보안 진단 및 보안 정책, 계획 수립

한국기술교육대학교
온라인평생교육원

학습내용

- 보안 개요
- 보안 정책 수립
- 보안 계획 수립

학습목표

- 보안에 대해 이해하고, 접근 방법을 숙지하여 활용할 수 있다.
- 보안 목표와 원칙, 전략을 이해하여, 보안 정책을 수립할 수 있다.
- 자산 분석에 따라 보안 기술과 표준, 솔루션을 적용하기 위한 보안 계획을 수립할 수 있다.

보안 개요

1 보안에 대한 개념

1 보안

1 보안에 대한 정의

보안이란? 위험, 손실 및 범죄가 발생하지 않도록 방지하는 상태

보안은 피해 발생 원인이 '인간의 행위'라는 점에서 '안전'이라는 개념과 구분

안전은 위험이 없어서 피해를 입을 수 없는 것을 말함

- 국어사전적 의미 : 안전을 유지함
- 사회의 안녕과 질서를 유지함
- 비밀 등이 외부에 누설되지 않게 보호

현재의 상태를 유지

손실·파손 등으로부터 보호

비밀의 보호

보안 개요

1 보안에 대한 개념

1 보안

2 보안에 대한 사고 사례

도난

현재 상태 손상

해킹

비밀 유출

자연재해

손실·파손으로부터 훼손

2 보안에 대한 특성

1 보안의 특성

대다수의 경우, '보안'은 '긍정적인 측면'보다는
'부정적인 측면'이 더 부각됨

1 보안에 대한 개념

2 보안에 대한 특성

1 보안의 특성

자체적인 준비

- 보안에 대한 계획, 구축, 운영은 조직 자체적으로 시행
- 부분적으로 '법'에 의한 강제 구축 요구
- 특정 기업·기관의 경우, 상급 기관으로부터 보안 체계에 대한 감사 실행

비용 지출

- 구축, 운영·유지보수를 위한 시간, 인력, 비용 등이 발생
- 대부분 비용은 자체 부담, '비생산적인 지출'로 평가
- 보안 체계 구현 시, 관리·유지보수 인력, 일정 규모 물리적인 공간 소모

외부 지원, 확장의 어려움

- '보안' Domain 접근 난이도
- 구축된 보안 체계는 확장, 변경, 성능 개선 등이 매우 어려움
- 대부분의 경우, 현재 상태의 상당한 변화를 야기(사용자의 거부감 발생)

