情 報 保 護 學 會 誌
第19卷 第6號, 2009. 12

주요정보통신기반시설 보호를 위한 취약점 분석·평가 관리 방안

박 순 태*, 이 완 석*, 노 봉 남**

요 약

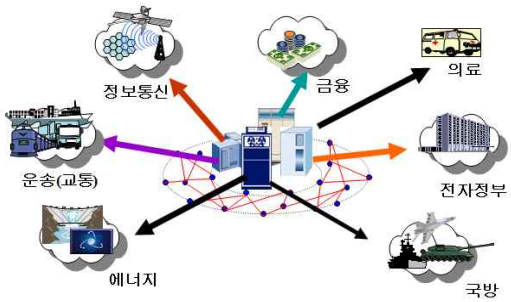
국내에서는 정보통신기반시설의 중요성을 인식하고 2001년부터 정보통신기반보호법을 제정하여 이중 국가·사회적 중요성이 높은 시설을 주요정보통신기반시설로 지정하여 국가차원의 관리를 하고 있다. 이러한 주요정보통신기반시설에 대하여 해당 관리기관은 시설에 대한 취약점 분석·평가를 실시하고 있다. 본고에서는 관리기관이 자체 수행 또는 외부 컨설팅 기관을 이용하여 해당 시설에 적합한 취약점 분석·평가가 이루어질 수 있도록 취약점 분석·평가 관리 방안을 제시하였다. 또한 방송·통신 분야 주요정보통신기반시설에 적용한 사례를 분석함으로써 분야별 취약점 분석·평가 관리 방안 적용결과를 검증하였다. 주요정보통신기반시설을 보유한 관리기관별 또는 소관 분야 주요정보통신기반시설을 관리하는 관계중앙행정기관은 제안하는 방안을 활용하여 해당 시설에 적합한 취약점 분석·평가를 수행 또는 관리할 수 있을 것이다.

Ⅰ. 서 론

국내에서는 2001년 금융·통신·에너지 등 국가와 사회의 중요한 정보통신기반시설을 체계적으로 보호하기 위하여 정보통신기반보호법을 제정 및 공포하였다. 『정보통신기반보호법』에서는 해킹, 컴퓨터바이러스, 기타 악성프로그램 유포를 비롯한 전자적 침해행위 수법의 급속한 발전과 더불어 그 피해가 증가함에 따라 정보통신기반시설에 대한 체계적인 보호와 관리를 할 수 있도록 주요정보통신기반시설의 지정 및 보호를 위한 예방·대응·복구 등과 관련한 규정을 다루고 있다.

정보통신기반시설이란 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호의 규정에 의한 정보통신망을 가리킨다.

또한 주요정보통신기반시설이란 관계 중앙행정기관이 전자적 침해 행위로부터 보호가 필요한지 여부를 정보통신기반보호법 제8조 규정에 의한 지정 기준을 고려하여 지정한 정보통신기반시설을 의미한다.[1] 이러한 주요정보통신기반시설을 개념적으로 나타내면 그림1과 같이 표현할 수 있다[2].



[그림 1] 주요정보통신기반시설 개념

분야별 정보통신기반시설은 법에서 정한 5가지 기준에 따라 중요도를 판단하여 주요정보통신기반시설로 지정하게 된다. 주요정보통신기반시설로 지정되면 6개월 이내에 취약점 분석·평가를 실시하여야 한다. 이후 매년 취약점 분석·평가를 실시하게 된다. 취약점 분석·평가 결과를 바탕으로 관리기관은 즉시 및 장·단기 조치를 하게 된다. 이러한 사항을 차기년도 보호대책 수립

* 한국인터넷진흥원({cptpark, wsyi}@kisa.or.kr)
** 전남대학교 시스템보안연구센터(bbong@jnu.ac.kr)

시 반영하여 주요정보통신기반시설에 대한 보호활동을 하게 된다. 또한 보호대책에서 수립한 각종 정보보호 조치사항이 계획한 대로 이루어졌는지에 대하여 다음해에 보호대책 이행여부 점검을 받게 된다. 이러한 일련의 과정을 통해 체계적인 주요정보통신기반시설 보호활동이 이루어진다.[3] 본고에서는 방송·통신 분야를 중심으로 주요정보통신기반시설의 지정으로부터 취약점 분석·평가 수행, 보호대책 수립 등 관련된 프로세스와 기존 취약점 분석·평가 관리가 적절히 수행되었는지를 살펴본다. 또한 이를 개선하기 위한 방안 및 적용 사례를 제시하여 주요정보통신기반시설 관리기관이나 소관 부처가 정책방향을 수립하는데 도움을 주고자 한다.

Ⅱ. 관련 프로세스

2.1 주요정보통신기반시설의 지정

『정보통신기반보호법』에서는 정보통신기반시설중 아래와 같이 5가지 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있도록 규정하고 있다.

