개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
1	2017-09-29	2010-19-29	초도 제정
2	2023-12-01	2023-12-01	디오토 상호변경

3	2024-08-01	2004-08-01	넥스오토 상호변경
4	2024-08-01	2004-08-01	시스템보안지침 내용변경
5	2025-02-03	2025-02-03	세션타임아웃 및 시간동기화 내용 추가
6	2025-02-03	2025-02-03	IT 인프라 현황관리 및 운영기준 내용 추가

목 차

1. 개요

1.1 목적

본 지침서는 서버시스템의 도입, 설치, 운영, 폐기 등의 업무 수행 시 시스템의 안전한 관리를 위해 준수해야 할 업무절차를 정의함으로써 불법 사용을 방지하고, 자산을 보호하는데 그 목적을 둔다.

1.2 적용범위

사내 운영되고 있는 모든 서버 등 하드웨어 및 응용시스템, 데이터베이스 등 소프트웨어와 이런 자산을 이용해 업무를 수행하는 모든 사용자들을 대상으로 한다.

1.3 용어 정의

1.3.1 시스템

서버, 저장장치 등의 하드웨어와 응용시스템, 데이터베이스 등의 소프트웨어를 총칭한다.

1.3.2 응용프로그램

일상의 업무를 전산 프로그램화한 어플리케이션 프로그램과 상용화된 소프트웨어를 의미한다.

1.3.3 데이터베이스

컴퓨터에 수록한 수많은 자료들을 쉽고 빠르게 추가, 수정, 삭제할 수 있도록 해주는 소프트웨어로서 데이터베이스 내의 정보를 검색하거나, 데이터베이스에 정보

를 저장 및 관리하기 편리하고 효율적인 환경을 제공하는 시스템을 의미한다.

1.3.4 무결성

데이터의 정밀성, 정확성을 의미하며, 데이터베이스에 저장된 값을 정확하게 유지하는 것을 의미한다.

1.4 책임 및 권한

1.4.1 전사보안책임자

① 서버시스템에 대한 도입 및 운영, 폐기에 대한 승인과 전반적인 관리책임을 가진다.

② 본 규칙에 따라 서버시스템의 보안 관리가 수행될 수 있도록 감독할 책임을 가진다.

1.4.2 기술보안담당자

① 서버시스템의 설치 및 운영, 폐기에 따른 보안 이행여부를 점검한다.

② 본 지침을 수정할 필요가 있다고 판단되는 경우 수정 후 전사보안책임자의 승인을 받는다.

1.4.3 시스템운영담당자

① 기술보안담당자와 겸임할 수 있다.

② 본 지침에 따라 서버시스템운영 및 장애처리업무를 수행한다.

③ 시스템의 효율적 보안관리를 위해 필요한 자원을 요청할 수 있다.

2. 시스템 운영

2.1 도입 및 설치

2.1.1 시스템 담당자는 반기 1회 이상 시스템 성능을 점검하여 도입 또는 폐기 여부를 검토하여야 한다.

2.1.2 새로운 서버시스템을 도입할 때 필요 시 BMT를 실시하고 도입 목적에 맞는 용량과 성능에 따라 도입을 결정한다.

2.1.3 시스템 설치 계획을 수립하고, 보안성 검토 및 승인을 받아 시스템을 설치한다.

2.1.4 시스템은 물리적 보안이 되어 있는 통제구역에 설치되어야 한다.

2.1.5 설치 후 자산관리 목록을 갱신하며, 결과를 전사보안책임자에게 보고한다.

2.2 운영

2.2.1 시스템의 처리속도 및 용량을 주기적으로 점검하여야 한다.

2.2.2 시스템 접근권한의 변동 사항을 주기적으로 점검하여 전사보안책임자에게 보고한다.

2.2.3 시스템 장애 시 신속한 업무 복구를 위해 OS 및 DB에 대한 백업을 주기적으로 수행하여야 하며, 수행결과여부를 기록관리하여야 한다.

2.2.4 시스템 공급업체의 보안관련 패치나 권고안 발생 시 적용여부 검토 후 주요정보를 백업하고, 보안패치를 적용하여야 한다.

