+ 허종오 · 한국 CISSP협회 연구분과 이사, 전자계산기기술사

물리적 보안과 법 규제, 대응 및 수사 도메인

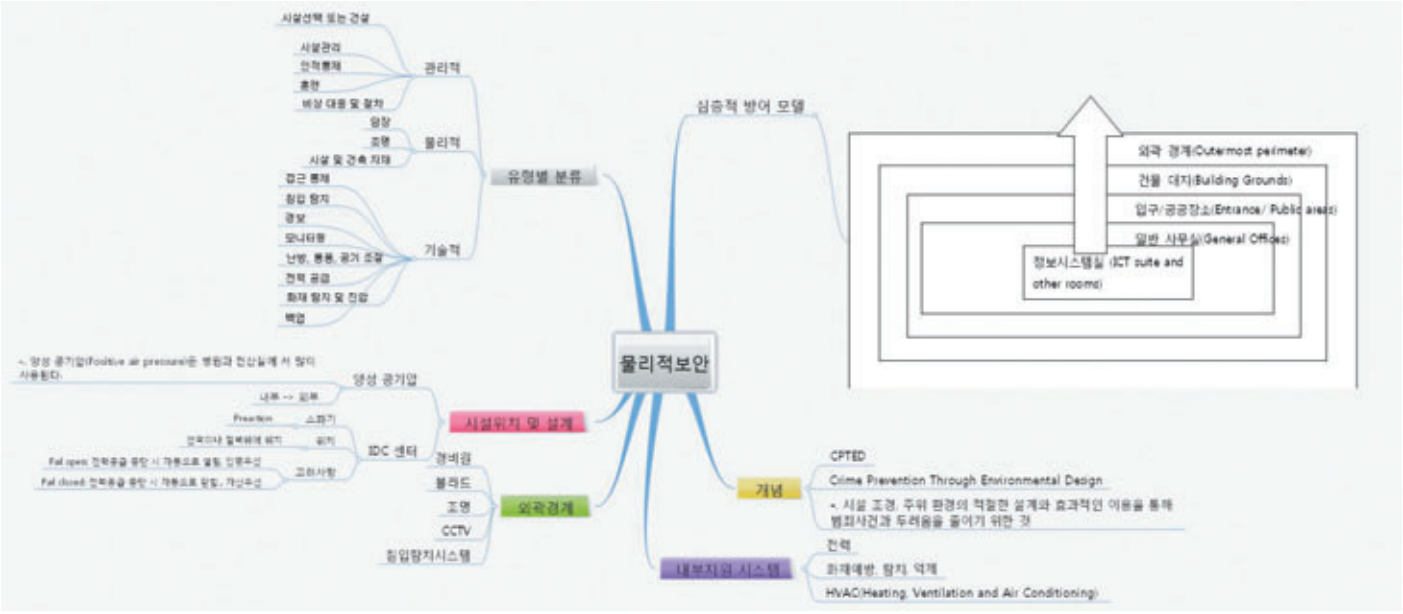
지난 호에서는 비즈니스 연속계획인 BCP와 운영보안 도메인에 대한 요점정리와 연습문제를 통해 CISSP로서의 응용 지식을 학습하였다. 이번 호에서는 CISSP의 10개 도메인 중에서 지금까지 학습한 관리적, 물리적, 기술적 지식들의 기반이 되는 물리적 보안과 법 규제, 대응, 수사에 대해서 알아보고자 한다. 특히, 이번에 학습하는 물리적 보안은 주요 보안 대책을 통해 원천적인 보안위협을 차단할 수 있는 보안 대책이며, 법 규제는 CISSP가 현장에서 자신의 활동에 대한 정당성과 함께 현장 인력들이 보안 정책을 따를 수 있도록 하는 강제성을 가질 수 있는 근거가 되므로 철저한 학습이 필요하다.

