e-Discovery 포렌식 자료를 위한 위기대응관제시스템 인증 연구

천우성°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: deux8522@gmail.com · prof1@paran.com

A Study of Authentication and encryption for e-Discovery Forensic Data

Woo-Sung Chun°, Dea-Woo Park*
°*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

GM대우차와 쌍용차에 관한 기술 유출 사고에서의 국가 경제적인 피해로 인하여 e-Discovery 제도 도입과 연구가 필요하다. 본 논문에서는 e-Discovery에 개념과 관련법안 및 권고안, 포렌식 수사절차에 대해 연구하고, 한국의 e-Discovery 사고 사례를 연구고, e-Discovery가 도입되면 포렌식 자료를 위한 보안관제시스템에서의 인증과 암호화를 연구하였다. 보안관제시스템의 접근과 인증을 위한 사용자인증과 기기인증에 대한 기술과 암호화 기술을 연구하였다. 본 논문 연구를 통하여 e-Discovery 제도의 도입과 포렌식 기술 발전에 기초자료로 활용될 것이다.

키워드: 전자증거개시(e-Discovery), 포렌식 자료(Forensic Data), 암호화(Encryption), 인증(Authentication), 보안관제시스템(Security Emergency Response System)

I. 서론

2009년 9월 한국법인에 취업한 한국인 연구원들이 GM대우자동차의 라세티 승용차 개발 기술을 통째로 빼내 실제로 러시아에서 불법복제 차량을 만든 것으로 드러나 막대한 산업기술 유출 피해를 본 것으로 추정된다. 이 불법복제 차량은 이미 러시아에서 'C100'이라는 브랜드로 1만2000~1만3000달러에 팔리고 있다[1].

수사 결과 C100 승용차를 개발하는데 쓰인 기술표준 문서는 GM대우의 기술표준과 완전히 같은 것으로 밝혀졌다. 기술표준문서는 자동차의 설계, 각종 실험방법, 부품의 재질 등에 대한 기준과 조건을 정한 문서로 자동차의 설계에 핵심적인 역할을 한다.

쌍용차 기술유출 사건의 수사에서는 정부의 지원으로 개발된 디젤 하이브리드 자동차 기술 등을 상하이자동차 측에 넘긴 혐의로 부정경쟁방지 및 영업비밀보호에 관한법률 등 위반 혐의로 쌍용차의 종합기술연구소장 이모씨 등 연구원 7명을 불구속기소했다.

그림 1은 2009년도 1분기 기술유출범죄 처리내역을 나타낸 것이다[2].

그림 1. 2010년도 1분기 기술유출 범죄처리 현장
Fig. 1. The first quarter of FY 2010 Technical Disclosure crime scene processing

기업이나 국가의 중요한 기술 유출 사고가 발생하면 피해액은 수천억원에서 수조원대에 이르러 국가 경제에 미치는 영향이 크다.

미국에서는 2006년 12월 1일 발효된 '미연방민사소송법(FRCP)'는 discovery의 대상이 되는 증거물의 범위에 ESI(Electronically Stored Information)을 포함하여 e-Discovery의 법률적 근거를 마련하였다. 한국에서도 기술유출과 경제적 피해에 책임을 정하기 위해 e-Discovery제도의 도입이 필요하며, e-Discovery에 대한 연구가 필요하다.

특히 기업의 중요한 기밀 유출에 관한 경제적 피해액과 경제적, 법률적, 기술적 파장을 고려 할 때, 우리나라에서도 e-Discovery 제도에 대비한 방법을 마련하고자 하는 연구 노력이 필요하다.

II. 관련 연구

2.1 e-Discovery

OSI2006년 12월 1일 발효된 '미연방민사소송법(FRCP)'는 discovery의 대상이 되는 증거물의 범위에 ESI(Electronically Stored Information)를 포함한다. 대부분의 미국 기업은 전자정보(ESI)의 법률적인 요구에 따른 벌금, 시간, 회사평판 등의 손실을 막기 위한 대책이 필요하다. 통상 10~100개의 상시 소송에 시달리는 기업의 입장에서는 소송에 능동적으로 대응하기 위해서는 관련정보를 쉽게 식별/보관할 수 있는 툴의 도입이 필요하다.

그림 2는 e-Discovery의 참고 모델이다.

