정보통신기반보호법 가이드

정보통신기반보호법 가이드

Information & Telecommunication
Infrastructure Protection Act Guide

2004. 12.

정보통신기반보호법 가이드

Information & Telecommunication
Infrastructure Protection Act Guide

2004·12

정보통신부

정보통신부

정보통신기반보호법 가이드

Information & Telecommunication
Infrastructure Protection Act Guide

2004. 12.

정보통신부

목 차

Information & Telecommunication Infrastructure Protection Act Guide

제1장 정보통신기반보호법 소개 ---------- 1
제2장 정보통신기반보호 추진체계 ---------- 5
제3장 주요정보통신기반시설의 지정 ---------- 13
제4장 주요정보통신기반시설 보호계획 수립 ---------- 19
제5장 침해사고의 예방과 대응 ---------- 35
제6장 정보공유 · 분석센터 ---------- 39
제7장 정보보호컨설팅전문업체 ---------- 43
제8장 의무와 벌칙 ---------- 49

[부록 I] 주요정보통신기반시설 지정평가 기준 사례 53
[부록 II] 취약점 분석 · 평가 항목(예시) ---------- 61

제1장 정보통신기반보호법 소개

1. 제정 취지
2. 추진 경과
3. 해외 동향

1. 제정 취지

- 정보화가 진전되면서 통신 · 금융 · 국방 등 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되고 전세계가 인터넷으로 연결됨에 따라
  - 해킹, 컴퓨터바이러스 유포 등 전자적 침해행위가 새로운 위협요소로 대두됨

- 주요 정보통신시설의 교란 · 마비는 사회 기반시설의 기능 마비를 초래하여 막대한 경제적 손실과 사회적 혼란을 야기할 가능성 증대

- 형법 및 정보통신망이용촉진및정보보호에관한법률 등에 해킹, 컴퓨터바이러스 유포행위에 대한 일부 처벌규정이 있으나
  - 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위한 체계적 사전예방 및 사후대응체계를 규정하는 법령이 미비

- 따라서 해킹, 컴퓨터 바이러스 등 전자적 침해행위로부터 주요 사회기반시설을 운영하는 정보통신시스템을 보호하기 위해 범정부적 대응체계를 구축하기 위한 법률 제정이 필요

2. 추진 경과

- 2000. 2 : 국무총리 주재로 열린 「사이버테러방지 관계장관회의」에서 「정보통신기반보호법」제정을 추진키로 함
- 2001. 1 : 정보통신기반보호법 제정 · 공포(법률 제6383호)
- 2001. 7 : 정보통신기반보호법 시행 및 시행령 공포(대통령령 제17308호)
- 2001. 8 : 정보통신기반보호법시행규칙 공포 · 시행(정보통신부령 제115호)
- 2002. 12 : 정보통신기반보호법 일부 개정(법률 제6796호)
- 2003. 6 : 정보통신기반보호법시행령 일부 개정(대통령령 제18006호)
- 2003. 6 : 정보통신기반보호법시행규칙 일부 개정(정보통신부령 제140호)

3. 해외 동향

가. 미 국

- 1996년 국가정보기반보호법(National Information Infrastructure Protection Act of 1996)을 제정
  - 컴퓨터 시스템과 정보의 비밀성, 무결성을 보호하기 위해 미국에 해가 되거나 외국에 이익을 주는 정보를 부정으로 획득하는 자와 국가 컴퓨터시스템의 운용에 위해를 가하는 자 등을 처벌

- 1998년 5월 주요기반시설에 대한 범정부적 보호체계를 구축하고자 대통령명령 제63호(PDD63, Presidential Decision Directive)를 발령

- 2001년 9월 20일, 부시 대통령이 의회 연설에서 국토안보사무국(the Office of Homeland Security)의 창설을 발표하고, 톰 리지(Tom Ridge)를 국토안보 사무국 국장으로 임명

- 2002년 1월 23일, 국토안보법(Homeland Security Act of 2002) 법률안이 미국 의회에 제출

- 2002년 5월 12일, 부시 대통령이 국토안보 대통령명령 제3호(Homeland Security Presidential Directive - 3)로 국토안보자문체계(Homeland Security Advisory System)를 마련

- 2002년 5월 19일, 부시 대통령이 대통령 직속 국토안보자문협의회(President's Homeland Security Advisory Council)의 창설을 담은 행정명령(Executive Order)을 발표

- 2002년 7월, 국토안보를 위한 국가전략(National Strategy for Homeland Security)을 발표하였고, 2002년 11월 12일 국토안보법(Homeland Security Act)이 미국 의회에서 통과됨

- 2003년 1월 24일, 행정명령 제13284호(Executive Order – 13284)가 발령되면서 국토안보부(DHS, Department of Homeland Security)가 청설하고, 2003년 2월 14일, 사이버스페이스 보안 국가전략(National Strategy to Secure Cyberspace)을 발표.

- 2003년 3월 1일 ~ 2003년 9월 30일, PICPB, CIAO, NIPC 등을 국토안보부로 이관하였고, 2003년 6월에는 국토안보부내에 NCSD(National Cyber Security Division)를 신설함. NCSD는 기존의 NIPC, CIAO, FedCIRC, NCS의 기능 및 역할을 흡수, 통합하였음.

- 2003년 9월 15일, US-CERT 설립

- 2003년 12월 17일, 국토안보 대통령령-7(Homeland Security Presidential Directive-7) 발표

나. 일 본

- 부정액세스행위금지 등에 관한 법률을 제정하여 2000년 2월부터 시행

- 정부 차원에서 사이버공격으로부터 정보통신기반을 보호하기 위한 각종 대책을 추진
  - 「정보통신기술전략본부」내에 전체 성청의 국장급 회의인 「정보보안대책추진회의」와 「민간전문가회합」을 설치 운영
  - 내각에는 정보보호 대책의 종합적인 추진을 위한 정보보안대책추진실과 각 성청의 보안대책에 관한 기술적인 조사, 조언 등을 행하는 전문조사팀을 설치 · 운영

- 「정보보안대책추진회의」에서 수립한「해커 대책 등의 기반정비에 관한 행동계획」(2000. 1)에 근거하여 주요정보통신기반시설을 사이버테러로부터 보호하기 위한 특별행동계획을 2000년 12월에 수립, 시행
  - 동 특별행동계획에 근거하여 사이버테러 대책과 관련되는 민관 연락 · 제휴 체제의 구축을 추진(2001. 10)

제2장 정보통신기반보호 추진체계

1. 개 요
2. 정보통신기반보호위원회의 구성 · 역할
3. 관계기관 및 관리기관의 역할

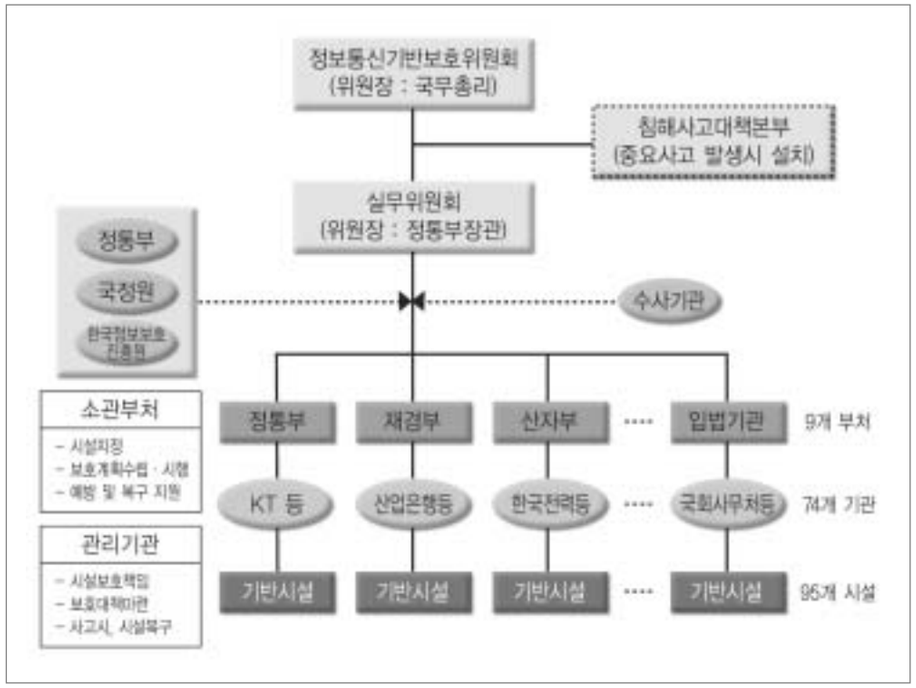
1. 개 요

- 전자적 침해행위는 기본적으로 컴퓨터와 정보통신망을 이용한 기술적인 문제일 뿐만 아니라, 다른 한편으로 타인의 생명과 재산을 침해하는 범죄행위로 더 나아가 국가안보에 대한 침해행위일 수 있음

- 따라서 전자적 침해행위에 대한 대응체계를 마련하는 데 있어 각 부처 · 기관의 대응업무가 상호 협력 및 보완될 수 있도록 하여야 할 것임

- 이에 따라 정보통신기반보호법에서는 안정적인 주요정보통신기반시설의 관리 · 운영을 위해 관계부처간 상호 긴밀하게 협력하는 방향으로 추진체계를 정비

주요정보통신기반시설보호 추진체계



2. 정보통신기반보호위원회의 구성 · 역할

가. 개 요

- 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위한 체계적이고 종합적인 범정부적 대응체계를 구축하기 위하여 국무총리 소속하에 정보통신기반보호위원회 설치
  - 위원회의 효율적인 운영을 위하여 실무위원회를 둠
  - 주요정보통신기반시설에 대한 침해사고가 광범위하게 발생한 경우 한시적으로 정보통신기반침해사고대책본부를 설치 · 운영

나. 정보통신기반보호위원회

- 주요사회기반시설의 운영 · 제어와 관련된 정보통신기반시설의 보호는 다수 부처와 관련되어 있으므로, 국가 차원에서의 효율적인 정보보호를 위하여 관계부처의 정보통신기반보호정책의 수립 · 시행을 총괄 · 조정하는 국무총리 소속의 위원회를 운영하여 이를 종합 · 조정하도록 함

- 구 성
  - 위원장 : 국무총리
  - 위　원 : 재정경제부장관 · 외교통상부장관 · 법무부장관 · 국방부장관 · 행정자치부장관 · 과학기술부장관 · 산업자원부장관 · 정보통신부장관 · 보건복지부장관 · 건설교통부장관 · 해양수산부장관 · 기획예산처장관 · 국가정보원장 · 금융감독위원회 위원장, 비상기획위원회 위원장
  - 간　사 : 국무조정실장

- 운 영
  - 위원장은 회의를 소집하고 회의를 소집하고자 하는 때에는 회의 일시, 장소 및 부의사항을 회의개최 7일전까지 각 위원에게 서면으로 통지. 다만, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니함

- 회의는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결
- 위원장은 법 제4조의 규정에 의한 사항의 심의를 위하여 필요하다고 인정되는 경우에는 관련 전문가 또는 전문기관의 장으로 하여금 그에 관한 검토보고를 하게 할 수 있음
- 위원회의 효율적인 운영을 위하여 위원회에 실무위원회를 둠

● 심의 사항
- 주요정보통신기반시설 보호계획의 종합 · 조정에 관한 사항
- 주요정보통신기반시설 보호정책의 조정에 관한 사항
- 주요정보통신기반시설의 지정 및 지정 취소 심의에 관한 사항
- 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항
- 주요정보통신기반시설 보호와 관련된 주요정책 사항으로 위원장이 부의하는 사항

다. 정보통신기반보호 실무위원회

● 구 성
- 위원장 : 정보통신부 장관
- 위　원 :
  - 위원회의 위원이 속하는 중앙행정기관의 차관급 공무원
  - 국무조정실 경제조정관, 비상기획위원회 사무처장
- 간　사 : 정보통신부 · 국가정보원의 정보통신기반보호업무를 관장하는 1급 또는 1급 상당 공무원

● 운 영
- 위원장이 필요하다고 인정할 때에 회의를 소집하며, 회의는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결
- 정보통신기반보호위원회에 제출된 안건과 정보통신기반보호위원회로부터 위임되거나, 정보통신기반보호위원회의 위원장으로부터 지시받은 사항을 검토 · 심의

