11장. 보안관리

박종혁

서울과학기술대학교 컴퓨터공학과

jhpark1@seoultech.ac.kr

개요

- 학습 목표
  - 보안 거버넌스와 보안 프레임워크의 개념을 이해하고 보안 정책의 절차를 파악한다
  - 보안 정책서에 포함해야 할 내용 및 효과적인 보안 정책을 운용하는 데 필요한 구성을 알아본다

목 차

1. 정보 보안 거버넌스

- **보안 거버넌스 (security governance)**
  - 조직의 보안을 달성하기 위한 구성원 간의 지배 구조

- **구현의 어려움**
  - 조직 구성의 어려움
    - 최고보안책임자(Chief Security Officer, CSO)를 CTO(Chief Technology Officer)나 CIO(Chief Information Officer) 밑에 두는 것이 효율적인지, 동등하게 두는 것이 효율적인지 결정하기가 어려움
    - 정보 보안 조직을 중앙 집중으로 체계화하는 것이 나을지, 각 IT 부서에 보안 담당자를 두고 연방 체제로 조직하는 것이 나을지 결정하기 어려움
  - 성과 측정의 어려움
    - 보안에는 상당한 비용이 들어가지만 사고가 일어나지 않는 한 성과를 측정하기 어려움
  - 조직의 무관심
    - 보안에 무관심한 경영진과 조직 구성원은 효율적인 보안 거버넌스를 구성하는 데 장애물임

- **구현 요건**
  - 전략적 연계
    - 비즈니스와 IT 기술의 목표, 정보 보안 전략이 서로 연계되도록 최상위 정보 보안 운영 위원회의 역할과 책임을 명시하고 정보 보안 보고 체계의 합리화를 이루어야 함
  - 위험 관리
    - 조직에 적합한 위험 관리 체계 수립, 지속적 관리하여 수용 가능한 수준으로 위험을 낮춰야 함
    - 확인된 위험은 적절한 자원을 할당하여 관리해야 함
  - 자원 관리
    - 정책과 절차 따른 정보 보안 아웃소싱 수행
    - 아웃소싱 정보 보안 서비스의 통제와 책임을 명시 및 승인하며 기업의 정보 보안 아키텍처와 전사적 아키텍처를 연계해야 함
  - 성과 관리
    - 모니터링, 보고 및 평가에 따른 성과 평가 체계를 운영하고 비즈니스 측면도 고려하여 성과 평가해야 함
  - 가치 전달
    - 구성원들에게 정보 보안의 중요성과 가치를 교육해야 함
    - 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영하고 자본의 통제 및 투자 프로세스를 정보 보안과 통합해야 함

- **점검 사항**
  - 보안 거버넌스가 잘 운영되고 있는 기업의 특징
    - 사업 전반의 이슈
      - 보안은 사업 전반을 관통하는 이슈로 조직 전반에 걸쳐 종적·횡적으로 관리해야 함
      - 보안 관리 프로그램(Enterprise Security Program, ESP)은 인력, 제품, 공장, 프로세스, 정책, 시스템, 기술, 네트워크, 정보를 포함하고 있어야 함
    - 경영진의 책임 의식
      - 경영진은 조직과 주주 및 공동체의 보안뿐만 아니라 경제적·국가적 보안 사항에 대한 책임 의식을 가져야 함
      - 이를 위해 적절한 재무 지원 및 관리, 정책과 감사를 수행해야 함
    - 사업의 필요조건
      - 보안은 사업의 필요조건으로, 소모되어 사라지는 비용이 아니라 회사의 가치를 높이기 위한 원가 요소로 이해해야 함
    - 위험 관리
      - 보안의 중요성은 노출된 위험의 크기에 좌우되므로 위험 관리 필요

- 역할과 책임
  - 경영진과 운영 조직의 R&R(Role & Responsibility)과 SoD(Segregation of Duties: 업무분장)가 명확해야 함
- 정책과 절차
  - 보안과 관련된 정책과 절차는 잘 정비되고 엄격하게 지켜져야 함
- 능력과 권한
  - 보안 조직에 속한 인원은 적합한 능력과 권한을 가져야 함
- 교육과 훈련
  - 모든 직원이 보안 인식을 갖추고 보안 교육과 훈련을 받아야 함
- 프로그램 개발 및 변경
  - 개발 및 변경과 같은 시스템과 소프트웨어의 생명주기에 따른 보안 통제가 이루어져야 함
- 계획, 수행 및 평가
  - 사업의 전략 및 계획을 수립할 때 보안을 고려해야 함
- 검토와 감사
  - 주기적인 검토와 감사로 보안 사항을 확인하고 개선해야 함

2. 보안 프레임워크

- **보안 프레임워크**
  - 보안 프레임워크는 조직 구성원 모두가 전문가가 아니더라도 조직의 보안 수준을 유지 및 향상하기 위한 체계

- **보안 프레임워크 모델**
  - ISMS
    - Information Security Management System: 정보보호 관리체계
    - 기업이 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적인 경영 시스템
  - PDCA
    - PDCA는 계획(Plan), 수행(Do), 점검(Check), 조치(Act)를 반복적으로 순환하여 수행하는 모델
    - PDCA 모델을 통해 ISMS를 발전시킬 수 있음

PDCA Model

- **ISMS와 PDCA 모델**
  - PDCA 각 단계에서 수행하는 업무
    ① 계획 (Plan): ISMS 수립 단계로 조직이 가진 위험 관리, 정보 보안 목적 달성 위해 전반적인 정책 수립
    - 프로세스를 위한 입력과 출력 규정
    - 프로세스별 범위 정의, 고객의 요구 사항 규정
    - 프로세스 책임자 규정
    - 프로세스 네트워크의 전반적인 흐름과 구성도 전개
    - 프로세스 간의 상호작용 규정
    - 의도한 결과나 그렇지 않은 결과의 특성 지정
    - 기준 측정
    - 모니터링 분석을 위한 방법 지정
    - 비용, 시간, 손실 등의 경제적 문제 고려
    - 자료 수집을 위한 방법 규정

