

FDS Strategy - BaroFDS 솔루션소개서

성공사례 분석을 통한 효과적인 Fraud Detect System 구축전략

2021. 1


Table of Contents :

Smarter Answer in Fraud Detection

1. FDS 동향	02
2. 성공적인 FDS 구성요소	06
3. BaroFDS 제품소개	15
4. Why BaroFDS?	30

금융시장환경 및 감독기관 요구사항


금융거래채널이 다양화되고 스마트 폰 등의 전자금융수단이 발전함에 따라, 개인정보 유출사고 및 각종 금융 사기가 급증하고 증가됨. 이에 금융감독기관은 금융회사에 자율권을 확대하고 사고 책임 범위를 확대하고 있음



- 스마트기기 영향으로 인터넷뱅킹 뿐만아니라 텔레뱅킹(ARS), ATM 거래 등 다양한 채널을 통해 거래가 증감됨
- 인터넷 뱅킹 33.9%, CD/ATM 41.2%


텔레뱅킹 13.3%, 대면거래 11.6%

거래채널다양화



- 2013.04 IBK직원 정보유출 적발
- 2013.05 손보사 개인정보 유출
- 2013.11 은행대출정보 유출
- 2014.01 카드3사 유출사건
- ...

개인정보유출증가



- 금융사기의 급증 및 지능화
- 금융사기단의 조직화 및 대규모화
- 외국인이 포함된 금융사기 증가
- 날로 발전하는 금융사기 패턴

금융사기증가

금융감독원 FDS 업무추진계획

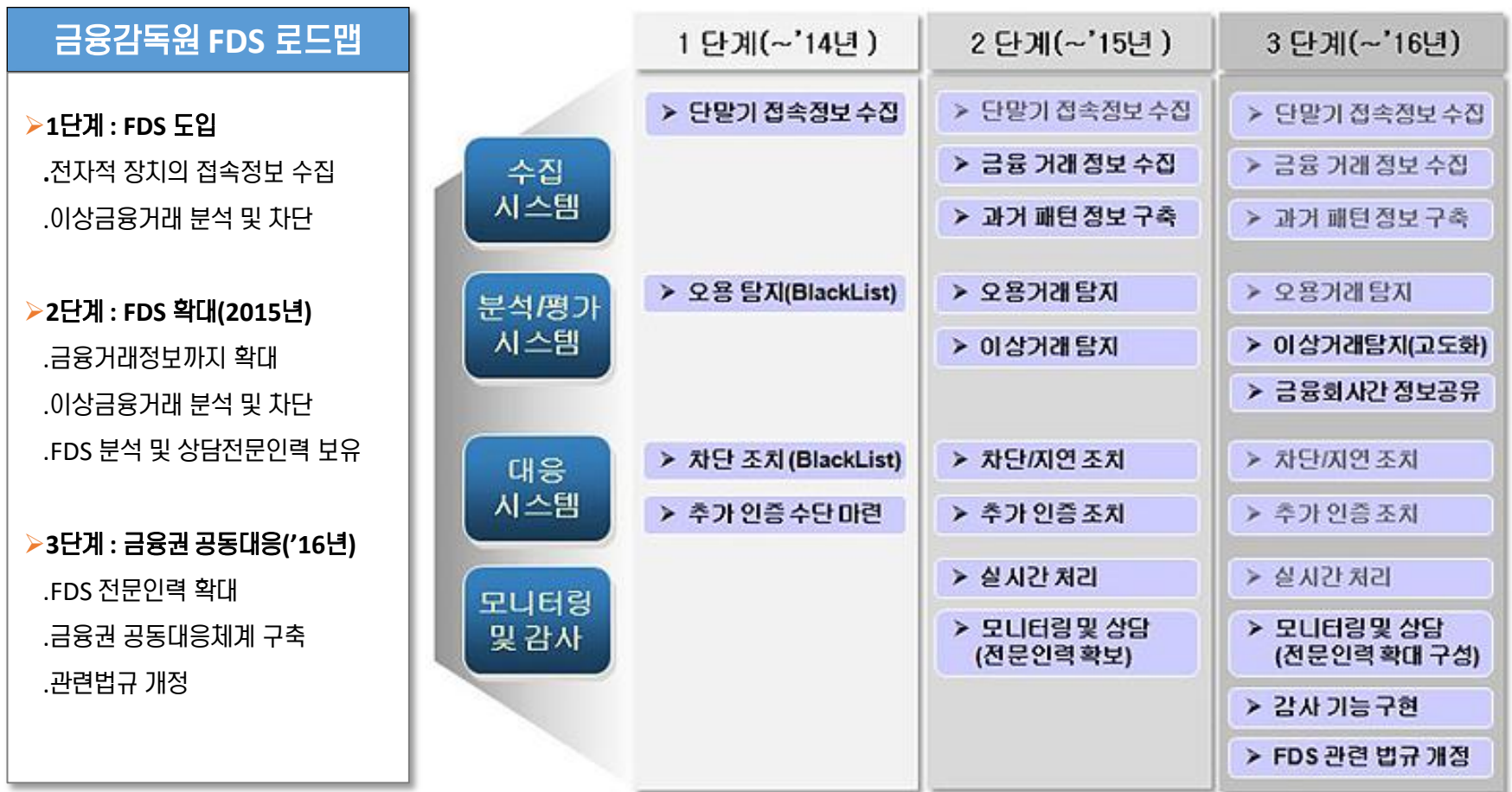
- ① 금융감독원 FDS 로드맵 (14~16년)
 - 1단계: 블랙 IP/MAC 기준 차단(14년)
 - 2단계: 금융거래분석 후 차단(15년)
 - 3단계: 전 금융권 공동대응체계 구축 (16년)

- ② FDS 구축완료 인정 범위
 - 블랙 IP/MAC차단까지는 FDS완료가 아님
 - 지속적인 이상금융거래유형 분석/적용/차단 체계가 구축되어야 완료

- ③ 그 외 금감원 입장
 - 기본적으로 전자금융사기는 금융회사 책임
 - **FDS Rule의 공개를 가용할 수 없음**
 - 15년 상반기에 구축시작 권고

금융감독원 FDS 로드맵 및 가이드라인

특히 2014년 하반기에 발생한 ‘농협 1억2천만 원 인출사고’가 대대적으로 언론에 보도되면서, 일반인들의 금융사고에 대한 관심이 폭증하였음. 이에 14년 12월, 금융감독원은 FDS로드맵을 발표하고 구체적인 구축가이드 라인을 제시하고, 금융사에 FDS 조기구축을 종용하고 있음



2015년 FDS구축동향과 실제 운영 현황

이에 따라 은행을 중심으로 FDS 구축이 활발하게 진행되고 있으며 대부분의 증권사에서 년 내에 FDS를 구축할 예정임.
그러나 실제 구축과 운영에 있어서는 FDS Know-how 부족으로 구축 및 실제 FDS운영에 어려움을 겪고 있음

금융권 FDS 구축동향

- 완료 은행: 신한,국민,농협,외환,하나,우리,씨티,경남,전북,부산
- 예정 은행: 6 개사 예정
- 완료증권사: NH투자,대신,메리츠,미래에셋, 신한금융투자, 유안타, 하이투자증권
- 예정증권사: 24개사 구축 예정

언론 동향

Da 디지털데일리

금융당국, FDS 미구축 금융사에 분쟁조정 시 책임분담 검토

파이낸셜뉴스 김경민 기자 2015.01.14

"보안이 미래다", 증권사 이상금융거래탐지시스템(FDS) 도입 광풍

보안뉴스

2015-01-15 15:41

'파밍' 사기 최초 은행 배상 판결...그 의미와 파장은?

피해자 36명 중 32명에 대해 20% 배상 판결...

구축업체

FDS 실제 현황은?

구축경험이 전무하여 솔루션의 기능만 강조

- 원인#1: 금융거래에 대한 기본적 이해 부족
- 원인#2: FDS 최적 Rule 부재 및 분석 Know-how 전무
- 원인#3: 빅데이터만을 강조함

금융권

구축한 금융사도 대부분 FDS 운영에 어려움을 호소

- 원인#1: 제 기능을 하기 위해서는 오랜기간 지속적인 분석과 경험으로 발전되어야 함.
- 원인#2: FDS 구축 업체에만 의존
- 원인#3: 대부분 금융회사에서는 추진은 보안관련팀에서 하지만 정확한 분석을 위해서는 업무에 정통한 담당자의 참여가 필요하므로 경영진의 적극적 인 의지에 따른 전사적 지원이 필요함

Table of Contents :

Smarter Answer in Fraud Detection

1. FDS 동향	02
2. 성공적인 FDS 구성요소	06
3. BaroFDS 제품소개	15
4. Why BaroFDS?	30

이상거래탐지율이 FDS 성공운영의 지표?

언론에서는 ‘이상금융거래탐지율’이 중요하다고 이야기하고 있으나, 이 지표가 실금융사고예방을 나타내는 지표는 아님. 성공운영의 지표는 전체이상금융거래탐지건수, 실제사고건수, 미탐지건수 등을 종합적으로 살펴야 함.