라. 침해사고대책본부

● 개 요
- 주요정보통신기반시설에 대한 중대한 침해사고가 발생한 경우 피해확산 방지, 침해자의 검거, 복구조치 등에 신속히 대응하기 위하여 정보통신기반침해사고대책본부 구성 · 운영
- 주요정보통신기반시설에 대한 침해사고는 재난과 같이 수시로 발생하는 것이 아니며, 평시에는 관련기관에서 1차적으로 대응하고 있으므로 중대한 침해사고가 광범위하게 발생한 경우에 한해 한시적으로 운영

● 구 성
- 본부장 : 정보통신기반보호위원회의 위원장이 침해사고가 발생한 정보통신기반시설을 관할하는 중앙행정기관의 장과 협의하여 임명
- 차　장 : 정보통신기반시설 보호와 직접 관련이 있는 중앙행정기관 소속 공무원중에서 대책본부장이 임명(2인)
- 본부원 : 정보통신기반시설 보호와 직접 관련이 있는 관계중앙행정기관 소속 공무원중에서 대책본부장이 지명하는 자 및 법 제15조제2항의 규정에 의하여 파견된 자

● 운 영
- 대책본부장은 대책본부를 대표하고, 그 업무를 총괄
- 대책본부장은 침해사고 피해의 효율적인 수습을 위하여 필요하다고 인정할 때에는 본부 구성원이 참여하는 회의를 소집
- 피해시설에 대한 복구조치, 피해확산 방지에 필요한 조치, 피해액 산정의 기준, 유사한 침해사고의 방지를 위한 예방대책에 관한 사항은 대책본부 회의를 거쳐서 시행

3. 관계기관 및 관리기관의 역할

가. 관계중앙행정기관의 역할

- 주요정보통신기반시설을 관리하는 관계중앙행정기관의 장은 소관분야별 주요정보통신기반시설을 지정하고 보호계획을 수립 · 시행하며, 보호지침을 제정하여 주요정보통신기반시설 관리기관에게 권고하거나 보호에 필요한 조치를 명령 · 권고함
  ※ 관계중앙행정기관은 소관분야 주요정보통신기반시설 보호업무를 담당하는 과장급 공무원을 정보보호책임관으로 지정

나. 정보통신부의 역할

- 정보통신부는 실무위원회 위원장 및 사안에 따라 국가정보원과 공동으로 간사업무를 수행

- 관계행정기관의 장과 협의하여 취약점 분석 · 평가에 관한 기준 및 보호계획 작성지침을 정하고, 이를 관계중앙행정기관의 장에게 통보

- 해당 주요정보통신기반시설 관리기관의 장이 보호조치를 시행함에 있어서 필요한 기술지원

- 정보보호컨설팅전문업체 지정 · 관리 및 정보통신기반시설 보호를 위한 기술개발 등

다. 국가보안 업무를 수행하는 기관의 역할

- 국가기관 및 지방자치단체의 장인 관리기관이 필요하다고 인정하여 요청하거나, 위원회의 위원장이 특정 국가기관 또는 지방자치단체의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명 받은 해당 관리기관에 대한 기술적 지원 업무를 수행
  - 주요정보통신기반시설보호대책의 수립 및 침해사고 예방 및 복구를 위한 기술적 지원

- 도로 · 지하철 · 공항 시설 등 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대하여는 국가보안업무를 수행하는 기관(국가정보원)이 우선적으로 기술지원
  - 특히 국가안전보장에 현저하고 급박한 위험이 있고 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 관계중앙행정기관의 장과 협의하여 신속한 지원 가능

- 다만, 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니됨

라. 주요정보통신기반시설 관리기관의 역할

- 주요정보통신기반시설을 관리하는 기관은 일차적인 보호책임을 지며, 이를 위해 소관시설에 대한 취약점을 분석 · 평가하고 보호대책을 강구
  - 취약점 분석 · 평가의 결과에 따라 매년 3월말까지 소관 주요정보통신기반시설을 안전하게 보호하기 위하여, 필요한 관리적, 물리적, 기술적 대책을 포함한 보호대책을 수립하여 관할 중앙행정기관의 장에게 제출

- 소관 주요정보통신기반시설이 교란 · 마비 또는 파괴된 사실을 인지할 때에는 관계 행정기관, 수사기관, 한국정보보호진흥원 등 관계기관에 통지하고, 해당 정보통신기반시설의 복구 및 보호에 필요한 조치 시행
  ※ 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 4급 · 4급 상당 공무원, 5급 · 5급 상당 공무원, 영관급 장교 또는 임원급 관리 · 운영자를 정보보호책임자로 지정

제3장 주요정보통신기반시설의 지정

1. 지정 대상
2. 지정 주체
3. 지정 기준
4. 지정 절차
5. 지정평가 기준 및 방법(예시)
6. 지정 취소

1. 지정 대상

● 주요정보통신기반시설의 지정 대상은 국가 · 공공기관 뿐 아니라 민간이 운영 · 관리하는 정보통신기반시설을 포함하며, 전자적 침해행위 발생시 국가안보, 국민의 기본생활 및 경제안정에 중대한 영향을 미치게 되는 주요 사회기반시설과 관련된 제어 · 운영시스템과 정보통신망을 말함

〈예시〉
- 도로, 지하철, 공항 시설
- 전력, 가스, 석유 등 에너지 · 수자원 시설
- 방송 중계, 국가지도통신망 시설
- 원자력, 국방과학, 첨단방위산업관련 정부출연연구기관의 연구시설 등

2. 지정 주체

● 중앙행정기관이 정보통신기반보호위원회의 심의를 거쳐 지정 고시하며, 지방자치단체의 장이 관리 감독하는 시설은 행정자치부장관이 지정

※ 중앙행정기관의 장은 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있음

3. 지정 기준

지정기준은 정보통신기반보호법 제8조 제1항의 규정에 의거하여 아래와 같은 5가지 기준에 의해 평가

● 관리기관이 수행하는 업무의 국가사회적 중요성
● 관리기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
● 다른 정보통신기반시설과의 상호 연계성
● 침해사고 발생시 국가안전보장과 경제사회에 미치는 피해규모 및 범위
● 침해사고의 발생가능성 및 복구의 용이성

4. 지정 절차

〈 주요정보통신기반시설 지정절차 〉

● 1단계 : 각 중앙행정기관의 ‘지정평가기준’ 마련
● 2단계 : 시설 관리기관의 ‘지정단위 선정’ 및 ‘지정여부 평가’
● 3단계 : 각 중앙행정기관의 ‘지정평가 결과 심사’
● 4단계 : 정보통신기반보호위원회 ‘지정여부 심의’
● 5단계 : 각 중앙행정기관의 ‘지정시설 고시’

가. 1단계 : 중앙행정기관장의 지정평가기준 마련

● 중앙행정기관 장은 주요정보통신기반시설 지정여부 평가기준(지정평가기준)과 지정방침을 마련하여 소관분야 지정대상시설 관리기관의 장에게 시달

나. 2단계 : 시설 관리기관의 지정단위 선정 및 지정여부 평가

● 지정대상시설 관리기관의 장은 지정단위를 선정하고, 관련된 세부시설의 범위를 선정

● 또한, 시설관리기관의 장은 중앙행정기관의 장이 통보한 지정평가기준을 근거로 주요정보통신기반시설 지정 여부를 평가하여, 그 결과를 중앙행정기관의 장에게 통지

다. 3단계 : 중앙행정기관의 지정평가 결과 심사

● 중앙행정기관의 장은 지정대상시설 관리기관의 장이 통지해 온 평가결과에 대해 그 적정성 여부를 분석 · 검토한 후
  – 소관분야의 정보통신기반시설중 전자적 침해행위로부터 보호할 필요성이 있다고 인정되는 시설을 정보통신기반보호위원회에 주요정보통신기반시설 지정 심의(안)으로 상정

- 지방자치단체의 장이 관리 · 감독하는 시설은 행정자치부장관이 지방자치단체의 장과 협의하여 심사

※ 중앙행정기관의 장은 지정대상시설 관리기관의 장이 해당 시설에 대한 평가를 부실하게 하였거나 상당한 이유 없이 누락하였다고 판단되는 경우 이를 다시 평가하도록 지시하거나 권고할 수 있음

라. 4단계 : 정보통신기반보호위원회 심의

● 기반보호위원회는 중앙행정기관의 장이 제출한 시설지정(안)을 심의 · 의결
- 중앙행정기관의 장은 정보통신기반보호실무위원회 및 위원회에 지정 심의안을 상정하여 심의를 받음.
- 심의에 있어 위원들이 판단하기 곤란한 사항이 있거나, 시설의 기능 등에 대해 궁금한 점이 있을 때에는 지정대상시설 관리기관의 장을 위원회에 출석시켜 의견을 청취할 수 있음

마. 5단계 : 중앙행정기관의 주요정보통신기반시설 지정고시

● 중앙행정기관의 장은 위원회의 심의 결과에 따라 소관분야 주요정보통신기반시설을 지정할 경우에는 지체 없이 해당 관리기관의 장에게 그 사실을 통보하고 이를 즉시 관보에 고시

※ 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있음.

5. 지정평가 기준 및 방법(예시)

가. 지정평가 기준(예시)

● 주요정보통신기반시설로 지정할 필요성이 있는지를 평가하는 방법으로, 정보통신기반보호법에서 제시한 지정기준(제8조)에 근거한 주요정보통신기반시설 지정평가 기준 사례 [부록 I]을 사용

- 지정평가기준표는 각 중앙행정기관의 장이 마련하여 지정대상시설관리기관의 장에게 통보할 수 있으며, 여기서는 정성적 방법의 지정기준표를 하나의 예로서 제시

※ 미국의 주요기반보호국(CIAO: Critical Infrastructure Assurance Office)의 지침인 "Practice for Securing Critical Information Assets"의 주요자산식별법을 참고하여 마련

- 지정의 현실성과 객관성을 위해 지정대상시설관리기관의 장과 해당 업무를 수행하는 담당자들이 1차적으로 직접 해당 시설의 중요성을 평가

나. 지정평가 방법(예시)

● 5개 항목별 반영비율은 중앙행정기관의 장이 소관분야의 특수한 사정들을 고려하여 관리기관 장과 협의하여 조정 가능

※ 예) 국방부의 경우, 5개 항목별로 20%씩 동일하게 반영하는 것이 아니라 국가 사회적 중요성을 중시하여 항목별 가중치를 반영할 수 있음

● 중앙행정기관은 해당 분야의 특수성을 반영하여 항목별 질문 문항의 내용을 추가 또는 제외하거나, 질문 항목별 가중치도 달리 부여할 수 있으며,

● 지정 필요성 여부를 결정하는 기준 또한 중앙행정기관의 장이 결정할 수 있음

※ 예) 일정점수 이상, 총점대비 몇% 이상, 최고점수 몇 개 이상

6. 지정 취소

● 중앙행정기관의 장은 관리기관이 해당업무를 폐지 · 정지 또는 변경하는 경우에는 주요정보통신기반시설의 지정을 취소할 수 있음

제4장 주요정보통신기반시설보호계획 수립

1. 주요정보통신기반시설 보호계획의 수립절차 및 주요내용
2. 취약점 분석 및 평가

1. 주요정보통신기반시설 보호계획의 수립절차 및 주요내용

가. 보호계획 수립 절차

● 주요정보통신기반시설 지정
- 관계중앙행정기관의 장은 정보통신기반보호위원회의 심의를 거쳐 소관분야의 주요정보통신기반시설을 지정

※ 주요정보통신기반시설 현황(2004. 11.) : KT 인터넷접속망 등 95개 시설
주요정보통신기반시설 관련 소관부처 : 정보통신부, 재경부 등 9개부처

● 관계중앙행정기관의 보호지침 제정 · 운영
- 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설 보호지침을 제정하여 해당시설 관리기관의 장에게 이를 지키도록 권고

