1주차 3차시 보안법규

【학습목표】

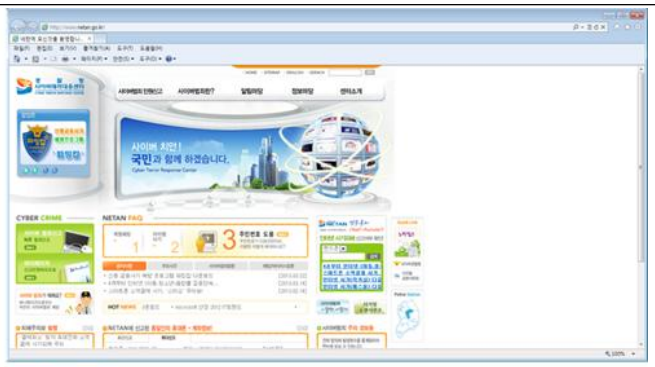
1. 보안전문가의 자격요건에 대해 설명할 수 있다.
2. 보안법의 개요를 파악할 수 있으며, 종류를 나열할 수 있다.

학습내용1 : 보안 전문가의 자격 요건

1. 사이버 범죄

1) 경찰청 사이버테러대응센터(http://www.netan.go.kr)에서는 해마다 국내의 보안 사고에 대한 통계를 발표함.

2) 사이버테러형 범죄가 약 15,000건, 일반 사이버 범죄가 약 100,000건에 이름



[그림 1-25] 경찰청 사이버테러 대응센터 사이트

3) 사이버 범죄의 유형

구분	내용
사이버 테러형 범죄	정보통신망 자체를 공격 대상으로 하는 불법 행위로서 해킹, 바이러스 유포, 메일 폭탄, 서비스 거부(DoS) 공격 등 전자기적 침해 장비를 이용해 컴퓨터 시스템과 정보통신망을 공격하는 행위
일반 사이버 범죄	사이버 공간을 이용한 일반적인 불법 행위로서 사이버 도박, 사이버 스토킹과 성폭력, 사이버 명예 훼손과 협박, 전자상거래 사기, 개인정보 유출 등의 행위

2. 윤리 의식

1) 정보통신윤리위원회(현 방송통신위원회)에서 2007년 6월 25일에 발표한 정보통신 윤리 강령을 살펴보자.

정보통신 윤리 강령

우리는 정보통신 기술의 발달로 시간과 공간을 넘어서 세계가 하나된 시대에 살고 있다. 정보통신 기술은 우리의 생활을 편리하게 하고 창조적 지식정보의 창출을 도와 새로운 가능성과 밝은 미래를 열어주고 있다.

우리는 그 동안 다 함께 뜻을 모으고 힘을 기울여 정보통신 강국으로 우뚝 서게 되었다. 하지만 그 위상에 걸맞지 않게 우리 사회는 불건전 정보 유통, 사이버 명예 훼손, 개인정보 침해, 인터넷 중독 등 정보 역기능 현상이 나타나고 있다. 최고의 정보통신 인프라와 함께 건전한 정보이용 문화가 확립될 때에 비로소 세계를 선도하는 진정한 정보통신 강국이 될 것이다.

우리 모두는 지식정보사회의 주인으로서 인류의 행복과 높은 이상이 실현되는 사회를 만들어 나가야 할 사명이 있다.

우리는 정보를 제공하고 이용할 때에 서로의 인권을 존중하고 법과 질서를 준수함으로써 타인에 대한 배려가 넘치는 따뜻한 디지털 공동체를 만들어 나가야 한다. 또한 개인의 사생활과 지적 재산권은 보호하고 유용한 정보는 함께 가꾸고 나누는 건전한 정보이용 문화를 확산해 나가야 한다.

우리는 궁극적으로 모두의 행복과 자유, 평등을 추구하며 인류가 정보통신 기술의 혜택을 고루 누릴 수 있도록 정보통신윤리를 지켜나가야 한다는 데 뜻을 모으고 이 뜻이 실현되도록 성실하게 노력할 것을 다짐한다.

- 우리는 타인의 자유와 권리를 존중한다.
- 우리는 바른 언어를 사용하고 예절을 지킨다.
- 우리는 건전하고 유익한 정보를 제공하고 올바르게 이용한다.
- 우리는 청소년 성장과 발전에 도움이 되도록 노력한다.
- 우리 모두는 따뜻한 디지털 세상을 만들기 위하여 서로 협력한다.

