디지털데일리 '금융 IT Innovation 컨퍼런스'

개인정보보호법 시행과 금융 보안 패러다임의 변화

Dec. 11st 2014

주제발표자 : KPMG삼정회계법인 문철호 상무

KPMG
cutting through complexity™

발표순서

I. 개인정보보호 개선 추진 배경

II. 금융기관 진단사례

III. 정보보호를 위한 To-do List

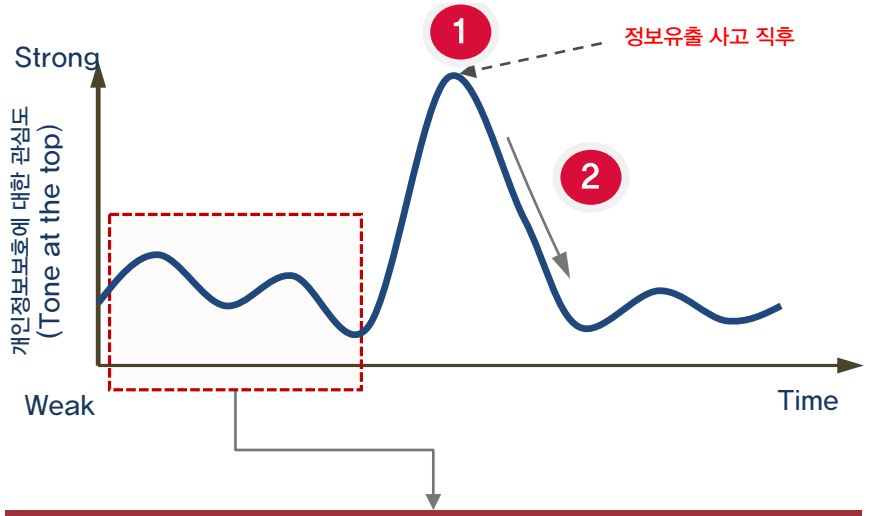
IV. 정보보호시스템의 미래

I. 개인정보보호 추진배경

1. 정보보호 패러다임의 변화요구
2. 최근 동향 (법률 제/개정, 감독기관)
3. 금융기관의 개인정보보호 이슈
4. 통제 패러다임의 변화 및 개선 방향

I.1 정보보호 패러다임의 변화 요구

통제구조의 근본적/실무적 개선을 통한
일시적 극단적 처방에서 종합적 대책으로의 전환점



정보취급 적정 여부에 대한 판단기준 및 절차는?

경영진 (Tone at the top)

- 정보보안 IT기술적 측면 강화를 위한 지속적인 투자 및 노력 (보안솔루션 도입 등)
  →정보보안 수준 등 Technical 측면 집중
  →정보보호 관리적(프로세스) 측면에 대한 관심도 감소

현업부서/영업점

- 업무목적 상 효율, 편의, 니즈 중시
- 업무상 필요정보 이외의 개인정보 요청/보유 가능

"정보 추출 및 제공 요구"

"정보 제공 및 가공"
(정보제공 적정 여부에 대한 판단기준 및 절차 미비)

암묵적 관행 발생 용이

IT/Compliance 부서

- 기술적 보안수준 및 사전 IT통제 초점
- 업무목적 상 필요여부에 대한 정확한 판단 어려움

1 정보유출 사고 발생으로 개인정보보호 관심도 급증 시기

사고발생 대응을 위한 일시적/극단적 대처

- 직원 PC에 저장된 개인정보 일괄 삭제, 점검, 처벌
- 인터넷 등 외부 유출 경로 차단
- USB 등 이동식 저장매체 사용 원천 통제 ……

업무 목적 상 개인정보 이용 및 처리가 불가피한 부서의 업무 중단/마비 초래

- ✓영업점
- ✓고객센터
- ✓심사
- ✓모집인 등 영업조직 관리
- ✓마케팅
- ✓기획
- ✓상품개발
- ✓리스크관리
- ✓위탁/제휴사

2 시간 경과에 따라 개인정보보호 관심도 감소 시기 → 개인정보 오남용 불감증 재발

악순환의 근본적인 원인

· 본부부서/영업점의 업무편의 추구
– "효율적인 업무처리를 위해 꼭 필요한 정보"라는 명목 하에 과도한 개인정보 요청 및 보유 경향

· 업무 유형별 필요 정보에 대한 판단 기준 부재
– 현업부서 내부적인 책임자 승인만 득하면 요구하는 정보를 제공할 수 밖에 없는 체계

"Tone at the Top 약화"

I.2 A Recent Trend (법률 제/개정 및 감독기관 동향)

법률의 지속적인 제/개정 및 종합대책 발표로
금융기관에 대한 규제의 범위와 강도가 강화되는 추세

법령	주요 제·개정 내역	시행일	시사점
개인정보 보호법	• 주민등록번호 처리 금지 (법령에 근거한 경우 제외)	2014. 08.07	8월부터 주민번호 처리 금지에 따라 각 금융기관은 대응방안 마련하여 시행 중
	• 주민등록번호를 내부망에 보관 시에도 암호화 하여 보관하여야 함	2016. 01.01	• 주민번호 암호화 보관에 따른 금융회사 시스템 변경 영향 클 것으로 보이며, • 현재 차세대 급 시스템 변경사업을 추진 중인 금융사 들은 모두 이 항목을 적용하는 추세임 (은행 중 전북은행이 차세대 수행 시 최초 적용 예정)
금융지주 회사법	• 영업 목적의 고객정보 공유 금지	2014. 11.03	• 그 동안 영업 목적으로 금융지주 내 공유했던 고객정보 공유 금지 • 정보 활용 범위 축소 및 프로세스 개선 필요
정보 통신망법	• 사생활정보 수집 제한, 마케팅 규제 강화		온라인 상 정보 수집 및 마케팅 프로세스 검토 및 개선 필요
	• 수탁자 법률 위반 시 처벌 강화, 개인정보 유출 시 처벌 강화		수탁자 관리 강화 및 개인정보 유출 방지 강화 필요

항목	취지	주요 내용	추진 현황
7.11 대책 (금융전산 보안 강화 종합대책) 2013.07.11 발표	• 2013.3.20 농협, 신한은행의 전산 사고를 계기로 금융권 전산보안에 대한 종합적인 개선대책 수립 • 주로 전자금융 등 해킹 공격에 대한 보안 강화에 중점	• 금융전산 위기대응체계 강화 • 금융회사의 전자금융기반시설 보안 강화 (망분리 의무화) • 금융회사의 보안인력·조직 역량 강화 • 금융이용자 보호 및 감독 강화 (FDS 구축 의무화) • 금융회사의 자율적 보안노력 지원	• 각 금융기관 별 망분리 및 FDS 구축 추진 중 • 관련하여 전기통신금융사기 피해방지 및 피해금 환급에 관한 특별법 시행 ('14.7.29)
3.10 대책 (금융분야 개인정보 유출방지 종합대책) 2014.03.10 발표	• 카드 3개사의 대량 개인정보 유출 이후 개인정보 유출 및 오남용 방지를 위한 종합대책 수립 • 전반적인 개인정보 내부통제 강화에 중점	• 개인정보의 「수집-보유·활용-파기」 등 단계별 금융소비자의 권리 보호 및 금융회사 책임 대폭 강화 • 금융회사가 확실하게 책임지는 구조 확립 • 해킹 등 외부로부터의 전자적 침해행위에 대해서도 7.11 대책 대폭 보강 • 이미 계열사와 제3자에 제공되었거나 외부유출된 정보로 인해 잠재적으로 피해가 발생할 가능성에 대해서도 대응방안 강구	• 2014년 말까지 금융당국 및 금융기관에 대부분 적용해야 함 (주민번호 암호화 보관 등 일부 2014년 이후 적용) • 사안 별로 2014년 6월, 9월, 12월까지 감독당국의 법령 제·개정 및 추가적인 가이드라인 제시 예정

I.3 금융기관의 개인정보보호 이슈

주요 시사점

- 관행적인 업무 프로세스를 견지하는 상황에서의 정보보호 관련 해결책은 근본적 해결책이 되지 못함
- 업무 Process 운영 효율과 IT System 통제 간 균형 있는 개선 필요

"개인정보 가공 및 활용주) 관련 불완전한 Process & System 통제 절차의 개선"

개인정보보호 관련 주요이슈

1. 계속되는 개인정보 유출사고
2. 감독기관의 규제강화
3. 지속적 개인정보 관련 법 제/개정
4. 전반적인 개인정보 체계 개선 요구
5. 지배구조에 따른 개인정보 이슈 부각
6. 시스템 위탁운영에 따른 개인정보 이슈
7. 통제부서와 실행부서간 불균형

금융기관	감독기관
"해킹 및 정보탈취 등은 내부통제 문제라기 보다는 범죄이며, 전형적 인재(人災)이다!"	"영업과 실적에만 치중하고 개인정보관리에 소홀한, 총체적 내부통제 부실이다!"

