情 報 保 護 學 會 誌
第 18 券 第 1 號, 2008. 2

기업의 원격 포렌식 시스템 구축의 필요성

박 보 라*, 심 미 나*, 이 상 진*

요 약

많은 기업이 대형 네트워크를 사용하고 있으며 이는 기업 내·외의 정보교환과 업무 원활화를 위하여 사용된다. 하지만 이러한 인트라넷(Intranet) 혹은 인터넷의 사용은 기업의 기밀 유출 혹은 사원들의 컴퓨터 자원 낭비로 이어지기도 하며 이는 사회적으로 큰 손실을 내기도 한다. 또한 E-discovery법의 시행에 앞서서 차후에 발생할 수 있는 많은 법적인 분쟁에 대비하기 위하여 기업은 디지털 증거들을 사전에 수집하고 보관 및 분석할 수 있어야 한다. 이를 위하여 기업들은 디지털 포렌식에 관한 정책 및 기술을 정립하고 확보해야 하며 특히, 원격 포렌식 시스템을 구축하는 데에 주력해야 한다. 정보보호 정책과 기술을 바탕으로 한 원격 포렌식 시스템을 구축하는 것은 기업 내 정보 유출의 방지, 포렌식 관점에서의 정보 수집 및 분석 그리고 법정 소송에의 신속한 대응을 가능하게 한다는 점에서 기업의 정보보안에 관한 노력과 예산을 많이 줄여줄 수 있다. 본 논문에서는 원격 포렌식 시스템의 개념, 그리고 각국의 원격 포렌식 시스템 구축 현황을 바탕으로 기업에서의 원격 포렌식 시스템 구축에 관한 필요성을 주장하고자 한다.

Ⅰ. 서 론

현대의 모든 기업은 사업의 발전을 위한 고유의 정보를 가지고 있으며 이는 해당 기업의 핵심 자산이 된다. 이러한 정보는 첨단 기술뿐 아니라 직원 및 기업과 관련된 개인들의 정보를 포함한다. 최근에는 이러한 정보를 노린 디지털 기기에 대한 네트워크 및 시스템에 대한 침해 사고뿐만 아니라 이를 포함한 사이버 범죄가 전반적으로 증가하고 있다. 기업의 기술과 정보를 보호하기 위해서는 기업 차원에서의 정보보안을 위하여 적절한 정보보안 수단을 강구해야 한다. 특히, 기업의 경우 여러 가지 법정 분쟁에 대응해야 하는 경우가 많기 때문에 디지털 포렌식 기술에 기반을 둔 증거 확보 및 증거 분석에 관한 정책을 확립하고 해당 기술을 보유하고 있어야 한다. 또한 사고가 발생하였을 때 즉각적으로 사고에 대응할 수 있는 시스템이 갖추어져 있어야 한다. 이상적으로는 증거 확보와 증거 분석이 동시에 혹은 연속적으로 시행되어야 하지만 실제로 사건 대응으로 인한 증거 확보와 디지털 포렌식 관점에서의 증거 분석에는 시간적으로 많은 격차가 존재하며 이는 증거 확보에 지장을 준다는 면에서 이를 보완할 '원격 포렌식 시스템'이 필요하다.

일반적으로 침해 사고 대응은 사고 대응에 관한 정책 및 절차의 정립 혹은 관련기관과의 협력관계를 구축함으로서 시작한다. 실제로 사고가 감지되었을 때는 포렌식 전문가가 검증받은 포렌식 도구로 해당 시스템에서 데이터를 획득하고 그 데이터를 분석한다. 그리고 사고 대응 중에 일어난 모든 일들, 그리고 사고 대응 팀에서 조사를 행한 모든 절차를 문서화하여 기록한다.

사고 대응은 네트워크나 시스템에 대한 불법적이고 비정상적인 접근에 대한 컴퓨터 보안 측면에서의 대응이다. 반면 컴퓨터 포렌식은 법적인 용어로서 이는 법정에서의 신뢰성을 획득하기 위해 컴퓨터 내의 데이터에서 증거를 발견해내는 것을 의미한다. 가장 이상적인 것은 사고 대응과 동시에 컴퓨터 포렌식을 하는 것이다. 법적인 문제를 고려하지 않은 사고 대응은 많은 증거를 훼손시키거나 잃을 수 있다. 또한 사고가 원거리에서 일어나거나 다수의 시스템에서 동시에 일어났을 때 즉각

본 연구는 정보통신부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S019-01, 정보투명성 보장형 디지털 포렌식 시스템 개발]

* 고려대학교 정보경영공학전문대학원 (danver123@korea.ac.kr, mnshim@korea.ac.kr, sangjin@korea.ac.kr)

적인 대응을 하기 어려우며, 컴퓨터 포렌식 관점의 증거 확보 및 수집에도 문제가 생긴다.

이러한 문제를 해결할 수 있는 것이 원격 포렌식 시스템이며 이는 상대적으로 멀리 떨어진 장소에의 컴퓨터 혹은 디지털 기기에 대한 분석을 실시간으로 가능하게 한다. 이를 고려할 때, 원격 포렌식 시스템을 구축하는 것은 신속성이 요구되는 네트워크 및 시스템 침해 사고 대응 절차상에서 비용 및 시간을 절약할 수 있는 최적의 방안이다. 따라서 시간, 비용 효율적이고 신속한 사고 대응이 가능한 원격 포렌식 시스템의 구축은 각종 침해 사고의 피해를 줄이기 위해 필수적이며 많은 증거를 보존하게 됨으로써 사고 대응의 질을 높일 수 있다.