보안 개요

1 보안에 대한 개념

2 보안에 대한 특성

2 보안을 적용하는 이유

기회비용 확보

- 사고 발생 시 소모되는 비용이, 보안 비용보다 과다

사고발생시지출비용 > 보안비용

사회적 손실

- 사고 당사자뿐만 아니라, 지역·국가 전체적인 손실 발생 가능

카드 고객의 신상정보 도난

2 보안에 대한 접근 방법

1 보안에 대한 접근

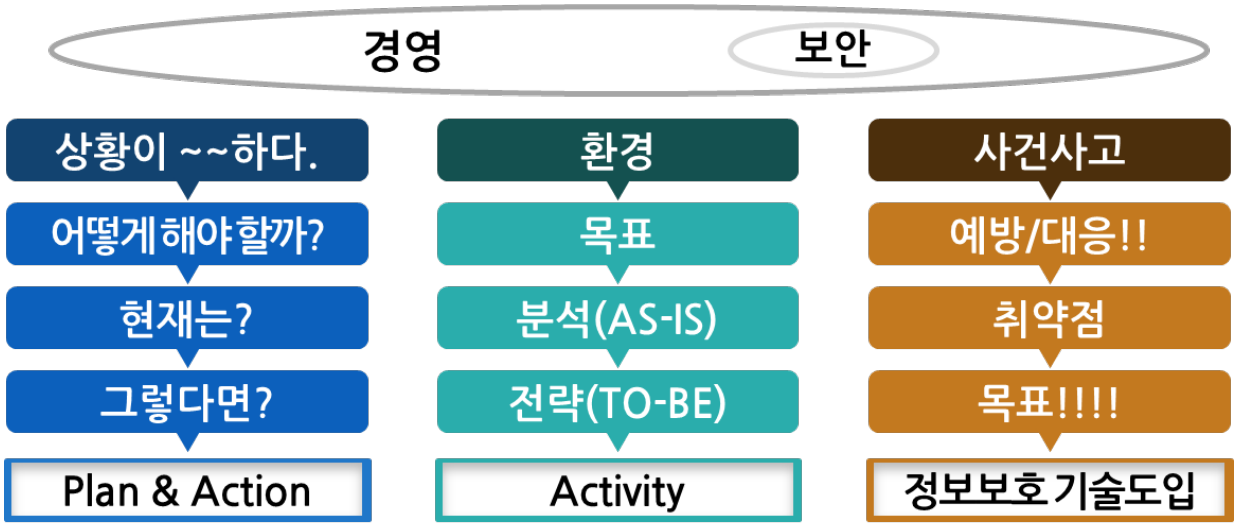
1 보안 접근 Mind-map

- 보안은 '창과 방패'의 '방패' 역할
- '창'의 공격을 방어하기 위한 '도구·기법·기술'
- 내부의 안녕을 유지하고, 외부의 침해·재해로부터 자산 보호
- '내부'와 '외부'를 명확히 인지하는 것에서부터 시작

