**SK헬스 서비스 클라우드 전환 정보보안 컨설팅**

**보안요건 이행점검 보고서**

**2022.6.15**

**1조 핼쑥해요**

**문서 이력**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **버전** | **주요내용** | **일자** | **작성자** | **검토자** |
| Ver0.1.0 | 보고서 초안 작성 | 2022.06.09 | 고해준, 도규탁 | 백성광 |
| Ver0.2.0 | 보고서 개요 작성 완료 | 2022.06.11 | 고해준, 도규탁 | 백성광 |
| Ver0.3.0 | 보고서 최종 수정 | 2022.06.17 | 고해준, 도규탁 | 백성광 |

목차

[Ⅰ. 개요 4](#_Toc106612216)

[**1.** **목적 및 배경** 4](#_Toc106612217)

[**2.** **점검 일정** 4](#_Toc106612218)

[**3.** **점검 인력** 4](#_Toc106612219)

[**4.** **점검 방법(수행 절차)** 4](#_Toc106612220)

[**5.** **점검 기준** 5](#_Toc106612221)

[**6.** **점검 대상** 8](#_Toc106612222)

[Ⅱ. 점검결과 10](#_Toc106612223)

[**1.** **점검결과 요약** 10](#_Toc106612224)

[**2. 점검결과 상세** 12](#_Toc106612225)

[**2.1 계정 권한 관리** 12](#_Toc106612226)

[**2.2 식별 인증** 16](#_Toc106612227)

[**2.3 접근 통제** 19](#_Toc106612228)

[**2.4 암호화 적용** 32](#_Toc106612229)

[**2.5 로깅 및 모니터링** 35](#_Toc106612230)

[**2.6 보안관리** 40](#_Toc106612231)

# **Ⅰ. 개요**

## **목적 및 배경**

SK헬스 서비스를 AWS 클라우드 환경에서 운영할 때 ISMS-P와 법률을 만족시키는 보안 요구사항 측면에서 클라우드 인프라를 점검한다. 보안요건정의서와 보안 아키텍처를 참고하여 보안 요구사항들이 충족•불충족한 지 식별하고 대책을 수립하는 데 그 목적이 있다.

## **점검 일정**

2022년 06월 08일부터 2022년 06월 16일까지 7일 간 수행하였다

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **분류** | **내용** | **2022년 6일** | | | | | | | | |
| **06.08** | **06.09** | **06.10** | **06.11** | **06.12** | **06.13** | **06.14** | **06.15** | **06.16** |
| **사전 준비** | 대상 범위 협의,  점검 방법 결정 |  |  |  |  | 휴일 | |  |  |  |
| **이행 점검** | 보안 요건 충족  여부 확인 |  |  |  |  | 휴일 | |  |  |  |
| **분석•평가** | 결과 보고서  작성 및 리뷰 |  |  |  |  | 휴일 | |  |  |  |

[표 1] 점검 일정

## **점검 인력**

|  |  |  |  |
| --- | --- | --- | --- |
| **이름** | **소속** | **파트** | **담당 업무** |
| 고해준 | 1조 핼쑥해요 | 보안요건이행점검 | 보안요건이행점검 및 조치방안분석 |
| 도규탁 | 1조 핼쑥해요 | 보안요건이행점검 | 보안요건이행점검 및 문서작성 |

[표 2] 점검 인력

## **점검 방법(수행 절차)**



[그림 1] 점검 절차

1. **현황분석**

보안 요건 점검 대상들을 파악하고, AWS 클라우드에서 제공하는 보안 서비스(eg. WAF, Network Firewall, Cloud Watch 등)들에 대해 전반적으로 분석한다.

1. **실사 점검**

SK헬스 서비스의 클라우드 인프라를 실사하여 보안 요건 항목들을 점검한다.

**3) 충족/불충족 평가**

SK헬스 서비스 클라우드 인프라를 점검한 것을 분석하여 보안 요구 항목 충족 여부를 판단한다. 점검 범위에 해당하지 않는 항목은 N/A로 표기한다.

1. **개선방안 제시**

충족/불충족 평가를 통해 도출된 결과를 통해 불충족 항목에 대해 보안설정 가이드라인을 제공한다.

## **점검 기준**

법률과 ISMS-P 인증의 기술적 보호조치 항목을 분류하여 보안요건정의서를 작성하였다. 이를 기준으로 보안요건정의 항목들이 SK헬스 서비스의 클라우드 인프라에서 충족하는지 점검을 이행한다.

보안요건정의서에서 요구하는 항목들을 나타내고 있으며, 상세 현황은 다음과 같다.