"사고원인 관련 다양한 시각이 존재하나, 실무적/현실적 해결책 제시에 한계"

고객	법률 및 보안전문가
"금융회사가 고객보다 우월한 지위로 정보를 맘껏 수집 및 활용하는 문화와 제도가 문제다!"	"금융회사가 법률을 위배했으며, 업무편의 중시 및 투자 미비로 보안 System상 허점이 많다!"

개인정보 유출 사고 원인은 "통제 준수와 업무편의 간 Conflict"

- **Process 통제 미비**
  외주직원의 정보 접근통제, 취급범위 및 처리절차에 대한 통제 설계 미비
- **System 통제 미비**
  USB 저장매체 통제/반출 관련 System 통제 point 및 승인절차가 적절히 설계·운영되지 못함

Key Word

"정보유출은 금융기관의 가장 심각하고도 강력한 경영위험 요인"

정보유출 근본원인 및 대응방안

현실적 통제 허점을 아우르는, 전행 개인정보 관리 절차상, 암묵적 관행 (운영의 미흡)을 유발하는 불완전한 업무 Process & System 설계가 근본 원인 !

→ 즉, 업무 Process 운영 효율과 IT System 통제 간 균형 있는 개선 필요

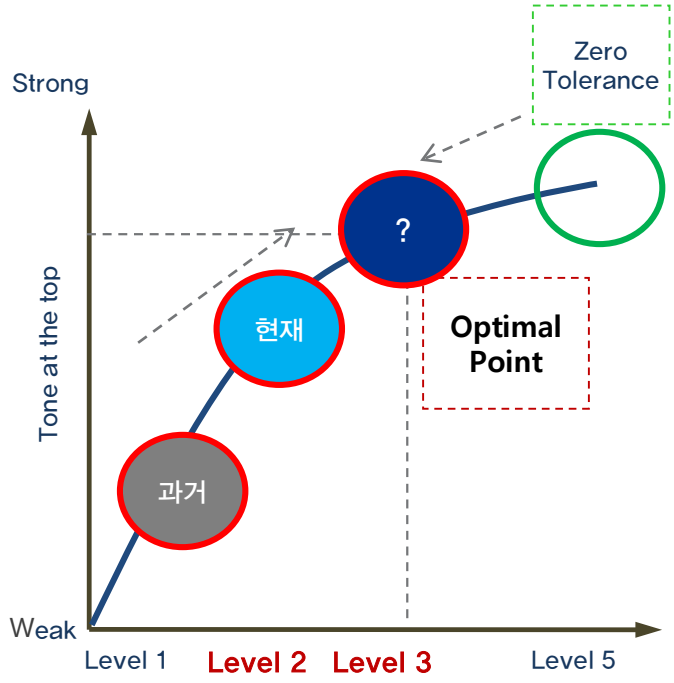
주) 업무부서가 마케팅, 경영분석, 고객지원, 업무위탁, 프로젝트 수행 등 다양한 목적으로, 고객으로부터 수집된 원천 DB로부터 고객 정보를 ①조회, ②전부 또는 부분 추출, ③변환 등 재가공 사용, ④정보의 Hardware적 또는 Software적 이동 및 보관하는 Process

I.4 통제 패러다임의 변화 및 개선방향

주요 시사점

- 경영진의 의지와 개인정보보호를 위한 내부투자가 동시에 이루어졌을 때 정보보호의 최적점에 도달 가능
- 사람과 운영측면의 통제절차는 프로세스적 접근과 모니터링이 핵심

> "실효적 개선을 위한 프로세스 개선을 통한 기술적 한계 극복에 Focus"



IT보안 강화 관련 투자 (Level 2)	→	사람과 운영 측면의 내부통제 관련 투자 (Level 3)

개선방향 1	업무 특성 별 개인정보 필요 수준 정의	• 개인정보 Life-Cycle관점의 점검을 통해 업무별 개인정보 필요 수준 명확화 → 수준별 관리체계 마련
개선방향 2	실효적 Process 개선을 통한 기술적 한계 극복	• 프로세스 개선을 통한 개인정보 Life-cycle별 통제 고유수준 강화 • 규정, 지침, 매뉴얼, 문서서식 등 재정비 • 개인정보보호 관리적 측면 강화를 위한 조직 및 제도 개선, 업무 프로세스 수립
개선방향 3	개인정보 이상징후 모니터링 개선	• 개인정보 내부 이용 및 유출 경로에 대한 통합적 관리 및 System 지원 • 이상징후 모니터링 : 유출 시나리오 기반 Advanced rule-based

I.4.1 개선방향 1 업무특성 별 개인정보 필요수준 정의

> 업무별 개인정보 취급범위/수준 정의 및 관리를 통한 오남용 예방

업무특성에 따른 개인정보 필요 수준 사전 정의 절차

1. **부서/프로세스별 개인정보자산 현황 파악**
   - 개인정보 정의 및 범위 확정
   - 다수 부서/프로세스에 수집되어, 보유 및 관리되고 있는 개인정보 자산 항목 식별

2. **Life Cycle 분석 대상 프로세스 식별**
   - 개인정보를 다루는 주요 프로세스를 기준으로 Life Cycle 분석 대상 식별

3. **Life Cycle 관점의 관리 수준 점검**
   - 프로세스별 개인정보 Life Cycle (수집, 이용, 처리, 삭제) 관점의 관리 수준 및 적정성 점검

4. **개인정보 과다 이용/보유 취급자 분석**
   - 업무 목적외 수집 정보, 목적 달성 후 미삭제 정보, 업무와 무관하게 접근 가능 정보 등을 분류

5. **개인정보 취급범위 필요수준 정의**
   - 부서/프로세스 단위의 업무 목적을 위하여 필요한 개인정보 취급 가능 범위 정의

개선 방안

1 개인정보 요청 시 제공 가능 여부에 대한 명확한 판단 기준

- 개인정보 취급범위를 벗어난 정보 요청 시, 사전 승인을 위한 판단 기준으로 활용

2 개인정보 접근 권한 관리 강화

- 각 부서별 직무에 따라 조회 및 이용 가능 한 개인정보에 대한 접근 권한관리 세분화 및 내부통제 강화

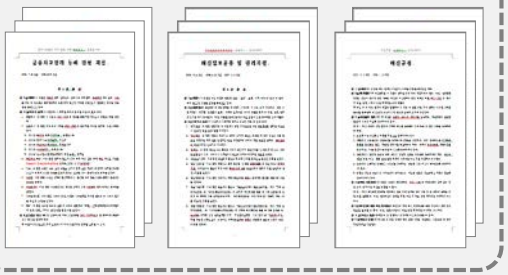
3 개인정보 취급자별 개인정보 관리 현황 모니터링

- 정의된 업무 목적 상 필요한 개인정보만을 수집하고 보유/이용하는지에 대한 모니터링 및 점검 가능

I.4.2 개선방향 2 실효적 Process 개선을 통한 기술적 한계 극복

> 업무 현실간 괴리가 없도록 실질적 보완통제 프로세스 재설계

개인정보보호 관련 규정/지침



Gap

"내부통제 규정과 업무 현실 간 이격도(離嗝度) 발생"

- 암묵적 관행
- 통제 절차 Skip 불가피
- IT통제 예외적용

- 고객의 무리한 요구사항
- 금융사간 경쟁 과열
- 제한된 영업점 인력
- 개인정보를 Key로 사용

내규/IT 100% 준수가 어려운 영업 현장의 현실

"통제의 빈틈은 시차를 두고 유출사고로 현실화"

1. 고객 동의가 누락된 정보 수집 존재
2. 권한부여, 변경, 말소 History 미보관
3. 외부직원 시스템 사용 통제 Process 미흡
4. 개인정보 수집에 대한 업무 지침 미흡