금융범죄 방지 'FDS' 효과 특특

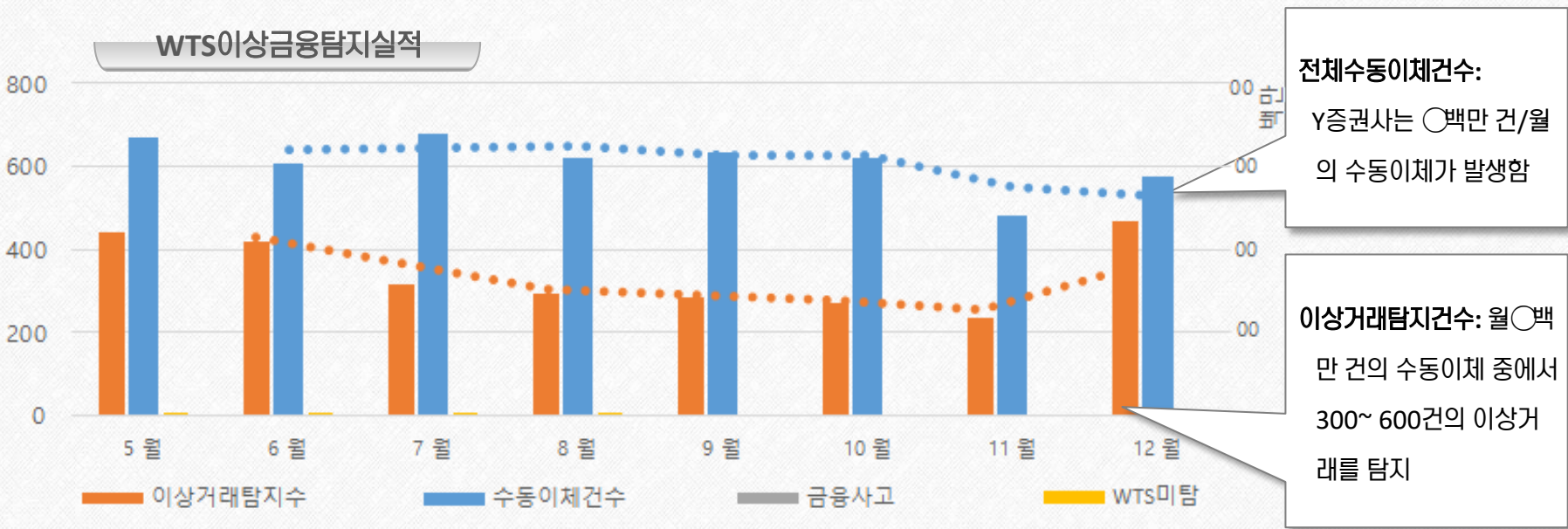
“도입이후 이상거래 70%이상 잡아내”
하나·신한·부산銀 이어 농협도 도입

최근 신종금융범죄가 잇따르면서 '이상금융거래탐지시스템' (FDS) 고도화 작업도 병행된다. 하지만 아직 은행들의 FDS 도입비율은 미미한 상황이다. 그만큼 은행들이 금융범죄 대응에 소홀했다는 방증이다. 하지만 선제적으로 FDS를 도입한 은행들은 FDS의 효과를 톡톡히 보는 것으로 나타났다. 금융당국까지 나서 시중은행들에 FDS 도입을 강조하는 이유다.

15일 금융권에 따르면 하나은행의 지난달 이상금융거래 탐지율은 71.7%를 기록했다. 전체 이상금융거래 중 70% 이상을 걸러낸다는 의미다. 하나은행이 FDS를 도입한 것은 지난 10월. FDS 도입을 전후해 이상금융거래 탐지율이 두드러지게 향상됐다. 실제로 하나은행의 지난 1월 이상금융거래 탐지율은 24.8%에 그쳤다. 이후 꾸준히 탐지율이 높아졌지만 지난 8월까지만 하더라도 50%를 넘지 못했다. 당장 농협은 이번주 중에 FDS 도입을 완료할 예정이다. 농협은 1월 1일부터 FDS 도입을 시작했다. 농협은 1월 1일부터 FDS 도입을 시작했다. 농협은 1월 1일부터 FDS 도입을 시작했다.

지난달 이상금융거래 탐지율은 71.7%를 기록했다. 전체 이상금융거래 중 70% 이상을 걸러낸다는 의미

- 14.12.16 머니투데이 기사 -
- 하나은행의 이상거래탐지율이 71.7%라고 언급
 - 그렇다면 나머지 28.3%는?
- ➔ 이상금융거래탐지율이 실효적으로 이상거래를 예방하는 지표로 인식하기 어려움



이상금융거래의 정의 및 핵심지표

FDS시스템 운영 관점에서 '이상금융거래'의 명확한 정의는? FDS시스템에서는 FDS룰을 통해서 탐지된 이상금융거래 중에서 실제 금융사고발생 여부에 따라 **정탐/오탐**으로 나뉨. 또한, FDS에서 **미탐**(탐지하지 못한 금융사고)도 이상금융거래의 범주로 포함되므로, 정탐률을 높이고 미탐률을 0%에 가깝게 운영하는 것이 시스템 방향성임.



FDS 성공사례: 모금용기관

2006년 시작된 보이스피싱은 2010년대 초반부터 파밍, 메모리해킹, 스미싱 등 신종전자금융사기수법과 맞물려 진화하고 있음. 대부분 금융사는 이에 대응할 시스템도 갖춰져 있지 않는 상황이나 모금용기관은 금융사기를 거의 완벽하게 방지하고 있음. 모금용기관 사례에서 **성공적인 FDS 구축의 중요 요소를 확인**하는 것이 필요

http://s1332.fss.or.kr/fss/kr/acro/free/fssbbs_view.jsp?seqno=131943&no=80&page=1&menu=squ040000

금융감독원 금융민원 소비자정보 참여마당 금융법규 업무자료 보도홍보 금융감독원

금융정책제안 | 국민검사항구제도 | 금융회사참여마당 | **자유게시판** | 금융범죄/비리/기타신고 | 공익신고 | 직원선정-불선정제보 | 뉴스레터신청 | 금융소비자리포트 | 장내파생상품보고 | 공매도포지션보고 | Q&A

금융소비자의 참여공간입니다. 국민여러분의 소리에 귀 기울이는 열린 금융감독원이 되겠습니다.

Home > 참여마당 > 자유게시판

참여마당

- 금융정책제안
- 국민검사항구제도
- 금융회사참여마당
- 자유게시판**
- 금융범죄/비리/기타신고
- 공익신고
- 직원선정-불선정제보
- 뉴스레터신청
- 금융소비자리포트
- 장내파생상품보고
- 공매도포지션보고
- Q&A

자유게시판

제목	유안타증권 IT운영팀 양운혁님 감사합니다.
조회수	604
첨부파일	

유안타증권 IT운영팀 ○○○ 님 감사합니다.

너무나 감사하는 마음에 글을 올립니다. 제가 11월 7일날 보이스피싱을 당했습니다. 알고도 당할수 있다고 얘기는 들었지만 설마 내가 당하겠어~ 당하는사람이 바보지라고 생각하던 제가 어처구니 없게 당했습니다.

... 중략 ...

근데 ○○, 유안타증권 똑같이 얘기를 해줬는데~~
○○은 막아내지 못하고, 유안타증권에서는 잘 막아줘서 피해가 없었습니다.
○○은 조금 불안한 곳이라 많은 돈이 오고가는 거래는 하지 않았지만
그래도 아주 오래전부터 거래를 해왔는데~
역시나 기대를 저버리고 실망을 안겨주었습니다.
앞으로 ○○은 거래를 하지 않을 생각입니다.

반면 유안타증권에서는 제가 보이스피싱당하고 있다는 걸 눈치채고
모든걸 차단하고 계속 문자와 전화를 해주었습니다.
그래서 저도 눈치를 채고 경찰에 연락을 하고 피해없이 마무리를 할 수 있었습니다.
당황해서 어찌할 바를 모르던 저에게 계속 걱정을 하면서 연락을 해줘서 너무 감사합니다.

앞으로도 유안타 증권 많이 이용하겠습니다.
특히 유안타증권 IT운영팀 ○○○님 감사합니다.

**금융사기방지는
더 이상 보안업무만이
아니라,
고객만족과 고객유치에 지대
한 영향을 미침!!**

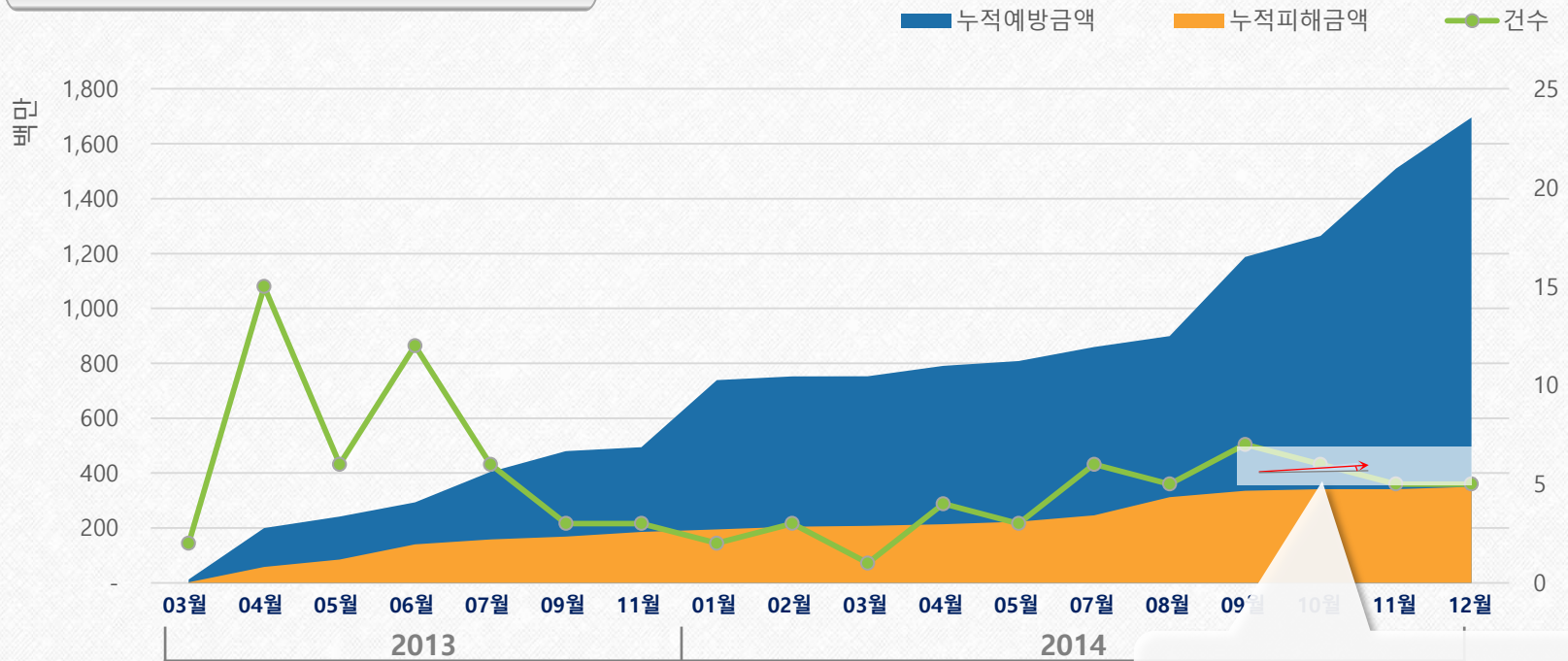
2014-11-07
○○은행과 모금용기관에 계
좌를 가지고 있던 고객이 보
이스피싱을 당한 경험을 등록
한 글로 모금용기관을 통해
금융사기를 방지할 수 있다는
내용과 감사인사를 등록.

