

# 푸드파이터 포트폴리오

침해사고 대응 기반 인프라 및 정보보호 체계 강화 사업

# 목차

정보 보호 컨설팅 기반 네트워크 웹 보안 사업

01

## 프로젝트 개요

프로젝트명  
정보보호 컨설팅 기반 네트워크·웹 보안 구축 프로젝트  
진행 기간 / 팀  
프로젝트(푸드파이터)  
본인 역할  
본인 역할

02

## 추진 배경 및 목표

서비스 운영 환경에서의 보안 위협 인식  
네트워크·웹 전반의 보호 체계 필요성  
보안 중심 설계를 목표로 한 프로젝트 수행

03

## 자산 식별 및 범위 정의

보호 대상 자산 식별  
네트워크·웹 취약 지점 분석  
주요 위협 시나리오 도출

04

## 보안 구조 설계

네트워크 분리 및 접근 통제 구조  
서버 및 계정 보안 정책  
웹 보안 대응 구조 설계

05

## 보안 대책 구현 및 검증

보안 설정 적용  
정책 적용 후 동작 확인  
공격 시나리오 기반 검증

06

## 결과 및 인사이트

보안 위협 대응 체계 구축 성과  
서비스 안정성 확보  
컨설팅 관점에서 얻은 실무적 인사이트

01

# 푸드파이터 프로젝트 개요

# 프로젝트 개요

정보보호 컨설팅 기반 네트워크·웹 보안 구축 프로젝트

## 목표

우리 사회의 보안 의식 향상

## 슬로건

해커의 식탁엔 우리  
이름이 없습니다

## 인재상

윤리적 사고  
열정  
책임감  
커뮤니케이션

# 프로젝트 개요

## 팀원 소개



김기수 / PM

전체 총괄  
네트워크 구축, 보안 장비  
PHP 웹서버 구축, 모의해킹



최장현 / PL

지사 리눅스 서버 구축  
MariaDB 구축, 모의해킹



이남혁 / 수행원

본사 리눅스 서버 구축  
PHP 웹서버 구축  
MariaDB 구축, 모의해킹



강버들 / 수행원

본사 네트워크 구축  
보안장비, 모의해킹



이태호 / 수행원

지사 네트워크 구축  
PHP 웹서버 구축,  
보안 장비, 모의해킹



이서진 / 수행원

윈도우 서버 구축  
MariaDB 구축, 모의해킹

# 프로젝트 개요

## 프로젝트 진행 기간

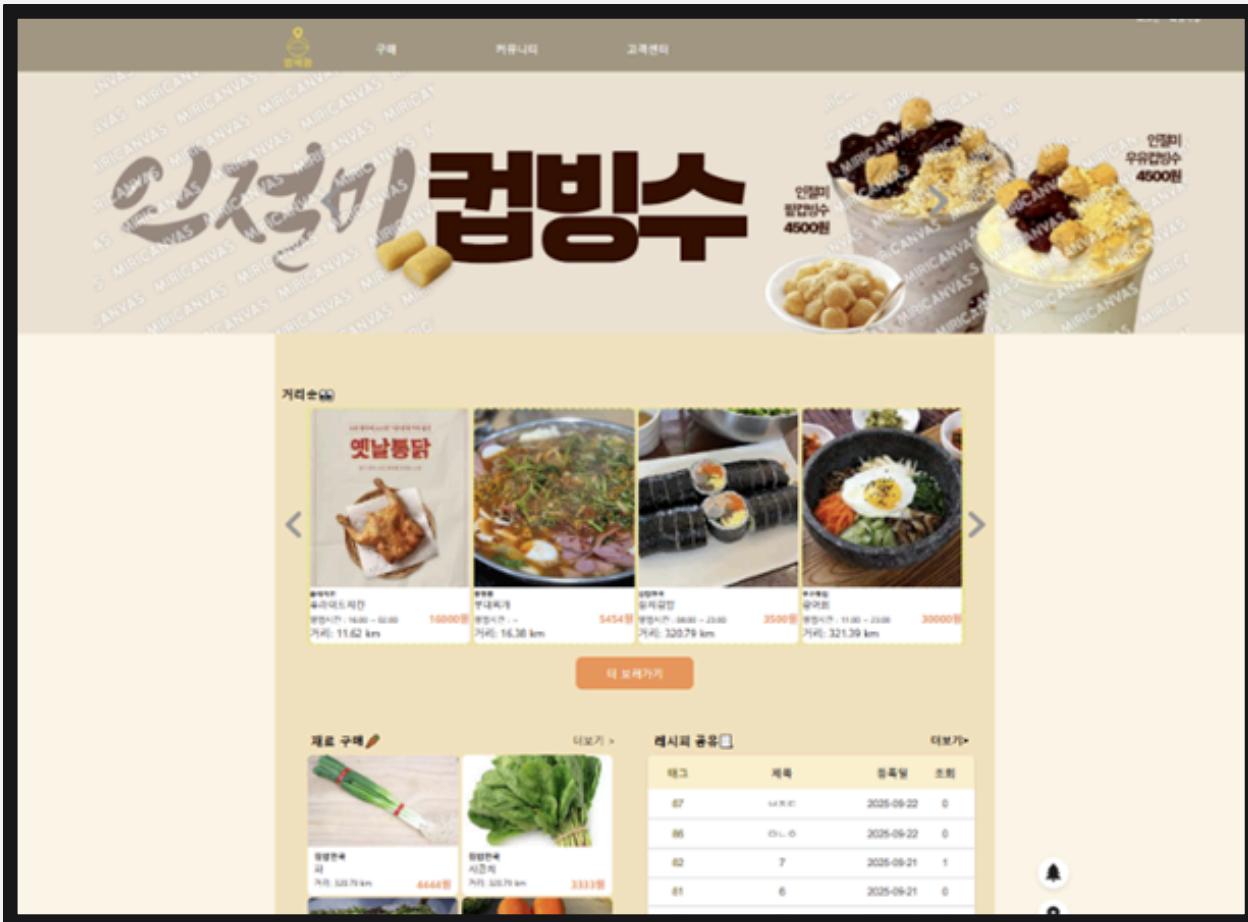
구조	Task	1w	2w	3w	4w	5w	6w
프로젝트 관리	제안서 작성	3일					
	킥 오프 미팅	1일					
	일정 수립	2일					
취약점 분석 및 평가	취약점 점검 대상 식별 및 분류	2일					
	취약점 본 점검(분석/평가)		5일				
	취약점 위험 분석/평가 수행		3일				
보안 정책 수립 및 조치 지원	취약점 개선 방안 도출		2일				
	취약점 조치 지원(보안설정)			7일			
	취약점 이행점검 수행				2일		
모의 해킹	모의해킹				3일		
문서화 및 보고	정보보안 지침 및 규정				3일		
	단기, 중기 보호대책 수립				2일		
	최종 보고					1일	

02

# 푸드파이터 추진 배경 및 목표

# 프로젝트 추진 배경

## 고객사 밥세권 서비스



판매자 잉여 재고 판매 + 저렴한 가격에 구매 가능



재고 최적화로 외식비  
절감과 환경 개선 실현



# 사업 목적

## 1. 사업개요

□ 사업명 : 2025년 밥세권서비스 취약점 분석 및 인프라 재구축

□ 사업기간 : 계약체결일 ~ A조

□ 주관부처 : 주관부처

구분	제안 요청
보안 진단 및 취약점	<ul style="list-style-type: none"><li>웹 서비스 및 인프라(서버, DBMS, 네트워크, 등)에 대한 종합 보안 점검 수행</li><li>OWASP Top 10 기반 웹 취약점 진단</li></ul>

## IV. 진단 대상 장비 구성

보안진단 대상

장비	장비 대수	점검대수	용도
PC(Windows)	36 대	10 대	각 부서/관리자 업무용 PC
웹 서버	1 대	1 대	홈페이지 / 고객 대상 서비스 제공
DNS 서버	1 대	1 대	도메인 주소 변환 서비스 운영
DB 서버	1 대	1 대	서비스 데이터 저장 및 관리
지사 로그 서버	1 대	1 대	시스템 및 보안 로그 저장
백업 서버	1 대	1 대	설정 및 DB 백업 데이터 저장
메일 서버	1 대	1 대	업무용 메일 송수신
SFTP 서버	1 대	1 대	네트워크 장비 설정

