나와 당신이 이어지며, 함께 공존하는 서울

I·SEOUL·U

2017년 하반기

정보보안 인식제고 교육

Action 정보보호

2017년 11월14일

순서

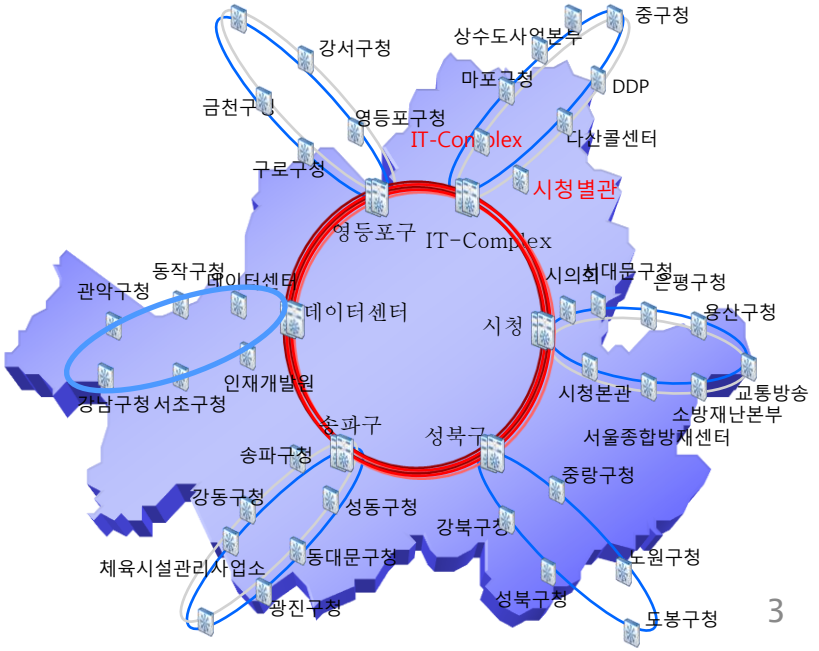
1. 전자정부 현황
2. 정보보호 실천
3. 보안사고 사례
4. 디지털 포렌식

서울특별시 전자정부 현황

시민이 상상하고, 서울이 실행하는
세계최고의 서울형 스마트시티

S플렉스센터 전경

- 인원 : 1,030명(구청577)
- S/W : 536종(공통-60종)
- 서버 :1,200대
- 정보통신망
  - e-SeoulNet
  - u-SeoulNet



서울시 사이버 보안 운영체계

정부/공공기관
- G-CERT(행안부)
- NCSC(국정원)
- 정부통합전산센터
- 경찰청 사이버

민간기관
- KISA
- ISAC
- CONCERT

서울시 정보통신보안담당관

사이버 안전센터

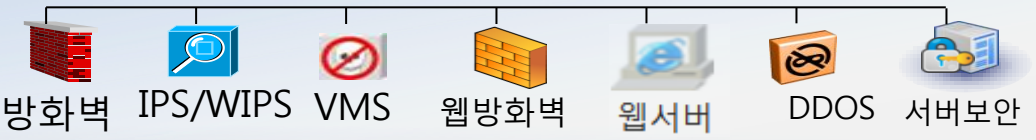
위협징후 탐지 | 통합보안 관제 | 종합보안 분석

전문업체
- 안랩
- 이글루시큐리티
- SK인포섹(주)
- ㈜윈스

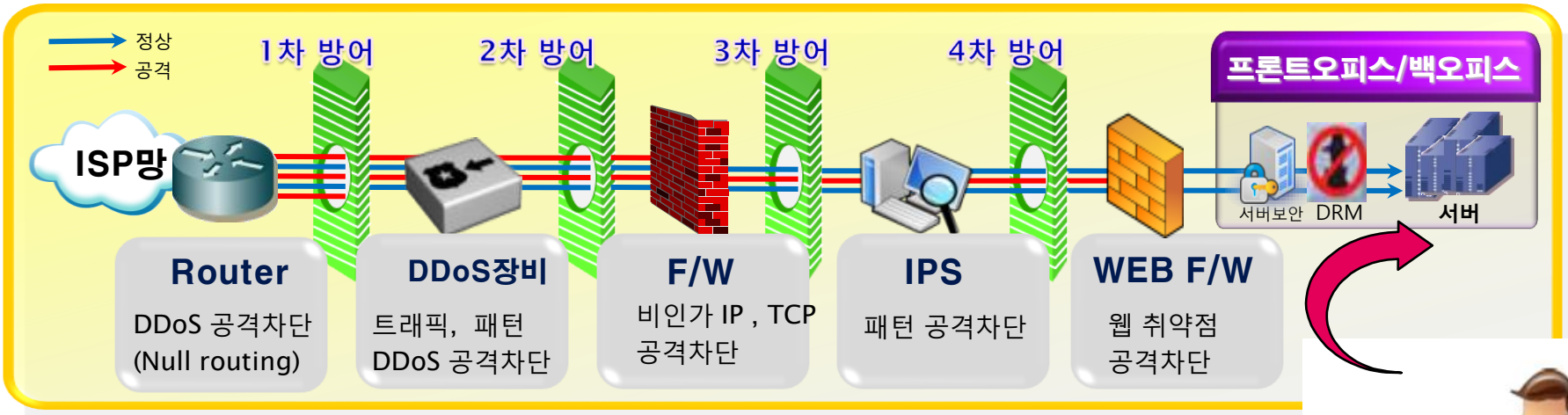
대외협력
- 대학교
- ETRI
- 한국정보보호협회

시 산하기관 , 25개 자치구, 기반시설(교통, 지하철, 수도, 가스 등)