② 수행 (Do) : ISMS 구현과 운영 단계로 수립된 정책을 현재 업무에 적용

- 각 프로세스를 위한 자원 분배
- 의사소통 경로 수집
- 대내외에 정보 제공
- 피드백 수용
- 자료 수집
- 기록 유지

③ 점검 (Check) : ISMS 모니터링, 검토 단계로 실제 정책이 얼마나 잘 적용 및 운영되는지 확인

- 프로세스의 측정과 이행이 정확한지 모니터링
- 수집된 정량적 · 정성적 정보 분석
- 분석 결과 평가

④ 조치 (Act) : ISMS 관리와 개선 단계로 제대로 운영되지 않는 경우에 원인을 분석하고 개선

- 시정 및 예방 조치 실행
- 시정 및 예방 조치의 유효성과 이행 여부 검증

• 정보보호관리체계 및 인증

구분	KISA ISMS (K-ISMS)	ISO 27001
인증주체	한국인터넷진흥원(KISA) : 국내표준 정보통신망이용촉진및정보보호등에관한법률에 근거	ISO/IEC : 국제표준 영국 BSI인증원의 BS7799규격에서 시작
인증기관	한국인터넷진흥원(KISA) 기업보안관리팀	BSI 인증원 DNV 인증원 SGS인증원
인증대상	제품을 생산하는 또는 서비스를 제공하는 기관의 조직 전체 또는 조직 단위 별, 지역별로 구분된 일부를 대상으로 함	
통제항목	정보보호 5단계 관리과정 요구사항 14개 필수항목, 문서화 요구사항 3개 필수항목, 정보보호대책 15개 분야 120개 세부항목 등 총 137개 항목	정보보호 관리과정 4개 도메인과 Annex 11개 도메인 133개 세부 통제항목으로 구성
사후심사	1년 주기 사후심사, 3년 주기 재심사	6개월 주기 사후심사, 3년 주기 재심사
인증절차	수립단계(인증 기반작업), 이행단계(최소3개월), 심사단계(문서심사, 본 심사) 3단계로 구분	

- **ISO 27001 (ISMS 국제인증)**
  - PDCA로 ISMS의 관리 과정을 확인하기 위한 ISO 27001의 보안 관리 항목

PDCA	항목
	1. Scope
	2. Normative references(참고 문헌)
	3. Terms and definitions(용어 및 정의)
계획 (Plan)	4. Context of the organization(조직의 상황) 4.1 Understanding of the organization and its context(조직과 상황의 이해) 4.2 Understanding the needs and expectations of interested parties(이해관계자의 요구 및 기대의 이해) 4.3 Determining the scope of the information security management system(정보 보호 경영 시스템의 범위 결정) 4.4 Information security management system(정보 보호 경영 시스템)
계획 (Plan)	5. Leadership(리더십) 5.1 Management commitment(경영진의 의지) 5.2 Policy(정책) 5.3 Organizational roles, responsibilities and authorities(조직의 역할 및 책임과 권한)
계획 (Plan)	6. Planning(기획) 6.1 Actions to address risks and opportunities(위험과 기회의 대처 활동: 정보 보호 위험 평가 및 위험 처리) 6.2 Information security objectives and planning to achieve them(정보 보안 목표 및 목표 달성 계획)
실행 (Do)	7. Support(지원) 7.1 Resources(자원) 7.2 Competence(적격성) 7.3 Awareness and training(인식 및 교육 훈련) 7.4 Communication(의사소통) 7.5 Documentation(문서화)
실행 (Do)	8. Operation(운영) 8.1 Operational planning and control(운영 계획 및 통제) 8.2 Information security risk assessment(정보 보호 위험 평가) 8.3 Information security risk treatment(정보 보호 위험 처리)
점검 (Check)	9. Performance evaluation(성과 평가) 9.1 Monitoring, measurement, analysis and evaluation(모니터링, 측정, 분석, 평가) 9.2 Internal audit(내부 감사) 9.3 Management review(경영진 검토)
조치 (Action)	10. Improvement(개선) 10.1 Nonconformity control and corrective actions(부적합 사항의 통제 및 시정 조치) 10.2 Continual Improvement(지속적인 개선)

- **ISO 27001의 보안 통제 분야**
  - ISO 27001이 추구하는 보안 프레임워크의 형태를 이해하는 것이 중요

분야	항목
A.5 보안 정책(Information security policies)	2
A.6 정보 보호 조직(Organization of information security)	7
A.7 인적 자원 보안(Human resource security)	6
A.8 자산 관리(Asset management)	10
A.9 접근 통제(Access control)	14
A.10 암호화(Cryptography)	2
A.11 물리적·환경적 보안(Physical & environmental security)	15
A.12 운영 보안(Operations security)	14
A.13 통신 보안(Communications security)	7
A.14 정보 시스템 개발 및 유지·보수(System acquisition, development & maintenance)	13
A.15 공급자 관계(Supplier relationships)	5
A.16 정보 보안 사고 관리(Information security incident management)	7
A.17 정보 보호 측면 업무 연속성 관리(Information security aspects of business continuity management)	4
A.18 컴플라이언스(Compliance)	8

