2018 JUNE 21

정보처리기사 실기

시스템 관리와 보안

KIM SEOKRAE

내용

1. 시스템 관리와 보안

1) A

ActiveX	마이크로소프트사에서 개발한 응용 소프트웨어들이 인터넷 환경 하에서도 수행될 수 있도록 해주는 플랫폼 통합 기술을 말한다. 오피스 파일과 같은 일반 문서뿐만 아니라 애니메이션, 3차원 가상현실 등을 실시간으로 인터넷 환경하에서 볼 수 있게 해준다.
AE (Authentication Exchange, 인증 교환)	사용자의 신분에 대하여 인증 과정을 수행하기 위하여 인증 정보를 교환하는 것을 말한다. 이를 위하여 암호 방식이나 MAC(메시지 인증 코드)를 많이 사용한다. 만일 MAC를 사용하면 메시지 전송 도중에 수신자가 변경되는지를 확인할 수 있다. 아울러 메시지가 순서 번호(Sequence Number)를 갖고 있다면 올바른 순서로 메시지가 도착하는지도 확인할 수 있다.
AMR (Automatic Meter Reading, 원격 검침)	가정이나 기업이 사용한 전기, 수도, 가스 등의 사용량을 일일이 방문하여 조사하지 않고 원격에서 검침 데이터를 읽을 수 있도록 한 시스템이다. 원격 검침 작업은 물론 수요자의 소비 패턴 분석은 물론 요금 고지서 발급도 자동으로 지원해준다.
Anti-Debugging	디버깅을 통하여 프로그램의 기능을 역추적하거나 이를 토대로 변조하는 것을 막는 기술을 뜻한다. 즉, 역공학(Reverse Engineering)에 의한 소프트웨어 저작권 침해를 예방하기 위하여 디버깅 작업을 하지 못하게 하는 기술이다.
APT (Advanced Persistent Threat, 지능형 타깃 지속 공격)	기존의 여러 가지 IT 기술과 해킹 방법들을 종합적으로 활용하여 다양한 종류의 보안 위협들을 지속적으로 만듦으로써 특정한 대상을 계속하여 공격하는 행위이다. APT 공격은 다음 순서로 이루어진다.
Attack Tool Kit	인터넷에 연결된 컴퓨터들을 공격하고자 악성코드와 해킹 도구들을 모아 놓은 것을 말한다.
Authentication (인증)	다수의 사용자를 지원하는 컴퓨터 시스템에서 특정 사용자가 자원을 접근하기 위하여 사용자 정보를 확인하는 일련의 보안 절차를 말한다. 사용자(주체)가 시스템 자원(객체)을 접근할 때 받게 되는 사용자 인증은 ① 식별(Identification), ② 인증(Authentication), ③ 허가(Authorization)의 과정으로 진행된다. 사용자 로그인 이름을 제시하는 것은 식별(Identification),

	사용자의 암호를 제시하는 것은 인증(Authentication), 사용자에 따라 적절한 접근권한을 부여하는 것이 허가(Authorization)이다.

2) B

Backup **(백업)**	데이터를 보호할 목적으로 일정한 시간이나 주기마다 데이터를 다른 안전한 장소에 복제하여 보관하는 행위이다. 백업방법에 따라 차등백업(Differential Backup)과 증분백업(Incremental Backup)으로 구분한다.
BCP **(Business Continuity Planning,** **업무 영속성 계획)**	조직의 내부적 혹은 외부적 위협이나 재해, 재난으로부터 조직의 자산과 기능을 효과적으로 보호하며 사고와 재단이 발생했을 때 신속히 복구할 수 있도록 함으로써 조직 기능과 업무가 중단됨 없이 지속될 수 있도록 세우는 제반 계획을 말한다.
Big Data **(빅 데이터)**	데이터가 생기는 양이나 형식, 주기 등이 기존 데이터에 비하여 방대하므로 기존 방식으로 처리하기 힘든 방대한 데이터를 말한다. 이들이 나타내는 의미를 잘 분석하면 사람들의 생활방식과 미래 행동양식을 예측할 수 있어서 큰 가치를 지니고 있다. 빅 데이터를 활용할 때 개인정보보호를 위하여 다음과 같은 “개인정보 비식별화 조처”를 취해야 한다.
Biometrics **(생체인식)**	모든 인간은 고유의 생체정보를 가지고 있어서 이를 인증수단으로 사용하여 본인을 확인할 수 있도록 한 기술을 말한다. 대표적으로 손가락 피부 밑 진피에서 만들어진 지문을 인식하는 경우, 손등이나 손목의 정맥 혈관을 적외선을 이용하여 인식하는 경우, 목소리를 인식하는 경우, 손금을 인식하는 경우 등이 있으며 이들 중 여러 개를 함께 사용하는 경우도 있다. 현재로서 가장 보편적인 것은 지문인식이다.
Blockchain **(블록체인)**	온라인 금융 거래 사용자들의 사용 정보를 하나의 블록을 만든 다음에 이전 블록과 연결하여 사용자들의 컴퓨터와 스마트폰 사이에 분산 저장하여 공동 관리하는 P2P 방식이다. 중앙 서버를 이용하지 않아서 관리 비용이 절감되며 해킹 등의 위험으로부터 더 안전하다. 이를 이용한 대표적인 사례가 비트코인(Bitcoin)이다.
Bohonara **(보호나라)**	한국인터넷진흥원(KISA)이 운영하는 정보보호 포털 사이트 명칭을 말한다. 웹 사이트 주소는 www.boho.or.kr이며,

	보안 관련 도구를 제공하고 여러 침해사고를 신고할 수 있다.
Botnet	악의적인 목적을 가지고 독립적으로 설치되어 행동하는 봇(Software Robot의 약자)들이 다수 모여서 서로 통신하는 네트워크를 이르는 말이다. 2009년 7 · 7대란을 일으켰던 DDoS 공격은 CNC의 지시를 받아 봇넷들이 특정 사이트를 공격함으로써 벌어졌다.
BPR **(Business Process Reengineering, 업무 재설계)**	기업 경영 전반을 분석하여 경영 목표 달성에 적합하도록 다시 설계한 후 이에 따라 기업 형태, 조직, 사업 분야, 사업 내용 등을 다시 구성하는 것이다. 기업 전체를 대상으로 한다는 점에서 기존의 업무 개선과 다르다. BPR을 지원하는 기술 요소로는 ① 그룹웨어, ② 컴퓨터 지원 공동 작업(CSCW), ③ 전략 정보 시스템(SIS)을 꼽을 수 있다.
Breadcrumbs **(브레드 크럼즈)**	동화 〈헨젤과 그레텔〉에서 자신들의 자취를 남기 위하여 길에 떨어뜨린 빵부스러기를 가리키는 말로서, 사용자가 컴퓨터와 인터넷상에서 탐색했던 복잡한 경로들을 시각적이며 체계적으로 보여 줌으로써 사용자의 위치를 손쉽게 파악하게 해주는 일종의 그래픽 인터페이스이다.
Brute Force Attack **(무차별 공격)**	목표 시스템을 공격하기 위하여 다양하고 방대한 값들을 꾸준히 입력하면서 시스템의 반응상태를 추적하는 공격으로 시간 낭비가 많을 수 있다.
BS 7799	정보 보안 경영 시스템에 대한 개발과 수립 및 문서화에 대한 요구 사항들을 안내한 국제 인증 규격이다. 1995년 영국 표준으로 제정된 것으로 1999년 개정을 거쳐 국제표준화기구(ISO)에 의해 국제 표준(ISO 17799)으로도 제정되었다.
Buffer Overflow Attack **(버퍼 오버플로우 공격)**	메모리에 할당된 버퍼의 크기를 초과하도록 고의로 데이터를 계속 입력하여 결국은 프로그램의 복귀주소 위치까지 이르도록 데이터를 계속 덮어쓴다. 이 때 복귀주소를 덮어 쓴 데이터는 본격적인 악성코드가 저장되어 있는 메모리 주소 값인데 이곳으로 복귀하면 해당 악성코드가 자동으로 실행된다.
Bufferbloat **(버퍼블로트)**	데이터통신망에서 패킷 손실을 막기 위하여 버퍼의 크기를 크게 만들었지만 이로 인하여 오히려 응답 문자(ACK: acknowledgement)와 같이 작은 크기의 패킷들이 갇혀서 전송되지 못하여 패킷전송이 느려지는 현상이다.

