GenAI Labs

IT 인프라 아키텍처 설계

3일 집중 커리큘럼 — TA 양성 과정

[WORKSHEETS] 수강생 워크시트 통합본

Student Worksheets — Day 1·Day 2 실습 8종

포함된 실습 워크시트 (총 8종)

D1-3	Day 1 · 11:00~12:00 **업무 시스템 흐름 분석**	3-Tier · 컴포넌트 매핑 · SPOF
D1-5	Day 1 · 14:30~16:00 **네트워크 서브네팅·VLAN 설계**	CIDR · VLAN · 망분리 · VirtualBox
D1-6	Day 1 · 16:00~17:00 **구조도 읽기·SPOF 식별**	구성도 해석 · SPOF · 권고안
D2-1	Day 2 · 09:00~10:30 **LUN 매핑·RAID·Multipath 설계**	DAS/NAS/SAN · RAID · LUN · I/O
D2-2	Day 2 · 10:30~12:00 **백업 설계서**	RPO·RTO · 3-2-1-1-0 · 랜섬웨어
D2-4	Day 2 · 14:00~15:00 **Failover 테스트**	Nginx · Keepalived · VIP HA
D2-5	Day 2 · 15:00~16:00 **용량 산정표**	TPS · CPU · IOPS · NW
D2-6	Day 2 · 16:00~17:00 **네트워크 흐름 장애 분석**	5 Why · Postmortem · TTA 양식

준수 표준

[국내] ISMS-P · TTA 감리 가이드 · KCMVP · NIA HW 규모산정 · 전자금융감독규정 · KISA 망분리
[글로벌] RFC · IEEE 802.x · ISO 27001/22301/20000 · TIA-942 · ITIL 4 · TPC-C/E · NIST CSF

D1-3

업무 시스템 흐름 분석

Day 1 · 11:00~12:00

수강생 워크시트

Day 1 · 11:00~12:00 — 업무 시스템 흐름 분석 워크시트

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 1 · 11:00 ~ 12:00 (60 분)
주제	사용자 요청부터 DB 까지의 흐름 (3-Tier·N-Tier)
준수 표준	ITIL 4 · ISMS-P · TTA 감리 · KCMVP / TOGAF(참고)
준비물	필기구
산출물	흐름 매핑표 · SPOF 분석표 · 토론 답안

1. 학습 목표

1. 사용자 요청이 사내 인프라 8 계층을 통과하는 흐름을 도식화한다.
2. 3-Tier(Presentation·Logic·Data) 및 N-Tier 아키텍처의 각 계층 컴포넌트를 실제 벤더·제품과 매핑한다.
3. 단일장애점(SPOF)을 위험도(Low/Medium/High/Critical) 기준으로 식별·우선순위화한다.
4. 이중화 방안을 Active-Active / Active-Standby / N+1 패턴으로 비교 권고한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- ITIL 4 Service Value System — 국내 대기업 IT 운영 표준
- ISMS-P 인증기준 1.2.1(정보자산 식별)·2.6.1(네트워크 접근/망분리)·2.5.5(특수 계정 및 권한 관리)·2.9(시스템 및 서비스 운영관리/가용성)
- TTA 정보시스템 감리 점검 가이드 — 공공 사업 의무 점검 항목
- KCMVP(국정원 암호모듈 검증)·CC 인증 보안 솔루션 우선 (공공기관·대학)
- 행정안전부 「공공 정보화 사업 가이드」 시스템 흐름도 양식

글로벌 표준 (참고)

- TOGAF ADM (참고) — Phase B/C/D 시스템 흐름
- ISO 27001:2022 A.5(정책) · A.8(자산관리) · A.13(통신보안)

2. 분석 대상 시나리오

시나리오 — OO 대학교 학사 통합 시스템

현황: 학생 12,000 명 · 교직원 1,500 명 · 동시 접속 최대 8,000 명 (수강신청 피크)

구성: 학사정보(수강·성적·등록) + 그룹웨어(메일·결재) + LMS(강의·과제) + 도서관 시스템

전제: 사내 데이터센터 · 24×7 서비스 · SLA 99.9% (월 다운타임 ≤ 43.2 분)

보안: 망분리 3 분리(업무망·DMZ·관리망) · 개인정보보호법 준수 · ISMS-P 인증 운영 중

오늘 분석할 트랜잭션: 학생이 외부 인터넷에서 수강신청 시스템에 로그인 → 강의 검색 → 신청 확정 → DB 반영

3. 업무 흐름 컴포넌트 매핑표

사용자 요청이 거치는 10 단계를 채우세요. 「예시 제품」 열은 발주처 자산 기준 1~2 개 작성 (KCMVP 검증필 우선).

