통합 IT 외주관리 플랫폼

J-TOPS

Total Outsourcing Platform System

조을 주식회사 조을

CONTENTS

1.1 회사개요

㈜좋을은 IT 인적자원의 안정적이고 효율적인 활용을 지원하는 보안 관리 플랫폼을 연구합니다.
고객 내/외부에서 는 발생하는 다양한 보안 위협에 대응하는 통합 관리 플랫폼을 추구합니다.

□ 개요

회 사 명	주식회사 좋을
설 립 일	2012년 09월
자 본 금	400,000,000
본 사	서울 강서구 양천로 551-24
사 업 분 야	외주관리시스템 개발 / 스마트워크센터 개발, 구축 / 정보유출방지솔루션

□ 특허 등록현황

[등록] 인증 시스템 및 방법

[등록] 보안 시스템, 이를 위한 단말기 및 보안 방법

[등록] 데이터 보안장치, 이를 구비하는 단말기 및 데이터 보안 방법과
컴퓨터로 읽을 수 있는 기록매체

□ 인증 현황

GS인증(1등급) 획득 J-TOPS v2.0 / 2017. 01

1.2 회사 연혁

2017
- 나라장터 조달 종합쇼핑몰 등록
- 한국공항공사 통합IT외주관리플랫폼 구축
- 건국대학교병원 통합IT외주관리플랫폼 구축
- J-TOPS v2.0 출시
- GS 인증(1등급) 획득 (J-TOPS v2.0 / 2017. 01)
- 굿모닝아이텍 영업 총판 계약

2016
- 한국광물자원공사
- 국무조정실 외주관리시스템 공급
- 근로복지공단 – 보험/복지, 의료보험 등

2015
- 한국중부발전 단말기통제시스템 공급
- 법무부 형사사범통계시스템 구축사업용 외주관리시스템 공급
- 한국원자력병원 망분리사업 외주관리시스템 공급
- 한국석유공사 망분리사업 외주관리시스템 공급
- 한국지역난방공사 정보보호고도화사업 외주관리시스템 확산
- 수서KTX 차세대보안시스템사업 외주관리시스템 공급
- 선문데이타시스템 영업 총판 계약
- 시큐에이스 영업 총판 계약

2014
- 합동참모본부 JWSC 외주관리시스템 공급
- 한.이스라엘 연구소 보안사업 외주관리시스템 공급
- 우정사업정보센터 외주관리시스템 추가 공급
- 전자정부 정보보호 솔루션페어 참가

2013
- 지란지교SNC 영업 총판 계약
- 지역난방공사 외주관리시스템 공급
- 우정사업정보센터 원격지단말관리시스템 공급
- 동북아역사재단 개인정보보호 솔루션 공급

2012
- 주식회사 좋을 법인설립

1.3 총판 및 파트너

□ 파트너쉽

[파트너와 시너지가 창출되는 Win-Win 전략을 지향합니다.]

□ 총판

지란지교에스앤씨 Solution & Consulting

(주)선문데이타 sunmoon data

GiT 굿모닝아이텍(주)

□ 프리미엄 파트너

saeoll Saeoll Information Technology 새올정보기술

WORLDSOFT

INVISIONIT

(주)엔젠시스 정보통신 전문기업

JL Infra (주) 제이엘 인프라 Co.,Ltd

joinusbiz 조인어스비즈

거명 ICT

주식회사 좋을

1.4 Reference

J-TOPS 대표 구축사례

한국광물자원공사

- 외주 인력 관리를 위한 지원 시스템 구축
- 원격지(서울) 단말을 본사(원주)에서 모니터링

한국지역난방공사

- 아웃소싱 운영에 대한 보안관리 강화 필요
- PM에 의한 자체 관리와 보안팀 상시 감사체계 확보
- 제3 협력업체 관리 강화 및 보안의식 강화

한국석유공사

- 내부망 작업에 대한 보안관리체계 강화 필요
- 관제실 상시 모니터링 체계 구축
- IT외주관리체계 확립

근로복지공단

- 서울 등 전국에 분산되어 개발되는 정보화 사업의 현황 파악 필요
- PM에 의한 자체 관리 및 보안지수 업데이트 체계 구축
- 사업자 자율 보안체계 확립 및 보안팀 감사 근거 확보

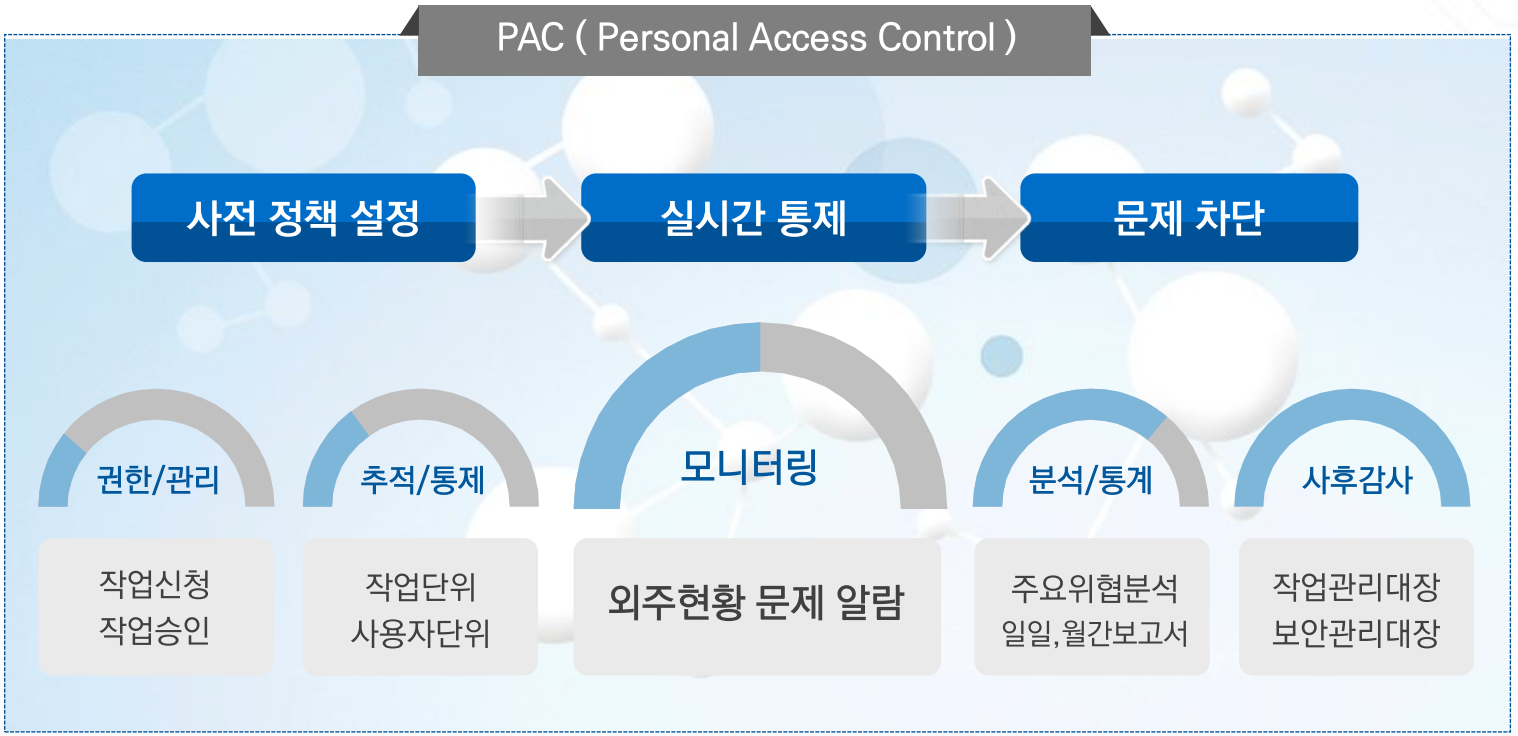
J-TOPS 레퍼런스

우정사업정보센터 | 근로복지공단 | 한국지역난방공사 | KNOC 한국석유공사
KOMIPO 한국중부발전 | 법무부 MINISTRY OF JUSTICE | 합동참모본부 R.O.K Joint Chiefs of Staff | KORES
NEXTIN Solutions | SR | 원자력병원 | 국무조정실 국무총리비서실
KAC 한국공항공사 | 건국대학교병원 KONKUK UNIVERSITY MEDICAL CENTER

2.1 J-TOPS 개요

□ IT 외주관리의 새로운 해결책 J-TOPS

[모니터링, 추적, 감사, 통계/분석 등 외주관리에 최적화된 기능 제공합니다.]



2.1 J-TOPS 개요

□ IT 외주관리의 핵심요소

외주인력 관리, 작업 관리, 보안 관리, 사업 관리

- 관리자 등급별 등록
- 작업자 등록
- 부서 및 업무배정
- 보안정책 사전설정

- 작업배정-보안정책 설정
- 실시간 작업수행 Log 수집
- 반출작업 지정
- 실시간 모니터링
- 동영상 검색
- Dashboard
- PC Shutdown

- 사업관리 단계 설정
- 단계별 수행업무 정의
- 투입인력 M/M 산출
- 산출물 관리

- 보안서약 수행
- 보안점검 수행
- 보안교육 수행
- 보고서 등록/결재

2.2 J-TOPS 도입근거

1 자체 점검 및 책임 강화

1-① 금융회사 자율점검 강화

가. 현황 및 문제점

□ 금융회사의 IT보안상 **취약점은 해당 금융회사가 가장 잘 파악**할 수 있으나,

○ **IT감사 전문인력이 부족**한 중소형 금융회사는 IT부문에 대한 위규사항 자체 감사·점검에 어려움

□ 규정상 **정보보안 및 외부주문보안 점검 의무***는 점검주기에 비해 점검항목이 많아 금융회사가 **형식적으로 이행할 가능성** 상존

* 정보보안 점검(전자금융감독규정 §37조의5) : 매월 점검(34개 항목), CEO에 보고
외부주문 보안점검(규정 §60①14) : 중요 점검사항 매일 점검(12개 항목)

나. 개선방안

□ IT감사 역량이 부족한 금융회사 지원을 위해 **IT 내부감사 가이드라인** 및 IT 내부감사요원 **교육프로그램**을 마련하고,

○ 상시적인 내부통제 강화를 위해 감사부서 내 IT감사 전담 인력을 배치토록 권고

□ 기 시행중인 **'IT부문 금융회사 내부감사 협의제도'***의 대상 금융회사 및 점검항목**을 확대하여 **내실화 도모**

* 금융회사가 자체감사를 통해 IT보안관련 미흡사항을 발굴·개선하고 금감원은 이행결과 확인 및 사후 관리('15년 38개 금융회사 대상으로 실시 중)
** 현재 외부주문, 전자금융사고 책임이행보험 등 6개 분야 13개 항목

□ **정보보안 및 외부주문 관련 보안 점검**의 실효성 제고를 위해 지나치게 세세한 점검항목을 **필수항목 위주로 개편**

[2015년 06월 19일 금융감독원/금융위원회 보도자료]

□ 전자금융감독규정 시행세칙 〈 시행 2016.11.11 〉

- 정보보안 점검항목
- 보안관리방안
- 중요 점검사항

□ 미래창조과학부/산업통상자원부 정보보안 세부지침

(국정원 국가 정보보안 기본지침 준용)

- 외부 용역업체 보안관리 방안
- 일일 용역사업 보안점검 리스트

□ IT 외주인력 보안통제 안내서

(한국인터넷진흥원(KISA), 방송통신위원회 발행)

- IT 외주용역 단계별 보안 강화 방안

□ 정보화사업 단계별 관리·점검 가이드 3.0

(미래창조과학부, 행정자치부, 한국정보화진흥원(NIA) 발행)

- 사업자 자체 보안관리체계 구축 및 운영

□ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

- 정보보호 관리체계 (ISMS)의 인증
- 외부자 보안 / 물리적 보안 / 시스템 개발 보안

2.3 J-TOPS 특징 및 주요기능

IT 외주관리 체계확립, 자동화, 모니터링, 실시간 감사자료 제공

체계적 자동화된 시스템

- 분산되어 작업하는 외주 전체현황 파악 및 모니터링
- 간단하고 편리한 One PC 멀티 사용
- 작업의 신청, 승인, 모니터링, 위협차단, 알람의 프로세스 자동화
- 대시보드, 3rd Party 연동
- 다양한 검색 및 보고 데이터 제공

개별 작업모니터링

- 단말 접속 실시간 모니터링
- 접속 단말의 실시간 사용중지 및 강제종료
- 단말 사용자 계정 및 통제정책 실시간 반영
- 차단 명령어, 차단프로그램, 차단IP/URL, 저장매체 (USB, ODD, Drive 등), N/W(LAN, Wi-Fi, Bluetooth 등)제어
- 사전 접속 정책 설정

Compliance 대응 및 감사 대비

- IT외주인력 보안통제 기준 준수
- 관리자 작업환경 설정 근거 및 작업 상세이력 확보
- 접속로그, 프로세스로그, 위협로그, 동영상로그 등 감사로그 수집(동영상로그에 의한 작업자 행위여부 판단)
- 단말 사용로그 보안 파티션 암호화 저장
- SLA 준수를 통한 긴급대응체계 확보

ITO 관리자 편의성 제공

- 직관적인 작업현황 파악으로 효율적인 외주 운영
- 사전 통제정책에 따른 이상징후 추적통제 편의성 제공(주요위협별, 작업자별, 기간별 등)
- HTML5 기반의 가시성이 확보된 실시간 대시보드 제공
- 시스템에 의한 일일 보안점검 자동화

