전자금융거래법(전자금융감독규정) 준수를 위한

DB 작업통제 솔루션 (QueryOne S)소개

2018.04

세종정보보안 Soft Garden

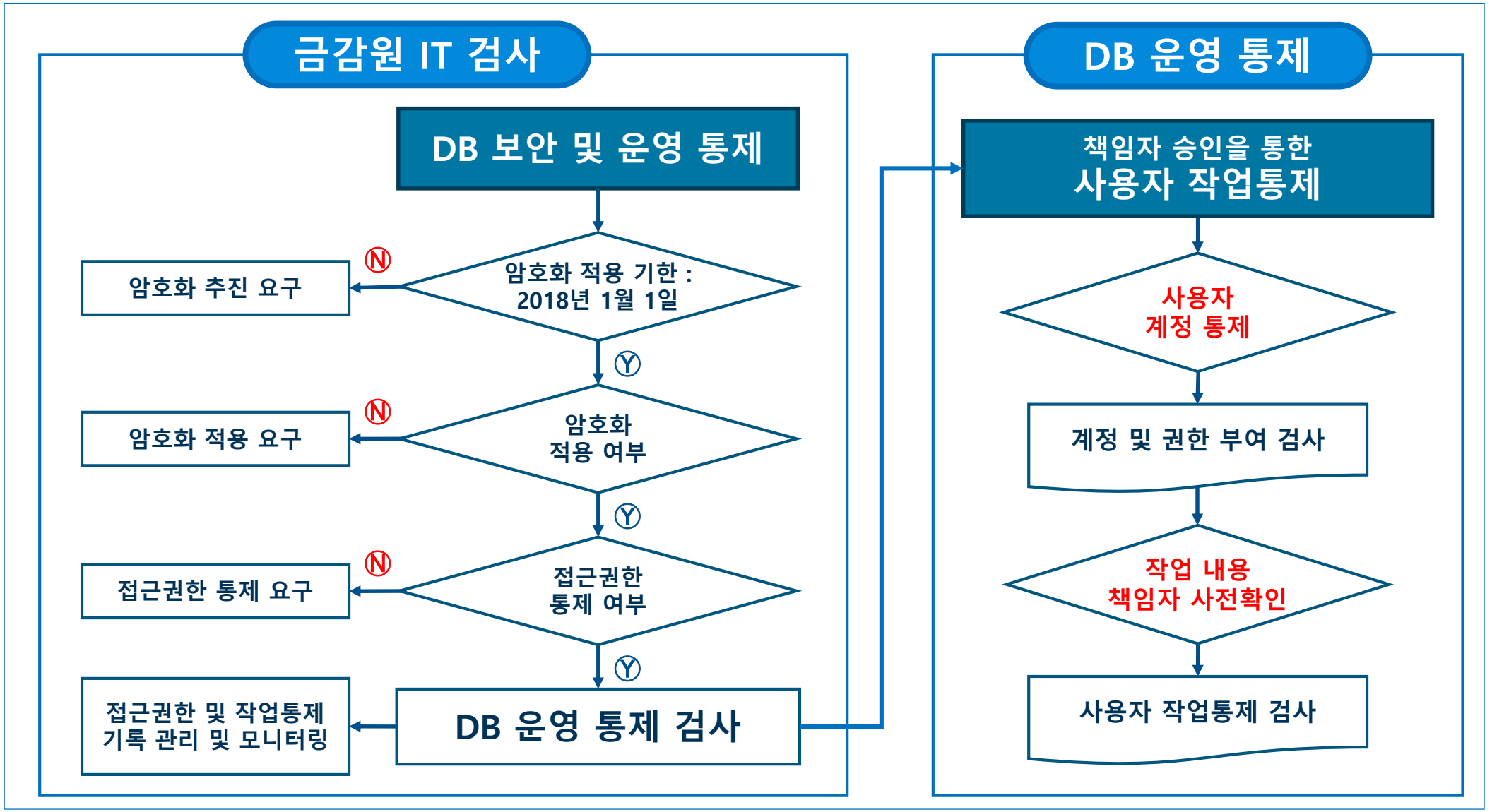
Agenda

1. DB 작업통제 필요성 : 금감원 검사 대응
2. DB 작업통제 솔루션 : QueryOne S
3. DB 접근 및 작업통제 검사 대응 방안

1. DB 작업통제 필요성 : 금감원 검사 대응

1.1 개인정보보호 관련 권한 및 작업통제

❑ 금융회사가 자율적인 IT보안체계를 확립할 수 있는 기반을 조성하기 위하여 내부통제 강화를 요구함



1. DB 작업통제 필요성 : 금감원 검사 대응

1.2 H 전자금융 전문업체 금감원 검사 공시

❑ 정보처리시스템 접근통제 관리강화

※ 제재조치일 : 2017년 10월 31일

- **H사는 DB 접근통제 솔루션을 도입하여 개인별로 DBMS 계정을 부여하고, 데이터베이스 변경문 실행 이력 저장 수행**
- **최금 금감원 검사는 접근통제에 추가하여 DBMS 작업에 대한 책임자 승인을 통한 이중 확인을 중점 점검하고 있음**

개선 사항

데이터베이스 접근통제 솔루션을 도입하여 개인별로 데이터베이스 계정을 부여하고, 데이터베이스 변경문(Query) 실행 이력을 남기고 있으나, 관리자 업무를 수행하지 않는 직원 O명에게 관리자 권한을 부여하고 있고, **외부주문업체 직원(O명)에게 운영계 데이터베이스 조회 권한이 과다하게 부여하고 있어 이를 통하여 고객정보 등을 임의로 조회할 가능성**이 있으므로 업무상 불필요한 데이터베이스 관리자 권한과 **외부주문업체 개발자의 운영계 데이터베이스 조회 권한을 회수**하고, 앞으로 **데이터베이스 접근권한에 대한 발급·회수 등의 통제 절차를 더욱 적정하게 수행**할 필요

운영 현황

- 데이터베이스 접근통제 솔루션을 도입하여 개인별로 데이터베이스 계정을 부여하고, 데이터베이스 변경문(Query) 실행 이력을 남기고 있음
  ➜ DB접근통제 솔루션은 어떤 사용자가 어느 DB에 접속하여 어떤 작업을 수행할 수 있는지에 대한 접근 및 권한 통제와 이력 관리를 수행
- 외부주문업체 직원(O명)에게 운영계 데이터베이스 조회 권한이 과다하게 부여하고 있음
- 데이터베이스 접근권한에 대한 발급·회수 등의 통제 절차를 더욱 적정하게 수행할 필요

➜ 접근 권한(조회)이 있는 사용자가 DB에 접속하여 수행하는 작업에 대한 책임자 승인에 의한 이중확인 통제가 필요함

① 전자금융감독규정 제28조(거래통제 등) **"전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인"** 준수를 위한 3자(책임자) 승인 프로세스 적용이 필요

② 최근 금감원 검사는 DB암호화 적용 이후 고객정보에 대한 조회, 저장 등에 의한 유출 방지를 위하여 DB 직접접속 작업에 대한 통제 프로세스 적용 여부를 집중적으로 검사를 진행하고 있음(계정관리, 접근통제 포함)

1. DB 작업통제 필요성 : 금감원 검사 대응

1.2 S캐피탈 금감원 검사 공시

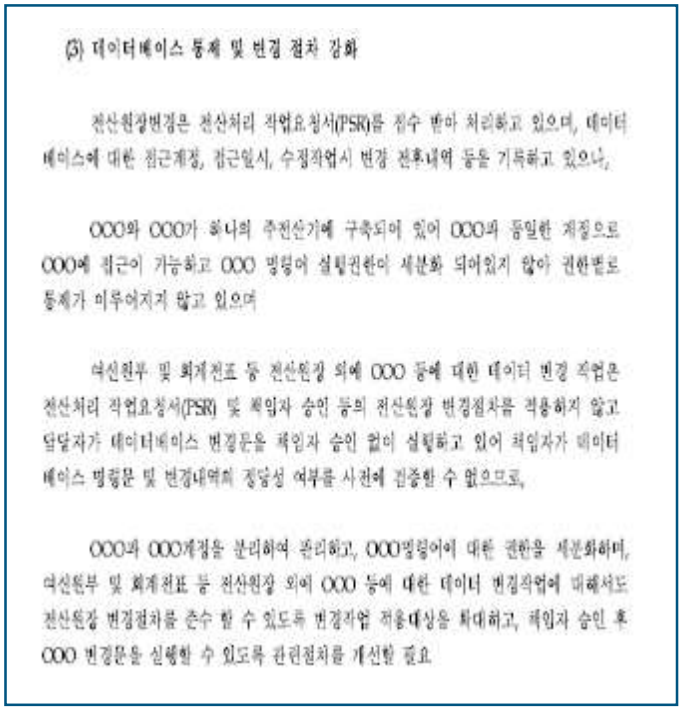
❑ 데이터베이스 통제 및 변경 절차 강화

※ 제재조치일 : 2017년 08월 14일

- **전산원장 이외 중요 DB에 대한 작업에 대하여 책임자가 사전에 명령문 및 변경내역에 대한 검증을 수행 필요**
- **DB 작업 Tool과 결재 시스템이 별도로 구성된 경우에는 결재에 기술된 내용으로 수행 여부를 사전 확인이 불가능함**

개선 사항

전산원장변경은 전산처리 작업요청서(PSR)를 접수 받아 처리하고 있으며, 데이터베이스에 대한 접근계정, 접근일시, 수정작업시 변경 전후내역 등을 기록하고 있으나, OOO와 OOO가 하나의 주전산기에 구축되어 있어 OOO과 동일한 계정으로 OOO에 접근이 가능하고 OOO 명령어 실행권한이 세분화 되어있지 않아 권한별로 통제가 이루어지지 않고 있으며 여신원부 및 회계전표 등 **전산원장 외에 OOO 등에 대한 데이터 변경 작업은 전산처리 작업요청서(PSR) 및 책임자 승인 등의 전산원장 변경절차를 적용하지 않고 담당자가 데이터베이스 변경문을 책임자 승인 없이 실행**하고 있어 **책임자가 데이터베이스 명령문 및 변경내역의 정당성 여부를 사전에 검증할 수 없으므로**, OOO과 OOO계정을 분리하여 관리하고, OOO명령어에 대한 권한을 세분화하며, 여신원부 및 회계전표 등 **전산원장 외에 OOO 등에 대한 데이터 변경작업에 대해서도 전산원장 변경절차를 준수 할 수 있도록 변경작업 적용대상을 확대하고, 책임자 승인 후 OOO 변경문을 실행할 수 있도록 관련절차를 개선할 필요**



(5) 데이터베이스 통제 및 변경 절차 강화

전산원장변경은 전산처리 작업요청서(PSR)를 접수 받아 처리하고 있으며, 데이터베이스에 대한 접근계정, 접근일시, 수정작업시 변경 전후내역 등을 기록하고 있으나,

OOO와 OOO가 하나의 주전산기에 구축되어 있어 OOO과 동일한 계정으로 OOO에 접근이 가능하고 OOO 명령어 실행권한이 세분화 되어있지 않아 권한별로 통제가 이루어지지 않고 있으며

여신원부 및 회계전표 등 전산원장 외에 OOO 등에 대한 데이터 변경 작업은 전산처리 작업요청서(PSR) 및 책임자 승인 등의 전산원장 변경절차를 적용하지 않고 담당자가 데이터베이스 변경문을 책임자 승인 없이 실행하고 있어 책임자가 데이터베이스 명령문 및 변경내역의 정당성 여부를 사전에 검증할 수 없으므로,

OOO과 OOO계정을 분리하여 관리하고, OOO명령어에 대한 권한을 세분화하며, 여신원부 및 회계전표 등 전산원장 외에 OOO 등에 대한 데이터 변경작업에 대해서도 전산원장 변경절차를 준수 할 수 있도록 변경작업 적용대상을 확대하고, 책임자 승인 후 OOO 변경문을 실행할 수 있도록 관련절차를 개선할 필요

DB 작업통제 강화

- 데이터베이스 명령문 및 변경내역의 정당성 여부를 사전에 검증할 수 없으므로, OOO과 OOO계정을 분리하여 관리
- 여신원부 및 회계전표 등 전산원장 외에 OOO 등에 대한 데이터 변경작업에 대해서도 전산원장 변경절차를 준수 할 수 있도록 변경작업 적용대상을 확대
- 책임자 승인 후 OOO 변경문을 실행할 수 있도록 관련절차를 개선

1.3 데이터베이스 운영 통제 비교

❑ 데이터베이스 운영 통제 관련 검토 사항

▪ **DB 접근통제 솔루션으로는 권한이 있는 사용자가 수행하는 작업에 대한 사전통제가 불가능하므로 DB 작업통제 솔루션 도입으로 DB 접속 작업에 대한 일원화된 통합관리로 개인정보 보호 및 관련 법규의 준수가 필요**

통제 항목	감독규정 준수를 위한 통제 방안	DB 관련 작업통제 검토 사항
접근 통제	▪ 사용자의 업무에 따라 접근할 수 있는 DBMS을 통제	• 접근 권한이 있는 사용자의 DB 접속에 대한 통제 방안은?
권한 통제	▪ 사용자의 업무에 따라 수행할 수 있는 DBMS 권한을 통제	• 개인정보 등 중요 정보에 대한 작업(조회 등)에 대한 세부 관리 방안은?
이력 관리	▪ 사용자가 수행한 작업에 대한 사전 및 사후 이력 관리	• 누가 어떤 작업을 수행하였는지에 대한 책임자의 승인 및 이력 관리는 ? • **결재 내용과 수행한 작업에 대한 통합 이력 관리 방안은?**
마스킹 적용	▪ 주민등록번호 등 개인정보에 대해서는 조회 시 마스킹 처리 ▪ 업무상 마스킹 해제가 필요한 경우 책임자 승인 후 해제	• **개인정보가 포함된 DB를 조회할 수 있는 권한을 보유한 사용자의 주민등록번호 등 개인정보 조회 통제는?**
명령어 통제	▪ 중요 시스템에 대한 중요작업 수행 시 작업 내용에 따라 책임자 결재 후 작업 수행	• 사전 승인 없이 개인정보 등 중요 정보에 대한 작업을 수행하는 경우 통제 방안은? • 결재 시스템에서 승인 된 작업과 상이한 작업을 수행하는 경우 통제는?
조회 관리	▪ 주민등록번호 등 개인정보에 대해서는 조회 가능 건수를 지정 ▪ 업무상 지정 건수 이상을 조회하는 경우 책임자 승인 후 조회	• 중요 정보에 대하여 과다한 조회를 하는 경우 사전 통제 방법은? • 100건 조회에 대한 승인 후 1,000건을 조회하는 경우 통제 방법은?
다운로드 관리	▪ PC 저장 및 클립보드 카피를 금지하며, 업무상 필요한 경우 책임자 승인 후 저장 ▪ 개인정보를 단말에 저장하는 경우 DRM 솔루션과 연동하여 자동으로 DRM 적용	• 개인정보 등 중요 정보를 조회 후 PC에 저장하는 경우 사전 통제 방안은? • 개인정보를 가공(앞자리 6자리와 뒷자리 7자리 분리) 저장하는 경우? • DRM 등을 우회하여 PC에 저장 후 다중 압축 및 암호 처리 후 외부로 전송하는 경우 통제 방안은?
계정 관리	▪ 사용자가 DB 계정 정보 입력 없이 DB 접속 가능하도록 관리 ▪ 사용자가 전출·퇴직 등 인사조치가 있을 때에는 해당 사용자 계정 삭제 등 접근을 통제	• DB 작업이나 장애 등으로 외부 인력이 DB에 접속하여야 하는 경우 DBMS의 계정 및 비밀번호 등 접속 정보는?

1.3 데이터베이스 운영 통제 비교

❑ 데이터베이스 운영 통제 솔루션 기능 비교

- **DB 접근통제 솔루션**은 사용자가 접속할 수 있는 DB 및 작업 내용에 대한 통제 및 사후 이력 관리를 수행함
- DB 접근통제 솔루션은 사용자가 수행하는 작업에 대한 책임자 승인을 통한 이중확인 적용이 불가능함
- 최근 검사에서는 DB에 접속 및 작업을 수행할 수 있는 **권한이 있는 사용자의 작업에 대한 사전 통제** 방안을 요구하고 있음
- **DB 작업통제 솔루션** 도입으로 직접접속 작업에 대한 일원화된 통합관리로 개인정보 보호 및 관련 법규의 준수가 필요

통제 항목	감독규정 준수를 위한 통제 개선 방안	작업Tool	접근통제	작업통제
접근 통제	▪ 사용자의 업무에 따라 접근할 수 있는 DBMS을 통제	X (미지원)	O (지원)	O (지원)
권한 통제	▪ 사용자의 업무에 따라 수행할 수 있는 DBMS 권한을 통제	X (미지원)	O (지원)	O (지원)
이력 관리	▪ 사용자가 수행한 작업에 대한 사전 및 사후 이력 관리	X (미지원)	△ (사전 통제 X)	O (지원)
마스킹 적용	▪ 주민등록번호 등 개인정보에 대해서는 조회 시 마스킹 처리 ▪ 업무상 마스킹 해제가 필요한 경우 책임자 승인 후 해제	X (미지원)	△ (책임자 승인 X)	O (지원)
명령어 통제	▪ 중요 시스템에 대한 중요작업 수행 시 작업 내용에 따라 책임자 결재 후 작업 수행	X (미지원)	△ (책임자 승인 X)	O (지원)
조회 관리	▪ 주민등록번호 등 개인정보에 대해서는 조회 가능 건수를 지정 ▪ 업무상 지정 건수 이상을 조회하는 경우 책임자 승인 후 조회	X (미지원)	△ (책임자 승인 X)	O (지원)
다운로드 관리	▪ PC 저장 및 클립보드 카피를 금지하며, 업무상 필요한 경우 책임자 승인 후 저장 ▪ 개인정보를 단말에 저장하는 경우 DRM 솔루션과 연동하여 자동으로 DRM 적용	X (미지원)	X (미지원)	O (지원)
계정 관리	▪ 사용자가 DB 계정 정보 입력 없이 DB 접속 가능하도록 관리 ▪ 사용자가 전출·퇴직 등 인사조치가 있을 때에는 해당 사용자 계정 삭제 등 접근을 통제	X (미지원)	△ (DB 계정 노출)	O (지원)

