1. 공단 공개 문제

* 전산실 관리자가 시스템 관리(보안, 해킹, 백업 등)를 위한 용어들 출제

1번) 정보시스템 운영 중 자연 재해나 시스템 장애 등의 이유로 대고객 서비스가 불가능한 경우가 종종 발생한다. 이와 같은 상황에서의 "비상사태 또는 업무중단 시점부터 업무가 복구되어 다시 정상가동 될 때까지의 시간" 을 의미하는 용어를 쓰시오. [배점 5]

o 답 : 목표 복구 시간

* 목표 복구 시간(RTO; Recovery Time Objective)

* RPO (Recovery Point Objective, 목표 복구 시점) [산업 12년3회]

: 조직에서 발생한 여러 가지 재난 상황으로 IT 시스템이 마비되었을 때 각 업무에 필요한 데이터를 여러 백업 수단을 활용하여 복구할 수 있는 기준점. 복구가 필요한 업무에 대하여 어느 시점까지 데이터가 필요한가에 따라 시점을 정한다.

2번) IT 인프라 서비스 연속성을 위해서는 백업시스템을 운영 관리하는 것이 필수적이다. 특히 대규모의 정보시스템은 그 데이터의 특성상 체계적인 백업이 요구된다. 이러한 백업 방식 중 Incremental Backup에 대하여 설명하시오. [배점 5점]

o 답 : 백업 대상 데이터 영역 중 변경되거나 증가된 데이터만을 백업 받는 방식

* 백업 방식

- 전체 백업 : 데이터 전체 백업
- 증분 백업(Incremental Backup): 백업 대상 데이터 영역 중 변경되거나 증가된 데이터만을 백업 받는 방식

[신기술 - 시스템 관리1]

3번) 다음 IT 보안관리에 관련된 <실무 사례>를 분석하여 괄호 ( )의 내용에 공통적으로 적용될 수 있는 기술을 영문 완전이름(Full-name) 또는 약어(약자)로 쓰시오. [배점 2]

<실무 사례>

컨설팅 업체 가칭 A사는 모처럼 대형 고객인 B사 수주를 앞두고 있었다. 하지만 최종 계약을 앞두고 날아 들은 B사의 요구에 당황하고 있다. B사는 "A사가 컨설팅 과정에서 공유하는 우리 정보를 사원 누구도 유출할 수 없다는 기술적인 증거를 대야 한다"는 조건을 걸었다. A사의 보안 시스템은 방화벽 밖에 없는 실정에서 이를 해결하기 위해서는 상당한 고민을 해야 했다.

그래서 보안 전문가인 귀하에게 의뢰한 결과 귀하께서는 다음과 같은 해석을 내놓았다. "기술적 증거"는 바로 ( ) 입니다. ( )은(는) 기업 내 주요 정보의 생성부터 보관, 유통, 폐기와 같은 전 과정을 통제하는 솔루션으로 콘텐츠 인증, 권한제어, 부정사용방지 등이 대표 기술이며, 흔히 ( )을(를) 문서 보안이라 생각할 수 있지만, 넓은 의미에서 음악이나 동영상 등에 대한 저작권 관리 기술도 포함됩니다. 관련 업계에서는 이를 구분해 기업용 문서 보안은 엔터프라이즈 ( ), 저작권 관리는 컨소머 ( )(으)로 지칭하고 있습니다.

o 답 : DRM

* 지문은 2007년 8월 기사에서 발췌됨

[신기술 - 시스템 관리1]

4번) 다음 신기술 동향과 관련된 설명에 가장 부합하는 용어를 쓰시오. [배점 3]

고정된 유선망을 가지지 않고 이동 호스트(Mobile Host)로만 이루어진 통신망으로 네트워크에서 각각의 이동 노드는 단지 호스트가 아니라 하나의 라우터로 동작하게 되며, 다른 노드에 대해 다중 경로를 가질 수 있다. 또한 동적으로 경로를 설정할 수 있기 때문에 기반구조 없는 네트워킹이라고도 한다.

o 답 : Ad-hoc

* Ad-hoc network (애드혹 네트워크)
: 노드(node)들에 의해 자율적으로 구성되는 기반 구조가 없는 네트워크.

