情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

국내 환경에 맞는 컴퓨터 포렌식에서의 초기 신고 시스템

이 하 영*, 김 현 상*, 최 운 호**, 이 상 진*, 임 종 인*

요 약

현재 국내에도 컴퓨터 포렌식의 중요성에 대한 인식이 확산됨에 따라 민·관·군의 여러 단체에서 포렌식 연구를 수행하고 있고, 침해사고 대응 센터와 같은 CERT 관련 단체들이 많아지고 있다. 하지만 현재 국내의 신고 시스템은 아직 1~1.5세대 정도로 분류된다. 또한 선진국들의 신고 시스템을 보면 어느 정도의 전문 지식이 없으면 신고서를 작성하기가 힘들게 되어있다. 본고에서는 선진국의 체계적인 신고 시스템을 바탕으로 일반인도 좀 더 쉽게 신고할 수 있는 신고 시스템의 체계를 설계, 구현한 시스템을 제안해 보고자 한다.

Ⅰ. 서 론

현재 국내의 인터넷 이용률을 살펴보면, 2001년 이후 세계 2~3위를 유지하고 있으며, 특히 초고속 인터넷 가입자 수는 2004년 1/4분기에 1150만 명에 육박하고 있다.[1] 이러한 세계 초일류 수준의 정보통신 인프라는 국가를 정보화 선진국으로 견인하는 주요 원동력이 되고 있다. 그러나 이러한 정보화의 순기능과 더불어 역기능 역시 늘어가고 있는 것이 사실이다. 특히, 컴퓨터 범죄는 매년 폭발적인 증가를 보이고 있으며, 경찰청 사이버 테러 대응센터의 통계자료[2]에 따르면, 2003년 한해만 약 5200여건의 컴퓨터 범죄가 발생하였다.

이러한 컴퓨터 범죄의 증가는 컴퓨터 범죄 수사의 과학적/체계적인 체질개선을 요구하게 되었고, 이를 이론적으로 뒷받침 하는 컴퓨터 포렌식이 사회적인 주목을 받게 되었다. 이러한 경향에 힘입어 컴퓨터 범죄를 담당하는 유관기관들이 속속 신설 및 확대 개편되어가고 있으며, 컴퓨터 포렌식 기술을 적극적으로 도입하려 하고 있다.

그러나 컴퓨터 포렌식 기술이 도입 초창기인 만큼, 아직 체계적이고 효율적인 사회 시스템 구축이 미비한 실정이다. 특히 컴퓨터 범죄의 시작점이며, 초동 수사에 핵심적인 역할을 담당하는 사고신고 체계는 공개 게시판에 글을 작성하는 수준에 머무르고 있다.

본 논문에서는 웹기반의 컴퓨터 범죄 신고 시스템이 갖추어져 있는 "대검찰청 인터넷 범죄수사센터"[3]와 "경찰청 사이버 테러 대응 센터"[4], "국가 사이버 안전센터"[5], 인터넷 침해사고 대응 지원 센터[6]의 사고신고 체계와 미국의 CERT[7]를 중심으로 한 신고체계를 비교 분석하여, 장·단점을 분석하고, 국내 환경에 적합한 신고 체계를 제안하고자 한다.

Ⅱ. 사고 대응팀의 개념

초기 신고의 내용이 중요한 이유는 신고를 받은 CERT팀이 그 내용 중심으로 사고여부를 판단하고 사고라 판단되었을 시에도 그 내용을 중심으로 사고의 종류, 초기 대응 절차 등을 결정해야 하기 때문이다.

신고자가 신고를 하면 CERT는 어떤 일들을 수행하는지 또한 평소에는 어떤 역할을 하는 지에 대해 알아보기 위해 CERT의 역할과 업무 절차에 대해서 알아보도록 하겠다.

본 연구는 대학 IT 연구센터 육성 지원 사업에 의해 수행 되었습니다.

* 고려대학교 정보보호 대학원(GSIS)/정보보호 기술 연구센터(CIST) ({newha, neoshine}@cist.korea.ac.kr, {sangjin, jilim}@korea.ac.kr)

** 금융결제원 금융 ISAC실 정보보호평가팀장 (tiger@kftc.or.kr)

1. 사고 대응팀의 역할

평상시에는 사고발생에 대비하여 다음과 같은 대응 준비를 한다.

- □ 조직원들의 교육
- □ 대응 전략을 위한 적절한 정책과 운영 과정 구비
- □ 사고 대응 조사, 분석, 보고 등의 문서양식 정형화
- □ 사고 조사 시 필요한 장비 구입

사고 접수 시에는 다음과 같은 일련의 업무를 진행한다.

