비상경제본부 회의 겸
경제관계장관회의
26-9-4
(공개)

공공분야 가상자산 보유·관리체계 개선방안

2026. 4. 10.

관 계 부 처 합 동

순 서

Ⅰ. 추진배경 및 현황

□ 국민의 **가상자산 보유·활용**이 **증가**[*]하면서 수사·징세 등 **법 집행 과정**에서 정부의 **가상자산 취득**도 **증가**[**]

* 국내 등록 계정수(만개): ('22말) 1,178 ('23말) 1,816 ('24말) 2,305 ('25말) 2,591
** 가상자산 강제징수액(억원, 국세청): ('22) 6 ('23) 368 ('24) 381 ('25) 639

○ 그러나, 가상자산 특성에 대한 **기관의 인식 부족, 관리 소홀**로 인해 **공공분야**의 **가상자산 유출 사고**가 **반복 발생**

< 기관별 가상자산 유출·분실 사례 >

- (**검찰청**) 업무 인수인계 과정에서 피싱 사이트에 접속해 가상자산에 접근 가능한 복구구문(니모닉 코드)을 입력하면서 320 BTC(300억원 상당) 탈취('25.8월)
- (**경찰청**) '21.11월 압류 후 USB에 보관한 22 BTC(21억원 상당) 분실 사실 파악('26.2월)
- (**국세청**) 보도자료를 통해 가상자산에 접근 가능한 복구구문(니모닉 코드)이 유출되며 400만 PRTG(수백만원 추정) 탈취('26.2월)

➡ **가상자산 보유·관리 실태 파악을 위한 전수점검 착수**

□ **재경부** 주재 **관계부처 회의**[*](3.4일)를 통해 중앙정부·지방정부·공공기관 등 가상자산 **보유·관리 현황 점검**

* 재경부 차관보(주재), 교육부·행안부·금융위·인사처·검찰·경찰·국세·관세청, 금감원 참석

○ **(보유) 법 집행기관**의 **압수·압류** 등 통한 **취득**이 **대부분**

* 법인의 가상자산 시장 참여 로드맵(금융위, '25.2월)에 따라 법 집행기관, 비영리법인 등의 즉시 현금화 목적 법인계좌 개설 허용

가상자산 보유현황 전수조사 결과(4.6일 기준)

분류	보유기관(금액)	취득 사유
중앙정부	▸ 경찰청(22억원), 검찰청(234억원), 국세청(521억원), 관세청(3억원) 등 **780억원**	▸ 수사·징세 과정에서 **압수·압류** 통해 보유
지방정부	▸ 지방세 징수 중 압류에 대비해 58곳에서 가상자산 계정은 생성했으나, **실제 보유 자산은 없음**	-
공공기관	▸ 적십자사(1.6억원), 서울대병원(2억원) 등 **3.6억원**	▸ **기부금**으로 수령

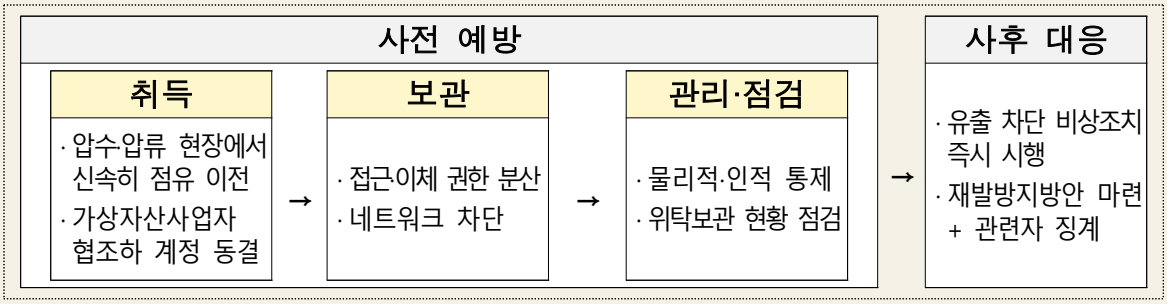
○ **(관리) 대부분 기관**에서 **내부관리 규정·지침**이 **없거나 구체성**이 **부족**(경찰청은 BTC 분실사고 이후 가상자산 압수물 관리체계 개선계획 시행중)

➡ **추가적 사고 방지·대응**을 위해 부처 의견수렴[*]을 거쳐 **관계부처 합동**으로 「**공공분야 가상자산 보유·관리 체계 개선방안**」 마련

* 재경부·금융위·국세청·관세청·검찰청·경찰청·금감원 등 실무협의회(3.12·19·26일)

Ⅱ. 가상자산 관리체계 개선방안

◇ **취득 → 보관 → 관리·점검 → 사고대응**으로 이어지는 가상자산 보유·관리 **全단계 체계적 관리 시스템** 마련



◇ 담당자 **교육훈련, 전담조직 지정** 등 **관리 역량 강화**

1. 보유 · 관리 全단계 체계적 관리 시스템 마련

< 사전 예방 >

□ **[취득] 법 집행**(압수·압류·동결)에 따른 가상자산 **통제권 확보**를 위해 **신속한 점유 이전, 거래소 계정 동결** 실시

○ **개인지갑** 등에 보관중인 가상자산은 압수·압류 **즉시 기관지갑***에 **전송**하는 등 **점유이전**을 **신속히 집행**

* 기관명의 지갑 별도 생성 또는 위탁사업자가 개설한 기관명의 지갑

○ **가상자산사업자**가 **보관**중인 가상자산은 가상자산사업자의 **협조***를 얻어 **법 집행 대상자**의 **거래소 계정 접근 차단**

