금융정보시스템 운영자의 접근통제 기법에 관한 연구

이재윤* · 심호성** · 김종배***

*금융결제원 · **(사)한국공개소프트웨어협회 · ***숭실대학교

A Study of Methods of Authentication and Access Controls for Financial Information System Operators

Jae-yun Lee* · Ho-sung Shim** · Jong-bae Kim***

*Korea Financial Telecommunications & Clearings Institute

E-mail : jae_yun_lee@kftc.or.kr

요 약

금융기관에서 운영하는 정보시스템은 고객의 다양한 정보를 기반으로 금융정보서비스를 제공하는 특징이 있다. 이러한 고객정보는 유출시 정신적 피해는 물론 금전적 손해까지 발생할 수 있다. 따라서 금융기관의 금융정보시스템은 운영자의 정당성에 대한 사전확인이 필수적이며, 정당한 운영자에 한해 정보시스템 관련 작업을 수행토록 하고 있다. 본 연구에서는 현재 금융정보시스템에서 사용되고 있는 운영자의 접근통제 기법에 관하여 연구하고자 한다.

ABSTRACT

Financial information systems in financial institutions are characterized in providing financial services concatenated with various types of customer information. The leakage of those information could lead to pecuniary loss and non-pecuniary loss such as psychological pains suffered, etc. in terms of customer damages. Therefore, it is imperative for the operational authentication to be confirmed previously in their access to the financial systems and in work operations.

The aim of this study is to analyze the methods of authentication and access controls for appropriate system operators.

키워드

금융정보시스템, 고객정보, 정당성, 접근통제

Ⅰ. 서 론

금융산업분야는 가계, 기업 및 정부 등 경제활동 수행주체인 금융거래고객과 직·간접적으로 연계됨은 물론 고객간 거래 관련 자금의 송·수신 과정에서 중개역할을 수행하는 중요 산업분야중의 하나이다. 고객간 자금거래를 중개하는 금융기관은 은행, 증권, 보험 및 신용카드사 등으로 세분화할 수 있다. 금융기관에서의 거래고객에 대한 다양한 금융서비스 제공은 고객정보를 중심으로 한 금융정보시스템을 기반으로 한다. 금융정보시스템에 대한 접근은 금융거래서비스를 제공받고자 시스템에 간접적으로 접근하는 고객 즉, 일반 사용자와 고객에게 금융서비스를 제공하기 위해 금융정보시스템에 직접 접속하여 정보시스템을 운영관리하는 운영주체 즉, 정보시스템 운영자로 구분할 수 있다.

금융정보시스템내 저장 및 운영관리되는 고객 관련 제반 정보는 유출시 직·간접 당사자에게 정신적 피해는 물론 막대한 금전적 손해를 입힐 수 있다. 따라서 금융기관의 금융정보시스템은 운영자의 정당성에 대한 사전확인이 필수적이며, 정당한 운영자에 한해 정보시스템 관련 작업을 수행토록 관련 규정[1,2]에 명시함은 물론 이를 정보시스템에 반영하여 운영관리하고 있다.

한편, 금융기관들은 다양한 고객정보의 안전관리에 많은 투자와 노력을 기울이고 있으나, 2013년의 농협 및 신한은행 등에서의 금융정보사고 발생과 2014년의 KB국민카드, NH농협 및 롯데 카

표 1. 금융정보시스템 관련 주요 컴플라이언스

구 분	주요 내용
금융시장 인프라에 관한 원칙 (PFMIs)	- 일반조직, 신용 및 유동성 리스크 관리, 결제, 중앙예탁기관과 가치 교환형 결제시스템, 채무불이행 관리, 일반사업 및 운영리스크 관리, 접근, 효율성, 투명성 등 9개분야 24개 원칙 - 원칙 17(운영리스크) : 정보시스템, 내부처리과정 및 인적자원의 결함 등으로 인한 서비스의 축소 또는 중단 리스크 → 운영 관리체계 구축, 방어체제 구축 및 운영방침, 절차 및 통제수단 등의 정기적 점검으로 운영리스크 줄이도록 정의
정보보호 관리체계 (ISMS)표준 (ISO/IEC 27001)	- 기업 보유 정보자산의 체계적·지속적 보호 - 관리과정 : ISMS의 수립, 구현 및 운영, 모니터 및 검토, 관리 및 개선 등으로 구성 - 통제 목록 : 통제분야, 통제목적 및 통제사항 - 통제 분야 : 관리적, 물리적, 기술적 통제 - 통제분야별 통제사항 . 인적보안 . 물리적·환경적 보안 : 출입통제 . 접근통제 : 시스템 및 사용자 통제
전자금융 감독규정 등	- 업무담당자 사용 단말기 보호 - 운영자(사용자)인증 등 정당성 확인 - 중요작업시 책임자 승인 등 이중확인 - 외부사용자의 최소한 작업권한 할당 - 사용자 계정의 개인별 부여 및 관리, 인가 여부 확인 - 정보시스템 접근·계정 사용권한·접근기록 통제관리용 추가 인증

