S/W 개발 분석 단계에서 감사 로깅

신성윤* · 진동수*** · 신광성* · 이현창** · 이양원*

*군산대학교 컴퓨터정보공학과

**원광대학교 정보전자상거래학부(융복합창의연구소)

***경인여자대학교 경영과

Legal System and Regulation Analysis by S/W Development Security

Seong-Yoon Shin* · Dong-Soo Jin*** · Kwong-Seong Shin* · Hyun-Chang Lee** · Yang-Won Lee*

*Dept. of Computer Information Engineering, Kunsan National University

**Div. Of Information and Electronic Commerce(Institute of Convergence and Creativity)
Wonkwang University

***Dept. of Business Administration, Kyung-In Woman's University

E-mail : {s397220, waver, ywrhee}@kunsan.ac.kr, hclglory@wku.ac.kr, dsjin777@kiwu.ac.kr

Acknowledgement : "This research is partially supported by Institute of Information and Telecommunication Technology of KNU"

요 약

본 논문에서는 감사 로그에서 부인 방지를 위해 모든 전자 금융 거래 관련 내역은 로깅 및 보관되어야 한다는 것도 제시한다. 그리고 어플리케이션 접속로그 및 중요 정보에 대한 조회 및 사용 내역은 로깅 및 검토되어야 한다는 것도 제시하도록 한다.

ABSTRACT

This paper suggests that all history related to electronic financial transactions should be logged and kept. And, it should be considered to check the details of application access log and major information.

키워드

감사로그(Audit Log), 접속 로그(Access Log), 중요 정보(Major Information)

Ⅰ. 서 론

감사 로깅 시스템은 사용자의 활동, 예외사항, 정보보안사건을 기록하는 감사로그를 생성하여야 하며 추후 조사와 접근통제 감시 지원을 위해 합의한 기간 동안 보존하여야 한다[1].

감사 로깅 시스템은 시스템 사용 내역과 통신망을 통한 접근 내역을 기록하는데, 이 내역은 불법적인 시스템 자원의 사용이나 통신망을 통한 불법 접근이 발생하였을 때, 그 경로를 추적하는 자료로 사용된다[2]고 하였다.

Ⅱ. 감사로깅

1. 감사 로깅의 원칙

시스템의 보안 수준을 유지하고, 법적인 규제 사항을 만족시키며, 악의적인 침해 행위나 내부 정보의 유출 행위를 감시하기 위해 필요한 모든 정보들은 저장되어야 하며 안전하게 관리되고 주

기적으로 검토가 가능한 형태로 레포트가 생성되어야 한다.

2. 어플리케이션 로그 생성 기준 정의

시스템에서 수행되는 거래들 중 전자 금융 시행 세칙, 전자상거래법, 정보 통신망 법, 상법 등에서 강제하는 거래 로그에 대해서 그 종류와 형태별로 정의한다. 어플리케이션 로그 생성 기준을 정의한 예는 그림 1와 같다.

업무 유형	대상정보
거래 직접 내용	거래종류
	거래금액 및 거래 수수료,거래 일시, 당사자 정보
	전자적 장치 종류
	전자적 장치 식별 정보
	거래계좌의 명칭 또는 번호
	해당 거래 관련 전자적 장치 접속 기록
	전자지급수단별 거래 승인 기록
거래 관련 정보	접속 일시 및 접속 종료 일시
	접속 실패 회수(연속) 및 접속 실패 사유
	거래 실패 회수(연속) 및 거래 실패 사유
요청 및 처리 사항	오류정정 요구사실 및 처리결과에 대한 사항
	전자금융거래의 신청 및 조건의 변경에 대한 사항
이용 및 관리 기록	정보시스템 가동기록
	이용자정보 조회기록
	중요 원장 사용기록

그림 1. 어플리케이션 로그 생성 기준(예시)

3. IT 인프라 로그 생성 기준 정의

시스템의 IT 인프라에서 내부 정보 유출 및 시스템 침해 시도 탐지를 위해서 저장이 필요한 로그에 대해서 정의한다. 그림 2는 IT 인프라 로그 생성 기준의 예시를 나타낸 것이다.

인프라	영역	로그
서버	인증	로그인 성공/실패
	계정	사용자/그룹 계정 생성,삭제,변경
	권한	권한의 생성,변경,삭제
	침해시도	프로세스 생성,변경,정지,삭제 시도(성공/실패)
데이터베이스	인증	로그인 성공/실패
	계정	사용자/그룹 계정 생성,삭제,변경
	권한	권한의 생성,변경,삭제
	정보작업	SQL DML, DDL, DCL 작업 구문 및 리턴데이터
네트워크장비	인증	로그인 성공/실패

그림 2. IT 인프라 로그 생성 기준(예시)

4. 감사 로깅의 기준 정의

정의된 생성 로그에 대해서 내부적 보안 요건이나 외부적 법적 요건 및 내부적 감사 역량을 고려하여, 로그에 대한 정기적 감사 실행 여부를 결정한다.

인프라	로그	정기 감사	실시간 모니터링
어플리케이션	전자금융 거래로그	-	-
서버	로그인 성공/실패	주간 감사 레포트	-
	업무 프로세스 중지 시도	주간 감사 레포트	실시간 SMS 경보
데이터베이스	로그인 성공/실패	주간 감사 레포트	-
	SQL DML, DDL, DCL 실행명령	주간 감사 레포트	-
네트워크장비	로그인 성공/실패	월간 감사 레포트	-

그림 3. 감사 로깅 기준 정의(예시)

III. 결론

감사로그에서 부인 방지를 위해 모든 전자 금융 거래 관련 내역은 로깅 및 보관되어야 한다는 것과 어플리케이션 접속로그 및 중요 정보에 대한 조회 및 사용 내역은 반드시 로깅 및 검토되어야 한다는 것 또한 제시하였다.

참고문헌

[1] http://cafe.naver.com/softwarequality/book1621832/7 31

[2] Kim Min Soo, Noh Bong Nam, “Information Security : Secure logging system with self-protecting function,” The Transactions of the Korea Information Processing Society , Vol. 6, No. 9, pp. 2442-2450, 1999