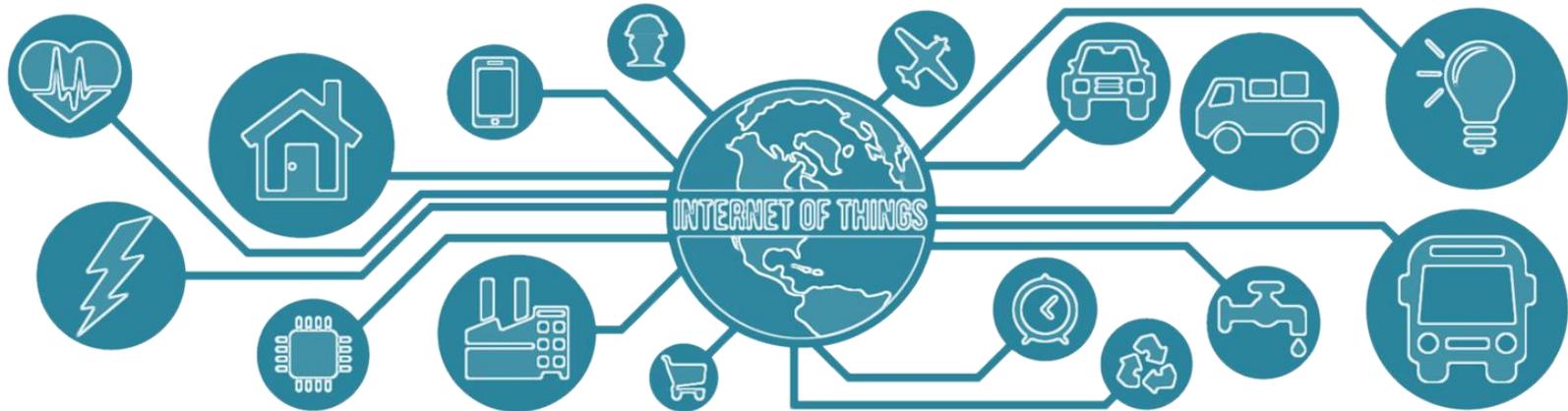


# 실효적 FDS 체계 구축 및 고도화 방안







※ 은행별 FDS를 통한 이상거래 적발 내역 ('15.1.1~'15.7.31)

(단위: 건, 천원)

회사명	FDS구축현황 ('15.8월현재)	이상거래 적발내역				
		탐지기간	이상거래 대응건수	이상거래 확정건수	이상거래 예방금액	
시 중 이 행	은행	구축 완료('15.4월)	'15.5.1~7.31	92,862	826	5,807,383
	은행	구축 완료('13.11월)	'15.1.1~7.31	2,608,508	20,230	23,121,621
	은행	구축 완료('14.12월)	'15.1.1~7.31	2,015,385	1,463	18,332,341
	은행	구축 완료('14.9월)	'15.1.1~7.31	25,324	1,323	3,145,000
	은행	구축 완료('15.1월)	'15.1.29~7.31	90,266	68	1,414,266
	은행	구축 완료('15.7월)	-	-	-	-
	은행	구축 완료('15.1월)	'15.2.1~7.31	6	0	0
지 방 은 행	은행	구축 완료('14.12월)	'15.1.1~7.31	1,860	8	45,040
	은행	구축 중(~'15.12월)	-	-	-	-
	은행	구축 완료('15.4월)	'15.4.18~7.31	2,242,189	0	0
	은행	구축 완료('14.1월)	'15.1.1~7.31	17,013	189	393,636
	은행	구축 완료('15.6월)	'15.6.26~7.31	4,859	0	0
	은행	구축 완료('15.6월)	'15.7.1~7.31	295	0	0
특 수 은 행	은행	구축 완료('14.12월)	'15.1.1~7.31	986,486	329	1,424,460
	은행	구축 완료('15.6월)	'15.6.8~7.31	879	0	0
	은행	구축 중(~'15.10월)	-	-	-	-
	중앙회	구축 완료('15.6월)	'15.6.22~7.31	68	0	0



낮은 이상거래 판정확률  
(1% 이하)



높은 대응건수

※ 은행별 FDS를 통한 이상거래 적발 내역 ('15.1.1~'15.7.31)

(단위: 건, 천원)

회사명	FDS구축현황 ('15.8월현재)	이상거래 적발내역				
		탐지기간	이상거래 대응건수	이상거래 확정건수	이상거래 예방금액	
시 중 이 행	은행	구축 완료('15.4월)	'15.5.1~7.31	92,862	826	5,807,383
	은행	구축 완료('13.11월)	'15.1.1~7.31	2,608,508	20,230	23,121,621
	은행	구축 완료('14.12월)	'15.1.1~7.31	2,015,385	1,463	18,332,341
	은행	구축 완료('14.9월)	'15.1.1~7.31	25,324	1,323	3,145,000
	은행	구축 완료('15.1월)	'15.1.29~7.31	90,266	68	1,414,266
	행	구축 완료('15.7월)	-	-	-	-
	은행	구축 완료('15.1월)	'15.2.1~7.31	6	0	0
지 방 은 행	은행	구축 완료('14.12월)	'15.1.1~7.31	1,860	8	45,040
	은행	구축 중(~'15.12월)	-	-	-	-
	은행	구축 완료('15.4월)	'15.4.18~7.31	2,242,189	0	0
	은행	구축 완료('14.1월)	'15.1.1~7.31	17,013	189	393,636
	은행	구축 완료('15.6월)	'15.6.26~7.31	4,859	0	0
	은행	구축 완료('15.6월)	'15.7.1~7.31	295	0	0
특 수 은 행	은행	구축 완료('14.12월)	'15.1.1~7.31	986,486	329	1,424,460
	은행	구축 완료('15.6월)	'15.6.8~7.31	879	0	0
	은행	구축 중(~'15.10월)	-	-	-	-
	중앙회	구축 완료('15.6월)	'15.6.22~7.31	68	0	0



비교적 높은 정확도  
(5% 상회)



타사대비 적은 대응건수

※ 증권사별 FDS를 통한 이상거래 적발 내역 ('15.1.1.~'15.7.31.)  
(단위: 건, 천원)