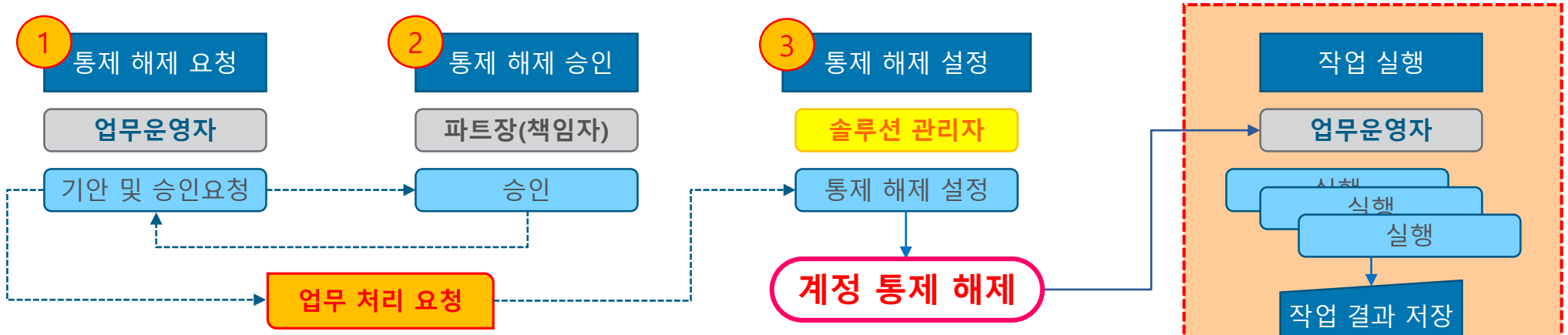
1. DB 작업통제 필요성 : 금감원 검사 대응

1.3 데이터베이스 운영 통제 비교

❑ 데이터베이스 운영 통제 솔루션 기능 비교

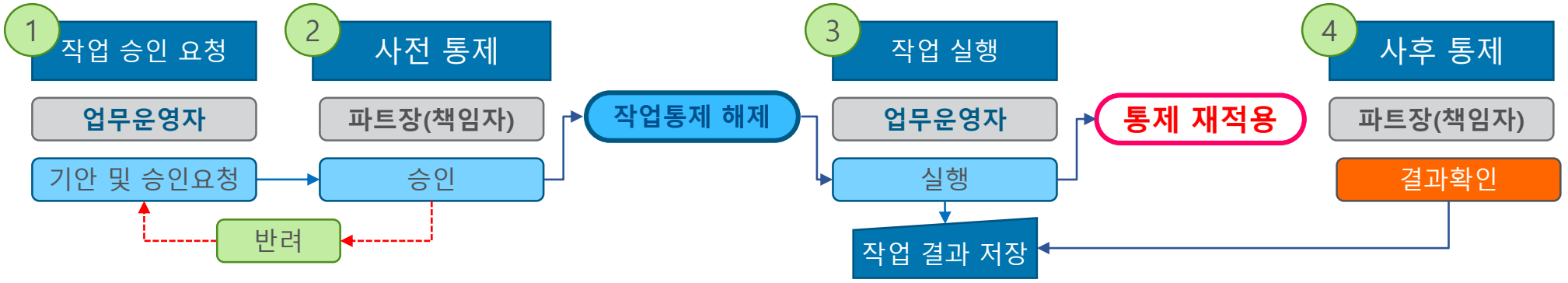
DB 접근통제 솔루션 통제 절차

※ DB접근통제 솔루션은 **통제 정책 해제**가 적용되면 이후의 작업 수행 및 작업 결과에 대한 **책임자 승인 등 통제 미적용**



DB 작업통제 솔루션 통제 절차

※ DB 작업통제 솔루션은 **작업 실행**에 대해서 통제 조건에 따라 책임자 승인 및 결과 확인으로 **사전 작업통제 적용**

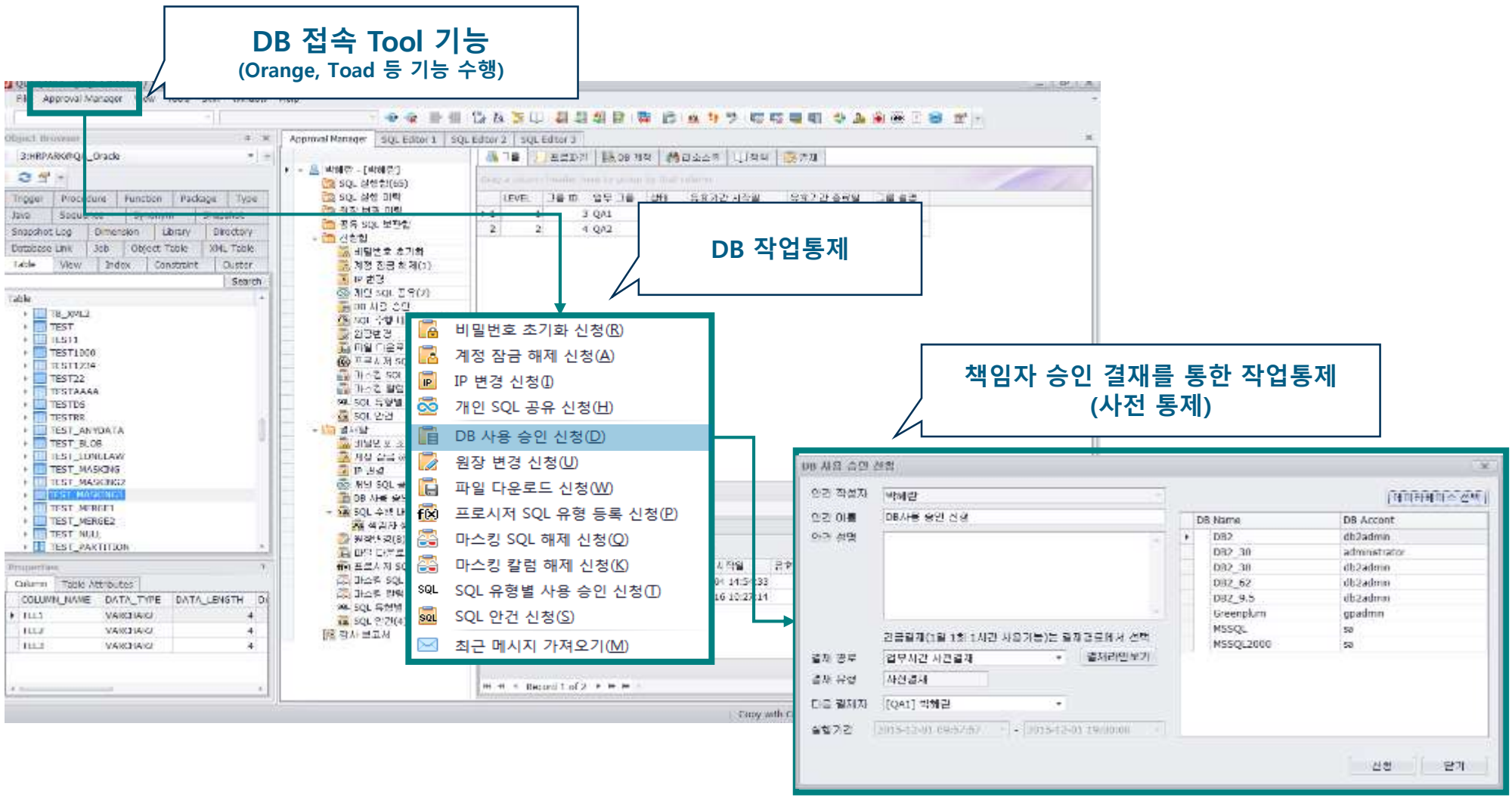


1. DB 작업통제 필요성 : 금감원 검사 대응

1.4 DB 작업통제 솔루션 적용 구성안

❑ DB 작업통제 솔루션 주요 기능

- **DB 작업통제 솔루션**을 이용하여 모든 DB작업에 대해서 **작업 Tool(기존 Orange 등)** 및 **작업통제** 기능 수행

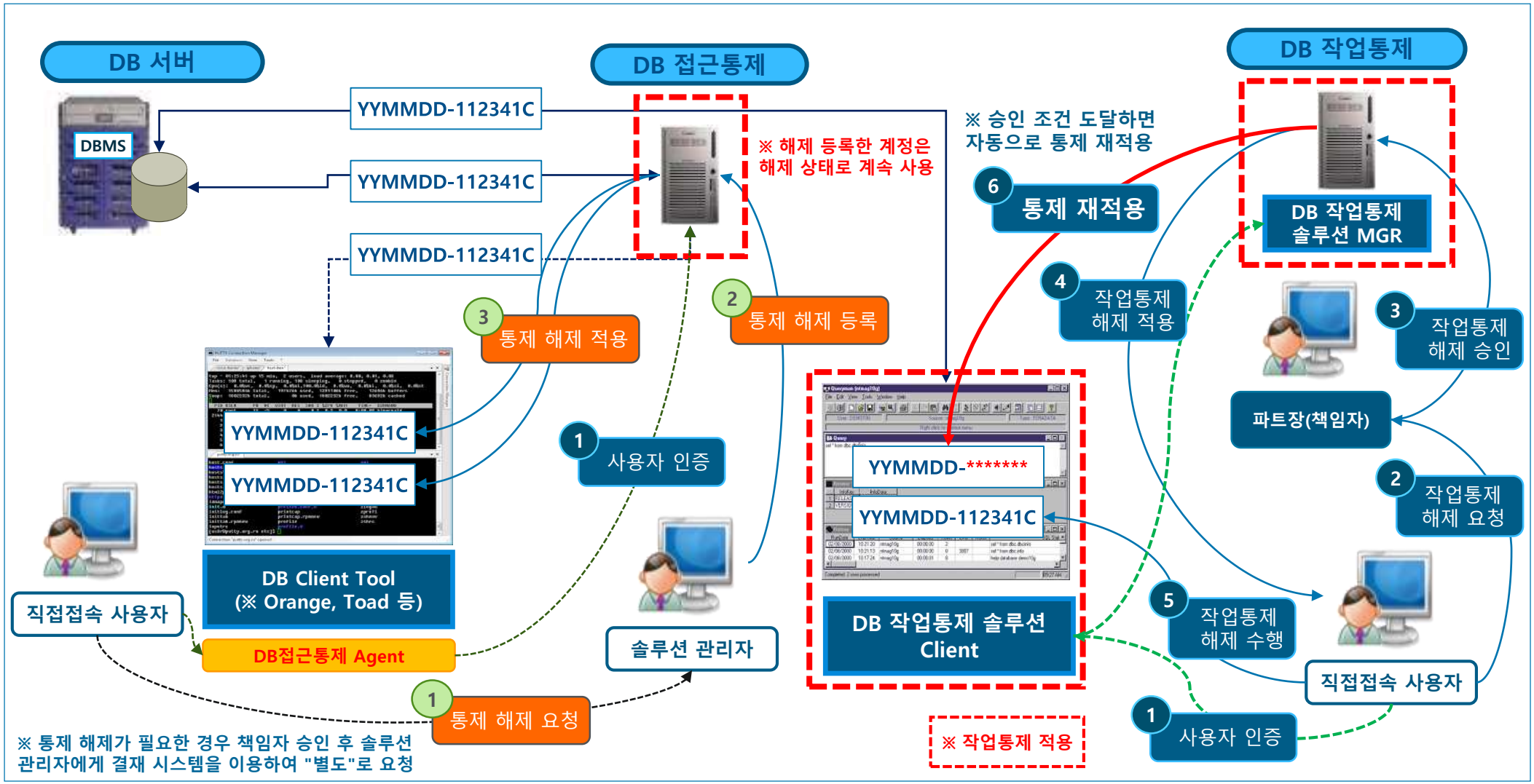


1. DB 작업통제 필요성 : 금감원 검사 대응

1.4 DB 작업통제 솔루션 적용 구성안

❑ DB 통제 솔루션 기능 비교도

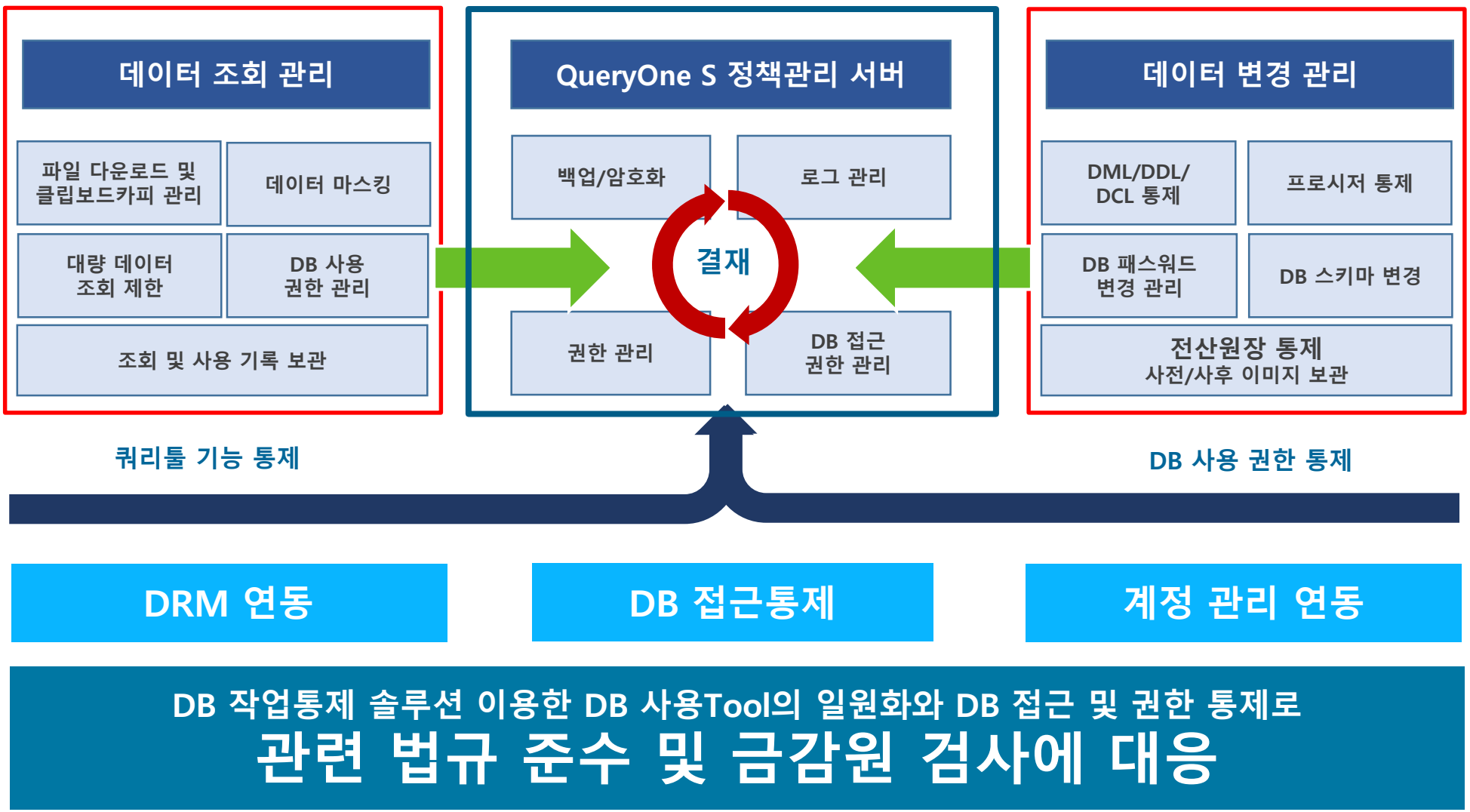
- **DB 접근통제 솔루션**은 접근권한통제 수행, **DB 작업통제 솔루션**은 작업 Tool(기존 Orange 등) 및 **작업통제** 기능 수행



2. DB 작업통제 솔루션 소개 (QueryOne S)

2.1 DB 작업통제 솔루션 개요

❑ 고객정보(고유식별정보) 및 전산원장, 주요정보의 조회 및 변경 등에 대하여 책임자 승인을 통해 관리



2.2 DB 작업통제 솔루션 기능

❑ DB 작업통제 솔루션 QueryOne S 통제 기능

분 류	기능	설명
계정 관리	가상 계정	• DB 사용 권한을 관리자가 분배하기 때문에, DB 계정 정보 유출 없이 DB 사용 가능. • 작업통제 솔루션 계정으로 1인 1계정 관리가 가능(모든 사용자에 대한 계정 통제 가능) **※ 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당 가능**
변경 차단/통제	**원장 변경 프로세스**	• 원장 변경에 대한 프로세스 적용 **※ 제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용**
	DML/DDL/DCL 통제	• DML, DDL 등 각 구문 별 변경에 대한 관리 기능
조회 차단/통제	**접근 DB 관리**	**• 사용 가능한 DB를 인원 별 그룹별 분배하며, 책임자 승인으로 접근 및 사용 가능한 DB를 부여**
	최대 조회 관리	**• 조회 가능 건수를 지정하고, 책임자 승인으로 지정 건수 이상 조회 통제 (마스킹 적용 포함)**
	다운로드 관리	**• PC에 저장 및 클리보드 카피를 관리하며, 책임자 승인으로 다운로드 할 수 있게 통제**
	마스킹	**• 마스킹 및 마스킹 해제를 관리하며, 책임자 승인으로 마스킹을 해제 할 수 있게 통제**
로깅	사용 기록 관리	• 실행 시간, SQL 문장, 성공/실패, 실행 횟수 등을 기록 및 리포트 제공
	조회 결과 저장	• 명령어(Select) 실행 결과를 파일로 저장 가능(저장 시 책임자 승인으로 통제)
	데이터 변경 전후 기록	• DML 실행 전/후 값을 암호화 저장
DB Tool 관리	Tool 기능 분배	• 인원별 그룹별 툴 기능을 세분화 시켜서 분배 **※ 개발자, 운영자, 업무 담당자 등 사용자의 업무별로 솔루션의 기능 사용을 통제**

2.2 DB 작업통제 솔루션 기능

❑ 전자금융감독규정 관련 규정

분 류	기능	관련 법규(전자금융감독규정)
DB 계정 관리	가상 계정	• 13조 2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
DB 변경 차단/통제 (전산원장 통제)	변경 프로세스	• 27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립 운용하여야 한다. • 28조 3. ② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.<개정 2013.12.3.>
	DML/DDL/DCL 통제	
DB 조회 차단/통제	**접근 DB 관리**	**• 13조 2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것**
	최대 조회 관리	**• 13조 10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)<개정 2013.12.3.>**
	다운로드 관리	**• 13조 13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)**
	마스킹	**• 13조 4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것 • 13조 10. 이용자 정보의 조회·출력에 대한 통제**
로깅	사용 기록 관리	• 14조 3. 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회 내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.<개정 2013.12.3.>
	데이터 변경 전후 기록	• 27조 2. ② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경 내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
DB Tool 관리	Tool 기능 분배	• 15조 4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것<신설 2013.12.3.>

2.2 DB 작업통제 솔루션 기능

❑ DB 작업통제 솔루션 QueryOne S DB 기능

분류	메뉴	주요 기능	지원 DB
Query 관리	SQL Editor	- Auto Complete, Intelli-Sense, Bookmark, SQL Formatting - 실행 결과 조작, Filtering, Grouping, Pivot, Image Viewer	전 DBMS
	PL/SQL Editor	- PL/SQL Debugging, Compile, Ref Cursor 지원	Oracle
	Plan Editor	- 예상 실행 계획, 런타임 실행 계획 조회 - Grid, Text, Tree 형태의 View 제공	Oracle
	Data Dictionary	- Dictionary 조회	전 DBMS
Data 관리	Data Export	- text, csv xls(x) 포맷과 Script 기능 제공, Binary 포맷 지원 - 대용량 데이터(4G 이상)의 경우 파일 분할 저장	전 DBMS
	Data Import	- Bulk Insert(Oracle, MS-SQL) 지원	전 DBMS
	Data Pump	- Oracle Client의 exp, imp Utility 지원	Oracle
	Data Loader	- DBMS Client의 Loader 기능 지원	Oracle, Vertica, Teradata, DB2, Tibero
품질 관리	Data Compare	- Data 및 Script(Table, View등) 비교 및 동기화 구문 생성	전 DBMS
	Script Generation	- Table, View, Procedure등 Object에 대한 Script 생성 기능	Oracle (지원 DBMS 추가 예정)
SQL 튜닝	Top N SQL	- 악성 쿼리 검색, 다양한 검색 조건 제공	Oracle, DB2, MS-SQL, Teradata, Tibero
	SQL Trace	- 실시간 Trace 파일 분석, Secure FTP 지원	Oracle, Tibero
	SQL Advisor	- 오라클 SQL Tunning Advisor 기능 지원	Oracle
DB 모니터링	Session Monitor	- Session Info, Process, I/O, Wait Event, All Cursor등 조회	전 DBMS
	Transaction Monitor	- 트랜잭션 모니터링 및 관리 도구 제공	Oracle, Tibero
	Lock Monitor	- Lock 모니터링 및 제거 기능 제공	Oracle, Tibero, DB2
	Database Monitor	- DB 리소스 사용량을 그래프로 실시간 표출	전 DBMS (Netteza 제외)
DB 관리	Space Manager	- DB 저장 공간 및 사용량 관리 기능	전 DBMS
	Security Manager	- User 상태 및 권한 관리, Object 권한 관리	전 DBMS (DB2제외)
	Health Check	- DB 상태를 보고서 형식으로 제공(txt, html, pdf 포맷 지원)	Teradata, Oracle, DB2, MS-SQL 등
	AWR Report	- 오라클에서 제공하는 AWR Report 조회	Oracle
	Alert Log Viewer	- alert.log 파일 분석	Oracle
브라우저	Object Browser	- Object 정보 및 속성 조회, Script 출력 기능, 테이블 생성/수정 기능	전 DBMS
	Templete Browser	- 문법 작성 가이드 및 예제 제공	전 DBMS

