

제26호

2021-4Q

전자금융과 금융보안

e-Finance and Financial Security

Leading Article

디지털 문해력과 금융

장원철, 서울대학교 통계학과 교수

Research

· 오픈소스 SW 공급망 공격 대응기술 동향

이희조, 고려대학교 컴퓨터학과 교수

· 블록체인 가상자산 관리의 보안성 강화를
위한 다자간 보안컴퓨팅 기술 동향

배경일, 아톰릭스랩 공동설립자

· 전기통신금융사기 최신 동향 및 피해사례
분석 프레임워크 소개

정영훈, 금융보안원 금융보안관제센터 대리



금융보안원
FINANCIAL SECURITY INSTITUTE



본 간행물에 게재된 내용은 금융보안원의 공식 견해가 아니며 집필자 개인의 견해를 밝힙니다. 본 간행물 내용의 무단전재를 금하며, 가공 인용할 때에는 반드시 출처 및 집필자를 명시하여 주시기 바랍니다.

인터넷 홈페이지(www.fsec.or.kr)를 이용하시면 본 연구지에 게재된 자료를 보다 편리하게 보실 수 있습니다.

제26호

2021-4Q

전자금융과 금융보안

e-Finance and Financial Security



금융보안원
FINANCIAL SECURITY INSTITUTE



CONTENTS

01

Leading Article

디지털 문해력과 금융

2

장원철, 서울대학교 통계학과 교수

02

Research

오픈소스 SW 공급망 공격 대응기술 동향

11

이희조, 고려대학교 컴퓨터학과 교수

블록체인 가상자산 관리의 보안성 강화를 위한 다자간 보안컴퓨팅 기술 동향

31

배경일, 아톰릭스랩 공동설립자

전기통신금융사기 최신 동향 및 피해사례 분석 프레임워크 소개

55

정영훈, 금융보안원 금융보안관제센터 대리

03

Issue·Trend

▶ 산업동향

금융권 메타버스(Metaverse) 동향 및 시사점	84
정진영, 금융보안원 보안연구부 책임연구원	

▶ 핀테크·신기술

양자보안기술 동향	93
김그린, 금융보안원 융합보안부 주임	
클라우드 기반 인텔리전트 에코시스템 주요 내용 및 시사점	112
이승봉, 금융보안원 융합보안부 과장	
캄보디아 CBDC '바콩(Bakong)' 기술 분석	122
김지훈, 금융보안원 융합보안부 대리	

▶ 법·정책

이사회의 금융보안 역할·책임 강화 관련 국외 동향 및 시사점	144
신성환, 금융보안원 보안연구부 연구원	

04

News·Notice

금융보안 교육 안내	178
금융보안원 소식	180
사원기관 소식	182



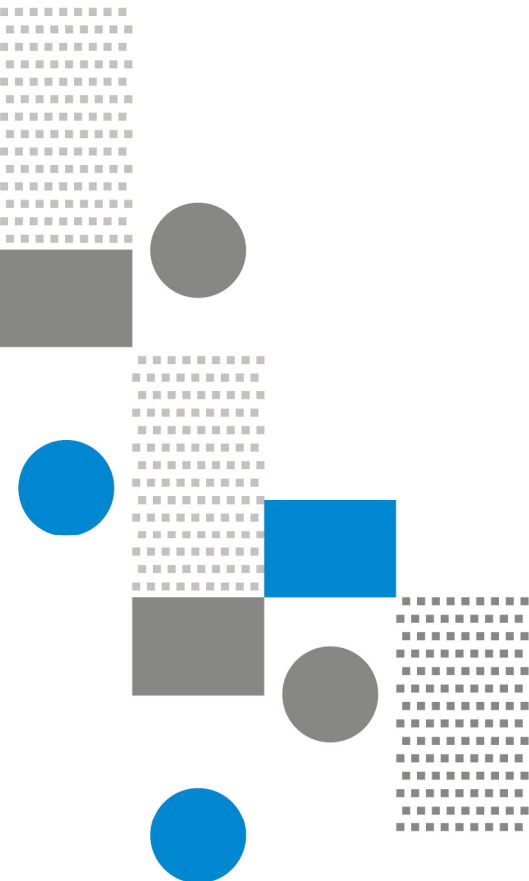
e-Finance and Financial Security

_01

Leading Article

디지털 문해력과 금융

장원철, 서울대학교 통계학과 교수



디지털 문해력과 금융

- 경제학과 교수님도 이 상품에 투자하셨어요



장원철, 서울대학교 통계학과 교수

1. 시작하면서

정기예금이 만료되어서 교내에 있는 은행을 방문하게 되면 창구직원이 여러 가지 금융상품을 투자하라고 권유하곤 한다. 대부분의 경우 평균 이상의 경제 지식을 가졌다고 생각하는 나에게도 생소한 용어들이 난무한 금융상품에 쉽게 투자하고 싶은 생각이 들지 않는다. 하지만 나와 같은 투자자들도 “조금 전에 다녀 가신 경제학과 교수님도 이 상품에 투자하셨어요”라는 말에 현혹되어서 묻지마 투자를 하는 경우가 종종 있다. 하지만 이러한 묻지마 투자에서 손실이 날 경우 얼굴도 모르는 경제학과 교수를 찾아가서 항의할 수는 없는 실정이고 그 경제학과 교수님이 없는 시간을 쪼개어서 금융상품을 연구해서 투자했을 확률은 거의 0에 가깝다. 옵션의 적절한 가격을 제시한 블랙-숄즈 방정식으로 노벨경제학상을 수상한 스탠퍼드 대학 경제학과 숄즈 교수의 투자 실패를 보더라도 이론으로 무장한 경제학자가 제시한 상품이 반드시 성공한다는 보장은 없다.

요즘은 “경제학과 교수”라는 용어를 AI, 혹은 로보어드바이저라는 말이 대체하고 있는 추세이다. 투자를 하기 위해서는 해당 상품을 반드시 이해해야 한다고 믿는 나와 같은 사람은 창구직원이 권유한 금융상품을 즉석에서 가입하기보다는 일단 사무실로 돌아와서 해당 상품에 관한 정보를 인터넷을 통해 검색하고 관련 용어들을 이해하려고 하지만 종종 검색엔진에 제공하는 너무 많은 정보 속에서 과연 내가 필요한 정보는 어떤 것인지 알아내는 것은 정말 쉽지 않다. 영화 ‘건축학개론’에서 주인공의 선배는 하드디스크가 1GB라는 걸 자랑하지만 내가 대학 재학시 20MB 하드디스크를 장착하고 집에 있는 게임을 다 넣어도 하드디스크 반도 차지 않는다고 고민한 걸 생각해 보며 우리가 접하는 디지털 정보의 양은 기하급수적으로 늘었다는 것을 알 수 있다.

사실 우리는 정보의 홍수 시대에 살고 있다고 해도 과언이 아니다. 뉴욕타임스의 한 호에 실린 정보의 양이 17세기 영국의 평범한 사람이 평생 소비하는 정보의 양과 비슷하다고 하니 양적인 측면 정보의 양은 어마어마한 성장을 한 것으로 생각할 수 있다. 이러한 추세에 맞추어 2015년 세계경제포럼에서는 기존의 교육에 포함되었던 문해능력, 수리능력, 과학지식에 더불어 새로운 교양 교육에 추가로 포함될 내용은 문제 해결을 위해 정보를 수집, 분석, 공유하는 컴퓨터 활용능력, 디지털 문해력이라고 선언했다. 그렇지만 앞에서 얘기한 것과 같이 수많은 정보 속에서 내가 필요로 하는 제대로 된 정보를 찾는 것은 건초더미에서 바늘 찾는 것에 비유할 수 있다. 특히 지금과 같은 팬데믹 상황에서 쏟아지는 코로나에 관한 무분별한 잘못된 정보를 세계보건기구에서는 인포데믹이라는 용어로 정의하고 있는 실정이다.

디지털 문해력은 여러 가지 측면에서 우리의 일상생활에서 정보 기반 의사결정의 중요성을 일깨워 줄 수 있다. 금융과 깊은 관련이 있는 디지털 문해력의 첫 번째 항목으로 리스크 측정을 들 수 있다.

다음의 사례 중 가장 리스크가 큰 행동은 무엇일까?

1. 아스트라제네카 백신을 맞아서 혈전이 생길 경우
2. 우연히 만난 사람의 휴대폰 뒷자리 5개 숫자를 맞추는 경우
3. 로또 100장을 샀을 경우 이 중 하나가 1등에 당첨될 경우
4. 스카이다이빙을 시도하다가 사망하는 경우

정답은 3번으로 약 8만분의 1 정도이다. 물론 로또 당첨은 리스크는 아니고 행운이라고 간주할 수 있지만 4가지 경우에서 가장 발생할 확률이 높은 경우이며 나머지 경우가 생길 확률은 약 10만분의 1 정도이다. 언론을 통해 백신 부작용이 흔히 일어나는 일이라고 생각하는 사람들은 로또 100장을 사서 당첨될 것이라고 믿는 편이 더 낫다는 이야기이다. 또 하나의 놀라운 통계 중 하나는 최근 5년간 무단횡단 사고는 연평균 5천 건에 달하며 치사율은 무려 8.4%에 달한다. 무단 횡단 횟수가 백신 접종 숫자에 훨씬 못 미칠 것이라는 걸 감안한다면 무단횡단의 리스크가 엄청나게 높다는 것을 알 수 있다. 하지만 우리 대부분은 무단횡단이 그렇게 위험하다고 생각해 본 적이 없을 것이다. 따라서 이러한 리스크를 이해하는 객관적인 방법은 우리가 일상생활에서 쉽게 체감하는 다른 리스크와 비교하여 보는 것이다. 백신 접종을 걱정한다면 무단횡단이야말로 절대 해서는 안 되는 위험 천만한 행동이다. 비슷한 예로 몇 년전 가슴기 살균제 성분인 CMIT, MIT가 포함 되었다고 난리가 난 치약 파동을 들 수 있다. 이러한 유해 물질은 일정수준 이상 인체 기관에 들어갈 경우 문제가 생긴다. 치약 파동 당시에도 유해 물질의 양은 현저하게 낮았고 실제로 같은 성분이 화장품 등에서 사용이 되고 있었다. 마찬가지로 세계 보건기구에서 가공육을 담배, 석면과 같은 1급 발암물질에 분류했지만 우리 국민의 평균 가공육 섭취량은 6g에 불과하며 세계보건기구가 위험한 섭취량으로 분류한 1일 평균 50g에는 현저히 미치지 못하는 수준이다. 즉 가공육을 지금의 10배 가까이 섭취하지 않는 한 가공육으로 인한 암 발병에 대해 걱정은 할 필요가 없다.

두 번째는 인과관계와 상관관계의 구별이다. 간단한 예로 한국에서만 통용되는 “밤에 선풍기를 틀고 자면 죽는다”라는 괴담이 있다. 혈액형 성격과 더불어 대표적인

한국형 괴담이지만 왜 이런 괴담이 생겼는지는 알 수 없다. 물론 여름철 한밤중에 심장마비나 뇌졸중으로 병원 응급실에 오는 사람 중 집에서 선풍기를 틀고 잤냐고 물어본다면 많은 사람이 선풍기를 켜놓고 잤다고 대답할 것이다. 하지만 선풍기 바람이 뇌졸중이나 심장마비를 유발했다는 건 터무니없는 이야기이다. 상관관계의 재미있는 예를 찾고 싶다면 Tyler Vigen의 웹사이트 (www.tylervigen.com)을 찾아보기를 권한다. 낚싯배에서 떨어져서 익사한 사람 숫자와 켄터키주의 혼인율의 상관관계를 비롯한 아주 허무맹랑한 상관관계에 관한 다양한 예를 제시하고 있다. 흡연이 폐암을 유발한다는 것은 이미 검증된 인과관계이지만 이 인과관계의 증명은 오랜 기간 동안 연구 결과물로서 인과관계를 증명하는 것은 생각만큼 쉽지는 않다. 상관관계를 인과관계로 오인하는 순간 무더운 여름밤에 선풍기는 반드시 꺼야 하고 익사자의 숫자를 줄이기 위해서는 켄터키주의 혼인율을 일정수준 이하로 통제해야 한다는 결론에 도달할 것이다.

세 번째로 언급할 내용은 “평균으로 회귀” 현상이다. 체벌신봉론자인 교사가 성적이 좋은 학생들을 칭찬하니 대부분 다음에 성적이 하락하고 성적이 나쁜 학생에게 체벌을 가하니까 대부분 성적이 올랐기 때문에 체벌이 교육에 필수적이라고 주장한다고 하자. 하지만 이 현상은 “평균으로 회귀”로 설명할 수 있다. 즉 체벌과 칭찬이 없었더라도 이런 현상이 일반적으로 일어나는 현상이다. 흔히 스포츠계에서 말하는 2년생 징크스, 혹은 금융상품도 당해 성적이 좋은 경우 다음 해에 대부분 곤두박질하는 것을 종종 보게 된다. 이런 현상도 역시 “평균으로 회귀”로 설명할 수 있다. “평균으로 회귀”가 생기는 이유는 다음과 같이 설명할 수 있다. 시험점수의 평균이 80점인 모집단에서 90점을 받은 학생이 10명이 있다면 이 학생들의 진짜 실력은 90점 미만인데 운 좋게 시험점수를 잘 받은 경우와 90 이상인데 시험을 못 본 경우로 생각할 수 있다. 모집단의 평균이 80점이라면 대부분의 경우는 운이 좋은 경우로 생각할 수 있다. 만약 시험을 다시 한번 본다면 운이 좋았던 학생들은 원래의 실력이 드러나는 경우가 많을 것이므로 대부분 점수가 하락하게 된다. 반대로 70점을 받은 학생들 10명을 대상으로 다시 시험을 본다면 여기서는 운이 나빠서 시험을 못 본 학생들이 많을 것이기 때문에 두 번째

시험에서 성적이 향상되는 것이다. 실제로 체벌효과가 있는지를 알아보기 위해서는 모든 학생에게 체벌을 행한 후 성적의 변화를 살펴보면 된다. 비슷한 예를 교통사고가 많이 나는 곳에만 교통단속 카메라를 달 경우 교통단속 카메라의 영향력을 과대평가한다는 연구결과가 있다. 전년도 교통사고 건수에 관계없이 임의로 교통단속 카메라를 설치한 결과 카메라의 사고방지 능력은 앞의 경우와 비교해서 1/3로 줄어들었다는 것이 연구진의 결론이었다.

마지막으로 “심슨의 역설”에 관한 설명을 하고자 한다. 사실 모든 경제 현상은 한가지 요인으로 설명할 수 없으며 여러 가지 요인이 관련되어 있다. 문제는 특정 요인을 고려하지 않을 경우 우리가 일어나고 있는 현상을 제대로 직시할 수 없다는 점이다. 다음과 같은 예를 생각해 보자. 하승진 선수는 3점 슛을 50개 시도해서 20개를 성공했고 양동근 선수의 경우 54개를 시도해서 22개를 성공했다고 하자. 이 경우 하승진 선수의 3점슛 성공률은 40%, 양동근 선수의 경우 41%이다. 2점슛의 경우 하승진 선수는 64개 중 31개를 성공해서 48%의 성공률을 보였고 양동근 선수는 39개를 시도해서 19개를 성공하여 49%의 성공률을 보였다고 하자. 여기서 놀라운 사실은 전체 슛 성공률은 하승진 선수가 114개 시도 중 51개를 성공해서 45%, 양동근 선수가 93개 시도 중 41개를 성공해서 44%이기 때문에 하승진 선수가 슛 성공률이 앞선다는 점이다. 이런 결과가 나온 이유는 하승진 선수는 상대적으로 슛 성공률이 높은 2점슛을 많이 던졌기 때문에 전체슛 성공률이 높게 나왔다. 비슷한 현상으로 미세먼지와 사망률 간의 관계는 음의 관계로 나타나는 것으로 보이지만 계절별로 미세먼지와 사망률 간의 관계를 구할 경우 양의 관계로 나타나는 것을 볼 수 있다. 즉 여기서 우리가 주의할 점은 모든 현상을 단지 2가지 변수 사이의 관계로 파악할 경우 실제 일어나는 현상과 정반대의 결론을 내릴 수 있다는 것이다. 진실은 양동근 선수가 슛이 보다 정확하고 미세먼지는 건강에 나쁜 영향을 미치지만, 단순히 전체 슛성공률만 고려한다면 사망률과 미세먼지와의 관계만을 살펴본다면 엉뚱한 결론을 내릴 수 있다. 우리가 관측하는 수많은 경제 현상도 하나의 단면으로만 본다면 실체를 파악할 수 없다.

“세상에는 3가지 종류의 거짓말이 있다. 거짓말, 새빨간 거짓말 그리고 통계”(lies, damned lies and statistics)라는 말은 우리에게 톰소여의 모험으로 익숙한 마크 트웨인이 만든 명언으로 알려져 있다. 하지만 이 명언의 원저자는 마크 트웨인이 아니다. 일설에 의하면 19세기 영국의 정치가이자 작가로서 수상에 오른 벤저민 디즈레일리가 말했다고도 알려져 있지만, 정답은 무명씨, 즉 원 저자가 누구인지는 알지 못한다. 사실 통계는 거짓말을 하지 않는다, 다만 이해한 만큼 보인다는 것을 명심해야 할 것이다. 건강검진에서 영양 관리에 관해 물어보는 질문에서 하루 과일 섭취량을 물어보는 질문을 바나나와 파인애플이 그려진 그림으로 대체했더니 본인은 파인애플을 매일 먹지 않는다고 이해하는 경우가 종종 있었다고 한다. 데이터 시각화를 하는 것도 중요하지만 주어진 정보를 이해할 수 있는 디지털 문해력을 배양하는 것이 이에 못지않게 중요하다는 얘기를 하고 싶다.

디지털 문해력은 현대 사회에 필수적인 데이터 기반 의사 결정을 위해 필수적으로 알아야 할 지식이며 결코 AI가 대신해줄 수 있는 것이 아니다. 그렇다면 이런 디지털 문해력을 갖추기 위해서는 어떤 노력을 해야 할까? 안타깝지만 디지털 문해력을 키우는 속성과정은 없다. 잠깐 주제를 바꾸어서 요즘 필자가 읽고 있는 레미제라블 원저에 관해서 얘기하고자 한다. 어릴 때 ‘장 발장’이라는 청소년용 축약판을 읽은 적은 있지만 원저에 대한 호기심에 5권 전집을 읽어보는 중인데, 첫 권에서 장발장은 백 페이지를 넘어서야 등장하고 자베르 경감은 3백 페이지가 되도록 등장하지 않고 있다. 하지만 다소 지루해 보이는 이런 부분을 넘어가면 원저가 주는 감동을 느낄 수 있듯이 디지털 문해력도 꾸준한 관련 서적 학습을 통해 이루어질 수 있을 것이다. 다행히 요즘 다양하고 재미있는 디지털 문해력 관련 서적들이 출간되어 있기 때문에 쉽게 관련 서적을 찾을 수 있을 것이다. 넷플릭스에서 잠깐 눈을 돌려 이러한 서적을 읽어보기를 권한다.



e-Finance and Financial Security

_02

Research

오픈소스 SW 공급망 공격 대응기술 동향

이희조, 고려대학교 컴퓨터학과 교수

블록체인 가상자산 관리의 보안성 강화를 위한 다자간

보안컴퓨팅 기술 동향

배경일, 아톰릭스랩 공동설립자

전기통신금융사기 최신 동향 및 피해사례 분석

프레임워크 소개

정영훈, 금융보안원 금융보안관제센터 대리



오픈소스 SW 공급망 공격 대응기술 동향

이희조*

I	서론	13
II	오픈소스 SW 공급망 공격 동향	14
	1. 오픈소스 활용 현황	14
	2. 공급망 공격 유형	15
	3. 오픈소스 보안 취약점	18
	4. 오픈소스 라이선스 위반	21
III	공급망 보안 강화방안	22
	1. 오픈소스 신뢰도 판단 기준	22
	2. SBoM 부품명세서 관리	23
	3. 오픈소스 컴포넌트 식별	25
	4. CVE 취약점 관리	27
IV	결론	29
	〈참고문헌〉	29

* 고려대학교 컴퓨터학과 교수, heejo@korea.ac.kr



요 약

오픈소스를 활용하는 것은 비단 개발 시간을 단축하는 것만이 아니라, 혁신 기술을 채용함으로써 경쟁력 있는 서비스를 개발하는데 매우 중요한 요소가 되었다. 하지만, 오픈소스는 잘 사용하지 않으면 라이선스 위반으로 인한 법적 위협뿐 아니라 보안취약점으로 인한 공격, 그리고 다양한 공급망 공격으로 인해 되돌릴 수 없는 치명적인 결과가 초래될 수 있다. 본 고에서는 최근에 급증하고 있는 오픈소스 공급망 공격 동향을 살피고, 공급망 보안 강화를 위한 오픈소스 신뢰도 판단 방법, 개발 및 유통과정에 소프트웨어 부품명세서인SBoM활용, CVE와 같이 치명적 취약점 패치여부 확인 등 오픈소스를 안전하게 활용하기 위한 대응 방안을 소개한다.

01

오픈소스 SW 공급망 공격 대응기술 동향

I 서론

“내가 더 멀리 보았다면 이는 거인들의 어깨 위에 서 있었기 때문이다.”

- 아이작 뉴턴

오픈소스를 활용하는 것을 종종 거인의 어깨에 서는 것으로 비유되고 있듯이, 경쟁력 있는 서비스를 개발하는데 오픈소스를 이용하는 것은 자연스러운 현상이 되었다. 이는 비단 개발시간을 단축시켜 경쟁업체보다 빨리 서비스를 개발하는 것뿐 아니라 혁신기술을 채용할 수 있게 하고, 더 높은 품질의 코드를 개발하게 하여 기술 경쟁력을 높이는데도 중요한 역할을 하기 때문이다.

하지만, 오픈소스를 활용하는데 있어서 주의를 기울이지 않으면 여러 문제가 발생할 수 있으며, 이러한 원인으로는 아래의 인식 오류로부터 기인하고 있다.

“오픈소스는 공짜 소프트웨어이다.”

“최신 버전 오픈소스는 보안취약점 패치가 되어 있어 안전하다.”

“많은 사람들이 사용하는 오픈소스가 더 보안 수준이 높다.”

오픈소스는 공짜가 아니고 라이선스를 준수하여야 한다. 또한, 최신 버전이라도 또 다른 오픈소스를 가져다 사용하는 경우 서브 컴포넌트는 업데이트 되지 않는 경우가 종종 발생하고 있어 서브 컴포넌트 업데이트 주기가 신뢰도 평가에 중요한 요소가 된다. 또한, 많이 사용하는 유명 오픈소스들에서도 치명적인 취약점들이 계속 발견되고 있어서 보안 취약점 동향을 파악하여 적극적인 보안관리를 하지 않으면 큰 피해를 입을 수 있다.

본 고에서는 오픈소스를 선택하고 사용하는데 있어서 법적, 기술적 위험관리의 필요성과 대응기술의 동향을 파악하여 효과적이며 안전하게 오픈소스를 활용하기 위한 방안에 대해 논의한다.

II 오픈소스 SW 공급망 공격 동향

1. 오픈소스 활용 현황

오픈소스의 활용은 IT산업 외에도 여러 산업분야에 AI, IoT, 빅데이터 적용이 확대되면서 급격하게 증가하고 있으며, 이는 다양한 통계에서도 이를 반영하고 있다. 오픈소스 저장소 깃허브는 2021년 10월 현재 2억개 이상의 프로젝트의 저장소로 사용이 되고 있고, 6천5백만명 이상의 개발자가 활동하고 있으며, 3백만개 이상의 회사와 조직이 이용하고 있다. 또한, 2021년 현재 Java, JavaScript, Python, .NET 4개 언어로 된 오픈소스 배포에 이용되는 패키지 매니저 Maven, npm, PyPi, NuGet에 등록된 오픈소스만 해도 1년전에 비해 20% 증가한 3천7백만 여개의 소프트웨어가 등록되어 있고, 다운로드 횟수는 전년도에 비해 73%나 증가하였다[1]. 또한, 상용 포함 소프트웨어의 98%가 오픈소스를 활용하고, 코드의 75% 이상이 오픈소스로 구성이 되어있다[2]. 또한, 소프트웨어의 84%에서 하나 이상의 보안 취약점이 발견되었으며, 65%의 경우는 라이선스 충돌이 발견되었다.

그림에서와 같이 깃허브에서 C/C++ 프로젝트 중에 포크횟수 기반으로 상위 10개의 프로젝트를 보면, 인공지능에 활용되는 구글 Tensorflow, 리눅스 커널, 비트코인 등은 원본 소스가 복사되어 이미 각각이 수만 개의 새로운 프로젝트에서 새로운 이름으로 개발이 진행되고 있음을 알 수 있다.

그림 1 깃허브 C/C++ 상위 10개 프로젝트의 포크횟수, CSSA, 2021년 10월

Rank	Project Name	Forks	Area
1	Tensorflow	86 K	AI
2	OpenCV	48 K	AI
3	Linux	39 K	IoT
4	Bitcoin	30 K	Blockchain
5	Git	22 K	OSS
6	Redis	20 K	DB
7	Darknet	18 K	DB
8	Pytorch	14 K	AI
9	Electron	13 K	Web
10	Arduino	12 K	IoT

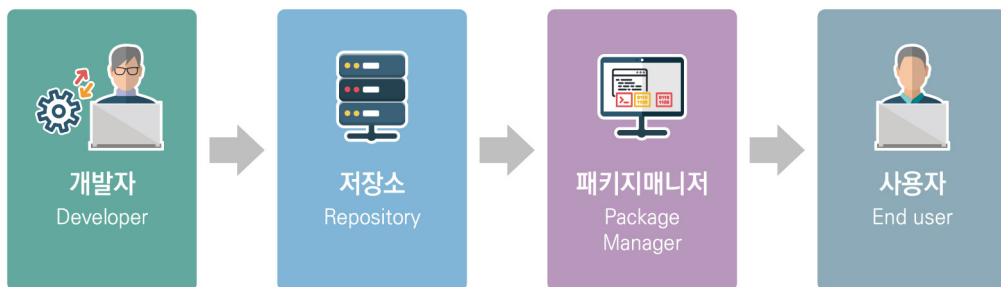
2. 공급망 공격 유형

소프트웨어 공급망(Supply Chain)은 소프트웨어가 개발자에 의해 개발된 후 사용자에게 도달하기까지 여러 단계로 구성된다. 개발자의 개발 환경부터 소스 코드 저장소, 최종 소프트웨어가 배포되는 플랫폼까지 포함될 수 있으며, 이러한 공급망은 각 소프트웨어를 개발하는 오픈소스 커뮤니티와 개발사, 그리고 소프트웨어 특성에 따라 달라질 수 있다. 특히, 오픈소스의 경우 재사용 빈도가 높아 사유 소프트웨어에 비해 공급망이 더 길어질 수 있으며, 상호 재사용으로 인해 복잡한 의존성을 가지고 있는 경우 또한 빈번하게 발생하고 있다.

이를 일반화하여 표현하면 오픈소스 공급망은 [그림 2]와 같이 개발자, 저장소,

패키지 매니저, 사용자 네 단계로 구성되고 있다. IoT 기기를 이용한 금융 서비스의 경우는 공급망이 더욱 길어질 수 있어서, [그림 2]의 사용자 부분이 제조사, 서비스 제공자, 사용자로 6단계로 구성 된다. 공급망의 각 단계는 공격 목표지점이 될 수 있으며, 모든 단계의 보호가 되지 않으면 공격이 가능해진다. 이는, 생태계의 상호 의존성을 보여주는 것으로, 금융기관은 솔루션이나 기기를 공급받는 제조사뿐 아니라 오픈소스 생태계의 보안관리 체계에도 관심을 기울여야 하는 이유가 되고 있다.

그림 2 오픈소스 공급망의 4단계 구성



2015년 이후 2021년 현재까지의 공급망 공격에 사용된 기법을 분류하여 보면, 공급망 단계별로 상이한 공격 형태 및 다양한 공격기법이 존재함을 알 수 있다. 오픈소스 공급망의 주요 단계에 관련된 대상 시스템으로는 개발서버, 저장소, 패키지 관리자가 있으며, 단계별 공격 유형은 아래와 같이 9개 유형을 포함하게 된다.

2021년 공급망 공격이 급증하고 있어서, 전년도에 비하여 650% 증가하였다[1]. 공급망 공격의 예로는 2020년 말 보고된 솔라윈즈 공격 외에도 2021년 7월 발생한 카세야 랜섬웨어 공격도 공급망 공격의 사례라 볼 수 있다. 최근 통계로 보면 3.1 의존성 혼돈공격과 3.2 타이포스쿼팅 공격과 같이 네임스페이스 공격 유형이 가장 자주 발생하고 있다.

그림 3 공급망 주요 단계의 해당 시스템에 대한 공격 유형

공급망 단계		공격 유형		공격 사례
1	개발 서버	1.1	서버 침투 및 악성코드 삽입	SolarWinds(2020-2021), Codecov(2021), Kaseya(2021)
		1.2	프로젝트 파일 대상 악성코드 배포	Octopus Scanner(2020), rest-client(2019)
		1.3	악성 IDE 배포	Xcode Repackaging(2015)
2	저장소	2.1	오편 패키지 탈취 (Orphan Package Takeover)	Arch User Repository takeover(2018)
		2.2	계정 탈취	Sawfish phishing campaign(2020)
3	패키지 매니저	3.1	의존성 혼동 (Dependency Confusion)	Alex Birsan's Research(2020-2021)
		3.2	타이포스퀀팅 공격 (Typo-squatting Attack)	Electron(2020), atlas-client(2020)
		3.3	악성 패키지 배포	1337qq-js(2020)
		3.4	계정 탈취	RubyGems-strong_password(2019)

의존성 혼동(dependency confusion) 공격이란 정상 소프트웨어의 이름과 동일한 이름의 새로운 버전 소프트웨어를 공급망에서 배포하도록 하는 공격으로, 자동화된 빌드 도구들이 다운로드 하도록 하거나 자동 업데이트로 인해 악성코드 전파 속도가 높아지는 경우이다. Alex Birsan은 2021년 2월 기업이 개별적으로 사용하는 패키지 이름과 동일한 이름을 공개 패키지 관리자 사이트에 등록하는 방식으로 페이팔(Paypal), 애플(Apple), 쇼피파이(Shopify), 넷플릭스(Netflix), 우버(Uber), 옐프(Yelp) 등 35곳이 넘는 기업을 손쉽게 공격이 가능함을 보였다[10].

타이포스퀀팅(typo-squatting) 공격은 정상 패키지와 유사한 이름의 패키지를 등록하여 사용자로 하여금 악성 패키지를 다운받아 사용하게 하는 경우를 말한다. 2020년 RubyGems 패키지 매니저에 700개의 악성 타이포스퀀팅 패키지가 발견이 되었으며, 예를 들면 acpc_poker_types라는 이름의 정상 패키지를 노린 acpc-poker_types라는 이름의 악성 패키지를 등록한 사례가 이에 해당한다.

공급망 공격은 한번의 공격으로 다수의 소프트웨어에 영향을 끼치고, 더 나아가 공격 대상 패키지에 의존하는 소프트웨어와 이를 사용하는 사용자까지 공격하는 증폭 효과를 가지고 있어, 치명적인 결과를 초래할 수 있게 된다. 또한, 오픈소스는 특성상 전세계 개발자 누구라도 참여하여 개발과 공유를 장려하고 있으므로,

악의적인 사용자 또한 공급망에 쉽게 접근이 가능하기 때문에, 공격은 쉽고 효과는 높아 공급망 공격은 점점 증가하는 추세에 있다. 이에 따라 소프트웨어의 공급망 보안의 중요성이 높아지고 있으며, 공급망 보안관리를 제도화하는 움직임이 국가별, 산업별로 증가되고 있다.

3. 오픈소스 보안 취약점

“보는 눈이 많다면 어떤 버그도 쉽게 잡을 수 있다.” - 리누스 법칙

오픈소스는 많은 사람들이 공개적으로 사용하고 이에 따라 보안 문제가 발생하면 바로 발견하여 해결할 수 있으므로 보안성이 높다는 주장이 리눅스 개발자의 이름을 따서 “리누스 법칙”이라 한다. 하지만, 모든 오픈소스가 이에 해당하지는 않아서 오픈소스라는 것만으로 안전이 담보되지는 못한다. 따라서, 오픈소스를 사용할 때는 오픈소스의 선정 및 평가, 그리고 사용하는 모든 라이프사이클에서 새로운 취약점에 노출되지는 않는지 정기적 보안 관리가 필요하게 된다.

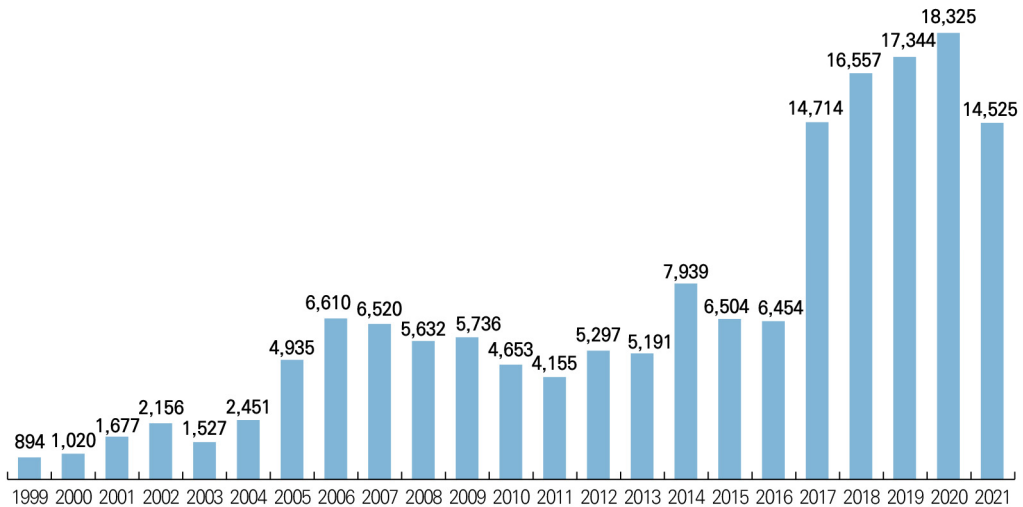
국제표준 취약점 식별번호로 사용되는 CVE(Common Vulnerabilities and Exposures)의 경우 2021년 9월 현재 16만개의 취약점을 공개하고 있으며, 하루 평균 50개의 신규 취약점이 발견되고 있다.¹⁾ 연도별 취약점 추이는 아래 [그림 4]에서 보여지고 있으며, 최근 5년간 신규 취약점이 그 이전에 비해 2배 이상 증가하였고, 매년 더 증가하는 추세를 보이고 있다.

CVE 취약점은 금융서비스의 공격에도 이용이 되고 있어서, 2014년 HeartBleed 취약점을 이용해 SSL/TLS로 보호되는 웹 또는 VPN 서비스에 대한 공격 등 많은 사례가 포함된다. 또한 최근에는 다양한 기기에서 사용중인 4개의 오픈소스 TCP/IP 스택에서 Namewreck 취약점이 발견되어 전세계 적으로 1억대 가량 기기가 공격에 노출이 되었고, 2021년 4월에 마이크로소프트에서 발견한 BadAlloc 취약점은 임베디드 기기와 산업용 OT기기에서도 많이 사용하는 다수의

1) <https://cve.mitre.org>

RTOS 에서 25개의 취약점이 발견된 경우이다. 이처럼 매일 발견되어 공개되는 취약점들은 금융서비스에 위협이 되는 사항으로 서비스에 영향을 끼치는지 동향 파악 및 관리가 필요하다.

그림 4 새롭게 공개되고 있는 CVE 취약점 연도별 트렌드

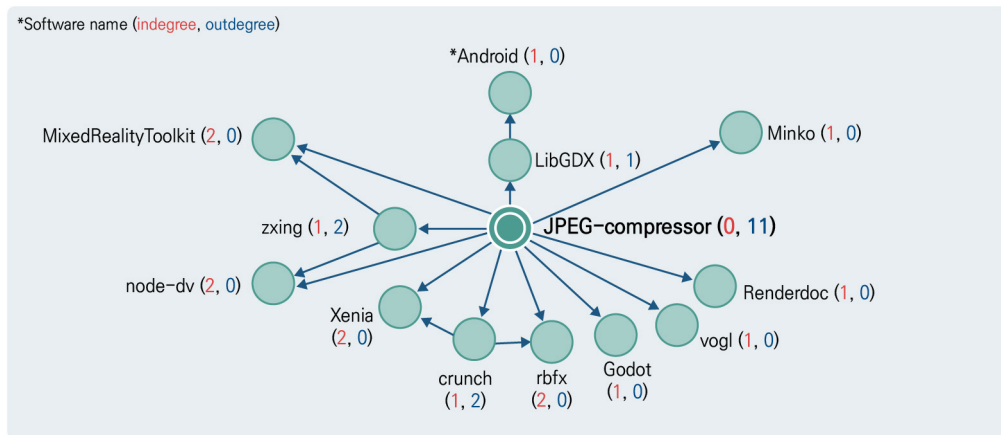


고려대 소프트웨어보안연구소(CSSA)²⁾의 최근 연구에 의하면, 많은 보안 기술 및 솔루션에서 사용하고 있는 CVE 정보의 2%는 취약한 소프트웨어에 대한 정보가 잘못되어 보안 패치 등 대처가 늦어지고 있음이 발견되었다[11]. 의학계에서 전염병의 첫 번째 감염자를 탐지하는 것은 광범위한 확산을 방지하기 위해 매우 중요한 요인이 된다. 마찬가지로, 소프트웨어 보안취약점의 최초 근원지를 정확하게 탐지하는 것이 전파된 취약점 조기 탐지에 큰 영향을 미친다는 점에 착안하여 자동화된 방식으로 정확하게 취약점의 최초 근원지, 즉 취약점이 최초로 발생한 지점을 의미하는 ‘Vulnerability Zero’를 탐지하는 기술을 개발했다. 취약점의 올바른 최초 근원지가 제공되는 경우, 해당 CVE취약점을 평균 6개월 이내에 패치가 되고 있었던 반면, 근원지가 잘못된 CVE의 경우 해당 취약점이 있는 오픈소스를

2) <https://cssa.korea.ac.kr>

사용 중인 소프트웨어는 2년이 넘어도 패치 되지 않고 지연되고 있음을 확인할 수 있었다[4].

그림 5 JPEG 취약점이 Android로 보고된 CVE의 타 오픈소스로의 취약점 전파경로



[그림 5]에서는 JPEG 취약점이 Android 취약점으로 등록이 되어있는 CVE-2017-0700 취약점이 다른 오픈소스에도 전파된 상황을 보여준다. 즉, JPEG-compressor를 사용하는 LibGDX, Godot 등은 취약한지를 알 수 없고 패치도 지연되고 있는 반면, 구글이 관리하는 Android만 빨리 패치가 가능했던 경우이다. 이는 구글처럼 많은 예산과 자원을 들여 적극적으로 취약점 관리를 하고 버그바운티도 운영하는 경우 더 많은 취약점 정보가 흘러가고, 반면 취약점 관리를 하지 않는 쪽은 취약점이 발견된지도 모르고 있어 해커의 공격으로 더 큰 피해를 입게 됨을 보여준다.

따라서 제품이나 서비스에서 발견되는 취약점 정보를 받아들일 수 있는 취약점 관리 체계를 운영하는 것이 취약점 정보를 먼저 입수하여 대처 함으로서 고객의 피해를 줄일 수 있게 해준다는 것을 알 수 있다. 취약점 관리체계는 최근 국가별 법제도 및 산업별 표준으로 요구사항이 증가되고 있으며, 2021년 5월 미국의 사이버 보안 행정명령의 공급망 보안, ISO/IEC 29147:2018 취약점 신고 및 책임 공개

국제표준, UNECE WP.29 자동차보안 취약점관리체계 등이 이에 해당한다.

이러한 보안관리 체계는 표준 및 인증의 요구사항을 위한 것뿐만 아니라 담당 팀과 프로세스를 적립해 둠으로써 보안 문제에 대한 빠른 대처에도 큰 기여를 할 수 있게 한다. 2021년 7월 발생한 카세야 랜섬웨어 공격은 사건발생 3개월 전인 4월에 네덜란드 팀에서 신고한 7개 CVE 취약점 중 패치 개발이 지연되었던 하나의 CVE가 공격에 이용되어 발생한 사건이다. 결과적으로 고객의 고객사 1500여개 기관에 랜섬웨어가 배포되었고 800억의 몸값이 요구되었다. 이미 보고되었던 취약점을 패치 개발과 배포 등 대응이 지연되어 발생한 사건으로 취약점 신고 및 관리 체계의 중요성을 보여주고 있다. 보안취약점 관리를 위한 조직과 절차에 대해서는 국제표준인 ISO 29147을 참고하여 구축이 가능하다[15].

4. 오픈소스 라이선스 위반

오픈소스는 공짜 소프트웨어가 아니고, 라이선스에 정의된 규칙을 따라 사용 하여야 한다. 라이선스의 종류는 OSI(Open Source Initiative)에 의해 검증하여 SPDX 표현으로 공개한 것만 114개에 이르고 있으며, 보안취약점 자동분석 도구 중 하나인 아이오티큐브의 래브라도는 501개의 라이선스 유형을 관리하고 있다. 이중에 MIT, BSD, Apache등 보다 자유로운 라이선스도 있지만, GPL(GNU General Public License)처럼 카피레프트 철학이 반영이 되어있는 라이선스도 존재한다. 대표적인 사례인 리눅스 커널은 GPLv2를 따르고 있고, 이를 이용하는 Android, Tizen, WebOS등의 운영체제와 이를 기반으로 개발된 스마트기기 또한 변경한 소스코드를 오픈소스로 공개해야 하는 의무가 부과된다.

오픈소스 라이선스 위반으로 인한 소송이 구글, 마이크로소프트, 시스코, IBM 등의 글로벌 기업뿐 아니라 한글과컴퓨터 등 국내 기업을 대상으로도 증가하고 있다[8]. 국내의 기업에서는 법무팀의 대응이 선제적으로 이뤄지고 있으나, 오픈소스는 법적인 이슈 외에도 보안 이슈가 점차 증가하고 있어 법무팀과 보안팀이 함께 효과적인 관리체계를 구축해 나갈 필요가 있다.

공개 취약점 정보의 불완전성과 매일같이 찾아지는 취약점 정보 홍수 속에서도 안전한 공급망 관리와 서비스 제공을 위해서는 오픈소스의 목록관리 및 보안성 검증, 업데이트 필요시 즉각적인 실행 체계 구축 등을 위한 오픈소스 거버넌스 체계의 구축이 시급하다.

III 공급망 보안 강화방안

1. 오픈소스 신뢰도 판단 기준

어떤 오픈소스를 사용할 것인가를 판단하는 기준은 여러 가지가 제시되고 있다. 앞서 소개한 바와 같이 포크 횟수나 스타 개수 또는 참여 개발자의 수처럼 인기 순위(popularity) 기반의 척도, 또한 얼마나 자주 업데이트를 하고 새로운 버전을 배포하는지 활동중심의 척도(activity), 그리고 버전관리와 문서작성 등의 성숙도(maturity) 기반의 척도 등 다양한 방식이 제안되고 있다[1]. 하지만, 오픈소스의 보안 측면에서 가장 중요하게 보아야 할 것은 “업데이트 빈도”를 빼놓을 수 없다.

다음은 고려대 CSSA에서 깃허브의 스타 갯수 기준으로 최상위 오픈소스 2000개를 아이오티큐브³⁾ 취약점 자동분석 플랫폼을 이용하여 분석했을때, 유명 오픈소스의 최신버전임에도 불구하고 15%에서는 알려진 CVE 취약점의 패치가 이뤄지지 않은 것을 확인할 수 있었다[5].

이는 오픈소스는 또 다른 오픈소스를 이용하여 개발을 하게 되는데, 내부에 있는 서브 컴포넌트가 업데이트 되지 않아서 발생하고 있다. 즉, 오픈소스가 최신 버전이라고 하여도 내부에 사용 중인 또 다른 오픈소스 컴포넌트는 최신 버전이 아닌 경우로, 적게는 3개월전 버전에서부터 길게는 10년전 버전의 컴포넌트가 사용 중임을 알 수 있었다[5,12].

3) IoTcube 퍼블릭 플랫폼은 <https://iotcube.net> 을 통해 전세계 누구라도 무료로 사용이 가능하다.

이와 같이 오픈소스의 최신버전이라도 서브 컴포넌트의 업데이트가 되지 않으므로써 보안 취약점에 노출될 수 있고, 이에 따라 최상위 소프트웨어뿐만 아니라 서브 컴포넌트에서 사용 중인 소프트웨어도 관리를 해야 하는 것을 나타내고 있다.

그림 6

C와 C++ 언어로 구성된 최신버전 오픈소스에서 CVE 취약점이 발견된 오픈소스 목록, CSSA 2020

Name	# CVE	Area	Name	# CVE	Area
Emscripten	15	Compiler	FFmpeg	15	Media
Turicreate	14	AI	kbengine	14	Game
Godot	10	Game	Linux	13	OS
Mongo	2	Database	RaspberryPi	13	OS
ArangoDB	2	Database	Freebsd	7	OS
OpenCV	1	Vision	OpenSSL	2	Security

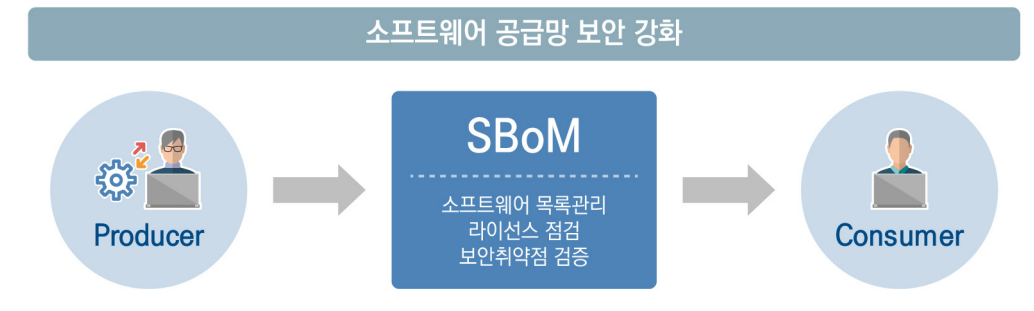
이에 따라, 오픈소스의 신뢰도 평가 척도는 서브컴포넌트를 포함한 업데이트 주기를 중심으로 해야 한다는 주장과 일치하는 결과를 보이고 있다.

2. SBoM 부품명세서 관리

소프트웨어 공급망 보안의 첫걸음은 사용중인 소프트웨어의 구성요소를 파악하는 것에서 시작할 수 있다[6]. 즉, 해당 제품이 어떤 소프트웨어의 어떤 버전들로 구성이 된 것인지를 나타내며(a “list of ingredients” in software) 이 정보를 소프트웨어 명세서, 혹은 SBoM(Software Bill of Materials)이라고 쓰고 “에스봄”이라 읽는다. IoT 기기와 금융을 포함하는 스마트 서비스, 그리고 다양한 기기가 복잡하게 운영되는 스마트 공장 및 자동차 등에서 SBoM을 파악하고 있으면,

라이선스 위반여부 및 새로 발견되어 보고된 취약점에 해당이 되는지 즉시 파악하여 대처함으로써 피해를 최소화할 수 있게 된다[9].

그림 7 SBoM을 활용한 소프트웨어 공급망 보안 강화



이에 따라, 미국에서는 2021년 5월 바이든 대통령의 행정명령으로 공급망 보안을 위한 SBoM 제공 의무화를 추진하고 있으며, 헬스케어 등 IoT 서비스에 시범 적용한 경험을 바탕으로 사이버보안 수준의 획기적 향상을 기대하고 있다.

