2채널을 이용한 강화된 내부 사용자 인증모델에 대한 연구

이재윤* · 심호성** · 김종배***

*금융결제원 · **(사)한국공개소프트웨어협회 · ***숭실대학교

A Study on the Models of an enhanced Internal system users Authentication using two channel

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

*Korea Financial Telecommunications & Clearings Institute

E-mail : jae_yun_lee@kftc.or.kr

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

Ⅰ. 서 론

지급결제서비스를 제공하기 위한 금융기관의 금융정보시스템은 정보통신기술의 지속적인 발전과 더불어 전화, PC, 스마트폰 등 전자금융거래 이용매체의 다양화로 인해 보안위협 등이 지속적으로 증가하고 있다.

정보통신기술의 발전에 따른 전자금융거래의 확산은 금융거래고객에게 편리성을 제공해 주는 잇점이 있는 반면, 서비스 처리과정의 보안 취약점을 이용한 보안위협과 전자금융사고의 발생가능성등이 상시 존재한다.[5] 이러한 전자금융거래 환경의 기본사항은 전자금융거래 서비스 이용자와 제공자에 대한 본인확인을 수행하는 것이다. 따라서 금융기관은 보안 취약점의 제거와 금융정보 유출방지 및 정당한 본인확인에 많은 투자와 노력을 기울이고 있다. 그럼에도 불구하고 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 접근에 대한 정당 사용자의 확인이 무엇보다 중요함을 알 수 있는 사례이다.

국가정보원 산업기밀보호센터가 제공한 2015년 자료에 따르면 정보기술 유출 주체중 전직 직원 52.8%, 현직 직원 27.1% 등 내부자에 의한 정보유출이 79.9%에 달하고 있다. 이는 기술가치 인지 및 기술에 대한 접근권한이 있는 내부자에 의한 유출이 대다수임을 알 수 있다.[4]

이에 본 연구에서는 2채널을 이용한 강화된 내부 사용자 인증모델의 제시를 위해 선행연구로써 정당사용자 인증기술수단과 조건 및 관련 컴플라이언스를 분석하여 금융정보시스템 내부 사용자의 정당성을 확인하는 모델을 제시하고자 한다.

Ⅱ. 관련 연구

금융기관의 금융정보시스템 보안영역은 관리적, 기술적, 물리적 영역 등 크게 3분야로 구분할 수 있다. 기술분야 보안영역은 네트워크, 정보시스템, 데이터, DB보안 및 단말기(PC)로 세분화할 수 있다. 본 논문에서 제시하는 사용자 인증모델은 기술분야 영역으로 금융정보시스템 관점의 접속주체는 금융거래고객인 서비스 이용자와 정보시스템을 운영 및 관리하는 내부 사용자로 구분할 수 있다. 금융정보시스템 내부 사용자는 접속 목적, 이용 매체, 역할 및 기능에 따라 다음과 같이 구분할 수 있다. 시스템의 최상위 권한으로 시스템에 접속하는 루트 관리자 계정접속, DBMS 및 데이타 등의 관리를 위한 DB관리자 계정접속, 업무운영을 위한 운영자 계정접속, 시스템 관리도구 등을 통한 시스템 접속, 콘솔을 통한 시스템 접속, 프로그램을 통한 접속, 시스템간 접속 등이 있다.