회사명	FDS구축현황 (15.8월현재)	이상거래 적발내역			
		탐지기간	이상거래 대응건수	이상거래 확정건수	이상거래 예방금액
증권	구축 완료('14.12월)	'15.1.1~7.31	97,348	1	840
증권	구축 완료('15.4월)	'15.6.26~7.31	175	0	0
증권	구축 완료('12.7월)	'15.1.1~7.31	6	0	0
증권	구축 완료('14.11월)	'15.2.1~7.31	1,133	1	58,000
증권	구축 완료('15.6월)	'15.6.19~7.31	0	0	0
증권	구축 완료('15.7월)	-	-	-	-
금융증권	구축 완료('14.10월)	'15.1.1~7.31	345	0	0
증권	구축 완료('14.12월)	'15.1.1~7.31	671	39	1,090,510
증권	구축 완료('15.7월)	-	-	-	-
증권	구축 완료('15.7월)	-	-	-	-
투자자	구축 완료('15.2월)	(추가인증 및 거래차단은 '15년 하반기에 적용)			
증권	구축('13.3월) 및 고도화('15.7월) 완료	'15.1.1~7.31	1,329	14	170,913
증권	구축 완료('15.7월)	-	-	0	-
증권	구축 완료('15.2월)	'15.3.1~7.31	21,504	0	0
증권	구축 완료('14.10월)	'15.1.1~7.31	460	0	0
증권	구축 완료('15.4월)	'15.4.29~7.31	2,288	0	0
증권	구축 완료('15.5월)	'15.5.29~7.31	0	0	0



**은행권과 동일한 현황**

- ❖ 5% 상회 판정을
- ❖ 비교적 적은 대응건수



# 이상금융거래 흐름도

인터넷

은행 Network

인터넷 뱅킹  
고객

채널

뱅킹  
애플리케이션

고객 계좌

금융거래 내용

고객 PC

인터넷 Banking

창구

ATM

폰 뱅킹

모바일 뱅킹

Hacking /  
Phishing /  
Pharming

금융사기범

실시간 판정

정상 이체 거래 1

정상 이체 거래 2

신규 인증서의 발급

추가 계좌 정보 탈취

이상 이체 거래 1

이상 이체 거래 2

**금융사기 행위패턴을 Scenario로 구성해 판별**

- ❖ 과거 접속이력 없는 단말을 통해 소액을 다중 이체
- ❖ 신규 인증서 발급 후 과거 이체이력이 없는 계좌로 5분 내에 이체

## FDS 고도화를 위한 핵심 요소

FDS 구축 과정에서 가장 중점을 두어야 할 Risk 요인은 **False-Positive**와 **False-Negative**를 최소화하는 것이며 이를 달성하기 위한 구체적인 실행 방안이 수반되어야 합니다.

“ Scenario기반 탐지를 보완하는 탐지방식이 필요 ”

“ Scenario기반 탐지에 대한 추가분석이 필요 ”



## FDS 고도화 모델

Scenario 기반 모델과 Risk 기반 모델을 병행 구현 : False-Positive(오탐)와 False-Negative(미탐)를 최소화

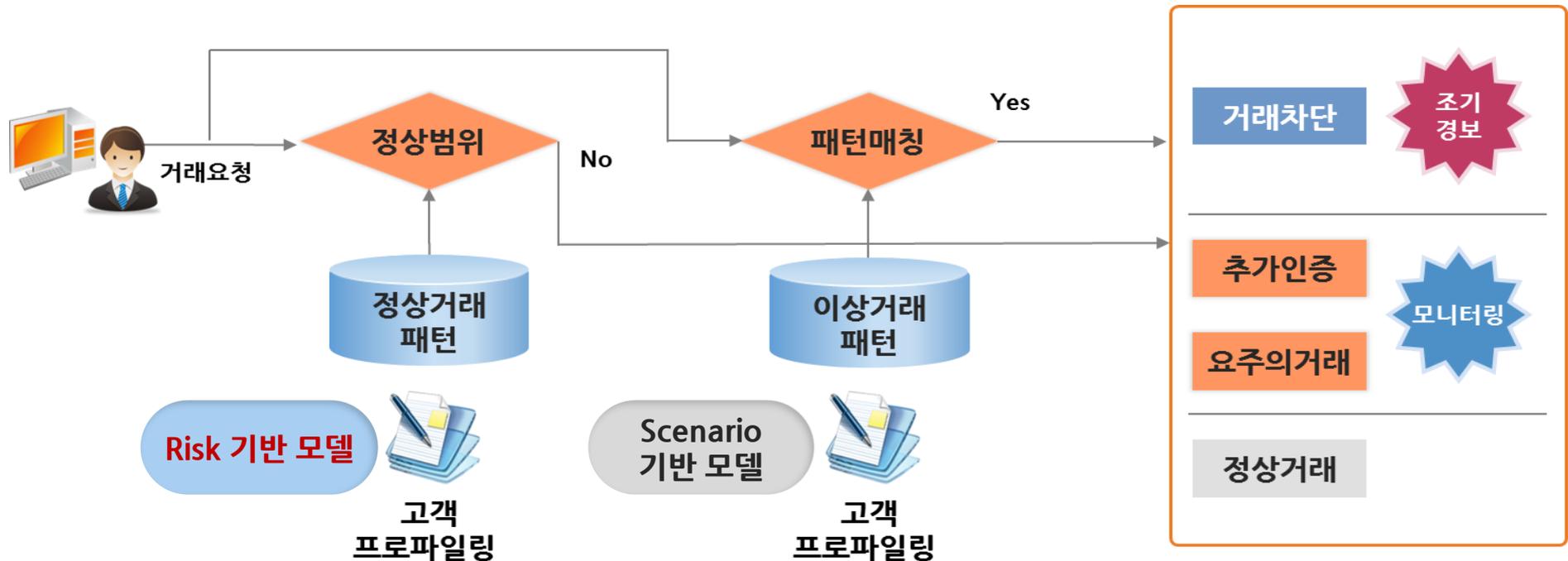
이상  
금융  
거래  
판정

Scenario 기반 모델

이상거래 패턴을 Scenario로 등록하고 이와 동일한 형태의 거래를 탐지  
( 예: 과거이력이 없는, 직전 거래와 다른 단말기에서 공인 인증서 재발급 후 신규 계좌 이체 )

Risk 기반 모델

사고 사례를 분석해 Risk 항목을 프로파일링하고 연관도 분석을 통해 거래 위험도를 판정  
( 과거 미사용 매체 + 신규 단말 + 미거래 지역 + 신규 계좌 = 75점 )



## FDS 고도화 절차

은행 및 증권업계 금융사고 사례 및 금융보안원에서 제시하는 전자금융거래 사기 유형을 수집/분석하여 금융거래 정보 분석 및 금융사기 행위 판정에 적용합니다.