2) 컴퓨터윤리기관(Computer Ethics Institute)에서 발표한 윤리 강령 10계명

- 컴퓨터를 타인을 해치는 데 사용하지 않는다.
- 타인의 컴퓨터 작업을 방해하지 않는다.
- 타인의 컴퓨터 파일을 염탐하지 않는다.
- 컴퓨터를 절도해서 사용하지 않는다.
- 거짓 증거로 컴퓨터를 사용하지 않는다.
- 소유권 없는 소프트웨어를 사용하거나 불법 복제하지 않는다.
- 승인이나 적절한 보상 없이 타인의 컴퓨터를 사용하지 않는다.
- 타인의 지적 재산권을 침해하지 않는다.
- 자신이 만든 프로그램이나 시스템으로 인한 사회적 결과에 책임을 진다.
- 동료를 고려하고 존중하는 방식으로 컴퓨터를 사용한다.

2) 인터넷활동협회 (IAB: Internet Activities Board) 에서 비윤리적으로 간주하는 행동
- 고의적으로 허가 받지 않고 인터넷 자원에 접근하려는 행위
- 인터넷의 이용을 막는 행위
- 의도적으로 시스템과 네트워크의 자원을 낭비하는 행위
- 컴퓨터 기반 정보의 무결성을 파괴하는 행위
- 타인의 사생활을 침해하는 행위
- 인터넷 전반의 실험에 있어서의 과실

3. 다양한 분야에 대한 전문성

1) 운영체제
- 네트워크와 병행한 운영체제(Operating System)에 대한 이해가 필요함.
- 실무적으로 가장 중요한 운영체제는 윈도우, 서버의 경우에는 유닉스 서버임.
- 최근에는 리눅스가 매우 다양한 형태로 발전하고 있음.

2) 네트워크
- TCP/IP는 1973년대에 만들어져 지금까지 네트워크의 기본이 되는 프로토콜임.
- 따라서 매우 중요하기 때문에 동작 하나하나까지 이해해야 함.

3) 프로그래밍
- 대체로 기본적인 C 프로그래밍과 객체지향 프로그래밍에 대한 이해, HTML 정도면 충분함.
- 하지만 수준 높은 보안 전문가가 되려면 프로그래밍 능력이 상당히 중요함.

① 보안 시스템 개발자 : 방화벽, 침임 탐지 시스템(IDS) 등의 보안 시스템 개발자는 프로그래밍을 깊이 배워야 함.
② 응용 프로그램 취약점 분석 테스터 : 리버스 엔지니어링(Reverse Engineering)을 이용한 게임과 상용 프로그램 테스터/취약점 분석가는 프로그래밍에 대해 자세히 알아야 하고, 특히 어셈블리어에 대한 깊은 이해가 필요.

4) 서버
- 보안 전문가는 서버를 이해하는 것이 필수적.
- 데이터베이스의 경우 기본적인 SQL 역시 공부가 필요함.

5) 보안 시스템
- 방화벽, 침입 탐지 시스템, 침입 방지 시스템, 단일 사용자 승인(SSO), 네트워크 접근 제어 시스템(NAC), 백신과 같은 보안 솔루션의 경우 각 시스템별 기본 보안 통제와 적용 원리, 네트워크상에서 구성, 목적 등을 이해해야 함

6) 모니터링 시스템
- 네트워크 관리 시스템(NMS), 네트워크 트래픽 모니터링 시스템(MRTG)과 같은 모니터링 시스템에 대한 기본적인 개념 정도는 필요함

7) 암호
- 암호와 해시의 차이
- 대칭키 알고리즘과 비대칭키 알고리즘의 종류와 강도
- 공개키 기반 구조에 대한 이해 필요

8) 정책과 절차
- 큰 조직의 보안 전문가일수록 보안 정책(Security Policy)과 해당 기업의 핵심적인 업무 프로세스에 대한 이해 필요.
- 보안 정책에서 가장 핵심적인 요소인 보안 거버넌스(Security Governance)에 대한 이해 필요.
- 보안 거버넌스란 '조직의 보안을 달성하기 위한 구성원들 간의 지배 구조'이다.
- 최근 발생한 대규모 보안 사고의 원인이 대부분 이러한 지배 구조의 부재 때문임.

