JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 9 : 2044~2055 Sep. 2015

다중요소 기반의 내부 사용자 인증모델에 관한 연구

이재윤[1] · 심호성[1] · 한경석[1] · 최용락[2] · 김종배[2*]

A Study on the Models of Internal system users Authentication considering Multi Factors

Jae-yun Lee[1] · Ho-sung Shim[1] · Kyeong-Seok Han[1] · Yong-Lak Choi[2] · Jong-bae Kim[2*]

[1]IT Policy and Management Dept. Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul 135-798, Korea
[2*]Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul 156-743, Korea

요 약

금융정보시스템은 다수의 거래고객과 다양한 정보를 기반으로 서비스를 제공하는 특징이 있다. 금융관련 고객 정보는 유출시 불법적인 목적으로 사용될 수 있어, 이를 사전에 방지하고자 많은 투자와 노력을 기울인다. 고객 정보 유출은 외부 서비스 이용자에 의한 유출은 물론 내부 정보시스템 사용자에 의해서도 빈번히 발생하고 있다. 이에 본 연구에서는 2채널을 이용한 강화된 내부 사용자 인증모델을 제시하여 금융정보시스템의 안정적 운영을 도모하고자 한다.

ABSTRACT

Financial information systems play such a pivotal role in the financial institution services that are provided for a large customers on the basis of various information including the personal information. As for the personal information collected during the transactions in the financial information systems, huge efforts and investment have been made to protect previously them from being inappropriately misused or illegally used if they could be released. Unfortunately, the frequent accidents on the leakage of sensitive personal information have occurred recently not only by external service users but even by internal system users. Therefore, the aim of this study is to suggest a model of advanced two-channel authentication for internal users in order to increase the stability of financial information systems with enhanced security.

키워드 : 사용자 인증, 정보 유출, 금융정보시스템, 정당성

Key word : User Authentication, Information Leakage, Financial Information System, Justification

Received 16 June 2015, **Revised** 10 July 2015, **Accepted** 23 July 2015

*** Corresponding Author** Jong-bae Kim(E-mail:kjb123@ssu.ac.kr, Tel:+82-2-828-7017)
Graduate School of Software, Soongsil University, Seoul 156-743, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.9.2044 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

지급결제서비스를 제공하기 위한 금융기관의 금융정보시스템은 정보통신기술의 비약적인 발전과 더불어 전화, PC, 스마트폰 등 서비스 이용매체의 다양화에 따라 정보 보안위협 등이 지속적으로 증가하고 있다.

정보통신기술의 발전에 따른 전자금융서비스의 지속적인 증가는 금융서비스 고객에게 편리함을 제공해 주는 이점이 있는 반면, 서비스 처리과정의 보안 취약점을 이용한 정보 보안위협과 전자금융사고의 발생 가능성 등이 상시 존재한다. 이러한 전자금융서비스 환경의 기본사항은 전자금융서비스 이용자와 서비스 제공자에 대한 정당한 본인여부 확인을 수행하는 것이다. 따라서 금융기관은 금융정보시스템 보안 취약점의 제거와 금융정보 유출방지 및 정당한 본인확인에 많은 투자와 노력을 기울이고 있다. 그럼에도 불구하고 2011년 H캐피탈사의 고객정보 해킹사건으로 175만 명의 개인정보 유출, N사 전산망 장애로 273대 서버 피해 및 삼성카드의 80만 건의 개인정보 유출, 2013년 H은행과 S은행의 금융전산사고 발생과 2014년 K카드, N 및 L카드의 개인 정보유출사고는 외주업체 직원에 의해 발생하였다. 이러한 유형의 금융정보 유출사고는 시스템 접근 및 사용권한을 불법적으로 획득하여 발생한 사례로써, 시스템 접근 시 정당 사용자의 확인이 무엇보다 중요함을 알 수 있는 사례이다.

국가정보원 산업기밀보호센터가 2015년 제공한 자료[5]에 따르면 정보기술 유출 주체 중 전직 직원 52.8%, 현직 직원 27.1% 등 내부자에 의한 정보유출이 79.9%에 달하고 있다. 이는 기술가치 인지 및 접근권한이 있는 내부자에 의한 정보기술유출이 대다수임을 알 수 있다. 이에 본 연구에서는 다중요소를 이용한 강화된 내부 사용자 인증프레임워크 제시를 위해 선행연구로써 사용자 인증기술, 지급결제제도위원회와 국제 증권 감독기구 기술위원회의 금융시장 인프라에 관한 원칙(PFMIs), 국제 정보보호 관리체계표준인 ISO/IEC 27001, 국내의 정보보호 관리체계 인증심사기준 - 정보보호 관리체계(K-ISMS), 행정기관 정보시스템 접근권한 관리 규정, 전자금융감독규정 등 지급결제시스템 운영기관의 내부 사용자 인증관련 제반 컴플라이언스[6-8, 12]를 분석하여 금융정보시스템 내부 사용자의 정당성을 확인하는 인증 프레임워크를 제시하고자 한다.

Ⅱ. 관련 연구

2.1. 지급결제시스템 개념

지급결제란 개인이나 기업 등 경제주체가 현금 등의 지급수단을 이용하여 경제활동으로 발생하는 거래당사자간 채권·채무관계를 해소하는 것이다[9]. 국내의 지급결제시스템은 거액자금을 취급하는 거액결제시스템의 운영기관인 한국은행, 소액자금을 대량으로 취급하는 소액결제시스템(Retail Payment System) 운영기관인 금융결제원, 증권결제시스템을 운영하는 한국거래소 및 한국예탁결제원과 외환 동시결제시스템을 운영하는 CLS(Continuous Linked Settlement) 은행 등이 있다. 소액결제시스템은 기업이나 개인의 소액결제를 처리하는 지급결제시스템으로 신용카드, 수표, 계좌이체 등의 지급수단과 관련된 결제시스템으로 어음교환시스템, 지로시스템, 은행공동망 및 전자상거래지급결제시스템으로 구분할 수 있다. 지급결제시스템 운영기관은 지급수단을 이용한 거래당사자간 지급결제서비스가 안정적으로 수행되도록 하여야 하며, 이를 수행하기 위한 요소자원으로 운영 인력, 하드웨어, 소프트웨어, 네트워크 및 보안장비 등을 갖추어 운영하고 있다[9].