전자금융거래의 사용자는 직접 대면이 불가하다는 특성으로 인해 금융기관이 요구하는 비밀정보를 제시하므로써 자신이 정당한 사용자임을 증명한다. 본인 확인기술로써 사용하는 인증수단은 다음 표 1과 같이 4가지로 구분할 수 있다.[5]

표 1. 사용자 인증기술 수단

구분	내용	사용예
지식 기반	자신만이 알고 있는 비밀정보	ID, 비밀번호, OTP, 주민등록번호
소유 기반	자신이 소유하고 있는 비빌정보	IC카드, 공인인증서
생체 기반	개인의 생체정보	지문,홍채,음성,얼굴
제 3자 인증	공인인증기관 등	-

이러한 사용자 인증기술 수단은 다양하게 존재함에도 불구하고 실제 사용은 널리 적용되지 못하고 있다. 정보시스템 내외부 사용자의 다양한 인증기술수단 사용에 대한 어려움 해소와 적용 확산을 위해 인증수단은 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 인증수단 적용을 위한 도입비용이 저렴해야 한다. 넷째 인증수단은 금융기관이 인증기술을 신뢰할 수 있어야 하며, 사용자와 금융기관간 상호 인증 등 양방향으로 작동하는 인증기술 제공으로 적절한 보안등급을 보장해야 한다. 다섯째 인증수단은 금융기관의 보안체계, 응용소프트웨어 및 웹사이트와 손쉽게 통합 및 확장 가능하는 등 손쉽게 관리될 수 있어야 한다. 마지막으로 인터넷을 통한 사용자 인증수단 배포시 PC, 핸드폰, POS(Point of

표 2. 금융정보시스템 사용자 인증관련 컴플라이언스

구 분	주요 내용
금융시장 인프라에 관한 원칙(PFMIs)	- 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/IEC27001)	- 관리과정 : 체계 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
정보보호 관리체계 (K-ISMS)	- 통제 분야 : 관리적, 물리적, 기술적 통제 - 통제분야별 통제사항 : 외부자 및 인적보안 . 물리적보안 . 접근통제 : 정책수립과 접근통제관리 . 모니터링 및 감사 : 정보자산 모니터링 및 보안 감사 수행
전자금융 감독규정 등	- 업무담당자 사용 단말기 보호 - 사용자(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

Sales) 등 다양한 통신채널에서 작동되어야 한다.[5, 9]

금융기관의 금융정보시스템 관련 내외부 접근자에 대한 제반 컴플라이언스는 표 2와 같이 관련 주관기관에 따라 매우 다양한 형태로 요구되고 있다.[3, 6, 7, 8]

따라서 본 연구는 금융정보시스템에 요구되는 다양한 컴플라이언스 관련 IT요소를 사용자 인증 관련 최적화 모델을 위한 기초자료로 사용하여 이를 충족시키는 모델을 제시하고자 한다.

Ⅲ. 내부 사용자 인증 모델

금융정보시스템 내외부 사용자 인증에 사용되는 수단은 매우 다양하며, 가장 많이 쓰이는 인증수단으로 ID와 비밀번호가 있다. 인증[1, 2]은 사용자 자신이 알고 있는 비밀번호를 금융거래서비스 과정에서 입력하므로써 정당한 사용자임을 인증받는 것이다. 이와 같이 한가지요소만 이용한 사용자인증이 단일 요소인증(Single Factor Authentication)으로 사용된 비밀번호는 단일 요소 인증수단이 된다. 이중요소인증(Two Factor Authentication)은 2개 이상의 인증수단을 이용하여 사용자 인증을 수행한다. 한 개의 수단만 사용하는 단일 요소인증 대비 2개 이상의 인증수단을 사용하는 다중 요소인증(Multi Factor Authentication)의 보안성이 높은 것은 당연하다.[5]

따라서 최근의 전자금융거래는 보안성 강화를 위해 대부분 2요소 이상의 인증수단 사용을 권고함에 따라 금융기관은 서비스 거래종류에 따른 다중요소 인증수단을 도입하여 적용중이다. 대부분 금융기관은 중요 금융서비스에 추가 인증수단을 적용하는 추세이다. 온라인 계좌이체에서 다양한 인증수단중 OTP인증수단이 가장 많이 이용되며, 거래를 실행하는 채널과 물리적으로 분리된 다른 채널을 이용하는 2채널 인증방법을 일반적으로 이용한다.[5]