학습내용2 : 보안 관련 법

1. 개념

1) 세계의 70% 이상의 해커가 학생이라고 한다.
- 해킹을 영리가 목적이 아닌 일종의 호기심에 수행하는 경우가 많음을 의미하지만, 역시 범죄로서 똑같이 처벌받는다.

[그림 1-26] 잘못된 길을 걷는 해커의 종말

2) 경찰청 사이버테러대응센터 홈페이지(www.netan.go.kr)에서 보안 관련 법률의 주요 내용을 살펴볼 수 있다.

2. 정보통신망 이용촉진 및 정보보호에 관한 법률

1) 안전한 정보통신망 환경을 조성하는 것이 목적, 정보통신과 관련된 가장 광범위한 법률임

2) 정보통신 서비스 사업자와 관련된 내용, 개인정보보호와 관련된 내용 등을 범죄로 규정함

3) 이를 어길 시에 3년~7년의 징역 또는 2천만 원~5천만 원의 벌금에 처함

4) '정보통신망 이용촉진 및 정보보호 등에 관한 법률'의 주요 범죄 사항

순번	적용 법조	범죄 내용
1	제70조 제1항	사이버 명예 훼손(사실 유포)
2	제70조 제2항	사이버 명예 훼손(허위사실 유포)
3	제71조 제1호	이용자 개인정보 수집
4	제71조 제3호	개인정보 목적 외 이용 및 제3자 제공

순번	적용 법조	범죄 내용
5	제71조 제5호	이용자 개인정보 훼손 · 침해 · 누설
6	제71조 제9호	악성프로그램(바이러스) 유호
7	제71조 제10호	정보통신망 장애 발생
8	제71조 제11호	타인 정보 훼손 및 타인 비밀 침해 · 도용 · 누설

순번	적용 법조	범죄 내용
9	제72조 제1항 제1호	정보통신망 침입
10	제72조 제1항 제5호	직무상 비밀 누설 및 목적 외 사용
11	제72조 제1항 제2호	속이는 행위에 의한 개인정보 수집
12	제73조 제1호	정보통신 서비스 제공자 등의 기술적 · 관리적 조치 미이행

순번	적용 법조	범죄 내용
13	제73조 제2호	영리목적 청소년유해매체물 미표시
14	제73조 제3호	청소년유해매체물 광고 청소년에게 전송
15	제74조 제1항 제1호	인증기관 인증표시 무단 표시 · 판매 · 진열
16	제74조 제1항 제2호	음란 문언/음향/영상 등의 배포 · 판매 · 전시

순번	적용 법조	범죄 내용
17	제74조 제1항 제3호	사이버 스토킹(공포불안을 야기시키는 말 · 음향 등의 반복 행위)
18	제74조 제1항 제4호	스팸메일 수신거부 회피 관련 기술조치 행위

순번	적용 법조	범죄 내용
19	제74조 제1항 제5호	전자우편주소 무단 수집 · 판매 · 유통 · 정보 전송에 이용
20	제74조 제1항 제6호	불법행위를 위한 광고성 정보 전송

3. 정보통신 기반 보호법

1) ISP(Internet Service Provider)나 주요 통신사와 같은 주요 정보통신 기반 시설에 대한 보호법

2) 다음과 같은 사항을 전자적 침해행위로 규정하고 있음

3) 주요 정보통신 기반 시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억 원 이하의 벌금에 처함

4) '정보통신 기반 보호법'의 주요 범죄 사항

순번	적용 법조	범죄 내용
1	제 28조	주요 정보통신 기반 시설 교란 · 마비 · 파괴
2	제 29조	취약점 분석 · 평가업무 등의 종사자 비밀 누설

4. 개인정보 보호법

1) '정보통신망 이용 촉진 및 정보보호 등에 관한 법률', '신용정보의 이용 및 보호에 관한 법률' 등의 개별 법령에서 다루고 있는 개인정보와 관련된 사항을 통합하여 규정한 법

2) 2012년에 시행되었으며, 각 규정에 따라 3년~10년의 징역 또는 3천만 원~1억 원의 벌금에 처하고 있음.