ISO 27001의 보안 통제 분야

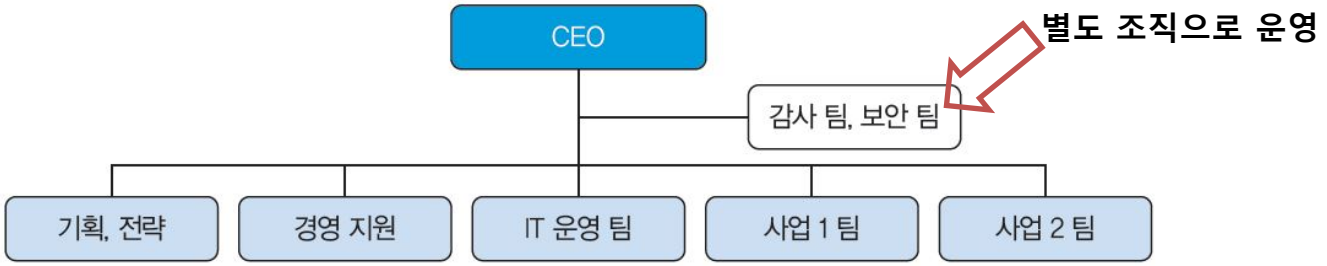
- **K-ISMS**
  - ISO 27001의 국제 표준을 포함하고 우리나라 상황에 맞는 보안 요건을 강화한 정보 보호 관리 체계
  - 기업이나 조직의 모든 보안 업무를 포괄하는 내용임

K-ISMS 인증

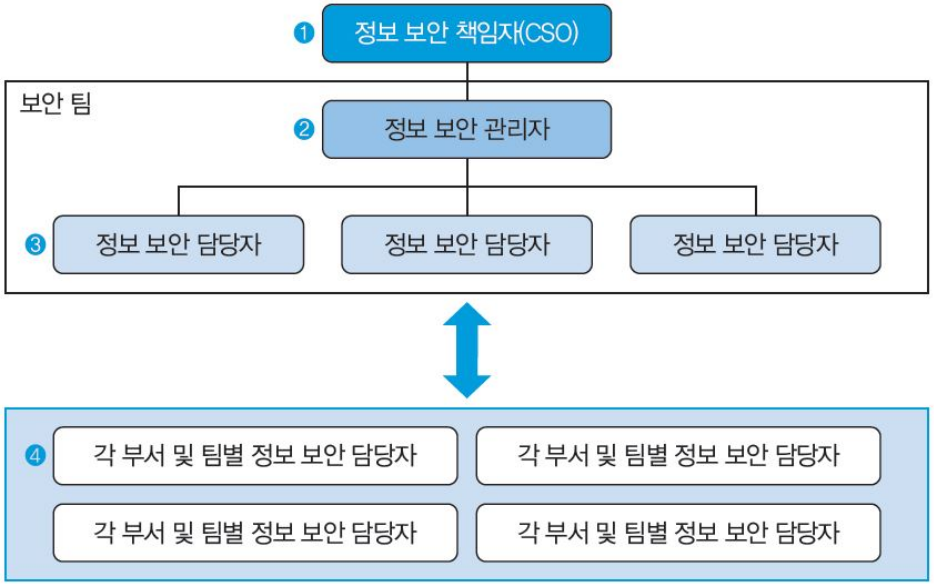
3. 보안 조직

- **보안조직**
  - 조직이 보안성 향상이라는 목표를 이루려면 보안 업무를 수행할 수 있는 자리를 마련하고 그에 맞는 역할과 책임을 주어야 함
  - 보안 조직에 권한과 책임이 적절히 부여되면 조직의 보안 수준을 높일 수 있음

- **보안 조직의 유형**
  - 보안 인력이 경영진 직속인 경우
    - 보안 팀을 CEO 또는 CSO 직속의 별도 조직으로 운영하는 것이 가장 바람직
    - 모든 부서의 보안 감사가 가능해야 하고 통제 정책과 운영을 보안에 적합하게 변경하도록 회사의 모든 팀과 커뮤니케이션 해야 하기 때문



- **보안 팀 내부의 인력 구성**



보안 팀의 구성

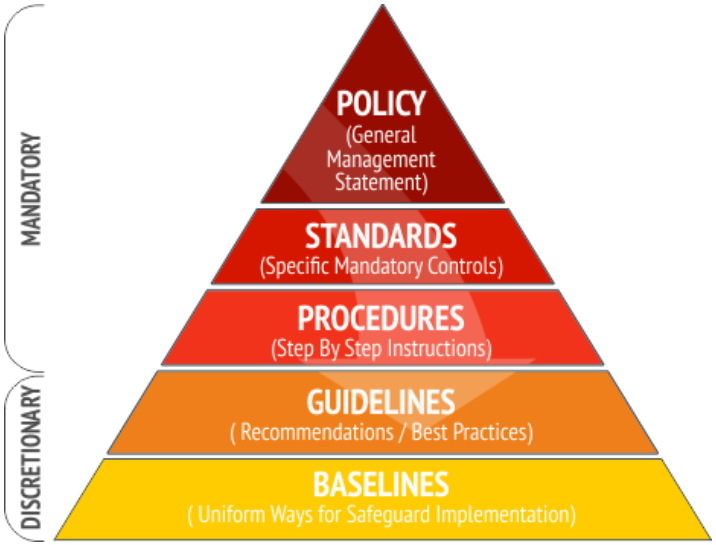
- 조직이 보안성 향상이라는 목표를 이루려면 보안 업무를 수행할 수 있는 자리를 마련하고 그에 맞는 역할과 책임을 주어야 함
- 보안 조직에 권한과 책임이 적절히 부여되면 조직의 보안 수준을 높일 수 있음

- **회사의 보안 조직을 구성할 때 고려 사항**
  - 기업의 크기
  - 시스템 환경(분산 또는 집중식 시스템)
  - 기업의 조직 및 관리 구조
  - 운영 사이트의 수와 위치
  - 사이트 간의 상호 연결 형태
  - IT 예산