본 연구는 다양한 컴플라이언스 요소의 요구내용을 IT관점에서 분석한 결과, 금융정보시스템의 내부 사용자 인증관련 IT요소별 모델은 표 3[3, 6, 7, 8]와 같은 요건을 충족하여야 하며, 관련 사용자 인증모델을 표 4와 같이 제시한다. 제시한 모델은 내부 시스템 사용자의 시스템 접근시 정당 사용자 확인을 위해 ID/비밀번호와 OTP 등 2채널을 이용하여 보안성을 강화하도록 설계 및 구현하였다. 또한 정보시스템 내부 사용자의 정보시스템 접근시 본인확인 인증강화를 위해 작업수행에 따른 중요도에 따라 인증방법을 차등화

표 3. 컴플라이언스 관련 내부 사용자 인증 모델 요건

구 분	내 용	컴플라이언스	모델 구성요소
금융정보시스템	금융거래고객에게 금융서비스를 제공하기 위해 사용하는 시스템	-	접근대상 정보시스템
서비스 이용자	금융서비스를 제공받고자 하는 금융거래 고객	-	금융 서비스 이용자
사용자·계정	- 정보시스템의 운영관리자 - 정보시스템 접속 목적에 따라 개인에게 부여	전자금융감독규정, 행정기관 정보시스템 접근권한 관리 규정	계정관리시스템 추적감사시스템 비밀번호관리시스템 정보시스템 내부 사용자
사용단말(PC)	- 사용단말을 중요단말기로 지정, 운영 - 단말 사용자의 사전 인가·인가자에 한해 사용 허용	전자금융감독규정, 행정기관 정보시스템 접근권한 관리 규정	PC
사용자 인증	비밀번호, 보안토큰, 스마트카드, HSM, OTP, 생체인식, IC카드	금융전산분야 종합대책, 행정기관 정보시스템 접근권한 관리 규정	ID/비밀번호, OTP 서버보안시스템
접근권한·통제	- 접근통제 수단(물리적, 기술적, 관리적) 강구 - 본인 확인 및 접근권한 수단 강구	PFMIs, ISO/IEC 27001, K-ISMS 전자금융감독규정, 금융전산분야 종합대책, 행정기관 정보시스템 접근권한 관리 규정	-
중요작업 수행승인	정보시스템에 영향 미치는 중요작업시 관리자 등 승인	전자금융감독규정	추적감사시스템 OTP 서버보안시스템
시스템 접근 및 활동기록	- 정보시스템 사용자의 접근과 수행활동 기록 유지 및 관리 - 사후 추적감사용 등으로 사용	전자금융감독규정, 금융전산분야 종합대책, 행정기관 정보시스템 접근권한 관리 규정	추적감사시스템 정보시스템 서버보안시스템

하도록 정보시스템을 설계, 구현하였다.

내부 사용자는 금융정보시스템에 접속하기 위해 ①사용자, ②단말(PC), ③계정관리시스템, ④추적감사시스템, ⑤비밀번호관리시스템, ⑥OTP시스템, ⑦방화벽, ⑧서버보안시스템 및 ⑨접속대상시스템 등 관련시스템의 접근에 필요한 계정 및 제반 정보를 사전 등록토록 하므로써 안전성을 강화하였다. 또한 관련 정보시스템을 상호 연계하여 관련 정보를 사전 공유하므로써 시스템 운영의 안정성을 강화하였다.

내부시스템 사용자가 시스템에 접속하여 단순작업시 ①②④⑥⑦⑧⑨ 및 작업수행의 순서로 작업할 수 있도록 구현하였다. 시스템의 Shutdown 등 시스템에 중대한 영향을 미치는 중요작업을 수행할 경우 안정성 확보 및 강화를 위해 ①②④⑥⑦⑧⑨에 부가하여 ⑤⑨⑧ 및 중요작업 수행 명령어 입력, ④⑥④⑨⑧ 및 중요작업 수행 명령어 실행 등으로 작업이 수행되도록 구현하였다.

