한국은행 THE BANK OF KOREA

금융결제 업무정보

금융결제국
디지털화폐기술1팀
2023. 10. 20(금)

미 연준의 "디지털자산 시스템의 개인정보보호 전략" 보고서 주요 내용 및 시사점

※ 미국 연방준비위원회 이사회가 발간하는 금융 및 경제 토론 시리즈 중 2023.9월 발표된 "Data Privacy for Digital Asset Systems" 보고서를 참조하여 요약한 자료임

<요 약>

□ **(개요)** 미 연준은 동 보고서에서 디지털자산 시스템 설계시 초기부터 개인정보보호 **정책과 기술을 동시에 고려하는 개인정보보호 전략을 수립하고 적용**할 것을 제시

○ 디지털자산 시스템에는 거래내역과 함께 이용자 ID, IP주소 등의 IT시스템 정보가 수집되어 동 정보를 통해 특정 이용자가 유추되지 않도록 **기밀성을 보장**하는 **개인정보보호 전략이 필요**

○ 효과적인 개인정보보호 전략 수립을 위해서는 개인정보보호 강화기술(Privacy-Enhancing Technologies)을 활용하는 **기술적 방식**과 개인정보를 안전하게 처리하는 체계 마련 등의 **정책적 방식을 조합하는 것이 필요**

□ **(시사점)** CBDC는 디지털 시스템 상에서 발행·유통되는 등 디지털자산과 유사한 특성을 가지고 있으므로, 우선적으로 당행 CBDC 활용성 테스트에 동 보고서에서 제시한 개인정보보호 전략 수립 방안을 적용할 계획

① CBDC 유통과정별로 **개인정보 흐름을 단계화(수집·이용·저장·파기)**하여 시스템 설계 초기부터 적정 기술을 도출하고 정책을 수립하는 전략 마련

— 개인정보의 흐름 단계별로 적용가능한 **개인정보보호 강화기술을 도출**하고 **적용하는 실증 실험을 진행**

— 개인정보 수집을 위한 **이용자 동의를 명확하게 징구**하고 이용자에게 개인정보보호법 상의 **정보 주권(열람권, 정정권, 삭제권 등)을 제공**하는 정책을 마련

② 또한, 현행 **개인정보보호법(개인정보처리자의 의무 등) 및 개인정보 관련 금융법상의 요구사항(신원인증, AML/CFT 등)**을 종합적으로 검토하여 개인정보보호 정책에 반영

작성자 : 이지은 과장(6690)

1 개요

□ 미 연준은 **디지털자산*** **시스템**에서 특정 이용자의 신원이 유추되지 않도록 **개인정보보호 전략**을 **수립**하는 **방안**을 **제시**

* 이용자 디지털 지갑 내 가치가 존재하는 디지털 객체로 보유자 간 양도가 가능한 토큰화된 유가증권, 예금, 가상자산 등을 포함하는 것으로 정의

○ 디지털자산 시스템의 **설계 초기**부터 **개인정보보호 체계** 및 **전략**을 **수립**하고 이에 **적합한 정책**과 **기술**을 **조화롭게 적용**할 것을 제시

2 보고서 주요 내용

□ 동 보고서는 **디지털자산 시스템** 관련 **개인정보보호 전략 수립**을 위해 디지털자산 유통 흐름에 따라 **다양한 개인정보보호 정책** 및 **기술**을 **동시**에 **활용**하는 **하이브리드 전략**을 수립하는 방안을 제시

가. 개인정보보호 전략 수립시 고려사항

(현금과 디지털자산간의 차이점)

□ 현금과 디지털자산은 거래를 위한 **정보수집 범위**, **정보처리 환경** 등이 **상이**하여 거래별로 개인정보를 수집하고 처리하는 방식도 상이

○ **현금**은 이용자간 물리적 형태로 교환되어 거래가 완료되기 때문에 거래를 위한 **IT시스템 지원도 필요하지 않으며**, **디지털 기록도 남기지 않음**

○ **디지털자산**은 발행, 유통 등이 **IT시스템**을 **활용**하여 이루어지므로, 이용자 ID, IP주소 등의 정보가 수집되어 거래내용과 함께 **디지털 장부**에 **기록**

결제수단별 거래시 요구되는 정보

	개인정보	금액	참가기관	메타데이터[3]	결제내역	공공장부
은행권(현금)	X	O	X	X	X	X
비허가형 네트워크[1] 디지털자산	X	O	O	O	O	O
허가형 네트워크[2] 디지털자산	O	O	O	O	O	X