1. 물리적 보안(Physical Security) 요점정리

물리적 보안은 자칫 IT 기술 기반의 보안 활동에 초점을 맞추는 최근에 추세로 인해, 간과 될 수 있는 도메인이다. 실제로 보안의 침해는 네트워크 침해나 악성코드 침해도 있으나, 전통적으로 내부자의 정보 유출, 외부자의 불법 침입으로 인해 발생하는 위협이 훨씬 더 큰 피해를 입힌다는 점을 상기하며, 물리적 보안의 중요성은 시대가 변해도 항상 기본적인 보안 지식으로 필요성을 인정받고 있다.

물리적 보안 도메인에서 학습해야 할 요점들은 Domain Map을 통해 한 눈에 알 수 있다.

[그림 1] 물리적 보안의 Domain Map



1-1. 물리적 보안의 정의와 위협

물리적 보안이란 회사의 자원, 데이터 장치, 시스템, 시설 자체의 취약점과 이를 이용한 외부와 내부의 공격으로부터 보호하여 안전한 상태를 유지하는 활동이라고 정의할 수 있다.

[표 1] 물리적 보안의 위협

구 분	내 용
자연 환경적 위협 (Environmental Threat)	– 홍수, 지진, 폭풍, 화재, 고온 – 누수, 습도, 먼지, 시스템 내 지나친 고 · 저온, 전압변동 및 손실을 포함
악의적 위협 (Malicious Threat)	– 물리적 공격, 도난, 비인가 된 접근, 공공시설 파괴, 방화, 도난 등 – Strikes, 폭동, 시민 불복종, 폭탄, 테러 등 – 비인가 된 접근, 파괴, 사기, 절취 등
사고적 위협 (Accidental Threat)	– 승인받지 않은 접근, 직원의 실수 – 단순한 사고, 보안 의무사항의 간과, 시스템 운영 미숙 등

1-2. 물리적 보안의 목표

물리적 보안은 외부와 내부의 위험을 저지, 지연, 탐지, 판단, 대응하는 것을 목표로 하고 있다.

[표 2] 물리적 보안의 목표

기능	설 명	사 례
위험 저지	저지를 통한 범죄/파괴 (Crime and disruption) 방지	담장, 경비요원, 경고사인 등
위험 지연	단계적 방어 메커니즘을 통한 충격 감소	자물쇠, 보안 요원, 장벽, 조명 등
위험 탐지	범죄 또는 파괴 탐지	연기 감지기, 모션 감지기, CCTV 등
위험 판단	사건을 탐지하고 충격레벨을 판단	경비원(사람만이 가능)
위험 대응	위험 발생 시 대응	화재진압 시스템, 비상대응 프로세스, 법적 강제사항 공지 (Law enforcement notification), 외부 보안 전문 컨설팅 등

1-3. 물리적 보안의 통제기법

위험에 대한 물리적 보안의 통제기법은 관리적, 기술적, 물리적 측면에서 대응할 수 있다.

1) 관리적 통제(Administrative controls)

- 시설 선택 또는 건설(Facility selection or construction)
- 시설 관리(Facility management)
- 인적 통제(Personnel controls)
- 훈련(Training)
- 비상 대응 및 절차(Emergency response and procedures)

2) 기술적 통제(Technical/Logical controls)

- 접근 통제(Access controls)
- 침입 탐지(Intrusion detection)
- 경보(alarms)
- 모니터링(CCTV)
- 난방, 통풍, 공기 조절(heating, ventilation and air conditioning, HVAC)
- 전력 공급(Power supply)
- 화재 탐지 및 진압(Fire detection and suppression)
- 백업(backups)

3) 물리적 통제(Physical Controls)

- 담장(Fencing)
- 잠금장치(locks)
- 조명(lighting)
- 시설 및 건축 자재(Facility construction materials)

[그림 2] 계층적 보안 모델

1-4. 주요 시설 위치 및 설계

조직이 보호해야 할 정보와 시스템을 포함하고 있는 주요 시설을 구축할 위치와 설계는 다음과 같은 판단기준을 고려해야 한다.

