SDAC

SDAC (Secure Direct Access Control)

직접접근제어시스템

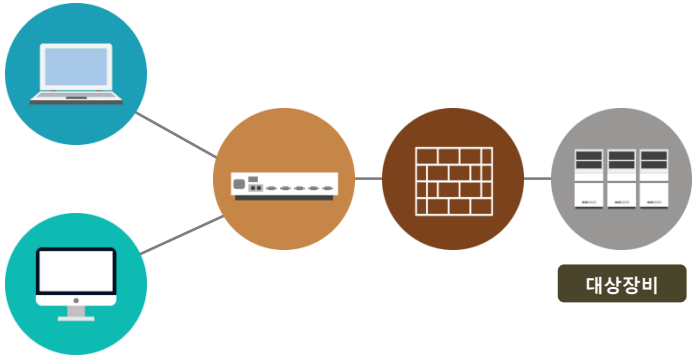
직접접근 단말장비 작업통제 및 감사 솔루션

CONTENTS

작업자PC 와 작업 대상장비와의 End-To-End 접속형태에 대한 접근 통제 (Proxy 역할을 하는 원격접근장비(Gateway)를 통하지 않고 직접 연결)

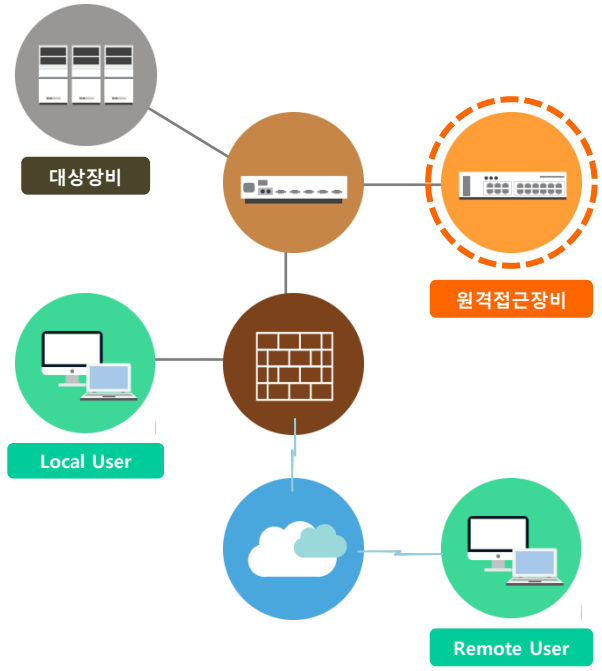
직접접근
(Direct Access)

노트북의 LAN·Serial 포트를 사용하여 대상장비(서버·네트워크·보안·스토리지 장비)에 직접(OffLine) 연결하는 접근방식



노트북·PC에서 네트워크(Online)를 통하여 대상장비(서버·네트워크·보안·스토리지 장비)에 TCP/IP로 접근방식

원격접근
(Remote Access)



원격접근장비(Gateway)를 통하여 대상장비로 접근하는 방식
(콘솔 직접연결 및 우회경로에 대한 보안대책 없음)

대안은 없고 관리는 해야만 하는 전산실 직접 방문 작업 , 사람에 대한 믿음이 보안대책인가요?

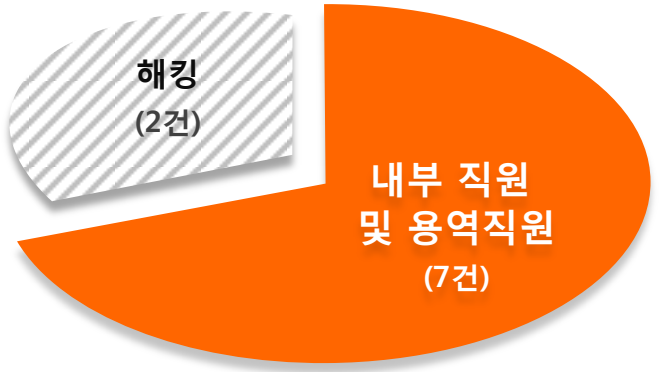
→ 직접접속 작업단말 통제와 접속 대상장비에 대한 통제 보안정책이 있어야 합니다.

가장 큰 보안취약점, 사람

→ 외부 해킹 공격에 의한 정보 유출 사고에 비해 내부자 보안통제 미비로 인한 의도적 중요 정보 유출 현상이 증가 추세

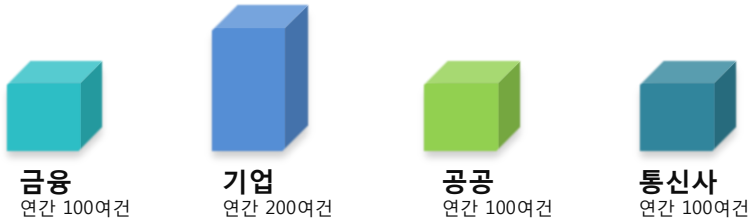
연도별 보안사고 사례

2014년 국내 금융사 정보유출 주체



[인적 요소에 의한 정보 유출이 압도적인 비율]

보안사고 발생 연간 건수



보안 사고 발생 시 민·형사상 손해배상

→ 법적 손해배상에 따른 경제적 손실뿐만 아니라 기업 대외이미지 추락 등 부정적 파급효과 발생

정보보호 규제강화 및 개인정보보호 조치 관련법 및 시행령		
개인정보 보호법	제 03조	개인 정보 보호 원칙
	제 29조	안전 조치 의무
표준 개인 정보 보호지침	제 04조	개인 정보 보호의 원칙
	제 26조	개인 정보의 유출
	제 41조	관리 책임자의 지정
개인정보의 안정성 확보 조치 기준	제 3조	내부 관리 계획의 수립·시행
	제 4조	접근 권한의 권리
	제 5조	비밀번호 관리
	제 6조	접근 통제 시스템 설치 및 운영
	제 7조	개인 정보의 암호화
	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 28조	개인정보의 보호조치
	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 30조	일괄 작업에 대한 통제
	제 32조	내부 사용자 비밀번호 관리