보안관제 시스템



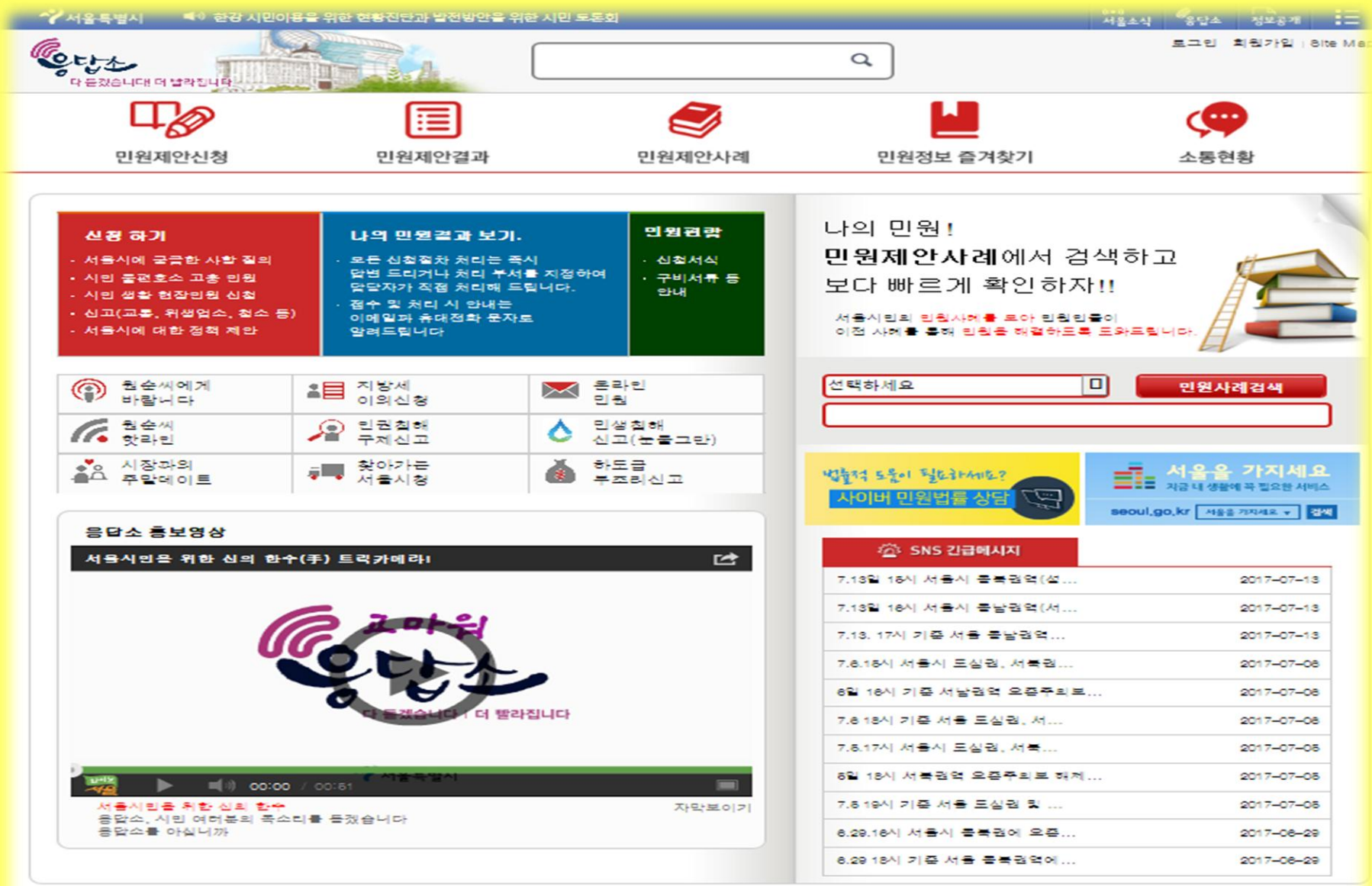
24시간 365일 보안관제



24시간 365일 보안관제

- 다단계 방어체계로 실시간 불법 침입 완벽 차단
- 웹해킹/악성코드는 민관, 군, 관 합동 공조대응
- DDoS 등 대규모 사이버테러 시 즉각 대응태세 유지

서울시 전자정부 평가 7회 연속 1위



전자정부 50주년 기념식(동영상)

2 정보보호 실천

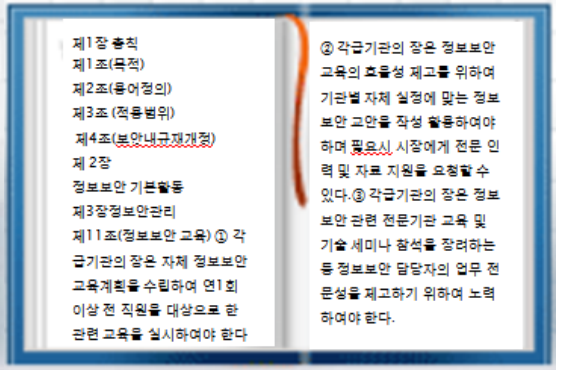
정보통신 보안업무 처리규칙

목 적

이 규칙은 「전자정부법」, 「정보통신기반보호법」 및 「국가 정보보안 기본지침」에 따라 서울특별시(이하 "시"라 한다) 각급기관이 수행하여야 할 정보통신 보안업무 전반에 관한 사항을 규정함을 목적으로 한다.

