Journal of Digital Contents Society Vol. 15 No. 1 Feb. 2014(pp. 121-128)
http://dx.doi.org/10.9728/dcs.2014.15.1.121

사이버거래 처리 구조 진단을 기반으로 한 뱅킹시스템 정보보호 성숙도 측정방법론 연구

방기천*

요 약

SSE-CMM은 보안엔지니어링을 공학, 보증, 위험 프로세스의 3가지 요소로 나누고 있으며 정보보호 성숙도 평가 모델과 수준을 제시하고 있다. 정보보호 성숙도 측정은 취약점 진단, 위험분석 방법론을 실무 현장에서 사용할 수 있도록 종합적으로 결론을 제시한다. 사이버거래의 일반적인 서비스는 인터넷 뱅킹, 모바일 뱅킹, 텔레뱅킹 등이다. 사이버거래 처리구조의 한 종류인 뱅킹시스템 정보보호 성숙도 측정방법론 연구 목적은 기존의 취약점 진단, 위험분석 방법론을 실무현장에서 사용할 수 있도록 종합적 결론을 제시한다. 안전성과 편리성을 확보하여 이용자들이 사이버 거래를 편리하게 이용할 수 있는 환경을 구축하는 것이 사이버 거래 활성화의 핵심이다. 특히 업무현장에서 정보보호 성숙도 측정을 통한 사이버뱅킹시스템의 안전성을 확보한다면 현장의 실무처리 결과로 많은 효과가 나타날 것으로 기대한다.

키워드 : 사이버거래, 처리구조 진단, 뱅킹시스템, 정보보호 성숙도, 측정방법론

A Study of Information Security Maturity Measurement Methodology for Banking System based on Cyber-based Transaction Processing Architecture Diagnosis

Kee-Chun Bang*

Abstract

SSE-CMM for security engineering, engineering, assurance, risk is divided into three elements of the process maturity assessment model and the level of information security presented. Maturity measurement of privacy, vulnerability diagnosis and risk analysis methodologies is used in practical field for present a comprehensive conclusion. The common cyber services are internet banking, mobile banking, telephone banking and the like. Transaction structure, a kind of cyber-banking system, information security maturity of the existing measurement methodologies for research purposes, vulnerability diagnosis and risk analysis methodologies to be used in practical field present a comprehensive conclusion. To ensure safety and convenience for the user, convenient to deal with cyber environment is the key to the activation of cyber trading. Particularly by measuring the maturity of cyber banking system to ensure the safety of the practice field much effects are expected as a result.

Keywords : Cyber-based Transaction, Processing Architecture Diagnosis, Banking System, Information Security Maturity, Measurement Methodology

1. 서 론

※교신저자(Corresponding Author): Kee-Chun Bang
접수일:2014년 02월 13일, 수정일:2014년 02월 26일
완료일:2014년 02월 28일
* 남서울대학교 멀티미디어학과
Tel: +82-41-580-2191, Fax: +82-41-580-2905
email: bangkc@nsu.ac.kr

▣ 이 논문은 2013년도 남서울대학교 학술연구비 지원에 의하여 연구되었음.

정보보호관리에 대한 인식이 확산되면서 정보보호 위험분석의 수요가 증가하고 있다. 그러나 업무현장에서의 실제 적용 가능성을 심각하게 고려하지 않고 해외의 특정 방법론과 도구를 그대로 발표하고 있어 이론적 모델이 현장실무에 적용이 어려운 사례도 발견되고 있다. 따라서 업무현장 실정을 고려한 체계적 정보보호관리, 위험분석 방법론 및 도구 개발을 위해 기존의 연구(보안 관리, 위험 분석, 평가 방법, 보호프로파일, 평가 프로세스, 자산분류, 위협 및 취약성 등)를 보강 및 추가 연구할 필요가 있다. 정보시스템, 서비스 개발 조직의 개발능력 평가를 위해 SSE-CMM (System Security Engineering-Capability Maturity Model) 연구가 수행되었다. SEI (Software Engineering Institutes)의 CMM이 소프트웨어 개발업자의 개발능력을 평가하고 조직의 성숙도 수준 측정 모델인 반면 SSE-CMM은 공학, 보증, 위험 프로세스의 3가지 요소로 보안엔지니어링을 나누며 성숙도 평가 모델과 수준을 제시한다. 본 연구는 이들 기존 연구를 근간으로 사이버 거래 뱅킹시스템을 대상으로 기술적 관점에서 정보 보호수준 성숙 단계를 정의하고자 한다. 이를 연구소재로 선택한 이유는 정보보호수준 성숙단계 진단은 기존의 취약점 진단, 위험분석 방법론을 실무현장에서 사용할 수 있도록 종합적으로 결론을 제시한다는 점이다. 특히 뱅킹시스템 환경의 사이버 거래에서의 안전성 확보를 위한 대안은 현장에서 실무적용 효과가 크게 나타날 것으로 확신하기 때문이다. 논문기술 순서는 서론, 관련연구로서 사이버거래의 종류, 사이버거래 발생현황을 기술하고 이어서 사이버거래 보안위협 요소 진단, 뱅킹시스템 중심의 정보보호성숙도 측정방법론 설계, 결론의 순서이다[2][5].