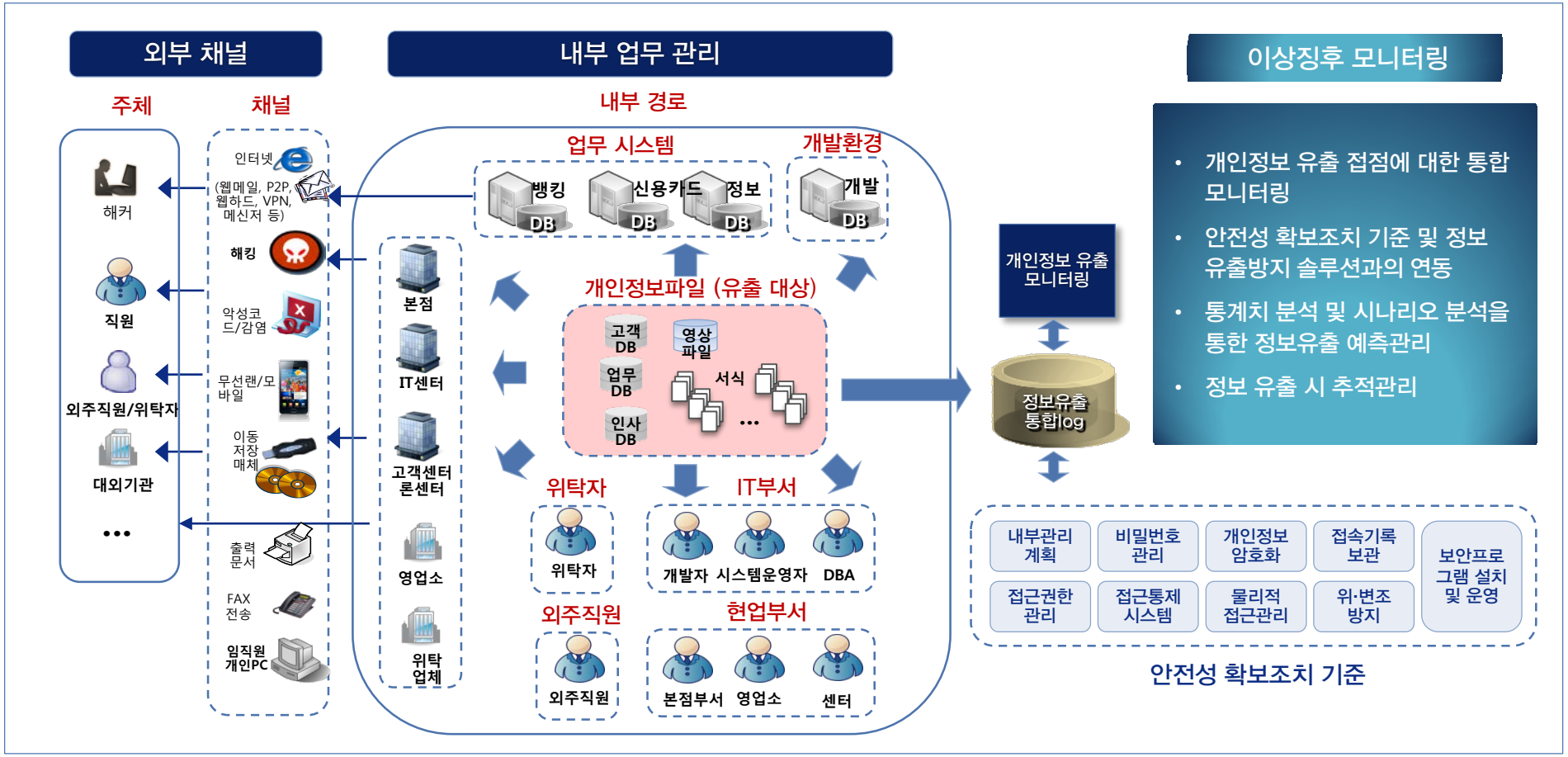
프로세스 재설계 방안

- IT통제와 업무 현실간 괴리가 없도록 실질적 보완통제 프로세스 재설계
- Critical Point별 상세 유출 시나리오에 따른 이상징후 모니터링
- 업무별 개인정보 취급 기준에 따른 System Blocking
- 규정/지침, 매뉴얼 현행화를 통한 현업 실무 가이드 제공
- 전행 업무 프로세스별 개인정보보호 관리체계 수립 및 개선 실행
- DB암호화 적용, 시스템 접근권한 강화 등 개인정보의 안전성 확보 조치 강화

KPMG cutting through complexity™

I.4.3 개선방향 3 개인정보 이상징후 모니터링 개선

> 유출경로 및 접점을 고려한 체계적인 정보관리 및 유출방지 Insight 제시



KPMG cutting through complexity™

II. 금융기관 진단사례

1. 개인정보보호 진단 Framework
2. 금융기관 현황진단 사례
3. 현행 정보통제의 문제점
4. 주요 취약점 및 개선과제
5. 개선 방향성

II.1 (Case study) 개인정보보호 진단 Framework

주요 시사점

- 개인정보보보호 활동 및 통제 수준 진단
  - 정보보호 거버넌스
  - 정보보호 관리 프로세스
  - 통합 모니터링
- 진단 Framework
  - 8대 주요 주제영역
  - 126개 진단 항목

금융기관 개인정보보호 활동 수준 및 현황을 진단하여 현 시점에서의 개인정보보호 통제수준에 대한 현실감 있는 평가의 필요성이 제기됩니다.

1 전행 정보보호 Governance

Policy & Compliance / 조직 및 역할 / 감사 등 전행 정보보호의 3 Line of Defense 체계

2 전행 정보보호 관리 프로세스

전행 개인정보 현황 및 Life-cycle 관리 / 유출 경로 및 접점에 대한 KRI* 식별 및 업무 프로세스 통제

3 전행 정보보호 통합 모니터링 시스템

개인정보보호, PC보안, 서버 및 네트워크 보안 등 법규준수, 오남용, 유출방지를 위한 안전성 확보 및 선제적 모니터링

대분류(8대 주제영역)	상세 진단 내용 (16개 중분류 (126개 소분류))
Governance/Mgt. 체계	규정, 지침 등의 개인정보 내부통제 업무 현황
	경영진, 위원회, 전담조직 역할 및 기능
	내/외부 이해관계자 교육 및 문화확산
점검 및 감사 체계	사전/사후 점검 및 감사
	고객정보 오남용 자체에 대한 제재기준
Legal 대응 체계	유관법률 및 행정당국 최신지침의 이행 수준
개인정보 Life-Cycle 관리 체계	개인정보 Life-cycle별 관리 현황
	개인정보 처리 승인/관리 업무프로세스 현황
사용자 관리체계	고객정보 이용 권한 및 조회 적정성
제3자 관리체계	고객정보 제공 및 제3자 정보관리 적정성
	외주업체(IT 및 위탁업체 포함) 통제 수준
IT 보안기술/침해대응 체계	이동저장매체 저장 및 외부전송 통제 적정성
	PC보안, 문서보안 등 기술적 보안 수준
	계정/비밀번호 관리, 고객정보 암호화 수준
통합 모니터링 체계	해킹 등 침해요인 및 사고대응 수준
	이상징후 탐지, 오남용 적발 등 모니터링 수준
	전행 Key Risk 관리 및 통합 모니터링 수준

*KRI : Key Risk Indicator

II.2 (Case study) 현황진단 사례(Key Message)

금융기관별로 약간의 편차는 존재하나, 개인정보를 처리하는 내/외부 직원에 의한 법규 미 준수, 오남용 및 유출위험은 아직도 상존하고 있는 것으로 판단해 볼 수 있습니다.