5번) 다음 신기술 동향과 관련된 설명에 가장 부합하는 용어를 쓰시오. [배점 2]

기존의 교통체계에 전자, 정보, 통신, 제어 등의 지능형 기술을 접목시킨 차세대 교통체계로 교통 관련 정보와 기상 정보, 도로상태 정보 등을 수집, 처리, 가공하여 유, 무선 통신 수단을 이용해서 도로변 교통 단말기, 차내 단말기, 교통 방송, PC 통신, 전화 등으로 차량 운전자 및 여행객들에게 전달함으로써 통행의 편의와 교통량의 원활한 소통을 이루기 위한 시스템이다.

o 답 : ITS

* ITS (Intelligent Transport Systems, 지능형 교통 체계) [기사 16년1회]

[신기술 - 시스템 관리1]

6번) IT 보안 관리 실무와 관련된 <실무 사례>에서 다음 괄호 ( ) 안에 가장 적합한 용어를 영문 약어(약자)로 쓰시오. [배점 10]
<실무 사례>

WEP는 무선랜의 표준인 IEEE 802.11 규약의 일부분으로 무선랜 간에 자료를 보호하기 위해 사용되는 알고리즘이다. 그러나 WEP는 수만개 정도의 패킷에 의한 공격에 그 키가 쉽게 해독이 가능하며, 이에 따라 WPA 기술이 와이파이 얼라이언스(Wi -Fi Alliance)에 의해서 무선랜에서 보안을 수행하기 위하여 제작된 프로토콜로 WEP의 취약점의 대안으로 개발되었다. 암호화나 인증을 위한 키가 고정되어 있기 때문에 고정 WEP는 보안 측면에서 많은 문제점을 갖고 있다. WEP는 키를 가지고 있는지의 여부로 기계를 인증하는 반면에 ( )는 네트워크 관리자가 사용자들을 인증할 수 있도록 한다. 즉 사용자가 네트워크에 합법적으로 접속했는지 접속할 권한이 있는지를 인증 서버를 통해 인증하도록 하는 프로토콜이다.

o 답 : 802.1X

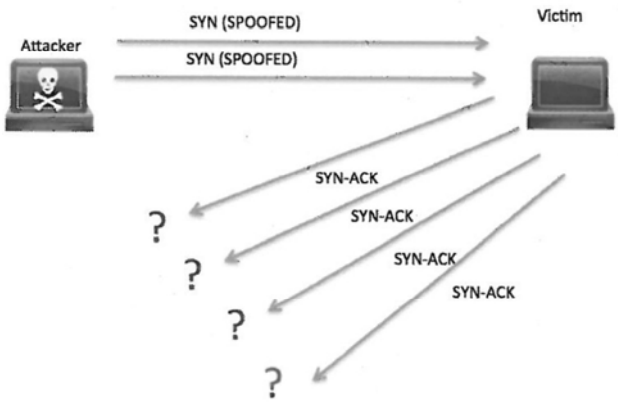
* WEP (Wired Equivalent Privacy, 유선급 프라이버시) [기사 11년2회]
: 유선 랜(LAN)에서 기대할 수 있는 것과 같은 보안과 프라이버시 수준의 무선 랜(WLAN)의 보안 프로토콜.
* Wi-Fi Alliance
: 무선랜 기술을 장려하고 표준을 준수하면 제품을 인증해 주는 동업 조합 (Wi-Fi는 와이파이 얼라이언스의 상표명)

[신기술 - 시스템 관리1]

* WPA (Wi-Fi Protected Access) [기사 11년2회]
: Wi-Fi에서 제정한 무선 랜(WLAN) 인증 및 암호화 관련 표준. 암호화는 웹 방식을 보완한 IEEE 802.11i 표준의 임시 키 무결성 프로토콜(TKIP)을 기반으로 하며, 인증 부문에서도 802.1x 및 확장 가능 인증 프로토콜(EAP)을 기반으로 상호 인증을 도입해 성능을 높였다. 특히 패킷당 키 할당 기능, 키값 재설정 등 다양한 기능이 있기 때문에 해킹이 불가능하고 네트워크에 접근할 때 인증 절차를 요구한다.