## 2. 추진 일정

안정화  
대한

정보  
시행

인프라  
보안

운영  
재능

VI. 투

## V. 제안요청 개요

### ● 제안서에 따른 내용으로 수행

### ● 자산 식별 및 분류

### ● 보안 구성 및 정책 분석

### ● 취약점 점검 및 위험도 평가

### ● 개선 조치 방안 수립

### ● 보고서 작성 및 전달

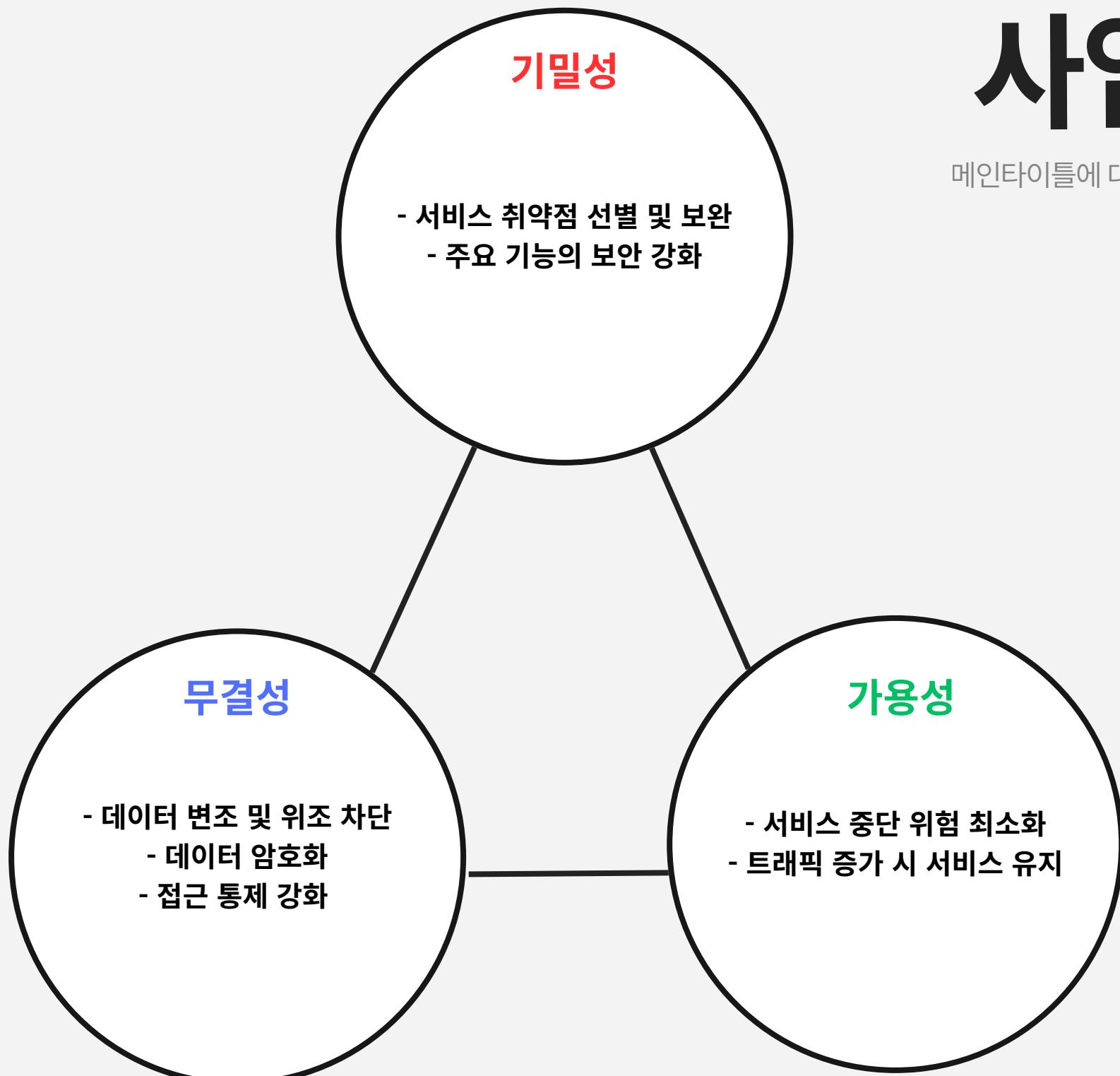
# 사업 목표

메인타이틀에 대한 세부 설명을 입력해 주세요.

## ✓ 이미지로 설득력을 높이는 레이아웃

사진 중심 레이아웃은 비주얼 임팩트를 높이고 싶은 프레젠테이션에 적합한 방식입니다. 시각 자료를 메인으로 활용해 내용을 설명하고 설득력을 높이기 위한 용도로 자주 사용됩니다.

사진을 화면의 전체 또는 상당 부분에 배치하고, 텍스트는 이미지 위나 하단에 간략하게 배치하여 메시지의 힘을 극대화할 수 있습니다. 주제와 가장 밀접하게 연결된 이미지를 선정하여 청중의 공감과 이해를 끌어낼 수 있도록 구성하는 것이 중요합니다.



# 공격 시나리오



✓ 서비스 이용 고객의 공격 예고

@NamhyuxTorvalds 트윗 스레드  
"식중독에 분노한 개발자의 폭수 선언" · 2025년 10월 31일

남혁스 토발즈 @NamhyuxTorvalds  
Seoul, South Korea - 2025.10.31

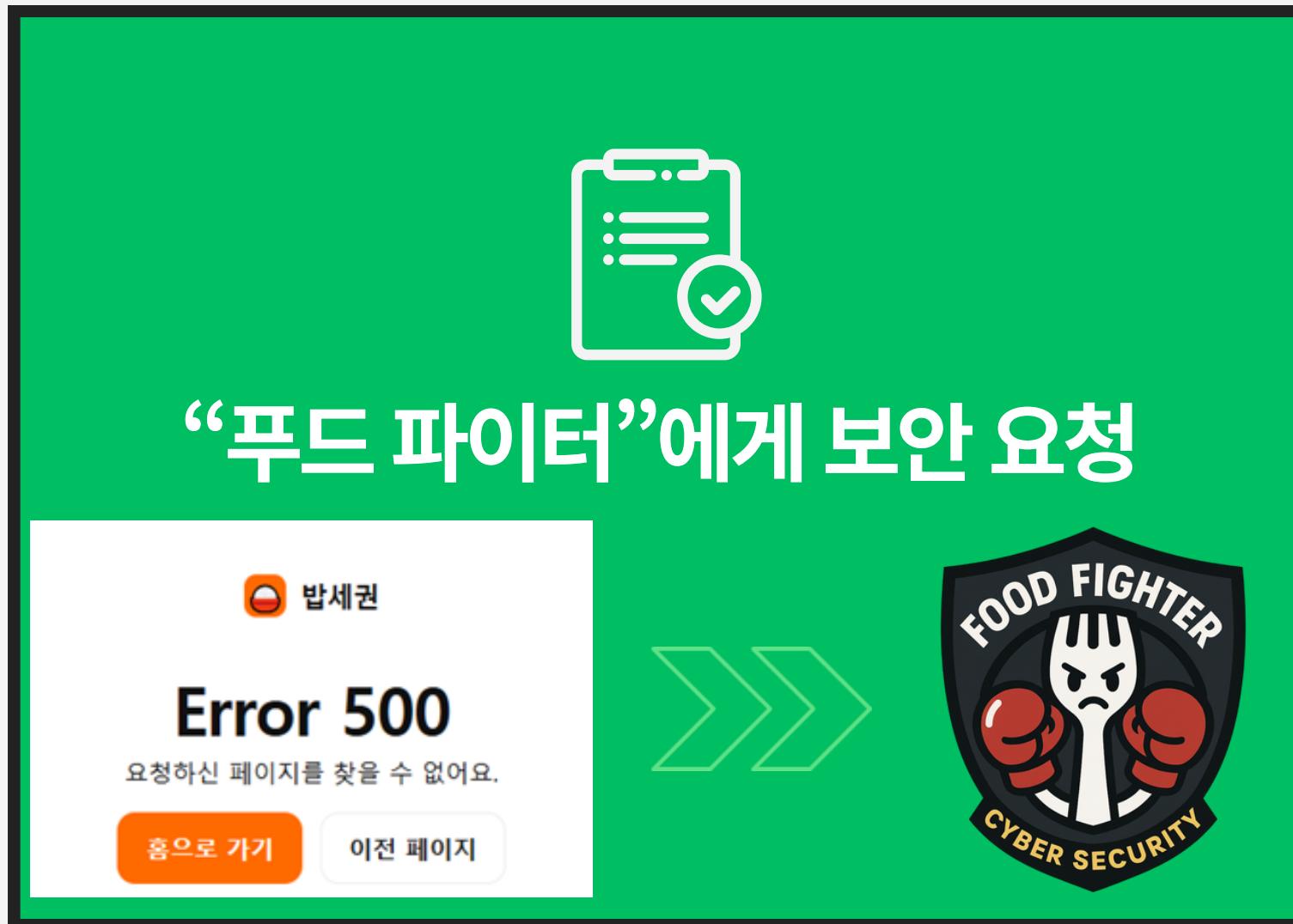
건방진 고객센터 직원에게 큰 실망을 했다.  
"기한임박 상품"이라길래 자신있게 주문했는데,  
그건 개이득이 아니라 사망 직전 빌드였다. 😱  
#BapGate #LinuxToLunch

312 1,204 8,329

남혁스 토발즈 @NamhyuxTorvalds  
2/8

내 위장이 지금 커널 패닉 중이다.