2. 관련연구

2.1 정보보호성숙도 모델

정보보호관리(ISM; Information Security Management)는 조직의 정보시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무를 몇 개의 통제 분야(클래스)로 나누고 각 통제 분야 별로 다수의 통제대책(컴포넌트)으로 구성된다. 관련된 모델은 영국의 BS-7799(ISO/IEC-17799), 독일 BSI (Bundesamt Fur Sicherheit in der Informarionstechnik)의 BSI IT Baseline Protection Manual, 카네기멜론 대학의 SSE-CMM, 한국의 정보보호관리 기준 ISM 등이 있다. 정보보안을 효과적으로 유지하기 위해서 정보시스템의 보안 기능에 대한 신뢰가 전제가 되어야 한다. 정보시스템의 보안성 평가는 보안 제품/시스템에 대한 평가와 제품의 생산 공정에 대한 평가로 구분 할 수 있다. 시스템 보안공학 능력 성숙도 모델(System Security Engineering - Capability Maturity Model; SSE-CMM)은 최종 산출물에 대한 품질의 통제에서 생산 공정 품질의 통제로 초점을 옮긴다는 현대적 품질 관리의 기본적인 철학을 보안 분야에 적용하고자 개발되었다. 미국 NSA의 후원하에 카네기멜론 대학의 소프트웨어공학연구소(SEI) 주관으로 1995년에 SSE-CMM 그룹이 발족되어 1999년에 모델과 평가방법 version 2.0이 발표된바 있다. SSE-CMM은 보안시스템의 효과적인 개발을 도모하기 위한 보안 공학적 원칙들이 개발기관에 얼마나 잘 내재화되어 있는지를 평가하기 위한 방법론으로 영역(domain)과 능력(capability) 두 측면의 표준화된 실무(practice)들로 구성된다. [1][3][4].

2.2 사이버거래의 유형

▪ 온라인 뱅킹

사이버거래의 가장 일반적인 서비스는 자금이체를 기본으로 예금 조회, 자동이체 등 금융거래와 각종 금융상품을 확인할 수 있는 기능이다. 거래수단에 따라 인터넷 뱅킹, 모바일 뱅킹, 텔레뱅킹 등으로 구분할 수 있다[8].

▪ Cyber Trading(온라인 증권거래)

온라인으로 주식을 비롯한 거래소에서 거래되는 모든 금융상품을 매매할 수 있는 시스템으로 매매주문, 거래내역 확인, 금융상품 조회 등의 기능이 있다. 거래수단에 따라 Web Trading, Home Trading, Mobile Trading으로 구분된다.

▪ Cyber Insurance(온라인 보험)

인터넷으로 보험 상품에 가입하거나 보험가입

신청을 할 수 있다. 또한 보험사가 취급하는 대출신청을 할 수 있다. 인터넷과 스마트폰에 의한 거래도 수행할 수 있다. 보험 특성상 자동차보험 외에는 온라인 보험이 많이 이용되지 않는다.

▪ Cyber 카드결제
사이버 거래의 가장 많이 활용되는 형태로 인터넷 등 온라인상에서 물품을 구매하고 대가를 온라인으로 지급하는 거래이다. 판매자, 구매자, 대금결제 지불중계업자, 쇼핑몰 운영자 등이다.

