情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

이기종 로그에 대한 통합관리와 IT 컴플라이언스 준수

김 완 집*, 염 흥 열**

요 약

로그 데이터는 네트워크 및 보안장비, 서버시스템, DBMS, 서비스 등에서 사용자의 행위를 기록하여 보관하며 있으며, 이를 통해 시스템의 안정적인 운영을 지원하거나, 해킹 등의 불법 침해를 당하였을 때 침입경로 추적과 취약점을 찾아내어 보완할 수 있는 중요한 자료이다. 하지만 로그 데이터는 여러 시스템에 각각 다른 형태로 산재하며 일시적인 기간 동안 저장되어 있거나, 해커에 의해 고의적으로 삭제되기도 하며, 저장 용량 문제로 인해 필요시에 없을 경우가 많다. 본 연구에서는 네트워크 장비와 보안장비의 표준로그인 syslog와 유닉스/리눅스 시스템과 윈도우즈서버의 로그에 대한 특성을 고찰하였으며, 특히 서비스로그로서 아파치 웹서버와 IIS서버의 로그에 대한 특징을 정리하였다. 여러 종류의 시스템에서 발생되는 로그를 통합하여 관리하기 위해서는 이기종 로그 데이터의 생명주기 방법론을 제시하였다. 또한, 최근에 IT보안 사고에 대응하여 규제준수를 요구하고 있는 국내외의 IT컴플라이언스에서 로그에 대한 관련 내용을 살펴보고, 그 준수할 방안을 제시한다. 결론으로 IT인프라의 보안강화적인 측면과 IT컴플라이언스 준수를 위해, 효율적인 로그에 대한 수집과 보관 및 활용성 측면에서의 이기종의 통합로그관리도입 필요성, 생명주기, 기술적 준비사항, 컴플라이언스 요구사항을 제시한다.

Ⅰ. 서 론

얼마 전, 중국의 한 해커가 한국의 대형 포탈사이트에서 고객정보를 불법으로 유출하여 거래를 하고 있는 것으로 밝혀졌으나, 정작 해당 사이트에서는 불법침입의 사실을 파악하지 못하고, 로그를 찾아보고자 하였으나, 짧은 기간의 로그만 남아 있어서 이마저도 추적할 수 없는 곤란한 일이 발생하였다. 이처럼 정보시스템의 발전에 따라 불법적인 해킹 등이 나날이 증가하고 지능화되어 가며, 또한 내부자에 의한 기밀자료의 유출 등 정보화의 역기능이 사회적인 문제로 대두되고 있다[1].

이에 대해, 각종 보안시스템으로 무장하여 대응하고 있지만 매번 새로운 해킹 공격은 새롭게 나타나며, 방어는 그 다음에 보완하여 대처하는 현실에서 나아가 기존 보안관리시스템을 강화할 수 있는 새로운 기술에 대한 관심이 높아지고 있다. 로그를 통한 행위추적 및 IT감사가 그에 해당된다.

개인정보는 OECD가 개인정보보호에 대한 8대 가이드라인을 제정할 만큼 그 중요성을 강조하고 있다. 그러나 정작 수많은 공공기관이나 기업조직이 개인 정보를 관리하는데 소홀히 하고 있으며, 적절한 투자가 이뤄지고 있지 않다[2].

시스템관리 및 해킹과 내부정보 유출에 대비한 관리방법으로 가장 기본적인 시스템 로그를 통한 취약점 분석 및 사후 증적 자료 확보를 위한 방안을 찾을 필요성이 있다.

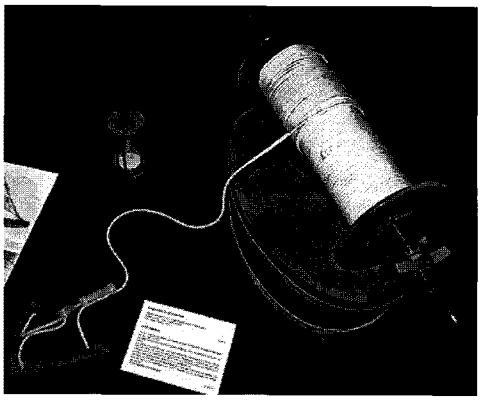
이를 위해, 본 연구는 로그에 대한 이론적 고찰 및 통합로그에 대한 기술적 측면을 설명하고, 국내외 IT컴플라이언스에 대한 규제사항을 열거하여, IT컴플라이언스를 준수하는 통합로그관리가이드라인을 제시하고자 한다.

Ⅱ. 로그에 대한 고찰

2.1 어원적 의미

로그(log)라는 단어의 어원은 항해 중인 배의 속력을

본 연구는 서울시 정보보안 정책 및 순천향대학교 정보보호학과 박사과정 관리로 수행되었습니다.
* 순천향대학교 정보보호학과 박사과정, 서울시청 정보통신담당관 정보보호정책팀장 (kimwj@seoul.go.kr)
** 순천향대학교 정보보호학과 교수 (hyyoum@sch.ac.kr)



〔그림 1〕 항속을 측정하기 위한 로그 킷

측정하기 위해 뱃머리에서 통나무 조각을 바다에 던져 넣은 후, 그것이 뱃꼬리까지 흘러간 시간과 배의 길이로 측정하는데 유래되어 현재까지도 배의 속력계라는 의미로 사용되고 있다. [그림 1]에서 보면 파리의 해양박물관에 전시되어 있는 유물로 ship log라는 킷(kit)인데 나무토막(log)을 실(log-line)로 연결하여 길이를 잴 수 있는 형태로 되어 있다. 이 로그킷을 사용하여 항속을 측정하여 항해일지에 기록하는 일을 로그라고 한다.

