2016년 정보보안 추진 계획(안)

2016. 3.

서울연구원
The Seoul Institute
도시정보센터
정보서비스팀

목 차

Ⅰ. 추진 개요

❑ 내•외부의 위협요인들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호•운영하기 위함

❑ 이를 통해, 국가 및 연구원 내부정보의 기밀성·무결성·가용성 확보

Ⅱ. 정보보안 관리현황

구 분			내 용
네트워크	유선	백본(Juniper)	- 콘솔 관리자 식별 및 인증 보안 강화 , 이중화
	무선	인증서버(AnyClick)	- WPA2 이상의 보안 알고리즘 사용 - 사용자 인증을 통한 접속기록 유지 - 업무망과 물리적으로 분리하여 보안 강화
정보보호 시스템	방화벽	유선방화벽	- 비인가 IP 및 포트 차단하여 내부 시스템 보호
		무선방화벽(Fortinet)	- 내.외부를 통과하는 트래픽에 대한 접근통제
		웹방화벽(Wapple)	- 웹서비스 운영시 해킹 탐지 및 방어를 통한 보호
	VPN	VPN(Juniper)	- 외부에서 업무망 접근시 암호화 터널링을 통한 접근
	스팸차단	스팸차단메일서버	- 메일 송수신시 필터링 조건에 의한 접근통제
데이터 보호	개인정보 보호	DB 암호화(D'amo)	- DB 내의 개인정보(주민등록번호)를 암호화하여 관리
	홈페이지	SSL 보안	- 브라우저와 서버간 처리정보를 암호화하여 송수신
PC보안	바이러스	Ahnlab V3 8.0	- PC 실시간 검사를 통한 악성코드 및 바이러스 감지 - 네트워크를 통한 해킹프로그램 침입 차단 - 개인 방화벽 설정을 통한 인터넷 연결 차단
		APC 관리서버	- 클라이언트 엔진 업데이트 중앙 관리 및 정책 적용 - 에이전트별 바이러스 및 악성코드 현황 관리
	PC보안 체크	내 PC 지키미 (Comvoy)	- OS,MS Office,한글 보안업데이트 점검 및 확인 - 로그인 패스워드 안정성 확인 - 화면보호기 설정 여부 점검 - 사용자 공유폴더 설정 여부 점검 - USB 자동 실행 허용 여부 점검 - 미사용 ActiveX 프로그램 존재여부 점검

Ⅲ. 정보보안 분야별 주요지침

가. 정보자산 보안관리

1) 네트워크 보안관리

① 유선망과 무선망은 분리 운영

② 무선망 사용자를 관리하여 인가된 사용자의 접속만 허가

③ 무선 사용자의 비밀번호는 연 1회 이상 변경하여 사용하도록 하고, 장기 미접속자는 접근이 불가능하도록 차단

④ 비인가 무선 AP는 정기적으로 점검하여 철수

⑤ 사용자 관련 접속로그 유지 및 국정원 인증 알고리즘을 사용하여 보안인증 강화

⑥ 우회 정보통신망은 자료유출 및 악성코드 유입의 원인이 되므로 매체제어시스템등을 활용하여 무선인터넷 접속장치를 차단

2) 웹서비스 보안

① 전체 웹서비스 대상으로 취약점을 점검 및 조치

② 웹방화벽을 통해 해킹 탐지 및 방어에 대응 할수 있도록 대비

③ SSL(Secure Sockets Layer)을 적용하여 브라우저와 서버 간에 개인정보 및 처리정보를 암호화하여 송수신함.

④ 전자우편 사용시 HTTPS, VPN 등을 통한 전송데이터를 암호화함

3) 보안서버 관리

① 서버관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내무방과 분리된 영역(DMZ)에 설치,운용하여야 한다.