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성
2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

법에서 정한 5가지 기준을 바탕으로 관련 부처 즉 관계중앙행정기관의 장은 주요정보통신기반시설의 지정여부 평가를 위한 기준을 마련하여 지정 대상 시설 관리기관의 장에게 통보할 수 있도록 정보통신기반보호법 시행령에서 세부사항을 규정하고 있다. 방송·통신 분야의 경우 표 1과 같이 세부 기준을 정하여 주요정보통신기반시설 지정에 활용하고 있으며, ISP 등에 대하여 주요정보통신기반시설 지정을 위한 세부 지표등을 검토할 수 있다.[2]

[표 1] 주요정보통신기반시설 지정 기준

지정 기준	세부 기준
당해기관 업무의 국가·사회적 중요성	국가/대국민 서비스 중요성
	취급정보의 중요도
당해기관 업무의 정보통신기반시설에 대한 의존도	시설에 대한 업무 의존도
	서비스의 연속성 의존도
다른 정보통신기반시설과의 상호연계성	시설의 타기관 연계성(연계량)
	시설의 타기관 연계성(연계질)
	시설기능 장애의 파급효과
침해사고 발생시의 피해규모 및 범위	업무수행 지속능력
	국가위기 초래정도 (지역적 피해범위)
	국가위기 초래정도 (체감 피해범위)
	정보유출 피해범위
침해사고 발생가능성 또는 복구의 용이성	전자적 침해 발생 가능성
	복구 요구 시간

2.2 주요정보통신기반시설의 취약점 분석·평가

『정보통신기반보호법』에서는 주요정보통신기반비설로 지정되면 6개월 이내에 취약점 분석평가를 실시토록 하고 있다.

정보통신기반시설에 대한 취약점 분석·평가 절차는 주요정보통신기반시설의 지정 여부와 관계없이 그림2와 같이 순환되는 사이클을 적용할 수 있다. 가장 우선적으로 전담반을 구성하여 취약점 분석·평가 계획을 수립한다. 이후 계획에 따라 취약점 분석·평가 대상을 선별하고, 다음 단계에서 선별된 대상에 대한 위협요인 및 취약점 분석을 실시한다. 다음 단계는 취약점 분석·평가된 결과를 바탕으로 기반시설의 위험(수준)을 평가한다. 마지막으로 취약점 분석·평가 대상 시설에 대한 보호대책을 수립하게 된다.

[그림 2] 취약점 분석·평가 절차

주요정보통신기반시설 관리기관은 자체 전담반을 구

성하거나 취약점 분석·평가시 객관성 및 실효성 확보, 전담반의 전문성 보강 등을 위하여 법에서 정한 외부 전문기관을 활용할 수 있다. 정보통신기반보호법에서 정한 취약점 분석·평가 기관은 한국인터넷진흥원, 대통령령이 정하는 기준을 충족하는 정보공유분석센터(ISAC : Information Sharing and Analysis Center), 법의 의해 지정된 지식정보보안컨설팅전문업체, 한국전자통신연구원 등이 있다. 현재 지식경제부에 의해 지정된 지식정보보안컨설팅전문업체는 표 2와 같다.

[표 2] 지식정보보안컨설팅전문업체 현황

지정 기관명	URL
롯데정보통신	http://www.ldcc.co.kr
시큐아이닷컴	http://www.secui.com
안철수연구소	http://www.ahnlab.com
인젠	http://www.inzen.com
인포섹	http://www.goinfosec.co.kr
A3 Security	http://www.a3security.com
STG 시큐리티컨설팅	http://www.stgsecurity.com

2.3 주요정보통신기반시설 보호대책 수립 및 이행

취약점 분석·평가를 완료한 관리기관은 보유한 주요정보통신기반시설을 효과적으로 보호하기 위하여 법에서 규정한 바에 따라 매년 보호대책을 수립하게 된다. 취약점 분석·평가 결과는 즉시, 단기, 중·장기로 구분하여 비용효과적으로 추진하게 된다. 이때 중요한 고려 요소는 관리기관의 가용 자산, 자산 및 자산이 제공하는 서비스의 중요도, 보호대책 수립비용 대비 효과 등 이다. 보호대책은 각 자산에서 발견된 위협요인 또는 취약점을 감소시키기 위하여 관리적·물리적·기술적 보호대책을 선별 또는 병행하여 사용할 수 있다. 또한 예전에 주요정보통신기반시설로 지정되었다면 계획된 보호대책을 포함한 기존의 보호대책 분석 결과를 검토하여 보호대책의 보완사항을 변경하거나 신규 보호대책을 추가할 수 있다. 관리기관이 보유한 주요정보통신기반시설에 대한 보호대책은 소관 부처 즉 관계중앙행정기관에 제출하여 부처가 마련하는 해당 분야 주요정보통신기반시설 보호계획 수립에 활용 된다.

2.4 주요정보통신기반시설 보호대책 이행 여부 확인

『정보통신기반보호법』에서는 주요정보통신기반시설 지정 후 보호대책에 대한 실효성을 높이고 사후관리 등을 위하여 주요정보통신기반시설에 대한 이행 여부를 확인할 수 있도록 규정하고 있다. 현재 법은 사후관리 체계에 대한 별도의 사항을 규정하고 있지 않기 때문이다. 관리기관의 인수·합병, 분할 등 변화되는 상황과 기반시설변경 사항을 포함하여 최초 취약점 분석·평가를 통해 수립한 보호대책의 목적과 목표를 달성하였는지를 확인하게 된다.

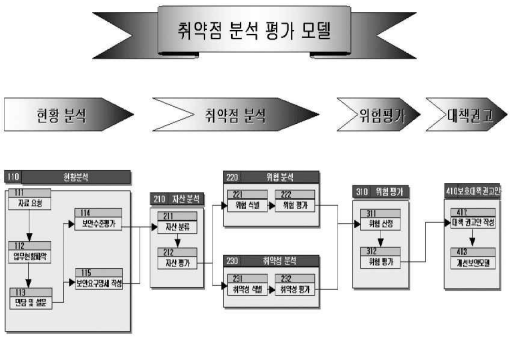
Ⅲ. 기존 취약점 분석·평가 및 관리

3.1 취약점 분석·평가 기준

『정보통신기반보호법』에서는 행정안전부 장관과 국가정보원장이 취약점 분석·평가에 관한 기준을 정하고, 이를 해당 관계중앙행정기관에 통보토록 하고 있다. 이때 취약점 분석·평가기준에 포함될 사항으로는 취약점 분석·평가의 절차, 취약점 분석·평가의 범위 및 항목, 취약점 분석·평가의 방법 등이 있다.