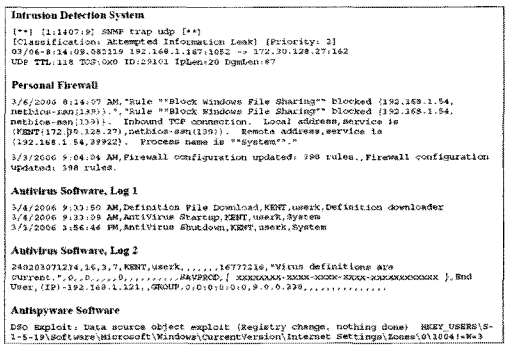
2.2 시스템 로그의 의미

본 연구에서 사용하고자 하는 로그의 개념은 시스템에 접속한 사용자들의 행위에 대한 결과를 저장한 기록이라는 의미로 본다. 여기에서 사용자는 좁은 의미에서는 시스템의 사용자(user)이며, 넓은 의미로는 다른 시스템과 통신장비 그리고 운영체제 및 프로세스를 모두 포함하는 의미로 다루고자 한다.

외부로부터 침입한 해커가 시스템에서 어떠한 일들을 행하였는지, 또는 사용자가 어떠한 명령어를 사용했는지 등 보안적인 의미의 정보들과 시스템이 처리한 업무와 에러 등의 시스템 운영정보들을 모두 기록하여 저장하고 있다. 즉, 시스템에서 행해지는 모든 일들에 대한 행위기록이 저장되어 있는 것이 로그이다.

이러한 로그는 대부분은 텍스트 형태로 파일로 저장되어 특정 위치에 일시적 또는 영구적으로 보관되고 있다. 시스템 운영자는 장애시나 보안사고 같은 상황이 발생하였을 때 특정 로그파일을 검색하여 필요한 정보를 찾아 조치를 하는 목적으로 사용된다.

시스템 로그는 해커의 침입을 감지 및 추적하고 서버



Intrusion Detection System

[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.085119 192.168.1.187:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87

Personal Firewall

3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54, netbios-ssn(139)).","Rule ""Block Windows File Sharing"" blocked (192.168.1.54, netbios-ssn(139)). Inbound TCP connection. Local address,service is (KENT:172.30.128.27),netbios-ssn(139)). Remote address,service is (192.168.1.54,39922). Process name is ""System""."

3/3/2006 9:04:04 AM,Firewall configuration updated: 398 rules.,Firewall configuration updated: 398 rules.

Antivirus Software, Log 1

3/4/2006 9:33:50 AM,Definition File Download,KENT,usark,Definition downloader
3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,usark,System
3/3/2006 3:56:44 PM,AntiVirus Shutdown,KENT,usark,System

Antivirus Software, Log 2

240203071214,16,3,7,KENT,usark,,,,,,,16777216,"Virus definitions are current.",0,,0,,,,,0,,,,,,,,,,#AVPROD,{ XXXXAAAA-XXXX-XXXX-XXXX-AAXXXXXXXXXX },End User,(IP)-192.168.1.121,,GROUP,0;0:0:0:0,9.9.0.239,,,,,,,,,,,,,,

Antispyware Software

DSO Exploit: Data source object exploit (Registry change, nothing done) HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=#=3

〔그림 2〕 다양한 종류의 로그들

접속실패의 원인을 찾아 그 문제를 해결하는 데 결정적인 단서를 제공하고 있으나, 그 로그 데이터가 여러 곳에 산재하여 관리자가 일일이 체크하지 못하는 경우가 많다. 시스템 로그 데이터가 시스템에서 발생하는 거의 모든 상황에 대한 기록을 저장하는 유일한 방법이기에, 시스템관리자와 보안 관리자는 어떠한 로그가 필요한지 어느 기간만큼 필요한 지, 정확하게 결정하여 필요한 데이터를 로그화하고 수집하여 분석하는 일이 중요하다. 그러므로 필요한 시스템 로그 데이터를 조직적이고 시기적절한 방법으로 수집하여야 하며, 그렇게 하기 위해서는 시스템별로 어떤 로그가 어떤 내용을 포함하고 있는 지, 그 로그 데이터는 어느 위치에 저장되는지 알아야 한다.

2.3 시스템 로그의 종류

본 논문에서 다루고자 하는 로그는 시스템 로그라는 용어가 더 정확한 의미이며, 시스템 로그는 시스템 운영체제의 로그, 보안장비 로그, 웹서버나 DBMS와 같은 시스템 소프트웨어의 로그, 서비스를 제공하는 애플리케이션 로그 등 아래 그림과 같이 수많은 종류가 있다 [3].

2.3.1 syslog

대다수의 통신장비와 보안장비에서의 로그 표준으로 syslog가 있다. syslog는 1980년에 Eric Allman이 BSD sendmail 프로젝트를 수행하면서 그 일부로 처음 개발되었고, 2001년에 시스코시스템즈의 C.Lonvick이 BSD syslog Protocol로 IETF Network Working Group에서

RFC 3164을 재정되어 널리 사용되다가[4], 최근 2009년 3월에 R.Gerhards에 의해 RFC 5424로 개정되었으며, 유닉스시스템과 그 유사한 운영체제 및 통신장비에서 일반화되어 표준 로그 프로토콜로 가장 널리 사용되고 있다[5].