2.4 J-TOPS 주요항목

IT 외주관리 플랫폼 주요 항목

관리자관리

- 관리자 등록
- 관리자 권한
- 관리자 부서

작업자관리

- 작업자 관리
- 작업 차단 / 허용

작업관리

- 작업자 설정
- 작업시간 설정
- 작업 단말 설정
- 접속 서버 설정
- 차단/통제 설정
- 매체 사용 설정
- 작업 결재

접속현황

- 모니터링
- Agent Log
- 동영상 Log
- 작업 타임라인

환경 설정

- 그룹 정책 설정
- 관리자 목록
- 관리자 IP 목록
- 비밀번호 규칙 설정
- 영상 설정

보안 관리

- 보안서약서 관리
- 보안교육 관리
- 보안 규정 및 양식함
- 보고서 / 교육자료 등록
- 정보시스템 관리
- 휴대용 저장매체 관리

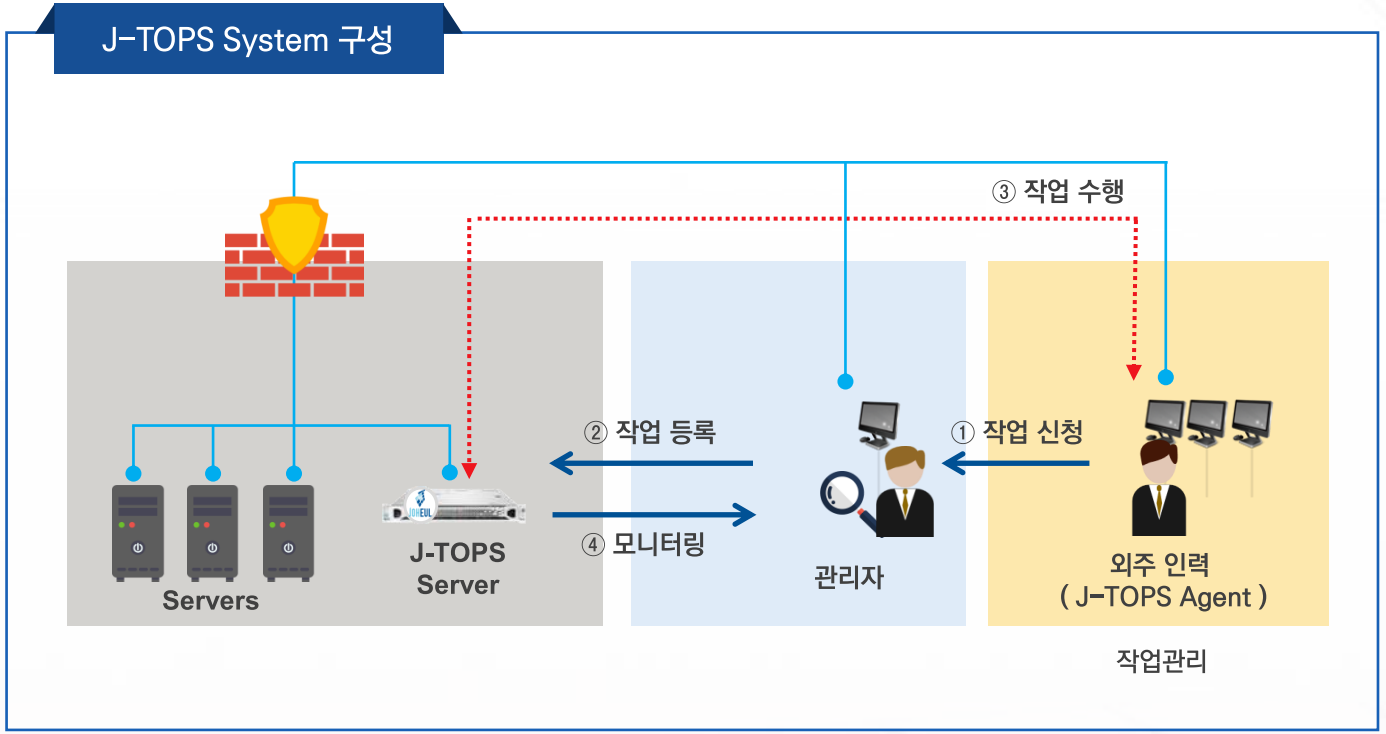
사업 관리

- 프로젝트 관리
- 작업자 관리

2.5 J-TOPS 시스템 구성

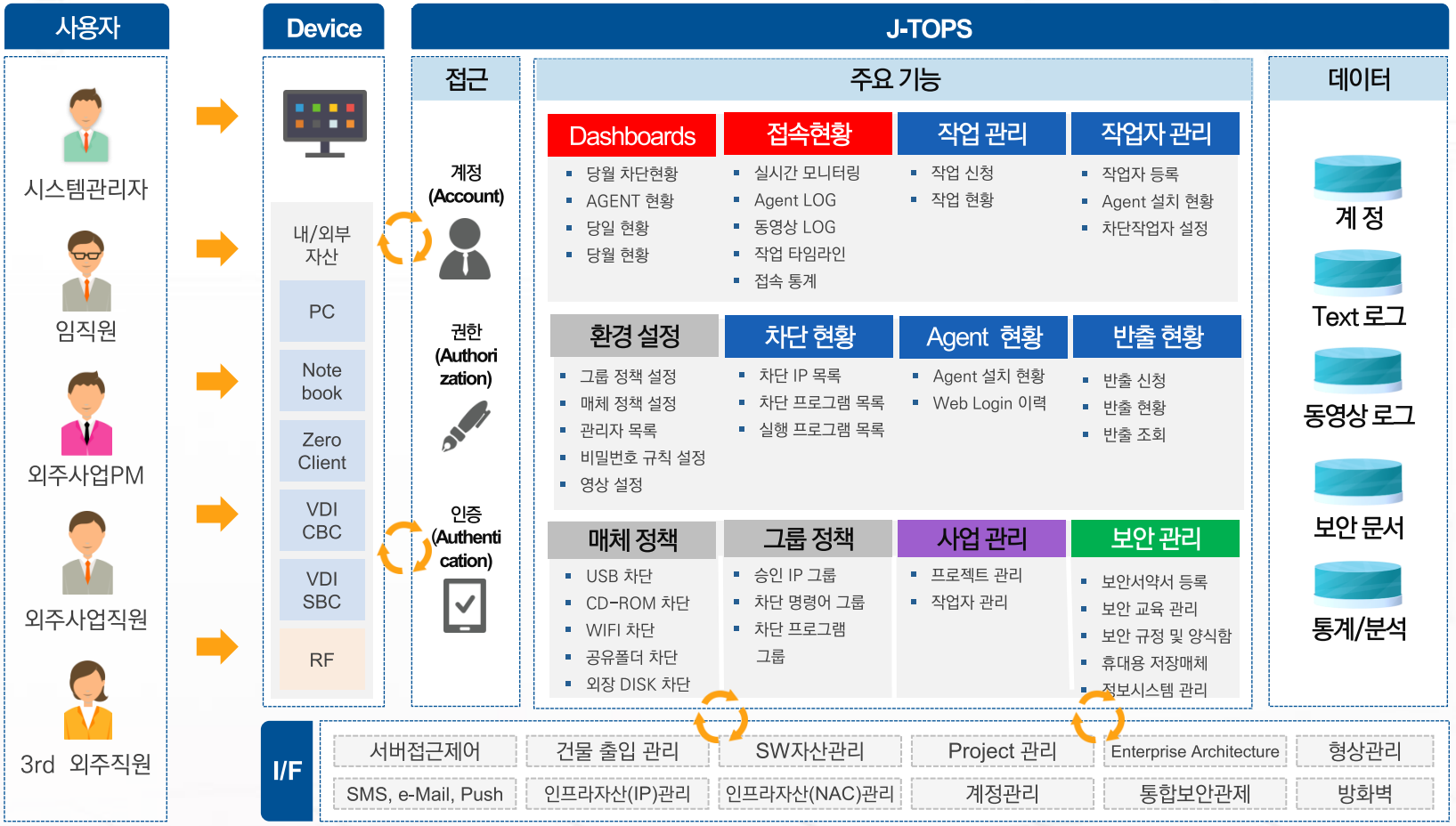
J-TOPS 서버에 관리자가 사전 정의한 정책 그룹에 따라 IT 외주 인력(작업자)의 컴퓨터에 J-TOPS Agent 를 설치하여
관리자가 설정한 **작업 기간 및 지정 PC에 한하여** 작업자가 작업할 수 있도록 통제합니다.

J-TOPS System 구성



2.5 J-TOPS 시스템 구성

외주인력의 출입부터 철수까지 일관된 관리 가능



2.6 J-TOPS 업무흐름

◻ 외주 관리 업무 흐름

사전통제정책 (Pre-Control Policy)

- 작업단위 정책설정
- HW, SW, SI 분류에 따른 정책 설정
- Whitelist or Blacklist 기반 정책설정
- USB, N/W, 명령어, 프로그램 등 위협시도에 대한 정책설정

All-In-One Agent

- 단말 IP 통제 : 승인된 IP만 Login 가능
- 단말 포트 및 미디어 통제 : 승인된 N/W,공유폴더 만 개방
- 작업단위 계정 통제 : 승인된 시간의 작업자 계정만 로그인 승인
- J-Putty, Domain Controller, Proxy Agent

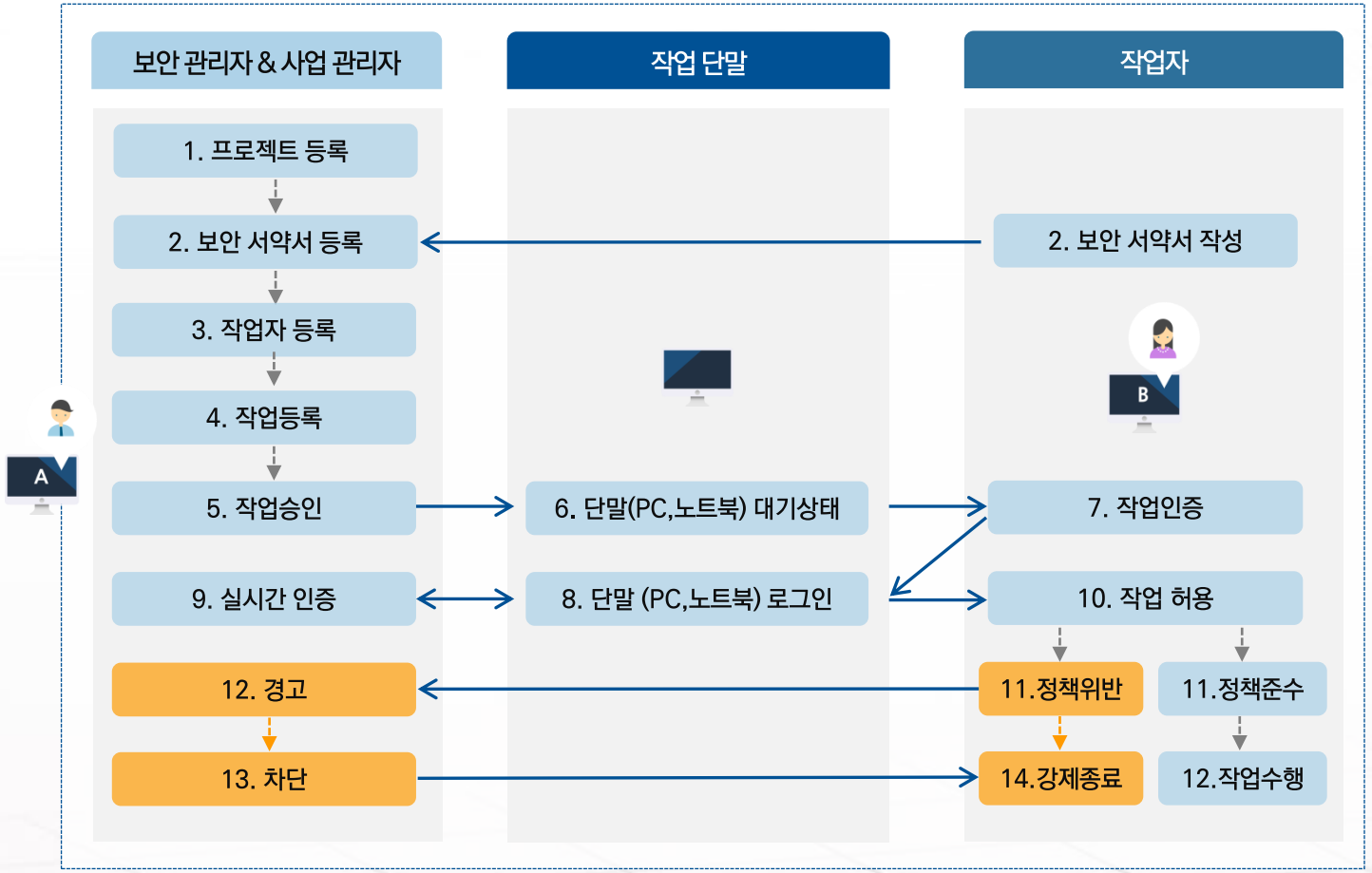
실시간 감시 (Monitoring)

- 단말의 접속부터 미승인 IP, 명령어, 프로그램, 포트 이용에 대한 이력 관리
- 작업별 수행 상태 모니터링
- One-Click PC Shutdown 및 재접속 차단

◻ 보안 기능 상세

2.6 J-TOPS 업무흐름

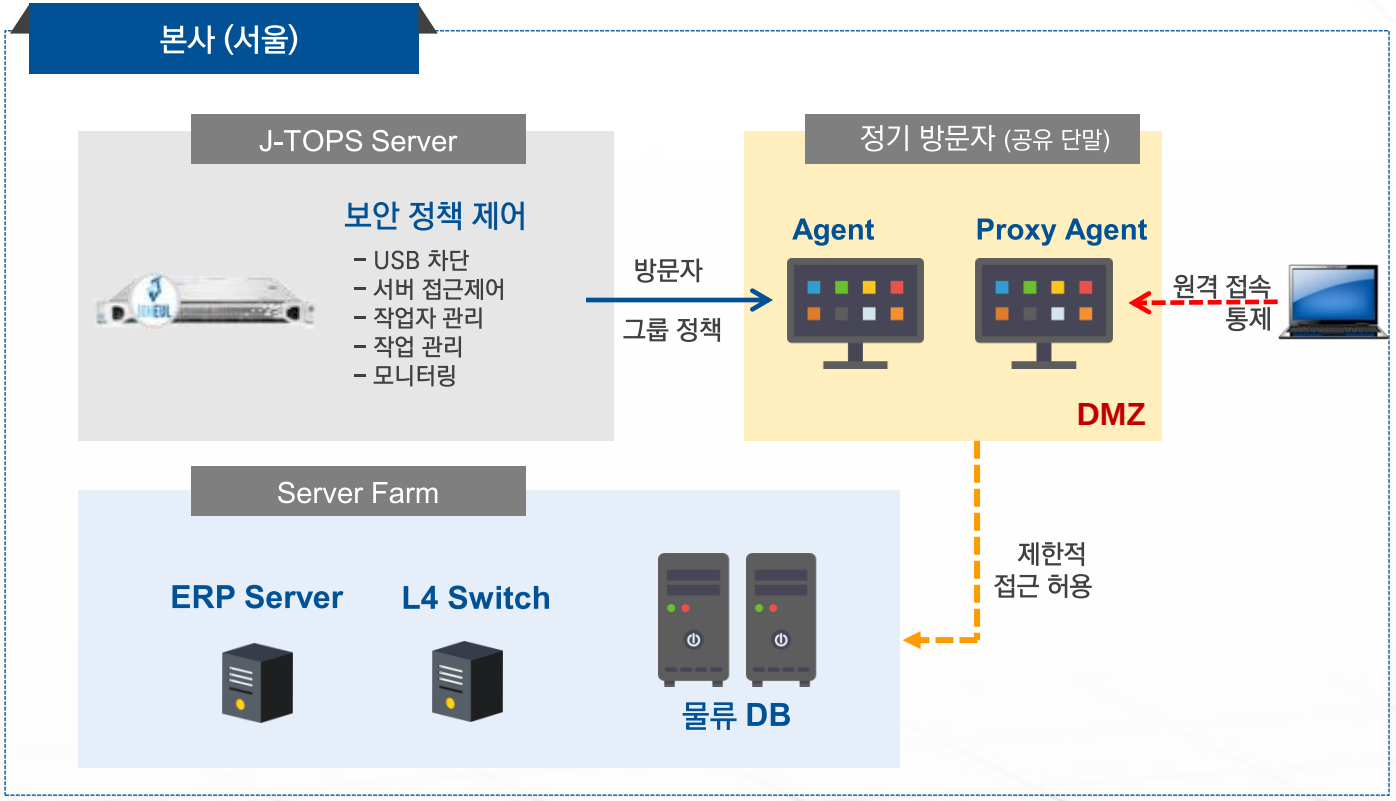
J-TOPS는 IT 개발 및 유지보수 업무에 상주 / 비상주 작업자들을 **보안 관리자 입장에서 효율적으로 관리**할 수 있는 플랫폼입니다.



