Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.729

안전한 전자금융거래를 위한 보안등급 기준마련 및 사례연구

장 길 영,† 김 인 석‡
고려대학교 정보보호대학원

Establishing Security Level Standards and Case Studies for Safe Electronic Financial Transactions

Kil-Young Jang,† In-Seok Kim‡
Korea University, Graduate School of Information Security

요 약

2015년 6월 24일 금융위원회에서는 보안성심의를 전면 폐지하고, 자체 보안성심의로 보안 수준 점검 의무를 갈음한다고 하였다. 금융기관의 보안담당자는 안전한 전자금융거래를 위해 보안성 검토를 할 경우에 CIA 보안등급을 기반으로 보안성심의를 수행하고 있다. 그러나 최근 인터넷,모바일 전자금융거래의 보안성 검토는 좀 더 깊이가 필요한 경우, 별도의 프로세스를 점검하거나 신기술, 보안 관련 자료를 참고하여 보안성심의를 수행하고 있다.

본 논문은 CIA 기반의 보안등급에 인증과 개인정보보호 지표를 추가한 CIAAP 보안등급을 제안하며 특히, 전자금융거래의 보안성 검토를 진행할 때 본 CIAAP 보안등급을 참고하여 개인정보보호 영역의 검토가 누락되지 않고, 강화된 인증 관련 지표의 추가를 통한 보안성 검토가 필요함을 제안한다.

ABSTRACT

On June 24, 2015, the Financial Services Commission (Financial Services Commission) completely abolished the security review process, and said that it would substitute self-security review obligations with self-security reviews.

Security officials at financial institutions conduct security reviews based on CIA security grade when they conduct security reviews for secure electronic financial transactions. However, the recent security review for Internet and mobile electronic financial transactions has carried out a security review, either by checking separate processes or by referring to new technologies and data related to security.

This paper proposes the CIAAP security gradesl with the addition of certification and privacy protection indicators to the CIA based security grades, especially through the security review of electronic financial transactions.

Keywords: Certificate, Electronic Financial Transactions, Authentication, Privacy Protection, Security Review

I. 서 론

1.1 연구배경

방송통신위원회 보도자료(2010.5.31), '전자금융거래 인증방법의 안전성 가이드라인'에 따르면, 금융감독기관은 '금융기관과 전자금융업자가 전자금융거래에 적합한 인증방법을 그에 관한 기술 중립성의 원칙에 입각해 자율적으로 선택할 수 있도록 해야 한다'고 발표하였다[1]. 아울러 금융기관과 전자금융업

Received(03. 28. 2018), Modified(05. 14. 2018), Accepted(05. 16. 2018)

† 주저자, kyjang93@gmail.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

자는 전자금융거래 이용자가 안전하고 편리하게 전자금융 서비스에 접근할 수 있도록 전자금융거래별 보안 위험 요인에 대한 분석에 따라 다양한 인증방법을 제공할 수 있도록 하고 있다. 여기서 중요한 점은 거래내역의 부인방지 기능이 예전과 달리 필수가 아니라 선택적으로 적용할 수 있도록 했다는 것이고, 따라서 금융기관 또는 전자금융업자는 이용자인증, 서버인증 및 통신채널 암호화의 요건을 갖춘 경우, 거래한도를 정하여 인증방법평가를 받아 금융거래를 할 수 있게 되었다는 것을 의미한다[1].

한국은행의 '2017. 3/4분기 국내 인터넷뱅킹서비스 이용현황' 보도자료를 보면, 2017년 9월 말 현재 국내 금융기관에 등록된 인터넷뱅킹(스마트폰뱅킹 포함) 고객수는 1억 3,246만명으로 전분기말 대비 4.3% 증가하였다[2].

스마트폰 이용 확산 추세에 따라 인터넷전문은행의 신규(카카오뱅크) 출범등에 따라 스마트폰뱅킹 실제 이용고객수는 5,666만명으로 전분기말 대비 11.7% 증가함에 따라 2015년 3월말(11.9% 증가) 이후 처음으로 두 자리수 증가율을 기록했다.

이러한 방송통신위원회의 인증방법에 대한 규제완화와 인터넷뱅킹의 이용자 확대에 힘입어 그에 따른 전자금융사고가 증가하였다.

2015년 11월 에너지경제신문에는, 금융보안규제의 완화로 타인의 카드정보를 도용한 부정사용률이 2015년 기준 3년 사이 5배나 늘어난 것으로 나타났다[3].

여신금융협회 산하 여신금융연구소 임윤화 연구원이 발표한 '유형별 카드 부정 사용 현황과 향후 보안과제 및 대응방향'에 따르면, 카드정보 도용 부정사용률은 3년 새 5배나 급증했다[4].

국내의 카드정보 도용 부정사용률이 급증하게 된 이유는 인터넷시장 성장에 따른 온라인 카드사용 확대와 간편결제 도입 등을 들 수 있다.

금융위원회의 'IT·금융 융합 지원방안' 보도자료(2015.1.27)에 따르면, 정부와 금융위원회 등 정책담당 부처들은 핀테크를 새로운 기회로 보고 이를 성장 동력 육성 분야로 활성화시키기 위해 다양한 정책들을 발표하였다. 이는 그동안 온라인 금융을 안전성 중심으로 운영하면서 발생한 각종 보안대책이 핀테크를 활성화 시키는데 걸림돌이 되고 있다고 판단한 것이다[5].

정부의 공인인증서 의무 사용 규제가 폐지되었음에도 불구하고 인터넷 서비스 이용자들은 인증 수단으로 여전히 공인인증서를 가장 선호하는 것으로 나타났다. 한편, 공인인증서를 자주 이용하는 분야는 금융업무이며 보관하는 저장매체는 PC하드디스크를 가장 많이 사용하고 있는 것으로 드러났다[6].