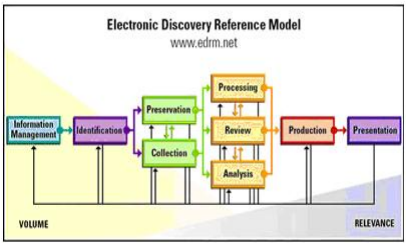

그림 2. e-Discovery 참고 모델
Fig. 2. e-Discovery reference model

2.1.1 e-Discovery 관련 법안 및 권고안

전자기록물을 법률적 증거자료로 인정하면서 e-Discovery 관련된 법안 및 권고안에 관한 내용을 표 1에 정리 하였다[3].

표 1. e-Discovery 관련 법안 및 권고안
Table 1. e-Discovery legislation and recommendations

No	전자기록물 관련 법안 및 권고안
1	SOX (Sarbanes-Oxley Act)
2	e-Discovery법 : FRCP 26 [2006 amendments to U.S.FRCP (Federal Rules of Civil Procedure) 개정]
3	SEC (Securities and Exchange Commission) Rule 17a-4
4	NASD (National Association of Securities and Dealers) Rules 3010 & 3110
5	FDA 21 CFR Part 11
6	HIPAA Privacy Rule
7	우리나라 전자거래 기본법

2.1.2 e-Discovery 포렌식 절차

미국에서는 디지털 증거에 대한 제출을 정당화하는 e-Discovery 제도가 시행되어 2006년 12월부터 시행되면서, 민 · 형사 분쟁 발생 시 방대한 양의 디지털 자료로부터 분쟁에 필요한 자료를 효율적으로 추출하는 포렌식 툴에 대한 연구뿐만 아니라, 포렌식 절차에 관한 연구가 필요하다. 그림 3은 미국 e-Discovery 포렌식 절차에 관한 연구 내용이다[4].

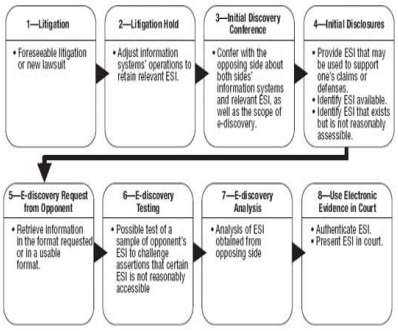

그림 3. e-Discovery 절차
Fig. 3. e-Discovery process

2.2 디지털 포렌식과 수사기술

디지털 포렌식(Digital Forensics)은 법정 제출용 디지털 증거를 수집하여 분석하는 기술을 말하며 인권을 강조하는 요즘 IT 관련 기관과 기업을 중심으로 많은 관심이 집중되고 있다[5]. 디지털 증거수집 및 분석과정은 기술적으로 복잡하고 난해하여 분석가의 전문성에 의해 증거의 무결성과 신뢰성이 결정된다. 첨단 과학기술을 이용하는 디지털 포렌식은 사법기관의 인권보호와 사법 정의 구현에도 필요하다. 그림 4는 디지털 포렌식 조사 개념도를 나타낸 것이다[6].

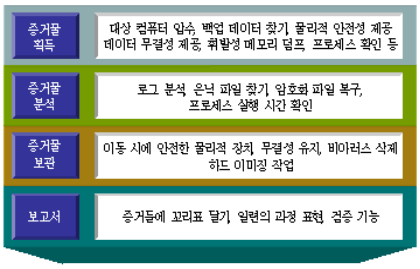

그림 4. 포렌식의 개요
Fig. 4. Forensic Overview

디지털 포렌식은 "전자적으로 처리되어 보관·전송되는 디지털 데이터를 적법한 절차와 과학적 기법을 사용해 수집·분석해서 증거로 제출하는 제반 행위"로 정의되고 있다.

디지털 포렌식은 검찰, 경찰 등의 국가 수사기관에서 범죄 수사에 활용되며, 일반 기업체 및 금융회사 등의 민간분야에서도 디지털 포렌식 기술의 필요성이 증가하고 있다. 예로써, 포렌식 기술은 보험사기 및 인터넷 뱅킹 피해보상에 대한 법적 증거 자료수집 및 내부 정보 유출 방지, 회계 감사 등의 내부보안 강화에 활용 가능하다[7].

