Seoul Design Foundation

" 청렴은 선택이 아니라 필수입니다 "

17년 정보인프라 취약점 보완을 위한 장비 및 솔루션 구매 계획

2017. 10. 26.

문서번호	전산정보팀-1499
결재일자	2017.10.27.
공개여부	비공개(5,7)
방침번호	대표이사방침 제(4313)호

선임	전산정보팀장	운영본부장	DDP경영단장	대표이사
10/26 장기영	10/27 노태화	10/27 강문석	10/27 유석윤	**10/27** 이근
협 조			선임	책임
			10/26 최지연	10/27 정은석

추진근거	- 17~18년 서울디자인재단 정보시스템 통합 운영 및 유지관리 사업 착수보고회 개최 결과보고(대표이사방침 제3920호, 2017.09.25.)		
대 내 외 협력현황	부서(단체)명	협의내용	협의결과
	기획경영팀	소요예산	17년 예산안에 따름
	경영지원팀	계약수행	나라장터 계약 진행
사 업 비	- 소요예산 : 총액 237,934,400원 . 예산과목1 : 재단, 일반관리비, 운영경비, 운영경비, 수선유지비(정보시스템 유지보수) . 예산과목2 : DDP, 기반운영사업, DDP정보화사업, DDP정보서비스운영관리, 자산취득비 . 예산과목3 : DDP, 기반운영사업, DDP일반관리비, 운영경비, 지급수수료		

서울디자인재단 (전산정보팀)

사전 검토항목

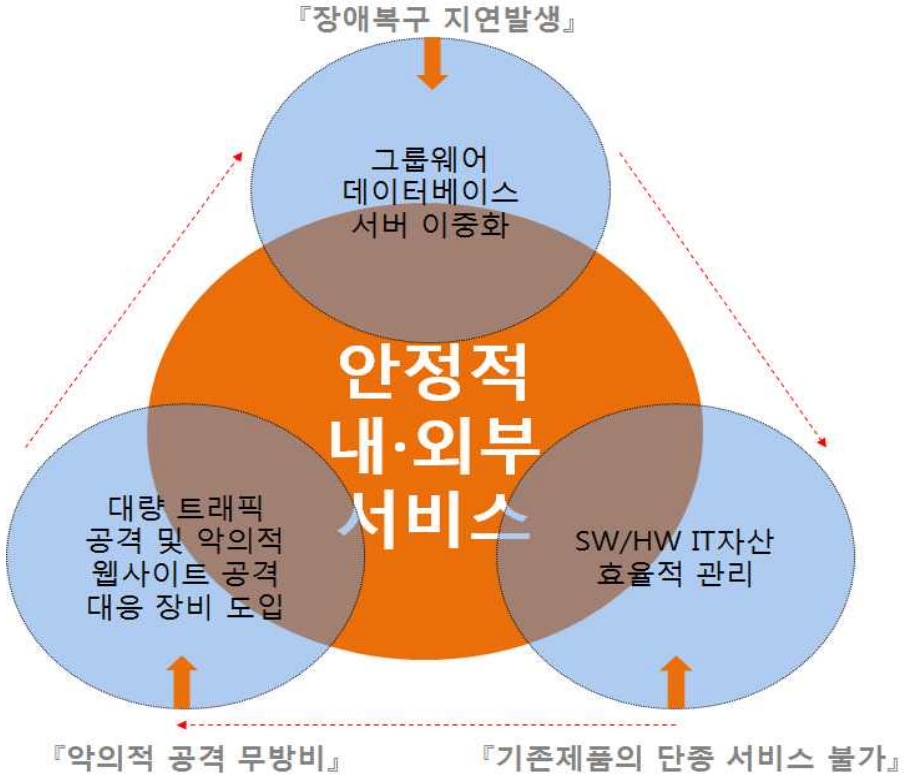
※ 해당사항이 없을 경우 '무 ✔' 표시하시기 바랍니다.

검 토 항 목	검토여부 '✔' 표시					
시 민 참 여 고 려 사 항	시 민 :	유 □ ( )	무 ✔			
	이 해 당 사 자 :	유 □ ( )	무 ✔			
	전 문 가 :	유 □ ( )	무 ✔			
	옴 브 즈 만 :	유 □ ( )	무 ✔			
법령및기타 고 려 사 항	법 령 규 정 :	교통 □	환경 □	재해 □	기타 □	무 ✔
	기 타 :	고용효과 □	노동인지 □	균형인지 □		
		취약계층 □	성인지 □	장애인 □	디자인 □	
		갈등발생 가능성 □	유지관리 비용 □	무 ✔		
타 자 원 의 활 용	중 앙 부 처 :	유 □ ( )	무 ✔			
	민 간 단 체 :	유 □ ( )	무 ✔			
	기 업 :	유 □ ( )	무 ✔			
관 계 기 관 및 단체 협의	관 계 기 관 :	유 □ ( )	무 ✔			
	관 련 단 체 :	유 □ ( )	무 ✔			

17년 정보인프라 취약점 보완을 위한 장비 및 솔루션 구매 계획

1차 정보화전략계획(ISP)의 정보인프라 수준 및 취약점 분석 결과에 대한 대응으로 서버, 보안장비, IT자산관리솔루션을 구매하고자 함.

