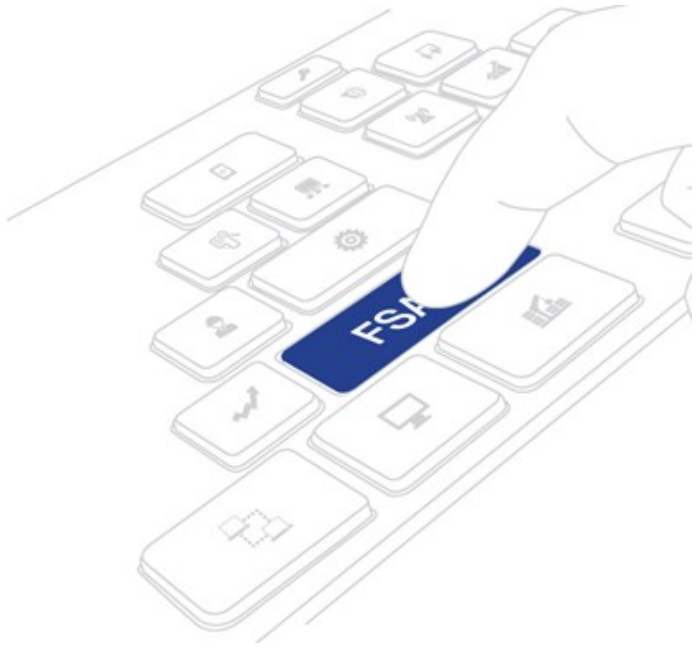
[기조연설]

금융보안 현황과 거버넌스 강화 방향

금융보안연구원 원장 김 영 린

2014. 6. 24



금융보안연구원
Financial Security Agency

목 차

Ⅰ 전자금융 현황

Ⅱ 전자금융 보안 위협 및 대응기술

Ⅲ 금융보안 거버넌스 강화

Ⅰ 전자금융 현황

1. 전자금융 현황

▶ 국내 주요 이용자 현황

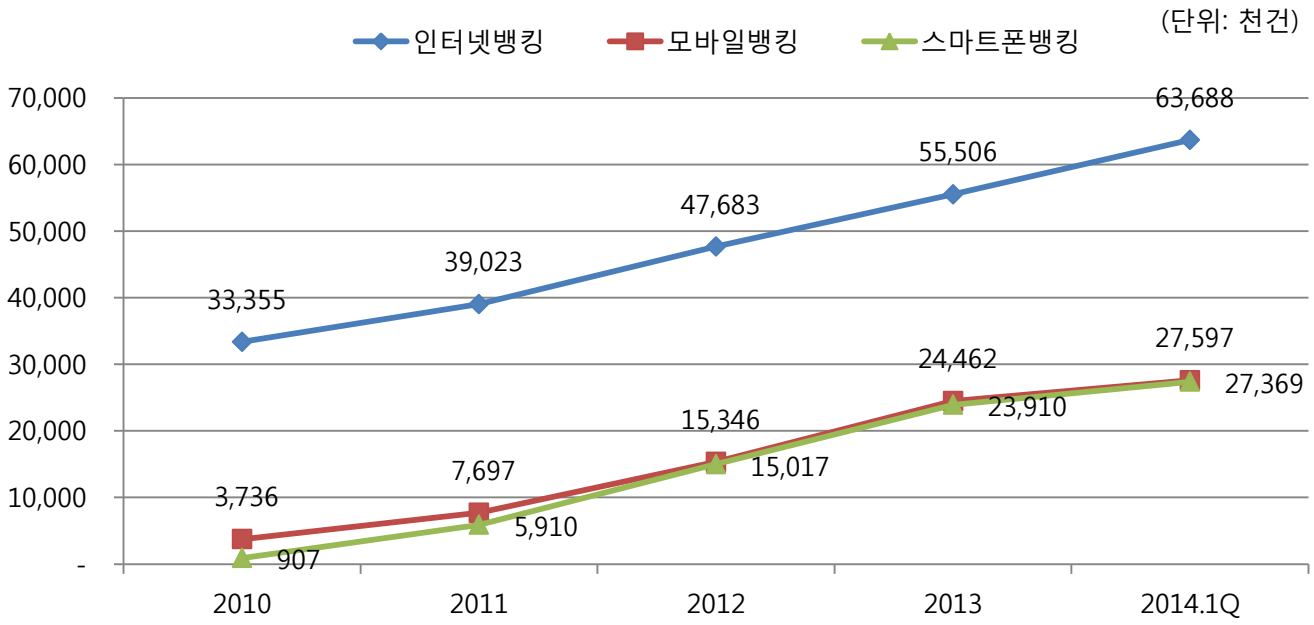
초고속인터넷 사용자	98.1% of total households (약 4,800 만명)
모바일 폰 사용자	110% of total population (약 5,400 만명)
공인인증서 사용자	53% of total population (약 2,600 만명)

* OTP 이용자 천만 돌파('14.5)

1. 전자금융 현황

▶ 인터넷뱅킹(모바일뱅킹 포함) 현황

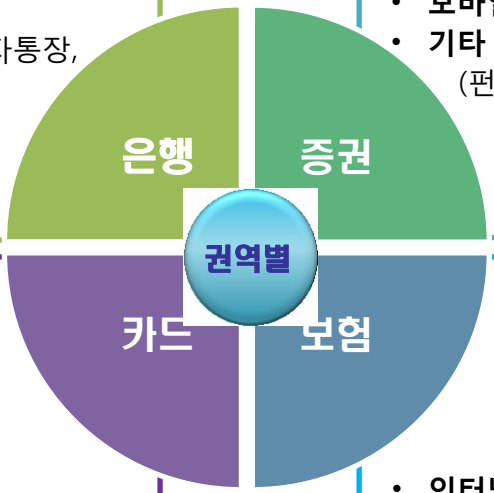
- '14년 ¼분기 이용금액(일평균 기준) 36조 1,394억원, 이용건수 6,368만건으로 전분기 대비 각각 3.9% (+1조 3,400억원), 14.7% (+818만건) 증가
- 스마트폰 기반 모바일뱅킹 이용건수 및 금액은 2,760만건, 1조 6,634억원으로 일 평균 이용률이 2010년 약 90만건에서 30배 이상 증가



[출처] 2014년 1/4분기 국내 인터넷뱅킹서비스 이용현황(한국은행, '14.5월)

2. 전자금융서비스 현황

▶ 금융사에서 제공하는 전자금융 서비스가 **채널별(온라인, 모바일 등)**로 **다양**해지고 있으며, 특히 **새로운 IT기술**을 활용한 **뱅킹, 결제 서비스** 등이 **지속적**으로 **출시**되고 있음



- **온라인 뱅킹 서비스**
  (오픈뱅킹, 인터넷뱅킹, 텔레뱅킹 등)
- **모바일 뱅킹 서비스**
  (VM뱅킹, 칩 뱅킹, WAP뱅킹, 스마트폰 뱅킹 등)
- **CD/ATM서비스**
- **금융IC카드 서비스** (현금카드결제, 전자통장, 전자화폐, 폰 ATM 등)
- **기타 서비스**
  (POS 뱅킹 에스크로, TV-ATM뱅킹, 스마트 브랜치, 뱅크월랫카카오 등)

- **폰 트레이딩 서비스**
  (ARS주식매매거래)
- **인터넷 트레이딩 서비스**
  (HTS, WTS)
- **모바일 트레이딩 서비스** (MTS)
- **기타 온라인 상품 서비스**
  (펀드, CMA, 방카슈랑스, ELS/DLS 등)

- **온라인 결제 서비스**
  (PC안심클릭, ISP결제)
- **모바일 결제 서비스**
  (간편결제, 모바일 ISP결제 등)
- **모바일카드**(IC방식, 앱방식)
- **전자지갑 로열티서비스**
  (쿠폰, 스탬프, 맴버쉽, 상품권)
- **토큰 결제 서비스**
  (바코드 결제, QR코드 결제, 가상카드번호 결제)
- **카드대출서비스**
- **부가서비스**(결제 편의성/보안성/생활 편의성)

