

Smart Korea 強國 도약을 위한
스마트 모바일 시큐리티 종합계획

2010. 12



방송통신위원회
KOREA COMMUNICATIONS COMMISSION

< 개 요 >

「스마트 모바일 시큐리티 종합계획」은 방송통신위원회가 미래 모바일 서비스·인프라 보안 품질 향상, 모바일 이용자 프라이버시 보호 확립, 모바일 정보보호 기반 조성 등 3대 분야 10대 중점과제 추진을 통해 우리나라 모바일 인터넷 분야의 보안수준을 선제적으로 업그레이드하고자 마련한 중장기('11~'15년) 계획입니다.

국내 스마트폰 가입자 수는 '10년 11월말 기준 625만 명(휴대폰 가입자의 12%)으로 '13년에 3천만 명을 돌파하고 '15년에는 4천만 명에 이를 것으로 예상되는 등 향후 스마트폰, 스마트패드(태블릿PC) 등 다양한 스마트 기기를 활용한 스마트 라이프가 가속화되어 '스마트사이어티' (Smartciety)가 본격적으로 도래할 것으로 예상됩니다.

※ '스마트사이어티'(Smartciety, Smart+Society): 스마트폰 등 각종 스마트기기로 대화와 소통이 이루어지고 업무처리, 학습, 의료진료 등 사회 전반에 스마트기술이 활용되는 사회를 지칭

이러한 유선에서 모바일 인터넷으로의 패러다임 전환은 서비스의 진화 및 생활패턴의 변화뿐만 아니라, 새로운 보안위협이 출현도 함께 야기하고 있습니다. 모바일 단말을 기반으로 한 SNS, LBS 등의 신규서비스 활성화로 개인 정보가 상시 수집, 분석, 이용 가능해 지면서 프라이버시 침해에 대한 사회적 우려가 증가하고 있으며, 개방형 플랫폼, 신규 컨버전스 서비스 등의 등장으로 예측하기 어려운 신규 보안 이슈들이 계속 제기되고 있습니다.

이에 방송통신위원회는 향후 3천만 스마트폰 이용자 시대를 맞이하여 잠재적 보안위협에 선제적으로 대비하고, 글로벌 모바일 보안시장에서의 국가 경쟁력을 확보하기 위한 선행적 보안대책을 준비하였습니다. 금년 상반기부터 '스마트폰 정보보호 민·관 합동대응반'(1월), '모바일 시큐리티 포럼'(4월), '미래융합 IT서비스 보안연구회'(5월) 등을 구성·운영해 오면서, 산·학·연·관 전문가들의 활발한 토의 및 자문을 거쳐 「스마트 모바일 시큐리티 종합계획」을 수립(2010.12.24)하였습니다.

방송통신위원회는 금번 「스마트 모바일 시큐리티 종합계획」 마련으로 향후 발생 가능한 보안위협에 사전 대비하여 침해사고에 의한 사회적 비용을 최소화 하는 동시에, 안전하고 신뢰할 수 있는 모바일 서비스 이용 환경을 구축함으로써 국민들의 삶의 질 향상에 크게 기여할 수 있을 것으로 기대합니다. 앞으로 방송통신위원회는 본 종합계획의 내실 있는 추진을 통하여 우리나라가 스마트 모바일 보안강국으로 도약할 수 있도록 더욱 노력하겠습니다.

Smart Korea 強國 도약을 위한 스마트 모바일 시큐리티 종합계획[요약]

2010. 12.

1. 추진배경

□ (모바일 단말의 확산) 국내 스마트폰 가입자 수는 '10년 11월말 기준 625만명(이동통신가입자의 12%)으로 금년 말까지 700만명 상회 예상

○ 국내 스마트폰의 누적 가입자는 '13년까지 3천만명을 돌파하고 '15년에는 4천만명에 이를 것으로 전망 (KISDI·KCC, '10.11월)

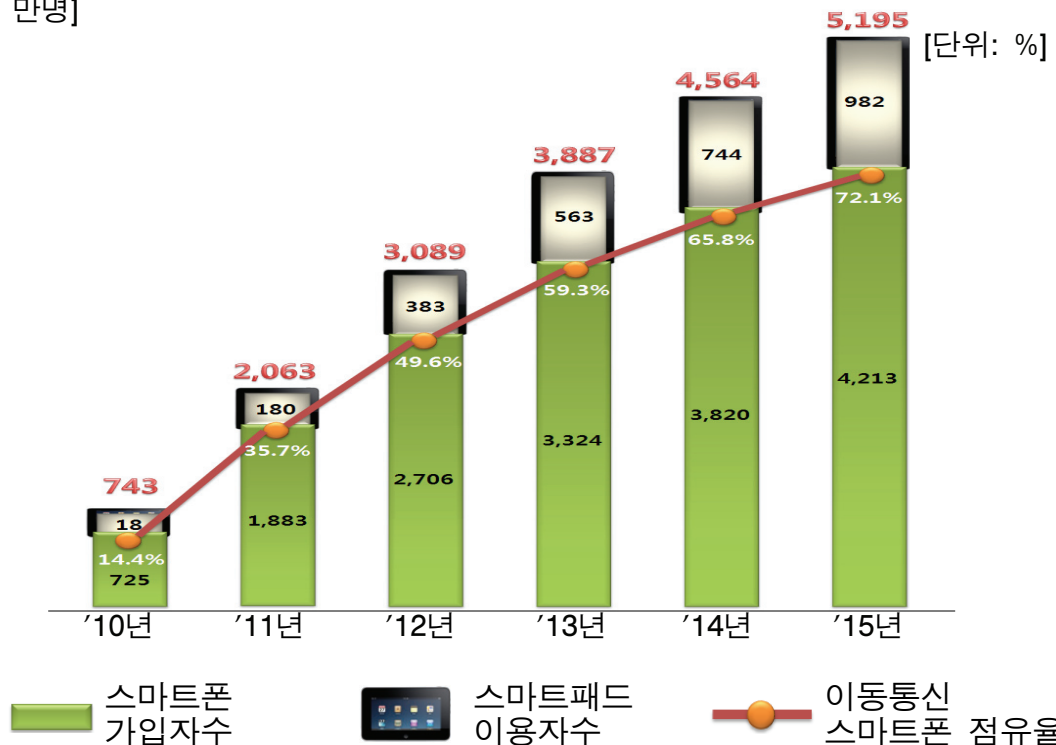
○ 스마트패드(태블릿PC) 이용자도 '10년 18만명에서 '15년 약 982만명으로 증가 예상 (KISDI·KCC, '10.11월)

⇒ 향후 스마트폰, 태블릿PC 등 다양한 스마트기기를 활용한 스마트 라이프의 가속화로 '스마트사이어티(Smartciety)'가 도래

※ '스마트사이어티'(Smartciety, Smart+Society의 합성어) : 스마트폰 등 각종 스마트 기기로 대화와 소통이 이루어지고 업무처리, 학습, 의료진료 등 사회 전반에 스마트기술이 활용되는 사회를 지칭 (방통위 금번 종합계획에서 처음 사용)

【 국내 스마트폰 및 스마트패드 (누적) 보급 전망 ('10~'15년) 】

[단위: 만명]



※ 출처 : 'Mobile voice and data forecast pack: 2010 - 15' OVUM(2010.5) 및 '2010 국가 정보화백서(NIA, 10.7월)' 기반으로 KISDI·KCC 예측 ('10.11월)

- **(모바일 시큐리티 위협)** 그러나 모바일 인터넷으로의 패러다임 전환은 서비스 진화 및 생활패턴의 변화와 함께 신규 보안위협이 출현도 야기
- SNS, LBS 등 모바일 단말 기반의 신규서비스 활성화로 개인정보가 상시 수집, 분석, 이용 가능해지면서 프라이버시 침해에 대한 우려 증가
 - 복합단말, 개방형 플랫폼, 신규 컨버전스 서비스의 등장으로 예측하기 어려운 신규 보안 이슈들이 계속 등장할 것으로 예상
 - 특히, 모바일 분야의 보안위협은 모바일 단말, 무선네트워크 및 모바일 기반 신규서비스, 융합 콘텐츠 등 4대 영역별로 구분 가능

【 모바일 4대 영역별 보안위협 】



- **(모바일 정보보호 시장의 확대)** '10년 국내 정보보안 시장규모는 9,179억원 (예측치)이며 그 중 모바일 보안시장은 약 57억원(0.6%) 차지 (KISIA, '09.12월)
- 국내 모바일 보안시장은 민간부문의 노력 및 정부의 보안정책 추진 등이 뒷받침되면, 시장의 급속한 성장세(연평균 206%)가 예상되어 '15년 약 2,078억원(12.9%)에 이를 전망
 - 세계 모바일 보안시장의 경우, 6년간('09~'15년) 2.2배 증가하여 '15년에 약 2,864백만 달러(약 3조원)가 될 것으로 전망(IDC, '10.5월)

- 향후 '3천만 스마트폰 이용자 시대'에 대비하여 안전한 모바일 인터넷 사회 구축을 위한 선행적인 준비가 필요한 시점
- 방통위는 급변하는 모바일 인터넷 환경에서 신규 보안위협에 선제적으로 대비하고 글로벌 모바일 보안시장을 선점하기 위해 중장기('11~'15년) 「스마트 모바일 시큐리티 종합계획」을 수립·추진

2. 비전 및 추진전략



3. 3대 추진분야 및 10대 중점과제

1. > 미래 모바일 서비스·인프라 보안품질 향상

① 신규 모바일 단말 보안 강화

- (모바일 백신 활성화 및 악성코드 점검 강화) 스마트폰 백신 신규 비즈니스 모델 발굴, 악성코드 점검 강화, 보안용 앱·솔루션 시험센터 구축 등
- (한국형 앱 게놈 프로젝트 추진) 앱의 기능적 특성, 보안위협 등의 분석을 통해 앱의 악성행위 여부를 파악하여 악성앱의 판단기준 마련 및 전용백신 개발 등에 활용

※ 美 모바일 보안업체 ‘룩아웃’, 약 30만개의 앱을 분석한 ‘앱게놈 프로젝트’ 추진(‘10.8월)

- (안전한 앱 유통 환경 조성) 스마트폰 앱에 대한 표준화된 검증 기준 및 절차를 마련해 이를 준수하도록 유도

※ 그린 마켓 인증서 : 앱에 대한 보안 검증 절차 및 가이드라인을 준수하고 지속적인 사후 관리를 수행하는 마켓을 선정하여, 신뢰할 수 있는 앱을 제공하는 마켓임을 정부가 인증

- (스마트패드 등 단말 보안 가이드라인 마련) 안전한 스마트 기기의 개발·보급을 위해 취약점 및 대응방법이 포함된 보안 가이드라인 마련

② 무선 네트워크 안전성 확보

- (무선랜 보안관리 강화 등) 무선랜 보안 표준모델 개발, 보안인식 제고 및 무선랜 보안 법제 개선 등

- 무선랜 보안운영 표준 모델에 기반한 공중 Wi-Fi존, 사설 무선랜 보안 운영 등의 주기적 점검

※ 현장 조사를 통해 무선 AP의 초기 패스워드 변경여부, 보안설정 여부, 인증, 암호화 지침 준수 여부 등을 점검

- (유·무선 연동구간 보안 연동체계 구축) DDoS 대응시스템 등 기존 유선망 중심의 보안체계를 무선망·IP 백본망 연동구간까지 확대

③ 신규 모바일 서비스·콘텐츠 보호

□ 모바일 오피스 보안 체계 마련

- (보안 가이드라인 개발·보급) 단말, 시스템, 법적 문제 등 스마트 워크의 보안 요소에 따른 정보보호 가이드라인의 개발 및 보급
 - 스마트워크의 원활한 추진을 위한 보안 기반 조성
- (법·제도 개선) 모바일 오피스 사업자의 법적책임 명확화와 이용자의 권익보호를 위한 관련 법제도 개선
 - 개인정보 제공 또는 위탁에 대한 통일된 법적 근거, 개인정보 유출·유실 시 배상방안 등에 대한 법적 기준 마련 등
 - 모바일 오피스를 구성하는 기술 및 제품의 보안성 평가 기준 마련 및 인증제도 개선
- (모범사례 발굴 및 확산) 보안성을 고려한 모바일 오피스 도입의 모범사례(Best Practice)를 발굴·홍보하여, 모바일 오피스 확산을 위한 기반 환경 조성

□ 모바일 SNS 보안 강화

- (SNS 정보유출 대응 법제 개선) 위치정보 등 개인정보 유출사고 사전방지를 위한 법제도 마련
 - 개인정보 수집시 개인정보 침해 위험성 사전 고지 및 수집동의 방안 마련 등
- (기술적 대응 방안 마련) 국내외 SNS 사업자와 협력하여 모바일 SNS의 취약점 보완을 위한 기술적 보호조치 강화
 - 단축(Short) URL을 악용한 악성코드 유포 및 피싱 사이트 유포 예방을 위하여 국내외 단축 URL 관련 정보 공유체계 구축 및 대응

□ 모바일 클라우드 보안체계 강화

- (모바일 클라우드 보안기반 마련) 이기종 플랫폼간 상호운용성 확보를 위한 통합인증 체계 구축 및 사고 원인 분석을 위한 ‘모바일 클라우드 포렌식’ 기술 개발
 - (서비스 표준화 및 대응체계 구축) 모바일 클라우드 서비스 이용자 보호를 위한 서비스·정책 표준화, 침해사고 대응능력 강화
 - 모바일 클라우드 서비스 유형, 정보의 민감도 등에 따라 차등화된 보안 서비스를 제공하기 위한 표준 SLA 가이드라인 마련
- ※ SLA(Service Level Agreement) : 서비스 수준 계약서
- 모바일 클라우드 서비스 제공자간 신종 위협정보 공유 및 신속 대응을 위한 침해대응체계 마련

□ 스마트 TV 보안 체계 구축

- (스마트TV 디바이스 보호체계 마련) 스마트TV 시스템 보호를 위한 스마트TV 기기의 취약점 분석 및 보안진단 체계 마련
- (콘텐츠 및 개인정보 보호방안 추진) 모바일 콘텐츠 특성에 따른 복제방지 솔루션 개발 지원 및 관리지침 마련

□ 모바일 뱅킹 보안 기반 조성

- (모바일 뱅킹 보안성 연구·개발) 신규 모바일 기기 출시에 따른 모바일 뱅킹서비스 보안성 연구 및 보안 취약성 분석기술 개발
- (보안가이드 개발 및 취약성 점검) 안전한 스마트폰 뱅킹 제공 및 이용을 위한 보안가이드 개발·보급
 - 금융당국과 공조하여 금융기관에서 제공하는 모바일 금융서비스의 안전성 및 보안취약성 점검 지원

2. 모바일 이용자 프라이버시 보호 확립

④ 모바일 개인정보 및 위치정보 보호 강화

- (관리책임 강화) 개인정보 암호화 등 보호수단 제공 및 관리책임 강화, 모바일 개인정보 유출사고 사전방지를 위한 법제도 마련
- (프라이버시 안전성 검증) 스마트폰 S/W 개발 및 휴대단말 제조 시 개인정보보호 가이드라인 제시, 앱 프라이버시 안전성 검증체계 구축
- (개인위치정보 자기제어시스템 구축) 위치정보사업자나 위치기반 서비스사업자로 하여금 이용자가 위치정보 사용내역을 확인할 수 있도록 하여 이용자의 자기 위치정보 통제권 강화

⑤ 모바일 스팸 방지 및 최소화

- (신규서비스의 스팸위험성 분석) SNS 등 신규서비스에서의 스팸 발생유형 및 취약점 분석, 법적·기술적 대응방안 선제적 연구
- (지능형 필터링 활용 확대) 스마트폰 등 모바일 전용 스팸신고 절차 간소화·간편화 및 지능형 스팸필터링 등 안티스팸 서비스 강화

⑥ 모바일 유해정보 유통 방지

- (유해정보 차단 앱 개발) 청소년들에게 모바일 기기를 통해 전파되는 유해정보를 차단할 수 있도록 앱 개발 및 설치 권고
※ 단말기 판매시 기본설정으로 유해정보를 차단하는 애플리케이션을 설치하여, 이용자의 연령에 따라 작동할 수 있는 조치 유도
- (앱 유해정보 모니터링 강화) 유통 중인 스마트폰용 앱의 유해성, 선정성 및 프라이버시 침해 여부 등 실태 조사

3. 모바일 정보보호 기반 조성

⑦ 모바일 보안기술 연구개발(R&D) 지원 확대

- (원천기술 개발) 모바일 보안의 공통기반, 단말·플랫폼, 무선망, 서비스, 콘텐츠에 대한 기초·원천 기술 개발에 집중 지원
 - 보안플랫폼(단말·플랫폼), 침해탐지·관제(무선망) 등 모바일 단말 및 인프라 보호를 위한 핵심 원천 기술 개발
 - 경량 암호(공통기반), 모바일 클라우드(서비스), 스마트 스크린(콘텐츠) 보안 등 스마트 모바일 서비스의 안전성 보장을 위한 기술 개발

⑧ 모바일 보안 시장 생태계 조성

- (모바일 보안 상생환경 조성) 모바일 보안업체와 단말 제조업체, 이통사간의 협력 어려움 타개 등을 위한 ‘(가칭)모바일 시큐리티 협의회’를 구성·운영
- (상용화 지원 강화) KISA, ETRI, 국보연 등 연구기관의 모바일 보안기술 개발 성과물에 대한 민간 이전 및 상용화 지원 강화
 - ‘(가칭)모바일 보안 상용화 지원센터’를 설립하여 보안제품 개발, 판매, 유지보수 등 전 단계에 이르는 통합 패키지형 지원 추진
- (표준화 및 해외진출 지원) 표준화를 통한 기업 간 과열경쟁·중복 투자 방지 및 홍보 로드쇼 개최 등 중소보안업체의 해외진출 지원
 - 산·학·연·관 협력으로 ‘모바일 보안표준 연구센터’를 설립하여 관련 기초 기술 확보 및 국내 기술의 글로벌 표준화 등 추진
- (모바일 보안 글로벌 핵심인재 양성) 우수 대학 대상으로 모바일 연구개발 인력 양성 지원 및 산업계, 국외 연구소와의 연계 교육 추진

⑨ 모바일 시큐리티 협력체계 구축 및 인식 제고

- (예방적 협력체계 강화) 스마트폰 등 각종 모바일 기기에 대한 침해 사고 예방·대응을 위해 정부, 민간기관간 공동협력체계 구축
- (모바일 보안분야 Think-Tank 육성·지원) 전문가그룹 지원을 통해 신규 모바일 위협 및 미래사회의 기술·사회·문화적 변화 분석
 - ※ 보안분야 연구 선도를 위해 국내 주요 연구기관 지원 및 상호협력 연구체계 구축
- (모바일 정보보호 문화 확산) 이통사, 제조사, 유관기관 등과 연계하여 다양한 모바일 디바이스 및 서비스를 활용한 인식제고 추진

⑩ 모바일 보안 법제 정비

- ‘(가칭)스마트 모바일 보안 법제연구회’ 구성·운영을 통해 스마트 기기, 신규 모바일 서비스의 안전한 이용 보장을 위한 법제도 개선 추진

4. 추진체계 및 재원계획

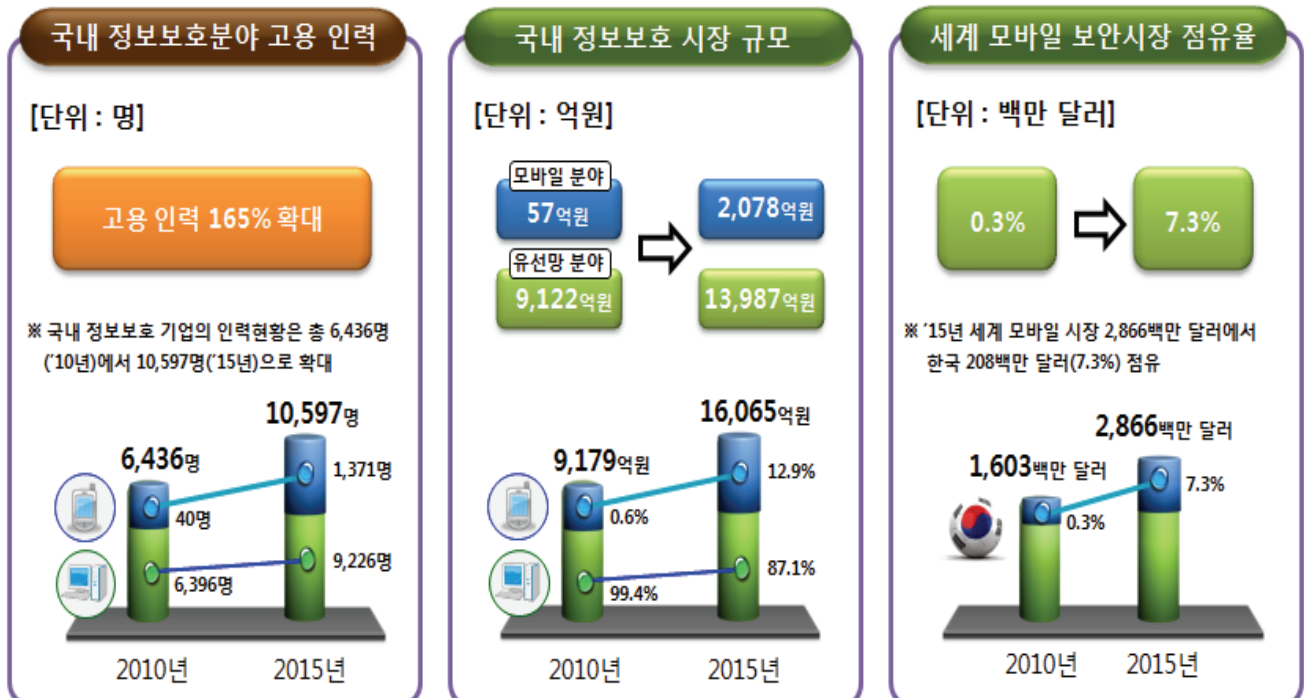
- (추진체계) 산·학·연·관의 주체별 역할 분담을 통한 유기적인 상호 협력 체계를 구축하여 「스마트 모바일 시큐리티 종합계획」 추진
- (재원계획) '11~'15년까지 정부·민간 부문의 예산확보를 통하여 약 998억원의 재원을 투입하여 종합계획을 추진
 - ※ 정부부문은 510억원(일반회계: 195억원, 기금: 315억원), 민간부문은 488억원
 - 정부예산은 방송통신위원회 소요제기 예산 기준이며, 기획재정부와의 협의 과정에 따라 변경될 수 있음
 - 민간부문 예산은 참여하는 업체 등의 사정에 따라 변동될 수 있음

5. 기대효과

- (미래 보안위협 감소) 향후 발생 가능한 보안위협에 대한 사전 대비로 침해사고 발생에 의한 미래 사회적 비용 최소화

- (안전한 모바일 사회 구현) 안전하고 신뢰할 수 있는 모바일 서비스 이용환경을 구축함으로써 국민들의 삶의 질 향상 기여
- (정책적 효과) 국가 정보보호 수준 업그레이드 및 신규 영역인 모바일 보안 분야의 개척을 통해 국가적 위상 제고
- (산업·경제적 성장 효과) 보안우려 해소와 함께 모바일 보안시장 활성화 촉진 및 산업경쟁력 제고, 신규 일자리 창출 효과 기대
 - 정보보호 분야의 전체 고용 인력은 '10년 6,436명 수준이나, 시장 확대를 통해 '15년 10,597명으로 '10년 대비 165% 일자리 확대
 - ※ 모바일 보안 종사자는 '10년 0.6%(48명)에서 '15년 12.9%(1,371명)를 차지 예상
 - 국내 모바일 보안시장은 '10년 57억원에서 '15년 2,078억원으로 확대되어, '15년 세계 모바일 보안시장의 7.3% 차지 전망

【 산업 · 경제적 기대효과 】



※ 출처 : [신규채용] KISIA('09.12월), [국내시장규모] 한국IDC('09.6월) 및 KISIA('09.12월), [세계시장점유율] IDC('10.5월) 기반으로 KISA 전망('10.11월)

Smart Korea 強國 도약을 위한 스마트 모바일 시큐리티 종합계획

2010. 12.

목 차

I. 추진 배경	1
II. 현황 및 전망	4
1. 모바일 인터넷 환경	4
2. 모바일 빅뱅과 정보보호	7
3. 모바일 시큐리티 위협	11
III. 비전 및 추진 전략	20
1. SWOT 분석	20
2. 비전 및 목표	21
3. 추진 전략 및 체계	22
IV. 주요추진과제	24
1. 미래 모바일 서비스·인프라의 보안품질 향상	24
① 신규 모바일 단말 보안 강화	24
가. 스마트폰 단말 보안 강화	24
나. 스마트패드 등 신규 기기 보안 대책 마련	28
② 무선 네트워크 안전성 확보	30
가. 무선랜 보안수준 제고	30
나. 유·무선 연동구간 보안성 강화	34
③ 신규 모바일 서비스·콘텐츠 보호	37
가. 모바일 오피스 보안 체계 마련	37
나. 모바일 SNS 보안 강화	40
다. 모바일 클라우드 보안 체계 강화	45
라. 스마트 TV 보안 체계 구축	48
마. 모바일 뱅킹 보안 기반 조성	52

2. 모바일 이용자 프라이버시 보호 확립	55
④ 모바일 개인정보 및 위치정보 보호 강화	55
가. 모바일 개인정보 보호	55
나. 모바일 서비스의 위치정보 보호	58
⑤ 모바일 스팸 방지 및 최소화	61
⑥ 모바일 유해정보 유통 방지	64
3. 모바일 정보보호 기반 조성	66
⑦ 모바일 보안기술 연구개발(R&D) 지원 확대	66
가. 단말 및 플랫폼 보호기술 개발	67
나. 모바일 인터넷 인프라 보호기술 개발	69
다. 스마트스크린 서비스 및 콘텐츠 보호 기술 개발	71
라. 모바일 클라우드 및 인프라 보호 기술 개발	73
마. 모바일 단말 적용을 위한 경량·저전력 암호/응용기술 개발	75
⑧ 모바일 보안 시장 생태계 조성	77
⑨ 모바일 시큐리티 협력체계 구축 및 인식제고	81
⑩ 모바일 보안 법제 정비	84
V. 추진 일정 및 주체, 소요 예산	86
VI. 기대효과	94
◇ 용어해설	96
◇ 부 록	105
I. 스마트폰 ‘이용자 10대 안전수칙’	
II. 스마트폰 정보보호 주체별 역할 (요약)	
III. 국내외 주요 모바일 악성코드 사례	
IV. 알기 쉬운 무선랜 보안 안내서	

I. 추진 배경

- 지난 10년간 인프라 구축 위주의 성장정책을 통해 세계 최고수준의 인터넷 이용환경을 조성했으며 이를 토대로 **모바일 인터넷시대** 도래
 - 스마트폰 등 각종 모바일 기기 활용이 증가하면서 인터넷 이용도 유선 중심에서 **무선 및 유·무선 통합** 환경으로 이동
 - 스마트폰, 스마트패드(태블릿PC), 스마트TV 등을 활용한 스마트워크, 모바일 클라우드 서비스 등의 등장으로 **스마트 라이프(Smart Life)** 가속화
 - ※ 스마트 라이프 : 스마트러닝(Smart-Learning), 스마트홈, 스마트카의 이용 등 ICT 융합기술의 실현으로 나타날 편리하고 효율적인 생활 모습을 지칭
- 유선에서 모바일 인터넷으로의 패러다임 전환은 IT서비스의 진화 및 생활패턴의 변화와 함께 **신규 보안위협**의 출현도 야기
 - 모바일 환경은 이종(異種)의 무선 인터넷접속으로 구성된 복잡한 구조와 한정된 네트워크 자원으로 인해 DDoS공격 등 침해위협에 취약
 - 모바일 단말에서의 LBS, SNS 등 서비스 특성에 따라 개인정보가 상시 수집·분석·이용되면서 **프라이버시 침해**에 대한 우려 증가
 - 복합단말, 개방형 플랫폼, 신규 컨버전스 서비스의 등장으로 예측하기 어려운 **신규 보안 이슈**들이 계속 등장할 것으로 예상
- 향후 모바일 인터넷은 무선 인터넷을 근간으로 모든 사물·기기가 연결되는 **사물지능통신(M2M)**으로 진화 예상
 - **Wi-Fi 인프라 확충, IPv6 전환, 4G통신 상용화** 등으로 모든 사물들이 **네트워크를 통해 자유롭게 연결**되는 시대 도래
 - ※ 사물지능통신(M2M) : 사람 對 사물, 사물 對 사물 간 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 융합 ICT 인프라

