IT 인프라 아키텍처 설계

구조도 읽기
SPOF 식별 · 위험도 매트릭스 · 권고안

Session 9 · Day 3 — 09:00 ~ 10:00 (60분)

구성도 5종 · 트래픽 흐름 · SPOF 체크리스트 · 4단계 위험도 · TTA 감리 양식

강사 박수현 · 🚀 젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

Session 9 — *회차 메타데이터*

📋 세션 정보

- **슬롯**: Day 3 · 09:00 ~ 10:00 (60분)
- **카테고리**: 분석 방법론 — 구조도·SPOF
- **연계 워크시트**: D3-0 「구조도 읽기·SPOF 식별」
- **선행 학습**: Day 1·2 전반 (인프라·NW·스토리지·보안·HA)
- **후속 학습**: Day 3 워크숍·RFP·5 케이스 — SPOF 분석을 직접 적용

🎯 핵심 메시지

> 「TA는 구성도에서 SPOF를 찾아내고, 위험도로 우선순위화하고, 한 페이지 권고안으로 의사결정자에게 전달한다」

🧭 학습 목표 (LO)

1. **구성도 5종 구분** — 논리·물리·NW·보안·DR
2. **트래픽 흐름 추적** — 단계별 경로·프로토콜·SLA 분해
3. **SPOF 식별** — 체크리스트 23항 활용
4. **위험도 매트릭스** — 영향도·확률 기반 4단계
5. **이중화 패턴 선택** — 비용·복잡도 비교
6. **권고안 작성** — TTA 감리 표준 1쪽 양식

Session 9 — *오늘의 흐름 (60분)*

🗺️ Part A~C (전반부 · 30분)

- **A. 구성도 5종 구분** — 논리·물리·NW·보안·DR
- **B. 구성도 읽기** — 트래픽 흐름 추적법
- **C. SPOF 식별 절차** — 23항 체크리스트

🗺️ Part D~F (후반부 · 30분)

- **D. 위험도 매트릭스** — 영향도×확률 4단계
- **E. SPOF 대응 패턴** — Active-Active·Standby·Cluster
- **F. TTA 감리 양식 + 워크시트 D1-6 연계**

Part A. 구성도 5종

논리 · 물리 · NW · 보안 · DR

8 슬라이드 · 약 13분

왜 구성도가 5종인가?

🎯 TA가 다루는 5가지 관점

- **① 논리 구성도** (Logical) — 기능 흐름·계층
- **② 물리 구성도** (Physical) — 실제 장비·랙·전원
- **③ NW 구성도** (Network) — VLAN·라우팅·방화벽
- **④ 보안 구성도** (Security) — 망분리·통제·인증
- **⑤ DR 구성도** (Disaster Recovery) — 백업·복제·사이트

📌 누가 어느 것을 보는가?

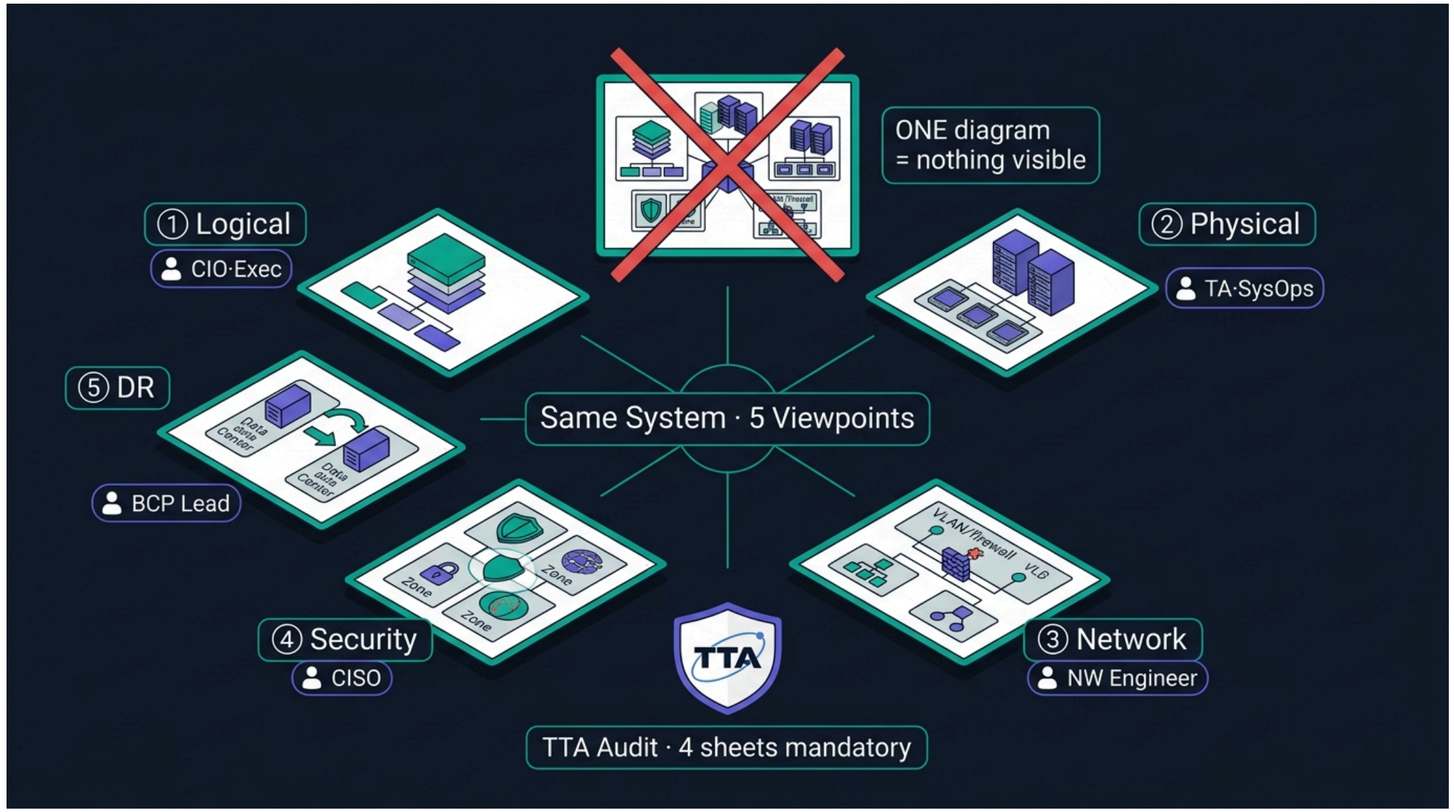
- **CIO·임원** → ① 논리
- **TA·시스템 운영자** → ②③ 물리·NW
- **CISO·보안** → ④ 보안
- **BCP 담당** → ⑤ DR