- **인터넷, 모바일 및 전화 보험서비스**
  (가입, 신청, 조회, 대출, 증명서 발급, 사고접수 등)
- **기타서비스** (전자청약서비스 등)

Ⅱ 전자금융 보안 위협 및 대응기술

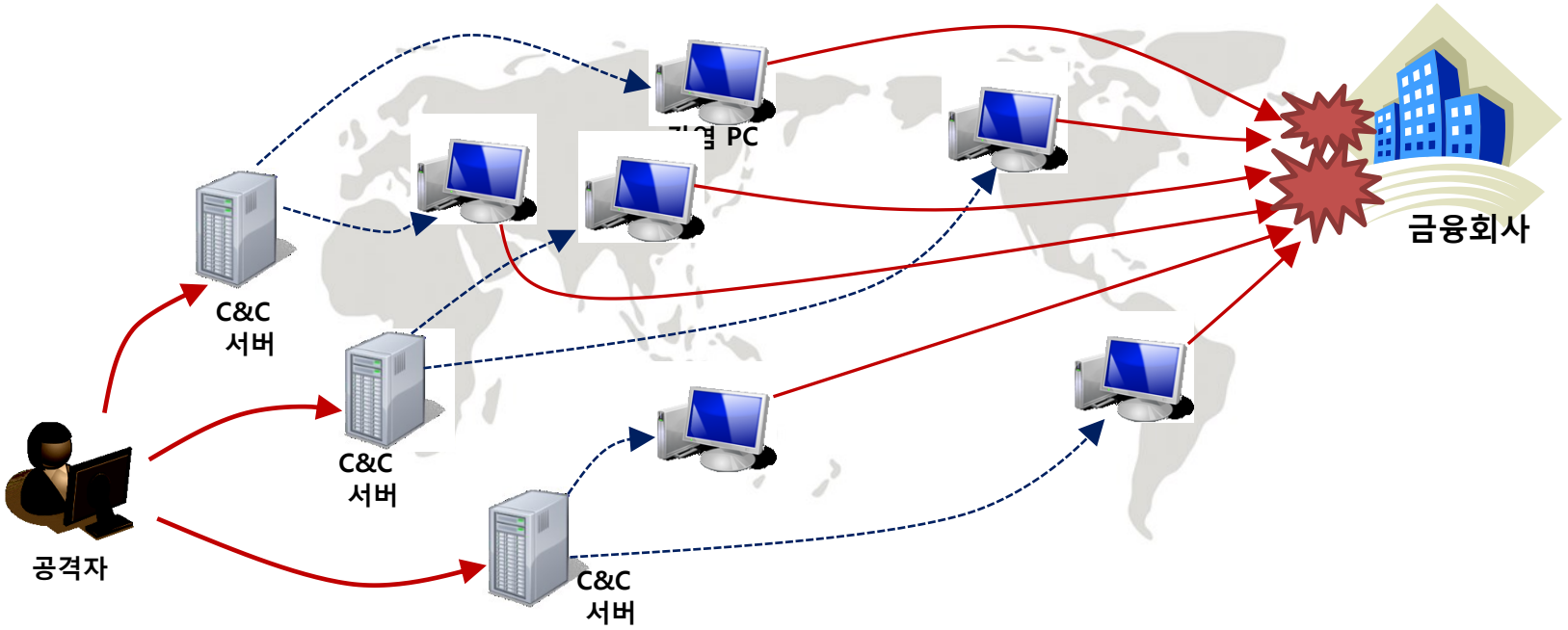
1. 전자금융 보안 위협

▶ 서비스 거부공격 (DDoS)

- 시스템을 악의적으로 공격하여 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격

➔ 2009.7, 2011.3, 대규모 DDoS 공격으로 인해 정부기관, 금융회사 등 피해 발생

· 최근까지 크고 작은 DDoS 공격 발생으로 인해 지속적인 위협 존재

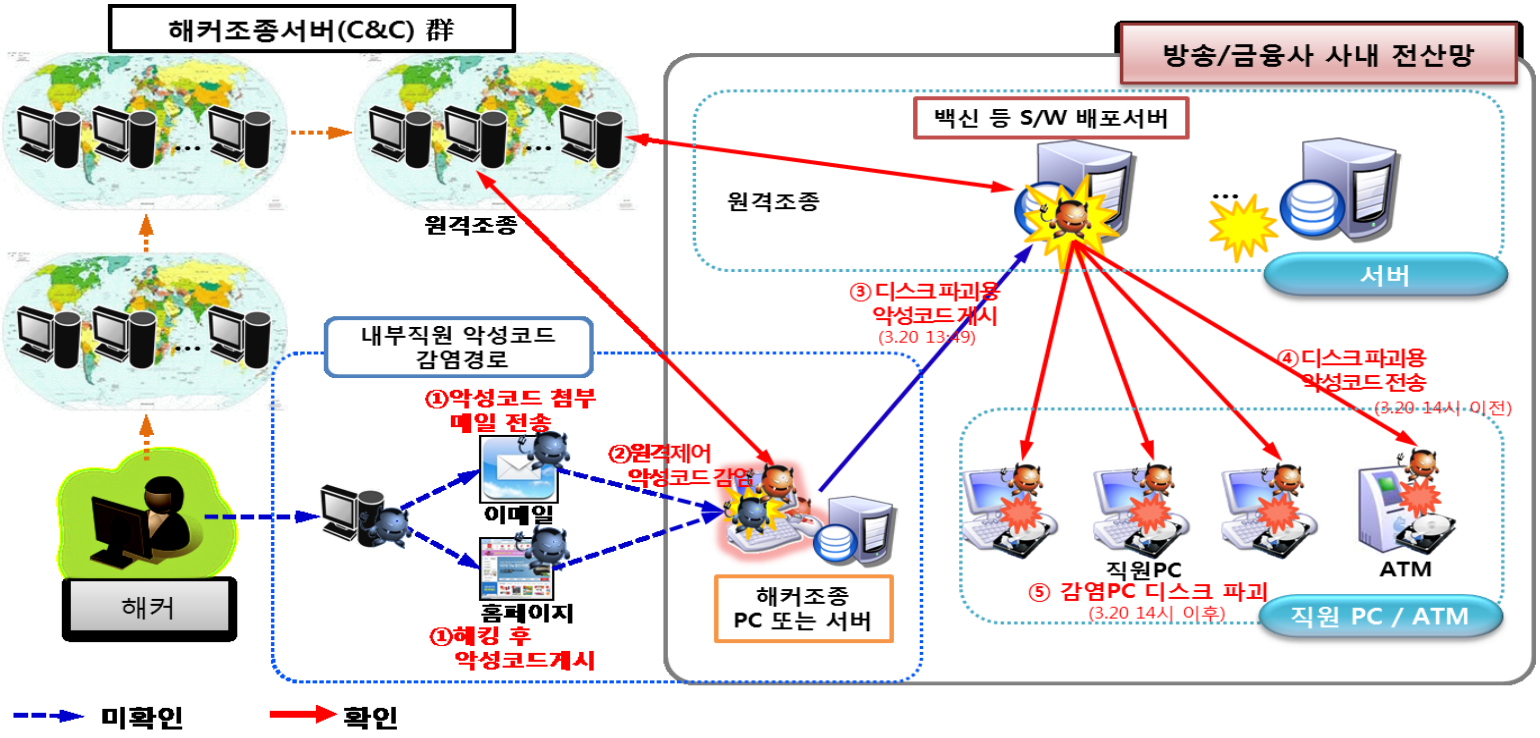


1. 전자금융 보안 위협

▶ APT [Advanced Persistent Threat]