시행일

- 제정 및 시행일시 : 2014.1.23
- 서울특별시규칙 제 3949호
- 담당기관 : 서울시 정보통신보안 담당관

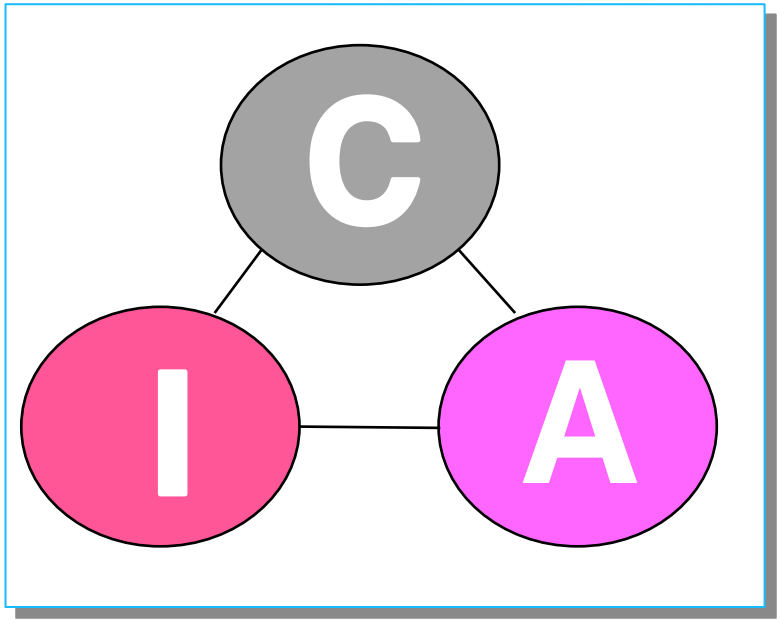

제1장 총칙
제1조(목적)
제2조(용어정의)
제3조 (적용범위)
제4조(보안내규제개정)
제 2장
정보보안 기본활동
제3장정보보안관리
제11조(정보보안 교육) ① 각 급기관의 장은 자체 정보보안 교육계획을 수립하여 연1회 이상 전 직원을 대상으로 한 관련 교육을 실시하여야 한다

② 각급기관의 장은 정보보안 교육의 효율성 제고를 위하여 기관별 자체 실정에 맞는 정보보안 교안을 작성 활용하여야 하며 필요시 시장에게 전문 인력 및 자료 지원을 요청할 수 있다.③ 각급기관의 장은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

내 용

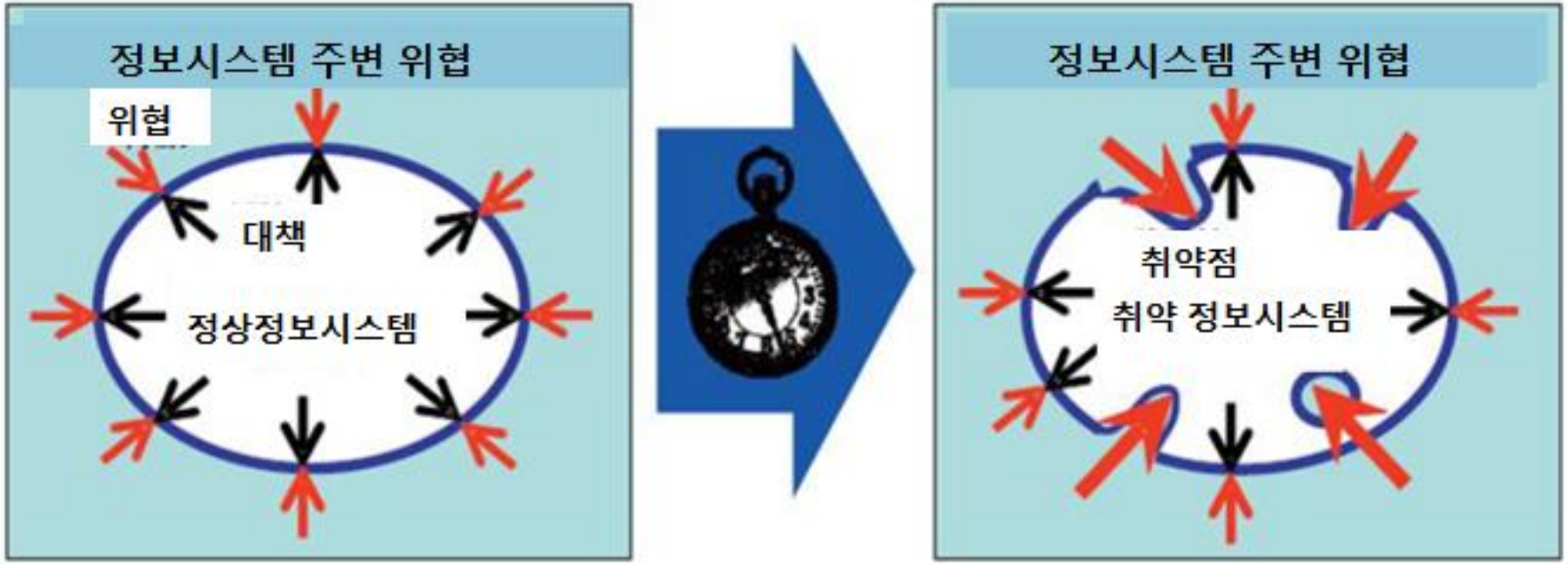
- 제1장 총칙: 제1조 (목적)~제4조(정보보안 내규 제. 개정
- 제2장 정보보안 기본활동 : 제11조(정보보안 교육) 제12조(보안진단의 날)
- 제3장 정보보안 관리 : 제24조 (pc관리)~제38조(정보자산 폐기)