2.2.5 하드웨어 및 운영체제상의 결함으로 인한 시스템의 문제발생에 대비하여 적절한 유지보수를 수행하여야 한다.

2.3 폐기

2.3.1 시스템 폐기요구 발생 시 승인 후 폐기 처리한다.

2.3.2 저장장치는 별도 폐기하여야 하며, 디가우저, 천공장치 등을 사용하여 정보가 복구되지 않게 폐기해야 한다.

2.3.3 폐기 완료 후 자산관리 목록을 갱신하여야 한다.

3. 시스템 보안

3.1 시스템설치 시 보안설정

3.1.1 시스템의 관리자를 선정하여야 한다.

3.1.2 비인가 접근이나 정보유출 등을 방지하기 위해 적절한 보안시스템을 갖추어야 한다.

3.1.3 시스템 설치 시 제공되는 기본계정 중 불필요한 계정은 삭제되어야 한다.

3.1.4 시스템 설치 시 제공되는 패스워드는 변경되어야 한다.

3.1.5 불필요한 서비스는 중지하여야 한다.

3.1.6 시간을 동기화하여 무결성을 보장하여야 한다.

3.2 시스템운영 시 보안설정

3.2.1 중요 업무 시스템은 개발, 테스트 및 운영시스템으로 분리 운영되어야 한다.

3.2.2 비밀, 민감한 정보는 전송 시 암호화되어야 한다.

3.2.3 개인정보 DB 내 민감한 정보에 대해서는 반드시 암호화하여 저장하여야 한다.

3.2.4 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해서는 복호화되지 않도록 일방향 암호화하여 저장한다.

3.2.5 화면보호기는 10분 이하로 설정하고 패스워드를 지정한다.

3.2.6 중요 업무 시스템은 로그인 성공 시 직전 로그인 정보가 화면에 표시되어야 한다.

3.2.7 데이터베이스, 소스코드, 운영체제, 응용프로그램 등 모든 시스템에 대한 접근통제가 적용되어야 한다.

3.2.8 시스템을 일정기간 미사용 시 자동로그오프나 세션중단기능이 설정되어야 한다.

3.2.9 보안관련 이벤트 로그 및 시스템접근로그는 3년 이상 보관한다.

3.2.10 임시적 외부 개발자나 용역업체 직원이 프로그램 개발, 변경에 참여하는 경우 제한된 방법 및 승인에 의하여 접속을 허용하도록 한다.

3.2.11 시스템에 대한 주기적인 취약점 점검 및 조치가 이루어져야 한다.

3.3 사용자 계정 관리

3.3.1 사용자 계정의 등록, 변경, 삭제는 공식적인 절차에 의거 수행되어야 하고, 계정의 등록, 변경, 삭제의 시행 이력은 관리되어야 한다.

3.3.2 유지보수, 장애처리 등의 목적으로 임시 발급된 계정은 업무 종료 즉시 삭제되어야 한다.

3.3.3 공용ID는 사용하지 않아야 하며, 모든 사용자는 유일한 계정이 부여되어야 한다.

3.3.4 계정이 생성되면 사용자 확인 후 전달되어야 하며, 사용자는 최초 로그인 후 초기 패스워드를 변경하여야 한다.

3.3.5 사용자의 퇴직 등 계정삭제 사유 발생 시 24시간 이내 권한이 삭제되어야 한다.

3.3.6 서버시스템 관리자는 주기적으로 계정 발급 및 로그인 현황을 검토하여야 한다.

3.3.7 시스템 접근로그는 최소 반기 1회 검토하여 퇴직자 계정 사용 여부, 계정도용에 대한 위험성이 분석되어야 한다.

3.4 패스워드 관리

3.4.1 패스워드의 길이는 최소 8자리 이상 숫자, 영문자, 특수기호를 포함하여 생성되어야 한다.

