?	√	
	교육 및 훈련의 대상에는 임직원 및 관련 외부자를 포함하고 있는가?	√	√
	교육 및 훈련은 정기 또는 수시(정책 또는 역할의 변경이 있는 경우)로 실시하고 이에 대한 기록을 남기고 있는가? 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하고 있는가?	√	√
권한 및 책임	개인정보를 관리하는 시스템의 명칭 및 목적, 이용범위, 운영조직, 시스템 운영자와 책임 소재 및 역할 등이 정의되어 있는가?	√	√
	전보 또는 퇴직 등 인사이동으로 개인정보취급자 변경시 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하고 해당 내역을 기록/관리 할 수 있는 절차를 마련하고 있는가?	√	√
	개인정보처리시스템의 권한 부여, 변경, 말소에 대한 내역을 5년 이상 보관하고 있는가?		√
	개인정보를 담당하는 직원(임시직, 제3자 포함)으로부터 개인정보보호 및 비밀유지 내용을 포함하고 있는 비밀유지 서약서에 서명을 받고 있는가?	√	√

[표 3.10] 감사항목9 - 보안사고 관리

구분	점검항목	유사감사 기준	관련법률
침해사고 대응체계 수립	개인정보 관련 침해사고가 발생하였을 경우 이를 식별하고 대응하기 위한 절차가 마련되어 있는가?	√	√
	보안관련 사고 또는 오류에 의한 개인정보 유출 등이 발생하였을 경우 긴급연락체계 구축, 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 대응 계획을 수립 · 시행하고 있는가?	√	
	보안사고 대응이 신속하게 이루어질 수 있도록 중앙집중적인 대응체계를 구축하고, 대응체계에는 내부직원뿐 아니라 외부기관 및 전문가들과의 협조체계가 반영되어 있는가?	√	
침해사고 대응 및 관리	개인정보 유출 등의 보안사고 발생 시 내부 보고체계에 따라 보고하고, 정보주체에게 관련 사실통지 및 적절하게 민원을 처리할 수 있는 시스템이 마련되어 있는가?	√	
	자사 · 대리점 · 고객센터 또는 협력업체 등이 원격지에서 비정상적으로 과다하게 개인정보를 조회하는 경우 이를 방지하기 위한 경고 시스템 등이 마련되어 있는가?	√	
	개인정보 침해사고 발생 시 이를 즉시 관련 직원에게 알릴 수 있는 예 · 경보시스템이 존재하는가?	√	√
	보안사고 처리 후 결과 분석 및 발견된 정보에 대해서는 관련 조직과 인력에 공유되어야 하며, 유사 사고방지를 위한 재발방지 대책을 수립하고 있는가?	√	
보안정보 제공	사내 임직원 및 서비스 이용자에게 해킹위험 , 계정 및 패스워드 관리, 접속관리 등에 대한 보안정보를 주기적으로 제공하고 있는가?	√	√

[표 3.11] 감사항목10 - 모니터링 및 감사

구분	점검항목	유사감사 기준	관련법률
로그관리	보안사고 처리 및 계약 증빙을 위하여 조직이나 개인에 대한 소송을 지원하기 위한 적정한 증거자료를 확보하고 있는가?	√	√
	로그 관리 시스템과 로그 정보는 무단 변경 및 비인가된 접근으로부터 보호하기 위해 백업 등의 보호대책을 수립하고 있는가?	√	√
	감사 기록의 명확성을 보장하고 법적인 자료나 징계 자료로서의 효력을 갖기 위하여 시스템 시각을 동기화하고 있는가?	√	
모니터링	직원이 보안 관련 사항을 위반할 경우 보안 위반사항에 대하여 자동적으로 기록되고 관리책임자에게 통보되는 절차가 고려되어 있는가?	√	√
	시스템 운영상의 시정 또는 개선을 요하는 사항이 발견될 경우 이를 시정 또는 개선하기 위한 절차가 마련되어 있는가?	√	√
	개인정보 접근에 대한 모니터링을 통해 정책과의 일치성을 주기적으로 검토하고, 접근통제 정책의 적정성을 확인하고 있는가?	√	
	개인정보 DB 접근·처리에 대한 로그기록의 감사 및 점검을 실시하는가? 실시한다면 그 주기는 어떠한가?	√	√
보안감사	개인정보보호 관련 정책의 준수여부를 확인하기 위한 보안감사 계획을 수립하여 시행하고 있는가?	√	√
	정보시스템의 사용을 감시하기 위한 절차 수립 및 로그기록의 결과를 정기적으로 검토하고 있는가?	√	√