본 논문에서는 원격 포렌식 시스템 구축의 필요성을 주장하기 위하여 다음과 같은 순서로 구성되어 있다. 우선 원격 포렌식 시스템의 개념과 목적, 기능, 한계점 그리고 현존하는 원격 포렌식 도구에 대하여 소개한다. 그리고 현재 한국을 비롯한 각국에 구축되어 있는 원격 포렌식 시스템에 대한 인식 혹은 구축 현황에 대해 살펴보고 그 필요성에 대해 역설한다. 마지막으로 원격 포렌식 시스템의 구축으로 인한 기업에서 가질 수 있는 기대 효과에 대해 논의하면서 결론을 짓는다.

Ⅱ. 원격 포렌식 시스템

디지털 증거를 다루는 것은 시간과 비용이 많이 드는 작업이다. 또한 디지털 증거를 다루는 사건은 증거 수집과 동시에 증거를 보존하는 작업이 이루어져야 하며, 최대한 빨리 사고에 대응해야 한다[1]. 복합적인 상황이 동시에 일어나는 사고 현장에서 사고에 대응하고, 컴퓨터 포렌식 관점에서 증거 데이터를 수집 및 분석하는 과정에서 가장 중요한 것은 시간이다. 하지만 해당 사고가 원거리에서 일어나거나 동시에 다수의 기기를 조사해야 한다면 즉각적인 사고 대응이 어렵고 현장에 도착할 때까지 증거의 변조 및 유실 상황을 막을 수 없다. 원격 포렌식 시스템은 이러한 문제를 해결할 수 있는 가장 좋은 방법이다.

2.1. 원격 포렌식 도구 및 시스템의 개념

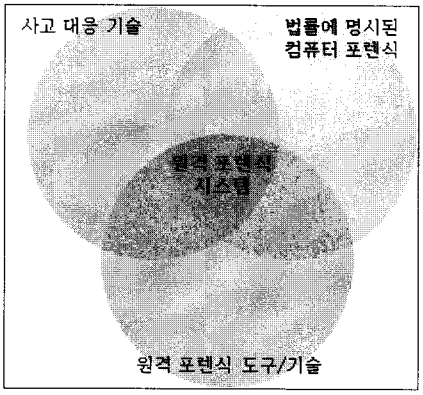
2.1.1. 원격 포렌식 도구

원격 포렌식 도구는 기존의 네트워크 및 시스템 침해 사고 대응 절차에서 사고의 감지, 사고 대응, 데이터의 수집과 분석 그리고 리포팅(Reporting)을 자동으로 하는 시스템이다. 개별적인 컴퓨터에 대해 행하던 사고 대응 및 컴퓨터 포렌식 수사절차를 자동화하여 원거리의 시스템에 대해서도 행할 수 있다. 원격 포렌식 도구를 사용하는 것은 휘발성 데이터의 확보가 중요한 네트워크 및 시스템에의 침해 사고에 대한 대응과 디지털 포렌식 관점에서의 증거 분석 간에 생길 수 있는 격차를 줄일 수 있다[2].

현재 대표적인 원격 포렌식 소프트웨어는 세 가지가 있다. ProDiscover IR 3.5(PDIR), EnCase Enterprise Edition 4.19a(EEE) 그리고 eTrust Network Forensic 등이 있다. 이 소프트웨어들은 원격 호스트로부터 디지털 증거를 보존하기 위하여 특별히 제작된 것으로, 원격지 시스템의 변화를 최소로 하면서 증거를 수집하고 분석하는 것이 가능하다[2]. PDIR은 특정 시간대에 하나의 시스템을 조사하기 위한 목적으로 설계되었으며 소수의 시스템을 조사하는 데에 적합하다. 반면, EEE는 기업 보안을 위한 구조이며 이는 접근 제어를 지원하며, 1시간에 최대 30,000대까지 네트워크 내의 모든 컴퓨터에 대한 조사가 가능하다[3]. EEE는 데이터의 조사 및 분석 시에 데이터가 무결성을 유지한 채로 보존될 수 있고, 네트워크 분석을 위한 시스템의 중지 시간을 최소화한다는 장점을 가지고 있다. EEE는 PDIR보다 기업용 보안 솔루션에 적합하다고 평가받고 있으며, 실제로 수사관들에게 수사에 관한 더 많은 정보를 제공하고 있다. Computer Associates 사(社)의 eTrust Nerwork Forensics는 세션 컨텐츠를 포함한 모든 네트워크 활동을 지속적으로 감시하고, 이들을 활용하기 쉬운 데이터베이스로 기록하는 솔루션으로 네트워크 커뮤니케이션이 보안, 네트워크 성능 및 가용성에 미치는 영향에 대한 전체적인 모습을 보여준다[8].

2.1.2. 원격 포렌식 시스템

원격 포렌식 시스템은 원격 포렌식 도구를 기업의 정보보호 절차나 규칙에 따라 운영하고, 사고 대응 중에 획득한 데이터를 법률에 명시되어 있는 '디지털 증거'로서의 효력을 가지도록 수집 및 분석할 수 있도록 운영하는 기술 및 제도적으로 통합된 컴퓨터 포렌식 시스템이다.



〔그림 1〕 원격 포렌식 시스템의 정의

2.2. 원격 포렌식 시스템의 구성 요소

원격 포렌식 시스템은 주로 사고가 발생한 혹은 사고를 발생시킨 컴퓨터, 수사관의 컴퓨터 그리고 두 컴퓨터의 매개체 역할을 하는 서버로 구성된다. 사고가 발생한 혹은 사고를 발생시킨 컴퓨터를 타깃(Target) 컴퓨터, 수사관의 컴퓨터를 에이전트(Agent)라 하자.

