데이터베이스 보안

황인탁
IRM 대표컨설던트

서 론

최근 정보시스템의 보안문제에 대한 관심이 높아지고 있다. 그것은 정보시스템의 역할이 확대됨과 더불어 정보시스템의 역기능들이 도출되면서 발생하는 심각한 경제적 · 사회적 손실을 현실적으로 직면하게 됨과 정보시스템으로 인한 정보의 집중, 정보관리체제의 집중으로 인한 상대적인 취약점의 확대에 기인한다. 실제로 최근 각종 정보망에 대한 해커들의 침입, 자연재해, 인위적인 재해 등에 의한 정보자원의 붕괴, 정보의 유출 · 파괴 · 변조 등 많은 보안 및 안전상의 취약점을 목격하고 있는 실정이다.

정보시스템은 여러가지 자원으로 구성된다. 하드웨어, 통신, 소프트웨어, 데이터, 인력 이들 5가지는 대표적 구성요소로써 각 요소들은 각 사용환경에 따라 세분되어질 수 있다.

이같은 정보시스템의 구성요소들은 모두 보안과 안전대책의 대상이 되며 정보시스템의 안전대책은 이들 요소들에 대한 개별적인 대응과 함께 총체적인 전략이 필요하다.

여기서는 정보시스템의 여러가지 자원중에서 데이터베이스의 안전에 대해서 살펴보도록 하겠다. 데이터베이스는 정보를 수록하고 관리하는 실체라는 점만으로도 매우 중요한 관리자원이다. 또한 최근의 데이터베이스 관리시스템은 프로그래밍과 운용체계(Operating System)와도 일정한 관계를 지니고 있다. 따라서 데이터베이스에 대한 안전위협은 그 파급효과가 직접적이고 매우 크다.

1. 정보시스템의 안전성이란?

일반적으로 정보시스템의 안전성을 정의할때 시스템의 가용성, 보안성, 목적성의 세가지 속성을 이야기한다. 데이터베이스의 안정성도 이상의 세가지 속성을 지니고 있으나 가장 직접적으로 관련되는 속성은 무결성이다. 무결성은 정보시스템의 핵심적인 속성으로서 기본적으로 확보되어야 할 것이다. 무결성은 다음의 다섯가지 특성으로 이루어진다.

'안전성(Completeness)', '정확성(Accuracy)', '승인(Authnrization)', '일관성(Consistancy)', '최신성(Updateness)' 데이터베이스의 안전대책은 위의 다섯 특성을 적절히 확보함으로써 일차 목표는 달성된다.

가용성은 정보시스템 자원을 활용하여 사용자에게 적정한 정보서비스를 제공하기 위한 관련자원의 상태유지 정도를 의미한다. 최적의 가용성을 유지하기 위해서는 시스템장애나 오류발생시

적절한 집단과 보수를 위한 유지보수 체계의 확립과 서비스 신뢰를 확보하기 위한 품질보증 등의 방법이 적용되어야 할것이다. 가용성의 내부 속성을 살표보면 '유지보수성', '신뢰성', '계속성' 으로 구성된다.

마지막으로 보안성은 누출되는 경우 조직에 유해한 결과를 초래할 수 있는 총체적인 정보를 보호하는 상태유지를 말한다. 보안성을 유지하기 위한 보편적인 기법으로는 다음의 세가지가 있다.

- 인증성(신분확인 기법)
- 기밀성(암호화 기법)
- 추적성(추적확인 기법)

이상의 정보시스템의 안전성을 구성하는 속성들은 정보시스템이 어떻게 안전대책을 갖추어야 하는가를 논리적으로 제시하고 있다.

2. 데이터베이스의 안전 요구사항

데이터베이스의 안전대책을 수립하기 위해 우리는 데이터베이스의 안전상의 요소들을 정의할 필요가 있다. 데이터베이스 시스템의 기본적인 아래 요구사항들은 앞서 언급한 정보시스템의 안전요소들과 유사하다. 데이터베이스에서의 안전요구사항은 다음과 같다.

① 물리적인 데이터베이스 무결성

데이터베이스의 데이터들이 전기적장애(정전, 쇼크 등)와 같은 물리적 충격에서 파괴되지 않고, 재구축할 필요성이 없도록 보호되어야 한다.

② 논리적 데이터베이스 무결성

데이터베이스의 구조는 어떤 Field의 값이 수정될 때 다른 Field에 영향을 주지 않도록 설계되어야 한다.

③ 단위 데이터의 무결성(Element Integrity)

각 단위 데이터는 정확한 값을 유지해야 한다.