– 특정 대상(기업, 개인 등)을 목표(정보의 탈취, 파괴 등)로 설정하고, 목표 달성을 위해 신규 취약성, 사회 공학적기법 등을 이용한 지능적인 공격을 지속적으로 시도하는 방식

· 사례 : 2011년 4월 농협 서버 270여대 피해, 2013년 3월 방송사 및 금융회사 PC 등 데이터 삭제



1. 전자금융 보안 위협

▶ 중간자 공격 [Man In The Middle Attack]

- 정보 교환 시 중간자가 끼어들어 정보를 도청 및 변조하는 공격을 의미
  - · 중간자의 위치가 통신구간에서 PC상 메모리와 웹 브라우저까지로 확대되고 있음
  - · [사례] 메모리 해킹[웹 페이지 중간자 공격 등]에 의해 2013년 하반기 약85건 피해 발생

Man In The Middle(MITM)

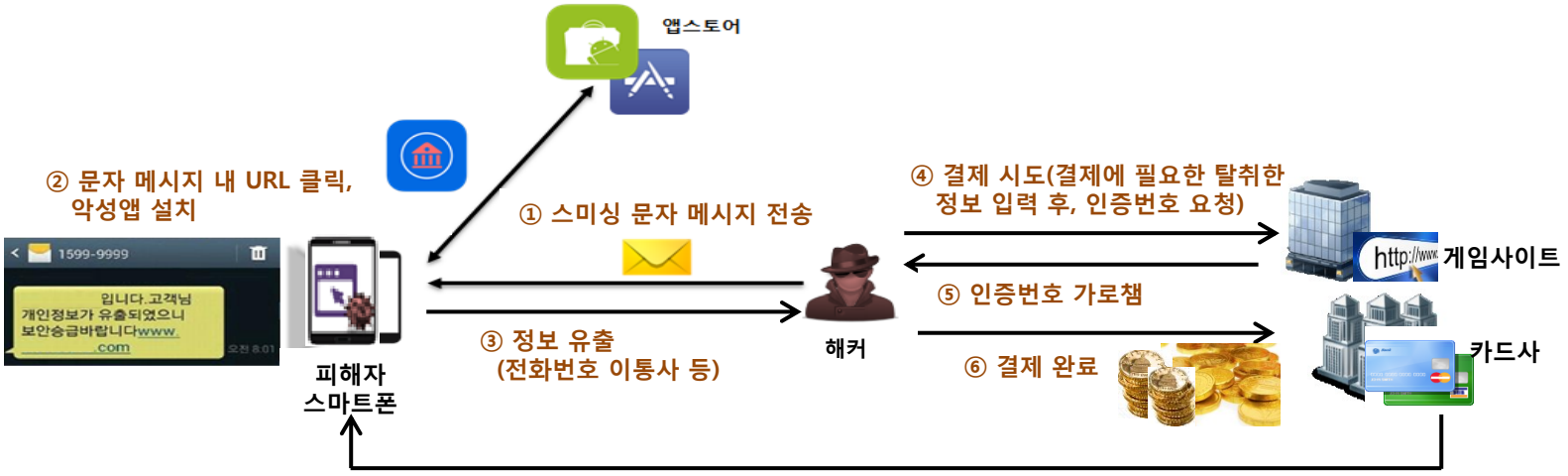
Man In The PC (MITPC)

Man In The Brower (MITB)

1. 전자금융 보안 위협

▶ 스미싱

- 스미싱(Smishing)이란, 문자메시지(SMS)와 피싱(Phishing)의 합성어로, 문자메시지 내 인터넷 주소를 클릭하면 악성코드가 설치되어 개인정보 탈취, 소액결제 등 금전피해를 끼치는 해킹 수법, **최근 금융권 대상 공인인증서 유출, 문자정보 탈취 등 발생**
- 스미싱 피해단계
  - 피해자가 문자메시지 내 URL 클릭 ➔ 스마트폰에 악성코드 설치 ➔해커의 소액결제 인증번호 탈취 ➔ **해커의 사이버 머니 구입 등 소액결제 완료** ➔ 스미싱 피해발생

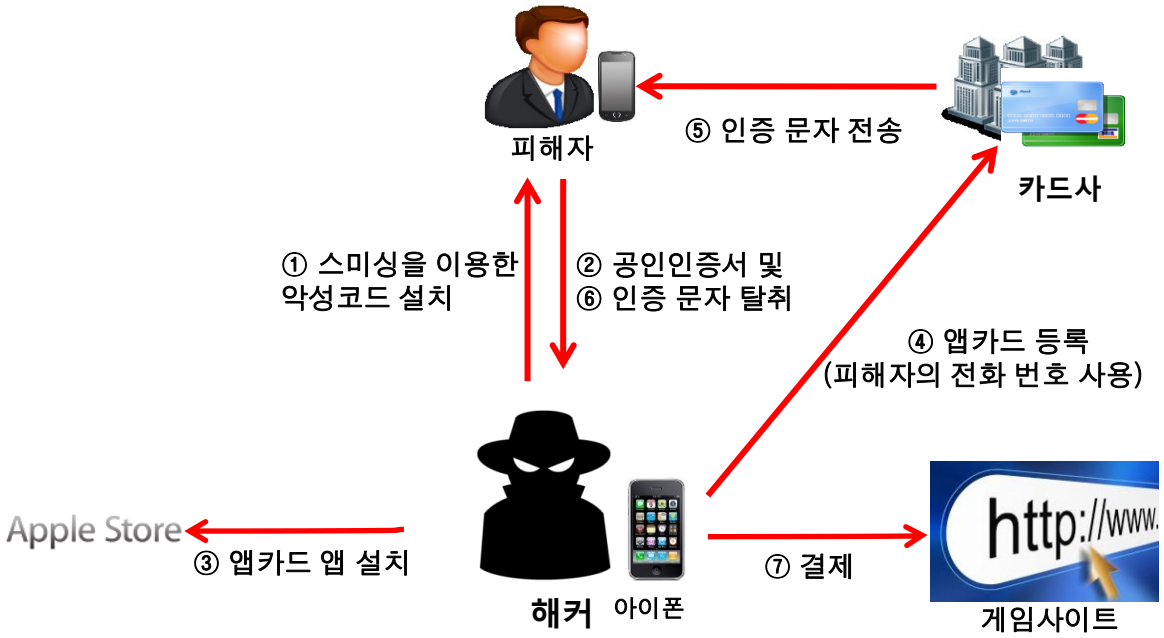


< 스마트폰 인증번호 탈취를 통한 소액결제 스미싱 >

1. 전자금융 보안 위협

▶ 명의 도용

- (아이폰) USIM에서 본인 전화번호를 불러올 수 없는 점을 이용하여 인증번호를 받는 전화번호를 **피해자의 번호로 입력**하여 **인증번호**를 중간에 가로채 **카드를 등록**
- (안드로이드폰) SMS/MMS 등을 공격목표 사용자에게 보내, 공격목표 사용자가 첨부된 **링크를 클릭**하게 되면, **악성코드를 설치**하여 공인인증서 유출 및 문자 메시지 유출



2. 최신 IT융합금융서비스 위협

▶ Big Data를 활용한 금융서비스

Big Data (빅데이터)개념

기존 관리 및 분석체계로는 감당할 수 없는 거대한 데이터의 집합을 지칭하며, 대규모 데이터와 관계된 기술 및 도구(수집 · 저장 · 검색 · 공유 · 분석 · 시각화 등)도 데이터의 범주에 포함