1 비효과적인 유출방지 프로세스 및 시스템 통제활동

내부직원의 개인정보 조회/가공/(유출매체)이동/보관활동에 대한 통제가 강화되었으나, 형식적 운영 가능성 상존

- 개인정보 조회 관련 업무목적 부합 여부 판단에 대한 어려움
- 금융기관 내 개인정보 취급자와 비취급자 구분의 부재
- 개인정보 조회/이용에 대한 단순 모니터링에 의존
- 전행, 부서(팀)별 또는 부서 간 개인정보 처리 단위업무에 대한 명확한 현황관리 부재
- 고위험 개인정보 처리업무에 대한 통제활동이 산재

2 상시 오남용이 가능한 시스템 권한 부여

본부/영업점/외주(도급) 직원의 통합 업무시스템 접근 권한이 광범위

- 영업중시 문화로 인해 거의 전 직원이 고객정보 취급 가능
- 직무 및 상시 필요범위를 벗어나는 "권한의 과다 부여"
- PC/USB등 시스템 유출매체 이용의 편리성

3 개인정보보호 측면의 통제 사각지대 존재

IT시스템/유출매체 통제관리 대비 사람/문서에 대한 실질적 통제의 어려움

- 내부직원 대비 제3자/도급업무에 대한 중점관리 필요
- 시스템/파일에 대한 통제 수준으로 문서관리 통제강화 대책 필요
- 본점 外 물리적 업무수행 거점에 대한 현장 통제 미흡

II.3 (Case study) 현행 정보통제의 문제점

추가유출 가능성과 업무 비효율이 공존하는 현 상황하에서는 개인정보 처리업무 특성별 KRI 식별과 비정상 사용에 대한 이상징후 모니터링 영역에 대한 개선이 필요할 것으로 판단됩니다.

잔존위험은?

"추가 유출가능성과 업무비효율이 공존"

As-Is 정보보호 통제 Concept

1. 정보공유 및 제공 접점에 대한 원천적 차단
2. 인가제를 통해 정보 Exposure 최소화 원칙
3. 현업부서장의 부서내 정보 권한 및 처리 승인
4. 정보보안실의 사전 Cross-check 및 점검
5. 설계된 유출방지 접점에 대한 모니터링

	내부통제 관점	Business 관점
1	☐ N/A	☐ 마케팅 분석 역량의 전행적 확대의 어려움
2	☐ 형식적 운영에 따른 통제 허점 발생 위협, 인가자 집중 위험	☐ 인가자 업무 집중 및 비인가자의 업무 범위/Skill 제한
3	☐ 내부통제보다는 성과 KPI 달성이 중요 → 형식적 승인 위험	☐ 부서내 과다한 승인업무 및 사유서 작성업무
4	☐ 실질적 Cross-Check 수행 및 사전적 점검 효과 미작동	☐ 형식적 Cross-Check업무로 인한 업무 비효율
5	☐ 업무별 평균 이상 과다 조회, 비정상 조회거래 인지 어려움	☐ N/A

II.4 (Case study) 주요 취약점 및 개선과제

> 효율적 통제를 통한 정보통제 최적화 및 완전성 확보에 주력

사전적/실질적 모니터링/승인/점검

- 개인정보 임의접근에 대한 편리성 제거
- 개인정보 조회/이용 이력 관리
- 선제적 오남용 및 유출방지 시스템
- 선택과 집중에 의한 리스크 관리

비효과적 통제 → **1** 개인정보 Life-cycle 통제전략

개선1> 개인정보 취급 인가제 운영(취급자 제한)
개선2> 사전적 조회/이용 모니터링 시스템 구축
개선3> 고위험 Life-cycle 상시 점검 및 관리
개선4> 정보유출 조기경보 체계 마련

개인정보 접근권한/경로 최적화

- CRM 및 통합업무시스템에 대한 차별화된 권한 설계 및 접근통제
- 개인정보 대량 집적, 재생산, 유출 가능 경로의 원천 차단

시스템 권한 과다 → **2** 사람-업무-시스템 간 통제 최적화

개선1> CRM 정보 및 권한 분리/축소
개선2> 직무기반의 차등적 시스템 접근 통제
개선3> 업무용 PC내 개인정보 처리 제한
개선4> 대량 데이터 취급 시 통제 강화
개선5> 유출매체 이용 추적관리 체계 운영

전행 차원의 통제 사각지대 해소

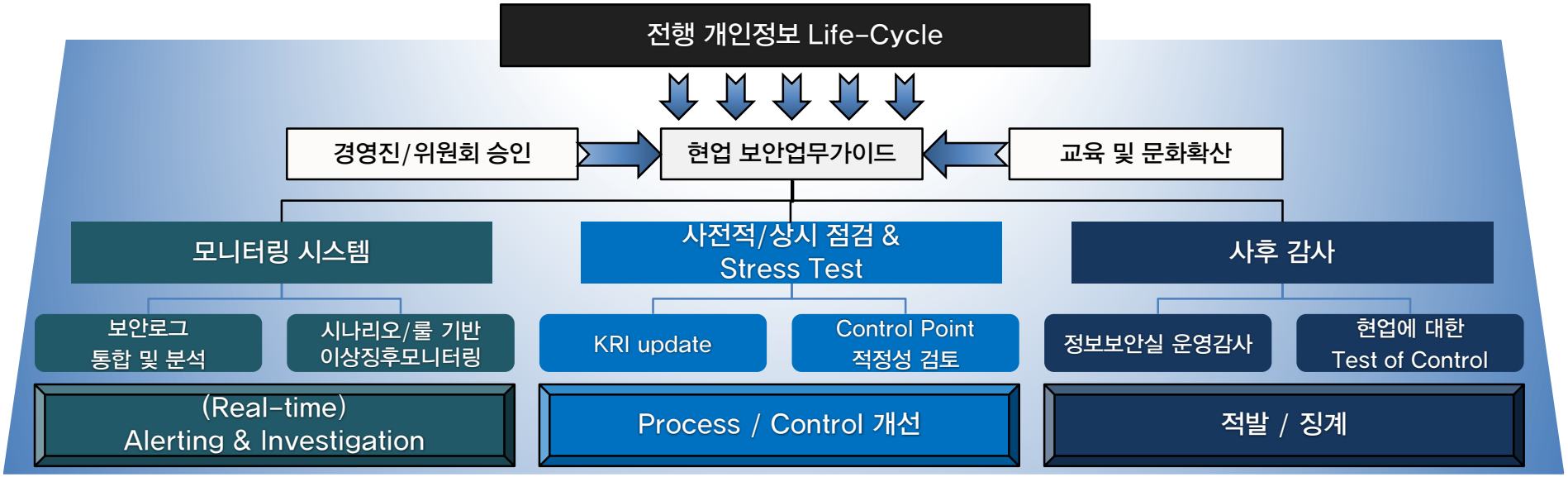
- 외부정보 제공 및 외부직원 관리 강화
- 불필요한 문서 생성 및 보관 동기 억제
- 지속적인 정보보호 강화 인프라 운영을 위한 현장 관리

통제 사각지대 → **3** 통제 완전성 Up-grade

개선1> 제3자에 대한 실질적 점검 관리 강화
개선2> 도급업무/직원에 대한 통제 관리 강화
개선3> 개인정보 포함 문서보관/파기 명확화
개선4> 영업점 점검/교육/의사소통 강화

II.5 (Case study) 개선방향성 (To-Be 내부통제 체계)

"정보보호 역량강화와 내/외부 직원에 의한 사고 방지를 위한 정보보호"



1 사전에 수립된 명확한 업무 가이드라인

- 사용자 편의성 보다는 정보보호 위주의 가이드라인 확립
- 단, 현업 성과와 Conflict 발생이 우려되는 통제 지양

2 시나리오/Rule기반 모니터링 및 사고 예측

- 현장감사보다 사전적 모니터링 점검 역량 비중확대

3 효율적인 교육수단의 도입

4 임원회의에 정보보호 주제 상정

- Tone at the Top과 명확한 Risk appetite 공유
- 통제 vs. 효율 Balance 개선기회로 활용

5 정기적인 점검 강화와 위반시 제재기준 확립

- 사고 후 징계방식이 아닌 규칙 위반행위 자체에 대한 제재

6 (중기) 보안조직 미래 정체성과 역할 Develop

- 유출방지 & 정보자산 관리 및 활용역량 강화 Mission

II.5 (Case study) 개선방향성 (To-Be 모니터링 체계)

"기술적+관리적 보안환경의 통합개선을 통한 예상치 못한 상황의 선제적 제어"

