별첨 #5. 로그 및 모니터링 지침

제 1 장 총칙

제 1 조(목적)

본 지침은 「밥세권 서비스 보안정책서」 제 10 조(로그 및 모니터링) 및 제 11 조(결제 보안)에 근거하여 시스템·네트워크·보안장비·애플리케이션·결제 로그의 수집·보관·모니터링 기준 및 절차를 규정함을 목적으로 한다.

제 2 조(적용 범위)

본 지침은 다음 영역의 모든 로그에 적용한다.

1. 서버(OS)·DB·웹/애플리케이션 로그
2. 네트워크 장비 및 보안장비(WAF, UTM, IPS 등)
3. 관리자 페이지·내부 시스템 접근 로그
4. 결제 트랜잭션 및 PG 연동 로그
5. 모니터링 시스템 및 장애 감지 로그

제 3 조(책임과 역할)

1. 정보보호책임자(CISO)
   - 로그 보존 기간 승인
   - 이상징후 보고 체계 승인
2. 정보보안담당자
   - 로그 분석 및 보안 이벤트 대응
   - 모니터링 정책 구성 및 운영
3. 시스템/네트워크 관리자
   - 로그 수집/전송 설정, 저장 인프라 운영
4. 보안팀
   - 애플리케이션 로그 작성 구조 유지
   - 민감정보 마스킹 준수

제 2 장 로그 수집 및 저장 기준

제 4 조(중앙 로그 수집 시스템)

1. 모든 로그는 **중앙 로그 서버(SIEM, Log Storage 등)**로 수집한다.
2. 로그 전송 프로토콜은 안전한 방식 사용
   - TLS 적용

- 인증키 기반 전송

3. 서버·보안장비가 로그를 전송할 수 없는 경우 즉시 담당자에게 알림이 발생해야 한다.

제 5 조(로그 수집 대상)

1. 시스템(OS) 로그
    - 인증/접근로그
    - 프로세스/서비스 로그
    - 에러/커널 로그
2. DB 로그
    - 접속로그(성공/실패)
    - 쿼리 로그(선별하여 적용 가능)
    - 권한 변경·계정 생성 로그
3. 애플리케이션 로그
    - 요청/응답 로그
    - 오류/예외 로그
    - 관리자 페이지 접근 기록
4. 보안장비 로그
    - 방화벽 허용/차단 로그
    - WAF 탐지/차단 로그
    - IPS/UTM 이벤트 로그
5. 결제 로그 / PG 연동 로그
    - 거래요청/결과 로그
    - Webhook/Callback 요청
    - Signature 검증 결과
    - Transaction ID

    ※ 5 년 이상 보관 필수

제 5 조(로그 수집 대상)

로그에는 다음 정보가 저장되어서는 안 된다.

- 주민등록번호·계좌번호 등 개인정보 원본
- 카드번호 전체, CVC, 유효기간
- 비밀번호(암호화·해시 포함 저장 금지)
- 인증토큰·API Key·Secret Key
- 내부 환경 변수가 노출되는 Error Stack

마스킹 예시

- 전화번호: 010-****-1234
- 이메일: h***@gmail.com

제 3 장 로그 보관 기준

제 7 조(보존 기간)

1. 시스템·DB·보안장비 로그: 1 년 이상
2. 결제 관련 로그(Transaction/정산/PG 연동): 5 년 이상
3. 법령 요구 시 기간 연장 가능
4. 백업 로그는 암호화 후 별도 저장

제 8 조(무결성 보호)

1. 로그는 삭제·변조 불가하도록 무결성 기능 적용
    - Hash(SHA-256 이상)
    - Append-only Storage
    - WORM 저장소 가능
2. 운영자는 로그를 임의 수정·삭제할 수 없다.

제4장 모니터링 운영 기준

제 9 조(실시간 모니터링 대상)

다음 항목은 실시간 모니터링 시스템에 연동한다.

1. 인증 관련
    - SSH/RDP 접근
    - 관리자 페이지 로그인 실패
    - 해외 IP 접근
2. 보안 이벤트
    - WAF/IPS 공격 탐지
    - 포트 스캔
    - Brute Force 공격
    - SQL Injection 탐지
3. 시스템 이벤트
    - CPU/Mem 과다 사용
    - Disk Full 임계치
    - 프로세스 비정상 종료
4. 결제 이벤트
    - 대량 반복 결제 요청
    - 동일 계정의 비정상 결제 오류

- Webhook 서명 검증 실패

제 10 조(이상행위 기준)

다음 행위는 이상행위로 간주하여 즉시 CISO 에 보고한다.

1. 동일 계정에서 짧은 시간 내 반복 로그인 실패
2. 비인가 IP 로부터 관리자 페이지 접근 시도
3. 해외 또는 위험국가 IP 접근
4. WAF/IPS 에서 중·고위험 공격 반복 탐지
5. 서버 설정 변경 또는 권한 상승 시 의심 패턴
6. 결제 트랜잭션 위변조 의심 패턴
7. 로그 전송 중단(서버/보안장비 로그 미수집)

제 11 조(모니터링 알림 기준)

모니터링 시스템은 다음 조건에서 경보(Alert)를 발생시킨다.

1. 경고(Alert) 레벨
    - CPU/Mem 80% 이상 5 분 지속
    - WAF Medium 수준 공격 탐지
    - 관리자 페이지 로그인 5 회 실패
2. 위험(Critical) 레벨
    - Root 계정 로그인
    - WAF High 수준 공격 탐지
    - UTM/IPS 에서 공격 차단 이벤트 발생
    - 서버 디스크 90% 이상

제 5 장 점검 및 보고

제 12 조(정기 로그 점검)

1. 보안 이벤트 로그 주간 점검
2. 시스템/애플리케이션 로그 월간 점검
3. 방화벽/WAF 정책 변경 로그 월간 점검
4. 결제 로그 정상 여부 월간 점검
5. 점검 결과는 1 년 이상 보관

제 13 조(로그 감사)

1. 반기 1 회 로그 감사 실시
2. 감사 항목
    - 계정 도용 의심내역
    - 비인가 접근

- 결제 관련 오류 및 위변조 의심

3. 감사 결과는 CISO 에게 보고

제 6 장 장애 및 사고 대응

제 14 조(로그 기반 사고 분석)

사고 발생 시 다음 순서로 로그를 분석한다.

1. 접속 로그(SSH/관리자)
2. WAF/IPS 탐지로그
3. 시스템 프로세스 및 오류로그
4. 네트워크 패킷/UTM 로그
5. 결제 트랜잭션 로그

분석 결과는 문서화하여 사고 대응 지침에 따라 처리한다.

제 15 조(로그 유실 방지)

1. 서버 로그 저장공간 부족 방지
2. 로그 로테이션(logrotate) 설정 필수
3. 장애 발생 시 로그 보존 우선 조치

제 7 장 예외 관리

제 16 조(예외 승인)

1. 로그를 수집하기 어려운 시스템 존재 시 예외 가능
2. 다음 항목 포함 필수
    - 사유
    - 위험 분석
    - 대체 방안

    CISO 승인 후 적용
3. 예외 기간 만료 시 원복

제 8 장 부칙

제 17 조(시행일)

본 지침은 2025 년 12 월 29 일부터 시행한다.

제 18 조(개정)

본 지침은 정보보보호책임자의 검토 후 개정한다.