접근 통제의 보안 요건 정의

신성윤* · 김창호* · 장대현* · 이현창** · 이양원*

*군산대학교

**원광대학교

Definition of Security Requirement in Access Control

Seong-Yoon Shin* · Chang-Ho Kim* · Dai-Hyun Jang* · Hyun Chang Lee** · Yang-Won Rhee*

*Kunsan National University

**Wonkwang University

E-mail : {s3397220, over386, daihjang, ywrhee}@kunsan.ac.kr, hclglory@wku.ac.kr

요 약

업무수행자(사용자)의 역할(Role)과 데이터 사용행위에 기반한 접근 및 권한 통제가 이루어져야 한다. 중요 정보의 대량 조회 및 변경 작업은 사전 결재를 득해야 한다. 일정 시간 무행위 세션에 대해 통제를 해야 한다.

ABSTRACT

Attendant services (user) roles (Role) and act on the data used should be based access control and permissions. Large amounts of important information to view and change the pre-approval must be acquired. Non-constant time for the session must control actions.

키워드

access control, pre-approval, control action, important information

Ⅰ. 서 론

개별사용자/그룹사용자에 대한 접근통제 규칙과 권한은 접근통제 정책에 명확히 언급하여야 한다. 접근통제는 논리적과 물리적 둘 다를 함께 고려하여야 한다. 사용자와 서비스제공자에게 접근통제 측면에서 충족하여야 하는 명확한 사업 요구사항을 제공하여야 한다[1].

유비쿼터스 환경에서의 접근통제를 위한 보안 요구사항은 아직 체계적으로 분석되지 않았고, 전통적인 접근통제 모델이 유비쿼터스 환경에 적합한지도 아직 분석되지 않았다. [2]에서는 접근통제를 위한 유비쿼터스 환경의 특징과 접근통제 요구사항을 분석하고, 기존의 접근통제 모델이 갖는 특징을 분석하여 제시한다.

Ⅱ. 접근 통제를 위한 원칙

시스템의 사용은 명확히 설계된 권한에 의해서 제한되어야 한다. 시스템 사용을 위한 주체, 객체, 행위가 정의되고 식별되어야 한다. 사전에 합의된 접근 제어 룰에 의해서 접근 및 사용이 통제되어야 한다.

Ⅲ. 접근 통제를 위한 정의

사용자의 계정(ID)의 발급, 운영, 변경, 폐기를 위한 시스템의 보안 요건을 내부 어플리케이션, 외부 어플리케이션 및 IT 인프라로 나누어서 다음의 기준에 따라 정의한다.

[사용자 유형 정의 (예시)]

인증 수단	유형 1	유형 2	유형 3	유형 4
내부 직원	현업 직원	청구 직원	IT 부서 개발	IT 부서 운영
협력조직 직원	아웃 소싱 직원	n/a	n/a	n/a
시스템 사용자	미들웨어	DB	n/a	n/a

[정보의 등급 지정 (예시)]

유형	성격	예시	1 등급	2 등급	3 등급
유형 1	실명확인정보	주민등록번호	금융거래 승인 및 본인승인 핵심정보 (예: 계좌 비밀번호, 패스워드 등)	본인확인 및 계좌확인 중요정보 (예: 주민번호, 계좌번호)	1 등급,2 등급외 일반정보 및 업무처리정보 (예: 주소, 이메일, 거래내역)
유형 2	신상정보	이름, 주소, 전화번호, 생일, 가족			
유형 3	거래/신용정보	아이디, 계좌번호, 거래내역			
유형 4	비밀번호	계좌비밀번호, 패스워드			

[시스템, 네트워크 등급 지정 (예시)]

유형	Type A	Type B	Type C
위치	DMZ	내부망	내부망
업무	거래처리	업무연계	채널
유형	운영 시스템	운영 시스템	개발 시스템

그림 1. 접근 통제를 위한 정의

IV. 어플리케이션 접근 통제

조직/그룹/직무 등에 따라 사용주체를 정의하고, 어플리케이션 화면에서 제공하는 서비스를 정의하여 Role 기반으로 이루어지도록 하며, 사용행위에 따라 좀 더 세부적인 통제가 이루어지도록 설계한다.

[사용자 주체에 따른 Role 정의 (예시)]

사용자/조직/그룹/직무		
Level 1	Level 2	level 3
임원	지점영업	일반주문
부서장	본사일반	지점전직원
지점장	본사영업	부실장전용
지점업무팀장	본사관리	부실점장전용
지점업무직원	본사업무	지점업무팀장전용

[사용 행위 타입 정의 (예시)]

서비스		Action Type									
		조회		입력	수정	삭제	다운로드		인쇄		
서비스 ID	설명	대량	마스킹				대량	마스킹	화면	기능	마스킹
KIS061032001	임원전용 서비스 001	V		V	V	V	V		V		V
KIS061022001	주문정보 조회 001	V	V					V		V	
KIS061021001	공지사항 001		V	V	V	V		V	V	V	

그림 2. 롤의 정의와 사용 행위 타입 정의·

V. IT 인프라(사버, DB, 네트워크) 접근 통제

[IT인프라 등급 별 접근통제 설정(예시)]

종류	IP 통제	클라이언트 프로그램 제한	추가 인증 실시
운영 시스템(외부)	OK	OK	OK
운영 시스템(내부)	OK	OK	-
개발 시스템	-	-	-

그림 3. IT인프라 접근 통제

VI. 결론

업무수행자(사용자)의 역할(Role)과 데이터 사용 행위에 기반을 둔 접근 및 권한 통제가 이루어져야 한다. 중요 정보의 대량 조회 및 변경 작업은 사전에 결재를 맡고서 얻어야 한다. 일정 시간 아무 행위도 하지 않는 세션에 대해 통제를 해야 한다.

참고문헌

[1] http://cafe.naver.com/softwarequality/book1621832/738

[2] 박희만, 이영록, 이형효, “유비쿼터스 컴퓨팅을 위한 접근통제 모델 분석,” 정보보호학회 논문지, 제19권, 제2호, pp. 35-42, 2009. 4