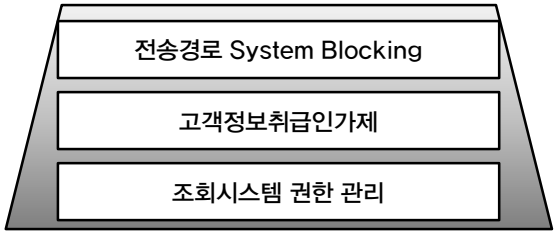
As-Is

해킹 방지 및 임직원 접근 통제를 위한 개별 모니터링

가시적 정보유출 접점의 흐름에 대한 기술적 보안 통제 中心

- 네트워크 트래픽 모니터링
- PC 개인정보 보유여부 모니터링
- DW상 고객정보 조회 모니터링
- 저장매체(USB 등) 모니터링
- E-Mail / Fax 모니터링
- 악성코드 탐지 모니터링
- VOC 모니터링
- 방화벽 모니터링 등

기술적 보안 통제



To-Be

통합보안관제시스템(ESM) 재구축

기존 보안 솔루션 상 모니터링 통합 및 지표간 상관분석 등 Skill-up

- 방화벽, 침입탐지 시스템, 가상사설망(VPN) 등 이기종 보안 솔루션을 하나로 관리
- 실시간 수집 중인 보안로그 중 중요 이벤트 발생 알람 기능
- 수집된 보안로그를 활용한 상관관계 분석 → 정교한 침해 유형 분석능력 제고

고객정보 조회 처리 내역 모니터링 시스템

예측이 어려운 오남용/유출 방지를 위한 Rule&시나리오 적용 탐지

- 업무특성별 개인정보 조회내역
- 주요 식별자* 조회 이력 분석
- 중요화면에 대한 별도 모니터링
- 상위 과다 조회자 집중 모니터링
- 정상치 대비 이상징후 패턴 분석
- 평균 이상 과다조회 패턴 분석
- 휴일 및 시간외 조회 모니터링
- Compliance 위반 시 자동통지

기술적 보안과 관리적 보안의 통합

III. 정보보호를 위한 To-do List

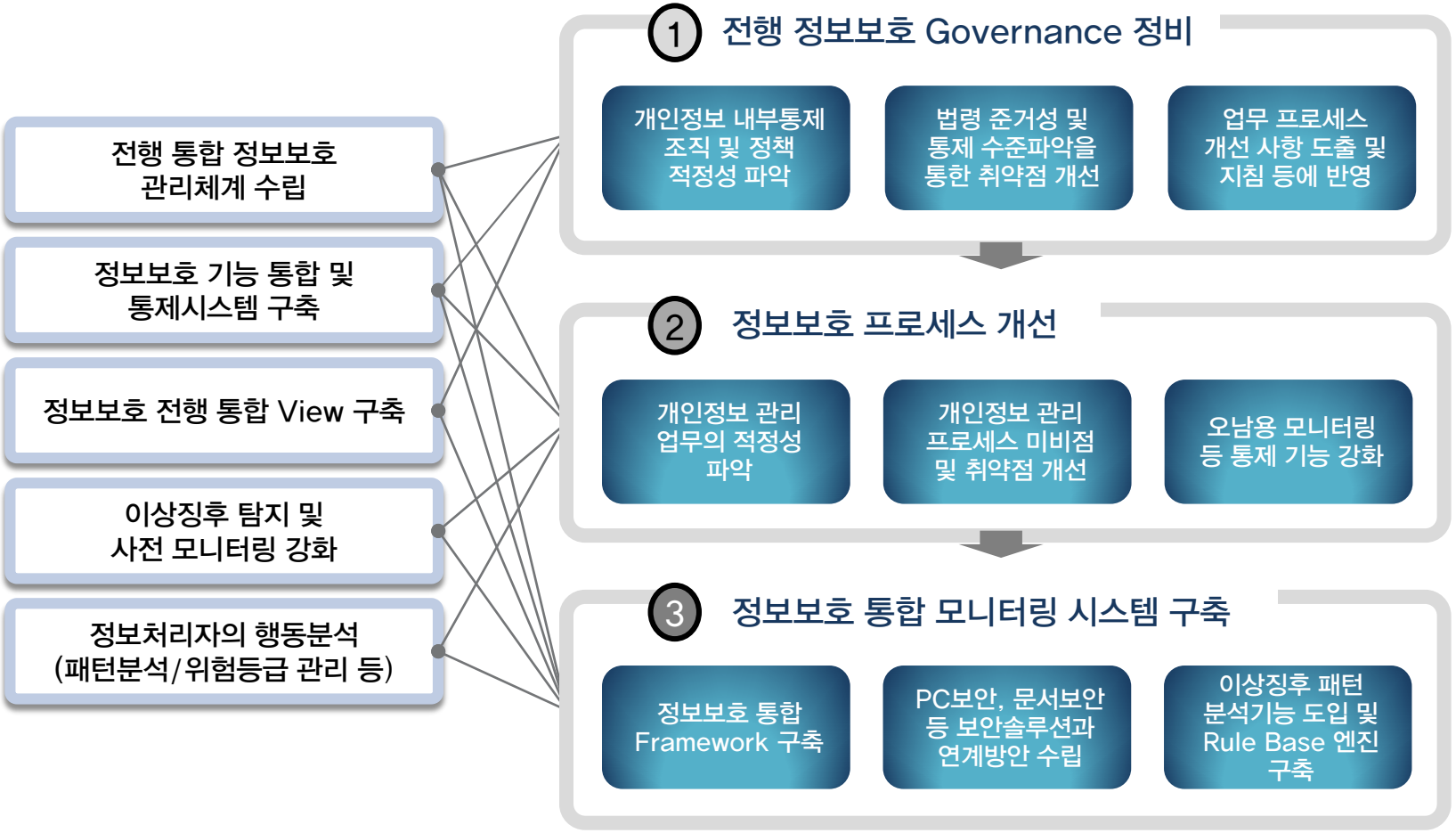
1. 개인정보보호 체계정비
2. 규제충족을 위한 To-do List
3. 정보보호 통제장치 Map

III.1 개인정보보호 체계 정비

주요 시사점

- 개인정보보호체계
  - Governance
  - Process
  - System
- 기술적/물리적 통제를 보완하는 관리적 측면의 체계정비로 완전성 극대화

전행 통합 View 구축을 위한 개인정보보호체계 정비가 요구되며, Governance / Process / System 차원의 각 영역별 구체적 개선과제 정의가 요구됩니다.



III.2 규제 충족을 위한 To-do List

정책/프로세스

기존 정책 업데이트

개인정보보호법, 정보통신망법, 신용정보보호법, 전자금융거래법 등 관련 법령 제·개정 및 감독당국 요구사항 반영

주민번호 처리업무 개선

주민번호 처리업무 중 법령에 의하지 않은 업무 파악 및 개선 (주민번호를 성명+생년월일로 대체 등)

개인정보 Life Cycle 별 업무 개선

1)수집업무 개선	• 개인정보 수집정보 최소화 및 관련 업무 개선 (동의서 양식 등)
2)보유 및 활용업무 개선	• 위탁사 관리 (VAN사,외주용역 관리 포함) / 제3자 제공업무 개선 등
3)파기업무 개선	• 보관기간 만료 개인정보 파기절차 수립 • 제3자 제공 개인정보 파기 확인 업무 수립

정보주체 권리강화 업무 개선

- 정보주체의 권리 요구 대응절차 수립
- 신용정보보호법 개선에 따른 외부 마케팅 업무 개선

Application

고객정보 DM 구축

- 고객정보 통합 및 관리 최소화를 위한 데이터 모델링

개인정보 암호화 관련 Application 반영

- 고유식별정보 등 개인정보 암호화에 따른 어플리케이션 영향도 파악 및 기능 구현

개인정보 Life Cycle 별 업무 개선에 따른 각 시스템 별 반영 필요 기능 구현

1) 개인정보 수집 시 관리기능	• 개인정보 항목 별 등급화 관리, 고객 동의정보 세분화 관리
2) 개인정보 별도 보관 기능	• 고객 탈회 시 등 별도보관 등 처리 기능 구현 (별도 DB 저장 및 타업무 접근 금지)
3) 개인정보 보관기간 만료 시 파기 기능	• 탈회 후 5년 경과 고객정보 파기 등 (제3자 제공업무의 경우 파기 확인 기능)

