Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

The Rational Improvement Plans of Inspection Standards on Vulnerability Analysis and Evaluation in Electronic Financial Infrastructure

Gwang-Bae Kim[1], **Hun-Yeong Kwon**[*2]

[1]*Department of Financial Security, School of Information Security, Korea University*
[2]*School of Information Security, Korea University*

ABSTRACT

To secure the safety and reliability of the electronic financial transactions, the financial company perform vulnerability analysis and evaluation on the electronic financial infrastructure. However, the financial sector vulnerability analysis and evaluation criteria that are used in the analysis and evaluation of electronic financial infrastructure vulnerabilities by financial companies have not been updated since its distribution in 2012, Although vulnerability analysis and evaluation agencies such as the financial information sharing and analysis center and the information security professional services company are updating their own vulnerability analysis and evaluation standards, since the standards are not standardized, financial companies are confused when performing vulnerability analysis and evaluation. n this paper, we analyze the problems of the existing analysis and evaluation criteria of the electronic financial infrastructure and propose a measure to establish a reasonable inspection standard in accordance with the characteristics of the financial institution's electronic financial infrastructure and suggest a supplementary point using the information security management system. In addition, We introduced example case of establishing the criteria of analyzing and evaluating the vulnerability according to the autonomous security system of the financial company

KEYWORDS: Information security, Financial security, Electronic financial infrastructure, Vulnerabilities analysis, ISMS(Information Security Management System)

ARTICLE INFO: Received 27 November 2017, Revised 6 December 2017, Accepted 8 December 2017.

[*]Corresponding author is with the Graduate School of Information Security, Korea University, 145 Anam-ro SeongBuk-gu Seoul, 02841, KOREA.
E-mail address: khy0@korea.ac.kr

1. 서 론

정보통신 분야가 급속도로 성장해가면서 다양한 기술변화를 겪고 있으며, 4차 혁명에 따른 금융 환경도 빠르게 진화되고 있다. 최근 금융 환경은 비대면 계좌개설, 간편 결제와 송금, 간편인증 등 스마트폰을 활용한 전자금융서비스가 다양해짐에 따라 스마트폰뱅킹 이용 건수와 금액이 증가하는 추세이며, 4차 혁명 기반기술인 인공지능·블록체인·생체인증·사물인터넷 등을 전자금융거래에 적용하여 핀테크 산업이 활성화되어 가고 있다. 이러한 전자금융거래의 발전에 비례하여 이를 위협하는 각종 전자적 침해 공격 또한 급증하였다. 2005년 국내 최초 인터넷뱅킹 해킹사건이 발생한 후 2009년 7.7 DDoS 사이버테러, 2011년 현대캐피탈 고객정보 유출사고 및 농협은행 전산망 장애사고, 2013년 3.20 및 6.25 사이버테러, 2014년 카드3사 개인정보 유출사고 등은 금융권에 큰 피해를 남겼을 뿐 아니라 사회적으로도 큰 혼란을 야기했다[1]. 이러한 전자적 침해사고에 대응하기 위해 정부 및 금융감독당국, 금융회사는 다양한 금융보안 정책을 수립해 이행하고 있다.

정부와 금융감독당국은 금융회사의 전자금융거래의 안정성과 이용자 보호를 위해 금융회사의 전자금융기반시설에 대해 취약점 분석·평가를 실시하고 이에 따른 보완조치의 이행계획 수립 등에 관한 사항을 「전자금융거래법」 등 법령으로 정하여 시행하고 있다. 이에 따라 금융회사는 매년 전자금융기반시설에 대해 취약점 분석·평가를 실시하여 관리적, 물리적, 기술적 보호조치를 하는 등 정보보호에 많은 노력을 기울이고 있다. 그러나 현행 금융회사에서 전자금융기반시설 취약점 분석·평가 시 활용하는 금융위원회 금융분야 취약점 분석·평가 기준은 전자금융기반시설의 안정성과 신뢰성을 위협하는 다양한 사이버 보안 항목에 대해 종합적으로 분석 및 평가하기에 한계가 있다.