제품에 포함된 상용 및 오픈소스 소프트웨어 컴포넌트 정보 등 소프트웨어 재료 명세서로서 SPDX, CycloneDX, SWID 등이 대표적인 표준이다. 소프트웨어 구성 요소 및 이들 간의 공급망 관계를 나열하고 식별하는 소프트웨어 재료 명세서로서 이름, 버전정보 외에 공급망 정보를 포함하고 있어서, 라이선스 등의 컴플라이언스 준수 여부뿐 아니라, 취약점 발견시 해당 소프트웨어에 취약점 존재 여부를 빠르게 파악하여 패치 시간을 급격히 단축하게 하는 등 보안 관리를 용이하게 한다. 특히, 부품업체가 상위 제품 생산자에게 납품할 때뿐 아니라 제품을 이용한 서비스를 고객이 도입할 때, 그리고 정기적으로도 새롭게 발견된 취약점을 손쉽게 확인이 가능함으로써 보안 문제점의 파악 및 해결을 도와주게 한다.

그림 8

자체 코드와 오픈소스, 외부 라이브러리를 부분별로 시각화한 소프트웨어 맵과 SBoM 제공사례



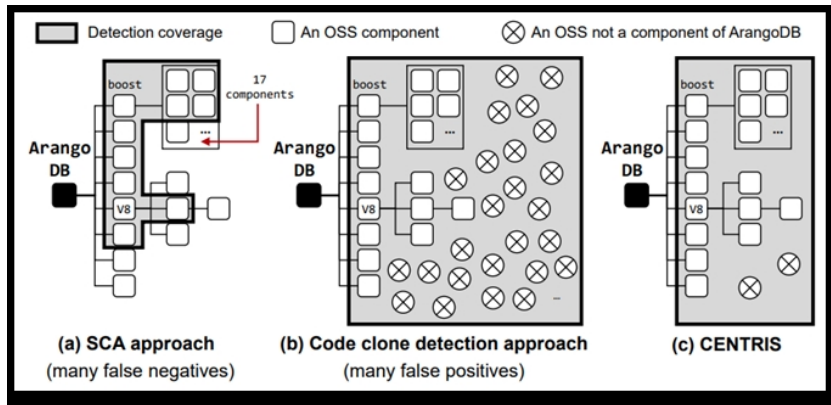
3. 오픈소스 컴포넌트 식별

오픈소스 소프트웨어는 재사용 되는 과정에서 원본 구조 및 코드가 수정되는 경우가 잦다. 고려대 CSSA에서 수행한 연구에 의하면 자주 사용되는 유명한 오픈소스 소프트웨어들의 95%는 코드 혹은 구조 수정과 함께 재사용되고 있다[12]. 기존의 알고리즘은 5%의 수정 안된 오픈소스는 정확히 탐지하지만, 95%에 이르는 수정된 오픈소스가 포함된 소프트웨어에서는 오탐이 많아 탐지 정확도가 10%에 그친다는 것을 알 수 있었다. 반면 코드 분할 및 중복 제거 알고리즘을 기반으로 동작하는 Centris는 수정된 오픈소스 구성요소가 포함되어 있어도 90% 이상의 정확도로 빠르고 정확하게 식별해 낼 수 있다[3].

[그림 8]은 오픈소스인 ArangoDB에 존재하는 17개의 서브 컴포넌트에 대해 기존 방식들과 Centris의 탐지 결과를 비교하여 보여주고 있다. 기존 SCA방식으로는 정상적인 컴포넌트를 못찾는 미탐이 많이 발생하고, 코드클론 탐지방식으로는 일부 코드만보고 해당 컴포넌트가 있다는 결과를 보고하면서 많은 오탐이 발생하게 된다. 이에 반하여 Centris는 17개의 컴포넌트를 모두 찾아주고 오탐도

현저히 작은 수준임을 보여주고 있다.

그림 9 ArangoDB 분석 결과 타 방식에 비해 월등히 높은 Centris 정확도



[그림 9]는 오픈소스인 ArangoDB에 존재하는 17개의 서브 컴포넌트에 대해 기존 방식들과 Centris의 탐지 결과를 비교하여 보여주고 있다. 기존 SCA방식으로는 정상적인 컴포넌트를 못찾는 미탐이 많이 발생하고, 코드클론 탐지방식으로는 일부 코드만보고 해당 컴포넌트가 있다는 결과를 보고하면서 많은 오탐이 발생하게 된다. 이에 반하여 Centris는 17개의 컴포넌트를 모두 찾아주고 오탐도 현저히 작은 수준임을 보여주고 있다.

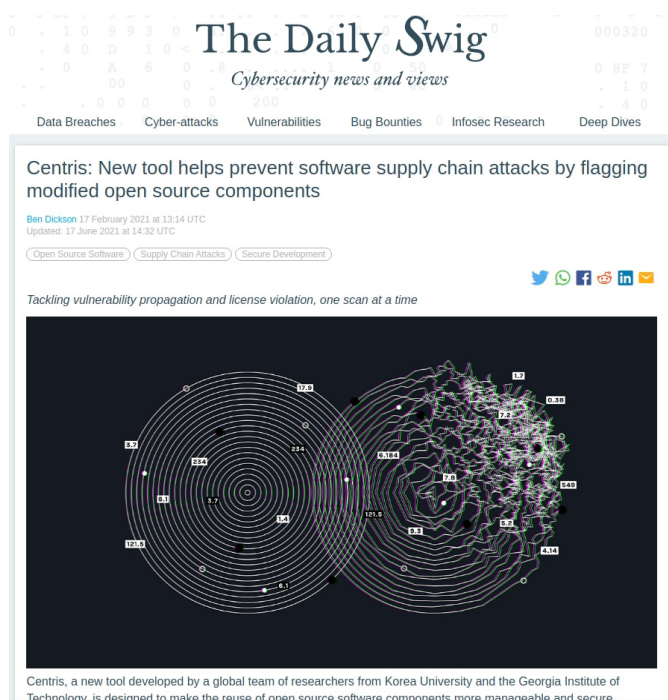
Centris는 소프트웨어 원심분리기(Centrifuse of Software)의 의미를 가지고 있으며, 아이오티큐브 퍼블릭 플랫폼을 이용해 공개가 되었으며,⁴⁾ 래브라도⁵⁾에도 적용이 되어 기업에서도 개발 또는 검수단계에 오픈소스 소프트웨어 구성요소를 정확하게 식별하고 SBoM을 관리하는 용도로도 사용할 수 있다. [그림 10]에서는 오픈소스가 재사용 빈도가 높아지면서 취약점의 전파경로로 사용될 수 있으며, Centris를 이용하여 수정하여 재사용하는 경우라도 서브 컴포넌트를 정확히 식별하여 공급망 보안을 높일 수 있다는 내용을 소개하고 있다.

4) <https://iotcube.net/centris>

5) <https://labrador.iotcube.com>

그림 10

소프트웨어 공급망 보안에 Centris가 효과적으로 활용될 수 있음을 소개, The Daily Swig 2021년 6월 17일



4. CVE 취약점 관리

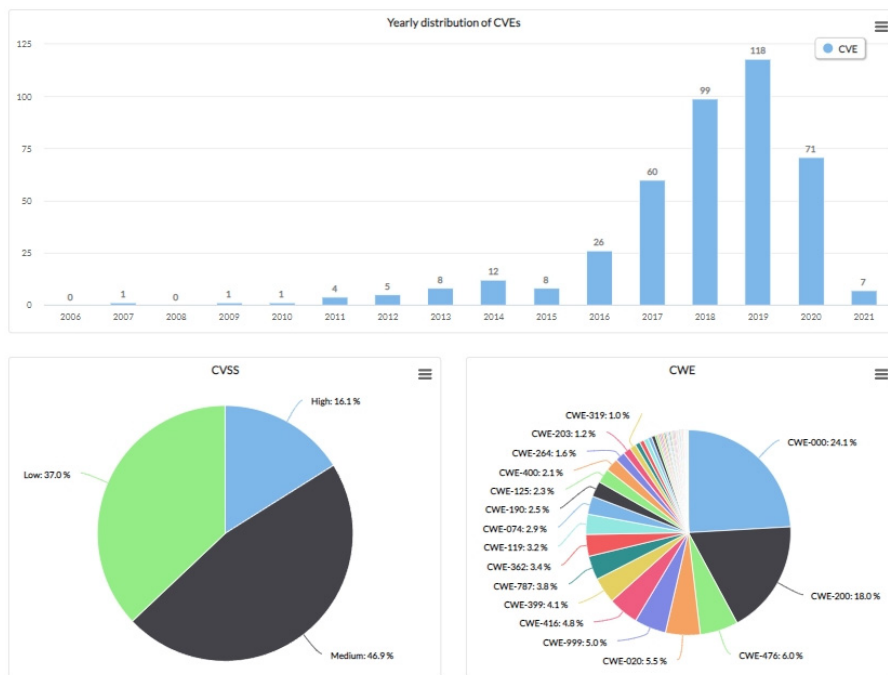
해킹 공격의 90%는 소프트웨어 취약점을 이용한 공격이라는 US-CERT 보고가 있듯이, 치명적인 취약점을 패치 업데이트하는 것은 보안의 매우 중요한 요소이다. 하지만, 소프트웨어의 취약점이 존재하는지 여부는 공급망 최상단에 있는 소프트웨어 또는 제품 명으로는 구분할 수 없다. 예를 들어, 삼성 갤럭시 스마트폰의 취약점은 삼성 갤럭시로 보고된 CVE 뿐만 아니라 안드로이드와 크로미움 브라우저 등 스마트폰에서 사용되는 SBoM 컴포넌트들 각각에 해당하는 CVE 취약점이 있는지를 확인하여야 한다.

아이오티큐브의 퍼블릭 버전을 이용하여 최신 스마트워치 펌웨어를 분석하였을 때, 3천8백만 라인으로 이뤄져 있는 코드에서 패치 되지 않은 CVE 취약점이 421개가 존재함을 알 수 있다. 이는 5년전에 릴리즈 된 Linux Kernel 4.9 버전을

사용하고 있는 부분에서 상당수 발견되는 것을 볼 수 있다.

패치가 되지 않은 코드가 반드시 보안 취약점으로 공격에 이용이 된다고 할 수는 없으나, PoC 익스플로잇까지 검증된 CVE이므로 익스플로잇의 가능성을 매우 높다. 따라서, 발견된 취약점 중에 심각도가 높은 취약점의 경우 대처가 필요하며, 버전 업그레이드뿐 아니라 백포팅(backporting) 기술을 적용함으로써 상위 호환성 문제를 없이 검증된 패치코드를 적용할 수 있다. 백포팅은 새로운 버전의 소프트웨어 또는 보안 패치를 낮은 버전에 포팅하는 것을 의미하며, 버전 업그레이드가 어려운 펌웨어나 오픈소스에도 적용이 가능한 해법이 된다.

그림 11 최신 스마트워치에서 오래된 오픈소스 컴포넌트 사용으로 인해 발견된 CVE 취약점 현황



IV 결 론

오픈소스의 활용은 경쟁력을 높여주지만 관리가 필요하다. 여기에는 공급망 보안을 위한 SBoM 리스트 관리, 라이선스 및 보안취약점 관리를 포함하게 된다. 안전하게 오픈소스를 사용하고 법적, 기술적 위험 관리를 위해서는 조직 및 프로세스를 미리 구축해 두어야 한다. 더불어 이와 같은 오픈소스 거버넌스 체계에서 꼭 필요한 것은 빠르고 정확하게 분석하고 새로운 정보를 업데이트 해주는데 도움을 주는 자동화된 오픈소스의 관리도구도 포함될 것이다. 하지만, 오픈소스 관리도구는 아주 강력하고 편리하지만 보조 도구로서 활용하고 최종 판단은 사용자가 하여야 할 것이다. 이를 위해서는 오픈소스 생태계의 특성인 높은 빈도의 재사용, 수정된 오픈소스 컴포넌트의 업데이트 지연, 그리고 소프트웨어 공급망을 통한 공격 등의 문제점을 인식하고 관련 기술과 도구를 활용하여 보안 관리를 해나갈 필요가 있다.



참고문헌

- [1] Sonatype, “2021 State of the Software Supply Chain,” Sep. 2021
- [2] Synopsys, “Open Source Security and Risk Analysis Report,” 2021
- [3] 보안뉴스, “오픈소스 커뮤니티 노리는 공급망 공격, 국내 연구팀 기술로 차단한다,” 2021년 3월 25일
- [4] ZDnet, “SW 취약점 최초 근원지 자동 탐색 기술 등장,” 2021년 9월 8일
- [5] 이희조, “오픈소스 소프트웨어 보안 취약점과 공급망 보안,” 한국정보보호학회 단기강좌, 2020년 11월
- [6] 이희조, “보안취약점 자동분석 플랫폼 IoTcube 소개”, 제5회 IoTcube 컨퍼런스, 2021년 8월
- [7] Open source licenses, OSI(Open Source Initiative), 2021
<https://opensource.org/licenses/alphabetical>

- [8] Open source license litigation, 2021, https://en.wikipedia.org/wiki/Open_source_license_litigation
- [9] 미국 NTIA, “Software Bill of Materials,” 2021, <https://ntia.gov/SBOM>
- [10] Alex Birsan, Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies The Story of a Novel Supply Chain Attack, 2021년 2월 10일, <https://medium.com/@alex.birsan/>
- [11] Seunghoon Woo, Dongwook Lee, Sunghan Park, Heejo Lee, Sven Dietrich, “V0Finder: Discovering the Correct Origin of Publicly Reported Software Vulnerabilities”, USENIX Security Symposium, Aug. 2021.
- [12] Seunghoon Woo, Sunghan Park, Seulbae Kim, Heejo Lee, Hakjoo Oh, “CENTRIS: A Precise and Scalable Approach for Identifying Modified Open-Source Software Reuse”, Int’l Conf. on Software Engineering(ICSE), May 2021.
- [13] Seulbae Kim, Heejo Lee, “Software systems at risk: an empirical study of cloned vulnerabilities in practice”, Computers & Security, Vol. 77, pp. 720-736, Aug. 2018.
- [14] Seulbae Kim, Seunghoon Woo, Heejo Lee, Hakjoo Oh, “VUDDY: A Scalable Approach for Vulnerable Code Clone Discovery”, IEEE Symposium on Security and Privacy, May. 22. 2017.
- [15] ISO/IEC JTC 1/SC 27, “Vulnerability disclosure”, ISO/IEC 29147:2018

블록체인 가상자산 관리의 보안성 강화를 위한 다자간 보안컴퓨팅 기술 동향

배경일*

I	블록체인 기술과 가상자산 시장 동향	33
II	블록체인 전자지갑의 핵심, 개인키	36
	1. 블록체인 전자지갑의 기능	36
	2. 블록체인의 개인키 체계	39
	3. 개인키 관리의 어려움	40
III	개인키 관리를 위한 암호학 발전 과정	42
	1. 샤미르 시크릿 셰어링	42
	2. 분산 키생성	43
IV	다자간 보안컴퓨팅 기술을 적용한 안전한 블록체인 전자지갑 기술	45
	1. 다자간 보안컴퓨팅 기반 전자서명 기법: 임계치 서명	45
	2. From Theories to Applications	48
	3. CBDC 적용 시나리오	50
V	결 언	52
	〈참고문헌〉	53

* 아톰릭스랩 공동설립자, k@atomrigs.io



요 약

블록체인 기반 가상자산 시장 가치와 거래량은 지속적으로 증가하고 있다. 블록체인에서는 사용자가 개인키를 전자지갑 내에 직접 생성하고 이를 이용해서 가상자산을 통제하게 된다. 따라서 가상자산을 안전하게 관리하기 위해서는 개인키의 보안성이 가장 중요하다. 암호학계에서는 개인키의 보안성을 위해 샤미르 시크릿 쉼어링, 분산 키생성 등을 연구해왔고 최근에는 다자간 보안컴퓨팅을 적용한 전자서명 기법의 연구가 활발하다. 이러한 기법들을 적절하게 활용할 경우 개인키의 보안성을 극도로 높일 수 있으므로 최근 늘고 있는 가상자산 탈취 사고 위험을 방지하는 데에 효과가 크다고 볼 수 있다. 이 글에서는 이러한 기술 중 하나인 다자간 보안컴퓨팅(secure Multi-Party Computation, secure MPC) 기반 전자지갑 기술에 대해 소개하고자 한다.

02 블록체인 가상자산 관리의 보안성 강화를 위한 다자간 보안컴퓨팅 기술 동향

I 블록체인 기술과 가상자산 시장 동향

블록체인은 은행과 같은 중앙화된 자산관리 대행 주체가 없이도 소유자가 자산을 보관하고 사용할 수 있도록 하는 인프라이다. 블록체인 데이터는 전 세계 커뮤니티가 운영하는 블록체인 노드들에 의해 관리되며 이 중 51% 이상의 담합이 없이는 조작이 불가능하다. 비트코인이나 이더리움 같은 대표적인 블록체인의 경우 수천 개의 블록체인 노드들이 운영되고 있다. 2021년 10월 기준으로 미국 내에서 운영되는 노드 비율이 각각 17%와 32% 수준으로 단일 국가의 통제만으로는 데이터 조작이 거의 불가능하다.

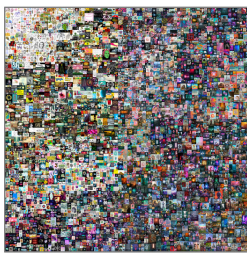
이러한 탈중앙성(decentralization)과 검열저항성(censorship-resistance)은 국가별 다양한 경제적/정치적 환경에 영향을 받지 않고 세계적으로 동일한 가치를 가지는 가상자산을 안정적으로 유지할 수 있게 하고 국가간 장벽이 없는 자산의 전송을 가능하게 한다. 예를 들면 경제 선진국과 후진국의 개인들이 가지는 1 이더(ETH)의 가치는 동일하고 두 나라 모두 자국민이 보유하고 있는 가상자산의 가치를 통제할 수 없다.

또한 기존의 자산과 달리 블록체인 가상자산은 자산 이체 과정에서 은행과 같은 중간자의 개입이 불필요하다. 한국에서 미국으로 송금할 때 국내은행과 미국 은행의 개입이 필요하고 상당한 수수료가 부과된다. 만약 한국보다 신용도가 낮은

아프리카나 남미의 작은 국가의 경우 한국보다 큰 수수료를 부담해야 한다. 블록체인의 가상자산을 송금할 경우 상대적으로 적은 트랜잭션 비용으로 몇 분 내에 이체가 가능하다. 이러한 특징으로 인해 타국에 파견 나가서 일을 하는 후진국의 근로자들이 본국의 가족에게 생활비를 송금하는 경우 은행을 통하지 않고 가상자산을 직접 송금하는 비율이 늘고 있다.

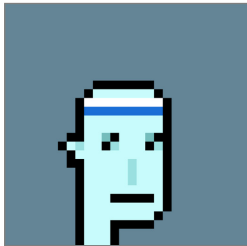
블록체인에서는 소유자가 직접 생성한 문자열 형태의 블록체인 주소로 가상자산을 관리하게 된다. 예를 들면 이더리움의 경우 40자리 16진수 문자열이다. 또한 특정 블록체인 주소가 보유한 가상자산은 공개적으로 조회가 가능하다.

그림 1 가상자산 예시 (이더리움 기반, 2021년 9월 기준 가치)



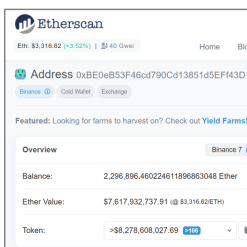
가상자산명:
Beeple's collage
'Everydays: The First 5000 Days'
sold for \$69 million at Christie's

소유자 블록체인 주소:
0x8bB37fb0F0462bB3FC8995cf17721f8e4a399629



가상자산명:
Cryptopunk #3100
sold for 4.2KΞ (\$7.58M)

소유자 블록체인 주소:
0x7b8961F67382C51C389726667ef7dD7CF95FEfd3



가상자산명:
ETH 2.297MΞ (\$7.62B)

소유자 블록체인 주소:
0xBE0eB53F46cd790Cd13851d5EFf43D12404d33E8

[그림 1]은 몇몇 가상자산과 이를 보유한 블록체인의 주소의 예를 보여준다. 위쪽의

두 예는 최근 화제가 되고 있는 NFT(Non-fungible Token)와 이를 보유한 주소를 보여주고 있다. 마지막 예는 세계 최대 가상자산 거래소인 바이낸스가 보유한 가상자산과 주소를 보여주고 있다. [그림 1]에서는 상당한 가치의 가상 자산과 주소를 예시적으로 보여주고 있으나 아주 작은 가치의 가상자산을 보유한 개인 주소들의 현황도 주소만 안다면 누구나 조회할 수 있다.

[그림 2]는 최근 5년간 주요 가상자산의 가치 총합(시가총액)과 공개된 거래량 총합을 보여주고 있다. 각국의 규제와 가상자산의 가치 변동성에 대한 논란에도 불구하고 가상자산의 전체 가치와 거래량은 지속적으로 증가하고 있다. 또한 블록 체인의 특성상 가상자산은 국가나 은행의 통제 없이 전자지갑을 가지고 있는 개인이나 기업은 누구나 보유할 수 있기 때문에 가상자산 소유자가 안전하게 가상 자산을 관리할 수 있도록 하는 기술이 암호학자들과 블록체인 기업들 중심으로 급속도로 연구 개발되고 있다. 이 글에서는 이러한 기술 중 하나인 다자간 보안 컴퓨팅(secure multi-party computation, secure MPC) 기반 전자지갑 기술에 대해 소개하고자 한다.

그림 2 가상자산 규모와 거래량 동향 (최근 5년, coinmarketcap.com)



II 블록체인 전자지갑의 핵심, 개인키

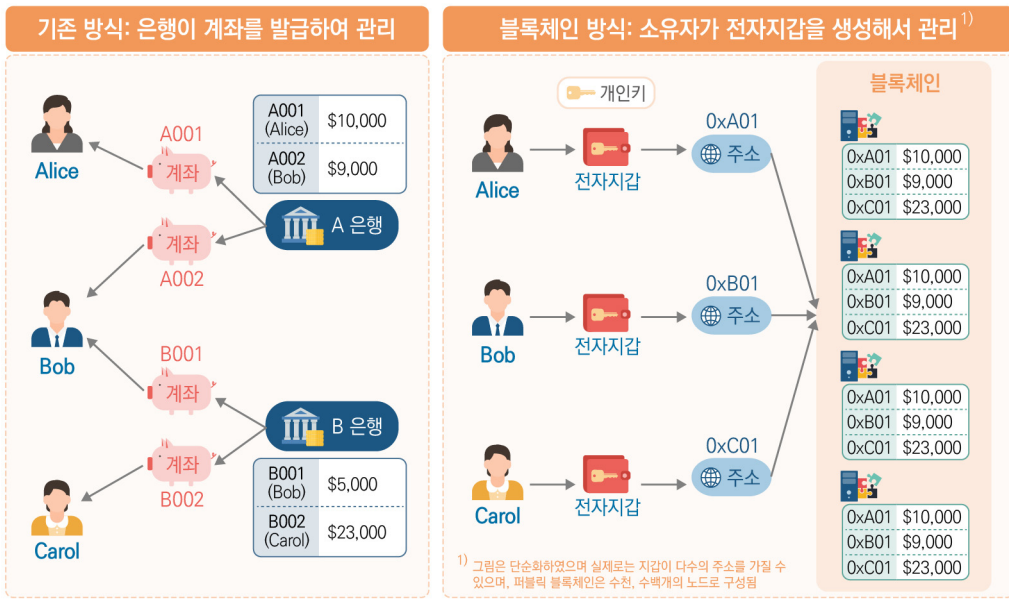
1. 블록체인 전자지갑의 기능

블록체인 상의 가상자산을 이체하고자 할 경우에는 공개된 블록체인 주소에 해당하는 개인키를 사용하게 된다. 블록체인 주소와 개인키의 관계를 좀 더 자세히 말하자면 개인키에서 공개키를, 공개키로부터 블록체인 주소를 생성한다. 반대로 블록체인 주소에서 공개키를 유추하거나 공개키에서 개인키를 유추하는 것은 현대 컴퓨팅 기술로는 불가능한 것으로 간주하면 된다¹⁾.

그렇다면 블록체인 가상자산은 은행과 같은 중간자 없이 어떻게 관리되고 이체 되는 것일까? 기존 금융자산의 경우에는 [그림 3]에서 보이는 바와 같이 자산 소유자가 은행이 발급한 계좌에 자산을 이체하고 실질적으로는 은행이 자산과 이체 권한을 보유한다. 자산 소유자는 은행이 자신의 자산을 안전하게 보관하고 원할 때 이체를 해줄 것이라는 강력한 신뢰를 가지고 있기 때문에 가능한 구조이다. 반면 블록체인에서는 자산 소유자가 직접 개인키와 블록체인 주소를 생성한다. 해당 주소로 자산이 이체될 경우 블록체인은 이를 기록 관리하고 소유자는 언제든지 자산 현황을 조회할 수 있다. 소유자가 자산을 이체하기 위해서는 이체 트랜잭션 전문을 생성하고 개인키로 전문에 대한 전자서명(digital sign)을 한다. 이후 트랜잭션 전문과 전자서명을 블록체인에 전송(broadcast)하고 블록체인은 서명을 검증한 후 자산을 이체한다. 이 모든 과정에서 은행과 같은 중간자의 도움은 필요가 없다.

1) 안정적으로 동작하는 양자 컴퓨터가 개발되면 쇼어(Shor)의 이론에 의해 공개키로부터 개인키를 수개월 혹은 수년 안에 도출하는 것이 가능하다고 보고 있으나 양자 컴퓨터의 개발은 단기간에 이루어지기 어렵기 때문에 이는 논외로 한다.

그림 3 전통적인 은행 계좌와 블록체인 전자지갑의 차이

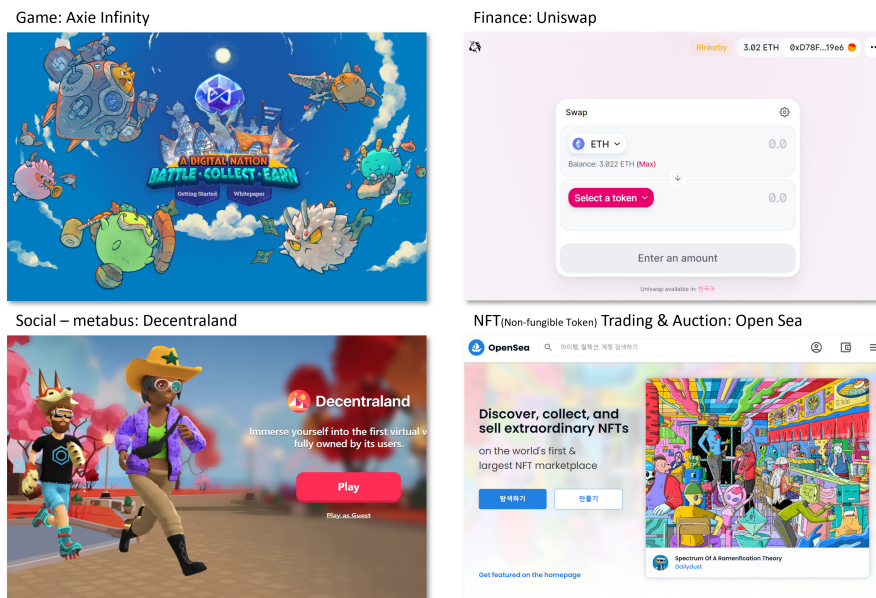


이러한 일련의 과정은 소프트웨어 전문가가 아닌 경우 직접 수행하기 어렵기 때문에 이를 지원하기 위해서 개인키 생성 및 보관, 전자서명, 블록체인 상호 작용을 지원하는 소프트웨어가 필요하다. [그림 3]에서 개인키를 담고 있는 전자 지갑이 바로 이 역할을 한다.

블록체인 전자지갑이 가지는 다른 중요한 기능은 바로 댁브라우징(Dapp browsing) 지원이다. 이더리움과 같이 스마트 컨트랙트(smart contract)를 지원하는 블록체인에서는 제삼자가 프로그램 수행 과정을 왜곡시킬 수 없는 탈중앙화된 어플리케이션인 Dapp(decentralized application)을 누구나 개발해서 배포하는 것이 가능하다. 스마트 컨트랙트의 Dapp이 작동하는 상황의 예를 들어보자. Alice, Bob, Carol이 특정 사업에 4:3:3으로 투자하고 수익을 동일 비율로 분배 받기로 한다. 이때 수익을 분배하는 방법 중 하나는 최대투자자인 Alice가 전체 수익금을 받아서 Bob과 Carol에게 각각 수익금의 30%씩 분배하는 것인데 이때 Bob과 Carol은 모든 과정에서 Alice를 신뢰해야 한다. 다른 방법은 은행과 같은 수탁사에게 수탁 비용을 지불하고 수익금 배분을 위탁하는 것이다. 이때 삼자는

은행의 분배 과정을 신뢰해야 한다. 반면 블록체인 Dapp을 이용하면 신뢰 관계가 없는 사용자들, 즉 전혀 일면식도 없는 사용자들 간에도 중앙화된 주체 없이 이러한 배분 과정을 수행할 수 있다. 예를 들면 블록체인 스마트 컨트랙트에 수익금이 입금되면 스마트 컨트랙트가 자동으로 Alice, Bob, Carol의 주소로 정해진 비율로 이체하도록 할 수 있다. 누구도 이 과정 개입해서 분배 비율과 과정을 왜곡시킬 수 없다. 이러한 방식을 적용해서 현재 이더리움 생태계에는 이미 다양한 Dapp들이 작동되고 있으며 단기간에 수조원에 이르는 거래 규모를 보이기도 한다. [그림 4]는 이더리움 상에 운영되고 있는 대표적인 Dapp을 보여준다. 이러한 Dapp은 신뢰 관계가 없는(trustless) 사용자들 간에 상호작용하는 것을 가능하게 하고 중앙화된 주체의 개입을 없애거나 최소화하였다. Dapp의 원활한 수행을 위해 중앙화된 주체가 개입한다 하더라도 Dapp의 수행 결과를 왜곡시킬 수는 없게 한다.²⁾

그림 4 분야별 대표적인 이더리움 기반 Dapp 예시



2) 중앙화된 주체가 개입하는 예를 들면 투표 Dapp의 경우 중앙화된 주체가 투표 종료 후 개표 트랜잭션을 수행하게 하되 투표 결과를 조작할 수 없고 개표 이후에는 누구나 개표의 정확성을 검증할 수 있게 할 수 있다.

[그림 4]의 화면들은 웹 기반의 사용자 인터페이스이며 이를 이용해서 사용자가 이더리움 블록체인에 있는 스마트 컨트랙트와 상호작용하게 된다. 이때 자산 이체와 마찬가지로 스마트 컨트랙트를 호출하는 트랜잭션을 생성해서 개인키로 전자서명 한 후 블록체인에 전파하게 되는데 이 과정을 뎀브라우징이라고 한다. 최신 블록체인 전자지갑은 사용자를 대신해서 이 전체 과정을 수행하는데 여기에서도 핵심은 개인키를 이용한 전자서명이라고 볼 수 있다.

2. 블록체인의 개인키 체계

비트코인, 이더리움, 바이낸스 체인, 클레이튼 등의 대표적인 공개 블록체인들과 하이퍼레저 및 기업형 이더리움 같은 폐쇄형 블록체인들이 사용하는 전자서명 암호 체계는 타원곡선 전자서명 알고리즘인 ECDSA(Elliptic Curve Digital Signature Algorithm)이며 secp256k1이라는 타원곡선을 사용해서 공개키 공간을 정의한다. 이때 공개키 공간의 원소 수를 차수(order)라고 하며 이는 소수(prime number)이다. 그리고 이 공개키 공간의 차수는 2256에 아주 가까운 수이다.

전자지갑은 0보다 크고 공개키 공간의 차수보다 작은 정수를 랜덤하게 선택해서 개인키를 도출한다. 이후에 타원곡선 연산을 통해서 개인키에 해당하는 공개키를 찾고 이 공개키를 해싱(hashing)에서 블록체인 주소를 도출한다.³⁾

앞에서 기술한 바와 같이 공개키 혹은 블록체인 주소로부터 사용자의 개인키를 역으로 도출하는 것이 현대 컴퓨팅 기술로는 불가능하다. 따라서 소유자가 개인키를 잘 보관하고 있다면 블록체인에 공개된 정보로부터 제삼자가 개인키를 유추하는 것이 불가능하고 타인의 자산을 이체하는 전자서명을 만드는 것 역시 불가능하다. 예를 들면 [그림 1]에 있는 높은 가치의 가상자산에 대한 블록체인 주소가 공개되어 있음에도 해당 개인키가 없으면 이 자산들을 탈취하는 것이 불가능하다.

3) 더 이상의 타원곡선 이론에 대해서는 이 글에서 더 이상 다루지 않을 것이다. 더 자세한 내용을 읽고 싶은 독자는 저자가 작성한 참고문헌 [1]을 읽어보기를 권한다.

이러한 암호학적 특성에 의해서 은행과 같은 중간자 없이 블록체인 가상자산을 소유자가 안전하게 관리할 수 있기 때문에 블록체인 가상자산을 일반적으로 암호화폐라 부르는 것이다.

3. 개인키 관리의 어려움

암호학적 특성에 기반한 개인키 중심의 소유권 행사는 블록체인이 가진 가장 중요한 기술적 특징 중 하나이다. 그런데 이는 실 사용환경에서 사용자들에게 상당한 어려움을 주는 요인이 되기도 한다. 바로 개인키의 분실 및 도난 등에 대비할 만한 표족한 대안이 없다는 것이다.

먼저 개인키를 분실할 경우 해당 주소에 있는 가상자산을 통제할 방법이 없다. 2021년 1월 Chainalysis의 보고서에 의하면 거의 20%에 해당하는 비트코인의 소유주가 개인키를 분실했고 소유권을 행사할 수 없는 상황이라고 주장하고 있다[2]. 이는 당시 가치로 약 \$140B에 해당하는 가상자산이다. 지금도 크고 작은 개인키 분실 사고는 끊임없이 일어나고 있다. 블록체인 주소나 공개키로부터 개인키를 도출할 수 없다는 것이 블록체인 가상자산의 안전성을 보장하고 있기는 하지만 사용자에게는 개인키를 절대로 잃어버리면 안 된다는 부담감을 주고 있는 것이다.

두 번째로 해커가 개인키를 탈취할 경우 개인키를 이용해서 언제 어느 곳에서도 타인의 가상자산을 자산이 통제 가능한 주소로 이체하는 것이 가능하다. 이러한 탈취 사건은 국내외에서 빈번하게 일어나고 있으며 누구보다 개인키의 보안 시스템을 잘 갖추고 있는 국내 양대 가상자산 거래소에서도 2019년 한 해에만 약 \$70M 규모의 가상자산을 탈취당하는 사건들이 발생한 바 있다. 최근에는 블록체인 기술 기업인 Roll이 개인키를 탈취당해서 약 \$5.7M의 이더를 잃은 바 있다. 보안 기술을 잘 갖춘 가상자산 거래소나 블록체인 전문 기술기업도 개인키를 탈취당하는 마당에 일반인이나 중소기업들이 개인키를 안전하게 보관하는 것은 더욱 어려운 일이다.

전통적인 금융시스템에서는 은행이 개입하여 이러한 위험을 상당히 경감시키는

것이 가능하다. 예를 들면 통장을 분실하거나 소유자가 사망할 경우에도 법적인 절차에 따라 자산 소유권을 재확보하는 것이 가능하다. 또한 신용카드를 제삼자에게 탈취당한 경우에도 전화 한통화로 카드 결제를 중지시킬 수 있다. 하지만 블록체인에서는 이러한 중간자의 도움을 받을 수 없기 때문에 개인키의 분실이나 도난은 가상자산의 즉각적인 분실로 이어진다고 볼 수 있다.

이러한 개인키 관리의 어려움에 대한 해법 중 가장 널리 사용되는 것은 하드웨어 기반의 HSM (Hardware Security Module) 장비로 개인키를 관리하고 HSM이 전자서명을 하도록 하는 것이다. 이 과정에서 개인키는 HSM 밖으로 유출되지 않는다. 개인이나 소규모 기업이 고가의 HSM 장비를 갖추고 운영하는 것은 쉽지 않기 때문에 개인들을 위한 USB 메모리 크기의 Ledger나 Trezor 같은 개인용 키관리 디바이스도 널리 사용된다. 이러한 디바이스들은 가격이 저렴하고 소지가 간편한 반면에 HSM에 비해 분실이나 고장의 위험이 높다. 일반적으로 이러한 위험성 때문에 12개 혹은 24개의 단어로 구성된 니모닉(mnemonic) 문구를 백업하고 향후 키관리 디바이스의 분실 혹은 고장 시 니모닉으로 개인키를 복원할 수 있도록 한다. 그런데 이 니모닉 문구 자체가 분실하기 쉽고 혹은 제삼자가 탈취할 경우 키관리 디바이스에 있는 개인키를 쉽게 복원할 수 있기 때문에 개인 키 관리가 가지는 어려움을 근본적으로 해결한다고 보기는 어렵다.

또 다른 대안으로는 상당히 높은 신뢰성과 데이터 보안 관리 능력을 가진 수탁 사업자의 개인키에 블록체인 가상자산을 위탁 보관하는 방법이 있다. 더욱이 Bitgo, Coinbase Custody, Fidelity Digital Assets 등의 가상자산 수탁 사업자들은 수탁 자산에 대한 분실 보험 서비스를 결합하여 안전성을 높이고 있다. 그런데 사용자들이 높은 수탁 비용을 지급해야 하며 사용자가 자산 이체를 원할 경우 최대 24시간의 준비 기간을 요구하고 있다. 위에서 언급한 블록체인의 탈중앙성과 소유자 주도의 자유로운 자산 사용이라는 장점은 저해되지만 대규모 자산을 취급하는 투자 회사나 거래소의 경우에는 적용 가능한 방법으로 볼 수 있다. 그러나 이 역시 일반 개인 사용자나 소규모 기업들이 활용하기에는 적합하지 않다.

III

개인키 관리를 위한 암호학 발전 과정

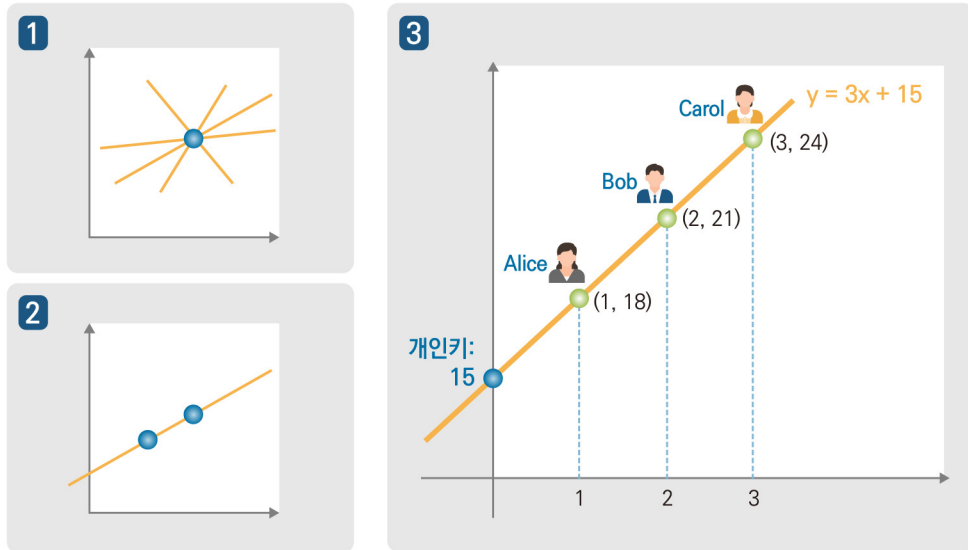
1. 샤미르 시크릿 셰어링

암호학계에서는 블록체인이 출현하기 이전부터 위에서 설명한 개인키 관리의 어려움에 대한 해법을 장기간 연구하고 있었다. 그 첫 번째 단초를 제공한 것은 1979년에 Adi Shamir에 의해 제안된 샤미르 시크릿 셰어링(Shamir Secret Sharing) 기법이다[3]. 이 기법을 활용하면 개인키를 다수의 셰어로 분배한 후 다수의 사용자에게 나눠주고 개인키가 필요할 때 이중 일부의 사용자가 가진 셰어들을 조합해서 개인키를 복원할 수 있다. 예를 들면 Alice, Bob, Carol이 개인키의 샤미르 시크릿 셰어를 나눠 갖고 이중 두 명의 셰어로 개인키를 복원할 수 있게 할 수 있다. 이중 한명이 단독으로 개인키를 복원할 수 없기 때문에 외부 해커가 한명의 셰어를 탈취해도 역시 개인키를 복원하는 것은 불가능하다. 또한 이중 한명이 셰어를 분실할 경우 나머지 두 명이 개인키를 복원하는 것이 가능하므로 일부 셰어의 분실에 대한 대비책이 될 수 있다.

[그림 5]는 이 예를 이용해서 샤미르 시크릿 셰어링에 대한 기본 개념을 보여준다. (1)에서 보듯이 공간의 한 점을 지나는 직선은 무한하게 존재한다. 그러나 (2)를 보면 공간의 두 점을 지나는 직선은 하나이다. 샤미르 시크릿 셰어링은 바로 이 원리를 이용한다. (3)은 위 예의 샤미르 시크릿 셰어링을 수행하는 순서를 보여준다. 개인키를 숫자 15라고 가정해 보자. 개인키를 알고 있는 딜러는 15를 Y절편으로 하는 직선을 그린다. 이때 직선의 기울기는 랜덤하게 설정하고 딜러 외에 아무도 모른다. [그림 5]의 예에서는 기울기가 3이다. 그리고 Alice, Bob, Carol에게 각각 직선 위의 점 (1,18), (2,21), (3,24)를 셰어로 나눠준다. 이후 세 명중 두 명이 협력하면 라그랑주 보간법(Lagrange interpolation)[4]을 이용해서 직선 $y = 3 * x + 15$ 를 복원할 수 있고 따라서 Y절편인 15를 알 수 있다. 만약 Eve에게 (4,27)을 셰어로 나눠주면 네 명 중 두 명이 셰어를 분실해도 개인키 복원이 가능해 지므로 개인키의 분실 위험성은 줄어든다. 이 방식을 응용하면

딜러가 T차 다항식을 랜덤하게 생성하고 T보다 큰 N명에게 쉐어를 분배함으로써 N명이 쉐어를 나눠 가지고 T+1명이 모여서 개인키를 복원 가능한 (T, N) 샤미르 시크릿 쉐어링을 구성할 수 있다.

그림 5 샤미르 시크릿 쉐어링 기본 개념



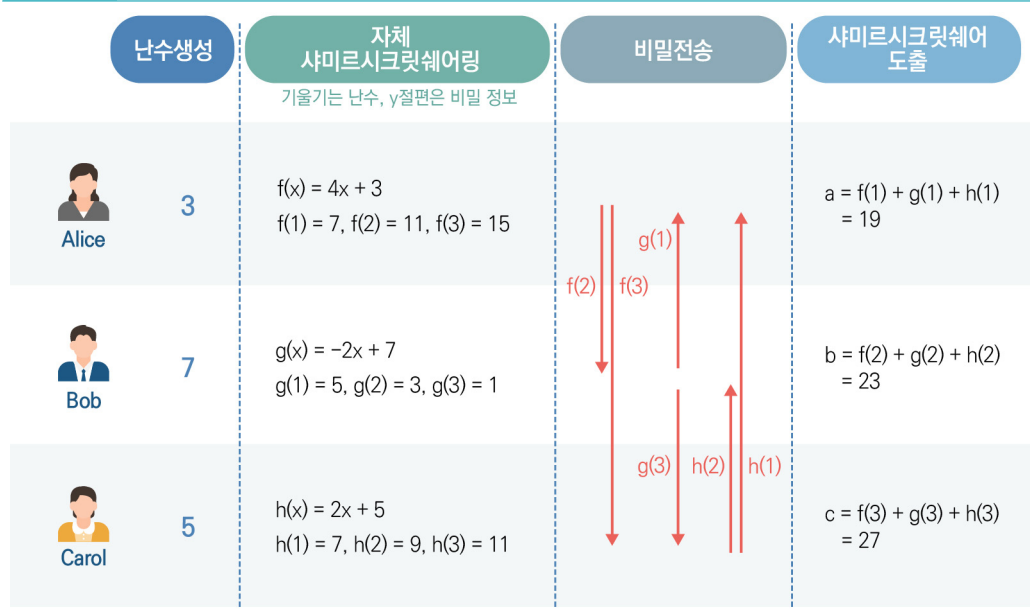
이후 샤미르 시크릿 쉐어링의 알고리즘적 완결성을 강화하기 위해서 딜러가 개인키를 왜곡하지 않고 제대로 샤미르 시크릿 쉐어링을 수행했는지를 참여자들이 검증할 수 있는 검증가능한 시크릿 쉐어링(verifiable secret sharing) 기법들이 개발되었다[5].

2. 분산 키생성

그런데 샤미르 시크릿 쉐어링만을 사용할 경우 또 다른 문제가 발생한다. 처음 개인키를 분배하는 과정에서 딜러가 온전한 개인키를 알고 있다는 것이다. 특히 블록체인과 같이 탈중앙화된 시스템에서는 개인키를 분배할 믿을 만한 주체의 존재를 가정하는 것은 적합하지 않다. 이러한 딜러 문제를 해결하기 위해서 블록

체인이 탄생하기 이전부터 분산 키생성(distributed key generation) 프로토콜이 개발되었다. 분산 키생성 프로토콜은 다수의 참여자가 딜러의 개입 없이 암호 프로토콜을 수행해서 자체적으로 샤미르 시크릿 셰어링을 하는 방식이다. 초기의 샤미르 시크릿 셰어링이 특정 개인키를 분배하는 방식인 것에 반해 분산 키생성은 이름에서 보는 바와 같이 프로토콜 수행 과정에서 개인키가 생성된다. 참여자들 중 누구도 자신의 셰어 외에 생성된 개인키를 알지 못하는 반면 공개키와 이로부터 파생되는 블록체인 주소는 참여자 모두가 알게 된다.

그림 6 분산 키생성 예시



[그림 6]은 분산 키생성의 기본 개념을 예시로 보여준다. 먼저 Alice, Bob, Carol이 각각 비밀정보 3, 7, 5를 랜덤하게 선정하고 이 수들의 합, 즉 15를 개인키로 하자고 합의한다. 비밀정보는 공유하지 않으므로 모두 개인키 15를 알지 못한다. 이후 각 참여자는 [그림 6]에 표시된 대로 프로토콜을 수행해서 15의 샤미르 시크릿 셰어인 19, 23, 27을 얻게 된다.

[그림 6]을 주의 깊게 살펴보면 세 참여자가 가지는 셰어는 $f(x) + g(x) +$

$h(x) = 4x + 15$ 로부터 생성된 샤미르 시크릿 쉐어임을 알 수 있고 개인키 15는 $f(x) + g(x) + h(x)$ 의 Y절편이 된다. 암호학적인 프로토콜을 잘 구성하면 일부 참여자가 다른 참여자의 비밀 정보를 유추하거나 자신이 원하는 개인키 생성을 유도하기 위해 암호 프로토콜을 왜곡하는 등 악의적인 행위(malicious activities)를 할 수 있다. 예를 들면 Rosario Gennaro가 [6]에서 제안한 분산 키생성 프로토콜은 이러한 악위적인 행위를 감지하고 해당 참여자를 제외시키는 등 능동적인 보안성(active security)을 가진다.

Shamir의 샤미르 시크릿 쉐어링과 Gennaro의 분산 키생성 프로토콜은 다음 장에서 소개할 다자간 보안컴퓨팅 기반 임계치서명 프로토콜의 기반이 된다.

IV

다자간 보안컴퓨팅 기술을 적용한 안전한 블록체인 전자지갑 기술

1. 다자간 보안컴퓨팅 기반 전자서명 기법: 임계치 서명

위에서 소개한 분산 키생성 프로토콜을 적용할 경우 Alice, Bob, Carol은 단일 개인키를 복원할 수 있는 샤미르 시크릿 쉐어를 가지게 된다. 그런데 여기에도 한계가 있다.

전자서명을 하려면 이 중 두 명의 쉐어를 모아서 라그랑주 보간법으로 개인키를 복원해야 한다. 그런데 복원하는 사람은 개인키를 알게 되므로 딜러가 없이 누구도 개인키를 모르게 분산 키생성을 했던 초기의 장점이 사라지게 된다. 블록체인 가상 자산의 경우 이 한계는 매우 중요한 문제가 된다. 만약 세 사람이 1,000억원 가치의 블록체인 가상자산을 관리하고 있다고 가정해 보자. 개인키를 알게 되는 순간 가상자산 전체의 통제권을 가지게 되기 때문에 세 사람 중 누구도 다른 사람이 개인키를 알게 되는 상황을 원하지 않을 것이다.