2.3.2 유닉스/리눅스시스템 로그

유닉스와 리눅스 시스템에서는 운영체제의 활동기록 및 접속기록에 대한 다양한 로그를 생성하고 있다. 이러한 로그는 대부분 시스템내의 /var와 같은 특정 디렉토리에 서비스나 어플리케이션별로 로그를 생성한다. 로그 형태는 아래 표와 같이 종류별로 다양하며, 보관형태는 대부분 텍스트로 구성되어 있다. 유닉스는 대표적으로 HP의 HP-UX, IBM의 AIX, 썬마이크로시스템즈의 Solaris 등이 있으며, 리눅스계열로 BSD, 레드햇 등 여러 종류가 있으나, 대체로 다음과 같은 로그를 표준으로 제공하고 있다[6].

〔표 1〕 다양한 종류의 유닉스/리눅스 시스템 로그

로그 종류	로그 설명
syslog	unix 시스템에서 로그 메시지를 처리하기 위한 표준화된 인터페이스이며, 운영체제 종류에 관계없이 동일 사용
sulog	su 명령어 사용을 기록하여 누가 superuser가 되었는 지와 사용자간 권한 switch를 시도하여 성공과 실패한 내용을 조사
acct/pacct	사용자에 의해 실행된 프로세스 로그
authlog	syslog.conf에 의한 인증 로그 기록
messages	시스템의 부팅시와 부팅 이후의 전반적인 각 종 메시지에 대한 로그
loginlog	시스템에 접속하기 위한 로그인시 규정이상 인증 실패시 로그인 정보 기록
lastlog	사용자의 마지막 로그인 정보 저장
access_log	접속 요청 및 시도에 대한 로그
error_log	접속 요청 시 에러에 대한 로그 기록
historylog	사용한 명령어에 대한 이력 기록
dmesg	커널 ring 버퍼를 보거나 제어, 부팅될 당시에 보여주는 각종 메시지 저장
xferlog	ftp 접근에 대한 사용 로그
utmp	현재 로그인한 사용자 정보인 유저 접근 및 계정정보에 대한 내용 저장하며, w, who, whodo, users, finger 등을 사용하여 정보 출력
wtmp	유저 접근 및 계정 정보, 시스템 reboot 등에 대한 정보를 가지고 있으며, last 등의 명령어를 이용하여 내용을 확인, utmp와 wtmp는 binary format으로 특정 명령 확인
cron/log	crontab 명령어의 실패 및 성공과 cron 데몬에 의한 스케줄링 내용기록

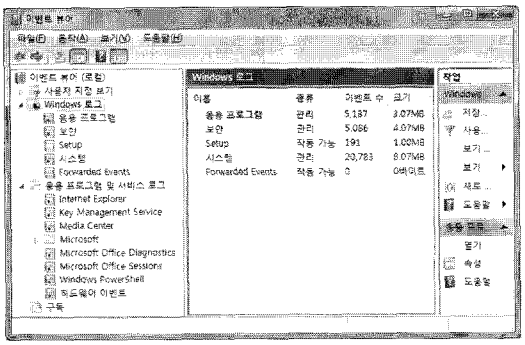
〔표 2〕 윈도우즈 로그의 종류

구분	특성
응용 프로그램 로그	윈도우즈 응용프로그램이 기록한 다양한 이벤트가 저장되며, 기록되는 이벤트는 소프트웨어 개발자에 의해 결정
보안 로그	유효하거나 유효하지 않은 로그온 시도 및 파일 생성, 열람, 삭제 등의 리소스 사용에 관련된 이벤트를 기록, 감사로그 설정을 통해 다양한 보안 이벤트를 저장 가능
시스템 로그	윈도우즈 시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드되지 않는 경우와 같이 구성요소의 오류 기록
디렉토리 서비스 로그	윈도우즈 액티브 디렉토리 서비스에서 발생하는 이벤트로 예를 들어, 서버와 글로벌 카탈로그 사이의 연결 무제 등을 기록
파일 복제 서비스 로그	윈도우즈 파일 복제 서비스에서 발생하는 이벤트로 예를 들어, 도메인 콘트롤러가 시스템 볼륨 변경 정보로 업데이트되고 있는 동안 발생하는 파일 복제 실패 등 기록
DNS서버 로그	윈도우즈 DNS서비스에서 발생하는 이벤트

2.3.3 윈도우즈 시스템 로그

마이크로소프트의 윈도우즈서버는 시스템, 보안, 응용프로그램 및 서비스 로그 등이 있다. 윈도우즈 서버의 로그는 syslog를 기본으로 제공하지 않으며, 독자적인 프로토콜을 채택하고 있으며, 이벤트뷰어를 통해 로그 검색이 가능하다.

〔그림 3〕 윈도우즈시스템의 로그들



Common 로그 형식

접근 로그의 전형적인 설정은 다음과 같다.