#	단계	역할	이 단계의 핵심 작업	프로토콜·포트	예시 제품 (작성)	응답시간 SLA

4. SPOF 분석

흐름에서 SPOF 5 개를 식별하고 위험도·이중화 방안을 작성하세요. 위험도 기준: Low/Medium/High/Critical.

#	SPOF 지점	장애 시 영향 (MTTR·사용자 수)	위험도	이중화 패턴	권고 솔루션 (KCMVP 우선)	추정 도입비용 (천만원)

5. 토론 및 권고안 (조별 30 분)

- Q1. 수강신청 피크(동시 8,000 명)에서 가장 먼저 병목이 발생할 컴포넌트 3 개와 측정 지표는? (예: WAS 스레드 풀 사용률·DB 커넥션 수·LB 백엔드 응답시간 P95)
- Q2. ISMS-P 2.6.1(네트워크 접근/망 분리) 관점에서 DMZ-내부망 경계에 부족한 통제는 무엇이며 어떤 솔루션을 권고하는가? (NGFW/WAF/IPS/SAC 중 선택 + 근거)
- Q3. SLA 99.9% → 99.99% 상향 시 추가 비용 대비 효과가 가장 큰 단일 투자 1 개를 선정하라. (TCO 5 년 정성 비교)

D1-5

네트워크 서브네팅·VLAN 설계

Day 1 · 14:30~16:00

수강생 워크시트

Day 1 · 14:30~16:00 — 네트워크 서브네팅·VLAN 설계 워크시트

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 1 · 14:30 ~ 16:00 (90 분)
주제	CIDR · VLAN · 망분리 · VirtualBox 모드
준수 표준	KISA 망분리 가이드 · 정보통신기반보호법 · TTA 감리 · ISMS-P / RFC 4632·1918
준비물	필기구 · 계산기 · VirtualBox 환경
산출물	서브넷 분할표 · VirtualBox 모드 매트릭스

1. 학습 목표

1. RFC 4632 CIDR 표기법으로 서브넷 마스크·네트워크·브로드캐스트·할당 가능 IP 를 계산한다.
2. 본사 1 개 층의 사설 IP 대역(RFC 1918)을 부서별 VLAN 으로 분할 설계한다.
3. KISA 망분리 가이드 기준 업무망·관리망·DMZ·게스트망을 분리한다.
4. VirtualBox NAT/Bridge/Internal/Host-Only 네 모드를 시나리오에 매핑한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- KISA 「망분리 가이드」 — 업무망·관리망·DMZ·외부망 분리 원칙
- 정보통신기반보호법 시행규칙 — 망분리 의무 대상
- TTA 정보시스템 감리 점검 가이드 — 네트워크 분할 설계
- ISMS-P 2.6.1 (네트워크 접근/망분리)·2.6.7 (인터넷 접속 통제)

글로벌 표준 (참고)

- RFC 4632 (CIDR) · RFC 1918 (Private IP)
- IEEE 802.1Q (VLAN) · 802.3 (Ethernet)

2. 분석 대상 시나리오

시나리오 — 본사 5 층 사옥 네트워크 설계

본사 1 개 층 입주 부서: 영업(70 명)·개발(120 명)·인사(15 명)·재무(20 명)

추가 분리 망: 관리망(20 대 장비 SSH·OOB)·VoIP(150 대 IP 폰)·게스트 WiFi(100 명 동시)·CCTV(50 대)

발급받은 사내 사설 IP 대역: 10.10.0.0/22 (1,024 개 IP — 사옥 단위 표준 할당)

L3 스위치 1 대(Cisco Catalyst 9300)·코어 라우터 이중화

ISMS-P 인증 대상 → 망분리 필수

3. 서브넷 분할 설계

주어진 10.10.0.0/22 (1,024 IP) 를 8 개 부서·용도로 VLSM 분할하세요. 부서별 실제 가용 IP(네트워크·브로드캐스트 차감) 가 수요를 충족해야 함.

부서/용도	VLAN ID	서브넷 (CIDR)	네트워크 주소	브로드캐스트	할당 가능 IP 수

4. VirtualBox 네트워크 모드 매핑

VirtualBox 모드	특징 요약 (DHCP·외부 접근·VM 간 통신)	이 모드가 적합한 시나리오

5. 토론 질문 (조별)

- Q1. 발급 대역 /22 (1,024 IP) 에서 8 개 망 수요 합계 545 IP 를 어떻게 효율적으로 분할하는가? VLSM 으로 부서별 크기를 어떻게 정하는가? (네트워크·브로드캐스트 차감 후 실제 가용 IP 까지 명시)
- Q2. 관리망(SSH·OOB)에 게스트 WiFi 에서 직접 도달이 가능하면 어떤 위험인가? ISMS-P 어떤 통제 위반인가?
- Q3. CCTV 50 대를 PoE 로 운영할 때 VLAN 설계 외에 고려할 NW 요소 3 가지는?

