전자금융거래법(전자금융감독규정) 준수를 위한

DB 직접접속 작업 통제 개선 방안

2018.09

세종정보보안

Agenda

1. DB 직접접속 작업 통제 개선 개요
2. DB 직접접속 작업 통제 개선 방안
3. DB 직접접속 작업 통제 솔루션 개요
4. 타 금융기관 DB 작업 통제 개선 사례
5. 타 금융기관 DB 통제 검사 지적 사례

1. DB 직접접속 작업 통제 개선 개요

1.1 DB 직접접속 작업 통제 개선 목표

❑ DB 직접접속 작업 통제 개선 목적

▣ 금감원 검사 대응 및 내부 통제 강화

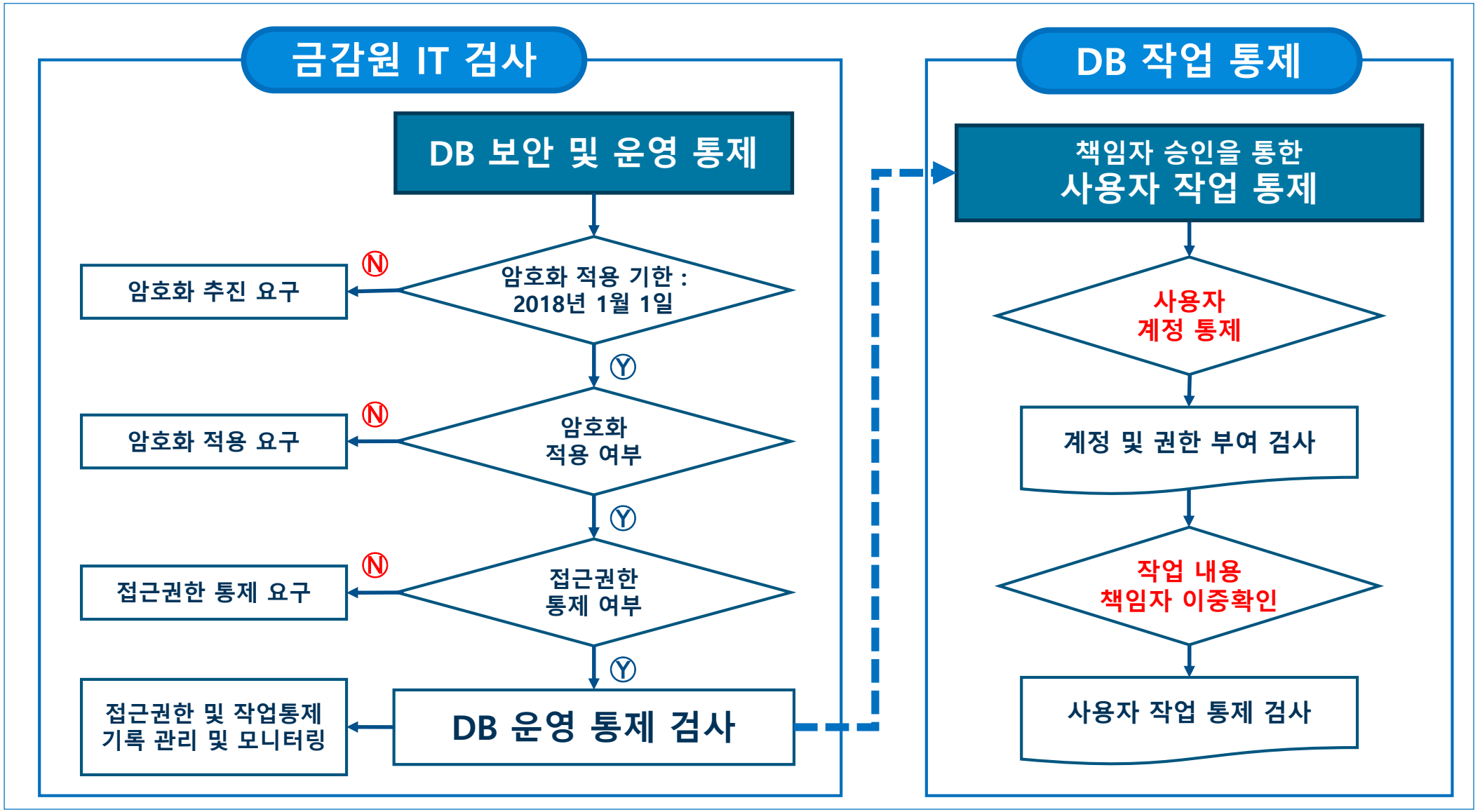
- DB 직접접속 작업 관련 금감원 검사 사항에 대하여 대응하고, 전산원장 변경 작업 등 DB 작업 관련 내부 통제 방안의 수립 및 적용
- DB에 대한 접근권한 부여 기준, 통제절차 수립 및 준수로 주민등록번호를 포함하는 고객정보 보호
- DB에 대한 접근권한 부여 내역의 전산기록과 관리책임자, 보안관리자 등의 제삼자 확인 및 관리
- DB 직접접속 작업에 대한 자동화된 책임자 승인을 통한 사전 통제로 고객정보 유출 등 보안사고 방지
- DB 직접접속 작업 수행 내용에 대한 기록 및 수행 내역 검사를 통한 사후 통제

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 부여하고 등록·변경·폐기를 체계적으로 관리**할 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 아니**하고, 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 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**
제27조 (전산원장 통제)	**① 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용** **② 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인** **⑤ 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존**
제28조 (거래통제 등)	② 금융회사 또는 전자금융업자는 전산원장, **주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인**을 해야 한다.
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

1. DB 직접접속 작업 통제 개선 개요

1.1 DB 직접접속 작업 통제 개선 목표

❑ DB 직접접속 관련 내부통제 강화



1.2 DB 직접접속 작업 통제 고려 요소

❑ DB 직접접속 작업 통제 개선 고려 요소

구분	항목	내용
통제 대상	전산원장	▪ 전자금융감독규정 제27조 (전산원장 통제) 해당 DB
	비전산원장	▪ 전자금융감독규정 제27조 (전산원장 통제) 이외 운영 DB
통제 범위	접근	▪ 업무별로 필요한 DB만 접속할 수 있도록 통제
	권한	▪ 접근이 가능한 DB에서 최소의 권한만 가능하도록 통제
	작업	▪ 접근권한이 있는 DB에 대해서 최소의 작업만 가능하도록 통제
통제 대상자	IT부서	▪ IT부서에서 DB 접근권한을 보유하여 작업을 수행하는 직원
	현업(비지니스)	▪ 현업부서에서 DB 접근권한을 보유하여 작업을 수행하는 직원
	기타	▪ 기타 DB 접근권한을 보유하여 작업을 수행하는 직원(외부직원 등)
수행 방법	중요단말	▪ 중요단말(PC)에서 DB접속 Client Tool을 이용하여 작업 수행
	서버	▪ 서버에서 DB 접속 Client Tool 및 Script 등을 이용하여 작업 수행

1.3 DB 직접접속 작업 관련 금감원 검사 대응

❑ DB 직접접속 작업 통제 관련 타 금융기관 검사 지적 사항

통제	검사 지적 사항	개선 방안
접근	▪ 개발담당직원이 운영 시스템(DB)에 접근 가능	계정 회수
	▪ 업무 변경자에 대한 계정 삭제 미적용	삭제 처리
권한	▪ 공용 및 사용자 그룹 계정의 입력,수정,삭제 권한 부여	권한 회수
작업	**▪ 주민등록번호 등 개인정보에 대한 마스킹 미적용**	**마스킹 적용**
	▪ 조회된 정보를 단말에 저장하는 경우 DRM 미적용	**DRM 적용**
	▪ 배치 프로그램을 이용한 이용자 정보 수동 변환 사용	변환 솔루션 적용
전산원장	▪ 전산원장 변경 작업에서 변경 전후 이미지 미저장	전산원장 변경통제
	▪ 전산원장 조회 작업에 대한 사전 통제(마스킹 등) 미적용	조회, 저장 통제