3.2 취약점 분석·평가 방법론

한국정보보호진흥원(현 한국인터넷진흥원)은 주요정보통신기반시설 관리기관 및 정보보호컨설팅전문업체가 활용하도록 2002년 취약점 분석·평가 모델을 개발하여 제공하였다.[4] KISA에 개발한 취약점 분석 평가 모델은 그림 3과 같이 현황분석, 취약점 분석, 위험평가, 대책 권고 순으로 진행되며 4단계 8개 프로세스 및 22개의 태스크로 구성된다.



[그림 3] 취약점 분석·평가 모델

취약점 분석·평가를 실시하는 주요정보통신기반시설 관리기관은 KISA가 제공한 취약점 분석·평가 모델, IPAK(Information Protection Assessment Kit), IAM(INFOSEC Assessment Methodology), VAF (Vulnerability Assessment Framework), OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)[5], Risk Management Guide for IT Systems 등을 참고하여 기관 실정에 맞는 방법론을 사용한다.

3.3 취약점 분석·평가 적절성 검토

주요정보통신기반시설 관리기관은 매년 취약점 분석·평가를 실시하고 그 결과를 정리하여 추진할 보호조치를 차기년도 주요정보통신기반시설 보호대책 수립에 반영한다. 주요정보통신기반시설에 대한 보호 조치는 보호대책서에 정의한 바에 따르게 되며 기반시설 및 관리기관 특성에 맞게 잘 수행된 취약점 분석·평가 결과가 보호대책서의 품질을 좌우하게 된다.

방송·통신 분야의 경우 방송통신위원회가 주관하여 소관 분야 주요정보통신기반시설 관리기관에 대한 보호대책 수립을 지원하기 위하여 한국인터넷진흥원 및 학·연 전문가로 이루어진 전문가그룹에 의한 보호대책 수립의 적절성을 검토한다. 이때 취약점 분석 평가가 해당 기관 및 시설의 특성을 반영하고 적절히 수행되었는지에 대한 검토를 병행한다.

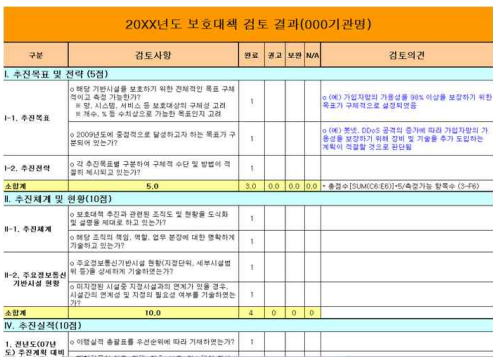
Ⅳ. 취약점 분석·평가 관리 개선 방안

4.1 기존 취약점 분석·평가 적절성 검토의 문제점

취약점 분석·평가에 대한 적절성 검토는 보호대책 검토의 일부로서 수행되었다. 주요정보통신기반시설 관리기관이 작성하는 보호대책에 대한 검토는 매년 해당 분야 관계중앙행정기관에서 제공하는 보호대책 수립 지침에서 정한 형식과 내용에 따라 보호대책 수립의 적절성 및 완성도를 검토한다.

취약점 분석·평가가 적절히 수행되었는지에 대한 확인 방법은 관리기관의 규모와 특정을 고려하지 않고 획일적이고, 단순 점검만 시행하였다. 기관별 112개 점검항목에 대하여 완료, 권고, 보완으로 구분하여 체크리스트 점검 및 의견을 기술하는 것이다. 그림 4와 그림 5에 보호대책을 검토하는 체크리스트 및 취약점 분석·평가에 대한 적절성 여부 검토 방법을 예로 들었다.

기존의 방법은 다양한 관리기관 및 주요정보통신기반시설의 특성을 반영하지 못하였으며 체크리스트에 의한 점검이 이루어지다 보니 취약점 분석·평가가 잘 되었는지 관리적·물리적·기술적 부분에 대한 심층적인 분석이 어려웠다. 또한 각 항목의 적절성에 대한 검토가 보호대책 검토에 참여하는 외부 전문가의 개인적인 역량과 주관에 의존하는 문제점이 있었다.


20XX년도 보호대책 검토 결과(000기관명)

구분	검토사항	완료	권고	보완	N/A	검토의견
I. 추진목표 및 전략 (5점)						
I-1. 추진목표	○ 해당 기반시설을 보호하기 위한 전체적인 목표 구체적이고 측정 가능한가? ※ 망, 시스템, 서비스 등 보호대상의 구체성 고려 ※ 계수, % 등 수치상으로 가능한 목표인지 고려	1				○ (예) 가입자망의 가용성을 99% 이상을 보장하기 위한 목표가 구체적으로 설정되었음
	○ 2009년도에 중점적으로 달성하고자 하는 목표가 구분되어 있는가?	1				○ (예) 정년, DDoS 공격의 증가에 따라 가입자망의 가용성을 보장하기 위해 장비 및 기술을 추가 도입하는 계획이 적절할 것으로 판단됨
I-2. 추진전략	○ 각 추진목표별 구분하여 구체적 수단 및 방법이 적절히 제시되고 있는가?	1				
소합계	5.0	3.0	0.0	0.0	0.0	* 총점수(SUM(C6:E6))*5/측정가능 항목수 (3-F6)
II. 추진체계 및 현황(10점)						
II-1. 추진체계	○ 보호대책 추진과 관련된 조직도 및 현황을 도식화 및 설명을 제대로 하고 있는가?	1				
	○ 해당 조직의 책임, 역할, 업무 분장에 대한 명확하게 기술하고 있는가?	1				
II-2. 주요정보통신기반시설 현황	○ 주요정보통신기반시설 현황(지정단위, 세부시설별 위 등)을 상세하게 기술하였는가?	1				
	○ 미지정된 시설중 지정시설과의 연계가 있을 경우 시설간의 연계성 및 지정의 필요성 여부를 기술하였는가?	1				
소합계	10.0	4	0	0	0	
IV. 추진실적(10점)						
1. 전년도 07년도) 추진계획 대비	○ 이행실적 총괄표를 주선순위에 따라 기재하였는가?	1				

