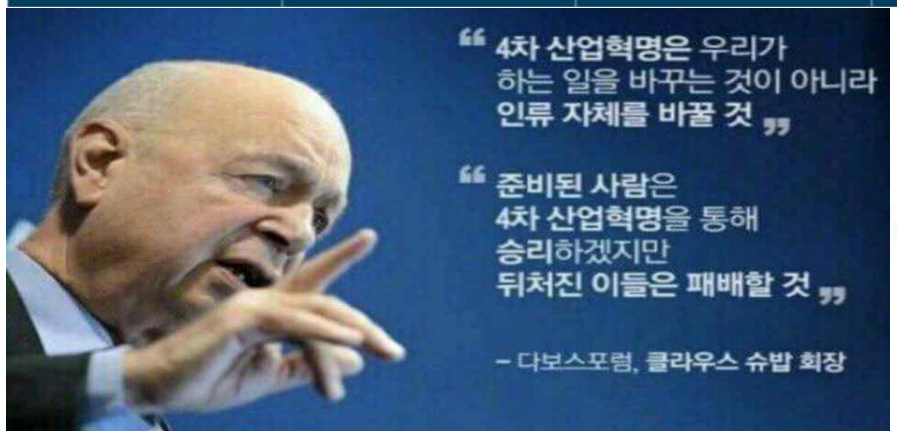
스마트 시대, 정보보안 인식의 변화

2018. 10. 12. 금

I·SEOUL·U
너와 나의 서울

함께서울
시민과 함께 세계와 함께

급변하는 사회 ⇒ 4차 산업혁명의 도래



- 2016년 다보스포럼에서 클라우스 슈밥이 4차 산업혁명을 주창한 이래 사회는 급변
- 모든 사물이 네트워크를 통해 연결되고(IoT) 인공지능(AI)을 통해 자동화
- 수많은 데이터(Big Data)를 효율적으로 처리하는 것이 가능한 시대로 변화

급변하는 사회 ⇒ 보안위협의 다양화

사물인터넷 분야별 보안 위협 시나리오

분야	주요 내용
스마트TV	스마트TV에 탑재된 카메라 해킹 → 사생활 영상 유출
스마트가전	로봇청소기 원격조종 애플리케이션 취약점 해킹 → 로봇청소기 탑재 카메라로 실시간 모니터링
공유기	수십만대 규모 공유기 해킹 → 악성코드 넣어 디도스 공격 창구 활용
스마트카	차량네트워크 침투 가능 조립 회로보드 → 브레이크 조작, 방향 설정, 경보장치 해제 등 가능
교통	도로차량 감지기술 내 광범위한 설계 및 보안 결함 발견 → 센서를 가장해 교통관리시스템에 위조 데이터 전송 가능
의료기기	인슐린 펌프 조작 → 치명적인 복용량 주입 가능

자료 : 한국과학기술기획평가원(KISTEP)

※ Source : 전자신문, 2016.08.06 (KAIST 전자공학과 시스템보안연구실 김용대 교수 연구팀)

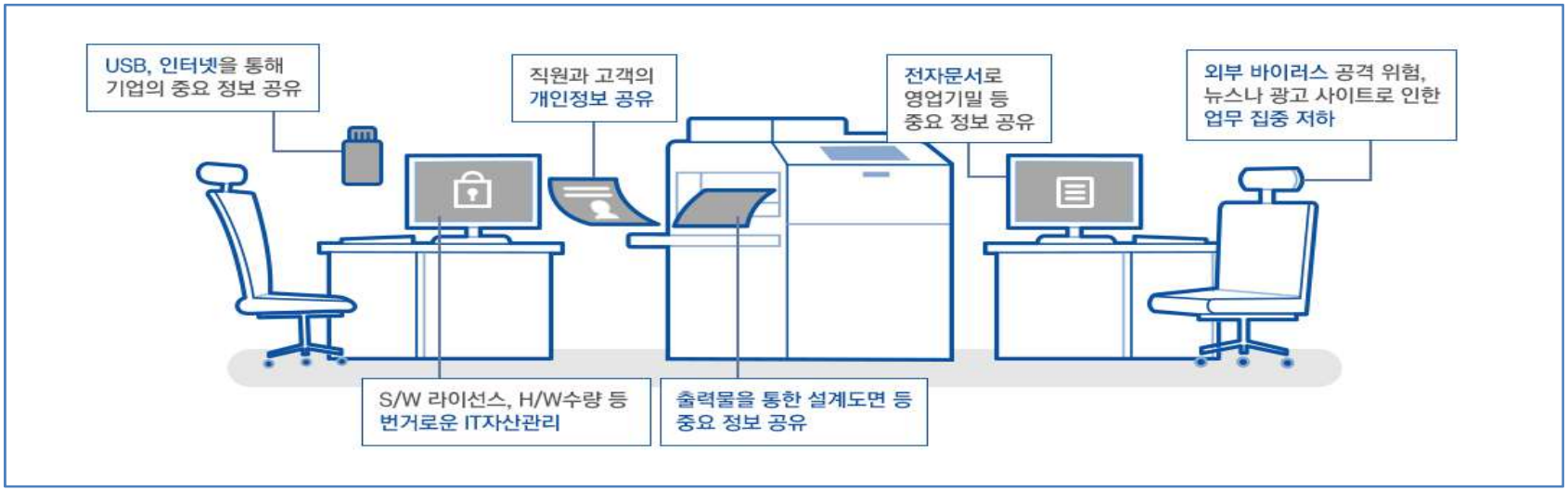
(의료기기 조작)