* EAP (Extensible Authentication Protocol, 확장성 인증 프로토콜)
: 무선망과 점 대 점 통신 규약(PPP: Point-to-Point Protocol)에서 사용되며 확장이 용이하도록 고안된 인증 방법.

7번) 정보시스템의 보안 관리와 관련하여 다음 〈개념도〉가 설명하는 DoS 공격 유형의 이름을 쓰시오. [배점 3]



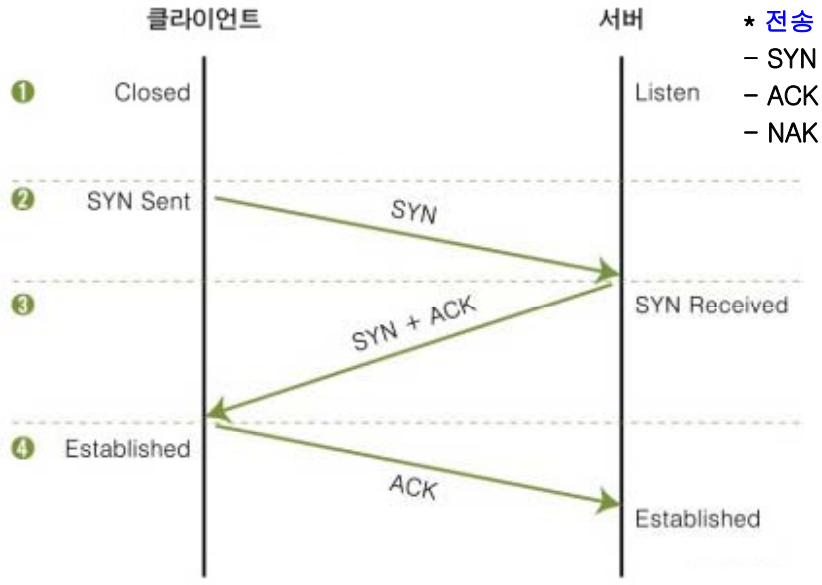
o 답 : SYN Flooding

* SYN Flooding 공격
: 대량의 SYN(동기 제어 문자, [기사 11년1회]) packet을 이용해서 타켓 서버의 서비스를 더 이상 사용할 수 없도록 만드는 공격 기법
- TCP 3-way handshaking 문제점 이용
- 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 함. 서버에 다시 ACK 패킷을 보내야 연결이 되는데, 보내지 않으면 대기 상태가 됨.

5

[신기술 - 시스템 관리1]

* TCP 3-way handshaking



* 전송 제어 문자
- SYN (SYNchronous idle) : 동기 문자
- ACK (ACKnowledge) : 긍정 응답
- NAK (Negative AcKnowledge) : 부정 응답

2. 보안 요소

1) 기밀성(Confidentiality)
: 인가(authorization)된 사용자만 정보 자산에 접근할 수 있는 것(ex. 방화벽, 암호)
2) 무결성(Integrity)
: 적절한 권한을 가진 사용자에 의해 인가된 방법으로만 정보를 변경할 수 있도록 하는 것(ex. 지폐는 오직 정부(적절한 권한을 가진 사용자)만이 한국은행을 통해(인가된 방법으로만) 만들거나 변경할 수 있다.)
3) 가용성(Availability)
: 정보 자산에 대해 적절한 시간에 접근 가능한 것을 의미한다. (ex. 24시간 편의점은 밤이든 낮이든 무엇인가 필요할 때 항상 얻을 수 있다. → 가용하다.)
4) 인증(Authentication) [기사 09년4회]
: 다중 사용자 컴퓨터 시스템 또는 망 운용 시스템에서, 시스템이 단말 작동 개시(log-on) 정보를 확인하는 보안 절차
5) 부인 방지(Non-Repudiation)
: 메시지의 송수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 사후에 증명함으로써 사실 부인을 방지하는 보안 기술. (ex. 전자 우편이나 메시지를 송신하고도 송신하지 않았다고 주장하는 송신자의 부인을 막는 송신 부인 방지)
6) 접근 제어(Access Control)
: 정보 보안 정책에 따라 사용자, 프로그램, 프로세서, 시스템 등을 허가된 주체만이 정보 시스템 자원에 접근할 수 있도록 제한하는 것