3) C

C4I **(Command, Control, Communication, Computer & Intelligence)**	우리 군의 전체 자원을 전산화한 후 네트워크로 연결해 효율적인 전쟁을 수행할 수 있도록 한 통합 전장 관리 체계이다. 육·해·공군별 통합 전술 지휘 체계를 구축한 후, 합동 참모본부가 기존 지휘 통제 체계인 CAPS를 계량하여 구축중인 합동지휘통제체계에 이를 통합하고, 미국의 통합전술지휘체계와도 연동시킬 예정이다.
CAPTCHA **(Completely Automated Public Turing test to tell Computers and Humans Apart, 자동 계정 생성 방지 기술, 캠차)**	인터넷 사이트에서 신규 회원 등록할 때 등록자가 컴퓨터인지 사람인지를 알아볼 목적으로 질문을 던져 응답을 확인하는 인증방식이다. 컴퓨터가 스스로 해독하기 어렵도록 만든 글씨나 숫자를 보여주고 사람인 경우만 입력에 성공할 수 있도록 제공·운영한다.
CC **(Common Criteria,** **공통 평가 기준)**	나라마다 상이한 정보보호시스템 평가 기준을 사용함으로써 발생하는 시간과 비용 낭비를 예방하고자 1999년 국제표준(ISO/IEC 15408)으로 채택된 정보보호 시스템 평가 기준을 말한다. 제1부 시스템의 평가원칙과 평가모델, 제 2부 시스템 보안 기능 요구사항, 제 3부 시스템의 7등급 평가를 위한 보증 요구사항으로 구성되어 있다.
CCL **(Creative Commons License)**	저작권의 부분적 공유를 목적으로 2002년에 만들어진 저작물 이용 허락 관련 표준약관이다. 미국에서 시작하였으나 세계 각국에서 나름대로 CCL를 만들어서 제공하고 있으며 한국에도 한국정보 법학회의 주관으로 2.0버전까지 나와 있다. 저작권자가 자신이 만든 저작물에 대하여 타인이 이용하는 방법과 이용 조건을 직접 표시하게 되어 있는데 표시 할 수 있는 기본 항목으로는 ① 저작자 표시(BY), ② 비영리(NC), ③ 변경 금지(ND), ④ 동일조건 변경 허락(SA)이 있다.
CERT **(Computer Emergency Response Team, 침해사고 대응팀)**	해킹과 같은 정보통신망 침해사고가 발생했을 때 이에 대응할 목적으로 조직의 업무 관할 지역 내에서 침해사고를 접수하여 처리할 뿐만 아니라 침해사고 예방과 사고에 따른 피해 복구 등의 임무를 수행하는 조직이다.
CIA Triad **(정보 보안의 3원칙)**	정보보안의 목표가 되는 정보보안 3원칙인 기밀성(C), 무결성(I), 가용성(A)을 만족시키는 것이다. ① 기밀성, Confidentiality: 인가받지 않는 대상에게는 정보를 공개하지 않는 것, ② 무결성, Integrity: 인가받지 않는 대상이 정보를 변경, 생성, 삭제하지 않도록 하는 것, ③ 가용성, Availability: 합법적 사용자가 합법적 정보를 요구

	할 때 적시에 제공되어야 할 것
Civic Hacking (시민 해킹)	시민들 중에서 ICT 개발자들이 자발적으로 모여서 정부가 공개하는 공공 데이터를 대상으로 분석하여 그 결과를 정부가 다시 활용할 수 있도록 해주거나 다른 시민들가 정보 교류 공동체를 운영하기도 한다.
CKO (Chief Knowledge Officer, 지식 총괄 책임자)	기업이나 조직 내에 존재하는 지식 자원을 종합적으로 관리함으로써 조직의 잠재적 가치를 높일 수 있는 전략을 제시하면서 변화를 주도하는 중역을 말한다. 자사의 상품이나 자사가 제공하는 서비스 관련 시장 정보, 이에 대한 고객들의 반응 등 기업의 전체 사원들이 알아야 할 지식을 신속하게 전달하고 공유하도록 한다. CKO는 기업 내의 지식 활동을 총괄하는 최고 책임자라 할 수 있다.
CLMS (Copyright License Management System, 저작권 라이선스 관리 시스템)	다양한 분야의 디지털 콘텐츠에 대한 저작권을 체계적으로 통합 관리하기 위한 시스템으로서, 모든 디지털 콘텐츠에 대한 사용계약 체결사항을 포함할 뿐만 아니라 사용 내역에 걸쳐 체계적으로 관리를 할 수 있도록 정부와 저작권 관련 단체가 추진하고 있는 시스템이다.
Contents Filtering (콘텐츠 필터링)	콘텐츠가 유통되는 과정에서 저작권을 침해하고 있는지를 판단하기 위해 도입된 기술이다. 만일 콘텐츠가 불법 복제된 것이라면 이를 유통되지 못 하게 하는 역할 등을 수행한다. 필터링의 기준으로는 특정 키워드를 걸러내는 키워드 필터링, 특징을 찾아서 걸러내는 특징점(feature) 필터링 등이 있다.
Convergence Security (융합 보안)	전통적인 정보보호 영역에서 잘 다루지 않았던 물리적 보안이나 장비 보안, 국가적/사회적 재해 · 재난 관제까지를 통합하여 다루는 진보된 보안 개념이다.
Copyright 운동	소프트웨어 저작권(Copyright)에 반대하는 운동이다. 1980년대에 MIT 대학의 리처드 스톨만 교수에 의하여 시작되었고 FSF(Free Software Foundation) 단체가 주도하고 있다. 이전에는 GNU 프로젝트 중심으로 활동하던 것을 최근에는 Linux 중심으로 활동하고 있다.
CRL (Certificate Revocation List, 인증서 폐기목록)	PKI와 같은 암호 시스템에서 더 이상 유효하지 않은 인증서의 일련번호 목록을 가리킨다. 인증기관이 부적절하게 인증서를 발급했거나 인증서의 개인키가 손상된 경우 혹은 사용자가 자신의 개인 키를 잃어버렸는지 확실하지 않은 경우에 해당 인증서가 여기에 포함된다.
CSO (Chief Security Officer,	정보 보안 대책 수립과 집행을 책임지고 기술적 대책과 법률적 대응까지 총괄하는 기업 내 최고 임원을 가리킨다.

최고 보안 책임자)	최고 정보 보안 책임자(CISO: Chief Information Security Officer)라고도 부른다.
CSRF (Cross Site Request Forgery)	XSS 공격과 상당히 유사하지만, XSS 공격에서는 악성 스크립트가 피해자의 컴퓨터에서 실행되는 반면, CSRF 공격에서는 피해자가 악성 스크립트가 서버에서 실행되도록 함으로써 공격이 이루어진다.
CTI (Cyber Threat Intelligence, 지능형 사이버 위협 대응)	지능형 지속 위협(APT)에 대응하는 사전 예방 개념으로서, 조직이 겪었던 과거의 위협 정보를 수집하고 분석하여 조직의 정보 자산에 위협이 될 수 있는 취약 요소를 파악함으로써 미래의 정보보안 위협에 적극 대응하는 방법이다.
Cyber Bullying	인터넷 환경하에서 이메일이나 전자게시물, SMS 등을 이용하여 특정한 개인이나 단체의 명예를 훼손하거나 심리적으로 괴롭히는 행위를 말한다.
Cyber Information Warfare (사이버 정보전)	해킹이나 악성코드 배포 등을 통하여 특정 국가의 정보통신 기반시설을 마비시킴으로써 사회 혼란을 야기하고 국가안보 및 명령지휘체계를 위협하는 공격 행위를 말한다.
Cyber Stalking (사이버 스토킹)	이메일, 게시판, 이동통신 등의 정보통신망을 이용하여 상대방에게 불안감이나 공포감을 지속적으로 유발하는 범죄행위로써, 사이버 스토킹 행위는 법에 의하여 형사 처벌된다.

