



13주차: 사회공학



ChulSoo Park

School of Computer Engineering & Information Technology

Korea National University of Transportation

E-Mail : pcs8321@naver.com

학습목표 (13주차)

- 사회공학(Social Engineering) 이해
- 사회공학의 위험성 이해
- 다양한 사회공학 기법 파악
- 사회공학 기법에 대응하는 방법 학습

12 CHAPTER

사회공학 (social engineering)



CONTENTS

1. 사회공학의 이해
2. 사회공학 기법
3. 사회공학 사례와 대응책
4. 8장 전자상 거래 보안
가상화폐, 암호화 통신, 콘텐츠 보안

1. 사회공학의 이해

1 사회공학의 개념

사회공학 동영상



1. 사회공학의 이해

1 사회공학의 개념

- 컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 이용하여 사람을 속여 정상 보안 절차를 깨뜨리고 비기술적인 수단으로 정보를 얻는 행위
- 조직의 보안 수준을 높이기 위해서는 사회공학 공격에 대한 조직 구성원의 보안 의식이 절실히 필요

사회공학을 잘 이용하는 케빈 미트닉 CNN 인터뷰

회사는 방화벽이나 침입탐지 시스템, 암호, 그리고 각종 보안 기술에 수십만 달러를 쓴다. 하지만 해킹 공격자가 믿을 만한 사람(이용할 수 있는 사람)이 공격자를 도와준다면 보안을 위해 쓴 돈은 아무 쓸모 없는 돈이 된다.(무용 지물)

if an attacker can call one trusted person within the company.

1. 사회공학의 이해

1 사회공학의 개념

- 조직에서 각종 점검을 이유로 패스워드를 물어보면 많은 사람이 의심 없이 패스워드를 알려줌
- 개인용 이메일과 인터넷 뱅킹의 패스워드를 동일하게 사용하는 사람
- 전산실에 각종 장비를 정기점검(예방정비, PM, Preventive maintenance)하러 온 협력 직원이라면 전산실의 서버에 접근하여 백도어 설치가 용이함.



1. 사회공학의 이해

1 사회공학의 개념

유지보수를 진행할 가능성이 높은 기업의 IT 자산

협력 업체	협력 업체
PIS 유지보수	유지보수로 메신저
TMS 유지보수	유지보수로 무선랜
거래명세서의	유지보수로 무정전전원공급장치
고속프린터 리본외	유지보수로 상상플러스 시스템
공사비 전산장비실유지보수	유지보수로 서버가상화
네트워크품질관리시스템(패킷로직)	유지보수로 서버가상화 이중화
보안관제 보안관제 서비스	유지보수로 세종IDC(Internet Data Center 사용
소프트웨어 라이선스	유지보수로 싱글사인온(SSO)
소프트웨어 오라클스탠다드	유지보수로 영업지원시스템 개발툴
시스템 유지보수비	유지보수로 유해차단소프트웨어
유지보수 경영계획시스템(MPS)	유지보수로 인사정보
유지보수로 DB ERP모니터링	유지보수로 전산장비(서버및스토리지)
유지보수로 DB MS-SQL	유지보수로 전자결재, 메일, 메신저 시스템
유지보수로 DB TMS모니터링	유지보수로 전자문서
유지보수로 DB리오그	유지보수로 전자세금계산서
유지보수로 EIS	유지보수로 접근통제및암호화
유지보수로 ERP긴급지원(ACS)	유지보수로 차세대UTM 1차,2차
유지보수로 ERP및DB	유지보수로 통신회선및장비
유지보수로 ERP서버및 스토리지	유지보수로 통합백업시스템
유지보수로 IT자산관리	유지보수로 팔콘CDP 백업시스템
유지보수로 PC및프린터	유지보수로 항온항습기
유지보수로 POP시스템 관리	유지보수로 회선품질
유지보수로 PRM	유지보수로 휴폐업조회이용료
유지보수로 SCM공급망시스템	임차료 DR센터유 닉스서버(M10-4)
유지보수로 TMS솔루션 및 통신스위치	임차료 ERP서버
유지보수로 TMS이중화솔루션	전산비용
유지보수로 Vmware	전산사용료 E2K 200 임대비용
유지보수로 WAS	전산사용료 인터넷 AS유지수수료(연간)
유지보수로 개인정보 웹방화벽	전산소모품 PC관련부품
유지보수로 그룹웨어및지식관리	전산소모품 기타
유지보수로 네트워크 모니터링 시스템	전산소모품 서버및주변장치관련부품
유지보수로 네트워크백본	전산소모품 프린터리본및카트리지
유지보수로 네트워크이블	컨설팅료 서버성능평가및튜닝
유지보수로 동영상스트림서비스	통신회선료 LG
유지보수로 레이저프린터	통신회선료 기타
유지보수로 매입통합시스템	통신회선료 세종

1. 사회공학의 이해

2 사회공학에 취약한 조직

- **직원 수가 많은 조직**
 - ✓ 서로 얼굴을 모르는 직원도 많아서 낯선 사람에 대한 경계심이 낮음
- **구성체가 여러 곳에 분산되어 있는 조직**
 - ✓ 다른 지점의 직원으로 가장하여 접근하기 쉬움
- **조직원의 개인 정보를 쉽게 획득할 수 있는 조직**
 - ✓ 조직 내에서 쉽게 획득한 개인 정보를 이용하여 공격 대상을 잘 알고 있는 것처럼 속여서 더 높은 수준의 정보 획득 가능
- **보안 교육을 하지 않는 조직**
 - ✓ 사회공학 공격에 대한 대응책이 마련되어 있지 않아 정보 유출이 쉬움
- **정보의 분류와 관리가 허술한 조직**
 - ✓ 정보는 중요도에 따라 분류 및 관리해야 하는데 이러한 분류가 명확하지 않은 조직에서는 정보가 쉽게 노출될 수 있음

1. 사회공학의 이해

3 사회공학에 공격 대상

- **정보의 가치를 모르는 사람**

- ✓ 업무와 직접 관련이 없는 사람은 정보의 가치를 알지 못하여 자신도 모르게 유출할 수 있음

- **특별한 권한을 가진 사람**

- ✓ 업무용 그룹웨어에서 정보에 접근하기 쉬운 특별한 권한을 가진 사람을 속여 공격 대상의 패스워드를 바꾼 뒤 해당 그룹웨어에 로그인할 수 있음

- **제조사 또는 판매사**

- ✓ 공격 대상 회사의 정보를 많이 알고 있고 시스템에 대한 접근 권한과 유지, 보수용 계정을 가지고 있어 정보 획득 가능

- **새로 들어온 사람**

- ✓ 낯선 사람과 새로운 환경에 적응하려고 경계심을 풀 때 회사 조력자로 가장하여 신상 정보나 시스템 접근 정보를 얻을 수 있음

1. 사회공학의 이해

1 사회공학의 개념

사회공학 동영상(1),2,3



1. 사회공학의 이해

3 사회공학에 공격 대상

법무팀 사례(법무 및 규정 시스템)

협력 업체	협력 업체
PIS 유지보수	유지보수로 메신저
TMS 유지보수	유지보수로 무선랜
거래명세서외	유지보수로 무정전전원공급장치
고속프린터 리본외	유지보수로 상상플러스 시스템
공사비 전산장비실유지보수	유지보수로 서버가상화
네트워크품질관리시스템(패킷로직)	유지보수로 서버가상화 이중화
보안관제 보안관제 서비스	유지보수로 세종IDC(Internet Data Center 사용
소프트웨어 라이선스	유지보수로 싱글사인온(SSO)
소프트웨어 오라클스탠다드	유지보수로 영업지원시스템 개발툴
시스템 유지보수비	유지보수로 유해차단소프트웨어
유지보수 경영계획시스템(MPS)	유지보수로 인사정보
유지보수로 DB ERP모니터링	유지보수로 전산장비(서버및스토리지)
유지보수로 DB MS-SQL	유지보수로 전자결재, 메일, 메신저 시스템
유지보수로 DB TMS모니터링	유지보수로 전자문서
유지보수로 DB리오그	유지보수로 전자세금계산서
유지보수로 EIS	유지보수로 접근통제및암호화
유지보수로 ERP긴급지원(ACS)	유지보수로 차세대UTM 1차,2차
유지보수로 ERP및DB	유지보수로 통신회선및장비
유지보수로 ERP서버및 스토리지	유지보수로 통합백업시스템
유지보수로 IT자산관리	유지보수로 팔콘CDP 백업시스템
유지보수로 PC및프린터	유지보수로 항온항습기
유지보수로 POP시스템 관리	유지보수로 회선품질
유지보수로 PRM	유지보수로 휴폐업조회이용료
유지보수로 SCM공급망시스템	임차료 DR센터유 닉스서버(M10-4)
유지보수로 TMS솔루션 및 통신스위치	임차료 ERP서버
유지보수로 TMS이중화솔루션	전산비용
유지보수로 Vmware	전산사용료 E2K 200 임대비용
유지보수로 WAS	전산사용료 인터넷 AS유지수수료(연간)
유지보수로 개인정보 웹방화벽	전산소모품 PC관련부품
유지보수로 그룹웨어및지식관리	전산소모품 기타
유지보수로 네트워크 모니터링 시스템	전산소모품 서버및주변장치관련부품
유지보수로 네트워크백본	전산소모품 프린터리본및카트리지
유지보수로 네트워크이블	컨설팅료 서버성능평가및튜닝
유지보수로 동영상스트림서비스	통신회선료 LG
유지보수로 레이저프린터	통신회선료 기타
유지보수로 매입통합시스템	통신회선료 세종

