개인정보보호법 대응을 위한 스마트 컴플라이언스 전략

2011/05/18

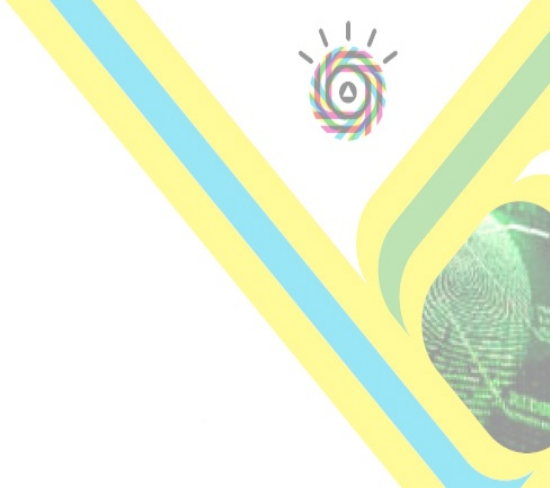
나병준 차장,IBM기술영업,CISSP

IBM Security Summit

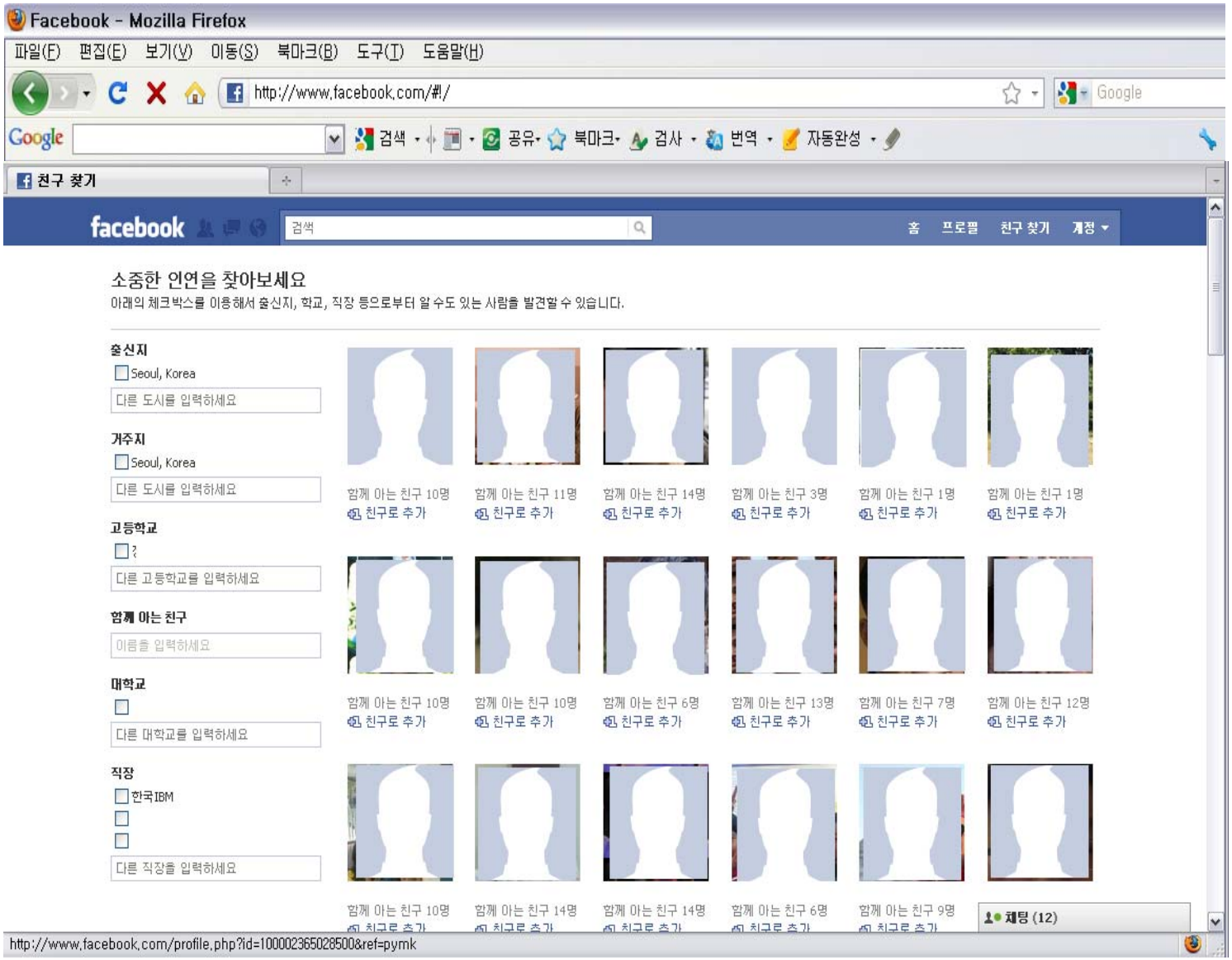
IBM Security Solutions. Secure By Design.

