

[붙임4] 취약점 분석·평가 점수 산출식 예시

□ 개요

- 각 취약점 점검항목에 대한 취약점 점수 지정 및 진단결과값 산출
- 관리적·물리적·기술적 취약점 점수 계산
 - 단, 기술적 취약점 점수는 각 자산별 점수의 평균으로 계산
- 관리적·물리적·기술적 취약점 점수를 합산
- 망분리 현황에 따른 비율 지정
- 합산된 관리적·물리적·기술적 취약점 점수에 망분리 비율을 적용하여 종합점수 산출

□ 취약점 점수 지정 및 진단결과값 산출

- 각 취약점 점검항목에 대해 중요도에 따라 점수 지정
 - ‘상’(필수항목): 10점, ‘중’(추가항목): 8점, ‘하’(추가항목): 6점
- 각 취약점 점검항목에 대해 진단결과값 산출

진단결과	평가항목의 중요도		
	상	중	하
○ (취약점 발견)	10점	8점	6점
× (취약점 제거)	0점	0점	0점
P (일부 취약점만 제거)	5점	4점	3점

□ 관리적·물리적 취약점 점수 계산

- 관리적·물리적 취약점 점검항목에 따라 취약점 점수를 각각 계산
- 점수 계산 방법
 - 모든 취약점이 식별되었을 경우의 점수합: A
 - 식별된 취약점들의 점수합: B
 - 계산식: $\frac{A-B}{A} \times 100$

□ 기술적 취약점 점수 계산

- 기술적 취약점 점검항목에 따라 자산별로 취약점 점수를 계산

- 모든 취약점이 식별되었을 경우의 점수합: A
- 식별된 취약점들의 점수합: B
- 계산식: $\frac{A-B}{A} \times 100$

o 자산별 점수를 합산하여 전체 자산 점수의 평균을 계산

- 자산의 수: N
- 자산별 점수: S1, S2, ..., Sn
- 계산식: $\sum_{n=1}^N S_n \div N$

□ 취약점 점수 합산

o 관리적·물리적·기술적 취약점 점검항목수의 비율을 고려하여 점수 합산

< 계 산 식 >	
·A : (관리적 취약점 점수 X 관리적 취약점 점검항목수)	
·B : (물리적 취약점 점수 X 물리적 취약점 점검항목수)	
·C : (기술적 취약점 점수 X 기술적 취약점 점검항목수)	
$\Rightarrow \frac{A+B+C}{\text{전체취약점점검항목수}}$	

□ 망분리 비율 지정

o 망분리의 종류에 따라 비율을 지정

구분	설명	적용 비율
물리적 분리	내부 네트워크와 외부 네트워크를 별도로 구축하였으며, 접점이 존재하지 않음	100%
논리적 분리	가상화 기술 등을 이용해 소프트웨어적으로 망 분리 또는 내부 네트워크와 외부 네트워크가 분리되어 있으나 접점이 존재하는 경우	95%
미분리	내부 네트워크와 외부 네트워크가 분리되지 않음	90%

※ 해당시설이 인터넷 연결이 반드시 필요한 경우에는 망 분리 비율을 적용하지 않음

□ 종합점수 산출

o 취약점 점수 합산값에 망분리 비율을 적용하여 최종 계산

- 전체 취약점 점수: A
- 지정된 망분리 비율: B

- 종합점수 계산식: $A \times B$

□ 점수 계산 예제

o 가정사항

- 관리적 취약점 점수 : 80점(점검항목수 10개)
- 물리적 취약점 점수 : 70점(점검항목수 5개)
 - ※ 관리적, 물리적 취약점 점수 계산과정은 18페이지에 기술되어 있으므로 생략하고
기술적 취약점 점수 계산과정을 중심으로 설명
- 대상자산 : 서버 1, 서버 2, 서버 3
- 정의된 취약점과 점수(점검항목 등급을 반영)

번호	취약점명	취약점 등급	점수
#1	시스템 정보 노출	상	10
#2	추측가능한 패스워드 사용	상	10
#3	패스워드가 없는 계정 존재	상	10
#4	Guest 계정 존재	상	10
#5	불필요한 서비스 활성화	상	10
#6	Anonymous FTP 활성화	상	10
#7	쓰기 가능한 Anonymous FTP 활성화	중	8
#8	SMTP expn/vrfy 명령을 통한 시스템 정보 획득 가능	중	8
#9	구 버전의 SNMP 사용	하	6
#10	쓰기 가능한 공유 폴더 존재	중	8
합 계			90

- 자산별로 식별된 취약점

번호	서버 1	서버 2	서버 3
#1	○		
#2	○	○	○
#3			○
#4			○
#5		○	○
#6			○
#7			
#8			
#9	○		
#10			

- 망분리 현황: 논리적 분리

o 점수 계산 절차

- 자산별로 기술적 취약점 식별 후, 점수를 계산(서버 3대 × 10개 점검항목)

번호	서버 1	서버 2	서버 3	점수
#1	○			10
#2	○	○	○	10
#3			○	10
#4			○	10
#5		○	○	10
#6			○	10
#7				8
#8				8
#9	○			6
#10				8
장비별 점수	71 $\frac{90-26}{90} \times 100$	78 $\frac{90-20}{90} \times 100$	44 $\frac{90-50}{90} \times 100$	
	※ 모든 취약점 점수의 합 : 90점			

- 기술적 취약점 점수 : $(71 + 78 + 44) / 3 = 64$ 점

(3개 자산의 점수를 합산하여 평균을 계산)

- 관리적·물리적·기술적 취약점 점수 합산 : $(80\text{점} \times 10\text{개}) + (70\text{점} \times 5\text{개}) + (64\text{점} \times 10\text{개}) / (10\text{개} + 5\text{개} + 10\text{개}) = 71\text{점}$

< 계 산 식 >

- A : (관리적 취약점 점수 X 관리적 취약점 점검항목수)
- B : (물리적 취약점 점수 X 물리적 취약점 점검항목수)
- C : (기술적 취약점 점수 X 기술적 취약점 점검항목수)

$$\Rightarrow \frac{A+B+C}{\text{전체취약점점검항목수}}$$

- 망분리 비율: 95%

(논리적 분리이므로 95%를 부여)

- 종합점수 계산: 71점 × 95% = 67점

(망분리 비율을 곱셈하여 종합점수를 계산)