2.2 DB 작업통제 솔루션 기능

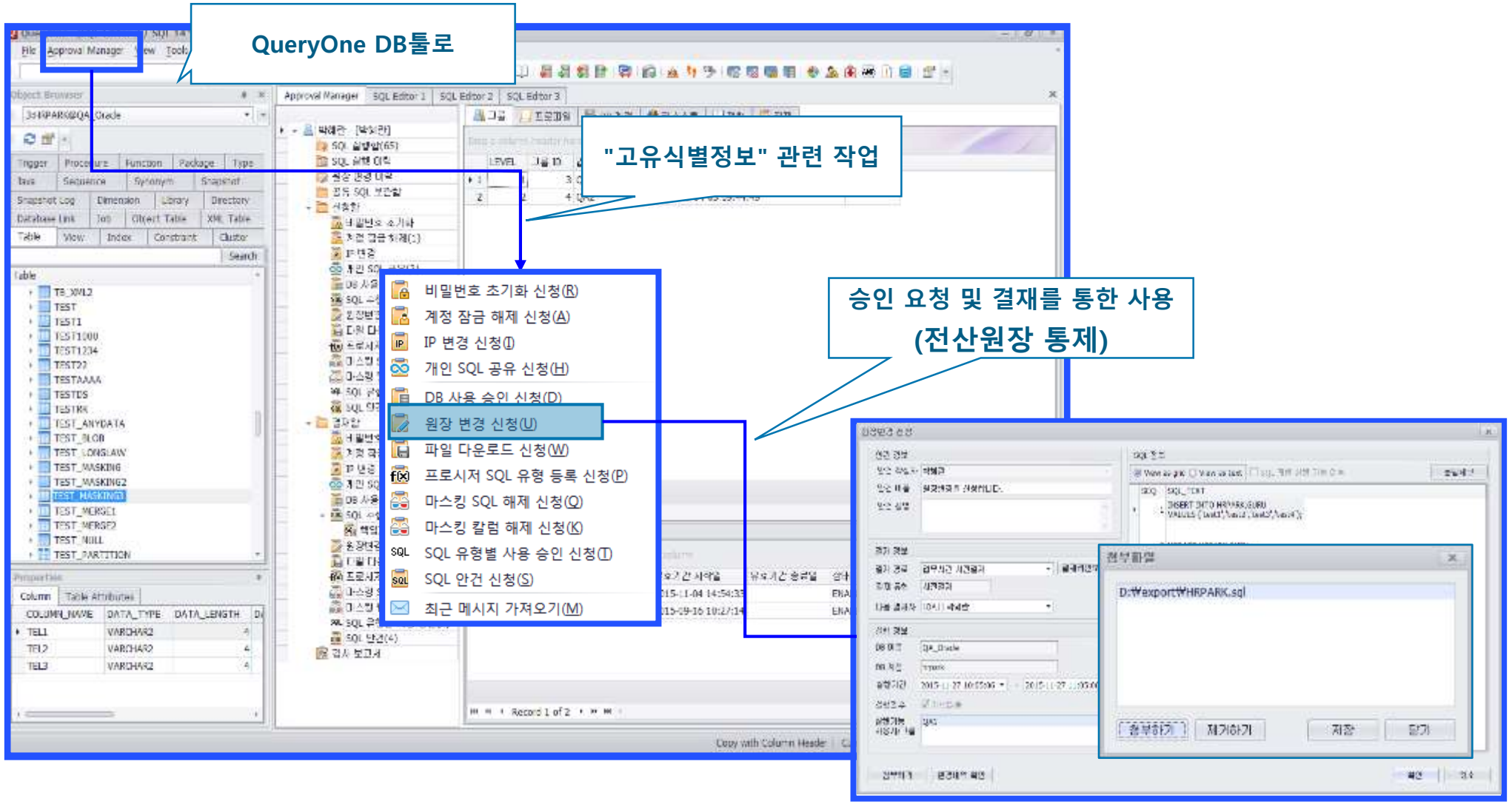
❑ DB 작업통제 솔루션 QueryOne S 지원 DBMS

- QueryOne S 하나로 15가지 DATABASE 에 접속하여 쿼리 실행 및 DB 관리 작업

DB명	지원버전	비고
Oracle	9i 이상	
DB2	9.5 이상	
MS-SQL	2000 이상	
MySql	5.6 이상	
Teradata	13.0 이상	
Sybase IQ	12.6 이상	
Sybase ASE	12.7 이상	
Tibero	4.0 이상	
Altibase	4.3.9 이상	
Greenplum	4.2 이상	
Vertica	7.02 이상	
PostgreSQL (PPAS 포함)	9.3.5 이상	
Netezza	6.1	
EXADATA	11g 이상	
HANA	1.0	
Informix	12.10.FC7	

2.3 DB 작업통제 솔루션 주요 기능

❑ 고객정보(고유식별정보) 및 주요정보의 DB 직접접속에 대한 통합적인 보안 대책의 적용

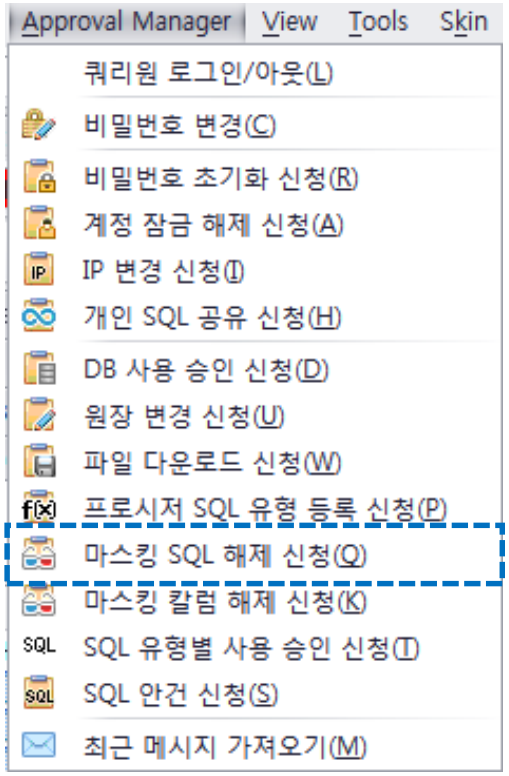


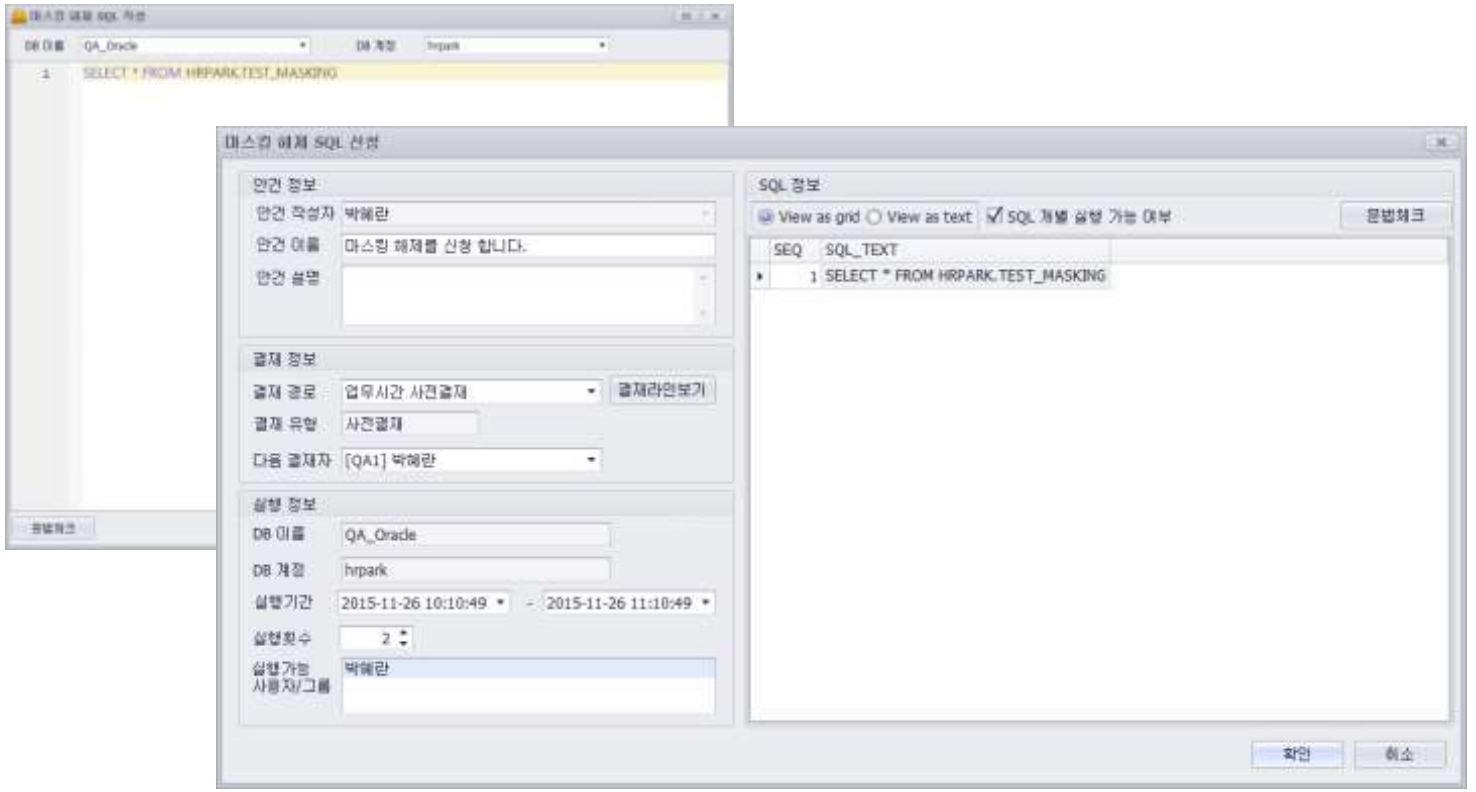
2.3 DB 작업통제 솔루션 주요 기능

❑ 고객정보(고유식별정보) 및 주요정보의 조회 방지를 위한 마스킹 및 승인 처리

- 데이터 마스킹을 통해 중요한 정보는 '*' 가 적용되어 조회
- 마스킹 해제 신청을 통해 승인이 되면 쿼리를 실행 하여 실제 데이터를 확인 할 수 있음

마스킹 결재 처리



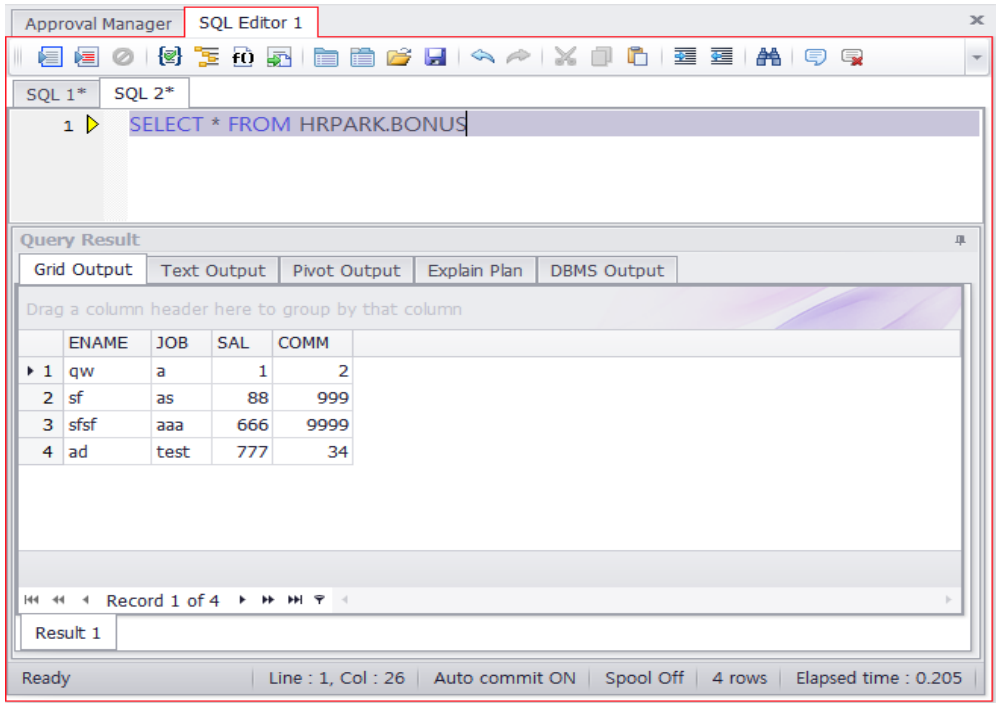


2.3 DB 작업통제 솔루션 주요 기능

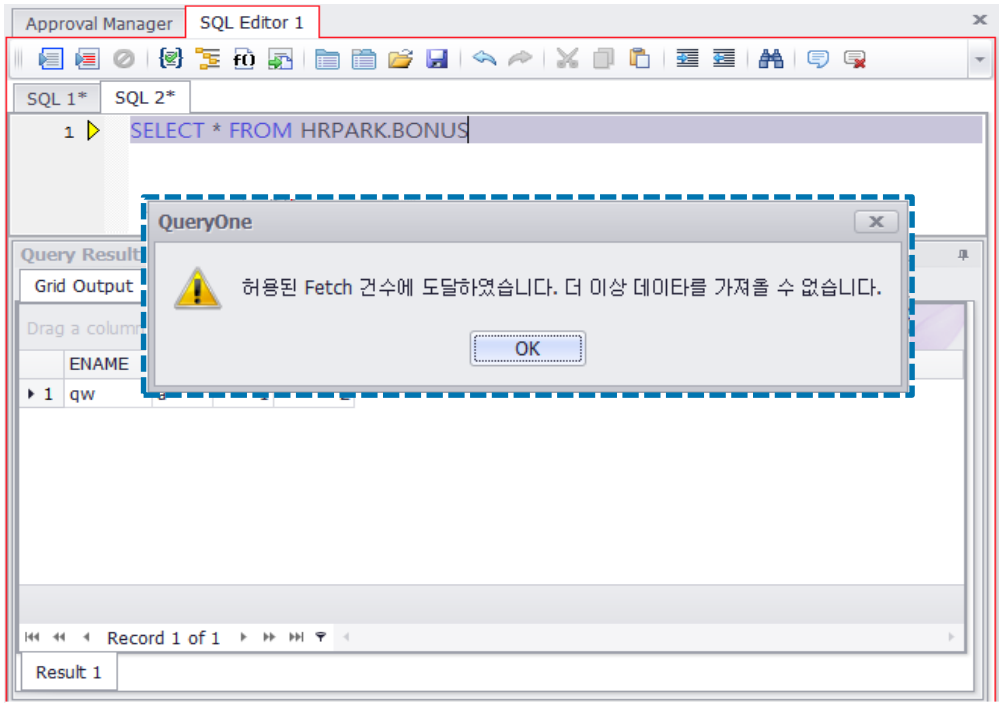
❑ 고객정보(고유식별정보) 및 주요정보의 대량 조회 방지를 위한 건수 제안 및 승인 처리

- 쿼리 조회 결과값을 **허용된** 건수 이상 볼 수 없도록 설정이 가능
- 지정 건 수 이상 조회가 필요할 경우 결재를 통해 정해진 횟수 이상의 ROW수를 조회 할 수 있음

조회 건수 무제한



조회 건수 제한

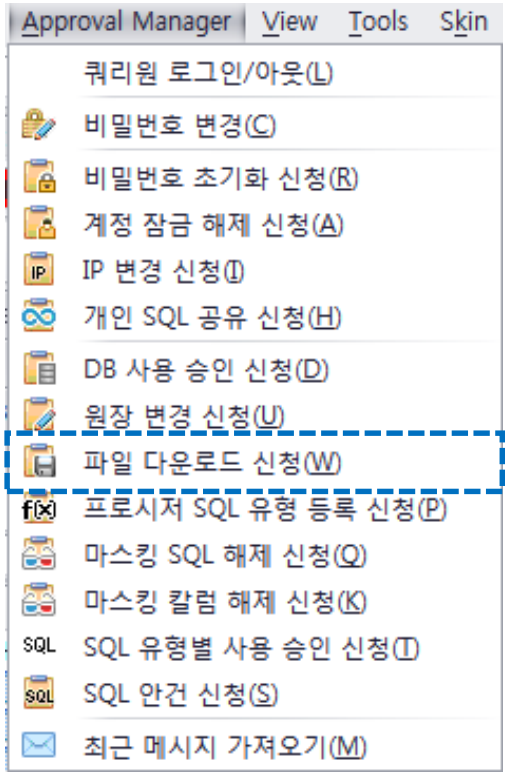


2.3 DB 작업통제 솔루션 주요 기능

❑ 고객정보(고유식별정보) 및 전산원장, 주요정보의 저장 방지를 위한 파일 다운로드 및 승인 처리

- 조회 결과를 저장 하기 위해서는 파일 다운로드 신청을 통해 승인 된 후에만 다운로드가 가능
- 파일 다운로드시 DRM과 연동을 통해 관리(암호화 저장)가 가능

다운로드(저장) 결재 처리

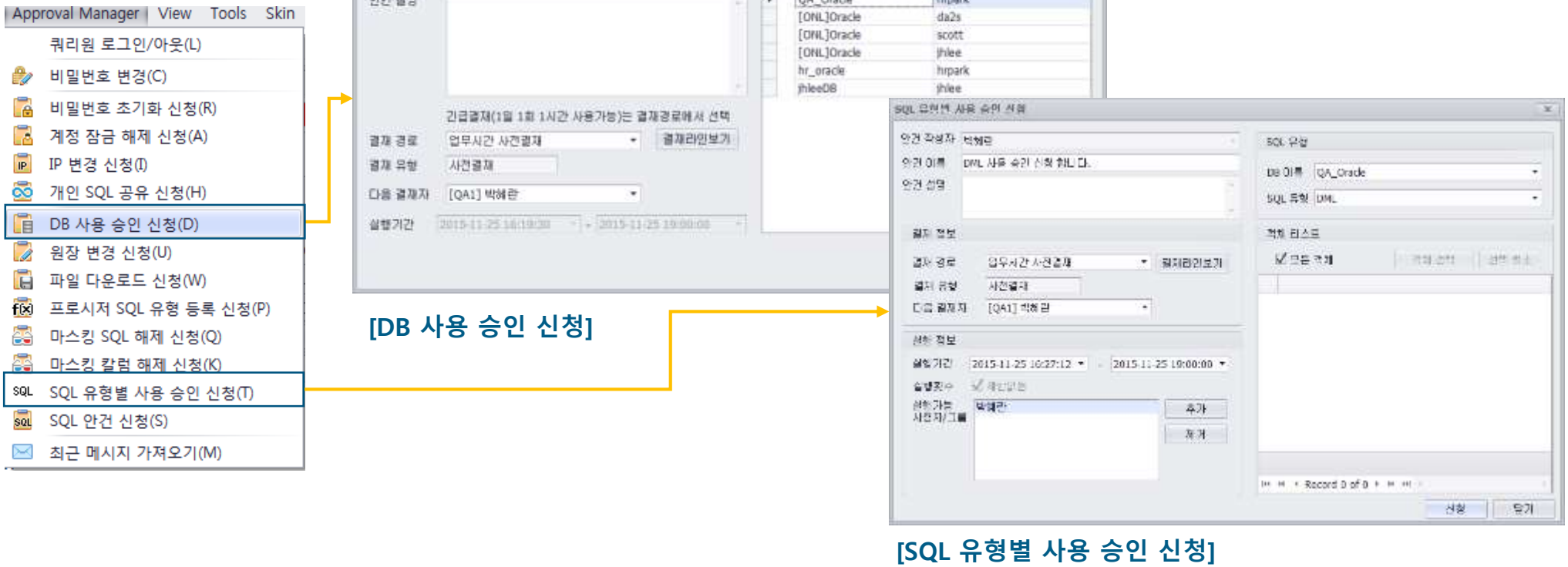


2.3 DB 작업통제 솔루션 주요 기능

❑ DB 사용 신청 및 SQL 유형별 사용 승인

- DB별 사용 권한은 관리자가 설정에 따르며, 자유롭게 사용/결재 후 사용/ 사용권한 없음으로 분류 할 수 있음
- SQL 유형(DDL ,DCL,DML 등)에 대한 분류도 가능하여 결재를 통해 사용 가능