4) D

Dark Data (다크 데이터)	정보 수집 대상으로 이미 모았지만 당장 데이터 분석에는 사용하지 않는 대량의 데이터를 말한다. 지금은 사용하지 않지만, 나중에는 언젠가는 사용할 거라는 이유로 보관만 하고 있어서 저장 효율성과 데이터 보안에 문제가 생기기도 한다.
Dark Web (다크 웹)	일반적인 정보검색엔진에서는 검색되지 않으며 특정한 환경에서의 웹 브라우저에만 접속되는 웹 사이트이다. 주로 사이버 범죄 사이트가 여기에 해당한다.
Database Security (데이터베이스 보안)	데이터베이스에 대한 보안 위협을 대비하기 위하여 사용하는 데이터베이스 보안 기술에는 크게 3가지가 있다. ① 접근통제: 허가 받은 사용자만이 데이터베이스를 접근하도록 한다. ② 가상테이블: CREATE VIEW를 이용하여 가상테이블을 제공함으로써 전체 데이터베이스 중에서 허가 받은 데이터만 접근하도록 한다. ③ 암호화: 중요한 데이터를 암호화하여 저장한다.
DDoS	DDos 공격은 기계나 네트워크 자원을 사용하기 원하는

(Distributed Denial of Service)	사용자들에게 이용이 불가능하도록 만드는 시도를 말한다. 일반적으로 이것은 한 명 이상의 사람들의 노력으로 구성되어 인터넷에 연결된 호스트의 서비스를 일시적으로나 무기한으로 방해라거나 연기시키는 것을 말한다.
DES (Data Encryption Standard, 데이터 암호 표준)	DES는 전자적 데이터를 암호화하는 대칭키 알고리즘으로서 한 때 가장 많이 사용되었다. 이 암호는 학문 세계의 현대 암호학의 발전에 가장 영향을 주었다. 그런데 DES는 현재에 있어서는 많은 응용에 있어서 안전하지 않았다고 알려졌다. DES는 미국 국립표준기술원(NIST)에 의하여 표준으로서 철회되었고 그 대안으로 나온 것이 AES(Advanced Encryption Standard)이다.
Digital Forensics	컴퓨터와 인터넷을 기반으로 이루어지는 범죄에 대하여 법적 증거자료를 획득하기 위하여 범죄와 관련된 디지털 장비 및 기억장치를 토대로 데이터를 수집, 보전, 분석하는 일련의 행위와 절차를 말한다. 디지털 포렌식은 디지털 장치의 유형에 따라 컴퓨터 포렌식, 네트워크 포렌식, 모바일 포렌식, 웹 포렌식 등으로 분류한다. 디지털 포렌식에서 지켜야 하는 원칙은 다음과 같다.
Directory System(DS)	PKI(공개키 기반구조)에서 유통되는 인증서, 사용자 정보 등을 모아서 관리하는 시스템을 말한다. 전화번호부를 Telephone Directory라고 부르는 것처럼, 어떤 주제에 관련된 정보를 모아서 집중하여 관리하는 시스템을 일반적으로 이르는 말에서 기인되었다.
DLP (Data Leakage/Loss Prevention, 데이터 유출/손실 방지)	조직 내부로부터 외부로의 정보 유출을 예방하기 위한 정보보호 대책이다. 조직 내부 사용자 모두에 대하여 컴퓨터 사용 행태와 네트워크 활용 행태 등을 총괄 모니터링하고, 필요할 경우 일부 기능을 통제함으로써 조직의 정보가 외부로 유출되는 사고를 예방할 수 있게 해준다. 대표적으로 4가지 기능을 제공한다. 접근통제, 암호화, 필터링, 감시
DoS (Denial of Service) 서비스 거부 공격	시스템이 정상적으로 서비스를 제공할 수 없도록 만드는 인터넷상의 공격 행위의 일종이다. 주로 TCP SYN flooding, 이메일 폭탄 등의 공격을 통하여 버퍼 오버플로우의 발생을 유도하여 공격한다. 여러 곳에 분산하여 에이전트를 미리 설치한 다음에 이들을 이용하여 DoS 공격을 하는 특별한 경우를 DDoS(Distributed DoS) 공격이라고 부른다.
DRM	음악, 영상, 출판물 등 각종 온라인 콘텐츠는 물론 소프트

(Digital Rights Management, 디지털 저작권 관리)	웨어, 이메일, 문서 등 기업의 디지털 자산에 대한 저작권을 보호하고 관리하는 기술이다. 온라인 콘텐츠의 경우 콘텐츠 자체 보안이나 저작권 보호 뿐만 아니라 콘텐츠의 생성·유통·사용·관리에 필요한 모든 프로세스를 지원한다. 디지털 콘텐츠를 암호화된 라이선스와 함께 포장하여 배포한다. 콘텐츠를 재생할 때 라이선스의 조건을 읽어 재생 여부를 결정하게 되며, 지불결제 수단과 병용되어 콘텐츠 사용료를 부과함으로써 콘텐츠의 유통과 관리를 지원한다. 기본적으로 불법 복제와 배포를 예방한다.
DRP (Disaster Recovery Plan, 재난 복구 계획)	지진, 화재, 홍수 등의 재난 상황에 대비하여 정보통신 기반시설의 하드웨어와 소프트웨어 자원 전체에 대하여 취해야 할 행동 계획을 미리 마련해 놓은 것이다.

5) E

EAM (Extranet Access Management, 엑스트라넷 접근관리)	인트라넷, 엑스트라넷, 클라이언트/서버 등 다양한 인터넷 환경하에서 특정한 자원에 접근할 때 사용자 인증 및 접근 권한 부여에 관한 관리를 수행하는 통합 솔루션으로서, 사용자의 분류와 등급에 따라 접근하는 시스템 자원이 다르다.
e-Discovery	e-Discovery는 전자적으로 저장된 정보(ESI, Electronically Stored Information)를 대상으로 한 재판에 필요한 증거나 서류를 제시하는 것 혹은 사실을 제시하는 과정과 절차를 말한다. e-Discovery 대상으로는 전자우편, 웹페이지, 휴대폰, 채팅, 데이터베이스 로그 등 광범위한 정보통신시스템이 포함된다. e-Discovery는 주로 디지털 포렌직(Digital Forensics)을 담당하는 조사관이 법정에 제출한다.
EFF (Electronic Frontier Foundation, 전자 프론티어 재단)	인터넷상에서의 표현의 자유를 중요시하는 국제적인 비영리 단체로서, 2012년 미국의 온라인 저작권 침해 금지 법안(SOAP: Stop Online Piracy Act)과 지식재산권 보호 법안(PIPA)에 대하여 반대하는 활동을 펼쳤다.
e-Passport (전자여권)	기존 여권의 위 · 변조 방지 및 여행자의 편익 도모를 위하여 세계적으로 시행하고 있는 새로운 여권을 말한다. 여기에는 여권 소지자의 사진, 홍채, 지문 등을 신원 확인 자료로 보관하고 있는 칩이 내장되어 있다. 국제 범죄나 테러 공격에 대비하여 입출국 기능을 정확하고 신속하게 처리하는 용도로도 사용한다.

EPC **(Electronic Product Code)**	모든 제품마다 고유의 일련번호를 부여하는 제품 번호 부착에 관한 새로운 표준을 말한다. 각각의 제품마다 고유한 번호가 부여되므로 데이터베이스와 연계되어 제품의 가격, 위치정보, 제조업체 정보를 알 수 있게 된다. 현재 사용 중인 UPC(Universal Product Code) 코드의 차세대 버전으로 RFID 태그에 내장되어 있는 코드이기도 하다. EPC(Electronic Product Code) Global에서 4가지 Class(Class 1, 2, 3, 4)로 분류하여 제시한 RFID 태그를 EPC Class라고 한다.
EPCM **(Electronic Postal Certification Mark, 전자우편 소인 마크)**	전자 우편물에 대하여 소인 기능을 부과하고자 만국우편연합이 만든 우편물 배달 서비스이다. 이전에는 DPM(Digital PostMark)이라고 불렀다.
ERM **(Enterprise Risk Management, 전사적 위험관리 시스템)**	기업이 직면하는 여러 가지 다양한 위험들을 전체 기업경영 측면에서 통합적으로 인식하고 관리하는 방식이다. 기존의 기업 위기관리가 개별부서 단위로 이루어졌다면 이것은 전체 기업의 시각에서 파악하고 체계적으로 전사적인 대책을 수립하여 효율적으로 위기를 관리할 수 있도록 해준다.
ESCROW Service **(에스크로 서비스)**	소비자와 구매자 사이의 신용관계가 불분명할 때 제 3자가 개입하여 거래 관계를 보호해 주는 서비스이다. 법률용어로서 ESCROW는 “조건부 양도증서”라고 번역한다.
ESM **(Enterprise Security Management, 통합 보완 관리 시스템)**	방화벽(firewall), 가상사설망(VPN), 침입탐지 시스템(IDS) 등의 다양한 보안 솔루션(장비, 소프트웨어)들을 통합하여 연동시켜 관리하는 시스템을 말한다. 보안 솔루션 하나가 제공하는 보안 능력보다 더 많은 능력을 다른 보안 솔루션과 연계하여 얻을 수 있게 된다. 보안 솔루션에서 발생하는 이벤트들의 상호간 연관성 분석을 통해 잘못된 보안 대책을 최소화하는 방향으로 발전하게 된다. ESM은 기존의 통합관리 수준에서 벗어나 이제는 시스템 자원관리(SMS), 네트워크자원관리(NMS) 등 종합적인 자원관리 시스템으로까지 확대되고 있다.
Exploit **(익스플로잇)**	컴퓨터 시스템이나 소프트웨어, 디지털 장비가 예상하지 못한 행동을 하도록 만들기 위하여 이들이 가지고 있는 취약점(Vulnerability)이나 버그(Bug)를 악용하는 행위 혹은 그 결과물을 말한다. 어떤 IT 시스템이 취약하다는 사실을 증명하기 위하여 의도적으로 기획하는 행위로 볼 수도 있다. DoS(서비스 거부 공격), 사용자 권한의 비정상적 상승, 악성코드 제작 활동도

	익스플로잇의 형태로 볼 수 있다.
Extranet **(엑스트라넷)**	여러 개의 인트라넷 간에 정보 공유가 가능하도록 연결된 광범위한 인트라넷을 이르는 용어이다. 각 인트라넷의 방화벽 기능을 엑스트라넷에 참여하는 외부 단체에는 적용하지 않음으로써 구현된다. 여러 기업 간에 표준화되고 개방적인 인터넷 기술을 사용하므로 구축과 운영이 경제적이다. 엑스트라넷을 이용하면 가상사설망(VPN)을 저렴하게 구축할 수 있다.