1.3 DB 직접접속 작업 관련 금감원 검사 대응

❑ DB 직접접속 작업 통제 개선 방안 및 대응 솔루션

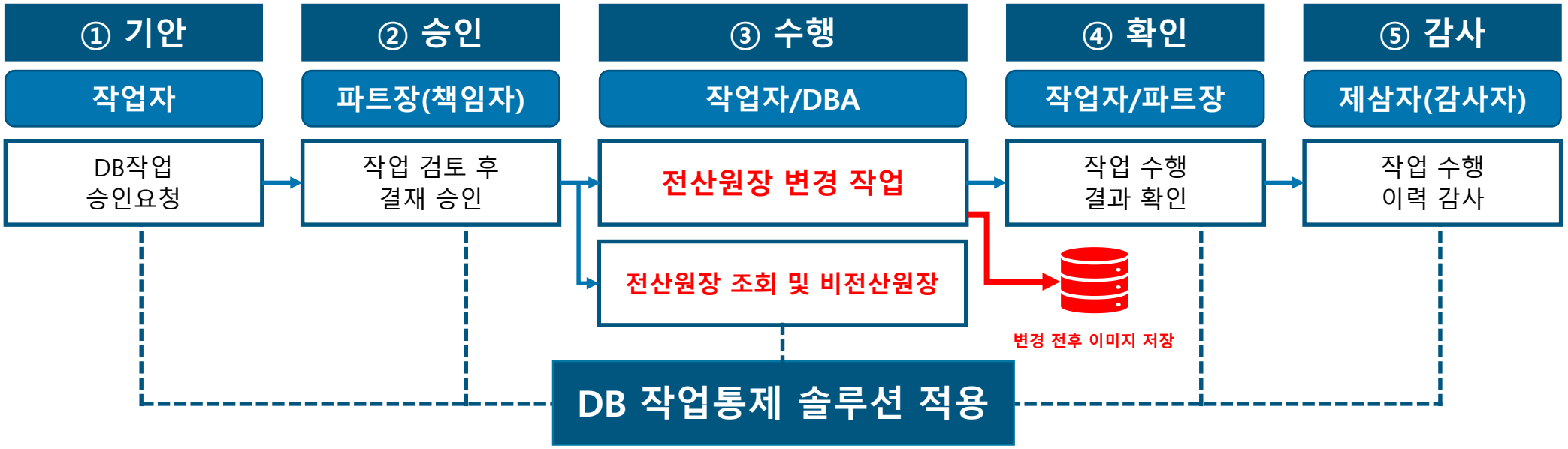
통제	검사 지적 개선 방안	대응 솔루션
접근	▪ 계정 정보(IP, Password, DB Port 등)에 대한 노출 금지	**DB 작업통제**
	▪ 업무 변경자에 대한 계정 삭제 적용	DB 접근통제
권한	▪ 공용 및 사용자 그룹 계정의 입력,수정,삭제 권한 회수	DB 접근통제
작업	▪ **주민등록번호 등 개인정보에 대한 마스킹 적용**	**DB 작업통제**
	▪ **조회된 정보를 단말에 저장하는 경우 DRM 적용**	**DB 작업통제**
	▪ 변환 솔루션을 이용한 이용자 정보 자동 변환 사용	테스트 데이터 변환
전산원장	▪ **전산원장 변경 작업에서 변경 전후 이미지 저장**	**DB 작업통제**
	▪ **전산원장 조회 작업에 대한 사전 통제(마스킹 등)**	**DB 작업통제**

1.4 DB 직접접속 작업 통제 개선 요약

❑ DB 직접접속 작업 통제 개선 솔루션 검토

솔루션	항목	검토 사항
DB 작업통제	작업수행	▪ DB 작업통제 관련 요구 기능에서 변경전후 이미지 저장 지원 ▪ **전산원장 조회, 개인정보 마스킹, 저장시 DRM 적용 등 지원**
	작업통제	▪ **전산원장 변경 작업과 전산원장 조회 작업 수행 및 관리 통합** ▪ **전산원장과 비전산원장 DB에 대한 작업 수행 및 관리 통합**

❑ DB 직접접속 작업 통제 개선 솔루션 적용



2.1 DB 직접접속 작업 통제 개선 방안

❑ 전산원장 통제 관련 전자금융감독규정해설

※ 금융감독원 전자금융감독규정 해설(2017.06) 89 Page

전산원장은 금융회사의 가장 중요한 정보로 고객 본인의 정상적인 거래 시에만 변경되어야 하나 프로그램 오류, 거래오류, 시스템 장애 등으로 인하여 변경이 불가피한 경우에는 엄격한 통제절차에 의하여 변경이 이루어지도록 하고 사후 철저한 검증 실시

전자금융감독규정 해설 상세 내역
전산시스템 장애 또는 프로그램 오류 등에 의한 전산원장 변경절차 수립 시 다음 사항을 고려 - 변경대상 및 방법 명시 : 사전에 변경대상을 지정하여 변경 대상정보에 대하여만 변경토록 하고, 만약 **절차에 지정된 변경 대상 이외의 정보에 대하여 변경이 필요한 경우에는 변경절차에 변경 대상 및 방법을 추가**(제1항) - 변경전후 내용의 자동기록 및 보존 : 온라인 이외의 방법으로 변경이 일어날 경우 거래 Log에 기록이 되지 않기 때문에 **별도의 프로그램이 작성되어 있지 않을 경우** 변경 내용에 대한 확인이 불가능하므로 반드시 **변경 전·후 내용이 기록되도록 프로그램이 준비되어 있어야 하고, 동 기록은 5년간 보관·관리(제5항)**
원장수정은 **불법수정과 고객정보 유출 등의 사고예방을 위하여 전담자를 지정하고 전용단말기를** 통해 수정할 수 있도록 하며 자체 감사부서의 상시감시대상에 포함하여 모니터링 실시(제2항)
전산원장 수정의 경우에는 제3자가 수정의 정당성을 사전 승인토록 하고, **원장 수정 전후내역을 전산기록(logging)하고 5년간 보존(제2항, 제5항)** - 전산원장 변경시 제3자의 범위는 객관적으로 확인이 가능한자로 감사부서, IT자체 감사 부서, 준법감시팀 등이 해당됨 - **정기적으로 실행되는 일괄작업(BATCH)의 경우 최초 1회시에만 적용하여도 가능**
주요 자료의 계상액과 각종 보조부, 거래기록, 전산원장 파일의 계상액이 상호 불일치할 경우 불일치 내용, 원인, 조치 사항을 전산시스템으로 5년간 보관하여 추후 사고 발생시 근거자료로 활용(제4항)
사고발생시 사고원인 추적 및 근거자료로 활용이 가능하도록 중요전산원장 접근(**조회, 수정, 삭제, 삽입 등**) 로그를 작업자, 작업일시, 작업내용 등의 전산자료 형태로 5년간 기록·보관(제5항)

구분	설명
타행 직접변경	▪ A은행의 경우 보통 월 2건 정도 수준이며, 일반적으로 각 안건에 3-4개의 쿼리가 포함되어 상신 되며, 결과값 기준으로 각 건당 20건 미만 ▪ K은행의 경우는 원장변경승인 신청이 평균적으로 월 5-6건 정도 수행되며, 각 건당 1건의 쿼리와 1개의 결과값 변경만 허용
정기 배치	▪ 배치로 처리되는 전산원장 변경 작업의 경우 **최초 1회만 검증 차원에서 변경 전후 이미지 저장**하고, 정기 배치에는 남기지 않음