🇰🇷 국내 표준 (TTA 감리 가이드)

TTA 감리 점검 항목 중 「설계 산출물」 분류: - 📄 시스템 구성도 (논리·물리 필수) - 📄 네트워크 구성도 (필수) - 📄 보안 구성도 (필수) - 📄 DR 구성도 (가용성 요구 시 필수)

⚠️ 「하나의 그림으로 다 표현」 실패

- 한 그림에 5가지 다 넣으면 → 아무것도 안 보임
- 5장으로 분리해야 각자 점검 가능



왜 구성도가 5종인가?

① 논리 구성도 vs ② 물리 구성도

📐 ① 논리 구성도 (Logical)

무엇을 보여주나 - 기능 블록 (Web·WAS·DB·Cache) - 데이터 흐름 (화살표) - 인터페이스·프로토콜 - 외부 시스템 연계

누가 그리나: TA · 아키텍트 **도구**: draw.io · Visio · PowerPoint **TTA 양식**: 박스 + 화살표 · A4 가로

핵심 — 「장비 모델·랙 위치는 안 그린다」

🏗️ ② 물리 구성도 (Physical)

무엇을 보여주나 - 실제 장비 모델·시리얼 - 랙 위치 (Rack-U) - 전원 (A·B선) - 케이블링 (FC·Ethernet 종류) - 면적·하중

누가 그리나: 시스템 운영자 · 설치업체 **도구**: AutoCAD · Visio Rack Shape **TTA 양식**: 랙 도면 + BoM 표

핵심 — 「실제 손으로 만질 수 있는 모든 것」

③ NW 구성도 — *VLAN · 라우팅 · 방화벽*

📡 무엇을 보여주나

- **L2** — 스위치·VLAN·STP
- **L3** — 라우터·서브넷·라우팅
- **L4** — 방화벽·LB
- **L7** — WAF·Anti-DDoS
- **IP 주소·VLAN ID**
- **케이블 종류·속도**
- **외부 회선** (KT·SKB·LGU+)

💡 표기 표준

- VLAN: 색깔 구분 (DMZ=빨강·업무망=초록)
- IP: CIDR (10.0.0.0/24)
- 회선: 굵기 표현 (10G·40G·100G)

🛠️ 국내 표준 도구

- **NetSpot · NetDiscover** (한국 SI)
- **SolarWinds Network Topology Mapper**
- **draw.io + Cisco/F5 Stencil**
- **Cisco Network Assistant**
- **국가공공기관: 자체 양식 (한컴 한셀)**

📋 필수 표기 항목

- 모든 장비 호스트명·IP·VLAN
- 회선 ISP·속도·계약 번호
- 방화벽 룰 요약 (상세는 별도 문서)
- 인터넷 게이트웨이·DMZ·내부망 경계

🇰🇷 TTA 점검 항목 (5개)

1. 망분리 구조 명확성
2. 이중화 표기 (실선·점선)
3. 회선 사양 명시
4. 보안 장비 위치
5. 외부 인터페이스

④ 보안 구성도 — *망분리 · 통제점 · 인증*

🔐 무엇을 보여주나

- **망분리 구조**: DMZ · 업무망 · 관리망 · 게스트
- **보안 장비 위치**: NGFW · WAF · IPS · Anti-DDoS · SAC
- **인증 시스템**: AD · LDAP · OAuth · SSO
- **암호화 경계**: TLS·VPN·IPSec 시작·종료
- **로그 수집 위치**: SIEM·ESM
- **백업·DR 경로**

🇰🇷 국내 표준 표기

- **KISA 망분리 가이드** 권장 도식
- **ISMS-P 인증 심사용** 별도 양식
- **국정원 보안적합성** 검토용 양식 (공공)
- **금융보안원 점검표** (금융)

📋 필수 통제 표기

- ☐ DMZ 경계 (외부 ↔ DMZ)
- ☐ 업무망 경계 (DMZ ↔ 내부)
- ☐ 관리망 분리
- ☐ 인증 통제점 (모든 진입로)
- ☐ 로그 수집 통제점
- ☐ 백업 망분리

⑤ DR 구성도 — *백업 · 복제 · 사이트 이중화*

🆘 무엇을 보여주나

- **Primary Site** (운영)
- **DR Site** (대기 · 별도 건물·지역)
- **복제 경로** (Sync·Async)
- **백업 매체** (Disk·Tape·Object)
- **RPO·RTO 표기**
- **Failover 절차** (자동·수동)

📦 국내 표준 패턴

- **Active-Standby** (가장 흔함)
- **Active-Active** (대형·금융)
- **Hot Standby** (1시간 내 절체)
- **Warm Standby** (1일 내)
- **Cold Standby** (백업만 보관)