정보자산 안전하게 지킨다

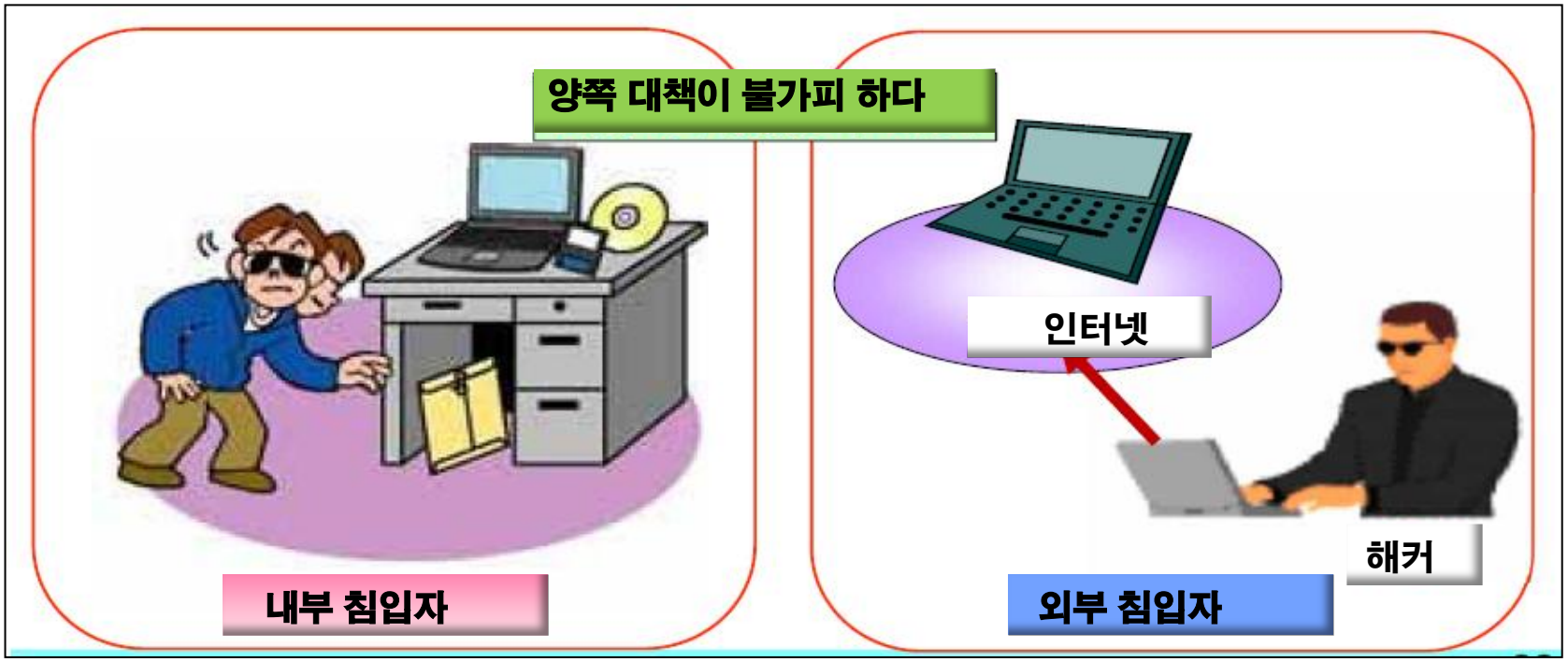


- 기밀성(Confidentiality): 허가된 사람만 정보시스템 접근 할 수 있도록 하는 것
- 무결성 (Integrity) : 보유하고 있는 정보가 정확하고 완벽한 상태를 유지하는 것
- 가용성 (Availability) : 권한자가 언제든지 정보에 접근 할 수 있도록 하는 것

정보시스템의 위협과 취약점



정보 자산의 정보유출 경로 ?



- 보안인식 부족, 직원의 부주의 등에 의한 사건 · 사고가 끊이지 않는다.
- 많은 사고는 평소의 정보 보안 의식강화로 막을 수 있다.

- 국가안보와 직결, 과다한 사회적 비용 발생
- 정부 또는 공공기관 신뢰성 실추

나의 PC는 안전한가 ?

인증
- NAC
- SSO
- IP관리(인터넷차단)

내PC지키미

자료유출방지
- 개인정보암호화
- 보안USB
- DRM(행정자료)

보안
- V3
- IPS
- 유해차단
- 방화벽
- DDoS차단

메일보안
- 스팸차단

- 외부로부터 해킹, 바이러스 유포방지 실시간 차단
- 내부직원 유해사이트 차단 접근, 불법 자료유출 실시간 모니터링

PC 보안관리 어떻게 ?

정보통신보안업무처리규칙 제24조 (PC 등 단말기 보안관리)

- 운영체제 및 프로그램 최신버전 업그레이드 유지
- 비밀번호 정기적으로 변경
- 화면보호, 부재 시 컴퓨터 절전 및 비밀번호 설정
- 백신프로그램, 불필요한 파일 삭제 등 pc 최적화 유지

주의사항

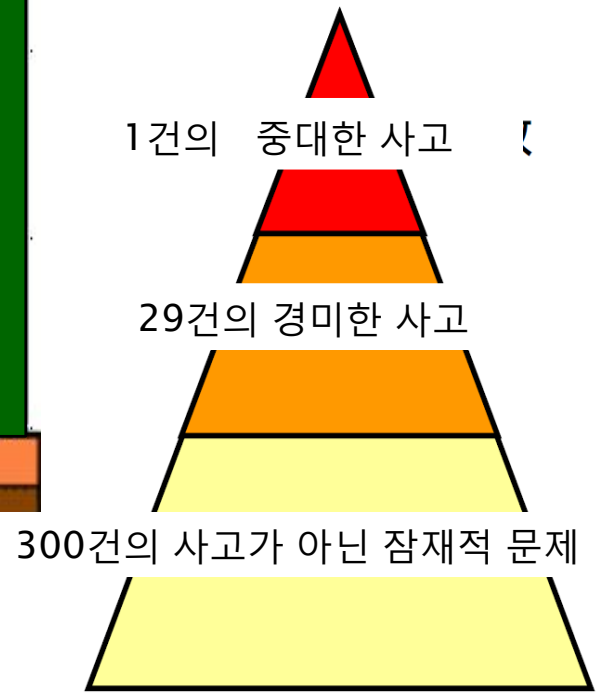
- PC, 인터넷 사용시 사용자 기록(log로그)이 남아 있어,
- 스푸핑(Spooing)경우 본인이 처리한 것처럼 기록되기 때문에 경우에 따라서는 해킹혐의를 받을 수 있다.