포렌식 수사 절차는 수사준비, 증거수집, 증거 보관 및 이송, 증거 분석, 보고서 작성 등의 다양한 단계로 구성되며 각 단계에서 다음 단계로의 절차연속성의 유지는 무엇보다 중요하다.

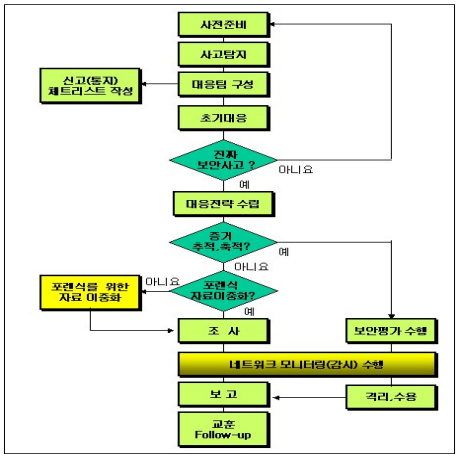

그림 5. 네트워크 포렌식 증거 수집 절차
Fig. 5. Network forensic evidence collection procedures

수사준비 단계에서는 증거의 수집 및 분석을 위한 포렌식 도구의 구비 및 장비 점검을 하여 신속한 수사가 이루어질 수 있도록 하며, 수사관에 대한 교육을 통해 운용 가능한 도구를 최대한 활용할 수 있도록 한다. 그림 5는 네트워크 포렌식 증거 수집 절차를 나타낸 것이다[8].

증거 수집 단계에서는 현장의 사진을 촬영하고, 압수수색 영장이 허용하는 범위에서 하드웨어, 소프트웨어, 보조기억장치 등을 수집한다. 대상 시스템이 활성화 되어 있는 상태일 경우에는 휘발성데이터를 수집한다. 하드디스크와 같은 저장 매체의 경우에는 무결성을 해치지 않도록 주의하여 이미징 작업을 수행하고 추후 변조되지 않았음을 입증하기 위해 해쉬값을 계산하여 저장한다. 증거 보관 및 이송단계에서는 디지털 증거물이 이송 및 보관 과정에서 손상되지 않도록 쓰기 방지 조치를 취하고, 정전기 방지용 팩을 사용하여 외부의 전자기력으로 인한 손상을 예방해야 한다. 증거 분석 단계에서는 상황에 따라 적절한 포렌식 도구를 이용하여 법정에 제출할 디지털 증거를 검색 및 복구한다. 보고서 작성 단계에서는 보고서를 읽게 되는 법관, 변호사 등 컴퓨터에 대한 지식이 부족한 사람이 보더라도 쉽게 알 수 있는 형태로 작성이 되어야 하며, 증거물 수집, 보관, 분석 등의 과정을 6하 원칙에 따라 명백하고 객관성 있게 작성되어야 한다[9].

III. e-Discovery 사고 사례 연구

3.1 GM대우자동차의 라세티 승용차 개발 기술 유출

사건의 발단은 GM대우의 기술을 확보한 황 상무가 2007년 7월 부하 직원 정모씨에게 외장형 하드디스크를 건넸다. 황 상무는 “여기에 저장된 파일을 다른 외장형 하드디스크에 여러 개 복사한 뒤 팀장들에게 전해서 팀원들이 활용할 수 있도록 하라”고 지시했다. 황 상무가 건넨 외장형 하드디스크에는 GM대우자동차의 승용차 ‘라세티’ 차체 및 섀시 관련 설계도면 파일 2103개와 GM대우의 기술 표준문서 파일 1534개가 담겨 있었다.

이 하드디스크를 건네받은 정 씨는 복사를 한 뒤 섀시 설계팀장 이모씨 등 각 부문 설계팀장들에게 나눠주었다. GM대우의 기술이 타가즈코리아로 유입되면서 신차 개발도 활기를 띠기 시작했고 올해 3월 ‘C100’이라는 신차 개발에 성공했다. 라세티 기술을 도용해 만든 ‘불법복제 라세티’였다.