* 정보보안 3원칙: 기밀성, 무결성, 가용성

3. 시스템 보안 기능

* 시스템 보안
: 권한 없는(허가받지 않은) 사용자에 의한 파일, 폴더 및 장치 등의 사용을 제한하여 보호하는 시스템 기능

1) 계정과 패스워드 관리
: 적절한 권한을 가진 사용자를 식별하기 위한 가장 기본적인 인증 수단
2) 세션 관리
: 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대한 관리로서, 일정 시간이 지날 경우 적절히 세션을 종료하고, 비인가자에 의한 세션 가로채기를 통제(ex. 자동 로그 오프)
3) 접근 제어
: 시스템이 네트워크 안에서 다른 시스템으로부터 적절히 보호될 수 있도록 네트워크 관점에서 접근을 통제.
4) 권한 관리
: 시스템의 각 사용자가 적절한 권한으로 적절한 정보 자산에 접근할 수 있도록 통제
5) 로그 관리
: 시스템 내부 혹은 네트워크를 통한 외부에서 시스템에 어떤 영향을 미칠 경우 해당 사항을 기록
6) 취약점 관리
: 시스템은 계정과 패스워드 관리, 세션 관리, 접근 제어, 권한 관리 등을 충분히 잘 갖추고도 보안적인 문제가 발생할 수 있는데, 이는 시스템 자체의 결함에 의한 것이다. 이 결함을 체계적으로 관리하는 것이 취약점 관리

4. 네트워크 보안(공격, 해킹)

1) 서비스 거부(Dos) 공격
- 취약점 공격형(Land 공격)
- 자원 고갈 공격형(Ping of Death, SYN Flooding, HTTP GET Flooding, HTTP CC, 동적 HTTP Request Flooding, Smurfing, Mail Bomb)
- 분산 서비스 거부(DDos) 공격

2) 스니핑 공격
- 스니핑
- 스위치 재밍
- SPAN 포트 태핑

3) 스푸핑 공격

4) 세션 하이재킹 공격

* LAND Attack (Local Area Network Denial Attack)
: 공격자가 패킷의 출발지 주소(Address)나 포트(port)를 임의로 변경하여 출발지와 목적지 주소(또는 포트)를 동일하게 함으로써, 공격 대상 컴퓨터의 실행 속도를 느리게 하거나 동작을 마비시켜 서비스 거부 상태에 빠지도록 하는 공격 방법. 수신되는 패킷 중 출발지 주소(또는 포트)와 목적지 주소(또는 포트)가 동일한 패킷들을 차단함으로써 이 공격을 피할 수 있다.

* Ping of Death (죽음의 핑)
: 인터넷 프로토콜 허용 범위(65,536 바이트) 이상의 큰 패킷을 고의로 전송하여 발생한 서비스 거부(DoS) 공격.

* HTTP GET Flooding
: 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것. 공격 패킷을 수신하는 웹 서버는 정상적인 TCP 세션과 함께 정상적으로 보이는 HTTP Get 요청을 지속적으로 요청하게 되므로, 시스템에 과부하가 걸린다.