[표 3] 주요 시설 위치 선정 시 고려사항

구 분	이 슈
가시성 (주변에 튀지 않게)	– 경계선 지역 – 건물 표시 및 간판 – 주변 지역 유형 – 지역 인구 밀도의 높고 낮음
경계선 지역과 외부 존재	– 범죄율, 폭동, 테러리즘 – 경찰, 의료기관, 소방서와의 인접성 – 주위 환경의 가능한 위험
접근성	– 도로 접근, 교통 – 공항, 철도, 고속도로와의 인접
자연 재해	– 홍수, 돌풍, 지진, 태풍의 발생 가능성 – 위험한 지형(지진, 낙석, 과도한 적설 및 강우량)

[표 4] 주요 시설 설계 시 고려사항

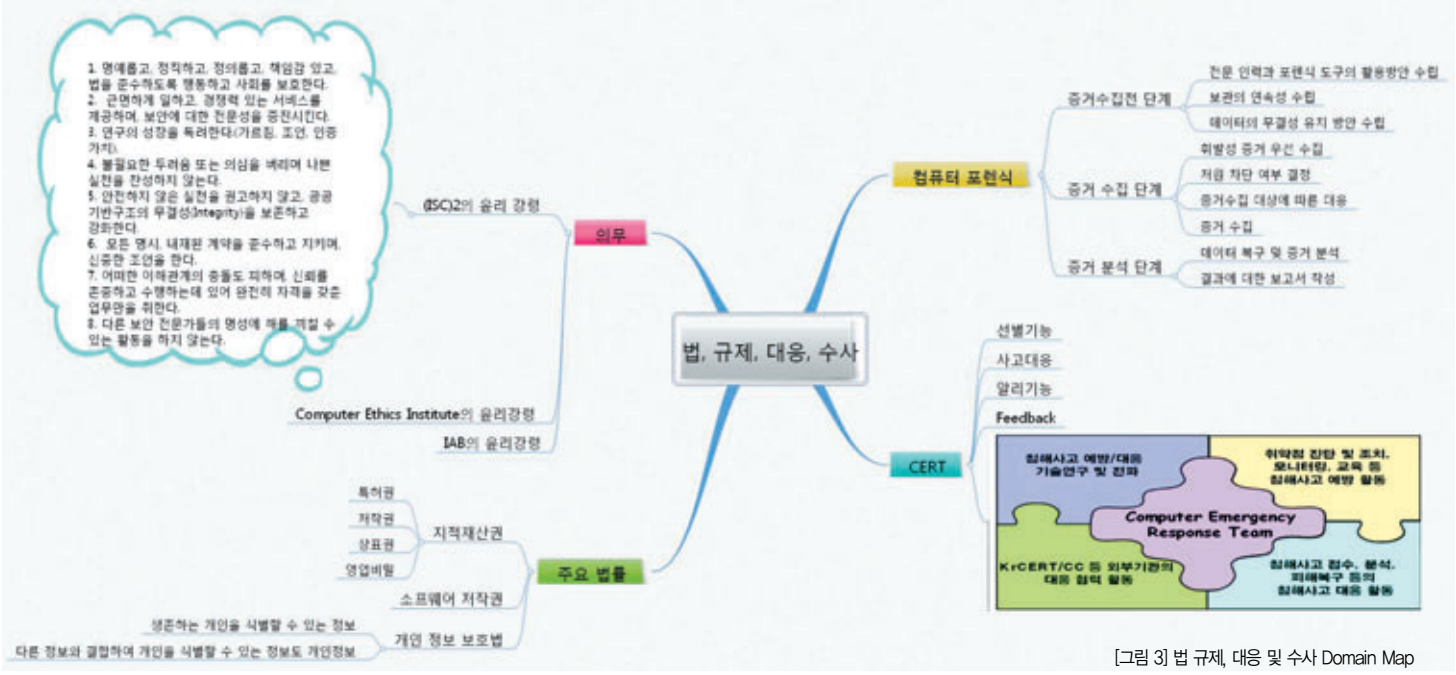
고려 항목	내 용
벽(Walls)	– 자재의 가연성(목재, 철재, 콘크리트) – 화재 등급(Fire rating) – 보호 지역의 보강(Reinforcements for secured areas)
문(Doors)	– 자재의 가연성(목재, 합판, 알루미늄) – 화재 등급 – 강제 진입에 대한 저항력(Resistance to forcible entry) – 비상 표시(Emergency marking)
천장(Ceilings)	– 자재의 가연성(목재, 철재, 콘크리트) – 화재 등급 – 천장 붕괴에 대한 고려 – 하중과 무게 지탱 등급(load and weight bearing rating)
창문(Windows)	– 반투명이거나 불투명 재질 – 비산 방지 – 경보 – 배치 – 침입자에 대한 접근성 – 보안 필름(Secure film): 유리에 추가되는 필름, 강도 강화
바닥(Flooring)	– 하중과 무게 지탱 등급 – 자재의 가연성(목재, 철재, 콘크리트) – 화재 등급 – 부조(raised) 바닥(전기적 접지)
난방, 통풍, 공기 조절 (Heating, ventilation, and air conditioning)	– 양성 공기압(Positive air pressure) – 보호된 공기 흡입구(protected intake vents) – 전용 전기 배선(dedicated power lines) – 비상 차단 밸브와 스위치 – 배치
전원 공급 (Electric power supplies)	– 백업 및 대체 전력 공급(backup and alternate power supplies) – 일정하고 안정적인 전원(clean power source) – 요구지역으로의 전용 송전선(dedicated feeders to required areas)
수도 및 가스 배관 (Water and gas lines)	– 차단 밸브(shutoff valves) – 배치 – 양성 흐름(positive flow): 빌딩 외부로 나가야 하며 역류되어서는 안 됨
화재 탐지와 진압 (Fire detection and suppression)	– 센서와 탐지기의 배치(placement of sensors and detectors) – 분사기(sprinklers)의 배치 – 탐지기와 분사기의 종류