성공적인 FDS요소 #1: RULE(1/2) – 운영실적과 FDS RULE

13년 03월 FDS도입한 Y증권사는 2년간 총 94회를 실제금융사고를 탐지, 이중 약 17억 원 규모의 금융사기를 예방함.

또한 **이상금융탐지 Knowhow(FDS RULE)가 축적**될 수록 피해금액이 거의 없어지는 추세를 보이고 있음

Y증권사의 WTS FDS 운영실적 추이



피해증가추이 1.4%

94 회 실제금융사고건수

2년간 실제 발생한 사고건수. 운영초기에 많은 시도가 감지되었음.

1,695 백만원 피해방지금액

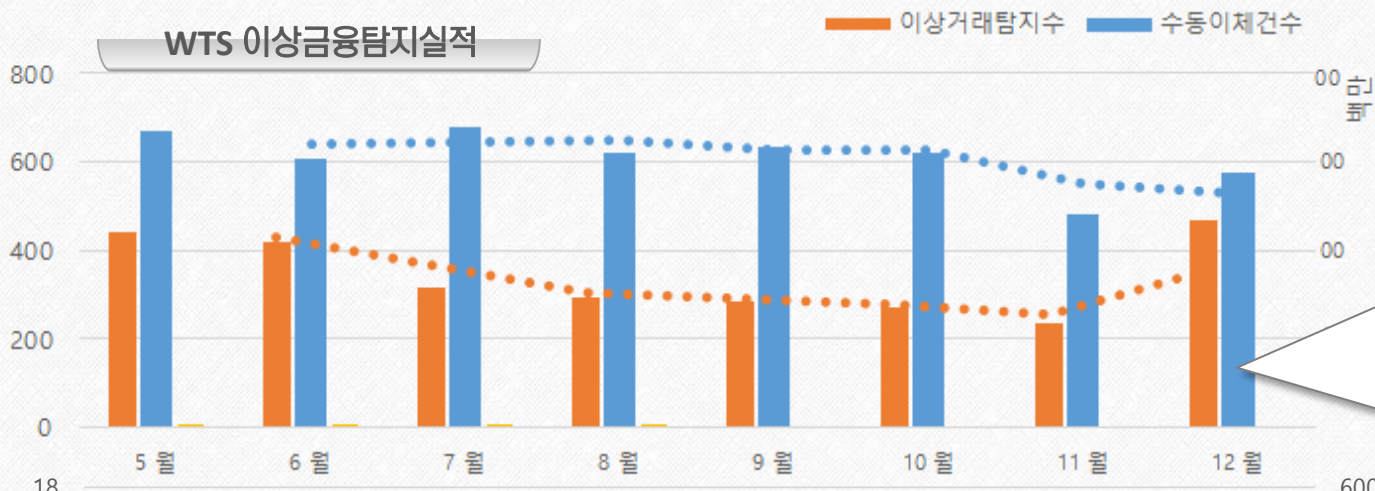
2년간 총 94회의 금융사기에서 약 17억 규모의 피해를 예방함

1.4% 피해증가율('14.9~12)

14'9월 FDS안정화 이후, 피해가 거의 발생하지 않는 추세를 보이고 있습니다.

성공적인 FDS요소#1: **RULE**(2/2) – RULE과 핵심지표의 상관관계

FDS는 수백만 정상거래 중에서 **0.0004%의 사고를 탐지**해야 함. **'백사장에서 바늘찾기'** 보다도 더 어려운 업무로 Rule 이 고도화될 수록 미탐을 0%에 가까워지고 정탐률은 높아지는 상관관계를 가짐.

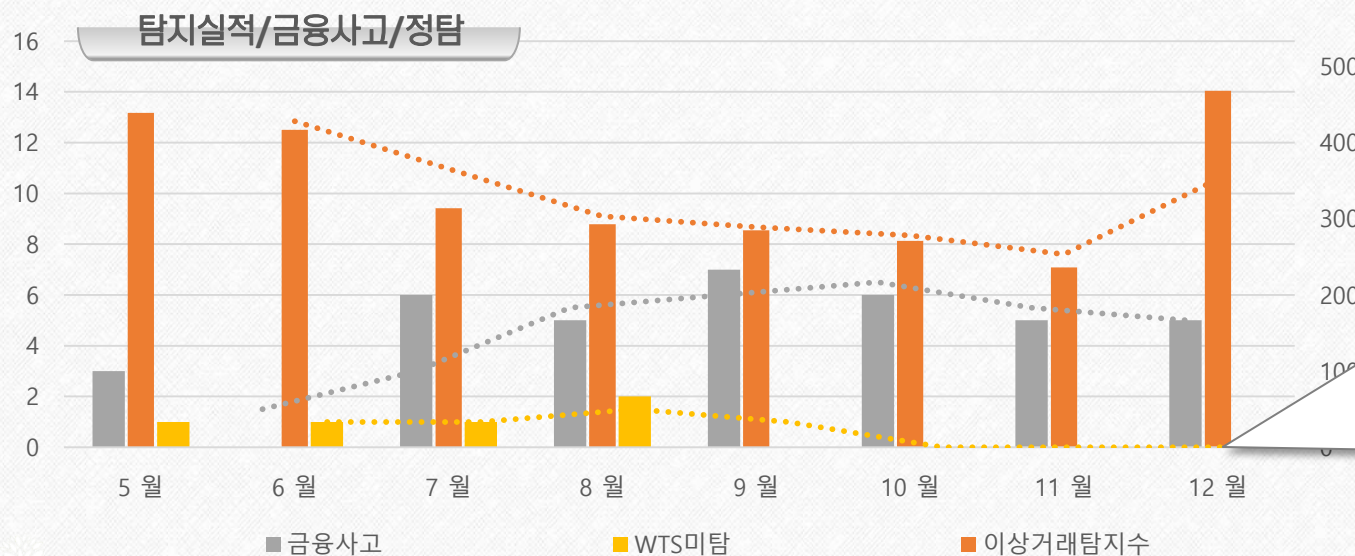


14.05~12(8개월) FDS운영실적

- 수동이체 ○ 백만건/월
- 이상거래탐지 400.7건/월
- 실제금융사고 5.1건/월
- 미탐 0.625건/월

전체금융거래대비 비율

- 정상거래비율 99.968%
- 이상거래로 탐지된 건수비율 0.032%
- 실금융사고비율 0.0004%
- 실미탐비율 0.00005%



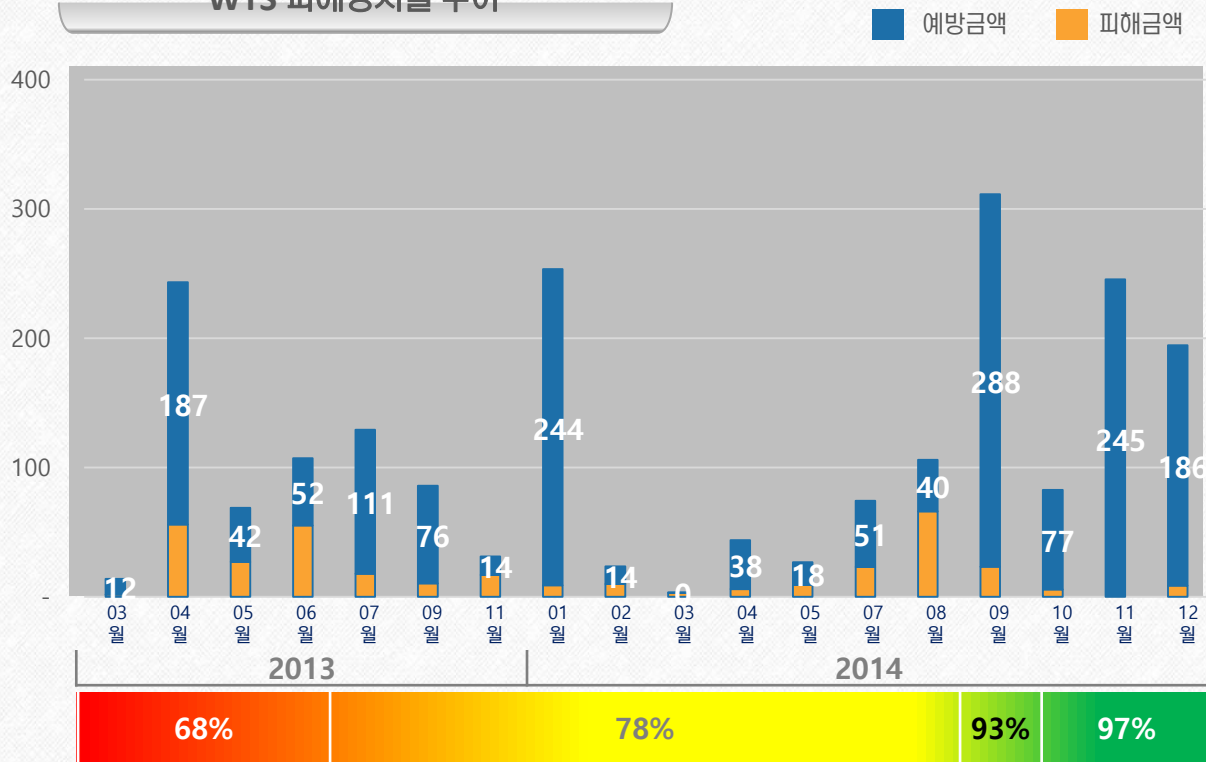
- 핵심은 이상금융거래탐지율이 아니라, 탐지하지 못한 **미탐률** 및 **실정탐률**이 중요!
- 미탐률 0%**는 모든 이상징후 탐지하고 있음을 의미
- 정탐률↑ 상승** 의미는 금융 사고방지↑, 업무효율성↑

➔ RULE이 고도화될수록 정탐↑, 오탐/미탐 ↓

성공적인 FDS요소#2: 사전차단 – 사전차단과 피해방지율

운영 초기, FDS운영 know-how 부족으로 사기 피해방지율이 67% 수준에 불과했음. 2014년 09월 금융사기근절을 위한 특단 조치로 이상거래로 탐지된 건에 대해 **사전차단 룰을 banking시스템에 적용**하여 97%대 수준으로 UP↑

WTS 피해방지율 추이



년	월	금융사고 시, 방지율	비고
2013	3	68%	FDS 시스템 오픈
	4		
	5		
	6		
	7		
2014	9	78%	의심거래 부가인증
	11		
	1		
	2		
	3		
	4		
	5		
	7		
	9	93%	사전차단
	10	97%	Rule 강화
	11		
	12		
12			

68% FDS 초기 운영시기 (초기)

FDS초기 운영 시에는 금융사고 대응에 대한 경험이 적어서 금융사고가 진행 중에 사고를 인지하는 경우가 많았음..

