중요 정보 자산 보안 – DB 보안

김우태 컴퓨터시스템응용 기술사
(matica5127@naver.com)

DB 보안

Concept	+DB 데이터 보안 - DB 보안 유형 - DB 보안 요구 사항, 보안 기능 - DB 보안 통제, 백업과 복구 장애 유형 +DB 관리자 보안 - DB 보안 관리 조직 별 역할 - DB 보안 관리 구성 항목 +DB 보안 구축 고려 사항
KeyWord	**물리/권한/운영 보호, 접근제어/보안 및 권한관리, 접근/추론/흐름 제어**

정보 시스템에서 가장 중요한 정보 자산이라고 할 수 있는 것이 바로 데이터베이스라고 할 수 있다. 이 데이터베이스에 수록된 중요 정보 자산을 어떻게 보호하는지가 정보보호에서 가장 중요한 부분이다.

데이터베이스 보안은 크게 **데이터보안**과 **관리자보안**으로 나눌 수 있으며, 이를 기반으로 시스템 운영 시 DB 보안 운영에 효율성을 요구한다.

1. DB 데이터 보안

1) DB 보안 유형

- 물리적 보안: 컴퓨터 시스템 데이터에 손상을 주는 위험으로부터 데이터베이스를 보호하는 것.
- 권한 보안: 데이터베이스 접근 권한을 가진 사용자만이 특정 접근 모드로 접근할 수 있도록 보호하는 것
- 운영 보안: 데이터베이스의 무결성에 대한 운영자 실수의 영향을 취소화하거나 제거하여 데이터를 보호하는 것

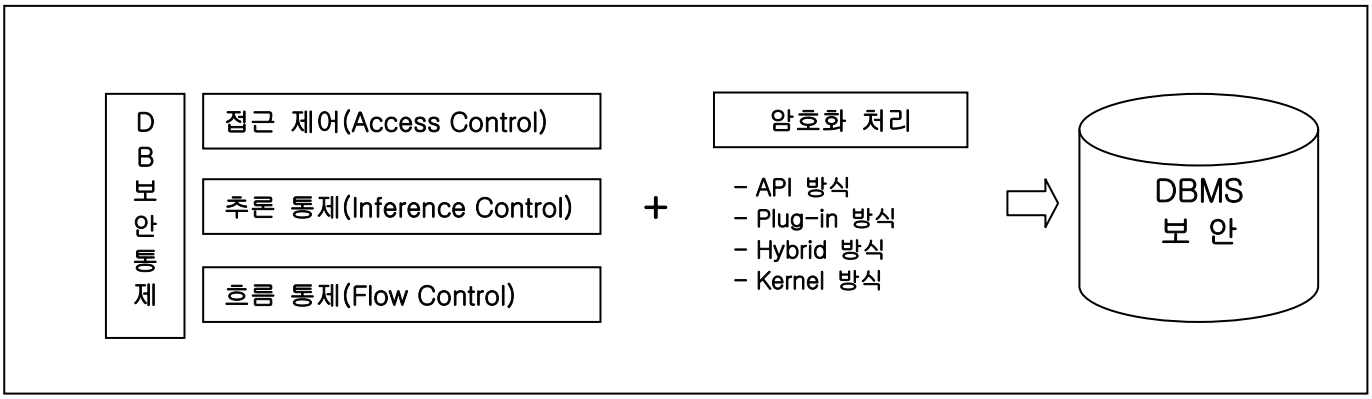
2) DB 보안 요구 사항 및 보안 기능

구 분	요 소	상세 설명
요구 사항	부적절한 접근 방지	- 권한이 인가된 사용자에게만 접근 권한을 부여하여 부적절한 사용자의 접근을 방지하여 접근을 통제해야 함.
	추론 방지	- 기밀이 아닌 데이터로부터 기밀 정보를 얻어내는 가능성을 추론이라고 하는데, 이를 불가능하게 해야 함.
	데이터 무결성	- RDBMS 의 경우를 말하며, 부적절한 접근으로 데이터의 변경이나 파괴, 저장 데이터 손상을 통제해야 함.
	감사 기능	- 데이터베이스의 접근에 대한 감사 기록이 생성되어야 하며, 이를 근거로 차후 분석이 가능하도록 해야 함.

	사용자 인증	- 데이터베이스의 견고한 사용자 인증 기능이 있어야 함.
	다단계 보호	- 데이터의 중요도에 따라서 단계를 나눌 수 있어야 하며, 단계별 권한 부여 등급이 달라지도록 하여 기밀성과 무결성을 보장할 수 있어야 함.
기 능	접근 제어(권한 보안)	사용자별 계정 관리가 이루어져야 하며, 그 과정을 통제할 수 있어야 함.
	권한 관리	사용자 및 사용자 그룹별 특정 데이터베이스 영역만을 선별적으로 접근할 수 있도록 권한 통제가 가능해야 함.

- DB 보안 통제는 접근 제어, 추론 통제, 흐름 통제를 통하여 인가된 사용자에게 암호화된 데이터베이스를 제공함.

3) DB 보안 통제, 백업과 복구 장애 유형



- 인가된 사용자에게만 데이터를 접근 제어할 수 있도록 데이터베이스를 구성해야 함.