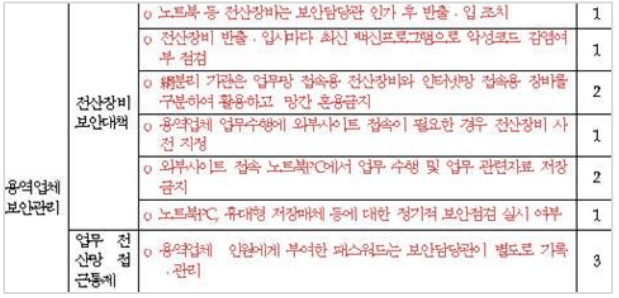
[처벌조항]

법 제 28조 제 1항 제 2호부터 제 5호까지의 조치를 하지 아니하여 이용자의 개인정보를 분실.도난.누출.변조.훼손한 경우 **2년 이하의 징역 또는 1천만 원 이하의 벌금과 1억 원 이하의 과징금 부과** (법 제 28조 제 1항, 제 73조 제 1호, 제 64조 3제 6호)

법 제 28조 제 1항에 따른 기술적.관리적 조치를 하지 않은 경우 **3천만 원 이하의 과태료 부과** (법 제 28조 제 1항, 제 76조 제 1항 제 3호)

[외부인력의 전산실 작업에 대한 운영 지침 내역]