2.2.1. 서버

서버는 에이전트에서의 타깃 컴퓨터로의 데이터 요청이나, 데이터 분석 결과 요청을 받아들여 해당 컴퓨터에서의 데이터 수집 및 데이터 분석을 진행한다. 예를 들어 네트워크 침해사고가 발생하였을 때, 사고가 발생한 컴퓨터에 존재하는 침해 탐지 소프트웨어가 네트워크 침입을 탐지하고 이를 서버에 보고하면, 서버는 에이전트로 해당 문제점을 알린다[1]. 문제점을 인식하면, 수사관은 서버를 이용하여 사고가 발생한 컴퓨터에 활성 데이터에 관한 정보를 요청하거나 리포팅 된 데이터 분석 결과를 요청할 수 있다.

서버는 타깃 컴퓨터와 에이전트를 중재하는 역할을 하는 개체로서, 두 기기 간에 전송되는 데이터를 수신할 수 있고, 디지털 매체에 저장할 수 있어야 한다. 타깃 컴퓨터로부터의 침입 탐지 사실을 에이전트로 송신할 수 있어야 하며 에이전트의 타깃 컴퓨터 조사 및 수사 결과를 서버에 저장할 수 있어야 한다. 이러한 기기간의 통신을 중재하는 것은 서버의 핵심기능이다. 또한 이러한 데이터를 안전하게 보관할 수 있어야 하며 서버에 존재하는 데이터로의 수사관의 접근이 용이해야 한다[1,2]. 또한 서버가 조사 및 분석을 에이전트에 의뢰하고 그 분석 결과를 에이전트로부터 수신하기 위해서는 등록된 에이전트에 대한 접근 제어 시스템이 서버에 구축되어 있어야 한다.

2.2.2. 타깃 컴퓨터

타깃 컴퓨터에서는 외부에서 타깃 컴퓨터로의 조사 및 분석에 관한 권한 부여와 관련한 접근 제어 시스템이 잘 갖추어져 있어야 한다. 또한 네트워크 및 시스템 침해 사고의 탐지가 이 컴퓨터에서 발생하는 만큼, 침입 탐지 시스템이 잘 실행되어야 하며 사고가 발생했을 때는 즉각적으로 서버에 해당 문제점을 자동으로 보고하는 시스템이 구축되어 있어야 한다[1,2].

2.2.3. 에이전트

에이전트에서는 원거리에서 시스템에 접속하여 검증받은 실행 파일을 실행시켜 특정 데이터를 획득하기도 하는데, 이 때 실행하고자 하는 실행 파일들의 해쉬 셋을 구축해 두어 해당 프로그램을 실행하고자 할 때는 서버의 해쉬 셋과 비교하여 실행하도록 한다. 이는 에이전트가 항상 읽기 전용 상태가 아니기 때문에 수사관이 소유하고 있는 컴퓨터 내의 실행 파일이 악성 코드에 감염된 상태로 피해 시스템에서 실행되는 것을 피하기 위함이다. 또한 에이전트에 설치된 원격 포렌식 도구는 피해 시스템에서 데이터를 수집할 때, 피해 시스템의 상태를 최소한으로만 변경시키는 상태를 유지하여 최대한 원래 상태를 유지해야 한다.[1,2]

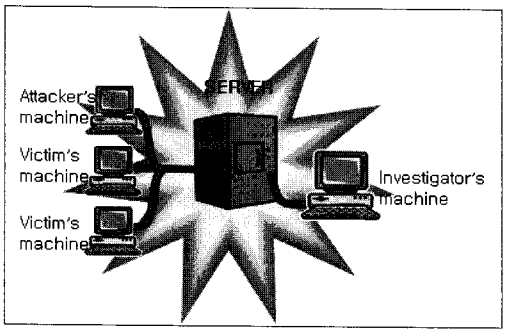
에이전트에서 타깃 컴퓨터로의 접근 권한을 획득하였다면 그 이후에 실행되는 모든 자동적인 조사 행위는 문서화된 규칙에 따라 시행되어야 하며 계속 리포팅(reporting) 되어야 한다.

2.3. 원격 포렌식 시스템의 기능 및 한계점

2.3.1. 기능

원격 포렌식 시스템의 기능은 다음과 같다.

첫째, 원격지에서 피해 시스템 혹은 침해 시스템에 대한 조사를 바탕으로 해당 시스템에서의 증거 탐색 및 확보가 가능하다. 이는 침해 사실이나 의심되는 행동이



〔그림 2〕 원격 포렌식 시스템의 구성요소

일어나면 즉각적으로 서버에 보고하는 원격 포렌식 시스템의 동작에 의하여 에이전트에 의한 타깃 컴퓨터의 실시간 감시가 가능한 것에 근거한다. 이러한 원격 시스템의 작동에 따라서 원격지 시스템에서 실시간으로 증거를 확보할 수 있다.

둘째, 활성 데이터의 즉각적인 수집에 유용하다. 이는 네트워크 및 시스템 침해 사고가 발생하였을 때, 사고지로의 이동 시간에 유실될 수 있는 휘발성 데이터를 일정 시간 간격으로 메모리를 덤프(dump)함으로써 가능하다. 따라서 메모리상에 존재하는 활성 데이터를 사고 발생과 거의 동시에 획득할 수 있다. 또한 일정 시간간격으로 덤프된 메모리 데이터를 분석함으로써 시간이 지남에 따라 시스템에서 어떠한 일이 일어났는지를 알 수 있다. 대표적인 원격 포렌식 시스템인 EnCase Enterprise Edition에서는 이러한 기능을 스냅샷(Snapshot)이라는 명칭으로 지원한다.

