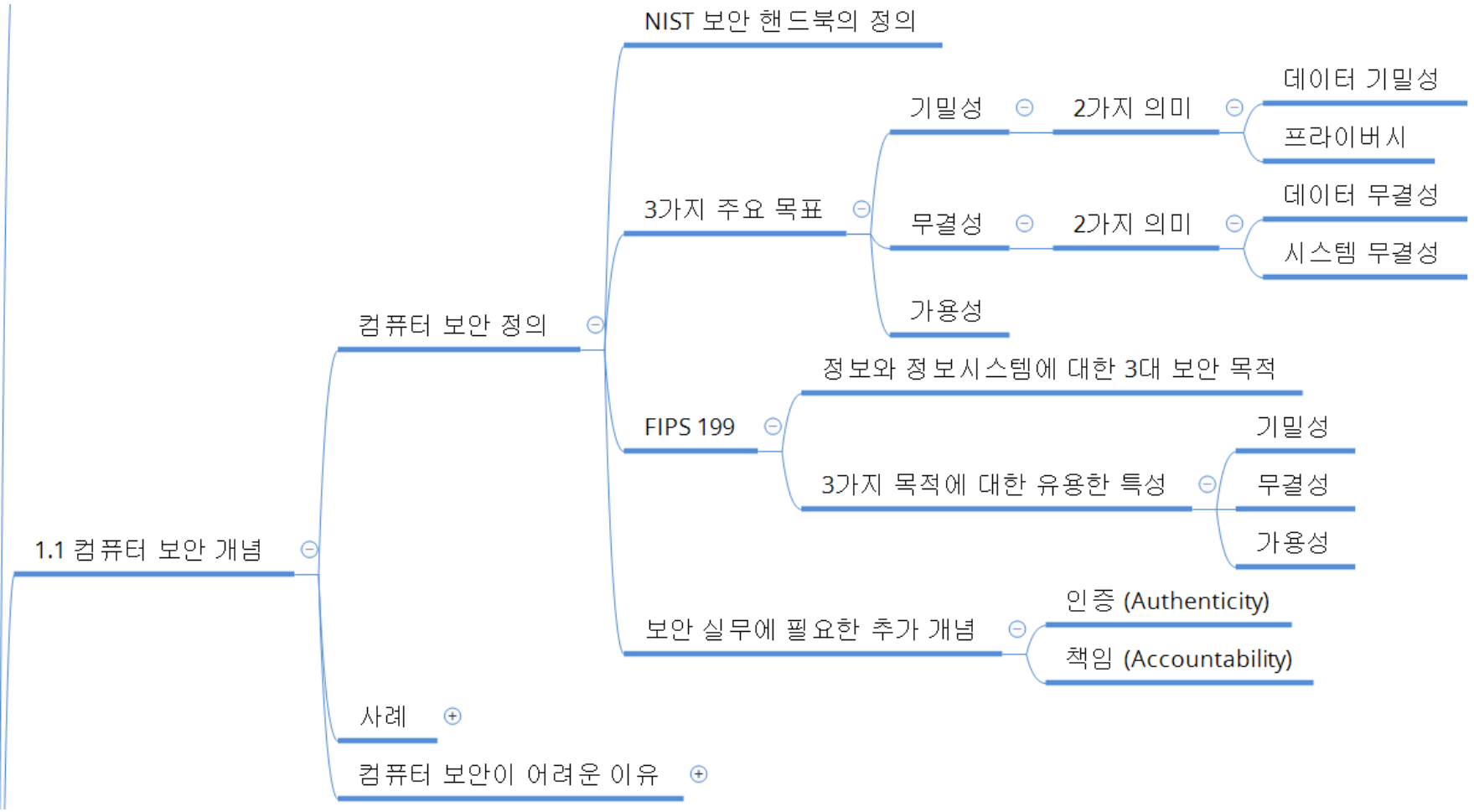
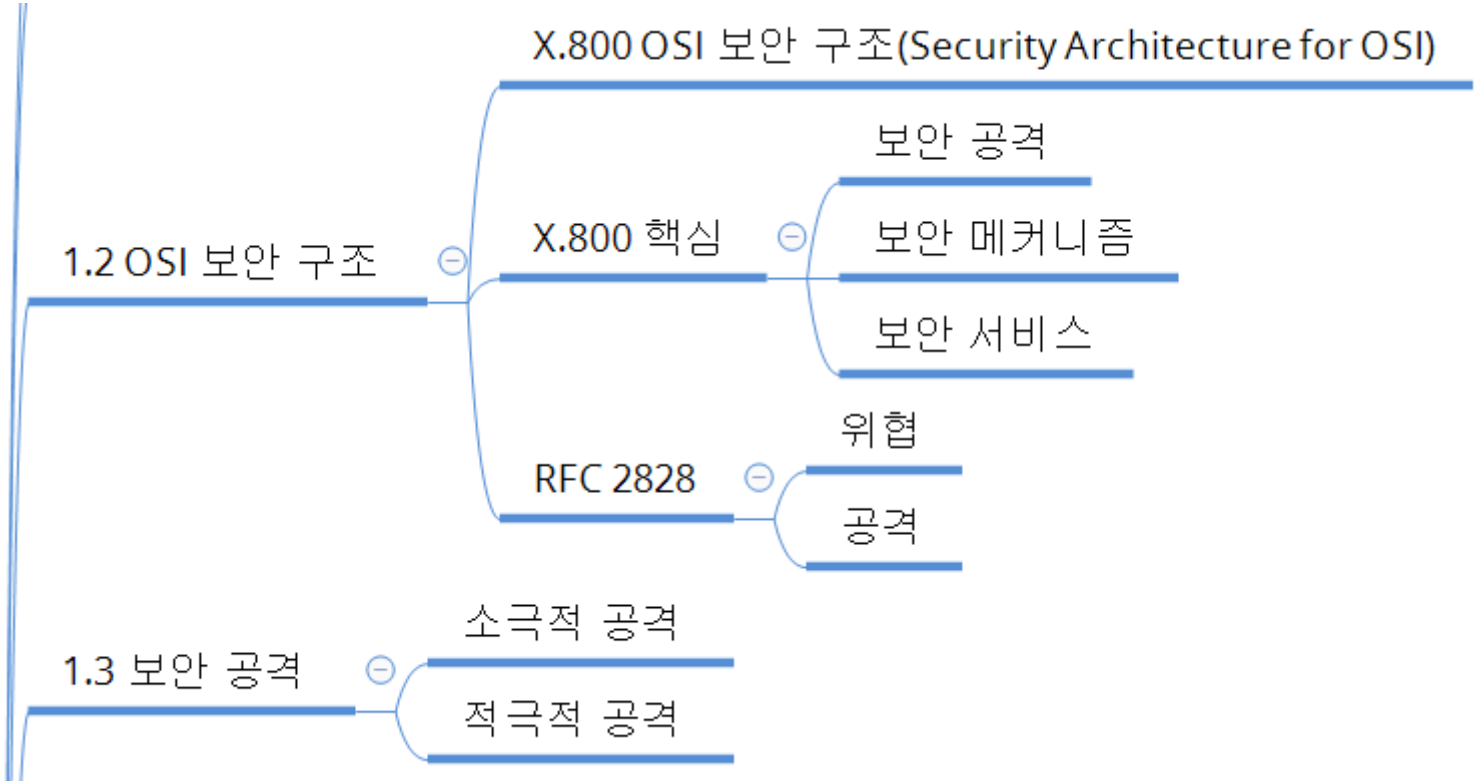
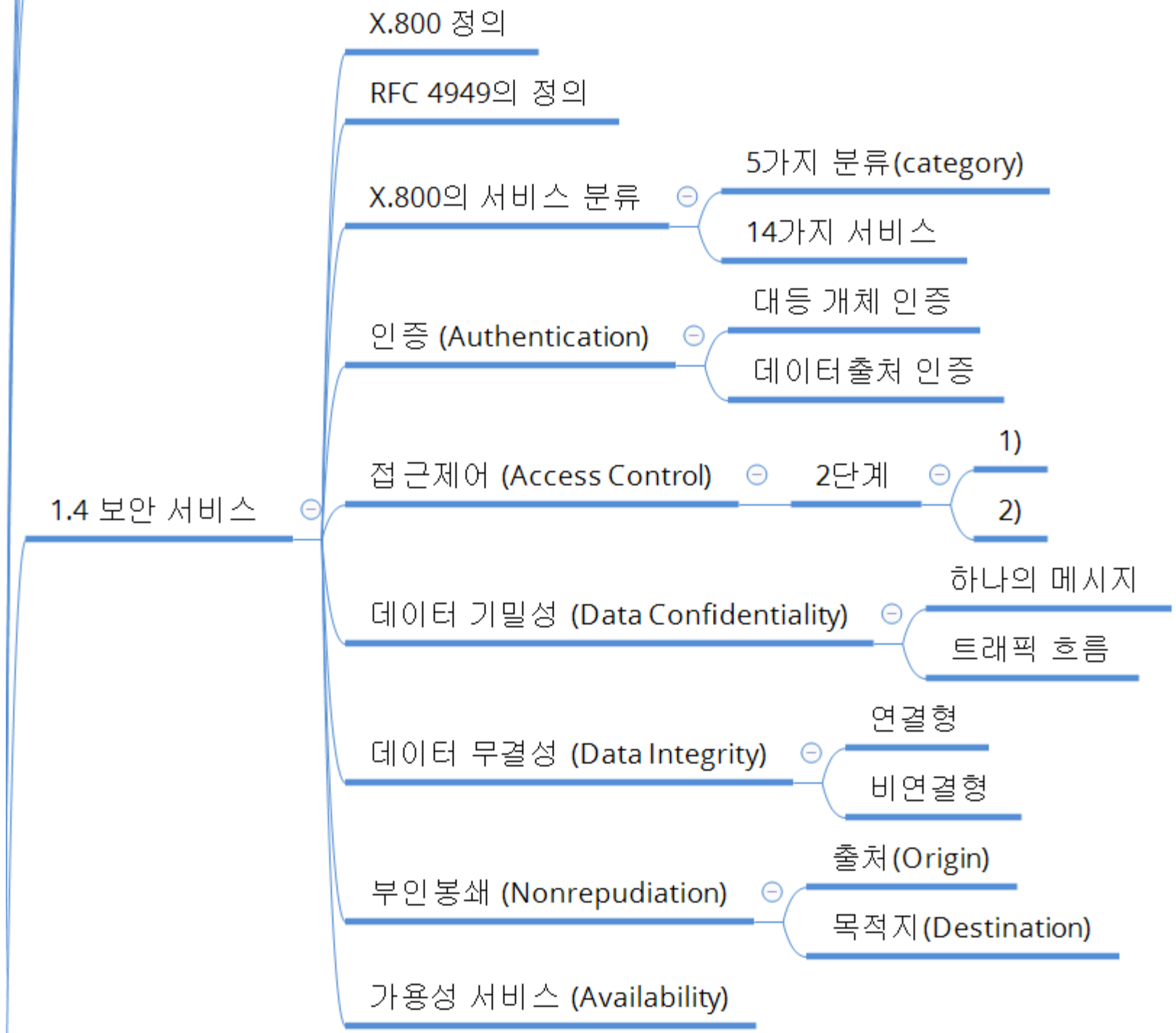
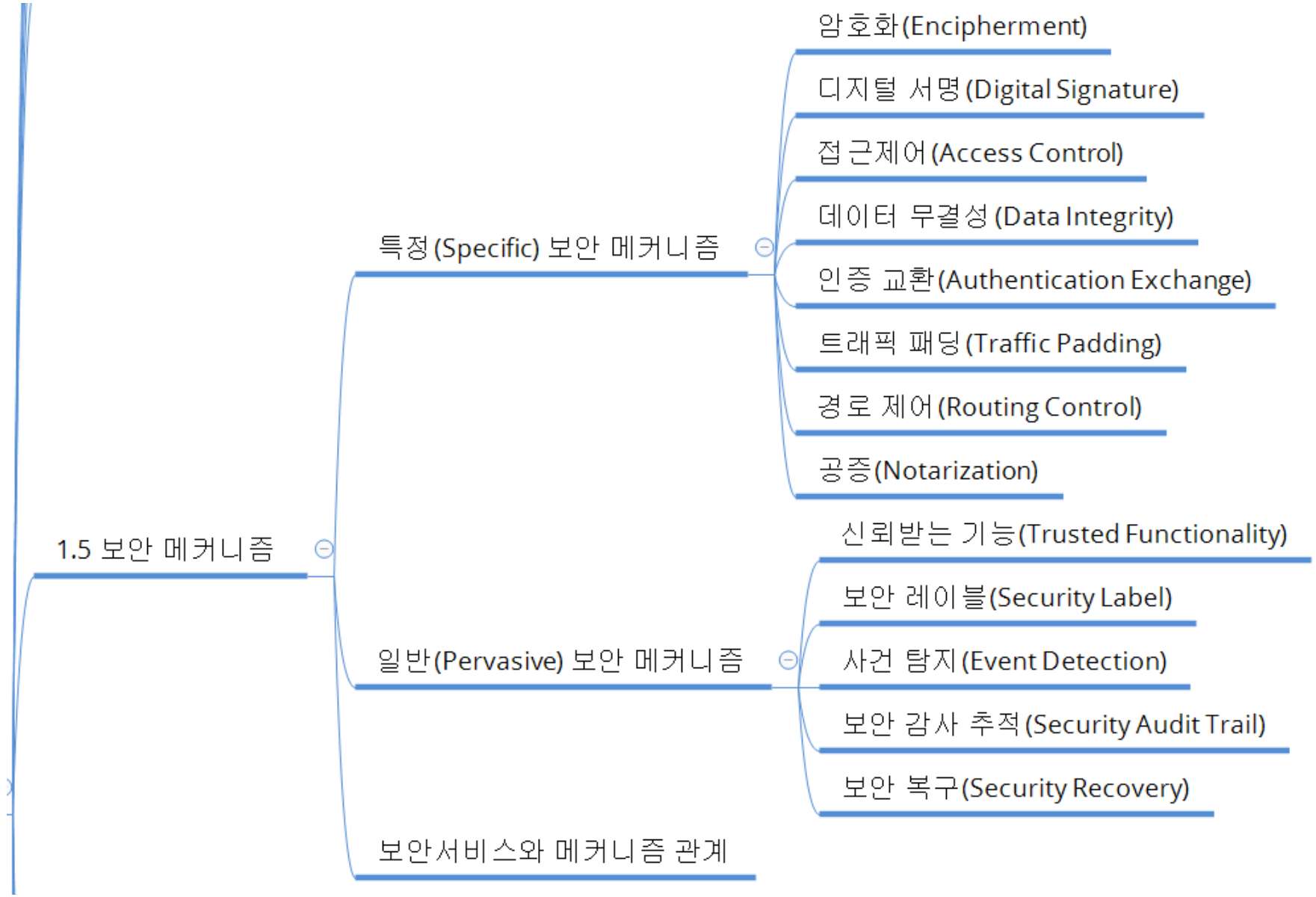
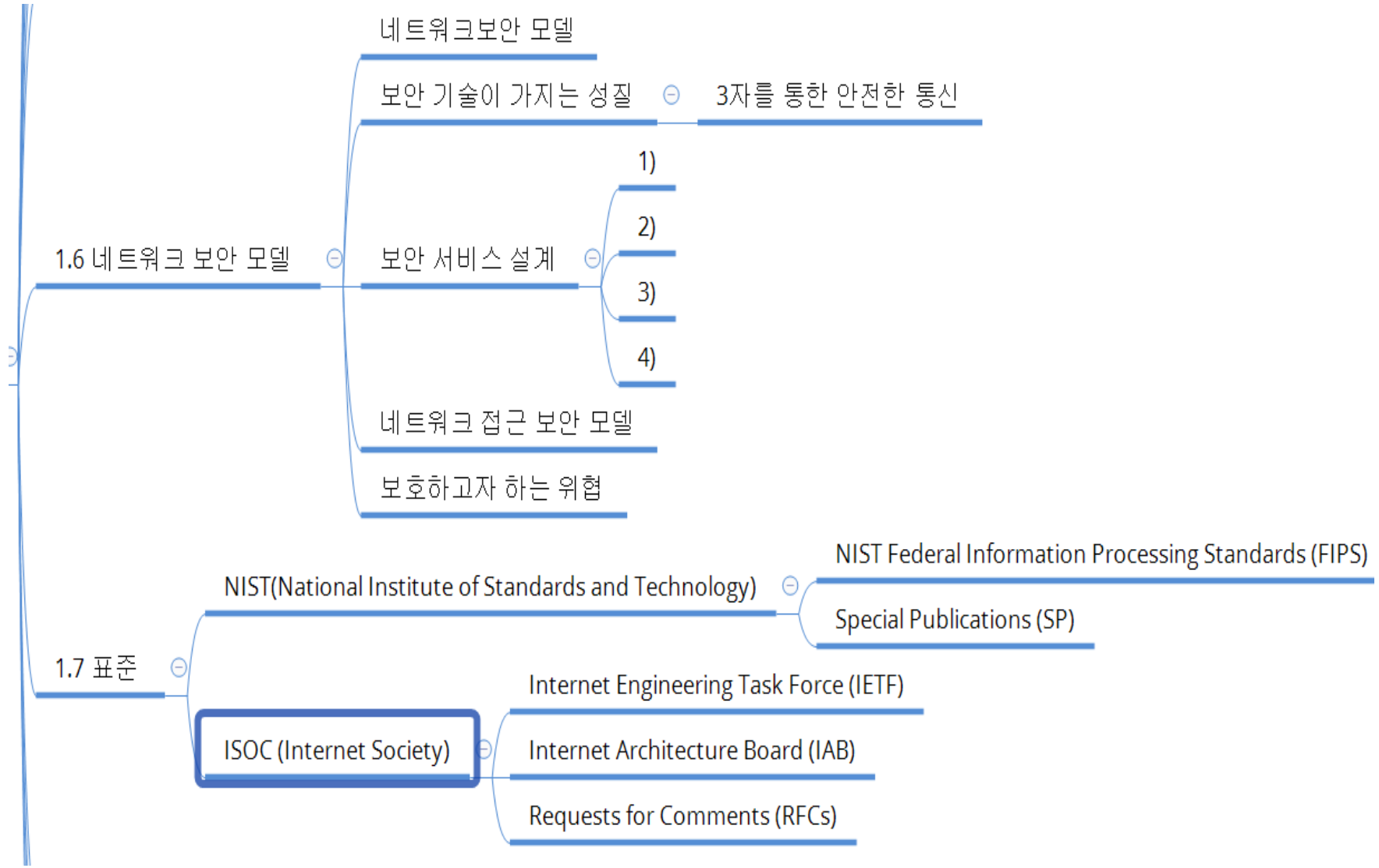

1.1 컴퓨터 보안 개념
컴퓨터 보안 정의
NIST 보안 핸드북의 정의
3가지 주요 목표
기밀성
2가지 의미
데이터 기밀성
프라이버시
무결성
2가지 의미
데이터 무결성
시스템 무결성
가용성
FIPS 199