* HTTP CC
: HTTP 1.1 버전의 CC(Cache-Control) 헤더 옵션은 자주 변경되는 데이터에 대해 새롭게 HTTP 요청 및 응답을 요구하기 위하여 캐시(Cache) 기능을 사용하지 않게 할 수 있다. 서비스 거부 공격 기법에 이를 응용하기 위해 'Cache-Control: no-store, must-revalidate' 옵션을 사용하면 웹 서버는 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가하게 된다.

* 동적 HTTP Request Flooding
: HTTP Get Flooding 공격이나 HTTP CC 공격은 일반적으로 지정된 웹 페이지를 지속적으로 요청하는 서비스 거부 공격이다. 그러나 이 두 가지 공격은 웹 방화벽을 통해 특징적인 HTTP 요청 패턴을 방어할 수 있다. 동적 HTTP Request Flooding은 이러한 차단 기법을 우회하기 위해 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청하는 기법.

* Smurfing (스머핑)
: 고성능 컴퓨터를 이용해 초당 엄청난 양의 접속신호를 한 사이트에 집중적으로 보냄으로써 상대 컴퓨터의 서버를 접속 불능 상태로 만들어 버리는 해킹 수법

* Mail Bomb (메일 폭탄)
: 스팸을 이용한 대량 메일을 전송

* DDos (Distributed Denial of Service attack, 분산 서비스 거부 공격)
: 감염된 대량의 숙주 컴퓨터를 이용해 특정 시스템을 마비시키는 사이버 공격. 공격자는 다양한 방법으로 일반 컴퓨터의 봇을 감염시켜 공격 대상의 시스템에 다량의 패킷이 무차별로 보내지도록 조정한다. 이로 인해 공격 대상 시스템은 성능이 저하되거나 마비된다.

* Sniffing (스니핑)
: 네트워크의 중간에서 남의 패킷 정보를 도청하는 해킹 유형의 하나.

* Snooping (스누핑)
: 네트워크상에서 남의 정보를 염탐하여 불법으로 가로채는 행위

* Spoofing (스푸핑, 속이다)
: 승인받은 사용자인 것처럼 속이는 것
- IP Spoofing: IP 속임, ARP Spoofing: MAC주소 속임

* 스위치 재밍 (Switch Jamming)
: 위조된 매체 접근 제어(MAC) 주소를 지속적으로 네트워크로 흘려 보내 스위치 저장 기능을 혼란시켜 더미 허브(dummy hub)처럼 작동토록하는 공격. 스위치를 직접 공격하며, MAC 테이블을 위한 캐시 공간에 버퍼 오버플로 공격을 실시하는 것과 같다.

* SPAN 포트 태핑 (Switch Port Analyzer)
: 스위치의 포트 미러링(Port Mirroring) 기능을 이용한 것. 포트 미러링이란 각 포트에 전송되는 데이터를 미러링하고 있는 포트에도 똑같이 보내주는 것으로, 침입 탐지 시스템이나 네트워크 모니터링 또는 로그 시스템을 설치할 때 많이 사용한다.

* Session Hijacking (세션 하이재킹)
: 다른 사람의 세션 상태를 훔치거나 도용하여 액세스하는 해킹 기법.

5. 파일 보호 기법

1) 파일의 명명 (Naming)
: 파일 이름을 모르는 사용자를 접근 대상에서 제외시키는 기법

2) 비밀번호 (Password, 암호)
: 각 파일에 판독 암호와 기록 암호를 부여하여 암호를 아는 사용자에게만 접근을 허용하는 기법

3) 접근 제어 (Access Control)
: 사용자의 신원에 따라 서로 다른 접근 권한을 허용한다 (접근 제어 행렬 응용)

6. 보안 기법

1) 외부 보안 : 불법 침입자나 천재지변으로부터 시스템을 보호하는 것
- 시설 보안 : 감지 기능을 통해 외부 침입자나 화재,홍수와 같은 천재지변으로부터의 보안

