‘블록체인 기반 비즈니스’를 위해 필요한 보안 전략은?

SK인포섹/하이테크사업본부 문병기 팀장

2018.03.22

Contents

I. 블록체인 Platform

II. 블록체인 비즈니스 보안 고려사항

III. 암호화폐 거래소 보안 대응전략

Contents

I. 블록체인 Platform

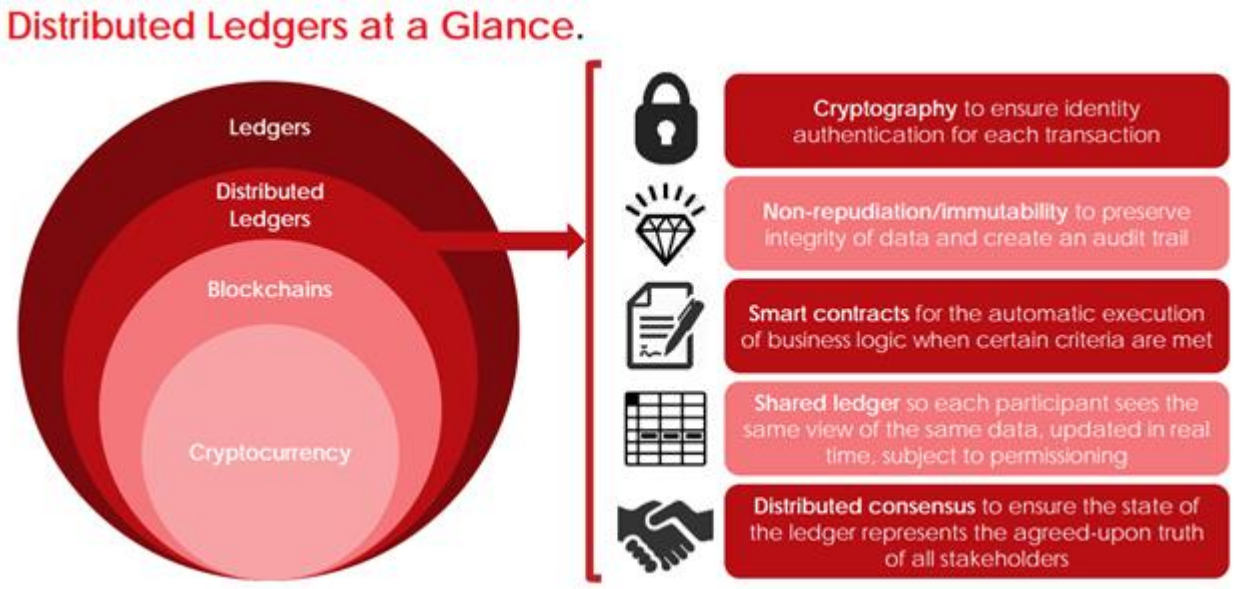
1. 블록체인 Platform 개요
2. 블록체인 Platform 종류
3. 블록체인 Platform 선택가이드

II. 블록체인 비즈니스 보안 고려사항

III. 암호화폐 거래소 보안 대응전략

1. 블록체인 Platform이란?

❑ 블록체인은 분산원장임



1	**암호화** 각 트랜잭션 신원확인
2	**부인방지/불변성** 데이터 무결성, 감사추적
3	**스마트계약** 조건 충족시 Biz Logic 자동실행
4	**공유원장** 동일데이터/시간, 실시간,권한
5	**분산된 합의** 모든 이해관계 합의 원장 증명

❑ 블록체인 Platform(분산원장 Platform)의 발전

Public → (확장) → **Private**

- Biz 요구사항 수용
- Biz Script 확장
- Consensus Protocol
- Permission
  : 개인인증/권한

DBMS는 Oracle, MS-SQL, MySQL 등 존재, 기업 Biz 고려하여 선정 및 구축
블록체인플랫폼도 다양하게 존재, 기업 Biz 고려하여 Platform 선정 및 구축

- 비트코인에서 출발 기업고객 대상 Private 개념 도입
- 경쟁 알고리즘 대신 협의 알고리즘(Consensus Protocol) 확장
- 기업관점 적용을 위한 Permission 개념도 현실화
- 기업요구사항 수용 위해 한계가 명확한 Bitcoin Script 확장하여 Smart Contract 개념 도입, Hyperledger는 Chaincode로 명명
- 비지니스적 요구와 그에 부응하기 위해 다른 기술적 해결과정을 개념화하여 다양한 블록체인 Platform 탄생

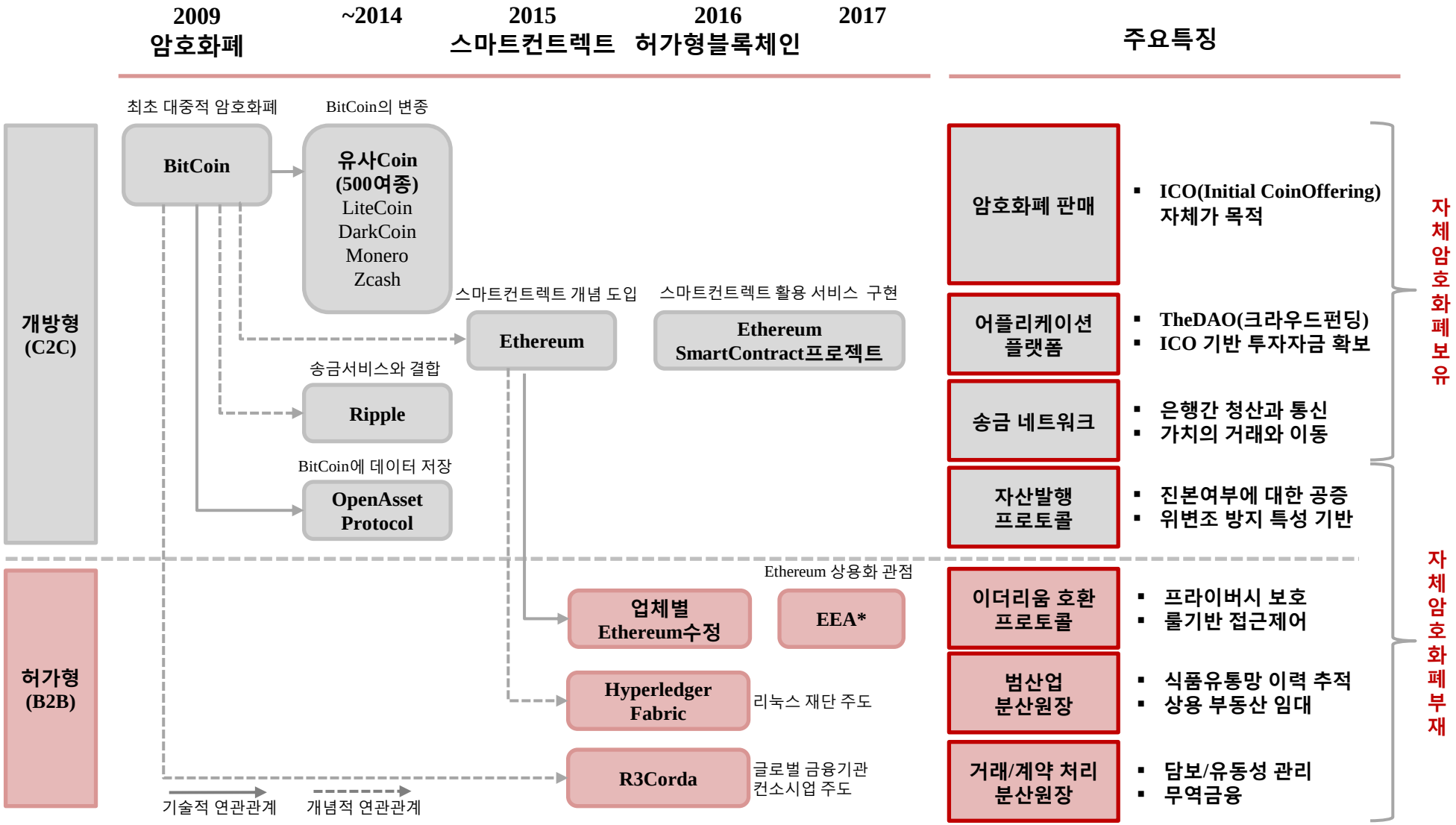
1. 블록체인 Platform 종류

❑ 블록체인 Platform 분류(현재도 계속 확산중)