- □ 사고에 맞는 적절한 팀의 구성
- □ 사고를 분석하여 조치
- □ 만약 법적인 절차로 갔을 때에는 디지털 증거를 법정에 제출할 수 있게 가공
- □ 사고 후에는 사고를 예방하고, 다시 유사한 사고가 발생하지 않도록 필요한 조치를 제공

2. 업무 절차

사고 대응팀의 역할과 목적을 좀 더 정확하게 알기 위해서 팀의 업무 절차에 대해 알아보도록 하겠다.

- □ 사고 전 준비 과정: 사고가 발생하기 전 CERT와 조직의 준비를 하기 위한 행동
- □ 사고 탐지: 가능성 있는 컴퓨터 보안 사고의 식별
- □ 초기 대응: 초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고대응 팀 소집, 사고에 대해 알기를 원하는 부서에게 통지
- □ 대응 전략 체계화: 알려진 사실의 결과에 기반을 둔, 최적의 전략을 결정하고, 관리자의 승인을 얻는다. 조사 결과를 참고하여 민사, 형사, 행정, 또는 그 밖의 소송이 적당한 지를 결정한다.
- □ 사고 조사: 데이터 수집을 통하여 수행한다. 어떤 사건이 언제, 누가, 어떻게 일어났는지, 다음번에 어떻게 방지할 것인지를 결정하기 위해 모인 데이터를 재검토한다.
- □ 보고서 작성: 의사 결정자에게 유용한 형태로 사고에 대한 정확한 보고서를 작성한다.
- □ 해결: 문제들을 식별하기 위한 보안 측정, 절차 변경, 과거 사건의 기록, 장기 보안 정책, 기술 수정 계획수립 등을 이끌어 낸다.

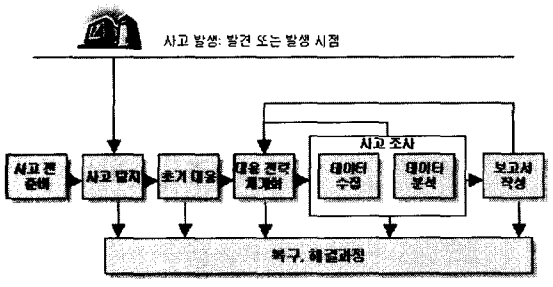


그림 1. 사고 대응 절차

Ⅲ. 사고 발생 시 신고대상

일반적으로 컴퓨터 보안 사고란 컴퓨터 시스템 혹은 네트워크 상에서 불법적 행위나, 허가받지 않은 행위로, 수용할 수 없는 활동을 말한다. 이러한 행동의 예는 다음과 같다.

- □ 사업 비밀의 탈취
- □ 전자 메일 스팸 (또는 harassment)
- □ 컴퓨터 시스템에 인가되지 않은 불법침입
- □ 도용(embezzlement)
- □ 아동 음란물의 소유 및 배포
- □ 서비스 거부 공격(Denial of Service)
- □ 업무 방해
- □ 도청(Extortion)
- □ 악성코드

위와 같은 행위들로 인한 사고들이 신고대상이 된다.

Ⅳ. 초기 신고의 필수 요소

이 절에서는 적절한 사고대응을 위해서 필수적인 신고 내용에는 어떤 것들이 있는지 알아보도록 하겠다. 우선 신고자 또는 조직의 신상에 관한 일반적인 정보와 피해정도와 같은 특정한 사항들을 위한 설문이 있어야 하겠다.

아래 표는 기본적으로 있어야 할 사항들을 서술해 놓은 것이다. 아래 내용의 세부 사항들은 바뀔 수 있겠지만, 기본적으로 들어가야만 원활한 초기수사가 이루어질 것이다.

표 1은 필요한 많은 정보들을 최소한으로 요약해 놓은 정보이다.

일반적으로 사고대응 조직은 초기 대응 점검표를 작성할 것이고, 신고 시스템의 설문 작성은 그에 맞는 적절한 정보들로 만들어야 한다. 또한 신고자의 주관

표 1. 초기 신고 필수 요소

일반적인 정보	사고가 탐지된 날짜 혹은 사고가 시작된 날짜 작성자의 연락 정보 사고 발견자의 연락 정보 사고 발생 기관 및 부서 정보
사고에 관한 특정 정보	사고의 타입 및 사고에 관한 기타 정보 조직 내부에서 파악된 사고의 개요 탐지 경로 피해 호스트의 중요도와 피해 수 피해 시스템에 관한 정보(OS, S/W, 용도 등)

이 개입될 여지가 있거나, 너무 많은 정보나 복잡한 정보를 요구하여 제 기능을 못하는 경우를 방지할 수 있는 설문들을 작성해야 할 것이다.