일부 전자서명 알고리즘들의 경우에는 이 문제를 쉽게 처리할 수 있는 서명 결합(signature aggregation)을 지원하기도 한다. 예를 들면 BLS[7]나 타원곡선

기반 Schnorr[8] 알고리즘의 경우 두 명이 각자의 쉼어로 서명한 다음 서명 정보(signature)만 공유하고 결합함으로써 개인키의 서명을 생성할 수 있다. 이때 쉼어 정보는 유출하지 않으므로 개인키는 아무도 모른다. 그러나 불행하게도 현재 대부분의 블록체인이 채용하고 있는 ECDSA의 경우에는 이러한 서명 결합을 지원하지 않고 있다⁴⁾.

이러한 이유로 ECDSA에 잘 적용될 수 있는 다자간 보안컴퓨팅(Secure Multi-party Computation) 기반 전자서명 기법들이 개발되었다. 다자간 보안컴퓨팅은 다수의 참여자들이 각자 보유한 비밀정보들을 유출하지 않고도(privacy preserving) 모두의 비밀정보를 입력값으로 하는 수식을 계산할 수 있게 하는 암호한 분야이다[9]. 또한 최종 결과는 각 참여자들이 검증 가능하다(verifiable). 단순한 예를 들면 Alice, Bob, Carol이 각자의 재산을 공개하지 않으면서 가장 재산이 많은 사람을 알아낸다고 세 사람 재산의 평균값을 계산할 수 있다. 이 기법을 ECDSA에 적용하자면 두 사람이 다자간 보안컴퓨팅에 참여해서 쉼어 정보의 비밀을 유지한 채 전자서명 수식을 계산하는 것이다.

또한 위에서 기술한 분산 키생성 프로토콜도 다자간 보안컴퓨팅으로 볼 수 있다. Alice, Bob, Carol이 각자 초기 생성한 난수를 비밀 정보로 하고 암호 프로토콜을 통해서 샤미르 시크릿 쉼어를 생성하여 나눠 갖는 것이다. 이 과정에서 다른 참여자의 비밀 정보(초기 생성 난수, 샤미르 시크릿 쉼어)를 알 수 없다(privacy-preserving). 또한 [그림 6]에서는 기술하지 않았지만 Feldman의 검증 가능한 시크릿 쉼어링[10]을 적용해서 각자 보유하게 된 샤미르 시크릿 쉼어가 올바르게 생성된 것인지를 검증할 수 있다(verifiable).

정리하자면 다자간 보안컴퓨팅을 적용할 경우 분산 키생성을 통해서 참여자들이 샤미르 시크릿 쉼어들을 가지게 되고 이 중 정족수를 채우면 암호 프로토콜을 통해서 개인키를 복원하지 않고도 전자서명을 생성할 수 있다. 이때 한명이라도

4) 이더리움 2.0에서는 BLS를, 비트코인 탭루트(taproot) 업그레이드에서는 타원곡선 기반 Schnorr를 지원할 예정이나 이미 대부분의 블록체인 소프트웨어들이 ECDSA를 기반으로 개발되어 있기 때문에 상당히 장기간 ECDSA가 주로 사용될 것으로 예상된다.

부족하면 전자서명을 생성할 수 없기 때문에 이를 임계치 서명(threshold signature)이라고도 부른다. 블록체인 가상자산의 가치가 올라가고 개인키 보호에 대한 요구가 커짐에 따라 다자간 보안컴퓨팅 기반 임계치 서명 이론이 최근 급속도로 발전하였고 2017년 이후 실제 어플리케이션에 적용 가능한 성능을 가진 이론들이 정립되었다. 다자간 보안컴퓨팅 기법을 적용해서 개인키를 복원하지 않고도 참여자들 간의 암호 프로토콜을 통해서 ECDSA 전자서명을 생성하는 프로토콜을 이 글에서 설명하기에는 암호학적 난이도가 너무 높다. 따라서 이글에서는 몇 가지 대표적인 기법과 특징을 간략하게 소개하고자 한다.

* Lindell17: 2 Party ECDSA [11]

Alice와 Bob이 각자 개인키 쉼어를 보유하고 두 쉼어의 곱이 개인키가 된다. Lindell17을 이용하면 각자의 쉼어를 공개하지 않고 개인키에 대한 전자서명을 할 수 있다. 둘 중 한사람이 쉼어를 잃어버리면 개인키를 복구할 수 없다는 단점이 있으나 속도가 매우 빠르고 알고리즘이 단순해서 단일 실패 지점(single point of failure)을 제거하는 것이 중요하고 고속 전자서명이 필요한 어플리케이션에서는 많이 사용되는 프로토콜 중 하나이다.

* GG18: ECDSA Threshold Signature Scheme [12]

분산 키생성을 통해서 N명이 샤미르 시크릿 쉼어를 도출한 후 이 중 T명이 공동 연산해서 디지털서명을 생성하게 된다. 2명의 참여자로 제한되어 있는 Lindell17에 비해 다수의 N명이 참여하는 (T,N) 샤미르 시크릿 쉼어링을 적용하므로 Lindell17에 비해 활용 범위는 넓은 반면 속도가 느리다는 단점이 있다.

* GG20: One round Threshold ECDSA [13]

GG18을 개선한 프로토콜이다. 디지털서명 이전에 사전 준비를 미리 해놓고 (offline processing) 전자서명을 해야 하는 시점에는 한 번의 통신(one round)으로 고속 전자서명을 할 수 있다. 예를 들면 야간에 배치로 많은 수의

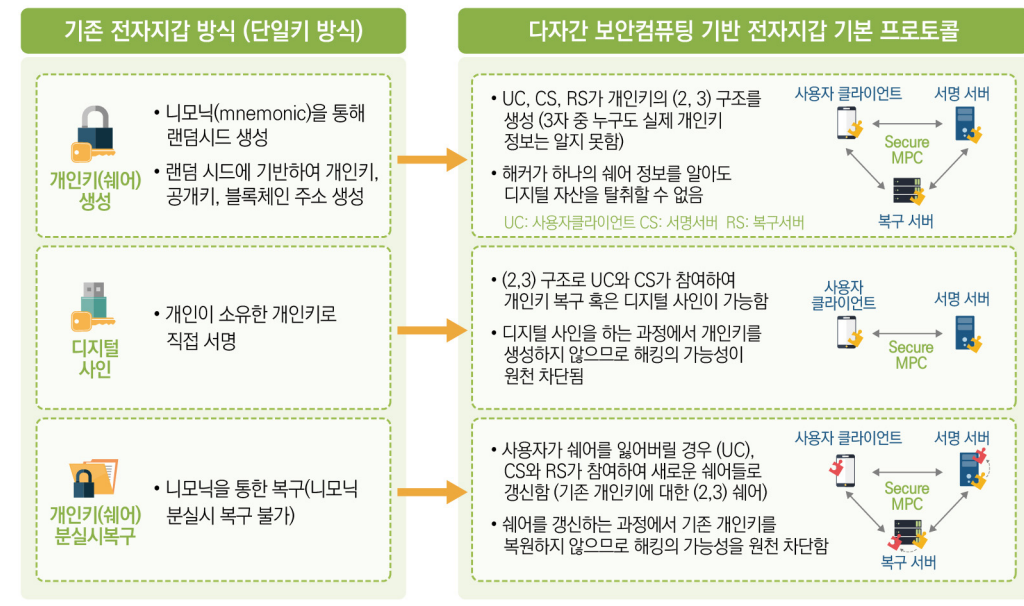
사전 준비를 하고 주간에는 다수의 빠른 전자서명을 할 수 있다.

이후에도 암호학계에서는 이 알고리즘들의 성능을 개선하기 위한 노력이 계속되고 있으나[14,15] 대부분의 방법론이 위 세 가지 방식중 하나의 범주에 속한다. 분산 키생성과 임계치 서명은 모두 다자간 보안컴퓨팅 기법을 기반으로 하고 있으며 두 프로토콜을 결합하여 사용할 경우 키생성과 사용의 전 과정에서 개인 키가 단일 지점에서 복원되지 않는다. 따라서 해커가 단일 지점을 공격해서 개인 키를 탈취할 수 있는 단일 실패 지점을 완벽하게 제거하는 것이 가능하다. 위 프로토콜이 가지는 또 다른 큰 장점은 프로토콜의 안전성이 수학적으로 검증되어 있다는 것이다. 따라서 위 프로토콜의 모든 단계를 제대로 구현한다면 보다 안전한 어플리케이션의 개발이 가능해진다.

2. From Theories to Applications

필자가 몸담고 있는 아톰릭스랩은 Lindell¹⁷ 기반의 Dekey Extension과 GG18 기반의 Dekey Corporate을 개발하고 상용화를 완료했다. Dekey Corporate의 핵심 프로토콜은 키웨어 생성, 전자서명 생성, 키웨어 복구 등이 있으며 [그림 9]은 Dekey Corporate와 기존 전자지갑의 차이점을 설명한다. 전 과정에서 다자간 보안컴퓨팅 기법을 적용하였기 때문에 사용자 클라이언트, 서명 서버, 복구 서버가 개인키를 알 수 없다. 따라서 단일 실패 지점이 존재하지 않는다.

그림 7 기존 전자지갑과 다자간 보안컴퓨팅 기반 전자지갑(Dekey Corporate) 비교



[그림 7]에서 소개한 프로토콜들은 학자들에 의해 그 보안성이 수학적으로 검증되어 있고 연구실 수준의 성능 최적화가 상당히 진행되어 있다고 볼 수 있다. 그럼에도 불구하고 필자의 경험상 실제 상용 어플리케이션을 개발할 경우에는 논문에 기술된 기본 프로토콜 외에 부가적으로 상당히 많은 부분을 고려해야 한다. 예를 들면 블록체인과의 상호작용, 통신 및 저장소의 보안, 동시 사용자 처리 등의 많은 부분에서 부가적인 개발이 필요하다. 특히 이론에서는 참여자들의 컴퓨터 성능을 일반적인 최신 PC 수준으로 가정한다. 그러나 실제 사용환경에서는 모바일이나 웹브라우저 등의 저성능 환경도 감안해야 하므로 보다 적극적인 최적화를 진행하지 않으면 사용하기 힘든 수준의 느린 성능을 보이기 쉽다.

이러한 난관을 뚫고 나면 개인키 보안에 대한 시장의 요구가 큰 블록체인 분야에서 굉장히 빠르게 상업화되는 경향을 보이고 있다. 상업화에 성공한 대표적인 기업들은 이스라엘 기술진 중심의 Unbound Securities, Zengo, Curv, Fireblocks, 덴마크 기술진 중심의 Sepior 등이 있고 한국에는 필자가 몸담고 있는 아톰릭스랩이 있다. 블록체인을 활용하는 중대형 기업들의 수요도 늘어가고

있다. 비트코인 결제를 시작한 PayPal의 경우 Curv를 수억 달러에 인수했고, 대형 거래소인 Gemini는 Shard X를 인수했다. Nasdaq에 상장된 미국 최대 가상자산 거래소인 Coinbase의 경우 자체적인 다자간 보안컴퓨팅 기반 전자서명 시스템을 개발하고 있고 앞의 해킹 사례에서 언급한 Roll 사의 경우 최근 Fireblock의 전자지갑 시스템으로 자사의 전자지갑을 전면 교체하고 있다.

3. CBDC 적용 시나리오

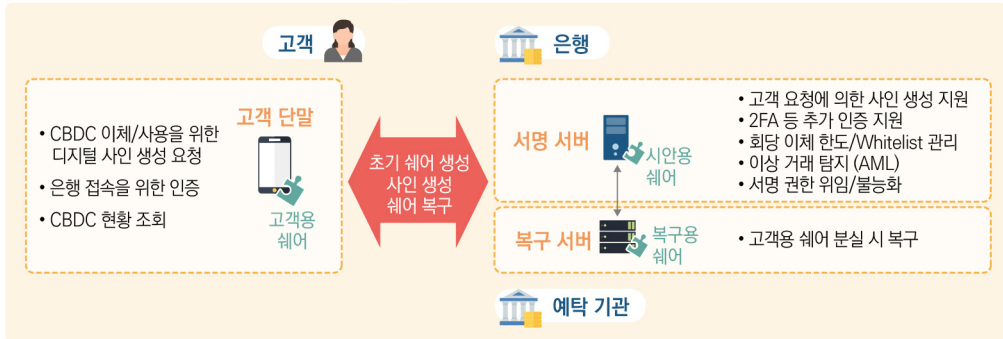
많은 국가들이 블록체인 기반의 CBDC(Central Bank Digital Currency) 발행을 검토하고 있고 한국은행 역시 파일럿 프로젝트를 진행하고 있다. CBDC에 블록체인 기술을 적용한다면 이 글에서 소개한 기술을 적용하는 것을 고려할 필요가 있다. 공개 블록체인의 사용자 베이스와는 달리 CBDC는 정부, 금융회사, 일반 국민 등 대다수가 보유하고 사용할 것이기 때문에 개인키의 안전한 보관은 당연히 중요한 이슈가 된다. 반면 사용자들에게는 기존의 은행 중심 금융시스템에서 제공하던 분실 시 재발급, 도난 시 이체 중지, 사망 시 상속 지원, 2단계 인증(2FA, 2 factor authentication) 등의 서비스를 여전히 제공할 필요가 있다. 또한 기존 공개 블록체인에서는 검열 저항성에 의해 불가능했지만 CBDC에서는 법적인 절차에 의한 정부와 금융회사의 제삼자 재산 압류 과정이 필요할 수 있다.

각 은행이 고객들의 CBDC를 대행 보관하고 기존 방식의 서비스를 제공하는 것이 일견 가장 쉽고 효율적인 방법으로 생각될 수 있다. 그러나 이 경우 기존 금융시스템과 별반 다를 바 없고 모든 금융회사는 CBDC를 위한 은행간 인터페이스를 새로 구축해야 한다.

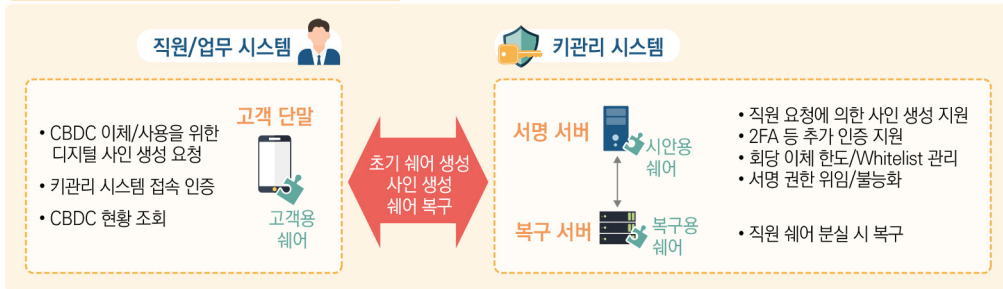
이 글에서 기술한 다자간 보안컴퓨팅 기반 전자지갑을 CBDC에 적용할 경우 블록체인 기술이 가진 장점을 살리면서도 위에서 언급한 금융서비스의 제공이 가능하다. [그림 8]은 Retail 고객용 전자지갑과 은행 내부용 전자지갑에의 적용 사례를 보여준다.

그림 8 CBDC 적용 시나리오

① CBDC Retail 고객용 지갑



② CBDC 은행 내부용 지갑



먼저 (1)에서 보는 바와 같이 일반 고객이 사용하는 전자지갑에 적용될 수 있다. 개인키를 고객, 은행, 예탁기관이 샤미르 시크릿 쉼어로 생성한 후 자산 이체는 고객과 은행이 가진 쉼어를 이용한 다자간 보안컴퓨팅 프로토콜로 수행한다. 이 과정에서 은행은 2FA, 이체 한도 관리, 자금세탁 방지 모니터링 등 기존 금융 시스템과 유사한 보안 서비스를 제공할 수 있다. 그리고 고객이 쉼어를 분실할 경우 은행과 예탁기관이 고객의 쉼어 복구를 지원할 수 있으며 법적인 절차에 의한 압류는 은행과 예탁기관이 가진 쉼어로 처리가 가능하다(두개의 쉼어로도 이체 가능). (2)는 은행 내부의 CBDC 자산 관리를 위한 전자지갑에 이 글에서 소개한 기술을 적용한 예이다. 위에서 소개한 바와 같이 강력한 블록체인 보안 기술과 경험을 가진 대형 가상자산 거래소조차도 내부인에 의한 개인키 탈취 사고가 빈번하게 발생한다. 이는 내부인이 개인키 자체에 접근할 수 있기 때문이다.

따라서 은행의 경우에도 이러한 보안 사고를 대비할 필요가 있다. (2)에서 보는 바와 같이 직원 혹은 업무 시스템은 개인키가 아닌 샤미르 시크릿 쉼어를 가지고 있고 자산 이체를 위해서는 서명 서버와의 암호 프로토콜을 수행한다. 이후 직원의 업무 변경 혹은 퇴사 시 서명 서버가 기존 쉼어를 불능화시키는 것이 가능하고 직원은 기존에 보유한 쉼어만으로는 자산을 통제하는 것이 불가능하다.

V 결 언

블록체인 가상자산의 가치와 활용성이 높아지고 있는 반면 개인키 관리의 어려움은 블록체인 사용자를 확대하는 데에 걸림돌이 되고 있고 대규모 가상자산을 다루는 기업들에게는 큰 리스크 요인이 되고 있다. 따라서 자연히 블록체인 분야에서는 개인키의 보안 요구가 증가하고 있다. 이 글에서는 개인키의 보안성을 높이기 위한 다자간 보안컴퓨팅 기반 기법들을 소개하였다. 이러한 기법들을 블록체인 전자지갑에 적용하면 다수의 참여자들이 샤미르 시크릿 쉼어링을 기반으로 분산 키생성을 수행하고 이 중 일부가 공동으로 전자서명을 하게 된다. 이 과정에서 참여자 단독으로는 개인키를 알 수 없기 때문에 단일 실패 지점을 완전하게 제거할 수 있다. 따라서 가상자산 커스터디와 거래소 같은 대규모 블록체인 가상자산을 다루는 기업은 물론 개인 전자지갑에 이르기까지 그 활용성이 매우 높다고 볼 수 있다.

블록체인 기술과 산업의 발전 속도가 빠른 만큼 다자간 보안컴퓨팅 기반 전자지갑 제품들도 최근 국내외에서 상용화되고 있고 해외 가상자산 관련 기업들의 경우 이를 적극적으로 도입하고 있다. 특히 국가 화폐의 발행 및 유통 시스템으로 논의되고 있는 CBDC를 블록체인 기반으로 구현할 경우 개인키의 안전한 관리가 가능한 전자지갑 기술은 인프라 요소로서 필수적이며 이 글에서 논의한 주요 기법들은 효과적인 해법이 될 것이다.



- [1] Bae, K., "Pairing-based Cryptography와 BLS signature의 이해 – Part 1," Medium, 2020.
- [2] New York Times, "Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes," Jan. 2021.
- [3] Shamir, A., "How to share a secret," Communications of the ACM 22.11, pp.612–613, 1979.
- [4] Waring, E., "VII. problems concerning interpolations," Philosophical transactions of the royal society of London 69, pp.59–67, 1779.
- [5] Pederson, T., "Non-interactive and Information-theoretic Secure Verifiable Secret Sharing," In Advances in Cryptology – Crypto 1991, pp.129–140, 1991.
- [6] Gennaro, R. et al., "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems," Journal of Cryptology, 2007.
- [7] Boneh, D. et al., "Short Signatures from the Weil Pairing," Advances in Cryptology ASIACRYPT, pp.514–532, 2001.
- [8] Schnorr, C.P., "Efficient identification and signatures for smart cards," Advances in Cryptology, Crypto '89, pp.239–252, 1989.
- [9] Cramer, R. et al., "General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme," Advances in Cryptology Eurocrypt. pp.316–334, 2000.
- [10] Feldman, P., "A practical scheme for non-interactive verifiable secret sharing," 28th Annual Symposium on Foundations of Computer Science, pp.427–438, 1987.
- [11] Lindell, Y., "Fast secure two-party ecDSA signing," In Annual International Cryptology Conference, pp.613–644, 2017.
- [12] Gennaro, R. and Goldfeder, S., "Fast multiparty threshold ecDSA with fast trustless setup," In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp.1179–1194, 2018.
- [13] Gennaro, R. and Goldfeder, S., "One round threshold ecDSA with identifiable abort," Cryptology ePrint Archive, Report 2020/540, 2020.

- [14] Canetti, R. et al., “UC non-interactive, proactive, threshold ECDSA with identifiable aborts,” In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp.1769–1787, 2020.
- [15] Damgård, I. et al., “Fast Threshold ECDSA with Honest Majority,” SCN 2020: Security and Cryptography for Networks, pp.382–400, 2020.

전기통신금융사기 최신 동향 및 피해사례 분석 프레임워크 소개

정영훈*

I	서론	57
II	전기통신금융사기 최신 동향	61
III	전기통신금융사기 피해사례 분석 프레임워크	64
	1. 사기 개요도	66
	2. 범행 수법	72
	3. 피해사례 분석 예	76
IV	결론	80
	〈참고문헌〉	82

* 금융보안원 금융보안관제센터 대리(jungyh@fsec.or.kr)



요 약

전기통신금융사기는 오래전부터 사회적 문제로 존재하였으나 여전히 피해액은 막대하고 범행 수법은 나날이 교묘해지고 있다. 전기통신금융사기 예방을 위해서는 피해사례 및 사기수법의 공유가 중요하나, 피해사례에 대한 종합적인 분석이 어려운 상황이다.

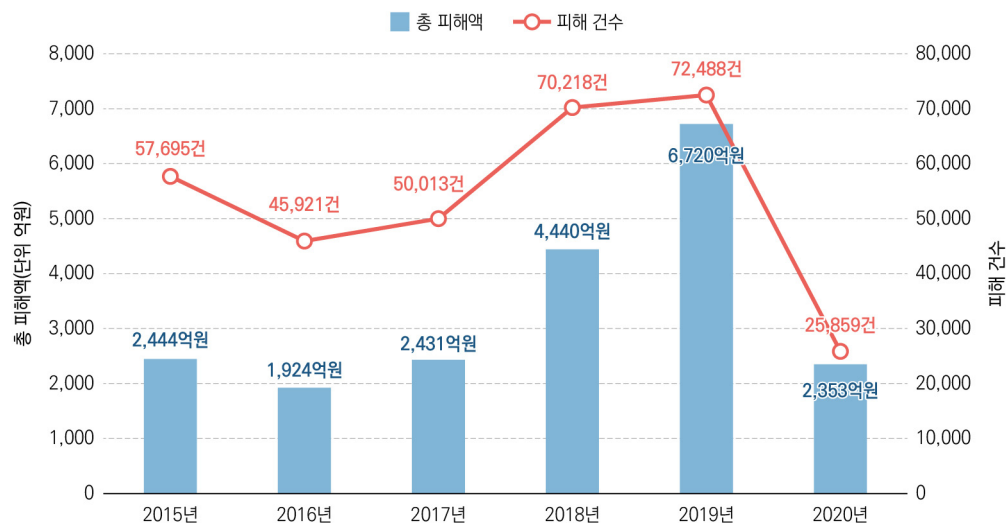
본 고에서는 전기통신금융사기 최신 동향을 살펴보고 피해사례 분석 프레임워크를 소개하여 보이스 피싱 피해사례를 체계적이고 효율적으로 분석할 수 있는 종합적인 분석 방법론을 제시하고자 한다.

03 전기통신금융사기 최신 동향 및 피해사례 분석 프레임워크 소개

I 서론

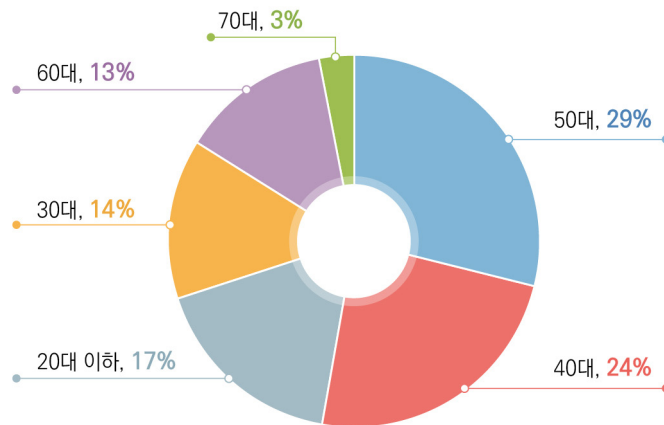
보이스피싱 등 전기통신금융사기는 국내에서 오래전부터 사회적 문제로 대두되었으며 금융감독원에 따르면 해당 범죄로 인한 피해는 2019년에 총 72,488건 및 6,720억 원을 기록하였다[1][2]. 이는 하루 평균 199건 및 18억 원에 달하는 막대한 수치이다.

그림 1 전기통신금융사기 피해액 추이(2016년~2020년) (출처 : 금융감독원)



일반적으로 고령층(60, 70대)에서 피해가 가장 클 것이라고 생각하는 경향이 있지만, 경찰청 통계에 따르면 해당 연령층의 피해자 비율이 16%로 가장 적다. 사회경제적 역량이 가장 높은 중장년층(40-50대) 피해자 비율이 총 53%로 과반수를 차지하여 가장 많이 피해를 당했으며, IT에 친숙하여 피해를 가장 적게 입을 것 같은 미성년자 및 청년층(20-30대)이 총 31%로 중장년층 다음을 차지하고 있다.¹⁾

그림 2 전기통신금융사기 피해 연령대 비율(2020년) (출처 : 경찰청)



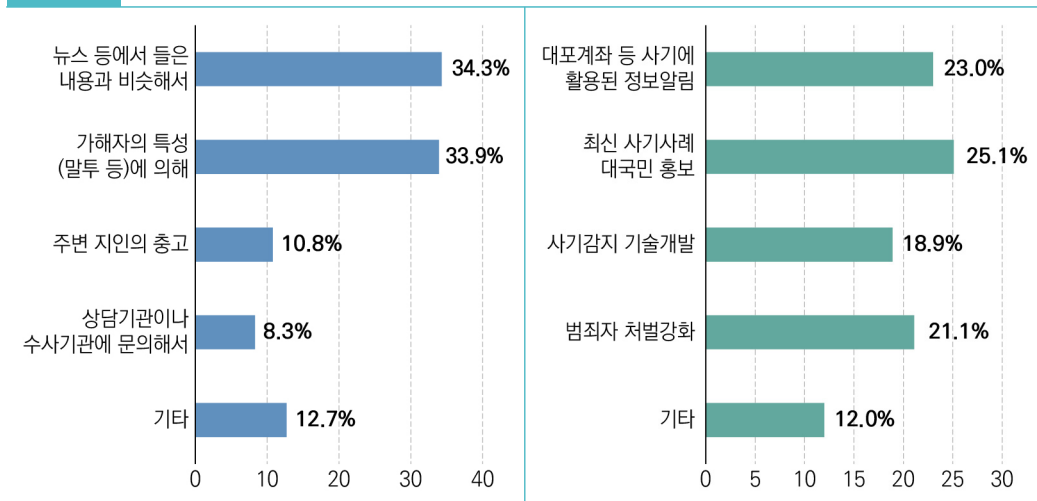
질적인 측면에서 보자면, 보이스피싱 등 전기통신금융사기는 금융사기와 전자적 침해위협, 자금세탁을 총체적으로 활용하는 방식으로 빠른 속도로 고도화되고 있다. 특히, 전화를 통한 금융사기에서 SMS, 카카오톡 등 다양한 채널로 확장되고, 더 나아가 악성앱(피싱, 원격제어 등), 전화번호 가로채기 등 고도화된 IT기술을 활용하기 시작했다. 또한 피해자금을 세탁하기 위해 가상자산 및 선불전자지급 수단 등을 활용한다.

서민금융연구원에 따르면 [표 1]에서 보듯이 전기통신금융사기에 노출된 개인이 전기통신금융사기를 인지한 방법으로는 ‘뉴스 등에서 들은 내용과 비슷해서 (34.3%)’로 1순위를 차지했으며 전기통신금융사기 예방을 위해 필요한 점으로 ‘최신 사기사례 대국민 홍보(25.1%)’가 1위를 차지하였다[3]. 이는 전기통신금융

1) 디지털타임스, 보이스피싱 피해자 예상밖이네... 40~50대가 왜이리 많아?, 2021.2.

사기를 예방함에 있어 피해사례 및 사기 수법에 대한 공유가 무엇보다 중요하다는 것을 시사한다.

표 1 전기통신금융사기 인지방법 및 사기 예방을 위해 필요한 점(출처 : 서민금융연구원)



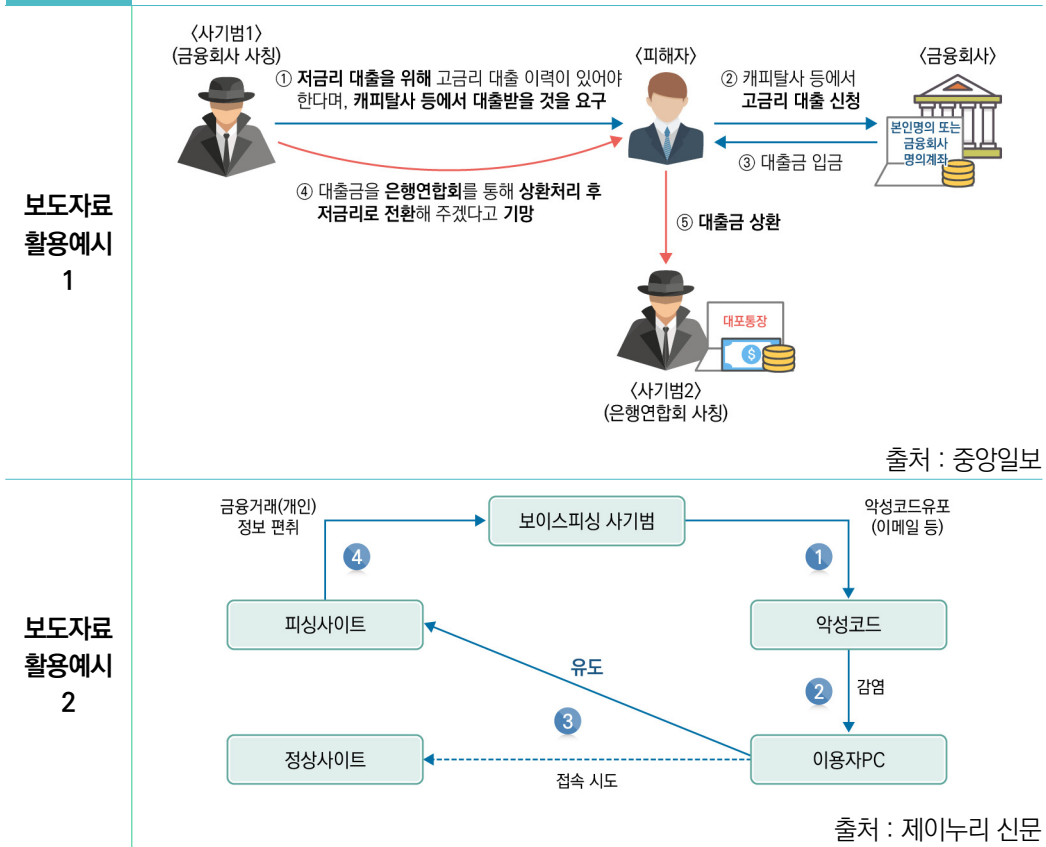
이에 따라 금융감독원 등은 관련 웹사이트²⁾를 운영하여 대국민 대상으로 다양한 사기 수법을 홍보하고 있으며, 금융회사와 금융보안원 등은 각종 협의체 등을 통해 기관 간 피해사례를 공유하는 등 전기통신금융사기 피해를 줄이기 위해 다양한 노력을 기울이고 있다.

그러나 보이스피싱 피해 사례를 공유하는데 있어, 보이스피싱 발생의 단계별 분석에 상당한 어려움이 있다. 일반적으로 금융권에서 보이스피싱 피해사례를 분석하는 방법은 [표 2]와 같이 보도자료, 회의자료 등을 활용하기 때문에 단편적으로 분석하는 수밖에 없다. 다시 말하면, 개별적인 전기통신금융사기 사례를 분석하기는 용이하나 고도화되고 다단계로 복잡하게 발생하는 전기통신금융사기의 전체 흐름 중 일부만 설명한다. 또한, 금융업권뿐 아니라 통신업권, 전자금융업권, 상업권 및 가상자산업권 등까지 연계되고 다양한 접근방식과 기망시나리오, 자금 편취방법 등을 활용하는 전기통신금융사기에 대한 분석이 어렵다. 그래서 보이스

2) 보이스피싱 지킴이 웹사이트(phishing-keeper.fss.or.kr)

피싱 피해사례를 체계적이고 효율적으로 분석하기 위해서는 보다 종합적인 분석 방법론이 필요하다.

표 2 일반적인 보이스피싱 피해사례 분석 개요도³⁾



본 고에서는 전기통신금융사기 최신 동향을 살펴보고, 다양한 사기 수법을 구조화한 전기통신금융사기 분석 프레임워크를 소개하고자 한다. 이를 통해서 체계적인 보이스피싱 피해사례 분석 및 관련된 기관의 보완사항을 파악하는 데에 참고자료가 되고 궁극적으로는 보이스피싱 예방 및 대응 활동에 도움을 제공하고자 한다.

3) 중앙일보, '저금리로 바꿔드려요' 이런 전화는 보이스피싱, 2017.5.
제이누리 신문, 제주도 보이스피싱으로 100억 털렸다, 2013.3.

II 전기통신금융사기 최신 동향

금융보안원과 금융업권 간 보이스피싱 대응협의체 논의 내용, 보도자료, 각종 포털 등을 통해 전기통신금융사기 관련 최신 동향을 분석하였다. 최근의 고도화된 전기통신금융사기 관련 특징은 아래 5가지로 요약할 수 있다.

첫째, 지속적으로 새로운 사기 수법을 고안한다. 현재 유행하는 사기 수법에 대한 금융회사의 대응 및 금융소비자의 경각심이 높아질 경우 새로운 수법을 적용한다.

둘째, 복합적인 접근방식을 이용한다. 전화, SMS 등 단일 채널이 아닌 ‘전화+SMS+원격제어앱’, ‘영상통화+위조공문’ 등 복합적인 접근방식을 활용한다. 전화를 이용한 보이스피싱 사기를 잘 알고 있는 피해자도 검찰 사무실로 위장한 방에서 검찰 명패를 찬 정장 차림의 남성과 영상통화를 하거나 검찰청장의 직인이 찍힌 위조공문을 받게 되면 기망당할 확률이 높아진다.

셋째, 정보통신 기술과 융합한 사기 수법을 이용한다.⁴⁾ 사기범은 피해자의 단말기에서 금융정보를 탈취하거나 전화번호를 가로채는 앱을 제작하여 배포한다. 단말기를 해킹하여 정상적인 홈페이지 대신 피싱사이트로 연결되도록 한다. 또한, 전화번호 변작중계기, 방화벽 등 고도화된 정보통신 기술을 활용하기도 한다.

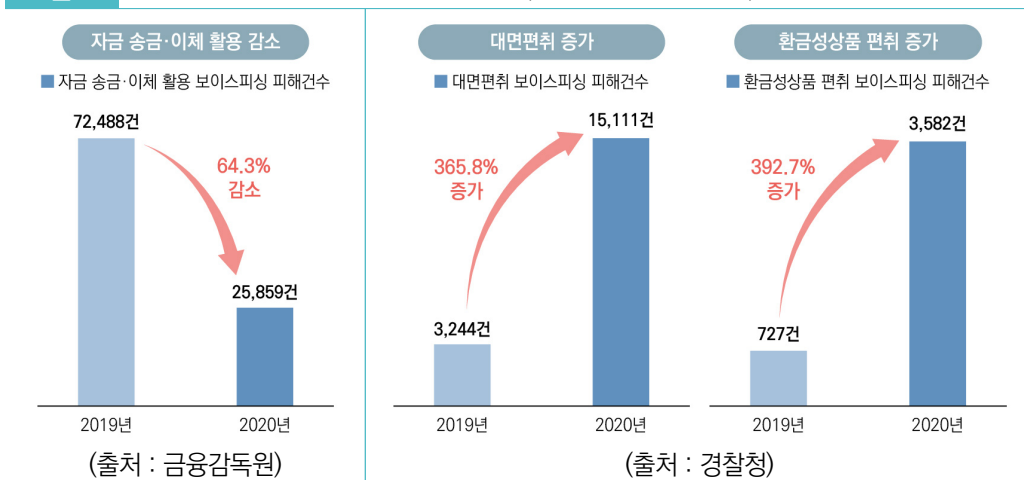
넷째, 금융회사 등의 전자금융거래 및 전기통신금융사기 관련 예방 정책을 신속히 파악하고 있다. 출금 또는 이체 등 거래 테스트를 통해 거래금액의 최대한도, 거래의 최대 횟수를 파악하거나 금융회사에서 새로운 보이스피싱 대응 시나리오 적용 시, 얼마 지나지 않아 회피 수법이 등장하곤 한다.

4) 금융감독원에 따르면 2020년에 보이스피싱 피해금 이체 경로는 모바일/인터넷뱅킹이 75.2%로 대부분을 차지하여 금융의 디지털·모바일화 진전 정도를 보여준다[1]. 이는 사기범이 정보통신 기술을 활용하는 배경이 되고 있다.

최근에는 금융권의 보이스피싱 예방 및 대응 강화로 자금 송금·이체보다는 대면 편취로 그 수법이 변화되고 있다. 금융감독원에 따르면 2019년도에 비해 2020년도에는 자금 송금·이체 활용 보이스피싱 피해건수는 약 3분의 1로 줄었으며[1] 경찰청에 따르면 대면편취를 통한 보이스피싱은 5배 가까이 급증하였다.⁵⁾

마지막으로, 자금세탁과 결부된다. 자금흐름 모니터링을 우회하기 위해 대포통장이나 전자지급수단, 가상자산 등을 활용하여 피해금을 세탁한다. 경찰청에 따르면 환금성 상품 편취를 통한 보이스피싱은 2019년도에 비해 2020년도에 약 5배 급증하였다.⁵⁾

그림 3 전기통신금융사기 범행 수법의 추이(2019년 → 2020년)



최근에 주로 나타나는 신종 사기 수법을 이용한 보이스피싱 사기 사례를 [표 3]에 정리하였다[4]. 원격제어나 전화번호 가로채기 등 정보통신 기술과 융합되거나 오픈뱅킹, 알뜰폰 등 편의성 중심의 서비스를 악용한 사례가 있다.

5) 이데일리, 계좌 이용 막자 직접 만나서...보이스피싱 수법 확 변했다, 2021.2.

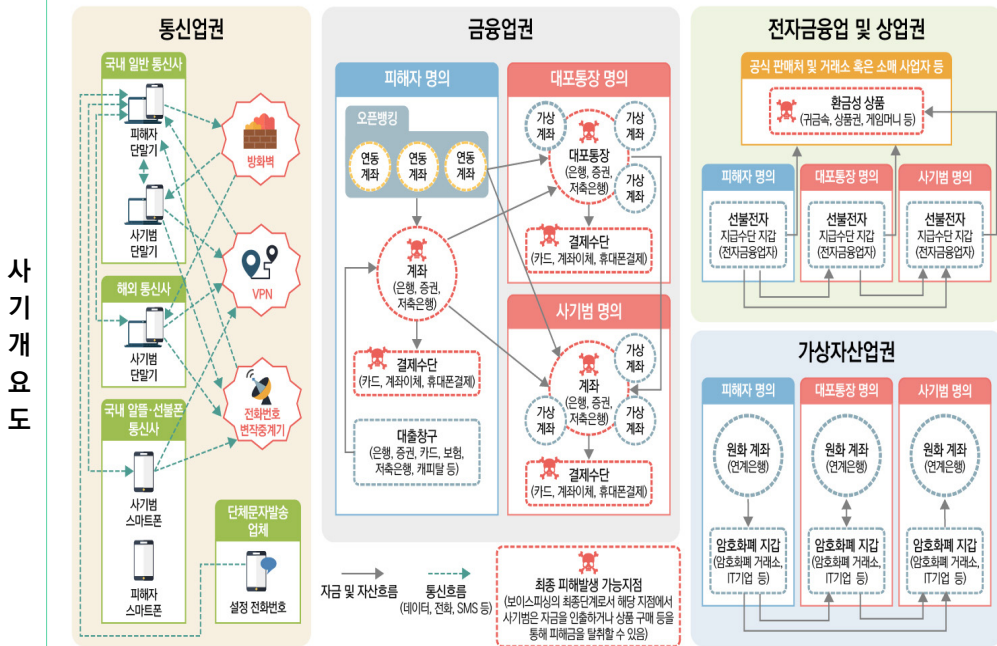
표 3 신종 보이스피싱 사기 사례

사기 사례	주요 내용
원격제어앱을 악용한 사기 사례	사기범은 경찰을 사칭하여 피해자로 하여금 휴대폰에 구글 앱스토어에서 원격 제어앱(팀뷰어)을 설치하도록 한 후 피해자 휴대폰을 장악하여 전자금융앱에서 금전 이체함
전화번호 가로채기 악성앱을 악용한 사기 사례	사기범은 대출을 제안하고 신용점수가 부족하여 대출을 발생시켜 갚는 방법으로 신용등급을 올리면 된다는 사기범의 전화를 받음. 피해자는 사기범의 요구에 따라 가짜 대출앱(전화번호 가로채기 악성앱)을 설치한 뒤 신용점수를 올리기 위해 OO카드사로부터 카드를 받고 상환하기 위해 OO카드사 대표전화로 전화함. 전화번호를 가로챈 사기범은 카드론 상환을 위해 다른 계좌로 금전 이체를 요구하였고 피해자는 대출금을 사기범이 지정하는 계좌로 이체함
알뜰폰 개통을 악용한 사기 사례	사기범이 취업 등을 미끼로 피해자의 신분증 등을 갈취하고, 이 정보를 이용하여 알뜰폰을 개통하고 이를 피해자 명의의 휴대폰으로 금융회사에 등록하여 대포 통장으로 간편송금함
오픈뱅킹을 악용한 사기 사례	사기범은 피해자 스마트폰에 원격제어앱을 설치하고, 스마트폰을 원격제어 하여 피해자 명의의 △△증권 계좌를 비대면 개설함. 사기범은 △△증권 모바일 앱의 오픈뱅킹 기능을 이용해 피해자 명의의 타 금융회사 계좌 잔액을 △△증권 계좌로 이체 후, △△증권에 입금된 피해자의 자금을 대포통장으로 이체함

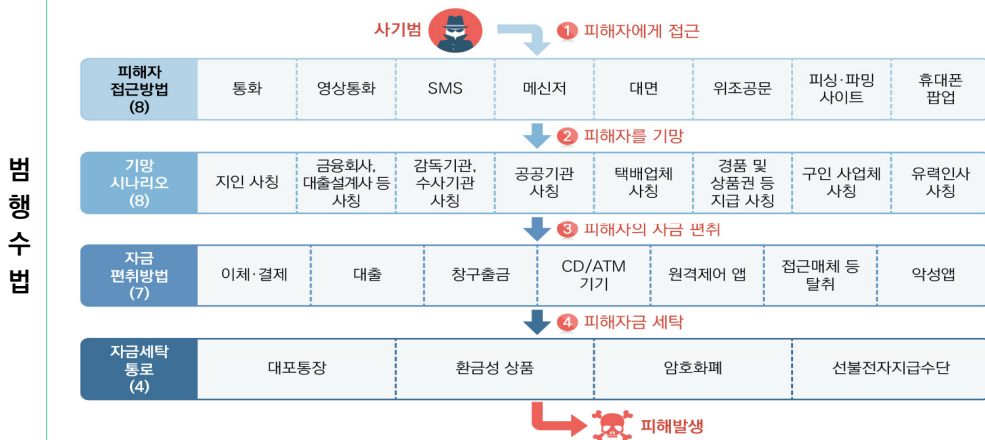
III 전기통신금융사기 피해사례 분석 프레임워크

금융보안원이 보이сп이스킹 피해사례를 효율적으로 분석하기 위하여 활용하고 있는 프레임워크는 [그림 4]와 같다.

그림 4 전기통신금융사기 피해사례 분석 프레임워크



* 확대 그림 : 81페이지 참고



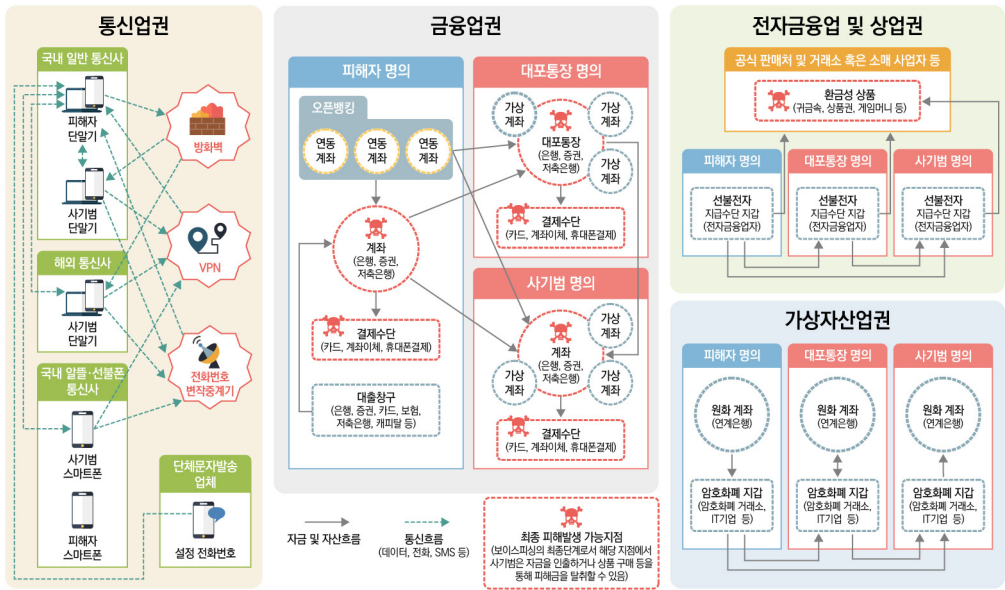
전기통신금융사기 피해사례 분석 프레임워크는 사기 개요도와 범행 수법으로 구성되며, 사기 개요도 및 범행 수법은 각각 개별적인 피해사례의 자금흐름 측면과 범행 수법 측면을 설명한다.

사기 개요도는 사기범이 피해자에게 접근하는 첫 단계부터 자금을 편취하고 자금을 세탁하는 마지막 단계까지의 과정 중에서 발생하는 자금 및 통신의 흐름을 도식화하여 표현한다. 자금의 흐름이란 보이스피싱 피해금이나 피해금을 세탁하기 위해 피해금으로 구매한 암호화폐, 선불전자지급수단 등을 의미하며 검은색 실선으로 표시된다. 통신의 흐름이란 사기범이 피해자에게 접근 시 활용하는 전화나 SMS, 또는 피해자가 사기범에게 전달하는 개인·금융정보 등 데이터의 흐름, 피해자 단말기에서 बैं킹앱을 통해 은행계좌에 접근하는 데이터의 흐름 등을 의미하며 연두색 점선으로 표시된다. 또한, 금융업권과 통신업권, 전자금융업 및 상업권, 가상자산업권을 포함한다. 각 업권은 사기범의 피해자금 탈취대상, 피해자 접근 및 기망 수단, 피해자금 세탁 통로로써 활용되며 자금 및 통신의 흐름을 설명하기 위한 필수적인 요소를 포함한다. 예를 들어 통신업권의 경우 단말기, 방화벽, VPN 등을 포함하며 금융업권의 경우 계좌, 결제수단, 대출창구 등을 포함한다. [그림 4]에서 빨간색 점선으로 표시된 최종 피해발생 가능 지점에서 사기범은 자금을 인출하거나 상품 구매 등을 통해 피해금을 최종적으로 탈취할 수 있다.

