가상자산 사업자 ISMS의 실무적 쟁점

발표 : ㈜이지시큐 박관서 수석 컨설턴트

AEGISECU
Easy ISMS Companion

CONTETNS

AEGISECU
Easy ISMS Companion

1. 가상자산사업자 ISMS 인증 개요

가상자산사업자의 ISMS 인증 필요성

1. “특금법” 개정 사항에서 가상자산사업자에 대한 신고를 의무화 (21년 9월 24일까지)
2. 가상자산사업자 신고를 위한 요건 중 “정보보호 관리체계 인증” 획득을 포함

특정 금융거래정보의 보고 및 이용 등에 관한 법률 (약칭 : 특정금융정보법)

시행 2021년 3월 25일

제7조(신고) . ① 가상자산사업자(이를 운영하려는 자를 포함한다. 이하 이 조에서 같다)는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 금융정보분석원장에게 신고하여야 한다

1. 상호 및 대표자의 성명
2. 사업장의 소재지, 연락처 등 대통령령으로 정하는 사항

② 제1항에 따라 신고한 자는 신고한 사항이 변경된 경우에는 대통령령으로 정하는 바에 따라 금융정보분석원장에게 변경신고를 하여야 한다.

③ 금융정보분석원장은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자에 대해서는 대통령령으로 정하는 바에 따라 가상자산사업자의 신고를 수리하지 아니할 수 있다.

1. 정보보호 관리체계 인증을 획득하지 못한 자
2. 실명확인이 가능한 입출금 계정[동일 금융회사등(대통령령으로 정하는 금융회사등에 한정한다)에 개설된 가상자산사업자의 계좌와 그 가상자산사업자의 고객의 계좌 사이에서만 금융거래등을 허용하는 계정을 말한다]을 통하여 금융거래등을 하지 아니하는 자. 다만, 가상자산거래의 특성을 고려하여 금융정보분석원장이 정하는 자에 대해서는 예외로 한다.

-이하 생략-

인증 종류

	ISMS(정보보호 관리체계 인증)	ISMS-P(정보보호 및 개인정보보호 관리체계 인증)
	기업·기관의 정보보호 체계에 대한 인증	기업·기관의 정보보호 체계와 개인정보 보호 영역을 모두 인증
인증 대상	ISMS 의무대상 기업·기관, 개인정보를 보유하지 않거나 개인정보 흐름의 보호가 불필요한 조직	보호하고자 하는 정보 서비스가 개인정보의 흐름을 가지고 있어 개인정보 처리 단계별 보안 강화가 필요한 조직
인증 기준	1.관리체계 수립 및 운영(16) 2.보호대책 요구사항(64)	1.관리체계 수립 및 운영(16) 2.보호대책 요구사항(64) 3.개인정보 처리단계별 요구사항(22)