셋째, 키로깅(Keylogging) 기능을 할 수 있다. 원격으로 키로깅 프로그램을 설치하여, 의심되는 시스템에서 정보를 획득하는 것이 가능해진다. 키로거 뿐만 아니라 원격으로 원하는 프로그램을 설치하고 실행하여 원격지의 시스템으로부터 원하는 정보를 획득하는 것이 가능하다.

넷째, 공격자의 신원을 확인할 수 있다. 원격 포렌식 시스템을 이용하여 해당 시스템을 탐색하고, 공격자가 본인의 신원을 감추기 위한 프로그램 등을 탐색하면서 공격자의 신원을 확인하는 것이 가능하다[1].

다섯째, 다양한 종류의 하드웨어를 이용함으로써 특정 공간(Room)을 감시하는 것이 가능하다. 원격 포렌식 시스템을 사용하는 것이 일반화되면 감시가 필요한 특정 공간에서, 여러 가지 종류의 하드웨어에 원격 포렌식 소프트웨어를 설치함으로써 특정 공간에서의 효율적인 감시가 가능하다. 이는 컴퓨터뿐만 아니라 네트워크에 연결되어 있는 모든 디지털 기기에 원격 포렌식 시스템을 구축하는 기술이 연구·개발됨으로써 가능할 것이다.

여섯째, 네트워크에 연결된 다수의 디지털 기기들을 동시에 분석가능하다. 앞서 제시한 다섯 가지의 기능들을 네트워크에 연결된 모든 디지털 기기에 대해 동시에 적용할 수 있으며 이 모든 기능들이 자동화되어 있어 대형 네트워크로 이루어진 집단에 대한 실시간 감사와 사후 조사에 유용하다. 즉, 원격 포렌식 시스템은 원격지에 있는 특정 기기에 대한 조사를 지원할 뿐만 아니라 해당 네트워크에 연결되어 있는 모든 기기에 대한 증거 확보와 증거 분석, 리포팅을 동시에 함으로써 기업에서의 포렌식 시스템으로서의 최적의 기능을 가지고 있다.

2.3.2. 한계점

원격 포렌식 시스템은 다음과 같은 한계점을 가진다. 우선 모든 원격 포렌식 시스템의 구성 요소가 네트워크에 연결되어있어야 하기 때문에, 네트워크 연결이나 데이터 저장 공간에 대한 Dos 공격에 취약할 수밖에 없다. 즉 네트워크 통신에서의 트래픽을 증가시키거나 엄청난 양의 데이터를 서버에 전송함으로써 서버에 데이터 저장 공간이 남아있지 않도록 하는 공격이 이루어질 수 있다. 이러한 Dos 공격은 이미 조사가 진행되고 있는 다른 수사관의 컴퓨터의 원격 수사 행위도 느리게 만들거나 중단시킬 수 있다.

둘째, 수사관의 컴퓨터에 존재하는 원격 포렌식 소프트웨어(에이전트 프로그램)를 주기적으로 업데이트해야 하는 어려움이 있다. 해당 소프트웨어가 다수의 컴퓨터에 설치되어 있다면, 서버 측에서 모든 소프트웨어를 업데이트 하는 것은 네트워크에 과부하를 일으킬 것이며 이 때 진행되는 원격 수사에 차질이 생길 것이다. 즉, 추가적인 원격 포렌식 소프트웨어 설치나 업데이트가 자동적으로 업무에 지장을 주지 않는 상태로 이루어 질 수 있어야 한다. 이러한 에이전트 프로그램 업데이트에 관한 사항은 원격 포렌식 시스템 운영 정책상에 최적의 방법이 명시되어야 할 것이다.

이 외에도 피해 시스템에 설치되어 있는 방화벽과 같은 프로그램에 의하여 원격 접속이 불가한 경우가 있으며, 원격 포렌식 시스템에 의하여 피해 시스템에서 얼마

나 많은 데이터가 변경되는 지 알 수 있는 도구가 없다. 그리고 악의적인 사용자가 IP 주소를 바꾸거나 DNS 정보를 수정함으로써 원격 포렌식 시스템으로의 연결을 차단하는 경우, 원격 포렌식 시스템의 동작이 불가능하다[1].

Ⅲ. 원격 포렌식 시스템 구축 현황

3.1. 외국의 원격 포렌식 시스템 구축 현황

3.1.1. 독일

2007년 11월에 독일 정부는 국가 수사 기관에 원격 포렌식 소프트웨어 사용을 허가함으로써 피해 컴퓨터나 혹은 침해 컴퓨터에의 원격 포렌식 수사를 허가하였다[5]. 2007년 초에는 독일의 연방 법원이 불법적으로 은밀하게 이루어지는 수사 및 그 수사로부터 획득한 증거는 무효하다고 판결하고, 따라서 원격 포렌식 시스템의 사용을 주장하는 연방 검찰의 요청을 거절하였다[4]. 하지만 실질적으로 일어나는 여러 침해 사고들을 현재의 감시에 관한 법률로는 충분한 조사를 하기가 어렵다고 판단하여 원격 포렌식 시스템의 개발 및 사용을 허가하였다.

즉, 독일에서는 사고 대응 기술 및 원격 포렌식 도구가 구비되어있으며 최근에 원격 포렌식 시스템을 광범위하게 사용하는 데에 관한 법률적인 배경이 마련되고 있는 중이다.

3.1.2. 미국

미국에서는 이미 2001년에 FBI가 일부 시스템에 키로거(Keylogger)를 원격으로 설치해두고 이를 이용하여 정보를 획득해 온 사실이 드러난 바 있다. 또한 2007년에 FBI가 공격자의 신원과 공격자가 본인의 신원을 숨기기 위해 사용한 소프트웨어를 밝히기 위하여 CIPAV(Computer and Internet Protocol Address Verifier)라는 원격 포렌식 소프트웨어에 대한 사용 허가를 연방 법원에 요청한 바 있다[4].