2.7 J-TOPS 적용유형

□ 정기 방문자 적용

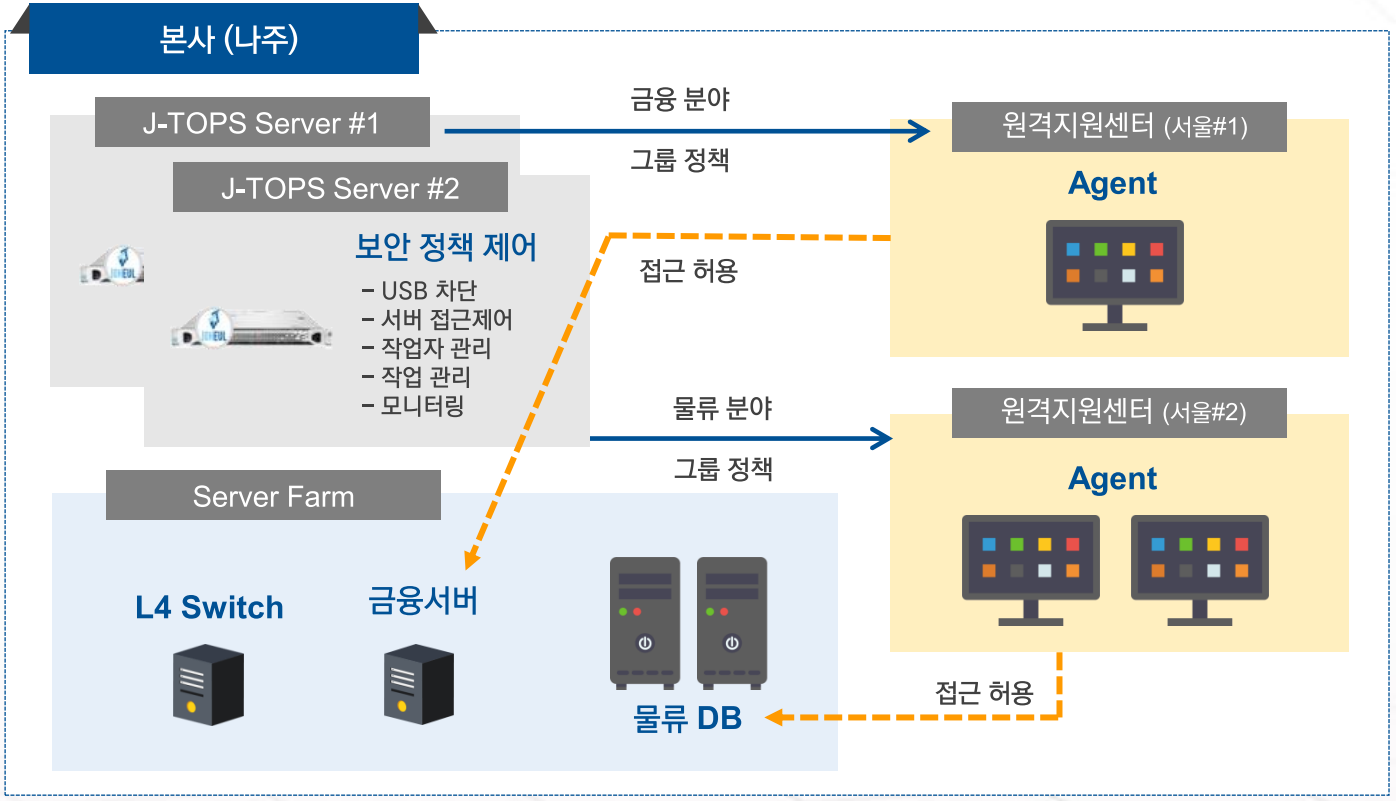
외주 IT 엔지니어의 정기 점검 방문을 위한 환경 구성으로 공유 단말을 지정하여,
해당 단말에서 특정 기간 동안 지정된 시스템으로 접속을 허용하는 작업을 배정하여 운용합니다.
DMZ 영역에 Proxy Agent 를 통해 Firewall 제어를 단순하게 관리할 수 있습니다.



2.7 J-TOPS 적용유형

□ 원격 지원 센터 적용

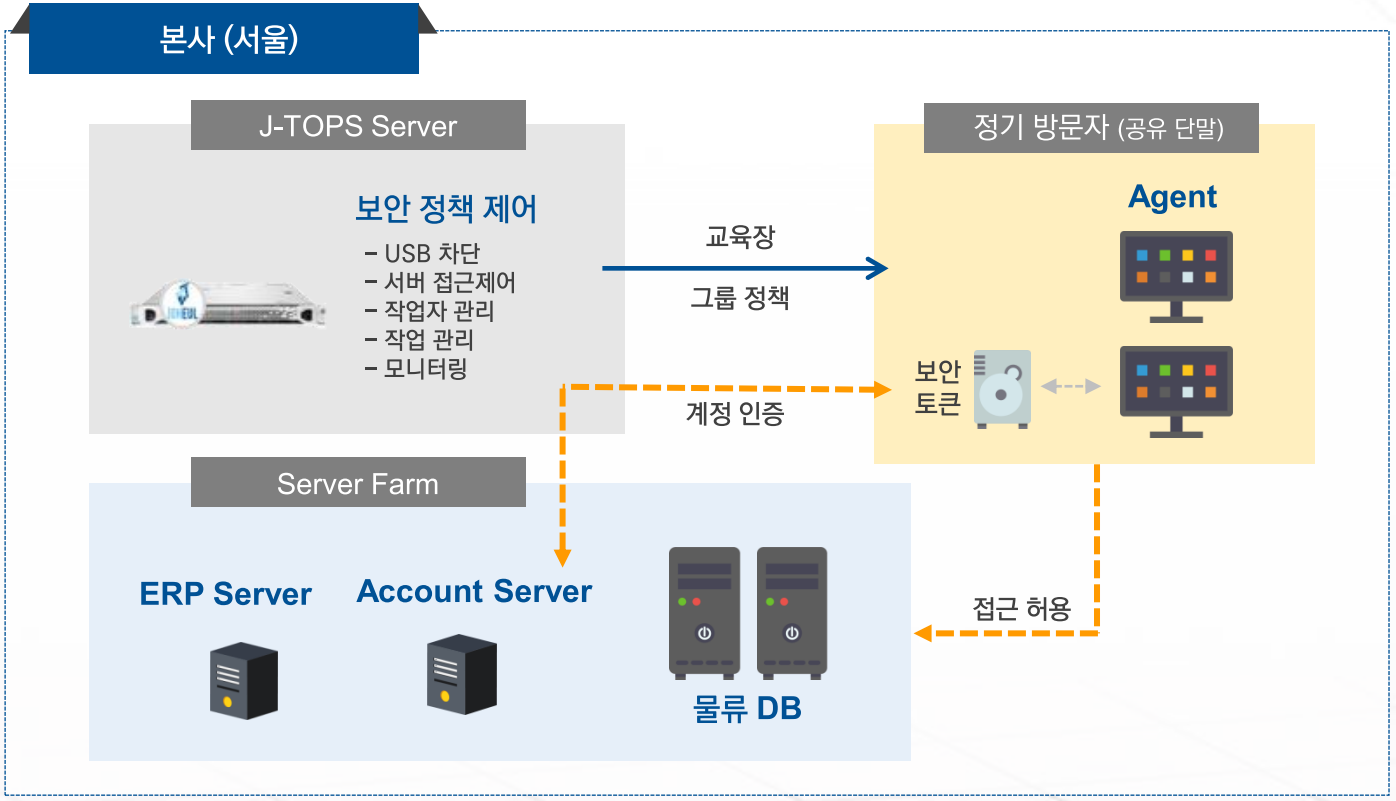
업무의 특성상 상호 분리해야 하는 이질적 업무인 경우, 유형별로 J-TOPS 를 각각 설치해 모든 설정 정보와 접근 정보 자체를 분리 운영하여 보안성을 향상시킬 수 있습니다.



2.7 J-TOPS 적용유형

◻ 계정관리 연동

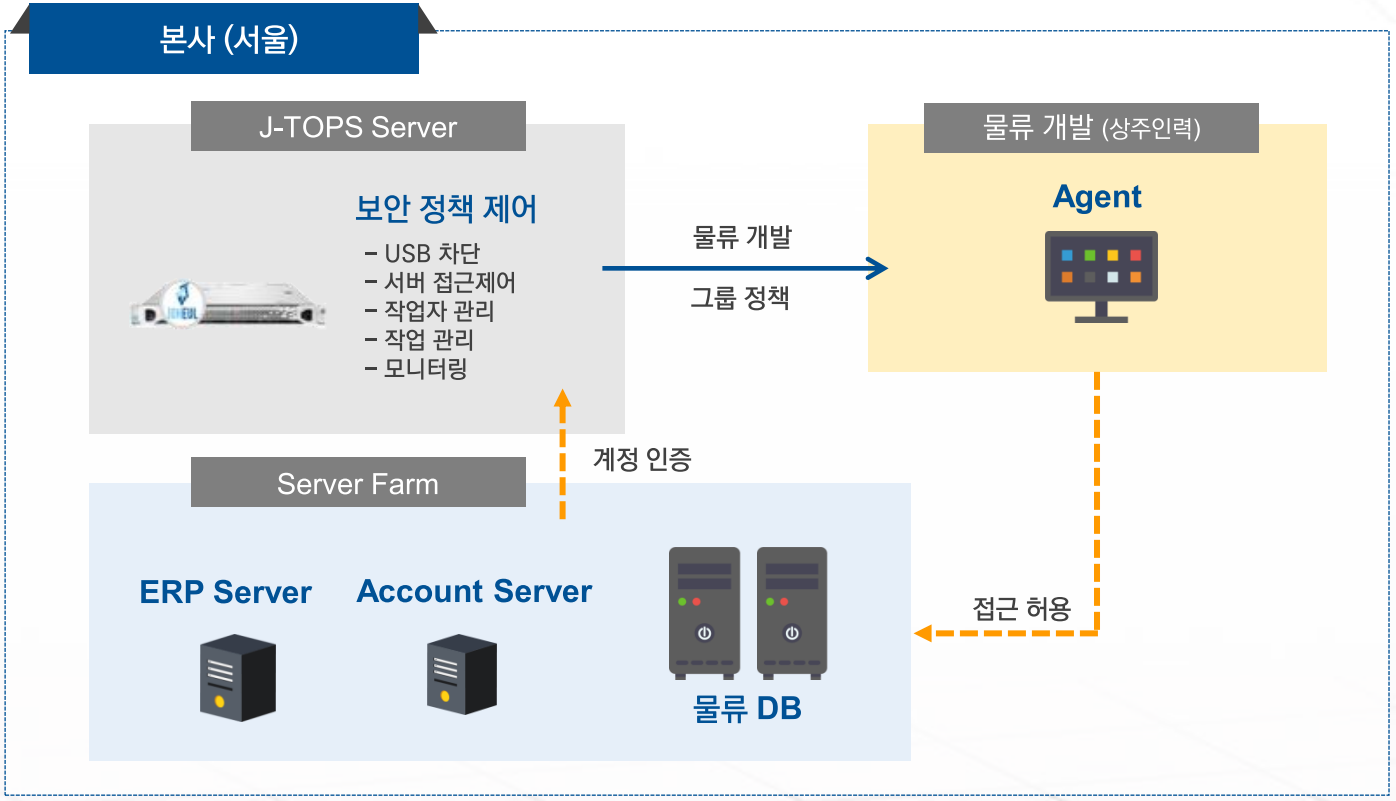
정보보안의 중요도가 극히 높은 일부 기관의 경우, 내부 인증을 위한 별도의 과정이 추가 적용됩니다.
바로, **보안토큰**을 통해 기관의 계정관리 서버에 인증을 받아 Agent 의 인증을 수행합니다.



2.7 J-TOPS 적용유형

□ 계정관리 연동

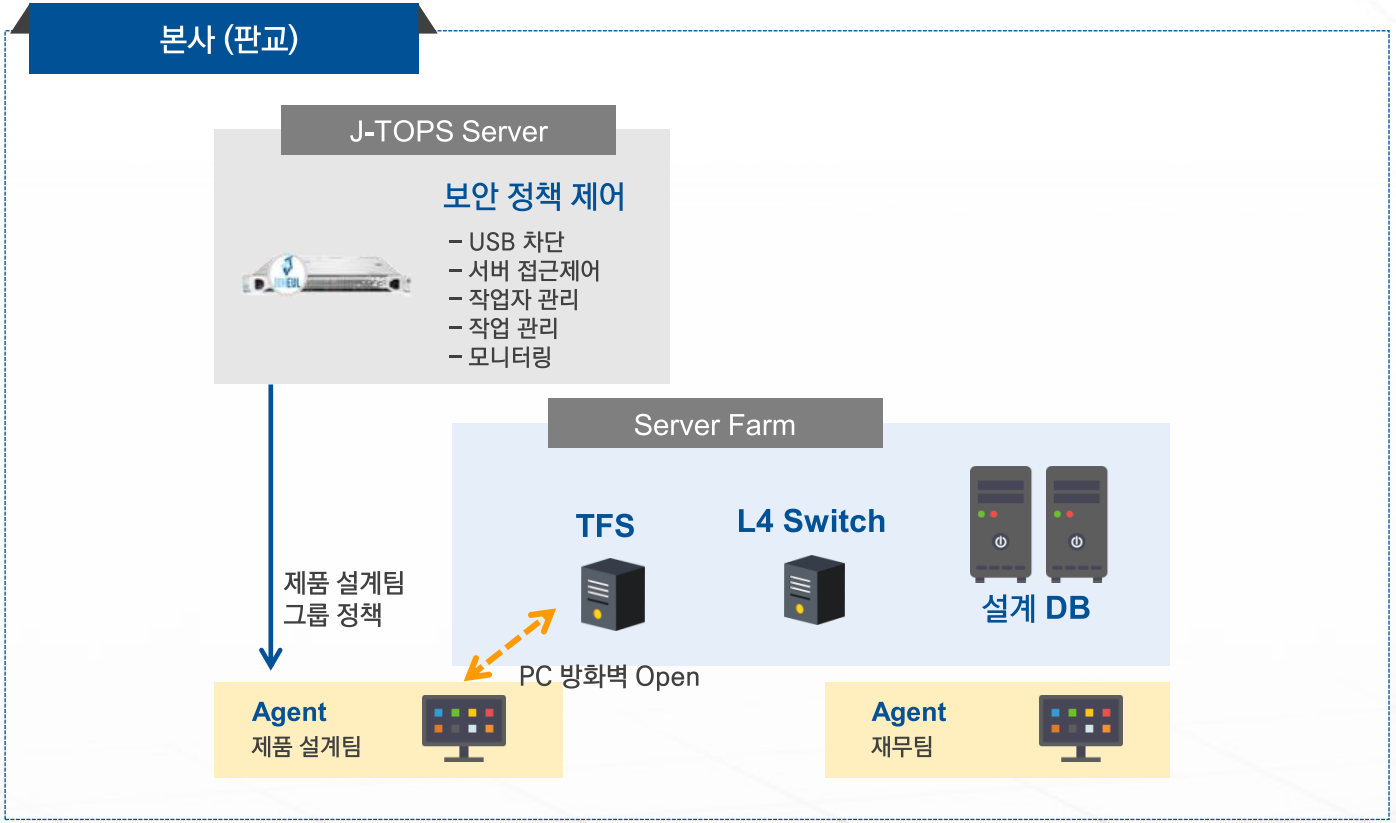
계정관리 서버에서 변경 사항이 있는 경우 J-TOPS 의 외부Open API 를 활용해 최신 정보를 변경하고, 이를 활용해 상주 인력의 입사자 / 퇴사자의 계정 관리를 수행합니다.



