Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.1, Feb. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.1.109

공공부문 보안취약점 감사 효율화 방안에 관한 연구

김 현 석†‡
감사원 (사무관)

A Study on the Efficiency of Auditing for Security Vulnerabilities in the Public Sector

Hyun-seok Kim†‡
The Board of Audit and Inspection of Korea (Deputy Director)

요 약

정보보안 활동의 목적은 해킹 등으로 인한 피해가 발생한 이후 그 원인을 찾아 후속 조치하는 것 뿐만 아니라 주기적인 보안 활동을 통해 제어시스템 등 중요 시스템의 해킹 피해 시 우려되는 대규모 물적·인적사고를 줄이는 데에 있다. 이에 각 기관에서는 관련 규정에 따른 보안감사모델을 활용하고 있지만 시간과 인력의 제약으로 인해 전사적 점검활동을 수행하는 것이 쉽지 않다. 본 논문에서는 최근 10년간 공공기관의 주요 취약점에 대해 분석해보고 국내외 보안감사를 위한 모델과 비교하여 효율적인 보안활동을 수행할 수 있는 보안감사모델을 제시하고자 한다.

ABSTRACT

The purpose of information security activities is to reduce large-scale material and human accidents that are concerned about hacking damage to important systems, such as control systems, through periodic preventive activities in addition to finding the cause and taking follow-up measures after damage caused by hacking. For this reason, although each institution is using a security work audit model in accordance with the relevant regulations, it is not easy to conduct company-wide inspection activities due to the constraints of manpower and time. Therefore, in this paper, we will analyze the major vulnerabilities of public institutions over the past 10 years and present a security audit model that can perform efficient security activities compared to the models for domestic and foreign security audits.

Keywords: Security Audit, Audit Model, Vulnerability Analysis

I. 서 론

정보통신기술의 발달로 사이버공간과 일상생활이 병존하는 시대가 도래하면서 사이버공격의 형태가 단순 정보탈취를 위한 해킹 수준을 넘어서 테러·전쟁의 양상으로 변화되는 등 국가·사회의 안전을 위협하기에 이르렀다. 또한 해킹에 의한 개인정보 유출사고('15. 3월 행안부 아이핀 75만 건 부정발급, '20. 6월 우리카드 12억 건)로 인해 국민과 기업의 사회·경제적 피해도 심각한 수준에 이르고 있다.

2020년 11월 국회 정보위 국정감사결과에 따르면 공공기관에 대한 사이버 공격 건수가 하루평균 162만 건으로 2016년 41만 건에 비해 약 4배가 급증한 것으로 나타나는 등 앞으로 지능화·대형화되고 있는 사이버 공격이 지속될 것으로 예상되어 각 기관은 내·외부 감사수단을 활용하여 정보시스템과 개인정보의 안전성 여부를 주기적으로 점검할 필요가 있다.

한편, 보안감사를 준비하거나 대비하기 위한 업무가 일상업무에 있어서 중요도가 높고 많은 비중을 차지하지만, 감사를 하는 입장에서 제한된 시간 내에

Received(11. 11. 2021), Modified(12. 14. 2021), Accepted(12. 14. 2021)
† 주저자, hyunseokkim@korea.kr
‡ 교신저자, hyunseokkim@korea.kr(Corresponding author)

별도 우선순위없이 모든 세부 사항의 준수여부를 확인하는 것은 제한될 뿐만 아니라 투입시간 대비 비효율적이다. 또한 감사자의 개인 역량에 따라 감사결과가 달라질 수 있고 감사중점 선정 시 필수적으로 점검해야할 사항이 매번 달라지게 되면 일관성있는 감사결과를 기대하기 어렵다. 이에 취약부문부터 우선적으로 점검하는 등 점검모델에 기반한 보안감사가 필요하다.

본 논문에서는 감사원에서 최근 10년 간('11년~'20년) 공공기관들을 대상으로 보안감사를 실시하여 처분요구한 268건의 감사결과들을 분석하고 이를 바탕으로 취약점들을 유형화하여 필수점검항목 선정을 위한 감사모델을 제시하고자 한다. II장에서는 제안모델과의 비교를 위해 6가지 국내·외 정보보안 기준 및 감사모델을 살펴보고 III장에서는 268건의 감사결과들을 유형별로 분류하며 IV장에서는 유형별 취약점들을 분석하여 모델로 제안, 기존 감사모델과 비교 분석한다. 이를 통해 공공분야 보안취약점에 대비하기 위한 발전방향을 제시하고 마지막 V장은 결론으로 마무리한다.

II. 국내외 정보보안 표준 감사모델

보안감사와 관련하여 국외 감사원 중 미연방 감사원은 IT분야 국제표준인 ISO27001[3]을 반영하여 2009년부터 선진국형 감사모델인 FISCAM[1]을 구현하였고, 세계감사원장 회의에서는 2014년에 정보보안 분야를 포함한 IT감사핸드북[2]을 개발하여 전 세계 감사원에 배포하기도 하였다. 국내에서는 공공부문의 경우, 보안감사 주무기관인 국정원에서 주요정보통신기반시설 보호대책 이행여부 확인해설서[6]를 바탕으로 점검을 하고 있고, 민간부문의 경우, ISMS-P[4]를 기반으로 보안수준에 대한 인증을 받도록 하고 있으며 금융부문의 경우, 금융감독원에 의해 IT감사 매뉴얼[5]을 활용하여 감사 시 활용하고 있다. 이에 본 논문에서는 대표적인 국외 감사모델, 국제표준, 국내 부문별 점검모델들을 분석하고 감사원에서 그간 중앙행정기관, 지방자치단체, 공공기관, 금융회사들을 대상으로 감사한 결과를 분석하는데 활용하고자 한다.

2.1 미연방감사원(GAO)의 FISCAM 모델

미연방감사원(GAO)은 2009년 연방정보시스템 감사모델로 FISCAM(Federal Information System Controls Audit Manuals)[1]을 채택하였다. 이 모델은 Table 1과 같이 일반 통제는 5개 분야 25개 점검항목으로, 응용프로그램 통제는 4개 분야 12개 점검항목으로 구성되어 있다.