또한 2006년 12월에 시행된 E-discovery로 인해 미국의 기업과 로펌(Law firm)들은 디지털 포렌식 전문가를 채용하여 적극적으로 활용하고 있으며 이들은 법정 분쟁이 발생했을 때, 원격 포렌식 도구를 사용하여 증거를 수집하고 분석하고 있다.

미국에서는 원격 포렌식 도구의 개발이 활발하며 또한 사고 대응 기술 및 절차가 정립되어 있다. 게다가 원격 포렌식 시스템을 사용하는 것에 관한 법률적인 배경까지 구축되어 있는 상황이다.

이러한 외국의 원격 포렌식 소프트웨어는 현재 수사상 겪는 어려움으로 인하여 그 사용이 합법화되고 있으며 원격 포렌식으로 획득할 수 있는 증거의 양이 늘어날 것으로 판단하고 있다. 반면, 미국과 독일의 보안 업체에서 정부 차원에서 실시되는 원격 포렌식 시스템에 의한 개인 PC로의 접근을 차단해야 하는가에 대한 논쟁이 일어나고 있으며, 원격 포렌식 시스템이 합법적으로 실행되는 트로이 목마라는 비난도 존재한다. 기업의 정보보안 정책에 의한 원격 포렌식 시스템의 필요성은 설득력을 가지고 법정 대응에의 이익이 드러나고 있으나 국가적인 원격 포렌식 시스템의 구축과 활용에 대해서는 기업 혹은 개인에 대한 국가의 감시가 합법화되는 것이 아니냐는 비판적 인식이 대부분이다.

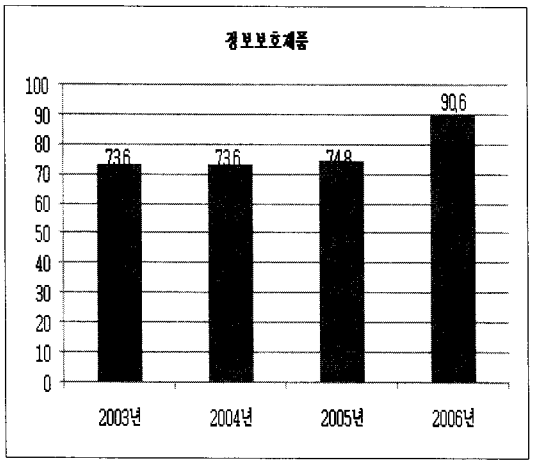
따라서 한국에 원격 포렌식 시스템을 구축할 때는 범국가적으로 기업을 상대로 강제로 시행해서는 안 되며, 원격 포렌식 시스템은 기업의 정보보호에 관한 하나의 대안으로서 자율적으로 기업이나 개인이 선택하여 사용할 수 있도록 해야 할 것이다. 또한 원격 포렌식 시스템의 장점이 외국에서 드러나고 있는 만큼 해당 시스템을 구축하여 기업 내의 정보를 보호할 수 있도록 권장해야 할 것이다.

3.2. 한국의 원격 포렌식 시스템 구축 현황

한국정보사회진흥원의 2006년 조사 결과에 따르면, 국내 기업의 정보보호(보안) 제품 이용률은 90.6% 이고 방화벽, 침입 탐지·차단 및 방지 제품 이용업체 비율이 2003년부터 전반적으로 증가한 것으로 드러났다.[1] 이러한 국내 기업의 정보보호(보안) 제품 설치 및 활용률의 증가는 최근의 정보보호 중요성에 대한 인식 제고 및 기업의 정보 유출로 인한 기업 내·외부적 손실에 대한 인식 등과 같은 인식의 변화에 의한 것이라 할 수 있다[6].

하지만 일반 정보보호(보안) 제품은 법정 분쟁에 대비한 통합적인 기능을 제공하지 못한다. 즉, 일반 정보

1) 출처 : 한국정보사회진흥원(2006년 정보화 통계조사)



〔그림 3〕 정보보호(보안)제품 이용 현황

보호(보안) 제품은 사고에 대응한 절차를 간략하게 로그로서 기록하지만 이러한 기록이 차후에 있을 수 있는 법정 분쟁에 대비하여, 사고 대응 절차에서 획득한 데이터를 증거로서 제출할 수 있는 요건을 만족하지 못하는 경우가 많다. 반면, 원격 포렌식 시스템은 사고 대응뿐 아니라 디지털 데이터를 '법적인 관점'에서 증거로서 수집하고 분석하는 통합된 기능을 제공하고 있기 때문에 원격 포렌식 시스템을 사용하는 것과 일반 정보보호(보안) 제품을 사용하는 것은 다르다.

현재 한국에서는 원격 포렌식 시스템의 구축이 거의 전무한 상태이다. 단지 몇몇의 기업에서만 EEE, PDIR과 같은 원격 포렌식 도구를 구입하여 네트워크를 이용한 중앙 시스템에서의 즉각적인 대응을 지원하고 있을 뿐이다. 실제로 EEE를 판매하고 있는 Guidance Sofrware 사(社)에 따르면 한국의 기업 중 EEE를 활용하고 있는 기업은 단 두 곳밖에 없다. Fortune 500의 기업 중 100개 이상의 기업이 원격 포렌식 도구를 활용하고 있는 것에 비하여 매우 낮은 수준이다[7]. 이것은 원격 디지털 포렌식의 중요성 및 효용과는 별개로 기업의 정보보안을 위한 새로운 대안인 원격 포렌식 시스템에 대한 인식이 낮기 때문이다. 이러한 인식에 따라 원격 포렌식 시스템 구축도 거의 없기 때문에 각종 네트워크·시스템에 대한 침해 사건을 실시간으로 분석하기도 어려울 뿐 아니라 비인가 접속 및 비정상 행위를 감시하는 것도 어렵다.

