복합인증체계기반 통합계정권한관리 솔루션 소개

iGRIFFIN®

㈜ 시 큐 브

CONTENTS

- 통합계정권한관리 소개
- 제안시스템 기술 설명

• 통합계정권한관리 소개

1. 배경 및 필요성

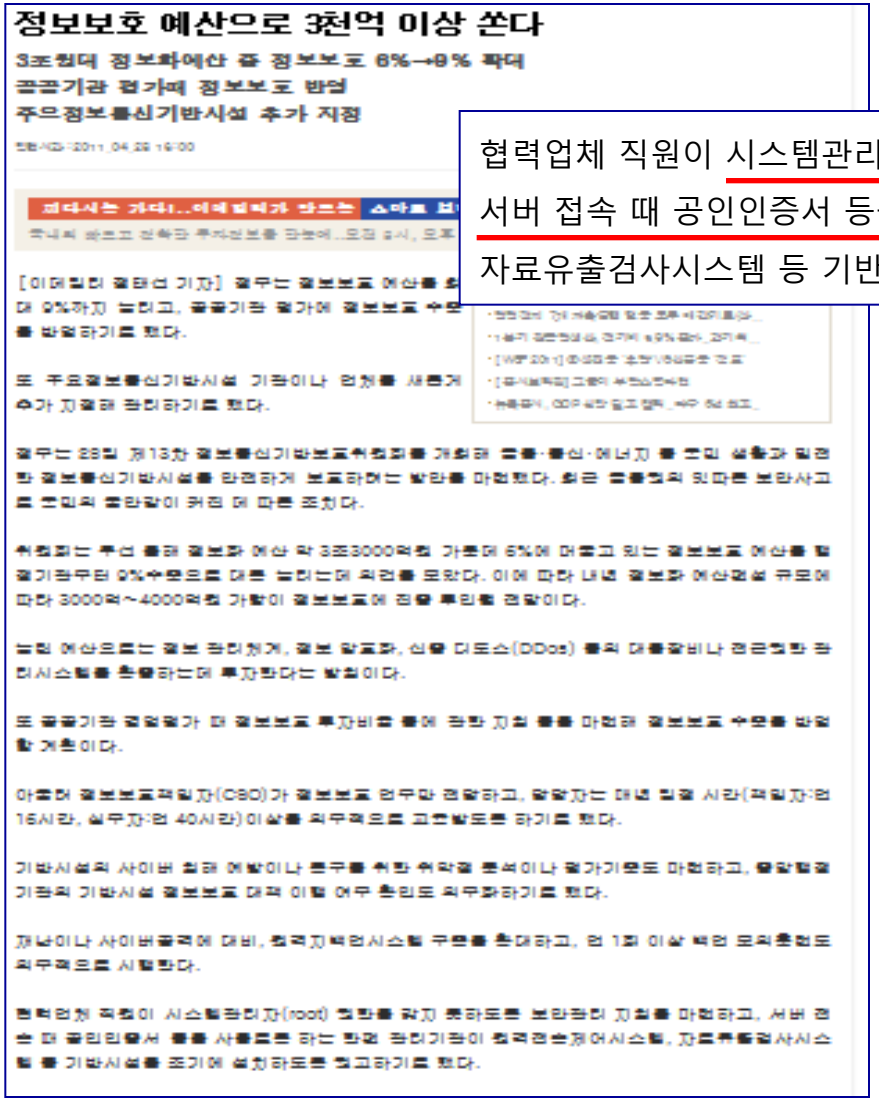
2. 문제점 및 해결방안

3. 구성도

4. 주요기능

5. 도입사례

통합계정권한관리 배경



정보보호 예산으로 3천억 이상 쓴다

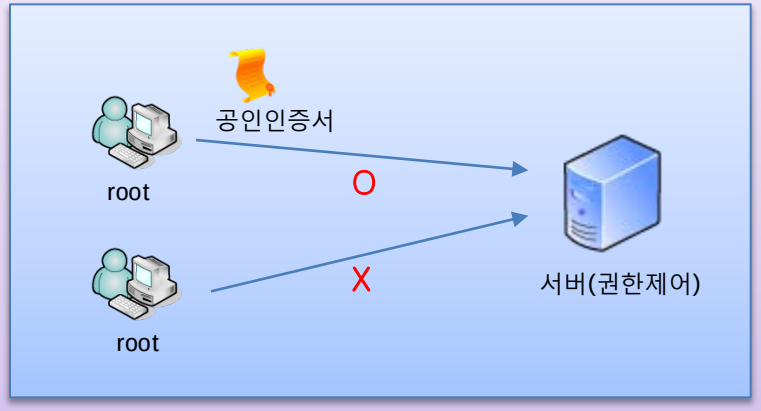
3조원대 정보화예산 중 정보보호 6%→9% 확대

공공기관 평가때 정보보호 반영

주요정보통신기반시설 추가 지정

협력업체 직원이 시스템관리자(root) 권한을 갖지 못하도록 보안관리 지침을 마련하고, 서버 접속 때 공인인증서 등을 사용토록 하는 한편 관리기관이 원격접속제어시스템, 자료유출검사시스템 등 기반시설을 조기에 설치하도록 권고하기로 했다.

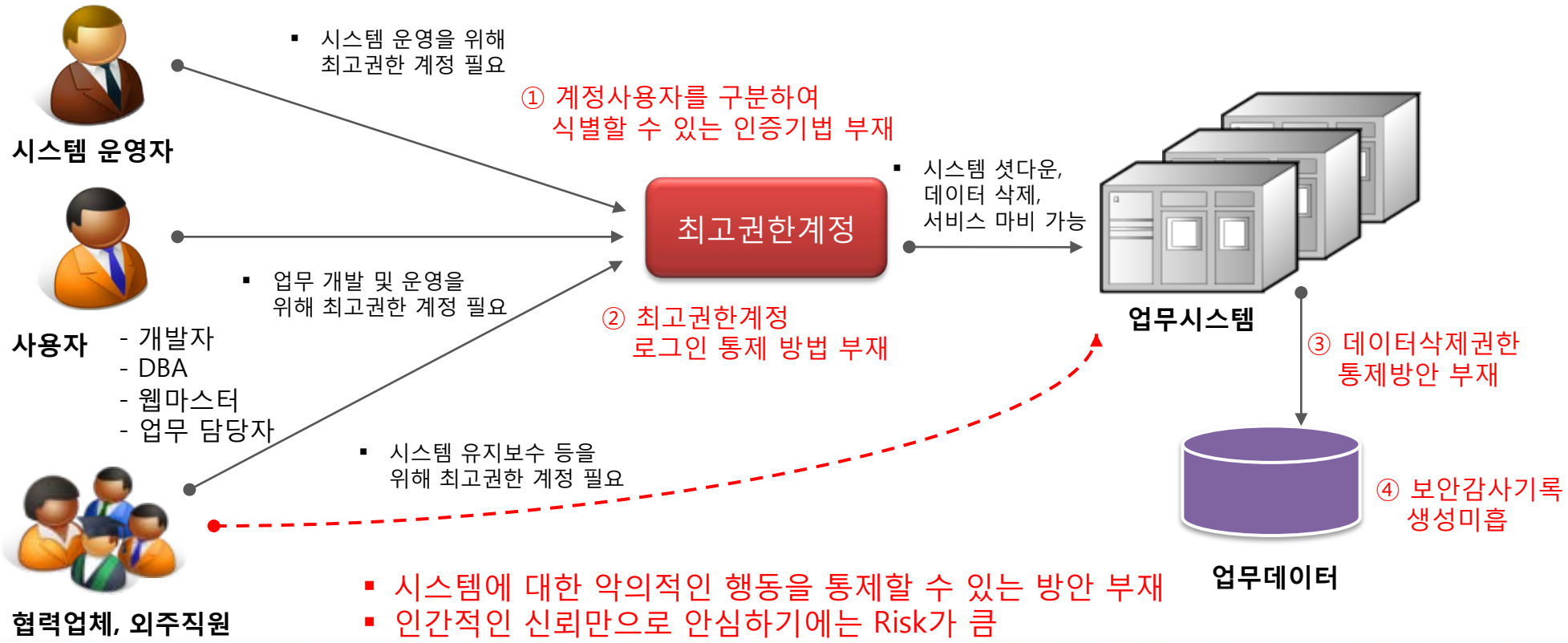
- 정보보호를 위한 시스템 접속 관리방안



- 시스템관리자 권한 제어
- 서버 접속 시 공인증서 등을 사용
- 접속제어 등 시스템 접근제어 기반 마련

통합계정권한관리 필요성

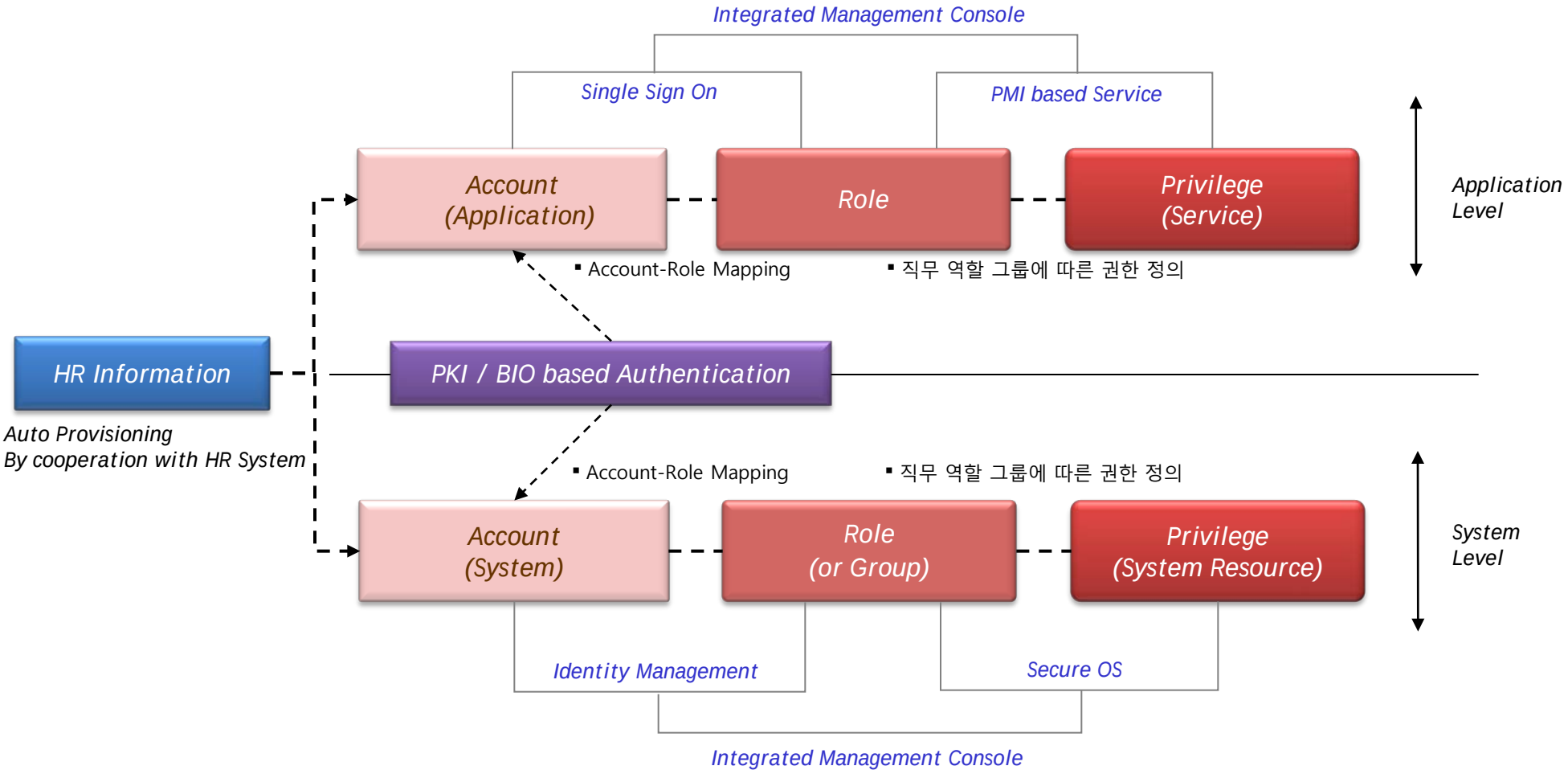
- 일반적인 상용시스템에서는 시스템 및 업무의 운영을 위해서는 시스템 특성상 최고권한계정을 필요로 하기 때문에 업무상 필요한 사용자에게 공유되어 있으며, 해당 사용자의 단순한 변심만으로도 시스템 전체를 마비 시킬 수 있는 형태로 운영되고 있어 본 사건의 원인도 여기에 있음
- 계정의 실 사용자를 식별하여, 업무상 꼭 필요한 경우에만 제한적으로 시스템에 접근할 수 있도록 통제하고, 접근한 후에도 해당 업무와 관련된 작업만 수행할 수 있도록 통제하며, 작업 내용을 감사기록으로 남겨 사후에도 감사추적을 할 수 있는 보안프레임워크가 필요함



