다중이용 웹서버 하에서의 보안운영체제 개선을 위한 로그관리 통제시스템 강화 방안 연구

김예중*
*고려대학교 컴퓨터 과학기술대학원 디지털공학과“
metro@21metro.co.kr

A Study on the strengthening Log Management Control System For Improving Secure Operating System Under Multi-using Web-server

Ye Joong Kim*
Dept. of Digital Information Engineering, Korea University

요 약

본 논문은 웹 서버에 저장되어 있는 로그관리 시스템을 이용하여 방문자들의 방문 기록을 관리하는 로그관리 시스템을 구현하였는데 첫째, 사용자 로그인 표시에 사용자 정보와 패스워드를 입력하고 서버에 접속하여 사용자를 확인하는 절차를 적용하였다. 둘째, 개인 정보보호 같은 취약점을 보완하기 위하여 클라이언트의 웹 브라우저에 포함된 로그관리시스템을 사용함으로써 서버와 안전한 사용자 로그인을 위한 채널을 생성하도록 하였다. 셋째, 사이트 접속 에러 분석시 웹사이트 관리할 때 방문자들이 불편함을 느끼지 않고 사이트에서 필요한 정보를 빠르고 쉽게 찾을 수 있도록 제공해 주고 허가된 비인가자의 접근 체크 기능을 부여하였다.

1. 서론

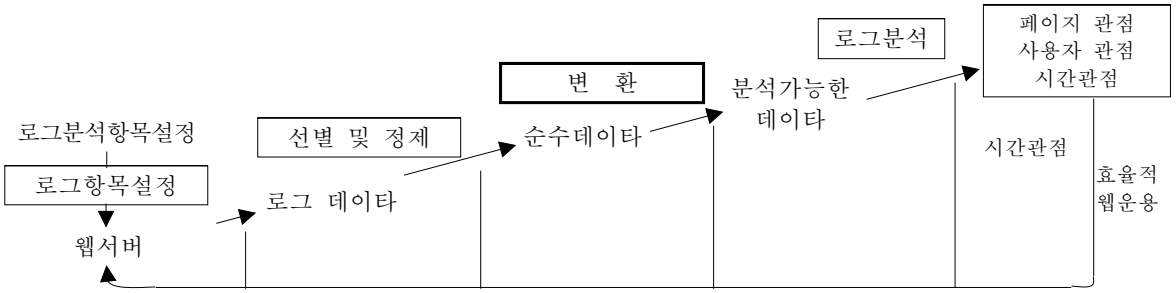
인터넷을 통한 정보공유 및 개인 신상정보의 교환 등이 활발히 이루어지고 있다. 네트워크 발달 및 전자상거래의 활성화는 사람들로 하여금 자신의 신상정보를 웹상에 싫든 좋든 다양한 거래로 노출시키게 하도록 요구하고 있다.[1]

기존의 인증 LOG관리 시스템 특징 및 문제점으로[2] ① 허가된 자, 비인가자의 접근체크 기능만 부여함으로서 ID 및 비밀번호 일치시 인가자로 인식케 되는 점과 ② 인가된자의 단순 자료처리 범위의 부여로 인가된 업무분야에 한정된 원시적 접근제한과 ③ 개인정보 원부 이용에 대한 내부통제 기능 미흡으로 인가된자의 개인정보 열람 및 무단 정보유출시 무단유출자에 대한 역추적에 한계를 갖는다. ④ 그 밖에 전산환경의 기술변화에 대응한 데이터웨어하우스 등 IT기술도입, 분산화일의 통합관리가 필요하고 외부침입(일반적 통제) 대비 강화 및 애플리케이션 통제 소홀에 따른 대응이 미비한 한계를 노정시키고 있다.[3][4]

본 연구에서는 현행 웹기반에서의 로그관리시스템을 확대 적용하여 개인정보조회의 로그 및 통계자료 활용과 액셀자료 등 대량자료에 대한 명부출력에 대해 로그의 자료가 축적이 가능케함으로써 대량고객에서의 개인정보 출력조회시 로그관리로 인한 통제나 보안관리가 가능케 함으로써 사용통제와 개인정보 노출시 축적된 로그자료를 바탕으로 신속한 조회 및 확인이 가능케 하는 시스템을 제안하는 데 목적을 둔다.

2. 개인정보보호를 위한 로그관리 시스템에 대한 고찰

2-1. 웹로그관리시스템 분석



자료 : 아이비즈넷(주), 인터넷 비즈니스 @i-biznet.com: 비즈니스 모델링에서 마케팅까지, 21세기 북스, 2000.6.

