Tutorial 2

# 인터넷 보안과 보안 컨설팅

안 혜 연
(씨큐어소프트)

# 인터넷 보안과 보안컨설팅

2000. 11.

㈜시큐어소프트

## Part I

◁ ○ ▷

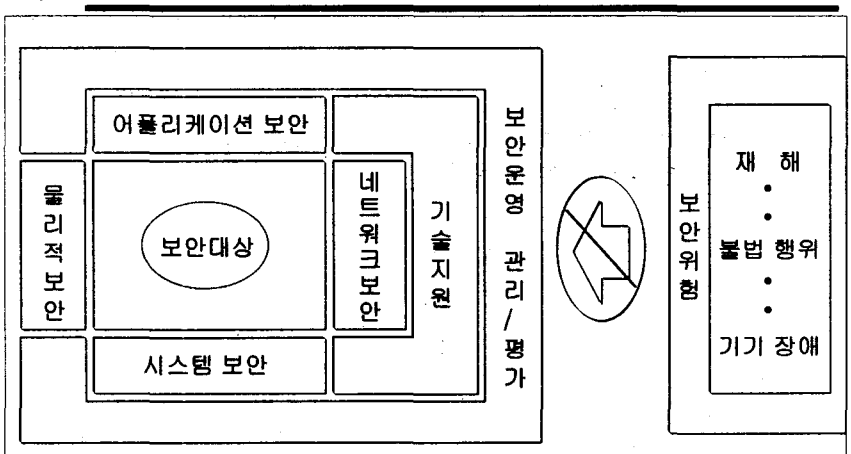
# Understanding IT Security

## Defining Information Security

- **정보 보호란?:** 데이터 및 시스템을 고의적 혹은 실수에 의한 불법적인 공개 (노출), 변조, 파괴 및 지체로부터의 보호
- 정보 보호의 목표
  - 비밀성 (Confidentiality)의 보장
  - 무결성 (Integrity)의 보장
  - 가용성 (Availability)의 보장
- 정보 보호 분류
  - 보안 관리
  - 네트웍 보안
  - 시스템 보안
    - **Operating System 보안**
    - **Workstation / PC security**
  - 어플리케이션 보안
  - 물리적 보안
  - 보안 평가



## Information Security Overview (I)




- 관리영역 : 보안운영, 기술지원
- 기술영역 : 물리적 보안, 네트워크보안, 시스템보안, 어플리케이션보안

## Information Security Overview (II)

- **Network** 보안
  - 허가 받지 않은 사용자의 자체 network 접근 방지
  - 보안 상 취약한 프로토콜에 (FTP, Telnet 등) 의한 network 접근 방지
  - 전송되는 자료의 기밀성 보장
  - 전송되는 자료의 변경방지
- **System** 보안
  - 허가 받지 않은 사용자의 시스템 접근 방지
  - 저장된 정보의 (사용자 계정정보 등) 기밀성 보장
  - 저장된 정보의 변경 방지
- **Application** 보안
  - 허가 받지 않은 사용자의 application 접근 방지
  - 사용되는 (저장 혹은 전송되는) 정보의 (사용자 신상정보, 계좌정보 등) 기밀성 보장
  - 사용되는 (저장 혹은 전송되는) 정보의 변경 방지
  - 정보 전송 부인 방지
  - Application의 이상 작동 시도 방지



## Security Technologies

| Security func. / Target | Authentication | Access Control | Confidentiality | Integrity | Non Repudiation |
|---|---|---|---|---|---|
| N/W | • ID / Password<br>• OTP | • IP filtering<br>• Protocol filtering<br>• Monitoring | • IP Tunneling | • IP Tunneling | |
| System | • ID / Password<br>• Smart card<br>• Biometrics | • Role-based access control<br>• Security attribute setup<br>• Pattern Dection | • File encryption<br>• Secure DBMS | • File Integrity Check<br>• Secure DBMS | |
| Appl. | • ID / Password<br>• Smart card<br>• Digital Certificate<br>• Biometrics | • User-type based access control | • Data encryption | • Digital Signature<br>• CheckSum<br>• MAC | • Digital Signature |