인터넷 서비스 인증 수단으로 응답자의 82.2%(복수응답)는 공인인증서를 선호하고 있는 것으로 나타났다. 공인인증서 다음으로 자주 이용하는 인증 수단은 ID/PW(33.2%), OTP(27.8%), E-Mail 및 SNS 계정(21.2%), 생체인증(16.6%) 방식의 순서였고 응답자들은 공인인증서 방식에 대해서는 '매년 갱신 및 재등록해야 한다', ID/PW 방식에 대해서는 '사용처 별로 ID/PW 기억하기가 어렵다.' OTP는 '휴대하기가 번거롭다.' E-Mail 및 SNS 계정 방식은 '보안이 취약하다.' 생체인증은 특히 여성층에서 '생체정보 노출에 대해 불안하다.'고 각 인증 수단의 불편함을 답했다[6].

특이할 만한 사항은 공인인증서 보안의 필수 요소인 저장매체로 USB메모리(56.0%)를 가장 안전하다고 선택, 기술적으로는 보안토큰(USB형 보안토큰, 스마트폰USIM, 스마트 카드 IC칩 등)이 가장 안전하다고 증명된 사실에 대해 일반 사용자들은 사실과 다르거나 올바른 정보를 제공받지 못한다고 할 수 있다. 또한 응답자 57.0%는 가장 안전하지 않은 PC하드디스크에 공인인증서를 보관하고 있다는 점에서 공인인증서 관리에 대한 인식 및 환경 개선이 필요해 보였다[6].

신규 인증 수단의 선택 기준으로 안전성(67.2%, 복수응답)과 편리성(54.0%, 복수응답) 을 선택하고 있으며 안전성과 편리성이 충족되는 서비스 인증 수단에 대해서는 비용을 지불하겠다는 응답도 47.4%로 나타났다. 비용 수준에 대해서는 1천원 이하가 가장 많았다. 결국 정보보안을 위한 필수 요소인 인터넷 서비스 인증수단은 불편함이 개선되고 안전을 위해 일부 비용이 발생한다 하더라도 공인인증서 기반의 인증 서비스가 최선이라는 답을 설문 조사 결과를 통해 알 수 있었다[6].

1.2 연구목적

인터넷을 이용하는 전자금융서비스는 보안문제가 뒤따를 수 밖에 없다. 그에 따른 적절한 보안대책을 마련하고 보안등급을 설정하는 것은 반드시 필요하다. 스마트폰을 이용한 전자금융서비스가 66.2%를 상회하는 만큼 보안대책 점검에 만전을 기하고 보안

등급 설정을 통해 보안의 중요성 기준등급을 마련하여 인증등급 부여와 함께 항상 관심을 갖고 보안관련 주의를 다하는 자세가 필요하다고 할 것이다.

1.3 CIAAP 보안등급 제안 이유

보안의 3요소는 흔히 CIA를 말한다. 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availablility) 이다. 정보보안은 개인과 기업에 영향을 미치며 거기에서 다루고 있는 개인정보, 금융정보와 같은 중요정보를 보호해야 한다. CIA Triad는 정보보안 조치에 포함되어야 하는 근본적인 목표를 보여주고 있다[7].

그런데 중요하게 다루어야 하는 전자금융거래에서는 특히 정당한 사용자 또는 권한이 부여된 그룹에게만 해당 거래를 허용해 주어야 하는 경우가 발생한다. 즉, 사용자를 인증(Authentication)하여 정당한 권한이 부여된 사용자인지를 확인하는 절차가 필요하다. 또한, 위에서 언급한 중요정보를 보호해야 하는데 비중요정보와 동일한 보안등급을 적용하거나, 일괄적인 높은 수준의 보안을 적용하는 것은 정보보안의 누락 또는 오남용의 우려가 있는 만큼 반드시 보안등급에 추가하여 중요도를 따져볼 필요가 있다.

Fig. 1. The goals of the CIA Triad are confidentiality, integrity and availability. These goals are used for information security solutions. (Image: Anthony Henderson)

II. 관련 연구

2.1 인증기술

2.1.1 배경

인터넷 기반의 전자금융은 그 특징이 비대면 거래이기 때문에 접속하는 이용자를 올바로 확인해야 하고,그렇지 못하면 타인에 의한 부정거래를 막을 수 없어 전자금융 사고가 발생할 수 밖에 없다[8]. 또한, 전자금융 이용시 필수 입력정보인 개인정보 및 금융거래정보 등의 민감정보가 온라인으로 송수신되기 때문에 타인에게 노출되지 않도록 올바른 이용자를 확인하는 전자금융 인증기술은 전자금융의 신뢰성을 확보하는 가장 중요한 수단이라 할 수 있다[8].

2.1.2 인증기술의 정의

인증기술(Authentication technique)은 원격지에 있는 사용자의 신원확인(Identification) 기능과 송수신자간 전송되는 거래내역의 무결성(Integrity)을 보장하는 거래인증(Transaction Authentica -tion) 기능의 두가지 의미를 모두 내포하고 있다. 특히, 전자금융에서 인증기술은 주로 거래내역의 무결성을 보장하여 부정거래를 방지하기 위해 사용되기도 한다. 부가적으로 사용자 또는 전자금융서버의 전자금융 이용사실에 대한 부인방지기능을 제공하여 전자금융의 신뢰성을 보장하는 기능을 포함할 수 있다[8].

2.1.3 인증기술의 분류

전자금융에 사용할 수 있는 인증기술을 인증팩터(Authentication Factor) 관점으로 분류한다면, Table 1.과 같이 '지식기반'(What you know),'소지기반'(What you have), '특징기반'(What you are)으로 분류하는 것이 일반적이다[8].