4. 보안 정책과 절차

- **보안 정책의 특성**
  - 규칙으로서 지켜져야 할 정책(regulatory)
  - 하려는 일에 부합하는 정책이 없을 때 참고하거나 지키도록 권유하는 정책(advisory)
  - 어떠한 정보나 사실을 알리는데 목적이 있는 정책(informative)

- **영미권의 보안 정책**
  - Security Policy
    - 조직의 상위 관리자가 만드는 것으로 보안 정책 중 가장 상위의 문서
    - 보안 활동의 일반적인 사항 기술
      - 보호하고자 하는 자산
      - 정보의 소유자 및 그의 역할과 책임
      - 관리되는 정보의 분류와 기준
      - 관리에 필요한 기본적인 통제 내용
    - 조직의 보안 정책이 어떤 원칙과 목적을 가지고 있는지 밝히는 것으로 내용이 장황하지 않고 쉽게 파악할 수 있어야 함
    - 새로운 보안 문서를 작성할 때 기초로 삼으며, 분량은 5쪽 정도이고 10쪽을 넘지 않음



- Standards
  - 소프트웨어나 하드웨어 사용처럼 일반 운영에서 지켜야 할 보안 사항 기록 문서
  - 일반적인 절차 표준을 담고 있음

- Procedures
  - 가장 하위 문서로 각 절차의 세부 내용을 매뉴얼 수준으로 담고 있는 것

- Guidelines
  - 하고자 하는 일에 부합하는 Standards가 없을 때 참고하는 문서
  - 어떤 상황에 대한 충고, 방향 등을 제시하여 어떤 행동을 할지 결정하는 데 도움을 줌

- Baselines
  - 조직에서 지켜야 할 가장 기본적인 보안 수준을 기록하는 문서

- **우리나라의 보안 정책**
  - 정보 보안 정책서
    - 보안 정책상 가장 상위 문서로 영미권의 Security Policy와 같음
    - 회사에서 보호할 정보 자산을 정의하고 정보 보안을 실현하기 위한 기본 목표와 방향성 설정
  - 정보 보안 지침서
    - 각 절차서의 기준이 되는 문서 정보 보안 조직의 구성과 운영에 관한 내용과 각 지침 절차의 기본 방향 등을 기술
  - 정보 자산 분류 절차서
    - 보호할 정보 자산을 명확하게 구별하고 적절히 분류한 내용 기술
      - 정보 자산 관리 체계: 자산의 식별, 분류, 등록, 자산의 중요도 평가 기준
      - 자산 운용: 자산 운용 방법, 자산 분류 및 중요도 평가 주기, 자산의 변경 및 폐기 절차

- 전산실 운영 절차서
  - 전산실의 출입을 통제하고 적절한 환경을 유지하기 위한 운영 절차서
    - 출입 관리, 방화 관리, 전산실 근무자 인수인계, 보고 및 조치 체계, 반·출입 관리

- 시스템 보안 절차서
  - 서버와 기타 운영 시스템의 보안, 운영 및 관리 방법에 대한 일괄적인 사항 기술
    - 시스템 운용: 시스템의 설치, 유지·보수, 장애 관리, 백업 및 매체 관리, 철수 및 폐기
    - 시스템 보안 사항 적용: 접근 제어, 패스워드 생성 및 관리, 백신 설치, 패치
    - 시스템 모니터링: 시스템 성능 모니터링, 로그 관리

- 네트워크 정보 보안 절차서
  - 네트워크 장비의 보안은 물론 운영 및 관리 방법에 대한 일괄적인 사항 기술
    - 네트워크 장비 운용: 네트워크 장비의 설치, 유지·보수, 장애 관리, 백업 및 매체 관리, 철수 및 폐기
    - 네트워크 장비 보안 사항 적용: 접근 통제, 패스워드 생성 및 관리, ISO 업그레이드
    - 네트워크 모니터링: 네트워크 모니터링, 로그 관리

- 보안 시스템 정보 보안 절차서
  - 방화벽, 침입 탐지 시스템, VPN 등과 같은 보안 시스템의 운영 및 관리 방법에 대한 사항 기술
    - 정보 보안 시스템 운용: 정보 보안 시스템 도입, 백업 및 매체 관리, 철수 및 폐기
    - 정보 보안 시스템 보안 사항 적용: 네트워크 접근 제어, 사용자 관리
    - 정보 보안 시스템 모니터링: 보안 시스템 모니터링, 로그 관리

- 개발 보안 절차서
  - 응용 프로그램의 개발 및 유지, 보수, 운영에 필요한 보안 관련 활동 기술
    - 응용 프로그램의 환경 구성: 개발자가 임의로 운영 환경production에 접근하여 프로그램을 변경할 수 없도록 개발 환경과 서비스를 제공하는 운영 환경을 분리
    - 응용 프로그램 개발: 보안 요구 사항 분석, 보안 기능 설계, 프로그래밍 시 주의 사항, 응용 프로그램 테스트
    - 응용 프로그램 운영: 소스 라이브러리 변경 이력과 접근 권한의 관리 및 통제, 백업

- 일반 사용자 정보 보안 절차서
  - PC 등으로 일반적인 업무를 보는 내부 구성원의 보안 관련 활동 기술
    - 내부 또는 외부로 전송되는 메일 관련 보안 사항
    - 개인 패스워드 관리
    - 책상 위 정리, 화면 보호기 설정
    - 일반적인 PC 보안 관리 사항, 웜과 바이러스 공격에 대한 대응

- 침해 사고 및 장애 대응 절차서
  - 침해 사고나 장애가 발생했을 때 대응 절차 기술
    - 침해 사고 대응 절차
    - 장애 대응 절차
    - 스팸 메일 처리
    - 웜, 바이러스 공격 대응
    - 시스템 복구 및 분석 절차