Agenda

- Introduction
- 개인정보보호법의 내용 및 고려사항
- 개인정보보호법에 대한 대응
- Closing



개인정보와 보안

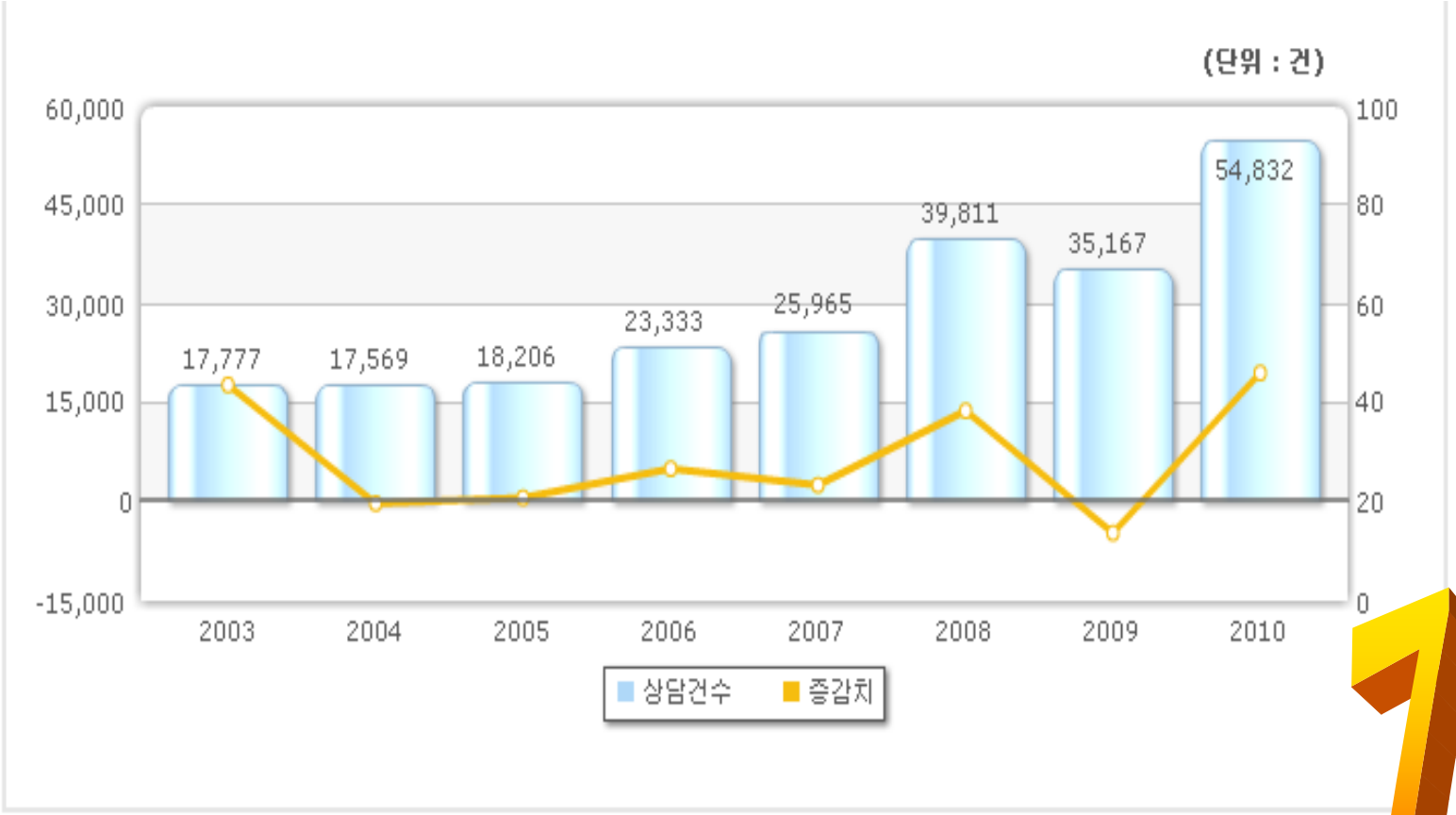


5.5

개인정보와 보안

- 인터넷 추적(Online tracking)
- 미국 중간 선거: 정치적 성향, 종교, 환경, 낙태…
- 쿠키: 연령, 성별, 거주지, 정치적 성향, 자녀, 연봉 수준…
- 인터넷 사용 행태