Table 1. GAO's FISCAM model

General control(5 areas, 25 check items)
① Security Management ② Access Control ③ Configuration Control ④ Segregation of Duties ⑤ Contingency Planning
Application control(4 areas, 12 check items)
① Application level General control ② Business Process Control ③ Interface Control) ④ Data Management System Control

여기서 일반 통제란 정보시스템 보안정책 개발, 직무분리가 명확한 정보시스템 관리 인원 조직화, 재난복구 계획 수립 등을 말하고, 응용통제란 각 응용프로그램에서 이루어지는 데이터 입력, 교환, 처리, 암호화 등을 말한다.

2.2 INTOSAI IT Audit Handbook

INTOSAI(세계감사원장회의)의 IT감사워킹그룹(WGITA)과 INTOSAI개발기구(IDI)는 2014년 2월 감사관들에게 IT감사에 관한 표준과 보편적으로 인정된 모범 사례를 제공하고자 IT감사 핸드북을 발간하였다. 이 핸드북은 IT감사를 수행하면서 감사관들이 살펴보아야 할 중요한 분야에 대하여 포괄적으로 설명하면서 ISSAI(International Standards for Supreme Audit Institutions, 감사원 국제기준)이 제시하는 일반적인 감사원칙들에 대해 기술되어 있다.

그 중 정보보안과 관련한 부분은 Table 2와 같이 별도로 감사매트릭스[2]를 마련하였고 해당 리스트들은 "평가방법(Assessment Methods)" 등 7가지 분야로 나누어 감사목표와 감사이슈(점검항목)를 제시하고 있다.

Table 2. Information Security Audit Matrix

A. Risk assessment	
1	Audit Issue 1: Assessment Methods
2	Audit Issue 2: Assessment Scope
3	Audit Issue 3: Mitigation
B. Information security policy	
4	Audit Issue 4: Information Security Policy
C. IT security organization	
5	Audit Issue 5: Confidentiality
6	Audit Issue 6: Organizational Structure
7	Audit Issue 7: Reconciliation
D. Communication and operation management	
8	Audit Issue 8: Policies and Procedures
9	Audit Issue 9: Network Control
E. Asset management	
10	Audit Issue 10: Configuration Management
11	Audit Issue 11: Asset Management
F. Human resources security	
12	Audit Issue 12: Employee Awareness and Responsibilities
13	Audit Issue 13: Training
G. Physical security	
14	Audit Issue 14: Organizational Safety in the Territory
15	Audit Issue 15: Physical Access
16	Audit Issue 16: Intrusion Prevention

2.3 국제 표준 모델 ISO27001

국제표준기구(ISO/IEC)에서는 정보보호 관리에 관한 표준안 및 인증체계로 ISO27001[3]을 개발하여 국제표준으로 확정하였다. 이 모델은 Table 3과 같이 11개 분야 133개 점검항목으로 구성되어 있고, 이후 한국인터넷진흥원이 국내 정보보호 표준을 정립하기 위해 정보보호 관리체계(ISMS: Information Security Management System)를 개발하는 근간이 되었다.

Table 3. ISO27001's control model

① Security Policy
② Organization of Information Security
③ Asset Management
④ Human Resources Security
⑤ Physical and Environmental Security
⑥ Communication and Operations Management
⑦ Access Control
⑧ IS Acquisition, Development and Maintenance
⑨ Information Security Incident Management
⑩ Business Continuity Management
⑪ Compliance

2.4 정보보호 및 개인정보보호 관리체계(ISMS-P)

과학기술정보통신부는 정보시스템의 보안표준 모델로 「정보통신망법」 제47조에 따른 정보보호 관리체계 인증(ISMS)을 고시하였고, 개인정보보호위원회는 개인정보 보호표준 모델로 「개인정보 보호법」 제32조의 2에 따른 개인정보 보호관리체계 인증(PIMS)을 각각 고시하였다. 두 인증 모델은 현재 정보보호 및 개인정보보호 관리체계(ISMS-P)[4]로 통합되어 기관과 기업이 정보보호 및 개인정보에 관한 국내 표준 인증을 받기 위해 활용되고 있다.

인증심사항목에 해당하는 정보보호 및 개인정보 관리체계 요구사항[4]은 Table 4와 같이 관리체계 기반 마련(Management System Establishment and Operation) 등 16개의 관리체계 수립 및 운영에 대한 항목과 인증 및 권한 관리 등 64개의 보호대책에 대한 항목, 그리고 개인정보와 관련하여 수집부터 파기에 해당하는 22개 항목으로 구성되어 있다.

Table 4. Information Protection and Personal Information Management System Certification Criteria

Item	Criteria	
1. Management system Establishment and operation (16)	1.1 Establishment of management system foundation(6) 1.3 Management system operation(3)	1.2 Risk management(4) 1.4 Management system inspection and improvement (3)
2. Protection measures Requirements (64)	2.1 Policy, Organization, Asset Management(3) 2.3 Outsider Security(4) 2.5 Authentication and Authority Management(6) 2.7 Encryption Application(2) 2.9 System and Service Operation Management(7)	2.2 Human Security(6) 2.4 Physical Security(7) 2.6 Access Control (7) 2.8 Information system introduction and development security (6) 2.10 System and Service Security

	2.11 Accident Prevention and Response(5)	Management(9) 2.12 Disaster Recovery(2)
3. Requirements for each stage of personal information processing (22)	3.1 Protective measures when collecting personal information(7) 3.3 Protective measures when providing personal information(3) 3.5 Protection of data subject rights(3)	3.2 Protection measures for retention and use of personal information (5) 3.4 Protection measures when personal information is destroyed (4)

2.5 금융감독원 IT감사(보안분야) 매뉴얼

금융감독원은 「전자금융거래법」 및 「전자금융감독규정」에 따라 종합검사 또는 IT부문검사 시 매뉴얼에 따라 Table 5와 같이 IT보안절차, IT보안리스크평가, IT보안 및 정보보호 전략, IT보안통제 구현, IT보안 모니터링 등 5개 평가항목 17개 세부평가항목[5]으로 구분하여 평가하고 세부평가항목에 대한 점검방식은 착안사항을 포함하여 점검해야할 항목을 기술하고 있다.

