스마트 강국은 정보보호에서부터

전자정부 정보보호 중기 추진계획

2011. 6. 28.

MINISTRY OF
PUBLIC ADMINISTRATION
AND SECURITY

MINISTRY OF
PUBLIC ADMINISTRATION
AND SECURITY

1. 추진배경

2. 전자정부 정보보호 현황

3. 추진 내용

1. 추진 배경

1. 추진 배경

세계 최고 수준의 전자정부 서비스 구현

- UN 전자정부 1위 ('10. 6월)
- 정보화 마을, 민원 24 등 UN 공공행정상 수상 ('11. 6월)

해킹·DDoS 등 사이버 위협 증가

48%가 정부 주요 사이트 대상 공격
- 7.7 DDoS ('09년)
- 3.4 DDoS ('11년)

은행 전산망 해킹 사고

H 캐피탈 보안 해킹사고(4.7)	175만 명 개인정보 유출
N은행 전산망 해킹 사고	전산망 2주간 마비

세계 1위의 전자정부 서비스를 안정적으로 제공하기 위해 전자정부 정보보호 종합대책 마련이 시급

2. 전자정부 정보보호 현황

가. 정보시스템 정보보호 현황

정보보호 인프라	❍ 중앙부처 및 시 · 도는 정보보호 인프라 구축 양호 ❍ 소속기관 및 시군구는 DDoS, 방화벽, 서버보안 등 설치미흡 (50%이하)
보안관제	❍ 중앙부처, 시 · 도 등 총 38개 보안관제센터 구축, 조달청 등 13개 중앙부처 미구축 (시군구는 시 · 도에 연계하여 관제)
내부자 보안관리	❍ 전산실 내부자 보안관리는 전반적으로 취약 - 전산실 출입이력 수기 관리, 출입시 노트북 등의 자료변경 여부 육안점검, 정보시스템 접근시 인증수단 취약 - 다수 기관의 전산실 근무인력 PC가 인터넷에 연결 ※ 전산실 출입시 공무원 현장 동행, 관리자계정 업체 미공유 등은 양호
비상시 복구 체계	❍ 중앙부처는 240개 핵심업무 선정, 그 중 72% 재해복구시스템 구축 (소속기관, 시 · 도, 시군구는 재해복구시스템 구축 미흡)

나. 공무원 PC 정보보호 현황

PC 보안	❍ PC 보안 인프라는 비교적 양호 – 백신SW는 모든 행정기관 설치, – 중앙부처 · 시도는 유해사이트 자동차단. 네트워크 접근제어 등 PC 보안 인프라 비교적 양호 ❍ 중앙부처 소속기관, 시 · 군 · 구 등 미 설치기관은 미흡
망분리	❍ 44개 중앙부처 본부 및 주요 소속기관 35개 완료

다. 정보보호 기반 여건 현황

정보보호 인력

❍ 정보보호 전담 공무원
- 중앙부처 : 평균 3.4명
- 시. 도 : 평균 5.1명

※ '11년 정보보호 전담 공무원 60명 증원(중앙 45명, 시 · 도 15명)

정보보호 인력채용

❍ 정보보호 분야 우수 인력 유치를 위한 공무원 채용제도 및 기술자격증 제도 도입 미흡
- 전산직 공무원 5급 · 7급 · 9급 시험과목에 보안 관련 과목 부재, 공채 및 특채 시험시 필요한 정보보호 관련 국가기술자격증 부재

전산직 7급 공채 과목	자료구조, 데이터베이스, 소프트웨어공학, 프로그램언어
전산직 필수 국가기술자격	정보관리, 전자계산조직응용, 전자계산기, 정보통신

정보보호 인력교육

❍ 정보보호 인력에 대한 체계적 교육 프로그램 부재
- PC보안 등 기초과정 위주, 이론 위주의 교육 치중

정보보호 업무인식

❍ 기관장은 정보보호 관심 미흡, 일반직원은 정보보호 인식 미흡으로 보안관리 소홀
- 정보보호 인력은 열악한 근무환경, 사고시 책임 추궁 등으로 업무 기피