금융위 조치요청 (2014.12.29) :
주요정보통신기반시설 긴급점검 결과 미흡사항 조치 요청

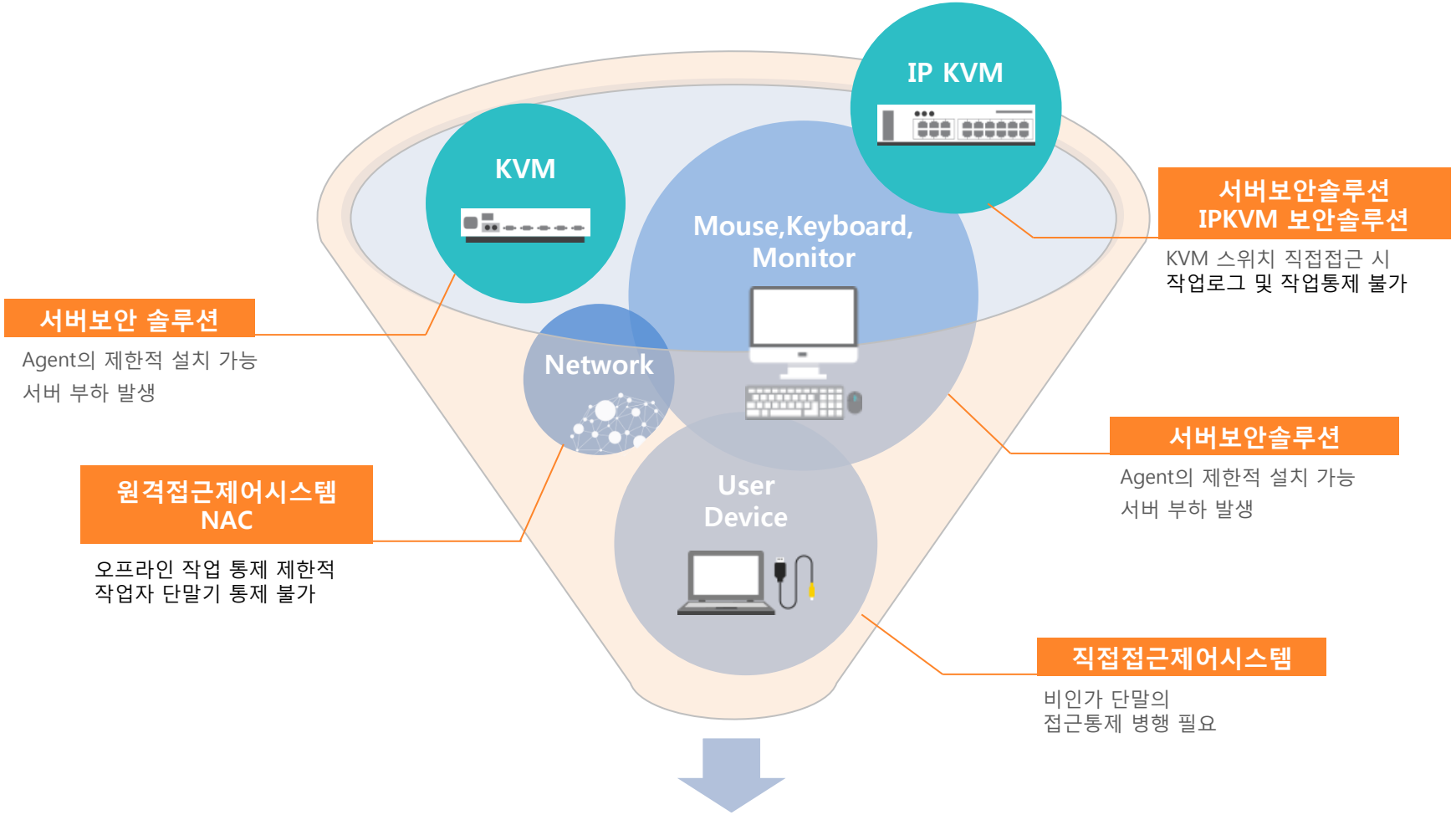


용역업체 보안관리	전산장비 보안대책	○ 노트북 등 전산장비는 보안담당관 인가 후 반출 · 입 조치	1
		○ 전산장비 반출 · 입시마다 최신 백신프로그램으로 악성코드 감염여부 점검	1
		○ 網분리 기관은 업무망 접속용 전산장비와 인터넷망 접속용 장비를 구분하여 활용하고 망간 혼용금지	2
		○ 용역업체 업무수행에 외부사이트 접속이 필요한 경우 전산장비 사전 지정	1
		○ 외부사이트 접속 노트북PC에서 업무 수행 및 업무 관련자료 저장 금지	2
		○ 노트북PC, 휴대형 저장매체 등에 대한 정기적 보안점검 실시 여부	1
	업무 전산망 접근통제	○ 용역업체 인원에게 부여한 패스워드는 보안담당관이 별도로 기록 · 관리	3

행정자치부 고시 제1호 (2014.11.25) :
행정기관 및 공공기관 정보시스템 구축·운영 지침

대상장비 접근방식에 따른 접근차단솔루션 및 한계점

→ 단일 보안솔루션 도입만으로는 모든 접근방식으로부터 대상장비의 접근통제 불가



전산실 출입 후 대상장비 (서버 · 네트워크 · 보안 · 스토리지 · 기타 장비)에 작업 단말기 (Notebook , PC)를 통한 케이블 (Serial , LAN) 직접연결 작업 시 작업이력관리 , 접근통제, 작업환경통제 , 로그수집 및 감사를 목적으로 한 국내 최초의 직접접근제어시스템

→ 보안정책에 따른 작업자 인증, 대상장비 접근제어, 포트 및 매체제어, 명령어·프로그램 통제, 로그 기록 등의 통제 및 감사로그를 수집하는 시스템

접속 및 권한인증

- 2Factor 인증 / 보안 강화 (지문인증)
- 작업단말 고유 식별정보와 지문인증토큰 복합인증 체계