Table 5. Audit manual detailed evaluationl items

Evaluation items	Detailed evaluation items
1. IT security procedures	Securing IT security system
	The role of management in the security system
	Monitoring and supplementing security procedures, etc.
2. IT security risk assessment	Clarification of information and information systems
	information collection and analysis; Risk assessment, management plan
3. IT security and information protection strategy	Information Security Policy and Regulations
	Technical design
	Outsourcing service security service management, etc.
4. Implementation of IT security control	Administrative information security operation status
	Technical information security operation status
	physical and environmental controls
	Prevention of hacking and malware infection
	human security
	data security, etc.
	Automated device security
5. IT security monitoring	Network configuration for efficient monitoring
	Monitoring result analysis and response, etc.

2.6 주요정보통신기반시설 보호대책 확인 모델

기반시설 관리기관은 「정보통신기반보호법」에 따라 매년 취약점 분석평가를 실시한 후 보호대책을 수립하여 이를 시행하고 국정원과 과학기술정보통신부는 관리기관이 자체 수립한 보호대책을 이행하였는지 여부를 점검하기 위해 "주요정보통신기반시설 보호대책 이행여부 확인해설서"[6]를 활용하여 제어시스템과 정보시스템을 점검하는데 Table 6과 같이 9개 분야 세부 68개 항목으로 구분하여 평가하고 있다.

Table 6. Checkpoints for the implemetation of major infrastructure

Evaluation items	
Basic Activities (Common, 7)	
Network configuration and access control(13)	Portable device security management(7)
Asset Management(4)	Threat Detection Removal(7)
System Security Management(12)	Incident response(5)
Updates and data transmission(7)	Service company security management(6)

2.7 기존 감사모델에 대한 분석

앞서 살펴본 6가지 감사모델에 대해 평가항목 기

준으로 분석한 결과 감사모델들 중 [1-4]의 경우, 정형화된 점검모델의 성격을 띄고 있고 [5]의 경우, 평가항목과 세부평가항목으로 구분한 뒤 세부평가항목에서 '필수', '선택'으로 구분하고 있으나 17개 세부평가항목 전체가 '필수'로 지정되어 있어 중요도 구분이 되어 있지 않다. [6]의 경우, 평가항목 중 세부항목에 대해 '상', '중', '하'로 구분하고 있으나, 세부항목 중 "취약점 분석평가결과 문제점 보완조치"의 경우 '상'으로 구분한 반면 "보호대책 이행여부 확인결과 문제점 보완조치"는 '중'으로 구분하고 있고 "용역업체 보안관리" 평가항목 내 "용역업체 외부 원격작업 금지"는 '하'로 구분되어 있는데 "용역업체 전산망 분리 운영 및 접근통제"는 '상'으로 되어 있는 등 유사성격업무들에 대해 중요도 등급 부여 기준이 모호하다. 이와 같이 기존 감사모델들은 각 개별 모델 내에서 평가항목의 중요도에 따른 구분이나 유사 평가항목 내 필수 점검여부를 확인하기 어려운 점이 있었다. 이에 본 논문에서는 기 확인된 감사결과들을 분석한 뒤 각각의 중요 점검항목을 도출하고자 한다.

III. 감사결과 및 주요 취약점 유형분석

3.1 감사결과 분석

공공기관은 정보보안 활동을 하기 위해 정보시스템 보안관리 및 개인정보 보호를 위한 물리적·관리적·기술적 보안활동 등을 분석하고, 각 기관의 주요정보 및 개인정보 시스템, 웹서버 등 업무시스템, 주요정보통신기반시설의 제어시스템, 용역업체 보안관리업무 등 정보시스템과 업무별 취약점을 분석한다.

이와 관련하여 감사원은 최근 10년간('11년~'20년) 공공 및 금융권 등을 대상으로 공공부문에서의 해킹 사고 등에 대비한 관리·감독 실태를 확인하기 위해 "금융소비자 보호 등 금융감독실태" 등 36차례[7-42]에 걸쳐 공공기관의 보안활동 실태를 감사하였다.

분석대상 36개 감사사항의 감사결과 268건 중 4개 감사사항의 감사결과 173건[1](65%)이 정보보안 전반에 대한 특정감사로 실시되었고 해당 특정감사들의 점검중점은 "주요정보시스템 점검", "개인정보 보호 및 관리", "추진체계 등 제도운영", "정보보호 인프라 구축" 등으로 구분되어 있으며 주요 감사대상 유형은 Table 7과 같다.

Table 7. Subjects to audit by type

type	audit subject
Information system management	critical control system, management information system(ERP etc.), web server, resource management system, personal information system, security related systems, etc.
Personal information protection and management	account management(update, delete, etc.), information management policy (information processing, registration), etc.
Infomation security infrastructure	disaster recovery measures, portable storage, security control system, etc.
Implementation systems and system operation	security management contingency plan, security system design, external service security, etc

특정감사들의 점검중점을 기준으로, 본 논문에서는 전체 감사결과를 "① 정보시스템의 안전조치 부적정, ② 개인정보 보호 및 관리 부적정, ③ 정보보호 인프라 구축 미흡, ④ 추진체계 및 제도운영 부적정"으로 분류한다. 그리고 분류 시, 각 유형별 감사결과 통계는 개별 감사결과 내에 중복(예. 하나의 감사결과 내에 정보시스템의 안전조치 사항, 인프라구축 사항 미흡, 제도개선 사항을 동시에 지적한 경우)사례가 많아 별도 산정하지 않는다.

