2023 Digital Finance & Cyber Security

디지털금융 및 사이버보안 이슈 전망

금융보안원

금융보안원
FINANCIAL SECURITY INSTITUTE

전망 분야별 세부 주제

보안 위협 및 대응 분야

1. 사이버 공격 경로로 악용될 수 있는 엔데믹 취약점
2. 랜섬웨어, 피싱 앱 등 사이버 위협의 끝없는 진화
3. 오픈소스 이용 활성화와 강조되는 공급망 보안
4. 디지털자산의 당면 과제, 리스크 관리체계 마련

디지털 신기술 및 리스크 분야

5. 대세로 자리잡은 클라우드와 보안 고려사항
6. 인공지능 활용, 공정성·보안성 확보를 통한 이용자 보호 필수
7. 디지털 신원증명 활용에 따른 기대와 우려

컴플라이언스 및 전략 분야

8. 금융보안 규제 합리화, 전제되는 자율보안
9. 마이플랫폼 시대, 데이터 확보와 보호
10. 금융권 채널 변화의 핵심 디지털 연결

01

사이버 공격 경로로 악용될 수 있는 **엔데믹 취약점**

제로데이 등 고위험 보안 취약점을 이용한 사이버 공격 증가

제로데이 취약점은 제조사 · 개발자가 인지하거나 공식적인 패치를 배포하기 전에 발견된 보안 취약점으로, 최근 이를 악용한 공격이 증가

* 제로데이 취약점 익스플로잇 건수에 대해 구글은 '20년 25개 → '21년 58개로, 미국 보안 회사 맨디언트는 '20년 30개 → '21년 80개로 증가하였음을 각각 발표

영향 범위가 광범위한 엔데믹 취약점으로 인한 위협 가능성

Log4j의 경우와 같이 취약점의 영향을 받는 시스템 수가 많고 광범위한 패치가 필요한 경우, 엔데믹 취약점(Endemic Vulnerability)으로 잔존하며 위협이 될 가능성

* 미국 사이버안전심의위원회는 Log4j의 취약한 인스턴스가 앞으로 10년 이상 시스템에 잔존할 것으로 평가하며 '엔데믹 취약점'이라 명명

US Cyber Safety Review Board warns that Log4j will remain 'endemic'

보안 취약점 모니터링 및 최신 패치 적용이 기본적이지만 매우 중요

02

랜섬웨어, 피싱 앱 등 **사이버 위협의 끝없는 진화**

랜섬웨어, 보이스피싱 악성 앱 등이 수법·기능 측면에서 계속해서 발전

랜섬웨어 (수법)

암호화 | DDoS | 데이터유출

다중갈취(Multi extortion)

보이스피싱 악성 앱 (기능)

2018년 하반기 (Shadowvoice)	2021년
전화번호 가로채기	전화 수신 위장
문자메시지 탈취	라이브 스트리밍
전화번호부 탈취	명령어 실행
스크린샷 탈취	
기기정보 탈취	

사이버 위협이 디지털 금융 서비스 및 환경, 기술을 역이용하며 진화

침해사고훈련 및 금융권 사이버 위협 정보공유 체계 적극 활용 필요

랜섬웨어 유포 방식 등 최신 공격 트렌드를 반영한 침해사고 대응훈련 실시를 통해 경각심을 높이고 정보보호 수칙(예 :출처가 분명하지 않은 이메일 열람 금지) 준수 필요

짧은 시간 내 특정 공격 방식을 다양한 타겟을 대상으로 수행 → 공격 방식을 신속하게 공유함으로써 동일한 방식의 업계 내 위험 전파를 무력화할 필요

02

랜섬웨어, 피싱 앱 등 **사이버 위협의 끝없는 진화**

제로 트러스트(Zero Trust)로 보안 패러다임 전환 필요

재택 · 원격근무, 클라우드 도입 등으로 변화하는 업무 환경, 진화하는 사이버 위협 등에 대응하기 위해서는 최소 권한 접근, 보안 가시성 확보 등에 기반한 제로 트러스트(Zero Trust)로 보안 패러다임 전환 필요