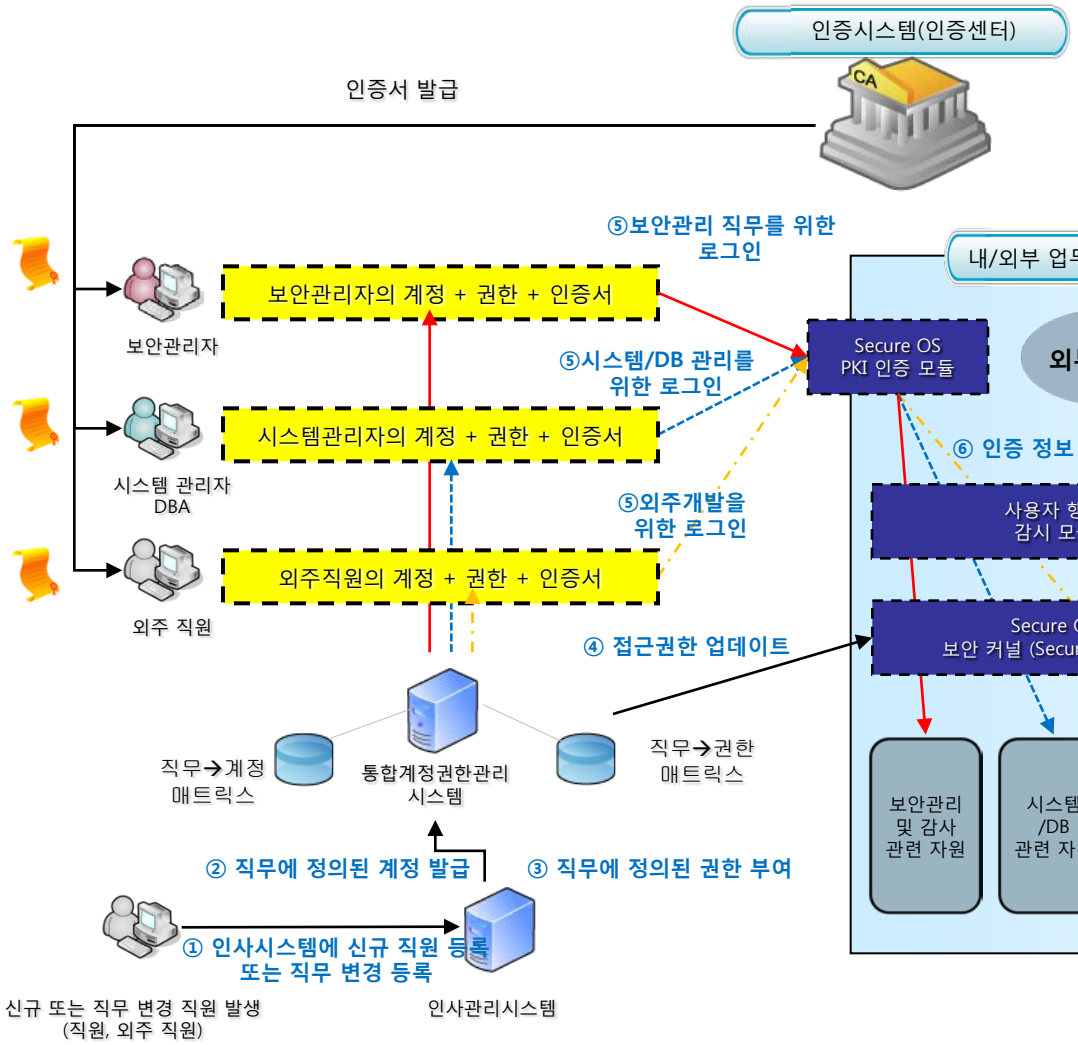
계정권한관리의 문제점 및 해결 방안

구분	문제점	해결 방안
계정 관리 측면	• 계정관리에 대한 일원화된 관리 미흡 → 시스템 관리자에 의해 임의적으로 생성 → root 권한을 소유한 사용자들에 의해 임의적으로 생성 • 신규/변경/폐기 등 Life cycle에 따른 관리 미흡 → 계정 생성 이후 관리체계 부재 → 생성했던 담당자 변경 시 서비스 가용성에 대한 영향 때문에 임의 삭제 불가 • 직무에 따른 계정 사용 현황 파악 불가 → 업무상 필요한 계정인지 여부 파악 불가 → 계정을 사용하고 있는 사용자 파악 불가 → 미사용 계정인지 여부 파악 불가	• 복합인증체계(PKI, BIO 등)과 연동된 계정관리체계 마련 • 신청 기반의 계정 관리 체계 마련 • 계정 신청 내역, 복합인증체계기반 시스템 로그인 로그 분석을 통한 계정 사용 내역 파악
권한 관리 측면	• 명령어에 실행에 대한 실시간/사전 승인절차 및 감사 체계 필요 • 접근통제 및 통제정책에 의한 사용자 계정통제 필요 → 시스템 자원 접근에 대한 통제 방안 부재 → 시스템 계정을 소유한 경우 시스템 자원 접근 가능 → super-user 통제 방안 부재 (권한 남용 가능) • 권한분리 방안 부재 → 일원화된 권한관리 방안 미흡 → 시스템 운영자, 보안 담당자, 업무 담당자 super-user 권한분리 방안 부재 → 특수계정 (DB계정 등)의 공유 계정 권한 관리 방안 부재	• 명령어에 실행에 대한 실시간/사전 승인절차 및 감사 체계 제공 • 복합인증체계와 연동 된 권한관리 체계 마련 • 신청 기반의 권한 관리 체계 마련 • 권한 신청 내역, 복합인증체계기반 행위감사로그 분석을 통한 권한 사용 내역 파악
감사 및 Compliance 측면	• 계정 사용 현황 (직무 상 필요한 계정 및 소유자 정보) 제공 방안 부재 • 계정 소유자의 시스템 작업 내용 감사 데이터 제공 방안 부재 • 시스템 내 데이터 접근통제 정책 및 통제 방안 제공 부재 • 법/제도 준수(Compliance) 방안 부재 → 개인정보보호법, 전자금융감독규정 등	• 계정-사용자 mapping 현황 자료 제공 • 복합인증체계 기반 사용자 행위 감사 내역 제공 • 권한 신청 및 접근통제 정책 현황 자료 제공 • 법/제도 준수(Compliance) 및 증거 자료 제공 가능

계정권한관리 내부통제 보안 모델



iGRIFFIN 시스템 구성도

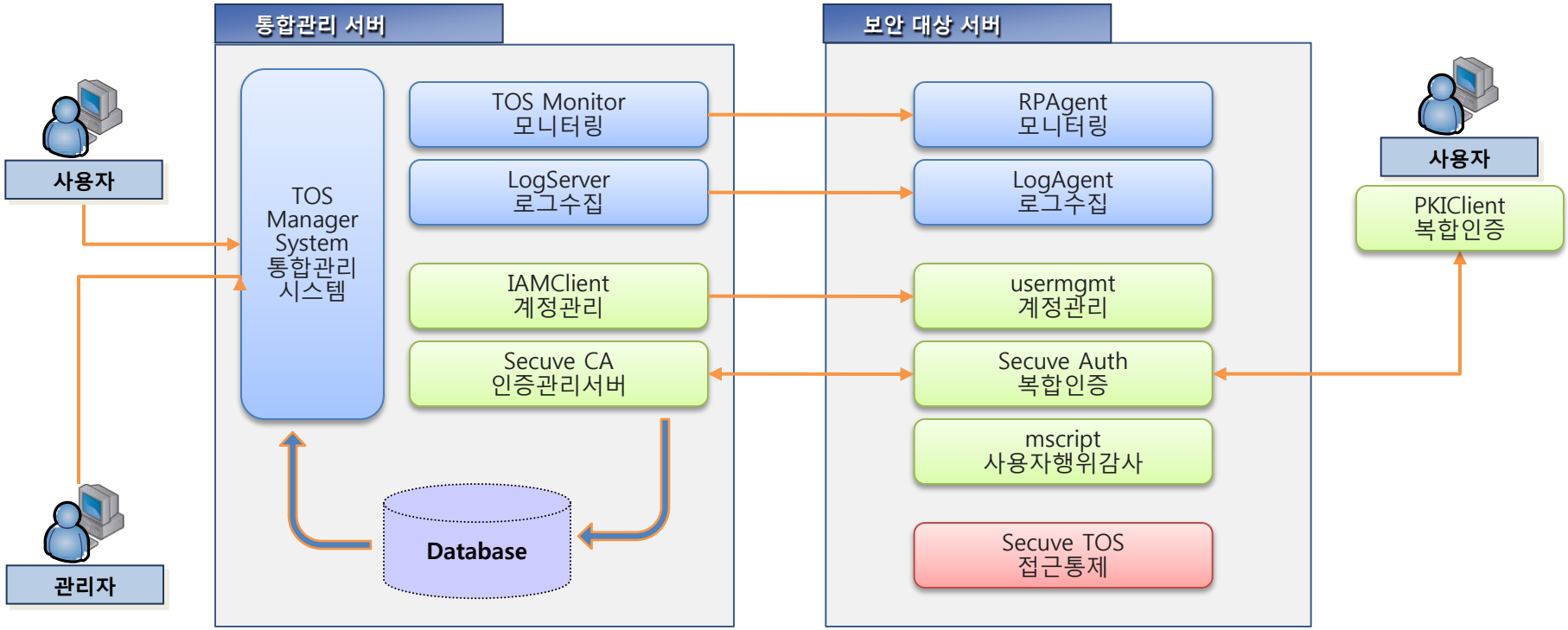


< 사용자 로그인 감사추적 데이터 >
- 로그인시간: 계정 : IP : **복합인증체계(사번)** : 서비스-인증방식 : 결과
- 2009-12-15 14:22:33 | root | **AA123456** | TELNET-PKI | SUCCESS

< 사용자 행위 감사추적 데이터 >
- 명령실행시간: 계정 : 세션: **복합인증체계(사번) : 실행 경로 : 실행 명령**
- 2009-12-15 14:22:33 : root : S12394 : **AA123456** : /home/test : vi aaa.txt

< 보안정책 위반 감사추적 데이터 >
- 시간: 계정 : **복합인증체계(사번) : 접근대상 : 작업 내용 : 결과**
- 2009-12-15 14:22:33 : root : **AA123456** : /home/aaa.txt : read : FAIL

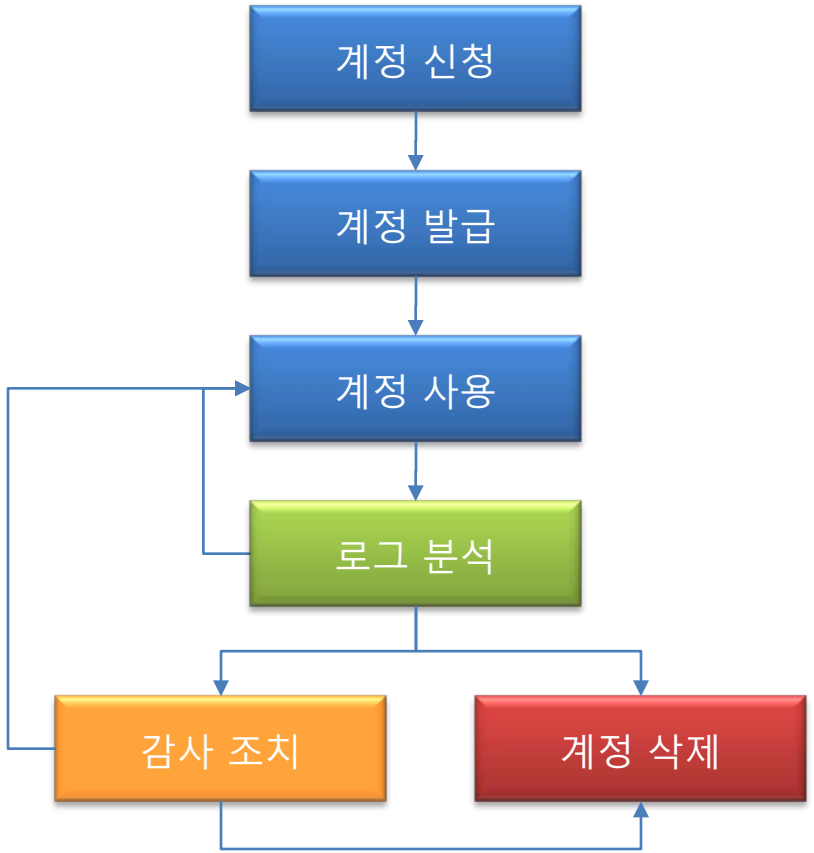
iGRIFFIN S/W 구성도



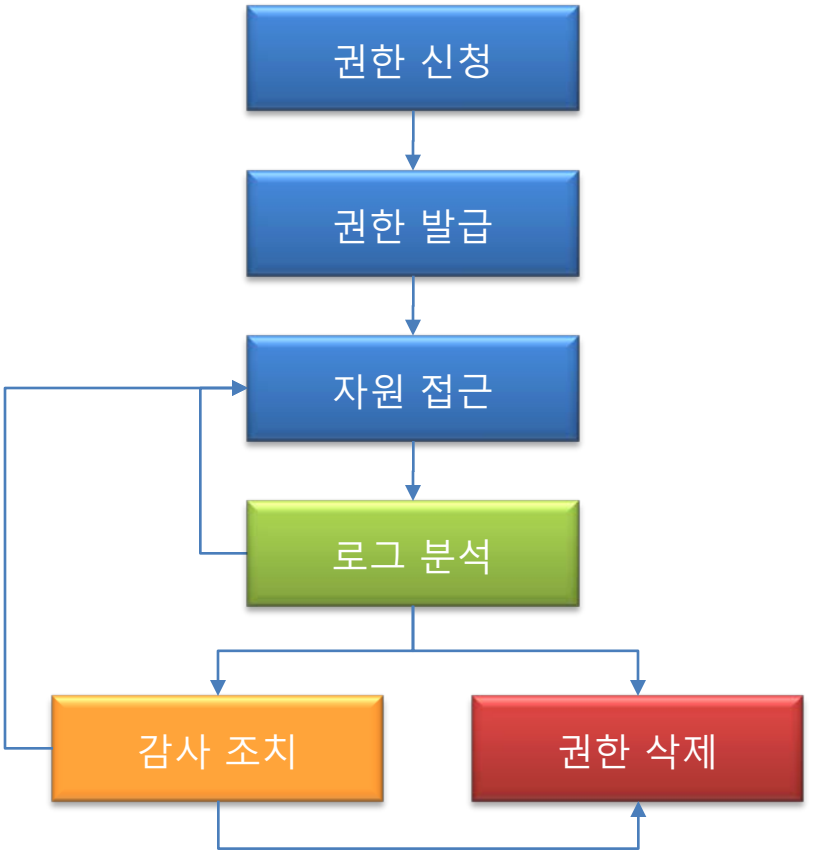
- **통합관리서버 운영 환경**

OS	Microsoft Window 2003 Server 이상
H/W	CPU: Intel Xeon Dual Core 2GHz*2EA 이상 MEM: 4GB Main Memory 이상 HDD: 300GB 이상
DBMS	MS SQL Server 2005 이상
Web Server	IIS 6.0 이상