3.2 쌍용자동차 디젤 하이브리드 기술 유출 사건

네트워크서울중앙지검 첨단범죄수사1부(한찬식 부장검사)는 11일 국고의 지원으로 개발된 디젤 하이브리드 자동차 기술 등을 상하이자동차 측에 넘긴 혐의로 부정경쟁방지 및 영업비밀보호에 관한법률 등 위반 혐의로 쌍용차의 상무급 종합기술연구소장 이모씨 등 연구원 7명을 불구속기소했으며, 연구소에 부소장으로 파견근무하면서 중국 본사의 지시로 이들 연구원에게서 첨단 기술을 빼낸 중국인 J씨를 같은 혐의로 기소중지했다[10].

검찰에 따르면 이씨 등은 2006년 7월 하이브리드 자동차 중앙통제장치(HCU)의 소스코드를 상하이차에 제공하라는 J씨의 요구에 따라 기술이전에 대한 이사회 결의 등 적법절차를 거치지 않고 비슷한 차종을 개발하는 상하이차에 소스코드를 유출한 혐의를 받고 있다.

특히 이씨 등은 2005년 4월 시험용 하이브리드차를 만들면서 지인을 통해 경쟁사인 현대자동차의 하이브리드차 전용 회로도를 불법으로 입수, 이를 연구 중이던 자사 제품에 사용한 것으로 드러났다. 또 이 씨 등은 2007년 6월 상하이차의 하이브리드차 개발에 필요하다는 이유로 쌍용차의 카이런 디젤 엔진과 변속기 기술자료를 이메일로 상하이차 측에 넘겨준 것으로 조사됐다.

검찰은 2006년 8월 상하이차가 쌍용차의 기술을 유출했다는 쌍용차노조의 고발장을 접수한 뒤 국가정보원 정보 등을 토대로 3년여간 수사를 벌여왔다[11].

IV. e-Discovery를 위한 보안관제시스템 연구

기업에서 e-Discovery 적용을 위해서는 기업의 보안관제시스템이 필요하다. 기업의 중요자료에 대한 사이버테러의 체계적인 대응을 위해서는 자동화된 협력대응 프레임워크 기반에서 사이버공격 사전 예·경보와 즉각적 대응/차단을 할 수 있는 통합 보안 제어기술이 필요하다.

기업의 일상 업무에 e-Discovery를 적용하기 위해서는 업무에서 발생하는 많고 다양한 보안 이벤트를 통해, 여러 보안 위협 발견 및 대응 가능한 e-Discovery 보안관제 기술 및 체계 개발과 e-Discovery의 복잡한 네트워크 구조에서도 사이버 보안 침해 상황을 쉽게 파악할 수 있는 가독성 높은 통합보안 모니터링시스템이 필요하다.

그림 6은 보안관제시스템 구성도를 나타낸 것이다.

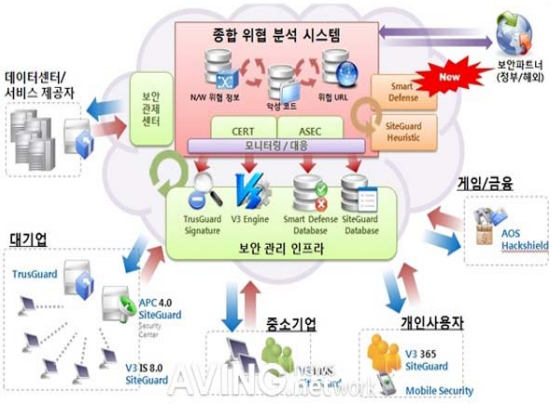

그림 6. 보안관제시스템 구성도
Fig. 6. Security Emergency Response System Configuration

그림 6처럼 국외 대규모 시스템에서의 권한관리 기술 분석을 통해 e-Discovery 환경에 적합한 제어기술로 대규모 기업 업무관리 솔루션 등 다양한 소프트웨어에서 구현된 권한 관리 기법에 대해 분석하여, 복잡한 구조의 e-Discovery 환경에 적합하도록 통합제어 모델을 설계하고, 이에 따라 통합제어를 하여야 한다.

국내 기업은 정보보호 기업과의 협력강화로 국내·외 표준 참조

하여 기존 네트워크 상태정보 분석 기술을 전력정보 분석을 통한 이상 징후 식별 기술에 접목시켜, e-Discovery에서의 보안상황 인지기술에 대한 핵심 IPR(Intellectual Property Right)을 확보한다. 해외 사례 분석 및 기 개발된 요소 기술 분석 및 참조하여 e-Discovery 환경에 적합한 3D 시각화기술 핵심 IPR 확보한다. 공통 메시지 및 프로파일 생성을 위한 국내·외 표준 참조하고 침해사고 프로파일 생성 및 공통 메시지 포맷을 설계하고, 이를 교환하기 위한 통합플랫폼을 개발하여야 한다.