*「국세징수법」 제55조③항, 「지방세징수법」제61조③항 등 개별법에서 체납자 소유 가상자산을 보관하는 가상자산사업자의 가상자산 이전 협조 의무 규정 중

○ **기부받은 가상자산**의 경우, **수령 즉시 처분**하여 리스크 전면 차단

* 비영리법인의 가상자산 현금화 가이드라인(금융위, '25.5월)에 따라 처분

□ **[기관지갑의 보관] 보관방법별 보안성 강화 조치 시행**

○ **(직접보관)** 가상자산 **접근권한 분산, 네트워크 차단** 등을 통해 가상자산 보관의 **보안성 강화**

- **(접근권한 분산)** 관리기관 지갑 생성시 발급되는 가상자산 **개인키·복구구문** 등 중요 정보의 **2인 이상 분할 확인** 의무화

* 개인키: 가상자산의 보관·전송 등을 위해 생성·이용되는 비공개 암호키
복구구문: 지갑의 도난 및 분실 시 가상자산에 대한 통제권을 복구하기 위해 사용되는 정보

- **(네트워크 차단)** 인터넷 연결이 차단된 **콜드월렛 보관**을 통해 **해킹 등** 사이버보안 위협에 따른 가상자산 **유출 방지**

○ **(위탁보관) 직접보관**에 따른 보안성 조치 + 旣 설정된 최소 인원 충족시에만 가상자산이 이체되도록 하는 **다중서명 체계** 적용

<참고> 콜드월렛 예시

■ 물리적 형태와 무관하게, **가상자산의 보관 및 전자서명 절차**가 **모두 인터넷과 분리된 환경**에서 이루어지는 경우 이를 **콜드월렛**으로 **분류**

하드웨어 월렛	종이 월렛	금속철판월렛
		

□ **[관리 · 점검]** 기관 보유 가상자산 **접근권한 통제, 위탁보관자산**의 **주기적 점검** 의무화 및 **관리 시스템 구축·관리**

○ **(보유자산 관리 강화)** 금고·도어락·CCTV 등 **물리적 통제장치 설치** 및 **출입권한** 목록 **정기 검토·갱신, 출입내역** 주기적 점검·보고

○ **(위탁자산 주기 점검) 위탁보관자산 실사 자료**, 입·출고 등 **거래내역** 및 **보안사고 발생 여부** 등 주기적 점검·보고

○ **(내부관리시스템)** 가상자산 주소 조회·관리, 집행내역 관리, 접근권한 관리 등을 위한 **가상자산 관리 시스템 구축·운영 가능**

< 사후 대응 >

※ **가상자산 보관·관리 중 사고의 유형**

- ■ 개인키·복구구문의 유출 또는 분실
- ■ 해킹·랜섬웨어 등 전자적 침해 공격
- ■ 가상자산의 비정상 거래 또는 무단 전송
- ■ 가상자산 지갑의 물리적 도난·훼손
- ■ 그 밖에 가상자산의 보관·관리에 위협이 되는 상황

□ **[즉시조치] 가상자산 유출** 등 발생시 **비상조치** 즉시 시행 및 **외부 해킹** 등의 경우 **유관기관 통보·보고**

○ **(비상조치)** 신규 가상자산 지갑 생성 및 **잔존자산 즉시 전송, 거래제한, 계정동결**, 관련 **시스템 접근권한 차단** 등

○ **(통보·보고) 피해금액**이 일정 **기준 이상**이거나 **외부 해킹** 확인시 **국정원·경찰청·한국인터넷진흥원**에 즉시 **통보** 및 **재경부·행안부 보고***

* 보고체계 : 중앙정부→재경부 / 공공기관 → 주무부처·재경부 / 지방정부 → 행안부

□ **[후속조치] 재발방지대책**을 포함한 **보고서** 작성 및 **가이드라인 위반**으로 인한 사고 발생시 **관련자 징계** 등 조치

2. 가상자산 관리 역량 강화

□ **[전담조직] 가상자산 관리 규모**에 따라 가상자산 취급 업무 등을 **관리·감독**하는 가상자산 **전담 조직·인력 설치 또는 지정**

○ **보유현황·거래내역 점검**, 기관지갑 관리, 교육·훈련 및 **사고 대응** 등 **가상자산 관리 총괄**

□ **[정기교육] 가상자산 관리 담당자 대상 정기교육 의무화**

○ 가상자산 **지갑 구조**, **개인키·복구구문 관리 방법**, 가상자산 확보·전송·보관 절차, **보안사고 대응** 절차 등 교육

□ **[모의훈련]** 가상자산 **업무 유관부서·전담조직** 등 참여, 가상자산 유출 사고 등 대응 모의훈련 **연 1회 이상** 실시

Ⅲ. 향후 계획

□ **관계부처 합동 가이드라인** 배포 및 **즉시 시행**(4.10일)