계정 및 권한 관리 Life Cycle



- 업무시간 외 로그인 시도
- 만료계정 로그인 시도
- 장기 미사용 계정 조치
- 비 소유 계정 로그인 시도
- 미사용 계정



- 업무시간 외 접근 시도
- 장기 미사용 권한 조치
- 권한 없이 접근한 경우 감사
- 과다 발급 권한 제한
- 미사용 권한 삭제

iGRIFFIN 특장점

구분	기존 계정관리시스템	iGRIFFIN
계정 관리 측면	• 계정관리 지원 - 서버 (Unix, Windows), DB계정 • 신청서 기반 워크플로우 지원 - 전자결재 연동 가능 • 사용자 매핑기능 제공 - Id/pw 기반 • **계정관리시스템 적용 강제화 방안 부재** **→ 시스템 관리자가 로컬에서 임의로 계정 생성 가능**	• 계정관리 지원 - 서버 (Unix, Windows), DB계정 (지원예정) • 신청서 기반 워크플로우 지원 - 전자결재 연동 가능 • 사용자 매핑기능 제공 - ID/PW 기반 사용자 매핑 **- PKI 인증서을 통한 복합인증체계 기반 사용자 매핑** **- BIO 지문인증을 통한 복합인증체계 기반 사용자 매핑** • **계정관리시스템 적용 강제화** **→ 서버보안을 통한 권한관리 기능을 이용해 로컬에서의 계정 생성 통제, 계정관리시스템을 통해서만 계정 생성 가능** • **Life cycle 기반 계정관리** **→ 복합인증체계기반 로그인 로그 분석을 통해, 미사용 계정, 과다 신청 계정, 비인가 사용 계정 등 감사추적 및 삭제 가능**
권한 관리 측면	• 권한관리 기능 없음	• **명령어 실행에 대한 실시간/사전 승인절차 제공** • 복합인증체계 기반(PKI, BIO인증 연동) 권한관리 지원 → super-user 권한분리 지원 • 신청서 기반 워크플로우 지원 - 전자결재 연동 가능
감사 및 Compliance 측면	• 계정관리시스템을 통해 생성된 계정 정보를 통해 계정별 소유자(계정-사용자 매핑) 내역 제공	• 계정관리시스템을 통해 생성된 계정 정보를 통해 계정별 소유자(계정-사용자 매핑) 내역 제공 • **복합인증체계 기반 사용자 행위 감사 내역 제공** **→ 사용자 Key-stroke, 작업 화면 등** • **권한 신청 및 접근통제 정책 현황 자료 제공** • **법/제도 준수(Compliance)를 위한 보안정책 적용 방안 및 보안정책 적용에 따른 감사 자료 제공 가능**

주요 기능 (1/2)

구분	상세 작업 내용
인증 및 권한분리	• 서버그룹별로 보안관리자의 권한을 일반,조회,시스템권한으로 분리
명령어 제어	• 명령어 실행에 대한 실시간/사전 승인절차 제공
서버관리	• 보안관리 대상 서버 자산 정보를 데이터베이스화 관리 • 주기적인 모니터링을 통한 시스템상태와 에이전트 운영현황 업데이트 • 관리대상 서버의 에이전트 운영모드 원격 제어 및 일괄 적용
모니터링	• 시스템 상태와 에이전트 운영현황을 볼 수 있는 대시보드 • 접근위반로그 발생 통계정보와 실시간 위반로그 모니터링 뷰 • 시스템 자원 사용률 모니터링 정보를 제공하는 대시보드 • 시스템 구성도를 도식화된 그래프로 볼 수 있는 대시보드
감사로그	• 관리 대상 서버에서 발생한 서버보안로그 통합 관리 • 접근통제 로그 / 사용자행위 감사로그 / PKI 인증로그 / 계정관리 로그 / 인증서관리 로그 검색 제공 • 다양한 검색조건을 통한 로그 검색, 엑셀파일로 결과 저장
보고서	• 자동 수집된 로그를 통해서 통합 보안로그 분석 보고서 생성 • 서버별, 기간별, 항목별 감사로그 통계 보고서 제공 • 다양한 분석 항목 지원(파일접근위반, 로그인위반, 네트워크위반, 관리자정책변경, 사용자접근내역) • 다양한 보고서 출력형식 지원(PDF, DOC, HTML, EXCEL 등)
관리자기능	• 보안관리자 등록 및 권한 설정 • 보안 관리자의 작업 이력 조회

주요 기능 (2/2)

구분	상세 작업 내용
계정관리	• 주기적으로 수집된 시스템 계정 정보를 통해 통합 계정관리 • 서버 계정 생성/수정/삭제 • 계정 암호 변경 • 계정 잠금/해제 • 계정 만료일 설정 • 계정 마지막 로그인시간 정보 조회 • 계정 현황 분석 (유휴계정/잠김계정/만료계정) • 계정 그룹 생성/수정/삭제 • 계정 그룹 맴버 변경(맴버 추가/제거)
인증서관리	• 사설 인증서 관리 센터 제공 • 인증서 발급 • 인증서 관리 • 인증서 잠금/해제 • 인증서 폐기 • 타기관인증서 등록
복합인증관리	• PKI인증서 기반 복합인증시스템을 구축, 보안강도를 강화 • 계정과 실사용자간의 인증서 매핑 • PKI인증로그를 통해서 실사용자 로그인 로그 생성 • 사용자행위로그와 연동을 통해 실사용자의 사용자행위로그 생성

상세 기능 > 관리자 인증 및 권한분리

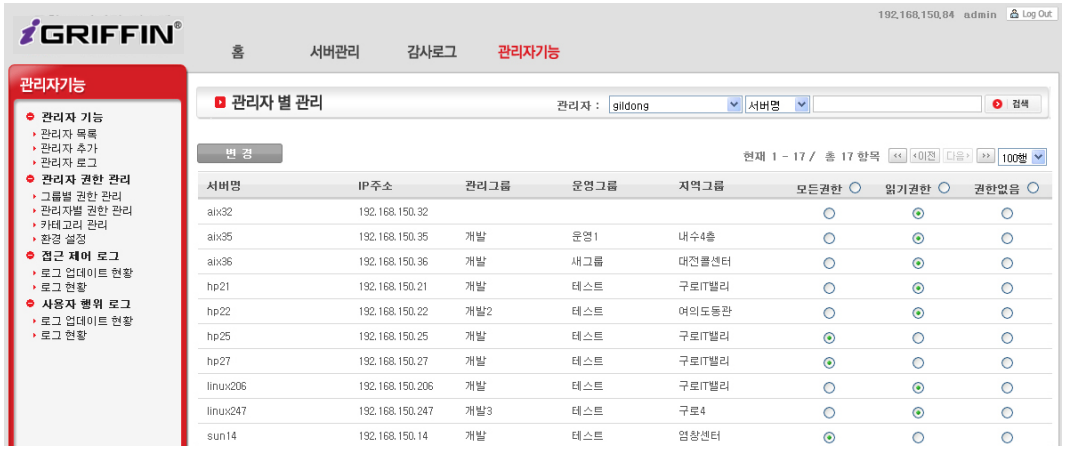
- 모니터링하는 관리자를 시스템관리자와 일반관리자로 분리
- 시스템 관리자는 모든 권한을 일반관리자는 주어진 권한만을 가짐
- 모든 서버에 대해 서버단위로 "모든 권한/읽기 권한/권한 없음" 으로 설정 가능

보안관리자 인증

- 보안관리자는 통합관리콘솔을 사용하기 위해서 인증 과정이 필요함
- 보안관리자 인증을 통해 관리자별 권한이 부여됨

개별 서버 권한 설정

- 관리자에게 개별 서버에 대한 권한을 설정

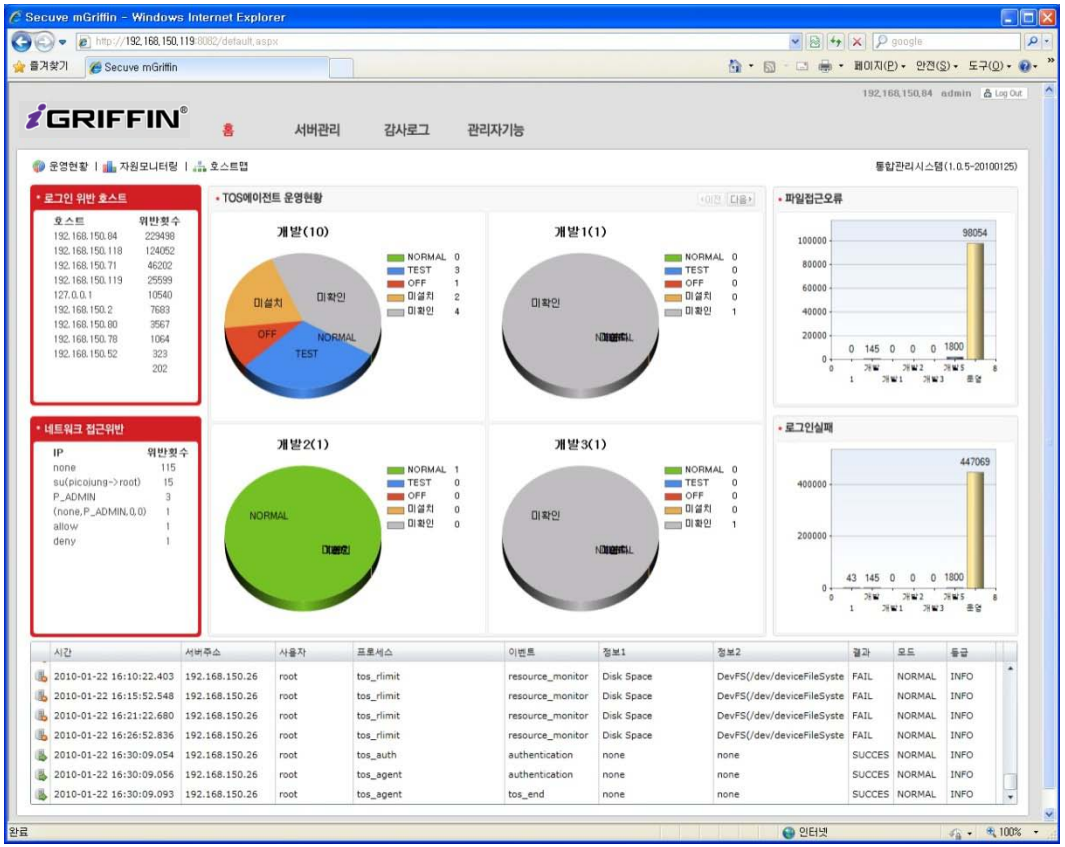


상세 기능 > 대쉬보드

- 그래프 형태를 통해 전체 서버 상황을 일목요연하게 확인 가능
- 여러 조건을 통한 서버의 상태 확인 가능
- 에이전트를 통해 주기적으로 등록된 서버의 정보를 갱신

운영현황

- 그래프를 통해 전체 서버의 운영 상태를 손쉽게 파악할 수 있음
- 서버 운영 상태 및 로그 현황의 확인이 용이
- 설정을 통한 실시간 업데이트 기능



상세 기능 > 원격 제어

- 해당 서버의 에이전트 운영 현황의 확인 및 제어 기능
- 선택한 복수의 서버에 대한 일괄 제어 기능

에이전트 제어

- 에이전트의 현재 운용 상태를 확인
- 에이전트의 운용 상태 변경 가능
- 제어에 의한 실행결과를 확인

[TOS에이전트정보]

설치여부	true	
설치디렉터리	E:₩Program Files (x86)₩Secuve₩TOS Agent for Windows	
설치일	2010-01-06 18:01:40	
버전	3.0	
포트	43000	
에이전트상태	Running	Start / Stop
운영모드	NORMAL	Normal / Test

일괄 제어

- 복수의 서버에 대한 일괄 작업 기능
- 일괄 작업 서버에 대한 결과 및 자세한 내용의 파악이 가능

Secuve TOS™

작업	TOS 에이전트 시작
관리자 아이디	admin
작업 시작 시간	2010-01-18 오후 1:52:34
전체 대상 서버	5항목
현재 처리중인 서버	aix36
현재 처리중인 서버IP	192.168.150.36
완료율	완료 서버 : 0 / 전체 서버 : 5 (0%)

작업중지

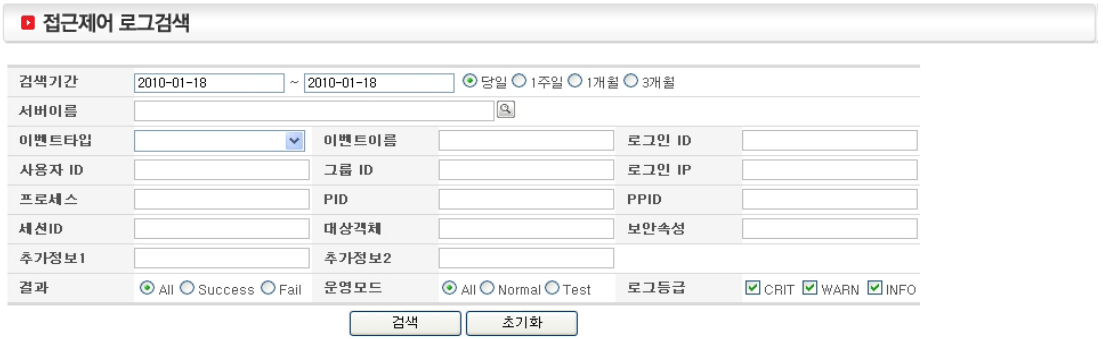
서버	결과	내용
aix36(192.168.150.36)	실행중	TOS 에이전트 시작
hp21(192.168.150.21)	대기중	대기중
hp22(192.168.150.22)	대기중	대기중
hp23(192.168.150.23)	대기중	대기중
hp25(192.168.150.25)	대기중	대기중

상세 기능 > 감사로그

- 보안 대상 서버의 로그 통합 관리
  - 이 기종 서버의 TOS 로그를 데이타베이스로 수집
- 주기적인 로그수집을 통해 관리 서버의 로그를 자동 수집
- 접근제어 / 사용자 행위 등의 로그를 다양한 조건을 통해 검색