라. IT 환경변화에 따른 신규위협 현황

스마트워크 보안위협	재택근무, 스마트워크센터, 모바일 이동근무 등 스마트워크 활성화에 따른 다양한 보안위협 증가 ❍ 재택근무 : 개인 PC에 자료 작성. 보관으로 정책정보 유출 가능, PC방에서도 재택근무서비스(GVPN) 이용 가능 ❍ 모바일근무 : 단말기 분실. 도난, 악성코드 감염 등 신규 위협 발생
신종 사이버공격	❍ 신종 사이버공격 증가 - 변종 DDoS 공격(RUDY 등) - 스마트폰 등 휴대용기기를 이용한 공격(PDoS) 등

3. 추진 내용

1. 정보보호 인프라 확충

DDoS, 스팸/ 바이러스	❍ 정부통합전산센터 또는 소관 중앙부처에 관련 장비를 확충 · 공동 활용하여 예산절감 · 운영 효율화
침입방지, 방화벽, 웹방화벽	❍ 정보보호 핵심 인프라로써 전 행정기관에 구축 – 방화벽의 경우 업무망과 인터넷 구간에 각각 장비 설치
서버보안	❍ 업무 중요도 분석(‘11.12) 후 주요 시스템을 대상으로 추가 설치

2. 보안관제 효율화

통합관제

❍ 중앙부처 중 관제대상시스템이 적은 기관은 상위기관 또는 정부통합 전산센터 등을 통해 통합관제

❍ 유관부처 및 시 · 도와 협의하여 세부 통합관제 방안 마련('11.8월)

보안관제 인력 확대

❍ 관제센터의 주관기관 정규 인력이 1명이상 상시 근무할 수 있도록 보안관제 인력 확대 추진

❍ 공공기관 보안관제를 실시하는 기관의 경우 행정. 공공기관 시스템 비율에 따라 공무원 증원

3. 내부자에 의한 보안위협 예방 · 조치

출입관리	❍ 출입이력관리시스템을 구축하여 출입이력 자동 기록관리
정보시스템 접근관리	❍ 전산실 근무 인력에 대해서는 원칙적으로 인터넷 차단 – 인터넷을 사용하고자 하는 경우 별도 PC 또는 공무원 PC 활용 ❍ 접근관리시스템 구축 – 인증서 기반의 시스템 접근, 금지명령어 자동 차단, 작업내역 관리 등의 효과적 수행
전산실 내부정보 유출 예방	❍ 전산실에 노트북 반입금지, 필요시 읽기전용매체(CD) 반입 – 내부 자료 유출방지를 위해 출력물 유출방지시스템 구축
법제도 개선	❍ 내부정보 유출행위자에 대한 처벌을 강화토록 「전자정부법」 개정 ❍ 「행정기관 정보시스템 접근권한 관리규정」(총리훈령) 등을 개정하여 내부자 정보유출 방지를 위한 의무 규정 보완

4. 비상시 복구 체계 구축

재해복구 시스템 구축

❍ 정부통합전산센터에 240개 국정핵심업무 중 미 구축된 67개 업무 재해 복구시스템 구축 우선 추진(~'12)

- 기관별 재해복구시스템의 경우 별도 연구용역을 통해 시스템의 중요도 등 진단 후 추진계획 수립('11년말)

5. 공무원 PC 정보보호 인프라 구축

유해사이트 자동차단 시스템 도입

❍ 全 행정기관에 P2P 등 유해사이트 자동차단 시스템 도입

- 시 · 군 · 구 및 주요 데이터를 취급하는 중앙부처 소속기관에 네트워크 접근제어 시스템 구축

❍ 중앙부처 소속기관 및 시 · 도의 스마트워크 환경 구축시 일부 보안시스템을 추가하여 망 분리 효과 도모

- 스마트워크 환경구축시 일부 보안시스템을 추가하면 논리적 망분리와 효과동일

6. 정보보호 인적 역량강화 및 인식제고

정보보호 인력 증원

○ 각급기관의 정보보호 적정인력 산정기준 마련(‘11.7 행안부)
- ‘10년 정보보호 인력 조직진단시 고려되지 않은 개인정보보호법 제정에 따른 업무, 정보통신기반 보호업무 등 추가 반영