V. 현재 국내의 신고 체계 고찰

현재 국내에서는 컴퓨터 포렌식 분야의 관심이 오래되지 않아 체계화된 신고체계가 아직은 미비하다. 그래서 어떤 점이 부족한지를 알기 위해 현재 국내 신고체계 시스템을 살펴보도록 하겠다.

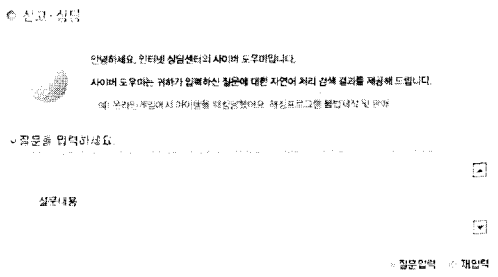


그림 2. 경찰청 사이버 테러 대응 센터

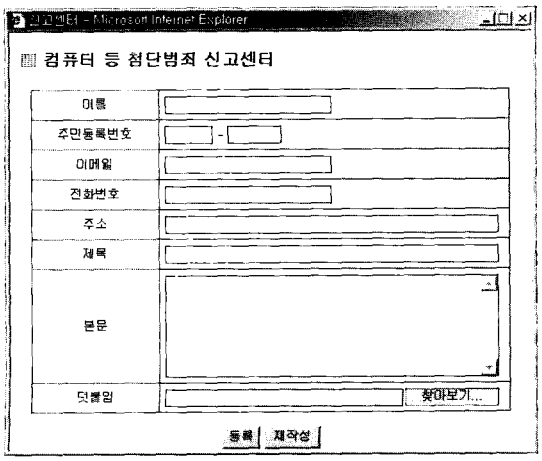


그림 3. 대검찰청 인터넷 범죄 수사 센터

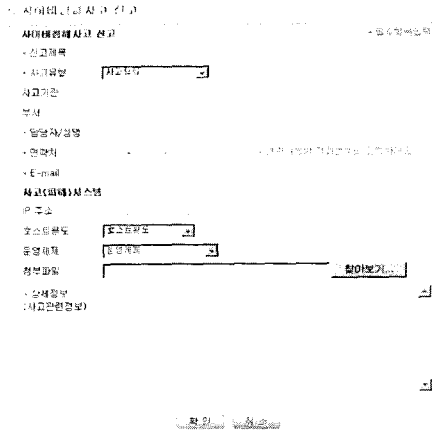


그림 4. 국가사이버안전센터

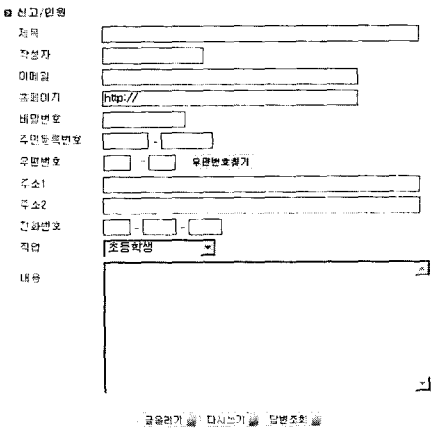


그림 5. 국군기무사령부

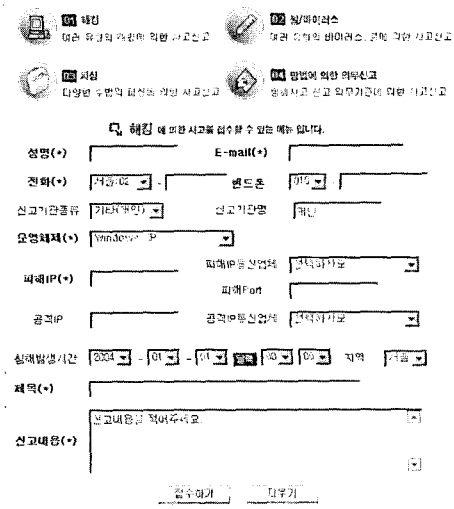


그림 6. 인터넷 침해사고 지원 대응 센터

위의 여러 기관들의 사고신고 체계를 살펴보면 대동소이 하며 위 그림들에서 알 수 있듯이 대부분 표 1의 일반적인 정보만을 기록하게 하고 있고, 실제 사고 조사에 필요한 사고에 관한 내용들은 사용자가 직접 입력하는 방식을 채택하고 있어 주관적인 견해에 의존할 수밖에 없으며, 전문가가 아니면 작성의 어려움이 있을 것으로 판단된다.

이와 같은 문제점들을 정리해 보면 다음과 같다.

신고자(기관)가 사고에 대한 지식이 전혀 없을 수 있음에도 불구하고, 사고에 대한 설명도 없고 사고의 내용을 수작업에 의지하고 있다.

사고에 대한 지식이 있는 사람이 있다하더라도 정확한 현상 파악은 힘들기 때문에 신고 내용에 오류가 있을 수 있다.