○ **재경부**는 **부처·공공기관**, **행안부**는 **지방정부** 대상 **가이드라인 배포**

○ **필요시 기관별** 상황에 맞는 **세부 가이드라인** 수립

별첨 **「정부 · 공공기관 가상자산 보관 · 관리 가이드라인」**

(관계기관 합동)

제1장 총칙

제1조(목적) 이 가이드라인은 정부, 지방자치단체 및 공공기관이 법 집행 및 업무 수행 과정에서 취급하는 가상자산을 안전하게 보관·관리하고, 사고 예방 및 대응에 필요한 최소한의 공통 기준을 정함을 목적으로 한다.

제2조(적용 범위) ① 이 가이드라인은 정부, 지방자치단체 및 공공기관이 다음 각 호의 업무를 수행하는 과정에서 취급하는 가상자산에 적용한다.

1. 「형사소송법」 제215조 내지 제219조에 따른 압수
2. 「국세징수법」 제51조 및 제55조에 따른 압류
3. 「지방세징수법」 제51조 및 제61조에 따른 압류
4. 「관세법」 제26조에 따른 압류 및 제296조, 제303조 내지 제309조, 제313조에 따른 압수
5. 「형사소송법」 제459조 내지 제462조, 제477조 내지 제479조, 제483조, 제484조에 따른 몰수 등 집행
6. 「기부금품의 모집·사용 및 기부문화 활성화에 관한 법률」 제4조 등 관련 법령에 따른 기부금 수령
7. 그 밖에 다른 법령에 따라 가상자산에 대한 압수·압류·동결·보관 등의 권한이 부여된 경우

② 타 기관과 공동으로 확보한 가상자산에 대해서는 별도의 합의가 없는 한 이 가이드라인을 준용하여야 한다.

제3조(용어의 정의) 이 가이드라인에서 사용하는 용어는 다음과 같다.

1. “가상자산”이란 「가상자산 이용자보호 등에 관한 법률」(이하 ‘가상자산이용자보호법’이라 한다) 제2조 제1호에 따른 가상자산을 말한다.
2. “가상자산사업자”란 「특정 금융거래정보의 보고 및 이용 등에 관한

법률」(이하 ‘특정금융정보법’이라 한다) 제7조에 따라 금융정보분석원장에게 신고 수리된 가상자산사업자를 말한다.

3. “가상자산 지갑”이란 가상자산 주소, 개인키 등 가상자산에 대한 접근 및 통제에 필요한 정보를 생성·저장·관리하고, 이를 통하여 가상자산의 보관·전송 등을 가능하게 하는 전자적 또는 물리적 수단을 말하며, 다음 각 목의 구분에 따라 어느 하나에 해당하는 것을 포함한다.

가. 지갑 형태에 따른 구분

1) 하드웨어 지갑: 외부 네트워크로부터 분리된 물리적 장치를 이용하여 개인키 등을 생성·저장·관리하는 가상자산 지갑

2) 소프트웨어 지갑: 응용프로그램 또는 시스템 소프트웨어를 이용하여 개인키 등을 생성·저장·관리하는 가상자산 지갑

나. 네트워크 연결 여부에 따른 구분

1) 콜드월렛: 인터넷 등 외부 네트워크로부터 분리된 상태에서 관리되는 가상자산 지갑

2) 핫월렛: 인터넷 등 외부 네트워크에 연결된 상태에서 관리되는 가상자산 지갑

다. 지갑 제공·관리 주체에 따른 구분

1) 가상자산사업자 지갑: 가상자산사업자가 이용자를 대신하여 개인키를 생성·보유·관리하거나 이에 준하는 방식으로 가상자산에 대한 접근 및 통제를 수행하는 지갑

2) 개인지갑: 이용자가 개인키를 직접 생성·보유·관리하여 가상자산에 대한 접근 및 통제를 수행하는 지갑

4. “가상자산 주소”란 블록체인 상 가상자산의 송·수신 및 보관내역을 식별하거나 가상자산 전송을 위하여 이용되는 불특정 다수에게 공개된 정보를 말한다.

5. “개인키”란 가상자산의 보관·전송 또는 그 밖의 관리를 위하여 생성·이용되는 비공개 암호키로서, 해당 가상자산 주소에 대한 접근·통제 권한을 부여하고 가상자산 전송을 승인하는 데 필요한 정보를 말한다.

6. “복구구문”이란 지갑의 도난 및 분실 시 가상자산에 대한 통제권을 복구하기 위해 사용되는 정보로, 복잡한 개인키를 사전에 정의된 일련의 단어 조합으로 대체하여 표현한 것을 말한다.