제로 트러스트 원칙

1. 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주
2. 네트워크 위치와 관계없이 모든 통신을 안전하게 함
3. 기업 리소스에 대한 접근은 각 세션에 기반하여 승인됨
4. 리소스에 대한 접근은 ID, 애플리케이션, 서비스, 자산의 상태 등 동적 정책에 의해 결정
5. 기업은 소유한 모든 관련 자산의 무결성과 보안 상태를 모니터링하고 측정
6. 리소스에 대한 모든 인증 및 승인은 동적으로 수행되며 접근을 허용하기 전 엄격히 적용
7. 기업은 자산, 네트워크, 인프라 통신 상태 정보를 수집하고, 이를 통해 보안을 개선

03

오픈소스 이용 활성화와 강조되는 공급망 보안

오픈소스를 포함한 소프트웨어 공급망의 사이버 리스크가 증가

오픈소스 대상 위협

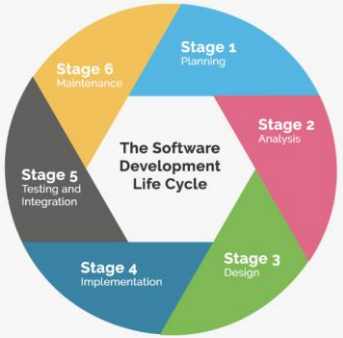
타이포스쿼팅(Typosquatting)

정상 패키지명과 쉽게 혼동될 수 있는 이름 사용
(예) jellyfish -> jelLyfish / electron -> electorn

디펜던시 컨퓨전(Dependency Confusion)