- 정보 보안 교육 훈련 절차서
  - 구성원의 정보 보안 인식을 향상하고 보안 관련 지식을 습득시키기 위한 내용 기술
    - 교육 시기와 교육 내용
    - 정보 보안 관련 교육 기관 선정 방침

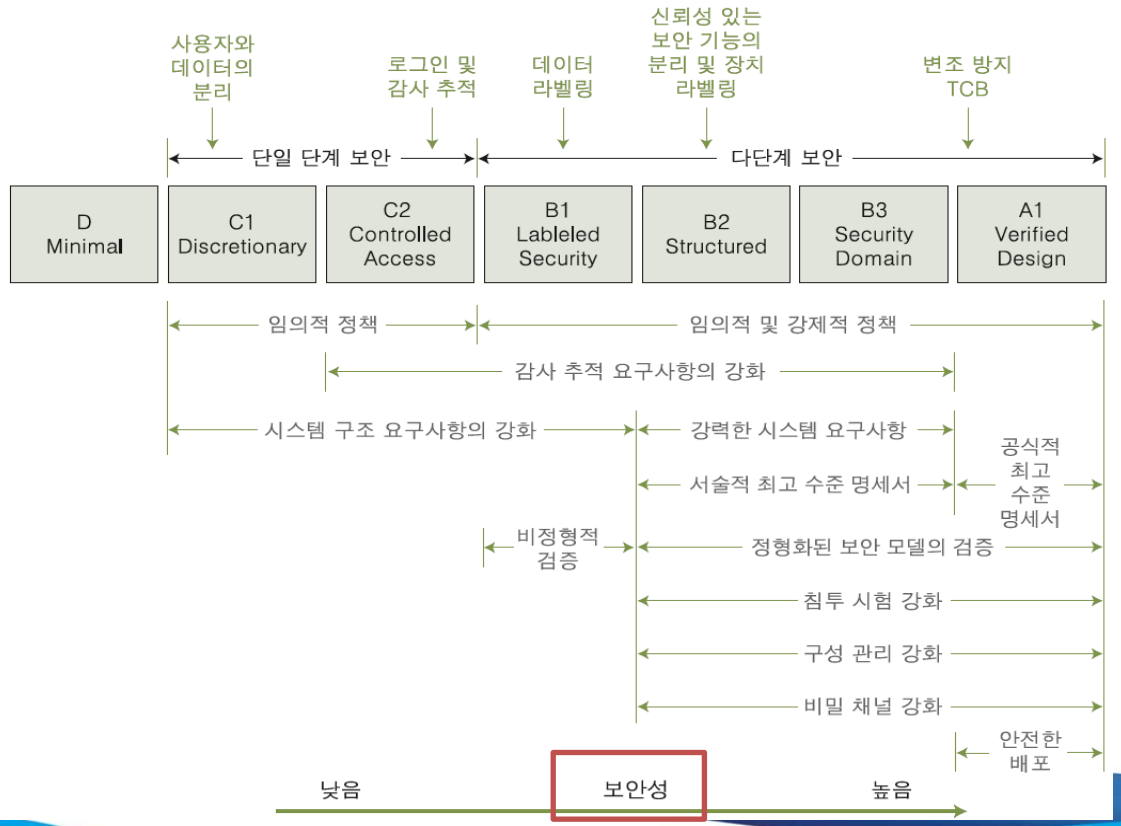
- 제삼자 및 아웃소싱 보안 절차서
  - 외주 업체가 지켜야 할 보안 사항과 관련 내용 기술
    - 외주 계약서에 포함해야 할 보안 사항 및 보안 책임 여부
    - 외주 인력의 통제 범위

- 보안 정책서 서식
  - 구체적인 내용
  - 정책서에 대한 개정 이력
  - 목적
  - 적용 범위
  - 역할 및 책임
  - 주요 용어에 대한 설명 추가

5. 보안 인증

- **보안 인증 개념**
  - 보안 인증은 소프트웨어나 시스템에 대한 품질 표시 마크

- **TCSEC**
  - TCSEC(Trusted Computer System Evaluation Criteria)는 오랜 역사를 가진 인증으로 지금까지도 보안 솔루션을 개발할 때 기준이 됨
  - TCSEC의 등급별 특성



5. 보안 인증

- TCSEC에서 분류하는 보안 등급
  - D: Minimal Protection
    - 보안 설정이 이루어지지 않은 단계
  - C1: Discretionary Security Protection
    - 일반적인 로그인 과정이 존재하는 시스템
    - 사용자 간 침범이 차단되어 있고 모든 사용자가 자신이 생성한 파일에 권한을 설정 가능
    - 특정 파일에 대해서만 접근 가능
    - 초기의 유닉스 시스템 해당
  - C2: Controlled Access Protection
    - 각 계정별 로그인이 가능
    - 그룹 아이디로 통제가 가능한 시스템 보안 감사가 가능
    - 특정 사용자의 접근 거부 가능
    - 윈도우 운영체제와 현재 사용되는 대부분의 유닉스 시스템 해당

