S/W 개발 분석 단계에서 접근 통제

신성윤* · 진동수*** · 신광성* · 이현창**

*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**

*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}@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 업무수행자인 사용자의 역할과 데이터 사용행위를 기반으로 한 접근 및 권한 통제가 이루어져야 한다는 점을 강조한다. 조직의 운명을 좌우하는 매우 중요한 정보의 대량 조회 및 변경 작업은 반드시 사전 결재를 취득해야 가능하다는 점도 제시한다.

ABSTRACT

This paper emphasizes the control of access and authorization based on the roles and the data using activities of users as task performers. Also, it requires to gain the necessary approval in advance for important tasks such as mass inquiry and change on important information to influence the very existence of the whole organization.

키워드

접근 통제(Access Control), 권한 통제(Authority Control), 조회 및 변경(Inquiry and Change)

Ⅰ. 서 론

접근 통제란 시스템과 네트워크 자원에 시도되는 허가되지 않은 접근에 대응하기 위한 첫 번째 방어수단 중 하나로서 접근을 승인하거나 거부함으로써 비 인가자에게 불법적인 자원 접근 및 파괴를 예방하는 하드웨어적, 소프트웨어적, 그리고 행정적인 관리를 말한다[1].

접근 통제 관련 연구로는, [2]에서는 기존의 DBMS 접근 통제 시스템의 구현 방식과 기능 연구, 한계점 분석, 개선방안 도출을 통해 개인정보 보호법을 준수할 수 있는 효과적인 DB의 보안 접근 통제 시스템을 제시하였다. [3]에서는 의료정보 유출 방지를 위하여, 현행 네트워크 접근 통제 시스템을 개선 및 적용한 네트워크 이중 접근 통제 모델을 제시하였고, [4]에서는 접근 통제의 전반에 관한 것을 다룬 IHE(Integrating the Healthcare Enterprise)의 IT 인프라 기술 프레임

워크 백서를 발간하여 접근 통제의 기반을 다졌다.

II. 접근통제의 원칙

국제 표준화 위원회에서 제시한 원칙에 따라서 우리는 다음과 같이 접근 통제의 원칙을 설정하였다.

첫째, 시스템의 사용은 명확히 설계된 권한에 의해서 제한 되어야한다는 것이다.

둘째, 시스템 사용을 위한 주체, 객체, 행위가 정의되고 식별되어야 한다는 것이다.

셋째, 사전에 합의된 접근 제어 룰에 의해서 접근 및 사용이 통제되어야 한다는 것이다.

III. 접근통제를 위한 정의

정보 보호의 3가지 정의인 기밀성, 무결성, 가용성에 대하여 다음과 같이 정의할 수 있다.

첫째, 기밀성(Confidentiality)이란 정보의 비밀이 누설되지 않고 지속적으로 유지되는 것을 말한다. 이는 반드시 허가된 객체에게만 정보가 제공되어야하며, 비인가된 객체로부터는 완벽히 차단 통제되어야 한다. 일반적으로 접근통제와 암호화를 통해 차단이 통제된다.

둘째, 무결성(Integrity)이란 허가되지 않는 객체으로 부터 정보의 위변조 및 삭제 등을 막는 것을 뜻한다. 이는 정보의 정확한 전달과 안정을 보장하는 것이다.

셋째, 가용성(Availability)이란 서비스가 계속 유지가 되어 허가된 객체에게 정보가 제공되는 것을 의미한다. 이는 혹시 모를 공격에 대비하여 정보를 백업시키거나 의심스러운 위험 요소로부터의 보호를 통해 보장된다.

정보 보호를 위한 3가지 정의를 우리는 보안의 3요소라고 한다.

IV. S/W 접근통제

S/W 접근통제란 IT 인프라 접근통제와 같은 말이다. IT 인프라 접근 통제란 서버, 데이터베이스, 그리고 네트워크에 대한 접근 통제를 말한다. 서버란 네트워크에 연결된 다른 컴퓨터에 서비스를 제공하기 위한 컴퓨터 또는 소프트웨어를 가리키는 말이다. 반대로 서버에서 보내 주는 정보 서비스를 받는 쪽이나 요구하는 쪽의 컴퓨터 또는 소프트웨어를 클라이언트라고 한다. 데이터베이스는 어떠한 조직 내에서 다수의 사람에 의해 공유되어 사용되어질 목적으로 컴퓨터가 접근할 수 있는 장치에 통합적으로 조직되고 관리되는 운영 자료의 집합을 말한다. 그리고 네트워크는 하나의 통신망을 뜻하며, 데이터 통신이라는 하나의 목적을 기반으로 하여 두 개 이상의 장치들이 연결되어 있는 통신 구조를 말한다.

그림 1은 출력 및 복사 시 보호 조치에 관한 구현 방법의 사례를 나타내고 있다.

요건 ID	요건 명	Num	상세 요건
00-00 -02	출력 및 복사 시 보호 조치	1	인쇄물을 출력 시 워터마킹 적용 - 로고, 일시, IP, 성명 등 표시 - 통장 프린터, 공문 발송 등은 업무 특성상 적용되지 않음
		2	어플리케이션 화면에 대한 캡처/복사 방지 기능을 적용 - 서버 DRM 적용 - 2등급 데이터
		로그	인쇄 출력 관련 로그를 생성 1. 로그 생성 시기 : 인쇄물 출력 시 2. 로그 포함 항목 : 일시, IP, 사번, 항목 등 3. 로그 보관 주기 : 1년

그림 1. 출력 및 복사시 보호 조치에 관한 구현 방법 사례

V. 결 론

본 논문에서는 업무를 수행하는 자인 주체적인 사용자의 역할과 데이터 사용행위를 바탕으로 한 접근 통제와 권한 통제가 이루어져야 한다는 점을 제시하였다. 상당히 중요한 정보를 대량으로 검색 및 조회하거나 수정 및 변경하는 작업은 반드시 사전 결재를 득한 후에 가능하다는 것도 제시하였다. 또한, 접근통제의 원칙과 정의에 대하여 설명하였고, 어플리케이션 접근 통제와 IT 인프라인 서버, 데이터베이스, 그리고 네트워크에 대한 접근 통제는 예를 들어서 직접 설명하였으며, 구현의 사례로서 한 기업의 접근통제에 대한 보안 요건의 정의를 실례로서 설명하였다.

참고문헌

[1] http://flyingwolf.co.kr/110185021556

[2] Jong-Il Baek, “Access Control Security Technology for the Protection Vulnerable DB Objects, Department of IT Application Technology, The Graduate School of Venture, Hoseo University, 2012

[3] Kyong-Ho Choi, Sung-Kwan Kang, Kyung-Yong Chung, Jung-Hyun Lee, “A Study of Network 2-Factor Access Control Model for Prevention the Medical-Data Leakage,” Jouranl of Digital Convergence, Vol. 10, No. 6, pp. 341-347, 2012

[4] Jörg Caumanns, Raik Kuhlisch, Oliver Pfaff, Olaf Rode, “IHE IT Infrastructure Technical Framework White Paper – Access Control,” IHE International, 2009