※ Source : https://youtu.be/QMR2JiH_ymU

(스마트결재 기능 조작)

(버스정보안내기기 조작)

사용자 환경 보안의 중요성



개인 업무 환경에 존재하는 다양한 보안 위협들을 악용한 사고로 개인 뿐만 아니라 조직이 피해를 입는 사례 발생

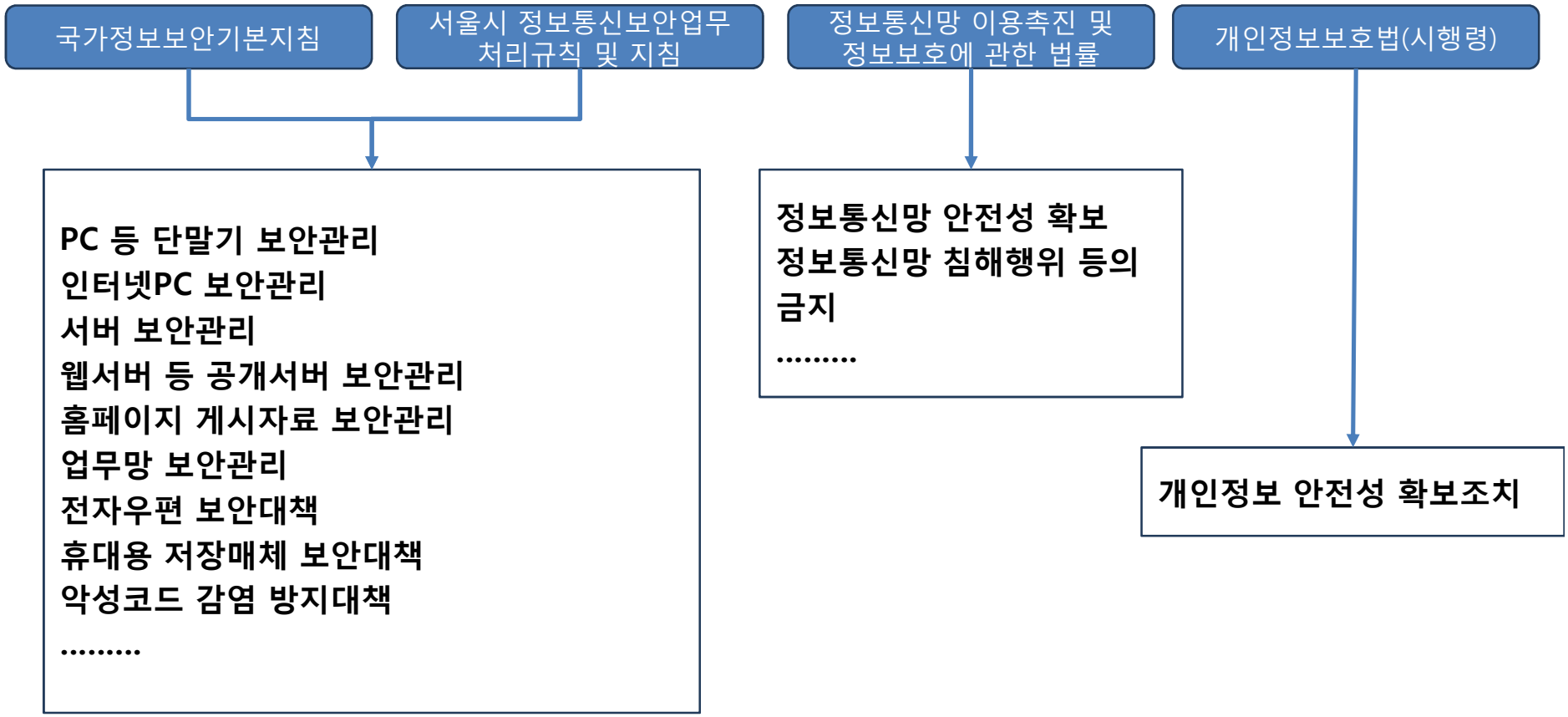
(이메일 피싱)