【 모바일 인터넷의 발전 단계 】



□ 따라서 향후 '3천만 스마트폰 이용자 시대'에 대비하여 안전한 모바일 인터넷 사회 구축을 위한 선행적인 준비가 필요한 시점

○ 급변하는 모바일 인터넷 환경에서 신규 보안위협에 대비하고 모든 국민이 안심하고 모바일 서비스를 이용할 수 있는 환경 조성

- 침해사고 발생에 따른 후속적 대응 위주에서 벗어나 발생 가능한 미래 모바일 침해 위협 및 사고에 대한 선제적 대응책 마련

※ 설계 단계부터 정보보호를 고려하면 주요 취약점의 80%가 감소되고, 운영 단계 이후 정보보호 비용의 60~100배 절감 (출처 : IBM시스템研, '09년)

○ 급증하는 국내 모바일 보안수요 충족 및 글로벌 보안시장 선점을 위해 혁신적 기술개발 유도 및 국내 모바일 보안산업 육성 지원

◆ 향후 도래할 3천만 스마트폰 시대의 안전한 Smart Mobile Life 촉진과 글로벌 모바일 보안시장에서의 국가경쟁력 확보를 위하여 중장기('11~'15년) 『스마트 모바일 시큐리티 종합계획』 수립·추진

종합계획 수립 추진 경과

- 금년 상반기부터 스마트폰 및 모바일 분야의 시큐리티 대응을 위한 다양한 협력체계를 구성·운영('10. 1월~)
 - 스마트폰 보안위협에 대한 선제적 예방 및 민·관 공동대응을 위해 「스마트폰 정보보호 민·관 합동대응반」 구성·운영(1월~)
 - ※ 대응반을 통해 '스마트폰 이용자 10대 안전수칙'(2월) 및 '주체별 역할방안'(7월)을 마련·발표하고, 국내 최초 스마트폰 악성코드(국제전화 무단발신)에 신속 대응(4월)
 - 잠재적인 모바일 보안위협 대응 자문을 위해 「모바일 시큐리티 포럼」(4월) 및 「미래 융합 IT서비스 보안연구회」(5월) 발족
- 모바일 전반에 대한 체계적·장기적 대책 수립을 위해 '스마트 모바일 시큐리티 종합계획(안)' 마련 추진('10. 5~11월)
 - 「모바일 시큐리티 포럼」, 「인터넷 정보보호 협의회」 등을 통해 종합계획 수립방향 정립(5~6월)
 - 종합계획 수립 전담반 구성·운영(6월~), 초안 완성(8월), 외부 전문가그룹 자문(9~10월, 총6회) 및 수정·보완
 - 「인터넷 정보보호 협의회」(11.26), 「모바일 시큐리티 포럼」(12.6), 「(위원장 주제) 모바일 보안업계 CEO 간담회」(12.13) 등을 개최하여 총체적 의견 수렴 및 보완
- 제77차 방송통신위원회 회의('10.12.24)에서 의결

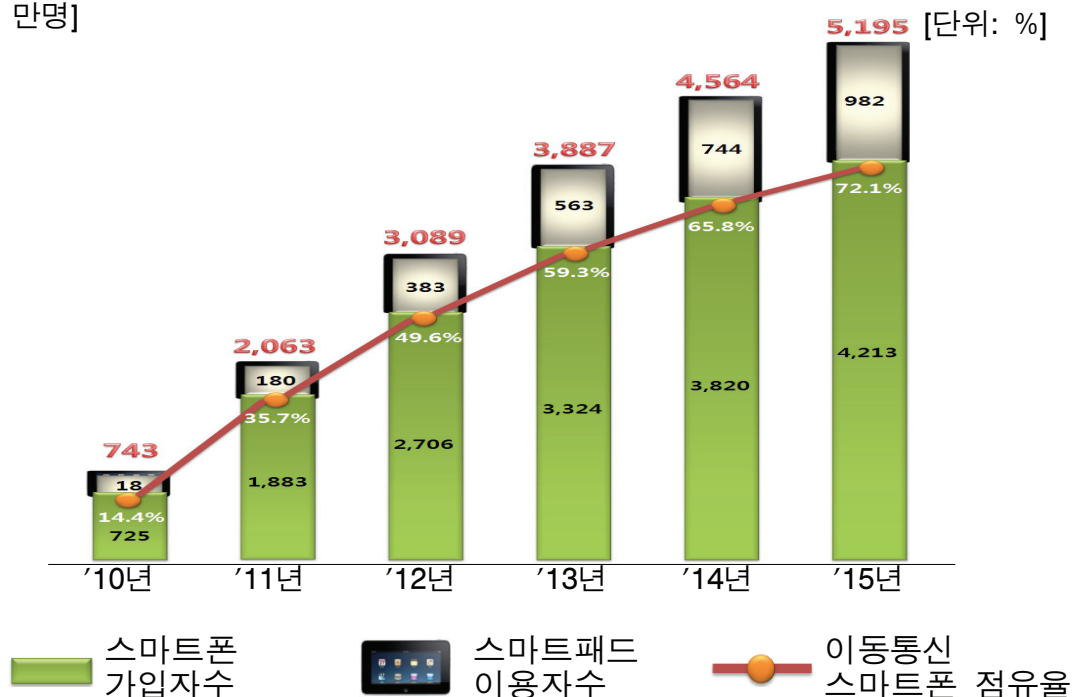
II. 현황 및 전망

1. 모바일 인터넷 환경

- (모바일 단말의 확산) 국내 스마트폰 가입자수는 '10년 11월말 기준 625만명으로 전체 이동통신 가입자의 12%를 차지
 - 금년 말까지 국내에는 700만대를 상회하는 스마트폰이 보급되어 이동통신 가입자의 약 14%를 차지할 것으로 예측
 - '13년에 국내 스마트폰 누적 가입자수는 3천만명을 돌파하고 '15년에는 4천만명을 넘어설 것으로 전망
 - 스마트패드(태블릿PC) 이용자도 디지털 멀티미디어 활용 증가로 인해 '10년 18만명에서 '15년 982만명으로 증가 예상
- ※ 스마트패드(Smart-pad) : 스마트폰, PC, 넷북 등의 장점을 갖춘 멀티미디어 디바이스로서 태블릿PC, 미디어 태블릿, 스마트북 등 다양한 명칭으로 호칭

【 국내 스마트폰 및 스마트패드 (누적) 보급 전망 ('10~'15년) 】

[단위: 만명]



※ 출처 : 'Mobile voice and data forecast pack: 2010 - 15' OVUM('10.5월) 및 '2010 국가 정보화백서(NIA, '10.7월)' 기반으로 KISDI·KCC 예측 ('10.11월)

- (모바일 트래픽 확대) '09년 9월 기준으로 국내 이용자(만12-59세)의 무선인터넷 이용률은 54.9%에 육박
 - '14년 무렵부터 전 세계적으로 무선 인터넷 이용자가 유선 인터넷 이용자를 추월할 것으로 전망 (출처 : 모건스탠리, '10.4월)
 - '14년 세계 모바일 트래픽 규모는 '09년 대비 약 40배 이상 증가 예상 (출처 : Cisco, '10.2월)
 - '15년 국내 무선데이터 트래픽 규모도 모바일 멀티미디어 콘텐츠 및 SNS 커뮤니티의 통신량 증가로 '10년 대비 약 40배 이상 증가 예상

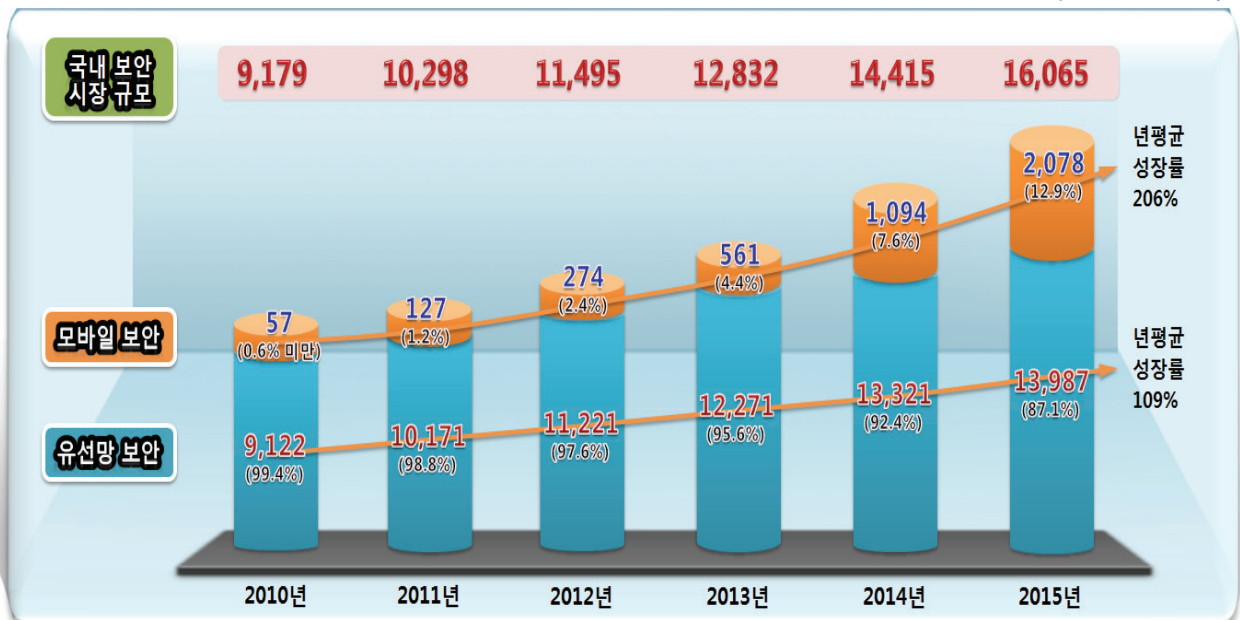
- (모바일 인터넷 네트워크의 고도화) 망 고도화(3G → 4G) 및 무선랜 인프라 구축 확대 등을 통해 모바일 인터넷의 경쟁력 확보
 - 4G(IMT-Advanced)인 m-WiBro와 LTE-A 구축 및 이중만강 연동 구축 확대를 통해 트래픽 이용량 증가와 병목현상을 일부 해결 전망
 - ※ 4세대 이동통신은 이동중 100Mbps, 정지시 1Gbps의 전송속도를 제공, 5세대에서는 이동중 1Gbps, 정지시 10Gbps 전송속도 제공 예상 (EC, Future Internet 2020, '09.5월)
 - 무선랜(Wi-Fi) 인프라를 이용한 무선 트래픽의 이통망 우회를 통해 이동통신망(3G)의 트래픽 부하 감소화
 - ※ 전세계 트래픽은 Wi-Fi 및 펌토셀을 통해 '10년 이통사 전체 트래픽의 16%에서 '15년 50% 수준으로 분산될 전망 (출처 : ABI 리서치, '10년)
 - ※ '10년 상반기, 국내에는 약 496만대의 상용·사설 AP가 이용 중 (출처 : KISA, '10년)

- (모바일 및 보안 시장의 확대) 모바일 시장은 콘텐츠를 중심으로 '13년까지 연평균 132%, 모바일 보안시장은 '15년까지 206% 성장 전망
 - 국내 모바일 콘텐츠의 시장 규모는 '10년 1조원에서 '13년까지 3조원 규모로 확대 예측 (출처 : KT경제경영연구소, '10.2월)
 - ※ '15년 이후 부터는 전자회의, 원격진료, 그린시티 등 차세대 무선인터넷 융합 서비스의 발굴을 통해 현재 모바일 시장의 80배 이상의 수요창출 기대 예상

- 세계 모바일 인터넷 콘텐츠·SW(앱) 및 서비스 매출은 '10년 587억 달러에서 '13년 1,070억 달러로 연평균 119% 확대 전망 (출처 : 모건스탠리, '10.2월)
- 앱스토어의 콘텐츠·앱 매출중 게임, 멀티미디어, 건강(생활) 부분의 비중이 전체의 69% 차지 예상 (출처 : Juniper 리서치, '09.5월)
- '10년 국내 정보보안 시장규모는 9,179억원(예측치)이며 그 중 모바일 보안시장은 약 57억원(0.6%) 차지 (출처 : KISIA, '09.12월)
- 국내 모바일 보안시장은 민간부문의 노력 및 정부의 보안정책 추진 등으로 시장의 급속한 성장세(연평균 206%)가 예상되어 '15년 약 2,078억원(12.9%)에 이를 전망 (출처 : KISA, '10.9월)
- 세계 모바일 보안시장의 경우, 6년간('09~'15년) 2.2배 증가하여 '15년에 약 2,864백만 달러(약 3조원)가 될 것으로 전망 (출처 : 'IDC, Worldwide Mobile Security 2010-2014 Forecast and Analysis', '10.5월)

【 국내 모바일 및 유선망 보안의 시장 및 점유율 전망('10~'15년) 】

(단위 : 억원)



※ 출처 : 'IDC, Korea Telecom Service & Equipment Market 2009~2013' 및 '2009 국내 지식정보보안산업 시장 및 동향 조사(KISIA)' 기반으로 KISA 산출

2.

모바일 빅뱅과 정보보호

- 최근 급속히 출현하고 있는 스마트 모바일 기술 및 신규 서비스는 우리 사회의 전 분야에 걸쳐 대혁신('Mobile Big Bang') 기회 제공
 - (산업·경제적 측면) 폐쇄적 산업구조가 개방되어 그동안 뒤쳐져 있던 국내 SW, 콘텐츠, 서비스 부문의 선진화 계기 제공
 - 이통사 중심의 폐쇄적 시장구조에서 벗어나 구글 안드로이드 앱마켓, 애플 앱스토어 등 개발자·고객 중심의 개방형 생태계 탄생
 - 스마트 단말을 통해 언제 어디서나 손쉽게 정보 생산·소비가 가능해져 전자책, 게임, 신문·잡지, 방송 분야에까지 대변혁 예고
 - ※ 디지털 콘텐츠를 다양한 단말에서도 이용할 수 있는 'N-스크린 서비스' 등의 도입으로 새로운 엔터테인먼트 서비스가 확산될 전망
 - '모바일 웹2.0 트렌드'가 국내·외 시장에 신규 모바일 비즈니스 모델의 확산을 더욱 가속화 시킬 것으로 예상
 - ※ 모바일 웹2.0 트렌드 : Web 2.0의 개방성·공유성·참여성에 모바일 특유의 이동성이 더해져 만들어지는 소비자의 새로운 문화와 행동을 지칭
 - 친구 및 타인과의 커뮤니케이션 서비스는 향후 상황정보 및 위치정보와 결합되어 신규 비즈니스 모델로까지 진화 예상
 - (사회·문화적 측면) 모바일 활성화는 경제성장 수단뿐만 아니라 선진 사회실현을 위한 양방향 소통의 수단으로도 활용
 - 사람·시스템·프로세스 등 사회 구성요소 전반에 스마트 기술이 적용되어 '스마트 라이프'가 실현되고 이를 통해 '스마트사이어티'('Smartciety')로 진입

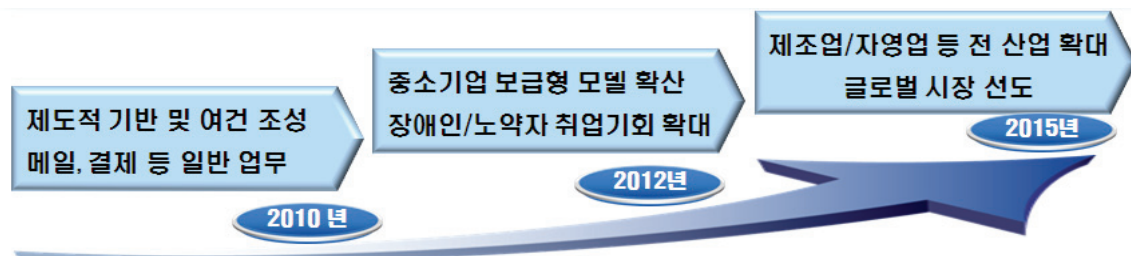
※ 스마트사이어티(Smartciety, Smart+Society의 합성어)

: 스마트폰 등 각종 스마트기기로 대화와 소통이 이루어지고 업무, 학습, 진료 등 사회 전반에 스마트 기술이 활용되는 사회 지칭(금번 종합계획에서 처음 사용)

- 원격으로 가사활동, 학습, 진료가 가능해지고 광범위한 정보공유를 토대로 새로운 사회적 관계가 형성되는 **IT 기반의 문화혁명** 도래
- 모바일 인터넷 이용이 일상화되면서 스마트 홈, 스마트 러닝, 스마트 헬스 등 스마트 라이프가 가속화
- 특히, **스마트워크(smart work)** 정착을 통해 기업·행정부문의 업무환경 개선 및 업무효율의 극대화 추구
- 종래의 사무실 개념을 탈피하여, 언제 어디서나 편리하고 효율적으로 업무에 종사할 수 있도록 하는 탄력적인 업무환경 제공

※ 스마트워크 근무율을 '15년까지 전체 공무원과 노동인력의 30%까지 높이는 방안을 범정부차원에서 추진 (출처 : 스마트워크 활성화 전략, '10.7월)

【 국내 스마트워크의 추진 목표 】



- 소셜네트워크(SNS)를 통해 개인간 공개적 커뮤니케이션 활동 증진과 동시에 사회 전반에 걸친 의제의 제안·감시 기능을 수행
 - 개인간의 사적인 대화·의견 교환을 넘어 사회적 이슈에 대한 논의 및 영향력 행사의 역할을 수행하여 사회 투명성 제고
- (환경·에너지 측면) '모바일 부문의 친환경 활동' 및 '모바일을 활용한 녹색성장'을 통해 「저탄소 녹색성장」 비전 달성에 기여

- **그린(Green) 방송통신 기술**을 개발하고 모바일 분야의 저전력, 효율적 에너지 이용을 가능하게 하여 기존 IT기술의 한계 극복
- 모바일 기술을 활용한 **에너지 수요공급 관리, 환경 감시** 등 생활 영역의 에너지 절약을 가능하게 하는 **그린 ICT서비스 활성화**

※ 그린ICT 서비스 시장 활성화를 통해, '13년까지 3조원 이상의 부가가치 창출 및 5만2천여 명의 고용 창출 효과 (출처 : 그린IT 국가전략, '09.5월)

※ ICT를 활용한 탄소배출 저감 효과 : '08년 2.5% → '12년 7.3% (출처 : NIA, IT부분 에너지 사용현황 분석, '08년)

□ **(정보보호가 핵심 경쟁력)** 이러한 모바일 빅뱅도 시큐리티에 대한 종합적·체계적 대비(對備) 없이는 **사상누각(砂上樓閣)**에 그칠 우려

○ 최근 모바일 서비스의 신뢰성 보장 및 개인정보 보호에 대한 사회적 요구가 증가하면서 **시큐리티 중요성에 대한 공감대 확산**

- 모바일 악성코드 및 새로운 공격 위협의 차단 등을 통해 신규 서비스의 **가용성 보장** 필요성 제기
- 위치정보, 인맥정보, 금융정보 등 다양한 정보의 활용이 증가함에 따라 개인정보에 대한 **관리·보호 요구 증가**

○ 모바일 시큐리티는 모바일 산업발전 및 서비스 활성화를 위하여 **필수 불가결한 전제(사회적 보험)**라는 인식이 중요

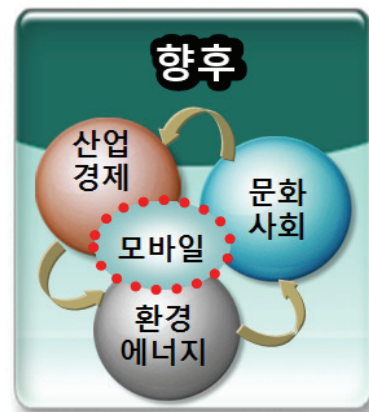
- 이용자의 안전한 모바일 서비스 이용 환경을 제공하여 산업 및 이용 활성화를 촉진하고 **사회적 우려를 근본적으로 차단**
- 향후 모바일 방송통신 미래서비스에 대한 **사전적 보안대비책 마련**으로 기술 발전에 따른 무선인터넷 신뢰성 기반 조성

【 모바일 빅뱅과 시큐리티의 중요성 】



성장동력 창출 마련

모바일 기술 적용
→
사회적 요구 반영



성장지속 및 각종현안 해결



※ 사회적 요구 : (산업) 잠재성장률 상승, 고용촉진, 환경오염 문제 해결
(사회) 신뢰 사회 조성, 사교육비 절감, 문화적 욕구의 다원화 등 해결
(기술) 컨버전스, 양방향, 개방형 기술발전에 대한 적용 요구 반영

3. 모바일 시큐리티 위협

가. 모바일 시큐리티 위협의 양태

- (기존 위협의 확대) 사이버 침해 공격, 바이러스·웜 감염, 개인정보 유출 등 기존 위협이 모바일 환경에서도 재현 가능
 - 악성코드 감염, DDoS 공격, 개인정보유출, 스팸 및 SNS피싱 등 기존(유선 환경)의 보안위협이 동일하게 발생 예상
 - ※ 올해 국내 최초로 윈도우 모바일 기반 스마트폰에서 국제전화 무단발신을 유발하는 악성코드(트레드 다이얼, TredDial) 발생 ('10.4월)
 - 신규 ICT서비스의 보안 취약성이 모바일 환경에서도 확산
 - IPTV, 클라우드 컴퓨팅 등 유선망의 신규 서비스가 무선 환경으로 확대됨에 따라 안전성을 위협하는 요인도 함께 전이
 - 모바일 기기 분실·도난시 기본적 보안조치(패스워드 설정 등) 미비로 인한 개인정보 노출, 사기 범죄에의 악용 등 피해 가능
- (새로운 위협의 출현) 기존 유선망과 다른 새로운 유형의 모바일 보안 위협의 출현 예상
 - 단말에 무선랜(Wi-Fi), 블루투스, 이동통신서비스(3G), GPS통신 등 복수의 통신기능이 기본 탑재됨에 따른 침해 경로의 다변화
 - ※ GPS통신 기반의 LBS서비스에서도 이용자 프라이버시에 대한 신규 침해유형 발생
 - 이통사에서 SW 안전성을 보장하는 폐쇄형 관리와 달리 사용자가 직접 개발하는 개방형 앱(App) 프로그램의 안전성 보장은 미흡
 - ※ 안드로이드 마켓에 등록된 애플리케이션 중 20%가 사용자의 개인정보에 접속하며, 5%는 통화가 가능한 권한을 가지는 등 개인정보 유출 가능(SMobile시스템, '10.6월)
 - SNS의 공개 커뮤니케이션 방식으로 인하여 개인정보 누설 및 사생활 침해 가능성 증가

나. 서비스·인프라 분야의 영역별 보안 위협

□ 개 요

- 모바일 서비스·인프라 분야의 보안위협은 모바일 단말, 무선네트워크 및 모바일 기반 신규서비스, 융합 콘텐츠 등 4대 영역별로 구분
 - (사용자/단말) 모바일 단말에서 기업·개인 정보유출, 부정·불법 사용, 임의조작 등을 유발시키는 위협
 - (네트워크) 무선 네트워크 전송구간(Wi-Fi, 블루투스, 3G, WiBro)에서 발생하는 DDoS 및 비인가 접속 등 네트워크 침해사고
 - (응용서비스) 모바일 클라우드 컴퓨팅, mVoIP, mIPTV, SNS 등 모바일 서비스에 대한 불법사용, 거부·오용에 대한 위협
 - (콘텐츠) 모바일을 통해 유통·이동되는 콘텐츠에 대한 불법 유출·삽입을 유발하는 저해요소

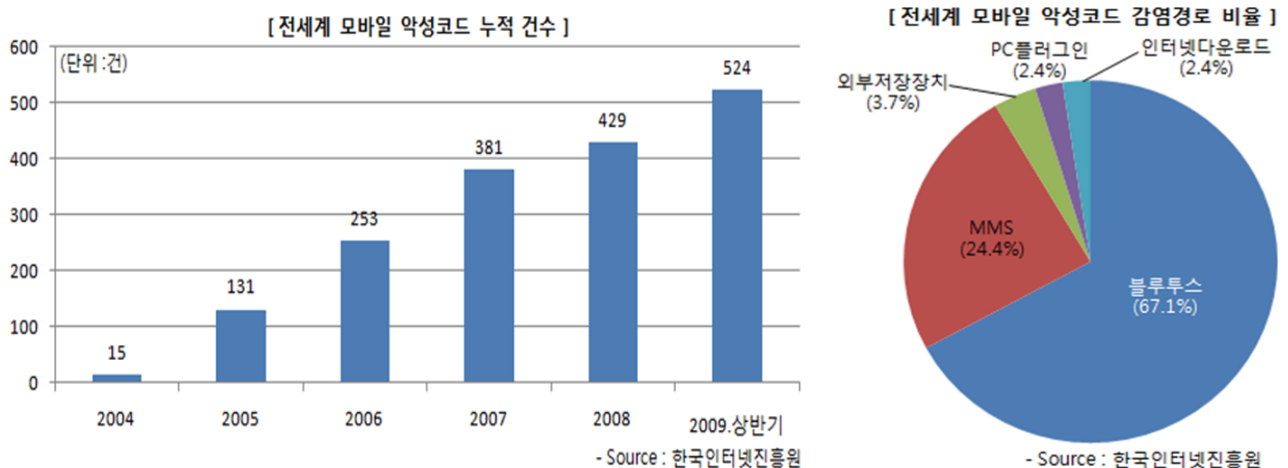
【 모바일 4대 영역별 보안위협 】



□ 단말 영역

- 보안이 검증되지 않은 앱 설치 및 모바일 기기의 자의적 변형·개조로 인한 보안 취약점 발생
 - 오픈마켓에서 애플리케이션에 대한 보안검증을 일부 제공하나, 시장경쟁 초기상황에서 높은 보안성 요구는 현실적으로 한계
 - ※ 애플리케이션 마켓(구글의 안드로이드마켓)에서 은행 프로그램을 가장해 이용자의 은행 비밀번호를 훔쳐가는 불법 소프트웨어 배포 사례 발생 ('10.1월)
 - ※ 7.7 DDoS 사태도 악성코드가 감염된 SW의 다운로드를 통해 유포 ('09.7월)
- 악성코드, 해킹 등의 위협에도 불구하고 단말의 전력소비 및 저장 공간의 한계로 인하여 고성능 보안제품 탑재는 어려운 실정
 - 전 세계 모바일 악성코드는 '09년 상반기까지 총 524종이 발견 되었으며, '10년 2/4분기까지 약 600여 종 이상 추정

【 해외 모바일 악성코드 발생 건수 】



- 스마트폰 분실·도난에 의한 개인정보유출 및 중요정보(금융정보, LBS 위치정보 등) 노출로 금전적 피해, 사생활 침해 등 발생
 - ※ 국외 스마트폰의 분실 가능성은 노트북의 15배 (마이크로트랜드, '09.6월)
 - ※ 스마트폰, 스마트패드, 넷북 등은 업무용으로도 활용 가능하나 기기 분실에 따른 기업 기밀정보의 유출 가능

□ 네트워크 영역

- 공공 또는 사설 무선랜(Wi-Fi) 사용과 블루투스를 통한 무선 송수신 기능의 이용 빈도가 증가함에 따라 무선 네트워크 위협 증가
 - 무선랜 장치(AP)를 통해 해커에 의한 무선 신호 스니핑, 정보 탈취용 거짓(rogue) AP설치, 접속 허점을 이용한 무단접속 공격 가능
 - ※ 모바일 접속구간(기기 ⇄ 무선인터넷) 및 인프라 접속구간(망 ⇄ 망)에 악성 코드 전이, 구간도청 등을 악용하여 서비스에 대한 장애 유발
 - 대량의 무선 패킷전송 등을 통한 모바일 DDoS 공격 시도 가능

【 무선랜 침해 유형 】

유 형	침해 동작
패킷 스니핑	무선구간에서 패킷수집 도구를 통한 멀티미디어 콘텐츠 유출 · 위변조, 패킷의 해독을 통한 암호화 인증 무력화를 시도
중간자 공격	기기간의 통신을 조작하는 MITM(Man-In-The-Middle) 공격을 통해 데이터를 장기간 유출하거나 거짓정보 삽입을 시도
비인증(rogue) AP	비인증된 AP로 모바일 기기를 유도(Wi-Fi 피싱)하고 사용자 로그인시 비밀번호/이메일/신용카드 등의 데이터를 해킹 시도
워드라이빙 (Wardriving)	차량으로 이동하며 구내 정보통신망(LAN)에 무단으로 접속하고, GPS를 이용해 지역별 무선액세스 접속 허점을 노출
암호사전 공격	암호사전(Dictionary)을 통하여 암호화된 비밀번호의 해독시간 단축 시도