# 공격 시나리오



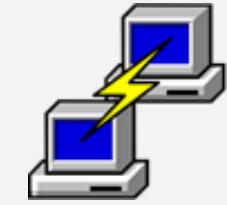
- 01 | 모든 네트워크 보안 설정 비활성화
- 02 | 밥세권 보안팀의 미흡한 초기 대응
- 03 | 데이터 베이스 삭제
- 04 | 밥세권 서비스 마비 & 보안 요청

# 사용 툴

## 사용 도구



GNS 1.5.3



Putty 0.83



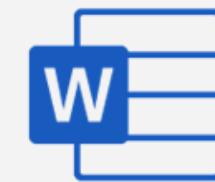
VMWare 17.6.2



Packet Tracer 8.2.2



Wireshark 4.4.9



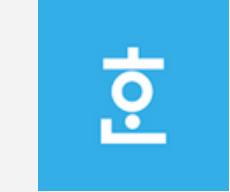
Word



PowerPoint



Excel



한글

## 협업 도구



Notion



Discord



Google Drive



KakaoTalk



NAS Server

# 사용 툴

## 사용 장비



Windows Server 2016  
Windows 10



Rocky Linux 8.1



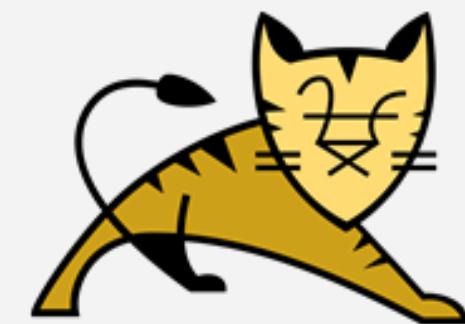
Sophos 9



kali 2024.4-amd64



PHP Server 7.2.24



Apache Tomcat 9.0



Cisco Router : Cisco 3660 Series 12.4(15)T9  
Cisco L3 SW : Cisco 3745 Router 12.4(11)T



CentOS 7

03

# 푸드파이터 자산 식별 및 범위 정의

# 자산 범위

분류	역할	본사	지사	합계
PC	부서별 PC	36 대	30 대	66 대
Window Servers	DNS, DHCP	2 대	2 대	4 대
Linux Server	SFTP, Mail, Log, DB, Backup, Web	6 대	6 대	12 대
L2 Switch	스위치, VLAN 세팅	4 대	3 대	7 대
L3 Switch	백본, 스위치, 라우팅	4 대	4 대	8 대
L4 Switch	로드 밸런싱	2 대	0 대	2 대
Security Device	UTM, WAF, 방화벽	3 대	2 대	5 대
총합		58 대	46 대	104 대

# 평가 기준

점검 범위



# 평가 기준

## 점검 범위



- 주요 정보통신 기반 시설 및 전자금융 기반 시설 취약점 평가 방법을 기준으로 점검 체계를 수립
- 서버(UNIX, WINDOWS), DBMS, 보안장비, 네트워크, 웹 영역별 보안 통제 항목을 기준에 따라 점검
- 취약점 파악 및 실제 점검 수행을 통해 전반적인 보안 수준을 평가

# UNIX 점검항목

주요 정보 통신 기반	전자 금융 기반	위험도	점검 항목
U-02	SRV-075	상	패스워드 복잡성 설정
U-03	SRV-127	상	계정 잠금 임계값 설정
U-04	SRV-012	상	패스워드 파일 보호
U-05	SRV-121	상	root 홈, 패스 디렉터리 권한 및 패스 설정
U-06	SRV-096	상	파일 및 디렉터리 소유자 설정
U-07	SRV-096	상	/etc/passwd 파일 소유자 및 권한 설정
U-13	SRV-091	상	SUID, SGID, Sticky bit 설정 파일 점검
U-14	SRV-095	상	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
U-37	SRV-042	상	웹 서비스 상위 디렉토리 접근 금지
U-46	SRV-069	중	패스워드 최소 길이 설정

# Windows 점검항목

주요 정보 통신 기반	전자 금융 기반	위험도	점검 항목
W-01	SRV-072	상	Administrator 계정 이름 변경 또는 보안성 강화
W-02	SRV-078	상	Guest 계정 비활성화
W-06	SRV-073	상	관리자 그룹에 최소한의 사용자 포함
W-07	SRV-020	상	공유 권한 및 사용자 그룹 설정
W-08	SRV-018	상	하드디스크 기본 공유 제거
W-29	SRV-066	상	DNS Zone Transfer 설정
W-30	SRV-034	상	RDS(Remonte Data Services) 제거
W-34	SRV-115	상	로그의 정기적 검토 및 보고
W-63	SRV-173	중	DNS 서비스 구동 점검
W-71	SRV-062	중	원격에서 이벤트 로그파일 접근 차단

# DBMS 점검항목

주요 정보 통신 기반	전자 금융 기반	위험도	점검 항목
D-01	DBMS-001	상	기본 계정의 패스워드, 권한 등을 변경하여 사용
D-02	DBMS-003	상	데이터베이스의 불필요 계정을 제거하거나, 잠금설정 후 사용
D-03	DBMS-007	상	패스워드의 사용기간 및 복잡도를 기관 정책에 맞도록 설정
D-04	DBMS-004	상	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
D-05	DBMS-013	상	원격에서 DB 서버로의 접속 제한
D-06	DBMS-004	상	DBA 이외의 인가되지 않은 사용자 시스템 테이블에 접근할 수 없도록 설정
D-10	DBMS-016	상	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용
D-13	DBMS-020	중	DB 사용자 계정을 개별적으로 부여하여 사용
D-17	DBMS-022	중	데이터베이스의 주요 설정 파일, 패스워드 파일 등과 같은 파일들의 접근 권한 설정
D-21	DBMS-024	중	인가되지 않은 GRANT OPTION 사용 제한

# 보안장비 점검항목

주요 정보 통신 기반	전자 금융 기반	위험도	점검 항목
S-01	ISS-017	상	보안장비 Default 계정 변경
S-02	ISS-018	상	보안장비 Default 패스워드 변경
S-03	ISS-020	상	보안장비 계정별 권한 설정
S-04	ISS-019	상	보안장비 계정 관리
S-05	ISS-021	상	보안장비 원격 관리 접근 통제
S-06	ISS-016	상	보안장비 보안 접속
S-07	ISS-024	상	Session timeout 설정
S-08	ISS-005	상	벤더에서 제공하는 최신 업데이트 적용
S-09	ISS-001	상	정책 관리
S-10	ISS-004	상	NAT 설정

# 네트워크 장비 점검항목

주요 정보 통신 기반	전자 금융 기반	위험도	점검 항목
N-01	NET-56	상	패스워드 설정
N-02	NET-12	상	패스워드 복잡도 설정
N-03	NET-11	상	암호화된 패스워드 사용
N-14	NET-52	상	사용하지 않는 인터페이스의 Shutdown 설정
N-05	NET-14	상	Session Timeout 설정
N-06	NET-48	상	최신 보안 패치 및 벤더 권고사항 적용
N-12	NET-40	상	Spoofing 방지 필터링 적용 또는 보안장비 사용
N-13	NET-47	상	DDoS 공격 방어 설정 또는 DDoS 장비 사용
N-29	NET-30	중	CDP 서비스 차단
N-32	NET-26	중	Proxy ARP 차단

# WEB 점검항목

주요 정보 통신 기반	전자 금융 기반	위험도	점검 항목
FU	SER-002	상	악성파일 업로드
FD	SER-010	상	파일 다운로드
AE	SER-039	상	관리자 페이지 노출 여부
IN	SER-003	상	부적절한 이용자 인가 여부
SC	SER-033	상	불충분한 세션종료 처리
XS	SER-041	상	크로스사이트 스크립팅 (XSS)
CF	SER-028	상	크로스사이트 요청변조 (CSRF)
DI	SER-029	상	디렉토리 목록 노출
IL	SER-020	상	화면 내 중요정보 평문노출 여부
SI	SER-001	상	SQL Injection