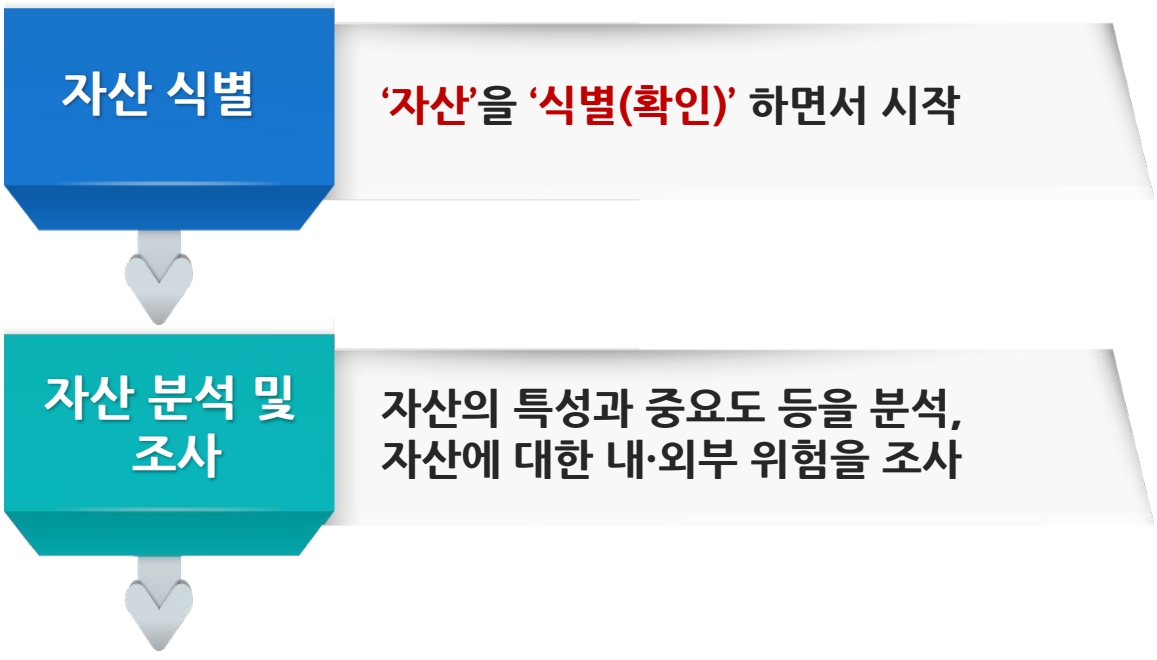
2 보안에 대한 접근 방법

1 보안에 대한 접근

1 보안 접근 Mind-map



2 보안의 적용



2 보안에 대한 접근 방법

1 보안에 대한 접근

2 보안의 적용

보안 구현을 위한 방향 도출
자산의 '가치'를 유지하기 위하여 '보안' 구현을 위한 환경적인 요소(전략)를 고려한 방향 도출

보안 체계 수립
방향에 따른 보안 체계(정책, 계획) 수립

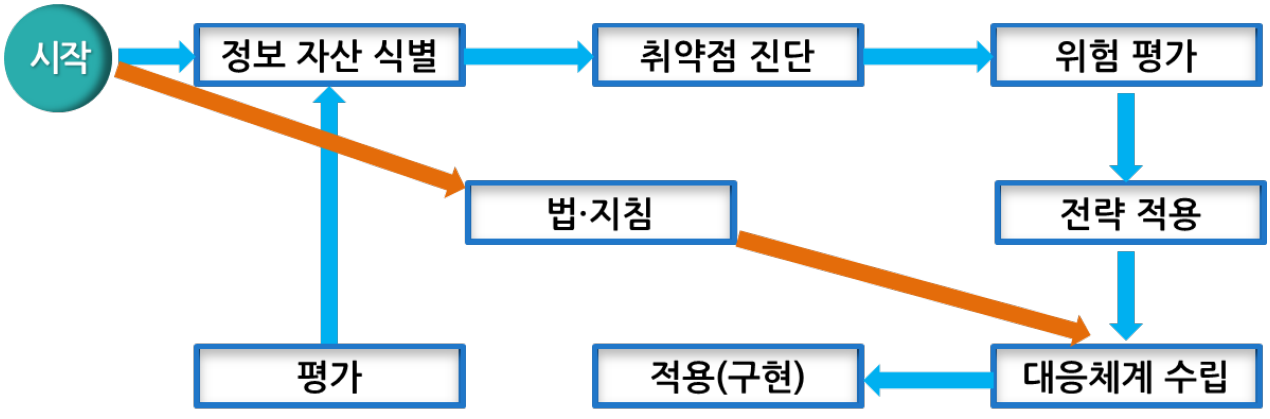
계획에 따른 운영
계획에 따른 보안 구축·운영,
운영 시 주기적인 평가&개선

'보안 체계'에 반영
'법·규정·지침'에서 요구하는 사항들을
'보안 체계'에 반영

2 보안에 대한 접근 방법

1 보안에 대한 접근

2 보안의 적용



보안 접근 개념도

3 보안 아키텍처

1 보안 아키텍처

1 보안 아키텍처의 개념

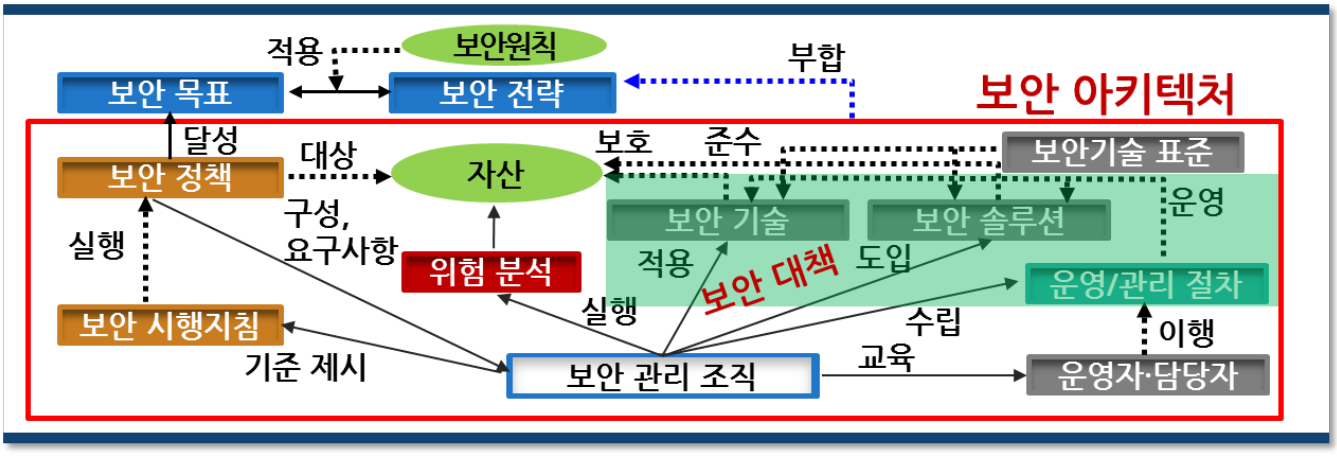
'보안' 전반에 대한 '설계'

조직의 '목표'에 따른 '자산 식별'부터 '구축·운영' 등의 전체 보안 Life-cycle에 대한 일련의 '계획과 실행'

3 보안 아키텍처

1 보안 아키텍처

1 보안 아키텍처의 개념



보안 아키텍처

2 보안 아키텍처 구성

B/B	내용	사례
보안 목표	▪ 전사 경영 목표에 종속적 ▪ 경영 목표를 만족할 수 있는 Sub 목표 ▪ 3~5개 정도	Ex) 택배사 ▪ 고객 신뢰도 향상을 위한 개인 정보 유출 방지 ▪ 제품 손망실 최소화로 고객 만족도 향상
보안 원칙	▪ 보안목표를 달성하기 위한 기본원칙 ▪ 어떠한 경우라도, 물러설 수 없는 특성	▪ 법령 준수 필수