7. “관리기관”이란 이 가이드라인을 적용받는 정부, 지방자치단체 및 공공기관으로서, 법 집행 및 업무 수행 과정에서 가상자산의 취급에 관한 보관·관리 업무를 수행하는 기관을 말한다.
8. “집행부서”란 관리기관 내에서 수사, 조사, 재판, 징수, 기부금 수령 또는 그 밖의 법 집행 등의 업무 수행 과정에서 가상자산을 직접 취급하는 부서를 말한다.
9. “가상자산의 전송”이란 블록체인을 통해 가상자산을 어느 하나의 가상자산 주소에서 다른 가상자산 주소로 이전하는 것을 말한다.
10. “가상자산의 취급”이란 가상자산에 대하여 제2조 각 호에 따라 압수·압류·동결 등을 하거나 이를 전송·보관·관리·반환하는 등 가상자산에 대하여 행하는 일체의 행위를 말한다.
11. “가상자산의 보관”이란 관리기관이 취급하는 가상자산 및 그에 대한 접근·통제수단을 기관지갑등 또는 수탁기관을 통하여 안전하게 유지하고, 무단 전송·분실·도난·훼손 또는 유출을 방지하는 것을 말한다.
12. “가상자산의 관리”란 관리기관이 취급하는 가상자산에 대하여 보관 현황 확인, 지갑 또는 계정 관리, 접근권한 관리, 기록 및 대장 관리, 실재성 점검, 위탁 관리, 교육·훈련 및 사고 예방·대응을 수행하는 것을 말한다.
13. “가상자산 거래”란 가상자산사업자 계정 또는 블록체인상에서 이루어지는 가상자산의 매매·교환·입출고·전송 등을 말한다.
14. “기관지갑등”이란 관리기관이 가상자산의 보관·관리를 위하여 사용하는 지갑 또는 계정으로서, 다음 각 목을 모두 포함한다.
    가. 제9조에 따라 관리기관이 직접 생성한 지갑으로서, 개인키(이에 준하는 접근수단을 포함한다)를 직접 보관·관리·통제하는 지갑
    나. 제11조에 따라 가상자산사업자에게 가상자산의 보관·관리를 위탁하기 위하여 체결된 계약에 따라 관리기관 명의로 개설된 지갑 또는 계정
    다. 가상자산사업자에게 관리기관 명의로 개설된 계정으로서, 나목에 따른 위탁관리에 해당하지 아니한 계정
15. “가상자산 압수”란 형사소송법 등에 따른 수사 과정에서 가상자산을 수사기관의 가상자산 지갑 또는 계정으로 전송하거나 그에 필요한

지갑·개인키·복구구문 등을 확보·보관하는 행위를 말한다.

16. “가상자산 압류”란 국세·지방세·관세 등 체납처분 또는 강제징수 절차에서 체납자의 가상자산에 대한 법률상 또는 사실상의 처분을 금지하고 그 재산을 환가할 수 있는 상태에 두는 집행처분을 말한다.
17. “가상자산 계정의 동결”이란 가상자산사업자가 보관 중인 가상자산에 대한 모든 거래를 일시적으로 제한하는 것을 말한다.
18. “티커”란 가상자산 식별을 위한 영문자 또는 숫자로 축약된 코드를 말한다. (예: 비트코인/BTC, 이더리움/ETH)
19. “메인넷”이란 독립적인 블록체인 네트워크를 말하며, 가상자산 주소의 생성, 가상자산의 발행·전송 등을 처리할 수 있는 플랫폼을 말한다.

제4조(기본 원칙) 관리기관은 가상자산 보관·관리에 있어 다음 각 호의 원칙을 준수하여야 한다.

1. 보안성 : 해킹 등으로 인한 가상자산의 탈취, 가상자산 지갑의 물리적 도난·파손에 대비한 보안 체계를 구축한다.
2. 무결성 : 가상자산의 취급과정 전반에 걸쳐 자산의 상태가 임의로 조작되지 않음을 보장하고, 블록체인상 잔액과 내부 기록의 상시 일치성을 유지한다. (단, 가상자산 전송 수수료 등 블록체인 네트워크 이용에 따라 불가피하게 발생하는 비용은 예외로 한다)
3. 책임성 및 투명성 : 가상자산 취급과 관련된 모든 행위와 행위자를 특정하여 기록하고, 사후 점검·감사가 가능하도록 절차를 표준화한다.
4. 최소 접근 : 직무상 필요한 최소 인원에게만 접근권한을 부여하고, 정기적으로 점검한다.

제2장 전담조직 및 역할

제5조(전담조직등의 설치 등) ① 관리기관은 가상자산 관리 규모에 따라 가상자산의 취급 및 보관·관리 업무를 관리·감독하는 전담조직 또는 전담인력(이하 “전담조직등”이라 한다)을 설치 또는 지정하여야 한다.

② 전담조직등은 다음 각 호의 기능을 수행한다.