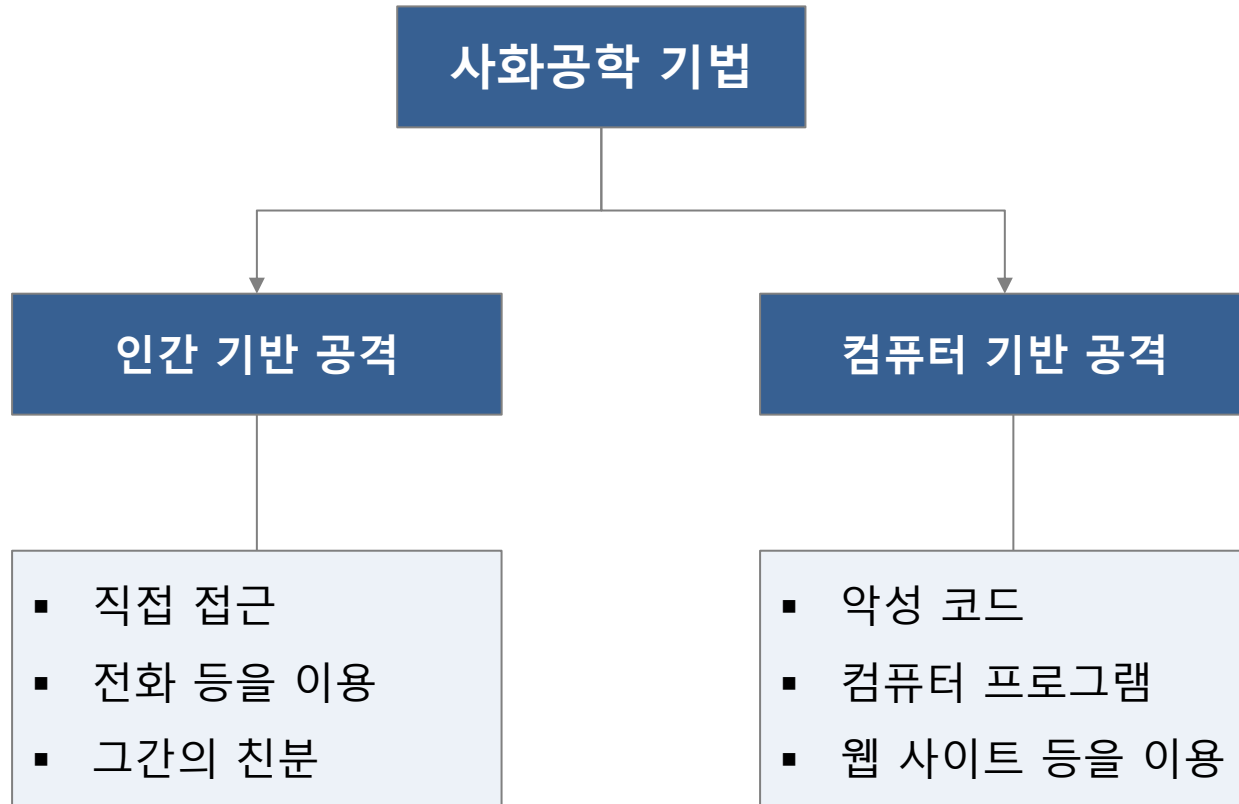
1. 사회공학의 이해

3 사회공학에 공격 대상

신뢰 기업 활용 사례(IP 스 2021년 스마트 공장 관련 교육 자료

비전&전략		1.(마이스터 기본소양)스마트마이스터의 이해	2021-08-12 오전 9:46
목표&성과 (Goal&KPI)	실시	2.(마이스터 기본소양)소통과커뮤니케이션	2021-08-12 오전 9:46
		4.(스마트공장 이해 및 사례)스마트공장 개요	2021-08-12 오전 9:42
		5.(스마트공장 이해 및 사례)스마트공장 전략수립	2021-08-12 오전 9:47
		6.(스마트공장 이해 및 사례)제조현장 스마트화 수준진단 이해	2021-08-12 오전 9:48
Level3 기업경영		7.(스마트공장 이해 및 사례)스마트 공장 보안위협 이해	2021-08-12 오전 9:49
		8.(스마트공장 이해 및 사례)스마트 공장 보안대책 이해	2021-08-12 오전 9:50
Level2	제품 개발	11.(프로세스의 스마트화)수요관리	2021-08-12 오전 9:50
		12.(프로세스의 스마트화)설계관리	2021-08-12 오전 9:50
		13.(프로세스의 스마트화)자재재고관리	2021-08-12 오전 9:51
		14.(프로세스의 스마트화)생산관리	2021-08-12 오전 9:51
제조운영		16.(프로세스의 스마트화)설비관리	2021-08-12 오전 9:51
		17.(프로세스의 스마트화)공정관리	2021-08-12 오전 9:52
		18.(프로세스의 스마트화)물류관리	2021-08-12 오전 9:52
Level1	Machine /Control	19.(프로세스의 스마트화)에너지관리	2021-08-12 오전 9:57
		20.(프로세스의 스마트화)인적자원관리	2021-08-12 오전 9:53
기계/제어	제조기술	21.(정보기술)정보기술	2021-08-12 오전 9:53
		22.(정보기술)정보화 전략수립	2021-08-12 오전 9:53
		23.(자동화기술)스마트공장 운영기술	2021-08-12 오전 9:54
		24.(자동화기술)스마트공장 자동화기술(AT)	2021-08-12 오전 9:54
		25.(프로젝트 관리 방법론)프로젝트 관리	2021-08-12 오전 9:54

2. 사회공학의 기법



일반적으로 사회공학 기법은 인간 기반의 수단을 이용하는 공격 형태를 지칭

직접적인 접근

직접 만나거나 전화, 온라인으로 접근하는 것

- **권력을 이용한 접근**

- ✓ 조직에서 높은 위치에 있는 사람으로 가장하여 정보 획득

- **동정심에 호소한 접근**

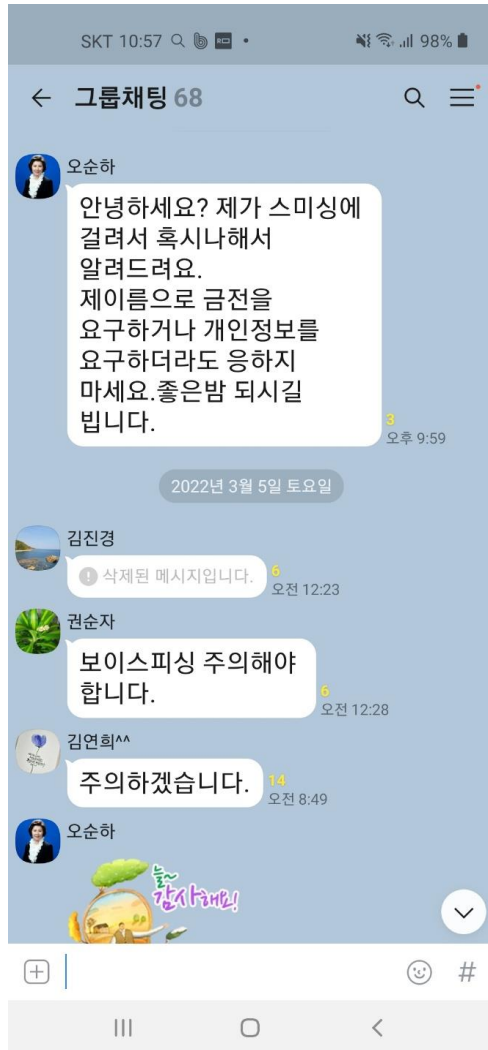
- ✓ 매우 긴급한 상황에 처해 도움이 필요한 것처럼 행동하는 경우

- ✓ 사례 : 산본, 응봉동

- **가장된 인간관계를 이용한 접근**

- ✓ 개인 정보를 얻어 신분을 가장한 뒤 공격 대상에게 정보 획득

직접적인 접근 사례1

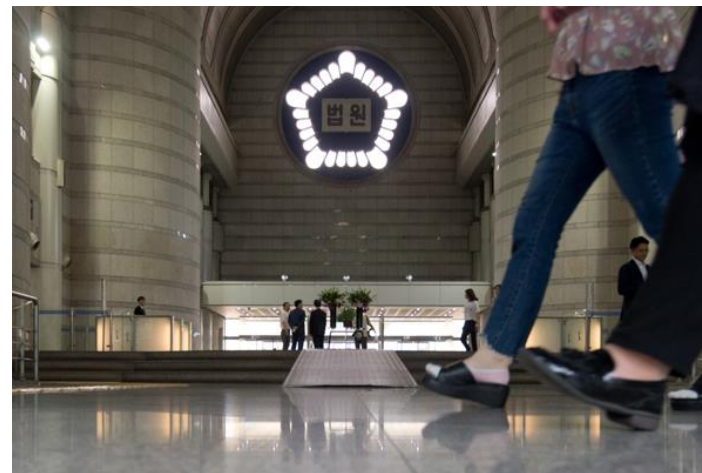


금융 사기 : 조카

직접적인 접근 사례2

[판결] "'개인정보 유출 사고' 인터파크, 피해 회원 1인당 10만원씩 배상하라"
서울중앙지법, 원고일부승소 판결

인터넷 쇼핑몰인 인터파크에선 지난 2016년 5월 인적사항을 알 수 없는 해커에 의해 내부 전산망이 해킹 당하는 사고가 발생했다. 이 사고로 인터파크가 관리하고 있던 회원들의 비밀번호와 생년월일, 휴대전화 번호 등 개인정보가 유출됐다.