신뢰되는 코드 요소 또는 패키지의 복사판(악성)을 업로드하여 악의적인 패키지가 설치되도록 유도

소프트웨어 공급망 대상 위협

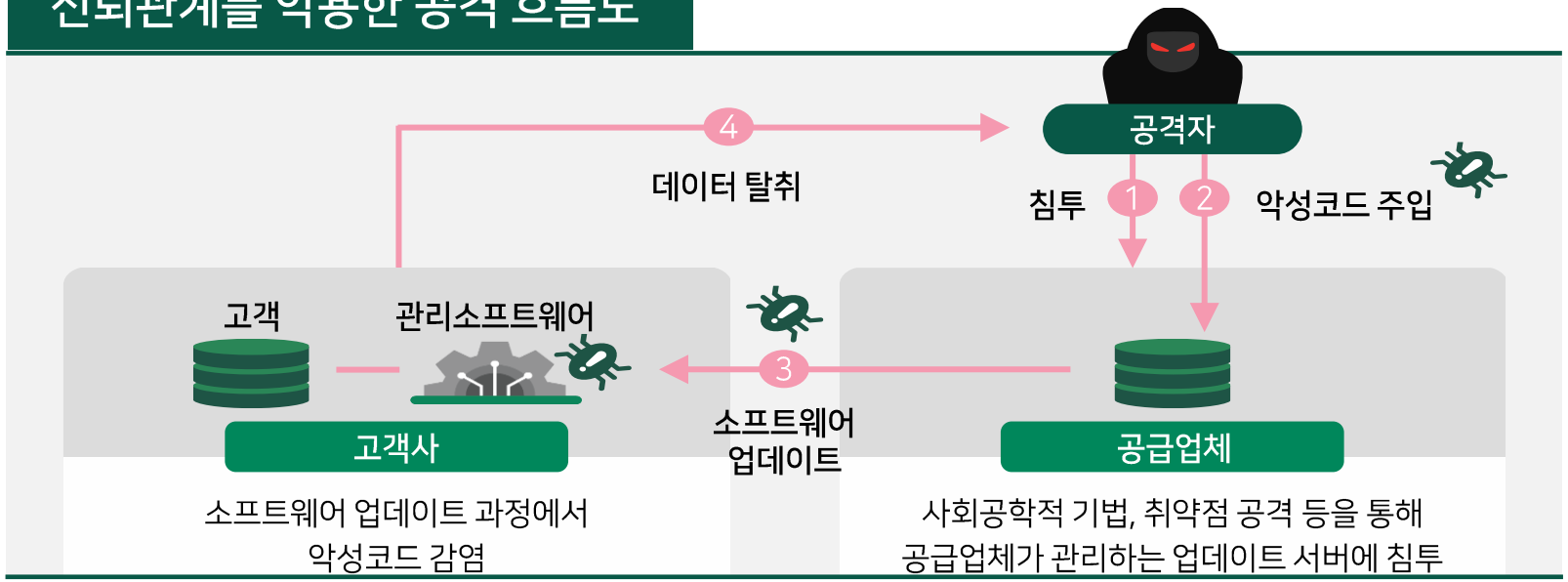


소프트웨어의 개발, 배포, 설치, 유지보수 과정에 개입

↓

변조된 소프트웨어가 사용자의 시스템에 전달

신뢰관계를 악용한 공격 흐름도



출처 : 유럽네트워크정보보호원(ENISA), 「Threat Landscape for Supply chain Attack」('21.7.) 참고 및 재구성

03

오픈소스 이용 활성화와 강조되는 공급망 보안

소프트웨어 자재 명세서(SBOM)를 기반으로 체계적인 관리 필요

- SBOM(Software Bill Of Materials)은 소프트웨어 공급망 강화를 위한 보안리스크 관리 수단
- 소프트웨어 개발에 사용된 다양한 구성 요소의 상세한 내용과 구성 요소 간 관계에 대한 기록

국외 SBOM 관련 동향

국가	내용
 EU	유럽네트워크정보보호원(ENISA) 'IoT 보안을 위한 가이드라인'('20.11월) - 공급망 보호를 위한 모범 사례로 SBOM 제공을 제안
 네덜란드	국가사이버안보센터(NCSC) '사이버보안 강화를 위한 SBOM 사용'('21.4월) - SBOM 활용 현황과 향후 방향을 전망
 미국	행정부 '사이버보안 향상에 관한 행정명령'('21.5월) - 소프트웨어 공급망 강화를 위해 SBOM 제출을 의무화

04

디지털자산의 당면과제, 리스크 관리체계 마련

디지털자산 관련 리스크 관리체계 마련을 위한 점진적 입법 추진 전망

디지털자산업의 내부 요인

- 디지털자산의 지급결제기능 강화
- 좁혀지는 디지털자산 기반 경제와 실물경제 사이의 간극
- 디지털자산에 내재된 높은 유동성 및 변동성 리스크 등

디지털자산업 외부의 충격

해킹 등 사이버 사고 발생

디지털자산 가치 폭락

디지털자산 사업자의 신뢰도 하락 등으로 인한 지급 불능 발생 시 실물경제 영향

출처 : 보험연구원, 「CEO Brief 가상자산 시장의 성장과 향후 주요이슈」('22.4월) 및 국회미래연구원, 「가상화폐의 파급효과와 정책 대안 연구」('20.12월) 내용 요약 및 재구성

국가	내용
국내	디지털자산 시장의 공정성 회복과 안심거래 환경 조성을 위한 법률안 발의('22.10월)
EU	EU 암호자산시장법률안(MiCA) 발표('20.9월) * Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive
미국	책임 있는 금융혁신법*안 발의('22.7월), 디지털자산의 포괄적 규제 프레임워크** 발표('22.9월) * Responsible Financial Innovation Act ** Fact Sheet: White House released first-ever comprehensive framework for responsible development of digital assets
일본	스테이블 코인의 투자자 보호 및 자금세탁 대응을 위한 자금결제법 개정('22.6월) * かつ効な済のを図るための済に関するのをする