○ 각급기관은 산정 기준에 따라 추가 인력 소요제기(‘11.8)
※ 행안부는 소요 제기한 인력규모 타당성 검증 및 증원(’ 11.9~)

우수 정보보호 인력 채용. 배치 확대

○ 전산직렬 시험과목 개정
- 5급. 7급. 9급 전산직렬 공채 시험과목에 정보보호 과목 신설
※ 공무원임용시험령 개정(7월) → 유예기간(2년)
→ ‘14년 시험과목 개정 시행

○ 정보보호전문가(SIS) 자격증을 국가기술자격증으로 격상하고 전산직렬 채용시험의 필수 자격증으로 추가 지정

○ 행정기관 대상 정보보호 전문인력 특채 가이드라인 마련. 배포
- 정보보호 특채시 우대 요건(학위, 자격증, 경력 등) 등 명확화

정보보호 담당자 교육 강화 및 인식제고

○ 정보보호 인력교육 프로그램 개발 및 일정 수준 교육 이수 의무화
- 정보보호 분야 신규배치 인력(배치 후 3개월 이내 기본교육), 기존인력(연 40시간 교육)

○ 정부업무평가 및 지자체 합동평가에 정보보호분야 비중 확대

○ 시 · 도 지사 협의회 등을 활용, 기관장 · 부기관장 정보보호 인식교육 실시

○ 정보보호 담당자 사기진작을 위한 정부포상 확대

7. 각 기관의 정보보호 수준 진단 · 컨설팅 및 지원강화

❍ 전자정부 정보보호인증체계 개선

- 기존 2단계 평가를 5단계 평가로 변경
- 행정기관의 자발적 개선 노력 유도
- 5단계 정보보호 수준 측정을 위한 점검영역. 항목. 방법. 절차 마련('11.12)

❍ 전 중앙부처 및 시도, 일부 소속기관. 시군구에 대해 컨설팅 지원 실시

- 전문심사원에 의한 진단을 통해 기관 맞춤형 보안대책 수립 지원

8. SW 개발시 보안취약점 집중 개선

SW개발보안 제도 의무화

❍ SW개발시 보안이 매우 중요
- 해킹 공격은 대부분 SW 보안취약점을 이용

❍ 감리대상 중 40억 원 이상 사업에 우선 적용하고 순차적 확대
- ('12.하반기) 40억원 이상 → ('13) 20억원 이상 → ('14) 감리대상 전사업

❍ SW개발 가이드 마련 및 관련자 교육 강화('11년 14회)

※ 소니社 - 7,700만명의 개인정보 유출('11)
- 웹취약점인 SQL인젝션 취약점이 원인임

기술이전

❍ 정부 주도로 개발한 프로그램 언어별 소스코드 취약점 진단도구를 민간에 기술이전
- 향후 취약점 진단도구는 민간 주도 개발

9. IT 환경 변화에 따른 신규 사이버위협 대응 강화

재택근무	○ 업무시스템 접속은 SBC 방식을 도입 – 개인 PC에 업무자료가 저장 불허(금지) – 업무서비스 접속은 등록된 PC(노트북)에서만 가능하도록 통제
모바일 행정서비스	○ 재택근무시 보안환경 외에 모바일 환경에 따른 보안 취약요소 보완 (단말 분실시, 원격에서 잠금 등) – 공통보안인프라 구축(MDM 등) 先구축('11.9, 행안부) 및 서비스 개시(각 부처)
신종 사이버공격	○ 향후 예측되는 신종 사이버공격에 대한 지속 연구 · 지원체계 강화 – 신종 사이버공격 연구협의회 구성 ※ 방통위, 국정원 등 유관부처 참여