2.1 DB 직접접속 작업 통제 개선 방안

❑ DB 운영 통제 관련 검토 사항

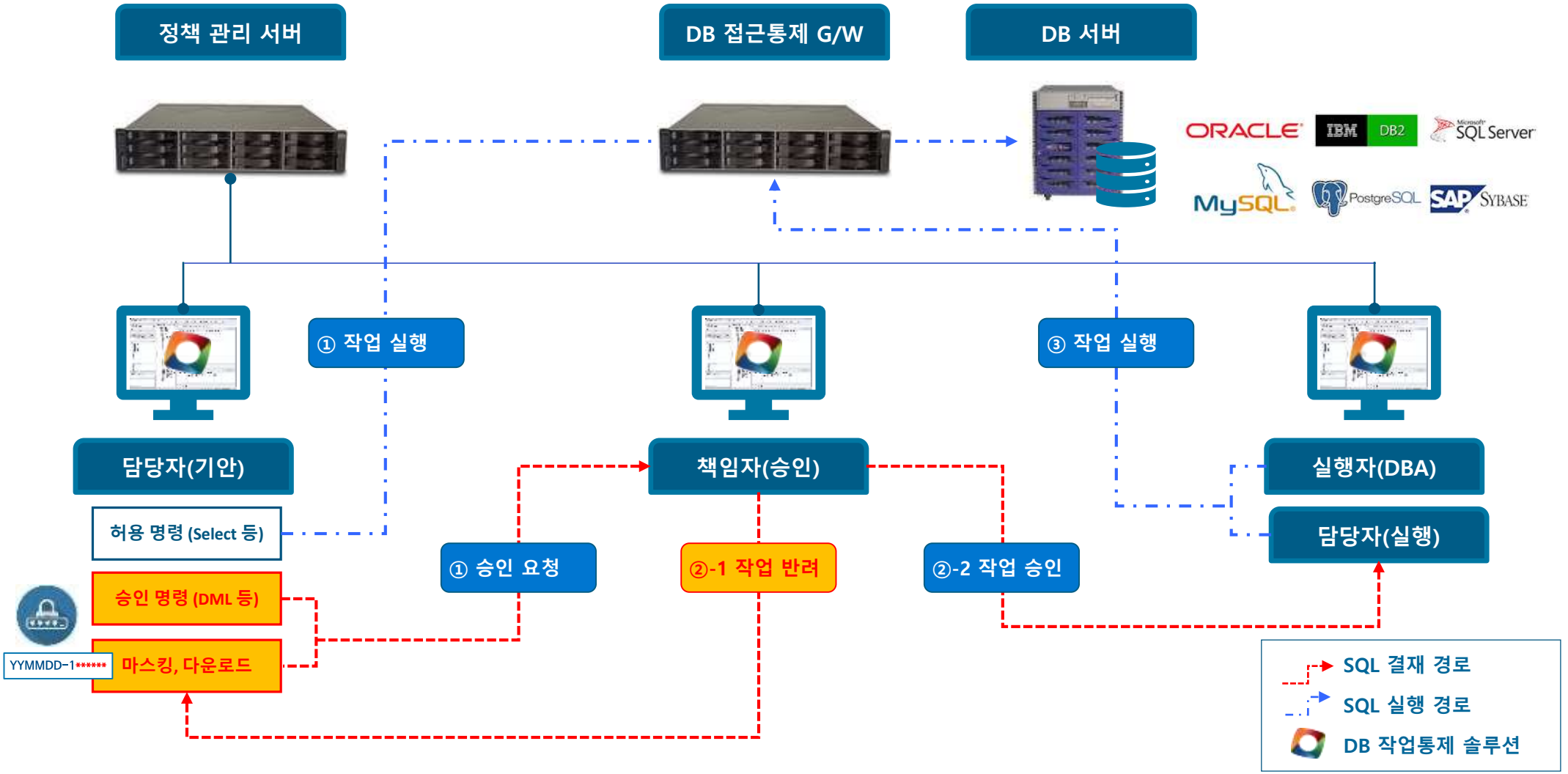
▪ **DB 접근통제 솔루션으로는 권한이 있는 사용자가 수행하는 작업에 대한 사전통제가 불가능하므로 DB 작업통제 솔루션 도입으로 DB 접속 작업에 대한 일원화된 통합관리로 개인정보 보호 및 관련 법규의 준수가 필요**

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?

