e-Discovery 시스템 설계와 관리를 위한 인증과 암호화

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

Design of Emergency Response e-Discovery Systems using Encryption and Authentication

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

● 요 약 ●

해외 기술 유출 사고로 인하여 한국 경제에 약 수조원의 피해가 발생하였다. 기업의 기술 유출과 사고 책임 소재를 증명하기 위한 e-Discovery시스템과 기업CERT/CC에 연구가 필요하다. 본 논문에서는 e-Discovery의 개념과 관련법안 및 권고안, 포렌식 수사절차에 대해 연구하고, 국내 e-Discovery 사고 사례와 해외 e-Discovery 사고 사례를 연구한다. e-Discovery가 도입되면 기업 CERT/CC에서 필요한 e-Discovery 시스템을 설계한다. e-Discovery 시스템의 접근과 인증을 위한 사용자인증과 기기인증에 대한 기술과 암호화 기술을 연구한다. 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), CERT/CC(Computer Emergency Response Team/Coordination Center)

I. 서론

GM대우차의 라세티 승용차 개발 기술을 빼내가서, 러시아에서 생산한 불법복제 차량은 '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 위반이다.

그림 1은 대검찰청 첨단범죄수사과에서 발표한 2009년도 1분기 기술유출범죄 처리내역이다[2].

그림 1. 2009년도 1분기 기술유출범죄 처리내역
Fig. 1. Technical Disclosure Crime Processing History at Q1 2009

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.

본 논문에서는 e-Discovery의 개념과 관련법안 및 권고안, 포렌식 수사절차에 대해 연구하고, 국내 e-Discovery 사고 사례와 해외 e-Discovery 사고 사례를 연구한다. e-Discovery가 도입되면 기업 CERT/CC(Computer Emergency Response Team/Coordination Center))에서 필요한 e-Discovery 시스템을 설계하였다. e-Discovery 시스템의 접근과 인증을 위한 사용자인증과 기기인증에 대한 기술과 암호화 기술을 연구한다.

II. 관련 연구

2.1 e-Discovery

2006년 12월 1일 발효된 '미연방민사소송법 (FRCP)'는

discovery의 대상이 되는 증거물의 범위에 ESI를 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.

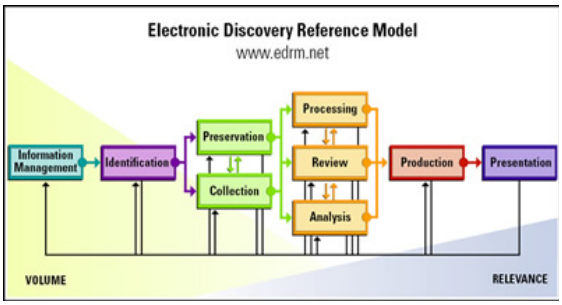

그림 2. e-Discovery 참고 모델
Fig. 2. e-Discovery reference model

2.2 e-Discovery 관련 법안 및 권고안

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

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

N0	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

2.3 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

III. e-Discovery 시스템 설계

기업에서 e-Discovery 적용을 위해서는 기업의 e-Discovery 시스템 설계를 하여야 한다. 기업의 중요자료에 대한 사이버테러의 체계적인 대응을 위해서는 자동화된 협력대응 프레임워크 기반에서 사이버공격 사전 예·경보와 즉각적 대응/차단을 할 수 있는 CERT/CC가 필요하다.

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

그림 6은 e-Discovery 관리시스템 구성도를 나타낸 것이다.

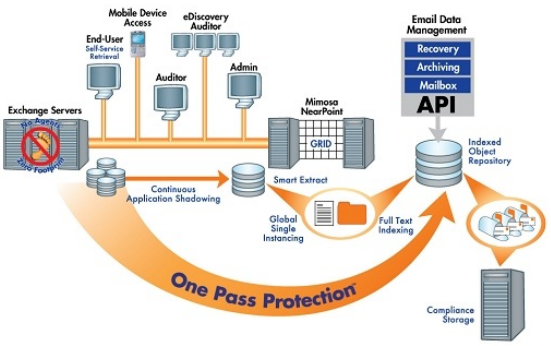

그림 6. e-Discovery 관리시스템 구성도
Fig. 6. e-Discovery Management System Configuration

e-Discovery 포렌식 자료를 위한 관리시스템은 인증과 암호화를 통한 신분확인, 접근제어, 무결성 검증에 대한 검증자료 확보를 위해서 기본 시스템 구축을 설계 연구한다.