또한 기업에서의 디지털 포렌식의 필요성에 인식하고 디지털 포렌식에 관해 제도나 기술을 축적하고 있는 기업도 존재하지만, 주로 기존의 디지털 포렌식에 대한 정책이나 수사 절차, 혹은 디지털 포렌식 도구를 사용하는 방법이나 몇몇 기술을 교육하는 형식으로 이루어진다. 하지만 기존의 디지털 포렌식 도구나 기술이 대부분 개인용 컴퓨터의 조사에 적합한 것임을 고려할 때, 침해사고의 위험이 항상 존재하는 기업의 대형 전산망에 대한 디지털 포렌식 도구 및 기술은 기존의 디지털 포렌식 도구나 기술과 구별되어야 한다는 것을 인식해야 한다. 실제로 한국에서 대형 전산망의 안전성 향상의 요구가 높아지면서, 대형 전산망용 디지털 포렌식 도구 즉, 원격 포렌식 시스템의 사용에 대한 필요성이 높아지고 있다.

[표 1]에서는 독일 및 미국, 그리고 한국에서의 원격 포렌식 시스템 구축에 관한 현황을 나타낸다. '법률적 배경', '사고 대응 기술 및 절차' 그리고 '원격 포렌식 도구 개발 기술'은 그림 1에서 나타낸 원격 포렌식 시스템을 정의하기 위한 요소들이다.

〔표 1〕 국가별 원격포렌식 시스템 구축 정도

필요사항 / 국가	법률적 배경	사고 대응 기술 및 절차	원격 포렌식 도구 개발 기술
독일	△	O	O
미국	O	O	O
한국	X	O	△

O : 잘 구축되어 있음
△ : 구축되는 중
X : 구축되어 있지 않음

Ⅳ. 원격 포렌식 시스템 구축에 필요한 사항

한국에서 원격 포렌식 시스템을 기업 차원에서 구축하기 위해서는 몇몇 충분조건이 필요하다. 즉, 현재의 기업의 컴퓨터 포렌식에 관한 인식이나 기술, 제도로는 이러한 시스템의 구축이 어렵다. 이 장에서는 기업에서 원격 포렌식 시스템을 구축하기 위해서 필요한 제도 및 절차에 관하여 대해 다룬다.

4.1. 디지털 증거 처리에 관한 관련 법안 제정

한국에는 아직 디지털 증거를 다루는 사항에 대한 법안이 마련되어있지 않다. 이러한 상황에서는 디지털 포렌식 기술을 이용하여 수집한 증거 데이터가 법정에서 신뢰를 얻어 증거로서의 효력을 충분히 발휘할 수 없다.

원격 포렌식 시스템을 이용하여 획득한 증거 데이터는 원격지에서 이루어지는 수사인 만큼 이 시스템을 검증하고, 이 시스템에 의하여 얻어진 데이터를 증거로서 인정할 것인지 아닌지에 대한 디지털 증거 처리에 관한 법안의 제정이 필요하다.

4.2. 디지털 포렌식 산업과 기술의 발전

한국에서 사용하고 있는 원격 포렌식 시스템은 미국이나 독일의 제품인 경우가 많다. 이러한 도구들을 이용하여 획득한 증거는 그 신뢰성 및 타당성을 국제적으로 인정받고 있기는 하지만, 도구의 응용 분야를 비롯한 여러 면이 우리나라의 실정과는 약간 맞지 않는다는 견해가 있다. 그러므로 국가 차원 혹은 민간 차원에서 디지털 포렌식 기술을 연구하는 산업이 발전하여 국내 실정에 맞는 원격 포렌식 시스템을 구축할 수 있어야 한다.

4.3. 디지털 포렌식 기술 필요성에 대한 인식 확산

기업에서는 정보보호를 위해 쓰이는 예산이 상대적으로 적은 편이다. 현재는 나아진 편이지만 2005년 정보통신부에서 발표한 '기업 정보보호 실태조사'에 따르면 1206년의 기업 중 40%는 정보보호를 위해 예산을 편성하지 않았고, 정보보호를 위해 예산을 편성한 기업 중에서도 39%는 전체 예산의 1%만을 정보보호를 위해 사용하였다. 비록 2005년의 조사 결과이지만 현재에도 형식적으로 정보보안 제품을 사용할 뿐이지 정보보호를 위해 많은 예산을 투입하지는 않는다. 이는 해당 기업의 정보보호에 대한 기업의 안일한 의식을 반영한 것이다. 기업의 정보를 보호하기 위해 가장 우선되어야 할 것은 정보의 중요성과 가치를 인식하고, 그 것을 보호하기 위한 디지털 포렌식 기술의 필요성을 인식하는 것이다.

디지털 포렌식의 방향에 대해 세계 각국의 벤치마킹 대상이 되고 있는 미국의 경우 국가적 차원에서의 디지털 포렌식의 기술 및 필요성에 관한 교육뿐 아니라, 민간 차원에서의 교육도 활성화되어있다. 미국의 국토 안보부와 앨라바마 주가 지원하는 국가 컴퓨터 포렌식 센터와 플로리다 올랜도의 NCFS(National Center for Forensics Science)와 같은 교육기관이 있다[7]. 또한 디지털 증거를 수집하고 분석하는 것이 공권력의 수사상에서 뿐만 아니라 일반 민간 기업들에게도 그 필요성이 인식되면서 민간 차원에서의 디지털 포렌식에 대한 교육도 활발히 이루어지고 있다.

