특집 12

국방 전산망의 침해사고 대응체계 개선을 위한 통합 로그센터 구축 연구

목 차

전승민 · 이을석
((주)엠투소프트 · (주)이너버스)

1. 서 론

정보화 사회로 발전하면서 통신서비스 이용자들은 보다 신속하고 다양한 서비스를 요구하게 되었으며, 컴퓨터와 정보통신 기술의 발달은 전자 메일, 파일 전송 등과 같은 기본적인 서비스뿐 만 아니라 분산 환경을 바탕으로 하는 멀티미디어, 전자 결재, 전자 상거래 등과 같이 복합적인 네트워크 서비스들로 확장되고 있다. 그리고 이와 같은 발전은 전송 속도의 고속화, 대용량의 데이터 전송 등으로 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 거두고 있는 반면, Open Network인 인터넷의 개방으로 인한 외부자의 시스템 불법 침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 공격 등 부정적인 기능들도 날로 증대시킴으로서, 이로 인한 피해 규모는 심각한 수준에 이르고 있다. (그림 1)은 인터넷침해사고대응센터에서 집계한 월간 침해사고 통계를 나타낸 것이다[1].

국군지휘통신사령부는[2] 국방정보통신기반체계에 대한 정보보호 대책 수립 및 집행을 총괄하고 있으며,국방 CERT(Computer Emergency Response Team)를 설치하고 국방통합관제체계를 운영하고 있다. 또한 사이버 침해 사전 탐지 및 대응을 위하여 통합 매니저 시스템, 침입탐지 시스템, 침입차단 시스템, 보안관제 에이전트, 취약점 진단 시스템, 바이러스 차단 시스템으로 구성된 통합보안관제체계를 구축 운용하고 있다. 현재 국방 CERT는 사이버 침해사고 발생 시 각 군의 전산실, 보안 관제 센터 등의 로그 분석을 개별적으로 진행하여야 하기 때문에 통합적인 로그 분석이 어려운 실정이다. 전군적인 대규모의 국방통합정보관리소인 메가센터 구축과 통신 속도의 증가, 군 업무 전산화의 증가 등으로 분석 할 로그가 대량화 되고 있어 분산되어 있는 로그의 전체적인 분석이 점차 어려워지고 있다. 그러므로 대량 로그의 통합 관리, 분석을 통해 전산망 침해사고의 대응체계를 개선할 필요가

1) 인터넷침해사고 동향 및 분석 2008년 8월호, http://www.krcert.or.kr
2) 미래 사이버 대전 국방 통합 CERT 구축 방안, 2005년, 김기동

구분	2007	2008											2008
	total	1	2	3	4	5	6	7	8	9	10	11	12	total
웜·바이러스	5,996	793	653	966	840	811	802	903	478					6,246
해킹신고처리	21,732	1,352	1,516	1,360	1,262	1,470	1,518	1,136	1,190					10,804
·스캔및레이	11,668	592	597	530	565	636	574	464	423					4,381
·피싱경유지	1,095	88	117	110	94	116	131	76	62					794
·단순침입시도	4,316	386	289	350	291	206	226	247	240					2,235
·기타해킹	2,360	239	226	235	227	231	218	242	220					1,838
·홈페이지변조	2,293	47	287	135	85	281	369	107	245					1,556
악성 봇(Bot)	11.3%	10.7%	13.0%	9.6%	9.6%	7.8%	8.9%	11.7%	9.7%					10.1%

(그림 1) 인터넷침해사고 통계

있다. 대량 로그를 통합 관리하고 체계적으로 분석할 수 있는 통합 로그센터의 구축은 전산망 침해사고에 대한 신속한 대응을 가능하게 한다.