[그림 4] 보호대책 검토 방법 예시


취약점 분석 평가 검토 결과(000기관명)

구분	검토사항	완료	권고	보완	N/A	의견
Ⅲ. 취약점 분석 평가 결과(30점)						
3.1. 개요		0	0	0	0	
	○ 취약점 분석평가 수행내역(수행기간, 수행대상, 수행주체, 소요예산, 관련조직 등)을 상세하게 기술하고 있는가?					
3.2. 점검방법 및 주요내용		0	0	0	0	
	○ 취약점 분석/평가 수행방법, 수행단계 및 중점 점검분야에 대해 구체적으로 기술하고 있는가?					
	○ 공격 시나리오 구성 및 모의해킹을 통해 침해사고 예방대책을 마련하였는가?					
	○ 취약점별 대책을 도출하고 전체 의견을 종합하여 중장기적 관점의 보호대책 추진계획을 정리하였는가?					
	○ 이전 취약점 분석평가에 의해 발견된 취약점을 중점 점검 분야에 포함하였는가?					
3.3. 점검결과 및 개선방향		0	0	0	0	
	○ 취약점 분석 평가 결과 도출된 취약점에 대하여 현황을 기록하고 조치계획을 정리하였는가?					
	○ 위험수준이 높은 취약점을 중심으로 현 상황에 대한 문제점과 의견을 기술하고 향후 보호대책에 대하여 기술하였는가?					
3.4 관리적 취약점 점검 항목		0	0	0	0	
	○ 정보보호정책 수립	0	0	0	0	
	- 주요정보통신기반시설의 자체 정보보호정책 수립 및 문서화 미비					
	- 상위 관리자에 의한 정보보호정책의 승인 절차 부재					
	- 컴퓨팅 환경 변화에 따른 정보보호정책의 정기적 검토, 개선 및 관계자 제공 소홀					
	- 보안사고 발생시 보고절차가 정책에 미반영					
	- 보안사고 유형과 사고조치 절차에 대한 관리원의 숙지 미흡					
	○ 정보보호조직 및 인력 보안	0	0	0	0	
	- 정보보호 전담조직의 구성, 운영 미흡					
	- 정보보호 전담조직 구성원별 역할과 책임의 문서화 부재					
	- 정보보호에 대한 계획, 구현, 승인 및 감독을 담당할 수 있는 정보보호 책임자 미지정					

[그림 5] 취약점 분석·평가 적절성 검토 방법 예시

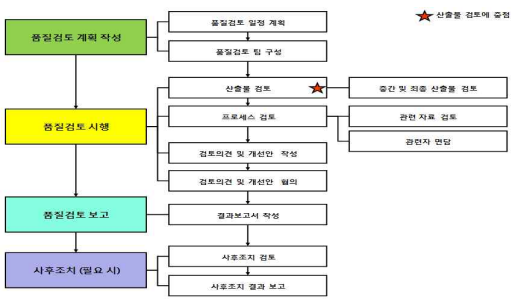
4.2 취약점 분석·평가 적절성 검토 개선 방안

한국정보보호진흥원(현 한국인터넷진흥원)에서는 기존의 보호대책 검토의 일부로 수행된 취약점 분석·평가에 대한 적절성 검토 방법을 개선하고 주요정보통신기반시설 관리기관이 취약점 분석·평가를 적절히 수행하기 위한 절차 및 가이드 등 관련 지침을 제공하기 위해 취약점 분석·평가 에 대한 관리방안을 개발하였다.[6] 취약점 분석·평가 관리방안은 관리기관의 시설

및 정보보호 조직의 규모에 따른 맞춤형 취약성 분석·평가 적절성 검토 프로세스를 적용할 수 있도록 하였다. 개선 점검항목에 대한 관리기관별 적용가능 항목 의견을 수렴하여 총 456개의 항목 중 시설 및 조직의 규모에 따라, 미적용 항목을 제외하고, 기반시설 관리기관을 기반시설 규모, 유형별로 분류하여 적용할 수 있도록 하였다.

취약점 분석·평가 관리 방안은 품질 관리를 위하여 3단계의 업무프로세스와 2단계의 지원프로세스로 구성되며, 각각 태스크와 액티비티가 정의되어 있다. 취약점 분석·평가 프로세스 단계별로 태스크와 액티비티는 프로세스점검항목, 프로세스 세부검토항목과 프로덕트 점검항목, 프로덕트 세부검토항목의 목록으로 구성된다.

