제34호
2023-4Q

# 전자금융과 금융보안

## e-Finance and Financial Security

[Research]



금융보안원
FINANCIAL SECURITY INSTITUTE

제34호
2023-4Q

# 전자금융과 금융보안

## e-Finance and Financial Security

금융보안원
FINANCIAL SECURITY INSTITUTE

# CONTENTS

## 01 Research



## 02 Issue·Trend

# 03 News·Notice

# 전자금융과 금융보안

# 01 Research

**대규모 사기성 웹사이트 탐지를 위한 효과적인 신경망 모델 구축방안**

조해현, 숭실대학교 교수

**데이터 공유 활성화를 위한 기술요건 및 기밀컴퓨팅 금융권 활용방안**

조지훈, 삼성SDS 상무

**유럽 디지털 신원지갑의 출현과 우리 금융권에 미치게 될 영향**

이종혁 세종대학교 교수

# 대규모 사기성 웹사이트 탐지를 위한 효과적인 신경망 모델 구축방안

**조해현***



* 숭실대학교 교수

# 요약

가짜 쇼핑 웹 사이트, 사기 암호 화폐 사이트 등은 사용자들이 돈을 지불하도록 유도하고 실제로 서비스를 제공하지 않는다. 이들은 정보 탈취가 목적인 일반적인 피싱과는 다르게, 사용자로부터 돈을 훔치는 것이 목적이다. 이러한 수법으로 범죄를 저지르는 사기 웹 사이트를 Fraudulent E-commerce-websites (FCWs) 라고 정의한다.

FCWs는 시간이 갈수록 합법적인 웹 사이트들을 고도화된 수준으로 모방하고 있으며, 그로 인해 피해는 점점 커져가고 있다. 그러나 현재까지 FCWs를 탐지하는 대규모 보안 시스템이나, 공개적으로 사용 가능한 데이터셋이 존재하지 않아 다양한 분류의 사기 웹 사이트를 탐지하는 것은 어려운 일이다.

본 고에서는 크라우드 소싱을 통해 데이터를 수집한 뒤, 이로부터 FCWs가 갖는 주요 공통 특성들을 추출하고 이를 기반으로 대규모의 FCWs를 탐지하는 기법을 소개한다.

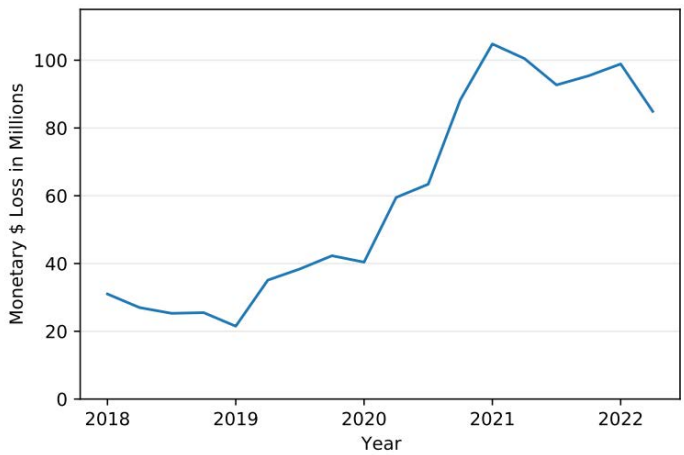

# 01 대규모 사기성 웹사이트 탐지를 위한 효과적인 신경망 모델 구축방안

## I 서론

피싱 범죄의 위협은 이제 어느 곳에나 존재하고, 이러한 범죄의 희생양은 점점 많아지고 있다. 불법 웹 사이트 및 피싱 사이트 탐지 방어 기술이 오랫동안 발전해왔음에도 불구하고 사기성 전자 상거래 웹 사이트(이하 FCWs)는 보안 생태계의 사각지대에 놓여있었다.

[그림 1]은 FTC가 밝힌 FCWs의 부류들 중 가짜 온라인 쇼핑 웹 사이트만으로 인해 발생한 재정적 손실 금액 그래프이다. 해당 그림으로부터 우리는 2021년 1분기에만 사기성 웹 사이트들 중 오직 하나의 유형으로부터 발생한 최대 금전적 손실이 1억 달러 이상임을 알 수 있다. 그리고 시간이 지날수록 그 피해 사례가 점점 증가한다는 사실도 이 그래프를 통해 확인할 수 있다.

그림 1 FTC[1]에 따른 분기별 온라인쇼핑 웹 사이트의 총 금전적 손실



더욱 큰 문제는 아직까지 대규모의 FCWs를 판별하는 프로그램이 제작되지 않았다는 점이다. 지금과 같은 추세가 이어진다면 이 피해는 지금보다 더 증가하게 될 것이다. 따라서 다양한 부류의 FCWs를 판별하고 이로부터 사용자를 보호하기 위한 프로그램이 필요하다는 것은 자명한 사실이다.

방어 프로그램을 제작하기 위해서는 실제로 존재하고 있는 FCWs의 데이터를 수집하고 데이터 분석을 진행해야 한다. 그러나 불법 사이트의 특성 상 가짜 웹 사이트는 빠르게 사라지기 때문에 FCWs의 목록을 조직화 하는 것은 어려운 일이다. 그리고 해당 사이트들은 단순히 이메일로만 전파되는 것이 아닌 여러 매개체를 통과하면서 사람들에게 전달되므로 데이터 수집 난이도가 높아진다.

또 다른 문제는 FCWs가 시간이 지남에 따라 발전한다는 점이다. 과거의 가짜 온라인 쇼핑몰은 터무니없이 낮은 가격을 제시했던 반면, 최근 가짜 온라인 쇼핑몰은 일반적인 쇼핑몰처럼 합리적인 가격을 책정하고 있다. 이 사례를 통해 우리는 불법 사이트 운영자들이 지나치게 낮은 가격은 사람들의 의심을 불러일으킨다는 것을 과거와는 달리 명확하게 파악하고 있고, 일반 사이트처럼 행동하려고 한다는 점을 알 수 있다.

앞에서 서술한 바와 같이 FCWs의 데이터를 수집하기 어려운 점과, 지속적인 FCWs의 발전은 대규모 FCWs 탐지 프로그램 제작에 있어 큰 장애물이다. 본 고에서는 크라우드 소싱을 통해 데이터를 수집한 뒤, 이로부터 FCWs가 갖는 주요 공통 특성들을 추출하고 이를 기반으로 대규모의 FCWs를 탐지하는 기법을 소개한다.

## II 연구배경 및 데이터 수집과 처리

### 1. 피싱과 FCWs의 차이점

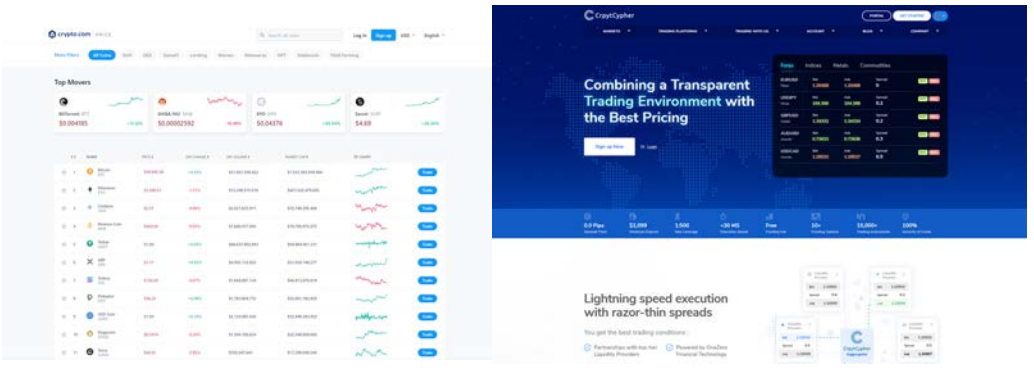
피싱과 FCWs는 모두 신뢰할 수 있는 사람 또는 기업이 접근한 것처럼 피해자를 속여 원하는 것을 얻어낸다는 특징을 갖는다. 그러나 이 둘은 공격의 목적과 공격의

방법에서 큰 차이점을 갖는다.

공격의 목적을 파악해보았을 때, 대부분의 피싱은 사용자의 암호나 주민 등록 번호와 같은 기밀 정보를 훔치는 것이 목적이다. 피싱의 공격자들은 미래에 수익을 창출할 수도 있는 사용자의 자격 증명 정보를 주로 훔친다[2]. 그러나 FCWs를 운영하는 범죄자들은 인터넷 사용자들로부터 돈을 갈취하는 것이 궁극적인 목적이다. 예를 들어, 사기 온라인 쇼핑몰들은 실제로 판매하지 않을 물건을 업로드해둔 뒤 사용자가 돈을 입금하면 그 물건을 배송해주지 않는 방식으로 운영된다. 가짜 애완동물 입양 사이트나 암호화폐 사이트, 자선단체 사이트 역시 비슷한 방법으로 사용자들에게 피해를 준다.

공격 방법의 관점에서 바라보면 피싱은 유명 브랜드를 사칭하거나 해당 브랜드 웹 사이트의 외관, URL 등을 따라한다. 그러나 FCWs는 사용자의 합법적인 전자상거래 사이트를 이용한 경험들을 바탕으로 일반 사이트를 가장한다. 이 차이점이 피싱 웹 사이트를 탐지하는 최신 기술이 FCWs를 효과적으로 분별하지 못하는 원인이 된다. 피싱 웹 사이트를 탐지할 때 사용되는 일반적인 기준이 바로 '일반 웹사이트와의 유사도' 이기 때문이다.

그림 2 합법적인 웹사이트(좌)와 FCWs(우)




[그림 2]에서 확인할 수 있듯, FCWs는 마치 일반 사이트처럼 체계적으로 디자인된 사이트의 테마를 갖고 있으며 소셜 미디어 로고와 적절한 연락처 페이지를 삽입해

방문자들에게 신뢰감을 얻는다. 또한 합법적인 루트로 보이는 금액 지불 화면을 개발함으로써 단순히 외관만으로는 이들을 탐지할 수 없다. 정확하게 웹 사이트를 복제하는 것 대신, 합법적인 웹 사이트의 기능과 UI와 비슷하게 사이트를 구현하는 것이 피싱과 FCWs의 주요 차이점이다.

## 2. 데이터 수집과 처리 방법

### 가. 데이터 수집

최신 데이터와 공개적으로 사용 가능한 데이터셋이 없기 때문에, FCWs 판별을 위한 가장 주요한 과제는 데이터를 모으는 것이다. 이 문제를 해결하기 위해 소셜 미디어 플랫폼 Reddit을 활용한다. Reddit은 3억 3천만 명의 사용자가 이용하는 플랫폼으로, 사용자들은 다양한 분야를 주요 토픽으로 삼는 서브레딧에서 의견을 나눌 수 있다[3]. 그리고 서브레딧에서는 submission이라는 기능으로 사람들과 토론이 가능한데, 해당 연구를 위해 FCWs가 주제인 서브레딧 /r/Scams의 사용자 submission 및 해당 의견 데이터셋들을 수집하였다.

2019년 12월부터 2021년 10월까지 /r/Scams의 submission을 지속적으로 크롤링한 결과, 해당 서브레딧에는 354,000명의 회원이 속해있으며 이곳에서 의심스러운 웹 사이트와 이메일 및 전화가 불법적인 루트인지를 토론하고 그에 관한 경험을 공유하고 있었다. 총 16,072개의 submission을 수집하였고 그 중 6,233개는 실제 URL을 포함하는 게시글이었다. 연구진은 수집된 URL에 대해 웹페이지의 전체 HTML 코드와 도메인 등록 정보를 WHOIS[4]를 이용하여 저장했다.

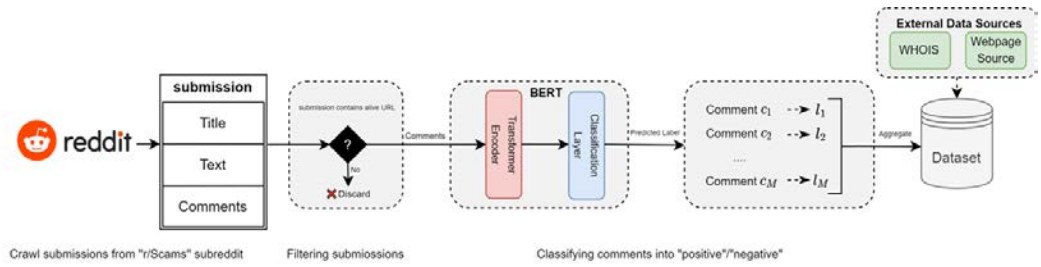
또한 2018년 12월부터 2019년 12월까지 게시물의 전년도를 소급하여 탐색해 17,442 건의 추가 submission과 2,881개의 URL(크롤링 당시에 운영되던)을 얻을 수 있었다. 최종적으로 33,514건의 submission을 분석하여 9,114건의 URL을 획득했고 이 데이터들은 라벨링 단계를 거친다.

## 나. 데이터 분류

/r/Scams 서브레딧의 관리자는 각 submission과 연관된 코멘트들을 엄격하게 관리하고 허위 사실을 곧바로 삭제하기 때문에 연구진은 서브레딧의 사용자 의견을 신뢰할 수 있다고 판단하였다. 따라서 9,114 건의 URL을 분류하기 위해 각 URL에 관련하여 /r/Scams 서브레딧 사용자 의견을 조사한 뒤 라벨을 부여하는 프로세스를 채택하였다. 모든 submission에는 하나 이상의 의견이 있으며, 의견은 submission 당 평균 9개에서 중간값 4개로 측정된다.

라벨링 프로세스를 자동화하기 위해 submission의 의견이 긍정적인 평가인지, 부정적인 평가인지 분류하는 자연어 처리(NLP) 모델을 훈련하고 사용한다. 자연어 처리 모델은 BERT 모델을 응용하여 만들어지며, {positive, negative} 라벨이 포함된 Stanford Sentiment Treebank 이진 분류 데이터셋을 사용하여 훈련을 진행했다. [그림 3]은 FCWs 수집 및 라벨링 프로세스의 개요를 보여준다.

**그림 3** FCWs 수집 및 라벨링 프로세스 개요




각 submission에 달린 의견들을 중요한 정보가 포함된 컨텍스트 벡터 g로 변환한 뒤 모델에 통과시켜 해당 벡터를 긍정 또는 부정 평가로 라벨링 한다. 만약 특정 URL이 긍정적인 평가보다 부정적인 평가를 더 많이 얻었다면 그 URL은 FCW로 지정된다.

### 다. 분류 데이터 검증

라벨링한 데이터에서 라벨 노이즈를 검증하고 평가하기 위해 두 가지 실험을 설계하였다. 먼저 Palo Alto Networks와 협력하여 실제 데이터셋에서 모델을 평가하였다. 지금까지 한 번도 본 적 없는 데이터셋(또는 수동으로 검증된 데이터셋)에서 모델의 오탐률은 2.46%, 탐지율은 94.88%로 확인되었다.

두 번째 실험에서는 데이터셋 내에서 2,000개의 웹사이트를 랜덤으로 선택하여 실험용 하위 데이터셋을 만들었다. 그리고 연구에 참여하지 않은, URL의 라벨들에 대한 정보가 없는 보안 전문가 3명을 섭외하였다. 전문가들은 각 URL에 접속하여 기능을 직접 체험해보거나 Reddit 스레드를 읽고 검색 엔진을 사용하여 웹 사이트가 합법적인 사이트인지 아닌지를 판별한다. 전문가 3명의 의견들을 취합하여 다수결로 각 URL에 라벨을 부여해보았고 그 결과 데이터셋에서 1.86%의 라벨 노이즈를 차지하는 1.98% FPR(False Positive Rate)과 1.63% FNR(False Negative Rate)를 얻을 수 있었다.

해당 라벨 노이즈는 데이터셋의 라벨 지정 프로세스 실행 중 사람 또는 기계에 의해 발생할 수 있다. 그러나 신경망에서 과적합을 방지하는 방법 중에는 데이터에 라벨 노이즈를 추가하는 방법이 있으며[5], 최근 연구에서는 라벨노이즈가 20% 이상인 상황에서도 신경망의 강건성이 유지됨을 보여주었다[6, 7]. 따라서 연구진은 해당 라벨 노이즈는 허용 가능한 요소라고 판단하였다.

이 데이터셋을 사용하면, 인간 사용자가 FCWs로 의심한 웹사이트를 모델이 FCWs로 탐지하게끔 편향된 결과를 만들 가능성이 생긴다고 생각할 수도 있다. 그러나 Reddit의 데이터에는 사용자가 사기 피해를 입은 뒤 해당 사이트를 공유하는 URL이 포함되어 있다. 또한 모델의 일반화 가능성을 입증하기 위해 모델에 사용되지 않은 데이터인 Palo Alto Networks에서 얻은 데이터셋을 활용했기에 이러한 가능성은 존재하지 않는다고 말할 수 있다.

## Ⅲ 신경망 모델 구현

### 1. FCWs 분류 및 공통 특징 추출

사기성 웹 사이트와 일반적인 웹 사이트의 구분 없이 각 유형의 웹 사이트에는 분류 모델이 각 사이트를 구별하는 데 도움이 되는 특징들이 존재한다. 이 특징은 총 4가지로, 각각 콘텐츠 기반, DNS기반, URL 기반, 소셜 미디어 기반으로 분류가 가능하고 각 항목에 포함된 하위 특징을 [표 1]에 제시한다.

**표 1** FCWs 특징 분류 및 하위 특징

| Feature category | Feature name | Feature type |
|---|---|---|
| 콘텐츠 기반 | Valid social media | Categorical |
| | # of external links | Quantitative |
| | # of script tags | Quantitative |
| DNS 기반 | Domain age | Quantitative |
| | Registration period | Ordinal |
| | Domain country | Categorical |
| | Host country | Categorical |
| | Same host & domain country | Ordinal |
| | Cheap registrar | Categorical |
| | Domain privacy | Ordinal |
| | Top 100K | Ordinal |
| URL 기반 | Cheap TLD | Ordinal |
| | Includes hyphen | Ordinal |
| | Includes digits | Ordinal |
| | Sub-domain level | Quantitative |
| 소셜 미디어 기반 | # of followers | Categorical |
| | Account age | Quantitative |
| | # of likes | Quantitative |

## 2. 신경망 모델 구현

위에서 정의된 특징들을 기반으로 FCWs 탐지를 위한 신경망 모델을 구현한다. 머신러닝 프레임워크인 PyTorch를 사용하며 모델의 각 hidden 레이어에는 {2048, 1024, 512, 256} 개의 뉴런이 존재한다. 최종적으로 Adam Optimizer를 사용하여 모델을 업데이트하는데, 테스트 단계에서 출력된 확률이 0.5보다 크면 사기 웹사이트로 판별된다. 모델의 입력값은 [표 1]에서 제시된 특징 벡터 x이고, 출력은 웹사이트가 합법 사이트인지, 불법 사이트인지의 확률 p이다.

비교 접근 방식은 Random Forest, SVM, XGBoost 이다. [표 2]에서 각 접근 방식에 대한 매개 변수 설정을 자세히 서술한다.

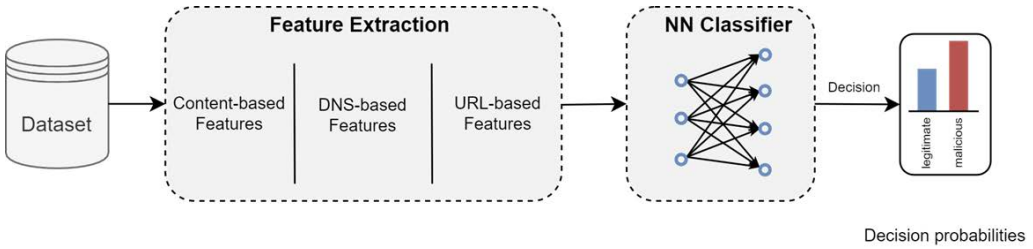
**표 2** 비교 접근 방식과 매개 변수 설정

| Model | Parameter | Value |
|---|---|---|
| SVM | kernel | rbf |
| | gamma | scale |
| RF | max_depth | 10 |
| | min_samples_split | 2 |
| | n_estimators | 100 |
| XGBoost | objective | binary : logistic |
| | eta | 1 |
| | n_estimators | 100 |
| | max_depth | 10 |

제안 모델은 총 6개의 계층으로 구성되는데, 모델에 입력되는 값이 FCWs일 확률을 출력하기 위해 네트워크를 통해 특징 벡터를 전달한다. 각 레이어의 아웃풋은 쌍곡탄젠트 함수에 학습 가능한 네트워크 파라미터를 통과시킨 값이고, 최종적으로 시그모이드 함수를 통과하게 된다.

이 작업을 위해 훈련 중 가중 교차 엔트로피 손실 함수를 사용한다. 합법적 사이트 샘플과 FCWs 샘플에 각각 0.8과 0.2의 가중치를 적용한다. 이 가중치 할당은 FCWs를 잘못 분류하는 것보다 합법적인 사이트의 샘플을 잘못 분류하는 것에 대해 더 많은 패널티를 부여한다. [그림 4]는 제안 모델의 훈련 과정을 그림으로 보여준다.

**그림 4** 제안 신경망 모델의 훈련 과정




MLP 분류기의 공식이 주어지면, 우리는 최적의 네트워크 매개변수를 찾는 것을 목표로 한다. 이를 위해 Adam Optimizer[8]를 사용하여 손실 함수 값을 최소화하고 네트워크 매개 변수를 최적화한다. 그리고 Batch Normalization (BN)[9]은 sigmoid 활성 함수 사용 시 발생하는 기울기 소실 문제를 해결하고 훈련 과정을 가속화시켜준다.

## 3. 성능 평가

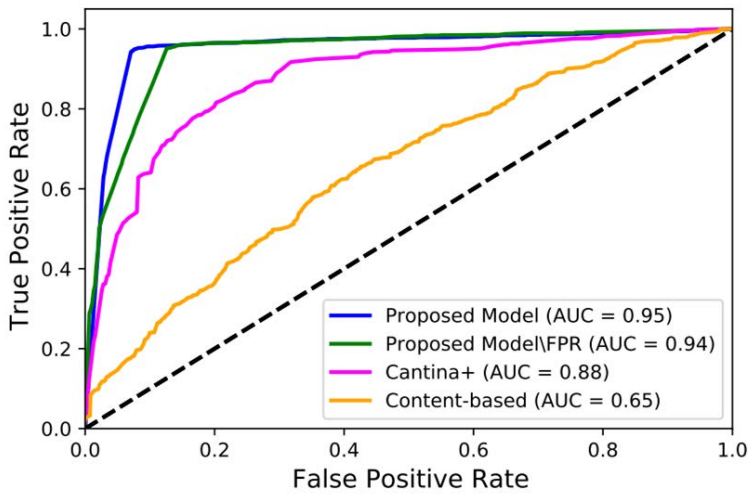
### 가. 타 프로그램과의 비교

CheckPhish, Cantina+, RealTime, HAN 네 가지 기존 기법들과, 제안 모델 구현부분에서 제시한 3가지 비교 접근 방식들과 비교하여 그 성능을 평가한다. 성능 평가 결과를 [표 3]과 [그림 5]에서 자세히 설명한다.

**표 3** 기준들과 비교한 제안 기법(BP)의 성능 비교

| Model | FPR (↓ better) | Detection Rate (↑ better) | F1 (↑ better) |
|---|---|---|---|
| BP+Random Forest | 1.84% | 72.79% | 0.81 |
| BP+XGBoost | 1.84% | 91.92% | 0.906 |
| BP+SVM | 3.33% | 78.92% | 0.825 |
| BP+NN | 1.68% | 87.14% | 0.924 |
| CheckPhish | 0.68% | 18.87% | 0.012 |
| Cantina+ | 22.22% | 79.72% | 0.769 |
| RealTime | 3.66% | 69.07% | 0.773 |
| HAN | 22.22% | 20.21% | 0.295 |

**그림 5** 제안 기법과 기존 기법들의 Receiver Operating Characteristic(ROC)곡선



위양성률, 탐지율, F1 점수 및 ROC 곡선 측면에서 모델을 평가한다. F1 점수는 정밀도와 재현율의 조화 평균이며 탐지율은 올바르게 분류된 사기성 웹 사이트의 비율을 나타낸다. [그림 5]의 매크로 평균 ROC 곡선은 서로 다른 임계값 설정에서 위양성률 비율에 대한 TPR을 플로팅하여 생성된 바이너리 분류기의 진단 기능을 나타낸다.

[표 3]에서 알 수 있듯이, 비교하는 프로그램들보다 제안된 모델은 높은 탐지율과 낮은 오탐률을 갖기에 FCWs를 탐지하는데 더욱 효과적이라 할 수 있다. 특히, Cantina+ 모델은 피싱 웹사이트[10] 탐지에는 적합했지만, FCWs를 잘 탐지하지는 못했다. 최종적으로 Cantina+에서 사용하는 특징 목록은 FCWs 탐지에는 적합하지 않다는 결론을 내릴 수 있었다. 또한 우리가 직접 설계한 특징에서 다양한 방법들의 결과를 비교해보았을 때 BP+NN이 위양성률이 낮고 F1 점수가 높기 때문에 FCWs를 탐지하는 데 가장 성능이 우수함을 알 수 있다.

BP+NN의 효과를 더 자세히 조사하기 위해 다른 실험을 설계한다. 각 범주의 80%를 훈련 세트로 사용한 다음 각 범주의 나머지 20% 에 대해 테스트셋으로 사용하여 테스트셋의 새로운 분할에서 BP+NN을 평가한다. 훈련 세트의 특성으로 인해 탐지율이 이전 실험과 다르다는 점에 유의하여야 한다. [표 4]는 이 실험의 결과를 나타낸다. BP+NN이 기준들에 비해 더 신뢰할 수 있다는 결론을 얻었음을 결과로부터 추론할 수 있다. BP+NN은 일부 범주에서 가장 높은 탐지율을 달성하지는 못했지만 FPR이 낮거나 F1 점수가 더 높다는 점에 의의가 있다.

**표 4** FCW 카테고리 별 분류기의 성능

| Category | Model | FPR (↓ better) | Detection Rate (↑ better) | F1 (↑ better) |
|---|---|---|---|---|
| Fake Online Shopping | BP+NN | **0.78%** | 61.47% | **0.747** |
| | CheckPhish | 0.82% | 1.45% | 0.028 |
| | RealTime | 3.18% | **62.92%** | 0.746 |
| Pet Scam | BP+NN | 0.83% | **70.58%** | **0.815** |
| | CheckPhish | **0.29%** | 0.00% | 0.0 |
| | RealTime | 2.18% | 62.92% | 0.746 |

| Category | Model | FPR (↓ better) | Detection Rate (↑ better) | F1 (↑ better) |
|---|---|---|---|---|
| Charity Websites | BP+NN | 1.51% | **59.25%** | **0.711** |
| | CheckPhish | **0.79%** | 1.98% | 0.036 |
| | RealTime | 8.33% | 54.54% | 0.600 |
| Cryptocurrency and Stock Market | BP+NN | 2.04% | 69.15% | **0.754** |
| | CheckPhish | **0.61%** | 0.00% | 0.0 |
| | RealTime | 12.76% | **69.56%** | 0.711 |
| Delivery Websites | BP+NN | 4.28% | **67.64%** | **0.767** |
| | CheckPhish | **0.00%** | 0.00% | 0.0 |
| | RealTime | 4.16% | 62.50% | 0.727 |
| Education Related Websites | BP+NN | 1.42% | **58.34%** | **0.769** |
| | CheckPhish | **0.00%** | 0.00% | 0.0 |
| | RealTime | 5.88% | 38.46% | 0.500 |
| Adult Content and Dating | BP+NN | **1.47%** | **98.52%** | 0.583 |
| | CheckPhish | 2.95% | 13.95% | 0.222 |
| | RealTime | 4.68% | 50.00% | **0.611** |

### 나. 실제 환경에서의 분류

실제 환경과 접하지 않은(훈련되지 않고 테스트 되지 않은) 데이터에서 제안된 모델을 검증하기 위해 /r/Scams 서브레딧에서의 사용자 연구를 실행했다. 우리는 IRB에서 승인한 프로토콜을 따랐고 기타 다른 참가자들로부터 어떠한 정보도 수집하지 않았다.

첫째로, /r/Scams에서 새로운 submission을 모니터링하는 Reddit 봇을 만들었다. 각각의 새로운 submissions 은 URL을 포함하는 제출만 처리하기 위해 정규식에 의하여 확인된다. 그 다음 [그림 5]의 테스트 단계에 따라 URL이 분류기에 의해 feature 추출 모듈에 전달된다. 결과 라벨은 사용자에게 결정을 알리기 위해 봇이 submission의 댓글로 개시한다. 또한 /r/Scams 사용자는 봇의 댓글에 있는 동의 또는 동의하지 않음 버튼을 클릭하여 피드백을 제출할 수 있다.

게시된 댓글에서 우리는 참가자들에게 Reddit 봇의 목적과 작업 및 수집하는 정보를 설명한다. 14개월 동안 8,174명의 사용자로부터 2,223 건의 제출에

대해 13,917 건의 응답을 수집했다. 이 중 298 건은 합법적인 사이트, 1,925건은 사기 사이트이다. 응답은 봇 댓글에 있는 동의 또는 동의하지 않음을 클릭한 사용자를 기준으로만 수집하였다.

**표 5** 14개월 동안 실제 환경 샘플에서의 제안 모델 성능

| Total # data | FPR | FNR | TPR | TNR | Accuracy |
|---|---|---|---|---|---|
| 2,223 | 1.34% | 1.66% | 98.34% | 98.65% | 98.38% |

결과를 검토했을 때, 제안된 기법이 주어진 시간동안 98.38% 동안 올바르게 라벨을 예측했음을 알 수 있었다. 우리는 사용자의 피드백에 대한 다수결을 봇의 응답 라벨로 결정했다. [표 5]는 실제 환경에서의 제안 모델의 성능을 나타낸 결과인데, 특히 [표 3]과 비교했을 때, 훈련되지 않은 데이터에 대해 제안 모델의 성능의 일관성을 알 수 있다. 테스트 데이터에서 사용자 연구는 98.38%의 정확도를, 제안 모델은 93.41%의 정확도를 나타냈으므로 제안 모델이 수동 분석에 가까운 성능을 제공할 수 있음을 나타낸다.

## Ⅳ 결론

우리가 개발한 신경망 모델은 FCWs로부터 사용자를 보호하기 위해 사용될 수 있다. Google Safe Browsing이나 Microsoft Windows Defender 와 같은 시중에서 사용되는 시스템과 제안 기술을 함께 사용한다면 피싱 및 악성 프로그램으로부터 사용자를 보호할 수 있을 뿐만 아니라 FCWs에 대해 사전에 경고를 받을 수 있다. 또한, FCWs 운영자들이 자주 사용하는 저렴한 도메인 등록 업체나 웹 사이트 구축 플랫폼이 제안된 프로그램을 FCWs 선별 방법으로 사용하는 것도 좋은 방법일 것이다. FCWs 사이트가 개설되기 전, 사이트를 스캔하고 조치를 취할 수 있기 때문이다.

그러나 FCWs와 관련된 연구[11, 12]가 진행되었음에도 불구하고 아직 FCWs 연구에 핵심적으로 도움이 되는 데이터셋은 부족하다. 대부분의 이전 연구는 스팸 전자 메일에서 URL을 크롤링하여 불법 상거래 사이트 URL을 찾았다. 제안 기법은 Reddit을 사용하여 데이터셋 부족을 해결했지만, 여전히 데이터셋의 한계는 존재한다. 또한 URL을 많이 수집하더라도 FCWs의 수명이 짧기 때문에 모델을 훈련하고 테스트하기 위한 URL이 제한된다는 점도 한계점에 속한다.

FCWs 분류의 근본적인 문제 중 하나는 실측 데이터가 부족하다는 것이다. 이를 해결하기 위해 각 URL과 관련된 피드백에 대한 감정 분석을 사용한다. 그러나 모델의 오류는 데이터를 왜곡할 수 있으며, 전문가가 수동으로 지정한 데이터도 동일한 문제를 겪을 수 있다. 그리고 인간이 감지하기에 어려운 FCWs가 있을 수도 있으므로, 이러한 FCWs는 /r/Scams에 게시되지 않는다. 따라서 /r/Scams에서 URL을 수집하는 것은 사람의 의심을 일으키는 FCWs로 편향될 가능성이 존재한다.

의미 있는 FCWs 특징을 찾는 것도 어려운 일인데, 훈련 데이터셋은 2018-2021년에 2년 동안 /r/Scams에서 수집되었으며 마찬가지로 유효성 검사 데이터 세트는 /r/Scams에서 2020-2021년 14달 이상 수집되었다. 이전에 본 적 없는 데이터 샘플에서도 높은 성능을 보인 것은, 시간이 지나 오래된 훈련 데이터셋이 있음에도 불구하고 높은 성능을 보여주었음에 제안 기법의 견고성을 증명하였다고 볼 수 있다.

제안 기법은 /r/Scams에 제출된 잠재적 FCWs에서 98.38%의 정확도를 달성하고 금융 회사의 2022년 8월 데이터셋에서 83.41%의 정확도를 달성했다. 우리는 이러한 결과가 현재 FCWs에 “급격한 개념 변경”이 거의 없다는 것을 보여준다고 믿으며, 아마도 이것은 현 시점 공격 방어 수준이 낮기 때문에 공격자들이 그들의 기술을 크게 변경할 필요가 없다는 것을 반증한다. 이처럼 FCWs를 향한 관심과 방어 대책은 아직 약한 수준이고, 더 큰 피해를 방지하기 위해서는 제안 기술과 같은 다량의 FCWs 를 집중적으로 분류하는 방어책이 지속적으로 개발될 필요성이 있다.

## 참고문헌

[1] F. T. Commission, "Consumer sentinel network data book2019," 2022, https://www.ftc.gov/reports/consumer-sentinel-network-data-book2021

[2] A. Oest, Y. Safei, A. Doupe, G.-J. Ahn, B. Wardman, and G. Warner, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis," in 2018 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2018, pp. 1–12.

[3] F. Team, "Reddit Statistics For 2021 (Demographics, Usage & Traffic Data)," 2021, https://foundationinc.co/lab/reddit-statistics/.

[4] "ICANN,"2019, https://www.icann.org/resources/pages/governance/bylaws-en.

[5] C. M. Bishop, "Training with noise is equivalent to tikhonov regularization," Neural computation, vol. 7, no. 1, pp. 108–116, 1995.

[6] D. Rolnick, A. Veit, S. Belongie, and N. Shavit, "Deep learning is robust to massive label noise," arXiv preprint arXiv:1705.10694, 2017.

[7] H. Song, M. Kim, D. Park, and J.-G. Lee, "Learning from noisy labels with deep neural networks: A survey," arXiv preprint arXiv:2007.08199, 2020.

[8] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," arXiv preprint arXiv:1412.6980, 2014.

[9] S. Ioffe and C. Szegedy, "Batch normalization: Accelerating deep network training by reducing internal covariate shift," arXiv preprint arXiv:1502.03167, 2015.

[10] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "Cantina+ a feature-rich machine learning framework for detecting phishing web sites," ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 2, pp. 1–28, 2011

[11] Wadleigh, J. Drew, and T. Moore, "The e-commerce market for" lemons" identification and analysis of websites selling counterfeit goods," in Proceedings of the 24th International Conference on World Wide Web, 2015, pp. 1188–1197.

[12] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in Proceedings of the 22ndinternational conference on World Wide Web, 2013, pp. 213–224.