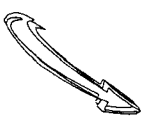
## Security Solutions

| Security func. / Target | Authentication | Access Control | Confidentiality | Integrity | Non Repudiation |
|---|---|---|---|---|---|
| N/W | ▪ Firewall<br>▪ IDS<br>▪ Vulnerability Analysis Tool | | ▪ VPN<br>▪ VirusWall | | |
| System | ▪ IDS<br>▪ Sever Security Tool<br>▪ Vulnerability Analysis Tool | | | | |
| Appl. | ▪ PKI<br>▪ SSO | | ▪ Secure E-mail | | |

㈜시큐어소프트 7

## Effective Security?

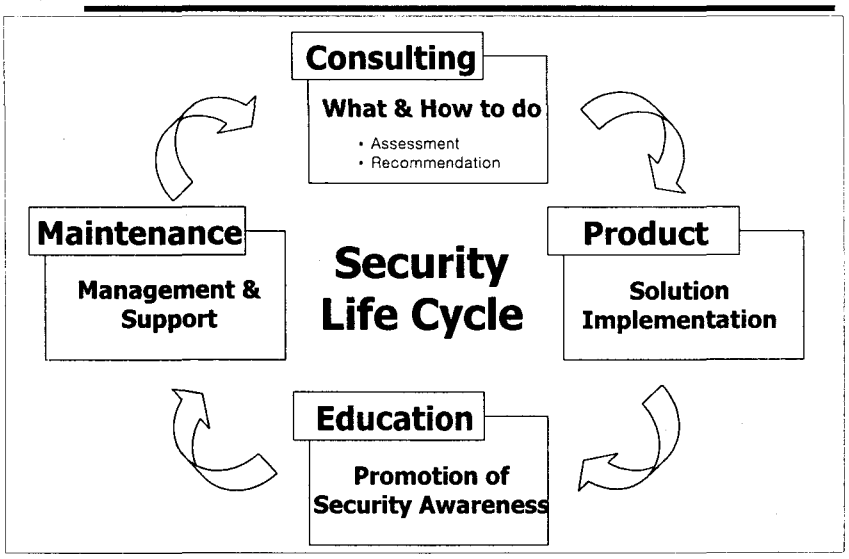
- 100% 완벽한 보안은 없다
- 컴퓨터 성능에 아무 도움이 되지 않는다
- 도입된 보안 대책이 반드시 필요한 것인지 확신할 수 없다
- 도입된 보안 대책이 효과적으로 작동할지를 확신할 수 없다
- 도입된 보안 대책의 성공 여부는 실패율에 의해서 측정된다
- *그럼에도 불구하고 안할 수는 없다*