🇰🇷 국내 표준 요구

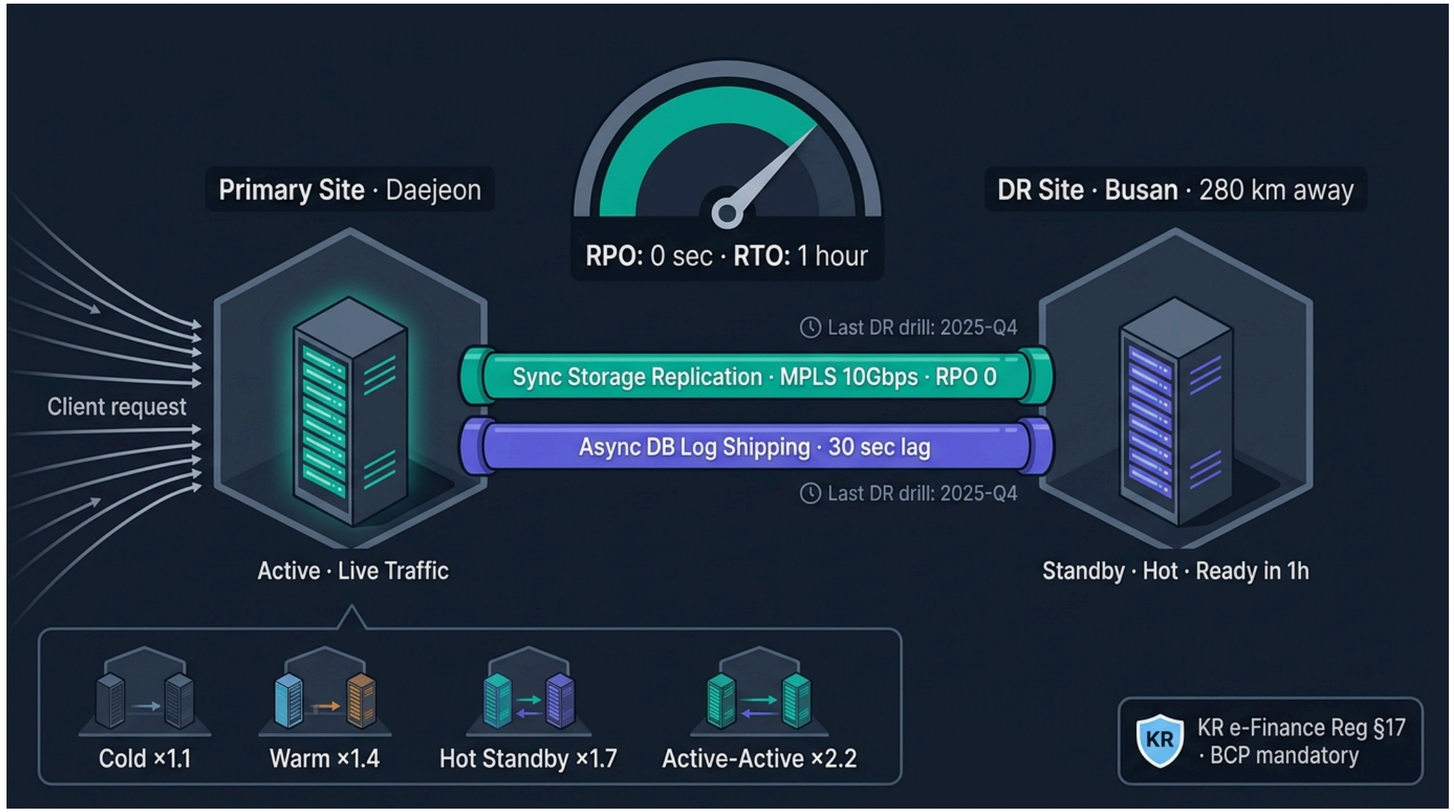
- **전자금융감독규정 제17조** — 백업·DR 시설 의무
- **행정기관 정보시스템 BCP 지침**
- **개인정보보호법 시행령 §30** — 백업 암호화
- **TTA 감리** — RPO·RTO 산정 근거

📊 핵심 표기 항목

- 두 사이트 간 거리 (km)
- 회선 사양 (전용회선·MPLS)
- 복제 방식 (Storage·DB·App)
- RPO·RTO 목표 + 측정값
- 마지막 DR 시험 일자

💰 비용 차이

- Active-Standby: 1× → 1.7×
- Active-Active: 1× → 2.2×
- 별도 사이트: 추가 5~20억



⑤ DR 구성도 — 백업 · 복제 · 사이트 이중화

Part B. 구성도 읽기

트래픽 흐름 추적 · 도식 기호 해석

7 슬라이드 · 약 11분

구성도 읽기 — *TA의 5단계 점검법*

1️⃣ 외부에서 시작 — 입력점 찾기

- 인터넷·외부 시스템·내부 사용자가 어디로 들어오나
- 회선·IP·도메인 확인
- **체크**: 입력점이 다중인가? (Web + API + Mobile)

2️⃣ 보안 경계 통과

- DMZ·방화벽·WAF 순서
- **체크**: 보안 장비 단계별 누락 없나? Anti-DDoS·WAF·NGFW·IPS·SAC

3️⃣ 부하 분산 (LB)

- L4/L7 LB 위치·이중화
- **체크**: SSL Termination 위치는?

4️⃣ 응용 계층 (Web·WAS·API GW)

- 각 계층 인스턴스 수
- **체크**: 인스턴스 1대인 곳 (SPOF!)

5️⃣ 데이터 계층 (Cache·DB·Storage)

- DB 이중화·Storage RAID
- **체크**: DB Primary 1대? Storage 단일?