6) F

Finger Vein Money **(지정맥 머니)**	소비자가 자신의 지정맥(손가락 정맥) 패턴을 자신의 지불 계좌와 함께 사전에 미리 등록 한 후 상품 구입 시마다 지정맥 인식을 통하여 본인 여부를 판단한 후 자동 지불하는 기술이다. 현금이나 신용카드를 소지하지 않는다는 점에서 편리하고 안전하다.
Firewall **(방화벽)**	방화벽은 미리 정해진 보안 규칙을 기반으로 유입, 유출되는 네트워크 트래픽을 감시하고 제어하는 네트워크 보안 시스템이다. 일반적으로 방화벽은 신뢰할 수 있고 안전한 내부 네트워크와 안전하거나 신뢰할 수 있다고 보기 힘든 인터넷과 같은 외부 네트워크간에 장벽을 설정한다.

7) G

Gap Filler **(갭 필러)**	통신이 잘 이루어지지 않는 사각지역에 신호를 재전송하여 수신 상태를 개선하는 시스템이다. 주파수 대역이 높을수록 신호의 직진성이 강해지므로 이런 경우 갭 필러가 필요하다.
GNU 라이선스	GNU 프로젝트는 이용자의 자유로움을 증진하기 위해 ① GPL(General Public License), ② LGPL(Lesser General Public License) ③ GFDL(GNU Free Documentation)라는 3가지 라이선스 모델을 제공하고 있다. GPL은 GNU 정신을 반영한 대표적인 오픈 소스 라이선스이고, LGPL은 GPL에 약간의 상용화를 허용한 라이선스이며, GFDL은 책이나 매뉴얼에 적용되는 GPL을 말한다.
GNU **(GNU's Not Unix)**	유닉스(Unix)의 상업적 확산에 반발하여 무료로 개발·배포하고 있는 유닉스 호환 운영 체제 또는 이와 관련된 정보

	공유 프로젝트를 가리킨다. GNU 프로젝트는 이용자의 정보 접근, 수정의 자유 증진이라는 목표를 가지고 있다. “모든 프로그램은 무료이어야 하며, 프로그램의 사용, 복사, 수정, 재분배에 대한 제한이 있어서는 안된다”라는 GNU 헌장이 정신을 내포한다. GNU 소프트웨어는 소프트웨어를 사용하기 위해서 지불된 비용의 유무에 관계없이 소프트웨어 소스에 대한 복제와 수정의 자유를 모든 사용자에게 부여한다.
G-PIN (Government-Personal Identification Number, 정부 개인인식번호)	정부(행정안전부)에서 제공하는 인터넷상의 개인식별번호이다. 기존의 주민등록번호 인한 개인정보 유출 사고를 예방하고자 이를 정부에서 대체수단으로 제공하는 개인인식번호로서, G-PIN은 생년월일, 성별 등의 정보가 담겨있지 않고 유출 시 언제든 다시 발급받을 수 있으며 숫자와 알파벳 13자로 구성된다. 중앙정부기관과 지방자치단체 등에서부터 시작해 전국 1만 5000개 공공기관에서 주민등록번호를 대체하여 사용하고 있다.
Grayware (그레이웨어)	인터넷 사용자가 어쩔 수 없이 자신의 컴퓨터에 설치하도록 유도한 후, 설치가 된 후에는 사용자의 기대와 다른 동작을 하여 시스템 성능을 악화시키거나 사용 불편을 초래하는 소프트웨어들을 총칭한다.

8) H

Hadoop	PC처럼 가격이 싼 컴퓨팅 서버들과 저장장치를 활용하여 가상화된 거대한 저장장치를 형성하고 그 안에 빅데이터(Big Data)를 상대적으로 쉽게 저장하고 활용하여 처리할 수 있도록 한 분산 파일 시스템이다. 2004년 미국 프로그래머 더그 컷팅이 방대한 데이터를 처리하기 위하여 구글의 맵리듀스(MapReduce) 등을 활용해 이를 개발하였다.
Hash Function (해시 함수)	임의의 가변길이 메시지를 고정 길이의 값으로 변환하여 출력하는 함수이다. 대표적인 해시 함수로는 MD5와 SHA가 있다.
Hoax (혹스)	이메일 전송을 통하여 불특정 다수의 사람들에게 컴퓨터 시스템에 대한 거짓 상황 정보를 유포함으로써 심리적 불안감을 조성하는 악성코드를 말한다.
Home Telematics (홈 텔레매틱스)	홈 네트워크와 텔레매틱스가 합성된 신조어이다. 차량 내부 단말기로 집안 홈 네트워크 시스템에 연결된 가전제품과 조명, 가스 밸브 등의 기기를 일괄적으로 제어

	할 수 있게 해준다.
Honeypot (하니팟)	보안 위협을 사전에 대응할 목적으로 해킹 공격과 악성코드 감염을 고의로 유도함으로써 해킹 기법과 악성코드 특성과 행위를 분석하여 그에 대한 예방책을 세우도록 하는 시스템이다.
Hot Spot (핫스팟)	무선 LAN 환경이 지원되는 제한된 장소를 가리킨다. AP(Access Point)가 설치된 곳으로 무선 LAN이 장착된 노트북 PC에서 인터넷을 사용할 수 있게 지원해준다.
HSM (Hardware Security Module, 보안토큰)	HSM은 암호화 관련 전체 과정(암호화, 복호화, 전자서명)을 내부적으로 안전하면서 빠르게 수행하는 하드웨어 장치를 이른다. 그런데 HSM을 구현하는 하드웨어의 형태가 다양해서 국내에서는 UBS 형태의 스마트칩을 사용하는 형태에 국한하여 “보안토큰” 이라고 명명했다.

9) I

IAM (Identity & Access Management, 계정 접근관리)	기업이나 조직의 전체 구성원들이 다양한 컴퓨팅 자원들을 접근할 때 일관성 있게 구성원의 신분을 확인하고 자원 접근을 제어하도록 하는 시스템이다. 통합 인증, 접근 권한 관리, 자동화된 계정 관리, 보안 로그 관리 등의 기능을 제공한다.
IDC (Internet Data Center)	정보의 저장, 관리 및 보급을 위한 중앙 저장소이다. 기업체들을 대상으로 중앙 집중식 호스팅 서비스 및 관련 데이터 서비스를 제공하는 회사를 가리키는 말이기도 하다. 호스팅 사업의 종류로는 ① 애플리케이션을 빌려주는 ASP, ② 서버 공간 일부를 웹 사이트로 빌려주는 웹 호스팅, ③ 서버 전체를 빌려주는 서버 호스팅, ④ 서버를 설치할 공간만 빌려주는 co-location이 있다.
IDS (Intrusion Detection System, 침입 탐지 시스템)	IDS는 네트워크와 시스템을 모니터링해서 악성 행위와 정책 위반이 있는지 찾아 관리 스테이션에 보고해주는 장비 혹은 소프트웨어 애플리케이션을 말한다. 어떤 시스템은 침입 시도를 중단시키기도 하지만 이것은 모니터링 시스템에 있어서 꼭 필요하거나 기대할 요소는 아니다. IDS는 거의 모든 조직의 보안 기반구조로서 이제는 필수 추가 사항이 되었다. IDS의 침입 탐지 기능 외에 방화벽을 활용한 유해 트래픽 차단 기능을 동일한 장비 내에 모두 구현한 것이 IPS(Intrusion Prevention System, 침입 예방 시스템)이다.
IM	기존의 싱글 사인 온(SSO) 기능과 엑스트라넷 접근관리