- 효과적인 보안 대책 구현
  - 최소한의 비용으로 최대한의 효과 달성
  - 비용과 손실의 합을 최소화

㈜시큐어소프트 8

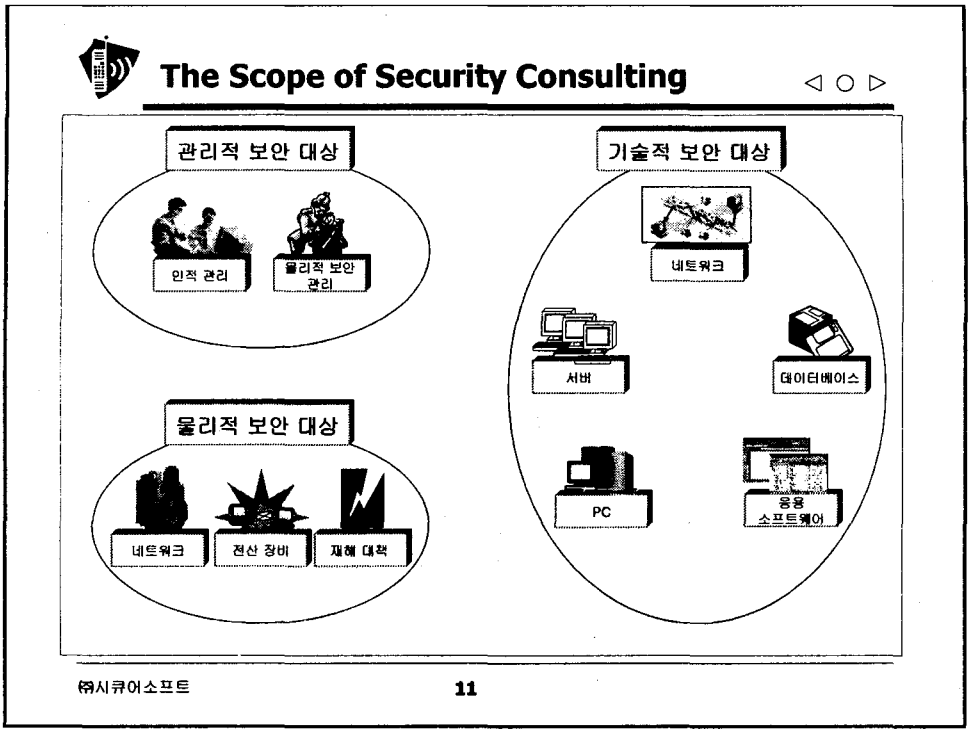
## Framework for Effective Security



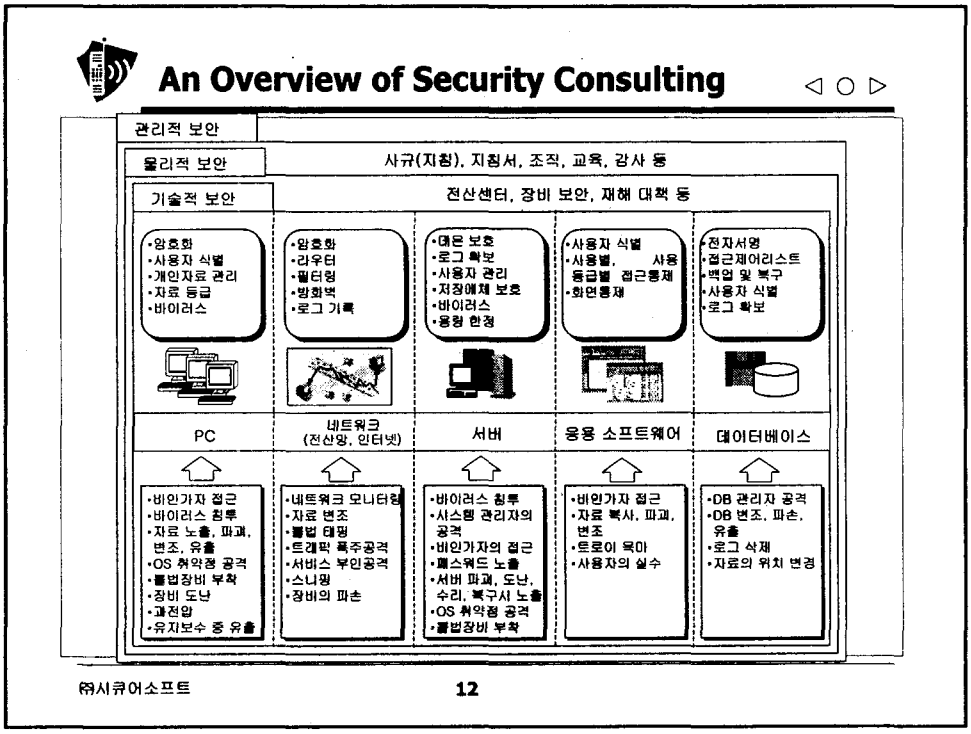



## Part II

# Understanding Security Consulting

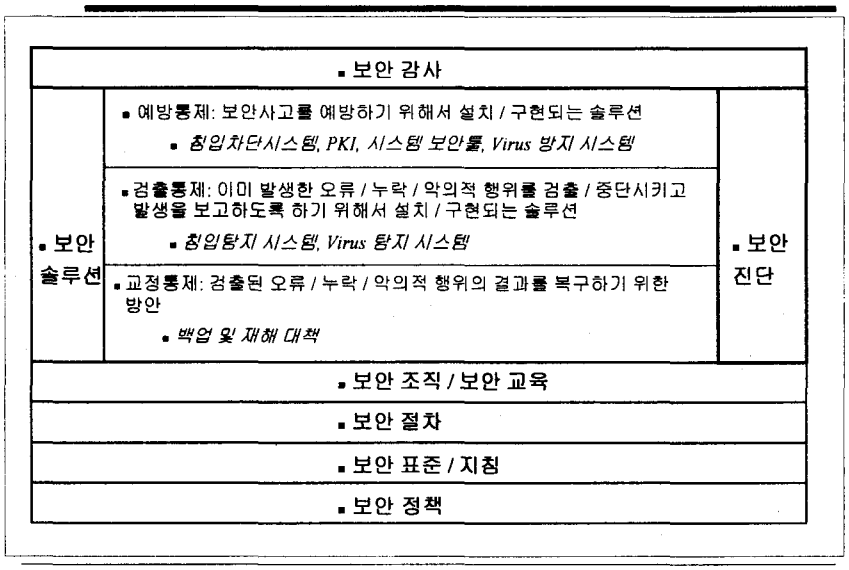



㈜시큐어소프트 11



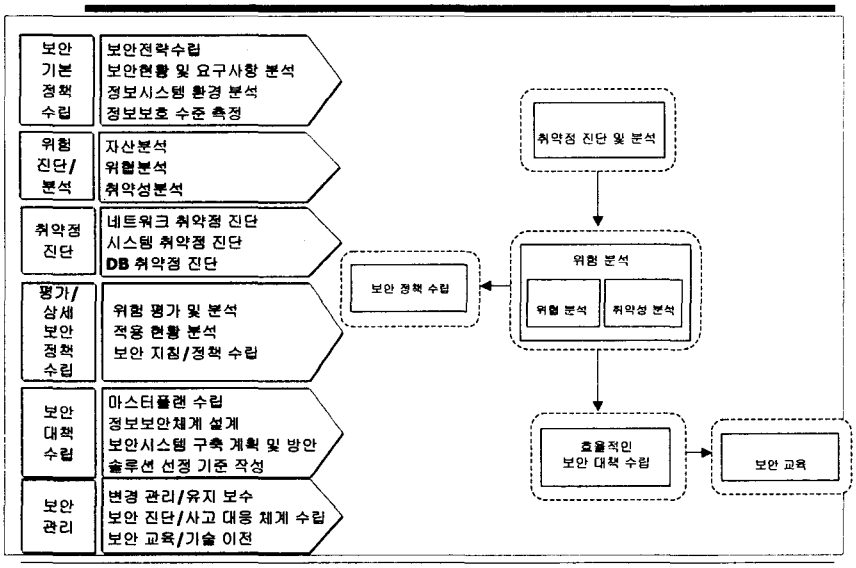

㈜시큐어소프트 12

## Framework for Effective Security






## Security Consulting Methodology

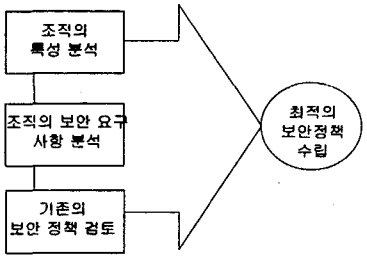


## Security Policy

- 보안 정책이란?
  - 조직의 정보자산 및 기술에 접근하기 위해 사용자들이 지켜야 하는 규칙을 기술한 문서
- 보안 정책의 고유성