2.2 DB 직접접속 작업 통제 솔루션 적용

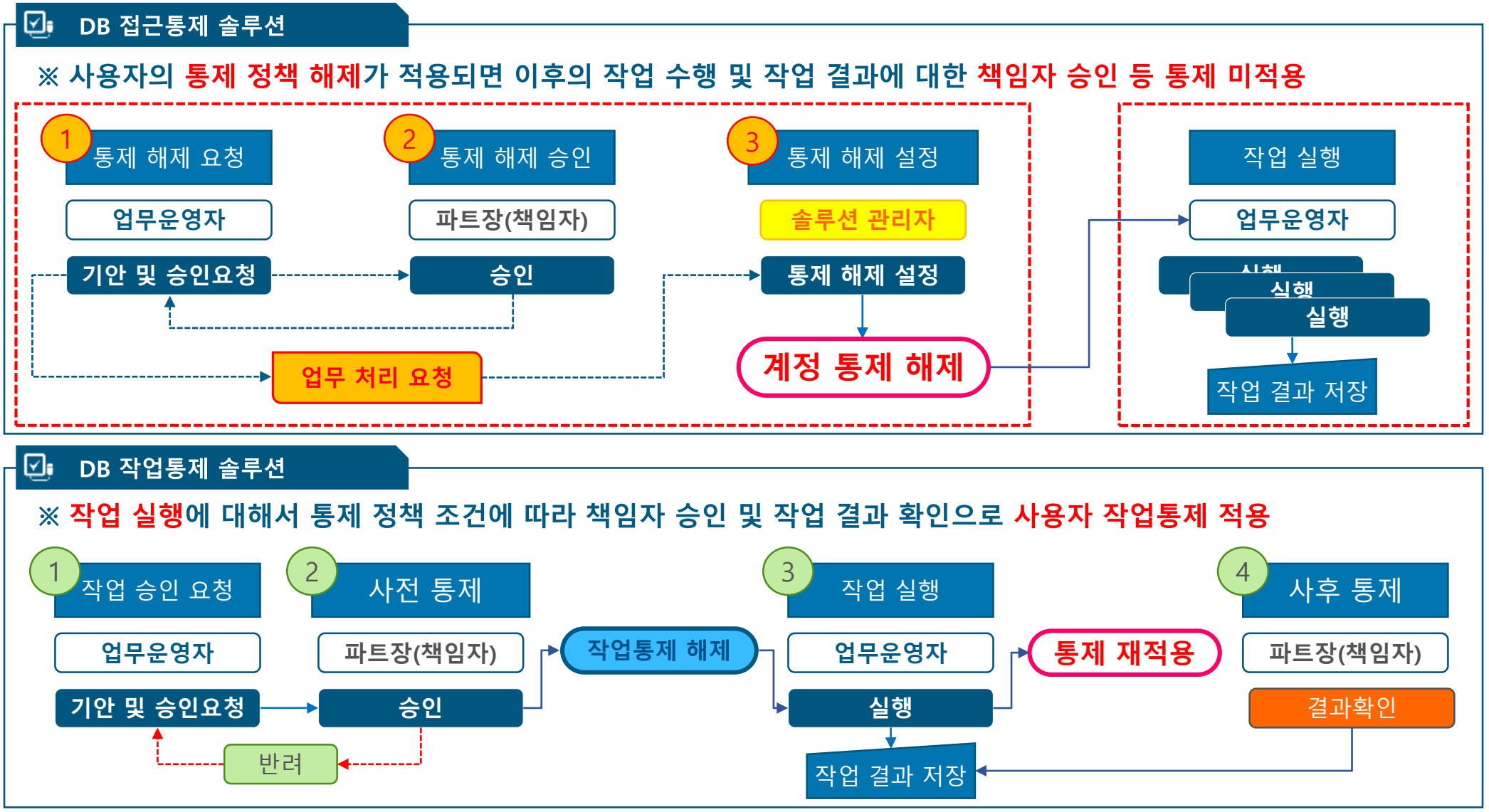
❑ DB 작업통제 솔루션 적용 프로세스

※ 전산원장 조회 작업 및 비전산원장에 대한 작업(조회·수정·삭제·삽입)은 DB 작업통제 솔루션을 이용하여 수행



2.2 DB 직접접속 작업 통제 솔루션 적용

❑ DB 직접접속 작업 관련 통제 솔루션 적용 프로세스



2.2 DB 직접접속 작업 통제 솔루션 적용

❑ DB 통제 솔루션 기능 비교

통제 항목	개선 항목	개선 방안	작업Tool	접근통제	작업통제
계정	▪ 공용계정 및 사용자 계정에 대한 권한 통제 ▪ 사용자 부서 이동, 퇴직 등 인사 변경이 발생한 경우 계정 통제	▪ 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)
마스킹	▪ 주민등록번호 등 고유식별정보에 대한 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	▪ 계정에 따라서 명령어(Insert, Updete, Delete, Select 등) 통제	▪ 중요 시스템에 대한 중요작업 수행 시 작업 내용에 따라 책임자 결재 후 작업 수행	X (미지원)	△ (책임자 승인 X)	O (지원)
조회	▪ 이용자 정보을 조회하여 테스트용 데이터로 사용	▪ 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	▪ 조회한 데이터를 DRM을 적용하지 않고 단말에 저장	▪ 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)
단말	▪ 개발자(외주 등)가 단말에 임의의 프로그램을 설치 하지 못하도록 통제	▪ 운영하고 있는 다양한 DBMS에 접속하는 Tool에 대한 표준화 ▪ EDW 등 DBMS를 직접 접속하여 사용하는 비지니스 부서 사용자에 대한 통제 적용	X (미지원)	X (미지원)	O (지원)

2.2 DB 직접접속 작업 통제 솔루션 적용

❑ DB 통제 솔루션 기능 상세 비교

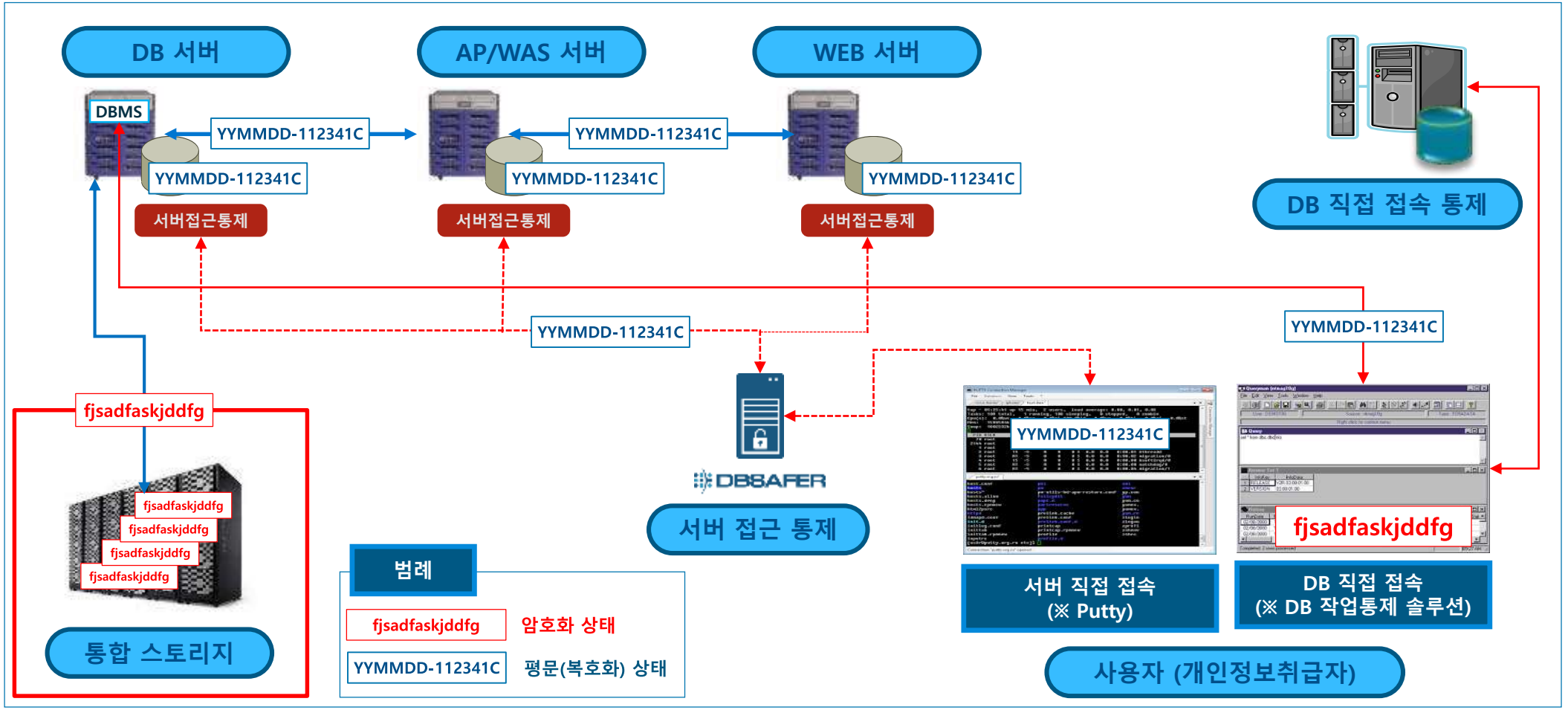
범례 : X 미지원, △ 일부지원 (책임자 승인 미지원 등), O 지원

솔루션 구분	솔루션 기능			통제 항목 대응					DB Tool 기능 대응
	설치 위치	기능구분	주요 기능	마스킹	명령어	조회 관리	다운로드	계정관리	
DB Tool (Toad등)	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 (Middleman)	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(DBInside)					
			▪ 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	

2.3 주민등록번호 등 개인정보에 대한 마스킹 적용

❑ DB 작업통제 솔루션 이용 마스킹 적용

- DBMS에 직접 접속하여 "개인정보파일"을 조회하면 DB 작업통제 솔루션의 기능을 이용하여 "**마스킹**"상태의 "**비식별화**"된 내용으로 출력하여 주민등록번호 등 개인정보 유출을 방지
- 개인정보취급자가 마스킹이 해제된 상태에서 조회하는 경우 조회 건수, 단말 저장 등에 대한 사전 통제 적용 필요

