Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.919

오픈소스 기반 분산원장기술 시스템을 위한 보안 강화 방안*

박 근 덕,[1†] 김 대 경,[2] 염 흥 열[2‡]
[1]서울외국어대학원대학교, [2]순천향대학교

Security Enhancements for Distributed Ledger Technology Systems Based on Open Source*

Keundug Park,[1†] Dae Kyung Kim,[2] Heung Youl Youm[2‡]
[1]Seoul University of Foreign Studies, [2]Soonchunhyang University

요 약

4차 산업 혁명 관련 신흥 기술로 주목받고 있는 분산원장기술은 오픈소스 기반 분산원장기술 시스템(또는 분산원장기술 플랫폼)으로 구현되어 다양한 애플리케이션(또는 서비스) 개발 시 널리 활용되고 있으나, 오픈소스 기반 분산원장기술 시스템에서 제공하는 보안 기능은 매우 미흡한 실정이다. 본 논문에서는 오픈소스 기반 분산원장기술 시스템 운용 시 발생할 수 있는 잠재적인 보안 위협을 식별하고, 국내 법규 및 보안 인증 기준(ISMS-P, Information Security Management System-Privacy)을 분석하여 보안 위협에 대응할 수 있는 보안기능 요구사항을 도출한다. 그리고 국제 표준인 공통평가기준(CC, Common Criteria)의 보안기능 컴포넌트 분석을 통하여 오픈소스 기반 분산원장기술 시스템에 필요한 보안 기능을 구현할 수 있는 방안을 제안함으로서 보안을 강화하고자 한다.

ABSTRACT

Distributed ledger technology, which is attracting attention as an emerging technology related to the 4th Industrial Revolution, is implemented as an open source based distributed ledger technology system and widely used for development with various applications (or services), but the security functions provided by the distributed general ledger system are very insufficient. This paper proposes security enhancements for distributed ledger technology systems based on open source. To do so, potential security threats that may occur under running an open source based distributed ledger technology systems are identified and security functional requirements against the security threats identified are provided by analyzing legislation and security certification criteria (ISMS-P). In addition, it proposes a method to implement the security functions required for an open source based distributed ledger technology systems through analysis of security functional components of Common Criteria (CC), an international standard.

Keywords: security, blockchain, distributed ledger technology (DLT) system, open source, blockchain platform, common criteria, security function

Received(05. 13. 2019), Accepted(07. 04. 2019)
* 본 논문은 과학기술정보통신부와 정보통신기획평가원이 지원하는 '차세대 ICT 환경에서의 보안 및 개인정보보호 기술 국제 표준화 추진' 사업의 일환으로 수행되었음 (과제번호: 20190006600012004)
† 주저자, jacepark926@gmail.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

I. 서 론

4차 산업 혁명 관련 신흥 기술로 주목받고 있는 분산원장기술(DLT)은 오픈소스(Open source) 기반 분산원장기술 시스템(또는 플랫폼)으로 구현되어 다양한 애플리케이션(또는 서비스) 개발 시 널리 활용되고 있다. 최근 과학기술정보통신부와 한국인터넷진흥원(KISA)은 블록체인 발전전략(2018)의 일환으로 민간주도 국민프로젝트를 추진하여 탈중앙화 기부 플랫폼, 블록체인 기반 중고차 서비스 플랫폼 개발, 블록체인 ID/인증 네트워크 기반 금융, 통신, 교육 분야, 서비스 개발 및 응용확산 등 3개 과제를 선정하였고 2020년도에 각 사업자를 통하여 시범 서비스를 운영할 계획이다. 또한 국민들이 체감할 수 있고 편익이 높은 6개 분야에서 블록체인 공공분야 시범사업을 - 온라인 투표 시스템(중앙선거관리위원회), 전자문서 발급 인증 시스템(외교통상부), 축산물 이력관리 시스템(농림축산식품부), 부동산 거래 시스템(국토교통부), 해외 직구를 위한 개인 통관 시스템(관세청), 해운물류 시스템(해양수산부) - 행정기관 등과 진행하고 있다. 그리고 다수의 기업들도 국가간 송금 시스템, 지역화폐(또는 모바일상품권) 거래 시스템, 온라인 지급결제 시스템 등 분산원장기술을 활용한 다양한 서비스를 개발 및 운영하고 있다.

앞에서 살펴본 바와 같이 공공 및 민간 분야에서 개발 및 운영하는 각종 서비스는 대부분 오픈소스 기반 분산원장기술 시스템(또는 플랫폼)(예: 하이퍼레저 패브릭, 이더리움 등)을 활용하고 있다. 이용자에게 제공되는 분산원장기술 기반 서비스는 기존의 중앙화된 시스템(Non-DLT system)과 분산원장기술 시스템을 포함하고 있어 서비스 운영 시 분산원장기술 시스템에서 발생할 수 있는 보안 위협 식별 및 대응이 절실히 필요하다.

따라서 본 논문에서는 오픈소스 기반 분산원장기술 시스템의 보안 강화를 위하여 제2장에서는 오픈소스 기반 분산원장기술 시스템에서 제공하는 보안 기능과 국내외 보안 관련 법규 및 인증 기준을 분석한 내용을 설명한다. 제3장에서는 이용자에게 서비스를 제공하기 위한 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 잠재된 보안 위협을 식별하고, 제4장에서는 제3장에서 식별한 보안 위협에 대응할 수 있는 보안기능 요구사항을 제안한다. 마지막으로 제5장에서는 향 후 연구 방향과 결론을 설명한다.

II. 관련 연구

본 장에서는 오픈소스 기반 분산원장기술 시스템에서 제공하는 보안 기능과 국내외 보안 관련 법규 및 인증 기준을 분석한 내용을 설명한다.

2.1 오픈소스 기반 분산원장기술 시스템

본 절에서는 오픈소스 기반 분산원장기술 시스템 중 대표적으로 널리 활용되고 있는 하이퍼레저 패브릭과 이더리움에서 기본적으로 제공하고 있는 보안 기능을 설명한다.

2.1.1 하이퍼레저 패브릭

하이퍼레저 패브릭(Hyperledger Fabric)은 리눅스 재단(Linux Foundation)에서 개발 및 유지 관리하고 있는 오픈소스 기반 분산원장기술 시스템으로서 허가형(Permissioned, Private) 분산 원장 네트워크와 스마트 계약(체인 코드)을 제공하는 것이 특징이다.[10]

하이퍼레저 패브릭에서 제공하는 보안 기능은 데이터 무결성, 신원 관리, 접근 통제, 암호화 등이 있다. 데이터 무결성 기능은 분산 원장에 저장된 거래 데이터에 대한 무결성을 검사하는 기능을 제공한다. 신원 관리 기능은 아이디(ID) 또는 시스템 개체(Entities)의 등록, 변경 및 삭제 기능과 인증 및 권한 부여 기능을 제공한다.[11] 접근 통제 기능은 분산 원장 네트워크를 채널 단위로 분리하여 각 채널에 대한 참여자의 접근을 통제할 수 있고, 또한 스마트 계약(체인 코드) 코딩을 통해 구현함으로서 프라이빗(Private) 데이터에 대한 접근을 통제할 수 있다. 암호화 기능은 프라이빗 데이터를 일방향 암호화(예: 해쉬) 또는 양방향 암호화를 할 수 있다. 또한 피어(Peer)에서 파일시스템 암호화를 통해 분산 원장 데이터를 암호화 할 수 있고, 피어 간 전송 구간 암호화는 전송 계층 보안 프로토콜(TLS, Transport Layer Security)을 활용하여 암호화 할 수 있다.[12]

2.1.2 이더리움

이더리움(Ethereum)은 이더리움 재단(Ethereum Foundation)에서 개발 및 유지 관리

하고 있는 오픈소스 기반 분산원장기술 시스템으로서 허가형(Private, Consortium) 및 비허가형(Public) 분산 원장 네트워크와 스마트 계약(Smart Contract)을 제공하는 것이 특징이다.[13]

이더리움에서 제공하는 보안 기능은 데이터 무결성, 신원 관리 등이 있다. 데이터 무결성 기능은 분산 원장에 저장된 거래 데이터에 대한 무결성을 검사하는 기능을 제공한다. 신원 관리 기능은 일반 계정(externally owned accounts)과 계약 계정(contract accounts)으로 구분된 계정을 등록, 변경 및 삭제하는 기능을 제공한다.[14]

2.2 법규에 근거한 보안 요구사항

본 절에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 시행령, 「개인정보 보호법」 및 시행령, 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회고시 제2015-3호), 「개인정보의 안전성 확보조치 기준」(행정안전부고시 제2017-1호), 「전자금융감독규정」(금융위원회고시 제2018-36호), 「전자정부법」 및 시행령 등 국내 법규에 근거하여 정보시스템에서 중요 정보 처리 시 안전성 확보에 필요한 기술적 보안 요구사항에 대하여 설명한다.