### 금융거래 정보 분석

#### Risk Factor 식별

- 접속정보 (IP,MAC,HDD 등)
- 거래정보 (계좌, 이체횟수, 이체금액,이체시간..)
- 중요정보 변경

#### 사기행위 분석

- 심야시간대 거래
- 특정금액 초과 거래
- 공인인증서 발급
- 신규단말 접속 거래
- 의심계좌 이체 거래
- 해외 접속 거래

### 금융사기행위 판정

#### Scenario 기반 모델

- 법적근거, 금보원 기술가이드를 근거로 사고사례를 통계 기법을 적용하여 시나리오 도출

#### Risk 기반 모델

- 사고 연관성이 높은 동시에 정상범주 고객프로파일 값을 벗어나는 Risk Factor를 기준으로 Risk Score를 도출하여 판정

## 금융 사고 사례 수집

### 은행권 사고 사례



### 증권업계 사고 사례

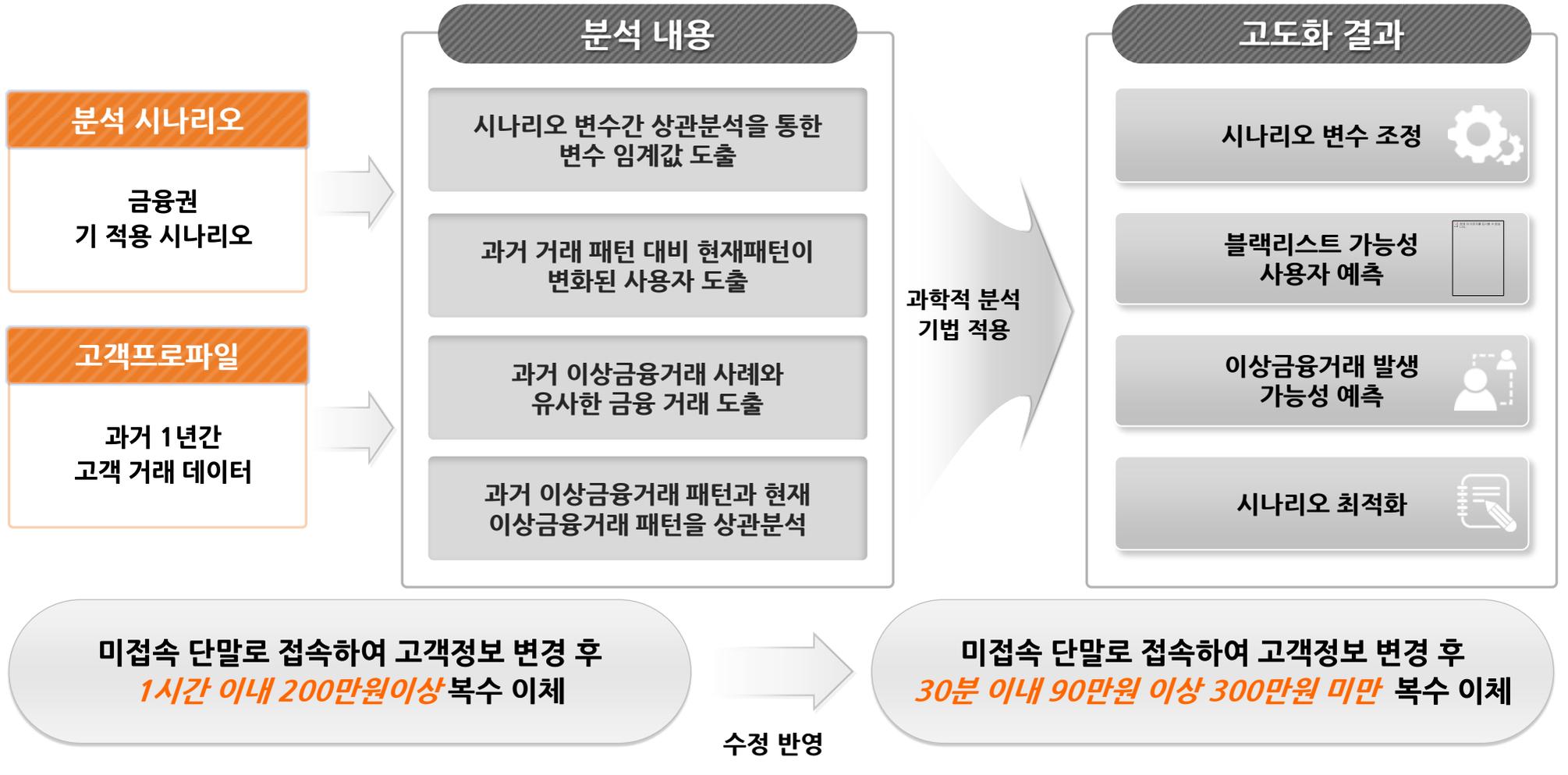


### 금융감독기관 가이드



## Scenario기반 모델 고도화

실사고 사례에 대한 세부 분석과 시나리오내 변수간 연관 분석을 통한 시나리오 고도화 및 잠재적 발생가능성 예측



## Risk기반 모델 체계

Risk Factor 기반의 사용자 프로파일을 작성 후 실시간 거래 정보와 프로파일을 비교하여 상이한 Risk Factor 및 연관도에 따라 이상금융거래로 판정합니다.