2.3 사이버거래 발생 현황

사이버 거래에서 가장 많이 이용되는 종목은 인터넷 뱅킹과 증권사의 Cyber Trading, 전자상거래 결제이다. 인터넷 뱅킹의 경우 은행이 수행하는 대고객 업무인 자금이체, 계좌거래 조회, 금융상품 조회 등 일반 은행 업무를 모두 처리할 수 있어 높은 이용률을 보인다. 2011년 기준 약 49억 건에 1경 7000조원이 거래되었다. 최근 스마트폰 뱅킹도 폭발적으로 거래 증가되어 일평균 스마트폰 뱅킹이용실적은 '10년 91만 건, 467억 원에서 '12년 2/4분기 1,182만 건, 7,900억 원으로 대폭 증가하였다[8].

<표 1> 전자금융거래 실적(단위:천건,십억원,%)

Year		2008	2009	2010	2011
Bank	Number of	4,302,658(79.9)	4,598,339(79.9)	4,727,308(78.6)	4,919,087(80.0)
	Amount of money	11,113,645(23.2)	13,540,262(26.1)	15,765,336(28.6)	17,043,581(28.1)
Securities	Number of	1,014,773(77.5)	1,187,471(77.6)	1,138,502(71.6)	
	Amount of money	6,078,487(57.1)	7,258,162(55.9)	10,533,939(44.9)	14,459,704(51.1)
Card	Number of	276,467(6.4)	312,291(6.1)	359,635(6.2)	415,219(5.9)
	Amount of money	84,766(20.8)	83,443(19.8)	70,690(15.2)	76,050(14.0)
Insurance	Number of	226(0.3)	222(0.3)	1,562(1.6)	2,797(3.2)
	Amount of money	93(0.1)	74(0.1)	214(0.6)	389(1.2)

<Table 1> E-banking Performance
* Source: Financial Supervisory Service(FSS)

3. 사이버거래 보안위협 요소 진단

3.1 사이버거래 뱅킹시스템 구조

사이버 거래는 인터넷을 비롯한 통신망 상에서 발생되는 모든 재화 및 용역의 거래와 이에 수반되는 지급결제이다. 사이버 거래의 종류는 자금이체, 자금결제, 각종 전자계약 등이 있다. 구매자가 인터넷 쇼핑몰과 같은 판매자의 사이트에서 물품을 구매하고, 이때 발생하는 물품대금을 제3자인 전자금융업자가 구매자로 부터 받아 판매자에게 지급하는 흐름도이다. 사이버 거래 뱅킹시스템 구조는 시스템구조, 기관구조, 처리구조로 정리된다.

▪ 시스템구조 : 5개 이상의 네트워크 도메인 구간으로 뱅킹시스템 구성

▪ 기관구조 : 5개 이상 뱅킹관련 기관 연동

▪ 처리구조 : 뱅킹서비스, 업무구조, 기술구조, 데이터처리구조, 사용구조

▪ 기술구조 : 네트워크, 서버, 운영체제, 데이터, 프로그램, 통신프로토콜, 단말시스템

3.2 사이버거래 보안사고 발생 실태

사이버 거래에서 사용되는 개인정보는 침해신고 상담건수가 해마다 증가하여 2012년도에는 166,801건으로 전년 대비 약 26.7% 증가하였다. 주민등록 번호 등 타인 정보의 훼손·침해 ·도용에 관한 침해 신고가 139,724건(전년대비 약 52% 증가)으로 가장 많았으며(전체의 83.8% 차지), 그 다음으로 기술적 ·관리적 조치 미비 관한 침해신고가 3,855건(전년대비 약 65% 감소)로 나타나고 있다[6]. 무엇보다 주민등록번호 등 민감한 개인정보에 대한 누출이 큰 비중을 차지하고 있어 그로 인한 물적, 인적 피해가 발생되고 있다. 2011년 개인정보침해 관련 접수민원 122,215건 중에서 119,659건은 권리, 법령, 유관기관 안내 등으로 해결된 단순 상담 민원이었으며, 이중 주민등록 번호 등 타인정보 침해· 훼손 ·도용이 67,094로 제일 비중이 높았다. 신고 ·처리된 2,556건은 사업자에 대한 법위반 여부 조사 등 사실 확인 조사를 거쳐 <표 2>와 같이 처리되었다[9].