정보주체 권리강화 관련 기능 구현

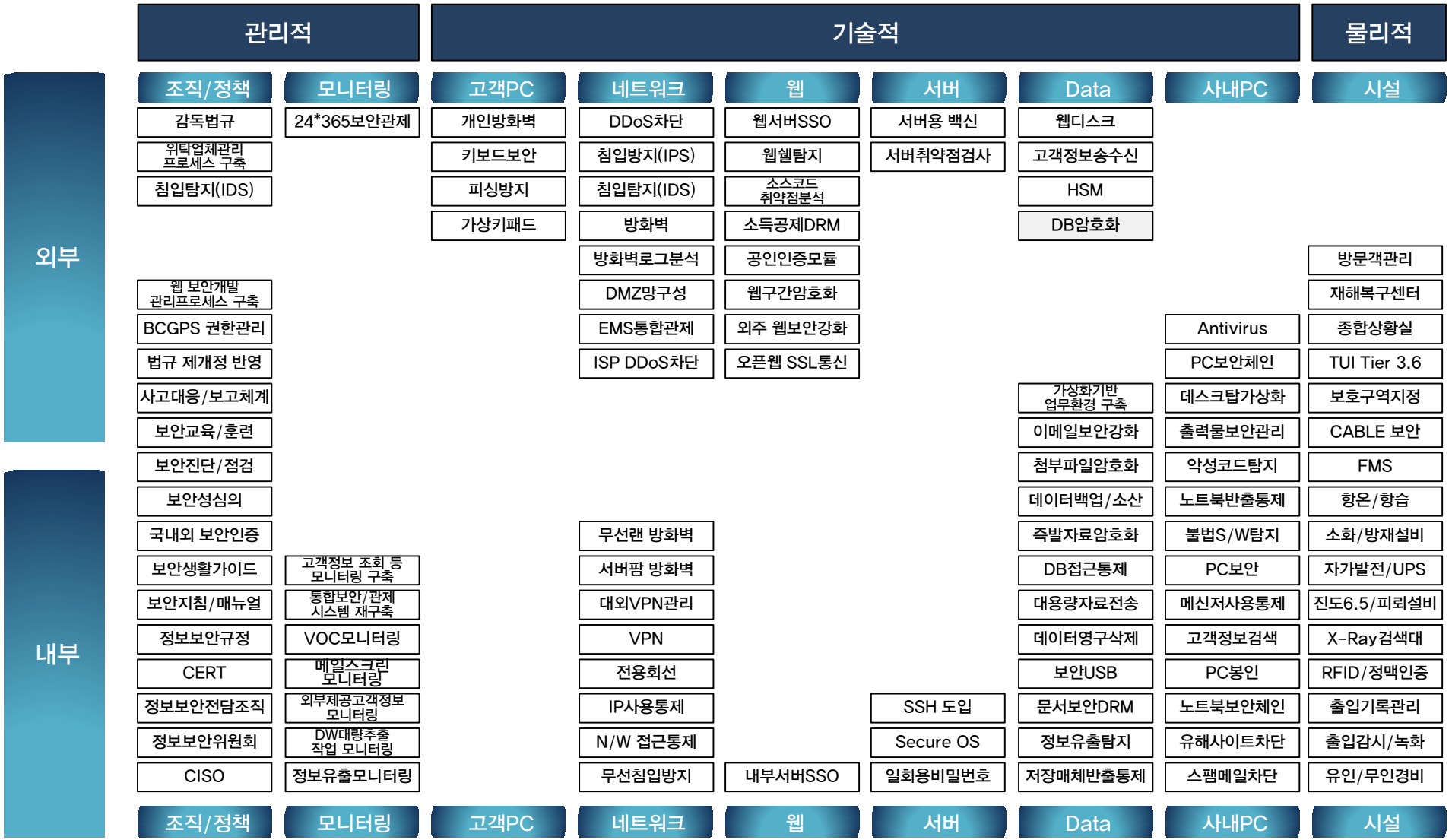
- 본인정보 이용/제공현황 조회시스템 구축
- 주요 채널 별 외부 마케팅 기능 개선

보안 Infra

해킹 등에 의한 정보 유출 및 파괴 방어체계 강화

1)고유식별정보 암호화	• 주민등록번호 등 (범위 및 암호화 방식 결정 필요)
2)망분리	• 금융회사 망분리 가이드라인에 의한 망분리 시행 (전산센터 '14년말, 본점/영업점 '16년말)
3)금융전산 보안 관제 범위 확대	• 금융거래시스템 외 교육, 홍보용 홈페이지까지 확대
4)보안체계 강화	• 금융전산 보안 인증제 기반 보안체계 수립
5)모바일 어플리케이션 안전성 강화	• 모바일 앱 보안 가이드라인 기준

III.3 정보보호 통제장치 Map



Ⅳ. 정보보호시스템의 미래

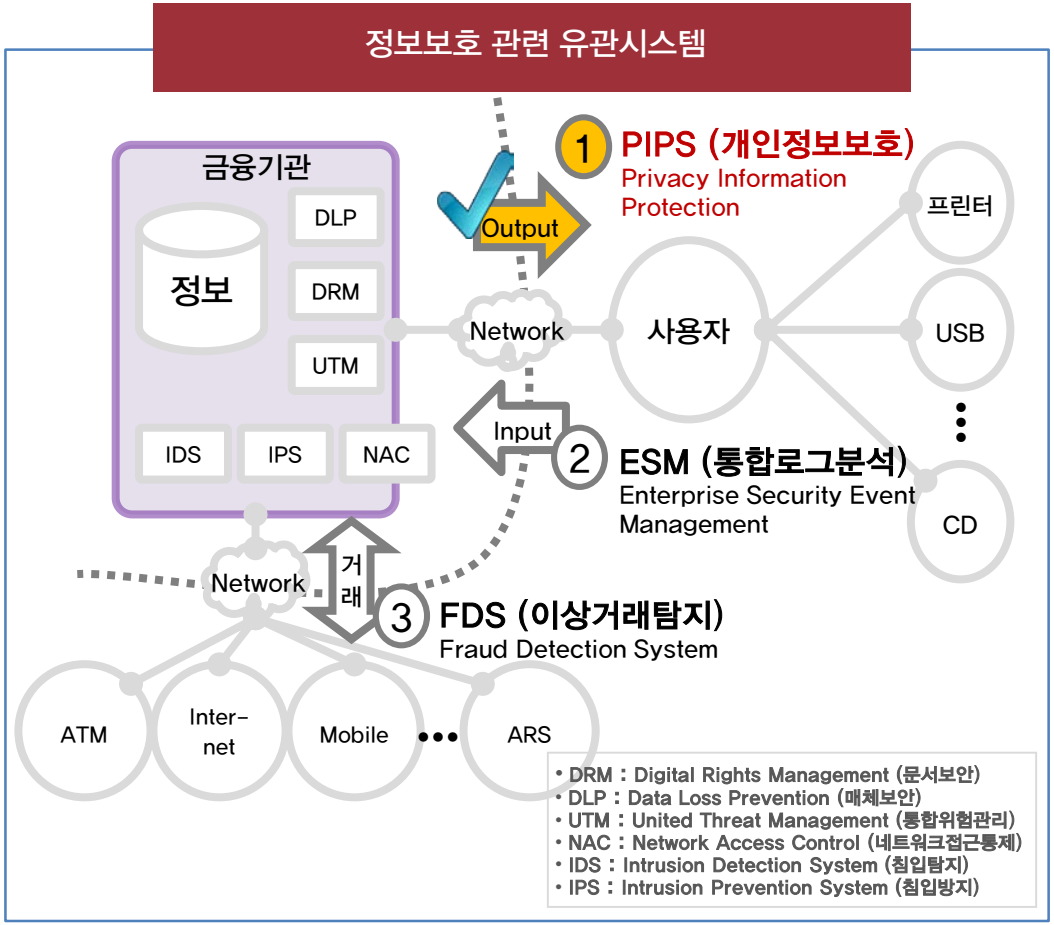
1. 정보보호관련 유관 시스템
2. 모니터링시스템 기능 구성(안)
3. 새로운 관점의 기술적 보안
4. 해외 적용사례 연구

IV.1 정보보호 관련 유관 시스템

주요 시사점

- 정보보호 관련 유관 시스템
  - PIPS
  - ESM
  - FDS
- 데이터의 방향성에 따른 특성을 고려한 통제 대책 요구
  - 내부정보 유출방지
  - 외부 침입 방지 및 통제
  - 이상거래 탐지 및 적발

현재 정보보호의 대상이 되는 시스템은 크게 3가지로 구분되며, 각각의 시스템은 데이터 흐름의 방향성에 따른 특성을 반영하여 설계/구현되어야 합니다.