방송통신위원회는 해커의 공격을 지능형 지속가능 위협(APT)으로 보고, 민관합동조사단을 구성해 인터파크의 개인정보처리시스템 등에 남아있는 접속기록 등을 토대로 개인정보 처리 및 운영 실태를 조사했다. 지능형 지속가능 위협은 해커가 다양한 보안 위협을 만들어 특정 기업이나 조직의 네트워크에 지속적으로 가하는 공격을 말한다. 그 결과 해커는 인터파크 직원의 네이버 계정을 불법적으로 도용해 접속한 뒤 악성코드를 심은 이메일을 보내 컴퓨터를 감염시키고, 회원들의 개인정보가 저장돼 있던 DB서버에 접속해 이를 모두 빼간 것으로 조사됐다. 이에 인터파크 회원 A씨 등은 "1인당 30만원을 배상하라"며 소송을 냈다.

도청

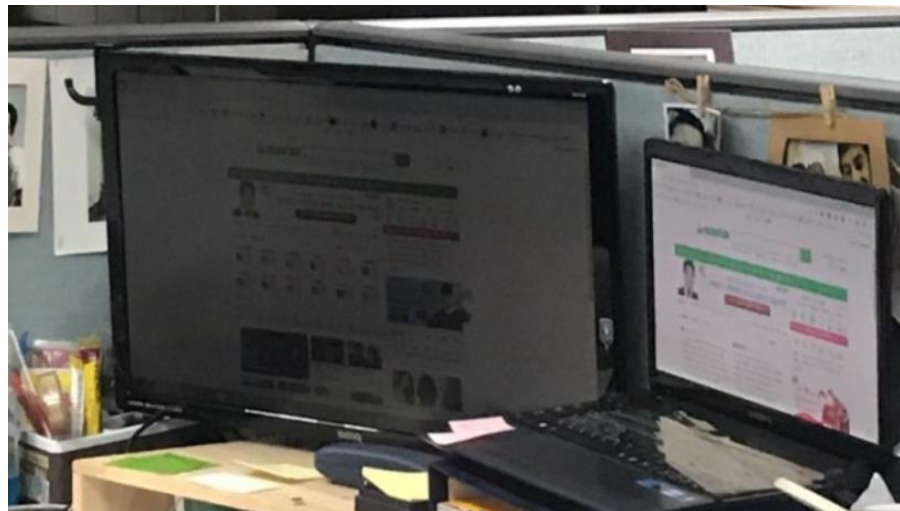
- 도청 장치나 유선 전화선을 통한 도청
 - 레이저 마이크로폰으로 유리나 벽의 진동을 탐지하여 음성으로 바꾸어 도청
 - 문에 귀를 대고 엿듣거나 슬그머니 가까이 다가가 엿듣는 것도 도청에 속함
 - 내부 직원이나 평소에 친하게 지내던 사람도 사회공학 공격자가 될 수 있음
-
- ✓ 내귀에 도청장치
 - ✓ 워터게이트 사건
 - ✓ 초원복집 사건
 - ✓ 삼성 X파일 사건
 - ✓ 국정원 불법 도청 사건
 - ✓ 정당 도청 의혹사건
 - ✓ NSA 기밀자료 폭로 사건

도청과 감청 차이

- 도청과 감청은 타인의 통화를 엿듣는다는 점에서는 동일한 행위지만 합법이나 불법이냐에 따라 용어가 달라진다. 도청은 말 그대로 남의 대화나 유무선 통화를 엿듣는 것으로 불법이다. 범죄나 정치적·경제적 이득을 목적으로 법원 등 정부 기관에 허가를 받지 않고 엿들으면 모두 도청이라고 할 수 있음.
- 통신비밀보호법은 우편물 검열과 전기통신 감청, 비공개 대화 녹음을 청취하는 것을 불법으로 규정하고 있다. 따라서 옛 안전기획부가 사전에 법원의 허락을 받지 않고 음식점에 도청 장치를 설치해 비공개 대화를 녹음한 것도 불법에 해당함.
- 그러나 통신비밀보호법 6, 7, 8조는 합법적인 방법으로 감청을 할 수 있도록 하고 있다. 이를 법적인 용어로 '통신제한조치'라고 하며 통상적으로 '도청'과 차별화해 '감청'이라는 용어를 사용한다.
- 감청이 허락되는 조건 중 하나는 군 검찰관을 포함한 검사가 범죄 수사 목적상 필요해 법원에 요청한 사례다. 또 대통령령이 정하는 정보수사기관이 국가안전보장과 관련하여 위해를 방지하기 위한 차원에서 합법적인 절차를 밟아 감청할 수 있음.

어깨너머로 훔쳐보기

- 작업 중인 사람의 뒤 로 다가가 그 사람의 업무 관련 정보나 패스워드 등을 알아내는 것.
- 최근엔 편광 필름을 많이 사용
- 패스워드는 별표(*)로 표시되어 이 방식으로 정보를 훔치기 어려움
- 손가락 움직임만으로 쉽게 유추할 수 있는 패스워드(예: qwer1234)는 쉽게 노출될 수 있으므로 주의 필요.(id : admin, pw : admin)



휴지통 뒤지기

- 다소 지저분하지만 효과적인 정보 수집 방법
- 휴지통 뒤지기로 얻을 가능성이 높은 정보

정보 1	정보 2
▪ 회사 인사 구조도	▪ 시스템 매뉴얼
▪ 업무관련 메모	▪ 회사 약관록
▪ 소스 인쇄본	▪ 회사 업무 일정
▪ 회사 전략	▪ 매출과 수익 구조
▪ 중요 행사 계획	▪ 하드디스크, 디스켓, USB 등 등

최근에는 정보가 외부로 유출되는 것을 막기 위해 문서 세단기를 많이 사용

휴지통 뒤지기



가정에서는 공공기관 활용



시스템 분석

- 포렌식을 사용한 시스템 분석가능
- 버려진 하드디스크나 컴퓨터를 사용하거나 정보를 얻고 싶은 대상의 노트북 또는 PC를 중고로 사서 분석하여 정보 획득
- 중요한 업무를 수행한 저장 장치의 내용은 Eraser와 같은 툴을 이용하여 삭제하려는 파일의 위치에 일괄적으로 0이라는 값으로 덮어쓰기를 해야 함
- 특수 장비를 이용하면 파일 삭제 툴로 삭제한 정보도 해독할 수 있으므로 완벽한 삭제가 필요할 시 강력한 자기장을 발생시키는 자기 소거 장치 이용
- Eraser
 - ✓ New Task를 통해 삭제 작업을 등록함
 - ✓ 등록할 수 있는 삭제 작업은 특정 파일, 폴더, 디스크, 휴지통

시스템 분석 Eraser 활용 사례



The screenshot shows the 'Seongdong-gu Smart Citizen Portal' (성동구 스마트포용도시) website. The header includes a search bar, weather information (03.05.토, -°C), and air quality data (미세먼지 101 $\mu\text{g}/\text{m}^3$, 나쁨). The main navigation bar lists various services like '전체메뉴', '종합민원', '행정정보', '성동참여', '열린성동', '분야별정보', 'HOT 인가검색어', and '출발지원금'. The '성동참여' (Seongdong Participation) section is highlighted, showing a list of services including '온라인접수' (Online Application), '행사/접수' (Event/Registration), '나의 행사접수' (My Event Registration), and '디지털 저장매체 파기서비스' (Digital Storage Media Destruction Service). The '서비스안내' (Service Guide) section provides information about the digital storage media destruction service, emphasizing the prevention of information leakage and damage from lost devices like PCs, notebooks, hard drives, and mobile phones.

시스템 분석

- 하드디스크 의 정보를 디스크에 쓰인 자기체가 약간 남기 때문에 일곱 번이나 쓰고 지워도 해독할 수 있음
- 잔존 자기체까지 완전히 삭제하려면 강력한 자기장을 발생시키는 자기 소거 장치를 이용해야 함



하드디스크 파쇄기



자기 소거 장치(탈자기 장치)

시스템 분석(악성 소프트웨어 전송)

- 서비스 제공 업체로 가장하여 바이러스나 백도어 또는 키보드 입력을 가로챌 수 있는 키로거 등을 전송하여 공격 대상이 설치하게 만드는 것
- 가까이에 있는 사람이라면 플로피 디스크나 USB 메모리에 담아 그 사람의 시스템에서 몰래 실행할 수도 있음
- 정보유출방지 솔루션(DLP, Data Loss Prevention)
 - ✓ 핵심기능 : 검출(Discover)과 차단(Prevent), 기록(Audit)
 - ✓ 검출(Discover) : 기능에서는 데이터가 개인정보인지, 기밀정보인지 파악
 - ✓ 주민등록번호, 카드번호, 핸드폰 번호 등 정보패턴에 따라 사전에 파일을 분류한 후 삭제, 암호화하여 PC, 서버, DBMS 내 저장된 불필요한 개인정보를 정리해 줌.
 - ✓ 차단(Prevent) : 정책 이상의 기밀정보가 외부로 반출될 경우 나가기 전에 차단하는 행위.
 - ✓ DLP는 DRM와 다르게 문서작성, 열람시에는 통제하지 않으며 오직 외부로 반출될 때만 통제

인터넷을 이용한 공격

- 다양한 검색 엔진으로 인터넷에 존재하는 공격 대상의 개인 정보와 사회 활동 정보를 수집하는 것.
- 일반 적으로 : 신상 털기
- 신상 : 이름, 주소, 소속 회사 및 직책, 주민 번호, 주소, 전화 번호, 사진, 이메일 등을 이용하여 인터넷에서 정보를 역추적하는 방식
- 벨기에 국방부도 뚫렸다... 전 세계 인터넷 뒤흔든 '로그4j'
 - ✓ 인터넷 서비스 개발에 직·간접적으로 사용되는 공개 소프트웨어(SW) '로그 4j(Log4j)'가 보안에 취약한 점이 드러나 벨기에 국방부가 해킹 공격을 받음.
 - ✓ 24일 방산·보안업계 등에 따르면 벨기에 국방부는 최근 로그4j의 보안 취약성을 이용한 사이버 공격을 받았다고 발표했다. 북대서양조약기구(NATO) 동맹국 중 처음으로, 이로 인해 일부 국방부 업무가 일시적으로 중단된 것.