2.2.1 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 시행령

본 절에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 시행령에 근거하여 정보통신서비스 제공자가 개인정보 파기 시 필요한 기술적 보안 요구사항에 대하여 설명한다.[1]

법 제29조(개인정보의 파기) ① 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다. 〈개정 2012. 2. 17., 2014. 5. 28.〉

1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우
3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집·이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우
4. 사업을 폐업하는 경우

② 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다.

시행령 제16조(개인정보의 파기 등) ② 정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다. 다만, 법 제29조제2항 본문에 따른 기간(법 제29조제2항 단서에 따라 이용자의 요청에 따라 달리 정한 경우에는 그 기간을 말한다)이 경과한 경우로서 다른 법령에 따라 이용자의 개인정보를 보존하여야 하는 경우에는 다른 법령에서 정한 기간이 경과할 때까지 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

2.2.2 개인정보 보호법과 시행령

본 절에서는 「개인정보 보호법」 및 시행령에 근거하여 개인정보처리자가 개인정보 파기 시 필요한 기술적 보안 요구사항에 대하여 설명한다.[2]

법 제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치

하여야 한다.
③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.
시행령 제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다. 〈개정 2014. 8. 6.〉
1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제

2.2.3 개인정보의 기술적·관리적 보호조치 기준

본 절에서는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회고시 제2015-3호)에 근거하여 정보통신서비스 제공자가 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 및 훼손되지 않도록 안전성 확보에 필요한 기술적 보안 요구사항에 대하여 설명한다.[1][3]

제4조(접근통제) ① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.
② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
③ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.
④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.
⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.
1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
⑦ 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.
⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.
1. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경
⑨ 정보통신서비스 제공자등은 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.
⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.
제5조(접속기록의 위·변조방지) ① 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다.
제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.
② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.
1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 바이오정보

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

제9조(출력·복사시 보호조치) ① 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

제10조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다.

2.2.4 개인정보의 안전성 확보조치 기준

본 절에서는 「개인정보의 안전성 확보조치 기준」(행정안전부고시 제2017-1호)에 근거하여 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적 보안 요구사항에 대하여 설명한다.[2][4]

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를

암호화하여야 한다.
④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.
③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.
제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

2.2.5 전자금융감독규정

본 절에서는 「전자금융감독규정」(금융위원회고시 제2018-36호)에 근거하여 금융 회사의 정보기술부문 안전성 확보 등을 위하여 필요한 기술적 보안 요구사항에 대하여 설명한다.[5]

제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.
1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것
② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.
③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회 내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.
④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.
1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
3. 정보처리시스템 내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록
제14조(정보처리시스템 보호대책) 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다.
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것
제15조(해킹 등 방지대책) ① 금융회사 또는 전

자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것
② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

제25조(정보처리시스템의 성능관리) 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.

제27조(전산원장 통제) ⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다.

제31조(암호프로그램 및 키 관리 통제) ② 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.

제32조(내부사용자 비밀번호 관리) 2. 비밀번호는 다음 각 목의 사항을 준수할 것
가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경
나. 비밀번호 보관 시 암호화
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

제33조(이용자 비밀번호 관리) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다.
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)

제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.
1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)
3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.
5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

제37조(인증방법 사용기준) 금융회사 또는 전자금융업자는 전자금융거래의 종류·성격·위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.

제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.
2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지

3. 계좌번호, 비밀번호 등 이용자 금융정보 무단 보관 및 유출 금지
4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립

2.2.6 전자정부법 및 시행령

본 절에서는 「전자정부법」 및 시행령에 근거하여 행정기관이 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 필요한 기술적 보안 요구사항에 대하여 설명한다.[6][7]

법 제56조(정보통신망 등의 보안대책 수립·시행) ③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.
시행령 제69조(전자문서의 보관·유통 관련 보안조치) ① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.
1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용

2.3 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증 기준

본 절에서는 「정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증 기준」에 근거하여 기업이 주요 정보자산을 보호하기 위하여 필요한 기술적 보안 요구사항에 대하여 설명한다.[8]

(2.5.2 사용자 식별) 사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
(2.5.3 사용자 인증) 정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
(2.5.4 비밀번호 관리) 법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
(2.6.1 네트워크 접근) 네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.
(2.6.3 응용프로그램 접근) 사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
(2.6.4 데이터베이스 접근) 테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
(2.6.6 원격접근 통제) 보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
(2.7.1 암호정책 적용) 개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
(2.7.2 암호키 관리) 암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.
(2.9.2 성능 및 장애관리) 정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.
(2.9.4 로그 및 접속기록 관리) 서버, 응용프로

그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.

(2.9.6 시간 동기화) 로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.

(2.10.4 전자거래 및 핀테크 보안) 전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위해 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.

(2.10.5 정보전송 보안) 타 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통해 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.

(2.10.8 패치 관리) 소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.

(3.1.1 개인정보 수집 제한) 개인정보는 서비스 제공을 위하여 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.

(3.1.2 개인정보의 수집 동의) 개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.

(3.1.3 주민등록번호 처리 제한) 주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.

(3.1.4 민감정보 및 고유식별정보의 처리 제한) 민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체(이용자)의 별도 동의를 받아야 한다.

(3.2.3 개인정보 표시제한 및 이용 시 보호조치) 개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무상 반드시 필요하지 않은 개인정보는 삭제하거나 또는 식별할 수 없도록 조치하여야 한다.

(3.2.4 이용자 단말기 접근 보호) 정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.

(3.4.1 개인정보의 파기) 개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.

(3.4.2 처리목적 달성 후 보유 시 조치) 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.

(3.4.3 휴면 이용자 관리) 서비스를 일정기간 동안 이용하지 않는 휴면 이용자의 개인정보를 보호하기 위하여 관련 사항의 통지, 개인정보의 파기 또는 분리보관 등 적절한 보호조치를 이행하여야 한다.

2.4 공통평가기준

국제 표준(ISO/IEC 25408)인 공통평가기준(CC, Common Criteria)은 IT 제품의 보안성을 평가하기 위한 공통 기준이다. 국내에서는 정책기관(과학기술정보통신부), 인증기관(IT보안인증사무국), 인정기관(국가기술표준원), 평가기관 등으로 평가·인증 체계를 구성하고, 「정보보호시스템 공통평가기준」(미래창조과학부고시 제2013-51호)에 따라 정보보호시스템 및 IT 제품의 보안성을 평가 및 인증하고

있다. 공통평가기준은 1부(소개 및 일반모델), 2부(보안기능요구사항) 및 3부(보증요구사항)로 구성되어 있고, 본 절에서는 제2부(보안기능요구사항)에 근거하여 클래스, 패밀리, 컴포넌트로 구성된 보안기능 요구사항을 설명한다.

(약어)
SFP : Security Function Policies (보안기능 정책)
SFR : Security Functional Requirements (보안기능요구사항)
TOE : Target of Evaluation (평가대상)
TSF : TOE Security Functionality (평가대상의 보안기능성)

2.4.1 보안감사 클래스

보안감사(FAU, Security audit) 클래스는 보안 관련 행동(즉, TSF에 의하여 통제되는 모든 행동)에 관련된 정보의 인식, 기록, 저장, 분석을 포함한다. 감사 레코드 결과는 어떤 보안 관련 행동이 발생했으며, 누가(어떤 사용자가) 이에 대한 책임이 있는가를 결정할 때 활용될 수 있다.[9]

○ 보안감사 자동대응(FAU_ARP, Security audit automatic response) 패밀리는 잠재적인 보안 위반을 암시하는 사건을 탐지한 경우에 취해야 할 대응행동을 정의한다.

FAU_ARP.1 보안 경보(Security alarms)에서, TSF는 잠재적인 보안 위반이 탐지되는 경우 대응행동을 취해야 한다.

○ 보안감사 데이터 생성(FAU_GEN, Security audit data generation) 패밀리는 TSF 통제하에서 발생하는 보안관련 사건의 발생을 기록하는 요구사항을 정의한다.

FAU_GEN.1 감사 데이터 생성(Audit data generation)은 감사대상 사건의 수준을 정의하고, 각 레코드에 기록해야 할 데이터의 목록을 지정한다.
FAU_GEN.2 사용자 신원 연관(User identity association)에서, TSF는 감사대상 사건과 개별 사용자 신원을 연관시켜야 한다.

○ 보안감사 검토(FAU_SAR, Security audit review) 패밀리는 인가된 사용자가 감사 데이터 검토에 이용할 수 있는 감사 도구에 관한 요구사항을 정의한다.