금융관련 감독기관에서는 금융서비스의 투명성 제고는 물론 정보시스템 운영의 안전성 강화를 지속적으로 요구하고 있다.[7, 8] 이와 같은 다양한 컴플라이언스[3, 6, 7, 8]가 요구됨에도 불구하고 표준으로 적용할 만한 수준의 금융정보시스템 내부 사용자 인증모델에 대한 조사 및 연구는 다소 부족한 실정이다. 다양한 컴플라이언스 요구내용을 기초로 금융정보시스템 내부 사용자 인증모델은 표 3의 모델요건을 충족하여야 한다.

본 연구에서는 다양한 컴플라이언스 요소에 기초한 금융정보시스템 내부 사용자 인증모델의 충족을 전제로 표 4와 같이 내부 사용자 인증모델을 제시한다.

Ⅳ. 결론 및 향후 연구과제

금융기관 정보시스템은 안전한 금융서비스 제공 및 안정적 운영을 위해 다양한 컴플라이언스가 존재한다. 기술분야 보안영역은 정당 서비스 이용자관점의 컴플라이언스 충족을 위해 다양한 접근정책 및 연구들이 활발히 진행되고 있으나, 내부 시스템 사용자 인증을 위한 모델관련 조사 및 연구는 부족한 실정이다.

따라서 본 연구는 이러한 현재의 금융정보시스템 운영상황을 고려하고, 다양한 컴플라이언스 요구를 충족시키는 금융정보시스템 내부 사용자관점의 인증모델 요건을 표 3[3, 6, 7, 8]과 같이 정의하였다. 모델 요건 정의를 기반으로 금융정보시스템 사용자 인증모델을 표 4와 같이 제시하여 시스템 운영의 안전성을 강화코자 하였다.

그럼에도 불구하고 금융정보시스템 관점의 내외부 사용자 접근은 서비스 이용자, 시스템 관리자 및 운영자, DB관리자, 콘솔 접속, 프로그램 및 시스템 관리도구를 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 접근용이성 및 사용 편의성, 휴대성, 소요 및 구축비용 등 경제성, 정보시스템 자원 사용의 효율성 등에 대한 연구가 다소 부족함에 따라 동 요소들이 고려되어 추진되어야 한다.

표 4. 금융정보시스템 내부 사용자 접근절차 및 모델

구분		인증절차	인증횟수	비고
사전 등록		①→②→③→④→⑤→⑥→⑦→⑧→⑨	9번	금융정보시스템 접근(업무수행)이전
금융 정보시스템 접근	단순작업 수행시	①→②→④→⑥→⑦→⑧→⑨→작업수행	7번	
	중요작업 수행시	①②④⑥⑦⑧⑨ + ⑤→⑨→⑧ + 중요작업 수행 명령어 입력 + ④→⑥→④→⑨→⑧ + 중요작업 수행 명령어 실행	16번	

참고문헌

[1] 윤승구, OTP를 이용한 인터넷뱅킹 시스템의 보안 강화 기법, 석사학위 연구, 2010.

[2] 정철우, 공인인증서 부정사용방지를 위한 사용자 단말인증시스템에 대한 실증적 연구, 박사학위연구, 2012.

[3] 국무총리훈령, 행정기관 정보시스템 접근권한 관리 규정 2013. 4

[4] 국가정보원, 산업기밀보호센터

[5] 금융결제원, 지급결제와 정보기술 pp. 119-139. 2007.1

[6] 금융결제원, 지급결제와 정보기술, 2012.10

[7] 금융위원회, 전자금융감독규정, 2013

[8] 금융위원회, 금융분야 개인정보 유출 재발방지 종합대책, 2014. 3

[9] Jonathan Penn, What To Look In Consumer Strong Authentication Solutions, Forrester, 2005.3