② 각급기관의 장은 비인가 서버 저장자료 절취, 위변조 및 분산 서비스서부 공격 등에 대비하기 위하여 국가정보원장이 안정성을 검증한 침입차단,탐지시스템 및 DDos 공격대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

③ 서버관리자는 비인가자의 공개서버내 비공개 정보에 대한 무단 접근을 방지하기 위하여 서버 접근 사용자를 제한하고 불필요한 계정을 삭제하여야 한다.

④ 공개서버의 서비스에 필요한 프로그램 개발하고 시험하기 위하여 사용된 도구(컴파일러등)개발 완료 후 삭제를 원칙으로 한다.

4) 저장매체 관리

① 정보시스템 및 스토리지 등의 외부 반출 및 폐기시에는 수리자에게 보안서약서를 징구하고, 반출시 하드 디스크는 분리, 저장장치 삭제, 필요한 경우 하드웨어 파기 등의 안정 조치 시행

② USB 저장매체의 자동 실행을 차단

5) CCTV 시스템 보안관리

① CCTV 운용에 관련 시스템을 비인가자의 임의 조작이 물리적으로 불가능하도록 설치하여야 함

② CCTV 상황실은 보호구역으로 지정 관리하고 출입통제장치를 도 입하여야 함

③ 관련 정보통신망 설치시 업무망 및 인터넷망과 분리 운영해야 함

6) PC 및 스마트폰 등 단말기 보안

① PC를 교체, 반납, 폐기하거나 고장으로 외부에 수리 의뢰시 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 시행

② PC의 공유기능 사용을 금함. 불가피할 경우에는 암호를 설정하여 사용하고, 사용즉시 공유기능 제거

③ PC의 도입시 아래와 같은 보호조치를 하여야 함

- 사용자별 비밀번호 사용
- 10분 이상 PC 작업 중단시 암호를 묻는 화면보호기 실행
- 백신 및 PC용 침입차단시스템 등 운용
- 내 PC 지키미를 설치하여 점검
- 소프트웨어(MS 오피스, 한글 등)의 업데이트는 최신으로 유지

④ 노트북 등 장비 반출입 절차 준수하여야 함

- 개인 소유의 노트북,PC 등을 무단 반입하여서는 안되며, 다만 부득이한 경우에는 정보보안담당관의 승인을 받아 사용할 수 있다.
- 관리책임자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신등을 활용하여 악성코드 유입 점검 또는 해킹 프로그램 감염 여부를 점검하여야 한다.

⑤ 스마트폰 사용시 보안 유의사항

- 의심스러운 애플리케이션 다운로드하지 않기
- 신뢰할 수 없는 사이트 방문하지 않기
- 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
- 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
- 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기
- 이상증상이 지속될 경우 악성코드 감염여부 확인하기
- 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기
- 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
- 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

⑥ 휴대용 저장매체 보안 관리

- 휴대용 저장매체 관리 책임자는 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조,훼손,분실 등에 대비한 보안대책을 강구하여 정보보안담당관의 승인을 받아야 한다
- 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하여 반출·입을 통제하여야 한다.

- USB 관리시스템을 도입할 경우 국가정보원장이 안정성을 확인한 제품을 도입하여야 한다.

7) 사이버 위기관리 대응 훈련

① 자체 정보통신망을 대상으로 매년 정기 또는 수시 사이버위기 대응 모의훈련(DDos 공격 , 해킹메일 훈련)등을 실시

② 출처가 불분명하거나 의심스러운 외부 전자우편 수신 대응 훈련

나. 인적 보안

1) 시스템 접근 권한에 따른 사용자 관리

① 사용자가 보직변경 , 퇴직 등 인사이동이 있을 경우 관련 정보시스템 접근 권한을 조정하여야 함

② 정보통신망을 통하여 비밀 등 중요정보를 취급하는 사용자에 대해 비밀취급인가 , 보안서약서 징구 등의 보안조치를 하여야 함.

2) 용역업체 관리

① 정보화사업의 사업계획서에 보안대책을 수립, 반영.