78% 의심거래 부가인증 시기

운영초기, 사고는 감지되었으나 피해예방 효과가 원하는 수준까지 이르지 않았기 때문에 이를 보완하기 위해 '의심거래에 대한 부가인증' 체계로 전환하였습니다. 초기에 성과는 얻었으나 여전히 만족스러운 수준은 아니었음.

97% Rule 강화 및 사전차단

14년 9월, banking에 사전차단룰을 적용하고 추가 Rule 반영하여 방지율이 93% 수준으로 높아져서 2014년 말에는 97%수준으로 피해방기가 높아지고 있음

성공적인 FDS#3요소: 이상거래탐지 후 금융사고대응체계

이상금융거래징후 탐지 후에는 금융사고를 줄이기 위해서는 대응체계가 필요. ① 이상금융거래징후탐지 시, 금융거래를 차단시키고 ② 고객(피해자)에게 이상거래에 대한 내용을 즉시 통보 ③ 고객에게 직접 통화하여 혹시 사기범에 현혹되었을지 모를 고객에게 상황을 인식시켜야 함. 즉, FDS는탐지 뿐만 아니라, 즉시 대응하는 시스템이 매우 중요.

금융감독원 자유게시판

자유게시판

http://s1332.fss.or.kr/fss/kr/acro/free/fssbbs_view.jsp?seqno=131943&no=80&page=1&menu=squ040000

제목 유안타증권 IT운영팀 임을석님 감사합니다.

조회수 604

유안타증권 IT운영팀 ○○○ 님 감사합니다.

... 중략 ...

반면 유안타증권에서는 제가 보이스피싱당하고 있다는 걸 눈치채고 모든걸 차단하고 계속 문자와 전화를 해주었습니다.

당황해서 어찌할 바를 모르던 저에게 계속 걱정을 하면서 연락을 해줘서 너무 감사합니다.

그래서 저도 눈치를 채고 경찰에 연락을 하고 피해없이 마무리를 할 수 있었습니다.

앞으로도 유안타 증권 많이 이용하겠습니다.
특히 유안타증권 IT운영팀 ○○○님 감사합니다.

대응절차#1
이상거래징후 탐지

대응절차#2
이상거래에 대한 고객통보
(SMS, 전화)

대응절차#3
통화 및 고객설득

대응절차#4
고객의 사후처리 안내

성공적인 FDS의 핵심구성요소

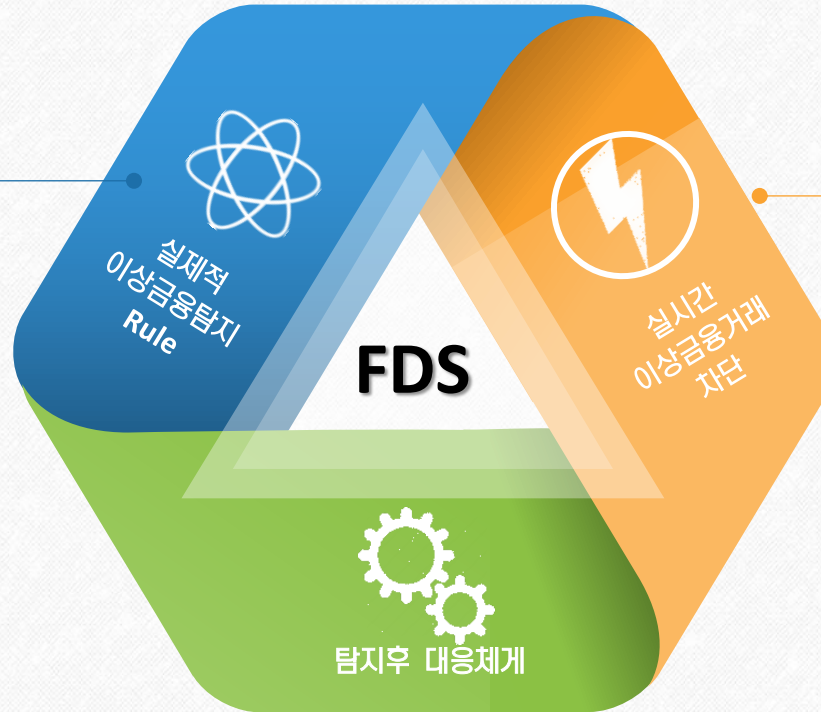
FDS구축에는 다년간의 축적된 FDS Knowhow가 필요함. 만약, 이런 운영을 최소화하면서도 **구축 즉시 성과를 내는 시스템**을 도입하려면 금융사고 대응경험에 기반한 **FDS Rule** 필수임. 또한, 탐지 즉시 사전차단이 가능한 초고속 Infra가 구 성되어야 하며, 사건 발생 후 이에 대응할 수 있는 사고대응체계가 구비되어야만 성공적인 운영이 가능!!!

FDS Rule

이상금융거래탐지 경험 지식 필요

FDS 시스템이 도입 후, 즉시 성과를 내기 위해서는, 이상금융거래 탐지에 대한 노하우가 확보되어야 함.

핵심은 FDS Rule !



FDS Response System
금융사고대응체계

차단 후, 빠르고 체계적으로 대응하는 것이 중요

함. **FDS 금융사고대응체계!**

Real-time

Transfer Block

이상금융거래의 실시간 차단

이상금융거래탐지 시, 이체 전에 차단이 되어야 금융사고가 예방됨. 즉, 초고속인프라가 필수임.

**실시간 차단을 위한
초고속 인프라!**

Table of Contents :

Smarter Answer in Fraud Detection

1. FDS 동향	02
2. 성공적인 FDS 구성요소	06
3. BaroFDS 제품소개	15
4. Why BaroFDS?	30

BaroFDS 소개

BaroFDS는 이상금융거래탐지 및 대응업무에 대한 **모금융기관의 2년간의 Know-how**을 바탕으로 개발된 금융권 유일의 검증된 FDS 솔루션으로서 복잡한 금융권 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있음.



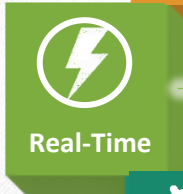
1. 현장에서 검증된 FDS Rule

2년간 모금융기관에서 운영된 FDS Rule 을 적용하여
즉시 현장 FDS적용 및 운영이 가능



2. 실시간 로그 수집 가능

다양한 환경에서도 간단한 환경 설정만으로도 쉽게 실시간 로
그수집이 가능하여, 복잡한 금융시스템환경에 적합



3. 실시간 사전차단 구현

In-Memory 기반 아키텍처로 설계되어, 이상금융거래탐지 즉
시 사전차단이 가능함.



4. 축적된 사고대응체계

2년간 현장 경험으로 축적된 대응체계가 시스템화 되어, 금
용사고 대응 및 처리가 용이합니다.