04

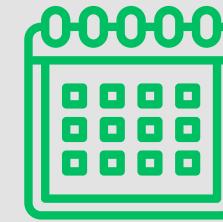
# 푸드파이터 보안구조설계

# 기존 인프라 문제점



## 장비 이중화 미비

단일 장비 장애 시 전체 서비스 마비



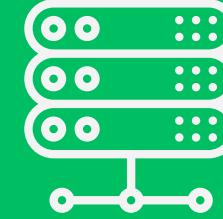
## 보안 장비 없음

DDOS, 웹 해킹 등 외부 공격에 취약



## DMZ 내부망 구분 없음

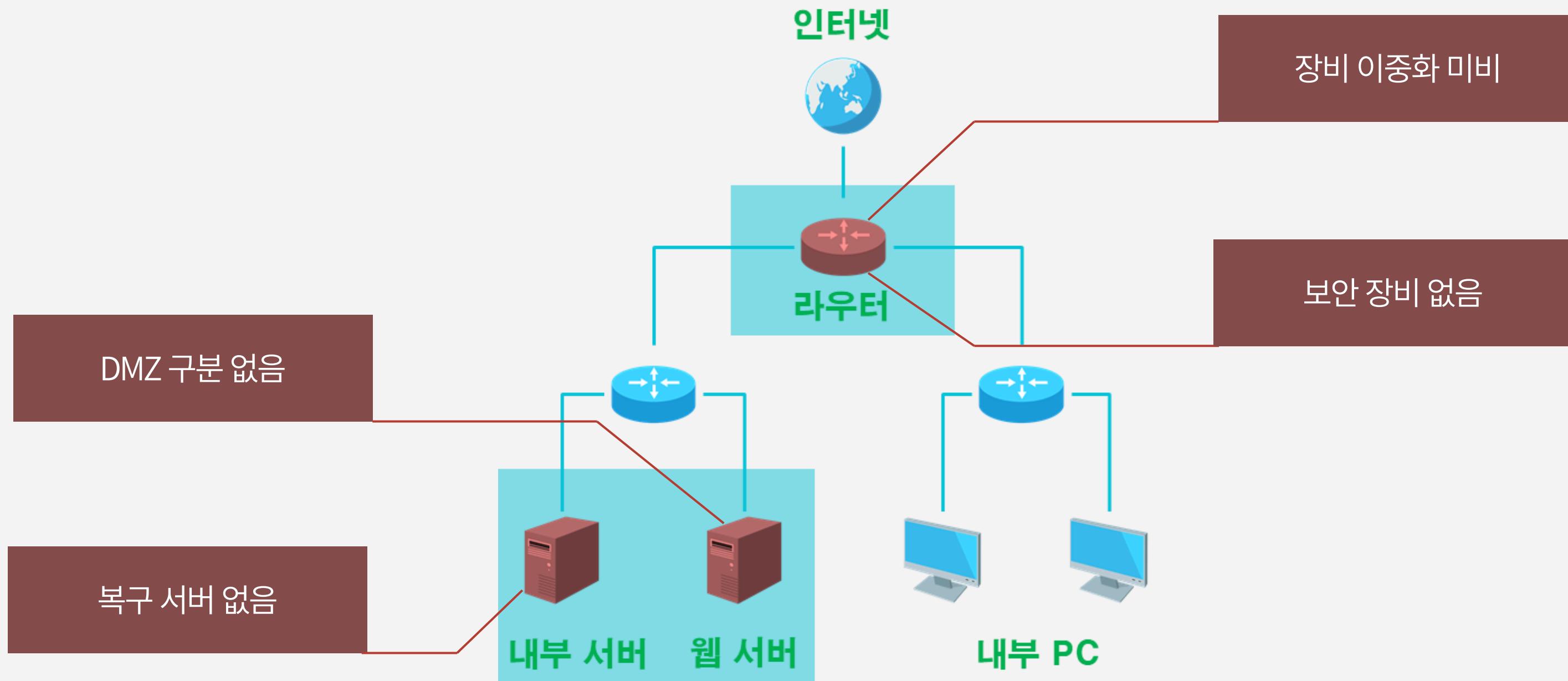
내부망 직접 노출 및 침투 용이



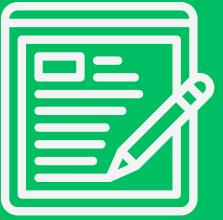
## 복구 서버 없음

데이터 손실 시 복구 불가

# 기존 인프라 문제점

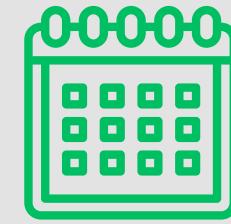


# 개선된 인프라



## 네트워크 장비 이중화

장애 시 자동 전환, 무중단 운영 가능



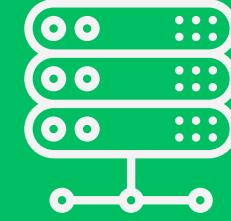
## UTM 장비 도입

DDOS 방어, IPS/IDS 탐지 가능