최근에는 보안사고 발생 시 침해사고의 원인 분석 및 피해 확산을 예방하기 위하여 로그정보에 대한 분석이 필수적이다. 이에 정보통신부의 "정보시스템 구축 운영과 관련한 기술 가이드라인"[3]에서는, "주요 시스템 및 장애에 대한 로그 보관, 백업(backup) 및 분석지침을 수립하고 로그는 최소 6개월 이상 백업을 유지 관리하여 주요 보안시스템(Firewall, IDS, VPN)의 로그는 매일 분석"을 권고하고 있다. 그리고 금융감독원의 "금융기관 전자금융업무 감독규정[4]"에 의하면 전산자료 유출, 파괴 등을 방지하는 정보시스템 가동기록 보존 및 인터넷 접속기록 금융기관은 1년 이상 별도 보관을 시행하고 있다. 그러나 중·소 공공기관과 중소기업에서는 로그분석시스템 및 대규모의 저장장치를 구축하고 이에 대한 지속적이고 체계적인 관리·운영을 담당하는 관리자를 별도로 운영하는 데는 기술적으로나 경제적으로 많은 애로사항을 갖고 있다. 이에 네트워크의 안정적 운용을 향상시키는 기술로 통합 로그분석·관리 기능을 제공하는 로그수집, 분석, 백업을 통합적으로 운용할 수 있는 통합 로그센터에 대해서 살펴보고자 한다. 본 논문의 구성은 제2장에서는 관련연구 및 기술 동향에 대해서 기술하고, 제3장에서는 통합 로그센터의 설계를 언급하고 제4장에서는 본 연구와 관련한 결론 및 향후 계획에서 대해서 언급하고자 한다.

2. 관련 연구

2.1 국내외 관련 분야 시장 동향

로그 분석 툴은 98년부터 본격적으로 시장이 형성된 후 초기에는 트래픽 관리가 필요한 인터넷마케팅 업체 위주로 수요층이 형성되었고, 기업과 공공기관의 업무가 클라이언트/서버에서 웹 서버 환경으로 전환되면서 트래픽 관리에 대한 인식이 제고되어 그 수요가 늘고 있는 상황이다. 특히 금융권과 대형 통신업체, 인터넷쇼핑몰들이 대대적으로 e비즈니스에 대한 보안을 강화하고 있으며, 정부가 전자정부 프로젝트를 강력하게 추진하면서 해킹이나 바이러스 침투에 따른 통신망 사고에 대비하기 위한 로그분석의 필요성이 공공기관에까지 확대되고 있다. 로그분석시스템에[5] 대한 정부규제강화, 기업의 인지도 확산에 힘입어 2005년 50억원 규모였던 로그분

3) 정보통신부, 정부혁신지방분권위원회, 한국전산원 제정, "정보시스템 구축 운영과 관련한 기술 가이드라인 버전 1.0", 2004년 4월

4) 금융감독원 금융기관 전자금융업무 감독규정 시행 세칙
- 제6조(전산자료 보호 대책) : 전산자료 유출,파괴 등을 방지하는 정보시스템 가동기록 보존
- 제10조(IP주소 사용 대책) : 인터넷 접속기록 1년 이상 별도 기록 보존

5) 디지털타임스 허정화 기자

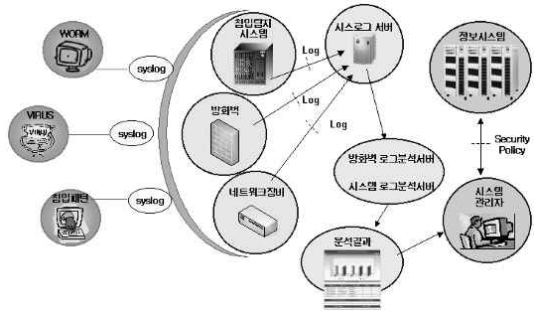
석 시스템 시장은 2008년 150~200억원 규모로 추정되며 해마다 대폭 증가하고 있는 추세이다.

미국 등 선진국에서는 IT컴플라이언스 준수를 위해 통합 로그센터 구축이 폭넓게 이루어지고 있다. IT컴플라이언스란[6] 새로운 규제나 법안, 권고 등 각 나라별 혹은 글로벌 감독당국이 제시한 각종 요건을 만족 시킬 수 있도록 기업의 정보시스템과 업무프로세스를 재정비하는 것을 의미 한다. 국내에서도 금융감독원의 '재해복구 시스템 구축권고'나 기업 회계 선진화를 위한 각종 법령 재정비등 국내용은 물론 바젤II와 사베인즈-옥슬리 등 해외 법안이나 권고사항과 관련된 IT컴플라이언스 수요가 올해부터 본격화될 전망이다.