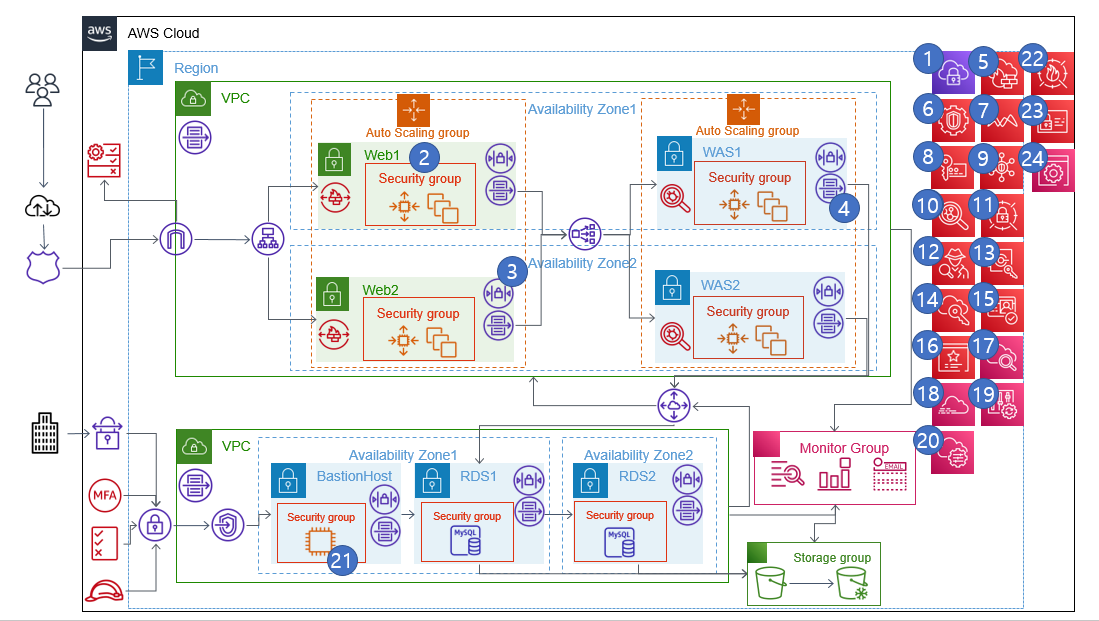
|  |  |  |  |
| --- | --- | --- | --- |
| **보안코드** | **영역** | **세부영역** | **항목명** |
| Sec101 | **계정∙권한 관리** | 사용자 계정 관리 | 개인정보 및 중요정보에 대한 비인가 사용자 접근 권한 설정 |
| Sec102 | 특수 계정 및  권한 관리 | 특수 계정의 권한 식별 및 관리 |
| Sec103 | 계정 비밀번호  관리 | 사용자 및 관리자 계정 비밀번호 관리 |
| Sec104 | 접근 권한 검토 | 사용자 계정의 접근 권한 이력 점검 |
| Sec105 | 보안시스템 관리 | 예외 정책 사용자 권한 관리 |
| Sec201 | **식별∙인증** | 사용자 인증 | 사용자 접근에 대한 인증 수단 적용 |
| Sec202 | 외부 접근 사용자 인증 | 외부 접근에 대한 사용자 인증 |
| Sec203 | 사용자 식별 | 사용자 계정 식별자 할당 |
| Sec301 | **접근**  **통제** | 네트워크 접근 | 네트워크 비인가 사용자 접근 통제 |
| Sec302 | 네트워크 영역 분리 및 통제 |
| Sec303 | 외부 네트워크 접근 통제 |
| Sec304 | 무선 네트워크 접근 통제 |
| Sec305 | 정보시스템 접근 | 정보시스템에 대한 접근수단 정의 및 접근 통제 |
| Sec306 | 정보시스템 접근에 대한 사용자 인증 통제 적용 |
| Sec307 | 정보시스템 접속 차단 |
| Sec308 | 서비스에 따른 독립된 서버 운영 |
| Sec309 | 정보시스템 관계없는 서비스 차단 |
| Sec310 | 응용프로그램  접근 | 응용프로그램 접근 권한 제한 |
| Sec311 | 응용프로그램 중요정보의 노출 최소화 |
| Sec312 | 응용프로그램 세션 관리 |
| Sec313 | 관리자 전용 응용프로그램 비인가자 접근 통제 |
| Sec314 | 데이터베이스  접근 | 데이터베이스 접근 통제 |
| Sec315 | 원격접근 통제 | 단말기 접근 통제 |
| Sec316 | 인터넷 접속 통제 | 외부 인터넷 접속 통제 |
| Sec317 | 망분리 적용 및 통제 |
| Sec318 | 보안시스템 통제 | 보안시스템 비인가자 접근 통제 |
| Sec401 | **암호화**  **적용** | 중요정보 암호화 | 개인정보 및 주요정보에 대한 암호화 적용 |
| Sec402 | 암호키 관리 | 암호키 접근 권한 관리 |
| Sec403 | 비밀번호 암호화 | 비밀번호 암호화 적용 |
| Sec501 | **로깅 및 모니터링** | 로그 관리 | 로그 기록 보관 및 관리 |
| Sec502 | 로그 기록 접근 권한 설정 |
| Sec503 | 정보시스템 이상징후 인지를 위한 모니터링 절차 이행 |
| Sec504 | 로그 시간 동기화 |
| Sec505 | 이상행위 발생 시 신속한 분석 및 점검 |
| Sec601 | **보안**  **관리** | 시험과 운영 환경 분리 | 시험 시스템과 운영시스템의 분리 |
| Sec602 | 시험 데이터 보안 | 실제 운영 데이터의 사용 제한 |
| Sec603 | 장애 관리 | 정보시스템의 장애 관리 |
| Sec604 | 클라우드 보안 | 클라우드 서비스 보안 통제 정책 이행 |
| Sec605 | 클라우드 서비스 관리자 권한 보호대책 적용 |
| Sec606 | 공개서버 보안 | 공개서버 DMZ 설치 및 보안시스템 보호 |
| Sec607 | 패치관리 | 공개 인터넷 접속을 통한 패치 제한 |
| Sec608 | 악성코드 통제 | 악성코드 보호대책 이행 |
| Sec609 | 취약점 점검 및 조치 | 최신 보안 취약점 분석 및 조치 |
| Sec701 | **개인정보보호** | 개인정보보호 | 개인정보처리시스템 법률 준수 검토 및 관리 |