Big Data 활용 금융서비스

· **금융 경영활동 분야**

마케팅, 투자 관리, 트레이딩, 리스크 관리, 고객 서비스, 신규 수익 창출 등

· **금융사고방지**

빅데이터 분석을 통해 금융사기 및 범죄 방지로 피해 · 손실 절감 가능

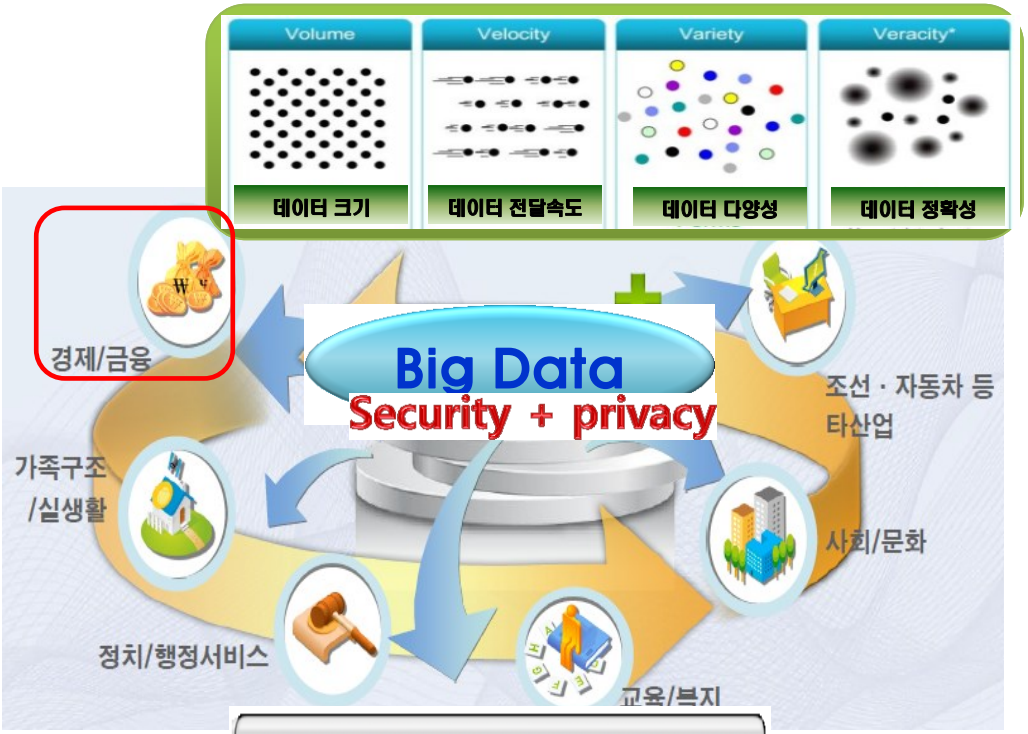
Big Data 활용 금융서비스에서 보안

· **수집 데이터의 보안**

수집되는 데이터 자체에 대한 보호를 위해 암호화, 침입방지, 접근제어, 정보유출방지 · 탐지 등의 보안기술 요구

· **Privacy**

Big Data의 수집/저장/운영/분석 2차 데이터 생성까지 프라이버시의 보호 필요



Big Data 활용 금융서비스와 보안

2. 최신 IT융합금융서비스 위협

▶ IoT 기반 금융서비스

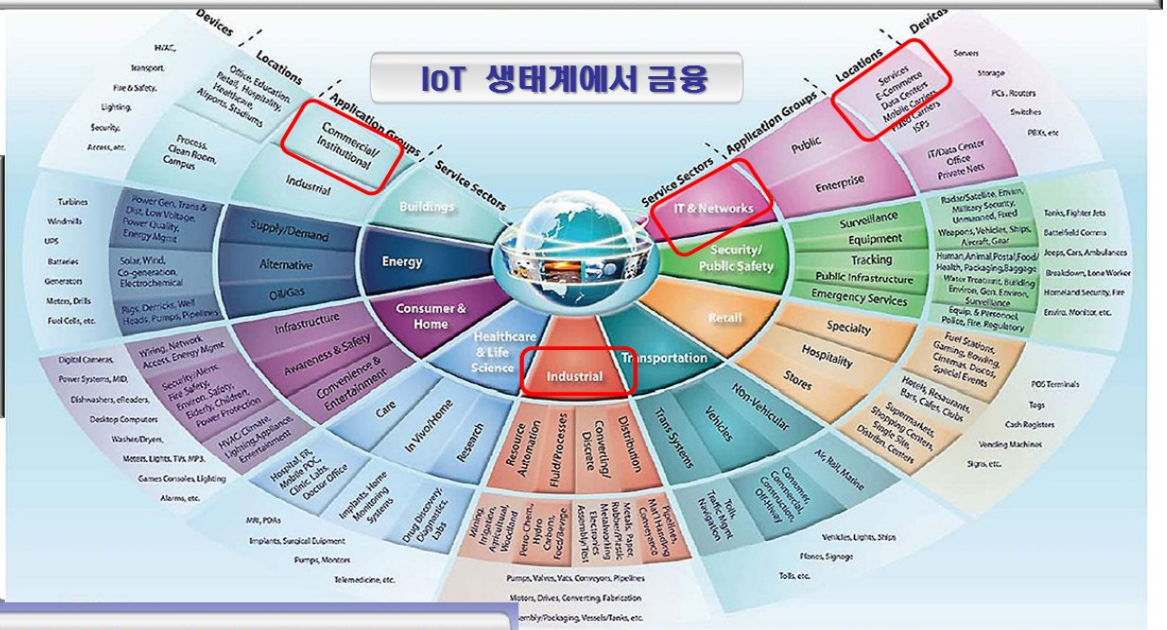
IoT (사물인터넷) 개념

인간, 사물, 서비스 3가지 요소에 대해 상호 협력적으로 소통, 네트워킹, 정보 처리 등 지능적 관계를 형성하는 사물 공간 연결망

IoT 에서 금융의 구성요소

- **스마트 디바이스** : 스마트폰, 스마트 가전(TV, 냉장고), 스마트 카 , 스마트 센서 등
- **센서 네트워크** : NFC, RFID, Bluetooth, Zigbee, WiFi, Li-Fi 등
- **IoT 신규 금융 서비스** : 스마트 디바이스와 센서 네트워크 기술이 생활 환경 곳곳에 이용됨에 따라 기존의 금융 인프라를 기반으로 한 새로운 전자금융서비스

IoT 생태계에서 금융



IoT 환경에서 전자금융서비스 보안

- **Privacy** : 전자금융서비스에서 프라이버시 보호 기술(PET, Privacy Enhancement Technology)의 제공
- **Device and Data Management** : 전자금융서비스 이용 시 디바이스 및 센서를 통해 수집되는 데이터의 기밀성 보장 등 보안성 강화
- **Identity and Trust** : 금융권 정보보호 인프라와 산업시스템의 상호 연동되는 기기 의 신뢰성 보증 강화
- **Security and Compliance** : 신규 전자금융서비스들에 대한 보안 기능 강화와IT 보안 컴플라이언스

3. 전자금융 보안 위협 대응기술

▶ 전자금융 보안 위협 대응을 위한 주요 보안기술을 10개 분야로 구분

Ⅲ 금융보안 거버넌스 강화

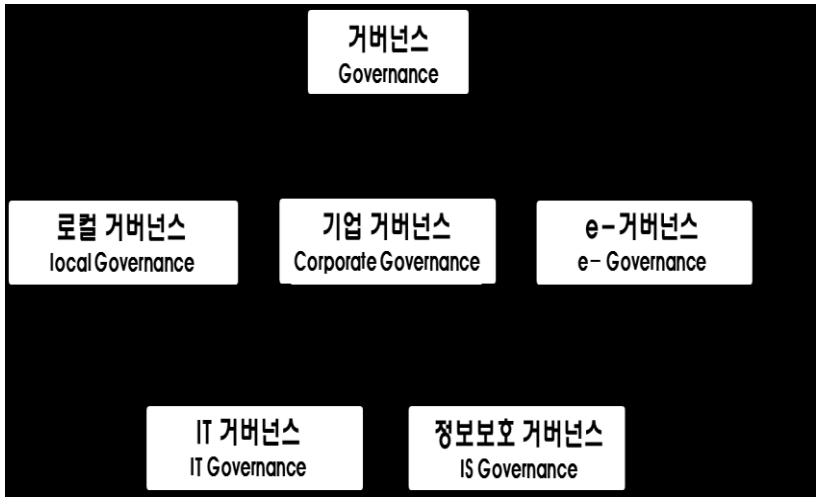
1. 정보보호 거버넌스

▶ 거버넌스 개요 [Governance]