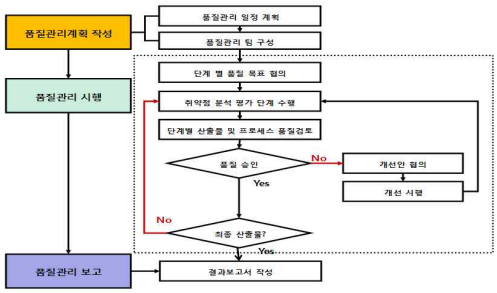
프로세스 점검항목은 업무·지원 프로세스 단계별 태스크와 하부 액티비티에 대한 점검 항목을 보다 구체적으로 설명하는 사항이므로 검토항목 개수만큼 첨부하면 된다. 그림 6은 취약점 분석·평가 품질을 검토하는 절차를 나타낸다.



[그림 6] 취약점 분석·평가 품질 검토 절차

또한, 취약점 분석·평가 품질 검토시 점검 항목은 다음과 같다. 품질 검토 시에는 산출물에 대한 검토를 중점적으로 실시하고, 산출물의 품질이 미흡할 경우 이에 대한 원인을 파악하기 위해 필요한 정도의 프로세스 검토를 수행한다. 취약점 분석·평가 수행 계획서에 나타난 단계와 태스크에 대한 산출물 검토를 수행하고, 필수 항목들을 중점적으로 검토하며, 필요한 경우에 한하여 산출물 품질 점검 항목의 선택 항목 및 프로세스 품질 점검 항목의 필수사항을 선택적으로 적용할 수 있다.

취약점 분석·평가 품질 관리 시 점검 항목은 다음과 같다. 해당 프로세스를 완료 후가 아닌 사전 또는 진행중에 검토함으로써 산출물의 품질을 저하시킬 수 있는 프로세스의 누락, 미흡한 점을 이른 시기에 발견할 수 있다. 또한 취약점 분석·평가 수행 계획서에 나타난 단계와 태스크에 대하여 단계 시작 시 필요한 준비 사항들에 관한 프로세스 품질 점검 항목들을 검토하고, 단계가 끝나는 시점에서 해당 단계의 프로세스 및 산출물 품질 점검 항목들을 검토한다. 모든 검토는 단계 시작 전에 품질관리인 및 외주 컨설팅을 이용할 경우는 발주 기관과 수행 기관의 협의에 따라, 자체 수행할 경우는 취약점 분석·평가 전담반과 함께 각 단계나 태스크에 대하여 검토할 품질 항목들을 선정하고 이를 기준으로 삼아 수행한다. 취약점 분석평가 품질관리 절차는 그림 7과 같다.



[그림 7] 취약점 분석·평가 품질 관리 절차

취약점 분석·평가 세부 점검항목은 다음과 같다. 프로세스 및 산출물의 품질 점검 항목 각각에 대하여 이것이 필수적으로 수행되어야 할 항목인지, 선택적으로 확인할 항목인지를 필수/선택으로 표시한다. 또한 품질 점검 항목을 확인하기 위하여 필요한 방식과 내용을 세부 검토 항목으로 작성한다. 해당 품질 점검 항목은 세부 내용 중 필수로 표시된 항목이 모두 yes 일 경우에만 yes 로 표시된다. 즉, 필수 세부 내용 중 하나라도 no 가 있으면 그 품질 점검 항목은 no 가 된다. 세부 검토 항목은 대체로 해당 사항이 산출물에 존재하는지를 확인하는 것이 주종이나 내용을 확인하거나 특정한 조건을 만족해야 하는 경우도 있게 된다.

취약점 분석·평가 세부 점검항목은 그림 8과 같이 5개 프로세스 456개 항목으로 구성된다.

대분류	항목수
1. 환경 및 요구분석	119
2. 취약성 분석 및 위험평가	139
3. 체계설계 및 계획수립	120
4. 프로젝트 관리	47
5. 교육, 기술이전 및 사후지원	31
합계	456

[그림 8] 취약점 분석·평가 타당성 세부 점검항목

4.1.1 환경 및 요구분석

환경 및 요구분석은 취약점 분석·평가의 첫 단계로서 업무 현황 분석, 보안현황 분석, 보안수준 측정, 요구사항 분석으로 구성된다. 그림 9에 환경 및 요구분석 단계에서의 세부적인 점검항목을 나타내었다.

1. 환경 및 요구분석			119
	1.1 업무 현황 분석		21
		1.1.1 업무분석	7
		1.1.2 산업환경분석	4
		1.1.3 조직분석	4
		1.1.4 정보시스템분석	6
	1.2 보안 현황 분석		62
		1.2.1 관리적 현황 분석	24
		1.2.2 물리적 현황 분석	17
		1.2.3 기술적 현황 분석	21
	1.3 보안수준 측정		19
		1.3.1 설문조사	9
		1.3.2 보안수준 측정	10
	1.4 요구사항 분석		17
		1.4.1 제안요청서 분석	3
		1.4.2 면담 및 자료 분석	3
		1.4.3 보안요구사항 도출	11

[그림 9] 환경 및 요구분석 프로세스 점검항목

4.1.2 취약성 분석 및 위험평가

취약성 분석 및 위험평가는 취약점 분석·평가의 두 번째 단계로 취약성 진단으로부터 위험평가 까지 세부 점검항목으로 구성된다. 그림 10에 취약성 분석 및 위험평가 프로세스의 세부 점검항목을 나타내었다.