개인정보와 보안



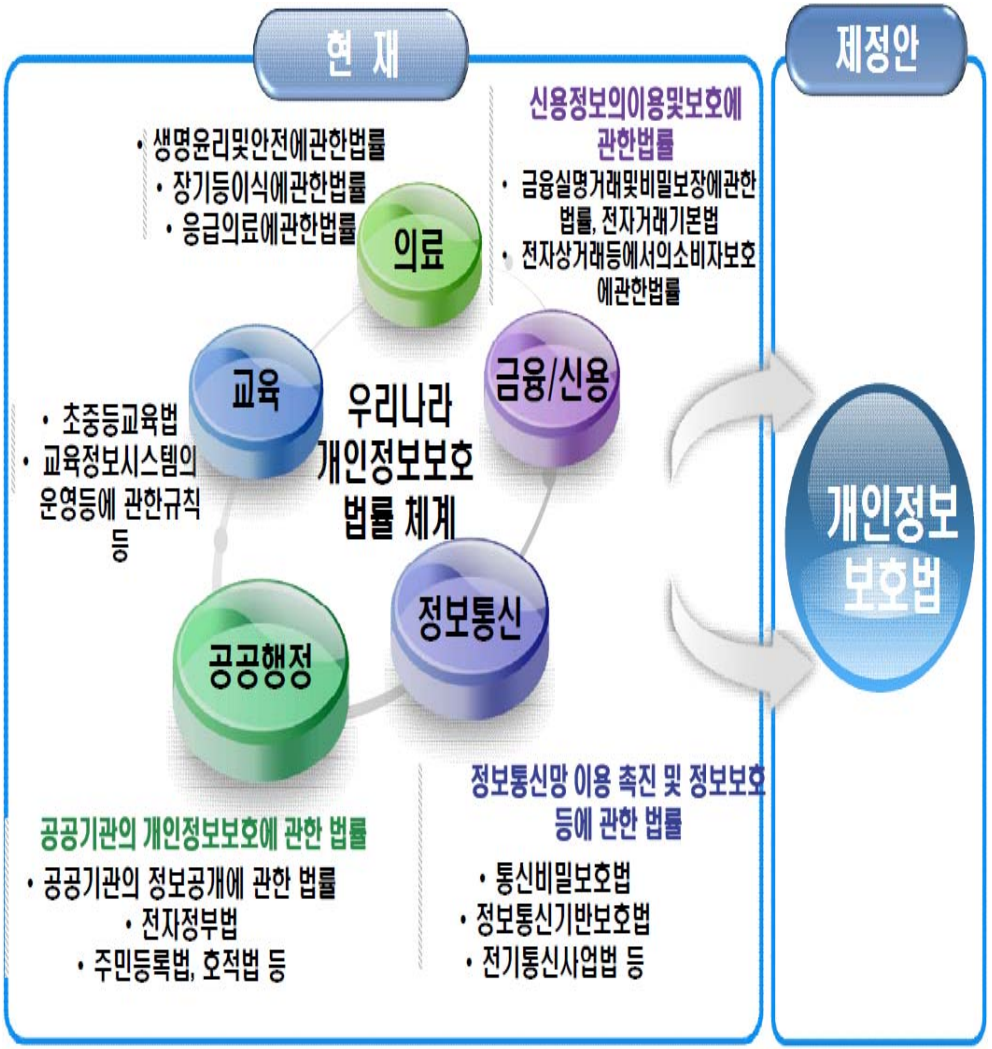
출처: KISA ISIS 인터넷통계정보시스템

개인정보와 보안

개인정보보호 2.0 시대의 개막 "개인정보보호법 제정·공포"

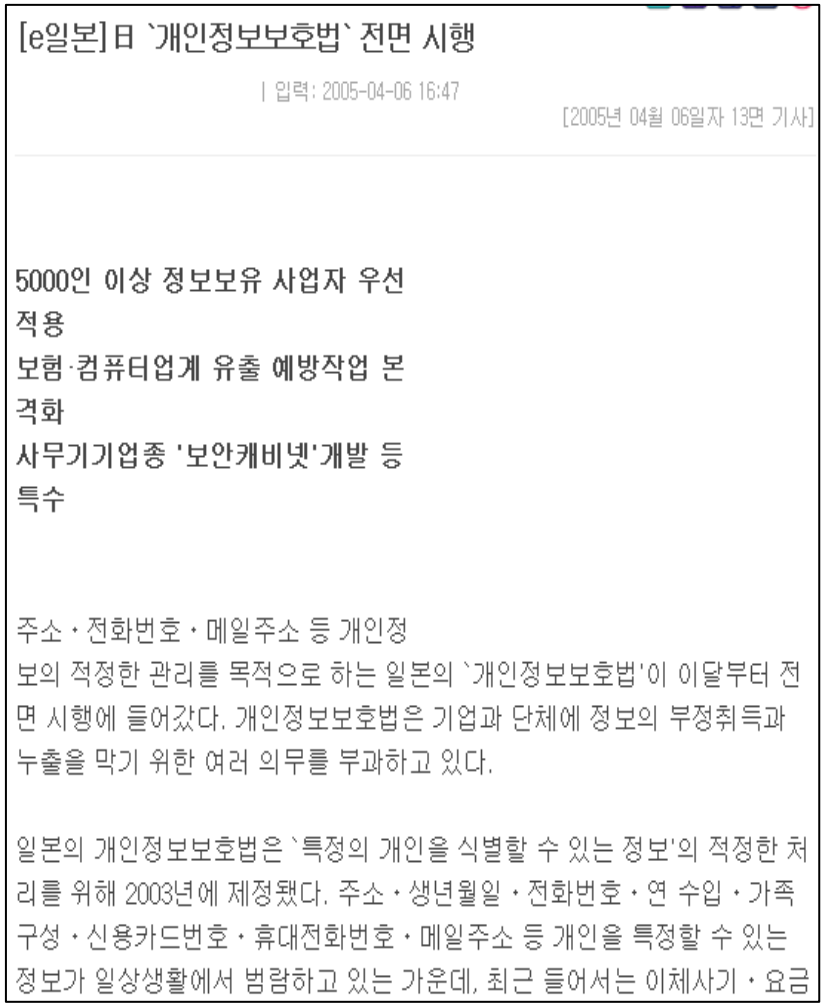
- 모든 공공기관·사업자를 규율대상으로 9월30일 전면시행 -

□ 2004년부터 입법논의가 시작된 『개인정보보호법(법률 제10465호)』이 3월 29일 공포되고, 공포 이후 6개월이 경과되는 2011년 9월 30일부터 전면 시행된다.



** 한국인터넷진흥원 발행 사업자를 위한 개인정보보호 질의 응답집에서 발췌

개인정보와 보안



[e일본]日 `개인정보보호법` 전면 시행

| 입력: 2005-04-06 16:47

[2005년 04월 06일자 13면 기사]

5000인 이상 정보보유 사업자 우선
적용
보험·컴퓨터업계 유출 예방작업 본
격화
사무기기업종 '보안캐비넷'개발 등
특수

주소·전화번호·메일주소 등 개인정
보의 적정한 관리를 목적으로 하는 일본의 `개인정보보호법'이 이달부터 전면 시행에 들어갔다. 개인정보보호법은 기업과 단체에 정보의 부정취득과 누출을 막기 위한 여러 의무를 부과하고 있다.