1. 개 요



- 사 업 명 : 17년 정보인프라 취약점 보완을 위한 장비 및 솔루션 구매 계획
- 사업내용 : 정보인프라 취약점을 보완하기 위한 서버 이중화 및 보안장비, 관리 솔루션 구매 설치
- 사업대상 : 그룹웨어(전자결재) 데이타베이스 서버 1식, 네트워크 보안장비 4식, IT자산관리솔루션 1식
- 구매비용 : 237,934,400원
- 사업기간 : 2017.11.20 ~ 12.31

※ 구매, 설치, 테스트 등에 따라 일정 변동 가능

■ 사업 배경

□ 정보인프라 전반적 취약점 진단에서 업무비중과 민감도가 가장 높은 전자결재 데이터베이스 장애 발생 시 복구 전까지 업무마비

□ 외부의 악의적인 공격 시 중요 업무자산을 보호하기 위한 안전장치 부재

■ 사업 목적

□ 그룹웨어(전자결재) 데이터베이스 장애 취약점 개선

□ 웹 해킹 및 대량 트래픽공격 대응

□ 소프트웨어 라이선스 및 하드웨어 자산 관리 효율성 증대

2. 취약점 및 대응 방안

■ 그룹웨어(전자결재) 서버

□ 취약점

- 아키텍쳐 구성진단을 통해 도출된 이중화 구성의 취약으로 재단은 단일서버 구성으로 악의적 공격 또는 장애 발생시 전자결재업무 및 정보공유 마비로 정상화 전 서비스 지연 발생

□ 대응방안

- 중요정보가 저장되는 데이터베이스 서버를 추가 구매/설치하여 Active- Standby[1], Active-Active[2] 등의 기법을 이용해서 이중화를 구성하여 장애 대응

1) Active- Standby : 한 쪽 장애시 나머지 한 쪽으로 서비스 자동 이관
2) Active-Active : 동시서비스 진행으로 한 쪽 장애발생시에도 무중단 서비스 가능

■ DDOS[3] 보안장비 미비

□ 취약점

- 다수의 공격자를 분산 배치하여 동시에 "서비스 거부 공격"을 진행 시 전체 네트워크 셧 다운 발생

□ 대응방안

- 특정 임계치 이상의 네트워크 트래픽 발생 시 추가로 들어오는 세션을 끊어 네트워크 성능을 안정적 운영

■ 웹 방화벽[4] 부재

□ 취약점

- 웹을 통해 이루어지는 외부의 침입이나 웹 공격 시 재단 및 DDP 홈페이지 등 외부 민감도가 높은 웹서비스에 큰 장애 발생

□ 대응방안

- 웹을 통해 이루어지는 외부의 침입이나 웹 공격을 탐지하고 공격을 사전에 차단, 방지할 뿐만 아니라 웹 보안 취약점을 외부에 노출되지 않도록 보완하여 지속적인 대시민 웹서비스

■ IT자산관리솔루션 노후화

□ 취약점

- 現시스템의 제품 단종 및 서비스 중단, 인력증가, 단기인력 유출입의 불확실성으로 PC, SW, IP 등 재단 IT자산에 대한 관리 부재로 중복 구매 및 배분 등으로 비용낭비, 관리의 어려움

□ 대응방안

- IT자산관리솔루션을 고도화하여 SW/HW 및 실물(고정)자산에 대한 정보를 정확히 파악하고 통제 및 관리하여 구매계획부터 통제관리, 자산의 매각 또는 폐기에 관련된 모든 과정을 관리하여 자산 사용에 대한 효율적인 관리

---

3) DDOS : 수십 대에서 많게는 수백만 대의 PC를 원격 조종해 특정 웹사이트에 동시에 접속시킴으로써 단시간 내에 과부하를 일으키는 해킹 공격

4) 웹방화벽 : 웹서비스 보안 솔루션으로 개인정보가 웹 게시판에 게시되거나 개인 정보가 포함된 파일 등이 웹을 통해 업로드 및 다운로드 되는 경우에 대해서 탐지하는 등 각종 웹 해킹에 대응함

3. 도입 개요

■ 그룹웨어 서버 추가 도입

□ 도입 개요

- 목　　적 : 그룹웨어 운영 안정성 강화
- 현　　황 : 1식 운영 중
- 도입 수량 : 서버 및 메모리 각 1식
- 도입 방법 : 나라장터 물품 발주