SQL 유형별 사용 승인



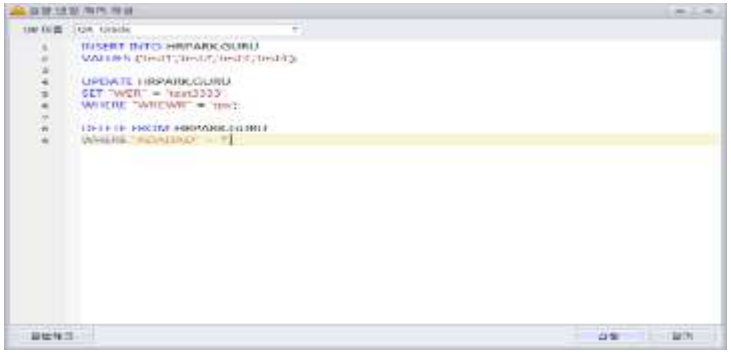
2.3 DB 작업통제 솔루션 주요 기능

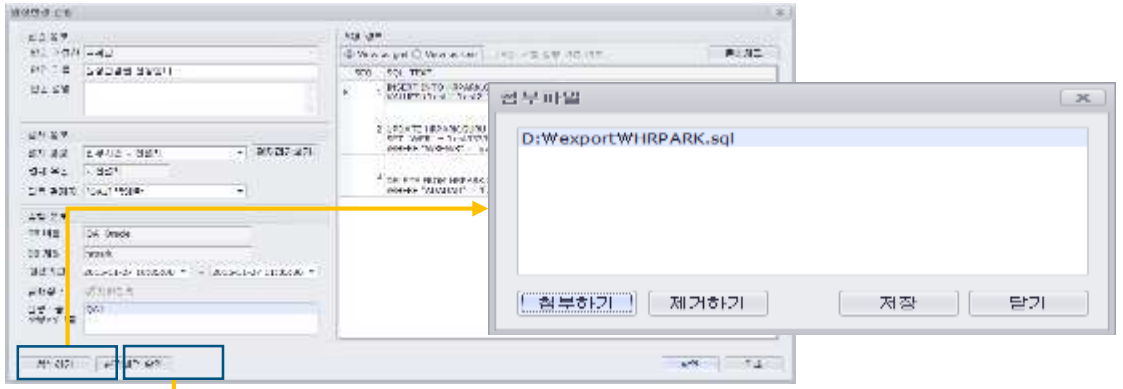
❑ 전자금융감독규정 제27조(전산원장 통제) 대응

- 원장 변경 쿼리를 작성 후 해당 쿼리에 대한 문법 체크를 진행하게 되며, 문법에 이상이 없을 경우 정해진 결재 루트를 따라 결재 진행
- 필요시, 첨부파일을 통해 원장 변경에 대한 사유를 첨부 (혹은 CSR No. 등을 기록)
- 결재자에 의해 원장 변경 신청이 최종 승인되면, 신청자는 특정 인원(DBA 등)에게 원장 변경 쿼리 수행을 위임

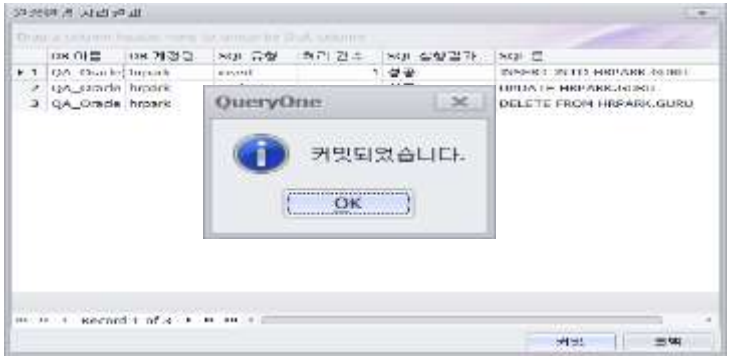
전산원장 통제 대응

[안건 작성]





[안건 승인]

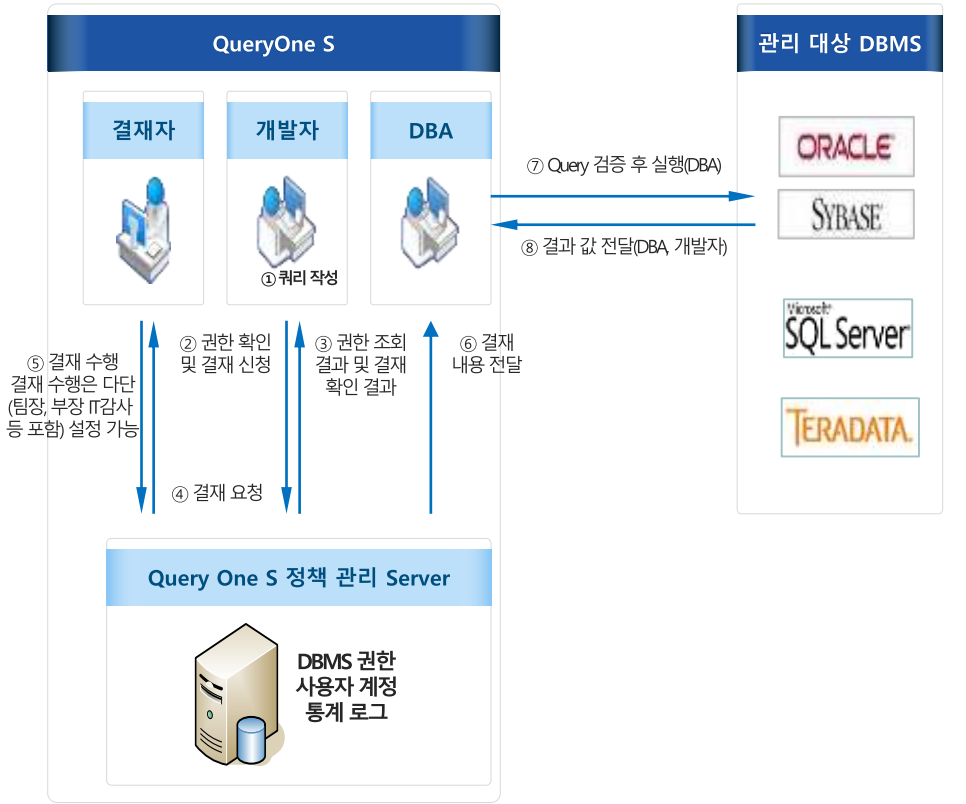


2.3 DB 작업통제 솔루션 주요 기능

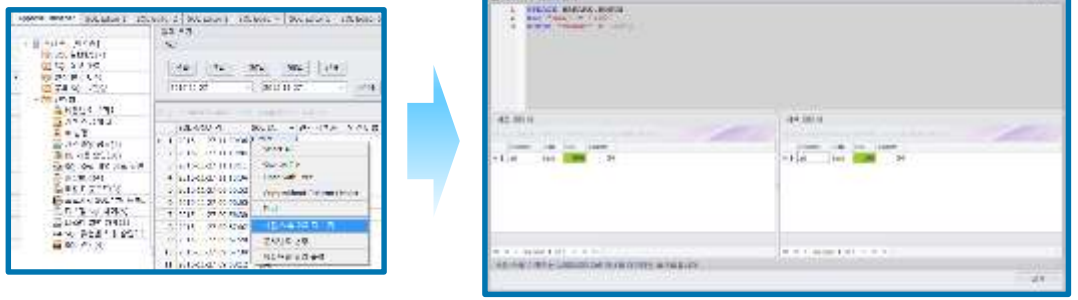
❑ 전자금융감독규정 제27조(전산원장 통제) 대응

- Insert/ Update/ Delete 등의 데이터 변경 수행시 결재자는 사전/사후 이미지를 확인하고 결재를 할 수 있으며, 해당 내용은 로그로 저장
- 변경된 데이터 중 기록할 데이터 건수는 QueryOne S Manager 에서 설정 가능
- QueryOne S Manager에서도 데이터 변경 이력 메뉴를 통해 사전/사후 이미지를 확인 및 변경 전/후 데이터는 색상이 적용되어 확인 가능

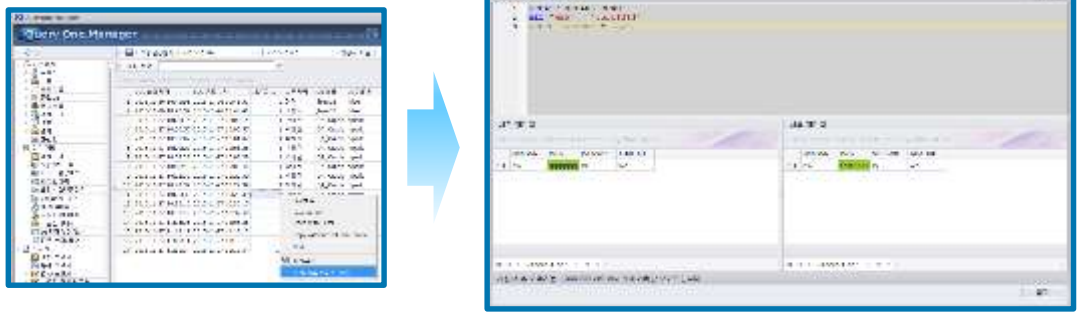
사전/ 사후 이미지 저장



[QueryOne S]



[QueryOne S Manager]

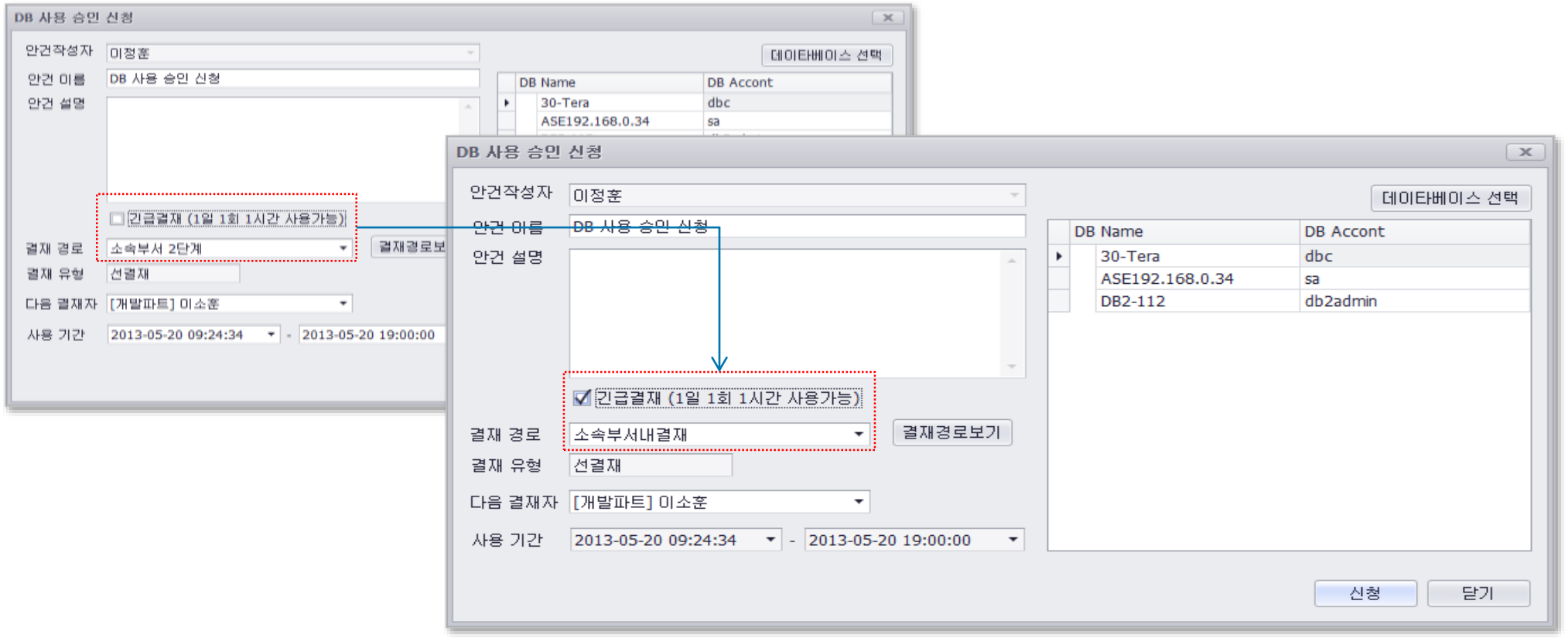


2.3 DB 작업통제 솔루션 주요 기능

❑ 긴급하게 운영 DB 사용이 필요한 경우 DB 사용 승인 신청

- 긴급하게 운영 DB 사용이 필요한 경우에는 긴급결재 신청 가능
- 긴급 결재 신청을 하게 되면 승인이 난 시점부터 1시간 동안 운영 DB를 사용할 수 있으며 1일 1회에 한정됨
- DB 사용 승인 신청 대화상자에서 긴급 결재를 체크하게 되면 긴급결재 신청이 되며 결재 경로가 바뀜

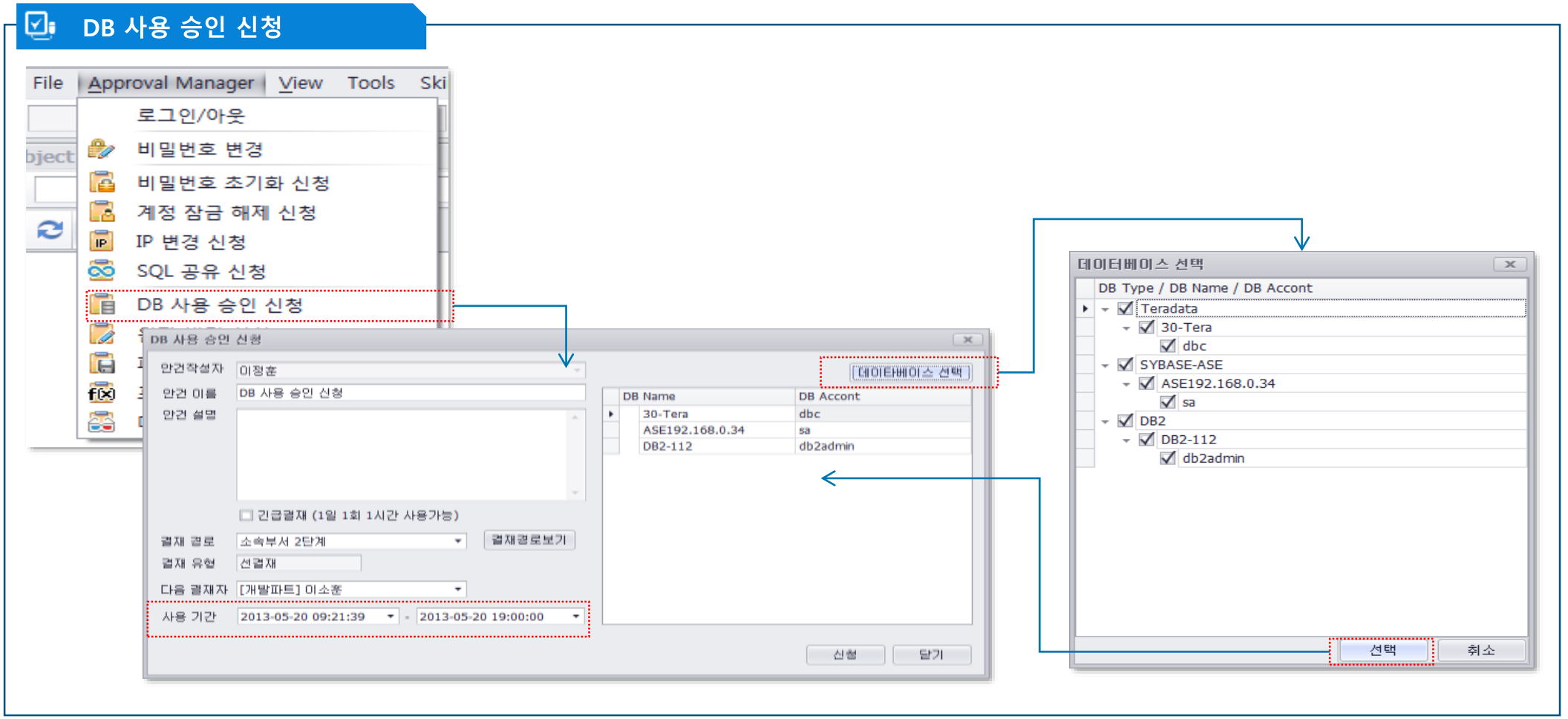
긴급결재 신청



2.3 DB 작업통제 솔루션 주요 기능

❑ "계정 발급 절차" 강화를 위한 DB 사용 승인 신청

- DB 사용 승인 신청을 통해 개인정보 등이 담겨있는 DB에 접근 및 사용이 가능 (전자금융감독규정 13조 10항, 전자금융감독규정 28조)
- 데이타베이스 선택 버튼을 클릭하여 사용하기를 원하는 운영 DB를 체크하고 선택버튼을 클릭
- 안건 이름 (필수항목)과 안건 설명, 결재자를 지정하고 신청 버튼을 클릭하면 신청이 완료

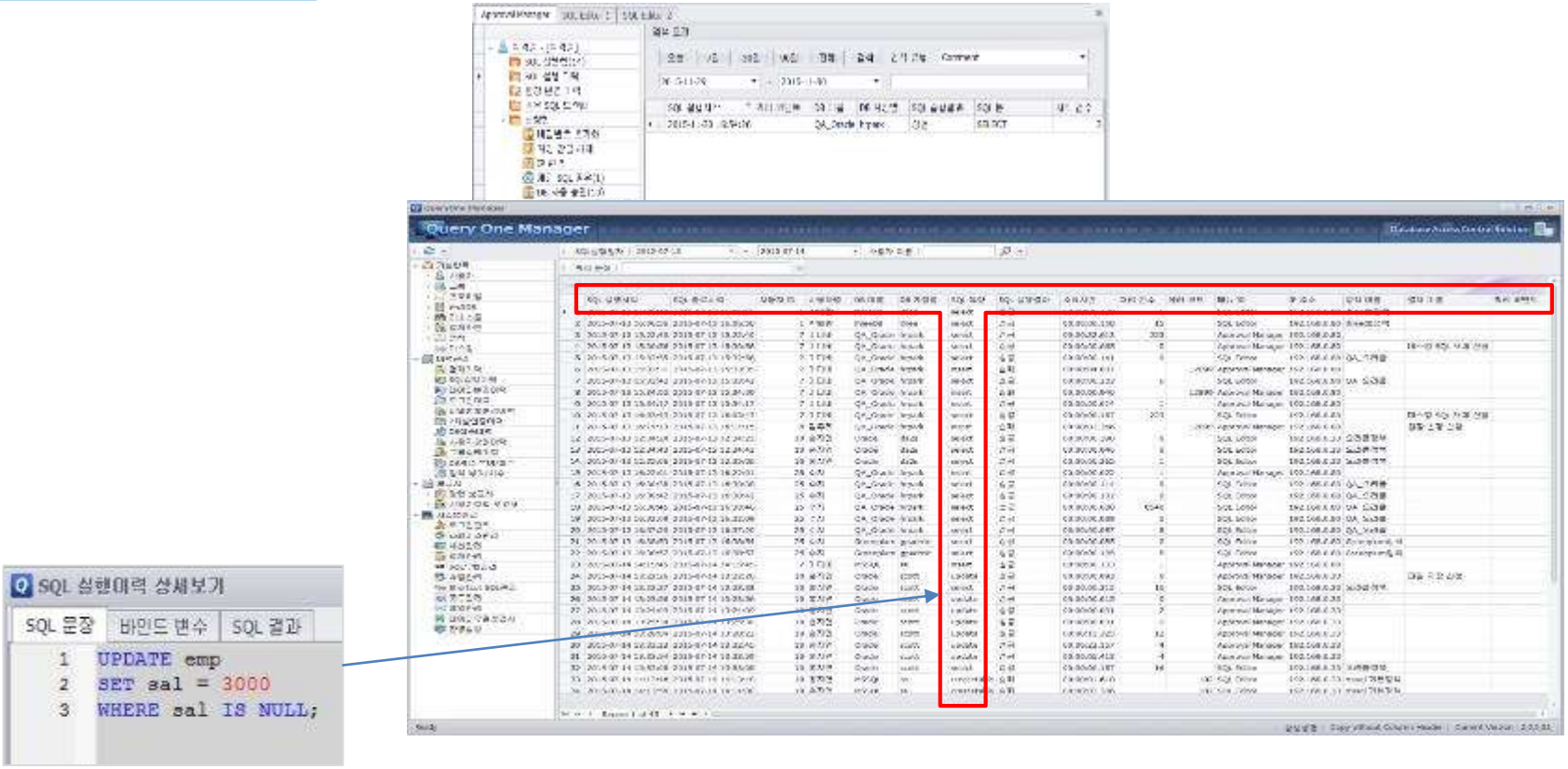


2.3 DB 작업통제 솔루션 주요 기능

❑ "작업 수행 통제" 강화를 수행 이력 관리

- SQL 실행 이력 메뉴를 통해 실행내역 확인 가능
- SQL 실행결과, SQL 유형, 조회건수, 소요시간 등을 확인 할 수 있음
- 수행 결과 저장 시 저장 ROW수 지정 가능, Manager의 SQL 실행 내역에서도 조회 가능
- 데이터 백업을 통해 장기간 수행 이력 관리 가능