2. 취약성 분석 및 위험평가			139
	2.1 취약성 진단		45
		2.1.1 진단대상 선정	7
		2.1.2 취약성 진단 수행	29
		2.1.3 진단결과 분석	9
	2.2 모의해킹		23
		2.2.1 대상 및 범위 선정	6
		2.2.2 시나리오 작성	7
		223 모의해킹수행및결과분석	10
	2.3 위험평가-자산분석		17
		2.3.1 자산조사 및 분류	8
		2.3.2 자산가치 산정	9
	2.4 위험평가-위협분석		16
		2.4.1 위협 조사	11
		2.4.2 위협평가	5
	2.5 위험평가-취약성 분석		15
		2.5.1 취약성 식별	6
		2.5.2 취약성 평가	9
	2.6 위험평가-기존대책분석		9
		2.6.1 기존 보호대책 식별	6
		2.6.2 보호대책 분석	3
	2.7 위험평가		14
		2.7.1 위험도 계산	8
		2.7.2 우선순위 결정	6

[그림 10] 취약성 분석 및 위험평가 프로세스 점검항목

4.1.3 체계설계 및 계획수립

체계설계 및 계획수립은 취약점 분석·평가의 세번째 단계로 정보보호 체계 설계, 정책/지침 및 절차 설계, 솔루션 설계, 마스터플랜 수립으로 구성된다. 주요정보통신기반시설로 지정되고 최초로 취약점 분석·평가를 실시할 경우 중요성이 높은 부분이다. 그림 11에 체계설계 및 계획수립 프로세스의 세부 점검항목을 나타내었다.

3. 체계설계 및 계획수립			120
	3.1 정보보호체계설계		18
		3.1.1 대책 도출	10
		3.1.2 정보보호체계 설계	8
	3.2 정책,지침 및 절차 설계		61
		3.2.1 정책설계	7
		3.2.2 지침설계	29
		3.2.3 절차설계	25
	3.3 솔루션 설계		12
		3.3.1 필수 기능요소 도출	7
		3.3.2 솔루션 선정 지침 정의	4
		3.3.3 보안시스템 구축안 제시	1
	3.4 마스터플랜 수립		29
		3.4.1 이행과제 도출	11
		3.4.2 이행계획 수립	18

[그림 11] 체계설계 및 계획 수립 프로세스 점검항목

4.1.4 프로젝트 관리

프로젝트 관리는 취약점 분석·평가의 네 번째 단계로 프로젝트 착수, 프로젝트 통제, 프로젝트 종료와 같은 세부 점검항목으로 구성된다. 그림 12는 프로젝트 관리 점검항목을 나타낸다.

4. 프로젝트 관리			47
	4.1 프로젝트 착수		16
		4.1.1 프로젝트 수행계획수립	16
	4.2 프로젝트 통제		19
		4.2.1 보고관리	9
		4.2.2 변경관리	10
	4.3 프로젝트 종료		12
		4.3.1 프로젝트 종료	12

[그림 12] 프로젝트 관리 프로세스 점검항목

4.1.5 기술 이전 및 사후 지원

기술 이전 및 사후 지원은 취약점 분석·평가의 마지막 단계로서 교육계획 수립 및 시행, 기술 지원, 사후 지원으로 구성된다. 외부 컨설팅이 아닌 자체 전담반에 의해 취약점 분석·평가를 수행할 경우 제외할 수 있다.

그림 13은 기술 이전 및 사후지원 프로세스 점검항목을 나타낸다.

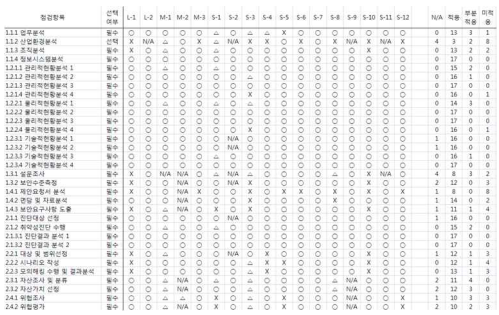
5. 교육, 기술이전 및 사후지원		31
	5.1 교육계획 수립 및 시행	11
	5.2 기술지원	10
	5.3 사후지원	10

[그림 13] 기술 이전 및 사후 지원 프로세스 점검항목

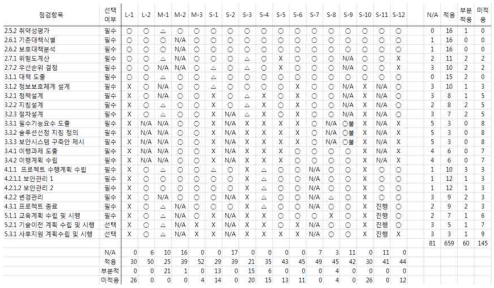
Ⅴ. 시범 적용 결과

5.1 방송·통신 분야 취약점 분석·평가 적절성 검토 시범 적용 결과

2009년 5월부터 8월까지 방송통신위원회 소관 17개 주요정보통신기반시설 관리기관을 대상으로 2010년도 보호대책에 취약점 분석·평가의 적절성 검토를 시범적용하였다. 5개 분야 56개 항목 및 456개 세부항목에 대하여 해당 항목의 관리기관별 적용 여부를 확인하였으며, 주요정보통신기반시설 관리기관 규모별, 유형별로 분석을 할 수 있었다. 규모에 따른 분류는 주요정보통신기반시설 세부시설의 규모를 Large(기반시설 100 이상), Medium(기반시설 100 미만~50 이상), Small(기반시설 50 미만)으로 하였다. 또한 유형별로는 인터넷 접속망, 이동전화, 인터넷전화서비스 등과 같이 기반시설로 지정된 유형별로 분류할 수 있다.



