Koreait 기관에서 사용자들의 보안 요구 사항을 분석하여 명세서를 작성하고 검증하고자 한다.

이에 주어진 시나리오 과제에 따른 문제를 해결하고 파일로 제출하시오.

1.1 ~ 1.2 아래의 보안요구사항에 대한 타당성 분석 및 결과 예시 화면에서 빈 칸에 적당한 내용을 서술하시오.

보안 요구사항	관련 법령 및 규정	타당성 분석 기준	타당성 분석 결과
정보는 허가된 사람만 열람할 수 있어야 한다.	• 전자정부법: 정보시스템의 안전성과 신뢰성 확보 • 정보통신망법: 정보보호조치에 관한 지침 준수 • 개인정보보호법: 개인정보에 대한 안전성 확보에 필요한 기술적·관리적 및 물리적 조치	• 정보에 대한 보안 등급 마련의 실현 가능성(일정, 예산 등) • 보안 등급을 고려한 온라인 접근, 오프라인 접근 방안 마련의 실현 가능성(일정, 예산 등) • 개인정보 암호화대상 확인 및 열람권한 부여 기능 실현 가능성(일정, 예산 등)	✓ 정보에 대한 보안등급 마련에 외부 전문가 활용하여 약 2개월 및 XXX원 소요되고 예산이 있으므로 타당성 있음.
모바일에서 내려받는 앱은 무결성이 검증되어야 한다.	• 정보통신기반 보호법: 모바일 관련 취약점 분석 및 평가에 따른 물리적·기술적 대책 수립 및 시행	• 모바일 앱에 대한 난독화 툴 활용 등의 실현 가능성 • 휴대폰 도난 등으로 모바일을 통한 시스템 접근 등에 대한 보안통제 방안의 실현 가능성	✓
외부에서 접근할 수 있는 웹페이지는 취약점이 없어야 한다.	• 정보통신기반 보호법: 웹 관련 취약점 분석 및 평가에 따른 물리적·기술적 대책 수립 및 시행	•	✓ 웹 취약점 점검 항목 보완하는데 20개 사이트 2년 이상 소요로 단계적 취약점 제거부터 우선적으로 수행

1. [보안 요구사항] 모바일에서 내려받는 앱은 무결성이 검증되어야 한다 - 타당성 분석 결과

법령 준수를 위한 휴대폰 관련 보안 지침 마련에 약 1.5개월 소요되므로 타당성 있음

2. [보안 요구사항] 외부에서 접근할 수 있는 웹페이지는 취약점이 없어야 한다 – 타당성 분석 기준

웹 취약점 점검의 모든 항목을 구현할 경우의 개발 일정 및 예산

1.3 ~ 1.4 보안 침해 시나리오에 의해 웹서버/DBMS의 경우 DDoS공격과 SQL Injection공격에 대해 취약한 부분이 확인되었을 때 IT자원에 대한 중요도를 5점 척도로 나타내고 보안요구사항의 우선순위 설정 시 전화면접과 대면면접을 실시할 예정으로 이에 대한 장단점에 대해 서술하시오.

	매우 아니다 (1)	아니다 (2)	보통이다 (3)	그렇다 (4)	매우그렇다 (5)
보안 요구사항을 구축하지 않을 시 보안 침해 발생 가능성이 높을 것으로 평가하는가?					●
보안 요구사항을 구축하지 않을 시 보안 침해로 인한 피해규모가 클것으로 평가하는가?					●
보안 요구사항이 관리적 중요도 관점에서 보안 침해 예방에 도움이 될 것으로 평가하는가?					●
보안 요구사항이 물리적 중요도 관점에서 보안 침해 예방에 도움이 될 것으로 평가하는가?					●
보안 요구사항이 기술적 중요도 관점에서 보안 침해 예방에 도움이 될 것으로 평가하는가?					●

DDoS 공격과 SQL Injection 공격은 웹 서버를 마비시켜 서비스 중단을 초래할 수 있으며 특히 SQL Injection의 경우 데이터 유출, 조작, 계정 탈취까지 발생할 수 있어 피해가 매우 심각하다. 따라서 두 공격 유형의 중요도는 5점으로 매우 높은 수준이다.

전화면접의 장점은 조사의 취지와 항목에 대한 정확한 설명과 이해가 가능하여 설문조사의 신뢰도가 높아진다. 단점으로는 전화 면접 수행 인력의 인건비가 부담되고, 전화 통화를 거부하거나 스팸으로 신고할 가능성이 있다.

