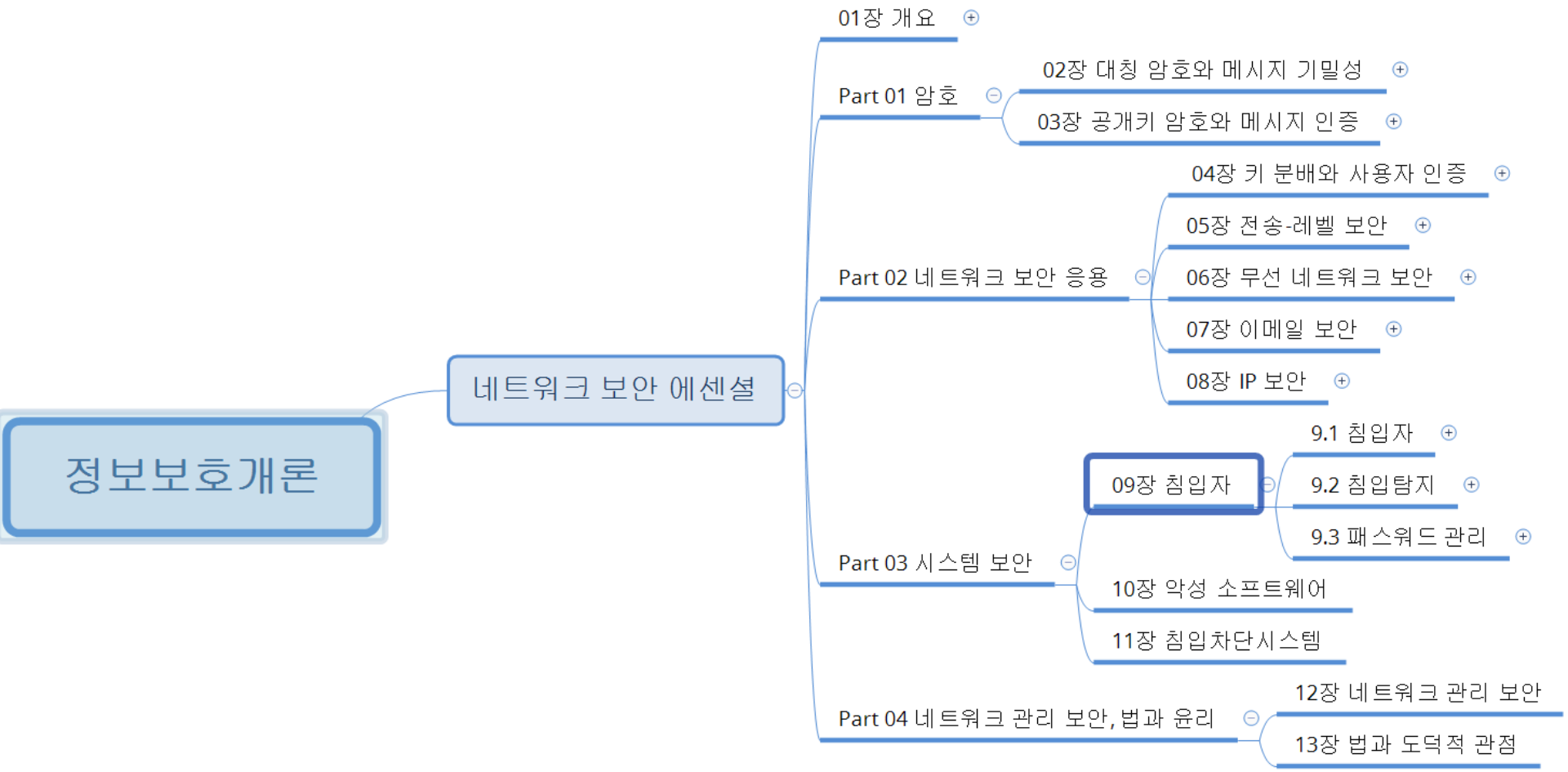
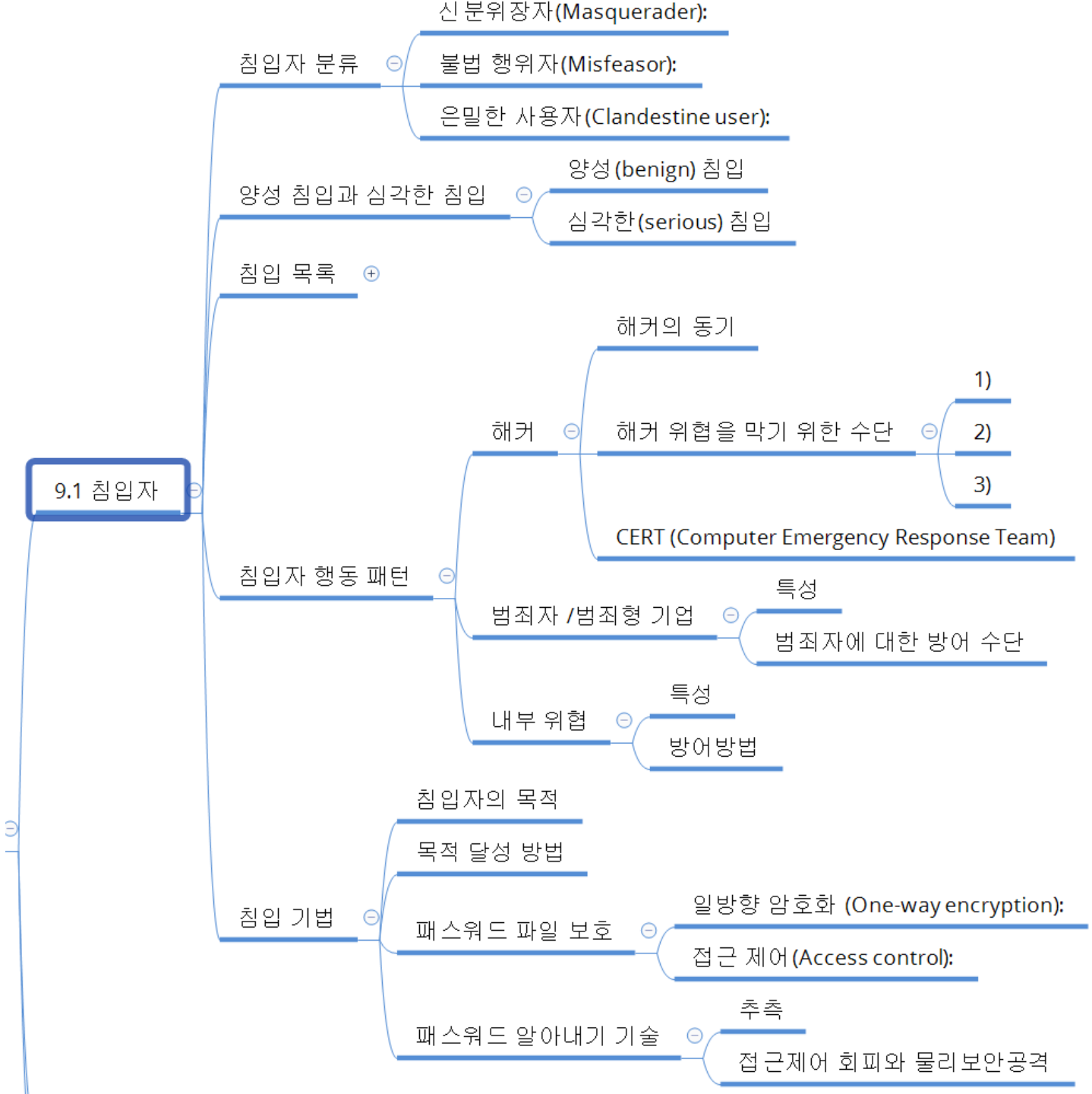
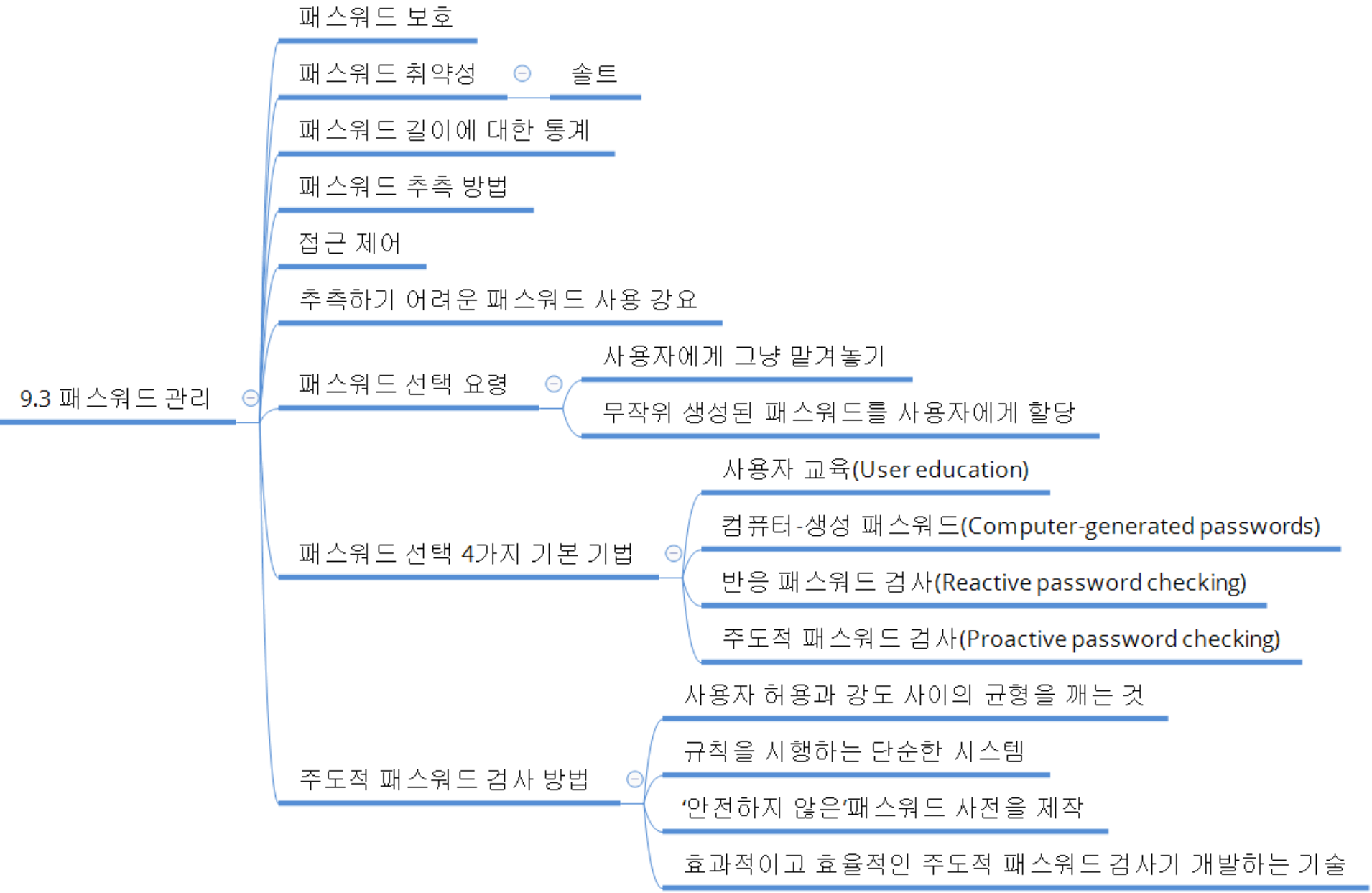
정보보호개론


네트워크 보안 에센셜
01장 개요
Part 01 암호
02장 대칭 암호와 메시지 기밀성
03장 공개키 암호와 메시지 인증
Part 02 네트워크 보안 응용
04장 키 분배와 사용자 인증
05장 전송-레벨 보안
06장 무선 네트워크 보안
07장 이메일 보안
08장 IP 보안
Part 03 시스템 보안
09장 침입자
9.1 침입자
9.2 침입탐지
9.3 패스워드 관리
10장 악성 소프트웨어
11장 침입차단시스템
Part 04 네트워크 관리 보안, 법과 윤리
12장 네트워크 관리 보안
13장 법과 도덕적 관점


9.1 침입자
침입자 분류
신분위장자(Masquerader):
불법 행위자(Misfeasor):
은밀한 사용자(Clandestine user):
양성 침입과 심각한 침입
양성(benign) 침입
심각한(serious) 침입
침입 목록
침입자 행동 패턴
해커
해커의 동기
해커 위협을 막기 위한 수단
