정보보호관리체계 특별점검 및 기술지원 수행

가상자산사업자 정보보호관리체계 특별점검 안내

2023. 06.

가상자산서비스 제공자의 정보보호 관리체계 구축·운영 점검 및 기술 지원을 통한 정보보호 수준 강화 및 종합적인 보호대책 수립

01 특별점검 개요

"가상자산서비스 제공자(거래소/지갑/보관서비스, NFT, 메타버스 등)의"
정보보호 관리체계 구축·운영 점검 및 기술 지원을 통한
정보보호 수준 강화 및 종합적인 보호대책 수립

정보보호 관리체계 점검

정보보호관리체계 운영현황 점검

가상자산서비스 제공사 10개 기관 점검
- 정보보호관리체계 80개 점검항목 및 가상자산 사업자를 위한 56개 세부점검항목 포함
- ISMS 인증기준에 따라 기술적·관리적·물리적 영역 및 개인정보에 대한 점검 실시
- 3인 1조의 전문가로 구성된 현장 점검 인력이 대한 서면/현장심사 수행

점검활동에 대한 결과 분석
- 특별점검 결과보고서, 만족도조사 및 수준 측정
- 대상 사업자 담당자와의 회의를 통해 상호간 결과를 확인

관리체계 구축 기술지원

중소 가상자산사업자 기술지원

다양한 기법의 취약점 점검 및 대응 지원
- AWS Sheild, Trusted Advisor 등과 같은 Managed 서비스 및 3rd party 솔루션 활용
- OSINT(Open Source Intelligence) 검색엔진을 활용한 표면웹(Surface Web) 사이버 위협 정보 수집
- MITRE D3FEND 기반의 방어체계 구축 및 보호대책 수립 지원

정보보호관리체계 수립 지원
- 정보보호 정책 · 지침 작성 지원
- 자산식별에 대한 기준 수립 지원
- 정보보호관리체계 운영명세서 작성 방안 제시

ISMS 운영 후속조치 지원

보완조치 지원 및 모범사례 제시

결함사항 보완조치 가이드 제공
- 발견된 결함사항을 조치할 수 있도록 보완조치 가이드를 제공
- 가상자산서비스에 적합한 정보보안 모범사례 등 지속적 관리방안 제시

정보보안 모범사례 제시
- 가상자산서비스에 적합한 모범사례를 확보하여 적용 가능한 방안 제시
- 정보보호 관리체계를 지속적으로 관리할 수 있는 방안 제시

지원 효과분석 및 발전방향 제시

효과성 분석 및 발전방향 제시

정보보호 관리체계 운영수준 측정
- 특별점검 전·후 정보보호 관리체계 운영수준을 측정
- 보안 취약점 개선 및 결함사항 보완조치 이행 등 기술지원에 따른 효과 분석

발전방향 제시
- 특별점검 시 발견된 주요 보안이슈 및 현장의 의견수렴
- 가상자산사업자의 보안 수준 향상을 위한 제도적 발전방향을 제시

02 점검 대상 및 일정

1 사업 목적	가상자산서비스 제공자의 안정적 서비스 제공과 이용자 보호를 위한 정보보호 관리체계 구축·운영현황 점검 및 기술지원
2 점검 대상	ISMS 인증 및 예비인증을 취득하지 않은 가상자산서비스 제공자(거래소, 지갑, 보관서비스, NFT, 메타버스 등
3 점검 일정	2023년 7월 ~ 2023년 10월 • 사업자 당 5영업일 소요 예정 • 세부 점검 일정은 첨부 '특별점검 신청서' 참조
4 점검 항목	(필수항목) 정보보호 관리체계 통제항목(80개) 및 가상자산사업자 세부통제항목(56개) (선택항목) 클라우드 보안 점검도구 활용 • (예) AWS GuardDuty, Inspector, Detective, Azure Defender 등
5 지원 방안	점검 전후 수준 측정을 통한 조치 방안 가이드 제공 및 기술 지원 정보보호 관리체계를 지속적으로 운영할 수 있도록 후속조치 지원 현장 이슈 수렴 및 사업자의 보안 수준 향상을 위한 발전방향 제시

03 점검 수행 절차

가상자산사업자 대상 정보보호 관리체계 구축·운영현황에 대해 서면·현장평가를 수행하여 운영현황 및 미비점을 포함하여 결과보고서를 작성하고, 대상 사업자 담당자와의 회의를 통해 상호간 결과를 확인합니다.