(그림 1) 웹 로그 분석 과정

<표 1> 웹 로그분석의 항목 및 분야

웹트래킹 측정단위	내 용
히트(Hits)	방문자가 웹사이트 접속시 그 안에 포함된 그래픽, HTML 등의 모든 파일 계산단위를 말한다.
페이지뷰 (Page View)	웹사이트 평가시 단위기준으로 가장 많이 사용하는 것으로 하나의 배너광고가 포함된 HTML 문서가 전송되어 사용자가 페이지에 접촉될 때 광고에 노출된 것으로 간주한다.
세션(Session)	방문자가 특정 사이트에 접속 연속적으로 페이지를 본 후 다른 사이트로 이동하는 과정을 하나의 방문으로 기록하는 것을 말한다.
방문자(Visitor)	특정 웹사이트를 한번이상 접속한 사용자들의 수를 파악하는 방법으로 쿠키나 사용자인증을 통해 방문자의 방문경로 및 웹사이트 방문형태를 분석하여 웹사이트의 컨텐츠 관리 및 전략수립에 이용된다.
래퍼럴 로그 (Referer log)	방문자가 어디를 통해서 사이트에 방문했는지 또는 검색엔진에서 어떤 키워드로 접속했는지의 정보를 알 수 있어 배너광고 효과를 파악하고 광고정책을 세우는 핵심자료가 된다.
에이전트 로그 (Agent log)	사이트를 접속하는 방문자의 웹브라우저 타입 및 버전OS(Operating System) 종류, 화면해상도, 어플리케이션 프로그램 등에 관한 정보를 제공해 최적화된 웹사이트를 구성할 수 있는 단서를 제공한다.
어세스 로그 (Access log)	클라이언트의 도메인주소나 IP, 일자, 송수신 속도, 요청 항목 등의 표준로그파일 형식을 말한다.
에러 로그 (Error Log)	웹서버의 오작동에 대한 모든 정보를 포함하고 있다. 에러로그가 30% 이상 넘어서면 사이트 신뢰성에 치명적이기 때문에 에러로그를 참조하여 주기적인 사이트 점검 및 수정보완을 해 주어야 한다.

3. 시스템 설계 구현 방법

3-1. 시스템 설계 기본 목표

첫째, 허가(인가)자의 접근체크 기능외 어플리케이션 통제 강화

둘째, 전산 환경의 기술변화에 대응한 새롭게 요구되는 기능에 맞게 신기술을 채용과 데이터웨어하우스 등 IT기술도입과 분산화일의 통합관리

셋째, 열람통제 유형에 따른 기능보완 측면에서 단말기상의 개인정보 조회 기능 구축

3-2. 보안 강화를 위한 로그관리시스템 설계

로그관리시스템 구축을 위해 먼저 Linux 시스템의 채택과 이 시스템을 이용한 기본 보안관리의 기본인 로그통계/현황 DB 구축과 동시에 로그자료 추출 및 수록을 위한 시스템을 구축한다. 그리고 세부정보 입력을 위한 자바 프로그램의 수정을 통하여 로그 통계용 관리자 전용 조회 프로그램의 작성과 함께 권한별 메뉴사용 현황 자료추출 및 타 지역 조회현황 조회 프로그램을 작성케 하는 연동시스템을 구축한다.

3-3. 서버에서 개인정보의 대량 명부출력 관리를 위한 로그관리시스템 구현 설계

(1) 세부추진사항

개인정보 명부출력 자바프로그램의 수정을 통해

개인정보 명부출력 통제와 명부출력 로그를 위한 자바 프로그램 수정을 통해 기능을 보강하고, 서버에서 로그시스템으로 전송된 개인정보 출력 리스트 로그자료를 로그통계/현황 데이터베이스 및 테이블에 적재케 하여 정상적으로 데이터 구축여부를 확인케 하였다.

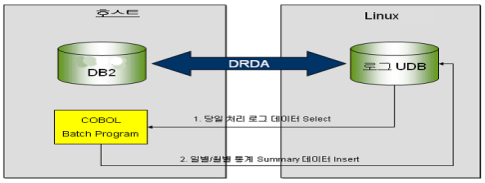
(2) 평가 및 검증

통합된 로그자료의 체계적인 관리 및 활용체제의 구축을 통해 기간별, 사용자별 통계현황 추출 가능토록 설계하여 출력을 통해 오류체크와 권한관리와 연계된 자료 활용 가능토록 설계된 내용대로 기능별 시스템 작동결과를 평가 검증하였다.