신고를 받은 대응 팀에서 실질적으로 초기대응을 하기 위한 어떠한 정보도 얻을 수 없다.

신고자(기관)에 대한 보안 정책이 포함되어 있지 않기 때문에 전송받은 정보를 신뢰할 수 없다.

사고 신고를 받으면 신고된 내용을 가지고 대략적인 초기 대응 전략을 구축할 수 있다면 굉장히 효율적일 것이다. 하지만 현재의 이 정보들을 가지고서는 실제 "누가, 어디에서 사고가 발생했다"라는 정보이외에는 얻을 수 있는 사전 지식이 없기 때문에, 신고 시스템으로서는 부적합하다 하겠다.

다음 절에서는 국내보다 먼저 시작한 미국 CERT 팀의 경우를 살펴보면서 어떤 식으로 처리하고 있는지 개략적으로 살펴보도록 하겠다.

Ⅵ. 해외의 신고시스템 고찰 및 국내 시스템과의 비교

해외의 신고시스템은 주로 호주, 미국, 네덜란드 등을 중심으로 조사했다. 미국의 워터 ISAC의 경우는 (이름, 전화번호, 이메일, 사고 내용)정도의 설문만을 받고 있었으며, 조사한 시스템 중에 가장 자세한 설문을 받고 있었던 곳은 호주의 CERT[3]와 미국의 CERT[4] 두 곳이 있었으며, 내용면에 있어서는 대동소이하였기 때문에 좀 더 자세한, 미국 CERT팀의 시스템을 집중적으로 분석하였다. 웹 페이지의 순서대로 분석해 보기로 한다.

초기 화면에는 사고에 대한 정의와 범위를 명확히 함으로써 신고대상의 범위를 확실히 하고, 전문가가 아닌 신고자들도 사고의 개념과 범위를 명확히 알 수 있고, 사고신고 시스템의 사용법을 간략히 설명하고 보안 정책으로 SSL을 사용했음을 알 수 있다.

초기 화면에서 동의를 선택하면 접속 정보를 입력하는 단계로 넘어간다. 이 단계에서는 신고자의 신상과 조직의 정보를 입력을 받는다. 신고자 조직의 국적, 조직의 성격, 신고자의 직위까지를 입력함으로써, 개별적인 대응을 도모하고 조직의 종류에 따라 그 다음 단계의 내용이 바뀜을 알 수 있으나, 본고에서는 공통되는 내용만을 다루기로 하겠다.

다음은 인프라 정보를 입력하는 부분이며, 침입자의 시도된 활동들과 완료된 활동들을 입력하게 되어 있고, 그 내용은 다음과 같다.

- □ 정보 노출
- □ IT 자원의 도난
- □ 다른 자산들의 도난
- □ 정보의 변조/파괴
- □ 피해 조직의 대외 이미지
- □ 공격자의 명성 증가
- □ 기타

일반 사고 정보 입력부분에서는, 사고를 탐지한 경로와 공격기술에 대한 정보를 요구한다. 아래와 같은 사고를 탐지한 경로를 얻음으로써 사고대응 시 증거 수집의 범위를 한정시킬 수 있다.

- □ 방화벽, 침입탐지 시스템과 같은 자동화된 소프트웨어
- □ 자동화된 로그 분석
- □ 수동 로그 파일 분석
- □ 시스템 이상 징후(crashes, slowness)
- □ 제 3기관에서의 통지
- □ 모름
- □ 기타

아래와 같은 공격기술에 대한 정보들을 얻음으로써, 사고 대응하기 전 대책을 수립할 수 있게 하였다.

- □ 바이러스, 트로이 목마, 웜, 기타 악성코드
- □ DOS계열
- □ 침해당한 컴퓨터에 대한 비인가 접속, 관리자권한 계정 침해, 웹 침해
- □ 스캐닝
- □ 기타

알려진 취약성 정보 입력단계에서는 공격기술 뿐만

아니라 기술에 대해 사용된 툴등의 정보를 얻음으로써 사고 대응의 목적과 범위를 한정할 수 있게 했다. 네트웍 정보를 입력하는 단계이며 내용은 다음과 같다.

[ ] 침입에 사용된 프로토콜(UDP, UCP, ICMP, IPSEC 등)
[ ] 소스 포트, 목적지 포트

공격의 피해 정도를 입력하는 단계에서는 침해의 범위 파악을 위해 다음과 같은 정보를 요구한다.

[ ] 침해당한 호스트 수
[ ] 침해당한 고객 수
[ ] 공격 시간
[ ] 탐지 시간
[ ] 현재 공격여부
[ ] 공격 지속 시간
[ ] 예상 복구 기간
[ ] 예상 피해 액수

호스트 정보를 입력하는 단계에서는 3가지의 선택이 나오는데 "계별 호스트 정보 입력"을 선택한 것으로 진행하도록 하겠다. 계별 호스트 정보를 입력하는 단계로써 다음과 같은 내용들을 요구한다.