### 고객 프로파일

고객: user01

일 거래시간	이체계좌	일 최대 이체횟수	일 최대 이체금액	거래지역
09:00 ~ 15:00	220030245	3	200만원	서울
거래 소요시간	IP	MAC	HDD	거래시도 오류
5분~10분	203.202.14.155	001E101F034E	EI43N09641G50	N

고객정보

계좌정보

단말정보

### 실시간 거래 데이터

고객: user01

거래시간	이체계좌	이체횟수	이체금액
2015-07-07 14:39:49	2200302456	4	500만원
거래지역	거래 소요시간	거래시도 오류	HDD
부산	7분	N	EI43N09641F78

인터넷  
뱅킹

모바일  
뱅킹

창구  
단말

프로파일 정보 검색



채널데이터 분석

Risk Factor 비교

고객 ID	거래시간	신규계좌	이체횟수	이체금액	거래지역	신규 단말			결과
						IP	MAC	HDD	
USER01	2015-07-07 14:39:49	2200302456	4	500만원	부산	213.218.14.145	001E101F050G	EI43N09641F78	탐지
	○	X	X	X	X	X	X	X	
USER01	2015-07-07 15:11:40	220030245	1	150만원	서울	203.202.14.155	001E101F034E	EI43N09641G50	정상

## Risk기반 모델 체계

위험도 산출 프로세스에 의해 최종 위험도(Risk Score)를 산정하고, 위험도(Risk Score)의 범위에 따라 고, 중, 저 위험으로 관리하며 고 위험의 경우 추가 인증을 통해서 관리합니다.

### 위험도 산출 프로세스

사고 Case	이체계좌	일 최대 이체횟수	etc..
사고1	2200302456	4	...
사고2	2302304878	3	...

가중치 계산

FDS 구축 사고사례 분석결과

Risk Factor별 사고발생 밀접도

적용결과

사고 case	이체계좌	일 최대 이체횟수	...	Risk Score
사고1	2200302456	4	...	68
사고2	2302304878	3	...	90

위험도 산출결과

### 위험도 관리

고위험

Risk Score : 70 ~ 100점

중위험

Risk Score : 40 ~ 70점 미만

저위험

Risk Score : 0 ~ 40점 미만

1. 고 위험 Risk Factor 식별
2. 고 위험 거래는 추가 인증으로 관리

## 금융거래 데이터 분석

### 금융거래 데이터 분석 목적

- 전자금융거래 이상 징후를 사전에 예측하기 위한 것으로 다양한 형태의 정형/비정형 금융거래 이벤트 데이터를 대상으로 빅데이터 플랫폼을 활용하여 과학적 분석 기법을 적용함으로써 금융사기 탐지의 가능성을 극대화

### Scenario 분석

- 과거 이상금융거래 사고 사례와 업무 경험에 기반한 직관적으로 파악이 가능한 모델
- Top-Down 방식 모델
- 과거 사고 사례가 적어도 사용이 가능하며 시스템 적용이 용이

상호보완

### 빅데이터 분석

- 데이터 기반으로 통계 및 머신 러닝 등의 과학적 기법을 적용한 모델
- Bottom-Up 방식 모델(Top-Down 방식 병행)
- 과거 사례가 적을 경우 고급 분석 기법을 적용이 곤란
- 시스템 적용이 상대적으로 어려움

FDS  
전자 금융 거래  
이상 징후 탐지



## 빅데이터 분석 주제

No	분석 주제	분석 주제 개요 및 목적
1	Scenario 고도화	<ul style="list-style-type: none"> <li>과거 금융사고 사례와 업무 경험 기반으로 만들어진 Scenario에 대해 데이터 분석을 통해 과다 탐지를 방지</li> <li>Scenario에 사용되는 변수의 전체 분포 또는 변수간의 상관관계를 파악하여 Scenario 임계값의 타당성을 판단 할 수 있는 근거자료로 활용</li> </ul>
2	과거 패턴 유사도 분석	<ul style="list-style-type: none"> <li>사용자별 접속단말기/사용자 변경정보/이체정보의 과거 패턴과 현재 패턴을 비교하여 과거 패턴 대비 현재 패턴이 매우 변화된 사용자를 탐지</li> <li>과거 금융사고 사례를 기반으로 만들어진 Scenario는 현재 시점의 거래 패턴이나 접속 및 사용자 변경정보를 탐지하고 있고 과거의 정보를 고려하지는 않았기 때문에 과거 패턴을 현재 패턴과 비교하여 이상금융거래 탐지 가능성을 증대</li> </ul>
3	사고 사례 기반 매칭 분석	<ul style="list-style-type: none"> <li>과거 금융 사고 사용자의 패턴을 중심으로 유사한 사용자를 조사</li> <li>과거 금융사고 사례 중심을 기반으로 유사한 패턴을 분석</li> </ul>
4	계좌 네트워크 분석(대포/의심)	<ul style="list-style-type: none"> <li>계좌와 계좌간의 관계에서 이체 흐름의 중심에 있는 계좌를 탐지(N:1 입금 이체 내역과 1:N의 출금 이체 내역의 관계에 있는 중심 계좌)</li> <li>금융사고 사례에서 찾을 수 없는 계좌와 계좌의 관계를 분석</li> </ul>