# 데이터 공유 활성화를 위한 기술요건 및 기밀컴퓨팅 금융권 활용방안

조지훈*



* 삼성SDS 상무

# 요약

지난 수년간 국내에서는 데이터 기반 산업 활성화를 촉진하기 위해 규제개선 등을 통해 외부 데이터를 결합하고 활용할 수 있도록 장려하고 있지만, 민간에서의 데이터 결합사례는 기대만큼 발생하고 있지 않다. 또한, 국내외에서 차세대 개인정보보호 강화기술인 PETs(Privacy Enhancing Technologies) 기반의 서비스를 제안하고 있지만 규모 있는 사업성과 또한 찾아보기 힘들다. 이것은 아직까지 PETs 기술의 성숙도가 낮은 이유도 있겠지만, 데이터 공유를 위한 명백한 다른 기술 요건이 존재하기 때문이다.

본 기고서를 통해 데이터 공유 활성화를 위한 여러 기술적 요건을 살펴보고, PETs 기술의 동향과 함께 특히, 시스템보안 기반의 접근방식인 기밀컴퓨팅(Confidential Computing, CC)기술에 대해 자세히 살펴보겠다. 마지막으로, 금융 분야에서의 적용 가능한 기밀 컴퓨팅 기반의 데이터 결합 서비스 방안을 소개하겠다.

# 02 데이터 공유 활성화를 위한 기술요건 및 기밀컴퓨팅 금융권 활용방안

## I 데이터 공유 활성화를 위한 기술적 요건

NVIDIA의 CEO, 젠슨황은 지난 5월 대만에서 열린 'COMPUTEX 2023' 키노트 세션에서 AI시대에는 데이터센터가 AI Factory가 될 것이라고 언급하였다. 즉, 지금까지는 주로 공장에서 원자재 및 부품 등을 공급받아 가공하고 조립하여 제품을 만들었다면, 향후에는 데이터센터도 데이터를 가공하여 서비스 및 제품을 만들어내는 시대가 올 것이라는 것이다.

지난 수년간 국내에서는 데이터 기반 산업 활성화를 촉진하기 위해 규제개선 등을 통해 외부 데이터를 결합하고 활용할 수 있도록 장려하고 있지만, 민간에서의 데이터 결합사례는 기대만큼 발생하고 있지 않다. 또한, 국내외 기업에서 차세대 개인정보보호 기술인 PETs (Privacy Enhancing Technologies) 기반의 서비스를 제안하고 있지만 규모 있는 사업적 성과 또한 찾아보기는 힘들다. 이것은 아직까지 PETs 기술의 성숙도가 낮은 이유도 있겠지만, 데이터 공유를 위한 명백한 다른 기술 요건이 존재하기 때문이다.

사실 데이터 교환 및 공유는 지난 수십 년 동안 우리 주위에서 진행되어 왔다. 공식통계를 위해 통계청은 여러 기관으로부터 데이터를 공유 받아 정책결정을 위한 통계작성을 진행하였으며, 금융회사들은 조인트벤처를 설립하여 신용정보를 공유해왔다. 위와 같은 기존의 데이터 공유 방식에서 신뢰는 계약 등의 정책으로 보장되었으며, 비용은 책정된 예산에 따라 진행하면 되었다. 특히, 데이터 제공자는 데이터 결합과 분석을 진행하는 조직이 의도된 대로 데이터를 사용하는지 검증할 수 있는 기술적 방안이 없기에 위와 같은 데이터 공유는 조직간 강력한 신뢰

기반으로 행해졌다.

그러나 데이터 공유가 민간의 다양한 영역으로 확대됨에 따라 위와 같은 데이터 공유방식은 한계를 드러내게 되었다. 민간에서의 무신뢰 및 저비용 기반의 효율적인 데이터 교환이나 공유가 활성화되기 위해서는 규제개선 및 PETs과 같은 핵심기술 외에도 고려할 다른 기술적 요소가 많다. World Economic Forum (WEF)에서는 데이터 교환 및 공유를 위한 참조모델을 제시하며 고려해야 할 다양한 기술적 요건을 제시하고 있다[1].

무엇보다도 데이터 교환 활성화를 어렵게 만드는 요인으로 'Data Discovery 및 Quality Control'을 생각해볼 수 있다. 데이터 교환 활성화를 위해서는 데이터를 중앙에 저장하지 않고 공통된 데이터 구조와 분류를 통해, 데이터 공급자와 데이터 수요자간 수요자가 원하는 데이터를 찾을 수 있어야 한다. 그리고 데이터 디스커버리가 되었다 하더라도 데이터가 불완전 하거나 잘못된 레이블이 달려 있는 경우 이를 정제하는데 상당한 비용이 소요되게 된다. 또한 데이터 결합이나 교환을 위한 표준의 부재 또한 데이터 공유 활성화를 어렵게 만드는 요인이다.

위에서 언급한 이슈를 해결할 수 있는 방안으로 'Data Virtualization'기술이 주목을 받고 있다. 기존에는 여러 데이터 소스들로부터 Data Lake, Data Warehouse, 혹은 Data Mart에 ETL등을 통해 데이터를 물리적으로 통합하여, 데이터 사용자들이 API나 SQL을 통해 접근하였다. 그러나 Data Virtualization에서는 실제 데이터는 물리적으로 이동하지 않고, Data Catalog, Cashing, Metadata Management 등을 제공하는 추상화 계층을 통해 데이터를 논리적으로 통합하고 데이터 분석을 가능하게 한다. 특히, 데이터 제공자들은 조직의 데이터가 외부로 전송되는 것에 대한 거부감이 있으며, 최근 데이터 주권에 대한 요구사항 높아짐에 따라 데이터의 물리적 이동이 더욱 어려워지고 있어 향후 Data Virtualization 기술에 대한 요구가 더욱 높아질 것으로 예상된다.

또한, 클라우드와 같은 Shared Infrastructure에서 데이터 교환, 공유 및 데이터 분석까지 이루어져야 한다. UNECE(UN 유럽경제위원회)에서도 효율적이고 안전한 데이터 결합분석을 위해서 Multi-Party Secure Private Computing-as-a-service (MPSPCaaS)가 필요함을 언급하고 있다[2]. 즉, 데이터 전달이나 교환이 목적이 아니라 데이터 공유를 통해 분석된 결과를 얻는 것이 중요하며, MPSPCaaS와 같은 공유된 플랫폼에서 PETs 기술로 데이터를 안전하게 보호하면서 데이터 분석이 수행되어야 함을 강조하고 있다.

현재까지 국내에서 데이터 공유 혹은 교환은 데이터 수요자가 원하는 데이터를 공급자가 KLT기반의 프라이버시 보호모델을 만족하도록 적절한 비식별화를 통해 제공하거나, 혹은 둘 혹은 이상의 조직의 데이터를 결합하여 비식별화된 데이터를 전달한다. 이러한 환경에서는 데이터 제공자는 비록 비식별화를 통해 데이터를 제공했다 하더라도 전달된 데이터가 서로 합의된 용도로만 사용되는지 확인할 수 있는 기술적 방안이 여전히 없으며, 재식별화에 대한 리스크 또한 존재하게 된다.

따라서 WEF와 UNECE에서 강조하고 있는 바와 같이 클라우드 혹은 공유 가능한 플랫폼에서 데이터 분석을 위한 파이프라인을 제공하여, 공유된 플랫폼 내에서만 데이터가 공유되고 분석된 결과만 데이터 수요자에게 전달될 수 있는 기술적 방안이 지원되는 것이 필요하다. 그리고 안전한 데이터 교환을 위해, PETs 기술 외에도 인증 및 권한관리 등의 보안, 그리고 개인정보보호 관련 규제를 대응하기 위한 기술 및 정책적 지원이 필요하고, 또한 이렇게 복잡한 요구사항을 구축하는 것은 상당한 비용이 요구될 수밖에 없으며, 이미 이러한 기본적인 보안 및 데이터 분석플랫폼을 구축하고 있는 클라우드 플랫폼을 활용하는 것이 현실적이다. 그러나 클라우드가 아니더라도 이미 일정 수준의 데이터 분석 플랫폼과 보안을 제공하는 데이터센터도 이러한 역할을 수행할 수 있다.

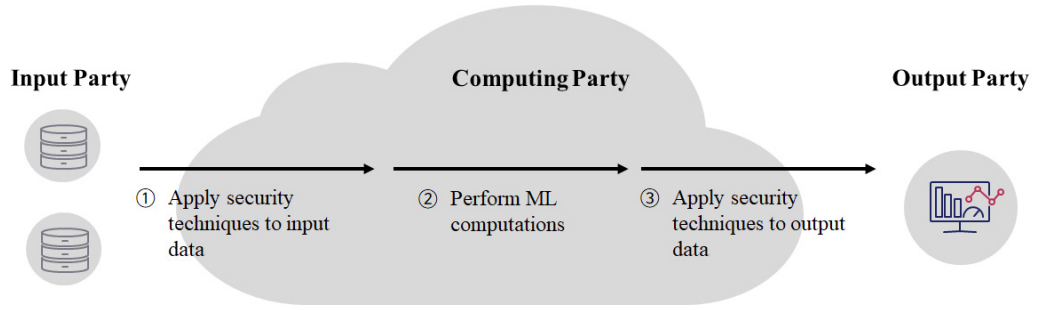
위에서 언급한 요인 외에도, 데이터 공유나 교환을 위해 신뢰를 제공할 수 있는 방안이 필요하며, 이를 위해 Audit Trail, 데이터 출처, Rating, IPR 등의 이슈가 정리되어야 한다. 또한 데이터 교환을 위한 Pricing, Metering, Invoicing 등의 서비스도 제공되어야 한다.

지금까지 안전한 데이터 교환을 위한 몇 가지 기술적 요건을 살펴보았다. 그러나 현재 강화되고 있는 개인정보보호 규제 환경에서 무신뢰 및 저비용 기반의 데이터 공유 및 교환을 위해서는 위에서 언급한 여러 기술적 요인 외에 차세대 개인정보보호 기술인 PETs 기술이 반드시 필요하다. 다음 장부터는 PETs 기술을 분류하고 최근 기술동향을 살펴보도록 하겠다.

## Ⅱ 차세대 개인정보보호 강화 기술 분류 및 기밀컴퓨팅

본 장에서는 데이터 결합분석 시 프라이버시 요구사항을 정의하고, 이러한 요건을 만족시킬 수 있는 기술을 분류한 후, 각 분야별로 기술동향을 간단히 살펴보겠다. [그림 1]에서와 같이 둘 혹은 그 이상의 Input Party가 데이터를 제공하고, 클라우드와 같은 Computing Party가 공유된 데이터를 받아 약속된 연산을 수행하고 그 결과를 Output Party에게 제공한다고 가정해보자. 이때 Input Privacy는 Computing Party에서의 결합분석을 위해 Input Party가 제공하는 Input Data 및 연산 과정에서의 어떤 중간결과도 데이터를 제공한 Input Party외에 노출되지 않아야 함을 의미한다. Output Privacy는 연산결과가 Output Party에게 제공될 때 민감한 개인정보나 재식별을 방지하는 것을 목표로 한다[3].

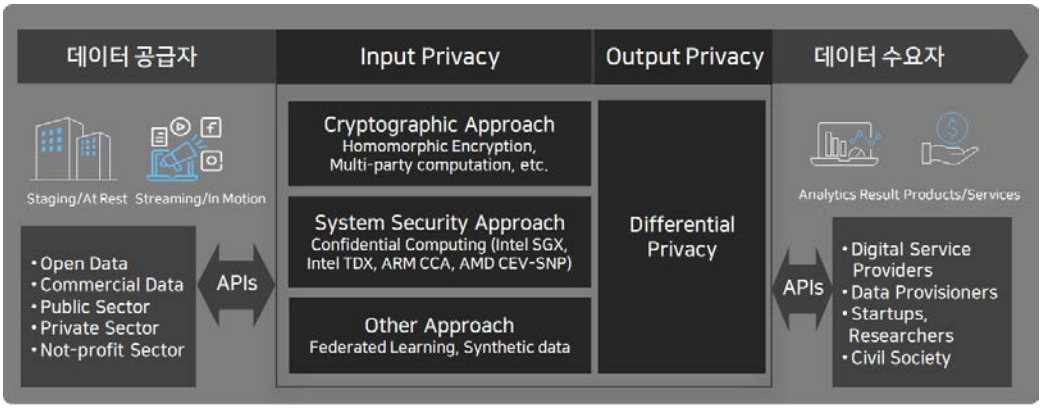
그림 1 개인정보보호 가능한 머신러닝 워크플로우 (ITU-T 기술문서, [4])



## 1. PETs(Privacy Enhancing Technologies) 기술 분류

Input Privacy를 제공하면서 데이터 결합분석을 가능하게 하는 두 가지 접근방법이 있다. 첫 번째로는 동형암호, 다자간 계산과 같은 암호(Cryptography)기술 기반 접근방법이 있으며, 두 번째로는 기밀컴퓨팅(Confidential Computing, CC)과 같은 시스템보안 접근 방법이 있다. 그 외에도 연합학습 및 합성데이터도 Input Privacy를 제공할 수 있다. 또한 차분 프라이버시 (Differential Privacy) 기술 등이 있다.[1)]

그림 2 데이터 결합분석에서의 프라이버시 요건



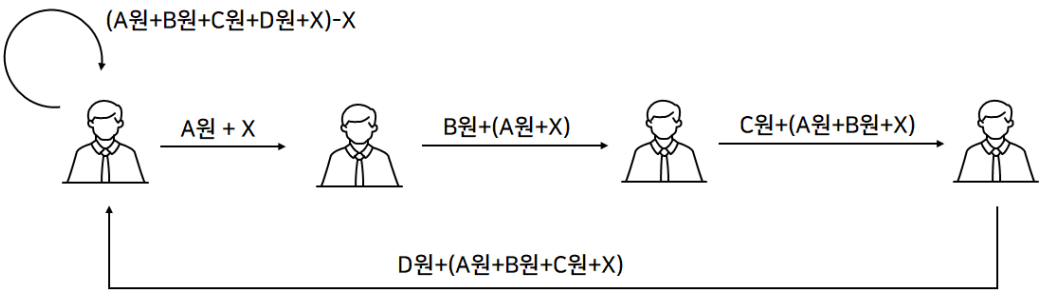

### 가. Input Privacy: 암호기술 기반 접근방식

동형암호, 다자간 계산과 같은 암호기술은 데이터를 암호화된 상태로 처리 혹은 분석하면서 Input Privacy를 제공할 수 있다. Gentry는 암호화된 상태에서도 연산이 가능한 동형암호(FHE, Fully Homomorphic Encryption)을 제안하였다[5]. 동형암호로 데이터를 암호화하여 외부로 전송하면 데이터를 처리하는 쪽에서는 해당 데이터에 대한 처리와 분석은 수행하지만 데이터에 대한 어떠한 정보도 알 수 없게 할 수 있다.

1) 한국정보통신기술협회에서는 Differential Privacy를 '차분 프라이버시'로 용어로 번역하고 있다.

혹은 다자간 계산(MPC, Multi-Party Computation)처럼 2개 이상의 조직이 각자의 데이터는 숨긴 채 공동의 목표인 특정 연산을 수행할 수도 있다. 이를 알기 쉽게 설명하면, [그림 3]과 같이 다자간 계산을 이용하여 특정 모임에서 각자의 연봉은 밝히지 않으면서 참석자들의 연봉의 합을 구할 수 있다. 먼저, 한 사람이 자신의 연봉에 특정 숫자를 더해 옆 사람에게 보내고, 그 숫자를 받은 사람은 받은 숫자에 자신의 연봉을 더해 옆 사람에게 보낸다. 이런 과정을 반복해서 처음 이 과정을 시작한 사람에게 숫자가 돌아오면, 그 숫자는 모든 사람의 연봉의 합에 자신이 더한 특정 숫자를 빼면 숫자가 된다. [그림 3]은 이해를 위한 예제이며, 실제 다자간 계산은 참여하는 조직의 입력 데이터를 숨기면서 분석이나 특정 연산을 진행할 수 있도록 수학적 암호기법을 사용하여 프로토콜을 설계한다.

그림 3 다자간 계산 (Multi-Party Computation) 예제




그러나 암호기술의 특성 상 설계사상의 안전성 외에도 알고리즘의 안전한 구현, 그리고 암호키 길이 등과 같은 보안파라미터 설정을 위해서 표준화가 필요하다. 안전한 암호알고리즘이라도 이에 대한 표준문서가 없다면 개발 시에 알고리즘을 안전하지 않게 구현하거나 충분한 보안성을 제공하는 파라미터를 사용하지 못하여 암호알고리즘이 보호하는 시스템이 취약해지는 사례가 많다. 무엇보다 동형암호의 경우 데이터 결합 시 데이터를 암호화된 상태에서 안전하게 분석할 수 있지만 이를 안전하게 복호화 할 수 있는 기술적인 가이드라인은 없는 상태이다. 따라서 암호기술 기반의 서비스가 제공되더라도 동형암호나 다자간계산을 안전하게 구현하였는지

검증할 수 있는 체계가 없는 상황이다.

표준화 동향으로는 ISO/IEC JTC 1/SC 27 (정보보안, 사이버 보안 및 개인정보보호) WG2(암호기술)에서 동형암호와 다자간계산 대한 표준화가 추진되고 있다. 먼저 4종의 동형암호 알고리즘에 대한 표준화 프로젝트(New Work Item Proposal)가 발의되었으며, 빠르면 '25년에 표준화가 완료될 예정이다. 다자간계산의 경우, Secrete Sharing 기반 다자간 계산이 표준화 마지막 단계에 와 있으며[6], 이외에도 Garbled Circuit 기반 다자간 계산, Oblivious Transfer와 같은 다양한 다자간계산 암호기술에 대한 신규 표준화 프로젝트가 WG2에서 논의되고 있다. ITU-T SG17 (정보보안)에서도 동형암호 기반 데이터 결합분석을 위한 보안 가이드라인 기술문서가 최근 채택된 바 있다[7].

그리고 동형암호의 경우 암호화된 상태에서 연산을 수행하다 보니 속도가 평문대비 연산속도가 느려지는 한계가 있다. 이를 극복하기 위해 DARPA DPRIVE (The Data Protection in Virtual Environment)[2]프로그램에서 동형암호로 암호화된 상태에서도 평문에서의 연산대비 10배 이내로 속도를 개선하는 것을 목표로 프로젝트를 진행 중이다. 또한, 칩셋 벤더에서도 FPGA기반의 동형암호 가속을 위한 여러 타입의 SW패키지를 개발하고 있다.[3] 이러한 성능 이슈에도 불구하고, 암호학적 기법의 장점은 안전하게 구현만 된다면 데이터의 안전성이 수학적으로 보장된다는 것이다. 또한 별도 HW 투자나 기존 인프라 변경 없이 다양한 환경에 유연하게 적용이 가능하다는 장점이 있다.

### 나. Input Privacy: 시스템보안 접근방식

금융권에서는 민감한 데이터를 보호하기 위해 오랫동안 시스템보안 접근방식을 사용해 왔다. 신용카드에 사용자의 민감한 정보를 보호하기 위해 Smart Card와 같은 HW 보안모듈을 사용하고 있으며, 데이터센터 내에서도 암호화 키 등 중요한

2) https://www.darpa.mil/program/data-protection-in-virtual-environments
3) https://www.intel.com/content/www/us/en/developer/articles/technical/homomorphic-encryption/accelerating-homomorphic-encryption-for-fpga.html

정보를 보호하기 위해서 Hardware Security Module과 같은 HW기반의 보안장비를 사용하고 있다. 이러한 특수 목적의 HW 보안모듈과 달리, 최근 일반 서버에서도 안전한 실행공간을 제공하는 기밀컴퓨팅(Confidential Computing, CC) 기술이 주목을 받고 있다. 현재 Linux Foundation Project로 진행되고 있는 Confidential Computing Consortium (CCC)[4]에서는 특히 틀라우드 환경에서의 기밀컴퓨팅 기술 확산을 위해 조직되어 운영되고 있으며, Intel, AMD, ARM, Google, Microsoft, RedHat 등 빅테크 기업이 참여하고 있다. 기밀컴퓨팅에 대해서는 다음 장에서 자세하게 살펴보도록 하겠다.

### 다. Input Privacy: 기타 방식

앞에서 언급한 기술들을 사용할 때에는 어떤 형태로든 데이터를 외부로 전송해야 한다. 반면, 연합학습(Federated Learning)은 데이터를 외부로 보내지 않고 로컬 기기나 환경에서 수집, 저장된 데이터 기반으로 학습한 결과를 중앙에서 수집하여 최종 분석을 완료하는 것이 가능하다. 그러나 연합학습은 데이터의 양이 부족한 경우 사용하는 기법이며, 수직적 데이터 결합분석은 불가능하여 금융권에서와 같이 이종간의 데이터 결합분석에 사용하기에는 한계점이 존재한다.

그리고 많은 경우 분석가들이 직접 데이터를 들여다보고 분석/처리할 필요가 있다. 합성데이터는 원자료와 동일한 통계적, 확률적 분포를 따르도록 생성된 자료이다. 특정 통계분포로부터 생성된 합성데이터는 다른 유형의 통계분석에 사용 시에는 정확성이 떨어진다는 단점이 있다. 최근에는 Generative AI 기반으로 합성데이터를 만드는 연구가 활발히 진행되고 있으며, 금융권에서도 합성데이터 활용 가능성에 대한 논의가 진행 중이다.[5]

4) https://confidentialcomputing.io/
5) 금융 분야 합성데이터 세미나 (2023.6.20., 금융보안원 개최)

### 라. Output Privacy

Output Privacy를 달성할 수 있는 한 가지 방안으로 데이터를 외부에 공유할 때 이전에 공유된 정보를 결합하여 특정 개인정보가 재식별이 되는 것을 방지하기 위해, Output Party에 제공하는 데이터 혹은 데이터 분석과정이나 처리과정 중에 노이즈를 더하는 것을 생각해볼 수 있다. Dwork[8, 9]에 의해 처음 제안된 차분 프라이버시 기술(Differential Privacy)은 개인정보를 수집할 때나, 혹은 조직이 데이터를 외부에 공유할 때 개인정보보호수준(Privacy Budget)을 정하고 해당 목표수준 안에서 데이터 노출정도를 제어할 수 있어 새로운 Privacy Measurement 방법론으로 주목받고 있다. 미국 NIST에서는 2018년에 차등정보보호에서 요구하는 개인정보보호 수준을 만족하는(Provable Guarantee) 합성데이터 생성 알고리즘에 대한 경진대회를 개최하기도 하였다.[6)]

물론 기존에도 개인정보 노출을 측정하기 위한 K-익명성과 같은 프라이버시 보호 모델이 존재하였지만, 이는 재식별과 같은 기술적인 한계점 뿐 아니라, 이러한 보호모델을 제대로 적용하면 상당한 정보손실이 발생한다. 특히, 데이터의 속성자(Attribute Value)가 늘어날수록 더 많은 데이터 삭제가 필요하여 'Curse of Dimensionality'이슈가 발생 한다[10]. 또한 K-익명성을 만족하더라도 동질적(Homogeneity) 공격 등이 가능하여, L-다양성(L-Diversity) 혹은 T-접근성(T-Closeness) 등의 추가적인 프라이버시 모델 적용이 필요하다. 특히, 데이터 결합 시에는 케이스마다 재식별의 리스크를 평가하는 적정성 평가 단계를 거치게 되어 상당한 비용과 기간이 소요되어 필연적으로 효율성이 떨어지게 된다. 무엇보다 차분 프라이버시 기술의 강점은 데이터 분석 및 공유 플랫폼이나 PETs 기술과 결합하여 프라이버시 노출과 평가를 자동화하고 할 수 있다는 점이다.

6) NIST. "2018 Differential Privacy Synthetic Data Challenge"

## 2. 기밀 컴퓨팅(Confidential Computing)

본 장에서는 개인정보보호 강화기술 중 기밀컴퓨팅(Confidential Computing, CC)기술에 대해서 상세히 살펴보겠다. 기밀컴퓨팅 환경에서 어플리케이션이나 데이터를 운영하게 되면, 주변에 실행중인 다른 어플리케이션, 운영시스템, 가상화 계층, 인프라, 그리고 시스템 운영자나 서비스 제공자의 접근을 차단할 수 있다.

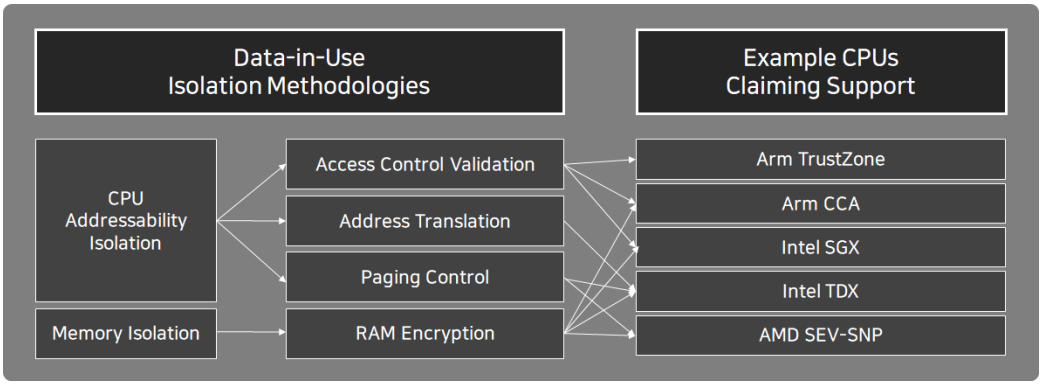
기밀컴퓨팅은 HW기반의 검증된(attested) 신뢰할 수 있는 실행환경(Trusted Execution Environment, TEE)을 제공하며,[7] 기밀컴퓨팅에서 정의한 TEE는 데이터의 무결성(data integrity), 데이터의 기밀성(data confidentiality), 코드 무결성(code integrity)을 기본적으로 제공해야 한다. 즉, 기밀컴퓨팅은 데이터 보호 뿐 아니라 데이터를 처리하는 어플리케이션에 대한 보호 기능도 제공한다. 또한, 기밀컴퓨팅은 사용자의 워크로드(어플리케이션, 데이터)가 사용자가 의도한 TEE를 지원하는 CPU에서 실행되었는지 확인할 수 있는 수단을 제공한다. 즉, 원격 플랫폼이 TEE 기술을 지원하는 Intel 혹은 AMD CPU인지를 확인할 수 있으며, 이는 공개키 기반의 증명(attestation) 기능을 통해 제공한다. 이로써, 사용자는 민감한 프로그램이나 데이터가 TEE가 없는 CPU에서 실행되거나, 인가되지 않은 프로그램이 TEE에서 실행되는 것을 방지할 수 있다.

한 가지 주목할 점은 동형암호와 같은 암호학적 접근방식과 달리 기밀컴퓨팅은 코드의 무결성도 제공한다는 점이다. 동형암호기반으로 데이터를 공유하는 경우 데이터 소유자가 암호화한 데이터를 전송하여 특정 연산을 수행할 때 기존에 약속된 연산을 변경하여 연산결과로부터 원본데이터의 유출을 가능하게 하는 공격이 가능하다. 그러나 기밀컴퓨팅에서는 데이터를 공유하거나 특정 원격 플랫폼에 전송하기 전에 전송될 데이터를 처리하는 어플리케이션 또는 코드가 의도된 대로 동작되는지, 또는 기존 코드로부터 위변조가 일어났는지를 위에서 언급한 'attestation' 기능을 통해 확인할 수 있다.

---

7) Confidential Computing Consortium에서는 Confidential Computing을 다음과 같이 정의하고 있다. "Confidential Computing is the protection of data in use using hardware-based, attested Trusted Execution Environments." [11]

그림 4 HW기반 격리기술 및 지원 CPU 예제[11]




위에서 '보호'한다는 용어를 사용하였는데, TEE의 HW나 Firmware는 아래의 방식으로 코드와 데이터를 보호할 수 있다[11].

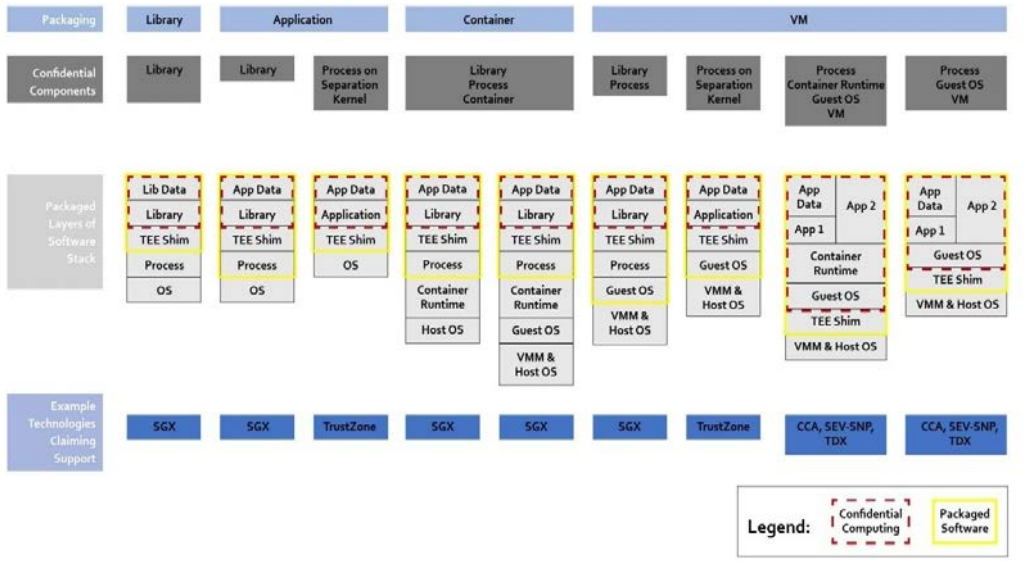
1. Access Control Validation: 메모리 영역의 접근을 특정 프로세스나 컨텍스트로 제한할 수 있다.
2. Address Translation: TEE 영역 밖에서는 메모리 세그멘테이션 정보에 접근할 수 없다.
3. Paging Control: TEE로 보호되는 데이터가 동작할 때 TEE 영역 밖의 프로세스는 CPU를 사용할 수 없다.

물론 공격자가 CPU를 통해 특정 데이터에 대한 접근이 불가하다면, Side Channel 공격 등을 통해 메모리에 있는 민감한 데이터에 대한 접근이 가능하다. 이러한 공격을 차단하기 위해 메모리(RAM)에 있는 데이터를 암호화하고 해당 데이터가 CPU 안에서만 복호화될 수 있도록 하는 것이 가능하다. TEE 모드에서 실행되는 모든 CPU 명령은 데이터를 메모리로 내보내기 전에 암호화하고 메모리에서 읽기 전에 복호화 하는 방식으로 특별히 설계되었으며, 연산과 암복호화가 하나의 CPU 명령으로 실행되도록 만들어져 있어 그 사이에 다른 명령이 개입하여 평문을 취하는 것이 HW적으로 불가능하다. 이로써, CPU와 메모리 사이에 오로지

암호화 된 데이터만 존재하는 기밀한 논리적 실행 환경이 만들어진다.

또한, CPU 명령어 내부에 구현된 HW 로직이 암복호화를 수행하므로 속도 저하가 거의 없으며, 이로 인해 기존에 불가했던 연산중인 데이터(data-in-use)에 대한 보호를 보장할 수 있게 된다. 또한, 저장된 데이터(data-at-rest)와 전송 중인 데이터(data-in-transit)에 대한 기존 보호 기술을 함께 적용할 경우, 비로소 클라우드 상에서 완전한 end-to-end 데이터 보안을 구현하는 것이 가능해진다. [그림 4]와 같이 프로세서 공급자들은 여러 기법을 조합하여 기밀컴퓨팅 기능을 제공한다. 기존에는 기밀컴퓨팅이 CPU 프로세스에서만 제공되었지만, 최근 GPU 환경에서도 기밀컴퓨팅이 제공되고 있다.[8)]

**그림 5** CC 적용을 위한 패키징 예제 [11]




출처: 상기 그림은 CCC (2022), "Common Terminology for Confidential Computing"에서 발췌.

8) https://www.nvidia.com/en-us/data-center/solutions/confidential-computing/

위에서 언급한 것처럼 기밀컴퓨팅에서는 TEE 환경 안에서 코드와 데이터 모두를 보호할 수 있으며, 보호하고자하는 패키징 대상에 따라 CCC[9]에서는 아래와 같이 용어를 정의하고 있다[11].

1. Confidential library: 특정 라이브러리를 TEE 안에서 실행하여 다른 라이브러리나 호스팅 환경으로부터 보호할 수 있다.
2. Confidential process: 특정 프로세스 혹은 어플리케이션을 TEE 안에서 실행하여 다른 프로세스나 호스팅 환경으로부터 보호할 수 있다.
3. Confidential container: 특정 컨테이너 이미지를 TEE 안에서 실행하여 다른 컨테이너나 호스팅 환경으로부터 보호할 수 있다.
4. Confidential VM: 특정 VM을 TEE 안에서 실행하여 하이퍼바이저 등의 호스팅 환경으로부터 보호할 수 있다.

[그림 5]는 실제로 보호하고자 하는 다양한 계층의 소프트웨어를 어떻게 패키징하여 기밀컴퓨팅으로 보호할 수 있는지 보여준다. 붉은색으로 표기한 영역이 TEE 안에서 실행되는 소프트웨어 계층이며, 노란색이 함께 패키징되어야 하는 영역을 나타낸다.

## III PETs 기술의 금융권 활용 방안

현재 국내 금융권에서 둘 이상의 조직이 데이터 결합을 진행하기 위해서는 별도의 신뢰기관을 통해 데이터 결합키를 제공받아 데이터 결합을 진행해야만 하는데, 그 이유는 결합키 생성과정에서 결합기관이 다른 정보와 결합하여 특정 개인을 재식별 하는 것이 기술적으로 가능하기 때문이다. 또한 결합과정에서 KLT기반의 프라이버시 보호모델을 만족하는지 적정성 평가를 진행해야하며,

9) https://confidentialcomputing.io/

이에 따라 결합에 사용되는 기간 및 비용이 늘어나게 된다. 또한, 결합과정을 거쳐 적정성 평가를 거친 데이터를 외부로 전달할 시 기술적으로 재식별 방지가 불가능하여 정책적으로 재식별을 방지할 수밖에 없다.

시장 리서치 기관은 앞서 언급한 데이터 공유 활성화를 위한 여러 기술적인 요건이 갖추어지는 데에는 5~10년이 소요될 것으로 예상하고 있으나[12], 현재 시장에서 제공되는 기술만을 활용하더라도 금융권에서 시도하고 있는 데이터 결합서비스를 안전하고 효과적으로 제공할 수 있다. 지금부터는 별도의 신뢰기관 없이, 기술적으로 재식별을 방지하면서 자동화된 데이터 결합서비스를 제공할 수 있는 방안을 제시하고자 한다. 먼저 TEE 환경을 제공하는 서버를 보유한 조직이 Computing Party로서 역할을 수행할 수 있으며, 데이터 결합을 원하는 조직들이 Input Party가 되어 TEE상에서 데이터 결합을 진행한다. 자세한 워크플로우는 아래와 같다.

1. Input Party들은 기밀 컴퓨팅에서 제공하는 'attestation'을 통해 Computing Party내 데이터결합을 진행할 서버가 CC기능(TEE 환경)을 제공하는 것을 확인하고, 서버의 TEE 환경에서 동작하는 어플리케이션이 사전에 협의된 방식으로 수행되는지 확인한다.
2. Input Party는 데이터 결합키 생성을 위한 최소한의 데이터를 암호화하여 Computing Party내 TEE 환경으로 전송한다.
3. Computing Party는 TEE 환경에서 전송된 데이터를 복호화 한 후 결합키를 생성하여 Input Party로 암호화하여 전송한다.
4. Input Party는 결합키에 해당하는 데이터를 암호화하여 Computing Party의 TEE 환경으로 보낸다.
5. Computing Party는 TEE내에서 전송된 데이터를 복호화하여 결합을 수행한 후, TEE 환경내에서 합성데이터를 생성하여 Output Party로 전송한다.[10]

10) Generative AI 기반으로 합성데이터를 생성 시에 모델 학습에 상당한 컴퓨팅 리소스가 필요하여 기존 암호기술기반

위에서 언급한 바와 같이, TEE를 활용할 시 성능저하 없이, 민감 데이터의 보호 뿐 아니라 TEE안에서 데이터를 처리하는 로직에 대한 위변조 또한 방지할 수 있다. 무엇보다 데이터 결합 후, 결합에 사용한 데이터에 대한 삭제 또한 데이터 제공자 측에서 기술적으로 확인이 가능하여 높은 신뢰도를 제공할 수 있다. 즉, Computing Party에서 데이터 결합을 수행하고 관련된 모든 데이터를 삭제하는 로직을 추가로 수행하도록 코드를 작성하고 데이터 결합을 위해 데이터를 전송하기 전 해당 로직이 변경되었는지 기밀컴퓨팅에서 제공하는 'attestation' 기능을 통해 확인할 수 있다.