1. 압수·압류 등에 따른 가상자산의 보유현황 및 조치 상태 등의

점검·관리
2. 가상자산의 압수·압류·보관·관리 등 관련 규정 제·개정
3. 지갑 구조 설계, 생성·폐기, 키 관리 등 가상자산 지갑 관리
4. 가상자산사업자와의 협력·계약(제11조에 따른 위탁관리를 포함한다) 관리
5. 기록·점검·평가·보고 체계 운영
6. 비상조치 수립·시행, 교육·훈련 계획·실시 등 보안·사고 대응
7. 그 밖에 가상자산의 안전하고 효율적인 취급·보관·관리를 위하여 전담조직등이 필요하다고 인정하는 행위

제3장 가상자산 압수·압류·동결

제6조(가상자산 압수·압류의 원칙) ① 집행부서가 피압수자·체납자(이하 "피압수자등") 명의의 가상자산 지갑 등에 보관중인 가상자산을 압수·압류할 경우에는 가상자산의 점유 이전(해당 가상자산에 대한 통제권 확보를 포함한다)을 기본 원칙으로 하며, 현장에서 가상자산을 기관지갑등으로 전송하여야 한다. 다만, 현장 여건상 즉시 전송이 곤란한 경우 등 불가피한 경우에는 피압수자등의 지갑 접근을 차단하거나 지갑 자체를 압수하는 등 임시 통제조치를 취한 후 신속하게 전송하여야 한다.
② 관리기관은 복수의 담당자로 하여금 상호견제가 가능하도록 책임과 역할을 분리하여 기관지갑등을 관리하여야 한다.

제7조(가상자산 압수·압류 등의 집행) ① 집행부서는 피압수자등이 직접 보관하는 가상자산에 대하여 관련 법령 등에 따른 적법한 절차를 거쳐 보유 사실을 확인하고 이를 기관지갑등으로 전송하는 방법으로 압수·압류 등을 집행하여야 한다.
② 집행부서는 압수·압류 등의 집행 전 다음 각 호의 사항을 확인하여야 한다. 다만, 사전에 확인이 불가한 경우에는 집행 과정에서 이를 확인할 수 있다.
1. 가상자산의 한글명칭, 티커
2. 메인넷 종류, 컨트랙트 주소

3. 송수신 가상자산 주소, 수량
4. 피압수자등이 직접 보관하는 지갑의 종류, 접근수단 보유 여부 및 접근 가능 여부

③ 집행부서는 본 전송에 앞서 최소 전송단위 수준으로 소액 전송 테스트를 실시하여, 수신 가상자산 주소 오기입, 메인넷 오류 등으로 인한 전송 실패 등을 예방하여야 한다. 다만, 가상자산 전송규모가 관리기관이 정한 기준에 따라 소액일 경우 테스트를 생략할 수 있다.

④ 제3항의 소액 전송 테스트 결과 이상이 없을 경우 본 전송 과정을 실시하여야 한다.

⑤ 집행부서는 집행 과정의 객관성·투명성 확보를 위해 피압수자등을 전송 과정에 참여하게 하고, 전송 과정을 녹화·기록하여야 한다. 다만, 수사·재판상 필요한 경우에는 그러하지 아니하며, 복구구문 등 중요정보가 노출되지 않도록 주의하여야 한다.

⑥ 집행부서는 전송 완료 후 가상자산 송수신 주소의 잔고 변동현황, 블록체인 거래내역을 피압수자등과 상호 확인·서명하고, 가상자산 전송결과보고서 등을 작성·보관하여야 한다. 결과보고서에는 제2항 각호의 사항과 압수일(압류일), 평가금액, 보관방식, 가상자산 주소 또는 가상자산사업자 계정, 담당자 등을 포함하여야 한다.

제8조(가상자산사업자에 대한 집행) ① 집행부서는 가상자산사업자가 보관하고 있는 피압수자등의 가상자산에 대하여 관련 법령 등에 따라 적법한 절차를 거쳐 압수·압류·몰수 또는 동결·추징보전 등의 조치를 취하여야 한다.

② 제1항에 따라 조치를 하는 경우 집행부서는 다음 각 호의 사항을 포함하여 가상자산사업자에게 서면으로 요청하거나 통지하여야 한다.

1. 피압수자등을 식별할 수 있는 정보(이용자 성명, 실명번호, 휴대전화번호 등)
2. 가상자산의 종류 및 수량
3. 조치의 종류 및 기간이 정하여진 경우 그 기간
4. 근거 법령 및 영장·명령서·결정서 등 관련 서류
5. 기관지갑등으로의 이전이 필요한 경우 그 주소 또는 계정

③ 집행부서는 제1항에 따른 조치의 완료 여부, 조치 시점, 거래 제한 범위, 당시 보관 중인 가상자산의 종류·수량 및 기관지갑등으로 이전된 경우 그 내역을 확인하여 작성·보관하여야 한다. 다만, 해당 사항이 전자적으로 기록되는 경우에는 해당 전자기록을 작성·보관할 수 있다.
④ 집행부서는 제1항에 따라 조치된 계정 또는 가상자산의 보관·조치 현황 및 특이사항(예: 거래유의종목 지정, 거래지원 종료 여부 등)을 주기적으로 확인하고, 그 결과를 기록·관리하여야 한다.
⑤ 제1항에 따른 조치의 해제가 필요한 경우에는 관련 법령 등에 따른 적법한 절차를 거쳐 해제를 요청하거나 통지하고, 그 사유 및 일시를 기록·관리하여야 한다.
⑥ 가상자산사업자는 제1항에 따른 조치와 관련하여 관리기관의 업무 수행에 협조하여야 한다.
⑦ 제1항에 따른 조치 중 가상자산을 기관지갑등으로 이전하는 경우에는 제7조 제3항부터 제6항까지를 준용한다.