대면면접의 장점은 조사의 취지에 맞는 가장 정확한 설문조사가 가능하다. 단점으로는 대면 방문 인력에 대한 교육이 필요하고 조사 대상 확장의 한계가 크다.

2.1 ~ 2.2 위의 내용을 토대로 IT자원에 대한 보안요구사항의 우선순위 선정을 위해 영향도 분석 및 최신 기술 동향에 대해 알아보려고 한다. 이 때 최신 기술 동향을 파악하기 위한 방법에 대해 서술하시오.

최신 기술 동향을 파악하기 위한 방법으로는

1. HW 및 상용 SW 제조업체를 알아보고 기술 설명회를 진행한다.

2. IEEE, Springer, ACM 등의 보안 관련 저널, 논문 및 학술 자료를 참고하여 최신기술의 연구 결과와 이론적 기반을 이해할 수 있다.

3. Black Hat, DEFCON, RSA Conference, POC 등 국내외 보안 관련 세미나 및 행사에 참여하여 최신 위협 정보, 기술 트렌드, 보안 사고 사례등을 직접 접해볼 수 있다.

4. GitHub, Stack Overflow 등에서 공유되는 최신 도구, 취약점 분석 자료, 실습 환경 등을 통해 실무적인 트렌드를 파악할 수 있다.

5. KISA(한국인터넷진흥원), ENISA(유럽 정보보호기구), NIST(미국 국립표준기술연구소) 등에서 발행하는 연례 보안 위협 보고서, 기술 동향 분석 자료 등을 참고함으로써 신뢰도 높은 정보를 얻을 수 있다.

2.3 ~ 2.4 아래 문서는 보안요구사항 명세 항목의 일부분으로 취약점 점검 시 확인한 DDoS, SQL Injection공격에 대한 명세 항목을 추가하여 작성하시오.

서버-UNIX	네트워크 장비	DB서버
계정관리 - 패스워드 관리 - 사용자 관리 - 운영자 관리	접근통제 - 관리자 계정 - 사용자 계정 - 네트워크 설정값의 유지	계정관리 - 계정 생성 및 폐기 - 입력 오류 탐지 - 접근 권한 관리
접근통제 - 구동파일 - 시스템 권한 - 원격 접근 - 파일 소유 등	운영통제 - 취약점 관리 - 장비 설정 변경 - 장비 철거 관리	로그관리 - 접근 및 관리 로그 - 감사로그 관리
로그관리 - 로그관리 및 보고 - 장애 관리 등	...	...

각 항목에 공격에 대한 명세 항목 추가

서버 – UNIX	네트워크 장비	DB 서버
공격 및 대응 관리 - DDoS 트래픽 탐지 및 차단 - DDoS 대응 매뉴얼 수립	공격 대응 및 방어 관리 - DDoS 대응 설정 - 이상 트래픽 탐지 시스템 연동	공격 대응 및 방어 관리 - SQL Injection 방지 - WAF, 쿼리 로그 수집 및 분석 - DB 접근 제어 및 이상 행위 탐지

3.1 보안요구사항의 오류를 검증하기 위한 검증기준 정의 시 보안요구사항 명세서의 최신 버전 확인에 대한 3가지 항목에 대해 서술하시오.

1 .버전 관리 및 변경 이력 확인

보안요구사항 명세서가 체계적으로 버전 관리되고 있는지 확인하며, 변경 이력을 통해 요구사항이 최신 위협에 따라 적절히 갱신되었는지를 점검한다. 각 변경사항에 대한 사유가 명확히 기록되어 있어야 하며, 이전 버전과의 비교를 통해 오류나 누락이 발생하지 않았는지 검토한다.