이 밖에도 개인간의 비밀번호 입력패턴 차이, 전

Table 1. Authentication Factor Classification

Classification	Content	Example
Knowledge-Base (What you know)	Knowledge base you know	ID/PASSWORD, Pre-registered question and answer method, etc
Possession-Base (What you have)	Based on authentication media you own	OTP Generator, HSM, Security card, Smart card etc.
Feature- Base (What you are)	Bioinformatics	Fingerprints, veins, iris, etc.

자적인 서명필체 등을 이용하는 인증팩터를 '행동기반'(What you do)으로 분류하기도 하며, 사용자의 전자금융 이용패턴, 이용위치 등 사용자의 알려진 사실에 기반한 인증팩터를 '알려진 사실 기반'(What known about you)으로 세분화하여 분류하기도 하지만 아직까지는 일부에서만 적용하여 분류하고 있다[8].

2.2 전자인증 관련 표준

2.2.1 TTAK.KO-12.0244

TTAK.KO-12.0244(전자거래 단계별 위험수준에 대한 인증서비스 지침)에서는 피싱·파밍 등 전자거래의 보안위협이 증가함에 따라 단일인증으로는 보안위협에 대응하는데 한계가 존재하기 때문에 전자거래의 인증단계를 분류하고 각 계층별 거래위험에 따라 보안성을 보장하기 위한 계층화된 인증서비스 지침을 정의하고 있다[11].

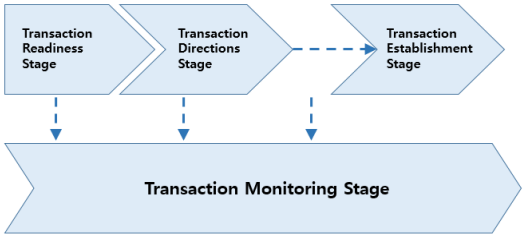

Fig. 2. Certification for Electronic Transactions Concept Map

2.2.2 TTAK.KO-12.0247

TTAK.KO-12.0247(전자거래 보증수준별 인증방법 요구사항)에서는 인증방법의 등급별 관리 요구사항을 제시하여 서비스 환경별 적합한 인증방법을 선택할 수 있는 지침을 제공하는 것을 목적으로 한다[12]. 인증방법의 보증수준을 정의하고 각 보증등급별 요구사항을 정의한다. 또한 각 인증방법에 대한 보증수준을 산정하는 기준을 제시하여 각 서비스 환경별로 적합한 인증방법을 적용하는 지침을 제공하였다[12].

2.2.3 TTAK.KO-12.0248

TTAK.KO-12.0248(국내환경에 적합한 실체인증 보증 프레임워크)에서는 스마트 환경에 적용할 수 있는 인증보증 프레임워크를 제시하며 이를 통해 전자

정부, 전자거래 등 다양한 온라인 인증 서비스의 수준 향상을 도모한다[13].

실체 인증 보증 프레임워크는 실체등록단계, 인증과정에서 이용되는 크리덴셜을 발행하고 관리하는 크리덴셜 관리단계, 실체의 신원을 인증하는 단계로 구성되는 기술적 사항에 신뢰수준을 부여하고 법 준수 및 계약준수, 정보보호 관리체계 및 감사 등의 요구사항으로 관리적 사항에 신뢰수준을 부여한다[10].

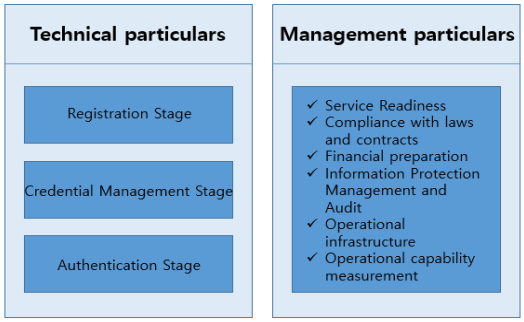

Fig. 3. Entity Authentication Assurance Framework

III. 전자 거래 서비스별 인증수단

3.1 전자 거래 서비스별 적합한 인증수단 도입을 위한 가이드라인

3.1.1 전자 거래 서비스 보증수준별 가이드라인

세계적으로 스마트기기 사용이 대중화 되면서 스마트폰이나 태블릿PC 등의 다양한 환경변화가 이루어졌다. 이런 환경은 기존의 대면 거래환경에서 비대면의 거래환경으로 거래환경의 변화를 가져왔다. 따라서 대면 거래환경 뿐 아니라 비대면 거래환경에서의 다양한 보안위협이 존재하고, 이에 대응하기 위한 인증방법의 등급을 정의할 필요성이 있다[10].

미국국립표준연구소(National Institute of Standards and Technology, NIST)에서는 지난 2013년도 전자 인증 가이드라인(SP 800-63-2,

Electronic Authentication Guideline)을 발표하고 인증방법에 대한 요구사항을 정의한 가이드라인을 제공하였다. 최근에는 앞서 제공한 가이드라인을 실질적으로 업데이트하고 구조를 재조정하는 움직임으로 SP 800-63-3, Digital Authenti cation Guideline 버전을 드래프트 하고 있다(2016년 9월 드래프트 문서 갱신). 이외에도 ITU-T X.1254와 ISO/IEC 29115는 객체인증 보증 프레임워크를 제정하여 인증방법에 대한 안전성 평가기준을 제공하고 있다[10].

한국정보통신기술협회(Telecommunications Technology Association, TTA)에서는 2014년도 TTAK.KO-12.0247(전자거래 보증수준별 인증방법 요구사항)을 제정하였다.

크리덴셜 관리단계의 보증수준별 요구사항과 인증기술의 강도별 보증수준 요구사항, 등록단계의 강도별 보증수준 요구사항을 정의한다. 크리덴셜이란 신원이나 자격을 주장하면서 증거로 제출된 데이터집합을 말하며 인증에 사용되는 인증정보 또는 인증정보를 생성하기 위한 비밀정보 등을 의미한다[10]

인증에 사용되는 크리덴셜은 생성, 발급, 이용등록(활성화), 저장, 폐기, 재발급, 기록 관리의 절차를 갖는다.