감사결과 Table 8과 같이 36개 감사사항에서 268건[7-42]의 위반사항이 있었다. 그리고 17개 감사사항(table에서 음영 표기)에서 정보보안 부문만 특정(나머지 19개 감사사항에서는 기관정기감사 등의 형태로 감사중점에 일부포함하여 정보보안 위반사항을 지적)하여 감사를 실시하였다[43].

구체적인 세부 감사결과는 「전자정부법」, 「정보통신기반보호법」, 「정보통신망법」, 「개인정보 보호법」 등의 법령과 '국가정보보안 기본지침', '국가사이버안전관리규정' 등 제도적으로 규정된 정보보안 활동 및 점검활동 영역에 근거하여 공통적으로 확인된 보안 취약점들을 중점으로 분석하였다.

1) "공공기관 정보보호 및 사이버안전관리실태"(94건), "금융권 정보보호 및 사이버안전 관리감독실태"(18건), "국가사이버안전 관리실태"(24건), "주요정보통신기반시설 사이버침해 대응역량 점검(37건)"

Table 8. Information security related audits[7-42]

Year	Audit item name	case
'11	Status of social service e-voucher business selection(C)	2
'12	Financial supervisory status including protection of financial consumers(P)	2
	State of national core infrastructure crisis management(S)	10
'13	Status of information security and cyber safety management of public institutions(S)	94
	Financial consumer protection and Supervision(S)	1
'14	Audit the operation of diplomatic missions abroad and the implementation of major projects by the Ministry of Foreign Affairs(S)	8
	Financial sector information security and cyber safety management and supervision(S)	18
	Financial execution management status(S)	2
	Institutional operation audit by the Ministry of Safety and Public Administration(I)	1
	Inspection and supervision related to personal information leakage of financial companies(S)	10
	Status of civil complaint handling in the first half(S)	1
'15	Police Agency Institutional Operation audit(I)	2
	Electricity support public institutions management status(S)	2
	Establishment and operation of the national integrated traffic information system(S)	13
	Local office of education financial management(5)(S)	1
'16	State of national cyber safety management(S)	24
	Current status of contract work for major information projects(S)	1
	Management status of response to threats to national safety(airport safety, firearms, and explosives)(S)	3
	Inspection of cyber-infringement response capabilities of major information and communication infrastructure(S)	37
'17	National tax information system utilization and security status(S)	2
	Construction and utilization of national geospatial data(S)	3
	Education information system establishment and operation status(S)	3
	Seoul National University Hospital electronic medical records unauthorized reading and leakage(S)	2
	Construction and utilization of information systems in the land and environment fields(S)	7
	State public official personnel pperation and management(S)	1
'18	Construction and utilization of public data(S)	1
	Management of public teacher appointment examination(S)	1
	Postal business management status(S)	4
	Inspection of allegations related to contract by the korea employment information service(S)	2
'19	Management status of agricultural product price stabilization subsidy support project(S)	1
	Operational inspection of local indigenous corruption, etc.Ⅲ(S)	2
	Korea foundation, overseas koreans foundation institutional operation audit(I)	1
'20	Operational status of diplomatic missions abroad and the headquarters of the Ministry of Foreign Affairs(S)	2
	Status of settlement support for north korean refugees(S)	1
	Pharmaceutical safety management status(P)	2
	Chungcheongnam-do institutional audit(I)	1
S: Specific audit(29), P: Performance audit(2), I: Institutional audit(4), C: Claim audit (1), Total: 36		268

본 논문에서는 관련 법령이 다수이고 정보통신기술 분야의 특성상 범위가 넓어 정보시스템과 관련된 기술 및 관리적 영역을 중점적으로 분석하면서, 최근 정보시스템에 대한 해킹 목적으로 개인정보를 탈취하는 등의 사례가 많이 발생하고 있어 정보시스템 안전조치와 관련된 정보보안(개인정보 감사결과사항 포함)에 국한하여 분석하였다.

3.2 주요 취약점 유형분석

본 논문에서 분석한 취약점들의 유형을 살펴보면, 서버와 같은 주요 정보시스템을 운용하는 관리자들이 계정관리를 부실하게 하여 외부로부터의 취약성을 방어하지 못하는 등 정보시스템의 안전조치를 미흡하게 한 사례, 내부 직원들 중 고객정보관리시스템과 같은 주요 응용시스템에 접근권한을 가진 일반 직원들이 사적 목적으로 시스템을 운용하는 등 개인정보 보호 및 관리를 소홀하게 한 사례, 위 두 가지 사례와 같은 기술적 취약점에 해당되지는 않지만 재해상황과 같이 사전에 대비할 수 있도록 정보보안 기반을 갖추지 못해 발생하는 인프라 구축 미흡 사례, 그리고 감사대상기관에서 기술적·관리적 취약점에 대한 조치를 하였으나 근본적으로 내부통제를 위한 보안규정 등 체계 및 제도 미흡으로 인해 보안취약성을 그대로 보이는 사례 등 4가지 취약 유형으로 구분할 수 있고 각 유형별 취약사례는 다음과 같다.

3.2.1 정보시스템의 안전조치 적정성

일반 사용자 단말기(PC 또는 노트북 등)에서 제어시스템 또는 업무시스템 등 정보시스템에 접속했을 때 제어망과 업무망을 연동하여 운영하거나 주요 시스템의 관리자 계정·비밀번호를 시스템 구축 시 초기값으로 운영하는 등 취약점 미조치 사례들이 있고 주요 취약점 유형은 Table 9와 같다.