🎓 5단계 점검 후 「3가지」 정리

1. **SPOF 목록** (단일 구성 컴포넌트)
2. **이중화 패턴** 각 계층 어떤 패턴
3. **보안 통제점** 누락 여부

구성도 도식 기호 — *국내 표준 표기*

기호	의미	비고
🔲 **사각형 박스**	시스템·서버·서비스	색깔로 영역 구분
🔵 **원형**	외부 시스템·사용자	「Internet」·「User」
▭ **둥근 사각형**	DB·Storage	Cylinder도 동일
⬡ **육각형**	인증·게이트웨이	OAuth·API GW
━ 실선	정상 트래픽	굵기로 회선 속도 표현
┄ 점선	백업·이중화 경로	Standby 연결
🟥 **빨강 박스**	DMZ · 외부 노출	위험 표시
🟩 **초록 박스**	업무망 · 내부	안전 영역
🟨 **노랑 박스**	관리망 · 격리	SSH·OOB 전용
⚡ **번개 아이콘**	SPOF · 위험점	강조

좋은 구성도 vs 나쁜 구성도

✅ 좋은 구성도

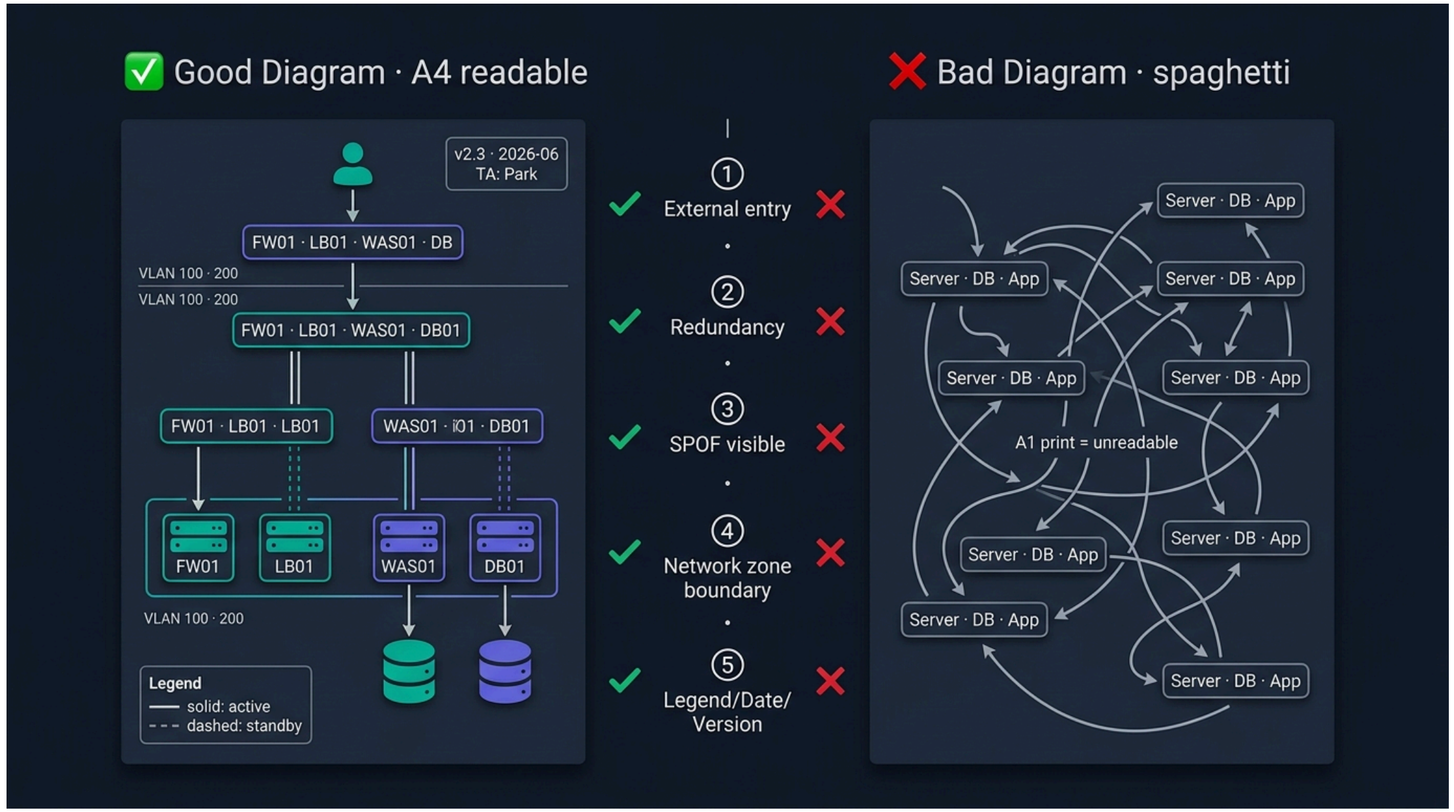
- **계층이 명확** — 위에서 아래로 외부→내부
- **이중화 표현** — 실선·점선·박스 분리
- **장비명·IP·VLAN 명시**
- **범례·기호 정의** 좌하단
- **A4 한 장**에 들어감 (또는 A3)
- **버전·날짜·작성자** 우상단

❌ 나쁜 구성도

- **화살표가 거미줄** — 어디서 어디로 가는지 모름
- **이중화가 안 보임** — 한 박스에 모두 표현
- **장비명 부재** — 「Server」·「DB」만 적힘
- **외부 인터페이스 누락**
- **A1 크기** 인쇄 시 글자 안 보임
- **버전 없음** — 5년 전 그림인지 알 수 없음

📌 점검 5문

1. 외부 입력점이 어디인가?
2. 이중화 패턴이 명확한가?
3. SPOF가 보이는가?
4. 망분리 경계가 명확한가?
5. 범례·날짜·버전 있는가?