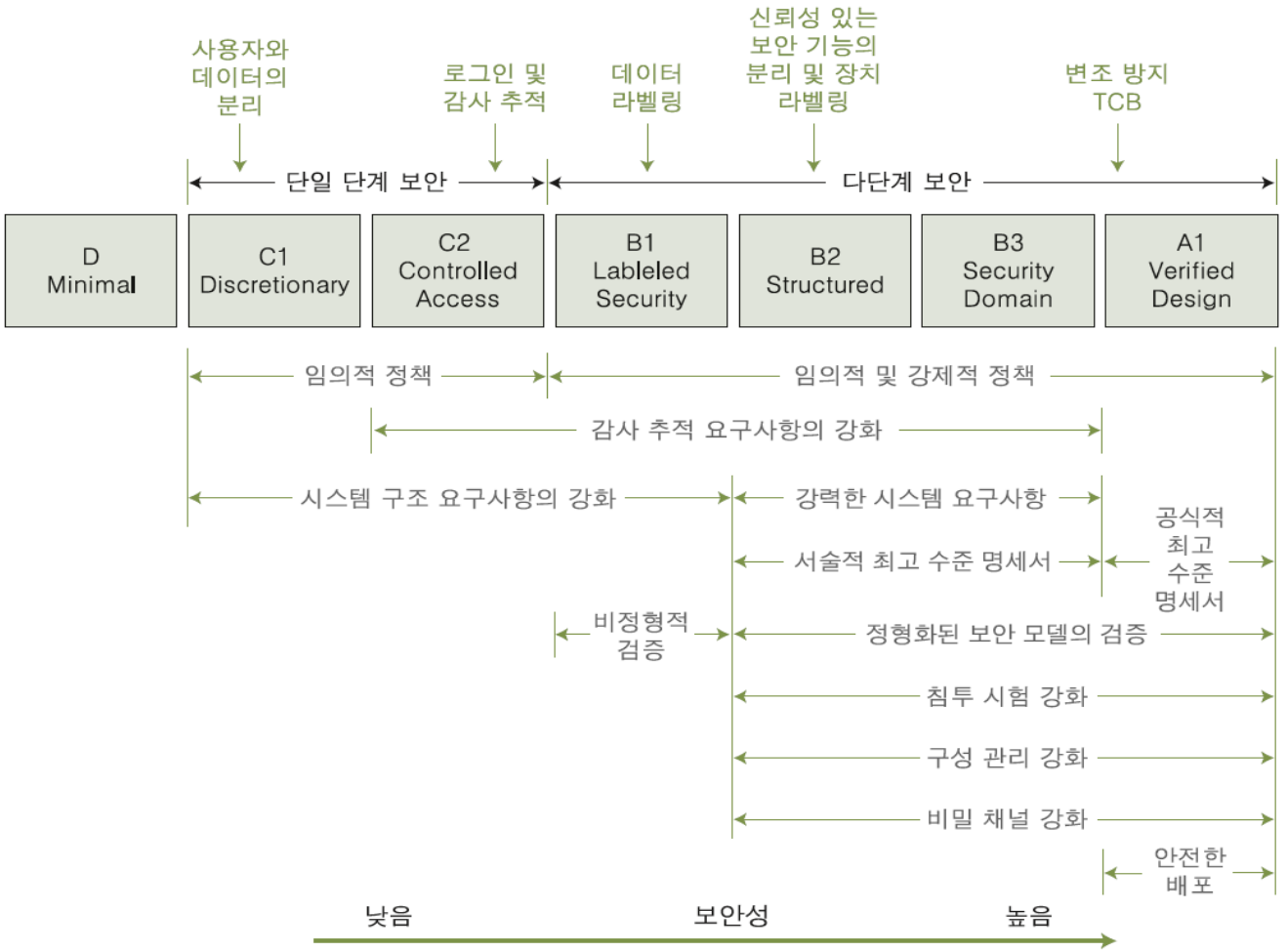
- B1: Labeled Security
  - 시스템 내의 보안 정책을 적용할 수 있고 각 데이터의 보안 레벨 설정 가능 시스템 파일이나 시스템의 권한 설정 가능

- B2: Structured Protection
  - 시스템에 정형화된 보안 정책이 존재
  - B1 등급의 기능을 모두 포함
  - 일부 유닉스 시스템은 B2 인증에 성공했고, 방화벽이나 침입 탐지 시스템과 같은 보안 솔루션은 주로 B2 인증을 목표로 개발

- B3: Security Domains
  - 운영체제에서 보안에 불필요한 부분을 모두 제거
  - 모듈에 따른 분석 및 테스트가 가능
  - 시스템 파일과 디렉터리 접근 방식을 지정하고 위험 동작을 하는 사용자 활동에는 백업까지 자동으로 이루어짐
  - 현재 이 등급을 받은 시스템은 극히 일부

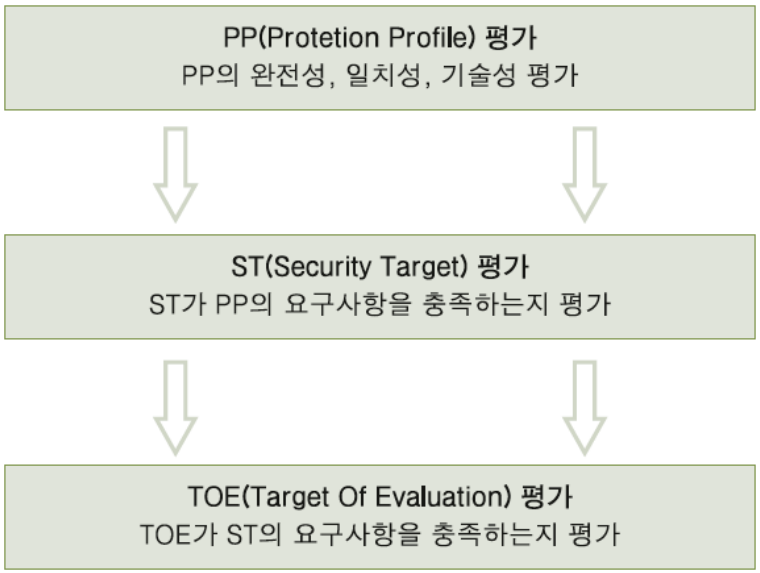
- A1: Verified Design
  - 수학적으로 완벽한 시스템
  - 현재 이 등급을 받은 시스템은 없으며 사실상 이상적인 시스템임