같은 인증기술이라도 지원되는 기능에 따라 보증수준이 다르기 때문에 인증방법에 따라 보증수준을 만족하기 위해서는 AR-1부터 AR-11의 "인증정보 강도별 보증수준 요구사항" 을 만족해야 한다.

그리고 인증수단의 등록단계의 보안강도는 신원확인을 위한 정보의 신뢰성과 신원 확인방법에 의해 결정된다[10].

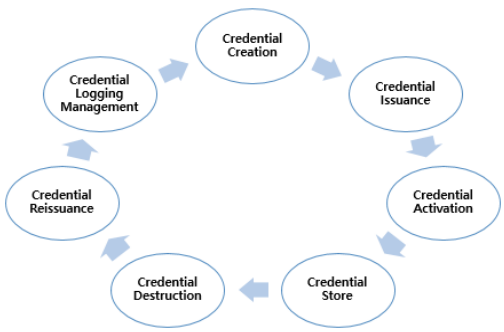

Fig. 4. Credential Management Lifecycle

Table 2. Requirements by certified technology strength

Authentication Information			Assurance Level(1 Level: High Level)		
			Level 1	Level 2	Level 3
Knowledge	Password		X		AR-1
	Question and answer authentication		X		AR-1
	Image Authentication		X		AR-1
Possession	OTP Token	Security Card	X	AR-3	AR-1
		Password List	X	AR-3	AR-1
		S/W OTP Generator	X	AR-4	AR-1
		H/W OTP Generator	AR-6	AR-5	√
		Transaction Signature S/W OTP	X	AR-4	AR-1
		Transaction Signature H/W OTP	AR-6	AR-5	√
	PKI Token	S/WCertificate	X	AR-7	√
		H/W Security Token	AR-8	√	√
		Transaction Signature Security Token	AR-9	√	√
	Etc.	IC Card Authentication	X	X	AR-5
		Credit Card Authentication	X	X	AR-1
Biometrics	Characteristic	Fingerprint	X	AR-10	√
		Iris	X	AR-10	√
		Face	X	AR-10	√
	Behavior	Signature Pattern	X	X	AR-11
		Keystroke	X	X	AR-11
Etc.	OOB Authentication	Telephone Authentication	X	AR-2	√
		Smart Phone App authentication	X	AR-2	√
		e-mail authentication	X	X	AR-2
		SMS authentication	X	X	AR-2

Table 3. Requirements for Registration Steps

Requirements for Registration Steps	Assurance Level (1 Level : High Level)		
	Level 1	Level 2	Level 3
Identification using trusted identification information	√	√	√
Verification of identification	√	√	X
Face - Face confirmation	√	X	X

IV. 전자금융거래 보안등급

4.1 전자금융거래의 인증등급 기준

4.1.1 안전한 인터넷뱅킹 서비스를 위한 요구사항 분석

안전한 인터넷뱅킹 서비스를 제공하기 위하여, 서비스 제공자는 보안 서비스에서 요구되는 일반적인 보안 요구사항을 만족해야 한다. 기밀성, 무결성, 가용성의 보안의 3대 요소를 만족해야 하며, 이와 함께 서비스 이용시 이용자가 계좌이체와 같은 서비스를 할 경우 이에 대한 부인을 할 수 없도록 부인방지를 만족해야 한다. 또한 서비스 이용자와 제공자의

Table 4. General security requirements for Internet banking services

Security Requirements	Description
Confidentiality	Data transferred upon service use must be encrypted so that the contents can not be known even if a third party acquires the information
Integrity	Ensure that data transmitted when using the service is not faked and modulated
Availability	Service users need to have unrestricted availability at any time
Non-Repudiation	Service users should not be able to make a denial when using services such as bank transfer
Authentication	Service users and service providers must be assured of each other through two-way authentication

Table 5. Security requirements to address threats from Internet banking services

Threat Factor	Security requirements responding to threats
Structural threat	Need to increase the security of the most vulnerable parts of the architecture that make up the Internet service
Threats to security assurance limitations of authentication means	Secure algorithms based on the secret key length underlying the modern encryption must be used, and keys length must be greater than or equal to the required key length per year
Threats from known attacks	Each attack needs to be deployed with corresponding security and solutions to eliminate threats to known attacks
Threats from attacks using unknown vulnerabilities	A vulnerabilities of a particular system have occurred, ensuring minimal security by using a separate terminal and channel that is not affected by poor security of the service

상호 인증도 필요하다고 하였다[16].

전자금융거래, 특히 인터넷뱅킹은 은행 측면에서는 비용절감과 같은 수익성을 제고하고, 사용자 측면에서는 시간과 공간 등의 제약을 벗어나 비대면 거래의 편리성을 제공한다. 하지만, 거래 사실 부인, 전송되는 정보의 무결성과 기밀성 보장의 어려움, 해킹 등 여러 문제점을 가지고 있다. 이에 따라 금융기관에서는 보안 강화를 위하여 공인인증서, 보안토큰, 보안카드, OTP 등 다양한 인증방법과 방화벽, 키보드 보안 프로그램, 백신 프로그램과 같은 많은 보안 메커니즘을 제공하고 있다. 그러나, 금융기관에 비해 상대적으로 보안이 취약한 개인 PC를 대상으로 하는 해킹 사건들이 증가하고 있으며, 중간자 공격(MITM:Man-In-The-Middle)과 메모리해킹은 현재의 인증 방식들에 대해서 취약점이 알려진 상태이다[17].

4.1.2 금융보안원 '자체 보안성심의 가이드'

금융위원회 고시 제2015-18호(2015.6.24)에서는 'IT·금융융합지원방안' 후속조치 이행, 금융회사

및 전자금융업자의 과도한 규제부담 완화 등을 위해 '보안성심의 '를 폐지하고 금융회사 자율보안체계를 확립하기로 하였다[18].