- 보안이 설정되지 않은 무선랜에서의 모바일 기기 사용은 무단사용, 해킹, 개인정보 유출, 도청 등의 보안위협에 노출 가능
 - 국내 15개 시·도, 29개 지역의 무선AP(42,997대) 보안현황 조사 결과, 약 44.8%가 無보안 설정되어 운영 중(출처: KISA, '10.7월)
 - ※ 특히, 조사 대상중 가정용 사설 AP 28,312대의 경우 55.2%가 보안 설정 미비
 - 전 세계 27개 공항 대상 무선랜 취약성 조사 결과, 80% 이상이 보안에 취약 (출처: 美 Air Tight Networks사, '10년 상반기)
 - ※ 조사대상의 59%가 無보안으로 운영되고 있으며, 21%는 취약한 WEP 방식 사용

□ 응용서비스 영역

- 스마트폰의 확산과 함께 모바일 뱅킹 이용이 증가하면서, 악성코드를 단말기에 감염시켜 금융정보를 유출하는 해킹사고 예상
- 이용자의 정보이용 동의 없이 스마트폰용 앱이 자의적으로 이용자 위치정보, 단말기 정보, 연락처 정보 등을 수집·유출 가능
 - ※ 스마트폰용 앱의 상당수가 동의 없이 폰ID, 이용자 위치, 나이, 성별 등의 개인 정보를 전송하고 있는 것으로 조사(월스트리트저널, '10.12월)
- 모바일 클라우드 서비스에 악의적으로 접근하여 저장되어 있는 기업의 기밀정보를 유출하거나 기업 전산망을 교란 가능
 - 관리 부주의, 실수 등 다양한 기술적·관리적 요인에 의한 컴퓨팅 서비스의 일시적 중단사고 발생 가능
 - ※ 아마존(Amazon) S3 서비스에서 서버간 통신의 설계과정 오류로 인하여 8시간 동안 서비스 중단 ('08.7월)
 - 클라우드 컴퓨팅 서비스 사업자가 폐업하는 경우 보관된 데이터의 대규모 유실 위협 존재
 - ※ 스토리지 서비스업체 미디어맥스(MediaMax)의 폐업으로 인하여 약 2만명 유료 이용자의 데이터가 유실 ('08.7월)
- 모바일 오피스는 기업 네트워크에 연결되어 이용자의 이동 및 단말 분실에 따른 해킹 및 기업정보 유출 등의 피해발생 가능
 - 회사 내부망과 모바일 단말기 사이의 통신시 트래픽 도청, 해킹 등을 통한 권한 없는 접근 및 정보유출 발생 가능
- 악의적인 사설 모바일 앱스토어·SNS 사이트로 유인하여 악성 프로그램 설치를 유도하는 등 새로운 형태의 공격이 증가 예상
 - SNS의 단문(short) URL 서비스를 악용한 피싱·사기 위협 발생
 - ※ 단문 URL(Short Uniform Resource Locator) : 인터넷 상의 파일주소(URL)를 모바일에서 이용하기 쉽도록 짧게 줄인 인터넷 주소

□ 모바일 콘텐츠 영역

- 암호화된 디지털저작권관리(DRM) 파일을 해독·해킹하여 콘텐츠 유출 및 비인가된 사용에 노출 가능
 - ※ DRM이 적용된 야후/냅스터 판매용 SW가 해킹프로그램에 의해 DRM 해지(암호화 풀린) 상태로 유포('06.9월)
 - ※ DRM이 적용된 아마존의 유료 콘텐츠가 비인가된 기기에서도 구동되도록 해킹된 사례 발견('09.12월)
- 모바일 기반의 불법 콘텐츠의 유통방식이 다양화·지능화
 - 탈옥(jail-break)을 통해 불법복제 앱을 사용하거나, 외장 메모리에 불법 앱을 복사하여 이용함으로써 저작권 문제 야기

다. 이용자 보호 분야의 보안 위협

- 모바일 환경에서 소셜네트워킹서비스(SNS) 등의 이용이 증가하면서 SNS를 통한 개인정보 유출 위험성도 증대
 - 스마트폰 등을 통해 SNS 이용이 확산되면서 개인정보가 부주의하게 노출되고, 악의적 목적으로 이를 거래하는 사례 발생
 - ※ 페이스북 150만명의 개인정보가 천명당 \$25~\$45에 거래(Networkworld, '10.4월)
 - 모바일 기기에 GPS가 탑재되어 개인의 위치 식별이 가능해짐에 따라 위치정보 오·남용 및 사생활 침해가 새로운 문제로 부각
 - ※ 모바일 기기의 위치기반 SNS '포스퀘어(Foursquare)'가 미국 등 지역에서 인기 상승하면서 특정인의 위치를 사전에 파악하고 빈집을 절도하는 범죄 발생
- 이메일, SMS 등에 대한 스팸규제가 강화됨에 따라 상대적으로 규제가 약한 신규 모바일 서비스로 스팸 이동 우려

- 스마트폰 이용 확대와 함께 모바일 광고시장이 본격적인 성장 국면에 돌입하면 스마트폰 등을 활용한 무작위 스팸 발송 증가 예상
- 스팸봇넷이 된 PC나 모바일기기를 원격조정하면 스팸머 신원을 숨긴 채 다량의 스팸 발송 및 지속적 스팸자원 확보가 가능
- ※ 휴대폰 OS인 심비안(Symbian)에서 '섹시 스페이스(Sexy Space)'라는 스팸 메시지 발송 가능 악성코드 발견 (트렌드 마이크로, '09.7월)

○ 모바일 기반의 불건전·유해정보에 대한 접근이 용이

- 모바일 기기의 개인화 특성과 함께 유해정보 차단 기능의 부재로 청소년들의 무분별한 불건전·유해정보 접근이 용이
- ※ 안드로이드 마켓 등 국외 앱스토어의 경우, 성인 인증 없이도 유해정보 다운 가능

라. **보호기반 분야의 위협**

- 국내 스마트폰 보안기술은 안티 바이러스, 방화벽, 디바이스 잠금 기능 등 단품형 기술로 구성되어 있으며 아직 초기단계의 기술 수준
- 모바일 환경에 적합한 저전력·저용량, 멀티미디어 서비스 및 통합 환경에서의 보안기술은 부족
- 국내 정보보호산업의 영세성으로 인한 경쟁력 저하와 모바일 보안 전문인력 부족 등으로 모바일 보안 시장의 성장 저해
- 협소한 내수시장 위주의 사업 영위 및 업체간 과다출혈 경쟁 등으로 수익 악화 및 보안인력 양성체계 부족으로 인력 수급 어려움
- 이용자의 보안에 대한 전반적인 인식 부족 및 모바일 오피스, 클라우드, SNS 등 신규서비스 보호에 대한 법제도적 장치 미흡

- 향후 모바일 인터넷은 매쉬업(mash-up) 기반으로 활성화됨에 따라 정보의 진정성 및 신뢰성에 대한 위협에 직면

※ 매쉬업(mash-up) 환경 : 서로 다른 영역에 속한 서비스 및 정보들이 다양한 형태로 결합되어 새로운 융합 서비스로 재창조되는 환경

- 근거 없는 정보에 관한 루머들이 모바일 미디어를 통해 확산되어 사회, 경제, 안보 등에 부정적 영향을 미치는 인포데믹스 위협 확대

※ 인포데믹스(InfoDemics, 정보(Information)+전염병(Epidemic)) : 근거 없는 정보가 급속히 전파되면서 사회경제적으로 혼란을 야기하는 현상을 지칭

- 악성 댓글, 사이버 모욕 등 불건전한 인터넷 활동으로 인한 정신적 피해, 기업 신뢰도 타격 등 다양한 피해 발생
- 개인의 사이버 활동이 증가될 미래 네트워크에서 일반 생활에서의 윤리보다 더욱 다양한 형태의 인터넷 윤리 관련 규정 필요

- 지능형 전력망(스마트그리드) 등 사회기반시설의 네트워크화로 침해 사고의 범위가 국가 주요기반시설까지 확산될 우려 증가

- 인터넷 위협 양상이 개인 차원의 금전적 이득뿐만 아니라 사회 혼란 야기를 목적으로 공공재를 겨냥한 사이버테러 형태로 진화

※ '09. 7월 국내 주요 정부기관, 금융사, 언론사, 주요 포털 등 사회적 파급효과가 큰 사이트 대상으로 사전 치밀히 계획된 분산서비스공격(DDoS)이 발생

- 악성코드가 원자력, 전기, 교통, 통신 등 국가 주요기반 시설의 제어 시스템 등에 침투해 오작동 및 시스템 마비 초래 가능

※ 최근 이란·중국 등에서 원자력발전소 등 주요 산업기반시설의 제어시스템에 오작동을 일으킬 수 있는 신종 악성코드(스턱스넷, Stuxnet) 출현('10.6월)

□ 새로운 인터넷 서비스의 활용으로 프라이버시 패러다임 변화

- 프로슈머화(prosumer)가 가속화되면서 개인정보에 대한 책임과 관리에 관한 이슈 및 사이버 정보의 소유권 문제 발생

※ 프로슈머화 : 이용자가 개인정보 콘텐츠의 주체로서 콘텐츠를 생성·소비

※ 이용자 개인이 직접 작성하여 사이버 공간에 공개한 블로그 게시물, 동영상 등이 타인에 의해 확산될 경우 책임과 소유권 문제 발생

- 개인신상정보, 행태정보까지 모바일 단말에 기록되고 집중됨에 따라 정보의 유출 발생 시 심각한 개인피해 발생

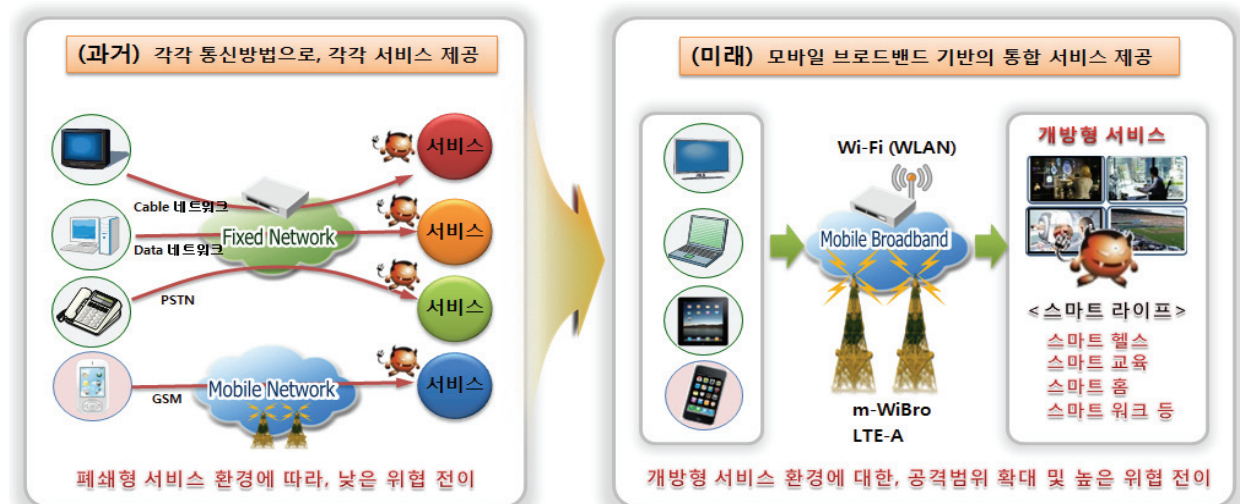
□ 스마트(smart)한 환경이 일상생활 전반에 걸쳐 확산됨에 따라 사이버 침해사고 등으로 개인의 삶까지 파괴될 가능성 증가

- 사이버공격 범위가 확대·전이되고 공격 형태가 다양화되면서 IT 서비스에 기반을 둔 일상생활에까지 위협 가능

- 스마트라이프 서비스의 경우 공격 파급효과가 일상생활까지 확대되어 건강, 금융, 생활 등 각종 정보의 유출 및 생활 마비 가능

- 사이버공격에 의한 개별 서비스의 피해는 모바일 브로드밴드에 연결된 개방형 서비스의 모든 영역으로 확산

【 스마트라이프 서비스에 대한 미래 위험성 증대 】



Ⅲ. 비전 및 추진 전략

1. SWOT 분석

【 강점 : Strengths 】

- 세계 최고 수준의 인터넷 인프라 환경 (광통신 보급 1위, OECD '08년)
- 우수한 유무선 인터넷 서비스 핵심기술의 확보
- 모바일 시큐리티의 필요성에 대한 사회적 인식 고조
- 혁신적인 신규 모바일 서비스의 이용 증가 및 시장의 확대

【 약점 : Weaknesses 】

- 모바일 환경 구축시, 정보보호(위협의 사전 대비)에 대한 기술력 미흡
- 모바일 정보보호 비즈니스 모델 및 원천 기술 부족
- 대기업과 중소 보안업체 간의 협력 부족 및 이용자의 보안 인식 미흡
- 모바일과 정보보호 기술을 겸비한 글로벌 전문인력 부족

【 기회 : Opportunities 】

- 모바일 단말 · 인터넷 이용확산에 따른 신규 보안 서비스의 성장잠재력 증가
- 정부와 민간의 모바일 보안산업에 대한 생태계 진흥 의지
- 세계 모바일 보안시장의 태동에 따른 글로벌 보안시장의 선점 기회 대두

【 위협 : Threats 】

- 모바일 신규위협 등장 및 대응책 부재 (서비스와 보안의 병행구축 미흡)
- 망 · 서비스 위협, 개인정보노출 증가 등에 대한 체계적인 보안 대책 부족
- 모바일 정보보호 원천기술에 대한 높은 국외 의존도

- (SO, 강점-기회) 모바일 오피스, 클라우드 등 신규 비즈니스 모델에서의 보안시장 생태계 조성을 통해 글로벌 경쟁력 확보
- (ST, 강점-위협) 모바일 활성화 및 정보보호에 대한 균형적 정책 추진을 통해, 모바일을 통한 생산성과 보안성 향상을 병행 추구
- (WO, 약점-기회) 모바일워크 등 신규서비스의 보안위협에 대한 사전적 대비책 준비를 통해 모바일 대중화 및 생산적 활용 촉진
- (WT, 약점-위협) 신규위협 증가, 보호 원천기술 부족 등을 해결하기 위해 민간 중심의 투자를 촉진하여 약점 최소화

2. 비전 및 목표

- 급변하는 유·무선 융복합 인터넷 환경 속에서 중장기 모바일 시큐리티 전략 추진을 통해 「스마트 모바일 보안강국」으로 도약
- 스마트 단말, 무선 네트워크, 응용서비스, 콘텐츠 등 각 분야별 선제적 보안대책 마련을 통해 미래 모바일 서비스의 보안품질 향상
 - 모바일 환경에서의 개인정보 유출방지, 스팸피해 최소화, 불건전 유해정보의 유통 차단 등을 통해 모바일 이용자 보호체계 확립
 - 글로벌 경쟁력 강화를 위해 상생적 보안생태계 조성, 모바일보안 연구·개발, 법제 정비 및 이용자 인식제고 등을 통해 보호기반 확충



3.

추진 전략 및 체계

□ 정책기조

모바일 활성화와 보안의 균형정책

◆ 모바일 보안 강화 추진이 서비스 활성화를 저해하지 않도록 **균형 있는 정책 추진**

※ 새로운 모바일 서비스가 활성화 될 수 있도록 개인 정보 활용과 보호를 동시에 고려하는 정책 추진

미래 모바일 위협의 사전적 예방

◆ 모바일 서비스 활성화 이전에 **기존** 보안 위협과 **신규**로 발생하는 위협에 대한 사전 대응 강화

※ 모바일 클라우드, 모바일 오피스, SNS, 스마트TV 등 신규 모바일 서비스에서 발생하는 보안문제 해결

※ 모바일 보안 R&D에 대한 민간·정부 투자 확대를 추진하여 신규 위협에 대한 사전적 대응책 확보

민간의 자발적 참여 유도

◆ 모바일 서비스 안전성 강화를 위해 **민간이 자발적으로 참여**할 수 있는 환경 조성

※ 앱스토어 운용자가 어플리케이션에 대한 안전성을 사전에 진단하여 앱스토어의 신뢰성 제고

모바일 시큐리티 산업 생태계 조성

◆ 모바일 보안서비스 시범사업 추진 및 민간 기술이전 등 **상용화 지원 강화**를 통해 시장 초기단계에서의 **모바일 보안수요 창출** 및 **중소 보안기업의 경쟁력 강화** 유도

※ 스마트워크, 모바일 오피스, 모바일 클라우드의 보안성 강화를 위한 시범사업 추진

※ ETRI, KISA, 국보연 등 연구기관의 성과물을 민간 이전하는 모바일 보안기술 이전행사를 정례화

□ 추진단계

- 이용자의 수요, 기반기술의 선도성, 新시장 창출 등과의 상승적 결합을 고려하여 단기/중장기 과제로 구분해 단계적으로 추진

【 단계별 주요 정책 】

추진 단계	서비스·인프라 보호	이용자 보호	보호기반 확충
단 기 (‘11~’12년)	· 모바일 백신 활성화 및 악성코드 점검 강화 · 신규 스마트기기 보안가이드라인 마련 · 무선랜 관리체계 확립	· SNS 개인정보 유출 차단 · 유해정보 차단 앱 개발·보급	· 민간 상생환경 조성 · 모바일 보안서비스 시험환경 구축 · 모바일 정보보호 문화 확산
중 기 (‘12~’13년)	· 앱 게놈 프로젝트 추진 · 안전한 앱 유통 환경 조성 · 모바일 클라우드 보안 기반 마련 · 모바일 오피스 보안체계 구축	· 위치정보 자기제어 마련 · 유해정보 자율규제 확립 · 모바일 스팸 지능형 필터링 활용 확대	· 모바일 보안 원천기술 개발 · 모바일 정보보호 법제 정비
장 기 (‘14~’15년)	· 유무선 통합망 신규위협 대응 강화 · 모바일 뱅킹 보안기반 강화	· 신규서비스 개인정보 대책 강화	· 기술개발 결과물 상용화 · 세계시장 본격 진출 · 글로벌 협력체계 다양화

□ 추진체계

- 보안강화를 위해 사업자, 이용자, 연구기관, 해외 유관기관, 정부의 주체별 역할 분담을 통한 유기적인 상호협력 체계 구축

【 주체별 역할에 따른 추진체계 】



Ⅳ. 주요 추진과제

1. 미래 모바일 서비스 · 인프라 보안품질 향상

① 신규 모바일 단말 보안 강화

가. 스마트폰 단말 보안 강화

개 요

◇ 스마트폰 애플리케이션과 앱스토어의 사전 보안검증체계 마련

□ 배경 및 필요성

- 현재 선진국(미국, 서유럽 기준)의 스마트폰 가입자의 비중은 전체 이동통신 가입자 수의 **30% 수준**에 육박(한국은 '10.11월말 12% 수준)
- 국내의 경우, **'11년 중반**(스마트폰 점유율 10%대 후반 예상)부터 급전적 이득(인터넷뱅킹, 증권 등)을 노리는 스마트폰 **악성코드의 출현** 예상
 - 현재까지 해외에서 발견된 모바일 악성코드는 약 600여 종으로 추정
 - ※ '09년 6월까지 발견된 스마트폰 악성코드는 총 524종 (출처 : Smobile Systems)
 - 해외 사례를 통해 유추해 볼 때 본격적인 악성코드 유포는 **'11년 하반기**(스마트폰 점유율 약 30%) 이후에나 나타날 것으로 전망
 - ※ '10.4월 국제전화를 무단 발신하는 악성코드(TredDial)가 국내 처음 발견 되었으나, 민관합동대응반에서 전화 차단, 이용자 통보 등의 조치를 통해 피해를 사전예방
- 개방형 스마트폰 앱스토어를 통해 누구든지 프로그램 제작, 배포가 가능하므로 애플리케이션을 통한 **악성코드 유포**가 용이
 - 국내 환경에 적합한 스마트폰 애플리케이션 보안 검증절차를 마련 하여, 앱스토어를 통한 악성 앱의 불법 유통을 사전 차단 필요

【 국내·외 주요 앱스토어 현황 】

구 분	애플 (앱스토어)	구글 (안드로이드마켓)	노키아 (Ovi 스토어)	SKT (T스토어)	KT (olleh 마켓)
검증체계	○	X	○	○	○
특 성	폐쇄형 강력한 통제	개방형 사용자에 책임부여	폐쇄형	폐쇄형 품질위주검증	폐쇄형 품질위주검증
앱 수 (10.10.5.기준)	272,924개	107,757개	12,072개	55,000개	4,884개

※ KT는 보안검증을 실시중이고 SKT의 경우 (가칭)‘모바일 애플리케이션 통합 보안검증시스템’을 구축할 예정이며, 구글은 앱에 대한 보안검증을 非수행

□ 추진 내용

○ (스마트폰 백신 보급 활성화) 백신 보급 확대를 위한 신규 비즈니스 모델 발굴 및 스마트폰 백신의 성능 강화

- 금융, 생활 등에 특화된 백신 유료화 비즈니스 모델 발굴을 통한 백신 보안솔루션 사업의 경쟁력 개선 유도

※ 금융(은행, 증권, 보험 등), 생활(게임 등) 분야에 B2B용 스마트폰 통합보안SW 발굴 등 무료 백신과 차별화된 보안SW가 공급될 수 있도록 정부 지원책 마련

- 영세 보안업체들이 백신 성능측정 및 각종 스마트폰 단말, 플랫폼별 통합 테스트를 할 수 있는 ‘모바일 백신 테스트베드’ 구축

○ (모바일 웹 악성코드 점검) 모바일 전용 웹페이지를 통한 악성코드 유포 피해 방지를 위해 ‘모바일 웹(web) 안전성 점검 시스템’ 구축

- 모바일 웹사이트 현황 파악 및 악성코드 점검시스템 구축 추진

※ ‘(가칭)모바일 보안표준 연구센터’를 통해 고가의 시험장비 및 교육장 환경을 지원하고, 백신 테스트베드 구축·제공, 모바일 웹 안정성 점검 실시 등 수행

- 모바일용 웹사이트 및 웹 앱(Web App)에 대한 악성코드 은닉 여부를 판별하여 필요시 악성코드 제거 조치 등 수행

○ **(한국형 앱 게놈 프로젝트 추진)** 앱 스토어에서 유통중인 앱을 분석해 개인정보 수집 범위 및 악성행위 수행 여부를 조사

※ 앱 게놈 프로젝트(App Genome Project) : 앱의 기능적 특성, 보안위협 등의 분석을 통해 앱의 악성행위 여부를 파악 (사례 : 美 모바일 보안업체 '룩아웃'에서 약 30만개의 앱을 대상으로 개인정보 수집 등 보안위협을 분석·발표, '10.8월)

- 이통사·제조사가 주축이 된 **도매-앱스토어** 및 구글·애플 등 업체가 제공하는 **소매-앱스토어**에서 유통되는 앱을 대상으로 추진

※ 도매 앱스토어 : K-WAC(Korea - Wholesale Applications Community) 등

- 국내외 오픈마켓 등에서 유통 중인 앱을 수집·분석하기 위한 **전담인력 확충 및 분석 환경**(통신사별 단말기 및 시스템 등) 구축

※ 이통사, 제조사, 백신사 등과 민·관 협의체를 구성한 후 검증대상 선정 기준, 앱 위험 분석용 자동툴, 시험 및 분석환경 등을 마련

- 유관기관 간 조사 결과 공유를 통해, 앱의 악성행위 판단 가이드 라인을 마련하고 스마트폰 전용백신 개발 및 업데이트 등에 활용

※ 국내외 스마트폰 앱스토어 마켓간 공조체제 추진 (분석용 프로그램 및 악성 행위 앱에 대한 조치 여부 관련 내용 등 정보공유)

○ **(안전한 앱 유통 환경 조성)** 스마트폰 앱에 대한 표준화된 검증 기준 및 절차를 마련해 이를 준수하도록 유도

- 이용자가 앱스토어에 등록된 앱을 신뢰할 수 있도록 앱의 위변조 검증 및 배포자 신원 확인을 위한 **코드서명 인증 체계** 구현

※ 코드서명 인증서 : 앱의 위변조를 검증하고 앱-개발자·배포자를 확인해주는 인증서

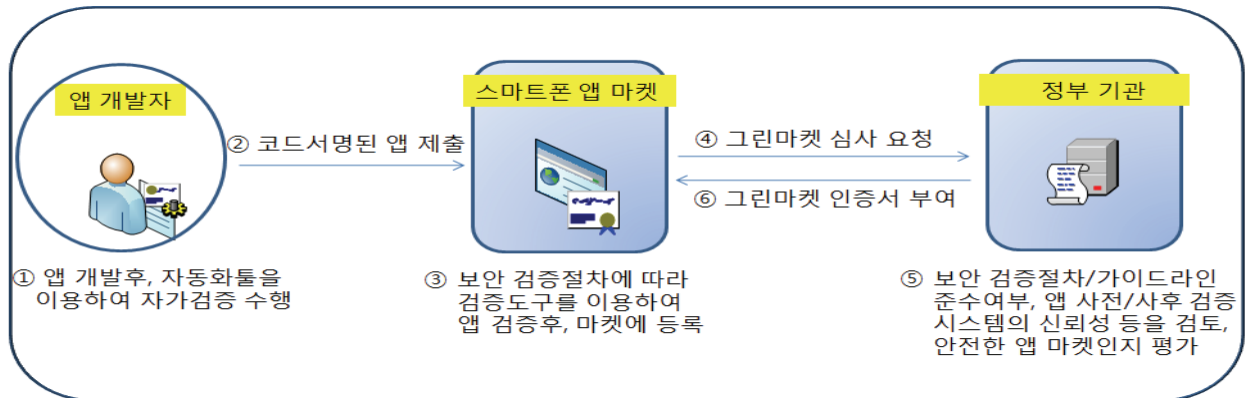
- 표준화된 스마트폰 앱 보안 취약성 검증 절차 마련 및 보안 가이드 라인을 개발하고, 보안 취약성 판단 도구 개발 지원

※ 스마트폰 앱 개발자 및 검증자를 위한 자동화툴(기능 테스트, 안전한 코딩 가이드 라인 준수 여부 검사 등)과 스마트폰 악성코드 행위 분석 도구 개발 추진

- 스마트폰 앱 보안 검증절차 및 가이드라인 등을 준수하는 스마트폰 앱 스토어에 '그린 마켓 인증서'를 부여하고 대상 공개

※ 그린 마켓 인증서 : 앱에 대한 표준화된 보안 검증 절차 및 가이드라인을 준수하고 지속적인 사후 관리를 수행하는 마켓을 선정하여, 신뢰할 수 있는 마켓임을 정부가 인증

【 안전한 스마트폰 앱 유통을 위한 '그린 마켓 인증 체계' 】



- (보안용 앱·솔루션 시험센터 구축) 스마트폰 전용의 보안 앱 검증센터를 구축해 스마트폰 및 패드에서 사용되는 보안 앱 및 솔루션 시험·검증

- 백신사 등 보안업체 뿐만 아니라 개인 프로그래머들이 개발한 보안 프로그램들을 검증하고 통과된 보안솔루션이 판매되도록 유도

※ 보안 앱 개발 및 판매 등은 일부 보안 업체에 한정되어 있고, 이용자는 이통사나 스마트폰 제조업체가 선택한 보안 프로그램을 수동적으로 사용하고 있는 상황

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 안전한 스마트폰 앱 유통 환경 조성						정부·유관기관, 이통사, 보안업체
	○ 스마트폰 백신 보급 활성화						유관기관, 제조사, 이통사, 보안업체
중기	○ 모바일 웹 악성코드 점검						정부·유관기관, 제조사, 이통사, 보안업체
	○ 한국형 앱게놈 프로젝트 추진						
장기	○ 보안용 앱·솔루션 시험센터 구축						정부·유관기관, 이통사, 보안업체