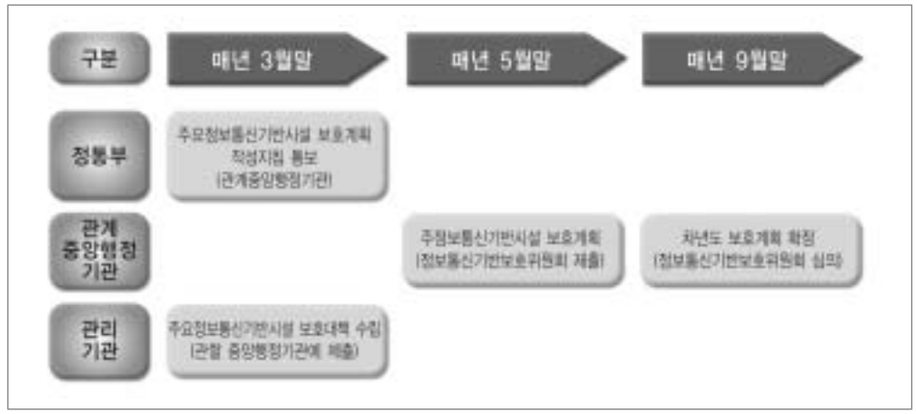
● 관리기관의 장은 소관시설에 대한 취약점 분석 · 평가 실시

● 관리기관의 보호대책 수립
- 주요정보통신기반시설 관리기관의 장은 취약점 분석 · 평가 결과를 반영하여 매년 3월말까지 소관 주요정보통신기반시설에 대한 보호대책을 수립하여 관계중앙행정기관에 제출

● 관계중앙행정기관의 보호계획(안) 수립
- 관계중앙행정기관의 장은 소관분야의 관리기관별 보호대책을 종합 · 조정한 후 매년 5월말까지 보호계획을 수립하여 정보통신기반보호위원회(실무위원회 경유)에 제출

● 위원회의 보호계획(안) 심의 · 확정
- 정보통신기반보호실무위원회 및 동 위원회는 9월말까지 보호계획(안)을 심의 · 확정

주요정보통신기반시설 보호대책/보호계획 수립 일정



나. 보호계획의 주요내용

● 주요정보통신기반시설 보호계획은 다음 사항을 주된 내용으로 하여 체계적으로 구성
- 소관분야 주요정보통신기반시설 보호대책의 기본방향 및 추진목표
- 전년도 주요정보통신기반시설 보호대책과 관련한 전체 추진실적 및 종합평가
- 보호조직 및 보호체계의 구축 · 운영에 관한 계획
- 침해사고로부터의 예방에 관한 계획
- 침해사고에 대한 대응 및 복구에 관한 계획
- 주요정보통신기반시설에 대한 차년도 계획

다. 보호계획의 수립시 주요 고려사항

1) 관계법령 및 보호지침의 준수

● 정보통신기반보호법 및 동법시행령 · 시행규칙과 소관분야별 보호지침에서 주요정보통신기반시설 보호를 위해 규정하고 있는 사항을 고려하여 누락되는 부분이 없도록 보호계획을 작성

2) 소관분야 각 관리기관의 보호대책을 상호연계

● 각 부처는 소관분야의 관리기관이 보호대책 수립 시에 필수적으로 고려해야 할 사항 등을 정하여 관리기관에 매년 2월말까지 통보

● 각 부처는 소관분야의 관리기관별 보호대책이 상호연계 되도록 종합 · 조정하여 보호계획을 작성
- 소관분야 각 주요정보통신기반시설별 보호대책간에 상호 중복되거나 기관별 협력으로 효율적 운영이 가능한 분야는 통합 · 조정하여 보호계획을 작성

● 각 부처는 보호계획의 실효성 확보를 위한 추진방안을 제시하고, 관리기관의 보호대책을 효과적으로 관리할 수 있도록 작성

3) 주요정보통신기반시설 보호관련 중점추진사항 반영

● 소관분야 주요정보통신기반시설의 보호를 위해 각 중앙행정기관에서 중점적으로 추진하고자 하는 사항을 중심으로 구체적으로 작성

● 특히, 주요정보통신기반시설에 대한 물리적 보호를 강화하기 위해 전 기관은 물리적 보호강화 방안 마련
- 물리적 보호 강화방안
  - 출입통제 강화
  - 소방시설 등 방호, 방제 대책 강화
  - 백업시스템 구축 및 데이터 백업 강화
  - 시스템 · 네트워크 장비 및 회선 이중화

4) 기타 준수사항

● 보호계획 작성시 작성 전담반을 구성하여 작업을 진행

● 부정확한 용어 사용을 지양하고 일반적이고 의미가 명확한 용어를 사용하되, 주요정보통신기반보호법령 및 관계법령에서 규정하는 용어를 사용하였을 경우에 그 의미는 해당 법령에서 규정하는 의미로 사용
※ 예시 : “주요정보통신기반시설”, “주요정보통신기반시설 보호대책”, “전자적 침해(행위, 사고)”, “정보통신망”, “제어 · 관리시스템” 등

● 제시된 목차 및 필요한 양식은 작성지침에서 제시된 것을 사용하되, 본 지침 외에 업무의 특성상 가감이 필요할 경우에는 수정 · 보완하여 작성

2. 취약점 분석 및 평가

가. 취약점 분석 · 평가의 필요성

● 주요정보통신기반시설의 안정적 운영과 동 시설에 내장된 중요 정보의 기밀성 · 무결성에 영향을 미칠 수 있는 전자적 침해행위 등 다양한 위협요인을 파악하고, 이들 위협요인에 대한 주요정보통신기반시설의 취약점 · 침해시 파급효과(피해규모 및 정도) 및 대책을 식별 · 분석 · 평가함으로써

● 주요정보통신기반시설에 대한 경제적(효과/비용)이고 실효성 있는 보호대책을 수립(법 제5조 제1항)하는데 필요한 정보를 제공하며, 동 대책에 기초한 효과적인 분야별 주요정보통신기반시설보호계획 수립의 근거를 제공

나. 취약점 분석 · 평가 근거

● 정보통신기반보호법 제8조에 의하여 지정된 주요정보통신기반시설 관리기관의 장은 동법 제9조와 동법시행령 제17조 내지 제19조에 따라 소관시설에 대한 취약점을 분석 · 평가하여야 함

● 정보통신부장관은 정보통신기반보호법 제9조에 따라 취약점 분석 · 평가 기준을 마련하여 관계중앙행정기관의 장에게 통보하여야 함

다. 취약점 분석 · 평가의 주체

● 취약점 분석 · 평가의 주체는 주요정보통신기반시설 관리기관(이하 '관리 기관')임.
- 관리기관이 직접 취약점 분석 · 평가를 하는 경우에는, '취약점 분석 · 평가 전담반'을 구성하여 소관 시설에 대한 취약점 분석 · 평가를 실시하여야 함(법 제9조)

※ 관리기관은 소관 주요정보통신기반시설의 특성에 따라 취약점 분석 · 평가를 수행할 수 있는 적정 인원의 전문인력을 확보해야 함

● 관리기관은 소관시설의 취약점 분석 · 평가 시 객관성 및 실효성 확보나, 취약점 분석 · 평가 전담반의 전문성을 보강하기 위해 필요한 경우 다음 기관에게 소관 시설의 취약점 분석 · 평가를 의뢰하거나 그 지원을 요청할 수 있음
- 한국정보보호진흥원
- 대통령령이 정하는 기준을 충족하는 정보공유 · 분석센터
- 법 제17조의 규정에 의하여 지정된 정보보호컨설팅전문업체
- 한국전자통신연구원

● 취약점 분석 · 평가를 외부 전문기관이 수행하는 경우에는 '취약점 분석 · 평가 전담반'을 구성하지 아니할 수 있음(법 제9조 제3항)

라. 취약점 분석 · 평가 주기 및 시기

● 관리기관은 2년마다 1번씩 정기적으로 소관시설에 대하여 정밀한 취약점 분석 · 평가를 수행하고, 이에 따라 적절한 보호대책 수립 · 시행

※ '정밀한 취약점 분석 · 평가'란 장기간에 걸쳐 정밀분석을 시행하여 보호수준을 점검하는 것을 말함

● 정밀한 취약점 분석 · 평가를 수행하지 않는 연도에는 소관시설에 대하여 간이 취약점 분석 · 평가를 실시하여, 보호대책 수립 · 시행

※ '간이 취약점 분석 · 평가'란 단기간에 기본적인 점검항목에 따라 보호수준을 점검하는 것을 말함

● 주요정보통신기반시설에 중요한 변화가 발생하거나 중대한 사고가 발생한 경우에는 정기적인 취약점 분석 · 평가와 별도로 관리기관의 장의 판단 하에 수시로 취약점 분석 · 평가를 시행할 수 있음

※ 주요정보통신기반시설의 중요한 변화에는 구성 장비의 추가 · 변경, 운영소프트웨어의 추가 · 변경, 네트워크 구성 변경, 관리조직 및 절차의 변경 등을 포함

● 주요정보통신기반시설로 새로이 지정된 경우에는 지정 후 6개월 이내에 취약점 분석 · 평가 시행
- 다만, 주요정보통신기반시설로 지정 후 취약점 분석 · 평가를 6개월 이내에 시행하지 못할 특별한 사유가 있는 경우에는 관할 중앙행정기관장의 승인을 받아 지정 후 9개월 이내에 시행

※ 주요정보통신기반시설로 지정되기 전 1년 이내에 지정 시설에 대하여 정밀한 취약점 분석 · 평가를 수행한 경우, 관리기관의 장은 관할 중앙행정기관장의 승인을 받아 기 실시한 취약점 분석평가를 토대로 간이 취약점 분석 · 평가를 실시하여 보호대책 수립 가능

※ 주요정보통신기반시설로 지정되기 전에 지정 시설에 대한 정밀한 취약점 분석 · 평가를 시작하여 시설 지정 후에 끝마친 경우에는 이를 토대로 보호대책 수립 가능

마. 취약점 분석 · 평가의 절차

1) 1단계 : 취약점 분석 · 평가 계획 수립

가) 관리기관 자체수행인 경우, 전담반 구성하여 수행(법 제9조 제2항)

● 관리기관은 취약점 분석 · 평가의 실효성과 전문성을 확보하기 위하여 계획 수립, 취약점 분석 · 평가 및 보호대책 수립에 이르는 전 과정을 전담하여 수행할 전담반을 구성
- 전담반은 다음의 구성 예를 참조하여 주요정보통신기반시설 관리 · 운영자, 업무담당자 및 분야별 정보보호 전문가들로 구성하고, 전담반 반장은 관리기관의 정보보호책임자(법 제5조 제4항)로 함

※ 관리기관은 소관 주요정보통신기반시설의 구성장비, 업무특징 등을 고려하여 분야별로 취약점 분석 · 평가를 효과적으로 수행할 수 있는 적정 인원의 전문인력을 확보해야 함

● 전담반은 취약점 분석 · 평가기준에 따라 소관 주요정보통신기반시설의 취약점 분석 · 평가 수행 범위, 점검항목, 절차, 산출물, 수행기간, 인원, 소 요예산 등을 포함한 취약점 분석 · 평가계획을 수립 · 시행

□ 취약점 분석 · 평가 전담반 구성 예

구 성 원	역할 또는 자격기준
반장 (정보보호책임자)	주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자 (취약점 분석 · 평가를 총괄하는 역할 수행)
기반시설 관리 · 운영자	기반시설을 구성하는 장비, 소프트웨어, 네트워크, 보안시스템 등에 대한 관리 · 운영 업무를 담당하는 자
기반시설 업무담당자	기반시설을 이용한 업무를 담당하고 있거나 기반시설의 비즈니스 프로세스를 이해하고 있는 자(정보의 가치 산정이 가능한 자) 예) 은행의 인터넷 뱅킹업무 담당자
네트워크 보안전문가	해당기관의 주요정보통신기반시설에서 운영되고 있는 네트워크 장비, 통신 프로토콜, 네트워크 구성 및 설정 등에 전문성을 가진 자
서버/메인프레임 보안전문가	해당기관의 주요정보통신기반시설에서 운영되고 있는 서버 및 메인프레임의 운영체제, 인증 및 접근통제, 암호화, 보안취약점, 취약점점검, 보안대책 등에 전문성을 가진 자
응용프로그램 보안전문가	해당기관의 주요정보통신기반시설에서 운영되고 있는 응용프로그램의 보안기능, 보안취약점, 보안대책 등에 전문성을 가진 자
보안관리 전문가	취약점 분석 · 평가 방법, 정보보호정책 및 관리체계 수립 등에 전문성을 가진 자

※ 취약점 분석 · 평가 실효성을 확보하거나 자체 전담반의 전문성을 보강하기 위해 필요한 경우, 한국정보보호진흥원 기반시설보호단(전화 02-405-5250), 국가보안연구소 취약성분석센터(전화 042-864-5015), 정보보호컨설팅전문업체 또는 정보공유 · 분석센터 등에 취약점 분석 · 평가를 의뢰하거나 지원을 요청할 수 있음

나) 외부 전문기관에 위탁 수행하는 경우(법 제9조 제3항)

