



SPAC SYSTEM



S
P
A
C



신뢰만으로 가능할까요?

망분리 환경에서의 원격접속 단말통제
외주용역직원에 대한 외주운영 및 개발환경
정보시스템 접근에 대한 원격작업통제/정보유출방지
신뢰 하나만으론 너무 위험합니다.



이거 하나면 충분할까요?



원격접속, 외주작업 PC
사용에 따른 위험



위험 명령어를 통한
시스템손상 및 악의적
개발소스 심기

비인가 외장매체를 통한
2차 정보유출



시스템 접속정보 노출 및
임의 접근 허용

원격접속 PC! 외부작업 PC!

이거 하나면 충분합니다!!



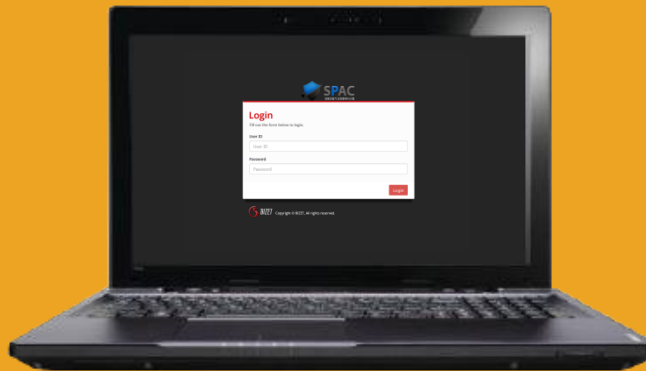
- ▣ 원격접속단말기 식별/인증
- ▣ 무설치 웹기반 통제 프로그램 내장
- ▣ 외주용역자 임의 단말기 작업통제
- ▣ 프로토콜/명령어/프로그램/매체사용/작업시간 통제
- ▣ 장치, 프로그램, 명령어 등 텍스트 및 동영상 로그수집
- ▣ 관리자/작업자 별 로그인 통제
- ▣ 정보시스템 임의접속 차단
- ▣ 프로토콜별 전용 접속프로그램 내장
- ▣ 접속권한별 접속 계정/암호 관리
- ▣ 텍스트 로그 시점별 동영상 호출 표시

접속작업 Workflow

STEP	작업내용	내부접속		원격접속
		운영/관리 외주작업	유지보수 방문작업	원격접속 단말작업
01	작업신청 상주작업, 정기점검, 긴급대응 등에 따라 작업신청, 지정, 예약 1. 작업자, 목적, 대상장비 신청 2. 일정, 매체사용 신청 3. 관리자 지정작업/긴급작업 시 신청 후 자동승인	 <ul style="list-style-type: none"> 정기/상주작업 사전 예약 등록 개별작업 관리페이지 작업신청 	 <ul style="list-style-type: none"> 유지보수 방문작업 템플릿 등록 장애대응 작업 개별 등록 	 <ul style="list-style-type: none"> 긴급작업 시 관리자 직접 등록 사전 등록 외부작업자 신청가능
02	작업승인 신청내역 확인 후 작업 PC / 작업토큰 지정 및 통제 / 보안정책 지정 승인 1. PC 및 작업토큰 배정 2. 명령어, IP, 프로그램 사용, 로그 수집 방법 등 통제정책 지정 3. 지정PC, 작업자 계정, 작업토큰인증 등 조합으로 작업인증 지정	 <ul style="list-style-type: none"> 신청내역 승인 시 작업PC, 작업 통제정책 지정 작업PC배정 	 <ul style="list-style-type: none"> 신청내역 승인 시 작업PC, 작업토큰, 작업통제정책 지정 작업PC, 작업토큰 배정 	 <ul style="list-style-type: none"> 원격접속 작업자 계정, 작업PC, 작업토큰, 통제정책 선별지정 작업인증, 작업 통제 및 실시간 감시정책 지정
03	작업 및 관제 내부, 원격접속 별 작업자 계정, 작업 PC, 작업토큰 인증 작업개시 및 감시 1. 로그인 후 지정된 작업권한 적용 2. 매체, 명령어, 프로그램 차단 등 통제정책 적용 및 로그수집 개시 3. 작업내역 실시간 대시보드 반영 및 위험행위 경보	 <ul style="list-style-type: none"> 지정정책에 따라 로그인 관리자 지정 보안정책 적용 허가된 정보시스템 접속 작업내역 실시간 대시보드 표시 	 <ul style="list-style-type: none"> 작업토큰 연결 후 로그인 정기작업 설정된 보안정책 적용 허가된 정보시스템 접속 작업내역 실시간 대시보드 표시 	 <ul style="list-style-type: none"> 작업토큰 연결 후 로그인 시도 작업자 계정 정확, PC 정보식별, 작업토큰 보안정책 확인 및 인증 정책적용 및 실시간 작업감시
04	보고 및 감사 작업완료 후 작업결과에 대한 보고서 작성 및 필요자료 전송 1. 관리페이지 내 작업보고서 입력 2. 텍스트 및 동영상 로그 자동업로드 3. 필요 시 작업 시 생성파일 업로드 4. 작업결과 종합보고서 출력 제출	 <ul style="list-style-type: none"> 관리페이지 내 작업 보고서 입력 관리자 지정방식에 의해 텍스트, 동영상 로그 자동전송 작업결과 종합보고서 출력 제출 	 <ul style="list-style-type: none"> 등록 양식에 따라 정기 점검, 유지보수 보고서 입력 관리자 지정방식에 의해 텍스트 및 동영상 로그 전송 작업 토큰 반납 	 <ul style="list-style-type: none"> 관리자 작업완료 보고 관리페이지 보고서 등록, 방문보고, 온라인 보고 등 관리자 지정방식에 따라 작업보고 진행 필요 시 작업토큰 회수