좋은 구성도 vs 나쁜 구성도

한국 SI 구성도 — *현장 관행*

🏗️ 일반적 관행

- **A3 PDF 출력**이 표준 (회의용)
- **한컴 한셀** 또는 PowerPoint
- **벤더 로고** 그대로 사용 (Cisco·F5·Oracle·NetApp)
- **계층별 색깔** — DMZ 빨강·업무 초록·관리 노랑
- **「⭐」·「★」 표기**로 SPOF·중요 강조
- **한글 위주** — 영문은 제품명만

📁 발주처별 차이

- **공공기관**: TTA 양식 또는 자체 양식
- **대기업**: 자체 표준 양식 (삼성·LG·SK 등)
- **금융**: 금융보안원 양식
- **대학**: 자유 (도구·양식 일관성 약함)

🎓 TA가 알아야 할 「현장 코드」

- 「**원장 그림**」 — 가장 최신·공식 구성도
- 「**현행화 그림**」 — 실제와 일치하는 갱신본
- 「**제안 그림**」 — RFP 응답서 첨부
- 「**최종본**」 — 감리·승인 후 확정본

💡 「그림과 실제가 다를 때」

- 가장 흔함 (현행화 미흡)
- TA는 **실측** + **갱신** 책임
- 변경관리(CMDB) 활용
- 분기 1회 점검 권장

실습 — *구성도 1장에서 무엇을 찾는가? (3분)*

📊 예시 구성도 (텍스트)

```
[Internet]
    |
[방화벽 단일]
    |
[L4 LB 단일]
    |
[Web ×2] → [WAS ×2]
              |
        [DB Primary]
              |
        [Tape 백업 단일]
```

🔎 발견 SPOF 5건

1. 방화벽 단일 → 외부 진입 차단 위험
2. L4 LB 단일 → 분산 실패
3. DB Primary 단일 → 데이터 손실
4. Tape 백업 단일 → 복구 실패
5. 인터넷 회선 1개? → DR 회선 X

💡 식별 흐름

- 위 그림에 SPOF 지점은 빨강 ⚡ 로 표시
- 위험도 매트릭스 적용 (다음 Part D)
- 권고안 작성 (Part F)

🇰🇷 TTA 점검 결과

- 가용성 점검 23항 중 8항 미달
- ISMS-P 2.9.2 위반
- 「가용성 등급 표」 작성 필요
- 권고: 즉시 이중화 검토

Part C. SPOF 식별 절차

정의 · 체크리스트 23항 · 식별 패턴

10 슬라이드 · 약 15분

SPOF (Single Point of Failure) — *정의와 유형*

📘 정의

> **SPOF** = 단일장애점 — *한 구성 요소의 장애가 전체 시스템 또는 핵심 기능을 중단시키는 지점*

🔍 SPOF 4가지 분류

1. **하드웨어 SPOF** — 서버·NW·Storage 단일
2. **소프트웨어 SPOF** — DB·WAS·인증서 단일
3. **인프라 SPOF** — 전원·냉각·회선 단일
4. **운영 SPOF** — 특정 인력·문서·계정 단일

📌 ISMS-P 관점

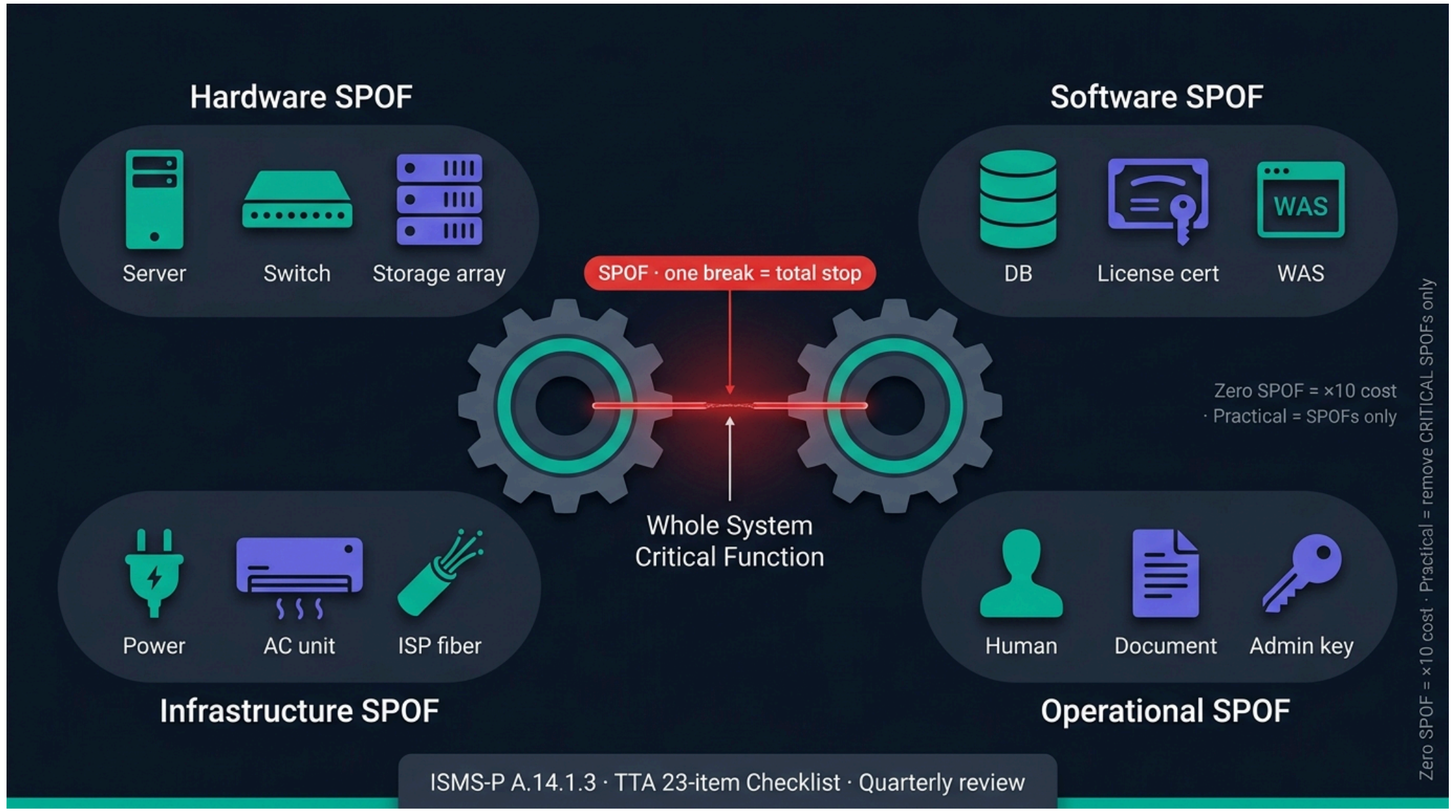
- **2.9.2** 「성능 및 장애관리」 — SPOF 식별·이중화
- **2.11.5** 「사고 대응 및 복구」 — SPOF 장애 대응
- **2.12.1** 「재해·재난 대비 안전조치」 — SPOF 영향평가