3. 통합 로그센터 시스템의 설계

3.1 통합 로그센터(Integrated Log Center)의 개요

통합 관제체계를 구축하고 이를 효율적으로 운영하기 위해서는 각종 전산장비와 보안장비의 로그를 통합하여 로그센터를 구축하는 것이 필요하다. 이것은 ESM, TSM, NMS, SMS등 각종 관리도구를 One-Point에서 장애관리를 할 수 있기 때문이다. 로그센터가 갖춰야할 주요기능은 Dashboard를 통한 통합관제가 필요하며, 통합 보고서를 제공하고, 실시간으로 데이터와 연동되어야 한다. 이를 통해서 정보보호, 시스템관제, 네트워크 관제, 응용서비스 관제를 통합할 수 있으며 보안 영업별로 문제점의 대응 체계를 확립할 수 있다. syslog는 장비의 에러 메시지나 보안사고의 이벤트를 정확히 기록하여 보안사고 발생시 원인 규명을 위한 근거 자료로 활용 가능하며 (그림 2)는 sysLog기반의 통합로그관리시스템(SILAS: SysLog-based Integrated Log Management System)의 개념적인 구조를 나타낸 것이다.



(그림 2) SysLog기반의 통합로그관리시스템의 개념적인 구조

3.2 통합 로그 센터의 제한 사항

통합로그 센터 구축을 위해서는 크게 준비공정, 자료관리, 소스데이터검증공정, 분석DB구축공정 그리고 통합 점검으로 시 아래와 같은 제한사항을 고려하여 구축한다. (그림 3)은 통합 로그센터 구축 계획 수립 과정별 세부 내용을 나타낸 것이다.

이러한 통합로그센터는 다수의 정보보호관리, 시스템관리 콘솔과 산재된 관리정보로 인해 장애 발생 시 다단계 접근경로 분석 및 문제파악 애로를 해결할 수 있어야 하는데, 국방망, 인터

(그림 3) 통합 로그센터 구축 계획 수립

6) 디지털타임스 박서기 기자

넷, 정부통합망 등 각 망별로 단위 운영시스템 운영에 따른 정보통합 및 융합의 어려움이 제약으로 존재한다. 하지만, 사이버위협이 증대됨에 따라 웹보안의 강화가 필요한 상황에서 소수의 인원으로 단시간 내에 장애 및 침해상황을 파악하고, 최단 시간 내 사고에 대응하기 어려운 실정이다. 이에 각종 전산장비에서 발생하는 다양한 로그를 통합하여 수집하는 것이 필요하며, 수집된 로그는 통합하여 분석하고 정기적으로 보안 담당자에게 리포트화 되어야 한다.

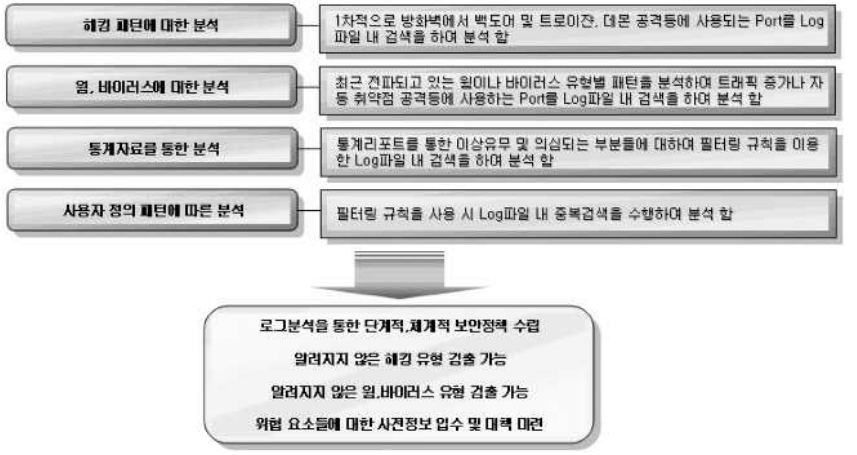
3.3 로그분석 모듈 설계

로그 분석 모듈은 일별 로그파일이 10Gbyte 이상의 대용량 로그파일 분석 기능과 멀티쓰레드, 멀티프로세스 환경을 지원함으로써 포괄적인 트래픽 분석과 해킹 패턴이나 최근 전파되고 있는 웜이나 바이러스 유형별 패턴을 분석한다. 그리고 단순 통계에 의존한 방법이 아닌 인공지능 알고리즘을 사용하여 시스템 사용자의 이상징후를 조기에 발견하고, 시스템으로의 침입시도를 파악할 수 있게 된다.