[표 3.12] 감사항목11 - 웹 어플리케이션 보안

구분	점검항목	OWASP Top 10	관련법률
인증	개인정보 변경 페이지 등과 같은 중요한 페이지에 접근할 경우 반드시 접근권한을 재점검 하도록 하는 루틴을 적용하고 있는가?	√	
	일정 횟수 이상 실패한 인증을 감지하는 기능 및 계정 잠금 기능이 구현되어 있는가?		
	패스워드 분실 조치의 구현은 이루어져 있는가?	√	
사용자 세션 관리	쿠키는 사용자가 알아볼 수 없도록 암호화되고 있는가?	√	√
	쿠키 및 세션 내용에는 권한상승과 관련된 값과 개인정보를 포함한 값을 이용하고 있는가?	√	
	쿠키 및 세션 만료 시간은 설정되어 있는가?	√	
	쿠키 및 세션 정보는 외부의 인가되지 않은 접근에 안전하게 구현되어 있는가?	√	√
	사용자 세션 인증은 쿠키 보다는 정보가 서버 쪽에 저장되는 세션통신을 이용하거나, 쿠키와 세션, IP Address 등 2개 이상의 값을 함께 검사하도록 설계되었는가?	√	
암호화	로그인 과정을 포함한 개인정보가 포함되는 모든 세션을 SSL(Secure Socket Layer)로 암호화 하는가?	√	√
로그	웹 어플리케이션에서 발생할 수 있는 모든 경우의 에러에 대해 대응할 수 있도록 조치되어 있는가? (에러에 의한 중요정보 노출 방지)	√	

4. 보안감사 점검항목의 검증 및 모의 보안감사

본 논문에서 도출된 보안감사 점검항목을 이용하여 국내에서 전자상거래 사이트를 운영하고 있는 A사를 대상으로 보안감사를 수행함으로써 점검항목에 대한 실증분석을 통해 타당성 및 실효성을 검증하고자 한다.

실증분석에 있어 전자상거래 업체를 선정한 이유는 정보시스템을 통하여 재화에 관한 정보를 제공하고 이용자의 청약에 의하여 재화를 판매하는 것을 업으로 하고 있는 통신판매의 특성에 따라 이용계약의 이행 또는 서비스 제공에 따른 요금정산을 위하여 사용자의 실명을 필요로 하고 있다.

사용자의 실명 확인은 회원가입 또는 개인정보를 통

해 이루어지고 있으며, 이렇게 수집되는 개인정보는 정보시스템 내에서 일정기간 동안 저장되어 관리되고, 이용이 완료된 시점에 적절한 방법을 통해 파기 되는 등 서비스 제공에 있어 개인정보의 수집에서 파기까지 개인정보 생명주기를 모두 포함하고 있다. 서비스 제공 및 개인정보의 수집, 활용 등의 단계가 웹 어플리케이션을 통해 이루어지고 있는 만큼 본 논문에서 조사된 모든 범위의 침해유형이 나타날 수 있는 형태를 가지고 있다고 판단되어 실증분석을 위한 대상으로 선정하였다.

4.1 보안감사 적용범위 및 방법

A사의 개인정보 수집 및 이용은 전자상거래를 통해 제품을 판매하기 위한 목적을 가지고 있으며, 개인정보의 생명주기에 따른 모든 업무처리가 정보시스템을 통해 이루어지고 있는 만큼 본 논문에서 도출된 개인정보의 모든 통제 분야를 적용하여 실시하였다.

A사를 대상으로 하는 보안감사는 논문에서 도출된 점검항목의 실증점검에 목적을 가지고 다음과 같은 방법을 통해 모의 보안감사를 수행하였다.

1) 개인정보보호 현황 분석을 통해 각 통제 분야에서 점검항목 선정
2) 개인정보보호 관련 정책 및 지침을 기반으로 서면검사 실시
3) 담당자와의 전화인터뷰 및 웹 어플리케이션 분석
4) 도출된 문제점에 대한 개선방안 마련

4.2 보안감사 수행 결과

본 논문에서 도출된 점검항목과 모의 보안감사 수행 시 적용된 항목, 점검결과에 따른 미이행 항목에 대한 현황은 다음과 같다.