	종류	Player Type 및 설명
Public BlockChain	Bitcoin, Ethereum, Ripple, Litecoin, Dash Peercoin, Nxt, Zcash, Monero, Lisk, Stellar	암호화폐, Steller(payment network), Lisk(public blockchain platform), Ethereum(Smart Contract)
Sidechain	RSK(a.k.a Rootstock), Blockstream, Counterparty	Bitcoin 단점을 극복(확장불가, 개선불가)하여 거래를 진행가능토록 수행, Bitcoin 변경없이 약점극복
Interchain	ARK, Aion, Icon, Wanchain	서로 다른 블록체인을 연결목적의 블록체인 비트코인으로 이더리움 dapp 참여가능기술
Extentions	HydraChain	이더리움과 호환기반 Private Blockchain 구축기술
Distributed ledger /Privarte blockchain	Corda, Juno, Bilon	분산원장 기술 , Private Blockchain Platform기술로 기업의 목적에 맞는 Biz 구축가능
Consortia /collaborative efforts	Hyperledger(구성:Blockchain Explorer, Fabric, Iroha, sawtooth Lake, etc)	금융, 헬스케어, 물류 공급망(SPC)등에서 블록체인 쉽게 사용하고자 하는 진보된 Platform
Development service	Eris-db, Multichain, Morphesus Labs	블록체인 응용 프로그램, 개발 간소화, 협업환경, 작업공간, 버전제어기술(Morphesus)
Consensus Protocol	Tendermint, Interledger	합의 알고리즘 기반으로 병렬 블록체인의 연결 시키는 블록체인 Network
Other	Enigma, BigChainDB	블록체인기능을 추가한DB(BigChainDB), 암호화폐 자동트레이딩플랫폼(Enigma)

2. 개방형/허가형 블록체인 비교

❑ C2C(개방형), B2B(허가형)



*EEA : Enterprise Ethereum Alliance : Ethereum 기반 솔루션간 호환성 추구

1. Blockchain 구축 가능 주요 Platform 비교

❑ 4가지 Blockchain 플랫폼 비교

	비트코인(Bitcoin)	이더리움(Ethereum)	IBM 패브릭 (Fabric)	R3 코다(Corda)
내제 화폐	O	O	X	X
네트워크 허가	공개형	공개형	제한형	제한형
데이터 전달 모델	모든 데이터를 모든 참여자에게 전파	모든 데이터를 모든 참여자에게 전파	암호화된 데이터를 채널 내의 참여자에게 전파	P2P(Point-to-Point)로 거래에 관련있는 참여자에게 전달
적용 분야	자금이체	범용	범용	금융
스마트계약	튜링 불완전성 (Script 기반)	튜링 완전성	튜링 완전성	튜링 완전성
개발	네트워크 표준(C++, Python 등)	EVM : ethereum virtual machine, Solidity언어로 개발	언어에 따라 다름 (Go, Java)	Deterministic JVM(Java Virtual Machine)
법적 유효성	Code is Law 개념	Code is Law 개념	법률문서가 레퍼런스 또는 첨부될 수 있음	리카르디안 계약 / 법률 문서가 래퍼런스 또는 첨부 될 수 있음
거래 검증	작업증명 (Pow)	작업증명(PoW) 이후 지분증명(Pos)으로 전환계획	장착형 합의 알고리즘	거래상대방간 유효성 합의 유효성은 노터리(Notary)로 합의
상태	Unspent Transaction Output	Account 기반 (주소와 잔고를 추적)	Key-value pair	UTXO (unspent transaction output)
트렌잭션 처리	네트워크 합의에 의해 제한	네트워크 합의에 의해 제한	수직/수평적으로 확장 가능	수직/수평적으로 확장 가능

2. 블록체인 Platform 선택 가이드

❑ 블록체인 Platform 체크항목 비교

체크항목	Bitcoin	Ethereum	Hyperledger Fabric
분류	퍼블릭 블록체인	퍼블릭 블록체인	프라이빗 블록체인
데이터전달모델	모든 데이터를 모든 참여자에게 전파	모든 데이터를 모든 참여자에게 전파	암호화된 데이터를 채널 내의 참여자에게 전파
합의 알고리즘 (거래 검증)	PoW	PoW (이후 지분증명 PoS 전환 예정)	1)PBFT
결제 완료성	없음	없음	있음
성능	약 10분마다 블록 생성	약 15초마다 블록 생성	갱신 시 합의를 확정, 우수한 성능 보장
트랜잭션 은닉화	트랜잭션 정보 공개	트랜잭션 정보 공개	트랜잭션 정보 공개/암호화 선택 가능
스마트 컨트랙트	거의 없음. 제한적인 용도로 사용 가능	이더리움 버츄얼 머신(EVM : ethereum virtual machine)에 동작하는 스마트 컨트랙트 구현 가능	2)체인 코드(Chaincode)를 통해 스마트 컨트랙트 구현 가능
개발	네트워크 표준(C++, Python 등)	EVM : ethereum virtual machine, 3)Solidity언어로 개발	언어에 따라 다름 (Go, JAVA)
최소 구성 대수	1대부터 가능 장애복구를 위해 최소 2대 필요	1대부터 가능 장애복구를 위해 최소 2대 필요	장애복구를 위해 최소 4대 필요
트렌잭션 처리	네트워크 합의에 의해 제한	네트워크 합의에 의해 제한	수직/수평적으로 확장가능
적용 분야	자금이체	범용	범용

Contents

I. 블록체인 Platform

II. 블록체인 비즈니스 보안 고려사항

1. 블록체인 비지니스 주요 보안위협 및 대응방안

2. 암호화폐 비즈니스 주요 보안위협 및 대응방안

III. 암호화폐 거래소 보안 대응전략

1. 블록체인 도입시 보안 위협항목

❑ ENISA(EU산하 정보보호기구) Report – 블록체인 도입시 고려할 보안

분류	No	보안위협	설명
키관리	1	✓ 키 도난 및 분실	✓ 공격자에게 키를 도난당하거나 분실된 키가 악용될 경우 자산 및 기밀 거래 메시지 유출
	2	✓ 취약한 키 생성	✓ 취약한 키 생성 알고리즘으로 인해 키 재생성 공격이 가능할 경우 자산 및 기밀거래 메시지가 유출 가능
거래 검증 및 합의	3	✓ 합의 가로채기	✓ 참여자 중 과반수(또는 운영주체)를 장악하여 블록체인의 합의 과정을 조작
	4	✓ 사이드 체인 내 비정상 거래 발생	✓ 메인 체인에서 유효하지 않은 자산이 사이드 체인에서 거래 가능
참여자 권한관리	5	✓ 개인정보 침해	✓ 거래정보에 대한 참여자의 접근권한 관리 부족시 개인정보 침해 가능
	6	✓ 권한 오남용	✓ 참여자의 내.외부 권한관리 부족시 금융회사 및 내부직원에 의한 보안사고 발생 가능
블록체인 S/W 보안	7	✓ 블록체인 S/W 취약점	✓ 블록체인 S/W에 보안 취약점이 존재할 경우 키 도난, 합의 조작, DDoS 공격 등에 악용가능
	8	✓ 스마트 컨트랙트 취약점	✓ 스마트 컨트랙트에 취약점이 존재할 경우 자산유출, 개인정보 침해, DDoS 공격 등에 악용가능
서비스 보안	9	✓ 분산 서비스 거부 공격	✓ 다수 참여자가 악성코드 등을 통해 공격자에게 장악될 경우 대량의 스팸거래를 발생 가능하며 이로 인해 블록체인 서비스가 중단 가능
	10	✓ 가용성 저하	✓ 블록체인의 처리속도 한계, 거래정보 급증으로 인해 추가 서비스 개발 및 확대 제한 등의 가용성이 저하
	11	✓ 비정상거래 탐지 불가	✓ 비정상거래에 대한 사전 탐지 및 차단 기술이 부족하여 사기거래, 자금세탁, 이중지불등의 거래가 발생 가능
	12	✓ 상호 운영성 미제공	✓ 블록체인간 자산교환, 기능 확장 등 연계 필요시 책임주체 및 표준규격이 명확하지 않아 예상치 못한 보안취약이 발생 가능