(악성코드 감염)

사용자 환경 보안의 중요성

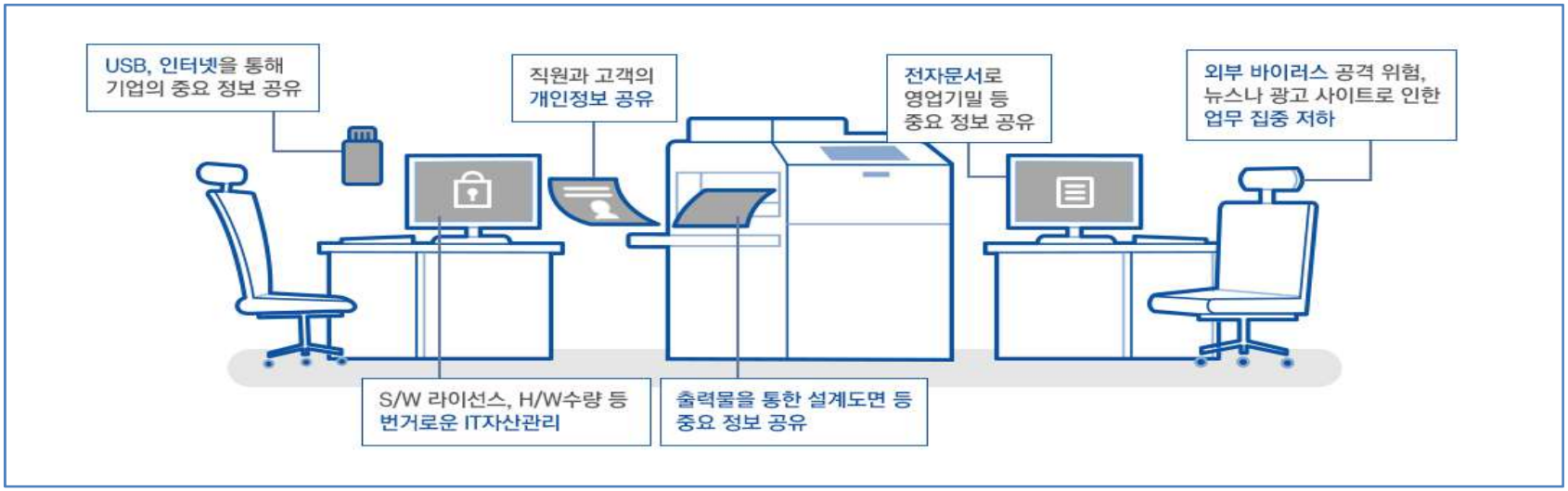
- 2017년 6월, 국내 웹 호스팅 업체 '인터넷나야나'는 랜섬웨어 감염으로 서비스 중이던 서버 153대 감염
- 해커에게 13억원을 지불하여 복호화하는 것으로 협상후 일단락
- 악성코드/랜섬웨어 대응에 있어 최악의 사례로 평가됨

업무환경에 대한 보안 준수 요구



국가정보보안기본지침(국가정보원), 정보통신보안업무처리규칙/지침(서울시)을 비롯해 다양한 법률에서 업무 환경 및 정보시스템 이용에 대한 보안 준수 사항 언급

사용자 업무환경 보안대책



보안대책

<u>보안 프로그램</u>을 통한 **<u>개인 업무 시스템 보안 강화</u>**

- **내PC지키미 : 업무용PC 보안점검 및 조치(백신 및 패치관리 포함)**
- **개인정보암호화 : PC내 개인정보 파일 암복호화**
- **바이러스 백신(V3) : 악성코드 감염 예방(탐지) 및 치료**
- **네트워크접근제어 : 비인가 노트북 등 네트워크 사용차단**
- **보안USB : 비인가 외부저장장치 사용 차단**
- **유해사이트차단 : 불법, 비인가 사이트 접근 차단**