3.4.2 패스워드에는 쉽게 추측할 수 있는 정보가 포함되지 않도록 한다. (예: 아이디와 동일한 패스워드, 규칙적인 문자/숫자, 사용자 이름, 사번 등)

3.4.3 사용자가 패스워드를 사용할 수 있는 최대 기간은 90일로 제한되어야 한다.

3.4.4 직전 5회 패스워드는 재사용이 불가해야 한다.

3.4.5 연속 5회(단 시스템 중요도에 따라 횟수 조정 가능) 입력 오류 시 해당 계정은 잠금 상태가 되어야 하며, 관리자는 사용자 확인 후 계정잠금해제 및 패스워드를 초기화 해야 한다.

3.4.6 패스워드는 일방향 암호화된 형태로 저장되어야 하며, 화면상에 읽을 수 없는 형태로 표시되어야 한다.

3.5 세션타임아웃

3.5.1 세션타임아웃의 적용 대상은 업무시스템에 접속하는 모든 계정(그룹웨어, MES, QMS, PLM 등)에 대해 세션타임아웃을 기본으로 적용한다.

3.5.2 단, 생산관제와 관련된 실시간 생산서열시스템과 보안에 관련된 에이전트 프로그램은 예외로 한다.

3.5.3 모든 시스템에 타임아웃 시간은 10분 이하로 설정한다.

3.5.4 타임아웃 방법은 해당 시스템에서 로그인 시간을 측정하여 설정된 시간을 초과하면 자동으로 해당계정 접속을 차단하고 강제로그아웃 상태로 만든다.

3.6 시간동기화

3.6.1 시간동기화의 목적

① 모든시스템은 시스템 무결성과 로그 정합성 확보를 위하여 정확한 시간동기화를 유지해야한다.

3.6.2 시간동기화 적용대상

① 사내운영서버(Web, DataBase, Application 서버 등)
② 클라이언트 PC 및 노트북
③ 네트워크 장비(라우터, 스위치, 방화벽 등)
④ 보안장비(IDS, IPS, Firewall 등)
⑤ 생산연계시스템(그룹웨어, MES, QMS, PLM 등)

3.6.3 시간동기화 방식 및 기준서버

① 운영서버 및 일반 PC
   a. OS 기본 제공 NTP 서버 또는 사내지정기준서버(NTP 내부 서버 등) 사용
② 네트워크 및 보안장비
   a. 해당 장비 제조사에서 권장하는 공식 NTP 서버 또는 내부 기준 서버를

사용

b. 설정 시 보안정책에 따라 외부 접근여부 고려

c. 생산연계시스템(인터넷 차단환경)

d. 외부 NTP 접근 불가 시, 관리자가 월 1회 이상 수동점검 및 동기화

e. 표준시계기준으로 시간 확인 후 수동 설정

f. 장비 간 시간 오차가 +/- 1분 이내로 유지되도록 관리

③ 예외처리 대상 및 관리

a. 예외처리대상

i. 인터넷 차단환경의 시스템

ii. 외부망 접근이 제한된 보안구역 내 장비

④ 예외처리방법

a. 수동시간 설정 시 기준 장비봐의 시간 비교 로그를 기록

b. 점검 내역은 점검표에 기록하여 보관(점검자, 확인시간, 오차범위 포함)

⑤ 정기점검

a. 점검주기: 분기 1회 이상

b. 점검항목

i. 시간오차확인

ii. 동기화 로그 확인

iii. 동기화 실패 시 원인 분석 및 조치

⑥ 점검결과: 보안점검보고서에 포함하여 보관

3.7 업무시스템 로그관리

3.7.1 사내에 업무용도로 사용하는 계정이 있는 모든시스템은 로그관리 대상이 된다.

3.7.2 로그관리대상 시스템은 전산자산관리대장의 서버현황을 참조하여 식별하며, 식규장비도입 시 정보보안그룹과 협의하여 대상 여부를 검토한다.

3.7.3 업무시스템에서 필수적으로 수집해야 하는 로그 항목은 다음과 같다.

① 사용자 접속기록 (로그인, 로그아웃 이력)

② 첨부파일 다운로드기록

a. 필요 시 계정생성/삭제/권한변경/시스템 오류등의 항목도 포함 가능하다.