본 논문의 2장에서는 전자금융기반시설의 개요 및 전자금융기반시설 정보보호의 중요성과 전자금융기반시설 취약점 분석·평가 법제에 대해 살펴본다. 3장에서는 금융회사 취약점 분석·평가 현황과 전자금융기반시설 취약점 분석·평가 점검기준 문제점에 대해 분석하고, 4장에서는 전자금융기반시설 특성에 맞는 합리적인 점검기준 수립 방안과 금융회사 자체기준수립 사례를 제시하고자 한다.

2. 전자금융기반시설의 이해

2.1 전자금융기반시설 개요

전자금융거래는 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다. 이러한 전자금융거래에 이용되는 정보처리시스템 및 정보통신망(전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계)을 전자금융기반시설이라 한다[2][3].

금융회사의 전자금융기반시설 구성은 은행권역, 증권회사권역 등 권역별로 다소 차이가 있으나 <그림 1>과 같이 내부시스템을 보호하기 위해 대체로 외부통신망과 내부통신망 사이의 독립된 통신망(DMZ; Demilitarized Zone)을 구성하고, 다양한 보안장치를 마련하여 운영하고 있는 것이 일반적이다[4]. DMZ구간에는 이용자가 금융회사와의 거래를 위해 접근할 수 있는 유일한 구간으로 웹서버 등이 위치하고 있다. 뱅킹서버구간은 DMZ구간에 위치한 서버들과 통신하는 인터넷 뱅킹서버 및 DB서버 등이 위치하고, 내부서버구간은 계정계, 정보

계 등 각종 금융정보를 처리하고 금융거래 정보를 관리, 분석하는 서버 등이 위치해 있으며, 대외계 구간은 금융공동망 등 타 금융회사의 거래에서 중계를 담당하는 서버가 위치해 있다[5].

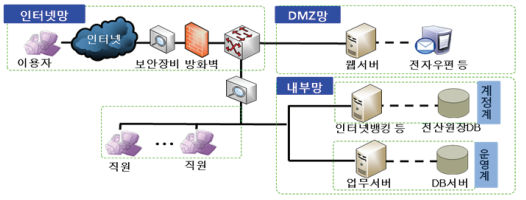

그림 1. 금융회사 정보통신망 구성
Figure 1. Financial Information&Communication Network configuration

2.2 전자금융기반시설 정보보호 중요성

1999년 국내 인터넷뱅킹서비스가 개시된 이후 급속한 발전을 거듭하여 2016년 9월말 기준 등록 고객수가 1억 2천만 명, 일평균 이용건수와 금액도 약 8,800만 건 및 41조 6천억 원에 이를 정도로 널리 이용되고 있다. 최근에는 정부의 핀테크 산업 활성화 정책 등으로 간편 결제와 송금, PG(전자지급결제대행, Payment Gateway), 직불·선불지급수단 등 전자지급 서비스도 2015년을 기점으로 크게 성장하고 있는 추세이다[1]. 이러한 전자금융거래에 이용되는 전자금융기반시설은 대량의 개인정보(주민등록번호, 계좌번호, 신용카드번호 등) 및 중요정보(금융거래정보, 비밀번호 등)를 처리하는 중요 정보시스템으로 구성되어 있기 때문에 정부 및 금융당국은 해당 시설보호를 위해 각종 법제도를 마련하고 있으며, 금융회사에서도 자율보안체계에 따라 실질적 보안강화를 위해 노력하고 있다[6].

2.3 전자금융기반시설 취약점 분석·평가 법제

전자금융사고가 지속적으로 발생함에 따라 전자금융거래의 안전한 기반 조성을 위해 관련된 법을 제정 및 개정하고 있다.

금융회사 취약점 분석·평가는 「정보통신기반 보호법」에 의해 주요정보통신기반시설로 지정 된 기관만 취약점 분석·평가를 수행해왔는데, 2013년 발생한 '3.20 사이버테러' 이후 「전자금융거래법」이 개정되어 <표 1>과 같이 금융회사의 전자금융기반시설에 대한 취약점 분석·평가가 의무화되었다. 이에 따라 금융회사는 전자금융기반시설에 대하여 연 1회(홈페이지에 대해서는 6개월에 1회) 이상 수행하고 결과보고 및 보완조치 이행계획서를 그 취약점 분석·평가 종료 후 30일 이내에 금융위원회에 제출하여야 한다[2][7].