보안대책1. 악성코드 감염예방

서울시 정보통신 보안업무 처리지침

제13조(PC 등 단말기 보안관리)
② 정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 단말기 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.
3. PC용 최신 백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 운영체제(OS) 및 응용프로그램(아래아한글, MS Office, Acrobat 등)의 최신 보안 패치 유지
④ 정보시스템 관리책임자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신 등을 활용하여 해킹프로그램 감염 여부를 점검하여야 한다.

제14조(인터넷PC 보안관리)
② 사용자는 인터넷PC에서 무단으로 업무자료의 작성·저장 및 소통을 금지하고 최신 백신을 활용하여 바이러스 감염 여부 등을 주기적으로 점검하여야 한다.

제22조(악성코드 감염 방지대책)

바이러스 백신 프로그램을 통한 악성코드 예방

- 매일 오후 12시 예약 검사 수행
- 예약 검사 이외에도 주기적으로 사용자 검사를 통한 악성코드 예방 필요

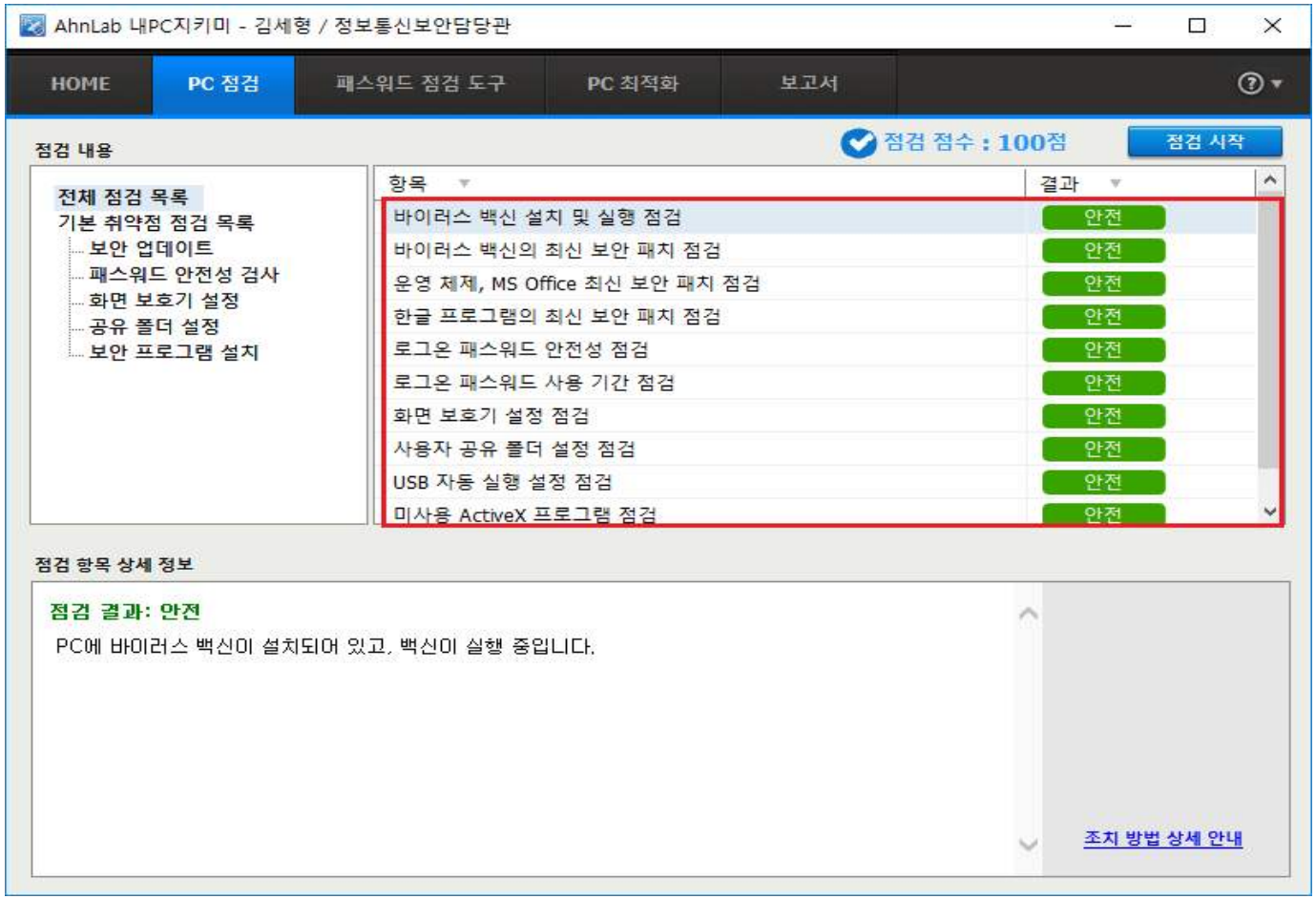
보안대책2. 업무용PC 보안강화

서울시 정보통신 보안업무 처리지침

제13조(PC 등 단말기 보안관리)
② 정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 단말기 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.
1. 장비(CMOS 비밀번호)·자료(문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용하고 지문인식 등 생체인식 기술 적용 권고