5. Rule Audit & Simulation

발생되는 미탐을 분석하여 신규 Rule을 만들고, 파라미터 조
정을 통하여 정탐을 높이는 룰 최적화를 손쉽게 실현

BaroFDS

어떤 환경에서던 각종 로그를

실시간 수집분석하여

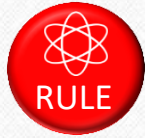
이상금융거래탐지 즉시,

사전차단이 가능한

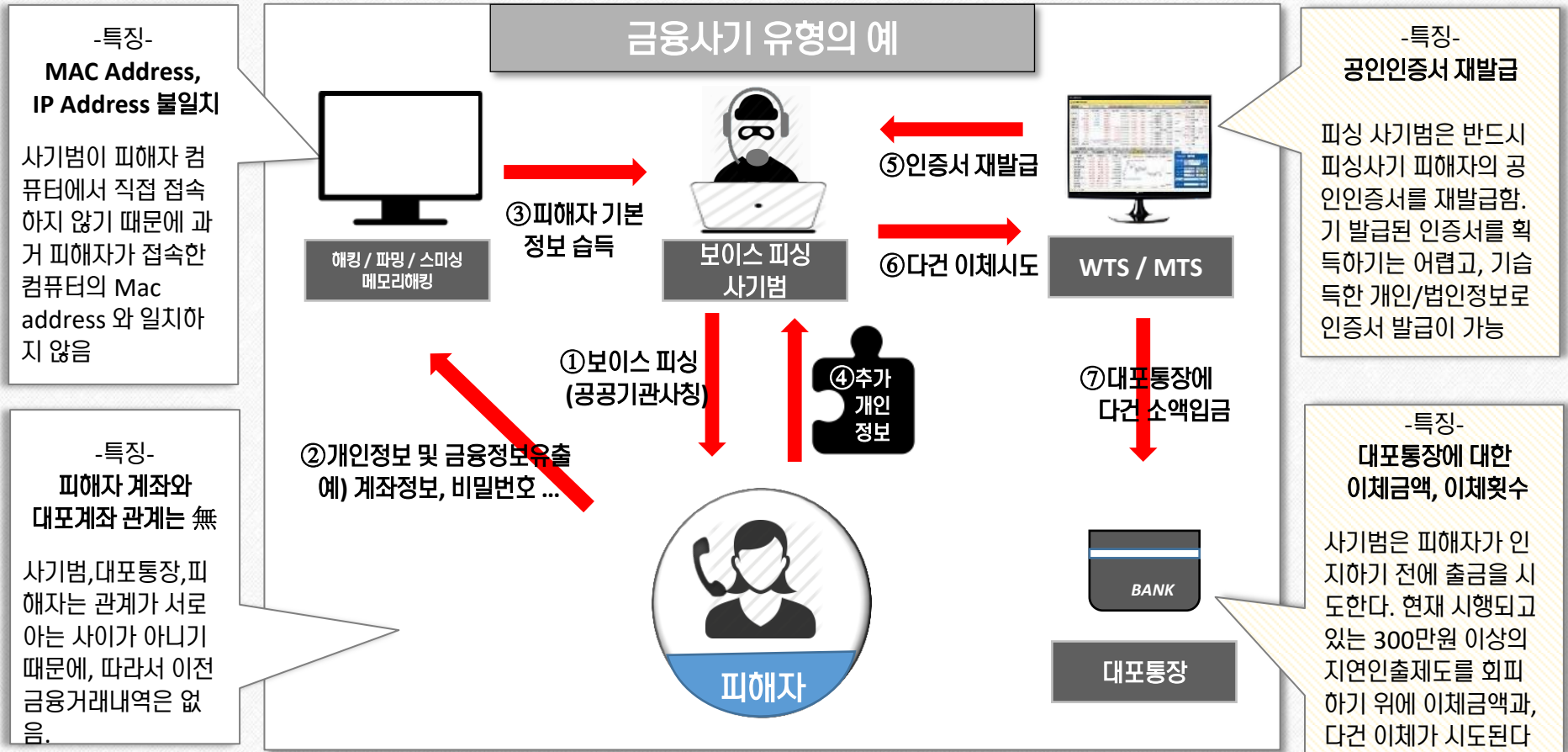
금융권의 유일의 검증된

Fraud Detection System

특징점#1 Rule(1/3) -이상금융거래의 특징과 이해



금융사기는 해킹/파밍 등으로 통한 피해자 대상자의 기초정보를 습득하고, 보이스피싱을 통하여 최종 정보를 획득하여 사기범죄를 실행. 이런 행위는 일상적인 행동과는 다르기 때문에, 이 패턴이 기록된 로그를 분석하면 탐지할 수 있는 이상금융거래인자의 도출이 가능하고 이를 조합해 Rule 구성이 가능.



실제 금융사기범이 수집한 개인정보



아이핀 계정 정보 (약 15건)

아이핀: 비번:

아이핀: 비번:

이동통신사 계정 (약 6건)

pi:

개인이 자주 사용하는 पास: **보이스 피싱에 관련된 정보도 다량 수집되어 있었다**

자주쓰는비밀번호:

kong07
kongkong7
kongkong7~
ahkrwl7616~
q1w2e3r4
as9595
as3037
kongkong07
park5591

대출정보 (약 627명 정보)

이름	D 주민번호	성 유대폰	주소	대출구분	직상명	지점	접수일시	처리상태
이민	7	이	경기	사업자				오로
이민	8	이	서울	직장인				오로
이민	9	이	경기	직장인				오로
이민	0	이	경남	직장인				오로
이민	1	이	경기	직장인				오로
이민	2	이	충북	직장인				오로
이민	3	이	강원	직장인				오로
이민	4	이	서울	직장인				오로
이민	5	이	경기	주부				오로
이민	6	이	경기	직장인				오로
이민	7	이	경기	직장인				오로
이민	8	이	경기	직장인				오로
이민	9	이	경기	직장인				오로
이민	0	이	경기	직장인				오로
이민	1	이	경기	직장인				오로
이민	2	이	경기	직장인				오로
이민	3	이	경기	직장인				오로
이민	4	이	경기	직장인				오로
이민	5	이	경기	직장인				오로
이민	6	이	경기	직장인				오로
이민	7	이	경기	직장인				오로
이민	8	이	경기	직장인				오로
이민	9	이	경기	직장인				오로
이민	0	이	경기	직장인				오로

와 같이 저장되어 있었다

위와 같이 패스워드 패턴 추출

사용자들이 자신의 어떤 신체

자신의 개인 정보들을 조합하

인증기능 정보 (

카드 번호, 카드

카드번호
비밀번호
카드종류



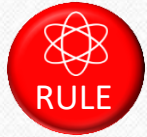
없음 확인리본은 가능 필요 없음 비밀번호만 노출 하면 가능

이러한 패턴은 흔하지 않지만 오해의 소지가 있습니다

통신사별 착신하는 방법과 필요한 서류, 그리고 착신된 전화로

인증 가능한 은행 등의 정보들이 저장되어 있다

특장점#1 Rule(2/3) – 이상금융거래탐지인자



BaroFDS에서는 이상금융거래징후를 찾아낼 수 있는 Value를 이상금융거래인자라고 지칭. 이런 인자들을 개별적/평면적으로 조사하는 것으로는 사기예방이 어려움. 인자들을 발생빈도나 범죄형태에 따라 체계적/구조적으로 조합하는 것이 중요하며 이를 어떻게 조합하느냐에 따라, 오탐/미탐이 결정됨

FDS 실운영을 통해 확인된 약 40 여개 이상금융거래인자 확보



이상금융거래탐지 인자 피라미드

특장점#1 Rule(3/3) – 조합된 인자기반 FDS RULE SET



FDS RULE은 여러 가지의 이상금융거래인자가 조합되어 구성됨. 실제 고객의 사용환경 및 행동패턴에 대한 축적된 로그를 기반으로 룰을 만들고, 사기건의 환경/패턴에서 이질성을 감지하여 이상금융거래를 탐지함

실제 RULE SET	#1 現수신된 ID의 IP와 mac 주소가 로그인 Table에 t-1일(전일) ~ T -365(전일) 에 없으면 비정상 #2 現수신된 ID의 IP 또는 mac 주소가 해외IP면 비정상임 #3 現수신된 ID의 접속매체가 로그인 테이블에 t-1(전일) ~ T-365(전일) 에 없으면 비정상임
-------------------	---



금융패턴 ① 동일PC 접속 ② 국내에서만 사용

IP address 123.45.0.137

mac 00:23:6C:7F:38:43

③ WTS로만 접속



IP address 202.113.0.XXX

mac 00:A0:CC:23:AF:4A

© HTS로 접속

사기범 환경 ㉠ 신규PC ㉡ 중국에서 접속

Login Table

	IP address	MAC
01/09	123.45.0.137	00:23:6C:7F:38:43
01/11	123.45.0.137	00:23:6C:7F:38:43
01/13	123.45.0.137	00:23:6C:7F:38:43
01/24	123.45.0.137	00:23:6C:7F:38:43
01/25	123.45.0.137	00:23:6C:7F:38:43
⋮	⋮	⋮
01/26	202.113.0.XXX	00:A0:CC:23:AF:4A

	Channel	IP Range
01/24	WTS	123.45.X.X KOR
01/25	WTS	
⋮	⋮	
01/26	HTS	202.113.0.XXX CHN

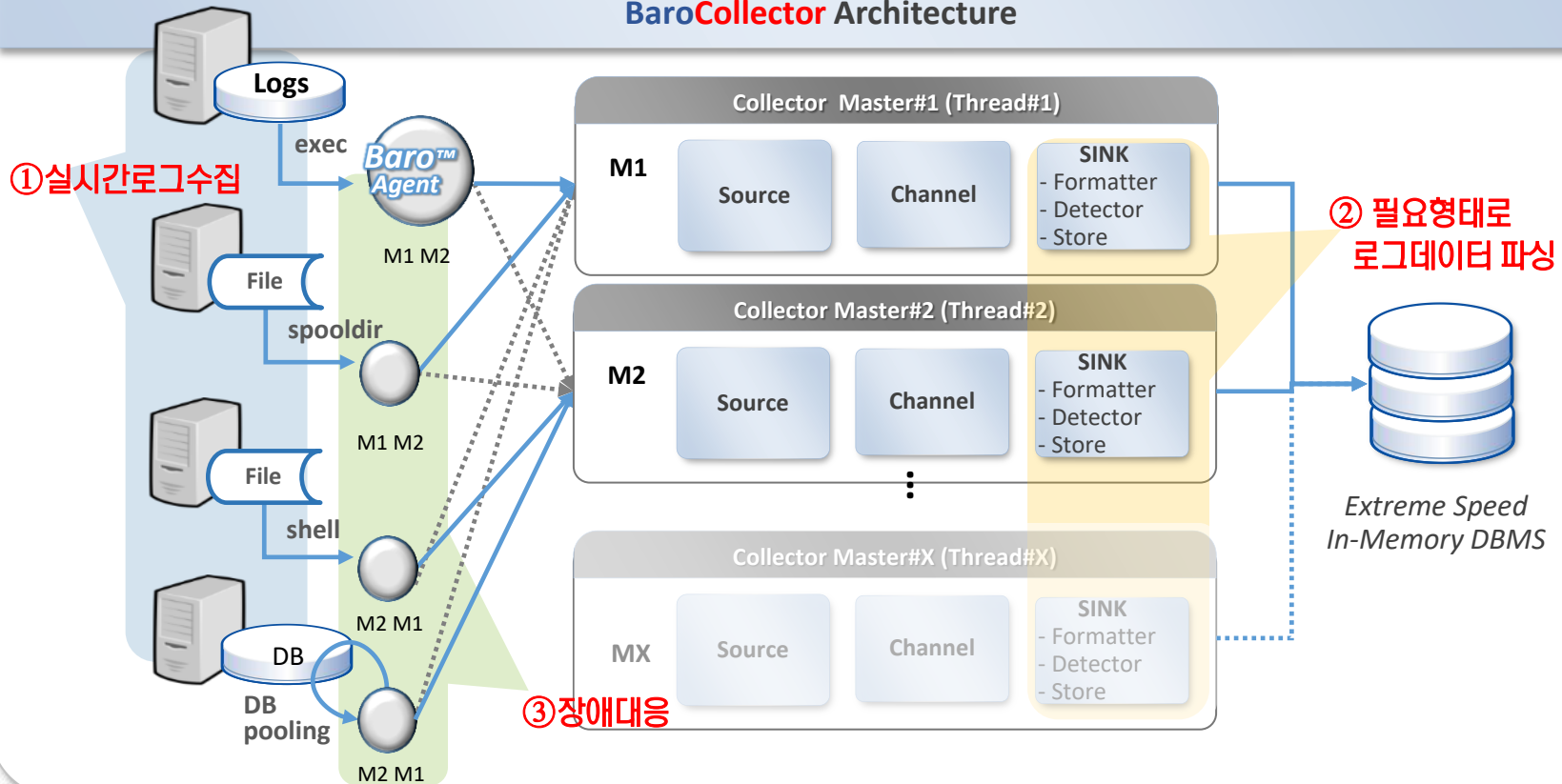
특장점#2 다양한 Platform을 지원하는 Log-Collector



FDS의 또 다른 핵심은 기존업무에 변경을 거의 주지 않고 로그를 실시간으로 수집하고, 이를 필요한 형태로 저장이 가능해야 함. **BaroFDS**는 J2EE기반의 Collector로 어떤 환경에서 즉시 로그수집이 가능함