지급결제서비스를 제공하기 위한 금융기관의 금융정보시스템 영역은 관리, 기술, 물리 영역 등 3분야로 구분할 수 있다. 관리 영역은 보안활동관련 정책, 표준, 지침, 기준 및 절차 등을 사전 정의하고 이를 관련자가 지키도록 하는 제반 관리활동이다. 기술 영역은 정보시스템에서 발생할 수 있는 제반 보안관련 위협을 사전 파악하고 이를 제거하거나 완화하기 위해 통제수단과 방안을 강구하고 이를 시스템으로 구축하여 운영 관리하는 제반활동이다. 마지막으로 물리 영역은 정보시스템이 설치된 건물이나 시설, 장비 등에 대해 허용되지

표 1. 사용자 인증과정
Table. 1 User authentication process

User	Identification	Authentication	Access Control Mechanism	Authentication	Access target system

표 2. 인증기술 유형
Table. 2 Authentication technology type

Type	Description	Feature	Examples
Knowledge-based (What you know)	Use a user's knowledge or information as a means for self-authentication	- no special device needed, easy exposure - easy use and change, dependent upon personal memory	ID/password, virtual keyboard, Q&A, pattern, image
Possession-based (What you have)	Use a user-possessed token information as a means for self- authentication	- high security, risk of theft and lost - inconvenient to carry, excessive build-up cost	IC card, accredited certificate, OTP (One Time Password)
Biometrics-based (What you are)	Use a user's own biometric characteristics as a means for self-authentication	- high security, serious problem if information is disclosed - excessive build-up and maintenance cost	Biometrics, signature, voice, face, fingerprint, vein, iris, behavioral feature

않은 접근이나 무단사용을 차단하고 모니터링 하는 제반 관리활동이다. 기술 분야 보안영역은 다시 네트워크, 정보시스템, 데이터, DB보안 및 단말기(PC)로 세분화 할 수 있다.

2.2. 사용자 인증기술

사용자 인증기술은 정보시스템이 본인임을 주장하는 요청자에 대해 해당 정보시스템에 등록되어 있는 정당한 사용자임을 인정해 주는 것으로 표 1과 같다. 사용자가 인증시스템에 자신이 누구임을 밝히는 식별, 접근대상시스템이 접근을 요청하는 사용자를 증명하는 인증, 접근이 허용된 사용자에 대해 접근통제 메커니즘에 기초하여 시스템 자원사용을 허가하는 권한부여 단계로 이루어진다. 특히 인증과정은 서비스 요청 자가 서비스 제공자로부터 서비스를 제공받기 위해 수행하는 필수적인 요구조건이다[3, 14, 15, 17, 22].

전자금융서비스의 이용자는 직접 대면이 불가하다는 특성으로 인해 금융기관이 요구하는 비밀정보를 제시함으로서 자신이 정당한 사용자임을 증명한다. 자신을 증명하는 본인 확인기술로써 사용하는 인증기술은 이용자가 알고 있는 것을 인증요소로 사용하는 형태, 이용자가 소유하고 있는 물건을 인증요소로 사용하는 형태, 이용자의 신체적 특징 또는 행동적 특징을 이용하는 형태의 인증 등 표 2[2, 11, 13, 22]와 같이 구분할 수 있다. 또한 일반적으로 사용되는 인증기술별 공격에 대한 방어능력은 표 3과 같다. MITM(Man In the Middle)공격은 공격자가 이용자PC와 접근대상시스템 사이에서 이용자의 정보를 가로챈 후 이를 변조하여 이용자 및 정보시스템으로 가장하여 통신하는 공격이다[11, 13, 17,19].

2.3. 인증대상 정보

전자금융서비스 시 인증대상 정보는 금융정보시스템 접근주체에 따라 서비스 이용자관점의 정보와 서비스 제공자관점의 정보로 구분할 수 있다. 서비스 이용자 관점의 인증대상 정보는 이용자와 금융정보로 구분할 수 있다. 이용자 인증은 금융기관 정보시스템의 특정 서비스 사용권한을 부여받기 위해 수행된다. 서비스 제공자관점의 인증대상 정보는 사용자 인증과 명령어 수행정보 등이 있다. 접근주체별 인증은 로그인 과정이 대표적인 사례로써 비밀번호, OTP, 생체정보, 공인인증서 등의 수단을 사용한다. 서비스 이용자 관점의 금

표 3. 인증기술별 공격방어 기능
Table. 3 Authentication technology-specific attack/defense function

Function	ID/ password	Security Card	OTP	Accredited Certificate
Denial prevention	n/a	n/a	n/a	Yes
Re-attack	Low	Middle	High(high defense level)	High
MITM attack	Low	Low	Middle	High
User PC attack	Low(low defense level)	Low	Low	Middle

융정보인증은 송수신 계좌번호, 금액 등 금융정보의 인증과 무결성을 위해 사용하는 것으로, 전자서명 기술이 대표적으로 이용되며, 전자서명은 공인인증서를 주로 사용한다[2, 11].