일본의 개인정보보호법은 `특정의 개인을 식별할 수 있는 정보'의 적정한 처리를 위해 2003년에 제정됐다. 주소·생년월일·전화번호·연 수입·가족구성·신용카드번호·휴대전화번호·메일주소 등 개인을 특정할 수 있는 정보가 일상생활에서 범람하고 있는 가운데, 최근 들어서는 이체사기·요금

- 니혼 생명: 전용키 전용 휴대 단말(50억 엔)
- 일본 전국은행 협회: DM/전화 영업 자율금지
- 히타치: HDD없는 전용 단말 도입(12억 엔)
- 미쓰비시 전기: 출입통제시스템 강화(25억 엔)

- 2004년 누출사건: 366건 (1,044만명)
- 2005년 : 1,032건 (881만명)

Agenda

- Introduction
- 개인정보보호법의 내용 및 고려사항
- 개인정보보호법에 대한 대응
- Closing

개인정보보호법의 내용 및 고려사항

- 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다 (개인정보보호법, 제2조)

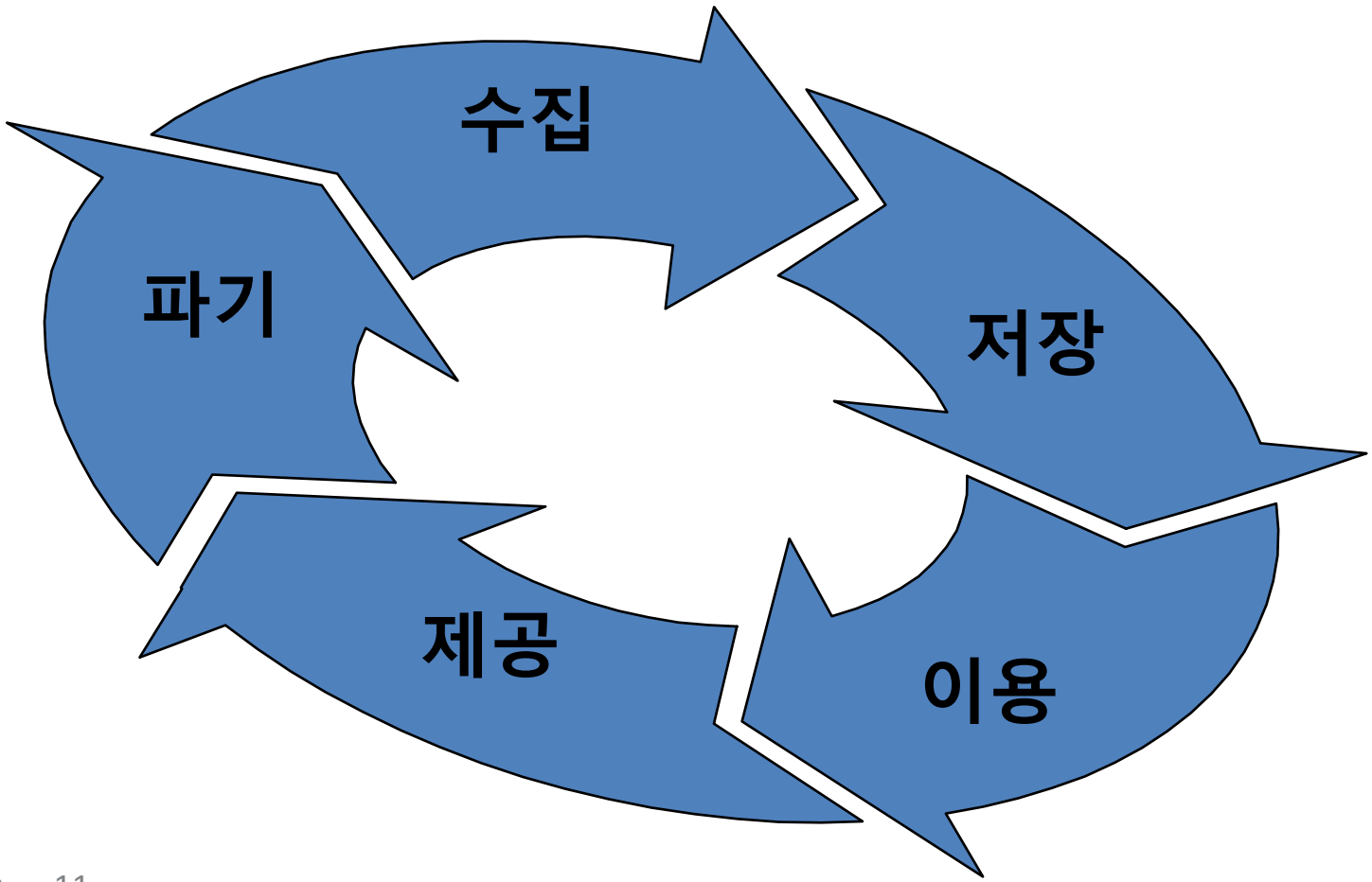
개인정보보호법의 내용 및 고려사항

- 속성정보: 이름, 성별, 나이, 생년월일, 주민등록번호, 주소, 전화번호…
- 활동정보
  - 가족, 출신 및 생활환경 : 결혼, 가족관계, 습관, 주거…
  - 학력 및 교육: 학력, 출신학교, 성적…
  - 고용 및 경력: 취업, 사업경력, 인사…
  - 재산.신용.납세 : 수입, 임금, 지출, 채무…
  - 사회보장/행정서비스: 정부로부터 급부, 급여, 면허…
  - 기타: 기타 개인 일상생활과 관련된 정보
- 민감정보: 인종.민족, 국적, 정치적 성향, 종교, 노조, 보건, 의료, 병역.."개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보"