보안 아키텍처 구성요소

3 보안 아키텍처

1 보안 아키텍처

2 보안 아키텍처 구성

B/B	내용	사례
보안 전략	▪ 보안 목표 달성을 위한 '특성' ▪ 자원·한계를 고려, 타 기관과 차별화	▪ 법적 요구사항 만족 ▪ 비용 최소화
보안 정책	▪ 보안 목표에 대한 방침 ▪ 보안 목표 달성 대상 범위 기술	▪ 개인 정보는 독립망에 존재하는 시스템에 저장 ▪ 배송 상품 취급 인력의 개인 물품은 최소화
보안 시행 지침	▪ 보안 정책을 이행하기 위한 기준 ▪ 책임과 역할, 보안 구현을 위한 기술 등을 포함	▪ 신입사원은, 입사 직후 총무팀을 방문하여 지문 등록 (담당자 홍길동)
보안 관리 조직	▪ 보안에 대한 기준·절차 등을 수립 및 감독하기 위한 전문 조직 ▪ 시스템을 관리 및 유지보수 할 조직과 구분	▪ 출입자 관리 시스템은 A사와 용역 계약

보안 아키텍처 구성요소

3 보안 아키텍처

1 보안 아키텍처

2 보안 아키텍처 구성

B/B	내용	사례
자산	▪ 조직에 보호·보안을 요구하는 자원 ▪ 조직·기업의 가치를 증명하는 실체	▪ 고객 정보 ▪ 배송 설비, 배송 담당 직원
보안 관리 조직	▪ 자산에 대한 내·외부에 존재하는 위협 발생 과정, 원인 조사, 분석 ▪ 위협의 발생 확률(=취약점 x 위협) ▪ 자산의 손실·파손 시, 발생하는 손실 분석	▪ 정전사고 : 1회 발생 예상/년 ▪ 정전사고 발생 시 손실액 : 약 2천만 원
보안 기술	▪ '운영·관리 절차'에 적용되는 보안 기술 ▪ 특정 자산을 보호하기 위해, 현재 상태에서 추가(Add-on) 적용 필요(Unique)	▪ 전신 Scan에는 금속 탐지기 시스템을 적용
보안 솔루션	▪ 범용적인 보안 기술을 집대성한 제품 ▪ 현재 자산의 상태 변화를 최소화 가능	▪ 비인가 차량 통제를 위한 '차량통제시스템' 적용

보안 아키텍처 구성요소

3 보안 아키텍처

1 보안 아키텍처

2 보안 아키텍처 구성

B/B	내용	사례
보안기술 표준	▪ 보안 기술에 적용되는 국내·국제 표준	▪ 금속 탐지기 시스템은 zones.100 표준 적용 ▪ ISO 9001 인증 획득 제품 적용
운영/ 관리 절차	▪ 정책 구현 Procedure ▪ 특정 Task 수행 순서	▪ 임직원 집하장 출입 시에는 전신 Scan 적용 ▪ ICT 센터 출입자는 출입 대장 작성
운영자/ 담당자	▪ 특정 업무에 대한 책임자 ▪ 서비스 및 기기 등의 담당자(정·부)	▪ 정보보호 솔루션 운영담당자 : 강감찬 과장 ▪ 정보보호 총괄책임자 : 유관순 이사