금융감독원 주도의 보안성심의가 금융회사에 과도한 부담을 지우고, 금융회사의 자체적인 보안 수준 확보 노력을 저해함에 따라 보안성심의를 전면 폐지하고, 신규 전자금융업무 시행에 대해서는 금융감독원 보안성심의가 아닌 자체 보안성심의로 보안 수준 점검 의무를 갈음하기로 하였다.

Table 6. Financial Security Institute Self-security review Guide [19]

Review standard	Inspection Items Number
Certification of parties to Transaction	12
Confidentiality and integrity of Transaction information	5
Protection Measures for Information Processing Systems	21
Measures to protect the customer's terminal	14
Prevention measures against information leakage	10
Fraud Detection System, Measures to prevent abnormal financial transactions	3
Ensure system availability and take emergency measures	12
Control of physical access to the system installation site	5
Total	82

금융보안원의 '자체보안성심의 가이드' 의 점검항목에는 다음 절에서 언급하게 될 개인정보보호 점검 부분이 표현되지 않은 것은 보완되어야 할 부분이라 생각된다.

거래당사자 인증(Certification of parties to Transaction)에 대한 세부 점검항목을 예를들면 다음과 같다[19].

① 인증방법의 적정성 :전자금융거래의 종류,성격, 위험수준등을 고려하여 안전한 인증방법을 사용하는지 점검

② 서비스 가입시 이용자 인증:서비스 가입시 적절히 이용자 인증이 실시되는지 점검

③ 서비스 이용시 이용자 인증:서비스이용(로그인, 이체,결제 등)시 적절히 이용자인증이 실시되는 지 점검

④ 세션 가로채기 방지: 이용자와 정보처리시스템 사이에 인증세션이 생성된 후 비인가자의 해당 세션정보를 이용한 인증이 불가능한지 점검

⑤ 다단계 가입자 확인:전자금융서비스 가입시 다단계로 가입자를 확인하고 있는지 점검

⑥ 거래 재활용 방지: 악의적인 의도를 가진자가 기존인증 ·거래정보를 재활용하여 부정인증 거래를 시도하는것을 방지하는지 점검

⑦ 인증우회방지: 사용자확인을 위한 인증단계를 우회하여(예:비밀번호 입력단계 우회등),전자금융서비스를 이용할 수 있는지 점검

⑧ 비밀번호 추측방지:비인가자가 인증정보 등을 추측하여 인증을 시도하는 공격을 방지하는지 점검

⑨ 정보처리시스템 인증:전자금융거래 이용자(또는 전자금융거래 이용자 프로그램)가 접속한 정보처리시스템이 정당한지 여부를 식별 및 인증하는지 점검

⑩ 인증 및 거래관련 기록관리:인증 및 거래 관련 기록을 보존하고, 관련 기록의 변경에 대한 보호대책을 제공하는지 점검

⑪ 인증수단의 관리:인증수단의 등록,발급,배포, 폐기와 관련하여 안전한 관리방안을 갖추고 있는 지 점검

⑫ 금융수단 등록시 개별인증:한번의 사용자인증으로 복수개의 금융수단이 등록되지 않는지 점검

4.1.3 개인정보보호의 중요성

개인정보들은 정보화 사회를 맞이하여 전자상거래,고객관리,금융거래 등 사회의 구성,유지,발전을 위한 필수적인 요소로서 기능하고 있다. 또한, 개인정보는 기업의 입장에서도 수익 창출을 위한 자산적 가치로서 높게 평가되고 있다[21].

하지만, 만약 누군가에 악의적인 목적으로 이용하거나 유출될 경우 개인의 안전과 재산에 큰 피해를 줄 수 있다. 매일 수신되는 스팸문자, 보이스 피싱,

나를 사칭한 메신저 상의 금융사기 등이 모두 개인정보 유출과 관련될 수 있다.

개인정보 유출로 인한 온라인에서의 피해는, 일단 발생한 경우 회복이 어려울 뿐만 아니라, 피해자 개인이나 특정 서비스 제공자에 의해 피해가 복구되기 전에 다른 게시판, 서비스 등으로 글이 전달됨으로써 2차 피해가 '실시간'으로 발생할 수 있다는 특성이 있다. 또한, 개인정보의 유·노출의 근원을 확인하는 데 많은 자원이 소요되기도 한다[21].

또한, 기업에서의 개인정보보호를 보면 정보화 사회의 기업들은 이용자들의 개인정보를 활용하여 다양한 맞춤형 서비스를 제공할 뿐만 아니라, 이러한 서비스를 통해 가치를 창출하고 있다. 이러한 이용자들의 개인정보는 궁극적으로 그 소유가 정보제공자 개인에게 귀속되는 것이며, 기업은 이를 이용자의 동의에 기초하여 수집,이용,제공 등의 활동을 하게 되는 것이다. 기업은 고객의 개인정보에 대한 '선량한 관리자' 로서의 역할을 다해야 하는 것이다[21].

이러한 기업의 입장에서 개인정보에 대한 관리 부주의로 인하여 개인정보를 유·노출하였을 경우 브랜드 가치의 하락, 평판의 악화는 물론이거니와 악의적인 단체, 개인의 협박이나 이용자의 손해배상청구 등으로 인하여 직,간접적인 재정상의 손해를 감수해야 한다.

개인정보에 대한 이용자의 소유권은 점차 사회적으로 강화되어가고 있으며, 실질적으로 개인정보 유출이 기업의 생존에 직접적 영향을 미치는 것으로 이해하여야 한다.