표 4. 주요국 금융거래 이중요소 인증기술 적용현황
Table. 4 Use of dual-element authentication technology in financial transactions of key states

State/place	Double-element authentication technology
ROK	OTP, accredited certificate
US	OTP, biometrics, location-based
Singapore	OTP, accredited certificate
Hong Kong	OTP, accredited certificate
China	accredited certificate, electronic signature

2.4. 금융정보시스템 접근 주체

본 논문에서 제시하는 사용자 인증모델 프레임워크는 기술 분야 영역으로 금융정보시스템 관점의 접근주체는 금융거래고객인 서비스 이용자와 정보시스템을 운영 및 관리하는 내부 사용자로 구분할 수 있다. 내부 사용자는 접속 목적, 이용 매체, 역할 및 기능에 따라 구분된다. 일반적으로 에뮬레이터 소프트웨어 사용 및 SSH(Secure Socket Shell)프로토콜을 사용하여 시스템의 최상위 권한으로 시스템에 접속하는 루트 관리자 계정접속, DBMS 및 데이터 등의 관리를 위한 DB관리자 계정접속, 업무운영을 위한 운영자 계정접속과 클라이언트 및 서버 소프트웨어 등 시스템 관리도구 등을 통한 시스템 접속, 콘솔을 통한 시스템 접속, 프로그램을 통한 접속, 시스템 간 접속 등이 있다.

2.5. 사용자 인증 강화요인

금융정보시스템 접근주체인 사용자 인증의 강화는 다양한 방법으로 구현할 수 있다. 금융정보시스템 내·외부 사용자 인증에 사용되는 기술은 매우 다양하며, 가장 많이 쓰이는 것으로 ID와 비밀번호가 있다. 인증[2, 4]은 사용자 자신이 알고 있는 비밀번호를 전자금융서비스 이용과정에서 사용하여 정당한 사용자임을 인증 받는 것이다. 이와 같이 한 가지 요소만을 사용하는 단일 요소인증 시 이용된 비밀번호는 단일요소 인증기술이다. 이중요소 인증(Two Factor)은 2개 이상의 인증기술을 이용하여 사용자 인증을 수행한다. 한 개의 기술만 사용하는 단일요소 인증 대비 2개 이상의 인증기술을 사용하는 다중 요소인증(Multi Factor)기술은 보다 강화된 보안의 제공 및 취약점의 제거가 가능하다[3, 4, 11, 18, 22].

전자금융서비스 과정에서의 위, 변조 가능성은 거래

표 5. 금융정보시스템 사용자 인증관련 주요 컴플라이언스
Table. 5 Key compliance related to financial information system user authentication

Type	Description
Financial market infrastructure -related principle(PFMIs)	- principle 17(operation risk): risk of service reduction or suspension due to flaw, etc. in information system, internal process and HR →regular inspection of operation management system build-up, defense system build-up and operation policy, process and control means, etc. to reduce operation risk by definition
Information protection management system(ISMS) Standard (ISO/IEC27001)	- management process: consisted of system building, realization and operation, monitoring and review, management and improvement, etc. - control list: control area, control purpose and control matter - control area : management/physical/ technological control - control area-specific control matter: personnel security. physical/environmental security: entrance/exit control . access control: system and user control
Information protection management system(K-ISMS)	- control area: management/physical/ technological control - control area-specific control matter: outside visitor and personnel security. physical security . access control: policy building and access control management - monitoring and audit: information asset monitoring and security audit
Electronic financial supervision regulation, etc.	user terminal protection – validity check such as user authentication, etc. dual check of responsible staff in key work – assign minimum necessary authority to work to external user individual user account assignment and management, authorization check information system access· account user right· authentication for access record control management

정보를 확인 및 승인하는 거래연동 인증기술이나 분리된 채널의 이용으로 인증정보를 확인, 처리하는 2채널 인증기술을 사용한다. 동 기술은 2요인 인증을 적용하더라도 공격자가 2채널을 동시 공격하기 힘들다는 점을 이용하여 안전성을 제고하는 것이다[13].

또한 인증채널은 이용하는 시점에 따라 그 효용성이 달라질 수 있으며, 권한의 사용은 특정서비스가 사용되는 시점에 적용하는 것이 비밀번호 등의 정보유출을 최소화한다는 점에서 바람직하다. 서비스 제공자가 공개된 영역에서 다수를 대상으로 서비스 제공 시 중요정보는 공개된 영역과 일정거리 유지가 필요할 경우 이용한다. 2채널 인증은 2요소 인증방식과 함께 이용한다. 사용자는 비밀번호로써 로그인후 일반적인 정보조회 수준 등의 권한만을 부여하고 중요정보 수정 또는 특정서비스 수행 시 별도의 권한을 추가로 획득하고 해당 작업의 승인을 위하여 다른 인증정보를 다른 채널을 통하여 제공한다. 따라서 동 방식은 절차의 보안성은 우수하나, 상대적으로 다른 인증방법보다 복잡하다[20, 21]. 다음은 접근주체가 사용하는 디바이스 인증기술로, 일회용 패스워드 기반의 인증서를 이용한 사용자 인증을 기반으로 제한된 디바이스만이 접근이 가능하도록 접근 제어목록 추가 및 접근제어를 수행하여 인증을 강화한다[1, 4]. 또한 단말기 인증기술은 NAC(Network Access Control)에서의 단말기 인증기술로, 단말의 인증식별 값을 인증서로 사용하며, 허용 IP주소를 이용하여 네트워크 접속 허용 또는 차단을 수행한다. 이러한 기술들은 대부분 사내 내부 사용 단말의 보안접근 통제를 위한 기술로 가치가 높다[4, 10, 13].