나. 스마트패드 등 신규 기기 보안 대책 마련

개 요

- ◇ 스마트패드, e북, PMP 등 스마트화 되어가는 다양한 단말기와 향후 개인 단말과 연결될 홈네트워크에 대한 보안대책 마련

□ 배경 및 필요성

- 삼성의 '갤럭시탭', 애플의 '아이패드' 등 7~10인치 크기의 터치 스크린을 가진 새로운 형태의 스마트패드가 등장
 - 스마트패드는 Wi-Fi, 3G 통신이 가능하며 일반 PC와 같이 인터넷 서핑, 파일 다운로드 등이 용이하여 향후 대중화 될 것으로 전망
 - ※ 세계 태블릿PC가 '10년 1,950만대에서 '14년 2억800만대 규모의 시장을 형성할 것으로 예상 (출처 : 가트너, '10.10월)
- 단말기 종류에 관계없이 동일한 이용자 경험(User Experience)을 제공받는 N-Screen 서비스가 스마트패드에서 활성화 될 것으로 전망
 - 드라마, 영화, 전자책, mp3 등 다양한 콘텐츠의 이용이 가능하고, 향후 PC에서와 같은 전자 금융결제 가능
 - '스마트 홈네트워크'의 중심 허브(Hub)로서 TV, 냉장고, 형광등 등 제품과 연결되어 각종 정보를 주고받는 역할 수행
- 향후 스마트패드를 통해 홈네트워크의 무단 동작 제어 및 스마트 그리드 전력정보 수집을 목적으로 하는 보안 위협 예상
 - 분산서비스거부공격(DDoS), 개인정보 노출, 과금정보 노출, 원격 제어 등 보안위협이 예상되므로 이에 대한 선제적 대응책 마련 필요
 - ※ 스마트그리드 : 기존 전력망에 정보통신 기술을 사용하여 전력 공급자와 소비자가 양방향으로 정보를 교환하여 에너지 효율을 최적화하는 인프라

□ 추진 내용

- (콘텐츠 위·변조 방지) CAS·DRM 융합 보안시스템 또는 디지털 워터마킹 응용 위·변조 방지 기술을 주요 콘텐츠에 적용 및 활용
 - CAS·DRM 등 융합 보안기술 적용 및 유출된 콘텐츠에서 불법 유출한 사용자를 식별하는 디지털 워터마킹 관련 응용 기술 개발
 - ※ 디지털 워터마킹 : 디지털 콘텐츠에 저작권 정보, 사용자 정보 등의 특정 정보, 즉 워터마크를 콘텐츠 자체에 삽입하고 추출하는 기술
- (스마트패드 보안안내서 마련) 안전한 스마트 단말기기의 개발·보급을 위해 취약점과 대응방법을 포함한 보안안내서 마련
 - 스마트패드의 기기별 보안 아키텍처 및 요구사항을 준용하며, 공통적 보안 특성에 맞는 세부 요건을 고려하여 개발
 - 국제 표준의 추진동향, 기술발전 동향, 시장 기술 현황에 따라 유연하게 적용 가능한 가이드라인 마련
- (Smart-Hub 보안체계 마련) 스마트패드의 홈네트워크 허브화에 대비하여 발생 가능한 공격 위협에 대한 보안 아키텍처 개발·도입
 - 홈네트워크 신뢰기반 통신구조 연구, 장애·오류극복, 고가용성 보장 및 서비스 지속 유지 등 신뢰보장용 보안 아키텍처 모델 확보
 - ※ 스마트허브에 대한 악성코드, DDoS 공격 등에 대한 근원적 차단뿐만 아니라 개인정보·프라이버시 보호를 위한 대응 인프라 구조 모델 개발

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 콘텐츠 위·변조 방지						정부·유관기관, 이통사, 보안업체 등
중기	○ 스마트패드 보안안내서 마련						정부·유관기관
장기	○ Smart-Hub 보안체계 마련						정부·유관기관, 보안업체 등

가. 무선랜 보안수준 제고

개 요

- ◇ 공중 무선랜의 체계적 보안 관리체계 수립, 이용자 인식제고 등을 통해 무선랜 보안수준 강화 추진

□ 배경 및 필요성

- 무선공유기(AP) 이용이 급격히 증가하면서 공개된 타인의 AP를 쉽게 접속하여 인터넷을 이용함에 따라 보안상 취약점이 노출
- (사설 무선랜) 이용자들이 보안설정 지식 및 인식 부족으로 보안 설정 없이 이용함에 따라 무단사용, 개인정보 유출 등 보안위협 존재
- (공중 무선랜) 공공장소에 AP 설치가 증가하고 있으나 누구나 접속할 수 있어 악의적 목적에 의한 악성코드 유포 시 추적·대응 어려움

※ 이통사별 공중 무선랜(와이파이존)을 확대 예정(KT 11년까지 10만곳, SKT '10.9월까지 1만곳, LGU+ 10년까지 11,000여곳, '10.7월 업계조사)

【 국내 무선랜 보급 현황('10.9월) 】

구 분	상용 무선랜 AP (olleh-KT, SKT-WiFi 등)	인터넷전화용 AP (KT-Qook, myLGnet 등)	사설 AP (가정용 AP, 휴대용 와이브로 AP 등)	합계
보급대수	18.7만	229.4만	292.5만	약 540.6만

【 국내 무선랜 AP 보안 현황 】

('10.7. 보안현황조사 결과 기준)

구 분		상용 무선랜 AP (alleh-KT, SKT-WiFi 등)		인터넷전화용 AP (KT-Qook, myLGnet 등)		사설 무선랜 AP (가정용 AP, 기업용 AP)		합계	
조사대수		2,831대		11,854대		28,312대		42,997대	
보안 설정	有	2,831대	100%	6,178대	56.2%	14,726대	52.0%	23,735대	55.2%
	無	-		5,676대	43.8%	13,586대	48.0%	19,262대	44.8%

□ 추진 내용

- (원클릭 보안솔루션 도입) 이용자에게 손쉽게 개인이 사용하는 사설 무선랜 보안설정을 강화할 수 있는 프로그램 제공
 - AP제조사들과 협력하여 보안 설정의 표준 인터페이스 및 데이터 포맷을 마련하여 '원클릭 무선랜 보안설정 솔루션' 개발 및 배포 지원
- ※ 원클릭 보안설정 솔루션 : 이용자들이 쉽게 무선 AP에 보안설정 강도를 높일 수 있도록 암호화 수준(WEP→ WPA2)을 자동 변환시키는 프로그램

【 솔루션 개념 및 주체별 역할 】



- (무선랜 보안 종합포털 구축) 무선랜 보안 관련 각종 정보 및 대응방안을 공유할 수 있는 장 마련
 - 무선랜 보안위협 및 대응방안 관련 정보 공유, 무선랜 보안설정 솔루션 배포, 무선랜 보안설정 방법(제조사별 안내 포함) 등 제공
- (무선랜 보안관리 강화) 인증우회, 데이터 유출 및 위변조, 접속 장애에 대한 위협 예방·대응 기술 개발 및 현장 점검
 - Wi-Fi존 보안관리(침해사고 감시·이력관리) 모델 마련
- ※ 사용자/기기 인증, 보안기술, 인증정보 등 표준 보안관리 모델 개발 및 시스템 구축

- 이용자 접속방법, 인증·암호화 보안설정, 개인정보 관리 등 Wi-Fi존 구축·관리체계 및 식별체계(SSID 등) 표시 방안 마련
 - 무선랜 보안운영 표준 모델에 기반한 공중 Wi-Fi존, 사설 무선랜 보안운영 점검 및 점검 결과에 따른 제도·홍보 방안 수립
- ※ 현장조사를 통해 무선 AP의 초기패스워드 변경 여부, 보안설정 여부, 인증, 암호화 지침 준수 여부 등을 점검

【 무선랜 보안운영 현황 점검 】



- (무선랜 보안 인식제고) 무선랜 이용자들의 보안인식 수준 제고를 위한 다양한 형태의 대국민 홍보 및 관련 사업자 제도
 - 무선랜 보안설정 관련 온·오프라인 대국민 홍보 실시

※ KISA 보호나라(www.boho.or.kr)에 무선랜 전용코너 개설, 무선랜 보안설정 팸플릿 제작·배포, 대중교통수단을 이용한 홍보, 무선랜 보안설정 관련 가이드 제작·보급, 반상회를 통한 ‘무선랜 보안설정 안내문’ 배포 등
 - 관련 사업자 제도를 통해 서비스 가입자(제품구매자)에게 무선랜 보안의 중요성과 설정방법 등의 안내 강화 유도

※ 무선 AP제품 사용설명서 개선 유도하고, 개인 이용자 대상 주기적 패스워드 변경 사용 등 안내, 기업 운영자 대상 무선랜 보안 교육 등 실시

○ (무선랜 보안 법제 개선) 무선AP 및 무선랜 사용시 보안 강화를 위한 법제도 개선

- 무선AP 제조·판매업자의 제품 출고시 보안설정 권장 문구표기 및 이용자에게 제공하는 무선 AP의 보안 설정 권고 규정

- 무선랜을 내부용으로 사용하는 기업이용자가 보유하는 고객의 개인정보보호를 위해 기업이용자의 무선랜 정보보호조치 구체화

※ 「정보통신망법」 제28조에 따른 ‘개인정보의 기술적·관리적 보호조치 기준’(고시)

- 인터넷전화 서비스 제공자(VoIP), 상용 무선 인터넷서비스제공자(ISP), 유·무선 공유기 제조·판매업자 등 사업자의 무선랜 보안사항 규정

※ 정보보호지침(안전진단 기준)에 무선랜 관련 항목 강화 및 「전파법」에 따른 ‘무선설비규칙’ (고시)에 반영

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 원클릭 무선랜 보안설정 솔루션 도입	■	■				제조사, 정부·유관기관
	○ 무선랜 보안 종합포털 구축	■	■				정부·유관기관
	○ 무선랜 보안 법제 개선	■	■				정부·유관기관
중기	○ 이용자 보안 인식제고를 위한 홍보 강화	■	■	■			정부·유관기관
장기	○ 공중 무선랜 보안관리 강화	■	■	■	■		이통사, 정부·유관기관

나. 유·무선 연동구간 보안성 강화

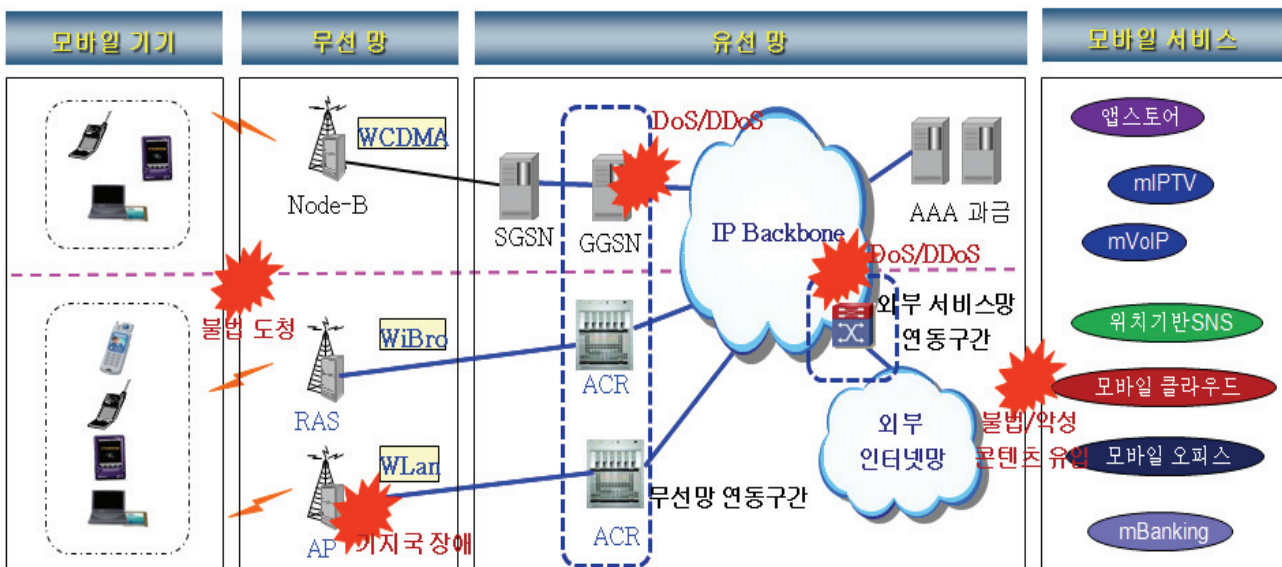
개 요

- ◇ 모바일 인터넷 망과 IP 백본망과의 연동망 구간에 네트워크 침입 탐지 및 대응시스템 구축 등을 통하여 연동구간의 보안성 강화

□ 배경 및 필요성

- 모바일 서비스 활성화를 위해 자유롭게 서비스를 제공할 수 있도록 서비스 망이 개방형 구조로 확대 추세이나
 - 연동 구간에서의 일부 장애 발생은 자칫 광범위한 지역에 걸친 모바일 인터넷 서비스 장애로까지 피해 범위가 확산될 우려
- 악성코드 감염 등으로 인한 내부 GGSN 구간 및 외부인터넷 서비스 망과 IP 백본망이 연계되는 구간 등의 DDoS공격 등 보안위협 존재
 - ※ GGSN(Gateway GPRS Supporting Node) : 이동통신망에서의 데이터 트래픽을 인터넷망과 같은 패킷교환망으로 연결시키는 통로 역할
 - 외부 인터넷 서비스 망으로부터 불법·사행성 콘텐츠 유통도 우려

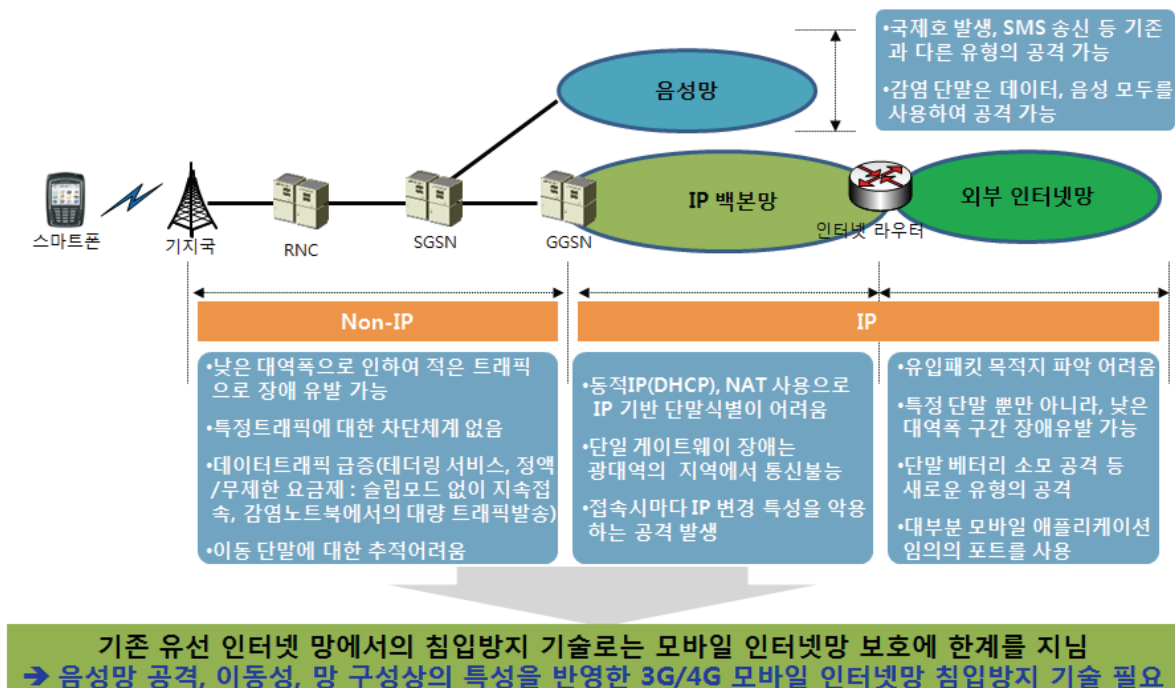
【 유무선 연동구간 및 유선 네트워크 보안 위협 】



□ 추진 내용

- (이동통신망내 보안위협 분석) 이동통신망 내 무선망과 IP 백본망간 연동 등에서 침해사고 예방·대응모델 연구 지원
 - 이동통신사가 관리하는 내부 무선망 내에서의 발생 가능한 침해 사고 위협 예방·대응 모델 연구
 - 다양한 망과 연동되는 환경에서 사이버 공격 탐지·차단 및 공격자 추적을 위한 '통합 침해사고 대응시스템' 도입
- (연동 게이트웨이 침해사고 대응) 이동통신망내 내·외부 연동 게이트웨이에 대한 침입 탐지 및 대응시스템 구축 유도
 - 이동통신망내 무선망과 IP 백본망간 연동 구간에 대한 DDoS 공격 등 침해사고 대응을 위한 침입 탐지 및 대응 기술 확보
 - 이동통신사가 관리하는 IP 백본망과 타 ISP가 관리하는 외부 인터넷망간 연동 등에 있어서 공격 위협 및 대응 모델 연구

【 기존 유선 인터넷 망에서의 침입방지 기술 한계 】



- (외부 인터넷망간 보안체계 마련) 이동통신 사업자들 간의 외부 인터넷망 연동 및 무선 인터넷 연결에서의 보안체계 구축
 - 외부 인터넷망으로부터의 유입되는 비정상적인 트래픽을 신속히 탐지하고 차단하는 보안체계 강화
 - 외부 인터넷망간 연동 구간에서의 서비스 장애를 방지 및 조기 차단·복구하기 위한 장애방지체계 도입
 - (신규 보안 위협 대응) 신규 보안취약점에 대비한 유·무선망 보안기술 및 침해사고 대응시스템 고도화 지원
 - 모바일 서비스 이용 단말(스마트폰, 스마트패드 등)의 악성코드 감염 예방·탐지 및 차단 대응체계 구축
 - 이·변종 악성코드 등장, 고도화된 해킹기법 등 점차 지능화되는 공격 및 다양한 신규서비스의 보안취약점 대응강화 방안 마련
 - 불법 서비스 트래픽을 무선기지국 및 연동 게이트웨이 단에서 탐지 및 차단할 수 있는 점검 체계와 그에 따른 보안 정책 마련
- ※ 모바일 서비스 및 데이터 특성을 반영한 불법·악성 서비스를 탐지하고, 차단할 수 있는 기술을 산·학·연 공동으로 기술개발 추진

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 이동통신망내 보안 위협 분석						이통사
	○ 연동 게이트웨이 침해사고 대응						이통사
	○ 외부 인터넷망간 보안체계 구축						이통사
중기	○ 신규 보안 위협 대응						정부·유관기관, 이통사

가. 모바일 오피스 보안 체계 마련

개 요

- ◇ 스마트워크의 대표적 유형인 모바일 오피스의 성공적 도입 및 기반 조성을 위해 예상 보안이슈에 대한 사전 대응체계 마련

□ 배경 및 필요성

- 최근 정부는 스마트워크 활성화를 위해 ‘스마트워크 인프라 고도화 및 민간 활성화 기반 조성(안)’을 발표('10.7.20)
 - 2015년까지 전체 공무원의 30%와 전체 노동인구의 30%까지 ‘스마트워크’ 근무율을 높여나갈 계획임
 - ※ 스마트워크(Smart work) : 종래의 사무실 개념을 탈피하여, 언제 어디서나(Anytime, Anywhere) 편리하게 효율적으로 업무에 종사할 수 있도록 하는 미래 지향적인 업무환경 개념으로 모바일오피스, 스마트워크센터, 재택근무 등 이용
- 최근 민간업계도 스마트폰을 이용한 모바일 오피스 등을 새로운 비즈니스 모델로 주목하는 등 도입 여건이 성숙되고 있으나,
 - 스마트폰의 개방성, 이용자의 이동성 및 SNS 등 신규 서비스와 연계 등에서 다양한 보안 취약점에 노출될 우려
 - 회사 내부망과 모바일 단말 사이의 통신시 트래픽 도청, 해킹 등을 통한 권한 없는 접근 및 정보유출 발생 가능
 - 단말기 분실로 인한 기업 내부정보 유출 및 내부 업무망 접근이 가능하여 모바일 오피스 도입의 가장 큰 저해 요인으로 인식
 - ※ 삼성경제연구소 CEO 설문조사 결과, 모바일 오피스 도입을 우려하는 가장 큰 이유로 경영자의 47.9%가 보안문제를 지적(출처 : 삼성경제연구소, '10.5월)

□ 추진 내용

- (가이드라인 마련) 스마트워크 확산을 지원하기 위해 모바일 오피스를 포함한 스마트워크 정보보호 가이드라인 마련·보급

< 스마트워크 정보보호 가이드라인 추진내용 >

구분	주요내용
관리적 보안	스마트워크 서비스 이용 시 정보의 취급 및 침해사고 대응절차 등
기술적 보안	스마트워크 단말기, 네트워크 인프라, 애플리케이션 보안 등
이용자 보안	스마트워크 이용자 보안교육, 정보자산 취급 및 관리 등

- (법·제도 개선) 민간부문의 모바일 오피스 도입 활성화를 위한 각종 보안 관련 법제도 정비
 - 모바일 오피스 사업자의 법적 책임 명확화와 이용자의 개인정보 보호를 위한 법제도 개선
 - 개인정보 제공 또는 위탁에 대한 통일된 법적 근거, 개인정보 유출·유실 시 배상방안 등에 대한 법적 기준 마련 등
 - ※ 필요시 정보통신망법, 통신비밀보호법, 위치정보보호법, 산업기술유출방지법 등의 개정을 통해 모바일 오피스 보안 환경 조성
 - 모바일 오피스를 구성하는 기술 및 제품의 보안성 평가를 위한 기준 제시 및 인증제도 개선
 - ※ 시스템 안전진단 등을 위한 ISMS, PIMS와 같은 인증 체계 구축을 통해, 정부 및 기업의 모바일 오피스 안전성 점검 및 강화
- (모범사례 발굴 및 확산) 보안성을 고려한 모바일 오피스 실제 도입의 모범사례(Best Practice)를 발굴 및 홍보하여 모바일 오피스 확산 환경 조성
 - 전자문서, 이메일을 통한 업무처리 환경에 따른 기록의 보존(Archiving) 및 관리, 개인정보보호, 주요 인프라의 효과적 보안 등 기업의 IT 컴플라이언스(Compliance) 준수

- (모바일 오피스 보안 테스트 환경 구축) 모바일 오피스 보안 기술의 테스트 환경을 구축·제공하여 민간의 기술 개발 지원
- (단말 보안) Ad-hoc 방식 접속 차단 보안장비, 데이터 수발신 정보 기록 시스템, 업무 문서나 메일 등의 저장 공간 최소화 및 기기 분실 시 원격 처리 기술 등
- (시스템 보안) 회사 내부망과의 통신 시 데이터 암호화, 애플리케이션·서버의 보안 강화 기술, 서버와 사용자간 상호 인증체계
 - ※ 안전한 모바일 오피스 보안체계에는 사용자·서버 인증 구비, 통신 구간의 도청 방지를 위한 SSL-VPN, IPSec VPN 등 암호화 통신체계 구축 필요
- (취약점 분석) 모바일 오피스 환경에서의 상황별, 레이어별 보안 취약점 분석 및 대응방안 마련

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 보안 가이드라인 개발·보급	■					정부·유관기관
	○ 모바일 오피스 법제도 개선	■	■				정부·유관기관
중기	○ 모바일 오피스 모범사례 발굴 및 확산		■	■	■		정부·유관기관 이통사 등 서비스업체
장기	○ 모바일 오피스 보안 테스트 환경 구축		■	■	■		이통사 등 서비스 업체

나. 모바일 SNS 보안 강화

개 요

- ◇ 신뢰관계를 기반으로 하는 실시간 소통채널인 SNS의 보안 위협에 대응해 안전 이용 가이드라인 마련, 보안 교육, 기술적 대책 마련 등 안전한 모바일 SNS 환경 구축

□ 배경 및 필요성

- 트위터, 페이스북 등 SNS(Social Network Service)를 통한 악성코드 유포, 피싱, 스팸 발송 등 보안 취약점 발견
 - SNS는 본인인증 절차 없이 가입이 가능하기 때문에 ID 위·변조는 물론 악의적인 목적에 의한 다량의 스팸 유포 가능
 - SNS가 DDoS공격이나 악성코드 전파를 위한 수단으로 이용되면서 모바일 단말의 좀비화에 이용 가능성 우려
 - ※ 트위터를 DDoS 공격의 명령서버로 이용한 사례 발견, 국내 미투데이를 통해 윈도우 업데이트 파일로 위장한 악성코드(악성 DLL파일) 유포 사례 발견('10. 7월)
 - 단축 URL을 이용해 피싱 사이트 및 악의적 사이트로의 연결을 유도함으로써 악성코드 감염, DDoS공격 등 위협 초래
- SNS를 통한 개인 정보의 과다 노출 및 수집, 불건전 정보유통 및 저작권 침해 등의 사회적 문제 발생 가능
 - SNS 검색 기능을 통해 프라이버시 노출이 증가되고, IP 주소, 단말기 정보, 위치정보 등 2차 정보들이 맞춤형 광고에 악용 우려
 - 개인정보가 타인에 의해 악의적으로 수집·이용될 경우 심각한 명예 훼손, 사이버 폭력 등뿐만 아니라 물리적 범죄 발생 가능
 - ※ 위치기반 SNS인 '포스퀘어(Foursquare)'가 미국 등지에서 인기가 상승하면서 개인의 위치를 파악, 빈집을 확인하고 절도하는 사례 발생

- 특히, 해외 모바일 SNS 서비스의 경우 제한적 본인확인제, 임시조치 등 국내법 적용에 논란
 - 페이스북, 트위터 등 해외 SNS 기업들은 관련 국내법의 효력이 미치지 않아 국내 이용자들의 권리침해 발생 우려가 높음
 - ※ 국내 사업자의 경우 게시글을 통한 명예훼손, 개인정보 침해 등에 대처하기 위한 권리침해 신고센터 운영 등 제도에 적극적인 반면, 해외 사업자의 경우 정확한 연락처 및 신고 프로세스가 없어 제도나 이용자 정보보호 편의측면에서 미흡

□ 추진 내용

- **(SNS 이용 안내 가이드라인)** 안전한 모바일 SNS 환경 구축 · 이용을 위한 안내서 개발 및 보급
 - SNS 이용 시 나타나는 보안위협을 분석하고 직장인 및 학생 등 대상별 알기 쉬운 안전 이용방법 · 개인정보 관리 가이드 개발 및 보급
 - 공공 · 행정기관 및 서비스제공업체 등의 정보시스템 관리자 및 보안 담당자 대상으로 업무지침 개발
- **(SNS 보안 및 윤리 교육 강화)** SNS 환경에서의 개인정보 보호를 위한 교육과 홍보를 통해 보안 및 윤리 의식 강화
 - 이용자의 적극적인 정보보호 참여 및 실천을 위한 교육 상시 실시
 - 모바일 SNS 보안 의식 고취를 위한 전 국민 대상 캠페인 전개
 - ※ 과도한 개인정보 노출 행위, 언행 자제 및 SNS 패스워드 관리 주의, 정보유출 피해 방지를 위한 보안 소프트웨어 설치 등 안내
- **(SNS 정보유출 대응 법제 개선)** 개인정보 유출사고 사전방지를 위한 개선된 법제도 마련 · 추진
 - 모바일 SNS 사업자에 대한 프라이버시 침해 위험성을 이용자들에게 사전에 알리도록 고지 의무화 추진

- ※ 개인정보 수집 시 개인정보 침해 위험성 사전 고지 및 수집 동의 방안 마련을 위해 **현행 정보통신망법상 개인정보 수집 시 의무 고지사항(수집·이용목적, 수집항목, 보유·이용기간)에 “개인정보 침해 위험성” 추가 등 검토**
- 개인정보보호 인식 및 보호방법에 미숙한 아동·청소년 등에 대한 과도한 정보 수집 제한 유도
- ※ 모바일 SNS를 통한 아동 위치정보 수집 등은 범죄 악용 우려가 있으므로 무분별한 정보 수집을 제한하는 등 아동·청소년 대상 안전한 서비스 제공 방안 마련
- 검색 엔진을 통한 SNS의 개인정보 검색에 따른 결과 제공 시 최소한의 부분적 통제를 위한 법제도 연구·마련
- SNS에서의 위치정보 및 지오태그(GeoTag) 설정 시 사용자 동의 요청·확인 의무화 추진