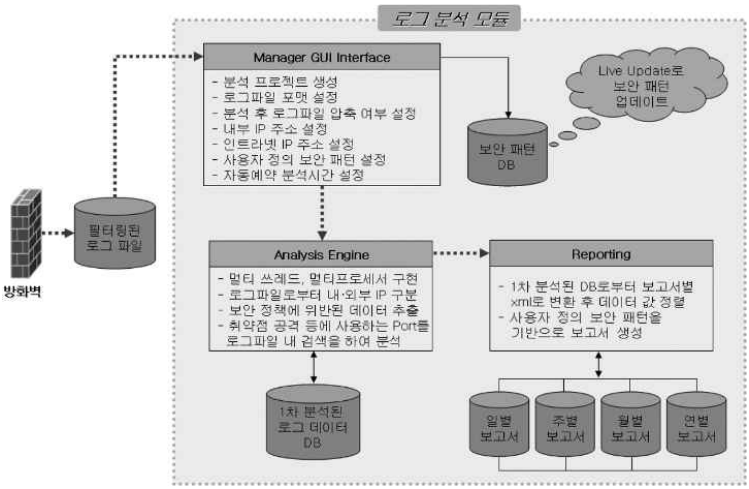
따라서 분산되어 있는 시스템들의 활동에 대한 종합적인 분석정보를 얻을 수 있으며, 공격의 원천과 위험수준 모두를 식별하고, 네트워크를 보다 더 쉽게 방어할 수 있는 정보를 고객에게 제공한다. 또한 위험요소 분석을 통해 최적의 보안정책을 수립할 수 있다. (그림 4)는 다양한 로그패턴을 분석하는 과정을 나타낸 것이다. 세부 로그분석 모듈의 동작 메커니즘은 (그림 5)와 같다.

3.4 로그 분석 리포팅 시스템 설계

통합 로그 관리 시스템은 대량의 로그 정보를 수집, 정제, 분석하여 관리자에게 효과적으로 제공해야 한다. 분석된 로그 정보를 효과적으로 제공하기 위해서는 정기적인 로그 분석 통계 정보의 보고, 위험 상황 발생 시 실시간 상황 보고, 표와 차트를 통한 직관적이고 분석적인 보고, 대용량 로그에 대한 요약 및 상세 정보를 효율적으로 제공하는 Drill Up/Down 기능의 보고가 필요하다. 정기적인 로그 분석 통계 정보 보고서는 로그 분석 리포팅 시스템에서 자동으로 제공하여야 하며, 이를 위해 스케쥴링 기능이 필요하다. 해킹 시도, 웜이나 바이러스의 감염 등 시스템에 위급한 상황이 발생했을 경우, 이러한 상황과 조치 사항에 대한 정보를 실시간으로 관리자에게 보고하기 위해 관리자의 휴대형 통신장비(핸드폰)에 SMS(Short Message Service) 발송 기능도 활용할 수 있다. 통계 정보에 대한 효율적 분