인증 범위

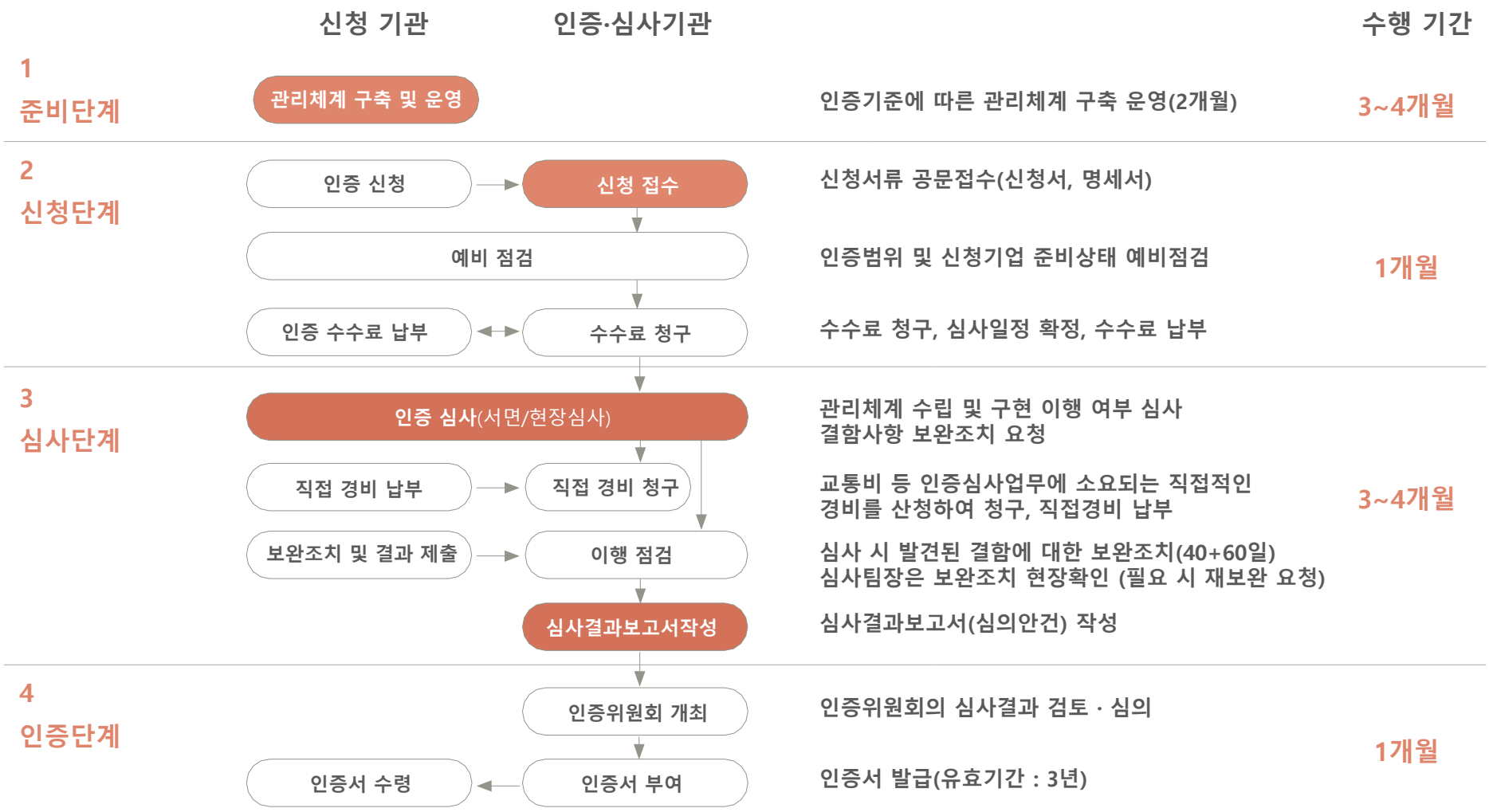
서비스 운영을 위한 조직 및 인력	서비스 운영을 위한 장소	서비스 운영을 위한 인프라	개인정보 처리를 위한 조직 및 인력	개인정보 처리를 위한 물리적 인프라
▪ 시스템 운영팀, 정보보안팀, 인사팀 등 ▪ 관제, 재해복구	▪ 시스템 운영장소 ▪ 정보서비스 운영 관련부서	▪ 서버, DBMS 네트워크, 정보보호시스템, 클라우드 콘솔 등	▪ 고객센터, 영업점, 물류센터 ▪ 개인정보보호팀 등	▪ 개인정보 취급 부서 ▪ 개인정보 취급 수탁사