e-mail 보안관리

정보통신보안업무처리규칙 제32조
(전자우편 보안대책)

- 메일 보내기 전 육안으로 대상 주소확인
- 중요 메일 송신 시 첨부화일 패스워드사용
- 공무수행 관련업무 사적 메일 사용금지
- 메일의 첨부파일이 자동 실행되지 않도록 설정
- 첨부파일 다운로드 시 백신으로 악성코드 검사 실시
- 주소지 불분명한 의심메일 열람 금지

Heinrichs law



✓통합보안관제센터에 신고하여야 한다. (신고메일 : scert@seoul.go.kr)

휴대용 저장매체 보안관리

정보통신보안업무처리규칙 제33조
(휴대용 저장매체 보안대책)

- 업무자료 보관 시 위변조, 훼손, 분실 등에 대비한 보안대책 수립
- 비밀자료가 저장된 휴대용 저장매체는 비밀등급 및 관리번호 부여 비밀관리기록부에 등재 관리 한다
- 파기 등 불용처리, 비밀용을 일반용 다른 등급의 비밀용으로 전환시 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용

※ 정보보안담당관은 주기적으로 미 등록 매체 사용 여부 등 보안관리실태 점검하여야 한다.

바이러스 예방 관리 ?

정보통신보안업무처리규칙 제34조
(악성코드 감염 방지대책)

- 인터넷 (네트워크)의 Web 사이트
- 전자 메일 첨부파일 통해 전파
- USB 메모리 등의 외부 저장 매체
- 네트워크로 부터 직접 공격에 의한 감염

주의사항

- PC 바이러스 백신 소프트웨어를 탑재
- 이상한 Web 사이트, 의심스러운 메일 억제한다
- 바이러스 백신 자동 업데이트 실시한다
  - 실시간 방어체계로 운영

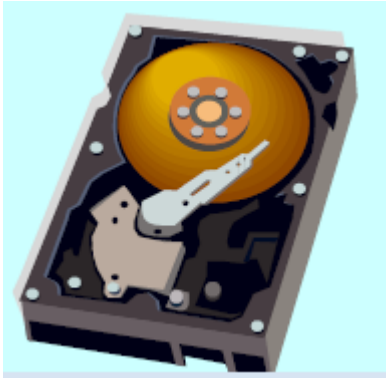
※ 백신 소프트웨어 과신은 금물 , 어디 까지나 사전 예방을 위한 소프트 웨어임
※ 백신은 예방 의학이며, 만병 통치약이 아님을 명심

전자정보 저장매체 불용처리(제38조)

정보기기 폐기

- 중요한 정보가 있는 PC 저장매체
- 폐기 경우 소거 전용 소프트 활용(1회이상포맷)
- 전문업체 의뢰 정보기기가 폐품 후

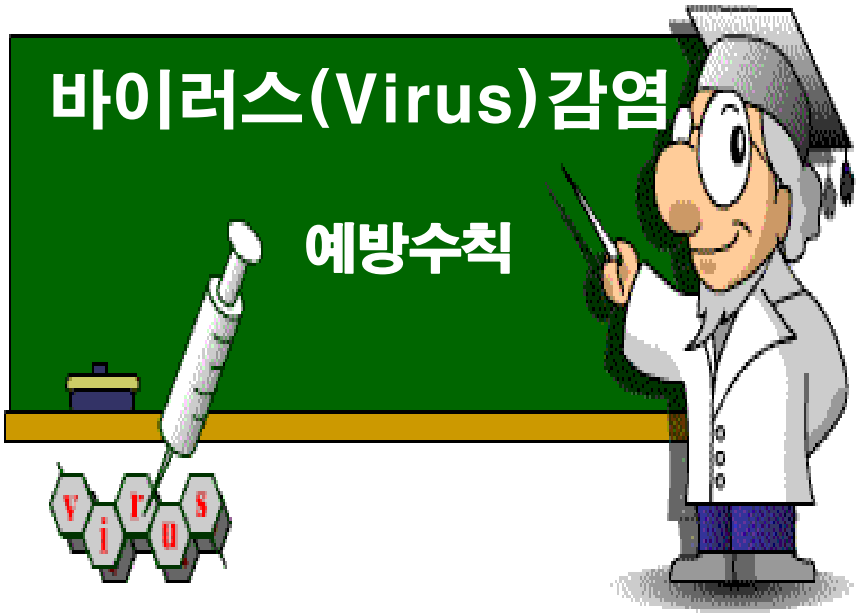
  전자데이타를 읽을 수 없도록 한다.



주의사항

- CD / DVD는 구부려 파쇠한다
- USB 메모리 등 플래시 메모리,
- PC 용 HDD도 파일 삭제 소프트웨어를 사용하거나
- 정보기기 파쇄 전문업체에게 의뢰한다.
- FAX, 복사기도 요주의! 버릴 때는 전문업체의뢰
- 디지털 카메라, 휴대 전화, PDA 단말기 데이터 삭제

바이러스 예방대책 ?



1. 백신프로그램은 ?
   최신판으로 업 데이트 한다
2. 메일 첨부화일은 ?
   먼저, 바이러스 검사한다
3. 다운로드 받은 화일은 ?
   먼저, 바이러스 검사한다
4. 응용프로그램은 ?
   익스프로 보안기능을 활용한다
5. 보안패치는 ?
   수시로 업데이트 한다
6. 바이러스 징후 ?
   놓치지 않는다
7. 만일대비 데이터는 ?
   반드시 백업하여야 한다

스마트 폰 보안사고

스마트폰 보안사고

- 단말기 도난, 분실, 무선 LAN WiFi 서비스
- 악성 코드 감염으로 인한 피해
- 권한 정보에 대한 액세스 권한
- 보안 응용 프로그램에 대한 제한
- 비공식 Site 앱의 입수 경로
- 정보 절취 목적 등의 악성 앱
- 공식사이트에서 이용자 정보 과도한 정보수집

스미싱(Smishing) 이란?