개인에게는 정신적 피해뿐만 아니라 명의도용, 보이스피싱에 의한 금전적 손해, 유괴 등 각종 범죄에 노출될 수 있고, 기업은 이미지 실추, 소비자단체 등의 불매운동, 다수 피해자에 대한 집단적 손해 배상 시 기업 경영에 큰 타격을 받으며 나아가 국가차원에서는 프라이버시 라운드의 대두에 따른 IT산업의 수출애로, 전자정부의 신뢰성 하락, 국가브랜드 하락에 영향을 미칠 수 있으므로 개인정보보호에 대한 중요성을 인식하고 철저한 관리 수행이 필요하다[21].

'정보통신망법' (2016년 9월23일 시행) 과 '징벌적 손해배상제'(2016년 7월 25일 시행), '스마트폰 앱 접근권한에 대한 동의'(2017년 3월23일 시행) 등 개인정보의 중요성 관련 내용을 요약하면 다음과 같다[22].

- 스마트폰 접근권한에 대한 이용자 동의권 강화
- 법률 간 유사용어 조정
- 개인정보 처리위탁제 개선
- 기업의 임원에 대한 책임강화
- 사기성 정보를 받은 이용자에 대한 통지 근거 마련
- 텔러마케팅 시 개인정보 수집출처 고지 의무화
- 징벌적 손해배상제 도입
- 개인정보 관련 범죄에 대한 몰수·추징 도입
- 노출된 개인정보 삭제,차단 조치 강화
- 불법정보의 범위에 개인정보거래 내용 포함
- 개인정보 국외이전 유형 구체화 등

4.1.4 개인정보보호 지표의 보안등급 추가 당위성

보안성심의에서 개인정보보호 지표 검토 누락에 따른 위험성은 아무리 강조해도 지나치지 않다. 본 저자의 근무경험 사례를 언급하면, '키맨 소개 시스템' 구축 보안성심의를 진행 중에 발생한 일이었다. 단순히 인사를 하며 건네받은 명함의 정보를 다른 법인인 계열사간의 "정보공유시스템 구축"을 추진하는 사업의 보안성검토에서 개인정보보호 영역의 검토를 누락하여 사업을 추진하려다 난관에 부딪힌 적이 있다. 단순한 명함을 교환하고 상대를 소개해주는 시스템 구축사업으로 기획한 것인데 사업 아이디어 자체가 법률적 문제에 부딪혀 되돌려 보낸 사례가 있었고, 또 다른 경우는 개인정보 제3자 제공의 필요성이 있는 업무인데 동의절차를 누락하여 사업의 전체 프로세스 검토단계에서 사업의 재검토를 요청한 사례 등 보안성심의에서 개인정보보호 지표는 보안성검토 체크리스트에 반드시 포함되어야 하는 중요지표임이 명확한 것이다.

V. CIAAP 보안등급

5.1 CIAAP 보안등급 제안

온라인에서 제공되는 많은 서비스들은 보안 요소를 고려하여 반드시 보안 대책을 강구하여야 한다[20].

이때 고려되는 일반적인 보안 요소는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availablility)이다. 3가지 보안 고려 요소를 이용하여 만든 보안 등급을 CIA보안등급이라 한다. 여기에 더하여 기존의 CIA 보안등급에 인증(Authentication), 개인정보보호(Personal Information Protection : Privacy) 지표를 추

가한 CIAAP 보안 등급 모델을 제안한다.

5.1.1 CIAAP 보안등급

5.1.1.1 기밀성(Confidentiality)

기밀성은 서비스가 제공될 때 서비스를 위한 정보가 임의로 공개되지 않아야 함을 의미하며, 서비스에서 사용되는 정보의 중요도에 따라 매우 민감한 정보와 그렇지 않은 정보로 분류하였다[20].

Table 7. Definition of Confidentiality

Security Factor	Degree of Level	Consideration
Confidentiality	H	Unable to release randomly because of high sensitive information
	L	Irrelevant with information being randomly released

5.1.1.2 무결성(Integrity)

무결성은 서비스를 제공하기 시작할 때의 정보가 서비스를 받을 때 변조 및 삭제되지 않고 서비스 받을 수 있어야 함을 의미하며, 서비스를 위해 사용되는 정보가 변조 및 삭제되었을 때 심각한 문제가 발생하는 민감한 정보와 그렇지 않은 정보로 분류하였다[20].

Table 8. Definition of Integrity

Security Factor	Degree of Level	Consideration
Integrity	H	Not falsify randomly due to high sensitive information
	L	Information which has no problem being falsified

5.1.1.3 가용성(Availability)

가용성은 제공되는 서비스가 사용자가 원할 때 서비스되어야 함을 의미하며, 사용자가 원할 때 서비스가 반드시 가능해야하는 민감한 정보와 서비스되지 않아도 큰 문제가 되지 않는 정보로 분류하였다[20].

Table 9. Definition of Availability

Security Factor	Degree of Level	Consideration
Availability	H	Always be available due to high sensitive information
	L	Information which has no problem being not in service

5.1.1.4 인증(Authentication)

인증은 사용자인증과 메시지인증으로 구분되며, 사용자인증은 신원확인(identification)과 유사하고 사용자의 신분을 확인 후 해당 서비스를 이용할 권한을 부여하기 위해서 사용된다. 메시지인증은 메시지의 위변조 없이 누구에 의하여 보내어진 것인지를 증명하는 것으로 전자서명을 통해 보증될 수 있다. 여기서는 전자금융거래가 정당한 사용자에게만 제공되어야 하는 보안고려사항으로 ID/PW 인증 후 서비스 종류별, 정당한 사용자 유형별 추가인증이 필요한 보안 지표이다.

Table 10. Definition of Authentication

Security Factor	Degree of Level	Consideration
Authentication	H	High level of service users' standard to verify are required
	L	Low level of service users' standard to verify are required
	N	No need to verify users

5.1.1.5 개인정보보호(Personal Information Protection : Privacy)

개인정보보호는 제공되는 서비스가 개인정보와 관련되어 개인의 민감한 정보(프라이버시)가 보호되어야 함을 의미하며, 서비스되는 항목을 판단함에 있어 개인정보보호법 등 관련법을 참고하여야 한다.