보안 아키텍처 구성요소

보안 정책 수립

1 보안 목표 수립

1 보안 목표

1 보안 목표 개념

조직·기관·기업의 **'경영 목표'**를 달성하기 위한 부가적인 **'목표'**

일반적으로 **'경영 목표'**에 대한 내재적인 **'지원 항목'**

2 보안 목표 구성

보안 목표 = **자산** + **(추상적) 보호 방법**

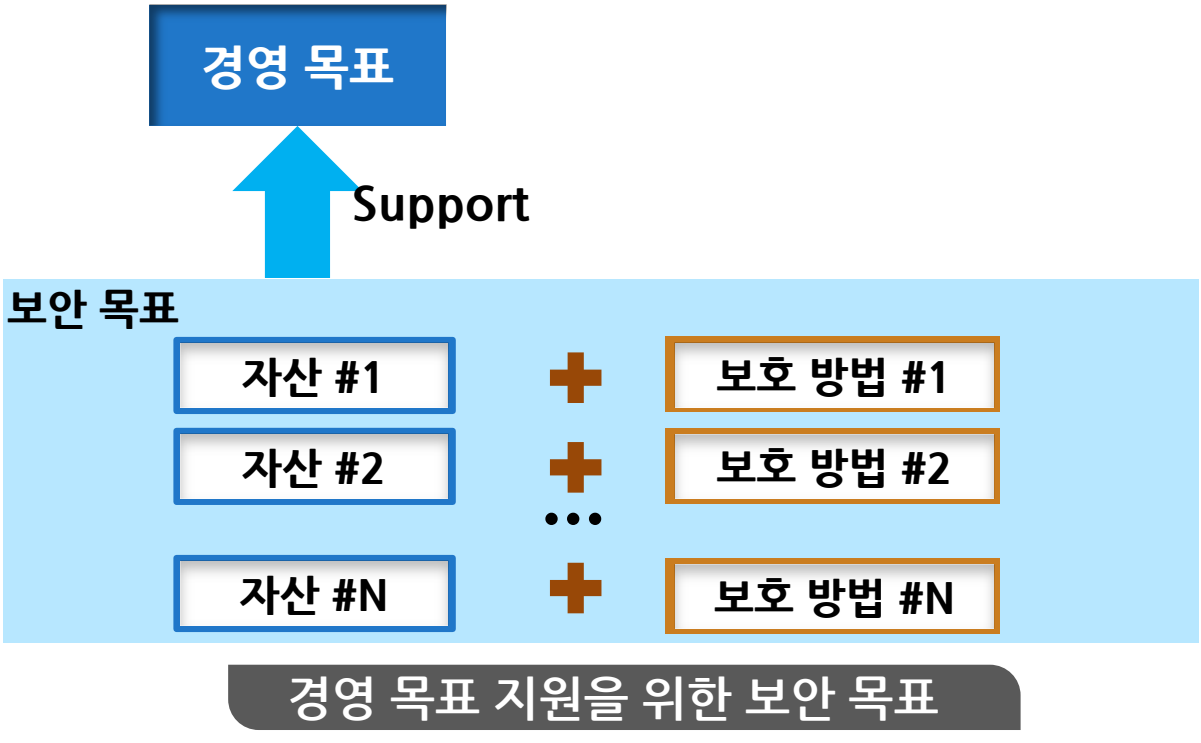
항목	설명
자산	조직 내·외부에 존재하는 '기업 존속 유지'에 근간이 되는 유·무형의 실체
보호 방법	자산의 가치를 유지·보호하고 활용할 수 있게 하는 수단

보안 정책 수립

1 보안 목표 수립

1 보안 목표

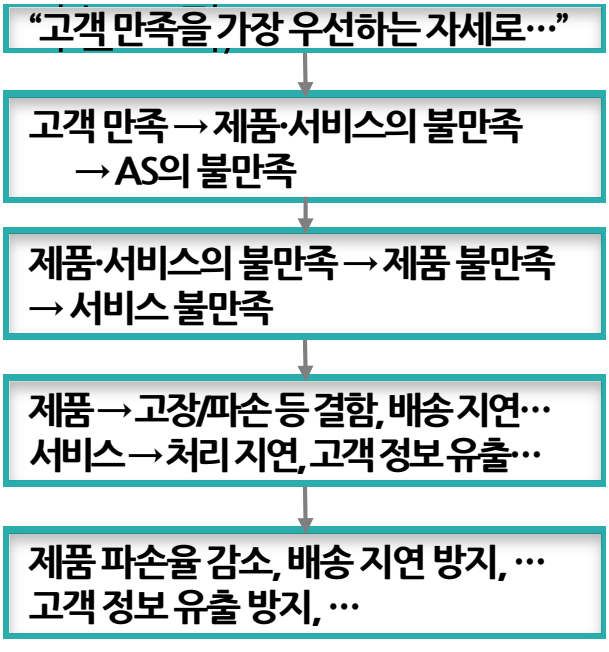
2 보안 목표 구성



1 보안 목표 수립

1 보안 목표

3 보안 목표 도출 절차



1 보안 목표 수립

1 보안 목표

4 보안 목표 도출 사례

경영 목표	자산	보호 방법
고객 만족도 향상	고객개인/주문정보	유출 방지
	상품배달체계	안정성, 신속성 유지/개선
매출 XXX억 달성	OOO제품관리체계	정확성 보장
	회계관리	법적 요구사항 준수
업계 1위 Market Share 달성	기술지원 체계	신속성 유지
	제품	안정성 향상
YYY 신제품 출시	신제품 관련 정보	기밀성 유지
	제품	품질 확보

2 보안 원칙,전략,수준

1 보안 원칙

1 보안 원칙 개념

- 보안 정책, 계획 등을 수립하고 구축하기 위하여 준수해야 할 일련의 추상적 기준
- 무조건 준수(예외 규칙 불허)
- 보안 대책(업무 Process, 보안 기술 적용, 보안 솔루션 선정 등)에 최종 적용(위반 여부 검토)