- 직무에 기반한 계정 권한 차등 및 분리

정책기반 접근통제

- 작업승인 된 지정 작업단말로만 작업
- 사용자 별 접근 권한 통제
- 대상장비 별 접근 프로토콜 통제
- 금지 명령어 및 악의적인 프로그램 구동 차단
- 미인가 포트, 매체 사용차단 및 작업시간 지정

로그기록 및 감사

- 디스크 보안파티션 영역에 작업행위 로그 기록
- 보안 파티션 기능을 통한 로그 위·변조 방지
- 모든 행위기반 텍스트 로그 및 Full 동영상 저장
- 카테고리 별 상세 이력과 키워드 중심의 통합 검색

관리서버 작업/정책 및 로그관리

- 직접접근제어시스템의 작업 관리, 작업 등록, 작업 통제정책 수립
- 인적자원, 작업 대상장비, 작업단말의 고유식별번호등록 및 관리
- 작업 별 명령어, 프로그램 통제 및 포트, 매체, 저장장치 사용통제 등의 정책 생성/등록
- 수집된 텍스트 로그 및 동영상 로그 저장 및 조회

지문인증토큰 정책/인증 매체

- 관리자 및 작업자 인증용 장치
- 관리서버에서 승인된 정책 및 접속 대상장비 IP, ID, P/W 저장 후 S-TOKEN 불출, 지정된 작업단말에서만 사용가능
- **S-AGENT**의 최초 로그인 시 **S-TOKEN** 연결 후 지정된 작업단말과 작업자 확인 후 로그인
- 인증 후 **S-TOKEN에** 저장된 보안정책을 작업단말의 보안파티션에 적용

단말 Agent 접근통제 프로그램

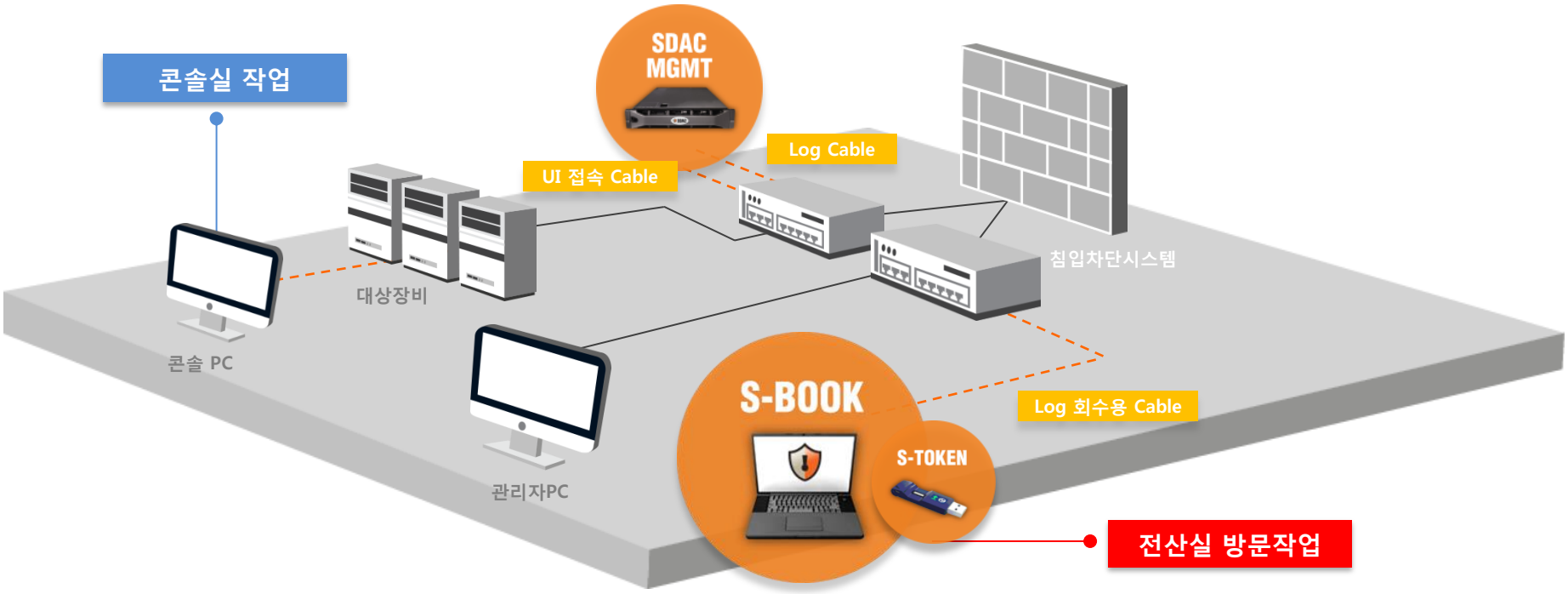
- 지정 작업단말에 설치되는 에이전트 프로그램
- 에이전트 설치 시 윈도우 및 사용자 접근이 차단되는 암호화 보안파티션 생성
- S-TOKEN의 보안정책 Agent에 적용 및 수행
- 작업 대상장비 접속 시 IP, ID, P/W의 자동접속 기능 제공 (bztool)