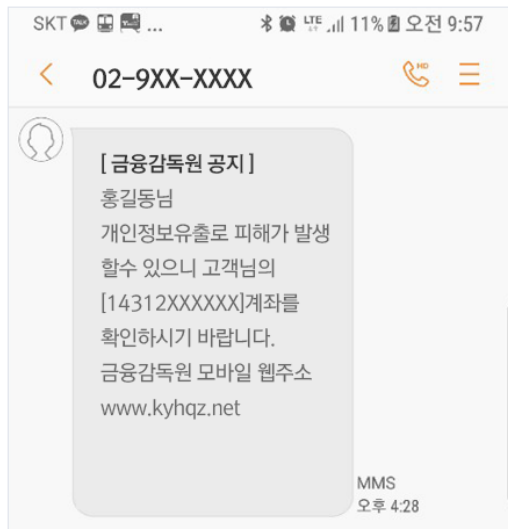
<https://biz.chosun.com/industry/company/2021/12/24/WMZEGGPLEBADZGIQMSAYLNAZNE/>

피싱(phishing)

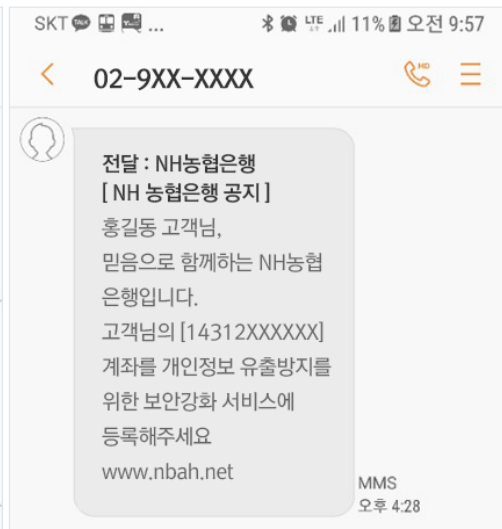
- 피싱은 'private data(개인정보)'와 'fishing'의 합성어
- 개인 정보를 불법으로 도용하려는 속임수의 한 유형.
- 공격 대상에게 그럴듯한 이메일을 보낸 뒤 링크(URL)에 접속하여 신용 정보나 금융 정보를 입력하게 함
- 피싱 메일에 포함된 링크의 특성
 - ✓ 링크 정보로 표시된 주소와 실제 리다이렉트주소가 다름
 - ✓ 공격 대상이 이용하는 URL과 유사한 URL로 연결 정보 변형
 - ✓ URL을 인코딩하여 사용자가 가짜 사이트의 링크 주소를 알기 어렵게 조작

피싱(phishing) 사례

- ✓ 링크 정보로 표시된 주소와 실제 리다이렉트주소가 다름
www.wishbank.com인데 소스에는 다른 IP 주소로 접속
- ✓ 공격 대상이 이용하는 URL과 유사한 URL로 연결 정보 변형
www.wishbank.com → www.wishback.com



금융감독원 사칭사례



농협은행 사칭사례

피싱(phishing) 사례

번호	제목	담당부서	등록일	첨부파일	조회수
66	'21.4월 인터넷 카페의 저금리 대...	불법금융대응단	2021-05-12		5056
65	'21.3월 30대 남성, 인터넷 투자 ...	불법금융대응단	2021-05-12		3236
64	인터넷 대환대출 신청 후 텔레그...	불법금융대응단	2021-05-12		2241
63	'21.3월 60대 여성, 사기범이 문...	불법금융대응단	2021-05-11		3756
62	'21.2월 딸이 보낸 문자로 착각하...	불법금융대응단	2021-05-11		4077
61	'21.2월 폰이 고장났다는 딸 사칭 ...	불법금융대응단	2021-05-11		1911
60	21.2월 60대 여성, 폰 액정이 깨...	불법금융대응단	2021-05-11		2266
59	'21.1월 대출권유 문자를 받고 신...	불법금융대응단	2021-05-11		2988
58	'21.1월 50대 여성, 폰이 고장났...	불법금융대응단	2021-05-10		2508
57	'20.12월 딸이 보낸 문자로 착각...	불법금융대응단	2021-05-10		2354

출처 : 금융감독원

피싱(phishing) 사례

최초 접근방법	피해자 연령	피해자 성별	사기 유형
인터넷 카페	30대	남성	대출병자형

(돈 버는 좋은 방법이 있으니..... 사례)

2021년 3월 중순 인터넷투자 카페에 대한대출을 조건이 어렵지 않고 이율도 최저로 금액도 최대로 해준다는 내용의 글을 보았습니다. 저는 투자금이 없었고 기존의 대출이 있는 관계로 글쓴이에게 메신저로 연락하였더니, 자기도 대출을 진행했고 그 덕분에 돈을 많이 벌 수 있었다라고 알려주었습니다.

조금 망설였으나 그 사람이 가족사진이며 이름이나 각종 정보들을 주고 해서 친해졌습니다. 그 사람과 다시 얘기를 해서 대출을 진행하였습니다.

그 사람이 “대출자금이 해외에서 들어오는 자금세탁용 검은 돈이어서 비밀스럽게 진행하고 5천만원 정도 보내면 한 2억원은 대출이 진행될 것이다” 해서

제가 “확실한 거냐? 책임질 수 있냐?” 물었는데,

그 사람이 “확실하고 책임질 수 있고 나도 두 아이의 아빠인데 거짓말 하겠냐?” 라고 하였습니다.

저는 그 말을 듣고 3월 26일 천만원씩 5천만원을 ○○은행 계좌로 송금했고

“기다리면 몇일 사이에 자금세탁이 되어 계좌로 입금될 것이다 기다리라” 말만 듣고 기다렸으나, 3월 31일 9만원, 4월 1일 237만원 및 444만원 나누어서 제 □□은행 계좌로 입금되었습니다.

그래서 “왜 이리 적게 입금 되냐?” 따져 물으니

그 사람이 “해외에서 자금세탁이 문제가 생겨 일부밖에 되지 않아 그렇다.” 하고

제가 “그러면 나머지 금액은 언제쯤 나오냐?” 물었더니

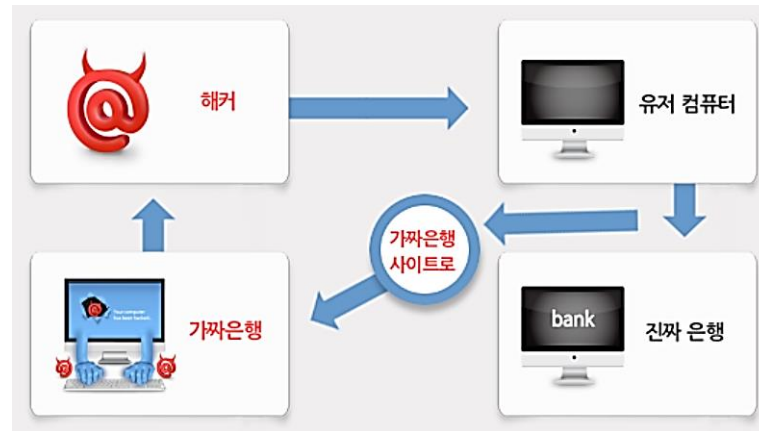
그 사람이 “기약은 알 수 없으니 기다려야 되고 내가 최대한 힘써 보긴 하는데 그러려면 뇌물(?)이 필요하다. 그래서 입금을 하면 빠르게 해결할 수 있고 오히려 금액이 더 크게 나오게 힘써 보겠다.”라고 하였습니다.

이 얘기를 듣고 처음에는 망설였으나 언제 나올지 기약도 없다 하고 돈을 못 받을 수도 있어서 뇌물로 돈을 쓰는 것밖에 방법이 없다 하여 입금한 5천만원이 생각나 최대한 돈을 빨리 마련하여 5천만원을 더 송금했습니다.

파밍(pharming)

- 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 악성 코드로 감염으로 DNS를 속여 사용자가 진짜 사이트로 오인하게 함으로써 개인 정보를 훔치는 수법
- “파밍(Pharming)”이란 악성코드에 감염된 PC를 조작해, 이용자가 인터넷 ‘즐거찾기’ 또는 포털사이트를 통해 금융회사 홈페이지에 접속하여도 피싱(가짜)사이트로 유도되어 금융정보를 탈취하여 유출된 정보로 예금인출하는 방식을 뜻합니다.
- DNS 스푸핑과 기본적으로 같은 공격이며 DNS 스푸핑 공격으로 개인 정보를 수집

파밍(pharming) 예방 수칙



예방 수칙

1. 사이트 주소가 정상인지 확인하고, 보안카드번호 전부는 절대 입력하지 마세요.
2. 공인인증서, 보안카드 사진 등을 컴퓨터나 이메일에 저장하지 마세요
3. OTP(일회성 비밀번호생성기), 보안 토큰(비밀번호 복사방지)등을 사용하기를 권장하며, 공인인증서 PC지정 등 전자금융 사기 예방서비스에 가입
4. 스마트폰 문자메세지에 포함된 인터넷주소 클릭하지 마세요
5. 무료 다운로드 사이트의 이용을 자제하시고, 출처가 정확하지 않은 파일이나 이메일은 즉시 삭제
6. 윈도우, 백신프로그램 등을 최신 상태로 유지
7. 파밍 등이 의심될때에는 신속히 경찰청 112센터가 금융기관 콜센터를 통해 지급정지를 요청

스미싱(smishing)

- 스미싱은 'SMS와 phishing의 합성어
- 문자 메시지로 무료 쿠폰 제공 후 링크 접속을 유도하여 개인 정보를 빼내는 수법
- 스미싱인 줄 모르고 무심코 문자 메시지의 링크에 접속하면 휴대전화 소액 결제 발생

예방수칙

1. 모바일 백신 설치 및 실시간 감시 기능 설정
2. 스마트폰 운영 체제 최신 업데이트
3. 문자메세지 내 포함된 인터넷 주소(URL) 클릭하지 지양

4. 루팅*, 탈옥** 등 스마트폰 기본 운영 체제 변경 지양

루팅: 안드로이드 운영체제의 최고 권한 계정인 루트 권한을 획득하는 것

탈옥: 애플기기의 운영체제인 iOS에 규정된 제한을 풀어 여러방면으로 사용이 가능하도록 하는 것.