그리고 Output Privacy 제공을 위해 합성데이터 생성시점에 차분 프라이버시 기술을 적용할 수 있다. 또한, 위와 같은 방식으로 데이터 결합을 진행할 시 기존 KLT프라이버시 모델을 사용하게 되어 상당한 데이터 손실이 일어나 Utility가 떨어지는 문제가 있었으나, 합성데이터 기반으로 데이터를 생성하게 되면 개인정보는 보호하면서 원본 데이터와 유사한 Utility를 제공할 가능성이 높아진다.

## Ⅳ 결론

본 기고서를 통해 데이터 공유 활성화를 위해서는 PETs 기술 외에도 다양한 기술적 요건이 있음을 살펴보았고, 한 가지 PETs 기술로 데이터 공유 및 결합을 위한 프라이버시 요건을 만족할 수 없다는 것을 확인할 수 있다. 현재 업계에서 제공하고 있는 기술로도 별도의 신뢰기관 없이 금융권에서의 데이터 결합을 안전하고 빠르게 진행할 수 있는 방안이 존재한다. 데이터 공유 활성화를 위해 더 넓은 시야로 기술을 조망하고 이를 빠르게 검증해 볼 수 있어야 하겠다.

으로는 현실적인 적용이 불가하였다. 그러나 최근 GPU 환경에서도 기밀컴퓨팅이 지원되어 평문 성능저하 없이 모델 학습이 가능하다.

## 참고문헌

[1] World Economic Forum (2021). “Towards a Data Economy: An enabling framework”

[2] UNECE (2022). “Open technical consultation on Towards a trustworthy Multi-Party Secure Private Computing-as-a-service infrastructure for official statistics”

[3] UN (2023). “UN PET Guide”

[4] ITU-T (2023). “Technical Report: FHE-based data collaboration in machine learning”, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17999

[5] Gentry, Graig (2009). “A Fully Homomorphic Encryption Scheme”. Ph.D. Thesis

[6] ISO/IEC FDIS 4922-2 (Information Security - Secure multiparty computaiton - Part 2: Mechanisams based on secret sharing

[7] IUT-T Q7/17, “TR.sgfdm (Technical Report: FHE-based data collaboration in machine learning)”

[8] Dwork, Cynthia et. al (2006). “Calibrating noise to sensitivity in private data analysis”. 《Theory of Cryptography: Third Theory of Cryptography Conference, TCC》Proceedings 3: 265-284

[9] Dwork, Cynthia (2006). “Differential Privacy”. 《International colloquium on automata, languages, and programming》: 1-12

[10] Aggarwal, Charu C (2005). “On k-anonymity and the curse of dimensionality”. 《VLDB '05》: 901-909

[11] CCC (2022), “Common Terminology for Confidential Computing”

[12] Gartner (2023), “Hyper Cycle for Data Security, 2023”

# 유럽 디지털 신원지갑의 출현과 우리 금융권에 미치게 될 영향

**이종혁***



* 세종대학교 교수

# 요약

2023년 11월 현재 대한민국에서 사용되고 있는 신원확인 수단은 계속해서 발전하고 있다. 하지만, 여전히 신원확인이라는 그 본래의 목적에 충실하다. 이러한 신원확인은 내가 대학을 졸업한 사람이라는 것을 증명하지 못하고, 내가 직장인이라는 것도 증명하지 못한다. 그때그때 필요할 때마다 각각의 증명서를 신원확인을 통해 검증받아야 한다. 그러한 증명서를 따로따로 보관해야 하는 것을 당연시 여긴다.

하지만, 이 모든 것들은 불편하고 비효율적이며, 신원확인이나 증명서를 발급 받는 과정에서 개인의 프라이버시가 과도하게 침해되거나 유출 될 염려가 있다. 내가 누구인지 간편하게 증명하고, 여러 증명서를 하나의 앱에서 관리하며, 꼭 필요한 개인정보만을 제공하는 길이 유럽에서 열리고 있다.

본 고에서는 유럽에서 빠르게 이루어지고 있는 디지털 혁신 중 하나인 디지털 신원지갑에 대해서 살펴보고, 우리 금융권에 미치게 될 영향에 대해서 살펴본다.


# 03 유럽 디지털 신원지갑의 출현과 우리 금융권에 미치게 될 영향

## I 시작하며

우리가 신원을 확인하는 이유가 뭘까? 이종혁이라고 말하는 이 사람이 정말 그 이종혁인지 확인해야만 그에 적합한 서비스를 제공해 줄 수 있기 때문이다. 어찌 보면, 금융 서비스를 제공하는 금융기관에서 신원확인 절차는 가장 먼저 이루어지는 것이기도 하다. 이러한 신원확인은 여러 가지 방법을 통해 이루어 질 수 있다. 아직까지도 은행 창구에 가면, 주민등록증/운전면허증과 같은 신분증을 요구하는 것이 당연시되고 인터넷/모바일 뱅킹을 사용하기 위해서는 인증서 기반의 신원확인이 일반적이다.

우리사회는 코로나19를 거치면서 많은 것들이 변했다. 사람들은 더더욱 개인화 되고, 온라인상에서 여가를 즐기고 업무를 수행하는 것이 일반화 되었다. 다시 말해, 사람들은 비대면으로 할 수 있는 그리고 비대면으로 하는 게 더 효율적인 일들이 무엇인지 알게 되었다. 금융 서비스도 마찬가지다. 많은 사람들은 바쁜 시간을 쪼개 은행에 도착해 대기표를 받고 은행 창구 앞에서 기다리는 일을 하고 싶지 않다. 어색하게 무엇 때문에 은행에 왔는지도 일일이 설명하고 싶지도 않다. 익숙한 인터넷 뱅킹이나 편리한 모바일 뱅킹을 통해 다양한 금융 서비스를 손가락 몇번의 터치로 편리하게 제공 받을 수 있다. 하지만, 여전히 인터넷/모바일 뱅킹은 인증서 기반의 신원확인이 요구된다.

우리는 편리한 것을 추구한다. 내가 이종혁이라는 것을 증명하기 위해 매번 서로 다른 서비스 제공자에게 그들이 요구하는 형태로 계속해서 신원확인을 받고 싶지

않다. 내가 대학을 졸업한 사람이라는 것을 증명해야 하고, 내가 운전 할 자격을 가지고 있다는 것을 증명해야 하고, 내가 서울에 거주하는 성인이라는 것을 증명하기 위해 매번 다른 서비스 제공자에게 신원확인을 받고, 그에 따른 증명서를 받아 따로따로 보관하고 싶지도 않다. 물론, '나'라는 것을 증명하기 위해 불필요한 내 개인정보가 그들에게 제공되는 것도 원치 않는다. 이 모든 것들이 다 불편하고 비효율적이며, 개인의 프라이버시가 과도하게 침해되거나 유출 될 염려가 있다. 내가 누구인지 간편하게 증명하고 내가 누구인지 간편하게 확인 할 수 있게 하고, 여러 가지 증명서를 하나의 앱에서 관리하며, 꼭 필요한 개인정보만을 제공하길 바란다. 이러한 멋진 일이 유럽에서 일어나고 있다. eIDAS 2.0 이라는 유럽연합의 법적 규정 [1]과 유럽 디지털 신원지갑(EUDI Wallet, EU Digital Identity Wallet)을 통해서 말이다[2].

본 고에서는 유럽에서 빠르게 이루어지고 있는 디지털 혁신 중 하나인 디지털 신원지갑에 대해서 살펴보고, 우리 금융권에 미치게 될 영향에 대해서 살펴본다.

## Ⅱ 우리의 신원확인 수단

1962년 주민등록법을 제정해 전국민을 대상으로 12 자리의 주민등록번호를 발급했다. 현재 우리가 사용하고 있는 주민등록번호는 1975년 주민등록법 시행령과 시행규칙의 개정으로 만들어진 13자리로 숫자이며, 이를 통해 생년월일, 성별 및 출생지역을 식별 할 수 있다. 국민을 관리하기 위한 번호로 시작됐지만, 주민등록번호는 우리나라 행정 편의성을 높였으며 신원확인의 근간으로 그 역할을 충분히 했다.

주민등록번호는 분명 행정의 편리성을 높이긴 했지만, 초기 인터넷 환경에서의 본인확인 수단으로써의 국민의 개인정보를 여과 없이 노출시키는 문제를 야기했다. 이를 해소하기 위한 방안으로 2013년 8월부터 인터넷과 같은 온라인 환경에서

민간이 주민등록번호를 수집하고 이용하는 것을 금지하였으며, 공공부문에서도 2015년 2월부터 법령에 근거하지 않은 경우 주민등록번호를 수집하는 것을 전면 금지시켰다. 이와는 별개로 우리 정부는 강력한 보안기능을 제공하면서 개인정보 노출을 줄이고자 1999년 2월 전자서명법을 제정하고 이를 통해 공인인증서의 도입하였으며, 온라인상에서 주민등록번호를 대체하기 위한 수단으로 2006년 10월 아이핀(i-PIN)의 활용 등을 추진했었다. 하지만, 잘 알다시피 공인인증서는 그 역할을 다 했으며, 아이핀은 여전히 활용도가 떨어지고 있다.

법률 제5792호에 의해 전자서명법이 1992년 2월 5일 제정되었다. 이는 그 당시 일어나고 있던 인터넷 붐에 의해 전자상거래를 활성화하기 위한 새로운 신원확인 수단이었으며, 공인인증서 기반의 전자상거래, 인터넷뱅킹, 전자정부의 시작이었다. 공인인증기관에서 인증한 전자서명은 법령이 정하는 서명 또는 기명날인과 동일한 법적 효력을 가지게 되면서, 공인인증서가 2020년 12월 10일 완전한 폐지가 될 때까지 우리 사회에서 신원확인을 위한 강력한 수단이었다. 공인인증서 폐기의 계기가 된 '별에서 온 그대'라는 당시 TV 드라마는 공인인증서에게는 '별에서 온 날벼락'과 같은 존재가 아닐까 생각 된다.

온라인상에서 개인정보보호에 대한 관심이 높아지면서, 그리고 계속해서 발생하는 보안 사고를 통한 주민등록번호의 대량 유출에 의해, 가상의 주민번호를 발급하고 이를 온라인상에서 활용하고자 하는 노력으로 2006년 10월 아이핀이 세상에 발표되었다. 주민등록번호를 가지는 대한민국의 성인 뿐만 아니라 국내에 거주하는 외국인에게도 아이핀을 발급하고, 초중고등학생에게 까지 아이핀을 보급하고자 노력을 했지만, 발급과 이용의 불편함 등으로 인해 널리 사용되지 못하고 있는 실정이다.

전자서명법 전부개정안이 2020년 5월 20일 국회를 통과하면서 사설인증서의 시대가 시작되었다[3]. 공인인증서와 기술적으로 같은 공개키기반구조(PKI, Public

Key Infrastructure)를 사용하는 사설인증서는 스마트폰에서 제공하는 생체인증 기술과 결합해 더욱 간편하고 강력한 신원확인 수단으로 자리 매김하고 있다.

새로운 신원확인 수단으로 빼놓지 않고 언급을 해야 할 것은 모바일 신분증이다. 2020년 6월 발표된 '디지털 정부혁신 발전계획'에 따라 전국민이 온라인뿐만 아니라 오프라인에서도 사용할 수 있는 디지털 신분증으로 스마트폰에 저장해 사용할 수 있는 모바일 신분증 개발이 시작되었다. 모바일 신분증의 첫 번째 결과물로 모바일 운전면허증이 2022년 1월 시범 서비스를 시작으로 2022년 7월 전국적으로 발급이 확대 되었다. 또한, 2023년 6월부터는 국가보훈등록증도 모바일 신분증으로 발급되기 시작했다. 모바일 신분증에 대한 첫 번째 표준화로 모바일 운전면허증이 한국정보통신기술협회(TTA, Telecommunications Technology Association)를 통해 2023년 12월 제정 목표로 개발되고 있다. [그림 1]은 현재 대한민국에서 사용가능한 모바일 운전면허증이다[4].

그림 1 모바일 운전면허증

분산원장기술(DLT, Distributed Ledger Technology)이 적용된 우리나라의 모바일 신분증은 자기주권신원(SSI, Self-Sovereign Identity)을 탈중앙화 방식으로 구현한 분산식별자(DID, Decentralized IDentifier) 기술을 이용한다. 이를 통해 꼭 필요한 정보만을 신원확인에 제공하기에 개인정보보호 관점에서 큰 진전을 가지고 있다고 말할 수 있다. 또한, 단순히 온라인에서만 사용이 가능한 신원확인 수단을 넘어서 오프라인에서도 법적으로 동등한 위치를 가지는 신원확인 수단이기도 하다.

2023년 11월 현재 대한민국에서 사용되고 있는 신원확인 수단은 계속해서 발전하고 있다. 하지만, 여전히 신원확인이라는 그 본래의 목적에 충실히 하고 있다. 특히, 우리나라의 모바일 신분증을 내부적으로 살펴보면, 사용자의 스마트폰에 탑재된 전자지갑에 모바일 신분증을 담고 있는 것인데, 이것을 여러 가지 증명서를 담는 형태로의 진화는 아직까지 이루어지지 않고 있다.

## Ⅲ 유럽의 움직임

우리나라가 1992년 온라인에서의 전자상거래 활성화를 위해 전자서명법을 제정한 것과 비슷하게 유럽에서도 1999년 '전자서명지침'을 제정해 유럽연합 회원국들이 디지털 단일시장을 갖고자 하였다. 하지만, 이러한 시도는 쉽게 이루어지지 않았다. 유럽연합 회원국들이 통일된 법제도를 가지고 단일한 디지털 시장을 만들기 위한 노력은 2016년 7월 1일부터 시행된 '유럽연합 전자신원확인 및 신뢰서비스에 관한 규정(eIDAS, electronic Identification, Authentication and Trust Services)'에 의해 가능해졌다[5]. 이를 통해 유럽연합은 온라인상에서의 신원확인과 전자서명(electronic signature), 전자인장(electronic seal), 전자시점확인(electronic time stamp), 전자등기배달서비스(electronic registered delivery service) 등과 같은 다양한 신뢰서비스(trust service)를 제공할 수 있게 되었다.

유럽연합은 여기에서 그치지 않고, 기존 eIDAS 규정을 보완하는 개정안 eIDAS 2.0 을 2021년 6월 3일 유럽의회와 이사회에 제출하였다. 개정안 eIDAS 2.0는 코로나19를 거치면서 폭발적으로 늘어난 비대면 서비스에 대한 요구, 공공을 넘어선 민간 서비스의 폭발적 성장, 일반개인정보보호법(GDPR, General Data Protection Regulation) 준수 등을 반영하며, 분산원장기술과 같이 새롭게 등장하는 기술을 수용하고 있다.

개정안 eIDAS 2.0는 유럽연합 회원국들이 각 나라의 국민과 거주자에게 유럽 디지털 신원지갑(EUDI Wallet) 발급을 의무화하고 있다. 유럽 디지털 신원지갑을 통해 자신의 신원확인을 위한 데이터에 대해서 사용자 독점적인 관리, 즉 자기주권신원(SSI)이 가능토록 하고 있으며, 온라인뿐만이 아니라 오프라인에서도 신원확인의 도구로 사용하고 공공이나 민간 서비스에서도 사용할 수 있다. 여기까지만 듣고 보면, 우리나라에서 사용 중인 모바일 신분증과 크게 달라 보이지 않는다. 모바일 신분증도 내부적으로 전자지갑을 가지고 있으며, 신원확인에 사용되기 때문이다. 하지만, 유럽의 디지털 신원지갑과 우리의 모바일 신분증과는 다음과 같은 부분에서 큰 차이를 가진다.

- 공공뿐만이 아니라 교통, 에너지, 금융, 건강, 교육, 통신과 같이 공공성이 높은 민간 서비스에서도 사용 의무화
- 신원확인 뿐만이 아니라 공공 및 민간에서 발행하는 다양한 증명서 탑재 가능
- 신원확인 및 증명서 발급을 위해 제공된 개인정보를 추적 가능
- 개인뿐만이 아니라 법인에게도 발급 가능

우리나라의 모바일 신분증도 신원확인 수단으로 편리하다고 생각되지만, 유럽의 디지털 신원지갑은 단순히 신원확인 수단을 넘어서 온오프라인에서 사용 가능한 전자지갑의 끝판왕 같아 보인다. 게다가, 유럽의 디지털 신원지갑은 단일국가에서 사용되는 것이 아니라 유럽연합 회원국들에 거주하는 개인들과 법인까지 다양한 구성원이 사용하게 된다. 특히, eIDAS 규정은 유엔국제상거래법위원회(UNCITRAL,

United Nations Commission on International Trade Law)와 같이 국제적인 전자상거래 입법에도 영향을 미치고 있기에, 개정안 eIDAS 2.0 이 예상대로 2024년 초에 공식적으로 채택되면, 그 파급력은 유럽연합을 넘어 전세계적으로 미치게 될 것이 자명하다. 예를 들어, 개정안 eIDAS 2.0이 문제없이 2024년 1분기에 규정으로 발효되면, 유럽연합 회원국들과 유럽연합에 전자상거래와 같은 서비스를 제공하는 기업들은 18개월 이내에 디지털 신원지갑과 관련 서비스 제공할 준비를 마쳐야 하는 상황이다. 시간이 많지 않다.

## Ⅳ 유럽의 디지털 신원지갑

### 1. 유럽 디지털 신원지갑의 정의와 유즈케이스

유럽연합은 디지털 단일시장을 이루기 위해 유럽 디지털 신원지갑(EUDI Wallet)을 개발하고 있다. 개정안 eIDAS 2.0에서 유럽 디지털 신원지갑은 사용자가 자신의 식별데이터 및 관련 속성을 저장하고, 필요시 해당 정보 및 자신의 전자서명, 전자인장 등을 생성하는 제품이나 서비스로 정의된다. 유럽 디지털 신원지갑에 대한 첫 번째 기술 문서로써, 2023년 1월 26일 유럽 디지털 신원지갑 아키텍처와 참조 프레임워크 문서(The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework - The European Digital Identity Wallet Architecture and Reference Framework, v1.0.0)가 공개됐다[2]. 문서의 제목에서 나타나듯이 유럽 디지털 신원지갑을 구현하는데 있어서 필요한 아키텍처와 참조 프레임워크(ARF, Architecture and Reference Framework) 정보를 제공하고 있으며, 계속적으로 업데이트 될 예정이다.

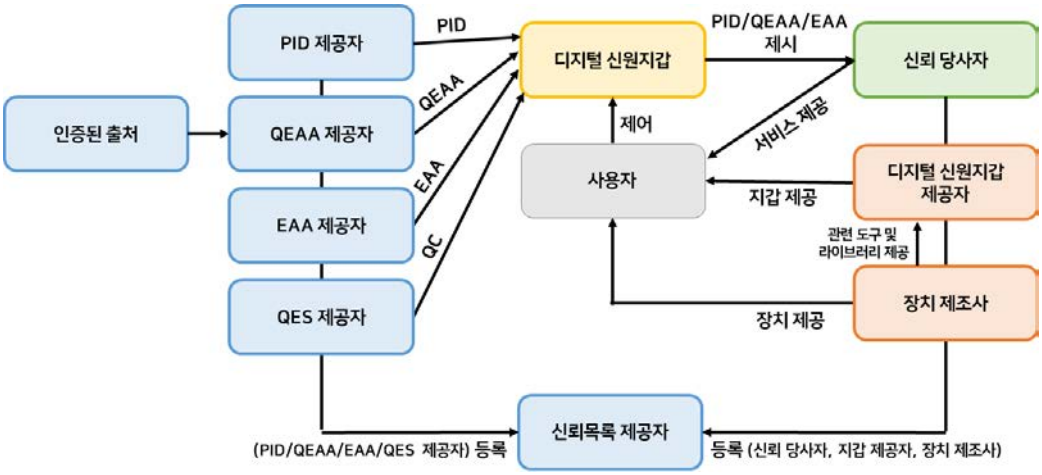
유럽 디지털 신원지갑의 ARF v1.0.0을 개발하기 위해 다음과 같은 초기 유즈케이스를 정하고 필요한 엔티티와 기능 요소들을 정의했다.

- Secure and trusted identification to access online services: 유럽 디지털 신원지갑을 통해 유럽 내에서 제공되는 공공뿐만 아니라 민간 분야의 다양한 온라인 서비스를 이용할 수 있다. 다시 말해, 온라인 로그인을 위해 디지털 신원지갑을 사용할 수 있다는 이야기가 된다.
- Mobility and digital driving licence: 유럽 내에서 통용되는 온오프라인의 운전면허 확인 수단을 넘어 관련된 다양한 서비스와 연계할 수 있다. 다시 말해, 도로교통법령 위반 정보 확인 및 범칙금/과태료 등을 디지털 신원지갑의 전자지급결제 서비스를 통해 납부가 가능하게 된다.
- Health: 유럽 디지털 신원지갑은 개인의 건강 정보를 저장할 수 있다. 예를 들어, 특정 질병에 대한 증명서를 통해 유럽 내에서 의료 서비스를 받을 때 제공할 수 있으며, 미리 발급 받은 처방전을 통해 다른 지역이나 국가에서 필요한 약을 처방 받을 수 있게 된다.
- Educational credentials and professional qualifications: 교육기관의 졸업장이나 특정 기술을 가지고 있다는 증명서를 디지털 신원지갑을 통해 제공할 수 있다. 예를 들어, 특정 대학의 특정 학과를 졸업 했다는 정보를 증명서 형태로 제공할 수 있게 된다.
- Digital Finance: 유럽 내에서의 온오프라인 결제 또한 디지털 신원지갑을 통해 이루어질 수 있다.
- Digital Travel Credential: 유럽 내에서의 여행 자격과 관련 된 증명서를 제공하는데도 디지털 신원지갑이 이용될 수 있다.

## 2. 유럽 디지털 신원지갑의 생태계

유럽 디지털 신원지갑 생태계는 [그림 2]와 같은 엔티티로 이루어진다. 생태계 안에서 유럽 디지털 신원지갑은 다양한 제공자로 부터 자신의 식별데이터 및 관련 속성을 제공 받고, 필요시 해당 정보 및 자신의 전자서명, 전자인장 등을 신뢰 당사자에게 제공한다.

그림 2 유럽 디지털 신원지갑의 생태계




사용자(User)는 유럽연합에 거주하는 사람이나 법인이 될 수 있으며, 유럽 디지털 신원지갑을 사용해 개인식별데이터(PID, Person Identification Data), 적격전자속성증명(QEAA, Qualified Electronic Attestation of Attributes), 비적격전자속성증명(EAA, Non-qualified Electronic Attestation of Attributes)과 같은 자신의 신원과 관련된 데이터를 독점적으로 저장, 관리할 수 있다.

유럽 디지털 신원지갑 제공자(EUDI Wallet Provider)는 사용자에게 디지털 신원지갑을 제공하며, 이는 유럽연합 국가이거나 각 국가가 위임/인정하는 조직이 될 수 있다.

개인식별데이터 제공자(PID Provider)는 신뢰할 수 있는 기관이어야 하며, 유럽 디지털 신원지갑 사용자의 신원을 확인하고, 필요한 개인식별데이터를 디지털 신원지갑에 제공한다. 또한, 사용자에 의해 신뢰 당사자에게 제출된 개인식별데이터에 대해 그 유효성을 확인할 수 있는 정보를 제공하게 된다. 이러한 개인식별데이터 제공자는 오늘날 공식 신분증을 발급하는 국가 기관이 될 수 있다.

신뢰 목록 제공자(Trusted List Provider)는 유럽 디지털 신원지갑이 신뢰할 수 있는 동작을 제공하기 위해 참여하는 다양한 엔티티들에 대한 신뢰 목록을 제공한다. 다시 말해, 유럽 디지털 신원지갑 제공자, 개인식별데이터 제공자와 같이 다양한 종류의 제공자들에 대한 신뢰 목록을 유지 관리함으로써 신뢰할 수 없는 임의의 혹은 악의적인 제공자로부터 유럽 디지털 신원지갑의 생태계를 보호한다.

적격전자속성증명 제공자(QEAA Provider)는 인증된 출처로부터 적격데이터를 받고 이를 통해 합법적으로 발급된 종이 형태의 증명과 동일한 법적 효력을 갖는 적격전자속성증명을 디지털 신원지갑에 제공한다. 이러한 적격전자속성증명은 어느 한 국가에서 발급 받았다 할지라도 당연히 다른 유럽연합 국가에서도 동일하게 인정이 된다. 참고로 적격전자속성증명 제공자는 자신이 제공한 적격전자속성증명이 사용자에 의해 어디서 어떻게 사용 되었는지에 대해 어떤 정보도 수집하지 않는다.

비적격전자속성증명 제공자(EAA Provider)는 인증된 출처로부터 데이터를 제공 받는 것이 아니라 공공을 포함해 다양한 민간의 신뢰 서비스 제공자로부터 제공받은 데이터를 사용자의 디지털 신원지갑에 제공한다. 예를 들어, 운전 면허증, 교육 자격증, 디지털 결제와 같은 신뢰 서비스가 될 수 있다. 물론 이러한 비적격전자속성증명의 일부 데이터는 적격전자속성증명 제공자로부터 제공될 수 있다. 비적격전자속성증명 제공자는 자신이 제공한 비적격전자속성증명이 사용자에 의해 어디서 어떻게 사용 되었는지에 대해 어떤 정보도 수집하지 않는다.

전자서명, 전자인장을 위한 적격/비적격 인증서(QES, Qualified and non-qualified certificate for Electronic Signature/seal) 제공자(QES Provider)가 존재하며, 사용자에게 Qualified and non-qualified certificate (QC)을 제공한다. 사용자는 이를 통해 적격전자서명과 적격전자인장을 만들 수

있으며, 이러한 작업은 디지털 신원지갑 내부에 존재하는 적격전자서명/인장 생성 장치를 사용하거나 외부의 적격전자서명/인장 생성 장치를 이용할 수 있다.

인증된 출처(Authentic Source)는 유럽연합에 거주하는 사람이나 법인에 대한 속성 정보를 저장하고 있는 공공 또는 민간의 저장소로 법률에 의해 인정되거나 요구되는 시스템을 의미한다. 예를 들어, 인증된 출처는 적격전자속성증명 제공자에게 다음과 같은 속성 정보의 진위를 확인해 줄 수 있다: 주소, 나이, 성별, 혼인 상태, 가족 구성, 국적, 교육 및 훈련 자격증, 전문 자격증, 공공 허가증 및 라이센스, 재정 및 회사 데이터.

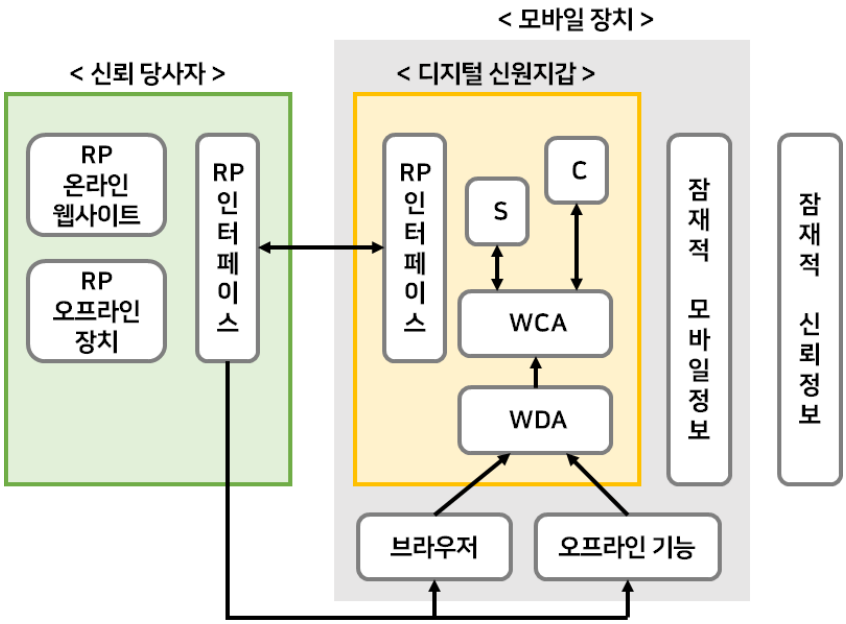
신뢰 당사자(RP, Relying Party)는 사람이나 법인이 될 수 있으며, 사용자에게 어떠한 서비스를 제공하기 위해 개인식별데이터, 적격전자속성증명, 비적격전자속성증명 등을 요구할 수 있다. 사용자는 자신의 디지털 신원지갑을 통해 필요한 개인식별데이터와 전자속성증명을 제공하고, 신뢰 당사자는 제공 받은 데이터를 확인 후, 필요한 서비스를 제공하게 된다.

이 외에도, 장치 제조사(Device Manufacturer), 적격/비적격전자속성 스키마 공급자(QEAA/EAA Schema Provider), 적합성 평가기관(Conformity Assessment Body), 국가인증기관(National Accreditation Body), 감독기관(Supervisory Body) 등이 유럽 디지털 신원지갑 생태계를 이루는 엔티티가 된다.

## 3. 신뢰 당사자와의 온오프라인 동작을 위한 인터페이스와 주요 구성요소

사용자에게 서비스를 제공하는 신뢰 당사자(RP)는 사용자의 디지털 신원지갑과 빈번하게 통신을 수행하는 엔티티가 된다. 유럽 디지털 신원지갑의 ARF v1.0.0은 [그림 3]과 같이 온오프라인 동작을 위해 필요한 인터페이스와 주요한 구성요소를 제시하고 있다.

그림 3 신뢰 당사자와의 온오프라인 동작을 위해 필요한 인터페이스와 주요 구성요소




신뢰 당사자는 웹사이트를 통해 디지털 신원지갑과의 온라인 통신을 수행하게 되며, 오프라인 통신을 위해 오프라인 장치를 따로 가지게 된다. 오프라인 통신은 인터넷 연결 없이 NFC, Bluetooth, QR 코드와 같이 근접에서 사용하는 것을 의미한다. 이를 위해 신뢰 당사자는 RP 인터페이스를 통해 온오프라인 통신을 수행하게 되며, 마찬가지로 디지털 신원지갑 또한 RP 인터페이스를 통해 온오프라인 통신을 수행한다. 참고로, RP 인터페이스는 다른 엔티티들과의 통신을 위해서도 이용된다.

디지털 신원지갑의 논리적인 구성 요소는 RP 인터페이스 이 외에도 신원지갑 구동 어플리케이션(WDA, Wallet Driving Application), PID/EAA 프리젠테이션 생성 어플리케이션(WCA, Wallet PID/EAA Presentation Creation Application), 신원지갑 데이터 저장소(S, Wallet Data Storage), 신원지갑 안전 암호 디바이스(C, Wallet Secure Cryptographic Device) 등이 존재한다. 신원지갑 구동 어플리케이션

(WDA)은 디지털 신원지갑의 사용자 인터페이스를 제공하며, 사용자 선택에 따라 결합될 PID, EAA 정보 및 표시될 속성 정보 등을 PID/EAA 프리젠테이션 생성 어플리케이션(WCA)에 전달한다. PID/EAA 프리젠테이션 생성 어플리케이션(WCA)은 신원지갑 데이터 저장소(S, Wallet Data Storage)에 저장되어 있는 사용자 식별데이터 및 관련 속성과 신원지갑 안전 암호 디바이스(C)에 저장되어 있는 사용자 키 및 인증서를 이용해 RP 인터페이스에 제공할 검증 가능한 프레젠테이션을 생성한다. 참고로 신원지갑 안전 암호 디바이스(C)는 우리가 잘 알고 있는 신뢰 실행 환경(TEE, Trusted Execution Environment) 또는 하드웨어 보안 모듈(HSM, Hardware Security Module)을 의미한다.

이 외에도 브라우저, 오프라인 기능과 함께 스마트폰의 주요한 구성요소로 잠재적 모바일 정보가 있다. 잠재적 모바일 정보는 스마트폰의 설정 및 펌웨어 정보 및 카메라, 지문 센서 등을 포함한다. 마지막으로 잠재적 신뢰 정보는 시스템의 키 정보 및 인증서, 데이터베이스 서버, 기타 신뢰 디바이스를 의미한다.

## V 마치며

간단하게나마 유럽에서 개발되고 있는 디지털 신원지갑에 대해서 살펴보았다. 기술적인 요소들을 살펴보면, 특이한 부분이 없다. 국내의 민간 전자지갑 기술은 빠르게 발전을 했고, 이미 다양한 증명서를 탑재하고 있다. 예를 들어, 네이버에서 제공하는 N전자증명서는 행정안전부와의 협약을 통해 건강보험자격득실확인서, 주민등록등본, 주민등록초본, 예방접종증명서 등을 포함해 30여종의 증명서를 탑재할 수 있다. 하지만, 이는 어디까지나 민간에서 개발한 전자지갑에 탑재된 증명서이고 이러한 증명서가 온오프라인에서 유럽의 디지털 신원지갑과 같은 법적인 효력을 가지는 지는 의문이다. 예를 들어, 은행 창구에 가서 본인확인을 위해 N전자증명서에 있는 증명서를 이용해 계좌신설이 가능할까? 본인의 경험상 안 된다.

유럽 디지털 신원지갑을 이루는 기술적인 요소들은 국내에서 모두 가지고 있거나 단기간 내에 빠르게 기술개발이 가능할 것으로 판단된다. 하지만 필요한 사항은 개정안 eIDAS 2.0에 따른 요건을 맞추는 것이다. 이것은 기술적으로 필요한 수준을 충족시키는 것뿐만 아니라 법적인 규정에 따라 필요한 서비스를 제공해야 하는 것을 의미한다. 국내에서 유럽연합 국가와의 전자상거래나 금융 서비스를 제공해야 하는 기업이나 기관이라고 하면, 이러한 부분에 대해서 미리 준비를 해야 할 것이다.

## 참고문헌

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 2021년 6월.

[2] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet Architecture and Reference Framework. Version 1.0.0, 2023년 1월.