🇰🇷 TTA 감리 점검

- **「가용성 점검 23항」** — SPOF 명세 의무
- 「SPOF 분석 보고서」 — 표준 산출물
- 분기 1회 점검 권장

💡 「SPOF가 0개?」 비현실적

- 모든 SPOF 제거 시 비용 ×10
- 실용: **Critical SPOF만 제거**
- 「수용 가능 SPOF」 결정도 TA 역할



SPOF (Single Point of Failure) — 정의와 유형

SPOF 체크리스트 23항 — *Part 1: 인프라 영역*

⚡ 전원·DC (5항)

1. ☐ 외부 전원 (한전 2회선)
2. ☐ UPS (이중화 N+1)
3. ☐ 디젤발전기
4. ☐ 분전반 (A·B선)
5. ☐ DC 냉각 (CRAC 이중화)

🌐 네트워크 (5항)

6. ☐ 외부 회선 (다중 ISP)
7. ☐ 외부 DNS
8. ☐ Core 라우터·스위치
9. ☐ Distribution 스위치
10. ☐ ToR 스위치

🛡️ 보안 (4항)

11. ☐ Anti-DDoS
12. ☐ WAF
13. ☐ NGFW (외부·내부)
14. ☐ SAC·인증 서버

💻 서버·OS (4항)

15. ☐ Web Server
16. ☐ WAS
17. ☐ API Gateway
18. ☐ Cache (Redis)

SPOF 체크리스트 23항 — *Part 2: 데이터·운영*

🗄️ DB·Storage (3항)

19. ☐ DB Primary

20. ☐ Storage (SAN/NAS)

21. ☐ 백업 시스템

🔄 DR·BCM (1항)

22. ☐ DR Site 또는 백업 사이트

👥 운영 (1항)

23. ☐ 핵심 운영 인력 (Single Person Dependency)

🎯 「체크」 방법

- ☐ 미점검 → 「확인 안 함」 → 점검 필요
- ❌ SPOF 있음 → 위험도 평가 → 권고
- ✅ 이중화 있음 → 상세 확인 (Sync/Async)

📋 산출물 형식

- 23항 점검표 (Excel)
- 「✅·❌·☐」 + 위험도 등급
- 미흡 항목별 권고안

💡 운영 SPOF (23번) 흔히 누락

- 「김OO 대리만 그 시스템 알아요」
- → 문서화·교차 훈련·OnCall 로테이션
- 휴가·이직 시 즉각 장애 가능

SPOF 식별 예시 — *그룹웨어 5계층 점검*

#	계층	발견된 SPOF	영향	즉각 위험?
1	외부 회선	단일 ISP (LG U+)	회선 장애 시 도달 불가	✅
2	외부 DNS	1대 (사내 BIND)	DNS 장애 시 전체 중단	✅
3	보안	NGFW 단일 + WAF 단일	외부 진입 차단	✅
4	LB	L4 LB 1대 (HAProxy)	백엔드 분산 실패	⚠️
5	Web	Nginx 2대 (정상)	—	❌
6	WAS	Tomcat 2대 (정상)	—	❌
7	DB	Oracle Primary 1대	데이터 손실·전체 중단	✅✅
8	Storage	NetApp 1대 (Dual Ctrl)	Ctrl 절체로 OK	⚠️
9	백업	Tape Library 1대	백업 실패	⚠️
10	운영	인력 2명·DBA 1명	DBA 휴가 시 위험	⚠️

⚠️ **Critical SPOF 4개** (1·2·3·7) **즉각 조치 권고** · ⚠️ Medium 4개 (4·8·9·10) — 6개월 내 개선

SPOF 식별 예시 — 그룹웨어 5계층 점검

SPOF 식별 도구·기법

🔧 ① Fault Tree Analysis (FTA)

- 「상위 사고 → 하위 원인」 트리
- 「전체 중단」 → AND/OR 조합으로 추적
- 단일 OR 노드 = SPOF
- 도구: draw.io · isograph FaultTree+

🔧 ② Dependency Mapping

- 시스템 간 의존성 도식
- CMDB (Configuration Mgmt DB) 활용
- 도구: ServiceNow CMDB · Device42

🔧 ③ Chaos Engineering (선택)

- 의도적 장애 주입 (실험)
- Netflix Chaos Monkey · Gremlin
- 한국 도입 적음 (위험 회피 문화)

🔧 ④ Walkthrough (가장 흔함)

- 실제 시스템 룸·구성도 동행 점검
- 운영자와 함께 「만약 이게 멈추면?」 질문
- 시간: 시스템당 2~4시간
- 산출: 점검 일지 + SPOF 목록

🔧 ⑤ DR Test (실측)

- 실제 절체 시험으로 SPOF 발견
- 「의외의 SPOF」 발견율 30%+
- 분기 1회 권장
- 위험: 운영 영향 → 야간·휴일

💡 가장 효과적 — 「④ Walkthrough」

- 비용·시간 적음
- 운영자 지식 활용
- 즉시 권고안 작성 가능

Part D. 위험도 매트릭스

영향도 × 확률 4단계 · Critical~Low

5 슬라이드 · 약 8분

위험도 4단계 — *Critical · High · Medium · Low*

등급	정의	발생 빈도	영향 시간	예시
🔴 **Critical**	전체 중단 또는 데이터 손실	연 1회+	4h+	DB Primary 단일 · DC 정전
🟠 **High**	부분 서비스 영향 또는 일시 중단	연 1~4회	1~4h	NGFW 단일 · LB 단일
🟡 **Medium**	일부 사용자 영향 또는 단시간	연 < 1회	30분~1h	NW 카드 · 라이센스 서버
🟢 **Low**	자동 복구 또는 영향 없음	연 0회	즉시	Web/WAS 이중화 완료