정보통신서비스와 서비스 제공을 위한 모든 정보시스템, 인력, 물리적 위치 등은 반드시 포함하여야 함

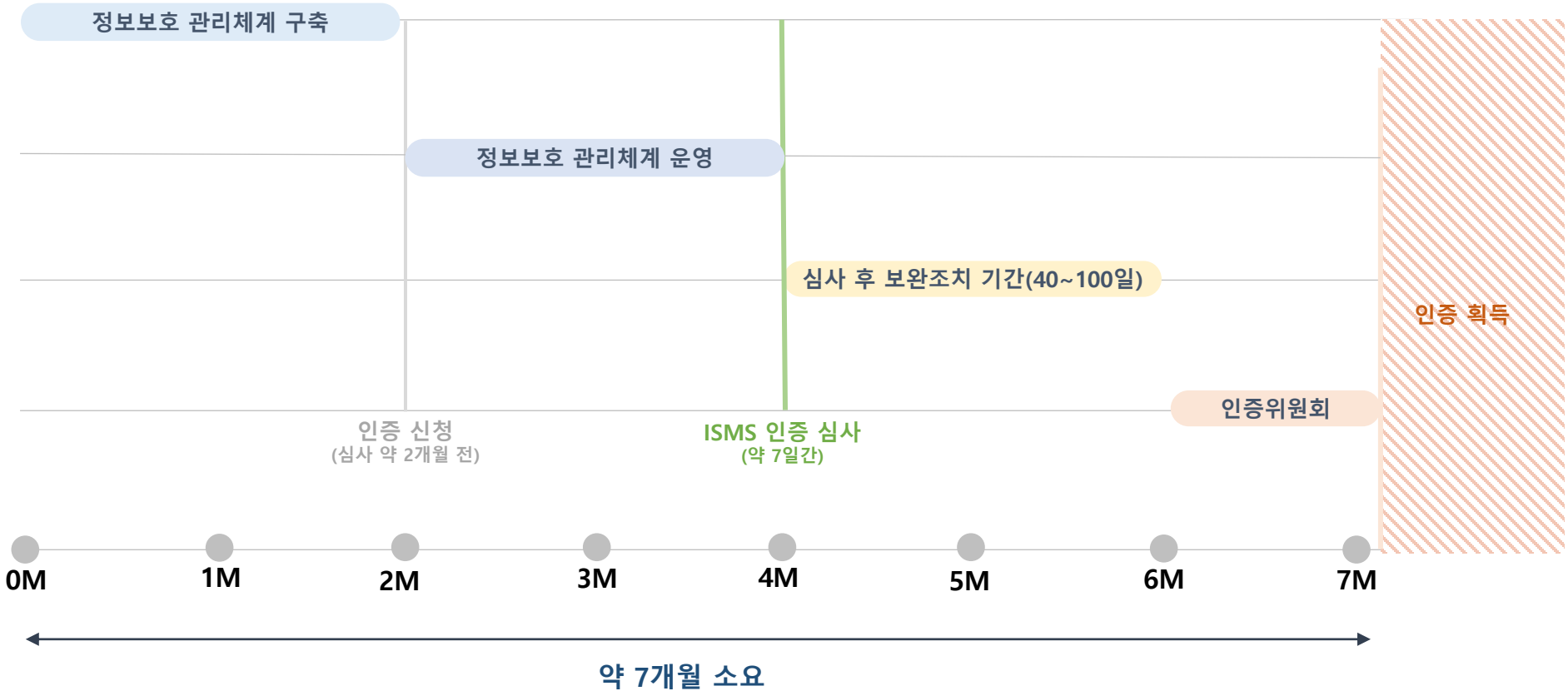
정보시스템 서비스와 개인정보 관련 업무를 상세하게 분석하여 Life Cycle(수집·보유·이용·제공·폐기)에 따라 개인정보 흐름에 해당하는 모든 서비스, 정보시스템, 인력, 물리적 위치 등을 포함하여야 함

2. ISMS 심사 절차

심사 절차



ISMS 인증 소요 기간



위는 가상자산사업자의 일반적인 소요 기간이며, 가상자산사업자의 현황과 인증 전략에 따라 상이할 수 있습니다.

인증 유지

구분	내용	심사 절차
최초심사	정보보호 관리체계 인증 취득을 위한 심사 (범위 변경 등 중요한 변경사항 발생시에도 최초심사)	준비단계 ~ 4 인증단계 진행 (인증 유효기간 : 3년)
사후심사	정보보호 관리체계를 지속적으로 유지하고 있는지에 대한 심사 (연 1회 이상)	2 신청단계 ~ 3 심사단계 진행 (인증 유효일로 부터 매1년)
갱신심사	유효기간(3년) 만료일 이전에 유효기간 연장을 목적으로 하는 심사	2 신청단계 ~ 4 인증단계 진행 (유효기간 만료일 이전에 신청)

3. 가상자산사업자 ISMS 주요 쟁점

가상자산사업자 ISMS 세부점검항목

구분	ISMS 항목	가상자산 사업자 추가 항목	전체 항목
관리 분야	80	**11**	91
물리 분야	16	**5**	21
기술 분야	138	**24**	162
금융 분야		**16**	16
합계	234	**56**	290

가상자산사업자 ISMS 인증심사 시

- 가상자산사업자 관련 항목 56개가 추가된 290개 항목으로 심사

가상자산사업자 ISMS 주요 쟁점

관리 분야

위험관리

가상자산 거래 서비스에서 발생할 수 있는 위험을 빠짐없이 식별・평가하고 있는가?
- 예. CEO 사망, 내부유출, 부정거래, 자연재해, 키 분실, 월렛서버 탈취 등