② 보안성 검토, 용역사업자와의 책임범위, 비상대책을 명시하고, 위반시 손해배상 청구 등을 계약서에 명시.

③ 용역업체의 원격작업 금지.(단, 부득이한 경우 IP·사용서비스·접근계정 제한, 암호화 통신 등 필요한 보안대책 마련 후 한시적으로 허용)

④ 용역사업 계약시 참가직원의 보안준수 사항과 위반시 손해배상 책임명시, 용역 참여인원에 대한 친필 보안서약서 제출

⑤ 용역사업 업체의 임의교체 금지 및 참여인원에게 별도의 계정을 개설하고, 계정별로 시스템 접근권한 부여.

⑥ 정보통신망도·IP 현황 등 용역업체에 제공할 자료는 인계인수대장 비치, 보안조치 후 인계인수하고 무단 복사 및 외부 반출 금지

⑦ 용역업체로부터 용역 결과물을 전량회수하고 비인가자에게 제공·열람 금지

⑧ 용역업체의 노트북 등 관련 장비를 반출·반입시마다 악성코드 감염여부, 자료 무단 반출 여부를 확인

다. 정보시스템 보안

1) 정보시스템 구축시 사업의 성격에 따라, 국정원 또는 서울시의 사전 보안성 검토 시행

2) 정보시스템 보안관리

① 정보시스템 접근 사용자의 비밀번호는 9자리 이상으로 설정하고, 분기 1회 이상 변경.

② 정보시스템 사용자를 업무에 따라 접근권한을 달리하고, 업무 담당자 변경시 즉시 반영.

③ 정보시스템 데이타베이스의 주요 정보는 암호화하여 관리.

④ 정보시스템의 시간은 표준시로 동기화.

⑤ 스케줄에 의한 백업을 시행하고, 월 1회 이상 점검.

라. 정보보안 예방점검

1) 정보시스템 및 보안서버 등 월1회 정기점검 및 수시점검 시행

2) 사이버 위협에 대비를 위한 수시 모니터링 및 연락체계 유지

3) 정보보안정책 및 시스템 취약점 개선, 보완, 내실화

마. 사이버 보안의 날 시행

1) 운영개요

- PC, 네트워크, 정보시스템 등 정보자산에 대한 보안상 취약점의 자체점검·보완을 통해 직원들의 정보보호 수준을 제고하고 사이버 안전을 확보하고자 함.

2) 관련근거

- 전자정부법 제56조(정보통신망 등의 보안대책 수립·시행)
- 국가정보보안기본지침 제17조(사이버보안진단의 날)
- 서울시 정보통신보안업무처리규칙 제12조(사이버보안진단의 날)

3) 매월 셋째 주 수요일 시행 (월 1회)

- 점검 결과는 기관장에게 보고 : 별첨 1, 2에 의거하여 집계

Ⅳ. 2016년 정보보안 중점사항

1. DLP (Data Loss Prevention) 보안 솔루션 도입 : 9월경

가. 개인정보 유출방지 : 개인정보 유출로 인한 기관의 법률적 책임에 대응

나. 연구자료 유출방지 : 개인별 화일의 암호화, 보안영역 지정

다. USB 등 휴대용 매체 제어
- 외장매체로 자료 저장시 로그관리
- 등록된 USB만 사용할 수 있도록 외장 매체 통제

라. 이메일을 통한 정보유출 방지 : 상용 이메일 차단(2017년 그룹웨어 개선 후 적용)