주: 1) 비허가형 네트워크 : 별도 인증 절차 없이 누구나 참여가능한 네트워크로 대표적으로 비트코인 블록체인 네트워크가 있음
2) 허가형 네트워크 : 허가된 참여자만이 네트워크에 참여할 수 있으며, 정해진 네트워크 운영 규칙에 따라야 하기에 보안과 신뢰성이 중요한 업무에 주로 이용
3) 메타데이터 : 특정 데이터에 관한 구조화된 데이터로서 예를 들어, 파일 저장 시 함께 저장되는 해당 파일에 관한 파일 이름, 저장 시간, 크기 등의 데이터를 총칭

(정보보호 기본원칙)

□ 디지털자산 시스템의 개인정보보호 전략 수립 시 일반 정보보호와 동일하게 관련 정보의 **기밀성, 무결성, 가용성**이 **보장**되도록 설계할 필요

○ **(기밀성)** 인가된 관리자 혹은 이용자에게만 정보에 대한 접근을 허용하는 한편, 해킹 등으로 정보가 유출되더라도 비인가된 이용자들에게는 정보가 유출되지 않도록 암호화 기술, 접근제어 정책 등을 적용

○ **(무결성)** 거래 과정에서 정보가 무단으로 위·변조되지 않도록 수신자가 정보 변경 여부를 확인할 수 있는 전자서명 기술 등을 적용

○ **(가용성)** 외부 재해, 사이버 공격 등이 발생해도 인가된 이용자는 항상 정보에 접근할 수 있도록 시스템 이중화, 정보 백업 등을 적용

(정보의 보호 수준)

□ 디지털자산 시스템에서 처리되는 **정보**의 **보호 수준**은 크게 **익명성**, **기밀성** 또는 **완전 공개**로 구분이 가능

○ **익명성**은 어떠한 정보를 통해서도 **이용자의 신원을 식별할 수 없는 것**으로 관련 정보는 개인정보에 해당하지 않음

— 다만 **거래**가 **누적**되면서 네트워크 및 IT시스템 식별자 등 **다양한 정보**들이 계속 **수집**되고 이를 **조합**하여 **이용자**의 **신원**이 **유추**될 수 있으므로 지속적으로 익명성*을 유지하기 어려움

* 국내에서는 합리적인 시간·비용·기술을 고려시 여타 정보를 이용하여도 개인을 식별할 수 없을 때 익명성을 가진다고 정의

○ **기밀성**은 **익명성**과 **완전 공개 사이**에 **존재**하는 단계로 **난독화** 및 **접근제어** 등의 기술을 통해 **개인정보**에 대한 **접근**을 **제한**하는 것으로 해당 정보는 개인정보에 해당

○ **완전 공개**는 **익명성**의 **반대 개념**으로 외부에 공개되는 정보지만 **이용자 요청**시 정보를 난독화하거나 제거가 가능한 것으로 해당 정보는 개인정보에 해당

→ 동 보고서는 이용자의 개인정보보호 수준을 제고하기 위해 **기밀성**을 **최대한 보장**하도록 **다양한 기술**을 **활용**하는 방안을 제시

(개인정보보호 관련 기술)

□ 동 보고서는 **개인정보보호 강화기술***(Privacy-Enhancing Technologies), **기밀성 유지 기술** 등 개인정보보호 관련 기술들을 소개

* 개인정보 수집·이용 시 해당 정보를 안전하게 처리할 수 있는 전체 기술을 지칭, 자세한 내용은 “<참고> 주요 개인정보보호 강화기술 현황” 참조

○ 암호화 기술, 디지털 서명 기술, 가명화 기술, 안전한 다자간 연산, 동형암호 기술, 영지식 증명 기술 등이 해당되며, 외부 침입을 방지하기 위한 네트워크 접근제어 기술 등도 포함

□ 또한 디지털자산 시스템 구현에 복수의 개인정보보호 관련 기술이 결합된 형태로 적용될 수도 있으며, 이러한 기술들이 반영된 디지털자산 시스템 구축 사례도 존재

○ **(프라이버시 코인)** Monero*, Zcash**등 디지털자산 시스템은 다양한 개인정보보호 강화기술이 적용되어 공개된 원장에서 이용자 개인정보의 기밀성을 보장

* 2014년 서비스를 시작하였으며 송금 거래 시 특정 그룹 구성원들의 개인키들을 섞어서 개인을 알 수 없도록 송신자 정보를 난독화하고, 거래 시마다 일회용 주소를 생성하여 거래내역을 난독화하는 암호자산

** 2016년 서비스를 시작하였으며 영지식 증명 기술을 통해 개인정보 노출없이 이용자 거래내역과 전자서명을 대조하여 진위를 판별하고 거래자 신원 및 거래금액을 익명화할 수 있도록 선택권을 제공하는 암호자산

○ **(스마트 계약)** 서면이 아닌 코드로 구현된 계약이며, 특정 조건이 충족되었을 시 자동으로 계약이 이행되는 프로그램으로, 관련 이용자 인증 시 영지식 증명 기술 등을 적용하여 기밀성을 보장