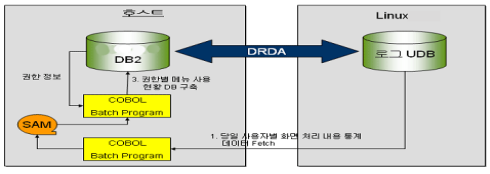
4. 연구결과 로그관리시스템 구현

4-1. 로그관리시스템 구현

로그관리 시스템구축에 있어 Linux 시스템 구축시 Host용 프로그램 신규작성과 동시에 로그통계/현황 DB구축을 하고, DB Table 관리용 배치 프로그램의 신규작성하여 배치 및 통계 DB용 배치 프로그램신규작성을 통해 로그통제기능을 강화시켰다.



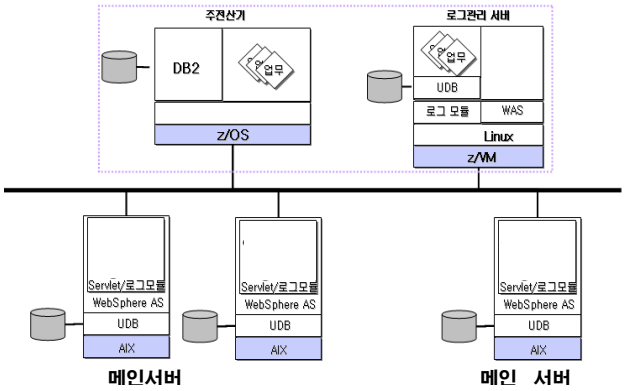
(그림 2) 각종 로그 통계 DB구축



(그림 3) 권한별 메뉴 사용 현황 DB구축

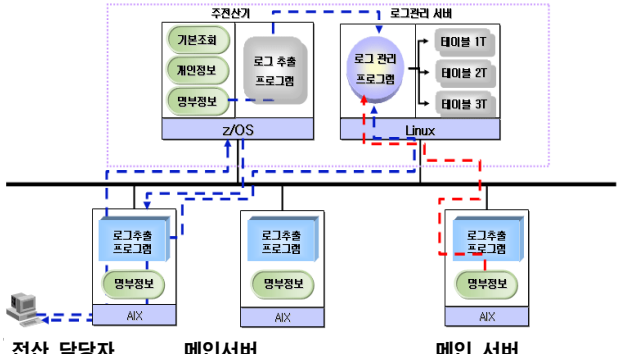
4-2. 로그관리시스템 상세 구현도

호스트환경에서 개인정보의 대량명부출력 로그관리에 있어 먼저 표준수정은 코볼 프로그램의 수정을 통해 보강하고 프로그램 수정은 단발성(1:1) 개인정보 및 기타 프로그램 수정과 다량의 리스트성 프로그램수정을 통해 보강하였다.



(그림 4) 로그시스템 상세도

테이블의 신규 생성에 있어 ① 일일로그테이블의 경우 LD001T(전체 트랜잭션), LD002T(개인정보(1:1) 내용), LD003T(명부성 개인정보(1:다수)내용) ② 기간로그테이블에서는 LD005T(전체 트랜잭션), LD006T(개인정보(1:1) 내용), LD007T(명부성 개인정보(1:다수) 내용) ③ 임시 테이블에서도 LD051T, LD052T, LD053T(LD005T, LD006T, LD007T 테이블로 데이터 load시 사용) ④ 사용자 관리 테이블은 LDJOBS(배치작업 현황 테이블), LD011T(사용자 관리 테이블), LD013T(로그통계 VIEWER 이력 테이블)를 생성하였다.



(그림 5) Linux 로그시스템 업무 구성도

4-3. 로그관리시스템 프로그램 수정평가 및 개선결과

시스템 설계에 있어 기존의 인증 LOG관리 시스템을 개인정보보호측면에서 조회 및 출력 프로그램에서만 보호기능을 적용해 오던 시스템 문제를 중점 설계시 반영한 내역은 다음과 같다.

첫째, 기존 시스템은 허가된 자, 비인가자의 접근체크 기능만 부여하여 ID 및 비밀번호 일치시 인가자로만 인식하는 제한된 기능으로 다양한 보호 욕구 방지에 한계를 드러냈다. 그리고 시스템 접근에 인

가된 업무분야에 한정된 원시적인 접근제한으로 운영에 원활한 효율을 기대할 수 없었다.

둘째, 개인정보 원부 이용에 대한 내부통제 기능의 미흡으로 무단유출자에 대한 역추적의 한계를 드러내 원인규명이 어려웠다.

셋째, 전산환경의 기술변화에 대응한 기존 탄력적인 시스템의 업그레이드 미비로 데이터웨어하우스 등 IT 기술도입과 분산화일의 통합관리가 필요했고, 외부침입(일반적 통제)에 대비에 대한 애플리케이션 통제 소홀로 개인정보사용의 다양한 이용환경에 탄력적인 대응이 지체되어 왔다.