드 등에서의 외주업체 직원에 의한 개인 정보유출사고 등이 빈번히 발생[1,2]하고 있다. 이러한 유형의 정보유출 사고는 금융정보시스템에 대한 접근권한의 획득 과정에서의 계정노출과 외부인 접속 허용 등으로 사고가 발생한 사례로써 정보시스템 접근에 대한 정당한 운영자의 접근통제가 무엇보다 중요함을 알 수 있는 대표적인 사례이다.

이에 본 연구에서는 지급결제제도위원회(CPSS-ISOCO)와 국제증권감독기구 기술위원회의 금융시장인프라에 관한 원칙(PFMIs, Principles for Financial Marcket Infrastructures)[3], 정보보호관리 체계(ISMS, Information Security Management System)표준인 ISO/IEC 27001[3], 전자금융감독규정 등[1,2]에서의 금융정보시스템 접근통제 원칙을 금융정보시스템 운영기관의 관리자 입장과 컴플라이언스 측면에서 분석하여, 금융정보시스템 운영자의 정당성을 확인하는 IT관점의 접근통제 기법에 대한 모델을 제시하고자 한다.

Ⅱ. 관련 연구

금융거래고객에게 서비스를 제공하기 위해 금융기관에서 운영관리하는 정보시스템은 금융거래고객이며 간접 접근자인 일반사용자와 금융정보시스템에 직접 접속하여 정보시스템을 운영관리하는 운영자로 구분할 수 있다. 금융정보시스템의 서비스 제공과 관련, 직·간접 접근자에 대한 통제관련 제반 컴플라이언스는 표 1과 같이 관련 주관기관에 따라 매우 다양한 형태로 요구되고 있다.[1,2,3]

따라서 본 연구에서는 금융정보시스템에 요구되는 다양한 컴플라이언스 관련 IT요소를 접근통제 관련 최적화 모델을 위한 기초자료로 사용하여 이를 충족시키는 모델을 제시하고자 한다.

Ⅲ. 금융정보시스템의 운영자 접근통제 모델

금융정보시스템의 직접 접근자인 운영자의 접근통제는 사전 등록된 정보를 이용하여 정당한 운영자임을 확인 및 인증하는 과정이다. 접근자의 정당성 확인 등 접근통제 수단[1,2,4]은 ID 및 패스워드, OTP(One Time Password), 지문 등 생체인식정보, 전자인증서, 스마트카드 등의 다양한 방식에 의해 수행된다. 금융정보시스템 운영자의 접근통제를 위해 사용되는 기술은 최근 들어 다양한 관련기술을 상호 연계 및 조합하여 사용함으로써 정보시스템 운영관리의 안전성이 강화되도록 하는 추세이다.

금융기관의 정보시스템 운영관련 감독기관에서는 금융거래고객에게 제공되는 서비스의 투명성 제고는 물론 정보시스템 운영의 안전성 강화를 지속적으로 요구하고 있다.[1,2] 이에 따라 금융정보시스템 운영관련 다양한 컴플라이언스[1,2,3]가 제공됨에도 불구하고 표준으로 적용할 만한 수준의 금융정보시스템 접근통제 모델에 대한 조사 및 연구는 다소 부족한 실정이다.

다양한 컴플라이언스 요소의 요구 내용을 IT관점에서 분석한 결과, 금융정보시스템의 운영자 접근통제 관련 IT요소별 모델은 표 2와 같은 요건을 충족하여야 한다.

본 연구에서는 다양한 컴플라이언스 요소에 기초한 금융정보시스템의 운영자 접근통제 관련 IT요소별 모델의 충족을 전제로 그림 1과 같은 운영자 접근 통제 모델을 제시한다.