범행 수법은 피해사례의 처음부터 마지막까지를 피해자 접근, 기망, 자금 편취, 자금세탁의 4단계로 구분하고 각 범행단계별로 사기범이 활용하는 구체적인 수법들을 포함한다. 예를 들어 피해자 접근방법의 경우 통화, SMS, 피싱·파밍사이트 등 총 8개 방법이 있으며, 자금세탁 통로의 경우 대포통장, 암호화폐 등 총 4개 통로를 포함한다. [그림 4]에서 이러한 세부 수법들을 이용하여 사기범이 각 단계에서 어떠한 범행 수법을 사용했는지 설명한다.

1. 사기 개요도

그림 5 사기 개요도



* 확대 그림 : 81페이지 참고

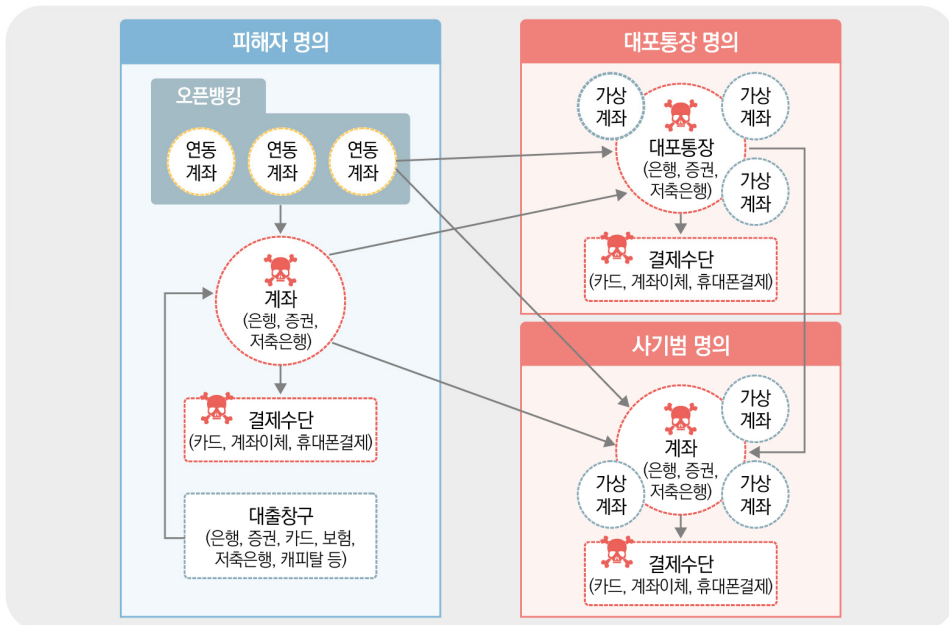
[그림 5]의 사기 개요도는 전기통신금융사기 발생 과정에서 나타나는 자금(또는 자산) 및 통신흐름을 단방향 또는 양방향 화살표로 표시하며 이는 실제 피해사례에서 자주 발생하는 자금 및 통신 흐름과 같다. 전기통신금융사기가 주로 발생하는 금융업권, 통신업권, 전자금융업 및 상업권, 가상자산업권을 포함하며 각 업권의 피해사례를 분석하기 위해 필요한 요소를 포함한다. 예를 들어 통신업권에는 단말기, 금융업권에는 계좌나 대포통장, 가상자산업권에는 암호화폐 지갑 등이 포함된다. 대다수 요소는 사기 발생과정 중 주요 주체라고 할 수 있는 피해자와 사기범 및 대포통장 명의인으로 소유자가 구분된다.

지금부터 사기 개요도에 표시된 금융업권, 통신업권, 전자금융업 및 상업권, 가상자산업권을 순서대로 상세히 설명하고자 한다.

가. 금융업권

금융업권은 계좌 등 자금을 송금·인출하거나 대출창구 등 자금을 빌리거나 결제 수단 등 자금을 결제할 수 있는 요소가 존재하기 때문에 사기범이 피해자금을 탈취하는 대상이 된다.

그림 6 금융업권의 사기 개요도



모든 요소들은 피해자와 사기범, 대포통장 명의인 소유로 구분되며 [표 4]와 같이 오픈뱅킹 연동계좌, 가상계좌 등을 포함하여 총 7개의 주요 요소로 구성된다.

표 4 금융업권 주요 요소 설명

주요 요소	설명
피해자 계좌	전기통신금융사기의 주 탈취 대상이 되는 피해자 명의의 계좌
오픈뱅킹 연동계좌	한 기관의 금융앱을 통해 여러 타 금융회사의 계좌를 조회하고 결제·송금 등을 할 수 있는 오픈뱅킹 서비스에 연동된 계좌. 해당 앱에 하나의 계좌 등록 후 본인인증 시,

주요 요소	설명
	피해자 명의의 모든 계좌를 등록하여 조회·이체 등의 업무가 가능하여 최근 사기범들의 표적이 됨
결제수단	카드, 계좌이체, 휴대폰 결제 등의 결제수단으로서 현금성 상품구매를 위한 수단으로 주로 이용됨
대출창구	은행, 증권, 카드, 보험, 저축은행, 캐피탈 등 피해자가 대출을 받을 수 있는 모든 기관의 대출창구로서 대출형 전기통신금융사기의 표적이 됨
대포통장	사기범이 명의를 도용한 계좌로서 금융경로의 추적을 피하고자 사기범이 제3자 명의의 계좌를 모집하여 대포통장으로 이용된다. 대포통장 거래 등 보이스피싱 범죄 가담 시 관련 처벌 규정(전자금융거래법 위반 또는 사기죄)에 의거하여 처벌되나, 이에 대한 인식이 미흡하여 일반인이 사기범으로부터 수수료를 약속받고 대포통장을 대여하여 보이스피싱 사기에 공모함 ⁵⁾
사기범 계좌	사기범 명의의 계좌로서 추적을 피하고자 자금세탁 통로를 거쳐 피해금을 사기범 계좌로 입금 받음. 사기범 계좌로 입금 받지 않고 피해자 계좌 또는 대포통장에서 출금한 피해금을 현금으로 탈취하는 경우도 다수임
가상계좌	인터넷쇼핑몰 등 여러 고객에게서 대금을 받는 업체가 고객에게 부여하는 고객 명의의 임시계좌이다. 업체 명의의 모계좌와 동일한 계좌이지만 계좌번호와 명의만 별도임. 실제 계좌 소유주인 모계좌의 명의인과 별개의 명의라는 점을 이용해 자금세탁을 목적으로 대포통장처럼 쓰이거나 피해자와 동일한 명의라는 점을 이용해 피해자 계좌인 것처럼 기망하여 자금을 입금받아 탈취하는 데에 활용됨 ⁶⁾

나. 통신업권

통신업권은 사기범이 피해자의 단말기에 접근하여 피해자를 기망하는 수단으로 활용된다. 단말기는 피해자와 사기범 명의로 구분되며 피해발생 양상이나 개통 과정 등에 차이가 있어 국내 일반 통신사와 국내 알뜰·선불폰 통신사, 해외 통신사로 구분하였다. 그 외에 사기범이 활용하는 VPN, 전화번호 변작중계기 등 정보 통신 기기를 포함하여 [표 5]와 같이 총 7개의 주요 요소로 구성하였다.

6) SBS, 범죄 악용되는 가상 계좌...금융실명제 사각지대, 2014.10. / 조선비즈, 가상계좌 국민 1인당 164개... 자칫 하면 털립니다, 2014.8.

그림 7 통신업권의 사기 개요도

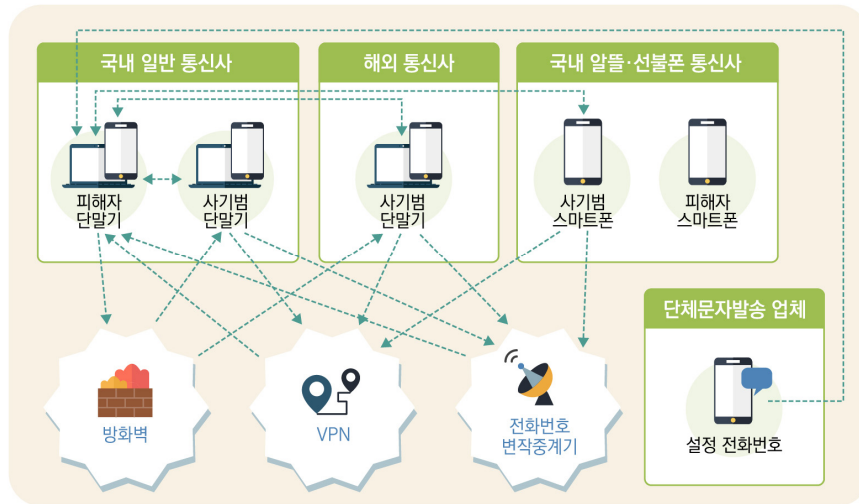


표 5 통신업권 주요 요소 설명

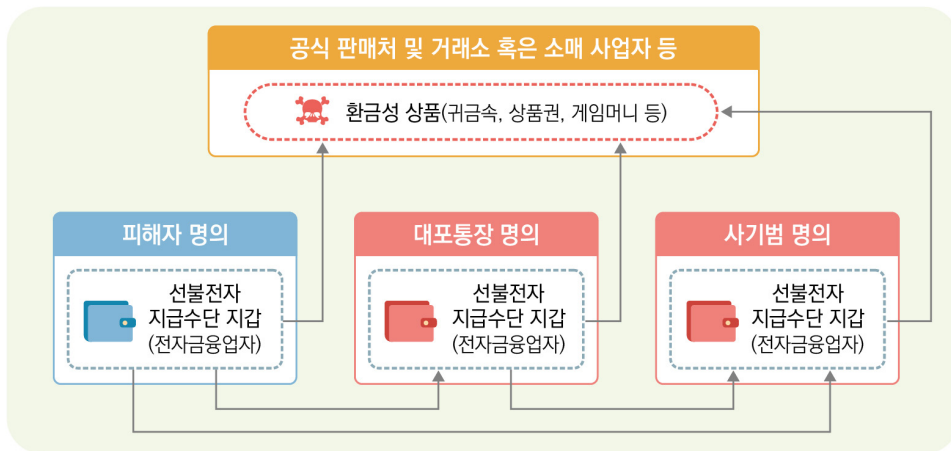
주요 요소	설명
피해자 단말기 (국내 일반 통신사)	국내에서 일반적으로 이용되는 피해자의 PC 또는 스마트폰으로서 전기통신금융 사기의 첫 공격 대상이 됨
사기범 단말기	사기에 이용되는 사기범의 PC 또는 스마트폰으로서 크게 세분류(국내 일반 통신사, 해외 통신사, 알뜰·선불폰 통신사)로 나뉨
피해자 단말기 (알뜰·선불폰)	알뜰·선불폰 통신사에서 개통된 피해자 명의의 단말기로서 피해자 명의 본인인증 등에 활용하기 위해 사기범이 피해자의 개인정보를 탈취하여 개통함
단체문자발송 업체	사기범이 단체 피싱문자 발송 등을 위해 이용함
방화벽	사기범이 운영하는 방화벽으로서 피해자가 피싱사이트 등에 접속할 때, 사기범이 피해자의 IP를 질의 후 등록하여 방화벽 등록 후 피싱사이트에 접속가능하도록 함. 이는 금융 보안원, KISA, 보안업체 등의 피싱사이트 탐지를 회피하고자 활용됨
VPN	가상사설망 서비스로서 사기범은 이를 통해 IP우회를 함
전화번호 변작중계기	전화번호를 변조하는 중계기로서 해외전화번호·인터넷전화번호를 국내번호 (010)로 변조할 때 이용됨. 변작된 발신번호를 ISP에서 이용중지하더라도 사기범은 또 다른 번호로 변조하여 범행을 실시할 수 있음

7) 국내 일반 통신사 : 국내개통 사기 이용 단말기 / 해외 통신사 : 해외개통 사기 이용 단말기(중국 및 동남아 국가가 다수를 차지함) / 알뜰·선불폰 통신사 : 국내개통 사기 이용 스마트폰 + 전화번호 차단을 우회하기 위해 사기범이 제3자 명의(외국인 포함)를 도용하여 개통한 대포폰

다. 전자금융업 및 상업권

전자금융업 및 상업권은 사기범이 선불전자지급수단⁸⁾이나 환금성 상품을 통해 피해자금을 세탁하는 통로로 이용된다. 선불전자지급수단을 통해 환금성 상품을 구매하여 자금을 탈취하는 경우가 많아 전자금융업권과 상업권을 같이 묶어서 표현하였다.

그림 8 전자금융업 및 상업권의 사기 개요도



선불전자지급수단 지갑은 피해자, 사기범, 대표통장 명의로 구분되며 [표 6]과 같이 총 2개의 주요 요소로 구성된다.

표 6 전자금융업 및 상업권 주요 요소 설명

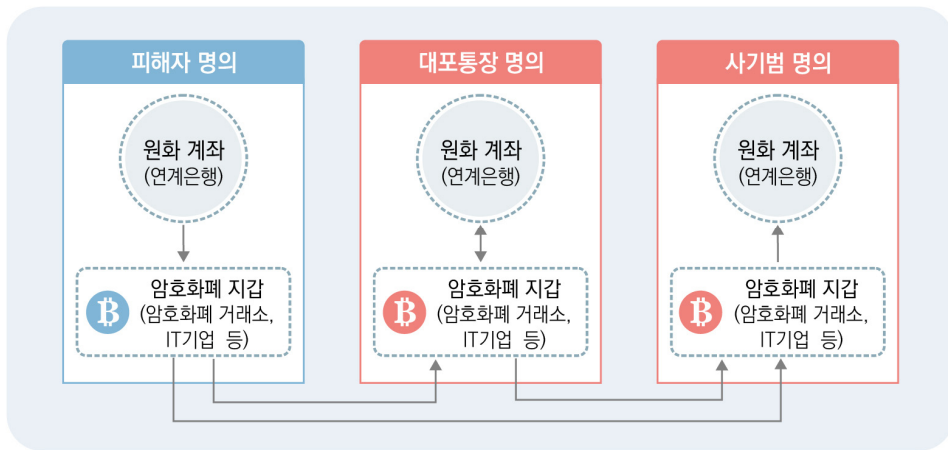
주요 요소	설명
환금성 상품	귀금속, 상품권, 게임머니 등 환금성이 높아 피해자금 세탁의 수단으로 이용되며 공식 판매처 ⁹⁾ 뿐 아니라 소규모 판매업자 ¹⁰⁾ 가 많이 존재하여 예방에 어려움이 있음 ¹¹⁾
선불전자지급 수단 지갑	전자금융업자가 발행한 선불전자지급수단을 저장하기 위해 전자금융업자가 관리하는 가상의 계좌이며 환금성이 높아 피해자금 세탁의 수단으로 이용됨

8) 전자적 방법에 따라 금전적 가치가 저장되어 있는 증표로서 전자금융업자에 따라 결제 수단만 지원하거나 타 명의인의 지갑에 이체하는 기능까지 제공하기도 함

라. 가상자산업권

가상자산업권은 사기범이 암호화폐를 통해 피해자금을 세탁하는 통로로 이용된다.

그림 9 가상자산업권의 사기 개요도



[표 7]과 같이 원화 계좌와 암호화폐를 저장하는 지갑을 포함하여 총 2개의 주요 요소로 구성되며 각 요소는 피해자, 사기범, 대포통장 명의로 구분된다.

표 7 가상자산업권 주요 요소 설명

주요 요소	설명
암호화폐 지갑	암호화폐를 저장하기 위해 암호화폐 거래소·IT기업 등이 관리하는 저장소이며 암호화폐 송금의 익명성 및 높은 환금성으로 인해 피해자금 세탁의 수단으로 이용됨
원화 계좌 (연계은행)	특정 암호화폐 거래소와 연계되어 고객의 암호화폐 구입자금(원화)을 보관하는 시중 은행 계좌. 일부 거래소는 연계 시중은행에 고객의 실명계좌를 두지 않고 거래소의 법인 계좌를 이용하여 고객의 암호화폐 거래를 중개하고 있어 피해자금 세탁에 더욱 취약함 ¹²⁾

9) 금거래소 또는 게임사 공식사이트 등 일원화된 구매채널

10) 금은방의 귀금속 판매, 편의점 및 카페의 기프트카드 판매, 상품권판매업체, 기프트콘 발송업체 등 소규모 구매채널

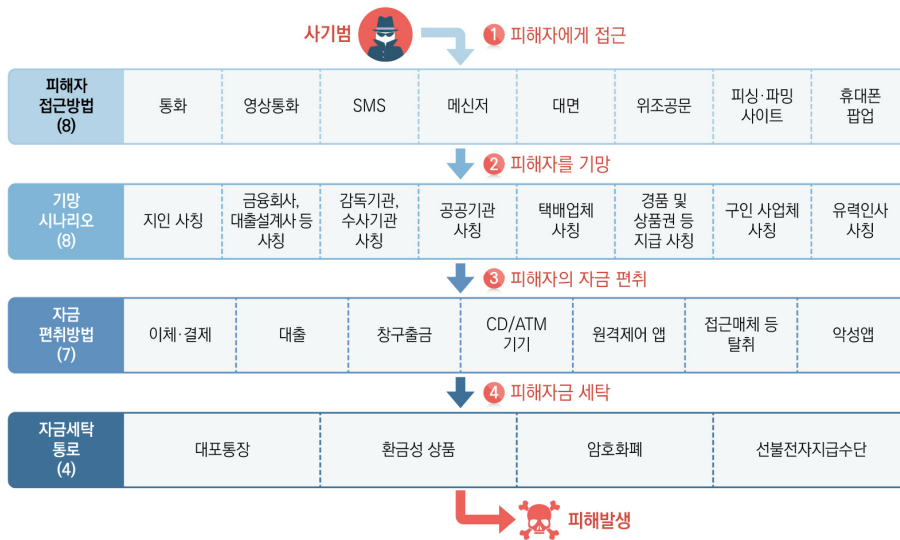
11) MBN, [단독] “금괴로 돈세탁”...금은방 신고로 잡혔다, 2020.11.

전라일보, 구글 기프트카드 악용 보이스피싱 ‘주의보’, 2021.6.

12) 서울경제, [S머니] 제도권 들어온 암호화폐...200여 거래소·잡코인 정리되나, 2020.3.

2. 범행 수법

그림 10 범행 수법



전기통신금융사기의 범행 단계를 사기범이 피해자에게 접근하는 단계, 피해자를 기망하는 단계, 피해자의 자금을 편취하는 단계, 피해자금을 세탁하는 단계로 구분하고 각 단계별로 세부 범행 수법을 나열한다. 피해자 접근방법부터 기망 시나리오, 자금 편취방법, 자금세탁 통로 순으로 범행이 진행되며 각 단계에서 어떠한 범행 수법을 사용했는지 표시한다. 실제 피해사례에서는 사기범이 각 단계별로 여러 범행 수법을 사용하는 경우도 많다. 범행 수법을 단계별로 나누어 피해자 접근방법, 기망 시나리오, 자금 편취방법, 자금세탁 통로 순으로 상세히 설명하고자 한다.

가. 피해자 접근방법

피해자 접근방법은 범행의 첫 단계에서 사기범이 피해자에게 접근하는 채널이다. 과거에는 전화나 SMS 등이 주로 이용되었지만 현재는 이외에도 영상통화나 메신저, 휴대폰 팝업 등이 이용되며 [표 8]과 같이 총 8개 방법으로 구성된다.

표 8 피해자 접근방법 설명

피해자 접근방법	설명
통화	사기조직에서 피해자에게 전화를 걸거나 문자, SMS 등을 통해 피해자가 전화를 하도록 유도하는 방법
영상통화	사기조직에서 피해자에게 영상전화를 걸거나 문자, SMS, 일반통화 등을 통해 피해자가 영상통화를 하도록 유도하는 방법
SMS	사기조직에서 피해자에게 문자메시지를 발송하여 접근하는 방법
메신저	컴퓨터 혹은 모바일 메신저를 통해 피해자에게 접근하거나 악성앱을 설치하도록 유도하는 방법
대면	수사기관, 금융당국 담당자를 사칭하여 통화, SMS 등으로 피해자를 기망한 후 대면으로 접촉하는 방법
위조공문	금융당국, 수사기관 등을 사칭한 위조공문을 송부하는 방법
피싱·파밍 사이트	금융회사, 유관기관, 수사기관, 포털 등을 모사한 피싱·파밍사이트를 만들어 피해자로 접근하게 하여 개인·금융 정보를 수집하거나 악성앱 등을 다운로드 받도록 하는 방법
휴대폰 팝업	피해자의 휴대폰에 악성앱을 실행하여 금융앱이 실행되는 시점에 금융회사 등을 사칭한 악성 팝업창이 실행되도록 하는 방법

나. 기망 시나리오

기망 시나리오는 사기범이 피해자를 속이기 위해 사용하는 수법이며 주로 특정인 혹은 기관 등을 사칭하는 형태로 발생한다. 과거에는 지인 사칭이나 금융회사 사칭 등이 주로 이용되었지만 최근에는 국민지원금 지급이나 백신 접종과 관련된 기관을 사칭하는 사례나 구인 사업체 등을 사칭하는 사례도 발생하며 [표 9]와 같이 총 8개 시나리오로 구성된다.

표 9 기망 시나리오 설명

기망 시나리오	설명
지인 사칭	지인(가족, 친구, 회사동료 등)을 사칭하여 협박, 자금유통 등의 상황을 가장하여 자금 편취하는 시나리오

기망 시나리오	설명
금융회사, 대출설계사 등 사칭	금융회사 혹은 대출상담사 등을 사칭하여 대환대출 등을 미끼로 자금 편취하는 시나리오
감독기관, 수사기관 사칭	검찰·경찰 등 정부기관을 사칭하여 피해자가 범죄에 연루되었다는 등의 수법으로 협박하여 금전이나 접근매체를 편취하는 시나리오
공공기관 사칭	건강보험료·국민지원금·백신접종 등 주요 공공업무를 수행하는 기관을 사칭하여 피해자의 개인정보를 요구하는 시나리오
택배업체 사칭	택배업체를 사칭하여 피해자의 개인정보를 요구하는 시나리오
경품 및 상품권 등 지급 사칭	경품이나 상품권·예매권·교환권 등 지급을 사칭하며 피해자의 개인정보를 요구하는 시나리오
구인 사업체 사칭	취업희망자 대상으로 구인 사업체를 사칭하여 피해자를 거짓으로 채용하고 업무상의 이유로 금전이나 접근매체, 본인확인수단 등을 요구하는 시나리오
유력인사 사칭	정치인 등 유력인사를 사칭하여 금전을 요구하는 시나리오

다. 자금 편취 방법

자금 편취방법은 사기범이 피해자에게 접근하고 기망에 성공한 후 피해자의 자금을 탈취하는 방법이다. 자금 이체뿐 아니라 대면으로 자금을 편취하거나 원격 제어 앱을 통해 사기범이 직접 피해자의 단말기를 조종하여 이체를 실행하는 방법을 사용하기도 한다. 자금 편취방법은 [표 10]과 같이 총 7가지 방법으로 구성된다.

표 10 자금 편취방법 설명

자금 편취방법	설명
이체·결제	피해자로 하여금 본인 계좌의 금원을 이체하거나 상품 등을 결제토록 하는 방법
대출	피해자로 하여금 대출을 유도하여 이를 이체하거나 상품 등을 결제토록 하는 방법
창구출금	피해자가 창구를 통해 현금을 출금토록 하여 이를 갈취하는 방법
CD/ATM 기기	피해자 또는 인출책 등이 CD/ATM기기에서 피해자 소유의 현금을 출금하거나 이체하여 이를 갈취하는 방법

자금 편취방법	설명
원격제어 앱	피해자가 원격제어 앱을 설치하도록 하여 금전 탈취, 휴대폰 내 금융·개인정보를 탈취하고 악성앱 등을 설치하는 방법
접근매체 등 탈취	공인인증서, OTP 번호, 비밀번호 등 접근매체나 신분증 등 본인확인 수단을 갈취하여 피해자의 बैं킹 계정에 접속하거나 피해자 명의 휴대폰을 개설, 비대면 계좌개설 등을 통해 자금을 편취하는 방법
악성앱	가로채기 전화번호 기능, 개인정보·금융정보 유출 기능, 키로깅 기능, 공인인증서 유출, DNS설정이나 hosts파일 ¹³⁾ 변조 기능 등을 가진 악성앱을 통해 자금을 편취하는 방법

라. 자금 세탁 통로

자금세탁 통로는 사기범이 금융회사 등의 감시망을 피해 탈취한 피해금을 세탁하는 수단이다. 과거에는 사기범이 모집한 제3자 명의인의 대포통장을 이용하는 사례가 많았으나 현재는 금융업권에서 벗어나 익명성이 강한 암호화폐나 환금성 상품 등을 구매하여 자금을 세탁하는 사례도 많이 발생하며 [표 11]과 같이 총 4개의 통로로 구성된다.

표 11 자금세탁 통로 설명

자금세탁 통로	설명
대포통장	사기범이 사전에 모집한 공범의 계좌로 피해자금을 이체하여 세탁하는 수단
환금성 상품	피해자금으로 귀금속, 상품권, 게임머니 등 환금성 상품을 구매하여 현금하거나 다른 상품을 구매하여 자금을 세탁하는 수단
암호화폐	피해자금으로 암호화폐를 구입하고 사기범(또는 대포통장 명의인)의 지갑으로 이체 후 판매하여 현금을 탈취함으로써 자금을 세탁하는 수단
선불전자지급 수단	피해자금으로 선불전자지급수단(000머니, 000포인트 등)을 충전하여 사기범(또는 대포통장 명의인)의 지갑으로 이체 후 현금하거나 다른 상품을 구매하여 자금을 세탁하는 수단

13) 문자형태의 인터넷도메인(<http://www.naver.com>)과 숫자형태의 IP주소(125.209.222.142)를 연결하는 설정 및 파일

3. 피해사례 분석 예

암호화폐 구매를 통한 전기통신금융사기 가상사례를 제시하여 금융보안원이 프레임워크를 이용하여 피해사례를 어떻게 분석하는지 설명하고자 한다.

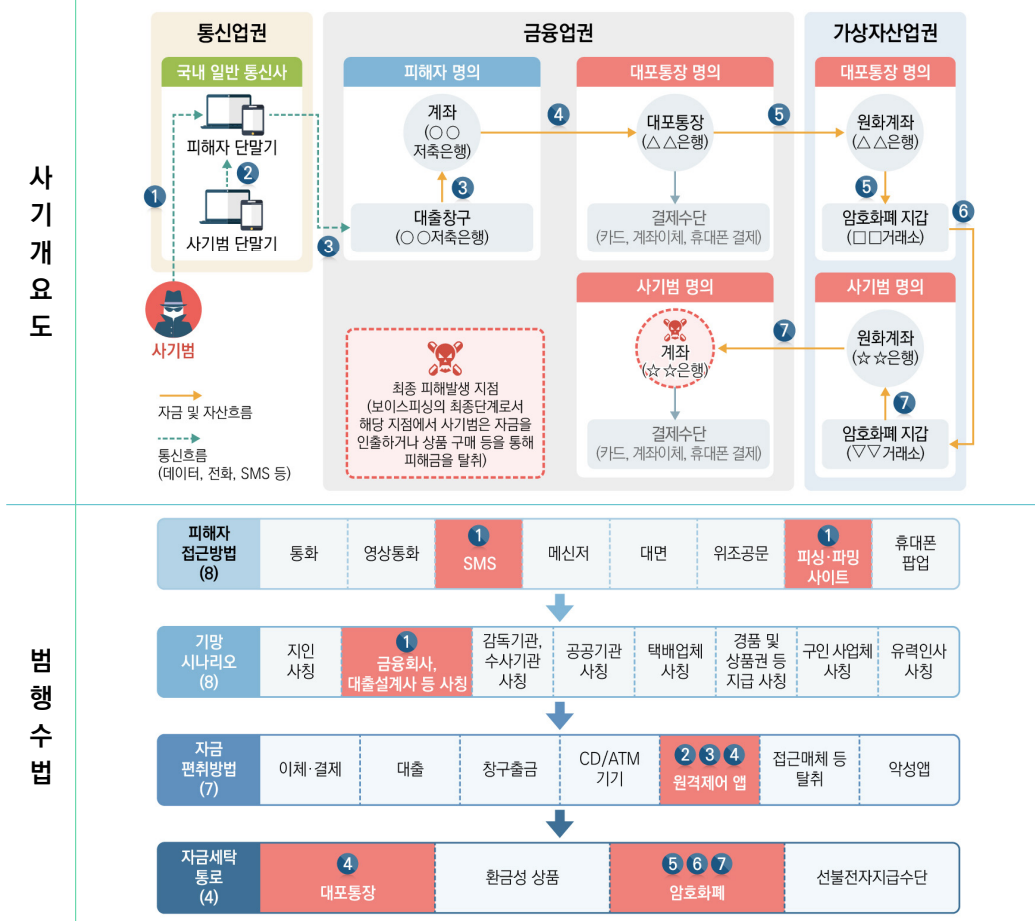
먼저, 우선적으로는 피해사례의 전체 과정을 이해하기 쉽도록 [표 12]와 같이 총 7단계로 구분한다. 피싱사이트 링크를 배포하고 원격제어 앱을 설치하도록 하여 자금을 편취 후 암호화폐를 통해 자금을 세탁하는 과정을 단계별로 설명하고 있다.

표 12 암호화폐 구매를 통한 전기통신금융사기 피해사례

범행단계	설명
① 피싱사이트 링크 배포	사기범은 SMS를 통해 금융회사 사칭 피싱사이트 링크를 배포
② 원격제어 앱 설치	해당 피싱사이트를 통해 피해자로 하여금 원격제어앱을 설치하도록 하고 해당 앱을 통해 피해자 단말기에 대한 원격조정권한 획득
③ 원격제어 : 대출실행	사기범은 피해자의 단말기를 원격제어하며 사전에 탈취한 피해자의 개인정보(계좌정보, 카드정보, 비밀번호 등)를 이용해 ○○저축은행에서 대출 실행
④ 원격제어 : 대모통장 이체	대출금(피해금)을 사기범이 사전에 모집한 공범의 대모통장으로 이체
⑤ 암호화폐 구입	공범은 □□거래소를 통해 피해금으로 암호화폐 구입
⑥ 암호화폐 이체	구입한 암호화폐를 사기범의 ▽▽거래소 암호화폐 지갑으로 이체
⑦ 사기범 계좌 이체	사기범은 해당 암호화폐를 팔아 원화를 ☆☆은행의 본인 계좌로 이체 후 현금 출금하여 탈취

다음으로는 7단계로 구분된 범행과정을 [그림 11]와 같이 단계별 숫자로 프레임워크에 표시한다. 범행과정 7단계를 프레임워크의 사기 개요도와 범행 수법에 모두 표시하며 전자는 자금 및 통신의 흐름을 나타내고 후자는 각 범행단계별로 사용되는 세부 범행 수법을 나타낸다.

그림 11 암호화폐 구매를 통한 전기통신금융사기 피해사례의 프레임워크 적용



① 단계에서는 사기범이 금융회사를 사칭하여 피싱사이트 링크가 포함된 SMS를 피해자에게 배포한다. 이는 사기 개요도 상에서 사기범으로부터 피해자 단말기로의 통신흐름으로 표시하며 프레임워크 내 범행 수법에서는 피해자 접근방법과 기망 시나리오에 각각 SMS, 피싱·파밍사이트 및 금융회사, 대출설계사 등 사칭으로 표시한다.

② 단계에서는 피해자 기망에 성공한 후 사기범이 피해자 단말기에 원격제어 앱을 설치하여 원격조정권한을 획득하는 것을 사기 개요도 상 사기범 단말기에서 피해자 단말기로의 통신흐름으로 표시한다.

③ 단계에서는 사기범이 피해자 단말기를 원격제어하여 피해자 명의의 ○○저축

은행 대출창구로 접근하여 대출을 실행하고 대출금을 ○○저축은행 계좌로 입금 받는다.

④ 단계에서는 해당 피해금을 △△은행의 대포통장으로 이체한다. 이는 범행 수법 상 대포통장을 이용한 자금세탁을 위한 것이다.

⑤ 단계에서 대포통장 명의인은 암호화폐를 구입하기 위해 □□거래소와 연계된 원화 계좌로 피해금을 입금한 후 암호화폐를 구입한다.

⑥ 단계에서 해당 암호화폐를 ▽▽거래소에 위치한 사기범의 암호화폐 지갑으로 이체한다.

⑦ 단계에서 사기범은 암호화폐 팔아 ☆☆은행의 본인 계좌에 원화로 이체한 후 현금으로 출금하여 피해금 탈취에 성공한다.

②·③·④단계는 범행 수법 중 원격제어 앱을 이용한 자금 편취방법을 이용한 것이다. ⑤·⑥·⑦단계는 범행 수법 중 암호화폐를 통한 자금세탁이 목적이다.

마지막으로는 프레임워크를 이용해 각 범행 단계별로 관련된 기관이 피해 예방을 위해 보완해야 할 사항을 [표 13]과 같이 고려할 수 있다.

표 13 사기 예방 관련 기관별 보완사항

범행단계	기관별 보완사항
① 피싱사이트 링크 배포	(해당 사항 없음)
② 원격제어 앱 설치	(백신업체) 고객 스마트폰에서 원격제어앱 설치 시도 탐지 시, 알람 경고 및 설치 시도 중지
③ 원격제어 : 대출실행	(○○저축은행) 고객 스마트폰에서 원격제어앱 실행 탐지 시, 자사 모바일앱 통한 금융 업무 제공 중지
④ 원격제어 : 대포통장 이체	(○○저축은행) 발견된 특징*에 대한 이상금융거래 모니터링 강화 * 대출 실행 직후 타 명의인의 계좌로 대출금 전액 송금 (△△은행) 대포통장 모니터링 강화
⑤ 암호화폐 구입	(△△은행) 발견된 특징*에 대한 이상금융거래 모니터링 강화

범행단계	기관별 보완사항
	* 타 명의인의 계좌로부터 자금 입금 직후 해당 자금을 암호화폐거래소 전용 계좌로 송금 (정보공유 업무협조를 통해 ④단계에서 △△은행으로 입금된 자금이 ○○저축은행의 대출금임을 △△은행에서 확인할 수 있다면 모니터링 정확도 향상) (□□거래소) 사기의심 계정 모니터링 강화
⑥ 암호화폐 이체	(□□거래소) 지갑 간 코인 송금 시 수취인의 성명과 지갑 주소를 파악하여 자금세탁 여부 모니터링 강화
⑦ 사기범 계좌 이체	(▽▽거래소) 사기의심 계정 모니터링 강화 및 발견된 특징*에 대한 이상금융거래 모니터링 강화 * 타 명의인의 지갑으로부터 암호화폐 입금 직후 암호화폐를 매도하여 고액의 원화를 본인의 은행계좌로 이체

② 단계에서는 피해자 단말기에 원격제어 앱이 설치될 시, 피해자 단말기에 설치된 백신에서 경고 알람을 띄우거나 설치를 중지해야 한다.

③ 단계에서는 원격제어 앱이 실행 중인 단말기에서 ○○저축은행으로부터 대출을 받기 위해 ○○저축은행 앱 실행 시, 앱에서 원격제어 앱 실행여부를 탐지하여 자사 बैं킹 앱을 종료시키도록 해야 한다.

④ 단계에서는 ○○저축은행에서 대출 직후, 대출금 전액을 타 명의인의 계좌로 송금하는 것에 대한 이상금융거래 모니터링을 통해 거래를 차단해야 하며, △△은행에서는 모니터링을 통해 대포통장 계좌에 대한 지급정지 조치를 해야 한다.

⑤ 단계에서 △△은행은 타 명의인으로부터 자금 입금 직후 해당 자금을 암호화폐 거래소 전용 계좌로 송금하는 것에 대한 이상금융거래 모니터링을 통해 거래를 차단해야 하며, 이때 해당 자금이 ○○저축은행으로부터 대출된 직후 이체된 자금이라는 것을 △△은행과 ○○저축은행 간 정보공유를 통해 파악할 수 있다면 모니터링의 오탐률을 낮출 수 있다. 또한 □□거래소에서는 과거 거래내역 등을 분석하여 사기의심 계정에 대한 모니터링을 실시하여 계정정지 조치를 해야 한다.

⑥ 단계에서 □□거래소는 트래블룰¹⁴⁾에 따라 발신자와 수신자의 신원정보를 파악하고 사기의심 거래자일시 해당 거래가 자금세탁 여부인지에 대한 모니터링을

14) 암호화폐거래소 내 지갑이 외부 지갑과 암호화폐를 주고받을 때, 발신자와 수신자의 신원과 거래내역을 가상자산 사업자가 보관하게 의무화하는 제도

실시하고 거래를 차단해야 한다.

⑦ 단계에서 ▽▽거래소는 과거 거래내역 등을 분석하여 사기의심 계정에 대한 모니터링을 실시하여 계정정지 조치를 해야 한다. 또한, 타 명의인의 지갑으로부터 암호화폐 입금 직후 암호화폐를 매도하여 고액의 원화를 본인의 은행계좌로 이체하는 것에 대한 이상금융거래 모니터링을 통해 거래를 차단해야 한다.

IV 결 론

본 고에서는 전기통신금융사기 최신 동향을 살펴보고 전기통신금융사기가 국가·사회적으로 이슈가 되고 있어 보이스피싱 피해 사례를 체계적이고 효율적으로 분석 가능한 프레임워크를 소개하였다. 현재 금융보안원과 금융회사 등은 보이스피싱 대응협의체 등에서 전기통신금융사기 피해사례 분석 프레임워크를 활용하고 있다.

전기통신금융사기는 범행 수법이 다양화되고 여러 업권으로 확장되는 등 계속 진화한다. 보이스피싱 피해는 일반인들이 익숙한 기존 수법뿐 아니라 금융과 통신이 결합된 신종 수법에서도 많이 발생하고 있고 최신수법은 마치 유행하듯 여러 금융회사에서 동시다발적으로 발견되고 있다. 이러한 전기통신금융사기를 예방하기 위해 금융보안원에서는 금융회사 및 관련 기관 간의 신속한 피해사례 공유 등을 통해 최신 범행 수법 및 자금세탁을 위해 전자금융업·상업·가상자산업권 등까지 확장되는 범행 수법을 포함하도록 프레임워크를 계속 점검하고 발전시키고 있다.

전기통신금융사기 피해사례 분석 프레임워크는 신종 피해사례에 대한 체계적인 이해, 타 기관 간 협조사항 파악 등 다양한 업무에 활용될 수 있을 것으로 기대한다. 또한, 앞으로 이 프레임워크가 전기통신금융사기의 수법에 대한 분류체계로서의 중요한 역할을 하고 최근 여러 업권에 걸쳐 발생하는 전기통신금융사기를 예방하기 위한 다양한 업권 간의 협력체계 구축에도 참고자료가 되어 궁극적으로 보이스피싱 예방 및 대응에 기여했으면 하는 바람이다.





- [1] 금융감독원, '20년 중 보이스피싱 현황 분석, 2021.4.
- [2] 금융감독원, 「보이스피싱, 그 기묘한 이야기」 홍보영상 제작·배포, 2018.4.
- [3] 서민금융연구원, 전기통신금융사기 해결방안을 위한 통합 솔루션 구축에 관한 연구, 2021.6.
- [4] 금융감독원, 보이스피싱 지킴이 웹사이트(phishing-keeper.fss.or.kr)
- [5] 대검찰청, 일명 '보이스피싱' 범죄에 가담한 대포통장 양도인의 방조범의 인정여부, 2008.6.
- [6] 금융위·과기정통부 등 관계부처 합동, 보이스피싱 척결 종합방안, 2020.6.

Issue · Trend

▶ 산업동향

- 금융권 메타버스(Metaverse) 동향 및 시사점
정진영, 금융보안원 보안연구부 책임연구원

▶ 핀테크·신기술

- 양자보안기술 동향
김그린, 금융보안원 융합보안부 주임
- 클라우드 기반 인텔리전트 에코시스템 주요 내용 및 시사점
이승봉, 금융보안원 융합보안부 과장
- 캄보디아 CBDC '바콩(Bakong)' 기술 분석
김지훈, 금융보안원 융합보안부 대리

▶ 법·정책

- 이사회에 금융보안 역할·책임 강화 관련 국외 동향 및 시사점
신성환, 금융보안원 보안연구부 연구원

◆ 최근 메타버스 시장이 성장하면서 국내·외 금융권에서도 점차 활용 전략을 확대하고 있어 관련 동향을 검토

1. 메타버스(Metaverse)란?

□ **(개념)** 가상(meta)과 세계(universe)의 합성어로 다양한 디지털 기술을 통해 경제·문화적 활동을 할 수 있도록 구현된 3차원 가상세계

※ 메타버스에 대한 다양한 정의가 존재하며, 아직 명확히 정립되지 않은 상황

□ **(유형)** 미국 가속화연구재단(ASF)은 가상현실 기술 적용 및 현실세계 반영 수준 등에 따라 메타버스를 4가지 유형*으로 구분

* ① 가상세계(VR), ② 증강현실(AR), ③ 거울세계, ④ 라이프로그킹(Lifeloggging)

※ 본 보고서에서는 기술 발전과 최근 활용 동향 등을 감안하여 몰입경험을 위한 기술(VR, AR 기기 등)의 적용여부와 관계없이 현실세계와 가상세계의 교차점으로서 경제·문화적 활동이 이뤄지는 3차원 가상세계를 메타버스라고 간주*

* 최근 메타버스 서비스들은 VR, AR 기기 등이 없이도 활용 가능한 점 등 고려

□ **(특징)** 디지털 자산을 통해 메타버스 내에서 콘텐츠 소비 및 경제 활동이 이뤄져 산업의 한계를 극복하고 새로운 수익모델을 창출

주) 정진영, 금융보안원 보안연구부 책임연구원

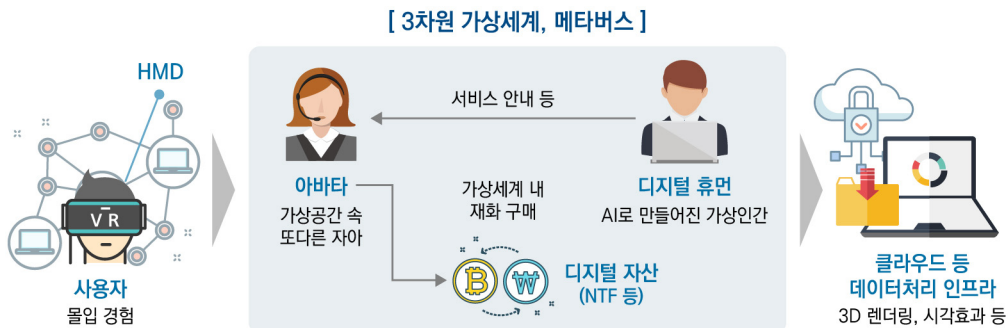
- 현실세계와 가상세계가 융합되어 사용자에게 몰입형 경험을 제공하며, 소비자 접근을 위한 새로운 디지털 플랫폼으로 이해

표 1 소비자 활용 디지털 플랫폼의 변천 과정

구분	웹 (2000~)	모바일 (2010~)	메타버스 (2020~)
주요 서비스	웹사이트, 블로그	모바일 애플리케이션, 스트리밍 서비스	3D 기반 게임·SNS, 가상현실 서비스
관련기술	서버-클라이언트 인프라 기술 등	4G LTE, 클라우드 등	블록체인(NFT), 가상현실(VR,AR) 등

- (적용 기술) 구현 방법에 따라 상이하나 일반적으로 몰입형 기술(Immersive Technology) 등 다양한 디지털 기술을 활용하여 구현

참고 메타버스 구현을 위한 주요 기술 예시



구분	구현 기술	설명
몰입형 기술	HMD (Head-mounted display)	- 안경처럼 착용하고 활용하는 디스플레이 장치로서 VR/AR 등을 통해 사용자의 몰입감을 극대화 * 오쿨러스(Oculus), HMD 오디세이, 기어 VR, 구글 글래스 등
	트래킹 (Tracking)	- 사용자의 행위 등 생체정보를 실시간으로 추적하여 가상세계에서의 행동으로 구현
	렌더링 (Rendering)	- 고화질 3D 콘텐츠 구현을 위한 컴퓨터그래픽 기술 * 유니티(Unity) 등 AR/VR 구현을 위한 물리엔진
	NUI (Natural User Interface)	- 키보드나 마우스 등 입력장치를 사용하지 않고 음성이나 동작 등을 통해 조작하는 인터페이스 * 머스크 등이 설립한 뉴럴링크(Neural Link)는 뇌의 전기신호를 처리하는 뉴로 테크놀로지 기술 개발 중

구분	구현 기술	설명
몰입형 기술	디지털 휴먼 (Digital Human)	- 최신 그래픽 기술을 통해 만들어진 메타버스 내의 가상 인간으로서 챗봇처럼 서비스 안내 등을 수행
	시각특수 효과(VFX)	- 실감형 콘텐츠 제작을 위해 메타버스 내에서 적용되는 특수영상 또는 시각효과
가상 경제	NFT (Non-Fungible Token)	- 블록체인 기술을 활용해 디지털 창작물(영상, 그림 등)에 고유의 인식값을 부여하여 특정인의 소유권을 기록 * NFT는 각 코인이 고유 값을 갖는 대체 불가능한 고유자산으로서 메타버스에서 디지털 자산으로 활용
데이터 처리 인프라	5G	- 방대한 규모의 데이터 전송을 위해 초고속, 초저지연, 초연결성 특징을 지닌 5G 네트워크 기술 활용
	클라우드 (Cloud)	- 사용자부터 수집한 대규모 데이터의 처리, 콘텐츠 스트리밍 등을 위한 클라우드 기술 활용
	모바일 엣지 컴퓨팅(MEC)	- 엔드포인트 기기(모바일 등) 단에서 데이터 처리 및 분석이 가능하도록 하여 부하를 분산하는 컴퓨팅 방식
	인공지능 (AI)	- 메타버스 내 개체 인식, 디지털 휴먼의 음성합성 및 자연어처리, 소비 데이터 분석 등에 활용

2. 금융권에서 주목하는 이유

□ 메타버스는 과거부터 활용되던 용어*였으나 다음과 같은 이유로 재조명되며 금융권에서 소비자 접근을 위한 신규 전략으로 주목

* 세컨드라이프(Second Life) 게임이 인기를 끌며 메타버스 개념이 알려지게 됨('03)

① **(몰입형 기술)** VR·AR 및 디지털 휴먼 등 기술이 극도로 발전함에 따라 사용자가 몰입하여 체험할 수 있는 환경이 마련

※ HMD 기기가 보편화됨에 따라 몰입형 기술을 체험할 수 있는 기회도 확대

② **(언택트 시대)** 코로나19 팬데믹 상황으로 인해 많은 기업과 소비자들은 비대면 서비스를 선호*

* 서울시민 1,200명 대상 조사 결과 약 80%는 코로나19 상황이 종료되어도 비대면 서비스를 사용할 것이라고 응답(서울연구원, '20.7월)

- ③ **(Z세대*)** 디지털 기술 활용에 익숙하며 현실세계와 가상세계를 구분 짓지 않아 가상세계에서의 소통 및 소비활동에 적극적

* '90년대 이후 태어난 젊은 세대로 디지털 네이티브(Digital Native) 세대라고도 함

- ④ **(디지털 자산)** 가상자산 등을 통해 사용자가 메타버스 내에서 경제활동을 수행할 수 있으며 특히, NFT의 등장으로 개인의 소유권이 인정됨에 따라 가상경제* 인프라를 구현할 수 있게 됨

* 경제활동이 현실에서 가상세계까지 확장되어 새로운 경험과 경제적 가치 창출

- ⑤ **(혁신 기회)** 현실 경제체제와 융합된 메타버스 내 가상경제가 실현되면, 다양한 비즈니스 기회 창출이 가능할 것으로 기대

- 또한, 소외계층을 위한 포용적 금융서비스 구현, MZ 세대를 겨냥한 마케팅 전략, 디지털 기술 활용을 극대화한 혁신적 서비스 제공 전략 등 메타버스의 무한한 가능성에 주목

※ 페이스북의 CEO인 마크 저커버그(Mark Zuckerberg)는 향후 5년내 페이스북을 SNS 기업에서 메타버스 기업으로 탈바꿈할 것이라고 선언('21.7월)