표 1. 전자금융기반시설 취약점 분석·평가 법·규정 현황
Table 1. Status of laws and regulations related to analysis and evaluation of vulnerabilities of electronic financial infrastructure

관련법령	취약점 분석·평가관련 주요내용
전자금융거래법	제21조의3 (전자금융기반시설의 취약점 분석·평가)
전자금융거래법 시행령	*전자금융거래법에서 위임된 사항 제11조의4 (전자금융기반시설 취약점 분석·평가의 내용) 제11조의5 (전자금융기반시설 취약점 분석·평가의 절차 및 방법 등)
전자금융감독규정	*전자금융거래법, 시행령에서 위임된 사항 제37조의2 (전자금융기반시설의 취약점 분석·평가 주기, 내용 등) 제37조의3 (전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등)
전자금융감독규정 시행세칙	제7조의2 (전자금융기반시설의 취약점 분석·평가의 내용)

3. 금융회사 취약점 분석·평가 현황 및 점검기준 문제점

본 장에서는 금융회사에서 수행하고 있는 전자

금융기반시설 취약점 분석·평가, 주요정보통신기반시설 취약점 분석·평가, 정보보호관리체계(ISMS; Information Security Management System) 인증 현황에 대해 점검기준 중심으로 알아보고, 전자금융기반시설 점검기준의 문제점을 도출하고자 한다.

3.1 전자금융기반시설 취약점 분석·평가

금융회사는 「전자금융거래법」에 따라 전자금융기반시설에 대해 연 1회(홈페이지는 연 2회)이상 취약점 분석·평가를 실시해야 한다[2].

취약점 분석·평가는 금융회사가 자체전담반을 구성하여 실시하거나 「정보통신기반보호법」에 의거 일정한 자격요건을 갖춘 금융분야 정보공유·분석센터(ISAC; Information Sharing and Analysis Center), 금융위원회가 지정한 침해사고대응기관 및 미래창조과학부가 지정한 정보보호 전문서비스 기업 등 전문성을 갖춘 외부기관에 의뢰하여 수행할 수 있다[2].

전자금융기반시설 취약점 분석·평가 점검 세부항목은 금융위원회 금융분야 취약점 분석·평가 기준을 활용하여 금융회사에서 자율적으로 정하여 점검하고 있다.

금융위원회 금융분야 취약점 분석·평가 기준은 2012년 6월 금융위원회에서 「전자금융감독규정」 제 15조(해킹 등 방지대책) 및 제 17조(홈페이지 등 공개용 웹서버 방지대책), 「금융IT부문 보호업무 모범규준」에 의거 금융회사 등은 주기적으로 취약점 분석·평가를 실시하는데 이와 관련하여 금융회사에 배포한 기준이다. <표 2>와 같이 전자금융감독규정 각 조 항을 근거로 구성한 정보보호관리체계 285개 항목과 기술분야 173개 항목으로 구성되어 있다. 전자금융기반시설, IT부문 사업 등 취약점 분석·평가 대상에 적합하지 않은 항목은 평가항목을 생략할 수 있으나 그 사유를 취약점 평가 결과에 명시하여야 하며, 평가대상의 특성, 위협, 취약성, 보안 이슈사항 등을 고려하여 선택적으로 평가항목을 추가할 수 있도록 하였다[8].

표 2. 금융위원회 금융분야 취약점 분석·평가 기준
Table 2. Financial Services Commission Vulnerability Analysis and Measurement Criteria in financial sector

통제항목		항목수
1	인력	4
2	조직	3
3	예산	2
4	건물 및 설비	19
5	전산실	17
6	단말기	13
7	전산자료	22
8	정보처리시스템	10
9	정보보호시스템	7
10	공개용 웹서버	22
11	전산망	1
12	IP주소	5
13	정보기술계획	4
14	정보기술사업	4
15	정보기술계약	9
16	정보기술감리	5
17	용량·성능관리	1
18	직무분리	8
19	전산원장통제	8
20	거래통제	2
21	프로그램통제	10
22	일괄작업 통제	5
23	암호프로그램·키관리통제	4
24	내부사용자 비밀번호관리	8
25	정보기술 이웃소싱	14
26	정보기술부문 실태평가	3
27	전자금융거래시 준수사항	10
28	이용자 유의사항 공지	5
29	보안성심의	3
30	이용자 비밀번호관리	11
31	취약점분석·평가	2
32	침해사고 예방	7
33	악성코드 감염방지	5
34	비상대책	17
35	재해복구센터	4
36	재해복구훈련	1
37	침해사고 대응훈련	2