2. 10분 이상 PC 등의 작업 중단시 비밀번호 등이 적용된 화면보호 조치
3. PC용 최신 백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 운영체제(OS) 및 응용프로그램(아래아한글, MS Office, Acrobat 등)의 최신 보안 패치 유지
4. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제

"내PC지키미"를 통한 업무용PC보안 점검&조치

보안대책2. 업무용PC 보안강화



「사이버보안 진단의 날」을 시행하여(매월 셋째 주 수요일) 정해진 점수(90점)를 만족하지 못하는 경우 인터넷 사용 차단

보안대책3. 외부저장매체 이용 차단

서울시 정보통신 보안업무 처리지침

제21조(휴대용 저장매체 보안대책)
① 휴대용 저장매체 관리책임자는 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위·변조, 훼손, 분실 등에 대비한 보안대책을 강구하여 정보보안담당관의 승인을 받아야 한다.
② 휴대용 저장매체 관리책임자는 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.
③ 휴대용 저장매체 관리책임자는 USB 관리시스템을 도입할 경우 국가정보원장이 안전성을 확인한 제품을 도입하여야 한다.

- 이하 생략 -

"보안USB 프로그램"을 이용한 외부저장매체 차단

보안대책3. 외부저장매체 이용 차단

- 보안USB 정책에 따라 CD/DVD, USB, 무선랜 등 외부 저장매체에 대한 사용 금지
  : 필요한 경우 담당자에게 승인을 받은 다음 이용 가능
- 부서별 보안USB를 통한 중요 자료 이용 가능