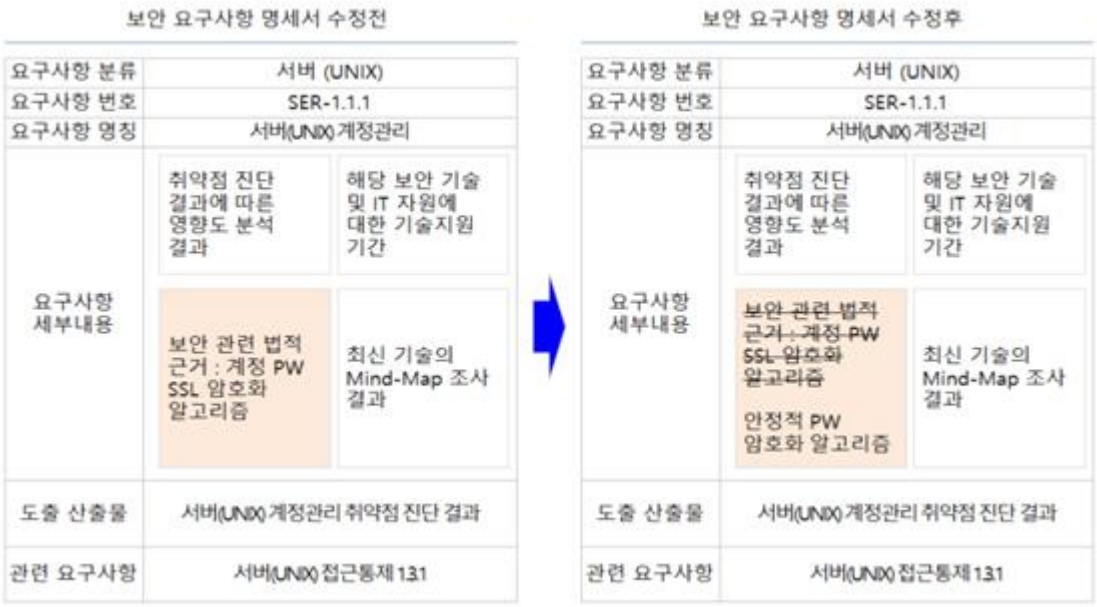
2. 최신 보안 위협 및 규제 반영 여부 확인

보안요구사항이 DDoS, SQL Injection 등 최신 보안 위협을 반영하고 있으며, OWASP Top 10, 개인정보보호법, 정보보호 관리체계(ISMS) 등의 관련 규제 기준을 충실히 따르고 있는지를 확인한다. 최신 위협에 대한 대응이 미비하거나 누락된 경우 오류로 간주된다.

3. 요구사항 간 정합성 및 누락 항목 확인

요구사항 간에 논리적 모순이나 중복이 존재하지 않으며, 각 시스템 영역(서버, 네트워크, DB 등)에 필요한 보안 항목이 빠짐없이 명시되어 있는지를 점검한다. 최신 버전이라 하더라도 특정 항목이 누락되었거나 일관성이 없으면 오류로 판단할 수 있다.

3.2 ~ 3.3 아래 그림은 보안 요구사항 명세서 수정 전/후를 도식화한 것으로 앞서 확인한 취약점 (DDoS/SQL Injection)에 대한 요구사항 세부내용을 작성하시오.



보안 요구사항 명세서 수정전

요구사항 분류	서버 (UNIX)	
요구사항 번호	SER-1.1.1	
요구사항 명칭	서버(UNIX) 계정관리	
요구사항 세부내용	취약점 진단 결과에 따른 영향도 분석 결과	해당 보안 기술 및 IT 자원에 대한 기술지원 기간
	보안 관련 법적 근거 : 계정 PW SSL 암호화 알고리즘	최신 기술의 Mind-Map 조사 결과
도출 산출물	서버(UNIX) 계정관리 취약점 진단 결과	
관련 요구사항	서버(UNIX) 접근통제 1.3.1	

보안 요구사항 명세서 수정후

요구사항 분류	서버 (UNIX)	
요구사항 번호	SER-1.1.1	
요구사항 명칭	서버(UNIX) 계정관리	
요구사항 세부내용	취약점 진단 결과에 따른 영향도 분석 결과	해당 보안 기술 및 IT 자원에 대한 기술지원 기간
	~~보안 관련 법적 근거 : 계정 PW SSL 암호화 알고리즘~~ 안정적 PW 암호화 알고리즘	최신 기술의 Mind-Map 조사 결과
도출 산출물	서버(UNIX) 계정관리 취약점 진단 결과	
관련 요구사항	서버(UNIX) 접근통제 1.3.1	

요구사항 세부내용 추가

요구사항 세부내용	DDoS 대응을 위한 ACL 설정 및 Rate-Limit 설정 여부 확인	이상 트래픽 감지를 위한 로그 수집 및 분석 체계 존재 여부 확인
	사용자 입력값 검증 여부 확인	- SQL Injection 방지를 위한 Prepared Statement 적용 여부 확인 - 입력값 필터링, WAF 탐지 룰 적용 여부 확인