38	전자금융사고보고	8
	정보보호관리체계	285
1	UNIX서버	44
2	Windows서버	46
3	데이터베이스	10
4	보안장비	16
5	네트워크장비	14
6	웹서비스	28
7	스마트폰뱅킹	15
	기술적 분야 합계	173
	합계	458

3.2 주요정보통신기반시설 취약점 분석·평가

표 3. 주요정보통신기반시설 취약점 분석·평가 점검기준
Table 3. Critical information communication infrastructure vulnerability analysis and Measurement Criteria

분류		항목수	
		필수 (상)	옵션 (중・하)
관리적 분야	1. 정보보호정책	4	4
	2. 정보보호조직	1	3
	3. 인적 보안	2	4
	4. 외부자 보안	2	3
	5. 자산분류	3	2
	6. 매체관리	2	3
	7. 교육및훈련	1	4
	8. 접근통제	7	14
	9. 운영관리	13	20
	10. 업무연속성	1	3
	11. 사고대응	3	10
	12. 감사	0	5
관리적 분야 합계		39	75
물리적 분야	1. 접근통제	2	1
	2. 감시통제	4	4
	3. 전력보호	1	3
	4. 환경통제	0	11
물리적 분야 합계		7	19
기술적 분야	1. 유닉스	43	30
	2. 윈도우즈	45	37
	3. 보안장비	16	10
	4. 네트워크장비	14	24
	5. 제어시스템	16	6
	6. PC	14	6
	7. 데이터베이스	11	13
	8. 웹	28	0
기술적 분야 합계		187	126
합계		233	220

「정보통신기반보호법」에 따라 주요정보통신기반시설로 지정된 금융회사는 주요정보통신기반시설에 대해 매년 취약점 분석·평가를 실시해야 한다[9]. 금융회사 주요정보통신기반 지정시설은 은행 인터넷뱅킹시스템, 증권사 사이버트레이딩시스템 등이 있으며, 2014년도 금융부문 주요정보통신기반시설 지정·관리 기관은 17개 은행과 15개 증권사를 포함하여 40개 기관, 49개 시설이 지정되어 있다[4].

주요정보통신기반시설 취약점 분석·평가 기준은 법령에 고시「미래창조과학부고시 제2013-37호]되어 있으며, <표 3>과 같이 점검항목은 관리적, 물리적, 기술적 분야별로 나누어져 있고, 중요도에 따라 상・중・하로 구분되어 있다. '상' 항목인 233개 항목을 필수 점검하고 '중'・'하' 항목인 220개 항목을 기관의 사정 및 당해 연도 주요정보통신기반시설 보호대책 수립지침에 따라 선택하여 점검한다[10].

3.3 정보보호관리체계(ISMS) 인증

2014년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 전년도 매출액 100억 이상 또는 전년도 말 기준 직전 3개월간의 일평균 이용자 수가 100만 명 이상인 금융회사는 의무적으로 ISMS 인증을 받도록 하였으나, 2016년 법이 개정되면서 의무화 대상에서 제외되었다[3]. 하지만, 금융회사는 2017년 9월 기준 10개 은행, 17개 금융투자, 5개 보험사 등 총 48개 기관이 인터넷 뱅킹 서비스 운영, 트레이딩 시스템 운영(HTS, MTS, WTS) 등을 인증범위로 정보보호관리체계 인증을 취득·유지하

고 있다[11].

정보보호관리체계 인증기준은 정보보호관리체계 인증 등에 관한 고시[과학기술정보통신부고시 제 2017-7호]로 지정되어 있으며, 정보보호관리과정과 정보보호대책으로 구성되어 있다.

금융분야 정보보호관리체계 인증기준 점검항목은 한국인터넷진흥원(KISA; Korea Internet & Security Agency) 253개 점검항목에 금융권 보안요구사항 및 금융권 특성을 반영하여 <표4>와 같이 324개 점검항목으로 이루어져 있다[12].