1 PIPS (개인정보보호)
Privacy Information Protection System

- 내부 정보의 외부 유출 방지
- 데이터의 흐름이 내부에서 외부로 흘러가게 되며 정보보호 프로세스를 통한 예방 및 로그분석 등을 통한 감시 시스템

2 ESM (통합로그분석)
Enterprise Security Event Management

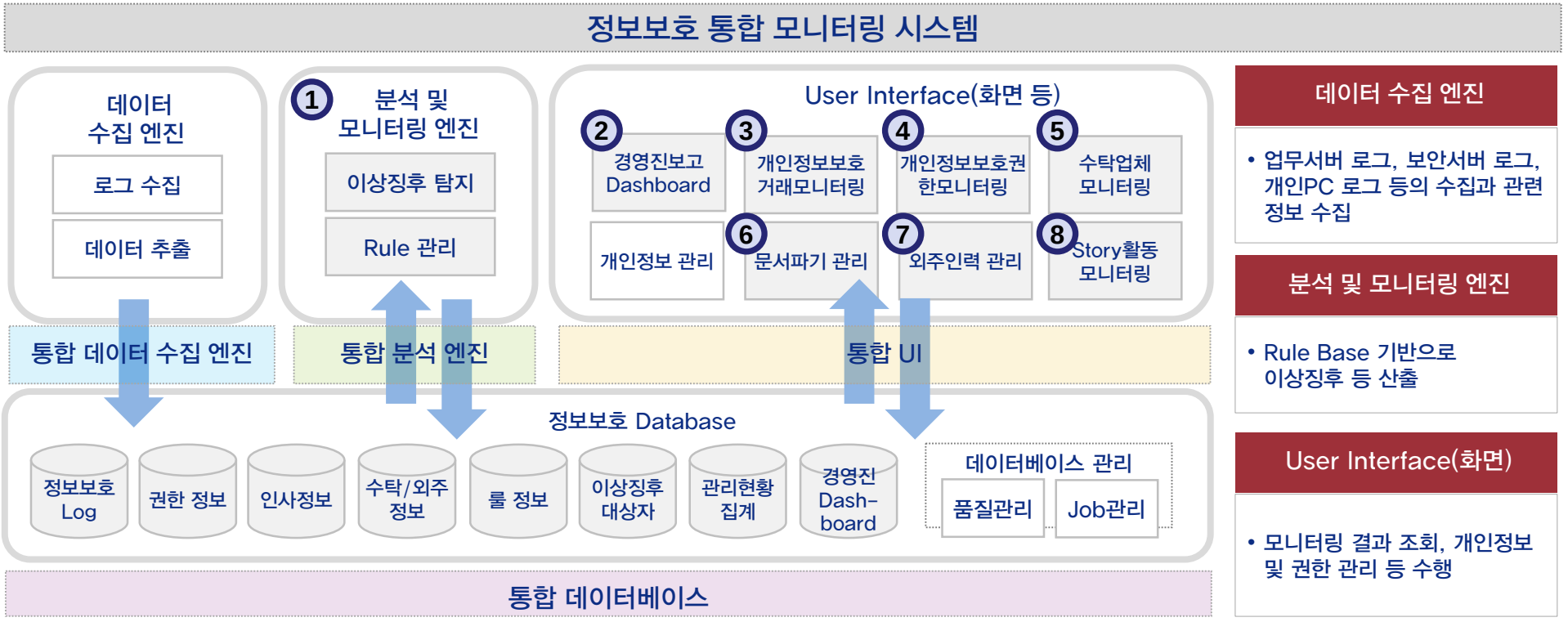
- 외부 침입 방지 및 접근통제
- 외부의 시스템 공격에 대비한 로그 분석 시스템의 통합을 통한 침입방지 정교화

3 FDS (이상거래탐지)
Fraud Detection System

- 이상거래 탐지 및 적발
- 전자금융 채널을 이용한 실시간 이상거래 탐지 및 패턴 분석을 통한 위험거래 탐지

IV.2 모니터링시스템 기능 구성(안)

데이터 수집 및 분석의 결과는 경영진 Dash-board, 거래모니터링 현황, 권한 모니터링 현황 등의 기능으로 개인정보 관리자에게 제공합니다.



데이터 수집 엔진

- 업무서버 로그, 보안서버 로그, 개인PC 로그 등의 수집과 관련 정보 수집

분석 및 모니터링 엔진

- Rule Base 기반으로 이상징후 등 산출

User Interface(화면)

- 모니터링 결과 조회, 개인정보 및 권한 관리 등 수행

*정보보호 통합 Framework 기반으로 각 영역 구축

IV.3 새로운 관점의 기술적 보안

최근 보안이슈의 핵심은 정보를 유출하려는 자의 진화속도를 시스템이 따라가는 못하는 한계상황이 존재한다라는 것이며 이를 극복하려는 새로운 시도들이 존재하고 있습니다.

DoD IT Asset Type	DARPA Reference System
NIPRnet	Windows DMSS
Laptop Encryption	Guardian Edge
DARPA VPN	Nortel
PDA	Blackberry/iPhone
SIPRnet	Windows DSN
JWICS	Windows DJN
Source Selection	TFIMs, I2O BAA Tool
Contract Management	GSA Advantage, SPS
Contract Invoicing	Wide Area Workflow
Payroll	MyPay
Benefits	Benefeds.com
HR	hr.dla.mil
Training	DAU
Collaboration	Defense Connect Online
Financial System, Local	Momentum
Financial System, Agency	DFAS
Credit Union	PFCU, NCU, etc.

Non-DoD IT Asset Type	Hacked on	Credentials lost
American Honda Motor Co.	27-Dec-10	4.9m
Bank of America	25-May-11	1.2m
Carnegie Mellon University	8-Oct-07	19k
Citigroup	27-Jul-10	30m
Clarkson University	10-Sep-08	245
Countrywide Financial Corp.	2-Aug-08	17m
Fidelity Investments	24-Sep-07	8.7m
Heartland Payment Systems	20-Jan-09	130m
IBM	15-May-07	2k
Johns Hopkins Hospital	22-Oct-10	152k
SAIC	7-May-08	630k
Sony	27-Apr-11	12m
Stanford University	6-Jun-08	82k
TD Ameritrade Holding Corp.	14-Sep-07	6.5m
Texas A&M University	9-Nov-08	13k
TJMax Stores	17-Jan-07	100m
U.S. Depart. of Veteran Affairs	14-May-07	103m
U.S. Marine Corp – PSU research	26-Jul-07	208k
Visa, MasterCard, and American Express	27-Dec-10	4.9m

Source: www.privacyrights.org/data-breach

- 개인정보호법 강화, 전자금융거래법 강화
- 비밀번호, 보안카드 해킹에 의한 불법 송금 책임 문제
- 내부자 해킹에 의한 불법 내부정보 유출 문제

2014.03.12 • 카카오톡해킹, 스마트폰해킹, 스마트폰위치추적

2014.04.15 • 진화하는 악성코드…금융거래 추가 인증 우회 우려

2014.05.08 • 공인인증서 유출 관련 악성코드 주의

2014.06.18 • 스마트폰 해킹, 백신도 소용없다" [위키트리]

2014.09.04 • 공인인증서 1400건 해킹돼…특정 사이트 접속하자마자 공인인증서 유출

2014.09.28 • 급부상하는 핀테크의 세계] IT, 금융으로 진격하다

2014.11.25 • 모 은행, 통장 예금 해킹 인출 – 수법이 미스터리

정보보호 프로세스 강화와 더불어 기술적 보안에 대한 재검토 요구

보다 강력하고 진보된 행동기반 보안 & 인증 솔루션 필요성 부각

(New Trend) 새로운 관점의 방어체계란?