[표 6] 보안요건정의서 항목 리스트

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ISMS-P는 정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷 진흥원 또는 인증기관이 증명하는 제도이다. ISMS-P항목 중 관리적•물리적 보호조치는 제외하고 기술적 보호조치 항목만을 대상으로 점검한다.   |  |  |  | | --- | --- | --- | | **통합인증** | **보호조치 분류** | **점검 여부** | | ISMS-P 인증항목 | 관리적 보호조치 항목 | N/A | | 물리적 보호조치 항목 | N/A | | **기술적 보호조치 항목** | **Y** |   [표 3] ISMS-P 보호조치 분류 항목   |  |  |  |  | | --- | --- | --- | --- | | **통합인증** | **분야 (인증기준 개수)** | | **기술적**  **보호조치 항목**  **개수** | | 관리 체계 수립 및 운영(16) | 1.1 관리체계 기반 마련(6) | 1.3 관리체계 운영(3) | **0개** | | 1.2 위험관리(4) | 1.4 관리체계 점검 및 개선(3) | | 보호대책 요구사항(64) | 2.1 정책, 조직, 자산 관리(3) | 2.7 암호화 적용(2) | **34개** | | 2.2 인적 보안(6) | 2.8 정보시스템 도입 및 개발 보안(6) | | 2.3 외부자 보안(4) | 2.9 시스템 및 서비스 운영관리(7) | | 2.4 물리 보안(7) | 2.10 시스템 및 서비스 보안관리(9) | | 2.5 인증 및 권한 관리(6) | 2.11 사고 예방 및 대응(5) | | 2.6 물리 통제(7) | 2.12 재해복구(2) | | 개인정보 처리 단계 별  요구사항(22) | 3.1 개인정보 수집 시 보호조치(7) | 3.3 개인정보 제공 시 보호조치(3) | **1개** | | 3.2 개인정보 보유 및 이용 시 보호조치(5) | 3.4 개인정보 파기 시 보호조치(4) | | 3.5 정보주체 권리보호(3) |  |   [표 4] ISMS-P기준   |  |  |  | | --- | --- | --- | | **법** | **시행령** | **고시** | | 개인정보 보호법 | 개인정보 보호법 시행령 | 개인정보의 기술적 ·관리적 보호조치 | | 개인정보의 안정성 확보 조치 | | 정보통신망법 | 정보통신망법 시행령 | 정보보호조치에 관한 지침 | | 위치정보법 | 위치정보법 시행령 |  | | 클라우드컴퓨팅법 |  | 클라우드컴퓨팅서비스 정보보호에 관한 기준 |  * **SK헬스 서비스의 인프라 단계에서 개인정보 및 중요정보 보호를 위해 준수해야 할 법률**   [표 5] 법률 분류 항목 |

## **점검 대상**

SK헬스 서비스 클라우드 인프라를 대상으로 보안요건 항목 리스트의 요구사항들을 점검한다. SK헬스 서비스의 클라우드 구성도와 AWS 보안 서비스는 다음과 같다. 운영체제, 어플리케이션, DBMS는 점검 대상에서 제외한다.