표 4. 금융분야 정보보호관리체계 인증기준 점검항목
Table 4. Inspection criteria of information security management system in financial sector

구분		항목수
정보보호 관리과정	1. 정보보호정책 수립 및 범위설정	4
	2. 경영진 책임 및 조직구성	6
	3. 위험관리	11
	4. 정보보호대책 구현	3
	5. 사후관리	7
	소계	31
정보보호 대책	1. 정보보호정책	14
	2. 정보보호조직	10
	3. 외부자보안	14
	4. 정보자산분류	7
	5. 정보보호교육	10
	6. 인적보안	12
	7. 물리적보안	27
	8. 시스템개발보안	28
	9. 암호통제	12
	10. 접근통제	52
	11. 운영보안	83
	11. 침해사고 관리	16
	13. IT재해복구	8
	소계	293
합계		324

3.4 전자금융기반시설 취약점 분석·평가 점검기준 문제점

첫 번째, 전자금융기반시설 취약점 분석·평가 점검기준으로 활용하는 금융위원회 금융분야 취약점 분석·평가 기준은 2012년 6월 배포되어 이후 업데이트되지 않고 있다. 전자금융감독규정 각 조항을 근거로 구성한 정보보호관리체계 점검항목은 금융회사가 자율적으로 전자금융감독규정 개정사항을 분석하여 점검항목에 반영하고 있으나 금융회사별 일관성이 없다.

두 번째, 기술적 분야 점검기준에서 전자금융거래 시 이용하는 채널 및 서비스에 대한 최신 위협 점검항목이 부족하다. 최근 핀테크 기술의 발달로 전자금융거래에 대한 채널이 다양화되고 신기술을 이용한 서비스 또한 증가 되고 있으나 금융분야 취약점 분석·평가 점검기준으로는 한계가 있다.

세 번째, 전자금융기반시설 점검기준에는 주요정보통신기반시설 점검기준에 있는 PC에 대한 점검기준이 없다.

네 번째, 전자금융기반시설 범위에 포함된 정보자산을 식별하지 못해 취약점 분석·평가 점검대상에서 제외될 확률이 높다. 2016년도 KISA 내부보고자료에 따르면 2015년 정보보호관리체계 인증심사 주요 결함 목록에는 인증범위의 정보자산 식별에 대한 결함이 두 번째로 많다[13].

마지막으로 일부 전자금융기반시설 취약점 점검 세부항목의 점검기준이 금융분야 정보공유·분석센터와 정보보호 전문서비스 기업별로 상이하다. 금융회사는 자체인력 및 전문인력 부족 등으로 전자금융기반시설에 대한 취약점 분석·평가를 외부기관에 의뢰하여 수행하고 있는데, 점검 기관별 동일 점검항목에 대한 점검기준이 서로 다르면 금융회사 취약점 분석·평가 결과 조치 및 이행계획 수립 시 혼란을 야기할 수 있다.

4. 전자금융기반시설 취약점 분석·평가 점검기준 개선 방안

4.1 전자금융기반시설 취약점 분석·평가 공통 점검기준 수립

전자금융기반시설의 취약점 분석·평가 점검기준을 현행화하고 전자금융거래 매체 및 서비스에 대한 최신 위협을 반영하여 금융회사의 취약점 분석·평가 수준을 전반적으로 향상시키기 위해 전자금융기반시설 취약점 분석·평가 공통 점검기준 수립을 제안한다.

전자금융기반시설 취약점 분석·평가 공통 점검기준 수립을 위한 방법으로 금융보안 관련 법령을 주관하고 금융보안정책 및 제도에 관한 사항 등을 총괄·관리하는 금융위원회와「정보통신기반보호법」에 따라 금융분야 정보공유·분석센터이며,「전자금융감독규정」에 따라 침해사고 대응기관인 금융보안원,「정보보호산업의 진흥에 관한 법률」에 따라 취약점 분석·평가 전문기관인 정보보호 전문서비스 기업[2] 그리고, 실제 전자금융기반시설 취약점 분석·평가를 수행하고 있는 금융회사가 참여하여 금융보안원 중심으로 금융보안 관계 법령을 분석하고 정보보호관리체계 점검항목을 최신화해야 한다. 더불어 금융권 전자금융기반시설 침해사고 현황에 대한 위협을 파악해 점검항목에 반영하여 주기적으로 금융회사에 배포해야 한다.