보안감사 수행결과 '개인정보보호 관리체계의 검토', '외부인의 개인정보 처리'분야가 가장 취약한 것으로 나타났으며, 이에 대한 원인으로는 개인정보보호 정책 및 개인정보보호 조직이 수립되지 않은 것으로 나타났다. 또한 '개인정보 보유 및 파기'분야의 경우 탈퇴한 회원의 정보가 자동 소멸되지 않고 DB에 그대로 남아 있으며, 개인정보를 담고 있는 저장매체의 폐기 절차 및 폐기된 매체에 대한 데이터 복구 방지 검증 절차가 마련되어 있지 않는 등 개인정보 처리에 있어 다수의 위험이 존재하는 것으로 확인되었다. '개인정보의 수집 · 이용 · 제공'분야의 경우는 적용 항목 및 미이행 항목이 1개인 관계로 결과가 0%로 나타났다.

하지만 정보보호 관리체계 수립 및 이행을 통해 정보보호에 대한 기반이 마련되어 있어 접근통제, 물리적 보안, 보안사고 관리, 모니터링 및 감사 부분은 매우 양호한 것으로 나타났다.

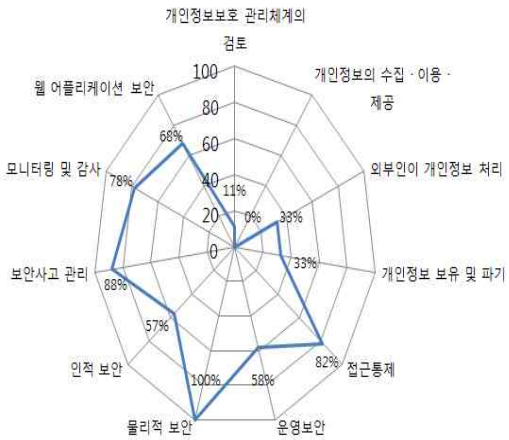
각 통제 분야별로 A사의 개인정보보호 현황을 도표화한 결과는 다음 그림과 같다.

4.3 보안감사 점검항목 검증 결과

실증점검을 위해 A사를 대상으로 보안감사를 수행한 결과 본 논문에서 도출된 점검항목 대비 감사에 적용된 점검항목에 대한 비율은 [그림 4.2]과 같다. 통제 분야 중 '개인정보의 수집 · 이용 · 제공'분야의 적용 비율이 낮은 원인으로는 2개의 점검항목 중 1개의 항목만이 적용되어 발생한 것이며, '외부인의 개인정보 처리' 분야의 경우는 A사의 서비스 특성상 개인정보를 위탁하거나 협력업체에 제공되지 않아 점검항목에서 제외된 항목이 다수 존재하는 것으로 확인되었다.

본 논문에서 도출된 총 보안감리 점검항목 대비 A사에 적응된 점검항목은 약 95%에 달하며, 앞서 제외된 상황을 고려해 볼 때 대부분의 점검항목이 보안감리를 수행하는데 적용이 가능하다는 결론을 얻을 수 있었다.

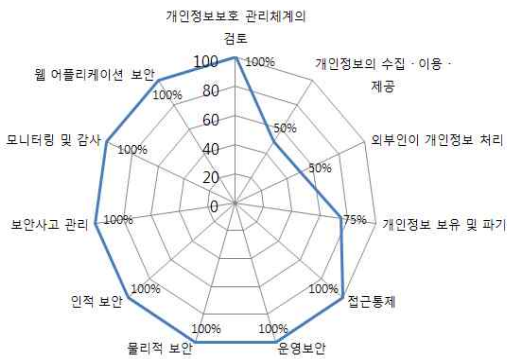
[그림4.3]은 적용된 보안감리 적용항목 대비 도출된 위험 비율을 나타낸 것으로 A사의 경우 정보보호 관리체계가 수립되어 이행되고 있음에도 불구하고 다수의 개인정보보호 관련 위험이 존재하고 있음을 나타내고 있다. 이러한 점을 통해 본 논문에서 도출된 점검항목을 실제 감사 프로젝트 등에 적용하더라도 정보시스템에서 개인정보 유출을 방지하기 위한 점검항목으로 이용가능하다는 점을 보여주고 있다.