[3] https://www.boannews.com/media/view.asp?idx=88316

[4] 모바일 신분증 – 제1부: 분산 식별자 기반 모바일 운전면허증, TTA, 2023년 10월

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014년 7월

# 02
# Issue·Trend

# EU 및 영국 금융 마이데이터 정책 현황과 API 표준 분석[주)]

## 1. 검토 배경

□ PSD2는 **고객의 동의를 바탕으로 제3자기관에 지급서비스 제공 및 고객 정보 공유 가능한 EU 오픈뱅킹* 정책을 지원**하는 지침으로

* 정보주체가 권리/권한을 가지고 개인데이터를 관리·활용 정책으로, 개인에게 개인데이터 관리·활용 권한을 보장하는 국내 금융 마이데이터 정책과 유사

**표 1** 지급결제산업지침(PSD)와 PSD2

| 구분 | 입법 목적 및 시행 경과 |
|---|---|
| PSD (Payment Services Directive) | - 지급결제산업 및 지급결제사업자를 정의하고 관련 감독규정을 포함한 EU 내 지급결제 지침<br>- 2007년 첫 제정 후 2009년 시행 |
| PSD2 | - 계좌개설기관의 지급결제시스템 및 데이터 개방 관련 규정을 신설<br>- 2016년 개정안 확정 후 2018년 시행 |

○ EU 집행위원회(EC)는 '23.6.28일 PSD2 현대화를 위해 **세 번째 지급결제 산업지침**(PSD3)과 **새로운 지불 서비스 규칙**(PSR) 도입과

○ 지급결제계좌보다 **더 넓은 범위의 데이터를 공유**할 수 있도록 **금융 데이터 접근을 위한 새로운 프레임워크***(FIDA) 입법을 제안

* Financial Data Access, 새롭게 제안된 금융 데이터 접근 프레임워크

주) 황송이, 금융보안원 보안연구부 책임

□ PSD2를 기반으로 **EU 및 영국에서 구현한 API 표준을 분석**하여 **PSR/PSD3와 FIDA 지침과 기술적 요구사항** 이해를 제고하고,

○ 향후 PSR/PSD3와 FIDA 도입에 대비하여 **현재 EU 및 영국에서 구현한 오픈뱅킹 API에서 변경되거나 추가될 기능**을 파악

➔ **EU PSR/PSD3와 FIDA 주요 내용을 분석하여 국내 금융 마이데이터에 적용 가능한 정보를 제공하고자 추진 동향 파악**

## 2. EU 및 영국의 금융 마이데이터

□ 금융 마이데이터는 금융사가 운영·관리하는 **개인 데이터를 정보 주체의 결정에 따라 제3자에 공개**(전송)하는 정책

○ **고객이 데이터 전송 동의 또는 요청**하면 데이터를 보유한 **금융회사에서 해당 고객 데이터를 개방**하는 방식으로 운영

□ **마이데이터 정책을 활성화**하기 위해 3가지 요구사항이 고려

○ **(법적 근거 마련)** 금융회사가 보유한 개인 데이터를 **제3자에게 전송 요구 가능한 정보 이동권 관련 법적 근거**를 마련할 필요

○ **(데이터 개방 의무화)** 개인의 데이터 공개 요청에 따라 금융회사가 **제3자에게 데이터를 개방하는 것이 의무화**될 필요

○ **(전송 및 접근 방법)** 상호 운용이 가능하도록 **통상적으로 사용하고 기계 판독이 가능한 형식**으로 구현할 필요

**표 2** EU 및 영국의 마이데이터 활성화를 위한 요구사항과 적용 방안

| 요구사항 | | 적용 방안 |
|---|---|---|
| 개인의 정보 이동권에 대한 **법적 근거** | | GDPR 시행 |
| 개인 요청에 따른 기업의 **데이터 개방 의무화** | ➔ | PSD2/Open Banking 3.0 시행 |
| 원활하고 안전한 데이터 **전송 및 접근 방법** | | API 방식* |

* [별첨1] 마이데이터 원칙 및 기능 요구사항

## (가) 법적 근거

□ EU GDPR* **시행**('18.5월)으로 정보주체의 **정보관리 권한을 확대·강화****하고 **정보주체 중심 데이터 활용**의 법적 기반을 마련

* General Data Protection Regulation: GDPR, 개인정보보호 일반 규정

** 4가지 정보주체 권리를 신설하여 정보관리 권한을 확대 및 강화

○ 특히, **개인정보 이동권**은 정보주체의 권리 강화뿐만 아니라, **기업간 공정한 경쟁 유도 및 데이터 활용 활성화***를 고려하여,

* 산재한 개인정보를 통합 관리하여 개인에게 유리한 서비스를 판별 가능

○ 정보주체는 컨트롤러에게 **기계 판독 가능한 형식**으로 데이터를 수령하고 **다른 컨트롤러에게 전송 또는 전송되도록 요구** 가능

○ EU는 **GDPR 시행으로 본인 데이터를 능동적으로 활용하고 처리하는 권리를 보장**하여 마이데이터 체제로의 제도적 지원

**표 3** GDPR에 정의된 정보주체의 권리

| 권리 | 내용 |
|---|---|
| **삭제권**(잊힐권리) | - 정보주체는 본인에 관한 개인정보의 삭제를 컨트롤러에게 요구할 권리를 가지며 컨트롤러는 개인정보 처리목적의 달성, 정보주체의 동의 철회 등의 경우에 개인정보를 삭제하여야 함 |
| **처리 제한권** | - 정보주체는 자신에 관한 개인정보의 처리를 차단하거나 제한할 권리를 가지며, 개인정보 처리가 제한되면 컨트롤러는 그 정보를 보관하는 것만 가능 |
| **개인정보 이동권** | - 정보주체나 다른 컨트롤러에게 **자신의 데이터를 제공할 것을 요구**할 수 있는 권리 |
| **프로파일링을 포함한 자동화된 의사결정** | - 법적 효력을 초래하거나 이와 유사한 중대한 효과를 미치는 사항에 대하여 프로파일링*을 포함한 자동화된 처리에만 근거한 인적개입 없는 결정의 적용을 받지 않을 권리<br>* 개인의 사적인 측면을 분석 및 예측하기 위한 자동화된 처리 |

## (나) 데이터 개방 의무화

□ EU는 GDPR 시행으로 산업 전반의 정보주체 권리를 보장하고, **PSD2*로 금융산업에 한정하여 개인의 자기정보결정권**을 구체화

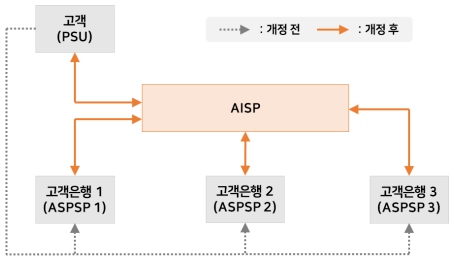
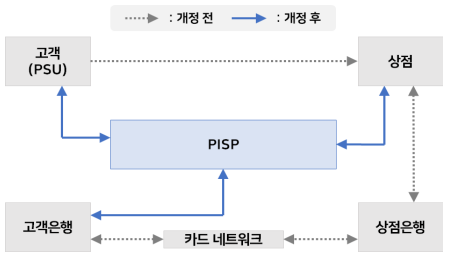
* Revised Directive on Payment Services: PSD2, 개정 지급결제 서비스지침

○ PSD2('18.1월 시행)는 EU 내 **은행이 고객 데이터를 API 방식*으로 제3자와 공유하고 API를 개방**(오픈 API 형태)하도록 요구**

* 단, 기술 중립성을 위해 API방식과 스크린 스크레이핑 접근 방식을 모두 허용

** PSD2 시행으로 금융사와 핀테크 기업간 **데이터 교환이 가능한 법적 기반** 마련

**표 4** PSD2에서의 제3자(TPP, Third-party Provider)

| 구분 | 계좌정보사업자(AISP)<br>(Account Information Service Provider) | 지급결제사업자(PISP)<br>(Payment Initiation Service Provider) |
|---|---|---|
| 역할 | - 사용자 동의 하에 지급결제계좌정보에 접근하여 집계(통합), 조회, 분석하는 서비스 제공 | - 사용자(지급인) 동의 하에 지급거래 개시, 거래에 필요한 정보 송·수신, 수취인 앞으로 지급지시 서비스 제공 |
| 특징 | - **(고객)** 자신의 재무상태에 대한 통합정보 확인할 수 있으며, 여러 은행 계좌 정보를 통합관리 가능<br>- **(제공자)** 리스크 관리, 상품 추천 등의 비즈니스로 확장 가능 | - **(고객)** 온라인 결제 시 필요 정보를 직접 입력하지 않고, 특정 PISP를 통해 안전하고 편리하게 결제 진행<br>- **(제공자)** 다양한 결제 옵션을 제공하여 결제 거래에 대한 수수료 부과 |
| 업무 프로세스 |  |  |

○ EBA(유럽은행감독청)는 **기업간 원활한 금융데이터 교환**을 위해 **규제기술 표준***('18.3월 공표, '19.9월 시행)과 **가이드라인**을 제정

* Regulatory Technical Standard, PSD2 하위규정으로 고객인증, 데이터 전송방식 등 원활한 정보이동권 행사 및 정보보안 강화를 위한 데이터 세부기준을 규정

○ 다만, **EU 내 단일화된 API 규격**(API 표준)**이 부재**하여 베를린 그룹, STET 및 PolishAPI* 등 다양한 기관에서 API를 개발

* **(베를린 그룹)** 오픈뱅킹 및 표준화 촉진을 위해 EU 주요 은행이 모여 결성, **(STET)** 금융 인프라 기업으로 프랑스 주요 은행들이 모여 이루어진 비영리조직, **(PolishAPI)** 폴란드 금융기관들의 오픈뱅킹 표준을 위한 비영리조직

□ 영국은 소매은행시장의 경쟁 제고를 위해 **은행이 보유한 고객계좌정보를 타 금융사에 안전하게 공유**할 것을 명령*('17.2월)

* 영국 경쟁시장국(CMA), Retail banking market investigation order 2017

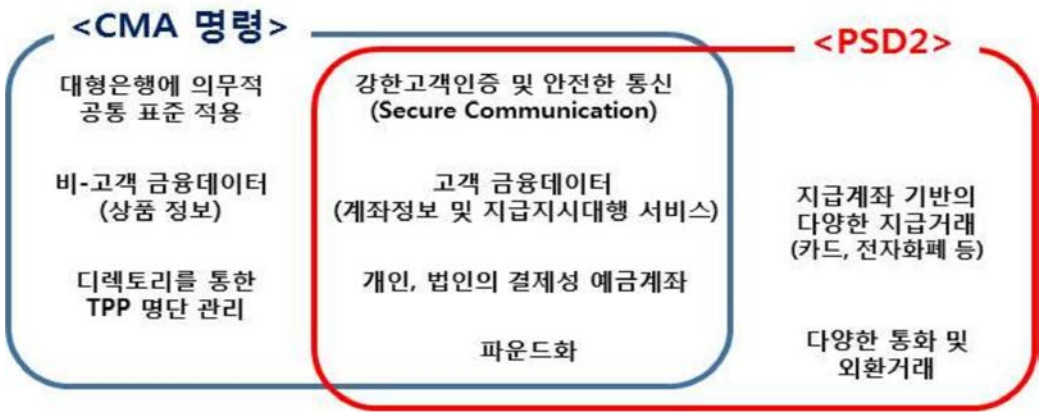
○ CMA 명령은 **고객·非고객 금융정보 공유**, 정보 공유 **API 표준 설계, 실행기구 설립** 등 구체적 오픈뱅킹 정책 체계를 마련

○ CMA 명령은 PSD2상 지급거래 서비스를 포함하지 않았으나, **오픈뱅킹 정책 추진 과정에서 지급결제서비스**를 포괄

○ 또한, **오픈뱅킹 이행기구*는 API 표준을 공개**(`18.9월)하였으며, 주요 9개 은행(CMA9)에 **의무적으로 API를 채택**할 것을 명령

* 영국 경쟁시장청(CMA)은 EU PSD2에 대응하여 오픈뱅킹 제도 운영을 지원하기 위해 오픈뱅킹 이행기구(Open Banking Implementation Entity, OBIE 또는 OBL)를 설립

**그림 1** CMA 명령과 PSD2간 포괄범위




※ [참고] 한국은행, 영국의 지급결제제도 개편 동향 및 특징('19.12월)

**표 5** 영국과 EU의 마이데이터 정책 비교

| 구분 | 영국 오픈뱅킹 | EU PSD2 |
|---|---|---|
| 제도 | PSD2, Open Banking Standard 3.0 | PSD2 |
| 적용대상 | CMA9 의무 적용('18년 기준)<br>※ '23.7월, 93개 계좌기관에서 적용 | EU 내 전 지급결제 계좌 |
| 데이터 전송/접근 | CAPIF* 방식<br>* Common API Framework | 금융회사 전용 API |
| 정보제공 범위 | 개인 계좌금융정보 및 금융상품 정보 | 개인 계좌금융정보 |

※ [참고] 보험연구원, 주요국 마이데이터 정책과 서비스 사례('21.8월)

**※ 국내 오픈뱅킹과 영국 오픈뱅킹 차이 – 정보 제공 요청 주체**

- **(국내 오픈뱅킹)** 은행이 제3자와 고객 데이터를 공유할 수 있도록 고객이 승인하면 은행은 고객 데이터에 대한 접근 권한을 보유
- **(영국 오픈뱅킹; 마이데이터 금융 영역)** 개인이 본인 금융 데이터 권리를 소유하고 제어하여, 은행에서 운영 및 관리 중인 본인 데이터를 제3자에게 공유하도록 요구

## 3. 마이데이터 API 표준

### (가) 영국 오픈뱅킹

□ **오픈뱅킹 이행기구***(OBIE)는 **금융 기관이 데이터 및 서비스를 제3자 공급자에게 안전하게 제공**할 수 있는 **표준 API***를 제공

* 규격화된 형식으로 데이터를 전송받는 데이터 교환 기술 표준

○ **(API 규격) OBIE는 의무 준수 여부를 구분**하여 표준 API를 제시하고, 이에 따라 **ASPSP*는 API를 개발하여 TPP에 공개**

* Account Servicing Payment Service Provider, 계좌 제공 지급서비스 제공자

○ CMA 명령 등 규제를 반영하여 **특정 지급거래 기능의 표준 준수 여부**를 의무(Mandatory), 조건(Conditional), 선택(Optional)으로 구분

**표 6** 영국 오픈뱅킹 API 표준

| 표준 | | 내용 요약 |
|---|---|---|
| API 기능 | ❶ 읽기/쓰기 API | - 오픈뱅킹 서비스 제공 업체들이 **소비자의 금융 계좌 데이터에 읽기/쓰기 접근을 제공**하기 위한 표준화된 방법을 정의<br>- 소비자가 다양한 금융 계좌에 대한 데이터를 안전하게 공유하고, 제3자 금융 서비스 제공 업체(TPP)가 소비자의 계좌에 대한 트랜잭션을 수행할 수 있도록 지원 |
| | ❷ 오픈 데이터 API | - 상품정보 등 **非 은행 계좌 정보에 해당하는 금융 데이터를 공유**하기 위한 표준화된 방법(통신절차)과 사용예제를 규정<br>- 다양한 금융 데이터에 대한 개방된 접근을 가능하게 하여 TPP가 혁신 서비스를 개발할 수 있도록 지원 |
| | ❸ 디렉터리 | - TPP가 API에 접근하는 것을 식별하고 TPP가 적절한 규제적 권한을 가지고 있는지 확인할 수 있도록 TPP 등록, TPP의 규제적 권한 확인, ASPSP 목록 확인, 정보 업데이트 지원 |
| | ❹ 동적 클라이언트 등록 | - TPP가 ASPSP에게 소프트웨어 문서 어설션*을 제출하여 ASPSP에 등록(OAuth 클라이언트를 생성)하기 위한 방법을 정의<br>* 소프트웨어 세부 정보와 보안 관련 사항을 포함한 문서 |
| | ❺ 경영 정보(MI) 보고 | - ASPSP와 TPP에 대한 MI 요구사항, 물리적 데이터 사전*, MI 데이터 JSON 스키마, 예시 보고 템플릿을 정의<br>* 관련 코드 목록, 제약 조건 및 카디널리티, 패턴 제약 조건, 등의 기술적 세부 정보와 메시지 사양의 필드별 설명을 제공 |

### ❶ 읽기/쓰기 API 기능 (v3.1.11)

○ TPP는 **사용자 동의 하에 은행 계좌에 접근**하여 읽기(계좌 잔액 및 거래 정보 가져오기) 및 쓰기(요청된 결제 수행) 기능을 수행

**표 7** 영국 오픈뱅킹 API 표준 – 읽기/쓰기 API (v3.1.11) 기능 상세

| 표준 | | 내용 요약 |
|---|---|---|
| 읽기 / 쓰기 API | 계좌 및 거래 API (계좌 정보) | - 계좌 정보와 거래 데이터를 가져오기 위해 사용<br>- AISP(Account Information Service Provider)는 사용자 동의를 받아 계좌 정보와 거래 내역에 접근 가능 |
| | 결제 개시 API (지급지시 대행) | - PISP(Payment Initiation Service Provider)는 사용자 동의를 받아 계좌에서 결제 거래를 개시 |
| | 자금 확인 API | - CBPII(Card Base Payment Instrument Issuer)이 ASPSP를 통해 계좌 잔액을 확인하여 지급지시에 상응하는 가용 자금 여부를 확인 |

| 표준 | | 내용 요약 |
|---|---|---|
| | 가변적 반복 결제 API | – 특정 기간 동안 주기적으로 변경되는 금액으로 반복 결제를 예약할 수 있는 기능을 제공<br>– 사용자는 해당 API를 사용하여 가변적 반복 결제를 설정하고, 자동으로 결제가 이루어지도록 처리 가능 |
| | 이벤트 알림 API | – 특정 이벤트*에 대한 알림을 제공<br>* 계좌 변경, 결제 완료 등 |
| | 리소스 및 데이터 모델 | – API 엔드포인트에서 사용하는 데이터 구조와 필드를 정의하여 일관된 데이터 교환을 지원 |

### ❷ 오픈 데이터 API 기능 (v2.4.0)

○ **읽기 전용 API**로 제한된 범위의 **非계좌 정보를 수집** 가능

**표 8** 영국 오픈뱅킹 API 표준 – 오픈 데이터 API (v2.4.0) 기능 상세

| 표준 | | 수집 가능 데이터 |
|---|---|---|
| 오픈데이터 API | 지점 위치 찾기 | – 주소, 연락처, 영업 시간, 제공 서비스 등을 포함 |
| | ATM 위치 찾기 | – ATM 위치, 이용 가능 여부, 수수료 등을 포함 |
| | 법인용 결제성예금계좌 | – 계좌 정보, 잔액, 거래 내역, 제공 서비스 등을 포함 |
| | 개인용 결제성예금계좌 | – 계좌 정보, 잔액, 거래 내역, 제공 서비스 등을 포함 |
| | 중소기업 대출 | – 소규모, 중소기업(SME) 대상 대출 관련 대출 조건, 이자율, 상환 옵션, 자격 기준 등을 포함 |
| | 중소기업 법인신용카드 | – 중소기업 법인카드 관련 신용 한도, 거래 내역, 제공 혜택, 계좌 관리 기능 정보 등을 포함 |

**표 9** 읽기/쓰기 API와 오픈 데이터 API 차이

| 읽기/쓰기 API | 비교 | 오픈 데이터 API(읽기 전용 API) |
|---|---|---|
| 은행 계좌 정보에 실시간 접근하고 결제 지시를 수행 | 기능 | 대출 비교, 예적금 비교, 금전 절약 팁과 같은 서비스를 제공 |
| 읽기, 쓰기 권한으로 은행 계좌에 접근하여 결제를 수행 | 데이터 접근 | 제한된 범위의 은행 계좌 정보에만 읽기 접근 가능 |
| OBIE에서 제공하는 규격 사용 | 규격 | 은행이 개별적으로 제공 |
| 사용자 동의 하에 TPP는 필요한 인증 및 권한 검증을 수행하고 사용자 은행 계좌에 접근 | 접근 권한 | 읽기 전용 접근만 제공하므로, 결제 또는 계좌 조작 등의 기능은 제공하지 않음 |

### ❸ 디렉터리 (v1.6)

○ **오픈뱅킹 디렉터리가 작동하는 방식**에 대한 상세한 기술적 정보와 **디렉터리 각 참가자의 역할과 기능**을 명세

**표 10** 디렉터리 제공 기능

| 기능 | 설명 |
|---|---|
| 인증 및 접근제어 관리 | - 오픈뱅킹 디렉터리와 상호작용하는 조직 및 개인의 신원 정보를 **eIDAS 인증서를 사용하여** 발급하고 관리 |
| 인증서 및 키 관리 | - **eIDAS* 인증서**(QWAC 또는 QSeal), **서명 키 및 암호화 키**를 업로드, 관리 및 제거하고, OB 디지털 인증서를 발급, 관리 및 폐지<br>* Electronic Identification, Authentication and Trust Services, EU 회원국 내 개인·조직·정부 기관 간 전자 거래에서 신뢰를 구축하기 위한 표준 |
| 디렉터리 정보 관리 | - TPP는 ASPSP와 상호작용하기 위해 디렉터리에 등록<br>- 디렉터리에 등록한 정보를 업데이트하고 검색<br>- API 또는 자체 서비스인 웹 응용프로그램으로 제공 |

○ TPP는 디렉터리에 등록된 **조직 정보를 관리**하고, ASPSP의 기술 정보(제공 API), 등록 상태 등 **필요 정보를 검색** 가능

○ ASPSP는 디렉터리 제공 기능으로 **조직 및 소프트웨어 상태, QTSP*의 유효성, 회원 국가별 NCA** 등록 상태**를 확인 가능

* Qualified Trust Service Provider, eIDAS 적격 신뢰 서비스 제공자

** 각 국가에서 금융 서비스와 관련된 규제와 감독을 담당하는 국가적인 권한 기관으로 영국은 FCA(Financial Conduct Authority, 금융행위청)가 해당 역할을 수행

### ❹ 동적 클라이언트 등록 기능 (v3.3)

○ **TPP가 ASPSP**에 소프트웨어 문서 어설션(SSA)을 제출하여, **실시간으로 자신을 등록할 수 있는 기능**을 정의한 API 규격

○ TPP가 OAuth 클라이언트를 수정해야 하는 일련의 상황*을 식별하고, **ASPSP는 관련 API 및 서비스 관리 기능**을 구현

* TTP는 SSA를 제출하여 등록 요청(POST 요청)➔SSA를 서명된 JSON 웹 토큰으로 전송➔ASPSP는 OIDC(OpenID Connect) 등록 사양 기반 SSA 유효성 검사➔ASPSP는 SSA 기반 클라이언트 등록➔ASPSP는 응답(성공 또는 실패)을 반환

**표 11** ASPSP 기능 요구사항

**6.3.4 동적 클라이언트 등록**

- OBIE는 ASPSP가 **TPP의 원활한 등록**과 가능한 **완전 자동화된 방식**으로 등록을 처리하며, TPP에게 **응답을 실시간 제공**하도록 보장해야 한다고 제안
- OBIE는 참가자 식별 **API를 통해 이미 이를 지원**하기 위한 기능을 제공

**6.4.2 ASPSP에서 재등록**

- 6.3.1(TPP와 ASPSP 간 현업 과정 개선) 또는 6.3.2(ASPSP의 권한 서버 기능 업그레이드로 인한 재등록)의 영향으로 ASPSP가 권한 서버 기능을 업그레이드하는 경우 TPP가 ASPSP와 다시 협업하기 위해 재등록할 필요
- OBIE는 TPP가 비즈니스 연속성을 유지할 수 있도록, 재등록과 동시에 새로운 시스템으로 전환이 가능하도록 지원하는 **병렬로 실행하는 솔루션을 ASPSP에서 구현할 수 있는지 타당성을 검토***할 것을 제안

  * 기존 TTP와의 상호 운용성, 데이터 이전, 테스트 및 검증 절차, 비용과 시간 외에도 해당 솔루션을 개발하기 위한 내부 기술 및 프로세스를 고려하여 실행할 필요

※ [참고] eIDAS 개선을 위한 생태계 준비

### ❺ MI(Management Information; 경영 정보) 보고 기능 (v3.1.11)

○ ASPSP 및 TPP의 **CMA 명령 준수 여부를 모니터링**하기 위해 ASPSP와 TPP는 **OBL(Open Banking Limited)에 MI를 제출할 의무***

* The Retail Banking Market Investigation Order 2017, Schedule 1 – Implementation Trustee Functions, Article (2) (j)

○ ASPSP와 TTP는 고객 정보, 직원 정보, 매출 정보 등 비즈니스 관련 데이터를 **MI 템플릿 주요 사용 지침에 따라 작성**할 필요

□ 영국은 API 표준 외 오픈뱅킹 참여자가 준수해야 하는 **가이드라인**과 보안 요구사항을 충족하기 위한 **보안 프로필**을 제공

○ **(가이드라인)** 법적 의무사항은 아니지만, 이를 준수한 경우 PSD2, RTS 등 **주요 규제 요건을 충족할 수 있도록 지원**

- **(고객 경험 가이드라인)** 오픈뱅킹 서비스 절차, 고객 인증 절차 등 **사용자 경험을 개선하기 위한 지침과 체크리스트를** 제공

- **(운영 가이드라인)** RTS-SCA* 구축을 위해 **ASPSP가 규제 요구사항을 준수하는 데 도움이 되는 지침과 체크리스트**를 제공

  * RTS on Strong Authentication & Secure Communication under PSD2

○ **(보안 프로필)** 금융 API 보안 수준*에 따라 **OAuth와 OIDC 기반** 인증 및 권한 부여를 위한 표준화된 보안 프로필**을 제공

  * **읽기 API**에는 **낮은 보안 수준**이, **읽기/쓰기 API**에는 **높은 보안 수준**이 적용

  ** **(OAuth)** 클라이언트 애플리케이션이 제한된 접근 권한을 가지고 인증 없이 리소스에 접근할 수 있도록 하는 인증 및 권한 부여 프레임워크**(OIDC)** OAuth 2.0 프로토콜 위에 구축된 신원 확인 프레임워크로 JSON 웹 토큰(JWT)을 사용하여 사용자 정보를 암호화하고 전달

**표 12** 영국 오픈뱅킹 가이드라인 및 보안 프로필

| 표준 | | 내용 요약 |
|---|---|---|
| 가이드라인 | 고객 경험 | - AISPs, BISPs, CBPIIs가 서비스 제공 시 고객 경험 개선을 위해 동의 및 고객인증 방법, 명확한 정보 전달, 간결한 서비스 구성 등의 지침 제공 |
| | 운영 | - 가용성 및 성능(성과지표), 전용 인터페이스 요구 사항, 문제 해결, 서비스 설계 및 테스트 지침과 운영 지침 체크리스트를 제공 |
| 보안 프로필 (보안 표준) | | - ASPSP와 TPP간 **API를 통한 지급거래 처리 시 보안성 향상**을 목적<br>- **(금융 등급 API, FAPI)** 데이터 읽기 API, 데이터 읽기/쓰기 API 관련 보안 인증 요청 변조, 코드 주입을 포함한 인증 응답 변조, 상태 주입, 토큰 요청 피싱과 같은 공격에 대한 제어를 지정<br>- **(CIBA*)** CIBA 흐름을 FAPI의 특정 부분과 통합하여 금융 수준의 보안을 필요로 하는 API에 적합한 보안 규칙과 권장 사항을 제공<br>* Client Initiated Backchannel Authentication, OIDC(OpenID Connect) 인증 흐름의 한 유형으로 응용 프로그램이 백그라운드에서 사용자 인증을 처리할 수 있는 방법을 제공 |

### (나) 베를린 그룹

□ **베를린 그룹*은 PSD2를 준수하기 위한 표준 API 개발 그룹**으로, 독일 은행을 포함하여 유럽의 다른 주요 은행들이 참여 중

* 10개의 서로 다른 유로존 국가(영국, 스웨덴, 덴마크, 노르웨이, 아이슬란드, 터키, 불가리아, 헝가리, 러시아, 세르비아, 스위스)의 26개 이상의 결제 산업 참여자로 구성된 협력체

○ EU 내 결제 체계와의 호환성을 위해 **PSD2 XS2A**(Access to Account)**에 대한 표준화된 API인 NextGenPSD2**을 구현

○ NexGenPSD2는 **상호 운용성, 구현 복잡성 완화**를 목표로 개방하였으며, **현재 유럽 오픈 뱅킹 API 80%**가 해당 표준을 사용

○ 또한, 오픈 뱅킹 생태계의 성장과 혁신을 촉진하기 위해 **API 구현 및 이용을 지원하는 운영 규칙과 구현 지침** 등을 공개

**표 13** NextGenPSD2 표준

| 표준 | 설명 |
|---|---|
| 소개 문서 (v2.0, '19.3.25)<br>(Introduction document) | - NextGenPSD2 소개와 API 필요성을 설명하는 문서 |
| 운영 규칙 (v1.3, '18.12.21)<br>(Operational Rules) | - NextGenPSD2 API를 구현하고 사용하는 데 필요한 운영 규칙을 정의한 문서<br>- **접근 권한과 보안, 요청 및 응답 포맷, 요청 제한사항, 오류 처리, 기타 운영 관련 사항** 등 오픈 뱅킹 API를 사용하는 모든 주체들이 지켜야 하는 내용을 포함 |
| 구현 지침 (v1.3.12, '22.7.1)<br>(Implementation Guidelines) | - NextGenPSD2 API를 구현하고 사용하는 데 필요한 구현 지침과 가이드라인을 제공하는 문서<br>- **API 엔드포인트, 인증 방법, 데이터 형식과 규격, 예제 요청과 응답, 오류 처리, 보안 및 개인정보 보호, 버전 관리 및 기타 구현 관련 사항**을 포함 |
| OpenAPI 파일 (v1.3.12, '22.7.29)<br>(OpenAPI file) | - **오픈 뱅킹 API의 스펙 및 규격**을 정의한 문서<br>- API를 사용하는 은행과 TPP간 상호운용성과 데이터 교환을 원활하게 하기 위한 필요한 정보를 포함 |
| 확장된 부가 가치 서비스<br>(Extended Value-added Service) | - 은행이나 금융 기관에서 부가 가치를 추가하기 위한 선택적 서비스에 대한 구현 지침과 OpenAPI 문서 |
| 정오표 문서<br>(Errata file) | - 불명확한 정보나 오류를 명확히 하기 위한 문서 |
| 기타 | - 국내 지급결제 정의서(Domestic Payment Definitions), 보안 사항(Security Bulletin), 변경 로그(Change Log) |

□ 베를린 그룹은 **EU 국가별 지급결제 체계 및 인프라 다양성***을 존중하여 EU 내 **공통 지급결제 체계의 기본적인 규격**만 정의

* EU는 국가별 자체적인 금융 서비스 규정과 법률을 운영하고 있어 지급결제 서비스에 적용되는 규칙과 규정에 차이가 존재할 수 있음

○ EU 국가별 지급결제 방식 차이로 인해 **해당 표준을 기반으로 API를 제작하였어도 전송 방식 및 규격에 일부 차이**가 존재

**표 14** NextGenPSD2 API 표준 주요 내용

| 대상 | 내용 |
|---|---|
| 문자 집합 및 표기법 | - 사용 가능한 문자 집합과 API 요청 및 응답 호출 표기법에 대한 데이터 포맷 및 규격을 정의 |
| 전송 계층 | - TLS 연결, EBA-RTS 요구사항을 준수한 인증, eIDAS 규정에 따른 인증서 발급 등 ASPSP와 TPP간 통신 요구사항을 정의 |
| 응용 계층 | - API 엔드포인트 접근 방법, API에서 사용되는 HTTP 응답 코드 등 응용 계층에서 API 처리 방법과 데이터 규격을 정의 |
| 지급결제 서비스 | - 단일 결제, 예약 결제, 다중/대량 결제, 정기 결제 등 지급결제 서비스에 대한 다양한 요청*과 처리 방법을 정의<br>* 지급결제 요청, 거래상태 조회 요청, 지급결제 조회 요청, 지급결제 취소 요청, 취소 승인 하위 리소스 조회 요청 등 |
| 계좌 정보 서비스 | - 계좌 잔액 조회, 거래내역 조회 등 계좌 정보 서비스에 대한 다양한 요청*과 처리 방법을 정의<br>* 계좌 정보 동의 요청, 동의 상태 조회 요청, 동의 조회 요청, 계좌 정보 조회 요청, 카드 계좌 정보 조회 요청 등 |
| 자금 확인 서비스 | - 결제 전 출금 가능 여부를 확인하는 서비스에 대한 요청과 처리 방법을 정의 |
| 구조 및 필드 | - 핵심 서비스인 단일 결제, 예약 결제, 다중/대량 결제에 대한 JSON 구조와 데이터 규격(필드)을 정의 |

**표 15** NextGenPSD2 API - 기본 서비스

| 서비스 | 요청 |
|---|---|
| 지급결제(PIS) | - 단일 결제, 예약 결제, 다중/대량 결제, 정기 결제, 결제 취소 |
| 계좌 정보(AIS) | - 계좌 정보 접근 동의 설정<br>- 접근 가능 계좌 목록 조회, 접근 가능 계좌 상세 정보 조회<br>- 특정 계좌 잔액 조회, 특정 계좌 거래 정보 조회<br>- 접근 가능 카드 계좌 목록 조회<br>- 특정 카드 계좌 잔액 조회, 특정 카드 계좌 거래 정보 조회 |
| 자금 확인(FCS) | - 자금 가용성 확인 |
| 지급결제/계좌 정보 | - 거래 일괄 승인(Signing baskets) |

## (다) STET

□ **STET는 베를린 그룹과 협력***하면서 **프랑스 지급결제 체계에 특화된 API**(STET PSD2 API v1.6.3.1, `22.10.3.)를 제공

* EU에 공통적으로 적용 가능한 항목은 공동으로 탐구하여 NextGenPSD2에 반영하고, 이를 재활용하여 EU내 각 국별 지급결제 체계에 적합한 자체 규격을 개발

○ **프랑스 은행은 STET PSD2 API를 통해 TPP**(AISP, CBPII, PISP)**가 금융 서비스를 제공하는데 필요한 기능을 지원**

**표 16** 계좌정보사업자(AISP) 필요 기능

| 제공 가능 기능 | 설명 | 상호작용 |
|---|---|---|
| 고객 정보 조회 | - 고객 계좌 정보를 얻기 위해 ASPSP에 요청 | ASPSP |
| 고객 동의 전송 | - 고객의 동의 사항을 ASPSP에 전송 | ASPSP |
| 계좌 데이터 조회 | - '계좌주', '당좌대월', '잔액' 등을 모두 조회 | - |
| 계좌 소유자 조회 | - 특정 계좌의 계좌주를 조회 | ASPSP |
| 당좌대월(overdraft) 조회 | - 특정 계좌의 당좌대월을 조회 | ASPSP |
| 계좌 잔액 조회 | - 특정 계좌의 잔액을 조회 | ASPSP |
| 거래 리스트 조회 | - '거래내역'과 '예상 거래' 등을 모두 조회 | ASPSP |
| 거래내역 조회 | - 특정 날짜 범위 내 모든 거래내역을 조회 | ASPSP |
| 예상 거래 조회 | - 특정 계좌의 입출금 예정인 거래을 조회 | ASPSP |
| 고객 신원 조회 | - 고객의 신원 정보를 조회 | ASPSP |
| 신뢰 송금자 조회 | - 자주 거래하는 송금자 정보를 조회 | ASPSP |

**표 17** 카드기반 결제수단발행자(CBPII) 필요 기능

| 제공 가능 기능 | 설명 | 상호작용 |
|---|---|---|
| 자금 가용성 확인 | - 결제 전 출금 가능 여부를 확인 | ASPSP |

**표 18** 지급결제사업자(PISP) 필요 기능

| 제공 가능 기능 | 설명 | 상호작용 |
|---|---|---|
| 지급결제 요청 전송 | - 실행할 지급결제 정보를 ASPSP에 전송 | ASPSP |
| 취소 요청 전송 | - 실행되지 않은 지급결제 요청을 취소 | ASPSP |
| 요청 승인 | - 지급결제 요청 또는 취소를 승인 | ASPSP |
| 요청 상태 조회 | - 지급결제 요청 또는 취소 상태를 조회 | ASPSP |