출처: KISA 개인정보영향평가 가이드

개인정보보호법의 내용 및 고려사항

- 개인정보의 처리: 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위 (개인정보보호법, 제2조)



개인정보보호법의 내용 및 고려사항

정보보호 영역 (기밀성, 무결성, 가용성)

Privacy 영역 (오남용)

개인정보보호법의 내용 및 고려사항

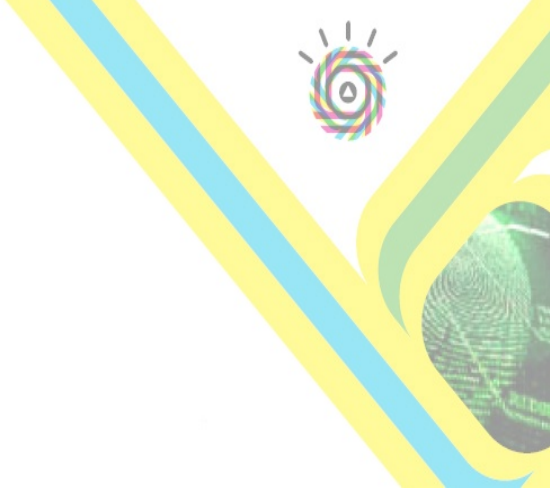
- 개인정보 보호법: 법률 제10465호, 2011.3.29 제정, 2011.9.30 시행

- 개인정보의 수집
  - 정보주체 동의 하에 최소한의 개인정보 수집
  - 최소한의 정보 외 개인정보 수집 미 동의에 대한 재화/서비스 제공 거부 금지
  - 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있어야 함
- 개인정보의 제공
  - 정보주체 동의(제공받는 자의 보유 및 이용기간 포함) 하에 제3자에게 제공(공유)
- 개인정보의 이용
- 개인정보의 파기
  - 보유기간 경과, 처리 목적 달성 후 지체 없이 개인정보 파기(타 법령 참조 필요)

개인정보보호법의 내용 및 고려사항

- 개인정보 처리 제한: 민감정보 처리 금지(별도 동의/법령에서의 요구)
- 고유식별정보 처리 제한 : 별도 동의, 주민등록번호 외 가입방법 제시, 암호화 등
- 공개된 장소에서의 영상정보처리기기의 제한
  - 목적: 구체적인 법령 사항, 범죄 예방/수사, 시설안전/화재, 교통단속...
  - 설치목적에 반한 임의조작, shooting range변경, 녹음 금지

개인정보보호법의 내용 및 고려사항



- 안전조치 의무: 기술적/관리적/물리적 조치 (대통령령)
- 개인정보 처리방침 수립.공개(대통령령)
- 개인정보 보호책임자 지정
- 공공기관
  - 개인정보파일의 등록/공개
  - 개인정보 영향평가
- 개인정보 유출 통지 의무

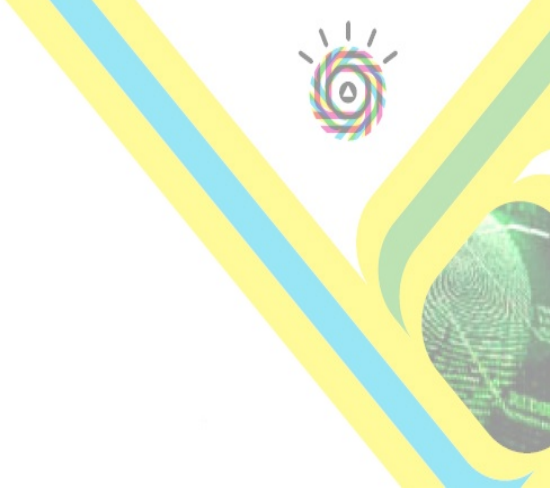
개인정보보호법의 내용 및 고려사항

- 개인정보 분쟁조정위원회: 집단분쟁조정...
- 개인정보 단체소송

- 적용제외
  - 통계법, 국가안전보장, 공중위생, 언론/종교단체/정당(취재.보도, 선교, 선거 입후보자 추천 등)
  - 동창회, 동호회 등 친목단체(일부 조항 제외)
- 벌칙
  - 징역, 벌금
  - 양벌규정
  - 과태료

Agenda

- Introduction
- 개인정보보호법의 내용 및 고려사항
- 개인정보보호법에 대한 대응
- Closing



개인정보보호법에 대한 대응

개인정보보호법에 대한 대응

- 개인정보 파악
- 개인정보의 처리 용도 정의
- 개인정보 Lifecycle에 따른 보호 조치 정의 및 적용
  - 저장
  - 이용
  - 파기