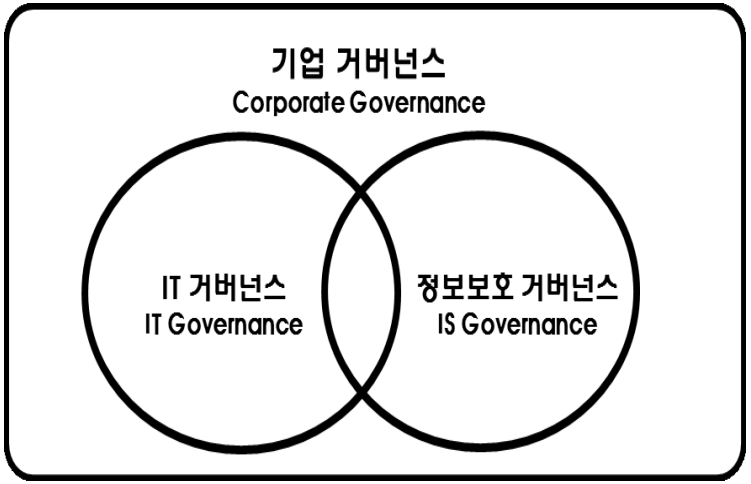
- 정부가 주도하는 통치(Government)가 아닌 **다양한 행위자들의 파트너쉽에 의한 협치**(協治)를 말하며, 사용되는 분야에 따라 조금씩 다른 의미를 내포하고 있음

경영학 : 주주, 종업원, 거래 기업, 지역사회 등 회사 관련 이해관계자들의 이해를 조정하여 의사결정, 결정된 사항의 집행 및 감시 감독(예: Corporate Governance)

행정학 : 정보의 의사결정 과정에 모든 민간 이해 당사자들이 참여하는 새로운 국가 통치 및 관리방식



〈 거버넌스의 주요 유형 〉



〈 기업, IT, 정보보호 거버넌스 간 관계 〉

1. 정보보호 거버넌스

▶ 기업 거버넌스 개요 (Corporate Governance)

기업 거버넌스 정의 (OECD)

- 기업 거버넌스는 기업 내 이해관계자(이사회, 관리자, 주주 등)간의 권한과 책임을 규정하고, 회사 관련 사안들에 대한 의사결정과 결정된 사항의 집행 및 감시절차를 기술
- 기업 거버넌스는 회사 목적과 전략을 설정하는 조직구조를 제공할 뿐만 아니라 그러한 목적을 획득하고 성과를 모니터링하는 수단을 제공

기업 지배 원칙 : 6대 분야 (OECD)

- **효과적인 기업지배구조를 위한 토대 보장** : 법규와 일관성 유지, 책임영역의 명확화
- **주주의 권한과 핵심소유 기능** : 주주의 권한 실행 보호 및 촉진
- **주주의 동등한 대우** : 모든 주주는 동등한 대우를 받을 것을 보장
- **기업지배에 있어서의 투자자의 역할** : 법규 등에 의한 투자자의 권리를 인정
- **공개와 투명성** : 기업의 재정상태, 성과 등 모든 자료가 시기적절하고 정확하게 공개
- **이사회의 책임** : 기업의 전략적 방향 설정, 이사회에 의한 효과적인 감독 등

1. 정보보호 거버넌스

▶ 기업 거버넌스 (Corporate Governance)

법규 준수와 관련된 주요 이슈

- **CSR (Corporate Social Responsibility, 기업의 사회적 책임)**
  - 주주, 고객, 거래처, 종업원 등에 대하여 기업이 지는 사회적 책임
  - 환경대책, 법규 준수(Compliance), 인권보호 등 40개 항목 기준 마련
  - CSR 관련 국제 협약 : UN Global Compact
  - SA8000(Social Accountability 8000) : 미국, 기업SR경영시스템 (현 ISO26000)
    : 기업이 윤리경영을 제대로 하고 있는지를 각 영역별로 평가하여 공인

- **PRI (Principle for Responsible Investment, 책임투자원칙)**
  - 코피 아난 7대 UN 사무총장이 주창(2006년 4월)
  - 금융기관의 투자의사 결정시 투자대상기업의 ESG(Environmental, Social and Governance) 이슈를 고려 (예: 소비자 및 종업원 인권보호, 환경보호 등 비재무적 요소)
  - PRI에 서명한 금융기관들은 기업의 이윤창출 능력뿐만 아니라 ESG요소를 중요한 근거로 투자

1. 정보보호 거버넌스

▶ IT 거버넌스 개요 (IT Governance)

IT 거버넌스 정의

- 기업 지배에 통합된 부분이며, 조직의 IT가 조직의 전략과 목적을 지원하고 확장하는 것을 보증하기 위한 리더쉽, 조직 구조, 프로세스로 구성, "이사회와 이사급 경영진의 책임" 정의

IT 거버넌스 목적

- 기업과 IT를 연계시키고 약속한 효익을 실현함
- 기회를 이용하고 이익을 극대화 할 수 있도록 IT를 사용함
- IT 자원을 책임감 있게 사용함
- IT 관련 위험을 적절히 관리함

IT 거버넌스 이슈 (참고)

- 최고경영진은 CIO와 IT 조직이 비즈니스 가치를 구현하도록 어떻게 하는가?
- 최고경영진은 CIO와 IT 조직이 자금 횡령, 잘못된 프로젝트에 투자하지 않도록 어떻게 하는가?
- 최고경영진은 CIO와 IT 조직을 어떻게 통제하는가?

1. 정보보호 거버넌스

▶ 보안 거버넌스 개요 (Security Governance)

보안 거버넌스 정의

- 보안 거버넌스는 기업 거버넌스의 부분집합으로 전략적 방향을 제시하고 목적 달성, 적절한 위험관리, 조직자산의 책임 있는 사용, 기업 보안 프로그램의 성공과 실패가 모니터링 됨을 보장
- 보안 거버넌스는 정보의 기밀성(Confidentiality), 무결성(Integrity), 연속성(Availability)을 위한 "이사회와 고위 경영진의 책임"으로 정의

보안 거버넌스 산출물 : 6가지

- **전략적 연계** : 조직의 목적을 지원하기 위한 정보보호와 사업전략 연계
- **가치전달** : 조직의 목적을 지원함에 있어서 최적화된 정보보호 투자
- **자원관리** : 정보보호 지식과 인프라를 효율적이고 효과적으로 이용
- **위험관리** : 정보자산의 잠재적 위험을 수용 가능한 레벨로 감소시키기 위한 적절한 수단 및 실행
- **성과측정** : 목표가 달성됨을 보장하는 정보보호 프로세스 측정, 모니터링과 보고
- **프로세스 통합** : 보안을 위한 조직 내 관리 보증 프로세스들의 통합

1. 정보보호 거버넌스

▶ 보안 거버넌스 개요 (Security Governance)