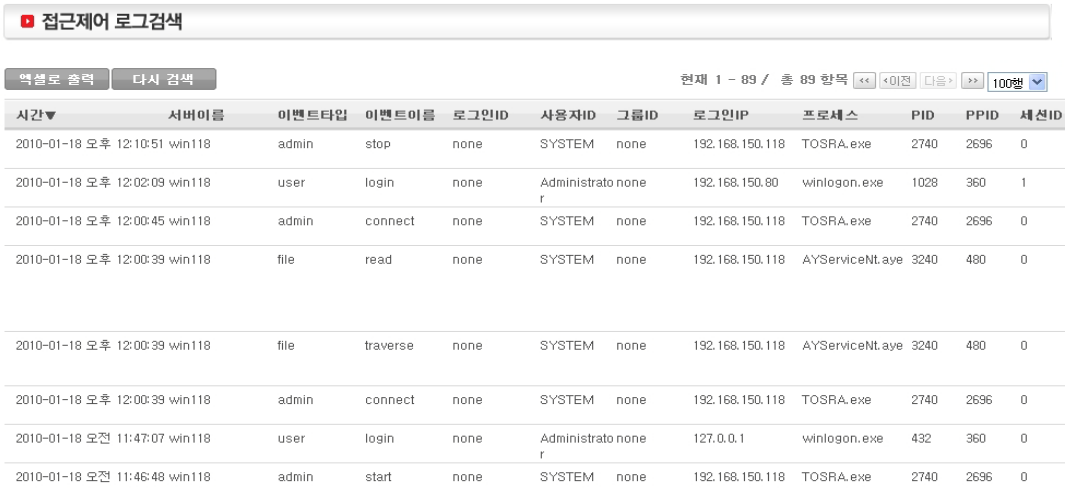
감사로그 검색 조건

- 검색기간별 조회 할 수 있는 여러 조건을 통해 단일 서버 또는 여러 서버의 로그를 검색



감사로그 검색 결과

- 검색된 로그결과를 각 항목별로 정렬할 수 있으며, 전체 리스트를 엑셀로 저장
- 상세보기를 통해 한 개의 로그에 대한 분석 용이

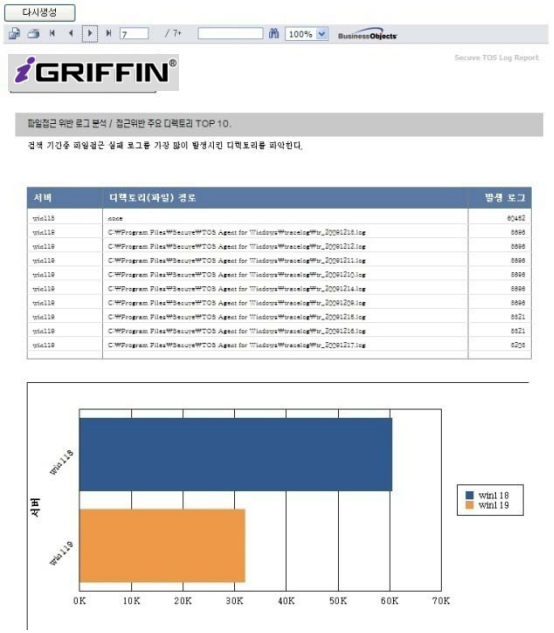


상세 기능 > 보고서

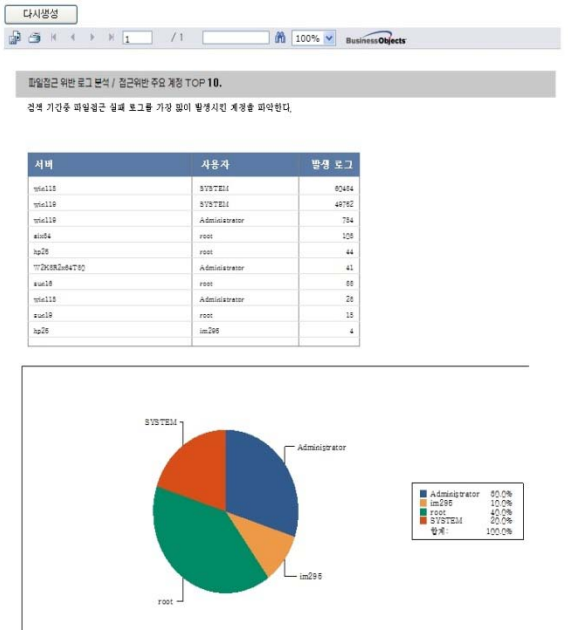
- 수집된 감사로그를 통한 각 항목별 보고서
- 기간별 특정 서버 또는 전체 서버별 보고서
- 다양한 보고서 항목 지원 (기본보고서, 상세보고서, 사용자정의 보고서)
- 다양한 파일 형식으로 저장 및 프린트 기능 지원

보고서 분석 결과

- 기간별 설정을 통한 로그 검색 결과를 이용해 보고서 생성
- 각 로그 분석에 대한 설명 제공
- 로그분석 결과에 대해 관리자가 쉽게 알아 볼 수 있도록 챠트 제공
- 챠트에 대한 상세내역을 제공해 세부정보 확인
- 다양한 파일 형식 저장(pdf, word, excel)
- 프린트 기능 지원



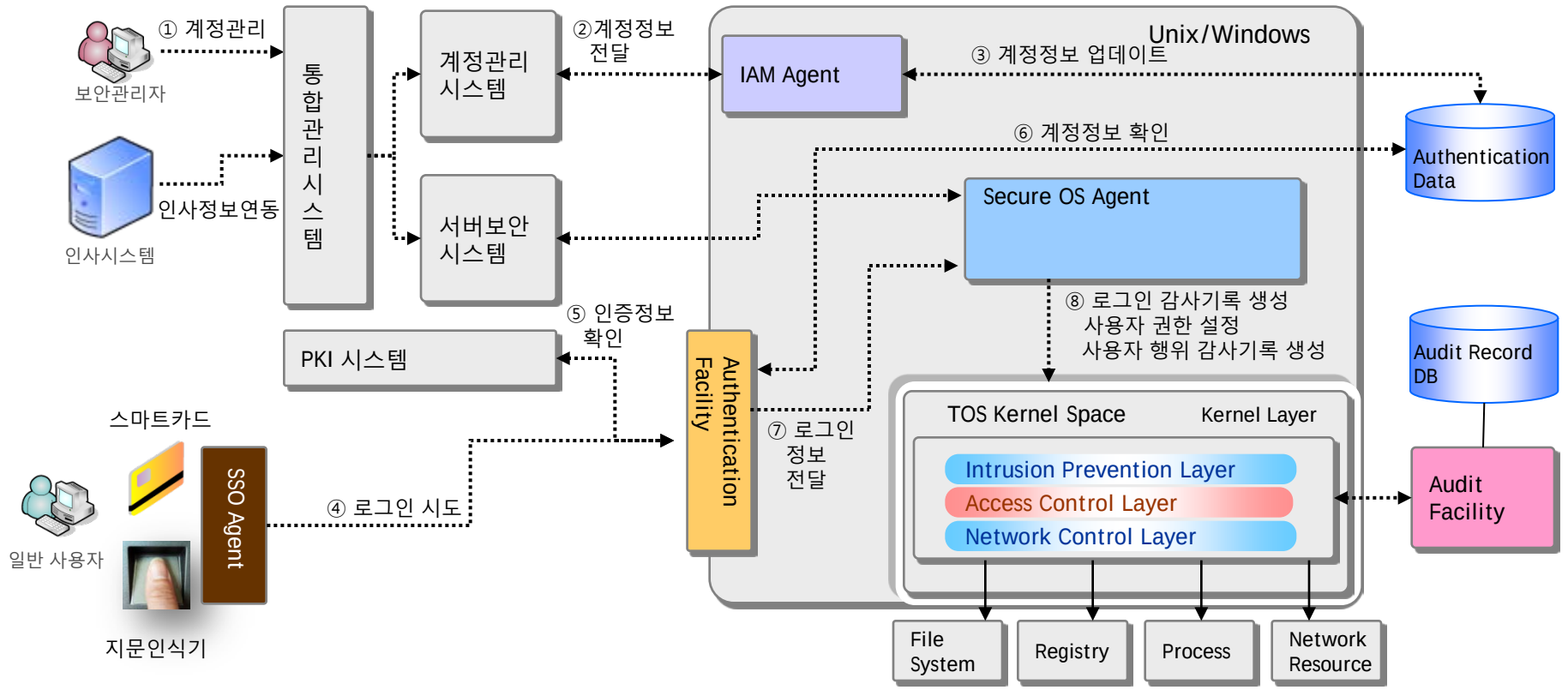
접근위반 주요 디렉터리



접근위반 주요 계정

계정권한관리 시스템 **도입사례**

K은행, D은행



특징	▪ 통합관리시스템을 통해 계정관리시스템과 서버보안시스템을 연동 관리 ▪ 인사정보를 연동하여, 계정/권한관리 Provisioning ▪ **PKI / 지문인증** 시스템과 연동하여, 복합인증체계 기반의 권한관리 및 보안 감사 ▪ **PKI / 지문인증** 정보를 이용하여, 복합인증체계 기반의 사용자 행위기록 생성	▪ 적용 대상 시스템 **Mainframe, Unix/Windows 서버, DBMS**