[그림 14] 방·통 분야 취약점 분석·평가 적절성 검토 시범 적용 결과 - 1



[그림 15] 방·통 분야 취약점 분석·평가 적절성 검토 시범 적용 결과 - 2

그림 14와 그림 15는 56개 항목에 대한 주요정보통신기반시설 관리기관별 적용, 부분적용, 미적용, 해당없음(N/A)을 표시한 결과이다.

5.2 환경분석 및 요구분석 시범 적용 결과

환경분석 및 요구분석 부분에서는 대부분의 관리기관이 정보시스템 분석, 관리적/물리적/기술적 현황 분석 부분을 적용하는 것으로 선택하였다. 또한 다수의 관리기관이 산업환경 분석 및 요구사항 분석의 제안요청서 분석을 미적용하는 것으로 선택하였다. 그림 16은 환경분석 및 요구분석 부분에 대한 시범 적용 결과이다.

수행단계	점검항목	선택여부	N/A	적용	부분적용	미적용
1.1 업무현황분석	1.1.1 업무분석	필수	0	13	3	1
	1.1.2 산업환경분석	선택	4	3	2	8
	1.1.3 조직분석	필수	0	13	2	2
	1.1.4 정보시스템분석	필수	0	17	0	0
1.2 보안환경분석	1.2.1 관리적현황분석	필수	0	15	2	0
		필수	0	16	1	0
		필수	0	17	0	0
		필수	0	16	0	1
	1.2.2 물리적현황분석	필수	0	14	3	0
		필수	0	17	0	0
		필수	0	17	0	0
		필수	0	16	0	1
	1.2.3 기술적현황분석	필수	1	16	0	0
		필수	1	16	0	0
		필수	0	16	1	0
		필수	0	17	0	0
1.3 보안수준측정	1.3.1 설문조사	필수	4	9	3	2
	1.3.2 보안수준측정	필수	2	12	0	3
1.4 요구사항분석	1.4.1 제안요청서 분석	필수	1	8	0	8
	1.4.2 면담 및 자료분석	필수	1	14	0	2
	1.4.3 보안요구사항 도출	필수	1	11	1	4

[그림 16] 환경분석 및 요구분석 시범 적용 결과

5.3 취약성 분석 및 위험평가 시범 적용 결과

취약성 분석 및 위험평가 부분에서는 대부분의 관리기관이 취약성 진단, 위험평가-취약성분석을 적용하는 것으로 선택하였다. 일부 미적용으로 선택한 부분은 모의해킹의 대상 및 범위선정, 시나리오 작성 및 위험평가-위협분석 부분이다. 그림 17은 취약성 분석 및 위험평가에 대한 시범 적용 결과를 나타낸다.

수행단계	점검항목	선택여부	N/A	적용	부분적용	미적용
2.1 취약성진단	2.1.1 진단대상 선정	필수	1	16	0	0
	2.1.2 취약성진단 수행	필수	0	15	2	0
	2.1.3 진단결과 분석	필수	0	17	0	0
2.2 모의해킹		필수	0	17	0	0
	2.2.1 대상 및 범위선정	필수	1	12	1	3
	2.2.2 시나리오 작성	필수	0	12	1	4
	2.2.3 모의해킹 수행 및 결과분석	필수	0	13	1	3
2.3 위험평가-자산분석	2.3.1 자산조사 및 분류	필수	2	11	4	0
	2.3.2 자산가치 선정	필수	2	12	3	0
2.4 위험평가-위협분석	2.4.1 위협조사	필수	1	10	3	3
	2.4.2 위협평가	필수	2	10	2	3
2.5 위험평가-취약성분석	2.5.1 취약성식별	필수	0	17	0	0
	2.5.2 취약성평가	필수	0	16	1	0
2.6 위험평가-기존대책분석	2.6.1 기존대책식별	필수	1	16	0	0
	2.6.2 보호대책분석	필수	1	16	0	0
2.7 위험평가	2.7.1 위협도계산	필수	2	11	2	2
	2.7.2 우선순위 결정	필수	3	10	2	2

[그림 17] 취약성 분석 및 위험평가 시범 적용 결과

5.4 체계설계 및 계획수립 시범 적용 결과

체계설계 및 계획수립 부분에서는 대부분의 관리기관이 정보보호 체계 설계를 선택하였다. 반면 다수의 관리기관이 솔루션 설계 및 마스터플랜 수립을 미적용 하는 것으로 선택하였다. 이는 과거에 지정되어 이미 여러 번의 취약점 분석·평가를 실시한 기관의 경우 솔루션이나 마스터플랜 수립은 경우에 따라 필요하지 않음을 알 수 있다. 그림 18에 체계설계 및 계획수립 부분에 대한 시범적용 결과를 나타내었다.

수행단계	점검항목	선택여부	N/A	적용	부분적용	미적용
3.1 정보보호체계 설계	3.1.1 대책 도출	필수	0	15	2	0
	3.1.2 정보보호체계 설계	필수	3	10	1	3
3.2 정책, 지침 및 절차설계	3.2.1 정책설계	필수	3	8	1	5
	3.2.2 지침설계	필수	2	8	2	5
	3.2.3 절차설계	필수	3	7	2	5
3.3 솔루션설계	3.3.1 필수기능요수 도출	필수	5	3	0	8
	3.3.2 솔루션선정 지침 정의	필수	5	3	0	8
	3.3.3 보안시스템 구축안 제시	필수	5	3	0	8
3.4 마스터 플랜 수립	3.4.1 이행과제 도출	필수	4	6	0	7
	3.4.2 이행계획 수립	필수	4	6	0	7

[그림 18] 체계설계 및 계획수립 시범 적용 결과

5.5 프로젝트 관리 시범 적용 결과

프로젝트 관리 부분에서는 다수의 기관이 프로젝트 통제 부분의 보안관리를 적용하는 것으로 선택하였다. 취약점 분석·평가의 특성상 취약점 분석·평가에 투입되는 인력은 해당 기관의 영업 기밀을 취득하게 되므로 보안관리를 중요시 하는 것으로 판단된다. 그림 19는 프로젝트 관리 시범 적용 결과를 나타낸다.