» 시나리오

» 사고 사례 기반  
매칭 분석

» 과거 패턴  
유사도 분석

» 계좌 네트워크  
분석

## 빅데이터 분석 모델

대분류	중분류	소분류	내용	현황	비고
Machine Learning	Supervised Modeling	<ul style="list-style-type: none"> <li>Logistic regression/Decision Tree/NN</li> </ul>	<ul style="list-style-type: none"> <li>과거 사고 사례를 기반으로 학습을 통해서 이상금융거래 탐지</li> </ul>	적용 어려움	<ul style="list-style-type: none"> <li>과거 사례가 적을 경우 모델링 생성이 곤란</li> <li>모델링 결과의 신뢰성 및 모델 생성이 어려움</li> </ul>
		<ul style="list-style-type: none"> <li>KNN(nearest Neighbor)</li> </ul>	<ul style="list-style-type: none"> <li>과거 사고 사례를 Distance 기반 학습을 통해서 이상금융거래 탐지</li> </ul>	적용	
	Unsupervised Modeling	<ul style="list-style-type: none"> <li>Clustering</li> </ul>	<ul style="list-style-type: none"> <li>사용자의 거래 패턴 등의 정보를 이용하여 Clustering을 구성한 후 군집의 중심으로 부터 멀리 떨어져 있는 Anomaly 개체를 탐지</li> </ul>	적용 어려움	<ul style="list-style-type: none"> <li>이상치에 민감하고 군집을 정의하는데 어려움이 발생</li> <li>전체 특성의 군집에는 큰 의미가 없는 경우 존재</li> </ul>
Anomaly detection	Statistical Distribution Based approach	<ul style="list-style-type: none"> <li>Control Chart limits</li> <li>Scoring model</li> </ul>	<ul style="list-style-type: none"> <li>사용 Pattern Index 기준 임계치 분석</li> </ul>	적용	
	Graphical Models Visualization	<ul style="list-style-type: none"> <li>Network Graph</li> <li>Filtering rule</li> </ul>	<ul style="list-style-type: none"> <li>계좌와 계좌와의 이상 징후에 대한 관계를 분석</li> </ul>	적용	
		<ul style="list-style-type: none"> <li>Lattice or Graph</li> </ul>	<ul style="list-style-type: none"> <li>사용자별 Pattern 비교를 위한 시각화</li> </ul>	효율성 부족	<ul style="list-style-type: none"> <li>상대적인 인력 공수 과다 소요</li> </ul>
Analytics Framework		<ul style="list-style-type: none"> <li>Basic Statistics</li> </ul>	<ul style="list-style-type: none"> <li>시나리오 분석 고도화</li> </ul>	적용	

## Scenario 고도화 분석

### 배경

- 과거 이상금융거래 사례를 기반으로 만들어진 Scenario내 변수의 임계점은 변수의 전체 분포를 반영되어 있지 않기 때문에 Scenario 기반 모델의 정탐률을 높이기 위한 분석이 필요

### 목적

- Scenario에 사용되는 변수의 전체 분포 또는 변수간의 상관관계를 파악하여 Scenario 임계값의 타당성을 판단할 수 있는 근거자료(데이터 기반 분석을 통한 결과)생성

### 시나리오 고도화 분석

#### STEP1. 변수 기초 분석

- 이체 횟수/이체 금액
- 특정 시간내 이체횟수/금액
- 신규 계좌 이체 횟수/금액
- 휴대폰 변경
- 인증서 발급
- 단말기 지정
- ...

#### STEP2. 변수 상관 분석

- 이체 횟수/이체 금액
- 특정 시간내 이체 금액/이체 횟수
- 신규 계좌 이체 횟수/이체 금액
- 휴대폰 변경&이체 시간
- 인증서 발급&이체 시간
- 단말기 지정&이체 시간
- ...

#### 분석 결과

#### 분석 결과 검토

#### 시나리오 고도화 활용

★ : 시나리오 고도화를 위해서 의사 결정에 필요한 데이터 기반 분석 결과를 제공하는 것이 목적이며 분석 결과 자체가 시나리오 고도화 되는 것은 아님

## Scenario 고도화 분석 예시

NO	데이터 정보 구분	기초 분석 항목	상관 분석 항목
1	이체 정보	<ul style="list-style-type: none"> <li>이체 금액 분포</li> <li>이체 금액 50만원~1000만원 상세 분포</li> <li>이체 횟수 분포(일별 기준)</li> <li>이체 횟수/누적 금액(일별 기준)</li> <li>특정(5분/10분) 시간 내의 이체 횟수(첫 거래 기준)</li> </ul>	<ul style="list-style-type: none"> <li>이체 횟수 별 이체 금액</li> <li>특정(5분) 시간 내의 이체 횟수 별 이체 금액</li> <li>특정(10분) 시간 내의 이체 횟수 별 이체 금액</li> <li>이체 횟수 별 이체 금액 기준 700만원 미만 이체 횟수의 분포</li> <li>이체 횟수 별 이체 금액 기준 50만원 초과 700만원 미만</li> </ul>
2	사용자 정보 변경	<ul style="list-style-type: none"> <li>단말기 지정서비스 등록 횟수(일별, ID별)</li> <li>휴대폰 번호 변경 횟수(일별, ID별)</li> <li>공인인증서 발급 횟수(일별, ID별)</li> <li>접속 후 횟수</li> </ul>	<ul style="list-style-type: none"> <li>단말기 지정서비스 등록 후 이체가 일어나는 시간</li> <li>휴대폰 번호 변경 후 이체가 일어나는 시간</li> <li>공인인증서 발급 후 이체가 일어나는 시간</li> <li>접속 후 이체가 일어나는 시간(최근 3개월)</li> </ul>
3	신규 계좌 정보	<ul style="list-style-type: none"> <li>과거 미거래 계좌로 이체하는 신규 계좌 분포</li> </ul>	<ul style="list-style-type: none"> <li>과거 미거래 계좌로 이체하는 행위 횟수 분포</li> <li>과거 미거래 계좌로 이체하는 행위 횟수 별 이체 금액 분포</li> </ul>
4	단말기 정보	<ul style="list-style-type: none"> <li>동일 ID로 접속하는 단말기 분포</li> <li>동일 단말기별 사용 ID 분포</li> </ul>	<ul style="list-style-type: none"> <li>동일 ID기준 MAC과 HDD 사용 분포</li> </ul>