2.7 J-TOPS 적용유형

□ 정규 직원 적용

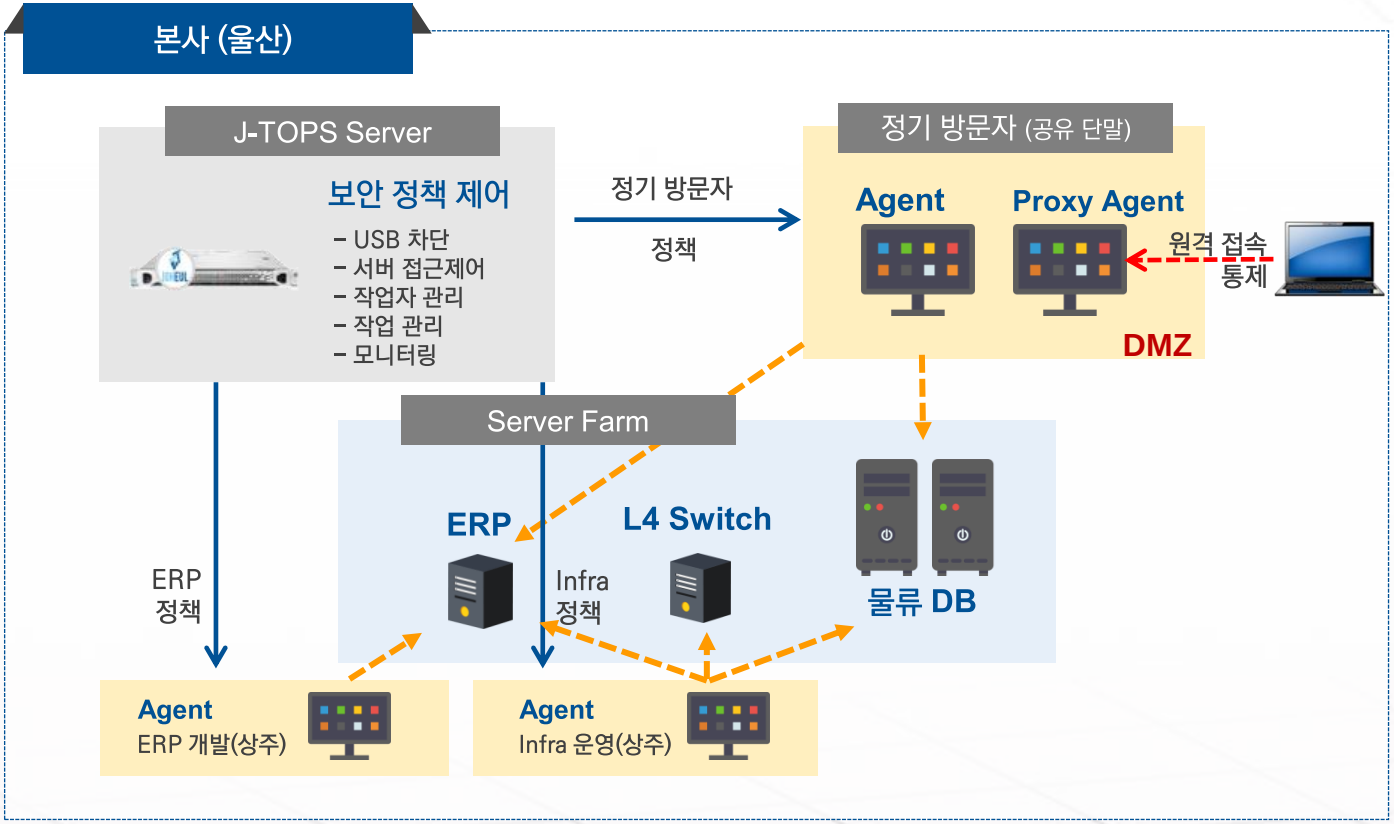
제품 설계 부서의 경우 설계 도면 등의 문서 보안을 위해 정규 직원들에게 적용하고, TFS 에 등록되어 있는 PC 의 경우에만 PC 방화벽을 Open 하도록 설정하여 정보보안 통제 활동을 강화합니다.



2.7 J-TOPS 적용유형

□ 외주 인력 적용(상주)

상주 외주 인력이 있는 경우 작업자 부서별로 그룹 정책을 배정해 작업을 통제하고, 별도의 정기 방문자들을 위해 공유 단말에 정기 방문자 정책을 배정해 관리합니다.



2.8 J-TOPS 기대효과

관리의 편의성과 모니터링을 통한 가시성 확보

외주인력 관리 편의성 증대

- 작업자 권한에 따른 보안 정책 설정
- 작업 배정으로 철저한 업무 통제
- 작업 수행 Log 수집 및 동영상 수집

작업 모니터링 강화

- 실시간 작업 상태 모니터링
- 보안정책에 따른 업무수행 범위 제한
- TimeLine 기반의 편리한 작업관리 UI
- 동영상, Text Log 수집으로 강력한 부인 방지
- 작업 단말의 반출입 통제 강화

사업 관리 효율성 증대

- 자동화되고 일관된 ITO 관리 프로세스 적용
- 비 IT 인력의 보안관리 역량 향상
- 간단한 보안관리 항목 설정
- 작업 Log 기반의 출퇴근 명부 작성
- 인력 투입 M/M 산정 편리
- 산출물 관리 자동화
- 보안점검 관련자료 자동 생성

자동화된 보안관리

- 단계별 보안관리 업무 자동화
- 보안 서약서 작성 및 스캔 등록 기능
- 보안교육 자동 실시 및 수료자 명부 관리
- 보고서 작성 및 관리 편의성 향상
- 보안점검 보고서 관리

위협통계 / 작업현황 자동 생성

- 인별 / IP 별 / 기간 등에 따른 자요 위협 통계 및 Report 자동 생성
- 담당자, 팀, 사업 등 단위별 작업 현황 실시간 확인

2.8 J-TOPS 기대효과

[정보화사업 보안지수 체크리스트(예시) – 공공, 금융 등 컴플라이언스 준수 모니터링 및 평가]

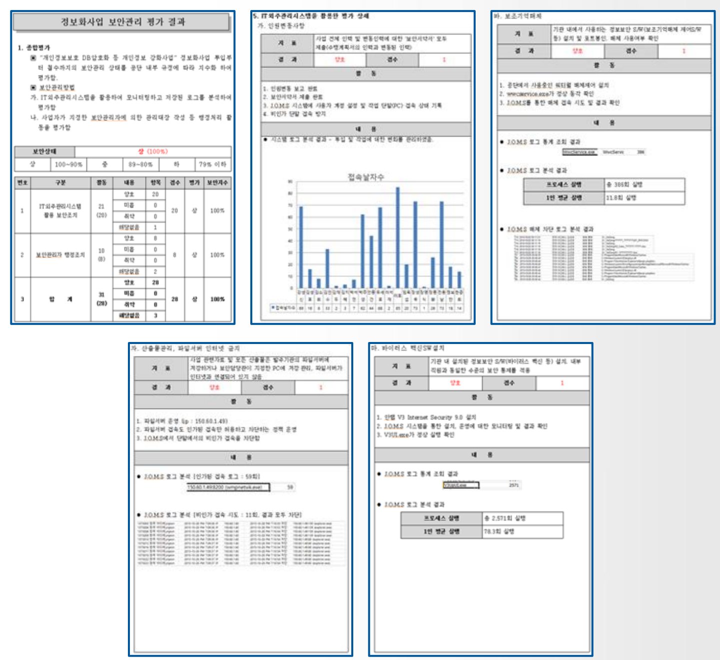
구분	No.	항목	활동내역	평가	점수	비고
IT외주관리 시스템 활용 보안조치	1	인원 변동사항 및 보안서약서 제출	J.OMS를 통한 개인 계정할당 관리, 변동사항 보고 및 보안서약서 제출 완료	양호	1	
	2	일일보안점검 수행	J.OMS를 통한 NW 접속, IP, 프로그램, USB 등 주요 위협 실시간 모니터링 및 일일 점검 수행, 이상 상황 발생에 대한 보고	양호	1	
	3	정보시스템관리대장 작성	J.OMS를 통한 PC, 노트북, 서버 등 대장관리	양호	1	
	4	반입시 악성코드 감염확인	Off line 상태에서 백신을 통한 확인 및 On line 시 J.OMS를 통한 프로세스 감시를 통한 실시간 확인	양호	1	
	5	반출 포맷	반출 신청을 통한 포맷절차 운용 및 무단 반출에 대한 안전조치로 J.OMS 에이전트를 통한 기기 접근 불가 운용	양호	1	J.OMS에이전트를 반출 포맷 시 즉시 삭제 운용
	6	바이러스 백신 SW	J.OMS 프로세스 수집을 통한 백신 운영 실시간 확인	양호	1	
	7	보조기억매체	관리자 감독하에 고객사에서 권고한 매체제어 SW 설치, J.OMS NW 및 미디어 매체제어를 통해 실시간 확인	양호	1	
	8	산출물관리, 파일서버 인터넷 금지	암호화된 파일서버 운영, 고객사에서 권고한 매체제어 운영, J.OMS를 통한 인터넷 접속 시도 모니터링	양호	1	
	9	전자우편	고객사에서 사용하는 메일 사용 및 첨부파일 암호화, J.O.M.S를 통한 상용메일 접속 시도 모니터링 및 차단	양호	1	
	10	네트워크 주소 관리	J.OMS IP관리를 통해 사업자가 사용하는 IP 및 접속이 허용된 IP를 관리하고 리스트를 상시 확인할 수 있음	양호	1	
	11	비인가 네트워크 차단	고객사 권고 NW 관리SW 설치 운용 및 J.OMS를 통해 비인가 IP접속에 대한 모니터링 및 차단 및 알림 운용	양호	1	
	12	접근 사이트 관리	업무상 필요한 사이트를 지정하지 않고 외부 사이트 접속을 차단함	양호	1	
	13	정보시스템 접근 권한관리	업무에 따라 J.OMS를 통해 정보시스템 접근을 사용자 계정을 통해 제한적으로 통제하고 시스템 및 어플리케이션 접근 권한을 제한적으로 운영함	양호	1	
	14	정보시스템 접근 및 계정, PW 관리	권한에 따라 작업자 단말에 대한 관리는 J.OMS를 통해 운영하고, 서버 및 장비에 대한 관리대장 기록 및 보고함	양호	1	
	15	정보시스템 작업 후 기록 확인	J.OMS를 통해 작업 event 및 동영상을 실시간 확인하고 기록을 저장함	양호	1	
	16	정보시스템 로그 확인	J.OMS에 저장된 작업 관련 로그를 계정별, 기간별 조회하고 확인함	양호	1	
	17	사용계정, NW사용 승인, 만료 시 차단	J.OMS를 통해 계정 및 NW 사용을 신청하고 보안관리자가 승인하며 승인된 기간이 만료되면 자동으로 차단됨	양호	1	
	18	로그 6개월 보관	모든 작업 로그는 J.OMS에 보관되며 event 로그 및 동영상이 6개월 이상 저장, 조회할 수 있음	양호	1	
	19	원격지 NW 접속 금지	고객사 내부에 위치한 작업장으로 원격을 위한 방화벽 개방 사실이 없으며 사업장 내부로의 직접 접속은 J.OMS를 통해 테더링 등 모니터링 하고 위반 시 차단, 알림	양호	1	
	20	무선인터넷	사업장 내부 모든 단말에는 고객사에서 권고하는 매체제어가 설치되어 있고 테더링 등 시도에 대해 J.OMS를 통해 실시간 모니터링 및 차단하고 있음	양호	1	
보안관리자 행정조치	1	사업장 비인가자 출입 및 접근통제	시건장치 구비, 출입관리대장 제출 완료	양호	1	
	2	보안교육실시	보안교육 실시 및 보고서 제출 완료	양호	1	
	3	사무실,장비에 대한 월 1회 점검 실시	월 1회 총 ?회 점검실시 및 보고서 제출 완료	양호	1	
	4	장비별 라벨 부착	장비 ?대, PC ?대, 노트북 ?대, 프린터 ?대 라벨 부착 완료	양호	1	
	5	반출입 신청서 및 관리대장	총 ?건의 반출입 신청 및 관리대장 기록 완료	양호	1	
	6	정보시스템 보안 취약점 확인	총 ?회 보안취약점 점검	양호	1	
	7	누출금지대상 정보 관리대장	관리자 감독하에 관리대장 작성, 파괴, 삭제 행위 및 보고	양호	1	
	8	보안확약서	전체 참여인원 총 ?명 보안확약서 제출	양호	1	
	9	백업과 대장관리	개발, 변경된 소스에 대해 주기적으로 백업을 실시했으며 대장에 기록함	양호	1	
	10	비공개정보 암호화	중요 정보에 대해 고객사에서 권고하는 DRM, DB암호화 SW를 이용하여 암호화하며, 외부 유출 시도에 대해 J.O.M.S를 통해 모니터링함	양호	1	

보안관리 체크리스트	항목수	보안수준	평가	점수	비고
IT외주관리시스템 활용 보안조치	20	양호 20 / 미흡 / 취약 / 해당없음	양호	20	
보안관리자 행정조치	10	양호 10 / 미흡 / 취약 / 해당없음	양호	10	
합 계	**30**	양호 30 / 미흡 / 취약 / 해당없음	양호	**30**	

□ OO기관 사례

- 사업관리자에 내부 지침에 맞춰 사업 진행 교육
- RFP에 자체 보안관리체계 구축 권고 및 가산점 부여
- 32개 내부 지침 공개 및 이행 권고
- 시스템에 의한 일일 점검 및 자동 보고