[ ] 피해 상황: 에이전트로 사용, 최종 공격지
[ ] 호스트 이름
[ ] IP 주소
[ ] 신고자의 해당 호스트에 대한 권한정도
[ ] 운영체제
[ ] OS의 패치 정도
[ ] 해당 호스트의 주요 용도: 데스크 탑, 노트북, 웹 서버, 메일 서버, 도메인 서버
□ 실제 피해: 없다, 파괴, 업무 방해
□ 예상되는 피해: 없다, 파괴, 업무 방해

이상에서 볼 수 있듯이 미국의 경우에는 국내와는 다르게 상당히 자세한 정보들을 요구하고 있다. 하지만 이 시스템에도 문제가 없는 것은 아닌데, 문제점들을 살펴보면 다음과 같다.

□ 요구하는 정보들이 너무 전문적이어서 상당한 수준의 지식을 요한다.
□ 요구하는 정보들이 자세하기는 하나, 신고자의 주관이거나 잘못된 정보들이 개입될 여지가 다분히 있다.
□ 그럼으로, 이 정보들을 신뢰할 수 없고, 실질적인 사고 대응당시에 새로 조사해야 할 여지가 많다.

마지막으로 다음 표 2에서 해외의 시스템과 국내의 시스템을 비교해 보도록 하겠다.

Ⅶ. 새로운 신고 시스템 모델 제안

위에서 살펴본 국내와 미국의 신고 시스템의 실례를 발판으로 좀 더 발전된 신고 시스템을 제안하도록 하겠다.

신고 체계는 전문적인 지식이 없는 사람도 작성할 수 있도록 간단해야 한다.

신고 받은 자가 오해할 소지가 없이 명확한 설문을 유도해야 한다.

사고대응은 급박한 경우가 많기 때문에, 대응을 효과적으로 할 수 있도록 하는 정보들이 포함되어야 한다.

사고 대응을 하기 전 최소한의 상황판단을 할 수 있는 객관적인 정보들을 포함하고 있어야 한다.

표 2. 국내 시스템과의 비교

구분	해외		국내				
	미국[7]	호주[9]	경찰청	대검찰청	국가사이버 안전센터	국군 기무사령부	인터넷 침해사고 지원 대응 센터
사고, 초기신고에 관한 설명	O	O	O	O	O(FAQ)	X	X
보안정책	O	O	X	X	X	X	X
초기 신고 필수요소	O	O	X	X	O(다수 포함)	X	O(다수 포함)
입력 정보의 객관성	X	X	X	X	X	X	X

위의 대안들로 국내의 현실에 맞는 다음과 같은 신고 체계를 제시해 보도록 하겠다.

이와 같은 간단하고 명료한 설문을 받은 후 사용자가 동의한다면, 출동하거나 상담하기 전 사고의 정황을 파악하기 위한 에이전트를 사고 시스템에 설치하고 정보를 수집한다. 수집하는 기본 정보는 시스템 명령어를 기본으로 하며, 필요에 따라 그 외 툴도 포함시킬 수 있다.

표 3. 신고 시스템 정보

일반정보	
신고기관, 부서, 담당자, 연락처, 메일	원활한 대응을 위한 가장 기초적인 정보
원하는 대응 방법	출동, 전화 상담, 이메일 상담을 선택함으로써 신고자의 의사를 확인함
피해상황	
공격탐지 시간	
탐지경로	IDS, firewall, 시스템 이상 징후 , 로그 분석, 제 3기관 통보 등을 선택하게 함으로써 출동 후 우선 조사 순위를 결정할 수 있다.
예상되는 사고 내용	웜, 스캐닝, 백도어, 트로이 목마등의 선택으로 대강의 대응 방법을 정한다.
피해 호스트 수, 용도	이 정보들을 가지고 사고의 심각도를 유추할 수 있다.
현재 공격 진행 여부	상동

표 4. 윈도우 정보

IP 정보	ipconfig /all
시스템 버전	ver
시스템 날짜	date /t
시스템 시간	time /t
사용자 정보	net user
서비스 정보	net share
포트 정보	netstat -na
로컬 그룹 정보	net localgroup
키 정보	doskey /history
메모리 정보	mem
세션 정보	net sess
ARP 정보	arp -a
로컬 서비스 정보	net share
캐쉬 정보	nbtstat -c
routing 정보	route print

표 5. 리눅스 정보

IP정보	ifconfig -a
시스템의 실행시간	uptime
시스템 정보	unname -a
파일시스템 사용 정보	df -k
환경 변수	env
프로세스 정보	psv -aux
네트워크 상태 정보	netstat -anp
라우팅 정보	netstat -nr
ARP 테이블 정보	arp
로그인 사용자 정보	w
WTMP 로그정보	last

이와 같이 피해 시스템에서 직접 정보들을 수집하면 신고조직의 부담도 줄일 수 있고 CERT관련 조직들도 신고자의 주관이 개입되거나 틀린 정보들을 배제한 객관적이고 정확한 정보들을 수집할 수가 있다.