수행 이력 관리

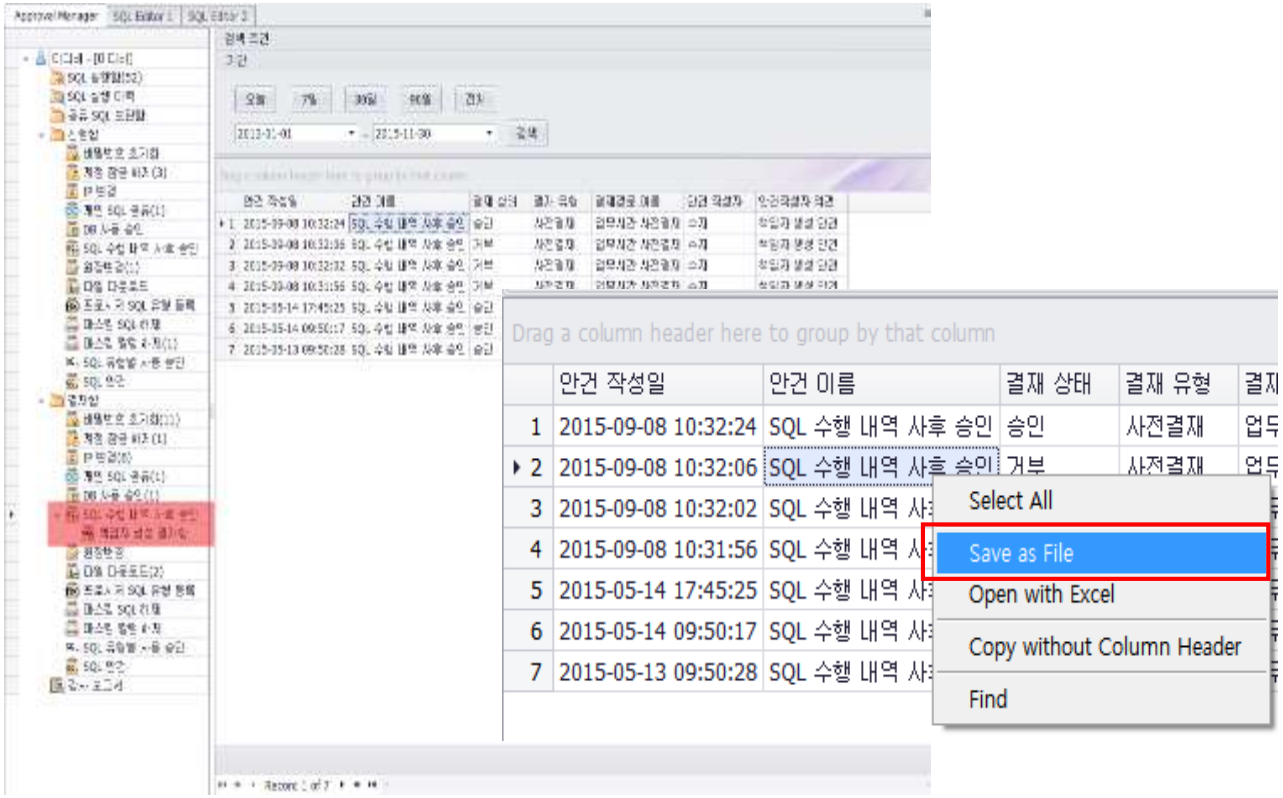


2.3 DB 작업통제 솔루션 주요 기능

❑ "작업 수행 통제" 강화를 사후 점검 절차

- 소속 부서, 소속 팀, 작업자, DB시스템, 일/주/월별, 기간별, 수행횟수, 결과건수 등에 따른 수행현황 조회
- 상기 수행현황 조회 결과에 대해 사후 점검자에 의한 결재기능 제공.
- SQL 수행 내역 사후 승인 메뉴를 통해 사후 승인 기능을 제공 하며, 해당 내역에 대한 파일 저장 가능
- 출력 가능한 문서 종류 : *.pdf, *.txt. *.xml, *.html, *.xls, *.csv

사후 점검 절차

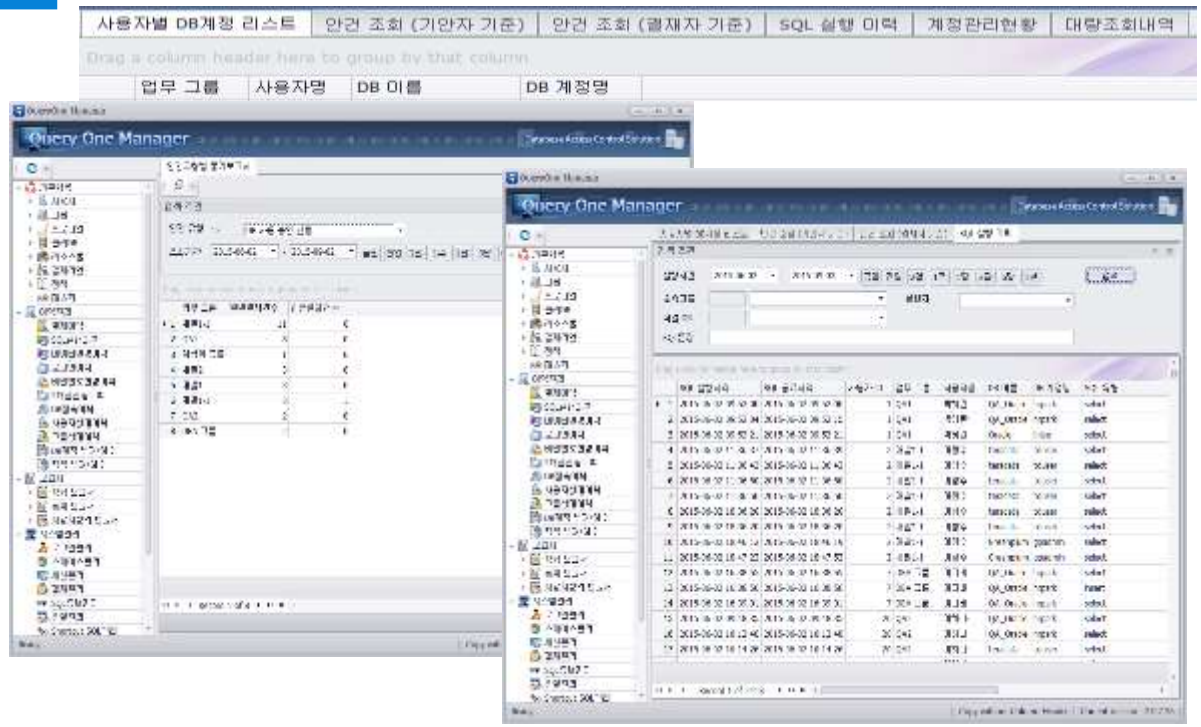


2.3 DB 작업통제 솔루션 주요 기능

❑ "작업 수행 통제" 강화를 보고서 유형

- 각종 SQL 수행이력에 대한 일/주/월/연간 각종 운영현황 및 점검 보고서 자동생성, 저장, 인쇄 기능 등
  - ☞ 날짜별/ 요일별/ 시간별/ DB시스템별/ 부서별 수행횟수, 수행횟수 기준 상위 작업자 등
- Manager 에서 보고서 형태에 따라 각종 SQL 수행 이력을 조회, 저장 할 수 있습니다.
- 정형보고서(사용자별 DB 계정 리스트, 안건 조회, SQL실행이력, 계정관리현황, 대량조회 내역), 통계보고서(안건유형별 통계보고서), 감사보고서, 사용자정의 보고서
- 사용자 정의 보고서에서 보고서 작성을 위한 쿼리문을 입력 수 결과 가져오기를 통해 보고서 형태의 결과를 출력할 수 있음

보고서 유형



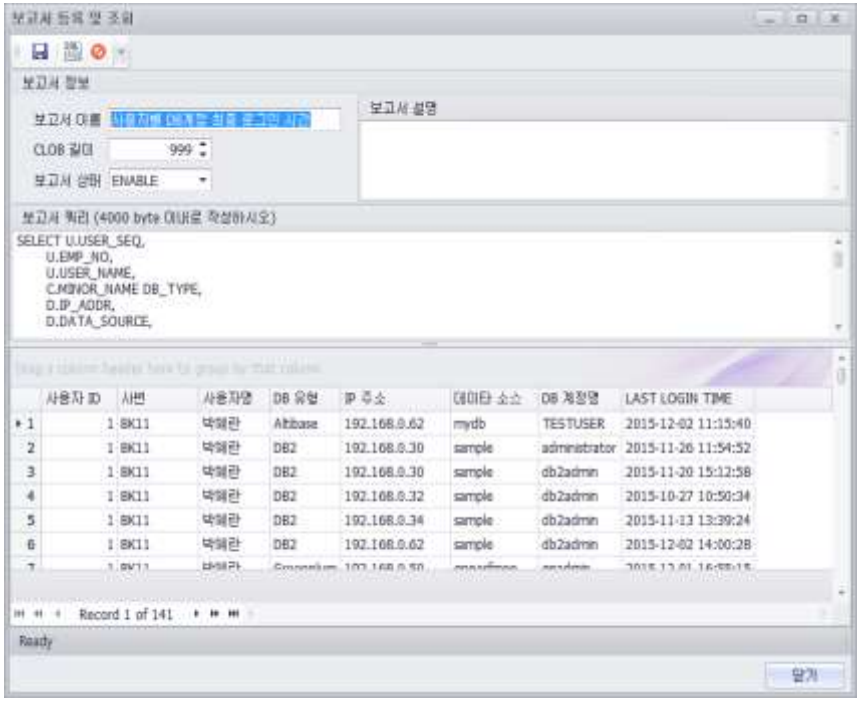
2.3 DB 작업통제 솔루션 주요 기능

❑ "작업 수행 통제" 강화를 사용자 정의보고서

- SQL 수행 패턴 분석을 통한 각종 보고서, 생성, 저장, 인쇄기능 등
  1> 작업자 기준 테이블별 접근횟수
  2> 테이블 기준 접근 횟수 상위 작업자
  3> 부서별 상위 SQL 수행 신청자 등
- 요구하는 보고서 외에 SQL 실행 시각, SQL 종료시각, 사용자, DBMS 기준, Table별, DBMS 계정별, SQL 유형별, SQL 실행 성공/실패, 소요시간, 처리건수, 에러발생기준, 정책이름기준, 수행IP기준 을 조건으로 조합하여 리포트 생성이 가능함

사용자 정의보고서

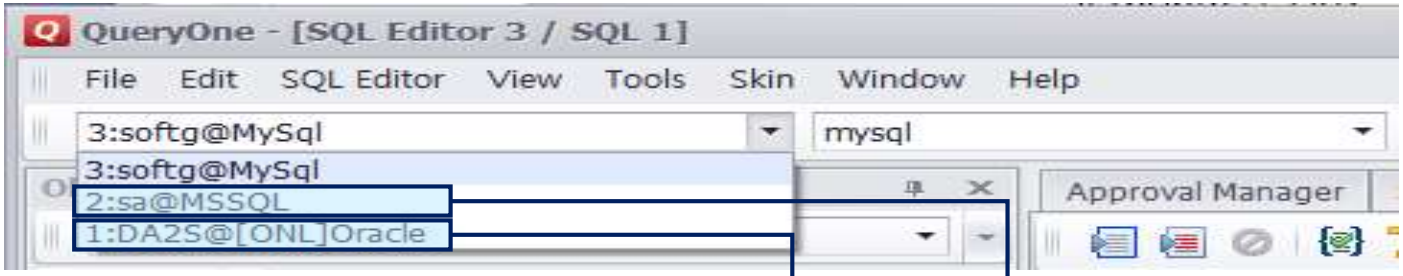
SQL 실행시각	+	사용자	+	Table별
+		+		+
SQL 종료시각	+	SQL 실행 성공/실패	+	처리건수
+		+		+
SQL 유형별	+	수행IP기준	+	에러발생기준
+		+		+
DBMS 계정별	+	정책이름기준	+	소요시간



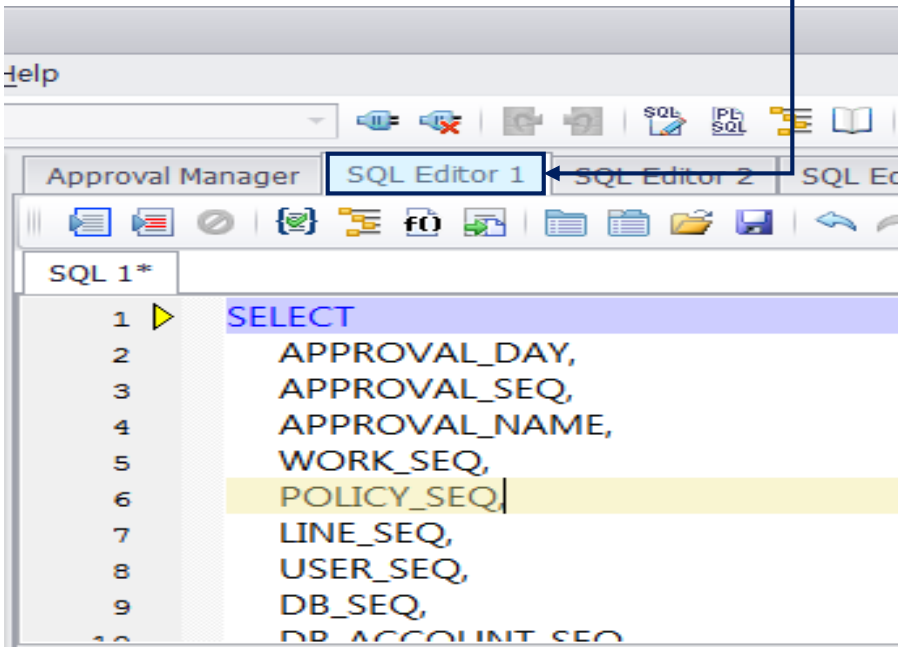
2.4 DB 작업통제 솔루션 DB Tool 기능

❑ 단일 화면에서 서로 다른 DB별로 세션 접속이 가능

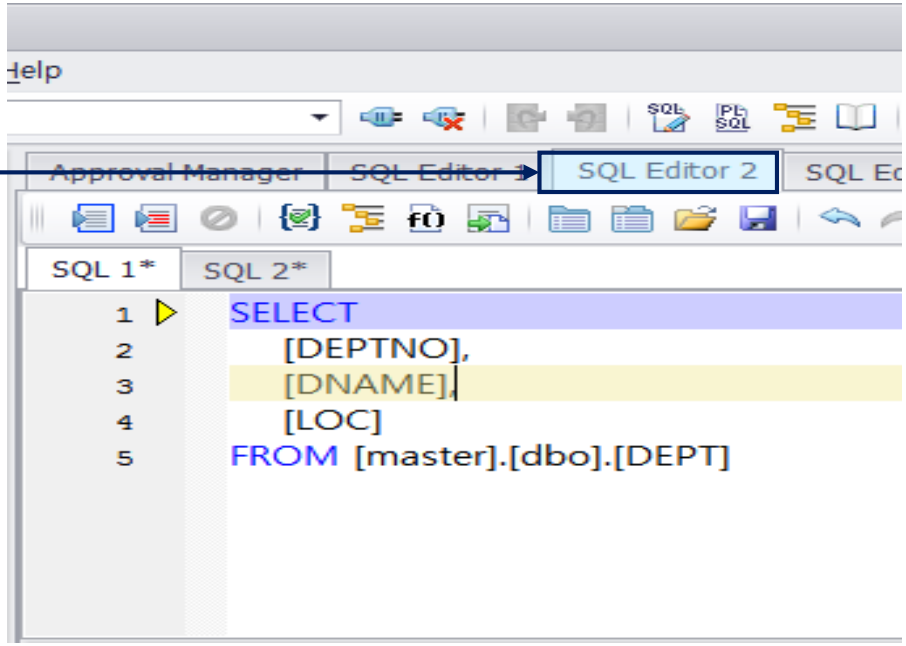
[Oracle과 MSSQL 동시 접속]



[Tab1에서 Oracle SQL 지원]



[Tab2에서 MSSQL 지원]

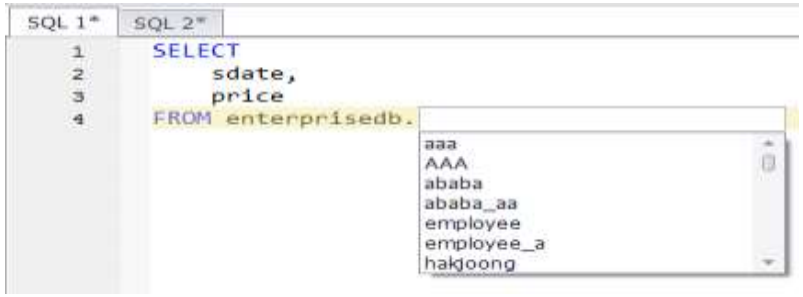


2.4 DB 작업통제 솔루션 DB Tool 기능

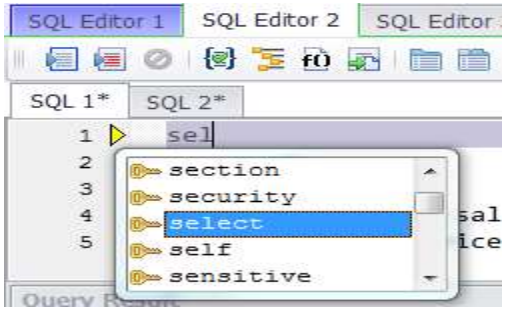
❑ SQL Editor

- SQL 편집 및 실행 기능
- Bind 변수, SQL Formatting, 문법 검사, 실행 계획 등의 기본적인 기능 지원
- 자동 완성 기능과 Intellisence 기능 지원
- SQL History와 개인 SQL 관리를 위한 Named SQL 제공

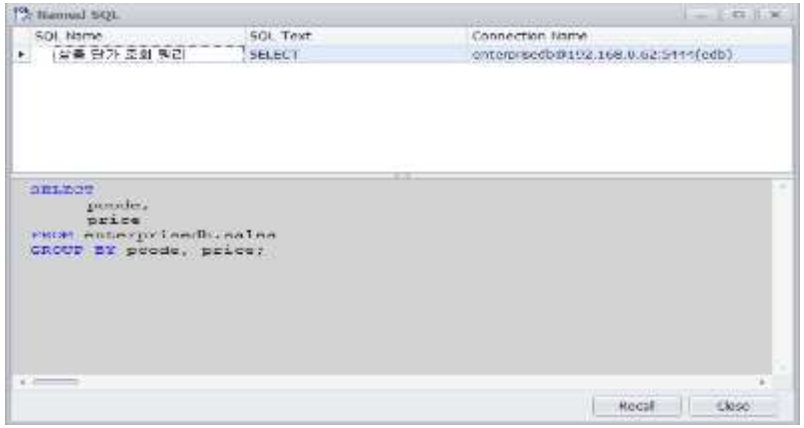
[자동 완성 기능]



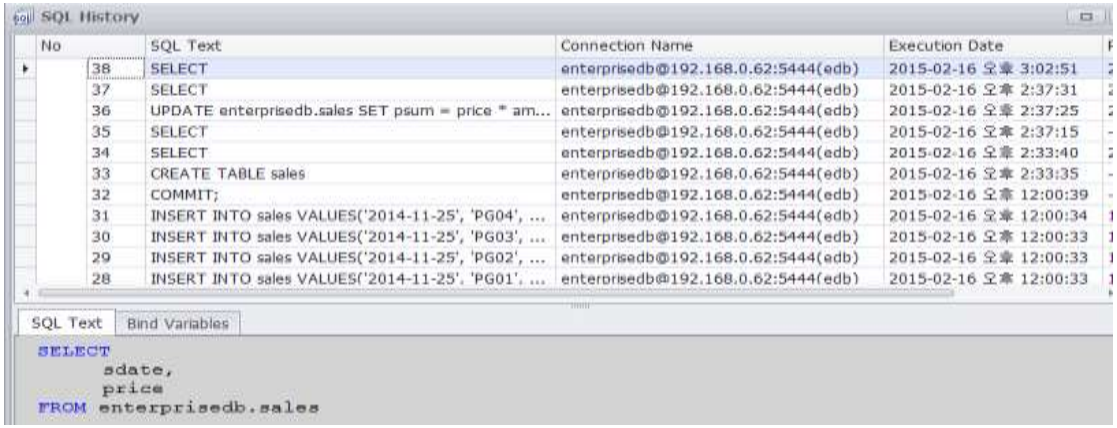
[Intellisence기능]



[Named SQL]