지금까지 물리적 보안의 기본적인 내용을 중심으로 설명하였다. 물리적 보안은 언급한 것 외에 건물의 자재 선정부터 소화기, 전력 선정, 경계방식 선정 등에서 추가적인 학습이 필요하다. 물리적 보안은 수험자 입장에서 많이 경험하지 못한 부분이 많기 때문에 교재 위주로 철저한 학습을 통해 개념을 확실히 익히는 것이 중요한 도메인이다.

분야	Key Factor	출제 비중
물리적 보안	– 제한 지역, 허가 방법과 통제 이해 – 활동 탐지기, 감지기, 경보장치 학습 – 침입탐지, 화재 감지, 예방과 진압방법 이해	낮음

2. 법 규제, 대응 및 수사 (Legal, Regulations, Compliance and Investigation) 요점정리

법 규제, 대응 및 수사는 CISSP가 기본적으로 준수해야 하며, 현업인에게 보안 준수를 요구하기 위해서 필요한 근거를 제공하는 기본적인 도메인이다. 또한, 최근에는 컴퓨터 범죄에 대한 수사를 법적인 증거성을 인정받기 위해서, 컴퓨터 범죄 수사학에 대한 지식도 함께 제공하는 도메인이다. 최근의 사이버 포렌식의 각광으로 중요성이 높아지는 도메인이다. 법 규제, 대응 및 수사 도메인에서 학습해야 할 요점들은 Domain Map을 통해 한 눈에 알 수 있다.



[그림 3] 법 규제, 대응 및 수사 Domain Map

2-1. 주요 법률 체계

법 규제, 대응 및 수사 도메인에서 가장 중요한 내용으로 CISSP가 보안 활동에 대한 근거로 제시해야 할 주요 법률에 대해서 알아보자. 법은 "국가 또는 정치적으로 조직된 사회에서 정립되고, 그 구성원에 대한 물리적 강제력을 배경으로 그 원하는 바를 스스로 실현하는 것을 목적으로 삼는 사회규범"으로 정의한다.