• 제안 시스템 기술 소개

1. 복합인증 및 행위감시 메커니즘

2. 상세설명

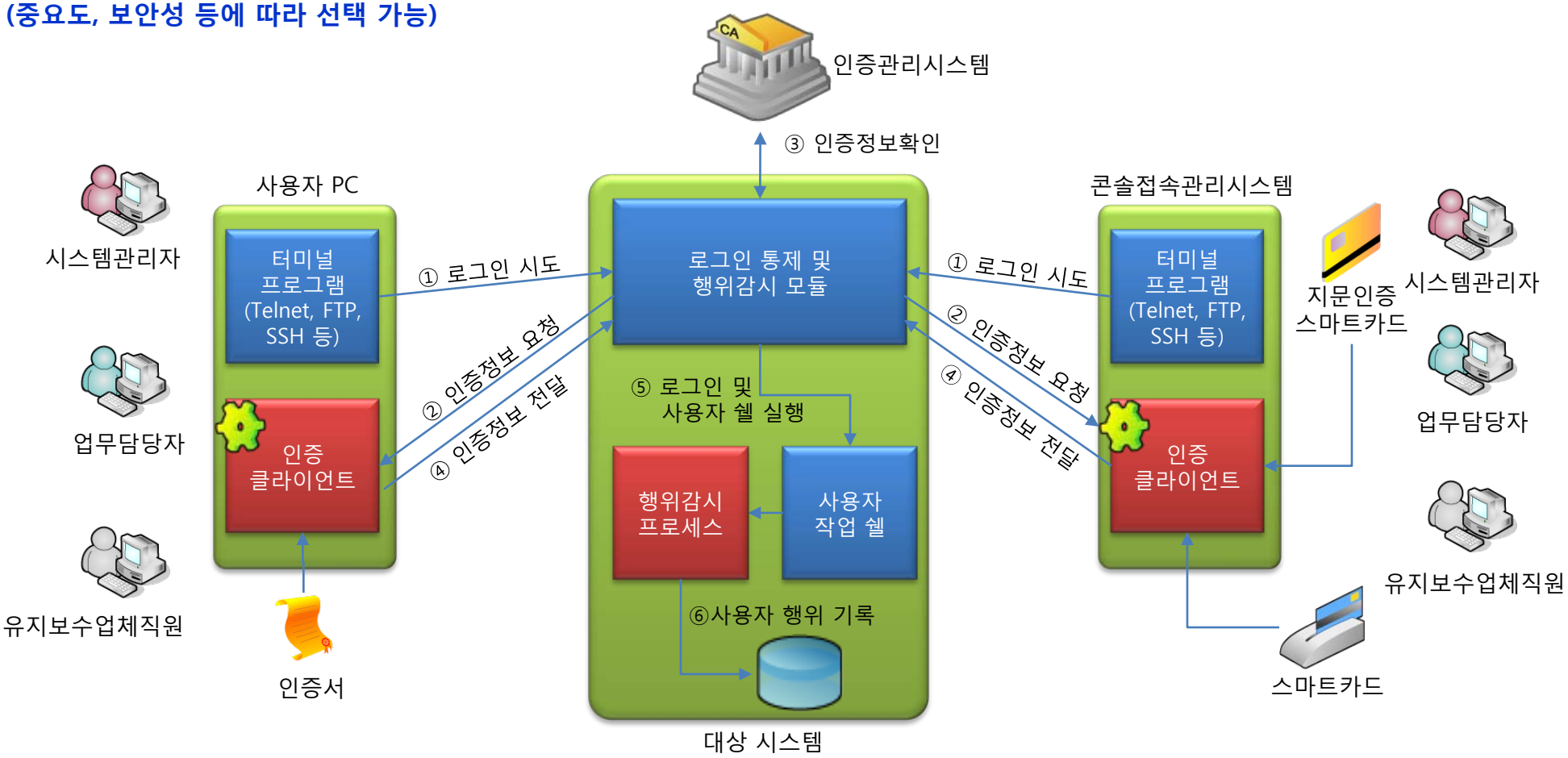
3. 대응 시나리오

4. 위변조 방지매체 저장

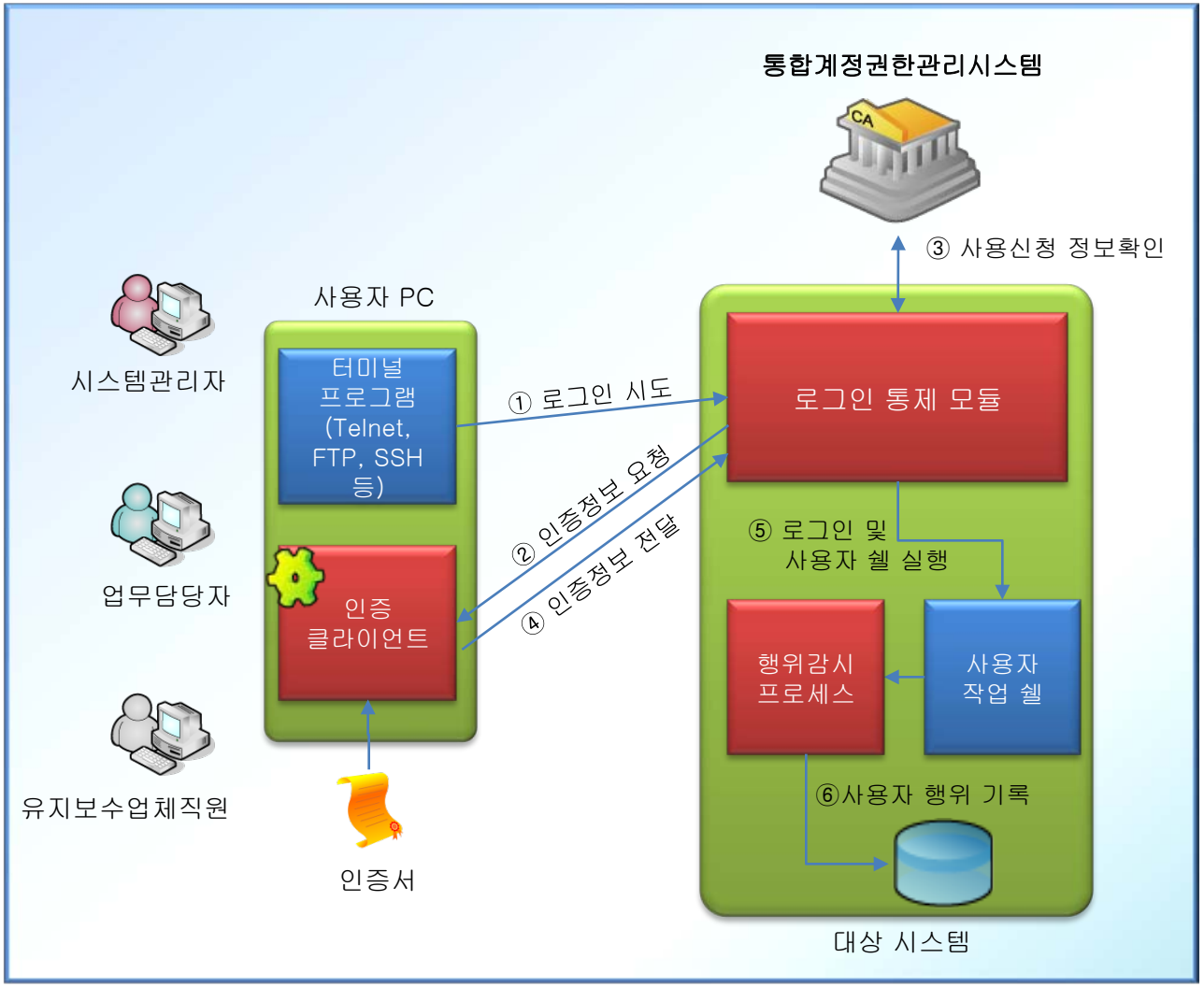
5. 기대효과

복합인증 및 행위감시 메커니즘

- 콘솔접속관리시스템과 사용자PC에 "인증 클라이언트"를 설치하고 대상 시스템에는 "로그인 통제 및 행위감시 모듈"을 설치
- 사용자는 기존에 사용하던 터미널 프로그램(SecureCRT, Putty, AlFTP 등 어떤 프로그램도 관계 없음)을 이용하여 대상 시스템에 접근 시도
- "로그인 통제 및 행위감시 모듈"과 "인증 클라이언트"가 background로 복합인증체계 인증 작업 수행
- 복합인증체계 인증을 위해 PKI 인증을 수행하며, 인증서 정보는 하드디스크 저장방식, 스마트카드 방식, 지문인증 스마트카드 방식을 지원 (중요도, 보안성 등에 따라 선택 가능)



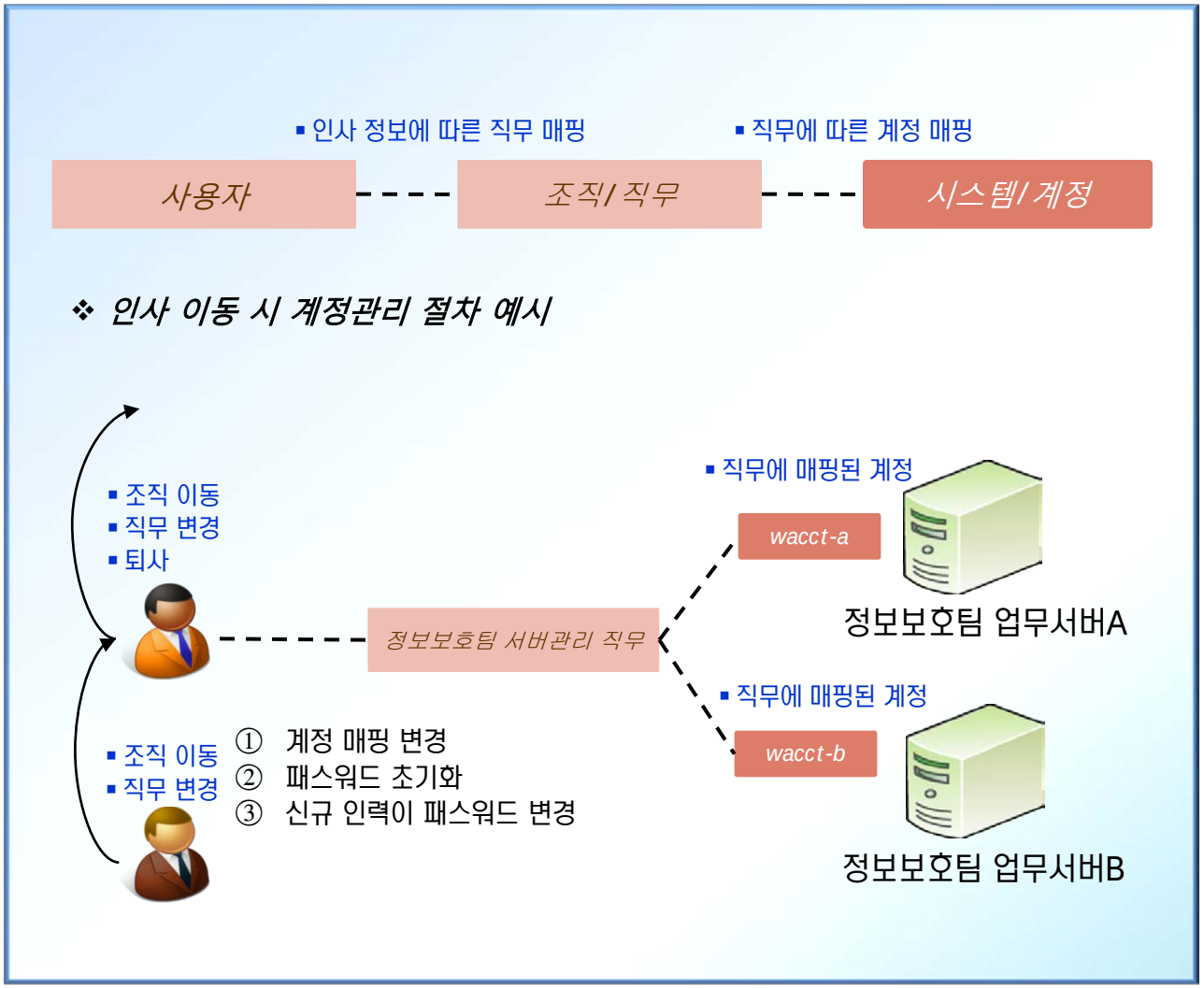
상세설명 - 복합인증체계기반 실 사용자 식별



- **수행 절차**
  - 각 사용자 별로 인증서 발급 및 등록
  - 사용자PC에 인증 클라이언트와 인증서 설치
  - 사용자가 시스템 접속 도구를 사용하여, 시스템에 로그인을 시도할 경우, 로그인 통제 모듈과 인증 클라이언트가 인증서를 이용해 인증 작업 수행하여, 실 사용자 신원을 확인
  - 확인된 사용자 정보를 통해 '통합계정권한관리시스템'에 계정 사용 가능 여부를 확인

- 인증 방식은 PKI인증서, 지문인증, 기 운영 중인 SSO 등 복합인증체계를 식별할 수 있는 인증기술은 연동 가능
- 시스템 접속 도구는 기 사용중인 어떠한 프로그램도 동작 가능

상세 설명 - 역할기반 계정관리

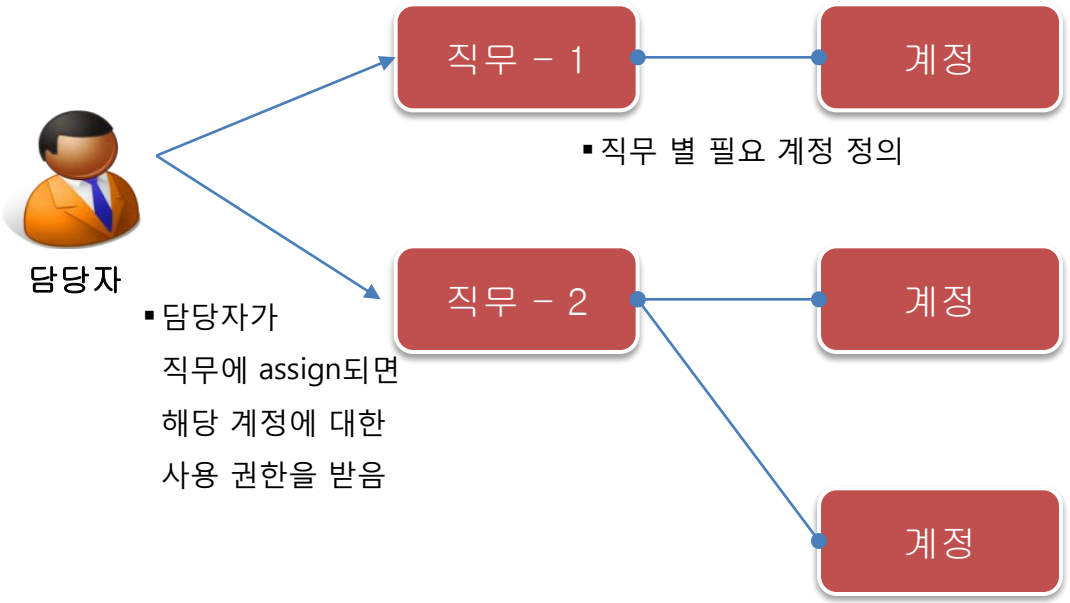


- **수행 절차**
  - 직무 별 업무상 필요한 계정을 정의
  - 해당 직무에 해당하는 사용자와 계정을 mapping
  - 사용자의 부서이동, 직무 변경, 퇴직 등이 발생할 경우 사용자와 직무간의 mapping 관계만 변경

- 사용자는 직무 변경 후 해당 계정과 password를 알고 있어도, 앞서 설명한 복합인증체계 기반 실 사용자인증을 통해, 해당 시스템에 접근할 수 없음
- HR정보와 연동될 경우, 인사이동 시 자동으로 계정까지 변경 관리되는 Auto-provisioning 시스템 구축 가능

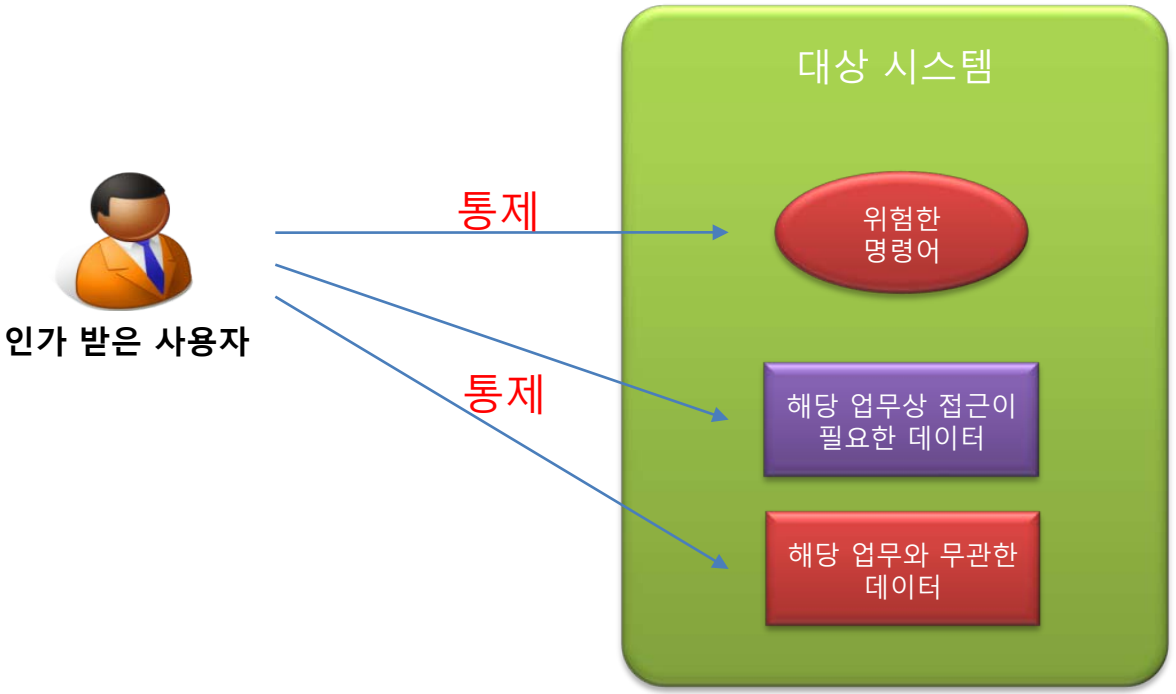
상세설명 - 계정관리방안

- 시스템에 존재하는 다양한 취약계정에 대한 관리 방안 필요
- 직무에 기반한 사용자 별 계정 부여 및 관리 방안 필요
- 업무 수행에 필요할 경우, 결재권자의 승인을 받아 계정 부여
- 전 시스템 상에 존재하는 계정은 **'담당자 – 업무 – 계정'**의 명확한 관계를 가진 계정만 존재하도록 관리
- 인사이동 (직무 변경, 퇴직 등) 발생 시 해당 인사정보에 해당 직무를 잃게 되면, 계정 사용권한도 자동으로 잃게 됨