[그림 2] SK헬스 클라우드 보안 구성도

|  |  |  |  |
| --- | --- | --- | --- |
| **번호** | **이름** | **번호** | **이름** |
| 1 | AWS VPN | 13 | AWS Single Sign-On |
| 2 | Security Group | 14 | AWS CloudHSM |
| 3 | Network Access Control List | 15 | Amazon Cognito |
| 4 | VPC Flow Log | 16 | AWS Certificate Manager |
| 5 | AWS Network Firewall | 17 | Amazon CloudWatch |
| 6 | Amazon GuardDuty | 18 | AWS CloudTrail |
| 7 | Amazon Macie | 19 | AWS Config |
| 8 | AWS Key Management Service | 20 | AWS Systems Manager |
| 9 | AWS Security Hub | 21 | Bastion Host |
| 10 | Amazon Inspector | 22 | AWS WAF |
| 11 | AWS Secrets Manager | 23 | AWS Identity and Access Management |
| 12 | Amazon Detective | 24 | AWS Management Console |

[표 8] AWS 보안 서비스

# **Ⅱ. 점검결과**

## **점검결과 요약**

점검 대상인 SK헬스의 클라우드 인프라가 ISMS- P의 기술적 보호조치 항목들과 법률들을 기준으로 정보보호 관점에서 안전하게 구성 되어있는지, 보안 요건 점검 항목 리스트를 살펴 해당 요구사항이 이행되었는지 점검한 결과이다.

항목 별 점검 결과 평균 이행률은 93.8%이고 식별•인증, 암호화 적용, 보안 관리 항목은 평균 이행률보다 높은 100%로 충족되었다. 반면 계정•권한 관리 80%, 접근 통제 83%, 로깅 및 모니터링 80%로 평균인 90.5%보다 이행률이 낮게 책정되었다.

**평균**

[그림 2] 이행 점검 결과 그래프

점검 항목별로 구분하여 보안요건항목을 충족•불충족으로 나누어 점검하였다. 이행 점검 통계는 아래와 같다.

|  |  |  |  |
| --- | --- | --- | --- |
| **이행 점검 통계** | | | |
| **구분** | **점검 항목** | | |
| **전체** | **충족** | **불충족** |
| 계정•권한 관리 | 5 | 4 | 1 |
| 식별•인증 | 3 | 3 | - |
| 접근 통제 | 18 | 15 | 3 |
| 암호화 적용 | 3 | 3 | - |
| 로깅 및 모니터링 | 5 | 4 | 1 |
| 보안 관리 | 9 | 9 | - |
| **통계** | 44 | 39 | 5 |

[표 9] 이행 점검 통계

## **2. 점검결과 상세**

### **2.1 계정 권한 관리**

**사용자 계정 관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec101 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 사용자 계정 관리 | 불충족 |
| **항목명** | 개인정보 및 중요정보에 대한 비인가 사용자 접근 권한 설정 | | |
| **요구사항 내용** | 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근 권한 생성‧등록‧변경 시 직무 별 접근 권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가? | | |
| **점검 현황** | 현재 IAM에서 확인 가능한 사용자 계정 중 일부 계정(eg. SK101-003)은 일반계정임에도 불구하고 AdministratorAccess 권한이 부여되어 있다. | | | |
| **보안요건 조치 방안** | 사용자 접근 권한 부여 방법  1. 접근 분류 체계에 따라 직무에 적합한 권한을 부여한다.  2. SK101-003에 대한 AdministratorAccess 권한을 제거하고 일반 사용자가 접근할 수 있는 범위를 설정한다.  3. IAM의 액세스 관리에서 알맞은 정책과 권한을 설정하고 직무에 맞는 계정을 선택한다. | | | |

**특수 계정 및 권한 관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec102 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 특수 계정 및 권한 관리 | 불충족 |
| **항목명** | 특수 계정의 권한 식별 및 관리 | | |
| **요구사항 내용** | 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도의 목록으로 관리하고 있는가? | | |
| **점검 현황** | IAM의 사용자 그룹으로 특수 목적을 위한 계정 분류 및 관리하고 있다.  텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**계정 비밀번호 관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec103 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 계정 비밀번호 관리 | 불충족 |
| **항목명** | 사용자 및 관리자 계정 비밀번호 관리 | | | |
| **요구사항**  **내용** | 사용자, 관리자 계정을 안전한 비밀번호를 설정하여 관리하고 있는가? | | | |
| **점검 현황** | IAM을 통해 비밀번호 정책을 수립하여 안전하게 관리하고 있다.  텍스트이(가) 표시된 사진  자동 생성된 설명  Cognito를 통해 사용자, 관리자 계정의 비밀번호 강도를 설정하여 관리하고 있다.  텍스트이(가) 표시된 사진  자동 생성된 설명 | | | | |
| **보안요건 조치 방안** | 공 란 | | | | |

