

통합 IT 외주관리 플랫폼

J-TOPS

**Total
Outsourcing
Platform System**



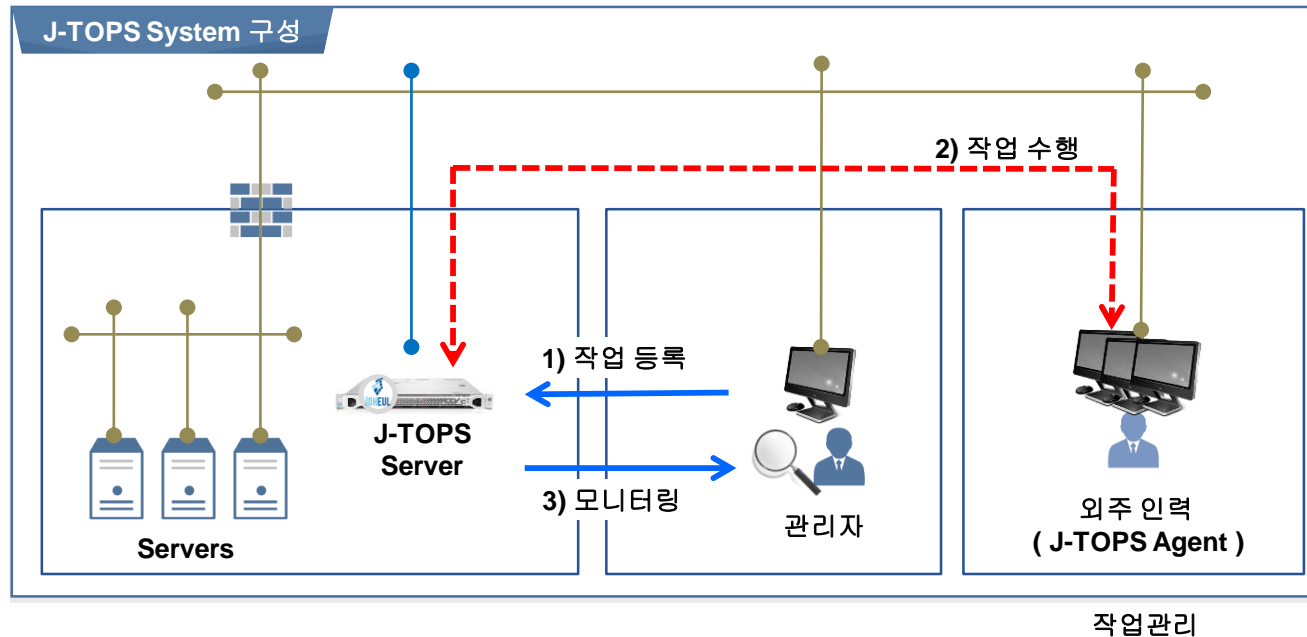
J-TOPS : 통합 IT외주관리 플랫폼

J-TOPS 는 IT 개발 / 유지보수 업무에 있어서 외부 기술 인력(작업자)의 참여 혹은 지원이 필요한데 상주 / 비상주 작업자들을 **보안 관리자 입장에서 효율적으로 관리**할 수 있는 플랫폼으로 관련 **특허 3개**를 등록하였고, **GS 인증**을 획득하였습니다.