작업단말 전용작업단말기

- 전산실에 방문하여 대상장비에 대한 직접연결 작업을 위한 전용노트북
- **S-AGENT** 설치 및 Tuning이 완료된 제품으로 관리자 정책에 따른 보안파티션 생성 및 적용
- 관리서버에 고유식별정보 사전 등록

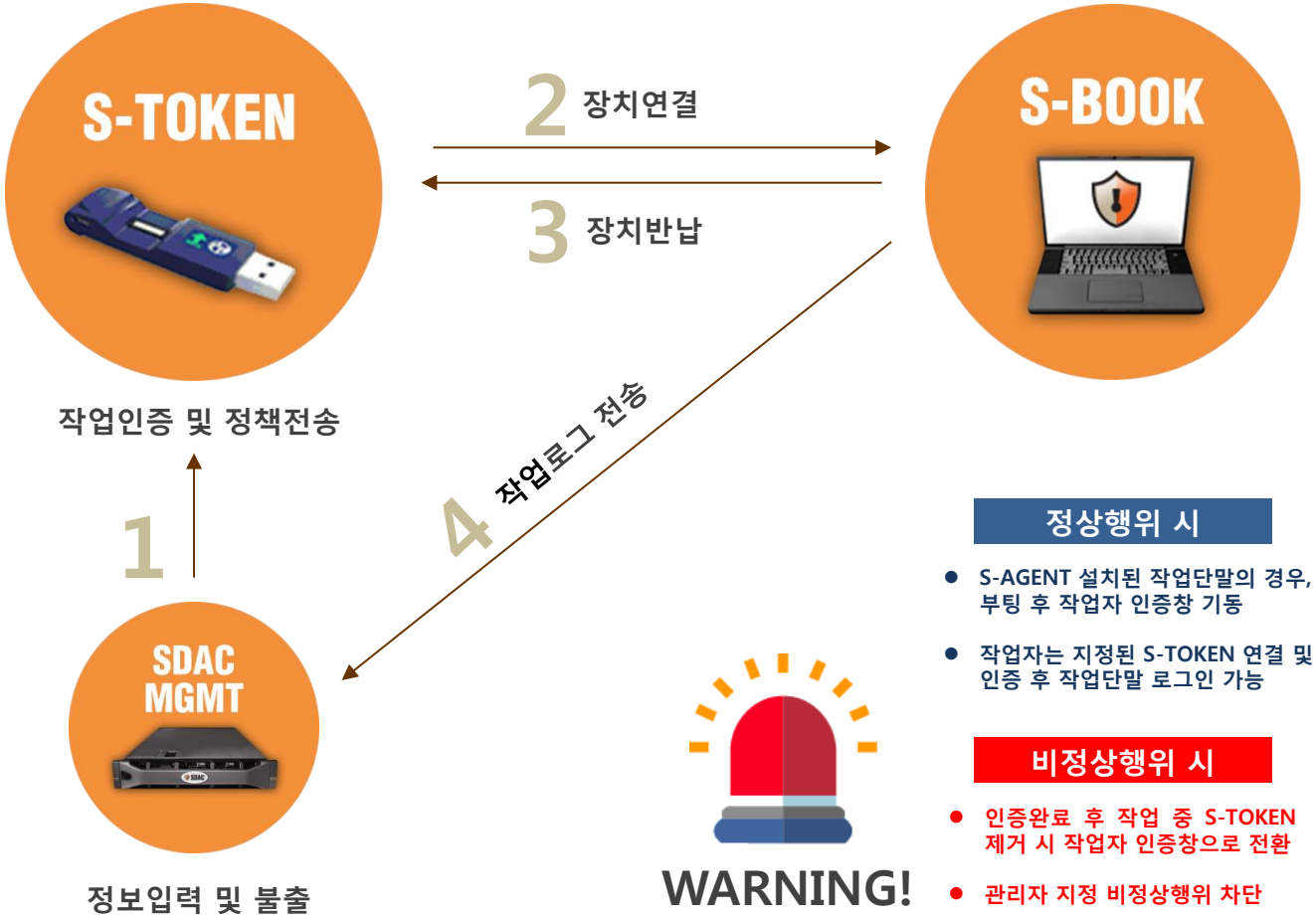
직접접근 작업 통제에 필요한 네트워크 인프라 아키텍처

→ MGMT 관리서버의 네트워크 구성과 작업단말(S-Book) 의 로그 회수용 네트워크 구성으로 분리되며, MGMT는 외부망에서 접근 불가능한 내부망에 위치