  - 효율적인 보안 대책 구현을 위해 조직의 특성 및 업무 목적에 따라 고유의 보안 정책이 요구 됨
- 모든 보안 행위의 기반이 되는 보안 정책
  - 보안 정책은 조직의 기술과 정보자산을 보호하기 위한 필수적인 요구사항을 사용자와 기술자, 그리고 관리자에게 통보
  - 보안 정책은 정보자산에 접근하는 사용자, 운영자, 관리자의 행위에 제약을 가함
  - 따라서, 보안 정책은 조직의 정보자산을 안전하게 보호하고 효율적으로 관리하기 위해 최우선적으로 수립해야 하는 항목임



## Security Policy Establishment




- 조직의 특성 및 업무 목적 파악
  - 조직의 사업 목적 고려
  - 제공되는 서비스와 보안과의 관계 고려
- 위험 분석을 통한 보안 요구 사항 분석
  - 조직의 서비스 운영 환경 검토
  - 조직의 중요 자산 정의: 자산의 중요도, 손실 가치, 복구 비용 고려
  - 중요 자산에 대한 위협 및 취약성 식별
- 기존 보안 정책 검토
  - 조직이 보유하고 있는 기존의 보안 정책 및 절차 검토
  - 조직의 정보기술 환경에 적합한지 검토
  - 필요시 조직의 요구사항을 최대한 충족시킬 수 있도록 보안 정책 수정, 보완