□ 소요 예산(안) : 54,343,300원

■ 보안 장비 신규 도입

□ DDOS 보안 장비 도입 개요

- 목　　적 : DDOS 공격 대응으로 보안 위협 사전 차단
- 현　　황 : 장비 미도입
- 도입 수량 : 2식 (이중화)
- 도입 방법 : 나라장터 물품 발주

□ 웹 방화벽 장비 도입 개요

- 목　　적 : 웹 해킹에 대한 대응 및 예방으로 운영 안정화
- 현　　황 : 장비 미도입
- 도입 수량 : 웹방화벽 2식(이중화) 및 로그서버 1식
- 도입 방법 : 나라장터 물품 발주

□ 소요 예산(안) : 174,196,000원

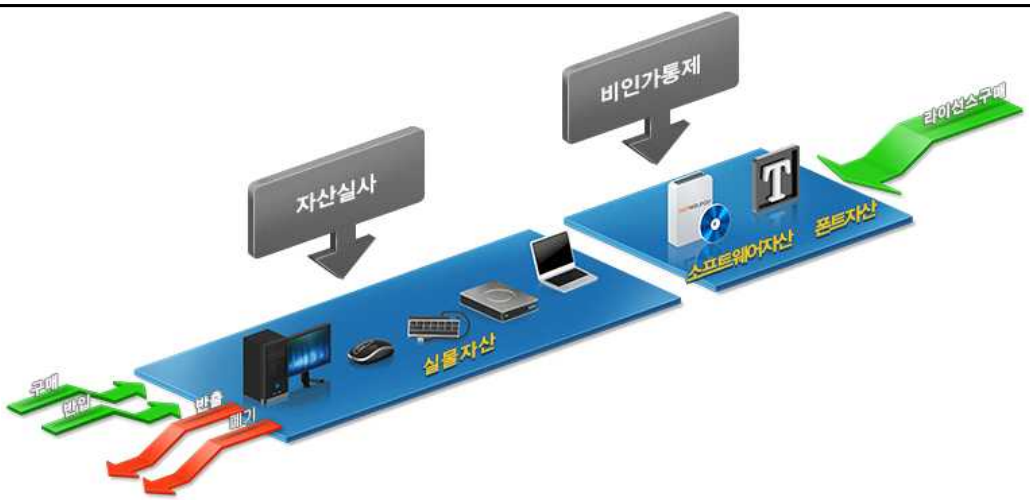
DDOS 보안 장비	웹 방화벽
	

■ IT자산관리솔루션 신규 도입

□ 도입 개요

- 목　　적 : IT자산관리 운영 안정화 및 효율화
- 현　　황 : 유지보수 불가능한 솔루션 운영중
- 도입 수량 : 300 USER
- 도입 예산 : 13,480,500원
- 도입 방법 : 나라장터종합쇼핑몰 구매

□ 소요 예산(안) : 13,480,500원



4. 도입 상세

■ 그룹웨어(전자결재) 서버

□ 도입 목적

- DB서버 이중화 구성을 통한 전자문서 관리 안정성 강화

- 장비 불량 발생 시 대체 서버 자동 지원으로 무중단 서비스 제공

□ 도입 배경

- 그룹웨어 업무 의존도 향상

- 전자문서 데이터 증가로 인한 관리 안정화 필요

□ 도입 효과

- 이중화 구성을 통한 데이터 관리로 업무시스템 신뢰도 강화

□ 도입 예산(안) : 50,257,900원(VAT포함)

□ 도입 장비 규격

구 분	품 명	규 격	수 량
그룹웨어 DB서버	HP-RX2800	- HP rx2800 i4 X2.53GHz*1P - 8Core - 32GB Memory - 300GB *2 Disk - MC/SG	1
메모리	HP-RX2800 i4 ADDON	- RAM 16GB	1

■ DDOS 보안

□ 도입 목적

- 네트워크 보안 강화 및 정보시스템 안정성 향상
- 실시간 과다 트래픽 탐지 및 심층 분석 기능 활용
- 비정상 패킷 및 세션 차단 기능 활용

□ 도입 배경

- DDOS 보안 장비 미운영

※ 참고 : '16년 서울디자인재단 정보시스템 통합 운영 및 유지관리 사업 계약 변경(안)(Ddos 제외) (대표이사방침 제1975호, 2017.05.23.)