(Identity Management, 통합 계정관리)	(EAM) 기능을 통합 확장한 보안 솔루션으로서, 조직 내부의 보안 정책에 따라 사용자 계정과 이에 부합하는 권한을 생성, 삭제하며 사용자별 시스템 자원 접근에 따른 감독과 감사기록 기능 등을 제공한다.
INDECS (Interoperability of Data in E-Commerce System)	전자상거래 시스템에서 디지털 콘텐츠의 저작권을 보호할 목적으로 저작권의 계약, 판매, 처리 등의 모든 과정에서 상호운용에 필요한 메타 데이터에 관한 통일된 형태의 저작권 보호 프레임워크이다.
Infodemics (인포데믹스)	어떤 의도를 가지고 인위적으로 만들어진 정보가 대중 사이에 급속도로 퍼지는 현상이다. Information(정보)과 Epidemics(유행병)의 합성어로서, 빠른 정보 확산으로 근거 없는 공포가 사회 전반에 조성되어 정치, 경제 분야에 각종 부작용이 일어나는 현상이다.
i-node Block (i-노드 블록)	유닉스 파일 시스템에서 각 파일이나 디렉터리에 관한 관리 정보를 저장하고 있는 블록으로서 각 파일마다 1개씩 존재한다. 저장되는 정보는 파일의 소유자, 접근권한, 접근시간, 파일의 크기, 파일 링크 개수, 파일이 저장된 데이터블록의 주소 등이다.
Internet Strike-out (인터넷 삼진아웃)	불법 복제물 제작 및 배포 등을 통하여 3회 이상 경고를 받은 사람에게 해당 온라인 서비스 제공자가 6개월 이내의 기간을 정하여 계정의 이용 정지를 명령하는 것이다.
Intranet (인트라넷)	개방된 인터넷 환경을 토대로 하여 지정된 조직만이 배타적으로 활용할 수 있는 정보 시스템 구축을 지원하는 인터넷 기술이다. 내부 정보의 불법 접근 및 외부 유출을 막기 위하여 방화벽(firewall)과 같은 보안 장비를 외곽에 설치해야 한다. 사용자는 웹 브라우저를 이용하여 웹서버 등을 통해 문서를 공유할 수 있다. 사용자의 사용 환경이 인터넷 환경과 동일하므로 업무 처리의 장소와 시간에 제약이 없다는 장점을 갖는다. 그룹웨어의 기능도 추가로 구현할 수 있으며 구축 비용이 비교적 저렴하다.
i-PIN (internet Personal Identification Number)	웹 사이트에 회원 가입을 할 때 기존의 주민등록번호 대신에 사용하는 인터넷 주민등록번호를 말한다. 회원 가입을 요청한 고객에 대해 신원확인을 완료한 후에 본인확인 기관이 온라인으로 고객에게 i-PIN을 발급한다. 주민등록번호는 유출되면 새롭게 이를 발급 신청할 수 없지만 i-PIN의 경우는 고객이 i-PIN 유출이 의심되면 언제든지 새로운 i-PIN으로 변경 발급받을 수 있다.

IPSec (IP Security)	IPSec은 통신 세션에서 각 IP 패킷을 인증하고 암호화함으로써 인터넷 프로토콜 통신을 보호하는 프로토콜 모음이다. 또한, IPSec은 세션 시작 과정에서 당사자 간의 상호 인증을 구축하는 프로토콜을 포함하고 있다. IPSec은 ISO 표준인 네트워크 계층 보안 프로토콜(NLSP)의 후속 프로토콜이다. IPSec은 AH(Authentication Header)와 ESP(Encapsulating Security Payload)를 제공함으로써 IPv6에서의 정보보안 서비스로 인증, 무결성, 비밀성을 만족시키는 서비스를 제공하고 있다.
IPv6	기존의 32비트 인터넷 주소방식인 IPv4를 대체할 새로운인터넷 주소 방식으로서, 16비트씩 8개 부분이 콜론(:)으로 구분되어 총 128비트의 확장된 주소 공간을 제공한다. IPv4는 43억 개의 주소를 생성하는 반면, IPv6는 43억 개의 주소를 생성한다. 인터넷 계층에서 보안 감사의 기능과 암호화 기법을 제공하는데, 유니캐스트(Unicast), 애니캐스트(Anycast), 멀티캐스트(Multicast) 라는 3가지 주소 유형을 제공한다.
ISMS (Information Security Management System, 정보보호 관리 체계)	회사와 같은 조직이 가지고 있는 정보자산을 신뢰성 있고 안전하게 활용하기 위하여 취하는 제반 정보보호 활동을 지속적이며 체계적으로 운영·관리하는 체계를 말한다. 우리나라의 경우 2002년부터 ISMS 인증 제도를 도입하여 이를 인증 받은 조직과 기업에 대한 대외 신뢰도 향상을 꾀하고 있다. 정보보호 관리 체계 및 인증제도에 대한 국제 표준규격은 'ISO 27001'이며, 영국의 경우 'BS-7799-1', 독일의 경우 'BSI'에 해당한다. ISMS는 정보자산의 기밀성(C), 무결성(I), 가용성(A)을 달성하기 위하여 다양한 보안 대책을 관리하고, 위험기반 접근방법에 기초하여 ① 정보보호 정책 수립 및 범위설정 → ② 경영진 책임 및 조직 구성 → ③ 위험관리 → ④ 정보보호 대책 구현 → ⑤ 사후관리 단계로 운영된다.
IT Compliance (IT 컴플라이언스)	기업 경영 환경을 IT 기반으로 변경할 때 지켜야 할 관련 법규나 행정 지침을 말한다. 예를 들어 전자문서 작성 규칙이나 기업 회계 감사자료 지원 시스템 구축 등은 IT 컴플라이언스에 속한다. 이것은 소비자의 권익을 보호하고 기업의 국제 경쟁력을 높이는데 필수적인 요소로 자리잡고 있다.
ITSM (IT 서비스 관리)	고객과 IT 서비스 제공자 간의 계약인 서비스 수준 관리(SLA)를 만족시키기 위한 모든 활동을 가리킨다. IT 서비스의 품질을 유지하며 궁극적으로 증진시키기 위한 활동으로서, 기업 내 IT 관리 역할을 서비스 관점으로 바꾸

	어 관리 하는 것이다. ITSMF(IT Service Management Forum)에서 표준화를 담당하고 있는데, 국제 표준으로 ISO 20000이 있다. 이것은 영국 표준인 BS 15000을 2005년 말 국제표준으로 승인한 것이다.

10)J

JCA (Java Cryptography Architecture, 자바 암호구조)	썬마이크로시스템즈사가 제작한 자바 개발 키트(JDK)에서 제공되는 암호구조이다. 특정한 암호 알고리즘에 독립적인 인터페이스를 제공함으로써 다양한 제품에서 제공하는 특정한 알고리듬을 사용자가 쉽게 이용할 수 있는 환경을 제공한다. 알고리듬을 다른 것으로 교체하기 쉽고, 특정한 포맷이나 운영 방식에 제한을 받지 않는 구조로 구성되어 있어서 유동적인 환경에 적합하다. 엔진 클래스(암호, 메시지 다이제스트, 서명)를 기반으로 하위 알고리듬을 호출하여 사용하고 있다.

11)K

Key Logger Attack (키 로거 공격)	키보드를 통하여 사용자가 입력한 내용을 가로채 외부에서 몰래 탐지해가는 해킹기법이다. 유출되는 정보 중에 사용자 계정 정보나 은행계좌 정보, 신용카드번호 등의 개인정보가 해커들이 노리는 핵심적인 정보인데 이들은 나중에 악용되어 더 큰 피해를 일으키게 된다. 키보드 외에 마우스의 입력좌표 값을 가로채 화면상의 정보를 유추해가는 기법도 공격에 포함된다.
KeyPair	공개키 암호 알고리즘에 사용되는 ① 개인키(Private Key)와 ② 공개키(Public Key) 쌍을 말한다. 이 중에서 1개는 암호화에 이용되고 다른 1개의 키는 복호화에 이용된다. 수학적 방법에 의해 암호화 및 복호화 과정을 수행한다.
Kill Switch (킬 스위치)	스마트폰과 같은 개인정보기기를 분실하였을 때 이를 습득한 타인이 불법으로 사용하거나 저장된 개인정보를 유출하지 못하도록 원격으로 기기 사용을 정지시키는 기능이다. 이 기능은 펌웨어나 운영체제 수준에서 제공된다.
KMS (Knowledge Management System, 지식 관리 시스템)	KMS의 목적은 많은 사용자들로 하여금 대량의 공유 하이퍼텍스트 안에 정보를 사용하고 나눌 수 있는 협업을 할 수 있도록 하는 데 있는데, 아예 처음부터 이 시스템은 진정한 다중사용자 시스템으로 설계된다. 공간적 하이퍼미디어 시

	스템으로서 KMS는 이메일, 전자게시판, 블로그 등과 같은 전자통신 공통형태는 물론 프레젠테이션, 문서, 데이터베이스, 소프트웨어 프로그램과 같은 외연적 지식 인공물에 대한 모든 형태를 표현할 수 있도록 고안된다.