Ⅲ. 내부 사용자 인증 모델

3.1. 인증기술 적용 동향

전자금융서비스 등 비대면 거래에서의 인증방법이나 기술이 개별적으로 이용되는 경우는 거의 없으며, 여러 기술이 복합적으로 연계·적용된다[21]. 각 인증방법이 특정 범위의 위협요소 대응에 적합하게 되어 있어 모든 범위의 위협요소 방어를 위해서는 각 기술의 적절한 조합[23], 이용이 필요하다. 따라서 인증기술의 조합·이용은 이용편의성에 영향을 미칠 수 있어 비대면 거래 이용의 만족도에 영향을 줄 수 있다[21].

최근의 전자금융서비스는 보안성 강화를 위해 대부분 2요소 이상의 인증기술 사용을 금융정책기관에서 권고함에 따라 금융기관은 서비스 거래종류에 따른 다중요소 인증수단을 도입하여 적용 중으로 표 4와 같다[13]. 대부분 금융기관은 중요 금융서비스에 추가 인증수단을 적용하는 추세이다. 온라인 계좌이체에서 다양한 인증수단 중 OTP 인증수단이 가장 많이 이용되며, 거래를 실행하는 채널과 물리적으로 분리된 다른 채널을 이용하는 2채널 인증방법을 일반적으로 이용한다[11]. 인증방법 및 기술은 각각의 장단점이 있어 특정방법의 적용이 반드시 바람직한 것은 아니다.

이러한 사용자 인증기술은 다양하게 존재함에도 불구하고 실제 사용은 널리 적용되지 못하고 있다. 정보시스템 내·외부 사용자의 다양한 인증기술 사용에 대한 어려움 해소와 적용 확산을 위해 인증기술은 다음과 같은 조건을 충족해야 한다. 첫째 일반 사용자의 사용에 따른 기술적 호환성이 보장되어야 한다. 둘째 모든 업체들이 표준을 통해 유사한 인증수단 개발 등 사용자가 사용하기 쉽도록 개발해야 한다. 셋째 인증기술 적용을 위한 도입비용이 저렴해야 한다. 넷째 인증기술은 금융기관이 인증기술을 신뢰할 수 있어야 하며, 사용자와 금융기관 간 상호 인증 등 양방향으로 작동하는 인증기술 제공으로 적절한 보안등급을 보장해야 한다. 다섯째 인증기술은 금융기관의 보안체계, 응용소프트웨어 및 웹사이트와 손쉽게 통합 및 확장 가능 하는 등 손쉽게 관리될 수 있어야 한다. 마지막으로 인터넷을 통한 사용자 인증수단 배포 시 PC, 핸드폰, POS(Point of Sales) 등 다양한 통신채널에서 작동되어야 한다[11, 16].

3.2. 내부 사용자인증관련 컴플라이언스

금융정보시스템 접근관련 제반 컴플라이언스는 표 5와 같이 관련 주관기관에 따라 매우 다양한 형태로 요구되고 있다[6-8, 12].

따라서 본 연구는 금융정보시스템에 요구되는 선행연구에서의 금융정보시스템 접근주체별 인증 강화요인과 다양한 컴플라이언스 관련 IT요소를 사용자 인증 관련 최적화 모델을 위한 기초자료로 사용하여 이를 충족시키는 내부사용자 인증 프레임워크를 제시하고자 한다.

표 6. 컴플라이언스 관련 내부 사용자 인증 모델 요건
Table. 6 Internal user authentication model requirements related to compliance

Type	Description	Compliance	model components
Financial information system	system used to provide financial service to financial customers	-	information system
Service user	Financial customers who want to receive financial service	-	financial service user
User account	-operation administrator of information system -granted to individuals according to information system access purposes	electronic financial supervision regulation, administrative organization information system access authority management regulation	account management, tracking audit, password management, information system, internal user
Terminal of use (PC)	-designate terminal of use as key terminal, operation -allowed to use only for terminal -user ex ante authentication and authenticated users	electronic financial supervision regulation, administrative organization information system access authority management regulation	PC
User authentication	password, security token, smart card, HSM, OTP, biometrics recognition, IC card	Financial computerization area comprehensive plan, administrative organization information system access authority management regulation	ID/ password, OTP server security system
Access authority ·control	-access control means(physical, technological, management) consideration -self-identification and access authority means consideration	PFMIs, ISO/IEC 27001, K-ISMS electronic financial supervision regulation, financial computerization area comprehensive plan administrative organization information system access authority management regulation	-
Main process performance authorization	Authorize administrator of important process affecting information system	electronic financial supervision regulation	tracking audit, OTP, server security system
System access and activity record	-record and manage information system user's access and performance activities -use for post-tracking audit, etc.	electronic financial supervision regulation, financial computerization area comprehensive plan, administrative organization information system access authority management regulation	tracking audit information server security system

3.3. 인증모델 요건과 내부 사용자 인증 프레임워크

관련 선행연구에서의 금융정보시스템 접근 주체별 인증 강화요인과 다양한 컴플라이언스 요소의 요구 내용을 IT관점에서 분석한 결과, 금융정보시스템의 내부 사용자 인증 프레임워크를 위한 IT요소별 모델은 표 6과 같은 요건을 충족하여야 한다. 현재 일반적인 경우 정보시스템에 접근하는 사용자에게 적용되는 사용자 인증 프레임워크는 그림 1과 같은 데 비해 본 연구는 표 6의 모델 요건 충족을 기반으로 그림 2와 같이 제시한다. 제시한 프레임워크는 내부 시스템 사용자의 시스템 접근 시 정당 사용자 확인을 위해 ID/비밀번호와 OTP 등 채널과 다중요소 인증을 이용한다. 또한 계정관리, 서버보안, 방화벽, 추적감사, OTP, 비밀번호관리시스템 등을 상호 연계하여 인증관련 제반 정보를 사전 공유토록 구현하였다.