D1-6

구조도 읽기·SPOF 식별

Day 1 · 16:00~17:00

수강생 워크시트

Day 1 · 16:00~17:00 — 구조도 읽기·SPOF 식별 워크시트

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 1 · 16:00 ~ 17:00 (60 분)
주제	구성도 해석 · SPOF · 권고안 작성
준수 표준	TTA 가용성 점검 · ISMS-P A.14.1.3 · 행정기관 BCP / ITIL 4 · ISO 22301
준비물	강사 배포 구성도 PDF
산출물	흐름표 · SPOF 분석 · 권고안 1 쪽

1. 학습 목표

1. 운영 중인 서비스 인프라 구성도에서 트래픽 흐름을 단계별로 설명한다.
2. SPOF(단일장애점)를 식별하고 위험도 매트릭스로 우선순위화한다.
3. 각 SPOF 에 대해 비용·복잡도가 다른 3 가지 대응 방안을 비교 권고한다.
4. 「인프라 안정성 진단 보고서」를 TTA 감리 양식으로 작성한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- TTA 정보시스템 감리 점검 가이드 — 「가용성 점검 항목 23 종」
- ISMS-P A.14.1.3 (가용성 설계)·A.16.1.5 (장애 대응)
- 행정안전부 「공공 정보화 사업 가이드」 — 시스템 구성도 표준 양식
- 행정기관 정보시스템 BCP 지침 — 영향평가(BIA) 필수

글로벌 표준 (참고)

- ITIL 4 Availability Management
- ISO 22301 (BCM) — Business Impact Analysis

2. 분석 대상 시나리오

시나리오 — 운영 중 그룹웨어 시스템 구성도

분석 대상: 전국 지점 5,000 명이 사용하는 사내 그룹웨어 시스템 (메일·결재·게시판·일정)

현 구성: 외부 인터넷 → 방화벽 1 대 → L4 LB 1 대 → WEB 2 대 → WAS 2 대 → DB Primary 1 대

백업: Tape Library 단일 서버 / 주 1 회 풀백업·일일 증분 / 오프사이트 X

SLA 99.5% 운영 중 → 99.9% 상향 요구

최근 6 개월 장애 5 건 (DB 다운 2 회·LB 다운 1 회·DC 정전 1 회·NW 카드 1 회)

3. 트래픽 흐름 단계별 분석

외부 사용자의 HTTPS 요청이 DB 까지 도달하는 흐름을 단계별로 기록하세요.

단계	통과 장비	프로토콜·포트	예상 응답시간	비고

4. SPOF 분석 보고서

SPOF 지점	장애 발생 시 영향 범위	위험도	권고 대응안 (비용·복잡도)

5. 위험도 매트릭스 (TTA 감리 양식)

위험도	정의 (연간 발생 빈도·영향 시간)	본 시스템에서 해당하는 SPOF
Critical		
High		
Medium		
Low		

6. 권고안 작성 (자유 서술 1 쪽 분량)

작성 가이드 — TTA 감리 가이드 「가용성 진단 보고서」 양식

- 현황 요약 → 위험도 평가 (Low/Med/High/Critical) → 우선순위별 개선안 → 예상 일정·비용
- 운영 영향이 큰 SPOF 3 개를 우선 다룰 것.
- 발주처 CIO 보고 형식 — A4 1 쪽 분량.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

D2-1

LUN 매핑·RAID·Multipath 설계

Day 2 · 09:00~10:30

수강생 워크시트

Day 2 · 09:00~10:30 — LUN 매핑·RAID·Multipath 설계 워크시트

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 2 · 09:00 ~ 10:30 (90 분)
주제	DAS/NAS/SAN · RAID · LUN · Multipath
준수 표준	NIA HW 규모산정 · TTA 감리 · ISMS-P · KCMVP / SNIA · T10/T11
준비물	필기구 · 계산기
산출물	LUN 설계표 · RAID 근거