Table 9. Vulnerable types by information system

system name	vulnerability	concerned results
control system	Bidirectional communication between business network and control system is possible, DB server administrator account not changed, etc.	Risk of driving malfunction
	Web server admin page exposure, admin account password not set, etc.	Risk of major information disturbance (forgery,alteration, deletion, etc.)
management information system	XSS vulnerability, neglect of administrator account management, etc.	Disturbing the XX market, such as reading or deleting information
	File upload vulnerability, unchanged administrator account, etc.	Leakage and forgery/ falsification of computer ledger DB information
web server	XSS vulnerability, file download vulnerability, etc.	Leakage, alteration and disturbance of logistic DB information
resource management system	ActiveX Control vulnerability, shared file operation, etc.	Confidential data (IP address, vulnerability analysis result, etc.) leaked
personal Information System	File upload and file download vulnerabilities, etc.	Member company information and power-related information leaked
security related systems, etc.	XSS vulnerability, vaccine server administrator account not changed, etc.	Main information such as internal work data, 6,000 PC IPs, etc.

3.2.2 개인정보 보호 및 관리 적정성

개인정보와 관련하여 사적으로 개인정보를 열람하거나 권한없는 자에게 공인인증서와 같은 인증정보를 주고 무단으로 개인정보를 열람하게 하여 관리가 부실하게 된 유형이다.

(사례 1) XX시 등 시·도 산하 X개 시·군·구 대상으로 X정보시스템에 입력된 열람용도와 실제 열람용도를 확인한 결과 총 X건 중 X건(X%)이 '·, ㅁ, 111' 등과 같이 열람용도를 알 수 없게 입력되어 있을 뿐만 아니라 X시 공무원 등은 타인의 개인정보를 사적 열람하거나 가족의 부탁을 받고 제공하는 등 개인정보 관리가 부실

(사례 2) XX통합관리망 접속기록을 확인한 결과 XX시 XX청 등 X개 시·군·구 소속 공무원(X명)이 시스템 접속에 필요한 사용자계정과 공인인증서를 자활근로자 등과 임의로 공유하고 있었고 자활근로자 X명은 업무와 관계없이 타인, 본인의 개인정보를 무단 열람하는 등 개인정보 관리가 부실

3.2.3 정보보안 인프라 구축 적정성

정보보안 인프라와 관련된 감사결과는 정보보안 활동으로 규정된 보안취약점 제거사업을 추진하면서 취약점을 식별하고도 이를 미이행하거나 보안장비 구축 후 업데이트를 실행하지 않아 신규 취약점에 쉽게 노출되어 해킹 공격의 대상이 되고 전체 시스템 마비 등 치명적인 피해가 우려되는 유형이다.

(사례 1) XX센터에서 X기관과 협의하지 않은 채 정보시스템 보안취약점 점검·제거 사업을 매년 추진하여 20XX년부터 20XX년까지 매년 X건에서 X건의 취약점을 발견하고도 제거한 건수가 X건에서 X건에 불과(평균 제거율 X%)하여 외부인(해커)이 위 보안취약점들을 이용하여 정보시스템에 침입할 우려

(사례 2) 정보시스템 보호를 위해 서버보안 장비(X종, X세트) 및 방화벽(X종, X세트)을 설치·운영하면서 서버보안 SW(짧게는 X개월에서 길게는 X년)와 방화벽 SW(짧게는 X개월에서 길게는 X년)를 최신버전으로 업그레이드하지 않고 구형 버전을 그대로 사용하고 있어 사이버침해에 제대로 대응하지 못할 우려

3.2.4 추진체계 및 제도운영 적정성

언론에 가장 많이 보도된 취약사례 중 하나로 관리적 관점에서 보안취약성에 대비할 필요가 있는 사항이며 감사결과 사례로는 용역업체 관리 소홀에 의한 내부자료 유출 위험이나 용역업체직원에 대한 신원조사 미실시로 인해 향후 보안사고 발생 요인을 사전에 차단하지 못하는 경우 등이 있다.

(사례 1) 각 기관에서 노트북 반입·반출 시 자료 무단 반출 여부 등을 매번 확인하는 하는 것이 번거롭다는 이유 등으로 제대로 확인하지 않아 X 등 X개 기관에서 용역업체 직원이 노트북 등에 기관 대외비 자료(전산망 구성도, IP주소 할당 현황 등) 또는 개인정보 등을 저장하여 반입·반출하거나 상용메일을 통해 전송하는 등 정보유출 위험이 있었고 X 등 X개 X에서 구축비용 1억 원 이상 X개 정보시스템 중 X개(X%) 정보시스템에서 용역업체 직원이 운영 중인 시스템에 직접 접근하여 작업을 하고 있는 등 정보유출 및 보안사고 위험

(사례 2) XX센터에서 출입자의 인적 위해요소를 차단하기 위해 상시 근무 용역업체 직원에 대한 신원조사를 하면서 업무 담당자가 X명에 대한 신원조사를 요구받고 X명에 대해서 신원조사를 의뢰하지 않는가 하면 미의뢰 사실을 숨기기 위해 X명에 대해 신원조사 결과 이상이 없는 것처럼 해당부서에 허위 통보

IV. 감사모델 제안 및 비교분석

보안감사를 수행함에 있어서 제한된 시간과 인력으로 전사적 감사활동을 수행하는 것은 현실적으로 어려우며 점검분야의 중요도를 고려한 필수 점검 영역을 식별하고 이를 반영한 모델을 개발하는 것이 필요하다.

이에 제안모델은 실제 감사결과 취약부문으로 식별된 사항을 점검항목에 포함하도록 중요도를 부여함으로써 보안감사 세부점검항목 작성 및 감사계획 수립 시 활용하는데 목적이 있다.

4.1 정보시스템의 안전조치 분야

제안모델의 첫 번째 분야는 정보시스템 안전조치 분야로, 취약점들을 종합하여 분석한 결과 필수 점검사항으로 정보시스템 서버 관리자 계정관리(Information system server administrator account management) 등 9가지 점검항목을 도출하였으며 전체 항목은 Table 10과 같다.