개인정보보호법에 대한 대응

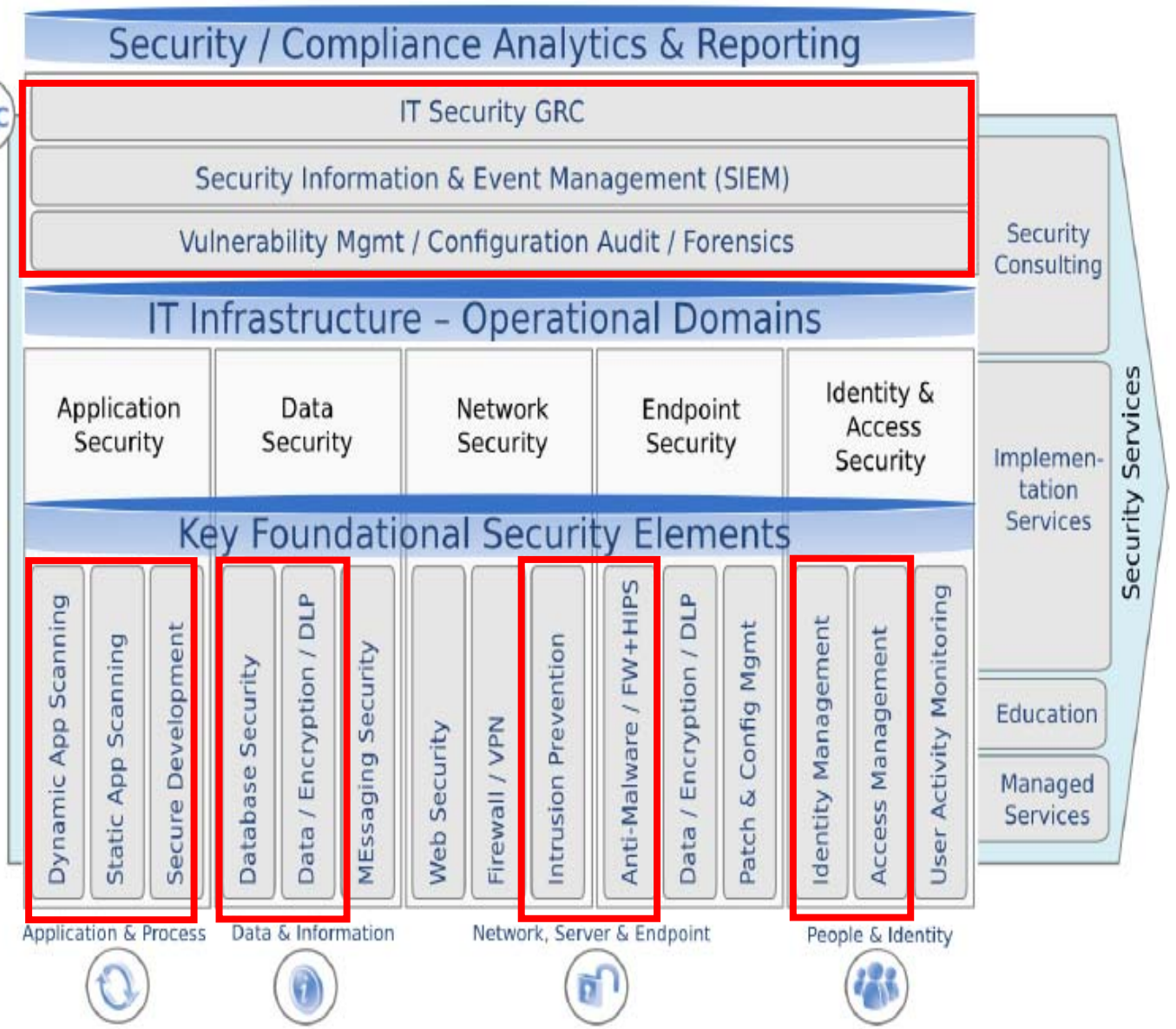
- 개인정보보호에 대한 관리계획 수립.시행
  - 내부 관리계획
  - 개인정보 보호 조직 (개인정보관리책임자 등)
  - 개인정보 Lifecycle(처리단계)에 대한 보호조치 명시
    - 수집
    - 이용
    - 저장
    - 제공(전송) – 제3자와의 합의서
    - 파기
  - 정기적 자체 감사
  - 개인정보취급자에 대한 교육 등
  - 물리적 접근 제한

- 개인정보영향평가

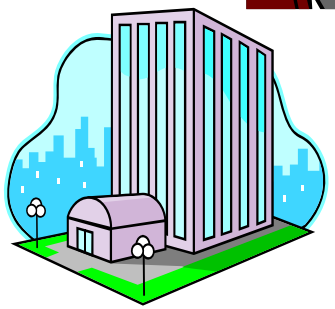
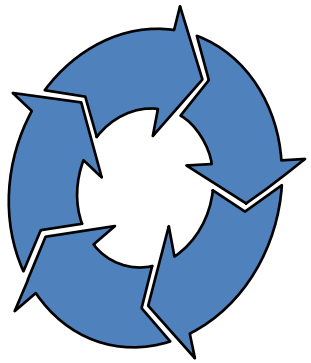
개인정보보호법에 대한 대응

- 접근권한, 인증 및 계정 관리
  - 접근권한의 차등 부여
  - 주기적인 접근 권한 관리
  - 권한 부여,변경, 말소에 대한 기록의 최소 5년 보관
  - 계정, 비밀번호 규칙
- 개인정보의 암호화 : 주민등록번호, 신용카드번호, 계좌 번호 등
- 접근통제: 불법 접근 및 침해사고 방지를 위한 시스템 설치.운영
- 접속 기록의 위.변조 방지
  - 개인정보처리시스템 접속 기록의 월1회 이상 정기적으로 확인.감독
  - 접속기록의 6개월 이상 보존.관리
  - 접속기록을 별도의 저장장치에 보관/정기적 백업 수행
- 보안프로그램의 설치 및 운영