- ① 실시간로그수집: 환경변수 설정만으로 Source 종류에 상관없이 실시간으로 수집 가능
- ② 필요형태저장: 로그포맷터를 보유해 환경변수만으로도 비정형/정형에 상관없이 원하는 형태로 저장가능
- ③ 부하분산: 순차적 배분(Round Robin), 동적배분(Random) 가능
- ④ 장애대응: 장애 시 이를 감지하여, 다른 Thread (또는 다른 Instance)로 대체 및 비정상 종료시 재기동으로 안정적 수집 가능

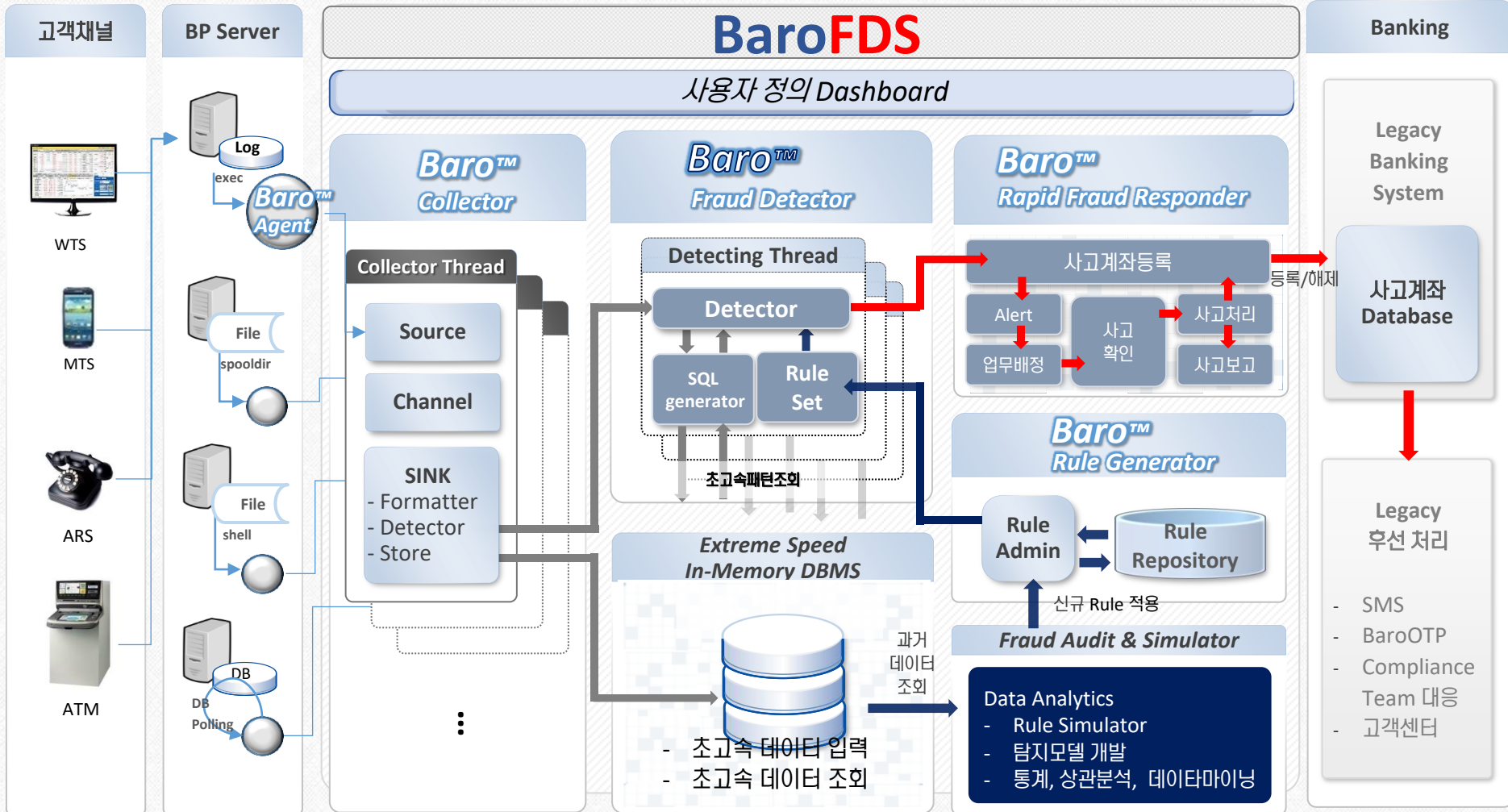
BaroCollector Architecture



특장점#3 초고속 인-메모리 아키텍처 (1/2)



BaroFDS는 극초고속 인메모리 기반 아키텍처로 설계되어, 이상금융거래인자를 기반으로 각종 로그발생 후 고객의 과거의 금융 프로파일을 빠른 시간에 분석 대조하여 이상거래징후를 탐지하고 거래를 차단함





이상징후탐지는 현재 패턴과 고객의 과거금융이력을 비교하여 상이성을 찾는 것이 핵심. 예로, 고객께서 127.168.*.* IP주소에서 과거에 한번이라도 접속했는지를 빠르게 검색한다면, 이상징후를 즉시 확인할 수 있음. 즉, 이상금융거래인자와 RULE을 극초고속으로 비교분석하는 것이 사전차단의 핵심임.

BaroFDS의 Query Performance

특정 대역대의 ip 주소를 특정 날짜에 대해서 검색 : **0.03초**

```
select hts_id from tb_item
where con_date = to_date('2015-01-05',
'YYYY-MM-DD') and ipv4 like '127.168.%.'
count(*)
```

86,267

[1] Row Selected

Elapsed Time : **0.03**



S사 - Search Performance

특정 대역대의 ip 주소를 특정 날짜에 대해서 검색 : **3.35초**

```
search tb_item con_date=2015-01-05 AND
ipv4=127.16.*.* | table hts_id
count(*)
```

86,267

[1] Row Selected

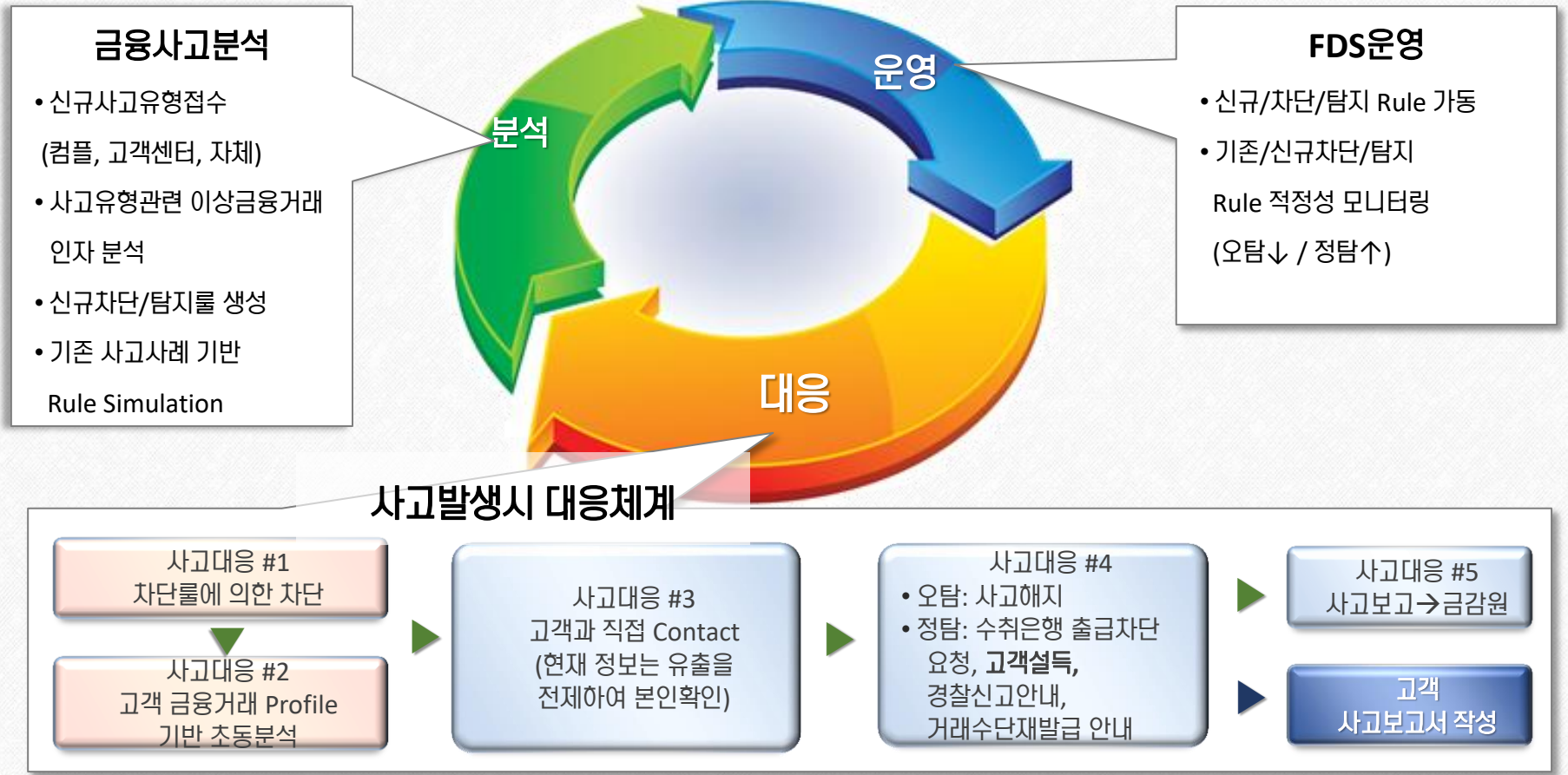
Elapsed Time : **3.35**



특장점#4 체계화된 FDS PROCESS (1/2)