3. 메타버스 관련 동향

(가) 정책 동향

- **(국내)** 관계부처 합동으로 가상융합경제 발전전략('20.12월)을 통해 가상경제 선도를 목표로 공공분야에 구체적 추진계획을 발표

- 특히, 취약계층을 대상으로 가상융합기술(XR*) 기술 기반 디지털 포용 서비스*를 제공하여 디지털 복지 범위를 확대할 계획

* 가상현실(VR), 증강현실(AR) 등을 포괄하는 기술로 XR(eXtended Reality)로 통칭

** 예) 청각장애인용 AR 수어 변환 서비스, VR 화재대응 훈련, 장애인 길안내 등

가상융합경제 발전전략 및 추진과제

- ① (XR 확산) 주력산업과 XR 연계, 민간 참여를 유도하고, 사회문제에 XR 적용
- ② (인프라 확충) XR 디바이스, 데이터, 네트워크를 확충, XR 관련 법제도 검토
- ② (기업 지원) XR 기업 육성을 위한 금융지원, 단계별 XR 기술을 기업에 보급

□ **(국외)** 적극적인 투자와 지원 정책과 더불어, 최근에는 메타버스 활용의 부정적 측면*을 고려한 잠재적 위험 해소방안도 논의

* 세계경제포럼(WEF)은 가상현실 기술 활용에 따른 개인정보보호 이슈, 금융 사기 등 부정적 영향 등을 검토하기 위해 가상현실 글로벌 미래위원회를 조직('19)

○ 메타버스 내 행위 등을 직접 규제하는 사례는 확인되지 않으며, 기존의 디지털 콘텐츠 및 데이터보호 규제 등을 적용하는 상황

○ 한편, 유럽연합(EU)은 인공지능(AI) 규제법안('21.4월)을 마련하여 사람과 상호작용하는 AI 서비스에 대해 투명성 의무*를 부여

* AI와 상호작용하고 있음을 사용자에게 인지시키고 인위적 생성 여부 등을 공개

○ 영국 정부는 몰입형 기술에 대한 대응방향을 발표('20.6월)하며, 딥페이크 방지 및 온라인 피해규제에 대한 계획을 공개

(나) 금융권 활용 동향

□ **(국내)** 메타버스 활용 초기 단계로 내부업무(재택근무 등) 및 Z세대 대상 외부 소통 등에 활용하면서 적용 가능성을 검토 중

○ 메타버스 전문기업과 협업하여 가상공간에 가상 영업점을 구현하거나 가상 경제 기반 금융서비스를 제공하는 방안도 추진

표 2 국내 금융권 메타버스 활용 사례

금융회사명	사례
KB국민은행	- 메타버스 내 영업점 개설 및 금융서비스 제공 추진
하나은행	- 하나글로벌캠퍼스를 구현하여 가상공간에서 직원 연수 진행
DGB 금융지주	- 경영진 회의 및 프로젝트 시상식에 메타버스 활용
IBK 투자증권	- 메타버스 환경에 맞는 금융서비스 제공을 위한 계획 추진
신한카드	- Z세대 맞춤형 선불카드를 출시하고 가상공간 구축 추진

※ 국내 금융권에서는 네이버제트사가 제공하는 메타버스 플랫폼 제페토(Zepeto)를 통해 경영진 회의, 내·외부 행사 등을 추진하는 등 메타버스에 대한 관심이 높음

그림 1 하나은행 가상연수원(좌), 신한카드 메타버스 내 업무협약(우)



□ (국외) 몰입형 기술을 금융 업무 및 비대면 서비스에 적용하며 디지털 휴먼 등 고도화된 AI 기술도 융합하여 활용하는 추세

표 3 국외 금융권 몰입형 기술 활용 사례

금융회사명	사례
Citi Bank	- MS社の 홀로렌즈(HoloLens) 기술을 활용해 금융 분석 업무등을 수행할 수 있도록 하는 AR 기반 서비스 활용
Visa Card	- 몰입형 결제를 유도하기 위한 AR 기반 앱 공개
Capital One	- AR 앱을 통해 자동차 대출 등 금융 관련 세부정보를 안내

그림 2 BNP 파리바 홀로그램 원격 회의(좌), 중국농업은행 디지털휴먼(우)



회의 참여자를 홀로그램으로 투영하여 같은 공간에 있는 것처럼 원격 회의



지점에 AI 기반 디지털휴먼을 배치하여 고객에게 금융 업무 안내 등을 수행

※ 한편, 메타버스 기업들은 NFT 등 가상자산을 기반으로 탈중앙화된 3D 게임 및 소셜 서비스 등을 제공하며 가상 경제 체계를 구현

참고 메타버스 기업의 서비스 사례

구분	사례
 디센트럴랜드(Decentraland)	- 이더리움 기반 가상자산 마나(mana)를 활용한 서비스를 구현하여 가상공간에서 부동산을 매매하는 것이 가능 * 토지소유권이 블록체인에 기록 - 사용자는 가상공간 등 콘텐츠를 제작하고 이를 통한 수익 창출이 가능
 어스2(Earth2)	- 실제 지도정보를 토대로 현실세계와 동일한 3차원 가상 세계를 구현 - 가상의 토지 및 부동산을 계좌이체, 신용카드, 페이팔 등의 방법으로 거래 - 사용자는 구매한 토지 및 부동산에 광고를 하거나 임대 수익을 받는 등의 방법으로 수익을 창출할 수 있음

4. 시사점

메타버스 내 가상경제 구현을 위한 점진적 접근 전략 필요

- 메타버스 서비스는 플랫폼적 특징*을 가지고 있어 가상경제 구현 시 선도적 기업이 유리한 지위를 가지게 될 것으로 예상

* 다수의 생산자와 소비자가 상호 작용, 네트워크 효과, 승자 독식 구조 등

- 메타버스를 Z세대와의 소통 전략 및 비대면 원격 협업 등 내부 업무에 우선 활용하면서 향후 가상경제 시대에 대비할 필요
- 몰입형 기술의 활용 가능성에 지속적인 관심과 함께 중·장기적 관점에서 이를 활용한 혁신적 금융서비스 추진을 검토

※ 사람의 뇌파 변동을 인식해 컴퓨터를 동작시키는 뇌 컴퓨터 인터페이스(BCI, Brain Computer Interface) 기술이 주목받는 등 몰입형 기술이 크게 발전 중

메타버스의 부정적 영향을 해소하기 위한 연구 및 대응 필요

- 메타버스는 방대한 개인·생체정보 등이 수집*될 수 있음에 따라 개인정보 보호 및 데이터 활용 대한 지속적인 연구가 필요

* VR·AR 기기를 통해 사람의 시선, 홍채, 생체 신호 등 민감한 개인정보가 수집

- 또한, 메타버스의 몰입 경험은 현실과의 구분을 어렵게 만들어 가상환경에서의 금융사기가 발생할 가능성도 존재

* 메타버스에서 알게 된 사람으로 인해 수천만 원의 사기피해 발생('21.4월, 한겨레보도)

- 아직 메타버스 도입에 따른 영향이 불분명함에 따라 금융권의 디지털 전환 지원과 불확실성 해소를 위해 메타버스의 부정적 영향과 대응방안에 대한 심층적인 연구 필요



- [1] 김효용, “언택트 시대, 실감콘텐츠 기술의 지향점”, 정보통신기획평가원(IITP) 주간기술동향, 2020.11.
- [2] 박종현, “이머시브 미디어 유망 서비스 및 파급 효과 분석”, 한국전자통신연구원(ETRI) Insight, 2018.12.
- [3] 삼성SDS 인사이트 리포트, “가상현실, 증강현실이 메타버스인가?”, 2021.6.
- [4] 하나금융경영연구소, “메타버스의 부상과 금융업의 변화”, Emerging Tech & Biz (Vol.2), 2021.4.
- [5] 한국정보화진흥원, “메타버스가 다시 오고 있다-메타버스를 둘러싼 기술적·경제적·사회적 기회와 현안-”, 2021.3.
- [6] Dick, E, “Balancing User Privacy and Innovation in Augmented and Virtual Reality”, Information Technology and Innovation Foundation(ITIF), 2021.4.
- [7] De Guzman, “Security and privacy approaches in mixed reality: A literature survey” ACM Computing Surveys(CSUR), 2019.10.
- [8] Gartner, “World Order 2.0: The Birth of Virtual Nations”, 2021.7.
- [9] Gartner, “Augmented Reality and Virtual Reality will transform Selling, 2020.12.
- [10] IAPP, “Establishing privacy controls for virtual reality and immersive technology”, 2020.9.
- [11] Kaspersky, “What are the Security and Privacy Risks of VR and AR”, 2021.3.
- [12] M Slater, “The ethics of realism in virtual and augmented reality”, Frontiers in Virtual Reality, 2020.3.
- [13] Norton Rose Fulbright, “The Metaverse: The evolution of a universal digital platform”, 2021.7.
- [14] WEF, “Industry review boards are needed to protect VR user privacy”, 2019.8.

I. 검토 배경

- (양자정보기술의 발전) 최근 금융, 보건, 교통 등 거의 모든 산업 분야에 양자정보기술*이 폭넓게 활용될 것으로 전망

* 물질의 최소단위인 양자(quantum)가 갖는 물리적 특성인 중첩, 얽힘, 불확정성을 정보처리(전송, 저장, 측정, 분석 등)에 활용하는 기술

- 특허청에 따르면, 지난 10년간 IP5*(미국, 중국, 유럽, 일본, 한국)에서 출원된 양자정보기술 특허는 10년 전보다 4배 증가한 총 6,777건으로 지속적으로 증가(연평균 19.9%)하는 추세(21.4.)

* 국제특허 출원 건 기준으로 선정된 지식재산권 선진 5개국

- (양자보안기술의 필요) 초고속 연산이 가능한 양자컴퓨팅은 기존 암호체계를 침해할 수 있으므로, 이를 효과적으로 대응할 수 있는 양자보안기술이 필요

- 기존 암호체계의 해독 가능성을 검증한 알고리즘(쇼어*, 그로버** 등)은 양자컴퓨팅에 의한 해킹공격 발생 가능성을 수학적으로 증명

* 초고속 소인수분해 연산을 통해 공개키 암호(RSA, ECC 등)를 해독(Peter Shor, 1994.)

** 초고속 검색 연산을 통해 대칭키 암호(AES 등) 및 Hash 값 해독(Lov Grover, 1996.)

- 구글 CEO는 특히 양자암호기술(2~3년 이내)과 양자클라우드기술(4~5년 이내)이 향후 금융분야에서도 널리 활용될 것으로 전망(21.)

주) 김그린, 금융보안원 융합보안부 주임

☞ 이에, 양자정보기술 발전으로 예상되는 보안 위협에 대응할 수 있는 양자 보안기술의 종류 및 연구동향에 대하여 조사·분석함

참고 양자정보기술의 등장과 발전 경과

□ **(연구의 발단)** 고전역학이 아닌 양자역학의 원리를 이용하면 고성능의 컴퓨팅 연산이 가능할 것이라는 생각에서 시작

- 양자역학은 비트(Bit) 대신 큐비트(Qubit)를 기본단위로 사용하며, 전자와 광자의 중첩과 얽힘*을 사용하여 불가능했던 복잡한 연산을 가능하게 하고 정보처리 소요 시간을 비약적으로 단축

* 중첩(Superposition)이란 0과 1이 동시에 존재하는 상태로 큐비트의 상태는 관측 시점에 확률적으로 0과 1중 하나로 결정되며, 얽힘(Entanglement)이란 앞쪽 큐비트의 상태가 결정될 때 다음 큐비트의 상태도 동시에 결정됨을 의미

□ **(개념 정립)** 물리현상을 양자컴퓨터로 모사(模寫)할 수 있다고 언급된 후 (Richard Feynman, 1982.), 양자병렬성을 통해 특정 문제*에 대한 빠른 연산이 가능함이 밝혀졌으며(Deutsch, 1985.), 정보통신과 결합한 새로운 응용분야로 양자정보기술 개념이 등장(MIT, 1996.)

* BQP(Bounded error, Quantum, Polynomial time): 양자컴퓨팅을 적용하여 효율적으로 풀 수 있는 문제들의 집합

- 구글은 자체 개발한 양자컴퓨팅 칩을 통해 '19년도에 가장 빠른 슈퍼 컴퓨터가 1만년 동안 수행해야 하는 연산을 3분 20초 안에 수행한 실험을 통해 양자 우위(Supremacy)를 증명(Nature, '19.10)

□ **(시장 형성)** 양자정보기술 시장은 IBM, 구글, 디웨이브시스템즈, 마이크로소프트, 노스롭 그루먼, 인텔 등의 참여로 점차 확대

- 美 경제지 포브스는 양자정보기술이 컴퓨터, 통신, 네트워크 등 정보통신 기술 뿐만 아니라 신약, 배터리, 금융 등 산업 전반의 패러다임을 뒤 흔드는 '2차 양자혁명'이 시작됐다고 분석('21.)

II. 양자정보기술 동향

① (정책 동향) 양자정보기술의 잠재적 가능성이 높게 평가됨에 따라 세계 주요국에서는 빠른 성장과 조기 정착을 위한 정책 발표

- (국내) 투자 확대, 관계 기관 간 교류, 선진 기술 확보 등을 통해 양자 분야 산업 활성화 정책 추진
- (국제) 대규모 전문 연구시설 마련(미국), 대규모 프로그램을 통한 전략적 투자(EU) 진행 등 국가적 차원에서 공격적으로 양자정보기술 활성화를 위한 정책 추진

표 1 주요 국가의 양자정보기술 정책 동향

구분	주요 현황
국내	- 과기정통부는 삼성·현대차 등 25개 기업과 한국과학기술연구원(KIST) 등 12개 연구기관 등과 '미래양자융합포럼'을 창립했으며, 미국과의 양자기술 공동연구 인력교류 확대 추진 방안 발표('21.6.) - '정보통신진흥 및 융합활성화 등에 관한 특별법' 개정으로 양자 분야 연구개발/인력양성 지원 등 산업활성화 방안 마련('20.5.)
미국	- 양자연구센터(5개) 발족('20.4) 및 '양자인터넷 전략적 비전' 발표('20.2.) - 양자정보과학기술의 연구·개발 등의 지원 및 국제 표준 개발 가속화를 위한 '국가 양자 이니셔티브 법안 제정'('18.12.)
유럽	- EU는 '퀀텀 플래그쉽 프로그램'을 통해 10년간 10억 유로 규모의 양자 기술 개발 프로그램 착수('18.10.) - 독일은 5년간의 '양자기술 기초부터 시장까지' 프로그램 마련('18.9.)
영국	- 양자컴퓨팅 상용화 및 사업화 지원에 1억 5,300만 파운드, 양자 분야 사업화에 7천만 파운드 등 38개 프로젝트 투자 발표('20.6.)
일본	- NTT, 도시바, 히타치 등 11개 기업의 양자 기술 협의회 구성('21. 예정) - 국가차원의 양자기술 이노베이션 전략 수립('20.1.) - '양자과학기술의 새로운 전개를 위한 추진방안' 수립('17.2.)
중국	- 양회를 통해 양자컴퓨터 집중 육성 계획 발표('21.) - 양자과학기술혁신연구소 설립 및 육성 지원 계획 발표('19.8.) - '양자기술혁신 및 개발계획' 및 '지난양자밸리' 조성 계획 발표('18.5.)

② **(시장 동향)** 양자정보기술 관련 시장은 '19년 세계 10.8억 달러, 국내 708억 원 규모에서 '27년 세계 55.9억 달러, 국내 3,516억 원의 규모를 기록할 것으로 전망(정보통신기획평가원, '20.12)

- **(국내 시장)** 연평균 21.2% 성장세로 통신 3사(SKT, KT, LGU+)를 중심으로 HW, SW 개발이 이루어지는 추세
- **(세계 시장)** 연평균 22.8% 성장세로 IBM, MS, 아마존 등 글로벌 IT 기업이 클라우드 등을 활용한 양자컴퓨팅 서비스를 출시하여 기술 접근성 및 자사 플랫폼으로의 유입을 확대하는 추세

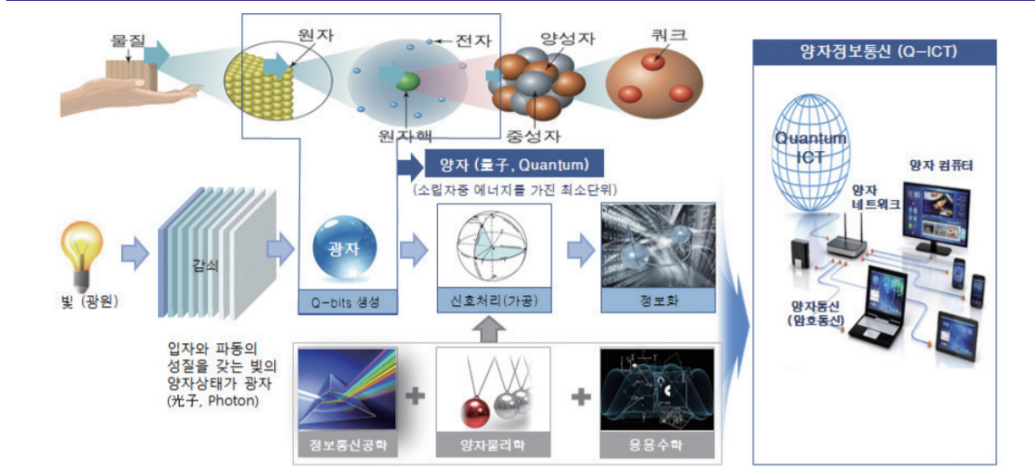
표 2 세계 주요 양자정보기술 보유 기업

구분	주요 서비스 현황
IBM	- '16년부터 클라우드 방식 서비스 제공, 델타항공 등에 적용
MS	- '21년부터 클라우드 서비스 '에저'에 양자 연구 플랫폼 준비
아마존	- 아마존 웹 서비스를 통한 양자컴퓨팅 서비스 제공
구글	- 연구 플랫폼 제공, 하드웨어 개발, 클라우드 서비스 제공
인텔	- 반도체 기반 양자 프로세서 개발 및 클라우드 서비스 제공
알리바바	- '18년부터 자체 클라우드를 통한 연산 실행 서비스 제공
디웨이브시스템즈	- 상용 양자컴퓨터를 생산하는 유일한 업체로 차세대 진행
Psi퀀텀	- 광자를 이용한 양자프로세서 하드웨어 및 SW 개발
삼성전자	- '17년부터 IBM 퀀텀 네트워크 파트너로 양자컴퓨터 활용
SKT	- 양자암호통신기업 IDQ를 인수, 가장 많은 특허 보유
KT	- 자체 개발한 양자통신 기술을 국가주요통신망 등에 적용
LGU+	- 양자내성암호 기술을 활용한 실험·검증 수행
아이온큐	- Trapped Ion 기반 양자프로세서 개발

III. 양자보안기술 정의 및 범위

- ① **(정의)** 양자정보기술 중에서 보안 분야에 적용 가능한 기술로 양자역학적 특성을 활용하여 양자컴퓨팅 연산 능력만으로는 공격할 수 없는 보안 기술을 총칭
- ‘양자정보기술’은 국내 특허청에서 사용하는 용어로 ‘양자컴퓨팅’, ‘양자통신’, ‘양자센서’로 구분
 - 한편, 동일한 의미로 ‘양자정보통신’(한국정보통신기술협회), ‘양자정보과학’(미국), ‘양자기술’(유럽), ‘양자과학기술’(일본), ‘양자제어’ 또는 ‘양자정보’(중국) 등의 용어로 다양하게 사용

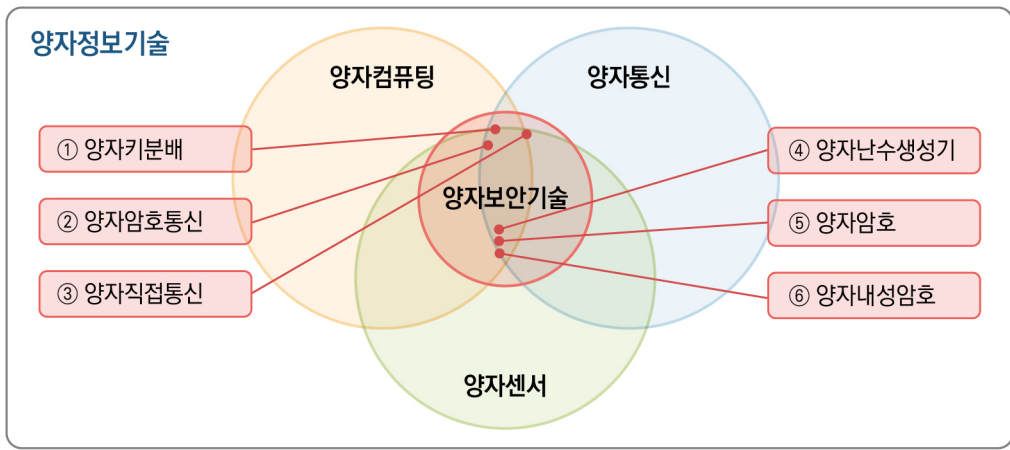
그림 1 양자정보통신 개념도



※ 출처: ICT R&D 기술로드맵 2025(정보통신기획평가원)

- ② **(범위)** 주요 양자보안기술에는 ①양자키분배, ②양자암호통신, ③양자직접통신, ④양자난수생성기, ⑤양자암호, ⑥양자내성암호 등이 있으며, 이를 중심으로 활발하게 연구 중

※ 양자보안기술에 대한 범위와 분류는 아직 정의 중인 단계로 본 보고서의 범위와 분류는 「2021 한국정보보호학회 양자보안연구회」 발표(‘21.3.) 내용을 준용

그림 2 양자보안기술의 범위

- 6개의 주요 양자보안기술은 목적·역할 측면에서 ❶양자역학활용 기술과 ❷양자위협대응 기술로 분류 가능

표 3 목적·역할에 따른 양자보안기술 구분

분류	주요 기술	설명
❶ ❷ 모두	① 양자키분배 (QKD, Quantum Key Distribution)	양자역학 현상(양자중첩 등)을 이용하여 암호 키를 안전하게 공유하는 기술
❶ 역학 활용	② 양자암호통신 (QCC, Quantum Cryptography Communication)	양자키분배(QKD)를 포함하며, QKD를 통해 공유 키 등을 이용하여 안전한 통신채널을 형성 하는 기술
	③ 양자직접통신 (QSDC, Quantum Secure Direct Communication)	양자채널 내에서 별도의 암호키 교환 없이 안전 하게 직접 메시지를 주고받을 수 있는 기술
	④ 양자난수생성기 (QRNG, Quantum Random Number Generator)	양자암호, 양자역학 현상을 활용한 노이즈 소스를 기반으로 하는 난수발생기
❷ 위협 대응	⑤ 양자암호 (QC, Quantum algorithm for Cryptanalysis)	양자키분배(QKD)를 포함하며, 양자역학적 성질을 이용하여 암호 프로토콜을 구성하는 기술
	⑥ 양자내성암호 (PQC, Post Quantum Cryptography)	대규모 양자컴퓨팅에서도 안전하다고 알려진 양자 저항성을 지닌 공개키 암호 기술 등

IV. 세부 기술별 동향

1. 양자키분배 (QKD, Quantum Key Distribution)

□ (정의) 양자역학의 ‘복제 불가능성 원리’와 ‘파동함수 붕괴 현상*’을 이용해 두 사용자 간 암호통신에 필요한 키를 비밀리에 공유할 수 있게 하는 기술

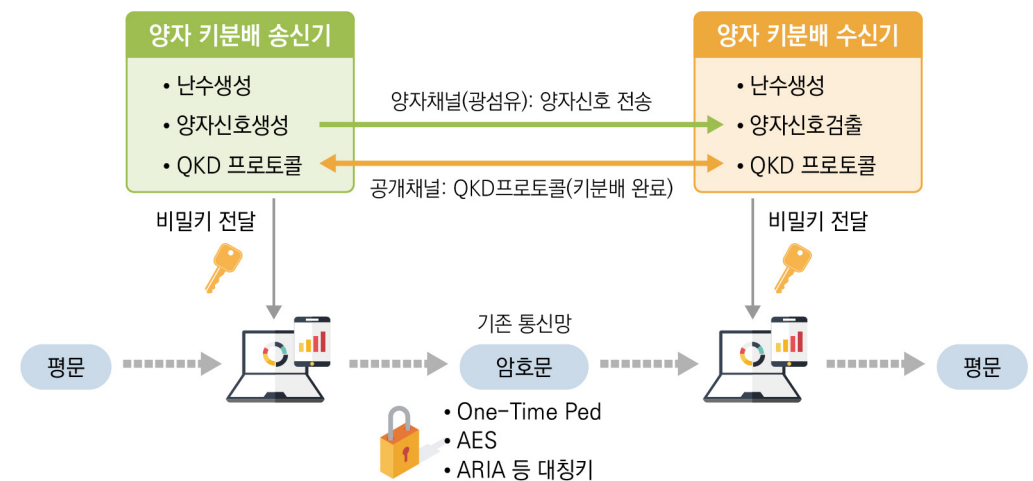
* 여러 고유상태가 중첩되어 있는 상태에서 관측을 하게 되면 하나의 고유상태로 갑자기 바뀌는 것으로 관측자가 결과에 영향을 주게 되는 현상을 의미함

○ 1984년, IBM 연구소가 처음 제안하였으며, 물리적 자연 현상에 기반하고 있어 공격자의 도청이 어렵다는 장점*을 지님

* 미국 NSA의 도청 폭로 이후(스노든, '13.) 도청에 원천적으로 안전한 기술로 주목

○ 유선/무선으로 모두 구현 가능하며, 유선은 광케이블, 무선은 인공위성을 이용하는 연구가 진행 중

그림 3 양자키분배 개념도



○ 광자의 민감성으로 에러 발생률이 높아 장거리 통신이 어렵고, 인증기능이 없어 중간자 공격에 취약한 문제를 해결할 필요

※ 美 국가안보국(NSA)은 QKD의 추가 암호 키·알고리즘·인프라 필요, DDoS 공격 취약 등을 근거로 국가 보안 시스템에서 배제하겠다고 밝혔지만('21.4.), 이는 QKD 기술 개발을 늦게 시작한 다른 국가들을 견제하기 위한 발표였다는 의견도 있음

- (현황) SKT와 KT를 중심으로 연구가 진행되고 있으며, 현재는 연구단계를 지나 사업단계로 접어들어 실제 구축 및 운용 중

표 4 양자키분배 사례

구분	사례
표준	ETSI - 양자키분배 위원회를 두고 9개의 GS와 2의 GR 출발/갱신
	ITU-T - 양자키분배 활용 등에 대한 표준화를 SG13, SG17에서 진행 - (SKT) SG17에서 양자키분배 기술 네트워크를 위한 보안 고려사항(SG17 TR. sec-qke) 등을 개발 - (KT) SG13에서 세계 최초 QKD 네트워크 표준 Y.3800, Y.3901 승인 및 Y.QKDN_CM, Y.QKDN_QoS 등 표준화 주도('18.~'20.)
	ISO/IEC - WG3에서 중국이 주도적으로 진행하였으며, 안전성 요구사항, 시험/평가 방법의 두 개의 과제로 나뉘어 CD로 진행
	TTA - TC2(통신망 기술위원회에서 ETSI 문서 도입 표준 개발 - TC5(정보보호 기술위원회) 국가 공공 도입에 필요한 프로토콜 규격과 보안 요구 사항 독자적 개발
연구	ETRI - GHz급 광원 및 검출 소자 기반 초소형 유선 QKD 칩/모듈 개발 착수('20.)
	KIST - KT와 함께 현대중공업 특수선 통신실을 중심으로 KT 울산 지사와 20km 구간을 QKD를 적용하여 구축
구현	SKT - 미국 버라이즌에 양자키분배기 공급('20.) - 스위스 IDQ를 인수하고 유럽과 미국에 QKD 수출(EU 퀀텀 플래그쉽 프로젝트에서 QKD의 60%를 공급한 1위 공급사) - 5G 전송망 일부(서울~대전, 대전~대구) 등에 QKD를 이용한 암호 기술 적용·운용
	KT - 한국정보화진흥원에서 발주한 초연결 지능형 연구개발망의 양자암호통신망 구축 및 운영사업자로 선정

2. 양자암호통신 (QCC, Quantum Cryptography Communication)

- (정의) 양자의 특성을 이용해 도청 불가능한 암호키 생성·분배 기술 등을 기반으로 하는 암호통신 기술

※ 암호화된 데이터를 송·수신하는 기술로서, 송신부는 암호화된 데이터를 전송하고 수신부는 양자키분배, 양자내성 암호 등을 사용하여 이를 복호화

- 1984년, IBM 연구소가 처음 제안한 통신 방식으로 파장·진폭 등을 이용하는 기존 통신과 달리 광자를 활용하는 방식

- 양자암호통신의 암호키는 양자역학 특성상 수신자가 정보를 받는 순간 정보가 결정되어 복제·탈취를 원천적으로 차단
- 양자암호통신 대칭키가 전송되는 데이터의 속도에 부합하여 생성된다면 보안성이 높은 OTP 형태로도 적용 가능

그림 4 양자암호통신 내 암호 키 분배 과정(BB84 프로토콜)

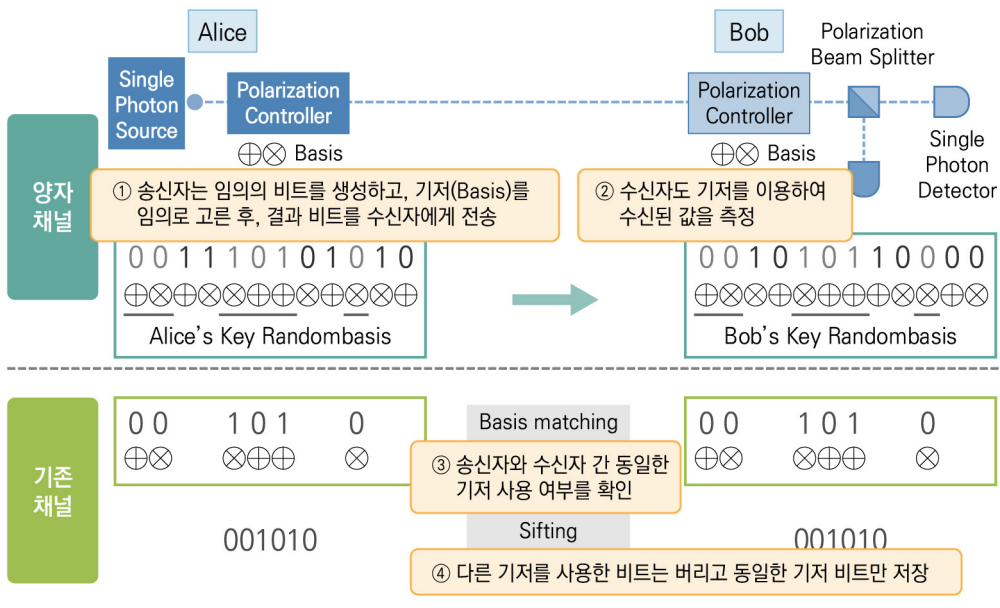


표 5 양자암호통신 주요 요소

구분	설명
광원	- 광자를 흠치는 도청 공격으로부터 보안성을 지키기 위해 단일광자 광원(사용자가 원하는 시간에 광자 하나만을 방사하는 광원) 사용
단일 광자 검출기	- 광학적 특성과 전기적 특성을 이용하여 단일 광자를 검출하는 기술
난수 발생기	- 도청자도 예측할 수 없는 무작위수(난수)를 생성하는 기술
양자 중계기	- 양자역학적 성질 중 '얽힘'을 이용하여 원거리 전송이 가능한 기술
양자암호 프로토콜	- BB84, Decoy based QKD, Plug & Play, Phase Differential Shift QKD 등 양자암호키 분배 및 전송을 위한 프로토콜

□ **(현황)** 한국전자통신연구원(ETRI), 한국과학기술연구원(KISTI) 등이 초기 연구를 진행하였으며, SKT, KT 등이 구현 중

표 6 양자암호통신 사례

구분		사례
표준	ITU-T	- 14개의 관련 표준 진행('20.4. 기준) - (SKT)양자암호통신 네트워크를 위한 보안 키 결합 및 제공 방식(X.1148), 보안 프레임워크(X.1740) 예비 승인 - (KT)개방형 양자암호 네트워크 예비 승인 및 양자암호통신 분야 세계 최초 국제 표준인 ITU-T X.3800 표준 제정
	ISO/IEC	- 양자암호통신의 실용화 이슈 논의(JTC 1 SC27)
	IEEE	- 양자통신과 양자통신 표준화 이슈를 함께 논의(P1913 등)
	TTA	- (KT)양자암호통신 상호운영 기술 표준 채택 등 2개 표준('21.)
연구	한국 정부	- 48개 정부 부처 '차세대 국가융합망' 양자암호통신 적용('21.)
	ETRI	- 무선 양자암호통신을 위한 핵심 집적화 부품 자체 기술로 개발·시스템화하여 실 환경에서 양자 신호 전송·복원 성공
	KISTI	- KT와 함께 양자통신 응용연구센터 개소 및 실용화 연구
	중국	- 위성 양자암호통신 기술을 1,120km 떨어진 곳에 구현('20.)
구현	SKT	- 기업용 IP 장비에 양자암호통신을 적용한 '퀀텀VPN' 개발('20.) - SK브로드밴드, 유알정보기술과 함께 한화시스템, 우리은행, CJ 올리브네트웍스에 양자암호통신망 구축
	KT	- 스마트폰 앱을 통해 양자암호통신을 구현하는 '양자 하이브리드 기술' 개발('21.4.)

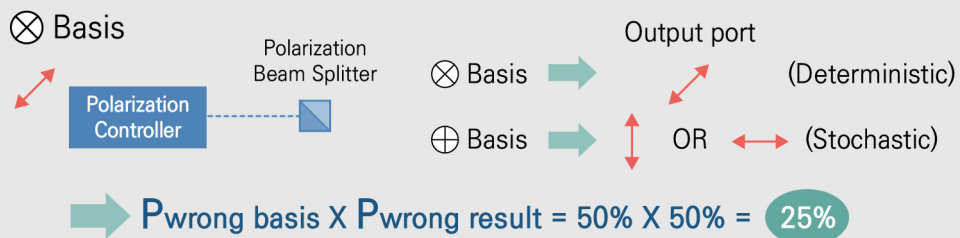
참고 양자암호통신이 도청에 안전한 이유

□ 양자암호통신 환경에서는 도청자가 중간에서 악의적으로 정보를 가로채기 하여 측정할 경우 본래의 양자 상태가 자동으로 깨짐

○ 이는 송·수신 간의 정보 비교를 통해 양자 비트오율(QBER, Quantum Bit Error Rate)을 측정하여 도청자 존재 파악이 가능*하기 때문

* 도청자가 기저(Basis)를 송신자와 맞추었다면 수신자에게 에러 없이 보낼 수 있지만, 송신자와 다른 기저를 맞추게 되면 확률적으로 에러가 발생(도청자가 존재하면 50% 확률로 다른 기저를 선택하고, 50% 확률로 다른 정보가 검출)

양자 복제 불가능성을 이용한 도청자 파악 과정



□ 이로 인해 양자키분배 과정에서 실제 비트(Bit) 정보 외의 기저를 공개하는 것만으로 어떤 정보가 실렸는지 송·수신자 간 공유 가능

기존 채널과 양자채널에서의 기저 공개 과정

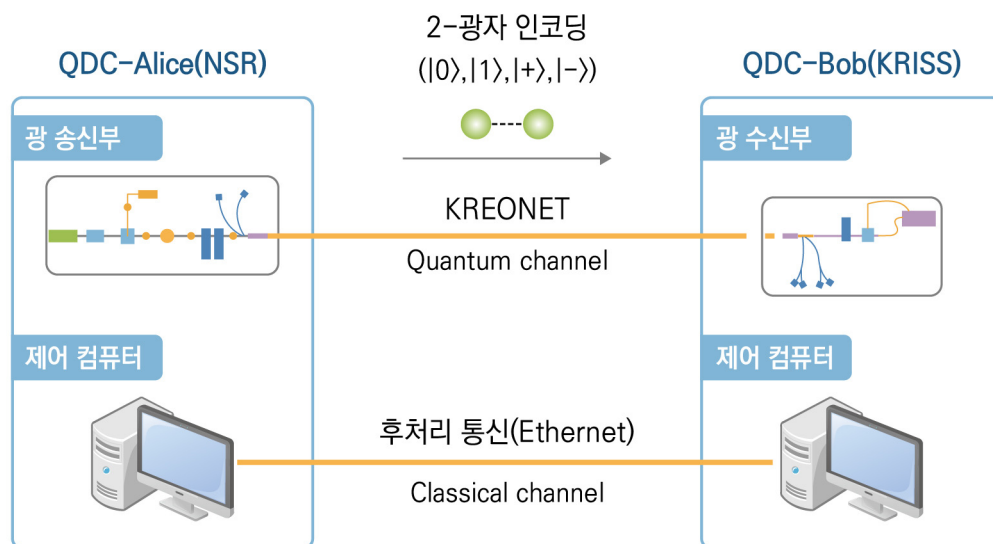


3. 양자직접통신 (QSDC, Quantum Secure Direct Communication)

- (정의) 기존 양자키분배 방식과 대칭키 기반 암호화 통신을 결합한 기술로, 비밀 메시지를 직접 전송하여 비밀키 관리 문제 해결을 통해 보안성 확보 가능
- 한국표준과학연구원(KRISS)과 국가보안기술연구소(NSR)가 세계 최초로 실증한 방식으로 두 연구소 사이 20km 구간의 시험 통신망에서 기술 구현이 이루어짐
- 기존 양자키분배 기술은 비밀키를 사용하여 사용자가 늘어날수록 비밀키 관리가 어려워지는 단점 존재
- 광원은 광자를 1개씩 만들 수 있고 검출기가 1개의 광자를 측정*할 수 있어서 통신 보안성 확보 가능

* 추가적으로 광원, 검출기, 채널 제어, 프로토콜 설계·검증 기술 및 실제 환경적용을 위한 낮은 광검출 효율, 광손실, 광신호 왜곡 보상 등에 대한 기술 개발 필요

그림 5 양자직접통신 개념도



4. 양자난수생성기 (QRNG, Quantum Random Number Generator)

□ (정의) 실 난수발생기*(TRNG)의 한 종류로 양자역학에 기반한 엔트로피 소스**가 높은 난수를 출력할 수 있게 하는 비결정적 난수발생기*** (NDRBG)를 의미

* True Random Number Generator: 물리적 현상으로부터 난수를 생성하는 기술로 패턴과 주기가 없으므로 유사(Pseudo)난수와 달리 난수 생성의 안전성 보장 가능

** 최종 출력 난수의 안전성은 엔트로피 소스에 의존하고 있어서 어떤 소스를 어떻게 구성하고 적용했는지가 전체 보안 시스템의 보안 강도를 결정

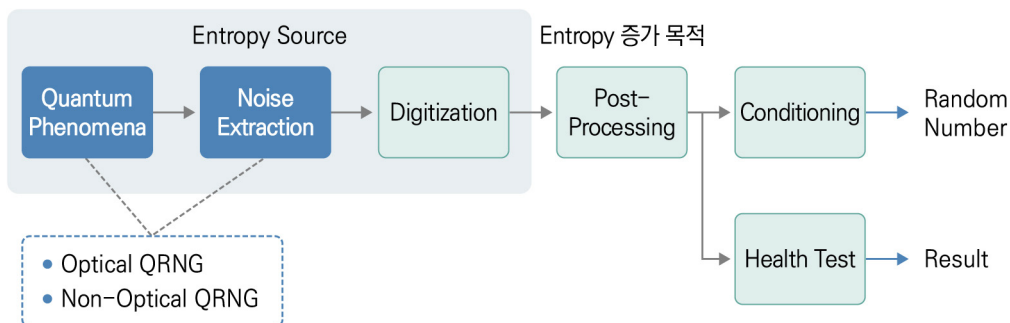
*** Non-Deterministic Random Bit Generator

○ 난수는 암호 알고리즘 설계에 가장 기본적인 요소로, 현대 암호의 안전성은 난수의 무편향성(unbiased), 숫자 무관성(uncorrelated), 예측 불가능성(unpredictable)에 기반함

○ 양자난수생성기는 무작위 특성을 보이는 양자 샷 노이즈(shot noise)의 물리적 임의성을 이용하여 예측이 불가능하고 패턴이 없는 순수 난수를 지속적으로 생성 가능

※ 기존의 난수 생성기는 수학적 함수 기반으로 얻은 유사난수를 사용하기 때문에 난수성을 완전하게 보장하기 어렵다는 단점을 지님

그림 6 NIST, SP 800-90b 양자난수생성기 적용 절차



- 일반적으로 Optical 방식과 Non-Optical 방식으로 구분
 - Optical 방식은 다양한 기관에서 연구되어 일부 상용화
 - Non-Optical 방식에는 방사성 붕괴 또는 shot noise를 이용한 방식이 있으며 노이즈의 명확한 분리가 중요
- **(현황)** 유럽 중심으로 활발한 연구가 진행중이며, 국내에서는 스타트업 EYL이 개발한 ‘양자난수생성기 칩’의 상용화에 성공

표 7 양자난수생성기 사례

구분		사례
표준	ITU-T	- (SKT)양자 노이즈 난수 생성기 구조(SG17 X.1702)
	ISO/IEC	- NDRBG에 필요한 주요 요소와 보안 요구사항 설명
	NIST	- 랜덤·통계적 테스트(SP 800-90B, 90C 등)
연구	보쉬	- IoT와 무인 자동차를 포함한 Bosch 주요 시장 적용 - 유럽 표준 개발을 위한 노력
	캠브리지	- IBM Quantum Network에 QRNG-as-a-service 제공 - Device-independent QRNG
	도시바	- 캠브리지 대학에서 연구 중, QKD 모듈에 QRNG 적용
	오크리지	- 공공, 에너지 영역, Crypt사와 협업하면서 소형 QRNG를 상용화하기 위한 IP 확보, 특허사용 계약
구현	KT	- EYL과 함께 방사성 동위원소를 소스로 자연붕괴 과정에서 발생하는 알파입자 측정을 기반으로 초소형 칩셋 개발
	SKT	- QRNG 적용 최초 지문인식 보안 키 ‘이지퀀트’ 출시(‘21.6.) - 비트리(BTREE)와 함께 세계에서 가장 작은 크기의 양자 난수 생성 칩셋 양산에 성공하였으며, 삼성전자와 협력을 통해 세계 최초의 양자보안폰 ‘갤럭시 A 퀀텀’에 탑재 - IoT, 자율주행 탑재 가능한 QRNG 칩셋 개발 예정
	LGU+	- 산업용 통신망에 접속하는 사용자 PC 접근보안 강화를 위해 양자 난수 기술을 탑재한 USB 토큰 제공

5. 양자암호 (QC, Quantum algorithm for Cryptanalysis)

- **(정의)** 양자역학의 불확정성 원리를 이용하여 양자 복제 불가능성을 적용한 암호체계
 - 시장조사기관 윌디벨롭먼트는 전 세계 양자암호 시장 규모는 '19년 1억 2,186만 달러에서 '27년에는 14억 577만 달러로 10배 이상 급증할 것으로 예상
- **(현황)** 일반적으로 양자암호는 양자키분배와 양자내성암호에 기반한 기술 연구가 필요하며, 국내의 경우 양자키분배 중심의 양자암호 연구가 집중
 - 양자암호에서 양자키분배는 컴퓨터 연산 능력 및 해독 알고리즘 발전과 무관한 지속적인 안정성 제공이 가능
 - 양자암호에서 양자내성암호는 기존의 공개키 암호의 기능을 제공하여 대체 기술로 적용 가능

표 8 양자암호 사례

구분	사례
SKT	- 양자암호 보안기술을 적용한 '갤럭시 퀀텀2' 발표 - 안드로이드 표준 키스토어의 로그인·인증·결재 기능에 양자보안기술 적용, SKT·신한은행·SC은행 등에 인증기술 적용('21.4.) - 5G 가입자 인증 서버에 양자암호 기술 적용 - 삼성전자와 양자보안 스마트폰 출시
KT	- 양자암호 기반 비화통신* 기술 발표('21.3.) * 비화기를 통해 도청을 방지하는 전용통신망 방식
LGU+	- LG CNS 등과 국내 최초로 IoT 양자보안칩을 개발('20.) - 드론 및 가정용 폐쇄회로 CCTV 등에 적용 계획('21.~)

6. 양자내성암호 (PQC, Post Quantum Cryptography)

□ **(정의)** 양자컴퓨팅의 기존 암호체계 해독 위협에 안전한 양자역학 기반의 암호 체계로, 격자 기반의 공개키 암호 알고리즘 등 양자컴퓨터로도 처리할 수 없는 새로운 알고리즘에 기반

○ '06년 PQCrypto 학회를 시작으로 '16년 NIST에서 PQC 표준을 공모* 하면서 전 세계적으로 본격적인 연구가 시작

* '17.12월, 1라운드에 제출된 69개 알고리즘(국내 5개 참가)이 공개·검증되었고, '20.7월, 3라운드 후보 7종과 예비 후보 8종을 발표 후 현재 계속 검증 중

○ 모바일기기 및 IoT기기 모두 유연하게 구현·적용 가능하며, 암호 키 교환, 데이터 암호·복호화, 무결성 인증 등 주요 보안 기능 제공 가능

표 9 양자내성암호 종류

종류	내용
격자 기반 (Lattice-based)	- 격자(Lattice) 위에서 계산하는 문제의 어려움에 기반하는 암호 시스템
코드 기반 (Code-based)	- 일반적인 선형 코드(Linear Code)를 디코딩하는 어려움에 기반하는 암호 시스템
다변수 기반 (Multi-variate)	- 유한체(Finite Field) 위에서 계산하는 다변수함수 문제의 어려움에 기반하는 암호 시스템
해시 기반 (Hash-based)	- 해시 함수의 안전성을 기반으로 한 전자 서명 시스템
아이소제니 기반 (Isogeny-based)	- 순서가 같은 두 타원곡선 사이에 존재하는 아이소제니(Isogeny)를 계산하는 어려움에 기반하는 암호 시스템

□ **(현황)** 국내에서는 Lizard, HiMQ-3 등의 알고리즘을 집중적으로 연구 중이며, LGU+는 PQC에 관한 실용화 연구를 검토

표 10 양자내성암호 사례

분야	구분	사례
표준	ISO/IEC	- JTC 1 / SC 27 / WG 2에서 표준화 진행 - 본격적인 표준화는 NIST 공모사업 완료 후 진행 예정이며, 해시 함수 기반 전자 서명에 대해선 우선 표준화 예정
	NIST	- IBM, 아마존, 구글 MS 등 글로벌 기업의 표준화 진행 - 美 국가표준기술연구소(NIST), 국가안보국(NSA) 등에서 '24년까지 양자내성 암호기술 표준화 및 검증 작업 완료를 목표로 기존 공개키 암호기술 전환작업 준비
	TTA	- 국내 NIMS에서 개발한 HIMQ가 TTAK.KO-12.0348로 등록 - 서울대에서 개발한 격자 기반 양자내성암호 Ring-Lizard가 TTAK.KO-12.0349로 등록
연구	ETRI	- '19년부터 대용량 양자컴퓨팅 환경에서의 양자 자원량 분석을 통한 기존 암호·양자내성암호 보안 기술 연구 중
	NSR	- 향후 4년 동안 세계 수준의 양자내성암호 개발을 목표로 기술개발 로드맵 수립 및 K-PQC 연구단 발족('21.5.)
	KISA	- 이스트시큐리티, 잉카인터넷, NSHC와 함께 'K-사이버방역 추진전략사업'으로 '양자내성암호 시범적용 추진 협약' 체결
	크립토크랩	- 유·무선 양자내성암호 분야 연구 수행
구현	MS	- PQC 소프트웨어 라이브러리 제작·배포
	구글	- 크롬브라우저 HTTPS 암호통신에 PQC 시험 적용
	아마존	- AWS HTTPS 암호통신에 PQC 시험 적용
	LGU+	- 서울대, 크립토크랩과 협업하여 세계최초로 양자내성암호기술을 소프트웨어 방식으로 기업 등 고객전용망에 활용되는 광전송장비에 적용('21.6.) - 양자내성암호가 탑재된 USB 보안토큰 'Q-PUF USB'를 개발하여 LG이노텍 공장(평택-부산, 640km), 을지대병원(서울-대전, 207km)의 전용회선에서 실증('21.1.) - 5G서비스 및 유·무선 가입자 서비스에 양자내성암호 기술 적용 예정

참고 양자키분배(QKD)와 양자내성암호(PQC)를 이용한 암호통신

□ **(일반 암호통신)** 두 사용자 A와 B가 비밀리에 메시지를 주고받기를 원하는 경우 아래와 같은 과정을 수행하며, ① ~ ④단계가 온전히 이루어지면 “암호통신을 한다”라고 함

- ① **(키 생성)** A는 난수 발생기를 사용해 비밀키를 생성
- ② **(사용자 인증)** A는 상대방의 신원이 B가 맞는지 확인
- ③ **(키 분배)** A는 자신이 생성한 비밀키를 B에게 전달
- ④ **(암호화)** A는 암호 알고리즘에 보내고자 하는 메시지를 넣고 공유한 비밀키로 잠근 후 B에게 전송

□ **(양자 암호통신)** 양자키분배(QKD)의 경우 ③의 기능을 제공하지만, 양자 내성암호(PQC)의 경우 ②, ③, ④ 뿐만 아니라 전자서명 까지도 제공 가능

- NCSC(英), 하버드(美) 등의 양자보안 전문가들은 양자컴퓨터 시대를 준비하기 위해 양자키분배 보다는 양자내성암호를 권고
- 단, PQC 역시 수학적 복잡성으로 인해 예상치 못한 오류 등이 발생할 수 있어 암호학자들은 완벽한 안전성 이론 정립에 노력

V. 시사점

- **(개념 및 표준 정립 필요)** 양자보안기술의 범위, 분류 기준 등에 대한 국가별, 산업별, 학계별 다양한 의견이 있으므로 명확하고 통일된 개념 및 표준의 조기 정립 필요
- 기술 상용화를 위한 상호보완성 보장을 목표로 ITU-T, NIST 등을 중심으로 표준화가 진행 중이며, 이를 통해 기술 성숙도 향상, 신규 서비스 도출 등이 가능할 것으로 보임

□ (기술 격차 해소 필요) 양자기술의 후발주자인 우리나라는 주요국과의 기술 격차를 좁히기 위한 정부 차원의 지원 필요

※ 제21대 국회 입법 정책 현안 보고서에 따르면, 한국의 양자컴퓨팅 기술은 미국에 비해 3년, 양자통신 기술은 2년의 기술 격차가 있는 것으로 평가되고 있음. 이는 정보통신기술 분야 중 최대 격차임

○ 미국, 유럽, 일본, 중국 등 세계 주요국은 오래전부터 양자 기술에 막대한 예산을 투자해왔으며 정책적 노력도 지속

※ 우리나라 정부가 5년간 445억 투자할 계획이었던 것에 반해 미국은 '18년 이후 4년간 1조 3,500억원, 중국은 약 17조원을 투자



참고문헌

- [1] 양자내성암호 및 양자암호기술 표준화 동향 및 전략(한국통신학회, '21.4.)
- [2] 양자정보기술의 시대가 오고 있다(특허청 보도자료, '21.4.)
- [3] 해외 주요국의 양자정보통신 정책 동향(한국통신학회, '21.2.)
- [4] ICT R&D 기술로드맵 2025(정보통신기획평가원, '20.12.)
- [5] 양자 보안이란 무엇인가(한국인터넷진흥원, '20.8.)
- [6] 양자키분배 네트워크를 위한 보안 요구 사항과 양자난수생성기 표준화 동향(한국정보보호학회, '20.8.)
- [7] 차세대 암호기술 '양자내성암호'와 '동형암호'(한국인터넷진흥원, '20.7.)
- [8] 양자키분배 시스템 기술개발 동향(한국전기전자재료학회, '20.)
- [9] 양자정보기술 동향 및 시사점(한국전자통신연구원, '19.4.)
- [10] 양자정보통신 현황과 전망(한국전자통신연구원, '19.)
- [11] 양자암호 기술 보안 표준화 동향(한국정보통신기술협회, '18.)
- [12] 양자암호와 포스트 양자암호에 관한 연구(정보처리학회, '16.)
- [13] 양자정보통신동향(한국전자통신연구원, '15.)
- [14] 물리계층의 신개념 보안통신기술, 양자암호통신(한국통신학회, '14.)
- [15] 양자암호통신 기술 소개 및 동향(정보통신기술진흥센터)

I. 개 요

- 美 CSA의 보고서 「클라우드 기반 인텔리전트 에코시스템*」 주요 내용을 분석하고 시사점을 검토

* 원문명 : Cloud-Based, Intelligent Ecosystems(2020.12.)