05

대세로 자리잡은 클라우드와 보안 고려사항

디지털 혁신을 위한 핵심 인프라로 자리잡는 클라우드

- 애플리케이션 운영, 업무 자동화, 빅데이터 분석 등 다양한 기술을 활용함에 따라 보다 유연한 인프라 운용이 가능한 클라우드 이용을 적극 검토
- 내부 직원 간 협업 강화 및 업무 생산성 증대를 위한 클라우드 기반의 서비스형 소프트웨어(SaaS) 활용

구분	사고원인 및 피해내역	발생연월
계정 도난	온라인 예약 소프트웨어 제공업자의 클라우드 접근 계정 도난으로 37만 명의 이름, 이메일 주소, 전화번호 등 개인정보 유출	'21.12월
설정 오류	비인가자가 클라우드 내 데이터에 접근 가능토록 설정, 클라우드 접속키, 데이터, 결제 내역 등 A사의 내부 문서 및 데이터가 온라인 상에 노출	'21.10월
CSP 운영 실수	유지보수 작업 중 고객 사이트 삭제로 400여 개의 서비스 중단	'22.4월

출처 : 관련 언론보도

클라우드 보안 강화 및 멀티 클라우드 등 출구전략 마련 필요

클라우드 보안 관리 강화

클라우드 보안 전문 인력 확보

사각지대 방지

MSP(Managed Service Provider) 이용 시에도 사내 정보보호 조직의 보안 관리 책임 철저

클라우드 보안 형상 관리 활용

CSPM

Cloud Security Posture Management

클라우드 자원, 애플리케이션, 데이터를 안전하게 관리할 수 있도록 통합 모니터링 및 관리 기능 제공

집중리스크 및 종속리스크 유의

집중리스크

제한된 수의 CSP에 여러 고객이 집중됨에 따라 사고 시 다수 피해 발생

종속리스크

특정 CSP에 의존 시 리스크 전이, 전환 비용 과다 발생

06

인공지능 활용, 공정성·보안성 확보를 통한 이용자 보호 필수

금융권 내 인공지능(AI) 이용이 활발

업무자동화	RPA 도입으로 '22.9월 현재 총 240개 업무에서 1인당 연간 약 170일 절감(B은행)
고객 응대	AI 상담원이 선결제와 한도 조정, 비밀번호 등록.변경 등을 상담(C카드)
신용 평가	담보대출 실행 후 등기 관련 변경사항의 사후 확인 및 전산 등록업무를 AI기반으로 자동화(D은행)
투자및상담	매일 뉴스를 분석하고, 투자 가치가 있는 정보를 선별하여 전달하는 AI 뉴스 서비스 운영 (E증권)
사이버보안	AI 기반 방어체계를 지향하는 보안 위협 대응 자동화 시스템 및 프로세스 구축(F은행)