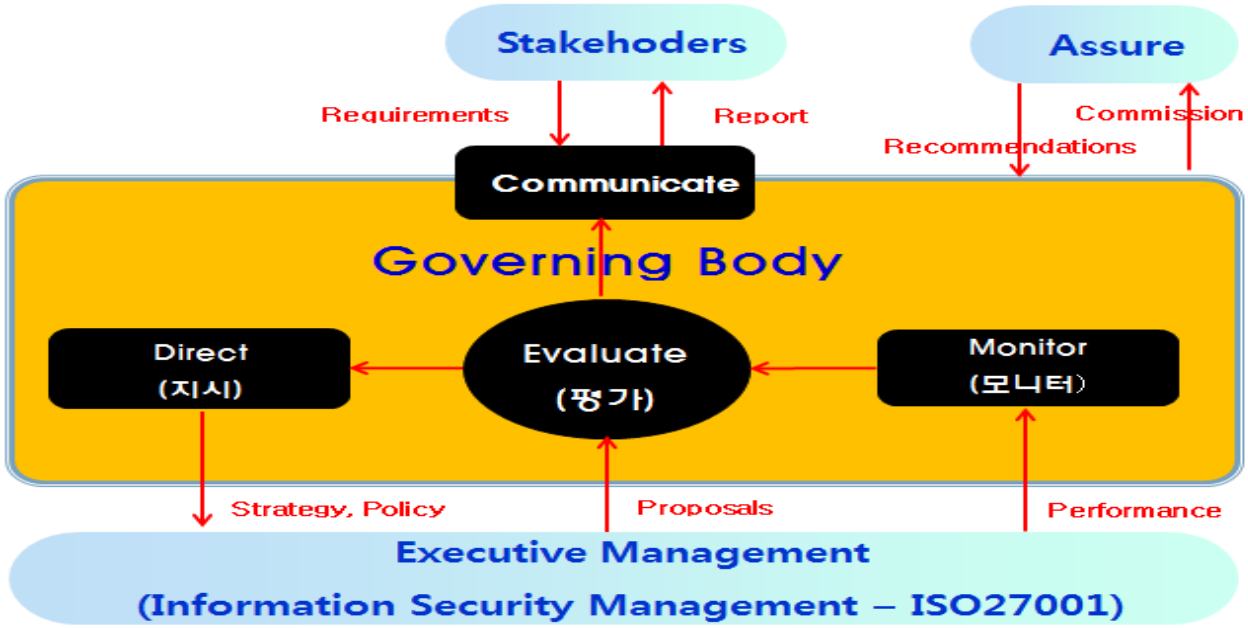
– 보안 거버넌스의 산출물과 관리 책임의 관계(예시)

구분	전략적 연계	위험관리	가치전달	성과측정	자원관리	프로세스 통합
이사회	• 명확한 연계 요구	• 위험허용도 수립 • 위험관리 정책감독 • 법규 준수 보장	• 보안비용 보고 요구	• 보안 효과성 보고 요구	• 지식관리와 자원 활용 감독	• 프로세스 통합 보증 정책 감독
임원	• 보안을 비즈니스 목적과 통합하는 프로세스 규정	• 모든 활동 내 위험 관리를 포함한 R&R 규정 • 법규준수 모니터	• 보안 구상 (initiatives)의 사업사례 연구 요구	• 보안활동 모니터링 및 측정지표 요구	• 지식획득과 효율적인 측정지표를 위한 프로세스 보증	• 통합을 위한 계획과 모든 보증요소 감독 제공
운영 위원회	• 보안전략과 통합 노력 검토와 지원 • 비즈니스 소유자의 통합지원 보장	• 신규 위험 식별 • 비즈니스 단위의 보안실무 촉진 및 법규준수 이슈 식별	• 비즈니스 기능을 지원하는 보안 구상의 타당성 검토 및 지원	• 보안구상의 사업 목적 충족 여부 검토 및 권고	• 지식획득과 배포 프로세스 검토	• 핵심 비즈니스 프로세스, 보증 제공자 식별 • 보증통합 노력 관리
CISO	• 보안전략 및 보안 프로그램 개발	• 위험/사업영향 평가 수행보장 • 위험완화 전략 개발 • 정책과 법규 준수 강제	• 보안자원 이용과 효과성 모니터링	• 모니터링 및 측정 지표 개발과 구현, 보안활동 지시와 모니터	• 지식 획득과 배포 방법론 개발 • 효과성 및 효율성 지표 개발	• 다른 보증제공자와 연락 • 중첩된 부분 식별 보장
감사	• 연계 수준에 대한 평가와 보고	• 조직 위험관리 실무와 결과에 대한 평가와 보고	• 효율성에 대한 평가와 보고	• 측정의 효과성 정도와 사용척도에 대한 평가와 보고	• 자원관리의 효율성에 대한 평가와 보고	• 상이한 관리영역에서 수행되는 보증프로세스의 효과성에 대한 평가와 보고

1. 정보보호 거버넌스

▶ 정보보호 거버넌스의 국제 표준 : ISO 27014 (2013년)

- 의사결정 권한과 책임의 할당, 비즈니스와 전략적 연계, 관련 법과 규정의 준수를 위한 프로세스 및 실행 체계
- 특히, 정보보호 거버넌스 **핵심 활동**인 Evaluate(평가), Direct(지시), Monitor(모니터)를 중심으로 Governing Body와 Executive Management (ISO27001) 역할 및 책임 정의



※ ISO 27014 Governance of information security

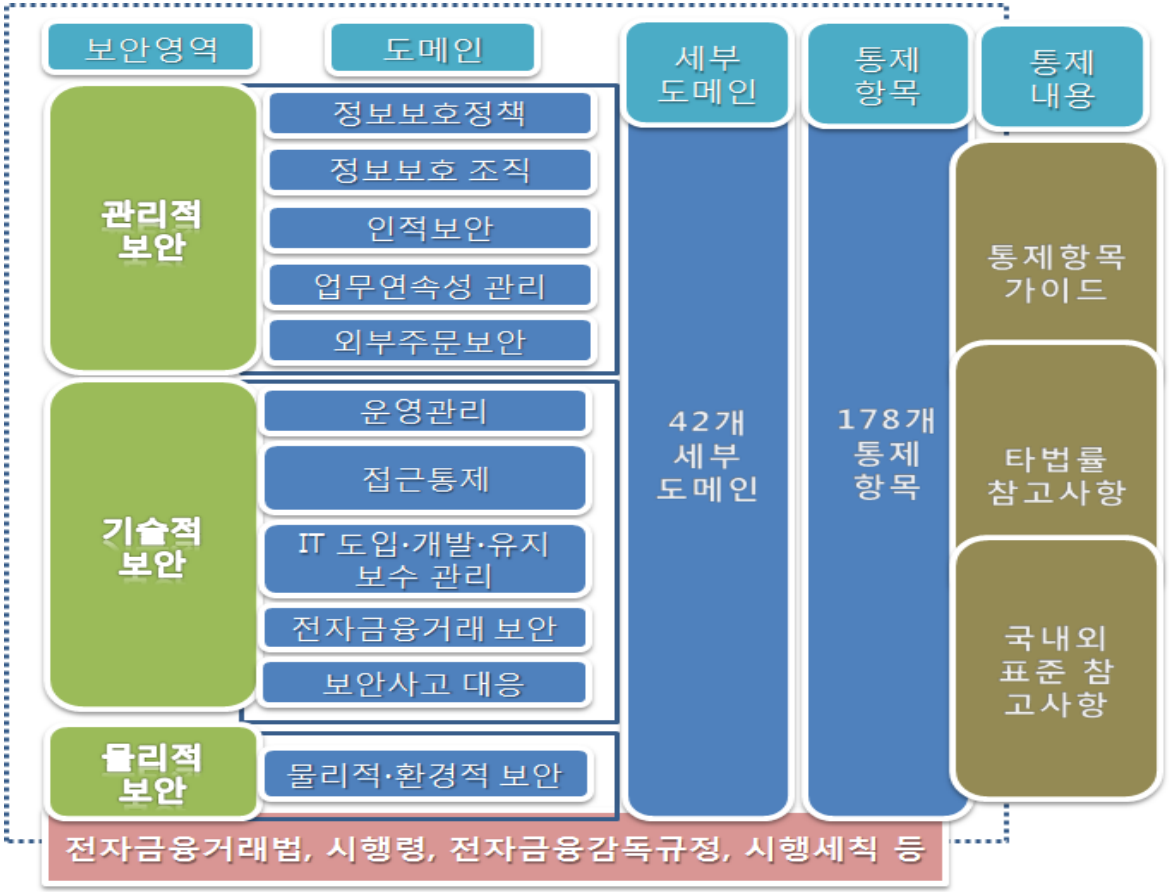
2. 금융권 컴플라이언스 가이드

▶ 금융IT 보안 컴플라이언스 가이드 – [분석 대상 및 도메인 구성]