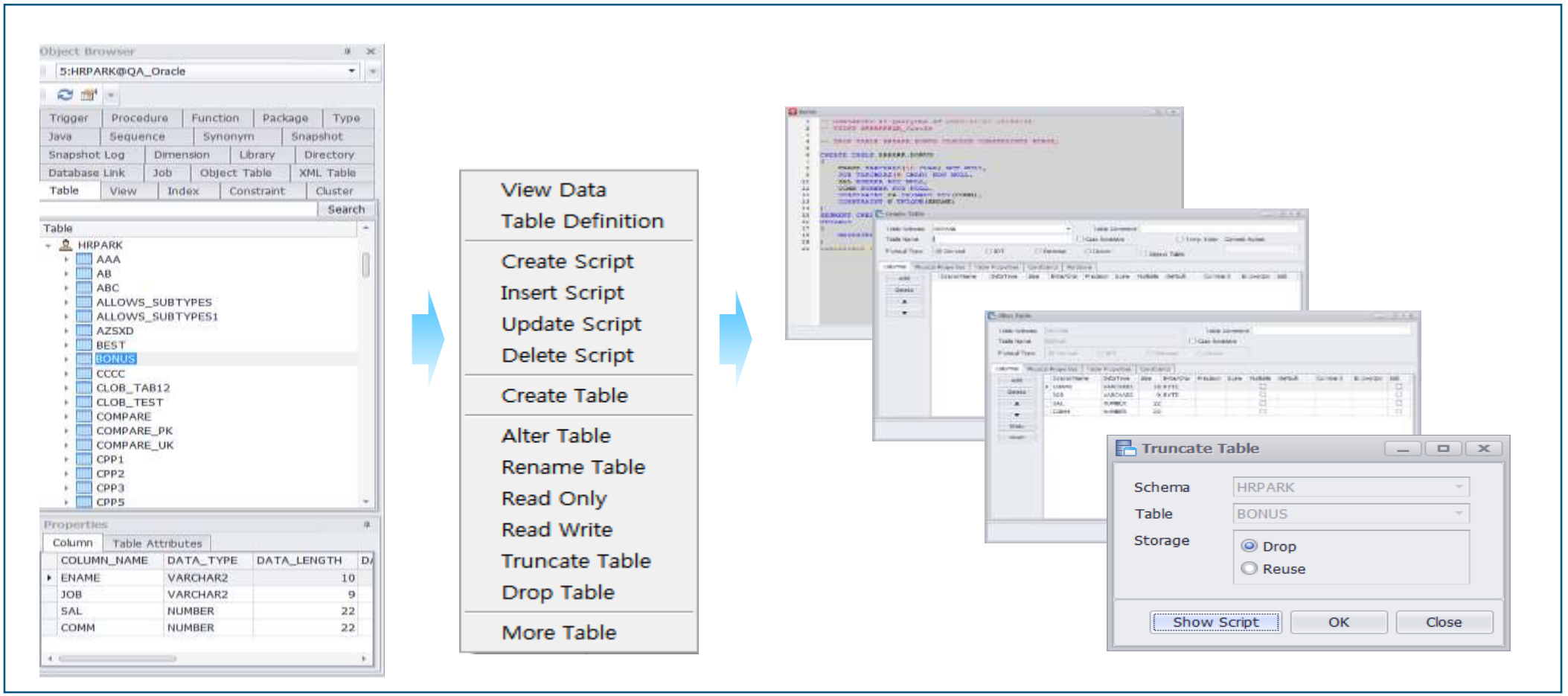
[SQL History]



2.4 DB 작업통제 솔루션 DB Tool 기능

❑ Object Browser

- Table, View, Index, Procedure등 DB Object를 관리
- 테이블 조회, 생성 및 변경
- Script 조회 및 생성 기능 제공

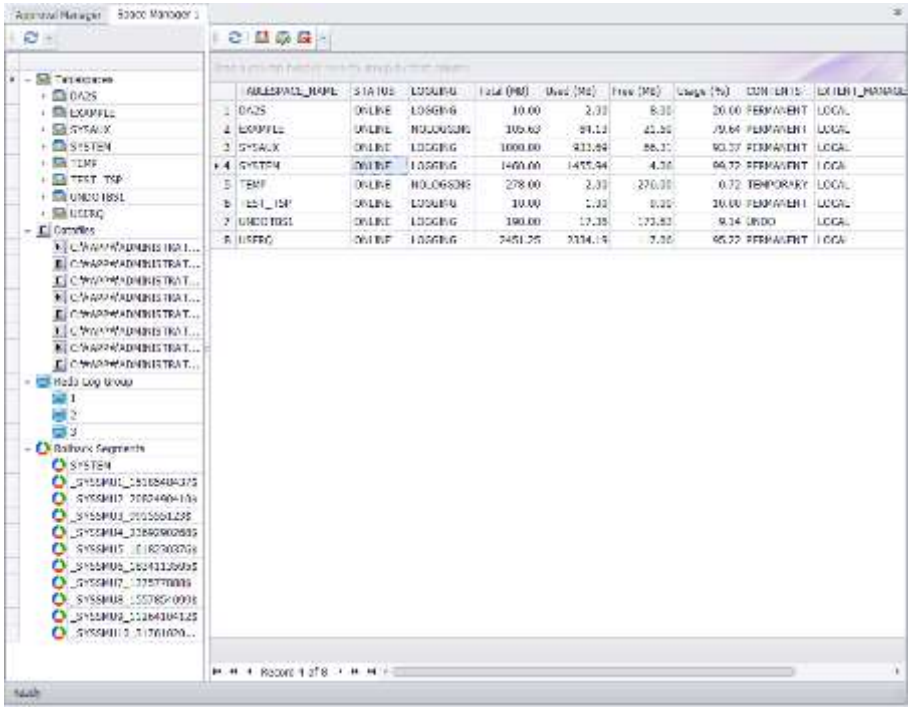


2.4 DB 작업통제 솔루션 DB Tool 기능

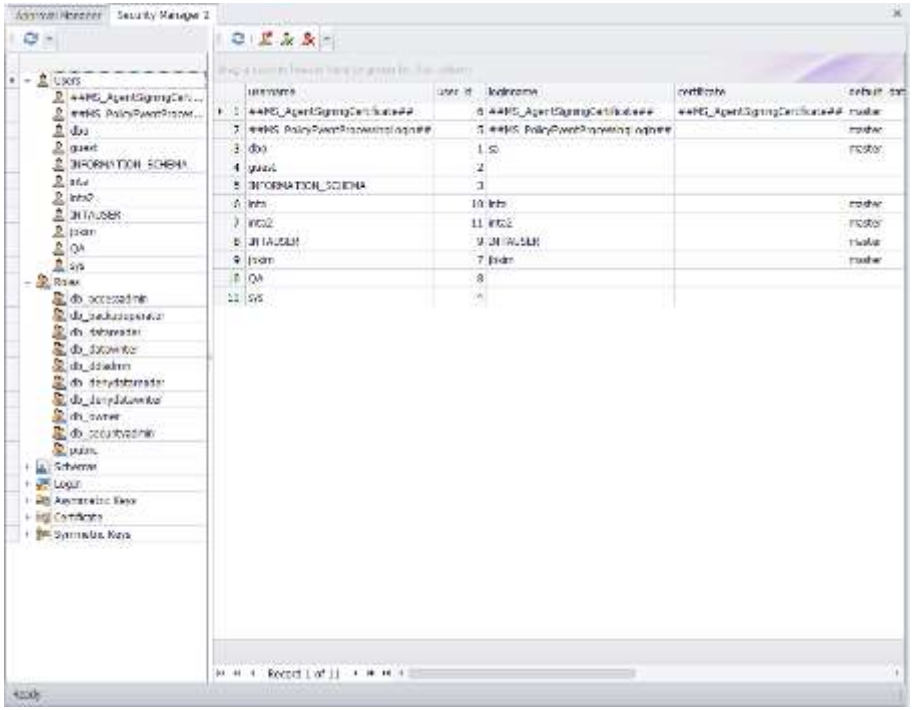
❑ Manager

- Space Manager – 테이블 스페이스, 데이터 파일 등의 데이터 공간을 효율적으로 관리
- 전체공간(Total), 사용한 공간(Used), 남은 공간(Free) 등으로 나누어 사용현황을 볼 수 있으며 테이블스페이스의 파일 생성/변경/삭제가 가능
- Security Manager – User, Role 등의 사용자에 대한 정보를 조회 및 변경
- User, Role등의 생성, 수정, 삭제 및 권한부여, 권한제거 등의 조작이 가능 및 부여된 권한을 Object기준으로 조회가 가능

[Space Manager]



[Security Manager]

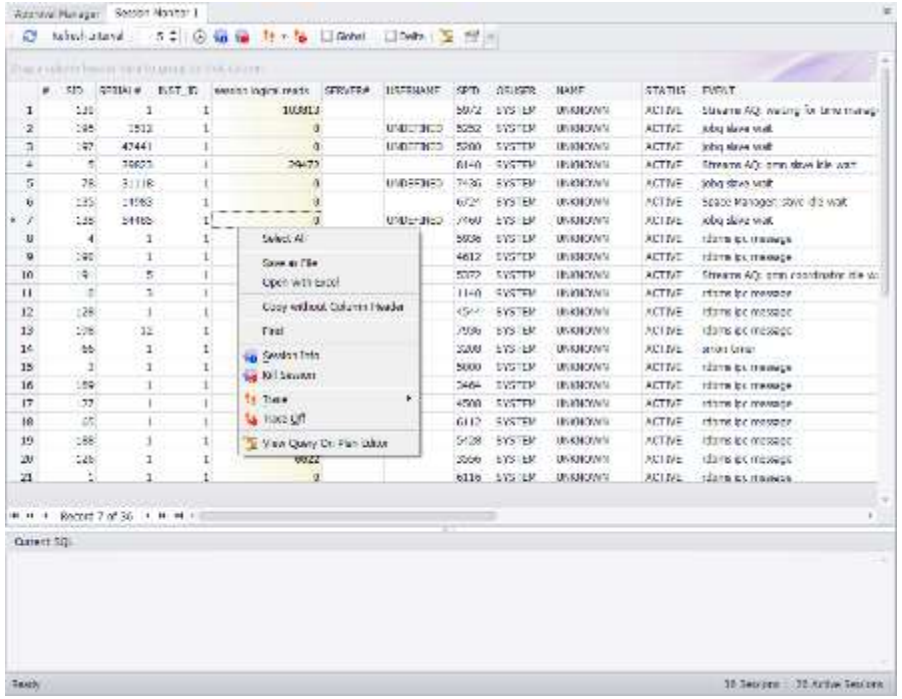


2.4 DB 작업통제 솔루션 DB Tool 기능

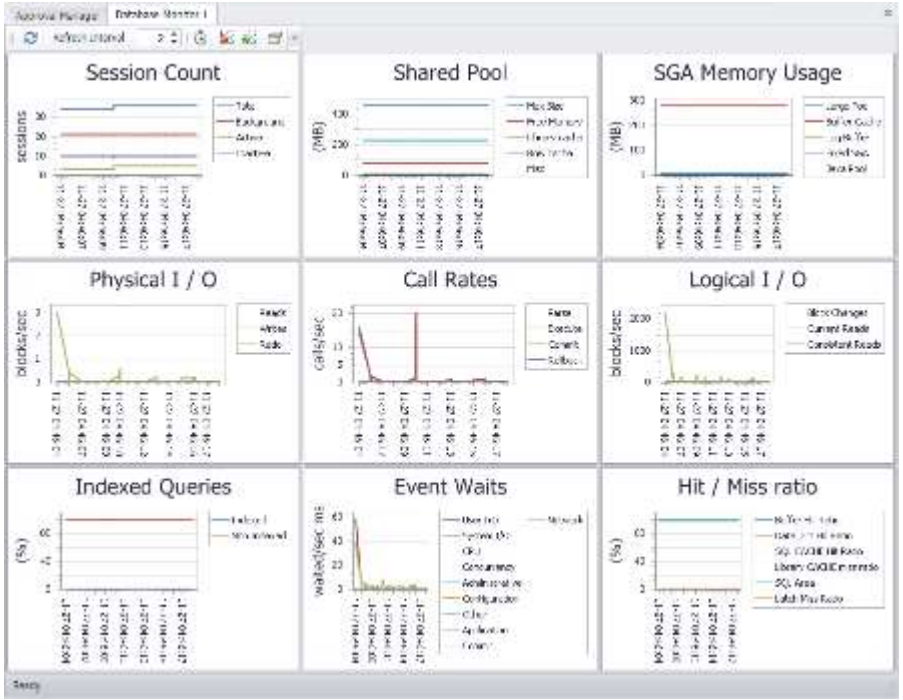
❑ Monitor

- Session Monitor - 각 DB별로 세션 접속 상태를 조회 할 수 있음
- 상세 세션 정보 조회와 문제가 있는 세션의 접속을 끊을 수 있으며 최종 실행된 Query를 확인 및 일정 시간 간격으로 갱신하여 모니터링 가능
- Database Monitor - DB내의 통계 데이터들을 차트로 확인 및 각 차트를 더블클릭 하면 큰 화면으로 전환이 가능

[Session Monitor]



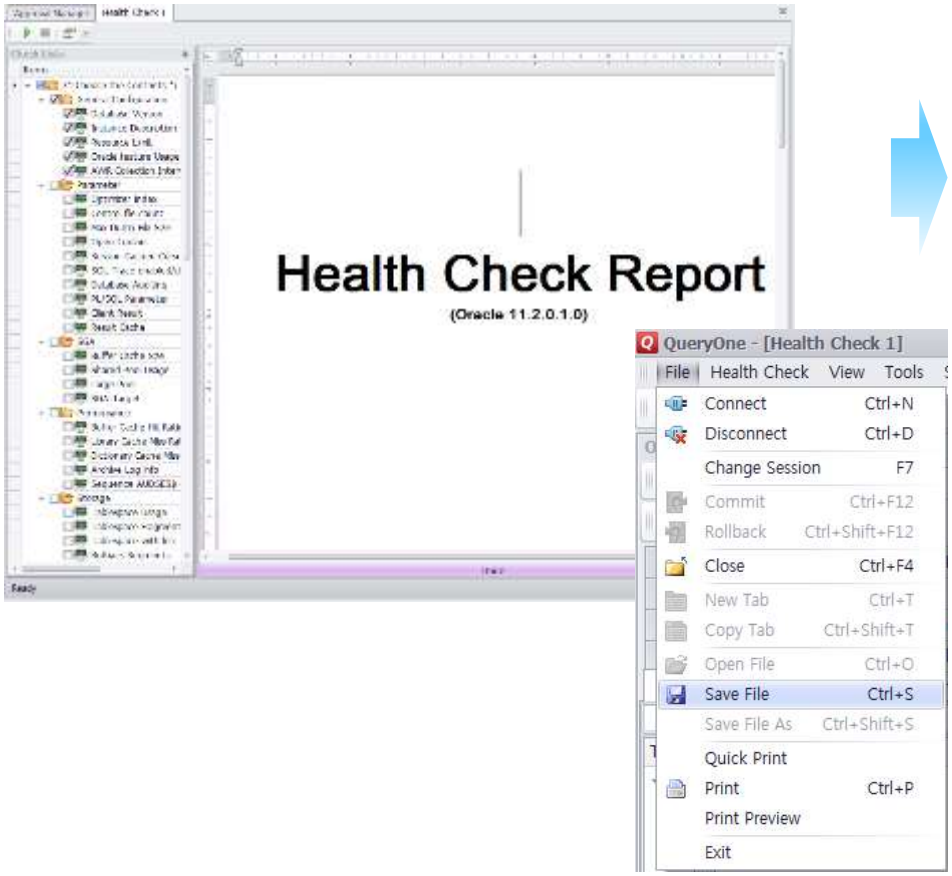
[Database Monitor]

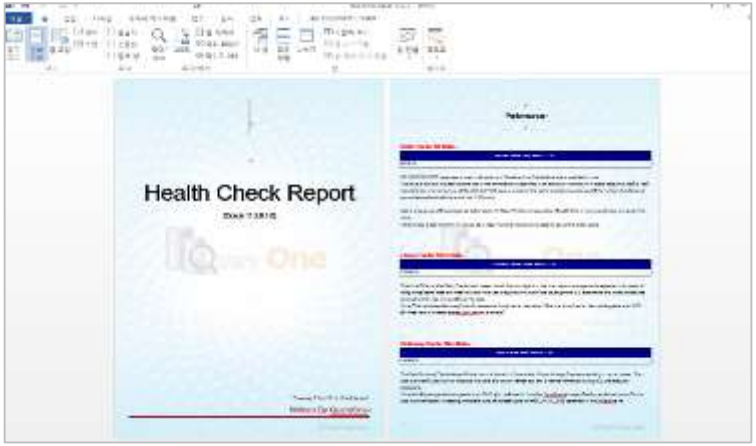


2.4 DB 작업통제 솔루션 DB Tool 기능

❑ Health Check

- 데이터 베이스 시작 이후에 대한 통계, 성능 관리에 대한 내용을 문서화 가능
- 체크 리스트에서 현재 DB의 체크 가능한 항목을 선택하여 문서화 (ex. Parameter, Wait Event, Performance등)
- 문서화된 결과를 보고서 형태의 파일(RTF, PDF, HTML, DOCX) 로 출력 가능





2.5 DB 작업통제 솔루션 주요 구축 사례

❑ S은행, 삼성생명 등 대규모 금융 사이트에 적용하여 운영

사업명	사업기간	발주처	비고
QueryOne도입	2015.12 ~	SK C&C	저축은행중앙회
DBMS 보안 툴 도입	2015.11 ~ 2015.12	삼성생명	
신한금융투자 데이터베이스 보안 강화 솔루션 도입	2015.11 ~ 2015.12	신한금융투자	
보안 데이타베이스 사용툴 도입(증설)	2015.11 ~ 2015.11	비에스인포	현대라이프생명
세븐럭 카지노 센터이전 및 인프라 재구축	2015.10 ~ 2015.11	벨정보시스템	그랜드코리아레저
QueryOne	2015.09 ~ 2015.11	피앤피시큐어	라이나생명
강남가스 DB보안시스템 구축(증설)	2015.02 ~ 2015.03	다우기술	강남도시가스
정보계 시스템 보안 쿼리툴 도입	2014.12 ~ 2015.02	삼성생명	
보안 데이타베이스 사용툴 도입	2014.09 ~ 2014.11	비에스인포	현대라이프생명
그룹공통업무 보안솔루션(증설)	2014.05 ~ 2014.06	신한데이타	신한금융지주
DB통제강화 S/W	2014.01 ~ 2014.03	신한은행	
그룹공통업무 보안솔루션	2013.12 ~ 2014.02	신한데이타	신한금융지주
강남가스 DB보안시스템 구축	2013.11 ~ 2013.12	GSITM	강남가스
DBMS 사용자 통제강화시스템	2013.04 ~ 2013.06	신한은행	

2.5 DB 작업통제 솔루션 주요 구축 사례

❑ S은행은 DB 암호화 솔루션(CubeOne)를 도입하여 API 암호화를 적용하였음

- 중요 정보의 암호화 적용을 통한 고유식별정보의 유출 가능성 원천 방지
- 개인정보보호법 및 신용정보법 등 암호화 관련 법규에서 요구하는 보안 수준 준수(“개인정보취급자 " 의 접근권한 통제)

암호화 적용 전

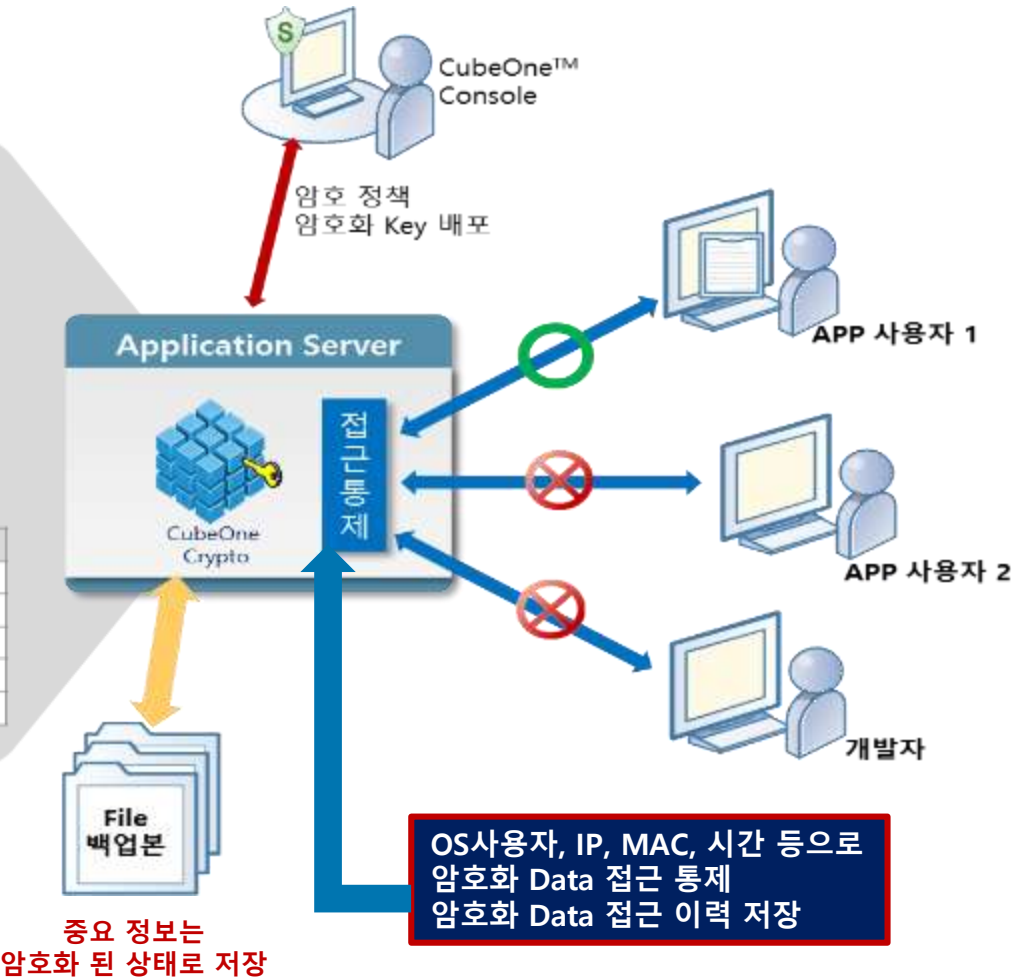
card_no	name	address	tel
212131314141	이몽룡	서울 강남 선릉 702-2	4077675
222232324242	성춘향	성 무신 322	3273849
232333334343	고주몽	강원 태 명륜 107	4458989
242434344444	임꺽정	충남 서산 효자 654-2	9763456
252535354545	홍길동	광주 서구 금남 107	3307636