## 03 솔루션 소개 및 구축 사례



## FDS : Heimdallr 소개

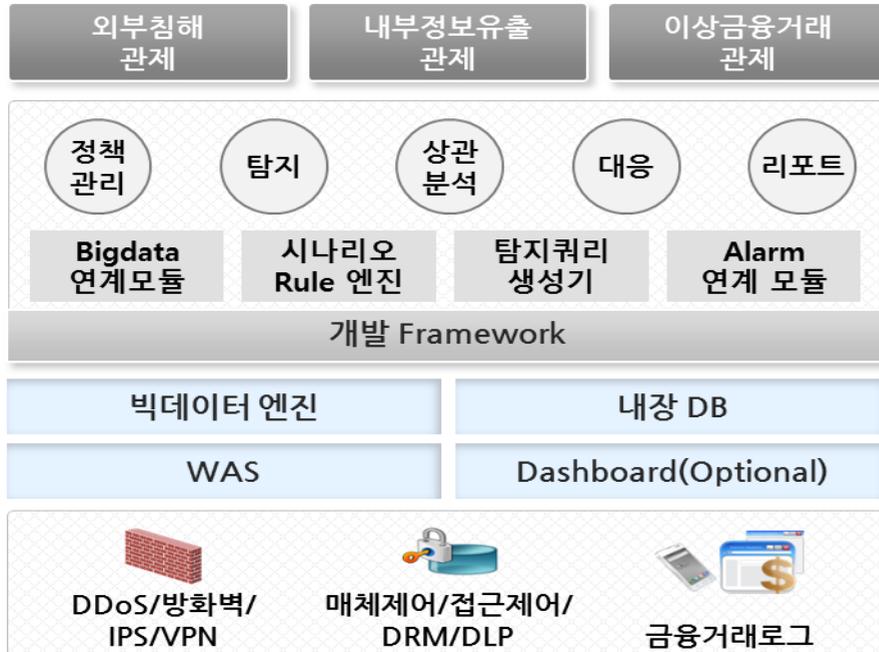
빅데이터 엔진을 기반으로 외부침해, 내부정보유출, 이상금융거래에 대한 실시간 데이터를 수집하고 연관 분석하여 비정상 행위를 탐지 및 차단할 수 있는 기능을 제공

외부침해 관제

내부정보유출 관제

이상금융거래 관제

### Heimdallr



### Heimdallr Framework

- 로그정보 식별 및 수집 기능 제공
- 직관적 시나리오 설정 관리 제공
- 개별분석 및 상관분석 기능 제공
- 비정형 데이터 수집 및 분석 기능

로그정보 식별 및 수집

시나리오 설정

상관분석 기능

비정형 데이터수집

### Heimdallr - 외부침해

- 외부침해 보안 솔루션 연동 제공
- 검증된 외부침해 시나리오 Rule Set 제공
- 시나리오 기반 위협 이벤트 실시간 탐지/분석



### Heimdallr - 내부정보유출

- 내부정보유출 보안 솔루션 연동
- 검증된 내부정보유출 시나리오 Rule Set 제공
- 시나리오 기반 내부정보유출 이벤트 실시간 탐지/분석



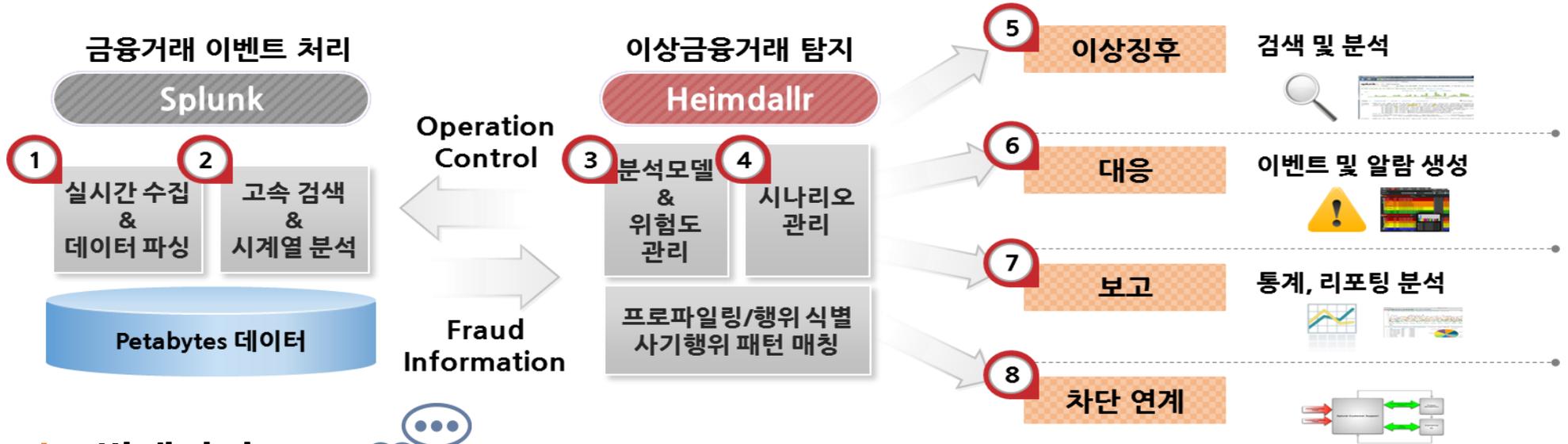
### Heimdallr - 이상금융거래

- 금융거래 로그 연동 제공
- 검증된 이상금융거래 시나리오 Rule Set 제공
- 시나리오 기반 이상금융거래 이벤트 실시간 탐지/분석



## FDS : Heimdallr 소개

Heimdallr은 이상금융거래 데이터 처리에 있어서 최적의 플랫폼인 빅데이터 엔진기반으로 개발되었으며 실시간으로 발생하는 정형/비정형 데이터 수집, 저장 및 분석에 있어서 우수한 성능과 기능을 제공합니다.



