ARR-VII-2017-①-62 제13호 I 2018-07

전자금융과 금융보안

e-Finance and Financial Security

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

ARR-VII-2017-①-62

제13호 | 2018-07

전자금융과 금융보안

e-Finance and Financial Security

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

제13호 | 2018-07

Contents

전자금융과 금융보안
e-Finance and Financial Security

Leading Article

망분리 이후 사이버 위협과 대응을 위한 제언

김성보, 현대해상(CISO)

1. 서론

기업은 언제나 사이버 위협에 노출되어 있다. 보이는 위협과 비교할 때 보이지 않는 위협인 사이버 위협은 언제라도 기업 존립에 큰 위기를 불러 올 수 있다. 기업들은 사이버 위협으로부터 자사를 안전하게 지켜내기 위해 정보보안에 각별한 관심과 투자를 시행하고 있다. 2016년은 기업 정보보안에 있어 큰 변화가 있었던 시기였고 변화의 중심에는 전사 네트워크 망분리(이하 "망분리"라 한다.) 사업이 자리 잡고 있다. 기업은 망분리라는 강력한 보호막을 갖춘 정보보호시스템 가운데서 운영되고 있다. 본고에서는 망분리 이후 기업의 사이버 보안 위협을 전사적 관점에서 분석해 보며, 보안 위협 분석과 함께 발생 가능할 것으로 예상되는 대응방안에 대해서도 제언한다.

2. 망분리 이후 전사적 관점에서 바라본 사이버 위협 분석과 대응

1년 앞서 망분리를 적용한 은행권 외 다른 금융권은 2016년 12월 31일을 기준으로 내부망과 인터넷망 분리를 핵심내용으로 하는 전사 네트워크 망분리시스템 구축을 의무적으로 실시하였다. 그 결과 전사네트워크는 내부망과 외부망으로 경계를 갖고 구분 되었으며, 각 기업은 망분리 환경에서 이전과는 다른 새로운

전사네트워크 운영 경험을 축적하는 시간을 보내고 있다. 이제 기업은 내부망을 중심으로 중요 자산을 보호할 수 있게 되었다. 인터넷은 별도로 준비된 외부망에서 사용하게 되어 인터넷 사용에 따라 필연적으로 발생하는 외부 침입에 의한 자산 침탈에 대해 현저하게 높아진 방어체계를 갖추게 된 것이다. 그렇다면 이제 외부의 사이버 위협으로부터 안심할 수 있는 것인가? 유감스럽게도 위협은 여전하며 그에 대한 대응 역시 필요하다. 내부망과 외부망 경계를 기준으로 있을 수 있는 사이버 위협을 살펴보면 크게 내부망과 외부망에서 각 4개씩 총 8개의 위협이 예상된다.

2.1 내부망 위협 분석

내부망은 안전한 것인가? 내부망이 안전하기 위해서는 외부와 연결된 포인트가 없어야 한다. 기업에서 과연 그 연결 포인트가 없을 수 있는가? 외부와 연결 포인트 없이 격리된 망 안에서 모든 작업이 가능한 것인가? 질문에 대한 답은 이미 알고 있다. 기업의 핵심 자원이 배치되어 있는 내부망에 외부로부터 접근할 수 있는 방법은 원칙적으로 없다. 닫아버린 문을 열 수 있는 방법은 안에서 열어야만 가능하다. 하지만 실제로 내부망과 외부망은 업무적인 필요성을 근거로 연결이 요구된다. 연결의 필요성을 주장하는 요구사항을 몇 가지로 분류해보면 1) 외부망에서 내부망으로 파일 전송이 필요한 경우, 2) 기업 고유의 업무 완성을 위해 외부 기관과 연결이 필요한 경우, 3) 내부망에 설치된 단말기 또는 장비들을 사용할 목적으로 다양한 매체 연결(예, USB)을 요구하는 경우, 4) 내부망에서 외부로부터 수신된 이메일(E-mail) 확인이 필요한 경우 등을 생각해 볼 수 있다. 각 요구사항을 순차적으로 살펴보면 다음과 같다.

1) 외부망에서 내부망으로 파일 전송이 필요한 경우

외부망에서 내부망으로 파일을 전달할 때 경계를 자유롭게 통과할 수 있는 수단이 필요하고 대부분의 금융회사는 망연계시스템을 사용한다. 망연계시스템

사용으로 내부망과 외부망은 무엇이든 주고 받을 수 있는 연결 수단을 확보하게 된다. 이러한 망연계시스템에 의해서 내부망에 외부 데이터가 유입될 수 있는 길이 열리게 되는 것이고 바로 이 지점에서 보안 위협이 나타나게 된다. 망연계시스템을 통해서 외부망에서 내부망으로 전달되는 파일은 외부망 쪽에서 생성되거나 기업 외부에서 작성되어 전달된 파일 형태가 되는데 이 파일에 예상치 않은 악성코드가 포함되어 있을 수 있다. 이러한 경우 파일을 통한 악성코드 유입을 사전에 예방 또는 차단할 수 있는 절차와 도구 등이 필요하다.

2) 기업 고유의 업무 완성을 위해 외부기관과 연결이 필요한 경우

내부망에서 처리하는 업무는 그 자체로 완성되는 일이 많지 않다. 업무 완성을 위해 외부에 있는 기관과 연결하여 처리하는 과정이 필요하다. 예를 들어 보험사의 경우 유관기관과 연결해야만 완성 될 수 있는 업무가 있다. 이 경우 나의 내부망에 안전하다고 확신하기에는 애매한 상대방과의 연결이 문제가 될 수 있다. 불확실하게 보이는 상대방과 연결되어야 하는 지점에서 보안위협이 발생할 가능성이 높다. 잘 알려진 워터링홀(Watering Hole)공격[1]이 그 예이다. 공격자는 목표 기관이 업무를 위해 연결해야만 하는 보안이 취약한 기관을 찾아내고, 이 기관에 악성코드를 잠복시켜 연결시 목표기관에 악성코드를 전송 하여 감염시킬 수 있다. 이러한 경우에는 외부기관과의 연결에서 상대 기관의 상황과는 별개로 자신이 운영하는 내부망을 안전하게 지키기 위한 절차와 도구 등이 요구된다.

3) 내부망에 설치된 단말기 또는 기타 장비들에 사용을 목적으로 다양한 매체 연결(예, USB)을 요구하는 경우

내부망에 위치한 전산 자산은 생각 이상으로 다양하다. 대부분의 자산에는 외부 자산 연결을 위한 매체를 갖고 있다. 대표적인 것으로 USB를 사용하기 위한

1) 사자가 먹이를 습격하기 위해 물웅덩이 근처에 매복하는 것과 유사하게 공격 대상이 주로 방문하는 웹사이트를 파악한 후 해당 웹사이트의 취약점을 이용하여 피해자 접속 시 악성코드에 감염되게 하는 공격 방법.

USB포트가 있다. 내부망에 있는 전산 자산에 외부 매체를 사용하여 접속하려는 시도 시점부터 보안 위협이 발생 할 수 있으며, 이러한 외부와의 연결 포인트는 전산 자산의 도입 초기시점에서 물리적으로 제거하는 것이 가장 바람직하지만 현실적으로 어렵다. 따라서 외부매체 사용을 위한 절차를 마련하고, 승인되지 않은 절차에 의해서는 사용할 수 없도록 하는 통제 장치 등을 확보하는 것이 필요하다. 특히 단말기에서만큼은 USB와 같은 장치가 작동하지 않도록 하는 조치가 필요하다. 일반적으로 USB에 대해서는 통제를 강하게 하지만 사용이 반드시 필요한 경우에는 일정한 승인 절차를 거쳐서 사용하게 하고 있다. 이 승인 단계에서도 보안 위협이 발생할 수 있다. 승인 절차는 정상적으로 진행되었음에도 USB에 예상하기 어려운 악성코드가 숨겨져 있다면 내부망이 위협받게 된다. 이를 해결하기 위한 솔로몬의 지혜를 떠올리게 만드는 지점이다.

4) 내부망에서 외부로부터 수신된 이메일 확인이 필요한 경우

정보보안에는 늘 생각하고 답을 찾아야 하는 모순된 가치가 있다. 안전성을 확보함과 동시에 사용자의 편리성을 확보해 주는 것으로 언제나 적절한 답을 찾는 노력이 요구된다. 외부로부터 수신된 이메일을 내부망에서 열람 가능하도록 해주어야 하는가 아니면 차단해야 하는가? 하는 것이 대표적인 사례이다. 물론 원칙은 차단하는 것이지만 사용자의 입장에서 내부망과 외부망을 오가며 업무를 수행하는 것이 생각 이상으로 번거롭고 불편할 수 있다. 이러한 불편은 대부분의 직원에게 해당되는 것이 아니라 일부 직원에게 한정될 가능성이 높은데 바로 그 일부 직원들의 업무가 비중있는 일일 경우 정보보호 담당자의 고민이 깊어진다. 이러한 상황에서 이메일 방어 훈련, APT 시스템 설치 등은 안전성을 높이고 사용에 있어 편리할 수 있도록 방법을 찾아주는 대안이 될 수 있을 것이다.

2.2 외부망 위협 분석

전사 수준의 네트워크 망분리에 의해서 자연스럽게 생기는 것이 외부망 개념이고 이러한 외부망은 인터넷 사용이 가능한 환경을 의미한다. 인터넷 접속이 가능하므로 외부 환경에 접속하는 순간 다양한 보안 위협에 노출되고 심각한 위험에 처할 가능성이 높아진다. 외부망 사용 환경에서 예상되는 보안위협이 발생하는 시점을 몇 가지로 분류해보면 1) 인터넷을 통해 외부 웹사이트에 접속하는 시점, 2) 외부로부터 수신된 이메일을 확인하는 시점, 3) 저장 매체를 통한 단말기 접속 시점, 4) DDoS 공격 발생 시점 등이다. 발생 시점별 위협을 살펴보면 다음과 같다.

1) 인터넷을 통해 외부 웹사이트에 접속하는 시점

인터넷 사용을 위해 외부에 접근하는 시점부터 사용자는 보안위협에 노출된다. 피싱, 파밍 등 보안과 관련해서 듣게 되는 다양한 용어들과 직면하는 출발점이라 할 수 있다. 기업들이 영업목적으로 운영하는 웹사이트 등은 직접적으로 위험에 노출되므로 적절한 방어 절차와 도구가 요구된다. 기업이 신뢰할 수 있는 것으로 생각하는 웹사이트도 예상과는 달리 위협적인 지점이 될 수 있으므로 외부 웹사이트 전체에 대해 위협을 늘 모니터링 할 수 있는 절차와 도구 역시 필요하다. 웹사이트 접근 제어 도구, 보안관제서비스, 패치관리 절차 등은 대표적인 대응수단이라 할 수 있다.

2) 외부로부터 수신된 이메일 확인 시점

기업뿐만 아니라 개인도 이메일 사용은 필수적이 되었다. 공격자의 입장에서도 이메일은 비용대비 효과가 높아 중요한 공격 수단이라 할 수 있다. 이메일에 첨부된 파일을 열어보는 것에서 이제는 메일 자체를 열람만 하더라도 위협에 노출되는 상황이 되었다. 이메일 사용을 포기하지 않는 한 이메일 사용으로 인한 위협은 계속될 것으로 전망되므로 시스템적인 대응과 더불어 임직원의 보안의식을 높이기

위한 교육 등의 노력이 필요할 것으로 보인다. 외부 포탈을 통한 이메일 접근 차단 등 정보보호 담당자가 솔로몬의 지혜를 가장 애타게 찾는 또다른 지점으로 보인다.

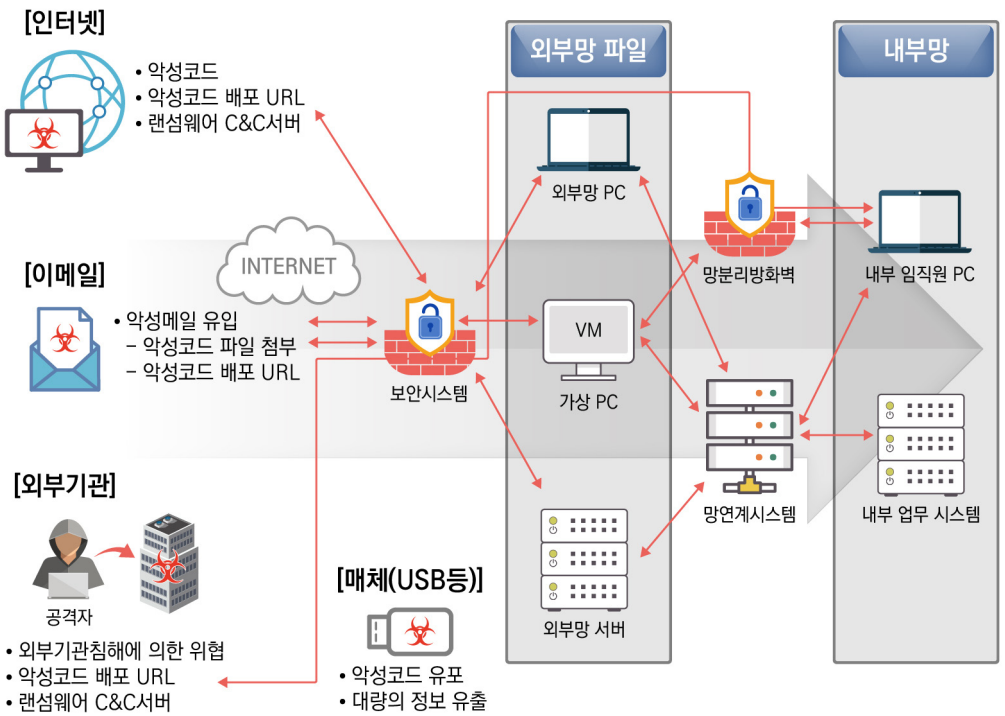
3) 저장 매체를 통한 단말기 접속 시점

내부망 위협에서 검토한 바와 같이 외부망에서도 단말기 또는 장비에 부착된 매체를 통한 접근 방식은 긴장감을 불러 일으키기에 충분하다. 저장 매체는 내부망 침투를 위한 거점으로 쉽게 활용할 수 있기 때문에 그만큼 공격에 시달릴 가능성이 높다. 여러 사례가 이미 공개되어 있고 그 내용도 엄청난 파장을 일으켰지만 그에 비해 만족할 만한 해결방안이 나왔다고 할 수 없다. 성실함과 꾸준함을 가지고 절차 준수, 임직원 교육 등 할 수 있는 모든 노력을 다 하는 방법으로 대응하는 것이 현재로서는 최선으로 보인다.

4) DDoS 공격 발생 시점

망분리와 거리가 있는 이야기이지만 기업 차원에서는 DDoS 공격을 현실적인 위협으로 언급하지 않을 수 없다. 대량의 데이터를 한 곳에 집중적으로 흘러가게 함으로써 다른 사용자가 시스템에 접근할 수 없도록 하는 공격이 가끔씩 나타나고 있고 공격에 사용되는 데이터 규모도 점점 증가하고 있는 추세이다. 흘러 들어오는 데이터양이 많으면 많을수록 그에 비례하여 방어가 더 어렵다. 특히 고객 접점에 있는 시스템들의 경우 공격으로 인해 서비스 중단이 발생한다면 심각성은 크지 않을 수 없다. 매출과 고객서비스에 차질이 있게 되면 금융회사에게는 그야말로 가장 큰 위협 중에 하나라 할 수 있을 것이다. 이 문제 대응을 위해 자체적인 대응시스템 구축, 통신사의 클린존 서비스, 금융보안원의 대피소 서비스를 대안으로 활용 할 수 있다.

그림 1 금융회사의 내·외부망 보안 위협 개념도



3. 기업 사이버 위협 대응을 위한 제언 – 가시성 확보

지금까지 망분리 사업에 의해 내부망과 외부망으로 분리 운영되고 있는 상황 및 기업 목표 달성을 위한 업무 요구사항과 그 요구사항을 수용하고자 하는 과정에서 필연적으로 나타나는 현실적, 잠재적 위협요인에 대해 살펴보았다. 위에서 제시한 위협은 그나마 경험 또는 사례를 통해서 드러난 것에 불과하다. 드러나지 않은 위협에 대해서도 충분히 파악하여야 한다. 정보보호에 탁월한 사람이라도 인지 능력에는 한계가 있다. 정보보호 담당자의 역량 의존도를 최소화하면서 드러나지 않은 위협에 효과적으로 대응하기 위해 전사적 관점에서는 무엇을 어떻게 해야 하는 것일까? 가시성 확보에 그 길이 있다고 생각한다. 기업 전체를 하나의 단위로 보고 기업을 전사적인 관점에서 살피는 노력, 전체적인 관점에서 위협 포인트를

찾고 대응하는 위협 분석, 평가, 대응체계 수립을 통해서 이러한 가시성 확보가 가능할 것이다. 최근 많이 부각되고 있는 인공지능 기술을 사용하는 것도 가시성 확보에 큰 도움이 될 수 있을 것으로 보인다. 전투기 조종사들이 가장 두려워하는 것은 상대방을 볼 수 없는데 상대방에서 날아온 미사일에 의해 격추되어야 하는 것이라고 한다. 그렇다면 먼저 적을 인지하고 미사일을 발사하는 그래서 직접 적을 보지도 않고 승리하는 일은 어떻게 가능할 수 있을까? 답은 레이더시스템에 있다고 한다. 정보보호 분야에서도 높은 수준의 가시성 확보 수단을 준비하고 확보한 가시성을 꾸준하게 향상시켜 가는 노력을 하여야 한다. 이러한 노력을 통해 망분리 환경 하에서 발생할 수 있는 사이버 사고의 예방, 차단, 복구할 수 있는 방안을 찾을 수 있을 것으로 기대한다.

4. 결론

각 기업의 네트워크 환경은 기업의 필요에 따라 구축되므로 구조와 환경이 동일할 수는 없겠지만 망분리를 의무적으로 이행했어야 하는 금융회사라면 크게 내부망 VS 외부망 구조로 네트워크 환경을 갖게 되었을 것이며, 내부망을 보호하기 위한 방안을 설계, 운영하고 있을 것이다. 본고는 내부망과 외부망에서 발생 가능한 위협을 분석하여 위협 항목을 제시하였고 제시된 위협에 대응하기 위한 의견을 정리하였다. 다만, 구체적인 대응은 각 사업장 환경에 적합한 방법을 찾아 적용해야 할 것이다. 이러한 탄탄한 보안을 위한 여정은 IT 기술을 사용하지 않게 되는 그날까지 끝나지 않는다. 사용자 편리성과 안전성이라는 모순적 가치에 대한 답을 찾는 여정도 그러할 것이다. 저자는 모순된 가치에 직면하였음에도 솔로몬의 지혜를 찾아 대안을 마련하여 새로운 길을 만들어낸 사람들을 가끔 만나게 되는데 그렇게 멋있을 수가 없다. 새롭게 시작된 망분리 항해에서 모순적 가치를 능숙하게 해결하는 멋진 여정을 하시길 기원한다.

Research

- 블록체인 국제 표준화 현황
- 신용카드 직승인 가맹점 개념과 동향
- 금융보안 정책 국내외 최신 동향 및 이슈

블록체인 국제 표준화 현황

오 경 희*

* TCA 서비스 대표, khoh@tcaservices.kr

요 약

블록체인을 포함하는 분산원장기술은 네트워크의 참여자들이 공인된 제3자 없이도 공동으로 거래 정보를 검증하고 기록, 보관함으로써 원장의 무결성 및 신뢰성을 확보하기 위한 기술이다. 신뢰할 수 없는 네트워크상에서 합의된 거래 기록을 유지 관리할 수 있다는 특징으로 인해 금융권뿐만 아니라 공공, 물류, 의료 등 광범위한 분야에 적용 가능한 새로운 플랫폼으로 기대를 모으고 있다.

전 세계적으로 다양한 블록체인 플랫폼과 응용 사례들이 나타나고 있는데, 이들은 서로 다른 사설 또는 오픈소스에 기초하여 다양한 방식으로 구현되고 있어 확장 및 상호운용이 어려운 상황이다. 이에 따라 국제적인 차원에서의 표준화 활동도 활발히 이루어지고 있다.

국내 금융권에서도 블록체인 기반의 응용 도입이 활발히 이루어지고 있으며 금융보안표준화협의회를 중심으로 금융권 블록체인 보안 표준이 개발되고 있다. 금융권은 이러한 국제 표준화 동향을 참조하여 현재 및 향후 개발·도입하고자 하는 블록체인 응용서비스가 확장성과 상호운용성을 확보할 수 있도록 하고 국내 기술과 표준이 국제 표준과 연동되고 나아가 선도할 수 있게끔 활용할 필요가 있다.

본고에서는 국제 표준화 기구에서 진행되고 있는 전반적인 블록체인 관련 표준화 활동을 소개하고 향후 진행되어야 할 방향을 제시한다.

01 블록체인 국제 표준화 현황

Ⅰ 서 론

1. 용어 정의

블록체인은 네트워크 상의 노드들 사이에서 합의를 통해 하나의 분산원장을 생성하고 공유하기 위한 기술 중 하나다. 블록체인은 트랜잭션들을 일정 크기의 블록에 모아 저장하고 선행 블록의 해시값을 새로 만들어지는 블록의 헤더에 기록함으로써 블록을 일렬로 연결하여 분산원장을 구성한다.

비트코인이나 이더리움 등의 가상통화가 블록체인 기술을 통해 구현되고 있어 일반인들에게는 블록체인이라는 용어가 더 잘 알려져 있으나 R3 Corda나 IOTA[1]와 같이 트리 형태로 트랜잭션들을 연결해서 관리하는 분산원장이 존재하기 때문에 학술적으로는 블록체인보다 분산원장기술이라는 용어가 더 포괄적인 표현이다.

분산원장기술(Distributed Ledger Technologies, DLT)은 네트워크상의 참여자들이 투명하게 거래정보를 검증하고 분권화된 합의를 통해 기록·보관함으로써 공인된 제3의 중개자 없이도 기록된 정보의 무결성과 원장의 일관성을 유지하게 해 준다. 거래기록의 변경에 대한 안전성, 중앙집권화 된 통제 없이 참가자들의

1) IOTA(아이오타): 사물 인터넷에 특화된 플랫폼에서 사용되는 가상통화

합의에 대한 기술적 신뢰를 제공한다는 두 가지 대표적인 특징으로 인해 분산원장 기술은 참여자들이 중개기관을 포함한 다른 참여자들을 신뢰하지 않거나 의존하고자 하지 않는 경우 기존의 비즈니스 프로세스로는 해결되지 않는 신뢰의 문제를 해결하는 새로운 혁신적인 기반 기술로 대두되었다.

일반인들에게는 블록체인이라는 용어가 더 널리 알려져 있기 때문에 표준화 기구에서도 블록체인이라는 타이틀을 내세우고 실제 기술문서 내용에서는 분산원장기술이라는 표현을 쓰는 경우가 많이 나타나고 있다. 본고에서는 기구 명이나 문서 제목과 같이 고정된 명칭에서 블록체인이라는 용어를 쓰는 경우 이를 그대로 사용하였고 설명에서는 분산원장기술이라는 용어를 사용하였다.

2. 분산원장기술의 전망

분산원장기술은 일찍이 없었던 방식으로 디지털 기술을 경제와 접목시키고 있다. 금융서비스를 제공하기 위한 새로운 수단을 가능케 했을 뿐만 아니라 정부, 법적 서비스, 책임성, 공급망 및 에너지 분배를 재정의 하고 있다. 또한 당사자 간에 자산과 에너지 등을 더 유연하게, 더 적은 수수료로 거래할 수 있는 시장을 형성할 수 있게 해주며, 자산의 유래를 투명하게 공유함으로써 문제의 소재를 더 빠르고 정확하게 확인하게 해준다. 이러한 변화는 법이 적용되는 방식, 정부가 경제와 정책 프레임워크를 관리하고 시민에게 서비스를 제공하는 방식, 그리고 시민권의 작동 방식에 근본적인 영향을 미칠 것이며, 사회적 신뢰를 재정의 하게 될 것이다.

이러한 전망에 따라 국내외를 막론하고 다양한 분산원장기술 시스템들이 개발, 실험되고 있다. 그러나 현재까지의 분산원장시스템들은 특정 응용 분야의 비즈니스 로직에 의존적인 방식으로 구현되는 것이 대부분이고, 구현 방식에 따라 성능 및 확장성에 한계가 있는 경우도 많다. 사설 프로젝트 간에는 개념 차이로 인해 연동이 불가능하고 오픈소스에 기반한 경우에도 구현 방식에 따른 차이 등으로 인해 상호운용과 연동을 보장하지 못한다.

3. 표준화 필요성

분산원장기술은 전세계의 다양한 서비스를 연결하는 인프라가 될 것이라고 선전되고 있지만 그것이 실제 달성되기 위해서는 표준화가 필수적인 선결 요건이다. 분산원장기술에 기초한 지역망과 국제 공급망이 연결되고 다양한 응용들을 상호 연계하기 위해서는 기본적인 참조 모델과 이에 기반한 기술적, 정책적 연동 표준이 필요하다.

이러한 요구에 따라 2016년 ISO에서 TC 307 블록체인 및 분산원장기술(Blockchain and Distributed Ledger Technologies)의 수립이 승인되었으며 2017년 4월 호주에서의 제1차 회의를 통해 표준화 작업이 개시되었다. 또한 ITU-T에서도 SG 17 산하에 블록체인 보안 신규 연구과제(Question) Q14를 수립하고 분산원장기술의 보안 표준을 개발하고 있다. 본고에서는 ISO와 ITU-T 2개 기구를 중심으로 국제적인 분산원장기술 표준화를 위한 노력들을 살펴볼 것이다.

Ⅱ ISO의 블록체인 표준화 현황

1. TC 307의 블록체인 표준화

가. TC 307 수립 및 구조의 변화

ISO 기술위원회(Technical Committee, TC) 307은 2016년 4월 호주에서 수립이 제안되었고 9월 ISO 기술관리위원회(Technical Management Board)에서 승인되었다. 이에 따라 17년 4월 호주에서 1차 회의가 개최되었고 가장 우선적으로 용어(Terminology) 표준 개발 및 이를 추진하기 위한 첫 작업반(Working Group, WG)의 수립이 결의되었다. 그리고 향후 진행을 위해 참조 아키텍처, 활용 사례, 보안 및 프라이버시, 신원, 스마트 계약 5개의 연구반(Study Group, SG)이 결성되었다. 그 후 2차, 3차 회의를 통해 새로운 작업반과 연구반, 다른

표준 그룹과의 합동작업반(Joint Working Group, JWG)이 생겨나는 등의 구조적 변화가 있었다. 그림 1은 1~3차 회의 진행 경과를 정리한 것이다.

그림 1 TC 307 구조 변화

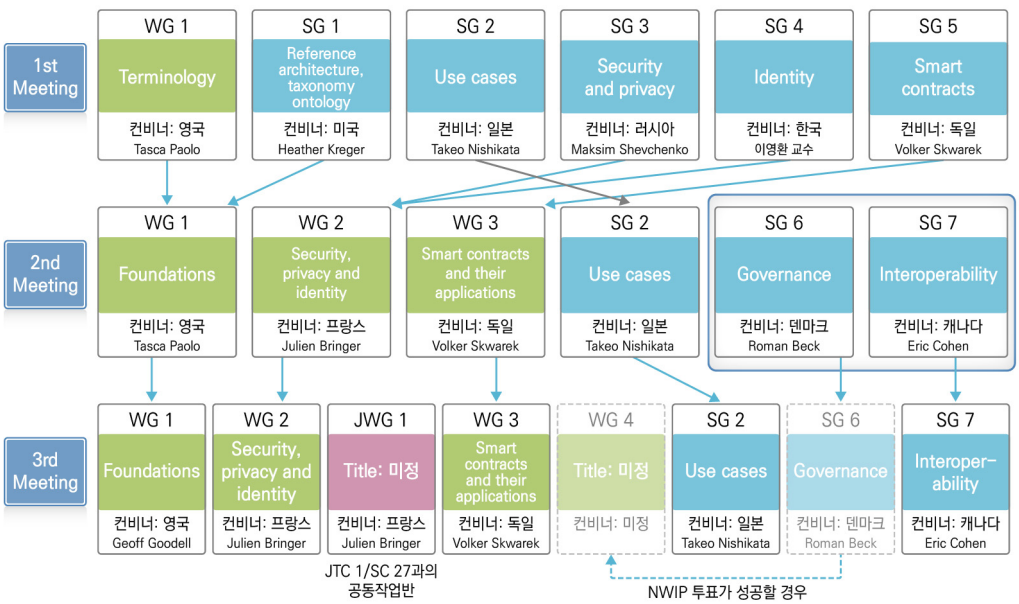


그림 1에서 볼 수 있듯이 TC 307은 현재까지 작업반 구성이 완료되지 않았고 계속적으로 새로운 표준 분야에 대한 연구가 이루어지고 있다. 연구반의 신설은 중요한 표준화 현안을 보여 준다. 현재의 추세는 기본이 되는 표준들에서 상호 운용성과 보안 관련 표준으로 확산되고 있는 상황이다. 또한 분산원장기술 표준에 영향을 미치고자 하는 국가 간의 경쟁도 드러난다. 성공적인 연구반 운영이 새로운 작업반 신설과 컨비너(Convener) 수임으로 이어지면서 컨비너십 획득을 위한 국가 간 경쟁도 만만치 않다. 2차 회의에서 나타난 구조 변경은 분산원장기술에 영향을 미치고자 하는 러시아에 대한 유럽의 견제라는 견해도 있다. 당시 러시아 대표단장이 KGB의 후신인 FSB를 위해 일하고 있었으며 분산원장기술에 대해 과도한 의욕을 표시하여 우려를 불러 일으켰다는 기사가 나오기도 했다.

나. TC 307 개발 표준 현황

3차까지의 진행에 따른 현재의 TC 307 개발 표준 현황은 아래 표와 같다.

표 1 TC 307 개발 표준 및 연구 현황

작업반/연구반	표준/ 연구 주제
WG 01: Foundations	• IS 22739 Terminology • IS 23257 Reference architecture • TR 23258 Taxonomy and ontology • TR Discovery issues related to interoperability • Study on "Data flow and data taxonomy for blockchain and distributed ledger technologies"
WG 02: Security, Privacy and Identity	• TR 23245 Security risks and vulnerabilities ※ SC 27 동의 여부에 따라 JWG 1으로 이동 예정 • TR Security of digital asset custodians • Study on "Security evaluation of consensus models"
WG 03: Smart contract and their applications	• TS 23259 Legally binding smart contracts • TR 23455 Overview of and interactions between smart contracts
JWG 1: Joint working group with ISO/IEC JTC1 SC27	• TR 23244 Overview of privacy and personally identifiable information (PII) protection • TR 23246 Overview of identity management using blockchain and DLT
SG 02: Use cases	• TR Use cases
SG 06: Governance	• TS Guidelines for governance ※ NWIP 투표 결과에 따라 WG 4로 전환 예정
SG 07: Interoperability	• Study on Interoperability issues related to cryptocurrencies' platform, utility and transaction tokens and other cryptographically supported digital assets or proxies for physical and intangible assets

1) ISO 22739 용어(Terminology)

ISO 22739는 이번 런던 회의에서 제목과 범위를 변경하였다. 2차 회의까지는 용어 및 개념(Terminology and Concepts)이라는 제목으로 진행하였으나 2차 회의에서 결의된 참조 아키텍처 표준이 분산원장기술 관련 개념들을 포함하게

되어 이와의 중복을 회피하기 위하여 순수하게 용어 정의만을 포함하기로 하였다. 프로젝트 리더는 캐나다의 Victoria Lemieux가 담당하고 있으며, 1차로 정의해야 할 용어들을 선정하고 선정된 용어들에 대한 정의를 개발하고 있다.

런던회의에서는 그간의 웹미팅을 통해 정의된 용어들 중 협의가 미진한 용어, 참조 아키텍처나 다른 그룹과의 협의가 필요한 단어들에 대한 토론이 주로 진행되었다. 블록체인, 블록, 노드, 사용자와 같은 기본적인 개념들의 정의에 대한 합의가 이루어졌으며, public/private과 permissionless/permissioned가 어떤 기준으로 정의되어야 할 것인지 등에 대한 심도 있는 토론과 합의가 이루어졌다. public/private은 DLT 서비스를 이용하는 사용자의 허가에 관한 것으로, permissionless/permissioned는 DLT시스템 내에서 노드가 수행하는 활동에 대한 허가에 관한 것으로 정의되었다.