[표 5] 법의 유형(목적에 따라서 공법, 사법, 사회법, 실체법)

구 분	목 적	사 례
공법	공익을 목적으로 국가나 지방 자치 단체를 법관계의 일방당사자로 삼고 있는 법	헌법, 행정에 관한 법령, 형법, 각종 소송법
사법	개인과 개인간의 자유로운 의지에 따른 생활관계를 규율하는 법	민법
사회법	사회, 경제적인 약자를 보호하기 위한 법	노동법
실체법	권리의무의 범위를 설정한 법	민법, 형법
절차법	분쟁해결의 과정을 정한 법	민사소송법, 형사소송법, 행정소송법

[표 6] 법의 유형(구성 형태에 따라서 성문법, 불문법)

구 분	내 용	사 례
성문법	국가 입법기관에서 일정한 절차를 거쳐 제정되는 제정법	헌법, 시행령, 시행규칙, 조약, 조례, 규칙
불문법	제정법의 형태를 취하지 아니하면서 강제 규범력을 지니게 되는 법	관습법, 판례

[표 7] 성문법의 유형

유 형	개 념	사 례
헌법(Constitution)	국가의 통치 조직과 통치 작용의 기본원리 및 국민의 기본권을 보장하는 근본 규범	헌법
민법(Civil Law)	일상 시민과 관련된 법으로 일상적인 사람들 사이의 관계를 규정하고, 죄의 유무가 아닌 책임론에 의거하여 판단	민법, 상법
형법(Criminal Law)	대중을 보호하기 위해 만든 국가 법, 위반 시 징역형(Jail Sentence), 제정법을 따름	형법
행정법 (Administrative Law)	행정기관(정보, 주, 시)에 의해 Rules, Regulations, Procedure 등의 형태로 제정된 법률	행정법 (화재탐지와 화재진압 시스템의 의무화)

※ CISSP는 성문법을 근거로 제시해야 한다.

[표 8] 개인정보의 유형

구 분	정적정보	동적정보
신체 · 의료	혈액형, 성별, DNA, 지문	병력 기록, 성전환 기록 등
인적사항	이름, 주민등록번호, 가족사항	이혼 기록, 주거 기록
통신 · 위치	전화번호, 회원 ID, 이메일 주소	통화 기록, 접속 로그인
교육	학력, 학교성적	상벌 기록

2-2. 윤리의무

CISSP는 기본적으로 강력한 윤리의식을 요구하고 있으며, $(ISC)_2$는 윤리강령을 통해 가이드라인을 제시하고 있다.

1) $(ISC)_2$의 윤리강령

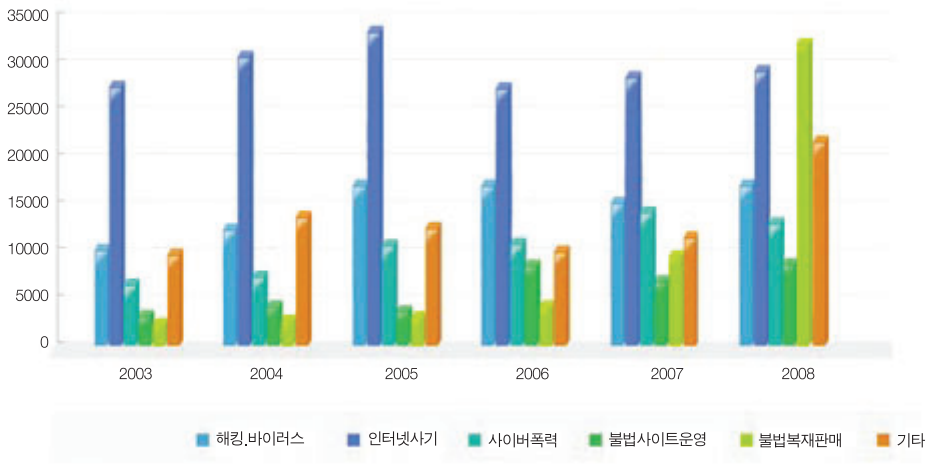
- 명예롭고, 정직하고, 정의롭고, 책임감 있고, 법을 준수하도록 행동하고 사회를 보호한다.
- 근면하게 일하고, 경쟁력 있는 서비스를 제공하며, 보안에 대한 전문성을 증진시킨다.
- 연구의 성장을 독려한다.(가르침, 조언, 인증 가치)
- 불필요한 두려움 또는 의심을 버리며 나쁜 실천을 찬성하지 않는다.
- 안전하지 않은 실천을 권고하지 않고, 공공 기반구조의 무결성을 보존하고 강화한다.
- 모든 명시, 내재된 계약을 준수하고 지키며, 신중한 조언을 한다.
- 다른 보안 전문가들의 명성에 해를 끼칠 수 있는 활동을 하지 않는다.
- 어떠한 이해관계의 충돌도 피하며, 신뢰를 존중하고 수행하는데 있어 완전히 자격을 갖춘 업무만을 취한다.