④ 접근 통제(Access Control)

사용자들은 허가 받은 정보를 허가 받은 취급범위(예를들면 Read, Write 등)내에서 활용할 수 있도록 통제되어야 한다.

⑤ 사용승인(User Authentication)

모든 사용자들은 사용증적과 데이터의 접근허가를 위해 시스템적인 승인절차가 필요하다.

⑥ 가용성(Availability)

사용자들은 일반적으로 데이터베이스에의 접근과 승인이 용이해야 한다.

- 데이터베이스의 무결성(Database Integrity)

데이터베이스가 데이터의 중앙저장소(Central Repository)로서 관리되어진다면 사용자는 데이터의 정확도를 신뢰해야만 할것이다. 이와 같은 상황은 데이터베이스 관리자로 인가받은자로서 데이터의 처리를 수행함을 보증한다. 또한 이때의 데이터는 불법적인 프로그램이나 외부의 영향, 즉 화재나 정전같은 재해로 부터 보호 받을 수 있다.

데이터베이스의 무결성에 대한 전반적인 책임은 DBMS, Operation System과 시스템 관리자에게 속해있다. 데이터베이스 무결성에 대한 대책중의 하나는 시스템상의 모든 File들에 대한 Back-up이다. 데이터베이스의 주기적인 Back-up는 자연재해에 대한 적절한 통제의 하나이다.

데이터베이스의 재구축을 위해서는 DBMS는 log file을 갖춰야 한다. 시스템에 중대한 장애가 발생했을때 데이터베이스의 Back-up copy와 log file상의 최근의 거래내역(transactions)으로 회복시킬 수 있다.

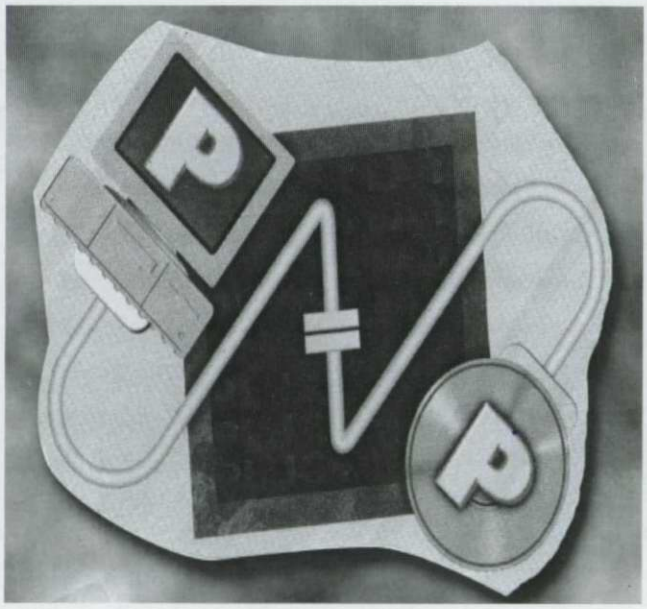
- 단위 데이터의 무결성(Element Integrity)

단위 데이터의 무결성은 정확성과 정밀성을 의미한다. 궁극적으로 데이터의 정확성은 사용자의 정확한 입력에 달려있다. 그러나 사용자의 입

력실수, 처리실수로 인한 데이터의 오류를 발견하기 위해 DBMS는 사용자를 지원할 수 있어야 한다.

DBMS는 세가지 단계로 단위데이터의 무결성을 관리한다.

첫번재는 'Field check'이다. Field check의 다양한 점검항목은 데이터와 정의단계에서 결정되어 진다. 두번째는 'Access Control'이다. 데이터베이스에서는 하나의 데이터 항목이 몇개의 장소에 보관되어진다. 따라서 하나의 데이터 항목이 변경될때 여러 File에서의 수정이 요구되어지며 그때마다 새로운 Check가 이루어진다. 누가 어떤 데이터의 갱신에 대한 권한을 갖고 있는가는 매우 중요한 점검항목이다. 두 사람 이상이 어떤 데이터를 동시에 갱신하려고 할때 데이터베이스 관리자는 문제 해결의 역할을 담당한다. 무결성 유지를 위한 세번째는 데이터베이스의 'Change Log' 관리이다. 'Change Log'는 데이터베이스의 모든 변경사항을 기록한 File로써 변경 전·후와 값을 갖고 있다. 데이터베이스 관리자는 데이터베이스를 복구할때 이 Log file을 사용할 수 있다.