2. 자산관리 솔루션 도입 : 7월경

가. PC의 H/W,S/W 사용현황 관리로 연구원 자산관리

나. 사전에 인가된 S/W 사용함으로 불법 S/W 사용 예방

다. 윈도우 패치를 포함한 각종 S/W 패치를 통한 취약점개선

3. '사이버 보안 진단의 날' 시행 강화 : 매월 셋째주 수요일

가. 개인별 보안 점수 매월 통계 분석 후 기관장 보고

나. 위험프로세스 외 분야별 취약성 통계분석

다. 월별 중점 점검 계획

구 분	중점 점검사항
공통사항 〈매월점검〉	o 정보화사업 입찰 · 계약 · 수행 · 종료 등 단계별 용역업체 보안관리 o 정보화시스템 현황, 통신망 구성도, IP 현황 등 정보통신망 자료관리 o 업무망 · 인터넷 분리기관은 망분리 정책 위배여부 점검 - 업무망에서 인터넷 우회접속 가능 여부 - 망간 자료전송시스템 보안점검 o PC 취약점 점검 및 제거여부 o 사용메일, 웹하드, P2P, 메신저 차단목록 갱신 · 추가 및 차단여부 o 인터넷 PC내 업무자료 저장여부 점검
1월 (1.20)	o 정보시스템 보안관리 실태 점검 - 중요정보 암호화 및 관리자 권한 설정 - 인터넷 등 외부망 연결 적절성 확인 o PC진단 결과 통계 작성(7~12月) - 전체PC 대수, 진단 PC 대수 - 백신설치 PC 대수, 바이러스 발견 · 치료 PC대수, 보안패치 적응완료 PC 대수 등 o 행정정보 홈페이지 게재관련 보안관리 강화 - 사전 보안성 검토를 거친 자료에 한해 홈페이지 게제 - 개인정보, 중요 정책정보는 비공개 - 비밀 등을 홈페이지에 게재한 경우 국정원 통보 및 경위조사 실시
2월 (2.17)	o 청사 내 무단 설치된 비인가 무선인터넷 시스템(AP) 점검 o 인가 무선인터넷 시스템(AP) 점검 - 암호화 적용 여부, 관리자 비밀번호 설정 여부(기본 비밀번호 사용 등) - 비인가 사용자 접근통제 대책 o 부처 내 상주 유지보수업체 보안점검 - 메신저, P2P, 웹하드 등 비인가 서비스 사용여부 점검 - PC내 중요자료 저장여부 확인
3월 (3.16)	o 노트북 관리현황 점검 및 재정비 - 노트북內 업무자료 존재여부, 대여 시 포맷 상태 점검여부, - 반납 후 노트북 포맷여부, 관리대장 관리 및 유지여부 등 점검 o 정보시스템 사용자 권한부여 적절성 확인 및 인증절차, 접속로그 백업 여부 점검 - 정보보호시스템 관리자 권한 무단접속 가능여부 점검 병행

구 분	중점 점검사항
4월 (4.20)	o 부처 내 공유폴더 사용실태 점검(비밀번호 설정 등 접근 통제 여부, 불필요 공유폴더등) o 방화벽、침입방지시스템 등 정보보안 장비 보안정책 재정비 o 사이버침해 대비 비상연락체계 재정비 - 대외기관, 부서 정보보안담당자등 유관 연락처
5월 (5.18)	o 업무용 시스템 및 홈페이지 등 정보시스템內 불필요 서비스 포트 활성화 여부 o 부처 시스템內 Telnet 등 원격서비스 사용여부 점검 및 사용목적 관리 등 재정비 - SSH 기본 포트 변경사용 및 접근제어 o 하드디스크 내장형 디지털 OA 기기 현황 파악 포트 변경사용 및 접근제어 o 해외출장자에 대한 보안조치 실태 점검 - 반출 노트북 등에 대한 보안성 검토 - FTA 등 중요 협상자 출장시 안전한 통신수단 확보 - 서약서 징구, 보안교육 확행 등
6월 (6.15)	o 부처내 상주 유지보수업체 보안점검 - 메신저, P2P, 웹하드 등 비인가 서비스 사용여부 점검 - PC내 중요자료 저장여부 확인 o 보안USB관리시스템 점검 - 비밀용, 대외비용, 일반용 USB 등 구분사용 여부 점검 - 매체제어시스템 정상작동 여부 점검 o 직원의 재택 · 파견 · 이동근무 등 원격 근무시 보안관리 절차 준수여부 확인 o 불용 PC, 복사기, 카메라 등 디지털 저장매체 불용처리 실태 확인
7월 (7.20)	o 노트북 관리현황 점검 및 재정비 - 노트북內 업무자료 존재여부, 대여 시 포맷 상태 점검여부, - 반납 후 노트북 포맷여부, 관리대장 관리 및 유지여부 등 점검 - 업무용·인터넷용 구분여부, WiFi 통신기능 차단여부 등 점검 o PC 진단 결과 통계 작성(1~6月) - 전체PC 대수, 진단 PC 대수 - 백신설치 PC 대수, 바이러스 발견 · 치료 PC대수, 보안패치 적응완료 PC 대수 등