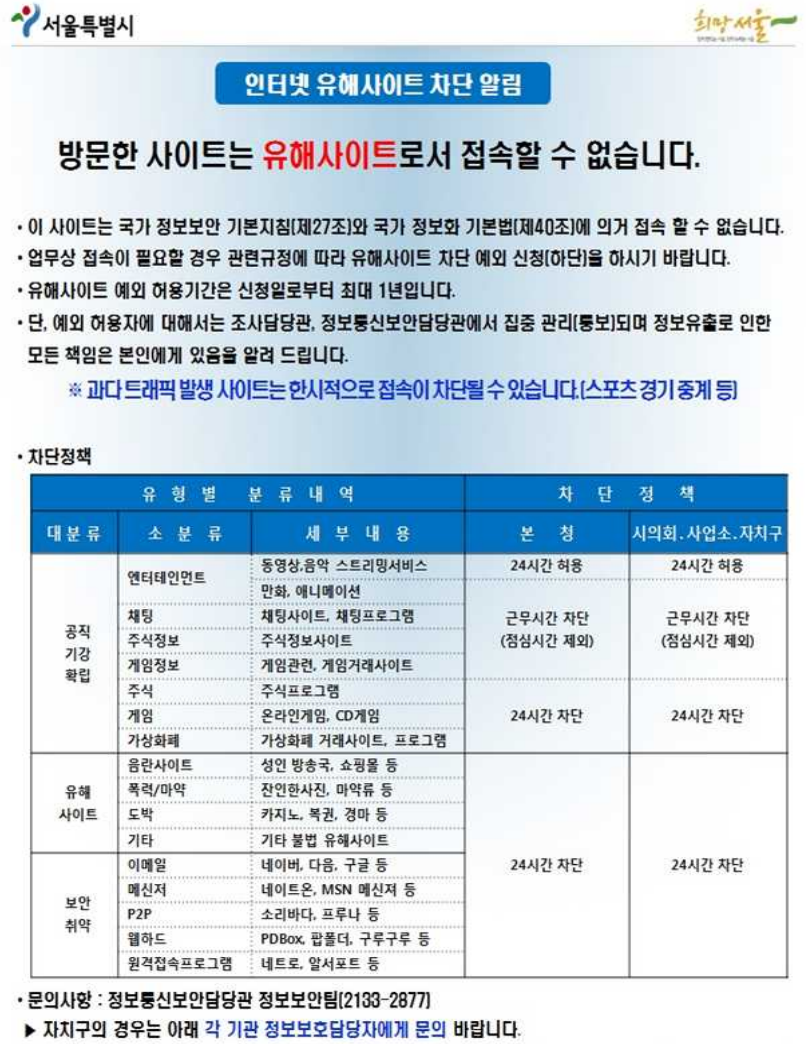
보안대책4. 비인가 사이트 접근 차단

서울시 정보통신 보안업무 처리지침

제14조 (인터넷PC 보안관리)
① 정보보안담당관은 인터넷과 연결된 PC(이하 "인터넷PC"라 한다)에 대하여 비인가자가 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.
3. 음란·도박·증권 등 업무와 무관한 사이트 접근차단 조치

제20조(전자우편 보안대책)
③ 사용자는 상용 전자우편을 이용하여 업무자료를 송·수신 할 수 없으며 기관 전자우편으로 송·수신한 업무자료는 활용 후 메일함에서 즉시 삭제하여야 한다.

"유해사이트 차단 시스템"으로 비인가 사이트 차단



서울특별시 희망서울

인터넷 유해사이트 차단 알림

방문한 사이트는 유해사이트로서 접속할 수 없습니다.

- 이 사이트는 국가 정보보안 기본지침(제27조)와 국가 정보화 기본법(제40조)에 의거 접속 할 수 없습니다.
- 업무상 접속이 필요할 경우 관련규정에 따라 유해사이트 차단 예외 신청(하단)을 하시기 바랍니다.
- 유해사이트 예외 허용기간은 신청일로부터 최대 1년입니다.
- 단, 예외 허용자에 대해서는 조사담당관, 정보통신보안담당관에서 집중 관리(통보)되며 정보유출로 인한 모든 책임은 본인에게 있음을 알려 드립니다.

※ 과다트래픽 발생 사이트는 한시적으로 접속이 차단될 수 있습니다.(스포츠 경기 중계 등)

- 차단정책

유형별 분류내역			차단정책	
대분류	소분류	세부내용	본청	시의회.사업소.자치구
공직기강 확립	엔터테인먼트	동영상,음악 스트리밍서비스	24시간 허용	24시간 허용
		만화, 애니메이션	근무시간 차단 (점심시간 제외)	근무시간 차단 (점심시간 제외)
	채팅	채팅사이트, 채팅프로그램		
	주식정보	주식정보사이트		
	게임정보	게임관련, 게임거래사이트		
	주식	주식프로그램	24시간 차단	24시간 차단
	게임	온라인게임, CD게임		
	가상화폐	가상화폐 거래사이트, 프로그램		
유해사이트	음란사이트	성인 방송국, 쇼핑몰 등	24시간 차단	24시간 차단
	폭력/마약	잔인한사진, 마약류 등		
	도박	카지노, 복권, 경마 등		
	기타	기타 불법 유해사이트		
보안취약	이메일	네이버, 다음, 구글 등		
	메신저	네이트온, MSN 메신저 등		
	P2P	소리바다, 프루나 등		
	웹하드	PDBox, 팝폴더, 구루구루 등		
	원격접속프로그램	네트로, 알서포트 등		