넷째, 업무의 개인정보 열람을 통제하기 위한 부서장 점검기능으로서 가입자의 열람내역을 일일이 점검 실시와 구체적인 열람사유 및 근거 등 확인을 통해 불필요한 열람을 방지하고 개인정보 열람 시 열람사유를 등록해야하는 불편을 가져왔다.

다섯째, 그밖에 업무보조 인력에게 제공된 각종 개인정보자료가 퇴근 시 회수되지 않고 업무보조 인력의 무단 사용과 PC와 프린터의 연결을 차단하지 못하여 개인정보 조회내용이 외부로 유출되는 사례가 빈번하였다.

따라서 이러한 문제해결을 위해 보안인증시스템을 도입하여 기능을 보강하였는데 이를 세분화시켜 보면 크게 네가지로 요약될 수 있다.

첫째, 시스템설계 결과허가(인가)자의 접근체크 기능보완을 통해 어플리케이션을 통제 강화하였고, 새롭게 요구되는 기능에 맞게 신기술의 채용과 데이터웨어하우스 등 IT기술을 도입하여 신 분산화일의 통합관리가 가능케 구현하였다. 또한 열람통제유형에 따른 기능보완 측면에서 단말기상의 개인정보조회기능도 함께 구축하였다.

둘째, 보안강화측면에서 개인정보명부출력의 자바프로그램의 수정을 통해 개인정보명부출력의 통제와 로그기능을 보강하고, 서버에서 로그시스템으로 전송된 개인정보 출력리스트 로그자료를 로그통계/현황 데이터베이스 및 테이블에 적재케 하여 정상적으로 데이터 구축여부를 확인할 수 있도록 하였다.

셋째, 허가(인가)된 자의 접근체크 기능외 어플리케이션 통제강화기능을 부여하여 ID 및 비밀번호 일치시 인가자료 인식케 함과 동시 열람시 열람목적에 따른 D/B를 생성시켜 인가된 자의 접속일지라도 접근 체크기능을 이중으로 강화시켰다.

넷째, 전산환경의 기술변화에 대응하기 위해 데이터웨어하우스등 IT신기술도입으로 분산화일의 통합관리가 되도록 개인PC까지 통합되었으며, 외부의 무단침입(일반적 통제)강화에 따른 내부적 애플리케이션(조회-열람)에도 통제시스템을 구축시켜 매기록 저장과 함께 인증강화로 기존의 무작의 조회열람에서 벗어나 단계별 통제인증으로 보완을 강화하였다.

Ⅴ. 결 론

본 연구는 이러한 요구에 부응하기 위하여 웹서버에 저장되어 있는 로그관리 시스템을 이용하여 방문자들의 방문기록을 관리하는 로그관리 시스템을 구현하였는데 그 결과를 보면 다음과 같다.

첫째, 온라인상에서 일단 노출된 개인정보는 원상복구가 곤란할 뿐만 아니라 언제, 어느 단계에서, 누구에 의해 개인정보가 누출되었는지를 확인하기가 어렵기 때문에 사용자로그인 표시에 사용자정보와 패스워드를 입력하고 서버에 접속하여 사용자를 확인하는 절차를 적용하여 개인정보의 보호를 적극적으로 보호하고 누출이나 무단침입으로부터 보호하기 위한 메커니즘을 적용하였다.

둘째, 개인정보보호 같은 취약점을 보안하기 위하여 클라이언트의 웹브라우저에 포함된 로그관리시스템을 사용함으로써 서버와 안전한 사용자로그인을 위한 채널을 생성하여 클라이언트와 서버 사이에 상호인증을 수행함과 동시에 사용자 인증 및 암호화된 메시지를 전송함으로써 인터넷 사용자 로그인에게 발생할 수 있는 취약점을 해결하였다.

셋째, 사이트 접속 에러 분석시 웹사이트 관리할 때 방문자들이 불편함을 느끼지 않고 사이트에서 필요한 정보를 빠르고 쉽게 찾을 수 있도록 제공해 주고 허가된 비인가자의 접근 체크기능여부로 원시적 접근제한과 무단정보유출시 역추적으로 개인 정보유출억제와 외부침입에 대한 애플리케이션 통제강화로 보안 미비한계를 강화하였다.

참고문헌

[1] 법제처 “공공기관의 개인정보보호에 관한 법률/정보통신망 이용촉진 및 정보보호 등에 관한 법률”

[2] 행정자치부 “공공기관의 개인정보화일목록집” 2002.12

[3] 김강 외 “정보시스템보안을 위한 위험분석모델” 한국 OA학회논문지 제7권 제3호 2002

[4] 이경호, 임종인 “전자정보와 정보보호 : 전자정부와 프라이버시” 한국정보보호학회지 제13권 제3호 2003