- TCSEC의 등급별 특성



- **ITSEC**
  - ITSEC(Information Technology Security Evaluation Criteria)는 TCSEC와 별개로 유럽에서 발전한 보안 표준
  - 기밀성만을 강조한 TCSEC와 달리 무결성과 가용성을 포괄하는 표준안 제시

- **CC**
  - 최근에 TCSEC와 ITSEC는 CC(Common Criteria)라는 기준으로 통합되고 있음
  - 1996년에 초안이 나와 1999년에 국제 표준으로 승인됨
  - CC 인증을 위한 평가 과정
    - ✓ PP(Protection Profile): 사용자 또는 개발자의 요구 사항 정의
    - ✓ ST(Security Target): 제품 평가를 위한 상세 기능을 개발자가 정의하여 작성
      - PP와 달리 기술적인 구현 가능성을 고려함
    - ✓ TOE(Target Of Evaluation): 획득하고자 하는 보안 수준



- 각 인증별 보안 등급

CC		TCSEC(미국)		ITSEC(유럽)		한국
EAL0	부적절한 보증	D	최소한의 보호	E0	부적절한 보증	K0
EAL1	기능 시험	C1	임의적 보호	E1	비정형적 기본 설계	K2
EAL2	구조 시험	C2	통제된 접근 보호	E2	비정형적 기본 설계	K3
EAL3	방법론적 시험과 점검	B1	규정된 보호	E3	소스코드와 하드웨어 도면 제공	K4
EAL4	방법론적 설계, 시험, 검토	B2	구조적 보호	E4	준정형적 기능 명세서, 기본 설계, 상세 설계	K5
EAL5	준정형적 설계 및 시험	B3	보안 영역	E5	보안 요소 상호 관계	K6
EAL6	준정형적 검증된 설계 및 시험	A1	검증된 설계	E6	정형적 기능 명세서, 상세 설계	K7
EAL7	정형적 검증					

6. 개인 정보 보호

- **개인 정보의 정의**

개인정보 보호법 제2조 1항
'개인 정보'란 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.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 6항
'개인 정보'란 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

- 개인 정보의 예
  - 신분 관계: 성명, 주민등록번호, 주소, 본적, 가족관계, 본관 등
  - 개인 성향: 사상, 신조, 종교, 가치관, 정치적 성향 등
  - 심신 상태: 건강 상태, 신체적 특징(신장, 체중 등), 병력, 장애 정도 등
  - 사회 경력: 학력, 직업, 자격, 전과 여부 등
  - 경제 관계: 소득 규모, 재산 보유 현황, 자금 거래 내역, 신용 정보, 채권·채무 관계 등
  - 기타 새로운 유형: 생체 정보(지문, 홍채, DNA 등), 위치 정보 등

- # OECD 개인 정보 보안 8원칙

① 수집 제한의 법칙(Collection Limitation Principle)
  - 개인 정보는 적법하고 공정한 방법을 통해 수집되어야 함

② 정보 정확성의 원칙(Data Quality Principle)
  - 이용 목적상 필요한 범위 내에서 개인 정보의 정확성, 완전성, 최신성이 확보되어야 함
  -

③ 목적 명시의 원칙(Purpose Specification Principle)
  - 수집 과정에서 개인 정보 수집 목적을 명시하고 그에 적합하게 이용되어야 함

④ 이용 제한의 원칙(Use Limitation Principle)
  - 정보 주체의 동의가 있거나 법 규정이 있는 경우를 제외하고 목적 외에 이용하거나 공개할 수 없음

- **OECD 개인 정보 보안 8원칙**

⑤ 안전성 확보의 원칙(Security Safeguard Principle)
  - 개인 정보의 침해, 누설, 도용 등을 방지하기 위한 물리적·조직적·기술적 안전 조치 확보해야 함

⑥ 공개의 원칙(Openness Principle)
  - 개인 정보의 처리 및 보호를 위한 정책과 관리자의 정보가 공개되어야 함

⑦ 개인 참가의 원칙(Individual Participation Principle)
  - 정보 주체의 개인 정보 열람·정정·삭제 청구권이 보장되어야 함

⑧ 책임의 원칙(Accountability Principle)
  - 개인 정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 함

- **PIMS**
  - PIMS(Personal Information Management System)는 KISA에서 주관
  - 기관 및 기업이 개인 정보 보호 관리 체계를 갖추고 체계적이고 지속적으로 보안 업무를 수행하는지 심사하여 기준을 만족하면 인증을 부여하는 제도
  - PIMS의 관리 체계 인증 심사 기준

영역	통제 사항	항목
1. 관리 체계 수립	개인 정보 관련 정책의 수립 절차 및 조직, 경영진의 참여	7
2. 실행 및 운영	기관 및 기업 내의 개인 정보 식별 및 위험 평가	5
3. 검토 및 모니터링	법적 준수 검토 및 내부 감사	2
4. 교정 및 개선	개인 정보 보호 개선 활동 및 내부 교육	2
5. 개인 정보 생명 주기 관리	개인 정보의 수집, 이용 및 제공, 보유, 파기 시 준수 사항	16
6. 정보 주체 권리 보장	개인 정보의 열람, 정정, 삭제, 정지 등과 관련한 준수 사항	4
7. 관리적 보호 조치	교육 훈련, 위탁, 침해 사고, 개인 정보 취급자 관리	10
8. 기술적 보호 조치	권한 및 접속 기록 관리, IT 인프라 보안, 암호화 관련 사항	32
9. 물리적 보호 조치	CCTV, 출입 통제, 매체 관리	8