FAU_SAR.1 감사 검토(Audit review)는 감사 레코드의 정보를 읽을 수 있는 기능을 제공한다.
FAU_SAR.2 감사 검토 권한 제한(Restricted audit review)은 FAU_SAR.1에서 식별된 사용자를 제외하고는 정보를 읽을 수 없도록 할 것을 요구한다.
FAU_SAR.3 선택 가능한 감사 검토(Selectable audit review)는 감사 검토 도구가 검토될 감사 데이터를 기준에 기반하여 선택할 수 있는 기능을 요구한다.

○ 보안감사 사건 선택(FAU_SEL, Security audit event selection) 패밀리는 모든 감사대상 사건 집합으로부터 TOE의 운영 중에 감사되어야 할 사건 집합을 선택하기 위한 요구사항을 정의한다.

FAU_SEL.1 선택적인 감사(Selective audit)는 보호프로파일/보안목표명세서 작성자가 명세한 속성에 기초하여, FAU_GEN.1 감사 데이터 생성에서 식별된 모든 감사대상 사건 집합으로부터 감사되어야 할 사건의 집합을 선택할 수 있는 기능을 요구한다.

○ 보안감사 사건 저장(FAU_STG, Security audit event storage) 패밀리는 TSF가 안전한 감사 증적을 생성하고 유지할 수 있도록 하는 요구사항을 정의한다.

FAU_STG.1 감사 증적 저장소 보호(Protected audit trail storage)는 감사 증적에 중점을 두고 있다. 감사 증적 저장소는 인가되지 않은 삭제 및 변경으로부터 보호되어야 한다.
FAU_STG.2 감사 데이터의 가용성 보장

(Guarantees of audit data availability)은 예상하지 않은 조건이 발생하여도 TSF가 감사 데이터를 유지하도록 보장하는 것을 명세한다.
FAU_STG.3 감사 데이터 손실 예측 시 대응 행동(Action in case of possible audit data loss)은 감사 증적의 임계치를 초과할 경우에 취해야할 대응행동을 명세한다.
FAU_STG.4 감사 데이터의 손실 방지(Prevention of audit data loss)는 감사 증적이 포화되는 경우의 대응행동을 명세한다.

2.4.2 통신 클래스

통신(FCO, Communication) 클래스는 특히 데이터 교환에 참여하는 측의 신원 보증에 관련된 두 개의 패밀리를 제공한다. 이들 패밀리는 전송된 정보의 발신자(발신 증명)와 수신자(수신 증명)의 신원 보증에 관련되어 있다. 이들 패밀리는 발신자가 메시지를 발신하였음을 부인할 수 없으며 수신자도 수신 사실을 부인할 수 없음을 보장한다.[9]

○ 발신 부인방지(FCO_NRO, Non-repudiation of origin) 패밀리는 정보의 발신자가 정보의 발신 사실을 성공적으로 부인하지 못하게 함을 보장한다.

FCO_NRO.2 강제적인 발신 증명(Enforced proof of origin)은 TSF가 항상 전송된 정보의 발신에 대한 증거를 생성할 것을 요구한다.

○ 수신 부인방지(FCO_NRR, Non-repudiation of receipt) 패밀리는 정보의 수신자가 정보의 수신 사실을 성공적으로 부인하지 못하게 하는 것을 보장한다.

FCO_NRR.2 강제적인 수신 증명(Enforced proof of receipt)은 TSF가 항상 수신된 정보의 수신 증거를 생성할 것을 요구한다.

2.4.3 암호 지원 클래스

TSF는 높은 수준의 여러 가지 보안목적을 만족시키기 위하여 암호기능을 채택할 수 있다. 이들은 식별 및 인증, 부인방지, 안전한 경로, 안전한 채널, 데이터 분리 등을 포함한다(여기에 한정된 것은 아니다). 암호 지원(FCS, Cryptographic support) 클래스는 TOE가 암호기능을 구현할 경우 사용되며, 하드웨어, 펌웨어, 소프트웨어로 구현될 수 있다.[9]

○ 암호키 관리(FCS_CKM, Cryptographic key management) 패밀리는 암호키 생명주기를 지원하고자 하는 것으로, 그에 따른 암호키 생성, 분배, 접근 및 파기 행동에 대한 요구사항을 정의한다.

FCS_CKM.1 암호키 생성(Cryptographic key generation)은 명세된 암호 알고리즘과 키 길이에 따라 암호키가 생성될 것을 요구한다. 명세된 암호 알고리즘과 키 길이는 할당된 표준에 기반할 수 있다.
FCS_CKM.2 암호키 분배(Cryptographic key distribution)는 명세된 분배 방법에 따라 암호키가 분배될 것을 요구한다. 명세된 분배 방법은 할당된 표준에 기반할 수 있다.
FCS_CKM.3 암호키 접근(Cryptographic key access)은 명세된 접근 방법에 따라 암호키에 대한 접근이 수행될 것을 요구한다. 명세된 접근 방법은 할당된 표준에 기반할 수 있다.
FCS_CKM.4 암호키 파기(Cryptographic key destruction)는 명세된 파기 방법에 따라 암호키가 파기될 것을 요구한다. 명세된 파기 방법은 할당된 표준에 기반할 수 있다.

○ 암호 연산(FCS_COP, Cryptographic operation) 패밀리는 암호 연산 수행에 대한 요구사항이 있을 때 항상 포함되어야 한다. 전형적인 암호 연산은 데이터의 암호화 및 복호화, 전자서명 생성 및 검증, 무결성 및 체크섬 검증을 위한 암호 체크섬 생성, 안전한 해시(메시지 다이제스트), 암호키의 암호화 및 복호화, 암호키 합의 등을 포함한다.

FCS_COP.1 암호 연산(Cryptographic Operation)은 암호 연산이 명세된 알고리즘과 명세된 암호키 길이에 따라 수행될 것을 요구한다. 명세된 알고리즘과 암호키 길이는 할당된 표준에 기반할 수 있다.

2.4.4 사용자 데이터 보호 클래스

사용자 데이터 보호(FDP, User data protection) 클래스는 사용자 데이터의 보호와 관련된 요구사항을 명세하는 패밀리들을 포함한다. FDP는 사용자 데이터와 직접적으로 관련된 보안속성뿐만 아니라 유입, 유출, 저장하는 동안 TOE 내의 사용자 데이터를 다루는 4개의 패밀리 그룹으로 나누어진다.[9]

○ 접근통제 정책(FDP_ACC, Access control policy) 패밀리는 명칭에 의해서 접근통제 SFP를 식별하고, SFP와 관련된 SFR의 식별된 접근통제 부분을 구성하는 정책들의 통제 범위를 정의한다.

FDP_ACC.1 부분적인 접근통제(Subset access control)는 TOE 객체의 일부에서 수행 가능한 오퍼레이션의 일부에 대하여 각각의 식별된 접근통제 SFP가 존재할 것을 요구한다.

○ 접근통제 기능(FDP_ACF, Access control functions) 패밀리는 접근통제 정책(FDP_ACC)에서 명명된 접근통제 정책을 구현할 수 있는 특정 기능에 대한 규칙을 서술한다.

FDP_ACF.1 보안속성에 기반한 접근통제(Security attribute based access control)는 TSF가 보안속성 및 명명된 속성그룹에 기반하여 접근통제를 수행하도록 한다. 또한, TSF는 보안속성에 기반하여 객체에 대한 접근을 명시적으로 인가하거나 거부해도 된다.

○ 데이터 인증(FDP_DAU, Data authentication) 패밀리는 실체가 정보의 확실성에 대하여 책임을 지도록 한다(예 : 전자서명). 본 패밀리는 정보내용이 위조되거나 부정하게 변경되지 않았음을 검증하기위하여 데이터의 특정 단위에 대한 유효성을 보장하는 방법을 제공한다.

FDP_DAU.2 증거 생성자의 신원을 포함한 데이터 인증(Data authentication with identity of guarantor)은 TSF가 확실성을 보장해 주는 주체의 신원을 설정할 수 있도록 요구한다.

○ TOE로부터의 사용자 데이터 유출(FDP_ETC, Export from the TOE) 패밀리는 TSF 중재하에 TOE로부터 사용자 데이터를 유출하기 위한 기능을 정의한다. 이 기능은 사용자 데이터가 유출된 후 그 보안속성 및 보호가 명백하게 유지되거나 무시될 수 있도록 하는 것이다. 본 패밀리는 유출 시의 제약사항과, 유출된 사용자 데이터와 보안속성 간의 연관성을 다룬다.

FDP_ETC.1 보안속성 없이 사용자 데이터 유출(Export of user data without security attributes)은 TSF가 TSF 외부로 사용자 데이터를 유출할 경우 적절한 SFP를 수행할 것을 요구한다. 이 기능에 의해서 유출되는 사용자 데이터는 사용자 데이터와 연관된 보안속성 없이 유출된다.