③ 파일 송수신기록

3.7.4 로그는 월 1회 이상 정기적으로 수집 및 점검하며, 이상 징후 발견 시 즉시 정보보안그룹과 협의 후 CSO에게 보고한다.

3.7.5 로그는 수집일 기준으로 최소 3년 이상 안전하게 보관하며, 보존 기간 경과 후에는 보안정책에 따라 안전하게 폐기한다.

3.7.6 로그보존사유

① 업무시스템 로그는 다음과 같은 목적으로 보존한다

a. 보안사고 발생 시 원인분석 및 신속한 대응을 위한 증적 확보

b. 사용자 행위 추적을 통한 내부 통제 및 감사 대응

c. 법적 분쟁 및 규제기관의 요청에 대한 대응 근거 확보

d. 개인정보보호법, 정보통신망법 등 관련 법령 및 기업 내부 정책의 준수를 위한 자료 유지

3.8 변경통제

3.8.1 서버, 저장장치 및 기타 하드웨어 변경통제

① 패치적용이나 시스템 파라미터(IP, 환경설정 값 등) 변경발생 시 타당성 검토 및 테스트를 수행한다.

② 주요정보 백업을 수행한 후 적용하고 그 기록을 보고한다.

3.8.2 데이터베이스 변경통제

① 패치적용이나 시스템 파라미터 변경발생 시 타당성 검토 후 테스트를 수행한다.

② 현재 설정값 백업 후 적용하고 그 기록을 보고한다.

3.8.3 응용프로그램 변경통제

① 응용프로그램 변경 및 적용은 공식적인 절차에 의거 수행되어야 한다.

② 변경 완료 시 해당 응용프로그램과 적용하고자 하는 운영환경이 회사가 정한 보안 정책을 준수하고 있는지 보안성 검토하여야 하며, 충분한 기능 검증 테스트를 수행하고 승인을 득한 후 운영환경으로 이관되어야 한다.

③ 주민등록번호, 계좌번호 등 개인정보 및 중요정보를 테스트 데이터로 사용할 경우에는 실 데이터를 변환해서 사용하여야 한다.

④ 응용프로그램 개발도 위와 같은 절차를 적용한다.

3.9 백업 및 매체관리

3.9.1 백업대상

① 업무에 사용되는 모든 시스템의 DataBase(또는 DB라고 한다.)

② 시스템 구동을 위한 운영 프로그램 및 구성파일(설정값 포함)
③ 시스템 운영 관련 로그파일 및 중요 문서
④ 사용자 계정 정보 및 권한 설정 정보 등
⑤ 개발 및 테스트 환경도 필요한 경우 포함할 수 있으며, 백업 대상 시스템 목록은 별도 관리한다.

3.9.2 백업주기

① 정기백업: 분기별 1회 이상
② 변경사항 발생 시 백업: DB 또는 설정 값 등 변경 시 즉시 백업
③ 일일백업: 중요 시스템에 대해서는 최소 일 1회 자동화 백업 수행
④ 임시 및 수동백업: 시스템 점검, 패치 전, 또는 비정기적 작업 시 사전 백업실시

3.9.3 백업방식

① 네트워크 백업: 별도의 백업서버 또는 NAS를 활용한 원격백업
② 이동식 저장매체: USB, 외장하드(HDD), LTO 테이프 등 사용 가능(보안정책에 따라 암호화 권장)
③ 클라우드 백업: 필요 시 보안이 보장된 클라우드 서비스 이용 가능
④ 자동화 툴(Tool) 사용: 백업 자동화 소프트웨어 또는 스크립트를 통한 주기적 실행 권장

3.9.4 백업파일 관리

① 파일명에는 반드시 백업일자(YYYY-MM-DD) 포함
② 확장자는 백업 프로그램에서 지정하는 확장자를 우선 적용하며, 없을 경우 .bak 사용
③ 백업 데이터는 보관기간(최소 1년 이상)에 따라 주기적으로 정리 및 폐기(삭제 전 보안 검토)

3.9.5 업무기준

① 중대한 시스템 장애 발생 시 백업 매체를 사용하여 최대 4시간 내 복구를 목표로 한다.
② 백업 수행 시 백업 완료 로그 및 검증 결과를 기록하고 관리한다.
③ 백업 중 시스템 과부하로 사용히 제한될 가능성이 있을 경우 필히 사전공지한다.
④ 백업 담당자는 정기적으로 복구 테스트를 실시하여 복구 가능할을 확인한다.