2. 블륵체인 보안위협 대응 방안(1)

❑ 보안위협 대응방안

분류	No	보안위협	설명	대응방안(SK인포섹)
키관리	1	✓ 키 도난 및 분실	✓ 관련가이드 준수 ✓ 키 분실 및 도난 대응 ✓ 키 복구 ✓ 다중서명 ✓ 용도별 키 할당 ✓ 암호화 및 사용 후 즉시 삭제	✓ 블록체인 키 대응정책 수립 ✓ KMS 기반 키관리체계 수립 ✓ 키관련 최신 보안가이드 적용 ✓ 인포섹 최신 탐지정책 적용기반 확보
	2	✓ 취약한 키 생성	✓ 안전한 키 생성 ✓ 안정성 검증	
거래 검증 및 합의	3	✓ 합의 가로채기	✓ 비정상 참여자 모니터링 ✓ 수수료 부과 및 거래 처리량 제한 ✓ 참여자 검증	✓ 프라이빗 블록체인 경우 참여자 보안 수준 유지 정책 수립 ✓ 지속적 모니터링 및 이상행위탐지체계 수립
	4	✓ 사이드 체인 내 비정상 거래 발생	✓ 합의통합	✓ 주 체인 거래검증, 블록생성 합의 과정 통합하도록 구축 ✓ 메인 체인 자산을 주로 해서 유효하지 않을시 거래 차단
참여자 권한 관리	5	✓ 개인정보 침해	✓ 채널 구성 ✓ 거래정보 삭제	✓ 거래와 무관한 제 3자 접근 차단 ✓ 거래정보 보관기간 규정 수립 경과후 무결성 확인 정보이외 세부 정보 삭제 정책 실시 ✓ 참여자 Permission 상세설계 ✓ 거래 암호화
	6	✓ 권한 오남용	✓ 스마트 컨드랙트 기반 통제	✓ 참여자 거래 및 서비스 참여 규칙 스마트 컨트랙트로 통제 ✓ 거래와 관련 내부 직원 서명 식별 ✓ FIDO기반으로 인증강화 ✓ 통합계정/권한관리체계를 스마트 컨트랙트와 연결

2. 블륵체인 보안위협 대응 방안(2)

❑ 보안위협 대응방안

분류	No	보안위협	설명	대응방안(SK인포섹)
블록체인 S/W 보안	7	✓ 블록체인 S/W 취약점	✓ 코드검토 ✓ 보안테스트 ✓ 안전한 개발 방법론	✓ 블록체인 S/W 형상관리 강화 ✓ 블록체인 S/W 상시 취약점 점검체계 ✓ 블록체인 S/W 소스코드 취약점 체계 ✓ 블록체인 S/W 시큐어 코딩 가이드 수립 ✓ 블록체인 S/W 상시 모의해킹 실시(정적, 동적, 침투 테스팅 등)
	8	✓ 스마트 컨트랙트 취약점	✓ 코드 검토 및 악성코드 탐지 ✓ 검증된 코드 사용	✓ 스마트 컨트렉트 전용 취약점 점검 체계 수립(정책, 모의해킹 포함)
서비스 보안	9	✓ 분산 서비스 거부 공격	✓ 스팸거래 차단 ✓ 거래요청 건수 제한 ✓ 거래허용 참여자 관리	✓ White list 관리 ✓ Spam 및 DDoS 대응체계 수립
	10	✓ 가용성 저하	✓ 유효성 검증 참여자 제한 ✓ 선택적인 거래정보 저장	✓ 유효성 검증 참여 노드수 최적화
	11	✓ 비정상거래 탐지 불가	✓ 거래허용 참여자 관리	✓ 모니터링을 통하여 비정상 거래 추적
	12	✓ 상호 운영성 미제공	✓ Pegged 사이드 체인 ✓ 표준 프로토콜 개발	✓ 자산 교환 안정성 기술 적용

1. 암호화폐 거래소 주요 보안 사고

❑ 블록체인 Biz, 암호화폐 해킹사례

피해정보			Wallet		APT
일시	거래소	피해규모	Hot	Cold	E-Mail
2017.04	야피존	55억원 암호화폐 도난	Y	N	Y
2017.06	빗썸	3만6천여명 개인정보 유출			Y
2017.09	코인이즈	21억원규모 암호화폐 도난	Y	N	Y
2017.12	유빗	17% 코인손실, 파산	Y	N	Y
2018.01	코인체크	5,659억 “NEM” 도난(일본)	Y	N	Y
2918.02	비트그레일	1,700만개 나노 도난(이탈리아)	Y	N	Y

원인

❑ 암호화폐 비즈니스 고려사항

1. APT 공격 대응 미흡
2. 미흡한 Wallet 보호
3. 내부자 PC 통제 미흡

블록체인 시스템을 설계시,
취약점은 반드시 존재한다는 전제
하에 방어대책을 수립 후
시스템을 구축해야 한다.

❑ 이더리움 취약점 이용한 DAO 해킹사건(600억 가치)

TheDAO는 DAO 토큰 구매를 위해 지불했던 이더 환불기능 존재

(취약점) 코드로 작동하는 이 기능은 일정시간 지난 후
반환요청처리되는 취약점을 보유하고 있었음

(해킹) 이 취약점을 인지한 해커는 환불 요청후 이더 환불받고 자신의 계정에서 DAO 토큰 차감되기 전 다시 환불 요청하는 방식으로 무한 환불 공격진행

고려
사항

1. 취약점 모니터링 상시 지속
2. 최신 취약점 발견시 즉시 적용
3. S/W 취약점 상시 관리체계 수립

2. 암호화폐 거래소 주요 점검항목

❑KISA 주요 점검 사항(암호화폐 거래소 운영시 참고)

Sample Case
(회사별 다른 관점 적용 필요)

❑ 암호화폐 비즈니스 고려사항

1. 정보보호 컨설팅/Audit
2. 망분리(논리적/물리적)
3. 주요단말 접속통제
4. 반출입 통제체계 (End-Point 보안)
5. 통합로그관리 시스템
6. 개인정보 통합모니터링
7. 내부정보 유출탐지/대응
8. 통합관제/모의훈련
9. Wallet 통제절차 수립
10. Wallet 모니터링/Audit (Hot/Cold Wallet)
11. 암호화 키관리(KMS)
12. 백업 및 복구체계

3. 블록체인협회 자율규제

❑ 블록체인협회 자율규제안(7가지규제안)

1 강력한 투자자 예치자산 보호장치 마련	예치금 100% 금융기관 예치	
	암호화폐 예치시, 콜드월렛 70%이상 의무화	
2 신규 코인 상장 프로세스 강화 및 투명성 제고	신규 코인 투명성 판단 평가정보 제공, 거래소는 평가프로세스 반영	
3 본인계좌 확인 강화 및 1인 1계좌 입.출금관리	대사 확인된 1인 1계좌로만 입.출금 제한 (대사확인 절차 시스템 , 강화된 가상계좌)	
4 오프라인 민원센터 운영 의무화	수시 민원접수 가능한 시스템 구축	
5 거래소 회원 요건강화	20억원 이상 자기자본 보유	
	금융업자에 준하는 정보보안시스템, 내부 프로세스 및 정보보호 인력 및 조직 운영	
6 불공정 거래의 규제를 통한 임직원 윤리 강화	미공개 중요정보(내부정보) 이용행위 금지, 위반시 개인까지 제재 권고	
7 독립적인 자율규제위원회 구성	자율규제 총 7인 가운데 전체 거래소 대표자 1인 포함 학계, 회계, 블록체인 전문가로 구성	