Fork의 정의는 회의 중 합의를 마치지 못하고 향후의 웹미팅을 통해 최종안을 도출한 후 CD(Committee Draft) 투표를 진행하기로 결의하였다. Fork의 정의는 분산원장 레코드의 불변성(Immutability)과 연결되어 많은 논의가 있었다. 분산원장기술이 추구하는 바가 기록의 불변성을 달성하고자 하는 것은 맞지만 가장 최신의 블록들은 특정 노드 상에서 채택되었다고 하더라도 다른 노드들의 합의에 따라 기각될 수 있으며, 51% 공격이나 하드 포크를 통해 다른 결과가 나타날 수 있다는 것이 논점이다.

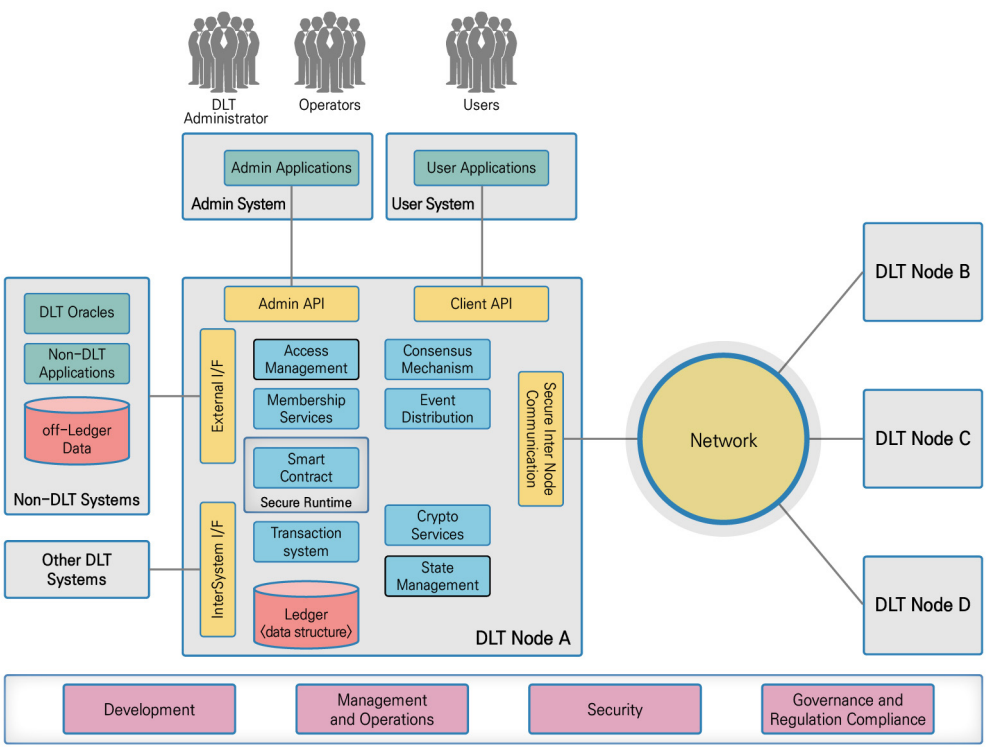
현재 70개의 용어가 선정되어 마무리 작업 중에 있으며 6월경에는 CD안을 완료하여 투표에 회부하는 것을 목표로 하고 있다.

2) ISO 23257 참조 아키텍처(Reference architecture)

참조 아키텍처는 분산원장시스템 설계의 기본 틀을 제공한다. 참조 아키텍처를 따름으로써 필수 기능 및 확장성과 상호운용성을 제공할 수 있는 분산원장시스템을 빠르고 효과적으로 개발할 수 있다. 참조 아키텍처는 기본 개념들과 DLT 시스템 유형을 설명하고 참여자의 역할과 책임 그리고 참조 아키텍처의 계층과 구성요소들을 정의한다. 미국의 Heather Kreger가 프로젝트 리더를 맡고 있다.

기능 구성요소들은 사용자 계층, DLT 외부시스템(Non-DLT Systems), API 계층, DLT 플랫폼 계층, 인프라 계층의 5개의 계층으로 나누어지며, 전 계층에 걸친 기능(Cross-Layer Functions)으로서 개발, 관리 및 운영, 보안, 거버넌스 및 컴플라이언스가 포함된다. 다음 그림은 시스템 관점에서의 DLT 시스템의 기능 구성요소를 보여준다.

그림 2 시스템 관점에서의 DLT 시스템 기능 구성요소



참조 아키텍처의 내용은 상당히 진행되었으나 아직 추가되어야 할 부분들이 남아 있다. 노드 증가에 따른 성능, DLT 서비스 관리, 크로스 체인 관리, 하위 체인과의 연결, 상호접속에 따른 서비스 통합, 스마트 계약 연동 등 상호운용성 관련 내용을 10월에 있을 모스크바 4차 회의까지 개발하여 4차 회의에서 CD 투표를 통해 합의하는 것이 현재의 목표이다.

3) TR 23258 분류체계 및 개념 간 관계망(Taxonomy and ontology)

분류체계 및 개념 간 관계망의 경우 작년 11월 회의에서 개발이 결의되었으나 프로젝트 리더인 Peter Luo의 멤버십 문제로 진행이 이루어지지 않았고 올해 5월 회의에서 첫 논의가 이루어졌다. 분류체계에 대해서는 참조 아키텍처에서 기존 진행된 내용이 일부 있어 작업 개시에 무리가 없으나 개념 간 관계망을 어느 수준까지 어떤 형태로 개발할 것인가에 대해서는 다양한 의견이 제시되었다. 개념 간 관계망 개발 경험이 있는 참가자가 많지 않아 먼저 다른 분야의 개념 간 관계망을 다룬 기존의 ISO 표준들을 검토하여 목표 산출물의 형태를 결정하기로 합의하였다. 이에 따라 차기 회의까지 기존 ISO 관련 표준의 분석과 실제 TR의 내용에 대한 2번의 기고 요청을 회람하고 이에 기초하여 웹미팅을 통해 차기 4차 모스크바 회의까지 1차 WD(Working Draft)를 개발하고 5차 더블린 회의에서 2차 WD를 개발하는 것을 목표로 하고 있다.

4) TR 23244 프라이버시 및 개인정보보호 개요

프라이버시 및 개인정보보호 개요 TR은 블록체인/DLT 시스템을 위한 프라이버시 프레임워크와 프라이버시 영향 평가, 그리고 블록체인/DLT 수명주기에서의 프라이버시 관리를 다루고 있다.

블록체인/DLT 시스템을 위한 프라이버시 프레임워크의 구성요소로는 액터(Actor)와 역할, 상호작용, 개인식별정보(Personall Identifiable Information), 프라이버시 보호 요구사항, 프라이버시 정책 및 통제를 들고 있다. 또한 이에 대한 참조로서 ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2를 참조하고 있다.

블록체인/DLT 시스템은 정보에 대한 접근과 통제가 노드 상에 분산되어 서로 다른 조직과 사람 간에 이루어진다는 근본적인 특성을 가지고 있다. 이러한 특성에 따라 프라이버시 관련 많은 현안들이 나타난다. 블록체인의 노드가 서로 다른 국가에 걸쳐 존재하게 되면 모든 이해관계자들에게 법적 만족을 보장하기 매우 어렵다. 국가에 따라 무엇이 개인정보인가에 대한 규정도 달라질 수 있고 블록체인

상에 기록된 개인정보는 잊혀질 권리나 데이터의 보관 지역에 관한 규제를 만족하기 어렵다.

이 외에도 법 규제가 변화하면서 개인정보보호 요건이 더욱 강화되는 현재의 추세라던가 암호 해독기술의 발전으로 현재의 보호 수준이 약화될 가능성, IoT 및 빅데이터 기술 발전으로 인한 모니터링 능력 강화 등이 장기적으로 개인정보 보호에 영향을 미칠 수 있다. 이 TR은 이러한 이슈들과 현재까지 개발된 표준 및 프라이버시 강화 기술들을 제시하고 있다. 이 표준은 ISO/IEC JTC 1/SC 27과의 JWG 1에서 지속 개발할 예정이다.

5) TR 23245 보안 위험 및 취약성

보안 위험 및 취약성 TR은 보안 위험 및 취약성에 대한 일반적 개요를 제공하면서 이들이 블록체인/DLT 시스템 상에서 어떻게 구체화될 지를 다루고 있다. 블록체인 특유의 보안 고려사항으로는 컨센서스 보안, 하드/소프트 포크 관리, 블록 내 데이터 관리에 관한 사항이 있다.

이 TR은 ISO 23257 참조 아키텍처에 기초하여 참조 아키텍처 내의 각 구성 요소에 대한 취약성을 제시한다. 주로 개발된 부분은 컨센서스 알고리즘에 관련된 취약성이다. 또한 기존 관련 표준에 대한 목록을 제시하고 있다. 이 표준은 ISO/IEC JTC 1/SC 27이 동의할 경우 JWG 1에서 지속 개발할 예정이다.

6) TR 23246 블록체인 및 DLT를 이용한 신원관리 개요

이 TR은 이번 회의에서 제목을 신원의 개요(Overview of identity)에서 블록체인 및 DLT를 이용한 신원관리 개요(Overview of Identity Management Using Blockchain and DLT)로, 범위를 신원 관리에 대한 개요를 제공하는 것에서 신원(Identity)의 정의, 권한부여(Authorization), 인증(Authentication), 접근 통제(Access Control)로 수정하였다.

이 TR에서는 블록체인/DLT 시스템에서 다루는 신원의 종류를 사람, 법적

개체, 자산, 프로세스로 분류하였고 블록체인 상에서의 검증 사슬을 설명하였다. 또한 이에 필요한 인터페이스를 보이고 비표준 ID의 처리 및 보안 관련 사항들을 설명하였다. 향후의 목표와 과제를 제시하고 전자적 신원 문서들을 검증하기 위한 인터페이스 검증, 폐기, 인증서 확인 등의 작업 흐름과 샘플 코드 수준까지 제시하였다.

이 TR은 이번 런던 회의에서 PDTR(Proposed Draft Technical Report)로 진행하는 것을 목표하였으나 JWG 1에서 지속 논의하기로 하였으며 국경 통제에 블록체인을 사용한 활용 사례, 공급망 관리와 블록체인의 이용 활용 사례의 2개 사례를 추가할 예정이다.

7) TR 23259 법적 구속력을 갖는 스마트 계약

이 TR은 스마트 계약이 작동하는 방식과 효익, 스마트 계약 간 상호 작용의 방법을 설명한다. 또한 스마트 계약의 기술적 법적 측면을 고려한다. 스마트 계약은 다양한 조건과 입력으로 작동할 수 있으며 다른 스마트 계약을 발효시킬 수 있다. 이들은 법적인 계약이 아닐 수 있지만 유사한 의무를 부과할 수 있다. 이 TR은 스마트 계약의 법적 측면을 분석하고 논의하기 위하여 트랜잭션 유형을 분류하고, 스마트 계약에 법적 효과를 부여하는 미국 주정부의 사례를 제시하며 스마트 계약을 설명 한다.

2. 여타 ISO 산하 기구에서의 블록체인 표준화

가. TC 215 건강 정보(Health informatics)

의료분야에는 블록체인 이용에 관한 연구가 앞다투어 이루어지고 있는 가운데 건강 정보학(Health Informatics)를 다루는 TC 215 에서는 작년 말 블록체인에 기반한 의료정보 관리를 위한 예비 작업 항목(Preliminary Work Item, PWI)이 발표되었다. 이 논의는 의료 정보 시스템 및 기기의 상호운용성을 다루는 WG 2에서

이루어 졌으며 한국의 주도하에 2018년 기술보고서 개발을 위한 신규 작업 항목을 제안하는 것을 목표로 작업 중에 있다.

이 기술보고서는 블록체인 기술이 적합한 의료 영역을 파악하는 것을 목표로 의료분야의 활용 사례를 수집한다. 또한 필요한 경우 현재 기술과의 갭분석을 시행하고, 의료기관들이 분산원장기술을 도입 할 때 필요한 권고를 제공하는 것을 범위로 하고 있다. 이 기술보고서가 개발되면 의료 기록 등 의료분야의 다양한 분산원장 응용 시스템의 개발과 도입이 촉진될 것으로 기대된다.

Ⅲ ITU-T의 블록체인 표준화 현황

1. ITU-T의 블록체인 관련 그룹 구조

가. ITU-T 연구반

ITU-T에서는 2017년 3월 정보보호 연구반 SG 17이 블록체인의 보안 측면에 관한 세미나를 주최하면서 관련 연구를 개시하였다. 이 세미나의 제목은 “블록체인의 보안 측면”이었으나 이후 이어진 논의를 통해 블록체인이라는 용어는 분산원장 기술의 특정한 구현 기술이자 상업적 트레이드마크에 가까운 것으로 간주되었고 UN 산하기구로서 상업적 접근을 경계하는 ITU-T에서는 블록체인이라는 용어 대신 분산원장기술(DLT)이라는 용어를 사용하고 있다.

ITU-T에서는 ISO와 달리 연구반(Study group, SG)에서 표준을 개발한다. 현재 ITU-T에서는 4개의 SG에서 분산원장기술 관련 표준을 개발 중에 있다. IMT 2020, 클라우드 컴퓨팅 및 신뢰 네트워크 인프라에 초점을 맞춘 미래 네트워크 연구반 SG 13, 멀티미디어 연구반 SG 16, 보안 연구반 SG 17, IoT 및 스마트 시티와 커뮤니티 연구반 SG 20이 그것이다. 또한 환경 및 기후변화를 다루는 SG 5의 경우, 개발하는 표준화 항목은 없으나 최근 개정된 산하 연구과제(Question)

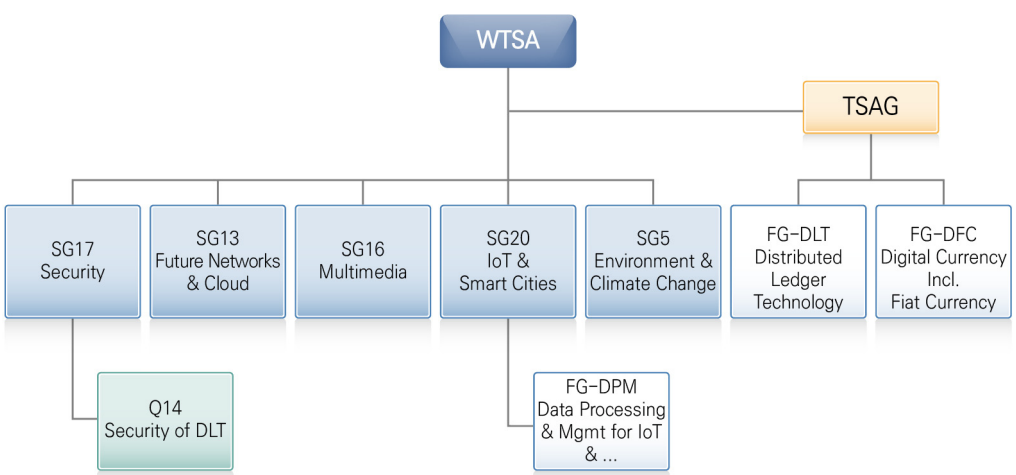
Q6의 업무에 블록체인 분야를 포함시켰다.

나. ITU-T 포커스 그룹

한편 ISO에서의 연구반과 마찬가지로, ITU-T 내에서도 직접 표준을 개발하지는 않지만 표준 개발에 필요한 폭넓은 사전 연구를 진행하고 향후 연구반에서 표준으로 개발할 수 있도록 표준화를 위한 기본적인 지침을 보고서로 발행하는 그룹이 있다. 이런 그룹을 포커스 그룹(Focus Group, FG)이라고 한다. ISO나 ITU-T는 공식 표준화 기구로서 국가 또는 기관 단위의 회원자격을 얻어야만 SG 회의에 참여할 수 있다. 그러나 FG는 ITU-T 회원 여부에 관계없이 사실 표준화 기구처럼 원하는 누구나 참여가 가능하다.

ITU-T 산하에는 분산원장기술 관련 3개의 FG가 있다. 이중 2개는 17년 블록체인 세미나의 결과로 ITU-T 표준화 자문그룹(TSAG) 산하에 신설되었다. 하나는 FG-DLT로 분산원장기술의 다양한 응용에 관한 그룹이며, 다른 하나는 FG-DFC로 디지털 법정 화폐를 포함하는 디지털 화폐에 관한 그룹이다. 그 외에 SG 20이 자체적으로 산하에 구성한 데이터 처리 관리 표준화 연구를 위한 FG-DPM이 존재한다. 그림 3은 SG와 FG 간의 관계를 나타낸 것이다.

그림 3 ITU-T 내 블록체인 관련 조직 구조



2. SG 17 Q14의 블록체인 보안 표준화

가. SG 17 Q14 블록체인 보안 연구과제

ITU-T SG 17은 블록체인 보안 세미나의 후속작업으로 FG-DLT를 TSAC에 제안한 후, 8월 회의에서는 신규 연구과제(Question) Q14, 분산원장기술의 보안 측면(Security Aspects for DLT)을 수립하였다. SG는 여러 개의 WP(Working Party)로 구성 되고, 각 WP의 연구과제(Question)에서 해당 분야의 표준을 개발한다. Q14에서는 2017년 8월 수립 당시 7개의 신규 표준화 작업 항목을 개시하였고 2018년 3월 2개의 신규 표준화 작업 항목을 추가로 승인하여 총 9개의 표준을 개발하고 있다. 표 2는 현재의 표준번호와 제목을 보여준다.

표 2 ITU-T SG 17 Q14 표준 항목

표준번호	표준 제목
X.sradlt	Security framework for DLT
X.sct-dlt	Security capabilities and threats of DLT
X.sadlt	Security assurance for DLT
X.ss-dlt	Security services based on DLT
X.strdlt	Security threats and requirements for digital payment services based on DLT
X.stov	Security threats to online voting using DLT
X.dltsec	Privacy and security considerations for using DLT data in identity management
X.das-mat	Security framework for the data access and sharing management system based on DLT
X.tf-spd-dlt	Technical framework for secure software distribution mechanism

1) X.sradlt

ISO TC 307의 참조 아키텍처는 DLT 시스템 자체의 아키텍처를 다루지만 X.sradlt는 DLT 시스템의 보안을 위한 프레임워크를 표준화한다. 그러나 DLT 시스템 아키텍처와의 연계가 필요하기 때문에, ITU-T 산하 FG-DLT에서 개발 중인

DLT Framework 작업을 참조하기로 하고 있다.

X.sradlt는 다양한 비즈니스 시나리오와 이에 대한 보안 위협의 유형과 특성을 분석한다. 또한 분산원장기술 응용 서비스의 보안을 강화하기 위한 보안 프레임워크를 정의하고 보안 강화를 위한 지침을 제공한다. 이 프레임워크는 공개 체인(Public Chain), 사설 체인(Private Chain) 및 컨소시엄 체인(Consortium Chain)에 모두 적용된다.

2) X.sct-dlt

X.sct-dlt는 DLT 시스템이 기본적으로 제공할 수 있는 능력과 DLT 시스템에서 발생할 수 있는 일반적인 위협을 설명한다. DLT 시스템의 일반적인 위협은 Q14 내의 다른 표준들과도 중복되는 부분이 있기 때문에 상세한 설명은 X.sct-dlt에서 제공하고 다른 표준들은 이 표준을 참조하거나 각 응용시스템에 특유한 위험만을 다루고 있다.

3) X.sadlt

X.sadlt는 DLT 시스템의 보안 보증 수준에 대한 지침을 제공한다. 데이터 무결성, 기밀성, 통신 보안, 크리덴셜 관리 측면에서 상, 중, 하 3개 수준으로 구성되는 보안보증 프레임워크를 제시하고 이들 각각의 보안 보증 수준을 위한 기술적 특징들을 제시한다.

4) X.ss-dlt

4X.ss-dlt는 분산원장기술을 이용한 보안 서비스의 효익과 활용 사례를 제시한다. 대표적 활용 사례로 분산원장기술 기반의 PKI, SDP(Software Defined Perimeter) 시스템 그리고 위협 정보 플랫폼을 설명한다.

5) X.strdlt

X.strdlt는 분산원장기술에 기반한 전자지불시스템을 다룬다. 특히 국가 간 전자송금에 있어서 분산원장기술은 상당한 강점을 갖는다. 이 표준은 전자송금을 중심으로 한 전자지불시스템을 설명하고 이에 대한 보안 위협과 보안 요구사항을 표준화한다.

6) X.stov

X.stov는 분산원장기술 기반의 전자투표시스템의 요구사항과 이에 대한 보안 위협 및 요구사항을 표준화한다. 전자투표라고 하면 일반적으로 선거와 같은 1인 1표 1회 비밀투표 요구사항을 생각하지만, 일반 사회에서 사용되는 주식회사의 의결 방식, 의견수렴을 위한 선호도 투표 등 다양한 투표 방식이 존재한다. 본 표준은 이러한 다양한 요구사항을 포함한다.

7) X.dltsec

X.dltsec은 분산원장기술을 이용하여 여러 조직이 신원 정보 및 속성을 교환할 때 고려해야 할 사항을 다룬다. 분산원장의 신원 정보에 대한 보안 위협을 설명하고 신원정보를 보호하기 위한 보안 최적 실무(Security Best Practice)와 구현 지침을 제공한다. 또한 신원 정보 교환 시 사용하는 인증 관련 위협을 완화하기 위해 사용될 수 있는 통제 지침을 제공한다.

8) X.das-mat

X.das-mat은 데이터 접근이 정책에서 규정한 목적으로 이루어지는지, 누구에게 제공되었는지를 추적하는 데이터 접근 및 공유시스템에 대한 보안 프레임워크를 제공한다. 이 표준은 데이터 접근 및 공유시스템의 참조 모델, 관련 객체와 이들의 역할 그리고 보안 위협 및 요구사항을 표준화한다. 또한 부록에 활용사례를 포함한다.

9) X.tf-spd-dlt

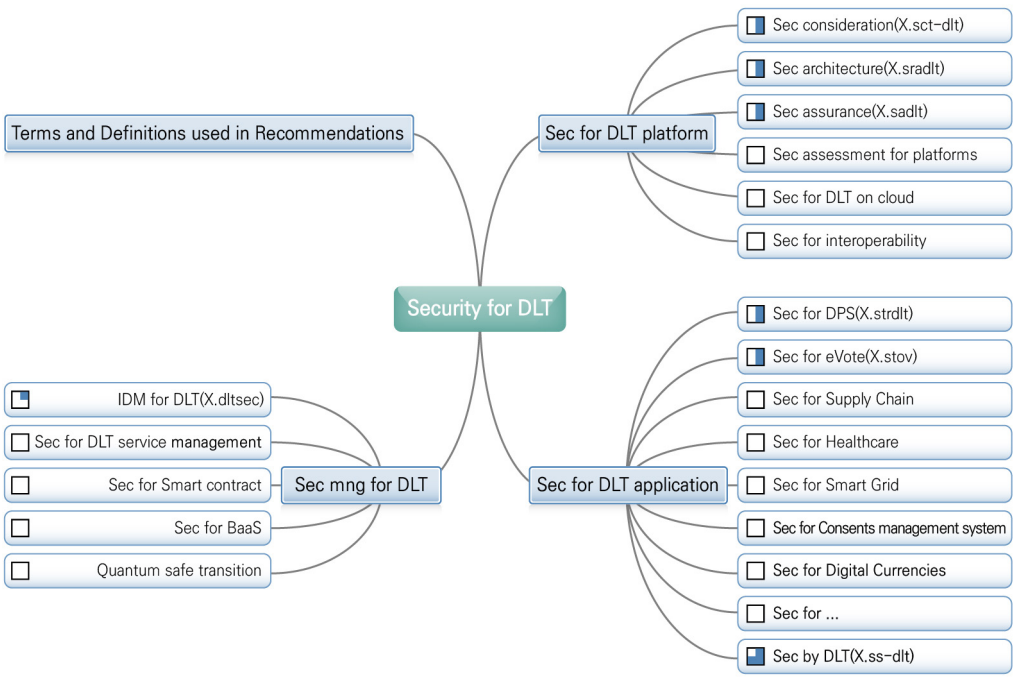
소프트웨어 배포에는 다운로드 링크를 수정하거나 소프트웨어 파일을 변경하여 악성코드를 포함시키는 등의 위험이 따른다. 이 표준은 소프트웨어 배포에 관련한 기존의 어려움을 상세히 분석하고 분산원장기술을 이용하여 신규 소프트웨어를 배포함으로써 다운로드 링크나 소프트웨어 파일등의 변경을 차단하기 위한 해결책을 제공한다.

10) Q14 향후 표준화 개발 방향

Q14는 현재 진행되는 표준에 기초하여 향후의 표준 진행방향을 제시하기 위한 분산원장기술 보안 표준화 로드맵을 마련하였다. 분산원장기술 표준은 크게 분산원장기술 플랫폼을 위한 보안표준, 분산원장기술 응용을 위한 보안 표준, 분산원장기술의 관리를 위한 보안 표준으로 나누어 볼 수 있다.

분산원장기술 플랫폼을 위한 보안 표준은 보안 프레임워크, 보안 보증, 상호운용성 등의 관련 보안 표준을 포함하며, 1차적인 중요성을 갖는다. 분산원장기술 플랫폼 자체에 대한 표준은 타 SG에서 진행될 수 있으며 이와 연계될 것이다. 분산원장기술 관리를 위한 보안 표준은 신원 관리, 서비스 관리, 스마트 계약 관리 등을 포함하며, 향후 나타날 수 있는 암호기술, 특히 양자암호의 진전에 따른 DLT 시스템 전환을 포함한다. 이들을 기반으로 하여 현재 진행 중인 분산원장기술 응용을 위한 표준 외에도 다양한 응용을 위한 보안 표준이 진행될 것이고, 이러한 표준들에서 사용된 용어 정의는 별도의 표준으로 다른 SG에서 관리될 수 있다. 아래 그림 3은 Q14의 분산원장기술 보안 표준화 로드맵을 나타낸 그림이고 향후 검토될 수 있는 표준은 흰색 박스, 현재 진행 중인 표준은 박스 안에 작은 푸른색 네모로 진척 상황이 표시되어 있다. 완전히 개발되어 발표된 표준은 푸른 박스로 표시된다.

그림 4 Q14의 분산원장기술 보안 표준화 로드맵

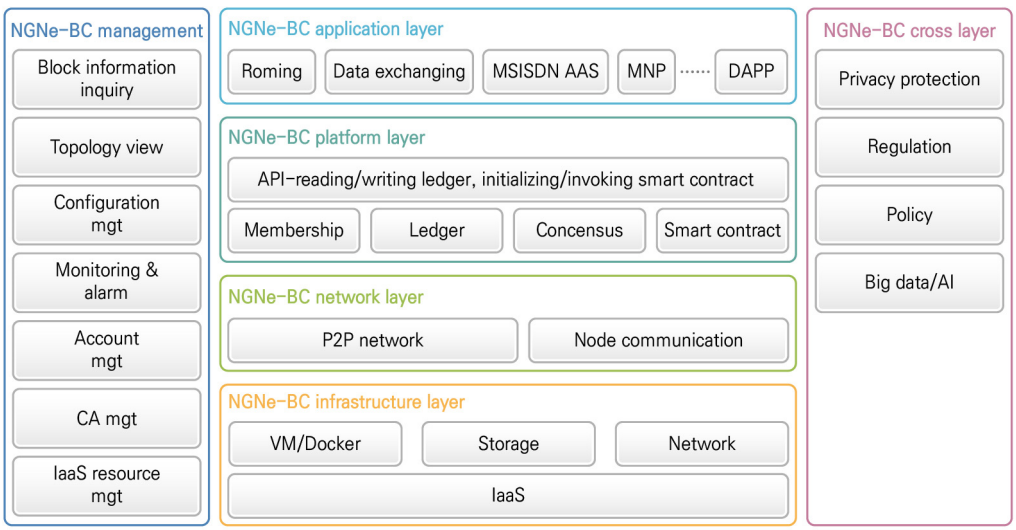


3. 여타 SG의 블록체인 표준화

가. SG 13에서의 블록체인 표준화

SG 13은 IMT 2020, 클라우드 컴퓨팅 및 신뢰 네트워크 인프라에 초점을 둔 미래 네트워크 연구반이다. SG 13에서는 분산원장기술 관련 2개의 표준을 개발하고 있다. Y.NGNe-BC-reqts, 차세대 네트워크에서의 블록체인 시나리오 및 능력 요구사항(Scenarios and capability requirements of blockchain in next generation network evolution)과 Y.BaaS-reqts, 클라우드 컴퓨팅 - 서비스 형태로 제공되는 블록체인 기능 요구사항(Cloud computing - Functional requirements for blockchain as a service)이 그것이다. 아래 그림 5는 차세대 네트워크에서의 블록체인 프레임워크를 보여주고 있다.

그림 5 NGNe-BC 프레임워크



나. SG 16에서의 블록체인 표준화

SG 16은 멀티미디어 관련 표준을 개발하는 연구반으로서 F.DLS, DLT서비스의 요구사항 및 능력(Requirements and Capabilities of Decentralized Ledger Services)이라는 표준을 개발하고 있다.

다. SG 20에서의 블록체인 표준화

SG 20은 IoT와 스마트 시티 및 커뮤니티에 관한 표준을 개발하는 연구반이다. SG 20에서는 Y.IoT-BoT-fw, 분산 서비스 플랫폼으로서의 사물 블록체인 프레임워크(Framework of Blockchain of Things as Decentralized Service Platform) 표준을 개발하고 있다. 또한 2018년 5월에는 Y.DEC-IOT-ARCH, 정보 중심 네트워크 및 블록체인에 기반한 분산 IoT 통신 아키텍처(Decentralized IoT Communication Architecture based on Information Centric Networking and Blockchain) 표준 개발을 개시하였다. SG 20은 산하에 IoT 데이터 처리 관리를 위한 포커스 그룹(FG-DPM)의 WG 3 “데이터 공유, 상호운용성 및 블록

체인"(Data Sharing, Interoperability and Blockchin)에서는 IoT-BC-overview, IoT와 블록체인 개요(Overview of IoT and Blockchain)라는 보고서를 개발하기 위한 작업을 수행하고 있다.

라. SG 5

SG 5는 신규 표준화 항목은 없다. 그러나 SG 5 산하 연구과제(Question) Q6가 수행해야 할 업무 내용을 개정하면서 블록체인을 포함하였다. 이에 따라 향후 블록체인 관련 연구가 진행될 수 있을 것으로 예상된다.

4. ITU-T 산하 포커스 그룹 활동

가. FG-DLT 활동

FG-DLT(Focus Group on Applications of DLT)는 분산원장기술 기반의 응용 및 서비스를 식별·분석하고, 이러한 응용 및 서비스가 국제적 규모로 구현되는 것을 지원하기 위한 최적 실무 및 지침을 작성하며 ITU-T 내 연구반에 표준화 작업 관련된 진행 방향을 제안할 목적으로 만들어졌다.

이를 위하여 FG-DLT는 ITU 및 타 표준 개발 기관, 포럼 등에서 진행되는 활동을 고려하여 상호운용이 가능한 분산원장기술 기반 서비스의 표준화 로드맵을 개발하고 ITU 회원국의 국가 정책 입안자 및 규제 기관에서 사용할 수 있는 규제 툴킷을 개발한다.

FG-DLT의 구체적인 목표는 1) 분산원장기술 관련 표준화 활동에 기여할 수 있는 타 기관과 연락 관계를 수립, 2) 분산원장기술 기반의 응용 및 서비스를 위한 생태계와 그 생태계 내 이해관계자들의 역할과 책임 식별, 3) 분산원장기술 기반 응용 및 서비스 구현의 성공적 활용 사례 식별, 4) ITU-T 연구반들을 위한 연구 아이템과 관련 활동을 제안하는 것이다.

FG-DLT는 2020년 4월까지 한시적으로 운영되는 조직으로 지금까지 2번의

회의를 진행하였다. 1차 회의에서는 작업반 구조를 확정하고 목표 산출물을 설정하였으며, 2차의 회의에서는 각 작업반 별로 산출물을 작성하고 있다. FG-DLT의 구조와 목표 산출물은 아래 표 3과 같다.