참고 CSA(Cloud Security Alliance)

- 2009년 설립된 미국의 비영리 조직으로, 클라우드 보안 관련 연구 및 보고서 발간, 보증 프로그램, 교육 및 자격증 관련 업무를 수행

- 주요 업무

- (조사·연구) 워킹그룹을 운영하여 개인정보보호, 보안 지침, 모범 사례, 프레임워크 등 클라우드 보안 관련 영역 조사 및 연구
- (STAR* 프로그램) 자체 평가(레벨1), 제3자 평가(레벨2)를 통한 클라우드 보안 보증프로그램 운영

* Security, Trust, Assurance and Risk

- (자격증) 클라우드 보안지식 자격증(CCSK), 클라우드 감사 자격증(CCAK) 등 운영

- 본 보고서는 수많은 보안 솔루션 도입이 오히려 기업을 취약하게 만드는 사이버 보안의 문제점으로 지적하면서,

주) 이승봉, 금융보안원 융합보안부 과장

- 해결책으로, 데이터 중심의 보안 운영이 필요하며, 이를 실현하기 위해 클라우드 기반 인텔리전트 에코시스템 구축을 제안

II. 주요 내용

1. 검토 배경

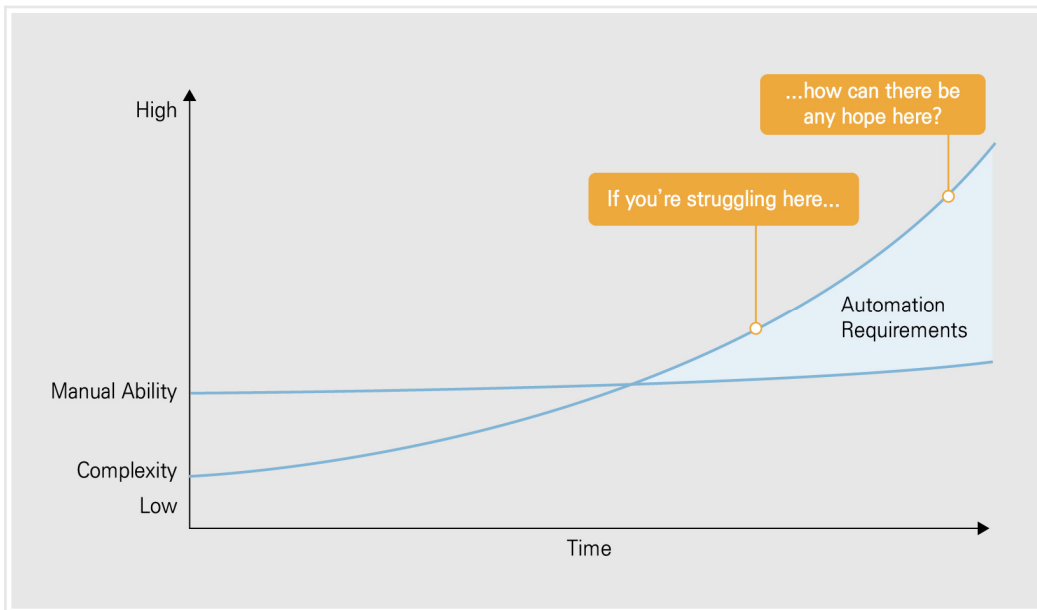
- 기업은 해킹 기술의 지속적인 진화에 따라 이를 방어하기 위해 새로운 유형의 보안 도구(solution, S/W, tool 등) 도입에 계속 투자
 - 보안 도구는 차세대(next-generation)란 이름으로 ‘데이터 손실 방지’, ‘통합 위협관리’, ‘탐지·대응 관리’, ‘사용자 행동 분석’ 등으로 발전하였으나, 모든 사이버 공격을 방어하는 데 한계
- 반복적인 보안 도구 도입을 중단하고, 클라우드 기반 데이터 통합·처리 자동화를 통해 데이터 중심 사이버 방어체계를 마련할 필요

2. 인텔리전트 에코시스템 필요성

(가) 기존 한계점

- 해킹 기술의 발전 및 정교한 공격을 방어하는데 소요되는 경비는 증가한 반면, 보안성 및 효율성은 오히려 감소

참고 기술 발전에 따른 복잡도와 수동 능력의 상관관계



- 기술이 발전함에 따라 복잡도는 급격하게 상승하는 반면, 사람의 수동 처리 능력은 이를 따라가지 못함

참고 기술 발전에 따른 도구 도입의 한계

- 美 시장조사기관(Ponemon)의 설문조사 결과(2020.7.)
 - 기업은 평균적으로 47개의 서로 다른 사이버 보안 솔루션 및 기술을 도입
 - IT전문가 53%는 자신이 도입한 사이버 보안 솔루션이 얼마나 잘 작동하는지 모른다고 응답
 - 응답자 39%만이 보안 투자로부터 목표한 완전한 가치를 얻고 있다고 답변
- 美 보안업체(ReliaQuest)의 보안기술 확산 보고서(2019.12.)
 - 응답자 70%는 지난해 5개 이상의 신기술을 도입하였으며, 19%는 20개 이상 도입하는 등 보안부서의 도구 도입은 점차 증가하고 있다고 평가

- 응답자 71%가 보안기술을 사용할 수 있는 역량을 키우는 것보다 더 빠르게 신기술이 출현하여 보안 도구 구현에 어려움을 겪고 있다고 답변
- 응답자 69%는 보안부서가 보안 도구를 관리하는 데 갈수록 더 많은 시간을 소비하고 있다고 진단하여 도구 유지보수의 부담으로 보안위협 대응 능력이 저하되고 있다고 평가
- 응답자 53%는 자사 보안부서가 지나치게 많은 보안 도구를 도입하여 보안에 부정적인 영향을 미치는 전환점에 도달했다고 판단하는 등 도구의 무분별한 확장으로 인해 기업의 보안 수준이 오히려 저하되었다고 평가

(나) 해결 방안

- 기업이 지속적으로 사이버 이벤트를 탐지, 대응 및 복구하기 위해서는 내부 보안 도구와 인텔리전스 정보의 통합 및 자동화가 구현되어야 하며, 이를 위해 다음의 세 가지 조건이 필요

① 사이버 보안 관점에서 인텔리전스 재정의

- (AS-IS) 보안위협 탐지 및 대응 평균 시간을 줄이기 위해 공격자의 전략, 기술, 방법 등의 외적인 데이터
- (TO-BE) 내부 보안 도구와 외적인 데이터로부터 유의미한 정보를 자동으로 추출, 변환, 정규화하는 조직의 역량

② 사이버 메모리 구축

- 효율적으로 악의적인 활동을 탐지·제거하기 위해 비정상적인 패턴 식별이 무엇보다 중요하므로,
- 내부 보안 도구와 외부 데이터로 구성된 이벤트를 저장하는 가상 메모리를 구축하고 머신러닝을 적용하는 것이 효과적

③ 안전한 인텔리전트 에코시스템 구축 및 유지

- 가상 메모리를 클라우드 기반으로 구축하면, 지속적으로 축적되는 방대한 데이터를 종합적으로 분석할 수 있으며,
- 연결된 사이버 방어 도구에 자동으로 업데이트되고, 다른 기관에 공유되어 합동 방어체계를 구성 가능

(다) 제약 사항

- 데이터 감지, 분석 등을 체계적으로 관리·처리하는 절차의 부재로 인하여 보안 도구 및 외부 데이터의 통합 및 자동화가 난해

참고 데이터 통합의 일반적인 저해 요소

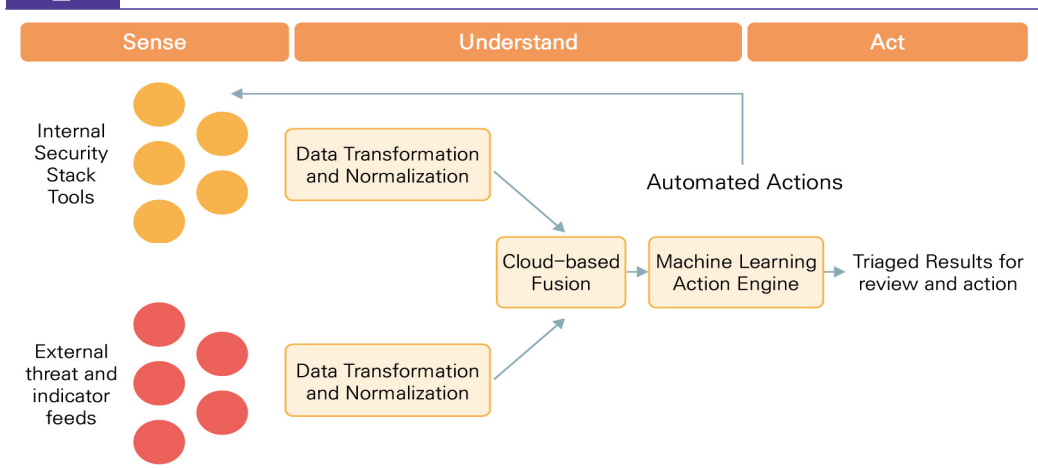
- ① 보안 및 공격 기술의 급격한 변화로 인해 당면한 신규 문제점을 해결하기 급급한 나머지 전반적으로 문제의 근본을 검토하지 못함
- ② TI(Threat Intelligence) 및 SOC(Security Operations Center)는 분리되어 운영되는 경우가 많고, 각 분야 담당자는 각자의 도구로 위협 모니터링에 전념하여 데이터 사일로(Silo)*를 야기
 - * 회사 내부에서 성이나 담을 쌓고 외부와 소통하지 못하는 현상
- ③ 데이터 전송 기술 및 교환 프로토콜이 준비되어 있지 않음
- ④ 보안 도구와 외부 데이터의 상이한 데이터 집합의 정규화 및 변환은 통합 및 자동화를 위한 “죽음의 계곡”
 - * (Valley of death) 스타트업이 처음 자본 출자를 받아 꾸준히 수익을 창출할 때까지 폐업하는 기간을 지칭
- ⑤ 보안 시스템에서 생성된 데이터로 관심이 이동하면서 소프트웨어나 제품 자체보다 데이터로부터 가치를 발견하는 데이터 과학 필요

3. 인텔리전트 에코시스템 구축방안

(가) 데이터 워크플로우 도입

- 데이터 통합 및 자동화를 위하여 내부 보안 도구와 외부 데이터를 신속하게 감지(Sense), 분석(Understand), 처리(Act)하는 데이터 워크플로우 수립 필요

그림 1 데이터 워크플로우 예시



- 센서(내부 보안 도구 및 외부 위협 정보)에서 수집한 데이터를 클라우드에 저장하여 정규화, 변환, 통합하고 머신러닝 학습을 통해 다양한 이벤트를 자동으로 처리함으로써 데이터 워크플로우를 수립

- 데이터 워크플로우는 SOAR* 도구 및 SOC 운영 효율성을 향상시키고 프로세스 워크플로우를 가속화하기 위한 전략적 필수 요소

* Security Orchestration, Automation, Response

- SOC는 다양한 경고 및 사고* 처리**를 위해 데이터를 통합하고 자동으로 처리하는 기능이 필요

* 네트워크 침입, 권한 남용, POS 침입, 자격 증명 스테핑, 신원 침해 등

** 경고 분류, 사고 분석 및 위협 식별 등

(나) 기본 구축 방안

□ 데이터 워크플로우를 강화하고 클라우드 및 머신러닝을 적용한 안전한 인텔리전트 에코시스템 구축

- **(클라우드)** 클라우드는 센서(내부 보안 도구 및 외부 인텔리전스)에서 수집된 데이터 통합 및 분석(데이터 변환, 정규화, 상호 연결 및 강화)에 용이
- **(머신러닝)** 머신러닝은 조직 내 또는 조직 간 이벤트 패턴의 식별 및 분류 자동화 지원
 - 대량의 정보를 효율적으로 활용할 수 있어 새로운 위협 탐지 능력이 향상

참고 머신러닝 적용 시 이점

- ① 정밀도*(precision) 및 재현율**(recall)의 개념을 적용하여 오류의 원인 파악, 평균 탐지시간(MTTD) 및 평균 대응시간(MTTR) 감소, 성능 평가 가능
 - * True라고 예측한 것 중 실제 True의 비율. False Positive의 수가 많을수록 정밀도가 떨어지며, 사이버 보안에서 위협 유형을 정확하게 탐지하는 모델의 능력을 나타냄
 - ** 실제 True인 것 중에 머신러닝 모델이 True로 예측한 비율. False Negative 수가 클수록 재현율이 낮아짐
- ② clustering* 및 entity resolution** 기술을 활용하여 생성된 경고를 분류
 - * 특성이 비슷한 데이터를 합쳐 그룹으로 분류하는 기술
 - ** 중복 데이터 처리 기술
- ③ 과거 데이터 집합으로부터 학습한 머신러닝 모델은 False Positive를 줄이고, 수집된 데이터에 실시간으로 점수를 매김으로써 실시간 공격 탐지가 가능
- ④ 잘 훈련된 머신러닝 모델은 이벤트 및 새로운 지표에 대한 점수를 예측함으로써 실시간으로 정보를 요약하고 조직의 MTTD 및 MTTR을 줄임

(다) 구축 핵심 요소

① 내부 보안 도구 및 외부 인텔리전스 소스는 서로 다른 데이터 집합을 처리할 수 있도록 API 우선 방식으로 구현

② 가공, 결합, 보완할 핵심 데이터 집합 식별

- SIEMs* 및 EDR** 시스템 등 경고를 생성하는 중요한 내부 보안 도구 식별

* 보안 사고 이벤트 관리(security incident event management systems) : 로그, 이벤트 정보 등 데이터의 실시간 모니터링 및 분석 솔루션

** 엔드포인트 탐지 및 대응(endpoint detection and response) : 엔드포인트에서 실행되는 프로세스의 비정상 행위를 정밀하게 탐지하는 솔루션

- 데이터 가공 및 결합 중 예외 처리할 화이트리스트 목록 작성

- 데이터가 필요한 필수 워크플로우 프로세스 도구 식별

- 내부 경고와 연관시킬 외부 위협 피드를 식별

③ 아래 기능을 수행하는 결합 플랫폼 식별

- API 또는 보안 스택 도구에서 데이터를 수집하는 기능

- 이메일 수집 기능

- 보안 도구 데이터 및 지표 저장소(사이버 메모리)

- 다양한 데이터 집합을 정규화하고 변환하는 기능

- 내부 보안 도구의 데이터를 외부 위협 소스와 연관시키는 기능

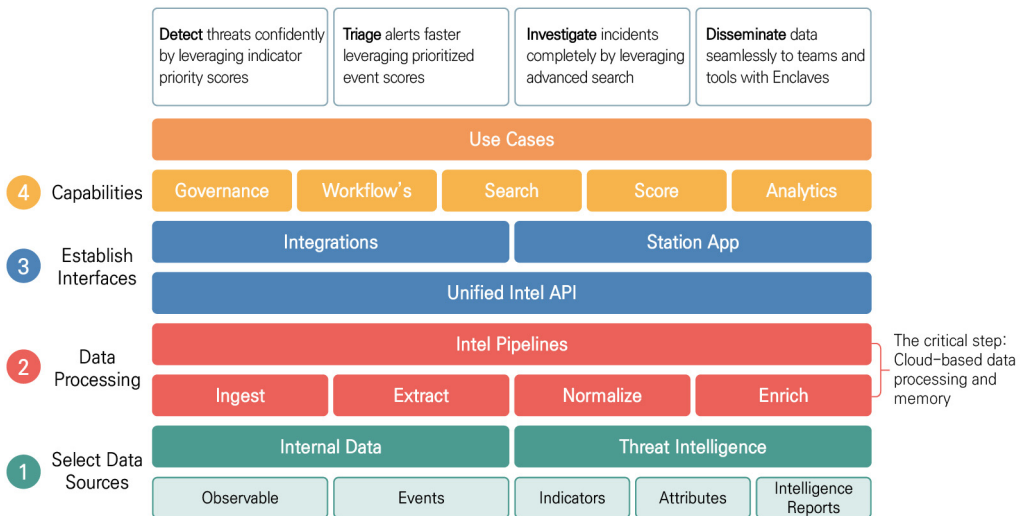
- 사용자 지정 아티팩트*뿐만 아니라 관찰 가능한 아티팩트를 추출하고 연관시키는 기능

* 로그 파일, 애플리케이션 생성 파일 등

- 내부 및 외부 데이터 집합의 질을 높이고 SIEM, EDR, 사례 관리 및 오케스트레이션 플랫폼 등의 보안 스택 도구를 양방향으로 업데이트하는 기능

- 머신러닝을 적용하여 패턴을 식별하고 적절한 태그를 사용하는 기능
- 데이터에 대한 적절한 액세스 및 보안 제어 기능(멀티팩터 인증, 관리 제어 권한)
- 데이터를 신속하게 수정하고 관련자와 데이터를 공유하는 기능

그림 2 인텔리전트 에코시스템 성숙도 모형



➤ 인텔리전트 에코시스템 성숙도는 4단계로 정의

- ① (데이터 수집) 내부 보안 도구 생성 데이터와 외부 위협 정보 수집
- ② (데이터 처리) 수집한 정보를 클라우드에서 수집, 추출, 정규화, 강화
- ③ (인터페이스 형성) 정보 API 통합 및 응용프로그램 배치
- ④ (활용) 거버넌스, 워크플로우, 검색, 점수 측정, 분석에 활용
⇒ (효과) 위협 탐지, 경고 분류, 사고 조사, 데이터 배포에 효과적

III. 결론 및 시사점

- (뉴패러다임) 기존 보안 도구에만 의존하는 사이버 방어체계에서 벗어나 클라우드 및 머신러닝을 활용한 데이터 중심의 인텔리전트 에코시스템 구축을 제안함으로써 새로운 보안 패러다임을 제시

- **(클라우드, 머신러닝, 데이터)** 클라우드, 머신러닝, 데이터를 보안 분야에 활용 시 가져다주는 이점에 주목할 필요
 - **(클라우드)** 데이터 통합, 분석 및 기관 간 사이버 방어 관련 정보 공유에 용이
 - **(머신러닝 및 데이터)** 과거 데이터를 머신러닝이 학습함으로써 False Positive, False Negative를 줄이고, 실시간 공격 탐지 가능
- **(추가 고려사항)** 중독공격*, 회피공격** 등 AI 관련 공격에 대한 대응 방안을 마련하고, 보안 도구 및 외부 데이터의 무결성, 신뢰성 보장을 위하여 블록체인 기술 연계도 고려해 볼 필요

* 학습 과정에서 악의적인 학습 데이터 주입하여 머신러닝 모델을 망가뜨리는 공격

** 머신러닝 모델 추론 과정 및 데이터를 교란하여 머신러닝을 속이는 공격

I. 검토 배경

- 세계 각국*에서는 중앙은행 디지털화폐(CBDC, Central Bank Digital Currency)를 개발 검토 중

* (소매용) 바하마, 캄보디아, 중국, 우크라이나, 우루과이, 에콰도르, 스웨덴 등
(도매용) 태국, 홍콩, 싱가포르, 캐나다, 영국, 프랑스, 유럽, 일본 등

- 중국인민은행은 '22년(베이징 동계 올림픽) 디지털위안 상용화를 목표로 시범 사용(전국 단위 및 인근 국가 간 역외결제) 진행 중
- 미국 보스턴 연방준비은행과 MIT는 디지털달러 연구 성과 일부와 프로토타입 공개 예정('21.3분기)
- 한국은행은 「CBDC 모의실험 연구*」 착수 예정('21.8월)

* 모의실험 환경을 구현하고 CBDC의 활용성 및 제반 업무의 정상 작동 여부 테스트

- '20.10월, 캄보디아 중앙은행(NBC)은 CBDC 프로젝트 “바콩(Bakong)”을 실현하기 위해 차세대 결제 시스템을 출시

※ 바하마 샌드달러(Sand Dollar)에 이어 세계 2번째 CBDC 개발 사례

- 허가형 블록체인, 오픈 소스* 활용, 계좌 기반, 폐쇄망 연결이 특징

* Hyperledger Iroha : 디지털 자산, 신원, 데이터 등을 관리하는 허가형 블록체인 플랫폼

- 화폐 발행 기능이 없어 중앙은행은 바콩을 CBDC가 아닌 차세대 결제 시스템으로 언급

※ 단, 시스템 개발사(日 소라미츠)에서는 바콩을 CBDC로 홍보 중

주) 김지훈, 금융보안원 융합보안부 대리

⇒ 이에 캄보디아 중앙은행 백서 등을 바탕으로 바콩 CBDC의 구현 특징을 조사하고 한국은행 CBDC와의 차이점을 분석함

참고 중앙은행 통화 체계 비교

▶ 소매용 결제 수단 비교

항목	현금	CBDC	간편결제 시스템
청산 자산으로서의 안전성	중앙은행의 직접적인 부채		상업은행의 부채, 예금보험, PSP*
소액결제 완결성	수령 즉시 (물리적 근접성)	참여자(PSP) 승인 즉시	
거액결제 완결성	거액결제 청산 없음	일괄청산(일일청산) 없음	은행 간 일괄청산 또는 실시간종액결제
사용자 및 상점 측면 비용	비교적 낮음	디자인 선택 (현금 및 타 디지털 결제와 경쟁)	일반적으로 낮음 (다른 서비스의 이득으로 유지)
신원확인 요구사항	없음 (고액결제 예외)	디자인 선택 (계좌 또는 토큰기반, 구현 여부에 따라 다름)	있음
사용자 익명성	높음		낮음
사용자 비밀보장	높음		시스템 디자인, 은행비밀보호법, 데이터보호법
오프라인 결제	가능		불가능
신규 디지털 기능	없음	전자상거래, 프로그래밍 가능한 소액결제	
역외결제	환전·송금 (거래 한도·규제)	현금에 비해 편리, 저렴한 수수료	국외 간편결제 시스템과 연결

* PSP : 지급결제 서비스 제공사(Payment Service Provider)

▶ 가치저장 속성 비교

항목	현금	CBDC		상업은행 예금
		계좌기반	토큰기반	
청구권	중앙은행			상업은행
안전장치	중앙은행 보장			예금보험
위험	분실, 절도, 사기	사기, 사이버위험	분실, 절도, 사기, 사이버위험	사기, 사이버위험, 유동성 부족, 파산
익명성	가능	불가능	가능	불가능
금리	없음	중앙은행 지정	중앙은행 지정 (오프라인 토큰 불가)	은행 지정

※ [출처] Bank for International Settlements(BIS), CBDC : an opportunity for the monetary system, BIS Annual Economic Report, '21.6.23.

II. 바콩 개발 목적

◆ 캄보디아 중앙은행은 '16년부터 ①자국 지급결제 시스템 개선, ②금융 포용성 확대, ③자국 화폐 사용 촉진을 목표로 개발 추진

참고 프로젝트 바콩 추진 경과

년도	추진내용
'16	- 캄보디아 중앙은행 내 워킹그룹 설립 (지급결제 시스템에서 블록체인 및 분산원장기술 사용)
'17	- 유스케이스 및 프로토타입 개발 - 분산원장기술 플랫폼으로 Hyperledger Iroha 선정
'18	- 프로토타입 테스트 결과 평가 - 비즈니스 프로세스, 시스템 프로세스, 내부 통합 시스템 조정 - 시연 및 논의를 위한 참여사(금융사, PSP) 모집
'19	- 시범 출시(4개 참여사) - 전국 단위 시범 출시(참여자 추가) - 역외 거래 실험 시작(말레이시아 Maybank 참여)
'20	- 백서 발표 - 정식 출시(16개 금융사, 2개 PSP)
'21	- 참여사 추가('21.6월 기준 21개 금융사, 4개 PSP)

① 자국 지급결제 시스템 개선

□ (기존 환경) 실시간 지급결제가 어려우며 업권별로 지급결제 시스템이 별도 구축된 환경

○ (거래 청산*) 업무 시간 중 하루 2회로 제한(일괄청산)

* NCS(National Clearing House)에서 수행

- (계좌 이체*) 대면**으로만 동일 은행 내에서 실시간 송금 가능(일일 1만 USD 상당 한도)

* 중앙은행의 FAST(Fast and Secure Transfer) 시스템 활용

** 대부분 은행이 인터넷·모바일 뱅킹 미제공

- (카드 결제) 역내 인프라* 참여사 간 상호호환은 가능하나, 24시간 운영 불가

* ATM 및 POS 단말 기반의 캄보디아 내 직불카드 지급결제 인프라

⇒ (개선 목표) 여러 참여사(금융사 및 PSP*) 및 고객이 통합 시스템을 사용하여 실시간 지급결제 지원(24시간 운영)

* 지급결제 서비스 제공사(Payment Service Provider)

② 금융 포용성 확대

- (기존 환경) 스마트폰 보급률은 96%로 상대적으로 높으나, 은행 계좌 보유율은 22%로 낮은 편

※ 대부분 은행이 인터넷·모바일 뱅킹 미제공으로 비대면 계좌 개설이 곤란

- 개별 회사마다 결제 서비스·앱을 출시하여 상호 호환 불가

⇒ (개선 목표) 중앙은행에서 상호호환이 가능한 비대면 계좌 개설 및 전자 금융거래 환경 제공

③ 자국 화폐 사용 촉진

- (기존 환경) 미국 달러(USD) 거래가 대부분

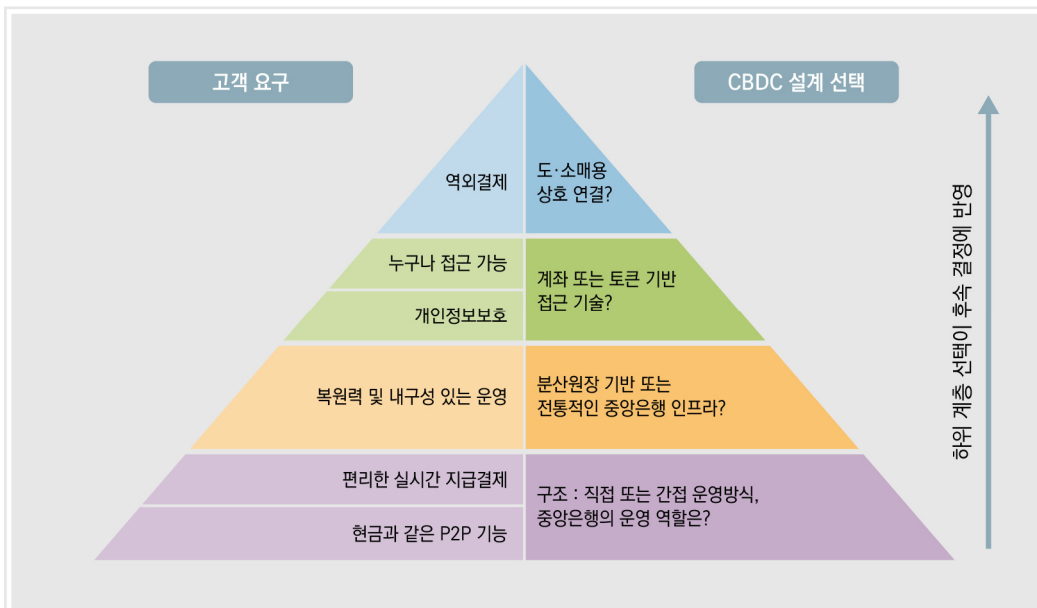
⇒ (개선 목표) 캄보디아 리엘(KHR) 사용 촉진 플랫폼으로 활용

Ⅲ. 바콩 구현 특징

1. 설계 측면

◆ CBDC는 고객의 요구에 따라 여러 설계 선택사항이 존재하며 중앙은행이 이를 선택하여 구현

참고 CBDC 설계 선택사항



※ [출처] Bank for International Settlements(BIS), The technology of retail central bank digital currency, BIS Quarterly Review, '20.3.1.

□ (실시간 거래) 탈중앙화 및 실시간 지급결제 지원

○ 고객 간(P2P) 직접 거래(바콩·은행 계좌 간 송금*, QR코드 결제)

* 바콩 네트워크를 통해 디지털화폐·은행 예금 송금 및 전환 가능

○ 거래 시간은 5초 이내

- (운영방식) 중앙은행은 참여사의 바콩 계좌를, 참여사는 고객의 바콩 계좌를 관리하는 간접 운영 구조 추구

※ [별첨 1] CBDC 구조 참조

- (시스템 업그레이드) 기존 FAST 시스템 업그레이드

- FAST의 유저 인터페이스(GUI), API, 게이트웨이 유지하되, 관계형 DB를 허가형 블록체인(Hyperledger Iroha)*으로 교체

* [별첨 2] 하이퍼레저 이로하(Hyperledger Iroha) 참조

- 역할 기반 접근 제어(role-based access control)* 활용

* 관리자가 그룹의 역할을 정의하고 적절한 권한을 부여하는 접근 제어 정책

- (블록체인) 거래 데이터를 블록체인에 저장

- 중앙은행 내 폐쇄망 인프라에 블록체인을 구축하여 중앙은행이 참여사에게 블록체인 노드 접속 권한을 부여하고 중앙은행 내 각 블록체인 노드는 거래의 유효성 확인

※ 비잔틴 장애 허용 합의 알고리즘('Byzantine Fault Tolerance' Consensus Algorithm) 적용 : 노드 장애(중단, 오류, 악의적 행동 등) 발생이 전체의 1/3 미만이면 시스템이 정상 작동하도록 허용

참고 CBDC와 블록체인 기술

- ▶ 블록체인이 CBDC 개발 시 필수 요소는 아니지만 여러 이점 존재
 - (소유권 전송) 가치를 공유하고 소유권을 전송하는 통합 플랫폼으로 디지털 자산 지원을 위한 핵심 요소
 - (프로그래밍 가능성) 사전에 프로그래밍된 조건에 의한 자동화된 지급결제
 - (감사(audit)) 변조 불가능한 투명한 거래 기록 활용
 - (상호호환성) 타 디지털 자산(타 국가 CBDC) 간 교환
 - ※ 서로 다른 블록체인 기반의 디지털 자산 간 교환을 지원하는 아톰릭 스왑(Atomic swap) 활용
- ▶ 전 세계 CBDC 프로젝트 중 88% 이상이 파일럿 또는 제작 단계에서 블록체인 활용

※ [출처] PwC, CBDC global index (1st Edition), '21.4월

□ (계좌 기반 가치저장) 계좌(account) 기반의 디지털화폐 구현

참고 CBDC 가치저장 방식(계좌기반, 토큰기반) 비교

가치저장	특징
계좌기반	- (가치저장) 은행 계좌처럼 신원확인을 거친 CBDC 계좌에 가치저장 - (가치이전) 가치이전 시기는 '수신자' CBDC 계좌에 가치이전 금액이 기재되는 시점 - (거래시작) 고객의 신분증 등을 통한 신원확인 후 거래 시작
토큰기반	- (가치저장) 교통카드 등 선불지급수단처럼 카드, 스마트폰 등에 가치저장 - (가치이전) 가치이전 시기는 CBDC 저장매체(스마트폰 등)에 데이터가 수수(收受) 되는 시점 - (거래시작) 고객이 보유한 암호학적 지식(개인키로 디지털 서명 생성)에 기반하여 거래가 시작되며 익명성* 지원 * 신원확인 수행은 고객의 선택사항(거래 한도 상향, 분실 시 복구 등 지원) ※ 경기도 지역화폐 카드는 무기명 선불카드로 발급되며 앱을 통해 카드 등록 후 분실신고 및 재발급, 소득공제 신청 등 가능

□ (기본 컴플라이언스) 참여사가 고객확인업무(KYC, Know Your Customer)* 및 자금세탁방지(AML, Anti Money Laundry) 수행

* 계좌 개설 시 실명확인증표(신분증·여권) 사본 제출, 실명확인증표 사진과 얼굴촬영화면을 AI 알고리즘으로 비교, 1회용 인증번호(OTP) SMS 확인

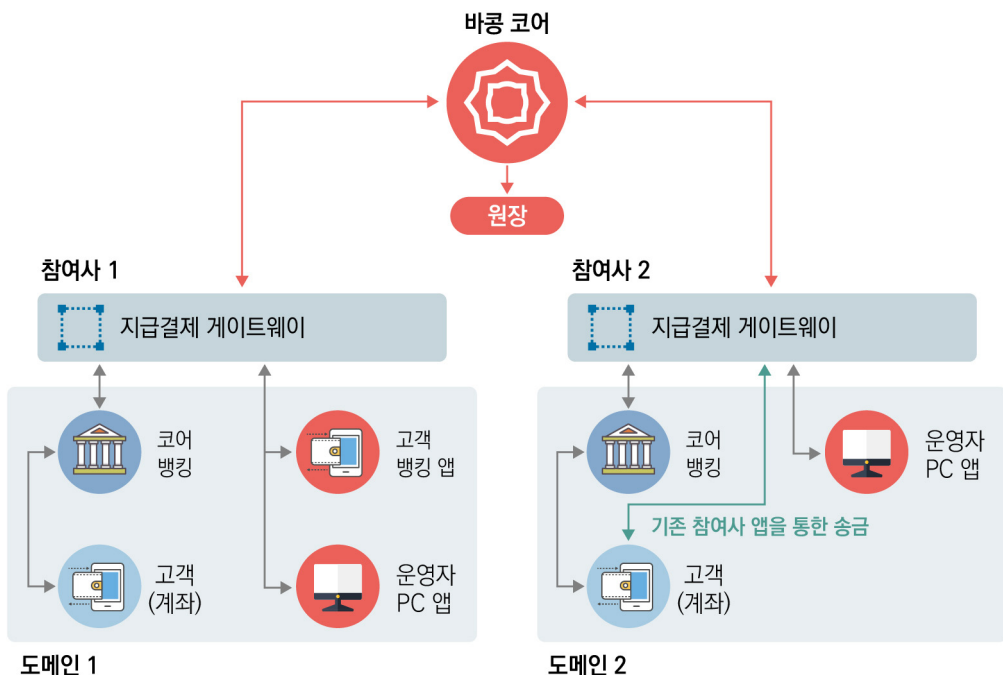
※ 캄보디아 신분증(여권) 및 휴대전화번호, 스마트폰을 소지한 캄보디아 국민만 사용 가능

○ 중앙은행은 거래 당사자의 신원을 드러내지 않음

2. 구조 측면

◆ 바콩 구조는 ①바콩 코어, ②지급결제 게이트웨이, ③도메인으로 구분

그림 1 바콩 구조



□ (바콩 코어) 분산원장 및 거래 처리 역량을 갖춘 시스템

- 지급결제 시스템이 처리한 모든 거래를 블록체인에 저장하여 모든 분산원장 노드에는 같은 데이터가 저장됨

□ (지급결제 게이트웨이) 참여사가 중앙은행으로부터 권한을 부여받아 바콩 네트워크에 연결

- 참여사가 고객확인의무(KYC) 및 거래 한도를 관리하고 고객 거래를 모니터링

□ (도메인) 참여사별로 도메인이 부여되어 고객의 바콩 계좌를 생성 및 관리

- (코어 बैं킹) 모든 고객 거래를 처리하는 시스템

- (고객 계좌) 캄보디아 리엘(KHR), 미국 달러(USD) 계좌 각각 개설 가능 (환전 불가)

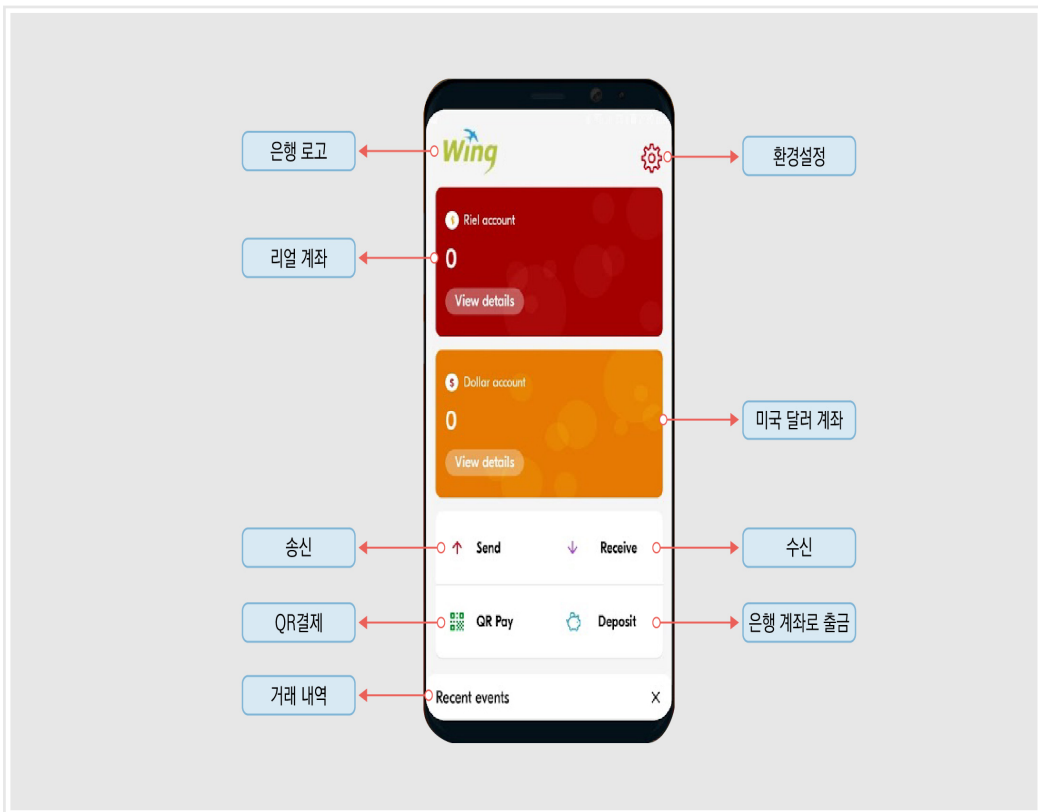
※ 보통예금 계좌(공동계좌, 정기예금 계좌 개설 불가)이며 이자 없음

- 계좌이체*를 통해 현금(은행 예금)을 디지털화폐로 전환

* 참여사의 인터넷·모바일 बैं킹 활용 또는 지점 방문(무통장입금)

- (고객 बैं킹 앱) 고객은 중앙은행이 제공하는 바콩 스마트폰 앱을 통해 계좌 접근

참고 바콩 스마트폰 앱 메인 화면



※ [출처] National Bank of Cambodia, Bakong System User Manual: Generic Mobile Application

○ (운영자 PC 앱) 참여사는 중앙은행의 PC 앱으로 계좌 접근

3. 계좌 관리 측면

□ (참여자 계좌) 참여사의 바콩 계좌는 중앙은행에 등록

○ 타 참여사의 바콩 계좌 및 은행 계좌, 중앙은행 청산 계좌와 거래 가능

□ (고객 계좌) 고객의 바콩 계좌 생성 시 거래 한도 적용

○ 거래 한도 상향*을 위해서는 대면 확인(은행 지점 방문) 필요

* 상향 전 : 일 500 USD (또는 2백만 KHR)

상향 후 : 일 2,500~50,000 USD (은행별 상이, 고객이 한도 축소 가능)

※ 일부 은행의 바콩 계좌 잔고는 거래 한도 초과 불가

○ 디지털화폐 송·수신을 위해 ①계좌 ID, ②전화번호, 또는 ③QR코드* 활용

* 금액 입력 : 수신자(상점)가 금액을 입력 후 QR코드를 생성하는 방식 또는 수신자(상점)의 QR코드를 송신자가 촬영 후 금액을 입력하는 방식 모두 지원

○ 타 바콩 계좌 또는 은행 계좌로 이체 가능

○ QR코드를 통한 계좌 복구 지원*

* 미리 생성한 복구용 QR코드 촬영 및 비밀번호를 입력하여 계좌 복구

4. 운영 측면

□ (거래 완결성) 블록체인에 기록된 거래는 취소가 불가하므로 사기 또는 잘못된 거래의 차단이 중요

○ 각 블록체인 노드에서 거래 건별로 실행 시점에 유효성 검증

참고 이중지불 차단(유효성 검증) 시나리오

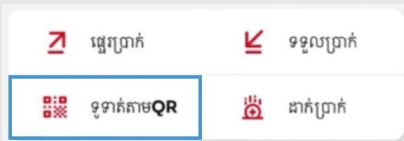
- ▶ A의 잔고는 1,000원으로 블록체인에 기록된 상태
- ▶ A가 B에게 1,000원을 송금하여 A의 잔고는 0원임
(블록체인에 송금 내역 및 A, B의 잔고 기록)
- ▶ A가 C에게 1,000원 송금(이중지불) 시도
- ▶ 각 블록체인 노드는 A의 잔고를 블록체인에서 확인 후 잔고 부족으로 송금 거절

○ 검증된 거래는 블록체인에 기록

- (성능) 5초 이내 거래 완료 및 초당 2천 건 거래 처리
- (복원력) 합의 알고리즘 적용으로 일부 노드의 장애 대응
 - 시스템 동작 중 블록체인 노드 추가 또는 삭제 가능
- (청산 시스템) 바콩 플랫폼과 중앙은행 내 청산 시스템 연결
 - 중앙은행 및 참여사(바콩 계좌 및 은행 계좌) 간 청산* 수행
 - * 청산 계좌의 잔고는 일 1회 갱신
- (개인정보보호) 고객정보와 거래정보 분리 저장
 - 고객확인 의무(KYC) 및 자금세탁방지(AML) 수행 시 고객정보는 참여사 시스템에 저장
 - IP 주소 등 거래정보는 블록체인에 저장(고객정보 제외)
- (QR코드 결제) QR코드 결제 국제표준 적용으로 참여사 앱 또는 POS 단말에서 바콩의 QR코드 인식 및 결제 처리 가능
 - ※ 간편결제 인터페이스와 연동 가능(간편결제 서비스 연동 계좌로 결제 대금 입금)

참고 QR코드 결제 시나리오

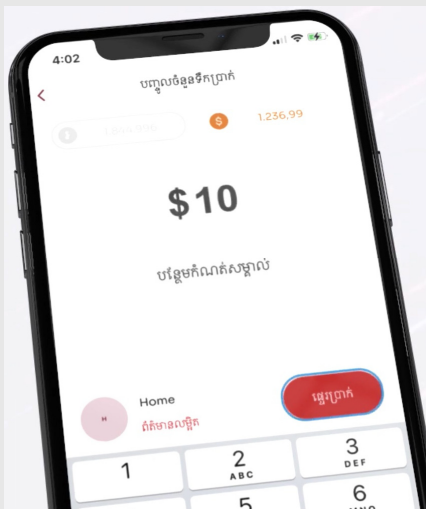
① 고객은 바콩 앱 메인 화면에서 'QR Pay' 선택



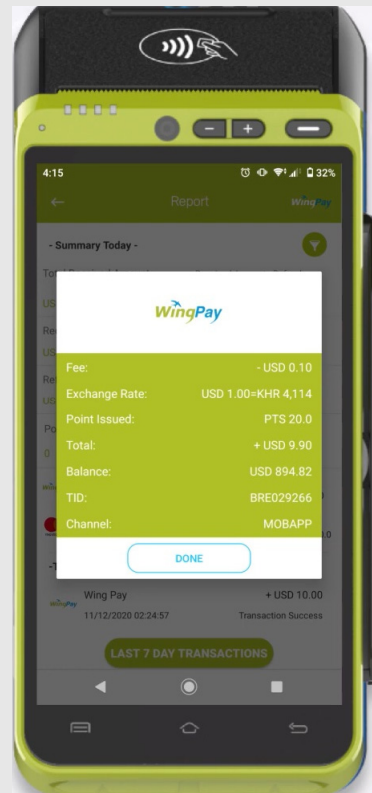
② 상점의 바콩 또는 간편결제 QR코드를 바콩 앱으로 인식



③ 고객은 상품 가격을 입력 후 거래 대금 지불



④ 상점의 POS 단말에서 거래 내역 (입금액 및 수수료 등) 확인



※ 바콩은 QR코드 결제 국제표준을 준수하는 간편결제 등 타 인터페이스와 호환 가능

※ [그림 출처] Wing, Bakong x Wing: The Next-Generation Mobile Payments and Banking

IV. 향후 필요 조치사항

◆ 캄보디아 중앙은행은 출시한 ‘바콩’을 자체 평가 후 예상되는 위험에 대한 향후 필요 조치사항을 언급

□ (뱅크런 우려) 디지털화폐의 현금전환이 용이하므로 ‘경제위기’, ‘은행파산’ 등의 위기 상황에서 다수 고객의 디지털화폐 대량 인출(뱅크런) 발생 우려

○ 중앙은행 또는 참여사의 청산계좌에 대한 인출 한도 제한 강화 등이 필요

□ (사이버 위협 증가) 다수의 참여사를 대상으로 하는 ‘악성코드’, ‘보이스피싱’ 등 사이버 위협 증가 우려

○ 중앙은행이 시스템 및 서비스에 대한 엄격한 보안 요구사항을 제도화할 필요

참고 보안 평가 내역

▶ Nettitude(영국 사이버보안 회사) : 화이트박스 테스트, 종합적인 침투 테스트

▶ 캄보디아 중앙은행 : 별도 보안 검토(review) 및 감사(audit)

▶ 회계법인 : 코드 감사(딜로이트) 및 플랫폼 사업 측면 감사(KPMG)

□ (기타 위험) 예기치 못한 시스템 장애 등으로 인해 지급결제 서비스의 전체 또는 일부 중단(연기) 현상 발생 우려

○ 발생 가능한 위험 시나리오에 대한 상세 업무연속성계획(BCP) 마련 필요

※ 인프라 이중화, 대체 운영 사이트, 원격 운영, 신속한 복구 등

V. 한국은행 CBDC와의 차이점

※ 한국은행은 CBDC 모의실험 연구를 추진 중으로 CBDC 설계 방식이 확정된 것은 아님

□ (추진 목적) 바코드는 ‘금융 포용성 확대’, ‘자국 화폐 사용 촉진’ 등을 위해 기존 지급결제 시스템을 업그레이드한 반면,

○ 한국은행은 현금 수요 감소 등 미래 지급결제 환경 변화에 대비하여 CBDC에 대한 제도적·기술적 필요사항을 우선 검토

□ (실시간 거래) 현금과 같은 실시간 지급결제시스템 구축은 동일

□ (블록체인 기반) 바코드는 중앙은행 내 폐쇄망 인프라에 블록체인 노드를 구축한 반면,

※ 기존 시스템의 관계형 DB를 블록체인으로 교체하여 거래 데이터의 무결성을 보장하나 모든 블록체인 노드가 물리적으로 한 기관에 종속되어 분산 정도가 다소 낮음

○ 한국은행 CBDC는 한국은행 및 참여사 인프라에 블록체인 노드를 구축하여 서로 연결할 것으로 예상

※ 한국은행 「CBDC 모의실험 연구」 제안요청서 중 ‘검증계 구성도 예시’에 근거

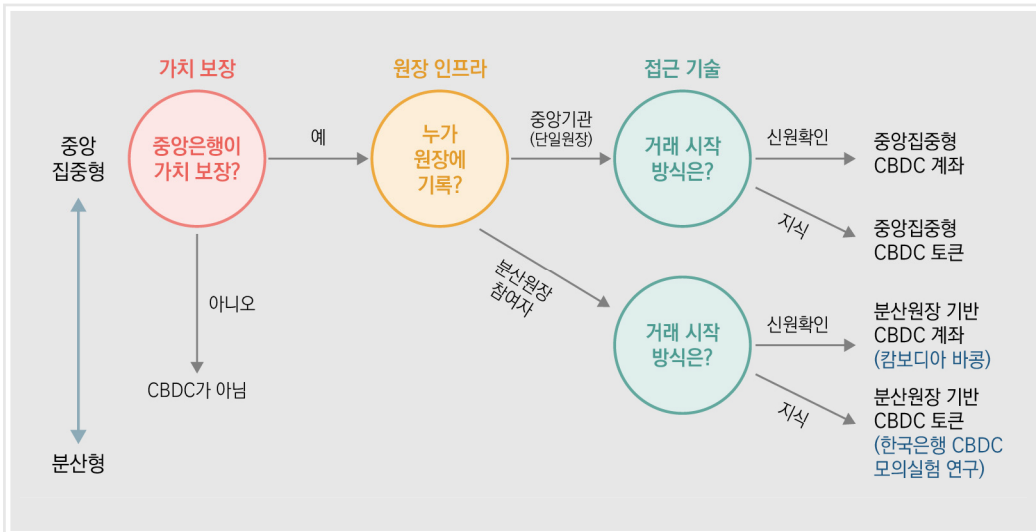
□ (가치이전 방식) 바코드는 계좌기반 방식으로 구현한 반면,

○ 한국은행 CBDC는 토큰기반 방식으로 구현할 것으로 예상

※ 모의실험 연구에서 전자지갑 발급·관리 등 기능 포함

□ (디지털화폐 관리) 중앙은행이 참여사의 계좌·토큰을 발급·관리하고 참여사는 고객계좌·토큰을 발급·관리하는 점은 유사

참고 원장 인프라 및 접근 기술에 따른 CBDC 분류



※ [출처] Bank for International Settlements(BIS), The technology of retail central bank digital currency, BIS Quarterly Review, '20.3.1.