○ **(믹싱 서비스)** 입금 정보를 암호화하여 저장하고 올바른 암호화 키를 가진 이용자만 출금할 수 있도록 조치하는 것으로, 입출금 사이의 연결 정보들을 난독화하여 정보의 출처를 알 수 없도록 처리

(개인정보보호 전략 수립 방식)

□ 개인정보보호 전략 수립은 크게 **시스템 설계(privacy by design)** 또는 **정책 수립 단계(privacy by policy)**부터 **개인정보보호를 중점 고려하는 두 가지 방식이 있으며** 때론 두 방식을 혼합한 **하이브리드** 방식이 있음

○ **(개인정보보호 중점 설계*)** 디지털자산 시스템 설계 시 개인정보보호 기술을 중심으로 개인정보보호 전략을 수립하는 방식

* 국내, EU 등은 IT시스템 **기획**부터 **구현**까지 개발 全 과정에서 개인정보 보호를 위한 기술 및 정책을 고려하는 것으로 정의

○ **(개인정보보호 중점 정책 수립)** 개인정보 처리시 이용자 동의를 구하고 개인정보 관련 사항을 고지하는 등의 정책을 중심으로 개인정보보호 전략을 수립하는 방식

○ **(하이브리드 방식)** 시스템 설계시 다양한 개인정보보호 기술과 정책을 조합하고 활용하여 전략을 수립하는 방식

→ 동 보고서는 **개인정보보호 전략**을 **수립**하기 위해 개인정보보호 강화기술, 접근제어 등과 같은 **기술적 도구**와 이용자 동의 체계 마련 등의 **정책적 도구**를 **함께 활용**하는 방안을 제시

나. 개인정보보호 전략 수립 방안

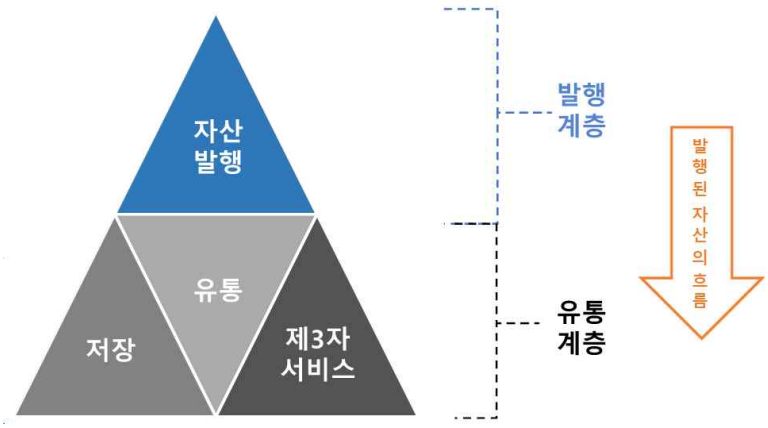
(계층별 전략 수립)

□ 동 보고서에서는 **다양한 개인정보보호 고려사항**을 **도출**하기 위해 **발행·유통과정을 각각 분리**하여 **개인정보보호 전략 수립 방안**을 **제시**

○ **발행계층**은 제한된 정보만 활용하여 디지털자산의 생성과 최초 배포만을 진행하기 때문에 업무에 적용되는 이용자 정보가 적어 개인정보보호 전략 수립이 비교적 용이

○ **유통계층**은 이용자 지갑에 디지털자산이 저장되고 거래되며, 제3자 서비스에도 이용될 수 있어 많은 이용자 정보가 활용되기 때문에 다양한 개인정보보호 강화기술 및 정책을 적용한 전략 수립이 필요

디지털자산 흐름별 계층화



○ 계층화된 구조에서 이용자 정보 취급범위에 따라 적용되는 기술이 크게 다르진 않지만, 활용사례에 따라 적합한 개인정보보호 강화기술을 선택하여 전략에 반영하는 것이 필요

— 신원, 보유자금 등의 인증이 필요한 경우에는 전자 서명 및 영지식 증명 기술이 적용될 수 있으며, 거래 내역을 통계 등의 목적으로 활용하기 위해서는 동형암호 기술 등이 적용된 전략 수립이 가능

디지털자산에 적용 가능한 개인정보보호 강화기술 예시

	신원 인증	보유자금 인증	정보 저장	정보 활용	감사
암호화 기술	O	X	O	X	X
동형암호 기술	X	X	X	O	O
디지털 서명	O	O	X	X	O
링(Ring) 서명	X	X	O	X	X
가명화 기술	O	X	X	X	X
영지식 증명	O	O	O	X	O

(추가 고려사항)

□ 개인정보보호 전략 수립 시 개인정보보호 강화기술 外 네트워크 설계, 전자지갑 정책, 불법적인 활동 방지, 처리량과 성능 등 다양한 추가 요소들에 대한 고려가 필요