표 3 ITU-T FG-DLT 작업반 별 산출물

WG	Title	Deliverables	
1	State of the Art: Ecosystem, Terms, Definitions, Concepts	D1.1	Terms & Definitions
		D1.2	Overview, Concepts, Ecosystem
		D1.3	Standardization landscape
2	Applications & Services	D2.1	Horizontal Applications &Services (e.g., data usage control, identity management, security)
		D2.2	Vertical Applications &Services (e.g., telco, fintech, supply chain, energy)
3	Technology Reference Framework	D3.1	Architectural aspects and reference framework
		D3.2	Overview of existing platforms and mapping to reference framework
		D3.3	Platform assessment criteria and methods
4	Policy Reference Framework	D4.1	Policy and regulatory dimensions and constraints for adoption of DLT-based applications
		D4.2	Mapping of existing DLT platforms to policy and regulatory dimensions and constraints, and assessment criteria
5	Standardization Roadmap	To Be Discussed	

FG-DLT의 결과물은 보고서로 발표될 것이며 표준화가 필요한 경우 ITU-T의 적절한 SG에서 FG-DLT의 결과물에 기초하여 표준을 개발할 것이다. 한편 FG-DLT는 2018년 10월 회의에서 표준화 로드맵과 FG-DLT 연장 여부를 포함하는 향후 계획을 개발할 예정이다.

나. FG-DFC 활동

디지털 법정 화폐(Digital Fiat Currency, DFC)란 중앙은행이 발행하는 디지털 화폐를 말한다. 이미 남태평양의 마셜공화국은 가상통화를 법정화폐로

사용하는 법을 통과시켰다. 미국, 영국, 중국 등도 디지털 법정 화폐 발행을 고려하고 있다고 발표한 바 있으며 특히 아프리카 등의 개발도상국이 화폐 관리의 비용을 절감하기 위해 FG-DFC의 수립을 강력히 지지하였다.

FG-DFC(Focus Group on Digital currency including Digital Fiat Currency)는 DFC에 관한 보안, 상호운용성, 위조 예방 및 소비자 보호/수용의 핵심 문제를 다루기 위한 것이다. 여기에는 분산원장기술만이 아닌 다양한 기술에 기초한 모바일 화폐를 포함하는 것을 목표로 하고 있다.

FG-DFC의 목표는 DFC의 도입에 따르는 경제적 효익과 영향을 연구하는 것으로 1) 금융 포용성(Finance Inclusion) 제고를 위한 디지털 법정화폐 생태계 조사, 2) 네트워크 참조 아키텍처(Reference Architecture)[2]의 기능과 DFC 구현 및 상호운용을 위한 기존 지불 시스템과의 통합에 필요한 프로세스 구성 요소를 매핑하고 3) 활용 사례, 요구사항 및 응용, 식별, 4) DFC 관련 보안, 규제, 소비자 보호, 부정 방지 및 위조 현안 및 대응에 대한 이해 심화, 5) 법정화폐 관련 국가 주권(Sovereignty) 보안, 투명성 및 검증 가능성을 식별하고 신뢰 보장을 위해 핵심 소프트웨어 및 하드웨어의 임치(Escrow)[3] 지침 제공, 6) 이를 통해 ITU-T의 표준화를 위한 신규 영역을 식별하는 것이다.

FG-DFC는 2년을 기한으로 작업을 진행하고 있으나 필요한 경우 연장될 수 있다. FG-DFC의 작업반과 산출물은 표 4와 같다.

표 4 ITU-T FG-DFC 작업반 별 산출물

WG	Title	Deliverables	
1	Regulatory and economic aspects	1	Repository on digital currency regulatory issues
		2	Regulatory framework
		3	Economic impact issues for digital currency

2) 네트워크를 구성하기 위해 필요한 기본적인 기능 및 기술적 설계와 관련된 정보를 간결하고 포괄적으로 나타낸 프레임워크(Framework)

3) 제조사 도산 등을 대비하여 소스코드 등을 제3의 기관에 위탁 보관하는 것

WG	Title		Deliverables
2	Ecosystem and reference architecture	1	Report on definitions and taxonomy for digital fiat currency
		2	Report on digital fiat currency ecosystem
		3	Report on interoperability scenarios for DFC implementation
		4	Report on use cases for digital fiat currency and integration framework with existing payment systems for interoperability and consumer protection
3	Security	1	Security architecture and reference model
		2	ICT security and governance reference model
		3	Use cases for big Data Analytics

다. FG-DPM 활동

ITU-T 산하에는 블록체인 관련 항목을 다루는 FG가 하나 더 있는데, IoT 및 스마트 시티를 지원하기 위한 데이터 처리와 관리에 관한 그룹인 FG-DPM(Focus Group on Data Processing and Management to support IoT and Smart Cities and Communities)이 그것이다. 이 FG는 IoT 및 스마트 시티 커뮤니티(SC&C)에 관한 표준화 그룹인 SG 20 산하에 수립되었으며 올 7월에 1차 회의를 거쳐 5개의 WG을 수립하였다. 이 중 WG 3 "데이터 공유, 상호운용성 및 블록체인(Data Sharing, Interoperability and Blockchain)"에서 블록체인 관련 연구를 수행하고 있다. FG-DPM WG3에서 개발 중인 블록체인 관련 산출물은 표 5와 같다.

표 5 ITU-T FG-DPM WG 3 블록체인 관련 산출물

Deliverables		Title of output document
D3.5	Overview of IoT and Blockchain	Draft Technical Specifications TS.IoT-BC-overview "Overview of IoT and Blockchain"
D3.6	Bockchain-based Data Exchange and Sharing Technology	Draft Technical Specifications "Blockchain-based data exchange and sharing technology"
D3.7	Using blockchain to improve data management	Draft Technical Specifications TR.IoT-BC-DM "Blockchain Based Data Management"

Ⅳ 사실 표준화 기구[4]에서의 블록체인 표준화 현황

1. W3C의 블록체인 관련 활동

가. 자기-주권적 신원(Self-sovereign identity)

W3C의 작업반 중 증명 가능한 주장(Verifiable claims) 작업반에서는 2017년 6월 증명 가능한 주장(Verifiable Claims)/크리덴셜 활용사례 TR을, 이어서 2017년 8월에는 증명 가능한 주장/크리덴셜 데이터 모델 및 표현 TR을 개발하였다.

활용사례는 실 사용자가 자기 주권적 신원을 주장하고자 할 때 이를 처리할 수 있는 환경과 구체적인 시나리오를 표현한다. 이 문서에서는 이를 제공할 수 있는 아키텍처를 정의하지는 않았다. 그러나 다음 발행된 데이터 모델 및 표현에서는 식별자 저장소로써 분산원장을 예로 제시하였다.

이러한 '증명 가능한 주장'은 자기 주권적 신원의 핵심이며 오프라인 신원에 비해 온라인 신원이 가지는 문제점을 블록체인이 제공하는 분산 및 암호를 이용해 해결할 수 있다. 증명 가능한 주장 작업반에서는 지속적으로 관련 이슈를 검토 개선하고 있다.

나. 기타 커뮤니티 활동

W3C에서는 표준을 개발하는 작업반(Working Group)은 검토 승인이 필요하지만, 관련 연구를 수행하는 커뮤니티는 완전히 참가자의 자율로 구성할 수 있다. 이러한 커뮤니티 그룹의 결과물은 보고서 형태로 그룹장이 발표할 수 있다. 현재 다수의 이러한 블록체인 관련 커뮤니티 그룹이 활동하고 있다. 블록체인 커뮤니티 그룹, 블록체인 디지털 자산 커뮤니티 그룹, 체인포인트 커뮤니티 그룹, 인터레저(Interledger) 지불 커뮤니티 그룹 등이 활동 중이며, 2018년

4) 공적 표준화 기구인 ISO, IEC, ITU-T 등과 대조적으로 업계를 중심으로 결성된 표준화 기구. IEEE, IETF, W3C 등이 대표적이다.

5월 30일에 스마트 계약 커뮤니티 그룹이 새로 생겼다. 앞서 언급했듯이 커뮤니티 그룹은 매우 자율적으로 만들어 질 수 있어 이후에도 다수의 커뮤니티 그룹이 생성될 수 있으며, 블록체인을 전면에 내세우지 않았지만 관련 연구를 수행할 수도 있다.

2. IEEE의 블록체인 표준화

가. P2418, 사물인터넷에서의 블록체인 이용 프레임워크 표준

IEEE 표준 연합 (Standards Association)에서는 블록체인 워킹 그룹을 수립하고 P2418 사물인터넷에서의 블록체인 이용 프레임워크(Framework of Blockchain Use in Internet of Things) 표준을 개시하였다.

이 표준은 IoT 응용 내에서 블록체인의 이용, 구현 및 상호작용에 대한 일반적인 프레임워크를 제공하는 것을 범위로 한다. 또한 IoT 내에서 블록체인에 관련된 확장성, 보안 및 프라이버시 문제를 다룬다. 이 프레임워크는 블록체인 토큰, 스마트 계약, 트랜잭션, 자산, 크리덴셜 네트워크, 허가형 및 공개형 IoT 블록체인을 포함한다. 이 표준은 2020년 10월 완료 예정이다.

IEEE는 또한 2018년 5월 “블록체인 시스템을 위한 데이터 포맷(Data Format for Blockchain Systems) 작업반을 구성하고 P2418.2 블록체인 시스템을 위한 표준 데이터 포맷(Standard Data Format for Blockchain Systems)을 개발하기로 승인하였다. 이에 따라 기존의 P2418은 P2418.1로 번호가 변경되었다.

V 향후 표준화 전망 및 국내 금융 표준화 대응 방향

1. 향후 표준화 전망

앞으로는 가상통화를 포함하는 토큰 관련 표준들과 공급망 관련 실무 운영을 위한 표준들, 다양한 응용들과 이에 관련된 스마트 계약, 그리고 이들의 상호

운용성을 위한 거버넌스에서 시작하여 인터페이스에 이르는 표준 등이 개발될 것이다. 기능이든 보안이든 요구사항 관련 표준들이 만들어지면 그 요구사항을 만족하기 위한 솔루션에 대한 표준들이 나오고, 이들을 평가하기 위한 표준에 대한 요구도 높아질 것이다. 이러한 표준들은 시장에 미치는 영향이 크므로 표준들이 개발되어 나올 때까지 기다렸다가 대응하기 보다는 기술 개발을 통해 주도적으로 참여할 필요가 있다.

한편 현황에서 볼 수 있듯이 표준화 기구 간에 표준화 대상이 조금씩 겹쳐지는 모습이 보이고 있다. W3C의 자기 주권적 신원은 기술 보고서 수준에서 만들어져서 타 표준화 기구에서 이를 고려한 표준 개발에 활용하고자 많은 논의가 이루어지고 있다. ISO의 연구반과 ITU-T의 FG의 작업 영역은 기존의 타 표준화 기구의 표준화 영역과 중복되는 부분이 많으나 이들은 주로 현황에 대한 분석 보고서 형태의 결과물을 개발하고 있으므로 이것을 표준 상의 문제로 보지는 않고 있다. 그러나 ITU-T SG 20의 Y.IoT-BoT-fw와 IEEE의 P2418, SG 17의 X.sct-dlt와 SG 16의 F.DLS의 경우 표준의 제목과 범위에 유사점이 커서 앞으로 표준 개발이 진행되면서 불일치나 노력의 중복이 발생되지 않도록 기구 간 상호 협력이 필요하다.

2. 국내 표준화 전망

국내에서는 금융보안원의 금융보안표준화협의회의 블록체인 분과를 통해 금융권 공통 블록체인 표준이 개발되고 있다. 이들 중 금융권 공통 블록체인 플랫폼 표준은 분산원장시스템 설계의 기본 틀을 제공하는 ISO 23257 참조 아키텍처와 매우 밀접하게 연관되어 있으며, 금융권 보안 요구사항은 ITU-T X.strdlt와 관련이 있다. 금융권 인증서 공동 활용을 위한 상호운용 방안도 고려되고 있다.

한편 국내에서도 거래소에 대한 규제 필요성이 강력히 제기되고 있어 TC 307 WG 2에서 새로 시작하는 디지털 자산 보관자의 보안 기술보고서가 좋은 참조로 활용될 수 있을 것이다. 또한 SG 07에서 새로 진행되는 토큰 등 다양한 자산에

관련된 상호운용성 연구는 향후 금융뿐만 아니라 각종 분산원장기술의 연계 서비스를 위해 필수적일 것이다.

VI 결 론

지금까지 분산원장기술에 관한 국제 표준화 현황을 살펴보았다. 국제 표준화 기구 중 가장 활발하게 활동하고 있는 것은 ISO TC 307과 ITU-T SG 17이다. TC 307은 분산원장기술 전반에 걸쳐 표준화를 수행하고 있고 ITU-T SG 17은 분산원장기술 보안 표준화에 집중하고 있다.

TC 307에서는 토대가 되는 용어, 참조 아키텍처 작업이 상당히 진행되어 왔으며 앞으로는 이를 기초로 보안, 스마트 계약 및 상호운용성 등으로 표준을 확장할 것으로 예상된다. 향후 ISO에서의 분산원장기술 관련 보안 표준화는 JWG 1을 통해 TC 307과 IT 보안기술 표준화를 담당하는 ISO/IEC JTC 1/SC 27과 공동 작업이 진행될 것이다. 한편 ITU-T에서는 SG 17 Q14를 중심으로 보안 프레임 워크부터 시작하여 보안 평가 및 다양한 응용시스템의 보안 표준들을 개발하고 있다. 또한 ITU-T 내의 다른 SG에서는 각기 중심 테마로 삼고 있는 클라우드, IoT 등 각 분야에서의 분산원장기술 활용을 위한 표준들을 개발하고 있다.

분산원장기술은 글로벌 인프라를 위한 기술이다. 국내의 금융권 표준이 만들어진다 해도 이것이 국제 분산원장네트워크에 연동되지 못한다면 큰 의미가 없어질 것이다. 글로벌 분산원장 네트워크에 연결하고 더 나아가 이를 통해 열리는 시장을 선점하기 위해서는 표준 개발 초기부터 이해관계자들이 참여하여 우리의 요구를 국제 표준에 반영할 필요가 있다. 올해 출범한 분산원장기술표준포럼에서는 이러한 국제 표준화 동향을 소개하고 개발 중인 표준안을 함께 검토하고 한국의 의견을 기고하기 위한 연구를 진행하고자 한다. 관심 있는 분들의 많은 참여를 바란다.

참고문헌

[1] World Economic Forum, Blockchain 4th industrial revolution Summary, https://toplink.weforum.org/knowledge/insight/a1Gb00000038qmPEAQ/explore/summary

[2] ISO, ISO-TC307_N0001_N0001_TMB_Resolutions_-_67_TMB_Meeting_Resol, 2016

[3] ITU-T, Report of the second meeting of Study Group 17 (Geneva, 29 August - 6 September 2017) https://www.itu.int/md/T17-SG17-R-0010/en, 2017

[4] ISO, ISO-TC307_N0194_TC307_Meeting_02_Resolutions_Final, 2017

[5] ISO, ISO-TC307_N0300_ISO_TC_307_-_Meeting_03_Resolutions_-_London_-_May_2018, 2018

[6] The new york times, “Blockchain will be theirs, Russian spy boasted at conference”, 2018. 04 29. https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html

[7] 정보보호학회지, 블록체인 국제 표준화 현황 오경희, 2017년 10월

[8] ITU-T SG 17 Q14, https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17&q=14

[9] ITU-T Focus Group on Application of Distributed Ledger Technology, https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[10] Focus Group on Digital Currency including Digital Fiat Currency, https://www.itu.int/en/ITU-T/focusgroups/dfc/Pages/default.aspx

[11] Focus Group on Data processing and management to support IoT and Smart Cities & Communities
https://www.itu.int/en/ITU-T/focusgroups/dpm/Pages/default.aspx

[12] W3C Verifiable Claims Working Group https://www.w3.org/2017/vc/WG/

[13] W3C Current groups https://www.w3.org/community/groups/

[14] IEEE, IEEE project 2418.1 - Standard for the Framework of blockchain use in Internet of Things,
http://standards.ieee.org/develop/project/2418.1.html

[15] IEEE, IEEE project 2418.2 - Standard data format for blockchain systems
http://standards.ieee.org/develop/project/2418.2.html

신용카드 직승인 가맹점 개념과 동향

박 해 철*

* TMX KOREA 대표이사, hcpark@tmxkorea.com

요 약

국내 신용카드 오프라인 거래는 해외와 달리 발급사와 매입사가 구분되지 않아, 가맹점과 카드사 사이에서 거래를 중계 처리하는 VAN사가 발전하였다. 그리고 현재 결제 시장 보안 강화를 위해 IC(Integrated Circuit)거래를 의무화하는 정책이 곧 시행될 예정이다.

최근 자영업자의 증가와 영세상인 보호 관점에서 가맹점 수수료를 인하하는 추세가 강화되고 있고 카드업계는 이를 위해 VAN사를 거치지 않는 직승인 방식을 확산하고 있다. 그러나 직승인 거래를 위해서는 VAN사가 담당하고 있는 IC거래 보안 환경을 카드사와 가맹점이 직접 구현해야 하는 이슈가 발생했다.

카드업계는 대형 가맹점 대상으로 직승인 거래 보안 기술 기준을 마련하여 대상 가맹점을 점차 확대 중이며, 현재는 중소형 가맹점까지 적용하기 위한 기술 기준을 마련하고 있다. 직승인 가맹점이 중소형까지 확산되려면 보안성이 확보된 오픈망 기반의 기술 기준 제정이 우선 필요하고, 이 밖에 필요한 과제들이 하나씩 해결되어야 할 것이다.

본고에서는 신용카드 오프라인 가맹점 시장의 구조와 보안 정책을 우선 살펴보고, 이를 통해 직승인 가맹점이 탄생한 배경과 개념, 향후 확대를 위해 필요한 보안 과제 등을 다뤄보고자 한다.

02 신용카드 직승인 가맹점 개념과 동향

I 서 론

국내 신용카드 시장은 가맹점 수수료 인하 정책으로 인해 많은 변화가 발생하고 있다. 그동안 성장 일변도의 시장이 성숙기에 접어들면서 적정 수수료에 대한 사회적 검토가 본격적으로 진행되고 있으며, 최근에는 높은 자영업자 비율로 영세상인 보호가 중요한 사회적 과제로 인식되면서 수수료 인하는 시장의 분명한 흐름이 되고 있다.

가맹점 수수료 인하로 카드사는 수익 구조가 약해질 수밖에 없으며, 이 충격을 최소화하기 위한 다양한 전략들이 검토·시행되고 있다. 그 전략의 일환으로, 가맹점과 카드사가 직접 거래를 처리하여 중계 사업자인 VAN사에게 지급하는 수수료를 절감하는 직승인 가맹점 방식이 본격적으로 확대되고 있다.

본고에서는 국내외 신용카드 오프라인 가맹점 시장의 구조와 관련 보안 정책을 우선 살펴보고, 이를 통해 직승인 가맹점이 탄생한 배경과 개념, 향후 확대를 위해 필요한 기술 및 보안 과제 등을 다뤄보고자 한다.

Ⅱ 신용카드 오프라인 가맹점 시장 현황

1. 국내 신용카드 오프라인 거래

가. 시장 및 거래 구조

신용카드 시장은 일반적으로 카드 회원, 카드 가맹점, 카드를 발급하고 거래를 승인하는 발급사, 가맹점의 거래 전표를 매입(카드 대금 지급)하는 매입사의 4당사자 구조이다. 그러나 국내 신용카드 시장은 발급사와 매입사가 구분되어 있는 해외와 달리 발급과 매입을 '카드사'가 모두 처리하는 3당사자 구조이다.

국내가 3당사자 구조로 발전한 것에는 여러 요인이 있겠지만, 90년대부터 정부 차원의 신용카드 사용 장려로 시장이 급속도로 성장하면서 가맹점 모집 및 인프라 보급이 비교적 쉽고 빠른 속도로 진행되었기 때문으로 생각된다.

카드사가 발급과 매입을 모두 수행하였지만, 치열한 경쟁 하에 회원 유치에 더 집중하면서 가맹점 관련 업무와 거래 데이터 중계 업무는 VAN(Value Added Network, 부가가치통신망)社에게 위탁하였다. 가맹점은 카드 사용 의무화 등으로 카드사가 노력하지 않아도 자연히 증가가 되었고, 특정 카드만 받도록 독점할 수도 없는 구조였기 때문에 제3자 위탁의 형태가 더 효율적인 상황이었다.

VAN사가 가맹점 업무와 거래 네트워크를 담당하면서 3당사자 체제의 단점인 가맹점 확장의 제약성이 제거되었고 다수의 카드사들이 가맹점을 공동으로 사용할 수 있는 환경이 조성되었다. 결과적으로 VAN사가 매입사의 역할을 부분적으로 수행하는 형태의 3당사자 구조로, 해외와는 다른 형태의 카드 시장이 만들어지게 되었다.

나. VAN사의 역할

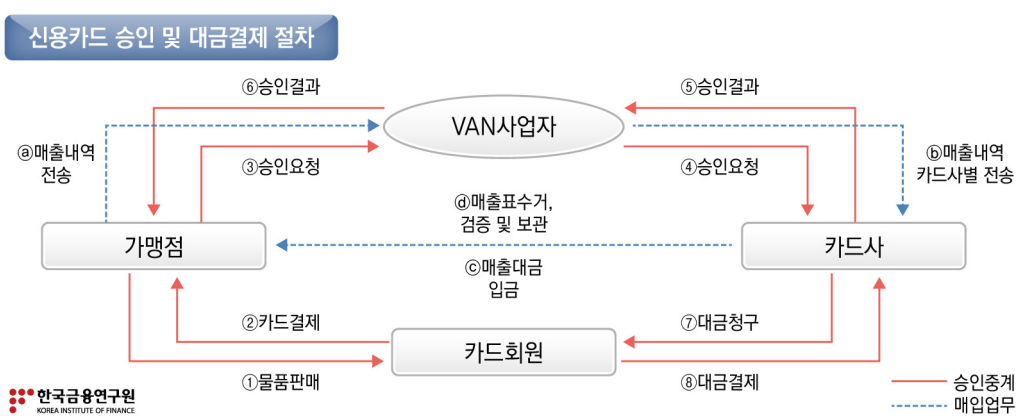
VAN 사업자를 더욱 세부적으로 구분하면 가맹점과 카드사간의 데이터 중계 인프라를 담당하는 VAN사와, VAN사 하위에서 가맹점을 실질적으로 영업, 관리

하고 1차 CS(Customer Service)까지 담당하는 VAN 대리점으로 구분된다. 소상공인이 점포를 열었을 때 신용카드 가맹점에 가입하는 업무를 처리하고, 카드 단말기를 제공하며, 카드 전표를 수거하여 카드사에 전달하는 등의 모든 업무는 대부분 VAN사와 VAN 대리점이 수행하고 있다. 이렇게 가맹점과 관련된 업무를 VAN사가 전담하게 되면서 카드사는 가맹점에 제공해야 할 업무나 인프라 등을 VAN사에 상당 부분 의존할 수밖에 없는 구조가 되었다.

신용카드 거래 규모가 폭발적으로 성장하면서 VAN사도 다수 설립되었고 가맹점 확보 경쟁이 치열하게 발생함에 따라, VAN사는 확보한 가맹점을 유지할 수 있는 공격적인 영업 정책을 실행하기 시작했다. 대형 가맹점에는 카드 수수료의 일부를 보전해주는 리베이트를 지급하기도 했고, 중소형 가맹점에는 카드 결제에 필요한 제반 장비(POS, 단말기, 서명패드 등)를 무상으로 제공하면서 약정 계약을 체결하는 것이 일반적인 영업 형태로 고착화 되었다.

한편 신용카드가 가맹점에 미치는 여러 가지 순기능에도 불구하고, 우리나라는 카드 결제 의무화와 상대적으로 높은 수수료로 인해 가맹점주들에게 카드결제는 부담스런 결제 수단으로 인식되고 있다. 이러한 가맹점주들의 불만은 VAN사의 가맹점 관리와 영업 정책 때문에 일정 부분 상쇄되는 측면도 있었지만 높은 수수료에 대한 근본적인 해결책은 되지 못했다.

그림 1 신용카드 거래 절차 (VAN사 역할)



2. 해외 신용카드 오프라인 거래

가. 해외 카드시장 구조

해외 카드시장은 국가별, 사업자별로 다양한 형태가 존재하고 있으나 일반적으로 4당사자 구조로 형성되어 있다. 카드를 발급하고 거래를 승인하는 발급사와 가맹점을 관리하고 매입을 수행하는 매입사가 구분되어 있고 두 사업자를 비자, 마스터카드와 같은 국제 브랜드 네트워크가 연결해 주고 있다. 물론 매입사 아래에는 우리나라의 VAN 대리점 역할을 하는 현장 영업 조직이 존재하나, 역할이나 존재감이 국내보다는 떨어진다고 볼 수 있다.

매입사가 가맹점을 영업하고 관리하기 때문에 카드 가맹점에 가입하면 국내처럼 한 번에 모든 카드사와 연결되는 것이 아니라 특정 카드만 결제되기도 하고, 이를 해결하기 위해 카드 단말기를 여러 대 설치하는 가맹점 형태도 다수 보이고 있다.

다만, 해외 카드 시장은 우리나라처럼 급속한 성장이나 치열한 경쟁의 과정이 상대적으로 덜해서인지 POS, 결제 단말기 등을 매입사가 무상 제공하기 보다는 가맹점이 구매하거나 대여하는 경우가 일반적이다. 이는 어느 VAN사를 이용하던 큰 차이가 없어 장비 제공 대신 약정으로 가맹점의 이탈을 방지 하고 있는 국내 시장과는 확연히 다른 차이점이다.

관련된 업무나 장비를 VAN사가 다 알아서 처리해주는 국내 상황이 가맹점주 입장에서 편리할 수도 있으나, 다양한 영업 상황이나 환경을 고려하여 유연하게 대응하기에는 한계가 있다.

일례로 해외에는 POS의 형태가 스마트기기의 발전에 따라 다양한 형태로 구현되고 있다. 그리고 가맹점주가 전용 POS 장비를 구매하지 않고 이미 보유한 PC나 스마트폰에 설치하는 소프트웨어 형태의 POS 사업도 성행하고 있으나 국내는 이러한 움직임이 미미한 실정이다. VAN사가 지급하는 장비에 가맹점의 의존도가 지나치게 높기 때문이다.

3. 신용카드 거래 보안 정책 및 현황

가. 오프라인 거래 보안을 위한 해외 IC칩 전환 추진

오프라인 거래와 관련한 신용카드의 보안은 IC칩의 도입이 가장 강력하고 현실적인 방안으로 마련되어 전세계적으로 진행되고 있다. 수 십 년간 카드 정보를 저장하고 카드 단말기로 전달하던 방식인 자기띠(마그네틱 스트라이프, MS)는 카드정보의 불법 취득과 복제가 너무나 간단하기 때문에 보안 수준이 가장 높은 하드웨어인 IC칩을 이용하여 보안을 확보하는 것이다. 이를 위해서는 카드는 물론 가맹점 단말기도 IC칩을 처리할 수 있도록 전환되어야 한다. 그래서 발급사와 매입사가 구분되듯 IC칩 전환도 카드와 단말기로 구분될 수 있다.

엄청난 비용이 수반되는 IC칩 전환의 효과가 강력하게 작용하기 위해서는 카드에서 자기띠를 완전히 제거해야 한다. 그러나 국가별로 전환 속도가 다르고 각 국 로컬 시장에서도 가맹점의 IC칩 전환율이 완벽히 진행되지 않기 때문에 대부분의 카드가 IC칩과 자기띠를 함께 장착하고 있다.

이러한 제한적인 환경에서도 전환 효과를 극대화하기 위해 국제 브랜드사들은 IC카드와 IC 단말기 간의 거래는 IC로 우선 처리되는 정책을 마련하였다. 결과적으로 IC가 장착된 카드의 자기띠에서 카드정보를 추출하여 마그네틱 카드 형태로 복제하여도 IC 단말기에서는 거래가 안 되게 정책적으로 막은 것이다. 그리고 IC로 전환되지 않은 카드 또는 단말기에서 발생하는 거래에 대해서는 해당 발급사와 매입사에 페널티 수수료를 적용하고, 사고 발생 시 책임을 지게하는 정책으로 회원사들의 IC칩 전환을 유도하고 있다.

무엇보다도 IC전환이 주변 국가들보다 늦게 되면, 카드 불법 복제와 관련된 국제 범죄 조직의 타겟 국가가 될 수 있다는 것이 가장 문제이다. 가맹점들이 대부분 마그네틱 단말기만 보유한 국가가 있다면 해외에서 카드를 복제하여 해당 국가에 가서 불법 거래(도둑 결제)를 시도하는 것이다. 결과적으로 거래와 연결된 금융사는 사고가 발생하여도 앞서 설명한 국제 브랜드사의 정책 때문에 손해배상 책임을 질 수 밖에 없어 피해가 막대해 질 것이다.

나. 국내 IC카드 발급 의무화

이러한 IC칩 전환이 국내에서는 2013년부터 IC카드 의무 발급 정책으로 본격적으로 시작되었다. 기존에 발급된 카드의 사용은 허용하되, 신규로 발급되는 카드는 모두 IC카드로 의무 발급하게 된 것이다. 기존에는 특수 목적이나 국제 브랜드사의 지원 등으로 일부 상품에만 적용하여 발급하던 IC카드를 전면적으로 발급하면서, 약 5년이 지난 현재는 자기띠만 장착된 신용카드는 거의 찾아볼 수 없다.

시행 과정에서 여러 가지 이슈가 발생하긴 하였으나, IC카드 발급은 발급사만 통제하면 되므로 IC 단말기보다는 비교적 추진이 용이하다. 다만 당연하게도 카드 단말기의 IC 전환이 없이 카드만 전환되면 보안에 아무런 효과가 없어 비용만 낭비하게 된다.

다. 국내 IC 단말기 의무화

이에 금융당국은 2014년 여신전문금융업법을 개정해 모든 신용카드 가맹점이 IC 단말기를 도입하도록 의무화했다. 이는 2014년 초 신용카드 정보유출사건이 발생하자 IC 단말기로 전환해 카드회원의 정보 보호를 강화하겠다는 취지였다. 하지만 당시 중소 가맹점주들이 새로운 카드단말기 도입비가 부담된다고 반발하자 3년간 유예기간을 부여했으며 이제 유예기간이 종료되어 모든 신용카드 가맹점은 2018년 7월20일까지 단말기 전환을 완료해야 한다. 이후에도 가맹점들이 마그네틱 전용 단말기를 쓰면 최대 500만원의 과태료를 물게 된다.

IC 단말기 의무화와 관련하여 VAN사가 신용카드 단말기를 금융위원회에 의무적으로 등록하는 제도(여신전문금융업법 제27조의 4, 동법 시행령 제7조의 6)가 생겼으며, 여신금융협회는 이와 관련한 보안 기준인 '신용카드 단말기 정보 보호 기준'을 수립하여 배포하였다. 앞서 설명한 대로 가맹점 단말기는 VAN사가 공급하고 있기 때문에 단말기 인증 및 등록을 VAN사가 담당하도록 법이 제정된 것이다.

여신금융협회가 제정한 정보보호 기술기준의 핵심은 민감한 신용카드 정보(카드번호 유효기간 등)를 단말기가 읽는 단계에서 암호화 하여 카드사 서버까지 E2E(End To End) 암호화를 유지하여 전송하는 것이다. 엄밀히 살펴보면 [단말기 – VAN사 – 카드사] 구간에서 VAN사의 보안키로 암복호화하기 때문에 종단인 카드사까지 암호화 하는 것은 아니다. 그러나 VAN사가 각종 위수탁 업무를 처리하기 위해 카드 정보를 복호화하고, 대신 [VAN사 – 카드사] 구간은 전용선으로 연결되어 있어 광의의 의미로 E2E로 해석할 수 있는 것이다.

아래 표는 신용카드 단말기 정보보호 강화를 위한 기술 기준과 관련하여 각 기관별 역할을 설명한 것이다.