□ (화폐 발행) 바콩은 디지털화폐 발행 기능이 없는 반면,

※ 계좌이체를 통해 현금 또는 은행 예금을 디지털화폐로 전환

○ 한국은행 CBDC는 디지털화폐 제조·발행·환수가 가능

참고 한국은행의 CBDC 제조·발행·환수 기능

- ▶ (제조) 중앙은행은 물리적으로 네트워크가 단절된 안전한 컴퓨터 환경에서 CBDC를 제조하여 발행 전까지 하드웨어 전자지갑에 보관
- ▶ (발행) 참가기관이 CBDC 발행을 요청하면 당좌예금 잔액을 차감하고 해당 기관의 전자지갑으로 제조된 CBDC를 전송하여 발행
- ▶ (환수) 참가기관이 반환할 CBDC를 중앙은행 CBDC 전자지갑으로 전송하면 중앙은행은 해당 기관의 당좌예금 잔액을 조정

※ [출처] 한국은행, (보도참고자료) 「중앙은행 디지털화폐 모의실험 연구」 용역 사업자 선정을 위한 입찰 공고 안내, '21.5.24.

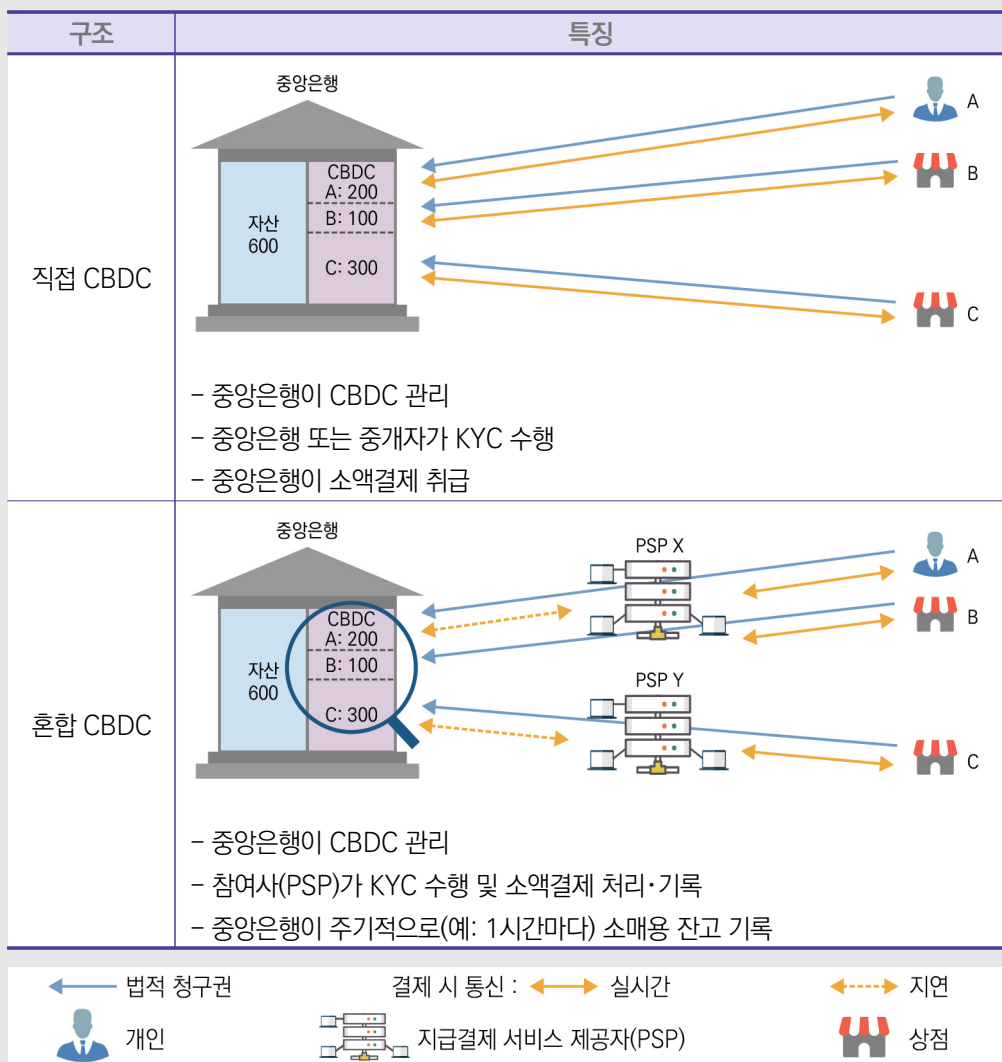
□ (스마트 계약) 바코드는 스마트계약을 지원하지 않는 반면,

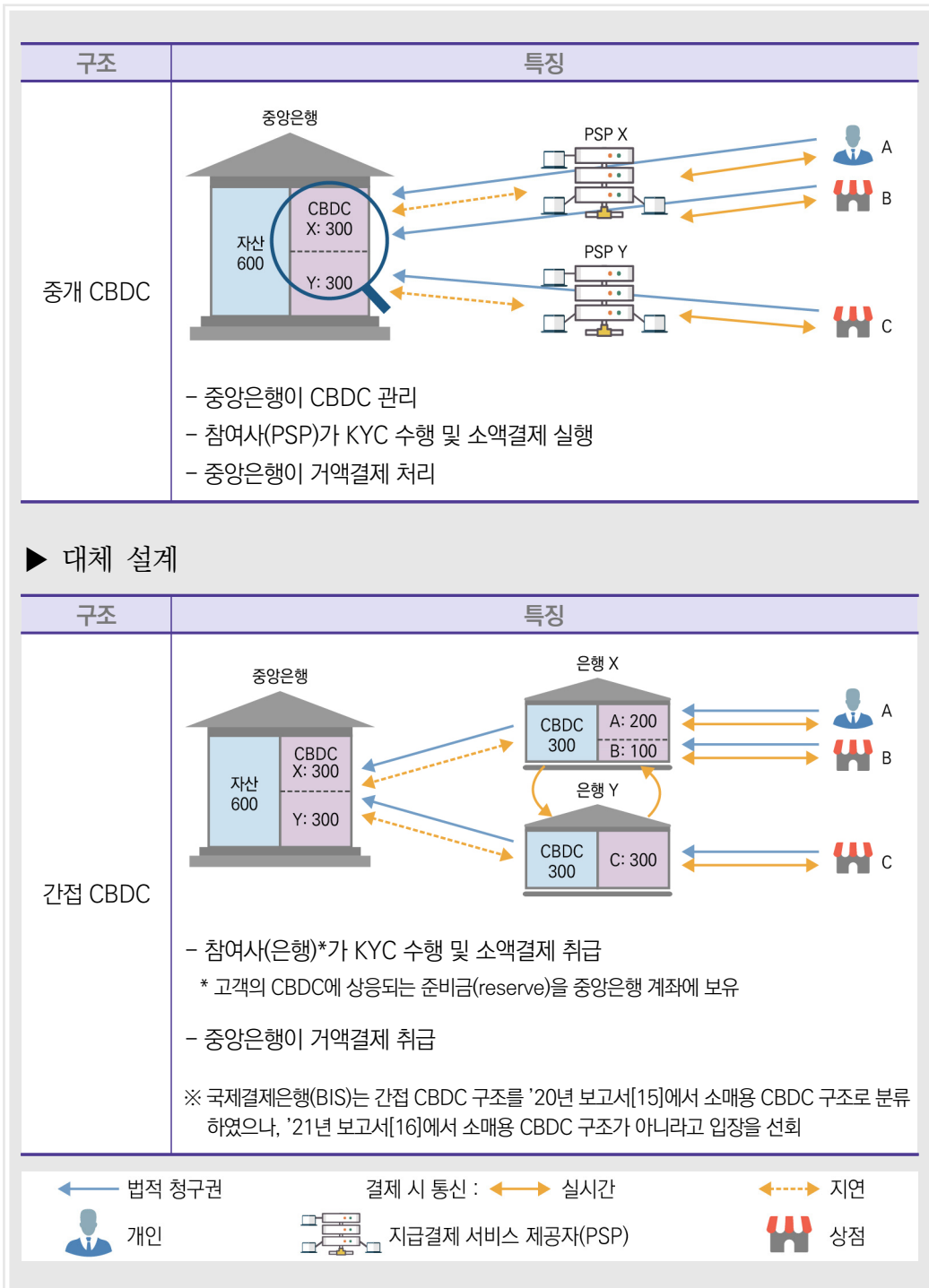
※ 기반 시스템인 하이퍼레저 이더가 스마트 계약을 지원하지 않음에 기인

○ 한국은행 CBDC는 요구사항에 스마트계약 지원을 명시

별첨 1 CBDC 구조

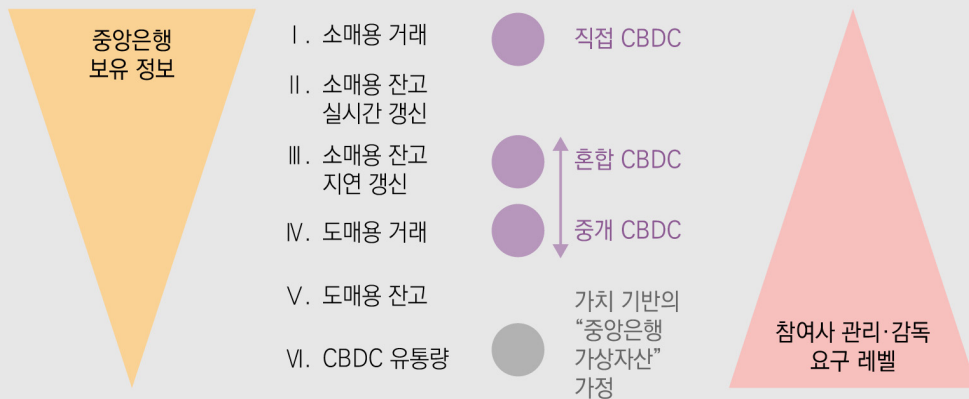
▶ 소매용 CBDC





▶ CBDC 구조 trade-off

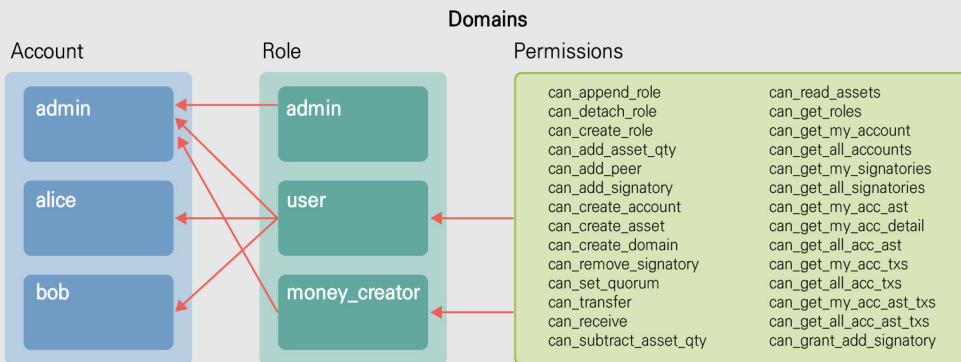
- 중앙은행 보유 정보가 많을수록 개인정보에 민감하나 범죄 예방에 유용
- 중앙은행 미보유 정보는 참여사에게 기록 및 관리 위임
- 참여사 관리·감독을 통해 시스템 점검 및 필요시 중앙은행 미보유 정보를 취득



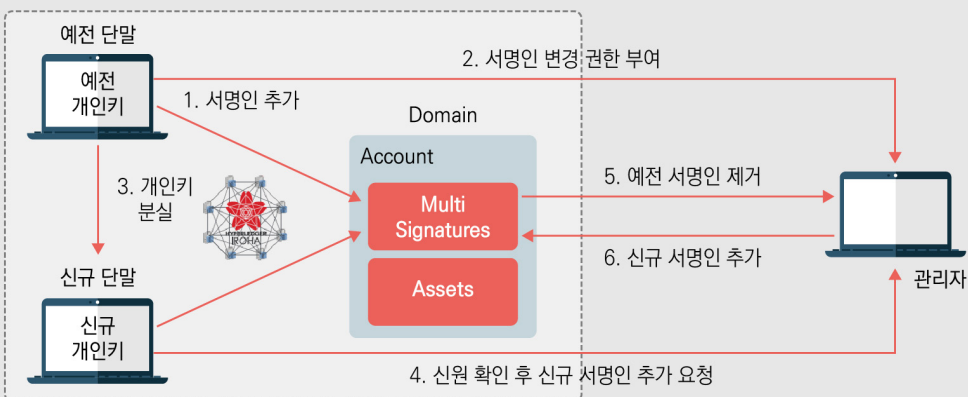
※ [출처] Bank for International Settlements(BIS), Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers No. 948, '21.6.8.

별첨 2 하이퍼레저 이로하(Hyperledger Iroha)

- ▶ (개요) 디지털 자산, 신원, 데이터 등을 관리하는 비즈니스 블록체인 플랫폼
 - 사전에 정의된 명령어를 사용하여 디지털 자산 생성 및 전송(스마트 계약 없음)
- ▶ (특징) 허가형 블록체인, 오픈 소스, 개발자를 위한 다양한 라이브러리 지원, 비잔틴 장애 허용 합의 알고리즘 적용, 모듈식 설계, 명령-쿼리 분리 원칙 등
- ▶ (접근 제어) 역할 기반 접근 제어(Role-Based Access Control, RBAC)
 - 계정(Account)에 역할(Role)을 부여하고 역할(Permission)별로 권한을 설정



- ▶ (키 복구) 개인키 분실 시 관리자와의 신원확인을 통한 개인키 변경 지원



- ▶ (유스케이스) 교육·의료 분야 증명서, 자산 국제송금, 신원 관리, 펀드 관리 등

※ [그림 출처] Soramitsu, Creating a better world through decentralized technologies, '19.12월



- [1] National Bank of Cambodia, Bakong – The Next-Generation Mobile Payments and Banking, <https://bakong.nbc.org.kh/en/>
- [2] National Bank of Cambodia, Project Bakong: Next Generation Payment System, '20.6월
- [3] National Bank of Cambodia, Bakong System – User Manual (Version 3.6.3)
- [4] RadioFinance, Cambodia's Serey clarifies: "Bakong is not a digital currency", '20.11.11.
- [5] Soramitsu, Kingdom of Cambodia Launches Central Bank Digital Currency, Co-Developed with Fintech Company Soramitsu, '20.10.28.
- [6] Global Blockchain Business Council, Soramitsu on Project Bakong: the First Retail Payments System Run by a Central Bank Using Blockchain, '20.4.30.
- [7] Hyperledger, Case Study: The National Bank of Cambodia boosts financial inclusion with Hyperledger Iroha, '20.11.12.
- [8] ABA Bank Cambodia, Bakong – ABA Transfers
- [9] ACLEDA Bank Plc., Fees and Limitations for ACLEDA Mobile's Fund Transfer
- [10] Cambodian Public Bank Plc., Bakong Payment System
- [11] Chief (Cambodia) Commercial Bank Plc., Bakong
- [12] LOLC (Cambodia) Plc., Bakong
- [13] PRASAC Microfinance Institution, Bakong Payment Service
- [14] Wing, Bakong x Wing: The Next-Generation Mobile Payments and Banking
- [15] Bank for International Settlements (BIS), The technology of retail central bank digital currency, BIS Quarterly Review, '20.3.1.
- [16] Bank for International Settlements (BIS), Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers No. 948, '21.6.8.
- [17] Bank for International Settlements (BIS), CBDC: an opportunity for the monetary system, BIS Annual Economic Report, '21.6.23.
- [18] PwC, CBDC global index (1st Edition), '21.4월
- [19] Hyperledger Iroha Documentation, <https://iroha.readthedocs.io/>

- [20] KOTRA 해외시장뉴스, 캄보디아 금융업, '20.10.26.
- [21] 한국은행, 중앙은행 디지털화폐, '19.1.25.
- [22] 한국은행, 「CBDC 모의실험 연구」 제안요청서, '21.5.24.
- [23] 정보통신정책연구원, CBDC 설계 고려사항 및 최근 동향, '21.5.30.

I. 검토 배경

□ AI, 클라우드 등 디지털 신기술의 발전과 팬데믹에 따른 비대면 문화 확산 등으로 금융의 디지털 전환이 급속하게 진행

○ 이러한 환경 변화는 사이버 공격 빈도의 증가*와 그에 따른 피해 규모 확대** 등 사이버보안 리스크의 상승으로 연결

* '19년 대비 '20년 한 해 동안 악성 소프트웨어는 358%, 랜섬웨어는 435%, 공급망 공격은 420% 증가
(출처 : Forbes, "Alarming Cybersecurity Stats", '21.3.2.)

** 美 Cybersecurity Ventures는 전 세계 사이버 범죄 피해 규모가 '19년 5조 2,470억 달러에서 '21년 6조 9,390억 달러, '25년에 10조 5,000억 달러에 이를 것으로 전망

□ 디지털 전환이 빠르게 진행된 금융분야에서의 사이버보안 사고는 중요 대고객 서비스 중단 등 금융회사의 운영에 큰 영향

○ 나아가, 사이버 리스크가 준법·평판·재무 등 경영상 핵심적 요소에 지대한 위협이 될 수 있다는 점과, 타 기관 및 경제 전반에 대한 시스템릭 리스크로 까지 발전 가능하다는 점에 주목할 필요

○ 이에 사이버보안은 기업의 최상위 의사결정기구이자 최종적 책임부담자인 이사회를 통해 적극적으로 관리하여야 한다는 인식이 확산

□ 이에 금융회사 이사회를 대상으로 사이버보안 관련 역할과 책임을 요구하는 국내·외 규제 및 정책 등을 조사하고 그 시사점을 검토

주) 신성환, 금융보안원 보안연구부 연구원

II. 국내 규제 요구사항

1. 현행 규제

□ 금융보안에 관한 최고경영자 또는 대표자의 역할 및 책임을 요구하는 경우는 현행 「전자금융거래법」 체계에 일부 존재

○ 그러나, 이사회·의결의 역할 또는 직접적 관여를 요구하는 내용은 「전자금융감독 규정」 제58조* 이외에는 부재

* 정보기술부문 실태평가 결과에 따라 취약점 개선에 관한 양해각서를 체결하는 경우(당해 실태평가 결과가 5등급 이거나, 직전 실태평가 결과가 2개 등급 이상 하락한 경우), 이사회 재적이사 전원의 서명을 받도록 규정

근거 규정	요구 사항	
전금법 §21④	대표자	- 금융회사가 매년 정보기술부문 계획을 수립·제출할 때 대표자의 확인·서명을 받도록 규정
감독규정 §8①	CISO	- 임직원의 정보보안 관련 법규 준수 실태를 정기적으로 점검하여 그 결과를 최고경영자에게 보고
	최고경영자	- 임직원의 관련 법규 위반 시 제재에 관한 세부기준 및 절차를 마련·운영할 책임
감독규정 §8-2①	CISO	- 정보보호위원회의 심의·의결사항을 최고경영자에게 보고
	최고경영자	- 특별한 사정이 없는 한 정보보호위원회 의결 내용을 준수
감독규정 §37-2⑤	CISO	- 전자금융기반시설 취약점 분석·평가에 따른 이행계획의 시행결과를 최고경영자에게 보고
		- 취약점 제거 등 조치가 불가한 경우 최고경영자의 승인을 얻을 것
감독규정 §37-5	CISO	- 임직원의 정보보안 점검항목(금융감독원)의 준수 여부를 매월 점검하여 결과 및 보완계획을 최고경영자에게 보고

2. 「전자금융거래법」 개정안

- 다만, 현재 국회 논의 중인 「전자금융거래법」 개정안(20.11.27.)에는 금융보안에 관한 이사회 역할·책임에 관한 사항이 다수 신설
- 이사회부터 임직원 개개인까지 금융보안에 관한 책무를 명확하게 정하여야 함을 금융보안 원칙의 하나로 제시(안 제20조의2 제3항)
 - 금융회사 등의 이사회는 금융보안에 관한 중요 사항을 결정하고 그 업무를 집행할 최종 책무가 있음을 규정(안 제20조의2 제4항)
- ①전사적인 금융보안 체계, ②전자금융업무 지속성, ③사고 피해 및 그 확산 방지 등 전자금융거래 및 정보자산의 안전성과 신뢰성에 관한 중요 사항은 이사회가 결정하도록 규정(안 제21조의2 제1항)
 - 아울러, 금융보안책임자로 하여금 위 중요 사항에 대한 이사회 결정을 지원하도록 책임을 부여(안 제21조의3 제3항 제4호의2)하고,
 - 필요한 경우 금융보안 업무의 집행현황을 이사회에 직접 보고하도록 규정(안 제21조의3 제5항)

Ⅲ. 국외 규제 요구사항

		미국		EU		싱가포르	호주
		FFIEC IT Handbook	23 NYCRR 500	DORA	EBA Guidelines	TRM Guidelines	CPG 234
전략·계획	기본 전략·계획 최종 승인	○	○	○	○	○	○
	기본 전략·계획 이행 상태 감독	○	○	○	○	○	○
	사이버보안 최종 책임 부담	-	-	○	-	-	○
거버넌스	전사적 거버넌스 형성	○	-	○	○	○	-
	CISO 등 독립성 보장	○	○	-	-	○	-
	독립적 감사권 보장	○	-	○	○	○	○
교육·문화	이사회 내부 전문지식 요구	○ (이해증진 노력)	-	○ (정기교육 수행)	-	○ (전문구성원 보유)	-
	임직원 대상 보안 교육	-	-	○	○	-	-
	사이버보안 문화 형성	-	-	-	-	○	-
정기검토	통제 등 효과성 검토	○	-	○	○	-	○
	정기적인 보고절차 마련	○	○	-	-	-	○
복원력	제3자 관계 관리·감독	○	-	○	-	-	-
	비즈니스 연속성 관리·감독	○	-	○	○	-	-

* 국외 주요 4개국(미국, EU, 싱가포르, 호주)의 최신 규제 요구사항을 중심으로 조사·정리(개별 규제의 상세 내용은 “[첨부] 국외 주요국 최신 규제 요구사항 세부 내용” 참조)

1. 사이버보안 전략·계획

(가) 기본 전략·계획에 대한 최종 승인

- ☐ 이사회는 조직의 사이버보안 전략 및 위협관리 프레임워크 등이 포함된 기본적인 ICT 전략 계획을 최종 승인하여야 함
- 또한, 이사회는 사이버보안과 관련한 조직의 리스크 성향(Risk Appetite) 및 리스크 허용한도(Risk Tolerance)를 정의해야 하며,
- 이러한 사이버보안에 관한 정책·기준들이 조직 전체의 비즈니스 전략 및 전사적 위협관리 체계와 일치할 수 있도록 보장해야 함

(나) 기본 전략·계획 이행 상태 감독

- ☐ 이사회는 사이버보안 기본 전략·계획의 이행 및 구체적 프레임워크 형성을 경영진이나 IT 운영위원회 등에 위임할 수 있으나,
- 그 주요 현황과 리스크 및 전략 내용의 변경사항을 정기적으로 보고받아야 하고, 이를 통해 최종적인 감독 권한을 행사할 필요

(다) 사이버보안에 관한 최종적 책임

- ☐ 이사회는 이러한 역할 수행을 통해 금융회사의 사이버보안 활동에 관한 최종적 책임을 부담할 필요

2. 사이버보안 거버넌스

(가) 전사적 사이버보안 거버넌스 체계 형성

- 이사회는 조직 내 사이버 리스크에 대한 적절한 관리를 보장하는 효과적인 사이버보안 거버넌스 체계 형성을 감독
 - 조직 내 모든 계층의 내부 구성원들에게 사이버 리스크 관리에 관한 역할과 책임이 명확히 설정되어 있는지 확인
 - 효과적인 ICT 리스크 관리를 위해 사이버보안 부문에 충분한 예산 및 인력이 할당되어 있는지 그 적절성을 감독

(나) 리스크 관리 기능의 독립성 보장

- 이사회는 사이버보안 정책의 집행을 책임지는 CISO 등 고위 임원을 지정하고 충분한 권한과 자원이 할당되도록 보장하고,
 - 리스크 관리 기능의 독립성을 보장하기 위해 CISO 등 보안 담당자가 이사회에 직접 보고할 수 있는 절차를 마련·보장할 필요

(다) 사이버보안에 대한 독립적 감사권 보장

- 이사회는 사이버보안 거버넌스 및 위험관리 프레임 워크의 효과성 검토를 위한 독립적·포괄적인 감사권을 보장해야 함
 - 이를 위해 ICT 관련 감사 계획 및 절차에 대한 주요 변경사항을 최종적으로 승인하고 그 내용을 주기적으로 검토할 필요

3. 사이버보안 교육 및 문화

(가) 이사회 내부의 전문지식 요구

- 이사회는 조직 수행하고 있는 주요 IT 활동과 그에 따라 조직이 직면할 수 있는 리스크를 명확히 이해할 수 있어야 함
 - 각 이사회 구성원은 사이버 리스크가 전체 사업 운영에 미치는 영향 및 관련 의사결정 사례 등에 대한 이해도를 높여야 하며, 이를 위해 관련된 교육을 정기적으로 수행할 필요
- 또한, 이사회는 필요에 따라 사이버 리스크에 관한 높은 이해 및 전문 지식을 갖춘 자를 그 구성원으로 포함할 필요

(나) 임직원에 대한 정기적 교육

- 이사회는 조직이 사이버 리스크와 관련하여 충분한 대응 능력을 갖추고 있는지 정기적으로 확인해야 하고,
 - 관련 업무 담당 임직원을 위한 전문적인 ICT 기술·위험 교육을 정기적으로 제공하고 그 효과성과 충분함을 검토할 필요
 - 또한, 전체 임직원을 대상으로 한 일반적인 사이버보안 교육을 최소 연 1회 이상 정기적으로 제공할 필요

(다) 사이버보안 문화 형성

- 이사회는 모든 임직원들이 사이버보안 리스크에 적절히 대응할 수 있도록 전사적인 리스크 관리 문화를 배양할 책임

4. 이사회의 정기적 검토

(가) 사이버보안 활동의 효과성 검토

- 이사회는 사이버보안 전략·계획의 구체적 이행을 담보하기 위해 사이버보안 프로그램의 효과성을 정기적(매년)으로 검토해야 함
 - 특히, ICT 업무연속성계획(BCP)과 재해복구계획(DRP), ICT 감사 계획 및 임직원 사이버보안 교육 프로그램의 효과성·적절성 등을 상세히 확인할 필요
- ICT·보안 리스크에 대한 위험평가 결과 및 그에 대한 통제조치의 적절성에 관한 전반적 사항을 최소 연 1회 검토·승인하여야 함

(나) 이사회에 대한 보고

- 이사회는 사이버보안에 관한 경영진의 책임을 명확히 규정하고, 보고 대상 리스크의 종류와 수준 및 보고 시기·범위·내용 등의 요구사항을 명확히 전달해야 함
 - 특히, 이사회는 CISO 등 경영진에게 대표적으로 다음 사항들에 대해 매년 또는 주기적으로 이사회에 보고하도록 요구할 필요

- 조직에 중대한 영향을 미치는 주요 기술 위협의 확대 또는 관련 사고 발생
- 주요 ICT 프로젝트의 수립·진행 현황 및 관련 리스크 상황
- 위험평가 기준 및 절차, 위험관리·통제 상황
- 제3자 서비스 이용 현황 및 관련 약정
- 사이버보안 훈련의 결과 및 관련 시정 조치
- 사이버보안 관련 법규 위반 사례 및 그에 대한 경영진의 대응
- 사이버보안 프로그램의 업데이트 권장사항

5. 사이버 복원력 고려

(가) 비즈니스 연속성 관리·감독

- 이사회는 조직의 비즈니스 연속성 관리(BCM)에 관한 기본적 정책을 최종적으로 승인할 책임이 있으며,
 - 구체적으로는 사이버 사고에 대한 대응절차 및 복구대책 등에 관한 세부 계획 수립 및 그 적절성에 대한 감독을 수행할 필요
- 이사회는 조직의 비즈니스 연속성 관리 능력의 효과성을 검증하기 위해 사고 대응 훈련 결과 등을 정기적으로 검토할 필요
 - 또한, 실제 발생한 ICT 관련 실패나 사고 사례와 함께 그 영향 및 대응·복구·시정 조치에 관한 사항을 검토하여야 함

(나) 제3자 관계

- 이사회는 조직의 제3자 선정 절차를 관리·감독해야 하며,
 - 제3자 선정 시 고려해야 할 주요 요소 등이 포함된 제3자 관련 기본 정책을 최종 승인하고 그 적절성을 주기적으로 검토해야 함
- 또한, 이사회는 특히 ICT 기술의 이용과 관련하여 조직이 체결한 주요 제3자 약정의 현황을 정기적으로 확인하고,
 - 제3자 관련 변경사항이 있는 경우 해당 변경이 조직 핵심 기능에 미칠 수 있는 잠재적 영향 등을 적시에 보고받아 검토할 필요

(다) 기타

- 이사회는 조직이 감독당국에 대한 사고보고 의무 등과 관련하여, 보고 필요사항 및 절차 등이 포함된 정책을 승인할 책임

IV. 이사회 역할 수행을 위한 방법론

- 위와 같이 국외 주요국이 금융회사 이사회에 요구하는 사이버보안 역할·책임에는 일정한 경향성을 찾을 수 있는데,
 - 이사회가 이를 실제 수행하는 과정에 있어 구체적으로 조직 내 어떤 사항을 어떻게 검토·감독해야 하는지 난해한 부분이 존재
- 이에 국외에서는 이사회들의 실제 업무수행에 실천적으로 참고할 수 있는 도구적 방법론에 대한 연구가 활발한바, 그 주요 내용을 소개

1. NCSC – Cyber Security Toolkit for Boards

(가) 개요

- 영국의 NCSC(National Cyber Security Centre)는 기업 활동의 핵심적 요소가 된 디지털 기술과 관련하여,
 - 영국 기업 이사회가 기업 내 사이버보안에 관한 중심축 역할을 잘 수행하고 기술 전문가들과의 활발한 논의를 증진할 수 있도록,
 - 이사회들의 사이버보안 관련 역할과 그 구체적 실천방법을 안내하는 「Cyber Security Toolkit for Boards」(이하 “툴킷”)를 발표(’19.4.)

- 이는 금융부문 한정이지 아닌 전 산업 분야에 걸쳐 적용되는 내용이고 강제력이 부여되지도 않는 참고용 안내서에 해당하지만,
- 이사회에 새롭게 요구되는 사이버보안 책임과 관련하여, 실질적으로 참고 가능한 구체적 방법론을 제시하고 있다는 점에서 유의미

(나) 주요내용

- 툃킷에 따르면 훌륭한 사이버보안이란, 사이버 리스크를 효과적으로 관리할 수 있는 해당 조직에 가장 적합한 프로세스를 마련하는 과정
- 이를 위해 이사회는 ①적절한 관련 정보를 수집하여 ②리스크 우선순위를 판별한 후, ③우선순위에 따라 각 리스크를 관리하는 순서로 프로세스를 구성·시행해야 하고,
- 이에 앞선 전제 조건으로서, ④조직 내 적절한 사이버보안 환경을 조성하는 역할을 선행해야 한다고 안내
- 툃킷은 위 4가지 단계에 있어 세부적으로 수행해야 하는 구체적 실행 섹션을 아래와 같이 9가지로 나누어 안내

적절한 사이버보안 환경 조성		
① 사이버보안 요소를 조직 목표·구조 등에 내재화 ② 사이버보안 전문가 양성 ③ 건전한 사이버보안 문화 형성·발전		
1. 관련 정보 수집	2. 리스크 평가 및 우선순위 판별	3. 판별된 리스크에 대한 관리
④ 핵심 정보자산의 식별 및 위험 평가, 통제의 기준선 설정 ⑤ 직면한 사이버위협에 대한 이해	⑥ 사이버보안을 위한 리스크 관리	⑦ 효과적인 사이버보안 통제의 구현 ⑧ 협력업체 및 공급업체와의 협력 ⑨ 사이버 사고 발생에 대한 대응 계획 수립

- 나아가 툴킷은 각 실행 섹션별로 이사회가 담당해야 하는 역할을,
 - ❶이사회가 직접 수행해야 하는 활동과 ❷이사회가 간접적으로 감독해야 하는 조직의 활동으로 나누어 안내
 - 또한, 상기 역할의 안정적 수행을 위해 이사회가 조직 내 사이버보안 전문가와 활발한 논의를 이어나가는 것이 중요한바,
 - ❸이사회가 사이버보안 전문가와의 중요 논의를 시작함에 있어 고려·확인해 볼만한 상세 질문사항*을 함께 제시
- * 질문 대상을 다음과 같이 셋으로 나누어 각각에 대한 고려·확인 요소를 나누어 제시 : (i) 개별 이사회 구성원, (ii) 전체 이사회, (iii) 전체 조직
- ※ 이상의 직·간접적 이사회 역할과 고려·확인이 필요한 상세 질문사항의 내용은 이어지는 “[참고] 「Cyber Security Toolkit for Boards」 주요 내용”을 참조

참고

「Cyber Security Toolkit for Boards」 주요 내용

실행 섹션	이사회의 직·간접 역할 및 상세 질문사항		
① 사이버보안의 조직 목표 통합	직접 수행	- 사이버보안이 조직의 목표 달성에 기여할 수 있도록 조직의 목표 설정에 사이버보안 요소를 통합 - 전체 이사회에서 책임을 갖고 사이버보안 활동을 수행하는 등 조직 구조 자체에 사이버보안 요소를 반영 - CISO 등 전문가와의 직접적인 협력이 가능하도록 보고 구조를 개편하고 커뮤니케이션을 증진	
	상세 질문 사항	to 이사회	(Q1) 이사회는 사이버보안이 이사회의 책임에 어떠한 영향을 미치는지 잘 이해하고 있는가? (Q2) 이사회가 조직의 사이버보안 접근 방식의 효과성을 확인할 수 있는 방법은 무엇인가?
		to 조직	(Q3) 현재 누가 조직의 사이버보안을 책임지고 있는가? (Q4) 사이버 리스크가 비즈니스 리스크와 통합 관리되도록 보장하는 프로세스가 있는가?

실행 섹션	이사회의 직·간접 역할 및 상세 질문사항		
② 사이버보안 전문가 양성	직접 수행	조직 내 사이버보안 전문가의 현황과 추가로 필요한 전문가 수요 등을 파악하고, 이사회 자체가 보유한 관련 지식수준도 평가할 것	
	감독 대상	- 구체적으로 어떤 분야의 사이버보안 전문가가 필요한지, 얼마나 급하게 필요한지 등에 관한 조직적 계획을 수립하고 있는지, 현재 보유한 전문가를 최대한 효율적으로 사용하고 있는지 - 다양하고 포용적인 인력 구축을 위해 단순히 기술적 인재 이상의 다양한 측면의 인재풀을 구축하고 있는지, 기존 인력에 대한 포용적 관리도 잘 이루어지고 있는지 - 조직 내의 사이버 전문성을 향상시키기 위해, 기존 직원 교육, 외부전문가 고용, 후원 등을 통한 미래 인력 개발 등 방안을 활용하고 있는지	
	상세 질문 사항	to 이사회 구성원	(Q1) 나는 사이버보안 결정을 책임질 수 있는 수준의 적절한 전문 지식을 보유하고 있는가?
		to 조직	(Q2) 조직에 필요한 사이버 전문성은 무엇이고, 이미 보유하고 있는 전문성은 무엇인가? (Q3) 현재 보유하고 있지 않은 전문성을 개발하기 위해 조직은 어떠한 계획은 갖고 있는가? (Q4) 사이버보안 기술 과제를 해결하기 위해 평등·다양하고 포괄적인 인력을 구축하고 있는가?
③ 사이버보안 문화 형성	직접 수행	이사회의 의사결정 과정에 있어 사이버보안 관련 절차에 예외를 두지 않고 철저히 준수함으로써 모범을 통해 조직 내 보안문화를 형성·장려	
	감독 대상	- 사이버보안 활동에 있어서 임직원의 자발적 역할을 중요하게 인식하고 이를 촉진·활용하기 위한 요소를 관련 프레임워크를 반영하는지 - 우려 사항을 확인하여 보고한 직원에게 불이익이 가지 않도록 하는 ‘정의로운 문화’를 형성하고 있는지	
	상세 질문 사항	to 이사회 구성원	(Q1) 나는 이사회 구성원으로서 건전한 보안문화를 선도하고 있는가?
		to 조직	(Q2) 조직은 건전한 보안 문화를 보유하고 있는가? (Q3) 건전한 보안 문화를 장려하기 위하여 조직적 차원에서 어떠한 조치를 취해야 하는가?
④ 핵심 기능 식별 및 기준 설정	직접 수행	조직의 중요 기능·목표를 식별하여 기술 전문가들이 해당 기능을 지원하는 자산들을 보호하는 데에 집중하도록 하고, 그 안에서도 우선순위를 확정	
	감독 대상	- 조직의 자산이 어떻게 연계되어 있는지 인식하고, 어느 부분에 취약성이 있는지 확인하고 있는지 - 이사회가 확정한 조직 기능의 우선순위에 따라 이를 지원하는 중요 기술 자산을 식별하고 그에 관한 기준을 설정하고 있는지	

실행 섹션	이사회의 직·간접 역할 및 상세 질문사항		
	상세 질문 사항	to 이사회	(Q1) 이사회는 사이버보안 우선순위 목표를 명확하게 전달하였는가? 해당 우선순위는 조직의 사이버보안 확보에 도움이 되고 있는가?
		to 조직	(Q2) 기술 시스템, 프로세스, 자산 등이 조직의 목표 달성에 어떠한 영향을 미치는지 명확히 이해하고 있는가? (Q3) 조직이 관리하는 시스템, 데이터 및 서비스를 어떻게 식별·추적하고 있는가?
⑤ 사이버위협에 대한 이해	직접 수행	• 조직 및 조직이 속한 산업부문과 관련된 사이버보안 위협에 대한 이해 • 동일 부문 타 조직과의 사이버보안에 관한 협조적 관계 구축 • 전문가와의 지속적 논의를 통해 조직이 직면한 사이버위협을 평가하고 능동적 대응이 필요한 우선순위를 설정 • 조직의 위협을 고려할 때 협력업체 및 공급업체로부터 발생하는 위협까지 함께 고려	
	감독 대상	• 무작위 공격의 위험성을 과소평가하지 않고, 조직을 겨냥한 특정 위협뿐 아니라 무작위 위협에 대한 대응방안도 함께 고려하고 있는지 • 많은 산업 파트너 또는 정부기관 등이 제공하는 우수한 위협 인텔리전스를 잘 인식하고 적절히 활용하고 있는지	
	상세 질문 사항	to 조직	(Q1) 조직과 가장 관련이 깊은 위협은 무엇이며 그 이유는 무엇인가? (Q2) 조직은 사이버 위협에 대한 최신 정보를 얻기 위해 어떠한 방안을 실행하고 있는가? (Q3) 조직의 일상적 비즈니스 수행에 위협 인텔리전스를 적용하고 있는가?
⑥ 사이버보안 리스크 관리	직접 수행	• 사이버보안을 조직 전체의 위험 관리 프로세스에 통합 • 당장의 위협 요인·수준의 감소를 사이버보안 활동의 성공으로 판단하지 말고 지속적으로 변화하는 위협 요인을 고려할 것	
	감독 대상	• 사이버 위협의 지속적으로 변화하는 특성을 잘 이해하고, 기존의 위험평가 방법에 지나치게 의존하지 않고 현실적 관점에서 정기적인 점검을 수행하고 있는지	
	상세 질문 사항	to 이사회	(Q1) 이사회는 수용 가능한 리스크와 수용 불가 리스크의 종류 및 수준을 명확히 정하였는가?
		to 조직	(Q2) 개별 의사결정에 있어 의사결정권자에게 사이버보안에 관한 최대한 많은 정보를 제공하는 조직적 차원의 프로세스가 형성되어 있는가? (Q3) 사이버 리스크가 조직 전체 비즈니스 리스크에 통합되도록 보장하는 프로세스가 있는가? (Q4) 사이버 리스크를 관리하기 위한 효과적이고 적절한 접근 방식을 마련·적용하고 있는가?

실행 섹션		이사회의 직·간접 역할 및 상세 질문사항	
⑦ 효과적인 통제 구현	직접 수행	• 통제수단의 효과성을 감독하기 위해서는 사이버보안에 관한 기초 지식이 필요하므로 전문가와의 논의를 통해 관련 이해를 증진할 것	
	감독 대상	• 대다수의 사이버 공격을 차단·예방할 수 있는 기본적인 사이버보안 통제부터 잘 적용하고 있는지 • 사이버보안 통제를 조직의 우선순위 위험 등에 알맞게 조정하고 있는지 • 사이버보안과 관련하여 단계적인 심층 방어체계를 구현하고 있는지 • 네트워크 경계에 대한 보안뿐 아니라 시스템 내부에서의 위협에 대한 방어 조치도 적절히 수행하고 있는지 • 조직의 요구사항 및 위험 상황의 변화에 따른 통제의 적절성을 주기적으로 평가·검토하고 있는지	
	상세 질문 사항	to 조직	(Q1) 사이버보안 통제의 효과성을 검증할 수 있는 절차가 마련되어 있는가? (Q2) 조직 내부에서 공격자가 입힐 수 있는 손해를 최소화하기 위해 어떠한 통제 수단을 적용하고 있는가? (Q3) 피싱, 소프트웨어 취약점 공격, 계정 탈취, 권한 남용 등 가장 일반적인 공격을 예방하기 위한 사이버보안 통제를 적절히 구현하고 있는가?
⑧ 협력·공급 업체 협업	직접 수행	• 협력·공급업체와의 계약 체결 등 모든 제3자 관계 결정에 있어 사이버보안 요소를 반영·고려할 것	
	감독 대상	• 전체 제3자 관계에 관한 사이버보안 요구사항을 명확하게 설정하고 실제 협력·공급업체들이 이를 충족하고 있는지 잘 확인하고 있는지 • 사이버보안 요구사항을 제3자 관계 계약조항에 포함하고, 테스트나 감사를 통해 보증을 요구하고 있는지 • 협력·공급업체가 보안 실패를 초래하는 경우를 가정하여 이를 염두에 두고 네트워크 및 시스템 보안을 설정·계획하고 있는지	
	상세 질문 사항	to 이사회	(Q1) 이사회는 협력·공급업체를 이용하는 명확한 전략을 수립하고 이에 대해 검토하고 있는가?
to 조직		(Q2) 조직은 다른 업체와의 데이터·시스템 연계 시 발생하는 위험을 어떻게 완화하고 있는가? (Q3) 협력·공급 관계에 관한 모든 의사결정에 있어 사이버보안 요소를 충분히 고려하고 있는가? (Q4) 조직이 타 기업에 대한 관계에서 공급업체에 해당하는 경우 관련 보안 요구사항을 충족하고 있는가?	