- *접근통제(Access Control)*

데이터베이스는 사용자의 접근 권한(Privileges)에 의해 논리적으로 구분된다. 모든 사용자가 접근가능한 일반 데이터가 있는 반면 특정사용자만이 접근가능한 데이터가 있다. 예를 들면 급여데이터, 판매데이터 같은 것이 제한될 수 있을 것이다. DBMS는 이와같은 접근정의에 의해 접근을 통제할 수 있어야 한다. 그러나 데이터베이스의 접근통제 기법은 각 단위 데이터 상호간의 연관성을 고려하기 때문에 좀더 복잡하다. Inference추론는 데이터베이스의 접근통제를 위해 사용되는 기법이다.

- *사용승인(User Authentication)*

DBMS는 철저한 사용승인을 요구할 수 있다. DBMS는 Operating system에 의해 허용된 사용승인외에 특별한 패스워드와 사용일시 등을 점검, 승인할 수 있다. DBMS는 OS위의 응용프로그램처럼 기능한다. 이것의 의미는 사용승인을 포함한 모든 명령 또는 데이터를 점검한다는 의미이다. 한편 DBMS는 프로그램과 시스템의 양면성을 지닌다. 즉 사용자들에게는 응용프로그램처럼 기능하며 한편으로는 하드웨어와 소프트웨어 자원을 통제하는 프로그램이기도 하다.

다음은 데이터베이스의 안전성에 대한 위협을 살펴보겠다. 데이터베이스의 안전성은 비승인원 접근이나 조작으로부터 데이터베이스를 보호함으로써 이루어진다. 데이터베이스와 관련된 행위 자체가 승인 받았는지를 결정하기 위해서는 두가지 과정이 필요하다.

첫째로 보호될 필요성이 있는 단위나 대상이 식별되어야 한다. 이러한 단위나 대상으로는 데

이터 필드, 레코드, 화일, 프로그램, 저장장치, 컴퓨터실 등이 있다.

둘째로, 승인정책이 이루어질 수 있는 기준이 설정되어야 한다. 이와같은 기준은 조직에서 설정한 정보관리규칙이나 기밀등급으로부터 도출할 수 있다. 완전하게 안전한 데이터베이스를 구축하기란 사실상 불가능한 일이다. 따라서 안전대책을 수립하는데 있어서의 촛점은 안전대책을 실시하는데 투여되는 비용과 이러한 안전대책으로 인해 보호될 수 있는 자산의 손실액을 적정선에서 균형있게 유지하는 것이다.

3. 데이터베이스 안전성의 위협요소

데이터베이스의 안전성에 관한 위협은 데이터의 노출, 조작, 파괴의 세가지로 구분된다.

- 데이터의 노출

데이터의 노출이란 데이터베이스의 내용이 알 필요(Need to know)가 있는 이외의 타인에게 노출되는 경우를 의미한다. 즉 비승인된 사람이 어떤 보고서나 시스템으로부터의 온라인 응답을 획득할 때, 또는 합법적인 사용자가 알 필요가 없거나 아니면 알아서는 안되는 데이터베이스의 특정부분에 대한 접근 권한을 얻었을 경우에도 해당된다. 절도는 데이터 노출의 극단적인 경우이다.

데이터 노출의 동기는 일반적으로 개인적인 이익에 있다. 비승인된 노출은 시스템에 대한 보다 광범위한 침해나 조작의 초기 단계에 작용한다. 도난당한 데이터에 패스워드나 트랜잭션 코드가 포함되어 있을 경우 침입자는 이를 사용하여 이후의 데이터베이스 사용시 합법적인 사용자로 가장하여 침입할 수 있게 된다.

- 데이터의 조작/파괴

데이터베이스의 비승인된 조작은 그 결과가 뒤늦게 드러나는 경우가 많지만 그 위협의 정도는 다른 위협의 형태와 같다. 어떤 개인이 개인의 이익을 위해 데이터 필드를 변경하거나 데이터베이스를 변경시키기 위해 변조된 또는 가상의 트랜잭션을 입력시킬 수 있을 것이다. 데이터베이스에 대한 접근을 불가능하게 하는 상황에서는 데이터 파괴를 고려할 수 있을 것이다.

인의적으로 데이터가 파괴되었을때 범죄행위의 수단으로 이용할 수 있다. 시스템이나 데이터베이스의 장애는 침입자로 하여금 시스템 디렉토리나 기타 민감한 데이터를 시스템 복구기간에 접근할 수 있는 기회를 제공할 수 있다.

데이터베이스 안전에 대한 위협은 비승인된 접근이나 접근된 데이터의 비적절한 사용과 관련되어 있기 때문에 이에 대한 대응조치도 접근통제나 데이터의 이용방법에 초점을 맞추어 설정되어야할 것이다. 이러한 안전대책은 물리적 측면, 기술적 측면, 관리적 측면으로 분류하여 검토할 수 있다.