구 분	중점 점검사항
8월 (8.17)	o 홈페이지 내 을지연습자료, 개인정보 등 민감자료 게시여부 점검 o 홈페이지 Database 점검 - 기본 패스워드 변경 등 계정、패스워드 보안관리 재정비 - 특이 Table 존재여부 점검 o 소속직원 비상연락망 일제 점검 및 훈련 실시 o 을지연습 대비 암호장비·논리, 보안자재 관리 o 을지연습 관련 비밀작성용 PC에 인터넷 연결 금지
9월 (9.21)	o 청사 내 무단 설치된 비인가 무선인터넷 시스템(AP) 점검 o 인가 무선인터넷 시스템(AP) 점검 - 암호화 적용 여부, 관리자 비밀번호 설정 여부(기본 비밀번호 사용 등) - 비인가 사용자 접근통제 대책 o 국회 '의정자료 전자유통시스템' 실태점검 및 사용 독려
10월 (10.19)	o 라우터, 스위치 등 네트워크 장비보안 재정비 - 관리자 비밀번호 설정여부(기본 비밀번호 사용 등) - 불필요 접근포트 차단 - ACL(접근제어목록) 재정비 등 o 불용PC HDD 정상 소거여부 확인 - PC반납시 개인이 중요자료 삭제후 반납, 불용 HDD 정상 소거여부 등 점검
11월 (11.16)	o 홈페이지 보안취약점 점검 - SQL인젝션, 파일 다운로드 웹 취약점 점검 - 관리자 접근 페이지 차단, 디렉토리 리스팅 여부 확인 o 부처 내 공유폴더 사용실태 점검(비밀번호 설정 등 접근통제 여부, 불필요 공유폴더 등) o 비밀 외주발간 시 보안대책 점검 - 발간업체 PC 등에 작업내용 저장 여부 중점 확인 - 비밀발간 의뢰시 출력물 또는 인가 받은 비밀용USB만 사용 여부
12월 (12.21)	o 장기간 미사용 등 불필요 VPN 계정 재정비 o 내년도 정보공개 관련 공개 · 비공개 기준 재정비 o 보안USB관리시스템 점검 - 비밀용, 대외비용, 일반용 USB 등 구분사용 여부 점검 - 매체제어시스템 정상작동 여부 점검

4. 서울시 2016 정보보안 관리실태 평가 시행 : 11월경

가. 정보 보안 정책

나. 정보 자산 보안 관리

다. 인원 보안

라. 사이버 위기 관리

마. 전자 정보 보안

바. 정보시스템 보안

5. 정보보안(개인정보) 교육 시행

가. 개인정보보호 교육 : 전직원 대상

나. 정보보안과 관련된 안내문을 전 직원을 대상으로 수시 공지

(예: 해킹메일 주의, 윈도우 업데이트, 보안취약점 조치요령, 의심스럽거나 출처가 불분명한 이메일 열람 금지, 외부 상용 이메일 원의 전자우편과 연계 사용 금지 등 보안 유의사항...)