그리고 위 9가지 점검항목을 기존 모델들의 점검항목과 비교해본 결과, Table 11과 같이 'I-1. 정보시스템 서버 관리자 계정관리(Information system server administrator account management)' 항목은 FISCAM 모델의 '일반통제의 접근통제(Access Control)' 점검항목에 해당

Table 10. Inspection items for information system safety

I-1. Information system server administrator account management
I-2. Separate management of control system and internal business network
I-3. Whether security check activities such as installation of vaccine programs
I-4. Check whether access records are managed
I-5. Adequacy of encryption and access record management when constructing an information system
I-6. Firewall policy setting adequacy
I-7. Software security vulnerability check adequacy
I-8. Appropriateness of exporting important data
I-9. Checking server major vulnerabilities using mock hacking

Table 11. Checklists for information system safety measures by domestic and foreign audit models

<table>
<tr><th colspan="2">2.1 FISCAM</th><th>2.2 Handbook</th></tr>
<tr><td colspan="2">- General control
② Access Control(I-1)</td><td rowspan="2">Audit Issue 5: Confidentiality(I-9)
Audit Issue 6: Organizational Structure(I-1,2)
Audit Issue 7: Reconciliation(I-5)</td></tr>
<tr><td colspan="2">- Application Control
① Application level General control(I-5,7)
② Business Process Control(I-4)
③ Interface Control (I-6)</td><td>Audit Issue 10: Configuration Management(I-4,6)
Audit Issue 11: Asset Management(I-3,7)</td></tr>
<tr><th colspan="2">2.3 ISO27001</th><th>2.4 ISMS-P</th></tr>
<tr><td colspan="2">⑥ Communication and Operations Management(I-6,8)
⑦ Access Control (I-1)</td><td>2.5 Authentication and Rights Management (I-4,5)
2.6 Access Control(I-1)
2.7 Encryption Enforcement(I-8)
2.8 Information system introduction and development security(I-6)</td></tr>
<tr><th colspan="2">2.5 FSA Manual</th><th>2.6 Checkpoints for infra</th></tr>
<tr><td rowspan="4">4.</td><td>Administrative information security operation status(I-1)</td><td rowspan="4">Network configuration and access control(I-2,5), Threat detection and removal(I-9), System security management(I-6), Update and data transmission(I-1,8)</td></tr>
<tr><td>Technical information security operation status(I-4,7)</td></tr>
<tr><td>Prevention of hacking and malware infection(I-6,9)</td></tr>
<tr><td>Automated device security(I-3)</td></tr>
</table>

되는 것을 확인할 수 있고 나머지 정보시스템 안전성 조치 분야 점검항목들도 기존 모델들의 점검항목에 포함됨을 알 수 있다.

4.2 개인정보 보호 및 관리 분야

개인정보 보호 및 관리 분야 취약점들을 종합하여 분석한 결과, 필수 점검사항으로 퇴직자에 대한 계정관리(Account management for retirees) 등 9가지 점검항목을 도출하였으며 전체 항목은 Table 12와 같다.

Table 12. Inspection items for personal information

P-1. Account management for retirees
P-2. Personal information access management
P-3. Examples of sharing personal information, etc.
P-4. Cases of private viewing of personal information
P-5. Management and supervision of consigned companies for personal information processing
P-6. Confirmation of unnecessary retention of personal information
P-7. Confirmation of the status of registration of personal information of public institutions
P-8. Confirmation of personal information destruction

그리고 위 8가지 점검항목을 기존 모델들의 점검항목과 비교해본 결과, 'P-1. 퇴직자에 대한 계정관리(Insufficient account management for retirees)' 항목은 INTOSAI IT Handbook 모델의 '교육훈련 (Audit Issue 13: Training)' 점검항목에 해당되는 것을 확인할 수 있고 나머지 개인정보 보호 및 관리 분야 점검항목들도 Table 13과 같이 기존 모델들의 점검항목에 포함됨을 알 수 있다.

Table 13. Checklists for personal information protection and management by domestic and foreign audit models

<table>
<tr><th>2.1 FISCAM</th><th>2.2 Handbook</th></tr>
<tr><td>- Application Control
④ Data Management System Control(P-2,5)</td><td>Audit Issue 12: Employee Awareness and Responsibilities (P-2,3,5,6,8)
Audit Issue 13: Training(P-1)</td></tr>
<tr><th>2.3 ISO27001</th><th>2.4 ISMS-P</th></tr>
<tr><td>④ Human Resources Security (P-2,3,4)</td><td>2.2 Human Security(P-4)
3.1 Protective measures when collecting personal information(P-3)
3.2 Protective measures for retention and use of personal information(P-6)
3.3 Protective measures when providing personal information(P-2)
3.4 Protective measures when</td></tr>
</table>

		personal information is destroyed(P-8) 3.5 Protection of data subject rights(P-5)
2.5 FSA manual		2.6 Checkpoints for infra
4.	data security (P-1)	As it deals only with information system management that operates infrastructure, there are no relevant inspection items in the field of personal information protection.
	human security (P-2,3,4)	

4.3 정보보호 인프라 구축 분야

정보보호 인프라 구축 분야 취약점들을 종합하여 분석한 결과, 필수 점검사항으로 재난복구조치 확립의 적정성(Adequacy of establishment of disaster recovery measures) 등 10가지 점검항목을 도출하였으며 전체 항목은 Table 14와 같다.