## Why 빅데이터?

### 지속적 원본 거래 데이터 축적

- 금융 사기 행위 징후를 분석하기 위해서는 장기간에 걸친 원본 거래 데이터의 수집을 기반으로 시계열 분석이 필요

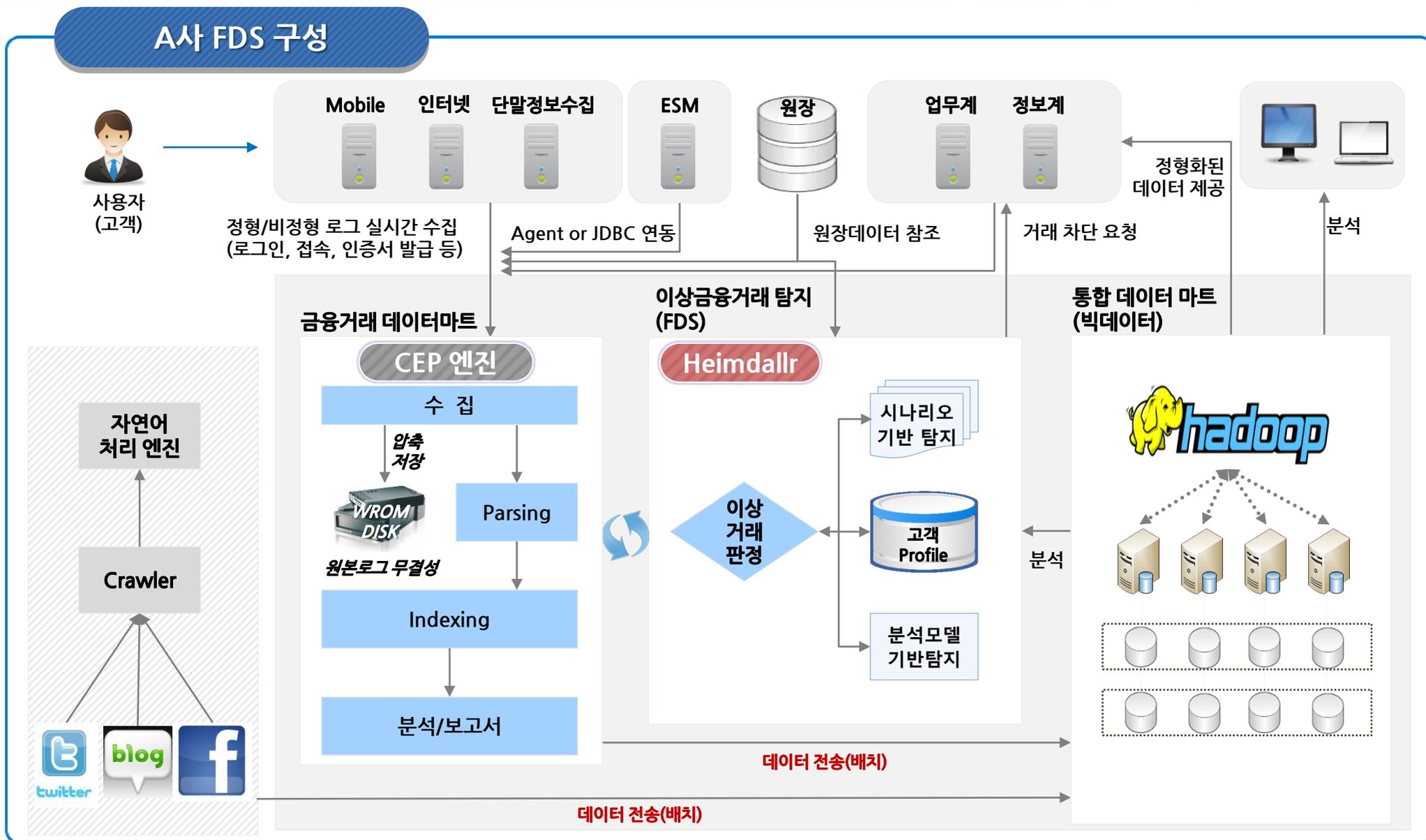
### 금융사기행위 탐지 모델 고도화

- 금융사기행위 탐지율을 높이기 위해서는 전체 고객 거래 데이터를 대상으로 다양한 측면의 과학적 분석 기법 적용 필요

### 업무 변경에 대한 유연한 대응

- 업무 로그와 트랜잭션 로그의 증가 및 변경 시 데이터 처리에 대한 신속하고 유연한 대응 체계 필요

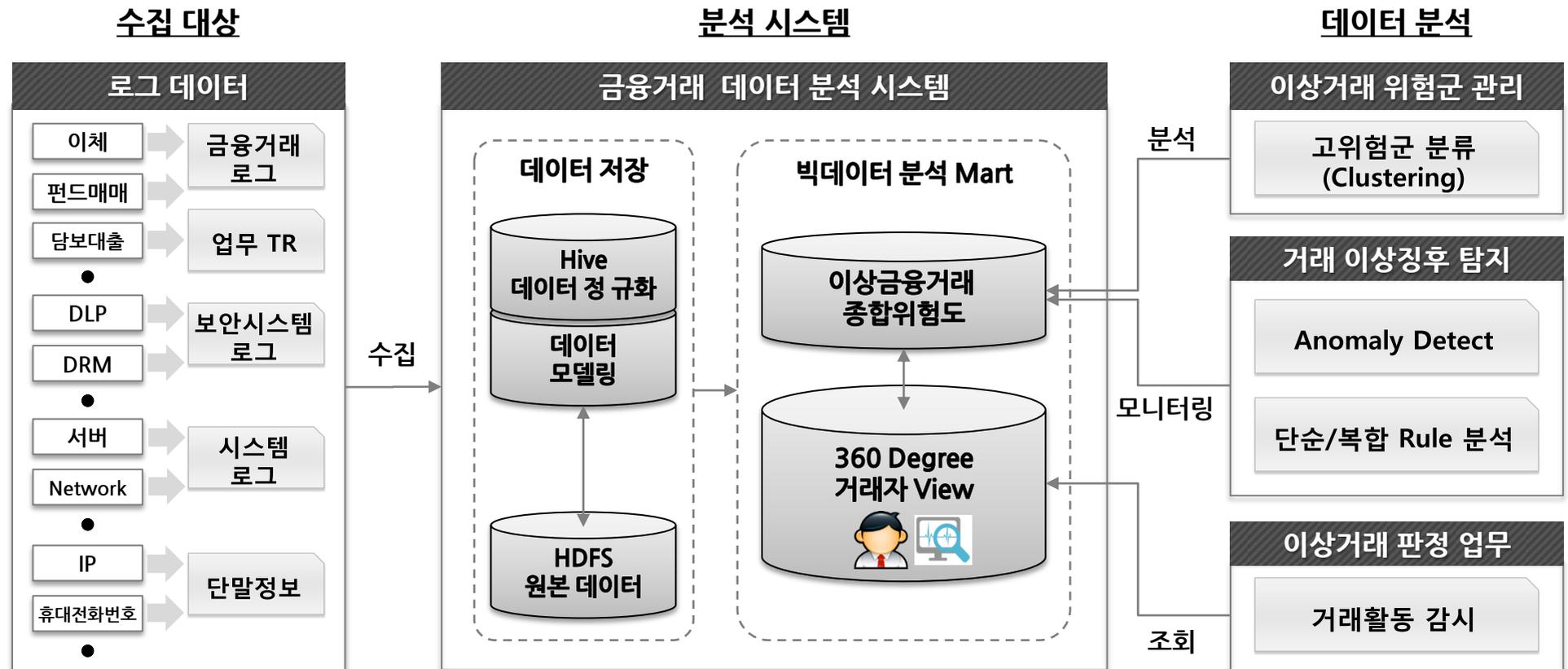
## A사 FDS 구성



## A사 금융거래 분석 플랫폼

다양한 형태의 업무 로그를 수집하여 빅데이터 분석 마트를 구축한 후 고급분석을 통해 이상거래 위험군의 분류 및 거래 이상징후를 탐지하고 이상거래 판정 업무를 지원합니다.