3.9.6 기타

① 시스템 담당자는 시스템 장애 시 신속한 업무복구를 위하여 백업을 수행하여야 한다.
② 백업은 시스템의 완전 소실의 경우에도 복구 가능한 수준으로 이루어져야 한다.
③ 백업매체는 비인가자가 접근할 수 없는 격리된 장소 및 화재 등 재난에도 망실되지 않는 장소에 보관하여야 한다.
④ 백업매체의 폐기 시에는 정보를 복구할 수 없게 폐기해야 하며, 관련 로그는 기록관리 및 그 결과를 보고하여야 한다.
⑤ 시스템의 장애 시에는 백업매체를 사용하여 신속하게 복구하여야 한다.

3.10 유지보수

3.10.1 공급사의 권장서비스 기간과 설명서에 따라 정비, 보수하여야 한다.

3.10.2 유지보수 서비스는 인가된 직원에 의해 시행되어야 하며, 유지 보수 작업 내역을 기록하여야 한다.

3.10.3 모든 보수내역과 의심되는 결함은 기록되어야 한다.

3.10.4 시스템 개발 및 유지보수는 규정된 절차에 따라 인가자에 의해 수행되어야 시스템 담당자는 유지보수 시에 동석하여야 한다.

3.10.5 시스템 담당자는 지속적으로 시스템의 취약성 정보를 수집하고, 해당 취약성에 대한 대응책을 수립, 적용하여야 한다.

3.11 용량 및 성능 관리

3.11.1 시스템 담당자는 시스템을 점검하고, 매월 정기 점검 보고서를 작성하여 부서장에게 보고하여야 한다.

3.12 보안패치

3.12.1 시스템 담당자는 시스템 별 보안취약점을 확인하고, 타당성 검토 및 테스트를 수행한 후 패치를 수행한다

3.12.2 시스템 별 보안패치 목록, 보안패치 작업일 등 패치적용 현황을 관리한다.

3.13 장비 반출

3.13.1 반출하기 위해서는 사전에 반출 승인권자의 승인을 받아야 한다.

3.13.2 자산의 반입 및 반출 시 해당 기록을 유지하여야 한다.

3.14 용도변경 및 폐기

3.14.1 서버 담당자는 해당 서버의 용도 변경 시 서버에 저장되어 있는 정보를 삭제해야 하며 장비의 프로파일을 작성, 갱신 및 유지해야 한다.

3.14.2 시스템 폐기요구 발생 시 승인 후 폐기 처리한다.

3.14.3 완료 후 자산관리 목록을 갱신하여야 한다.

3.15 IT 인프라 현황관리

3.15.1 IT 인프라라고 함은 서버, 스토리지, 네트워크 관련 장비를 정의한다.

3.15.2 서버 및 인프라와 관련하여 분기 1회 이상 하기 항목에 대하여 측정 및 점검 진행한다.

① 서버: CPU, 메모리, 내장디스크, 네트워크 연결상태, 파일시스템, 로그파일, 주요 시스템 프로세스 등

② 스토리지: 사용률 및 가용률, 평균 응답시간, 캐시메모리 성능, 초당 디스크 I/O 등

③ 네트워크 장비: 네트워크 장비의 연결상태, 네트워크 포트상태, 대역폭 사용률, 네트워크 충돌률, 네트워크 I/O 에러율, 구간별 응답시간, 초당 패킷율 등

3.15.3 상기 내용으로 측정 및 점검 진행하여 과부하 및 장애발생 여지가 있으면 문제점 파악 후 해결방안을 CSO에 보고하여 승인 후 조치한다.