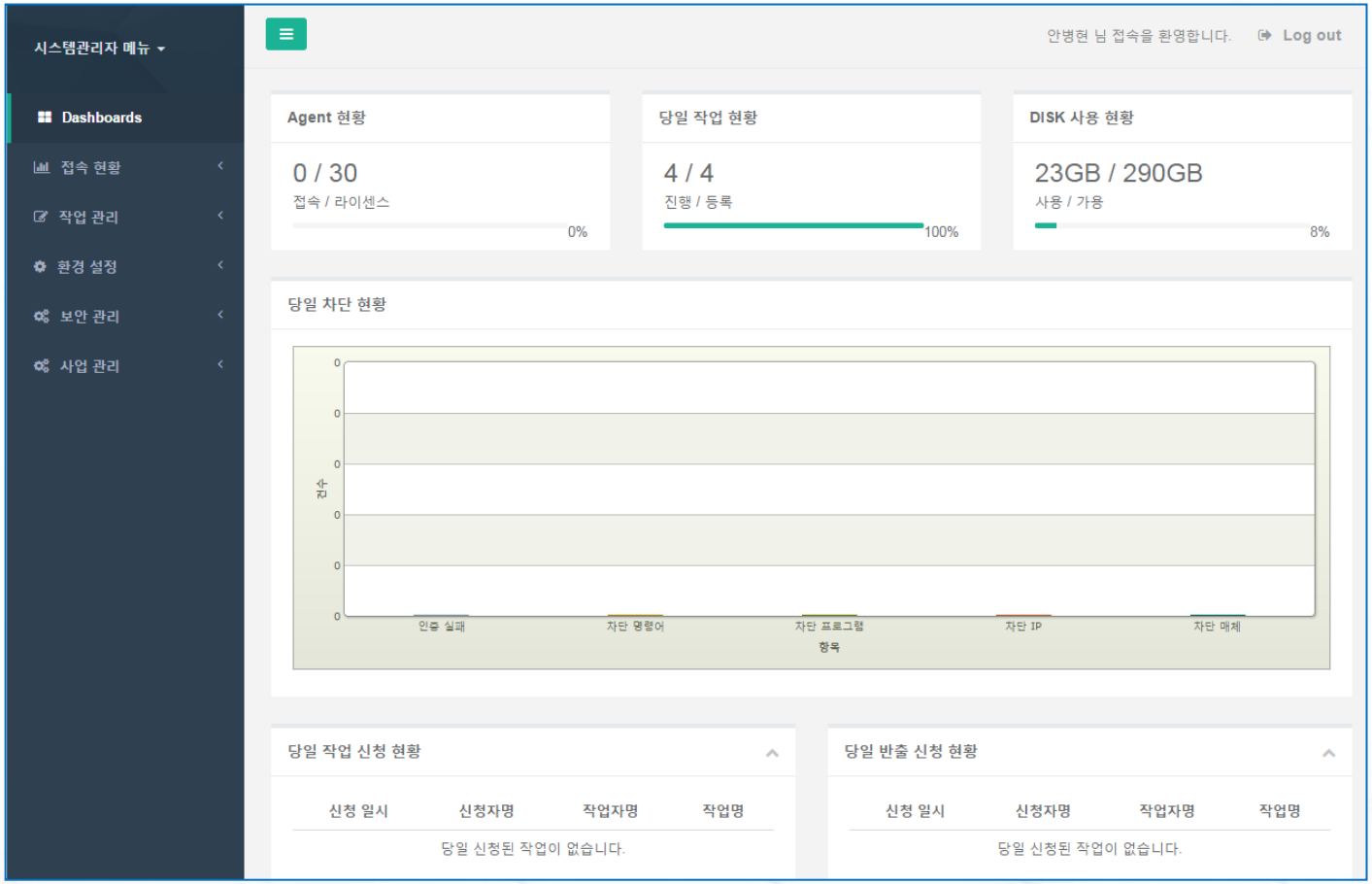
□ 정보화사업 보안지수 평가 보고서



주식회사 좋을

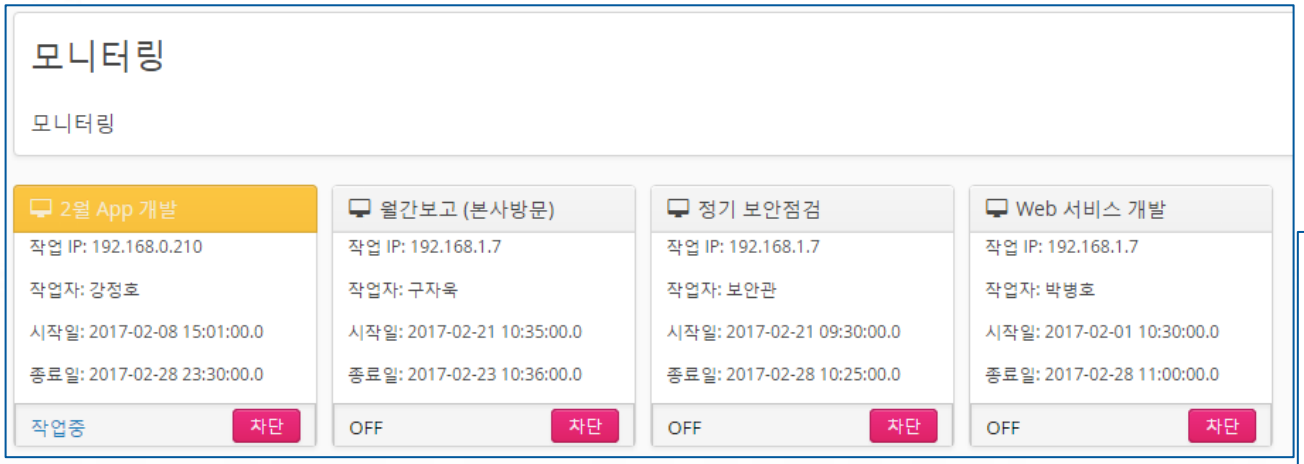
2.9 J-TOPS 주요화면

Dashboards

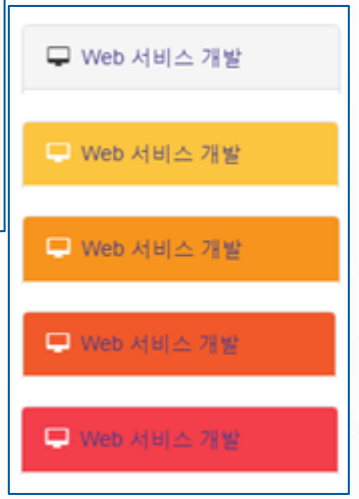


2.9 J-TOPS 주요화면

접속 현황 : 모니터링



작업 : 위험 지표



2.9 J-TOPS 주요화면

접속 현황 : 접속 통계

조회일 2016-02-21 기간 2016-02-21 ~ 2017-02-21 조회

2017-02-21 일일 작업 현황

합계	진행중	미진행
5	1	1

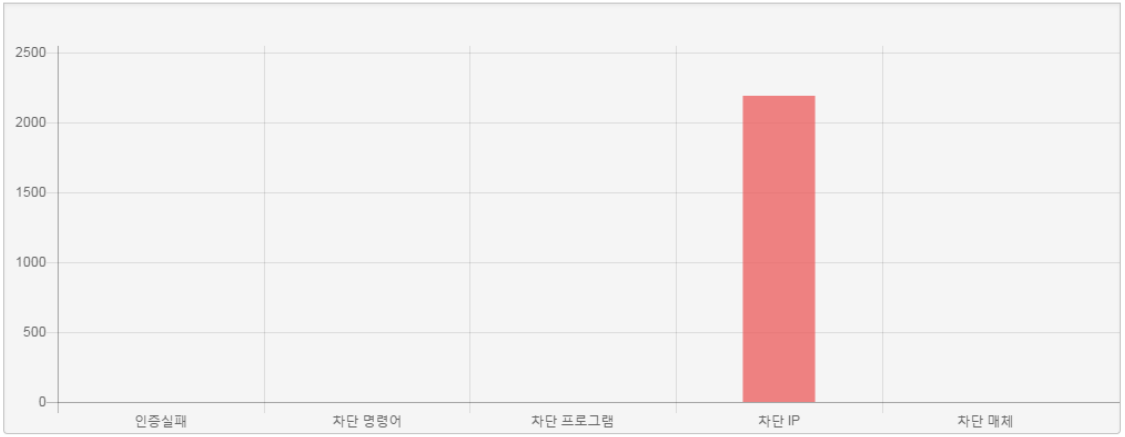
2017-02월간 작업 현황

합계	진행중	미진행
6	1	1

2017-02-21일일 접속 현황

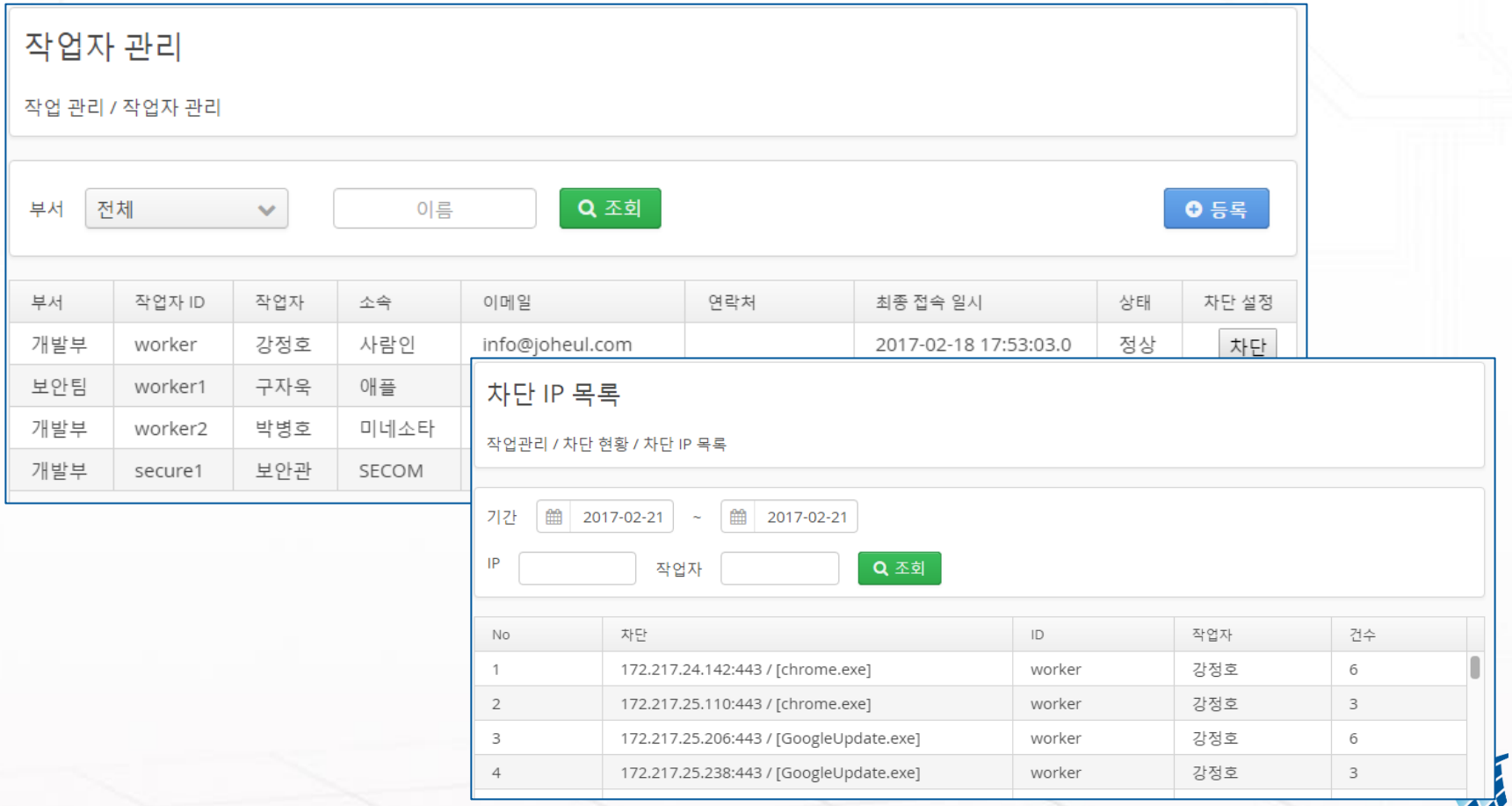
당일 접속(계)	인증 실패	차단 명령어	차단 프로그램	차단 IP	차단 매체
2,189	0	0	0	2,189	0

2017-02-21 접속현황



2.9 J-TOPS 주요화면

작업 관리 : 작업자 관리, 차단 IP 목록



작업자 관리

작업 관리 / 작업자 관리

부서 전체 | 이름 | 조회 | 등록

부서	작업자 ID	작업자	소속	이메일	연락처	최종 접속 일시	상태	차단 설정
개발부	worker	강정호	사람인	info@joheul.com		2017-02-18 17:53:03.0	정상	차단
보안팀	worker1	구자욱	애플					
개발부	worker2	박병호	미네소타					
개발부	secure1	보안관	SECOM					

차단 IP 목록

작업관리 / 차단 현황 / 차단 IP 목록

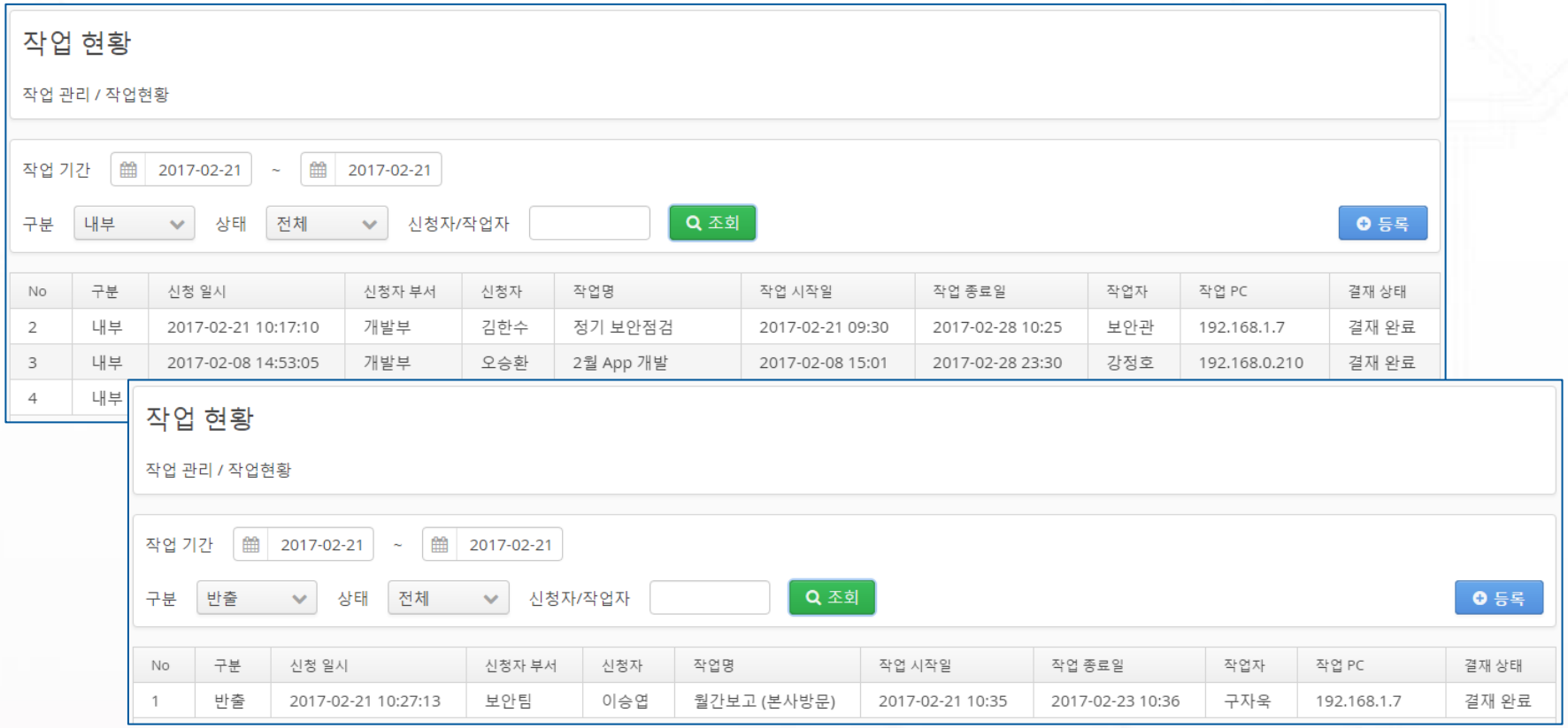
기간 2017-02-21 ~ 2017-02-21

IP | 작업자 | 조회

No	차단	ID	작업자	건수
1	172.217.24.142:443 / [chrome.exe]	worker	강정호	6
2	172.217.25.110:443 / [chrome.exe]	worker	강정호	3
3	172.217.25.206:443 / [GoogleUpdate.exe]	worker	강정호	6
4	172.217.25.238:443 / [GoogleUpdate.exe]	worker	강정호	3