1. 학습 목표

1. 업무 시스템별 I/O 특성(랜덤/순차·R/W 비율·동시성)을 분석한다.
2. RAID 레벨·LUN 크기·Multipath 경로를 시스템별로 적합하게 설계한다.
3. Hot Spare·Tiering·Snapshot 정책을 함께 결정한다.
4. KCMVP 검증필 스토리지 솔루션을 우선 검토한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- NIA 「정보시스템 하드웨어 규모산정 지침」 — 스토리지 용량 산정
- TTA 정보시스템 감리 점검 가이드 — 스토리지 설계 항목
- ISMS-P A.8.2 (자산 분류·암호화)·A.12.3.1 (백업)
- KCMVP 검증필 스토리지 (공공 우선)

글로벌 표준 (참고)

- SNIA (Storage Networking Industry Association) 표준
- T10 SCSI Architecture Model · T11 FC standards

2. 분석 대상 시나리오

시나리오 — OO 대학 통합 시스템

단일 SAN 스토리지(NetApp AFF A800 · 가용 용량 200TB)에서 다음 4 개 업무를 운영한다:

① 학사 DB (Oracle 19c RAC · OLTP · 동시 300 사용자 · 일 4TB 쓰기 · 트랜잭션 응답 ≤ 30ms)

② 그룹웨어 첨부파일 (NAS NFS · 일 2TB · 5 년 보관 · 평균 파일 1MB)

③ CCTV 영상 (순차 쓰기 · 일 10TB · 30 일 보관 · 4K 30fps)

④ 가상화 데이터스토어 (VMware vSphere · 50 개 VM · 부팅·운영 디스크)

보안: 개인정보보호법 → 학사 DB 는 AES-256 암호화 의무

3. LUN 설계표

#	업무	I/O 패턴 (R/W·랜덤/순차)	RAID 레벨	LUN 크기·개수	Multipath	Snapshot 주기

4. RAID 선정 근거

업무	선정 RAID	성능 (IOPS)	가용성 (장애 허용)	용량 효율	선정 근거

5. 토론 (조별)

- Q1. RAID-5 vs RAID-6 vs RAID-10 중 학사 DB 에 가장 적합한 것은? 근거는?
- Q2. CCTV 영상에 Tiering(SSD → HDD → Tape) 적용한다면 단계별 보관 기간은?
- Q3. 200TB SAN 에서 5 년 후 용량 부족이 예상될 때 확장 방안 2 가지 비교 (Scale-up vs Scale-out)

D2-2

백업 설계서

Day 2 · 10:30~12:00

수강생 워크시트

Day 2 · 10:30~12:00 — 백업 설계서 워크시트

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 2 · 10:30 ~ 12:00 (90 분)
주제	백업 정책 · RPO/RTO · 3-2-1-1-0 · 랜섬웨어 대응
준수 표준	전자금융감독규정 §17 · 행정기관 백업 지침 · ISMS-P A.12.3 · TTA / ISO 22301 · NIST SP 800-34
준비물	필기구
산출물	백업 대상·주기·RTO/RPO·3-2-1-1-0 점검표

1. 학습 목표

1. 백업 대상 시스템을 분류·우선순위화한다.
2. 백업 주기·보존 기간·RPO·RTO 를 시스템별로 정의한다.
3. 랜섬웨어·물리 재해에 대비한 3-2-1-1-0 백업 정책을 적용한다.
4. 전자금융감독규정 제 17 조 / ISMS-P A.12.3 통제를 만족한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- 전자금융감독규정 제 17 조 (백업 의무·이중화)
- 행정기관 정보시스템 백업 관리 지침 (행정안전부)
- ISMS-P A.12.3.1 (백업)·A.12.3.2 (백업 매체 관리)·A.17 (사업연속성)
- TTA 정보시스템 감리 점검 가이드 — 백업·DR 점검 항목
- 개인정보보호법 시행령 §30 (개인정보 백업 시 암호화)

글로벌 표준 (참고)

- ISO 22301 (Business Continuity Management)
- NIST SP 800-34 (Contingency Planning) — RPO/RTO 정의
- 3-2-1-1-0 (Veeam 권장 백업 표준)

2. 분석 대상 시나리오

시나리오 — OO 대학 백업 정책 수립

보호 대상: 학사 DB + 그룹웨어 + LMS + 도서관 + 가상화 + 파일서버 6 시스템

총 데이터: 약 100TB · 일일 변경량 5TB · 5 년 보관 의무

백업 환경: Veeam B&R 12 + Tape Library (LTO-9) + 별도 백업망

사고 발생 시 영향: 학사 DB 손실 → 학기 수강·성적 데이터 손실 → 사회 문제

최근 보안 환경: 국내 대학 랜섬웨어 피해 다수 → Air-Gap 백업 필수

3. 백업 대상 정의

#	시스템	데이터 분류	데이터 양 (TB)	중요도 (상/중/하)

4. 백업 주기·보존 정책

시스템	Full 주기	증분 주기	보존 기간	백업 윈도우

5. RTO·RPO 목표

시스템	RTO	RPO	근거 (서비스 영향)