2) 내부 보안 : 하드웨어나 운영체제의 내장된 기능

3) 사용자 인터페이스 보안 : 사용자의 신원을 운영체제가 확인하는 절차를 통해 불법침입자로부터 보호

7. 자원 보호 기법

: 컴퓨터 시스템에서 사용되는 자원들(파일, 프로세스, 메모리 등)에 대하여 불법적인 접근방지와 손상 발생 방지

1) 접근 제어 행렬(access control matrix)
: 자원 보호의 일반적인 모델로, 객체에 대한 접근 권한을 행렬로써 표시한 기법

영역 \ 객체	파일	프로세스	메모리
권우석	E	REW	E
김영희	RW	NONE	R

- 권한 (E : 실행가능, R : 판독가능, W : 기록가능, NONE : X)

객체	접근 제어 리스트
파일	(권,E), (김,RW)
프로세스	(권,REW)
메모리	(권,E), (김,R)

2) 접근 제어 리스트(access control list) → 접근제어행렬에서 열(객체) 중심
: 객체와 그 객체에 허용된 조작 리스트 이며, 영역과 결합되어 있으나 사용자에 의해 간접적으로 액세스되는 기법

3) 권한 리스트(capability list) → 접근제어행렬에서 행(영역) 중심
: 접근 제어 행렬에 있는 각 행, 즉 영역을 중심으로 구성한 것으로서 각 사용자에 대한 자격들로 구성되며, 자격은 객체와 그 객체에 허용된 연산 리스트

권우석	
파일	E
프로세스	REW
메모리	E

김영희	
파일	RW
프로세스	NONE
메모리	E

8. 기타 용어 (기출 용어 포함)

* 키워드 위주로 용어를 암기하세요.
- 서술형 문제도 키워드를 포함해서 입력하면 부분점수 이상 인정됩니다.
- 시험 일주일 전부터 집중적으로 암기하세요.

* CAPTCHA (캡차, Completely Automated Public Turing test to tell Computers and Humans Apart, 자동 계정 생성 방지 기술)
: 주로 웹사이트 회원 가입 절차에서 사용자가 사람인지 컴퓨터인지를 판별하기 위한 시도 응답 인증 방식

* Biometrics (생체 인식)
: 사람의 신체적, 행동적 특징을 자동화된 장치로 추출하고 분석하여 정확하게 개인의 신원을 확인하는 기술.

* Escrow Service (에스크로(임치) 서비스)
: 전자 상거래 등에서 구매자와 판매자 사이에 중개 서비스 회사가 개입해 상품 인도와 대금 지불을 대행해 주는 서비스. 소비자의 피해를 최소화하기 위해 도입된 제도로 대부분 오픈 마켓을 운영하는 업체들은 이 제도를 도입, 운영하고 있다.

* Software Escrow (소프트웨어 에스크로(임치))
: 소프트웨어 개발자의 지식재산권을 보호하고 사용자에게는 저렴한 비용으로 소프트웨어를 안정적으로 사용하고 유지 보수를 받을 수 있도록 하기 위해서 소스 프로그램과 기술 정보 등을 제3의 기관에 보관하는 것. 소프트웨어 에스크로(임치)의 목적은 소프트웨어 저작재산권자의 지식재산권을 보호하며, 저작재산권자의 폐업, 파산, 소프트웨어 개발 관련 정보 멸실 등의 사건이 발생할 경우 소프트웨어 사용 권한이 있는 사용자에게 보관된 자료를 제공하는 등 정당한 사용자의 권리를 보장하는 데 있다.

[신기술 - 시스템 관리1]

* Splogger (스플로거)
: 스팸(spam)과 블로거(blogger)의 합성어로 다른 사람의 콘텐츠를 무단으로 복사해 자신의 블로그에 게재하는 블로거 또는 제품 광고나 음란물 등을 유포하는 광고성 블로거.

* Cyber Stalking (사이버 스토킹)
: 정보 통신망을 이용해 악의적인 의도로 지속적으로 공포감이나 불안감 등을 유발하는 행위.

* Vandalism (반달리즘)
: 다수가 참여할 수 있도록 공개된 문서의 내용을 훼손하거나 엉뚱한 제목으로 변경하고 낙서를 하는 일. 유럽 중세시대의 민족이동 당시에 악평이 자자하던 반달족의 무자비한 로마문화 파괴 및 약탈 행위를 비유하는 말이다.