개인정보보호의 레벨등급은 H와 L로 분류하고 H는 E와 P로 세분하였다. E(Economy)는 제공되는 항목이 개인의 경제적인 손익에 영향을 미치는 경우이고, P(Personal Information Protection : Privacy)는 제공되는 항목이 개인의 프라이버시 보

호 및 침해와 관련되는 경우를 나타낸다.

Table 11. Definition of Personal Information Protection (Privacy)

Security Factor	Degree of Level		Consideration
Privacy	H	E	What is provided affects the economic gains and losses of the individual.
		P	The item provided relates to privacy protection and encroachment on the individual.
	L		Does not have anything to do with privacy protection

5.2 CIA와 CIAAP 보안등급 비교

전자금융거래의 주요거래 중 '신용카드 현금서비스 거래'와 '금융계좌 이체거래'에 대하여 CIA 와 CIAAP 보안등급을 적용하여 비교·분석하면 다음과 같다.

5.2.1 CIA 보안등급

신용카드 현금서비스(Credit Card Loan(Cash Service,Card Loan)) 거래화면에 대한 CIA 보안등급을 적용해 본 표이다.

Table 12. Credit Card Loan(Cash Service, Card Loan) for CIA Security Levels

Internet/Mobile Transaction	C	I	A
Credit Card Loan(Cash Service,Card Loan)	L	H	H

금융거래의 계좌이체(Financial account transfer) 거래화면에 대한 CIA 보안등급을 적용해 본 표이다.

Table 13. Financial account transfer for CIA Security Levels

Internet/Mobile Transaction	C	I	A
Financial account transfer Check	L	H	H

5.2.2 CIAAP 보안등급

신용카드 현금서비스(Credit Card Loan(Cash Service,Card Loan)) 거래화면에 대한 CIAAP 보안등급을 적용해 본 표이다.

Table 14. Credit Card Loan(Cash Service,Card Loan) for CIAAP Security Levels

Internet/Mobile Transaction	C	I	A	A	P
Credit Card Loan(Cash Service,Card Loan)	L	H	H	H	H

금융거래의 계좌이체(Financial account transfer) 거래화면에 대한 CIAAP 보안등급을 적용해본 표이다.

Table 15. Financial account transfer for CIAAP Security Levels

Internet/Mobile Transaction	C	I	A	A	P
Financial account transfer Check	L	H	H	H	H

5.2.3 CIA 보안등급과 CIAAP 보안등급 적용의 비교 분석

CIA 보안등급을 적용한 경우보다 CIAAP 보안등급을 적용하면, 예를 들어 ID/PW로 인증했을 경우는 '신용카드 현금서비스' 와 '금융거래 계좌이체' 시 추가인증(공인인증서 등)을 요구하여 인증 단계의 보안등급이 추가됨으로 보안이 강화됨을 알 수 있다. 인증 단계를 통해 정당한 사용자임을 확인한 후 전자금융거래를 가능하도록 하여, 인증단계를 고려하지 않은 CIA 보안등급을 적용한 경우보다 인증단계를 고려한 CIAAP 보안등급이 보다 강화된 것으로 볼 수 있다. 추가적으로 개인정보보호의 보안등급 지표를 추가한 경우는 다음 장(6.전자금융거래의 보안등급 적용사례)의 사례적용에 언급된 내용으로 "카드상품조회/이벤트안내/고객FAQ" 등과 같이 개인정보와 관련이 없는 전자금융거래의 경우는 P항목을 고려할 필요가 없겠지만 그 외의 대다수 전자금융거래의 경우는 개인정보보호 측면의 보안등급을 추가한 CIAAP 보안등급을 적용함으로써 CIA 보안등급만을 고려한 경우보다 개인정보보호 측면의 보안검토가 누락되지 않도록 하는 절차가 반드시 필요하다.

VI. 전자금융거래의 보안등급 사례적용

다음은 국내 K카드사의 '전자금융 주요거래'에 대하여 CIAAP 등급을 적용한 표이다.

Table 16. Application of Security Levels CIAAP to Electronic Finance Major Transactions (A 'K' domestic credit card company)

Internet/Mobile Transaction	C	I	A	A	P
Join Membership	H	H	H	H	P
Credit Card Use(Bill/Certificate/Performance Management)	L	H	H	L	P
Credit Card Use(Credit Card Limit Increase)	L	H	H	H	E
Payment	L	H	H	H	E
Information Change	L	H	H	H	P
Credit Card Product Check/Event Guide/Customer FAQ	L	L	L	L	L
Issue and Application of Credit Card	H	H	H	H	P
Credit Card Loan(Cash Service, Card Loan)	L	H	H	H	E
Partial Payment Forward Agreement	L	H	H	H	E
General Loan/Car Loan	L	H	H	H	E
Pointree(Give,Payment)	L	H	H	H	E
Automatic Payment(Apartment maintenance cost,Gas,Phone bill) Registration	L	H	H	H	P
Convenience Service(Notification,Specifying the Use Device,Check Card SmallCredit Payment,Overseas Usage,Auto Care)	L	H	H	L	E
Payment Service(ISP,Overseas Payment)	L	H	H	H	E
Starshop(Member Store)Finding/Travel,Shopping	L	L	L	L	L
Customer counseling(Theftand Loss)	L	H	H	H	P
Accredited certificate Management	H	H	H	H	P

위의 표는 CIA 보안등급에 인증(Authentication)과 개인정보보호(Privacy)를 더하여 CIAAP 보안등급을 제안한 것으로 국내 K카드사의 전자금융 주요거래에 대하여 적용한 것이다. 금융기관의 전자금융서비스이기 때문에 모든 보안등급이 H(높음)가 나왔으며, 기밀성은 회원가입, 카드발급 및 신청, 공인인증서 관리 등 개인의 정보를 입력해야 하는 단계가 존재할 경우 키보드보안 등을 통한 암호화 조치로 기밀성이 H(높음)로 나타났고 그 외는 기밀성을 L(낮음)로 정의하였다. 단순 조회성 거래인 상품조회, 이벤트안내, 여행·쇼핑 방문하기 등의 거래는 CIAAP 보안등급은 다른 거래와 비교하여 상대적으로 L(낮음)로 나타났다. 특히, 개인정보보호 영역은 개인의 프라이버시 보호(P) 보다는 경제적인 손익부분(E)의 거래가 조금 더 많이 나타났다.