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

〔그림 4〕 아파치웹서버의 로그

2.3.4 웹서버 접속 로그

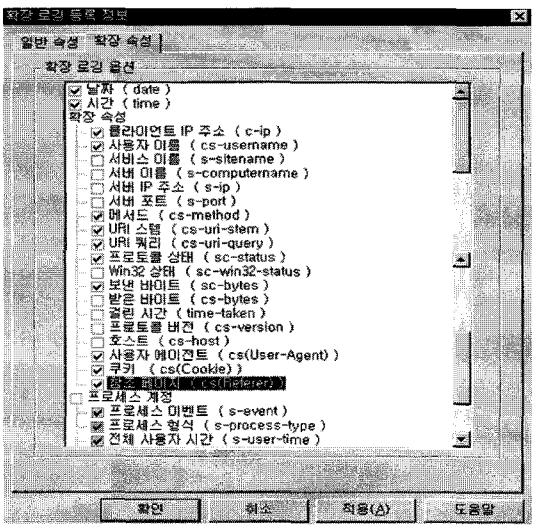
일반적으로 많이 사용하고 있는 웹서버로는 공개소프트웨어인 아파치 웹서버와 윈도우즈서버에서 기본으로 제공하고 있는 IIS 등이 있다.

먼저, 아파치 웹서버는 오류로그(Error log)와 접속로그(Access Log)가 있다. 오류로그는 존재하지 않는 페이지 접속시 403오류 등을 기록하며, 접속로그는 CustomLog로 로그 저장 위치와 LogFormat을 설정할 수 있다.

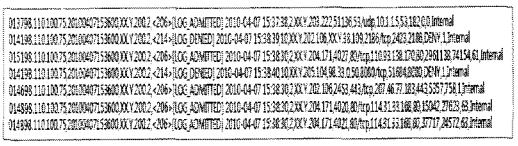
마이크로소프트의 웹서버인 IIS는 W3C 로그 포맷과 IIS확장 로깅 옵션이 있으며, 확장옵션에서는 사용자가 로깅할 항목을 선택하여 운용할 수 있는 편이성을 제공한다.

2.4 이기종 로그의 특성

시스템 로그의 종류를 살펴 본 것처럼, syslog는 표준으로 제정되었기 때문에 포맷은 일정한 형태를 가지고 있지만, 일반적인 운영체제와 통신 및 보안장비에서 생



〔그림 5〕 IIS의 로그 포맷으로 선택적으로 적용



〔그림 6〕 방화벽 장비의 로그 예제

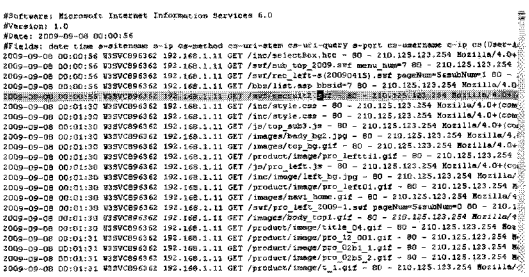
성하고 있는 로그들은 그 형태가 다르다.

syslog는 그 구성이 Header부와 메시지 부로 되어 있으며, 헤더부는 타임 스탬프와 호스트명 또는 IP주소를 포함하고 있으며, 메시지부는 메시지를 생성시킨 프로세스 이름인 Facility와 메시지의 중요도를 나타내는 Severity와 메시지 본문내용을 포함하고 있다.

위 [그림 6]은 방화벽장비에서 발생시킨 sysog 데이터의 샘플로 일반적인 syslog 표준 포맷을 따르고 있다.

W3C에서 정의한 웹서버 로그를 살펴보면 웹서버 버전정보, 생성일자, 시간, 생성 포맷, 접속자 IP주소, 사용자 계정, 웹서버 이름, 웹서버 IP주소, 서버 포트, HTTP 메소드, 요청 페이지, 요청 파라메터와 응답코드 그리고 마지막으로 사용자쿠키 정보를 기록하고 있다.

이렇게 장비와 운영체제에서 로그 포맷이 상이하여 호환성 문제가 생길 것을 우려하여 TTA에서는 국내 표준으로 보안장비에서의 로그 포맷을 표준화하였으나, 실제 장비를 제조하고 있는 업체에서 잘 지켜지지 않고



〔그림 7〕 웹서버의 접속 로그 예제

10.4 CIM_LogEntry

CIM_LogEntry represents the log entry within the log in the managed system.

Table 16 – Class: CIM_LogEntry

Elements	Requirement	Notes
InstanceID	Mandatory	Key
LogInstanceID	Optional	See section 7.1.1.
LogName	Optional	See section 7.1.2.
RecordID	Mandatory	None
CreationTimestamp	Mandatory	None
RecordData	Optional	See section 7.1.3.
RecordFormat	Optional	See section 7.1.4.
ElementName	Mandatory	The property shall match pattern ".*".

〔그림 8〕 TTA에서 정의한 로그데이터 항목

있다[7].

또 하나의 특징으로 로그 데이터가 대용량이라는 특성을 가지고 있다. 로그 데이터에 포함되는 내용이 대체로 행위자, 행위시간, 행위 대상, 행위내용을 포함하고 있으며, 세세한 행위가 일어난 대부분의 내용을 기록하기 때문에 발행하는 량이 매우 많게 된다. 지방자치단체 중 가장 큰 기관인 OO시의 경우 150여 대의 웹 서버와 30여 대의 보안장비에서 발생되는 로그는 일간 200GB가 되며, 초당 발생건수로 환산하면 10,000EPS(Event per Second)가 된다. 이렇게 대용량으로 로그가 발생하게 되면 로그 데이터를 보관하기 위한 저장 공간이 대용량으로 필요하게 되며, 사후에 로그를 검색하려할 때도 문제가 된다.