점검 대상 사업자 선정

KISA와 협의를 통하여
특별점검 사업에 적합한
대상 사업자 선정

점검 항목 및 방법론 적용

사업자 환경에 따른
세부 점검항목 및
클라우드 보안 점검도구
활용방안 수립

운영현황 점검

사업자가 제출한 증적자료 및 실사를 통해 정보보호 관리체계 운영 적정성 확인

- 정보보호 정책, 지침, 절차 등 내부규정 존재 여부
- 해당 규정의 인증기준 충족 여부 평가
- 담당자 인터뷰, 관련 시스템 확인을 통한 기술적·물리적 보호대책 수립
- 운영현황에 대해 서면/현장점검 수행

점검 결과 분석

특별점검 결과보고서,
만족도조사, 통계, 회의록 등
작성 및 보고

후속조치 지원

결함사항 보완조치 지원 및
관리체계 지속가능성을 위한
방안 제시

발전방향 제시

특별점검 전·후 수준측정 및
보안성 강화를 위한
제도적 발전방향 제시

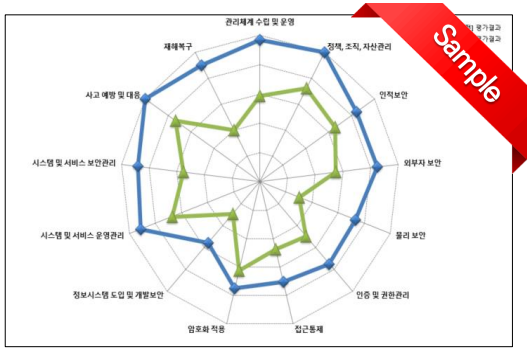
04 운영현황 분석

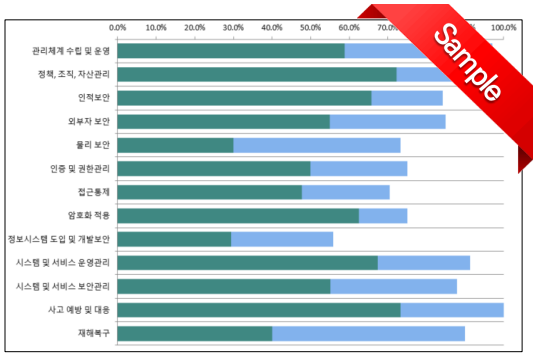
Key point 정보보호 관리체계(ISMS) 운영현황 분석을 위하여 인증기준에 따른 적합성 여부를 인터뷰 및 실사 등을 통해 점검합니다.

정보보호관리체계(ISMS) 운영현황 분석

1. 관리체계 수립 및 운영 (4개 분야, 16개 통제사항)	2. 보호대책 요구사항 (12개 분야, 64개 통제사항)	
1.1 관리체계 기반 마련	2.1 정책, 조직, 자산관리	2.8 정보시스템 도입 및 개발 보안
1.2 위험관리	2.2 인적보안	2.9 시스템 및 서비스 운영 관리
1.3 관리체계 운영	2.3 외부자 보안	2.10 시스템 및 서비스 보안관리
1.4 관리체계 점검 및 개선	2.4 물리 보안	2.11 사고 예방 및 대응
	2.5 인증 및 권한관리	2.12 재해복구
	2.6 접근통제	
	2.7 암호화 적용	

정보보호관리체계(ISMS) 현황 분석 결과 (예시)





정보보호 현황 분석 절차

정보보호 정책·지침 검토	정보보호 정책·지침의 적정성 검토
⌄	
정보보호 활동에 대한 증적 검토	인증기준 별 정보보호 정책·지침 준수 여부 및 활동 증적 검토
⌄	
인터뷰 및 실사	인증기준 별 담당자 인터뷰 및 현장 실사
⌄	
정보보호 현황 분석	기술적 · 관리적·물리적 정보보호 현황 분석

05 관리체계 구축 지원

Key point 운영현황 분석 결과와 정보보호 정책 및 지침을 검토하여 정보보호관리체계 구축을 위한 기술지원 방안을 제시합니다.