제4장 가상자산 지갑의 생성 및 보관·관리

제9조(가상자산 지갑의 생성) ① 관리기관은 압수·압류한 가상자산의 보관·관리를 위해 직접 가상자산 지갑을 생성할 수 있다.
② 지갑 생성 시 쓰이는 PC 등 전자기기에 대해 해킹, 악성코드 감염에 대비하여 보안성을 확보하여야 한다. (예: 백신 등 보안프로그램 설치·최신화, 불필요한 프로그램 삭제, 인터넷 사용 제한, QR코드 인쇄를 통한 가상자산주소 전달 등)
③ 지갑 생성 시 생성되는 개인키, 복구구문, PIN 번호 등 중요정보는 2인 이상의 담당자가 각자 맡은 부분만을 분할하여 확인하여야 한다. 이 경우 담당자 간에 서로의 분할기록 내용을 직접 낭독하거나 촬영·녹음되지 않도록 유의하여야 한다.
④ 지갑 주소의 개인키, 복구구문, PIN 번호는 종이, 철판 등 비전자적 방법으로 기록하고 봉인한 후, 물리적으로 서로 다른 장소에 분산 보관하여야 하고, 중요정보는 평문 파일, 사진, 메신저, 전자우편 등으로 저장·전송하여서는 아니 된다. (예: 복구구문이 24개의 영단어인 경우,

관리자A가 1~12번, 관리자B가 13~24번 영단어를 분할하여 기록관리)
⑤ 복구구문은 개인키를 복구할 수 있는 일종의 마스터키 역할을 수행하므로, 권한이 없는 제3자가 접근하지 못하도록 통제하여야 한다.
⑥ 사건별, 피압수자등별 지갑주소를 각각 생성하여 분리 관리하고, 가상자산 주소는 가상자산 압수·압류 등의 집행 및 수량 관리 등을 원활히 수행하기 위하여 전자적 방법 등으로 지갑주소 관리대장을 기록·관리하여야 한다.

제10조(가상자산 지갑의 보관) ① 가상자산 지갑, 개인키, 복구구문, PIN 번호 등은 봉인된 상태로 다음 각 호의 통제장치를 적용하여야 한다.

1. 물리적 통제 : 외부인의 접근이 통제되는 독립된 공간, 잠금장치(예: 금고, 도어락 등) 설치, CCTV 설치, 인터넷 연결 제한(콜드월렛 보관) 등
2. 인적 통제 : 출입·접근권한 관리, 접근이력 기록 등

② 전담조직등은 출입권한 목록을 정기적으로 검토·갱신하고, 출입대장, CCTV 기록 등을 통해 출입권한에 따른 실제 출입내역을 주기적으로 확인하여야 한다.
③ 관리기관은 다음 각 호의 어느 하나에 해당하는 경우 새로운 복구구문이나 개인키로 신규 가상자산 지갑을 생성하여 자산을 전송한 후, 기존 가상자산 지갑(복구구문 및 개인키를 포함한다)은 폐기 처리하여야 한다.

1. 해킹, 가상자산 탈취 등이 발생하였거나 발생할 것으로 예상되는 경우
2. 개인키, 복구구문 등 중요정보가 유출되었거나 유출될 것으로 예상되는 경우
3. 그 밖에 전담조직등이 가상자산의 선제적 보호조치가 필요하다고 인정하는 경우

④ 관리기관은 가상자산의 유출·도난 및 전송 과정에서 발생할 수 있는 사고 예방을 위하여 다음 각 호의 사항을 포함한 보안대책을 내규로 마련하여야 한다.

1. 가상자산 보관 장소 접근 통제 및 출입 기록 관리
2. 봉인 상태 및 보관 현황의 정기적 점검

3. 담당자 변경 시 인수인계 절차 및 접근권한 즉시 회수
4. 사고 발생 시 긴급 대응 절차

제11조(가상자산의 위탁보관) ① 관리기관은 가상자산의 안전한 보관 및 효율적 관리를 위하여 필요한 경우 별도 계약 등을 통해 다음 각 호의 사항을 외부 전문기관(이하 “수탁기관”이라 한다)에 위탁할 수 있다.

1. 압수·압류 가상자산의 전송 관련 지원
2. 압수·압류 가상자산의 보관 및 관리
3. 보관 중인 가상자산에 대한 주기적 실재성 점검 및 그 결과의 보고
4. 그 밖에 관리기관이 필요하다고 인정하는 업무

② 관리기관은 가상자산사업자 중에서 다음 각 호의 사항을 고려하여 수탁기관 선정기준을 마련하여야 한다.

1. 위탁보관에 필요한 보안성
2. 관련 업력, 재무건전성, 과거 제재이력 등 사회적 신용
3. 보관·관리 업무 수행의 편의성
4. 그 밖에 관리기관이 중요하다고 인정하는 사항

③ 제1항에 따른 수탁기관과 계약을 체결시 다음 각 호의 사항을 포함하여야 한다.