- DDOS 공격 대응 불가로 정보시스템 운영 안정성 저하

□ 도입 효과

- 네트워크 안정성 향상으로 무중단 업무시스템 신뢰성 강화

□ 도입 예산(안) : 99,000,000원(VAT포함)

□ 도입 장비 규격

구 분	품 명	규 격	수 량
DDOS 보안 장비	SNIPER ONE-d2000	* S/W : Sniper Version V3.0 ONE-d 2000 - TCP,UDP,ICMP,Frag 등 각종 DDoS 방어 - Triple'S 엔진을 통한 정상트래픽 대역폭 보장 - In Line 모드 지원 및 Bypass 지원 - 네트워크 트래픽 2~4Gbps 처리 * H/W 제원 - CPU : 2.4GHz 8Core * 1 - RAM : 32GB / SSD : 64GB / HDD : 2TB - NIC : 1G *4port (max. 8port)	2

■ 웹 방화벽 보안

□ 도입 목적

- 대표 홈페이지 데이터 등 중요 자원 관리 안정성 향상

- 웹서비스 보안 강화 및 해킹 공격 대응 능력 향상

- 로그서버 도입으로 이상 징후 발견 및 사전 대응 가능

□ 도입 배경

- 웹방화벽 보안 장비 미운영

- 다양한 웹 해킹 공격 대응 불가로 웹 데이터 관리 안정성 저하

□ 도입 효과

- 웹 서비스 운영 안정성 향상으로 중요 자원 관리 신뢰성 강화

□ 도입 예산(안) : 75,196,000원(VAT포함)

□ 도입 장비 규격

구 분	품 명	규 격	수 량
웹방화벽 장비	WEBFRONT-K1600	- Port : 8 * 1G Fiber port, 8 * 1G - 동시 세션수 : 1,200,000 - SSD / HDD : 160GB / 1TB - 메모리 : 4GB - Throughput : 600Mbps - 10000TPS SSL 카드	2
	AV2 Server (로그 서버)	- CPU : Intel Quad-Core Xeon 2.x GHz - RAM : 2GB - HDD : 500GB (SATA-II)	1

■ IT자산관리솔루션

□ 도입 목적

- 소프트웨어 라이선스 및 하드웨어 관리 효율성 향상

- PC 보안 업데이트 자동화 등 전산 보안 관리 강화

□ 도입 배경

- 운영중인 솔루션 단종으로 유지보수 불가

- 인사정보 연동 미지원으로 관리 정보 현행 자동화 불가능

□ 도입 효과

- 인사 정보 연동으로 IT자산관리 현행화 가능

- PC 보안 자동 업데이트로 전산 보안 관리 강화

- 소프트웨어 라이선스 관리 전산화(체계화)

□ 도입 예산(안) : 13,480,500원(VAT포함)

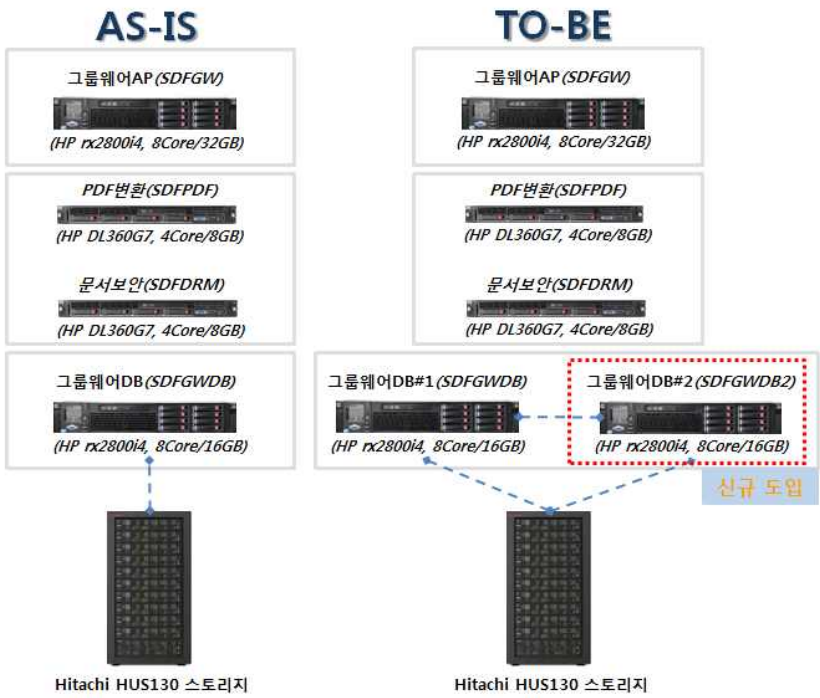
□ 도입 장비 규격

구 분	품 명	규 격	수 량
IT자산관리 솔루션	넷헬퍼	IZEX NetHelper V7.5 Upgrade (Client)	300

5. 시스템 구성 방안

■ 그룹웨어(전자결재) 서버

□ 시스템 구성



□ 작업방안

구 분	수행 업무	작업 시간	비 고
그룹웨어 DB서버 구성작업('17년 11월 30일(목) ~ 12월 05일(화))			
서버 H/W 설치	- 장비 반입 1. 장비 DDP ICT센터 Rack Mount 설치 2. 전원연결 및 공급	10:30 ~ (0.5h)	-