**접근 권한 검토**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec104 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 접근 권한 검토 | 불충족 |
| **항목명** | 사용자 계정의 접근 권한 이력 점검 | | |
| **요구사항 내용** | 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근 권한 생성‧등록‧부여‧이용‧변경‧말소 등의 이력을 점검하고 있는가? | | |
| **점검 현황** | CloudTrail을 통해 사용자 계정 접근 권한 변경 등 이력을 로그로 남겨 CloudWatch Log로 보내고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**보안 시스템 관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec105 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 보안시스템 관리 | 불충족 |
| **항목명** | 예외 정책 사용자 권한 관리 | | |
| **요구사항 내용** | 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가? | | |
| **점검 현황** | IAM에서 Network Firewall에 대한 정책을 생성하고 보안 시스템의 예외 정책 사용자에게 읽기 권한만 부여하여 관리하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

### **2.2 식별 인증**

**사용자 인증**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec201 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 사용자 인증 | 불충족 |
| **항목명** | 사용자 접근에 대한 인증 수단 적용 | | |
| **요구사항 내용** | 정보시스템 및 개인정보처리시스템에 대한 접근 시 사용자 인증 수단(인증서, OTP등)을 사용하고 있는가? | | |
| **점검 현황** | IAM의 MFA 추가 인증을 통해서 사용자 인증 수단을 추가적으로 사용하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**외부 사용자 인증**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec202 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 사용자 인증 | 불충족 |
| **항목명** | 외부 접근 사용자 인증 | | |
| **요구사항 내용** | 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증 수단 또는 안전한 접속 수단을 적용하고 있는가? | | |
| **점검 현황** | 텍스트이(가) 표시된 사진  자동 생성된 설명Client VPN 엔드포인트를 설정하여 외부에서 Bastion Host에 접근하기 위한 안전한 수단을 제공하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**사용자 식별**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec203 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 사용자 식별 | 불충족 |
| **항목명** | 사용자 계정 식별자 할당 | | |
| **요구사항 내용** | 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 있는가? | | |
| **점검 현황** | 텍스트이(가) 표시된 사진  자동 생성된 설명Cognito를 통해서 사용자에 대한 식별자를 할당해서 개인정보 취급자 및 사용자를 구분하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