○ 또한, PSD2 규정을 준수하고 보안 요구사항을 충족하기 위해 **인증, 인가, 권한 관리, 사기 탐지 등의 기능**을 함께 제공

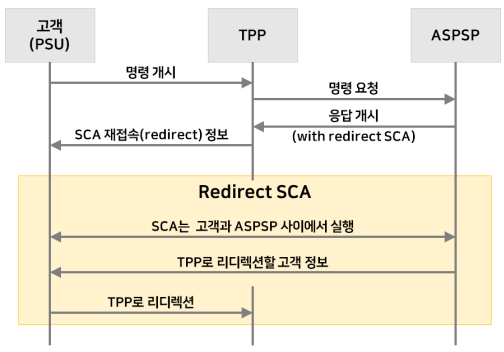
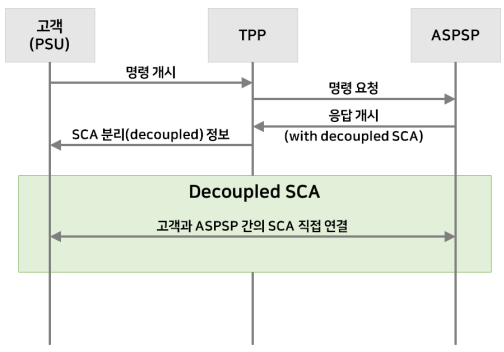
○ STET는 API 개발을 돕기 위해 **TPP 필요 기능, API 데이터 구조 및 사용 예시 등을 담은 STET PSD2 API 표준***을 발표

* Part 1: Framework, Part 2: Functional Model, Part 3: Interaction Examples

**표 19** STET PSD2 API 표준 – 구성 방식

| 항목 | 방식 |
|---|---|
| 접근 네트워크 | 인터넷 |
| 네트워크 프로토콜 | HTTP 1.1 (Minimum) |
| 데이터 암호화/교차 인증 | TLS 1.2<br>※ 양측 eIDAS 인증서(QWAC) 확인 |
| 인증 프로토콜 | OAuth2 |
| 응용 프로토콜 | REST |
| 응용 인증 | http-signature |
| 고객 SCA 접근법 | REDIRECT, DECOUPLED<br>※ TPP 기능에 따라 인증 방식에 차이 존재 |
| 데이터 형식 | JSON/UTF8 |
| 기술 설명서 | SWAGGER 2.0 |

**표 20** TPP의 고객 인증 처리 방법 – 2가지 접근 방식

| REDIRECT(재접속) 방식 | DECOUPLED(분리) 방식 |
|---|---|
|  |  |

## 4. PSR/PSD3와 FIDA 주요 내용

□ EU는 **PSD2 검토조항(제108조)에 따라 EU 내 PSD2 적용 현황과 영향을 파악**하고 필요시 지침 개정을 위한 이니셔티브를 구성

○ **규제검토위원회**(RSB)*의 PSD2 평가 결과, 오픈뱅킹의 긍정적 성과 외에도 **EU 지급결제 시장에 현존하는 문제**를 식별**

* Regulatory Scrutiny Board, EU 집행위원회 산하 기관

** [별첨2] RSB의 PSD2 검토 결과

**표 21** EU 지급결제 시장의 식별된 주요 문제

| 문제 | 결과 |
|---|---|
| 사칭 등 사회공학 사기 위험 증가 | - 사기 위험에 노출된 사용자 |
| 오픈뱅킹 프레임워크의 불완전한 작동<br>(인터페이슨 품질과 성능 차이) | - 오픈뱅킹 서비스 제공 어려움<br>- 신규 플레이어의 경쟁력 저하 |
| EU 금융 감독기관의 일관되지 않은 권한·의무 | - 의무에 대한 불확실성<br>- '포럼 쇼핑*' 발생<br>* 유리한 재판관할권을 찾아 재판 |
| 은행과 비은행 PSP간 불공정한 경쟁의 장<br>(비은행 PSP의 계좌 개설 어려움) | - 비은행 PSP의 경쟁력 저하 |
| 국내 한정된 대다수의 지급결제시스템 | - 국외 지급결제 서비스 수용 한계 |

○ 검토 결과를 바탕으로 EU 집행위원회(EC)는 **Payment Service Regulation (PSR)/PSD3와 오픈 파이낸스 프레임워크**(FIDA)를 제안

**표 22** PSR/PSD3(PSD2 개정안) 및 FIDA 주요 내용

| 개정 이니셔티브 | 개정 및 제정안 주요 내용 |
|---|---|
| [ PSD3 지침 제안 ]<br>COM*(2023) 366 final<br>* commission | - 지급결제기관(PI, Payment Institution) 허가/감독 규정 명확화<br>- 전자화폐기관(EMI, Electronic Money Institution)을 PI의 하위 범주로 통합하고, 전자화폐지침(EMD2)* 폐지<br>* the second Electronic Money Directive, 2009/110/EC<br>- 결제완결성지침(SFD, Settlement Finality Directive) 개정*<br>* 지급결제시스템 직접 참여 가능한 기관 목록에 PI 추가<br>- 독립형 ATM 운영자에 대한 현금 인출 서비스 규정 |
| Implementing<br>Regulation, 규정 이행령 | |

| 개정 이니셔티브 | 개정 및 제정안 주요 내용 |
|---|---|
| [ PSR 규칙 제안 ]<br>COM(2023) 367 final | - PI의 은행 계좌 접근 강화(접근 거부 및 철회 사유 상세 제공)<br>- 지급결제 서비스를 위한 조건 및 정보 요구사항 투명성<br>- 지급결제 서비스 제공 및 사용 관련 권리와 의무<br>- 오픈뱅킹 기능, 데이터 보호 등의 공통 개선 사항 |
| [ FIDA 규칙 제안 ]<br>COM(2023) 360 final | - 금융 데이터 접근 및 사용에 대한 관리 프레임워크로, 금융정보서비스 제공자(FISP) 법적 권리/의무, 요구사항 등을 정의 |

□ PSR/PSD3는 ❶**소비자 보호 및 신뢰 강화,** ❷**오픈뱅킹 경쟁력 향상,** ❸**집행 및 이행 개선,** ❹**비은행 PSP의 접근성 개선**을 목표

○ **PSD3는 EU 지침**(Directive)으로서 **국내법으로 적용**되며, **PSR은 EU 규칙**(Regulation)으로서 발효 후 **EU 회원국에 직접 적용** 예정

※ **(지침, Directive)** EU 회원국을 구속하나, 형식과 수단의 선택은 회원국에 유보
**(규칙, Regulation)** 국내법 제정 없이 모든 회원국 내 직접적인 효력 행사

**표 23** PSR/PSD3 상세 내용

| 목표 | 개선 방안 상세 내용 |
|---|---|
| ❶ 소비자 보호·신뢰<br>–<br>사기 위험에 따른 책임 및 SCA 강화 | **[사기 완화 및 책임]**<br>- 모든 신용 이체에 대한 IBAN/이름 확인 확장<br>- 전용 IT 플랫폼을 통해 사기 정보 공유하는 법적 근거 마련<br>- 거래(transaction) 모니터링 강화<br>- 사기에 대한 고객 교육 의무<br>- 사기 피해자(IBAN/이름 확인 실패로 인한 스푸핑 사기)의 환불 권리<br>**[SCA**(Strong Customer Authentication) **강화]**<br>- SCA 적용 의무 면제 대상 명확화 및 사기 방지 조치 도입<br>- 원격 결제 시, 결제인은 결제 금액과 수취인을 명확히 인지<br>- SCA 적용 단순화: AISP는 ASPSP에 처음 접근 시 SCA 의무 적용*, 이후 접근에 대한 SCA 책임은 AISP에게 전가<br>* 단, 사기가 의심되는 경우 제외<br>- SCA 의무 강화: 전자지갑(예시, 삼성페이) 등의 지급결제서비스를 제공하는 PSP에게 SCA 책임을 전가<br>- PSP가 모든 사용자의 필요와 상황에 적합한 SCA 방법을 이용할 수 있도록 보장하고 요구<br>※ 단일 기술, 기기 또는 메커니즘에 의존하지 않도록 보장 |

| 목표 | 개선 방안 상세 내용 |
|---|---|
| ❶ 소비자 보호·신뢰<br>–<br>소비자 권리 및<br>정보 투명성 강화 | **[정보 요구]**<br>– EU에서 제3국으로의 신용이체 및 송금에 대해 투명성* 강화<br>* 환전 수수료, 자금 수령 예상 시간 등 정보 제공 의무<br>– 지급결제계좌 명세서(statement)의 투명성* 강화<br>* 수취인(예시, 상인)을 명확하게 식별하는데 필요한 정보를 포함<br>– ATM 수수료의 투명성* 강화<br>* EU국 내 다른 ATM 운영자가 부과하는 모든 수수료 정보를 제공<br>**[소비자 권리 강화]**<br>– 예약금으로 인해 차단된 자금이 예상 최종 금액과 비례하도록 변경하고 차단된 자금의 지급을 가속화하는 방안 마련<br>– 소매업자에게 특정 금액 이하의 현금 제공 서비스를 제공할 수 있도록 하여 현금의 가용성 향상<br>– 서비스 제공을 위해 필요한 최소한의 개인 정보에만 접근을 허용하고, 은행은 고객이 TPP에게 부여한 모든 권한을 시각화하고 관리할 수 있는 대시보드를 제공하도록 요구 |
| ❷ 오픈뱅킹 경쟁력<br>–<br>오픈뱅킹 기능 향상 | – 전용 인터페이스와 대체 규정을 영구적으로 유지해야 할 의무 제거* 및 '데이터 접근 금지 장벽 목록**' 제공<br>* 비즈니스 연속성을 확보하기 위해 특정하고 일시적인 상황에서 오픈뱅킹 서비스 제공자는 대체 규정을 이용 가능<br>** 데이터 접근을 방해하거나 제한하는 것들에 대한 목록<br>– 설정한 마감일까지 전용 인터페이스를 복원 못한 경우 은행에 벌금 부과, TPP에 영업 손실에 대한 손해 배상 청구 권리 제공으로 오픈뱅킹 제공업체의 비즈니스 연속성을 보호 |
| ❸ 집행 및 이행 | – EMI와 PI 하위 범주로 포함<br>– PSP에 적용되는 대부분의 지급결제 관련 규정(PSD2)은 직접 적용 가능한 규제(PSR)에 포함 |
| ❹ 비은행 PSP 접근 | – 지급결제 시스템 직접 참여자 목록에 결제기관(PI)을 포함 |

※ [참고] 유럽 집행위원회(EC), Payment service: revised rules to improve consumer protection and competition in electronic payments('23.6.28.)

□ FIDA(FInancial Data Access)는 **금융 기관이 고객과 상호 작용하는 과정에서 수집, 저장, 처리되는 포괄적인 데이터* 접근**을 목표

* 고객이 전송하는 데이터(**전송 데이터**), 금융 기관과 상호 작용으로 발생하는 데이터(**거래 데이터**), 금융 상품 및 계약 특징과 관련된 데이터(**비개인 데이터**)

○ FIDA를 통해 **불명확한 데이터 공유 규칙, 부족한 데이터 접근 범위, 부재한 표준화된 전송 형식과 인터페이스** 문제를 해소

**표 24** FIDA 주요 내용

| 구분 | 설명 |
|---|---|
| 필요성<br>(문제) | - 접근 가능한 데이터 범위 불명확, 고객의 공유 권한을 관리하는 도구 부재, 데이터 공유 규제 불명확, 표준화되지 않은 데이터 공유 방식 |
| 데이터 범위 | - 대출, 저축, 투자, 개인연금, 非생명보험, 기업신용평가 데이터 포함<br>- 단, 개인신용평가, 생명, 질병, 건강보험 데이터(민감 데이터)는 제외 |
| 접근 방식 | - 고객에게 비용 없이 전자적 방식으로 데이터 권한(접근/제공)을 부여<br>- 고객 요청에 따라 고객 데이터를 제공해야 할 의무를 도입<br>- 고객 데이터와 공유 인터페이스 표준화 촉진<br>- 데이터 공유는 고객 동의하에 진행하고, 권한 관리 대시보드 구현 |
| 촉진 방안 | - **(경제적 동기)** 데이터 보유자 및 사용자 간에 표준 및 인터페이스 구현 비용을 분담하여 고품질의 데이터 접근 인프라 구축을 유도<br>- **(책임 소재)** 데이터 남용, 금융 범죄, 사기 등 위험에 대비하여 명확하고 예측 가능한 책임 체제 필요<br>- **(거부 요인 방지)** 책임 리스크로 인한 데이터 보유자의 데이터 제공 거부 가능성을 최소화하기 위해 분쟁 해결 메커니즘을 구축 |
| 소비자 신뢰 강화 방안 | - 고객 권한 강화, 민감한 데이터 제외, 대시보드를 통한 고객 허가 요구, 데이터 사용자*에 대한 권한 및 감독 규제 마련<br>* 규제된 금융 기관, 금융 정보 서비스 제공자(FISP), PSR/PSD3 인가된 AISP |

## 5. 시사점

□ 국내 마이데이터 사업자는 계좌 및 관련 거래내역 정보에 접근하는 **AISP에 해당하나, 접근 가능 데이터 범위가 PSD3*와 상이**

* EU내 지급결제 산업 활성화를 위해 오픈뱅킹 규정 강화, 데이터 접근 및 이용 증진, 소비자 보호 강화를 개선

**표 25** PSR/PSD3, FIDA, 국내 금융 마이데이터 비교

| 비교 | PSR/PSD3 | FIDA | 국내 금융 마이데이터 |
|---|---|---|---|
| 비용(수익) | X / 비계약적 접근 | O / 비용 분담 제안 | O / 과금체계 마련 중 |
| 데이터 범위 | 지급결제계좌 데이터 | 지급결제계좌 데이터 외 모든 금융 데이터 (전송/거래/非개인)<br>※ 민감한 데이터 제외 | 모든 개인 금융 데이터<br>※ 국내 마이데이터 사업자는 AISP에 해당 |
| 지급결제 기능 여부 | O | X | X |
| 목표 | 지급결제서비스 개선 | 금융 데이터 접근 확장 | 소비자 편의성 제고 및 빅데이터 산업 활성화 |

○ FIDA* 입법 제안으로 지급결제계좌 데이터에 한정되어 있던 **EU 내 AISP가 접근 가능한 데이터 공유 범위가 확장**

* 지급결제계좌 데이터에 한정된 데이터 공유 범위 확장 및 전송규격과 전송 방식의 표준화 추진

○ PSR/PSD3 인가된 AISP는 FIDA 규율 하에 **모든 금융 데이터에 접근 가능하여, EU 내 금융 산업 혁신이 촉진**될 것으로 전망

○ 또한, **국내 금융 마이데이터 사업자**도 FIDA를 통해 **EU 시장에서의 서비스 가능성과 기회가 확대**될 것으로 전망

□ PSR/PSD3에서 소비자 보호 및 신뢰 강화를 위한 **SCA, 투명성제고 사항 외에 API 관련 변경 사항**은 없는 것으로 파악

○ FIDA에서 금융 기관, FISP, AISP의 지급결제계좌 데이터 외 **모든 금융 데이터 접근을 위해 API가 추가 구현**될 것으로 전망

○ 입법 추진 동향과 변경/추가된 API 방식(데이터 규격, 전송방식)을 파악하여 **향후 필요시 국내 표준 API 방식과 함께 논의**될 필요

□ **FIDA에서 데이터 보유자와 사용자에게 API 표준화 비용 분담**을 제안하였으며, 이는 **국내 금융 마이데이터 과금체계** 목표와 유사

○ 향후 국내 금융 마이데이터 **과금체계 조정 추진 시, 해외 사례 차원에서 공유**하기 위해 지속적으로 모니터링할 필요

**표 26** API를 통한 수익 모델

| 항목 | 주요 내용 |
|---|---|
| 데이터 모델 | - API 제공기관이 정보(접속 시간대, 건수 등)를 분석해 유로로 제공 |
| 거래 모델 | - TPP가 API 제공기관에게 API 통한 지급거래 완료 시 요금을 납부 |
| 종량제 모델 | - TPP가 API 제공기관에게 API 이용 건 별로 요금을 납부 |
| 구독 모델 | - TPP에 API 제공기관이 일정기간 동안의 (고정/가변적) 사용료를 바탕으로 API 패키지를 제공 |
| 프리미엄 모델 | - 기본서비스는 무료로 제공하되 심화 서비스의 경우 유료화 |
| 매출 공유 모델 | - TPP가 API 제공기관에 매출 중 일정 비율로 납부 |

※ [참고] 한국은행, 영국의 지급결제제도 개편 동향 및 특징

## 별첨1 마이데이터 원칙 및 기능 요구사항

□ **마이데이터**로 기업 중심 개인정보 관리·활용 체계*를 **정보주체인 개인에게 데이터 권한**을 부여**함으로써 인간 중심 체계로 전환

* 개인 데이터 접근, 이동, 활용 등에 대한 통제권 및 결정권

** 동일인의 동일한 데이터 산재, 기관별 개인정보 관리 수준 상이, 개인정보 관리 비용, 법률 리스크, 정보주체의 개인정보 추적 어려움 등의 문제 존재

○ 마이데이터 글로벌*은 **원활한 인간 중심 관리·활용 체계 전환**을 위해 마이데이터 운영자에게 **6가지 마이데이터 원칙**을 제시

* 개인 데이터의 결정권을 개인에게 부여하는 것을 목표로 국제적인 마이데이터 서비스의 선도적 정책 방향을 제시하는 국제 비영리단체

○ 이에, **마이데이터 운영자**는 개인이 본인 데이터를 **안전하고 쉽게 관리할 수 있도록 도구 및 서비스**를 구축하여 제공 가능

[운영자를 위한 마이데이터 원칙]

| 마이데이터 원칙 | 설명 |
|---|---|
| ❶ 인간 중심 관리·활용 | - 개인이 **본인 데이터에 대한 통제 권한**(자기결정권)을 가지고 있는 상태로, 운영자 또는 다른 주체가 개인 데이터를 처리하거나 사용할 때 항상 개인의 권한을 유지할 필요 |
| ❷ 데이터 통합의 중심 | - 개인이 여러 서비스와 데이터를 한 곳에서 효과적으로 관리하고 활용할 수 있도록 운영자는 다양한 서비스와 데이터를 **개인의 요구에 맞춰 통합하여 제공**해야 할 필요<br>- 운영자는 개인 중심적인 통합의 역할을 수행하여 개인에 대한 책임(보호의무)을 가지고 개인 데이터를 안전히 관리할 필요 |
| ❸ 데이터 권한 부여 | - 운영자가 개인이 데이터를 요청받았을 때 허용을 부여하는 것 외에도 **다양한 실질적인 선택권*을 갖도록 지원**할 필요<br>* 개인이 자율적으로 데이터를 관리하고 활용할 수 있는 권한 |
| ❹ 이식성(접근 및 재사용) | - 운영자는 개인에게 데이터 통제 권한 지원뿐만 아니라 **자신만의 용도로 데이터를 활용**(재사용)**할 수 있도록 지원**할 필요 |
| ❺ 투명성 및 책임 | - 운영자는 개인에게 본인의 데이터가 **어떻게 수집되고 사용되는지에 대한 정보를 제공**할 필요<br>- 운영자는 개인 데이터 사용에 대한 결과에 책임을 져야 하며, 필요시 조치를 취해 개인과의 신뢰를 유지할 필요 |
| ❻ 상호운용성 | - 운영자는 **데이터를 전송할 때 표준을 준수**하여 개인이 운영자간 데이터를 전송할 수 있는 환경을 조성할 필요 |

※ MyData Global, Understanding Mydata Operators('22.3월)

□ **마이데이터 원칙에 따라 투명하고 인간 중심적인 데이터 개방 환경을 제공**하기 위해 운영자는 **9가지 핵심 기능을 보장**할 필요

[EU 마이데이터 운영자(Operator)의 핵심 기능 요소]

| 목적 | 핵심 기능 요소 | 설명 |
|---|---|---|
| 식별·권한 부여 | ❶ 신원 관리 | - 신원 도메인(identity domains)에 연결된 서로 다른 개인 및 조직의 인증과 권한을 처리하고, 신원과 권한을 연결 |
| | ❷ 권한 관리 | - 개인이 본인 데이터를 통제하는 법적 권리를 행사할 수 있도록 지원<br>- 데이터 교환에 대한 기록*을 보존할 필요<br>* 통지, 동의, 권한, 지령, 법적 근거, 목적 선호 등 |
| 생태계 구성 | ❸ 서비스 관리 | - 서비스는 개인이 다양한 데이터를 이용할 수 있도록 다른 참여자(데이터 소스)와의 연결을 지원하여 데이터 이동성과 재사용성을 향상<br>- 이에, 서비스 관리는 데이터 소스와 서비스의 관계와 연결을 관리할 수 있도록 지원<br>- 개인이 데이터를 자유롭게 활용하고 참여자간 상호 작용을 증진시킬 수 있는 기능*을 제공<br>* 동적 연결 구성, 데이터 접근제어, 기술적인 연결 관리 등 |
| | ❹ 가치 교환 | - 데이터 교환의 결과로 생성된 가치*를 확보하거나 적절하게 추적하고 활용할 필요<br>* 금전적 가치, 크레딧, 평판, 포인트 등 |
| 데이터 관리 | ❺ 데이터 모델 관리 | - 데이터의 의미를 명확하고 일관되게 유지하기 위해 데이터 구조, 속성, 관계를 정의하고 데이터 표현 방법을 제공<br>- 서로 다른 시스템에서 생성한 데이터를 효과적으로 상호 작용 및 통합 가능하도록 데이터 모델 변환* 기능도 제공<br>* 데이터의 의미와 해석을 유지하면서 데이터의 구조나 형식을 다른 데이터 모델로 변환 |
| | ❻ 개인정보 전송 | - 마이데이터 참여자 간에 안전한 데이터 교환이 가능하도록 표준화된 인터페이스(API)를 구현 |
| | ❼ 개인정보 저장 | - 개인의 통제하에 다양한 데이터를 개인 데이터 저장소*에 통합할 수 있도록 지원<br>* PDS(Personal Data Store), 개인이 본인 데이터를 저장, 관리 및 통제할 수 있는 공간 및 시스템 |
| 보안(투명성)·신뢰 제공 | ❽ 거버넌스 지원 | - 개인과 조직 간에 신뢰할 수 있는 관계를 확립하기 위해 기본적인 거버넌스 프레임워크를 준수할 수 있도록 지원 |
| | ❾ 로깅 및 책임 | - 운영자가 제공하는 서비스 내 발생하는 모든 정보 교환을 추적하고 누가 언제 어떤 정보에 접근했는지에 대한 투명성을 위해 필요 |

※ MyData Global, Understanding Mydata Operators('22.3월)

## 별첨 2 RSB의 PSD2 검토 결과

※ [참고] EU 역내시장 지급결제 서비스에 관한 PSD2 검토 최종 보고서('23.6.28.)

### □ 오픈뱅킹 인터페이스

| 구분 | 오픈뱅킹 인터페이스 문제 및 방안 |
|---|---|
| 문제 | - 데이터 접근 **API 품질·성능** 차이<br>- ASPSP의 **API 구현 비용** 부담<br>- TPP에 API 이용 요금 청구 제약<br>- TPP의 **낮은 API 사용** 빈도(TPP는 주로 자체 인터페이스 사용) |
| 방안 | - 새로운 단일 API 표준 도입 대신 **API 집계자***(aggregator) 사용<br>* 단일 구현 지점을 제공하여 다수의 다른 API에 대한 동시 연결을 허용<br>- 개정안에 데이터 **인터페이스 성능 최소 요구사항** 규정<br>- ASPSP는 데이터 **접근 권한 대시보드 구현**하여 고객에게 제공<br>- **주 인터페이스**(API)**, 대안 인터페이스**(스크린 스크레이핑) **제공** 유지<br>* 서비스 제공에 필요한 전용 인터페이스를 구현한다면 두 인터페이스 요구사항을 계속 유지할 필요 없음<br>- AISP를 PSD에서 **FIDA*로 이전**하는 것을 고려<br>* Financial Data Access, 결제 계좌 데이터 이상의 금융 데이터 접근 의무를 확대하는 금융 정보 데이터 접근에 관한 입법 제안(오픈 파이낸스라고도 지칭) |

### □ 규제 적용 범위

| 구분 | 규제 적용 범위 문제 및 방안 |
|---|---|
| 문제 | - 새로운 서비스 제공자 중 일부*는 **기술 서비스 제공자**(TSP, Technical Service Provider)로서 **PSD2 범위에서 제외**<br>* **(지급결제 수단)** 즉시 지불 결제, 전자화폐 토큰 등<br>**(결제 수단)** 전자지갑 등<br>**(지원 서비스)** 구매 후 지불(buy-now-pay-later), 요청 지불(request-to-pay) 등<br>- DORA(Digital Operational Resilience Act) 위원회는 **PSD2 범위 안에 '결제 시스템 운영업체 및 결제 처리 활동에 관여하는 주체'를 고려**할 것을 지시<br>※ DORA는 EU 법률에 따라 규제되고 감독되는 금융 기관에만 적용되므로 PSD2 규제받지 않는 PSP(Payment Service Provider)는 DORA 범위에서 벗어남 |
| 방안 | - 현재 PSD2에 포함되지 않은 많은 서비스와 해당 제공업체는 이미 유럽 중앙은행/유로시스템 감독(PISA 감독 프레임워크)을 받고 있거나 곧 받을 것으로 전망되어, **새로운 감독 조항을 추가하는 것은 중복 규제**로 판단<br>- PSD2는 최종 사용자에게 제공하는 서비스를 규제하는 것이므로, **지급결제 서비스 아닌 지원 서비스는 PSD2 규제에 포함하지 않음**<br>- 특정 조건을 만족하는 ATM 운영자에 대한 PSD2 규제 적용 제외 조항을 제거하고 **더 가벼운 등록 제도와 적절한 수준의 규제로 지급결제 서비스를 제공하지 않는 PSP도 PSD2 범위에 포함**하는 것을 제안 |

## □ 소비자 보호

| 구분 | 소비자 보호 문제 및 방안 |
|---|---|
| 문제 | - **(수수료 규제)** 유로가 아닌 다른 화폐로 이뤄지는 신용/직불 거래에는 PSD2의 수수료 부과 금지 규정*이 미적용<br>* 신용카드나 직불 카드와 같이 교환 수수료 규제가 적용된 지급결제 서비스 제공자는 고객에게 추가 요금(카드 사용 수수료 등)을 부과할 수 없음<br>- **(EU 역외 거래)** EU 역내에서 제3국으로의 송금 및 신용 거래에 대한 비용과 수수료에 대한 투명성을 규제하지 않음<br>- **(통신망 공급자)** 통신망 공급자에 의한 지급결제는 거래당 EUR 50, 월 EUR 300으로 제한되며, 통신망 공급자에 의한 지급결제는 소비자 통신망 청구서에 포함되어 청구되기 때문에, PSD2 규제에 적용하지 않음<br>- **(디파짓)** 불확실한 금액 지불을 지급결제 카드로 사용할 때 디파짓이 불필요하게 높거나 반환 시기가 서비스 제공자별 각기 다르며, 특정 서비스의 경우 소비자의 명시적인 반환 요청을 요구하는 문제 |
| 방안 | - 모든 통화를 포함하여 모든 신용/직불 거래에 대해 수수료 부과 금지 규정을 도입하는 것을 제안<br>- 소비자가 EU 외 다른 나라로 신용카드 자동이체 및 송금할 때 환율에 따른 예상 비용과 송금이 수령되는 예상 시간을 알려주는 의무를 제안<br>- 휴대폰 결제 등 통신망 공급자에 의한 지급결제는 PSD2 규제에 적용되지 않으며, 기존 한도를 그대로 유지하며 적정성을 지속 모니터링할 예정<br>- 미사용된 디파짓의 반환 속도를 높이고 디파짓이 최종 결제 금액과 비례하도록 요구하는 개정안을 제안 |

## □ 보안 및 사기 방지

| 구분 | 보안 및 사기 방지 문제 및 방안 |
|---|---|
| 문제 | - 오픈뱅킹 서비스에 SCA(강화된 사용자 인증) 도입으로 지급결제 사기가 크게 감소하였으나, **구현 복잡성, 시스템 구축 및 유지 관리 비용 증가, 거래 편의성 저해, 사용자 경험 저해 문제**가 발생<br>- SCA는 **사회 공학을 통한 사기 공격에 효과가 미미**하며, 소비자는 해당 유형의 사기 공격에 대한 환불 권리를 보장할 수 없음 |
| 방안 | - SCA는 지급결제 사기를 방지하는데 매우 효과적임으로 **현행 유지**<br>- PSP간 사기 정보를 공유하는 법적 근거 마련, 소비자 대상 교육 조치 의무, IBAN/이름 검증 서비스 적용 확대, SCA 적용 개선 등 사기 예방 및 보상을 위한 **새로운 조치를 제안**<br>- 사회 공학을 통한 사기 공격으로 손해를 입은 경우 소비자가 환불받을 수 있는 보호장치의 필요성을 인식하여 **책임 규정 개정 등을 고려** |

## □ 디리스킹 및 경쟁

| 구분 | 디리스킹 및 경쟁 문제 및 방안 |
|---|---|
| 문제 | - 비은행 PSP가 지급결제 서비스를 제공하기 위해 지급결제를 처리할 수 있는 주요 인프라에 접근해야 하나, 은행의 디리스킹 문제로 지급결제기관(PI)과 전자화폐발행기관(EMI)의 서비스 제공이 어려움*<br>* 비은행 PSP는 지급결제계좌서비스를 제공할 수 있지만 은행과 달리 대출은 할 수 없으며, 서비스 제공 자격을 얻기 위해 고객 자금을 은행에 보호할 필요<br>- 결제완결성*지침(SFD, Settlement Finality Directive)에 비은행 PSP 미포함<br>* 지급결제제도 참가 금융기관의 이체지시에 따라 동 제도를 통해 이뤄지는 결제는 어떠한 상황이나 법률에 의해서도 취소가 불가능하고 지급결제제도가 정하는 절차에 따라 무조건적으로 이루어질 필요 |
| 방안 | - 은행이 비은행 PSP를 대상으로 접근을 거부하거나 서비스를 취소하는 경우, 거부 사유에 대한 강력한 설명 요구 사항이 PSD2 개정안에 포함<br>- 중앙은행은 재량에 따라 비은행 PSP의 계좌 서비스 제공을 허용<br>- 위원회는 PI를 SFD 대상에 포함하도록 개정할 것을 제안<br>- PI를 지급결제시스템 참가자로 인정하는 것에 대한 강화된 규칙과 적절한 위험 평가가 PSD2 개정안에 포함 |

## □ 집행(Enforcement)

| 구분 | 집행 문제 및 방안 |
|---|---|
| 문제 | - PSD2는 EBA의 의견 및 지침이 있음에도 불구하고 지급결제 시장의 다양한 이해관계자에 의해 PSD2가 다르게 해석되고 구현<br>- PSP가 본인들에게 유리한 방식으로 PSD2 규칙을 적용 |
| 방안 | - 벌칙 관련하여 국가 관할 당국의 집행력을 강화하고, PSD2 규칙 대부분을 직접 적용 가능한 규정으로 전환 |

## □ 기타

| 구분 | 기타 문제 및 방안 |
|---|---|
| 문제 | - **(소규모 지급결제기관)** 지급결제 거래 규모(임계치)가 적은 소규모 지급결제기관(PI)에 완화된 감독 요구사항을 적용 가능<br>- **(단순화)** 금융 감독 당국에서 전자화폐(EM) 상품 및 서비스와 PI가 제공하는 지급결제 서비스를 구별하는 데 어려우며, 유사성을 악용하여 전자화폐를 발행하는 일부 기관에서 지급결제기관(PI)으로만 허가를 신청하여 전자화폐지침2(EMD2)의 요구사항을 우회 |
| 방안 | - **(소규모 지급결제기관)** 완화된 감독 수준으로 문제가 발견되지 않았으나, 소규모 지급결제기관(PI) 해당 요구사항(임계치)을 주기적으로 업데이트<br>- **(단순화)** 규제 차익 거래를 방지하며, 공정한 경쟁 환경을 위해 전자화폐기관(EMI)과 지급결제기관(PI)을 규율하는 규정을 통합 |

# 유럽연합(EU)의 「사이버 복원력 법안」 주요 내용 및 시사점[주)]

**EU 집행위**는 **H/W 및 S/W 제품**의 **보안성 강화**를 위해 「**사이버 복원력 법안**(Cyber Resilience Act, 이하 'CRA')」 제정을 **추진** 중*으로 법안 **주요 내용** 및 **시사점**을 검토

* '22.9.14에 법안이 발의된 후, '23.7월 수정안이 유럽 이사회에서 논의 → 이후 유럽의회 논의 및 투표과정을 거쳐 법안 채택 예정(법안 채택 시 2년 후 시행)

## 1. 법안 추진 배경

□ **(제조업체)** H/W 및 S/W **취약점**에 대한 **조치 미흡**, 일관성 없는 **보안 업데이트** 등 **제품**의 **보안 수준**이 전반적으로 **저조**

□ **(이용자)** 제품에 대한 **이해**와 **정보접근성**이 **부족**하여 **적정한 보안수준**을 갖춘 제품을 **선택** 또는 **사용하지 못하는 문제**

➜ EU 집행위는 H/W 및 S/W 제품의 **보안성 강화**를 통해 **보안사고 발생 위험을 경감**하기 위해 **CRA 제정**을 추진

※ '21년까지 사이버범죄로 지출한 연간 비용이 전 세계적으로 5조 5천억 유로에 달함.(출처 : Cybersecurity Ventures)

[CRA의 2대 전략 및 4대 목표[주)]]

| 구분 | 내용 |
|---|---|
| 2대 전략 | 1. 취약점이 적은 제품이 시장에 출시되고, 제조업체가 제품 생명주기 동안 보안을 중요하게 고려하도록 보장(안전한 제품개발 여건 조성)<br>2. 이용자가 제품 선택이나 사용 시 보안을 고려할 수 있는 여건 조성 |
| 4대 목표 | 1. 제조업체가 제품 생명주기에 걸쳐 제품의 보안을 개선하도록 보장<br>2. 일관된 사이버보안 프레임워크를 보장하여 제조업체의 규정준수 촉진<br>3. 제품의 보안 속성에 대한 투명성 제고<br>4. 이용자(기업, 소비자)가 제품을 안전하게 사용할 수 있도록 지원 |

주) EU집행위는 보도자료에서 '주된 목표', '세부 목표'로 명시하였으나, 본 보고서에서는 쉬운 이해를 위해 '2대 전략' 및 '4대 목표'로 문구 조정

주) 이준호, 금융보안원 보안연구부 수석

## 2. 법안 주요 내용

[주요 내용]

□ 제품을 **시장에 출시**할 때 **보안성 보장**을 위해 필요한 사항
□ 제품의 **설계 · 개발 · 생산** 시 필수 **보안 요구사항** 및 **경제운영주체***의 **의무**
* 제조업체, 대리인, 수입업체, 유통업체, 제품을 수정할 수 있는 자연인 · 법인
□ 제품 생명주기 동안 보안성 확보를 위해 **취약점 조치** 관련 **요구사항** 및 제조업체의 **사고보고 의무**
□ **시장 감시** 및 **집행**에 관한 사항

### (1) 적용범위(Scope)

□ 장치나 네트워크에 **디지털 요소가 포함된 제품**(이하 '제품')이 본 **법안의 적용 대상(금융분야 제품**도 본 법안 적용 대상에 해당)

○ 다만, **의료 및 차량, 항공 등** 일부에 대해서는 **법안 적용 배제**

[법안 적용 배제 기준]

① **EU 內 타 규정이 적용되는 경우**
ⅰ) 인체용 의료기기 및 해당 기기용 부속품(Regulation 2017/745)
ⅱ) 인체용 체외 진단 의료기기 및 해당 기기용 부속품(Regulation 2017/746)
ⅲ) 자동차 및 트레일러, 해당 차량을 위한 시스템/구성요소/별도의 기술장치(Regulation 2019/2144)
② **EU 內 타 규제에 의해 인증받은 경우** : 민간 항공 안전(Regulation 2018/1139)
③ **국가안보**나 **군사목적**으로만 개발된 제품, **기밀정보 처리용도**로 특별히 설계된 제품
④ **필수 보안 요구사항과 관련된 위험을 다루는 내용이 타 EU 규제에 포함된 경우**