❑ 암호화폐 비즈니스 고려사항

1. Cold Storage Biz(Cold Wallet)
2. 증적관리(보안포털) 시스템 구축
3. 금융 수준 보안 컨설팅 (프로세스, 조직, 인력)
4. 금융 수준 보안 아키텍쳐 (시스템,NW)
5. 민원상담관리 시스템 (챗봇활용-프로세스 정립)
6. 내부통제/정보유출 시스템 (Big-Data기반 시스템)
7. Security Governance 체계 (Compliance 통합 Audit, ISMS)

◆ 콜드월렛 : 블록체인 네트워크와 연결이 끊긴 오프라인 상태의 지갑

◆ 대사확인 절차 시스템 : 암호화폐 거래소가 가진 이용자 정보(성명.은행계좌.거래소가 부여한 가상계좌번호 등)를 은행이 확인한 후 이용자 본인 확인이 되었을때 암호화폐 가상계좌와 연동된 하나의 은행계좌에서만 원화로 입출금이 되도록 하는 것

4. 블록체인 규제 예상

❑ 암호화폐 규제일지

❑ 한국블록체인협회 자율규제 첫 심사

한국 블록체인협회 총 33개 거래소(취급업소) 대상 자율규제, 21개 업체 참여

글로스퍼(준비중), 넥스코인(준비중), 두나무(업비트), 비티씨코리아닷컴(빗썸), 스트리미(고팍스), 에스코인, 오케이코인 코리아, 웨일엑스(준비중), 지닉스(준비중), 카이렉스(준비중), 케이씨엑스(준비중), 코미드, 코빗, 코인원, 코인웨이(준비중), 코인제스트(준비중), 코인플러그(CPDAX), 크립토컴퍼니(준비중) 플루토스디에스(준비중), 한국디지털거래소(준비중), 후오비코리아(준비중)

❑ 거래소 인가제로 선회 가능성 ↑

뉴욕모델 고려, 신고제 ▶ 인가제 전환예고(지방선거 이후)

(뉴욕모델 세부규제 15개나 되어 인가가 까다로움, 제도권에서 시장 감독 목적)

❑ 2018 ISMS 의무 암호화폐거래소 지정

빗썸, 코인원, 코빗, 업비트 4대 거래소 인증의무
(대상:매출액 100억이상, 일평균 방문자수 100만이상)

- 인증 의무 아닌 거래소도 자발적 유도
- 중소규모 거래소 (PIMS, ePRIAXY Mark)획득지원

- 민간기업과 공동으로 '사이버 보안 모의훈련' 실시
- KISA 상황실에서 거래소 모니터링 실시
- 법규위반 사업자 '서비스 임시 중지조치'제도 도입
- 피해자 구제목적 '집단소송제도','배상보험' 의무화

❑ 암호화폐 비즈니스 고려사항

제도권 편입 가능성↑

- 보안정책 강화
- 정책준수 감독
- 인증취득/갱신 지원
- 강화된 보안인프라
- 통합보안 관제체계
- 강화된 개인정보통제

1. 암호화폐 거래소 정보보호 컨설팅
2. 암호화폐 거래소 상시 보안 진단
3. 암호화폐 거래소 Total Outsourcing
4. 암호화폐 거래소 통합관제체계 수립

Contents

I. 블록체인 Platform

II. 블록체인 비즈니스 보안 고려사항

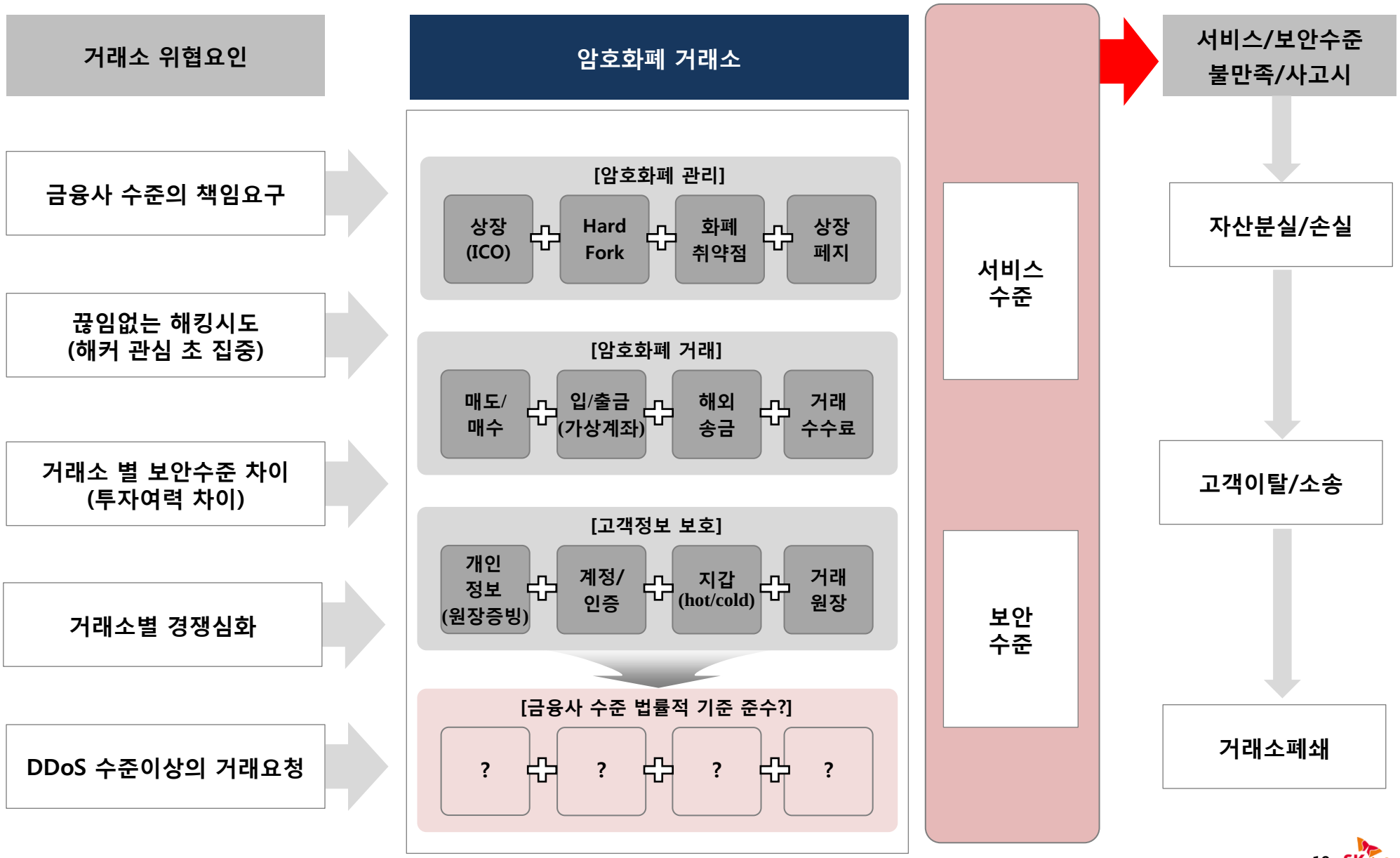
III. 암호화폐 거래소 보안 대응전략

1. 암호화폐 거래소 위험요인은?

2. 암호화폐 거래소 대응 전략은?

3. SK인포섹 보안 서비스 모델

1. 무엇이 위험한가?