2.9 J-TOPS 주요화면

작업 관리 : 작업 현황, 반출 현황 화면



작업 현황

작업 관리 / 작업현황

작업 기간 2017-02-21 ~ 2017-02-21

구분 내부 상태 전체 신청자/작업자 조회 등록

No	구분	신청 일시	신청자 부서	신청자	작업명	작업 시작일	작업 종료일	작업자	작업 PC	결재 상태
2	내부	2017-02-21 10:17:10	개발부	김한수	정기 보안점검	2017-02-21 09:30	2017-02-28 10:25	보안관	192.168.1.7	결재 완료
3	내부	2017-02-08 14:53:05	개발부	오승환	2월 App 개발	2017-02-08 15:01	2017-02-28 23:30	강정호	192.168.0.210	결재 완료
4	내부									

작업 현황

작업 관리 / 작업현황

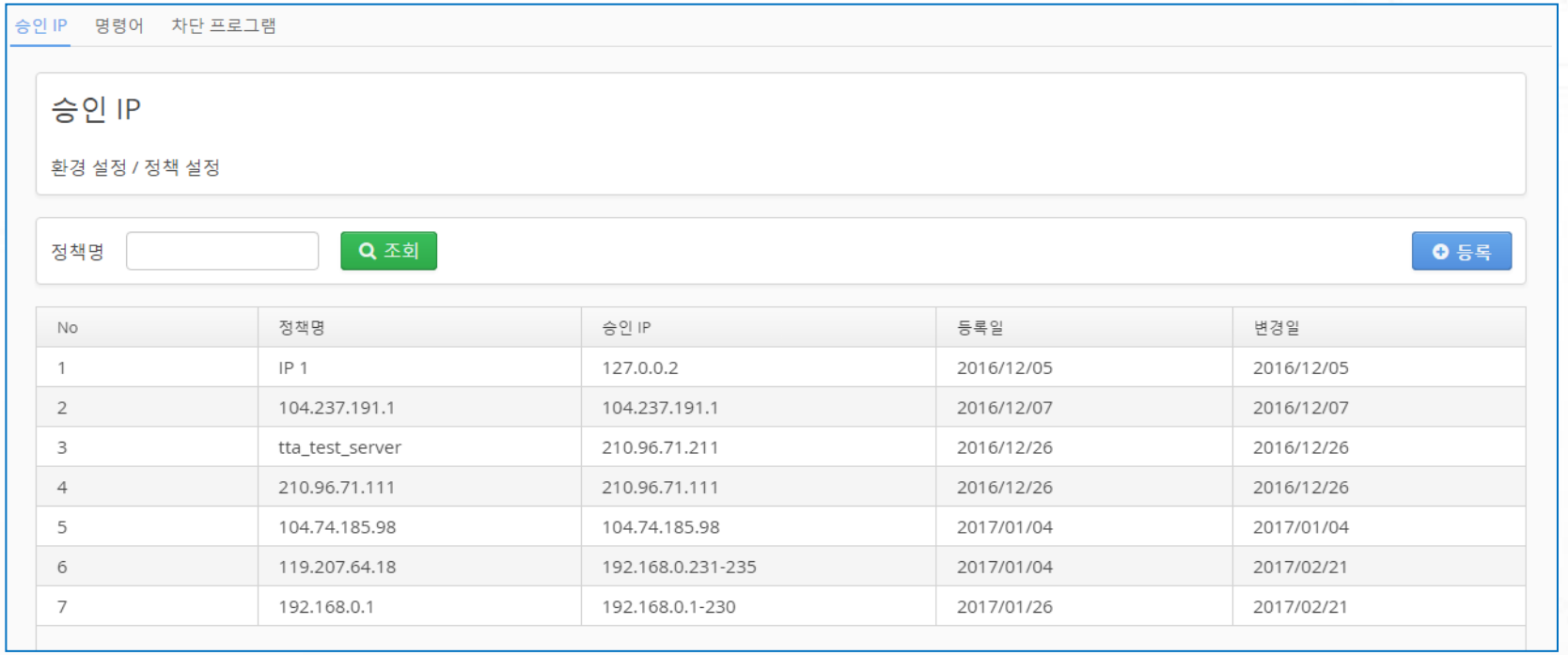
작업 기간 2017-02-21 ~ 2017-02-21

구분 반출 상태 전체 신청자/작업자 조회 등록

No	구분	신청 일시	신청자 부서	신청자	작업명	작업 시작일	작업 종료일	작업자	작업 PC	결재 상태
1	반출	2017-02-21 10:27:13	보안팀	이승엽	월간보고 (본사방문)	2017-02-21 10:35	2017-02-23 10:36	구자욱	192.168.1.7	결재 완료

2.9 J-TOPS 주요화면

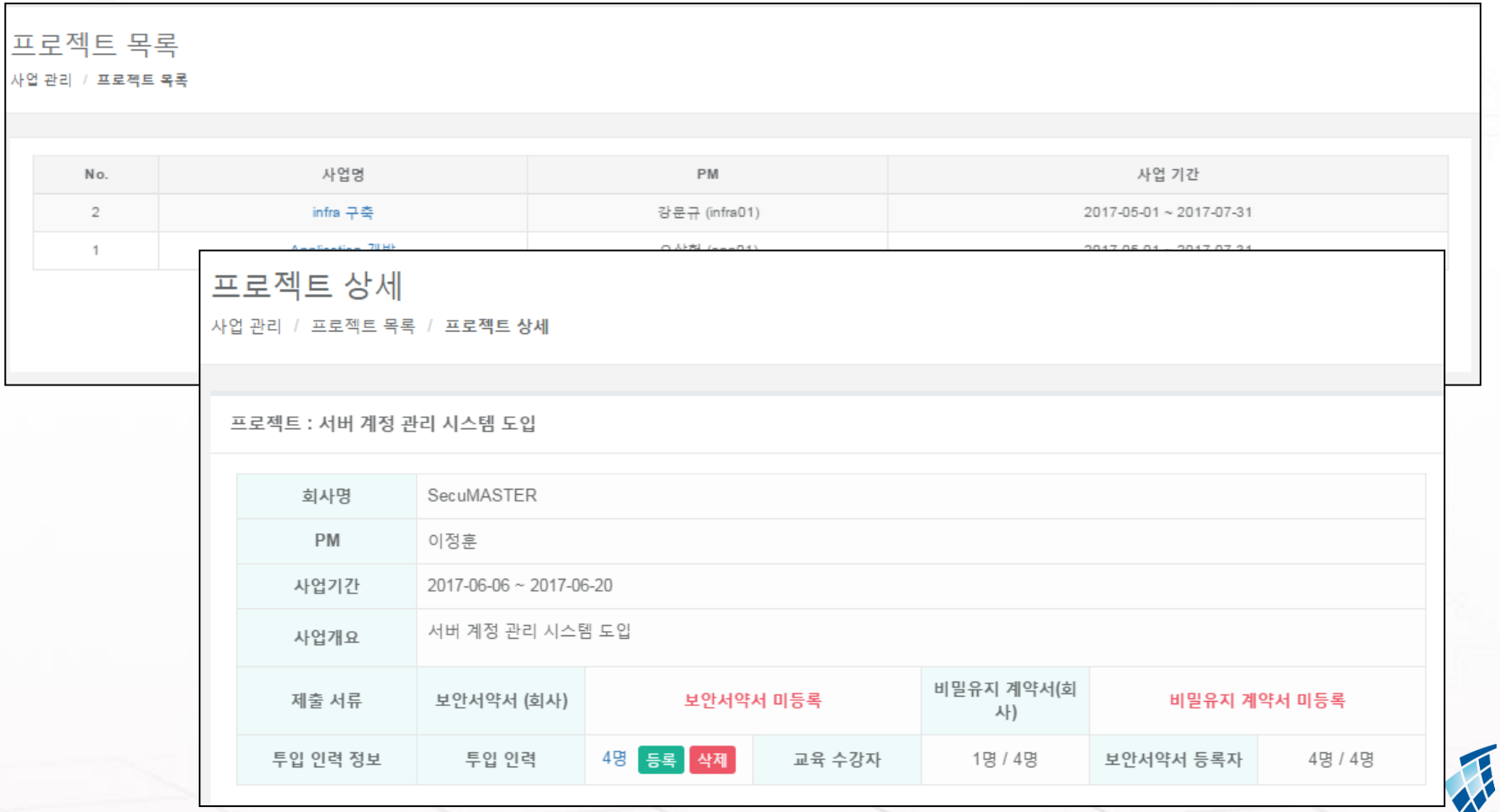
환경 설정 : 정책 항목 설정



No	정책명	승인 IP	등록일	변경일
1	IP 1	127.0.0.2	2016/12/05	2016/12/05
2	104.237.191.1	104.237.191.1	2016/12/07	2016/12/07
3	tta_test_server	210.96.71.211	2016/12/26	2016/12/26
4	210.96.71.111	210.96.71.111	2016/12/26	2016/12/26
5	104.74.185.98	104.74.185.98	2017/01/04	2017/01/04
6	119.207.64.18	192.168.0.231-235	2017/01/04	2017/02/21
7	192.168.0.1	192.168.0.1-230	2017/01/26	2017/02/21

2.9 J-TOPS 주요화면

사업 관리 : 프로젝트 목록



프로젝트 목록

사업 관리 / 프로젝트 목록

No.	사업명	PM	사업 기간
2	infra 구축	강문규 (infra01)	2017-05-01 ~ 2017-07-31
1	Application 개발	오상현 (app01)	2017-05-01 ~ 2017-07-31

프로젝트 상세

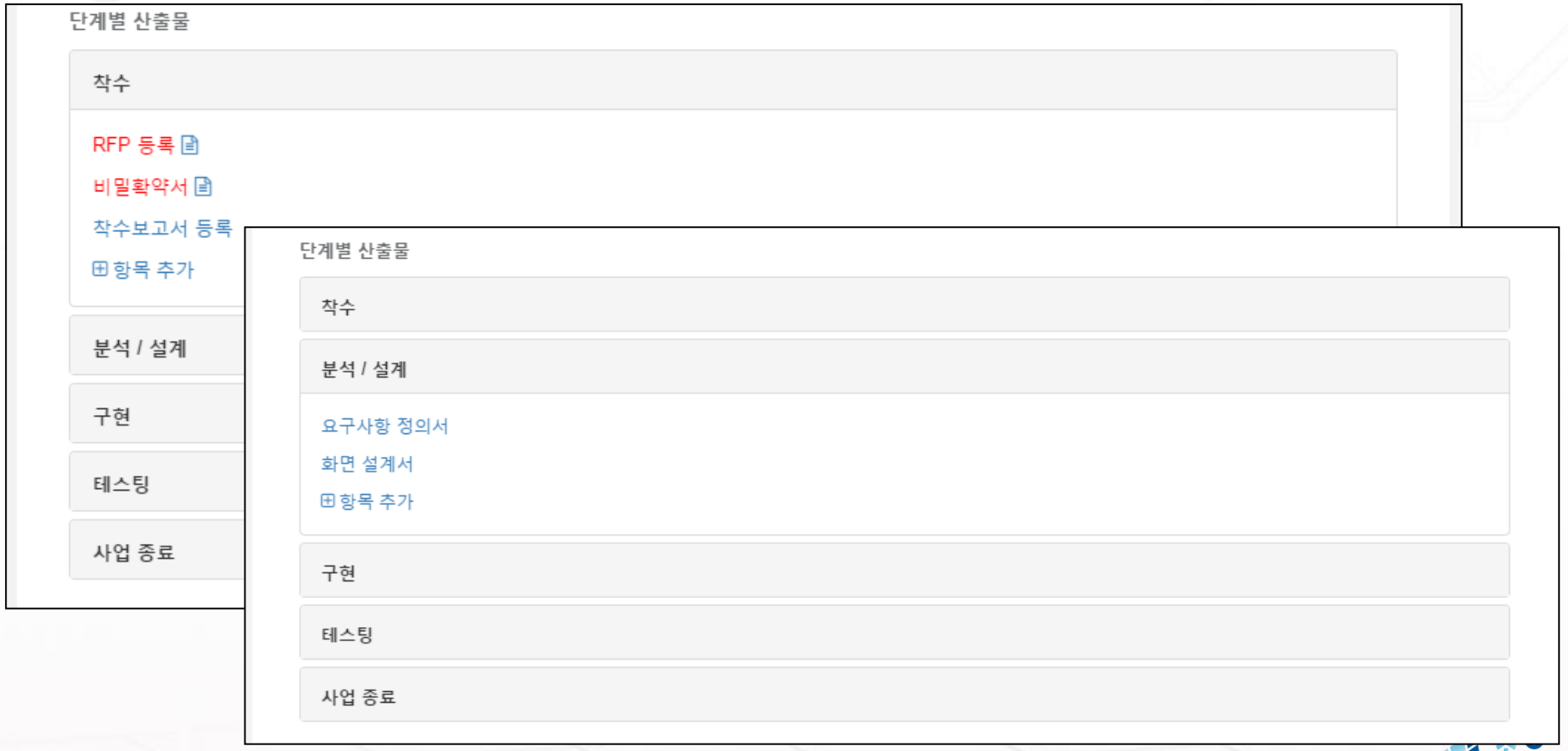
사업 관리 / 프로젝트 목록 / 프로젝트 상세

프로젝트 : 서버 계정 관리 시스템 도입

회사명	SecuMASTER					
PM	이정훈					
사업기간	2017-06-06 ~ 2017-06-20					
사업개요	서버 계정 관리 시스템 도입					
제출 서류	보안서약서 (회사)	보안서약서 미등록		비밀유지 계약서(회사)	비밀유지 계약서 미등록	
투입 인력 정보	투입 인력	4명 등록 삭제	교육 수강자	1명 / 4명	보안서약서 등록자	4명 / 4명