## NAT 기반 망분리

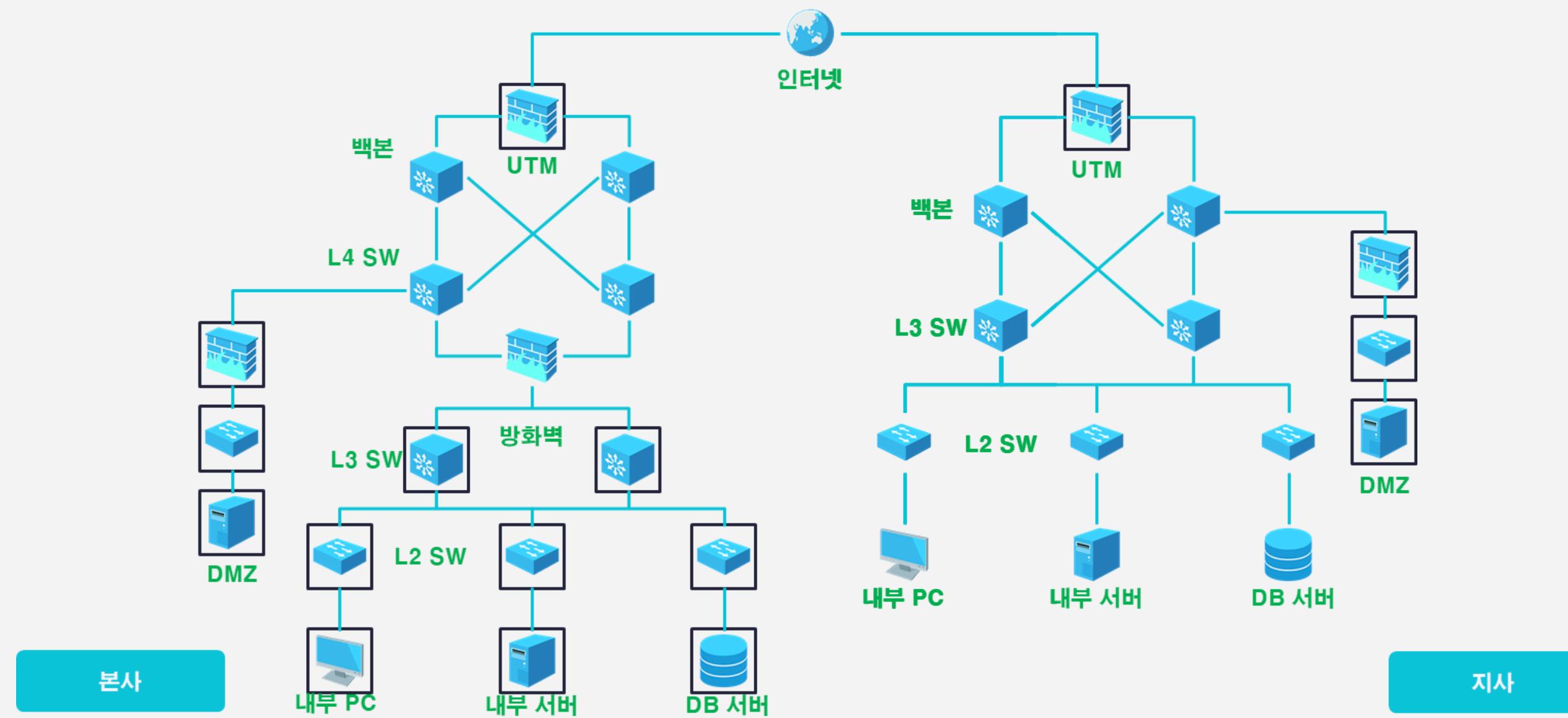
서비스 망 / 업무망 논리적 분리



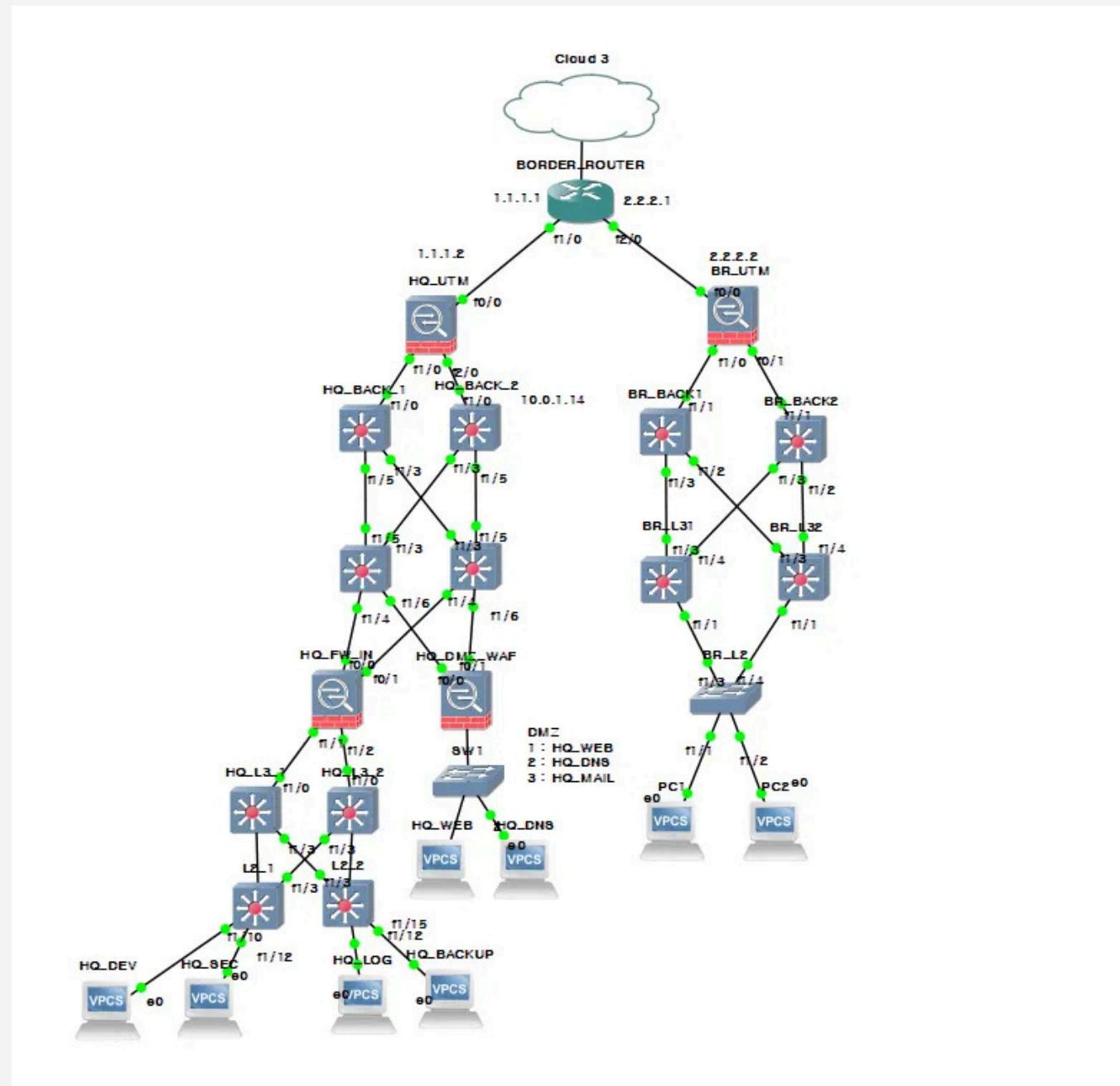
## 로그 및 파일 백업 서버 구성

데이터 손실 시 대응 체계 마련

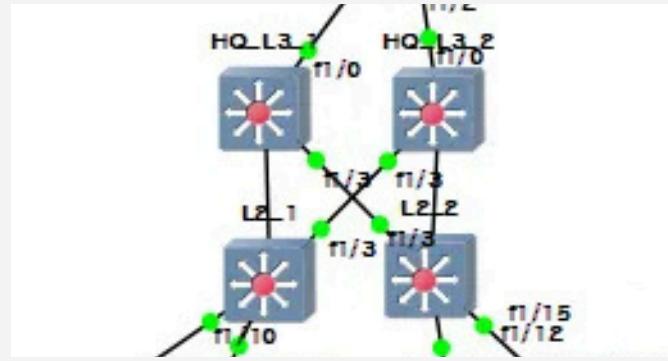
# 개선된 인프라



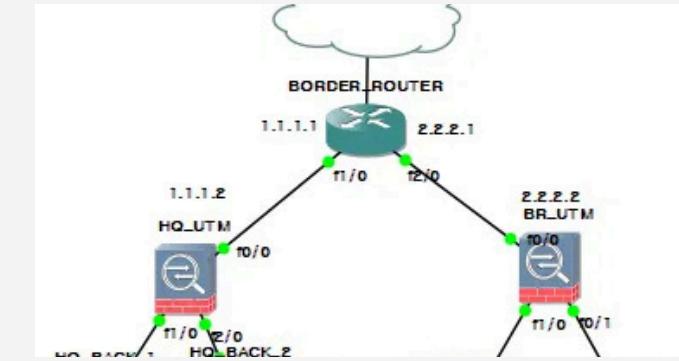
# 인프라 가상 구축



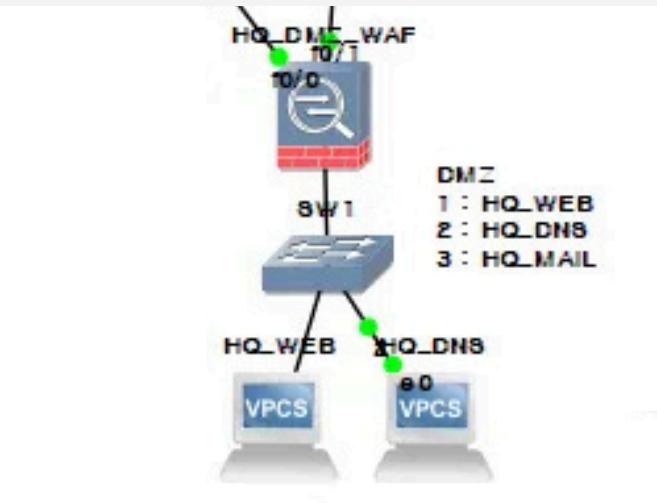
# 인프라 가상 구축



네트워크 장비 이중화



UTM 장비 도입



NAT 기반 망분리



로그 및 파일 백업 서버 구성

# 개선 현황

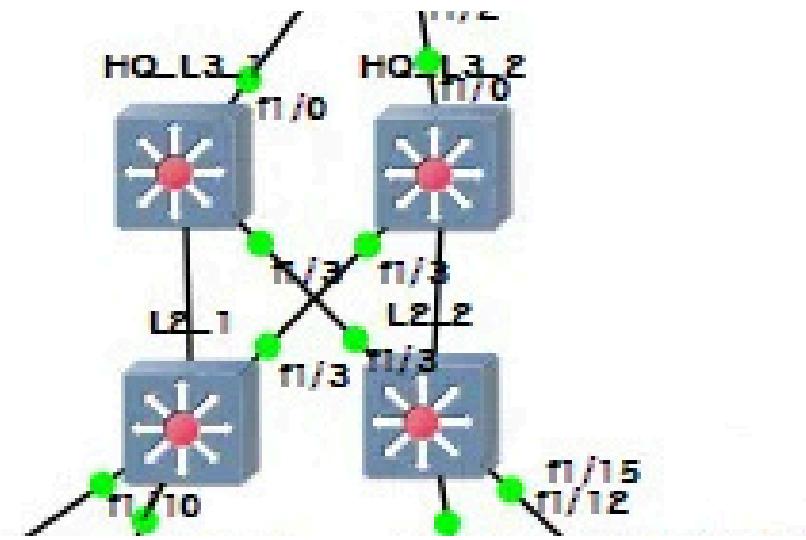
인프라 개선 이전 vs 이후

## 장비 이중화 미비

단일 장비 사용으로 인한 장애 시 서비스 중단 위험

VS

## 네트워크 장비 이중화



# 개선 현황

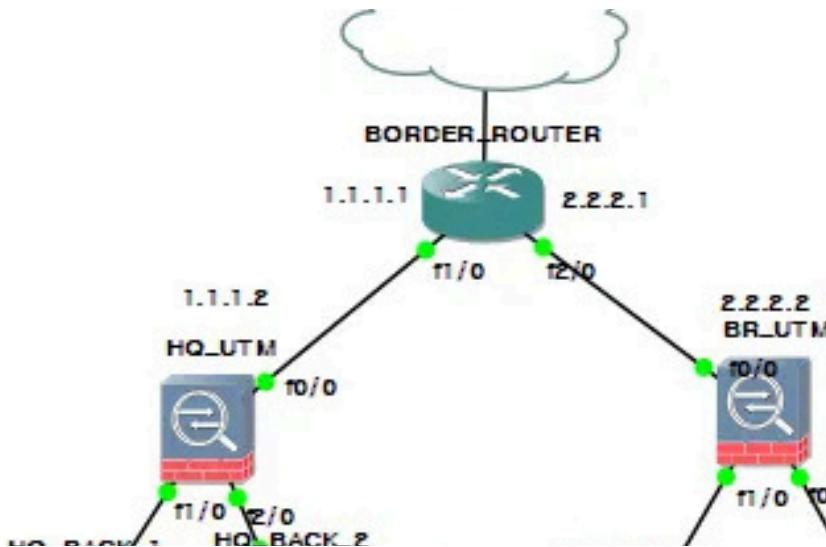