거래소 위협요인
금융사 수준의 책임요구
끊임없는 해킹시도
(해커 관심 초 집중)
거래소 별 보안수준 차이
(투자여력 차이)
거래소별 경쟁심화
DDoS 수준이상의 거래요청
암호화폐 거래소
[암호화폐 관리]
상장 (ICO)
Hard Fork
화폐 취약점
상장 폐지
[암호화폐 거래]
매도/ 매수
입/출금 (가상계좌)
해외 송금
거래 수수료
[고객정보 보호]
개인 정보 (원장증빙)
계정/ 인증
지갑 (hot/cold)
거래 원장
[금융사 수준 법률적 기준 준수?]
?
?
?
?
서비스 수준
보안 수준
서비스/보안수준 불만족/사고시
자산분실/손실
고객이탈/소송
거래소폐쇄

2. 암호화폐 거래소의 지위는?

거래소의 지위는 무엇으로 해석할까?

기업(?) → **금융(?)**

1. 전체적인 보안 접근 방법

암호화폐 거래소 Biz 특성

1. 신규 투자 시장 (블록체인 기술기반)
2. 거래금액 2조 8천억 (코스닥 2조 4천억)
3. 법적지위 통신판매사업자 (정보통신망법, 개인정보보호법적용)
4. 은행 가상계좌 발급 (입금/출금 거래 목적)
5. 정부정책(1인1계좌)수립 (거래세,신고제 검토)
6. 수수료 비지니스 (막대한 이익, 과세예고 OO%)
7. 오픈 준비업체 투자여력↓ (수익 미창출, 보안투자 어려움)

암호화폐 거래소 Biz Risk

1. 정부정책, Compliance 강화 (제도권 통제 범위 - 정조준)
2. 유사수신, 자금세탁 통로 (감독기관 상시 통제 및 감시체계)
3. 해커들의 Main Target (암호화폐 14% 해커탈취, 1조이상피해)
4. 인가제 전환시 손실발생 (인가대상 미지정 가능성존재)
5. 보안체계 및 시스템 미흡 (현재 지속적으로 도입 중)
6. 취약점관리 및 대응 안됨 (블록체인, 지갑, 소스 등 취약점 대응 상시 체계 실시 필요)
6. 운영/관리 위한 조직체계 미흡 (역할자 미지정, CISO 등)

암호화폐 거래소 고려사항

- 암호화폐 거래소는 투자여력, 일정, 역량 등을 고려하여 맞춤형 아키텍쳐 수립 필요

SK infosec

사전 보안체계 정립 서비스

- 컨설팅 체계점검
- ISMS기준 점검
- 아키텍쳐점검

정책 변화 상시 대응 서비스

- 정책 변화에 대한 법률적, 정책적, 시스템적 변화 상시 자문 서비스

SK infosec

- 정보보호체계수립
- 보안인증취득
- 보안관제서비스
- 관제시스템구축
- 토탈아웃소싱(SI)
- 클라우드구축/모니터링

통합 OA 콜 센터 운영/보안시스템 운영

소스코드 취약점 점검

상시 인프라 취약점 점검

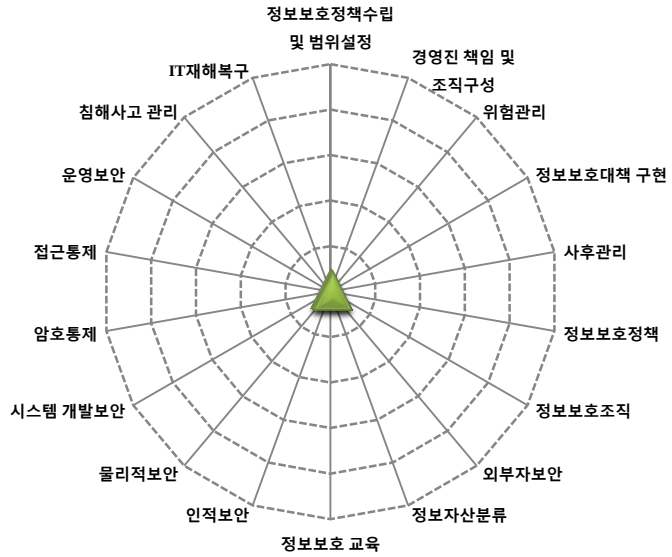
2. Compliance 접근 방법

통제분야			ISMS 세부통제항목 (253개)	F-ISMS 점검항목 (324개)
번호	통제내용			
[정보보호 관리과정]				
1	정보보호정책수립 및 범위설정		4	4
2	경영진 책임 및 조직구성		4	6
3	위험관리		11	11
4	정보보호대책 구현		3	3
5	사후관리		6	7
[정보보호 보호대책]				
1.1	정보보호정책	정책의 승인 및 공표	5	5
1.2		정책의 체계	3	3
1.3		정책의 유지관리	5	6
2.1	정보보호조직	조직 체계	5	7
2.2		역할 및 책임	2	3
3.1	외부자보안	보안요구사항 정의	1	1
3.2		외부자 보안 이행	3	13
4.1	정보자산분류	정보자산 식별 및 책임	4	4
4.2		정보자산의 분류 및 취급	3	3
5.1	정보보호교육	교육 프로그램 수립	5	5
5.2		교육 시행 및 평가	5	5
6.1	인적보안	정보보호 책임	8	8
6.2		인사규정	3	4
7.1	물리적보안	물리적 보호구역	14	17
7.2		시스템 보호	3	3
7.3		사무실 보안	4	7
8.1	시스템개발보안	분석 및 설계 보안관리	7	7
8.2		구현 및 이관 보안	12	18
8.3		외주개발 보안	3	3
9.1	암호통제	암호 정책	5	9
9.2		암호키 관리	3	3
10.1	접근통제	접근통제정책	1	1
10.2		접근권한 관리	9	10
10.3		사용자 인증 및 식별	9	11
10.4		접근통제 영역	27	30
11.1	운영보안	운영 절차 및 변경 관리	5	9
11.2		시스템 및 서비스 운영 보안	25	35
11.3		전자거래 및 정보전송 보안	3	5
11.4		매체 보안	9	9
11.5		악성코드 관리	8	9
11.6		로그관리 및 모니터링	6	16
12.1	침해사고관리	절차 및 체계	5	6
12.2		대응 및 복구	6	7
12.3		사후관리	3	3
13.1	IT재해복구	체계 구축	1	3
13.2		대책 구현	5	5

❑ F-ISMS 점검항목 차이

유지	147
변경	105
신규	72
합계	324

❑ F-ISMS 진단결과



3. 보안 Architecture 접근방법

◆ 각 영역별 1/2/3/4에 대한 등급은 SK인포섹이 판단하는 Service의 등급임. 각 등급별로 방안을 수립하여 대응이 필요함. Level이 높을수록 영역별 대응력이 높아짐.

4. Service Level 달성 접근방법

❑ 보안 Service Level 적용 필요성

현재 보안수준에 대한 기준모호

보안수준에 대한 판단 거래소 별로 제 각각

신생 거래소입장 과다한 투자는 어려움

기존 거래소 변화 즉시 대응 어려움

구축/관제/컨설팅측면의 체계적 접근이 필수

SK Infosec 보안 지원 Service Level 명세
(Domain별 관제/구축/컨설팅 구분하여 추진)

No	Domain	Level 1 (필수)	Level 2 (기본)	Level 3 (강화)	Level4 (관리)
1	보안통제체계	1	2	3	4
2	서비스보안	1	2	3	4
3	구간암호화	1	2	3	4
4	OA/인프라보안	1	2	3	4
5	콜센터 보안/운영	1	2	3	4
6	개발 보안	1	2	3	4
7	End-Point 보안	1	2	3	4
8	Forensic	1	2	3	4
9	사법대응	1	2	3	4
10	망분리/망연계보안	1	2	3	4
11	통합모니터링/관제	1	2	3	4
12	Business Risk	1	2	3	4

Illustration

❑ 보안 Service Level 기준

Level 1(필수)

최소 도입 기준 적용

Level 2(기본)