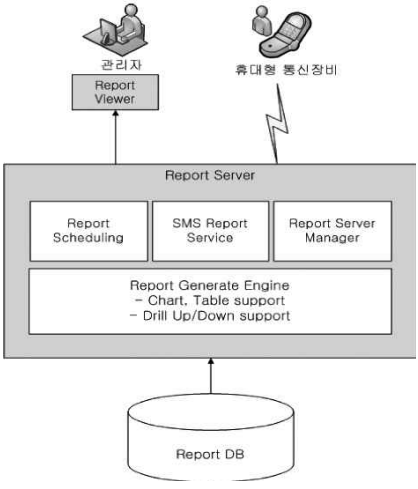


(그림 4) 다양한 로그패턴 분석 과정



(그림 5)세부 로그분석 모듈의 동작 메커니즘

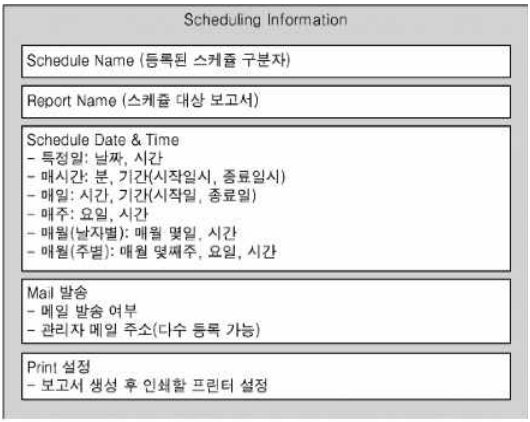
석을 위해서는 표와 차트를 통한 로그 정보의 일목요연한 표현 기능이 필요하고, 차트는 로그의 보안 영역별 분포, 트래픽의 시간별 추이 등 종합적인 분석 정보를 직관적으로 제공할 수 있어야 한다. 로그 정보는 대량의 데이터에 관한 정보이기 때문에 요약 정보와 상세 정보를 효율적으로 제공하고, 대량 데이터의 효율적 분석을 위해 OLAP(Online Analysis Processing) 수준의 분석 기능이 필요하다. 국내에는 이러한 기능을 제공하는 상용 리포팅 소프트웨어들이 있으며, 로



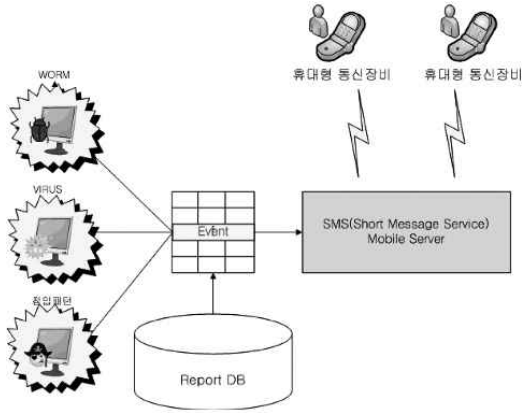
(그림 6) 로그 분석 리포팅 시스템 구성도

그 분석 리포팅 시스템은 이런 다양한 기능과 보고서의 개발 생산성, 유지보수성을 위해 상용 리포팅 툴을 이용하는 것이 매우 효과적이다. (그림 6)은 로그 정보를 유/무선으로 관리자에게 제공하기 위한 로그 분석 리포팅 시스템의 구성도이다.

로그 분석 리포팅 시스템의 스케쥴링 기능은 보고서를 자동으로 생성하여 관리자에게 전달하거나 보관하는 기능이다. 스케줄링 기능은 어떤 보고서를 언제 생성할 것인지 설정하고, 생성된 보고서를 관리자에게 메일로 전달할 수 있어야 한다. 스케쥴링 보고서의 생성 날짜와 시간은 보안상 각별히 관찰해야할 특정일에 대한 설정과 정기적인 보고서가 생성될 작업 시기와 주기의 설정 기능이 필요하다. 정기적 매월 보고서의 작성 작업 시기에 대한 설정은 매월 몇일과 함께 매월 몇째주 무슨 요일의 작업 일시 설정 기능이 가능함으로서 관리 및 점검기준에 따른 유연한 로그 분석 보고서를 생성할 수 있어야 한다. 스케쥴링 보고서는 보고서가 생성되면서 파일 형태로 보관되어야 하며, 보고서 생성과 함께 인쇄되어 보관될 수도 있어야 한다. (그림 7)은 리포팅 스케쥴링 정보의 구성도이다.