● 법 제9조 제3항에 의하여 관리기관이 취약점 분석 · 평가를 외부전문기관에 위탁시 자체 전담반을 구성하지 않을 수 있음
  - 다만, 관리기관은 전문기관의 취약점 분석 · 평가 수행과 관리기관의 보호대책 운영이 업무 연속성을 확보할 수 있는 방안을 강구해야 함

● 자체 수행의 경우와 마찬가지로 취약점 분석 · 평가 계획 수립 · 시행

2) 2단계 : 취약점 분석 · 평가 대상 선별

● 취약점 분석 · 평가 대상 주요정보통신기반시설의 구성 및 업무내용을 확인하고, 취약점 분석 · 평가 및 보호대책 수립이 필요한 세부자산을 선별하여 그 목록 및 구성도 작성
  - 주요정보통신기반시설을 직접적으로 구성하는 세부장비, 소프트웨어, 데이터, 문서, 설비 등은 물론 해당시설을 운영 또는 지원하기 위한 장비들도 가급적 포함하여 대상 선별

※ [부록 II] 1. 주요정보통신기반시설 세부자산 분류기준(예시) 참조

● 해당자산에 손상, 노출, 변조 등의 피해 발생시 업무 수행에 미치는 영향 등을 고려하여 자산별 중요도 부여
  - 중요도가 높게 부여된 자산에 대해서는 위협요인 및 취약점 분석, 취약점 평가 단계에서 중점적으로 분석 · 평가하고 보호대책 수립

※ [부록 II] 2. 주요정보통신기반시설 자산 중요도 부여기준(예시) 참조

3) 3단계 : 위협요인 및 취약점 분석

가) 위협요인 분석

● 주요정보통신기반시설에 실제 문제가 발생하였거나 또는 발생할 수 있는 위협요인 식별

※ 위협요인이란 화재, 사용자 오류, 웜·바이러스 등과 같이 기반시설에 손실을 끼칠 수 있는 원인이나 행위를 말함

- 위협의 행위자(내·외부인), 접근경로(네트워크 또는 물리적 접근) 등의 요소를 종합적으로 고려하여 실제 발생 가능한 위협요인 식별
- 전산실 장애관리일지, IT 조직의 사고대응일지 등을 통하여 이미 발생했던 위협요인 식별

※ [부록 II] 3. 위협요인 식별 및 수준측정(예시) 참조

● 식별한 각 위협요인별 발생 원인·빈도와 침해시 영향 등을 고려하여 수준측정기준을 설정하고 위협의 수준 측정
- 식별한 위협요인에 대하여, 위협 발생시 업무에 미치는 영향과 발생주기 등을 고려하여 위협측정기준을 설정하고, 위협의 수준 측정
- 업무환경의 변화에 따라 새롭게 발견되거나 중요성이 부각된 위협에 대해서는 위협의 수준을 높게 측정

나) 취약점 분석

● 소관시설의 특수성을 고려하여 취약점 점검항목을 마련하고, 소관시설에 존재하는 기술적·관리적·물리적 취약점 식별
- 시스템/네트워크 취약점 점검도구를 이용한 자동점검, 체크리스트를 이용한 수동점검, 로그분석, 모의해킹 등을 통해 기술적 취약점에 대해 점검

※ [부록 II] 4. 기술적 취약점 점검 항목(예시) 참조

- 정보보호정책, 표준, 지침, 절차 등 관련자료의 검토 및 담당자 면담 등을 통한 이행여부 확인으로, 관리적 취약점에 대해 점검

※ [부록 II] 5. 관리적 취약점 점검 항목(예시) 참조

- 소관 정보통신기반시설의 보호구역, 전산실 등의 출입통제, 경보체제 등 물리적 취약점 점검

※ [부록 II] 6. 물리적 취약점 점검 항목(예시) 참조

● 취약점 항목별 점검결과를 토대로, 자산의 취약점이 침해당했을 때 관련업무에 미치는 영향을 고려하여 취약점 평가기준을 설정하고 기술적·관리적·물리적 취약점에 대해 취약점 수준 측정

※ [부록 II] 7. 취약점 점검결과 및 수준측정(예시) 참조

● 자산의 위협요인과 취약점을 최소화하기 위한 기존 보호대책의 적정성, 효율성 및 문제점 등 파악·분석
- 보안지침, 보안절차규정 등 관련문서 검토와 업무담당자와의 면담 등을 통해 기존 보호대책 및 이미 계획된 대책 평가
- 기존 보호대책 평가시 보호대책의 적정성, 효율성 뿐만 아니라 대책이 실제로 이행되고 있는지에 대해서도 평가

※ [부록 II] 8. 기존 보호대책 평가(예시) 참조

4) 4단계 : 취약점 평가(위험수준 평가)

● 자산·위협·취약점 분석을 통하여 획득한 자료와 분석결과를 바탕으로, 취약점에 대한 종합적인 평가 수행
- 자산 중요도 및 위협·취약점 수준, 위협요인과 취약점과의 상관관계 등을 고려하여 취약점 평가(위험수준 평가)등급을 산정하기 위한 기준 수립
- 자산 중요도, 위협수준, 취약점수준, 기존 보호대책의 적정성 및 이행여부 등을 고려하여 취약점에 대한 평가등급을 부여하고, 평가등급이 실제 어떤 의미를 가지며 업무수행에 어떤 위험을 초래할 수 있는가에 대한 평가의견 기재

※ [부록 II] 9. 자산별 위협을 고려한 취약점 평가(위험수준평가)결과 작성(예시) 참조

5) 5단계 : 보호대책 수립

● 관리기관의 가용자산, 자산의 중요도, 보호대책 수립비용 대비 효과 등을 고려하여 효율적인 보호대책 수립 및 동대책의 집행방법 채택
- 보호대책은 각 자산에서 발견된 위협요인 또는 취약점을 감소시키기 위하여 관리적·기술적·물리적 보호대책을 선별 또는 병행하여 사용할 수 있음
- 기존 보호대책(계획된 보호대책 포함) 분석결과를 검토하여 기존 보호대책의 보완사항 또는 신규 보호대책 기재
- 보호대책 보고서는 보호대책 집행시의 제한사항, 기대효과분석 결과 등도 포함하여 작성

※ [부록 II] 10. 보호대책 작성(예시) 참조

※ [부록 II] 11. 보호대책 보고서 작성(예시) 참조

바. 취약점 분석 · 평가의 범위(대상)

● 정보통신기반보호법 제8조에 따라 중앙행정기관에 의해 지정된 주요정보통신기반시설
  – 또한 상기 주요정보통신기반시설을 운영 · 지원하기 위한 시스템(업무용 PC 등) 및 네트워크 등도 가급적 포함

● 주요정보통신기반시설 보호와 관련된 관리 · 운영사항
  – 주요정보통신기반시설을 관리 · 운영하는 인력에 관한 사항
  – 주요정보통신기반시설과 관련된 물리적 시설 및 환경에 관한 사항
  – 주요정보통신기반시설 및 동 시설 보호대책(정보보호시스템 포함)의 운용 · 시행과 관련된 사항

사. 취약점 점검 항목

1) 취약점 점검 항목 선정시 고려사항

● 취약점 분석 · 평가시 기술적 취약점, 관리적 취약점, 물리적 취약점에 대한 점검이 필요함

● 취약점은 시스템 · 네트워크 구성의 변경, IT 기술의 변화, 신규 공격방법의 출현 등에 의해 변동될 수 있으므로 각 관리기관은 취약점 점검 항목의 주기적인 갱신이 필요함

● 각 관리기관에서는 기술적, 관리적, 물리적 사항을 참조하여 취약점 점검 항목을 가감하여 정할 수 있음

가) 기술적 사항

● 주요 정보의 기밀성 · 무결성 · 가용성을 보장하기 위하여 비인가자에 의한 자원 접근 취약점, 정보 유출 및 변조 취약점, 정상적인 서비스를 저해하는 지연 및 마비 가능성, 악성 프로그램 감염 여부 등을 점검

나) 관리적 사항

● 정보통신기반시설의 보호를 위한 정보보호정책 수립 및 관리 취약점, 정보보호조직 및 인적 보안 취약점, 정보보호 인식 및 교육 · 훈련 부재, 정보시스템 운영 · 관리 취약점, 비상계획 및 침해사고대응 취약점 등을 점

다) 물리적 사항

● 주요정보통신기반시설 출입자 통제 및 감시 소홀, 기반시설의 지원설비(전원공급장치, 소방시설 등) 설치 · 운영 미비사항 등을 점검

아. 취약점 분석 · 평가의 방법

● 취약점 분석 · 평가계획 수립시 취약점 분석 · 평가 주기, 해당 관리기관의 정보보호요구사항, 가용할 수 있는 자원(전담반의 전문성, 기간, 예산), 취약점 분석 · 평가 대상시설의 규모 등을 고려하여 구체적인 취약점 분석 · 평가 수행방법 결정

〈 취약점 분석 · 평가 수행방법 〉

구 분		설 명
정밀한 취약점 분석 · 평가	특 징	장기간에 걸쳐 대상시스템에 대한 정밀분석을 시행하여 보호수준 점검
	방 법	– 취약점 분석 · 평가 절차를 준용하여 각 단계 수행 – 자산 중요도 평가, 위협요인 분석 및 취약점 분석, 취약점 평가(위험수준 평가) 등의 과정을 충실히 수행
간이 취약점 분석 · 평가	특 징	단기간에 최소의 자원을 사용하여 수행하는 방법으로, 대상시스템에 대한 기본적인 점검항목에 따라 보호수준 점검
	방 법	– 취약점 분석 · 평가 절차를 준용하되, 취약점 분석 · 평가의 목적을 훼손하지 않는 범위 내에서 일부의 절차 간소화 및 생략 가능 – 전년도에 수행한 정밀 취약점 분석 · 평가의 산출물을 참고자료로 활용 예) 취약점 점검 및 이를 감소시키기 위한 보호대책 수립에 중점을 두어 취약점 분석 · 평가의 단계를 수행하고, 자산 중요도, 위협목록은 전년도의 산출물을 이용
혼합형 취약점 분석 · 평가	특 징	혼합형 수행방법을 채택하는 경우 정밀분석대상 자산과 그렇지 않은 자산을 구별하여 점검
	방 법	정밀분석대상 자산에 대해서는 정밀방식 적용, 그렇지 않은 자산에 대해서는 간이방식 적용

- 취약점 분석 · 평가 수행방법은 정밀한 취약점 분석 · 평가, 간이 취약점 분석 · 평가, 혼합형 취약점 분석 · 평가 등이 있음

● 주요정보통신기반시설 관리기관에서 2년마다 1번씩 실시하는 정기 취약점 분석 · 평가는 정밀한 취약점 분석 · 평가를 수행하되
- 해당 관리기관의 정보보호요구사항, 가용자원, 대상시설의 규모 등을 고려하여 모든 대상에 정밀분석을 수행하는 것이 부적정한 경우, 혼합형 취약점 분석 · 평가를 수행
- 혼합형 취약점 분석 · 평가를 채택하는 경우, 정밀분석대상 자산과 그렇지 않은 자산을 구별하고 그 내용을 취약점 분석 · 평가계획에 반영

● 전년도에 정밀한 취약점 분석 · 평가를 수행하였을 경우에는 간이 취약점 분석 · 평가를 수행하되, 기반시설에 중요한 변화 발생시에는 관리기관 장의 판단하에 정밀한 취약점 분석 · 평가 수행 가능
- 전년도에 수행한 취약점 분석 · 평가 이후 추가된 자산도 취약점 분석 · 평가 대상에 포함
- 매년 새로운 취약점들이 등장하므로 취약점 분석시 취약점 항목을 갱신하여 수행

※ 취약점 분석시, 전년도에 수행한 정밀한 취약점 분석 · 평가 결과 수립한 보호대책이 수행되고 있는지 여부를 확인하는 과정도 포함하여야 함

1) 취약점 분석 · 평가 방법

● 주요정보통신기반시설 세부자산별 또는 업무 프로세스별로, 식별된 취약점이 위협요인에 의하여 침해당할 가능성 및 침해시 영향을 정량적 또는 정성적 방법으로 평가

※ 관리기관의 실정에 따라 정량적 또는 정성적 분석 등 평가방법 채택

※ 정량분석(Quantitative Analysis)
- 정보시스템 및 관련자산에 대한 자산가치, 위협 및 취약점 정도를 화폐 가치로 환산하고 이 값을 토대로 위험의 정도 역시 화폐가치로 환산하는 방법