1)
2)
3)
CERT (Computer Emergency Response Team)
범죄자 /범죄형 기업
특성
범죄자에 대한 방어 수단
내부 위협
특성
방어방법
침입 기법
침입자의 목적
목적 달성 방법
패스워드 파일 보호
일방향 암호화 (One-way encryption):
접근 제어(Access control):
패스워드 알아내기 기술
추측
접근제어 회피와 물리보안공격


9.2 침입탐지
침입탐지의 필요성
침입자와 합법적 사용자 행동 프로파일
긍정오류와 부정오류
침입탐지 방법
통계적 변형탐지(Statistical anomaly detection)
규칙-기반 탐지(Rule-Based Detection)
두 방법의 차이
감사기록
기본 감사기록 (Native audit records)
탐지-전용 감사기록 (Detection-specific audit records)
도로시 데닝이 개발한 탐지-전용 감사기록 예
통계적 변형탐지
두 가지 부류
임계값 탐지
프로파일링 기법
임계값 탐지(threshold detection)
프로파일-기반 시스템(profile based)
규칙-기반 침입탐지
두 가지 방법
변형탐지
침투식별
규칙-기반 변형탐지 (Rule-based anomaly detection)
규칙-기반 침투식별(Rule-based penetration identification)
기본-비율 오류
분산 침입탐지
분산 침입탐지 시스템 설계 문제점
분산 침입탐지 시스템의 예
분산 침입탐지 구조
에이전트 구조
시스템 감사 구현 절차
허니팟
침입탐지 교환 형식


9.3 패스워드 관리
패스워드 보호
패스워드 취약성
솔트
패스워드 길이에 대한 통계
패스워드 추측 방법
접근 제어
추측하기 어려운 패스워드 사용 강요
패스워드 선택 요령
사용자에게 그냥 맡겨놓기
무작위 생성된 패스워드를 사용자에게 할당
패스워드 선택 4가지 기본 기법
사용자 교육(User education)
컴퓨터-생성 패스워드(Computer-generated passwords)
반응 패스워드 검사(Reactive password checking)
주도적 패스워드 검사(Proactive password checking)
주도적 패스워드 검사 방법
사용자 허용과 강도 사이의 균형을 깨는 것
규칙을 시행하는 단순한 시스템
'안전하지 않은'패스워드 사전을 제작
효과적이고 효율적인 주도적 패스워드검사기 개발하는 기술