신고기관이나 개인의 정보와 사고신고 정보를 노출시키지 않기 위해 SSL통신을 이용하고, 이 시스템에서 사용하는 빌트인 명령어들이 침해당했을 경우 수집한 정보를 신뢰할 수 없기 때문에 에이전트안에 명령어를 포함하고 해쉬값 비교를 통해 무결성을 보장한다.

Ⅵ. 신고 시스템 구현

시스템 사양: 펜티엄4 1.70MHZ, 256RAM, 레드햇 9.0(아파치 2+ssl, php4, mysql,)
주소/신고 화면:https://163.152.146.175/~ha/
관리자 화면: https://163.152.146.175/~ha/admin/admin_index.html

1. 시스템 개요

다음의 설문은 전문적인 지식이 필요 없는 것이 대부분이기 때문에 비교적 정확한 설문 작성을 할 수 있다.

신고 설문 작성 후 사용자가 동의를 하면 기초 자료 수집을 위한 에이전트를 ActiveX 방식으로 자동 설치하고 증거를 수집한다. 신고의 모든 단계가 끝나면, CERT 관리자는 다음과 같은 피해 호스트에 포함된 정보들을 분석하여 초기 대응을 위한 준비를 하고, 원하는 대응 방법을 선택한 데로 대처할 수 있다.

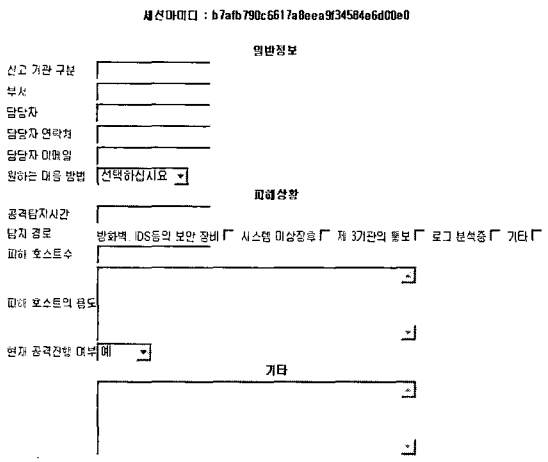


그림 7. 신고 설문 중 일부

로그 정보 수집 cb2f255bea96801c6dfce20928d868e5
동의하시면 자동으로 정보를 수집합니다.
동의하지 않으시면 직접 설문을 작성해야합니다.

보다 정확한 사고대응을 위해 동의해주십시요.

그림 8. 로그 정보 수집 화면

IX. 구축 시스템 실험

초기 신고 시스템이 실제 사고수사에 도움이 될지에 대해 직접 테스트 해보았다. 공격도구로는 DOS 공격도구인 targa를 사용하였다. 직접 공격을 하고 공격당하고 있는 시스템에서 신고하는 시나리오를 만들어 보았다.

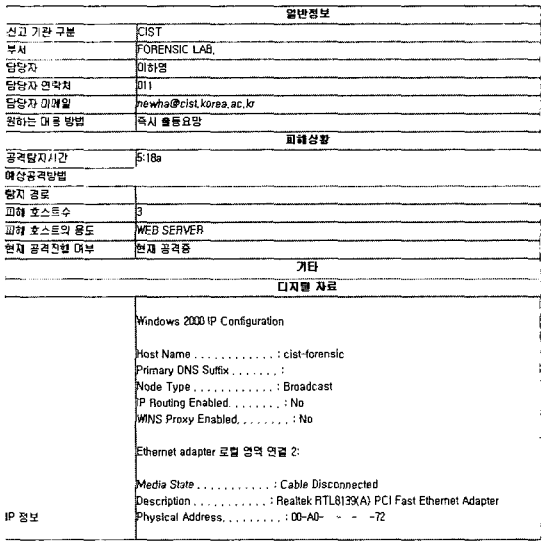
□ 신고자는 이러한 공격에 문외한이라는 가정 하에 다음과 같은 신고가 들어왔다.
□ 신고내용 : 컴퓨터 성능이 갑자기 너무 느려서 지금 당장 출동이 필요합니다.(신고 접수 결과 그림 9)

이 신고내용과 수집된 증거들 중 연관된 증거들을 살펴보도록 하겠다.