Ⅳ. 결론 및 향후 연구과제

다양한 금융거래고객에게 안전한 금융거래서비스를 제공하기 위해 금융기관에서 운영관리하는 금

표 2. 접근통제 컴플라이언스 관련 IT요소별 모델 요건

구 분	내 용	비 고
금융정보 시스템	금융거래고객의 금융서비스 제공을 위해 사용하는 기반 시스템	
일반 사용자	금융서비스를 제공받고자 하는 금융거래 고객	
운영자 · 계정	- 정보시스템을 운영관리하는 사람 - 정보시스템 접속 목적에 따라 개인에게 부여되는 계정	전자금융감독규정
사용 단말	- 사용단말을 중요단말기로 지정, 운영 - 단말 사용자의 사전 인가 · 인가자에 한해 사용 허용	전자금융감독규정
운영자 인증	비밀번호, 보안토큰, 스마트카드, OTP, 생체인식, IC카드 등	금융전산분야 종합대책
접근 권한 · 통제	- 접근통제 수단(물리적, 기술적, 관리적) 강구 및 점검 - 본인 확인 및 접근권한 수단 강구	PFMIs, ISO/IEC 27001 전자금융감독규정 금융전산분야 종합대책
중요 작업 수행 승인	정보시스템에 영향 미치는 중요작업시 관리자 등 승인	전자금융감독규정
시스템 접근 기록	- 정보시스템 사용자의 접근기록 유지 및 관리 - 사후 추적감사용 등으로 사용	전자금융감독규정 금융전산분야 종합대책

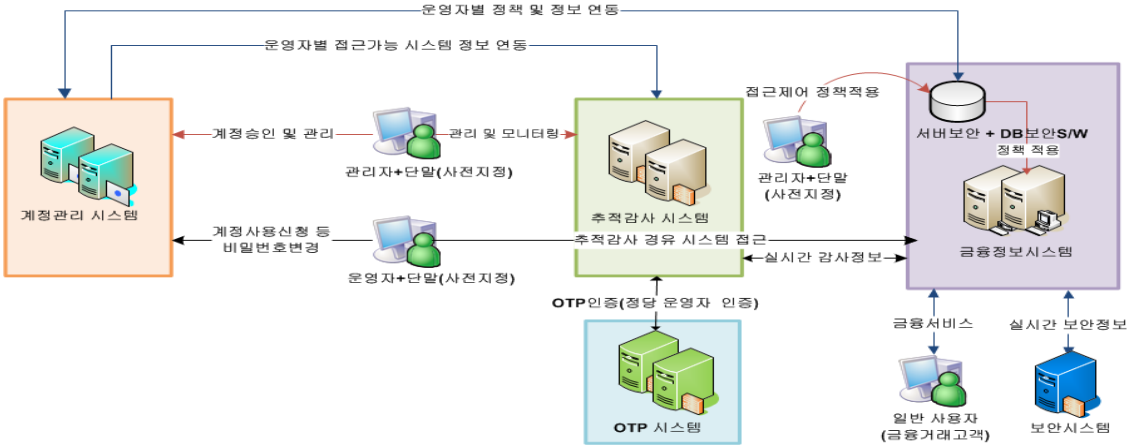

그림 1. 금융정보시스템 운영자 접근통제 모델

융정보시스템은 다양한 관련 컴플라이언스가 존재한다. 그럼에도 불구하고 표준적으로 적용할 만한 수준의 금융정보시스템 운영자관점의 접근통제 모델관련 조사 및 연구는 부족한 실정이다.

따라서 본 연구에서는 이러한 현재의 금융정보시스템 운영 상황을 고려하고, 다양한 컴플라이언스 요소를 충족시키는 정보시스템 운영자관점의 접근통제 관련 IT요소별 모델 요건을 표 2와 같이 정의하였다.

또 이에 기반하여 금융정보시스템 운영자 접근통제 모델을 제시하여 금융정보시스템 운영의 안전성을 강화코자 하였다.

그러나 금융정보시스템 운영의 안전성 강화는 특정 기술요소의 단일 구현으로 충족되는 것이 아닌 관련 다양한 기술요소들이 상호 연계하여 적용되었을 때 안전성을 한층 강화할 수 있다. 또한 금융정보시스템의 접근 경로가 매우 다양하다는 점을 고려할 때 다양한 접근경로에 대한 통제도 동시에 고려되어야 하며, 정보시스템 운영자의 접근통제 강화를 통한 운영관리의 안전성만을 강조함에 따른 정보시스템 자원 사용의 효율성 저하를 해소하기 위한 연구도 반드시 고려되어야 한다.

참고문헌

[1] 금융위원회, 전자금융감독규정, 2013
[2] 금융위원회, 금융분야 개인정보 유출 재발방지 종합대책, 2014. 3
[3] 금융결제원, 지급결제와 정보기술. 2012. 10
[4] 김상욱, 스마트단말도입시 보안통제 수준 향상에 관한 실증적 연구, 박사학위연구, 2011.