### (2) 일반 사항(General provisions)

□ **보안** 등 **중요 디지털요소가 포함**된 제품은 잠재적 보안 취약점 영향을 고려해 **'중요 제품'**으로 간주

○ **중요 제품**은 **보안위험 수준**에 따라 **클래스Ⅰ**과 **클래스Ⅱ**로 구분(보안위험수준 : 클래스Ⅰ < 클래스Ⅱ)되며, **적합성 평가 규제**가 적용

※보안위험 수준은 제품의 보안 기능 및 사용 목적·환경 등을 고려하여 선정

**[중요제품 간주 대상**(상세 내용은 법안 부록Ⅲ(별첨 3) 참조)]

| 클래스 I | 클래스 II |
|---|---|
| ID 관리, 비밀번호 관리, 악성S/W 탐지·대응, 가상사설망, 네트워크 관리, 네트워크 트래픽 모니터링, 보안 이벤트 관리, 어플리케이션 관리, 원격 접속, 모바일장치 관리, 클래스 II에 포함되지 않는 운영체제/방화벽/라우터/마이크로프로세서/사물인터넷, 마이크로컨트롤러 등 | 서버/PC/모바일장치 운영체제, 가상화 지원, 공개키(인증서)인프라, 산업용 방화벽, 범용 마이크로프로세서, 보안요소, 하드웨어 보안모듈(HSM), 암호화 프로세서, 스마트카드 및 토큰, 로봇 컨트롤러, 스마트계량기 |

□ **EU 집행위**는 위험수준을 고려하여 **'매우 중요한 제품'**을 **지정 및 규제** 가능

○ 매우 중요한 제품의 지정은 NIS* 지침에 따른 **필수기관****에서 **사용**하거나, 해당 기관의 **활동에 미치는 영향 등**을 고려

* 「Network and Information System 2 Directive」(네트워크 및 정보시스템 지침 2)

** 은행 부문의 신용기관, 금융시장인프라 부문의 거래소, 중앙청산소(CCP)가 포함

○ **매우 중요한 제품**에 대해서는 향후 **인증**을 **의무화**할 계획

### (3) 경제운영주체의 의무 (Obligations of economic operators)

□ **(제조업체)** 보안사고 예방을 위해 **필수 보안 요구사항**(별첨 1)에 따라 제품을 **설계·개발·생산**

[제조업체의 주요 의무]

- 사용자의 건강・안전 등 사고영향 최소화를 위해 제품의 기획·설계·개발·생산·배송·유지관리 단계에서 평가결과를 고려
- 제조업체는 제품 출시 시 기술문서(§23・별첨 5)를 작성(SBOM 등)하고, 위험 평가 결과를 포함
- 제3자로부터 공급받은 구성 요소를 제품에 사용하는 경우 제3자 실사
- 예상되는 제품수명 또는 출시 후 5년 중 짧은 기간동안 취약점을 필수 요구사항(별첨 1의 section 2)에 따라 처리하고, 취약점 공개 정책을 포함한 정책 및 절차 마련
- 선택된 적합성 평가절차(chosen conformity assessment procedures)를 진행하고, 이를 통해 제조업체의 프로세스가 입증된 경우 'EU 적합성 선언(EU declaration of conformity)' 작성 및 CE 마크를 부착
- 제품이 적합성을 유지할 수 있도록 절차를 마련

○ 사용자에게 제공되는 정보 및 안내는 전자적 또는 물리적 형태로 제공하되, 사용자가 쉽게 이해할 수 있는 언어로 작성하여 가독성을 제공
○ 예상되는 제품 수명 또는 출시 후 5년 中 짧은 기간동안 필수 보안 요구사항에 위반된다는 사실을 알거나 그렇게 믿을 만한 사유가 있는 경우, 제조업체의 절차에 따라 조치를 즉시 취하고 제품을 리콜
○ 제조업체의 운영 중단으로 의무 준수가 어려운 경우, 사전에 해당 사실을 시장감시당국 및 제품 이용자에게 통지
○ 제품에 악용할 수 있는 취약점이 발견되거나 보안에 영향을 미치는 사고가 발생하는 경우 해당 사실 및 취약점 세부 내용, 시정·완화 조치 등을 지체 없이(최초 인지 후 24시간 이내) ENISA에 통지

□ **(대리인)** 제조업체로부터 명시적으로 **위임받은 업무**를 수행

[대리인의 주요 의무]

○ 제조업체의 'EU 적합성 선언' 및 기술문서를 제품 출시 후 10년간 보관
○ 시장감시당국의 요청이 있을 경우 적합성 입증에 필요한 모든 정보와 문서를 제공
○ 제품과 관련하여 취한 모든 위험 제거 조치에 대해 시장감시당국과 협력

□ **(수입 업체) 필수 보안 요구사항**(별첨 1 참조) 및 취약점 처리 요구사항(별첨 1의 section 2)을 **준수하는 제품만 시장 출시**

[수입업체의 주요 의무]

○ 제조업체의 적절한 적합성 평가절차 수행, 기술문서 작성, CE 마크 부착, 사용자에게 제공할 정보 및 안내 구비 여부 등 확인
○ 제품에 수입업체의 상호, 등록된 상호나 상표, 주소 및 이메일 주소 등을 표시
(단, 제품에 표시가 어려울 경우 포장 등에 표시)
○ 제품이나 제조업체의 프로세스가 필수 보안 요구사항에 부합되지 않는다는 사실을 알거나 그렇게 믿을만한 사유가 있는 경우 즉시 시정조치 또는 리콜
○ 제품에 취약점 발견 시 이를 지체 없이 제조업체에 알리고, 만약 중대한 보안 위험이 있는 경우 즉시 시장감시당국에 통지
○ 제조업체의 'EU 적합성 선언' 및 기술문서를 제품 출시 후 10년간 보관
○ 시장감시당국의 요청이 있을 경우 필수 보안 요구사항 및 취약점 처리 요구사항 입증에 필요한 모든 정보 및 문서를 제공
○ 제품과 관련하여 취한 모든 위험 제거 조치에 대해 시장감시당국과 협력

□ **(유통업체)** 제품을 **출시**할 때 본 규정에 따른 보안 요구사항에 대해 **적절한 주의**를 기울일 필요

[유통업체의 주요 의무]

- ㅇ CE 마크 부착, 제조업체가 이용자에게 제공하는 정보・안내, 'EU 적합성 선언' 제공 여부, 수입업체의 상호 등의 제품 표시 여부를 확인
- ㅇ 제품이나 제조업체의 프로세스가 필수 보안요구사항에 부합되지 않는다는 사실을 알거나 그렇게 믿을만한 사유가 있는 경우 제품을 출시하지 말아야 하며, 이로인해 심각한 보안위험을 초래할 경우 제조업체 및 시장감시당국에 통지
- ㅇ 제품이나 제조업체의 프로세스가 필수 보안 요구사항에 부합되지 않는다는 사실을 알거나 그렇게 믿을만한 사유가 있는 경우 즉시 시정조치 또는 리콜
- ㅇ 제품에 취약점 발견 시 이를 지체 없이 제조업체에 알리고, 만약 중대한 보안 위험이 있는 경우 즉시 시장감시당국에 통지
- ㅇ 시장감시당국의 요청이 있을 경우 필수 보안 요구사항 및 취약점 처리 요구사항 입증에 필요한 모든 정보 및 문서를 제공
- ㅇ 제품과 관련하여 취한 모든 위험 제거 조치에 대해 시장감시당국과 협력

### (4) 제품의 적합성(Conformity of the product with digital elements)

□ **(적합성 추정)** EU 관보에 게재된 **통일규격*** 또는 그 일부에 부합하는 제품은 **필수 보안 요구사항을 준수**하는 것으로 추정

* 「Regulation 1025/2012」 §2(1)(c)에 따른 통일규격(harmonised standard)으로, EU 집행위 요청으로 채택된 유럽 표준을 의미

○ 통일규격이 아닌 **공통사양* 준수 제품**은 공통사항에 명시된 내용에 대해 해당 **필수 보안 요구사항**을 **준수**하는 것으로 추정

* 통일규격이 없거나 미흡한 경우 또는 표준화 절차가 지연되거나 유럽 표준화기구에서 표준화를 거부하는 경우, EU 집행위는 필수 보안 요구사항에 대한 공통사양 채택 가능

○ **유럽 보안 인증제***에 따라 `EU 적합성 선언' 또는 인증서를 받은 제조업체의 제품은 **필수 보안 요구사항**을 **준수**하는 것으로 추정

* 「Regulation 2019/881」에 따라 채택되고 EU 집행위원회가 지정한 인증제

□ **(적합성 평가) 제조업체**는 '법안 부록Ⅵ'(별첨 6)에 기반하여 제품의 **적합성 평가**와 **필수 보안 요구사항**의 **충족 여부**를 확인

○ 적합성 평가는 **4개 모듈***로 구분되며, 일반제품과 중요제품(클래스Ⅰ, 클래스Ⅱ)별로 **중요도**에 따라 **적합성 평가 모듈**을 선정

* 모듈A(제조업체 내부통제 절차에 기반한 평가), 모듈B(EU-type 심사), 모듈C(내부 생산통제에 기반한 평가), 모듈H(전체 품질보증에 기반한 평가)

[제품 중요도별 적합성 평가방법]

| 구분 | | 적합성 평가방법 |
|---|---|---|
| 일반 제품 | | 모듈 A |
| 중요제품 | 클래스 Ⅰ | 모듈 A + 적합성 추정(통일규격, 공통사양, 사이버보안 인증제)*<br>* 적합성 추정이 어려울 경우 제3자를 통한 '모듈B + 모듈C'나 '모듈H' 적용 |
| | 클래스 Ⅱ | 제3자를 통한 '모듈 B + 모듈 C' 또는 '모듈 H' |

□ **(EU 적합성 선언)** 제조업체는 '법안 부록Ⅵ'(별첨 4)에 따라 **필수 보안 요구사항** 충족 여부를 포함한 **'EU 적합성 선언'**을 작성

○ **'EU 적합성 선언'**은 지속 **업데이트**하여야 하며, 제조업체는 이를 통해 제품의 적합성 준수에 대한 **책임**을 **부담**

□ **(CE* 마크)** 「Regulation 765/2008」 §30에 따른 일반원칙을 준수

* CE(Conformity to European) : EU 시장이 단일화되면서 역내 기술장벽 제거를 위해 소비자 안전, 건강·위생, 환경보호와 관련된 EU 조건을 준수함을 인정(EU 시장에 제품을 수출하기 위해서는 필수적으로 인증 취득 필요)

※ 네이버 지식백과 시사상식사전(terms.naver.com/entry.naver?docId=74442&cid=43667&categoryId=43667)

○ EU **회원국**은 **CE 마크 관리**를 위한 **체계**를 마련하고, 해당 마크가 **부적절**하게 **사용**되는 경우 **적절한 조치**를 취할 필요

[CE마크 부착 방법]

- CE 마크는 눈에 잘 띄고 읽기 쉬우며 지워지지 않도록 제품에 부착(제품 특성 상 부착이 어려운 경우는 포장에 부착)
- S/W의 경우 CE마크는 웹사이트에 게시
- CE 마크는 눈에 잘 띄고 가독성이 유지된다면 마크의 높이를 5mm 이하로 표기 가능
- CE 마크는 출시 전에 부착돼야 하며, 특별한 위험 또는 용도를 나타내야 하는 경우에는 CE 마크에 이어서 픽토그램(pictogram)이나 기타 마크를 표시
- CE 마크 뒤에는 적합성 평가절차에 관여하는 인증기관*의 식별번호를 표시

  * 본 법안에 따라 지정된 적합성 평가기관

□ **(기술문서)** 제품과 제조업체가 **필수 보안 요구사항**을 **준수**함을 **법안 부록V** (별첨 5)에서 사항에 따라 기재

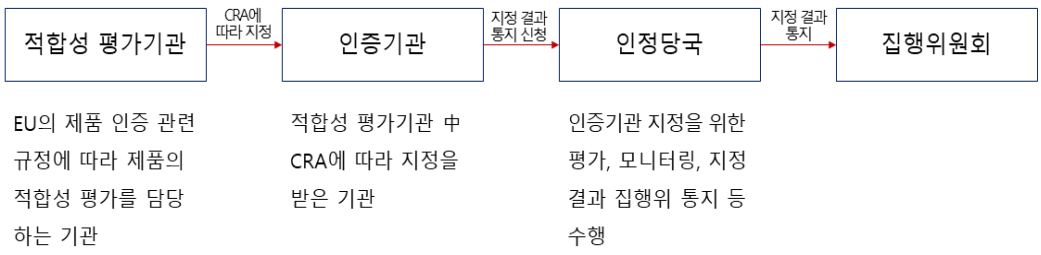
○ 기술문서는 **제품 출시** 전에 작성되어야 하고, 예상 제품 수명기간동안 또는 5년 中 짧은 기간 동안 **지속적**으로 **업데이트**

### (5) 적합성 평가기관 통지(Notification of conformity assessment bodies)

□ EU 회원국은 자국의 **적합성 평가기관을 EU 집행위원회 및 다른 회원국에 통지**

○ 적합성 평가기관 中 CRA에 따라 지정을 받은 경우 **인증기관**이 되며, 적합성 평가기관 및 인증기관은 지정된 **인정당국**이 관리

[적합성 평가기관 간 관계]




[인정당국에 대한 요구사항]

- ㅇ 적합성 평가기관과 이해상충이 발생하지 않는 방식으로 설립
- ㅇ 활동의 객관성과 공정성을 보장할 수 있도록 조직되고 기능
- ㅇ 적합성 평가기관에 대한 통지를 이에 관여하는 사람이 담당하는 것은 불가
- ㅇ 적합성 평가기관의 활동이나 컨설팅을 상업적 또는 경쟁적으로 제공하는 것은 불가
- ㅇ 취득한 정보의 기밀을 보호
- ㅇ 적절한 업무수행을 위해 전문인력을 충분히 보유

□ **적합성 평가기관**은 평가하는 조직 또는 제품과 **독립적인 제3기관**이어야 하며, 평가업무를 수행할 수 있는 **인프라**를 갖출 필요

[적합성 평가기관에 대한 요구사항]

ㅇ 적합성 평가업무를 수행하기 위한 기술과 충분하고 적절한 경험을 갖춘 직원 보유
ㅇ 적합성 평가 수행절차에 대한 설명, 해당 절차의 투명성과 재생산 능력을 보장 (인증기관으로서의 수행 업무와 다른 활동을 구분하는 정책과 절차를 마련)
ㅇ 사업규모, 사업운영 부문, 구조, 해당 제품 기술의 복잡성 정도, 생산공정의 대량 또는 연속적 특성을 적절히 고려한 활동수행을 위한 절차
ㅇ 책임보험에 가입 (단, 회원국에서 직접 책임을 부담하는 경우 등은 제외)
ㅇ 직무상 비밀 준수의무를 부담

□ EU **집행위원회**는 **인증기관에 식별번호를 부여**하고 기관 목록, 식별 번호, 통지된 활동 등의 최신 상태를 공개

○ **EU 집행위원회는 인증기관의 역량 또는 요건 및 책임**의 이행에 대해 **의심**이 있거나 의심이 제기되는 경우 **조사를 실시**

- 조사결과, 문제가 있을 경우 **통지 취소**를 해당 인증기관을 관리하는 EU 회원국에 알려 **시정조치를 요청**

[인증기관의 의무]

ㅇ 본 법안에 따라 적합성 평가를 실시하되, 경제운영주체에 불필요한 부담을 초래하지 않도록 비례성을 고려
ㅇ 제조업체가 통일규격 등의 요건을 충족하지 못 할 경우 적절한 수정을 요구하거나 적합성 인증서를 未 발급
– 또한, 증명서 발행 이후 해당 제품이 더 이상 요건을 충족하지 못한다고 확인하는 경우 적절한 시정조치를 요구하거나 해당 증명서를 중지 또는 취소
ㅇ 인증서의 거절・제한・중지・취소, 통지의 범위・조건에 영향을 미치는 상황, 적합성 평가에 관해 시장감시기관에서 받은 정보 요청, 적합성 평가활동 등을 인정당국에 통보

### (6) 시장감시 및 집행(Market Surveillance and Enforcement)

□ EU **회원국**은 효과적인 CRA 시행을 위해 **1개 이상의 시장감시기관**을 지정

□ **시장감시기관**은 특정 제품* 등에 대하여 본 법안 준수 여부 및 위반 적발 등을 위하여 **'특별 단속'**(simultaneous coordinated control actions)을 **실시**

○ EU집행위는 특별 단속을 계획·이행하며, 시장감시기관은 필요 시 **집행위원회 소속 직원**이나 **해당 위원회가 승인한 그 밖의 자**에게 **특별 단속 참여**를 **요청**

[시장감시기관의 역할]

○ 타 시장감시기관, ENISA, 데이터보호법 감독당국 등과 정보 공유 또는 협력할 수 있으며, EU 집행위는 시장감시기관간 공유를 촉진
○ EU 집행위의 지원을 받아 경제운영주체에게 지침 및 조언을 제공
○ 매년 활동 결과를 EU 집행위에 보고
○ 필수 보안 요구사항에 대한 적합성 평가를 위해 경제운영주체에 각 제품의 설계・개발・생산, 취약점 처리에 관한 데이터 수집 권한을 행사
○ 제품이 중대한 보안 위험을 야기할 수 있다고 판단되는 경우 해당 제품 평가 실시
- 기준 요건을 충족하지 못할 경우 지체 없이 관련 운영자에게 위험에 상응하는 요건의 준수를 요구하거나 시장에서 철수 등 시정조치를 요구 (해당 사실을 인증기관에도 통지)
- 제조업체가 시정조치를 따르지 않은 경우 시장에서 이용을 금지・제한하거나 철수・회수하기 위한 적절한 임시조치를 시행하고 이를 지체 없이 EU 집행위 등에 통보
○ 적합성 표시 또는 'EU 적합성 선언'이 부착되지 않거나 잘못 부착, 적합성 평가를 한 인증기관의 식별번호 미 부착, 기술문서를 이용할 수 없거나 불완전 등을 확인하는 경우 제조업체에 규정 준수를 요구
- 이 같은 요구에도 불구하고 제조업체가 이를 준수하지 않을 경우 관련 EU 회원국은 해당 제품에 대해 이용을 제한 또는 금지하거나 철수 또는 회수를 위해 조치

### (7) 벌칙(Penalties)

□ 필수 보안 요구사항 및 제조업자 의무 등 위반 시 최대 **1,500만 유로** 또는 **매출액*의 최대 2%** 中 높은 금액의 **과징금** 부과

* 직전 회계연도 전 세계 연간 총 매출액(이하 동일)

○ 인증기관 및 시장감시기관에 **부정확 또는 불완전한 정보**를 **제공**하는 경우, **최대 500만 유로** 또는 **매출액의 최대 1%** 中높은 금액의 **과징금** 부과

□ 과징금 부과시 위반의 **성격 및 중대성,** 유사 위반행위에 대해 타 시장감시기관이 **이미 과징금**을 **부과**했는지 여부, 사업자의 **규모** 및 **시장 점유율** 등을 종합적으로 고려

## 3. 시사점

□ EU집행위원회는 **CRA 제정**을 통해 **디지털제품 보안사고 예방** 및 **이용자**가 이를 **안심**하고 **선택·사용**할 수 있는 **환경 조성**을 **도모**

○ **디지털제품 보안위험 수준별**로 **규제**를 **차등 적용**하며, 최소 보안요구사항, 적합성 평가, 특별단속 등 필요 사항을 **구체적**으로 **규정**

○ 제품 출시 시 기술문서(SBOM 등) 기재 의무화 등 **제3자**로부터 **전이될 수 있는 위험을 사전 차단**하기 위한 방안도 마련

□ **국내 금융분야**도 디지털 전환에 따른 각종 **디지털제품**(금융 S/W)이 지속적으로 **시장에 출시**되고 있으므로,

○ 디지털제품 설계·배포·이용까지의 **全 과정**에서 **보안성**을 **확보**하고, **적정한 시장감시**가 이루어질 수 있도록 **정책마련**도 **고려** 필요

□ 아울러, EU에 **진출한 국내 금융회사 등**의 디지털제품이 **CRA 적용 대상**에 해당될 것으로 보여, **법안 제정 동향***을 면밀히 **모니터링** 할 필요

* CRA 채택 시 2년 이후 시행 예정

○ 필수 보안요구사항 준수 의무 등 **CRA 위반 시 높은 수준의 과징금***이 **부여**됨을 고려

* 최대 1500만 유로(약 70억 원), 전세계 연간 총 매출액의 2% 중 높은 금액

## 별첨 1 법안의 [부록 Ⅰ] - 필수 보안 요구사항

**1. 제품의 속성과 관련된 보안 요구사항**

(1) 제품은 위험에 따라 적절한 수준의 사이버보안을 보장하는 방식으로 설계, 개발, 생산되어야 한다.

(2) 제품은 악용될 수 있는 알려진 취약점 없이 제공되어야 한다.

(3) §10(2)에 따른 위험평가에 기초하여 해당되는 경우 다음의 사항을 따라야 한다.

(a) 제품을 원래 상태로 재설정할 수 있는 기능을 포함하여 보안이 기본으로 설정된 상태로 제공

(b) 인증, 신원 또는 액세스 관리 시스템을 포함하되 이에 국한되지 않는 적절한 제어 메커니즘을 통해 무단접속으로부터 보호

(c) 저장, 전송 또는 기타 처리된 개인 또는 기타 데이터의 기밀성을 보호 (예, 저장 또는 전송 중인 관련 데이터를 최첨단 메커니즘으로 암호화)

(d) 저장, 전송 또는 기타 방식으로 처리된 데이터, 개인 또는 기타 데이터, 명령, 프로그램 및 구성의 무결성을 사용자가 승인하지 않은 조작이나 수정으로부터 보호하고 손상에 대해 보고

(e) 적절하고 관련성이 있으며 제품의 사용 용도와 관련하여 필요한 데이터로 제한되는 개인 또는 기타 데이터만 처리(데이터의 최소화)

(f) 서비스 거부공격에 대한 복원력 및 완화 등 필수기능의 가용성 보호

(g) 다른 장치나 네트워크에서 제공하는 서비스의 가용성에 미치는 부정적 영향 최소화

(h) 외부 인터페이스를 포함한 공격 표면을 제한하도록 설계・개발・생산

(i) 적절한 악용 완화 메커니즘과 기술을 사용하여 사건의 영향을 줄일 수 있도록 설계・개발・생산

(j) 데이터, 서비스 또는 기능에 대한 액세스 또는 수정을 포함하여 관련 내부활동을 기록 및/또는 모니터링하여 보안 관련 정보를 제공

(k) 해당되는 경우, 자동 업데이트 및 사용 가능 업데이트에 대한 사용자 알림을 포함하여 보안 업데이트를 통한 취약점 해결 가능성 확인

**2. 취약점 처리 요구사항**

(1) SBOM 작성 등 제품에 포함된 취약점과 구성요소를 식별 및 문서화

(2) 제품 관련 위험에 대한 보안 업데이트 제공 등 지체 없이 취약점 해결

(3) 제품 보안에 대한 효과적・정기적 테스트 및 검토 실시

(4) 보안 업데이트가 제공되면 취약점에 대한 설명, 사용자가 영향받는 제품을 식별할 수 있는 정보, 취약점의 영향, 심각성, 사용자가 취약점을 해결하는 데 도움이 되는 정보 등에 대한 정보 공개

(5) 협의된 취약점 공개 정책을 수립 및 시행

(6) 제품 및 여기에 포함된 타사의 구성요소의 잠재적 취약점에 대한 정보공유 촉진(취약점을 보고할 수 있는 연락 주소를 제공하는 등의 조치 포함)

(7) 제품에 대한 업데이트를 안전하게 배포하여 악용 가능한 취약점을 적시에 수정 또는 완화할 수 있는 메커니즘 제공

(8) 확인된 보안 문제를 해결하기 위해 보안패치 또는 업데이트를 사용할 수 있는 경우, 사용자에게 취해야 할 잠재적 조치를 포함한 관련 정보를 제공하는 권고 메시지와 함께 지체 없이 무료로 배포

## 별첨 2 법안의 [부록 II] – 사용자에게 제공되는 정보 및 안내

제품에는 최소한 다음의 사항이 함께 제공되어야 한다.

1. 제조업체의 이름, 등록 상호나 상표, 제조업체에 연락할 수 있는 주소 및 이메일 주소를 제품에 표시(표시할 수 없는 경우 포장 또는 동봉된 문서에 표시)
2. 제품의 취약점에 대한 정보를 신고하고 접수할 수 있는 연락창구
3. 제품, 관련 지침 및 사용자 정보를 식별할 수 있는 유형(type), 배치(batch), 버전 또는 일련번호의 정확한 식별자 또는 다른 요소
4. 제조업체가 제공하는 보안환경, 제품의 필수기능 및 보안속성에 대한 정보 등 사용 용도에 대한 설명
5. 제품을 사용 용도나 합리적으로 예측가능한 오용*되는 것과 관련해 중대한 위험을 초래할 수 있다고 알려진 또는 예측가능한 모든 상황
   * 제품을 사용 용도에 맞지 않는 방식으로 사용하는 것을 의미. 이는 합리적으로 예측가능한 인간의 행동이나 다른 시스템과의 상호 작용으로 인해 발생할 수 있음(§3(26) 참고)
6. SBOM에 대한 접근 여부 및 위치 (해당하는 경우)
7. EU 적합성 선언에 접근할 수 있는 인터넷 주소 (해당하는 경우)
8. 제조업체가 제공하는 기술보안 지원의 유형과 언제까지 제공되는지, 최소한 사용자가 보안 업데이트를 받을 수 있는 시기
9. 다음의 사항에 대한 자세한 안내 또는 해당 안내・정보를 참조할 수 있는 인터넷 주소
   (a) 초기 시운전 중이거나 제품 수명기간동안 안전한 사용을 보장하기 위해 필요한 조치
   (b) 제품 변경이 데이터 보안에 미칠 수 있는 영향
   (c) 보안 업데이트 설치 방법
   (d) 사용자 데이터의 안전한 삭제를 포함한 제품의 안전한 폐기

## 별첨 3 법안의 [부록 Ⅲ] - 디지털 요소가 포함된 중요 제품

### 클래스 Ⅰ

1. ID 관리 시스템 소프트웨어 및 권한 있는 액세스 관리 소프트웨어
2. 독립형 및 임베디드 브라우저
3. 비밀번호 관리자
4. 악성 소프트웨어를 검색, 제거 또는 격리하는 소프트웨어
5. 가상사설망(VPN) 기능이 있는 제품
6. 네트워크 관리 시스템
7. 네트워크 구성 관리도구
8. 네트워크 트래픽 모니터링 시스템
9. 네트워크 리소스 관리
10. 보안 정보 및 이벤트 관리(SIEM) 시스템
11. 부팅 관리자를 포함한 업데이트/패치 관리
12. 애플리케이션 구성 관리 시스템
13. 원격 액세스/공유 소프트웨어
14. 모바일 장치 관리 소프트웨어
15. 물리적 네트워크 인터페이스
16. 클래스 Ⅱ에 포함되지 않는 운영체제
17. 클래스 Ⅱ에 포함되지 않는 방화벽, 침입 탐지 및/또는 방지 시스템
18. 클래스 Ⅱ에 포함되지 않는 라우터, 인터넷 연결용 모뎀 및 스위치
19. 클래스 Ⅱ에 포함되지 않는 마이크로 프로세서
20. 마이크로 컨트롤러
21. 「NIS 2 지침」의 [부록 Ⅰ]에 따른 필수 기관이 사용하기 위한 애플리케이션 특정 집적회로(ASIC) 및 현장 프로그래밍 가능 게이트 어레이(FPGA)
22. 프로그래밍 가능 논리 제어기(PLC), 분산 제어 시스템(DCS), 수치 제어 공작 기계(CNC), 원격감시 제어 시스템(SCADA) 등 클래스 Ⅱ에 포함되지 않는 산업 자동화 및 제어 시스템(IACS)
23. 클래스 Ⅱ에 포함되지 않는 산업용 사물인터넷(IoT)

### 클래스 Ⅱ

1. 서버, 데스크톱 및 모바일 장치용 운영체제
2. 운영체제 및 이와 유사 환경의 가상화된 실행을 지원하는 하이퍼 바이저 및 컨테이너 런타임 시스템
3. 공개키 인프라 및 디지털 인증서 발급자
4. 산업용 방화벽, 침입 탐지 및/또는 방지 시스템
5. 범용 마이크로프로세서
6. PLC 및 보안 요소에 통합하기 위한 마이크로 프로세서

7. 라우터, 인터넷 연결용 모뎀 및 산업용 스위치
8. 보안 요소
9. 하드웨어 보안 모듈(HSM)
10. 안전한 암호화 프로세서
11. 스마트카드, 스마트카드 리더 및 토큰
12. PLC, DCS, CNC, SCADA 등 「NIS 2 지침」 [부록 Ⅰ]의 필수기관이 사용하도록 설계된 IACS
13. 「NIS 2 지침」의 [부록 Ⅰ]에 따른 필수기관이 사용하기 위한 산업용 IoT
14. 로봇 감지 및 액추에이터 구성요소와 로봇 컨트롤러
15. 스마트 계량기

## 별첨 4 법안의 [부록 Ⅳ] – EU 적합성 선언

EU 적합성 선언에는 다음의 정보를 모두 포함시켜야 한다.

1. 제품을 식별할 수 있도록 하는 이름 및 유형, 추가정보
2. 제조업체 또는 그의 권한을 위임받은 대리인의 이름과 주소
3. EU 적합성 선언이 공급자의 전적인 책임 하에 발행되었다는 진술서
4. 선언의 목적물(추적 가능한 제품 식별정보. 필요한 경우 사진 포함 가능)
5. 선언의 목적물이 EU 조화에 관한 법률을 준수한다는 진술서
6. 사용된 통일규격 또는 적합성이 선언된 기타 공통사양 또는 사이버보안 인증에 대한 참조
7. 해당되는 경우, 인증기관*의 이름과 번호, 적합성 평가절차에 대한 설명, 발급된 인증서의 식별정보
   * §33 및 기타 관련 EU 조화에 관한 법률에 따라 지정된 적합성 평가기관을 말함
8. 추가 정보 :

서명 및 대리인 .....

(발행 장소 및 날짜)

(이름, 부서) (서명)

## 별첨 5 법안의 [부록 V] – 기술문서의 내용

§23에 따른 기술문서에는 최소한 다음의 정보가 포함되어야 한다.

1. 다음의 사항을 포함한 제품에 대한 일반적인 설명
   (a) 사용 용도
   (b) 필수 요구사항 준수에 영향을 미치는 소프트웨어 버전
   (c) 하드웨어 제품인 경우 외부 특징, 표시 및 내부 레이아웃을 보여주는 사진 또는 일러스트레이션
   (d) [부록 II]에 명시된 사용자에게 제공되는 정보 및 지침
2. 다음의 사항을 포함한 제품의 설계, 개발, 생산 및 취약점 처리 프로세스에 대한 설명
   (a) 제품의 설계・개발에 대한 완전한 정보 (해당되는 경우 도면 및 설계도 및/또는 소프트웨어 구성요소가 서로를 기반으로 구축되거나 공급되고 전체 프로세스에 통합되는 방식을 설명하는 시스템 아키텍처 설명 포함)
   (b) SBOM, 협의된 취약점 공개 정책, 취약점 보고를 위한 연락 주소 제공, 업데이트의 안전한 배포를 위해 선택한 기술 솔루션에 대한 설명을 포함하여 제조업체가 마련한 취약점 처리 프로세스에 대한 완전한 정보 및 사양
   (c) 제품의 생산 및 모니터링 프로세스에 대한 완전한 정보와 사양, 이러한 프로세스의 검증에 대한 제공
3. 제품이 설계・개발・생산・제공・유지관리 단계에서의 사이버보안 위험 평가(§10)
4. 유럽연합 관보에 전체 또는 일부가 적용된 통일규격의 목록, §19에 따른 공통사양 또는 「Regulation 2019/881」에 따른 사이버보안 인증제. 통일규격, 공통사양, 사이버보안 인증제가 적용되지 않은 경우 기타 관련 기술사양 목록을 포함하여 [부록 I]의 section 1・2에 따른 필수 요구사항을 충족하기 위해 채택된 솔루션에 대한 설명.
   통일규격, 공통사양, 사이버보안 인증제가 부분적으로 적용된 경우, 기술문서에는 적용된 부분을 명시.
5. [부록 II]의 section 1・2에 따른 필수 요구사항에 대한 제품 및 취약점 처리 프로세스의 적합성을 확인하기 위해 수행한 테스트 보고서
6. EU 적합성 선언 사본
7. 해당되는 경우, §3(37)에 따른 SBOM (시장감시당국이 [부록 I]에 따른 필수 요구사항의 준수 여부를 확인할 수 있도록 하기 위해 필요한 경우 시장감시당국의 합리적인 요청에 따른 추가 제공)

## 별첨 6 법안의 [부록 VI] – 적합성 평가절차

**내부통제에 기반한 적합성 평가절차 (모듈 A 기준)**

1. 내부통제는 제조업체가 2・3・4번의 의무를 이행하고 제품이 [부록 I ]의 section 1에 따른 모든 필수 요구사항을 충족하고, 제조업체가 [부록 I ]의 section 2에 따른 필수 요구사항을 충족함을 단독 책임으로 보장하고 선언하는 적합성 평가절차이다.

2. 제조업체는 [부록 V]에 설명된 기술문서를 작성해야 한다.

3. 제품의 설계, 개발, 생산 및 취약점 처리
   제조업체는 설계, 개발, 생산 및 취약점 처리 프로세스와 그 모니터링을 통해 제조 또는 개발된 제품의 디지털 요소와 제조업체가 시행하는 프로세스가 [부록 I ]의 section 1・2에 따른 필수 요구사항을 준수하도록 필요한 모든 조치를 취해야 한다.

4. 적합성 표시 및 적합성 선언
   4.1. 제조업체는 본 규정의 관련 요건을 충족하는 각 개별 제품에 CE를 부착해야 한다.
   4.2. 제조업체는 제20조에 따라 각 제품에 대해 EU 적합성 선언을 작성(서면)하고 제품이 출시된 후 10년간 기술문서와 함께 국가당국이 권한 하에 처리할 수 있도록 보관해야 한다. EU 적합성 선언에는 해당 선언이 작성된 제품이 식별돼야 한다. 선언의 사본은 요청 시 관련 당국에 제공돼야 한다.

5. 수권대리인
   4번에 따른 제조업체의 의무가 위임장에 명시된 경우, 제조업체를 대신하여 제조업체의 책임 하에 제조업체의 권한을 위임받은 대리인이 이행할 수 있다.

**EU-type 심사 (모듈 B 기준)**

1. EU-type 심사는 인증기관이 제품의 기술 설계・개발과 제조업체가 시행하는 취약점 처리 프로세스를 검토하여 제품이 [부록 Ⅰ]에 따른 필수 요구사항을 충족하고 제조업체가 [부록 Ⅱ]에 따른 필수 요구사항을 충족한다는 것을 증명하는 적합성 평가절차의 일부이다.

2. EU-type 심사는 3번에 따른 기술문서 및 증빙자료를 검토하여 제품의 기술 설계・개발의 적절성을 평가하고, 제품의 하나 이상의 중요 부분(생산 유형과 설계 유형의 조합)에 대한 표본을 검사하는 방식으로 진행한다.