IV.4 해외적용 사례 연구 (Denmark Danske Bank& Nordics Bank (1/2))

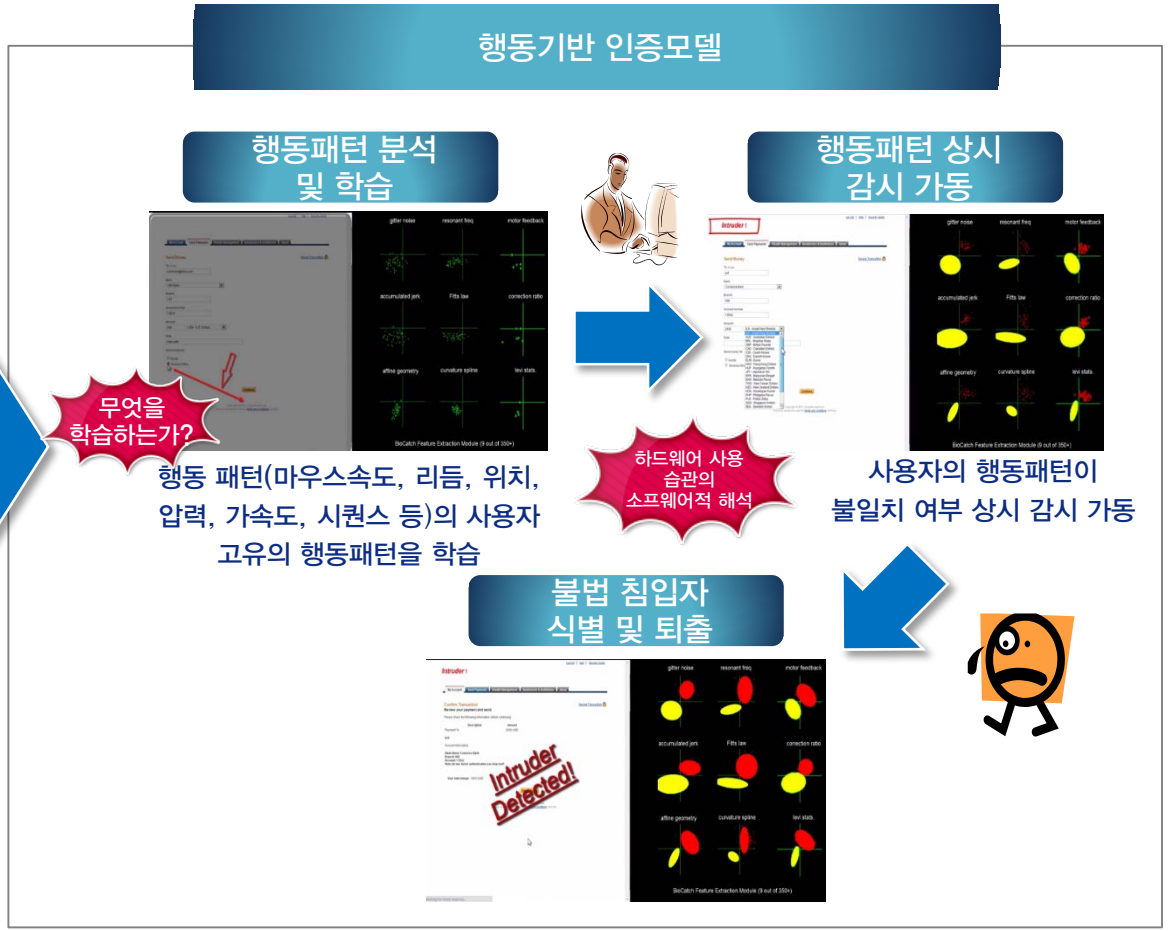
덴마크 Danske Bank와 Nordics Bank에서 시도되고 있는 행동기반 보안/인증 모델은 내부정보 보호 및 PC 환경에서의 인터넷뱅킹 보안.인증 시스템으로 기술보안 한계극복의 좋은 사례가 될 것입니다.

BehavioSec

Real world usage examples

- 20,000 user trial at Danske Bank.
  - 99.7% capture rate. All session.
  - Let to 2.5 million user roll out.
- 1,200,000 user mobile in nordics
  - Just key flight on 6 digit PIN.
  - 94% capture rate
  - Moving to 4 Million user roll out
- Web shop / payment with credit card payments NY
  - Distinguish between the correct user and an imposter in 97.52% to 99.87% of the cases for a single session.
- In 2014 we will be a new security layer for over 10 million internet bank users across the Nordics

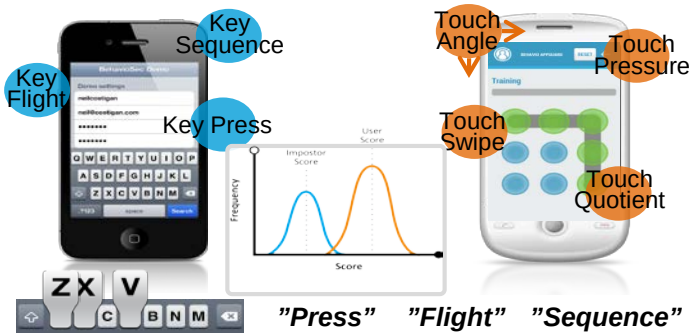
기존 룰베이스 모니터링과는 다른 관점의 행동 패턴 학습모형

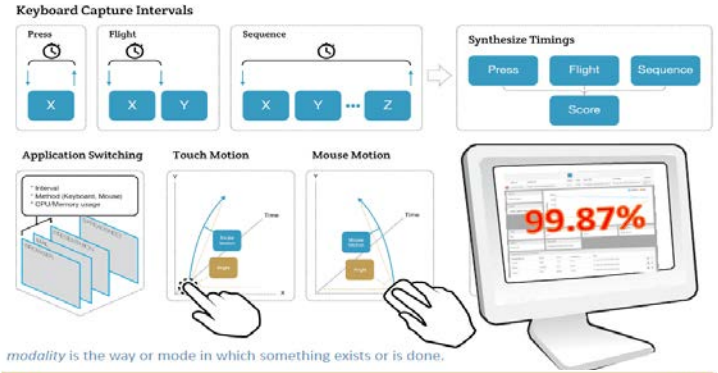


KPMG cutting through complexity™

IV.4 해외적용 사례 연구 (Denmark Danske Bank& Nordics Bank (2/2))

컴퓨터나 모바일 디바이스가 악성 코드에 감염되어 핵심 비밀번호가 유출 되거나 분실 되더라도 안전하게 인터넷/모바일 뱅킹을 할 수 있는 보안 인증 기술에 대한 관심이 그 어느 때 보다 높은 것이 사실 입니다.





Test	Score
Key Press	0.77
Key Flight	0.68
Key Sequence	0.95
Combining them with Bayes' theorem gives: A = 0.77*0.68*0.95 = 0.49742 B = (1-0.77)*(1-0.68)*(1-0.95) = 0.00368	
Combined score: A/(A+B) = 0.49742/(0.49742+0.00368) = 0.992656156	

행동패턴 분석

- 사용자의 행동 패턴, 예를 들어, 속도, 리듬, 위치, 압력, 가속도, 시퀀스 등 차이를 기반으로 사용자의 행위를 추적하면서 높은 정확도로 실제 사용자 진위 여부를 확인해 줍니다.
- 사용자가 어떻게 타자를 치고 스크린을 밀고 확대하는지 등을 기억하며, 스크린 터치 시 자주 가해지는 압력의 세기와 특정 문자들을 입력할 때 그 사이에 생기는 간격을 계산하고, 평소 사용자가 기기를 드는 각도, 마우스를 놓은 위치도 기록합니다.
- 사용자의 행동패턴을 액션 별로 인지 트레이닝을 통해 습득 & 축적 후 이를 통계 분석을 통해 사용자 진위 여부를 정확히 판단합니다.

부적절 사용자의 식별률

- Danske Bank 사용자 : 2만 명 기준 99.8%
- 인터넷 쇼핑 신용카드 사용자 : 97.52~99.87 %
- 단순 6자리 비밀번호 사용자 : 94%

**"비밀번호가 분실되어도,
공인인증서가 유출되어도,
심지어 디바이스(모바일폰,PC)가 점유되어도,
2채널 인증이 무력화 되더라도 안전하게 사용자 보호"**


Q&A
KPMG
cutting through complexity™

KPMG

cutting through complexity™

Thank you

The End

"문의사항이나 궁금하신 사항이 있으시면 아래 연락처로
연락 주시면 성심 성의껏 답변해 드리도록 하겠습니다."

문철호 상무이사

KPMG 삼정회계법인
Management Consulting Services

Tel ：(02)2112-0869
Fax：(02)2112-0152
Mobile：010-3378-7086

cmoon@kr.kpmg.com