FDP_ETC.2 보안속성을 포함한 사용자 데이터 유출(Export of user data with security attributes)은 TSF가 유출되는 사용자 데이터와 보안속성을 정확하고 명백하게 연관시킬 수 있는 기능을 사용하여 적절한 SFP를 수행할 것을 요구한다.

○ TOE 외부로부터 사용자 데이터 유입(FDP_ITC, Import from outside TOE) 패밀리는 TSF의 중재 하에 TOE로 사용자 데이터를 유입하기 위한 메커니즘을 정의한다. 이 메커니즘은 사용자 데이터가 적절한 보안속성을 가지며 적절히 보호되도록 하는 것이다. 이 패밀리는 유입 시의 제약사항과 요구되는 보안속성의 결정, 사용자 데이터와 관련된 보안속성의 해석을 다룬다.

FDP_ITC.1 보안속성 없이 사용자 데이터 유입(Import of user data without security attributes)은 보안속성들이 사용자 데이터를 정확히 표현하고, 객체로부터 분리되어 제공될 것을 요구한다.

FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입(Import of user data with security attributes)은 보안속성들이 사용자 데이터를 정확히 표현하고, TOE의 외부로부터 유입되는 사용

자 데이터와 정확하고 명백하게 연관될 것을 요구한다.

○ 잔여정보 보호(FDP_RIP, Residual information protection) 패밀리는 자원이 하나의 객체로부터 회수되고 다른 객체에 재할당되었을 때 자원 내에 포함된 어떠한 데이터도 가용하지 않음을 보장하기 위한 요구사항을 다룬다. 잔여정보 보호 패밀리는 자원 내에 포함된 데이터가 논리적으로 삭제되었거나 반환되었지만, TSF가 통제하는 자원에 여전히 남아서 다른 객체에 재할당될 수 있으므로, 이러한 데이터에 대한 보호를 요구한다.

FDP_RIP.2 전체적인 잔여정보 보호(Full residual information protection)는 TSF가 자원의 할당이나 회수 시에 TSF에 의해 통제되는 모든 객체에 대해서 모든 자원의 잔여정보 내용이 가용하지 않음을 보장할 것을 요구한다.

○ 저장된 데이터의 무결성(FDP_SDI, Stored data integrity) 패밀리는 TSF에 의해 통제되는 저장소(container) 내에 저장되어 있는 동안의 사용자 데이터 보호를 다루는 요구사항을 제공한다. 무결성 오류는 메모리나 저장 장치에 저장된 사용자 데이터에 영향을 미칠 수 있다.

FDP_SDI.1 저장된 데이터의 무결성 검사(Stored data integrity monitoring)는 TSF가 식별된 무결성 오류에 대해서 TSF에 의해 통제되는 저장소 내에 저장된 사용자 데이터를 검사할 것을 요구한다.
FDP_SDI.2 저장된 데이터의 무결성 검사 및 대응행동(Stored data integrity monitoring and action)은 오류 탐지의 결과로서 취해져야 하는 대응행동을 허용함으로써 첫 번째 컴포넌트에 부가적인 기능을 추가한다.

○ TSF 간 전송되는 사용자 데이터 비밀성(FDP_UCT, Inter-TSF user data confidentiality transfer protection) 패밀리는 사용자 데이터가 TOE와 다른 신뢰된 IT 제품 간에 외부 채널을 통하여 전송되는 동안 사용자 데이터의 비밀성을 보장하기 위한 요구사항을 정의한다.

FDP_UCT.1 기본적인 전송 데이터 비밀성(Basic data exchange confidentiality)의 목적은 전송 중인 사용자 데이터를 노출로부터 보호하는 것이다.

○ TSF 간 전송되는 사용자 데이터 무결성(FDP_UIT, Inter-TSF user data integrity transfer protection) 패밀리는 TOE와 다른 신뢰된 IT 제품 간에 전송 중인 사용자 데이터에 대하여 무결성을 제공하고 탐지 가능한 오류로부터 복구하기 위한 요구사항을 정의한다.

FDP_UIT.1 전송 데이터 무결성(Data exchange integrity)은 전송된 사용자 데이터의 변경, 삭제, 삽입, 재사용 오류 탐지를 위한 요구사항을 다룬다.

2.4.5 식별 및 인증 클래스

식별 및 인증(FIA, Identification & authentication) 클래스의 패밀리는 요청된 사용자의 신원을 설정하고 증명하기 위한 기능요구사항을 다룬다. 식별 및 인증은 사용자가 적절한 보안속성(예 : 신원, 그룹, 역할, 보안 수준, 무결성 수준)과 연관되는 것을 보장하도록 요구한다.[9]

○ 인증 실패(FIA_AFL, Authentication failures) 패밀리는 실패한 인증시도의 횟수와 인증시도 실패 시의 TSF 행동에 대한 값을 정의하기 위한 요구사항을 포함한다. 매개변수는 실패한 인증시도의 횟수, 시 간의 한계치를 포함하지만 이에 한정되지는 않는다.

FIA_AFL.1 인증 실패 처리(Authentication failure handling)는 사용자 인증시도 실패 횟수가 명세된 값을 넘으면 TSF가 세션 설정 과정을 종료시킬 수 있을 것을 요구한다. 또한, 세션 설정 과정의 종료 후 관리자가 정의한 조건이 일어날 때까지 TSF가 사용자의 계정이나 시도가 이루어진 진입점(예 : 워크스테이션)을 폐쇄할 수

있어야 한다.

○ 모든 인가된 사용자는 SFR을 수행하기 위하여 사용되는 사용자 신원 외에 보안속성의 집합을 가질 수 있다. 사용자 속성 정의(FIA_ATD, User attribute definition) 패밀리는 TSF의 보안 결정을 지원하기 위해 필요한 사용자 보안 속성을 사용자와 연관시키기 위한 요구사항을 정의한다.

FIA_ATD.1 사용자 속성 정의(User attribute definition)는 각 사용자에 대한 사용자 보안속성이 개별적으로 관리될 수 있도록 한다.

○ 비밀정보의 검증 및 생성(FIA_SOS, Specification of secrets) 패밀리는 제공된 비밀정보에 대하여 정의된 허용 기준을 적용하고 정의된 허용 기준을 만족시키는 비밀정보를 생성하는 메커니즘에 대한 요구사항을 정의한다.

FIA_SOS.1 비밀정보의 검증(Verification of secrets)은 비밀정보가 정의된 허용기준을 만족시킴을 TSF가 검증할 것을 요구한다.
FIA_SOS.2 비밀정보의 생성(TSF generation of secrets)은 TSF가 정의된 허용기준을 만족시키는 비밀정보를 생성할 수 있을 것을 요구한다.

○ 사용자 인증(FIA_UAU, User authentication) 패밀리는 TSF가 지원하는 사용자 인증 메커니즘의 유형을 정의한다. 또한, 본 패밀리는 사용자 인증 메커니즘이 기반해야 하는 요구되는 속성들을 정의한다.

FIA_UAU.2 모든 행동 이전에 사용자 인증(User authentication before any action)은 TSF에 의해서 허용될 다른 모든 행동 이전에 사용자를 인증할 것을 요구한다.
FIA_UAU.5 다중 인증 메커니즘(Multiple authentication mechanisms)은 특정 사건에 대하여 사용자 신원을 인증하기 위하여 서로 다른 인증 메커니즘이 제공되고 사용될 것을 요구한다.
FIA_UAU.6 재인증(Re-authenticating)은 사용자의 재인증이 필요한 사건을 명세하는 능력을 요구한다.
FIA_UAU.7 인증 피드백 보호(Protected authentication feedback)는 인증하는 동안 제한된 피드백 정보만이 사용자에게 제공될 것을 요구한다.

○ 사용자 식별(FIA_UID, User identification) 패밀리는 TSF에 의해서 관리되어야 하고 사용자 인증을 요구하는 다른 모든 행동을 수행하기 전에 사용자를 식별하도록 요구되는 조건을 정의한다.

FIA_UID.2 모든 행동 이전에 사용자 식별(User identification before any action)은 TSF에 의해서 허용될 다른 모든 행동 이전에 사용자를 식별할 것을 요구한다.

2.4.6 프라이버시 클래스

프라이버시(FPR, Privacy) 클래스는 프라이버시 요구사항을 포함한다. 이 요구사항은 다른 사용자에 의하여 신원이 발견되고 오용되는 것에 대하여 사용자를 보호한다.[9]

○ 가명성(FPR_PSE, Pseudonymity) 패밀리는 사용자가 사용자 신원의 노출 없이 자원이나 서비스를 사용할 수 있지만, 그 사용에 대하여 책임이 추적될 수 있음을 보장한다.