<표 2> 최근 5년 개인정보 침해신고 현황
(단위:건)

Division	2007	2008	2009	2010	2011
Solution and charging	289	445	1,495	1,162	2,107
Adjust disputes	90	172	145	191	126
law enforcement agencies	18	25	16	5	13
Administration	31	37	41	10	20
No violation of law	53	62	10	47	54
Application withdrawn	211	72	103	126	80
Not investigated	155	175	329	247	156
Sum	847	988	2,139	1,788	2,556

<Table 2> Privacy Complaint Past Five Years (Unit: case) *Source : Korea Internet & Security Agency (KISA) Privacy Complaint Center

4. 뱅킹시스템 중심의 정보보호 성숙도 측정 방법론

4.1 측정 단계별 수행방법

본 연구는 위험분석 방법론을 토대로 뱅킹시스템을 중심으로 사이버거래에서의 보안관리 수행과정으로서 정보자산, 위협, 취약성, 대응책을 중심으로 대상 정보 환경의 위험을 측정하는 절차와 기술을 제시한다.

1) 위협평가 : 정보시스템 자산에 대한 내외부로부터의 보안 침해위협을 점검, 평가, 모의침투, 보안체크리스트 점검

2) 취약점평가 : 정보보호취약점 평가 운용중인 정보시스템 자산이 위험에 노출될 수 있는 가능성과 요소 수준 점검

3) 보안체계진단 : 기술적 정보보호 체계 진단 정보시스템에 가해지는 정보보호침해 위험을 회피 또는 감소시킬 수 있는 기술적 분야의 대응체계 진단.

4) 위험도측정 : 자산, 위협, 취약점, 보안체계 단계산정, 위험도를 연계 분석하여 현재의 위험수준 평가.

5) 보안체계 진단 : 기존의 보안대책이 위험도를 얼마나 축소시키는지에 대한 수준 평가.

6) 정보보호성숙도 수준측정 : 1)-5) 이상의 산출 결과를 바탕으로 정보보호성숙도 수준을 종합적 평가.

<표 3> 단계별 측정 수행방법

Step	Threat Assessment	Vulnerability Assessment	Security System Diagnosis	Risk measurement	Security System Diagnosis	Level of information security measures
Perform Contents	•Information Security Threat Assessment	•Information Protection Vulnerability Assessment •Information Security Management Vulnerability Assessment	•Technical Information Security System Diagnosis	•Risk Calculation	•Diagnostic effectiveness of security measures	•Information Security on the basis of the measurement results derived
Perform How	•simulated penetration • security checklist •Development of measurement methods	•Use the measurement tool •security checklist •a visit •discussion •Development of measurement methods	•Development of protection system inspection	•assets, threats, Vulnerabilities, and security system Calculated in step •Development of risk calculation method	•Estimation of functional relationships between risk and security system	•Privacy Level of development of measurement methods •5 steps of maturity

<Table 3> Step-by-step How to Perform Measurements

4.2 사이버 구간별 처리업무

본 논문에서 사용하는 금융정보 뱅킹시스템 구간은 고객사용자구간, 네트워킹구간, 웹서비스구간, 내부사용자구간으로 구분할 수 있다. 정보시스템 트래픽 구간별 도메인 분류는 보안기술 적용이 가능하도록 네트워크 영역을 구분한다. 구분 기준은 보안기술의 적용이 필요한 영역, 트래픽 경로와 트래픽 성격이 타 도메인과 차별화가 가능한 영역, 보안기술 적용시 타 영역의 보안기능으로 기능 중복이 발생치 않는 영역에 따라 도메인을 설정하는 기준은 세부적 단계로 적용될 수 있지만 보안기능 중복이 발생하고 응답지연과 필요이상 네트워크 구조 복잡을 초래하게 된다. 트래픽정보 유통과정은 정보입력 -> 근거리 무선 전송 -> 호스트로 전송 -> 트래픽 분석 -> 처리과정으로 연계된다[10].