SPAC은 정보시스템 접속작업 개념을 새롭게 제시합니다.

정보시스템 접속작업 관제, 통제, 감사를 위한
원격접속 단말통제 및 외주용역 관리시스템



- ▣ 관리서버 접속을 통해 승인 정보시스템 접속 (별도 게이트웨이 장비 설치 또는 네트워크 구성변경 없음)
- ▣ 내부 운영자 단말기 지정 및 작업전용 USB 장치 지정 기능 제공
- ▣ 원격접속 전용 PC사용 지정 또는 미지정 PC사용을 위한 에이전트 미설치 단말기 통제환경 제공
- ▣ 작업 승인 시 접속가능 프로토콜 지정 및 전용접속 프로그램 제공으로 접속정보 노출 차단
- ▣ 관리자에 의해 지정 또는 허가된 단말기, 사용자, 인증 장치 소유자만이 접속이 허가되는 강력한 보안통제 기능 제공
- ▣ 원격접속은 물론 유지보수, 정기점검 등의 일상작업까지 일원화된 관리/통제 기능 제공

SPAC은 단말기는 원격접속 작업과 외주용역 작업통제에 대한 체계화된 WorkFlow를 제공합니다.



외주용역자 단말기 통합 관제 시스템



실시간
전체 작업 현황
데시보드 지원



작업자 신청
실시간 데시보드 표기 및 실시간 알람



통제 단말기
실시간 로그 전송



보안 위반 행위 발생 시
데시보드 표기 및 실시간 알람



보안 위반 행위 단말기 관리자
즉시 통제 기능 제공



SPAC은 작업 감사 추적 시스템 입니다.

텍스트/동영상 로그 연동 기능을 통한 입체적 감사 시스템 제공

- ▣ 텍스트 이벤트(작업자인증/명령어/프로그램/매체사용/대상장비접속) 로그 제공
- ▣ Snapshot이 아닌 풀 동영상 단말기 작업 로그 제공
- ▣ 각 텍스트 이벤트 로그 발생 시점의 동영상 로그 연동 기능 제공
- ▣ 텍스트와 동영상 로그 연동을 통한 사용자 단말기 작업 행위에 대한 입체적 추적 감사
- ▣ 텍스트로그를 클릭하면 자동으로 해당 시점의 동영상을 호출하여 표시

도입효과

원격접속 단말통제 및 외주용역관리시스템 SPAC는 내부업무시스템 다양한 접속작업과 유지보수 및 정기 점검 등의 일상 작업에 대한 일원화된 보안통제 및 감사로그 수집 기능을 제공합니다.



정보보호 규제강화 및 개인정보보호 조치 관련법 및 시행령		
개인정보의 안정성 확보 조치 기준	제 3조	내부 관리 계획의 수립·시행
	제 4조	접근 권한의 권리
	제 6조	접근 통제 시스템 설치 및 운영
	제 8조	접속 기록의 보관 및 위·변조방지
개인정보의 기술적·관리적 보호 조치 기준	제 4조	접근통제
	제 5조	접속 기록의 위·변조 방지
정보 통신망 이용 촉진 및 정보 보호 등에 관한 법률	제 45조	정보 통신망의 안정성 확보 등
	제 46조	집적된 정보 통신 시설의 보호
전자 금융 감독 규정	제 12조	단말기 보호 대책
	제 14조	정보 처리 시스템 보호 대책
	제 15 조	해킹 등 방지대책
전자금융 감독규정 시행세칙	제 2 조	망분리 적용 예외 (제 2 조의 2)
	별표 7	망분리 대체 정보보호통제



SPAC SYSTEM



서울시 영등포구 양평로 98 M&G타워 4층
대표전화 : 02.6925.4452 / Fax : 02.6925.4453

www.bizet.co.kr