○ 디지털자산의 성질에 따라 다양한 네트워크 방식(비허가형, 허가형, 중앙집중형, 분산형 등) 중 적합한 네트워크 방식을 선택

○ 신원확인, AML/CFT 등 불법적인 거래를 방지하기 위한 업무에서도 기밀성을 유지하면서 정보를 활용할 수 있도록 전략을 수립

○ 또한, 전자지갑과 관련하여 개인정보보호 관리 책임을 분산시킬 수 있는 다양한 전자지갑 관리 방식도 고려 가능

— 전자지갑이 저장되는 위치에 따라 소프트웨어를 활용하는 핫 월렛, USB 등 별도 물리적 장치에 저장하는 콜드 월렛 방식이 존재

— 또한 전자지갑 관리주체에 따라 이용자가 직접 지갑을 제어하는 비수탁형과 금융기관 등 제3자가 관리하는 수탁형 방식이 존재

3 시사점 및 향후 계획

□ CBDC와 디지털자산 시스템은 **디지털 환경**에서 **금융거래**를 **처리**하는 **공통점**을 가지고 있어, 동 보고서에서 제시한 개인정보보호 전략 수립 방안을 당행 CBDC 관련 연구에 참고할 계획

○ 당행 CBDC 시스템 설계 초기부터 개인정보보호 기술과 정책이 조화롭게 적용될 수 있도록 관련 기술과 정책의 적용 가능성을 점검

○ 또한 CBDC 유통과정별로 **개인정보 흐름을 단계화**하여(수집·이용·저장·파기) **개인정보보호 강화기술 및 정책을 동시에 고려한 개인정보보호 전략 수립**을 추진

— CBDC의 유통과정별로 다양한 개인정보보호 강화기술을 적용하는 실험을 진행

— 개인정보 활용을 위한 이용자 동의를 명확하게 징구하는 한편, 이용자에게 정보 주권(열람권, 정정권, 삭제권 등)을 제공

CBDC 유통과정별 개인정보의 단계별 흐름

CBDC 내 처리되는 개인정보의 단계별 흐름

□ 특히 동 보고서는 기술적 부분을 중점적으로 설명하고자 법적인 고려사항을 배제한 개인정보보호 전략 수립 방안을 제시하고 있어, **현행 개인정보보호 관련 규제환경**을 **검토**하여 **당행 전략**에 **반영**이 필요

○ 국내 개인정보보호법(개인정보처리자의 의무 등) 및 개인정보 관련 금융법상의 요구사항(신원확인, AML/ CFT 등)을 검토하여 정책에 반영 예정

<참고>

주요 개인정보보호 강화기술 현황

□ 암호화 기술(Encryption)

○ 전송·저장된 정보의 기밀성을 유지하는 기본 기술로, '암호키'를 활용하여 암호문으로 변환하고 필요시에 해독할 수 있는 기술

— 비대칭키 암호화는 연관된 서로 다른 키쌍으로 암호화와 복호화를 수행하는 기술로 특정인만 관리하는 '개인키'와 대중에 공개한 '공개키'의 쌍으로 이루어진 암호화 방식

— 대칭키 암호화는 동일한 암호키로 암호화와 복호화를 진행하는 기술로 암호통신을 위해 사전에 송·수신인간 암호키 공유가 필요

□ 가명화 기술(Pseudonymization)

○ 개인정보의 일부를 삭제하거나, 일부 또는 전부를 대체하는 등의 방법으로 특정 개인을 알아볼 수 없도록 처리하는 기술

□ 디지털 서명 기술(Digital Signature)

○ 비대칭키 암호화 기술 기반으로 디지털 서명을 개인키로 암호화하여 상대방에게 전달하고, 상대방은 공개키로 해독하여 서명이 위·변조되지 않음을 확인함으로써 신원을 인증하는 기술

— 링 서명은 서명인의 신원이 식별되지 않도록 디지털 서명시 개인키와 익명의 집합 참가자 전원의 공개키 등 복수 암호키를 활용하는 기술

□ 다자간 계산(MPC: Multi Party Computation)

○ 원본 정보 노출 없이 정보를 분산 및 공동 계산하여 정보의 기밀성을 유지한 상태로 분석이 가능한 기술로 현재 계속 발전 중

□ 동형암호 기술(Homomorphic Encryption)

○ 암호화된 상태의 정보를 해독하지 않고 연산 및 분석 등을 수행함으로써 해독 과정에서 발생할 수 있는 개인정보 침해 우려를 제거하는 기술

□ 영지식 증명 기술(Zero-Knowledge Proof)

○ 자신의 신원 정보 자체를 전달하거나 노출시키지 않고도 자신이 그 정보의 소유주임을 증명하는 기술