개인정보보호법에 대한 대응

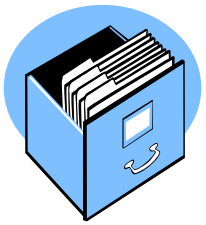


개인정보보호법에 대한 대응



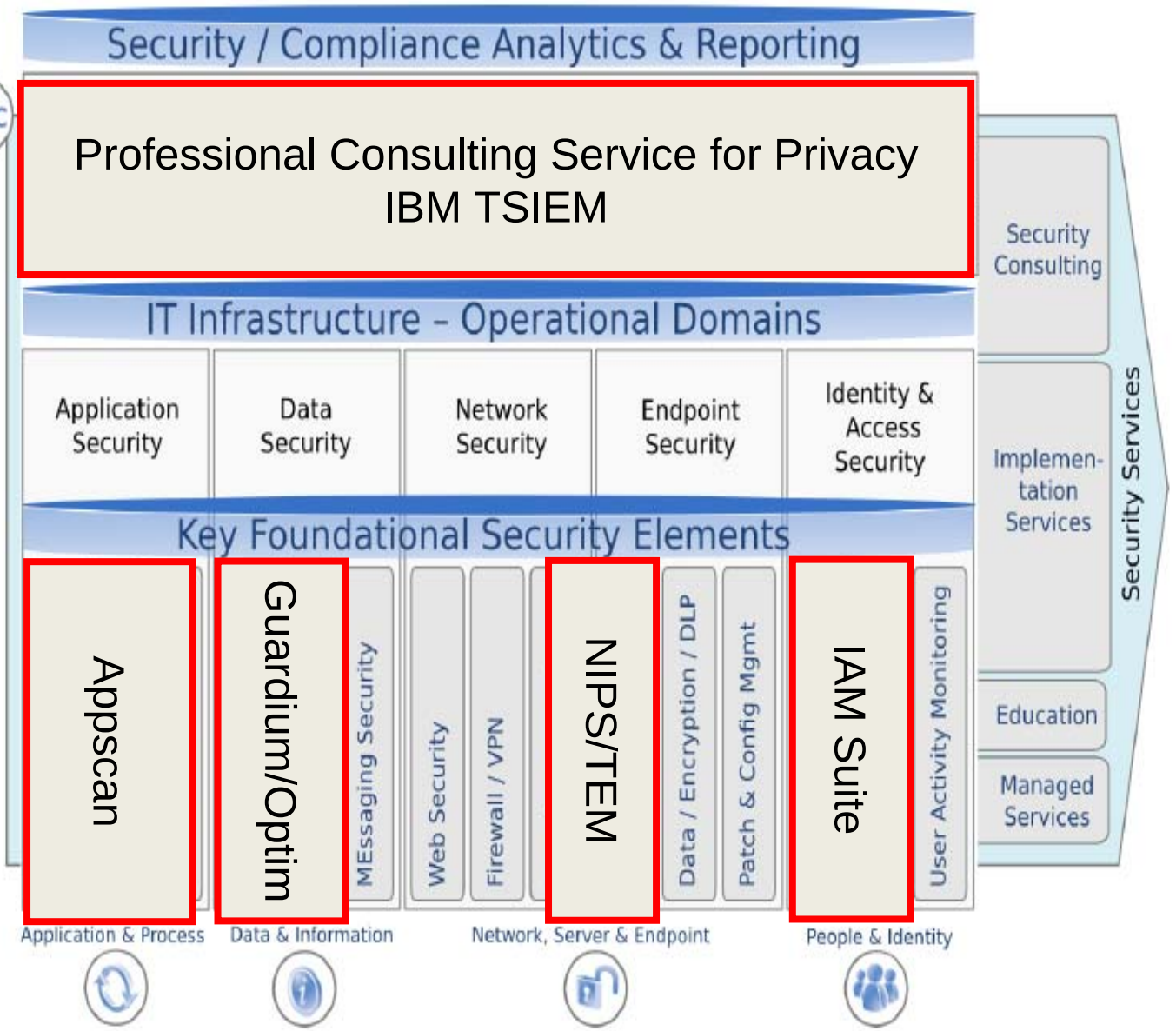




개인정보보호법에 대한 대응

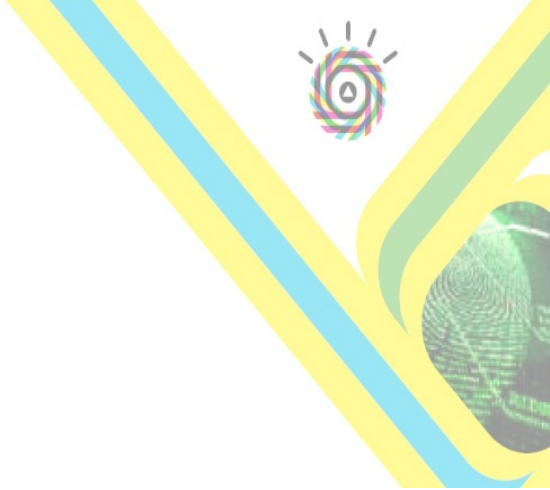
- 개인정보보호 조직 구성
- 개인정보 처리 부서 파악
- 개인정보의 처리 용도 정의 : 개인정보영향평가, 개인정보의 분류
- 개인정보 Lifecycle에 따른 보호 조치 정의 및 적용
  - 수집 : 수집 범위/목적 정의, 포괄적 동의 금지 등
  - 저장 : 문서, 단말, 서버, Application, Database에 대한 통제 등
  - 이용 : 접근통제, 접근로그 관리 등
  - 제공(전송) : 3자와의 협약, 내/외부 전송 통제 등
  - 파기 : 파기에 대한 방법
- 보호 조치 및 역할을 정의한 문서
- 확인(감사)