📌 **TA 의사결정 원칙** - Critical: **즉각 조치** (3개월 내) - High: **6개월 내** 개선 - Medium: **연간 계획** - Low: **모니터링만**

영향도 × 확률 매트릭스 — *위험도 계산법*

📊 영향도 (1~5)

- **5** 전체 중단·데이터 손실
- **4** 핵심 기능 중단
- **3** 일부 사용자 영향
- **2** 성능 저하만
- **1** 영향 없음

📊 확률 (1~5)

- **5** 연 2회+ 발생
- **4** 연 1회
- **3** 1~2년 1회
- **2** 3~5년 1회
- **1** 10년+ 1회

🧮 점수 = 영향도 × 확률

- **20~25** → Critical
- **12~19** → High
- **6~11** → Medium
- **1~5** → Low

📋 예시

- DB Primary 단일: 5×4 = 20 → Critical
- L4 LB 단일: 4×3 = 12 → High
- 라이센스 서버 단일: 3×2 = 6 → Medium
- 사용자 PC 1대 고장: 1×5 = 5 → Low

💡 실무 적용

- 점수가 같아도 「영향도 우선」
- 영향도 5 → 무조건 Critical/High

우선순위 결정 — *ROI를 함께 본다*

📊 우선순위 공식

> **우선순위 = (영향도 × 확률) ÷ 도입 비용**

📋 예시 — 그룹웨어 SPOF 4건

SPOF	위험도	비용(억)	우선순위
DB Primary	20	1.8	11.1
외부 DNS	16	0.05	**320 ★**
NGFW	12	0.8	15
Tape 백업	9	1.2	7.5

> **외부 DNS가 1순위** — 비용 500만원으로 위험 16점 해결

💰 ROI 계산

- **다운타임 1회 손실**: 추정 3억 (그룹웨어)
- **DB DataGuard 도입**: 1.8억 · 5년 회피 확률 90%
- **회수 기간**: 1억 8천 ÷ 3억 = 0.6년 (8개월)
- **5년 ROI**: 1,000%+

🎯 TA의 「3가지 ROI 분석」

1. 도입 비용 (HW·SW·인력)
2. 운영 비용 (라이센스·유지보수)
3. 회피 손실 (다운타임 × 발생률)

💡 발주처 보고용

- 위 표를 **A4 한 장**으로 정리
- 우선순위 1·2·3만 강조
- 「투자 ↔ 회피 손실」 비교

위험도 평가 — *자주 하는 실수 5가지*

❌ 실수 1 — 「확률 낮음」으로 무시

- 「DB 다운은 10년에 한 번 → Low」
- 한 번 발생 시 손실 100억 → 영향도 5
- 진짜 위험도: 5 × 2 = 10 (Medium)

❌ 실수 2 — 위험도와 비용 분리 평가

- 「Critical이니 무조건 즉각 조치」
- 비용 50억 → 예산 부족 → 결국 안 함
- → **ROI 함께 계산**

❌ 실수 3 — 「확률」을 과거 데이터만

- 「3년간 무사고 → 확률 0」
- 다음 해 첫 사고 → 통계 0

❌ 실수 4 — 영향도를 「기술」로만

- 「DB 다운 → DB 다시 켜면 됨」
- 실제: 학기 등록 마감 직전 다운 = 사회 문제
- → **비즈니스 영향** 포함

❌ 실수 5 — 「모두 Critical」

- 위험 회피하려고 다 Critical
- 의사결정자: 「다 중요하면 다 안 중요」
- → 정직한 등급 분류

✅ TA의 「위험도 평가 원칙」

- 영향도: **기술 + 비즈니스 + 사회**
- 확률: **과거 + 미래 + 외부 환경**
- 비용: **도입 + 운영 + 회피 손실**

Part E. SPOF 대응 패턴

Active-Active · Standby · Cluster · DR

6 슬라이드 · 약 10분

SPOF 대응 — *5패턴 한 줄 카탈로그*

Active-Standby · Active-Active · N+1 (Cluster) · Hot Standby (DR) · Cold Standby (백업)

> SPOF가 식별되면 위 5패턴 중 하나로 묶어 결정한다 — **절체 시간 · 비용 · 상태 보유 여부** 3축이 결정 변수.

📚 **본문은 Session 8 `## HA 패턴` (N+1·N+M·2N·2N+1·A-A 5종 비교 + 다이어그램)** 에서 다룬다. - 계층별 대응(DNS·WAF·NGFW·LB·Web·WAS·DB·Storage) 표 - Active-Active vs Active-Standby 결정 카드 (Stateless ↔ Stateful) - Split-Brain 방지 (Quorum · STONITH · Fencing)

본 회차에서는 SPOF **식별→등급→수용 결정**의 흐름에만 집중한다.