실행 섹션	이사회와 직·간접 역할 및 상세 질문사항		
⑨ 사고 발생에 대한 대응 계획	직접 수행	• 조직이 사이버사고 대응계획을 수립·시행하고 있는지 확인 • 사고 대응 과정에서 이사회가 부담해야 하는 역할에 대해 명확히 인지 • 사고 대응 훈련에 적극적으로 참여 • 이사회로서 사이버사고에 대한 궁극적 책임을 부담하고, 특정 담당자에게 책임을 묻지 않는 ‘No-Blame’ 문화를 조성할 것	
	감독 대상	• 사이버 공격을 식별·확인할 수 있도록 모니터링 체계를 구축하고 있는지, 개별 공격이 사고로 인식되는 임계값을 명확히 설정하고 있는지 • 중요 보호대상 기능과 위협, 기술 자산 등에 대한 사전 지식을 바탕으로 사고의 영향도를 예상하고 적절한 대응 방안을 검토하는지 • 사고에 따른 피해를 최소화하기 위해 공격자의 행동 등을 제약하기 위한 선제적 조치를 수행하는지 • 당국 보고, 법적 책임, 이해관계자에 대한 대응 등 요소를 모두 고려한 사고 대응·관리 계획을 세우고 있는지 • 사고대응·관리 계획을 정기적으로 테스트하고 있는지 • 기존 사고에서 교훈을 얻어 리스크, 통제, 계획 등에 대한 효율성을 평가하고 있는지	
	상세 질문 사항	to 이사회 구성원	(Q1) 이사회 구성원으로서 사이버보안 사고 발생 시 내 역할에 대해 충분히 이해하고 있으며, 충분한 관련 교육·훈련을 받았는가?
		to 이사회	(Q2) 이사회는 사고가 발생한 경우 조직 구조적 측면에서 누가 상황을 주도하고 의사결정 권한이 누구에게 있는지 잘 알고 있는가?
		to 조직	(Q3) 조직 차원의 사고관리 계획이 수립되어 있는가? 해당 계획의 효과성을 어떻게 보장하고 있는가? (Q4) 조직 내에서 사고 발생을 인지할 수 있게 하는 요소는 무엇이며, 해당 정보는 조직 내에서 어떻게 공유되는가? (Q5) 사고 발생 시 어디로 도움을 요청해야 하고, 어떠한 지원을 받을 수 있는지 알고 있는가? (Q6) 조직은 기존의 사고 및 사고 유사 경험으로부터 교훈을 얻어 대응하고 있는가?

2. 카네기 국제평화재단 – Cyber Capacity-Buidling Toolbox

(가) 개요

- 카네기 국제평화재단은 금융산업 전반의 사이버 위험 수준이 가장 취약한 회사에 의해 결정됨을 파악하고 그 개선을 위하여,
 - 상대적으로 보안 역량이 낮은 소규모 금융회사가 참고 가능한 사이버보안 역량 강화 툴박스(Cyber Capacity-Building Toolbox)를 발표*
- * 카네기 국제평화재단 外 IMF, SWIFT, 미국 FS-ISAC, 스텐타드차타드(SC), 사이버대비연구소(Cyber Readiness Institute), 글로벌 사이버협회(Global Cyber Alliance)가 공동 연구를 통해 발표('19.7.)
- 가이드는 금융회사 조직 내에서 사이버보안 활동과 관련한 주체를 계층을 나누어 각자의 역할을 구체적으로 안내
 - 그중에는 이사회와 사이버보안 리더십 역할을 설명하는 이사회 레벨 가이드(Board-Level Guide – Cybersecurity Leadership)도 포함
 - 아직 이사회와 사이버보안 역할이 명확히 정립되지 않았다면, 소규모 아닌 일반 금융회사도 이를 참고 가능할 것으로 사료

(나) 주요 내용

□ 이사회는 사이버 리스크 거버넌스와 관련한 다음의 기본 사항에 대하여 명확히 답변할 수 있도록 확인 필요

- ① 관련 법규 요구사항을 충족했는가?
- ② 사이버보안 노출을 정량화하고 금융 복원력을 평가했는가?
- ③ 보안 노출이 기관의 승인된 위험성향(Risk Appetite) 범위 이내로 포함 되도록 개선 계획을 마련했는가?
- ④ 이사회는 경영진이 제공한 조직의 사이버 복원력 관련 정보에 대해 정기적으로 논의를 수행하는가?
- ⑤ 최근 훈련이 진행된 이사회와 역할을 포함한 사고대응 계획을 마련하고 있는가?
- ⑥ 사이버 리스크 관리를 담당하는 주요 직원의 역할이 명확하며, 그것이 3선 방어 기준에 적합한가?
- ⑦ 조직의 사이버 리스크 상태에 대한 독립적인 감사·검증을 받았는가?

□ (감독) 이사회는 사이버 리스크에 대한 궁극적 책임을 갖고 전략, 정책 및 활동을 감독해야 하며, 구체적으로 다음 역할을 수행

- ① 사이버 리스크 및 복원력 감독에 대한 최종적인 책임을 부담
- ② CISO 등 임원을 지정하여 사이버 복원력 관리 현황을 보고하도록 하고 해당 임원의 정기적인 이사회 참여를 보장하며 임무 수행에 필요한 충분한 권한 및 자원을 할당
- ③ 매년 조직의 기본 전략 및 위험성향(Risk Appetite)에 부합하는 위험 수용한도(Risk Tolerance)를 정의
- ④ 매년 공식적이고 독립적인 사이버 복원력 검토가 수행되도록 보장
- ⑤ 조직에 적합한 사이버 복원력 계획을 수립·구현하고 테스트를 통해 지속적으로 개선되도록 감독하고, CISO 등 책임 임원이 그 결과를 정기적으로 이사회에 보고하도록 함
- ⑥ 사이버 복원력 및 위험평가를 전사적 경영전략, 리스크 관리, 예산 및 자원 할당 등 절차에 통합
- ⑦ 정기적으로 ①~⑥의 효과성을 검토하고 지속적인 개선을 위해 독립적인 자문의 활용을 고려

□ **(정보의 최신성 유지)** 사이버 리스크에 대한 이사회의 효과적 관리·감독은 이사회 구성원이 보유한 정보의 최신성에 따라 결정

- 이사회 구성원이 사이버 위협으로 인한 리스크를 이해하고 관리할 수 있는 적절한 최신 기술 및 지식을 갖추도록 보장해야 함
- 조직에 대한 신규 위협 및 규제 환경 변화에 관한 정례 브리핑을 수행하고, 사이버보안 우수기업과의 교류 등에 참여
- 경영진이 이사회에 사이버 리스크와 구체적 위협 및 사고대응 결과 등에 대해 정략적이고 이해 가능한 보고를 하도록 요구

- 공급망 취약성이나 제3자 의존성, 이사회 간 정보공유 격차 등 체계적 문제에 대한 인식을 공유
- **(문화 형성)** 이사회는 조직의 핵심 가치, 리스크 문화 및 사이버 복원력에 대한 기대치를 설정하고 모범을 보여야 함
 - 모든 임직원이 사이버 복원력에 대한 중요한 책임이 있음을 인식하도록 하는 조직 내 사이버보안 문화를 촉진
 - 안전성과 건전성에 대한 조직 문화의 영향을 고려하여, 그 조성·관리에 관한 경영진의 역할을 감독하고 사이버보안 문화에 대한 모니터링 및 평가를 수행
 - 모든 구성원이 신뢰성 있게 행동하며, 조직 내·외부에서 관찰된 부적합 사항을 즉시 보고하도록 명확하게 규정

3. 시사점

(규제·제도적 측면) 이사회 역할 강화 및 전체 비즈니스 연계성 확대

- 국내의 현재 「전자금융거래법」 체계는 금융회사 이사회에 대한 사이버 보안 관련 역할 요구가 다소 부족한 편이나,
 - 국회 논의 중인 개정안에는 이사회에 금융보안 관련 중요 사항을 결정·집행할 최종 책무를 부여하는 등 진일보한 내용들이 포함
- 다만, 아직 법률 수준의 규정만 제안된 상황이어서, 조사 대상 주요국 요구 사항과 비교하면 원칙적·포괄적 내용에 그치는 한계
 - 따라서, 추후 시행령이나 감독규정 등 하위규정을 통해 이사회가 부담하는 금융보안 책무의 내용을 구체적으로 보충할 필요

- 특히, 이사회는 금융보안 관련 결정에 조직 전체 비즈니스 전략 및 위험관리 체계와의 연계를 반드시 고려하도록 하여, 금융보안에 관한 보다 적극적이고 전략적인 고려를 촉진할 필요가 있을 것

(조직·전략적 측면) 개별 금융회사 이사회의 적극적 역할 수행 필요

- 향후 변경될 「전자금융거래법」에 대한 컴플라이언스를 충족하고 확대된 사이버 위협에 조직적 차원에서 적절히 대응하기 위해,
 - 금융회사는 사이버 위협을 IT 부문에 한정된 운영 리스크가 아닌, 조직 최고 의사결정기구인 이사회가 적극적으로 통제·관리할 필요가 있는 전략적 리스크로 고려할 필요
- 특히, 금융회사 이사회는 디지털 대전환 속 사이버 위협은 더는 완전 예방을 목표로 하기 어려운 리스크라는 점을 인지해야 함
 - 또, 사이버 사고는 조직의 사업 전체에 피해를 미친다는 점과, 나아가 심할 경우 금융산업, 실물경제 전반에 대한 피해로까지 확대될 수 있다는 점을 명확히 인식할 필요
- 이를 통해, 이사회는 사이버 위협을 어느 범위까지 예방의 대상으로 삼고 어느 수준 이상을 회복의 관점에서 접근할지에 대한 결정*과,
 - * 위험 이전의 관점에서 사이버 보험의 활용 등도 고려 가능
 - 실제 사고 발생에 대비한 핵심 기능의 지속, 시스템 리스크로의 전이 가능성 차단 등 운영복원력(Operational Resilience) 관점의 전략적 결정에 적극적으로 나설 필요

[실천적 측면) 모범사례 등 적극적 활용을 통한 최적화 방법론 마련

- 이처럼 금융보안은 전사적 리스크로 이사회를 통해 관리되어야 하나, 국내에는 이를 이사회가 직접적으로 책임지고 실천할 수 있게 하는 실행체계가 아직 미진한 상황
- 따라서, 금융회사 이사회는 새로운 역할 수행을 위한 구체적 방안 확보를 위해, 본 보고서의 제시 자료를 비롯한 국내·외 도구적 방법론 및 모범사례 등을 적극 참고할 필요
- 나아가 이를 중심으로, 국내의 기업·금융환경 특성 및 자사의 구체적 상황을 반영한 최적화된 방법론을 마련에 노력할 필요

첨부 국외 주요국 최신 규제 요구사항 세부 내용

I. 미국

1. FFIEC IT 검사 핸드북

(가) 개요

- (FFIEC) 미연방 금융기관 검사위원회(Federal Financial Institution Examination Council)로서 미국 내 5개 금융감독당국*의 통일적 금융감독을 위해 검사 원칙과 표준을 제시하는 역할

* FRB(Federal Reserve Board), FDIC(Federal Deposit Insurance Corporation), NCUA(National Credit Union Administration), OCC(Office of the Comptroller of the Currency), CFPB(Consumer Financial Protection Bureau)

- **(IT Examination Handbook)** 미국 내 금융기관에 대한 IT 부문 검사에 관한 FFIEC 제안사항으로 그 자체로 법적 구속력은 없으나,
 - 구속력 있는 미연방 규정집의 내용을 다수 포함하며 각 감독당국 검사 시 검사기준으로 활용하는 만큼 실질적 준수가 필요
 - FFIEC의 IT Examination Handbook은 총 11개 소책자*로 구성
 - * “Audit”, “Business Continuity Management”, “Development and Acquisition”, “E-banking”, “Information Security”, “Management”, “Architecture, Infrastructure, and Operations”, “Outsourcing Technology Services”, “Retail Payment Systems”, “Supervision of Technology Service Providers”, “Wholesale Payment Systems”
 - 이사회의 역할 관련 사항은 Management(일반적 IT 관리)와 Information Security(정보보안 관련) 및 Business Continuity Management(비즈니스 연속성 관리 관련)에서 주로 규정

(나) 주요 요구사항

① 전반적 IT 관리

- 이사회는 조직의 기본 IT 전략계획과 정보보안 프로그램을 비롯한 기타 IT 정책을 최종적으로 승인
 - 이를 위해 이사회의 각 구성원은 조직의 IT 활동 및 그 위험을 올바르게 이해할 수 있도록 노력할 필요
- 구체적으로 이사회는 다음의 임무를 수행
 - 전체 비즈니스 전략과 일치하는 기본 IT 전략계획을 검토·승인하고, 여기에 정보보안에 관한 전략을 포함
 - 조직 내 효과적인 IT 거버넌스 구조 형성을 감독

- 제3자의 건전성, IT 보안 등 요소를 고려한 제3자 선정절차 감독
- 주요 IT 프로젝트 및 그 예산, 수행성과에 관한 변동사항을 상시 확인·감독하고, 특히 중요한 프로젝트의 경우 직접 그 시행을 승인
- IT 부문에 대한 예산 및 인력의 적정성 감독
- 이사회 및 감독당국에 대한 보고 필요사항 및 그 절차 등에 관한 정책 승인
- IT에 대한 독립적이고 포괄적·효과적인 감사권을 보장
- 이사회는 특정 IT 활동의 설계·구현 및 모니터링을 경영진이나 IT 운영위원회* 등에 위임 가능
 - * IT 부문 및 다른 비즈니스 부문의 고위 관리직과 실무 담당자로 구성
- IT 관련 경영진, IT 운영위원회 등은 위임받은 주요 활동 상태와 IT 리스크, 전략 등 변경사항에 대해 정기적으로 이사회에 보고
- 이사회는 위임에도 불구하고 보고서 등을 통해 계속해서 조직의 IT 활동에 대한 최종적인 감독 권한을 행사

② 정보보안 관련

- 정보보안과 관련하여, 이사회는 조직 내 정보보안 계획·정책을 최종적으로 승인하기 위해 관련 비즈니스 사례와 보안위험이 전체 비즈니스에 미치는 영향 등에 대한 이해를 증진할 필요
- 또한, 이사회는 정보보안 프로그램의 개발·구현·유지·관리 책임을 고위 경영진에 할당하고, 이를 적절히 감독해야 함
 - 여기에는 책임의 할당, 리스크 평가, 통제구현, 통제효과 모니터링, 보고 절차 및 허용 가능한 위험 수준에 관한 사항이 포함

- 이사회는 적어도 매년 정보보안 프로그램의 상태 및 효과성을 검토하고, 이를 위해 경영진은 매년 아래 사항을 이사회에 보고
 - 리스크 평가 절차, 리스크 관리 및 통제
 - 제3자 서비스 제공자 약정
 - 정보보안 훈련 결과
 - 규정 위반 및 그에 대한 경영진의 대응
 - 정보보안 프로그램 업데이트 권장사항
- 또한, 이사회는 IT 보안 기능의 독립성을 보장하도록, CISO 등 정보보안 담당자가 이사회에 직접 보고할 수 있는 절차를 보장

③ 비즈니스 연속성 관련

- 이사회는 비즈니스 연속성 관리(이하 “BCM”)와 관련하여, 조직 내의 핵심 기능을 식별하고 상호의존성을 분석하여 해당 기능의 중단 영향도를 평가하는 과정 전반을 감독할 필요
 - 특히, 계열사와 제3자 서비스 제공자 등이 제공하는 기능을 포함하여 전사적 관점에서의 효과적인 BCM 정책을 최종 승인
- 이사회는 BCM 정책을 승인함에 있어 조직의 전체 비즈니스 전략 및 위험 선호도와의 일치 여부 등을 고려해야 하고,
 - 구체적인 사고대응절차, 재해복구대책 등 내용을 포함하는 BCM 계획의 수립도 적절히 감독할 필요

- 이사회는 BCM 정책 및 전략·계획 등의 효과성을 검증하기 위한 훈련의 결과를 정기적으로 검토
 - 이를 위해 매년 경영진으로부터 BCM 프로그램의 전반적 상태와 연습·훈련 결과에 대한 서면 보고를 받아야 함
- 아울러, 이사회는 BCM 프로그램의 설계 및 운영 효율성을 검토하기 위한 내·외부 감사 기능을 독립적으로 보장하여야 함

2. 뉴욕주 금융서비스 사이버보안 규정 (23 NYCRR 500)

(가) 개요

- 뉴욕주 금융서비스국(DFS, Department of Financial Services)이 주관하는 주(州)법으로 뉴욕 내 인·허가된 모든 금융기관들에 적용
 - 미국 내 사이버보안 관련 법적 구속력을 가진 최초의 주법에 해당 ('17.3.1. 제정 후 규정별 유예기간을 거쳐 '19.3.1. 전부 발효)
 - 대상기관의 정보시스템 및 고객정보의 보호를 목표로 하며, 각 회사가 위험 수준을 평가하고 적절한 방식을 채택하도록 요구

(나) 주요 요구사항

- 규제 대상기관은 이사회의 승인을 얻은 서면화된 사이버보안 정책을 수립하여 유지·준수해야 함
- 규제 대상기관은 사이버보안 정책 집행 및 사이버보안 프로그램의 실행을 책임지는 CISO를 지정해야 함

- CISO는 정책의 구현 상황과 프로그램의 효과성 및 주요한 사이버보안 위협 및 사고에 대하여 이사회에 적어도 매년 서면 보고
- 각 기관은 매년 4.15일까지 이전 연도에 동 법률의 요구 사항을 준수하였음을 증명하는 서면 진술서를 감독당국에 제출
- 그리고 해당 서면 진술서를 증명할 수 있는 관련 기록과 일정, 데이터 등을 5년간 유지

II. EU

1. 디지털운영복원법(안) (DORA)

(가) 개요

- EU 금융부문의 빠른 디지털 전환 추세에도 기존 규제 체계는 포괄적 규칙이 부재하여 규제 중복, 과다 준수 비용 등 문제 발생
- 이에 EU 집행위원회는 EU 내 금융기관 전체에 통일적으로 적용되는 ICT 리스크 관리 방안을 제시하기 위한 목적으로 디지털운영복원법(Digital Operational Resilience Act, DORA) 초안을 발표('20.9.)
- 아직 확정되지 않은 초안의 형태에 불과하여 법적 구속력은 없지만, 가장 최근의 디지털 리스크 규제 관점을 확인하기에 적절

(나) 주요 요구사항

- 금융회사는 모든 ICT 위협에 대한 효과적이고 신중한 관리를 보장하는 내부 지배구조 및 통제 체계를 갖추어야 함

□ 금융회사의 경영기관(Management Body*)은 이러한 ICT 위험관리 프레임워크와 관련된 모든 사항에 대해 승인 및 감독 책임을 부담

* Management Body란 기업의 전략·목표를 설정하고 경영 의사결정을 감독하며 기업의 사업을 효과적으로 지휘하는 기관을 의미(§3·22, Directive 2014/65/EU §4①36)하는 것으로, 이사회 또는 그 위원회를 포함하는 개념으로 이해 가능

○ 구체적으로 경영기관이 수행해야 하는 임무는 다음과 같음

- 금융회사의 ICT 위험 관리에 관한 최종 책임 부담
- 모든 ICT 관련 기능에 대한 명확한 역할과 책임 설정
- ICT 리스크에 대한 적절한 리스크 허용 수준을 결정
- 금융회사의 ICT 업무연속성계획(BCP) 및 재해복구계획(DRP)을 승인·감독하고 주기적으로 그 효과성을 검토
- ICT 감사 계획 및 감사 절차에 대한 중요 변경사항을 승인하고 그 내용을 주기적으로 검토
- 관련 직원을 위한 ICT 위험·기술 교육을 포함하여, 디지털 회복력 증진을 위한 적절한 예산을 배정하고 그 효과성을 정기 검토
- 제3자 서비스 제공업체의 이용 및 선정에 관한 금융회사의 정책을 승인하고 주기적으로 검토
- ICT 서비스 이용에 관하여 제3자와 체결한 약정과 관련한 모든 주요 변경사항, 그리고 그로 인해 중요·핵심 기능에 미칠 수 있는 잠재적 영향에 대해 시기적절하게 보고받아야 함
- ICT 관련 사고 및 그 영향과 그에 대한 대응, 복구 및 시정 조치에 대해 시기적절하게 보고받아야 함

□ 경영기관 구성원은 ICT 리스크와 그것이 금융회사 운영에 미치는 영향도를 적절히 이해 및 평가하기 위해 필요한 교육을 정기적으로 수행하고 지식의 최신 상태를 유지해야 함

2. EBA ICT·보안 리스크 관리 가이드라인

(가) 개요

□ EBA(European Banking Authority)가 관할 금융회사 내·외부 ICT 및 보안 리스크 관리에 대한 통일적 요구사항 설정을 위해 발표한 지침('20.6.30.)

○ 이는 CRD*에 따른 신용기관·투자회사와 PSD2**에 따른 PSP(지급결제 서비스 제공자)에 대하여 법적 구속력을 가짐

* Directive 2013/36/EU, Capital Requirements Directive

** Directive (EU) 2015/2366, Payment Services Directive

(나) 주요 요구사항

□ 경영기관(Management Body)은 전체 비즈니스 전략의 일부로 ICT 전략을 구현하도록 설정·승인·감독할 전반적인 책임을 부담

○ 한편, ICT 전략은 제3자 종속성을 포함한 ICT 아키텍처 전략 및 발전 방향에 대한 내용을 포함해야 함

□ 또한, 경영기관은 조직의 ICT·보안 리스크의 적절한 관리를 위해 효과적인 내부 거버넌스와 위험관리 프레임워크를 구현해야 함

○ 특히, ICT 기능, 정보보안 리스크 및 비즈니스 연속성 관리에 관한 각 내부 주체의 역할과 책임을 명확히 설정할 필요

□ 경영기관은 조직의 ICT 전략 구현 및 효과적인 ICT·보안 리스크 관리를 위한 충분한 인력·예산 규모를 확보하여야 함

○ 또한, 모든 임직원들이 정보보안과 ICT·보안 리스크에 관해 적절한 교육을 최소 매년 받을 수 있도록 보장해야 함

- ICT·보안 위험관리 프레임워크와 관련하여, ICT·보안 위험평가 결과 및 그 통제에 관한 사항은 경영기관에 시기적절하게 보고되어야 함
 - 아울러, 경영기관은 위험관리 프레임워크의 지속적 발전을 위해 최소 1년에 1번 이상 이를 검토·승인하여야 함
 - 경영기관은 ICT 감사 및 그 빈도를 포함한 감사계획을 승인해야 함
- 경영기관은 금융회사 및 고객의 데이터와 정보의 기밀성·무결성·가용성을 보장하기 위한 정보보안 계획을 승인해야 함
- 금융회사의 ICT 프로젝트 수립·진행 및 관련 위험은 프로젝트의 중요도 및 규모에 따라 개별적/통합적으로 경영기관에 보고되어야 함
- 금융회사는 조직의 사업 연속성을 보장하기 위한 비즈니스 연속성 계획(BCP)을 문서화해야 하며, 이는 경영기관에서 승인되어야 함
 - 아울러, BCP는 주기적으로 테스트 되어야 하며 그 결과 및 식별된 결함에 대한 처리는 문서화되어 경영기관에 보고되어야 함

III. 싱가포르

1. MAS 기술 리스크 관리 가이드라인 (TRM Guidelines)

(가) 개요

- MAS(Monetary Authority of Singapore)는 강화된 기술 위험에 금융기관이 적절히 대응할 수 있도록, 기술 리스크 거버넌스의 수립 등을 주요 내용으로 TRM(Technology Risk Management) 가이드라인을 개정(21.1.)
 - 이는 법적 구속력을 갖지는 않으나, 금융기관은 제공 서비스의 위험 및 복잡성에 비례하여 동 가이드라인을 적절히 참고하도록 권고

(나) 주요 요구사항

- 이사회는 IT 운영 환경의 보안, 신뢰성, 복원력을 달성하기 위해 효과적인 내부 통제 및 리스크 관리 관행을 구현해야 할 책임
 - 이를 위해 이사회는 사이버 위협 등 기술 리스크를 적절히 이해·관리 가능한 구성원을 보유해야 하고, 충분한 관련 지식 및 경험을 갖춘 CISO 등 전문가를 임명해야 함
- 이사회는 기술 리스크 관리전략의 수립·구현을 보장하고, 금융회사 주요 IT 결정이 조직의 리스크 성향과 일치하도록 감독해야 함
 - 또한, 모든 임직원들이 기술 리스크에 적절히 대응할 수 있도록 하향적 리스크 관리 문화를 배양해야 할 책임을 부담
- 구체적으로 이사회 또는 그 위원회가 부담하는 책임은 다음과 같음
 - 기술 위험 관리 프레임워크의 구축·유지·관리를 감독
 - 기술 위험 관리 프레임워크 및 전략을 감독하는 위험 관리 기능의 독립성을 보장
 - 조직 내 기술 위험 관리 전략 실행을 책임지는 고위 임원에게 충분한 권한과 자원을 할당하고, 이사회에 대한 접근 권한을 보장
 - 조직의 리스크 성향 및 리스크 허용한도를 승인
 - 기술 위험 관리 전략의 최신성 확보를 위한 정기적인 검토 수행
 - 기술 위험을 관리하는 경영진의 역량을 평가
 - 조직의 통제, 위험 관리 및 거버넌스의 효과성을 평가하기 위한 독립적인 감사 기능을 보장

- 고위 경영진은 조직에 중대한 영향을 미칠 수 있는 핵심적인 기술 위험의 확대 또는 사고에 대해 시의적절하게 이사회에 보고해야 함
- 이사회는 기술 사용과 관련된 위험에 대한 인식을 제고하고 기술 위험 관리 관행에 대한 이해를 증진하기 위한 교육을 받아야 함

IV. 호주

1. APRA 건전성 실무 가이드라인 (CPG 234)

(가) 개요

- APRA(Australian Prudential Regulation Authority)가 발간(19.6.)한 금융 회사의 정보보안 실무에 관한 지침으로서, 그 자체로 구속력을 갖지는 않음
 - 그러나, 호주 내 관련 법률이나 규정 및 법적 구속력을 가지는 APRA의 건전성 기준(Prudential Standards)의 내용을 포함하고,
 - 규제·감독당국인 APRA의 건전한 실무 기준에 대한 관점을 제공하는 기준이라는 점에서 실질적인 준수가 필요

(나) 주요 요구사항

- 이사회는 상위 기준인 CPS 234에 따라, 금융회사의 정보보안에 대한 최종적인 책임을 부담하고,
 - 회사의 정보자산에 대한 위협의 규모·범위에 상응하는 방식으로 정보보안을 유지하여 회사의 지속적이고 건전한 운영을 보장해야 함

□ 이사회는 이러한 책임 수행을 위해 다음 사항을 고려할 수 있음

○ 역할 및 책임

- 이사회가 정보보안에 관해 관여할 수준을 경영진에게 명확히 설명
- 여기에는 책임의 위임, 리스크 및 사고의 상위 보고, 보고의 시기, 범위, 내용 등 요구사항을 포함

○ 정보보안 능력

- 취약점 및 위협과 관련하여 회사의 정보보안 능력이 충분한지 고려
- 정보보안 기능을 지원하기 위한 충분한 투자를 보장
- 정보보안 전략의 이행과 관련한 진행 상황을 감독

○ 정책 프레임워크

- 정보보안 정책이 이사회에 기대치를 충분히 반영하는지 검토

○ 정보보안 통제의 구현

- 정보보안 통제의 효율성과 회사 정보자산의 전반적인 건전성에 관하여 보고받고 필요한 경우 관련 사항을 적극적으로 감독

○ 정보보안 통제의 효과성 검증

- 통제환경 전반에 걸친 효과성 검증의 범위가 충분한지 정기적으로 확인하고 필요한 경우 적극적으로 감독
- 검증 결과를 기반으로 정보보안 통제의 효율성 관련 견해를 형성

○ 내부 감사

- 정보보안에 관한 독립적인 감사를 위하여 내부 감사 기능의 기술, 역량 등의 충분성을 고려
- 감사 결론에 기초한 정보보안 통제의 효과에 대한 견해를 형성

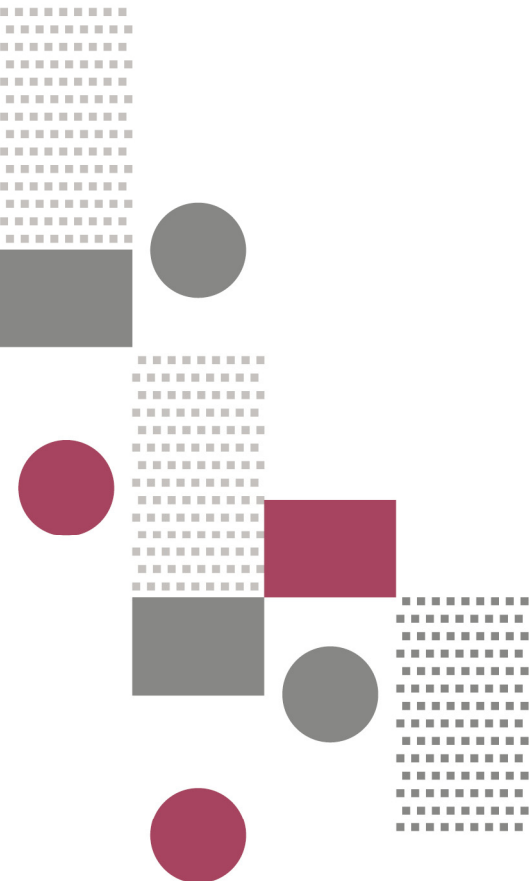
_04

News · Notice

금융보안 교육 안내

금융보안원 소식

사원사 소식



01 금융보안 교육 안내

교육일정 및 모집인원

연번	과정명	형태	일정	교육시간	정원
1	정보보호시스템 운영관리 실무	실습	11.2.~11.5.	4일(28h)	15
2	금융권 개인신용정보 보호	이론	11.3.~11.5.	3일(18h)	45
3	금융 법제도 대응을 위한 정보보호 및 개인정보보호 관리체계 실무	이론	11.8.~11.9.	2일(16h)	25
4	클라우드 보안서비스 운영 실습	실습	11.9.~11.12.	4일(28h)	15
5	금융데이터 가명, 익명 처리 및 활용	실습	11.17.~11.19.	3일(18h)	15
6	2022년도 전자금융기반시설 보안 취약점 평가기준 안내	실습	11.18.	1일(2h)	15
7	이더리움을 이용한 블록체인 플랫폼 구축 실습	실습	11.23.~11.26.	4일(24h)	15
8	금융 APT 공격과 대응	실습	11.24.~11.26.	3일(18h)	15
9	금융 정보보호 및 개인정보보호 관리체계	이론	12.1.~12.3.	3일(18h)	40

연번	과정명	형태	일정	교육시간	정원
10	금융권 취약점 점검 방법론의 이해	실습	12.1.~12.3.	3일(18h)	15
11	안드로이드 모바일 앱 취약점 분석	실습	12.8.~12.10.	3일(18h)	15
12	금융권 개인정보보호 실무	이론	12.8.~12.10.	3일(18h)	45
13	금융분야 클라우드컴퓨팅서비스 제공자 안전성평가 기준 및 평가방법	이론	12.17.	1일(6h)	40

※ 세부 커리큘럼 및 자세한 사항은 금융보안교육센터 홈페이지(<https://edu.fsec.or.kr>)를 참고해주시기 바라며, 상기 일정은 사정에 따라 변경될 수 있습니다.

02 금융보안원 소식

금융보안원, 2022년도 신입직원 채용 실시(8.9.)

금융보안원은 금융의 디지털 전환 및 4차 산업혁명시대의 금융보안을 선도할 2022년도 신입 직원을 채용을 진행한다. ▲채용 분야는 일반기획 및 IT(정보보호 포함), ▲채용인원은 30명 내외이며, ▲8.18.(수)~9.3.(금)까지 입사 지원서를 접수하여 필기전형 및 1·2차 면접 전형을 거쳐 12월 중 최종 합격자를 발표할 예정이다.

금융보안원, 금융분야 데이터전문기관 지정 1년의 주요 성과(8.12.)

금융보안원은 데이터전문기관으로 지정받아 지난 1년간 데이터 결합 39건(완료 33건, 진행 6건) 및 익명처리 적정성 평가 35건(완료 34건, 진행 1건)을 수행하는 등 데이터 결합·활용 시장을 선도('21.8.5. 기준)했다. 앞으로도 국내 데이터 시장의 데이터 결합을 선도하는 데이터 전문기관으로서 단순 결합뿐만 아니라, 재식별 가능성 검토 등 결과에 대한 안전성 검토와 분석·활용을 지원하여 국내 데이터 산업이 보다 활성화될 수 있도록 지속적으로 노력할 예정이다.

* 금융위원회는 금융보안원을 금융분야 첫 데이터전문기관으로 지정('20.8.6.)

국내 유일의 금융권 특화 사이버침해 위협분석 대회인「FIESTA 2021」개최(8.17.)

금융보안원은 금융권에 특화된 사이버 침해 위협분석 대회인 「FIESTA* 2021」을 '21.9.3.(금)~9.13.(월)까지 포렌식·악성코드·모바일·웹해킹 등 총 4개 분야에 걸쳐 개최하였다. 올해는 랜섬웨어(Ransomware), 지능형지속위협(APT) 등 최신 사이버 침해위협 트렌드를 반영하여 실제 침해사고 대응 프로세스와 유사한 시나리오를 구성함으로써 실제적인 침해 위협분석 능력을 평가하였다. 대회 성적이 우수한 6개팀(금융회사 재직자와 대학(원)생 각 3팀씩)을 선정하여 금융보안원장상과 포상금을 시상하였다.

* FIESTA는 Financial Institutes' Event on Security Threat Analysis의 약자로 스페인어로 축제를 뜻하며 대회를 축제처럼 즐기자는 의미로, 2018년부터 금융보안원이 금융권에 특화된 사이버침해 위협분석대회로 개최해오고 있음

제4회 금융보안관리사 합격자 41명 배출(9.13.)

금융보안원은 '21.9.10.(금) 제4회 금융보안 관리사(CFSE, Certified Financial Security Expert) 최종 합격자 41명을 발표하였다. 지금까지 금융권 IT·정보보호 담당자를 대상으로 ▲법·제도 ▲관리체계 ▲IT ▲보안 등의 전문 교육과정 운영과 검정시험을 통해 2018년 이후 총 132명의 금융보안 전문가를 배출하였다. 또한 '21.9.14.(화)부터 '21.10.27.(수)까지 제5회 금융보안관리사 교육과정을 이어 진행하는 등 금융보안 전문인력을 지속적으로 배출해 나갈 예정이다.

* 금융보안관리사는 금융보안원이 시행하는 금융위원회 소관 등록민간자격으로 금융권에 필요한 검증된 보안 전문 인력을 양성하기 위한 과정보형 자격제도임

금융정보보호 컨퍼런스「FISCON 2021」11월 23일 온·오프라인 개최

금융보안원은 국내 최대의 금융정보보호 컨퍼런스인 「FISCON 2021」을 '21.11.23.(화) 여의도 콘래드서울 호텔에서 개최하고, 온라인으로 실시간 생중계할 예정이다. 컨퍼런스는 오프닝 행사(개회식, 특별 및 기조강연), 세미나(주제강연, 비공개세션) 개최, 정보보호산업 전시 등으로 진행된다.

▲(개회식) 김영기 금융보안원 원장 개회사, 윤재옥 국회 정무 위원장, 이세훈 금융위원회 사무처장, 이찬우 금융감독원 수석부원장 등 주요인사 축사 및 시상식 ▲(특별 및 기조강연) 서울 경찰청 금융범죄수사대 이범주 경정의 특별강연, 김병철 금융감독원 디지털금융감독국장의 기조 강연 진행 ▲(주제강연) 총 3개 트랙, 18개 주제 강연 ▲(비공개세션) 금융권 주요회사(금융보안원 대의원사) 대상 비공개 전문 강연 ▲(전시) 한국정보보호산업협회(KISIA) 주관으로 국내 주요 정보보호 기업의 다양한 금융보안 관련 제품 및 서비스를 전시



Financial Information Security Conference 2021
금융정보보호 컨퍼런스
FISCON 2021
DATE 21.11.23(Tue)
VENUE Conrad Seoul, Grand Ballroom 3F

디지털 플랫폼 시대,
금융보안의 도전 과제와
미래 전략

• 행사 프로그램

시간	주요강연	비공개세션
09:00-09:30	개회식	개회식
09:30-10:00	주제강연	주제강연
10:00-10:30	주제강연	주제강연
10:30-11:00	주제강연	주제강연
11:00-11:30	주제강연	주제강연
11:30-12:00	주제강연	주제강연
12:00-12:30	주제강연	주제강연
12:30-13:00	주제강연	주제강연
13:00-13:30	주제강연	주제강연
13:30-14:00	주제강연	주제강연
14:00-14:30	주제강연	주제강연
14:30-15:00	주제강연	주제강연
15:00-15:30	주제강연	주제강연
15:30-16:00	주제강연	주제강연
16:00-16:30	주제강연	주제강연
16:30-17:00	주제강연	주제강연

주최
금융보안원
금융정보보호협회
금융정보보호학회
금융정보보호학회
금융정보보호학회
금융정보보호학회
금융정보보호학회
금융정보보호학회
금융정보보호학회

03 **사원기관 소식**

SC제일은행 'Women in FinTech' 아카데미 2기 데모데이·수료식 개최(8.26.)

SC제일은행은 여성 청년 핀테크 창업가 육성을 위한 사회공헌 프로그램인 'Women in FinTech 아카데미' 2기의 데모데이와 수료식 행사를 온택트방식으로 개최했다고 8월 26일 밝혔다. 데모데이에는 앞서 5주간 10회의 집중적인 핀테크 교육과정을 거쳐 선발된 아카데미 2기의 15개 팀이 참여했다. 각 팀의 대표들은 엔젤투자자 등으로 구성된 평가위원회와 온라인 관객을 대상으로 빅데이터, NFT, 블록체인 등 4차 산업의 핵심기술과 비대면 금융 서비스 기술 등을 반영한 핀테크 창업 아이디어를 발표했다. 이 경연을 통해 4개 부문(Women in Fintech Innovator, Creator, Frontier, Starter)에서 6개 우수팀이 최종 선정됐다.

신한금융투자 직원 대상 ICT 콘퍼런스 개최(8.26.)

신한금융투자는 임직원들의 정보 기술 역량 강화를 위해 지난 8월 6일부터 ICT 콘퍼런스를 시작하여 진행하고 있다고 8월 26일 밝혔다. ICT 콘퍼런스는 사내 비대면 화상회의를 통해 최근 기술 동향에 관한 설명과 질의응답으로 진행되며, 기본적인 이해부터 실제 업무에 적용을 돕는 다양한 사례를 다룬다. 신한금융투자는 신한금융그룹이 추진하는 디지털 트랜스포메이션 전략에 발맞춰 ICT콘퍼런스와 같은 다양한 프로그램을 통해 직원들의 디지털·ICT 역량을 지속적으로 강화하고 있다.

KB손해보험 '자동차보험 AI 자동심사 시스템' 개발(9.15.)

KB손해보험이 업무 자동화를 통한 자동차(이륜차)보험 가입 심사료 업무 효율 및 고객 편의성을 높일 수 있는 '자동차보험AI자동심사 시스템'을 최근 도입했다. 이 시스템은 우선 이륜자동차의 운행용도 판단을 위한 사진심사에 활용된다. 기존에는 보험심사 담당직원이 직접 고객이 제출한 사진을 보고 운행용도 심사를 진행했으나 AI기반 자동심사 시스템에서는 '이미지에서 의미있는 객체의 종류와 그 위치를 정확하게 찾아내는 기술'의 머신러닝 방식을 통해 박스형태의 배달통 장착 여부를 AI가 찾아내 이륜자동차의 운행용도를 자동으로 판단한다. 이에 따라 고객의 심사 대기 시간이 대폭 감소게 됐고 보험심사 담당직원 들의 업무도 효율적으로 운용이 가능해졌다.

IBK기업은행 '금융사기 AI 모니터링시스템' 도입(9.16.)

IBK기업은행은 보이스피싱 피해로부터 고객의 자산을 보호하기 위해 '전기통신금융사기 AI 모니터링 시스템'을 도입한다고 밝혔다. 이 시스템은 AI가 보이스피싱 사례 학습으로 이상 거래에 나타나는 반복적인 거래 등을 분석해 빠르고 정확한 실시간 보이스피싱 사기 및 대포통장 탐지대응이 가능해 피해를 사전에 예방할 수 있다. 또한 AI의 주기적인 학습을 통해 신종 보이스피싱 사기수법도 신속하게 파악할 수 있어 유사 피해확산 조기 차단이 가능하다. 아울러 기업은행은 시스템 도입과 함께 여러 유관기관과의 협약을 체결해 특정 사기에 취약한 대상을 사전 선별하고 지속적인 모니터링으로 피해를 예방할 계획이다.

KB증권 핀테크와 협력해 서비스형 बैं킹플랫폼 구축(9.23.)

KB증권은 다양한 핀테크사와 협력해 새로운 차원의 금융서비스를 제공하기 위해 서비스형 बैं킹(BaaS) 플랫폼을 구축했다고 9월 23일 밝혔다. 'BaaS'는 금융기관이 제3자(핀테크 등)에게 새로운 서비스를 개발할 수 있도록 계좌개설, 주식·금융상품 매매 등 금융기관의 서비스를 하나의 솔루션처럼 만들어서 쉽고 편리하게 쓸 수 있도록 지원한다. 핀테크사는 금융회사와의 협업이 필요하고 새로운 차원의 고객경험을 제공하기 위해서는 금융회사의 지원이 큰 도움이 되기 때문에 KB증권은 디지털 생태계 확장에 적극적으로 나서며 서비스형 बैं킹을 주도한다는 계획이다.

교보생명 빅데이터 클라우드 시스템 구축(9.23.)

교보생명은 임직원을 위한 '빅데이터 클라우드 시스템(Ocean)'을 구축하고 서비스를 전격 개시했다고 9월 23일 밝혔다. 앞서 지난 2월 교보생명은 방대한 빅데이터 분석과 자유로운 인프라 확장이 가능하도록 자사의 빅데이터 시스템 및 중요 워크로드를 아마존웹서비스(AWS)로 이전한다고 밝힌 바 있다. 이번 클라우드 시스템 도입으로 현업 분석가는 자신의 PC로 클라우드 환경에 접속해 분석 소프트웨어 및 당사 데이터를 별도의 준비 없이 즉시 사용할 수 있게 된다. 즉, 현업 부서에서 근무하면서 동시에 데이터 분석의 기본과 메커니즘을 이해하는 현업 데이터 분석가 양성을 위한 여건이 조성된 것이다.

부산은행 핀테크 스타트업 육성 'BNK 핀테크랩' 모집(9.24.)

BNK부산은행은 핀테크 분야 스타트업을 육성·발굴하기 위해 'BNK핀테크랩 4기'를 모집한다고 밝혔다. 지역 핀테크 산업 생태계를 조성하고 핀테크 업계와 상생할 수 있는 혁신 사업모델을 만들기 위해 마련한 프로그램이다. 10월3일까지 신청서를 접수한 후 서류심사와 비대면 평가를 통해 10월 중순 15개 내외의 기업을 선정하고 내년 2월까지 총 5개월간 'BNK핀테크랩 4기'를 운영할 계획이다. 선정된 핀테크 스타트업에게는 ▲BNK금융그룹 계열사와 협력 모델 발굴 ▲법률 상담 및 컨설팅 ▲1대 1 맞춤형 멘토링 ▲투자유치를 위한 연계 지원 ▲사업 공간지원 등 다양한 창업기업 육성 프로그램을 제공한다.

※ 사원기관의 디지털금융·핀테크 또는 정보보호 관련 소식을 알리고 있습니다. 이와 관련하여 아래의 주소로 보도자료(링크 등)를 보내주시면 내용을 반영하고자 하오니 많은 참여 부탁드립니다.

E-Mail : research@fsec.or.kr

Tel : 02-3495-9711~13

전자금융과 금융보안 관련 전문가 기고 안내

전자금융과 금융보안 관련 기술·제도·정책 등의 연구 자료를 제공하기 위해 간행물 형태로 금융회사, 금융당국 및 유관기관에 배포하고 있습니다. 해당 간행물을 통해 금융권의 현안, 논평, 시사점 등 다양한 사안에 대해 공유하고 발전방향 등을 함께 모색하고자 전문가 기고를 안내하오니 여러분의 많은 참여 부탁드립니다.

1. 모집분야

□ 전자금융 및 금융보안 관련 현안사항(정책 및 기술) 및 시사점 등

전자금융 및 금융보안 관련 연구(안) 예시

분야	전자금융 및 금융보안 관련 연구(안) 예시
보안 정책·관리	국내외 전자금융과 금융보안 관련 법률 및 제도 개선방안, 자율규제 방안 등
인증·암호기술	전자금융 신 인증기술 연구, 금융부문 암호기술 보안성 연구 등
서비스·응용SW 보안	스마트 결제 서비스 보안 기술, 금융 SW 시큐어 코딩 방안 등
모니터링·네트워크 보안	금융사 APT 대응 방안, 이상거래탐지시스템 기술 연구 등
스마트 기기·차세대 보안	스마트 단말 보안 강화 기술, 금융부문 빅데이터 분석 기술, 금융권 클라우드 보안 등

2. 기고신청

□ (제출 항목) ① 기고자명 및 소속(기관 및 부서명), ② 원고제목, ③ 목차, ④ 요약 내용(A1 1매 이내)

※ 선정 이후 작성해야 할 원고분량은 A4용지 15~20매 내외(폰트 12 등)입니다.

□ (제출 시기) 상 시

□ (제출처) 금융보안원 보안연구부 연구총괄팀

- e-Mail : research@fsec.or.kr Tel : 02-3495-9711~13

3. 기타

□ 수록된 원고에 대해서는 금융보안원의 지급기준에 따라 소정의 원고료 지급

□ 선정된 주제에 대해 접수 후 2주 이내 별도 안내

※ 기고신청 건은 선정되지 않을 수 있습니다.



온·오프라인
병행 개최

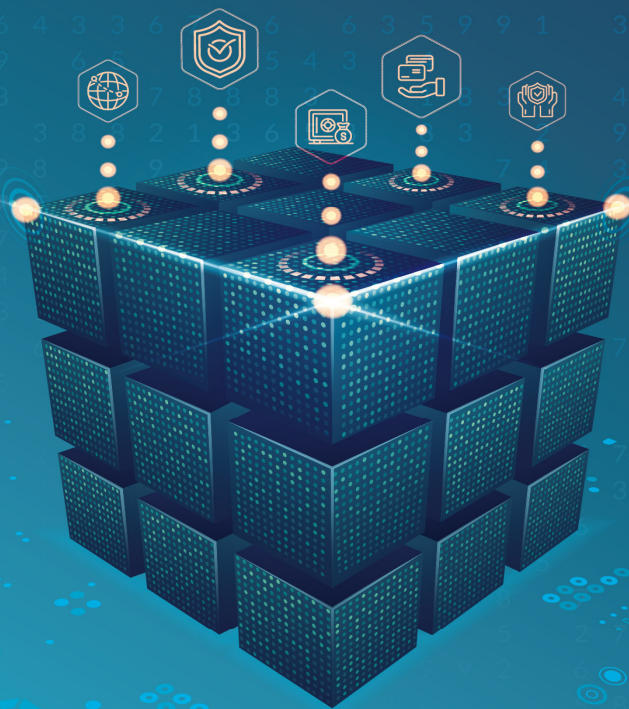
Financial Information Security Conference 2021

금융정보보호 컨퍼런스

FISCON 2021

DATE 21. 11. 23(Tue)

VENUE Conrad Seoul, Grand Ballroom 3F



디지털 플랫폼 시대,
금융보안의 도전 과제와
미래 전략

주최



금융보안원

금융정보보호협의회



금융보안포럼

후원



금융위원회



금융감독원

kisia 한국정보보호산업협회

전자금융과 금융보안

발 행 2021년 11월

발 행 인 김 영 기

발 행 처 금융보안원

주 소 경기도 용인시 수지구 대지로 132

(비매품)

본 문서의 내용은 금융보안원의 서면 동의 없이 무단전제를 금합니다.
본 문서에 수록된 내용은 고지없이 변경될 수 있습니다.

전자금융과 금융보안

e-Finance and Financial Security

금융미래를 열어가다 금융보안파트너

금융보안원

FINANCIAL SECURITY INSTITUTE

전자금융과 금융보안 | 제26호



9 772671 708004

ISSN 2671-7085