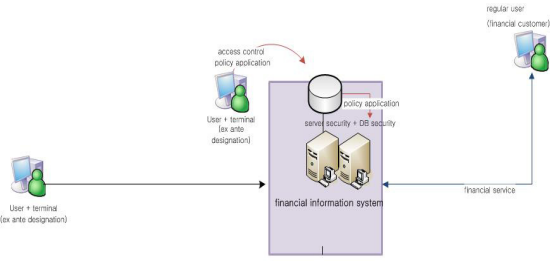

그림 1. 내부 사용자 인증 프레임워크(일반적인 경우, As-Is)
Fig. 1 internal user authentication framework (general cases, As-Is)

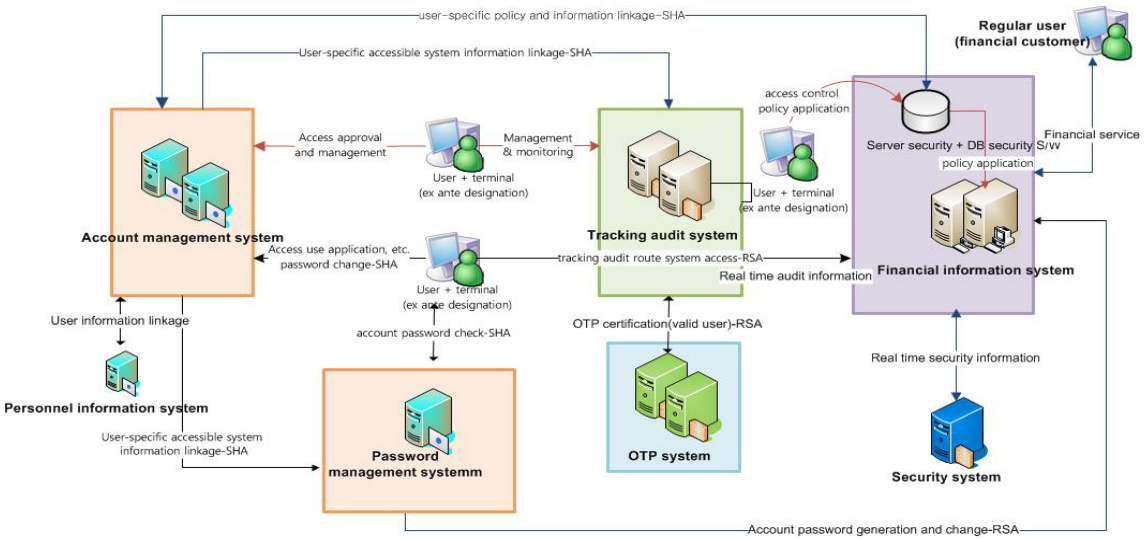

그림 2. 내부 사용자 인증 프레임워크(연구자 제시, To-Be)
Fig. 2 internal user authentication framework (proposed by researcher, To-Be)

사용자의 시스템 접근과정에서 관련시스템 상호간 사전 공유된 정보를 사용토록 하여 보안성을 강화하였다. 또한 정보시스템 내부 사용자의 정보시스템 접근 시 정당 사용자의 인증강화를 위해 작업수행의 중요도에 따라 인증기술의 적용단계 차등화는 물론 인사 명령 등에 의한 담당사무 변경 및 퇴직자 등의 정보가 즉시 반영되어 정당 사용자를 인증토록 하고, 작업수행자의 작업 수행에 대한 기록관리가 가능토록 정보시스템을 설계, 구현하였다.

금융정보시스템 사용자는 시스템 접속이전 관련 정보를 사용자 - 단말(PC) - 네트워크-방화벽-계정관리시스템 - 추적감사시스템 - 비밀번호관리시스템-OTP시스템-서버보안시스템 및 접속대상 정보시스템 등 10단계 과정을 통해 관련시스템에 사전 등록하여야만 관련시스템 접속이 가능하다.

금융정보시스템 사용자가 사전 등록과정을 완료 후 시스템에 접속하여 단순 작업이 필요할 경우 사용자-단말(PC) - 네트워크-방화벽-추적감사시스템 - OTP시스

표 7. 일반적인 경우(5단계 접근, 인증시스템 2회 적용)
Table. 7 General cases (5-phased access, 2 rounds of authentication system application)

Components	user	terminal(PC)	authentication system		financial information system
			firewall	server security	
Access phase (route)	1	2	3	4	5

표 8. 연구자 제시 사전등록(10단계 접근, 인증시스템 6회 적용)
Table. 8 ex ante registration proposed by researcher (10-phased access, 6 rounds of authentication system application)

Component	user	terminal (PC)	Network (IP management system)	authentication system						financial information system
				fire wall	account management (personnel information connection)	tracking audit	pass word	OTP	server security	
Access phase (route)	1	2	3	4	5	6	7	8	9	10

표 9. 연구자 제시 단순작업(8단계 접근, 인증시스템 4회 적용)
Table. 9 Simple process proposed by researcher (8-phased access, 4 rounds of authentication system application)

component	user	terminal (PC)	network (IP management system)	authentication system				financial information system
				fire wall	tracking audit (account management - personnel information connection)	OTP	server security	
Access phase (route)	1	2	3	4	5	6	7	8

템-서버보안시스템 및 접속대상 정보시스템 등의 8단계과정을 통해 작업수행이 가능하여 시스템 운영의 안전성이 확보되도록 구현하였다. 또한, 사용자가 금융정보시스템에 접속하여 일상적인 작업 수행 후 시스템의 Shutdown 등 시스템에 중대한 영향을 미치는 중요작업을 수행할 경우 사용자-단말(PC) - 네트워크-방화벽-추적감사시스템 - OTP시스템-서버보안시스템 및 접속대상 정보시스템-비밀번호관리시스템-서버보안시스템-접속대상시스템-중요작업 수행 명령어 입력-추적감사시스템-서버보안시스템-OTP시스템 - 추적감사시스템-접속대상 정보시스템-중요작업 수행명령어 실행의 18단계 과정을 통해 작업수행이 가능하여 시스템 운영의 안전성이 확보되도록 설계 및 구현하였다.