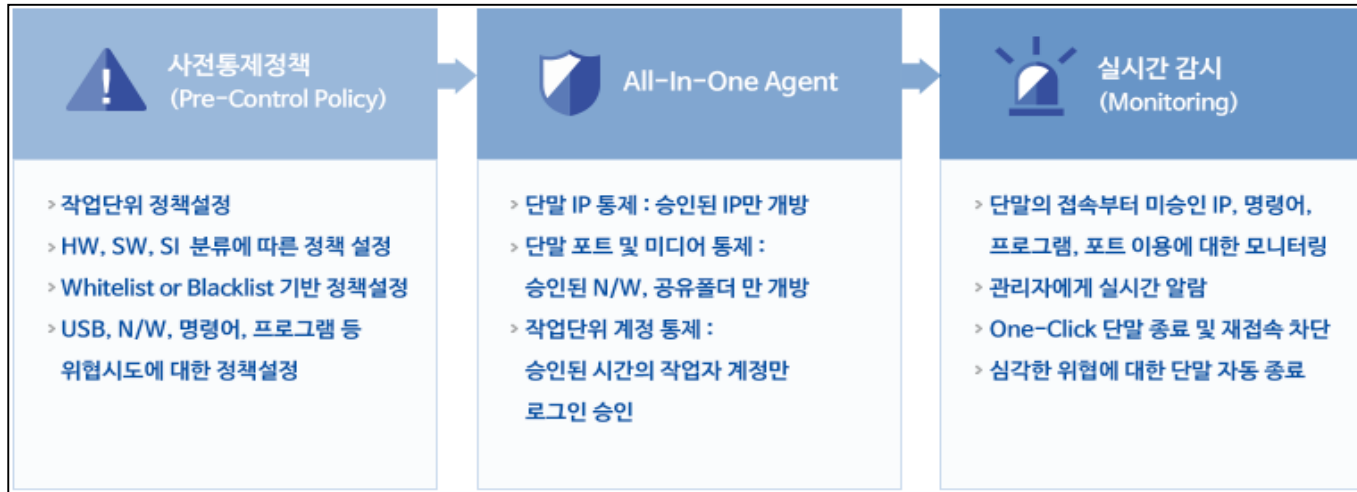
J-TOPS 시스템 구성

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 PC 한해 작업자가 작업할 수 있도록 통제합니다.

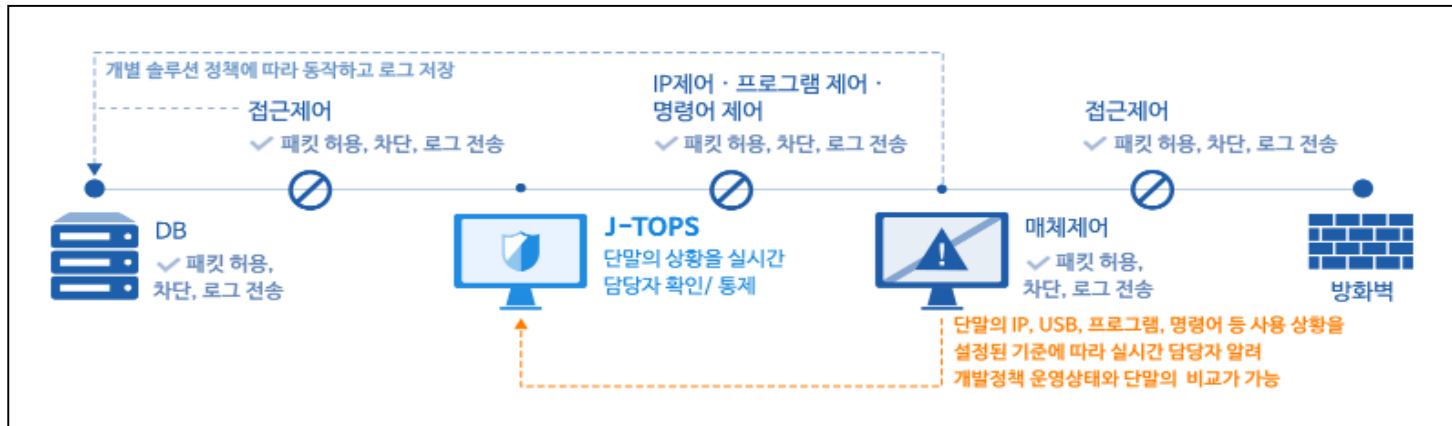


J-TOPS 업무 흐름

외주 관리 업무 흐름



매체 제어 / 접근 제어 업무 흐름



J-TOPS 도입 근거

1 자체 점검 및 책임 강화

1-① 금융회사 자율점검 강화

가. 현황 및 문제점

- ☐ 금융회사의 IT보안상 취약점은 해당 금융회사가 가장 잘 파악할 수 있으나,
 - IT감사 전문인력이 부족한 중소형 금융회사는 IT부문에 대한 위규사항 자체 감사·점검에 어려움
- ☐ 규정상 정보보안 및 외부주문보안 점검 의무는 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 매월 점검(12개 항목)