그러므로 시스템 로그 데이터를 다루는데는 다양한 형태의 로그와 대용량이라는 두 가지 특성을 고려하여야 하며, 관리자는 형태 측면에서 동일한 포맷으로 정형화와 대용량 측면에서 검색에 대한 속도를 높일 수 있는 방안을 찾아야 한다.

2.5 시스템 로그의 활용

시스템 로그는 일반적으로 알려진 웹로그를 통한 접속자 성향 분석으로 마케팅 자료로 활용하는 용도외에, 본 연구에서 관심사인 시스템의 실패 로그를 검색하여 원인 제거를 통한 운영의 안정성 확보와 침입 여부 및 취약점을 파악하여 조치하는 보안적인 측면에서의 활용성이 요구된다. 또한 각종 로그 데이터를 IT 컴플라이언스의 규정한 기간 동안 보관의 의무를 다하여 조직의 신뢰를 향상하고, 원본 로그를 훼손없이 보관하여 사건이 발생하였을 시에 근거로 제시할 수 있는 자료 확보의 이점이 있다.

〔표 3〕 이기종 로그의 특성

구분	특성
형태의 다양성	syslog, 웹로그, 시스템로그, DB로그 등 다양한 형태로 존재하며, syslog와 W3C 등 소수의 표준화된 포맷이 있으나, 모두 서로 상이하여 통합하기 어려움이 있음
대용량 로그	시스템마다 발생하는 매 행위를 기록하기에 한 사용자가 거쳐가는 노드마다 로그는 발생하며, 대체로 일일 수십GB씩 저장됨. 장기간 보관에 따른 대용량 저장 장치와 검색의 속도 문제가 있음

〔표 4〕 시스템 로그의 활용

구분	로그 데이터 활용
웹 로그	접속자의 성향 파악 및 구매 패턴 인지 웹 사이트 개선 방안으로 활용 마케팅 자료로 활용 불법 침입 및 서비스 거부 공격 파악
처리 로그	시스템에서 정상적인 처리결과 기록 정상적인 운영상태 확인
실패 로그	시스템의 운용 상태 파악 및 점검 시스템의 실패에 대한 원인 파악 및 조치 불법적인 해커의 침입 여부 및 경로 파악
감사 로그	로그 데이터 중에 미인가 객체에 대한 접근, 규정 횟수 이상의 로그온 실패, 정책에 대한 설정 변경 등 권한 및 보안 관리 활동
IT 컴플라이언스	규정에서 정의된 로그 데이터 수집 및 저장 명시된 보관기간동안 저장 규제 준수를 통한 조직의 신뢰도 향상
포렌식	사건 발생 시 수사 자료 및 근거 제시

〔표 5〕 로그 활용을 위한 검색 방법

구분	로그 데이터 활용
시간 기반 검색	특정 기간을 명시하여 해당 로그 데이터를 검색
사건 기반 검색	특정 키워드를 중심으로 해당 로그 데이터 검색

따라서 수집된 로그를 잘 활용하기 위해서는 분류와 검색이 중요하다. 분류는 여러 항목 중 발생시간, 대상, 행위자, 행위내용 등 필수적인 항목을 선별하고 정형화하는 일이 선행되어야 한다. 또한 용이한 검색을 위해서는 검색속도를 고려하여 저장방법을 결정해야 한다. 특히, 검색은 시간 기반의 검색과 사건 기반의 검색이 주로 이뤄지므로 시간대 별로 나눠서 저장될 필요가 있다. 대부분의 검색은 먼저 특정 기간을 선택하여 이뤄지기 때문에 대용량의 로그 데이터 중에 해당 기간 내의 데이터로 국한시켜서 검색을 해야 한다.

Ⅲ. 통합로그관리에 대한 기술적 요구사항

3.1 통합로그관리의 필요성

로그의 특성이 이기종과 대용량이라는 두 가지 특징을 가지고 있다는 것은 앞 II장에서 살펴보았다. 로그는 장비, 운영체제 그리고 어플리케이션까지 다양한 종류

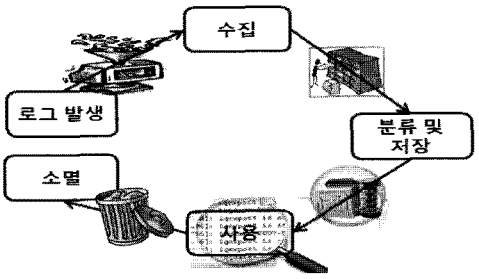
에서 만들어지며, 그 형태가 로그파일로 있을 때에는 파일에서 새로 추가된 내용을 에이전트를 통해 수집하거나, 주로 대부분 통신 메시지를 통해 수집되고 저장된다. 로그는 대부분 발생한 장치 내에 일정기간이나 일정한 저장용량의 크기로 제한되어 자체적으로 관리된다. 그러나 로그는 사후관리적인 측면이 많기에 필요한 시점에서 관련된 로그를 사용하고자 할 때에 정작 해당되는 로그는 삭제되어 없어질 때가 많으며, 그처럼 난감한 일도 없을 것이다. 바로 이러한 로그의 특성으로 인해 네트워크의 여러 장치에서 발생된 로그를 한곳으로 통합하여 저장 및 보관의 필요성이 대두되는 것이다.