2. 금융권 컴플라이언스 가이드

▶ 금융IT 보안 컴플라이언스 가이드 – [가이드 구성 (ver 1.1, 2014.5)]

– 11개 도메인, 42개 세부도메인, 178개 통제 항목



2. 금융권 컴플라이언스 가이드

▶ 금융개인정보보호 컴플라이언스 가이드 – [분석 대상]

금융개인정보보호 컴플라이언스 참조가이드

도메인 및 통제 항목(9개 도메인, 84개 통제)

1. 정책(3개) 2. 조직 및 책임(3개) 3. 인적보안(2개) 4. 영상정보 처리기기의 보안(5개) 5. 위수탁 보안(6개) 6. 보안사고 대응(4개)

7. 안전성 확보조치(8개) 8. 정보주체의 권리보장(15개) 9. 처리단계별 보호(38개)

통제항목가이드

- 금융분야 개인 정보보호 가이드라인
- 개인정보자체점검체크리스트
- 개인정보보호법령 및 지침고시 해설서
- 개인정보의 안전성확보조치 기준 고시 및 해설서
- 개인정보 위험도 분석 기준 및 해설서
- 개인정보 암호화 조치 안내서
- 개인정보 영향평가고시 및 해설서
- 개인정보영향평가 수행안내서

금융관련 특별법

- 전자금융거래법
- 금융실명제법
- 금융지주회사법
- 은행법
- 자본시장법
- 보험업법
- 여신전문금융업법
- 상호저축은행법
- 전기통신금융사기 피해급 환급에 관한 특별법
- 금융기관의 업무 위탁등에 대한 규정
- 특정 금융거래정보의 보고 및 이용등에 관한 법률

기타 타법관련

- 정보통신망법
- 위치정보법
- 통신비밀보호법
- 근로기준법
- 주민등록법
- 전자서명법
- 국가인권위원회법
- 소비자기본법
- 전자거래기본법
- 전자상거래법
- 전자어음발행유통법
- 외부감사에 관한 법률
- 외국환거래법

국내외 표준

- PCI DSS Ver2.0
- ISO 27001
- 정보보호관리체계 인증
- BASEL Ⅲ
- 개인정보보호관리체계인증

개인정보보호법

- 동법 시행령, 시행규칙
- 표준 개인정보보호 지침
- 개인정보의 안전성 확보 조치

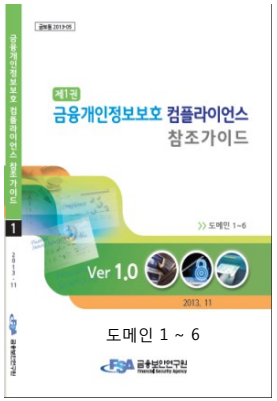
신용정보법

- 동법 시행령, 시행규칙
- 신용정보감독규정
- 신용정보감독업무 시행세칙

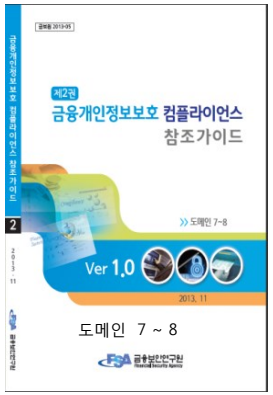
2. 금융권 컴플라이언스 가이드

▶ 금융개인정보보호 컴플라이언스 가이드 – [가이드 구성(ver 1.0, 2013.11)]

– 9개 도메인, 84개 통제 항목



도메인 1 ~ 6



도메인 7 ~ 8

분석내용

관련 법률

일반법

1. 개인정보보호법

- 동법 시행령, 시행규칙
- 표준 개인정보보호 지침
- 개인정보의 안전성 확보 조치

특별법

2. 신용정보법

- 동법 시행령, 시행규칙
- 신용정보감독규정
- 신용정보감독업무 시행세칙

도메인

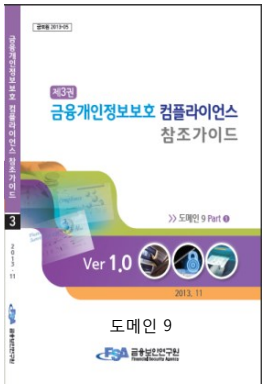
1. 정책
2. 조직 및 책임
3. 인적 보안
4. 영상정보처리기기의 관리
5. 위수탁 보안
6. 보안사고 대응
7. 안전성 확보조치
8. 정보주체의 권리보장
9. 처리단계별 보호

도메인·통제항목

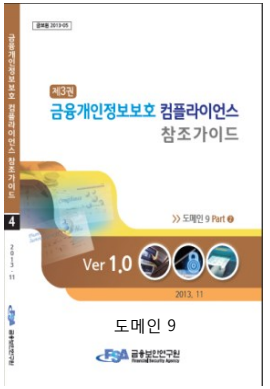
9개 도메인 84개 통제항목

금융 관련 특별 법률 참조사항

1. 전자금융거래법
2. 금융실명거래법
3. 금융지주회사법
4. 은행법
5. 자본시장법
6. 보험업법
7. 여신전문금융업법
8. 상호저축은행법
9. 전기통신금융사기 피해금 환급에 관한 특별법
10. 금융기관의 업무위탁등에 대한 규정
11. 특정 금융거래정보의 보고 및 이용등에 관한 법률