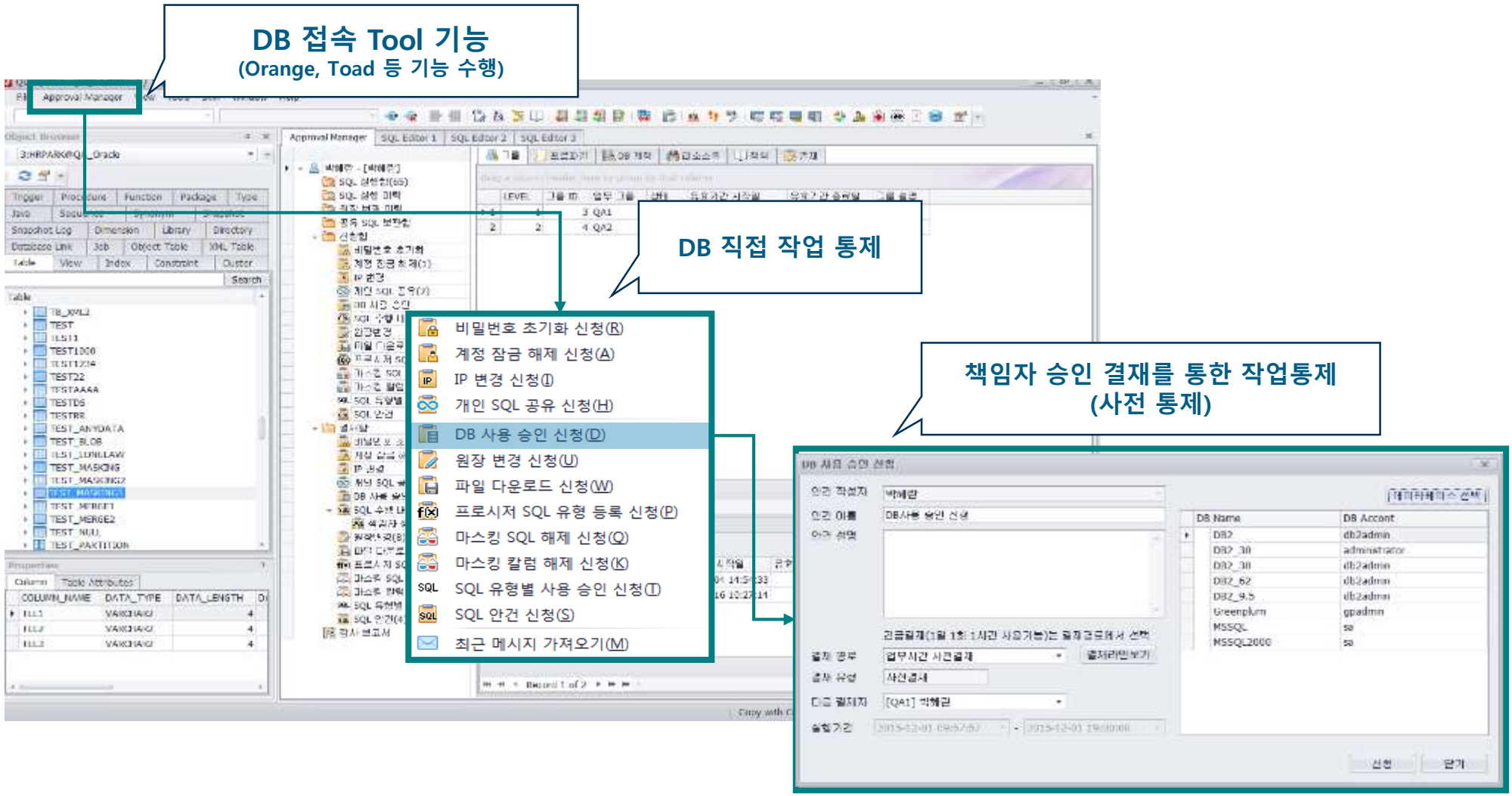


3. DB 직접접속 작업 통제 솔루션 개요

3.1 DB 작업통제 솔루션 적용 구성안

❑ DB 작업통제 솔루션 주요 기능

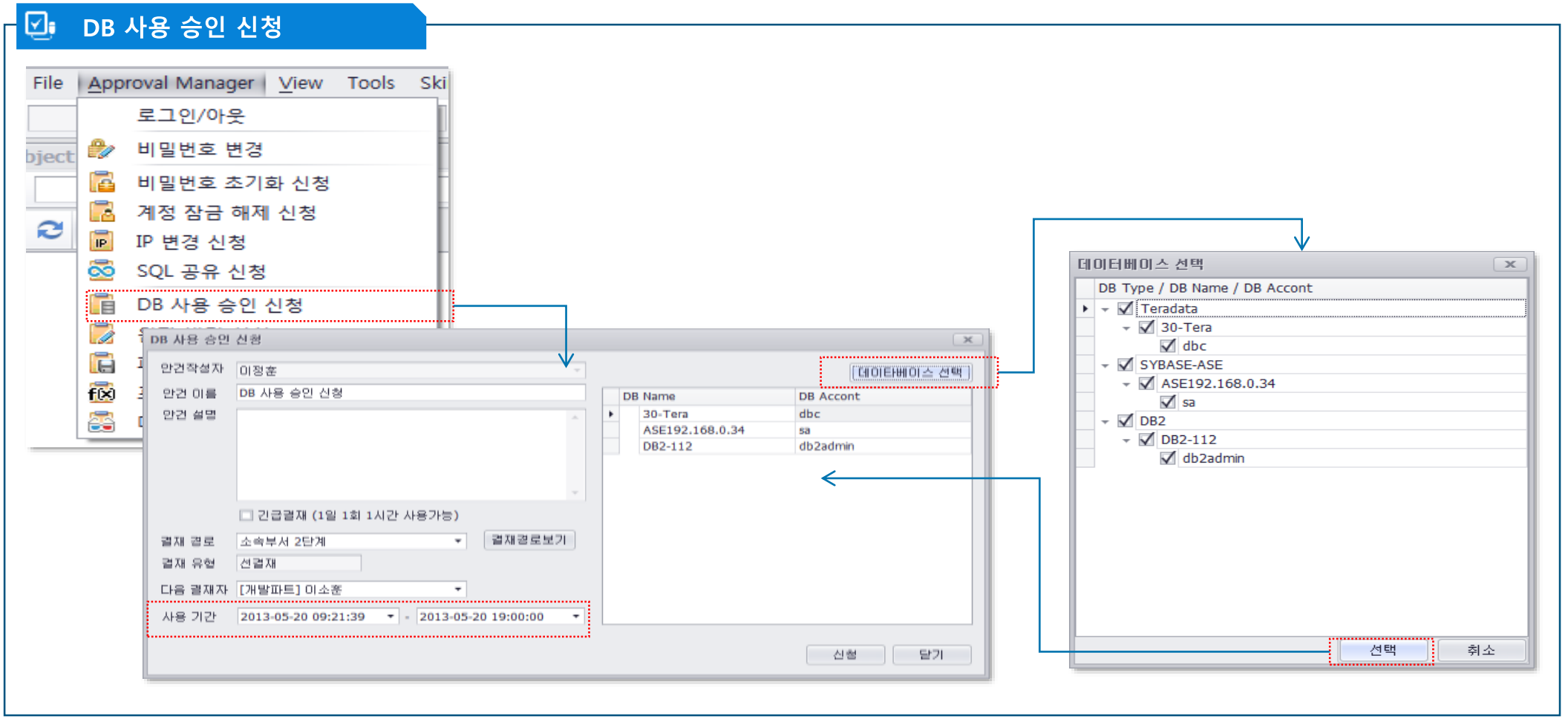
- **DB 작업통제 솔루션**을 이용하여 모든 DB작업에 대해서 **작업 Tool(기존 Toad 등)** 및 **작업통제** 기능 수행