1. 위탁 업무의 범위 및 방법
2. 보관 중인 가상자산의 실재성 점검 주기 및 결과 보고 방법
3. 관리기관의 실질적 통제 권한 보장
4. 수탁기관의 보안 의무 및 사고 발생 시 즉시 통보 의무. 이 경우 제19조에 따른 사고 대응 절차를 준용한다.
5. 계약 해지 또는 수탁기관 변경 시 자산 반환 절차
6. 수탁기관의 폐업, 파산, 「특정금융정보법」에 따른 가상자산사업자 신고 기간 만료 및 말소 등 긴급상황 발생 시 대응 절차

제12조(위탁보관 가상자산의 보관·관리) ① 수탁기관은 다음 각 호에 따라 관리기관이 위탁한 가상자산을 안전하게 보관하여야 한다.

1. 기관별, 피압수자등별 지갑 주소를 각각 생성하여 분리 보관
2. 다른 이용자 자산과 분리 보관

3. 콜드월렛 보관
4. 재해·재난, 도난 등에 대비하여 보안시설 구비, 키 분실 방지 대책 및 백업·복구체계 마련
5. 다중서명 체계, 암호화 등 보안조치 적용
6. 그 밖에 관리기관이 필요하다고 인정하는 사항

② 관리기관의 요청에 따라 수탁기관에서 가상자산이 출고되는 경우, 사전에 관리기관 내 적절한 전결권자의 승인을 받아야 한다. 이 경우 수탁기관은 임직원 1인이 단독으로 출고를 처리할 수 없도록 업무 및 역할을 명확히 분장하여야 한다.

③ 관리기관은 수탁기관의 가상자산 실재성 점검자료, 입출고 등 거래내역, 보안사고 발생 여부 등을 주기적으로 점검하여야 한다.

④ 관리기관은 수탁기관이 부여한 이용자식별번호(ID), 비밀번호, 추가 인증수단 등 중요정보가 외부에 유출되지 않도록 관리하여야 한다.

⑤ 수탁기관의 폐업, 파산, 「특정금융정보법」에 따른 가상자산사업자 신고기간 만료 또는 말소, 그 밖의 사유로 위탁관리가 불가능하게 된 경우, 관리기관은 즉시 대체 수탁기관을 지정하거나 직접 보관 체계로 전환하는 등 필요한 조치를 취하여야 한다.

제5장 가상자산 보관·관리의 점검 및 기록관리 등

제13조(가상자산 보관·관리의 점검) 집행부서는 다음 각 호의 사항을 주기적으로 점검하여 전담조직등에 보고하고, 미흡한 사항에 대해서는 개선조치를 하여야 한다. 다만, 진행중인 수사·재판에 관련된 정보 또는 공소의 제기 및 유지에 관한 사항은 보고 대상에서 제외할 수 있다.

1. 제7조 제6항에 따른 결과보고서의 작성·보관 여부
2. 확보된 가상자산과 결과보고서 간 동일종류·동일수량 보관·관리 여부
3. 제8조 제3항에 따른 내역의 작성·보관 여부
4. 제8조에 따라 조치된 계정 또는 가상자산의 조치·해제 상태와 관련 기록의 일치 여부
5. 제12조에 따른 위탁보관 가상자산의 보관·관리 현황, 실재성 점검 자료, 입출고 등 거래내역 및 보안사고 발생 여부

6. 개인키, 복구구문, PIN 번호 등 중요정보에 대한 봉인 해제, 훼손 또는 비인가 접근 여부
7. 압수물 보관장소 및 봉인물품 등에 대한 출입·접근권한 관리 현황 및 실제 출입내역

제14조(전산시스템의 구축·운영) ① 관리기관은 가상자산의 안전한 관리와 체계적이고 효율적인 업무 수행을 위하여 가상자산 관리 시스템을 구축하여 운영할 수 있다.

② 제1항에 따라 가상자산 관리 시스템을 구축·운영하는 경우에는 다음 각 호의 기능을 포함하여야 한다.

1. 가상자산 주소 조회·관리
2. 가상자산 압수·압류 등 집행내역 조회·관리
3. 기관지갑등의 가상자산 수량 및 입출고 등 거래내역의 조회·관리
4. 시스템 접근권한 관리 및 인증
5. 시스템 접근 및 작업 이력 기록

③ 관리기관은 제2항 제4호에 따른 접근권한을 업무 수행에 필요한 최소한의 범위에서 부여하여야 한다.

제15조(가상자산의 기관 간 전송) 보관 중인 가상자산에 대하여 기관 간 전송이 필요한 경우에는 보안성·무결성, 증거능력 등의 문제가 발생하지 않도록 기관 간 협의한 방식으로 전송하여야 한다.

제16조(기부 가상자산의 처리) 관리기관이 가상자산을 기부받아 현금화하려는 경우에는 금융위원회가 마련한 「비영리법인의 가상자산 현금화 가이드라인」에서 정한 절차를 준용한다.