### **2.3 접근 통제**

**네트워크 접근**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec301 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 네트워크 접근 | 불충족 |
| **항목명** | 네트워크 비인가 사용자 접근 통제 | | |
| **요구사항 내용** | 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근 통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가? | | |
| **점검 현황** | VPC의 NACL에서 SSH 접근에 대한 사용자를 제한하고 SSH의 인바운드 소스에는 개발자나 운영자 등 인가된 사용자의 IP 주소를 지정하고 있다.  텍스트, 스크린샷, 실내이(가) 표시된 사진  자동 생성된 설명 | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec302 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 네트워크 접근 | 불충족 |
| **항목명** | 네트워크 영역 분리 및 통제 | | |
| **요구사항 내용** | 서비스, 사용자 그룹, 정보 자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 통제하고 있는가? | | |
| **점검 현황** | VPC에서 서브넷 영역을 논리적으로 분리하여 네트워크 접근을 통제하고 있다.  테이블이(가) 표시된 사진  자동 생성된 설명 | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec303 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 네트워크 접근 | 불충족 |
| **항목명** | 외부 네트워크 접근 통제 | | |
| **요구사항 내용** | 데이터베이스 서버 등 중요 시스템이 외부와의 연결을 필요로 하지 않은 경우 사설 IP로 할당하여 외부 IP 접근 통제를 하고 있는가? | | |
| **점검 현황** | VPC를 통해 웹 서버, 데이터베이스 등에 A클래스 대역의 IP를 할당하여 외부 네트워크를 접근 통제를 하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec304 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 네트워크 접근 | 불충족 |
| **항목명** | 무선 네트워크 접근 통제 | | |
| **요구사항 내용** | 무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화 등 무선 네트워크 보호대책을 적용하고 통제하고 있는가? | | |
| **점검 현황** | SK헬스 내부에서 무선 네트워크를 사용하고 있지 않으므로 해당 요건은 점검 사항에서 제외한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**정보시스템 접근**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec305 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 정보시스템 접근 | 불충족 |
| **항목명** | 정보시스템에 대한 접근 수단 정의 및 접근 통제 | | |
| **요구사항 내용** | 서버, 네트워크시스템, 보안시스템 등 정보시스템 별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가? | | |
| **점검 현황** | 텍스트이(가) 표시된 사진  자동 생성된 설명IAM를 통해 사용자 별 접근 가능한 서비스를 제한하고 있다.  텍스트이(가) 표시된 사진  자동 생성된 설명VPC의 보안 그룹을 통해 EC2 인스턴스에 접근 가능한 위치와 수단을 정의하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec306 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 정보시스템 접근 | 불충족 |
| **항목명** | 정보시스템 접근에 대한 사용자 인증 통제 적용 | | |
| **요구사항 내용** | 정보시스템 및 개인정보처리시스템에 대한 접근 시 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전하게 식별하고 통제하고 있는가? | | |
| **점검 현황** | IAM 기본 암호정책으로만 접근 제한을 하고 있음     1. 암호 최소 길이 2. 암호 만료 시 관리자 재설정 필요 3. 암호 재사용 제한 4. 사용자 자신의 암호 변경 허용 5. 암호 만료 활성화 | | | |
| **보안요건 조치 방안** | IAM에서 지정된 횟수의 로그인 시도가 실패한 경우 계정에서 사용자를 통제하는 잠금 정책을 생성해서 불법 로그인 시도를 제한할 수 있다. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec307 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 정보시스템 접근 | 불충족 |
| **항목명** | 정보시스템 접속 차단 | | |
| **요구사항 내용** | 정보시스템에 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가? | | |
| **점검 현황** | Single Sign-On를 통해 사용자가 일정 시간 업무처리를 하지 않을 경우 로그인할 수 있는 시간을 설정하여 시스템이 차단되도록 하고 있다.  텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec308 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 정보시스템 접근 | 불충족 |
| **항목명** | 서비스에 따른 독립된 서버 운영 | | |
| **요구사항 내용** | 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가? | | |
| **점검 현황** | VPC를 통해 서브넷을 구분하여 WEB, WAS, DB를 독립적으로 서버를 구성하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec309 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 정보시스템 접근 | 불충족 |
| **항목명** | 정보시스템 관계없는 서비스 차단 | | |
| **요구사항 내용** | 정보시스템의 사용 목적과 관련이 없거나 침해 사고를 유발할 수 있는 서비스 또는 포트를 확인하여 차단하고 있는가? | | |
| **점검 현황** | VPC NACL을 통해 WAS에 대한 인바운드 규칙(Flask, SSH, 동적 포트) 포트 범위를 오픈하고 나머지 허용되지 않는 포트를 차단한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**응용프로그램 접근**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec310 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 응용프로그램 접근 | 불충족 |
| **항목명** | 응용프로그램 접근 권한 제한 | | |
| **요구사항 내용** | 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근 권한을 설정하고 있는가? | | |
| **점검 현황** | SK헬스 서비스에 응용 프로그램의 영역은 점검 대상에서 제외한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec311 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 응용프로그램 접근 | 불충족 |
| **항목명** | 응용프로그램 중요정보의 노출 최소화 | | |
| **요구사항 내용** | 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하고 있는가? | | |
| **점검 현황** | SK헬스 서비스에 응용 프로그램의 영역은 점검 대상에서 제외한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec312 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 응용프로그램 접근 | 불충족 |
| **항목명** | 응용프로그램 세션 관리 | | |
| **요구사항 내용** | 일정 시간 동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가? | | |
| **점검 현황** | SK헬스 서비스에 응용 프로그램의 영역은 점검 대상에서 제외한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**데이터베이스 접근**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec314 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 데이터베이스 접근 | 불충족 |
| **항목명** | 데이터베이스 접근 통제 | | |
| **요구사항 내용** | 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근 통제 정책에 따라 통제하고 있는가? | | |
| **점검 현황** | IAM에서 일반 사용자 계정에 RDS의 전체 접근 권한인 AmazonRDSFullAccess 권한을 부여하고 있다. 정보시스템, 응용프로그램을 별도로 식별하고 있지 않다.  텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| **보안요건 조치 방안** | RDS 생성 시 퍼블릭 액세스 권한 설정해서 퍼블릭 IP주소를 할당하지 않고 VPC 내부의 인스턴스 및 응용프로그램만을 연결할 수 있게 한다. VPC 보안 그룹을 설정하여 데이터베이스 접근을 통제해야 한다.  데이터베이스에 접근하는 사용자를 식별하여 IAM에서 접근 권한을 알맞게 부여한다. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec315 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 원격접근 통제 | 불충족 |
| **항목명** | 단말기 접근 통제 | | |
| **요구사항 내용** | 내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근 통제 하고 있는가? | | |
| **점검 현황** | 현재 원격으로 정보시스템 운영 시 Client VPN 연결을 통해 단말에 대한 접근 통제는 불가능한 상태이다. | | | |
| **보안요건 조치 방안** | 단말기에서 Amazon Workspaces에 접근 후 내부 업무용 시스템 접근하도록 아키텍처를 구성하여 특정 단말에 대해 접근 통제 한다. | | | |