표 1 신용카드 단말기 정보보호 기술 기준 관련 기관별 역할

구분	기관명	주요 내용
정책기관	금융위원회	• 신용카드 단말기 정보보호 관련 제도 마련 및 정책 수립 • 신용카드 단말기 등록 / 관리 지침 고시
위탁기관	여신금융협회	• 신용카드 단말기 등록 및 기술기준에 관한 업무 – 신용카드 단말기 등록 / 관리 절차 마련 및 시행 • 신용카드 단말기 정보보호 기술기준 시험기관 및 인증기관 업무 – 신용카드 단말기 정보보호 기술기준에 따른 시험 및 성적서 발급 – 신용카드 단말기 정보보호 시험결과 인증 및 인증서 발급
의뢰기관	부가통신사업자, 카드리더기 제조업체 등 신용카드 단말기 개발 및 운영 주체	• 신용카드 단말기 정보보호 기술기준에 따른 제품 개발 • 보안 취약점 점검 및 보완 조치
사용기관	신용카드 가맹점 등	• 금융위원회에 등록된 안전한 신용카드 단말기 구축 운영

Ⅲ 직승인 가맹점의 의미 및 동향

1. 가맹점 수수료 인하를 위한 시장 변화

국내 신용카드 시장에서 관련 사업자들의 거의 모든 수익 원천은 가맹점 수수료이다. 해외에서도 가맹점 수수료가 큰 부분을 차지하고는 있으나 국내는 포인트 등의 회원 마케팅 비용, 단말기 무상 보급과 같은 사업자들의 영업 비용까지 대부분 가맹점 수수료로 해결하는 구조이므로 해외와 비교 시 상대적으로 높은 수수료를 유지하는 구조가 되었다.

그러나 자영업자 비중이 점점 증가하고 영세상인 보호 등의 사회적 이슈가 생겨났고 이를 위해 가맹점 수수료의 합리적이고 공정한 재산정이 정부 차원에서 몇 차례에 걸쳐 진행 중에 있다. 가맹점 수수료의 문제점이나 적정성은 이 글의 주제가 아니므로 차치하더라도, 가맹점 수수료 인하는 분명하고 신속하게 진행되고 있는 시장 환경 변화이다.

가맹점 수수료를 인하하면 카드사는 수익이 줄어들 수밖에 없을 것이며, 이러한 시장 변화에 대응하기 위해 카드사가 선택한 방법은 당연히도 비용 절감이다. 비용 절감은 다양한 방법과 분야에서 추진될 수 있는데 가장 직접적인 방법 중의 하나는 카드사의 비용 중 큰 부분을 차지하고 있는 VAN 수수료를 절감하는 것이다. 이에 VAN 수수료 구조를 정액제에서 정율제[1]로 바꾸는 등 비용 절감을 위한 자구책들이 진행되고 있다. 그러나 이는 VAN사의 경영 부담으로 편중될 수 있기 때문에 리베이트를 법으로 금지하여 VAN 시장 정상화를 위한 제반 정책들이 동시에 진행되었다.

또 하나의 비용 절감 방법은 가맹점과 카드사간의 거래 데이터를 직접 송수신하여 VAN 수수료를 원천적으로 절감하는 방법이다. 이를 카드업계에서는 '직승인'

1) 정액제는 결제 금액에 무관하게 결제 건당 같은 수수료를 지급하는 것이고, 정율제는 수수료율을 정해 결제 금액에 따라 수수료가 변동되는 것이다. 이러한 제도는 카드 결제 비중이 매우 높아 소액거래가 빈번한 국내 환경에서는 VAN 수수료가 감소하는 결과로 이어진다.

이라고 부르고 있다. 직승인 거래 방식은 과거에도 일부 적용된 사례가 있으나 가맹점 수수료 인하 추세로 인해 카드사들이 적극적으로 확대하고 있다.

2. 직승인 가맹점 이슈 및 동향

카드 결제와 관련된 가맹점의 거의 모든 장비와 업무를 VAN사가 전담하던 형태의 국내 환경에서 직승인 적용은 가맹점에게 결코 쉽지 않은 과제이다. 직승인 적용 시 카드사의 VAN 비용 절감분이 가맹점 수수료 인하로 연결되기 때문에 가맹점 역시 비용을 절감할 수 있는 대안이 될 수 있으나, 거래 상의 E2E 보안, IC 단말기 정보보호 기준 등 각종 인프라 및 보안 환경을 직접 구현해야 한다.

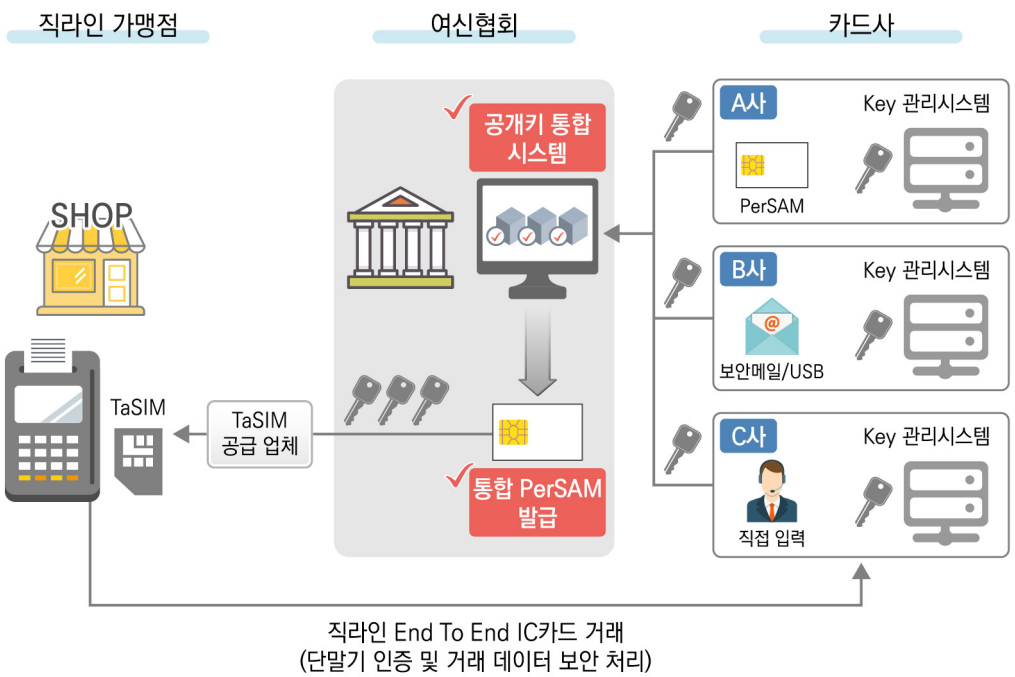
대규모의 거래 건수와 금액이 카드 결제로 처리되는 백화점, 마트 등의 대형 유통회사들은 약간의 가맹점 수수료 인하에도 효과가 크기 때문에 카드사와 공동으로 추진하기 시작했다. E2E 보안을 위해 카드사와 전용선을 연동하고 VAN사가 처리하던 각종 시스템 업무를 자사 서버에 구축하여 직접 운영하고, 연동 카드사를 점차 확대하는 방식으로 진행해 왔다. 그리고 초기 직승인 가맹점들은 시기상 IC 단말기 의무화 정책과 무관하게 구현되었기 때문에 전용선 연동만으로 보안 환경이 대부분 갈음되었고, IC 단말기 전환 정책이 부분적으로 진행되면서 IC거래는 VAN사 중계를 이용하고, 마그네틱 카드는 직승인으로 연동하는 등 상황에 맞춰 거래를 변환 하는 방식으로 운영되었다.

그러나, IC 단말기 전면 의무화가 확정되면서 직승인 가맹점과 카드사는 고민에 빠지게 된다. 직승인으로 처리하던 마그네틱 카드 거래가 아예 금지되기 때문에 IC거래를 직승인으로 처리해야 되는 상황에 놓인 것이다. IC 단말기는 금융위원회 등록을 위해 시험인증을 통과해야 하는데 기존의 기술 기준은 VAN사를 대상으로 한 것이라 직승인 거래가 전혀 고려되지 않았다. 단말기 개발과 시스템 수정을 위한 기술 기준조차 없었던 것이다.

직승인 가맹점 확대가 필요한 카드업계는 오랜 검토와 협의를 거쳐 '직승인(라인) 가맹점 보안처리를 위한 기술 기준'을 2016년 제정하게 된다. 거래 정보의 암호화를

위해 VAN사가 보급한 카드 단말기에는 해당 VAN사의 암호화 키(Key)를 주입하는데, 직승인 가맹점 단말기에는 각 카드사의 키를 모두 주입해야 한다. 이를 어떤 절차와 기술에 따라 구현할지에 대한 기준이 마련된 것이다.

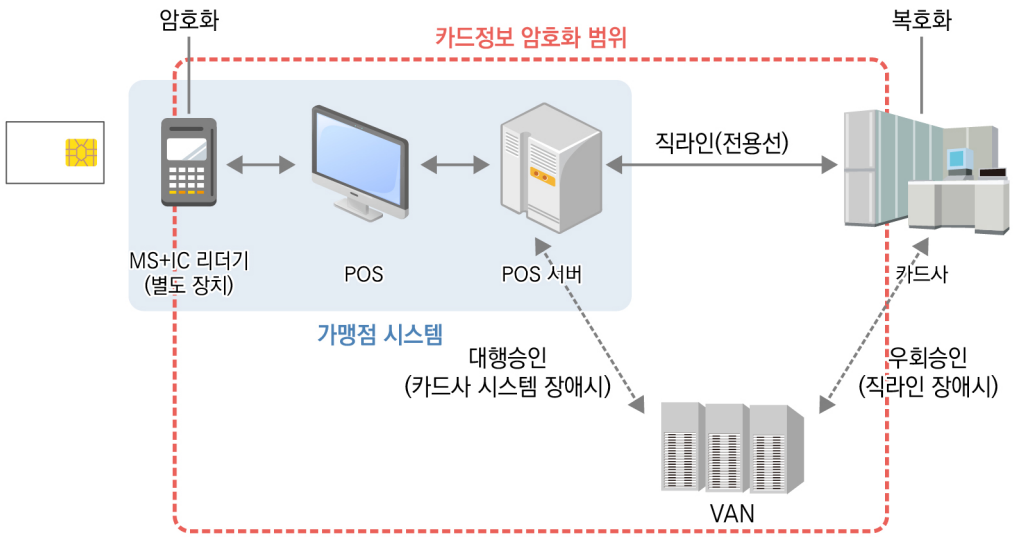
그림 2 직승인(라인) 가맹점 거래 보안 키(Key) 배포 절차



카드사가 생성한 암호화 키는 공개키로 생성되어 여신협회에 안전한 방법으로 전달된다. 여신협회는 이를 보안 매체인 PerSAM(Personalize Security Access Module)[2]카드에 통합 저장하여 가맹점에 전달하게 된다. 가맹점은 전달받은 암호화 키를 TaSIM(Terminal Authentication Subscriber Identification Module)[3] 카드에 옮겨 단말기 슬롯에 장착한다. 이 키를 이용하여 가맹점은 단말기를 카드사에 인증 받고, 이후 IC카드 거래를 수행하게 된다.

2) 암호화 Key 또는 인증용 Serial 번호 등을 안전하게 담아 전달하는 모듈
3) IC단말기를 카드사가 최초 인증할 때 사용되는 SIM 카드 타입의 보안 모듈

그림 3 직승인(라인) 가맹점 거래 보안 구성 및 범위



3. 중소형 가맹점 직승인 도입을 위한 움직임

직승인 가맹점의 IC카드 거래를 구현하기 위해 카드사들은 대형 유통사에 우선 적용하였고, 다음 단계는 중소형 가맹점을 대상으로 한 적용이다. 현재 직승인 보안 기술 기준은 가맹점 서버와 카드사간의 전용선 설치를 기본 전제로 하고 있다. 그러나 중형 유통사나 프랜차이즈 정도의 가맹점이라면 이를 구현할 만한 시스템 인프라와 기술 인력을 보유하기 어려우며, 전용선을 운영하는 비용 또한 만만치 않다. 따라서 일반 개인 사업자의 가맹점은 더더욱 적용이 어려운 상황이다.

이를 해결하기 위해 작년부터 여신금융협회와 금융보안원이 공동으로 신용카드 인프라 표준개발그룹을 만들어 중소형 가맹점에서도 직승인 결제를 구현할 수 있는 기술 기준을 제정 중에 있다. 이 기술 기준의 핵심은 전용선 통신이 아닌 인터넷, 와이파이, 무선통신 등 오픈망을 이용하여 직승인 거래를 구현하는 것이다.

표준개발그룹에서 추진하고 있는 또 하나의 방안은 대형 가맹점 직승인에 적용한 하드웨어 기반의 보안모듈(TaSIM) 외에 소프트웨어 기반의 보안모듈에 대한 기준을 마련하는 것이다. 다만 소프트웨어 기반은 구현 방법이 다양하고 개발 주체에 따라 적용할 수 있는 기술도 여러 가지가 있을 수 있기 때문에 특정

기술을 강제하지 않기 위해 반드시 준수해야 할 보안 기준 정도만 제정하고 있다. 보안이나 결제 관련 개발 회사들이 해당 보안 기준을 만족할 수 있도록 소프트웨어 솔루션을 개발한다면, 가맹점이나 결제 장비 업체들은 각자의 환경이나 비용 구조에 맞는 방식을 채택할 수 있게 되어 선택의 폭이 넓어질 것이다.

4. 직승인 확산을 위한 보안 과제

전용선 대신 오픈망을 이용하게 되면 그에 따른 보안 확보도 쉽지 않게 된다. 특히 전용선 사용을 전제로 특별히 고려하지 않았던 통신 보안 채널 확보 방안이 중요해지고, POS 등 결제 장비에 대한 취약점 보완도 면밀히 검토해야 한다. 또한, 소프트웨어 기반의 보안모듈 적용은 소프트웨어 관련 보안취약점이 발생하게 되므로 이러한 취약점을 제거하기 위한 보안기준이 제시되어야 하고 소프트웨어 개발사들은 해당 기준을 철저히 준수하여야 한다. 이러한 과제들을 해결하기 위해 중점적으로 검토해야 할 사항들은 다음과 같다.

가. CA 설립 및 운영

기술 기준 제정도 중요하지만 실질적인 시장 도입을 위해서는 통신 보안 채널 운영을 위해 필요한 인증서를 생성 관리하는 CA(Certificate Authority. 인증기관)가 설립되어야 한다. 이 CA를 누가, 어떻게 운영할지에 대한 정책적인 고민도 같이 진행되어야 기술 기준 제정 이후 관련 기관들이 실행에 옮길 수 있을 것이다.

검토 방향에 따라서는 CA의 역할을 조금 더 확대하여 POS에서 카드사와 통신해야 할 각종 부가적인 업무 처리[4]를 중계하는 방안도 검토가 가능할 것으로 보인다. 다만 CA 설립 준비로 전체적인 일정이 지연되는 것을 최대한 막으려면 반드시 필요한 업무를 우선 처리하되 역할의 확장은 단계적으로 진행되어야 할 것이다.

4) 예를 들어, 카드사에서 추가되는 BIN(금융기관별로 부여되는 카드번호 앞 6자리) 정보를 업데이트해야 카드 결제시 어느 카드사인지 확인하여 분기 처리가 가능하다. 일반 거래는 VAN사가 관리를 하나, 직승인의 경우 POS가 카드사 서버에 직접 접속하여 정기적으로 체크해야 하는 업무 등이 있다.

나. 거래(승인) 전문 호환 방안 검토

카드 거래 전문은 각 카드사 별로 기본 포맷은 유사하나 각종 부가 서비스를 처리하기 위해 계속 수정되어 오면서 제각각 다른 형태로 운영되고 있다. VAN사는 카드사별 전문 양식을 지속 관리하기 때문에 POS에서 올라온 거래 전문을 각 카드사에 맞는 형태로 전환 생성하여 처리할 수 있으나, 직승인의 경우에는 POS 단위에서 이러한 전환을 처리해야 한다. 따라서 전체적인 통합은 어렵더라도 부분적인 통합이나 각 카드사에서 호환될 수 있는 범용적인 전문 제정이 필요하다. 이는 모든 카드사들이 참여하여 문제가 발생하지 않도록 꼼꼼히 검토해야 하는 사항이다. 왜냐하면, 한 번 적용된 이후에는 수정하기가 어려운 영역이기 때문이다.

POS 개발사들이 모든 카드사의 전문을 별도로 분석 적용하는 것이 현실적으로 불가능하기 때문에 다른 부분의 기술 기준이 마련되더라도 현행 전문의 수정 없이는 직승인 확산에 있어 큰 걸림돌로 작용할 가능성이 높다.

다. 소프트웨어 보안 솔루션 확보 및 인증 방안 수립

앞서 중소형 가맹점 직승인 기술기준의 특징 중, 소프트웨어 기반의 보안 모듈을 언급했다. 표준 그룹에서 제정한 보안 기준을 충족할 수 있는 솔루션을 개발하기 위해서는 해당 기준이 명확하고 현실적이어야 한다. 해당 솔루션의 시장성이 불명확한 현재 여러 실력 있는 개발사들이 참여하고 경쟁할 수 있으려면 모호한 기술 기준으로는 참여 유도가 어려울 것이다.

또한, 해당 보안 모듈을 테스트하고 인증할 수 있는 체계도 마련해야 한다. 공식적인 인증 절차가 없는 보안 모듈을 실환경에 적용하여 연동할 금융사는 없기 때문이다. 다만, 지금까지 보안성 점검이 진행되던 영역이 아니기 때문에 현재 운영 중인 단말 인증 절차에 통합될 수 있는지, 아니면 적절한 기관이 있는지에 대한 신중한 조사와 검토가 필요할 것이다.

Ⅳ 결 론

지금까지 신용카드 오프라인 결제 시장의 구조, 보안정책과 가맹점 수수료 인하에 도움이 될 직승인 가맹점 확산 동향 및 필요한 보안 과제까지 살펴보았다.

중소형 가맹점을 위한 직승인 보안 기술 기준이 마련되어도 단기간 안에 영세 가맹점까지 적용되긴 어려울 것이다. 이는 기술, 보안 문제뿐만 아니라 여러 가지 시장 구조 문제나 경제적 효율성까지 종합적으로 검토해야 되는 사안이다. 또한 올해 7월에 시행 예정인 IC 단말기 전면 도입 준비로 카드업계가 매우 분주한 시기를 보내고 있어 직승인 확산에 많은 노력을 기울이지 못하고 있다.

그러나 가맹점 수수료가 전체적으로 낮아지는데 있어 직승인 가맹점의 확산은 크게 도움이 될 것이 확실하므로 그 수혜 대상을 조금씩 늘릴 수 있는 방법을 계속 고민하고 연구하여야 할 것이다.

직승인 방식의 확대는 해외에 비해 다소 획일화 되고 경직된 신용카드 결제 인프라 구조를 변화하여 가맹점의 목적과 상황에 따라 다양한 방식을 선택할 수 있도록 환경을 개선하는 순기능도 있을 것이라 본다. 물론 이러한 변화에는 보안 확보가 반드시 전제가 되어야 하며 본고에서 제시한 보안 과제가 적절히 해결되어야 한다.

참고문헌

[1] 양용현, 방세훈, 윤경수. “신용카드산업의 시장구조 개선 및 중장기적 발전에 관한 연구”. 2013

[2] 신승만, 정남기, 오민홍. “신용카드 수수료 체계의 문제점 및 개선 방안”. 2013

[3] 여신금융협회. “신용카드 단말기 정보보호 기술기준”. 2015

[4] 여신금융협회. “직승인(라인) 가맹점 보안처리를 위한 기술기준”. 2016

금융보안 정책 국내외 최신 동향 및 이슈

정책연구팀*

* 금융보안원 보안연구부 정책연구팀, ejsong@fsec.or.kr

03 금융보안 정책 국내외 최신 동향 및 이슈

Ⅰ 금융보안 정책의 시대적 변천

1. 금융보안 인프라 구축('00년~'10년)

▶ 인터넷뱅킹 서비스 개시('99년)를 계기로 전자금융사고 예방을 위한 정책·기술 분야 인프라(Infra)를 구축하는 시기

□ **(정책분야)** 국내 최초로 인터넷뱅킹 해킹사고가 발생하여 관계부처 합동으로 「전자거래 안전성 강화 종합대책(보안프로그램 OTP 등)*」을 발표('05년)

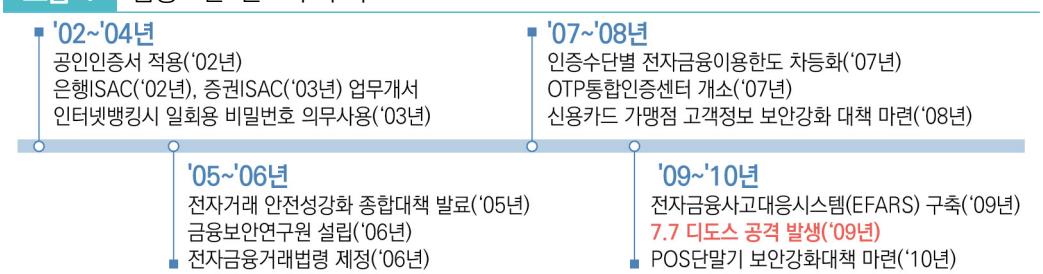
○ 금융보안의 기본 규제에 해당되는 전자금융거래법규(법, 시행령, 감독규정)도 제정·시행('06년)

□ **(기술분야)** 세계 최초로 공인인증서('02년)를 전자금융거래에 적용하였고, 거래인증 강화를 위해 OTP통합인증센터를 구축('07년)

○ 금융권 사이버테러 대응강화 및 기술지원을 위해 금융보안을 전문적으로 수행하는 기구*도 설립·운영

* 은행ISAC('02년, 금융결제원), 증권ISAC('03년 코스콤), 금융보안연구원('06년)

그림 1 금융보안 인프라 구축



2. 금융보안 고도화('11년~'14년 상반기)

▶ 고객정보 유출 등 금융보안 사고가 지속적으로 발생하여 재발방지대책을 통해 금융보안을 강화하는 시기

□ ('11년) OO캐피탈 고객정보(42만건)유출, OO은행 전산망 마비 사고 발생
➜「금융회사 IT 보안강화 종합대책」 마련

○ CISO 지정 의무화 등 금융회사의 상당한 주의와 감독 의무를 강조하는 책임주의 원칙 표방

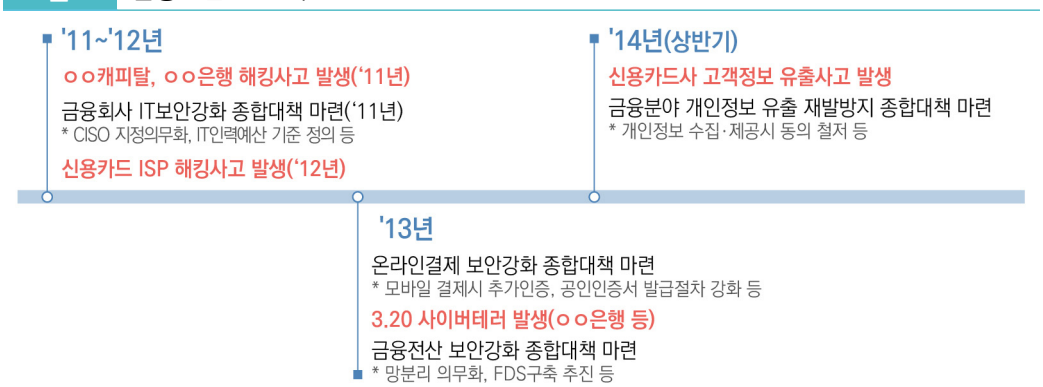
□ ('13년) 은행권 대상 침해공격이 발생하여 인터넷뱅킹 등 마비(3.20사이버테러)
➜「금융전산 보안강화 종합대책」 마련

○ 망분리 의무화, 이상금융거래탐지시스템(FDS) 구축 확대 등 제도·기술분야 보안관리 체계 강화에 중점

□ ('14년) 신용카드사의 고객정보(1억건 이상) 유출사고 발생➜「금융분야 개인정보 유출 재발방지 종합대책」 마련

○ 금융소비자의 자기결정권 보장, 개인정보 유출 형벌 상향 등 금융회사의 과도한 개인신용정보 수집·사용 관행에 제동

그림 2 금융보안 고도화



3. 자율보안 및 혁신금융 (‘14년 하반기~현재)

▶ 핀테크 산업 활성화 등을 계기로 금융보안의 패러다임이 ‘사전 규제’에서 ‘사후관리 및 자율보안’으로 전환되는 시기

□ **(사전규제 정비)** 핀테크 산업 발전에 장애요인으로 지적된 사전적·획일적 보안규제를 대폭 정비

○ 보안프로그램 설치의무(‘15.2월), 공인인증서 사용의무(‘15.3월), 사전 보안성심의 제도(‘15.6월), OTP 사용의무(‘16.6월) 폐지, 클라우드 규제 개선(‘16.10월), 혁신적 금융서비스 규제 특례(추진중)

□ **(자율보안체계 확립 지원)** 금융보안 컨트롤타워, 금융IT 융합보안 지원 등을 위해 금융보안원을 설립(‘15.4월)하고, 금융당국은 자율보안의 기본방향인 「금융IT부문 자율보안체계 확립 방안」 발표(‘15.6월)

○ 과태료 등 사후관리 강화(‘16.8월), FDS 정보공유체계 구축 및 정보공유 시스템 고도화 추진, 자체 정보보호 수준진단 도구 배포(추진중), 금융보안 레그테크 추진(추진중)

□ **(혁신 추진)** 핀테크 혁신 활성화 방안(‘18.3월), 금융분야 데이터활용 및 정보보호 종합방안(‘18.3월), 금융분야 클라우드 이용 확대방안(‘18.7월) 등을 발표하여 4차 산업혁명에 발맞춘 적극적인 혁신 추진 중

Ⅱ 최근 주요 정책 동향

1. 빅데이터 활성화 및 개인정보보호

(1) 금융당국 주요 추진 정책

▶ 금융분야 데이터활용 및 정보보호 종합방안(금융위, '18.3.19.) 및 금융분야 개인정보 보호 내실화 방안(금융위, '18.5.11.)을 발표하고 해당 사항 반영을 위해 신용정보법 개정 추진 중

가. 금융분야 빅데이터 활성화

□ 「익명정보」 및 「가명처리정보」 개념을 도입하고, 원칙중심의 법제도를 마련하여 빅데이터 이용을 허용하고,

※ (익명정보) 더 이상 개인을 식별할 수 없도록 처리된 정보 ➜ 개인정보 아님, 자유로운 활용

※ (가명처리정보) 추가적인 정보를 사용하지 않으면, 개인을 식별할 수 없도록 처리된 정보 ➜ 통계 작성, 과학연구 등 목적 활용

○ 전문기관(금융보안원, 신용정보원)을 통해 비식별조치 적정성 평가를 받도록 의무화

○ 익명·가명처리정보의 기술적·관리적 보호조치를 의무화하여 빅데이터 활용의 책임성 강화

□ 금융정보 DB(신정원, 보험개발원), 빅데이터 분석시스템(신정원), 빅데이터 중개 플랫폼(금보원) 등 빅데이터 인프라 구축 및 운영

나. 금융분야 데이터 산업의 경쟁력 강화

□ 금융정보(예금, 대출, 카드거래 등) 통합조회서비스를 제공하는 본인신용정보관리업을 도입하고,

○ 자본금요건을 최소화하되 정보유출 등에 대비한 배상책임 보험 가입을 의무화

○ 정보주체의 명시적 동의에 기반해서만 업무를 수행하며, 스크레이핑 방식*이 아닌 API 방식**으로 서비스 제공

* 스크린 스크레이핑(Screen Scraping) 방식: 핀테크업체가 고객으로부터 로그인정보 등을 제공받아 금융회사 웹페이지에 직접 접속하여 화면의 정보를 취득하는 방식

** API(Application Programming Interface) 방식: 핀테크업체가 금융회사가 제공한 별도 접근경로로 통신 및 요청하여, 고객의 정보를 취득하는 방식

□ 신용정보회사 및 카드사의 빅데이터 관련 업무 허용, 신용정보산업(CB)의 진입규제 완화 및 지배구조·행위 규제 도입 등

다. 개인정보보호 내실화

□ 정보활용 동의서 내용을 단순화·시각화하고, 선택 항목별 평가등급을 산정*하여 정보주체에 제공

* 사생활 침해 위험 및 소비자 혜택 등 반영

○ 선택적 동의사항에 대해 동의 항목을 목적·기관별로 세분화하여 개별적으로 동의여부를 선택할 수 있도록 개선

□ 프로파일링 대응권*, 개인신용정보 이동권** 등을 통해 소비자의 개인정보 자기결정권 보장 강화

* 자동화된 의사결정(보험료 자동 산정 시스템 등)에 대한 정보주체의 설명요구, 이의제기권 등

** 정보주체가 본인의 개인신용정보를 보유한 기관으로 하여금 본인정보를 제3자에게 이동시키도록 할 수 있는 권리

□ 금융권 정보활용·관리 실태 상시평가제를 도입하고, 그 결과가 지속적으로 우수한 기업에 인증마크 부여

○ 아울러, 금융위의 포괄적 조치명령권*을 신설하여 대량의 정보유출·침해사고 등에 신속히 대응할 수 있도록 함

* 금융회사, CB사 등의 정보 수집·이용·제공에 대한 포괄적 조치명령권

(2) 관련 국외 주요 동향

▶ EU, 중국 등 다수 국가에서 개인정보에 대한 정보 주체의 권리, 국외 이전 요건 강화 등 개인정보보호가 강화되는 추세

가. (EU) 개인정보보호 규정(GDPR) 시행

□ EU의 GDPR이 '18.5월 시행될 예정으로 세부내용 및 파급효과에 전 세계적 관심이 모아지고 있음

○ EU外 기업도 EU시민의 데이터를 처리할 경우 규정이 적용되며 막대한 과징금 부과 등 여파가 상당할 것으로 예상

※ 국내 금융권도 EU에 서비스를 제공하는 경우 해당되므로 적극적 대응 필요

표 1 GDPR 주요내용

구분	주요 내용
적용 범위	• EU내 설립된 기관의 개인정보 처리 활동 뿐만 아니라, EU외 기업도 EU 내 정보주체에게 서비스를 제공하는 경우 등 적용되며, EU내 대리인을 지정해야 함 • (개인정보 정의) IP주소, 쿠키 등도 개인정보로 간주, 유전정보와 바이오정보 등을 민감정보로 분류, 가명처리(추가정보없이 정보주체 식별 어려움) 적용 시 다양한 실익 부여
기업 책임성 강화	• 개인정보 처리 시 GDPR에서 정의하는 6가지 원칙을 준수해야하며, 이를 증명할 수 있어야 함 • 개인정보 유출시 72시간 내 감독당국 및 소비자 통지 의무 • DPO(개인정보관리책임자)의 의무 지정 • 고위험 처리에 대한 개인정보 영향평가 수행
정보주체 권리강화	• 정보주체는 열람권, 정정권, 삭제권, 처리제한권, 개인정보 이동권, 반대권, 프로파일링 등 자동화 처리 거부 권리 보유
개인정보 국외이전	• EU 집행위가 적정한 개인정보보호 수준을 갖추고 있다고 승인한 국가에는 개인정보의 국외이전을 허용 • 그 외 국가에서는 승인된 행동강령, 인증 메커니즘 등 적절한 보호조치가 있을 때에만 이전 가능 * 현재 우리나라는 방통위에서 적정성 평가 승인 추진 중
과징금	• 연간 매출을 기반으로 과징금을 부과하며, 심각한 위반인 경우 최대 2천만 유로 또는 직전연도 매출의 4% 부과

※ 최근 국내에서 GDPR 대응 및 유사법규 도입 적극 논의 중(국회 접수 정보통신망법 개정안 2건 이상, 개인정보보호법 개정안 1건 이상)

나. (중국) 네트워크 안전법 시행 등

□ 네트워크안전법('17.6월 시행)에 따라 중국內 수집·생성된 개인정보의 국외이전을 제한*하고 있으며,

* 자국민 데이터보호 목적, 업무상 이전 필요 시 중국당국이 정한 보안평가를 받도록 규정

○ 또한, 최근 개인정보 사고 피해가 증가함에 따라 개인정보 안전규범('18.5월 시행)을 국가 표준으로 제정

※ 안전규범은 표준으로 의무준수 대상은 아니나, 이를 토대로 감사가 진행될 것으로 예상

다. (미국) 데이터보호 관련 각종 법안 발의

□ 신용평가업체 에퀴팩스社의 고객정보 유출사태('17.9월) 이후 데이터보호 관련 법안이 다수 발의되었으며, 사회적 분위기에 따라 통과가능성이 높을 것으로 예상