FPR_PSE.2 추적가능한 가명성(Reversible pseudonymity)은 TSF가 제공된 별칭에 기반하여 원래의 사용자 신원을 결정하는 기능을 제공할 것을 요구한다.

2.4.7 평가대상의 보안기능성(TSF) 보호 클래스

TSF 보호(FPT, Protection of the TSF) 클래스는 TSF를 구성하는 메커니즘의 무결성과 관리에 관련된 기능요구사항 패밀리와, TSF 데이터의 무결성에 관련된 기능요구사항 패밀리를 포함한다.[9]

○ 외부전송 TSF 데이터의 비밀성(FPT_ITC, Confidentiality of exported TSF data) 패밀리는 TSF와 다른 신뢰된 IT 제품 간의 전송 TSF 데이터를 인가되지 않은 노출로부터 보호하기 위한 규칙을 정의한다. 이러한 데이터는 패스워드, 키, 감사 데이터, TSF 실행 코드와 같은 중요한 TSF 데이터가 될 수 있다.

FPT_ITC.1 외부전송 TSF 데이터의 비밀성 (Inter-TSF confidentiality during transmission)은 TSF가 TSF와 다른 신뢰된 IT 제품 간에 전송 중인 데이터를 노출로부터 보호하도록 보장할 것을 요구한다.

○ 외부전송 TSF 데이터의 무결성(FPT_ITI, Integrity of exported TSF data) 패밀리는 TSF와 다른 신뢰된 IT 제품 간에 전송 중인 TSF 데이터를 인가되지 않은 변경으로부터 보호하기 위한 규칙을 정의한다. 이러한 데이터는 패스워드, 키, 감사 데이터, TSF 실행 코드와 같은 중요한 TSF 데이터가 될 수 있다.

FPT_ITI.1 외부전송 TSF 데이터의 변경 탐지 (Inter-TSF detection of modification)는 다른 신뢰된 IT 제품이 사용된 메커니즘을 인식한다는 가정 하에, TSF와 다른 신뢰된 IT 제품 간에 전송 중인 TSF 데이터의 변경을 탐지하는 능력을 제공한다.

○ 타임스탬프(FPT_STM, Time stamps) 패밀리는 TOE의 신뢰할 수 있는 타임스탬프 기능에 대한 요구사항을 다룬다.

FPT_STM.1 신뢰할 수 있는 타임스탬프 (Reliable time stamps)는 TSF가 TSF 기능에 신뢰할 수 있는 타임스탬프를 제공할 것을 요구한다.

2.4.8 자원 활용 클래스

자원 활용(FRU, Resource utilisation) 클래스는 처리 능력 및 저장 용량과 같은 요구된 자원의 가용성을 지원하는 세 개의 패밀리를 제공한다.[9]

○ 오류에 대한 내성(FRU_FLT, Fault tolerance) 패밀리의 요구사항은 장애가 발생한 경우에도 TOE가 정확한 운영을 유지하는 것을 보장한다.

FRU_FLT.1 오류에 대한 내성 : 부분적용 (Degraded fault tolerant)은 확인된 장애가 발생한 경우에도 식별된 기능의 동작을 정확히 지속하도록 TOE에게 요구한다.

○ 자원사용 우선순위(FRU_PRS, Priority of service) 패밀리의 요구사항은 TSF가 TSF의 통제 하에 있는 자원이 사용자 및 주체에 의해 사용되는 것을 통제할 수 있도록 하여, TSF 통제 하의) 높은 우선순위 행동이 항상 낮은 우선순위 행동에 의한 부당한 간섭이나 지연없이 수행되도록 한다.

FRU_PRS.1 자원사용 우선순위 : 부분적용 (Limited priority of service)은 주체에게 TSF 통제 하의 일부 자원의 사용에 대한 우선순위를 제공한다.

○ 자원 할당(FRU_RSA, Resource allocation) 패밀리의 요구사항은 TSF가 사용자 및 주체에 의한 자원 사용을 통제할 수 있도록 하여, 인가되지 않은 자원의 독점으로 인한 서비스 거부가 일어나지 않도록 한다.

FRU_RSA.1 최대 할당치(Maximum quotas)는 사용자와 주체가 통제된 자원을 독점할 수 없음을 보장하는 할당치 메커니즘에 대한 요구사항을 제공한다.

2.4.9 평가대상(TOE) 접근 클래스

TOE 접근(FTA, TOE access) 클래스는 사용자 세션 설정을 통제하기 위한 기능요구사항을 명세한다.[9]

○ 동시 세션 수의 제한(FTA_MCS, Limitation on multiple concurrent sessions) 패밀리는 동일 사용자에 속하는 동시 세션의 수를 제한하는 요구사항을 정의한다.

FTA_MCS.1 기본적인 동시 세션 수의 제한(Basic limitation on multiple concurrent sessions)은 TSF의 모든 사용자에게 적용되는 한계치를 제공한다.

○ 세션 잠금 및 종료(FTA_SSL, Session locking and termination) 패밀리는 TSF가 TSF에 의한 세션과 사용자에 의한 세션을 잠금, 잠금 해제 및 종료하는 능력을 제공하는 요구사항을 정의한다.

FTA_SSL.3 TSF에 의한 세션 종료(TSF-initiated termination)는 TSF가 명세된 사용자 비활동 기간 후 세션을 종료하는 요구사항을 제공한다.
FTA_SSL.4 사용자에 의한 세션 종료(User-initiated termination)는 사용자에게 사용자 자신의 상호작용 세션을 종료하는 기능을 제공한다.

2.4.10 안전한 경로/채널 클래스

안전한 경로/채널(FTP, Trusted path/channel) 클래스의 패밀리는 사용자와 TSF 간의 신뢰된 통신 경로와 TSF와 다른 신뢰된 IT 제품 간의 신뢰된 통신 채널에 관한 요구사항을 정의한다.

○ TSF 간 안전한 채널(FTP_ITC, Inter-TSF trusted channel) 패밀리는 보안상의 중요한 기능 실행을 위하여 TSF와 다른 신뢰된 IT 제품 간의 안전한 채널 생성에 대한 요구사항을 정의한다.

FTP_ITC.1 TSF 간 안전한 채널(Inter-TSF trusted channel)은 TSF가 자신과 다른 신뢰된 IT 제품 간에 안전한 통신 채널을 제공할 것을 요구한다.

III. 분산원장기술 시스템에 대한 보안 위협

본 장에서는 이용자 애플리케이션을 구동하기 위하여 오픈소스 기반 분산원장기술 시스템에서 제공하는 기능을 설명하고, 시스템 운영 시 발생할 수 있는 보안 위협을 식별한다.

3.1 분산원장기술 시스템의 기본 기능

본 절에서는 이용자 애플리케이션을 구동하기 위하여 오픈소스 기반 분산원장기술 시스템에서 제공하는 기본 기능을 설명한다.

분산원장기술 시스템은 이용자 애플리케이션 및 외부 시스템과 인터페이스를 가질 수 있고 신원 관리, 원장 관리, 암호키 관리, 패치 관리, 전자지갑 관리, 스마트 계약, 분산 합의, P2P 통신 등의 기본 기능으로 구성된다. 신원 관리 기능은 분산원장기술 시스템을 이용 및 운영하는 사용자를 인증하고 권한을 부여하는 것으로 외부 시스템인 비대면 인증 시스템(예: 휴대폰 본인 인증, I-PIN 등)을 활용할 수 있다. 원장 관리 기능은 거래 데이터를 저장하고 있는 원장의 무결성을 주기적으로 점검하고 분산 합의, 스마트 계약 등에 의하여 신규 원장을 추가하거나 검색하는 것으로 외부 시스템인 데이터베이스 관리 시스템을 활용하여 원장을 저장 및 검색할 수 있다. 암호키 관리 기능은 전자 서명, 데이터 암호화 등에 필요한 암호키의 생성, 분배, 접근, 파기 등을 처리하는 것으로서 외부 시스템인 암호키 관리 시스템을 활용할 수 있다. 패치 관리 기능은 분산원장기술 시스템을 구성하는 소프트웨어를 자동으로 업데이트 하는 것으로 외부 시스템인 소프트웨어 패치 관리 시스템을 활용할 수 있다. 전자지갑 관리 기능은 분산원장기술 시스템에서 제공할 수 있는 디지털 자산의 생성, 이용, 보관, 파기 등을 처리하는 것으로서 외부 시스템인 디지털 자산 보관 시스템(예: 콜드 월렛 등)을 활용할 수 있다. 스마트 계약 기능은 이용자가 특정 조건에 만족하는 경우 자동으로 실행되는 계약을 이행하는 것으로 외부 시스템인 비정상 거래 탐지 시스템을 활용하여 이상 거래를 탐지할 수 있다. 분