2 보안 원칙 표준

- NIST Security Principles
- OECD Guidelines
- GAISP (Generally Accepted Information Security Principles)
- Security Models

2 보안 원칙,전략,수준

1 보안 원칙

2 보안 원칙 표준

SSE-CMM, CMMI

ISO 27001

Security Assurance, Criteria (TCSEC, ITSEC, CC), 등

3 NIST 보안 원칙

NIST(미국 국립표준기술연구소) 800-14에서 제시한 보안 원칙

(변경)

- SP 800-14는 2018년도 3월에 폐기됨
- 개정 내용은 SP 800-12 Rev. 1, SP 800-53, SP 800-30 Rev. 1, SP 800-37 Rev. 1, SP 800-39에서 제시

2 보안 원칙,전략,수준

1 보안 원칙

3 NIST 보안 원칙

자산	보호방법
인식 (Awareness)	모든 참여자는 정보시스템과 네트워크 보안의 필요성을 명확히 인식
책임 (Responsibility)	모든 참여자는 정보시스템과 네트워크의 보안에 대한 책임이 부여됨
대응 (Response)	모든 참여자는 보안사고를 적시에 방지하고 탐지하며 대응할 수 있도록 협력적인 자세로 행동
윤리 (Ethics)	모든 참여자는 다른 사람의 법적 권익을 존중
민주적 (Democracy)	정보시스템과 네트워크 보안은 민주주의 사회의 기본적 가치와 조화
위험 분석 (Risk Assessment)	모든 참여자는 위험 평가분석 업무를 시행

2 보안 원칙,전략,수준

1 보안 원칙

3 NIST 보안 원칙

자산	보호방법
설계 및 적용 (Design & Application)	보안 설계 참여자는 정보시스템과 네트워크의 설계 시 보안을 기본적 요소로 포함
보안 관리 (Management)	포괄적 접근 자세로 지속적인 보안 관리 수행
재평가 (Reassessment)	모든 관련자는 보안을 주기적으로 리뷰하고 재평가 분석하여, 보강

2 보안 원칙,전략,수준

2 보안 전략

1 개념

- 보안 목표 달성을 위한 보안 대책을 수립·구현에 적용되는 고려사항
- 환경적인 제약사항을 '극복'하기 위한 추상적 방법론
- 환경적 2가지 제약사항을 극복하기 위한 방향 제시

보안 정책 수립

2 보안 원칙,전략,수준

2 보안 전략

2 환경적 제약사항

절대적 제약사항

- 조직의 현재 상황에 대한 물리적·논리적인 제약사항
- 사례
  - 비용, 시간, 인력적 한계
  - 법적인 강제사항

상대적 제약사항

- 절대적 제약사항을 극복한 이후, 경쟁/유사 조직과의 '비교'에 의한 제약사항
- 시장 점유율, 인지도, 평판 (경쟁적 우위권 확보 항목 전체)

3 보안 전략의 도출

- 조직의 내·외부 현황 조사 및 분석(비용, 시간, 인력, 법)
- 보안 목표의 강제/선택 사항 구분
- 분석 결과 통합/공통점 도출, 시사점/방향성 도출

2 보안 원칙, 전략, 수준

2 보안 전략

4 사례

보안 목표	강제/선택	환경 분석	방향성
고객 개인/주문 정보 유출 방지	법적 강제	▪ 사업 분야의 법적 준수 필요 ▪ 초기 투자금 다소 부족	▪ 법적 요구사항 우선 ▪ 비용효과 고려
상품 배달 체계의 안정성, 신속성 유지/개선	선택		
OOO 제품 관리체계의 정확성 보장	선택		
회계 관리의 법적 요구사항 준수	법적 강제		

보안 전략 수립 절차 및 사례

3 보안 정책 도출

1 보안 정책 개념

1 개념

- 조직·기업·기관의 '보안' 전반에 대한 명세
- 보안 목표에 종속적이며, 보안을 수행해야 하는 **당위성 기술**
- **기술·절차·(구체적) 방법 제외**, 필요에 따라 일부 항목 생략 가능

2 보안 정책 구성요소

항목	설명	정책 문구 사례
범위	보호해야 할 자산 명시	소화 시설을
목표	'보호'하는 근거	시설 안전을 위하여
방법	'보호'하기 위한 '추상적'인 방법	점검해야 한다.
책임과 권한	수행 조직에 대한 권한·책임	당직자는

3 보안 정책 도출

1 보안 정책 개념

3 보안 정책 도출 사례

제3장 인적 보안

제 1조(내부 인력 관리)

① (보안서약) 모든 임직원은 전사 비밀유지를 위한 서약서에 서명해야 한다.