또한, 다른 측면에서 보면 발생되는 로그가 대용량이라는 점이다. 특히 F/W이나 IDS/IPS와 같은 보안장비인 경우 접속되는 트래픽에 대한 거의 모든 로그를 남기기 때문에 1초에 수 만 로그를 발생시키고 있다는 것이다. 또한 해킹과 같은 침입에 대한 경로를 추적하기 위해서는 네트워크에 연결되어 수많은 장비의 로그를 한 곳으로 모아서 검색을 통한 분석 작업을 하기 위해서는 통합하여 수집하여야 하며, 당연히 대상 장비 수가 많아지게 되며 그러한 장비들에서 발생되는 로그는 대용량이 될 수밖에 없다.

3.2 통합로그관리의 생명주기

이기종 장치에서 발생되는 다양한 형태의 대용량 로그를 장기간 보관한다는 것은 고가의 대용량 저장 장치를 갖춰야 하기에 불필요한 예산 낭비일 수 있다. 각 조직마다 특성이 있지만 최소한의 IT 컴플라이언스에서 규정한 기간을 보관하여야 한다. 통합로그관리는 수집된 로그를 생명주기 기법을 통해 관리하게 된다. 생명주기 기법이란 말 그대로 발생된 로그를 수집하여 검색에 편리한 형태로 정형화하여 보관하고, 필요시에 검색을 통해 로그를 분석하게 되며, 보관기간이 경과될 경우 해당 로그를 삭제하여 로그 용량을 최적화하는 방법을 의미한다.

대부분의 로그가 텍스트형태인 점을 감안하여 보관할 때는 압축 기법을 사용하여 저장 공간을 효율적으로 사용해야 한다. 로그를 압축하여 저장할 때에 불편한 점이 있는데, 특정 로그를 찾아보고자 할 때, 검색을 위해서는 압축을 해제해야 한다는 점이다. 그러나 최근에는 검색기술이 발전하여 압축상태에서도 검색이 가능한 제품들이 있다. 그러면 압축해제를 위한 저장 장치와 시간을 절약할 수 있는 장점이 있다. 통합로그관리에 대한 생명주기를 발생에서부터 소멸까지 그림으로 이해하기 쉽게 표현하면 다음과 같다.



〔그림 9〕 통합로그의 생명주기 관리

3.3 통합로그관리를 위한 준비 사항

3.3.1 네트워크 요소 파악

조직이 갖추고 있는 IT인프라에 대해 총체적인 로그를 수집하기 위해서는 구성된 네트워크 요소를 파악하는 것이 선행되어야 한다. 라우터와 스위치 등 네트워크 장비, F/W, IDS/IPS 또는 VPN 등과 같은 보안장비, 서버시스템, 어플리케이션 및 DB가 그 대상이 되겠다.

3.3.2 수집 대상 선정

네트워크를 구성하고 열거된 장치들을 통틀어 네트워크 요소(NE)라 하고, 각 요소가 어느 노드에 연결되어 있는지 그 토폴로지를 파악하고 있어야 한다. 그래야만 대용량의 로그가 발생하였을 때 서비스 트래픽에 영향을 주지 않고 수집할 수 있도록 로그 수집장치를 설치할 위치를 고려할 수 있기 때문이다.

3.3.3 수집 장치 선정

그 다음은 로그 수집 장치를 선정해야 한다. 대부분의 로그는 표준인 syslog를 사용하고 있기에 syslog 데몬이 탑재된 프루브라고 하는 어플라이언스 형태의 장치를 통해 수집된다. 그 수집 장치에 대한 처리 성능과 수집해야 할 로그 발생량을 고려하여 수집 장치의 위치와 수량을 계산해야 한다. 수집 장치의 성능은 현재 발

생되는 로그량과 향 후 수년 내 증가될 로그 발생량을 함께 고려하여야 한다. 이는 한국정보통신기술협의에서 제정한 정보시스템 하드웨어 규모산정 지침 기준(TTAK.KO-10.0292)을 참조하면 적정한 용량을 산정할 수 있는데 도움이 된다. 또한 더불어 로그 수집장치에 대한 상태 모니터링 및 장애 시 대응할 관리정책을 수립하여야 한다[8].

3.3.4 로그 저장 장치 선정

로그가 수집되면 로그를 데이터로 저장하여야 하며, 원본 로그가 위변조에 의해 훼손이 없다는 것을 증명할 수 있도록 보관하여야 한다. 사후에 로그를 통해 침입이나 오남용에 대한 사후 증적자료로 채택될 수 있도록 하기 위해서이다. 원본 로그에 대한 저장 방식으로는 여러 방법이 있다. 암호화, ROM디스크가 있으며 최근에는 WORM(Write Once Read Many)디스크를 사용하는데 무엇보다 중요한 것은 저장장치에 대한 안정성과 도입 예산과 관련하여 선정되어야 한다.

HDD는 쓰고 읽기가 가능한 반면 원본로그 저장에 대해 해쉬 또는 암호화처리가 되어 있어야 하며, 생명주기 관리시에 용이한 측면이 있다. ROM인 경우에는 비용이 저렴하고, 이동성이 좋은 반면에 보관시 분실에 대한 우려가 많다. 또한 검색시 대용량을 지원하지 못한 관계로 불편함이 따른다. 이에 대한 대안이 WORM인데 비용이 고가이지만, ROM의 특성을 가지고 있고, 대용량을 지원한다는 점이 장점이다. WORM의 재활용을 위해서는 보관기간이 지난 로그 데이터를 H/W적인 접근으로 삭제하여 생명주기를 관리할 수 있는 Retain 기능이 필요하다.