본 연구에서 제시한 프레임워크와 일반적인 경우의 프레임워크는 사용자의 수행 작업 중요도별 인증시스템 차등 적용 및 다중 인증시스템 적용과정에서 접근단계 차이 및 인증시스템의 적용 횟수 등에서 표 7, 8, 9, 10과 같이 차별화된 정보시스템 사용자의 정당성을 인증·검증함으로서 운영의 안정성이 강화됨을 확인할 수 있다. 내부 사용자 인증 프레임워크로 제시한 주요 구성요소별 세부 처리과정에서 사용자 인증 강화를 위해 사용되는 주요기능은 표 11과 같다.

금융정보서비스를 고객에게 제공하기 위해 서비스 제공자 관점에서 사용하는 PC는 중요단말기로 지정하여 운영한다. 지정된 중요단말기는 정해진 정보시스템 운영이외 다른 용도로 사용할 수 없으며, 사전 등록 및 지정된 사람만이 단말기에 접근 및 사용할 수 있도록 접근 통제를 함으로서 안정성을 확보한다. 단말기의 사용 및 접근통제 강화를 위해 신분증 인식단말기를 PC 단말기와 연동하고 사용자는 단말기 사용 시 신분증과 단말기의 부팅 패스워드 등을 통하여 접근한다. 또한 정보시스템 운영관리의 보안성 및 안전성 강화를 위해 사용자가 사용할 PC단말기는 출발지 PC단말기의 IP 주소와 접속대상 금융정보시스템의 IP주소, 사용 프로토콜, 적용기간, 및 사유 등을 명시한 오프라인상의 사전 등록신청서에 의해 사전등록 요청한다. 동 요청에 의해 관련 정보를 방화벽에 등록 후 실제 접속 및 작업 시 동 등록 정보에 의해 통과 허용 여부 판단 후 접속 및 작업이 가능하다.

또한 금융정보시스템 내부 사용자의 시스템 접근 시 통제 강화를 위해 방화벽에 관련 제반 정보를 사전 요청받아 등록 후 사용자가 금융정보시스템에 접근 시 사전 등록된 정보에 의하여 정당성 여부를 확인한다. 금융정보시스템 사용자는 중요단말기로 사전 승인받아 사용하는 PC 및 접근대상 금융정보시스템의 제반 정보(PC의 IP주소, 접근대상 서버IP등)를 승인권자 앞 사전

표 10. 연구자 제시 중요작업(18단계 접근, 인증시스템 10회 적용)
Table. 10 key process proposed by researcher (18-phased access, 10 rounds of authentication system application)

Component	user	terminal (PC)	network (IP management system)	authentication system					financial information system	Key command input/ execution
				fire wall	tracking audit (account management-personnel information connection)	pass word	OTP	server security		
Access phase (route)	1	2	3	4	5/13/15	9	6/14	7/10/16	8/11/17	12/18

표 11. 내부 사용자 인증 프레임워크 구성요소별 주요 기능
Table. 11 Main functions of internal user authentication framework components

component		Main function
User + terminal		internal user who accesses the financial information system to perform work and provide financial service to financial customers and operates and manages the system
		terminal (PC) used by the user in order to access the financial information system
Personnel information system		system that integrates every individual organization members'personnel information, company staff numbers, division of work, job descriptions, etc. to operate and manage
Network (IP management system)		system that controls and tracks the network access to financial information system by allocating a fixed IP based on the user terminal (PC) MAC address allowed for pre-access
Certification system	Firewall	system that registers a user's terminal (PC) and the information (PC and system IP, etc.) of financial information system at an advance request in order for a user to check validity based on system access start information
	Account management system	system that manages (application, approval, change, deletion, etc.) and mutually connects the account on the side of system which is granted to a user of the information system before using it with related systems (personnel information, server security, tracking audit, password management, financial information system)
	Tracking audit system	system that authorizes valid user based on the data on a user's accessible information system list shared with the account management system upon user access to information system between user terminal and financial information system; conducts the monitoring, activity record saving, etc. of the user's work performance activities after information system access in mutual connection with other relevant systems (account management, server security, OTP, financial information system)
	OTP system	system as a means to reinforce authentication, which checks user authority validity additionally upon the execution of main system commands affecting the system at the point of user information system access and after the access such as Shutdown, Reboot,, andHalt and newfs in mutual connection with other relevant systems (tracking audit, server security, financial information system)
	Password management system	system that connects main account passwords of system administrator authority, etc., with other relevant systems (account management, financial information system) in real time and uses them for regular automatic password change management and approval to use a key process of the information system during a specific time
	Server security system	system that controls the mutual connection of user service authority regarding system access, program and command execution, data access, etc. with other relevant systems (account management, tracking audit, password management system)
	DB security system	system that controls the access and authority of a user accessing the information system database
Financial information system		system that a user accesses to provide financial information service to financial customers. The system connects with other relevant authentication systems (account management, server security, tracking audit, password, DB security system) for operational management.

등록 요청한다. 승인 자는 요청에 대한 정당성 여부를 확인한 후 관련 정보를 방화벽에 등록한다. 방화벽에 등록된 정보는 사용자가 금융정보시스템에 접속코자 할 경우 동 정보를 이용하여 접속관련 제반 정당성을 확인한 후 금융정보시스템 접근이 가능하다.