그리고 위 10가지 점검항목을 기존 모델들의 점검항목과 비교해본 결과, 'F-1. 재난복구조치 확립의 적정성(Adequacy of establishment of disaster recovery measures)' 항목은 INTOSAI IT Handbook 모델의 정책과 절차 'Audit Issue 8: Policies and Procedures' 점검항목에 해당되는 것을 확인할 수 있고 나머지 정보보호 인프라 구축 분야 점검항목들도 Table 15에서와 같이 기존 모델

Table 14. Inspection items for construction of information security infrastructure

Detailed inspection items
F-1. Adequacy of establishment of disaster recovery measures
F-2. Application security verification
F-3. Adequacy of management of portable storage media
F-4. Adequacy of information security measures
F-5. Server management adequacy and security control adequacy check
F-6. Appropriate use of security control system, etc.
F-7. Adequacy of repeated security vulnerability measures
F-8. Adequacy of security equipment update
F-9. Adequacy of building disaster recovery system
F-10. Disaster recovery center establishment and operation standards adequacy

Table 15. Checklists in the field of information security infrastructure construction by domestic and foreign audit models

2.1 FISCAM	2.2 Handbook
- General control ① Security Management (F-2,7)	Audit Issue 1: Assessment Methods(F-7) Audit Issue 2: Assessment Scope(F-9) Audit Issue 3: Mitigation (F-6)
	Audit Issue 8: Policies and Procedures(F-1) Audit Issue 9: Network Control(F-5)
	Audit Issue 14: Organizational Safety in the Territory(F-10) Audit Issue 15: Physical Access(F-4) Audit Issue 16: Intrusion Prevention(F-8)
2.3 ISO27001	2.4 ISMS-P
③ Asset Management (F-5,9,10) ⑤ Physical and Environmental Security(F-4) ⑩ Business Continuity Management (F-9,10) ⑪ Compliance(F-1)	2.1 Policy, Organization and Asset Management(F-1) 2.3 Outsider Security (F-9) 2.4 Physical Security(F-4) 2.9 System and service operation management (F-6) 2.10 System and service security management (F-5) 2.11 Accident prevention and response(F-7) 2.12 Disaster Recovery (F-10)
2.5 FSA manual	2.6 Checkpoints for infra
4. physical and environmental controls(F-4)	Asset management (F-5,9,10), Portable device Security management(F-2,3)
5. Network configuration for efficient monitoring (F-5)	
Monitoring result analysis and response(F-6,7)	

들의 점검항목에 포함됨을 알 수 있다.

4.4 추진체계 및 제도운영 분야

정보보호 인프라 구축 분야 취약점들을 종합하여 분석한 결과, 필수 점검사항으로 재난복구조치 확립의 적정성(Adequacy of establishment of disaster recovery measures) 등 8가지 점검항목을 도출하였으며 전체 항목은 Table 16과 같다.

그리고 위 8가지 점검항목을 기존 모델들의 점검항목과 비교해본 결과, 'S-1. 재난복구조치 확립의 적정성(Adequacy of establishment of disaster recovery measures)' 항목은 FISCAM 모델의 '일반통제의 업무분리(Segregation of Duties) 점검항목에 해당되는 것을 확인할 수 있고 나머지 추진체계 및 제도운영 분야 점검항목들도 Table 17에서와 같이 기존 모델들의 점검항목에 포함됨을 알 수 있다.

Table 16. Inspection items for implementation systems and system operation

Detailed inspection items
S-1. Service company security management
S-2. Management, such as checking whether measures are taken after security review
S-3. Check whether the target of security vulnerability diagnosis is omitted
S-4. Personnel management, such as background check for regular employees other than employees
S-5. Security system design adequacy
S-6. Appropriateness of designation of major information and communication infrastructure
S-7. Appropriateness of integrated control of personal information in the medical sector
S-8. Adequacy of external service security management

Table 17. Checklists for implementation systems and system operation fields by domestic and foreign audit models

2.1 FISCAM	2.2 Handbook
- General control ③ Configuration Control(S-2,3,6) ④ Segregation of Duties(S-1) ⑤ Contingency Planning(S-5)	Audit Issue 4: Information Security Policy(S-1,5)
2.3 ISO27001	**2.4 ISMS-P**
① Security Policy(S-5) ② Organization of Information Security(S-6) ⑧ IS Acquisition, Development and Maintenance(S-2) ⑨ Information Security Incident Management (S-1)	1.1 Laying the foundation for the management system (S-1) 1.2 Risk management (S-2) 1.3 Management system operation (S-7) 1.4 Management system inspection and improvement (S-2)
2.5 FSA manual	**2.6 Checkpoints for infra**
1. Securing IT security system(S-5)	Basic activities(S-1), Incident response (S-2,3), Security management of service companies (S-4,8)
1. The role of management in the security system(S-6)	
1. Monitoring and supplementing security procedures (S-2)	
2. Clarification of information and information systems (S-1)	
2. Information collection and analysis(S-8), Risk assessment management plan(S-3)	
3. Information Security Policy and Regulations (S-4)	
3. technical design(S-5)	
3. Outsourcing service security service management(S-8)	

V. 결 론

본 논문에서는 감사자의 개인 역량에 독립적이면서 감사중점 선정 시 일관성있는 감사결과를 확보하기 위한 보안 감사모델을 제시하고자 많은 감사결과를 분석하였다. 이를 통해 정보시스템의 안전조치 등 4가지 분야 35개 항목으로 구성된 모델을 제시함으

로써 제한된 인력 및 시간으로 효율적인 점검이 이루어질 수 있도록 하였다. 물론 35개 항목만 점검하면 모든 취약점을 확인할 수 있는 것은 아니지만, 본 논문에서 제시하는 해당 분야별 필수 점검항목이 최근 10년 간의 감사결과를 통해 확인된 실증적 점검항목이라는 것에 의미가 있고 현재까지도 이러한 보안취약점들은 지속적으로 점검대상이 되고 있어 보안감사 수행 시 세부 점검계획 작성 등에 활용할 수 있다. 향후 연구방향으로는 최근 들어 랜섬웨어 공격이나 APT 공격 등 과거와 달리 지능적인 공격양상을 띤 해킹사례가 많아지고 있는 만큼 이를 점검할 수 있는 모델에 대한 연구를 진행하고자 한다.

References

[1] GAO, Federal Information System Controls Audit Manuals(GAO-090232G), Feb. 2009

[2] INTOSAI WGITA-IDI, Handbook on IT Audit for Supreme Audit Institution, Appendix VII, pp. 107-115, 2014

[3] Wikipedia, ISO/IEC 27001, http://en.wikipedia.org/wiki/ISO/IEC_27001:2013 search

[4] Korea Internet & Security Agency, "Introduction of system" in "Certification of information protection and personal information protection management system" (isms-p.kisa.or.kr)

[5] Financial Supervisory Service, IT Audit Manual, pp. 474-497. 2019.