(그림 7) 리포팅 스케쥴링 정보 구성

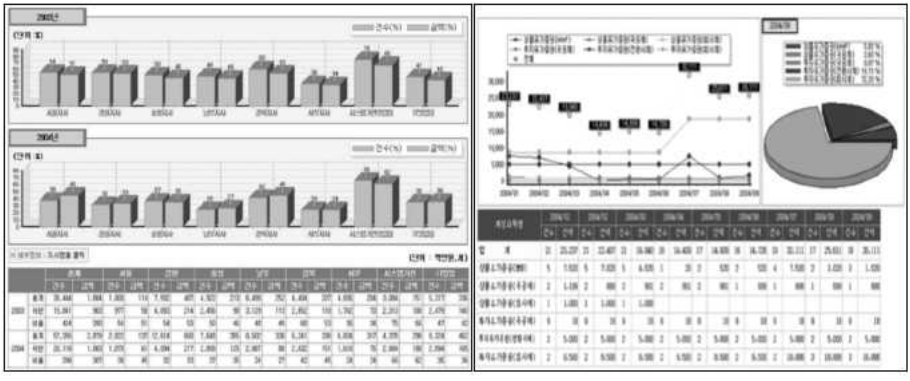


(그림 8) SMS Critical Report 개념적 구조

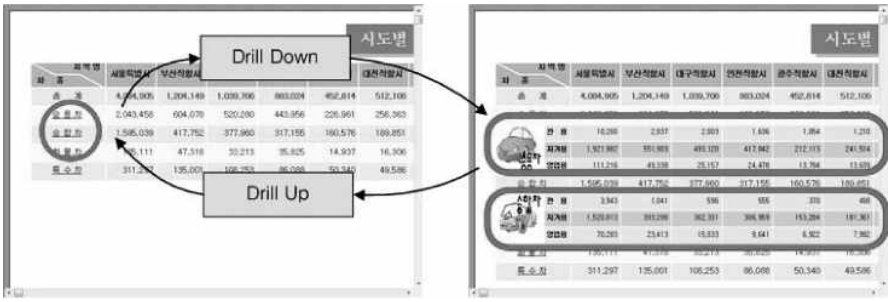
SMS 발송 기능은 위급 상황을 실시간으로 관리자에게 전달함으로서 피해를 최소화하고 보안 취약점을 최대한 신속히 조치할 수 있도록 한다. Report DB에 웜, 바이러스, 침입패턴 등의 보안상 문제가 되는 로그 정보가 있으면, SMS Mobile Server를 통해 관리자의 핸드폰에 실시간 해당 정보와 조치 사항을 전달하여 적절한 대응을 할 수 있도록 보고해야 한다. 이러한 긴급 상황에서 관리자에게 신속한 대응을 요구하는 상황보고를 SMS Critical Report라고 한다. (그림 8)은 SMS Critical Report의 개념적 구조를 나타낸 것이다.

표와 차트는 대용량 데이터의 통계정보를 관리자가 신속하게 판독할 수 있도록 해준다. 표는 대용량 데이터를 일목요연하게 표현할 수 있고 로그 정보와 같이 데이터의 변화가 중요한 정보의 추이에 대한 직관성을 제공한다. 차트는 로그의 분류별 분포도, 구성비, 추이, 변화의 정도 등 로그의 분석적 정보를 제공한다. 보고서는 표와 차트로 대용량 로그 정보를 전달함으로서 관리자의 보안상 판단 능력에 도움을 제공해야 한다. (그림 9)는 다양한 형태의 표와 차트로 구성된 보고서 샘플이다.

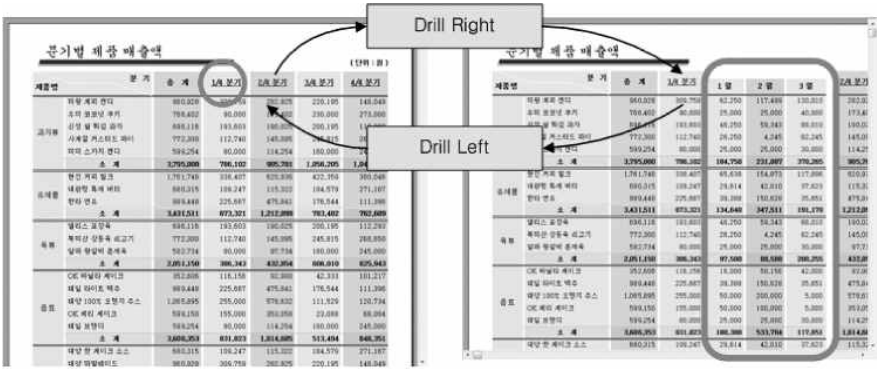
로그 분석 리포팅 시스템에서 OLAP수준의 분석기능을 위해 Drill Up/Down 기능이 있어야 한다. Drill Up/ Down 기능은 대용량 로그 정보