※ 정성분석(Qualitative Analysis)
- 자산가치, 위협, 취약점, 그리고 위험의 정도를 화폐 단위로 환산하지 않고, 상 · 중 · 하 등으로 그룹화하여 표현하거나 서술형태로 표현하는 방법

2) 외부 정보보호전문기관에 취약점 분석 · 평가 위탁시 고려사항

● 관리기관이 소관 주요정보통신기반시설의 취약점 분석 · 평가를 외부 정보보호전문기관에 위탁하는 경우,
- 해당 기관의 내부인력이 함께 참여토록 하고, 취약점 분석 · 평가를 위탁받은 기관이 이를 직접 수행하도록 함

● 관리기관은 외부 전문기관이 취약점 분석 · 평가 업무 수행과 관련하여 취득한 관리기관의 비밀정보를 외부에 유출하지 않도록 적절한 조치를 취하고
- 전문기관은 취약점 분석 · 평가 업무와 관련하여 작성한 기록 및 자료를 안전하게 보존하며
- 정보보호컨설팅전문업체 지정이 취소되거나 업무를 폐지한 때에는 취약점 분석 · 평가에 관한 기록 및 자료를 관리기관에게 반환하거나 이를 폐기토록 하고, 그 폐기의 적정성 여부를 확인하여야 함

● 다수의 기관이 정보통신망을 통하여 상호간에 연관된 업무를 수행하는 경우 상호연동되는 주요정보통신기반시설에 대한 취약점 분석 · 평가는 해당 관리기관의 동의를 얻어 수행토록 함

제5장 침해사고의 예방과 대응

1. 침해사고의 정의 및 종류
2. 보호지침의 제정 및 보호조치
3. 침해사고 대응업무

1. 침해사고의 정의 및 종류

가. 침해사고의 정의

- 침해사고란 다음의 행위가 발생하여, 주요정보통신기반시설의 운용이 교란, 마비 또는 파괴된 경우를 말함
  - 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작, 파괴, 은닉 또는 유출하는 행위
  - 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스, 논리폭탄 등의 프로그램을 투입하는 행위
  - 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

나. 침해사고의 종류

- 바이러스, 트로이잔호스, 웜, 백도어, 공격 스크립트 등을 유포, 설치, 실행시켜 피해를 야기시키는 악성코드 공격(Malicious Code Attack)
  - 비인가된 시스템 접근, 비인가된 파일 접근, 그리고 네트워크 정보수집을 포함한 비인가된 네트워크 정보 접근 등의 비인가된 접근
  - 네트워크 서비스의 취약점을 이용하여 서비스를 무단 이용하는 비인가된 서비스 이용
  - 네트워크나 시스템의 정상적인 서비스를 마비 또는 파괴시키는 서비스 방해
  - 공식적인 목적이외의 용도로 시스템 및 네트워크 사용하는 행위 등

2. 보호지침의 제정 및 보호조치

가. 보호지침의 제정

- 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있음

- 관계중앙행정기관의 장은 기술의 발전 등에 따라서 보호지침을 주기적으로 수정 · 보완하여야 함

- 보호지침을 제정함에 있어서 다음의 사항을 포함하여야 함
  - 정보보호체계의 관리 · 운영
  - 취약점 분석 · 평가 및 침해사고 예방
  - 침해사고 대응 · 복구에 관한 사항

- 관계중앙행정기관의 장은 보호지침을 제정 · 수정 또는 보완한 경우 이를 소관 관리기관의 장에게 통지

나. 보호조치

- 관계중앙행정기관의 장은 제5조제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 분석하여 필요하다고 인정하는 때에는 해당 관리기관의 장에게 주요정보통시기반시설의 보호에 필요한 조치를 명령 또는 권고 할 수 있음

- 정보통신부장관은 보호조치 명령 · 권고를 받은 해당관리기관의 장이 보호조치를 시행하는데 필요한 기술적 지원을 할 수 있음
  - 다만, 법 제7조제2항에 해당하는 경우 국가보안업무를 수행하는 기관이 지원

3. 침해사고 대응업무

가. 침해사고 통지

- 중대한 침해사고 발생시 이를 인지한 해당 정보통신기반시설 관리기관의 장은 관계행정기관 또는 수사기관 또는 보호진흥원 중 필요한 기관에 통지
  - 이는 중대한 침해사고를 당한 관리기관과 침해사고의 성격에 따라 피침해자의 선택적 통지를 가능하게 하기 위함

- 중대한 침해사고가 광범위하게 발생한 경우에는 정보통신기반보호위원회에 통보하여 침해사고대책본부를 구성 · 운영

나. 피해확산의 방지와 긴급대응

- 침해사고 발생시 대책본부에 의한 대책이 취해지기 이전에 침해행위, 침해상황 등에 대한 조사 및 피해의 확산방지를 위하여 긴급한 대응조치가 필요함

- 이와 관련하여 수사기관은 주요정보통신기반시설에 대한 침해사고의 긴급대응을 위하여 침해사고 발생시 긴급현장출동 및 추적수사, 침해사고 수사와 관련한 국제협력의 업무를 수행

다. 복구조치

- 주요정보통신기반시설 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 하며, 복구 및 보호조치를 위하여 필요한 경우 관계행정기관의 장 또는 한국정보보호진흥원장에게 지원을 요청할 수 있음

- 관계행정기관의 장 또는 한국정보보호진흥원장이 지원요청을 받은 때에는 침해기관의 피해복구가 신속히 이뤄질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 주요정보통신기반시설 관리기관의 장과 함께 적절한 조치를 취하여야 함

제6장 정보공유 · 분석센터

1. 정의
2. 설립주체
3. 설립 및 변경통지
4. 정보공유 · 분석센터의 취약점 분석 · 평가

1. 정의

● 정보공유 · 분석센터(Information Sharing & Analysis Center : ISAC)는 전자적 침해행위에 관한 정보를 분석하고, 침해사고 발생시 이를 관계기관에 신속하게 배포하여 주요정보통신기반시설에 대한 공격을 효과적으로 예방 · 탐지 · 대응할 수 있는 시스템임

● 정부는 정보공유 · 분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있음

2. 설립주체

● 금융 · 통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 업무를 수행하고자 하는 자는 정보공유 · 분석센터를 구축 · 운영할 수 있음
- 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
- 침해사고가 발생하는 경우 실시간 경보 · 분석체계 운영

3. 설립 및 변경통지

● 정보공유 · 분석센터의 장은 정보공유 · 분석센터를 구축한 날부터 30일 이내에 다음 각 호의 사항을 관계중앙행정기관의 장에게 통지
- 명칭 및 사무소의 소재지
- 대표자 및 임원의 인적사항(성명, 주소, 주민등록번호 및 경력)
- 주요업무 등

● 관계중앙행정기관의 장은 통지 받은 사항을 정보통신부장관에게 통보하여야 함

4. 정보공유 · 분석센터의 취약점 분석 · 평가

● 설립기준
- 납입자본금 20억원 이상
- 15인 이상의 기술인력(5인 이상의 고급기술인력 포함)
- 업무 수행 및 자료의 안전관리 설비
- 정보보호관리규정의 제정 및 준수

※ 취약점 분석 · 평가를 수행하는 정보공유 · 분석센터의 기준에 관한 세부적인 사항과 그 기준심사에 관하여 필요한 사항은 정보통신부 장관이 고시

● 복수의 가입기관이 정보통신망을 통하여 영업을 수행하는 분야에 있어서 상호연동된 시설에 대한 취약점 분석 및 평가에 대해서는 해당 가입기관의 동의를 얻어 시행

제7장 정보보호컨설팅전문업체

1. 제도의 도입 배경
2. 정보보호컨설팅전문업체의 지정기준
3. 정보보호컨설팅전문업체의 지정절차
4. 정보보호컨설팅전문업체의 지원업무
5. 정보보호컨설팅전문업체의 보호대책
6. 지정 취소 등

1. 제도의 도입 배경

- 전자적 침해행위의 고도화 · 다양화로 조직 내부의 자원만으로는 각종 정보위협에 효과적으로 대응하기가 곤란해짐
  ※ 정보보호는 조직의 핵심적인 관리과정의 하나로서 기술과 관리 두 측면에서 종합적인 대응이 필요

- 주요정보통신기반시설의 관리기관이 법에 따라 수행할 취약점 분석 · 평가 및 보호대책을 안전하고 신뢰성 있게 지원하는 역할 수행

- 주요정보통신기반시설을 성공적으로 보호하기 위해서는 민 · 관의 긴밀한 협력이 필수적

2. 정보보호컨설팅전문업체의 지정기준

- 인력요건 :고급기술인력 5인 이상을 포함하여 기술인력 15인 이상일 것
  ※ 기술인력의 자격기준은 시행규칙 별표 1에서 정하고 있는데, 고급기술인력은 Project Manager급에 해당

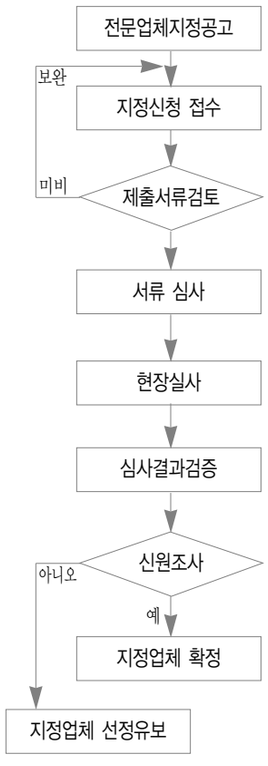
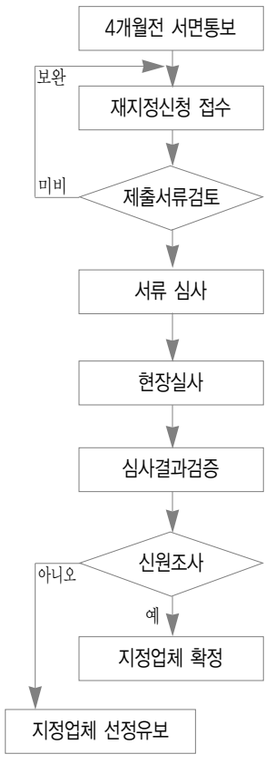
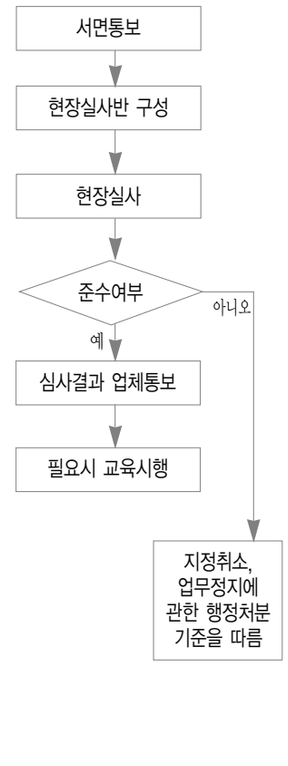
- 자본요건 : 납입자본금이 20억원 이상일 것

- 설비요건 :신원확인 및 출입통제를 위한 설비, 기록 · 자료의 안전관리를 위한 설비 등을 갖출 것

- 능력요건 :업무수행능력심사에서 정통부장관이 정하는 기준점수 이상을 취득할 것
  ※ 시행규칙 별표 2의 규정에 의한 업무수행능력평가는 경험, 전문화, 신뢰도, 기술개발실적 분야의 계량평가항목 70점과 비계량평가항목인 기술심의위원회의 종합심사 30점으로 구성되어 있음

- 정보보호요건 : 정보보호관리규정을 정하고 이를 준수할 것
  – 업무수행구역 및 설비에 대한 보호대책
  – 인원에 대한 보호대책
  – 문서 및 전산자료에 대한 보호대책
  – 기타 정보통신부장관이 필요하다고 인정하는 보호대책

3. 정보보호컨설팅전문업체의 지정절차

지 정	재 지 정	사 후 관 리
필요시	지정업체의 유효기간 만료시 (3년)	1년(해당 년도에 지정, 재지정된 업체 제외)
		
인력 요건, 자본 요건, 설비 요건, 정보보호 요건, 업무수행능력 요건	※ 지정 기준과 동일	인력 요건, 자본 요건, 설비 요건, 정보보호 요건, 변동사항신고 의무