* CLMS (Copyright License Management System, 저작권 라이선스 통합 관리 시스템)
: 정부가 디지털 저작물에 대한 체계적인 관리를 위해 추진하고 있는 시스템. 정부와 저작권 관련 단체는 저작권의 이용 계약 체결과 사용 내역 등 통합적인 관리를 위해 저작권 라이선스 통합 관리 시스템 구축을 추진해 왔다. 적용 분야도 음악과 어문 분야에 이어 영화 등 각종 영상과 외국 음악, 나아가 방송 콘텐츠까지 구축을 확대하고 있다.

* MODEM (Modulator-Demodulator, 변복조기)
: 컴퓨터나 단말 등에서 나가는 디지털 신호를 아날로그 신호로 변환하고(변조기), 들어오는 아날로그 신호를 디지털 신호로 변환하는(복조기) 역할

[신기술 - 시스템 관리1]

* MAN (Metropolitan Area Network, 도시권 통신망)
: 구내 정보 통신망(LAN)과 광역 통신망(WAN)의 중간 정도의 지역을 망라하는 정보 통신망.

* u-Health
: 정보통신기술(ICT)을 의료 서비스에 접목하여 언제 어디서나 이용 가능한 원격 의료 및 건강 관리 서비스.

* Digerati (디저라티)
디지털(digital)과 리터라티(literati)의 합성어로 컴퓨터, 정보 통신 등 디지털 분야의 지식이 많은 사람을 지칭하는 용어. 즉, 디지털 사회에서 정보 통신 산업을 이끌어 가는 사람을 말한다.

* PostNet (Postal Numeric Encoding Technique)
: 우체국 택배와 국제 특별 수송(EMS)을 강화하기 위해 우편물에 RFID 칩을 달아 언제 어디서나 실시간으로 그 우편물의 위치를 확인할 수 있는 우편 물류 시스템.

* DMB (Digital Multimedia Broadcasting 디지털 멀티미디어 방송) → 손 안의 TV
: 음성, 영상 등 다양한 멀티미디어 신호를 디지털 방식으로 고정·휴대·차량용 수신기에 제공하는 방송 서비스.
- 위성 DMA: 위성 전파를 통해 전국의 DMB 단말기에 방송을 전달
- 지상파 DMA: 지상파 방속국(KBS 등)의 기지국을 통해 방송을 전달

* 케듀롬 (Keduroam)
: 국공립 대학 정보기관 협의회에서 운영하고 있는 무선랜 공동 사용 서비스. 국공립대학 간 별도의 회원 가입 없이 이용자 소속 대학에서 사용 중인 아이디(ID)로 다른 학교에서도 무선랜 서비스를 이용.

[신기술 - 시스템 관리1]

* deep learning
: 컴퓨터가 여러 데이터를 이용하여 마치 사람처럼 스스로 학습할 수 있게 하기 위해 인공 신경망(ANN: Artificial Neural Network)을 기반으로 하는 기계 학습 기술. (ex. 알파고 바둑)

* IPA (Intelligent Personal Assistant 지능형 가상 비서)
: 개인 비서처럼 사용자가 요구하는 작업을 처리하고 사용자에게 특화된 서비스를 제공하는 소프트웨어 에이전트. 인공 지능(AI) 엔진과 음성 인식을 기반으로 사용자에게 맞춤 정보를 수집하여 제공하고, 사용자의 음성 명령에 따라 일정 관리, 이메일 전송, 식당 예약 등 여러 기능을 수행한다.
- 애플(Apple) 시리(siri), 구글의 구글나우(Google Now), 마이크로소프트의 코타나(cortana)

* TensorFlow (텐서플로)
:구글(Google)사에서 개발한 기계 학습(machine learning: 인공 지능의 한 분야로 컴퓨터가 학습할 수 있도록 하는 알고리즘과 기술을 개발하는 분야) 엔진.