2-3. 컴퓨터 범죄

최근에는 컴퓨터의 보편화와 네트워크의 고속화로 컴퓨터를 이용하여 불법적으로 정보를 취득하고 이를 이용한 금전적 이득을 취하는 컴퓨터 범죄가 증가하는 추세이다. 특히, 최근의 컴퓨터 범죄는 다음 두 가지의 특징을 가지고 있다.

1) 상업화 : 사이버 공격을 통해 불법적으로 획득한 이용자 및 기업의 정보를 고객에게 서비스로서 제공하는 상업화가 빠르게 진행

2) 조직화 : 독립적으로 운영하거나 개인 해커와 해커 그룹들은 공통적인 목적을 갖고 계층적인 사이버 범죄로 교체



[그림 4] 컴퓨터 범죄 현황(출처: 경찰청 사이버테러 대응 센터)

[표 9] 주요 컴퓨터 범죄

유 형		내 용
단순해킹		PC 해킹, 홈페이지, 카페, 도메인, 서버 해킹
해킹과 결합된 범죄	금융범죄	ID 도용, 피싱, 클릭 사기(Click Fraud)
	자료 및 정보 관련 범죄	분산 서비스 거부공격(DDos), 랜섬웨어
컴퓨터 바이러스 및 악성 프로그램 유포		컴퓨터 바이러스 제작 · 유포, 해킹 프로그램 제작 · 유포, 스팸 제작 · 유포, 스파이웨어 제작 · 유포
기타 비윤리적인 행위		명예훼손, 스토킹, 음란물 유포 및 관련 범죄

[표 10] 컴퓨터 범죄자의 분류

구 분	설 명
Hacker	컴퓨터를 심층탐구하며, 컴퓨터에 대한 자기의 능력과시를 즐기는 사람
Script Kiddies	인터넷에서 다른 사람들이 작성한 스크립트나 프로그램을 사용하여 침투하는 사람
Hack-Activist	정치적 목적으로 자신의 기술을 사용하는 사람으로 법을 어겨도 정치적인 이유로 자신의 행동을 정당화함
Cracker	정보 시스템의 보안 침해자, 제3자를 위해 일하는 해커
Phreaker	전화 시스템에 매혹된 사람으로서 통상 전화 시스템에 대한 지식을 이용하여 자신이 사용하는 전화요금을 다른 사람이 물도록 하는 불법행위자

2-4. 컴퓨터 범죄 수사학

컴퓨터 범죄가 증가함으로써 이에 대한 수사기법에 대한 전문성 확보가 중요하게 되었다. 따라서, 일명 컴퓨터 포렌식으로 불린다.