5. 스미싱 차단앱 설치(※ 이동통신사별로 스미싱 차단앱 기본설치 및 제공)
6. 비밀번호 설정되지 않는 무선 공유기(WiFi)에 접속 지양
7. 앱 다운로드시, 공식 애플리케이션 마켓 이용

스미싱(smishing) 사례

번호	제목	작성자	등록일	조회수	첨부
116	설 명절 택배 배송 사칭 관련 스미싱 주의	사이버수사연구분 석계	2022-01-20	3297	
115	요소수 판매 빙자 사이버 사기 주의	사이버수사연구분 석계	2021-11-08	2918	
114	가상자산 거래소 사칭 문자 피싱 주의	사이버수사연구분 석계	2021-11-03	2340	
113	코로나 상생 국민지원금 관련 스미싱 주의	사이버수사연구분 석계	2021-09-06	4883	
112	코로나 재난지원금 가장 스미싱 피해주의	사이버수사연구분 석계	2021-08-05	2607	
111	잔여백신 예약 안내 가장 피싱 주의	사이버수사연구분 석계	2021-07-27	2104	
110	가상자산 거래소 사칭 스미싱 주의	사이버수사연구분 석계	2021-05-31	5098	
109	메신저 피싱 소액 사기 피해주의	사이버수사연구분 석계	2021-03-19	14490	
108	2차 긴급재난지원금 가장 스미싱 경보	사이버수사연구분 석계	2020-09-23	6925	
107	추석명절 사이버범죄 예방경보 알림	사이버수사연구분 석계	2020-09-22	3210	

출처 : 경찰청 사이버 수사대

스미싱(smishing) 사례

< 코로나 재난지원금 관련 스미싱 주의 >

경찰청에서 알려드립니다.

최근 코로나19 재난지원금을 미끼로 한 피싱 사기가 늘어날 조짐이 보여 관련 내용을 알려 드립니다.

스미싱 문자 예시(인터넷주소(URL) 클릭을 유도함)

유형	① 안내 사칭	② 신청 사칭	③ 접수 사칭
(예시) 재난지원금 지급 스미싱	[00부 지원금 신청 안내] OO일 안내하세요 귀하는 지원금 5차 신청대상자에 해당 되므로 온라인신청(http://kr-law.com) 에서 신청하시기 바랍니다.	귀하는 5차 재난지원금 신청대상자 입니다. 신청하기를 클릭하세요 신 청하기-> http://t2m.kr/caTW	5차 재난지원금신청이 접수되었 습니다. 다시 한번 확인 부탁드립니다. http://n.syid.cloud

위와 같이 문자 내용에 코로나 재난지원금 안내신청접수 등을 미끼로 인터넷주소(URL) 클릭을 유도한 뒤, **악성앱 설치 유도 및 개인정보 탈취**가 예상됨에 따라 피해를 예방하기 위한 방법을 다음과 같이 알려드립니다.

1. 출처가 불분명한 사이트 URL 클릭 주의 및 삭제
2. 확인되지 않은 사이트에 휴대전화번호, 계정정보 등 **개인정보 입력 금지**

기타 예방수칙은 경찰청 홈페이지

(<https://cyberbureau.police.go.kr/prevention/prevention1.jsp?mid=020301>)에서
확인하실 수 있습니다.

- 경 찰 청 -

3. 사회공학 사례와 대응책

- 가장 효과적인 방법은 조직 구성원들에게 **보안 관련 교육**을 하여 보안 의식을 높이고 낯선 사람에 대한 경계심을 갖도록 하는 것
 - ✓ 전화로 정보를 요청했을 때 상대방이 정보를 확인한 후 전화하겠다고 하면 공격자는 이를 거절하고 정보를 줄 때까지 기다리겠다고 함, 공격자는 자신의 위치를 노출하지 않기 위해 전화번호를 알려주려 하지 않음. (어느 휴일 날 의료비 환급 전화)
 - ✓ 긴급한 상황이나 정상적인 절차를 밟기 어려운 난처한 상황이라면서 정보를 요청
 - ✓ 내부 또는 외부의 높은 직책에 있는 사람으로 가장
 - ✓ 조직의 규정과 절차가 법에서 정한 것과 일치하지 않는다고 항의하여 정보를 획득하려 함
 - ✓ 정보를 요청한 후 관련 사항에 대한 질문을 받으면 불편함을 표출, 정보를 확인해야 하는 책임자일지라도 고객이 불편함을 드러내면 질문하기 어렵다는 점을 악용하는 것
 - ✓ 회사의 높은 사람 이름을 언급하며 특별한 권한을 가진 것처럼 가장
 - ✓ 잡담을 계속하여 주위를 산만하게 함으로써 상대방이 정보를 흘리게 유도

3. 사회공학 사례와 대응책

사회공학 대응책

경찰청 사이버수사국의 예방 규칙

공통	사이버 사기(직거래 사기)	사이버 사기(쇼핑몰 사기)	스미싱
파밍	계정도용	악성프로그램	메모리해킹
스팸메일 · 메시지	스파이앱	몸캠피싱	랜섬웨어
디도스(DDoS) 공격	IoT 해킹	스피어 피싱	로맨스스캠
게임사기	이메일 무역사기	개인정보 침해	사이버스토킹

출처 : 경찰청 사이버수사국

<https://cyberbureau.police.go.kr/prevention/prevention1.jsp?mid=020301>

3. 사회공학 사례와 대응책

사회공학 대응책

이메일 이용시 주의점



1. 출처가 불분명한 이메일이나 첨부파일은 열지 말고 삭제한다.
2. 첨부파일 열람 및 저장 전에는 반드시 백신으로 검사한다.
3. 메일을 통해 개인정보제공을 요구하는 서비스의 경우 가급적 이용을 자제한다.
만약 이용할 경우 반드시 해당 업체 홈페이지에 직접 접속하여 꼼꼼히 확인한 후 이용한다.
4. 날마다 메일을 체크하고 중요하지 않은 메일은 즉시 지운다.
5. 이메일프로그램 또는 이메일제공서비스의 다양한 차단기능을 살펴보고 활용한다.
6. 인터넷 게시판 등에 이메일 주소를 남길 때 신중히 한다.
7. 인터넷 서비스 가입시 광고메일 수신 여부를 반드시 확인한다.

온라인 금융거래 주의점



1. 은행, 신용카드 등 금융기관 사이트는 즐겨찾기를 이용하거나, 주소를 정확하게 입력하고 이용한다.
2. 금융기관 등에서는 전화나 메일로 개인정보를 확인하는 경우는 없으므로 정보를 요청하는 메일은 일단 의심한다.
3. 공인인증서는 반드시 USB 등 이동식 저장장치에 보관한다.
4. 보안카드는 반드시 본인이 소지하고, 온라인 다른 곳에 기재해 두지 않는다.
5. 온라인 금융거래 이용 후, 이를 알려주는 휴대폰 문자서비스를 이용한다.
6. 시간이 걸리더라도 금융기관에서 제공하는 보안프로그램은 반드시 설치한다.
7. 금융기관 이용 비밀번호 등은 기타 다른 사이트의 비밀번호와는 다르게 설정한다.
8. 공공장소 PC는 보안에 취약하므로 온라인 금융거래 이용을 자제한다.

3. 사회공학 사례와 대응책

사회공학 대응책

■ 가족의 안전한 사이버 생활



1. 컴퓨터를 개방된 공간에 두고 가족들이 공유할 수 있도록 한다.
2. 자녀가 가입한 사이트, 카페 및 자녀의 ID가 무엇인지 알아둔다.
3. 자녀가 사이버상에서 하는 활동에 대해 항상 대화한다.
4. 온라인 게임은 규칙을 정해서 이용하도록 하고, 아이템이나 계정 거래 등에 대해 알아둔다.
5. 부모의 주민번호, 신용카드번호 및 기타 비밀번호를 공개하지 않는다.
6. 자녀에게 다음의 인터넷 수칙을 알려준다.
 - 인터넷 채팅의 익명성을 알려주고 이름, 주소, 학교 등 신상정보를 알려주지 않도록 한다.
 - 부모의 허락없이 인터넷을 통해 직접 사람을 만나지 않도록 한다.
 - 부모의 허락없이 부가적인 요금을 내야하는 정보나 게임 등을 이용하지 않도록 한다.
 - 인터넷 게시판에 글을 쓸 때는 에티켓을 갖추어야 한다.
 - 저작자의 허락없이 저작물을 인터넷에 올려 저작권을 침해하지 않도록 한다.