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 참조하여 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.

IV. e-Discovery 자료의 인증과 암호화 연구

4.1 e-Discovery 인증 구성

e-Discovery를 기기인증 체계는 해외에서 사용되는 Verisign 등의 인증 체계를 분석하여, [그림 7]처럼 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.

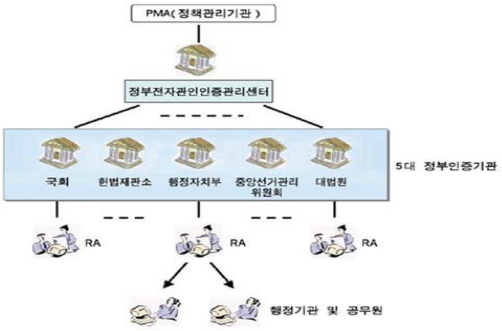

그림 7. 인증 구조 구성도
Fig. 7. Authentication scheme configuration

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. e-Discovery사용자인증서와 기기인증서 비교
Table 2. e-Discovery and the device certificate, the certificate compared to users

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

4.2 인증 정보 무결성 확보를 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.

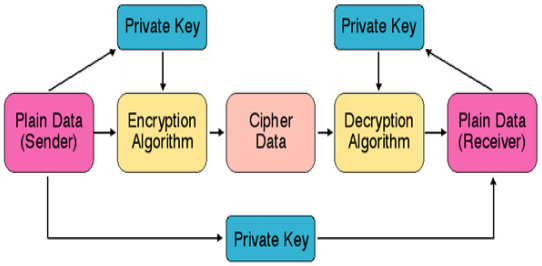

그림 8. 암호화 구조
Fig. 8. Encryption scheme

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 관리 시스템으로 접근하는 모든 device에 인증서를 통하여 접근 할 수 있게 한다.

V. 결론

우리나라에서 발생한 GM대우차와 쌍용차에 관한 기술 유출 사고와 같이 국가 경제적인 파급효과로 인하여 e-Discovery 제도 도입이 시급한 상황이다.

본 논문은 기술 유출 사고에서 손해배상과 법률적인 책임을 판단하기 위해서는, e-Discovery를 통한 기업의 일상 업무에서 포렌식 절차에 맞게 법적 근거 자료로 사용가능한 e-Discovery 포렌식 자료를 생성하여야 한다. 이를 위해서 본 논문에서 제안한 e-Discovery를 위한 관리시스템을 구성하고, 보안 관리의 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 관리시스템의 도입으로 포렌식 자료를 생성하여야 한다.

향후 연구로는 e-Discovery 제도에 도입에 따른 법제화 과정에서 보안 관리의 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] 대검찰청 기술유출·인터넷범죄수사, “2009년도 1분기 검찰처리내역,” 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.

[3] 김정하, “우리나라의 국가기록물관리를 위한 제연,” 국제지역연구, 11(3), 187-212쪽, 2007.

[4] Silka Maria Gonzalez, CISA, CISM, CPA, CISSP, CITP, “New Rules Regarding e-discovery,” Information system control journal, 3, 2007.

[5] 이창훈, 백승조, 김태완, 임종인, “E-Discovery를 위한 디지털 증거 전송시스템에 대한 연구,” 정보보호학회논문지, 18(5), 171-180쪽. 2008. 10.

[6] 연합신문, “‘검찰’ 쌍용차 첨단기술 中에 유출됐다,” http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=001&aid=0002969606, 2009. 11.

[7] 유영현, 송봉규, 박상진, 디지털포렌식(Digital Forensic) 전문인력의 필요성과 양성방안,” 한국경찰학회보, 22, 253-284쪽, 2009.