출처 : 한국금융연구원,「금융업의 인공지능 활용과 정책과제」('22.2월) 및 관련 언론보도

AI 활용 시 신뢰성·보안성 확보 및 이용자 보호가 매우 중요

금융권 인공지능 활용 활성화 및 신뢰확보 방안 주요내용

* 금융보안원 참여 과제는 파란색으로 표기

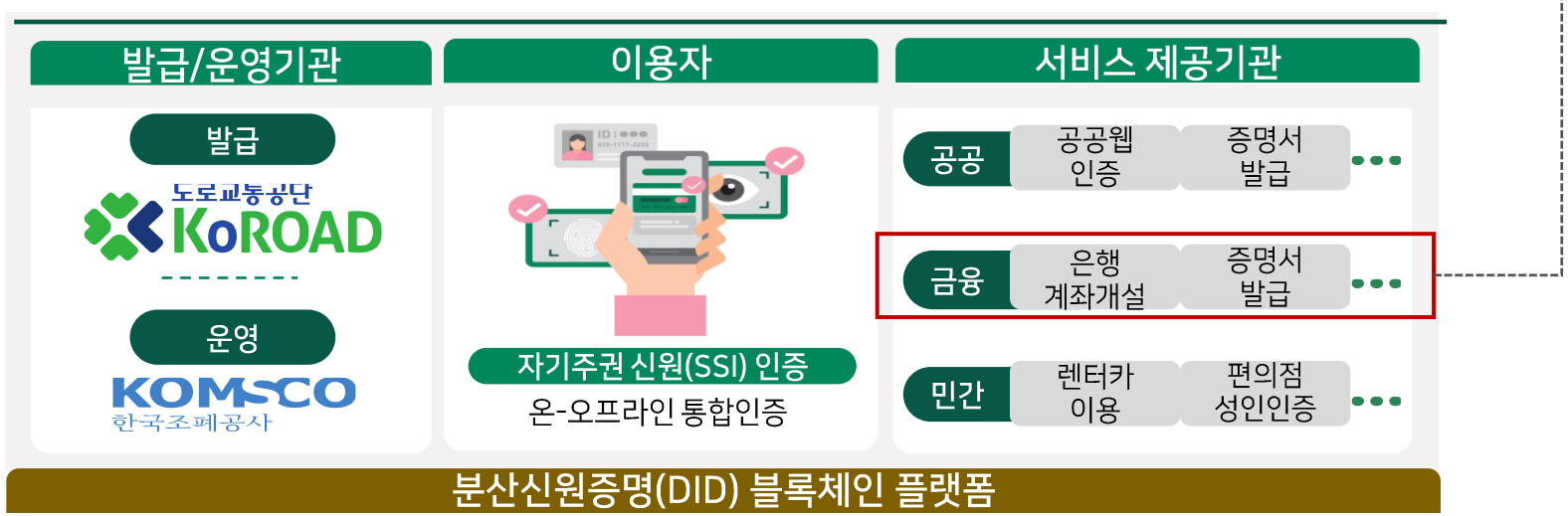
양질의 빅데이터 확보 지원	AI 활성화를 위한 제도 정립	신뢰받는 AI 활용 환경 구축
금융 AI 데이터 라이브러리 구축	금융 AI 개발·활용 안내서 발간	금융 AI 테스트베드 구축
금융권 협업을 통한 데이터 공동 확보	설명가능한 AI (eXplainable AI, XAI) 요건 마련	AI 기반 신용평가모형 검증체계 마련
데이터 전문기관 추가지정	망분리 및 클라우드 규제 개선	AI 보안성 검증체계 구축
		AI를 활용한 효율적 감독체계 구축

07

디지털 신원증명 활용에 따른 기대와 우려

금융권 모바일 운전면허증 사용 허용 ('22.7월~)

13개 은행 영업점 창구, 4개 은행 스마트폰 앱에서 계좌개설 등 금융거래에 이용



출처 : 라온시큐어, 「대한민국 최초의 디지털 신분증」('21.11월)

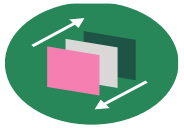
모바일 신분증 활용 관련 보안 위협 대응 및 디지털 격차 해소 필요

08

금융보안 **규제 합리화,** 전제되는 **자율 보안**

디지털 전환을 지원하기 위해 클라우드 및 망분리 규제 개선을 추진

「금융분야 클라우드 및 망분리 규제 개선방안」주요 내용

구분	현황	개선
 클라우드	중복·유사한 CSP 평가 항목	중복·유사한 평가항목 정비 (평가항목을 141개에서 54개로 축소)
	비중요업무도 모든 이용규제 준수 필요	중요·비중요 업무간 클라우드 이용 절차 차등화
	금융회사 등이 각각 CSP 평가 수행	금융보안원 대표평가제 도입
 망분리	획일적·일률적인 물리적 망분리 규제	개발·테스트 분야 망분리 예외
		비전자금융업무 및 SaaS에 대한 망분리 예외 추진 (규제 샌드박스)
		(중장기) 단계적 망분리 완화 추진

금융권의 자율적인 보안 강화 노력 제고 필요

보안성을 고려한 안전한 네트워크 인프라 구성, 소스코드 보안 관리를 위한 내부정책 수립・운용, 소스코드 유출에 대비한 침해사고 대응절차 마련 등 내부통제 강화 및 추가 보안 대책 마련 필요