7. ISMS-P 소개

ISMS-P 인증의 개요

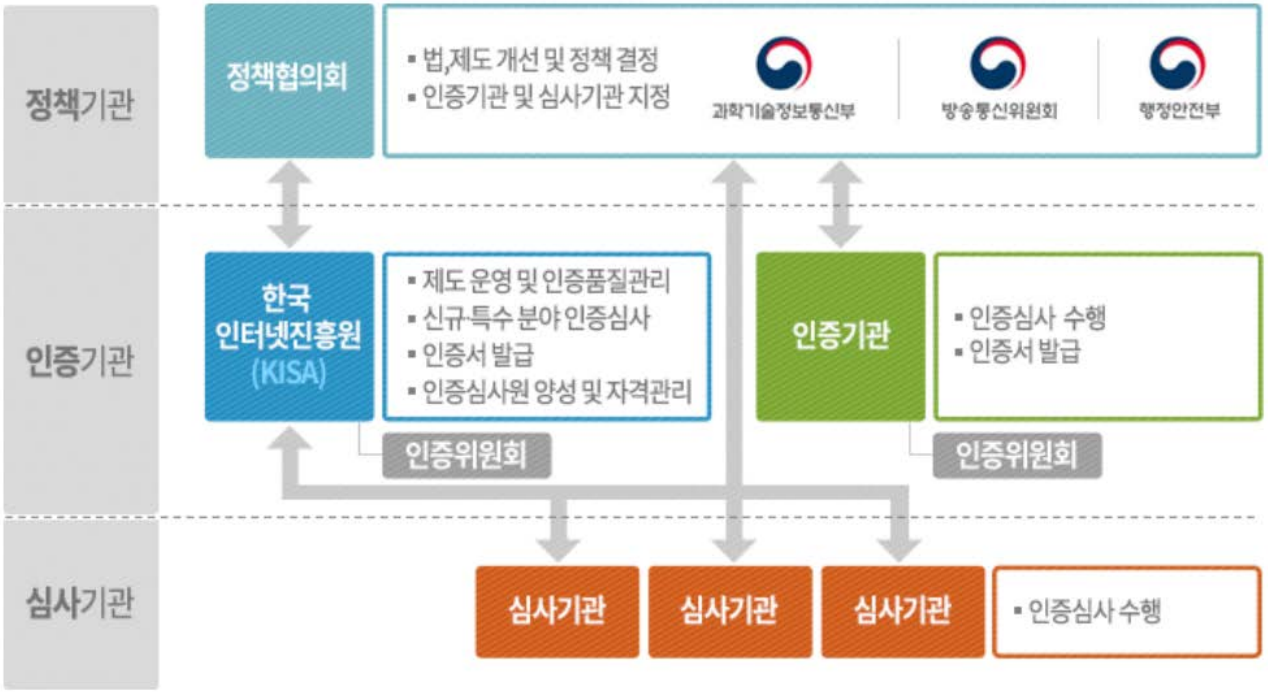
정보보호 및 개인정보보호 관리체계 인증

정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

정보보호 관리체계 인증

정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

- 인증체계



- 정책기관(협의회) : 과학기술정보통신부, 행정안전부, 방송통신위원회
- 인증기관 : 한국인터넷진흥원

- 인증기준


1. 1 관리체계 기반 마련
1.2 위험관리
1.4 관리체계 점검 및 개선
1.3 관리체계 운영
1. 관리체계 수립 및 운영 (16개)
2. 보호대책 요구사항(64개)
2.1 정책, 조직, 자산관리
2.2 인적보안
2.3 외부자 보안
2.4 물리 보안
2.5 인증 및 권한관리
2.6 접근통제
2.7 암호화 적용
2.8 정보시스템 도입 및 개발보안
2.9 시스템 및 서비스 운영관리
2.10 시스템 및 서비스 보안관리
2.11 사고 예방 및 대응
2.12 재해복구
3. 개인정보 처리단계별 요구사항(22개)
3.1 개인정보 수집 시 보호 조치
3.2 개인정보 보유 및 이용 시 보호조치
3.3 개인정보 제공 시 보호조치
3.4 개인정보 파기 시 보호조치
3.5 정보주체 권리보호

구분		통합인증	분야(인증기준 개수)	
ISMS-P	ISMS	1.관리체계 수립 및 운영(16)	1.1 관리체계 기반 마련(6) 1.3 관리체계 운영(3)	1.2 위험관리(4) 1.4 관리체계 점검 및 개선(3)
		2.보호대책 요구사항(64)	2.1 정책, 조직, 자산 관리(3) 2.3 외부자 보안(4) 2.5 인증 및 권한 관리(6) 2.7 암호화 적용(2) 2.9 시스템 및 서비스 운영관리(7) 2.11 사고 예방 및 대응(5)	2.2 인적보안(6) 2.4 물리보안(7) 2.6 접근통제(7) 2.8 정보시스템 도입 및 개발 보안(6) 2.10 시스템 및 서비스 보안관리(9) 2.12 재해복구(2)
	-	3.개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7) 3.3 개인정보 제공 시 보호조치(3) 3.5 정보주체 권리보호(3)	3.2 개인정보 보유 및 이용 시 보호조치(5) 3.4 개인정보 파기 시 보호조치(4)

참고문헌

- 양대일, 정보보안개론(개정3판), 한빛아카데미, 2018
- Calder, Alan, and Steve Watkins IT governance: A manager's guide to data security and ISO 27001/ISO 27002 Kogan Page Ltd , 2008
- K-ISMS 인증, 한국인터넷진흥원, 2019
- 손우용, and 송정길 "통합보안 관리시스템의 침입탐지 및 대응을 위한 보안 정책 모델 " 한국컴퓨터정보학회논문지 9 2 (2004): 81-87
- Veiga, A Da, and Jan HP Eloff "An information security governance framework " Information systems management 24 4 (2007): 361-372
- ISMS-P, KISA (2019) https://isms.kisa.or.kr/main/ispims/intro