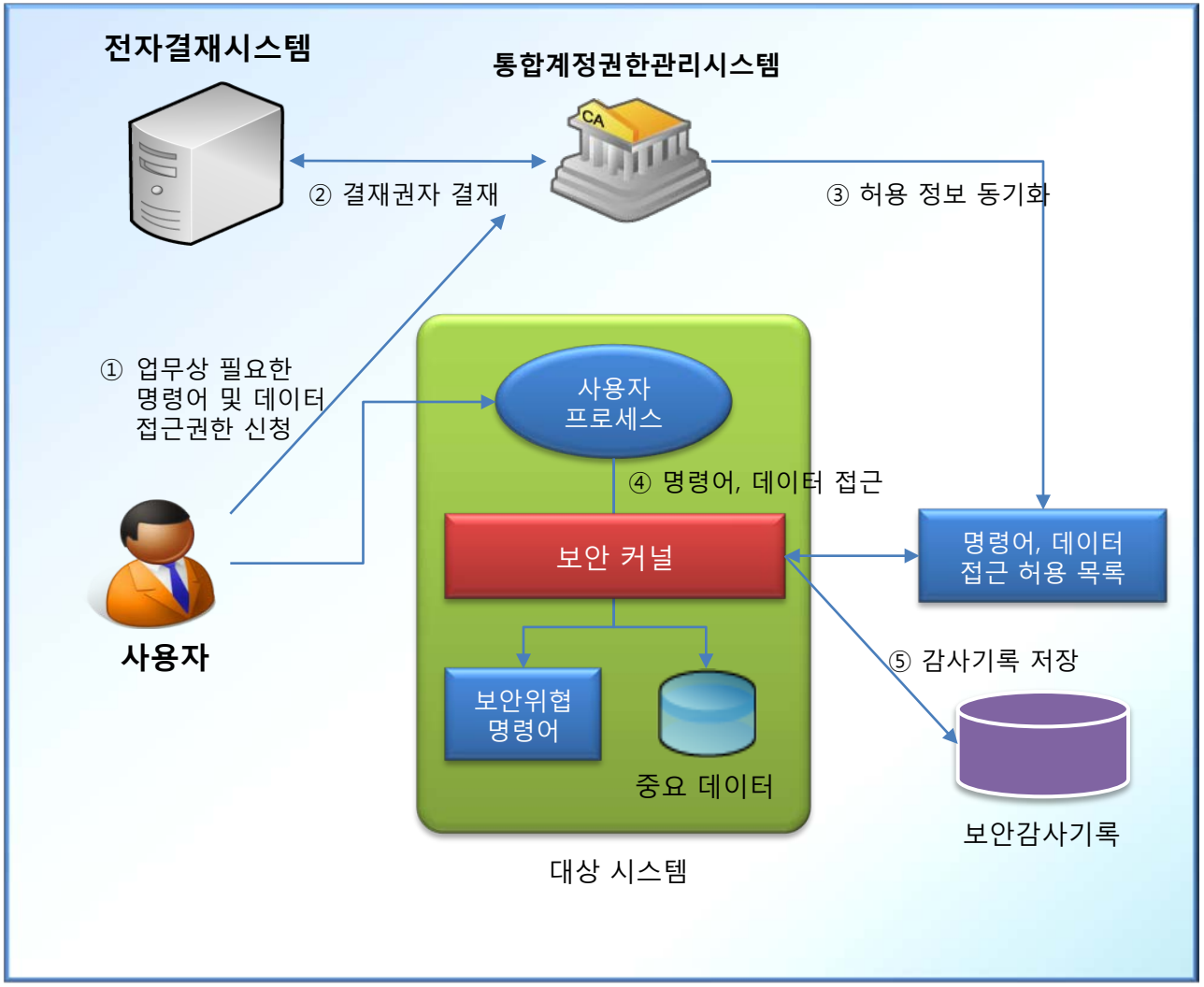


상세설명 - 권한제어방안

- 작업이 승인된 사용자가 시스템에 접근한 후, **예정된 작업만 수행하도록 강제화**할 수 있는 방안 필요
  - 시스템에 **위험을 미칠 수 있는 주요 명령어**의 실행 권한 통제
  - 해당 **업무상 꼭 필요한 데이터만 접근할 수 있도록 강제화**하는 권한 통제



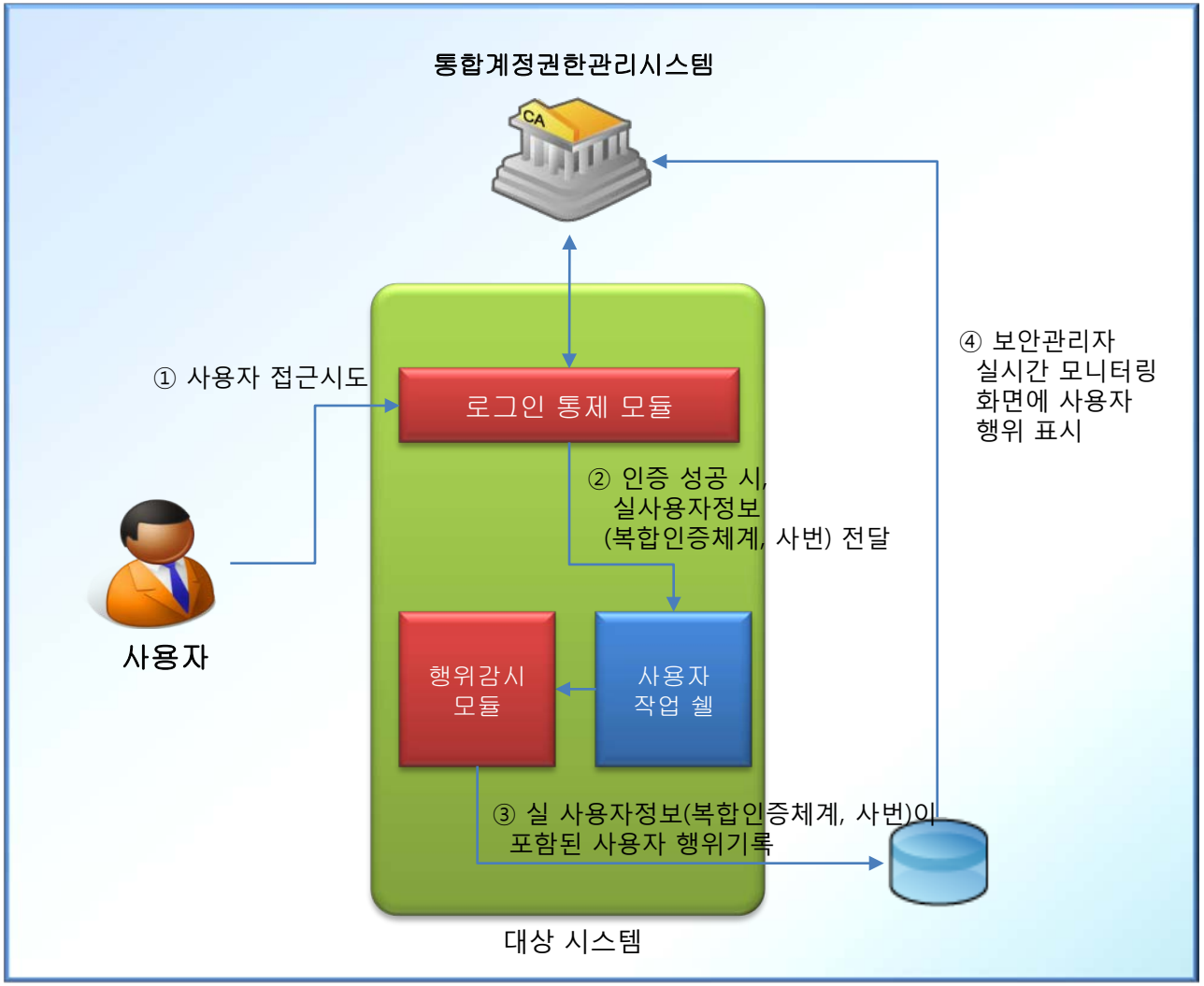
상세설명 - 명령어/데이터 접근 통제



- **수행 절차**
  - 사용자는 업무상 필요한 명령어 및 데이터에 대한 접근 신청을 수행
  - 결재권자와 보안관리자의 승인
  - 허용 정보 동기화
  - 사용자 작업 수행
  - 사용자 접근에 대한 감사기록 저장

- **신청 및 결재된 내역 없이는 최고권한계정 사용자도 해당 명령어 및 중요 데이터 접근 불가**
- **보안감사기록을 통해, 해당 명령어 실행 기록 및 데이터 접근 기록 확인**

상세설명 - 사용자 행위감사

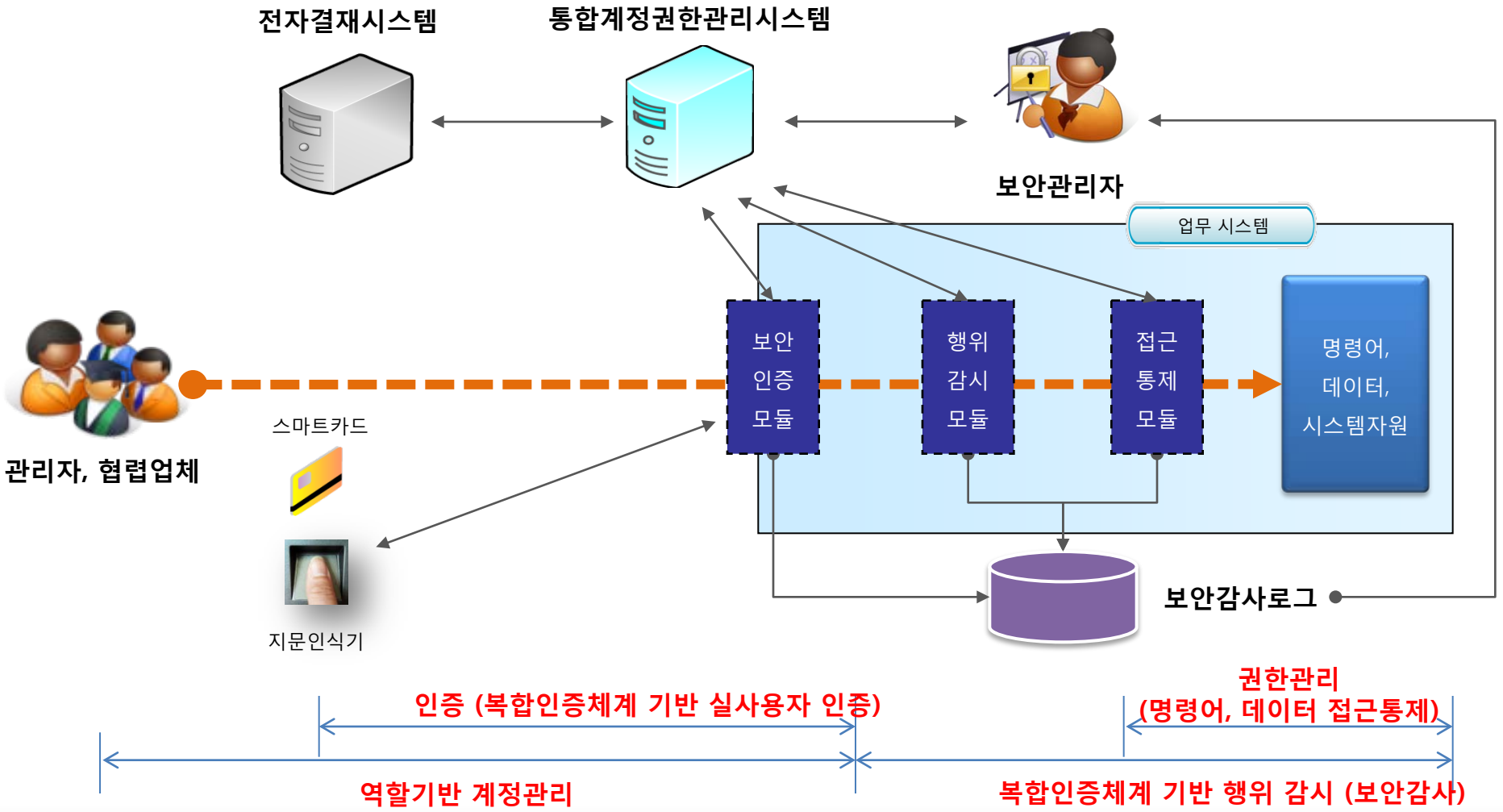


- **수행 절차**
  - 사용자 로그인 시, 실 사용자 신원확인을 거친 후, 실 사용자 정보(복합인증체계, 사번 등)를 행위감시 모듈에 전달
  - 사용자의 모든 key-stroke 행위를 실사용자 정보와 함께 감사로그에 기록
  - 비정상 행위 수행자는 보안관리자 모니터링 시스템에 실시간 로그로 표시

- **비정상 행위는 보안관리자에 의해 다양한 형태로 정의**
- **Windows 계열도 동일하게 지원하며, 사용자 이벤트 발생 시 화면 캡쳐를 기록하는 방식으로 제공**

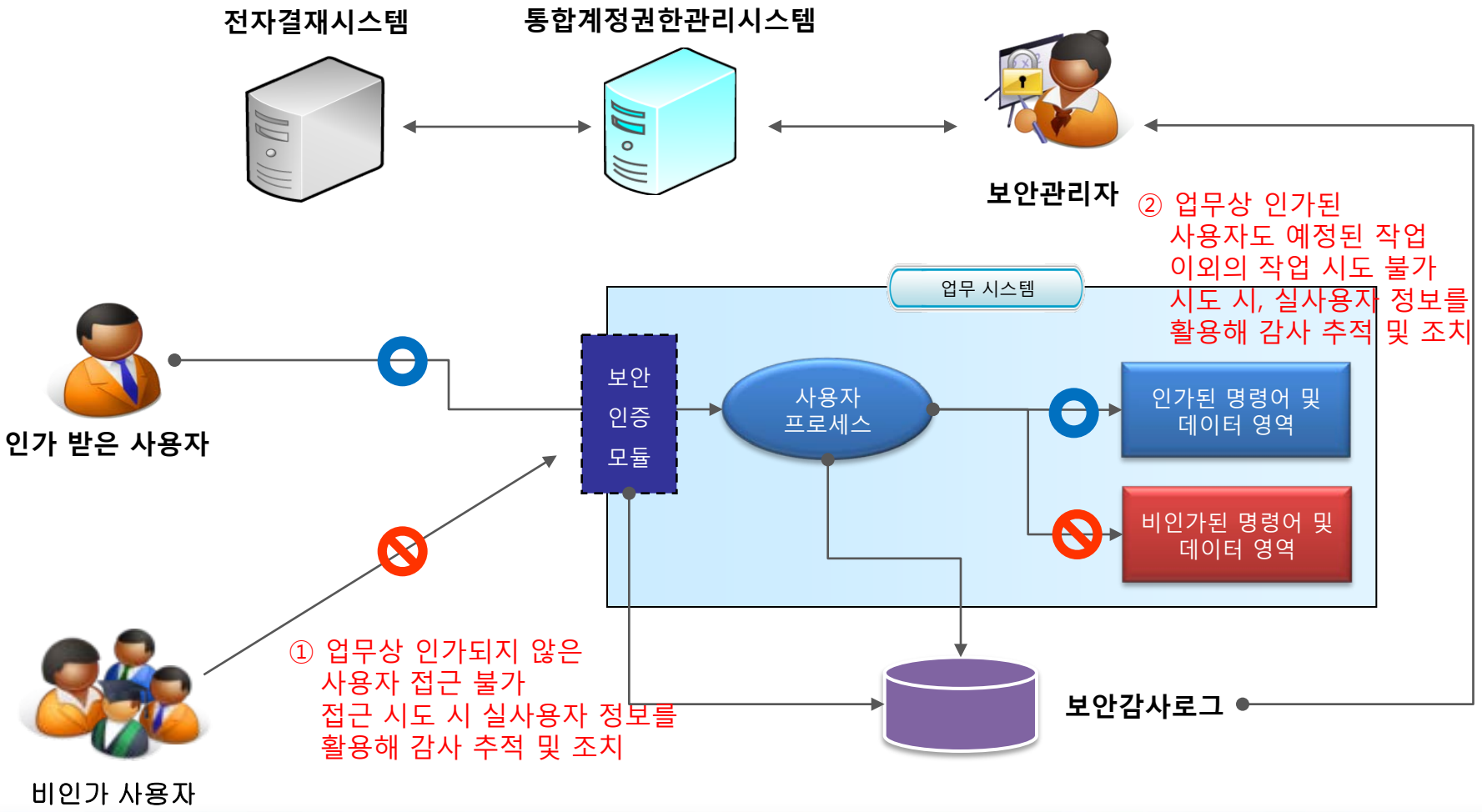
상세설명 - 단계별 시스템 제어

- 시스템 데이터 및 서비스의 안정성 확보를 위해서는 **'인증-계정-권한-보안감사'**의 4단계 시스템이 **Workflow 기반의 관리 기능**과 결합된 모습으로 구현될 경우 **보안성과 효율성 극대화** 가능