» 이상 금융거래 탐지를 위한 빅데이터 분석



A사 FDS 구축 결과

도입목적

대용량 데이터 저장소 및 분석 인프라 구축

분산 병렬 처리 프로세스를 통한  
장기 데이터 분석 환경 구축

빅데이터 분석 기술을 활용한  
이상금융거래 탐지 고도화

빅데이터 플랫폼 도입

빅데이터 기반  
FDS 구축

도입효과

오픈소스 R 분석 도구를  
활용한 상용 솔루션 대체

상용 고급 분석 솔루션  
초기 도입 비용 **절감**

시나리오 고도화 분석을  
통한 False Alarm 최소화

기존 시나리오  
Detect 탐지 대상  
**약 40% 감소**

사용자 패턴기반 위험도  
등급화를 통한 탐지

이상금융거래의 새로운  
탐지 방법 타당성 확인

과거 이상금융 거래사고의  
패턴과 유사한 현재의 부정  
혐의자를 탐지

탐지모델 고도화 제고

계좌와 계좌간의 관계에서  
이체의 흐름에 중심에 있는  
계좌를 탐지

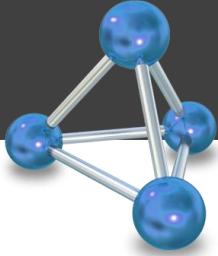
SNA Visualization 분석을  
통해 정량적 파악이 어려운  
신규 패턴 도출



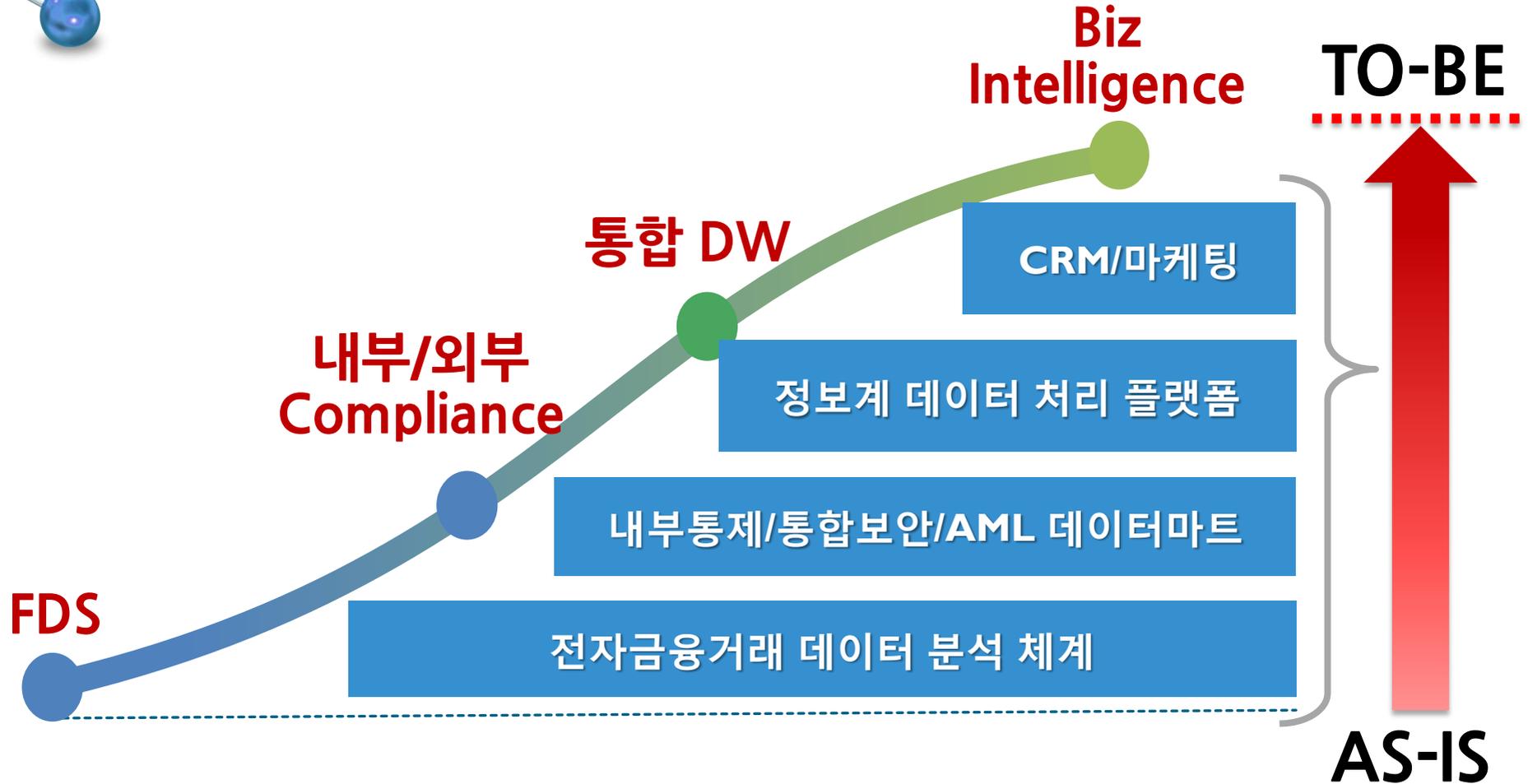
# “Data-driven 기술”과 “고급 분석 역량”을 통한 FDS 고도화가 필요



**“차별화된 FDS 경쟁우위 확보”**



# “전사 데이터 분석 플랫폼으로의 점진적 확장 추세”



  
**THANK YOU**

---

 **동양네트웍스(주)**