정보와 정보시스템에 대한 3대 보안 목적
3가지 목적에 대한 유용한 특성
기밀성
무결성
가용성
보안 실무에 필요한 추가 개념
인증 (Authenticity)
책임 (Accountability)
사례
컴퓨터 보안이 어려운 이유


1.2 OSI 보안 구조
X.800 OSI 보안 구조(Security Architecture for OSI)
X.800 핵심
보안 공격
보안 메커니즘
보안 서비스
RFC 2828
위협
공격
1.3 보안 공격
소극적 공격
적극적 공격


1.4 보안 서비스
X.800 정의
RFC 4949의 정의
X.800의 서비스 분류
5가지 분류(category)
14가지 서비스
인증 (Authentication)
대등 개체 인증
데이터출처 인증
접근제어 (Access Control)
2단계
1)
2)
데이터 기밀성 (Data Confidentiality)
하나의 메시지
트래픽 흐름
데이터 무결성 (Data Integrity)
연결형
비연결형
부인봉쇄 (Nonrepudiation)
출처(Origin)
목적지(Destination)
가용성 서비스 (Availability)


1.5 보안 메커니즘
특정(Specific) 보안 메커니즘
암호화(Encipherment)
디지털 서명(Digital Signature)
접근제어(Access Control)
데이터 무결성(Data Integrity)
인증 교환(Authentication Exchange)
트래픽 패딩(Traffic Padding)
경로 제어(Routing Control)
공증(Notarization)
일반(Pervasive) 보안 메커니즘
신뢰받는 기능(Trusted Functionality)
보안 레이블(Security Label)
사건 탐지(Event Detection)
보안 감사 추적(Security Audit Trail)
보안 복구(Security Recovery)
보안서비스와 메커니즘 관계


네트워크보안 모델
보안 기술이 가지는 성질
3자를 통한 안전한 통신
1)
2)
1.6 네트워크 보안 모델
보안 서비스 설계
3)
4)
네트워크 접근 보안 모델
보호하고자 하는 위협
NIST Federal Information Processing Standards (FIPS)
NIST(National Institute of Standards and Technology)
Special Publications (SP)
1.7 표준
Internet Engineering Task Force (IETF)
ISOC (Internet Society)
Internet Architecture Board (IAB)
Requests for Comments (RFCs)