4.2 금융분야 정보보호관리체계 인증 확대

전자금융기반시설 범위에 포함된 정보자산을 식별하지 못해 취약점 분석·평가 점검대상에서 제외될 수 있는 문제점을 해결하기 위해 금융분야 정보보호관리체계 인증 확대가 필요하다.

금융보안원 사원기관수는 2017년 4월 기준 은행 18개, 금융투자 38개, 보험 42개, 금융유관기관 5개, 중소·서민 33개, 전자금융업자 12개, 기타 39개로 총 187개 기관이지만, 정보보호관리체계 인증을 취득·유지하고 있는 기관은 48개뿐이다[11][16].

금융분야 정보보호관리체계 인증은 <표 5>에서와 같이 정보자산분류 점검기준에 정보자산식별에 대한 통제항목이 포함되어 있으며, 매년 정보자산 분류에 대한 인증심사가 이루어져 전자금융기반시설 자산누락에 대한 예방 및 검증을 할 수 있다.

표 5. 금융분야 정보보호관리체계 인증 정보자산 식별 통제항목
Table 5. Information security management system of financial sector Information asset identification control item

통제항목	통제목적	점검항목
정보자산 식별	조직의 업무 특성에 따라 정보자산 분류기준을 수립하고 정보보호관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한, 식별된 정보자산을 목록으로 관리하여야 한다.	정보자산(정보시스템, 정보보호시스템, 정보, 전산자료 등)의 분류기준을 수립하고 정보보호관리체계 범위 내 모든 정보자산을 식별·관리하고 있는가?
		식별된 정보자산을 다음 항목이 포함된 별도 목록으로 관리하고 있는가? - 정보자산명, 자산번호, 모델명, 용도 - 정보자산별 책임자, 관리자, 관리부서 - 정보자산에 대한 보안등급 등
		정기적으로 정보자산 현황을 조사하고 정보자산목록을 최신으로 유지하고 있는가?

이 밖에도 금융분야 정보보호관리체계 인증은 전자금융기반시설의 정보보호관리체계에 대해 '일회성 관리', '부분적 보안'이 아닌 '지속적 관리', '전사적 보안'으로 관리체계를 강화할 수 있는 장점이 있다[14].

4.3 금융회사 자체 점검기준 수립

정보통신기술의 발달과 핀테크 기술이 전자금융

서비스에 적용되는 속도가 급격히 진전되면서 전자금융기반시설에 대한 취약점 분석·평가 점검기준으로는 다양하고 고도화된 전자금융 위협에 대응하기에는 여전히 한계가 있다.

정부 및 금융감독당국은 전자금융 침해사고 대응 및 금융권 IT보안 강화를 위하여 그동안 금융회사에게 특정 보안·인증기술의 사용 의무 등 보안 관련 규정을 항목별로 세세하게 규제해왔다. 하지만 전자금융거래법, 정보통신기반보호법과 하위규범 등에서 규제하고 있는 전자금융기반시설 취약점 분석·평가 점검기준은 기술발전 사항을 모두 반영하여 기준을 제시하는 것이 한계가 있기에 큰 틀에서 최소한의 기준만을 제시하고 금융기관이 어느 정도 자율성을 가지고 전자금융기반시설의 안전대책을 수립할 수 있도록 해주어야 하며, 금융회사 또한 이러한 자율보안을 위해 자체 점검기준을 수립해야 한다[15].

자체 점검기준은 금융회사의 전자금융기반시설 특성 및 IT 환경을 고려하여 수립한다.

<표 6>은 3장에서 제시한 전자금융기반시설 취약점 분석·평가의 문제점을 개선하여 A금융회사에 적용한 자체 점검기준 수립 사례이다.