4. 정보보호컨설팅전문업체의 지원업무

- 주요정보통신기반시설의 취약점 분석 · 평가 업무
- 주요정보통신기반시설보호대책의 수립 업무
- 정보통신서비스제공자와 집적정보통신사업자에 대하여 매년 정보보호지침에 따른 정보보호 안전진단 실시

5. 정보보호컨설팅전문업체의 보호대책

- 지정심사단계
  - 모든 기술인력에 대한 보안업무규정에 따른 신원 조사
  - 정보보호관리규정의 제정 및 그 실효적 준수여부에 대한 현장실사
- 프로젝트수행단계
  - 시행령 제18조제2항의 규정에 의한 관리기관의 조치의무
  - 취약점분석 · 평가기관의 재위탁금지의무
  - 보안관계규정의 적용
  - 관리기관과 정보보호컨설팅전문업체가 계약을 체결하는 경우
    - 비밀유지, 기록 · 자료의 관리 및 폐기, 인원통제, 감사 등
    - 컨설팅과 솔루션공급계약의 분리

6. 지정 취소 등

가. 지정취소에 처하는 경우

- 정보통신부장관은 정보보호컨설팅전문업체가 다음의 경우에 해당하는 때에는 정보통신부령이 정하는 바에 따라 정보보호컨설팅전문업체의 지정 취소를 명하여야 함
  - 속임수 기타 부정한 방법으로 지정을 받은때
  - 법 제17조제4항의 규정에 의한 정보보호컨설팅전문업체 지정기준에 미달한 때
  - 법 제18조의 규정에 의한 결격사유에 해당된 때(임원이 결격사유에 해당된 날부터 3월 이내에 당해 임원을 개임시 제외)

나. 지정취소 또는 업무의 전부 · 일부정지에 처하는 경우

- 정보통신부장관은 정보보호컨설팅전문업체가 다음의 경우에 해당하는 때에는 정보통신부령이 정하는 바에 따라 정보보호컨설팅전문업체의 지정취소를 하거나 3월 이내의 기간을 정하여 업무의 전부 또는 일부의 정지를 명할 수 있음
  - 업무를 수행하면서 알게된 정보를 오용 또는 남용하여 주요정보통신기반시설의 운영에 장애를 가져온 때
  - 기타 정보통신기반보호법 또는 동법에 의한 명령을 위반한 때

제8장 의무와 벌칙

1. 형벌에 처하는 경우
2. 과태료에 처하는 경우

1. 형벌에 처하는 경우

가. 주요정보통신기반시설 침해행위 등의 금지의무 위반

● 주요정보통신기반시설을 침해하는 행위를 하여 주요정보통신기반시설을 교란 · 마비 또는 파괴한 경우 10년 이하의 징역 또는 1억원 이하의 벌금을 부과

※ 형법
컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해하는 경우 5년이하의 징역 또는 1천5백만원이하의 벌금을 부과

※ 정보통신망이용촉진및정보보호등에관한법률
악성프로그램을 전달 또는 유포하거나 정보통신망에 장애를 발생하게 하는 행위를 하는 경우 5년이하의 징역 또는 5천만원이하의 벌금을 부과

● 주요정보통신기반시설을 침해하는 행위 유형
- 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나, 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작 · 파괴 · 은닉 또는 유출하는 행위
- 데이터를 파괴하거나, 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스 · 논리폭탄 등의 프로그램을 투입하는 행위
- 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나, 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

나. 기관종사자의 비밀유지의무 위반

● 다른 법률에 특별한 규정이 있는 경우를 제외하고 기관에 종사하는 자 또는 종사 하였던 자가 그 직무상 알게된 비밀을 누설한 경우 5년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금을 부과

● 비밀유지의무기관의 종류
- 주요정보통신기반시설에 대한 취약점 분석 · 평가업무를 하는 기관
- 침해사고의 통지 접수 및 복구조치와 관련한 업무를 하는 관계기관
- 정보공유 · 분석센터

2. 과태료에 처하는 경우

가. 정보통신기반시설 관리기관의 소관 주요정보통신기반시설 보호대책에 대한 보호조치명령 위반

● 관계중앙행정기관장은 주요정보통신기반시설보호대책을 분석하여 필요하다고 인정하는 때에는 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있으며
- 명령에 대한 이행확보의 차원에서 이를 위반한 경우 1천만원 이하의 과태료를 부과함

나. 정보공유 · 분석센터 업무종사자 인적사항 등 신고의무 위반

● 정보공유 · 분석센터의 장은 구축한 날 또는 통지할 사항이 변경된 때부터 30일 이내에 업무종사자의 인적 사항 등 대통령령이 정하는 사항을 관계중앙행정기관의 장에게 통지

● 통지사항
- 명칭 및 사무소의 소재지
- 대표자 및 임원의 인적사항(성명 · 주소 · 주민등록번호 및 경력)
- 주요업무
- 회비 · 수수료 등 재원조달방식
- 조직운영규칙(법인인 경우에는 정관 포함)
- 업무를 위탁하는 경우에는 해당수탁기관의 명칭 및 사무소의 소재지, 대표자 및 임원의 인적사항 등

● 통지의무를 위반하는 경우 정보공유 · 분석센터의 안전 · 신뢰성 담보 차원에서 1천만원 이하의 과태료를 부과하도록 함

다. 정보보호컨설팅전문업체의 업무 휴지 · 폐지 · 재개시 신고의무 위반

● 정보보호컨설팅전문업체가 업무를 휴지 · 폐지 · 재개하는 경우 일정한 기간(30일)을 두어 정보통신부장관에게 동 사실을 신고하도록 하고 이를 담보하기 위하여 1천만원 이하의 과태료를 부과

라. 정보보호컨설팅전문업체의 자료제출의무 위반

● 정보보호컨설팅전문업체가 정보통신부장관으로부터 관련 서류 또는 자료의 제출을 요구받고 특별한 사유없이 관련서류 또는 자료를 제출하지 아니하거나 허위로 제출한 경우 1천만원 이하의 과태료 부과

마. 정보보호컨설팅전문업체 지정취소시 자료반환 · 폐기의무 위반

● 정보보호컨설팅전문업체는 지정이 취소되거나 업무를 폐지한 때에는 주요정보통신기반시설의 취약점 분석 · 평가업무와 관련하여 작성한 기록 및 자료를 관리기관의 장에게 반환하거나 이를 폐기하여야 하며 이의 위반시 1천만원 이하의 과태료를 부과

부록 I 주요정보통신기반시설 지정평가 기준 사례

1. 개 요
2. 지정평가 세부기준(안)
3. 지정평가 기준(안) 운용방법
4. 「지정대상시설 관리기관」의 지정평가보고서 작성방법

1. 개 요

● 정보통신기반보호위원회 등 기반시설 지정관련기관이 객관적으로 기반시설 지정여부를 판단할 수 있도록 정보통신기반보호법 제8조 제1항의 규정에 의한 지정기준을 구체화
  – '동법 제8조 제1항의 5개 지정기준' 에 대한 각각의 세부기준 마련

※ 정보통신기반보호법 제8조 제1항의 규정에 의한 5개 지정기준

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 당해기관이 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

● 지정평가의 용이성을 제고하기 위해, 법제8조 제1항의 5개 지정평가기준별의 중요도에 따라 최고 평가점수(가중치)를 배정한 평가기준(안) 마련

〈법제8조 제1항의 5개기준별 최고 평가점수(안)〉

구 분	업무의 국가 사회적 중요성	업무의 기반 시설 의존도	타 기관시설 과의 연계성	침해사고 발생시, 피해규모	침해사고 발생 가능성 또는 복구 용이성	합 계
최고 평가점수	20점	15점	20점	30점	15점	100점

2. 지정평가 세부기준(안)

가. 당해기관 업무의 국가사회적 중요성(20점)

평가기준	해당점수				평가점수
당해기관의 주요업무가 국가안보 · 사회질서 유지 · 국민생활 안정유지 등에 필요한 공공적 업무에 해당되는 정도는?	높음	보통	낮음	없음	
	20	16	12	0	

※ 판단 時 고려사항 : 당해기관의 업무가 국방, 행정, 치안, 통신, 전력, 수도, 금융, 물류, 의료 등 공공서비스에 해당되는지 여부, 당해기관의 업무가 국가기밀(또는 기간산업)과 관련된 정보, 데이터, 기술 등에 해당되는지 여부 등을 종합고려

나. 당해기관 업무의 정보통신기반시설에 대한 의존도(15점)

평가기준	해당점수				평가점수
당해기관의 주요업무를 수행하는 데에 당해기관의 정보통신망 및 전산시스템(임차시설 포함)에 의존하는 정도는?	높음	보통	낮음	없음	
	15	12	5	0	

※ 판단 時 고려사항 : 당해기관의 업무 대부분이 반드시 해당 지정대상시설을 기반으로 처리되어야 하는지 여부, 해당 지정대상시설이 주요업무처리 과정에 기여하는 정도, 당해기관의 주요업무가 해당 지정대상시설에 의존하여 연중무휴로 서비스가 제공되는지 여부, 침해사고 발생시 대체 시설을 이용하여 당해기관의 주요업무 처리가 가능한지 여부 등을 종합고려

다. 다른 정보통신기반시설과의 상호연계성(20점)

평가기준	해당점수				평가점수
당해기관의 지정대상 평가시설과 타 정부기관 및 민간분야의 정보통신망, 전산시스템과의 상호연계성 정도는?	높음	보통	낮음	없음	
	12	10	5	0	
당해기관의 지정대상 평가시설의 기능장애가 타 정부기관(통신, 전력, 수도, 금융, 운송, 의료 등 공공적 서비스 제공기관 포함)의 업무 및 자산에 미치는 영향 정도는?	높음	보통	낮음	없음	
	8	6	3	0	

※ 당해기관의 지정대상시설과 타기관의 연계성 정도 판단 時 고려사항
  : 당해기관의 업무 수행을 위해, 타기관의 시스템을 이용하는 정도는/범위는
※ 당해기관 장애시, 타 기관의 업무 및 자산에 미치는 영향판단 時 고려사항
  : 당해기관의 업무 장애시, 국방, 행정, 치안, 통신, 전력, 수도, 금융, 물류, 의료 등 타 공공서비스 기관의 업무수행에 미치는 영향정도 등을 종합 고려

라. 침해사고 발생시의 피해규모 및 범위(30점)

평가기준	해당점수				평가점수
당해기관의 지정대상 평가시설에의 전자적 침해사고 발생시, 당해기관의 업무 수행을 위한 대체 방법 존재 등 지속적 업무수행 능력 정도는?	높음	보통	낮음	없음	
	0	2	6	8	
당해기관의 지정대상 평가시설에의 전자적 침해사고 발생시, 국가위기 상황(국방, 행정, 치안, 통신, 전력, 수도, 금융, 운송, 의료 등 공공 서비스 중단에 따른 혼란) 초래 정도는?	높음	보통	낮음	없음	
	15	13	5	0	
당해기관의 지정대상 평가시설에의 전자적 침해사고 발생시, 국가기밀(또는 기간산업)정보 · 데이터 · 기술 또는 개인 프라이버시에 관한 사항 등 정보의 유출 · 변조로 인한 피해 정도는?	높음	보통	낮음	없음	
	7	5	3	0	

※ 침해사고 발생시, 업무지속능력 판단 時 고려사항
: 수작업 등으로 업무를 지속할 방법이 있는지, 타 기관을 통해 업무를 지속할 방법이 있는지 등을 종합고려

※ 침해사고 발생시, 국가위기 초래정도 판단 時 고려사항
: 경제적 피해의 범위수준은(국지적인가/전국적인가), 정치적, 사회적 피해의 질적인 수준은(당해기관의 문제인가/국가적 문제인가), 물류, 금융, 항만, 무역 등 국민의 일상생활 영위에 불편을 끼치는 정도 등을 종합고려

※ 침해사고 발생시, 주요정보의 유출 · 변조 피해수준 판단 時 고려사항
: 정보유출 · 변조로 인한 피해범위는(특정 소수인가/불특정 다수인가), 정보유출 · 변조로 인한 피해수준은(당해기관의 문제인가/ 국가차원 또는 사회 · 경제적 차원의 문제인가) 및 당해기관이 다루고 있는 정보의 질적 수준 등을 종합고려

마. 침해사고 발생가능성 또는 복구의 용이성(15점)