운영체제 재구성	- 운영체제 재설치 1. HP-UX B.11.31 OS 재설치 2. 번들패치 설치	11:00 ~ (1.0 h)	
네트워크 연결	- 네트워크 연결 1. 그룹웨어 용도 IP Address 할당 2. 네트워크 정상 테스트	13:00 ~ (0.5 h)	
스토리지 연결 SAN 구성	- 스토리지 연결용 SAN 구성 1. SAN 케이블 포설 2. SAN Port 할당 3. 신규서버 SAN Port Zoning	13:30 ~ (1.0 h)	

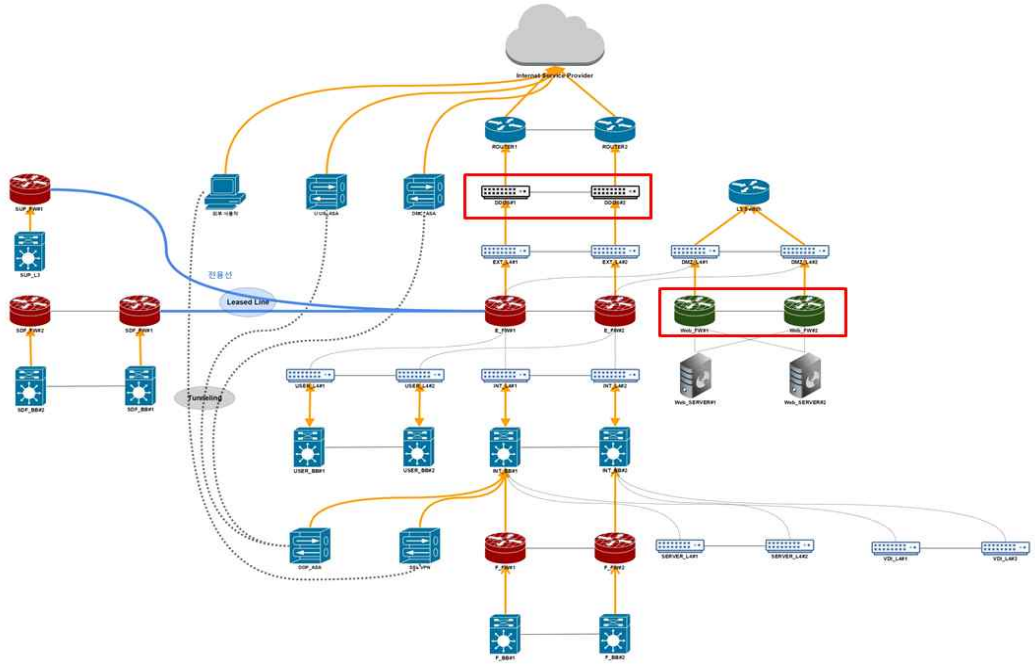
※ 작업 계획은 변동될 수 있음

구 분	수행 업무	작업 시간	비 고
스토리지 할당 작업('17년 12월 06일(수))			
스토리지 연결 SAN 구성	- 스토리지 연결용 SAN 구성 1. SAN 케이블 포설 2. SAN Port 할당 3. 신규서버 SAN Port Zoning	10:30 ~ (0.5h)	-
스토리지 용량 할당	- 스토리지 LUN Assign 1. 히다찌 스토리지 LUN 할당 2. 신규서버 할당 LUN 확인	13:30 ~ (1.0 h)	

※ 작업 계획은 변동될 수 있음

■ DDOS 및 웹 방화벽 보안

□ 시스템 구성



□ 작업방안

구 분	수행 업무	작업 시간	비 고
DDOS 구성작업(2017.11.20.~ 2017.11.27.)			
Wins DDoS Network config 구성	- Wins DDoS 사전 config 1. inline mode Network config 구성 2. 보호대상 시스템(서버) 및 기본 정책 config	00:00 ~ (0.5h)	-
상하단 장비 케이블 구성	- 물리적 구성 1. 상하단 장비 인터페이스 확인	00:30 ~ (0.5 h)	패치코드 준비
Standby DDoS 마운트 및 절체	- Standby DDoS 장비 마운트 및 절체 1. 장비 마운트 2. 케이블 절체 3. Active 케이블 단절후 정상 통신 확인 -> tcpdump, 로그, 서비스 테스트	01:00 ~ (0.5 h)	Active-Active 구성일 경우 3항 생략후 정상 통신 확인
Active DDoS 마운트 및 절체	- Active DDoS 장비 마운트 및 절체 1. 장비 마운트 2. 케이블 절체 3. Standby 케이블 단절후 정상 통신 확인 -> tcpdump, 로그, 서비스 테스트	01:30 ~ (0.5 h)	Active-Active 구성일 경우 3항 생략후 정상 통신 확인
모니터링	- 서비스 테스트 외 정상 통신 확인 1. 서비스 테스트 및 정상 통신 확인 2. DDoS 탐지모드 적용 및 로그 확인	02:00 ~ (0.5 h)	탐지모드 적용