【 위치기반 프라이버시 보호 】



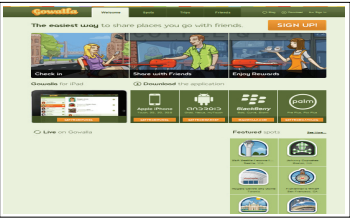
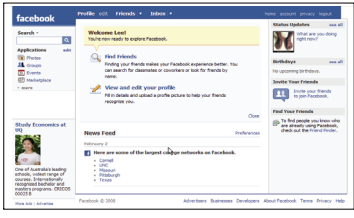
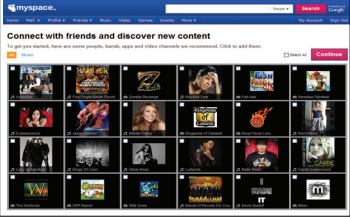
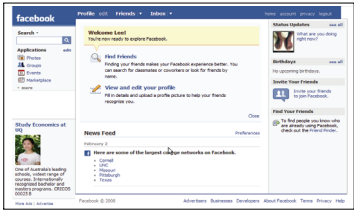
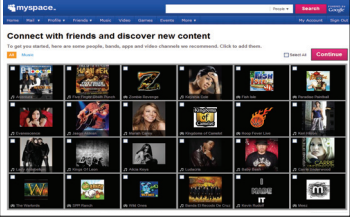
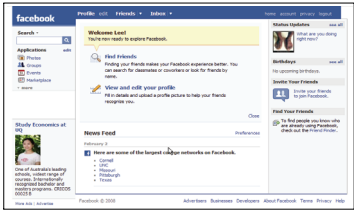
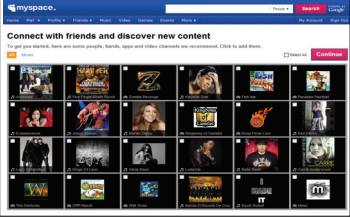
- (기술적 대응 방안 마련) 국내외 SNS 사업자와 협력하여 모바일 SNS의 취약점 보완을 위한 기술적 보호조치 강화
- 단축 URL을 악용한 악성코드 유포 및 피싱 사이트 유도 예방을 위하여 국내외 단축 URL 관련 정보 공유체계 마련
- 스팸, 피싱, 악성코드 등 불법 유해 콘텐츠의 유입 방지를 위한 지능형 자동 필터링 기술 도입 등
- 신뢰성 높은 SNS 제공을 위해 사용자 인증 기술 도입 및 제공

- (글로벌 스탠다드 마련) 관련 법제도의 '글로벌 스탠다드(Global Standard)'를 통해 글로벌 경쟁 활성화 및 이용자 보호 정책 실현
 - 해외 SNS 사업자들의 정보보호지침 준수를 위한 정부의 권고 노력 및 모바일 SNS 이용자의 권리 보호를 위한 글로벌 기준 마련 선도
 - ※ 정보보호 지침 준수 여부에 대한 지속적 관리, 삭제 권한·사고 책임소재·프로필 무단 점유에 대한 법적 책임 명확화 등 기준 제시 등
 - 국내외 SNS 사업자들이 공정경쟁 제도의 틀 안에서 사업을 영위할 수 있도록 미래지향적·합리적인 법제도 개선
 - ※ 국내 기업의 규제 역차별 문제가 발생하지 않도록 국내 규제를 국제적인 수준으로 조정하여 국외 SNS 서비스사업자를 포함한 새로운 정의 및 행위 범주에 포함, 새로운 기술 및 시대적 흐름을 반영하여 경쟁 상황에 맞게 법제도 개선 등
 - SNS를 통한 위협 발생시 공동으로 신속히 대처하기 위한 국내외 업체를 포함하는 정보보호 핫라인 마련

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ SNS 이용 안내 가이드라인 제작 및 배포	■					정부·유관기관 서비스제공자
	○ SNS 정보유출 대응 법제 개선	■	■				정부·유관기관
중기	○ SNS 보안 및 윤리 교육 강화	■	■	■			서비스제공자
	○ 기술적 대응방안 마련	■	■	■			서비스제공자
장기	○ 글로벌 스탠다드 마련	■	■	■	■		정부·유관기관

【 주요 SNS별 위협요인 】

구 분	트위터(Twitter)	고왈라(Gowalla)	포스퀘어(Four Square)
개 요	회원간 휴대폰이나 웹을 통해 최대 140자의 짧은 메시지를 실시간 주고받는 마이크로블로깅서비스	위치기반으로 일종의 아이템 찾기 게임을 제공하는 서비스	이용자의 현재위치를 기준으로 LBS, SNS, 게임의 요소를 복합적으로 제공
			
위협요인	목적의 활용 - follower들에게 공개되는 정보가 포털의 검색엔진을 통해 수집되어 유도 이용자 인식부족 - 자신의 위치정보, 사생활 정보를 무분별하게 공개 기타 - follower들의 무제한적 접근 허용	신원정보의 유출 - 이용자가 공개한 전화번호, 주소, 사진 등 유출 가능 이동경로의 유출 - 이용자의 이동경로 및 지정학적 선호도가 시간대별로 유출 가능 정보조작 - 상업적, 정치적 목적으로 특정 위치에 대한 정보를 왜곡 또는 조작	위치정보의 노출 - 위치 프로파일링이 가능하여 범죄 악용 가능 신원정보의 유출 - 트위터 등 일반적인 SNS가 가지는 개인정보 관련 위협 요인 보유
			
개 요	고등학교, 대학, 기업, 비영리조직, 군대 및 지역 커뮤니티 등을 대상으로 한 인맥구축 서비스	- 구글맵 기반의 Social Map 서비스 - 페이스북, 트위터 등과 연동 가능	음악 콘텐츠 중심의 SNS
			
위협요인	신상정보 수집 - 이용자 동의없이 인적 네트워크에 대한 정보 수집 가능 개인정보의 공개 유도 - 개인정보의 노출과 공개를 유도하는 방향으로 서비스 진행	위치정보 노출 - 위치정보기반 S/W를 통한 양방향서비스로 24시간 위치정보 노출 가능	청소년 보호장치 미흡 - 콘텐츠 특성상 청소년들이 많이 이용하지만 보호대책 미흡
			

다. 모바일 클라우드 보안 체계 강화

개 요

- ◇ 안전하고 신뢰할 수 있는 모바일 클라우드 서비스를 제공하기 위한 기술적·관리적 보호방안 마련

□ 배경 및 필요성

- 모바일 클라우드 서비스는 모바일 단말기를 통해 외부의 컴퓨팅 자원을 활용하는 서비스로, 향후 '스마트워크' 서비스 등의 기반이 되는 등 그 역할과 중요성이 증대

※ 세계 시장규모 '09년 4억달러→ '14년 95억달러로 급성장 전망(Juniper Research, '10.2월)

- 이용자 정보를 집약해 저장하고 이동성을 제공하는 모바일 클라우드 서비스 환경의 특성상 데이터 유실이나 유출에 대한 위험 존재

- 클라우드 환경 관리소홀 및 보안취약성으로 인한 악성코드 감염으로 저장정보 유출 및 서비스 가용성 제한

- 다양한 클라우드 서비스 제공을 위한 3G, Wibro, Wi-Fi 등 무선 통신구간에서의 보안위협으로 인한 정보유출 가능

- 모바일 클라우드 서비스의 활성화를 위한 신뢰성 확보 필요

- 모바일 클라우드 서비스의 안전성 확보 및 인식제고를 위한 기술적·관리적 보호조치가 요구

- 특히, 서비스 초기단계인 현시점에서 활성화를 위한 안전한 모바일 클라우드 서비스 제공 기반을 마련할 필요

※ 미국 18세 이상 성인 2,200여명을 대상으로 조사한 바에 따르면, 클라우드 컴퓨팅 서비스 이용자 가운데 90%가 개인정보 유출 우려(P&A Project, '08년)

□ 추진 내용

- (모바일 클라우드 보안기반 마련) 모바일 클라우드 통합 인증 체계 마련 및 침해사고 대응능력 강화
 - 모바일 클라우드 인증 표준 기술 개발 및 이기종 모바일 클라우드 플랫폼 간 상호운용성 확보를 위한 **통합인증 체계 구축**
 - 모바일 클라우드 서비스 제공자의 폐업·파산·물리적 시스템 파손에 따른 이용자 데이터 유실 방지를 위한 **백업 시스템 구축 의무화**
 - 모바일 클라우드 서비스에서의 보안침해사고 책임추적성 확보 및 신속한 대응을 위한 「**모바일 클라우드 포렌식**」 기술 개발
 - 송수신 데이터의 비밀성·무결성 보장을 위한 모바일 클라우드 단말과 클라우드 서버 간 **보안채널 개발** 및 안내서 마련
- (서비스 표준화 및 인식제고) 모바일 클라우드 서비스 이용자 보호를 위한 서비스·정책 표준화 및 사용자 교육
 - 모바일 클라우드 서비스 유형, 정보의 민감도 등에 따라 차등화된 보안 서비스를 제공하기 위한 표준 SLA 가이드라인 마련 및 배포
 - ※ 모바일 클라우드 서비스 제공자는 서비스수준 계약서(Service Level Agreement, SLA)를 통해 사용자가 기대하는 보안수준의 서비스 제공을 보장
 - 모바일 클라우드 서비스 제공자로 하여금 사용자 보안 인식제고를 위한 안내서 또는 가이드라인 제작·배포 유도
 - 국내에 서비스를 제공하는 국내외 사업자에 대한 보안 및 개인 정보보호와 관련한 관리적·기술적 법적 기준 마련
 - ※ 국외에 서버를 두고 국내에 모바일 클라우드 서비스를 제공하는 사업자에 대한 명확한 정보보호 관리체계 마련 등

- (신종위협 정보 공유) 모바일 클라우드 서비스 제공자간 신종 위협 정보 공유 및 신속 대응을 위한 종합적인 보안 침해대응체계 마련
 - 모바일 클라우드 모범사례 발굴 및 보안 테스트베드(Test-bed) 구축을 통한 관련 정보 공유
- ※ 모바일 클라우드 서비스의 보안 테스트베드 구축 및 정보공유 단계
- (1단계) 정보공유 요구사항 추출 및 분석을 통한 공유체계 시범구축 ('11년)
 - (2단계) 관련 대형 모바일 클라우드 제공업체 대상 先 적용 ('12년)
 - (3단계) 기 구축된 정보공유체계의 노하우 및 DB를 중소기업과 공유 ('13년)
- 모바일 클라우드 서비스에서의 악성코드 전파 현황 및 코드 분석 등 정보 공유 및 지속적 모니터링 실시
 - 기술적·관리적 차원에서 모바일 클라우드 침해대응체계를 개발하고 영세한 중소 클라우드 서비스 업체에 관련 기술 이전

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 서비스 표준화 및 인식제고						정부·유관기관
중기	○ 모바일 클라우드 보안기반 마련						서비스제공자
장기	○ 신종위협 정보 공유						정부·유관기관 서비스제공자

라. 스마트 TV 보안 체계 구축

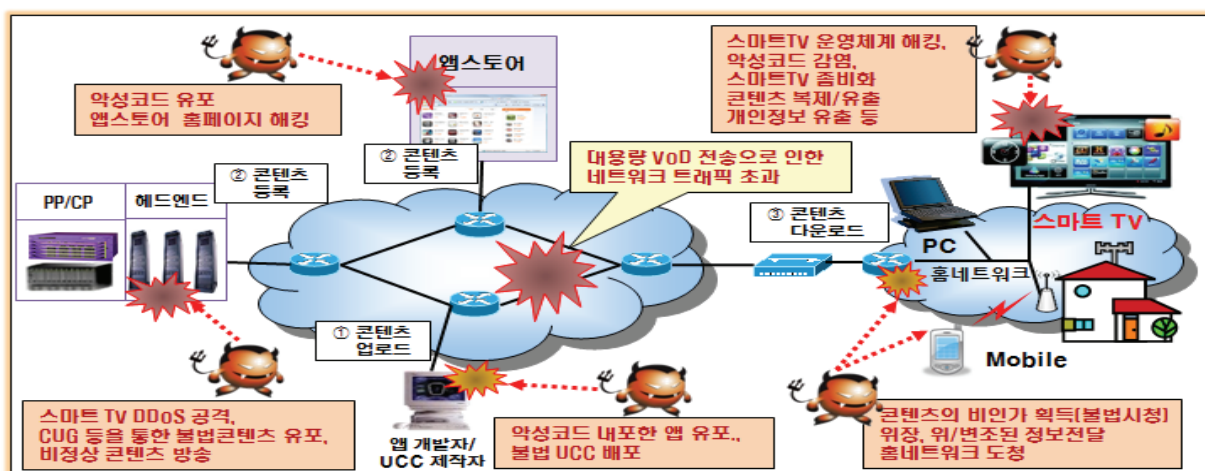
개 요

- ◇ 인터넷에 연결된 TV를 통해 양방향 방송서비스 시청이 가능한 스마트 TV는 스마트폰과 태블릿 PC 등과 이어진 N스크린 전략의 중요한 핵심으로 부각
- ◇ 앱을 통한 악성코드 유포, 콘텐츠의 불법유통, 네트워크 취약성 공격 등의 보안위협이 발생할 가능성이 있어 서비스·네트워크, 디바이스, 콘텐츠, 개인정보 차원에서의 보안대책 강구

□ 배경 및 필요성

- o 스마트TV는 셋톱박스를 활용하지 않고 TV내 별도 OS를 구현하여 앱스토어를 비롯한 다양한 서비스를 제공
 - 기기, 서비스·네트워크, 콘텐츠, 개인정보에 대한 신규위협 발생 가능
 - 기존 인터넷망 보안위협인 콘텐츠 비인가 획득, 정보유출 및 위장, 패킷 도청, 재전송 공격 등이 스마트TV에서도 재현 가능

【 스마트 TV 정보보호 위협 개념도 】



【 스마트 TV 정보보호 위협 】

구분	위협 종류	내용
스마트TV 기기 위협	○ 스마트 TV 시스템 해킹	○ 스마트 TV 운영체제, 응용프로그램(웹 브라우저 등)의 취약점을 악용한 시스템 해킹 공격 - 스마트 TV의 잠비화 - 콘텐츠 불법 복제 및 유출, 사용자 정보 획득
	○ 개인인증정보 유출/공유	○ 편리한 사용을 위해 스마트TV 내에 인증정보 저장 - 도난 등 발생시 인증정보 남용 가능성 - 가족내 사생활 보장 불가
	○ 탈옥을 통한 위협노출	○ 탈옥을 통한 개인화 과정에서 스마트TV 제공자가 제공한 기본제공 보호장치 해제 - 성능향상을 위한 조작으로 보안위협 증가
서비스 및 네트워크 위협	○ TV 앱스토어를 통한 악성코드 유포	○ TV 앱스토어를 통한 악성코드, 바이러스가 감염 파일 유포 - 악성코드 감염에 따른 스마트 TV 잠비화 - 결제정보, 사용자 정보 등 획득
	○ TV 앱스토어 웹사이트 공격	○ 앱 스토어 운영 사이트 공격 - 콘텐츠 불법 유출, 사용자 정보 획득 - 사용자의 앱스토어 접근 방해
	○ 스마트 TV DoS 공격	○ 스마트 TV를 악용한 네트워크 장비, 주요서버에 대한 DDoS 공격으로 방송 및 인터넷 서비스 마비 - 잠비 스마트TV를 통한 DDoS 공격
	○ 홈 네트워크 도청	○ 적절하게 보안되지 않은 홈 네트워크에 접근 - 콘텐츠 불법 복제 및 유출 - 사용자 정보 획득
	○ 응용서비스 취약성	○ 스마트TV에서 제공하는 응용서비스의 취약성으로 인한 위협 - 취약성을 공격하여 악성코드 감염 - 결제정보, 사용자 정보 등 획득
	○ 대용량 VoD 사용으로 인한 트래픽 초과	○ VoD 중심의 서비스는 대용량의 네트워크 대역폭을 소진하기 때문에 네트워크 용량 초과 위험 - 네트워크 품질 저하 또는 사용불가 위험
콘텐츠위협	○ 콘텐츠 불법시청	○ 스트리밍 방식이나 다운로드 방식을 통한 VoD 시청 시 불법 패킷 가로채기를 통해 불법시청 - CAS/DRM을 적용되지 않은 콘텐츠 불법시청 가능
	○ 비정상 콘텐츠 방송	○ 스마트 TV 제어권을 탈취하거나, 특정사이트 연결 유도를 통해 공격자가 원하는 방송 강제방영 - 사용자 시청권 방해, 서비스 사업자 피해
	○ CUG / UCC	○ CUG(Close User Group) 및 UCC를 통한 불법 콘텐츠 유통 - 콘텐츠 불법 유통
개인정보 위협	○ 맞춤형 서비스로 인한 개인정보 수집	○ 맞춤형 서비스 제공을 위한 개인정보 유출 - 사용자에게 따른 이용패턴, 사용내역 등 개인정보 수집
	○ SNS 서비스 도·감청으로 인한 개인정보 유출	○ SNS 서비스 이용 도·감청으로 인한 개인정보 유출 - 사용자의 인맥, 관심분야 등 개인정보 유출
	○ 개인 건강정보 유출	○ 스마트TV를 통한 원격진료 등의 서비스 도청 - 병명, 병력 등 개인 건강정보 유출
	○ 사생활 도·감청	○ 화상회의 및 영상통화 도·감청 - 통화 내역, 회의 내역 등 사생활 정보 유출
	○ 거래정보 유출	○ 스마트TV를 사용한 상거래(T-커머스) 도청 - 신용카드 번호, 금액, 물품정보 등 거래정보 유출

□ 추진 내용

- **(서비스 및 네트워크 보호 강화)** 스마트TV 서비스 및 네트워크 보호를 위한 기술적 조치를 강화하고 정보보호 관리체계 마련
 - TV 앱스토어에 대한 주기적인 보안 취약점 점검 및 웹방화벽 등 해킹방지 솔루션 적용 지원
 - 콘텐츠의 업로드시 악성코드 사전분석 절차 마련 의무화 및 비인가자의 침입차단·방지 등 정보보호 솔루션 적용
 - N스크린 서비스를 위해 구축된 홈네트워크의 비인가 접근 및 도청을 방지하기 위한 기술 개발
- **(스마트TV 디바이스 보호체계 마련)** 스마트TV 시스템 보호를 위한 스마트TV 기기의 안전점검 및 진단 체계 마련
 - 스마트 TV의 접속 시 중앙 서버와의 사용자 인증강화 및 악성코드 차단 솔루션을 기본 탑재하여 판매 유도
 - 스마트 TV 운영체제 취약점 분석 및 패치 개발과 함께 자동 보안 패치 설치 방안 마련
- **(콘텐츠 보호방안 추진)** 콘텐츠 특성에 따른 접근제어, 복제방지 솔루션 적용 및 관리지침 마련 등 보호방안 마련
 - 콘텐츠의 불법적인 사용·전달·삽입 방지 및 불법 콘텐츠 추적 등을 위한 DRM, 지문기능(Finger Printing) 등 보안솔루션 적용
 - 영상 콘텐츠의 프라이버시 및 저작권 분쟁 방지, 콘텐츠 불법 유출 방지를 위한 접근제어 및 보안기술 적용 등 보호대책 마련
 - CUG(Close User Group)이나, UCC를 통한 불법 콘텐츠를 주기적으로 조사 및 조치하는 관리지침 마련

- (개인정보 보호방안 마련) 스마트TV를 통한 개인정보 수집·유출 방지 기술 도입 및 방안 마련
- 스마트TV의 맞춤형 서비스를 위한 사용자 정보 수집 범위 및 권한을 한정하는 가이드라인 마련
- 원격진료 등 신규 서비스 도입 시 개인정보 수집 및 유출 가능성 차단을 위한 기준 및 절차 개발
- 화상회의, 영상통화 등 영상과 음성을 주고받는 서비스의 통신 과정 및 상거래(T-커머스) 내용을 암호화하는 기술 적용

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 개인정보 보호방안 마련						정부·유관기관 및 서비스제공자
중기	○ 스마트TV 서비스 및 네트워크 보호 강화						서비스제공자
	○ 스마트TV 디바이스 보호체계 마련						서비스제공자
장기	○ 콘텐츠 보호방안 추진						정부·유관기관 및 서비스제공자

마. 모바일 뱅킹 보안 기반 조성

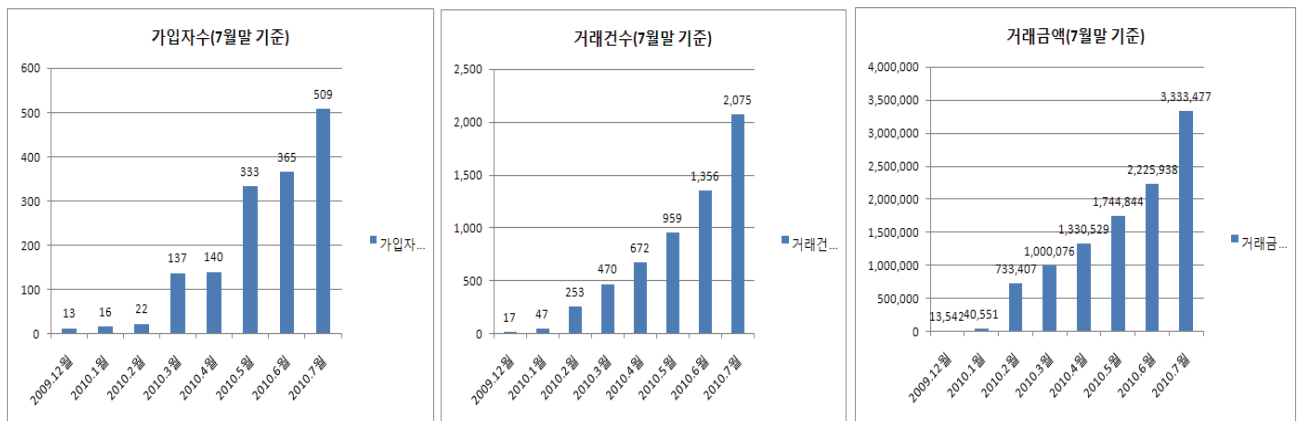
개 요

- ◇ 스마트폰 등을 이용한 모바일뱅킹 이용자가 크게 증가할 것으로 예상되므로 안전한 이용을 위한 보안 기반 조성
 - ※ 모바일 뱅킹 : 금융 업무에 IT를 적용하여 자동화·전자화를 구현하는 전자금융의 수단으로 일반적인 은행거래와 증권, 상거래 등을 포괄

□ 배경 및 필요성

- '10년 2/4분기의 국내 모바일뱅킹의 일평균 이용건수는 262만건이며, 일평균 자금이체 금액은 4,078억원 규모
 - ※ 전체 인터넷뱅킹 이용건수(일평균 3,291만건)의 8.0%를 차지하며, 이체 금액(일평균 29조 9,548억원) 대비 1.4% 수준(한국은행, '10.7.27)
- 특히, '09년말 스마트폰을 이용한 전자금융서비스가 본격적으로 도입됨에 따라 모바일뱅킹 이용자는 더욱 급증할 것으로 전망

【 국내 스마트폰 전자금융거래 현황 】



(출처: 금융감독원, '10년 7월말 기준)

- ※ 스마트폰 전자금융거래 가입자 수 : 1,535 천명(월평균: 192천명),
- 스마트폰 전자금융거래 거래건 수 : 5,850 천건(월평균: 731천건),
- 스마트폰 전자금융거래 거래 금액 : 10,422,364 백만원 (월평균: 1,302,796백만원)

- 그러나 최근 모바일 뱅킹 이용이 급증하면서 다양한 보안위협도 대두
 - 오픈마켓 및 P2P를 통해 전파되는 금융 애플리케이션을 가장한 피싱 프로그램에 의한 중요 금융거래정보 노출 및 악성코드에 의한 중요 금융거래정보의 탈취 가능성 우려
 - 루팅(rooting) 및 탈옥(jailbreak)등 플랫폼 변조에 의한 관리자 권한 획득으로 플랫폼 보안기능 우회 등의 보안위협 증가

□ 추진 내용

- (모바일 뱅킹 보안성 연구·개발) 신규 모바일 기기 출시에 따른 모바일 뱅킹서비스 보안성 연구 및 보안 취약성 분석기술 개발
 - 태블릿 PC, e-Book 등 신규 모바일 기기의 분석환경을 구축하고 보안성 기술 연구개발
 - 각 플랫폼별 보안 취약성 분석기술을 개발하고 모바일에 탑재되는 보안제품의 모바일 뱅킹 안정성 연구
- (모바일 뱅킹 보안가이드 개발) 안전한 스마트폰 뱅킹 제공 및 이용을 위한 보안가이드 개발 및 보급
 - 스마트폰 뱅킹서비스 보안위협 대응방안 연구를 바탕으로 모바일 뱅킹 보안가이드를 개발하고 홍보 및 안내
- (모바일 뱅킹 보안취약성 점검) 금융당국과 공조하여 금융기관에서 제공하는 모바일 금융서비스의 안전성 및 보안취약성 점검
 - 뱅킹을 비롯한 증권거래, 모바일 소액결제, 보험, 카드 등 금융기관에서 제공하는 신규 금융서비스의 보안 취약성 점검을 확대
 - 취약점 발견시 관련 보안 정보 제공 및 개선 조치 지원

- (H/W기반 금융보안모듈 프레임워크 개발) 하드웨어 기반 모바일 뱅킹 보안 프레임워크(TuFI) 개발 및 표준화 지원
 - 모바일 뱅킹을 위해 필요한 주요 정보를 저장하고 단말기 운영 환경을 보호하기 위해 인증메커니즘 및 지급결제 프로토콜 개발 등
- ※ TuFI 모듈: Trusted u-Financial Infrastructure의 약어로서 전자금융거래를 위해 필요한 주요 정보를 저장하고, 단말자체의 운영 환경을 보호(SW 위·변조 방지) 하기 위한 메커니즘을 보유한 하드웨어 모듈
- (안전한 온라인 ID 관리체계 조성) 모바일 환경에 적합한 인증서비스 이용환경 개선과 이용이 쉽고 상호운용이 가능한 국내 온라인 ID 생태계(Identity Ecosystem) 구축
 - 다양한 인증기술의 활성화 및 국내 경쟁력 제고를 위한 모바일 전자인증 전략 로드맵 개발 등 추진
 - 사용자 중심의 안전하고 편리한 온라인 ID 서비스 체계 마련
 - 국내 온라인 ID 생태계 프레임워크 개발 및 운영을 위한 산·학·연·관 간의 협력체계 구성

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 모바일 뱅킹 보안가이드 개발						정부·유관기관
중기	○ 모바일 뱅킹 보안성 연구·개발						이통사 등 서비스 업체
	○ 모바일 뱅킹 보안취약성 점검						정부·유관기관
장기	○ H/W기반 금융보안모듈 프레임워크 개발						정부·유관기관
	○ 안전한 인증기반 및 온라인 ID 생태계 조성						정부·유관기관

2. 모바일 이용자 프라이버시 보호 확립

4. 모바일 개인정보 및 위치정보 보호 강화

가. 모바일 개인정보 보호

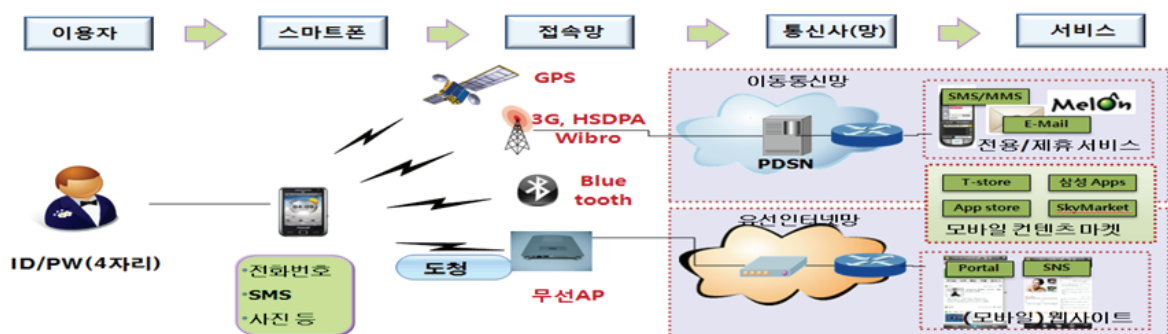
개 요

- ◇ 스마트폰 등 모바일기기에서 이용되는 S/W 개발이나 휴대 단말 제조사 개인정보보호 권고 제시 및 S/W의 프라이버시 안전성 검증체계 구축

□ 배경 및 필요성

- 인터넷 이용이 스마트폰, 스마트패드 등 모바일 환경으로 확산되면서 무선인터넷 환경에서의 개인정보 유출 위험성도 증대 추세
- 다양한 인터넷 접속환경으로 인한 악성코드 감염 및 개인정보 유출 경로가 다양화
- SNS를 스마트폰 등에서 이용하면서 이를 통해 자신의 정보를 기본으로 제공하는 방식으로 인해 개인정보 노출이 심화 가능