SaaS 관련 망분리 예외 추진 예정 → 향후 샌드박스 운영 성과에 따라, SaaS 이용 관련 망분리 규제 개선으로 이어질 가능성 (사례 : K사 금융기술연구소에 대한 망분리 규제 예외조치('20.4월)

09

마이플랫폼 시대, 데이터 확보와 보호

금융-비금융 연계를 통한 플랫폼 전략, 데이터 및 이용자 보호 고려 필요

금융-비금융 연계를 통한 플랫폼 전략 추진 사례

기업	제공 서비스	플랫폼 형태	서비스 내용
신한은행	배달 서비스	직접 제공	고객과 가맹점 등 플랫폼 참여자 모두에게 혜택을 제공하는 상생 배달앱
	이커머스 연계	제휴	온라인 셀러를 위한 특화 금융상품 제공 및 플랫폼 활용 공동 마케팅 추진
우리은행	택배 서비스	제휴	택배 플랫폼 전문업체와 제휴하여 은행앱에서 택배 서비스 제공
NH농협은행	꽃 배달 서비스	제휴	한국화훼농협의 화훼상품을 은행앱에서 주문 배송
국민은행	알뜰폰 상품 결합	직접 제공	기존 금융 고객을 유지하거나 신규 고객 유치를 위해 알뜰폰 서비스 제공 및 통신비 할인 혜택 제공

출처 : 관련 언론보도

초개인화된 맞춤형 금융·생활 서비스를 제공하는 마이플랫폼(My Platform)으로 발전 예상

데이터 확보 경쟁 과열, 정보 독과점 및 개인정보 유·노출 등 경계 필요

초개인화 서비스(마이플랫폼)

양질의 개인정보가
대량 집중 및 융합됨을 전제

→

데이터 확보 경쟁 과열,
소수 플랫폼의 정보 독과점 등 이슈를 방지하고
개인정보의 유출 및 노출을 경계할 필요

금융권 **채널** 변화의 핵심 **디지털 연결**

금융권 대면·비대면 채널이 '디지털' 과 '연결'로 고도화

최근 금융권 디지털 점포 추진 사례

출처 : 관련 언론보도

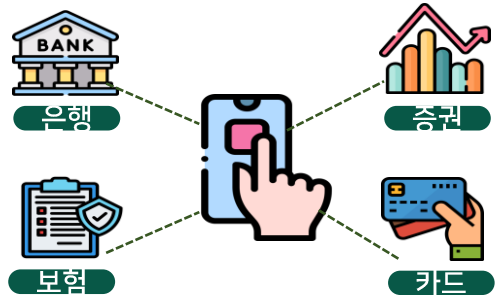
무인 기반으로 운영. 디지털 데스크, 스마트키오스크, 로봇 컨시어지 , 종합금융기기(STM)를 통한 체크카드 및 보안매체 발급, 현금 및 수표 입출금, 화상상담 전용 창구를 통한 통장개설 등 가능

(사례) 신한은행-GS리테일, KB국민은행-노브랜드 등 협업을 통한 디지털 혁신 점포 운영

옴니채널

독립적으로 운영되는 채널의 유기적 연결

디지털 유니버설 금융화



하나의 앱으로 다양한 금융서비스 연결

채널 변화에 따른 디지털 리스크 관리에 집중 필요

- 디지털 혁신 점포 내 설치된 기기의 고장 등 돌발 상황에 따른 서비스 지연, 키오스크 등 셀프 서비스 기기를 노린 사이버 위협 등 운영·보안 리스크에 대한 대응 방안 마련 필요
- 디지털 연결로 인해 발생 가능한 보안 위험을 방지하기 위해 서비스 개발, 운영, 유지보수 시 철저하게 테스트 및 점검할 필요 (* 통합앱에서 MTS 접속 시, 타인의 증권계좌 정보가 노출되는 사고 발생 ('22.4월))

Thank you.