[표 11] 컴퓨터 포렌식 절차

구 분	분 류	설 명
사용 목적	정보추출 포렌식	디지털 저장매체에 기록되어 있는 데이터를 복구하거나 검색하여 찾아내고, 회계 시스템에서 필요한 계정을 찾아 범행을 입증할 수 있는 수치데이터를 분석하거나 이메일 등의 데이터를 복구 및 검색하는 과정을 통해서 범행 입증에 필요한 증거를 발견 및 확보하는 것
	사고대응 포렌식	해킹과 같은 침해행위로 인해 손상된 시스템의 로그, 백도어, 루트킷 등을 조사하여 침입자의 신원, 피해내용, 침입경로 등을 파악하는 것
수집 대상	휘발성 증거에 대한 포렌식	레지스터(Registers) 및 캐쉬(Cache), 메모리(Memory)의 내용이나 네트워크 연결 상태, 실행 중인 프로그램 상태, Swap 파일 시스템의 내용, 기타 하드디스크에 저장된 파일 및 디렉토리에 대한 시간속성 정보들과 같이 생성 및 접근 과정에서 본래의 정보 및 데이터가 쉽게 변하거나 훼손되는 휘발성 정보 및 데이터에 대해 파악하는 것
	디스크 증거에 대한 포렌식	하드 디스크, 플로피 디스크, 컴팩트 디스크(CD), DVD, USB 메모리 등과 같이 비휘발성 저장매체로부터 디지털 정보 및 데이터를 획득, 분석하는 작업
분석 대상	컴퓨터 포렌식	Windows나 Unix와 같은 운영체제를 탑재한 범용 컴퓨터를 대상으로 하는 디지털 포렌식
	임베디드(모바일) 포렌식	핸드폰과 같은 모바일기기나 디지털 카메라, 캠코더, PDA와 같은 다양한 디바이스에 대한 디지털 포렌식
	네트워크 포렌식	컴퓨터나 핸드폰과 같은 통신 디바이스를 사용해서 통신이 이루어지는 경우에 이런 통신 디바이스에서 네트워크 정보, 사용자 로그, 인터넷 사용 기록 등과 같은 정보를 수집 및 부석하는 포렌식

[표 12] 컴퓨터 포렌식 도구

도 구	설 명	관련 소프트웨어
디스크의 이미징과 복제도구	원본 디스크에 손상이나 변경이 가해지는 것을 방지하기 위해 원본 디스크를 물리적으로 동일한 형태의 다른 디스크로 복제하거나 미러(Mirror) 이미지 파일을 생성하는 도구	SafeBack, SnapBack, DataArrest, Encase, MagicJumbo DD-121, MASSter500
데이터 무결성 도구	증거물이 훼손되지 않았음을 검증해 주는 도구	HashMD5
데이터 복구 및 분석 도구	디스크에서 삭제되거나 손상된 데이터를 분석하고 복구하는 도구	국내: FinalData, DataMedic, LiveData 국외: Encase, FTK(Forensic ToolKit), TCT(The Coronor's Toolkit)
암호 복구 도구 암호를 알아내기 위한 도구	다양한 서버용 시스템이나 문서 파일에 암호가 설정된 경우 Office XP Password Recovery(AOXPPR)	Password Recovery, Passware Kit, Advanced
데이터 조사 도구	많은 문서들이 증거와 관련이 있는지 확인	Quick View Plus, Simmani, Google 등의 검색 도구
증거수집 도구	컴퓨터나 인터넷에서 증거를 수집할 때 사용	Adobe acrobat, Webzip, Hypersnap, SnagIt

지금까지 법 규제, 대응 및 수사에 대해서 알아보았다. 본 도메인은 출제 빈도는 낮지만 CISSP으로써 필히 알아야 할 기본 내용을 제공하므로, 기본 지식으로 학습이 필요하다. 다만, 최근에 시나리오 문제에서 윤리강령을 기반으로 CISSP의 판단을 묻는 문제를 물어보고 있으니, 이 부분에 대한 준비가 필요하다.

분 야	Key Factor	출제 비중
법 규제, 대응 및 수사	– 법, 규정, 그리고 범죄 숙지 – 라이센싱과 소프트웨어 저작권 침해 숙지 – 수출입법과 논점 학습 – 증거 유형과 법정에서의 용인 가능성 학습 – 사건 처리 프로세스 이해	낮음

지금까지 6개월간 CISSP가 되기 위해 학습해야 할 지식을 10가지 도메인으로 구분하여 살펴보았다. 많은 지식을 담기에는 지면상 모자란 점이 있었으나, CISSP를 준비할 때 필요한 주요 지식과 최근의 시험 경향 등을 바탕으로 학습 방향을 제시하기 위한 본래의 취지는 충분히 제공되었다고 생각한다. 그러므로, CISSP에 관심이 있거나 준비하고 있는 예비 보안 전문가들에게는 입문서의 역할을 할 것으로 보인다.