【 무선인터넷 환경에서의 개인정보 침해 】



- 전화번호, SMS, 사진 등 정보 열람 시 4자리 비밀번호는 취약
- 중요 개인정보에 접근 제한하는 접근 통제수단 미비
- 무선AP 망을 통해 통화 시 암호화 통신기능이 없어 도청 가능
- 스마트폰 분실 시 저장된 개인정보 등 유출 가능

□ 추진 내용

- (개인정보보호 수단제공 및 관리책임 강화) 스마트폰 등 모바일 단말의 개인정보 보호 수단을 제공하고 비밀번호 설정 등 관리
 - 제조사 및 서비스제공자가 휴대 단말기 내에 저장된 개인정보 저장시 암호화 기능 제공
 - 전화번호부, 사진 등 주요 개인정보 접근 시 안전한 비밀번호 (암호키, PIN 설정 등) 기능 제공
 - 스마트폰 분실 또는 도난 시 개인정보 유출 방지를 위해 원격 삭제 기능 제공
- (앱 및 기기 제조시 개인정보보호 권고) 스마트폰 S/W 개발 및 휴대 단말 제조 시 개인정보보호 권고 제시
 - 애플 앱스토어, 안드로이드 마켓, T-스토어, 슈퍼 앱스토어 등을 통해 판매되는 프로그램 개발시 개인정보보호 권고 제시
 - 휴대 단말기 제조시 개인정보의 이용, 저장, 관리 등에 있어 개인정보보호 강화에 필요한 최소기준 제시
 - ※ 휴대 단말기 내 본인 개인정보의 통제권을 소유자에게 부여하는 기준 제시
 - 개인정보 종류, 수집목적, 수집기간 등 고지 및 이용자 동의 획득 절차의 공통 형식 제공
 - ※ 휴대 단말기의 앱 프로그램 개발 시 활용할 수 있는 공통 형식을 개발자에게 배포
- (개인정보침해 신고 및 보호수단 이용 편의성 제고) 모바일 인터넷 이용 환경에 적합한 이용자 편의성 제고
 - 고충발생시 전문상담 및 고충처리 창구마련을 위해 'e콜센터 ☎118'과 관련 홈페이지 등에 '스마트폰 개인정보 침해 상담코너' 운영

- 스마트폰 등 모바일 환경에서 아이핀 발급·이용이 용이하도록 UI 개선, 모바일용 표준 웹페이지 개발 등 이용 편의성 제고

※ 스마트폰에서 PC용 웹페이지에 접속하면 아이핀 이용이 가능하나 아이핀 발급·인증 팝업창이 잘려 보이는 등 이용 불편 사항을 개선

○ (앱 프라이버시 안전성 검증) 스마트폰용 앱 등 SW의 프라이버시 안전성 검증체계 구축

- 스마트폰 이용자 등을 대상으로 애플리케이션 취약점 정기 발표

※ 이용률이 높은 주요 모바일 애플리케이션에 대한 개인정보 침해 위험요소를 분석하여 정기적으로 홈페이지, 간행물 등에 게재하고 보도자료 등 배포

- 일반 응용프로그램이 악성코드를 이용하여 개인정보 수집, 생성 및 파기를 하지 못하도록 사전검증

※ 상용·무료 응용 프로그램에 대한 프라이버시 안전성 검증 기술 개발 및 앱의 안정성 관련 인증 제도의 도입

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 개인정보 보호 수단 제공 및 관리 책임 강화	■					이통사, 제조사
	○ 기기제조사 개인정보보호 권고	■	■				정부·유관기관
	○ 개인정보보호를 위한 이용자 편의성 제고	■	■				정부·유관기관
중기	○ 스마트폰 앱의 프라이버시 안전성 검증	■	■	■			정부·유관기관 및 이통사

나. 모바일 서비스의 위치정보 보호

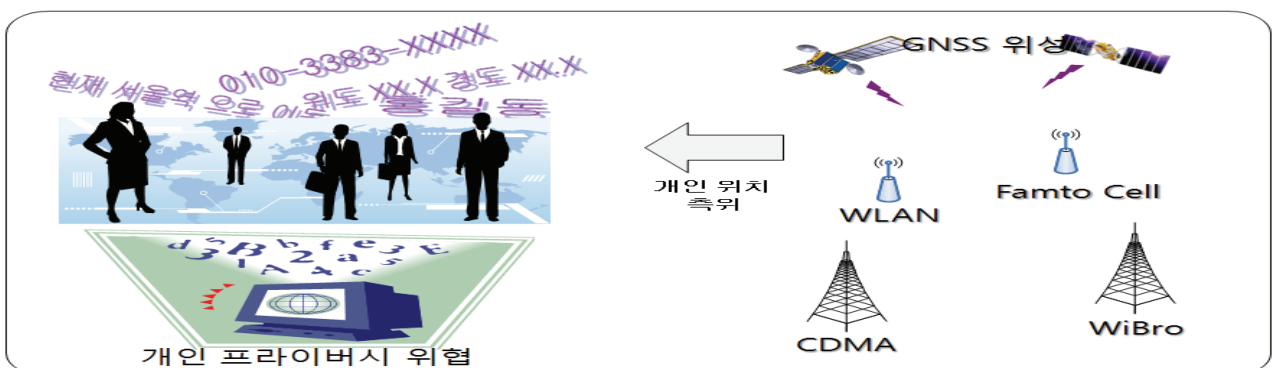
개 요

- ◇ ‘개인위치정보 자기제어시스템’을 구축하도록 하여 이용자의 자기 위치정보 통제권을 강화하고, 공공 목적의 위치정보 활용 확대에 따른 보호조치 강화

□ 배경 및 필요성

- 주변정보제공, 길찾기 등 개인의 위치정보에 기반하는 서비스가 확대되고 있으며 위치기반 광고 등 다양한 형태의 서비스 등장
 - 특히 위치기반 SNS는 타인과의 인맥관리, 정보공유 등의 사회성·이동성·실시간성과의 결합으로 이용자 확대 추세
- 위치정보의 노출로 인해 심각한 프라이버시 침해가 우려되며, 범죄에까지 악용될 가능성이 있음
 - 스마트폰에 악성코드를 설치하여 단말기를 자동으로 측위 후 3G, Wi-Fi 등을 이용하여 외부의 제3자에게 허락 없이 전송 가능
 - 특정 이용자의 위치정보를 프로파일링하여 빈집털이 등 범죄에 악용 가능
 - 위치기반 SNS의 경우도 트위터와 같이 일반적 SNS 기능을 제공하므로 개인정보의 과도한 노출·공유 등 유사한 위협요인을 내포

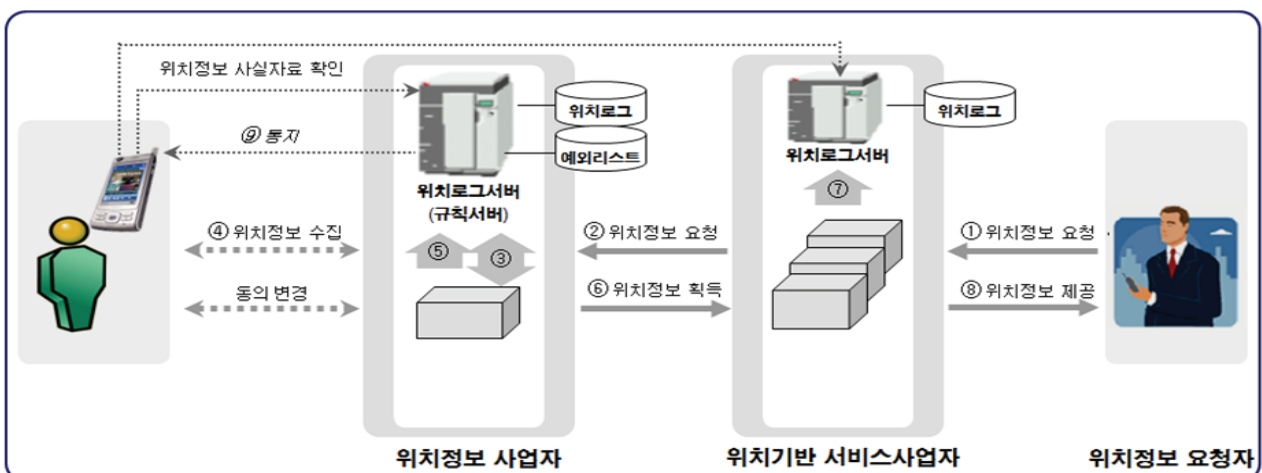
【 개인 위치 프라이버시 위협 】



□ 추진 내용

- (모바일 기기 위치정보제공 기능 설정변경) 스마트폰 등 모바일 단말에 GPS off 기능 설정
 - 국내 단말 제조사 및 이통사에 위치정보를 나타낼 수 있는 GPS를 초기에 off로 설정하도록 권고하고 이용자가 선택적으로 사용할 수 있도록 유도
 - GPS 기능을 사용하는 앱이나 서비스 이용시 자동 on/off 되도록 하거나 이용자에게 상태를 고지하도록 설정
- ※ 위치정확도에 관한 고시 법제화 등을 통해 추진하되, 법제화가 어려운 경우 정보통신기술협회(TTA) 표준으로 마련하는 방안 등 고려
- (개인 위치정보 자기제어시스템 구축) ‘개인 위치정보 자기제어 시스템’ 구축을 유도하여 이용자의 위치정보 통제권 강화
 - 위치정보사업자 및 위치기반 서비스사업자로 하여금 이용자 자신의 위치정보 사용 확인 및 설정 변경이 가능한 서비스 제공 유도
- ※ 개인 위치정보 자기제어 시스템 : 이용자가 PC나 스마트폰을 통해 언제든지 자신의 위치정보 설정 변경 및 사용내역 확인을 할 수 있는 관리시스템
- 이용자를 대상으로 개인위치정보 자기제어 시스템 활용 방법 안내

【 개인 위치정보 자기제어 시스템 개요 】



- (공공목적의 위치정보 보호조치) 긴급구조 등 공공목적의 위치정보 활용확대를 위한 보호조치 강화
 - 개인위치정보가 오·남용되지 않도록 시스템을 구축하고, 긴급구조 기관 등이 위급한 상황에 위치정보를 신속하게 활용할 수 있도록 법원 사후승인 절차를 마련

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 모바일 기기 위치정보제공 기능 설정변경	■					이통사, 제조사
	○ 공공목적의 위치정보 활용 보호 조치 강화	■	■				정부·유관기관
중기	○ 위치정보 자기제어 시스템 구축	■	■	■	■		정부·유관기관

개요

- ◇ 모바일 간편 스팸 신고시스템 구축, 지능형 스팸필터링 기능 활용 확대 등을 통해 SNS 등 신규 서비스를 통한 스팸 방지방안 강구

□ 배경 및 필요성

- 스마트폰 등 모바일 기기가 광고전송 수단으로 사용될 수 있어, 원치 않는 정보인 스팸의 발송수단으로 악용 가능
 - 사용자의 스마트폰을 악성코드에 감염시켜 모바일 봇넷을 구성 후 원격 조정하여 대량 스팸을 분산 발송할 위험 증가
 - 휴대가 용이한 스마트폰에서 기존의 휴대전화·이메일·게시판 스팸 등을 모두 경험함에 따라, 이용자가 느끼는 스팸 피로도 심화
- 국산 스마트폰이나 일반폰에는 간편 스팸신고 기능이 탑재되어 있으나 외산 스마트폰에는 동 기능이 없어 이용자 불만이 지속 제기
 - ※ 아이폰 등 외산 스마트폰에 간편 신고 및 필터링 기능 미탑재로 고객 불만 증가 (한국경제TV, '10.5.28)
- 지능형 스팸 필터링 서비스는 국내 이통 3사 모두 무료로 제공 중이나, 인지도가 낮아 아직은 이용률 저조

【 이통사별 지능형 스팸 필터링 서비스 현황('10.9월) 기준 】

이통사	SKT	LGU+	KT	합계
제공시기	'07.12월	'10.1.27일	'10.4.6일	-
전체 이용자	2,524만명	893만명	1,563만명	4,980만명
가입자 수 (전체 대비)	290만명 (11.4%)	34만명 (3.8%)	35만명 (2.2%)	359만명 (7.2%)

□ 추진 내용

- (신규 서비스의 스팸위험성 분석) 신규 모바일 서비스에서의 스팸 발생 유형 분석, 법적·기술적 대응 연구
 - 위치기반서비스(LBS)를 이용한 Push형 모바일 광고유형 조사 및 스팸위험성 분석
 - SNS별 스팸 전송기법 조사 및 국내·외 법 관할 문제, 기술적 대응방안 등 서비스 성격에 맞는 대책 수립
 - ※ Push형 광고 : 웹상의 정보를 서버가 이용자에게 밀어주는 ‘푸시 기술(push technology)’을 이용해 사용자에게 콘텐츠(광고 포함)를 제공하는 것
 - ※ 크게 ‘전송’형태의 스팸과 ‘게시’형태의 스팸이 존재할 수 있으나, 트위터의 경우 일반적인 의미의 ‘전송’, ‘게시’와 다르며, 스팸밍 기법도 매우 다양
- (스팸방지 안내서 개정) 환경변화를 반영하여 사업자나 이용자 대상 지침 변경 시 ‘스팸방지 안내서 개정’을 통해 신속히 대처
- (스팸전용신고 웹페이지 구축) 스마트폰 모바일 전용 스팸 신고 웹페이지 구축
 - 간편 신고기능이 탑재되지 않은 외산 스마트폰 등 휴대폰 이용자들을 위한 KISA 모바일 전용 스팸신고 웹페이지 구축·운영
 - ※ 스마트폰에서 무선인터넷에 연결하여 현재 신고웹페이지(www.118.or.kr)를 접속할 수 있으나, 기존 홈페이지가 그대로 보여 가독성이 떨어지는 상황
 - ※ 스팸전용신고 웹페이지와 함께 ‘e콜센터 ☎118’을 국민들이 적극 이용하도록 유도하는 등 다양한 신고 채널 확보
- (지능형필터링 활용 확대) 스마트폰에 이통사의 지능형 스팸필터링 기능 활용을 확대하고 악성코드 감염 스마트폰에서의 스팸차단
 - 이통사와 협력하여 청소년 가입자의 일괄 가입을 추진하고, 일반 이용자는 신규 가입시 기본 제공 추진

※ 지능형 스팸필터링 서비스는 이통사 서버에서 다양한 정보를 통해 스팸여부를 판단, 차단하기 때문에 이용자에게 스팸이 수신되지 않도록 함

- 초고속인터넷가입자 대상으로 Wi-Fi망 및 3G망에서 이메일발송 포트(25번) 사용 제한을 통해 스마트폰 發 스팸 차단

※ 정상이용자를 위해 메일서버/클라이언트에서 대체포트를 설정하면 메일발송 가능

【 무선망 스팸 차단】

발신망		차단 여부	차단 시기
무선랜(Wi-Fi)	초고속인터넷망	O	'11년~
이동통신망(3G)		O	'12년~

※ '09.10월 발표한 「스팸방지 종합대책」에 따라, 스마트폰 역시 SMS 1일 발송량 500통 제한 등 일반 휴대전화와 동일하게 스팸 규제를 받고 있음

- (스팸방지 법제 개선) 정보통신망법상의 스팸 규정 보완 및 사업자 약관 등을 통해 무분별한 스팸 유포 방지 등 개선책 마련

- 트위터의 경우 '트윗'이나 'DM(direct message)' 등은 모두 「정보통신망법」 스팸규정 적용이 곤란한 점을 보완

※ '트윗' 등은 '게시'의 성격을 가지고 있으나, 망법 제50조의7(영리목적의 광고성 정보 게시의 제한)의 스팸기준인 '구체적으로 밝힌 거부 의사 표시' 행위를 이용자가 하기 어렵기 때문에 스팸의 적용이 어려움

- 모바일 SNS 등에서 현행 망법의 전송과 게시행위 범주에 속하지 않는 행위를 규제의 범위에 포함하도록 추진

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 신규서비스 스팸 위험성 분석	■					정부·유관기관
	○ 모바일 스팸전용 신고 웹페이지 구축	■					정부·유관기관
중기	○ 스팸방지 법제 개선	■	■	■			정부
장기	○ 스팸방지 안내서 개정		■		■		정부·유관기관
	○ 지능형 필터링 활용 확대	■	■	■	■		정부·유관기관 및 이통사

개요

- ◇ 청소년 등에게 모바일 기기를 통해 전파되는 유해정보를 차단할 수 있도록 앱을 개발·보급하고 지속적인 모니터링 실시

□ 배경 및 필요성

- 스마트폰 등 모바일 기기는 개인화된 기기로 청소년 등이 유해 정보에 접근하기 용이한 환경을 제공
 - 사회적 안정을 저해하고, 특히 정서적 발달단계에 있는 어린이와 청소년의 건전한 도덕관념 왜곡 및 모방범죄 등 부작용 초래 우려
- ※ 최근 트위터 서비스를 이용한 음란·친북 등 불법유해정보의 유통이 확산됨에 따라 사회적 우려가 증가 (국내 트위터 이용자 : 약 111만명('10.8.31일 기준), 국외 : 1억5백77만명)
- 따라서 SNS 등 모바일 서비스의 빠른 정보 전파력을 이용한 불법유해정보 교환에 대해서는 신속한 차단조치가 중요
 - 아울러 새로운 모바일 기기를 통해 유통·확산되는 유해정보에 청소년의 접근을 사전 방지할 수 있는 적정 규제수준과 대응책 마련 필요

□ 추진 내용

- (자율규제 강화) 방심위, 이통사, 해외사업자와 협력 강화를 통해 사업자가 불법유해 정보를 신속하게 처리할 수 있도록 지원
 - 트위터 등 인터넷서비스를 이용한 음란물 유포자에 대해서 경찰청과 협조하여 적극적으로 수사가 진행될 수 있도록 지원 강화
- ※ 불법유해정보 유포자는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제73조 제74조(벌칙)에 따라 2년 이하 징역 또는 1천만원 이하의 벌금에 해당

- (모바일 콘텐츠 등급서비스) 음란·폭력 등 불건전 정보로부터 청소년을 보호하기 위해 모바일 콘텐츠 등급서비스 제공
 - ‘방송통신심의위원회’의 ‘인터넷내용등급서비스’ 기준을 준용하여 선정성, 폭력성 등에 따른 애플리케이션의 이용가능 등급 표시
 - ※ ‘인터넷등급서비스’의 등급기준 : 불건전성과 연령별로 4등급 구분
- (유해정보 차단 애플리케이션 개발·보급) 단말기 제작·출시 시 유해정보 차단 애플리케이션을 기본 설치하도록 제조사·이통사와 협의
 - 청소년 등 이용자의 연령에 따라 정보접근 가능 범위를 설정하고, SW를 실행할 수 있도록 유도
 - 외산 스마트폰 등 기본설치가 어려운 경우는 앱스토어를 통해 애플리케이션을 보급하여 선택적으로 설치하여 사용하도록 권고
- (앱 유해정보 모니터링 강화) 유통 중인 스마트폰용 앱의 유해성, 선정성 및 프라이버시 침해성 여부 등 실태 조사
 - 애플리케이션의 유해정보를 수집·분석하여 실태를 점검하고, 성인 정보 등을 구분하여 이용대상별로 제공

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 모바일 콘텐츠 등급서비스						정부·유관기관
	○ 유해정보 차단 앱 개발 및 보급						제조사, 이통사
중기	○ 유해정보 점검 및 모니터링						정부·유관기관, 이통사
장기	○ 유해정보 신속처리 등 자율규제 강화						정부·유관기관, 이통사 등

3. 모바일 정보보호 기반 조성

7. 모바일 보안기술 연구개발(R&D) 지원 확대

□ 모바일 연구개발 개요

- 모바일 공통기반, 단말·플랫폼, 무선망, 서비스, 콘텐츠에 대한 기초·원천 보안 기술 개발에 집중
 - 보안플랫폼(단말·플랫폼), 침해탐지·관제(무선망) 등 모바일 단말 및 인프라 보호를 위한 핵심 원천 기술 개발에 집중
 - 경량 암호(공통기반), 모바일 클라우드(서비스), 스마트 스크린(콘텐츠) 보안 등 스마트 모바일 서비스의 안전성 보장을 위한 기술 개발에 집중
- 민간 수요업체(보안산업체, 이동통신사 등)의 요구사항·상황을 적극 수용한 개방형 R&D(Open Research) 체계화로 진행
 - 국내외 기업, 대학, 연구소 간 연계를 통해 모바일 보안 현안 해결 및 미래 모바일 서비스 선도를 위한 보안핵심기술 발굴



가. 단말 및 플랫폼 보호기술 개발

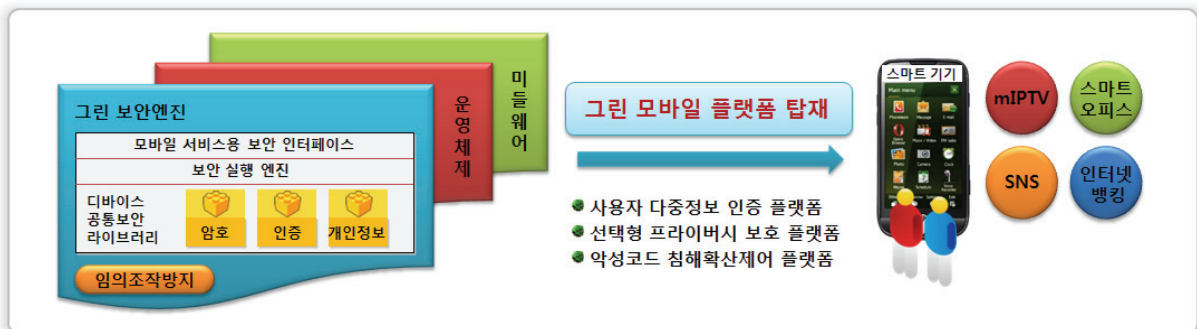
개 요

- ◇ 모바일 플랫폼에서의 보안 통제기술 개발 및 이중 무선망·서비스로의 위협 전이 차단 기술 확보

□ 배경 및 필요성

- 모바일 개방형 플랫폼 등장과 스마트폰의 급격한 보급 증가로 인해 새로운 모바일 보안 위협에 대한 우려가 고조
 - 정보 유출, 불법 접근 등 단말의 보안 위협은 응용 SW(백신 등)로 대응하여야 하나, 단말기 성능 제약에 따라 개발에 한계 야기
 - 모바일 개방형 플랫폼에 공통적으로 탑재 가능하고, 저전력·저성능 등 실행 환경을 고려한 보안 플랫폼 기술 개발 필요
- ※ '10년 2분기 시장에서 안드로이드폰(17.2%)은 아이폰(14.2%)을 앞지르며 개방형 플랫폼 보급이 점차 증가(가트너, '10.6월)함에 따라 이에 따른 대응방안 필요

【 저전력, 저성능 고려한 그린 보안 플랫폼 】



- 앱스토어 유통환경, 다양한 무선인터넷 접속 등 보안에 취약한 모바일 서비스 환경의 공격 위협이 네트워크 또는 서비스 전역으로 확산 우려
 - 모바일 단말에서 악성코드 및 해킹에 의한 단말의 임의 조작과 공격 트래픽 확산제어를 위한 보안 미들웨어 확보 필요
 - 무료 앱 다운로드 등과 같은 탈옥 스마트폰에 의한 모바일 보안 위협 확산을 방지할 수 있는 네트워크 접속제어 기술 개발 요구

□ 추진 내용

- 모바일 디바이스를 위한 그린 보안 플랫폼 기술 개발
 - 사용자 다중정보 인증 및 선택적 프라이버시보호, 모바일 단말 원격 증명 기술
 - 서비스 및 단말 환경에 따른 공통 보안 플랫폼의 경량형 동적 재구성 모듈 및 분리형 신뢰 실행 환경 기술 개발
- 임의조작을 방지하고 악성 트래픽으로부터 스마트폰 사용자와 무선망을 보호하는 기술 개발
 - 다중암호 · 인증 · APP실행검증 · 트래픽검증 알고리즘을 지원하는 초경량 저전력 **MTM(Mobile Trusted Module)** 개발

【 MTM기반 모바일 단말 보안 플랫폼 】



- TSS(TCG Software Stack) 모듈 및 MTM기반 침해단말 접속제어

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
중기	○ MTM기반 단말 보안 플랫폼 기술 개발						연구기관, 단말 제조사
장기	○ 그린 보안 플랫폼 기술 개발						연구기관

나. 모바일 인터넷 인프라 보호기술 개발

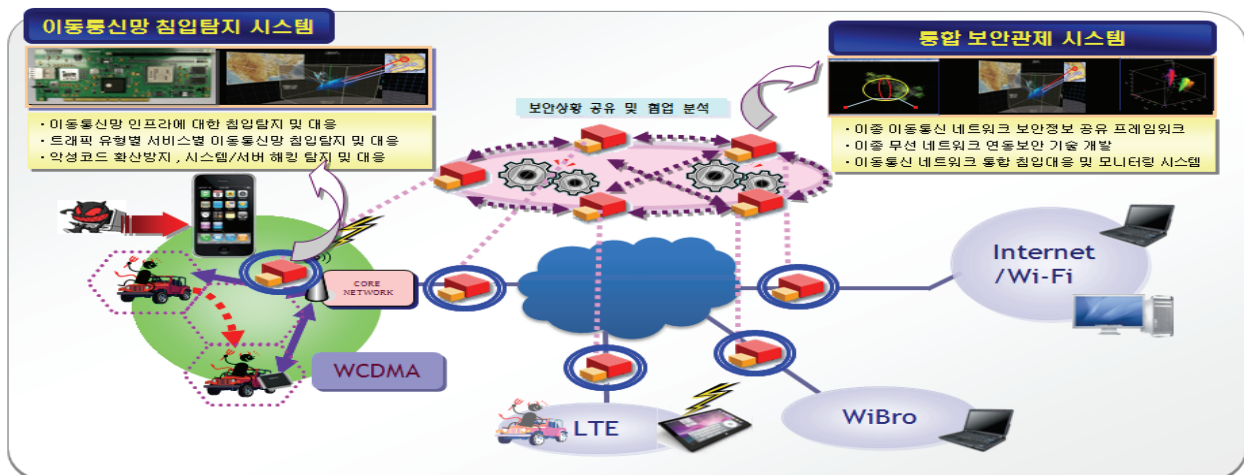
개요

- ◇ 무선 인터넷 망에서의 DDoS 등 사이버 공격 대응기술 및 유무선 통합망에서의 네트워크 인프라 안정성을 보장하기 위한 기술 개발

□ 배경 및 필요성

- 다양한 모바일 기기가 연결되는 무선인터넷 망에서의 불법 접근, 해킹 및 악성코드, DDoS 등 모바일 공격의 감시·관제 및 대응 기술 확보 필요성 대두
- WCDMA, Wi-Fi, WiBro 등 이기종 네트워크 간의 연결에 따라 망 전이에 따른 위협이 존재하며, 단일 지점의 공격피해가 전체 무선인프라로 확산될 위험 존재
 - ※ 연동(로밍) 환경에서 보안사고 발생시, 전이에 따른 대규모 피해가 예측되며 관제기능 부재로 인하여 책임소재 규명이 불명확
- 이동통신망 연동 보안 게이트웨이에서 모바일 공격의 탐지·확산 차단 및 이동통신망의 제어·관제 필요성 대두
- 감염된 스마트폰을 좀비로 만들어 스팸 및 DDoS 공격에 활용 가능함으로 이를 자동 탐지 및 대응하는 기술 확보 필요

【 이기종 무선망 침해사고 대응 및 유무선 통합 관제 기술 】



□ 추진 내용

- 무선망 및 이기종 이동통신망에 대한 침해위협 탐지·대응 기술 개발
 - Wi-Fi 네트워크 서비스 위협모델 연구 및 무선 침입탐지·대응 기술
 - WiBro 네트워크 서비스 위협모델(접근제어 라우터에 DDoS공격 등) 연구 및 DDoS 대응기술 개발
 - 이동통신망 상에서 시도되는 서비스·시스템에 대한 불법 접근, 해킹 및 악성코드 전파 등의 침해에 대한 사전 탐지기술 개발
 - 이동통신 네트워크(WCDMA/LTE) 접속형태, 사용자 행위분석, 이동통신 리소스, 좀비 스마트폰 감시를 통한 DDoS 탐지 및 대응기술
 - 이동통신망에서 서비스/시스템에 대한 불법 접근, 해킹 및 악성코드 전파행위에 대한 감시 및 관제 기술 개발
 - 차세대 이동통신 네트워크에서 PDoS 대응 등의 연계형 DDoS 통합관제 기술 개발
- ※ 무선망 인프라의 안전성 보장을 위해 트래픽 모니터링 및 분석기술을 개발하여, 무선접속 구간을 통해 통합망으로 유입되는 트래픽의 분석·제어
- 이동통신망 보안 상황정보의 공격 연관성 분석, 예상 공격패턴 분석을 통한 이동통신망 통합 보안정보 공유 프레임워크 개발