인프라 개선 이전 vs 이후

보안 장비 없음

보안 장비 미구축으로 외부 공격 및 내부 침해  
대응 불가 위험

VS

UTM 장비 도입



# 개선 현황

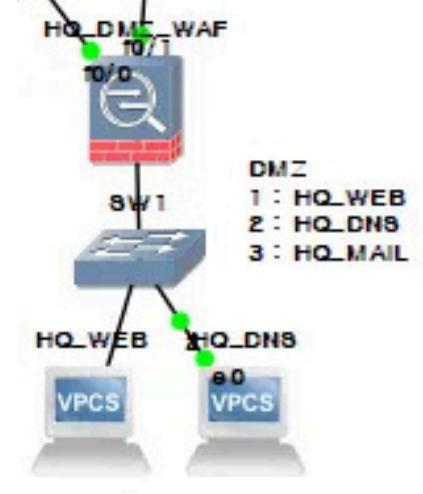
인프라 개선 이전 vs 이후

**DMZ 내부방 구분 없음**

DMZ와 내부망 미분리로 인한  
내부 시스템 직접 노출 위험

**VS**

**NAT 기반 망분리**



# 개선 현황

인프라 개선 이전 vs 이후

복구 서버 없음

백업·복구 체계 부재로 장애 발생 시  
데이터 유실 및 복구 지연 위험

VS

로그 및 파일 백업 서버 구성

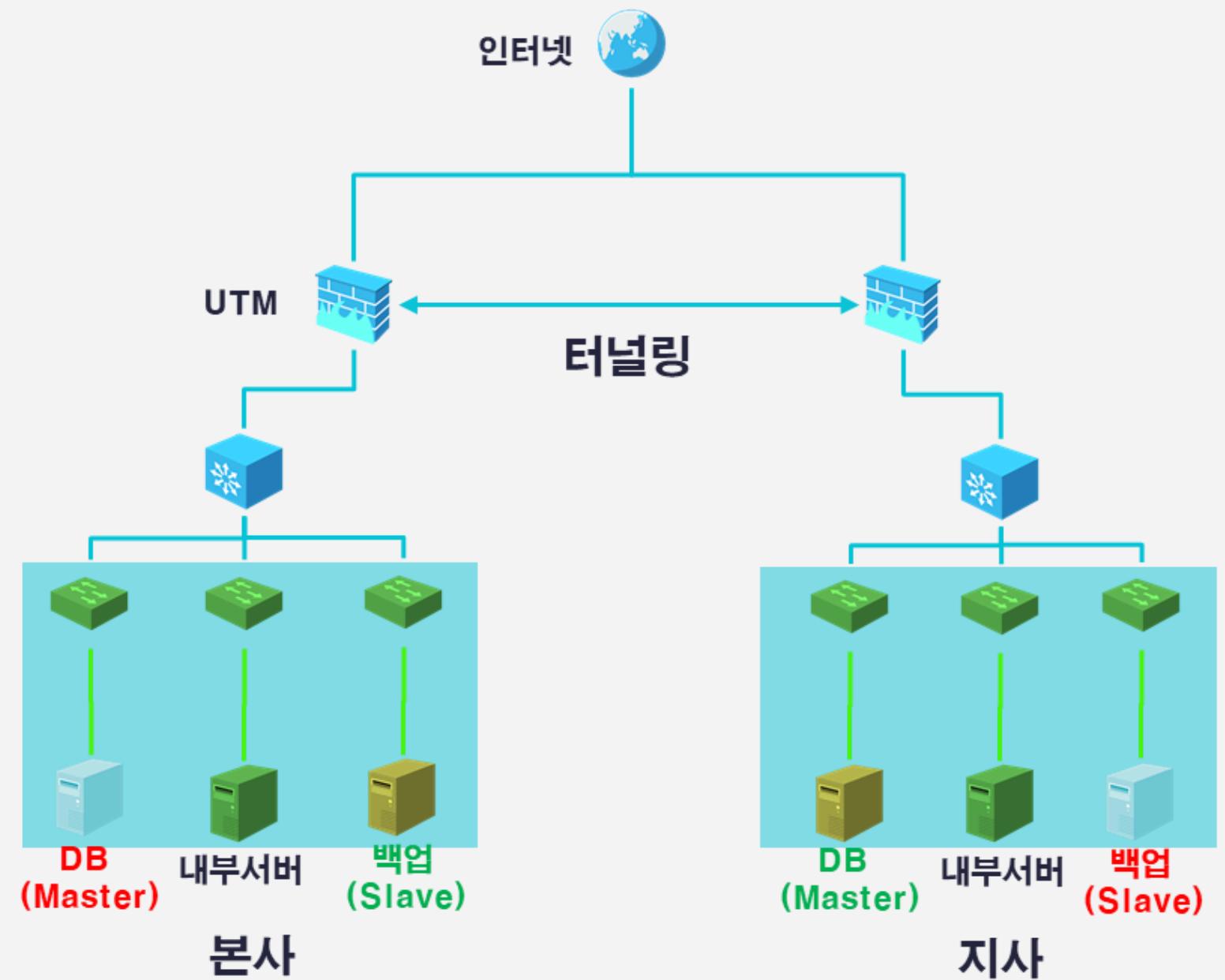


05

# 푸드파이터 보안 대책 구현 및 검증

# 이남혁

- 본사 리눅스 서버 보안 점검 및 구축
- DB 이중화(Master-Slave) 및 암호화
- 백업 서버 구축
- PHP 웹서버(관리자 페이지) 구축
- 관리자 페이지 모의해킹 및 방어