이상금융거래탐지는 지금까지의 금융업무와는 전혀 다른 업무로, 진화하는 금융사기범들의 사기수법을 지속적으로 모니터링하고 이를 FDS에 반영해야 함. **BaroFDS**는 모 증권사에서 검증된 체계를 기반으로 운영되어, 분석→운영→대응이 선순환으로 운영되어 계속 변화하는 금융사기에 효과적 대응이 가능

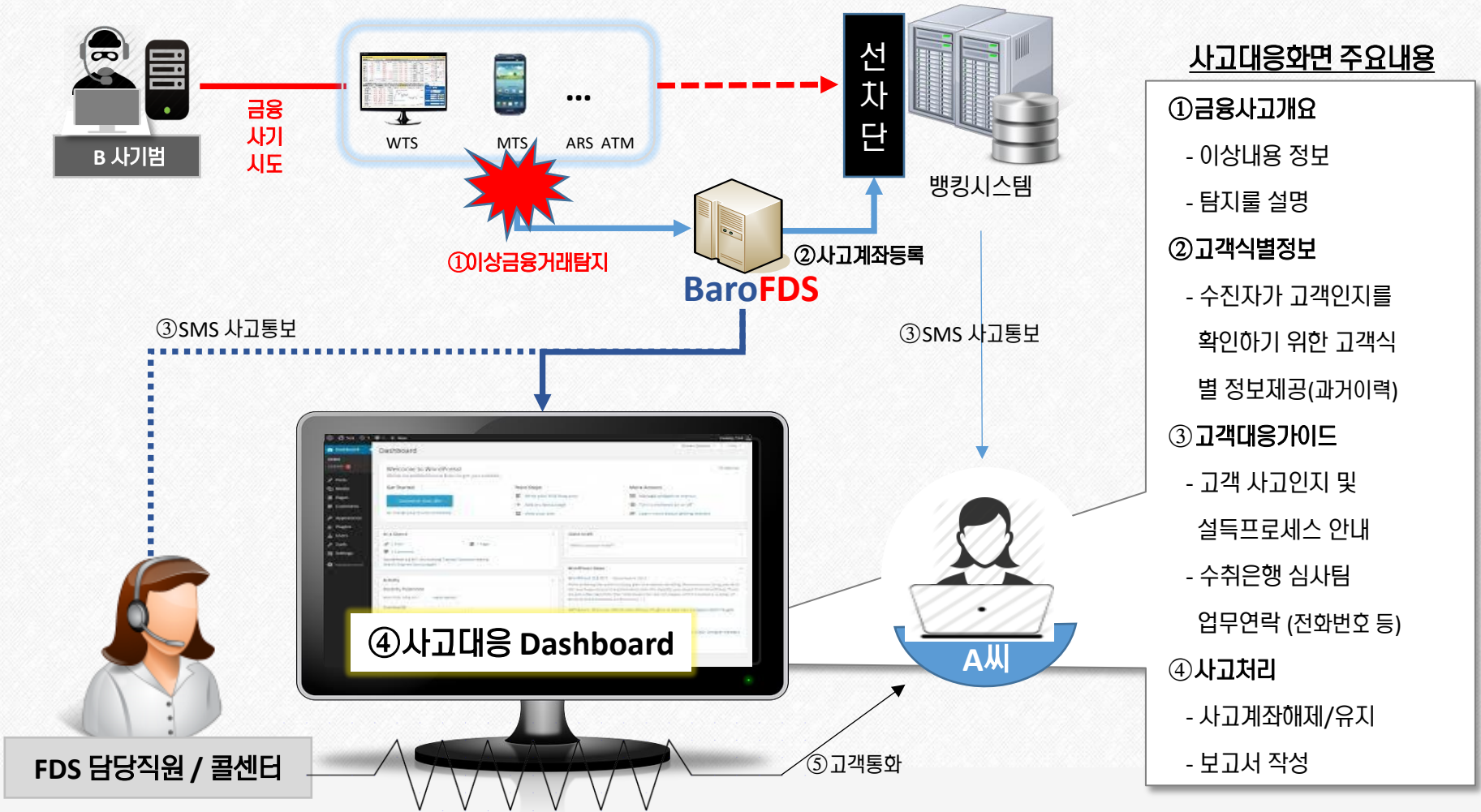


특장점#4 체계화된 FDS PROCESS (2/2)



고객이 보이스피싱을 당하고 있을 경우, 사기범의 농간으로 대부분 정확한 상황인지를 못하고 있음.

BaroFDS는 주요 이상거래탐지 시, 즉시 거래를 차단하고 FDS담당직원 및 고객에게 사고를 SMS 안내함. 또한, FDS담당직원에게 사고대응 및 처리를 위한 1 point view를 제공하여 즉시 사고대응이 가능



사고대응화면 주요내용

- ① 금융사고개요
 - 이상내용 정보
 - 탐지를 설명
- ② 고객식별정보
 - 수신자가 고객인지를 확인하기 위한 고객식별 정보제공(과거이력)
- ③ 고객대응가이드
 - 고객 사고인지 및 설득프로세스 안내
 - 수취은행 심사팀 업무연락 (전화번호 등)
- ④ 사고처리
 - 사고계좌해제/유지
 - 보고서 작성

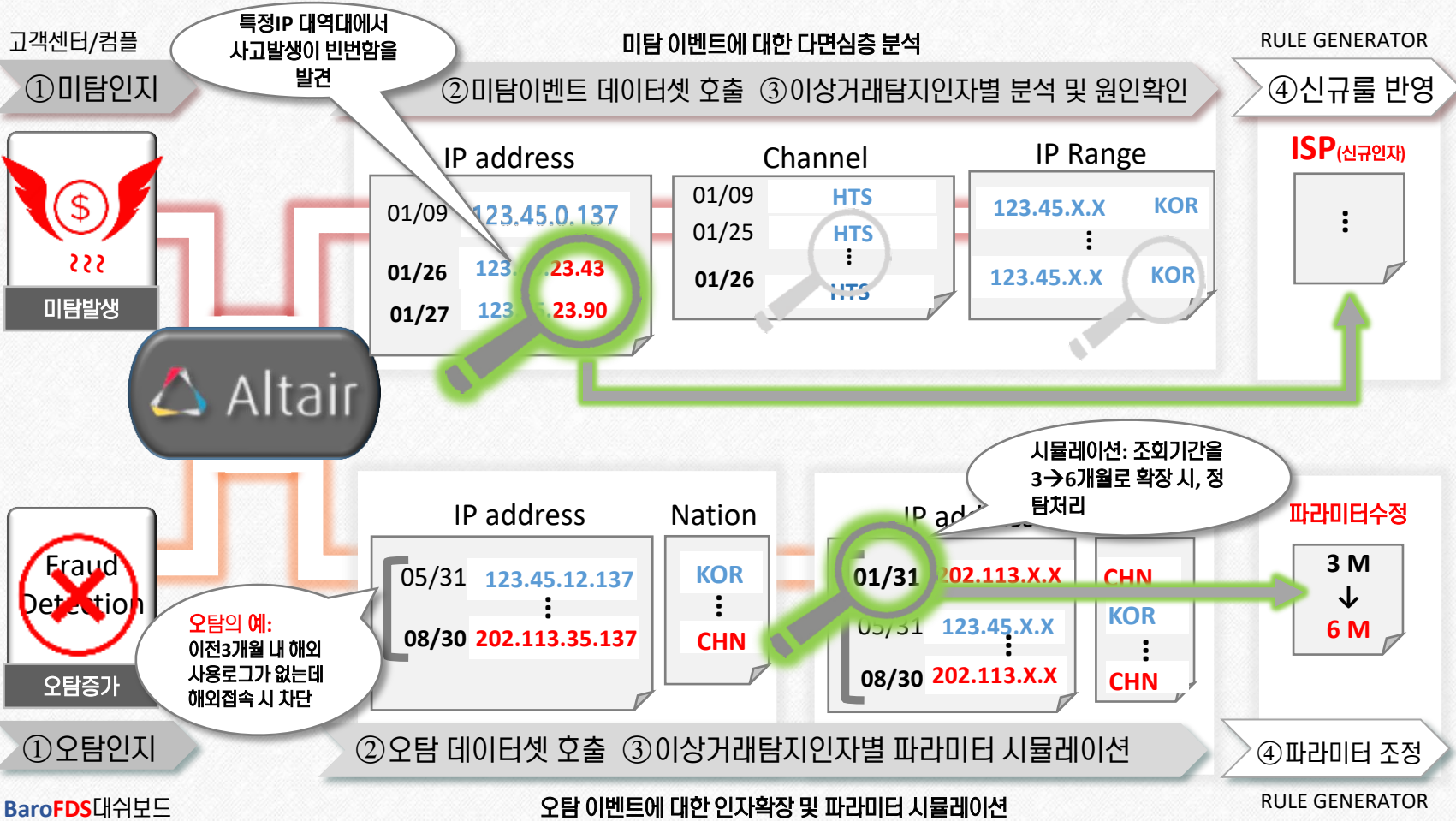
특장점#5 Rule Audit 및 Simulation



금융사기는 지속적으로 진화하기 때문에 Rule도 이에 따라 지속적으로 추가되어야 함. 또한 오탐증가로 인한 업무 생산성이 하락하는 문제가 발생하기 때문에 이를 개선할수 있는 도구가 필요. **BaroFDS**는 데이터분석솔루션을 활용하여 추가적인 신규를 개발이 가능하고 시뮬레이션을 활용한 정탐률 향상이 가능함