2 FACTOR 작업인증

→ 작업단말(S-Book)을 사용하기 위해서는 OS(Windows7)의 Administrator 계정의 ID, PW를 입력 후 S-TOKEN내 저장된 작업자/관리자 지문 일치 시 사용가능



로그인 및 화면 잠금

→ S-Book 및 S-PC는 최초 작업자 또는 관리자에 대한 인증 및 권한 확인을 수행하며, 로그인 및 화면 잠금은 관리자 모드와 사용자 모드로 구분

S-AGENT 로그인창

사용자 인증

- **S-TOKEN**을 연결하고 불출 시 등록된 작업자 지문 인증수행
- **S-TOKEN**에 등록된 작업 PC 정보와 연결 작업단말 정보 일치 여부 확인

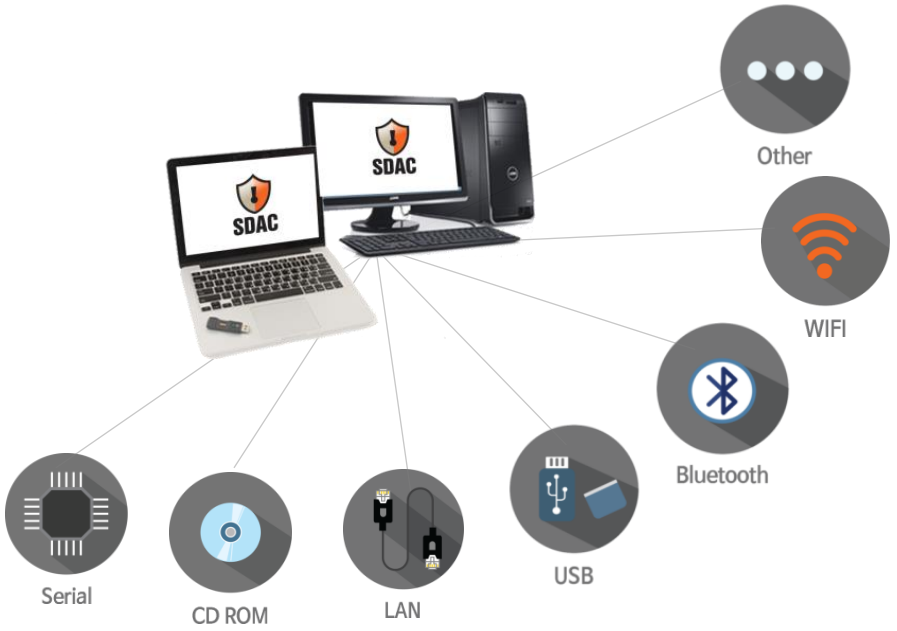
관리자인증

- 관리자에 의해 지정된 관리자 인증 수행 후 로그인
- 작업자 작업완료 후 저장된 로그를 MGMT로 회수

작업통제 및 정책관리

→ 관리자에 의해 승인된 물리적·논리적 환경 내에서만 작업이 가능하도록 통제하며, 그로 인한 자료 무단복제·반출 등의 위법 행위 원천 차단

물리적 통제



논리적 통제

대상장비 접속 통제 및 접속정보 보호

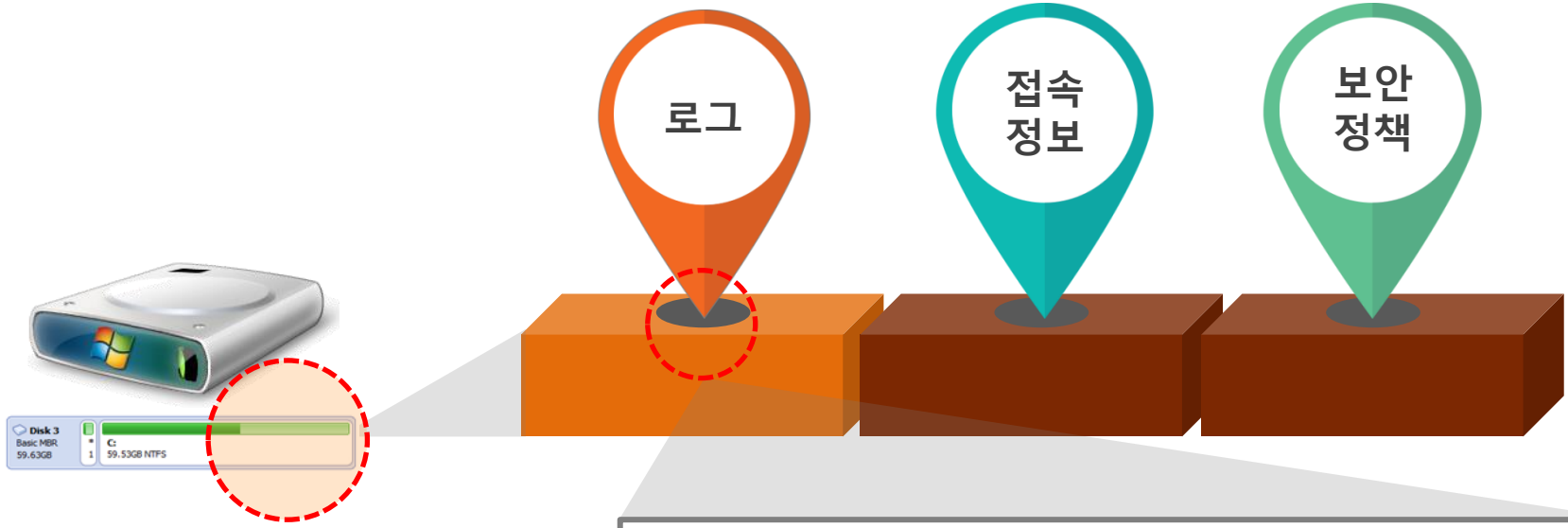
→ 작업자에게 접근 대상장비 자동접속 기능 및 접속정보(IP, ID, PW) 노출 차단 기능의 지정 승인된 대상장비 접속 UI 제공 (Bztool - 원클릭 자동 접속 App)