12)L

Land Attack	DoS 공격의 일종으로서 패킷의 출발지 IP주소와 도착지 IP 주소를 동일하게 지정함으로써 공격 대상이 스스로에게 SYN 패킷을 계속하여 보내게 하는 공격으로 공격 대상은 루핑(looping)에 빠지게 된다.
LEA (Lightweight Encryption Algorithm, 경량고속블록암호화)	국내 국가보안기술연구소에서 개발한 블록 암호 기술로서, AES보다 2배 정도 빠른 속도로 암호화할 수 있고 코드의 크기는 약 1/8, 전력 소모량도 약 1/2로 줄일 수 있다.
Linux	리눅스는 많은 수의 하드웨어 플랫폼에서 실행되며 무료로 배포될 수 있는 오픈 소스 운영체제이다. 주요 리눅스 커널은 리누스 토발즈에 의하여 개발되었다. 무료인데다가 PC와 매킨토시를 포함한 많은 플랫폼에서 실행될 수 있기 때문에 리눅스는 상업용 운영체제에 대한 최고로 인기 있는 대인이 되고 있다.

13)M

Malware (맬웨어)	사용자의 시스템을 파괴하거나 사용자의 정보를 유출함으로써 악의적인 활동을 수행하도록 의도적으로 제작된 소프트웨어에 대한 일반적인 명칭이다.
MC-Finder (Malicious Code-Finder, 악성코드 탐지기)	악성코드가 설치되어 있는 웹 사이트들을 찾아서 대응하는 악성코드 자동 탐지 프로그램을 말한다. 악성코드는 웹 사이트의 취약점을 이용하여 운영자 몰래 설치된다. 악성코드가 설치되어 있는 웹 사이트를 방문하면, 사용자의 PC에 악성코드가 다운로드 되어 설치된다.
MOTP (Mobile One Time Password, 모바일 일회용 비밀번호)	내용유출을 방지하기 위하여 사용해온 1회용 암호(OTP, One Time Password)를 스마트폰과 같은 개인용 모바일 단말기에서 사용하는 OPT를 〈MOTP〉라 부른다.

14)N

NAC (Network Access Control,	2005년 가트너 그룹이 정보 시스템 예방 차원에서 네트워크 보안 체계를 구현하는 것을 목적으로 제시한 새로운 네

네트워크 접근통제)	트워크 보안 패러다임이다. 새로운 네트워크 장비를 도입한다기보다는 전체 네트워크에 대한 접근제어를 수행하는 것으로, 사전에 결정된 조직 내 보안정책을 지키지 않는 사용자에게 네트워크 접속을 제한함으로써 악성코드, 해킹으로부터 조직 내 컴퓨터 시스템과 네트워크, 사용자 단말기를 보호하게 된다. NAC의 모델은 ① 접속 단말에 대한 보안 평가, ② 보안 문제에 대한 대응, ③ 네트워크 접근허용, ④ 보안 정책 준수에 대한 지속적인 모니터링, ⑤ 대응 업무 순환 절차의 순서로 구현된다.
NAC (Network Admission Control, 네트워크 승인 보호)	보안 정책에 부합된 단말기만 네트워크에 연결할 수 있도록 해줌으로써 사설망의 보안을 강화하는 방식이다. 사용자 환경이 엄격하게 통제될 수 있는 기관이나 조직에서 이상적으로 사용될 수 있다.
Network Isolation (망 분리)	외부 인터넷망으로부터의 불법 접근과 내부정보유출을 방지하기 위하여 내부 업무망을 외부 인터넷망과 분리하는 조치로서 ① 보안성이 높은 '물리적 망 분리'와 ② 가상화를 이용한 '논리적 망 분리'가 있다. 국내에서는 금융전산센터에 대하여 2014년부터 의무화 되어있다.
Network Neutrality (네트워크 중립성)	네트워크 사업자들은 통신망상의 모든 컨텐츠에 대하여 어떠한 차별도 없이 동등하게 취급해야 한다는 원칙이다. 이 원칙을 보장하기 위하여 구체적으로 ① 상호접속, ② 비차별, ③ 접근성이라는 3가지 세부원칙이 모든 통신망에 동등하게 적용되어야 한다. 유럽연합(EU)이 정보사회보고서에서 요구하고 있는 중요한 원칙이다.
NFC (Near-Field Communications, 차세대 근거리 무선통신)	전자태그(RFID)의 한 종류로서 비접촉식 근거리 무선통신 모듈을 말한다. 10cm 내외의 가까운 거리에 떨어진 단말기들 사이에 데이터를 송수신하는 기술로서 13.56MHz의 주파수 대역을 사용한다. 구매 대금의 결제뿐만 아니라 상품정보 유통, 출입통제 시스템 등에도 활용된다. 특히 휴대폰 기반의 이동식 지불 수단으로 점차 확대 사용되고 있다.

15)O

OTP (One Time Password, 일회용 비밀번호)	사용자가 시스템에 로그인할 때와 같이 사용자 인증 시마다 매번 다른 비밀번호를 생성하는 기술을 말한다. 딱 한 번만 사용할 수 있는 비밀번호라고 할 수 있다.
OWASP TOP 10	OWASP Top 10은 OWASP(The Open Web Application Security Project)라는 단체에서 웹 애플리케이션을 중심으

	로 3년 단위로 업데이트하여 발표하는 웹 취약점 목록이다. OWASP는 주로 웹에 관한 정보 노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구해오고 있다.

16)P

P3P **(Platform for Privacy Preferences)**	세계 인터넷 표준화 기구인 W3C에서 개발한 개인정보보호 표준 플랫폼으로서, 웹 브라우저로 어느 웹 사이트를 방문하면 자동으로 웹 사이트의 개인정보 수준을 읽은 후, 이용자가 미리 설정해놓은 정보공개 수준과 비교하여 정보를 선택적으로 보여주는 기술이다. 이용자가 웹 사이트를 검색할 때 방문한 웹 사이트의 P3P 요구 수준을 요구하게 되며, 해당 웹 사이트는 개인정보 요구 수준을 이용자에게 전송함으로써 구현된다. 이때 이용자가 미리 설정한 정보공개 수준과 웹 사이트가 제공하는 정보요구 수준이 일치할 경우 접속이 가능하지만 그렇지 않을 경우 정보 공개 수준이 맞지 않는다는 팝업 메시지 창이 뜨면서 원활한 접속이 이루어지지 않는다. 이를 통해서 이용자가 직접 자신의 개인정보 보호 수준을 통제할 수 있다.
PET **(Privacy Enhancing Technology,** **프라이버시 강화 기술)**	사용자의 개인정보 노출을 최소화하면서도 다양한 인터넷 서비스를 이용할 수 있도록 해주는 정보보호 기술을 말한다. 예를 들어, 사용자 등록을 할 때 서비스 제공자에게 개인 정보 제공을 최소화할 수 있도록 해주는 익명 인증 기술도 여기에 속한다.
Pharming **(파밍)**	합법적으로 소유하던 사용자의 도메인을 탈취하는 기술로서, DNS의 정보를 변조하여 가짜 사이트를 진짜 사이트로 오인하도록 유도한 후 개인정보를 훔치는 범죄 수법이다. 인터넷 주소 자체를 강탈해 사용하기 때문에 사용자들이 쉽게 속게 된다.
PI **(Personal Information,** **개인 정보)**	살아있는 개인을 식별할 수 있는 정보로서 ① 인적사항(이름, 주민등록번호, 이메일주소)을 비롯하여 ② 신체적 정보(얼굴, 지문, 홍채, 진료기록), ③정신적 정보(종교, 가치관, 성향, 인터넷 검색 기록), ④ 재산적 정보(금융정보, 개인신용정보), ⑤ 사회적 정보(학력, 전과, 병역, 취업) 등도 여기에 포함된다.
PIA	개인정보가 포함된 IT 시스템에 중요한 변경 사항이 발생하는 경우, 내재된 개인정보 침해 위험성을 미리 발견하고 적절한 대응책을 수립하기 위해 도입하는 제도이다.
PII	생존하는 개인을 식별할 수 있는 모든 정보를 가리킨다. 예