가상화폐 관련 용어

- 가상화폐와 전자화폐
- 지갑
- 블록체인
- 채굴



가상화폐 관련 용어

- 가상화폐는 전자화폐와 다름
- 전자화폐는 [전자금융거래법](#)(2조 15항) : “이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보”로 정의
- 가상 화폐는 “금전적 가치”가 없기 때문에 가짜 화폐에 가깝다.
- 가상 화폐의 대표 주자 :
- 2008년 10월 사토시 나카모토 논문<비트코인-P2P 전자 화폐 시스템>
- 1998년 웨이 다이(Wei Dai)가 제안한 암호화 화폐라는 개념으로 처음 실현
- 거래수수료가 없거나 거의 들지 않은

가상화폐 비교















디지털통화와 현금·전자화폐의 비교

	현금	전자화폐	디지털통화(가상화폐)
발행기관	중앙은행	금융기관, 전자금융업자	없음
발행규모	중앙은행 재량	법정통화와 일대 일 교환	알고리즘에 의해 사전 결정
거래기록·승인	불필요	발행기관	블록체인(분산원장) 기술
화폐단위	법정통화	법정통화	독자 단위
법정통화와 교환	-	발행기관이 교환을 보장	가능하나 보장되지 않음
교환가격	-	고정	수요-공급에 따라 변동
사용처	모든 거래	가맹점	참가자

출처 한국은행 2015년도 지급결제보고서

가상화폐 순위

# ▲	이름	가격	24h %	7d %	시가총액 ⓘ	거래량 (24시간) ⓘ	유통 공급량 ⓘ	
☆ 1	 Bitcoin BTC 구매하기	₩36,390,459.67	▲1.07%	▼1.82%	₩693,053,124,670,763	₩23,833,732,829,697 655,193 BTC	19,052,131 BTC	
☆ 2	 Ethereum ETH 구매하기	₩2,247,643.07	▲3.25%	▼9.64%	₩271,586,050,495,018	₩15,873,626,926,036 7,070,007 ETH	120,962,601 ETH	
☆ 3	 Tether USDT	₩1,253.38	▲0.04%	▼0.30%	₩90,904,667,223,019	₩45,890,973,358,529 36,618,636,738 USDT	72,537,249,554 USDT	
☆ 4	 USD Coin USDC 구매하기	₩1,254.48	▼0.06%	▼0.35%	₩67,360,036,021,043	₩5,226,143,683,911 4,165,620,892 USDC	53,690,902,946 USDC	
☆ 5	 BNB BNB 구매하기	₩384,817.63	▲1.66%	▼2.14%	₩62,840,258,211,878	₩1,827,934,796,150 4,749,498 BNB	163,276,975 BNB	
☆ 6	 XRP XRP	₩484.30	▲0.52%	▼7.22%	₩23,396,290,189,549	₩1,062,367,828,851 2,195,140,984 XRP	48,343,101,19	

지갑

- 코인능 거래하려면 비트코인 지갑 필요
- 지갑은 은행의 계좌와 같은 역할
- 비트코인 이용자가 지갑 프로그램을 통해 공개 주소를 만들면 개인 키가 함께 생성 됨.

'전자지갑'이란?

우리가 보통 돈을 지갑이라는 곳에 넣고 다니잖아요. 같은 맥락으로 가상화폐를 보관할 수 있는 것이 전자지갑입니다.

'전자지갑' 만들기

전자지갑은 각 코인 홈페이지에서 만들 수 있지만, 보통 가상화폐 거래소에서 전자지갑을 만듭니다.

가상화폐 거래소 중에서 거래량이 많은 곳인 '빗썸'에서 전자지갑을 만들도록 하겠습니다.

블록체인

- 블록체인은 최초의 블록으로부터 바로 앞 블록의 링크를 가지고 있는, 연결된 리스트로 분산되어 저장 및 관리
- 블록에는 거래 정보가 포함 되어 있으며, 블록의 집합체인 블록체인에는 비트코인의 모든 거래 정보가 담겨 있어 거대한 분산 장부

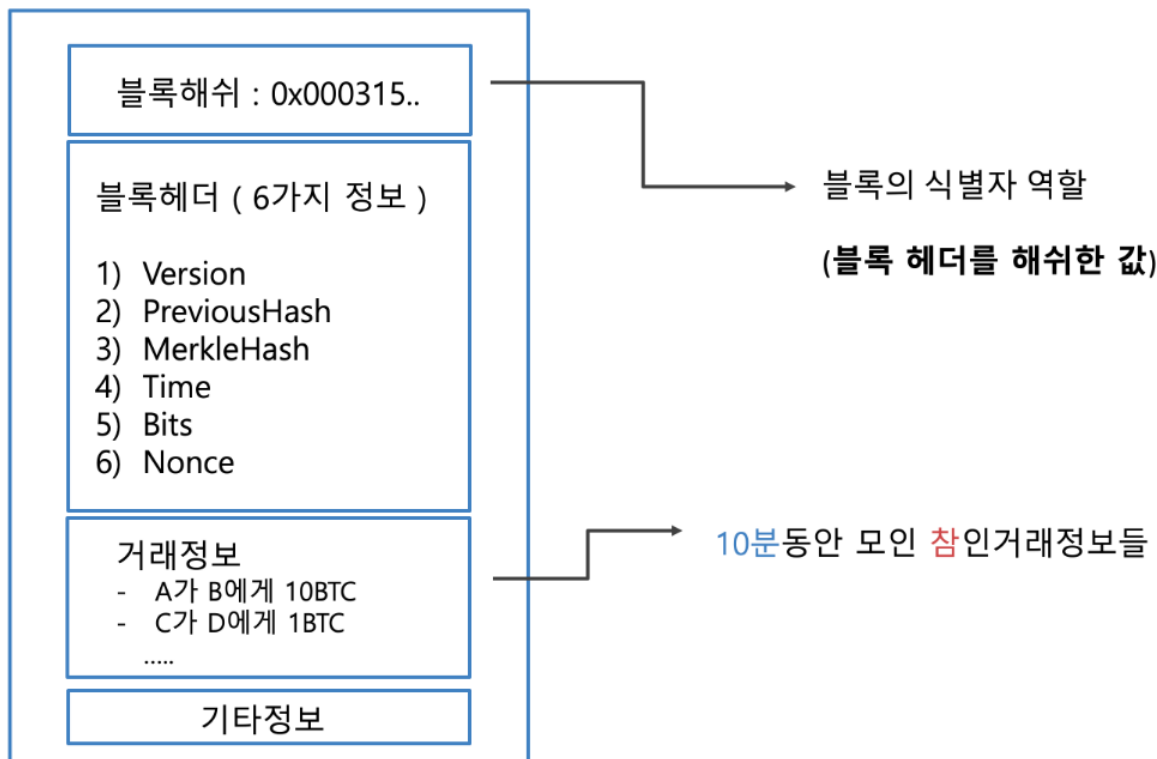
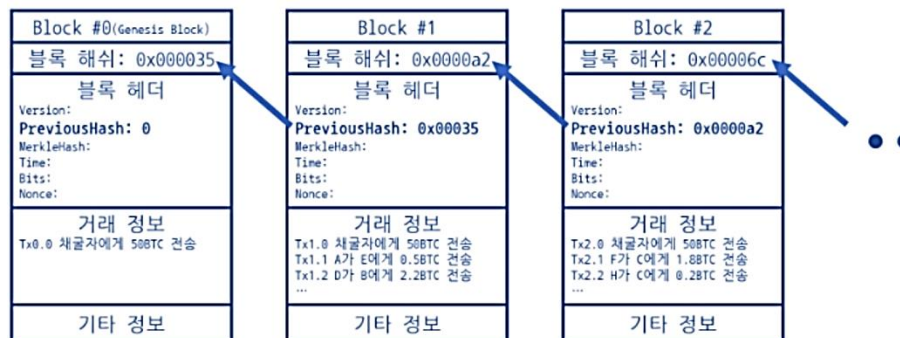
항목	설명
version	소프트웨어/프로토콜 버전
previousblockhash	이전 블록의 기타 정보를 제외한 값의 해시 값
merklehash	현재 블록의 거래 내역에 대한 해시 값
time	블록이 생성된 시간
bits	난이도 조절용 수치
nonce	처음에 "0"에서 시작하여 조건을 만족하는 해시 값을 찾아 낼때까지 1씩 증가하는 계산 횟수

4. 전자 결재와 가상화폐

6

가상화폐(비트코인)

블록체인 구성



채굴

- 전자화폐 : 처음에 시제 돈을 주고 구입
- 비트코인 : 채굴이라는 과정을 거쳐 생성
- 채굴 과정 : 지속적인 해싱 작업을 통해 목표 값(target value) 이하의 해시 값을 찾는 과정
- 채굴 완료 : 새로운 블록을 블록체인에 추가하는 작업을 완료 했음을 증명할 때 이루어짐.
- 사용되는 알고리즘 : SHA256을 사용하며 SHA256을 두 번 적용함



블록체인 거래

- ① 이용자는 거래 상대방의 지갑 주소와 이체할 비트코인 액수 결정하여 자신의 개인 키로 서명하고 이체 신청
- ② 이체 신청에 대한 고유한 해시 값이 발행
- ③ 이체 신청 내역을 채굴자가 자신의 개인 거래 풀에 넣어 보관.
- ④ 블록에 넣을 이체 신청 내역의 우선순위를 정한 뒤 이를 기준으로 채굴 과정인 목표 값 해싱 진행. 목표 값 해싱에 성공하면 블록을 발행
- ⑤ 이체 내역을 담은 블록이 네트워크로 전파
- ⑥ 이체 내역의 이체 확인(confirmation)이 1이 됨
- ⑦ 네트워크로 해당 블록을 전파 받은 다음 채굴자가 블록을 생성하면 다음 블록도 네트워크로 전파되고 이체 내역의 이체 확인이 2가 됨
- ⑧ 위의 과정을 끝없이 반복
- ⑨ 이체 받는 주체가 이체 내역을 인정하면 이체 확정이 됨