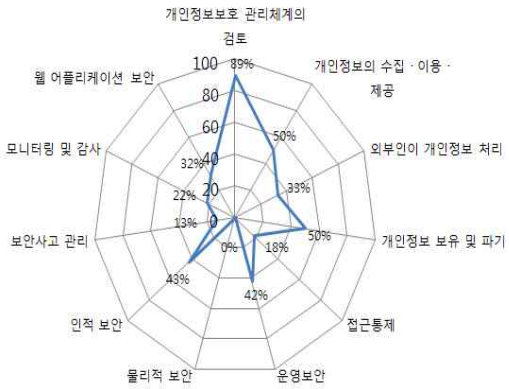
[그림 4.1] 통제 분야별 개인정보보호 현황

[표 4.1] A사 실증 적용 점검항목 현황

통제분야	구분	점검 항목	적용 항목	미이행
개인정보보호 관리체계의 검토	개인정보보호 정책	6	6	6
	개인정보 관리조직	3	3	2
개인정보의 수집・이용・제공	개인정보의 이용・제공	2	1	1
외부인의 개인정보 처리	외부인의 개인정보 처리	6	3	2
개인정보 보유 및 파기	개인정보 보유 및 파기	4	3	2
접근통제	접근통제 정책	2	2	0
	사용자 접근관리	7	7	2
	접근통제 영역	2	2	0
운영보안	운영보안	7	7	3
	암호통제	2	2	2
	취약점관리	1	1	0
	백업	1	1	0
	유지보수	1	1	0
물리적 보안	물리적 보안	3	3	0
인적 보안	교육	3	3	1
	권한 및 책임	4	4	2
보안사고 관리	침해사고 대응체계 수립	3	3	0
	침해사고 대응 및 관리	4	4	1
	보안정보 제공	1	1	0
모니터링 및 감사	로그관리	3	3	0
	모니터링	4	4	2
	보안감사	2	2	0
웹 어플리케이션 보안	인증	3	3	1
	사용자 세션관리	5	5	1
	암호화	1	1	1
	로그	1	1	0
	웹 공통	12	12	4
	권한관리	2	2	1
	관리자 페이지 접근통제	1	1	0
합계		96	91	34



[그림 4.2] 도출된 점검항목 통제 분야별 적용률



[그림 4.3] 적용항목 대비 도출된 위험 도출 비율

5. 결 론

정보화시대의 도래와 더불어 인터넷과 정보통신 인프라의 발전으로 각종 유용한 정보들을 대량으로 처리할 수 있게 되었으며, 이러한 환경은 우리의 일상생활에 많은 편리함을 제공해 주고 있다. 그러나 이를 악용한 정보화 역기능 현상이 주변 곳곳에서 나타나고 있다. 특히 정보화 사회에서 경제주체의 활동이 개인정보를 매개로 하여 유지・운영되고 있는 관계로 개인정보가 상업적 가치를 지니게 되어 개인정보의 유출 및 오・남용 등의 보안사고가 끊이지 않고 있다.

이와 더불어 정보의 가치가 산업사회에서의 물질이나 에너지 못지않게 중요해지고 있으나, 정보보호를 위한 사회적 공감대 형성은 개인정보를 위협하는 위험요소의 발전 속도에 미치지 못하고 있는 현실이다. 위협에 대한 대응체계도 제한적으로 이루어지고 있는 실정에서 정보보호를 위한 보안감사 기법 또는 조직의 계획도 체계적으로 이루어지지 못하고 있다.

이러한 문제들을 해결하기 위한 방안으로 본 논문에서는 국・내외 정보보호 관리체계 및 인증기법을 분석하고 국내뿐만 아니라 전세계적으로 문제시되고 있는 개인정보 유출 방지를 위한 새로운 보안감사 점검항목을 도출하였다. 각 점검항목은 개인정보 생명주기 및 점검범위에 따라 개인정보보호 관리체계, 기술적・관리적・물리적・인적・웹 어플리케이션 보안등을 포함한 11개 통제분야로 분리하여 개인정보가 유출될 수 있는 위험을 도출하여 이를 해결할 수 있는 방안을 마련하는데 활용될 수 있도록 하였다. 또한 도출된 보안감사 점검항목의 실효성과 타당성을 검증하기 위하여 개인정보 유출사례 및 모의 보안감사를 수행하였다.