표 6. 자체 점검기준 수립 사례

Table 6. Self-Check Standard Establishment Case

통제항목		항목수
1	인력	4
2	조직	9
3	예산	2
4	건물 및 설비	19
5	전산실	17
6	단말기	4
7	전산자료	22
8	정보처리시스템	15
9	정보보호시스템	6
10	공개용웹서버	13
11	전산망	1
12	IP주소	5
13	정보기술계획	4
14	정보기술사업	4
15	정보기술계약	9
16	정보기술감리	5
17	용량·성능관리	1
18	직무분리	8
19	전산원장통제	8
20	거래통제	2
21	프로그램통제	11
22	일괄작업 통제	5
23	이용자 유의사항 공지	5
24	암호프로그램·키관리 통제	4
25	내부사용자 비밀번호 관리	8
26	정보기술 이웃소싱	14
27	정보기술부문 실태평가	3
28	전자금융거래시 준수사항	7
29	보안성심의	2
30	이용자 비밀번호 관리	11
31	취약점분석·평가	5
32	침해사고 예방	7
33	악성코드 감염방지	5
34	비상대책	17
35	재해복구센터	4
36	재해복구훈련	1
37	침해사고 대응훈련	2
38	정보기술부문· 전자금융사고 보고	8
	정보보호관리체계	277
1	UNIX서버	44
2	Windows서버	46
3	데이터베이스	10
4	보안장비	16
5	네트워크장비	14
6	PC	14
7	웹서비스	32
8	스마트폰뱅킹	19
9	홈트레이딩시스템	8
	기술적 분야 합계	203
	합계	480

정보보호관리체계 분야에서는 「전자금융감독규정」의 각 조항을 분석하여 기존 285개 항목에서 15개 항목이 추가되고, 23개 항목이 삭제되어 277개 항목으로 변경되었다.

기술적 분야에서는 주요정보통신기반시설 점검기준의 PC에 대한 '상' 점검 항목 14개를 추가하였다. 또한, <표 7>에서와 같이 증권회사 전자금융기반시설 특성인 홈트레이딩시스템(HTS; Home Trading System) 매체에 대한 점검항목 8개를 추가하였다.

표 7. 홈트레이딩시스템 점검항목
Table 7. Home Trading System Inspection Items

No	구분	점검항목
1	HTS 안정성 제고	PC용 보안프로그램에 대한 최신 업데이트 지속 실시
2		PC용 보안프로그램 임의 해제 시 HTS 이용 제한
3		이용자 PC에서의 고객정보 보호 강화
4		이용자 PC 메모리 해킹에 대한 대응
5	전자금융거래인증	이용자 인증정보 재사용
6		비밀번호 변경 시 본인 확인절차 실시 여부
7	전자금융거래 무결성	거래정보 무결성 검증
8		거래 시 소유주 확인 여부

<표 7>의 전자금융거래인증, 전자금융거래 무결성 점검항목은 전자금융거래 서비스 위협에 관한 점검항목으로 웹서비스, 스마트폰뱅킹 점검항목에도 각각 추가하였다.

5. 결 론

전자금융거래에 이용되는 전자금융기반시설은 대량의 개인정보 및 금융정보를 처리하는 중요 정보시스템으로 침해사고 발생 시 금융권뿐만 아니라 사회적으로도 큰 혼란을 야기했었다. 전자금융기반시설 취약점 분석·평가는 이러한 침해사고를 예방하고 전자금융거래의 안정성과 신뢰성을 확보하기 위한 주요한 제도이다.

본 논문에서는 금융회사에서 수행하고 있는 취약점 분석·평가 현황을 파악하고, 취약점 분석·평가의 점검기준의 문제점을 분석하여 개선방안을 제시하였다. 현행 전자금융기반시설 취약점 분석·평가 점검기준의 문제점은 정보보호관리체계 분야에서 점검기준이 현행화 및 표준화되지 않았으며, 기술적 분야에서는 전자금융거래 매체 및 서비스의 최신 위협에 대한 점검기준으로 한계점이 있고, 취약점 분석·평가 시 대상자산을 누락시킬 위험이 크다. 이러한 문제점을 해결하기 위해 정책적으로 전자금융기반시설 취약점 분석·평가 공통 점검기준 수립을 제안하였으며, 취약점 분석·평가 시 발생할 수 있는 정보자산 누락과 전자금융기반시설에 대한 일회성 관리, 부분적 보안의 한계점을 개선하기 위해 금융분야 정보보호관리체계 인증 확대 실시를 제안하였다. 아울러 금융회사 자체점검기준 사례는 전자금융기반시설 취약점 분석·평가 시 유용하게 활용되었으면 한다.