금융정보시스템 사용자는 접속하고자 하는 금융정보시스템 사용에 앞서 계정관리시스템을 통하여 접속 희망 금융정보시스템에서 사용할 계정등록을 신청하여 승인권자의 승인을 통해 계정을 발급받는 다. 동 시스템은 계정등록 신청자에게 계정 부여 시 인사정보시스템 등과 연동하여 정당한 사람인지 사전 확인 후 계정을 부여한다.

등록 신청 시 제공정보는 접속대상시스템, 계정권한 및 역할, 사용기간, 비밀번호 및 신청사유 등을 명시하며, 등록신청과정에서 접속대상 금융정보시스템과 동 내용을 실시간으로 연동 및 정보를 공유한다. 동 공유된 정보는 사용자가 금융정보시스템에 사후 접근 시 정당한 사용자 등 확인에 활용된다. 또한 퇴직자 및 담당 수행업무 변경 등의 사용자 정당성에 대한 주기적 확인을 통해 시스템의 불법 접근 원천차단 및 정보유출 방지를 위해 인사정보시스템과 관련시스템을 상호 연동하여 관련정보를 상시 공유한다.

또한 추적감사시스템은 계정관리시스템과 연동하여 사용자의 접근대상 금융정보시스템 접근과정에서 접근경로의 중앙통제 역할과 사용자의 모든 수행 작업내용을 기록하고 관리한다. 접근통제 관리를 위해 5회 로그인 실패 시 접근 계정이 잠긴다. 동 시스템에서 사용하는 IP정보를 접근대상시스템에 사전 등록하여 실제 사용자가 동 시스템을 통해 시스템에 접근 시 정당성을 확인하여 사용자 인증을 강화하였다.

비밀번호관리시스템은 접속대상 금융정보시스템과 실시간 연동하여 사용자가 중요작업 등을 수행하고자 할 경우 중요작업 수행에 필요한 관련정보(접속대상시스템, 접속계정, 요청 사유, 사용기간 등)제공을 통해 승인권자의 사전 승인을 득한다. 이를 통해 공용계정의 비밀번호 생성 및 금융정보시스템과 연동, 관련 정보를 사전 공유하고 공유된 정보는 사용자 접근 시 정당 사용자 인증에 사용한다. 일반적인 경우의 계정에 대한 비밀번호는 개인이 생성, 작성 및 접속대상시스템에 등록되어 유지 관리된다. 생성과정에서 개인 연관정보로 생성하여 외부에 쉽게 노출될 가능성이 크며, 이로 인해 불법적으로 사용될 여지가 상시 존재한다. 또한 관리과정에서 잊어버릴 가능성이 상존하며, 주기적인 변경과정에서 오타 등에 의한 의도치 않은 비밀번호 생성 가능성 또한 배제할 수 없는 것이 현실이다. 그러한 단점을 해소하기 위해 계정에서 사용되는 비밀번호를 동 시스템을 통해 발급하고 발급된 정보는 접근대상시스템에 실시간 공유된다. 공유된 계정의 비밀번호는 사용자가 시스템에 접근 시 정당한 사용자임을 확인하는 데 사용된다.

OTP관리시스템은 특정 작업수행시의 OTP인증 필요시에 OTP생성에 사용할 스마트폰 관련 제반 정보(소속, 이름, 이용 장소, 스마트폰 MAC 등)를 승인자 앞 신청에 의하여 사전 등록한다. 등록신청은 동 시스템 사용에 필요한 앱을 인터넷을 통해 사용할 스마트폰에 다운로드 후 ID 및 패스워드(Activation Code)등을 통해 등록 후 사용한다. 특정작업 수행은 추적감사시스템 접근, 금융정보시스템 내 중요 명령어 수행, 웹서버 접근 등의 과정에서 OTP관리시스템과 사용자의 스마트폰에서 생성한 OTP정보에 의하여 정당 사용자 여부를 확인한다. 접근 통제 관리를 위해 5회 OTP 입력 오류 시 OTP사용이 제한된다.

서버보안시스템은 계정관리시스템 및 OTP관리시스템과 연동하여 금융정보시스템 사용자의 접근통제를 수행한다. 사용자가 시스템에 영향을 미칠 수 있는 중요명령어 입력 후 OTP관리시스템을 통하여 정당 사용자 확인과정을 거치면 서버보안소프트웨어는 동 사용자의 중요명령어를 실제 금융정보시스템에서 실행하게 된다. 또한 허가되지 않은 일반계정에서 루트 권한관리자로 SU(Switching User)할 수 있는 권한을 제한하여 사용자 인증강화는 물론 금융정보시스템의 안정적 운영이 가능하다.

Ⅳ. 결 론

금융정책기관에서는 금융서비스의 투명성 제고는 물론 정보시스템 운영의 안전성 강화를 지속적으로 요구하고 있다[7, 8]. 이와 같은 다양한 컴플라이언스가 요구됨에도 불구하고 표준으로 적용할 만한 수준의 금융정보시스템 내부 사용자 인증모델 및 관련 프레임워크에 대한 조사 및 연구는 다소 부족한 실정이다. 따라서 선행연구의 접근주체별 인증 강화요인과 다양한 컴플라이언스 요구 내용을 기초로 금융정보시스템 내부 사용자 인증모델 요건을 충족시키는 프레임워크를 그림1과 같이 제시하였다.