정보보호 정책 및 지침 제·개정 지원

관련 법률 분석 (예시)

정보보호 관련 법률
- 정보통신망법/시행령/규칙

개인정보보호 관련 법률
- 개인정보보호법/시행령/규칙

가상자산 관련 법률
- 특정금융거래법/시행령/규칙

법/규제 준거성 및 정보보호관리체계 분석 결과 요건 정의
- 관련 법령 분석, 내부 정책 및 지침 검토
- 정보보호관리체계 분석 결과에 따른 개선사항 도출
- 도출된 개선 사항들에 대한 반영 방안 협의

정보보호 정책 및 지침 제·개정 (예시)

제·개정 사항에 대해 신구 대조표 작성

Sample

정보보호 조직 운영지침	
As-IS	제 3항 (정보보호 최고 책임자) ① 정보보호 책임자 지정 후 과학기술정보통신부에 신고하여야 합니다.
To-Be	제 3항 (정보보호 최고 책임자) ① (생략) ② 〈신설〉 정보보호 책임자 지정 시 제 4항의 업무 외의 다른 업무를 겸직할 수 없다.
개정사유	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3(정보보호 최고책임자의 지정 등)제3항 신설에 따른 관련 조항 추가

정보보호관리체계 운영 명세서 작성 가이드 제공 (예시)

Sample

통제 항목	ISMS 인증심사를 위한 정보보호관리체계 인증기준 (관리체계 수립 및 운영 16개, 보호대책 요구사항 64개 총 80개)
통제 내용	관리체계 수립 및 운영 요구사항, 보호대책 요구사항에 대한 인증기준 별 의미하는 바를 작성
수립 여부	관리체계 수립 및 운영은 필수적으로 수립 및 구축해야 하므로 Y/N으로 수립 및 구축여부 작성
운영 현황	ISMS 인증기준의 요구사항에 대해 어떻게 대응한 것인지 작성 누가, 언제, 무엇을, 어떻게 적용하고 있는지 상세하게 작성
관련 문서	ISMS 인증기준을 만족하는 내용이 포함되어 있는 기관의 정보보호 정책·지침의 세부 조항 작성
증적 자료	ISMS 인증기준을 만족하는 내용이 포함되어 있는 기관의 증적자료) 작성

정보보호관리체계(ISMS) 운영 현황표 작성 (예시)

① 정기적으로 수행해야하는 정보보호 활동들을 취합/정리하여 누락없이 수행할 수 있도록 합니다.
② 각 정보보호 활동 사항에 대해 언제/누가 수행하는지 명확한 이행계획을 명시하도록 합니다.
③ 정보보호 활동의 수행 근거를 매핑하여 법적 준수사항을 체크하고 이행 증적을 남기도록 합니다.

Sample

No	정보보호 활동	이행 주기	이행계획			검토자 (확인/승인)	근거문서	이행증적	
			시기	주체					
1	• 연간 정보보호 계획 수립	연1회	00월	보안팀	홍길동	임꺽정	정보보안 규정	연간 정보보호 계획서	3.1
2	• 보안서약서 징구 및 관리	필요 시	-	보안팀	홍길동	임꺽정	인적보안 지침	보안서약서	6.1.3
… 중략 …									
10	• 침해사고 대응 훈련	연1회	00월	보안팀	홍길동	임꺽정	침해사고 보안지침	• 침해사고 대응 훈련 계획서 • 침해사고 대응 훈련 결과 보고서	12.2.1

06 조치방안 가이드

Key point 발견된 결함사항을 보완하고 정보보호 관리체계를 지속적으로 운영할 수 있도록 후속조치를 지원하겠습니다.

결함사항 조치방안 가이드 제공

Sample

ISMS_특별점검(정보보호 관리체계 점검결과 조치방안 가이드

통제사항	통제내용		세부점검항목
보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.	179	조직에서 운영하고 있는 보안시스템에 대한 운영절차를 수립·이행하고 있는가?
		180	보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가?
		181	보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가?
		182	보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가?
		183	보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가?
		184	개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 관련 법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?

모범사례 제시

Sample

모범 사례 9 – 트러스티드 어드바이저 활용

AWS는 AWS 트러스티드 어드바이저(AWS Trusted Advisor)라는 무료 서비스를 ...
대한 '비용 최적화', '성능', '보안', '내결함성', '서비스 한도'에 대한 모범 사례 점검 기...
있다. 개인정보보호 및 중요 데이터 보호를 위해서는 트러스티드 어드바이저에...
안' 점검 항목을 주기적으로 모니터링하거나 트러스티드 어드바이저의 '보안' 점...
치 권고 알람이 발생하는 경우 이메일 등을 통해 알람 정보를 수신하도록 구성할 ...