스미싱(smishing)은 문자메시지(SMS)와 피싱(Phising)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량으로 전송 후 이용자가 악성 앱을 설치하도록 유도하여 금융정보 등을 탈취하는 신종 사기수법입니다

급증하고 있는 스마트폰 Virus

출처 : AV-TEST
http://www.av-test.org/en/tests/mobile-devices/android/

Last update 2017.10.20

The best antivirus software for Android

AV-TEST Product Review and Certification Report – Sep/2017

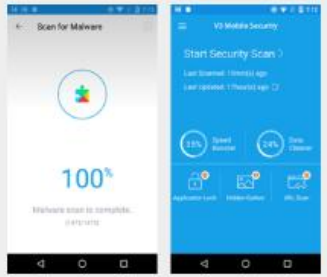
AhnLab

Version	3.1
Platform	Android 6.0.1
Report	173501
Date	Sep/2017

AhnLab

V3 Mobile Security

During September 2017 we evaluated 21 mobile security products for Andr
settings. We always used the most current version of all products for the te
to update themselves at any time and query their in-the-cloud services. We
detection and usability, including performance and false positives. Products

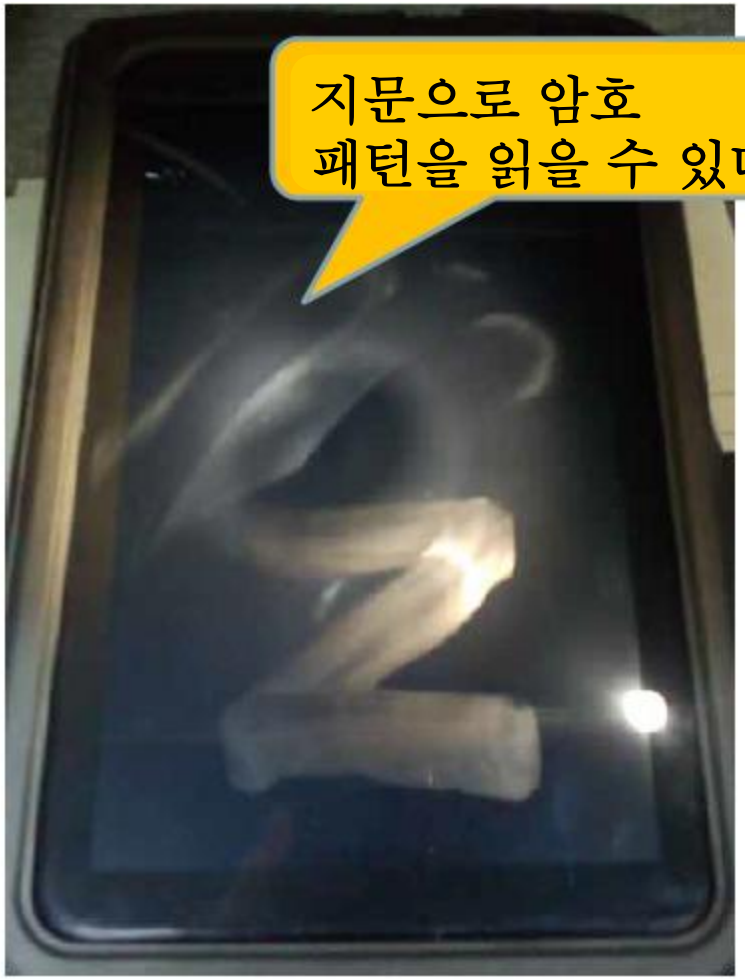


Detection of the latest Android malware in real-time 3,016 samples used	99.8%	95.7%
Detection of the latest Android malware discovered in the last 4 weeks 2,917 samples used	100%	98.4%
Protection Score	●●●●●●	**6.0/6.0**