6. 3-2-1-1-0 정책 검토

3-2-1-1-0 정책

3 개 사본 · 2 개 매체 · 1 개 오프사이트 · 1 개 오프라인(Air-Gap) · 0 개 검증 실패

기준	현재 설계 충족 여부	미흡 시 보완안

토론 질문

- Q1. 100TB 전체를 매주 풀백업하면 백업 윈도우가 부족하다. 어떻게 해결?
- Q2. 랜섬웨어가 백업 서버까지 침범하면 어떻게 복구? Immutable Backup 의 의미는?
- Q3. 학사 DB RTO 4h 를 1h 로 단축하려면? 추가 비용 vs 효과 비교

D2-4

Failover 테스트

Day 2 · 14:00~15:00

수강생 워크시트

Day 2 · 14:00~15:00 — Failover 테스트 결과 워크시트

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 2 · 14:00 ~ 15:00 (60 분)
주제	Nginx Reverse Proxy · WEB/WAS · Keepalived VIP
준수 표준	ISMS-P A.14.1.3 · TTA · 행정기관 BCP / TIA-942 · ITIL 4 · RFC 5798
준비물	VM 환경 (Ubuntu + Nginx + Keepalived)
산출물	Failover 측정값 · 운영 개선안

1. 학습 목표

1. Nginx Reverse Proxy + WEB/WAS 이중화 구성을 직접 만든다.
2. Master 장비를 강제 중단해 Failover 동작을 확인한다.
3. 절체 시간(MTTR)을 측정하고 운영 시 개선 포인트를 도출한다.
4. TIA-942 / SLA 등급 기준으로 결과를 평가한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- ISMS-P A.14.1.3 (가용성 설계)·A.16.1 (장애 대응)
- TTA 정보시스템 감리 — 「가용성 점검 항목 23 종」
- 행정기관 정보시스템 BCP 지침 — MTTR·MTBF 측정

글로벌 표준 (참고)

- TIA-942 (DC Tier) · Uptime Institute Tier I~IV
- ITIL 4 Availability Management
- RFC 5798 (VRRPv3)

2. 분석 대상 시나리오

실습 구성도

Client ──→ Nginx LB (VIP 192.168.56.100) ──┬──→ WEB1 (192.168.56.11) ──→ WAS1

└──→ WEB2 (192.168.56.12) ──→ WAS2

Keepalived 로 VIP HA · MASTER/BACKUP · advert_int 1s · priority 150/100

3. Failover 테스트 결과

테스트 시나리오	절체 시간 (초)	데이터 손실	사용자 영향 (5 점)	비고

4. 운영 개선안

_____

_____

_____

_____

_____

_____

_____

_____

토론

- Q1. Failover 시간 < 3 초가 항상 좋은가? 어떤 트레이드오프?
- Q2. WAS Session Replication 을 안 쓰면 Failover 시 무슨 일이 발생하나?
- Q3. Split-Brain 은 어떻게 방지하나?

D2-5

용량 산정표

Day 2 · 15:00~16:00

수강생 워크시트

Day 2 · 15:00~16:00 — 용량 산정 워크시트 (5 축: CPU·Memory·IOPS·NW·Storage)

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 2 · 15:00 ~ 16:00 (60 분)
주제	TPS·CPU·Memory·IOPS·NW·Storage 5 축 정량 산정 (가상화·SMT·NUMA 보정)
준수 표준	NIA TTAK.KO-10.0292/R3 · 행정안전부 BMT · TTA 감리 · ISMS-P 2.9 / SPEC CPU 2017 · TPC-C · TPC-H · SPECjbb2015 · STAC
준비물	엑셀 (별도 템플릿) · 계산기 · 시나리오 카드
산출물	5 축 산정표 · 보정계수 적용 표 · 1·3·5 년 확장 계획서

1. 학습 목표

1. 동시접속자·트래픽 패턴 입력으로 CPU·메모리·IOPS·NW·스토리지 5 축을 산정한다.
2. TPS·서비스 시간·가용률·안전계수의 정량 공식(NIA TTAK.KO-10.0292/R3)을 적용한다.
3. 가상화 오버헤드·Hyper-Threading 효과·NUMA 영향을 보정계수로 반영한다.
4. 3 년·5 년 후 데이터·트래픽 증가율을 반영해 Scale-up/Scale-out 전환 시점을 결정한다.
5. 벤치마크 점수(SPEC CPU 2017·TPC-C·SPECjbb2015)를 정확한 단위로 인용해 실제 제품(Intel Xeon Scalable·AMD EPYC·IBM Power10) 코어로 환산한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