표 2 에퀴팩스 사태 이후 발의된 법안과 내용

발의처	발의년월	법안 내용
뉴욕주 법무부	'17.11.	• 생체정보 등 사적정보(Private Information)에 대한 보안조치 등을 전 사업 분야에 적용하는 데이터보호법 제안
美상원	'17.11.	• 금융소비자가 부담하는 신용정보 조회 동결 수수료를 폐지하도록 하는 소비자보호법 개정안 발의 ※ 현재는 신용정보조회 동결을 요청할 경우 일정 수수료가 부과되나 신용정보 동결 요청이 폭증함에 따라 본 법안이 제안
美상원	'17.11.	• 기업 보안사고 발생 시 해당 내용을 소비자 및 당국에 30일 이내에 알리도록 하는 데이터 위반 통지법 발의 • 보안사고 통지의무를 알고도 고의적으로 숨기는 개인은 5년 이하의 징역 및 벌금이 부과
美상원	'18.1.	• 정보 유출사고 발생 시 피해자 1인당 최대 100달러의 과징금을 부과하도록 하는 데이터 유출 보상법 발의

라. (일본) 빅데이터 공동활용 포털사이트 구축 등

□ 광범위한 데이터를 쉽게 이용 및 분석할 수 있도록 민·관 보유 빅데이터 개방 및 공동활용 포털사이트 구축 추진('20년)

○ 또한, 개인정보보호법 개정('17.6월)을 통해 익명가공정보 가공 및 활용 관련 사항을 명시하여 활성화 추진

마. (베트남) 사이버보안법 통과

□ 사이버보안법('19.1월 발효 예정)에 따라 자국민 데이터의 현지 보관을 요구하고 있으며,

○ 공안부 요청 시 인증 정보를 제공하거나 게시물을 삭제해야 하고, 사생활 정보 등의 침해 방지를 위한 기술적·관리적 조치를 적용해야 함

2. 핀테크 활성화 및 보안 리스크 대응

(1) 금융당국 핀테크 혁신 활성화 방안

▶ 핀테크 혁신 활성화 방안 발표(금융위, '18.3.20.), 금융혁신지원 특별법안 발의(민병두의원 등, '18.3.6.) 등을 통해 핀테크 혁신을 추진하고, 관련 보안 리스크 대응 방안을 제시

가. 혁신적 금융서비스 실험·지원

□ 금융혁신지원 특별법 제정(국회 입법절차 진행중)을 통해 혁신금융서비스에 대해 시범인가 및 규제특례 적용

○ 특별법 제정 이전에도 법 개정 없이 가능한 위탁테스트, 지정대리인* 등 금융 테스트베드 본격 시행('18년)

* 혁신금융서비스 지정대리인 심사위원회 운영규칙 제정('18.상)

□ 핀테크 기업에 투자하는 민·관 합동 펀드 조성, 해외 금융당국과 핀테크 MOU체결 확대, 금융신산업 R&D 지원* 추진 등

* 블록체인 핵심기술개발 등(과기부·금융위 공동)

□ 핀테크지원센터 예산지원 추진(특별법에 지원근거 마련 추진) 등을 통해 조직을 확대 및 강화하고,

○ 관련 민간협의체 활성화, 테크자문단 운영 및 금융위내 CFO(Chief Fintech Officer) 지정 등을 통한 핀테크 산업 지원 체계 강화

참고 1 금융혁신지원 특별법 발의(안) 주요내용

□ **(혁신금융서비스 지정)** 금융위가 구성한 혁신심사위원회에서 혁신금융서비스 지정여부를 심사*

* 서비스 혁신성, 소비자 편익, 금융소비자 보호방안의 충분성 등 확인

□ **(지정 시 특례)** 혁신금융서비스로 지정된 경우 2년의 기간 내에서 특정 금융규제를 적용받지 않고 서비스 이행 가능

○ 혁신금융서비스 지정기간 만료 후 법령에 따른 정식 인허가를 받은 경우, 1년의 범위 내에서 해당 서비스에 대한 배타적 운영권한 보유

□ **(지정 사업자의 의무)** 시범운영 경과를 금융위에 정기적으로 보고하고, 시험운영 사실 및 위험발생 가능성 등을 이용자에게 사전 고지

○ 서비스 제공과정에서 이용자 손해 발생 시 혁신금융사업자의 고의나 과실이 없어도 이를 배상(관련 책임보험 가입 등 필요)

□ **(업무 위탁)** 금융회사는 혁신금융서비스 시범운영 관련 일부 업무를 지정된 대리인(금융회사 신청, 금융위 지정)에게 위탁 가능(2년 내)

□ **(감독 및 검사)** 지정감독기관은 혁신금융사업자, 지정대리인 및 업무위탁 금융회사에 대해 동법 준수여부를 감독하고, 그 결과에 따라 혁신금융서비스 지정취소, 서비스중지 등 건의 가능

□ **(기타)** 혁신금융서비스 지원기관의 운영 및 유지보수 관련 비용 정부 출연 및 보조 가능, 본 법안은 타 금융관련법령에 우선하여 적용

나. 금융권 서비스 고도화

□ 온라인 기반 금융투자상품 거래 확대를 위한 비대면 허용 범위 확대 및 관련 플랫폼(영상통화 등) 개발 지원(코스콤)

○ 로보어드바이저 테스트베드 지속 실시, 크라우드펀딩 관련 업종제한 및 투자한도 규제 개선 등 자본시장 핀테크 활성화

□ 신기술과 보험을 접목한 보험 상품 개발, 자율주행차 보험 상품 연구 추진, 온라인 소액보험 판매 허용('18.상) 등 인슈테크 활성화

다. 핀테크 시장 확대

□ 계좌기반의 모바일 간편결제 활성화*, 신규 결제방식 도입 제약 규제 정비 등

* 별도 단말기나 VAN망 등이 불필요한 앱투앱 계좌결제서비스(토스 시범도입, K뱅크·카카오뱅크 개발 중) 사업기반 조성 지원 등(세부 추진방안 추후 발표 예정)

□ 금융권 공동API의 확대를 유도하고, 개별 오픈API 활성화를 위한 민간 TF(금보원, 금결원, 일부 금융회사)를 구성하여,

○ 보안점검 가이드 등 개별API 지원방안 마련('18.하), 개별 오픈플랫폼 보안 취약점 점검, 혁신서비스 보안성 심사 강화 등 추진

□ 본인확인서비스 등 블록체인 활용분야를 확대하고, 금융권 블록체인 테스트베드를 구축(금보원, 코스콤)하여,

○ 금융회사의 블록체인 네트워크와 연결·활용 가능한 인프라 제공, 혁신 금융서비스 개념 검증 지원 등

* 블록체인 활용 시 상충되는 개인정보보호 관련 제도 보완('19~)

□ 신규 핀테크 서비스 등을 반영한 전자금융업 개편 검토('18년), 전자금융업자 건전경영 감독 실효 수단 확보('19년, 전금법 개정)

라. 핀테크 혁신 리스크 대응

□ 혁신기술 보안진단 및 컨설팅 등 보안 지원(금보원, 핀테크지원센터)을 강화하고,

○ 보조업자에 대한 금융권 공동점검의 효과적 수행·관리를 위한 보조업자 현황, 점검자료 취합·검증 지원 시스템 구축(금보원)

○ 금융회사·금보원 간 침해정보 공유체계 자동화, 이상금융거래정보 공유대상 확대(저축은행) 등 정보공유시스템 고도화('18.하)

○ EMP 데이터 소실 대응('18.하, 가이드라인), 금융권 공동 데이터 소산센터 구축 추진(한국은행) 등 혁신기술 보안대응 강화

□ 핀테크 기업 등에게 금융관련 법규 등 컴플라이언스 정보를 체계적으로 제공할 수 있도록 오픈API 구축('18.하, 금감원·금보원)

○ 금융회사의 보안수준을 자동으로 점검하는 금융보안 레그테크 시범사업 실시('18.하, 금감원·금보원)

참고 2 레그테크 정의 및 최근 동향

(1) 레그테크(RegTech)란?

□ 규제(Regulation) + 기술(Technology)의 합성어로, IT 기술을 활용하여 컴플라이언스 업무 등을 효율화하는 기술

* 인공지능 등 IT 신기술을 통해 규제관련 업무를 자동화하는데 초점

(2) 국내외 금융권 레그테크 최근 동향

1) 국내 동향

□ 레그테크의 개념과 필요성이 논의되며, 금감원은 관련 전문가로 구성된 레그테크 포럼을 구성·운영*하고, 레그테크 활성화 세미나 개최('17.10월)

* 금감원, 금보**원**, 금융회사 등의 레그테크 전문가가 참여('17.3~9월까지 운용)

○ 금융당국(금융위, 금감원)은 '18년 업무계획에서 레그테크 도입 및 활성화 기반조성 계획 등을 발표

□ 금융보안원은 금융보안 분야 레그테크 시스템 구축을 추진 中으로 '18.9월 서비스 개시 예정

○ 코스콤, KISA, 금융회사, 준법관리 회사 등에서도 레그테크 사업을 본격적으로 검토 중

2) 국외 동향

□ 영국, 호주, 싱가포르 등에서 금융당국 주도로 레그테크 활성화를 위한 각종 행사(포럼 등) 개최는 물론, 레그테크 개발 프로젝트도 다수 진행 중

○ 규제 이슈가 많아 관련 수요가 큰 유럽 및 미국을 중심으로 레그테크 업체가 증가하고 있으며, 특히 유럽은 GDPR 등 금년도 신규 적용 규제가 많아 레그테크를 통한 규제 준수 자동화 필요성이 더욱 부각

(2) 금융감독당국 IT·핀테크 감독·검사 계획

▶ IT·핀테크 분야 감독·검사 계획을 발표(금감원, '18.3.9.)하여, 혁신 친화적인, 리스크 중심의 감독체계 구축과 핀테크 지원 및 금융소비자 보호 강화 추진 계획을 제시

가. IT분야① - 혁신 친화적인 IT감독 체계 구축

□ 핀테크, 모바일 전환 등 전자금융 환경 변화로 발생하는 IT리스크를 관리하고,

○ 정보보호 문화 구축, 자체 정보보호 수준진단 등 금융회사 자율보안체계 확립 지원

□ 전자금융거래 사이트 엑티브엑스 제거, 블록체인 기반 인증 등 다양한 인증수단 도입 등을 통해 금융소비자 편의성 제고

나. IT분야② - 리스크 중심 상시감시 강화 및 IT검사 역량 집중

□ IT보안에 대한 경영진 역할 및 책임을 강조하고, 중대 위반행위에 대한 제재를 강화하여 자율책임 경영을 강화하며,

○ 리스크 중심 상시 감시 후 취약 부분 테마검사를 추진하고, 각종 신규 사업* 관련 보안 실태 및 외주업체 통제 점검 실시

* 모바일페이 등 신종 결제서비스, 차세대 시스템 구축 등 대규모 IT사업 등

다. IT분야③ - 전자금융소비자 보호 강화 및 소통 활성화

□ 이상금융거래 탐지시스템(FDS) 계량평가 지표 등을 활용하여 운영 실효성을 확보하고,

※ '17년 은행 및 증권회사에서 FDS 운영을 통해 총 3,665건, 445.8억원의 사고 예방, 1개사 기준 연평균 79.6건, 9.7억원의 예방 효과(금감원, '18.6.14.)

○ 전자금융사고 발생 시 책임배상 절차를 개선하여 전자금융소비자 보호 강화

□ 정보보호 유관기관 공조체계 강화, 국제 금융권 소통 활성화 등을 통한 국내외 유관기관 협력 강화

라. 핀테크분야 - 핀테크 산업 혁신 성장 지원 및 금융소비자 보호 강화

□ 규제 테스트베드 적극참여, 레그테크 발전 협의체 구성, 핀테크 현장 자문 업무 확대 등을 통한 혁신적 핀테크 생태계 구축

○ 특히, 글로벌 블록체인 컨소시엄 참여, 금융권 도입 지원방안 검토, 자문위원단 구성 등을 통한 블록체인 기술 활성화 지원

□ 간편송금업자, 전자지급결제대행업자(PG사) 등 전자금융업자 관리 강화를 통해 이용자 자산 보호를 강화하고,

○ P2P 대출 투자자 교육, 가이드라인 내용 정비 및 이행실태 점검 등을 통해 P2P 대출시장 건전성 제고

(3) 관련 국외 주요 동향

▶ EU를 중심으로 새로운 유형의 금융서비스 사업자를 정의하고, 기존 은행 등이 이들에게 오픈API를 제공하도록 제도화하는 등 금융정보자기결정권을 적극 강화하는 추세

가. (EU) 제2차 지급결제서비스지침(PSD2) 시행

□ EU에서 지급결제서비스지침 개정(PSD2, '18.1.13. 시행)을 통해 계좌정보서비스, 지급개시서비스 등 신규 지급서비스 제공자를 정의하고, 금융 당국 등록·관리 대상에 포함

○ 또한, 사용자 인증 절차를 강화하고, 기존 은행 등은 제3의 지급서비스 제공자를 위한 오픈 API를 제공하도록 하였으며, 세부 기준을 규제기술표준 형태로 제정(RTS-SCA, '19.9.14. 시행)

나. (일본) 전자결제 대행업 등록 및 오픈 API 제공 노력 의무

□ 은행법 개정('17.5월 성립)을 통해 전자송금서비스 및 계좌관리서비스를 「전자 결제 등 결제 대행업」으로 정의하고, 등록한 업체만 서비스를 제공할 수 있도록 함

○ 또한, 은행에서는 대행업체와의 제휴 및 협력에 대한 정책을 '18.3월까지 고시하도록 하여 API 제공을 위해 노력*하도록 함

* 오픈 API 제공이 의무화된 것은 아니나, 다수 주요 은행이 제공 추진 중

○ 이에, 일본 은행연합회에서는 오픈API 관련 개발 및 전문 표준, 보안 원칙 등을 발표했으며, 각 은행에서는 지난달 API 지원 일정 등 개별 정책을 고시함

(개별은행 고시 예시) 미츠비시 UFJ 은행

※ 전자결제 등 결제 대행업체와의 제휴 및 협력에 대한 정책
1) 기본방침: 오픈 이노베이션을 촉진 및 고객 편의 제공을 위해, 전자결제 등 대행업체와 제휴 및 협력을 이용자 보호에 유의하면서 추진
2) 제공 기능 및 완료 시기
• BizSTATION(기업뱅킹) API: 조회 및 기본이체('17.4월 완료), 일부이체('18.4월 예정)
• 미츠비시UFJ 다이렉트(개인뱅킹) API: 조회('18.2월 예정), 이체(검토중)
3) 시스템 설계, 운용 및 유지보수 정책
• 자체적으로 중계 시스템 구축, 시스템 설계, 운용 및 유지보수 실시
• 데이터교환형식-JSON, 액세스형식-REST, 인증방식-OAuth 2.0
4) 기타: 담당부서 및 문의 URL, 테스트 가능한 은행API 개발자 포털 제공

다. (미국, 영국, 중국) 핀테크 산업 지원

□ **(미국)** 뉴욕과 실리콘밸리 중심으로 등장한 핀테크 스타트업, 유수의 ICT 기업, 세계적 투자규모 등을 기반으로 성장했으며,

○ 뉴욕 핀테크 스타트업 지원 프로그램(이노베이션 랩) 등 네거티브 방식의 규제를 통해 활성화되었고,

○ 최근 텍사스, 워싱턴, 일리노이 등 7개주에서는 상호 허가 결과 승인 등 핀테크 사업 허가 절차 간소화 추진 중('18.2월)

□ **(영국)** 금융당국 이원화, 이노베이션 허브, 규제 샌드박스, 테크시티 조성 등 정부의 적극적인 지원에 힘입어 세계적인 핀테크 허브로 주목받고 있음

□ **(중국)** 기존 금융인프라의 주체 간 불균형 대비, 핀테크의 포용적 금융 실현 명분으로 정부는 적극적으로 핀테크 산업을 지원,

○ 알리페이 등 세계적 기업을 다수(세계 10대 기업 중 5개) 보유하고 있으며, 핀테크 산업 거래 규모는 전 세계 1위를 기록('17년)

○ 다만, 최근 핀테크 금융서비스의 부작용 확대로 인터넷 전문은행 설립 요건 강화 등 규제를 강화하는 추세

3. 기타 사항

(1) 정부 주요 추진 정책

▶ 공인인증서 폐지, 금융권 클라우드 이용 확대, 노플러그인 추진 등 IT 신기술 활성화를 위한 다양한 논의가 진행되고 있으며, 특히 정부는 제4차 산업혁명위원회 주도의 해커톤을 통해 논의된 내용을 적극 반영하고 있음

가. 공인인증서 폐지

□ 공인전자서명 제도의 근거가 되는 전자서명법 개정안이 정부 및 국회에서 각각 발의되었으며, 현재 입법예고 및 심사 중

표 3 전자서명법 개정안 주요내용

구분	주요내용
정부발의안 (과기정통부 입법예고, 3.30.)	〈공인전자서명 제도 폐지 및 인증업무 평가제 도입〉 • (공인전자서명 제도 폐지) 공인전자서명 제도 관련 조문을 삭제하고, 일반 전자서명에 유사(일부 상이) 효력 부여 * 법적추정력 삭제, 전자서명요건 삭제, 본인확인기능 삭제, 전자 형태 이유 법적효력 부인 금지 명시 • (인증업무 평가제) 전자서명인증업무 운영기준을 마련하고, 전자서명인증사업자는 평가 및 확인을 거쳐 운영기준 준수 증명서를 발급 받을 수 있음
고용진의원 (더불어민주당) 대표발의안(3.6.)	〈공인전자서명 제도 폐지 및 인증기관 등록제 도입〉 • (공인전자서명 제도 폐지) 공인전자서명 제도 관련 조문을 삭제하고, 일반 전자서명에 유사(일부 상이) 효력 부여 * 법적추정력 삭제, 전자서명요건 유지, 법적효력 관련 별도 명시 없음 • (인증기관 등록제) 공인인증기관 지정제 폐지, 인증기관 등록제 신규 도입, 등록 조건 및 의무 등 기존 지정제와 매우 유사
박성중의원 (자유한국당) 대표발의안(3.7.)	〈블록체인기술 기반 전자서명에 효력 부여〉 • 공인전자서명 제도 유지, 블록체인 기술 기반 전자서명 중 요건을 갖추어 과기정통부 장관 지정 받은 경우 동일 효력 부여
신용현의원 (바른미래당) 대표발의안(4.6.)	〈블록체인기술 기반 공인인증 전자서명 지정〉 • 공인전자서명 제도 유지, 블록체인 기술 기반 전자서명 중 요건을 갖추어 과기정통부 장관 지정 받은 경우 공인인증 전자서명으로 지정하고, 동일 효력 부여

나. 금융권 클라우드 이용 확대

□ 현행 규정 상 클라우드 컴퓨팅 이용이 제한되는 신용정보 등에 대해 국내 소재 클라우드 서비스 이용을 허용

※ 국외소재 클라우드 서비스는 중·장기적 검토

○ 신용정보를 클라우드로 안전하게 이용할 수 있도록 기준을 마련하고, 금융회사 보고의무 및 금융당국 조사권 등 클라우드 이용에 대한 감독·검사 강화

참고 3 금융분야 클라우드 이용 확대방안 주요내용

□ **(클라우드 서비스 이용범위 확대)** 개인신용정보, 고유식별정보를 처리하는 중요정보 처리 시스템도 클라우드를 활용할 수 있도록 규제 개선

○ 사고 발생시 법적 분쟁, 소비자 보호·감독 관할, 개인정보보호 등의 문제로 국내 소재 클라우드에 한해 우선 허용(국외는 중장기 검토)

□ **(클라우드 서비스 기준 도입)** 안정성을 확보하기 위해 클라우드 이용·제공 시 기준을 마련

○ (금융회사) 중요정보 클라우드 이용 시 안전성 관리를 강화

○ (제공자) 금융위 특수성을 반영해 클라우드 서비스 제공자가 기본적으로 준수해야 할 기준을 마련

* 서비스 기준은 자율통제 또는 인증제로 운영되며, 운영 방식은 금융권 클라우드 서비스 이용 활성화를 위한 제도개선 TF('18.7월중, 금융위, 금감원, 금보원, 금융회사, 전문가 등)를 통해 검토 추진

□ **(클라우드 서비스 이용 감독·검사 강화)** 금융회사를 통한 간접 감독을 강화(클라우드 서비스 이용 관련 금융회사 보고의무 강화)하고,

○ 법령 개정을 통한 전자금융보조업자에 대한 감독·조사 근거 확보 방안 검토

다. 노플러그인 정책 추진

□ 노플러그인(No Plug-in) 정책은 웹사이트 이용 시 엑티브 엑스를 포함하여 별도 프로그램 설치가 필요 없도록 하는 정책으로,

○ VIP가 청와대 수석·보좌관 회의('17.12월)에서 공공분야 노플러그인을 정책 목표로 제시하고, '18년내 추진을 지시

참고 4 4차 산업혁명위 규제·제도혁신 해커톤

□ 4차산업혁명위원회(대통령직속)에서 규제·제도혁신 해커톤을 개최, 정부·산업계·학계·시민단체 등 관계자들이 1박 2일간 집중토론을 진행하여 사회적 합의를 도출

표 4 규제·제도혁신 해커톤 주제 및 결론

구분	주제 및 결론
제1차 ('17.12.21.~12.22.)	1. 핀테크(금융서비스 사용자의 금융정보 자기 결정권 증진 방안) • 민간주도 핀테크 협의체 구성, 핀테크업체가 금융법상 주체로 활동할 수 있는 방안 검토, 금융정보자기결정권 구현을 위한 금융권 API 공개 의무화는 사회적 추가 논의 필요 2. 위치정보보호법 개선 방향 토론 • 개인위치정보가 서비스제공에 필수적인 경우 사전고지 방식, 비식별위치정보와 사물위치정보를 보호 대상에서 제외, 위치기반서비스사업자 진입 규제 완화 및 사후 책임 강화 등 3. 혁신의료기기 신속심사 및 허가제도 개선 방안 토론 • 첨단의료기기 허가-평가 신속화, 의료기기산업 육성법 조속 제정 등
제2차 ('18.2.1.~2.2.)	1. 개인정보의 보호와 활용의 균형 방안 마련 • 개인정보 관련 법적 개념체계 정비(개인정보, 가명정보, 익명정보), 익명정보는 법에 명시하지 않고 개인정보의 개념을 보완, 가명정보 법적 근거 마련 2. 공인인증서(전자서명법 개정) • 공인인증서 폐지 관련 전자서명 정의 및 법적 효력, 안전성 평가제도 도입, 주민등록번호 수집·이용 비의무화, 전자서명 선택 제한은 법령에 근거, 제도 개선으로 국민체감 제고
제3차 ('18.4.3.~4.4.)	1. 개인정보의 보호와 활용의 조화 • 가명정보 목적이외 이용(기록 보존, 학술연구, 통계 등), 익명처리 절차, 기준, 평가 등 마련(제3 기관 활용 가능), 데이터 결합(미합의), 정통망법, 신정법, 위치정보법 상 중복, 유사 조항 통일 2. 공공분야 클라우드 이용 활성화 • 클라우드 이용 가능 정보 등급제(미합의), 공공기관 클라우드 이용 시 절차 및 방법론 개선, 클라우드 보안인증제 인식제고, 클라우드 도입에 따른 공공기관 경영평가 등 인센티브 3. 드론산업 활성화 • 인증/검정 절차 간소화, 비행승인 및 항공촬영허가 관련 규제 완화, 드론 분류기준 정비, 드론용 면허 주파수 확보, 시범사업공역 추가 확보 및 비시범사업자 대상 개방

(2) 관련 국외 주요 동향

▶ 미국, 유럽 등 다수 국가에서 사물인터넷, 클라우드 등 IT 신기술 활성화를 적극 추진하고 있으며, 이와 별개로 국외에서는 최근 사이버보안 강화 관련 정책이 다수 발표되고 있음

가. 사물인터넷, 클라우드 등 IT 신기술 활성화 추진

□ **(사물인터넷)** 미국에서는 각 연방별 IoT 지원 정책 및 가이드라인을 수립·운영 중이며, 美상원에서는 연방에서 구매하는 IoT 기기 보안 표준을 정의하는 사물인터넷 보안강화법이 발의('17.8월)

○ EU에서는 DSM 전략*에 따라 예산 투자 등 각종 IoT 관련 정책 지원 추진중

* EU DSM(Digital Single Market) 전략: 유럽연합 내부의 장애물을 제거하여 디지털 단일시장을 구축하고자 하는 전략(3개 주제, 16개 세부과제 발표, '15.5월)

□ **(클라우드)** 미국은 '12년 클라우드 퍼스트 정책 및 FedRAMP*를 발표하여, 공공 및 민간영역에서 클라우드 활용이 활성화되어 있음

* FedRAMP(Federal Risk and Authorization Management Program): 美 공공분야 클라우드 보안 인증 프로그램

○ EU는 클라우드 활성화를 위한 규정*, 금융권 클라우드 이용 관련 권고**를 발표하는 등 적극 추진 중이며, 호주 및 일본에서도 일부 금융회사가 시스템 클라우드 이전을 추진 중

* EU내 非개인정보의 자유로운 활용에 대한 규정(안)(Framework for the free flow of non-personal data in the European Union, '17.9월 제안) 中 사용자와 클라우드 제공자 간 데이터 이동 관련 장애요소 제거 관련 내용 포함

** 유럽 은행청(EBA), 클라우드 제공자 업무 위탁에 대한 권고('18.7월 발효)

나. 사이버보안 강화

□ **(미국)** 최근 사이버보안 강화 및 금융소비자 보호를 위한 다양한 정책이 발표되고 있음

○ 백악관은 사이버보안 강화 행정명령('17.5월) 및 국가 안보전략 2017('17.12월)을 통해 금융 등 핵심기반시설 사이버위험 관리 강조

○ 美연방정부는 신규 취약점을 검토하여 해당 취약점의 내용을 공개하도록 하는 정책(VEP) 발표('17.11월)

○ 뉴욕주는 금융회사 정보보호 조치 요구 규정 및 지침을 발표('17.10월)하고, 신용평가기관에 등록 의무(~'18.2) 및 사이버보안 규정 준수 의무(~'19)를 부과하는 신규 규정* 제정

* 신용평가 기관에 대한 등록 요구사항 및 금지행위(23 NYCRR 201)

○ 증권거래위원회는 주식회사의 보안사고 발생 시 관련 내용을 공개하도록 의무화하는 가이드라인 시행('18.2월)

○ NIST는 사이버보안 프레임워크의 개정('17.12월)을 통해 공공부문뿐만 아닌 민간에서의 적극적 도입을 권장

□ **(EU)** EU집행위는 EU에 사이버위협이 위기가 될 수 있음을 언급하며, 사이버보안 강화 전략을 발표('17.9월)하여,

○ ENISA*의 권한 확대를 주 내용으로 하는 사이버보안법(안)을 제안하고('18년 중 통과 예상), EU회원국이 네트워크 및 정보보호지침(NIS, '16.7월)의 완전하고 신속한 준수('18.5.9. 까지)를 독려

* 유럽네트워크정보보호원(European Union Agency for Network and Information Security): EU의 사이버보안 전문기관으로 정책수립·집행 지원, 사이버 대응 훈련 및 보안 관련 가이드 제정 등을 수행 중

EU 사이버보안 전략 관련 법규 주요내용

1. EU 사이버보안법(안) 주요내용
   ① ENISA를 EU의 사이버보안 기관으로 지정하여 기존 '20년까지인 존속기한을 무제한으로 설정하고 사이버보안과 관련된 업무목표 설정 및 역할 부여
   ② ENISA는 EU의 공식기구로 연합법원의 허가 없이는 법적 조치가 불가능하며, 기관의 소속 임직원은 공무활동 중 발생한 분쟁에 대해 면제특권이 부여
   ③ EU전역에서 활용할 수 있도록 ICT 제품 및 서비스에 대한 EU 차원의 보안 인증제도(ECCS)를 수립하도록 하여 인증절차의 효율성 개선

2. 네트워크 및 정보보호지침 주요내용
   ① 침해사고대응팀 구축 등 사이버보안 역량 강화
   ② EU회원국 간 정보공유 등 협력 증진
   ③ 금융 등 주요기반시설에 대한 보호조치 등

□ **(중국)** 네트워크 안전법을 제정('17.6월 시행)하여 주요정보기반시설을 정의하고 해당 시설 운영자에게 안전보호의무를 부과

○ 관련 하위규정으로 네트워크 제품 및 서비스 보안심사방법, 주요정보기반시설 보호 방법 등을 제정하여 보안 관리 의무 강화

Ⅲ 시사점

□ 빅데이터, 핀테크 등 新기술을 활용한 금융혁신을 위해서는 개인정보 유출, 해킹 사고 등 부작용에 대한 대책이 필수적

○ 금융당국은 적극적인 산업 육성과 함께 안전한 금융환경 조성을 위해 다양한 금융보안 정책을 추진 중

➜ 따라서, 금융권에서도 안전한 금융혁신 추진을 위해, 신기술 활용에 따른 보안리스크를 면밀히 분석할 필요

Issue·Trend

산업동향

- 중국의 차세대 인공지능 발전 규획 및 실행 계획

핀테크·신기술

- AI로 인해 발생 가능한 보안 위협 및 권장 사항
- 양자컴퓨팅과 포스트 양자암호 동향
- 최신 바이오 인식 기술의 동향 및 활용 사례
- 국내·외 금융권 챗봇 활용 현황 및 주요 보안고려사항
- 머신러닝을 활용한 해외 기업의 악성코드 탐지 연구 소개

법·정책

- 「금융혁신지원 특별법안」 주요 내용 및 시사점
- 전자서명법 개정 추진 동향 및 시사점

중국의 차세대 인공지능 발전 규획 및 실행 계획

□ 개요

○ ‘17년 7월, 중국은 ‘차세대 인공지능 발전 규획’을 발표하고, 그 해 12월, ‘차세대 인공지능 산업 발전 촉진을 위한 3개년 실행 계획’(이하 ‘실행 계획’)을 발표

- 중국 국무원이 발표한 ‘차세대 인공지능 발전 규획’은 장기적인 관점에서 중국의 인공지능 발전 방향을 제시
- 중국 공업정보화부[1]에서 발표한 ‘실행 계획’은 ‘차세대 인공지능 발전 규획’을 기반으로, 중국이 인공지능 발전을 위해 2018년부터 2020년까지 수행할 구체적인 행동 방향을 제시

○ 이에 본고에서는 중국의 ‘차세대 인공지능 발전 규획’ 및 ‘실행 계획’의 주요 내용에 대해 간략히 소개

□ 차세대 인공지능 발전 규획

‘차세대 인공지능 발전 규획’은 중국이 인공지능 발전을 위해 수행할 중점 임무와 이를 이행하기 위한 지원 방안으로 구성

1) 산업, 에너지, 정보통신 정책 등을 담당하는 중국 국무원 산하의 중앙 정부 부처

(가) 중점 임무

○ (혁신 체계 구축) 기초 이론 체계, 핵심 기술 체계, 혁신 플랫폼을 구축하고 인재 양성 및 유치를 통해 인공지능 과학기술 혁신 체계를 구축

○ (산업 발전 환경 구축) 인공지능으로 신흥 산업 육성, 기존 산업 및 기업의 스마트화[2]를 추진하고 인공지능 혁신 단지를 조성

○ (안전한 스마트 사회 건설) 스마트 서비스 제공, 사회 관리의 스마트화, 인공지능을 이용한 공공 안전 보장으로 안전하고 편리한 스마트 사회 건설