4. 데이터베이스의 안전대책

① 신분확인

데이터베이스의 안전성 확보 첫단계는 접근통제이다. 접근 통제에는 컴퓨터나 주변장치 및 전산환경을 보호하기 위해 실시되는 관리정책과 물리적 통제를 위한 시건장치, 장비, 방문자의 감시통제 등의 물리적 측면, 그리고 DBMS에 포함된 사용자 인증절차 등 기술적 측면이 복합적으로 구성된다.

접근통제의 첫번째 단계는 신분확인이다. 신분확인은 일반적으로 각각의 사용자에게 신분확인번호(User I.D)를 할당함으로서 이루어진다. 사용자는 신분확인 번호를 입력하고 시스템은 입력된 번호를 확인한다. 신분확인 식별자를 사용함으로써 데이터베이스 이용에 대한 추적과 안전

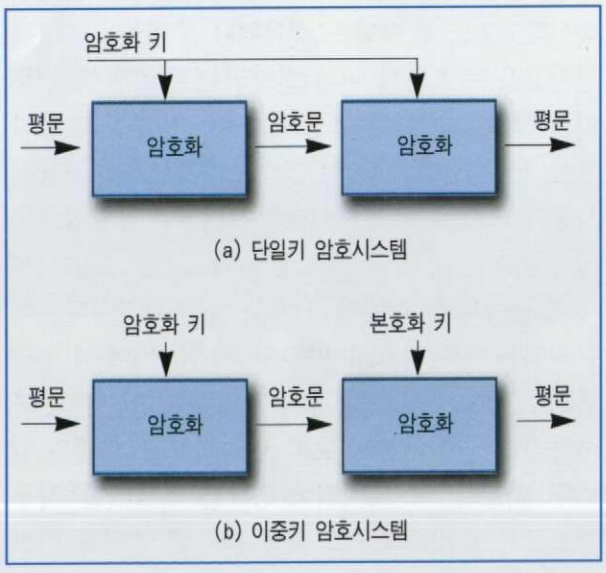
감시가 가능해 진다. 신분확인이 되면 사용자는 사용인증을 위해 패스워드의 입력을 요청받는다. 입력된 패스워드가 시스템에 등록된 패스워드와 일치하는지를 확인한 후 접근이 허용된다.

신분인증의 또다른 방법에는 Magnetic Card(최근에는 I.C Card도 이용), 지문이나 음성인식 등을 이용한 신분인식 기법이 사용되고 있다.

② 사용자 권한 인증

신분확인과 인증은 시스템 전체나 DBMS 설비를 보호하기 위해 설계된다. 반면 권한인증은 데이터베이스 내의 특정항목을 보호하는 역할을 수행한다.

일반적으로 사용자는 데이터베이스 항목에 대해 Read-only, Write-only, Read and Write 분류된 접근권한을 갖는다. 시스템의 접근권한을 부여하기 전에 그항목에 대한 모든 승인된 사용자 접근통제 리스트를 확인한다. 접근권한을 부여하고 적절한 접근수준을 정의하는 절차는 매우 다양하며 권한절차는 여러가지 다양한 수준에 의거하여 설정될 수 있다.



③ 암호화(Encryption)

정보의 도난, 도청에 적극적인 대응을 위해 사용되는 기본적인 기법이 암호화이다.

암호화는 데이터를 저장이나 전송에 앞서 부호화하거나 암호문으로 변환하는 절차를 의미한다. 암호화된 메시지가 수신되거나 검색될 경우 복호화 되어야 한다. 이와 같은 과정은 비 승인된 사용자에 의해 습득된 데이터의 가치를 감소시킨다.

일반적으로 암호화 기법은 안전성을 위한 암호화과정의 기밀성에 의존해 왔다. 그러나 최근의 기법은 암호화 키에 의존하는 공개된 알고리즘을 사용하고 있다. 다음은 암호화키에 의한 암호화 절차이다.

④ 안전성검사(Security Audit)

안전성의 구축감사나 검토는 조직의 안전성 제고 노력에 중요한 일부분을 차지한다. 데이터베이스 관리자는 안전성 침해사건이 발생하였을 경우 안전감시를 실시함으로써 침해에 대한 추적을 용이하게 행할 수 있다. 안전성 감사는 데이터베이스에 대한 접근의 성공과 실패, 안전성에 대한 주기적인 검사의 두가지 측면을 가지고 있다.