최근의 보안 시장은 클라우드 컴퓨팅과 스마트 보안 등 빠른 추세로 변화고 있으나, CISSP의 기본 지식을 제대로 가지고 있다면, 급변하는 변화에도 능동적으로 대처할 수 있을 충분한 지식이 될 것으로 보인다. 따라서, 기본부터 확실히 하는 준비를 통해 보안 전문가로서의 전문성을 확보해나가는 방향을 제시하면서, 6개월간의 연재를 마친다.

3. 연습 문제

간단한 문제를 통해서 이번 호에서 배운 도메인에 대한 이해능력을 키우자. 중요한 것은 실제 시험에서는 이보다 어려운 문제가 출제되나, 기본을 알면 충분히 풀 수 있는 문제이다. 문제를 풀고 잘못 이해하는 부분은 요점정리를 통해 재학습이 필요하다.

▣ 물리적 보안

1. 주변 불빛의 밝기가 불안정한 지역에 CCTV를 설치할 때 추가적으로 고려해야 할 것은 무엇인가?

① Manual Focus Lens　② Auto Focus(Iris) Lens
③ 전압안정화 장치　④ CCTV의 설치높이

2. 소음이 많은 환경에서 유리창을 통해 침투하는 침입자를 방지/탐지할 목적으로 사용될 수 있는 감시 장치는 무엇인가?

① 조명　② Lock
③ Pressure Pad　④ Motion Detector Sensor

3. 하드디스크의 완전한 정보 삭제기법은 무엇인가?

① Overwrite　② Degauging
③ Imaging　④ Destruction

4. 통제된 구역을 출입할 때 전자배지를 착용하는 이유는 무엇인가?

① 직원들의 출입기록을 남기기 위해
② 들어오는 인원과 나가는 인원의 동일여부를 확인하기 위해
③ 허가되지 않은 사람의 접근을 통제하기 위해서
④ 특정 서버의 접근권한을 얻기 위해서

5. HVAC이 작동 시 창문개방 후 내부공기는 양여압(Positive Pressurization)이다. 이때 창문을 열었을 경우 공기는 어떻게 되어야 하는가?

① 공기가 내부에서 외부로 나간다.

② 공기가 외부에서 내부로 들어온다.

③ 공기가 순환한다.

④ 공기의 흐름이 어떻게 되어도 상관없다.

▣ 법 규제, 대응 및 수사

1. 기업 내부의 중요한 데이터의 유출로 인해 컴퓨터 포렌식을 의뢰 받았을 때 현장에 도착한 사이버수사관이 가장 먼저 취해야 할 행동은 무엇인가?

① 접근통제를 위한 가드라인을 설치한다.

② 증거물의 보존을 위해 비디오카메라나 사진촬영을 한다.

③ 추가적인 데이터유출을 막기 위해 네트워크 케이블을 뽑는다.

④ 시스템을 안전하게 종료시킨다.

2. 사이버수사를 진행할 때 디스크 이미징 작업을 하는 이유는 무엇인가?

① 전체 디스크를 비트레벨로 복사하여 모든 물리적 섹터를 저장하기 위해

② 법원에서 규정한 정책에 의해서

③ 백업속도가 빨라서 작업시간을 단축할 수 있어서

④ 수사기간 중 운영의 연속성을 보장하기 위해서

3. 회사가 법률과 관련해서 정책을 규정하려고 할 때 CISSP가 지원해야 할 사항은 무엇인가?

① CISSP는 법률부서와 상담하여 법률을 해석한다.

② 경영진이 보안관리자와 법률을 해석하도록 한다.

③ 직접 법을 읽고 해석한다.

④ 법률이 공표될 때까지 기다린다.

4. 개인정보보호법에 명시되어 있는 개인정보는 해당 목적에만 사용되어야 한다. 여기서 해당목적에 포함되는 것은 무엇인가?

① 목적의 명확성 ② 이용의 제한 ③ 안전보호원칙 ④ 책임의 원칙

5. 한 기업이 수년간의 연구 끝에 독창적인 제품을 제작하였을 때 아이디어 자체를 보호하기 위한 것은 어떤 것인가?

① 특허권 ② 라이센스 ③ 저작권 ④ 영업비밀

정답 : ②, ④, ④, ③, ①, ②, ①, ①, ②, ④