로그의 저장 방식은 원본 로그를 그대로 저장하기에는 저장 용량에 따른 비용문제가 결부된다, 그러므로, 로그 저장 시에는 압축기법이 사용되며, 대부분의 로그 데이터가 텍스트 형태이기에, 압축을 하였을 때의 저장 용량은 크게 90% 이상의 효과를 볼 수 있다.

로그 저장 장치의 용량 산정은 앞서 언급한 TTAK.KO-10.0292를 참조하면 된다. 여기에는 향 후 수년간 증가와 작업 공간 및 백업용량이 함께 반영할 수 있으므로 용량부족이 발생하지 않도록 할 수 있으며, 또한 지나치게 많은 용량 산정으로 인해 예산을 낭비하는 일이 없도록 할 수 있다.

3.3.5 로그 분석

수많은 이기종의 로그 데이터가 대용량으로 저장되어 있을 때 필요한 로그를 검색하는 일은 매우 어려운 일이다. 그러므로 대용량 로그 검색에는 몇 가지 기술적인 접근이 필요하다. 로그가 대부분 용량문제로 인해 압축저장 형태로 되어 있음을 감안하여 검색하고자 할 때는 압축을 풀어야 하는 불편함이 발생한다. 그러나 최근의 검색 알고리즘은 압축상태에서도 검색가능한 기술이 개발되어 있으므로, 그러한 기술을 적용한다면 검색을 위한 압축해제의 불편함은 개선할 수 있다.

먼저, 특정한 사건의 로그 검색을 위해서는 시계열 분석이 필요하다. 로그가 발생하였던 시간을 인지하고 해당 기간에 저장된 로그를 선별하여 검색대상으로 삼는다. 두 번째는 사건을 인지할 수 있는 키워드를 선정하는 것이다. 가장 많이 쓰이는 것이 IP주소가 된다, IP주소는 행위자를 알 수 있으며, IP주소가 있는 항목을 지정하고 해당 IP주소를 검색하여 로그를 필터링하여 표본을 줄이도록 한다. 이렇게 필터링된 로그를 다시 시계열로 나눠 검색된 로그간의 관계를 분석하게 되며, 해당된 원본 로그에 대한 추출작업을 마치게 된다. 관리자는 해당 로그를 통해 취약점을 개선하거나, 사건 수사의 증적자료로 제시할 수 있다.

〔표 6〕 통합로그관리를 위한 준비사항

구분	준비 사항	비고
네트워크 요소 파악	- 네트워크 토폴로지 - 장치 구성정보(종류, O/S 버전 등) - 장비 수량	
로그 수집 대상 선정	- 수집해야 할 가치가 있는 장비를 선별 - 로그 발생 주기 및 량 조사 - 로그 분석의 가치 고려 - 컴플라이언스와 예산을 대비하여 로그 보관 기간과 용량 고려한 대상 선정 - 로그 수집 장치를 설치할 위치 고려	
로그 수집 장치	- 수집기 처리 성능(eps) 조사 - 설치 위치 및 수량 선정 - 관리 정책을 수립 향후 로그 발생량 증가 계획 포함 성능 산정	향후로그 발생량 증가 계획 포함 성능 산정
저장 장치	- HDD 디스크, ROM, WORM - 사용의 편리성 측면 고려 - 비용과 용량과의 상관관계를 고려	
로그 분석	- 관련 항목 연관 분석 - 시계열 분석 - 원본로그 추출 - 로그 통계 보고	

Ⅳ. IT컴플라이언스와 통합로그관리

IT와 관련된 각종 컴플라이언스들은 전자적 기록물을 포함하여 보관하고, 책임지도록 하며, 사용을 위한 접근기록까지 보관하도록 명시하고 있다. 그러한 기록을 로그라고 할 수 있으며, 정보시스템을 이용한 로그관리는 여러 측면에서 정부 및 공공기관과 기업조직에 많은 이득을 제공하고 있다.

〔표 7〕 로그 관련 각종 국내외 IT 컴플라이언스

구분	내용	비고
공공기관의 개인정보보호에 관한 법률	개인정보 이용에 대한 로그 필요성 명시	한국
정보통신망 이용촉진 및 정보보호 등에 관한 법률	개인정보 이용 및 제공에 대한 로그 필요성 명시	한국
공공기관 정보시스템 운영가이드라인	주요 정보시스템 및 정보보호시스템에 대한 로그 보관 및 분석지침을 수립하고, 로그는 최소 6개월 이상 보관명시	NIA (한국)
행정기관 정보시스템 접근권한관리 규정	정보시스템 이용 내역 및 기록의 보관 내용 명시	(총리훈령 제526호)
전자금융감독규정 시행세칙	이용자정보 조회시 자동기록 및 1년이상 보존 명시	한국
개인정보의 기술적·관리적 보호조치 기준	정보통신서비스 제공자는 접속기록 저장 및 월 1회 이상 확인·감독, 접속기록 위변조 방지 및 백업 보관	한국
ISO 27001	감사로깅, 로깅정보의 보호, 관리자/운용자 로그, 시간 동기화 명시	국제표준
Sarbane-Oxley Act(SOA)	회계감사의 투명성과 내부통제강화 보고서 공시규정 로그 데이터 5년 보관명시	GAO, SEC
HIPPA	병원이나 의료관련기관에 보관되어 있는 의료기록 및 건강 정보에 대한 자료관리 규제, 로그 데이터 6년 보관명시	DoHH (미국)
GLBA	금융기관이 고객의 개인 정보에 대한 안전조치강제 로그 데이터 6년 보관명시	FDIC, SEC (미국)
BaselII	은행의 위험관리 규제 로그 데이터 7년 보관명시	BIS (국제기구)
USA PATRIOT Act 2001	9.11테러에 대응해 금융,보험회사의 고객 식별 및 수상한 거래 기록 보고	DoD (미국)
Califonia SB 1386	컴퓨터 보안사고 공표 강제	Califonia State Gov. (미국)