Data를 암호화 상태로
영구적으로 변환

암호화 적용 후

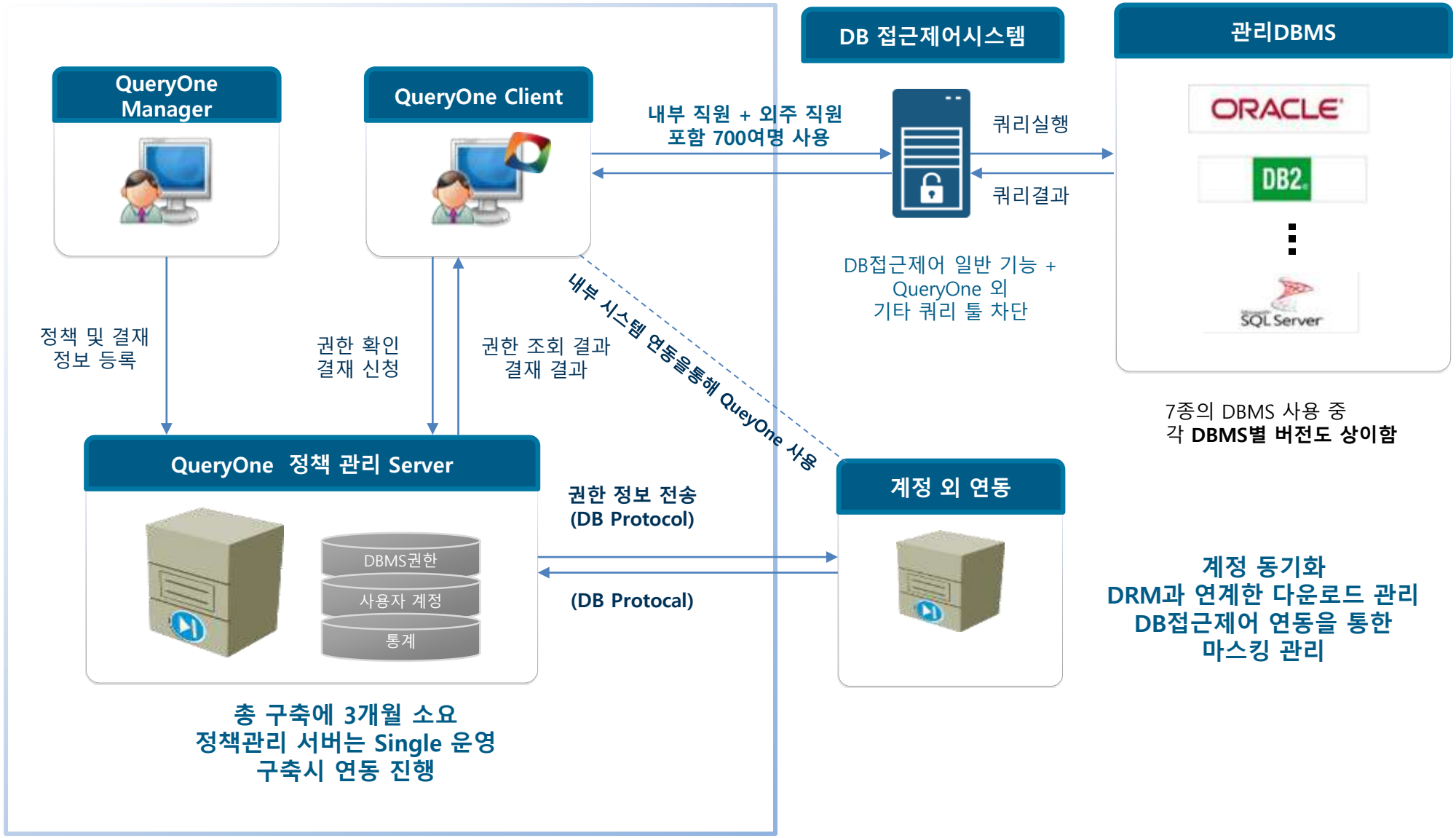
card_no	name	address	tel
HJDFGJHSFDSKJFDK	KDJHFSHIQUWIEWHU	서울 강남 선릉 702-2	4077675
EUYWRDBHJHHXDSLK	IEUWYRFGHVJKDFOE	무신 322	3273849
NCEIWOINCDIUBCNC	YUTEWFGHBVDJHFBV	태백 명륜 107	4458989
OEWJIRJCDKNIWJER	TYGUHJGVFDCIUKHG	충남 서산 효자 654-2	9763456
MXSKLOAWOQWUDHIQ	RYUEFHJCNIUQJSSK	광주 서구 금남 107	3307636

※ 신용정보법, 신용정보업 감독규정
접근권한을 서비스제공을 위하여 필요한 최소한의 인원에게만 부여하고, 개인신용정보취급자의 업무가 변경되었을 경우 지체 없이 개인신용정보처리시스템의 접근권한을 변경 또는 말소.



2.5 DB 작업통제 솔루션 주요 구축 사례

❑ S은행 구축 사례



3.1 금감원 DB 운영 통제 검사 개요

❑ 금감원 DB 운영 통제 검사 대응 목적

▣ 금감원 검사 대응 및 내부 통제 강화

- 금감원 IT보안 검사 개선 사항에 대하여 선도적으로 대응하고, 내부 통제 방안의 수립 및 적용
- 데이타베이스에 대한 접근권한 부여 기준, 통제절차 수립 및 준수로 주민등록번호를 포함하는 고객정보 보호
- 데이타베이스에 대한 접근권한 부여 내역의 전산기록과, 관리책임자, 보안관리자 등의 확인 및 관리
- 데이타베이스 직접접속 작업에 대한 자동화된 책임자 승인을 통한 사전 통제로 고객정보 유출 등 보안사고 방지
- 데이타베이스 직접접속 작업 수행 내용에 대한 기록 및 수행 내역 검사를 통한 사후 통제

▣ 데이터베이스 운영 통제 관련 전자금융감독규정 준수

관련 규정	데이터베이스 운영 통제 관련 전자금융감독규정 상세 내역
제13조 (전산자료 보호대책)	① 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용 1. **사용자계정과 비밀번호를 개인별로 부여**하고 등록·변경·폐기를 체계적으로 관리할 것 2. 외부사용자에게 사용자계정을 부여하는 경우 **최소한의 작업권한만 할당**하고 적절한 통제장치를 갖출 것 4. 전산자료의 입력·출력·열람을 함에 있어 **사용자의 업무별로 접근권한을 통제**할 것 10. **이용자 정보의 조회·출력에 대한 통제**를 하고 테스트 시 이용자 정보 사용 금지 13. **단말기에 이용자 정보 등 주요정보를 보관하지 아니하고**, 단말기를 공유하지 아니할 것 14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 **계정 변경 등 접근을 통제**
	③ 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 자동적으로 기록 하고, 그 기록을 1년 이상 보존
	⑤ 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용 다만, 정보처리시스템 관리자의 **주요 업무 관련 행위는 책임자가 제28조 제2항에 따라 이중확인 및 모니터링**
제23조 (비상대책 등의 수립·운용)	① 장애·재해·파업·테러 등 긴급한 상황긴급한 상황이 발생하더라도 업무가 중단되지 않도록 업무지속성 확보방안을 수립·준수 **2. 백업 또는 재해복구센터를 활용한 재해복구계획**
제27조 (전산원장 통제)	① 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용
제28조 (거래통제 등)	② 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 **중요작업 수행 시 책임자가 이중확인**
제30조 (일괄작업에 대한 통제)	1. 일괄작업은 **작업요청서에 의한 책임자의 승인**을 받은 후 수행할 것 5. 책임자는 **일괄작업 수행자의 주요업무 관련 행위를 모니터링**할 것

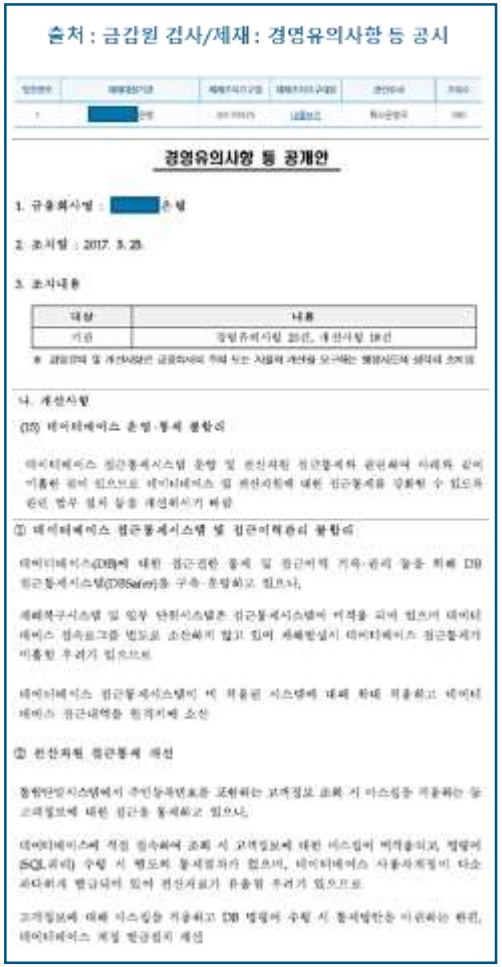
3.2 I은행 금감원 데이터베이스 운영 통제 검사 공시 내용

❑ 데이터베이스 운영 통제 개선사항

▪ 데이터베이스 접근통제시스템 운영 및 전산자원 접근통제와 관련하여 아래와 같이 미흡한 점이 있으므로 데이터베이스 및 전산자원에 대한 접근통제를 강화할 수 있도록 관련 업무 절차 등을 개선하시기 바람

개선 구분	개선 사항
데이터베이스 접근통제시스템 및 접근이력관리 불합리	데이터베이스(DB)에 대한 접근권한 통제 및 접근이력 기록 관리 등을 위해 **DB접근통제시스템(DBSafer)을 구축 운영**하고 있으나, **재해복구시스템 및 일부 단위시스템은 접근통제시스템이 미적용** 되어 있으며 데이터베이스 **접속로그를 별도로 소산하지 않고** 있어 재해발생시 데이터베이스 접근통제가 미흡할 우려가 있으므로 **데이터베이스 접근통제시스템이 미 적용된 시스템에 대해 확대 적용**하고 **데이터베이스 접근내역을 원격지에 소산**
전산자원 접근통제 개선	**통합단말시스템에서 주민등록번호를 포함하는 고객정보 조회 시 마스킹을 적용**하는 등 고객정보에 대한 접근을 통제하고 있으나, 데이터베이스에 **직접접속하여 조회 시 고객정보에 대한 마스킹이 미적용**되고, **명령어(SQL쿼리) 수행 시 별도의 통제절차가 없으며**, 데이터베이스 **사용자계정이 다소 과다하게 발급**되어 있어 전산자료가 유출될 우려가 있으므로 **고객정보에 대해 마스킹을 적용**하고 **DB 명령어 수행 시 통제방안을 마련**하는 한편, **데이터베이스 계정 발급절차 개선**

출처 : 금감원 검사/제재 : 경영유의사항 등 공시



경영유의사항 등 공개안

※ 개선사항은 금융회사의 주의 또는 자율적개선을 요구하는 행정지도적 성격의 조치임

3.3 데이터베이스 운영 통제 검사 대응 현황

❑ 데이터베이스 운영 통제 현황

- 기존에는 계정 및 접근통제 위주로 검사를 진행하였으나 현재는 "**권한 있는 사용자의 행위**"에 대한 작업통제를 검사
- I은행 검사에서는 **DB접근제어 솔루션의 적용 여부** 및 작업 수행 시 **작업 내용(조회 포함)에 대한 책임자 결재 처리를 통한 이중확인** 등 적절한 통제 수행 여부에 대하여 검사를 진행함
- I은행은 **DB 명령어 수행 시 통제를 위한 책임자 승인** 등 DB 직접접속 작업통제 등에 대하여 개선사항을 요구 받음

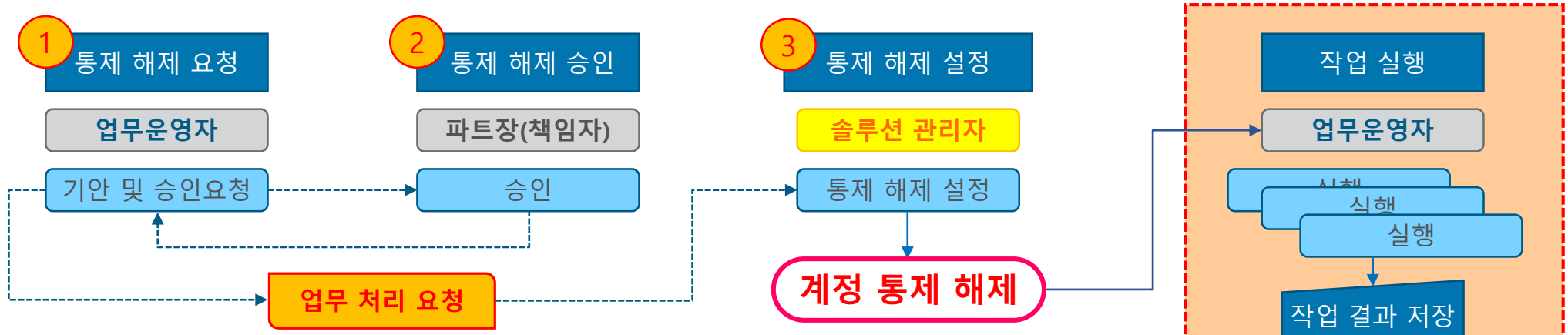
개선 사항	통제 항목	감독규정 준수를 위한 통제 상세 내역	I은행	S은행	비고
접근통제시스템 추가 적용	**접근통제 확대**	• **전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제** • 운영 및 재해복구 등 모든 DB서버에 대해서 접근통제 시스템을 적용하여 통제	△	O	
접근내역을 원격지에 소산	**재해 복구 대책**	• **백업 또는 재해복구센터를 활용한 재해복구계획 수립 및 적용** • 운영센터의 접근통제 정책을 재해복구 센터에 소산하여 재해시 업무지속성 확보	X	O	
고객정보에 대해 마스킹 적용	**마스킹 적용**	• 주민등록번호 등 개인정보에 대해서는 조회 시 마스킹 처리하여 정보 유출을 방지	△ (부분적용)	O	
		• 마스킹 해제가 필요한 경우 조회 조건별로 **책임자 승인** 후 해제	X	O	
DB 명령어 수행 시 통제방안을 마련	**명령어 통제**	• 전산원장, 고객정보 등 중요 시스템에 대한 **중요작업 수행 시 책임자가 이중확인**	△	O	
	조회 관리	• **전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제** • 주민등록번호를 포함하는 고객정보는 조회 가능 기준을 수립하고 개인정보취급자 등이 업무상 필요한 경우 **책임자 승인** 후 조회	△ (책임자 승인 X)	O	
	다운로드 관리	• **단말기에 이용자 정보 등 주요정보를 보관하지 말고, 불가피한 경우 책임자 승인** • PC 저장 및 복사 등을 금지하며, 업무상 필요한 경우 **책임자 승인** 후 저장 • 개인정보를 단말에 저장하는 경우 DRM 솔루션과 연동하여 자동으로 DRM 적용	△ (책임자 승인 X)	O	
데이터베이스 계정 발급절차 개선	**계정 관리**	• **DB 직접접속 권한을 부여하는 경우 필요한 최소한의 인원에게 최소한의 범위로 제한** • DB 사용 권한을 관리자가 분배하여 DB 계정 정보 유출 없이 DB 접속 가능하도록 관리 • DB 직접접속 계정은 개인별로 부여하고, 사용자 인사조치시 접근을 통제	△	O	

3.3 데이터베이스 운영 통제 검사 대응 현황

❑ 데이터베이스 운영 통제 비교

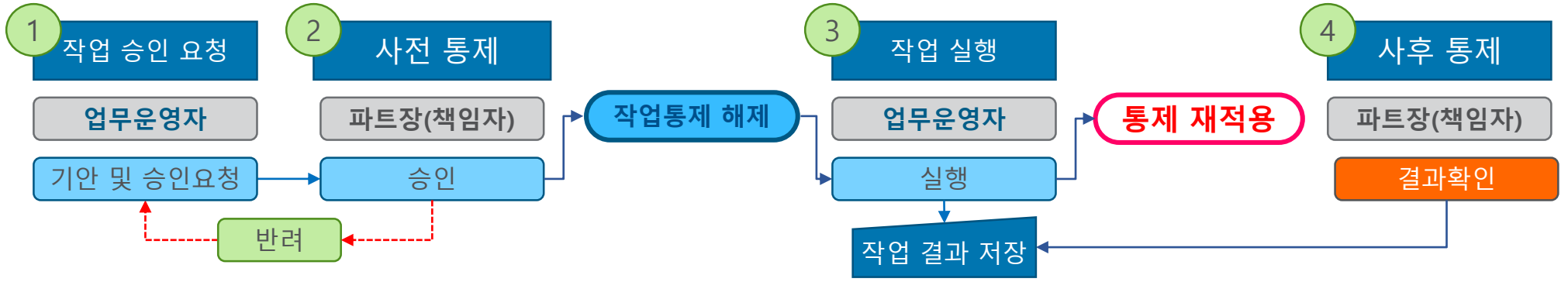
I은행 DB 운영 통제

※ I은행은 사용자의 **통제 정책 해제**가 적용되면 이후의 작업 수행 및 작업 결과에 대한 **책임자 승인 등 통제 미적용**



S은행 DB 운영 통제

※ S은행은 **작업 실행**에 대해서 통제 정책 조건에 따라 책임자 승인 및 작업 결과 확인으로 **사용자 작업통제 적용**



3.4 금감원 검사 개선 대응 현황

❑ 데이터베이스 운영 통제 개선 현황

- **DB 접근통제 솔루션**은 I은행과 S은행 모두 동일한 벤더사의 솔루션을 도입하여 운영하고 있음
- I은행은 **DB 접근통제** 개선을 위하여 "사이트 라이선스 도입" 협상을 진행 중이며, "**DB 직접접속 작업**" 통제 개선을 위하여 업무담당자의 Select 등의 SQL 명령어(DML) 수행 시 **책임자 승인** 등 개선 방안에 대해서 검토 하고 있음
- S은행은 **DB 접근통제** 개선을 위하여 "**사이트 라이선스**"을 적용하였으며, "**DB 직접접속 작업**" 통제 개선을 위하여 2013년 기존 사용 솔루션을 **A사의 DB 작업통제 솔루션**으로 교체하여 개선 지적사항 없이 검사에 대응