## Security Procedures

◁ ○ ▷

- **보안 지침이란?** 조직의 정보자산을 어떻게 관리하고 보호할 것인가에 대해 세부적으로 기술한 문서
- **보안 정책과 보안 지침의 다른 점**

| | 보안 정책 | 보안 지침 |
|---|---|---|
| 성격 | 강제적 | 선택적, 권고적 |
| 내용 | 일반적인 핵심 사항 | 구체적인 세부 사항 |
| 수립 기간 | 오랜 기간(수 년 or 수십 년) | 몇 년 이내 |
| 변경 | 자주 변경되지 않음 | 빈번히 변경 |

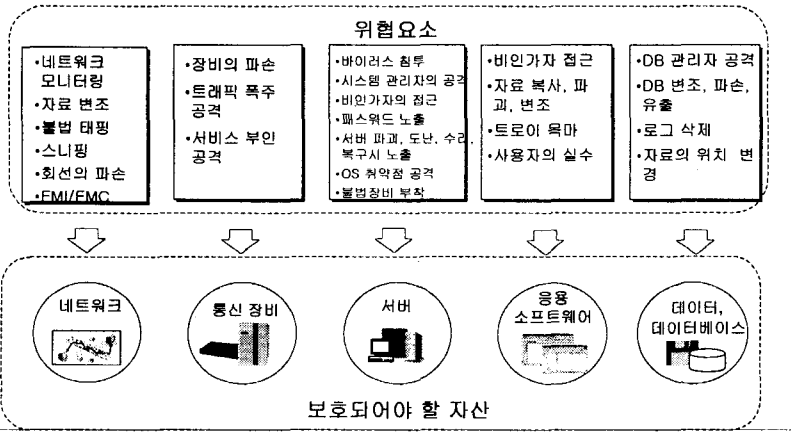
- **보안 정책 및 보안 지침 예**
  - 보안 정책 : 외부망에서 내부망으로의 접근은 원칙적으로 차단한다.
  - 보안 지침 : ftp 프로토콜은 다음과 같이 통제한다.
    - 외부-> 내부 : 모든 접속 차단
    - 내부-> 외부 : get 허용, put 차단



## Risk Assessment

◁ ○ ▷

- **위험분석 목적:** 위협분석, 취약성 분석, 기존 보안대책 분석을 통해 보호되어야 할 정보시스템의 위험수준을 판단하고, 이에 대한 대응책을 도출하여 정보보호수준을 향상시킴



## Risk Assessment Methodologies

◁ ○ ▷

- 위험분석 목적
  - 위협분석, 취약성 분석, 기존 보안대책 분석을 통해 보호되어야 할 정보시스템의 위험수준을 판단하고, 이에 대한 대응책을 도출하여 정보보호수준을 향상시킴
- 위험분석 방법론
  - 정량적 위험분석
    - 과거자료분석법
    - 수학공식 접근법
    - 확률분포법
    - 점수법
  - 정성적 위험분석
    - 델파이법
    - 이야기식 시나리오
    - 순위결정법
  - 위험분석 소프트웨어: BDSS(Bayesian Decision Support System), Buddy System, AnalyZ, Control-It, RiskWatch, Cobra, HAWK(국내)



## Risk Assessment Details

◁ ○ ▷

- 위협분석
  - 조직의 자산에 피해를 가할 수 있는 잠재적인 요소인 위협을 파악하고 발생 가능성을 분석함
    - 위협파악 : 위협유형, 위협주기 산출
    - 위협속성 : 무결성, 비밀성, 가용성, 정보유출, 파괴 등
    - 위협순위 : 자산에 대한 영향에 따라 위협의 중요도를 정함
- 취약성 분석
  - 조직의 자산이 가지고 있는 취약성을 점검하여 전반적인 취약성의 정도 분석
    - 네트워크, 시스템, 데이터베이스 취약성 점검
    - 위험분석 방법론 또는 취약점 분석 tool (스캐너) 이용
    - 취약성의 위험성에 따른 취약성 등급 제공