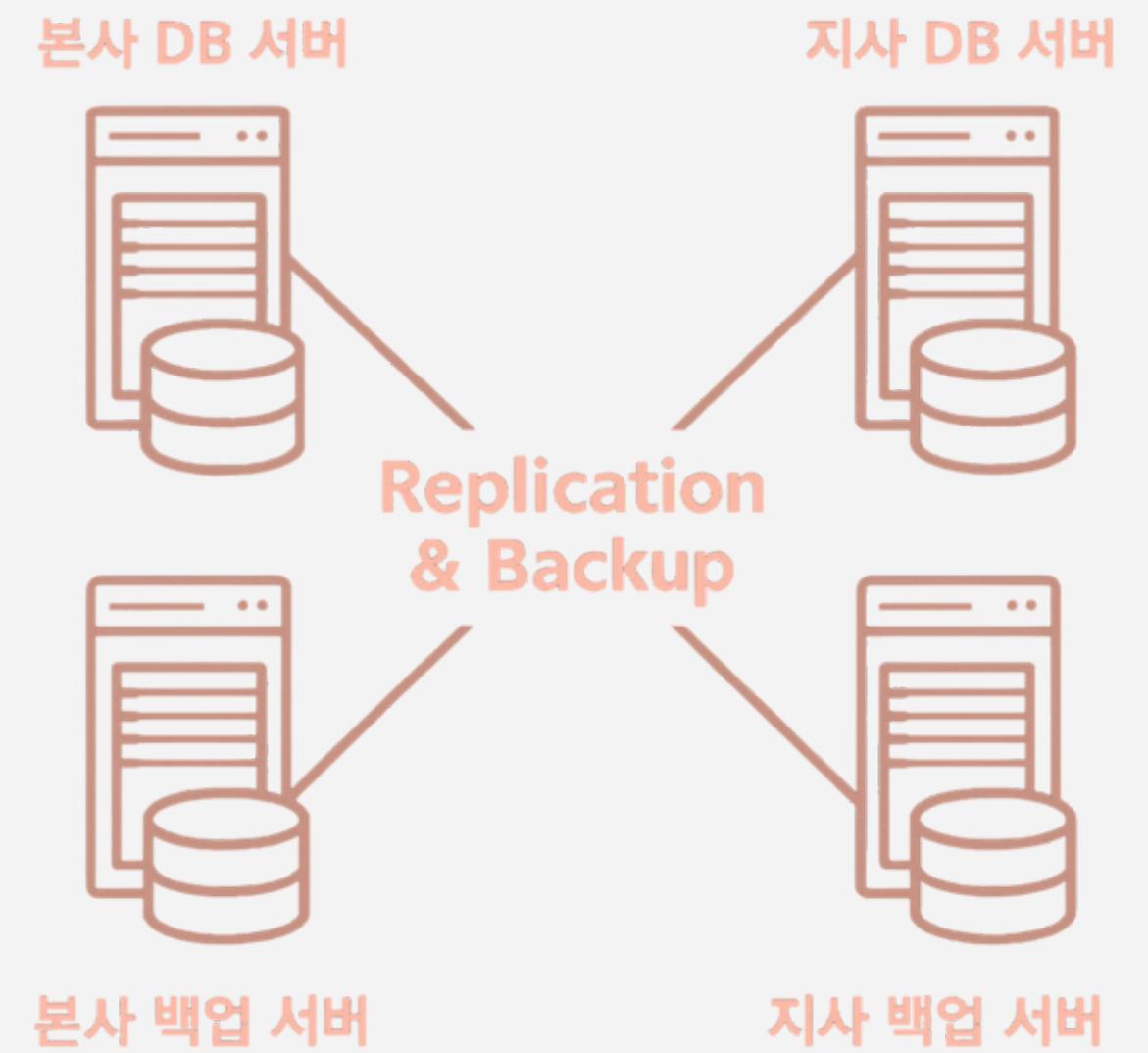
# 본사 리눅스 서버 보안 점검 및 구축

- 본사 SFTP/MAIL/LOG/DB/BACKUP 서버 취약점 점검 및 보안 점검 실행
- 주요 정보통신기반시설 취약점 가이드에 따라 보안 점검 후 조치 이행
- 서버 간 연동 구조, 필요 계정 등 논의

● 본사 SFTP서버 → 지사 백업서버	남혁	● 완료
● 본사 LOG서버 ↔ 지사 백업서버	남혁	● 완료
● 본사 MAIL서버 ↔ 지사 백업서버	남혁	● 완료
● 본사 DB(master) ↔ 지사 백업서버(slave) 이중화	남혁	● 완료
● 본사-보안 DB서버-보안설정	남혁	● 완료
● 본사 DB서버 - DBMS 주통기반 상세점검(1차)	남혁	● 완료
● 지사-보안 BACKUP서버-보안 점검	남혁	● 완료
● 본사-보안 DB서버-보안 점검	남혁	● 완료
● 본사-보안 MAIL서버-보안 점검	남혁	● 완료
● 본사 -보안 SFTP서버-보안 점검	남혁	● 완료
● 본사-보안 LOG서버-보안 점검	남혁	● 완료
● 본사 서버 연동 구조	남혁	● 완료
● 본사-LOG서버_보안설정	남혁	● 완료
● 본사-SFTP서버_보안설정	남혁	● 완료
● 본사-MAIL서버_보안설정	남혁	● 완료

# 본사·지사 DB 이중화

- 본사·지사 간 DB 이중화 구조 구축으로 데이터 안정성 확보
- Master-Slave 구조 기반으로 데이터 변경 사항을 실시간 복제
- 복제본을 통해 조회 트래픽 분산 및 운영 안정성 강화



# 본사·지사 DB 이중화 - 동기화

- 덤프로 동일한 데이터 기준을 맞춘 뒤,  
Master 변경사항이 Slave로 실시간 전  
달 시작
- Slave의 IO·SQL 동작 상태가 모두 정상  
으로 표시되어 복제 과정에 오류가 없음

```
[root@HQ_DB_SEC backup]# mysqldump -u root -p -A > /backup/all_1126.sql
Enter password:
[root@HQ_DB_SEC backup]# scp /backup/all_1126.sql 20.0.0.89:/backup
root@20.0.0.89's password:
all_1126.sql                                              100% 1998KB   1.3MB/s   00:01
[root@HQ_DB_SEC backup]# 
[root@BR_BACKUP_SEC ~]# cd /backup
[root@BR_BACKUP_SEC backup]# ll
합계 4000
-rw-r--r--. 1 root root 2045556 11월 26 23:34 all.sql
-rw-r--r--. 1 root root 2045553 11월 26 23:42 all_1126.sql
[root@BR_BACKUP_SEC backup]# 
MariaDB [(none)]> START SLAVE;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW SLAVE STATUS\G;
***** 1. row *****
Slave_IO_State: Waiting for master to send event
Master_Host: 10.0.0.73
Master_User: slave
Master_Port: 3306
Connect_Retry: 60
Master_Log_File: mysql-bin.000004
Read_Master_Log_Pos: 342
Relay_Log_File: mariadb-relay-bin.000002
Relay_Log_Pos: 555
Relay_Master_Log_File: mysql-bin.000004
Slave_IO_Running: Yes
Slave_SQL_Running: Yes
Replicate_Do_DB: babseguen
```

# 본사·지사 DB 이중화 - 복제 검증

- Master(DB서버) : 모든 원본 데이터 처리 및 쓰기 연산 담당
- Slave(백업서버) : 실시간 읽기 전용 복제본 유지
- 서비스 장애 시 Slave를 활용하여 데이터 손실 최소화

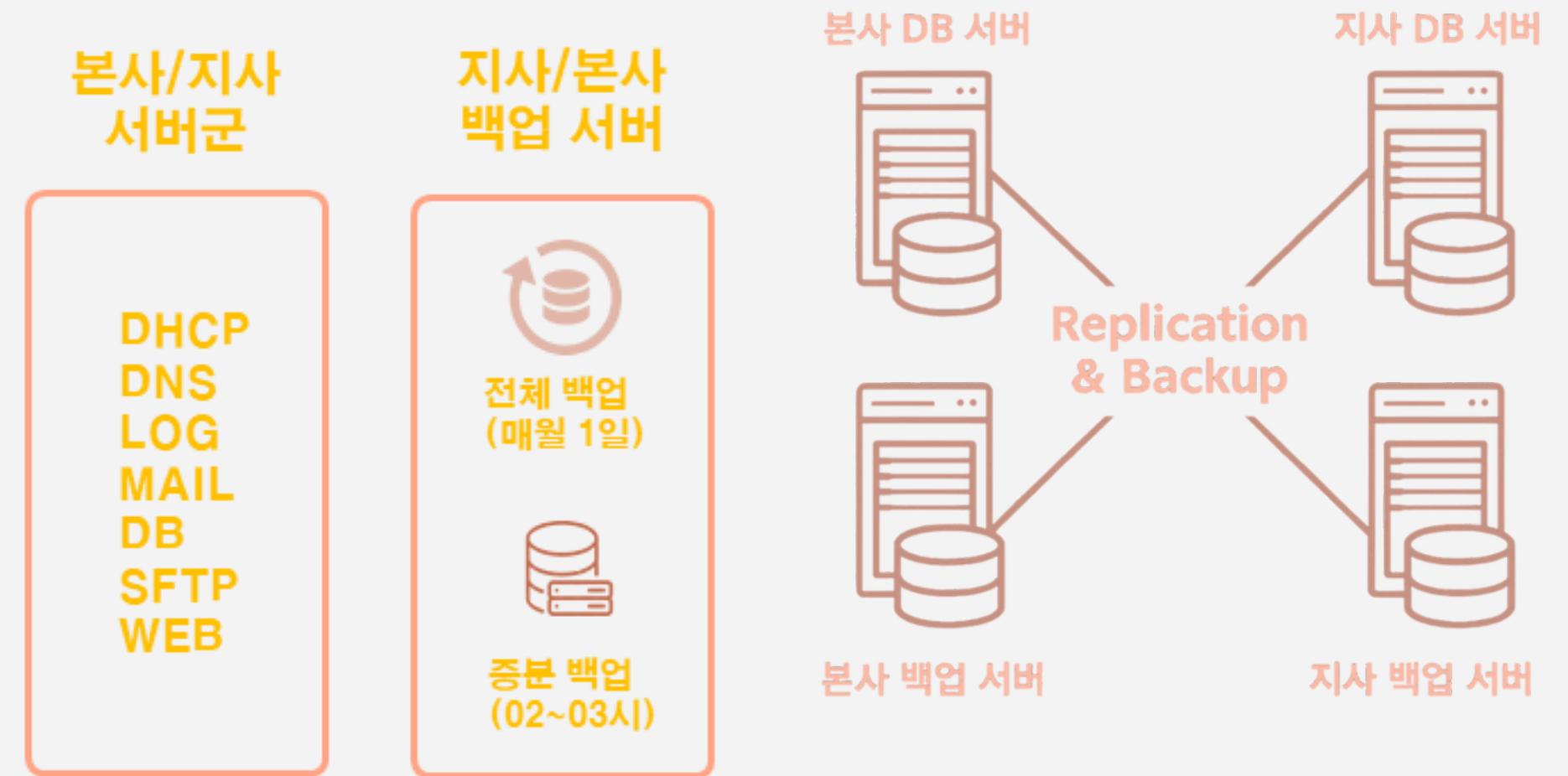
```
[root@HQ_DB_SEC backup]# mysqldump -u root -p -A > /backup/all_1126.sql
Enter password:
[root@HQ_DB_SEC backup]# scp /backup/all_1126.sql 20.0.0.89:/backup
root@20.0.0.89's password:
all_1126.sql                                              100% 1998KB   1.3MB/s   00:01
[root@HQ_DB_SEC backup]# 

[root@BR_BACKUP_SEC ~]# cd /backup
[root@BR_BACKUP_SEC backup]# ll
합계 4000
-rw-r--r--. 1 root root 2045556 11월 26 23:34 all.sql
-rw-r--r--. 1 root root 2045553 11월 26 23:42 all_1126.sql
[root@BR_BACKUP_SEC backup]# 
MariaDB [(none)]> START SLAVE;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> SHOW SLAVE STATUS\G;
***** 1. row *****
Slave_IO_State: Waiting for master to send event
Master_Host: 10.0.0.73
Master_User: slave
Master_Port: 3306
Connect_Retry: 60
Master_Log_File: mysql-bin.000004
Read_Master_Log_Pos: 342
Relay_Log_File: mariadb-relay-bin.000002
Relay_Log_Pos: 555
Relay_Master_Log_File: mysql-bin.000004
Slave_IO_Running: Yes
Slave_SQL_Running: Yes
Replicate_Do_DB: babseguen
```