통제 항목	I은행 대응 사항	S은행 대응 사항
접근통제 확대	사이트 라이선스 도입 검토	▪ **사이트 라이선스 적용**
재해 복구 대책	소산 방안 검토	▪ 백업 데이터를 DR센터에 소산 보관
마스킹 적용	DB 직접접속 작업통제 개선 방안 등 검토 ※ 책임자 승인 등 결재 프로세스 적용	▪ 주민등록번호 등 개인정보에 대해서는 조회 시 마스킹 처리 **(주민등록번호 등 주요정보)** ▪ 업무상 마스킹 해제가 필요한 경우 책임자 승인 후 해제 **(N회 이하로 24시간 허용)**
명령어 통제		▪ 전산원장, 고객정보 등 중요 시스템에 대한 작업 수행 시 작업 내용에 따라 책임자 결재
조회 관리		▪ 주민등록번호 등 개인정보에 대해서는 조회 가능 건수를 지정 **(N,000건 이하)** ▪ 업무상 지정 건수 이상을 조회하는 경우 책임자 승인 후 조회 **(N,000건 이상인 경우 2회)**
다운로드 관리		▪ PC 저장 및 클립보드 카피를 금지하며, 업무상 필요한 경우 책임자 승인 후 저장 **(매회)** ▪ 개인정보를 단말에 저장하는 경우 DRM 솔루션과 연동하여 자동으로 DRM 적용 **(자동 적용)**
계정 관리		▪ 사용자가 DB 계정 정보 입력 없이 DB 접속 가능하도록 관리 **(작업통제 솔루션 ID로 접속)** ▪ 사용자가 전출·퇴직 등 인사조치가 있을 때에는 해당 사용자 계정 삭제 등 접근을 통제
S은행 통제 정책		▪ **사용자의 담당 업무 및 소속 등에 따라 통제 정책(접근권한, 가능 작업 등)을 차별화하여 적용** ▪ 불가 기능은 사용하지 못함 (승인 받더라도 불가) ▪ 제한된 기능을 사용하려면 결재/승인을 받아야 함 ▪ 제한 기능의 사용시간은 기준은 12시간으로 설정함(통제 기능별 별도 설정 가능)

3.5 금감원 검사 개선 대응 방안

❑ 데이터베이스 운영 통제 개선 방안

- **DB 접근통제 솔루션**은 전산 원장 및 개인정보 처리 등 중요 DB 서버에 대해서 운영 및 재해복구 시스템 전체 적용 필요
- 주민등록번호 등 고객정보는 모든 업무에서 마스킹을 적용하고, 마스킹 적용 해제에 대한 **책임자 승인** 등 통제 적용 필요
- 기존에 사용하고 있는 **DB Client Tool**이 수행 작업(조회 및 저장 등)의 **책임자 승인** 등 통제 적용 불가한 경우 교체 필요
- 업무 운영자가 사용하는 업무용 공용 계정 및 특권 계정에 대한 **DB 접속 및 계정 정보의 노출 금지** 등 통제 강화 필요
- **DB 작업통제 솔루션 도입으로 직접접속 작업에 대한 일원화된 통합관리로 개인정보 보호 및 관련 법규의 준수가 필요**

통제 항목	감독규정 준수를 위한 통제 개선 방안	작업Tool	접근통제	작업통제
접근통제 확대	▪ 미 적용 DB 서버 수량 조사 후 대응 방안 수립 적용	X (미지원)	O (지원)	O (지원)
재해 복구 대책	▪ IDC 와 DRC에 이중화 구성하여 소산 적용	※ (해당 없음)	O (지원)	O (지원)
마스킹 적용	▪ 주민등록번호 등 개인정보에 대해서는 조회 시 마스킹 처리 ▪ 업무상 마스킹 해제가 필요한 경우 책임자 승인 후 해제	X (미지원)	△ **(책임자 승인 X)**	O (지원)
명령어 통제	▪ 중요 시스템에 대한 중요작업 수행 시 작업 내용에 따라 책임자 결재 후 작업 수행	X (미지원)	△ **(책임자 승인 X)**	O (지원)
조회 관리	▪ 주민등록번호 등 개인정보에 대해서는 조회 가능 건수를 지정 ▪ 업무상 지정 건수 이상을 조회하는 경우 책임자 승인 후 조회	X (미지원)	△ **(책임자 승인 X)**	O (지원)
다운로드 관리	▪ PC 저장 및 클립보드 카피를 금지하며, 업무상 필요한 경우 책임자 승인 후 저장 ▪ 개인정보를 단말에 저장하는 경우 DRM 솔루션과 연동하여 자동으로 DRM 적용	X (미지원)	X **(미지원)**	O (지원)
계정 관리	▪ 사용자가 DB 계정 정보 입력 없이 DB 접속 가능하도록 관리 ▪ 사용자가 전출·퇴직 등 인사조치가 있을 때에는 해당 사용자 계정 삭제 등 접근을 통제	X (미지원)	△ **(DB 계정 노출)**	O (지원)

3.6 금감원 데이터베이스 운영 통제 중점 검사 항목

❑ 데이터베이스 직접접속 작업을 통한 암호화된 고객정보(주민등록번호 등) 유출 사고 방지

구분	관련 법규	상세 내용
암호화 대상	개인정보호법 제24조의2 안전성 확보조치 기준 제7조	• 시행령 제19조 : **주민등록번호, 여권번호, 면허번호, 외국인등록번호** • **비밀번호, 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 바이오정보**
보호 방법	개인정보호법 제24조의2 고유식별정보 보호	• 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 **암호화 등 안전성 확보에 필요한 조치**
안정성 확보	시행령 제30조 개인정보의 안전성 확보 조치	• 개인정보처리시스템의 개인정보에 대한 **접근 통제 및 접근 권한의 제한** 조치 • 개인정보를 안전하게 저장·전송할 수 있는 **암호화 기술의 적용** 또는 이에 상응하는 조치 • 개인정보 침해사고 발생에 대응하기 위한 **접속기록의 보관 및 위조·변조 방지**를 위한 조치

❑ 데이터베이스 직접접속 작업통제 방법(전자금융감독규정 제13조(전산자료 보호대책) 등 관련 조항)

- 암호화된 고객정보(고유식별정보 등)가 저장된 DB에 직접접속하여 수행하는 조회 등 중요 작업에 대한 통제 강화 필요
- 개인정보취급자**(계정)**가 고객정보를 처리하는 DB에 접속**(접근)**하여 조회**(권한)**을 수행하는 명령어**(작업)**에 대한 통제

구분	관련 솔루션	주요 통제 방법
계정관리	계정관리 솔루션 DB 접근통제 솔루션 DB 작업통제 솔루션	• 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것 • 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 접근을 통제할 것 • 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용
접근권한	DB 접근통제 솔루션	• 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당 • 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
작업수행	DB 작업통제 솔루션	• 이용자 정보의 조회·출력에 대한 통제 • 전산원장, 주요정보 또는 이용자 정보 등이 저장된 시스템에 대한 중요작업 수행 시 책임자가 이중확인 • 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것

3.7 S증권 금감원 검사 공시

❑ 데이터베이스 조회시 자가승인 불합리 개선사항

- **S증권사는 전산운영을 SO (주) OOO에 위탁 운영하여, 개발 및 운영에 대해서 SO (주) OOO 직원이 수행하고 있음**
- **고객정보 조회 등에 업무파트장(책임자)의 자가승인으로 DB 직접접속 작업통제 방안의 개선을 지적 받았음**

개선 사항

전산업무를 토털 아웃소싱(Total Outsourcing)하는 업체인 OO㈜ OOO에 위탁 운영하고 있으며 동 사 유지보수 직원 등이 고객정보가 포함된 데이터베이스를 조회할 경우 담당업무 총괄 책임자의 승인을 받도록 운영하고 있으나,

책임자급인 OO㈜ OOO 업무파트장은 데이터베이스를 조회할 경우 본인이 직접 자가승인이 가능하여 DB통제를 우회할 가능성이 있으므로

OO㈜ OOO 유지보수 직원 등이 시스템을 유지보수, 운영하면서 데이터베이스를 조회하는 경우 책임자 또는 제3자에 의한 통제절차를 마련하여 본인이 직접 승인할 수 없도록 관련절차를 개선하시기 바람

운영 현황

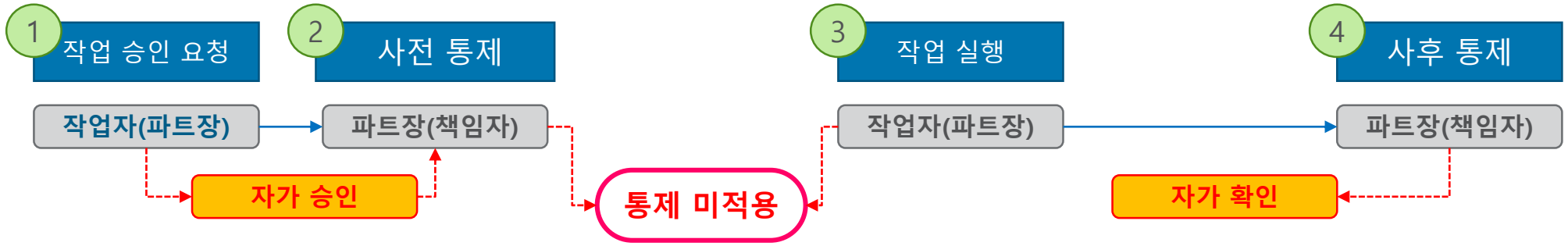
- S증권은 2007년도부터 W사의 접근제어솔루션과 작업통제솔루션를 사용하여 오다가, 2013년~2014년도에 W사의 접근제어솔루션로 업그레이드하여 사용하고 있음
- 검사 대응을 위해 DB접속에 대한 전 로그는 남기고, DML 및 원장 변경 등에 대해서는 작업통제솔루션의 결재기능을 사용하고 있음
- 사용하고 있는 DB접근제어 솔루션의 기능 부족으로 인한 자가승인이 아닌, 업무상 편의를 위해 슈퍼사용자(DBA 업무책임자 등)의 결재를 자신으로 설정해 놓은 정책설정의 문제로 판단됨
- 전자금융감독규정 제28조(거래통제 등) **"전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인"** 준수를 위한 3자 승인 프로세스 적용이 필요
- **최근 금감원 검사는 DB암호화 적용 이후 고객정보에 대한 조회, 저장 등에 의한 유출 방지를 위하여 DB 직접접속 작업에 대한 통제 프로세스 적용 여부를 집중적으로 검사를 진행하고 있음(계정관리, 접근통제 포함)**

3.7 S증권 데이터베이스 운영 통제 검사 개선 방안

❑ 데이터베이스 운영 통제 비교

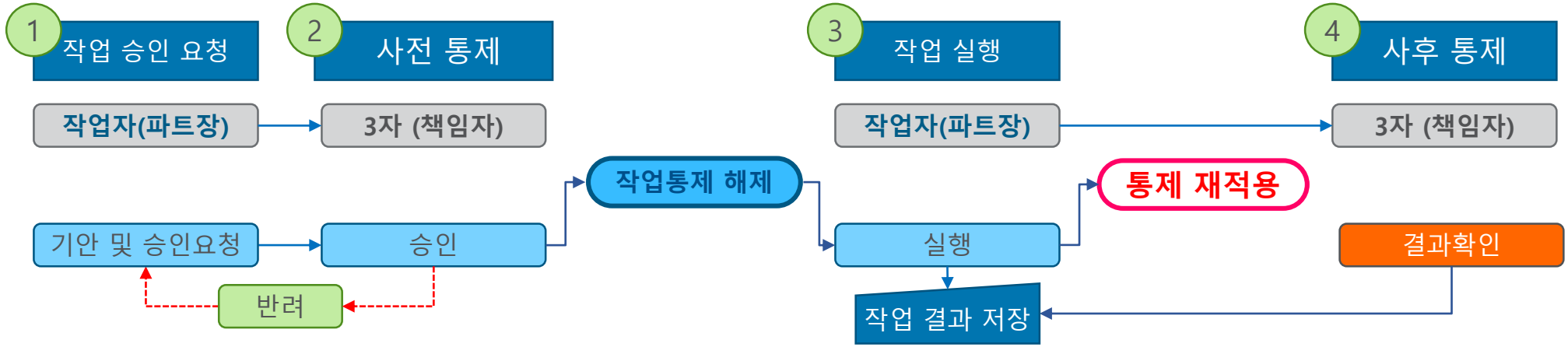
S증권사 DB 운영 통제 지적

※ 업무파트장은 데이터베이스를 조회할 경우 본인이 직접 자가승인이 가능하여 DB통제를 우회할 가능성 있음



S증권사 DB 운영 통제 개선

※ 업무파트장이 데이터베이스를 조회할 경우 3자(책임자) 승인을 통한 작업 내용에 대한 사전/사후 통제를 적용



3.8 S은행 : 데이터베이스 운영 통제

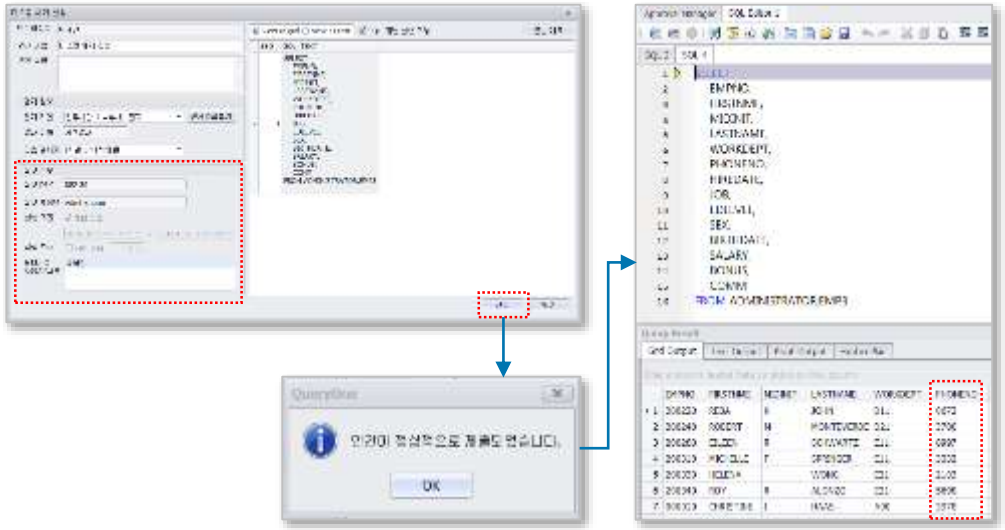
❑ S은행은 DB 직접접속 작업통제 및 금감원 검사 대응을 위하여 2013년 "DB 작업통제 솔루션" 교체 도입

금감원 종합검사 (2010년)	• 데이터베이스 사용에 대한 통제 절차 미흡 - 계정계시스템 XX개, DW시스템에 XXX개의 사용자계정 등록되어 운영 중이며, 부적절한 데이터 조회 및 변경이 수행되는 경우 정보유출, 성능저하 등 문제발생 소지가 있어 적절한 통제절차 마련 필요함

- S은행은 800여명의 직접접속 사용자가 있는 DW를 구축 운영하고 있었으며, 일부 계정계 업무에 W사의 DB 작업통제 솔루션을 적용하였음
- 2010년 검사 결과에 대응하기 위하여 "DB Tool 기능"과 DW를 지원하며, "책임자 승인" 등 통제 기능을 제공하는 솔루션 검토
- 기존 솔루션(W사 솔루션 등)은 검사 대응 불가로 판단하고, 요구 기능을 만족하는 A사의 DB 작업통제 솔루션을 교체 도입하여 최적화함

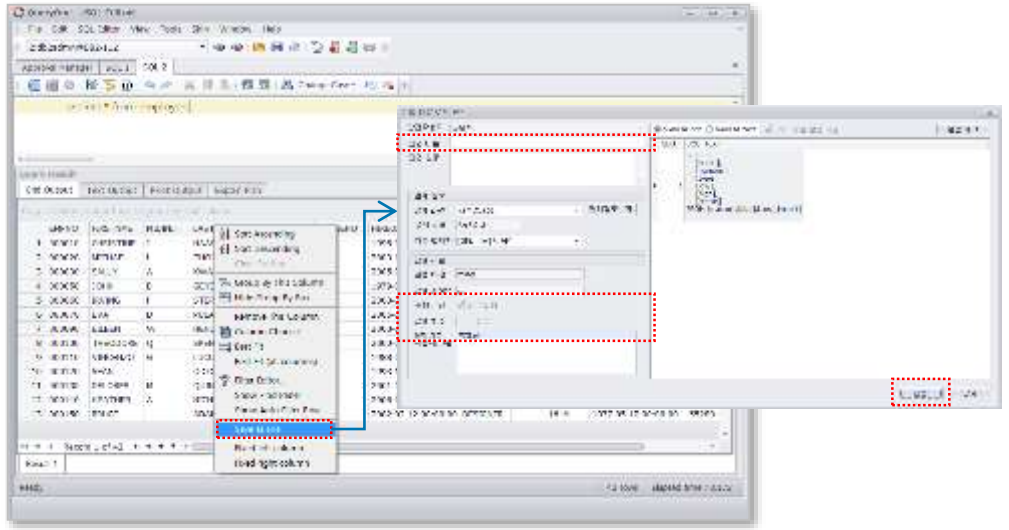
마스킹 해제 승인

. 작업명 (필수) 및 작업 내용에 대한 설명을 작성
. 승인 작업의 실행 기간, 실행 횟수는 관리자에 의해 설정 가능
. 승인 완료 후 SQL 에디터에서 해당 컬럼을 조회하면 마스킹이 해제 되어 조회
. 단, 해당 DB에 대한 사용 권한을 가진 경우에만 조회 가능 (전자금융감독규정 13조 1항 4, 10호)



파일 저장 승인

. 운영 DB 데이터 조회 결과를 반출 (PC 에 저장)은 금지되어 있음
. 업무상 필요하면 책임자에게 사전 승인 신청하여 저장 (전자금융감독규정 13조 1항 13호)
. 승인 작업의 실행 기간, 실행 횟수는 책임자에 의해 설정 가능
. 단, 해당 DB에 대한 사용 권한을 가진 경우에만 저장 가능 (전자금융감독규정 13조 1항 4, 10호)



3.8 S은행 : 데이터베이스 운영 통제

❑ 데이터베이스 운영 통제 정책

소속	업무	운영 DB 정책 적용					
		조회	데이터 저장	조회 건수	마스킹	데이터변경	스키마변경
IT 운영	DBA	가능	가능	가능	가능	결재	결재
	ETL	가능	가능	가능	가능	결재	결재
IT 개발	DA	기본권한	결재	결재	결재	결재	불가
	개발자	기본권한	결재	결재	결재	불가	불가
외부 직원	개발자	결재	불가	불가	불가	불가	불가
	유지보수	불가	불가	불가	불가	불가	불가

❑ 데이터베이스 운영 통제 결재

소속	업무	운영 DB 결재 라인		
		1차 (필수)	2차 (필수)	3차 (사후 통제)
IT 운영	DBA	DBA팀장	운영팀장	보안팀
	ETL	DBA팀장	운영팀장	보안팀
IT 개발	DA	개발팀장	운영팀장	보안팀
	개발자	개발팀장	운영팀장	보안팀
외부 직원	개발자	개발팀장	운영팀장	보안팀
	유지보수	DBA팀장	운영팀장	보안팀

3.9 데이터베이스 운영 통제 솔루션 기능 비교

❑ 데이터베이스 통제 솔루션 기능 비교표

범례 : X 미지원, △ 일부지원 (책임자 승인 미지원 등), O 지원

솔루션 구분	솔루션 기능			통제 항목 대응					DB Tool 기능 대응
	설치 위치	기능구분	주요 기능	마스킹	명령어	조회 관리	다운로드	계정관리	
DB Tool (Orange, Toad 등)	단말	DB Tool	▪ DB 접속 기능 (계정 입력 화면 등)					X	O
			▪ DB 사용 기능 (SQL 편집, 실행 등)		X				
			▪ DB 운영 관리 기능 (데이터 관리, 성능 관리 등)						
접근통제	단말	접근통제	▪ 사용자 인증 기능 (가상계정)					O	X
	관리 서버	DB Tool	▪ DB 접속 기능 (DB 접속용 Client 기능)						
		접근통제	▪ 계정 관리					O	
			▪ 접근권한 정책	△	△	△	X	O	
		작업통제	▪ DB 변경 관리 기능 (원장 및 DML 통제)	별도 솔루션					
			▪ 작업통제 기능 (마스킹, 조회, 다운로드 등)	△		△	X		
	DB 서버	접근통제	▪ 우회 접속 (관리 서버 미경유 접속) 차단 기능						
작업통제	단말	접근통제	▪ 사용자 인증 기능 (가상계정)					O	O
		DB Tool	▪ DB 접속 기능 (DB 접속용 Client 기능)						
			▪ DB 사용 기능 (SQL 편집, 실행 등)		O				
			▪ DB 운영 관리 기능 (데이터 관리, 성능 관리 등)						
		작업통제	**▪ DB 변경 관리 기능 (원장 및 DML 통제)**		O				
			▪ 작업통제 기능 (마스킹, 조회, 다운로드 등)	O		O	O		
	관리 서버	접근권한 작업통제	▪ 계정 관리					O	
			▪ 접근권한 정책, 작업통제 정책	O	O	O	O	O	

Soft Garden

검사합니다

Thank you

세종정보보안㈜
강 윤 채 / 부대표
T : 010-2047-5543
E : yckang@sejonginfo.co.kr