한국에서는 디지털 포렌식의 개념의 사회적으로 널리 알려지지도 않았으며 따라서 디지털 포렌식 기술의 필요성에 대한 인식도 낮다. 그러므로 디지털 포렌식의 개념과 기술 연구에 대한 필요성 등을 인식시키기 위한 교육이 국가적 차원 및 민간 차원에서 활성화되어야 한다.

V. 원격 포렌식 시스템 구축의 기대효과

세계적으로 원격 포렌식 도구의 사용에 관한 필요성이 부각되고 있으며 특정 국가에서는 국가적 차원에서 원격 포렌식 도구의 사용이 장려되고 있기도 하다. 대형 네트워크를 사용하고 있는 기업과 같은 집단에서 내·외부 네트워크 및 시스템 침해사고를 예방하거나 대응하고 또한 네트워크의 안전성을 향상시키기 위해서는 원격 포렌식 도구의 보편화가 필요하다. 원격 포렌식 시스템을 구축함으로써 얻게 되는 기대효과는 다음과 같다.

5.1. 기업 정보 유출 방지 가능

한국 산업보안 연구소의 발표에 따르면 지난 4년간 기업의 첨단 기술의 유출에 따른 손실은 95조 9,000억 원에 달한다[7]. 또한 첨단 기술의 유출뿐 아니라 고객의 개인 정보가 유출되어 약 400억 원을 배상한 일본의 '소프트 뱅크', 100만 고객의 개인 정보가 외부로 유출되어 재산적 피해를 입은 '리니지2'의 '엔시 소프트'의 경우를 보더라도 기업의 정보 유출은 사회적, 경제적으로 매우 많은 손실을 야기하고 있다.

원격 포렌식 시스템은 내·외부로부터의 네트워크 침해 사고로 인한 기업의 정보 유출을 사전에 예방할 수 있으며 사후 증거 확보에 유용하다. 이는 자동화된 침입 탐지 시스템 및 침입 차단 및 방지 시스템에 의하여 네트워크 내의 비정상 트래픽 등을 관찰함으로써 침해 사고를 예방할 수 있을 뿐 아니라, 침해 사고가 일어난 경우에도 실시간으로 해당 트래픽을 관찰하고 증거를 확보해 둠으로써 피해를 최소화할 수 있다.

따라서 원격 포렌식 시스템은 내부자 혹은 외부자의 네트워크 침해 및 데이터 자원 유출을 방지하는데 효과적이다.

5.2. 법적으로 유효한 증거를 신속하게 수집 가능

원격 포렌식 시스템은 사고가 일어났을 때 대형 네트워크에 연결된 기기들로부터 '증거'를 확보하고 분석하기 위해 제작된 도구이므로, 증거를 수집하고 분석함에 있어서 디지털 포렌식의 기본 원칙을 준수하고 있다. 즉, 신속성의 원칙, 연계 보관성(Chain of Custody)의 원칙, 무결성의 원칙, 그리고 정당성의 원칙 등을 지키고 있다.

우선 증거 수집의 과정이 신속하고 실시간으로 진행되고 있으므로 '신속성의 원칙'을 지키고 있다. 또한 증거를 수집하는 모든 과정을 자동적인 리포팅 기능으로 문서화해 둠으로써 '연계 보관성의 원칙'을 지키고 있다. 그리고 수집하는 증거에 해쉬 값을 부여하여 해쉬 셋을 구축하는 등의 증거의 무결성을 보장하기 위한 기능을 함으로써 차후에 해당 증거의 위·변조 여부를 판단할 수 있게 하는 것이 '무결성의 원칙'을 지키는 것이라 할 수 있다. 게다가 증거의 획득 절차가 일반적인 디지털 포렌식에서의 검증받은 증거 수집 절차에 따라 자동화되어 있으므로 '정당성의 원칙'을 지키고 있다고 할 수 있다.

그러므로 원격 포렌식 시스템을 이용하여 신뢰성 있게 수집된 증거는 법원에서도 그 효력을 인정받을 수 있다.

5.3. 신속한 법적 소송의 대응책 마련

미국의 경우, E-discovery법에 따라 기업들은 자체적으로 디지털 증거를 축적하여 차후에 있을 수 있는 법정 분쟁에 대하여 신속한 대응을 대비하고 있다. 기업이 원격 디지털 포렌식 시스템을 활용하면 해당 사건의 진위 여부를 수월하게 밝힐 수 있다.

한국의 형사·민사 소송법은 아직은 디지털 증거물에 관한 규정이 없는 실정이다. 문서화된 법령이 존재하지 않는 까닭에 한국에서의 디지털 증거에 관련된 사건은 판례법을 따르거나 법관의 주관적인 판단에 의존하여 결론이 난 경우가 대부분이다. 구체적으로는, 원고 측은 피고 측이 실제로 가진 증거 데이터의 종류를 알 방법이 없으며 소시 사실 부인 시 효과적인 제재수단도 마련되어 있지 않다. 즉, 디지털 데이터의 증거로서의 효력이 작았다. 하지만 한국도 Discovery법과 E-discovery법의 도입의 필요성이 대두되고 있고, 그 시행을 앞두고 있다. 따라서 이러한 법에 따라 기업들은 디지털 증거 및 기록을 축적해둔다면 상시적으로 디지털 증거를 확보해두는 것이며, 차후에 법정 대립이 생기더라도 해당 기업의 무죄를 입증하는 데 유용할 것이다.

또한 최근에 기업이 보유한 정보를 안전하게 관리하는 것에 대한 법안들이 통과되고 있는데, 2007년 2월 실시된 전자금융거래법과 2007년 11월 실시된 개인정보보호법이 그 대표적인 현안이다[7]. 기업의 정보보호에 관한 사항이 법제화 되고 있으므로 기업들은 기업정보를 철저히 관리하기 위해서 노력해야 하며, 이는 많은 연구와 예산이 필요한 일이다. 원격 포렌식 시스템을 사용하는 것은 그러한 수고를 덜어준다.