References

[1] *2017 National information security white paper*, National Intelligence Service, 2017.

[2] Financial Services Commission, *Electronic financial transactions Act*, 2017.

[3] Ministry of Science and ICT, *Enforcement decree of the act on promotion of information and communications network utilization and information protection, Etc.,* 2017.

[4] The Board of Audit and Inspection of Korea, *Information security and cyber safety management and supervision actual condition in financial sector, 2014.*

[5] I. S. Kim, U. S. Jeong, J. G. Park J. H. Lee, and *K. S. Hong, Electronic financial*

security theory, IT Forum, 2015.

[6] K. D. Park, and H. Y. Youm, *Improvements of information security level in electronic financial infrastructure*, Journal of the Korean Institute of Information Security and Cryptology. Vol. 26, No. 6. pp. 1605-1618, 2016.

[7] Financial Services Commission, *Enforcement decree of the electronic financial transactions Act,* 2017.

[8] Financial Services Commission, *Vulnerability analysis and measurement criteria in financial sector*, 2012.

[9] Ministry of Science and ICT, *Act on the protection of information and communications infrastructure*, 2017.

[10] Ministry of Science, ICT and Future Planning, *Critical network infrastructure vulnerability analysis and measurement criteria(Ministry of science, ICT and future planning notice No. 2013-37)*, 2013.

[11] Financial Security Institute, *Status of issuance of information security management system certificate(Nov. 10, 2017)*, 2017.

[12] Financial Security Institute, *Inspection criteria of information security management system in financial sector*, 2017.

[13] Korea Internet & Security Agency, *2016 ISMS certification status*, 2016.

[14] Korea Internet & Security Agency, *Information security management system certification system guide*, 2017.

[15] S. J. Park, *A study on the harmonization of public regulation and self-regulation for the constructing secure e-banking environment,* Mokpo University, 2016.

[16] *2016 financial security institute annual report*, Financial Security Institute, 2016.

전자금융기반시설 취약점 분석·평가 점검기준의 합리적 개선방안

김광배[1], 권헌영[2]

[1]*고려대학교 정보보호대학원 금융보안학과*
[2]*고려대학교 정보보호대학원*

요 약

금융회사는 전자금융거래의 안전성 및 신뢰성을 확보하기 위하여 전자금융기반시설에 대해 취약점 분석·평가를 실시하고 있다. 그러나 금융회사에서 전자금융기반시설 취약점 분석·평가 시 활용하는 금융분야 취약점 분석·평가 기준은 2012년도에 배포된 이후 업데이트되지 않았으며, 금융분야 정보공유·분석센터, 정보보호 전문서비스 기업 등 취약점 분석·평가 전문기관이 자체적으로 현행화 작업은 진행하고 있으나 표준화되어 있지 않아 금융회사에서 취약점 분석·평가 시 혼란을 야기하고 있다. 본 논문에서는 현행 전자금융기반시설 취약점 분석·평가 점검기준의 문제점에 대해 분석하고 금융회사 전자금융기반시설 특성에 맞는 합리적인 점검기준을 위한 방안과 정보보호관리체계 인증을 활용한 보완점을 제안하였다. 또한, 금융회사 자율보안체계에 따른 취약점 분석·평가 자체점검기준수립 사례를 제시하였다.

Hun Yeong Kwon is currently a Professor of Graduate School of Information Security at Korea University. He received his Ph.D, in Law from Yonsei University in 2005 and LL.M., LL.B. degree from Yonsei University. He is mainly responsible for running the Special Committee on Legal System of Open Data Strategy Council under the Prime Minister as Chairman, the Cybercommunication Academic Society as Vice President and the Korea Society

of Internet Ethics as President. His main research area is: Law and Policy on Cybersecurity, Information Security, Privacy and Personal Information Protection, E-government, Informatization and ICT

E-mail address: khy0@korea.ac.kr

Gwang Bae Kim received the bachelor's degree in the Department of Information and Communication Engineering from the Soongsil University in 2002. He is a M.S. student in Korea University Graduate School of Information Security, Seoul, Korea. He is currently in charge of vulnerability analysis and evaluation, information security certification management concerning Information Security at Shinhan Investment.

E-mail address: dreamkgb@naver.com