1)인터넷 통신망구역

오픈 프로토콜 TCP/IP 통신프로토콜을 사용하는 관계로 Line Tapping, 중계기관, 업무 담당자에 의하여 송・수신되는 정보의 노출이 쉽게 이루어 질 수 있는 문제가 있다.

2)인터넷 뱅킹시스템 구간

대부분의 금융회사는 동 구간에서 암·복호화가 실행되고 있어 내부 지원에 의한 정보 유출 취약점이 있다. 또한 방화벽에만 의존하고 있어 외부로부터의 접근이 가능함에 따라 해킹에 의한 정보유출 가능성도 높은 구간이나, 고객 원장 등 주요정보는 저장되어 있지 않다.

3)은행호스트 구간

고객원장, 거래기록, 개인정보 등의 중요 정보가 집중되어 있고, 프로그램의 개발 등의 사유로 다수의 내부 직원의 접근이 필요함에 따라 이들의 정보 유출 문제가 가장 심각한 부분이다.

4) 사용자구간

고객이 인터넷뱅킹을 위해 사용하는 구간으로서 정보보호취약성이 노출될 위험이 높은 구간이다. 외부로부터의 접근이 용이함에 따라 해킹에 의한 정보 유출 가능성도 높은 구간이다.

<표 4> 사이버거래 처리구간별 처리업무

Systems section		Guest User Area	Networking section	Web Services Section	servers section	Internal User Area
System Configuring resources		.Customer terminal .Customer Network	.Public .Communication Equipment	.Security Equipment . Web Server .Application Server	.Security Equipment . DB server . The account server	. For internal use Terminal
Perform Business	Customer	.Customer's business connections		. User Authentication . The access control	.Banking service	
	Finance Company	Electron Finance	Sending and receiving data	.The input data processing	.Banking services processing . Data Processing .Security Management	.Internal business .Treatment .Security Management
	Electron Finance		Sending and receiving data	.E-banking services		
	Certification Organ			. User Authentication		

<Table 4> Cyber-processing Tasks by Section

4.3 뱅킹시스템 구간별 위협요소 진단

측정대상 금융기관에서 실제 발생되었던 위협 중 데이터채집이 가능한 분야, 측정대상 금융 기관에서 실제 발생되었던 위협 중 발생빈도수 조사가 가능한 분야를 채집한다. 위협평가와 취약점평가간 연계 평가가 가능한 분야로서 현실적으로 금융업무 현장에서 정보보호분야 금융사고 실적 통계를 관리하지 않거나 금융 사고에 대한 엄격한 보안을 유지하므로 이 요건을 충족시키는 분야 데이터를 채집하기 용이하지 않다. 따라서 본 연구에서는 평가 측정방법론을 제시하고 채택방법은 각 업무 현장에서 선택적으로 적용토록 한다.

<표 5> 뱅킹시스템 처리 구간별 위협요소

Section	Threats	Check items threat
User Area	Data theft Illegal S / W running	Certificate management Inputs hacking attacks Security line Tone generation touch screen
Network segment	Data taps Data modulation	Wiretapping (Telephone banking, ATMs)
Web Services Section	Input data errors Lack of access control Lack of rights management Certification vulnerable	Exposed to the external lookup information Exposure security card password Non-financial companies electronic financial services E-banking fraud
Server segment	Lack of security settings Lack of Patch Management Weak management server	Internal control, information management,
Internal network	Lack of access control	Vulnerable to identity verification procedures Lack of customer notification management Vulnerable customers consent

<Table 5> Banking System by Processing Sections Threats

4.4 5개영역 보안위험도 평가의 틀

시스템 상에서 취약점점검 분야는 네트워크 구조를 기준으로 네트워크, 서버, 운영체제, 데이터, 프로그램, 통신프로토콜, 단말시스템으로 구분된다. 취약점 점검방법은 수동점검과 자동점검으로 구성된다. 자동점검은 실제상황 점검, 상세점검, 특정 취약점 점검시 사용한다. 수동점검은 점검대상 시스템을 대상으로 체크리스트 점검을 실시한다. 수동점검은 전반적인 점검으로서 자동점검에 포함되지 못하는 항목을 점검한다. 단기점검이며, 핵심 단일종목을 중점 점검 및 직접 조사 방법이다. 보안위험도 평가는 보안위험도 평가체계 설계에 제시된 절차에 의거 정량적 평가를 실시하며, 위협강도, 위협 발생 빈도, 위협등급 평가, 대책평가를 실시하고 자산,

취약점, 위협 등급을 산정한 결과를 대책과 비교하여 마지막으로 위험수준을 산출한다. 위협영향 평가는 위협평가 방법에 의해 결정되며, 각 단계의 세부점수는 정보자산에 대한 피해 범위(금액)로 차등을 둔다.