Ⅵ. 결 론

지난 2005년 미국 월가의 금융투자회사 모건스탠리가 레블론사에 약 6억 달러를 배상했다. 결정적인 패소 원인은 법원의 증거개시요청 즉, Discovery법에 응하지 못했기 때문이었다. 법원은 모건스탠리에게 자문 내용이 담긴 이메일을 제출하도록 요구했으나 모건스탠리는 해당 이메일을 보유하고 있지 못했다. 미국과 사업으로 연결된 기업에게 Discovery법, E-discovery법은 매우 중요한 사항이다. Discovery법은 법률상 소송에 처하게 된 당사자 모두가 소송과 관련하여 어떤 증거물들을 소유하고 있는지를 공개해야한다는 법이다. 이는 재판상 시간의 절약과 재판에의 공정성을 가하기 위함이다. 이러한 Discovery법을 전자적 증거에 적용한 것이 E-discovery법이다. 이러한 E-discovery법 즉, 전자 증거 개시법이 한국에서 발효되면 미국과 관련되어 있지 않은 모든 한국의 기업도 디지털 증거 데이터를 상시에 확보해둘 필요가 생긴다. 그리고 그러한 증거 데이터를 디지털 포렌식의 관점에서 확보하고 신뢰성 있게 분석하기 위해서는 원격 디지털 포렌식 시스템의 구축이 필수적이다.

기업에서 원격 디지털 포렌식 시스템을 구축해야 하는 이유는 다음과 같다. 우선 기업 정보 유출의 심각성이 증가되고 있으며 E-discovery의 시행이 사실화 되고 있기 때문이다. 기업에서 일어나는 기업 정보 유출사고는 대부분 내부자의 실수나 혹은 악의적인 내부자에 의해 일어나며, 이는 기업의 내부자에 대한 감사의 필요성을 나타내는 것이다. 따라서 기업에서는 디지털 포렌식 시스템의 구축이 필수적이며 이는 원격 포렌식 시스템 구축의 필요성을 역설한다. 또한 E-discovery의 시행으로 기업들이 신뢰성 있는 디지털 증거의 수집과 분석을

이행하여야 하며 이 과정에서 원격 포렌식 시스템을 사용함으로써 그 비용과 절차에 대한 수고를 경감할 수 있다.

기업의 보안 담당자들은 기존의 범죄 수사를 위한 디지털 포렌식 기술, 기업이 보유해야 할 디지털 포렌식 기술 및 제도에 대한 지식을 습득하는 한편, 기업의 정보보안수준을 향상시킬 수 있는 디지털 포렌식을 효율적으로 활용할 수 있는 방안인 원격 포렌식 시스템 구축에 관한 필요성을 인식하고 이를 적극 활용하여야 할 것이다. 또한 이러한 원격 포렌식 시스템 구축이 사후 조치가 아닌 사전 예방적인 활동이 되어야 하며 이는 비용 및 여러 정책에 대응하기 위한 필수적인 작업이라는 사실을 인식하는 것이다.

참고문헌

[1] Jacob Pennock, Damon Smith, and Geoffrey Wilson, "Design and Implementation of a Remote Forensic System", Foundstone, www.foundstone.com

[2] Eoghan Casey, Aaron Stanley, "Tool Review - remote forensic preservation and examination tools", Digital Investigation(2004) 1, 284-297

[3] Encase Enterprise Edition, http://www.guidancesoftware.com/products/ee_index.aspx

[4] Dr.Marco Gercke, "REMOTE FORENSIC SOFTWARE", Lecturer at the University of Cologne Germany, Chaos Communication Camp, 10th August 2007.

[5] John Leyden, "Germany seeks malware 'specialist' to bug terrorists", The Register, http://www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/, 21th November 2007

[6] 송혜인, 백기연, 지상호, 유진호, "개인 및 민간기업 정보보호 트랜드 분석", 한국정보보호진흥원, 2007.03

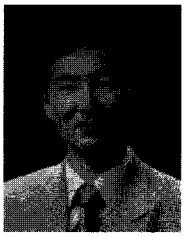
[7] 임종인, 박신화, 박춘화, 유희석, 정재성, "온라인 세상의 질서 수립을 통한 신뢰의 구축, Digital Forensics", LG Global Challenger 2007.

[8] Computer Associates™, "eTrust Network Forensics 및 eTrust Network Forensics Mobile Edition Fact Sheet",

〈著者紹介〉

박 보 라 (Bora Park)
2007년 2월 : 부산대학교 수학교육과 학사
2007년 3월~ : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 디지털 포렌식

심 미 나 (Mina Shim)
1999년 2월 : 성신여자대학교 전산학과 이학사.
2004년 2월 : 고려대학교 정보보호대학원 공학석사
1995년 12월~2000년 2월 : (주) 삼보 컴퓨터 시스템 엔지니어
2000년 3월~2001년 8월 : (주) 한국썬교육센터 썬시스템 강사
2002년 6월~2004년 3월 : (주) 인젠 보안컨설턴트
2002년 3월~현재 : 고려대학교 정보경영공학전문대학원 정보보호정책연구실 연구원
<관심분야> 개인정보보호, 정보보호영향평가제도, 정보보호법률, 컴퓨터 포렌식



이 상 진 (Sangjin Lee)
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수,
2001년 9월~현재 : 고려대학교 정보경영공학전문대학원 교수
<관심분야> 대칭키 암호, 정보은닉 이론, 컴퓨터 포렌식