VII. 결 론

본 CIAAP 보안등급은 전자금융거래의 기본적이고도 공통적인 형식의 보안등급 지표로 활용할 수 있으며, 특히 인증 및 개인정보보호 지표를 보안등급 항목에 추가하여 '보안성 심의' 등 보안검증을 수행하여야 한다. 왜냐하면, CIA 보안등급 외 추가로 인증단계를 통해 정당한 사용자임을 확인한 후 전자금융거래를 가능하도록 하여, 인증단계를 고려하지 않은 CIA 보안등급을 적용한 경우보다 인증단계를 고려한 CIAAP 보안등급이 보다 강화되고, 특히 금융권의 경우 P(개인정보보호)부분을 고려하지 않고 추진하다 법률적인 문제를 해결하지 못하고 중단된 사업의 사례가 있는 만큼 간과해서는 안될 부분이다. 개인정보, 금융정보와 같은 중요정보를 보호하기 위해서는 반드시 보안등급 지표에 포함이 되어야 한다.

아쉬운 점은 CIAAP 보안등급에 대하여 좀 더 깊이 있는 연구를 통해 세분화된 보안등급 분류기준을 마련하는 것이 필요하다.

References

[1] Korea Communications Commission, "Safety guidelines for electronic financial transaction authentication methods", May. 2010

[2] Bank of Korea, "2017 Year the third

quarter Domestic Internet banking service use status“, Nov. 2017
〔3〕 Energy economy newspaper, “Card information theft crime rate is a three-fold increase in three years … why?”, Nov. 2015
〔4〕 Lim Yoon Hwa, “Status of fraudulent use of cards by type and future security challenges and responses”, The Loan Association, Loan Institute of Finance, Nov. 2015
〔5〕 Financial Services Commission, “IT· Financial Fusion Support Plan”, Jan. 2015
〔6〕 Realmeter, Internet service authentication means, “Certified certificate preferred”, http://www.realmeter.net/2016/08/인터넷-서비스-인증-수단-공인인증서-가장-선호/, Aug. 2016
〔7〕 Anthony Henderson, http://panmore.com/the-cia-triad-confidentiality-integrity-availability, Mar. 2017
〔8〕 Financial Security Institute, “A Study on the New Technology for Certification of Electronic Finance”, Mar. 2011
〔9〕 Chang-Jin Lee, “A study on security requirements for privacy in a home cloud environment”, Master's Thesis, Department of Information Security Engineering Graduate School of Soonchunhyang University Asan, Korea, Feb. 2017
〔10〕 Tae-Kyu Jung, “Security Requirements Analysis and Guidelines for Using Electronic Authentication”, Master's Thesis, Department of Information Security Management, Chungbuk National University, Korea, Feb. 2017
〔11〕 TTAK.KO-12.0244, “Authentication Service Guideline for The Layered Risk Level in Online Transaction“, TTA(Telecommunications Technology Association), pp.1-2, Dec. 2014
〔12〕 TTAK.KO-12.0247, “Requirements for E-authentication Method of Assurance Level”, TTA(Telecommunications Technology Association), pp.1-13, Dec. 2014
〔13〕 TTAK.KO-12.0248, “Suitable Framework for Entity Authentication Assurance in The Local Environment”, TTA(Telecommunications Technology Association), pp.1-16, Dec. 2014
〔14〕 TTAK.KO-12.0313, “Authentication Assurance Levels Based on Trust Elevation Applicable to Financial Services”, TTA(Telecommunications Technology Association), pp.7-9, Dec. 2017
〔15〕 ITU-T X.1254, Entity authentication assurance framework, Sep. 2013.
〔16〕 Jae-Sik Lee, “A Design of Service Provider Model and Authentication Scheme for Secure Internet Banking”, Ph.D. Thesis, Soongsil University, Jun. 2013
〔17〕 Han-Na You, “A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment”, The Journal of The Korean Institute of Communication Sciences 36(8), 2011. 8, pp.939-946 (8 pages), Nov. 2011
〔18〕 Financial Commission Notice, 2015-18 (2015.6.24.), Jun. 2015
〔19〕 Financial Security Agency, “Financial Company Self-Security Review Guide”, Dec.2016
〔20〕 Yeun-su Choo, “Security Assessment Metrics Model for Online Services”, The Journal of Korea Information and Communications Society ′14-04 Vol.39C No.04, pp.326-333, Apr. 2014
〔21〕 Soo-Ho Lee, “Researching information system security survey”, Master's Thesis, Konkuk University, Dec. 2012
〔22〕 Korea Internet Security Agency, KISA

Online Privacy Portal, URL=https://
www.i-privacy.kr/jsp/user4/intro/defin
e3.jsp

〈저자소개〉

장 길 영 (Kil-Young Jang) 정회원
2000년 2월: 경북대학교 공과대학 무기재료공학과 졸업
2016년 9월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 전자금융보안, 보안정책, 보안성심의, 전자금융법규 등

김 인 석 (In-Seok Kim) 정회원
1973년 2월: 홍익대학교 전자계산학과 졸업(학사)
2003년 2월: 동국대학교 정보보호학과 졸업(석사)
2008년 2월: 고려대학교 정보경영공학과 졸업(박사)
2009년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규