로그는 적절한 기간 동안 컴퓨터 보안 기록이 충분하며 훼손되지 않고 보관되어 있음을 보장하여 컴플라이언스를 준수할 수 있으며, 이를 통해 기관의 신뢰를 향상시키는데 기여하며,

둘째로, 로그를 정기적으로 검토하고 분석하여 보안사고, 정책 위반, 악의적 활동, 운영적인 결함을 바로 식별이 가능하며,

셋째로, 외부로 침입하여 들어온 불법 접속 및 내부의 중요 기밀정보 유출 등 각 종 보안 사고를 해결하는데 유용한 정보를 로그를 통해 제공할 수 있으며,

넷째로, 감사와 포렌식 분석을 수행하여 조직의 내부조사를 지원하며, 그 baseline을 준비할 수 있으며[9],

다섯째로, 운영 경향과 장기적인 문제점을 들을 확인하도록 도움을 준다.

이러한 이점을 때문에, 여러 컴플라이언스들이 특정 로그들을 저장하고 재검토하도록 규정하고 있으며, 다음과 같은 국내외의 규정들을 찾아 볼 수 있다[10].

Ⅴ. 결 론

본 논문에서 살펴 본 바와 같이 로그는 매우 중요한 정보자산임에도 불구하고, 그 가치를 인정받지 못하여 잘 관리되고 있지 않았었다. 그러나 로그를 통해 안정적인 시스템을 유지하고 개선하며, 보안강화를 위한 중요한 근거자료가 되며, 각종 IT규제 준수에 대한 IT위상을 높일 수 있을 것으로 기대된다.

본 논문에서 제시한 이기종의 다양한 로그를 통합하여 관리할 수 있는 가이드라인에 따라 로그의 생성에서부터 사용과 소멸에 이르기까지 생명주기를 관리할 수 있는 참고 자료로 활용할 수 있다. 또한 원본 로그가 훼손 없이 잘 보관되는 경우 침해사고와 같은 경우 사건수사에 참고할 수 있는 근거 자료로 제시가 가능하여 유리한 측면이 있다. 특히, 개인정보를 다루고 있는 공공 및 민간기관 등에서 로그를 통한 개인정보 보호에 주의를 기울인다면 OECD에서 요구하고 있는 개인정보보호에 대한 가이드라인을 준수하게 되어 국가의 위상이 높아질 것으로 기대된다.

본 연구에서 다루지 못하였던 로그표준화에 대한 부분으로 효율적인 로그분석 시스템 구축 프레임워크, 구축 사례를 통한 로그분석 시스템 특징 및 효과성 분석은 본 연구를 확장하여 발전시킬 필요가 있다.

참 고 문 헌

[1] 보안뉴스, "中해커, 'N포탈 1200만명 고객DB' 판매 시도", http://www.boannews.com

[2] 한국정보보호진흥원, "개인정보보호를 위한 DB 보안감사로그 표준화 연구", KISA, p9, 2008

[3] Karen kent, Murugiah Souppaya, "Guide to Computer Security Log Management", NIST SP 800-92, pp. ES-1~ES-3, 2006

[4] RFC 3164, The BSD Syslog Protocol, IETF Working Group, pp10-11, 2001

[5] RFC 5424, The BSD Syslog Protocol, IETF Working Group, p8, 2009

[6] 안정철, "시스템 로그 분석", 이비컴, pp38~39, 2005

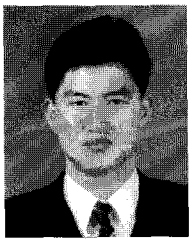
[7] TTA.OT-10.0164, "분산시스템 자원대상 레코드로그관리 항목 프로파일", 한국정보통신기술협회, p21, 2009

[8] 한국정보통신 기술협회, "정보시스템 하드웨어 규모산정 지침기준(TTAK.K0-01.0292), 2008, http://sizing.nia.or.kr

[9] SANS, "SANS Annual 2009 Log Management Survey", pp. 14~16, 2009

[10] 한국정보보호진흥원, "개인정보보호를 위한 DB 보안감사로그 표준화 연구", KISA, p12~31, 2008

〈著者紹介〉



김 완 집 (Wan Jib, Kim)
정회원

1991년 2월 : 숭실대학교 전기공학과 졸업
2005년 9월 : 성균관대학교 정보통신대학원 석사
2008년 9월~현재 : 순천향대학교 정보보호학과 박사과정
관심분야 : 정보보호정책, 디지털포렌식, 융합보안, IT기반시설 통합보안

염 흥 열 (Heung-Youl Youm)
종신회원

1981년 2월: 한양대학교 전자공학과 졸업
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원(역), 수석부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