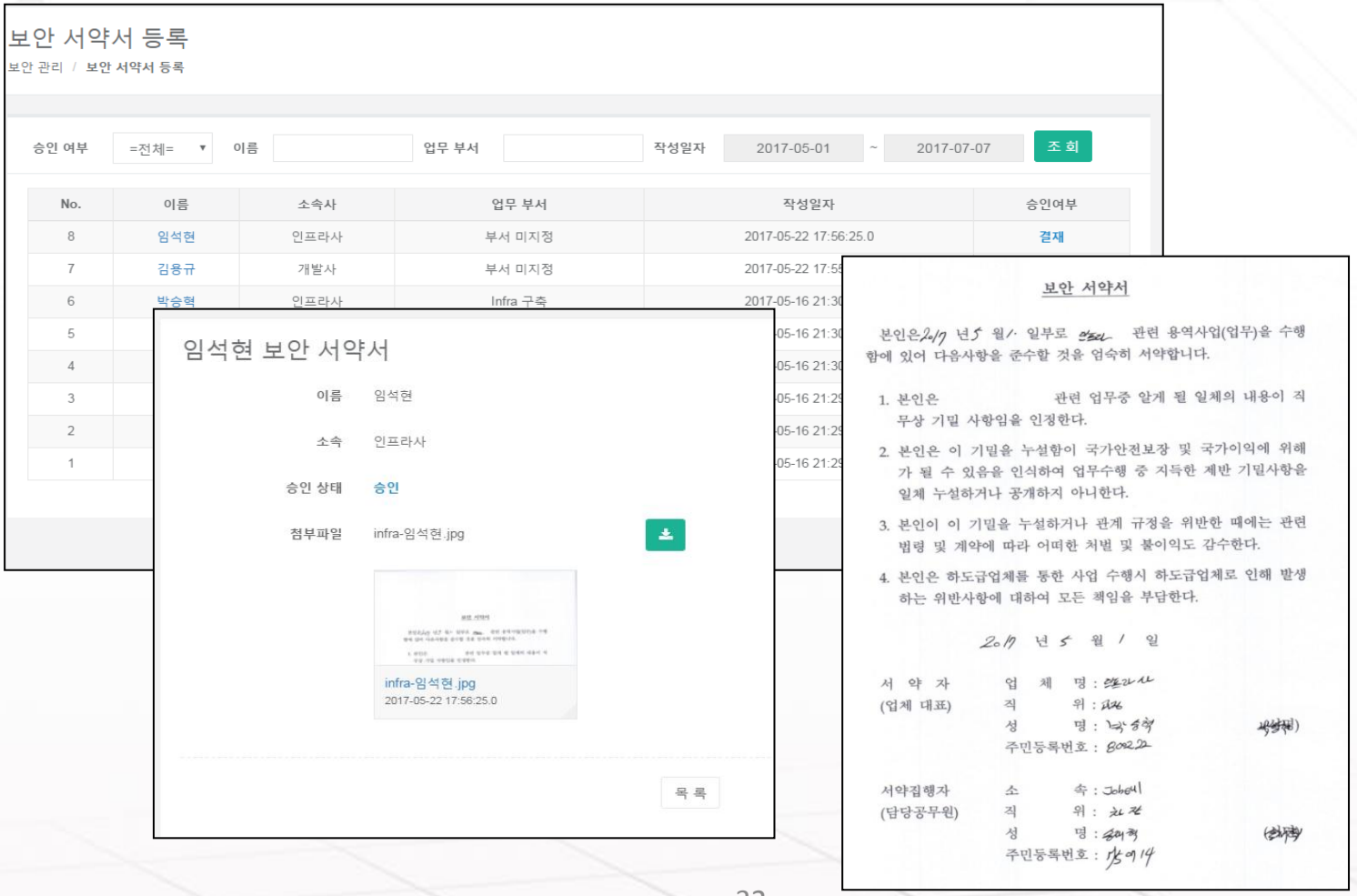
2.9 J-TOPS 주요화면

사업 관리 : 프로젝트 단계별 산출물 관리



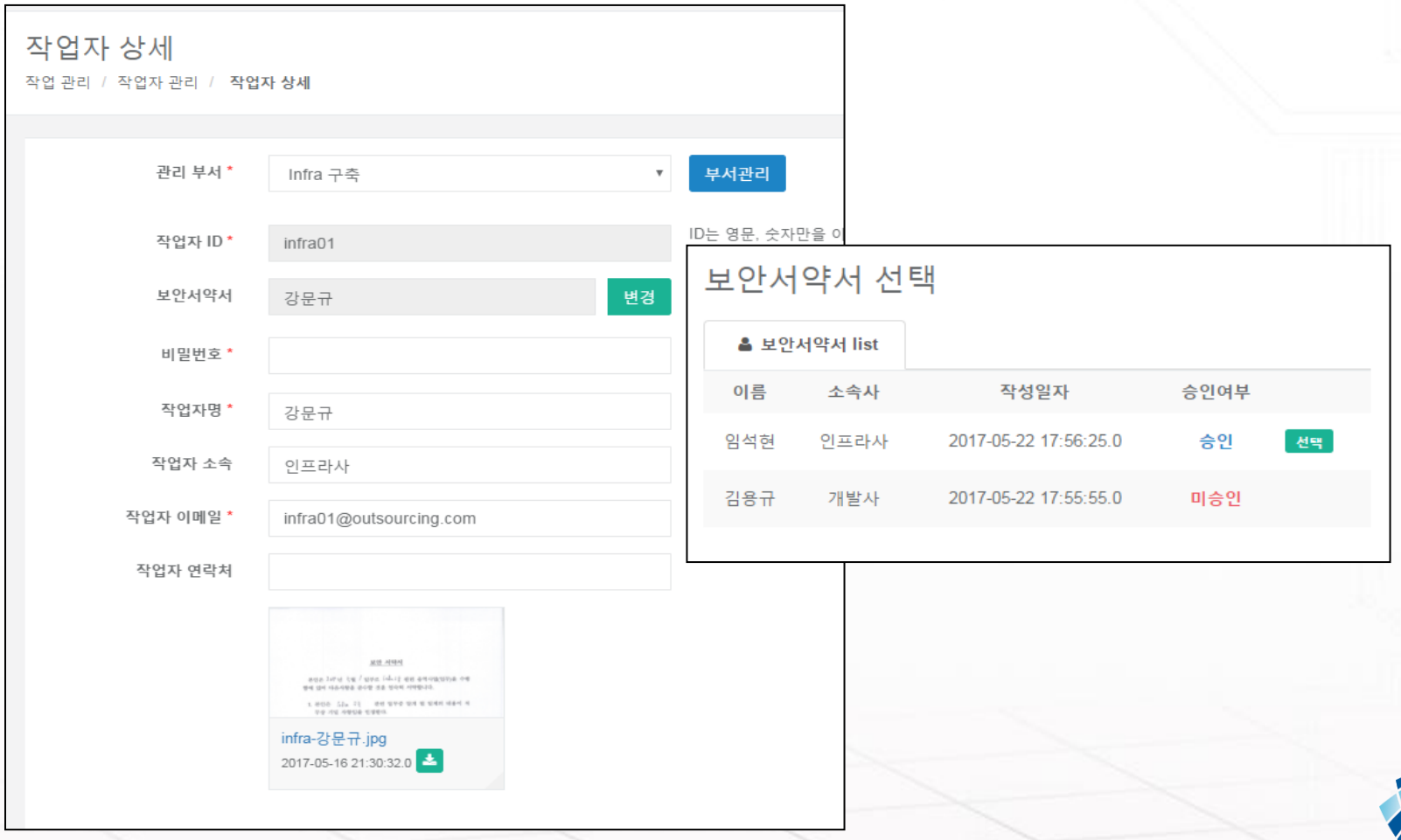
2.9 J-TOPS 주요화면

보안관리 : 보안서약서 등록



2.9 J-TOPS 주요화면

작업 관리 : 작업자 상세

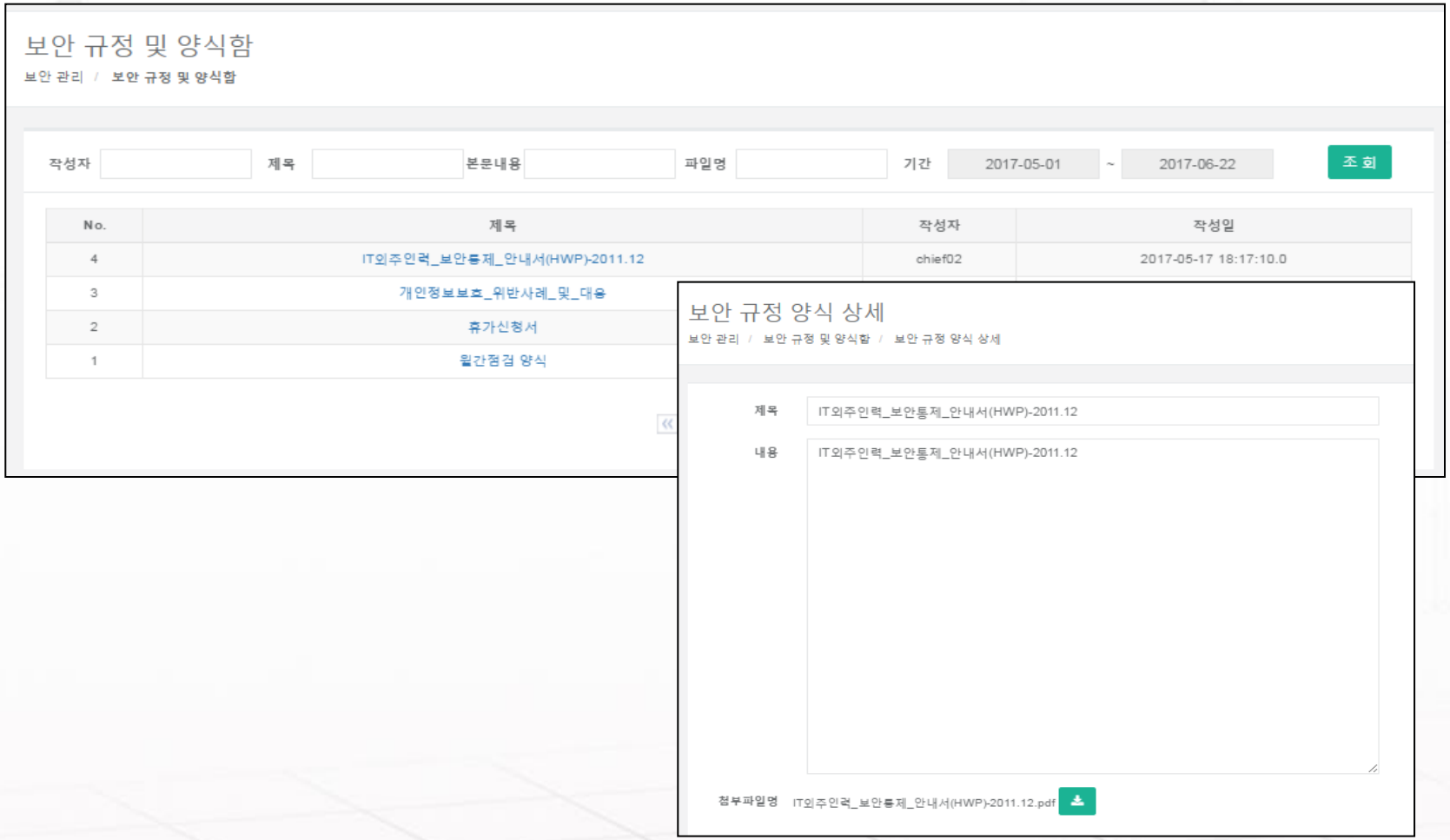


2.9 J-TOPS 주요화면

보안관리 : 보안 규정 및 양식함, 보고서 등록

2.9 J-TOPS 주요화면

보안관리 : 보안교육 자료 및 수강 현황



2.9 J-TOPS 주요화면

사업관리 : 작업자 목록

작업자 목록

사업 관리 / 작업자 목록

이름	ID	관리부서	소속	IP 주소	등록 일자	보안서약서 등록 일시	최근 보안교육 일시
오상현	app01	Application 개발	개발사	192.168.11.128	2017-05-16	2017-05-16 21:32:12	2017-05-17 15:12:18
방승환	app02	Application 개발	개발사	192.168.0.81	2017-05-16	2017-05-16 21:32:18	2017-05-17 15:12:28
나신일	app03	Application 개발	개발사	미등록	2017-05-16	2017-05-16 21:32:06	2017-05-17 15:12:36
강문규	infra01	Infra 구축	인프라사	미등록	2017-05-16	2017-05-16 21:31:41	2017-05-17 15:11:41
박승혁	infra02	Infra 구축	인프라사	192.168.0.8	2017-05-16	2017-05-16 21:31:48	미수강
김선현	infra03	Infra 구축	인프라사	192.168.0.93	2017-05-16	2017-05-16 21:31:35	미수강

3.1 J-TOPS 지원분야 : 금융

전자금융감독규정 시행세칙 (금융감독원, 시행일 : 2016.11.11)

제7조의3(정보보호최고책임자의 업무) 규정 제37조의 5에 따라 감독원장이 정하는 **정보보안 점검항목은 별표 3-2**와 같다. 〈신설 2015.4.8〉

제9조의2(외부주문등에 대한 기준) ① 규정 제60조 제1항 제7호에 따라 감독원장이 정하는 **보안관리방안은 별표5-2**와 같다.
② 규정 제60조 제1항 제14호에 따라 감독원장이 정하는 중요 점검사항은 **별표 5-3**과 같다. 〈신설 2015.4.8〉

PROJECT	세부항목
제7조의 3 (정보보호 최고책임자의 업무)	[별표 3의 2] 정보보안 점검항목
제9조의 2 (외부주문 등에 대한 기준)	[별표 5의 2] 보안관리방안
	[별표 5의 3] 중요 점검사항

3.1 J-TOPS 지원분야 : 금융

□ [별표 3의 2] 정보보안 점검항목

구분	점검항목	J-TOPS
단말기	**업무담당자 이외의 단말기 무단조작 금지 조치 여부**	**지원**
	정보처리시스템 접속 단말기의 정당한 사용자인가를 확인할 수 있는 기록 유지 여부	**지원**
	중요 단말기의 외부 반출 금지 여부	**지원**
	중요 단말기의 인터넷 접속 금지 여부	**지원**
	중요 단말기의 그룹웨어 접속 금지 여부	**지원**
	단말기에서 보조기억매체 및 휴대용 전산장비 접근 통제 여부	**지원**
전산자료	이용자 정보 조회.출력 통제 여부	**지원**
	단말기 공유 금지 여부	**지원**
	전산자료 및 전산장비의 반출·반입 통제 여부	**지원**
	사용자 인사 조치 시 지체 없이 해당 사용자계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템 접근을 통제하고 있는지 여부	**지원**
정보처리시스템	**내부통신망의 비인가 전산장비·무선통신 접속 통제 여부**	**지원**
해킹 등 방지대책	정보보호시스템에 업무목적 이외 기능 및 프로그램 제거 여부	**지원**
	무선통신망 이용 업무에 대한 승인 및 사전 지정 여부	**지원**
이용자 유의사항	비밀번호 유출위험 및 관리에 관한 사항의 공지 여부	**지원**
	제공하고 있는 이용자보호 제도에 관한 사항의 공지 여부	**지원**
	해킹.피싱 등 전자적 침해방지에 관한 사항의 공지 여부	**지원**