블록체인 보안

- 실물이 없는 비트코인은 입출금 내역인 장부로만 존재, 그 장부에 나타난 금액 합계가 잔액이 됨
- 거래 내역을 조작한다면 그것은 바로 장부를 조작하는 일
- 장부를 조작한다는 것은 변조된 블록을 생성하여 전파시키는 데 성공한다는 의미지만 현실적으로 불가능

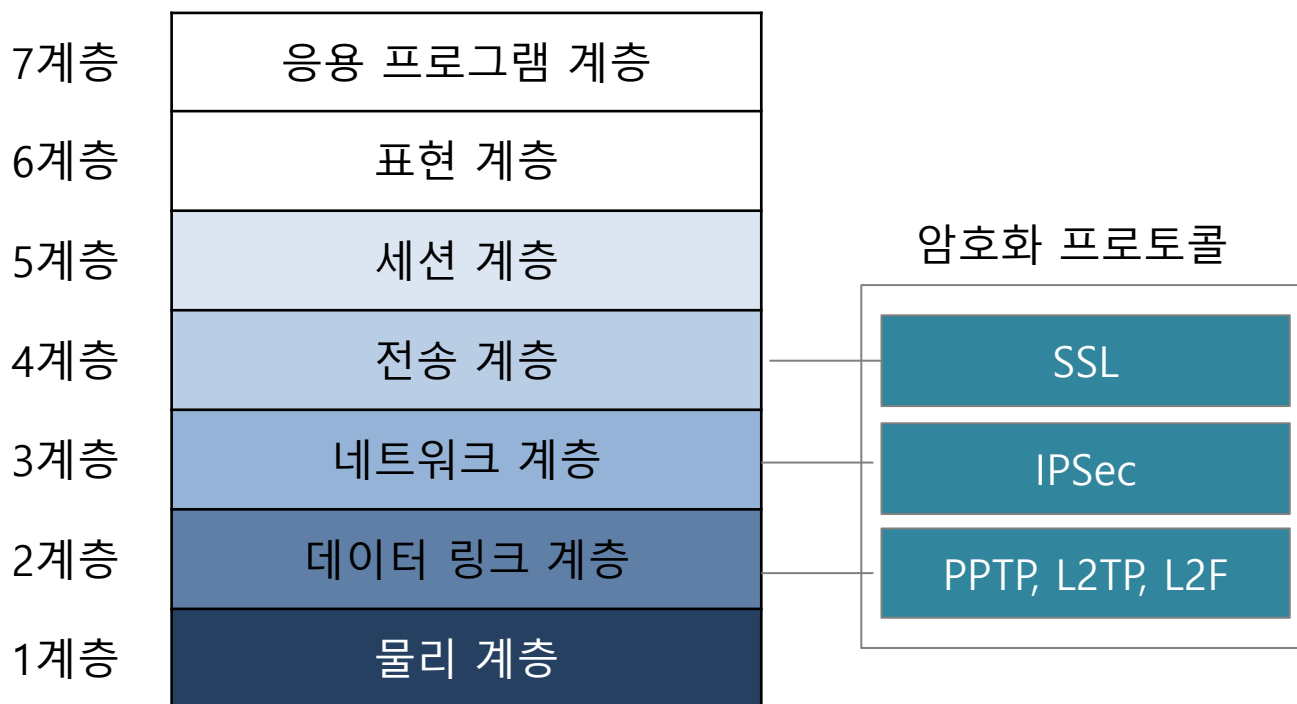
표 8-4 비트코인의 잔액 확인 과정

거래 순번	거래 종류	금액
0	최초 지갑 생성	
1	입금	4
2	출금	-2
3	입금	10
4	출금	-2
5	출금	-2
잔액		8

표 8-5 비트코인의 조작된 잔액 확인 과정

거래 순번	거래 종류	금액
0	최초 지갑 생성	
1	입금	4
2	출금	-2
3	입금	10
4	출금	-2
5	출금	-2
6	조작된 입금	10000
조작된 잔액		10008

- 암호화 통신은 전자 상거래를 하는 데 필수 수단임.
- 암호화 활용 : 네트워크 암호화와 전자 우편 암호화
- OSI 각 계층에서 동작하는 암호화 프로토콜은 2~4계층에서 동작



2계층의 암호화 프로토콜 : PPTP, L2TP, L2F

PPTP

- PPTP(Point-to-Point Tunneling Protocol) : PPP를 기반(마이크로소프트 제안)
- 두 대의 컴퓨터가 직렬 인터페이스로 통신할 때 이용
- 전화선을 통해 서버에 연결하는 PC에서 자주 사용

L2TP

- 시스코가 제안한 L2F(Layer 2 Forwarding)와 PPTP의 결합
- 둘 다 IP, IPX, NetBEUI, AppleTalk 등의 다양한 상위 로컬 네트워크 프로토콜 사용
- 사용 인증 : PAP, CHAP, MS-CHAP, EAP
- 데이터 암호화 및 압축(CCP, ECP) 등의 보안 기능 사용

PPTP와 L2TP의 프로토콜 비교

구분	PPTP	L2FP
네트워크	통신을 위한 양단 네트워크 IP 기반	Frame relay, ATM 등에도 사용
터너링	두 시스템 사이에 하나의 터너링만 지원	여러 개의 터널을 허용, QoS 에 따라 다른 터널 이용
압축및인증	해당 기능 없음	해더 압축 및 터널에 대한 인증 기능 제공

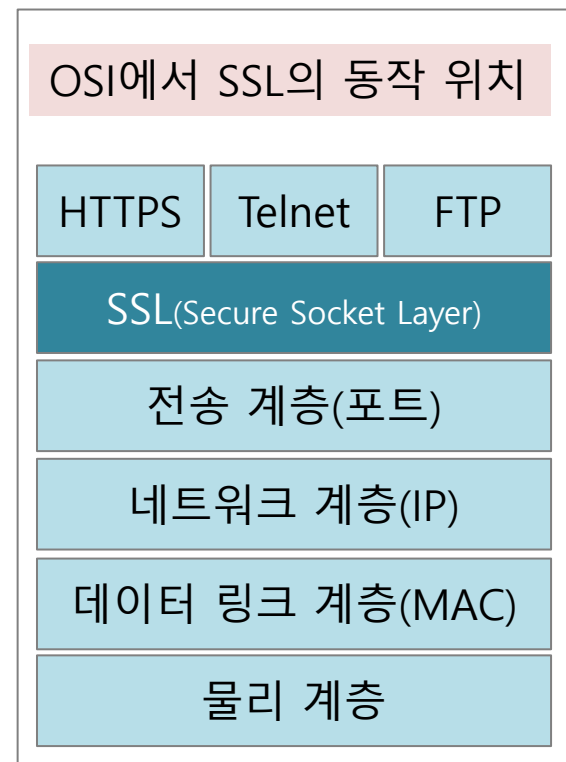
3계층의 암호화 프로토콜 : IPSec

IP를 기반으로 한 네트워크에서만 동작

기능	설명
AH (Authentication Header)	데이터 전송 도중에 변조 되었는지를 확인할 수 있는 데이터 무결성 검사 데이터를 스니핑한 뒤 해당 데이터를 다시 보내는 공격 차단
ESP (Encapsulating Security Payload)	메시지 암호 제공 암호화 알고리즘 : DESCBC, 3DES, RC5, IDEA, 3IDEA, CAST, blowfish가 있음
IKE (Internet Key Exchange)	ISAKMP, SKEME, Oakley 알고리즘 조합으로 두 컴퓨터 간의 보안 연결 설정 IKE를 이용한 연결에 성공하면 8시간 동안 SA(Seucrity Association) 유지 , 8시간 이후는 SA를 다시 설정해야 한.

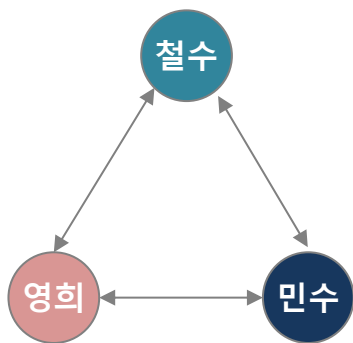
4계층의 암호화 프로토콜 : SSL

- **SSL의 기능** : 서버 인증, 클라이언트 인증, 암호화 세션으로 구분
- **클라이언트 인증** : 클라이언트의 인증서를 확인하여 서버에 접속할 자격이 있는지 확인
- **암호화 세션** : 암호화된 통신(40 bit와 120 bit 암호화 세션 형성)
 - ✓ 국내 : 40 bit 암호화를 제공하는 모듈 사용
- **서버 인증** : 클라이언트가 공개 키 기술을 이용하여 서버의 인증서가 신뢰 받는 인증 기관에서 발행 된 것이지 확인하는 작업
- 4계층과 5계층 사이의 프로토콜