[6] Ministry of Science and ICT and Korea Internet & Security Agency, "Detailed Guide to Analysis and Evaluation Methods for Technical Vulnerabilities in Major Information and Communication Infrastructure", Dec. 2017.

[7] Board of Audit and Inspection, "Financial Supervision Act, including Financial Consumer Protection", pp. 68-76, Feb. 2012.

[8] Board of Audit and Inspection, "Actual status of social service e-voucher business selection (National Assembly audit)", pp. 37-42, Oct. 2011.

[9] Board of Audit and Inspection, "State of Crisis Management of National Core Infrastructure", pp. 102-105, Dec. 2012.

[10] Board of Audit and Inspection, "Public Institutions Information Protection and Cyber Safety Management Status", pp. 26-98, Mar. 2012.

[11] Board of Audit and Inspection, "Financial Consumer Protection and Supervision"(local action completed), 2013

[12] Board of Audit and Inspection, "Operation of diplomatic missions abroad and the implementation of major projects of the Ministry of Foreign Affairs", pp. 105-109, Nov. 2014.

[13] Board of Audit and Inspection, "Actual status of financial sector information protection and cyber safety management supervision", pp. 10-12, Apr. 2014.

[14] Board of Audit and Inspection, "Financial Execution Management Status", pp. 46-50, Apr. 2014.

[15] Board of Audit and Inspection, "Institutional operation audit by the Ministry of Safety and Public Administration", pp. 31-39, Aug. 2014.

[16] Board of Audit and Inspection, "Actual Inspection and Supervision of Personal Information Leakage of Financial Companies", pp. 57-62, Jul. 2014.

[17] Board of Audit and Inspection, "The status of handling civil complaints in the first half of the year", pp. 25-28, Sep. 2014.

[18] Board of Audit and Inspection, "National Police Agency Operation

Audit", pp. 55-58. Jun. 2015.
[19] Board of Audit and Inspection, "The Current State of Management of Public Institutions that Support Electricity", pp. 32-34, Jun. 2015.
[20] Board of Audit and Inspection, "Construction and Operation of the National Integrated Traffic Information System", pp. 14-19, Oct. 2016.
[21] Board of Audit and Inspection, "Local Office of Education Financial Management(5)(Ministry of Education, Seoul Office of Education)", pp. 61-65, Dec. 2015.
[22] Board of Audit and Inspection, "National Cyber Safety Management Status", pp. 140-146, Apr. 2016.
[23] Board of Audit and Inspection, "Main informatization business contract business promotion status", pp. 41-52, Aug. 2016.
[24] Board of Audit and Inspection. "Public Safety Threat Factor Response Management(Airport Safety and Firearms and Explosives)", pp. 46-47, Sep. 2016.
[25] Board of Audit and Inspection . "Checking the capability to respond to cyber breaches of major information and communication infrastructure"(Secret), Nov. 2016.
[26] Board of Audit and Inspection, "National Tax Information System Utilization and Security Status", pp. 31-32, Jan. 2017.
[27] Board of Audit and Inspection, "Construction and Utilization of National Geospatial Data", pp. 159, 2017.
[28] Board of Audit and Inspection, "Educational Information System Establishment and Operation Status"(local action completed), 2017.
[29] Board of Audit and Inspection, "Unauthorized reading and leakage of electronic medical records at Seoul National University Hospital", pp. 24-34, Mar. 2017.
[30] Board of Audit and Inspection, "Construction and Utilization of Information System for Land and Environment", pp. 58-69, Sep. 2017.
[31] Board of Audit and Inspection, "Status of National Public Official Personnel Management and Management", pp. 68-73, Nov. 2017.
[32] Board of Audit and Inspection, "Construction and utilization of public data", pp. 158-175, Jun. 2018.
[33] Board of Audit and Inspection, "Public Teacher Appointment Exam Management Status", pp. 31-34. Aug. 2018.
[34] Board of Audit and Inspection, "The Postal Business Management Status", pp. 53-65, Oct. 2018.
[35] Board of Audit and Inspection, "Inspection of allegations related to contract by the Korea Employment Information Service", pp. 15-21, Aug. 2018.
[36] Board of Audit and Inspection, "Management Status of Agricultural Product Price Stabilization Subsidy Support Project", pp. 25-28. Aug. 2019.
[37] Board of Audit and Inspection, "Regional Indigenous Corruption, etc. Startup Inspection Ⅲ", pp. 32-42, Jun. 2019.
[38] Board of Audit and Inspection, "Korea Foundation, Overseas Koreans Foundation Institutional Operation Audit", pp. 49-52, Jul. 2019.
[39] Board of Audit and Inspection, "Operation of diplomatic missions abroad and the headquarters of the Ministry of Foreign Affairs", pp.

93-97, Jan. 2020.
〔40〕 Board of Audit and Inspection, "The Status of Settlement Support for North Korean Refugees", pp. 43-46, Mar. 2020.
〔41〕 Board of Audit and Inspection, "Pharmaceutical Safety Management Status", pp. 31-33, Jul. 2020.
〔42〕 Board of Audit and Inspection, "Chungcheongnam-do Institutional Audit", pp. 121-125, Oct. 2020.
〔43〕 Board of Audit and Inspection. "An Research on Efficient Audit Methodology for Information Security and Cyber Safety ", Dec. 2021.

〈저자소개〉

김 현 석 (Hyun-seok Kim) 정회원
2000년 3월: 육군사관학교 관리학과
2006년 2월: 고려대학교 컴퓨터학과 석사
2009년 2월: 고려대학교 컴퓨터학과 박사
2000년 3월~2012년 2월: 육군 정보통신장교
2012년 6월~현재: 감사원 감사관(사무관)
〈관심분야〉 정보보호, 정형검증, 암호프로토콜, IoT네트워크