Failover test	- 이중화 failover test 1. 상하단 케이블 절체로 failover test 2. LLCF 동작 확인	02:30 ~ (0.5 h)	
안정화	*- 보호대상장비 DDoS 탐지모드 모니터링* 1. 일정기간 보호대상장비 모니터링 및 로그수집 2. 수집로그 분석 및 차단 정책 적용	-	설치 완료후 약 7일 이후

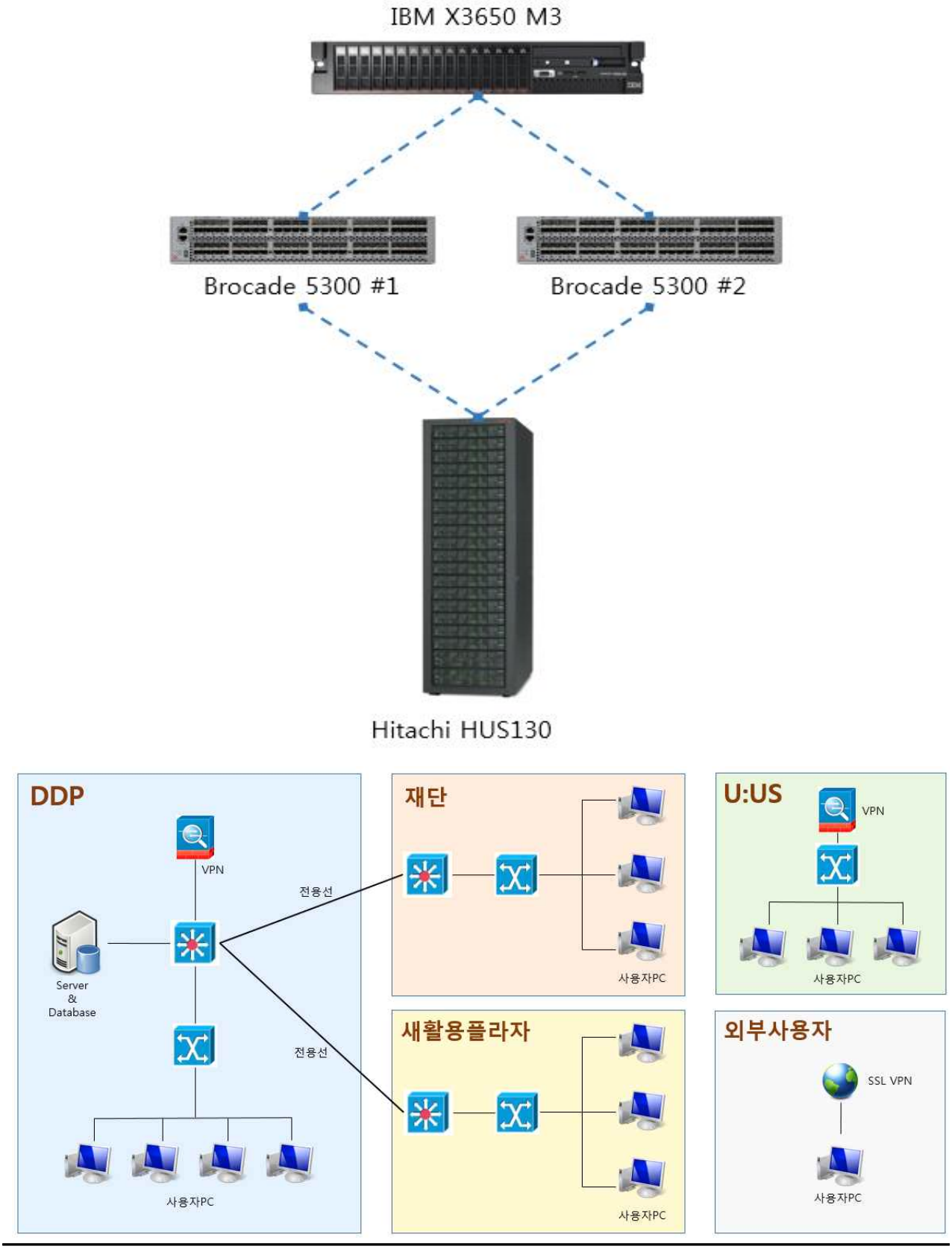
※ 작업 계획은 변동될 수 있음

구 분	수행 업무	작업 시간	비 고
웹방화벽(WAF) 구성작업(2017.11.28.~ 2017.12.05.)			
웹방화벽Network config 구성	- WAF 사전 config 1. inline mode Network config 구성 (현장 구성에 따라 routing mode 구성) 2. 보호대상 Application config -> URL, IP 등 3. Log Analyzer 구성	00:00 ~ (0.5h)	-
상하단 장비 케이블 구성	- 물리적 구성 1. 상하단 장비 인터페이스 확인 2. 물리적 케이블 구성 -> Log Anaylzer 케이블 포설	00:30 ~ (0.5 h)	패치코드 준비
Standby WAF 마운트 및 절체	- Standby WAF 장비 마운트 및 절체 1. 장비 마운트 2. 케이블 절체 3. Active 케이블 단절후 정상 통신 확인 -> tcpdump, 로그, 서비스 테스트	01:00 ~ (0.5 h)	Active-Active 구성일 경우 3항 생략후 정상 통신 확인
Active WAF 마운트 및 절체	- Active WAF 장비 마운트 및 절체 1. 장비 마운트 2. 케이블 절체 3. Standby 케이블 단절후 정상 통신 확인 -> tcpdump, 로그, 서비스 테스트	01:30 ~ (0.5 h)	Active-Active 구성일 경우 3항 생략후 정상 통신 확인
Log Analyzer 마운트	- Log Analyzer 마운트 및 케이블 절체 1. 장비 마운트 2. 케이블 절체 3. WAF 연동 및 로그 수신 확인	02:00 ~ (0.5 h)	