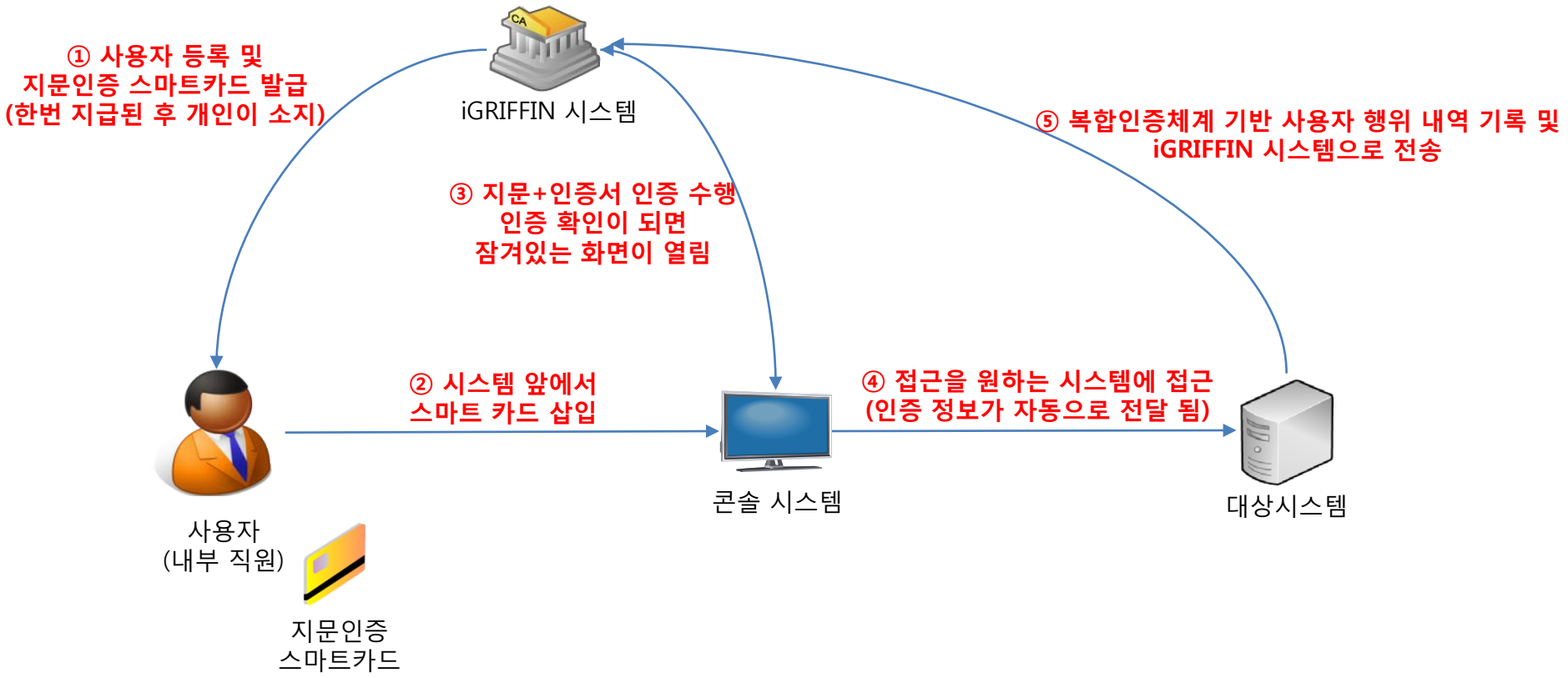
대응시나리오

- 사전에 승인 받은, 사용자만이 시스템에 접근하여, 예정된 작업만을 수행 → 시스템적으로 보안관리자가 확신할 수 있는 시스템
- 업무 담당자의 업무 수행을 위해 접근 권한을 부여하지 않을 수는 없지만, 업무 수행에 필요한 최소한의 권한만을 예정된 시간에만 부여하여 보안 Risk를 최소화



대응시나리오 - 사용자 접근 (1/4)

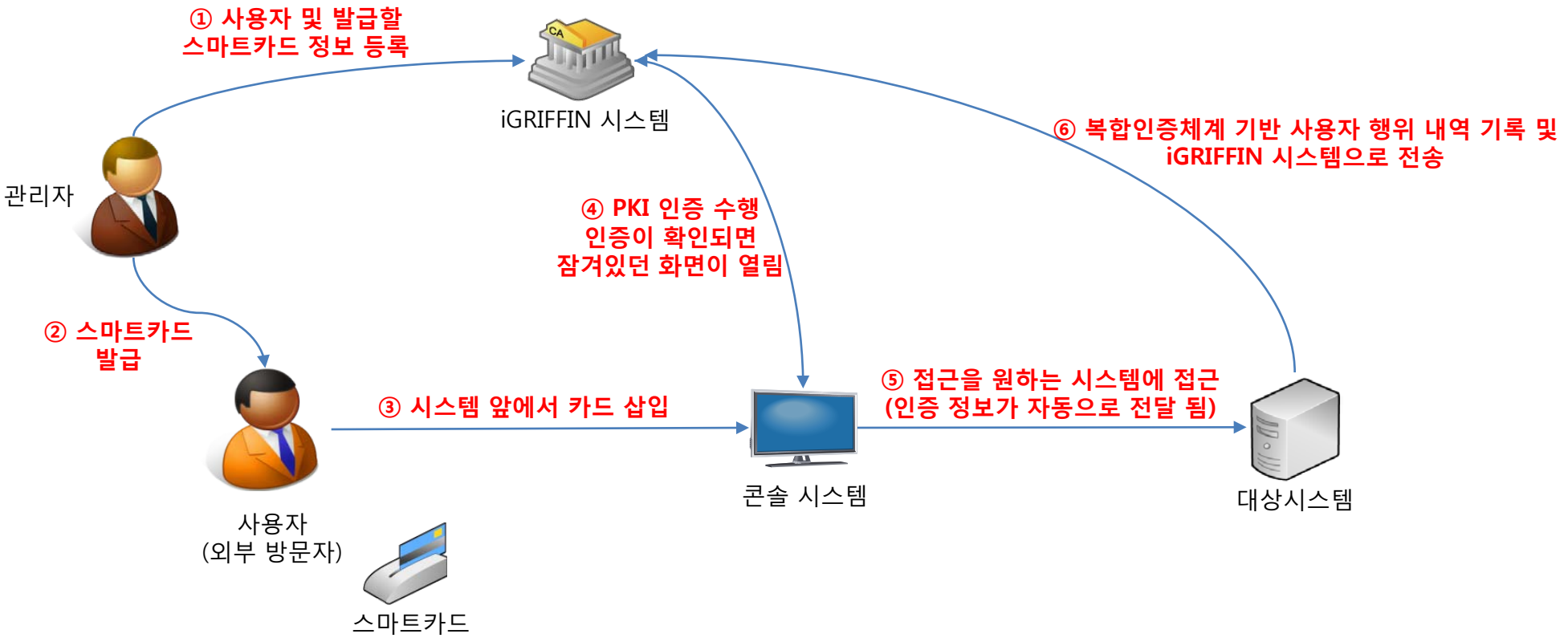
- **콘솔시스템 접근 시나리오 (내부 직원)**



※ HMC, SMS 콘솔 시스템에 로컬 네트워크 연결이 연결되어 있어야 함

대응시나리오 – 사용자 접근 (2/4)

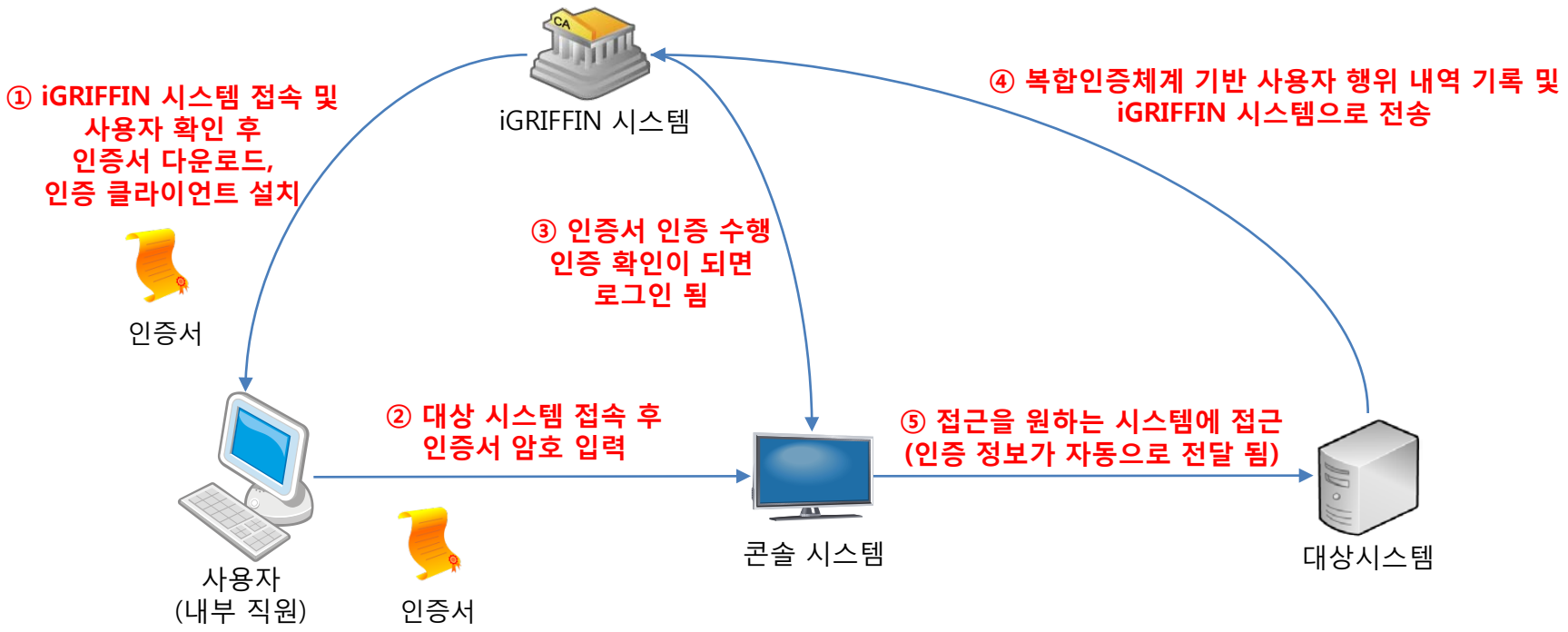
- **콘솔시스템 접근 시나리오 (외부 방문자)**



※ HMC, SMS 콘솔 시스템에 로컬 네트워크 연결이 연결되어 있어야 함

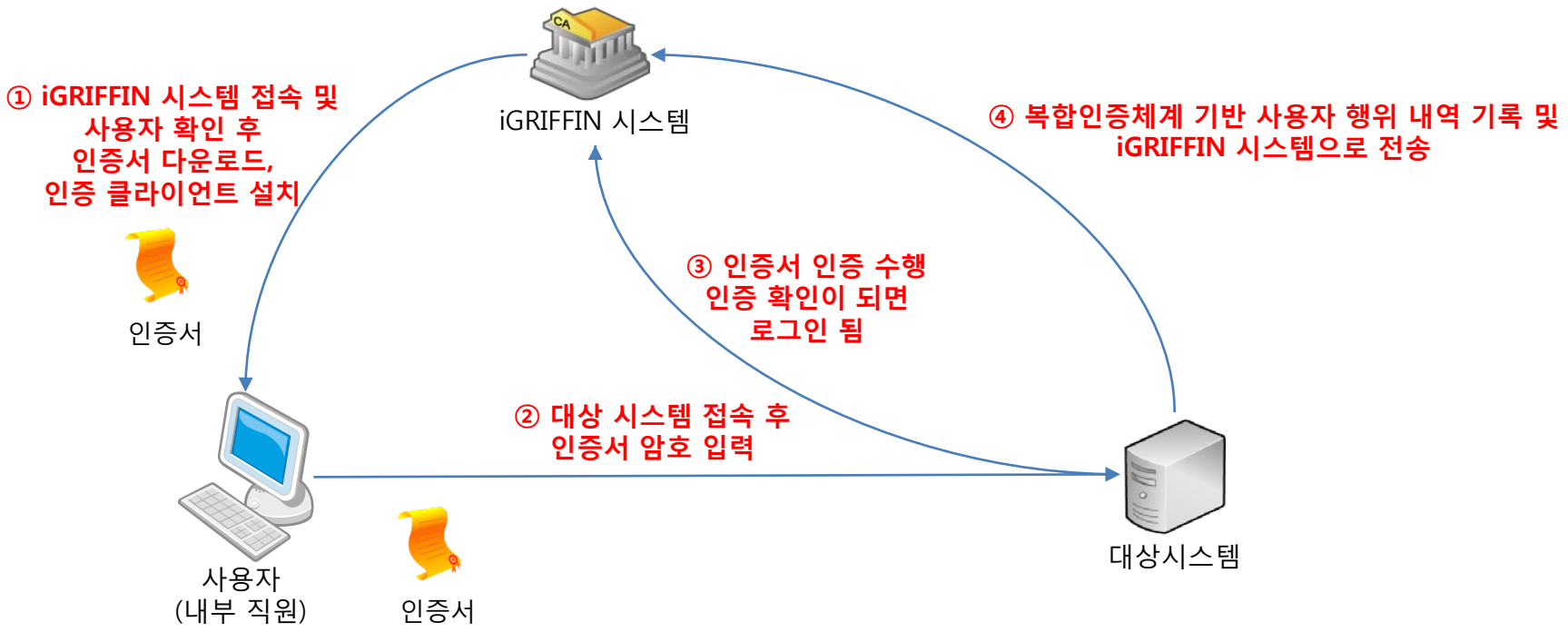
대응시나리오 - 사용자 접근 (3/4)