나. 개선방안

- ☐ IT감사 역량이 부족한 금융회사 지원을 위해 IT 내부감사 가이드라인 및 IT 내부감사요원 교육프로그램을 마련하고,
 - 상시적인 내부통제 강화를 위해 감사부서 내 IT감사 전담 인력을 배치토록 권고
- ☐ 기 시행중인 'IT 부문 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 점검의 실효성 제고를 위해 지나치게 세세한 점검항목을 필수항목 위주로 개편

[2015년 06월 19일 금융감독원/금융위원회 보도자료]

전자금융감독규정 시행세칙

- 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 관리등급 부여에 관한 고시)

- 외부자 보안 / 물리적 보안 / 시스템 개발 보안

전자금융감독 규정 시행세칙

전자금융감독규정 시행세칙 (금융감독원, 시행일 : 2016.11.11)

제7조의3(정보보호 최고책임자의 업무) 규정 제37조의 5에 따라 감독원장이 정하는
정보보안 점검항목은 별표 3-2와 같다. <신설 2015.4.8>

제9조의2(외부주문 등에 대한 기준) ① 규정 제60조 제1항 제7호에 따라 감독원장이 정하는
보안관리방안은 별표5-2와 같다.

② 규정 제60조 제1항 제14호에 따라 감독원장이 정하는 **중요 점검사항**은 **별표 5-3**과 같다.
<신설 2015.4.8>

조항	세부 항목
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

전자금융감독 규정 시행세칙

[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
	비밀번호 유출위험 및 관리에 관한 사항의 공지 여부	지원
이용자 유의사항	제공하고 있는 이용자보호 제도에 관한 사항의 공지 여부	지원
	해킹, 피싱 등 전자적 침해방지에 관한 사항의 공지 여부	지원

전자금융감독 규정 시행세칙

[별표 5의 2] 보안관리방안

단계	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 유출여부 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 내부분서 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

전자금융감독 규정 시행세칙

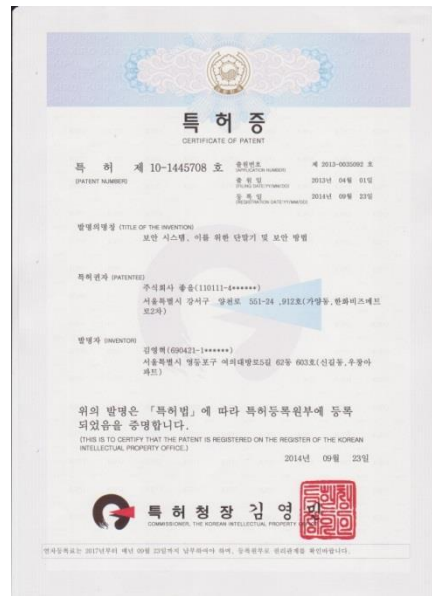
[별표 5의 3] 중요 점검사항

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

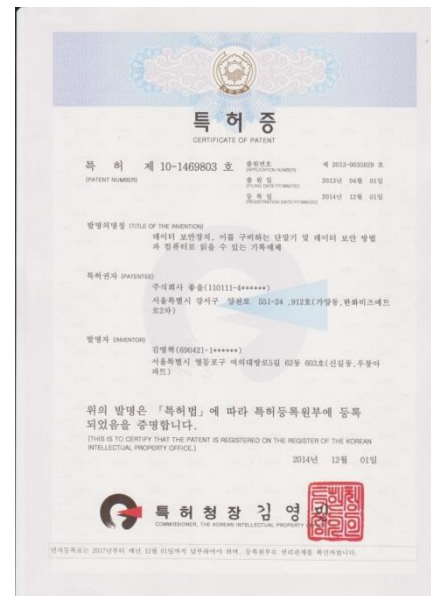
인증 및 보유 특허



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

고객사



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

References



우정사업정보센터



근로복지공단



KOMIPO
한국중부발전



법무부
MINISTRY OF JUSTICE



합동참모본부
R.O.K Joint Chiefs of Staff



동북아역사재단
NORTHEAST ASIAN HISTORY FOUNDATION

NEXTIN
Solutions

KTX 수서



원자력병원

회사소개



(주) 제이엘 인프라는 국내 유일의 IT 외주 관리 전문 업체인
주식회사 종을의 프리미엄 파트너 입니다.

개발사



서울 강서구 양천로 551-24
(가양동, 한화비즈메트로2차 911, 912호) T. 02-6957-1919
Copyright2015 JOHEUL Co., Ltd. All Right Reserved