3.16 운영기준

3.16.1 서버, 스토리지, 네트워크 장비의 성능 및 용량 점검 시, 하기와 같은 운영 기준을 적용한다.

① 서버

a. CPU 사용률 80% 이상일 경우 "경고" / 90% 이상일 경우 즉시조치 필요

b. 메모리 사용률 75% 이상일 경우 "경고" / 80% 이상일 경우 즉시조치 필요

c. 디스크 사용률 85% 이상일 경우 "경고" / 95% 이상일 경우 즉시조치 필요

② 스토리지

a. 사용률 85% 이상일 경우 "경고" / 90% 이상일 경우 즉시조치 필요

b. 캐시메모리 성능이 90% 이하일 경우 "경고" / 80% 이하일 경우 즉시 조치 필요

③ 네트워크

a. 대역폭 사용률 80% 이상일 경우 "경고" / 90% 이상일 경우 즉시조치 필요

b. 네트워크 충돌률이 1% 이상일 경우 "경고" / 5% 이상일 경우 즉시조치 필요

c. I/O 에러율 1% 이상일 경우 "경고" / 5% 이상일 경우 즉시 조치 필요

3.17 보안시스템 운영 현황관리 및 점검절차

3.17.1 운영현황 관리

① 사내에 운영하고 있는 필수 보안시스템은 모든 장비에 적용되어야 한다.

② 단, 보안프로그램(에스원 SESP 등) 실시간 서열 정보와 실적 수집의 FA망은 예외로 한다.

③ 보안시스템이 정상적으로 운영되고 있는지 설치율, 사용율, 예외장비, 점검결과 등을 포함한 리스트를 작성하여 현황을 관리한다.

3.17.2 운영현황 관리절차

① 목적

a. 본 절차는 보안시스템(백신, 방화벽, IPS, NAC, 에스원 SESP 등)의 설치 및 운영 상태를 체계적으로 관리하고, 정상적으로 운영되고 있는지를 정기적으로 점검하여 보안 수준을 유지·강화하는 것을 목적으로 한다.

② 적용대상

a. 본 절차는 사내에서 운영 중인 모든 보안시스템 및 이를 관리하는 정보보안그룹를 대상으로 한다.

③ 운영현황 관리항목

a. 설치율: 전체 대상 장비 중 보안시스템이 실제 설치된 장비의 비율

b. 사용률: 설치된 시스템 중 현재 정상적으로 작동 중인 시스템의 비율

c. 예외기준: 시스템 적용이 불가능한 장비(예시: FA망, 서열정보시스템 등)은 예외 장비로 지정하여 목록화

d. 점검결과: 설치유무, 실행상태, 삭제흔적 등의 점검 내용 기록

3.18 보안시스템 운영현황 관리절차

① 정보보안그룹은 보안시스템 설치 대상 장비 리스트를 작성하고, 설치여부, 운영상태, 예외여부 등의 정보를 포함하여 최신 상태로 유지한다.

② FA망 등 보안시스템 적용이 불가능한 장비는 예외 장비로 등록하며, 예외 사유와 승인내역을 문서화하여 정보보안협의체에서 정기적으로 검토한다.

③ 보안시스템 운영 현황은 월 1회 정기 점검하며, 필요 시 수시 점검도 병행할 수 있다.

④ 점검은 IT 자산관리시스템을 활용한 자동점검을 원칙으로 하며, 시스템이 없는 경우에는 정보보안그룹 주관으로 직접 수동 점검을 실시한다. 또한 일부 장비에 대해 무작위 샘플링 방식으로 정상 실행 여부를 확인할 수 있다.

⑤ 점검결과, 시스템이 비정상적으로 동작하거나 삭제 흔적이 발견된 경우, 해당 사용자에게 구두 경고 후 즉시 시정조치를 요청한다. 시정이 이루어지지 않을 경우 보안 위반자 처리규정에 따라 조치한다.