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
중기	○ 무선 침입탐지 기술 개발						연구기관, 보안산업체
장기	○ 이기종 이동통신망 침입탐지 및 대응기술 개발						연구기관, 이동통신사
	○ 이동통신망 통합보안 관제기술 개발						연구기관, 보안산업체

다. 스마트 스크린 서비스 및 콘텐츠 보호 기술 개발

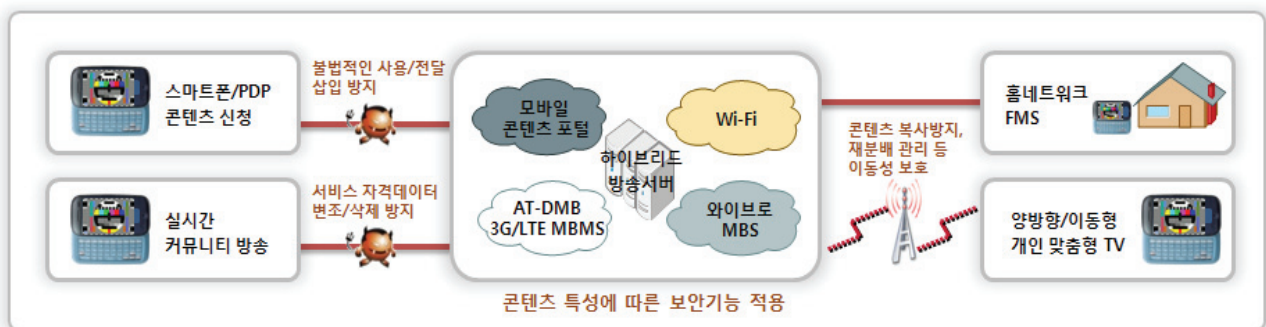
개 요

- ◇ 스마트폰, 스마트TV 등 다양한 단말을 통해 끊임 없는 서비스를 제공하기 위한 콘텐츠 보안 기술 및 콘텐츠 저작권 관리 기술 개발

□ 배경 및 필요성

- 보안 수준이 다른 다양한 모바일 단말 간에 자유로운 이동 및 소비가 가능한 스마트 스크린 서비스를 위한 콘텐츠 보안 기술 필요
 - 현재 각 사업자들이 독자적인 기술 규격을 채택하여 단말에 다수의 콘텐츠 보호 기술 탑재 시 재개발, 수정 등 큰 비용이 소모
 - ※ 현재의 콘텐츠 이동은 사업자의 고정된 단말간에만 가능하며, 다양한 기기종이 디바이스 간의 이동은 불가능한 상황임
- 모바일 콘텐츠의 불법적인 사용·전달, 이용자 서비스 자격 관련 데이터의 변조·삭제 및 콘텐츠 불법 유출에 대한 대응 필요

【 스마트 스크린 서비스 및 콘텐츠 보호 】



- 스마트폰, 스마트 TV 등의 실시간 서비스가 늘어나면서 청소년들의 유해 사이트, 동영상 노출 급증에 따른 사회 문제 야기
 - 스마트 스크린 사용자를 식별하고, 사이트/동영상 등의 유해 여부를 판단하여 필터링하는 기술 개발 필요

□ 추진 내용

- OSMU(One-Source Multi-Use) 기반의 스마트 스크린 서비스를 지원하는 콘텐츠 보안 상호연동 기술 개발
 - 사용자가 구매한 보호된 콘텐츠의 장소와 단말간 이동시에도 해상도, 화질, 프레임률 등의 변환을 지원하여 중단 간의 보안을 보장하는 기술
 - 기기 및 플랫폼 독립형 보안 코드 규격을 정의하고 콘텐츠 내장형 스마트 코드 생성 기술을 개발
- 스마트 스크린 환경에서 안전한 콘텐츠 서비스 환경을 위한 지능형 콘텐츠 보호 기술 개발
 - 스마트 스크린 서비스 중간 경로에서 콘텐츠의 불법적인 사용·전달·삽입 방지, 데이터의 변조·삭제 방지 기술
 - 콘텐츠 복사방지와 재분배 관리기능과 콘텐츠 특성에 따라 차별화된 사용 규칙(Usage Rule) 및 보안기능 적용기술 개발
- 실시간 콘텐츠의 분석 및 차단을 수행하여 실시간으로 불법·유해 정보를 차단하는 기술 개발
 - 불법·유해사이트 등급화기반 사이트 차단 기술, 콘텐츠 특징 기반 불법·유해 콘텐츠 패턴 인식 및 차단 기술 개발

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
중기	○ 지능형 콘텐츠 저작권 관리 기술 개발						보안업체
장기	○ 스마트 스크린 서비스 보호 기술						연구기관
	○ 모바일 환경에서의 불법·유해 콘텐츠 차단 기술 개발						연구기관, 이동통신사

라. 모바일 클라우드 및 인프라 보호 기술 개발

개 요

- ◇ 대규모 모바일 데이터의 보안 모니터링과 안전성 유지를 위한 모바일 클라우드 보안 프레임워크 및 가상화 보안 기술 확보

□ 배경 및 필요성

- 모바일 서비스의 확대와 대규모 데이터 컴퓨팅의 안전성이 부각되면서 **모바일 클라우드 보안** 문제가 중요한 이슈로 등장
 - ※ 세계 모바일 클라우드 시장은 '15년까지 약 52억달러 전망 (출처: ABI Research)
- 모바일 클라우드 컴퓨팅에서 발생하는 **대량의 보안이벤트** 모니터링을 효율적으로 처리하는 보안 프레임워크 개발이 필요
 - ※ 유럽의 ENISA 기구에서는 클라우드 컴퓨팅 보안 프레임워크를 위해 'Cloud Computing Information Assurance Framework'를 진행
- 정보의 생명주기 관리, e-Discovery, 가상화 보안 기술 등을 통해 대량의 클라이언트 데이터 관리에 따른 보안 위협 해소
- 모바일 클라우드 서비스(SaaS, PaaS, IaaS) 환경에서의 서비스 안전성을 보장하기 위한 인증, 자원 접근통제·암호화 통신의 강화 필요
 - 클라이언트/서버 간의 정보 유출, 사용자 계정 도용 등의 서비스 위협을 해소할 수 있는 IAM(통합계정관리)와 네트워크 보안 기술 필요

□ 추진 내용

- 모바일 클라우드 보안 프레임워크 및 가상화 보안 기술 개발
 - 클라우드 서비스 통합 인증 및 권한 관리, 스토리지의 기밀정보 보호, 취약점 분석, 서비스 연속성 보장 기술 등

- Guest 시스템 모니터링 및 네트워크 비정상행위 탐지 등을 위한 보안 모니터링 분석·관리 기술 개발
- 가상 머신들 간의 제어, 로그, 데이터 연관성 분석 및 클라우드 서비스 e-Discovery 정보 관리 기술



- o 모바일 오피스, UC 등 클라우드 환경에서 기기 인증, 자원 접근통제·암호화, 정보유출방지 등 모바일 클라우드 서비스 보안 기술

※ UC(Unified Communication) : 메신저, 이메일, 전화뿐 아니라 영상회의에 이르기까지 모든 의사소통 수단을 단일시스템으로 통합해 효율적으로 관리

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
중기	o 모바일 클라우드 서비스 보안 기술						연구기관, 보안업체
장기	o 모바일 클라우드 보안 프레임워크 개발						연구기관

마. 모바일 단말 적용을 위한 경량·저전력 암호/응용기술 개발

개 요

- ◇ 모바일 인프라, 서비스, 콘텐츠에 공통 적용 가능하고 저사양 단말에서도 유연한 동작이 가능한 경량암호 응용기술 개발

□ 배경 및 필요성

- PC기반 암호기술을 확보하였으나 모바일 분야의 인프라·서비스·콘텐츠 등 신규 환경에 적합한 공통기반 기술로는 한계
 - SEED/HIGHT 등 국산암호 최적화 구현기술 및 경량·저전력화 가능한 신규암호 구현기술 개발 필요
 - ※ 국내 암호 : HIGHT('05년), ARIA('04년), SEED('99년), ECKCDSA('99년) 등
- 저사양 모바일 단말·센서의 수집정보 보호 등 응용분야에서 암호기술을 유연하게 사용하기 위한 보안통신 기술 개발 필요
 - 스마트폰, 무선AP 등 모바일 기기 및 중계장비에 탑재 가능한 고효율 인증 및 서명 등 암호기반 보안통신 기술 확보
 - ※ 미국은 NIST(국립표준기술원)의 주도로 HW적합성·안전성·경량성을 고려한 AES를 개발·표준채택 이후 글로벌 보안시장에 이용을 확대
- 암호기술 및 보안통신기술의 가용성을 지속적으로 유지하기 위한 정기적 안전성 재평가 기술 및 검증체계 개발 필요
 - ※ 유럽 ECRYPT(암호기술 및 표준화 프로젝트) 그룹에서는 암호 및 보안 프로토콜의 안전성 및 효율성 분석을 매년 검토

□ 추진 내용

- 국내 표준암호(SEED, ARIA, HAS 등)의 처리속도 향상 및 SW·HW구현시 유연하게 적용가능한 암호기술 경량화 연구

- HW 및 SW(32/64bit)에서 고속동작 가능하고 현재까지 알려진 공격에 대하여 안전성이 증명가능한 경량암호 기술 확보
 - 저전력 환경에 적용가능한 서명·인증·키관리 등 암호기술 개발 및 세계시장 진출을 위한 국제 표준화(ISO, IETF 등) 병행 추진
- ※ 모바일 금융, 스마트카드, RFID/USN 등 디바이스의 자원제약에 구애받지 않고 확장성(scalable)이 유연(flexible)하게 가용되는 암호기술 확보

○ 모바일 센서에서 수집하고, 제공하는 정보의 안전한 저장, 가공 및 전송 체계 구축을 위한 초경량 보안통신기술 및 모듈 개발

- 저사양, 저전력 모바일 센서에 적용될 수 있는 인증 기술 개발
- 모바일 센서망에서의 불법적인 정보수집 및 센서 저장정보의 위변조 방지기술 개발
- 센서용 저용량의 Secure 데이터 스토리지/통신채널관리 모듈개발

○ 블록암호, 해쉬함수, 서명 등 암호기술 및 모바일 센서 보안통신 기술의 안전성 및 성능 평가/검증을 위한 보안성 검증체계 개발

※ 보안성 검증체계 : 암호 및 보안통신 활용 이전에 설계·구현 과정에서의 신규 위협 및 취약점에 대한 분석 등을 수행하여 안전성을 강화하는 검토 체계

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
중기	○ 모바일용 경량 보안통신 기술 개발						보안업체, 연구기관
장기	○ 암호/용융기술 보안성 검증체계 개발						연구기관
	○ 암호 저전력·경량화 기술 개발						학계

개요

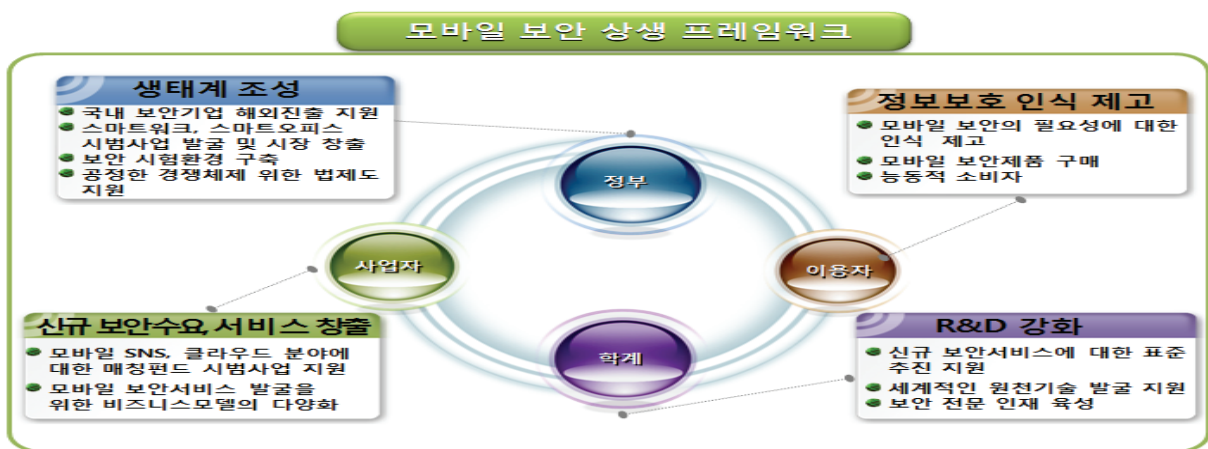
- ◇ 모바일 보안시장 생태계 조성을 위해 보안 서비스의 차별화·다양화 지원, 정당한 수익 배분, 민·관 정보공유 강화 등 공정경쟁 기반 구축
- ◇ 모바일 보안 인력의 전문성 제고와 신규 인재 확보를 위한 산·학 협력을 통한 전문인력 양성

□ 배경 및 필요성

- 국내 보안 산업은 기업의 영세화, 비즈니스 모델의 빈곤, 내수시장 위주의 사업 영위 등으로 성장 동력을 확보하기 어려운 상황
 - 안정적 시장을 두고 업체간 과다출혈 경쟁으로 수익 악화 및 산업 경쟁력 약화
 - 협소한 국내 시장위주의 사업 영위로 수출 등 해외시장 진출이 저조하여 기업성장에 한계
- 대형 S/W사업 통합발주 관행 및 낮은 유지보수요율로 정보보안 업체가 적정한 개발·구축 대가를 받기 어려운 구조
 - 장애발생 책임문제, 관리 불편 등으로 SW 분리발주가 저조하고, 선진국(20%)에 비해 국내 평균 유지보수요율도 매우 낮음(7~8% 수준)
- 모바일 보안 등 신규 보안 수요는 증가하고 있으나 보안인력 양성 체계 부족으로 인력 수급 불균형이 중대
 - 해커 등 정보보안전문가 양성기관 부재, 정보보호 관련학과 보유 대학도 16개에 불과하며 산학 연계도 미흡한 실정
 - 낮은 급여 수준과 불안정한 미래로 우수 보안인력의 대형 SI, 포털 등으로 이직 증가

□ 추진 내용

- (모바일보안 상생환경 조성) 모바일 보안 시장 활성화를 위해 중소기업, 이통사, 대기업 간의 상생 협력 환경 조성
 - 영세 보안업체의 수익성 개선을 위한 보안제품 개발 적정대가 보장 방안 강구
 - 대기업과 영세 보안업체들 간의 통합발주 계약을 지양하고 직접 업체가 계약하는 분리발주 지원책 및 기술력 위주의 평가방법 마련



※ 모바일 보안업체와 단말 제조업체, 이통사간의 협력 어려움 타개 등을 위한 ‘(가칭)모바일 시큐리티 협의회’ 구성·운영

- (모바일 보안서비스 시험환경 구축) 정부 유관기관에서 중소기업의 다양하고 차별화된 보안제품을 테스트할 수 있는 환경 제공
 - C-P-N-T의 보안시스템 구축 및 보안S/W 적용 등을 시험·검증할 수 있는 환경을 제공하여 제품의 성능 및 신뢰성 확보
 - ※ C-P-N-T(콘텐츠-플랫폼-네트워크-단말, Content-Platform-Network-Terminal)
 - 필요시 민간과의 매칭 펀드 조성을 통한 시험환경 구축
- (상용화 지원 강화) ETRI, KISA, 국보연 등 연구기관의 성과물을 민간 이전하는 모바일 보안기술 이전행사 등을 정기적으로 개최
 - ‘(가칭) 모바일 보안 상용화 지원센터’를 설립·지원하여 보안제품의 개발·판매·유지보수 등 전 단계에 이르는 통합 패키지형 지원 실시

- (신규 보안 서비스 표준화 추진) 학계와 협력하여 기업 간 과열 경쟁 및 중복투자 절감을 위한 신규 보안 서비스 표준화 추진
 - 산·학·연·관간 협력으로 '모바일 보안표준 연구센터'를 설립하여 관련 기초 기술 확보 및 글로벌 표준화 지원
 - ※ 모바일 보안표준 연구센터 설립과 운영 지원을 통해 클라우드서비스, 스마트폰 등의 보안표준 연구 및 선진 외국 대학, 연구소 등과 공동 연구 수행
 - 모바일 클라우드 서비스, 스마트폰 보안 등 중점 표준화 분야 설정을 통해 전략적으로 국제 표준화 (ITU-T, JTC 1, 3GPP 등) 추진
- (국내기업 해외진출 지원) 국내 보안 기업들의 제품 품질 향상 및 수출경쟁력 제고를 위한 해외진출 지원 강화
 - 글로벌 모바일 보안시장 현황 분석을 통해 국내 기업의 해외진출 마케팅전략 수립 및 현지화 사업추진에 필요한 정보 정기적 제공
 - 중소 보안업체와 대규모 IT업체 간의 협력을 통한 해외 모바일 시큐리티 프로젝트 공동 참여 추진
- (민·관 협력 인력양성 추진) 모바일 시큐리티 분야 관련 업체에서 필요한 인력을 공급할 수 있도록 업계와 연계된 교육프로그램 운영
 - 관련 부처와 협력하여 보안관련 고용계약형 석사과정에 모바일 보안 분야 과정을 정규화하고 지원 강화
 - ※ '11년도 지식정보보안 고용계약형 석사과정에 모바일 보안 분야가 신규 개설 되었으나 인원배정 등이 유동적이어 향후 정규화 및 규모 확대 등 부처간 협력 추진
 - 우수 취업(졸업)예정자를 대상으로 취업 후 현장 즉시 투입을 위한 실무중심의 OJT(On the Job Training) 교육 과정 운영 및 취업 지원
 - ※ 중소기업의 요구수준을 반영하여 교육 수료 후 산업현장에 적용 가능한 '스마트폰 앱 프로그래머 과정' 개설(연간 800명, KAIT인력센터)

- (모바일 보안 글로벌 핵심인재 양성) 국내 우수 모바일 연구개발 인력 양성을 위한 이론·실무 연계 교육 및 국제 공동연구 지원 등
- 정보보호를 포함하는 '융·복합형 신규 무선인터넷 기술과정'을 개설하여 전문가 양성 지원 및 산업 현장에의 요구 만족
 - ※ 모바일 웹, 애플리케이션, 정보보호, 웹 디자인 분야 등을 포괄하며 기초/심화 등 분야별 단계로 구성된 교육 과정 구성(연간 200명, KISA 아카데미)
- 글로벌 경쟁력을 갖는 모바일 보안 인력 양성을 위해 선진 외국 대학과의 국제 공동연구 지원 및 연계 교육 추진

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 모바일 보안 상생환경 조성	■	■				정부·유관기관 및 민간업체
	○ 모바일 보안서비스 시험환경 구축	■	■				정부·유관기관
중기	○ 상용화 지원 강화	■	■	■			정부·유관기관
	○ 신규 보안 서비스 표준화 추진	■	■	■	■		정부·유관기관
장기	○ 국내 보안 기업 해외진출 지원	■	■	■	■	■	정부·유관기관
	○ 민·관 협력 인력양성 추진	■	■	■	■	■	정부·유관기관, 이통사, 보안업체
	○ 모바일 보안 글로벌 핵심인재 양성	■	■	■	■	■	정부·유관기관 및 교육기관

개요

- ◇ 모바일 환경에서 사이버 위협이 빠르게 증가하는 상황에서 안전한 이용 환경 조성을 위해 국내·외 유관기관과의 공조 강화
- ◇ 다양한 모바일 기기와 서비스를 이용한 홍보활동을 강화하고 청소년, 기업 및 정보보호 취약계층 등 대상별 홍보 콘텐츠 개발·보급

□ 배경 및 필요성

- 국내 모바일 시큐리티 주요 유관기관간 긴밀한 협력체계 구축 및 국외 선도 기업과의 정보교류 필요
 - 구글, 애플 등에서 운영되는 앱스토어 등은 국내 법제를 강제하기 어려워 협력체계 구축을 통한 국내환경 반영 필요
- 스마트폰 보급은 급속하게 진행되고 있으나 모바일 보안에 대한 전반적인 인식 및 실천수준은 저조
 - ※ 국내 스마트폰 사용자 대상으로 스마트폰 백신사용에 대한 설문조사결과 응답자의 52.3%가 백신을 사용하지 않고 있다고 응답(전자신문 설문조사, '10.5.4)
 - 다양한 모바일 기기를 활용하여 실시간, 즉각적인 보안 관련 정보 전달 및 홍보를 통해 모바일 보안 인식제고 효과 극대화 필요

□ 추진 내용

- (예방적 협력체계 강화) 스마트폰 악성코드 침해사고 예방 및 대응을 위한 정부 및 민간기관 공동 협력체계 구축 강화
 - 백신사, 이통사, 제조사 등과 모니터링 협력체계를 구축하고, 악성코드 및 취약점 정보 공유
 - ※ 주기적으로 국내외 모바일 악성코드, 취약점, 네트워크의 이상 징후를 파악하여 관련 정보를 공유할 수 있는 시스템 마련

- 「스마트폰 정보보호 민관 합동대응반」을 통해 개인정보유출, DDoS공격 등 침해사고에 대비한 공동 대응 훈련 강화
 - ※ '09년 모바일 악성코드 공동대응 모의 훈련시 통신사 및 백신사가 참여하였으나, '10년 이동통신사(3개), 제조사(3개), 백신업체(6개) 및 기타 보안업체 등으로 확대(연1회 실시)
- (모바일 보안분야 Think-Tank 육성·지원) 전문가그룹 지원을 통해 신규 모바일 위협 분석, 미래사회의 기술·사회·문화적 변화 전망 및 중장기 대응전략 등 마련
 - 「모바일 시큐리티 포럼」, 「인터넷 정보보호 협의회」, 「미래융합 IT 서비스 보안연구회」 등 기 구성된 전문가그룹의 확대·개편 검토
 - 모바일 보안 분야 연구 선도를 위해 ETRI, KISDI 등 국내 우수 연구기관 지원 및 상호협력연구 체계 구축
- (글로벌 협력체계 다원화) 안전한 모바일 환경 조성 및 침해사고 방지를 위해 해외 선두업체와의 협력체계 다각화
 - 안드로이드 마켓, 애플 앱스토어 등 국내에서 이용중인 해외 스마트폰 앱 마켓과 앱의 보안검증 절차 관련 협약 체결
 - 국제공동 협력연구체계를 구축하여 글로벌 모바일 기업(애플, 구글 등) 및 해외 보안업체(시만텍, 시스코 등)와 공동으로 신규 보안위협 정보 공유 및 취약점 분석·대응기법 연구
- (모바일 취약계층 교육) 농어촌 지역, 아동, 학생, 주부, 노인 등 모바일 취약계층 대상 정보보호 교육 활성화
 - 민관 협력 및 연계사업을 통해 전국 학교, 사회복지센터, 주민센터 등 모바일 취약계층에 대한 찾아가는 모바일 보안 교육 실시
 - ※ 이통사, 봉사단체, 온누리 캠페인, 인터넷드림단, 대학 정보보호 동아리 등과 연계

- 어린이 및 노년층 등 모바일 기기의 정보보호 취약 계층에게 불법 유해정보 예방 및 보안설정과 관련된 맞춤형 교육 콘텐츠 개발
- (모바일 정보보호 문화 확산) 이통사, 제조사, 유관기관 등과 연계하여 다양한 모바일 디바이스 등을 활용한 보안 인식제고 효과 극대화
- 제조사는 출시 제품에 기본적으로 제공되는 앱(App)을 통해 보안 경고
 - ※ 스마트폰 등 기기 출고시 패스워드 설정, 백신설치 등의 보안수칙 및 이용자 보안 책임에 대한 경고를 앱이나 배경화면 등의 형태로 안내할 수 있도록 탑재
 - ※ 스마트폰 안전 확인 기능을 탑재하여 백신 업데이트 여부 등 안내
- 이통사는 스마트폰 가입 시 모바일 관련 보안사고 관련 '긴급 SMS' 수신 동의 취득 절차 마련 및 홍보관을 활용하여 정보보호 안내
 - ※ SKT 티움, KT 올레스퀘어 등 이통사 IT기기 체험관 활용
- 이통사 및 제조사는 매뉴얼, 청구서 등을 통해 보안수칙 및 사고 신고접수 절차 등을 안내하고 보안위협 정보 등 제공
 - ※ 매뉴얼 내에 보안수칙 내용 삽입 및 스티커형 단독 안내장 제공, 요금 청구서 활용(이메일 청구서 배너 형태, 오프라인 청구서 뒷면 인쇄) 등

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
단기	○ 예방적 협력체계 강화						정부·유관기관, 이통사, 보안업체
중기	○ 모바일 정보보호 문화 확산						정부·유관기관 및 이통사, 제조사
장기	○ 모바일 보안분야 Think-Tank 강화						정부·유관기관, 민간연구기관
	○ 글로벌 협력체계 다원화						정부·유관기관, 해외업체
	○ 모바일 취약계층 모바일 정보보호 교육						정부·유관기관, 이통사, 봉사단체

개요

- ◇ 스마트 모바일 시대로의 진입에 따른 신규 디바이스, 서비스의 안전한 이용을 보장하기 위한 법·제도 개선

□ 배경 및 필요성

- 정보통신서비스 제공자 등이 관리하는 정보통신망에 대한 해킹, 정보 유출 등 침해행위는 ‘정보통신망법’ 등 현행법을 통해 규율 가능하나,
 - 개인이 소유·관리하는 무선랜, 단말기 등의 보안상 허점을 악용한 DDoS 공격, 개인정보 침해, ID 도용 등으로부터 피해를 예방하고 차단하기 위한 법제도적 장치는 미흡한 상황
- 소셜네트워킹서비스(SNS), 모바일 클라우드 등 신규 서비스가 무선 인터넷 환경으로 확산되면서 이에 대한 법제도적 보완 필요

【 모바일 정보보호 위협에 따른 현행 법률의 문제점 】

위협	현행 법률상 문제점
모바일 기기에 의한 정보보호 위협	○ 현행 법률(정보통신망법)은 PC 등에 의한 유선 정보통신 서비스 이용 환경을 기준으로 규정 ○ 다양한 단말과 이동성 그리고 위치, 상황, 행태 정보 등을 처리하는 융합 환경을 완전히 규율하기 어려움
이동성에 따른 위치, 행태 등 새로운 정보수집·이용	○ 현행 법률(정보통신망법)은 정보수집과 관련해 사전동의 원칙과 열람·정정·철회 권리의 보장으로 이용자를 보호 ○ 모바일 환경에서는 이러한 보호장치의 작동 보완 필요
모바일 기기의 정보보호 및 개인정보보호 안전성	○ 현행 법률(정보통신망법)은 정보통신서비스 이용단말에 대한 정보보호 및 개인정보보호 문제는 이용자의 책임으로 규율 ○ 명의도용시에도 채권추심기관으로부터 일차적 청구대상으로 지정되는 등 이용자 손실보호 문제 발생

□ 추진 내용

- (정보보호 관리체계 재정비) 정보보호 관리체계 인증(ISMS) 등 기존의 서비스 기반 정보보호제도를 모바일 서비스에 적용 확대
 - 관련 기준에 모바일 서비스 관련 정보보호 요구사항 반영, 통신망 및 타 이용자 보호를 위한 감염 단말기의 영향 최소화 방안 강구
 - (보안·개인정보보호 평가제도 도입) 스마트폰, 태블릿PC, 스마트 TV 등 모바일 단말별로 보안·개인정보보호 기준을 마련
 - 관련 업체가 자율적으로 적합성을 평가받도록 관련 제도 마련
 - 현행 정보보호 관련 법률의 고지, 동의, 이용자 권리보장 요건을 모바일 기기 사용 및 수시 정보수집에 맞도록 보완
 - (신규 모바일서비스 보호 법제 개선) 모바일 클라우드, 모바일 오피스 등 신규서비스 보안 강화를 위한 법제도 개선
 - 모바일 클라우드 서비스 등 신규 서비스에서의 정보보호 및 데이터 국외이전, 국제재판 관할 문제 등 연구
 - 중요 서비스 중단·오류에 대한 책임, 수탁자 관리·감독 책임 등 신규 서비스 활성화를 위한 관련 법제도 정비
- ※ 신규기술 적용 및 서비스 이용시 보안문제의 책임이나 권익보호 등 법제 개선 연구를 위한 '(가칭)신규 모바일 서비스 보안 법제 연구회' 구성·운영