평가기준	해당점수				평가점수
당해기관의 지정대상 평가시설에 대한 전자적 침해사고 발생 가능성은?	높음	보통	낮음	없음	
	5	4	1	0	
침해사고 발생 대비관련 예방 · 대응계획 수립 시행 및 백업시스템을 운용하고 있는가?	있음		없음		
	1		3		
당해기관의 지정대상 평가시설에의 전자적 침해사고 발생시, 침해사고 복구 소요기간은?	2일 이상	24 시간내	12 시간내	1시간 내	
	7	6	4	1	

※ 침해사고 발생 가능성 판단 時 고려사항
: 과거 침해사고 발생정도, 최근에 방화벽 · 침입탐지시스템(IDS) · 통합보안관리시스템(ESM) 등 보안 장비설치 유무, 사이버공격 기술발달 정도 등을 종합고려

※ 예방 · 대응계획 수립여부 판단 時 고려사항
: 침입사고 발생을 예방하기 위한 예방수칙 및 비상연락망, 장비운영 매뉴얼, 비상시 복구조직 운영, 대응교육실시 여부 등의 세부적인 절차와 방법을 명기한 예방 · 대응계획서가 수립되어 있는지의 여부 확인

※ 복구의 용이성 판단 時 고려사항
: 과거 침해사고 복구경험, 침해사고 복구대응능력(시스템 백업,자료 백업 등) 등을 종합고려

3. 지정평가 기준(안) 운용방법

● 중앙행정기관의 장은 정보통신기반보호법시행령 제14조의 규정에 따라 평가기준을 지정대상시설 관리기관의 장에게 통보하고, 지정대상시설 관리기관의 장이 시설지정 평가업무를 수행토록 지휘
- 또한, 중앙행정기관의 장이 해당 분야의 특수성을 반영하여 5개 항목별 세부 평가기준 내용을 추가 또는 제외하거나, 세부 평가기준별 점수를 달리 부여하고자 할 경우에는,
- 법제8조 제1항의 5개 지정평가 항목별 최고 평가점수에 각각 ±0.20%이내의 가중치를 두어 산정한 최고(최저) 점수내에서 조정 · 평가

〈중앙행정기관의 지정평가 특이점 반영시 평가점수 권고(안)〉

구 분		업무의 국가 사회적 중요성	업무의 기반 시설 의존도	타 기관시설 과의 연계성	침해사고 발생시, 피해규모	침해사고 발생 가능성 또는 복구 용이성	합 계
최고 평가점수 (기본)		20점	15점	20점	30점	15점	100점
가중치 적용시	최 고 (+0.20%)	24점	18점	24점	36점	18점	120점
	최 저 (-0.20%)	16점	12점	16점	24점	12점	80점

※ 주1) 가중치 적용시에는 5개 항목별로 20%씩 일율적으로 반영을 하여도 되고, 각각의 항목별로 20%이내에서 각각 다르게 적용하여도 됨

※ 주2) '업무의 국가사회적 중요성(기본 20점, 가중치 적용시 24점~16점)'의 세부평가기준의 내용을 추가 또는 제외하더라도, 동 항목의 점수는 24점~16점 이내에서 반영

● 중앙행정기관의 장은 관리기관의 지정평가 보고서의 적정성을 심사한 후, 평가점수가 총 80점 이상(또는, 중앙행정기관의 장이 별도로 정하는 점수이상)일 경우에는, 당해시설을 주요정보통신기반시설로 지정하기 위한 시설지정(안)을 마련하여 정보통신기반보호위원회에 상정

4. 「지정대상시설 관리기관」의 지정평가보고서 작성방법

가. 기관 소개

● 당해 기관의 주요업무에 대해 구체적으로 기재

나. 지정단위 및 세부시설 선정

● 당해기관의 업무중 중요한 업무를 지원하는 정보통신기반시설과 주요 세부시설을 선정하여, 아래의 양식에 따라 작성

〈지정단위 및 세부시설 선정 작성 양식 및 작성사례〉

지정단위	세부시설	설치장소	수량	처리업무 (시스템의 역할)
지방행정 정보망	- 침입차단시스템 - 통합보안관리시스템 - ATM스위치 - 라우터 · ·	- 16개 시도 - 16개 시도 - 16개시도, 232개시군구 - 망센터 및 16개시도 · ·	48 1 248 33 · ·	- 지방행정정보망 침입차단 - 16개시도의 보안시스템 통합관리 - 초고속국가망 ATM서비스에 접속 - 지방행정정보망 네트워크경로 관리 · ·

〈주〉 지방행정정보망은 '01년 12월에 행정자치부가 지정한 주요정보통신기반시설임

● 선정된 정보통신기반시설에 대한 시스템 개요와 시스템 구성도

다. 지정평가 결과 및 의견

● 지정단위별 평가결과는 다음양식에 따라 작성하고, 평가결과에 대한 당해기관의 의견을 작성

- 지정단위별 세부평가 내역은 첨부

구 분	업무의 국가 사회적 중요성	업무의 기반 시설 의존도	타 기관시설 과의 연계성	침해사고 발생시, 피해규모	침해사고 발생 가능성 또는 복구 용이성	합 계
지정단위 명칭 기재	?점	?점	?점	?점	?점	?점

부록 II 취약점 분석 · 평가 항목 (예시)

1. 주요정보통신기반시설 세부자산 분류 기준(예시)
2. 주요정보통신기반시설 자산 중요도 부여기준(예시)
3. 위협요인 식별 및 수준측정(예시)
4. 기술적 취약점 점검 항목(예시)
5. 관리적 취약점 점검 항목(예시)
6. 물리적 취약점 점검 항목(예시)
7. 취약점 점검결과 및 수준측정(예시)
8. 기존 보호대책 평가(예시)
9. 자산별 위협을 고려한 취약점 평가 (위험수준평가)결과 작성(예시)
10. 보호대책 작성(예시)
11. 보호대책 보고서 작성(예시)

1. 주요정보통신기반시설 세부자산 분류기준(예시)

□ 세부자산 분류기준 예

분 류	설 명
정보/데이터	조직정보, 인사정보, 자금정보 등 조직의 중요한 정보자산 예) 금융정보, 개인정보, 구성파일, 보안설정파일 등
문서 및 서류	업무와 운영 등에 관련된 문서 예) 보안정책서, 운영 및 절차서, 네트워크 및 시스템 구성도 등
하드웨어	조직의 업무, 서비스를 수행하기 위해 필요한 하드웨어 예) 메인프레임, 서버, 방화벽, 라우터, 스위치, PC 등
소프트웨어	조직의 업무, 서비스를 수행하기 위해 필요한 소프트웨어 예) 웹서버 SW, 메일서버 SW, DB 서버 SW, 인사급여 시스템 등
건물/설비	정보자산운영을 위해 필요한 시설 예) 화재탐지장치, 전력시설, CCTV 등

2. 주요정보통신기반시설 자산 중요도 부여기준(예시)

□ 자산 중요도 부여기준표 예

평 가	평가 기준
매우높음(VH)	자산에 대한 피해 발생시 업무가 마비될 정도의 극심한 피해가 발생함
높음(H)	자산에 대한 피해 발생시 업무의 마비는 발생하지 않으나 업무 수행에 심각한 지장을 초래하거나, 업무 전반에 영향을 미침
중간(M)	자산에 대한 피해 발생시 업무 수행의 효율성이 저하되거나, 일부 업무 기능에만 영향을 미침
낮음(L)	자산에 대한 피해 발생시 업무 수행에 거의 영향을 끼치지 않음

※ 주요정보통신기반시설의 세부자산(하드웨어, 소프트웨어 등)을 식별할 경우, 각 세부자산이 핵심업무에 미치는 영향에 따라 중요도를 차별화하여 평가

3. 위협요인 식별 및 수준측정(예시)

□ ○○기관 인터넷뱅킹 시스템 웹서버

• 위협요인 식별 예

위협시나리오					위협설명
행위자		접근경로	동기	결과	
인간 (내부자)		네트워크	우연	변경	유지보수중 관리자의 실수로 특정파일 이름 변경
				노출	관리자의 환경파일 설정실수로 인한 고객신상정보 노출
				손실/파괴	파일 또는 디렉토리 삭제
			고의	변경	특정 파일로 이름을 변경하거나 파일 내용 조작
				노출	내부자의 고객신상정보를 제3자에게 제공
				손실/파괴	파일 또는 디렉토리 삭제
				방해	내부자에 의한 논리폭탄 설치
		물리적 접근	…	…	…
인간 (외부자,제3자)		네트워크	…	…	…
		물리적 접근	…	…	…
기술 결함	SW 결함	–		손실/파괴	수행 중 오류로 인한 웹 디렉토리 삭제
	통신 문제			손실/파괴	통신회선 손상
				방해	통신서비스 중단으로 인한 웹서비스 중단
	전원 문제			방해	갑작스런 전원 공급 중단으로 인한 웹서비스 중단
자연 재해	화재, 홍수	–		손실/파괴	대형 화재 또는 홍수로 인한 시스템 손실 또는 파괴
				방해	대형 화재 또는 홍수로 인한 웹서비스 중단
	…			…	…
…				…	…

※ 행위자 : 인간(내부자, 외부자 · 아웃소싱 등 제3자), 기술결함, 자연재해 등
※ 접근경로 : 물리적 접근, 네트워크 등
※ 동기 : 우연, 고의 등
※ 결과 : 변경, 노출, 손실/파괴, 방해 등
※ 위협요인 식별시 ‘별표 6. 위협목록(예시)’ 참조

□ 위협수준 측정 기준표 예

평 가	발생주기 또는 발생가능성	위협에 의한 영향
매우높음(VH)	가능성 매우 높음(1년에 4회 이상 발생)	손실이 매우 크고 업무가 장시간 중단됨
높음(H)	가능성 높음(1년에 2회~3회 발생)	위협으로 인한 손실이 크나 업무의 중단을 초래하지 않음
중간(M)	가능성 있음(1년에 1회 발생)	위협으로 인한 손실이 있으나 업무에 심각하게 영향을 끼치지 않음
낮음(L)	자산의 Life Cycle 동안 거의 발생하지 않음	위협으로 인한 손실이 매우 경미함

※ 발생가능성(발생횟수/년)은 대상기관의 상황에 맞도록 기준 조정 필요

4. 기술적 취약점 점검 항목(예시)

구 분	취약점 점검 항목
사용자 신분위장	– 사용자 신분확인 및 인증 메커니즘 취약점 – 패스워드 관리 소홀 – 패스워드 파일 미보호 – 로그인 절차 무시 – 비밀번호가 없는 임시계정의 방치 – 송신자의 신분확인 및 인증 메커니즘 취약점 (팩스, 이메일 등을 이용한 발신자 가장)
네트워크에 대한 비인가된 접근	– 무선랜 사용자 및 단말기 인증 메커니즘 취약점 – 네트워크 접근통제 메커니즘 취약점 – 네트워크 프로토콜의 버그 – 네트워크간의 잘못 설정된 신뢰관계 – 네트워크 트래픽 감시/분석 메커니즘 취약점 – 내부 네트워크/시스템 정보(IP주소, 사용자ID, 컴퓨터ID 등) 공개 – 네트워크 통신장비 및 시스템 원격관리기능 취약점 – 네트워크 관리기능의 무단실행가능 취약점 – 불필요한 서비스 제공
소프트웨어에 대한 비인가된 접근	– 부재시 로그아웃 불이행(또는 자동 로그아웃기능 부재) – 소프트웨어의 잘 알려진 버그들 – 멀티유저 환경에서 다른 사람의 정보를 알 수 있는 채널 존재 – 개방형 기술(ODBC 등)을 이용한 접근통제 메커니즘 우회 경로 존재 – 산재되어 중복 보관되는 구조화되지 않은 저장 상태 – 사용자 ID와 패스워드가 소스에 포함된 프로그램 존재 – 소프트웨어 접근통제 메커니즘 취약점 – 소프트웨어 접근권한의 잘못된 할당 – 감사기록 및 추적기능의 부재 – 비정상적인 실행 종료 – 사용자환경의 부적절한 제한(즉, 일반사용자가 개발자료 및 운영시스템에 접근 가능한 환경) – 시스템 및 응용프로그램의 구성 · 설정 오류 – 소프트웨어 기능시험에 사용된 실제 데이터의 방치
저장매체에 대한 비인가된 접근	– 데이터 무결성, 기밀성 메커니즘(암호화) 부재 – 저장매체 폐기시 데이터 미삭제 – 저장매체에 대한 불법 복제 – 유지보수자에 의한 자료 유출
전송데이터 유출 및 변조	– 유 · 무선 전송데이터 보호메커니즘(암호화) 부재 – 무선랜 전파도달 거리조절 및 암호화 부재 – 송 · 수신자의 신원확인, 송 · 수신 정보의 무결성 및 기밀성을 보장하기 위한 전자서명법상의 전자서명인증체계(행정기관의 전자공문서 유통을 위한 시스템의 경우 전자관인인증체계) 부재 – 안전하지 않은 이메일 서비스 사용(암호메커니즘) – 시스템관리자에 의한 불법적인 이메일 감시 체계 미비 – P2P, 메신저 등을 통한 정보 유출
서비스지연 및 마비	– 회선의 용량 부족 – 인터넷 웜, 서비스거부공격 등에 의한 트래픽 폭주 대응책 부재 – 병목지점(라우터, 침입차단시스템 설치지점)에서의 오류 – 전송회선에 대한 전기적 간섭 – 손상된 회선 및 네트워크 연결요소의 고장 – 잘못 설정된 통신 소프트웨어 존재
악성 프로그램	– 인터넷, P2P 프로그램 등으로부터 소프트웨어 다운로드 및 사용 – 백업 체계 미비 – 메일폭탄 및 논리폭탄 감시 프로그램 존재 여부 – 불법적인 소프트웨어 반입 – 바이러스 백신 설치 및 주기적인 업데이트 미비