수행단계	점검항목	선택여부	N/A	적용	부분적용	미적용
4.1 프로젝트 착수	4.1.1 프로젝트 수행계획 수립	필수	1	10	3	3
4.2 프로젝트 통계	4.2.1 보안관리	필수	1	12	1	3
		필수	1	12	1	3
	4.2.2 변경관리	필수	3	9	2	3
4.3 프로젝트 종료	4.3.1 프로젝트 종료	필수	2	9	2	3

[그림 19] 프로젝트 관리 시범 적용 결과

5.6 교육, 기술이전 및 사후 지원 시범 적용 결과

교육, 기술이전 및 사후 지원 부분에 대한 시범적용 결과 다수의 관리기관이 사후지원-사후지원 계획수립 및 시행 부분을 미적용하는 것으로 선택하였다.

수행단계	점검항목	선택여부	N/A	적용	부분적용	미적용
5.1 교육계획	5.1.1 교육계획 수립 및 시행	필수	2	7	1	6
5.2 기술이전	5.2.1 기술이전 계획 수립 및 시행	선택	3	5	1	7
5.3 사후지원	5.3.1 사후지원 계획수립 및 시행	선택	3	3	1	9

VI. 결 론

지금까지 전자적 침해행위에 의한 사고가 발생할 경우 국가·사회적으로 많은 영향을 끼치는 주요정보통신기반시설을 보호하기 위하여 지정부터 취약점 분석·평가 및 보호대책 수립 등을 통한 주요정보통신기반시설의 보호활동을 살펴보았다. 취약점 분석·평가는 주요정보통신기반시설을 보유하고 있는 관리기관이 법에서 정한 바에 따라 기관과 시설의 특성을 반영한 방법론을 적용하여 수행할 수 있다.

이때 중요한 점이 자체 전담반에 의한 취약점 분석·평가 수행 또는 외부 컨설팅 기관을 이용한 취약점 분석·평가 여부와 관계없이 취약점 분석·평가가 적절히 이루어졌는지에 대한 품질 관리이다. 이를 위하여 5개 프로세스에 대한 품질 관리 방안을 마련하고 방송·통신 분야의 주요정보통신기반시설 관리기관을 대상으로 향후 취약점 분석·평가시 반영할 것인지 여부를 시범적용을 통해 확인하였다.

방송통신위원회 등과 같이 소관 분야의 주요정보통신기반시설을 관리할 책임이 있는 관계 중앙행정기관은 본고에서 제안하는 방안 등을 활용하여 부처 특성을 반영한 취약점 분석평가 적절성 검토 방안 마련하고, 주요정보통신기반시설 보호계획에 내용 반영할 수 있다. 또한, 주요정보통신기반시설 관리기관은 취약점 분석·평

가 수행시 자체 수행, 외주 용역 등을 구분하여 기관 특성에 맞게 적절성 검토 방안을 마련하고, 그 검토 결과를 바탕으로 향후 취약점 분석·평가에 활용할 수 있을 것이다.

참고문헌

[1] 국회, 정보통신기반보호법, 2009. 5

[2] 박순태, 이완석, 노봉남, "ISP 주요정보통신기반시설 지정 지표", *한국정보보호학회 동계학술대회 논문집*, 19권 2호, pp.277-281, 2009.12

[3] 행정안전부, 한국인터넷진흥원, "정보통신기반보호 가이드", 2009.11

[4] 한국정보보호진흥원, "취약점 분석 평가 모델", 2002.12

[5] Christopher J. Alberts, Sandra G. Behrens, Richard D. Pethia, William R. Wilson, "Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0, CMU/SEI-99-TR-017, 1999. 6 http://www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm

[6] 한국정보보호진흥원, "주요정보통신기반시설 취약점 분석·평가 관리업무 가이드", 2008.10

<著者紹介>

박 순 태 (SoonTai Park)

정회원

1992년 2월 : 단국대학교 전자계산학과 학사

1994년 2월 : 국민대학교 정보과학대학원 정보통신학과 석사

1996년 3월~현재 : 전남대학교 정보보호협동과정 박사과정

1994년 7월~1999년 9월 : 육군 전산장교

2000년 4월~현재 : 한국인터넷진흥원 서비스보호팀

<관심분야> 정보보호, 정보보증, IT 보안성 평가, 정보보호 인력 양성, 정보통신 기반 보호

이 완 석 (Wan S. Yi)

정회원

1991년 5월 : Va. Tech. 전산과학과 학사

2001년 2월 : 동국대학교 정보보호학과 석사

2004년~현재 : 성균관대학교 전자공학과 박사과정

1996년~현재: 한국인터넷진흥원 서비스보호팀 팀장

<관심분야> 정보보증, 정보보호 제품 평가, 정보통신 기반보호, 신규 IT서비스 보호

노 봉 남(Bong-Nam Noh)

정회원

1978년 2월 : 전남대학교 수학교육학과 학사

1982년 2월 : KAIST 대학원 전산학과 석사

1994년 2월 : 전북대학교 대학원 전산과 박사

1983년~현재: 전남대학교 전자컴퓨터정보통신공학부 교수

2000년~시스템보안 연구센터 소장

<관심분야> 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리