3. 제조업체는 자신이 선택한 단일 인증기관에 EU-type 심사 신청서를 제출해야 한다.
   신청서에는 다음이 포함돼야 한다.
   - 제조업체의 이름과 주소 (권한 있는 대리인이 신청서를 제출한 경우 대리인의 이름과 주소도 함께 기재)
   - 다른 인증기관에 동일한 신청서를 제출한 적이 없다는 서면 신고서
   - 기술문서는 [부록 I ]에 따른 필수 요구사항 및 [부록 II ]에 따른 제조업체의 취약점 처리 프로세스에 대한 제품의 적합성을 평가할 수 있어야 하며, 위험에 대한 적절한 분석 및 평가가

포함되어야 한다. 기술문서에는 해당 요구사항을 명시하고 평가와 관련된 한 제품의 설계, 제조 및 작동을 다루어야 한다. 기술문서에는 해당되는 경우 최소한 [부록 V]에 따른 요소가 포함돼야 한다.

- 기술 설계・개발 솔루션과 취약점 처리 프로세스의 적절성을 뒷받침하는 증거. 이 증빙 증거에는 특히 관련 통일규격 및/또는 기술사양이 완전히 적용되지 않은 경우 사용된 모든 문서가 기재돼야 한다. 증빙자료에는 필요한 경우 제조업체의 해당 실험실 또는 제조업체를 대신하여 그의 책임 하에 다른 테스트 실험실에서 수행한 테스트 결과가 포함되어야 한다.

4. 인증기관은 다음과 같이 해야 한다.
   4.1. 기술문서 및 증빙자료를 검토하여 [부록 I ]의 section 1에 따른 필수 요구사항을 갖춘 제품의 기술 설계・개발과 [부록 I ]의 section 2에 따른 필수 요구사항을 갖춘 제조업체가 마련한 취약점 처리 프로세스의 적절성을 평가해야 한다.
   4.2. 표본이 기술문서에 따라 개발이나 제조됐는지 확인하고, 관련 통일규격 및/또는 기술사양의 해당 조항에 따라 설계・개발된 요소와 해당 표준의 관련 조항을 적용하지 않고 설계・개발된 요소를 식별해야 한다.
   4.3. 제조업체가 [부록 I ]에 따른 요구사항에 대해 관련 통일규격 및/또는 기술사양의 솔루션을 적용하기로 선택한 경우, 해당 솔루션이 올바르게 적용됐는지 확인하기 위해 적절한 시험 및 테스트를 수행하거나 수행하도록 한다.
   4.4. [부록 I ]에 따른 요구사항에 대한 관련 통일규격 및/또는 기술사양의 솔루션이 적용되지 않은 경우 제조업체가 채택한 솔루션이 해당 필수 요구사항을 충족하는지 확인하기 위해 적절한 시험 및 테스트를 수행하거나 수행하도록 해야 한다.
   4.5. 시험 및 테스트가 수행될 장소에 대해 제조업체와 합의한다.

5. 인증기관은 4번에 따라 수행한 활동과 그 결과를 기록하는 평가보고서를 작성해야 한다. 인증기관은 인정당국에 대한 의무를 침해하지 않는 범위 내에서 제조업체의 동의가 있는 경우에만 해당 보고서의 내용 전부 또는 일부를 공개해야 한다.

6. 유형 및 취약점 처리 프로세스가 [부록 I ]에 따른 필수 요구사항을 충족하는 경우, 인증기관은 제조업체에 EU-type 심사 인증서를 발급해야 한다. 인증서에는 제조업체의 이름과 주소, 심사결론, 유효성 조건(있는 경우), 승인된 유형 및 취약점 처리 프로세스를 식별하는 데 필요한 데이터가 포함돼야 한다. 인증서에는 하나 이상의 부속서가 첨부될 수 있다.

   인증서와 부속서에는 제조 또는 개발된 제품이 검사대상 유형 및 취약점 처리 프로세스에 적합한지 평가하고 서비스 中 통제가 가능하도록 모든 관련 정보가 포함되어야 한다.

   유형 및 취약점 처리 프로세스가 [부록 I ]에 따른 필수 요구사항을 충족하지 않는 경우, 인증기관은 EU-type 심사 인증서 발급을 거부하고 신청자에게 거부 사유를 자세히 명시하여 통보해야 한다.

7. 인증기관은 승인된 유형 및 취약점 처리 프로세스가 [부록 I ]에 따른 필수 요구사항을 더 이상 준수하지 않을 수 있음을 나타내는 일반적으로 인정된 기술 상태의 변경 사항을 파악하고, 그러한 변경 사항에 대한 추가 조사가 필요한지 여부를 결정해야 한다. 만일 필요하다면 인증기관은 제조업체에 이를 알려야 한다.

   제조업체는 승인된 유형에 대한 모든 수정사항과 [부록 I ]에 따른 필수 요구사항 또는 인증서의

유효성 조건 준수에 영향을 미칠 수 있는 취약점 처리 프로세스를 EU-type 심사 인증서와 관련된 기술문서를 보유한 인증기관에 알려야 한다. 이러한 수정은 원래의 EU-type 심사 인증서에 추가하는 형태로 승인을 받아야 한다.

8. 각 인증기관은 발급 또는 철회한 EU-type 심사 인증서 및/또는 이에 대한 추가 사항에 대해 해당 인정당국에 통보해야 하며, 주기적으로 또는 요청 시 거부, 정지 또는 기타 방식으로 제한되는 인증서 및/또는 이에 대한 추가 사항의 목록을 해당 인정당국에 제공해야 한다.

   각 인증기관은 거부, 철회, 중단 또는 기타 방식으로 제한한 EU-type 심사 인증서 및/또는 이에 대한 추가 사항과 요청이 있는 경우 발급한 인증서 및/또는 이에 대한 추가사항에 대해 다른 인증기관에 알려야 한다.

   집행위원회, 회원국 및 기타 인증기관은 요청 시 EU-type 심사 인증서 및/또는 이에 대한 추가 사본을 입수할 수 있다. 요청이 있는 경우, 집행위원회와 회원국은 인증기관이 수행한 기술문서와 심사결과 사본을 받을 수 있다. 인증기관은 인증서의 유효기간이 만료될 때까지 EU-type 심사 인증서 사본, 부속서 및 추가 사항, 제조업체가 제출한 문서를 포함한 기술 파일을 보관해야 한다.

9. 제조업체는 제품이 시장에 출시된 후 10년간 국가당국이 권한 하에 처리할 수 있도록 기술문서와 함께 EU-type 심사 인증서, 부속서 및 추가 사항의 사본을 보관해야 한다.

10. 제조업체의 수권대리인은 위임장에 명시된 경우 3번에 따른 신청서를 제출하고 7번 및 9번 항목에 따른 의무를 이행할 수 있다.

**내부 생산통제를 기반으로 하는 유형에 대한 적합성(모듈 C 기준)**

1. 내부 생산통제에 기반으로 하는 유형에 대한 적합성은 제조업체가 2・3번 항목에 따른 의무를 이행하고 해당 제품이 EU-type 심사 인증서에 기술된 형식에 적합하며 [부록 I ]의 section 1에 따른 필수 요구사항을 충족함을 보장하고 선언하는 적합성 평가절차의 일부이다.

2. 생산

   2.1. 제조업체는 생산 및 그 모니터링을 통해 제조된 제품이 EU-type 심사 인증서에 기재된 승인된 유형 및 [부록 I ]의 section 1에 따른 필수 요구사항을 준수하도록 필요한 모든 조치를 취해야 한다.

3. 적합성 표시 및 적합성 선언

   3.1. 제조업체는 EU-type 심사 인증서에 설명된 유형에 부합하고 법령의 해당 요건을 충족하는 각 개별 제품에 CE 마크를 부착해야 한다.

   3.2. 제조업체는 제품 모델에 대한 적합성 선언(서면)을 작성하여 제품이 시장에 출시된 후 10년간 국가당국이 권한 하에 처리할 수 있도록 보관해야 한다. 적합성 선언에는 해당 선언이 작성된 제품 모델이 명시되어야 한다. 적합성 선언의 사본은 요청 시 관련 당국에 제공되어야 한다.

4. 수권대리인

   3번에 따른 제조업체의 의무가 위임장에 명시된 경우, 제조업체를 대신하여 제조업체의 책임 하에 제조업체의 권한을 위임받은 대리인이 이행할 수 있다.

**전체 품질 보증에 기반한 적합성(모듈 H 기준)**

1. 전체 품질 보증에 기반한 적합성은 제조업체가 2・5번에 따른 의무를 이행하고, 해당 제품(또는 제품 카테고리)이 [부록 I ]에 따른 필수 요구사항을 충족하며, 제조 업체가 시행하는 취약점 처리 프로세스가 [부록 II ]에 따른 요구사항을 충족함을 자신의 단독 책임으로 보장하고 선언하는 적합성 평가절차이다.

2. 제품의 설계, 개발, 생산 및 취약점 처리

   제조업체는 해당 제품의 설계, 개발 및 생산과 취약점 처리를 위해 3번에 따라 승인된 품질 시스템을 운영하고, 해당 제품의 수명주기동안 그 효과를 유지해야 하며, 4번에 따라 감시받아야 한다.

3. 품질 시스템

   3.1. 제조업체는 해당 제품에 대해 자신이 선택한 인증기관에 품질 시스템 평가 신청서를 제출해야 한다.

   신청서에는 다음의 사항을 포함해야 한다.

   - 제조업체의 이름과 주소 (권한 있는 대리인이 신청서를 제출한 경우 대리인의 이름과 주소도 함께 기재)
   - 제조 또는 개발하려는 각 제품 카테고리의 한 모델에 대한 기술문서 (기술문서에는 해당되는 경우 [부록 V]에 따른 최소한의 요소가 포함되어야 한다.
   - 품질 시스템에 관한 문서
   - 다른 인증기관에 동일한 신청서를 제출한 적이 없다는 서면 신고서

   3.2. 품질 시스템은 제품이 [부록 I ]의 section 1에 따른 필수 요구사항을 준수하고 제조업체가 시행하는 취약점 처리 프로세스가 [부록 I ]의 section 2에 따른 요구사항을 준수하도록 보장해야 한다.

   제조업체가 채택한 모든 요소, 요구사항 및 조항은 서면 정책, 절차 및 지침의 형태로 체계적이고 질서정연하게 문서화되어야 한다. 품질 시스템 문서는 품질 프로그램, 계획, 매뉴얼 및 기록에 대한 일관되게 해석될 수 있어야 한다.

   특히 다음의 사항에 대한 적절한 설명이 포함되어야 한다.

   - 설계, 개발, 제품 품질 및 취약점 처리와 관련된 품질 목표와 경영진의 조직 구조, 책임 및 권한에 대한 설명
   - 적용될 표준을 포함한 기술 설계・개발 사양, 관련 통일규격 및/또는 기술사양이 완전히 적용되지 않는 경우, 제품에 적용되는 [부록 I ]의 section 1에 따른 필수 요구사항을 충족하기 위해 사용될 수단
   - 적용될 표준을 포함한 절차적 사양 및 관련 통일규격 및/또는 기술사양이 완전히 적용되지 않는 경우, 제조업체에 적용되는 [부록 I ]의 section 2에 따른 필수 요구사항이 충족되도록 보장하는 데 사용될 수단
   - 해당 제품 카테고리와 관련된 제품을 설계・개발할 때 사용할 설계・계발 관리뿐만 아니라 그 검증 기술, 프로세스 및 체계적인 조치에 대한 설명
   - 해당 생산, 품질관리 및 품질보증 기술, 프로세스 및 체계적 조치에 대한 설명

- 생산 前부터 後까지 수행될 심사・ 테스트와 그 실시 빈도
- 심사 보고서 및 테스트 데이터, 교정 데이터, 관련 인력에 대한 자격보고서 등의 품질 기록
- 필요한 설계 및 제품품질 달성 여부와 품질 시스템의 효과적 운영을 모니터링하는 수단

3.3. 인증기관은 품질 시스템을 평가하여 3.2.번에 따른 요구사항의 충족 여부를 결정해야 한다.

관련 통일규격 및/또는 기술사양을 구현하는 국가 표준의 해당 사양을 준수하는 품질 시스템의 요소와 관련하여 해당 요구사항을 준수하는 것으로 추정한다.

심사팀에는 품질관리 시스템에 대한 경험 외에도 관련 제품 분야 및 제품 기술에 대한 평가자로서의 경험과 본 규정의 해당 요건에 대한 지식이 있는 구성원이 한 명 이상 포함되어야 한다. 심사에는 제조업체의 사업장이 있는 경우 해당 사업장에 대한 방문 평가가 포함되어야 한다. 심사팀은 3.1.번에 따른 기술문서를 검토하여 제조업체가 본 규정의 해당 요건을 파악할 수 있는지 확인하고 제품이 해당 요건을 준수하는지 확인하기 위해 필요한 검사를 수행해야 한다.

제조업체 또는 그의 권한을 위임받은 대리인에게 결정이 통보된다.

통보에는 감사 결과와 합리적인 평가결정이 포함되어야 한다.

3.4. 제조업체는 승인된 품질 시스템에서 발생하는 의무를 이행하고 적절하고 효율적으로 유지될 수 있도록 이를 유지해야 한다.

3.5. 제조업체는 품질 시스템을 승인한 인증기관에 품질 시스템에 대한 의도된 변경사항을 알려야 한다.

인증기관은 제안된 변경사항을 평가하고 변경된 품질 시스템이 3.2.번에 따른 요건을 계속 충족하는지 또는 재평가가 필요한지 여부를 결정해야 한다.

인증기관은 그 결정을 제조업체에 통보해야 한다. 통보에는 심사 결론과 합리적인 평가결정이 포함되어야 한다.

4. 인증기관의 책임있는 감시

4.1. 감시의 목적은 제조업체가 승인된 품질 시스템에서 발생하는 의무를 적법하게 이행하는지를 확인하는 것이다.

4.2. 제조업체는 평가 목적으로 인증기관이 설계, 개발, 생산, 검사, 테스트 및 보관 현장에 접근할 수 있도록 허용해야 하며, 특히 필요한 정보를 제공해야 한다.

- 품질 시스템 문서
- 분석, 계산, 테스트 등의 결과와 같이 품질 시스템의 설계 부분에서 제공하는 품질 기록
- 검사보고서 및 테스트 데이터, 교정 데이터, 관련 인력에 대한 자격보고서 등 품질 시스템의 제조 부분에서 제공하는 품질 기록

4.3. 인증기관은 제조업체가 품질 시스템을 유지・적용하고 있는지 확인하기 위해 주기적으로 감사를 실시해야 하며, 제조업체에 감사보고서를 제공해야 한다.

5. 적합성 표시 및 적합성 선언

5.1. 제조업체는 CE 마크를 부착하여야 하고, 3.1.번에 따른 인증기관의 책임 하에 [부록 I ]에 따른 요구사항을 충족하는 각 개별 제품에 후자의 식별번호를 부착해야 한다.

5.2. 제조업체는 각 제품 모델에 대한 적합성 선언을 서면으로 작성하여 제품이 출시된 후 10년간 국가당국이 권한 하에 처리할 수 있도록 보관해야 한다. 적합성 선언에는 해당 선언이 작성된 제품 모델이 표시되어야 한다.

요청 시 적합성 선언 사본을 관련 당국에 제공해야 한다.

6. 제조업체는 제품이 시장에 출시된 후 최소 10년이 되는 기간동안 다음의 사항이 국가당국의 권한 하에 처리될 수 있도록 보관해야 한다.
   - 3.1.번에 따른 기술문서
   - 3.1.번에 따른 품질 시스템에 관한 문서
   - 승인된 것으로서 3.5.번에 따른 변경사항
   - 3.5.번, 4.3.번 및 4.4.번에 따른 인증기관의 결정 및 보고서

7. 각 인증기관은 발급 또는 철회된 품질 시스템 승인에 대해 해당 인증기관에 통보해야 하며, 주기적으로 또는 요청 시 품질 시스템 승인이 거부, 정지 또는 기타 방식으로 제한되는 목록을 해당 인증기관에 제공해야 한다.
   각 인증기관은 거부, 중단 또는 철회한 품질 시스템 승인과 요청이 있는 경우 발급한 품질 시스템 승인에 대해 다른 인증기관에 알려야 한다.

8. 수권대리인
   3.1.번, 3.5.번, 5번 및 6번에 따른 제조업체의 의무는 위임장에 명시된 경우 제조업체를 대신하여 제조업체의 책임 하에 제조업체의 권한을 위임받은 대리인이 이행할 수 있다.

법·정책

# 베트남 개인정보보호 관련 시행령 주요 내용 검토[주)]

## 1. 개요

□ **베트남 사이버보안법*** **하위지침**으로 아래의 **개인정보보호 관련 규제 2건**이 **최근 제정·발효**

* 베트남의 사이버보안 및 개인정보보호를 다룬 법('18.6월 제정)

[최근 제정·발효된 베트남 개인정보보호 관련 규제]

| 규정명 | 규정 내용 |
|---|---|
| 개인정보보호 시행령 13 (Decree 13) | 개인정보에 대한 기본 내용을 담은 베트남 최초의 포괄적 개인정보보호 규제('23.7월 발효) |
| 사이버보안법 시행령 53 (Decree 53) | 사이버보안법 中 개인정보 데이터 현지화 등에 대한 사항을 구체적으로 정의한 규제('22.10월 발효) |

□ 베트남 진출(또는 진출 예정)한 **사원기관의 컴플라이언스 지원**을 위해 개인정보보호 관련 **규제 세부 내용**을 **검토**하여 **안내**

[참고] 국내 금융회사의 해외점포 현황

| 순위 | '23.3월 기준 | '20.3월 기준 |
|---|---|---|
| 1 | **베트남**(58개사), 중국(58개사) | 중국(60개사) |
| 2 | 미국(55개사) | **베트남**(54개사) |
| 3 | 인도네시아(32개사) | 미국(52개사) |

출처 : 금융중심지 지원센터

주) 이명영, 금융보안원 보안연구부 책임

## 2. 개인정보보호 시행령(Decree 13) 주요 내용

### 가. 개요

□ **(적용 대상)** 베트남 기관 및 개인*, **베트남에 진출**한 **외국기관 및 외국인**, 베트남 **개인정보 처리에 직접 참여 또는 관련**된 **외국기관 및 외국인 → 베트남 진출 국내 금융회사**도 포함

* 해외에서 활동하는 베트남 기관 및 개인도 해당

□ **(주요 내용)** 개인정보 및 민감정보 정의, 정보주체의 권리(동의, 삭제 등), 개인정보 영향평가, 개인정보 국외 이전 등이 포함

[개인정보보호 시행령 목차]

**제1장** 총칙
**제2장** 개인정보보호업무
　　**1절** 정보주체의 권리와 의무
　　**2절** 개인정보처리 시 개인정보 보호
　　**3절** 개인정보의 영향평가 및 해외이전
　　**4절** 개인정보 보호를 위한 조치 및 조건
**제3장** 기관, 조직, 개인의 책임
**제4장** 시행

### 나. 주요 내용

#### [1장] 총칙

□ **(용어 정의)** 개인정보, 정보주체, 개인정보관리자, 제3자, 개인정보 국외 이전 등에 대해 용어 정의

○ **국내 개인정보보호법**과 용어 정의가 **유사**하나, 개인정보에 **사이버공간 활동 이력** 및 **디지털 계정**을 **포함**하는 점이 특징

[개인정보보호 시행령 內 용어 정의 세부 내용]

| 용어 구분 | 용어 내용 |
|---|---|
| 1) 개인정보 | ○ 특정 개인에 관한 정보, 특정 개인을 알아볼 수 있는 기호·문자·숫자·이미지·음성 또는 이와 유사한 전자정보<br>○ 개인정보는 **기본 개인정보***와 **민감 개인정보****로 구분<br>* 이름, 성별, 거주지, 국적, 사진, 전화번호, 주민등록번호, 여권번호, 가족관계, **사이버공간 활동 이력, 디지털 계정**, 특정인 알아볼 수 있는 기타 정보 등<br>** 사생활과 관련된 개인정보로서 위반시 개인의 정당한 권리와 이익에 직접 영향을 미치는 정보(정치, 종교, 의료, 인종, 민족, 유전적·생물학적 특성, 성생활, 범죄, **계좌정보, 예금정보, 위치정보**) |
| 2) 특정 개인정보 | ○ 개인의 활동으로 형성된 정보로서 다른 저장된 정보과 결합하여 특정 개인을 알아볼 수 있는 정보 |
| 3) 정보주체 | ○ 개인정보에 반영된 개인 |
| 4) 개인정보처리 | ○ 개인정보에 영향을 미치는 행위로 개인정보 수집·기록·분석·저장·편집·결합·접근·암호화·이전·삭제·파기 또는 관련 행위 |
| 5) 개인정보관리자 | ○ 개인정보 처리 목적 및 처리 수단을 결정하는 조직 또는 개인 |
| 6) 개인정보처리자 | ○ 개인정보관리자와의 계약 또는 협의를 통해 개인정보관리자를 대신하여 정보처리 수행하는 조직 또는 개인 |
| 7) 개인정보처리 관리자 | ○ 개인정보 처리에 있어 처리 목적 및 처리 수단을 결정하고 개인정보를 직접 처리하는 조직 또는 개인 |
| 8) 제3자 | ○ 정보주체, 개인정보관리자, 개인정보처리관리자 外 개인정보 처리 조직 또는 개인 |
| 9) 개인정보 국외 이전 | ○ 사이버공간, 전자적 장비·수단 또는 기타 형태를 이용하여 베트남 국민의 개인정보를 베트남 영토 밖으로 이전하거나, 베트남 영토 밖의 장소를 이용하여 베트남 국민의 개인정보를 처리하는 행위<br>- 조직, 기업 및 개인이 정보주체 동의 목적에 따라 베트남 국민의 개인정보를 해외 조직, 기업, 관리부서로 이전<br>- 개인정보관리자, 개인정보처리자 및 개인정보처리관리자가 베트남 영토 외부에 설치된 자동시스템을 이용하여 정보주제 동의 목적에 따라 베트남 국민 개인정보 처리 |

□ (**개인정보 보호 원칙**) 별도 규정이 없는 경우 **개인정보 매매 금지**, 개인정보의 기술적 조치에 의한 훼손방지 등 **개인정보 보호의무 이행** 등

□ (**규정 위반행위 처리**) **규정을 위반**한 기관, 조직 및 개인은 위반 정도에 따라 관계법령에 의한 **징계, 행정처분 또는 형사처벌** 가능

□ **(개인정보보호 관리)** 개인정보보호 관리는 **베트남 정부**가 **총괄**

□ **(금지 행위)** 베트남에 **대항하는 정보의 생성**이나 **국가 안보, 행정기관 업무방해** 등을 금지 행위로 명시

[국내 개인정보보호법과 비교(금지 행위)]

| 구분 | 베트남 | 한국 |
|---|---|---|
| 금지 행위 | 베트남에 대항하는 정보 생성 행위, 국가안보 및 치안, 기타 조직 및 개인 권익 영향 미치는 행위, 관할기관 개인정보보호 업무 방해 행위 | 거짓이나 그밖의 부정한 수단·방법으로 개인정보 취득·동의 받는 행위, 업무상 알게 된 개인정보를 누설하거나 권한 없는 타인에게 제공하는 행위, 정당한 권한없이 타인 개인정보 이용, 훼손 멸실, 변경, 위조, 유출 행위 |

## [2장] 개인정보보호 업무

□ **(정보주체 권리)** 개인정보 처리에 대한 정보주체의 동의 및 반대 권리 등을 보장하고 있으며, 정보주체 요구 시 **72시간 이내에 처리**

[국내 개인정보보호법과 비교(정보주체 권리)]

| 구분 | 베트남 | 한국 |
|---|---|---|
| 정보주체 권리 | 정보를 제공받을 권리 | (좌동) |
| | 개인정보 처리 동의 및 동의 철회 결정 권리 | 개인정보 처리 동의 및 동의범위 선택 결정 권리 |
| | 개인정보 열람 및 수정 요구 권리 | 개인정보 열람 및 전송요구권 |
| | 개인정보 삭제 요구 권리 | 개인정보 정지, 정정·삭제 및 파기 요구 권리 |
| | 소송제기권, 손해배상청구권, 자기보호권 | 피해를 구제받을 권리 |
| | 개인정보 처리 반대 권리<br>- 개인정보 공개 또는 광고 목적 사용 방지<br>- 정보주체 요구 시 72시간 이내 조치 | - |
| | - | 완전히 자동화된 개인정보 처리에 따른 결정 거부 또는 설명 요구권 |
| | 개인정보 처리 제한 권리<br>- 정보주체 요구 시 72시간 이내 조치 | 개인정보 처리 정지 권리<br>- 정보주체 요구 시 10일 이내 처리 |

□ **(정보주체 동의)** 개인정보 처리에 대한 동의는 정보주체가 **아래 사항을 숙지**하고 **자발적으로 동의**한 경우에 한해 유효

[개인정보 처리 동의 시 정보주체 숙지 필요사항]

| | |
|---|---|
| ㅇ 처리해야 할 개인 정보의 유형 | ㅇ 개인정보 처리목적 |
| ㅇ 개인정보를 처리할 수 있는 조직 및 개인 | ㅇ 정보주체의 권리와 의무 |

□ **(정보주체 동의 철회)** 정보주체의 동의 철회 요청 시 **동의 철회에 따른 손해 등을 통보**하고, 동의철회를 **확정**하면 **정보처리를 중단**

※ 동의를 철회하더라도 철회 전에 동의한 정보처리의 적법성은 미 영향

ㅇ 동의 철회는 **전자적 또는 검증가능한 형태**여야 하며, **서면**으로 **출력·복사**가 가능

[개인정보처리 주체별 동의 철회 의무사항]

| 구분[주] | 세부 내용 |
|---|---|
| 개인정보관리자 | 정보주체로부터 동의철회 요청을 받은 경우, 동의철회시 발생할 수 있는 결과 및 손해 통보 |
| 개인정보관리자, 개인정보처리자 및 제3자 | 정보주체가 동의철회를 확정(동의철회를 서면으로 표현)하면 정보주체의 정보처리를 중지하고 관련 조직 등에게 정보처리 중지 요청 |

주) 개인정보처리관리자는 모든 의무사항 이행 필요

□ **(개인정보 처리 통지)** 개인정보 처리 목적, 방식 등에 대해 개인정보 처리 前 **정보주체**에게 **1회 통지**

[국내 개인정보보호법과 비교(개인정보 처리 통지)]

| 구분 | 베트남 | 한국 |
|---|---|---|
| 통지 주기 | 개인정보 처리 前 1회 | 연1회 이상 주기적으로 개인정보 이용내역 통지 |
| 통지 내용 | ㅇ 개인정보 처리 목적<br>ㅇ 개인정보 처리 목적과 관련하여 사용되는 개인정보 유형<br>ㅇ 개인정보 처리 방식<br>ㅇ 개인정보 처리 목적과 관련된 기타 조직 및 개인에 대한 정보<br>ㅇ 예상치 못한 결과 및 손해<br>ㅇ 개인정보 처리 시작 및 종료 시간 | ㅇ 개인정보 수집·이용 목적 및 수집한 개인정보 항목<br>ㅇ 개인정보를 제공받은 자<br>ㅇ 개인정보 제3자 제공 목적<br>ㅇ 제3자에게 제공한 개인정보 항목 |

□ **(개인정보 제3자 제공)** 개인정보의 **제3자 제공**을 **정보주체**가 **개인정보관리자**에게 **직접 요청**

※ 국내는 개인정보처리자가 정보주체의 동의를 받아 개인정보를 제3자에게 제공

[개인정보 제3자 제공 주요 내용]

| 구분 | 주요 내용 |
|---|---|
| 제공 기한 | ○ 개인정보관리자 또는 개인정보처리관리자는 별도 규정된 경우를 제외하고는 정보주체의 요청 시 **72시간 이내**에 개인정보를 제3자에게 제공 |
| 제공 요청 방법 | ○ 정보주체가 직접 또는 대리인을 통해 개인정보관리자 또는 개인정보처리관리자의 오프라인 지점을 방문하여 개인정보 제공 요청<br>○ 개인정보 제3자 제공을 요청받은 자는 요청자에게 개인정보제공요청서 작성을 안내할 책임 부과<br>○ 작성된 개인정보제공요청서는 메일, 우편, 팩스를 통해 개인정보관리자 또는 개인정보처리관리자에게 전달 |
| 제공 요청 접수 | ○ 개인정보관리자 또는 개인정보처리관리자는 개인정보 제공 요청을 접수하고, 개인정보 제공 절차 및 목록 감시 책임이 부과 |
| 개인정보 제공요청 처리 | ○ 개인정보관리자 또는 개인정보처리관리자는 적합한 개인정보 제공요청을 받은 후 개인정보 제공시기, 장소 및 제공 방법(우편, 팩스 등) 등에 대해 통지하고, 본 시행령에 명시된 절차에 따라 개인정보 제공 |
| 개인정보 제공 요청서 | ○ 아래 내용을 포함하여 베트남어로 작성<br>- 요청자 성명, 거주지 주소, 주민등록번호<br>- 제공 받을 개인정보<br>- 개인정보 제공 방법<br>- 개인정보 제공 요청 사유 및 목적 |
| 개인정보 미제공 사유 | ○ 아래에 해당되는 경우 개인정보관리자는 개인정보 미제공<br>- 국가안보에 손해를 입히는 경우<br>- 타인의 신체·정신적 건강에 영향을 미치는 경우<br>- 정보주체가 개인정보 제공, 위임을 동의하지 않는 경우 |

□ **(개인정보 수정)** 정보주체는 개인정보의 수정이 필요한 경우 **개인정보관리자의 동의**를 받아 이를 열람하고 **직접 수정**

○ 기술적 사유로 정보주체가 개인정보를 **직접 수정하지 못하는 경우** 개인정보관리자에게 **수정을 요청***하고, 개인정보처리자는 개인정보관리자의 동의를 확인 후 **개인정보를 수정**

* 수정이 어려운 경우 72시간 이내에 정보주체에게 관련 사실 통지

[국내 개인정보보호법과 비교(개인정보 수정)]

| 구분 | 베트남 | 한국 |
|---|---|---|
| 정정기한 | 개인정보 수정 요청 시 신속하게 수정해야하며, 수정이 어려운 경우 **72시간 이내**에 정보주체에게 통지 | 개인정보 수정 요청을 받은 날로부터 **10일 이내** 정정 조치 또는 불조치 사항 통지 |
| 정정방법 | ○ 개인정보관리자의 동의를 받아 정보주체가 직접 개인정보를 수정<br>○ 기술적 사유로 정보주체가 직접 수정하지 못할 경우 개인정보관리자에게수정 요청<br>○ 개인정보처리자 및 제3자는 개인정보관리자가 동의하였음을 확인한 경우에 한하여 개인정보 수정 가능 | 정보주체는 개인정보처리자에게 개인정보 수정 요청 |

□ **(개인정보 보관, 삭제 및 파기) 정보주체는** 개인정보를 **직접 삭제**하거나 **개인정보 (처리)관리자**에게 **삭제 요청** 가능

[개인정보 삭제 관련 주요 내용]

| 구분 | 주요 내용 |
|---|---|
| 삭제 조건 | ○ 동의한 수집·목적이 더 이상 필요치 않음을 확인하고 정보삭제 요청시 발생한 손해를 부담하기로 한 경우<br>○ 동의를 철회한 경우<br>○ 정보주체가 정보처리를 반대하며 개인정보관리자가 개인정보 처리 사유가 없는 경우<br>○ 개인정보 동의된 목적에 따라 처리되지 않거나 개인정보처리가 법률 위반한 경우<br>○ 개인정보가 관계법령에 따라 삭제되어야 하는 경우 |
| 삭제 기한 | ○ 개인정보관리자 또는 개인정보처리관리자는 별도 규정된 경우를 제외하고는 정보주체의 요청 시 **72시간 이내**에 개인정보 일체 삭제 |
| 복구불가 삭제조건 | ○ 개인정보관리자, 개인정보처리관리자, 개인정보처리자 및 제3자는 아래의 경우 복구 불가하게 삭제<br>– 개인정보가 부적절한 목적으로 처리된 경우 또는 정보주체 동의한 목적 달성한 경우<br>– 개인정보 저장이 개인정보관리자, 개인정보처리관리자, 개인정보처리자 및 제3자의 운영에 필요하지 않은 경우<br>– 개인정보관리자, 개인정보처리관리자, 개인정보처리자 및 제3자가 해산, 폐업, 파산신고 또는 관계법령에 따라 영업활동 종료한 경우 |

□ **(CCTV 등으로 수집된 개인정보 처리) 공공장소에서 녹음 또는 영상촬영** 시 정보주체에게 관련 사실을 통지

○ 녹음을 금지하는 국내와 달리 베트남은 **국가 안보 및 치안**을 위해 **녹음을 허용**

[국내 개인정보보호법과 비교 (CCTV 등으로 수집된 개인정보 처리)]

| 구분 | 베트남 | 한국 |
|---|---|---|
| 녹음기능 | 사용 가능 | 사용 불가 |
| 조치사항 | 녹음 또는 영상촬영시 정보주체에게 관련 사실 통지 | 정보주체가 영상촬영을 인식하도록 안내판을 설치 |

□ **(아동 개인정보 처리) 만 16세 미만**을 아동으로 분류하며, 아동 개인정보 처리 시 **아동 및 부모(대리인) 동의** 필요

○ 다만, **7세 미만의 아동**인 경우는 **부모(대리인) 동의만**으로도 개인정보 처리 가능

[국내 개인정보보호법과 비교 (아동 개인정보 처리)]

| 구분 | 베트남 | 한국 |
|---|---|---|
| 아동 기준 | 만 16세 미만 | 만 14세 미만 |
| 동의 대상 | 아동 및 부모(대리인) 동의 필요<br>※단, 7세미만 아동은 부모(대리인) 동의만으로도 개인정보 처리 가능 | 아동 및 법정대리인 동의 필요 |

□ **(광고 및 마케팅 관련 개인정보 보호) 제품 광고 및 마케팅 목적**으로 개인정보 처리 시 **정보주체 동의** 필요

○ 다만, 개인정보 처리 동의 시 정보주체가 **광고 내용, 방법 등을 사전 숙지**하고 있음이 전제

□ **(개인정보의 무단 수집, 양도, 매매)** 개인정보처리자 등은 개인정보가 **시스템 등에 의해 무단 수집**되지 않도록 **방지 조치 이행**

○ 정보주체의 동의 없이 **개인정보를 수집·이전·매매**하는 **소프트웨어 설정**이나 **기술적 장치 설치** 등의 행위는 **불법**

□ **(규정 위반행위 통지)** 개인정보관리자는 **개인정보보호 규정 위반행위 발견** 시 **72시간 이내**에 **공안부에 신고**

※ 72시간 초과 시 신고지연사유서를 공안부에 제출

○ **개인정보처리자는** 개인정보보호 **규정 위반행위를 발견**한 경우 **개인정보관리자**에게 신속하게 **통지**

[개인정보처리자의 규정위반 행위 통지 내용]

ㅇ 시간, 장소, 행동, 조직, 해당 개인정보 유형 등을 포함한 개인정보 위반행위 설명
ㅇ 개인정보 보호 부서 및 담당자 연락처
ㅇ 개인정보보호규정 위반행위로 발생할 수 있는 결과 및 손해 설명
ㅇ 개인정보 위반행위로 인한 손해 최소화 및 시정 조치

○ **개인정보관리자는** 개인정보 위반행위 **확인서를 작성**하고 **공안부와 협력**하여 위반행위를 처리

[국내 개인정보보호법과 비교 (규정위반 행위의 신고 기준)]

| 구분 | 베트남 | | 한국 | |
|---|---|---|---|---|
| | 개인정보(처리)관리자 | 개인 | 개인정보처리자 | 개인 |
| 신고 근거 | 개인정보보호 규정 위반 | 개인정보보호 규정 위반, 목적 외 개인정보 처리, 정보주체 권리 미보장 등 | 개인정보 유출 | 개인정보 침해 |
| 신고 대상 | 공안부 사이버보안 및 하이테크범죄예방국 | | 개인정보보호위원회, 한국인터넷진흥원 | |
| 신고 기한 | 72시간 이내 | - | 5일* | - |