3.2 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



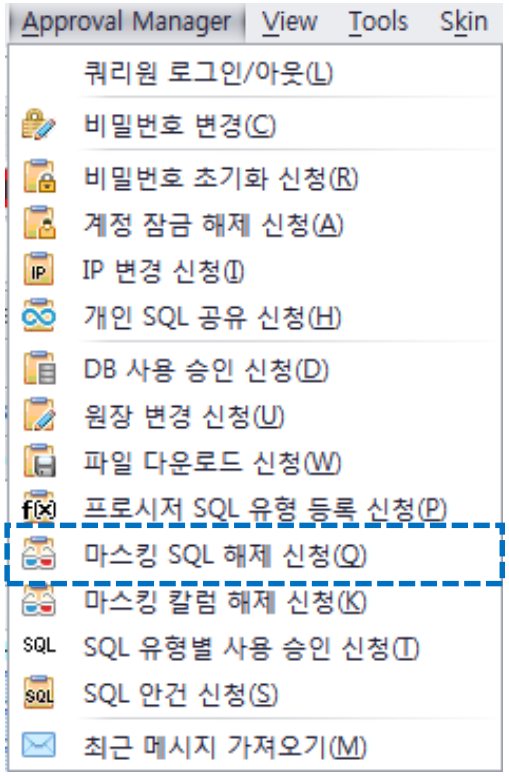
3. DB 직접접속 작업 통제 솔루션 개요

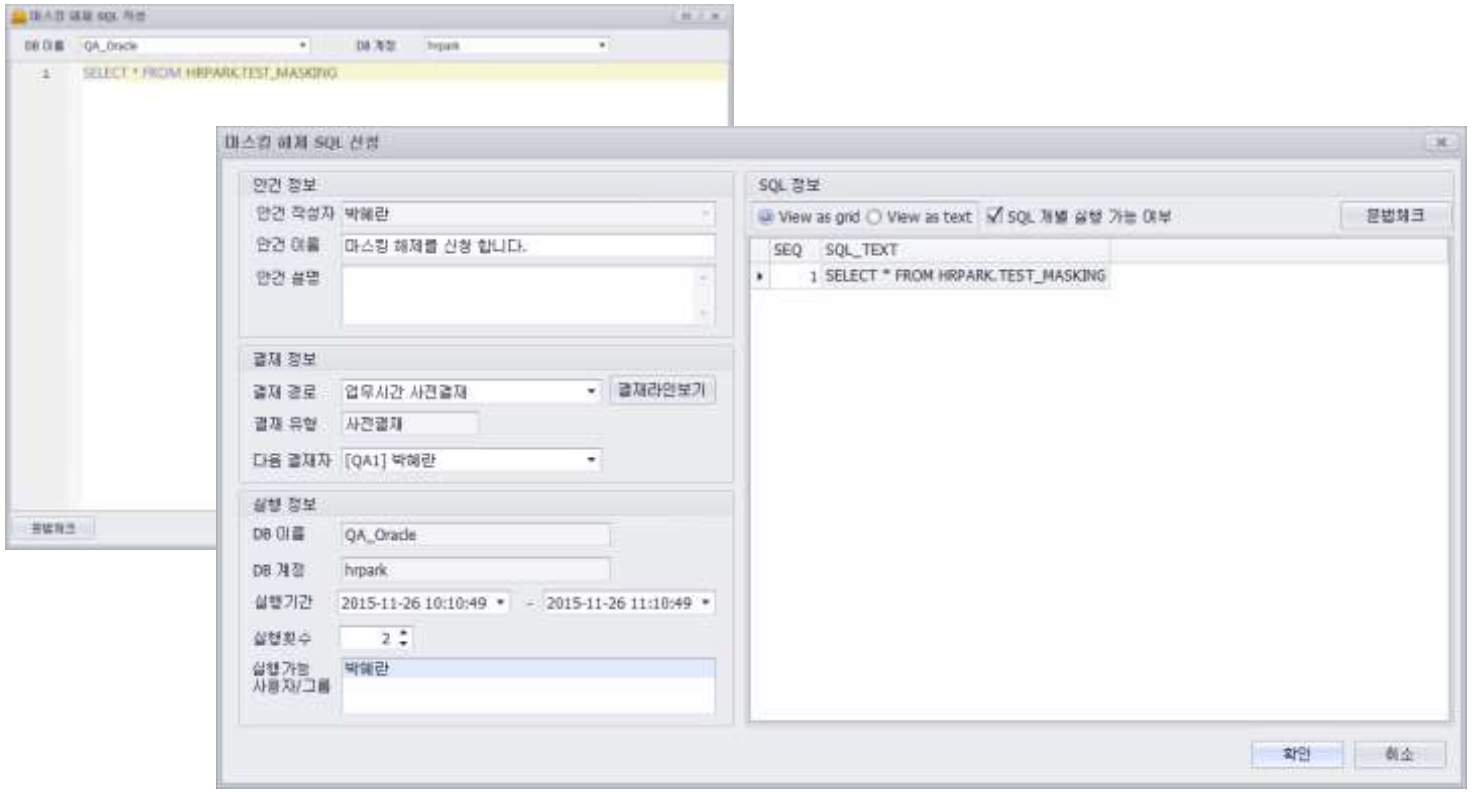
3.2 DB 작업통제 솔루션 주요 기능

❑ 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



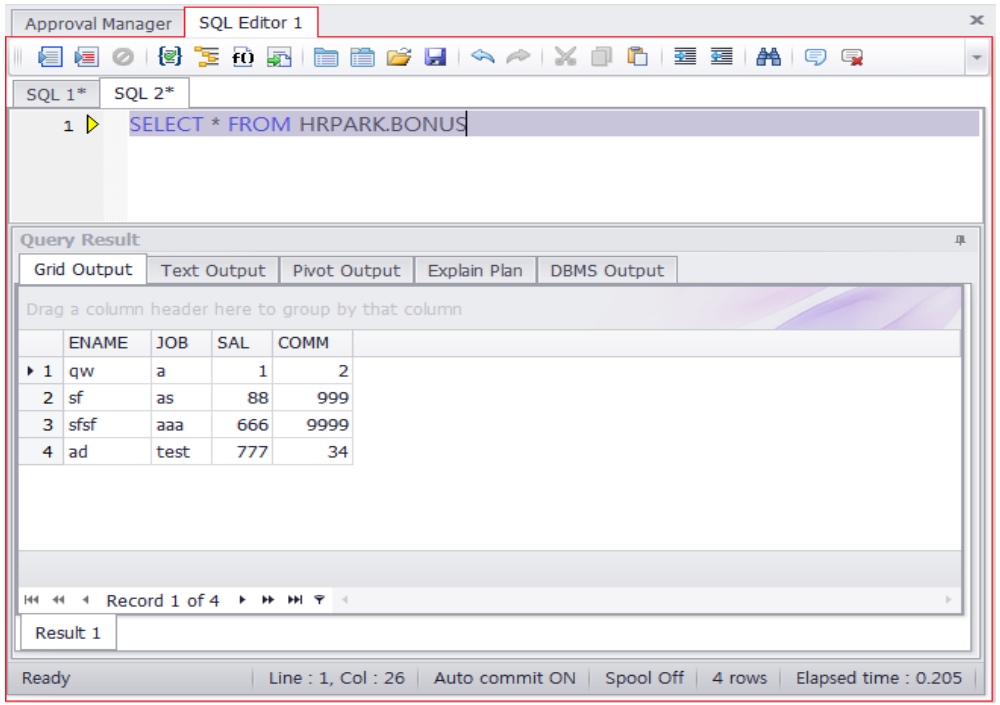


3.2 DB 작업통제 솔루션 주요 기능

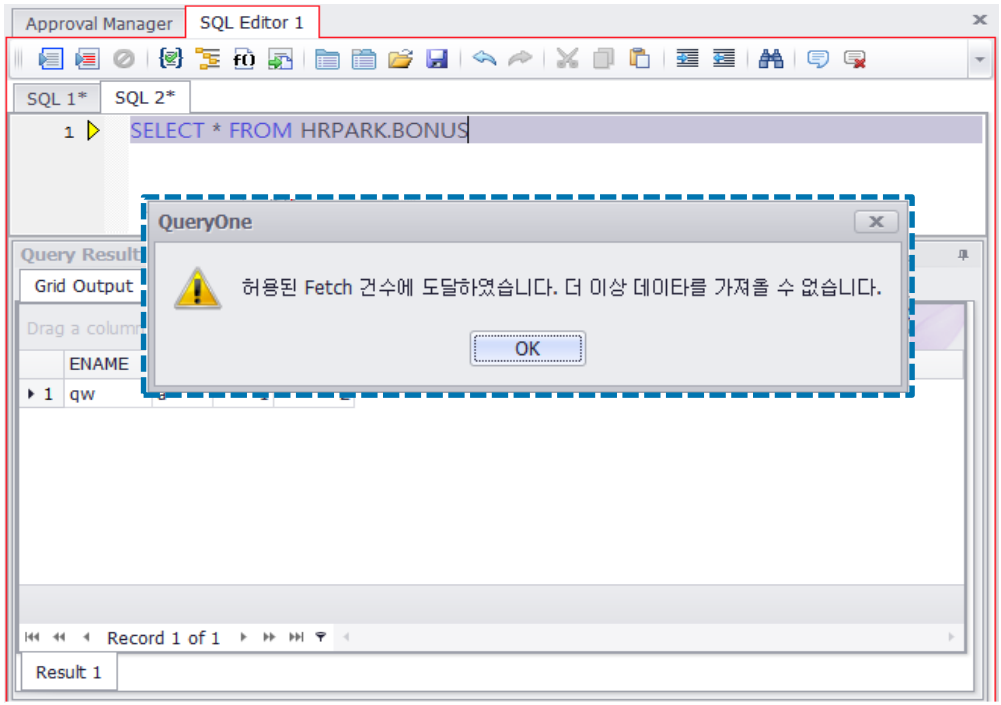
❑ 고객정보(고유식별정보) 및 주요정보의 대량 조회 방지를 위한 건수 제안 및 승인 처리