RULE감사 및 신규를 개발 프로세스

정탐 향상을 위한 Simulation Process



FDS 경쟁사 비교







현재 시장에서는 FDS를 실제로 구축하고 운영하면서, 실제 금융사고를 대응해 본 솔루션업체가 전무함. **BaroFDS**는 모 금융기관에서 축적된 Know-how를 기반으로 제품이 개발되어 시스템 Open 즉시 FDS의 정상운영이 가능하면서도 실제적 성과를 바로 낼 수 있는 있는 국내 유일의 FDS Package SW임

	FDS 도입 시, 기술검토항목	BaroFDS	기존 FDS 업체
 FDS RULE	<ul style="list-style-type: none"> 검증된 이상금융거래탐지인자 있는가? 경험기반 RULE SET이 있는가? 	<ul style="list-style-type: none"> 검증된 40 여개 이상금융거래탐지인자 보유 경험기반 RULE SET 보유 	<ul style="list-style-type: none"> 구체적 이상금융거래탐지인자 모름 경험기반 RULE SET 초기 수준
 COLLECTING	<ul style="list-style-type: none"> 실시간 수집이 가능한가? 다양한 환경에 적용이 용이한가? 	<ul style="list-style-type: none"> 실시간 수집이 가능 금융환경에 적합한 설정 및 적용 	<ul style="list-style-type: none"> 실시간 수집 불가 환경 별로 추가적 개발 필요
 REAL-TIME	<ul style="list-style-type: none"> 1초 이내에 고객의 1년 이상의 금융이력 조회가 가능한가? 	<ul style="list-style-type: none"> 1초 이내 최대 3년치 데이터 조회 가능 	<ul style="list-style-type: none"> Hadoop 기반의 배치처리 실시간 분석 불가
 RESPONSE PROCESS	<ul style="list-style-type: none"> 뱅킹과 통합된 대응화면이 있는가? 단계별 사고 대응 가이드가 가능한가? 	<ul style="list-style-type: none"> 뱅킹과 연계된 통합 VIEW 제공 단계별 조치 및 가이드 안내 	<ul style="list-style-type: none"> 뱅킹과는 분리된 시스템 단계별 조치 및 가이드 안내 없음
 ANALYSIS & UPDATE	<ul style="list-style-type: none"> 데이터를 분석하여 새로운 금융사고패턴을 확인할 수 있는가? 	<ul style="list-style-type: none"> 분석 및 시뮬레이션 가능 	<ul style="list-style-type: none"> 원초적 데이터마이닝, 통계분석만 가능 (FDS Knowhow 부족으로 분석 어려움)

TCO & 구축기간

기존 업체들은 전형적인 SI Project의 형태로 FDS 프로젝트를 진행됨. 그러나, FDS업무는 정형화된 업무가 아닌 사기 범에 대한 대응 업무이기 때문에 외부회사가 이를 분석하여 정형화하는 것은 매우 어려움. 또한 빅데이터 수집에 초점을 맞추기 때문에 구축기간이 5개월 이상 걸리며 HW/SW/인력투입비용도 과다 소요됨

	FDS 도입 시, 기타 검토항목	BaroFDS	기존 FDS 업체
 비용	<ul style="list-style-type: none"> SI개발로 진행되는가? 저렴한 비용으로 구축할 수 있는가? 	<ul style="list-style-type: none"> BaroFDS는 국내 유일의 Package 형태의 FDS SW 경쟁사 대비 최대 60% 저렴 	<ul style="list-style-type: none"> SI개발형태 진행됨 Rule, Solution 보다는 인력투입량에 따라 비용이 증가
 시간	<ul style="list-style-type: none"> 짧은 시간 내에 구축이 가능한가? 구축 즉시, 업무운영이 가능한가? 	<ul style="list-style-type: none"> 최소 1개월, 최대 2~3개월 소요예상 도입 즉시, 실효적 FDS운영가능 	<ul style="list-style-type: none"> 최소 5개월 ~ 7개월 소요 도입하더라도, 정상운영까지 6개월 이상이 소요됨
 인력	<ul style="list-style-type: none"> 프로젝트에 투입되는 인력은? 적은 인원으로도 운영가능한가? 	<ul style="list-style-type: none"> 컨설팅,구축,Customizing - 3명 예상 사고대응시스템의 운영으로 최소인원으로도 운영 가능 	<ul style="list-style-type: none"> 최소 10명 이상 대응체계가 없어, 필요 운영인력을 예측하기 어려움
 업데이트	<ul style="list-style-type: none"> 변화하는 금융사기에 대응가능하도록 지속적인 RULE 업데이트가 가능한가? 	<ul style="list-style-type: none"> Rule Factory (Rule subscription) 계약 체결 시, 지속적인 신규적인 신규Rule 업데이트 가능 	<ul style="list-style-type: none"> Rule개발하는 전담자를 두기 어렵, 지속적인 업데이트가 어려움

구축사례 – 모금융기관 FDS고도화

모금융기관은 FDS구축하여 성공적으로 운영하고 있는 금융보안에 선도적인 금융사임. 이번 BaroFDS의 도입으로 금융사기 근절은 물론 더 높은 업무효율성과 고객만족이라는 달성한 대표적인 FDS 구축사례임.

시스템 개요

- 2013.3월, 국내 최초로 FDS시스템을 도입
- 도입 이후, 지속적인 금융사고 및 이상금융거래 분석을 통해서 Rule 최적화하여 업계 최고의 부정거래방지 실적을 보유한 시스템

도입배경

- 최초 도입으로 인한 FDS 한계점이 존재
 - 데이터 수집 및 분석을 위해 SPLUNK를 도입하였으나 검색속도 지연으로 이상이체거래의 실시간 차단이 어려움
 - 고과금체제로 인하여 대량 데이터 수집 /저장에 한계 존재함
 - 탐지범위 확대가 불가
 - 추가적인 RULE반영 시, SPL전문가 필요했음
 - 뱅킹과의 연계가 불가하여, 구조가 이원화되어 업무효율성 저하

기대효과

- 실시간 사전차단: RULE기반 검색을 **0.03초 이내 처리하여, 이상 이체거래 발생 전 사전차단이 가능**
- 오탐률 저하: 대량데이터 처리가 가능해 탐지범위가 확대되고 거래채널 추가 가능하여, 이에 따라 **오탐률↓/업무효율성↑**
- 고객 만족도 향상: 금융사고 예방을 증가되고 또한 오탐이 적어져 **금융보안과 고객만족의 두마리 토기를 잡음**

시스템 구성도

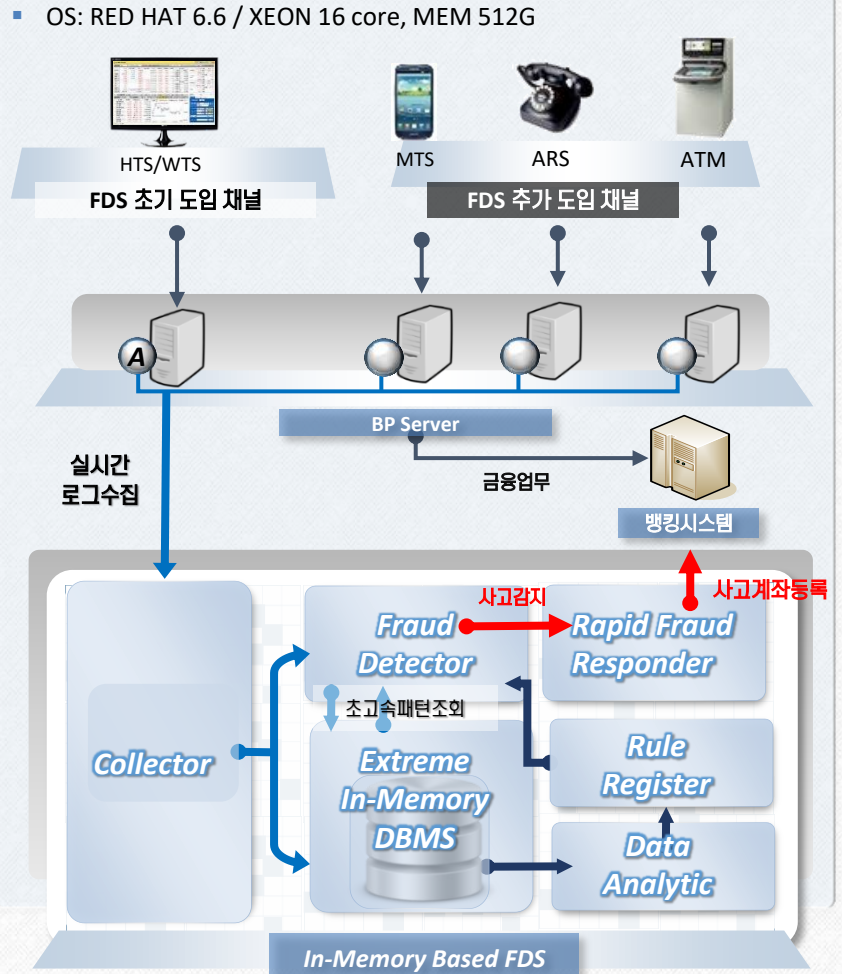


Table of Contents :

Smarter Answer in Fraud Detection

1. FDS 동향	02
2. 성공적인 FDS 구성요소	06
3. BaroFDS 제품소개	15
4. Why BaroFDS?	30

Why BaroFDS?

BaroFDS는 국내 FDS시장에서 유일하게 현장에서 검증되어 개발된 솔루션으로 ①검증된 FDS Rule을 보유하여, 도입즉시 성과도출이 가능하고 ②어떠한 금융환경에서도 손쉽게 로그수집이 가능하며 ③탐지 즉시 실시간 차단이 가능하도록 초고속 인메모리기반 아키텍처로 설계되어 있으며 ④사고대응프로세스를 갖추어 사고예방효과가 극대화됨. 이 모든 것을 짧은 구축기간과 합리적인 비용으로 구축 가능한 국내 유일의 솔루션임.

BaroFDS

손쉬운 로그수집

다양한 환경에서도 간단한 환경 설정만으로도 쉽게 실시간 로그 수집이 가능하며, 복잡한 금융 시스템환경에 적합

사고대응체계

2년간 현장 경험으로 축적된 대응체계가 시스템화 되어, 금융사고 대응 및 처리가 용이

비용&시간 절감

Package SW 형태로 구축하여 구축기간이 감소되고 이에 따른 비용이 절감됨