다. 정보보안 담당 직원 연간 40시간 이상 교육 이수

Ⅴ. 별첨 보안지도 체크리스트

기관(부서)명 : 작성일 : 2016. . .

구분	번호	점 검 항 목	결과 (○/×)	점검 주체
PC 보안 진단 실시	1	「사이버보안진단의 날」 자체 행사계획을 수립하였는가?		기관
	2	「사이버보안진단의 날」 행사 관련 3일前 기관 업무망에 공지하였는가?		〃
	3	PC진단프로그램을 「사이버 · 보안진단의 날」에 실행하였는가?		개인
진단 결과 보완	4	PC진단프로그램 실행후 파악된 취약점을 보완 조치하였는가?		〃
		1) 바이러스 백신 설치 및 실행 여부		〃
		2) 바이러스 백신의 최신 보안패치 여부 점검		〃
		3) 운영체제, MS Office의 최신 보안패치 설치 여부		〃
		4) 한글프로그램의 최신 보안패치 설치 여부 점검		〃
		5) 로그인 패스워드 안전성 여부		〃
		6) 로그인 패스워드의 분기 1회 이상 변경 여부		〃
		7) 화면보호기 설정 여부		〃
		8) 사용자 공유 폴더 설정 여부		〃
		9) USB 자동 실행 허용여부 점검		〃
		10) 미사용(3개월) ActiveX 프로그램 존재 여부 점검		〃
중점 점검	5	「사이버보안진단의 날」 월별 중점점검사항을 점검하였는가?		기관

「사이버보안진단의 날」 체크리스트

▢ 기관(부서)명 : _____

구분	번호	공 통 점 검 항 목	
PC 진단 실시	1	자체 보유중인 PC는 모두 몇 대입니까?	전체 PC ( )대
	2	PC진단프로그램(내PC지키미)이 설치된 PC는 몇 대입니까?	설치 PC ( )대
	3	이번 달 내PC지키미로 점검을 수행한 PC는 몇 대 입니까?	수행 PC ( )대

구분	번호	서울시 정보보안평가시스템 항목	
정보 보호 검토	4	'사이버보안진단의 날' 월별 중점 점검사항에 대해 매월 점검하는가?	Y / N / 기타( ) ※ **근거자료 필수**(N은 불필요)
	5	'사이버보안진단의 날' 수행 결과 발견된 문제점 · 미비점 등을 조치하고 있는가?	Y / N / 기타( ) ※ **근거자료 필수**(N은 불필요)
PC 보안 관리	6	사용자는 윈도우 자동 업데이트를 설정하고 매월 최신 업데이트를 수행하는가?	전체 ( )대 중 ( )대 수행
	7	최신 업데이트를 적용한 백신프로그램으로 월 1회 이상 검사를 수행하는가?	전체 ( )대 중 ( )대 수행
	8	사용자 생성 공유폴더를 사용하는가?	전체 ( )대 중 ( )대 미사용

구분	번호	1월 중점 점검항목 [매월 중점점검 사항]	
정보 시스템 보안관리	9	o 정보시스템 보안관리 실태 점검 - 중요정보 암호화 및 관리자 권한 설정 - 인터넷 등 외부망 연결 적절성 확인 o PC진단 결과 통계 작성(7~12月) - 전체PC 대수, 진단 PC 대수 - 백신설치 PC 대수, 바이러스 발견 · 치료 PC대수, 보안패치 적응완료 PC 대수 등 o 행정정보 홈페이지 게재관련 보안관리 강화 - 사전 보안성 검토를 거친 자료에 한해 홈페이지 게제 - 개인정보, 중요 정책정보는 비공개 - 비밀 등을 홈페이지에 게재한 경우 국정원 통보 및 경위조사 실시	○ / X

2016. 1. .

작 성 자 정보보안담당자 직급 성명 (인)

확 인 자 부 서 명(팀장) 직급 성명 (인)