○ (스마트 인프라 구축) 네트워크, 빅데이터, 고성능 컴퓨팅 인프라를 구축하여 인공지능 발전에 기여

표 1 중점 임무의 세부 내용

중점 임무	세부 내용
혁신 체계 구축	• (기초 이론 체계) 빅데이터 지능 이론[3], 뇌 컴퓨팅 이론, 양자 지능 컴퓨팅 이론 등 인공지능과 관련된 기초 이론 연구 강화 • (핵심 기술 체계) 자율 시스템, 지능형 가상현실 모델링 기술, 자연어 처리 기술 등 인공지능의 핵심 기술 연구 • (혁신 플랫폼) 인공 지능 소프트웨어 및 하드웨어 인프라 플랫폼, 자율 시스템 지원 플랫폼, 인공지능 기초 데이터 및 안전 검사 플랫폼 등 구축 • (인재 양성 및 유치) 대학에 인공지능 학과 개설, 해외 우수 인공지능 인재 유치 등을 통해 중국의 인공지능 인재 풀(pool) 마련
산업 발전 환경 구축	• (신흥 산업 육성) 인공지능을 활용하여 지능형 로봇, 지능형 운송 수단, 지능형 단말기[4] 등 개발 • (산업의 스마트화) 제조·농업·물류·금융 등의 중점 산업에 인공지능을 적용하여 산업의 스마트화 추진 • (스마트 기업) 기업의 핵심 업무에 인공지능 기술을 적용하여 기업을 스마트화하고 인공지능을 적용한 스마트 공장 운영을 장려하며, 인공지능 산업의 선도 기업 양성 • (인공지능 혁신 단지) 인공지능 산업 혁신 단지 및 연구 센터 건설

2) 인공지능을 적용하여 발전시킨 것을 '스마트'라고 표현
3) 빅데이터로부터 지식을 추출하고 의사 결정까지 지원하는 것
4) 스마트폰, 차량용 스마트 단말기, 스마트 시계, 스마트 이어폰, 스마트 안경 등

중점 임무	세부 내용
안전한 스마트 사회	• (스마트 서비스) 교육·의료·건강 및 양로 등 민생과 관련된 분야에 인공지능을 활용하여 스마트 서비스를 제공 • (사회 관리의 스마트화) 행정·사법·도시·환경 등의 관리에 인공지능 기술을 적용하여 관리 인프라의 스마트화 추진 • (공공 안전 보장) 범죄 관리, 공공 구역 보안, 식품 안전 평가, 자연 재해 모니터링 시스템 등에 인공지능을 적용하여 공공 안전 보장 능력을 향상
스마트 인프라 구축	• (네트워크) 5G 기술을 연구 개발하여 인공지능 시스템의 데이터 전송 속도를 높이고, 사물인터넷 인프라를 구축 • (빅데이터) 대규모의 데이터 인프라를 구축하여 인공지능 연구 개발을 위한 대용량의 데이터를 제공하고 데이터 안전 및 개인정보 보호를 강화 • (고성능 컴퓨팅) 슈퍼 컴퓨팅, 분산 컴퓨팅 인프라 및 클라우드 컴퓨팅 센터를 구축하여 인공지능 응용 프로그램을 지원

(나) 지원 방안

○ (법률, 규정, 윤리 규범 제정) 인공지능과 관련한 법적, 윤리적, 사회적 문제에 대한 연구를 강화하고 인공지능의 건전한 발전을 보장하는 법률, 규정, 윤리 규범을 제정

○ (정책 마련) 인공지능 스타트업 및 중소기업에 대한 세제 우대, 첨단 기술 기업의 세제 혜택 및 연구 개발 비용 공제 등의 정책 마련

○ (표준 및 지식재산권) 인공지능 기술 표준을 제정하고 인공지능 분야의 지식재산권 및 특허 보호를 강화

○ (안전 감독 및 평가) 인공지능의 안전에 대한 감독 및 평가 시스템을 구축

- (전체 과정 관리·감독) 인공지능 알고리즘 설계, 제품 개발 및 활용 등 전체 과정에 대해 관리·감독을 수행
- (처벌 강화) 인공지능 산업에서 발생한 데이터 남용, 개인정보 침해, 윤리 위반 행동 등에 대해 처벌을 강화

- (네트워크 보안) 인공지능 네트워크 보안 기술 연구 개발로 인공지능 시스템의 네트워크 보안을 강화
- (안전성 및 성능 평가) 인공지능의 위험성, 불확실성, 해석 가능성 등을 평가하는 안전성 테스트 플랫폼을 구축하고 인공지능 시스템의 성능을 평가

○ (인공지능 기술 교육 강화) 인공지능 기술에 대한 직업 훈련 시스템을 구축하고, 회사 및 기관은 소속 직원들에게 인공지능 기술 훈련을 수행

○ (인공지능 대중화) 초·중·고등학교에 인공지능 교육과정을 배치하고, 인공지능 기업 및 연구기관이 구축한 오픈소스 플랫폼을 대중에게 개방

□ 차세대 인공지능 산업 발전 촉진을 위한 3개년 실행 계획

'실행 계획'은 '차세대 인공지능 발전 규획'에 기반 하여 제조업을 중심으로 여러 산업에 인공지능을 적용하기 위한 중점 임무와 이를 이행하기 위한 지원 방안으로 구성

(가) 중점 임무

○ (인공지능 제품 개발 촉진) 인공지능 제품 및 서비스를 개발하여 의료, 농업, 금융 등에 활용

표 2 2020년까지의 인공지능 제품 및 서비스 개발 목표

제품 및 서비스	목표
지능형 네트워크 연결 차량	• 신뢰할 수 있고, 안전하며, 실시간 지능형 인터넷이 연결된 차량용 스마트 플랫폼을 개발
지능형 서비스 로봇	• 지능형 서비스 로봇의 환경 인지, 자연스러운 상호 작용, 자율 학습 등과 같은 핵심 기술을 개발
의료 영상 진단 시스템	• 대부분의 일반적인 질병을 1% 미만의 거짓음성률(false-negative rate)과 5% 미만의 거짓양성률(false-positive rate)로 탐지하는 시스템을 개발

제품 및 서비스	목표
비디오 영상 인식 시스템	• 복합적이고 동적인 영상에서 얼굴 인식률은 97%를 넘고 정확한 인식률은 90%를 초과하며, 지역별 얼굴 특징을 인식하는 시스템을 개발
지능형 음성 대화 시스템	• 중국어 인식의 정확도가 평균 96% 이상 도달해야 하며, 5m 떨어진 거리에서의 중국어 음성 인식률은 93% 이상 되고, 대화 의도 인식의 정확도는 90%를 초과하는 시스템을 개발
지능형 번역 시스템	• 중(中)-영(英) 번역 및 영-중 번역의 정확도는 85%를 초과하며, 소수 민족 언어와 중국어 간의 번역 정확도도 향상된 시스템을 개발
스마트홈 제품	• 스마트홈 제품의 종류를 확대하고, 스마트TV 보급률이 90%를 넘어야하며, 보안 제품의 지능 수준을 향상

○ (핵심 구성 요소 개발) 스마트 센서, 신경망 칩, 오픈 소스 플랫폼과 같은 하드웨어 및 소프트웨어의 핵심 구성 요소를 개발하여 기반을 강화

○ (지능형 제조 발전을 심화) 인공지능을 활용하여 제조업의 핵심 기술 및 장비를 제조하고 새로운 패러다임을 형성

- (핵심 기술 및 장비 제조) 인공지능 기술을 사용하여 CNC 기계[5] 및 산업 로봇의 셀프 기능과 지능 수준을 향상하고 적층 가공[6] 장비의 가공 정확성과 제품 품질을 향상
- (새로운 패러다임 형성) 제조 회사가 네트워크 및 지능형 생산 장비를 사용하고, 데이터를 분석 및 처리 하는 기계학습 기술을 적용하는 등 제조업의 새로운 패러다임을 형성

○ (지원 시스템 구축) 학습 자원, 표준 테스트 플랫폼 및 지식재산권 서비스, 지능형 네트워크 인프라, 네트워크 보안 시스템 등 인공지능 발전을 지원할 수 있는 시스템을 구축

5) CNC(Computer Numerical Control) 기계: 컴퓨터를 내장한 자동화 공작 기계(기계를 만드는 기계)
6) 원료를 여러 층으로 쌓거나 결합시키는 3D 프린팅 작동 방식

표 3 인공지능 발전을 지원하는 시스템

시스템	구축 방안
학습 자원 시스템	• 산업, 의학, 금융, 운수 사업 및 음성 인식, 자연어 처리와 같은 기초 분야에서 고품질의 인공지능 학습 자원, 표준 테스트 데이터 셋을 구축하고 공유
표준 테스트 및 지식재산권 서비스	• 인공지능의 연결성, 보안 및 프라이버시 보호 등의 표준 테스트를 지원하고, 인공지능 기술의 특허 및 지식재산권 서비스 플랫폼을 구축
지능형 네트워크 인프라	• 5G와 같은 고속, 고용량, 낮은 지연 시간의 지능형 차세대 네트워크를 구축
네트워크 보안 시스템	• 지능형 네트워크 연결 차량, 스마트홈과 같은 핵심 인공지능 제품을 중심으로 취약점, 보안 테스트, 공격 탐지 및 대응 등과 같은 보안 기술 연구

(나) 지원 방안

○ 중점 임무의 이행을 보장하기 위해 조직 강화, 지원 확대, 혁신 및 기업가 정신 장려, 인재 양성 활성화, 개발 환경 최적화가 필요

- (조직 강화) 정부와 기업 등이 조직을 구성하여 시너지 효과를 내고, 정부 부처와 지역의 협력을 강화하며, 인공지능 선도 기업 집단 및 산업 단지를 건설
- (지원 확대) 제품 안전성 및 보안성 검증 플랫폼 구축, 인공지능 기술 개발 등을 지원하고, 인공지능 발전에 필요한 자본 유입을 위해 인공지능 회사와 금융 기관의 협력 강화를 지원
- (혁신 및 기업가 정신 장려) 인공지능 연구소 및 제조 혁신 센터를 설립하고, 인공지능 기술의 공동 연구 개발을 위해 기업, 과학 연구 기관, 대학을 지원
- (인재 양성 활성화) 학교는 인공지능 관련 공동 프로젝트를 수행하고, 기업 및 기관 등은 인공지능 인재를 양성하도록 장려
- (개발 환경 최적화) 인공지능 관련 정책 및 법규를 연구하고, 관련 업계의 데이터 개방을 촉진하며, 국제 협력을 장려

□ 결 론

○ 중국은 정부의 적극적인 인공지능 지원 정책과 기업들의 공격적인 투자가 이어지면서, 인공지능 산업이 급격히 성장하는 추세

- 중국 정부는 '차세대 인공지능 발전 규획' 등의 로드맵을 발표하면서 국가적 차원에서 인공지능 산업을 육성

○ 국내에서도 금융, 의료 등 여러 분야에서 인공지능을 도입하고 있는 만큼, 중국을 포함한 해외의 인공지능 발전 동향을 살피는 것이 필요

AI로 인해 발생 가능한 보안 위협 및 권장 사항

□ 개 요

○ AI 기술이 발달하면서 기술의 활용 범위가 지속적으로 확대되고 있지만, 일각에서는 이로 인해 발생 가능한 보안 위협을 우려

○ '18년 2월, 영국 옥스퍼드대, 신미국안보센터(Center for a New American Security)[1] 등으로 구성된 AI 전문가 그룹[2]은 AI와 관련된 보안 위협에 관해 'AI의 악의적 사용(The Malicious Use of Artificial Intelligence)' 보고서를 발표[3]

○ 이에 본고에서는 'AI의 악의적 사용' 보고서를 기반으로 AI로 인해 발생할 수 있는 보안 위협 및 이에 대응하기 위한 권장 사항을 소개

□ AI를 활용한 공격 및 AI를 노린 기만 공격

(가) AI를 활용한 공격

○ 공격자는 AI를 활용하여 기존 공격 방식을 고도화하거나 새로운 방식의 공격을 수행

- (기존 공격 방식의 고도화) 공격자는 공격에 필요한 노동력, 지능, 기술에 AI시스템을 활용함으로써 공격 비용을 감소시키고 대규모의 공격을 빠르게 수행 가능

---

1) 신(新)미국안보센터(Center for a New American Security): 미국의 국가안보 및 국방정책을 개발하는 싱크탱크
2) Future of Humanity Institute, 옥스퍼드대, Centre for the Study of Existential Risk, 캠프리지대, 신(新)미국안보센터, Electronic Frontier Foundation, OpenAI 등을 포함한 14개 기관의 전문가 26명
3) Brundage M., et al. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation." arXiv preprint arXiv, 2018.

- (예시) 공격자는 자동화된 AI시스템으로 SW 취약점을 찾아, 짧은 시간 동안 대량의 공격 수행

- (새로운 방식의 공격) 공격자는 AI를 통해 기존 기술로는 수행하기 어려웠던 새로운 공격 방식 도출
  - (예시) AI가 오바마 전(前) 미국 대통령의 음성과 영상을 학습하여 오바마 대통령과 유사한 음성[4] 및 영상[5]을 만듦으로써 거짓 뉴스 생성(그림 1)

그림 1 AI를 이용한 거짓 뉴스 생성의 예

(나) AI를 노린 기만 공격

○ AI를 노린 기만 공격은 공격자가 AI 시스템을 교란시키는 공격으로, 대표적으로 ①적대적 예시(Adversarial Examples), ②데이터 중독(Data Poisoning), ③은닉 음성 명령 등이 존재

4) Arik S.O., et al. "Deep Voice 2: Multi-speaker neural text-to-speech." arXiv preprint arXiv, 2017.
5) Suwajanakorn S., et al. "Synthesizing obama: learning lip sync from audio." ACM Transactions on Graphics (TOG), 2017.

① 적대적 예시 공격

- 공격자가 AI 시스템이 인식해야하는 이미지에 노이즈를 추가하여, 시스템이 잘못 인식하도록 하는 공격
  - (예시) 공격자는 교통 표지판에 스티커(노이즈)를 부착하여, 자율주행차량이 '정지' 표지판을 '속도 제한' 표지판으로 잘못 인식하도록 함으로써 사고 유발(표 1)[6]

표 1 적대적 예시를 사용한 공격의 예

상태	표지판	시스템 인식 결과
정상		정지
스티커 부착	 	속도 제한

② 데이터 중독 공격

- 공격자가 AI 시스템의 학습 과정[7]에 잘못된 레이블이 부착된 데이터를 삽입하여, 시스템이 부정확한 결과를 도출하도록 하는 공격
  - (예시) 공격자가 AI기반 악성파일 탐지 시스템의 학습 데이터에 잘못된 레이블이 부착된 데이터를 넣어 악성파일을 탐지하지 못하도록 유도(표 2)[8]

6) Evtimov I., et al. "Robust physical-world attacks on machine learning models." arXiv preprint arXiv, 2017.
7) AI 시스템이 어떤 것을 판별하기 위해 레이블이 부착된 데이터를 학습하는 과정으로, 부착된 레이블에 근거하여 데이터를 학습하기 때문에 레이블의 정확도가 중요
8) Biggio B., et al. "Poisoning attacks against support vector machines." arXiv preprint arXiv, 2012.

표 2 데이터 중독을 사용한 공격의 예

정상	
공격	

③ 은닉 음성 명령 공격

- 공격자가 AI는 인식하지만 사람은 해독하지 못하는 백색 소음의 명령[9]을 음성 인식 시스템에게 들려줌으로써 은밀하게 명령을 지시하는 공격
  - (예시) 공격자는 구글의 음성 인식 시스템 '나우(NOW)'에게 "사이트 A에 접속해"라는 명령을 백색 소음으로 들려줌으로써 대상 기기가 악성 사이트A에 접속하도록 유도[10]

□ 권장 사항

○ 'AI의 악의적 사용' 보고서에서는 AI로 인한 보안 위협에 대응하기 위해 우선적 권장 사항과 장기적 권장 사항을 제시

- 우선적 권장 사항은 AI 전문가와 정책 담당자의 역할에 대해 제시
- AI 전문가는 악의적으로도 사용될 수 있는 AI의 양면성을 인지하고, 자신의 연구 결과가 악용될 수 있는 가능성을 고려하여 연구 수행

9) AI 기반 음성 인식 시스템은 입력되는 음성에 전처리 과정을 거쳐 잡음 등을 제거하고 명령을 인식하기 때문에 백색 소음 속에 숨어있는 사람의 음성을 구분 가능

10) Carlini N., et al. "Hidden Voice Commands." USENIX Security Symposium, 2016.

- 정책 담당자는 AI 전문가와 협의하여 AI 연구개발을 저해하지 않으면서 AI 악용을 방지·완화할 수 있는 정책을 마련하고, AI의 위협에 관한 논의 활성화 방안 수립
- 장기적 권장 사항은 AI 전문가와 정책 담당자 등이 지속적으로 연구하고 발전시켜 나가야할 연구 과제를 제시
- (사이버안전보장공동체 구성) 레드팀[11]을 구성해 AI 시스템의 보안 취약점을 찾아서 해결하거나 취약점 검사 도구 개발 등을 수행
- (연구 결과 공개) AI 연구 결과의 악용 방지를 위해 연구 결과에 대한 위험 평가, 결과 공개 범위 등에 대해 논의
- (책임 문화 구축) 안전한 AI 환경 조성을 위해 AI 전문가들이 지켜야할 윤리·사회적 책임에 대한 교육 체계 마련
- (기술적·정책적 해결책 개발) 사생활 보호를 위한 조치, AI 시스템 모니터링, AI 관련 규제 등 기술적·정책적 해결 방안 개발

□ 결 론

○ AI를 활용하여 기존 공격 방식을 고도화하거나 새로운 방식의 공격을 수행할 수 있으며, 동시에 AI 시스템을 교란시키는 방식의 공격 등이 등장 가능

○ 현재 금융권에서도 업무자동화, 금융서비스, 신용평가 등에 AI를 도입[12]하고 있으며, 이에 따라 AI로 인해 발생 가능한 보안 위협에 대해 지속적인 모니터링 필요

11) 시스템을 점검, 보완하기 위하여 시스템의 취약점을 찾고 공격하는 역할을 하는 팀
12) 국내·외 금융권 머신러닝 도입 현황, 금융보안원, 2017.

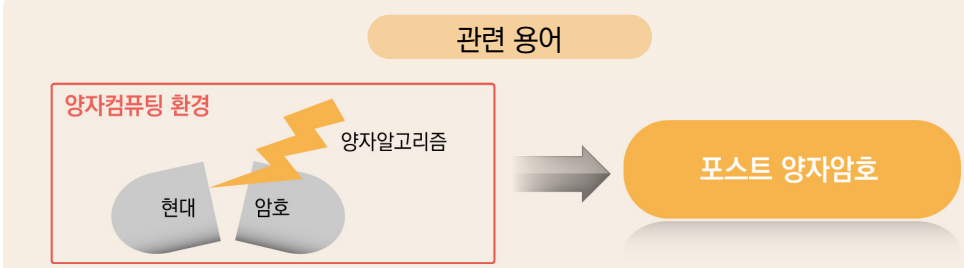
양자컴퓨팅과 포스트 양자암호 동향

□ 개 요

○ 현대 암호의 안전성은 일반 컴퓨팅 환경에서 일정 시간 내에 해독이 불가능한 수학적 난제에 기반

○ 하지만 양자컴퓨터의 개발이 가시화되면서 전문가들은 양자컴퓨터를 활용한 고속 연산 알고리즘(양자알고리즘)에 의해 현대 암호[1]의 안전성 저하를 우려[2]

○ 이에 따라 양자컴퓨터를 사용한 공격에도 안전한 포스트 양자암호(Post-quantum cryptography) 개발이 암호학계에서 관심을 받고 있음



- (양자컴퓨터) 양자의 역학적 특성(얽힘, 중첩 등)을 이용해 초고속 연산이 가능한 미래형 컴퓨터
- (양자알고리즘) 양자컴퓨터에서만 사용할 수 있는 연산으로서, 특정 분야에서 초고속 연산을 수행하는 알고리즘
- (포스트 양자암호) 현대 암호 알고리즘과 달리, 양자컴퓨터로 암호를 해독하는 환경에 안전한 암호 알고리즘

1) 공인인증서 내의 RSA 암호, IoT 기기 내의 ECC 기반 암호 등
2) 양자 컴퓨터가 실용화 되지 않는 이상 현재 암호시스템은 안전하지만 컴퓨팅 및 해킹 기술의 발전을 예측하는 것은 사실상 불가능에 가깝기 때문에 보안 관련 분야는 항상 선제적 대응을 해야한다.(출처: KISA '최종연구보고서' 양자컴퓨팅 환경을 고려한 현대암호 안전성 연구)

□ 양자알고리즘이 현대 암호에 미치는 영향

양자알고리즘

양자알고리즘은 양자컴퓨터에서만 연산 가능한 특수 목적의 알고리즘으로 대표적인 알고리즘은 Grover, Shor알고리즘이 있음

① Grover 알고리즘[3]은 정렬되지 않은 데이터베이스에서 특정 조건을 만족하는 데이터를 찾는 알고리즘이며 양자컴퓨터를 이용한 검색(search)에 탁월한 성능을 갖는 알고리즘

② Shor 알고리즘[4]은 수학적 난제에 해당하는 인수분해 문제를 빠른 시간 안에 풀 때 활용되는 알고리즘

○ 현대 암호에 적용된 수학적 난제의 일부는 양자알고리즘으로 해독 할 때 합리적인 수준(연산량, 비용, 시간 등)에서 해독 가능

① Grover 알고리즘은 특정 값을 빠르게 찾는 특성을 통해 경우의 수 검색으로 대칭키와 단방향 해시함수의 입력 정보를 찾아[5] 낼 수 있음

- Gover 알고리즘에 대응하기 위해 양자알고리즘의 해독 성능을 고려하여 대칭키 길이(사이즈)와 해시함수의 출력 길이(사이즈)가 증가되어야 함

② Shor 알고리즘은 인수분해 문제를 빠른 시간 안에 효과적으로 풀 수 있는 알고리즘이므로 인수분해 문제에 기반한 공개키 방식의 암호에서 비밀키가 유출 될 수 있음

- 인수분해, 이산대수 문제가 아닌 새로운 구조에 기반한 공개키 알고리즘을 개발해야 함

3) Grover L.K., "A fast quantum mechanical algorithm for database search", 28th Annual ACM Symposium, 1996
4) S.J.Lomonaco Jr. "Shor's Quantum Factoring Algorithm", American Mathematical Society, 2002
5) D.J. Bernstein, "Cost Analysis of Hash Collisions: Will Quantum Computers Make SHARCS Obsolete?", 2009

표 1 양자알고리즘이 현대 암호에 미치는 영향 (NISTIR 8105 기준 재구성)

구분	현대 암호 알고리즘	목적	영향
대칭키 암호	AES, DES, ARIA, SEED 등	암호화	• Grover 알고리즘의 빠른 검색으로 대칭키를 찾아냄 • 대칭키의 길이(사이즈)를 2배 증가
단방향 함수	SHA256 등	해시 함수	• Grover 알고리즘의 빠른 검색으로 입력정보를 찾아냄 • 출력 길이(사이즈)를 3배 증가
공개키 암호	RSA	서명, 키설정	• Shor 알고리즘의 빠른 인수분해로 비밀키를 찾아냄 • 새로운 구조에 기반한 알고리즘 개발이 필요
	ECDSA, ECDH, EC-KCDSA (타원곡선암호)	서명, 키교환	
	DSA, KCDSA (유한체암호)	서명, 키교환	

○ 현대 암호 알고리즘 중 대칭키와 단방향 함수는 각각 키와 출력 길이 증가로 양자알고리즘에 의한 영향을 감소시키고 안전성을 보장할 수 있으나,

- 공개키 암호의 경우 구조적 문제로 새로운 구조에 기반한 암호시스템 개발이 필요

□ 포스트 양자암호(Post-quantum cryptography) 동향

○ 암호학계에서는 양자컴퓨터가 상용화된 이후에도 안전*하게 이용할 수 있는 암호시스템인 '포스트 양자암호' 개발에 관심

* 암호시스템의 기반문제[6]를 위협하는 새로운 '양자알고리즘'이 개발되지 않는 한 유효한 이론적 암호해독 방법이 없는 상태

- 포스트 양자암호는 양자의 특성을 이용한 큐비트 대신 고전비트(0 또는 1)를 사용하므로 일반 컴퓨팅 환경에서 사용가능

6) 기반 문제: 다변수다항식, 부호, 격자, 해시 충돌쌍 등 공개된 정보로 비공개 정보에 대한 유추가 어려운 문제

○ 포스트 양자암호의 대표적인 알고리즘은 다음과 같으며, 대부분 양자 알고리즘의 영향으로 새로운 설계가 필요한 공개키 암호에 해당

표 2 포스트 양자암호의 대표적인 알고리즘과 특징 (KISA[10], 위키피디아 자료 재구성)

분야	설명	대표적인 알고리즘	특징
다항식기반	수학적으로 특정 조건을 만족하는 집합에서 다변수 함수를 푸는 것이 어려움을 기반으로 하는 암호시스템	Rainbow	• 서명 사이즈 작음 • 키 사이즈 큼
코드 기반	오류수정 코드[7]에 기반하는 암호시스템	QC-MDPC, Wild McEliece	• 암·복호화 속도 빠름 • 키 사이즈 큼
격자 기반	수학적으로 어떤 조건을 만족하는 집합에서 특정 문제를 푸는 것이 어려움을 기반으로 하는 암호시스템	SS-NTRU, NTRU Prime, LWE-Frodo	• 다양한 응용 존재 • 속도가 빠름 • 변수 설정 문제
Isogeny[8] 기반	수학적으로 어떤 조건을 만족하는 집합에서 특정 값을 찾는 것이 어려움을 기반으로 하는 암호시스템	SIDH	• 간단한 구현 • 연산 속도 느림
해시 함수 기반	해시 함수의 안전성을 기반으로 한 전자서명 시스템[9]	XMSS, SPHINCS	• 안전성 증명 가능 • 서명 사이즈 큼

○ 각 포스트 양자암호가 가진 특징 중 단점을 줄이고 장점을 부각시키는 방향으로 연구가 진행 중임[10]

- 다항식, 코드기반 분야의 경우 키 사이즈를 감소시킬 수 있는 알고리즘에 대해 연구를 진행 중
- 코드기반 분야의 경우 암호화에 비해서 복호화가 느리기 때문에 복호화 속도 향상 방안에 대해 연구를 진행 중

---

7) 메시지와 추가 정보를 같이 수신하게끔 하여 전송 중에 생기는 오류에도 올바른 메시지를 복원할 수 있도록 하는 기법
8) [수학용어] Isogeny(아이소제니, 등원사상): 특정 조건을 만족하는 집합 사이의 특수한 함수
9) 각각의 적절한 해시함수를 이용하여 서로 다른 해시 기반 서명 체계를 갖춘 시스템으로서 사용되는 해시함수의 충돌 저항성에 의해 안전성을 보장
10) KISA, 양자컴퓨팅 환경을 고려한 현대암호 안전성 연구, 2016

- 격자기반 분야의 새로운 Ring[11] 구조를 기반으로 한 알고리즘이나 Ring을 사용하지 않는 standard-LWE[12] 기반의 암호 시스템에 대한 연구를 진행 중
- 서명 크기가 작은 stateful[13] 구조 알고리즘 개발

○ 美 표준기구 NIST에서는 2016년 12월부터 2017년 11월까지 포스트 양자암호 표준화를 위한 공모를 진행하였음

- 2018년부터 5년간 제출된 신기술을 분석하여 검증하고 그 후 2년 간 임시 표준 개발에 착수 할 예정

□ 결 론

○ 금융권에서는 거래정보 및 주요 고객정보의 기밀성과 무결성 등을 위해 암호모듈이 다방면에 사용되고 있음

○ 양자컴퓨팅의 발전과 새로운 양자알고리즘의 개발로 현 금융권에 적용된 현대암호의 안전성이 저하될 우려가 있으므로,

○ 양자컴퓨터가 현대암호에 미치는 영향을 최소화하고, 대응할 수 있도록 사전에 포스트 양자암호 등에 대해 연구 결과를 주시할 필요가 있음

11) [수학용어] 추상대수학에서 덧셈과 곱셈이 정의된 대수 구조의 하나
12) LWE(Learning with Errors): search LWE와 decision LWE로 분류 가능, search LWE는 LWE 샘플로부터 비밀 벡터를 찾는 문제, decision LWE는 LWE 분포와 랜덤한 분포 사이를 구분하는 문제
13) 보안을 위해 문서별로 서명할 때마다 새로운 키 쌍을 생성해야하는 Stateful 스킴의 반대 개념이며, 대표적인 stateless 서명구조로는 2015년에 제안된 SPHINCS가 있음

최신 바이오 인식 기술의 동향 및 활용 사례

□ 개요

○ 바이오(생체) 인식은 생체 정보나 행동 특성을 사용해서 사람을 인식하는 것으로 본인 확인 용도로 활용되고 있음

○ 최근 바이오 인식 기술은 비접촉 방식, 개인 단말사용, 인공지능 기술의 접목 등 사용자 편의성과 보안성을 높이기 위한 방식으로 발전

- 초기 바이오 인식 기술은 접촉 방식으로 공용 단말기를 사용 하는 환경 등에 대한 사용자의 심리적 거부감이 있었으나,
- 바이오 인식 기술이 스마트 폰과 같은 개인 단말기에 적용되면서 사용자의 심리적인 거부감이 감소되고 동시에 사용자의 편의성이 증가하게 됨

○ 따라서 최근 각광받고 있는 바이오 인식 기술인 지문카드, 얼굴인식, 정맥 인식 방식에 대해 해당 기술의 동향과 활용 사례를 살펴보고자 함

□ 바이오 인식 기술 유형 및 활용 사례

(가) 지문카드

○ 초기 지문카드는 지문 정보가 저장된 지문카드와 지문 인식용 단말기가 필요했지만, 최근에는 지문카드에 지문을 인식하는 센서가 탑재되어 별도의 지문인식용 단말기를 필요로 하지 않음[1)]

1) The Rise of Biometric Cards, Edition January 2018, embeddedsecuritynews.com

○ 지문카드는 지문 템플릿[2]의 저장 위치, 지문을 인식하는 센서 위치, 지문의 정상 여부를 판독하는 위치에 따라 유형이 분류됨

- 지문카드의 유형은 Template on Card(ToC), Match On Card (MoC), Biometric System on Card(BSoC)로 분류

표 1 지문카드 유형

유형	위치(저장/인식/판독)			본인 확인 시 이동되는 정보 / 이동 방향
	지문 템플릿 저장	지문 인식센서	지문 판독	
① ToC	IC카드	단말기	단말기	템플릿 정보 / IC카드 ➜ 단말기
② MoC	IC카드	단말기	IC카드	지문 정보 / 단말기 ➜ IC카드
③ BSoC	IC카드	IC카드	IC카드	-

① (ToC) 지문 인식센서가 단말기에 탑재되어 지문 인식과 지문 판독이 단말기에서 진행

- 본인 확인(지문 판독)을 위해 지문 템플릿은 IC카드에서 단말기로 이동되므로 이동 과정 중 정보유출에 대비가 필요

② (MoC) 지문 인식센서가 단말기에 탑재되어 있어 지문 인식은 단말기에서 진행되나, IC카드에 비교모듈(지문템플릿과 인식된 지문정보 비교)이 탑재되어 있어 IC카드에서 판독

- 지문 판독을 위해 단말기에서 인식된 지문 정보가 IC카드로 이동되므로, 이동 과정 중 정보유출에 대비가 필요

③ (BSoC) 지문 인식, 지문 템플릿, 지문 판독 모두 IC카드에서 저장 및 연산되어 지문관련 정보의 이동이 없어 생체 정보유출에 대한 위협이 적음

※ 다만, 지문카드에서 인증 결과값 전송에 대한 대비는 필요

○ 지문카드 중 BSoC는 ToC와 MoC에 비해 보안성이 높고, 지문 인식을 위해 별도의 단말기를 교체할 필요가 없어 그 활용도가 높을 것으로 예상

2) 생체 특징을 추출하여 등록 또는 저장된 생체 데이터, 센서를 통해 취득된 생체 이미지 정보를 부호화 한 것이며 효율적인 저장과 정합이 가능하도록 되어 있음(TTA IT용어사전)

- EMV는 2017년 남아프리카 공화국에서, 2018년 1월 미국에서 시범 사업을 시작하였으며, 국내 카드사는 시스템 연동 작업을 진행 중[3)]
- 중국 인민은행은 56억장의 기존 카드를 BSoC카드로 교체하는 작업을 시작[4)]