기본 보안 대응체계 확보

Level 3(강화))

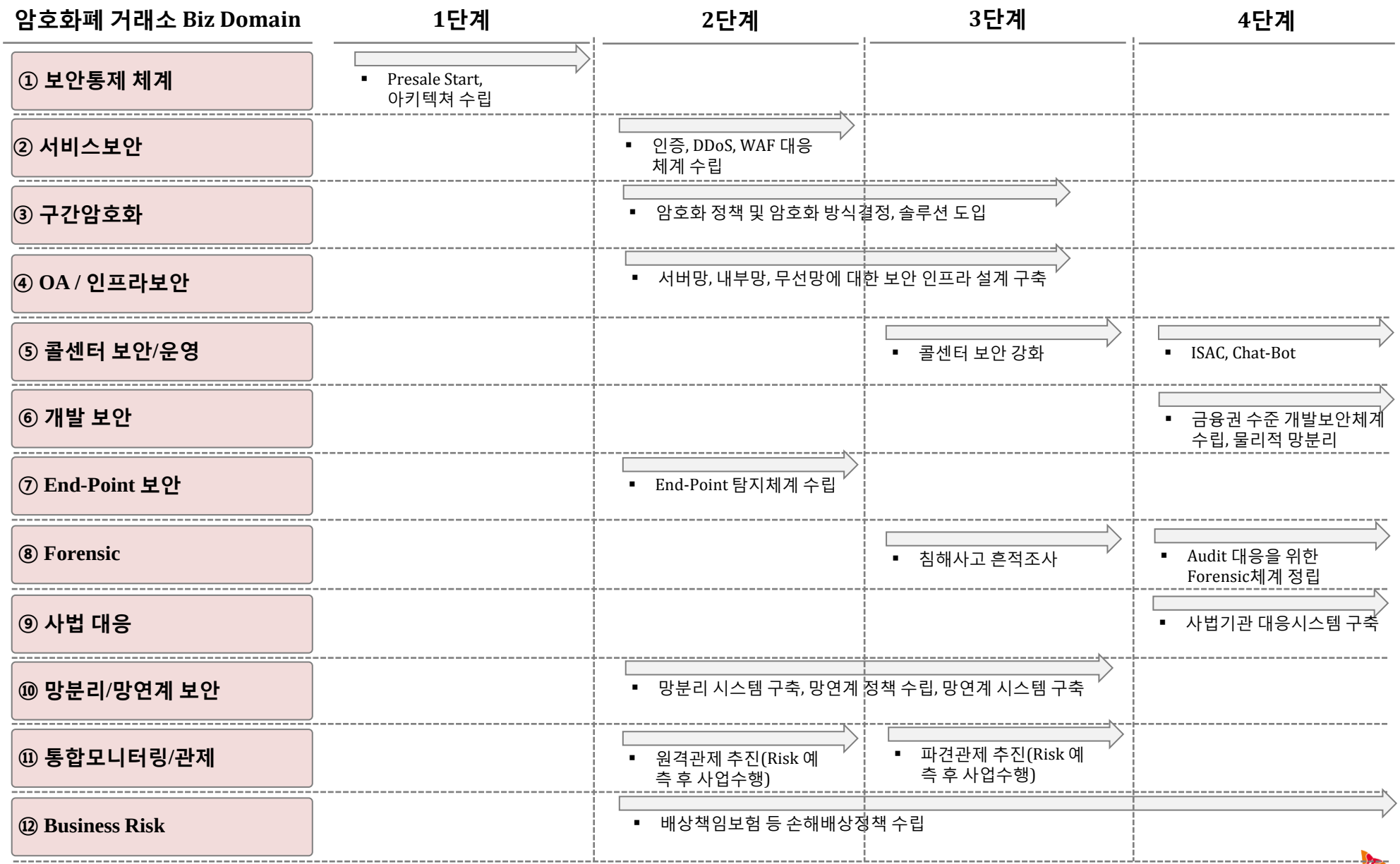
전문 보안 대응체계 확보

Level 4(관리)

보안관리/통제 가시성 확보

- 보안 Level 지원 서비는 현재 거래소의 상황 및 수준을 고려하여 SK Infosec 영업대표와 협의하여 결정

5. 단계별 추진 접근방법


암호화폐 거래소 Biz Domain
1단계
2단계
3단계
4단계
① 보안통제 체계
▪ Presale Start, 아키텍쳐 수립
② 서비스보안
▪ 인증, DDoS, WAF 대응 체계 수립
③ 구간암호화
▪ 암호화 정책 및 암호화 방식결정, 솔루션 도입
④ OA / 인프라보안
▪ 서버망, 내부망, 무선망에 대한 보안 인프라 설계 구축
⑤ 콜센터 보안/운영
▪ 콜센터 보안 강화
▪ ISAC, Chat-Bot
⑥ 개발 보안
▪ 금융권 수준 개발보안체계 수립, 물리적 망분리
⑦ End-Point 보안
▪ End-Point 탐지체계 수립
⑧ Forensic
▪ 침해사고 흔적조사
▪ Audit 대응을 위한 Forensic체계 정립
⑨ 사법 대응
▪ 사법기관 대응시스템 구축
⑩ 망분리/망연계 보안
▪ 망분리 시스템 구축, 망연계 정책 수립, 망연계 시스템 구축
⑪ 통합모니터링/관제
▪ 원격관제 추진(Risk 예측 후 사업수행)
▪ 파견관제 추진(Risk 예측 후 사업수행)
⑫ Business Risk
▪ 배상책임보험 등 손해배상정책 수립

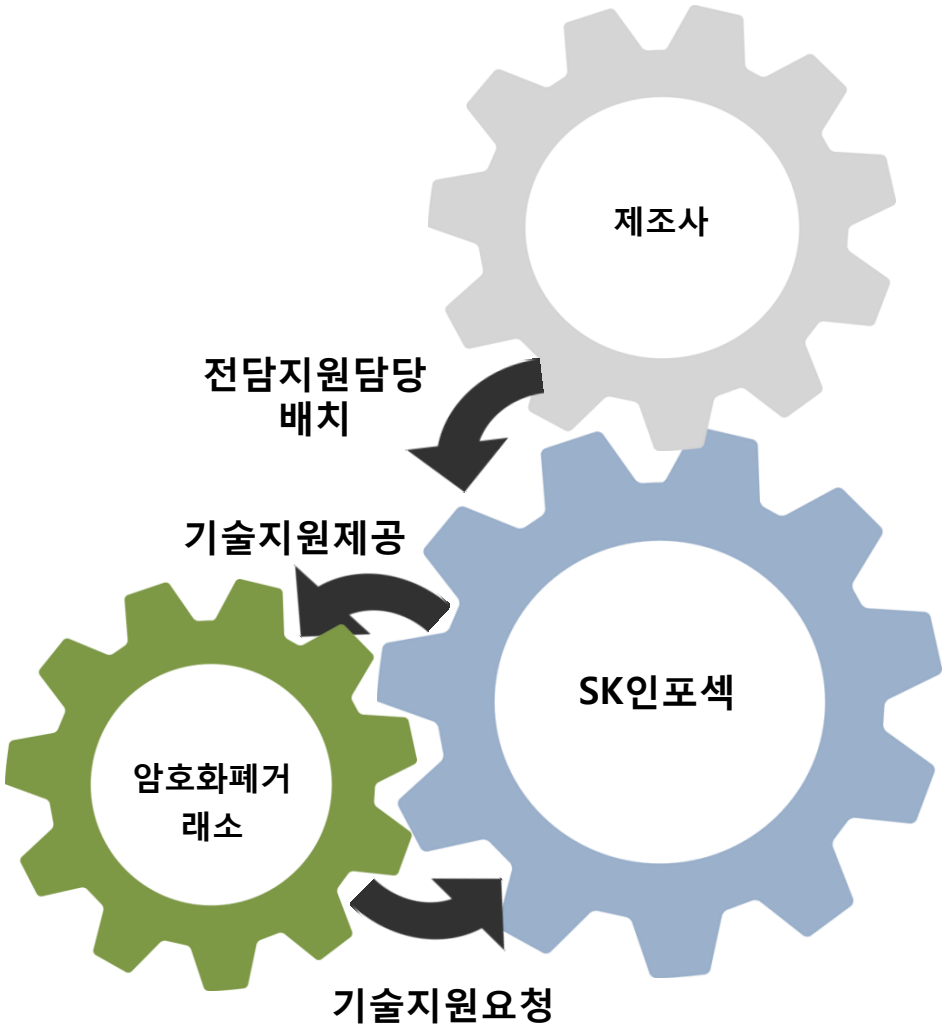
1. 암호화폐 거래소 대응체계 수립

SK인포섹은 암호화폐 거래소에 대해 맞춤형 컨설팅을 수행합니다.