(Personally Identifiable Information, 개인식별정보)	를 들어, 이름, 주소, 이메일주소, 주민등록번호, 신용카드번호 등이 여기에 속한다. 특정 정보로부터 개인을 직접 식별할 수는 없어도 다른 정보와 결합하여 최종적으로 식별할 수만 있다면 이들은 모두 개인 식별정보로 분류된다.
PIMS (Personal Information Management System, 개인정보보호 관리 체계)	고객의 개인정보를 다루는 조직(기업)이 조직 전체에 걸쳐 고객의 개인정보를 안전하게 다룰 수 있도록 구축한 체계를 말한다. 우리 정부에서는 각 기업의 PIMS에 대하여 3개 분야 119개의 점검항목을 두어 법적 필요조건을 만족하는지 조사하여 이를 만족할 때 인증서를 부여하고 있는데 이를 PMIS 인증제(개인정보보호 관리 체계 인증제)라고 부른다.
Ping of Death	인터넷 통신 명령 Ping을 사용하여 ICMP 패킷을 보낼 때 정상보다 아주 큰 패킷을 보내면 라우팅을 거치는 동안 아주 작은 조각들로 바뀌어 전송됨으로써 단시간에 많은 ICMP 패킷들이 보내져서 결국 인터넷 서버가 다운되도록 하는 일종의 서비스 거부(DoS) 공격이다.
PKI (Public Key Infrastructure, 공개키 기반구조)	공개키 암호 시스템을 안전하게 사용하고 관리하기 위한 정보보호 표준 방식이다. ITU-T의 X.509 방식과 국가별 지역별로 실정에 맞게 보완 개발되고 있는 비X.509 방식이 있다. 여기에서 유통되는 인증서, 사용자 정보 등을 모아서 관리하는 시스템을 Directory System(DS, 디렉터리 시스템)이라고 부르며, PKI를 운영할 수 있도록 지원해주는 구성 조직으로서 암호화에 필요한 공개키를 발급해주고 관리하는 조직을 인증기관(CA, Certification Authority)이라 부른다. PKI에 새로운 사용자가 가입하고자 할 경우, 등록 기관이 새로운 사용자의 정보를 검증하여 이곳에 인증서를 요청하면 이를 발급해준다. 이 인증서 안에는 사용자의 성명과 공개키, 인증서의 유효 기간 등이 들어 있다.
PMS (Patch Management System, 패치 관리 시스템)	소프트웨어(특히 운영체제)의 해당 패치들을 신속하게 다운로드 받아 설치하고 관리하는 프로그램으로서, 스마트 업그레이드를 체계적으로 지원한다.
PPI (Program Protection Information, 프로그램 보호 정보)	지상파 디지털 방송 프로그램에 저작권 정보를 포함하여 송출함으로써 방송 프로그램의 저작권을 보호하는 기법 중의 하나이다.

17)R

Ransomware (랜섬웨어)	몸값(Ransom)과 제품(Ware)으로 구성된 합성어로서, 컴퓨터 안에 저장된 문서나 정보를 소유자의 동의 없이 감추거나 변형한 후(즉, 인질처럼 처리한 후) 몸값 결제를 해주어

	야만 다시 접근할 수 있도록 해주는데 활용되는 악성코드를 말한다.
Registry (레지스트리)	MS 윈도우 운영체제에서 시스템 하드웨어 장치에 대한 정보, 설치된 프로그램과 설정 환경 정보, 사용자 계정들에 대한 프로파일 등에 관한 중요한 시스템 정보를 보관하는 데이터베이스이다.
Rootkit (루트킷)	자기 자신이나 다른 프로그램들을 보이지 않도록 숨김으로써 사용자나 백신 프로그램이 발견하지 못하도록 하는 악성코드이다.
RPO (Recovery Point Objective)	심각한 사건이 발생했을 때 업무 영속성(BCP)이 보장되는 한도 내에서 IT서비스로부터 사라질 수 있는 데이터의 최대 허용 주기를 말한다.
RTE (Real Time Enterprise, 실시간 기업 경영)	기업 운영에 필요한 제반 정보들을 온라인 실시간으로 유통함으로써 바람직하지 못한 업무 지연을 제거하고, 기업의 의사 결정 속도를 가속함으로써 기업 경제력을 높이는 경영 방식이다. SEM(Strategic Enterprise Management)을 이용하여 기업 경영 정보를 실시간 현황판으로 보여줌으로써 핵심 경영 정보를 실시간으로 공유하도록 해주며 빠른 의사 결정이 가능하도록 해준다. RTE의 구성요소로는 ① 기업 자원 관리(ERP), ② 공급망 관리(SCM), ③ 고객 관계 관리(CRM), ④ 비즈니스 프로세스 관리(BPM)를 꼽을 수 있다.
RTO (Recovery Time Objective, 목표 복구 시간)	지진이나 화재 등의 비상사태 때문에 중단되었던 업무가 다시 복구하는 데까지 소요되는 시간에 대한 목표값을 가리킨다.

18)S

Secure OS (보안 운영체제)	컴퓨터 운영체제의 보안 결함으로 인하여 발생 가능한 각종 해킹으로부터 컴퓨터 시스템을 보호하기 위하여 기존의 운영체제 내에 관리자 인증 보안 기능을 추가한 운영체제이다.
Server Farm (서버 단지)	서로 네트워크에 연결되어 있지만, 물리적으로는 한 곳에 놓여있는 서버들의 그룹을 가리킨다. 업무 부하를 분산함으로써 내부 처리를 능률화하고, 다중 서버들의 능력을 활용함으로써 계산 과정을 촉진하게 해준다.
SLA (Service Level Agreement, 서비스 수준 관리)	원래는 통신 사업자가 통신망 이용자에 대해서 통신망의 전송 품질을 보증하는 계약을 가리키는 용어였다. 일반적으로는 SLA는 정보 제공자와 기업체가 서로 주고받는 서비스의

	품질 계약 보증서로서, 통신망과 관련된 비용을 경감하는 것이 주된 목적이다. 따라서 목표치를 설정해서 필요한 데이터를 수집, 관리할 필요가 있다. ① 사전 준비, ② SLA 개발, ③ 운영 및 개선의 주기를 거치면서 SLA는 유지된다.
Smart Token (스마트 토큰)	보안 기능을 추가한 스마트카드로서, 생김새는 USB 메모리 형태를 갖는다. 공인인증서, 보안 모듈, 은행카드 기능을 담당한 IC칩 등을 내장하고 있어서 일반 스마트카드로서의 기능은 물론 인터넷 뱅킹용 전자통장으로도 사용할 수 있다.
SMiShing (스미싱)	휴대폰의 SMS 문자 서비스를 이용하여 바이러스와 같은 악성코드에 감염시켜 개인 정보를 빼가는 해킹 기법이다. SMS(Short Message Service, 단문 서비스)와 Phishing(피싱)이 합성된 단어이다. 해커로부터 휴대폰 문자를 받은 사용자가, 휴대폰 인터넷을 사용하여 지시된 웹사이트를 방문했을 때, 악성코드가 휴대폰으로 다운로드 되어 감염되는 시나리오를 갖는다.
Sniffing (스니핑)	네트워크상에 통과하는 패킷들의 내용을 엿보는 행위이다. 이처럼 패킷을 엿봄으로써 로그인 과정 중의 계정명과 패스워드 정보를 비롯하여 주요 내용을 불법으로 추출할 수 있다.
Social Engineering (사회 공학)	컴퓨터 시스템이나 인터넷의 물리적, 기술적 취약점을 이용하지 않고 이를 이용하는 사용자의 심리나 사회 문화적 반응을 예견하여 정보나 권한을 탈취하는 행위를 말한다.
SPAM (스팸)	SPAM은 수신자가 원하지 않는 대량의 메시지를 무차별로 보내기 위하여 대부분의 방송 미디어나 디지털 전달 시스템을 포함하여 전자적 메시지 발송 시스템을 사용하는 것을 말한다. 가장 널리 인식되는 SPAM의 형태는 이메일 SPAM이지만, 다른 미디어에서 일어나는 유사한 남용에도 이 용어는 적용된다.
Sphere Phishing (스피어 피싱)	조직 내 상급자나 관리자를 사칭하여 사원들의 개인 정보를 빼내는 해킹 행위를 말한다. Sphere(지위, 계급)와 Phishing(피싱, 개인정보탈취)의 합성어로서, 일종의 사회공학적 기법이다.
Splogger	광고와 블로그 운영자라는 단어를 결합시켜 만든 새로운 용어로서, 다른 사람이 만든 저작물을 무단으로 도용하기도 하며, 불법으로 광고물이나 음란물을 배포하는 광고성 블로거를 말한다.
Spoofing	다른 사람의 컴퓨터 시스템에 접근할 목적으로 IP 주소를