4.5 위험도 산정

4.5.1 위험도 산출식

현재 운용중인 정보시스템 자산이 진단 당시의 환경에서 위협, 취약성 진단결과 어느 정도 위험 수준을 보여주고 있는가를 산정한다. 위협평가 , 취약성평가, 보안체계평가 결과를 연계 산출한다. 위험도 산출 공식은 위협 = 위협 영향 * 위협발생빈도(T)이며 취약성 = 자산이 가지고 있는 정보보호 항목 약점의 수치(V)이다. 자산가치(A)는 정보자산이 가지고 있는 계량 수치이다. 위험도 = 위협, 취약성, 자산 가치 승산에 의한 예상손실수치(ALE : Annual Loss Exposure) =T*V*A이다.

1) 자산가치 = 자산의 경제적 가치
2) 취약성 = 자산이 가지고 있는 보안약점
3) 위협강도 = 위협영향 수준
4) 위협발생빈도 = 일정기간 위협 발생횟수
5) 위협수준 = 위협강도*위협발생빈도
6) 위험도 = 위협수준과 보안대책 관계

<표 6> 산출결과에 의한 위험도 등급

Division	VL	L	M	H	VH
Risk Rating	1-20	21-40	41-60	61-80	81-100

<Table 6> Severity Rating by the Calculation Results

4.5.2 영역별 가중치 부여

가중치의 개념은 평가지표의 동일 분류내 척도를 산출한 후 각 지표의 중요도를 평가하여 중요도별로 가중되는 값을 부여한다. 가중치는 현장업무 전문가 집단에 의한 진단평가와 협의 결과에 따라 적용여부와 대상, 적용수준을 결정한다(델파이법의 취지). 가중치 유형은 종합 평가용 가중치, 단일가중치 = 자산기준, 업무 기준, 다중가중치 = 자산기준, 업무기준, 프로세스기준, 보안기능 기준 중 복수의 기준 합산 또는 승산 등 이다. 가중치 값은 동일그룹 부여 대상 전체를 100% 범위내 값을 항목에 상대적 배분한다. 본 연구에서 제시하는 가중치 범위는 일반 뱅킹 업무를 기준으로 예시 사례이며 실제산정은 현장 업무 성격, 규모, 프로세스 단계, 프로세스 중요도, 평가의 시기적 특성을 기준으로 재산정해야 한다.

<표 7> 보안수준평가용 가중점수산출 메트릭스

Importance of evaluation functions				Information Security Level Evaluation					
Rating	Weighted Score	Item Number	Function Score	VL	L	M	H	VH	Subtotal
				0.2	0.4	0.6	0.8	1.0	Weighted Score

<Table 7> Weighted Scores Calculated Level of Security Metrics for Evaluation

4.6 성숙도수준 등급 결정 기준

산출된 정보보호지수를 활용하여 정보보호 수준의 위치를 판단하기 위한 정보보호수준 단계를 정의한다. 기존 연구된 정보보호수준 성숙단계를 참고하였으며, 그 구성 체계를 같이 하도록 하였다. 정보화가 진전될수록 정보보호수준 또한 진전되어야 한다.

▪ 미추진 단계 : 정보보호 활동이 구체적으로 추진되지 않는 단계이다. 정보보호 인식이 부족하며, 정보보호 기술도입이 이루어지지 않는다.

▪ 초기단계 : 바이러스 백신 등 기본적인 정보보호 기술이 도입되어, 기본적 보호기능 만 수행.