② (보안교육) 모든 임직원은 일정 주기에 따라 사내 정보보호 인식제고를 위한 정보보안 교육에 참여해야 한다.

제3장 인적 보안

제 2조(외부 인력 관리)

① (외근 및 재택근무 금지)전사 임직원은 개발에 관련된 업무 수행을 재택근무 방식으로 수행할 수 없다.

② (개발 참여 외부인력 금지) 제품 개발 범위 내에서 소요되는 기술의 외부 인력 참여를 금한다.

③ (아웃소싱 범위 제한) 제3자 또는 아웃소싱은 제품, 개발 범위를 벗어나 기술 소요 범위로 한정한다.

3 보안 정책 도출

1 보안 정책 개념

3 보안 정책 도출 사례

제3장 인적 보안

제 2조(외부 인력 관리)

④ (제3자 의무) 외주업체 직원, 임시직, 계약관계에 있는 특수인은 회사의 임직원과 동일한 정보보호 책임과 의무를 갖는다.

⑤ (제3자 접속제한) 개발과 관련된 제3자 접속은 금지한다.

2 보안 규칙

1 보안 규칙 수립

추상적인 보안 정책을 '실무에 적용'하기 위하여, 최대한 상세히 기술

수행 주체, 책임자, 기술(표준 포함), 솔루션을 상세히 기술

보안 기술의 적용 대상, 범위, 적용 절차 등 **오용·오해의 소지가 없도록 상세히 기술**

3 보안 정책 도출

2 보안 규칙

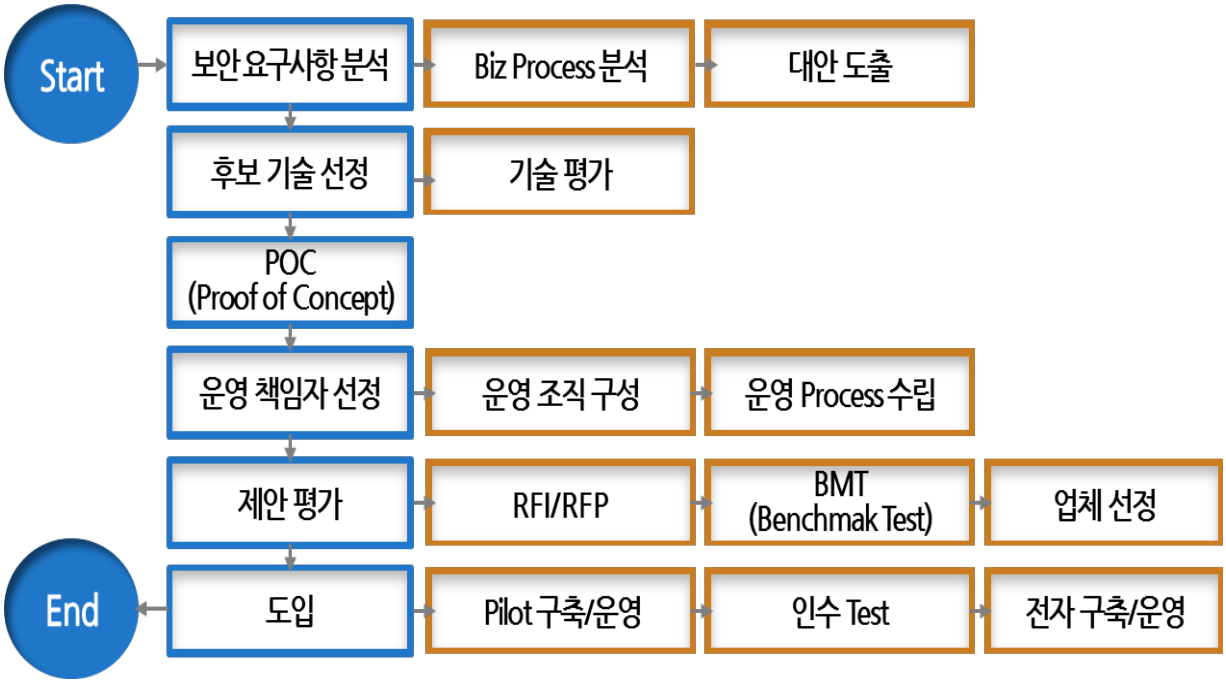
2 보안 규칙 수립 사례

⑤ (내부 네트워크 기밀 유지) 정보통신망에 사용되는 IP주소를 체계적으로 관리하여야 하며, 내부 정보 통신망을 보호하기 위하여 사설 주소체계(NAT : Network Address Translation)를 이용하여야 하며, 다음의 원칙을 준수하여 Firewall 정책을 설정한다.