- **IP 콘솔 시스템 접근 시나리오**



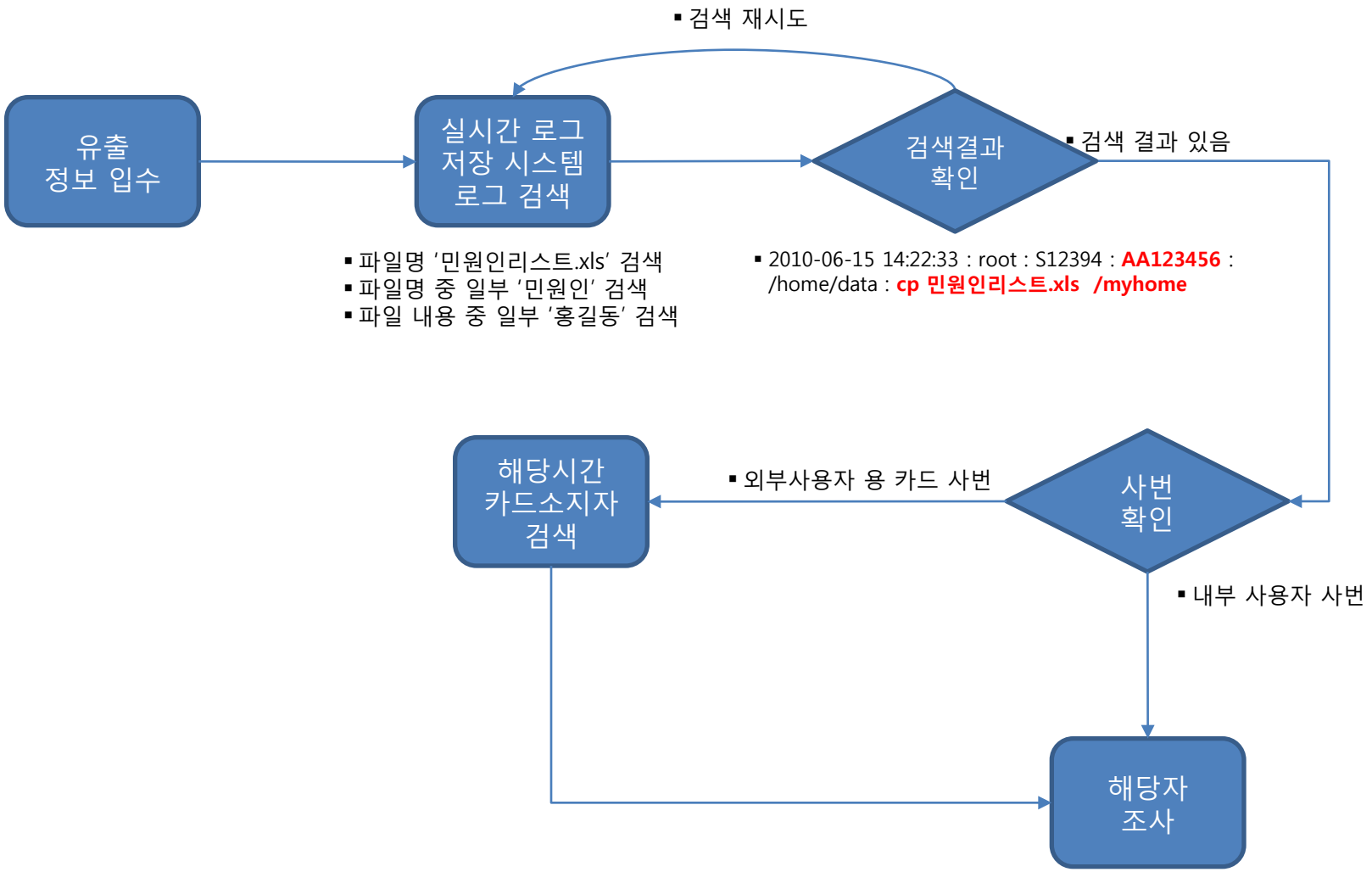
대응시나리오 - 사용자 접근 (4/4)

- **PC 사용자 접근 시나리오**



대응시나리오 - 내부정보유출 대응/추적

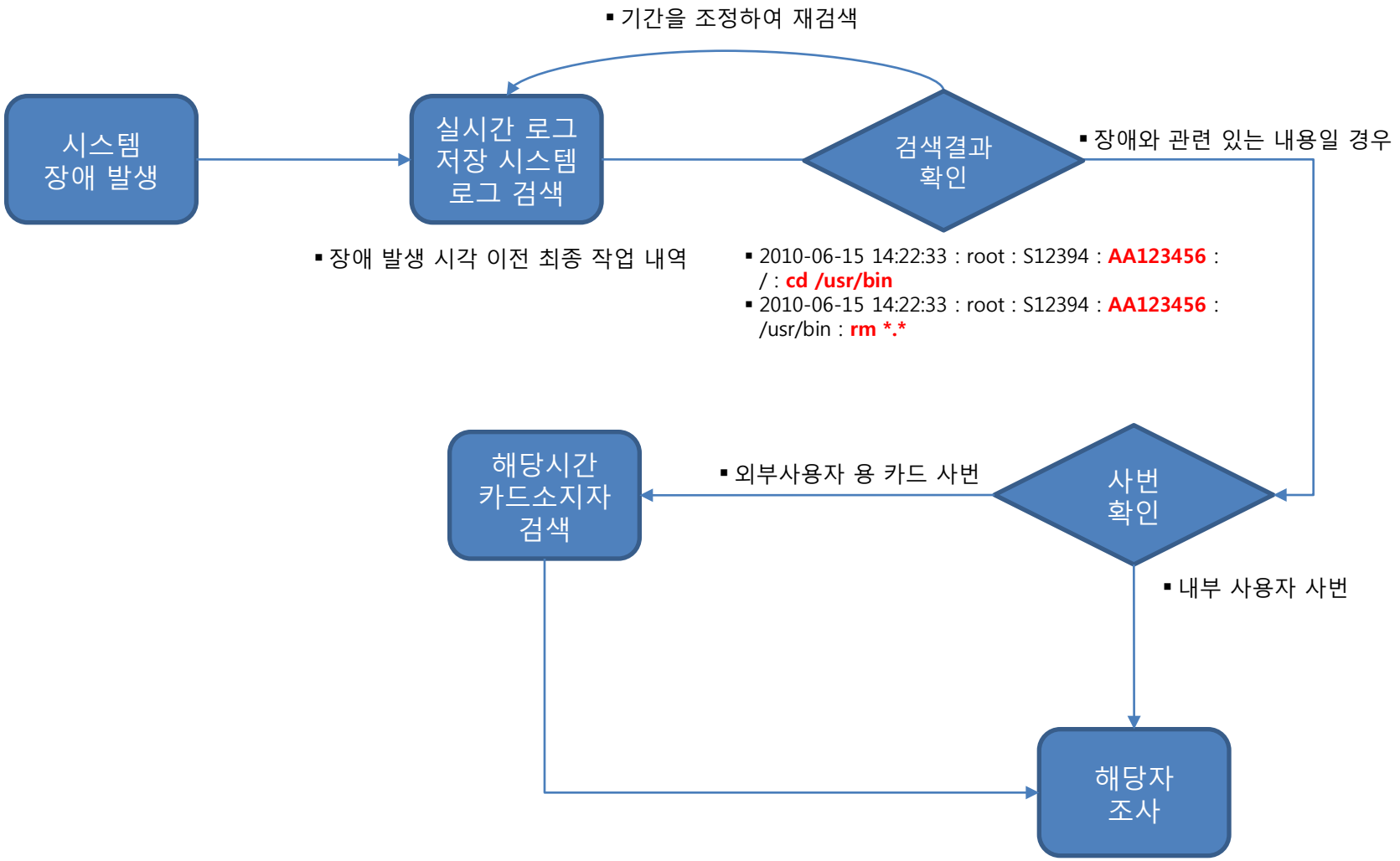
- **내부정보유출 대응 시나리오**
  → 파일명 '민원인리스트.xls'



대응 시나리오 - 시스템 장애 발생 시

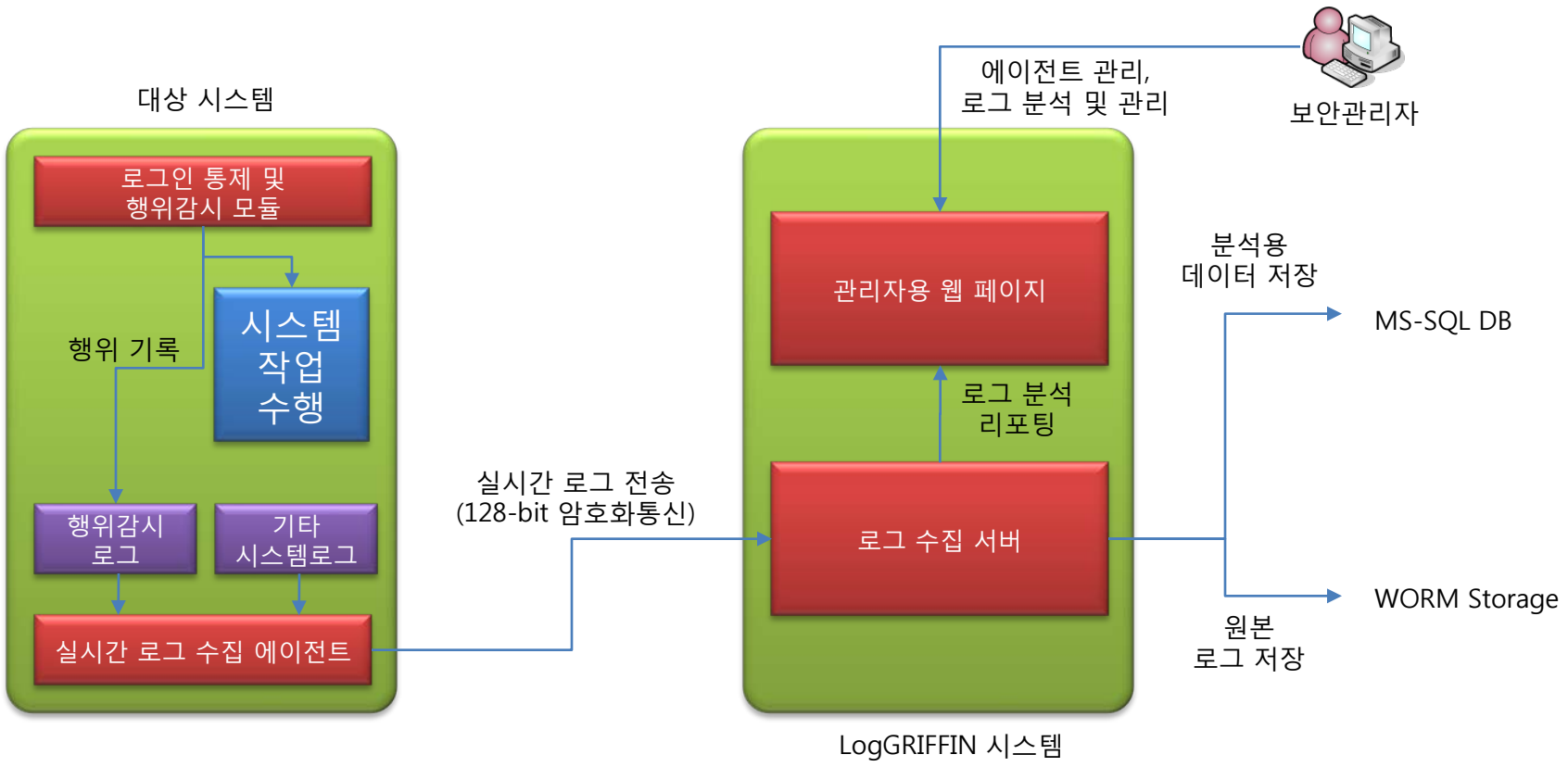
- **시스템 장애 대응 시나리오**

  → /usr/bin 아래 모든 파일 삭제로 인한 시스템 Hang



위변조 방지매체 저장

- 복합인증체계 기반의 사용자 행위 감시 로그를 실시간으로 수집하여 위변조가 불가능한 저장매체(WORM Storage)에 저장
- 저장된 로그는 암호화통신을 이용해 서버로 전송되며, 수집된 로그는 분석용 데이터는 DB에, 원본 로그는 WORM Storage에 저장
- 관리자는 관리자용 웹 페이지를 통해 에이전트 관리, 로그 분석, 로그 관리 등을 수행
- 로그 데이터는 사용자 행위 감시로그 뿐 아니라 기타 다양한 시스템 로그도 수집 가능



기대 효과

복합인증체계기반 통합계정 권한관리

- 계정 기반이 아닌 복합인증체계 기반 행위 감시로 정확한 작업자와 작업 내용 파악 가능
- 보안 사고 시 책임을 입증할 수 있는 명백한 자료로 활용 가능
- 시스템 장애 시에도 장애의 원인은 빠르게 파악할 수 있고, 빠른 대응이 가능함
- 콘솔접속관리시스템에서의 작업도 추적 관리 가능

실시간 위변조 방지 로그 저장

- 행위 감시 로그를 실시간으로 위변조 불가능한 저장매체에 저장하여, 보안사고 시 증거 자료로 활용
- 관리자, 운영자 등 시스템 관리 권한을 가지고 있는 사용자도 로그 위변조 불가
- 사용자 행위 감시 로그 뿐 아니라 다양한 시스템 로그도 저장 가능

감사합니다