이처럼 개인정보와 관련된 유출사례, 감사 기준 등을 종합적으로 수집・분석하여 정보시스템 운영시의 개인

정보 보호를 위한 보안감사 방법론을 제시하기 위한 목적으로 본 논문을 진행하였다.

하지만 본 연구에서는 개인정보보호의 측면에서만 보안감사 기준을 제시하였으므로 정보시스템 운영시 IT인프라 및 네트워크, SW, HW 등의 부분에 대한 감사 기준은 반영되지 못하였다. 또한 앞으로 다가올 유비쿼터스 시대의 무선통신 기술 등 새로운 기술에 대해서 고려하지 않았다. 향후 연구에서는 위와 같은 새로운 기술 및 정보시스템 운영상의 다양한 부분까지 고려하여 연구를 수행하여야 할 것이다.

6. 참 고 문 헌

[1] 권호열(2004), 「SSE-CCM과 ISO/IEC 12207의 IT 보안감리 프로세스 비교」.

[2] 김종기 (2008), 「BS7799 정보기술 보안관리 지침 표준화동향」, 부산대학교 경영학부.

[3] 라이지움 연구출판부, 「CISA Area.1 Ver.012 IS 감사 프로세스」, Lyzeum, p21.

[4] 박태완, 「ISO 27001 인증의 동향과 중요성」, 한국인정원 인증포커스 제6권, 10-15.

[5] 유재성(2009), 「정보시스템 분석 및 설계단계에서의 개인정보보호 감리 방법에 관한 연구」, 건국대학교 정보통신대학원 석사학위 논문.

[6] 유진석 외 4명(2005), 「유비쿼터스 시대의 국가간 개인정보 유통정책의 해외사례 연구 및 우리나라의 대응방안」, 서강대학교 정보통신 학술연구과제.

[7] 이문구(2004), 「정보시스템 보안관리를 위한 위험분석 방법론」, 전자공학회 논문지 제41권 제6호 통권 300호, 13-22.

[8] 이지용(2009), 「정보보호아키텍처에 근거한 정보보호감리모형에 관한 연구」, 건국대학교 정보통신대학원 석사학위 논문.

[9] 이창범(2003), 「현행 프라이버시 보호 담당기구의 성과와 한계」.

[10] 전인석(2009), 「정보보호 관리체계를 이용한 개인정보보호 수준 측정모델」, 건국대학교 정보통신대학원 석사학위 논문.

[11] 전자신문(2009), 『LG텔레콤 고객 개인정보 무방비 노출』.

[12] 조태희 (2004), 「정보보호관리 표준 및 인증제도」, 한국정보보호 진흥원 취약성분석팀.

[13] 한국인터넷 진흥원,「연도별 인터넷 이용자 수 통계현황」.

[14] 한국정보보호 진흥원(2006), 「개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구」.

[15] 한국정보보호 진흥원(2005), 「기업의 개인정보영향평가 수행을 위한 가이드」.

[16] 한국정보보호 진흥원(2005), 「정보보호 관리체계 홍보브로셔(정보보호 관리체계 인증)」.

[17] 한국정보보호 진흥원, 「ISMS 인증심사 기준」, http://www.kisa.or.kr/kisa/isms/jsp/isms_0010.jsp.

[18] 황경태(2005), 「정보시스템 통제 감사」, 삼영사.

[19] 황경태 외(2004), 「정보보호 관리체계 인증준비 가이드」, 한국정보보호 진흥원.

[20] John Pescatore(2005), 「해킹기법의 변화」「웹 어플리케이션 보안」, Gartner Group.

[21] STG Security(2002), 「BS7799 소개」.

저 자 소 개

이 동 녘

명지대학교에서 학사, 석사학위를 취득하였고, 관심분야는 정보시스템 감사, MIS 등이다.

주소: 경기도 용인시 기흥구 언남동 동일하일빌 120-201

박 정 선

서울대학교에서 학사, 한국과학기술원에서 석사학위를 취득하였고, 미국 텍사스주립대학교 경영학박사를 취득하였으며, 한국전산원에서 선임연구원을 거쳐 현재는 명지대학교 산업경영공학과 교수로 재직 중이다.

주소: 경기도 용인시 처인구 남동 명지대학교 공학관 507호