제6장 교육 및 훈련

제17조(교육) ① 관리기관은 가상자산의 안전한 관리 및 사고 예방을 위하여 가상자산 관리 업무 담당자를 대상으로 정기적인 교육을 실시하여야 한다.

② 교육 내용에는 다음 사항이 포함되어야 한다.

1. 가상자산·블록체인의 기본 개념
2. 가상자산 지갑 구조에 대한 이해
3. 개인키 및 복구구문 관리 방법
4. 가상자산 확보·전송·보관 절차
5. 지갑 관리대장 작성 및 가상자산 보유현황 관리 방법
6. 보안사고, 오송금 예방 및 대응 절차
7. 사고 발생 시 비상조치 및 보고 절차
8. 위탁관리 운영 시 유의사항

③ 관리기관은 교육 실시 내역을 기록·관리하여야 한다.

④ 관리기관은 필요한 경우 관계기관 합동 교육 또는 외부 전문기관을 활용하여 교육을 실시할 수 있다.

제18조(모의훈련)

① 관리기관은 가상자산 유출 등 사고 대응을 위한 모의훈련을 연 1회 이상 실시할 수 있다.

② 관리기관은 제1항에 따른 모의훈련을 실시하는 경우 집행부서, 전담조직등, IT·보안 부서 등을 참여시킬 수 있으며, 필요한 경우 외부 전문기관 또는 관계기관 합동으로 실시할 수 있다.

③ 관리기관은 제1항의 모의훈련 결과를 평가하여 개선계획을 수립할 수 있다.

제7장 사고 대응 및 책임

제19조(사고 대응) ① 집행부서와 수탁기관은 다음 각 호의 어느 하나에 해당하는 경우 즉시 전담조직등에 보고하여야 한다.

1. 개인키·복구구문의 유출 또는 분실
2. 해킹·랜섬웨어 등 전자적 침해 공격
3. 가상자산의 비정상 거래 또는 무단 전송
4. 가상자산 지갑의 물리적 도난·훼손
5. 그 밖에 가상자산의 안전한 보관·관리에 중대한 위협이 되는 상황

② 전담조직등은 제1항에 따른 보고를 받은 즉시 다음 각 호의 비상 조치를 취하여야 한다.

1. 신규 가상자산 지갑을 생성하여 잔존 자산을 즉시 전송
2. 수탁기관·가상자산사업자에 대한 거래 제한 또는 계정 동결 요청
3. 가상자산사업자에 대한 비정상 거래 차단 요청
4. 관련 시스템 접근 권한 즉시 차단 및 접속 이력 보존

③ 전담조직등은 사고의 중대성을 고려하여 다음 각 호의 구분에 따른 내부 보고기준을 마련하고, 유관기관에 통보하여야 한다.

1. 의무 통보: 피해 금액이 관리기관이 정한 규모 이상이거나 외부 해킹이 확인된 경우 국정원·경찰청·한국인터넷진흥원에 즉시 통보
2. 임의 통보: 그 밖의 경우 필요에 따라 유관기관에 통보

④ 관리기관은 사고 발생 후 다음 각 호의 후속 조치를 취하여야 한다.

1. 사고 경위 및 피해 현황을 포함한 초기 보고서 작성
2. 사고 원인 분석, 피해 범위 확정 및 재발 방지 대책을 포함한 최종 보고서 작성
3. 피압수자등 및 이해관계인에 대한 사고 사실 통보
4. 재발 방지 대책의 이행 여부를 주기적으로 점검

⑤ 관리기관은 제3항의 의무 통보 대상에 해당하는 사고 발생 시 다음 각 호의 구분에 따라 즉시 보고하여야 한다.

1. 정부의 경우 : 재정경제부
2. 지방자치단체의 경우 : 행정안전부
3. 공공기관의 경우 : 주무부처, 재정경제부

⑥ 재정경제부 및 행정안전부는 제5항에 따른 보고를 받은 경우 금융위원회의 협조를 얻어 관계기관 협의, 개선 권고, 제도 보완 등 필요한 조치를 취할 수 있다

제20조(위반 시 책임) ① 관리기관은 이 가이드라인의 위반으로 가상자산의 분실·탈취·부정사용 등이 발생한 경우, 관련자에 대하여 징계·형사 고발 등 필요한 조치를 취할 수 있다.

② 관리기관은 기관별 인사·감사 규정에 따라 위반 유형과 제재 기준을 마련·적용하여야 한다.

제21조(세부 가이드라인의 수립 등) ① 관리기관은 이 가이드라인을 토대로 해당 기관의 업무 특성을 반영한 세부 가이드라인을 자율적으로 마련하여 시행할 수 있다.
② 관리기관은 제1항에 따라 세부 가이드라인을 마련한 경우 근거 법령 개정, 실무 운영사례 등을 반영하여 이를 주기적으로 수정·보완하여야 한다.

부 칙
제1조(시행일) ① 이 가이드라인은 발표 즉시 시행한다.
② 제14조에 따른 가상자산 관리 시스템 구축 등 전산 관련 사항은 각 기관별 준비 상황을 고려하여 시스템이 구축되는 대로 시행할 수 있다.