* 정보통신 서비스제공자의 경우 24시간 이내

□ **(개인정보 영향평가서)** 개인정보관리자는 **개인정보 처리 개시 시점** 부터 개인정보 **영향평가서를 작성·보관**

○ 영향평가서는 개인정보 처리 후 **60일 이내**에 **공안부에 제출**

[개인정보 영향평가 세부 내용]

○ 개인정보(처리)관리자는 개인정보 처리를 시작한 시점*로부터 개인정보 영향평가서를 작성·보관
* 개인정보처리자는 개인정보관리자와 계약을 이행한 시기를 개인정보 처리 시작 시점으로 적용

○ 개인정보관리자 등은 개인정보 영향평가서를 개인정보 처리한 날로부터 60일 이내에 공안부에 제출

○ 공안부는 제출받은 개인정보 영향평가서를 검토하고, 미흡하다고 판단되는 경우 개인정보처리자 등에게 보완을 요청 (개인정보처리자 등은 보완요청 사항을 반영)

○ 개인정보 영향평가서 내용

| 개인정보관리자·개인정보처리관리자 | 개인정보처리자 |
|---|---|
| ○ 개인정보관리자 및 개인정보처리관리자 신원정보 및 연락처<br>○ 개인정보관리자 및 개인정보처리관리자의 개인정보 보호 담당부서 및 담당자의 성명, 연락처<br>○ 개인정보 처리목적<br>○ 처리할 개인정보의 유형<br>○ 외국조직 및 개인을 포함하여 개인정보를 수신하는 조직 및 개인<br>○ 개인정보 국외이전 사항<br>○ 개인정보 처리시기, 개인정보 삭제 또는 파기 예정시기(해당시)<br>○ 적용되는 개인정보 보호조치<br>○ 개인정보 처리의 이점에 대한 평가, 예상치 못한 결과 및 손해, 동 결과 및 손해 최소화 또는 제거 조치 | ○ 개인정보처리자의 신원정보 및 연락처<br>○ 개인정보처리자의 개인정보처리 담당부서 및 담당자의 성명, 연락처<br>○ 개인정보관리자와의 계약에 따라 처리되는 개인정보의 유형 및 처리업무에 대한 설명<br>○ 개인정보 처리시기, 개인정보 삭제 또는 파기할 예정시기(해당시)<br>○ 개인정보 국외 이전 사항<br>○ 적용되는 개인정보 보호조치<br>○ 예상치 못한 결과 및 손해, 동 결과 및 손해 최소화 또는 제거 조치 |

□ **(개인정보의 국외이전)** 개인정보를 국외로 이전하는 자는 **개인정보국외이전 영향평가서**를 작성하여 **공안부에 제출 및 통지**

[개인정보 국외 이전 세부 내용]

○ 개인정보 국외이전자는 개인정보 처리한 날로부터 60일 이내 공안부에 개인정보 이전 영향평가서를 제출

| 개인정보 국외이전자 | ➜ | 공안부 |
|---|---|---|

* 개인정보 이전 영향평가서 원본 1부를 개인정보 처리일로부터 후 60일 이내 제출

○ 개인정보 이전 완료 후, 정보이전 관련사항 및 담당부서, 담당자 연락처를 공안부에 서면 통지

| 개인정보 국외이전자 | ➜ | 공안부 |
|---|---|---|

* 개인정보 전송 후 정보이전 관련 사항 및 담당 부서, 담당자 연락처 서면 통지

○ 공안부는 개인정보 국외이전 영향평가서 검토 후 미흡하다고 판단되는 경우 개인정보 국외이전자에게 보완을 요청

○ 국외이전자는 공안부의 개인정보 국외이전 영향평가서 보완요청 사항을 반영하여 영향평가서를 수정하여야 하며, 동 평가서 작성기간은 수정 요청일로부터 10일 이내로 제한

○ 공안부는 ①개인정보 보호규정 위반행위 발견, ②베트남 국민 개인정보 유출 및 손실 발생을 제외하고 연 1회 개인정보 국외이전 사항을 점검

○ 공안부는 다음에 해당하는 경우, 개인정보 국외이전자에게 개인정보 국외이전중단을 요구
- 국외이전 개인정보가 베트남의 국가안보 및 이익을 침해하는 활동에 사용된다는 사실을 확인한 경우
- 개인정보 국외이전자가 공안부가 요청한 개인정보 영향평가서 수정 요구를 미이행한 경우
- 베트남 국민의 개인정보 유출 또는 분실이 발생한 경우

○ 개인정보 국외이전 영향평가서 내용
- 베트남 국민 개인정보 국외이전자 및 이를 수신하는 자의 신원정보 및 연락처
- 개인정보 국외이전자의 베트남 국민 개인정보 이전·수령 관련 부서 및 담당자 이름·연락처
- 베트남 국민의 개인정보를 국외로 이전한 후 개인정보처리에 대한 설명 및 해석
- 국외로 이전되는 개인정보 유형에 대한 설명
- 동 시행령의 개인정보 보호규정 준수현황 및 적용되는 개인정보 보호 조치 설명
- 개인정보처리 이점에 대한 평가, 예상치 못한 결과 및 손해, 동 결과 및 손해를 최소화하거나 제거하기 위한 조치
- 정보주체가 요구사항에 대한 피드백 및 이의제기 방법을 숙지하였음을 전제로 정보주체가 국외이전을 동의한다는 사실
- 개인정보처리에 있어 베트남 국민의 개인정보 이전자 및 수령인 간 구속력과 책임을 명시하는 문서(첨부)

□ **(개인정보 보호조치) 개인정보 처리 全 과정**에 대해 관리적, 기술적 **보호조치*** **등의 적용 의무**을 부여

* 관리적 조치, 기술적 조치, 관할 국가관리기관이 취하는 조치, 관할 국가기관이 취한 조사 및 절차, 기타 관계 법령에서 정한 조치

○ 개인정보 中 **민감정보***인 경우에는 기본 개인정보 보호조치 外 담당자 지정 등 **추가적인 보호조치 의무**가 부여

* 사생활 관련 개인정보로서 위반시 개인의 정당한 권리, 이익에 직접 영향을 미치는 정보(정치, 종교, 의료, 인종, 민족, 유전적·생물학적 특성, 성생활, 범죄, 계좌·예금정보, 위치정보)

[일반 개인정보 및 민감정보간 보호조치 의무 비교]

| 일반 개인정보 | 민감정보 |
|---|---|
| ○ 개인정보의 관리적·기술적 보호조치 등 준수<br>○ 개인정보 처리 또는 삭제·파기 전 시스템 및 네트워크 보안 확인 | ○ (좌 동)<br>○ (좌 동)<br>○ 개인정보보호 담당 부서 및 담당자를 지정하고 관련 정보를 개인정보보호 전담기관에 제공<br>○ 민감정보를 처리 사실을 정보주체에 통지<br>※ 관계 법령에 의해 동의없이 처리되는 개인정보나, 공공장소 녹음 및 영상촬영을 통해 수집된 개인정보 등은 예외 |

□ **(기타)** 공안부 산하 **사이버보안 및 하이테크 범죄예방국**을 **개인정보보호 전담기관**으로 지정

○ 개인정보보호에 대한 국가 방침, 개인정보보호 현황, 개인정보 규정위반 행위 통지 등을 위해 **개인정보보호 포털을 운영**

[개인정보보호포털 기능]

○ 개인정보보호에 대한 당의 방침, 지침, 정책 및 국가 법률 정보 제공
○ 개인정보 보호에 관한 정책 및 법률 선전·보급
○ 개인정보 보호 현황 및 관련 정보 업데이트
○ 사이버공간을 통한 개인정보 보호 활동에 대한 정보, 서류 및 자료 제공
○ 유관기관, 조직 및 개인의 개인정보보호 업무 평가 결과 제공
○ 개인정보 보호에 관한 규정위반행위 통지
○ 관계법령에 따라 개인정보 침해행위 및 협조행위에 대해 경고
○ 관계법령에 따라 개인정보 보호 위반행위 처리
○ 기타 개인정보 보호에 관한 법률에서 규정된 업무 수행

## [3장] 기관·조직·개인의 책임

□ 개인정보관리자, 개인정보처리자 등의 **개인정보보호 책임**을 구분하여 명시

[개인정보보호 책임 구분]

| 개인정보관리자 | 개인정보처리자 |
|---|---|
| 정보처리업무의 관리적·기술적 보호조치, 개인정보 보호조치를 구현하고 필요에 따라 검토 및 업데이트 | 동 시행령 및 기타 관계 법령에 명시된 개인정보 보호조치를 성실히 이행 |
| 개인정보처리 이력 기록·저장 | - |
| 개인정보보호 규정 위반 통지절차 준수(72시간 이내 공안부 신고) | - |
| 적정한 개인정보 보호조치를 이행하는 개인정보처리자를 선정하고 개인정보 처리 | 개인정보관리자와 정보처리 계약(협의) 체결 시에만 개인정보를 획득하며, 계약에 준수하여 개인정보 처리 |
| 정보주체의 권리 보장 | 개인정보 처리 완료 후 모든 개인정보는 삭제 또는 개인정보관리자에게 반환 |
| 개인정보 처리 과정에서 발생한 정보주체의 손해에 대한 책임 | (좌 동) |
| 개인정보보호에 관해 공안부 및 국가기관과 협력하여야 하며, 개인정보 위반행위 조사시 필요 정보 제공 | (좌 동) |

※ 개인정보처리관리자와 제3자는 개인정보관리자 및 개인정보처리자의 책임을 모두 준수할 필요

## [4장] 시행

□ 동 시행령은 **'23년 7월 1일**부터 시행

○ 다만, **영세·중소·신생 기업**은 설립일로 부터 2년 이내에는 **개인정보보호 담당부서 및 담당자 관련 규정 유예***

* 개인정보를 직접 처리하는 영세·중소·신생기업은 유예를 미 적용

[참고] 개인정보보호 시행령의 개인정보 처리 관련 준수사항(요약)

| 구분 | 주요 내용 |
|---|---|
| 기본 개인정보 | **(대상)** 이름, 성별, 거주지, 국적, 사진, 전화번호, 주민등록번호, 여권번호, 가족관계, 사이버공간 활동 이력, 디지털 계정 등<br>**(조치사항)** ❶ 개인정보 보호조치 준수, ❷ 개인정보 저장장치 처리 및 삭제·파기하기 전에 **개인정보 처리시스템·장비**의 **네트워크 보안 확인** |
| 민감 개인정보 | **(대상)** 정치, 종교, 의료, 인종, 민족, 유전적·생물학적 특성, 성생활, 범죄, 성생활, 계좌정보, 예금정보, 위치정보 등<br>**(조치사항)** ❶ 기본 개인정보 의무사항, ❷ **개인정보 보호 담당부서 및 담당자 지정**, ❸ **개인정보보호 담당부서 및 담당자 정보를 개인정보보호 전담기관에 제공**, ❹ **민감정보 처리 정보주체 통지** |
| 보호조치 | 정보처리업무의 관리적·기술적 보안조치 구현 |
| 정보주체의 권리 | • 개인정보 처리 제한 – 정보주체 요구로부터 **72시간 이내**<br>• 개인정보 처리 반대 – 정보주체 요구로부터 **72시간 이내**<br>• 개인정보 제공 – 정보주체 요구로부터 **72시간 이내**<br>• 개인정보 정정 – 신속하게 정정하며 정정불가시 **72시간이내 통지**<br>• 개인정보 동의 철회 – **동의철회 결과 및 손해** 정보주체 **통지**, **동의철회서 접수 후** 정보주체 **정보처리 중지** |
| 개인정보보호 규정 위반 통지 | **72시간 이내 공안부 신고** |
| 개인정보처리 통지 | 개인정보 처리 전 1회 사전 통지 |
| 아동 개인정보 처리 | 만 7세이상 아동(16세미만)은 아동 및 아동 부모의 동의 필요 |
| 개인정보 무단수집 제한 | 개인정보 무단수집 소프트웨어나 기술적 장치 설정 등은 불법 |
| 개인정보 영향평가 | • 개인정보처리시 개인정보처리 영향평가서 작성 및 보관<br>• 개인정보 처리 후 **60일 이내 공안부 제출** |
| 개인정보 국외 이전 | • 개인정보 처리 시작일로부터 **60일 이내 제출**<br>• 개인정보 **이전 완료 후 정보 이전사항 및 담당자 연락처 공안부 서면 통지**<br>• 국외이전자는 국외이전 영향평가서 **내용 변경 시** 수정요청일 **10일 이내 수정**<br>• **공안부는** 다음의 경우 **국외 이전 중단 요구**<br>1) 이전 개인정보가 베트남 국가안보 침해시, 2) 국외이전 영향평가 미흡 판단, 3) 내용변경 평가서 제출 규정 미준수, 4) 베트남 국민 개인정보 유출 또는 분실시 |

## 3. 사이버보안 시행령(Decree 53) 주요 내용*

* 시행령 내용 中 베트남 현지 데이터 보관 및 지사 설립 내용만 검토

### 가. 베트남 현지 데이터 보관

□ **(적용 대상)** 베트남에서 사업을 영위하는 **국내 및 외국기업**

□ **(의무 사항)** 베트남 서비스 이용자의 **개인정보*, 생성정보**, 관계정보**** 데이터는 **베트남 현지에 보관**

* 개인정보 : 개인을 식별할 수 있는 기호, 문자, 영상, 음향 또는 동등한 형태의 정보

** 생성정보 : 계정 이름, 서비스 사용시간, 신용카드 정보, 이메일, 마지막 로그인 또는 로그아웃 세션 IP 주소, 계정 또는 데이터와 연관 등록된 전화번호

*** 관계정보 : 베트남 서비스 이용자와 교류하는 그룹의 정보

□ **(보관 형식)** 기업 **자율적**으로 결정

□ **(데이터 보관기간)** 베트남 현지 데이터 보관 의무기간은 **데이터 보유 요청**을 받은 때부터 **종료될 때까지**이며 **최소 24개월**

### 나. 베트남 현지 지사 설립

□ **(적용 대상)** 베트남에서 **통신서비스, 전자상거래, SNS 서비스, 온라인 게임 등**의 사업을 영위하는 **외국기업**

□ **(의무 사항)** 베트남 內 **지사 또는 사무소**를 **설립**

□ **(현지 지사 설치기간)** 기업이 베트남에 **지사 또는 사무소 설치 요청**을 받았을 때부터 **서비스를 더 이상 제공하지 않을 때까지**

## 다. 공통 사항

□ **(데이터 저장 및 지사 등 설립 절차) 공안부**는 기업에 **데이터 저장 및 지사 등 설립**을 촉구하고, 국외 기업은 **12개월 이내**에 **의무 이행**

[데이터 저장 및 지사 등 설립 절차]

**❶ 공안부 장관** → **❷사이버보안 및 하이테크범죄예방국** → **기업**

❶ (공안부 장관) 현지 데이터 저장, 지점 또는 대표사무소 설립 요청 결정

❷ (사이버보안 및 하이테크범죄예방국) 기업에게 데이터 저장 및 베트남 지사 설립 촉구, 관련기관에 국가관리 기능 수행 통보

→ 공안부 장관이 결정한 날로부터 **12개월 이내** 국외기업 데이터 현지 보관, 지점 또는 사무소 현지 설치 의무 이행 필요

□ **(시스템 로그 보관기간) 사이버보안법 제26조 제2항 b호**에 따라 관련 **시스템 로그**(법 위반 조사·처리 목적)는 **12개월 이상 보관**

[베트남 사이버보안법 제26조 제2항 b호 내용(번역)]

b. 정보시스템 또는 서비스를 직접 관리 기관은 공안부 산하 사이버보안 전담부서 또는 정보통신부 관할기관 요구가 있는 경우 24시간 이내에 베트남 치안방해 등에 해당하는 정보를 삭제하고 정보공유를 차단하며, 동 위반 조사 처리에 대한 시스템 기록을 저장

□ **(기타) 외국기업**에 한해 데이터 현지 저장이나 지사 등의 설립이 **불가능**한 경우, **3영업일 이내 공안부 산하 사이버보안국에 통보**

○ **공안부** 산하 사이버보안국은 **불가항력의 진위여부를 확인**하며, **외국기업**은 **30영업일 이내**에 **시정방안**을 모색

## 4. 시사점

□ **베트남 개인정보보호 규제**는 국내 규제와 비교하여 **영향평가서 제출**, 정보주체 요구에 대한 **처리기간 등 내용이 상이**하므로,

○ 베트남에 진출(또는 진출 예정)인 **사원기관**은 베트남의 **개인정보 법령 체계**에 대한 **이해** 및 **규제 내용**의 **면밀한 파악**이 요구

[개인정보보호 시행령 13 및 사이버보안 시행령 53 주요 내용]

| 개인정보보호 시행령 13 | 사이버보안 시행령 53 |
|---|---|
| 정보주체의 권리, 개인정보처리 영향평가, 개인정보 국외이전 영향평가, 개인정보보호 규정 위반 통지, 개인정보관리자&개인정보처리자 의무, 기본 개인정보&민감정보 조치사항, 관리적·기술적 보호조치 등 | 데이터 현지 저장, 현지 지사 또는 사무소 등 설립 의무 |

○ 특히 개인정보 처리, 개인정보 국외 이전, 데이터 현지 보관 등에 대해 **베트남 공안부 신고·통지 의무**에 대해 주의 필요

□ **개인정보보호 시행령**에서 규제 위반에 대한 **구체적 징계 수준을 명시하고 있지는 않으며,**

○ 동 시행령에 **별도 유예기간**을 두지 않거나 **구체화하지 않은 규제**사항들이 있어 **베트남 규제 동향**에 대한 **지속적인 파악** 필요

※ 베트남 정부는 본 시행령을 기반으로 '24년에 개인정보보호법을 제정할 계획

# 전자금융과 금융보안

# 03
# News · Notice

금융보안 교육 안내

금융보안원 소식

사원기관 소식

# 01 금융보안 교육 안내

## 집합교육 교육 일정 (12월 과정)

| 연번 | 과정명 | 형태 | 일정 | 교육시간 | 정원 |
|---|---|---|---|---|---|
| 1 | 금융권 취약점 분석·평가의 이해 | 실습 | 12.4.~12.5. | 2일(12h) | 15 |
| 3 | 금융 IT감사 실무 | 이론 | 12.4.~12.6. | 3일(18h) | 25 |

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

# 02 금융보안원 소식

## 금융정보보호 컨퍼런스「FISCON 2023」개최(11.9.)


금융보안원은 11월 9일(목) 여의도 콘래드 호텔에서 국내 최대 금융정보보호컨퍼런스「FISCON 2023」를 〈미래 금융 전략, 금융보안 프렌들리〉란 주제로 성황리에 개최 하였으며, 금융회사를 비롯한 민·관·산·학·연 전문가, 일반인, 학생 등 1,400여 명이 참석하였다. 개회식에는 김주현 금융위원장, 이명순 금융감독원 수석부원장을 비롯한 금융회사 CEO, 금융 및 정보보호 유관협회·기관장 등이 참석하여, 금융의 디지털 혁신과 함께 사이버위협이 고도화되고 있는 현재, 금융보안 친화적(Friendly)인 환경 조성의 필요성에 주목하였다. 韓·美·日 금융보안 전문가가 한 자리에 모여 금융권 AI 및 글로벌 사이버 위협 동향에 대한 특별강연을 진행하였으며, 디지털금융 및 금융보안 관련 전략, 기술, 대응 세 분야에서 총 18개 주제에 대한 강연을 진행하였다.

## 금융보안원이 전망하는 2024년 디지털금융 및 사이버보안 이슈(11.2.)

금융보안원은 2024년에 발생될 수 있는 이슈 및 선제적 대응방향을 제시하는 2024년 디지털금융 및 사이버보안 이슈 전망을 발표하였다. 2024년 핵심 이슈로 금융보안을 일상과 비즈니스 속 필수 가치로 인식하자는 '금융보안 프렌들리' 전략을 제시하고, 디지털금융 정책(자율보안체계 전환, 사이버복원력, 클라우드 마이그레이션), 보안 위협(하이브리드 위협, SBOM, 딥페이크), IT 혁신(디지털지갑, 책임감 있는 AI, 금융 사물인터넷) 3가지 주제별로 이슈를 각각 선정하였다. 금융보안원 김철웅 원장은 "지능화·고도화되고 있는 보안 위협을 원천 차단하는 것이 불가능한 상황에서, 디지털금융 서비스의 편의성과 더불어 안전성도 균형있게 확보될 수 있도록 全 금융생태계는 보안성의 가치에 주목할 필요가 있다"라고 강조하였다.

### 「코리아 핀테크 위크 2023」에서 금융보안 세미나 개최(8.17.)

금융보안원은 금융위원회가 주최하는 「코리아 핀테크 위크 2023」 행사의 일환으로 '핀테크 4.0 시대의 금융보안 전략'을 주제로 8월 31일 금융보안 세미나를 개최하였다. 이번 세미나에서는 금융보안원 등의 산·학 전문가들이 AI, 전자지갑, SW 공급망 보안 등 디지털 혁신 기술의 사이버 공격·보안 위협을 분석하고 모범 사례 소개 및 대응 방안을 발표하였다.

### 금융권 사이버 침해위협 분석대회, 「FIESTA 2023」 개최(8.21.)

금융보안원은 금융회사 침해 대응 역량 강화와 정보보호 우수인력 발굴을 위해 「FIESTA 2023」을 개최하였다. 본 대회는 최근 이슈가 되는 침해사고 사례를 기반으로 다양한 문제를 출제해 금융권에 실제로 발생할 수 있는 침해위협 상황을 분석하고 대응하는 역량을 평가한다. 특히 올해는 대회를 사전 체험할 수 있도록 「FIESTA 플레이존」을 신규 운영하여 입문자도 흥미를 갖고 대회에 참가하여 잠재된 실력을 발휘할 수 있도록 대회 진입장벽을 완화하였다. 참가 대상은 금융보안원 사원기관 재직자 및 대학(원)생이며, 성적이 우수한 6개팀에게는 금융보안원장상과 포상금을 시상하고, 금융보안원 입사 지원 시 우대 혜택을 제공할 계획이다.

### KISA-금융보안원, 데이터 비식별화 보증요건 ITU-T 국제표준으로 최종 채택(9.14.)

금융보안원(FSI)은 KISA와 공동 제안한 '데이터 비식별화 보증요건(X.rdda)'이 국제표준으로 채택되었다고 밝혔다. KISA와 FSI는 8월 29일(화)부터 9월 8일(금)까지 고양시 KINTEX에서 개최된 ITU-T 표준화 회의(SG17, 정보보호연구반)에 참석해 대응한 결과, 제안한 표준안이 국제표준으로 채택되었다. 제안한 국제표준(ITU-T X.Suppl.39)은 데이터의 비식별화를 보증하기 위한 요구사항의 내용 중심으로 담고 있다. 그동안 비식별화된 데이터의 적정성을 평가하는 공인된 국제적 기준이 없어 사업자들이 느꼈던 규제 불확실성에 대한 불안감도 해소하는 계기가 될 것으로 예상한다. 개인정보가 포함된 데이터의 비식별화와 관련한 국제표준 개발과 확산을 위하여 협력해온 양 기관은 향후에도 지속적인 상호 협력 예정이다.

### 전자금융사고 예방을 위해 「이상금융거래탐지시스템(FDS) 운영 가이드라인」을 마련(10.4.)

금융감독원과 금융보안원은 전자금융사고 예방을 위해 「이상금융거래탐지시스템(FDS) 운영 가이드라인」을 발표하였다. 금융거래에 대한 외부 위협이 계속해서 확대되고, 지능화되는 추세를 보임에 따라 업계가 공동으로 대응할 필요성이 증대하여 T/F를 구성하여 동 가이드라인 마련하였다. 앞으로, 국내 은행업권에서는 주요 피해유형이 반영된 '이상거래탐지룰'이 공통 적용되고, 이에 더하여 개별 은행의 거래특징 등을 반영한 자체 탐지룰이 추가 적용되어 전자금융거래의 안정성이 크게 향상될 것으로 기대한다. 금감원 및 금보원은 앞으로도 동 가이드라인에 대한 업계의 피드백을 지속적으로 반영·개선하여, 새로운 위협 발생시에도 그에 대한 업계 전반의 대응력이 향상되어 금융분야 전자금융거래 안전성이 한층 강화될 것으로 기대한다.

## 금융이 묻고 데이터가 답한다「FSI Data Challenge 2023」시상식 개최(10.31.)


금융데이터거래소를 운영하는 금융보안원은「FSI Data Challenge 2023」시상식과 우수작 발표회를 10월 30일에 개최하였다. 3회째를 맞는 이번 대회는 △ 카드소비 형태에 따른 보험종목별 사고율 분석 △ 지역별 라이프스타일 분석을 통한 전기차 구매 고객 예측을 주제로 전국 대학교·대학원생으로 구성된 총 81개 팀이 참여하였으며, 창의성, 타당성 및 전문성을 평가하여 최종 7개 팀을 수상자로 선정하였다. 금융위원장상(1위)은「신용평가모형을 통한 전기차 구매 선호 등급 산출」주제를 제안하였다. 이번 대회 수상자에게는 상장과 함께 총 2,000만원 상당의 상금을 제공하였으며 금융보안원 입사 지원 시 채용 혜택을 제공할 계획이다.

## 최정예 화이트해커팀 'RED IRIS' 출범(11.6.)

금융보안원은 지난 10월 대통령 주재로 실시한 '청년 화이트 해커와의 대화'를 계기로 사이버 안보를 강화하는 구체적인 실행방안의 일환으로 지능화·고도화되는 해킹 위협에 효과적으로 대응하기 위해 최정예 화이트해커로 구성된 금융권 전문 레드팀 'RED IRIS(레드 아이리스)'를 출범하였다. 레드팀은 방어자 관점의 전통적 보안에서 벗어나 실제 해커의 시각에서 해킹 시나리오를 발굴하고 보안 취약점을 찾는 전문 모의해킹 조직으로, 금융시스템 보안 취약점에 대한 정보공유 및 모의해킹 교육 제공 등을 통해 금융권의 사이버 공격 대응 역량을 제고할 계획이다.

## 「제7회 금융보안원 논문공모전」시상(11.9.)

금융보안원은 '디지털 금융혁신과 금융보안'을 주제로 제7회 금융보안원 논문공모전을 실시하였다. 4월 1일부터 8월 31일까지 금융회사, 대학(원)생, 금융소비자, 관련 분야 종사자 등 전 국민을 대상으로 논문을 신청받았으며, 예비 심사, 본심사, 수상작 선정 등 3단계로 심사를 진행하여 대상 1편, 최우수상 1편, 우수상 3편, 장려상 3편 등 총 8편을 11월 9일(목)에 금융보안원 주최 금융정보보호 컨퍼런스「FISCON 2023」에서 시상하였다.

## 2024년도 신입직원 채용 실시(9.4.)

금융보안원은 2024년도 신입직원을 채용할 예정이다. 채용 분야는 일반기획, 회계·세무, IT 3개 분야로 구분되며 서류·필기·면접전형을 거쳐 12월 중 최종 합격자를 발표할 계획이다.

# 03 사원기관 소식

**신한투자증권, KB증권, NH투자증권** 토큰증권 '공동망' 구축을 위한 컨소시엄 발족(9.12.)

토큰증권 공동 인프라를 구축하기 위해 신한투자증권과 KB증권, NH투자증권이 '토큰증권 컨소시엄' 발족을 위한 업무협약(MOU)을 체결하였다. 신한·KB·NH 컨소시엄은 토큰증권 발행 및 유통 체계는 블록체인의 핵심 기술인 분산원장 방식의 계좌관리에 기반해 이뤄지기 때문에 새로운 인프라 구축이 필수적이라고 판단하여, 공동 인프라 구축 범위를 확정하여 이르면 연내 인프라 구축 사업을 발주할 예정이다.

**중소기업은행** '안면인식기술과 위치확인기술을 활용한 내점고객 대상 실명확인 서비스' 혁신금융서비스 신규 지정(9.13.)

중소기업은행의 안면인식기술과 위치확인기술을 활용한 내점고객 대상 실명확인 서비스는 기존 고객이 내점해 대면 금융거래시 안면인식기술 및 추가인증방식(위치인증 또는 PIN번호인증)을 활용해 기존 실명확인증표를 불러오는 방식을 통해 실지명의를 확인하는 서비스가 금융위원회 정례회의를 통해 혁신금융서비스로 신규 지정되었다. 금융당국은 고객이 실명확인증표 실물을 지참해 제시하지 않더라도 안면인식기술 및 추가인증방식을 활용해 기존에 등록된 실명확인증표 스캔 이미지를 이용함으로써 실지명의를 확인할 수 있도록 특례를 부여하였으며, 중소기업은행은 내년 초 전산 구축을 완료한 후 서비스를  출시할 예정이다.

**우리은행** 우리은행 모의해킹 경진대회(우리콘) 우수 화이트해커 5팀 시상식(9.15.)

우리은행은 금융보안원과 공동으로 진행한 '제3회 모의해킹 경진대회' 시상식을 10월 15일에 개최하였다. 대회는 8월 7일부터 11일까지 5일간 진행되었고, 블랙 해커의 공격에 쉽게 노출될 수 있는 디지털뱅킹 위험 요소를 찾아냄으로써 사이버위협에 선제적으로 대응하기 위한 취지로 마련됐다. 금융보안원 보안전문가, 화이트해커, 정보보호학화 교수진으로 구성된 심사위원들은 해킹 피해의 위험도와 영향도를 고려해 총 5개 팀을 우수팀으로 시상했다. 사이버 위협이 점차 지능화·고도화됨에 따라 선제적 대응하고 정보보호 우수인력 양성에 지속적으로 힘쓸 것으로 전했다.

**카카오뱅크** 안면 위변조 탐지 기술 TTA 검증 완료(10.17.)

카카오뱅크는 비대면 인증 시 얼굴 위변조 여부를 AI로 판별하는 자체 개발한 얼굴 위변조 탐지 기술이 한국정보통신기술협회(TTA)의 V&V(확인 및 검증, Verification & Validation) 시험에서 높은 수준의 성능 기록을 달성하였다. 카카오뱅크는 150만 개 이상의 안면 위변조 데이터를 활용해 탐지 기술을 개발하였으며, 실제 얼굴 이미지와 인쇄물, 스크린 이미지를 혼합한 약 50만 개의 평가 데이터가 활용됐다. 카카오뱅크는 입증된 기술력을 바탕으로 안면 인식 기술 등 자체 개발한 금융 솔루션에 대한 공급 기반을 마련할 계획이다.

**NH투자증권** 국제 개인정보보호 표준 'ISO 27701' 인증 획득(10.17.)

NH투자증권은 글로벌 국제표준 인증기관인 DNV의 심사를 통해 국제표준화기구(ISO)가 제정한 국제 개인정보보호 경영시스템 표준인 'ISO 27701' 인증을 획득하였다. 해당 인증은 ISO에서 제정한 개인정보보호 분야의 가장 권위 있는 국제 표준 인증으로, 이를 획득하기 위해서는 개인정보 수집 및 처리·시스템 안정성 등 유럽 개인정보보호법(EU-GDPR)에서 요구하는 총 8개 분야 49개 관리 기준을 모두 충족해야만 취득할 수 있다. NH투자증권은 고객 개인정보보호를 위해 지난 2021년 '정보보호 및 개인정보보호 관리체계 인증(ISMS-P)'을 최초 취득했고, 2022년엔 국제 정보보호 관리체계 표준인 'ISO 27001' 인증을 획득해 유지해 오고 있다.

**하나은행** 하나원큐 조각투자 연계서비스 출시(10.24.)

하나은행은 10월 25일부터 4대 시중은행 가운데 처음으로 '하나원큐 조각투자 연계 서비스'를 출시하였다. 하나원큐 조각투자 연계서비스는 하나은행 대표 모바일앱인 '하나원큐'를 통해 부동산·음원 등 해당상품을 판매하는 조각투자사로 쉽고 간편하게 접속할 수 있다. 해당 서비스는 혁신금융서비스로 지정받은 '루센트블록'과 '뮤직카우'를 우선 연계하였다. 두 회사와 조각투자 관련 계좌관리, 신탁 등 긴밀한 협업관계를 유지하며, 향후 토큰증권, 웹3.0 선도를 위해 미래에셋증권과 SK텔레콤과 함께 사업을 준비하고 있다.

**신한금융** 신한금융 앱 브랜드 '신한 SOL'로 통합(10.31.)

신한금융은 11월 1일부터 신한은행, 신한카드, 신한투자증권, 신한라이프 등 4대 주요 그룹사의 디지털 애플리케이션 브랜드를 '신한 SOL'로 통합해 운영한다. 이번 개편을 통해 신한금융그룹의 디지털 앱은 ▲[은행] 신한 SOL → 신한 SOL 뱅크 ▲[카드] 신한 Play → 신한 SOL 페이 ▲[증권] 신한 알파 → 신한 SOL 증권 ▲[라이프] 신한 스퀘어 → 신한 SOL 라이프로 명칭이 각각 변경되었다. 신한금융은 그룹사의 주요 상품 및 서비스를 단 하나의 앱으로 편하게 이용할 수 있는 '유니버설 간편앱'을 연내 출시할 예정이다.

※ 사원기관의 **디지털금융·핀테크** 또는 **정보보호** 관련 소식을 알리고 있습니다. 이와 관련하여 아래의 주소로 보도자료(링크 등)를 보내주시면 내용을 반영하고자 하오니 많은 참여 부탁드립니다.
e-Mail : research@fsec.or.kr Tel : 02-3495-9711~9713

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

## 2. 기고신청

□ **(제출 항목)** ① 기고자명 및 소속(기관 및 부서명), ② 원고제목, ③ 목차, ④ 요약 내용(A4 1매 이내)

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

□ **(제출 시기)** 상 시

□ **(제출처)** 금융보안원 보안연구부 연구기획팀

- e-Mail : research@fsec.or.kr  Tel : 02-3495-9711~9713

## 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.**

# 2024 디지털금융 및 사이버보안 이슈 전망

금융보안원

Key Issue
핵심이슈

## 디지털 경쟁력, 금융보안 프렌들리 전략이 필수

F

Financial Policy
### 디지털금융 정책

더 이상 거스를 수 없는 패러다임,
**자율보안체계** 전환


깨지지 않는(anti-fragile) 탄력성,
**사이버복원력**


**클라우드 마이그레이션,**
하드웨어 넘어 **소프트웨어**로

S

Security Threat
### 보안 위협

공격채널의 다양화, 영역을 넘나드는
**하이브리드 위협** 고조

S/W 공급망 공격 성행,
**SBOM**의 중요성이 강조

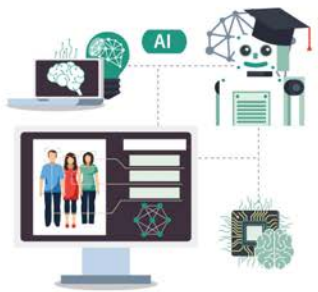

피싱 범죄, '내 얼굴과 목소리까지도?'
**딥페이크** 기술 악용

I

IT Innovation
### IT 혁신

모든 것을 담는다,
**디지털지갑** 경쟁 가속화

AI의 안전성과 신뢰성 확보,
**책임감 있는 AI** 구현




사물과 디지털금융의 만남,
**금융 사물인터넷(FoT)**

# 전자금융과 금융보안


| | |
|---|---|
| 발 행 | 2023년 11월 |
| 발 행 인 | 김 철 웅 |
| 발 행 처 | 금융보안원 |
| 주 소 | 경기도 용인시 수지구 대지로 132 |

(비매품)

제34호 | 2023-4Q

# 전자금융과 금융보안

e-Finance and Financial Security

금융미래를 열어가는 금융보안파트너

금융보안원

FINANCIAL SECURITY INSTITUTE

전자금융과 금융보안 | 제34호


ISSN 2671-7085