서비스 구축/운영 안전성	보안 아키텍쳐 컨설팅	• 보안 아키텍쳐 관점 추진 방안 제시 - 보안 아키텍쳐 설계, Network Remodeling(Hole분석) - Cloud vs. On-Premise 까지 고려한 Hybrid 보안 설계(솔루션 포함) - 서비스 모델에 따른 기술적/관리적 보안 아키텍처
	보안 프로세스 수립 컨설팅	• 환경에서의 보안정책 구현 및 보안업무 절차/가이드 수립 - 계정관리, 권한관리, 접근통제 등 주요 보안정책 구현 지원 - 서버, 네트워크, DB, 보안장비 등 인프라 보안업무 절차/가이드 수립
자산 보호	보안 모니터링 체계 수립 컨설팅	• 보안 운영현황 및 위협 모니터링 체계 수립 - Cloud 및 내부 인프라 포함된 하이브리드 운영현황 및 로그 모니터링 - 내/외부 침해시도 등 보안 위협 모니터링 보안관제 체계 수립
	보안 위험평가 컨설팅	• 환경의 다양한 보안 위험요소 도출 및 조치 지원 - 모의해킹 진단을 통해 서비스 관리/이용 상의 보안위험 평가 - 보안감사, 시스템 취약점 진단을 통한 관리적/기술적 보안위험 평가
Compliance 요구사항 준수	Compliance 관리체계 수립 컨설팅	• Compliance 요구사항 준수 및 관리체계 수립 - ISMS, ISO27001 등 정보보호 관리체계 인증 취득 지원 - 법적 요구사항 준수에 필요한 보안 관리체계 수립 지원
	Privacy 체계 수립 컨설팅	• 데이터 보호 중심의 Privacy 체계 수립 - 데이터 암호화, 접근권한 통제 등 개인정보보호 체계 수립 - 데이터 복제, Host 자원 공유 환경에서 안전한 개인정보보호 관리

2. Total Outsourcing 서비스 제공

SK인포섹은 Total Outsourcing으로 고객 개별 대응에 대한 불편함을 최소화하기 위해 통합 보안형태 진행합니다.



기술지원

- 기술지원 요청 시 상시 대응(유선, 방문)
- 장애 시 단계별 기술지원
  ① Call ② 원격지원 ③ 방문지원 ④ 제조사 지원
- 월 1회 정기방문 점검 수행
- 보안솔루션 교육 지원
- 최신 보안 동향 제공

운영/관제/모의해킹/진단 수행

- 장비 가용성 점검
- 시스템 운영
  ① 그룹관리 ② 정책점검 ③ 로그분석 ③ 사용자 대응 ④ 변경작업 ⑤ 장애처리
- 자산/현황관리, 백업관리
- IT보안관제(침입탐지,모의훈련)/모의해킹(정기,테마)
- 보안진단(시스템,모바일,IoT 보안진단)

사업/품질관리

- 운영 개선안 도출/보안정책 수립 및 관리 지원
- 사업수행계획서 및 산출물 제공(주간,회의록)
- 업무/조직 변경 지원 및 인원의 변동 관리

Compliance 준수

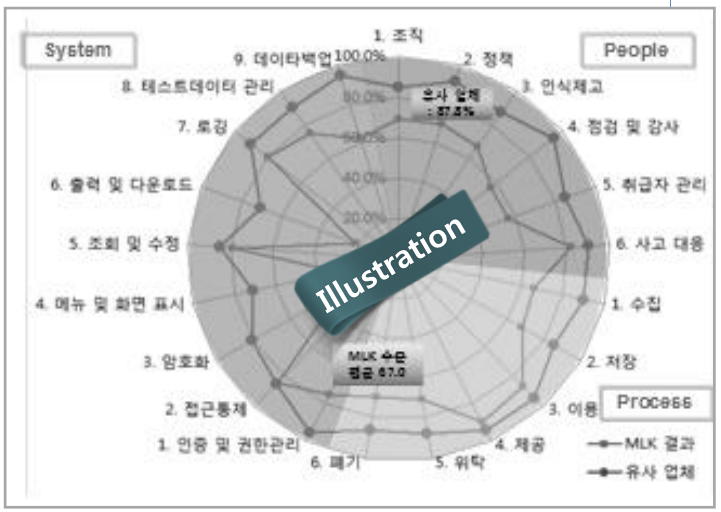
- 데이터 전 Life-Cycle에 걸친 통합 보안 제공
- 사용이력 모니터링 및 사후 감사 방안 제공

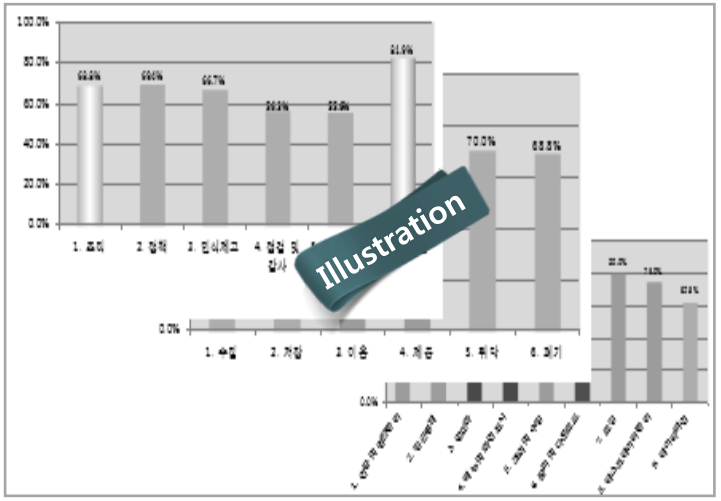
3. 개인정보점검 대응 컨설팅

SK인포섹은 개인정보에 대한 점검을 기반으로 타업체 대비 추진 방안을 제시합니다.