# 백업 서버 구축

- 본사·지사 백업 서버 구축으로 데이터 보호 체계 강화
- 전체 백업 : 특정 시점의 전체 데이터를 통째로 백업하는 방식
- 증분 백업 : 이전 백업 이후 변경된 데이터만 저장하는 방식



# 백업 서버 구축

본사/지사  
서버군

지사/본사  
백업 서버

DHCP  
DNS  
LOG  
MAIL  
DB  
SFTP  
WEB



전체 백업  
(매월 1일)



증분 백업  
(02~03시)

- 서비스별 분리 저장 구조 설계

- DB만 전체 + 증분 백업을 사용, 나머지  
서버는 파일 단위 전체 백업 방식

```
[root@BR_BACKUP_SEC backup]# ll
```

```
합계 32
```

```
drwxrwx---. 4 root backup 4096 11월 28 00:00 dhcp
drwxrwx---. 4 root backup 4096 11월 28 00:00 dns
drwxrwx---. 4 root backup 4096 11월 28 00:00 log
drwxrwx---. 4 root backup 4096 11월 28 00:00 mail
drwxrwx---. 4 root backup 4096 11월 27 11:32 mariadb
drwxrwx---. 4 root backup 4096 11월 28 00:00 sftp
drwxrwx---. 2 root backup 4096 11월 27 11:51 tmp
drwxrwx---. 4 root backup 4096 11월 28 00:00 web
```

# 백업 서버 구축

- 백업 서버로 수신된 전체 백업,  
증분 백업을 일자별로 체계적으로 저장

```
[root@BR_BACKUP_SEC mariadb]# ll
합계 8
drwxr-x---. 4 root backup 4096 12월  9 12:11 full
drwxr-x---. 15 root backup 4096 12월  9 11:53 inc
[root@BR_BACKUP_SEC mariadb]# cd full
[root@BR_BACKUP_SEC full]# ll
합계 8
drwxr-x---. 6 root backup 4096 11월 27 02:00 2025-11-27
drwxr-x---. 6 root backup 4096 12월  1 02:00 2025-12-01
[root@BR_BACKUP_SEC full]# cd ../inc
[root@BR_BACKUP_SEC inc]# ll
합계 52
drwxr-x---. 6 root backup 4096 11월 26 02:10 2025-11-26
drwxr-x---. 6 root backup 4096 11월 27 02:10 2025-11-27
drwxr-x---. 2 root backup 4096 11월 28 02:10 2025-11-28
drwxr-xr-x. 2 root root    4096 11월 29 02:10 2025-11-29
drwxr-xr-x. 2 root root    4096 11월 30 02:10 2025-11-30
drwxr-xr-x. 2 root root    4096 12월  2 02:10 2025-12-02
drwxr-xr-x. 2 root root    4096 12월  3 02:10 2025-12-03
drwxr-xr-x. 2 root root    4096 12월  4 02:10 2025-12-04
drwxr-xr-x. 2 root root    4096 12월  5 02:10 2025-12-05
drwxr-xr-x. 2 root root    4096 12월  6 02:10 2025-12-06
drwxr-xr-x. 2 root root    4096 12월  7 02:10 2025-12-07
drwxr-xr-x. 2 root root    4096 12월  8 02:10 2025-12-08
drwxr-xr-x. 2 root root    4096 12월  9 02:10 2025-12-09
```

# 백업 복구 무결성 검증

- 백업 파일 단위의 해시 비교로 무결성 검증 수행
- 문제가 되었던 LSN 불일치 오류는 prepare 단계에서 최초로 감지
- 모든 서비스 파일을 SHA256 기반으로 검증하여 전체 백업 체계 안정성 확보

```
INC_DIR="$BASE/mariadb/inc"
mkdir -p "$HASH_BASE/mariadb/inc"

for dir in "$INC_DIR"/*; do
    if [[ -d "$dir" ]]; then
        for file in "$dir"/*; do
            if [[ -f "$file" ]]; then
                HASHFILE="$HASH_BASE/mariadb/inc/${basename $dir}_${basename $file}.sha256"
                check_file_integrity "$file" "$HASHFILE"
            fi
        done
    fi
done
```

```
FULL_DIR="$BASE/mariadb/full"
mkdir -p "$HASH_BASE/mariadb/full"

for dir in "$FULL_DIR"/*; do
    if [[ -d "$dir" ]]; then
        echo "[INFO] FULL 백업 prepare 테스트 : $dir" >> "$LOGFILE"
        mariabackup --prepare --target-dir="$dir" >> "$LOGFILE" 2>&1
```

```
SERVICES=("dhcp" "dns" "log" "mail" "sftp" "web")

for svc in "${SERVICES[@]}"; do
    echo "---- [$svc] ----" >> "$LOGFILE"
    mkdir -p "$HASH_BASE/$svc"

    for file in $(find "$BASE/$svc" -type f); do
        HASHFILE="$HASH_BASE/$svc/$(echo $file | sed 's/\//_/g').sha256"
        check_file_integrity "$file" "$HASHFILE"
    done
done
```

# 백업 복구 무결성 검증

- 전체 백업의 LSN 구조가 정상적으로 기록되어 백업본 자체의 무결성이 확인됨
- 백업 서버에서 필수 파일 (LSN, binlog, 데이터파일) 모두 온전함
- 백업 수신·무결성 검증·로그 정리가 자동 스케줄로 구성된 백업 운영 체계 구축

```
[root@HQ_DB_SEC ~]# cat /backup/db/full-2025-12-03/xtrabackup_checkpoints
backup_type = full-backuped
from_lsn = 0
to_lsn = 1743798
last_lsn = 1743807
[root@HQ_DB_SEC ~]# ll
[root@BR_BACKUP_SEC full]# ll
합계 8
drwxr-x---. 6 root backup 4096 11월 27 02:00 2025-11-27
drwxr-x---. 6 root backup 4096 12월 1 02:00 2025-12-01
```

```
[root@BR_BACKUP_SEC full]# cd 2025-12-01/
[root@BR_BACKUP_SEC 2025-12-01]# ll
합계 12344
-rw xr-x---. 1 root backup 16384 12월 1 02:00 aria_log.00000001
-rw xr-x---. 1 root backup 52 12월 1 02:00 aria_log_control
drwxr-x---. 2 root backup 4096 12월 9 11:52 babseguen
drwxr-x---. 2 root backup 4096 12월 9 11:52 babseservice
-rw xr-x---. 1 root backup 325 12월 1 02:00 backup-my.cnf
-rw xr-x---. 1 root backup 2560 12월 1 02:00 ib_logfile0
-rw xr-x---. 1 root backup 12582912 12월 1 02:00 ibdata1
drwxr-x---. 2 root backup 4096 12월 9 11:52 mysql
drwxr-x---. 2 root backup 4096 12월 9 11:52 performance_schema
-rw xr-x---. 1 root backup 28 12월 1 02:00 xtrabackup_binlog_info
-rw xr-x---. 1 root backup 77 12월 1 02:00 xtrabackup_checkpoints
-rw xr-x---. 1 root backup 540 12월 1 02:00 xtrabackup_info
```

```
# root@BR_BACKUP_SEC:/usr/local/bin
# 1시간마다 서버 백업 수신 정리
0 * * * * /usr/local/bin/rsync_receive.sh

# 매일 새벽 05:00 무결성 검사
0 5 * * * /usr/local/bin/check_integrity.sh

# 로그 정리 (매일 새벽 05:10)
10 5 * * * /usr/local/bin/cleanup_integrity.sh
```