- 개발 조직의 Network를 영업/기술지원/경영지원 등의 여타 부서와 분리
- 내부 제공 Server에 대한 Traffic 외 비인가 유입 Traffic 차단
- 업무와 관련 없는 Service 연관된 유출 Traffic의 차단
- 과도한 Network Resource 점유 Traffic의 차단
- 기타 내부 Network 및 Service에 위험이 될 수 있는 Traffic의 차단

1 보안 구축 절차

1 보안 구축 절차



2 보안 기술, 표준, 보안 솔루션

1 보안 기술, 표준, 솔루션

1 보안 기술, 표준, 솔루션 구분

기술

- 특정 보안 기능을 제공하는 전문적인 방법
- 기술 적용을 위한 전문적인 지식 및 Skill 필요
- 대부분의 경우, '특화'된 '자산'과 '방법'의 일부분으로 적용
- 다수의 보안(복합) 기술을 적용, 목표한 '보호 방법'의 구현

표준

- 기술에 대한 국·내외 표준
- 특정 기술에 대한 최소한의 기능, 성능, 안정성 보장
- 해당 기술에 대한 상호 호환성 보장

솔루션

- 단일 기술이나 복합 기술(조합된 형태)을 '제품' 단위로 구현한 통합체
- 해당 기술의 구매자(수용자)가 많아 범용적
- 상대적으로 일반적인 수준의 지식·기술 요구(구축, 운영)

2 보안 기술, 표준, 보안 솔루션

1 보안 기술, 표준, 솔루션

2 보안 기술, 표준, 솔루션 사례

3 보안 계획 수립

1 보안 계획 수립

1 보안 계획 수립에 대한 고려사항

보안 구축 및 운영에 대한 전반적인 사항에 대한 Master Plan을 수립하는 일련의 행위

실행 당위성과 절차, 일정, 사전 준비 사항, 변경 전·후에 대한 명확한 제시

- 실무자가 이해할 수 있을 정도의 '상세 수준'으로 계획 수립
- 이해관계자 전체에 대한 '합의' 도출
- 각 진행 과정에서 이루어지는 행위에 대한 근거 기록
- 모든 목표(Object), 행위(Action)에 대하여 "Why?"에 대해 답변 가능 수준으로 준비

보안 계획 수립

2 보안 계획에 포함되는 내용

항목	설명	사례
자산	▪ 조직 내·외부에 존재하는 '기업 존속 유지'에 근간이 되는 유·무형의 실체	전자문서
보호 방법	▪ 자신의 가치를 유지/보호하고 활용할 수 있게 하는 수단	유출/변조 차단
보안 설계	▪ 자산을 보호하기 위반 방법을 '적용'하기 위한 논리적, 물리적 위치 ▪ 방법에 대한 구체적인 '보안 기술'이나 '보안 솔루션'	DRM 적용
기술 표준	▪ 기술 구현에 사용되는 국내·외의 표준 기술 ▪ 해당 기술/솔루션에 대한 인지도, 안정성 및 성능, 인증 획득 여부 등	암호, Hash 알고리즘
구축 절차	▪ 해당 '보안 기술'이나 '솔루션'을 도입하기 위한 절차	RFP→제안평가→선정→도입→운영
운영 조직	▪ 해당 '보안 기술'이나 '솔루션'을 운영하는 전문/전담 조직 및 인력	정보시스템 관리팀
운영 절차	▪ 도입 후 결재에 따른 정책 관리, 임의 정책 관리 불가	결재 후 담당자 참조
보안 교육	▪ '보안 기술'이나 '솔루션'을 적용 이후 변경되는 사항에 따른 전달	프로세스 변경 교육

학습정리

1. 보안 개요

- 보안 구축은 상당 수준의 전문적인 지식과 기술을 요구
- 보호 자산의 특성을 분석하여 전략에 따라 보안 정책 및 계획을 수립하고 구축/운영 실행

2. 보안 정책 수립

- 보안 정책은 추상적인 수준으로 작성되는 일련의 당위성과 목표를 기술
- 보안 정책은 경영 목표를 뒷받침하며 원칙과 전략에 따라 작성

3. 보안 계획 수립

- 보안 계획은 실무자가 이해할 수 있을 수준으로 상세히 작성
- 목표와 환경, 실행 근거 등을 최대한 기술