모니터링	- 서비스 테스트 외 정상 통신 확인 1. 서비스 테스트 및 정상 통신 확인 2. 웹application 탐지모드 적용 및 로그 확인	02:30 ~ (0.5 h)	탐지모드 적용
Failover test	- 이중화 failover test 1. 상하단 케이블 절체로 failover test 2. LLCF 동작 확인	03:00 ~ (0.5 h)	라우팅 모드일 경우 3항 생략후 HA Test
안정화	*- 보호대상Application탐지모드 모니터링* 1. 일정기간 보호대상Application 모니터링 및 로그수집 2. 수집로그 분석 및 차단 정책 적용	-	설치 완료후 약 7일 이후

※ 작업 계획은 변동될 수 있음

■ IT자산관리솔루션

□ 시스템 구성



□ 작업방안

구 분	수행 업무	작업 시간	비고
통합자산관리 서버 구성작업 (2017.11.28.)			
서버 재구성	*- Windows Server 2008 설치* 1. 네트워크 설정 2. 보안패치 및 백신 설치	09:00 ~ 15:00 (6H)	유휴 서버
스토리지 할당	*- Hitachi 통합스토리지#1 할당* 1. 광케이블 포설 2. HUS130 및 SAN 스위치 LUN Assign 3. 서버에 LUN 할당(1TB)	15:00 ~ 18:00 (3H)	

※ 작업 계획은 변동될 수 있음

구 분	수행 업무	작업 시간	비고
통합자산관리 솔루션 구성작업 (2017.11.29.)			
S/W 설치	*- 솔루션 구성을 위한 작업* 1. IZEX NetHelper 7.5 설치 2. MS SQL 2008 설치	13:00 ~ 15:00 (2H)	
인사DB 연동	*- 재단 그룹웨어 인사DB와 연동*	15:00 ~ 18:00 (3H)	
테스트 작업 (2017.11.30.)			
테스트	*- 구축 완료 테스트* 1. 인사DB 연동 테스트 2. 서버, Agent 간 정상 동작 확인	09:00 ~ 18:00 (9H)	