V. e-Discovery를 위한 보안관제의 인증과 암호화 연구

5.1 인증을 위한 구성

e-Discovery를 기기인증 체계는 해외에서 사용되는 Verisign 등의 인증 체계를 분석하여, 그림 7처럼 e-Discovery의 고유식별값을 인증서의 필드값에 반영하고 별도의 난수값으로 유출되지 않도록 하여 다른 e-Discovery에서는 작동이 되지 않도록 하고 전자서명 기술을 통한 상호인증으로 접속 정보의 무결성 확보한다.

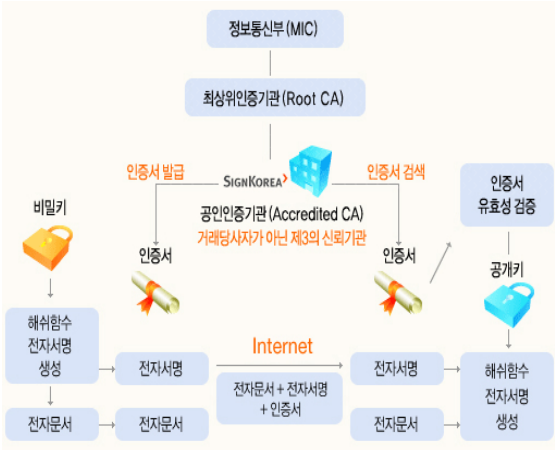

그림 7. 인증 구조 구성도
Fig. 7. Authentication scheme configuration

또한 안전한 PKI 기반의 인증서 분배 및 관리 정책을 적용한다. 기업의 정보전달 활동에서 실시간 정보를 교환하기 위한 유선 혹은 무선의 다양한 통신 방식을 통하여 중요한 정보를 송수신 하게 된다. 이때 안전한 데이터 송수신을 위해 네트워크에 접속되는 모든 device에 대해 ECC(Elliptic Curve Cryptosystem)기반의 인증서를 탑재하여 데이터 암호화 및 인증을 수행한다.

e-Discovery를 위한 각 단말이 서버와 데이터에 접속을 할 때에는 상호간 인증서를 제출하여 유효성 검증을 하게 되는데, 효율적인 검증을 위해 SCVP(Server-based Certificate Validation Protocol) 방식을 사용하여 기기의 부하를 최소화 한다. 또한 인증서의 기간만료 혹은 해킹 우려 등의 사유로 인해 교체가 되어야 할 경우 이를 가능하게 하는 온라인상의 재발급 및 폐기 기능 등을 제공한다.

표 2는 공인인증서와 기기인증서 비교를 한 표이다.

표 2. 사용자인증서와 기기인증서 비교
Table 2. User certificates and equipment compared to the certificate

	사용자 인증서	기기 인증서
대상	사람	기기
인증방법	인증서	인증서, Mac 어드레스, 시리얼넘버 등
인증서 신청자	인증서 이용자	기기 제조업자
인증서 보관장소	PC, 이동식저장매체	기기내 비휘발성 메모리
인증서 암호	사용자 암기	기기내 저장
효력	추정 효력	(효력부여 범위 이견)

5.2 인증을 위한 암호화 기술

그림 8처럼 인증서의 저장방식이 S/W인 경우 난수 값을 통하여 암호화하고 H/W 저장이 가능한 경우 칩 내부 인증서를 저장한다. 또, 모든 device간 통신은 TLS(Transport Layer Security)를 통하여 암호화 한다.