## Vulnerability Assessment (I)

◁ ○ ▷

- 취약점 분석의 필요성
  - 네트워크, 시스템, 데이터베이스, 그리고 어플리케이션은 조직의 중요 정보를 처리하며, 필수적인 서비스와 응용 프로그램을 제공
  - 네트워크, 시스템, 데이터베이스, 그리고 어플리케이션은 자체적으로 취약점 내포
  - 인터넷 접속과 내부망으로의 접속으로 인한 위험성 증가
  - 조직의 중요 정보 처리 및 필수 서비스는 위협에 노출



## Vulnerability Assessment (II)

◁ ○ ▷

| | |
|---|---|
| 네트워크 취약점 분석 | ▪ 네트워크 구조 분석<br>▪ **Router,** 스위칭 디바이스 점검<br>▪ 네트워크 서비스 취약점 분석 |
| 시스템 취약점 분석 | ▪ 시스템 사용자 계정 및 패스워드 취약점 분석<br>▪ 파일 접근 권한 설정 점검<br>▪ 시스템 서비스 구성 취약점 분석<br>▪ 파일 소유권, 백도어 파일 등 파일시스템 점검 |
| 데이터베이스 취약점 분석 | ▪ 사용자 권한 및 취약한 패스워드 점검<br>▪ 시스템 무결성 점검 |
| 어플리케이션 취약점 분석 | ▪ 어플리케이션 무결성 점검<br>▪ 사용권한 설정 점검<br>▪ 가능 동작(결과, 수행과정 등) 점검 |
| 실제 침입시험 | ▪ 네트워크 및 시스템의 취약점 및 피해 가능성 확인<br>▪ 정보시스템에 대한 침입자의 접근 권한 획득 시험<br>▪ 감사기록, 모니터링, 침입탐지 및 대응상황 점검 |

## The Way to Effective Security

◁ ○ ▷

- 진단 내용을 바탕으로 단계적이고 체계적인 취약점에 대한 보안 대책 방안 제시
- 보안솔루션 선정 및 제시
  - 기업의 환경에 적합한 최적의 보안솔루션 제시
  - 기업의 요구사항 및 적절한 비용산정에 의한 보안솔루션 선정
- 보안시스템 아키텍처 디자인
  - Web 기반 또는 클라이언트/서버 환경에서 기업 정보시스템의 신뢰성을 높이기 위한 기술적 보안체계 구축
- 통합 보안 모델 제공
  - 기업의 안전한 인트라넷 구축
  - 조직의 중요 서버 및 데이터 보안체계 구축



## Education (I)

◁ ○ ▷

**목 적**

- 정보보안에 대한 인식 제고
- 부주의나 고의에 의한 보안 사고 최소화
- 정보 보안 기술 전수
- 효율적인 정보보안체계 설계/구축 지원
- 보안 점검 및 사고 대응, 유지보수

⇨ 보안 인력 양성

**대상**

- 경영층 및 관리자
- 보안업무 담당자
- 시스템 운영자
- 개발자
- 일반 사용자

**누구에게, 어떻게 ?**

**SecureSoft의 기술력 + 경험 + ?(모든것)**

- 필요지식 및 업무에 따라 교육 내용을 차별화
- 다양한 욕구를 만족(이론+실습)
- 실전에 사용할 수 있는 기술과 방법을 교육

## Education (II)

◁ ○ ▷

- 교육 내용

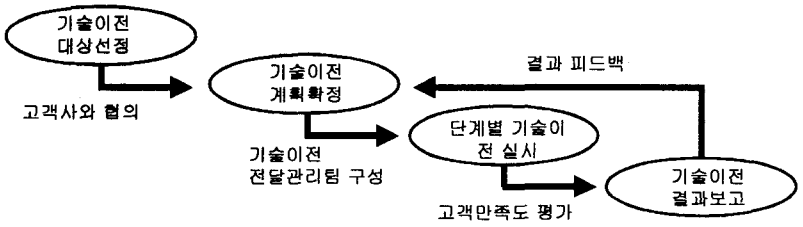
| 대상 | 주요 내용 | 비고 |
|---|---|---|
| 경영층 및 관리자 | 정보보호의 필요성 및 기술 개요<br>정보보호 체계 구축 절차<br>보안관리 | 모의 Hacking Demo |
| 보안업무 담당자 | 정보보호 기술<br>보안업무 범위 및 역할<br>보안 정책 및 지침 수립 방법<br>정보보호 체계 구축 방법<br>점검 및 진단, 해킹 및 사고 대응 절차<br>유지보수 | 정책/지침 수립 실습<br>점검/진단 실습 |
| 시스템 운영자 | 정보보호의 필요성 및 기술 개요<br>시스템별 보안 요구 기능 및 대책 구현 방법<br>보안 제품 이해 및 운영 기법<br>해킹 및 사고 대응 방법 | 시스템 보안 기능 설정 및 분석 방법 실습<br>툴 사용법 실습 |
| 개발자 | 어플리케이션별 보안 요구 기능 및 취약점<br>어플리케이션 보안 기술<br>구현 사례 및 실습 | 프로그래밍 실습 |
| 일반사용자 | 정보보호의 필요성<br>사용자 준수 사항<br>PC보안 및 바이러스 방지 | PC 보안 및 바이러스 방지 기능 설정 실습 |