개인정보보호법에 대한 대응

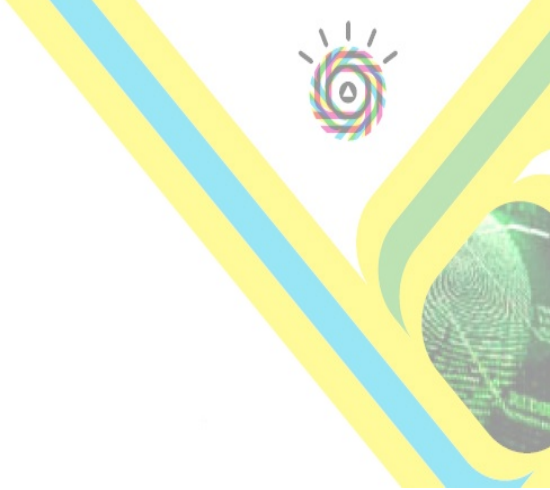


Agenda

- Introduction
- 개인정보보호법의 내용 및 고려사항
- 개인정보보호법에 대한 대응
- Closing

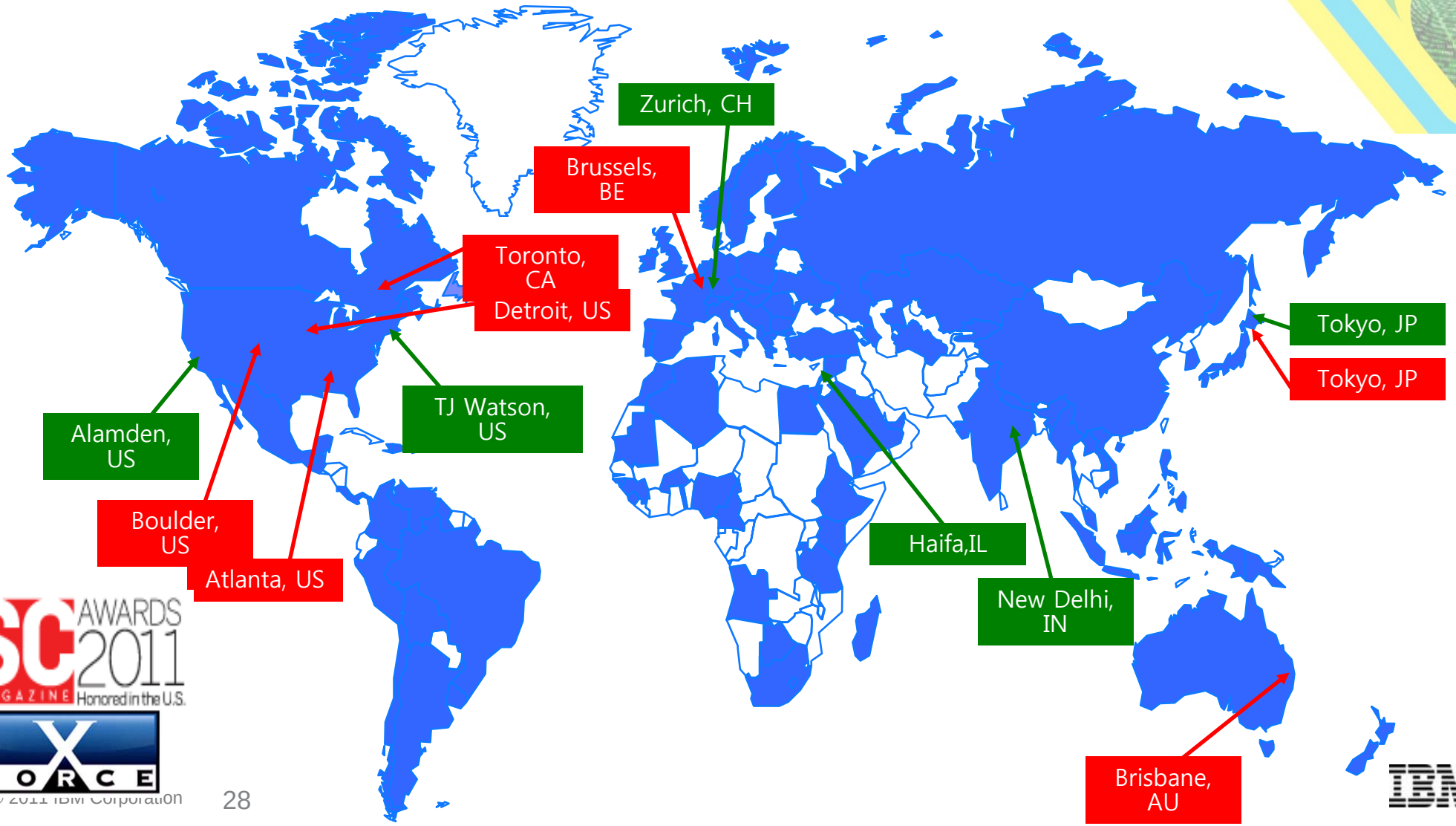


Summary



Why IBM?

전세계 7군데 보안 관제센터 + 6군데 보안연구 센터 + 133개국 보안관제 + 2200+ 보안 관제서비스 + 15,200+ 관리 장비 + 10억개 이상 보안 이벤트 모니터링



SC AWARDS 2011 MAGAZINE Honored in the U.S.

X FORCE

IBM

감사합니다!

www.ibmsecurity.co.kr

- 영업상담: 최효진 부장 (hjchoi@kr.ibm.com, 010-4995-8272)
- 기술상담: 나병준 차장 (bjna@kr.ibm.com, 010-4995-4843)