- 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

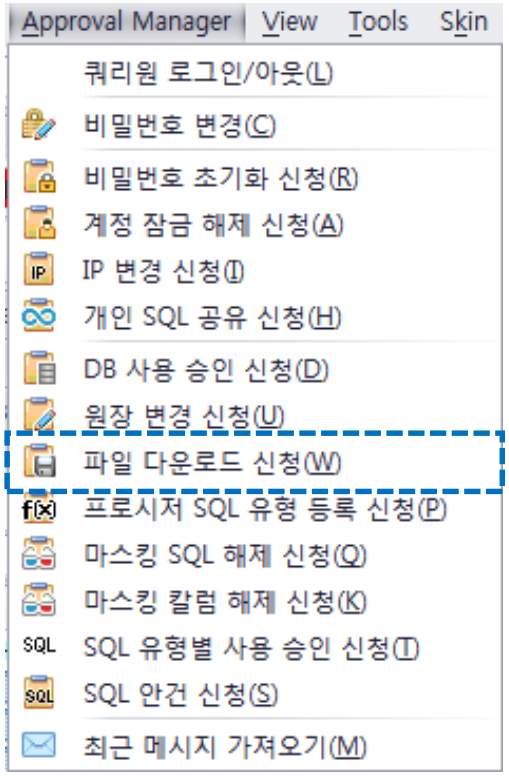


3.2 DB 작업통제 솔루션 주요 기능

❑ 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



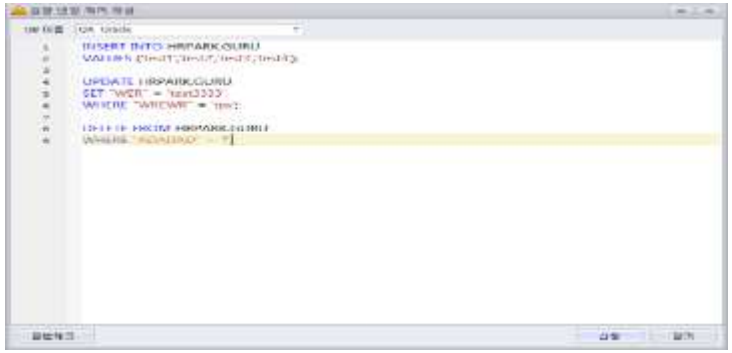
3.2 DB 작업통제 솔루션 주요 기능

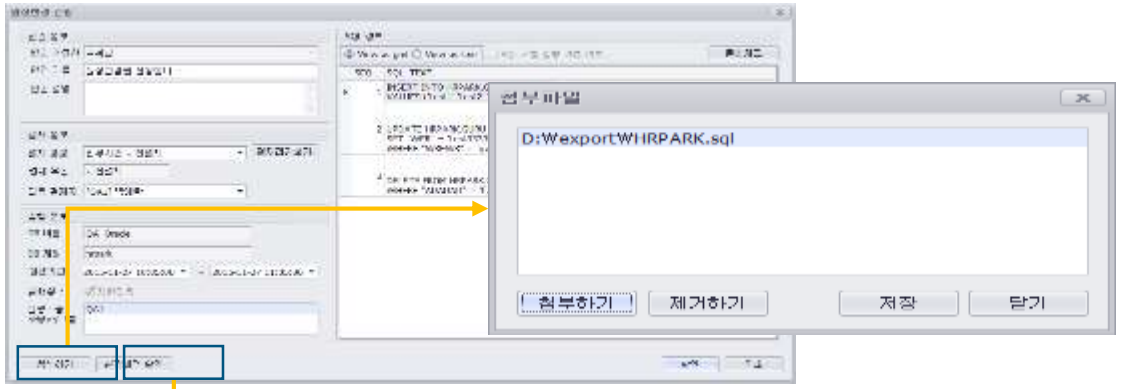
❑ 전자금융감독규정 제27조(전산원장 통제) 대응

- 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

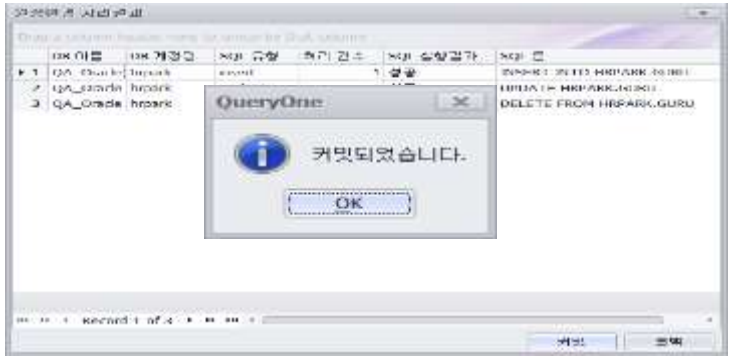
전산원장 통제 대응

[안건 작성]