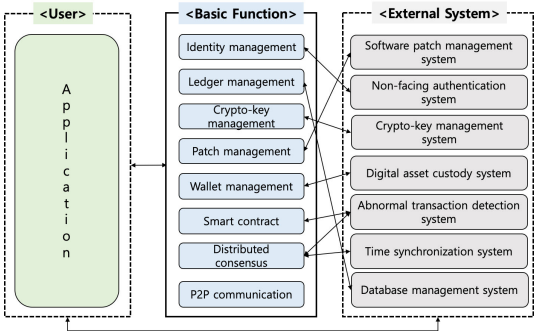

Fig. 1. Distributed ledger technology (DLT) system running user application

산 합의 기능은 신규 거래에 대한 검증과 신규 원장 생성, 공유, 검증 및 저장을 수행하는 것으로 외부 시스템인 비정상 거래 탐지 시스템을 활용하여 이상 거래를 탐지할 수 있고 또한 외부 시스템인 표준 시간 동기화 시스템을 활용하여 신규 거래 발생 시간을 정확하게 기록할 수 있다. P2P 통신 기능은 분산 원장 네트워크에 참여하는 노드(컴퓨터) 간에 데이터 통신을 수행하는 것이다.

3.2 분산원장기술 시스템에 대한 보안 위협

본 절에서는 이용자 애플리케이션을 구동하기 위하여 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 보안 위협을 식별한다.

3.2.1 이용자 익명성

거래의 당사자인 이용자의 신원 확인(예: KYC)을 이행하지 않아 익명의 이용자 간에 거래가 발생한 경우 해당 거래의 책임성을 보장할 수 없고, 또한 자금세탁 및 테러자금조성 등에 악용될 수 있다.

(약어) KYC : Know Your Customer

3.2.2 소프트웨어 위·변조

분산원장기술 시스템을 운영하기 위하여 각 노드에 설치된 소프트웨어(스마트 계약 포함)가 악의적으로 위·변조되거나 악성 코드에 감염되면 분산 원장 파괴, 서비스 지연을 초래하거나 이용자 손실이 발생할 수 있다.

3.2.3 암호키 유출

거래 당사자인 이용자의 전자서명용 개인키를 유출하게 되면 타인에 의한 무단 거래로 인하여 이용자 손실이 직접적으로 발생하게 되고, 중요 데이터를 암호화한 암호키를 유출하게 되면 중요 데이터 유출에 따라 이용자의 2차 피해가 발생할 수 있다.

3.2.4 비인가된 접근

분산 원장에 대한 무단 접근, 스마트 계약 무단 실행, 분산 원장 네트워크에 대한 무단 접근 등 비인가된 접근이 허용될 경우 서비스 중단 및 이용자 손실이 발생할 수 있다.

3.2.5 중요 데이터 유출 및 위·변조

분산 원장 네트워크를 통하여 노드 간에 거래 데이터, 원장 데이터 등을 전송 시 중간자 공격(Man-in-the-middle attack)에 의하여 데이터 유출 및 위·변조가 발생할 수 있어 분산 원장의 훼손 및 이용자의 2차 피해 등을 초래할 수 있다.

3.2.6 시스템 장애

분산원장기술 시스템을 운영하기 위한 소프트웨어의 오류, 분산 원장 네트워크 참여하는 노드의 시스템 자원(예: CPU, 메모리, 네트워크, 스토리지 등) 부족 등에 기인하여 서비스 지연을 초래할 수 있다.

3.2.7 감사 기록 손실

분산원장기술 시스템 운영에 관한 기록, 이용자 행위에 관한 기록 등이 무단 변경 또는 삭제되어 보안 사고 발생 시 책임 추적이 불가능할 수 있다.

3.3 분산원장기술 시스템의 보안 위협 대응

본 절에서는 오픈소스 기반 분산원장기술 시스템

Table 1. Countermeasure between security function of Hyperledger Fabric and security threat

Security Function of Hyperledger Fabric	Security Threat						
	ST1	ST2	ST3	ST4	ST5	ST6	ST7
Data integrity					△		
Identity management	△						
Access control				△			
Cryptography			△				

주1) ST1=User anonymity, ST2=Software tampering, ST3=Crypto-key leakage, ST4=Unauthorized access, ST5=Data leakage and tampering, ST6=System error, ST7=Audit log loss

주2) △ = 일부 만족

Table 2. Countermeasure between security function of Ethereum and security threat

Security Function of Ethereum	Security Threat						
	ST1	ST2	ST3	ST4	ST5	ST6	ST7
Data integrity					△		
Identity management	△						

(하이퍼레저 패브릭, 이더리움)에서 제공하는 보안 기능과 보안 위협 간의 대응 관계를 설명한다.

IV. 분산원장기술 시스템 보안 강화 방안

본 장에서는 이용자 애플리케이션을 운영하기 위한 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 보안 위협에 대응하는 보안기능 요구사항을 도출한다. 그리고 공통평가기준에 근거한 보안기능 컴포넌트를 활용하여 보안기능 요구사항을 구현하기 위한 방안을 제안하고, 이러한 보안기능 요구사항이 국내 법규 및 보안 인증 기준에 근거한 정보시스템 운영 시 안전성 확보를 위한 기술적 보안 요구사항을 만족함을 설명한다.

4.1 보안기능 요구사항

본 절에서는 이용자 애플리케이션을 운영하기 위한 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 보안 위협에 대응하는 보안기능 요구사항을 도출하고 공통평가기준에 근거한 보안기능 컴포넌트를 활용하여 보안기능 요구사항을 구현하기 위한 방안을 제안한다.

4.1.1 식별 및 인증

분산원장기술 시스템은 본인 확인 절차에 따라 이용자 또는 애플리케이션을 식별하고 인증하는 수단을 제공할 필요가 있다. 또한 거래의 중요도에 따라 강화된 인증 수단(예: 일회용 패스워드, 인증서 등)을 적용한다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FIA_AFL.1 인증 실패 처리
- FIA_ATD.1 사용자 속성 정의
- FIA_SOS.1 비밀정보의 검증
- FIA_SOS.2 비밀정보의 생성
- FIA_UAU.2 모든 행동 이전에 사용자 인증
- FIA_UAU.5 다중 인증 메커니즘
- FIA_UAU.6 재인증
- FIA_UAU.7 인증 피드백 보호
- FIA_UID.2 모든 행동 이전에 사용자 식별
- FTA_MCS.1 기본적인 동시 세션 수의 제한
- FTA_SSL.3 TSF에 의한 세션 종료
- FTA_SSL.4 사용자에 의한 세션 종료

※ 제2장의 2.5.4 식별 및 인증 클래스, 2.4.9 평가대상(TOE) 접근 클래스 참조

4.1.2 보안 감사

분산원장기술 시스템은 이용자의 행위 이력을 기록하고 안전하게 보관하여 보안 사고 발생에 대한 책임을 추적할 수 있는 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FAU_ARP.1 보안 경보
- FAU_GEN.1 감사 데이터 생성
- FAU_GEN.2 사용자 신원 연관
- FAU_SAR.1 감사 검토
- FAU_SAR.2 감사 검토 권한 제한
- FAU_SAR.3 선택 가능한 감사 검토
- FAU_SEL.1 선택적인 감사
- FAU_STG.1 감사 증적 저장소 보호
- FAU_STG.2 감사 데이터의 가용성 보장
- FAU_STG.3 감사 데이터 손실 예측 시 대응 행동
- FAU_STG.4 감사 데이터의 손실 방지
- FPT_STM.1 신뢰할 수 있는 타임스탬프

※ 제2장의 2.4.1 보안감사 클래스, 2.4.7 평가대상의 보안기능성(TSF) 보호 클래스 참조

4.1.3 통신 보호

분산원장기술 시스템은 분산 원장 네트워크에 참여하는 노드 간의 중요 정보 전송 시 안전한 통신 수단을 제공한다. 또한 분산원장기술 시스템과 외부 시스템 간의 중요 정보 전송 시 안전한 통신 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같

은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FCO_NRO.2 강제적인 발신 증명
- FCO_NRR.2 강제적인 수신 증명
- FPT_ITC.1 외부전송 TSF 데이터의 비밀성
- FPT_ITI.1 외부전송 TSF 데이터의 변경 탐지
- FTP_ITC.1 TSF 간 안전한 채널