* 누름힘 접촉 (force touch)
: 터치스크린에 손가락으로 누르는 힘의 강도를 인식하여 다르게 동작하는 촉각 센서 기술.

* 인터클라우드 컴퓨팅 (inter-cloud computing)
: 둘 이상의 클라우드 서비스 제공자 간의 상호 연동을 가능케 하는 기술.

* 증발품 (vaporware)
: 판매 계획 또는 배포 계획은 발표되었으나 실제로 고객에게 판매되거나 배포되지 않고 있는 소프트웨어

[신기술 - 시스템 관리1]

* 인터넷 삼진아웃제 (Internet Strike-out)
: 저작권법에 따라 정부가 불법 복제물 따위의 복제·전송으로 3회 이상 경고한 복제·전송자에게 해당 온라인 서비스 제공자가 6개월 안으로 기간을 정하여 해당 복제·전송자의 계정을 정지할 것을 명령하는 것.

* 손가락 정맥 지불 (finger vein money)
: 손가락 정맥의 형태를 인식기로 읽어 본인 여부를 판단, 대금을 지불하는 방식.

* DRP (disaster recovery plan, 재난 복구 계획)
: 시설의 하드웨어나 소프트웨어상의 재해나 재난 발생에 대비하여, 실제 상황이 발생했을 때 취해야 할 행동 계획을 미리 준비하는 것.

* Hotspot (핫스폿)
: 무선 랜을 통하여 인터넷에 접속할 수 있는 지역. 공항, 호텔, 커피숍, 전시장, 도심지 번화가 등 비교적 소규모 공간에 사용자가 밀집된 지역에 제공되는 와이파이존이 좋은 예이다.

* IDC (Internet Data Center)
: 전자 상거래를 행하는 기업으로부터 서버를 맡아서 그 기업의 인터넷 사업을 운용/대행하는 시설.

* IT 규제준수 (IT Compliance)
: 기업의 활동이 정보시스템에 의존하는 바, 고객의 개인정보 보호, 자료의 보관, 기업의 회계 및 재무보고의 신빙성을 투명하게 하기 위해, 기업이 따라야 하는 규정과 지침 및 법규를 준수하는 것.

[신기술 - 시스템 관리1]

* 그린 IT
: 정보 기술 전 분야에서 유해 물질 사용을 자제하고 에너지 절감을 통해 친환경 제품과 서비스를 제공하는 개념.

* 녹색 기술 (Green Technology)
: 에너지와 자원을 절약하고 효율적으로 사용하여 온실 가스 및 오염 물질의 배출을 최소화하는 기술.

* social search
: SNS 상의 콘텐츠처럼 이용자들이 이전에 만들어 놓은 데이터베이스에서 콘텐츠를 검색하는 서비스.

* digilog
: Digital과 Analog의 합성어로 디지털 기술과 아날로그적 정서가 결합한 제품과 서비스, 또는 아날로그 시대에서 디지털 시대로 넘어가는 변혁기에 위치한 세대.

* foodtech (먹거리테크)
: 최신 정보기술(IT)을 활용한 음식 관련 서비스를 칭하는 신조어. 빅 데이터, 블루투스 비콘(beacon), 온오프라인 연결 비즈니스(O2O) 등과 같은 최신 IT를 활용하여 사용자에게 맛집 추천, 식당 예약, 음식 주문 등의 서비스를 편리하게 제공한다.

* telematics
: 텔레커뮤니케이션(telecommunication)과 인포매틱스(informatics)의 합성어로, 자동차 안의 단말기를 통해서 자동차와 운전자에게 다양한 종류의 정보 서비스를 제공해 주는 기술. 자동차에 위치 측정 시스템(GPS)과 지리정보 시스템(GIS)을 장착하고 운전자와 탑승자에게 교통 정보, 응급 상황 대처, 원격 차량 진단, 인터넷 이용 등 각종 모바일 서비스를 제공하는 것이다.