3) '정보통신망 이용촉진 및 정보보호 등에 관한 법률'의 주요 범죄 사항

순번	적용 법조	범죄 내용
1	제22조	동의 없는 개인정보 수집
2	제23조	민감한 개인정보 수집 및 필요 최소한의 개인 정보 이외의 정보를 제공하지 아니했다는 이유로 서비스 제공 거부
3	제31조	법정대리인의 동의 없는 아동 개인정보 수집
4	제24조	동의 받은 목적과 다른 목적으로 개인정보 이용
5	제23조의 2	주민등록번호 외의 회원가입 방법 미조치

순번	적용 법조	범죄 내용
6	제24조의 2	이용자 동의 없는 개인정보 제3자 제공
7	제25조	이용자 동의 없는 개인정보 취급 위탁 및 개인정보 취급 위탁 사실 미공개
8	제26조 제1항	영업양도 등 미통지
9	제26조 제3항	영업양수자 등이 당초 목적과 다른 목적으로 개인정보 이용 또는 제3자 제공

순번	적용 법조	범죄 내용
10	제27조	개인정보 관리 책임자 미지정
11	제27조의 2	개인정보 취급 방침 미공개
12	제28조 제1항 제1호, 제6호	기술적·관리적 조치 미이행
13	제28조 제1항 제2호~제5호	기술적·관리적 조치 미이행으로 인한 개인정보 누출

순번	적용 법조	범죄 내용
14	제28조의	개인정보 취급자의 개인정보 훼손, 침해, 누설
15	제29조	개인정보 미파기
16	제30조	이용자의 동의 철회, 열람, 정정 요구 미조치

순번	적용 법조	범죄 내용
17	제30조 제5항	개인정보 오류 정정 요청에 대한 필요 조치를 하지 아니하고 개인정보 제3자 제공, 이용
18	제30조 제6항	이용자의 동의 철회, 열람, 정정 요구를 개인정보 수집 방법보다 어렵게 함

5. 통신비밀 보호법

1) 통신비밀을 보호하고 통신의 자유를 신장하기 위해 1993년에 처음 제정됨.

2) 다음의 범죄 사실에 대해 10년 이하의 징역과 5년 이하의 자격 정지에 처하고 있음.

3) '통신비밀 보호법'의 주요 범죄 사항

순번	적용 법조	범죄 내용
1	제 16조 제1항 제1호	전기통신 감청 및 비공개 타인 간 대화녹음 · 청취
2	제16조 제1항 제2호	지득한 통신 및 대화내용 공개 · 누설
3	제16조 제2항 제2호	통신제한조치 집행 등 관여 공무원의 비밀 공개 누설

순번	적용 법조	범죄 내용
4	제16조 제3항	통신제한조치 집행 등 관여 통신기관 직원 비밀 공개 누설
5	제16조 제4항	사인의 통신제한조치 취득내용의 외부 공개 및 누설

6. 저작권법

1) 저작자의 권리와 이에 인접하는 권리를 보호하고 저작물의 공정한 이용을 위한 목적으로 2006년 제정됨

2) 범죄 사실에 따라 3년~5년의 징역 또는 3천만 원~5천만 원의 벌금에 처하고 있음

3) '통신비밀 보호법'의 주요 범죄 사항

순번	적용 법조	범죄 내용
1	제136조 제1항	저작재산권 등 재산적 권리의 복제 · 전송 · 배포 등
2	제136조 제2항 제1호	저작인격권을 침해하여 저작자 명예 훼손
3	제136조 제2항 제3호	데이터베이스 제작자 권리를 복제 · 배포 · 전송으로 침해

순번	적용 법조	범죄 내용
4	제136조 제2항 제5 · 6호	기술적 보호조치 제거 · 변경 등과 같은 침해 행위
5	제 137조 제6호	허위 저작권 주장 , 복제 · 전송 중단 요구로 ISP 업무방해

【학습정리】

1. 보안분야에 전문가가 되기 위한 소양으로는 운영체제, 네트워크, 프로그래밍, 서버, 보안시스템, 모니터링, 암호, 정책과 절차 등의 소양이 요구된다.

2. 세계의 70% 이상의 해커가 학생이라고 한다. 해킹을 영리가 목적이 아닌 일종의 호기심에 수행하는 경우가 많음을 의미하지만, 역시 범죄로서 똑같이 처벌받는다.

3. 보안관련 법으로는 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신 기반 보호법, 개인정보 보호법, 통신비밀 보호법, 저작권법 등이 있다.