※ 제2장의 2.4.2 통신 클래스, 2.4.7 평가대상의 보안기능성(TSF) 보호 클래스, 2.4.10 안전한 경로/채널 클래스 참조

4.1.4 암호 통제

분산원장기술 시스템은 이용자 간의 거래 시 전자서명, 중요 정보 전송 또는 저장 시 데이터 암호화 등을 위한 암호키를 안전하게 처리(생성, 이용, 보관, 파기 등)할 수 있는 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FCS_CKM.1 암호키 생성
- FCS_CKM.2 암호키 분배
- FCS_CKM.3 암호키 접근
- FCS_CKM.4 암호키 파기
- FCS_COP.1 암호 연산

※ 제2장의 2.4.3 암호 지원 클래스 참조

※ 국가·공공기관 경우 국가정보원장이 승인한 암호 모듈을 사용하여야 함

4.1.5 접근 통제

분산원장기술 시스템은 비인가자가 중요 정보자산(예: 분산 원장, 스마트 계약, 분산 원장 네트워크 등)에 무단으로 접근하는 것을 통제할 수 있는 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FDP_ACC.1 부분적인 접근통제
- FDP_ACF.1 보안속성에 기반한 접근통제

※ 제2장의 2.4.4 사용자 데이터 보호 클래스 참조

4.1.6 개인정보 보호

분산원장기술 시스템은 이용자의 개인정보가 유출 및 노출되지 않도록 안전하게 처리(예: 수집, 이용, 보관, 파기 등)할 수 있는 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FPR_PSE.2 추적가능한 가명성

※ 제2장의 2.4.6 프라이버시 클래스 참조

4.1.7 데이터 보호

분산원장기술 시스템은 이용자의 거래 데이터, 분산 원장 데이터(개인정보 포함) 등 중요 정보가 유출 또는 위·변조 되지 않도록 안전하게 전송 또는 저장하는 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FDP_DAU.2 증거 생성자의 신원을 포함한 데이터 인증
- FDP_ETC.1 보안속성 없이 사용자 데이터 유출
- FDP_ETC.2 보안속성을 포함한 사용자 데이터 유출
- FDP_ITC.1 보안속성 없이 사용자 데이터 유입
- FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입
- FDP_RIP.2 전체적인 잔여정보 보호
- FDP_SDI.1 저장된 데이터의 무결성 검사
- FDP_SDI.2 저장된 데이터의 무결성 검사 및 대응 행동
- FDP_UCT.1 기본적인 전송 데이터 비밀성
- FDP_UIT.1 전송 데이터 무결성

※ 제2장의 2.4.4 사용자 데이터 보호 클래스 참조

4.1.8 자원 가용성

분산원장기술 시스템은 분산 원장 네트워크에 참여하는 노드의 시스템 자원(예: CPU, 메모리, 네트워크, 스토리지 등) 부족, 분산원장기술 시스템을 운

영하는 소프트웨어 오류 등에 대응하여 시스템 가용성을 극대화 할 수 있는 수단을 제공할 필요가 있다. 본 보안기능을 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FRU_FLT.1 오류에 대한 내성 : 부분적용
- FRU_PRS.1 자원사용 우선순위 : 부분적용
- FRU_RSA.1 최대 할당치

※ 제2장의 2.4.8 자원 활용 클래스 참조

4.2 보안이 강화된 분산원장기술 시스템

본 절에서는 보안 기능이 반영된 분산원장기술 시스템의 모델을 제안한다.

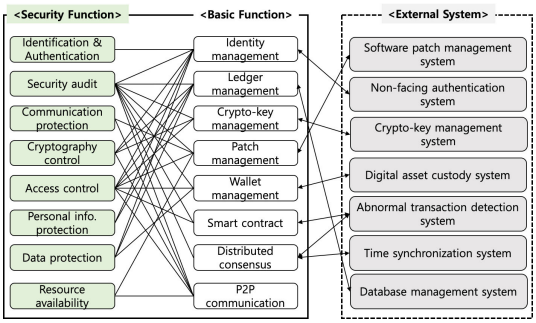

Fig. 2. A model of security-enhanced distributed ledger technology system

Fig. 2에서 보는 바와 같이 보안 기능과 기본 기능의 연관성은 Table 3과 같다.

Table 3. Relationship between security function and basic function

Security Function	Basic Function
Identification & Authentication	• Identity management
Security audit	• Identity management • Ledger management • Crypto-key management • Patch management • Wallet management • Smart contract • Distributed consensus • P2P communication
Communication protection	• Patch management • P2P communication
Cryptography control	• Identity management • Ledger management • Crypto-key management • P2P communication
Access control	• Identity management • Ledger management • Crypto-key management • Patch management • Wallet management • Smart contract • P2P communication
Personal info. protection	• Identity management • Ledger management
Data protection	• Identity management • Ledger management • Wallet management
Resource availability	• Patch management • P2P communication

Fig. 3에서 보는 바와 같이 보안이 강화된 분산원장기술 시스템은 보안 기능, 외부 시스템 및 이용자 애플리케이션과 인터페이스를 가진다. 이용자 애플리케이션의 서비스 목적에 따라 외부 시스템은 일부 변동될 수 있다.

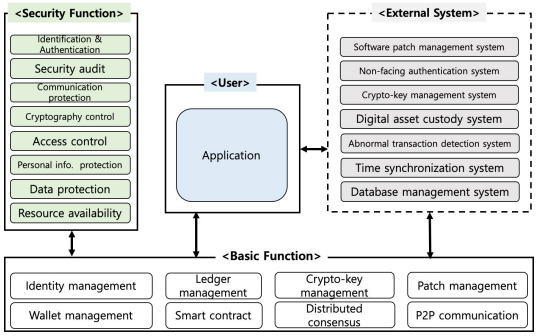

Fig. 3. A model of security-enhanced distributed ledger technology system running user application

4.3 보안 기능과 법규 및 보안 인증 기준에 근거한 보안 요구사항 간의 부합성

본 절에서는 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부

합성을 설명한다.

4.3.1 식별 및 인증

본 절에서는 '식별 및 인증' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	제4조(접근통제)
개인정보의 안전성 확보조치 기준	제5조(접근 권한의 관리) 제6조(접근통제)
전자금융감독규정	제13조(전산자료 보호대책) 제14조(정보처리시스템 보호대책) 제17조(홈페이지 등 공개용 웹서버 관리대책) 제32조(내부사용자 비밀번호 관리) 제33조(이용자 비밀번호 관리) 제34조(전자금융거래 시 준수사항) 제37조(인증방법 사용기준)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	2.5.2 사용자 식별 2.5.3 사용자 인증 2.5.4 비밀번호 관리 2.6.3 응용프로그램 접근 2.6.6 원격접근 통제

4.3.2 보안 감사

본 절에서는 '보안 감사' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	제4조(접근통제) 제5조(접속기록의 위·변조방지)
개인정보의 안전성 확보조치 기준	제5조(접근 권한의 관리) 제8조(접속기록의 보관 및 점검)
전자금융감독규정	제13조(전산자료 보호대책) 제27조(전산원장 통제)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	2.9.4 로그 및 접속기록 관리 2.9.6 시간 동기화

4.3.3 통신 보호

본 절에서는 '통신 보호' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	제6조(개인정보의 암호화)
개인정보의 안전성 확보조치 기준	제7조(개인정보의 암호화)
전자금융감독규정	제34조(전자금융거래 시 준수사항)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	2.6.6 원격접근 통제 2.10.5 정보전송 보안

4.3.4 암호 통제

본 절에서는 '암호 통제' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	제6조(개인정보의 암호화)
개인정보의 안전성 확보조치 기준	제7조(개인정보의 암호화)
전자금융감독규정	제31조(암호프로그램 및 키 관리 통제) 제32조(내부사용자 비밀번호 관리) 제33조(이용자 비밀번호 관리) 제34조(전자금융거래 시 준수사항)
전자정부법 및 시행령	-법 제56조(정보통신망 등의 보안대책 수립·시행) -시행령 제69조(전자문서의 보관·유통 관련 보안조치)
보안 인증 기준(ISMS-P)	2.7.1 암호정책 적용 2.7.2 암호키 관리

국가·공공기관이 분산원장기술 시스템을 운영하는 경우, 「전자정부법」 및 시행령에 따라 국가정보원장이 승인한 암호 모듈(검증필 암호 모듈)을 사용하여야 한다.