## Knowledge Transfer

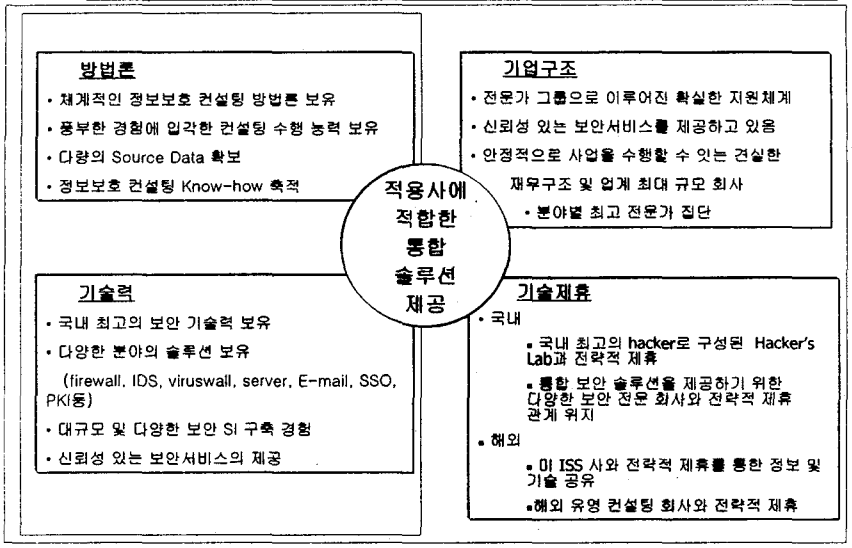
◁ ○ ▷

- 기술이전 체계




- 기술이전 방식 및 내용
  - 프로젝트 공동 수행
    - Bench Marking 및 Pilot 구현의 공동 수행으로 실무레벨의 기술전수
    - 분야별 보안 실무 가이드 공동 작성을 통한 향후 정보보호 체계의 유지 능력 보유
  - 교육
    - 각종 Tool의 활용 법 및 Report 분석 활용 법
    - 감사 및 진단시의 주요 핵심 기술 전수

## SecureSoft's Security Consulting






## Conclusion

- (주)시큐어소프트: *보안의 A to Z 를 제공할 수 있는 국내 유일의 보안 업체*
  - **Consulting** - 보안 정책 / 보안 진단등을 위한 최적의 정보 보호 구축 방안 제시
  - **해킹 방지 및 대응을 위한 현실적인 솔루션 제공**
    - 침입차단시스템 (수호신 v2.0) - 국내 유일의 국가 인증 (K4E) 취득
    - 침입탐지 및 대응 시스템 (RealSecure) - 최대 해킹 패턴 DB보유 (400여개)
    - 네트워크 / 서버 / DB 보안 취약점 분석 시스템
    - PKI 솔루션 (SecurePKI)
    - VPN 솔루션 / Desktop 보안 솔루션 / Virus 솔루션
  - **최적의 정보 보호 시스템 구축을 위한 통합 솔루션 (Integrated Security)**
  - **보안 교육 사업을 통한 보안 인력 양성**
  - **Managed Security Service**
    - 정기적인 보안 진단 서비스
    - 보안 관련 제품 관리 및 유지 보수 서비스
    - 침입탐지 경보 및 대응 서비스 (조기 경보 서비스)