(나) 얼굴인식

○ 초기 얼굴인식 기술은 본인 확인 용도로 활용 시 인식률이나 정확도가 낮아 적용분야가 한정적이었음

- 얼굴인식 기술은 비접촉식 센서의 사용 등으로 다른 인식 기술에 비해 사용자 편의성이 높은 기술로 평가받으나,
- 얼굴이 인식될 때 주변 환경에 따라 얼굴의 색깔, 모양 등이 변화되어 인식률 또는 본인 확인 시 인증 정확도가 낮아지는 단점이 존재
  - 예를 들어 적외선 카메라 영상, 2차원 영상으로 인한 얼굴인식 기술은 조명, 표정, 노화 등 얼굴변화에 따라 인식률이 떨어짐
- 따라서 초기 얼굴인식 기술은 본인 확인 시 정확도가 낮고 인식 오류에 대한 위험이 적은 분야*에 주로 활용[4)]

  * 소비자 식별 후 맞춤형 광고 송출 등 마케팅 분야

○ 최근의 얼굴인식 기술은 카메라가 탑재된 스마트폰이나 ATM에 탑재되어 본인 확인 용도로 활용되고 있는 추세[5)]

- 아이폰은 Face ID(얼굴 이미지(템플릿))를 생성하여 안전한 저장 장소에 보관하고, 특수 카메라를 통해 사람의 얼굴을 입체적으로 인식하여 본인 확인 등으로 사용[6)]
- 미국의 USAA는 스마트뱅킹 시 본인 확인을 위한 얼굴인식 기술을 도입[7)]하였고, 중국의 알리바바, 농업 은행도 본인 확인을 위한 용도로 활용[8)]

---

3), 4) 전자신문, 지문만 인식하면 끝...간편결제 끝판왕 생체인증 신용카드 등장, 2018.02.21
4) CIOKOREA, 새로운 고객참여와 경험, 안면 인식이 주도하는 마케팅 혁신, 2016.08
5) TECHM, 아이폰X를 통해 본 안면인식의 세계, 2017.11
6) Apple, Face ID Security, 2017.11
7) 전자금융과 금융보안, 바이오인증 최신 활용 및 보안 동향, 2016.07

- 알리바바는 얼굴인식을 사용한 결제 서비스 출시('17.09)

(절차) 매장에서 원하는 메뉴 선택 ➜ 안면인식 진행 ➜ 휴대번호 입력 ➜ 미리 등록해 놓은 얼굴 사진과 기계에 찍힌 얼굴 비교

- 농업 은행은 얼굴인식기술을 ATM에 적용[9]('17.09)

(절차) 얼굴인식 출금 시스템 선택 ➜ 안면인식 진행 ➜ 휴대폰 번호, 인출금액, 비밀번호 입력 ➜ 현금 인출

○ 또한 얼굴인식 시스템의 인식률과 정확도를 높이기 위해 인공지능과 접목

- 인공지능은 환경에 따라 변화하는 사람의 얼굴을 데이터화하여 학습함으로써 사용자의 다양한 외모 변화에도 본인 확인을 위한 정확도를 높일 수 있게 됨[10]

- 예를 들어 딥러닝의 학습 과정을 통해 실제 얼굴 유형과 유사한 3차원 영상을 만들어 입체적인 얼굴 정보를 기반으로 본인을 확인[11]
- 또한 다양하게 변화하는 이용자의 얼굴을 학습하여 본인을 확인[12]

(다) 정맥인식

○ 정맥인식 기술은 다른 인식 기술에 비해 하드웨어 구성이 복잡하고 소형화가 어려워 고비용 투자가 요구되었으나 최근에는 소형화된 정맥 인식 시스템이 개발되고 있는 추세[13]

- 정맥인식 기술의 주요 특징은 사용자의 신체 훼손 등이 있어도 인식 기술을 사용할 수 있으며, 다른 인식 기술에 비해 본인 확인을 위한 정확도가 높음

- 예를 들어 지문인식은 지문이나 손가락이 없는 사람 또는 젖은 손 등

8) 보안뉴스, 얼굴인식 기술, 중국인의 일상에 '성큼', 2018.03
9) 중국을 알리고 세계를 보도하다 '얼굴 스캔으로 현금 인출, 중국 안면인식 시대 도래', 2017.09.
10) Apple, Face ID Security Guide, 2017.11
11) NIPA 이슈리포트 2017제20호 지능정보시대 안면인식 기술에 주목하라
Apple 홈페이지, Face ID에 적용된 첨단 기술에 관하여
12) Apple, Face ID Security Guide, 2017.11
13) 디지털 타임스, '지정맥' vs '장정맥' 생체인증 기술 공방... 뭐가 다르길래, 2017.07
Fujitsu, 손바닥 정맥 인증 솔루션, www.fujitsu.com

외적 영향에 따라 등록 실패율*이 높으나 정맥인식 기술은 외적 영향이 적어 등록 실패율이 낮음

○ 이러한 장점으로 인해 정맥인식 기술은 본인 확인에 적합한 인식 기술로 평가받고 있고[14] 최근에 은행의 ATM기, 카드의 결제서비스 등에서 활용 중

- 2015년 이후 신한은행, 국민은행, 대구은행 등에서는 특수 지점에 스마트 ATM기를 설치하여 서비스 중
- 2017년 롯데카드는 장정맥 인증을 활용한 결제 서비스를 출시하고 계열사와 추가 가맹점 제휴를 통해 서비스를 확대
- 국내 공항에서는 국내선 항공기 탑승을 위한 본인 신원확인 절차에 손바닥 정맥 인증 기술이 도입[15]

□ 결 론

○ 초기 바이오 인식 기술은 위생과 정보유출 등에 대한 우려로 사용자의 심리적 거부감[16]이 높은 기술이었으나, 개인 단말기 사용 등으로 인해 이를 해소시키고 있음

○ 또한, 최근 인식 기술은 인공지능, 시스템의 최적화 등으로 인식률과 본인 확인에 대한 정확도를 높이면서 고성능의 새로운 기술이 지속적으로 개발

○ 하지만 새로운 기술이 개발될수록 바이오 정보 위조 및 유출에 대한 보안 위협이 수반될 것으로 예상

○ 따라서 기술 변화에 따라 바이오 정보 위조 및 유출에 대한 보안위협을 사전에 예측하고 시스템 설계 시 반영할 필요가 있음

---

14) 정보통신기술진흥센터 기술정책단 2017-44 ICT Brief
15) MBC 뉴스, '29일부터 지문·정맥 인증으로 국내선 항공기 탑승', 2018.1.22
16) 바이오인증기술 최신 동향 및 정책과제, 한국은행, 2016.08

국내·외 금융권 챗봇 활용 현황 및 주요 보안고려사항

□ 개 요

○ 챗봇(Chatbot)은 사람의 언어를 이용하여 사람과 대화를 하는 컴퓨터 프로그램으로, 주로 고객과의 상담을 위해 다양한 분야에서 활용

- 챗봇의 장점은 ①인건비 및 고용관리비용 저렴, ②업무 중단없이 고객 응대 가능 ③고객의 필요함을 신속하게 분석 등이 해당

○ 금융권에서는 최근 비대면 거래가 활성화됨에 따라 금융상품 설명 및 판매·결제 등에 챗봇을 이용한 고객응대가 증가하는 추세

- 고객 입장에서도 금융상품에 대한 궁금증을 언제든 바로 해소할 수 있어 향후 챗봇을 활용한 금융서비스는 더욱 확대될 것으로 예상

○ 챗봇은 금융수요자에게 신속·편리한 서비스를 제공할 수 있는 반면 개인정보 유출과 같은 위협이 유발될 수 있어 발생 가능한 보안 위협을 예측하고 대응 방안을 고려할 필요

□ 국내·외 금융권 챗봇 활용 현황

○ 국내 주요 금융회사는 자체 플랫폼 또는 카카오톡 등 외부 플랫폼을 이용하여 챗봇 기반의 금융서비스를 고객에게 제공 중에 있으며, 챗봇 도입 현황은 다음과 같음

표 1 국내 금융권 챗봇 주요 도입현황 (2018년 6월 기준)[1)]

	기관명	서비스명	도입시기	플랫폼	AI 적용
은 행	농협은행	금융봇	2016.10.	카카오톡	X
	우리은행	위비봇	2017.9.	자체 플랫폼	○
	신한은행	쏠	2018.2	자체 플랫폼	○
증 권	대신증권	벤자민	2017.2	자체 플랫폼	○
보 험	라이나생명	-	2017.06	카카오톡 등	○
	DB손해보험	알림톡	2016.12	카카오톡	X
카 드	현대카드	버디	2017.8.	자체 플랫폼	○
	신한카드	모바일 챗봇	2017.6.	네이버 등	X
저축은행	웰컴저축은행	웰컴봇	2017.9.	카카오톡	○
	OK저축은행	오키톡	2017.9.	카카오톡	X
	JT친애저축은행	-	2017.8.	카카오톡	X
	KB저축은행	케비봇	2017.12.	자체 플랫폼	X

○ 국외 주요 금융회사는 보험업권에서 2007년 최초로 챗봇을 도입하였으며 점차적으로 다른 업권에서도 도입하기 시작하였음

표 2 국외 금융권 챗봇 도입현황[2)]

업 권	기관명	서비스명	도입시기	AI 적용
은 행	Bank of America(미국)	ERICA	2016.10	○
	Capital One(미국)	ENO	2017.03	○
	Ally Bank(미국)	Ally Assist	2015.05	○
	Absa Bank(남아공)	-	2016.04	○
	Mitsubishi(일본)	MAI	2016.03	○
	HSBC(영국)	Amy	-	○
	Hang Seng Bank(홍콩)	HARO, DORI	-	○
	J.P.Morgan(미국)	COIN	2016.06	○

1) "유비원 기고 | 인공지능(AI) 챗봇의 전망과 활용을 위한조건", CIO Korea, 2017 등 국내 언론보도 참조
2) https://www.chatbots.org 및 해외 언론보도 등 참조

업 권	기관명	서비스명	도입시기	AI 적용
은 행	DBS Bank(싱가폴)	-	2017.01	○
	Royal Bank of Scotland(영국)	Luvo	2016.09	○
	Lloyds Banking Group(영국)	How To	2010.10	○
	Santander U.K(영국)	-	2017.02	○
보 험	AXA(홍콩)	Alex	2017.09	○
	HDFC Life(인도)	-	2017.03	○
	Co-op Insurance(영국)	Mia	2011.10	X
	Link4(폴란드)	Magda	2012.09	X
	Allianz(호주)	Allie	2012.03	X
	RBC Insurance(캐나다)	Arbie	2011.03	X
	Nationale-Nederland(네덜란드)	Nienke	2011.02	X
	Crédit Agricole(프랑스)	Marc	2007.12	X
카 드	MasterCard(미국)	Kai	2016.10	○
	American Express(미국)	-	2016.09	○

○ 국내·외 주요 금융회사를 대상으로 챗봇 활용 현황을 조사한 결과, 챗봇은 시나리오 기반의 챗봇과 AI기술을 적용한 챗봇으로 분류될 수 있음

- 시나리오 기반의 챗봇은 고객과의 대화 시나리오를 사전에 정의한 후 사용자가 입력하는 키워드에 따라 금융상품 소개, 영업점 안내 등 간단한 업무 위주의 서비스를 제공
  - 동 챗봇은 제한적 질문에 대해 정해진 답을 출력하기 때문에 AI기술을 적용한 챗봇보다 새로운 보안위협이 미비할 것으로 예상
- AI기술을 적용한 챗봇의 경우 복잡한 질문에도 응답할 수 있고 자기학습도 가능하여 다양한 서비스 제공이 가능
  - 일부 국외 금융회사는 고객 상담뿐만 아니라 송금, 카드분실 신고·정지 등 국내에 비해 다양한 서비스를 제공
  - 고객의 개인정보 및 중요정보 유출, 챗봇의 자기학습으로 인한 이상동작 가능성 등 새로운 보안위협이 예상

챗봇에 AI 활용이 필수인지 여부

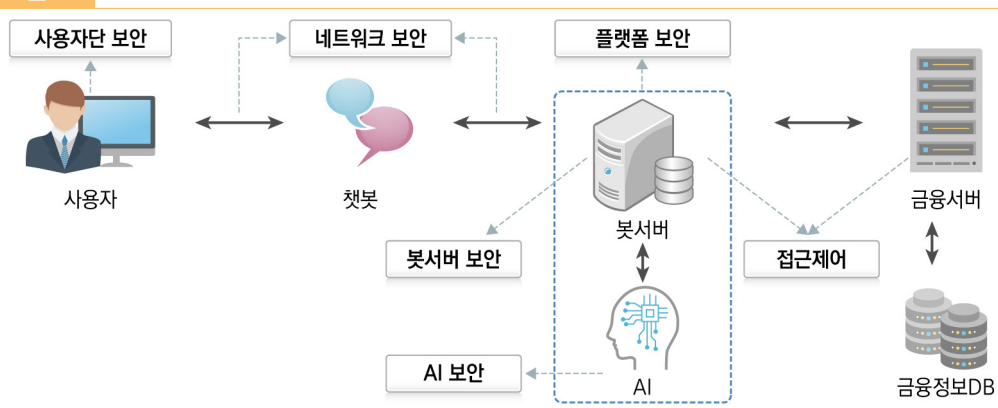
- AI 기능이 챗봇의 성공을 보장하지는 않으며 챗봇의 목적에 따라 AI 기능 활용 시 장·단점을 고려하여 활용 여부를 결정해야 함[3)]
  - (장점) 자연어 처리 및 복잡하고, 다양한 업무 대응과 정보 제공 가능
  - (단점) 사용자의 질문에 맞춰 답변하므로 명확한 정보 전달 및 영업 등 챗봇의 고유 목적을 효율적으로 달성하도록 구현하는 것이 어려우며, 개인정보 유출 등의 보안 위협이 증가

※ 네이버 톡톡서비스의 경우 AI 기능 활용이 매출 향상에 도움이 되지 않는다고 판단해 시나리오 기반 챗봇 구현[4)]

□ 챗봇 기반 금융서비스의 주요 보안고려사항

○ 챗봇 기반의 서비스는 일반적으로 사용자, 챗봇, 봇 서버, 금융서버, 금융정보DB로 구성되어 있고 구조는 아래 그림과 같음
- 챗봇의 구성요소별 발생 가능한 보안위협을 파악하고 이에 대한 적절한 대응방안 마련이 필요
- (주요 보안고려사항) ①사용자단 보안, ②봇서버 보안, ③플랫폼 보안, ④접근 제어, ⑤네트워크 보안 및 ⑥AI 보안

그림 1 챗봇 구조 및 보안기능



3) "Designing Bots:Creating Conversational Experiences", Amir Shevat 외 1명, 2017
4) "네이버톡톡, 간편주문챗봇 만든 이야기", 네이버, 2017

○ (사용자단) 사용자가 비정상적인 챗봇을 설치 및 사용할 경우, 피싱 또는 파밍 공격 등으로 보안위협이 발생할 수 있으며, 이로 인해 사용자의 주요 정보 유출 가능

- 금융회사는 챗봇에 대한 식별 기능을 제공하고, 챗봇을 통해 입력되는 중요정보를 사용자 단말기에 저장하지 않거나 불가피한 경우 안전한 암호알고리즘을 적용

○ (플랫폼) 카카오톡 등 타사 플랫폼을 이용하여 서비스를 제공할 경우 해당 플랫폼의 보안취약점은 챗봇에도 반영되므로, 플랫폼의 보안취약점 및 시큐어코딩 점검결과 등을 확인

○ (AI보안) AI기술 적용 시 고객이 입력한 단어에 대해 AI가 의도치 않은 행위를 수행하여 개인정보유출 등의 보안위협이 발생

- AI 행위에 제한을 두어 이상행위 수행을 제한하고 AI 대답에 개인정보 포함여부 확인 등 필터링 수행

○ 그 외에 사용자 계정과 봇서버 보안 및 접근제어, 네트워크 보안, 웹서버 보안 등 금융서비스에서 일반적으로 고려되는 보안사항에 대해 대비가 필요

□ 시사점

○ 금융산업에 적용되는 챗봇 중 AI기술을 적용한 챗봇은 아직까지는 연구, 개발 및 적용이 초기단계이므로, 보안요소를 신중히 고려하여 금융서비스에 반영 필요

- 네트워크 보안, 웹서버 취약점뿐만 아니라 AI기술, 챗봇 플랫폼 등에 의한 보안위협을 파악하고 대응 방안을 마련하여 안전한 금융서비스 구축

머신러닝을 활용한 해외 기업의 악성코드 탐지 연구 소개

□ 개 요

○ 보안 전문가에 의해 정의된 악성코드 탐지 규칙만으로는 꾸준히 증가하고 있는 신종·변종 악성코드[1]를 효과적으로 탐지하는 것이 어려움

- 이에 산·학계에서는 악성코드의 규모와 다양성을 고려하여 머신러닝을 활용한 악성코드 탐지를 연구

○ 본 보고서에서는 글로벌 회사인 카스퍼스키 랩(Kasperskey Lab)과 앤비디아(Nvidia)에서 공개한 머신러닝 기반의 악성코드 탐지 연구를 간략히 소개[2]

□ 머신러닝 기반 악성코드 탐지

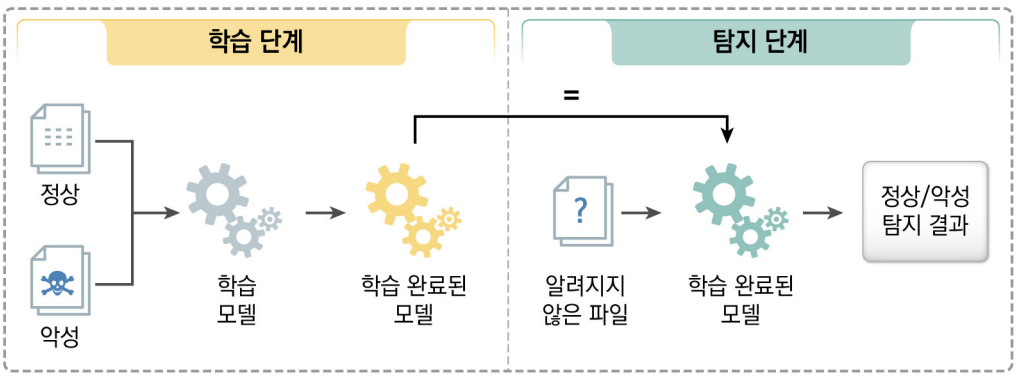
○ 머신러닝 기반의 악성코드 탐지란 정상파일 및 악성코드가 포함된 파일(이하 '악성코드')로 학습 모델을 학습시킨 후, 학습된 모델로 의심스러운 파일의 악성 여부를 탐지하는 것(〈그림 1〉 참고)

- (학습 단계) 학습 모델을 파일들의 특징정보(문자열, 명령어, 바이트 정보, API 호출 기록 등)와 레이블(정상/악성코드)로 학습시킴으로써 모델이 악성코드 탐지에 최적화 되도록 함
- (탐지 단계) 학습된 모델을 이용하여 입력된 파일이 정상파일인지 악성코드인지를 구별

---

1) http://www.av-test.org/en/statistics/malware,
Threats Report, McAfee Labs, 2018.5.
2) Machone Learning for Malware Detection, Kasperskey Lab,
Edward Raff, Malware Detection by Eating a Whole EXE, NVIDIA, 2017.

그림 1 머신러닝을 활용한 기본적인 악성코드 탐지 시스템 예시



○ 카스퍼스키 랩과 앤비디아는 〈그림 1〉과 유사한 머신러닝 기반의 악성코드 탐지 시스템을 개발

- 시스템 설계 시 악성코드의 다양성과 규모, 분석 업무의 효율 등을 감안하여,
- 시스템이 일반성, 강건성(Robust), 확장성, 처리율, 설명가능성 등의 특징을 갖도록 함

표 1 카스퍼스키 랩과 앤비디아에서 시스템 설계 시 고려한 주요 요소

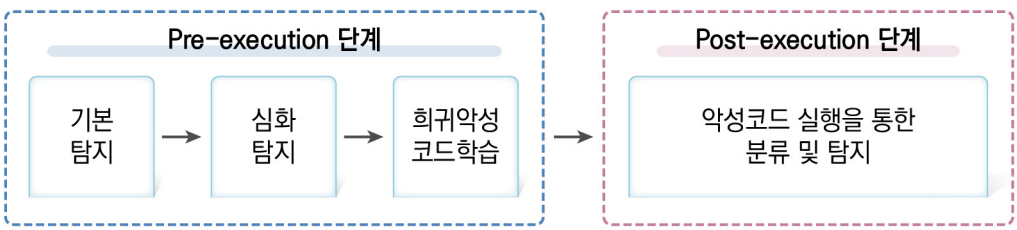
고려 요소	설 명
일반성	• 시스템이 머신러닝에 사용된 데이터셋에 대해서만 좋은 탐지 성능을 보이는 것이 아니라 새로운 악성코드에 대해서도 우수한 탐지 성능을 보이도록 해야 함
강건성	• 신종 악성코드뿐만 아니라 기존의 것을 일부 변형한 악성코드에 대해서도 탐지가 가능하도록 해야 함
확장성 및 처리율	• 악성코드의 수가 급격히 증가함에 따라 시스템도 확장 가능해야 하며, 처리율 역시 보장 되어야 함
설명가능성	• 입력된 파일이 악성코드로 분류된 경우, 이에 대한 분류 원인(예: 파일의 메타정보, 명령어 등)을 제공할 수 있어야 함

□ 카스퍼스키 랩의 악성코드 탐지 실험

○ (실험 방향) 카스퍼스키 랩은 악성코드 탐지 과정을 여러 단계로 구성하여 각 단계에서 머신러닝을 활용한 파일 학습 또는 악성코드 탐지를 수행

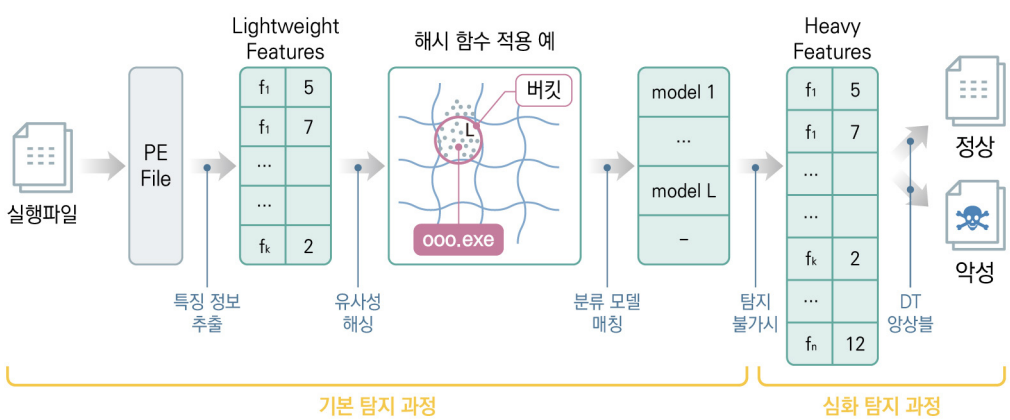
○ (시스템 구성) 악성코드 탐지 과정을 악성코드 Pre-execution(실행 전) 단계와 Post-execution(실행 후) 단계로 구분

그림 2 카스퍼스키 랩의 악성코드 탐지 시스템 구성도



- (Pre-execution(실행 전) 단계) 악성코드 실행 없이 수집 가능한 정보(파일 포맷, 바이트, 추출된 텍스트 등)를 학습하여 악성코드를 탐지
  - 동 단계는 사용되는 악성코드의 정보에 따라 기본 탐지, 심화 탐지, 희귀 악성코드 학습 단계로 나뉨(〈그림 3〉 참고)

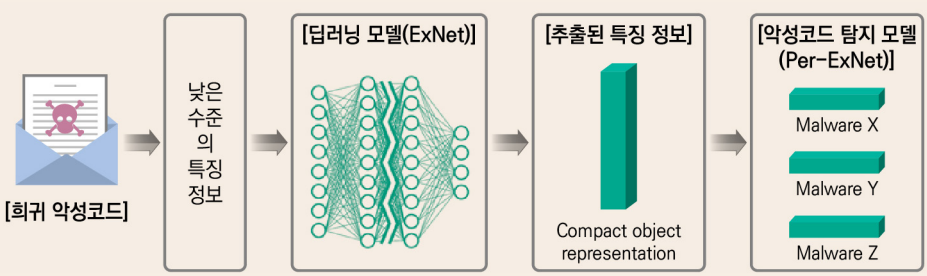
그림 3 Pre-execution(실행 전) 단계의 처리 과정



- (기본 탐지) 실행파일의 기본적인 특징정보(Lightweight Features)로 유사성 해싱(Similarity Hashing) 함수[3]를 학습시킨 후 정상파일과 악성코드를 분류
  - 유사성 해싱 함수는 특징정보의 해싱값에 따라 악성코드를 적절한 버킷에 분류
  - 만일, 버킷이 정상파일과 악성코드가 혼합된 경우 심화 탐지 단계를 수행
- (심화 탐지) 실행파일에서 추출 가능한 모든 특징정보(Heavy Features)로 유사성 해싱 함수를 학습시킨 후 앙상블 알고리즘[4]을 통해 정상파일과 악성코드를 분류
  - 만일, 분류 결과에 정상파일과 악성코드가 혼합된 경우 아래와 같은 희귀 악성코드 학습 단계를 수행

희귀 악성코드 학습

- 희귀 악성코드들을 탐지할 수 있도록 딥러닝 모델(ExNet, exemplar Network)로 이들의 특징정보를 추출하는 단계
  - 추출된 특징정보는 희귀 악성코드 및 이와 유사한 악성코드를 탐지하는 딥러닝 모델(Per-ExNet, Per-exemplar classifiers)에 사용

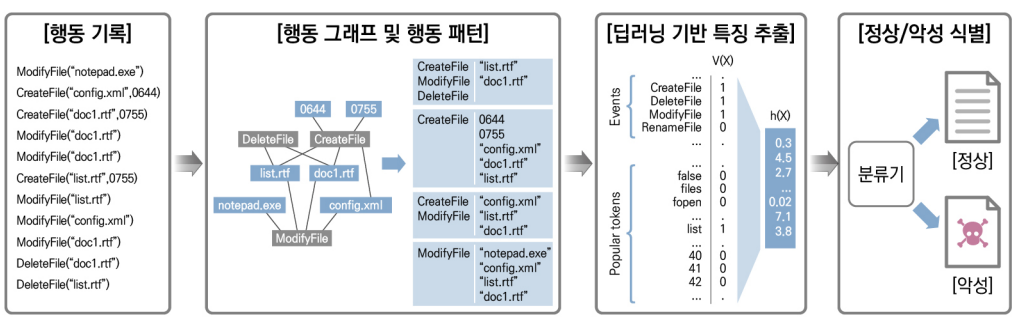


〈딥러닝 모델 기반의 희귀 악성코드 특징정보(패턴) 추출 과정〉

3) 유사성 해싱(Similarity Hashing): 유사한 입력을 같은 버킷에 할당하는 지역민감해싱(LSH)에 학습 개념을 도입한 것. 입력된 파일의 특징정보와 레이블(정상/악성)로 지도학습을 수행하여 악성코드 탐지에 최적화된 해싱 함수를 만듦
4) 의사결정나무 앙상블: 여러 개의 의사결정나무를 학습시켜 다수의 분류 결과를 도출한 후 투표 등의 방식으로 최적의 분류 결과를 찾아내는 방법

- (Post-execution(실행 후) 단계) 암호화, 난독화 등으로 Pre-execution 단계에서 악성코드 분류가 어려운 경우 Post-execution 단계를 수행
  - 동 단계는 악성코드를 실행하여 수집한 정보(발생한 이벤트, 프로세스 행위 기록 등)로 딥러닝 모델을 학습시켜 악성코드를 탐지
    - 악성코드 실행 시 수집되는 프로세스의 동작 기록으로 행동 그래프 및 행동 패턴을 생성하고,
    - 딥러닝 모델로 생성된 행동 패턴의 주요 특징정보를 추출한 후 분류 모델을 거쳐 정상파일과 악성코드를 분류(〈그림 4〉 참고)

그림 4 Post-execution(실행 후) 단계의 수행 과정



○ (실험 결과) 카스퍼스키 랩은 시스템에서 강건성, 확장성, 처리율, 설명가능성을 고려함으로써, 악성코드의 작은 변화에도 탐지 성능(오탐율 등)을 보장(강건성)하고,

- 대량의 악성코드 처리에 적합하며(확장성 및 처리율), 탐지 결과에 대한 담당자의 이해(설명가능성)를 도울 수 있는 시스템을 구축

표 2 카스퍼스키 랩 탐지시스템의 주요 설계 고려 요소

고려 요소	탐지 시스템에 고려 요소를 적용한 방식
강건성	• 입력된 파일은 각 단계를 거치면서 정상/악성으로 분류되는 한편, 제대로 분류되지 않은 파일은 면밀한 분석을 위해 다음 단계로 전달 • 희귀 악성코드의 경우 별도의 학습 단계를 통해 특징정보를 추출하고 추후에 사용함으로써 탐지 가능한 악성코드의 범위를 확장

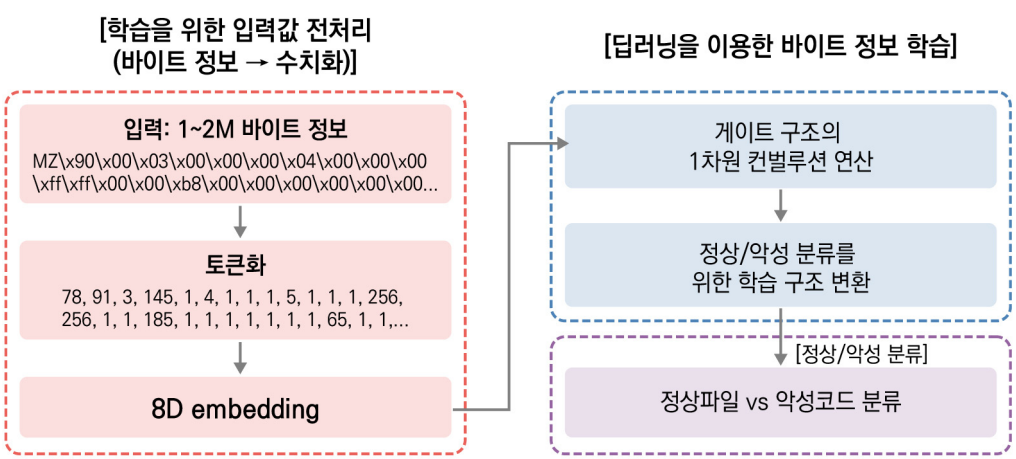
고려 요소	탐지 시스템에 고려 요소를 적용한 방식
확장성 및 처리율	• 악성코드의 탐지 난이도에 따라 기본적인 단계에서 악성코드로 분류되거나, 직접 실행되는 단계를 거쳐 악성코드로 분류되기도 함 • 이는 각 단계에 전달되는 파일의 양을 단계적으로 줄이는 것으로써 모든 악성코드에 동일한 탐지과정이 적용되지 않게 하여 시스템의 확장 가능성과 처리 속도를 높임 • 또한 카스퍼스키 랩은 연산 속도가 빠른 해시 함수를 사용하여 처리 속도를 향상
설명가능성	• 악성코드 탐지에 사용되는 특징정보를 구분하여 학습시킴으로써 탐지 결과가 설명 가능함을 보임 • 예를 들어, 악성코드의 API 함수 사용 정보를 특징정보로 하여 학습할 경우 최종 분류 결과의 도출 근거로 API 함수를 사용

□ 앤비디아의 악성코드 탐지 실험

○ (실험 방향) 앤비디아는 윈도우 실행파일(.exe)의 악성코드 탐지를 위해 파일의 바이트 정보로 딥러닝 모델을 학습시켜 악성코드 탐지를 수행

○ (시스템 구성) 악성코드 탐지를 위해 시스템을 실행파일의 바이트 정보 전처리 단계, 바이트 정보로 딥러닝 모델을 학습시키는 단계, 정상파일과 악성코드를 분류하는 단계로 구성

그림 5 딥러닝 기반의 악성코드 분류 모델(MalConv) 아키텍처

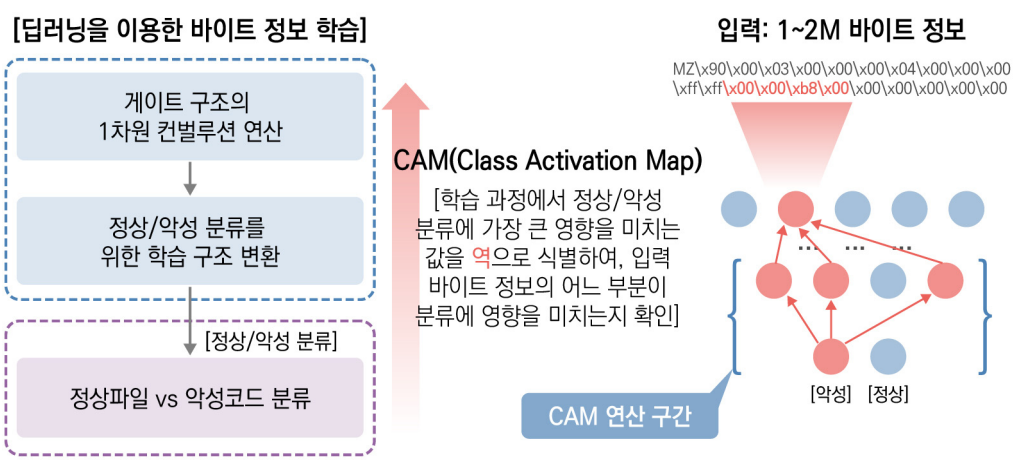


- (학습을 위한 입력값 전처리) 실행파일의 바이트 정보(16진수)를 학습 알고리즘 입력값에 적합한 형태로 변환
- (딥러닝을 이용한 바이트 정보 학습) 합성곱 신경망[5](CNN)에 2개의 컨벌루션 연산을 수행하는 게이트 구조를 적용하고, 정상/악성 분류를 위한 구조를 추가하여 학습
- (정상/악성 분류) 딥러닝 학습 결과를 이용하여 정상파일과 악성코드를 분류

○ (분류 기준 도출) 앤비디아에서는 CAM(Class Activation Map[6]) 방식을 활용하여 실행파일이 악성코드로 분류되게 된 근거를 찾음

- CAM은 정상/악성 분류 단계까지 학습 과정의 연산 결과 중 가장 큰 값을 식별하여 입력된 바이트 정보 어느 부분에 해당하는지를 계산(〈그림 6〉 참고)

그림 6 CAM 방식을 이용한 악성코드 분류에 가장 큰 영향을 미친 바이트 부분 탐색



5) 합성곱 신경망(CNN): 입력 데이터의 특징을 추출하는 다수의 층(layer)과 분류를 수행하는 완전연결층(fully connected layer)으로 구성된 신경망. 특징을 추출하는 다수의 층들은 이전 층에서 전달받은 정보에서 특징정보맵을 생성(합성곱 연산)하는 층과 이를 다음 층으로 넘기기 위해 크기를 축소(풀링 연산)시키는 층으로 구성. 특징 추출이 완료되면 완전연결층을 거쳐 악성코드 분류 등을 수행

6) Zhou, Learning Deep Features for Discriminative Localization, CVPR, 2016.