가상자산 거래 및 운영에서 발생 가능한 위험을 식별 및 평가하고, 각 위험에 대한 보호대책을 마련

- 핫월렛/콜드월렛 개인키 백업을 통한 대책 마련
- 핫월렛/콜드월렛 자산 및 전송절차 모니터링
- 월렛서버 탈취에 대비한 멀티시그 구현 등

가상자산사업자 ISMS 주요 쟁점

관리 분야

멀티시그

가상자산별 블록체인에서 멀티시그를 제공하지 않는 경우, MFA(Multi Factor Authentication), 키분할, 자체 구축한 멀티시그 방식 등 이를 대체하기 위한 안전장치가 보호대책에 포함되어 있는가?

멀티시그가 적용 가능한 월렛에 멀티시그를 적용하고, 적용이 불가능한 코인의 경우 그에 상응하는 대책 마련

- 블록체인의 스마트 계약 등을 통해 멀티시그 구현
- 개인키를 분리 및 암호화 보관
- 자체적으로 멀티시그 방식 구현 (블록체인이 아닌 어플리케이션에서 멀티시그 구현)

가상자산사업자 ISMS 주요 쟁점

물리 분야

월렛룸

콜드-핫 월렛 관련 보관, 금고, 월렛 사용을 위한 공간 등 중요 통제구역을 일반 업무/보호구역과 별도로 분리하고, 통제구역으로 지정 및 관리하고 있는가?

콜드월렛 전송 또는 보관을 위한 장소를 별도로 분리 및 중요 통제구역으로 지정하고 적절한 보호대책을 마련

- 최소한의 출입자 지정 및 출입통제
- CCTV 및 월렛룸 출입통제장치 등 마련
- 외부침입을 고려하여 유리창문, 얇은벽 등을 금지
- 콜드월렛 보관 시 안전한 금고 내 보관 및 반출입 절차 마련
- 출입관리시스템, CCTV 및 출입관리대장 등을 통해 매월 출입의 적절성 등 점검

가상자산사업자 ISMS 주요 쟁점

기술 분야

노드서버

가상자산 노드서버존(블록체인 참여 및 거래를 발생시킬 수 있는 서버 등)은 내부 및 다른 서버존의 장비들과 불필요한 통신/터미널 접속이 발생하지 않도록 접근을 제어하고 있는가?

핫월렛 보관을 위한 별도 네트워크망 구성 및 네트워크간 불필요한 통신 차단

- 외부와 블록체인 통신을 위한 노드서버와 핫월렛 보관 서버를 분리
- 각 네트워크망에서 불필요한 접근을 차단하도록 방화벽 등으로 제한

가상자산사업자 ISMS 주요 쟁점

기술 분야

망분리

월렛 접근 인원/시스템에 대한 별도 네트워크 존을 구성하고 접근통제 정책을 적용하고 있는가?

월렛 관련 시스템에 대한 네트워크 분리 및 운영 PC에 대한 네트워크 망을 분리

- 핫월렛 서버 네트워크망 분리
- 핫월렛 운영(ADMIN 시스템 접근, 서버 접근 등) PC에 대한 망분리 (물리적 망분리)
- 콜드월렛 전송 PC 망분리

가상자산사업자 ISMS 주요 쟁점

금융 분야

이상행위 분석 및 모니터링

월렛 접근과 관련하여 실시간 알람 등을 통해 사고 방지 체계를 구축하고 있는가? 월렛에 대한 비인가 접근, 권한 오남용, 개인키 접근 및 유출, 비인가자에 의한 가상자산 이체 등 비정상 행위를 탐지, 대응할 수 있도록 관련 로그 검토 및 모니터링 기준과 절차를 수립・이행하고 있는가?

월렛 접근에 대한 실시간 알람 시스템 구축 및 이상행위에 대한 분석과 모니터링 절차 마련

- 핫월렛 접근 시 실시간 알림의 경우 권고하고 있음(필수 X)
- 핫월렛 서버, 가상자산을 전송 가능한 ADMIN 페이지 등에서의 행위를 모두 기록하고 모니터링
- 콜드/핫 월렛의 자산 보유 현황을 모니터링하여, 이상징후 탐지

감사합니다.

AEGISECU
Easy ISMS Companion

(주)이지시큐
06024 경기도 성남시 대왕판교로 815 4층(KISA정보보호 클러스터) | T.1855-1535 | E. isms@aegisecu.com
http://www.aegisecu.com/