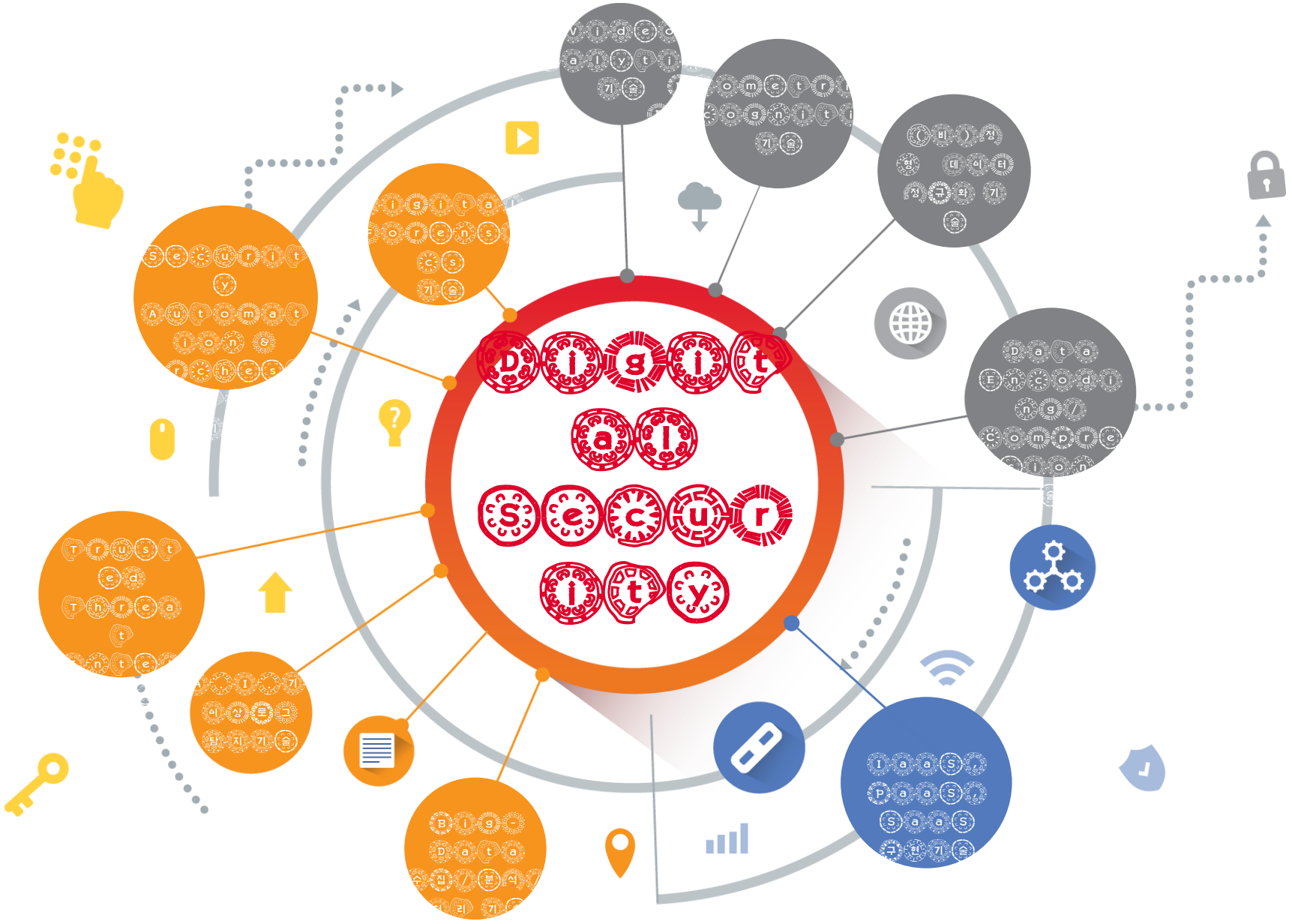
개인정보보호점검 수행 결과 예시

영역	분류	준수도	유사 업체
PEOPLE	1.조직	68.8%	85.0%
	2.정책	69.4%	92.0%
	3.인식제고	66.7%	87.0%
	4.점검 및 감사	56.3%	950.0%
	5.취급자 관리	55.6%	85.0%
	6.사고 대응	81.9%	90.0%
PROCESS	1.수집	66.3%	90.0%
	2.저장	67.5%	85.0%
	3.이용	86.8%	95.0%
	4.제공	90.3%	94.0%
	5.위탁	70.0%	88.0%
	6.폐기	68.8%	86.0%
SYSTEM	1.인증 및 권한관리	75.0%	96.0%
	2.접근통제	83.3%	85.0%
	3.암호화	31.3%	80.0%
	4.메뉴 및 화면 표시	29.2%	71.0%
	5.조회 및 수정	79.2%	85.0%
	6.출력 및 다운로드	21.9%	70.0%
	7.로깅	80.0%	90.0%
	8.테스트데이터 관리	75.0%	90.0%
	9.데이터 백업	62.5%	95.0%



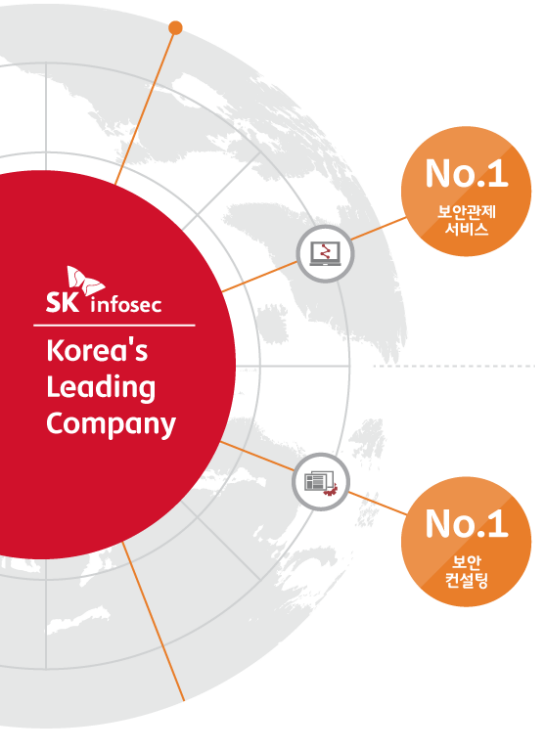


4. 보안 위협 탐지 및 통합 대응역량(Digital Security)



6. SK인포섹 회사개요

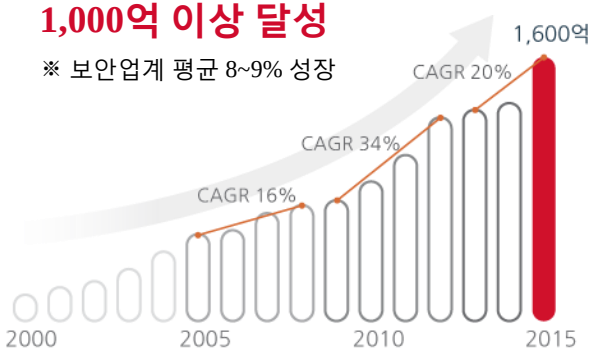
보안, 그 이상의 가치를 제공하는 기업, 고객의 가치를 보호하는 기업 국내 정보보안 1위 SK인포섹입니다.



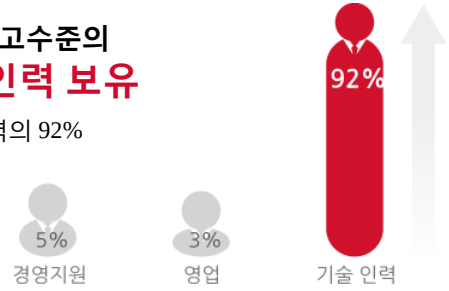
- 국내 최다 고객이 선택한 다년간 노하우의 최고 보안 수준 (1,600개 이상 기업)
- 최대 Intelligence를 보유한 Big Data 분석기술 (1일 1억건 통합로그 처리)
- 국내 최고수준의 최다 보안관제 전문인력 보유 (관제인력 수 : 800명 이상)

- 12년 연속 업계 1위 ('14년 시장 점유율 1위 M/S 23%, 고객 재수주율 1위)
- 국내 최다 보안컨설턴트 보유 (컨설턴트 수 : 140명 이상)
- 국내 최고 수준의 화이트 해커 최다 보유

4년 연속
1,000억 이상 달성
※ 보안업계 평균 8~9% 성장



업계 최고수준의
기술인력 보유
전체 인력의 92%



- 국제침해사고대응협의회(FIRST) 국내 최초 민간기업 회원
- 글로벌 사이버위협연합(CTA) 국내 최초 가입
- 보안관제 전문업체 [과학기술정보통신부]
- 정보보호컨설팅 전문업체 [과학기술정보통신부]
- 개인정보 영향평가 기관 [행정안전부]

- 한국인터넷진흥원(KISA) 정보보호관리체계 인증 [ISMS 03-002]
- ISO27001 국제품질 인증 [DNV]
- IT서비스 Center of Excellence 인증 [BenchmarkPortal]
- ITO Service ISO 20000 인증 [BSI]
- IQNet 국제 품질 인증

보안 그 이상의 믿음