* 일부 기능은 추가 개발 필요

3.1 J-TOPS 지원분야 : 금융

□ [별표 5의 2] 보안관리방안

No.	구분	세부사항	J-TOPS
수행	인력	용역사업 참여인원에 대해서는 '정보 유출' 방지 조항 및 개인의 자필 서명이 들어간 보안서약서 징구	지원
		용역사업 수행 前 참여인원에 대해 법적 또는 금융회사 또는 전자금융업자의 규정에 따른 비밀유지 의무 준수 및 위반 시 처벌내용 등에 대한 보안교육 실시 * 유출 금지 대상정보 및 정보 유출 시 부정당업자 제재조치 등에 대한 교육 병행	지원
		금융회사 또는 전자금융업자는 사업 수행 중 업체 인력에 대한 보안점검 실시, '유출금지 대상 정보' 외부 유출 여부 확인	지원
	사무실. 장비	용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시	지원
		용역직원이 노트북 등 관련 장비를 외부에서 반입하여 내부 망에 접속 시 악성코드 감염여부 및 반출 시마다 자료 무단반출 여부 확인	지원
		인가 받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 금융회사 또는 전자금융업자의 승인하에 사용	지원
	내.외부망 접근 시	금융회사 또는 전자금융업자는 개발시스템과 운영시스템을 분리하고, 용역업체는 업무상 필요한 서버에만 제한적 접근 허용	지원
		용역사업 수행 시 금융회사 또는 전자금융업자 전산망 이용이 필요한 경우 – 사업 참여인원에 대한 사용자계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 허용되지 않은 금융회사 또는 전자금융업자의 내부문서 접근 금지 – 계정별로 부여된 접속권한은 불필요시 즉시 해지하거나 계정을 폐기 – 참여인원에게 부여한 계정은 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인 – 금융회사 또는 전자금융업자는 내부서버 및 네트워크 장비에 대한 접근기록 이상 여부를 정기 점검	지원
		용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 금융회사 또는 전자금융업자의 보안통제하에 제한적 허용	지원
		용역업체 사용 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 원천 차단	지원

* 일부 기능은 추가 개발 필요

3.1 J-TOPS 지원분야 : 금융

□ [별표 5의 3] 중요 점검사항

No.	점검항목	J-TOPS
1	이용자 정보의 조회·출력에 대한 통제 및 이용자 정보 조회시 사용자, 사용일시, 변경·조회내역, 접속방법 기록·관리	지원
2	운영시스템 접속·사용 통제	지원
3	내부통신망의 비인가 전산장비·무선통신 접속 통제 (정보처리시스템을 이용한 통제 장치 마련시 통제 장치에 대한 일일점검으로 대체 가능)	지원
4	전산자료 및 전산장비 반출·반입 통제	지원
5	전산실 등 출입자 관리기록부 기록·보관	지원
6	인터넷(무선통신망 포함) 사용 통제 (정보처리시스템을 이용한 통제 장치 마련시 통제장치에 대한 일일점검으로 대체 가능)	지원
7	USB 등 보조기억매체 사용 통제	지원

* 일부 기능은 추가 개발 필요

3.2 J-TOPS 지원분야 : 공공기관

정보보안 세부지침 '미래창조과학부'

□ 제36조 (용역사업 수행단계)

구분	관리항목	J-TOPS
참여인원에 대한 보안관리	1. 용역사업 참여인원에 대해서는 **보안서약서 징구** 2. 용역사업 수행前 참여인원에 대해 법적 또는 발주기관 규정에 의한 비밀유지 의무 준수 및 위반 시 처벌내용 등에 대한 보안교육 실시 3. 발주기관은 사업 수행 중 업체 **인력에 대한 보안점검 실시**, '누출금지 대상 정보' 외부 누출여부 확인	지원
자료에 대한 보안관리	3. 용역사업 관련 **자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지**하고 용역 발주기관과 용역업체간 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자 우편을 이용, 첨부자료 암호화 후 수발신	지원
사무실·장비에 대한 보안관리	2. 용역업체 사무실 또는 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시 3. 발주기관 내부에서 용역사업을 수행할 경우 용역 참여직원이 노트북 등 관련장비를 **외부에 반출·입시마다 악성코드 감염여부 및 자료 무단반출 여부 확인** 4. **인가받지 않은 USB 등의 휴대용 저장매체 사용을 금지**하며 산출물 저장을 위해 휴대용 저장매체가 필요한 경우 발주기관의 승인하에 사용	지원
내·외부망 접근 시 보안관리	1. 용역업체 사용 전산망은 방화벽 등을 활용하여 해당기관 업무 망과 분리 구성하고 업무상 **필요한 서버에만 제한적 접근 허용** 2. 사업참여 인원에 대한 사용자 계정은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 기관 **내부문서 접근 금지**하고 불필요 시 곧바로 권한을 해지하거나 계정을 폐기 3. 참여인원에게 부여한 패스워드는 사업 **보안 담당자가 별도로 기록 · 관리하고** 수시로 해당 계정에 접속하여 저장된 자료와 **작업이력 확인** 4. 용역사업 보안관리담당은 서버 및 장비운영자로 하여금 **내부서버 및 네트워크 장비에 대한 접근 기록을 매일 확인**하여 이상유무 보고 5. 용역업체에서 사용하는 PC는 **인터넷 연결을 금지**하되, 사업수행상 연결이 필요한 경우에는 발주기관의 보안통제 하에 제한적 허용 6. 발주기관 및 용역업체 전산망에서 **P2P, 웹하드 등 인터넷 자료공유사이트**로의 접속을 방화벽 등을 이용해 **원천차단**	지원

* 일부 기능은 추가 개발 필요

3.2 J-TOPS 지원분야 : 공공기관

정보보안 세부지침 '미래창조과학부'

□ 정보보안 기본활동 (정보보안점검 체크리스트)

No.	점검항목	J-TOPS
1	사이버보안진단의 날을 내실 있게 수행하는가?	지원
2	정보보안 위규 · 사고, 정보통신망 장애 발생 시 보고체계 및 조치절차가 있는가?	지원
3	정보시스템 사용자에 대한 심사 등 인적보안 절차 · 방법을 강구 중 인가?	지원
4	보직변경 등 인사이동시 정보시스템 접근권한을 신속하게 조정하는가?	지원
5	서버 · PC 등 정보시스템 현황을 제대로 파악하는가?	지원
6	정보통신장비(노트북 등) 반출 · 반입 통제를 철저히 하는가?	지원
7	업무자료를 상용 전자우편으로 전송하고 있지 않는가?	지원

* 일부 기능은 추가 개발 필요

3.2 J-TOPS 지원분야 : 공공기관

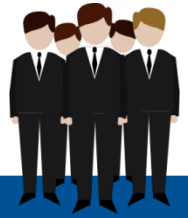
정보보안 세부지침 '산업통상자원부'

□ 제23조 (인적보안) 일일 용역사업 보안점검 리스트

No.	J-TOPS 점검항목	J-TOPS
1	용역업체 사용 전산망과 기관 전산망의 분리여부 (VLAN 분리 포함)	불가
2	용역업체 직원 PC의 **내부 정보시스템 접근 통제** 여부	지원
3	P2P, 웹하드, 메신저 등 불필요한 **인터넷 접속 차단** 여부	지원
4	용역업체 직원에 주요 계정 비밀번호 제공 여부	지원
5	용역업체 직원에 비밀번호 부여시 관련사항 별도 기록 여부	지원
6	용역업체 직원에 시스템 관리자 계정 단독 접근 여부	지원
7	**노트북PC 등 휴대형 정보시스템을 시스템 관리용 PC로 활용** 여부	지원
8	용역업체 직원 등에 의한 기관 **외부에서의 원격 접속 · 작업** 여부	지원
9	용역업체 정보시스템 접근 시 **작업이력 로깅** 기능 사용 여부	지원
10	용역업체 PC에 설치된 운영체제 및 응용프로그램 최신상태 유지 여부	불가
11	용역업체 PC 백신 프로그램 자동 업데이트 및 실시간 감시기능 사용 여부	불가
12	용역업체 PC USB · CD-RW · **무선랜 등 매체 통제** 여부	지원
13	용역업체 PC 비밀번호 및 화면보호기 설정 여부	지원
14	용역업체 직원의 비인가 정보통신장비(노트북 등) 휴대 · 반입 여부	지원

* 일부 기능은 추가 개발 필요

3.3 ISMS 인증 개요



정보보호 관리체계 인증 심사기준
(정보보호 관리과정12개 + 정보보호대책 92개)

총 104개 인증기준에 대해 적합성 평가

정보보호 관리과정 (5단계, 12개 인증기준)

정보보호 정책 수립 및 범위설정	정보보호대책 구현	사후관리
	경영진 책임 및 조직구성	위험관리

정보보호 관리과정 (13분야, 92개 인증기준)

1. 정보보호 정책	4. 정보자산 분류	7. 물리적 보안	10. 접근통제
2. 정보보호 조직	5. 정보보호 교육	8. 시스템 개발보안	11. 운영보안
3. 외부자 보안	6. 인적 보안	9. 암호통제	12. 침해사고 관리
			13. IT 재해복구

J-TOPS 지원
4분야 24항목

PROJECT	인증기준 수	주요 점검항목 수
정보보호 관리과정	12	28
정보보호 대책	92	225
소계	104	253

3.3 ISMS 인증 항목

통제분야	통제목적	통제사항	통제내용
7.물리적 보안	7.1 물리적 보호구역	7.1.3 보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 **작업 절차를 수립**하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
	7.3 사무실 보안	7.3.2 공용업무 환경보안	사무실에서 공용으로 사용하는 사무처리기기, 문서고, 공용 PC, 파일서버 등을 **통해 중요정보 유출이 발생하지 않도록 보호대책을 마련**하여야 한다.
8. 시스템 개발 보안	8.1 분석 및 설계보안관리	8.1.3 보안로그 기능	정보시스템 설계 시 사용자의 인증,권한 변경, 중요정보 이용 및 유출 등에 대한 **감사 증적을 확보**할 수 있도록 하여야 한다.
		8.1.4 접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 **접근권한**을 부여할 수 있도록 하여야 한다.
	8.2 구현 및 이관 보관	8.2.2 개발과 운영 환경분리	**개발 및 시험 시스템**은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 **원칙적으로 분리**하여야 한다.
	8.3 외주개발 보안	8.3.1 외주개발보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 **보안요구사항을 계약서에 명시하고 이행여부를 관리 · 감독**하여야 한다.

3.3 ISMS 인증 항목

통제분야	통제목적	통제사항	통제내용
10. 접근통제	10.1 접근통제 정책	10.1.1 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 **접근통제 정책을 수립**하여야 한다.
	10.2 접근권한 관리	10.2.1 사용자 등록 및 권한부여	정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 **사용자 등록 및 해지 절차를 수립**하고 업무 필요성에 따라 **사용자 접근권한을 최소한으로 부여**하여야 한다.
		10.2.2 관리자 및 특수 권한 관리	정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 **계정 및 권한을 식별하고 별도 통제**하여야 한다.
		10.2.3 접근권한 검토	정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용 (장기간 미사용), 변경(퇴직 및 휴직,직무변경, 부서변경)의 적정성 여부를 **정기적으로 점검**하여야 한다.
	10.4 접근통제 영역	10.4.1 네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 **접근통제** 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자그룹, 정보자산의 중요도에 따라 내외부 네트워크를 분리하여야 한다.
		10.4.2 서버 접근	**서버별**로 접근이 허용되는 사용자, 접근제한 방식, **안전한 접근수단 등을 정의**하여 적용하여야 한다.
		10.4.3 응용 프로그램 접근	사용자의 업무 또는 직무에 **따라 응용프로그램 접근권한을 제한**하고 불필요한 중요정보 노출을 최소화해야 한다.
		10.4.4 데이터베이스 접근	**데이터베이스 접근을 허용**하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.
		10.4.5 모바일 기기 접근	모바일기기를 업무 목적으로 내. 외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 **접근통제 대책**을 수립하여야 한다.
		10.4.6 인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급. 운영하는 **주요직무자**의 경우 **인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저등)를 제한**하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 **통해 인터넷 접속내역을 모니터링하여야** 한다.

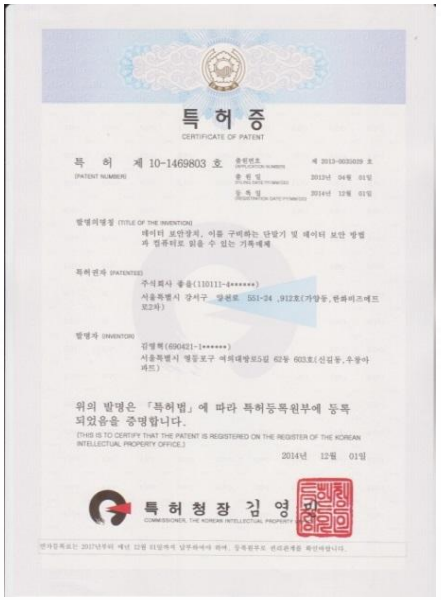
3.3 ISMS 인증 항목

통제분야	통제목적	통제사항	통제내용
11. 운영보안	11.1 운영 절차 및 변경 관리	11.1.1 운영절차 수립	정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 **시스템 운영을 위한 절차를 수립**하여야 한다.
		11.1.2 변경관리	정보시스템 관련 자산의 **모든 변경내역을 관리**할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다.
	11.2 시스템 및 서비스 운영보안	11.2.5 원격운영관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 **특정 단말에서만 접근을 할 수 있도록 제한**하고, **원격지**에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 **원칙적으로 금지**하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안 (백신, 패치 등) 등의 보호대책을 수립하여야 한다.
		11.2.6 스마트워크 보안	**재택근무, 원격협업** 등과 같은 원격 업무 수행 시 이에 대한 **관리적. 기술적 보호대**책을 수립하고 이행하여야 한다.
		11.2.7 무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.
	11.4 매체 보안	11.4.1 정보시스템 저장매체 관리	정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 **저장매체 폐기 및 재사용 절차를 수립**하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
		11.4.2 휴대용 저장매체 관리	조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 **절차를 수립**하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.
	11.6 로그 및 모니터링	11.6.3 접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 **사용자 접근**이 업무상 허용된 범위에 있는 지 **주기적으로 확인**하여야 한다.

3.4 GS 인증 및 보유 특허

GS 인증 (1등급)
J-TOPS v2.0 (2017. 01)

보안 시스템, 이를 위한 단말기
및 보안 방법
(J-TOPS 플랫폼 기반 특허)



데이터 보안장치, 이를 구비하는
단말기 및 데이터 보안 …

인증 시스템 및 방법

찾아오시는 길

감사합니다.

㈜좋을

주소 : 서울 강서구 양천로 551-24 (가양동, 한화비즈메트로 2차 911,912호)
TEL : 02 6957 1919
FAX : 02 6957 1912

좋을
주식회사 좋을