5. 관리적 취약점 점검 항목(예시)

구 분	취약점 점검 항목
정보보호정책 수립	– 주요정보통신기반시설의 자체 정보보호정책 수립 및 문서화 미비 또는 정책의 불이행 – 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 전직원의 숙지 미흡
정보보호조직 및 인적보안	– 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 – 정보보호시스템을 관리 · 운영하는 정보보호 담당자 미지정 – 정보보호지침 및 절차에 대한 위반시 공식적인 징계절차 부재 – 기밀정보 취급담당자의 기밀준수 서약서 미작성 – 직원의 인사이동이나 퇴직시 계정삭제 등 적절한 보안조치 미비 – 위탁업체 등 외부자가 주요정보통신기반시설에 접근하는 경우에 대한 적절한 통제 절차 수립 및 이행 미흡 – (주요정보통신기반시설을 위탁하는 경우) 위탁계약시 서비스제공자의 정보보호관련 지시엄수, 정보에 관한 비밀유지, 정보의 제3자 제공 금지 및 사고시의 책임부담 등에 대한 규정 부재 또는 당해 계약내용을 서면 또는 전자적 기록으로 미보존 – 주요정보통신기반시설을 위탁 관리하는 업체 또는 개인이 비밀유지 각서 미작성 – 외부자의 주요정보통신기반시설 접근 기록 관리 및 감사 미비
정보자산 분류	– 정보보호의 대상이 되는 하드웨어, 소프트웨어 등 주요정보자산 조사 미실시 – 정보자산별 소유자, 관리자 등 책임자 미지정 – 자산의 보안등급에 따른 취급절차 불이행
교육 및 훈련	– 관리기관 임직원의 정보보호 정책 및 지침 숙지 미흡 – 시스템관리자 등 정보보호와 관련된 업무 종사자를 대상으로 한 정기적인 정보보호교육 미실시 – 직원을 대상으로, 재난과 비상시에 취할 절차에 관한 정기적인 훈련 미실시

구 분	취약점 점검 항목
정보통신시스템 운영 · 관리	– 보안정책을 반영한 세부 운영절차 부재 – 정보처리설비 및 시스템의 변경(H/W, S/W)을 통제하는 절차 부재 – 핵심적인 사업정보 및 소프트웨어 백업의 정기적 수행 미흡 – 비인가자에 의한 정보유출 또는 오용을 방지하기 위한 정보의 취급 및 저장절차 부재 – 정보보호정책에 의한 주기적인 패스워드 변경 미수행 – 민감한 정보를 수록하고 있는 매체에 대한 사용내역과 승인된 사용자/응용프로그램에 대한 기록 유지절차 부재 – 정보시스템 부정 접근 방지를 위한 제반보호조치에 관련 기준 수립 및 시행 미흡 – 프로그램의 설치, 변경, 및 시스템/네트워크 정책 설정시 사전/사후 통제할 수 있는 절차 부재 – 소프트웨어 사용에 대한 관리감독 소홀 – 라우터의 접근제어기능 또는 침입차단시스템의 필터링 기능 등을 이용한 정보시스템과 외부 네트워크와의 미분리 – 운영환경 및 개발환경의 미분리 – 정보보호시스템 로그의 주기적인 관리 소홀 – 각종 로그에 대한 보관 및 관리 절차 부재
업무연속성 관리 및 보안사고 관리	– 재난, 비상사태 대응을 위한 비상계획과 재난복구방안의 문서화 미비 – 자연재해 등 문제 발생시 신속하고 체계적인 문제복구 및 처리를 담당할 추진조직 체계 부재 – 비상시를 대비하여 안정적인 전원공급 대책 부재 – 비상사태 또는 침해사고 대비 H/W, S/W에 대한 예비요소 확보 미흡 – 배선작업에 대한 문서화 미비 – 해킹 등 침해사고 대응 방법 및 절차 수립 미비 – 취약점 점검 소프트웨어 등을 이용한 주기적인 취약점 점검 미실시 – 내부자료 유출방지를 위한 로그파일 감시, 자동탐지 S/W 등 대처 방법 부재 – 침해사고 발생시의 보고절차 수립 및 증거자료 수집 · 보관체계 부재 – 신종바이러스 출현시 해당 바이러스를 치료할 수 있는 백신프로그램의 신속한 도입 및 배포 절차 부재

6. 물리적 취약점 점검 항목(예시)

구 분	취약점 점검 항목
출입 통제 및 감시	– 정보시스템 및 라우터 등의 정보통신망 설비가 설치 · 운영되는 장소에 대한 부정한 접근을 방지하기 위한 출입통제 및 감시 소홀 – 주요정보통신기반시설에 대한 제한구역 설정 미흡 – 불법 침입 등에 대비한 물리적 보안시설 설치 운영 소홀 – 물리적 보안시설에 대한 운영 담당자 미지정 – 각종 백업 미디어에 대한 안전한 장소(제3의장소등) 보관 미흡 – 정보 및 물리자산의 반입/반출 감시메커니즘 부재
지원시설 관리	– 주요정보통신기반시설의 안정적인 전원공급을 위한 UPS, 자가발전설비 등의 설치 · 운영 소홀 – 화재감지센서 및 소화설비 등 설치 · 운영 소홀 – 수해로부터 보호위한 주요정보통신기반시설물의 방수시공 미흡 – 주요정보통신기반시설의 24시간 항온 · 항습 유지 · 관리 소홀

7. 취약점 점검결과 및 수준측정(예시)

□ ○○기관 인터넷뱅킹 시스템 웹서버 취약점 점검결과

구 분		점검항목	점검결과	수준 측정
관리	접근통제	사용자 패스워드 관리 절차의 수립 여부	사용자 패스워드 생성 절차 및 주기적 변경 등 관리절차가 지침서에 기술되어 있으나 명확하지 않음	L
	운영 · 관리 절차	주기적 패치 절차 수립 여부	지침서에 패치관련사항이 존재하지 않음	M
	…			
물리	전산실 보안	UPS 또는 자가발전 설비 설치여부	전산실내 UPS가 설치되어 있음	L
	제한구역 출입통제	출입자의 신원확인여부	제한구역 출입구에서 출입자의 신원확인 등 출입통제 수단이 없음	H
	…			
기술	패스워드 관리	사용자 패스워드 취약여부	패스워드가 없거나 취약한 패스워드를 가진 사용자가 존재함 – 아이디 : test, 패스워드 : 없음 – 아이디 : webadmin, 패스워드 : webadmin	H
	…			

※ 수준측정 설명
- 매우높음(VH) : 자산복구가 불가능하거나 피해규모가 아주 큰 경우
- 높음(H) : 자산의 복구는 가능하나 그 피해규모가 비교적 큰 경우
- 중간(M) : 자산을 쉽게 복구가능하고 피해규모가 비교적 적은 경우
- 낮음(L) : 취약점이 자산에 별다른 영향을 끼치지 않는 경우

8. 기존 보호대책 평가(예시)

□ ○○기관 인터넷뱅킹 시스템 웹서버 기존 보호대책 평가

취약점 분류	기존 보호대책	기존 보호대책 평가
패스워드 취약	– 지침서에 패스워드 관리절차가 기술되어 있으나, – 개별 시스템에는 패스워드 정책이 구현되어 있지 않고 – 패스워드 설정여부는 전적으로 개별 사용자에 일임	보완필요 (개별 시스템에 패스워드 관리 정책 구현 필요)
…		

9. 자산별 위협을 고려한 취약점 평가(위험수준평가)결과 작성(예시)

□ 자산별 위협을 고려한 취약점 평가(위험평가) 결과

업무/시스템명	자산 분류	자산명	자산 가치	위 협		취 약 점		기존 대책	평가 등급	평가 의견
				내 용	수준	내 용	수준			
인터넷 뱅킹 시스템	소프트웨어	웹서버	M	네트워크를 통한 비인가자의 시스템 권한 획득	H	패스워드가 취약한 사용자 계정 존재 (test,webadmin)	H	보완 필요	6	※ 의견1
				…						

※ 평가등급은 아래의 평가등급 산정표 활용

※ 의견1 : 패스워드가 설정되어 있지 않거나 패스워드와 아이디가 동일한 사용자(test:없음, webadmin:webadmin)가 존재하여 외부의 공격자가 웹서버에 불법으로 접근(로그인)할 수 있고, 로그인 후 정보를 유출하거나 웹서버 관리자(root) 권한 획득을 시도할 수 있으므로 보호조치가 필요함

□ 평가등급 산정표 예

위협		L				M				H				VH			
취약점		L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
자산	L	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	M	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	H	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	VH	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10

※ (자산, 위협, 취약점) 값이 (L, L, L)인 경우 평가등급을 1로 하고, 자산, 위협, 취약점 값 중 하나가 1등급씩 높아질 때마다 1을 더하여 평가등급 산정

※ 자산, 위협, 취약점 값 중 어느 하나가 VH인 경우 평가등급 산정표의 값에서 1을 더하는 등 가중치를 부여하여 평가등급을 산정하는 방법도 가능
(예) 자산, 위협, 취약점이 (VH, M, H)인 경우 7 대신 8로 산정

10. 보호대책 작성(예시)

□ ○○기관 인터넷뱅킹 시스템 웹서버 보호대책

위협	취약점	평가 등급	기존 보호대책	보호대책
네트워크를 통한 비인가자의 시스템 권한 획득	패스워드가 취약한 사용자 계정 존재(test, webadmin)	6	보완필요 (지침서에 패스워드 관리절차가 기술되어 있으나 개별 시스템에는 패스워드 정책이 구현되어 있지 않음)	- 패스워드 관리절차가 이행되도록 개별 시스템에 패스워드 정책 구현 • 패스워드 없는 계정 생성 불가 • 패스워드 추측이나 크래킹을 막을 수 있도록 패스워드를 안전하게 생성 및 주기적으로 변경 - 주기적인 점검 수행 • 패스워드 점검도구를 이용하여 주기적으로 사용자 패스워드 검증
				정보보호지침에 명확한 패스워드 관리정책 언급
...				

11. 보호대책 보고서 작성(예시)

□ 개요
- ○ 수행목적 및 전략
- ○ 수행범위 및 대상
  - – 주요정보통신기반시설 현황
  - – 정보보호관리문서 현황
- ○ 보호대책 요약
  - – 전년도 추진계획 대비 실적
  - – 현황평가 및 개선방향

□ 부문별 보호대책
- ○ 관리적 보호대책
- ○ 물리적 보호대책
- ○ 기술적 보호대책
  - ※ 취약점 분석 · 평가 방법 및 내용, 결과 포함

□ 정보보호 추진계획
- ○ 취약점 분석 · 평가 계획
- ○ 침해사고 예방 계획
- ○ 침해사고 대응 · 복구 계획

□ 비용 및 기대효과 분석

□ 기타

정보통신기반보호법 가이드

2004년 12월 인쇄
2004년 12월 발행

발행인 : 이 홍 섭
발행처 : 한국정보보호진흥원
서울시 송파구 가락본동 78번지
IT벤처타워(서관)
Tel : (02) 4055-114
인쇄처 : 호정씨앤피
Tel : (02) 2277-4718