**원격접근 통제**

**인터넷 접속 통제**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec316 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 인터넷 접속 통제 | 불충족 |
| **항목명** | 외부 인터넷 접속 통제 | | |
| **요구사항**  **내용** | 주요 정보시스템(DB서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가? | | |
| **점검 현황** | VPC의 보안 그룹을 이용해 WAS, RDS에 대한 인터넷(HTTP, HTTPS 등)에 대한 접속을 통제하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec317 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 인터넷 접속 통제 | 불충족 |
| **항목명** | 망 분리 적용 및 통제 | | |
| **요구사항 내용** | 법령에 따라 인터넷 망 분리 의무가 부과된 경우 망 분리 대상자를 식별하여 안전한 방식으로 망 분리를 적용하여 접근 통제하는가? | | |
| **점검 현황** | 2개의 VPC로 망 분리하여 피어링 연결 설정을 통해 각각의 VPC를 연결하여 접근 통제하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**보안시스템 통제**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec318 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 보안시스템 통제 | 불충족 |
| **항목명** | 보안시스템 비인가자 접근 통제 | | |
| **요구사항 내용** | 보안시스템 관리자 등 접근이 허용된 인원수를 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? | | |
| **점검 현황** | IAM을 통해 일부 사용자한테만 접근 권한을 부여하여 보안시스템에 접근 가능한 인원수를 최소화하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

### **2.4 암호화 적용**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec401 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 중요정보 암호화 | 불충족 |
| **항목명** | 개인정보 및 주요 정보에 대한 암호화 적용 | | |
| **요구사항**  **내용** | 암호 정책에 따라 개인정보 및 중요 정보의 저장 시 암호화를 수행하고 있는가? | | |
| **점검 현황** | 텍스트이(가) 표시된 사진  자동 생성된 설명RDS를 생성할 때 암호화 활성화 기능을 통해 정보를 저장 시 암호화를 수행하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**중요정보 암호화**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec402 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 암호키 관리 | 불충족 |
| **항목명** | 암호키 접근 권한 관리 | | |
| **요구사항**  **내용** | 암호키 사용에 관한 접근 권한을 최소화하고 있는가? | | |
| **점검 현황** | KMS를 통해 암호키 사용 접근 권한을 설정하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**암호키 관리**

**비밀번호 암호화**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec403 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 비밀번호 암호화 | 불충족 |
| **항목명** | 비밀번호 암호화 적용 | | |
| **요구사항 내용** | 개인정보처리시스템에 저장 시 암호화 적용을 하고 있는가? | | |
| **점검 현황** | 텍스트이(가) 표시된 사진  자동 생성된 설명Secrets Manager를 통해 개인정보처리시스템에 저장 시 KMS 키를 사용하여 암호화하고 있다. | | | |
| **보안요건**  **조치 방안** | 공 란 | | | |

### **2.5 로깅 및 모니터링**

**로그 관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec501 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 로그 관리 | 불충족 |
| **항목명** | 로그 기록 보관 및 관리 | | |
| **요구사항 내용** | 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그를 보관 및 관리를 하고 있는가? | | |
| **점검 현황** | VPC Flow log를 사용하여 네트워크 시스템에 대해서 S3에 로그를 기록 관리하고 있다.  CloudWatch에서 로그 그룹을 설정해서 관리하고 있다. | | | |
| **보안요건**  **조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec502 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 로그 관리 | 불충족 |
| **항목명** | 로그 기록 접근 권한 설정 | | |
| **요구사항 내용** | 정보시스템의 로그 기록에 대한 접근 권한은 최소화하여 부여하고 있는가? | | |
| **점검 현황** | IAM 통해 계정에 S3와 CloudTrail에 대한 접근 권한을 부여하고 있다 | | | |
| **보안요건**  **조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec503 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 로그 관리 | 불충족 |
| **항목명** | 정보시스템 이상징후 인지를 위한 모니터링 | | |
| **요구사항 내용** | 정보시스템 관련 오류, 오‧남용(비인가 접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 하고 있는가? | | |
| **점검 현황** | Security Hub를 통해 정보시스템에 이상징후를 인지하고 대상 별로 모니터링하고 있다. | | | |
| **보안요건**  **조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec504 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 로그 관리 | 불충족 |
| **항목명** | 로그 시간 동기화 | | |
| **요구사항 내용** | 로그 및 접속 기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 각 정보시스템의 시간을 표준시간으로 동기화하고 있는가? | | |
| **점검 현황** | CloudWatch를 통해 정확한 로그를 분석하기 위하여 Local time zone을 설정하여 표준시간으로 동기화 하고 있다. | | | |
| **보안요건**  **조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec505 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 로그 관리 | 불충족 |
| **항목명** | 이상 행위 발생 시 신속한 분석 및 점검 | | |
| **요구사항**  **내용** | 내‧외부에 의한 침해 시도, 개인정보 유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가? | | |
| **점검 현황** | Detective를 통해 정보시스템에 접속하는 네트워크 트래픽, IP등 로그를 수집하고 모니터링하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec506 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 개인정보보호 | 불충족 |
| **항목명** | 개인정보처리시스템 법률 준수 검토 및 관리 | | |
| **요구사항 내용** | 개인정보처리시스템에 대한 접속 기록은 법적 요구사항을 준수할 수 있도록 관리하고 있는가? | | |
| **점검 현황** | 현재 CloudTrail을 통해 개인정보처리 시스템의 접속 기록을 남기고 있다.  1. 계정 식별자 (개인정보 취급자 ID)  2. 접속 일시(접속한 시간 또는 업무 수행 시간)  3. 접속지 정보(접속IP)  4. 처리 정보 주체 정보(이용자 ID, 및 개인정보)  5. 수행업무(조회, 변경, 입력, 삭제 등)  개인정보처리 시스템에 대한 접속 기록을 별도의 저장장치를 통해 백업하고 있지는 않음. | | | |
| **보안요건 조치 방안** | 기록 백업 방법 순서  1. S3에서 버전 관리를 사용해서 활성화시킨다.  2. SDK를 사용하여 기존의 S3 버킷에서 다른 버킷으로 복사한다.  3. Amazon Glacier를 사용하여 백업한다.  4. 자체 백업되는 프로덕션 서버로 백업한다. | | | |