트러스티드 어드바이저 서비스는 고객의 AWS 기술지원 등급에 접근할 수 있는 검...
가 있다. AWS 베이직 서포트 및 AWS 개발자 서포트 고객은 핵심 보안 검사 및 ...
대한 모든 검사에 액세스할 수 있다. AWS 비즈니스 서포트 및 AWS 엔터프라이즈...
비용 최적화, 보안, 내결함성, 성능, 서비스 할당량을 포함한 모든 트러스티드 어드...
액세스할 수 있다.

결함 조치 지원

- 발견된 결함사항 보완조치 및 ISMS 인증 취득에 필요한 사전준비 지원

관리방안 제시

- 가상자산서비스에 적합한 정보보안 모범사례 등 지속적 관리방안 제시
- 이용자 피해 예방을 위한 보안강화 방안 제시

07

점검 전후 수준 측정

Key point 특별점검 전·후 수준을 비교하여 기술지원에 대한 효과를 분석하고 가상자산사업자 보안성 강화를 위한 발전방향을 제시하겠습니다.

기술지원 전·후 수준 측정

D. 기술적 보호 방안 (32점)

Sample

구분	진단 내용	전	
22	**중요자산의 보호를 위한 보안시스템을 운영하고 있습니까?** ① 회사 내부에 보안 시스템을 구축하여 운영 중이고, 필요에 따라 외부업체에 맡김 (4점) ② 외부 업체를 통해 보안 시스템을 운영 중 (2점) ③ 보안 시스템 없음 (0점)	4	4
22-1	**보안시스템을 운영하고 있다면, 어떠한 시스템을 활용하고 있습니까? (복수응답 가능)** ① CCTV 등 감시 카메라 장치 ② 출입통제시스템(비밀번호, 출입카드, 지문/정맥인식 등) ③ 비밀관리 프로그램 ④ 기타(웹방화벽) * 3개 이상 4점, 2개 2점, 1개 1점, 해당없음 0점	2	2
23	**아래와 같은 보안활동을 하고 있습니까? 각 활동별 실시 정도를 선택하여 주십시오.** 보안활동 실시 정도 / 매일 / 주 1회 이상 / 월 1회 이상 / 연 1회 이상 / 실시하지 않음 1) 출입문, 캐비닛, 개인서랍 시건 여부 확인 ① ② ③ ④ ⑤ 2) 문서 및 도면 방치여부 확인 ① ② ③ ④ ⑤ 3) 노트북 방치 여부 확인 ① ② ③ ④ ⑤ 4) PC전원 OFF 여부 확인 ① ② ③ ④ ⑤ 5) 화면보호기설정 및 패스워드사용 여부확인 ① ② ③ ④ ⑤ * 매일 또는 주 1회 이상 항목 4개 4점, 매일 또는 주 1회 이상 항목 3개 3점, 매일 또는 주 1회 이상 항목 2개 2점, 매일 또는 주 1회 이상 항목 1개 1점, 해당사항 없음 0점	0	0
24	**정기적인 보안감사*를 실시하고 있습니까?** ① 정기적으로 실시 (4점) ② 필요시에만(비정기적) 실시 (2점) ③ 실시안함 (0점) * 보안감사 : 보안시스템이 안전하게 운영되고 있는지를 조사하고 분석하는 행위 감사 대상은 기업의 보안 정책 수립부터 운영에 관련된 모든 사항을 포함함	0	4
25	**정보시스템 사용 내용에 대한 로그(Log)*를 관리하고 계십니까?** ① 회사 자체적으로 정보시스템 사용 로그를 주기적으로 관리함 (4점) ② 회사 자체적으로 정보시스템 사용 로그를 필요할 때마다 비정기적으로 관리함 (2점) ③ 정보시스템 사용 로그를 별도로 저장 및 관리하지 않음 (0점) *로그 : 시스템 접근 시 이용자가 행한 모든 행위를 기록한 파일로써 외부에서 침입을 해온 공격자 및 사용자가 시스템에서 어떤 일을 했는지, 어떠한 명령어를 사용했는지, 시스템에 보안상에 저촉이 되는 행동을 하지 않았는지 등에 대한 정보를 담고 있음	2	4

기술지원 효과 분석

- 특별점검 전·후 정보보호 관리체계 운영수준을 측정
- 보안 취약점 개선 및 결함사항 보완조치 이행 등 기술지원에 따른 효과 분석

발전 방향 제시

- 특별점검 시 발견된 주요 보안이슈 및 현장의 의견수렴 등을 통해 가상자산 사업자의 보안성 수준을 높이기 위한 제도적 발전방향 제시

THANK YOU

가상자산사업자 정보보호관리체계 특별점검