구 분	요 소	상세 설명
DB 보안 통제 항목	접근 제어(Access Control)	- 표면적으로는 운영체제의 접근 통제와 유사한 통제 구조 - 접근 권한(Access Right)이 있는지 검사하여 허용 여부 결정함. - 접근 제한 메커니즘(접근 거부, 허용, 수정), 접근 규칙
	추론 통제(Inference Control)	- 간접적 데이터 노출로부터 데이터를 보호하기 위한 통제 항목 - 사용자가 읽은 X가 X에 대한 함수 f를 적용하여 Y=f(X)인 데이터 Y를 얻기 위해 추론을 사용하는 것을 통제함. - 간접 접근을 통한 추론, 상관 데이터의 통제
	흐름 통제(Flow Control)	- 접근 가능한 객체간의 흐름을 조절 - 임의의 객체에 포함되어 있는 정보가 명시적 또는 암시적으로 높은 보안수준에서 낮은 보호수준의 객체로 이동하는 것 검사 - 허용 가능한 정보 흐름의 식별을 요구
복구 장애 유형	사용자 오류	- 운영자 및 사용자에 의해서 주요 데이터의 임의 추가, 수정, 삭제시 발생 할 수 있는 장애 유형임.
	명령문 장애	- 유효하지 않은 SQL 구성에 의해 명령문 장애가 발생하면 실행이 취소되고, 제어 권한이 사용자에게로 돌아감.
	프로세스 장애	- 데이터베이스의 접속 프로세스의 장애에 의한 유형임. - 비정상적인 접속 해제나 프로세스 강제 종료 등 ……

	인스턴스 실패	- 작업에 필요한 인스턴스 생성에 문제가 있어 더 이상 수행이 불가능한 장애 유형임.

- 데이터 보안을 구축하는데 있어서 견고한 보안 통제 수단을 구축하는 것도 중요하지만 관리하고 운영할 수 있는 체계를 정립하는 것은 더욱 중요함 요소하고 할 수 있음.

2. DB 관리자 보안

- DB 보안을 체계적으로 구축하고 유지, 관리 하기 위해 DB 보안 관리 Framework를 기반으로 이에 관련된 DB 보안 정책 관리, 변경관리, 분석관리, 운영관리, 성능 및 장애 관리, 로그 및 백업 관리 등의 절차와 관리 조직, 관리 인력 등이 유기적으로 DB 보안 관리체계를 구성해야 한다.

1) DB 보안 관리 조직 별 역할

구분	상세 설명
경영진	- 기업의 보안 사고에 대한 지속적인 관심 표명 - 보안 담당 임원의 선임 권한
보안 담당 임원	- CSO, CISO - 보안 전담 조직 구성/지휘 및 투자 의사 결정, 전사적 지원 확보
DB 보안 담당자	- 체계적인 보안 정책 수립 - 정보 자산 접근 통제 및 데이터 보안 구축 및 운영 수행
시스템 관리자	- 시스템 관리 측면에서 DB 보안 담당자를 Assist
DBA	- 데이터베이스 관리 측면에서 DB 보안 담당자를 Assist
임직원	- 보안 정책 숙지 및 준수 - 정보 등급에 따른 데이터베이스 관리 등급 부여

- DB 보안 담당자는 DB 보안 관리를 수행하는 세부 업무를 분류하고 지속적인 관리 및 운영을 해서 예방 보안에 각별히 주의하여야 함.

2) DB 보안 관리 구성 항목

구 분	상세 설명	비 고
보안 정책 관리	- DB 보안 구축, 운영에 관련된 정책 및 관련 기준, 절차, 지침 등을 문서화하여 관리	DB 보안 담당자에 의해 수립
변경 관리	- 보안 정책이 변경 관리 절차에 의해서 통제되고 관리되어야 함.	정보시스템운영관리와 일관성 유지가 필요함
운영 관리	- 보안 솔루션의 구성관리, 변경관리, 운영인력 관리(필요 시)및 운영상태 점검 등의 활동 수행	
로그 및 백업 관리	- 중요 보안로그를 정의하여 상시 백업하고, 감사 기능에 부합될 수 있도록 관리되어야 함.	기술 요소별 상세 관리 내용을 반영
모니터링 체계 수립	- 성능 확인(저하 여부), 장애 시 즉시 감지가 가능한 체계를 구축해두어야 함.	시스템 가용성 확보, 장애 예측
성능 및 장애 관리	- 장애에 대비한 장애 복구 계획 수립 - 장애 유형 및 중요도에 따른 등급 산정/ 관리	장애 대응 Matrix

권한 관리/접근 통제	- 사용자별 권한 관리를 하여 등급별 접근을 통제하는 정책 수립 - 장애 발생시 즉각적인 접근 통제 진행.	직무 변경 시 즉시 대응/반영
취약점 개선 관리	- H/W 결함, S/W 취약점 등을 점검하고, 보안 패치 등으로 지속적인 취약점 개선 활동 전개	- 지속적인 개선 의지가 중요함.
침해 사고 대응 체계 수립	- 침해 사고 대응을 위한 기준 및 프로세스 정립	- compliance 에 대한 숙지

3. DB 보안 구축 고려 사항

- DB 데이터 보안 체계 및 조직체계, 프로세스에 대한 문서화를 진행하고, 준수할 수 있도록 제도화 및 경영진의 지속적인 관심 유도 필요함.
- DB 보안 실무자의 지속적인 업무 수행 능력 확보를 위해서 정기적이고, 적절한 교육 프로그램의 제공이 필요함.
- PDCA 의 Cycle 내에서 관리체계의 주기적 점검 > 개선점 도출 > 반영되도록 해야 함.

"끝"

[참고 문헌]
1) 정보보호개론, 정익사
2) 정보보안기사/산업기사, 시대고시기획
3)http://www.dbguide.net/db.db?cmd=view&boardUid=152803&boardConfigUid=9&categoryUid=216&boardIdx=145&boardStep=1