□ 결론 : 신고자가 관리하는 서버가 갑자기 느려졌다고 신고했고 위와 같은 증거들을 보았을 때 DOS류의 공격을 받고 있을 가능성이 크다고 판단할 수 있다.

표 6. 테스트 정보

ipconfig	이 정보로 신고자의 ip와 mac 주소를 알 수 있다.	
ARP	Interface: 163.152.xxx.xxx on Interface 0x1000003 Internet Address Physical Address Type 163.152. xxx.xxx 00-40-xx-xx-4f-09 dynamic 163.152. xxx.xxx 00-09-xx-xx-08-b1 dynamic 163.152. xxx.xxx 00-03-xx-xx-ec-0a dynamic 163.152. xxx.xxx 00-0f-xx-xx-a8-da dynamic	이 증거로 신고자의 컴퓨터가 default 시간동안 다음과 같은 IP들과 통신을 한 것을 알 수 있다.
netstate	Proto Local Address Foreign Address State TCP 0.0.0.0:135 0.0.0.0:0 LISTENING TCP 0.0.0.0:445 0.0.0.0:0 LISTENING TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING TCP 0.0.0.0:1053 0.0.0.0:0 LISTENING TCP 163.152.xxx.xxx:135 163.152. :2788 ESTABLISHED TCP 163.152.xxx.xxx:139 0.0.0.0:0 LISTENING TCP 163.152.xxx.xxx:1035 163.152.xxx.xxx:445 TIME_WAIT TCP 163.152.xxx.xxx:1037 163.152.xxx.xxx:445 TIME_WAIT TCP 163.152.xxx.xxx:1038 163.152.xxx.xxx:445 TIME_WAIT TCP 163.152.xxx.xxx:1041 163.152.xxx.xxx:445 TIME_WAIT TCP 163.152.xxx.xxx:1042 163.157.xxx.xxx:445 ESTABLISHED UDP 0.0.0.0:135 *:* UDP 0.0.0.0:445 *:* UDP 0.0.0.0:1026 *:* UDP 0.0.0.0:1044 *:* UDP 163.152.xxx.xxx:137 *:* UDP 163.152.xxx.xxx:138 *:* UDP 163.152.xxx.xxx:500 *:*	이 증거를 보아 "163.152.xxx.xxx"에서 여러 포트로 접속을 시도 했음을 알 수 있다.
start	AhnLab Task Scheduler COM+ Event System Computer Browser DHCP Client Distributed Link Tracking Client DNS Client Event Log IPSEC Policy Agent Logical Disk Manager Messenger MonSvcNT Network Connections Plug and Play Print Spooler Protected Storage Remote Procedure Call (RPC) Remote Registry Service Removable Storage RunAs Service Security Accounts Manager Server System Event Notification Task Scheduler TCP/IP NetBIOS Helper Service Windows Management Instrumentation Driver Extensions Workstation	이 증거를 보았을 때 정상적이지 않은 서비스가 없음으로 보아 Back Door와 같은 종류에 의한 시스템 자원의 잠식은 아님을 알 수 있다.



일반정보	
신고 기관 구분	CIST
부서	FORENSIC LAB.
담당자	이하영
담당자 연락처	011
담당자 이메일	hewha@cist.korea.ac.kr
원하는 대응 방법	즉시 출동요망
피해상황	
공격탐지시간	5:18a
예상공격방법	
탐지 경로	
피해 호스트수	3
피해 호스트의 용도	WEB SERVER
현재 공격진행 여부	현재 공격중
기타	
디지털 자료	
IP 정보	Windows 2000 IP Configuration Host Name . . . . . : cist-forensic Primary DNS Suffix . . . . . : Node Type . . . . . : Broadcast IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No Ethernet adapter 로컬 영역 연결 2: Media State . . . . . : Cable Disconnected Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet Adapter Physical Address. . . . . : 00-A0- ~ - -72

그림 9. 관리자 화면 중 일부

이 시나리오처럼 사용자의 복잡한 입력 작업 없이 간단히 현재 컴퓨터의 상태와 자동으로 수집된 증거들만을 가지고, 대강의 현상을 파악할 수가 있다. 이는 신고자와 CERT팀 모두에게 시간과 노력을 절감하는 결과를 가져다 줄 것이다.

X. 결론 및 향후 연구 과제

세계 최고 수준의 국내 IT 인프라 환경은 사고 대응관점에서 보면 오히려 굉장한 난관이라 할 수 있다. 그럼으로, CERT팀에서는 평시에 해당 조직에 최적화 된 모든 전략과 행동양식을 만들어 놓고 조직원들을 교육시켜야 한다.