「수용 가능 SPOF」도 TA의 결정 — *비용 vs 위험*

🎯 모든 SPOF 제거가 불가능한 이유

- 비용 ×3~10
- 운영 복잡도 ↑
- 「이중화의 이중화」 끝없음

📋 「수용 가능 SPOF」 예시

- **사용자 PC** (개인 책임)
- **외부 ISP 회선** (다중 ISP 비용 부담 시)
- **DC 단일** (별도 DR Site 비용 부담 시)
- **운영 인력 단일** (24x7 OnCall 부담)

💡 결정 기준

- **연 손실 < 도입 비용** 일 때 수용
- 단, **공식 문서화** 필수
- 의사결정자(CIO·CISO) 결재

📄 「수용 SPOF 등록부」 작성

- TTA 감리 산출물의 한 종류
- 등록 항목:
- SPOF 명
- 위험도 · 영향
- 미해결 사유 (비용·기술·운영)
- 보완책 (백업·수동 절체)
- 결재자 · 결재일
- 재검토 주기 (분기 1회)

🇰🇷 ISMS-P 인증 시

- 수용 SPOF는 **1.2.4 보호대책 선정** 영역 (위험 수용)
- 위험 수용 보고서 제출
- 감리·심사 시 정당성 입증

Part F. TTA 감리 양식 + 워크시트 연계

6 슬라이드 · 약 10분

TTA 감리 — *「가용성 진단 보고서」 표준 양식*

📋 표준 5절 구성

1. **현황 요약** — 시스템 개요 + SLA 목표 + 운영 인력
2. **위험도 평가** — Critical/High/Med/Low 등급별 SPOF 개수
3. **우선순위별 개선안** — 1·2·3순위 + 구체적 방안
4. **예상 일정·비용** — 총 비용 + 단계별 일정
5. **ROI** — 도입 비용 ÷ 회피 손실

📑 분량

- **A4 1쪽** (요약) + 부록 (상세)
- CIO·임원 보고 양식

✅ TTA 점검 시 확인 사항

- ☐ 위험도 등급 기준 명시
- ☐ 영향도·확률 정의
- ☐ 우선순위 결정 근거
- ☐ ROI 계산 과정
- ☐ 의사결정자 결재란
- ☐ 재검토 주기 명시

💡 자주 빠지는 것

- **ROI 계산** — 「Critical이라 해야 한다」만으로는 부족
- **재검토 주기** — 분기 1회 또는 반기 1회
- **이행 점검표** — 권고안만 있고 이행은 누가?

권고안 1쪽 — *예시 (그룹웨어 시스템)*

📄 가용성 진단 권고안

[현황] 본 그룹웨어는 5,000명이 24×7 사용하는 핵심 시스템이나, DB Primary·방화벽·LB·백업이 단일 구성으로 SLA 99.5% 미달 위험 상존. 최근 6개월 5건 장애 중 4건은 단일장애점 직접 영향.

[위험도 평가] Critical 2건(DB · DC 전력) · High 3건(방화벽 · LB · 백업) · Medium 1건(NW 카드). Critical 2건 미해결 시 99.9% SLA 달성 불가.

[우선순위별 개선안] - **1순위** DB DataGuard Standby (1.8억·6개월) — RPO 0·RTO 30s - **2순위** NGFW + L4 LB Active-Standby 이중화 (1.4억·3개월) — 외부 진입 안정화 - **3순위** Veeam + Object Storage 오프사이트 백업 (1.2억·3개월) — 랜섬웨어 대응

[예상 일정·비용] 총 4.4억 · 9개월. ROI: 다운타임 1회당 손실 추정 3억(생산성+기회비용) → 연 1회 회피 시 회수.

[결재] 작성: TA 박OO · 검토: CIO 김OO · 승인: CEO 이OO · 일자: 2026-XX-XX

워크시트 D1-6 연계 — *직접 작성한다*

📝 워크시트 D1-6 과제

1. **트래픽 흐름 단계별 분석** (8단계)
2. **SPOF 분석 보고서** (6개 SPOF)
3. **위험도 매트릭스** (4단계 분류)
4. **권고안 작성** (TTA 양식 1쪽)

⏱️ 진행 가이드 (60분)

- **이론 강의** (60분) ← 지금까지
- 워크시트는 D1 16시까지 진행
- 강사 답안·해설 별도 배포

💡 정답 힌트

- 슬라이드 18·19 (23항 체크리스트) 활용
- 슬라이드 24·25 (위험도 매트릭스) 적용
- 슬라이드 36 (권고안 양식) 그대로

📋 산출물 평가 기준

1. SPOF 6개 식별 정확성
2. 위험도 4단계 분류 합리성
3. 권고안 우선순위 + 비용
4. ROI 계산
5. 「수용 가능 SPOF」 명시

Session 9 — *정리*

🎯 오늘 다룬 것

1. **구성도 5종** — 논리·물리·NW·보안·DR
2. **구성도 읽기 5단계** — 외부에서 안으로
3. **SPOF 체크리스트 23항** — 전원·NW·보안·서버·DB·운영
4. **위험도 매트릭스** — 영향도×확률 4단계
5. **대응 패턴 5종** — A-A·A-S·N+1·Hot/Cold Standby
6. **TTA 감리 양식** — 1쪽 권고안

💡 핵심 메시지 (TOP 3)

1. **TA는 구성도에서 SPOF를 찾아내는 사람** — 못 본 SPOF는 반드시 장애로
2. **위험도는 영향도×확률** — 비용·ROI 함께 본다
3. **수용 가능 SPOF도 의사결정** — 문서화·결재 필수

🇰🇷 표준 참조

- **국내**: TTA 가용성 점검 23항 · ISMS-P 2.9.2 · 행정기관 BCP · 전자금융감독규정 §17
- **글로벌**: ITIL 4 Availability · ISO 22301 BCM

Session 9 — *마무리*

📝 워크시트 D3-0

- 본 강의 직후 진행 (60분)
- 슬라이드 18·19·24·36 표준 그대로 활용
- 강사 답안 + 해설 별도

🎓 학습 가치

- **「SPOF 식별」은 모든 케이스 분석의 출발점**
- 본 회차 직후 RFP 분석·5 케이스에 그대로 적용
- 실무에서는 분기 1회 SPOF 점검 정착이 목표

💼 실무 적용 — 이번 주

1. **현재 시스템 구성도 5종** 점검 (오래된 것 갱신)
2. **23항 체크리스트** 직접 적용
3. **위험도 매트릭스** 작성 → CIO 보고
4. **수용 SPOF 등록부** 시작 (없다면 작성)
5. **분기 1회 점검** 일정 등록

🚀 GenAI Labs

강사 박수현 · 젠아이랩스(GenAI Labs) CEO / CTO