- NIA·TTA 「정보시스템 하드웨어 규모산정 지침」 TTAK.KO-10.0292/R3 (2023.12 개정) — 공공·SI 표준
- 행정안전부 BMT(Bench-Mark Test) 지침 — 도입 전 성능 검증
- TTA 정보시스템 감리 점검 가이드 — 「용량 산정서」 표준 양식 (입력값·공식·산출값·검증값 4 단)
- ISMS-P 2.9.1(변경 관리)·2.9.3(성능 및 장애 관리) — 임계치 정의·모니터링 의무
- 한국지능정보사회진흥원(NIA) 「공공 클라우드 전환 사업 규모산정 보완 지침」

글로벌 표준 (참고)

- SPEC CPU 2017 (SPECrate® · SPECspeed® × Integer · Floating Point) — spec.org, 발행

SPEC(Standard Performance Evaluation Corporation)

• TPC-C (tpmC, 신주문 트랜잭션/분, OLTP)·TPC-H (QphH@Size, 22 개 SQL-92 ad-hoc 쿼리, DW) — tpc.org, 발행 TPC(Transaction Processing Performance Council)

• SPECjbb® 2015 (max-jOPS·critical-jOPS, SLA 10·25·50·75·100ms) — Java 서버 워크로드

• STAC Benchmark Council (STAC-A2 옵션·VaR · STAC-M3 틱 분석 · STAC-N1 네트워크) — 금융권 전용 (stacresearch.com)

• NIST SP 800-145(Cloud Definitions)·ISO/IEC 19086(SLA)

2. 분석 대상 시나리오

시나리오 — 사내 그룹웨어 신규 구축 (Day 2 · 15:00~16:00)

사용자: 정규 5,000 명 + 외주 1,500 명 = 6,500 명

동시 접속 추정: 평균 1,500 명 · 피크 4,500 명 (출근 9 시 · 점심 13 시 · 분기마감 일자)

사용자당 평균 요청: 분당 6 회 · 평균 응답 크기 50KB · 평균 트랜잭션 CPU 시간 80ms

일일 신규 데이터: 메일 첨부 50GB · 결재 문서 20GB · 일정 5GB = 75GB/day

데이터 증가율: 연 15% (3 년 후 ×1.52 · 5 년 후 ×2.01 · 복리 1.15^N)

SLA: 99.9% (연 다운타임 ≤ 8.76h) · 응답시간 P95 ≤ 2 초 · DB 트랜잭션 응답 ≤ 30ms

도입 검토 HW: 신규 x86 2-소켓 (Intel Xeon 6 Granite Rapids 또는 AMD EPYC 9005 Turin) + Oracle 19c RAC 2-node + NetApp AFF C-Series

가상화: VMware vSphere 8 도입 검토 · 컨테이너 K8s 는 일부 신규 시스템에 한해 적용

3. CPU·메모리 산정 — 5 축 중 ①·②

TPS·CPU 시간·가용률·안전계수를 정량 공식으로 풀고, HW 보정계수(가상화·SMT·NUMA)를 적용해 최종 코어 수를 도출하세요.

#	항목	계산 공식 (단위 명시)	산출값	보정계수 적용 후

4. IOPS 산정 — 5 축 중 ③ (DB·로그·백업)

Little's Law 와 디스크 IOPS 한계(SATA HDD 75~150 · SAS 10K 175 · SAS 15K 220 · SATA SSD 30K · NVMe SSD 200K+) 기준으로 LUN 구성을 결정하세요.

용도	Read/Write 비율	피크 IOPS (계산)	디스크 종류·개수	RAID 펜널티 적용 후

5. NW 대역폭 산정 — 5 축 중 ④

구간	평균 트래픽 (Mbps)	피크 트래픽 (Mbps)	회선 권장 (안전계수 명시)

6. 스토리지 용량 산정 — 5 축 중 ⑤ (1·3·5 년 연차)

항목	1 년차	3 년차 ($\times 1.15^2$)	5 년차 ($\times 1.15^4$)

7. 토론 및 권고안 (조별 30 분)