대상장비 접근정보 노출 없음

- 지정 대상장비만 접근가능
- 접근가능 목록 표시
- 전용 접속 Tool을 통한 접속

로그추출 및 위·변조 방지

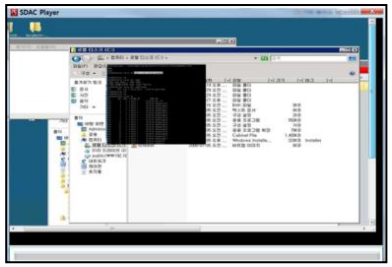
→ 최초 로그인부터 작업종료 시점까지의 작업내역에 대한 텍스트·동영상 로그를 보안파티션 영역에 저장하여 위·변조 방지에 따른 무결성 보장



보안 파티션

- **S-AGENT** 설치 시 하드디스크에 암호화 파티션 생성
- 드라이브로 지정될 수 없으며 OS 미 할당 파티션 인식
- 보안정책/접속정보/로그 등 정보저장
- 추출 된 로그 보안파티션 보관 후 MGMT로 전송
- 디스크 용량 및 로그추출 정책에 따라 지정
- 작업로그 지정 된 작업번호 기반 관리

동영상 로그



텍스트 로그

SDAC | 전산실 직접방문 작업통제 운영

작업자 작업신청 내역에 대한 관리자 작업승인 시 수립된 보안정책에 의거 직접 방문작업 통제

→ 직접방문 작업 전용 노트북(S-Book)을 통한 작업환경 통제 및 로그추출

1 신청

작업신청
대상장비/작업목적/
작업시간/작업환경 등

2 승인

장치 인계
S-Token, S-Book

전산실 출입
지정된 작업 수행

3 회수

장치 반납
S-Token, S-Book

로그 회수
작업 이벤트 및
동영상

[구축사례 : 정부통합전산센터 금융결제원 한국기계연구원 **]**

콘솔실 PC단말기 로부터 대상장비 접근통제 및 작업환경 통제

→ S-TOKEN 저장 정책에 따른 장비접속 및 보안통제 수행 후 로그 저장

관리자 작업자

1 신청

작업신청
대상장비/작업목적/
작업시간/작업환경 등

SDAC MGMT

2 승인

장치 인계
S-Token

콘솔실 출입
지정된 작업 수행

통제 및 로그

SERVER
NETWORK
SECURITY
STORAGE
ETC

3 회수

장치 반납
S-Token

로그 회수
작업 이벤트 및
동영상

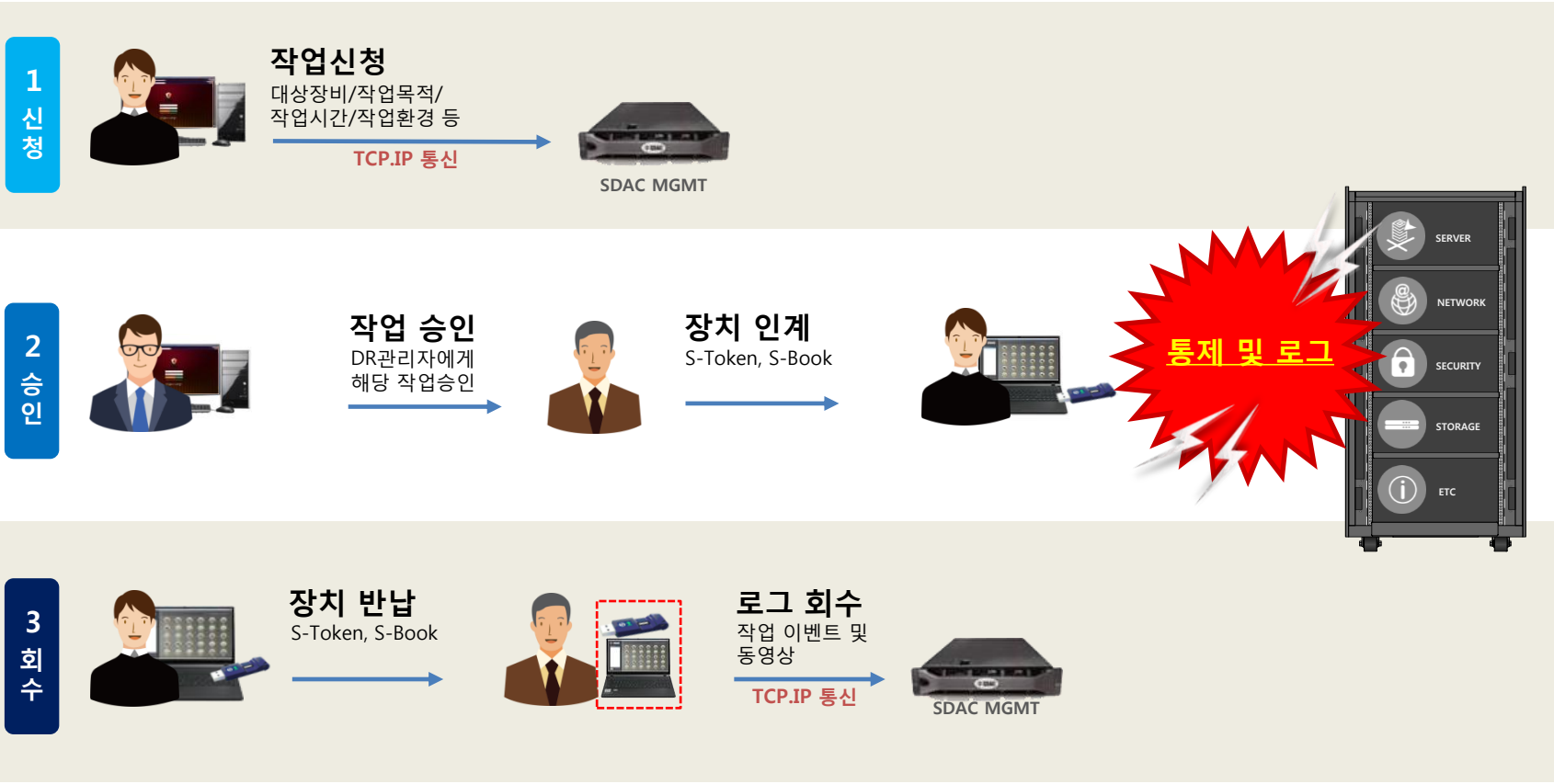
SDAC MGMT

[구축사례 : 정부통합전산센터 금융결제원 한국기계연구원 **]**

SDAC | 본사 및 원격지 (DR/지점) 센터 운영

본사 SDAC 관리서버를 통한 본사 및 원격지센터 대상장비 직접접근 작업통제 운영

→ 본사 관리자는 본사·원격지 대상장비에 대한 등록 및 작업 승인 권한이 있으며, 원격지 운영자는 장치(S-Book, S-Token)인계 권한만 부여

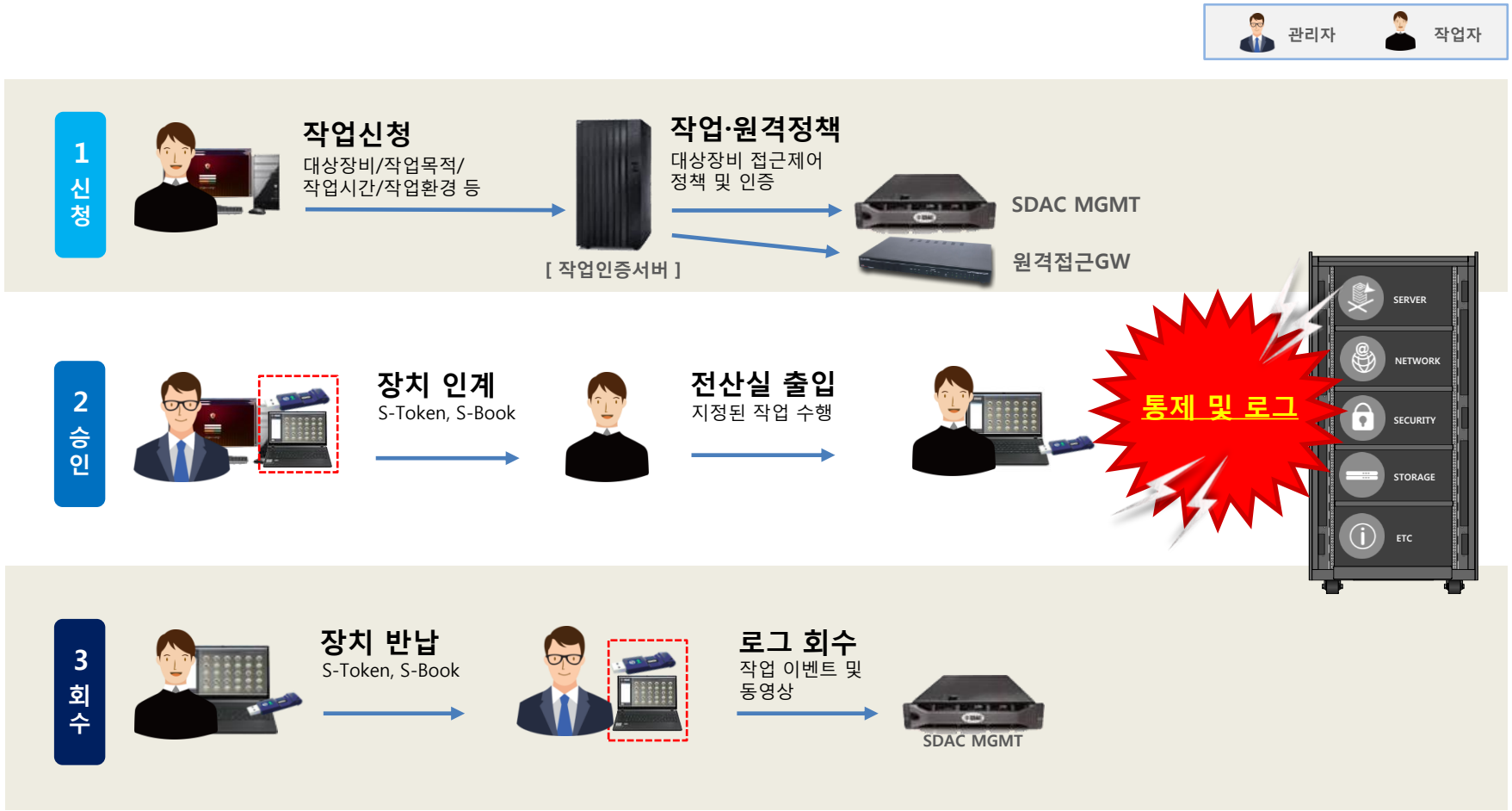


[구축사례 : 금융감독원]