(스푸핑)	변조한 후 합법적인 사용자인 것처럼 위장하여 시스템에 접근함으로써 나중에 IP 주소에 대한 추적을 피하는 해킹 기법의 일종이다.
Spyware (스파이웨어)	사용자의 컴퓨터에 설치되어 사용자의 개인정보를 몰래 유출하는 소프트웨어로서, 처음에는 애드웨어(Adware)에서 출발하였으나 그 기능이 확대되어 보안 문제를 일으키고 있다.
SQL Injection	내부적으로 데이터베이스를 활용하는 웹 모듈에서 SQL 쿼리(query)를 처리할 때, 쿼리 내용에 사용자 인증을 우회하는 조건이나, 운영체제 명령을 직접 호출할 수 있는 명령을 삽입하여 데이터베이스 관리자 권한을 획득하는 등의 불법 공격을 행하는 것을 말한다.
SSO (Single Sign-On, 싱글 사인온)	한 번의 로그인으로 각종 업무 시스템이나 인터넷 서비스에 여러 번의 로그인 과정 없이 접속하여 이용할 수 있게 해주는 보안 응용 솔루션이다. 각 시스템마다 존재하는 사용 인증 절차를 매번 밟지 않고서도 하나의 계정에 대한 단일 로그인 만으로 다양한 시스템에 접근할 수 있어서 사용자의 편의성이 높아지고, 사용자 인증 등의 관리가 수월해진다. 인증을 위하여 주로 공개키 기반구조(PKI, Public Key Infrastructure)를 사용한다.
Stuxnet (스턱스넷)	독일 지멘스사의 SCADA(원격 감시 제어 시스템)의 제어 소프트웨어에 침입하여 시스템을 마비시킴으로써 SCADA를 활용하는 원자력발전소, 송배전망, 가스관 등을 마비시키는 악성코드를 말한다.
Switch Jamming (스위치 재밍)	네트워크 스위치 장비 내에 보관되어 있는 주소 테이블의 용량을 넘치도록 공격함으로써 스위치가 원래 기능을 잃어버리고 접수한 트래픽을 브로드캐스팅하도록 만드는 해킹 기술이다.
SYN Flooding	TCP/IP의 3-Way Handshaking 과정을 악용하여 수만 개의 SYN 패킷만을 동시에 특정 사이트에 전송함으로써 해당 사이트의 수신 큐가 오버플로우 상태가 되어 서비스가 정상적으로 이루어지지 못하도록 만드는 공격이다.

19)T

Teardrop Attack (티어 드롭 공격)	송신측에서 IP 패킷을 내보낼 때 패킷 간의 일련번호를 어긋나도록 의도적으로 고쳐서 보냄으로써 수신측에서 패킷들을 정상적으로 재조합하지 못하도록 방해하는 일종의 DoS 공격이다.

TEMPEST (Transient ElectroMagnetic Pulse Emanation Standard, 템피스트)	컴퓨터나 휴대폰과 같은 통신기기를 사용할 때 공중에 누성되는 전자파를 다른 사람이 불법으로 수신함으로써 정보가 유출되는 것을 방어하기 위한 대책이다.
Tokenization (토큰화)	모바일 결제 시스템에서 신용카드 정보를 직접 사용하지 않고 토큰으로 변환하여 사용하는 기법이다. 모바일 결제를 이용하는 각 상점에서는 신용카드 정보를 저장하지 않고 토큰 데이터만을 저장한다. 그 대신에 토큰 서버가 신용카드 정보와 토큰 데이터를 저장하여 관리한다. 따라서 토큰 데이터를 유실해도 신용카드 정보가 유출되지 않는 장점이 있는 반면, 토큰 서버에 대한 보안 강화가 필요하다. 2014년 EMV 카드 표준으로 제정되었다.
Trap Door (트랩도어)	컴퓨터 이용 범죄의 한 가지 방식으로 프로그램 코드 중에 정식 승인 절차를 거치지 않고서도 들고날 수 있도록 만들어 놓은 출입구를 말한다. 불법 정보 수집 혹은 파괴를 목적을 활용한다.
Trojan Horse (트로이 목마)	사용자에게는 마치 유용한 프로그램인 것처럼 위장하여 사용자들로 하여금 거부감 없이 설치를 유도하는 악성 프로그램이다.
Tunneling (터널링)	인터넷상에서 눈에 보이지 않는 통로를 만들어 두 지점 간에 통신을 지원한다. 하위층 통신 규약의 패킷을 캡슐화하여 상위층 통신 규약에서 다툼으로써 두 지점 간에 통신이 이루어진다. 네트워크 계층 통신 규약의 패킷을 이보다 상위 계층의 패킷을 이보다 상위 계층의 통신 규약으로 캡슐화하는 경우가 많다. 예를 들어, 멀티캐스트 통신망, IPv6 통신망(6bone)이 여기에 속한다.
Turbo code (터보 코드)	데이터 통신 중에 발생하는 비트 오류를 최소화하기 위하여 사용하는 오류 정정 부호(ECC)의 일종이다. IMT-2000이나 위성통신 시스템에서 사용한다.
Tvishing	일종의 PC인 스마트TV에 악성 소프트웨어를 설치해 스마트TV에 대한 최고 접근권한을 획득하는 일련의 행위를 말한다.

20)U

UPNP (Universal Plug & Play, 범용 플러그 앤 플레이)	기존의 PNP(Plug-and-Play, PnP, 플러그 앤 플레이)는 컴퓨터에 다양한 주변기기를 접속할 수 있도록 해주는 기술인 반면, UPNP는 가정의 홈 네트워크에 다양한 주변기기를 접속하여 공유할 수 있도록 해주는 기술이다.
USIM	인증을 목적으로 휴대전화 소유자의 개인 정보를 저장하는

(Universal Subscriber Identity Module, 범용 가입자 식별 모듈)	모듈을 이르는 말로 스마트카드로 제작된다. 휴대 전화가 분실되거나 교체되어도 소유자의 개인 정보에 대한 유지와 보호가 가능하다.
UTM (Unified Threat Management, 통합위협관리)	다양한 보안 솔루션 기능을 하나로 통합한 보안 솔루션으로서, 방화벽, 침입방지시스템(IPS), 침입탐지시스템(IDS), DB 보안, VPN, 웹 보안, 콘텐츠 보안 등 다양한 보안 솔션들이 꾸준히 개발되면서 이들 솔루션의 운용에 따라 많은 비용과 공간, 인력이 요구되므로 이를 감소시킬 목적으로 보안 솔루션들을 묶어 운영하는 기술이다.

21)V

Vandalism (반달리즘)	유럽 중세 시대 때 로마문화를 무자비하게 파괴하고 약탈했던 반달족에서 기인한 용어로서, 일반 네티즌을 대상으로 공개된 문서에 대하여 제목과 내용을 훼손, 변경, 낙서하는 행위를 가리킨다. 게시된 글을 대상으로 일부 혹은 전부를 지우거나 내용을 고의로 왜곡하는 행위이며, 욕설과 비방, 광고, 저질 낙서와 그림을 추가하는 행위를 말하는 용어이기도 하다.
VPN (Virtual Private Network, 가상사설망)	인터넷과 같이 공개된 통신기반시설을 사용하여 멀리 떨어진 사무실이나 개인 사용자에게 그들이 속한 조직의 네트워크를 안전하게 접근할 수 있도록 제공해주는 네트워크를 말한다.

22)W

Watermarking (워터마킹)	디지털 콘텐츠의 저작권을 보호하기 위하여 암호나 코드 등의 마크를 은닉 삽입하는 기술로서, 불법복제의 증거로 활용할 수 있을 뿐 아니라 불법 변조를 막을 수도 있다. 일종의 "디지털 낙관"이라고 불리며 이미지, 오디오, 동영상 등 모든 분야에 적용된다.
WEP (Wired Equivalent Privacy)	무선 LAN(Wi-Fi)의 표준을 정의하는 IEEE 802.11 규약의 한 영역으로서 무선 LAN에서 발생 가능한 보안 문제와 프라이버시 침해를 예방하기 위하여 암호 기법을 사용한다.
WPKI (Wireless PKI, 무선 공개키 기반구조)	무선 인터넷상에서의 사이버 주식 거래나 인터넷 뱅킹을 할 때 외부 침입으로부터 보호 받거나 개인 정보 누출을 예방하기 위하여 사용하는 무선 인터넷 공개키 기반 구조이다.

23)X

XSS (Cross Site Scripting)	공격자가 미리 작성해 놓은 악성 스크립트(XSS)를 인지하지 못한 피해자가 웹 브라우저를 통해서 실수로 이를 자신의 컴퓨터 안에 다운로드하여 실행함으로써 스크립트 실행 결과가 공격자에게 전달되도록 하는 공격이다.

24)Z

Zero Day Attack	시스템이나 네트워크의 취약점이 발표되어 이에 대한 대책이 수립되어 적용되기도 전에 먼저 이루어진 취약점 기반 공격을 말한다.
ZeuS	사용자의 온라인 뱅킹 로그인 정보를 훔칠 목적으로 설계된 범죄용 소프트웨어 도구로서 인터넷 뱅킹용 악성코드를 만들고 이와 관련된 봇넷(BotNet)을 생성한다.
Zombie (좀비)	컴퓨터상에 악의적으로 사전에 설치됨으로써 나중에 해커로부터 조정당하여 시스템을 공격하거나 서비스 방해에 동원되는 악성코드 혹은 악성코드가 설치된 컴퓨터를 말한다.