▪ 발전단계: 기업 구성원이 정보보호에 대한 관심이 높아지며, 보안기술 도입, 적용

▪ 성숙단계 : 정보보호 인식이 높은 수준으로 성숙되고 정보보호 기술로 인해 체계적 보안

▪ 고도화단계 : 정보보호 정책이 경영전략과 함께 추진되며, 정보보호 조직이 독립되어 운영되는 수준. 정보보호성숙도수준 등급판정은 종합의견으로 정보보호성숙도수준 등급 설정 기준을 5개단계로 결정한다. <표 8>은 5개 단계의 정보보호 성숙도 수준설정과 성숙도 수준별 점수범

위 설정을 보여준다.

<표 8> 정보보호성숙도수준 평가표

Rated areas		Measurement Index Score	Weighted Score	Evaluation Score	Maturity level rating				
					Not promoted	Beginning	Development	Maturity	Advancement
					1-20	21-40	41-60	61-80	81-100
Vulnerability Retention	Network								
	Operating System								
	Database								
	Applications								
	Client								
	Security System								
	Subtotal								
Technology Security System	Privacy Policy								
	Incident Response								
	Emergency Planning								
	Infrastructure Holdings								
	Security Management								
	Risk Management								
Technology Security Implementation	Intermittent vulnerability								
	Network								
	Operating System								
	Database								
	Applications								
	Client								
	Security System								
	Subtotal								

<Table 8> Information Security Maturity Level Rating Tables

5. 결 론

사이버 거래는 향후 스마트폰과 전자상거래, B2C의 활성화로 그 증가 폭은 더욱 빠르고 광범위하게 진행될 것이다. 위험을 방지하기 위하여 각종 보호수단을 사용하면 시스템을 제공하는 금융회사나 사업자들은 그만큼의 인력과 비용이 투자되고, 이용자의 입장에서는 각종 보안 시스템을 설치하고 비밀 번호, 공인 인증서, 전화인증번호, OTP 등 복잡한 본인확인 수단을 사용함에 따라 사용의 편리성이 떨어지게 된다. 따라서 안전성과 편리성을 조화하여 이용자들이 가장 편리하게 이용할 수 있는 사이버 거래 환경을 구축하는 것이 사이버 거래 활성화의 핵심이라 할 수 있다. 사이버거래 처리구조 진단을 기반으로 한 뱅킹시스템 정보보호 성숙도 측정 방법론 연구를 연구소재로 선택한 이유는 정보보호수준 성숙단계 진단이 기존의 취약점 진단, 위험분석 방법론을 실무현장에서 사용할 수 있도록 종합적으로 결론을 제시한다는 점이다. 특히 뱅킹시스템 환경의 사이버 거래에서 안전성 확보를 위한 대안 도출은 실무적용 효과가 크게 나타날 것으로 확신하기 때문이다. 본 논문으로 연구하는 방법론은 향후 운영 업무에 참고 되기를 기대한다.

References

[1] S. C. Noh, A Study of Evaluation Methodology of Maturity Level for Technical Security Models Based on SSE-CMM, Sep. 2012.

[2] CMM http://www.freesoft.or.kr/osd/html/software/introduction3.htm

[3] SSE-CMM Org http://www.sse-cmm. org/

[4] CCRA(Arrangement on the Recognition of Common Criteria Certificates) http://www.commoncriteria.org.

[5] SSE-CMM, “Project, Systems Security Engineering Capability Maturity Model (SSE-CMM) - Model Description Document”, V.2, http://www.sse-cmm.org, Apr. 1999.

[6] CC, Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, Aug. 1999.

[7] British Standards Institution(BSI), “BS-7799”, 1999.

[8] I. S. Kim, Korea University, Cyber Safety Measures of Trading, May 2013.

[9] H. S. Lee, Measures of Privacy in Cyberspace, May 2013.

[10] S. C. Noh, "Assurance Method of High Availability in Information Security Infrastructure System", Springer LNCS 3794, Dec. 2005.

방 기 천

1981: 서울대학교 전자공학과 (학사)
1988: 성균관대학교 정보처리학 (석사)
1996: 성균관대학교 전산통계학 (박사)

1984~1995: MBC 기술연구소
1995~현재: 남서울대학교 멀티미디어학과 교수
관심분야: 멀티미디어콘텐츠, 멀티미디어 응용, 웹기반 정보시스템 등