본 연구에서 제시한 내부사용자 인증 프레임워크는 금융정보 보안위협이 가중되는 금융정보시스템 운영환경과 내부 사용자에 대한 적용가능 인증 표준 프레임워크가 미비한 현실 상황에서 사용자 인증강화를 위해 다중채널 및 다중 요소를 사용한다. 제시된 프레임워크는 실제 구축된 기관의 실 업무에 적용하여 내부 사용자의 금융정보시스템 접근 시 사용자의 정당성 인증 및 접근통제 강화 수단으로 활용하여 시스템 운영관리의

안전성 확보는 물론 중요정보의 불법 유출에 대한 대응이 가능토록 하였다. 또한 동 프레임워크는 개별 금융기관의 개선모델로 유용하게 활용될 수 있을 것으로 기대된다.

그럼에도 불구하고 금융정보시스템 관점의 내·외부 사용자 접근은 서비스 이용자, 시스템 관리자 및 운영자, DB관리자, 콘솔 접속, 프로그램 및 시스템 관리 도구를 이용한 접속 등 접속경로가 매우 다양함에 따라 다양한 접근경로에 대한 통제가 동시에 고려되어야 한다. 또한 정보시스템 운영의 안정성 강화를 위한 사용자의 접근통제 강화만을 강조함에 따라 사용자의 접근 용이성 및 사용 편의성, 휴대성, 소요 및 구축비용 등 경제성, 정보시스템 자원 사용의 효율성 등에 대한 연구가 다소 부족함에 따라 동 요소들이 고려되어 추진되어야 한다.

REFERENCES

[1] Jae-yong Kim, *A Study on Hone Network user Authentication by using A Certificate based on OTP*, 2009.

[2] Seung-gu Yun, *Enhanced techniques of internet banking security system using OTP*, 2010.

[3] Yong-Jae Lee, *Study on user authentication and e-banking system using a dual channel*, 2011.

[4] Cheol-woo Jeong, E*mpirical studies on the user terminal authentication system for fraud prevention certificate*, 2012.

[5] NIS, *Industrial confidentiality Center*, 2015.

[6] Prime minister's Directive, *Information system access rights management provisions of the Administrative agency*, 2013.

[7] FSC, *Electronic banking supervisory regulations*, 2013.

[8] FSC, *Relapse prevention comprehensive measures of leakage of personal information of the financial sector*, 2014.

[9] Bank of Korea, *the payment system in Korea*, 2009, 2014.

[10] KFTC, *Payment and information technology, electronic banking security measures and OTP Usage*, 2006.

[11] KFTC, Payment and information technology, *safety analysis of Internet banking authentication means* pp. 119-139, 2007.

[12] KFTC, *Payment and Information Technology*, 2012.

[13] KFTC, *Certification means your major sectoral studies of electronic financial transactions*, 2012.

[14] Eun-Jeong Choi, Chan-Oe Kim, Joo-Seok Song, Password-Based Authentication Protocol for Remote Access using Public Key Cryptography, *Kiise*, Vol. 30 No. 1, pp. 75-80, 2003.

[15] Sung-Woon Lee, Hyun-Sung Kim, Kee-Young Yoo. A Password - based Efficient Key Exchange Protocol. *Kiise*, Vol. 31 No. 4, pp. 347-352, 2004.

[16] Jonathan Penn, *What To Look In Consumer Strong Authentication Solutions*, Forester, 2005.

[17] FIPS 113. *Computer Data Authentication*. May, 19 1985.

[18] Phoenix Technologies, *CS HAN. Trust connector*. 2006.

[19] Forouzan. *Cryptography and Network Security*. McGraw-Hill, 2007.

[20] K. Renaud, M. Al-Fairuz, *Multi-channel, Multi level Authentication for More Secure ebanking*. 2010.7

[21] KFTC, P*ayment and information technology, current status and future prospects of authentication methods*, pp. 31-69, 2011.

[22] Jae-sik Lee, *Secure Internet Banking service model design and certification scheme,* 2013.

[23] Je-gook Kim, *An Empirical Study on Early Warning Model of Industrial Technology leakage in the Public Energy Sector*, 2013.

이재윤(Jae-yun Lee)

1985년 한남대학교, 전자계산학과 학사
1994년 건국대학교 산업대학원 전자계산학과 석사
2015년 ~ 현재 숭실대학교 대학원 박사과정
※관심분야 : 전사적 아키텍처(EA), 업무지속성계획(BCP)

심호성(Ho-sung Shim)

2015년 현재 (사)한국공개소프트웨어협회 상근 부회장으로 재직 중
2015년 ~ 현재 숭실대학교 대학원 박사과정
※관심분야 : SW교육사업, 국제 공개SW 개발자 대회 등

한경석(Kyeong-seok Han)

1979년 서울대학교, 국어교육학사
1984년 서울대학교 경영학 석사
1989년 미국 퍼듀대학교 대학원, 경영정보시스템 전공 박사
1989년 미국 휴스턴 대학교 조교수
1983년 ~ 현재 숭실대학교 경영학부 교수 재직
※관심분야 : Technical MIS, Digital Economity, Agent-Eased Simulation, Web Programming, ERP, 회계정보시스템, E-Business, 전자상거래, 중소기업정보화

최용락(Yong-Lak Choi)

2001년 숭실대학교 대학원 공학 박사
2006년 숭실대학교 정보과학대학원 소프트웨어공학과 교수
2012년 ~ 현재 숭실대학교 SW특성화대학원 교수 재직
※관심분야 : 데이터모델링, 소프트웨어공학, 정보전략 기획

김종배(Jong-Bae Kim)

2002년 8월 숭실대학교 정보과학대학원 석사
2006년 8월 숭실대학교 대학원 컴퓨터학과 박사
2001년 ~ 2012년 (주)이엔터프라이즈 대표이사
2012년 ~ 현재 숭실대학교 SW특성화대학원 교수
※관심분야 : 소프트웨어공학, 정보보호, 오픈소스소프트웨어