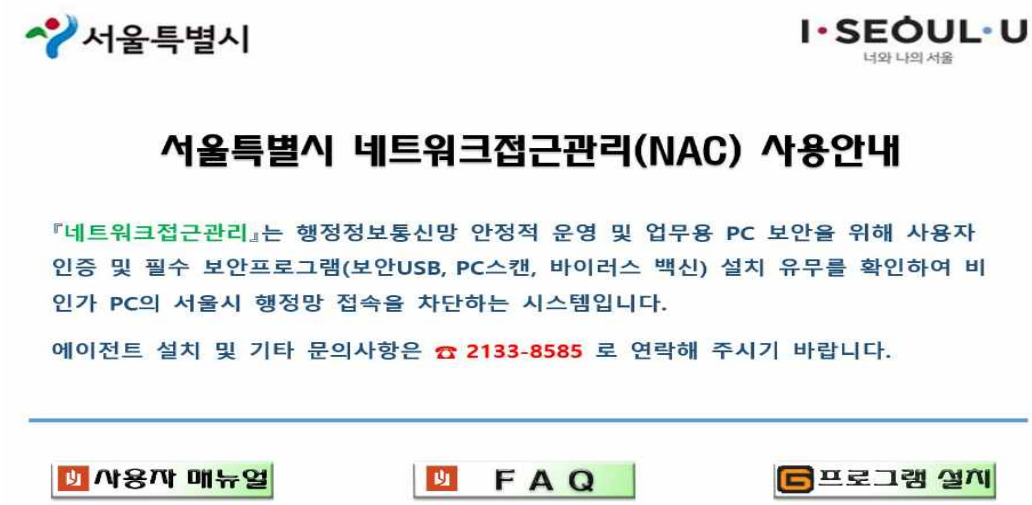
- 문의사항 : 정보통신보안담당관 정보보안팀(2133-2877)
  ▶ 자치구의 경우는 아래 각 기관 정보보호담당자에게 문의 바랍니다.

보안대책5. 비인가 노트북 등 이용 차단

서울시 정보통신 보안업무 처리지침

제19조(업무망 보안관리)
① 시장은 업무자료를 소통하기 위한 업무망 구축시 인터넷과 분리하도록 망을 설계하여야 한다. 이 경우 다음 각 호의 보안대책을 강구하여 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.
2. 비인가 장비의 업무망 접속 차단대책(네트워크 관리시스템 등)
③ 업무망 관리자는 정보시스템에 부여되는 'IP주소'를 체계적으로 관리하여야 하고, 비인가자로부터 업무망을 보호하기 위하여 사설주소체계(NAT)를 적용하여야 한다. 또한, IP주소별로 정보시스템 접속을 통제하여 비인가 정보통신기기나 PC등을 이용한 업무망內 정보시스템 접속을 차단하여야 한다.

"네트워크 접근관리 시스템"으로 비인가시스템 차단



악성코드 예방 & 정보보안 수칙

I·SEOUL·U
너와 나의 서울

악성코드 감염 예방 수칙

이렇게만 해도 악성코드 감염 및 피해를 최소화 할 수 있다

사전 예방 5대 수칙

1. 사용하는 모든 프로그램을 최신 버전으로 유지
2. PC, 스마트폰에 최신의 백신 프로그램 설치
3. 팝업 차단 기능 설정
4. e메일 주소 배포 자제 및 계정 패스워드 주기적 변경
5. 중요 자료는 정기적 백업 수행

정보보호 10대 생활수칙

1. 자동 업데이트 가능한 백신 소프트웨어 설치 및 실시간 감시기능 사용
2. 출처가 의심스러운 E-mail은 열람하지 말고 삭제
3. 운영체제(윈도우 등)에서 제공하는 자동업데이트 및 방화벽 기능 사용
4. 패스워드는 9자리 이상 특수문자를 포함하여 만들고 3개월마다 변경
5. 개인 컴퓨터에 부팅·로그인·화면보호기(10분) 패스워드 설정
6. 공유폴더 사용을 최소화하고 사용시 반드시 패스워드 설정
7. 신뢰할 수 있는 웹사이트에서 제공하는 프로그램 설치
8. 중요한 자료는 패스워드를 설정하여 네트워크에 연결되지 않은 PC에 저장
9. 비인가된 소프트웨어 사용을 금하고 정품 소프트웨어 사용
10. 중요한 자료는 메일을 통해 주고받지 말고 불가피한 경우 패스워드 설정

안전 이용 6대 수칙

1. e메일 수신 시, 발신자(이름, 계정 등) 및 제목 확인
2. 첨부파일 실행 및 링크 클릭시 주의
3. SNS 및 정부기관을 사칭하는 협박성 e메일 주의
4. 신뢰할 수 없는 사이트 방문 자제
5. 파일 공유 사이트에서 파일 다운로드 및 실행 시 주의
6. 모르는 사람이 작성한 게시글 및 단축 URL 클릭 금지

정보보안은 남이 해 주는 것이 아니라 내가, 우리가 하는 것!!!