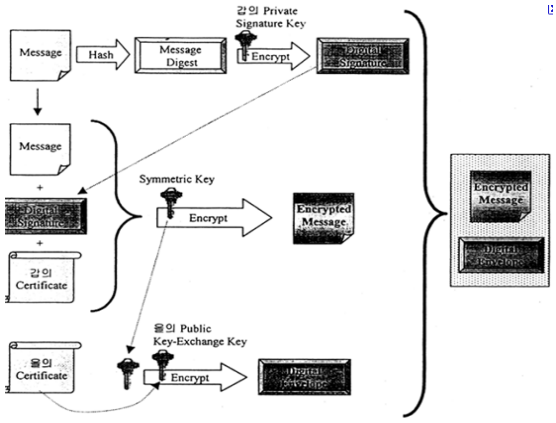

그림 8. 암호화 구조
Fig. 8. Encryption scheme

기기와의 접속이 시도될 때 인증서 제출을 요청하여 유효한 인증서가 아닐 경우 접속 차단하고 기기인증서 발급 시 관련 업체의 대면확인으로 기기제조사와 기기의 연관 정보 확보한다.

e-Discovery의 개체 인증 이외에 관제 시스템으로 접근하는 모든 device에 인증서를 통하여 접근 할 수 있게 한다.

VI. 결론

GM대우차와 쌍용차의 기술유출 사고와 같이 기술 유출 사고는 국가의 경제적인 손해를 끼치고 그에따른 파급효과로 인하여 e-Discovery 제도 도입이 시급한 상황이다.

본 논문은 e-Discovery의 국내의 사고 사례와 해외 사고 사례

를 연구하였고, 사고에서 손해배상과 법률적인 책임을 판단하기 위해서는, 기업에서 일상 업무에 포렌식 절차에 맞게 자료를 생성하고, 법적 근거 자료로 사용가능한 포렌식 자료를 생성하여야 한다. 이를 위해서 본 논문에서 제안한 e-Discovery를 위한 보안관제시스템을 구성하여야 하고, 보안 관제의 인증과 암호화를 하기 위해 기기인증과 사용자 인증을 나누어서 비교 하였으며, 인증을 위한 암호화 기술을 연구하였다. 이 기술을 바탕으로 기업들은 회사자료들을 e-Discovery하는 노력을 해야 하며, 체계적인 보안관리시스템의 도입으로 포렌식 자료를 생성하여야 한다.

향후 연구로는 e-Discovery 제도에 도입에 따른 법제화 과정에서 보안 관제의 인증과 암호화를 제도에 넣는 연구가 필요하다.

참고문헌

[1] 동아닷컴, “GM대우 출신 연구 인력 100여명 영입,” http://www.donga.com/fbin/output?n=200909100175, 2009. 9.

[2] 연합뉴스, “검찰 “쌍용차 첨단기술 中에 유출됐다”(종합),” http://www.yonhapnews.co.kr/bulletin/2009/11/11/0200000000AKR20091111089851004.HTML, 2009. 11.

[3] 김유승, “『공공기록물 관리에 관한 법률』의 제정 의의와 개선방안,” 한국기록관리학회지, 8(1), 5-25쪽, 2008. 6.

[4] Silka Maria Gonzalez, CISA, CISM, CPA, CISSP, CITP, New Rules Regardinge-discovery, Information system control journal, Vol 3, 2007.

[5] 강동욱, “디지털증거 수집에 관한 형사소송법 개정안에 대한 검토,” 경상대학교 법학연구소, 18(3),2010.

[6] 권양섭, “디지털 포렌식 법률체계 구축 방안,” 한국법학회, 법학연구, 35권, 357-382쪽, 2009. 8.

[7] 이규안, 박대우, 신용태, “포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구,” 한국컴퓨터정보학회논문지, 11(6), 175-184쪽, 2006. 12.

[8] 전명길, “디지털증거의 수집과 증거능력,” 한국법학회, 법학연구, 41권, 317-336쪽, 2011. 2.

[9] 디지털 포렌식 연구센터, 네트워크 증거 수집 절차, http://forensic.korea.ac.kr/guide/cfg.php?type=9, 2009. 6.

[10] 대검찰청 첨단범죄수사과 기술유출범죄수사센터 통계, 2009년도 1분기 기술유출범죄처리내역, http://www.spo.go.kr/user.tdf?a=user.board.BoardApp&c=2002&seq=16&board_id=icic_b03&cp=2&pg=1&npp=10&catmenu=110204&chungcd=01000000, 2009. 5.

[11] 서울신문, “검찰 쌍용차 첨단기술 中에 유출됐다,” http://service.seoul.co.kr/news/newsView.php?id=20091111800033&spage=3, 2009. 11.