4.3.5 접근 통제

본 절에서는 '접근 통제' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	제4조(접근통제)
개인정보의 안전성 확보조치 기준	제6조(접근통제)
전자금융감독규정	제13조(전산자료 보호대책)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	2.6.1 네트워크 접근 2.6.3 응용프로그램 접근 2.6.4 데이터베이스 접근

4.3.6 개인정보 보호

본 절에서는 '개인정보 보호' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	-법 제29조(개인정보의 파기) -시행령 제16조(개인정보의 파기 등)
개인정보 보호법 및 시행령	-법 제21조(개인정보의 파기) -시행령 제16조(개인정보의 파기방법)
개인정보의 기술적·관리적 보호조치 기준	제9조(출력·복사시 보호조치) 제10조(개인정보 표시 제한 보호조치)
개인정보의 안전성 확보조치 기준	제13조(개인정보의 파기)
전자금융감독규정	제60조(외부주문등에 대한 기준)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	3.1.1 개인정보 수집 제한 3.1.2 개인정보의 수집 동의 3.1.3 주민등록번호 처리 제한 3.1.4 민감정보 및 고유식별정보의 처리 제한 3.2.3 개인정보 표시제한 및 이용 시 보호조치 3.2.4 이용자 단말기 접근 보호 3.4.1 개인정보의 파기 3.4.2 처리목적 달성 후 보유 시 조치 3.4.3 휴면 이용자 관리

개인 정보를 분산 원장에 저장하는 경우, 분산원장기술의 특성 상 분산 원장에 한 번 저장된 정보는 변경 또는 삭제가 어려우므로 '개인정보 보호' 보안 기능은 관련 법규의 기술적 보안 요구사항인 '개인정보의 파기'를 만족하기 위하여 별도의 개인 정보 분리 및 완전 삭제 기능을 구현할 필요가 있다.

4.3.7 데이터 보호

본 절에서는 '데이터 보호' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	제6조(개인정보의 암호화)
개인정보의 안전성 확보조치 기준	제7조(개인정보의 암호화)
전자금융감독규정	제17조(홈페이지 등 공개용 웹서버 관리대책) 제32조(내부사용자 비밀번호 관리) 제33조(이용자 비밀번호 관리) 제60조(외부주문등에 대한 기준)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	2.5.4 비밀번호 관리 2.10.4 전자거래 및 핀테크 보안 2.10.5 정보전송 보안

4.3.8 자원 가용성

본 절에서는 '자원 가용성' 보안 기능과 법규 및 보안 인증 기준(ISMS-P)에 근거한 기술적 보안 요구사항 간의 부합성을 설명한다.

법규	기술적 보안 요구사항
정보통신망법 및 시행령	해당 사항 없음
개인정보 보호법 및 시행령	해당 사항 없음
개인정보의 기술적·관리적 보호조치 기준	해당 사항 없음
개인정보의 안전성 확보조치 기준	해당 사항 없음
전자금융감독규정	제14조(정보처리시스템 보호대책) 제15조(해킹 등 방지대책) 제25조(정보처리시스템의 성능관리) 제34조(전자금융거래 시 준수사항)
전자정부법 및 시행령	해당 사항 없음
보안 인증 기준(ISMS-P)	2.9.2 성능 및 장애관리 2.10.8 패치 관리

4.4 보안 기능과 보안 위협 간의 대응 관계

본 절에서는 보안 기능과 보안 위협 간의 대응 관계를 설명한다.

Table 4. Countermeasure between security function and security threat

Security Function	Security Threat						
	ST1	ST2	ST3	ST4	ST5	ST6	ST7
Identification & Authentication	O						
Security audit							O
Communication protection					O		
Cryptography control			O				
Access control				O			
Personal info. protection					O		
Data protection					O		
Resource availability		O				O	

주1) ST1=User anonymity, ST2=Software tampering, ST3=Crypto-key leakage, ST4=Unauthorized access, ST5=Data leakage and tampering, ST6=System error, ST7=Audit log loss

주2) O = 만족

V. 결 론

최근 공공 및 민간 분야에서 널리 활용되고 있는 오픈소스 기반 분산원장기술 시스템(예: 하이퍼레저 패브릭, 이더리움 등)에서 일부 보안 기능을 제공하고 있으나 분산원장기술 시스템에서 발생할 수 있는 이용자 익명성, 소프트웨어 위·변조, 암호키 유출, 비인가된 접근, 데이터 유출 및 위·변조, 시스템 장애, 감사 기록 손실 등 보안 위협에 적절히 대응하기에는 매우 미흡하다.

국가·공공기관, 금융 회사 및 민간 산업체에서 분산원장기술 시스템 운용 시 고려하여야 할 법적 준거성을 확인하기 위하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 시행령, 「개인정보 보호법」 및 시행령, 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회고시 제2015-3호), 「개인정보의 안전성 확보조치 기준」(행정안전부고시 제2017-1호), 「전자금융감독규정」(금융위원회고시 제2018-36호), 「전자정부법」 및 시행령, 「정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증 기준」 등 국내 법규 및 보안 인증 기준에 근거하여 정보시스템에서 중요 정보 처리 시 안전성 확보, 기업의 정보 자산 보호 등에 필요한 기술적 보안 요구사항을 분석하였다.

오픈소스 기반 분산원장기술 시스템에 대한 보안 위협인 이용자 익명성, 소프트웨어 위·변조, 암호키 유출, 비인가된 접근, 데이터 유출 및 위·변조, 시스템 장애, 감사 기록 손실 등에 대응할 수 있는 식별 및 인증, 보안 감사, 통신 보호, 암호 통제, 접근 통제, 개인정보 보호, 데이터 보호, 자원 가용성 등 보안기능 요구사항을 도출하고 국내 법규 및 보안 인증 기준에 근거한 기술적 보안 요구사항과의 부합성을 설명하였다.

결론적으로 IT 제품의 보안성 평가를 위한 국제 표준인 공통평가기준(CC, Common Criteria)의 보안기능 컴포넌트를 분석하여 이용자 애플리케이션을 운영하는 분산원장기술 시스템에 필요한 보안 기능을 구현할 수 있는 방안을 제안함으로서 오픈소스 기반 분산원장기술 시스템의 보안을 강화하고자 한다.

References

[1] Korea Communications Commission, "「Act on promotion of information and communications network utilization and information protection, etc.」," Jun. 2018

[2] Ministry of the Interior and Safety, "「Personal information protection act」," Jul. 2017

[3] Korea Communications Commission, "「Criteria on technical and administrative security measures of personal information」(Korea Communications Commission Notice No. 2015-3)," May 2015

[4] Ministry of the Interior and Safety, "「Criteria on measures ensuring the safety of personal information」(Ministry of the Interior and Safety Notice No. 2017-1)," Jul. 2017

[5] Financial Services Commission, "「Electronic Financial Supervisory Regulations」(Financial Services Commission Notice No. 2018-36)," Dec. 2018

[6] Ministry of the Interior and Safety, "「Electronic government act」," Oct. 2017

[7] Ministry of the Interior and Safety, "「Enforcement Decree of Electronic Government Act」," Dec. 2018

[8] Korea Internet & Security Agency, "「Personal Information & Information Security Management System (ISMS-P) Certification Criteria」," Jan. 2019

[9] National Security Research Institute, "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002," pp. 21-180, Apr. 2017

[10] Internet homepage of Hyperledger Fabric , "https://wiki.hyperledger.org/display/fabric/Hyperledger+Fabric," Mar. 2019

[11] Hyperledger Architecture Working Group, "Hyperledger Architecture Volume 1," Aug. 2017

〔12〕 Internet homepage of Hyperledger Fabric , “https://hyperledger-fabric.readthedocs.io/en/latest/,” Mar. 2019
〔13〕 Internet homepage of Ethereum, “https://www.ethereum.org/,” Mar. 2019
〔14〕 Internet homepage of Ethereum Homestead Documentation, “http://www.ethdocs.org/en/latest/index.html,” Mar. 2019

〈저 자 소 개〉

박 근 덕 (Keundug Park) 종신회원
1992년 2월: 동아대학교 전산공학과 학사
2015년 8월: 순천향대학교 대학원 정보보호학과 석사
2018년 2월: 순천향대학교 대학원 정보보호학과 박사
2018년 3월~현재: 서울외국어대학원대학교 국제교양학과/AI블록체인연구소 조교수
2018년 9월~현재: TTA PG502 특별위원/에디터, PG1006 간사/특별위원
2017년 8월~현재: ISO/TC 307 전문위원/국제표준에디터
2017년 2월~현재: ITU-T SG17 위원/국제표준에디터
2012년 2월~현재: 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 심사원
〈관심분야〉 분산원장기술 보안, 정보보호관리체계, 개인정보보호, 클라우드 컴퓨팅 보안

김 대 경 (Dae Kyung Kim) 종신회원
1995년 2월: 경성대학교 컴퓨터공학과 학사
2004년 2월: 순천향대학교 대학원 정보보호학과 석사
2007년 2월: 순천향대학교 대학원 정보보호학과 박사과정(수료)
〈관심분야〉 분산원장기술 보안, 4차산업혁명기술 보안, 개인정보보호, 정보보호관리체계

염 흥 열 (Heung Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2017년~현재: ITU-T SG17 의장
2016년 5월~현재: 개인정보보호표준포럼 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