### **2.6 보안관리**

**시험과 운영 환경 분리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec601 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 시험과 운영 환경 분리 | 불충족 |
| **항목명** | 시험 시스템과 운영시스템의 분리 | | |
| **요구사항 내용** | 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가? | | |
| **점검 현황** | 현재 SK헬스 클라우드 인프라는 운영시스템으로만 구성되어 있어 점검 항목에서 제외한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec602 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 시험 데이터 보안 | 불충족 |
| **항목명** | 실제 운영 데이터의 사용 제한 | | |
| **요구사항 내용** | 정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가? | | |
| **점검 현황** | 현재 SK헬스 클라우드 인프라는 운영시스템으로만 구성되어 있어 점검 항목에서 제외한다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**시험 데이터 보안**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec603 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 장애 관리 | 불충족 |
| **항목명** | 정보시스템의 장애 관리 | | |
| **요구사항 내용** | 정보시스템의 장애를 인지하고 탐지 및 관리를 하고 있는가? | | |
| **점검 현황** | GuardDuty를 통해 정보시스템의 이상행위를 탐지하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**장애 관리**

**클라우드 보안**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec604 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 클라우드 보안 | 불충족 |
| **항목명** | 클라우드 서비스 보안 통제 정책 이행 | | |
| **요구사항 내용** | 클라우드 서비스 이용 시 비인가 접근, 설정 오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 이행하고 있는가? | | |
| **점검 현황** | 접근 통제와 계정•권한 관리 항목에서 요구사항을 충족하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec605 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 클라우드 보안 | 불충족 |
| **항목명** | 클라우드 서비스 관리자 권한 보호대책 적용 | | |
| **요구사항 내용** | 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가된 접근, 권한 오남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근 통제, 감사 기록 등 보호대책을 적용하고 있는가? | | |
| **점검 현황** | 계정•권한 관리, 식별•인증, 암호화 로깅 모니터링에서 요구사항을 충족하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec606 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 공개서버 보안 | 불충족 |
| **항목명** | 공개서버 DMZ 설치 및 보안시스템 보호 | | |
| **요구사항 내용** | 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가? | | |
| **점검 현황** | VPC의 라우팅 테이블에 Web-Subnet을 연결하여 퍼블릭 서브넷으로 설정하고 Network Firewall에 연결하여 보호하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**공개서버 보안**

**패치관리**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec607 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 패치관리 | 불충족 |
| **항목명** | 공개 인터넷 접속을 통한 패치 제한 | | |
| **요구사항 내용** | 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가? | | |
| **점검 현황** | VPC의 보안 그룹을 통해 WAS의 인바운드 규칙에서 HTTP 포트를 막아 인터넷 접속 패치를 제한하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**악성코드 통제**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec608 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 악성코드 통제 | 불충족 |
| **항목명** | 악성코드 보호대책 이행 | | |
| **요구사항 내용** | 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보호대책을 이행하고 있는가? | | |
| **점검 현황** | WAF를 통해 Rule을 설정하여 다양한 악성코드 등 공격으로부터 보호대책을 이행하고 있다.  텍스트이(가) 표시된 사진  자동 생성된 설명 | | | |
| **보안요건 조치 방안** | 공 란 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **점검 항목** | Sec609 | | **점검**  **결과** | 충족 |
| **점검 기준** | **분류** | 취약점 점검 및 조치 | 불충족 |
| **항목명** | 최신 보안 취약점 분석 및 조치 | | |
| **요구사항 내용** | 최신 보안 취약점이 정보시스템에 미치는 영향을 분석하여 조치하고 있는가? | | |
| **점검 현황** | Security Hub를 통해 정보시스템에 미치는 보안 취약점을 심각도 별로 분류한다.  Inspector를 통해 정보시스템에 미치는 보안 취약점 분석하고 있다. | | | |
| **보안요건 조치 방안** | 공 란 | | | |

**취약점 점검**