⑥ 정보보안그룹은 월 1회 이상 점검 결과를 CSO에게 보고하며, 이상 징후 발견 시 에는 즉시 보고하여야한다. 보고 내용에는 설치율, 사용률, 예외장비현황, 점검 결과 및 조치 내용을 포함한다.

3.18.2 기록보관

① 운영현황 리스트 및 점검 결과는 최소 3년 간 보관하며, 정보보호정책에 따라 비인가자가 접근하지 못하도록 안전하게 저장하고 관리한다.

3.18.3 웹방화벽 적용기준 및 운영절차

① 적용기준

a. 적용대상

i. 웹 방화벽(Web Application Firewall, 이하 WAF)은 외부에서 접근 가능한 웹 애플리케이션 서버에 대해 기본적으로 적용한다.

ii. 다음 조건 중 하나 이상에 해당하는 시스템은 웹 방화벽 적용 대상이다.

- ●외부 접속이 가능한 웹 애플리케이션 서버
- ●민감 정보(개인정보, 금융정보 등)를 처리하는 웹 시스템
- ●고객 서비스(전자상거래, 회원 가입/로그인 등)를 제공하는 시스템
- ●외부 API, 웹 연동이 있는 내부 시스템

iii. 적용 예외가 필요한 경우 보안협의체를 통한 사전 심의 후 CSO 승인을 받아야 한다.

b. 설치 기준

i. 웹 방화벽은 별도 장비 또는 UTM 장비 내 모듈로 구성할 수 있으며, 시

스템 구조에 따라 독립형 혹은 클러스터형으로 설치한다.

ii. 테스트, 개발 환경에도 외부와 연동되는 경우에는 WAF를 적용하며, 서비스 오픈 최소 1주 전에 적용을 완료해야 한다.

c. 운영절차

i. 정책 수립 및 설정

●보호 대상 시스템의 트래픽 패턴 및 보안 위협을 사전 분석한 후 정책을 수립한다.

●WAF 정책은 기본 룰셋을 기반으로 업무 특성에 따라 조정하며, 보안협의체의 사전 검토를 거친다.

●초기 운영은 모니터링 모드로 시작하여 정책을 안정화한 뒤 차단 모드로 전환한다.

●SSL 복호화를 위해 인증서 및 키 관리 절차는 기술보안팀이 책임지고 수행한다.

ii. 운영 및 점검

●기술보안담당자는 WAF의 작동 상태, 탐지/차단 로그를 매일 점검하며 이상 발생 시 즉시 대응한다.

●시스템 변경(도메인, 경로, 포트 등) 시 정책 재검토 및 재적용 절차를 수행한다.

●공격 탐지 시 알림 시스템을 통해 실시간으로 통보되도록 설정하며, CSO와 관련 부서에 공유한다.

iii. 정책 변경 및 예외 관리

●정책 변경 시 다음 절차를 따른다

●변경 요청 → 기술보안팀 사전 검토

●보안협의체 심의

●테스트 환경 검증

●CSO 승인

●운영 반영 및 이력 기록

iv. 정책 변경 및 예외 등록 로그는 최소 6개월간 보관한다.

v. 예외 처리는 최소화하며, 반드시 위험 분석 후 제한적으로 적용한다.

d. 업그레이드 및 유지관리

i. 시그니처 및 정책은 자동 업데이트로 구성하며, 오류 발생 시 수동 업데이트를 즉시 수행한다.

ii. 펌웨어 및 관리도구는 분기별로 점검하여 최신 상태를 유지한다.

iii. 긴급 위협(CVE, 제로데이 등) 발생 시 관련 보안정책은 수시로 적용한다.

e. 로그관리

i. 로그는 요청 URL, 원본 IP, 공격유형, 차단여부 등 주요 항목을 포함한다.

ii. 월 1회 이상 로그를 수집 및 분석하여 이상행위를 식별하며, 보고서를 작성하여 CSO에게 보고한다.

iii. 로그는 최소 3년간 보관하며, 위변조 방지를 위한 별도 저장소에 안전하게 보관한다.

iv. 로그 접근 권한은 기술보안담당자에 한정하고, 접근 이력은 기록·관리한다.