- Q1. NIA TTAK.KO-10.0292/R3 의 「피크 계수」·「안전계수」·「보정계수」 셋의 차이를 정량 예시로 설명하라. 동일한 값을 중복 곱하면 어떤 부작용이 생기는가?
- Q2. SMT(Intel HT·AMD SMT) 가 켜져 있을 때 vCPU 개수와 물리 코어를 어떻게 환산하는가? Hyper-Threading 의 워크로드별 효과(15~30%) 를 산정에 반영하는 보수적 방식은? (SPECrate 2017 기준)
- Q3. 가상화(VMware vSphere 8) 오버헤드 와 컨테이너(K8s) 오버헤드 를 산정에 반영하는 보정계수를 비교하라. Hypervisor·Pod·Sidecar 까지 누적되는 경우 어떻게 계산하는가?
- Q4. NUMA 노드 경계를 넘는 메모리 접근의 약 30% 추가 지연이 OLTP DB 산정에 어떤 영향을 주는가? Oracle RAC·SAP HANA 에서 NUMA-aware 튜닝(numactl·hugepages) 을 산정 단계에서 어떻게 반영하는가?
- Q5. 3 년 후 트래픽·데이터가 2 배가 될 때 Scale-up(서버 교체) 와 Scale-out(노드 추가) 의 분기점은? 도입 시점에 미리 준비해야 할 「Scale-out 준비 6 대 설계 요소」 는?
- Q6. AI 추론 서버(NVIDIA L40S 48GB GDDR6 ECC vs H100 80GB HBM3) 를 신규 그룹웨어 검색·요약 기능에 도입할 때, GPU 용량 산정 공식(동시 사용자 × 토큰/s × 모델 파라미터 GB) 은?

D2-6

네트워크 흐름 장애 분석

Day 2 · 16:00~17:00

수강생 워크시트

Day 2 · 16:00~17:00 — 네트워크 흐름 장애 분석 보고서

강의명	IT 인프라 아키텍처 설계
일시·소요	Day 2 · 16:00 ~ 17:00 (60 분)
주제	5 Why · 조치 순서 · Postmortem
준수 표준	TTA 감리 · ISMS-P A.16.1 · 행정기관 장애 보고 지침 · 전자금융감독규정 / ITIL 4 · Google SRE
준비물	강사 배포 장애 시나리오
산출물	5 Why · 조치 순서표 · Postmortem

1. 학습 목표

1. 사용자 요청 한 건의 5-tuple(src/dst IP·port·proto) 흐름을 클라이언트→DC 경계→WAS→DB 까지 단계별 명령으로 추적한다.
2. 장애 진단을 L1 케이블 → L2 ARP/STP → L3 routing → L4 TCP → L7 HTTP 5 계층 트리로 분해하고 각 계층의 진단 명령·도구·판정 기준을 작성한다.
3. 선택한 장애 시나리오를 5 Why 로 근본 원인까지 추적하고 TTA 감리 양식의 Postmortem 보고서를 작성한다.
4. 재발 방지 조치를 「기술(자동화)·프로세스(변경관리)·통제(권한)」 3 축으로 도출하고 ISMS-P 통제번호와 매핑한다.

본 워크시트가 따르는 표준

국내 표준 (필수)

• TTA 정보시스템 감리 점검 가이드 — 「네트워크 점검 항목」·「장애 대응 점검 항목」

• ISMS-P 인증기준 2.9.4(로그 및 접속기록 관리)·2.10.6(업무용 단말기기 보안)·2.11.1(사고 예방 및 대응체계 구축)·2.11.2(취약점 점검 및 조치)·2.11.5(사고 대응 및 복구)

• 행정기관 정보시스템 장애 보고 지침 (행정안전부) — 「선보고·후조치」 24h 내 보고 의무

• 전자금융감독규정 제 73 조 (전산장애 보고) — 금융기관은 발생 인지 즉시 보고, 24h 내 상세 보고서 제출 의무

• KISA 「DDoS 대응 가이드(2023)」 — L3·L4 볼륨 공격 + L7 애플리케이션 공격 구분 대응

글로벌 표준 (참고)

• RFC 7011 (IPFIX, 2013-09) · RFC 3954 (Cisco NetFlow v9, 2004-10) · RFC 3176 (InMon sFlow, 2001-09) — 흐름 데이터 표준

- RFC 1213 (MIB-II, 1991-03) — SNMP 표준 MIB (ifInOctets·ifOutErrors 등 NW 카운터)
- ITIL 4 Incident Management · Problem Management
- Google SRE Workbook 「Blameless Postmortem」 (참고)
- ISO 20000-1:2018 (IT Service Management) · ISO 27035 (Information Security Incident Management)

2. 분석 대상 시나리오

시나리오 — OO 대학교 수강신청 시스템 NW 흐름·장애

구성: 학생 PC(외부 인터넷) → ISP → 사내 게이트웨이 → NGFW → L4 LB(F5 BIG-IP) → Web(Nginx, DMZ) → API GW → WAS(JEUS) → DB(Oracle 19c RAC) → SAN