도메인 9

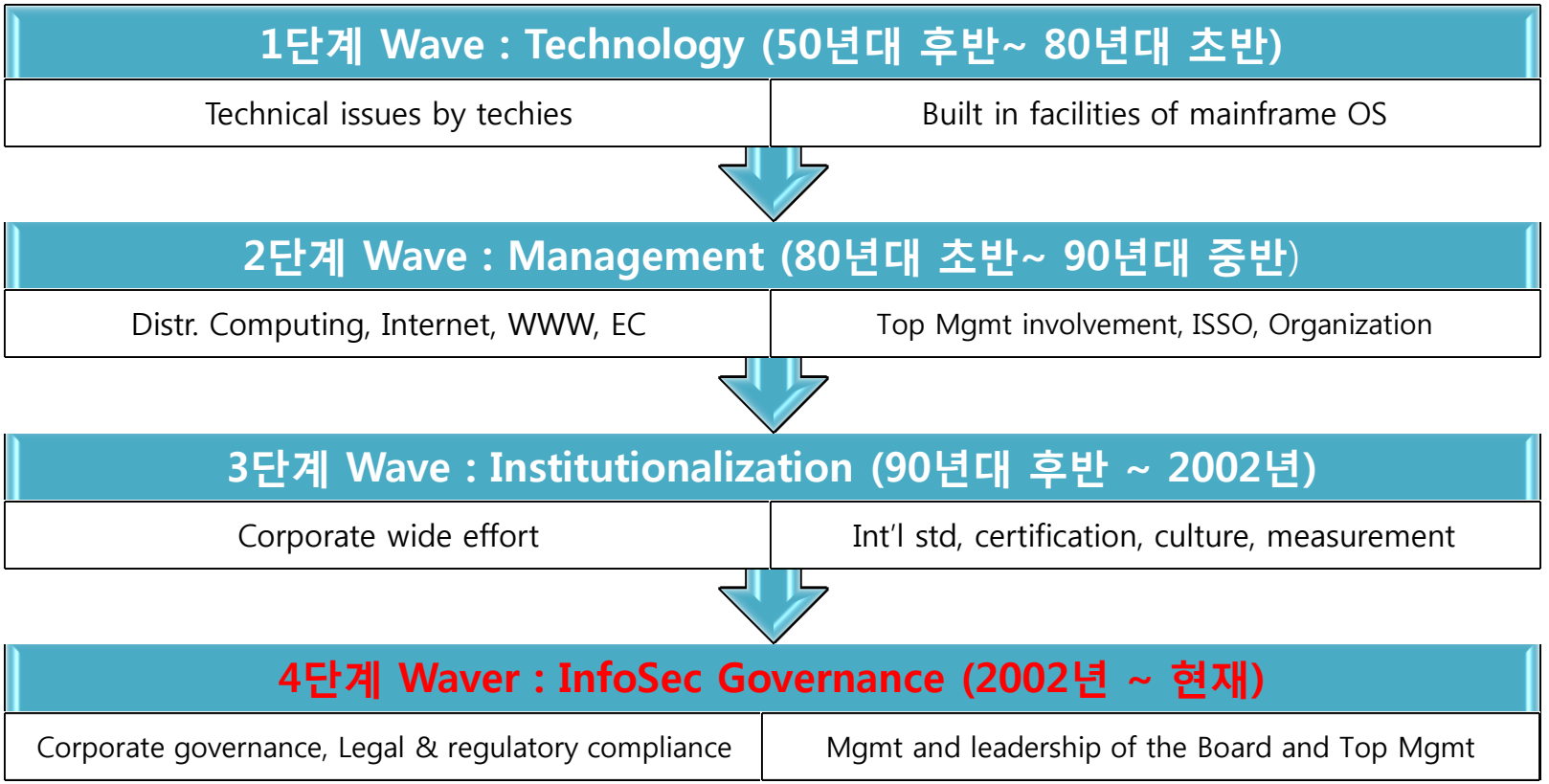


도메인 9

3. 금융보안 거버넌스 추진 방향

▶ 정보보호 패러다임 변화

– 정보보호(Information Security) 패러다임은 기술적 관점에서 관리, 제도화 단계를 지나 정보보호 거버넌스 단계로 진입함



[출처] B. Solms, Information Security-The Fourth Wave, Computers and Security, 2006

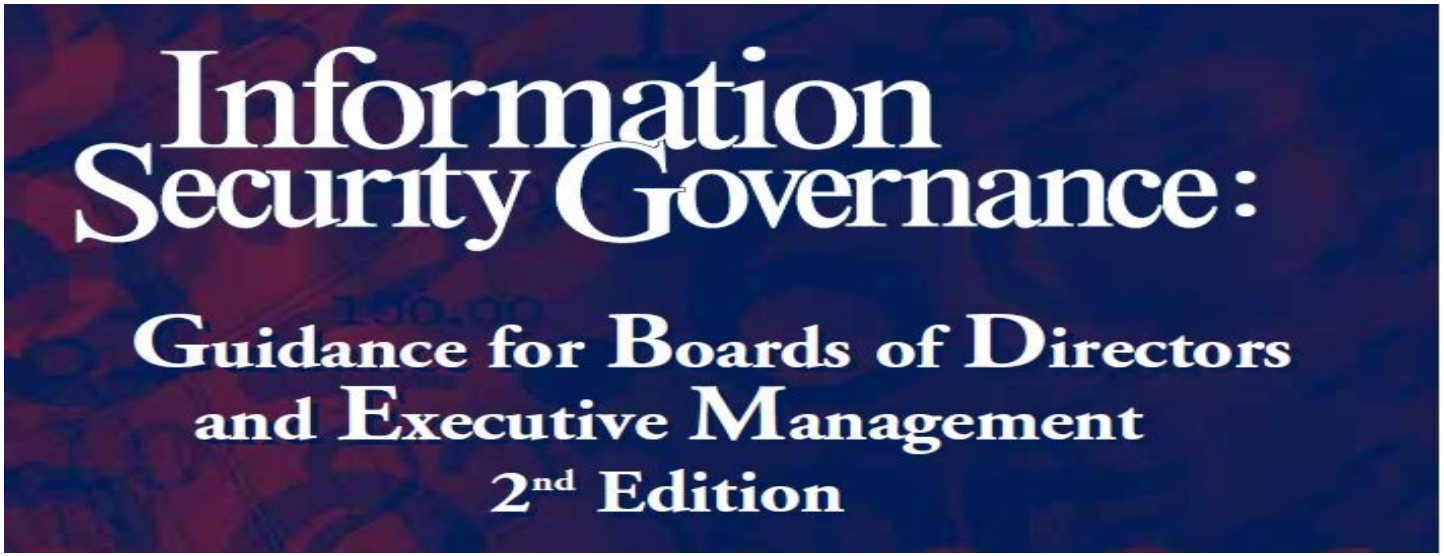
3. 금융보안 거버넌스 추진 방향

▶ (사례) 정보보호 거버넌스 가이드

- '06년 미국 ITGI (IT Governance Institute) 는 **정보보호 거버넌스** 관련 **이사회**와 **경영진**을 위한 가이드를 발간

※ ITGI : '98년 ISACA에 의해 설립, IT 거버넌스, 관리 등 관련 저널, 교육, 컨퍼런스 개최 등 수행

- 본 가이드는 정보보호 거버넌스 개념, 중요성, **역할 및 책임(이사회, 경영진, 위원회, CISO 등)**, **성공적인 구축 전략** 등을 담고 있음



3. 금융보안 거버넌스 추진 방향

▶ 금융보안 거버넌스 체계 구축

- 전 금융권으로 금융보안 거버넌스 체계가 확산될 수 있도록 금융회사 경영진의 인식 전환 및 구체적인 실행방안 등 **금융보안 거버넌스 확립 방안**을 수립

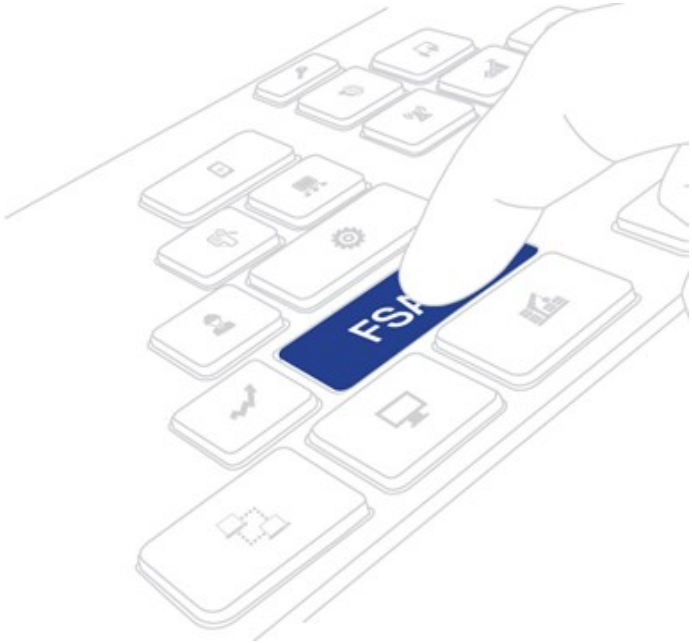
> * **확립 방안의 주요 내용** : 이사회, C-Level(CEO, CISO 등), 실무부서 등 역할 및 책임 명확화, CISO 통제권 강화, 보안활동의 모니터링 및 효과성 측정 방법, 외부 보안감사 역할 등

- 금융보안 거버넌스 확립방안에 대한 객관성 확보를 위해 산 · 학 · 연 전문가를 선정하여 "**금융보안 거버넌스 자문위원회**" 운영 중(14.4월)

- 국내 금융회사 보안 거버넌스 현황 파악을 통해 "**금융보안 거버넌스 체계 구축을 위한 중장기 계획**" 수립 예정(14.7월)

- 국내 금융회사 조직체계 등 현황조사 및 국제 표준 및 우수 사례 등을 조사·분석하여 "**금융보안 거버넌스 가이드라인**" 발간 예정 (14.12월)

감사합니다



금융보안연구원
Financial Security Agency