(그림 9)표와 차트로 구성된 보고서 샘플



(그림 10) Drill Up/Down 동작 과정



(그림 11) Drill Left/Right 동작 과정

를 요약 정보와 상세 정보로 나누어 문제의 원인을 빠르게 찾을 수 있도록 해주는 기능이다. 관리자는 요약 정보를 통해 문제 발생 영역을 찾아내고, 해당 요약 영역의 상세 정보로 접근하여 문제의 원인을 빠르게 파악할 수 있다. Drill Up은 상세 정보를 접어(Fold) 요약 정보를 제공하는 것을 말하고, Drill Down은 요약 정보를 아래로 펼쳐(Expand) 상세 정보를 제공하는 것을 말한다. 위아래로 요약 정보와 상세 정보를 제공하는 것처럼 좌우로 요약 정보와 상세 정보를 제공하는 것을 Drill Left/ Right라 한다. (그림 10)은 Drill Up/Down 동작 과정을 나타낸다. (그림 11)은 Drill Left/Right 동작 과정을 나타낸다.

4. 결론 및 향후 계획

본 논문에서는 통합 로그센터시스템의 설계를 제안하였으며, 이종의 전산 인프라에서 발생하는 각기 다른 포맷의 로그정보를 분석하여 유연하게 리포팅할 수 있는 시스템을 소개하였다. 이러한 시스템은 대용량의 로그파일을 분석, 보안 정책에 위배된 로그 데이터를 추출하여 해킹 공격에 대한 유형별 보고서를 제공할 수 있으며, 내부 사용자의 네트워크 사용에 대한 분석을 통하여 트래픽 사용, 서비스 사용 등에 대한 유연한 보고서를 제공할 수 있는 통합 로그센터 모듈을 설계 하였다. 이에 본 연구에서 제안한 설계 내용을 기반으로 향후에는 시스템의 구현 및 평가의 과정이 필요하며, IT인프라를 기반으로 한 정보유출 시도를 탐지하는 다양한 보안 룰셋을 개발할 필요가 있다. 이렇게 개발된 보안 룰셋은 로그 분석 리포팅 시스템을 이용하여 보안 담당자에게 다양하고 유연한 보고서를 제공하여 국방 정보보안체계를 과학적으로 프로세스화 할 수 있을 것이다.

참고문헌

[1] C. Pfleeger, 'Security in Computing Second Edition' Prentice Hall, 1997.

[2] Check Point Firewall-1 OPSEC Open Specification Version 1.01, Check Point Software Technology, Inc., Nov 8, 1998.

[3] Check Point OPSEC SDK Version 4.1 Release Notes, Check Point Software Technology, Inc., Nov 2, 1999.

[4] James L. Peterson, "Petri Net Theory and The Modeling of Systems", Prentice-Hall, 1981.

[5] IT 보안 해설서, http://members.nate.com/hayonia/it12- firewall.html

[6] 인터넷 보안과 방화벽 개론, http://guardian.syds.com/data/fire__data/fire__data.htm#spec

[7] 인터넷침해사고대응센터, http://www.krcert.or.kr/ report/technical__report.jsp

[8] Netsecure Technology, http://www.netsecuretech.com/ products/pro__symant__fire100.asp

[9] 정보시스템 보안 및 효율적인 방화벽, http://www. kmi.re.kr/english/public/

[10] 국내 해킹시도 탐지 분석, http://www.superuser.co.kr/security/certcc/tr2000-09.htm

[11] 해킹 패턴과 윈도우 보안 전략, http://www.ezhack. net/about/winhack.asp

[12] 김기동, '미래 사이버전 대비 국방 통합 CERT 구축 방안', 아주대학교, 2005.

저자약력

전 승 민

1991년 아주대학교 전자계산학과 (공학사)
1993년 아주대학교 컴퓨터공학과 (공학석사)
1994년~2001년 한국정보공학 부장
2001년~현재 (주)엠투소프트 연구소장
관심분야 : 리포팅 소프트웨어, X-Internet, AJAX, RFID 관련 응용솔루션
이 메 일 : smchun@m2soft.co.kr

이 을 석

1996년 아주대학교 전자공학과 (공학사)
1996년~1998년 삼성전자 시스템사업부 연구원
1999년~2000년 TrendMicro Korea 개발팀장
2000년~2001년 (주)유아이소프트 개발팀장
2001년~현재 (주)이너버스 대표이사
관심분야 : 로그분석툴, 보안
이 메 일 : uslee@logcenter.com