⑤ 데이터베이스 관리자의 역할 정립

데이터베이스의 안전대책 설정에는 데이터베이스관리자(DBA)의 역할이 매우 중요하다. DBA는 조직내의 안전성에 대한 현존하는 위협을 우선적으로 식별하여 분석해야 한다. 이를 통해 DBA는 데이터베이스를 보호하기 위해 필요한 안전대책의 유형과 범위를 선택할 수 있다.

다음으로 DBA는 권한승인 정책을 규정하고 절차를 관리하고 사용중인 안전성 기법에 의해 요구되는 특정의 기밀 데이터에 대한 책임을 지녀야 한다.

DBA는 패스워드와 데이터베이스의 키를 할당하고 이들의 보호에 책임을 져야 한다.

접근 요청은 DBA에 의해서 검토되고 협조되어야 한다. 그러나 DBA의 권한 승인에 대한 결정은 임의적이어서는 안되며, 반드시 현존하는 정책에 근거를 두어 이루어져야 한다.

그밖에 DBA는 현재의 내부통제가 어디에 필요한 지를 검토하고 논의해야 한다. 또한 DBA는 안전시스템에 시험을 기획하고 실행함으로써 안전성 침해사건이 검출될 수 있는 가능성을 증가시켜야 한다. 마지막으로 DBA는 데이터베이스의 내용과 처리결과에 대한 통계적 표본추출 검증을 실시하는것도 바람직하다. 이상의 DBA의 역할은 데이터베이스의 안전성에 중점을 둔 DBA의 기능을 정의한 것이다. 데이터베이스의 관리는 많은 부분이 DBA에 집중되어 있으므로 DBA 자체가 중요한 안전대상이기도 하다. 따라서 DBA에 대한 적절한 인사관리방안도 검토되어야 한다.

이상 살펴본 데이터베이스의 안전대책을 요약해 보면 다음과 같다.

방 안	노출된 위협	절 차	정 책
신분확인 및 권한인증	전체 전체	ID No. 할당 Password 할당	합법적인 데이터베이스 사용자에 대한 규정
권한인증	전체	특권의 부여, 박탈	알 필요 및 사용할 필요성에 대한 규정
암호화	노출	선택된 알고리즘	민감한 데이터 및 처리에 대한 규정
감사	조작	선택된 데이터의 검증 및 데이터베이스 구조의 검증	감사 시기와 범위의 규정

결 론

정보시스템은 사용자가 필요로 하는 정보를 완성하고, 정확하며, 승인을 받아 최신의 상태로 일관성 있게 제공하여야 하며 적합한 사용자가 원하는 때에 바로 제공함을 그 목적으로 한다. 정보시스템의 안전대책은 정보시스템이 기본적으로 지니고 있어야 하는 특성, 속성을 파악함으로써 올바르게 준비할 수 있을 것이다. 안전대책이란 그 대상 시스템의 본래의 목적을 달성하기 위한 통제 및 견제기능이다. 시스템은 그 목적을 달성하는데 있어 각종 처리과정에서 오류와 예상치 않은 사태가 발생할 수 있으며, 이를 사전에 계획된 목적에 도달하게 하기 위하여 오류와 예기치 못한 상태를 바로잡기 위한 장치 즉, 견제가 필요하다.

모든 시스템은 자신의 목적을 달성하는데 있어 여러가지 장애요인을 가지고 있으며 이러한 장애요인 또는 위협요소에 대처하기 위한 자체방어 시스템으로서 안전대책과 내부통제기능의 설정이 요구되는 것이다.

데이터베이스는 정보시스템을 구성하는 요소중에서 가장 중요한 데이터를 관리한다. 정보시스템의 또다른 구성요소인 하드웨어, 소프트웨어는 그 위협요소를 정의하거나 대응방안을 수립하기에 보다 더 명확할 수 있다. 그러나 데이터베이스는 정보시스템의 속성중 하나인 인간/기계 연계성(Man Machine Interface)이 특히 강조되므로 위협의 범위가 더욱 포괄적인 특성이 있다. 따라서 데이터베이스의 안전성을 검토할때 시스템적인 대책수립과 더불어 인간관리적인 측면이 중요하게 다루어져야 할 것이다.

데이터베이스의 안전대책을 떠올리면 그 범위와 기술적 어려움으로 막연한 생각이 들곤한다. 그러나 안전위협의 명확한 실체와 정의를 규명하면 그 대책의 마련은 그리 어려운 일은 아니다. 무엇보다도 중요한 것은 안전에 대한 의식과 대책의 실현일 것이다.

끝으로 이번 데이터베이스의 안전대책에 대한 소개가 여려분의 정보자원에 대한 인식전환의 기회가 되기를 바라며 좀더 발전된 내용을 갖고 다시 소개할 수 있는 기회가 있기를 바란다. DC