SDAC | 직접접근제어와 원격접근제어의 운영

기존 원격접근제어 정책서버와의 병행 운영

→ 작업인증서버를 통한 작업자 작업신청 분류에 따른 직접·원격접근제어시스템으로 수립정책 적용 (연동)



[구축사례 : 정부통합전산센터 **]**

기존 접근제어시스템이 해결하지 못한 직접방문 작업에 대한 보안대책 구비

→ 내부자원의 보호 및 안정적인 시스템 인프라 운영을 비롯한 실제 도입을 통해 실현된 효과 분석

	AS-IS	TO-BE
보안 측면	• 작업자에게 대상장비 접속정보(ID/PW/IP) 노출 • 관리자 동행 불구 시 작업 감시/통제 어려움 • 위험 명령어 입력 및 프로그램 실행 차단 불가 • 정보 유출 및 복제에 대한 위험요소 존재	• 작업자에게 암호노출 없이 대상장비 접근 가능 • 허용된 장비에만 접근 가능 (임의 타장비 접속불가) • 금지 명령어·프로그램 실행 사전 차단 • 작업단말 매체 및 드라이브 통제로 위험요소 제거
관리 측면	• 전산실 방문 작업자의 수기 방문 등록 및 처리 • 작업시간 지연 시에 추후 담당자 연락 • 상호 신뢰 인간관계에 의존하여 보안의식 저하 • 작업행위 부인 시에 분석절차 및 시간 발생	• 통합적인 전산실 출입관리 분석 및 작업내역 분석 • 작업시간 통제로 지연시 발생하는 기회손실 감소 • 관리감독 강화로 업무의 효율화 및 보안의식제고 • 텍스트 및 동영상 로그관리로 작업자 부인방지
운영 측면	• 장비로그 외 작업행위에 대한 상세 로그 부족 • 악의적인 작업행위 통제 미흡으로 리스크존재 • 작업자 실수로 인한 장비 장애 발생 가능성 내포 • 사람에 대한 통제 수행, 장비 및 행위는 미통제	• 보안사고 시 로그기반 신속한 원인 추적 및 대응 • 사고예방으로 대외신뢰도 및 경쟁력 강화 • Human Error 발생 방지에 따른 장애발생 최소화 • 작업목적에 따른 작업환경 통제 및 승인

	SDAC MGMT	S-TOKEN	S-BOOK
			
Operation System	CentOS	—	Windows 7 Professional 32Bit
CPU (Core/Ghz)	4 Core 2.4Ghz 이상	32Bit ARM Core	Intel® Core™ i3 이상
Main Memory	8GB	—	4GB DDR3 이상
Storage	1TB * 2 이상	—	500GB 이상
Network Interface	100 / 1000 * 4	—	100 / 1000 * 1 UTP
Power Supply	300W Redundant	—	—
DBMS	MariaDB	—	—
etc		조달청 BIO 보안토큰 제품지정	

소프트웨어품질인증서

Certificate of Software Quality

상호또는성명 : 비젯(206-8-88597)
BIZET Inc.

소프트웨어의명칭 : 에스닥 엔터프라이즈 v1.0
SDAC Enterprise v1.0

인증번호 : 14-0274

제조자및제조국가 : 비젯/대한민국
BIZET Inc./Republic of Korea

인증년월일 : 2014년(Year) 11월(Month) 3일(Day)

기타 :
Others

위 소프트웨어는 소프트웨어산업진흥법 제13조에 의하여 품질이 인증되었음을 증명합니다.

We testify that the quality of foregoing software has been certified under the Software Industry Promotion Act.

2014 년(Year) 11 월(Month) 3 일(Day)

TTA 한국정보통신기술협회장
CEO & President
Telecommunications Technology Association

Certificate of Software Quality

Trade Name or Applicant : BIZET Inc.(206-81-88597)

Name of Software : SDAC Enterprise v1.0

Certification No. : 14-0274

Manufacturer and Nation : BIZET Inc./Republic of Korea

Date of Certification : 2014. 11. 3

Others :

We testify that the quality of foregoing software has been certified under the Software Industry Promotion Act.

2014. 11. 3

TTA CEO & President
Telecommunications Technology Association

SDAC

THANK FOR YOUR ATTENTION

감사합니다

▪ 총판사 : SMPRO | 대표전화 : 02-6454-5100 | 팩스 : 02-461-8159 | 홈페이지 : www.sm-pro.co.kr | 이메일 : sales@sm-pro.co.kr
| 주소 : 서울특별시 강남구 테헤란로 427, SBI타워빌딩 19층

▪ 개발사 : 주식회사 비 젯 Differentiated Security Partner | 대표전화 : 02-6925-4452 | 팩스 : 02-6925-4453 | 홈페이지 : www.bizet.co.kr | 이메일 : clrchr@bizet.co.kr
| 주소 : 서울특별시 영등포구 양평로 98 M&G타워 4층