주소 (예시): 학생 PC 203.0.113.45, 외부 VIP 211.34.56.78:443, 내부 Web 10.20.10.11:8080, WAS 10.20.20.21:9090, DB Listener 10.20.30.31:1521

오늘 분석할 트랜잭션: 학생이 https://수강신청.대학.ac.kr/apply 로 POST 요청 → 강의 신청 → DB INSERT 까지 한 건

최근 6 개월 NW 관련 장애 (강사 배포 — 1 건 선택해 §5 분석):

① [L1] 2026-03-05 11:00 Core 스위치 라인카드 LED Amber · 일부 VLAN 단절 · MTTR 4h

② [L2] 2026-04-18 14:20 STP 토폴로지 변경 폭주(TCN Flood) · 일부 VLAN 1~2 초 단절 반복 · MTTR 1.5h

③ [L3] 2026-05-22 09:40 OSPF 라우팅 루프 (LSA 비대칭) · 일부 사용자 트래픽 블랙홀 · MTTR 2h

④ [L4] 2026-07-09 13:10 F5 BIG-IP SNAT Pool 포트 고갈 (65535/IP 초과) · TCP 연결 실패 · MTTR 1h

⑤ [L7] 2026-09-25 10:00 외부 SYN Flood 30Gbps + Slowloris 동시 공격 · 게이트웨이 마비 · MTTR 2h

3. 5-tuple 흐름 추적표 (정상 트랜잭션)

학생 PC(203.0.113.45) → DB Listener(10.20.30.31:1521) 까지 요청 1 건이 거치는 NW 구간을 단계별로 추적하세요. 「검증 명령」 열은 해당 단계에서 실제 실행할 진단 명령(tcpdump·ss·MTR 등)을 1 개 이상 작성합니다.

#	구간	5-tuple (src→dst · port · proto)	통과 장비/소프트웨어	기대 RTT	검증 명령 (실행 위치 명시)

4. 장애 진단 5 계층 트리

「학생이 수강신청 페이지가 안 열린다」는 신고를 받았다고 가정. L1 케이블 → L2 ARP/STP → L3 routing → L4 TCP → L7 HTTP 순으로 단계별 진단 명령·판정 기준·다음 단계 결정 규칙을 작성하세요.

계층	확인 대상	진단 명령·도구	정상 판정 기준	비정상 시 다음 단계
L1 물리				
L2 데이터링크 (ARP·STP·VLAN)				
L3 네트워크 (IP·라우팅·ICMP)				
L4 전송 (TCP·UDP·포트)				
L7 응용 (HTTP·TLS·DNS)				

5. 5 Why 근본 원인 분석

장애 시나리오 ①~⑤ 중 1 건을 선택해 「왜?」를 5 번 반복하세요. 마지막 Why 는 반드시 기술 원인이 아닌 「프로세스·통제·문화」 원인으로 도달해야 합니다.

선택한 시나리오: ( )번

Why 1.

_____

Why 2.

_____

Why 3.

_____

Why 4.

_____

Why 5.

_____

6. 영향 범위·복구 조치 순서

장애 인지(MTTA) → 1 차 진단 → 임시 조치 → 정상화 확인 → 회의 소집 순으로 작성하세요. 「ITIL 4 Incident Management」 의 「Detect → Diagnose → Resolve → Close」 4 단계를 반영합니다.

순서	조치 내용	예상 소요	담당 (역할)	ITIL 단계

7. Postmortem 요약 (TTA 감리 양식)

장애 시작 시각	
최초 인지 시각 (MTTA)	
복구 완료 시각	
총 다운타임 (MTTR)	
영향 사용자/시스템	
근본 원인 (5 Why 결과)	
재발 방지 조치 — 기술	
재발 방지 조치 — 프로세스	
재발 방지 조치 — 통제 (ISMS-P 통제번호 명시)	

8. 토론 및 권고안 (조별 30 분)

- Q1. Blameless Postmortem 의 정의는 무엇이고, 한국 조직 문화에서 정착이 어려운 이유 3 가지와 정착 방안을 제시하라.
- Q2. ISMS-P 2.11.5 「사고 대응 및 복구」 요구사항을 만족하는 산출물 3 종을 나열하고, 본 시나리오에 적용하라.

- Q3. 1 차 알람(자동 감지)과 2 차 알람(에스컬레이션)을 어떻게 분리·설계하는가? Zabbix·PagerDuty 예시로 답하라.
- Q4. 본 시나리오에서 NetFlow v9(RFC 3954) 또는 IPFIX(RFC 7011) 도입 시 가장 큰 운영 가치는 무엇인가? 미도입 상태에서의 진단 한계와 비교하라.