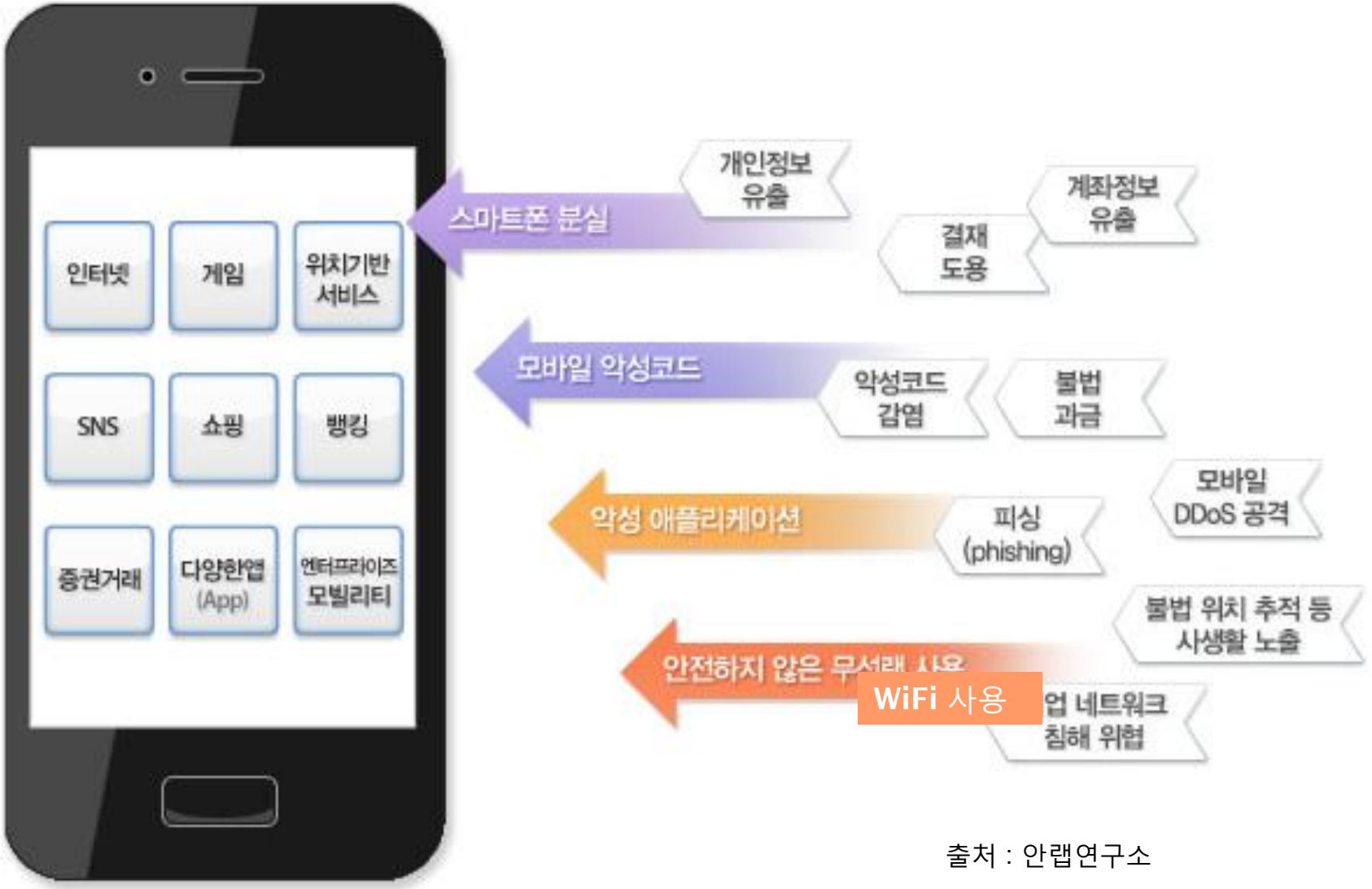
	September	Industry average
Performance: The app does not impact the battery life	✓	
Performance: The app does not slow down the device during normal usage	✓	
Performance: The app does not generate too much traffic	✓	
False warnings during installation and usage of legitimate apps from Google Play Store 2,006 samples used	0	0
False warnings during installation and usage of legitimate software from third party app stores 937 samples used	0	0
Usability Score	●●●●●●	**6.0/6.0**

스마트폰 취약점 예시

Android



스마트폰 보안 위협 요인



출처 : 안랩연구소

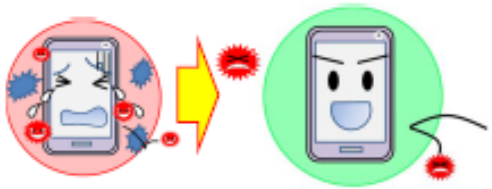
스마트폰을 안전하게 사용 할려면 !!!

AhnLab V3 Mobile Plus
(개발: Ahnlab)

알약 안드로이드
(개발: 이스트소프트)

I OS업그레이드

스마트폰 OS 업데이트 필요함
기존OS사용은 바이러스 감염 취약성 높아, 업그레이드 통지 즉시 설치



II 전용백신 사용

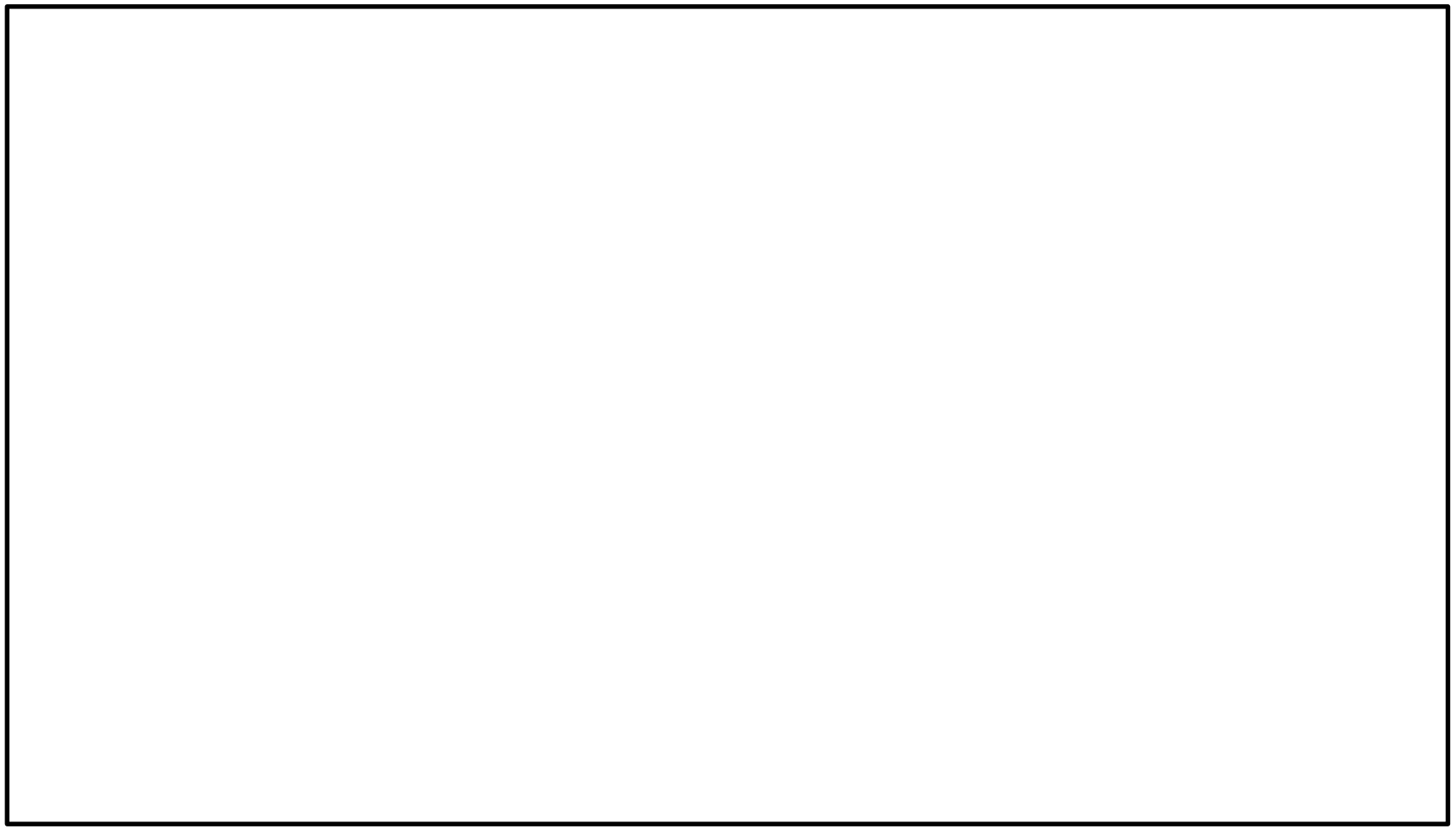
바이러스 혼입된 앱 스마트폰은 휴대전화회사 모바일 전용 바이러스 백신 설치 한다