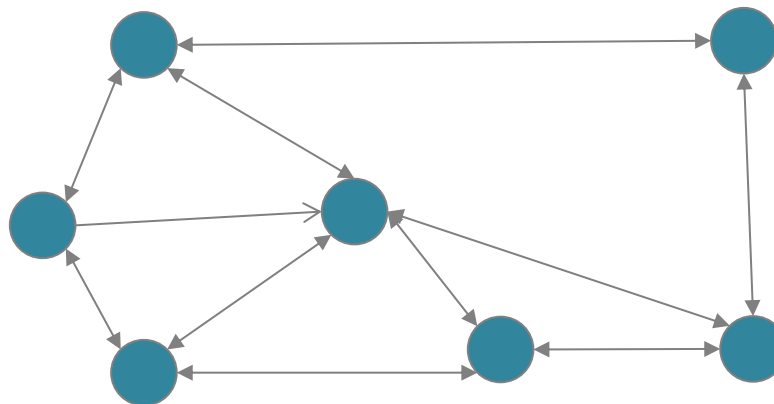


PGP(Pretty Good Privacy)

- 아직 메일의 암호화는 일반화 되지 못함
- 1991년에 IDEA 알고리즘과 RSA 알고리즘 조합을 조합
- 세션 키를 암호화하기 위해 : IDEA 알고리즘
- 사용자 인증 위한 전자 서명 : RSA 알고리즘 이용



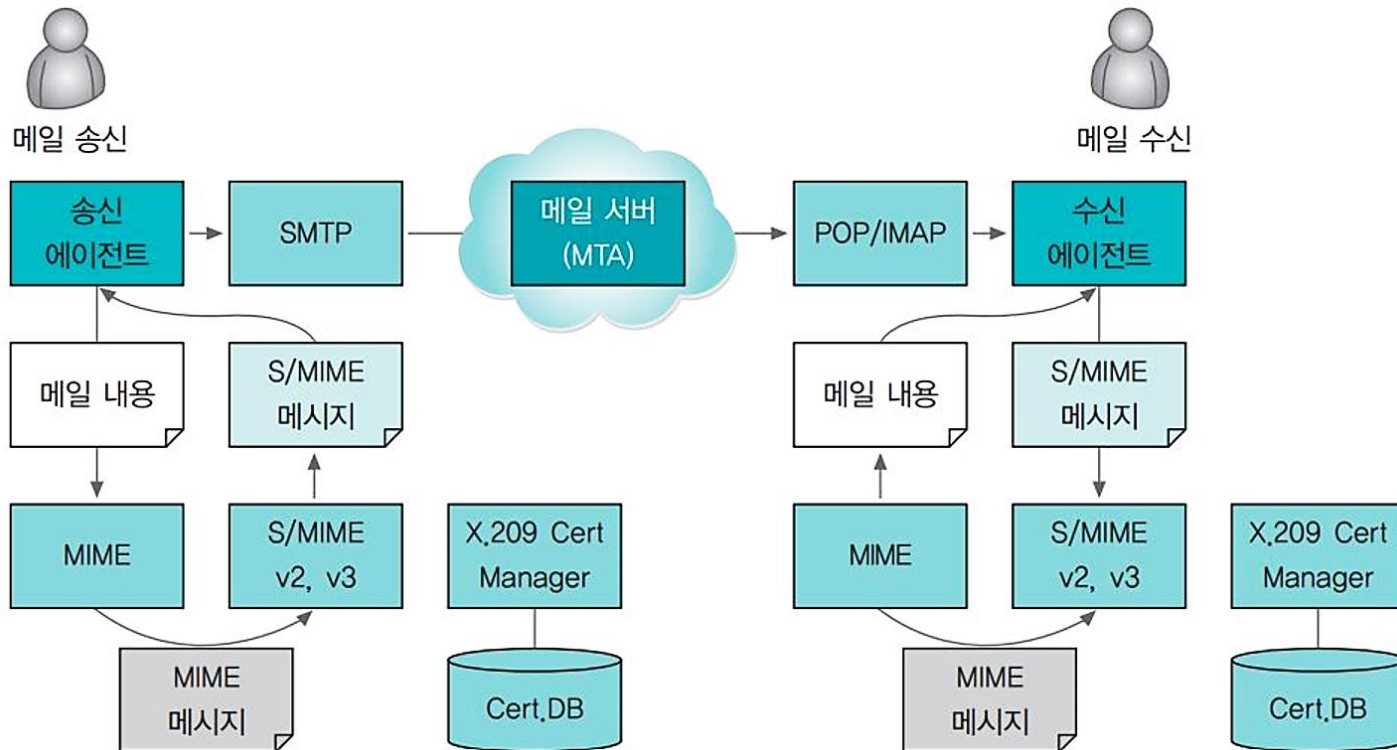
PGP의 상호 인증(예)



인터넷에서 PGP의 상호 인증(예)

S/MIME(Secure MIME)

- 인증서를 통해 암호화한 이메일 서비스 제공
- MIME(Multipurpose Internet Mail Extensions)는 전자 우편을 위한 인터넷 표준 포맷



S/MIME의 동작

6. 콘텐츠 보안

1 스테가노그래피

- 전자 상거래의 보안에서 중요한 문제 중 하나는 저작권(copyright).
- 저작권 보호 방법 : 스테가노그래피와 워터마크가 대표적인 방법.
- 스테가노그래피 (steganography) : 정보를 숨기는 데 목적이 있음
- 스테가노그래피는 전달하려는 기밀 정보를 파일, 메시지, 이미지 또는 비디오를 다른 파일, 메시지, 이미지 또는 비디오 안에 숨기는 심층 암호 기술.
- 스테가노그래피 기법은 문서의 저작권을 보호하는데 사용되기도 하나, 만일 이러한 기법들이 기업의 기밀 정보를 유출하는데 사용된다면 기업의 경쟁력 약화와 많은 금전적 피해가 발생할 수 있음을 예상할 수 있을 것이며, 따라서 기업은 다양한 기법들을 통해 정보가 유출될 가능성이 있으므로 항상 주의를 기울여야 할 것



- **워터마크(watermark)** : 과거에 편지지에 제작사를 표시하기 위하여 ㄱㅏㅏㅏ를 희미하게 인쇄했던것을 말함.
- 워터마크는 페이지 전면에 옅은 색으로 무늬를 나타내는 기술.
- 영상이나 비디오 파일에도 워터마크 삽입

영 두 내 용	권 령 권 자				비 고
	초 상 권	상 영 사 권	무 선 전 송 권	기 타 권	
1. 영상의 저작권에 관한 사항					
가. 기본영상 및 제작수입					
나. 제작비용에 관한 사항					
다. 기타 일반적인 권리사항 등					
2. 영상자료의 관리에 관한 사항					
가. 기본영상					
나. 영상 및 자료를 관리 등에 관한 사항					
3. 영상의 관리 업무					
가. 기본영상					
나. 제작비용에 관한 사항					
다. 일반적인 사항					



영 두 내 용	권 령 권 자				비 고
	초 상 권	상 영 사 권	무 선 전 송 권	기 타 권	
1. 영상의 저작권에 관한 사항					
가. 기본영상 및 제작수입					
나. 제작비용에 관한 사항					
다. 기타 일반적인 권리사항 등					
2. 영상자료의 관리에 관한 사항					
가. 기본영상					
나. 영상 및 자료를 관리 등에 관한 사항					
3. 영상의 관리 업무					
가. 기본영상					
나. 제작비용에 관한 사항					
다. 일반적인 사항					



Thank you

INFORMATION SECURITY



협력 업체	협력 업체
PIS 유지보수	유지보수로 메신저
TMS 유지보수	유지보수로 무선랜
거래명세서외	유지보수로 무정전전원공급장치
고속프린터 리본외	유지보수로 상상플러스 시스템
공사비 전산장비실유지보수	유지보수로 서버가상화
네트워크품질관리시스템(패킷로직)	유지보수로 서버가상화 이중화
보안관제 보안관제 서비스	유지보수로 세종IDC(Internet Data Center 사용
소프트웨어 라이선스	유지보수로 싱글사인온(SSO)
소프트웨어 오라클스탠다드	유지보수로 영업지원시스템 개발툴
시스템 유지보수비	유지보수로 유해차단소프트웨어
유지보수 경영계획시스템(MPS)	유지보수로 인사정보
유지보수로 DB ERP모니터링	유지보수로 전산장비(서버및스토리지)
유지보수로 DB MS-SQL	유지보수로 전자결재, 메일, 메신저 시스템
유지보수로 DB TMS모니터링	유지보수로 전자문서
유지보수로 DB리오그	유지보수로 전자세금계산서
유지보수로 EIS	유지보수로 접근통제및암호화
유지보수로 ERP긴급지원(ACS)	유지보수로 차세대UTM 1차.2차
유지보수로 ERP및DB	유지보수로 통신회선및장비
유지보수로 ERP서버및 스토리지	유지보수로 통합백업시스템
유지보수로 IT자산관리	유지보수로 팔콘CDP 백업시스템
유지보수로 PC및프린터	유지보수로 향온항습기
유지보수로 POP시스템 관리	유지보수로 회선품질
유지보수로 PRM	유지보수로 휴폐업조회이용료
유지보수로 SCM공급망시스템	임차료 DR센터유 닉스서버(M10-4)
유지보수로 TMS솔루션 및 통신스위치	임차료 ERP서버
유지보수로 TMS이중화솔루션	전산비용
유지보수로 Vmware	전산사용료 E2K 200 임대비용
유지보수로 WAS	전산사용료 인터넷 AS유지수수료(연간)
유지보수로 개인정보 웹방화벽	전산소모품 PC관련부품
유지보수로 그룹웨어및지식관리	전산소모품 기타
유지보수로 네트워크 모니터링 시스템	전산소모품 서버및주변장치관련부품
유지보수로 네트워크백본	전산소모품 프린터리본및카트리지
유지보수로 네트워크이블	컨설팅료 서버성능평가및튜닝
유지보수로 동영상스트림서비스	통신회선료 LG
유지보수로 레이저프린터	통신회선료 기타
유지보수로 매입통합시스템	통신회선료 세종