※ 작업 계획은 변동될 수 있음

6. 기대 효과

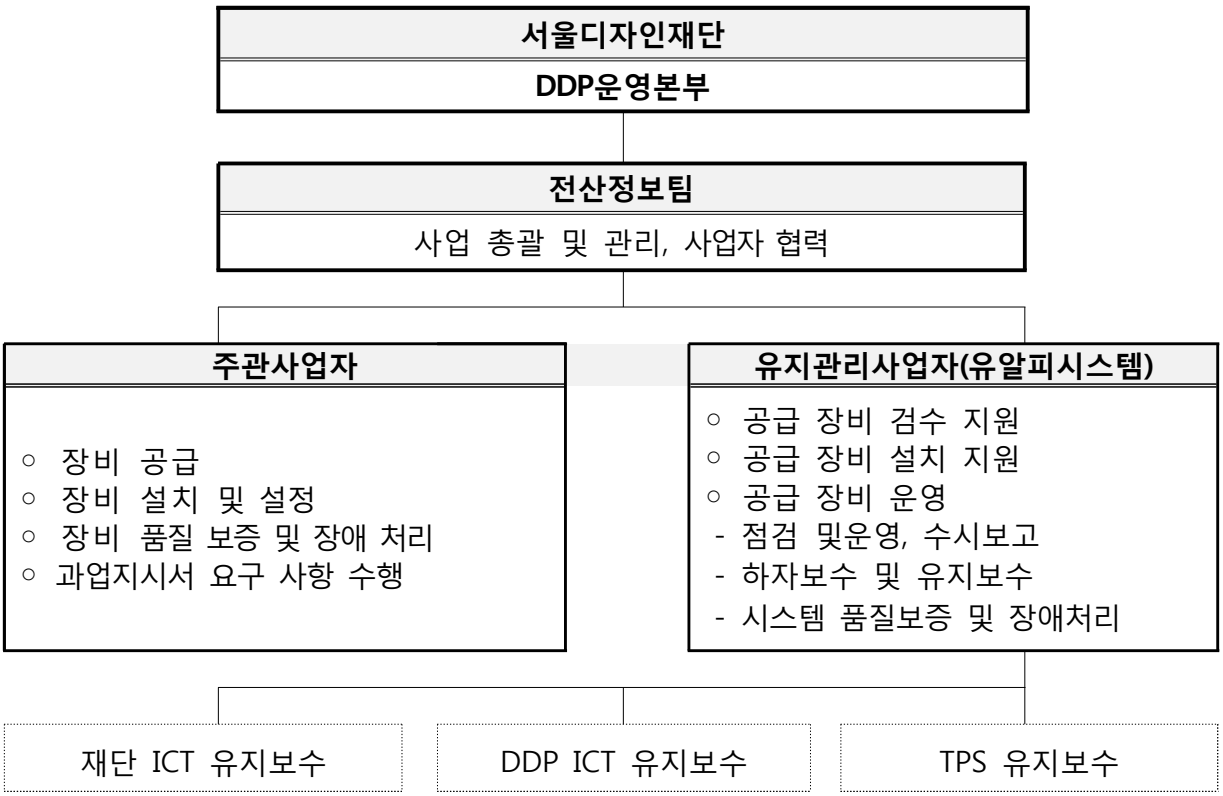
- 장애발생 시 실시간 복구, 업무 연속성 확보 및 서비스 중단 최소화
- 시스템 및 네트워크 자원에 대한 다양한 형태의 침입행위 사전 탐지, 비정상/정상 트래픽 공격의 효과적인 방어
- 재단 IT자산보호 및 지속 서비스 보장, IT자산의 라이프 사이클 관리 및 운용성, 확장성, 정확성 확보

7. 추진 절차 및 체계

- 추진 절차

사업 계획수립	=	전산정보팀	대표이사사업방침
▼			
보안성 검토	=	정보통신보안담당관	7일 (예상소요일)
▼			
계약심사 의뢰	=	계약심사과	5일 (예상소요일)
▼			
공고	=	경영지원팀	공고기간 : 10일
▼			
낙찰자 선정	=	경영지원팀	가격투찰
▼			
적격심사	=	경영지원팀	
▼			
계약체결	=	경영지원팀	
▼			
사업추진	=	전산정보팀	계약일로부터 1개월

■ 추진 체계



8. 행정 사항

■ 소요 예산(안) : 237,9334,400원 (※17년 예산)

□ 예산과목

□ 보안 장비 신규 도입 : 174,196,000원

- 예산과목 : 재단, 일반관리비, 운영경비, 운영경비, 수선유지비
- DDOS 보안 장비 : 99,000,000원
- 웹방화벽 장비 : 75,196,000원

□ 그룹웨어 서버 추가 도입 : 50,257,900원

- 예산과목1 : DDP, 기반운영사업, 정보화사업, 정보서비스운영관리, 자산취득비
- 예산과목2 : DDP, 기반운영사업, 일반관리비, 운영경비, 지급수수료

□ IT자산관리솔루션 신규 도입 : 13,480,500원

- 예산과목1 : 재단, 일반관리비, 운영경비, 운영경비, 수선유지비
- 예산과목2 : DDP, 기반운영사업, 일반관리비, 운영경비, 지급수수료

※ 붙임 : 1. 17~18년 서울디자인재단 정보시스템 통합 운영 및 유지관리 사업
착수보고회 개최 결과보고 1부.
2. 산출기초조사서_17년 정보인프라 취약점 보완 및 강화 사업 1부.
3. 견적서_17년 정보인프라 취약점 보완 및 강화 사업 각 1부.
4. 과업지시서(초안)_17년 정보인프라 취약점 보완 및 강화 사업 각 1부. 끝.