III 앱 다운로드 시 주의점

OS 제공사업자와 이통사 등이 안전심사를 실시하는 앱 프로그램만 사용토록 하여야 한다
앱설치시 프로그램 기능과 제한 사항을 확인 한다

3 피해사례

랜섬웨어 피해 방송보도(2017.5)



랜섬웨어란(Ransomware)?

랜섬웨어 = 몸값 + 소프트웨어

시스템을 잠그거나 데이터를 암호화 하여 사용할 수 없도록 하고 이를 인질로 금전요구 하는 악성 프로그램

KISA 자료인용

표적형공격 정보유출

IPA자료인용

- 공공기관 기밀문서 유출(2016년)
- 대기업 고객 개인정보유출(2016년)

디지털 포렌식

디지털포렌식(Digital Forensic) ?

Forensic

Conventional

실생활의 범죄 현장 증거 수집/ 분석

- 지문/혈흔/족적/성문
- DNA
- 문서/인장/필적감정
- 알리바이(alibi)

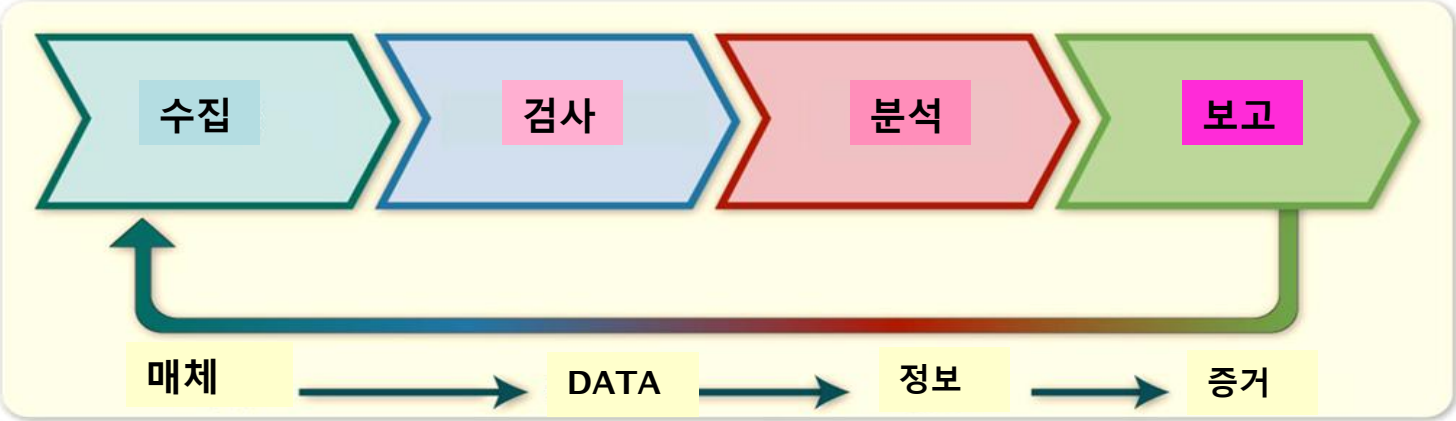
Digital

컴퓨터 등 디지털기기와 네트워크상 전송되는 디지탈자료를 적법한 절차와 과학적 기법을 사용하여 수집 분석하여 증거로 제출하는 제반 행위

- pc, 노트북, 하드디스크, USB
- 네트워크, 인터넷사용기록
- 전자우편, 악성코드,
- 데이터 베이스
- CCTV
- 스마트폰

Digital Forensic 절차

2016년5월19일 형사소송법 제313조 개정 ,진정성 성립 시 증거능력 인정



데이타의 무결성을 유지하면서 관련 데이터 기록, 소스로 부터 취득 후 라벨링

⇩

수집 데이터를 자동방법, 수동기법 조합으로 법의학의 처리 주목할 만 데이터 추출

⇩

법적으로 정당하다고 인정되는 기술 및 기법사용 분석 의문해결 유용한 정보 추출

⇩

분석결과 추정을 배제하고 사실관계 증명 위한 수집절차, 방법, 분석사용된 TOOL

출처 : 미국국립표준기술연구소 Special Publication 800-86

개인 PC데이터 보전방법 절차도

조사대상 PC

HDD
원본

추출

포렌식
전용기기

이미지
카피

증거보전용
HDD(사본)

증거분석용
HDD(사본)

삭제된 영역이나 미 사용영역을 포함한
HDD 내의 데이터를 완전 복사한다

복사원본 HDD	삭제 영역	사용영역	삭제 영역	미사용 영역	동일성 검증
		완전복사			
복사사본 HDD	삭제 영역	사용영역	삭제 영역	미사용 영역	

맺음말