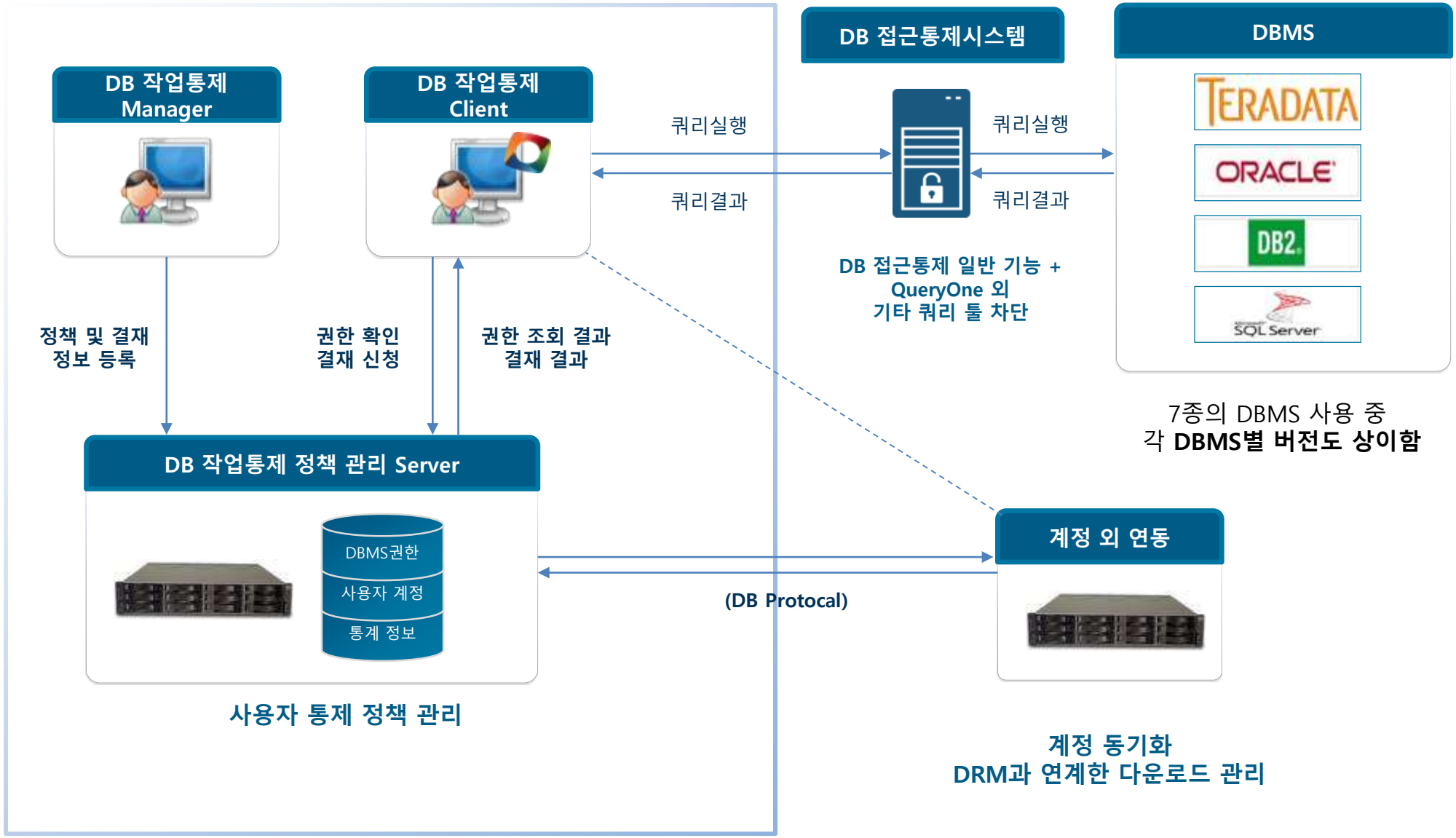
[안건 승인]



4. 타 금융기관 DB 작업 통제 개선 사례

4.1 A은행 DB 운영 통제 개선 구성도

❑ A은행 솔루션 적용 구성도



4. 타 금융기관 DB 작업 통제 개선 사례

4.2 A은행 DB 운영 통제 개선 적용

❑ A은행은 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

- A은행은 700여명의 직접접속 사용자가 있는 DW를 구축 운영하고 있었으며, 일부 계정계 업무에 W사의 DB 작업통제 솔루션을 적용하였음
- 2010년 검사 결과에 대응하기 위하여 "DB Tool 기능"과 DW(Teradata)를 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

통제 항목	통제 정책
접근통제 확대	▪ **사이트 라이선스 적용**
마스킹 적용	▪ 주민등록번호 등 개인정보에 대해서는 조회 시 마스킹 처리 **(주민등록번호 등 주요정보)** ▪ 업무상 마스킹 해제가 필요한 경우 책임자 승인 후 해제 **(N회 이하로 HH시간 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 N회)**
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
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)

4. 타 금융기관 DB 작업 통제 개선 사례

4.2 A은행 DB 운영 통제 개선 적용

❑ DB 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

❑ DB 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

5. 타 금융기관 DB 통제 검사 지적 사례

5.1 H 전자금융 전문업체 금감원 검사 공시

❑ 정보처리시스템 접근통제 관리강화

- **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)

5. 타 금융기관 DB 통제 검사 지적 사례

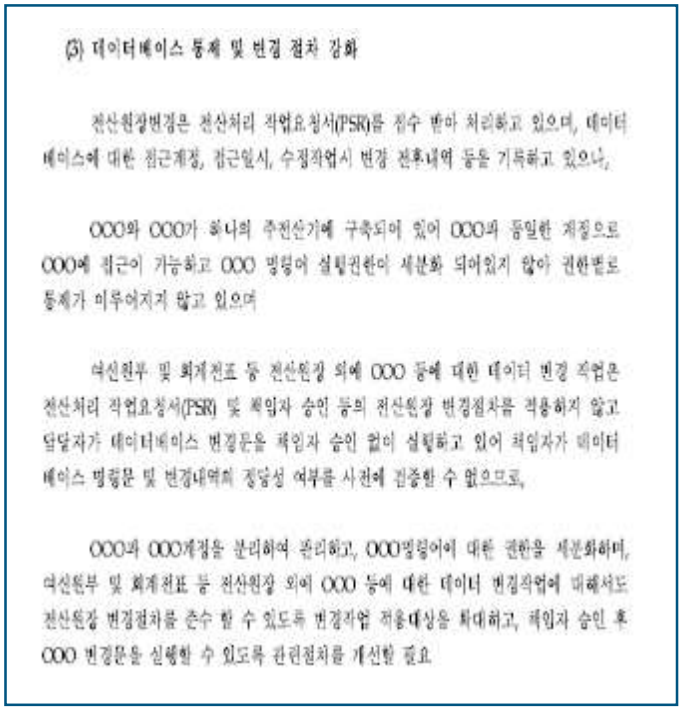
5.2 S캐피탈 금감원 검사 공시

❑ 데이터베이스 통제 및 변경 절차 강화

- **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

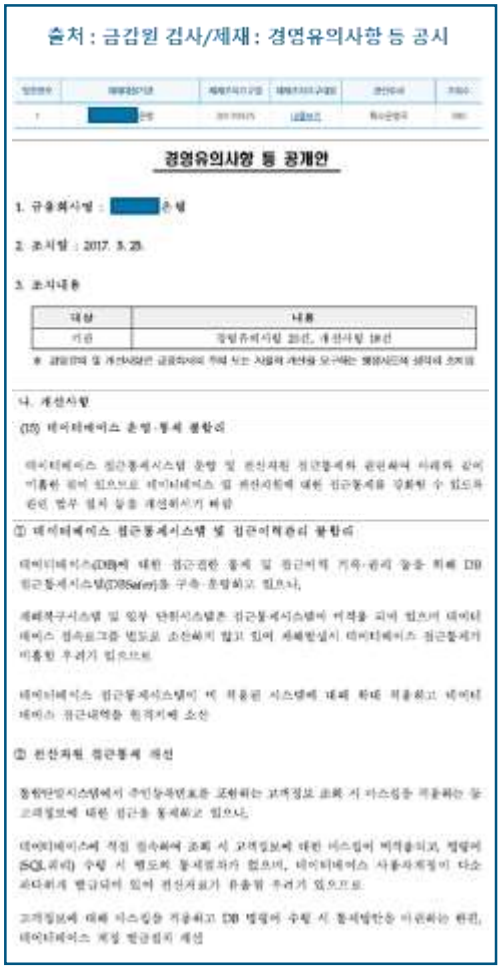
5. 타 금융기관 DB 통제 검사 지적 사례

5.3 I은행 금감원 검사 공시

❑ 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

5. 타 금융기관 DB 통제 검사 지적 사례

5.4 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)**

감사합니다
Thank you

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