○ (시스템 테스트) 앤비디아에서는 바이트 블록[7], 파일 메타 정보를 특징 정보로 활용한 학습 모델과 제시한 모델(Malconv)의 정확도를 비교하여 제시한 모델의 타당성을 검증

○ (실험 결과) 앤비디아는 시스템 설계 시 일반성, 강건성, 확장성, 처리율, 설명가능성, 특징정보 의존성을 고려함으로써, 악성코드의 작은 변화에도 탐지 성능(오탐율 등)을 보장(강건성)하고,

- 범용적 시스템을 위해 학습만을 위한 데이터셋을 사용(일반성)하였으며, 바이트 정보만을 사용하여 특징정보 추출 과정을 축소(특징정보 의존성 감소)
- 또한 대량의 악성코드 처리에 적합하며(확장성 및 처리율), 탐지 결과에 대한 담당자의 이해(설명가능성)를 도울 수 있는 시스템을 구축

표 3 앤비디아 탐지시스템의 주요 설계 고려 요소

고려 요소	탐지 시스템에 고려 요소를 적용한 방식
일반성	• 딥러닝 모델 학습에 사용되는 데이터셋을 두 개의 전혀 다른 출처로부터 수집하여 그룹 A, B로 구분 • 두 개의 그룹 A, B 중 하나의 그룹으로만 모델을 학습시키고 다른 그룹으로 성능을 검증하여 모델의 일반성을 향상
강건성	• 바이트 정보를 고정된 길이로 분할하지 않고 파일 전체의 바이트 정보를 학습함으로써, 일부만 변형된 악성코드들도 탐지할 수 있는 가능성을 높임
확장성 및 처리율	• 학습 과정의 계산 복잡도가 바이트 정보 길이에 선형적으로 증가하도록 설계
설명가능성	• 악성코드 탐지에 가장 큰 영향을 미치는 요인을 추적하여 해당 요인이 바이트 정보와 매핑되는 부분을 식별함으로써 탐지 결과가 설명 가능함을 보임
특징정보 의존성	• 바이트 정보만을 사용하여 학습을 위한 특징정보 추출 과정을 축소시켰으며, 이는 특정 특징정보에 대한 의존성을 낮춤

7) 바이트 블록: 바이트 정보를 고정된 길이로 분할한 단위

□ 결 론

○ 글로벌 회사*에서 머신러닝을 활용한 악성코드 탐지 실험을 공개한 것은 사이버보안 분야에 머신러닝의 도입이 구체화되고 있는 좋은 사례

* 사이버보안 분야의 카스퍼스키 랩, 머신러닝 하드웨어 개발 분야의 앤비디아

- (카스퍼스키 랩) 악성코드 탐지를 단계적으로 구성하여 의심스러운 파일에 레이블(정상/악성)을 정함으로서,
  - 최종적으로 보안 전문가가 분석해야하는 악성코드의 양을 줄여 분석 업무의 효율성을 향상

- (앤비디아) 바이트 정보의 부분적인 특징정보가 아닌 전체 바이트 정보를 학습하는 것의 중요성을 기존의 학습 모델(바이트 블록, 파일의 메타 정보 활용)과 비교하여 보임

○ 악성코드 분석 관련 담당자들은 머신러닝을 활용한 새로운 탐지 방식을 통해 악성코드 분석에 필요한 추가적인 유용한 정보를 얻고, 이를 활용할 수 있도록 예의 주시할 필요가 있음

「금융혁신지원 특별법안」 주요 내용 및 시사점

□ 개요

○ 핀테크 산업 육성 등을 위한 「금융혁신지원 특별법안」이 발의*됨에 따라 법안의 주요 내용 및 관련 시사점을 검토

* '18.03.06. 민병두 의원 대표발의 (발의의원 : 총 45명)

□ 법안의 제정 경위

○ 본 법안은 미래 신사업·신기술 혁신 지원을 위해 정부에서 '18.1월 발표한 규제혁신 추진방안*에 포함된 내용

* 「신산업·신기술 분야 규제혁신 추진방안」('18.1.22, 국무조정실)

- '규제 샌드박스' 도입을 위한 4개 분야* 입법 추진내용 中 금융(핀테크) 분야 도입과 관련한 근거 입법에 해당

* ICT 융합(정보통신융합특별법/과기정통부), 핀테크(금융혁신지원특별법/금융위), 산업융합(산업융합촉진법/산업부), 지역형 규제샌드박스(지역특구법/중기부)

[참고 1] 규제 샌드박스(Regulatory Sandbox)란?

- 어린이 놀이터처럼 제한된 환경에서 규제를 풀어(탄력 적용) 신사업을 테스트(시범사업) 하도록 하는 것, 영국에서 핀테크 산업 육성을 위해 최초 시도

○ 금융위는 '17.3월 「금융규제 테스트베드 도입방안」을 마련하여 현행법 허용 범위 內*에서 규제 샌드박스를 지원(1단계)해 왔음

* 비조치의견서 발급, 핀테크 기업의 혁신 금융서비스를 금융회사에 위탁 테스트 등

- 금번 「금융혁신지원특별법」은 상기 도입방안의 2단계 조치로 규제 샌드박스를 명시적으로 법제화·구체화한 사항

□ 법안 주요내용

각종 금융규제로 인해 핀테크 기업 등이 혁신적 금융서비스를 개발하여도 이를 시장에서 시범운영(테스트)하기가 불가능한 상황
이에, 지정된 혁신금융서비스에 한해 일정기간 금융규제를 면제(또는 완화)하여 시범운영 수행을 허용하는 것이 법안의 핵심 내용

(가) 혁신금융서비스 지정

○ **(신청 대상)** 금융회사 또는 국내에 영업소를 둔 「상법」상 회사

○ **(심사 주체)** 금융위가 관련 전문가 등으로 구성(15인 이내)하는 「혁신심사위원회」에서 혁신금융서비스 지정여부를 심사*

* 서비스 혁신성, 소비자 편익, 금융소비자 보호방안의 충분성 등을 확인

[참고 2] 「혁신금융심사위원회」 구성

구 분	위원회 구성
위원장	금융위원회 위원장
위원 (15인 이내)	① 금융위 소속 공무원(시행령에서 규정) ② 위원장이 임명한 자(차관, 교수, 법률전문가, 기술·금융관련 업계 임직원 등)

○ **(심사 기간)** 심사는 신청 접수 後 30일 이내에 완료하며 최대 2회, 최장 60일 범위 內에서 심사기간 연장 가능

(나) 혁신금융서비스 지정 시 특례

○ **(규제 특례)** 혁신금융서비스로 지정된 경우 2년의 범위 內*에서 금융규제를

적용받지 않고(규제 특례) 서비스 이행 가능

* 1회에 한해 2년 이내로 혁신금융서비스 지정기간 연장신청 가능 (별도 심사필요)

- 혁신금융서비스 별 특례대상 규제는 서비스 지정심사 과정에서 금융위가 특례를 인정한 규제만 해당

※ 이용자 피해나 금융시장 안정성 저해우려 등이 있는 규제는 특례를 미 인정

○ **(배타적 운영권한)** 혁신금융서비스 지정기간 만료 後 법령에 따른 정식 인허가를 받은 경우,

- 해당 사업자는 1년의 범위 內에서 혁신금융서비스에 대한 배타적(독점적) 운영권한을 보유

(다) 혁신금융서비스 사업자(이하 "혁신금융사업자")의 의무

○ **(운영경과 보고)** 혁신금융사업자는 혁신금융서비스 시범운영 경과를 금융위에 정기적(총 3회)으로 보고

[참고3] 혁신금융사업자 보고시기 및 보고내용

구 분	보고 시기	보고 내용
초기 보고서	혁신금융서비스 지정 후 30일이 경과한 날부터 10일 이내	• 서비스 이용건수 및 총 거래액 • 서비스 이용자 수 및 특징
중기 보고서	혁신금융서비스 지정기간의 1/2이 경과한 날부터 30일 이내	• 금융사고 또는 이용자로부터의 손해배상청구 등 분쟁 현황 • 해당기간 이후의 서비스 운영계획 등
최종 보고서	혁신금융서비스 지정기간 만료일의 30일 이전	(상기 보고내용) + 현재 특례적용을 받고 있는 규제에 대한 향후 준수계획(추가)

○ **(이용자 고지)** 혁신금융사업자는 서비스 시험운영 사실 및 그로인한 위험발생 가능성 등을 이용자에게 반드시 사전 고지

※ 위험고지 後 서비스 제공에 따른 이용자 동의도 획득 필요

○ **(손해배상)** 서비스 제공과정에서 이용자에게 손해가 발생할 경우 혁신금융사업자는 고의나 과실이 없어도 이를 배상*

* 손해배상액 : 이용자 손해액의 최대 3배가 넘지 않는 범위에서 고의 또는 과실유무 등을 고려하여 법원에서 결정

※ 현행 신용정보법도 개인신용정보 누출 등에 대해 손해의 3배를 넘지 않는 범위에서 신용정보 이용자에게 배상할 책임을 부과

- 손해배상 이행을 위해 혁신금융사업자는 책임보험에 가입하거나 금융위와 협의하여 별도의 손해배상 방안 마련 필요

(라) 혁신금융서비스 업무위탁

○ 금융회사는 혁신금융서비스 시범운영에 필요한 일부 업무를 2년의 기간 內에서 지정된 대리인('지정대리인')에게 위탁 가능

- '지정대리인'은 금융회사 등의 신청을 받아 금융위가 지정

(마) 감독 및 검사

○ 지정감독기관(금감원 등)은 혁신금융사업자, 지정대리인 및 지정대리인에 업무를 위탁한 금융회사에 대해 동법 준수여부를 감독

- 검사결과에 따라 지정감독기관은 혁신금융서비스 지정취소나 서비스 중지 등을 관련 행정기관(금융위 등)에 건의 가능

(바) 기타

○ **(정부 지원)** 정부는 혁신금융서비스 지원기관의 운영 및 유지 보수에 필요한 비용의 전부(또는 일부)를 출연 또는 보조 가능

○ **(타 법과의 관계)** 본 법안은 타 금융관련법령에 우선하여 적용

○ **(법 시행)** 공포 後 3개월이 경과한 날부터 시행

□ 시사점

○ 규제 샌드박스를 통해 기업이 규제의 제약 없이 新기술 금융 서비스를 테스트해 볼 수 있어 핀테크 산업의 활성화가 기대

- 이는 기존 사전규제와는 달리 시장출시를 우선허용하고 사후 규제하는 방식으로 新기술 금융규제체계 전환의 의미도 내포

○ 규제 샌드박스를 통한 규제특례 등에도 불구하고 이용자 보호에 관한 사항은 기존 금융업 수준으로 엄격히 규정

- 특히, 고의·과실이 없어도 혁신금융사업자는 배상책임을 면할 수 없어 보안사고에 대한 보다 철저한 대응이 요구
  - 이를 위해, 혁신금융서비스 지정 추진시 계획단계에서 면밀한 보안대책 검증은 물론, 서비스 개시 이후에도 정기 취약점 분석·평가 등 체계적인 보안관리가 요구

○ 그간 규제로 인해 적극적인 활용이 어려웠던 금융권 클라우드 서비스도 규제특례로 인해 활용범위가 확대될 수 있어,

- 자체 IT역량이 부족한 핀테크 기업의 초기 시스템 구축·운영비용 절감은 물론 클라우드 산업의 동반성장도 기대

※ 현재 법안이 발의만 된 상황이므로 향후 국회 논의 과정, 법 시행에 필요한 하위 법령 제정 추이 등을 주시할 필요

전자서명법 개정 추진 동향 및 시사점

□ 개 요

○ 공인 전자서명 제도의 근거가 되는 전자서명법 개정안이 정부* 및 국회**에서 각각 발의됨에 따라 주요 내용 등을 검토

* 과학기술정보통신부 입법예고('18.3.30.)

** 고용진의원 대표발의('18.3.6.), 박성중의원 대표발의('18.3.7.)

□ 개정안 주요 내용

1. 정부(과기정통부) 발의안

공인전자서명 제도 폐지 및 전자서명인증업무 평가제 도입

(1) 공인전자서명 제도 폐지

○ 공인인증서, 공인인증기관 등 용어 정의 삭제, 공인전자서명의 법적 추정력 관련 조문 삭제 등 공인전자서명 제도 폐지

* 그 외 공인인증서를 통한 본인 확인 기능 등 삭제

- 일반 전자서명에 서명, 서명날인, 기명날인으로서의 효력을 부여하고, 전자적 형태를 이유로 법적 효력이 부인되지 않도록 명시

(2) 전자서명인증업무 운영기준 및 평가제

○ (운영기준) 과기정통부장관이 업무관리, 이용자 권리 보호 등을 포함한 전자서명인증업무 운영기준을 마련할 수 있도록 규정

- 동 기준을 준수하는 전자서명인증사업자는 평가기관의 평가 및 인정기관의 확인을 거쳐 운영기준 준수 증명서를 발급 받을 수 있도록 하는 전자서명인증업무 평가제 도입

※ 기존 공인인증기관은 법 시행일부터 1년간 본 평가를 통과한 것으로 봄

○ (사업자 의무) 증명서를 받은 전자서명인증사업자는 인증업무준칙 작성·게시, 과기정통부 검사, 신원확인, 배상책임 등의 의무 부담*

* 기존 공인인증기관의 의무와 유사하나 시설 보호조치, 기록 관리, 장애발생 신고 의무 등 다수 제외됨 (「[참고1] 과기정통부 전부개정안 상세 변경 사항」 참조)

※ 위 의무는 모두 증명서를 발급 받은 사업자에 대해서만 부과되고 있음

2. 고용진 의원(더불어민주당) 대표발의안

공인전자서명 제도 폐지 및 인증기관 등록제 도입

(1) 공인전자서명 제도 폐지

○ 공인인증서, 공인인증기관 등 용어 정의 삭제, 공인전자서명의 법적 추정력 관련 조문 삭제 등 정부발의안과 같이 공인전자서명 제도 폐지

- 다만, 정부발의안과 달리 공인전자서명의 요건*을 일반 전자서명에서도 유지하였고, 법적 효력 부인 관련 내용은 명시하지 않음

* 전자서명생성정보가 가입자에게 유일하게 속함, 서명 당시 가입자가 전자서명생성정보 지배·관리, 전자서명 후 해당 전자서명 및 문서 변경여부 확인 가능

※ 「[참고2] 전자서명 요건 및 효력관련 조문 비교」 참조

(2) 인증기관 등록제 도입

○ 기존의 공인인증기관 지정제를 폐지하고, 인증기관 등록제를 신규 도입하되, 등록 조건 및 의무 등은 기존 지정제와 매우 유사*

* 업무폐지 시 인계 및 정지인증서 회복 신청기한 관련 조항은 삭제했고, 기록보관 대상에 효력정지·폐지기록을 추가하는 등 일부 조항만 변경

3. 박성중 의원(자유한국당) 대표발의안

블록체인기술 기반 전자서명에 효력을 부여

○ 블록체인기술 기반 전자서명 중 기술적·관리적 요건(대통령령)을 갖추어 과기정통부장관의 지정을 받은 경우 공인전자서명과 동일한 효력 부여

□ 시사점

○ 전자서명법 개정안이 다양하게 제시되고 있어, 공인인증체계의 변화가 예상되는바, 추후 법 개정 논의를 지속 주시할 필요

참고 1 과기정통부 전부개정안 상세 변경 사항

구분	현행	개정안
전자서명인증 업무준칙 등	• 과학기술정보통신부 장관 신고	• 인터넷 홈페이지 등에 게시
휴지·폐지 시	• 다른 기관에 인계	• 요금의 환불, 가입자 개인정보 폐기 등 가입자 보호조치
신원확인 방법	• 과학기술정보통신부령에 명시	• 대통령령에서 정함
검사 범위 축소	• 검사 범위가 운영기준 준수사실 표시 여부, 인증업무준칙 작성·게시·준수, 휴폐업 사실 게시·통지 방법 이행 여부, 신원확인 절차 및 방법 준수 여부로 명시되어 축소됨	
인증서 관련 세부내용 삭제	• 인증서 포함 사항 명시(가입자 이름, 전자서명검증정보 등) • 이용범위 또는 용도 제한 인증서 발급 가능	• 관련내용 없음
	• 유효기간을 적정하게 정해야 함	• 관련내용 없음(다만, 업무 준칙 포함 내용에 명시)
기타 삭제 조항	• 정당한 사유 없이 인증역무 제공 거부할 수 없음 • 공인인증서 및 전자서명생성정보의 관리, 인증기관 시설 보호 등에 대해 전자서명 인증업무지침 고시 • 다른 공인인증기관의 인증업무 양수 시 신고 • 업무정지 처분에 갈음한 과징금 부과 • 상호인정을 위한 외국정부와 협정체결 • 효력 소멸·정비·폐지 관련 • 인증업무 관련 설비의 운영 • 공인인증서를 이용한 본인확인 • 전자서명생성정보의 관리 • 인증업무에 관한 기록의 관리(10년 보관 의무) • 장애발생 신고 의무	• 관련내용 없음(다만, 일부는 운영기준에 고시될 것으로 추정)
	• 시설, 자료 및 이용자 보호조치	• 운영기준에 고시될 예정

참고 2 전자서명의 요건 및 효력 관련 조문 비교

현 행	개 정 안
第3條(전자서명의 효력 등) ① ~ ③ (생략) 〈신 설〉	第3條(전자서명의 효력 등) ① ~ ③ (현행과 같음) ④ 블록체인기술(구성원 간 직접 연결 방식을 기반으로 각각의 정보가 저장된 블록이 사슬처럼 연결되는 분산화된 정보 처리 기술을 말한다)을 기반으로 한 전자서명 중 대통령령으로 정하는 기술적·관리적 요건을 갖추어 과학기술정보통신부장관의 지정을 받은 전자서명은 공인전자서명과 동일한 효력을 가진다.

현 행	정부발의안	고용진 의원 대표발의안
제2조(정의) 2. "전자서명"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다. 3. "공인전자서명"이라 함은 다음 각목의 요건을 갖추고 공인인증서에 기초한 전자서명을 말한다. 가. 전자서명생성정보가 가입자에게 유일하게 속할 것 나. 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것 다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것	**제2조(정의)** 2. "전자서명"이라 함은 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.	**제2조(정의)** 2. ---------- ---------- ---------- ---------- ----------정보로서 다음 각 목의 요건을 갖춘 것을 말한다. 가. 전자서명생성정보가 가입자에게 유일하게 속할 것 나. 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것 다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것
제3조(전자서명의 효력 등) ① 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다. ② 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다. ③ 공인전자서명외의 전자서명은 당사자간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.	**제3조(전자서명의 효력)** ① 법령의 규정 또는 당사자간의 약정에 따른 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다. ② 제1항 이외의 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 법적 효력이 부인되지 아니한다.	**제3조(전자서명의 효력)** ① 전자서명은 당사자간의 약정에 따른 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다. ② 다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 인증기관으로부터 발급받은 인증서에 기초한 전자서명이 있는 때에는 이를 충족한 것으로 본다.

News · Notice

- 금융보안 교육 안내
- 금융보안원 소식
- 사원사 소식

01 금융보안 교육 안내

교육일정 및 모집인원

연번	과정명	형태	일정	교육시간	정원	비고
1	정보보호 전략 수립 및 관리 대책	이론	8.8(수)~8.10(금)	3일(18h)	40명	
2	금융 네트워크 공격과 대응	실습	8.20(월)~8.22(수)	3일(18h)	25명	변경
3	4차 산업혁명과 금융 비즈니스 모델	이론	8.22(수)~8.24(금)	3일(18h)	40명	신규
4	금융권 빅데이터 분석 실무	실습	8.27(월)~8.29(수)	3일(21h)	25명	신규
5	금융 웹서비스 공격과 대응	실습	9.3(월)~9.5(수)	3일(18h)	25명	
6	금융권 개인(신용)정보보호 - 관리자	이론	9.5(수)~9.7(금)	3일(18h)	40명	변경
7	금융권 블록체인 도입 적용방안	이론	9.12(수)~9.14(금)	3일(21h)	40명	신규
8	금융 모바일 악성코드 공격과 대응	실습	9.17(월)~9.19(수)	3일(18h)	25명	
9	금융권 물리 보안	이론	10.10(수)~10.12(금)	3일(18h)	40명	변경
10	금융 APT 공격과 대응	실습	10.10(수)~10.12(금)	3일(18h)	25명	
11	금융정보보호관리체계	이론	10.24(수)~10.26(금)	3일(18h)	40명	변경
12	정보보호 전략 수립 및 관리 대책	이론	11.7(수)~11.9(금)	3일(18h)	40명	
13	금융 빅데이터 비식별 조치 및 활용	실습	11.13(화)~11.15(목)	3일(18h)	25명	변경
14	금융권 IT컴플라이언스	이론	11.14(수)~11.16(금)	3일(18h)	40명	변경
15	금융권 개인(신용)정보보호 - 취급자	이론	11.21(수)~11.23(금)	3일(18h)	40명	변경
16	모바일 시큐어 코딩	실습	11.26(월)~11.28(수)	3일(21h)	25명	신규

※ 세부커리큘럼 및 자세한 사항은 금융보안교육센터 홈페이지(http://edu.fsec.or.kr)를 참고해주시기 바라며, 상기 일정은 사정에 따라 변경될 수 있습니다.

02 금융보안원 소식

금융회사 대상 침해사고 대응훈련 실시(4.16.)

금융보안원은 날로 지능화되고 있는 사이버공격에 대비하고 금융회사의 침해사고 대응능력을 강화하기 위하여 189개 금융회사를 대상으로 2018년도 침해사고 대응훈련을 4월부터 12월까지 상시적으로 실시할 계획이다.

제2기 금융보안 최고책임자 과정 개설(5.4.)

금융권 정보보호최고책임자(CISO)를 대상으로 「제2기 금융보안 최고책임자 과정」을 개설하고, 5.3일 입교식을 개최하였다. 이 과정에서는 금융보안 정책, 최신 보안기술 트렌드, 보안사고 사례 등의 강연으로 구성된 교육 프로그램을 7월까지 12주 동안 실시할 계획이다.

해킹분석대회 FIESTA 2018 개최(7.16.)

침해사고대응기관으로서 필수적인 최신 침해위협 대응 기술력과 분석 역량을 갖춘 전문 인력을 양성하기 위해 금융보안원 내부적으로 "해킹을 분석하라, FIESTA 2018!" 대회를 개최하였다. 위협분석 교육과 악성코드·포렌식 분석 대회를 병행함으로써 대회 참여를 통한 전문성 강화에 초점을 맞추었다.

2018년도 금융보안자문위원회 전체회의 개최(6.28.)

금융보안원은 급변하는 금융환경 변화에 대응한 금융보안 전문기관의 역할을 강화하기 위하여 21人의 전문가로 2018년 금융보안자문위원회를 구성하고 제1차 전체회의를 개최하였다. 금번 전체회의에서는 「금융권 블록체인 추진 현황과 보안 측면의 향후 대응방향」에 대한 주제로 자문위원들이 다양한 의견을 교환하였다.

03 사원사 소식

코스콤 메리츠자산운용과 업계 최초 비대면 펀드 투자 앱 출시(4.16.)

국내 자산운용 업계 최초로 지점방문 없이 비대면으로 계좌개설 및 펀드투자까지 가능한 모바일 펀드판매 어플리케이션이 출시됐다. 코스콤과 메리츠자산운용은 모바일 펀드 판매시스템 '메리츠 펀드투자' 앱을 가동 완료했다고 밝혔다.

우리은행 차세대 전산시스템 정상 가동(5.8.)

우리은행은 차세대 전산시스템 '위니(WINI)'를 공식 가동했다. 2004년 이후 14년만에 도입하는 차세대 전산시스템으로, 기존에 분리 운영되던 시스템을 하나의 단말로 통합 구축함으로써 효율성을 높였고 최고급 정보보호 기술을 활용해 고객정보 보호 및 금융사기 예방도 한층 강화하였다.

ABL생명 모바일 고객센터에 지문·홍채 등 바이오인증 도입(5.8.)

ABL생명은 자사 모바일 고객센터에 지문, 홍채 등 바이오인증 서비스를 도입했다. 이번 서비스 도입으로 고객센터를 내방하지 않고도 스마트폰에서 별도의 공인인증서 없이 각종 보험내용 조회, 보험금 청구, 보험계약 대출, 중도인출 등의 업무를 처리할 수 있다. 또한 바이오인증 도입과 함께 다양한 본인인증을 통해 보안카드 없이 업무를 처리할 수 있는 환경을 구축하였다.

현대캐피탈 KT와 'AI 단말기 활용한 금융 및 서비스 개발'을 위한 업무협약 체결(5.9.)

현대캐피탈이 KT와 함께 음성인식 기반의 차량용 AI 단말기를 활용한 금융 및 서비스 개발을 위한 업무협약을 체결했다. 이번 협약을 통해 축적된 데이터를 기반으로 운행 습관을 분석한 다양한 정보를 제공하는 등 개인화 서비스를 내놓을 계획이다.

네이버 프라이버시센터내 GDPR 안내 페이지 공개(5.15.)

네이버는 프라이버시센터를 개편하여 유럽연합의 일반개인정보보호법(GDPR) 인포그래픽 등 관련 정보를 제공하는 GDPR 메뉴를 오픈하였고, 개인정보영향평가 수행을 위한 CNIL PIA 한국어 매뉴얼을 함께 공개하였다. 이러한 정보들은 일반 이용자나 전문인력이 부족한 스타트업 등이 이해하기 쉽도록 인포그래픽으로 제공하고 있다.

신한금융투자 시중 증권사 최고 '국제신용등급' 획득(5.15.)

신한금융투자는 국제 신용평가 기관인 무디스(Moody's)와 에스엔피(S&P)로부터 시중 증권사 최고 신용등급인 'A3', 'A-'등급을 각각 획득하였다. 신한금융투자는 안정된 국제신용등급 획득으로 글로벌 시장과 IB비즈니스에서 경쟁력을 확보하게 되었다.

SC제일은행 로보틱 프로세스 자동화 확대로 업무 효율화 추진(5.16.)

SC제일은행은 로보틱 프로세스 자동화(RPA,Robotic Process Automation)를 통한 업무 프로세스 개선으로 직원들의 단순 업무량을 줄이고, 고객서비스의 질을 높이기 위한 혁신적인 변화에 나섰다. 올해 인사, 재무, 리스크 등 일반관리 및 지원 분야를 대상으로 30개 업무 부분에 RPA를 추가 적용할 예정이다.

교보생명보험 KISA와 손잡고 인슈어테크 활성화 추진(5.28.)

교보생명은 KISA와 인슈어테크 활성화를 위한 포괄적 업무협약(MOU)를 체결했다. 교보생명은 KISA와 함께 인슈어테크 기업이나 스타트업을 선발하여 인큐베이팅을 지원하고 핀테크 아카데미를 운영할 예정이다.

NH농협은행 빅데이터 플랫폼 NH빅스퀘어 구축 완료보고회 개최(5.28.)

NH농협은행은 지난 23일 빅데이터 플래폼「NH 빅스퀘어(BigSquare)」 구축 완료회를 개최하였다. 앞으로 NH 빅스퀘어를 통해 새로운 인사이트 발굴과 데이터 분석기반으로 고객별 특성과 상황에 맞는 서비스를 제공할 수 있게 되었다.

KB국민은행 대화형 뱅킹 플랫폼 리브똑똑 정식 오픈(6.15.)

KB국민은행은 시범 운영중이던 차세대 모바일뱅킹 플랫폼 리브똑똑(Liiv TalkTalk)을 26일 정식 오픈했다. 리브똑똑에서 나눈 대화 내용은 해외 아마존 클라우드 서버에 저장돼 사생활이 보호되며, 국내 최초로 첨단보안 솔루션 'TAP'을 도입해 암호화된 메시지를 주고받을 수 있어 해킹이 불가능한 수준으로 보안성을 강화하였다.

하나카드 한국은행과 빅데이터 기반 경기예측력 제고를 위한 업무협약 체결(6.28.)

하나카드는 한국은행과 경기예측 고도화를 위한 빅데이터 활용 전략적 업무협약을 체결했다. 하나카드와 한국은행은 이번 협약을 발판으로 장기적으로 빅데이터 관련 긴밀한 파트너십을 구축해나갈 예정이다.

푸르덴셜생명 핀테크 혁신을 위한 '이노베이션 데이' 진행(5.31.)

푸르덴셜생명은 글로벌핀테크 스타트업 7개사를 초청하여 '이노베이션 데이'를 개최하였다. 이날 행사에는 미국·싱가포르·한국 푸르덴셜 생명 임직우너과 데이터로봇·거쉬클라우드·인슈어리움 등 핀테크 스타트업 관계자 100여명이 참석했다. 최근 핀테크 업계에서 주목하는 기술과 플랫폼에 대한 소개와 함께 푸르덴셜생명의 핀테크 운영 현황 등이 소개됐다.

※ '전자금융과 금융보안'은 사원사의 **핀테크** 또는 **정보보호 관련** 소식을 알리고 있습니다. 이와 관련하여 보도자료(링크 등)를 보내주시면 내용을 반영하고자 하오니 많은 참여 부탁드립니다.
E-mail: research@fsec.or.kr Tel: 02-3495-9713

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	국내·외 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, 금융회사 망분리 방안 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: 02-3495-9713

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.