그런 연후에 초기대응 행동요령에 필요한 정보들을 얻을 수 있는 사고신고 시스템을 개발하면 신속하게 사고 대응을 할 수 있을 것이다.

위에서 테스트해 본 봐와 같이 수집된 증거들과 신고자의 신고의 연관성을 조사하면 사고의 개요를 알아낼 수 있으며, 그 것을 바탕으로 실제 사고 대응에 들어가기에 앞서 대략의 사고대응 전략을 세움으로써 매우 효율적이고 신속한 사고 대응을 할 수 있을 것이다.

향후 실제 CERT에 접목시켜 실전에서 사용해 보고, 신고 설문의 현실화와 증거 수집 에이전트에 OS 내부명령어 외에 유용한 FREEWARE들을 식별하여 추가할 예정이다.

위와 같은 향후 연구 과제들을 해결하여 침해사고 대응에 좀 더 효율적인 대응을 할 수 있도록 노력할 것이다.

참 고 문 헌

[1] 인터넷 통계 검색 시스템, http://isis.nic.or.kr/main/issue_list.html

[2] 사이버 테러대응 센터 범죄통계, http://ctrc.go.kr/statistics/index.jsp

[3] 대검찰청 인터넷 범죄수사 센터, "http://icic.sppo.go.kr/"

[4] 사이버 테러대응 센터, "http://www.ctrc.go.kr/rule/index.html"

[5] 국가 사이버 안전 센터, "http://www.ncsc.go.kr/"

[6] 인터넷 침해사고 대응 지원 센터, "http://www.certcc.or.kr/"

[7] US-CERT, "http://www.us-cert.gov/"

[8] 인터넷 침해사고 대응 센터, "http://www.krcert.or.kr/"

[9] AUSCERT, "http://www.auscert.org.au/"

[10] 이현우 · 심정재, "사례로 배우는 해킹사고 분석 &대응"

[11] CERT Coordination Center, "http://www.cert.org/"

[12] Chris Prosise, Kevin Mandia, "Incident Response Computer Forensics, Second Edition", "McGraw-Hill/Osborne"

[13] SURFnet-CERT, "http://cert.surfnet.nl"

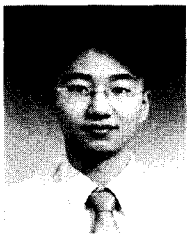
[14] 종합침해사고 시스템 1 : http://www.cprsoftware.com/products.html

[15] 종합침해사고 시스템 2 : http://www.bestpractical.com/rtir/

〈著 者 紹 介〉

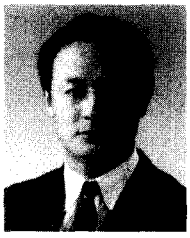
이 하 영 (Ha-Young Lee)

2003년 : 고려대학교 학사
2003년~현재 : 고려대학교 정보보호 대학원 석사과정
〈관심분야〉 컴퓨터 포렌식, 위험분석, 컴퓨터 범죄 수사 프로세스



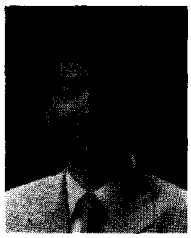
김 현 상 (Hyun-Sang Kim)

2002년 : 경희대학교 학사
2004년 : 고려대학교 정보보호 대학원 석사
2004년~현재 : 한국정보보호학회 조기경보시스템연구회 WG07 "로그기록을 중심으로한 네트워/시스템 포렌식" 부운영자
2005년~현재 : 고려대학교 정보보호 대학원 박사과정, 한국정보보호학회 조기경보시스템연구회 WG07 "로그기록을 중심으로한 네트워/시스템 포렌식" 부운영자
〈관심분야〉 컴퓨터 포렌식, 조기경보, 침해사고 후속조치 자동화, 분산처리 컴퓨팅



최 운 호 (Un-Ho Choi)

1990년 : 광운대학교 학사
1995년 : 광운대학교 대학원 전자계산학과 석사
2004년 : 한세대학교 대학원 정보보호공학과 박사
1989년~1996년 : 한국전산원 선임연구원
1996년~2001년 : 한국정보보호진흥원 팀장
2002년~현재 : 금융결제원 금융ISAC실 정보보호평가팀장
2003년~현재 : 한국정보보호학회 이사
2004년~현재 : 한국정보보호학회 조기경보시스템연구회 위원장
2004년~현재 : 국가정보보안협의회 조기경보시스템연구회 위원장
〈관심분야〉 조기경보, 블랙리스트, 관제센터운영, 침해사고신고 자동화 등



이 상 진 (Samgjin Lee)

1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임연구원
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식

임 종 인 (Jong-in Lim)

1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1986년 3월~2001년 1월 : 고려대학교 자연과학대학 정교수
2001년 2월~현재 : 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 정보보호 이론, 정보보호 정책