□ 추진 일정

단계	추진 사항	일 정					주 체
		'11	'12	'13	'14	'15	
중기	○ 정보보호 관리 법제 재정비						정부·유관기관
	○ 정보보호 및 개인정보보호 평가제도 도입						정부·유관기관
	○ 신규 모바일 서비스 보호 법제 개선						정부·유관기관

V. 추진 일정 및 주체, 소요 예산

1. 추진 일정

추진 사항	일 정				
	'11	'12	'13	'14	'15
1. 미래 모바일 서비스·인프라 보안품질 향상					
① 신규 모바일 단말 보안 강화					
가. 스마트폰 단말 보안 강화					
o 안전한 스마트폰 앱 유통 환경 조성					
o 스마트폰 백신 보급 활성화					
o 모바일 웹 악성코드 점검					
o 한국형 앱게놈 프로젝트 추진					
o 보안용 앱·솔루션 시험센터 구축					
나. 스마트패드 등 신규 기기 보안 대책 마련					
o 콘텐츠 위·변조 방지					
o 스마트패드 보안안내서 마련					
o Smart-hub 보안체계 마련					
② 무선 네트워크 안전성 확보					
가. 무선랜 보안수준 제고					
o 원클릭 무선랜 보안설정 솔루션 도입					
o 무선랜 보안 종합포털 구축					
o 무선랜 보안 법제 개선					
o 이용자 보안 인식제고를 위한 홍보 강화					
o 공중 무선랜 보안관리 강화					
나. 유·무선 연동구간 보안성 강화					
o 이동통신망내 보안 위협 분석					
o 연동 게이트웨이 침해사고 대응					
o 외부 인터넷망간 보안체계 구축					
o 신규 보안 위협 대응					

추진 사항	일 정				
	'11	'12	'13	'14	'15
③ 신규 모바일 서비스·콘텐츠 보호					
가. 모바일 오피스 보안 체계 마련					
o 보안 가이드라인 개발·보급	■				
o 모바일 오피스 법제도 개선	■	■			
o 모바일 오피스 모범사례 발굴 및 확산	■	■	■		
o 모바일 오피스 보안 테스트 환경 구축	■	■	■	■	
나. 모바일 SNS 보안 강화					
o SNS 이용 안내 가이드라인 제작 및 배포	■				
o SNS 정보유출 대응 법제 개선	■	■			
o SNS 보안 및 윤리 교육 강화	■	■	■		
o 기술적 대응방안 마련	■	■	■		
o 글로벌 스탠다드 마련	■	■	■	■	
다. 모바일 클라우드 보안 체계 강화					
o 서비스 표준화 및 인식제고	■	■			
o 모바일 클라우드 보안기반 마련	■	■	■		
o 신종위협 정보 공유	■	■	■	■	
라. 스마트 TV 보안 체계 구축					
o 개인정보 보호방안 마련	■	■			
o 스마트TV 서비스 및 네트워크 보호 강화	■	■	■		
o 스마트TV 디바이스 보호체계 마련	■	■	■		
o 콘텐츠 보호방안 추진	■	■	■	■	■
마. 모바일 뱅킹 보안 기반 강화					
o 모바일 뱅킹 보안가이드 개발	■	■			
o 모바일 뱅킹 보안성 연구·개발	■	■	■		
o 모바일 뱅킹 보안취약성 점검	■	■	■		
o H/W기반 금융보안모듈 프레임워크 개발	■	■	■	■	■
o 안전한 인증기반 및 온라인 ID 관리체계 조성	■	■	■	■	■
2. 모바일 이용자 프라이버시 보호 확립					
④ 모바일 개인정보 및 위치정보 보호 강화					

추진 사항	일 정				
	'11	'12	'13	'14	'15
가. 모바일 개인정보 보호					
○ 개인정보 보호 수단 제공 및 관리 책임 강화	■				
○ 기기제조사 개인정보보호 권고	■	■			
○ 개인정보보호를 위한 이용자 편의성 제고	■	■			
○ 스마트폰 앱의 프라이버시 안전성 검증	■	■	■		
나. 모바일 서비스의 위치정보 보호					
○ 모바일 기기 위치정보제공 기능 설정변경	■				
○ 공공목적의 위치정보 활용 보호조치 강화	■	■			
○ 위치정보 자기제어 시스템 구축	■	■	■	■	
⑤ 모바일 스팸 방지 및 최소화					
○ 신규서비스 스팸 위험성 분석	■				
○ 모바일 스팸전용 신고 웹페이지 구축	■				
○ 스팸방지 법제 개선	■	■	■		
○ 스팸방지 안내서 개정		■		■	
○ 지능형 필터링 활용 확대	■	■	■	■	
⑥ 모바일 유해정보 유통 방지					
○ 모바일 콘텐츠 등급서비스	■	■			
○ 유해정보 차단 앱 개발 및 보급	■	■			
○ 유해정보 점검 및 모니터링	■	■	■		
○ 유해정보 신속처리 등 자율규제 강화	■	■	■	■	
3. 모바일 정보보호 기반 조성					
⑦ 모바일 보안기술 연구개발(R&D) 지원 확대					
가. 단말 및 플랫폼 보호기술 개발					
○ MTM기반 단말 보안 플랫폼 기술 개발	■	■	■		
○ 그린 보안 플랫폼 기술 개발	■	■	■	■	
나. 모바일 인터넷 침해사고 대응 기술 개발					
○ 무선 침입탐지 기술 개발	■	■	■		
○ 이기종 이동통신망 침입탐지 및 대응기술 개발	■	■	■	■	
○ 이동통신망 통합보안 관제기술 개발	■	■	■	■	

추진 사항	일 정				
	'11	'12	'13	'14	'15
다. 스마트스크린 서비스 및 콘텐츠 보호 기술 개발					
○ 지능형 콘텐츠 저작권 관리 기술 개발					
○ 스마트 스크린 서비스 보호 기술					
○ 모바일 환경에서의 불법·유해 콘텐츠 차단 기술 개발					
라. 모바일 클라우드 및 인프라 보호 기술 개발					
○ 모바일 클라우드 서비스 보안 기술					
○ 모바일 클라우드 보안 프레임워크 개발					
마. 모바일 단말 적용을 위한 경량·저전력 암호/응용기술 개발					
○ 모바일용 경량 보안통신 기술 개발					
○ 암호/응용기술 보안성 검증체계 개발					
○ 암호 저전력·경량화 기술 개발					
⑧ 모바일 보안 시장 생태계 조성					
○ 모바일 보안 상생환경 조성					
○ 모바일 보안서비스 시험환경 구축					
○ 상용화 지원 강화					
○ 신규 보안 서비스 표준화 추진					
○ 국내 보안 기업 해외진출 지원					
○ 민·관 협력 인력양성 추진					
○ 모바일 보안 글로벌 인재 양성 지원					
⑨ 모바일 시큐리티 협력체계 구축 및 인식제고					
○ 예방적 협력체계 강화					
○ 모바일 정보보호 문화 확산					
○ 모바일 보안분야 Think-Tank 강화					
○ 글로벌 협력체계 다원화					
○ 모바일 취약계층 모바일 정보보호 교육					
⑩ 모바일 보안 법제 정비					
○ 정보보호 관리 법제 재정비					
○ 정보보호 및 개인정보보호 평가제도 도입					
○ 신규 모바일 서비스 보호 법제 개선					

2.

추진 주체

사업명	방통위	KISA	관련기관
1. 미래 모바일 서비스·인프라 보안품질 향상			
① 신규 모바일 단말 보안 강화			
가. 스마트폰 단말 보안 강화	정보보호팀	코드분석팀	이통사, 제조사, 보안업체, 앱 개발업체
나. 스마트패드 등 신규 기기 보안 대책 마련	정보보호팀	코드분석팀	이통사 보안업체, 앱 개발업체
② 무선 네트워크 안전성 확보			
가. 무선랜 보안수준 제고	정보보호팀	무선 인터넷팀	이통사, 제조사
나. 유·무선 연동구간 보안성 강화	정보보호팀	융합보호 R&D팀	이통사
③ 신규 모바일 서비스·콘텐츠 보호			
가. 모바일 오피스 보안 체계 마련	스마트워크팀	신비즈니스 콘텐츠팀	이통사, 서비스업체
나. 모바일 SNS 보안 강화	정보보호팀	정책연구팀, 개인정보 보호기획팀	이통사, 서비스업체
다. 모바일 클라우드 보안 체계 강화	지능 통신망팀	신비즈니스 콘텐츠팀	이통사, 서비스업체
라. 스마트 TV 보안 체계 구축	스마트TV팀	융합보호 R&D팀	서비스업체
마. 모바일 뱅킹 보안 기반 조성	인터넷정책과, 정보보호팀	전자인증팀	금융보안 연구원
2. 모바일 이용자 프라이버시 보호 확립			
④ 모바일 개인정보 및 위치정보 보호 강화			
가. 모바일 개인정보 보호	개인정보 보호윤리과	개인정보 보호기획팀	이통사, 서비스업체
나. 모바일 서비스의 위치정보 보호	개인정보 보호윤리과	개인정보 보호기획팀	이통사, 제조사, 서비스업체
⑤ 모바일 스팸 방지 및 최소화	네트워크 윤리팀	스팸대응팀	이통사

사업명	방통위	KISA	관련기관
⑥ 모바일 유해정보 유통 방지	네트워크 윤리팀	인터넷윤리팀	방송통신심의위, 이통사, 서비스업체
3. 모바일 정보보호 기반 조성			
⑦ 모바일 보안기술 연구개발(R&D) 지원 확대			
가. 단말 및 플랫폼 보호기술 개발	정보보호팀, 녹색기술팀	융합보호 R&D팀	ETRI, 정보보호 PM실
나. 모바일 인터넷 침해사고 대응 기술 개발	정보보호팀, 녹색기술팀	융합보호 R&D팀	ETRI, 정보보호 PM실
다. 스마트스크린 서비스 및 콘텐츠 보호 기술 개발	정보보호팀, 녹색기술팀	융합보호 R&D팀	ETRI, 정보보호 PM실
라. 모바일 클라우드 및 인프라 보호 기술 개발	정보보호팀, 녹색기술팀	융합보호 R&D팀	ETRI, 정보보호 PM실
마. 모바일 단말 적용을 위한 경량·저전력 암호/응용기술 개발	정보보호팀, 녹색기술팀	융합보호 R&D팀	ETRI, 정보보호 PM실
⑧ 모바일 보안 시장 생태계 조성	정보보호팀	정책연구팀, 아카데미팀	KISA, 이통사, 제조사, 서비스 업체
⑨ 모바일 시큐리티 협력체계 구축 및 인식제고	정보보호팀	정책연구팀, 코드분석팀, 홍보팀	NCSC, APCERT, 방송사, 포털
⑩ 모바일 보안 법제 정비	정보보호팀	법제분석팀	법제처, 국회 문방위

※ 산·학·연·관의 주체별 역할 분담을 통한 유기적인 상호 협력체계를 구축하여
‘스마트 모바일 시큐리티 종합계획’ 추진

- 방통위, KISA, ETRI, 관련 사업자들이 참여하는 ‘스마트 모바일 시큐리티 종합
계획 추진 전담반’(반장: 네트워크정책국장)을 구성·운영
- 전담반에서 주기적으로 집행 실적을 점검하고, 2차년도 부터는 시장, 제도 등의
상황변화를 반영한 연 단위 시행계획을 수립하여 추진

3.

소요 예산

(단위 : 백만원)

사업명		'11	'12	'13	'14	'15	계
1. 미래 모바일 서비스·인프라 보안품질 향상							
① 신규 모바일 단말 보안 강화							
가. 스마트폰 단말 보안 강화	정부	650	750	700	550	400	3,050
	민간	800	1,200	1,570	1,600	1,700	6,870
나. 스마트패드 등 신규 단말 보안 대책 마련	정부	30	60	70	50	50	260
	민간	500	600	610	660	680	3,050
② 무선 네트워크 안전성 확보							
가. 무선랜 보안수준 제고	정부	300	500	500	200	-	1,500
	민간	600	600	510	560	590	2,860
나. 유·무선 연동구간 보안성 강화	정부	20	130	150	-	-	300
	민간	800	1,200	1,500	1,300	1,300	6,100
③ 신규 모바일 서비스·콘텐츠 보호							
가. 모바일 오피스 보안 체계 마련	정부	20	380	300	300	100	1,100
	민간	1,000	1,100	1,300	1,400	1,300	6,100
나. 모바일 SNS 보안 강화	정부	100	200	300	100	-	700
	민간	200	230	160	190	160	940
다. 모바일 클라우드 보안 체계 강화	정부	250	300	300	300	100	1,250
	민간	530	640	680	550	840	3,240
라. 스마트 TV 보안 체계 구축	정부	20	1,000	500	100	100	1,720
	민간	300	300	310	310	320	1,540
마. 모바일 banking 보안 기반조성	정부	20	300	380	300	100	1,100
	민간	400	450	230	240	240	1,560
2. 모바일 이용자 프라이버시 보호 확립							
④ 모바일 개인정보 및 위치정보 보호 강화							
가. 모바일 개인정보보호	정부	150	130	100	100	100	580
	민간	630	520	580	670	770	3,170
나. 모바일 서비스의 위치정보 보호	정부	250	300	300	200	150	1,200
	민간	100	100	100	100	100	500
⑤ 모바일 스팸 방지 및 최소화	정부	30	30	15	10	5	90
	민간	800	300	350	750	600	2,800

사업명		'11	'12	'13	'14	'15	계
[6] 모바일 유해정보 유통 방지	정부	50	40	30	5	5	130
	민간	330	410	440	470	500	2,150
3. 모바일 정보보호 기반 조성							
[7] 모바일 보안기술 연구개발(R&D) 지원 확대							
가. 단말 및 플랫폼 보호기술 개발	정부	1,000	1,500	2,000	1,500	1,500	7,500
	민간	300	300	400	300	300	1,600
나. 모바일 인터넷 침해사고 대응 기술 개발	정부	1,000	1,500	2,000	1,000	1,000	6,500
	민간	300	300	400	300	300	1,600
다. 스마트스크린 서비스 및 콘텐츠 보호 기술 개발	정부	1,000	1,500	2,000	1,500	1,500	7,500
	민간	300	300	400	300	300	1,600
라. 모바일 클라우드 및 인프라 보호 기술 개발	정부	250	1,500	2,000	1,000	1,000	5,750
	민간	300	300	400	300	300	1,600
마. 모바일 단말 적용을 위한 경량·저전력 암호/응용기술 개발	정부	230	1,000	1,000	1,000	1,000	4,230
	민간	100	100	100	100	100	500
[8] 모바일 보안 시장 생태계 조성	정부	30	1,000	1,200	1,200	1,000	4,430
	민간	100	100	100	100	100	500
[9] 모바일 시큐리티 협력체계 구축 및 인식제고	정부	100	350	500	500	300	1,750
	민간	100	100	100	100	100	500
[10] 모바일 보안 법제 정비	정부	30	100	100	100	100	430
	민간	-	-	-	-	-	-
소요 예산	정부	5,530	12,570	14,445	10,015	8,510	51,070
	민간	8,490	9,150	10,240	10,300	10,600	48,780
	전체	14,020	21,720	24,685	20,315	19,110	99,850

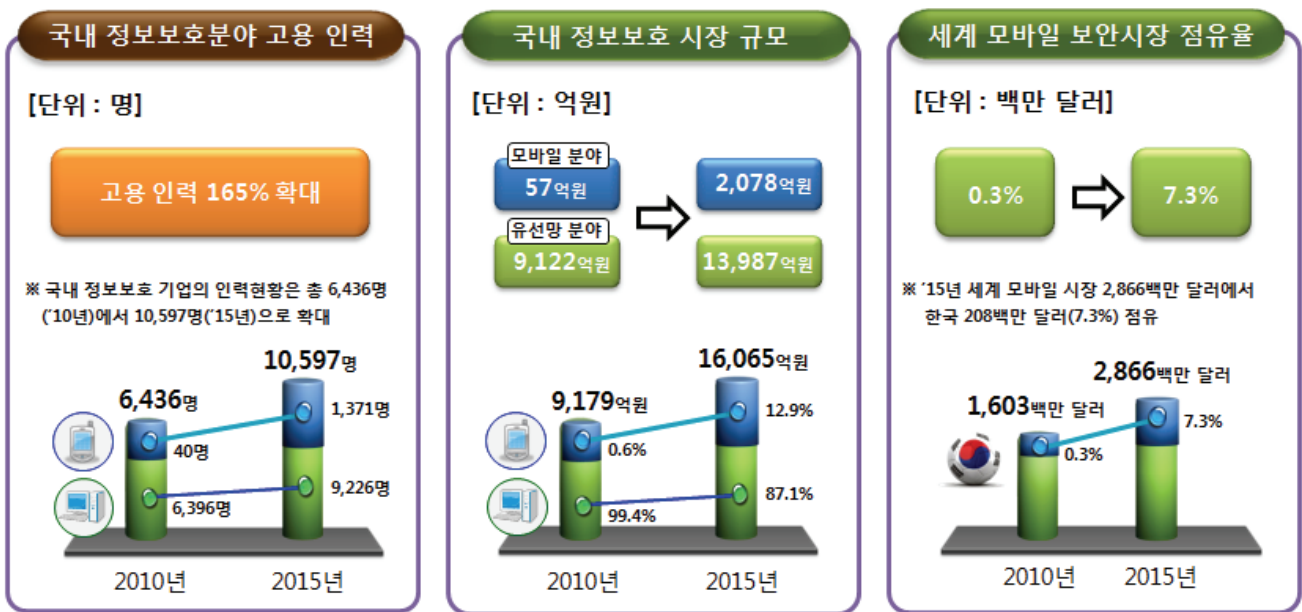
※ 정부예산은 방송통신위원회 소요제기 예산 기준이며, 기획재정부와의 협의 과정에 따라 변경될 수 있음

- 당해 연도별 투자규모는 추정치이며, 참여하는 업체 등의 사정에 따라 변동될 수 있음

VI. 기대 효과

- (미래 보안위협 감소) 향후 발생 가능한 보안위협에 대한 사전적 대비로 침해사고 발생에 의한 미래 사회적 비용 최소화
 - 4천만대 이상의 스마트기기가 사용될 무선인터넷 시대에서 모바일 침해사고는 7.7 DDoS 피해 수준을 크게 뛰어넘을 것으로 예상
 - ※ '09년 7.7 DDoS사건의 피해액은 363억원~544억원 추정 (현대경제연구원, '09.7월)
 - 모바일 사이버공격 발생으로 인해 서비스 장애 발생 시 일반 국민을 비롯한 기업, 정부의 혼란과 경제적 손실을 사전에 차단
- (안전한 모바일 사회 구현) 안전하고 신뢰할 수 있는 모바일 서비스 이용환경을 구축함으로써 국민들의 삶의 질 향상 기여
 - 급변하는 모바일 환경에 대한 보안 예방체계를 구축하여 사이버 침해사고의 위협으로부터 안전한 스마트사이어티(Smartciety) 구현
 - SNS, LBS 등 신규 모바일 응용서비스 환경에서 발생 가능한 개인 정보유출, 피싱, 사이버폭력 등 다양한 역기능을 사전 예방
- (산업·경제적 성장 효과) 보안우려 해소와 함께 모바일 보안시장 활성화 촉진 및 산업경쟁력 제고, 신규 일자리 창출 효과 기대
 - 정보보호 분야의 전체 고용 인력은 '10년 6,436명 수준이나, 시장 확대를 통해 '15년 10,597명으로 '10년 대비 165% 일자리 확대
 - ※ 정보보호 분야 전체 고용 인력 중 모바일 보안 종사자 비율은 '10년 0.6%(48명)에서 '15년 12.9%(1,371명)으로 증가 예상
 - 한국의 모바일 보안시장은 '10년 57억원에서 '15년 2,078억원으로 확대되어, '15년 세계 모바일 보안시장의 7.3% 차지 전망

【 산업 · 경제적 기대효과 】



※ 출처 : [신규채용] KISIA('09.12월), [국내시장규모] 한국IDC('09.6월) 및 KISIA('09.12월), [세계시장점유율] IDC('10.5월) 기반으로 KISA 예측('10.11월)

- (국가 정보보호 수준 제고) 국가 정보보호 수준 업그레이드 및 신규 영역인 모바일 보안 분야의 개척을 통해 국가적 위상 제고
 - 유무선 분야 세계 최고수준의 인프라·서비스 환경 보유국으로서 글로벌 모바일 보안 분야 선도
 - 모바일 보안 관련 법제도 정비를 통해 모바일 서비스의 기반 환경 구축 및 인터넷 이용의 신뢰성 향상
- (모바일 보안 대국민 인식 제고) 이용자 대상 보안 홍보, 사업자 계도를 추진하여 보안인식 제고 및 사회 전반의 보안 수준 향상
 - 일반 국민이 알기 쉬운 모바일 보안 가이드라인 개발 및 적극적인 보급을 통해 정보보호 수준 향상
 - 모바일 기기 이용 시 발생 가능한 개인정보 및 위치정보 침해 소지를 사전에 예방함으로써 이용자의 프라이버시 보호 수준 제고

◆ **3-Screen 서비스**

동일한 콘텐츠를 모바일 화면, PC 화면, TV 화면으로 언제 어디서나 끊김없이 이용할 수 있는 서비스

◆ **4G 통신**

휴대전화 네트워크의 용량과 속도(100Mbps, 정지시 1Gbps)를 증가시키기 위해 고안된 4세대 무선 기술(4G)로써, 3GPP계열의 LTE Advanced와 WiMAX 계열의 IEEE 802.16m계열을 기술 표준으로 준용

◆ **ARIA (Academy, Research Institute, Agency)**

아리아(ARIA)는 국내 학계·연구소·정부가 공동으로 스마트카드 등의 초경량 환경 및 고성능 서버에 적합하도록 개발한 블록 암호 알고리즘으로, 기술표준원의 한국산업규격 KSX1213으로 고시

◆ **CAS (Conditional Access System)**

CAS(수신제한시스템)은 방송콘텐츠에 암호를 설정하고 시청 권한을 받은 소비자에게만 유료방송을 제공하는 디지털 방송 제어시스템

◆ **DDoS (Distribute Denial of Service)**

분산 서비스 거부(DDoS) 공격은 서버 시스템들의 리소스를 독점하거나, 파괴함으로써 시스템들이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격

◆ **DM (Direct Message)**

1:1로 대화하는 것으로 'DM'은 나를 팔로우하는 사람들이 볼 수 없도록 사적인 대화나 오픈하지 말아야 할 대화를 당사자끼리 직접 주고받을 때 사용

◆ **DRM (Digital Rights Management)**

디지털 저작권 관리(DRM)는 디지털 콘텐츠의 불법복제와 유포를 막고 저작권 보유자의 이익과 권리를 보호해주는 기술과 서비스

◆ **FMC (Fixed Mobile Convergence)**

무선랜을 통한 유무선 통합 서비스로 휴대폰으로 인터넷 전화 사용 가능

◆ **FMS (Fixed Mobile Substitution)**

이동통신망을 이용한 유무선 대체서비스로 일정 지역내에서 유선전화통화시 유선전화 이용요금이 발생하도록 하는 서비스

◆ **GGSN (Gateway GPRS Supporting Node)**

인터넷망과 같은 다른 패킷교환망으로 연결시키는 통로 역할

◆ **GPS (Global Positioning System)**

인공위성을 통해 자신의 위치를 정확히 알아낼 수 있는 전 지구 위치 파악시스템

◆ **HTTPs (Hypertext Transfer Protocol over Secure Sockets Layer)**

하이퍼텍스트 전송 규약(HTTP) 계층 아래의 SSL 계층에서 사용자 요청된 페이지를 암호화·복호화하여 제공하는 웹 프로토콜(통신규약)로써, TCP/IP 에서 HTTP 포트 80 대신에 포트 443을 사용

◆ **HSDPA (High-Speed Download Packet Access)**

고속하향패킷접속, 화상통화가 가능하고 고속으로 데이터를 전송받을 수 있는 3세대 이동통신서비스

◆ **IPSec (Internet Protocol Security)**

인터넷 상에서 데이터 스트림을 구성하는 각 IP Packet을 인증, 암호화 하여 안전한 Internet Protocol 통신을 지원하는 프로토콜

◆ **IPv6**

IPv4에 이어서 개발된 128bit의 주소체계를 가지는 인터넷 프로토콜(IP) 주소 표현 방식의 차세대 버전

◆ **ISAC (Information Sharing & Analysis Center)**

정보공유분석센터로 주로 사이버테러 취약점과 침해요인, 대응방안에 관한 정보를 가입기관에 제공하고 침해사고가 나면 실시간 경보와 분석업무를 수행

◆ **IT Compliance**

IT-컴플라이언스(compliance)는 기업을 운영할 경우 내외부적으로 반드시 지켜야 하는 법적 규제 사항이나 지침을 지칭

◆ **LBS (Location Based Service)**

위치기반서비스(LBS)는 '결합서비스(LBS+모바일SNS, LBS+증강현실)'의 형태로 진화

◆ **M2M (Machine to Machine)**

사람 對 사물, 사물 對 사물 간 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 융합 ICT 인프라

◆ **MTM (Mobile Trusted Module)**

모바일기기에 H/W 칩(chip)로 장착되어 인증, 암호화, 앱 검증 등 보안 기능을 고속으로 처리하는 모듈

◆ **N-Screen 서비스**

클라우드 컴퓨팅을 이용하여 동일한 멀티미디어 콘텐츠를 다양한 기기에서 시청할 수 있도록 고안된 시스템

◆ **OSMU (One-Source Multi-Use)**

하나의 소스로 여러 분야, 장르에서 활용하여 원천 소스보다 고부가가치를 창출하는 것을 의미

◆ **P2P (Peer to Peer)**

종단간의 단말장치(PC 또는 단말기)가 중앙 서버에 접속하여 데이터를 송·수신 하지 않고 상호간에 미리 규정된 통신 프로토콜을 기반으로 동작하는 방식

◆ **PDOS (Permanent Denial of Service)**

스마트폰 등 무선기기에 필요한 펌웨어(Firmware)를 원격 업데이트 할 때, 악성 코드가 삽입되어 목표 시스템을 다운시키는 서비스 거부공격

◆ **PIN (Personal Identification Number)**

기기에 대한 접근 및 동작을 제한하기 위해 설정된 일련의 숫자로 구성된 개인인증 번호 또는 패스워드

◆ **SDK (Software Development Kit)**

소프트웨어 개발 도구, 특정 운영체제 환경 또는 플랫폼에서 구동되는 프로그램 개발하기 위해 제공되는 개발 프로그램

◆ **SEED**

전자상거래, 금융, 무선통신 등에서 전송되는 중요한 정보를 보호하기 위해 국내 암호전문가들이 순수 국내기술로 개발한 128비트 블록암호알고리즘으로, 국내 TTAS.KO-12.0004 및 국제 ISO/IEC 18033-3 표준으로 지정

◆ **SNS (Social Network Service)**

웹상에서 이용자들이 인적 네트워크를 형성할 수 있게 해주는 서비스로 트위터, 싸이월드, 페이스북 등이 대표적인 서비스

◆ **SSL (Secure Socket Layer)**

인터넷 프로토콜(Internet protocol)이 보안면에서 기밀성을 유지하지 못한다는 문제를 극복하기 위해 개발된 프로토콜

◆ **TuFI (Trusted u-Financial Infrastructure) 모듈**

전자금융거래를 위해 필요한 주요 정보를 저장하고, 단말자체의 운영 환경을 보호(SW 위·변조 방지)하기 위한 메커니즘을 보유한 하드웨어 모듈

◆ **USIM (Universal Subscriber Identity Module)**

비동기 3세대 이동통신(WCDMA)의 단말기에 삽입되는 스마트카드로, 사용자인증, 과금, 글로벌 로밍, 전자 상거래 등 다양한 기능을 한장의 카드에 구현한 기술

◆ **VPN (Virtual Private Network)**

인터넷과 같은 공중망(public network)을 마치 전용선으로 사설망(private network)을 구축한 것처럼 사용할 수 있도록 해주는 메커니즘

◆ **WAP (Wireless Application Protocol)**

휴대폰(스마트폰)에서 이동통신망을 이용하여 무선 인터넷을 지원하기 위한 프로토콜

◆ **그린 ICT**

컴퓨팅 자원의 에너지 효율성을 극대화하고 폐기물의 재활용을 통한 환경 문제 해결을 주된 목적으로 하는 새로운 친환경 ICT 기술을 의미

◆ **개방형 모바일 플랫폼 (운영체제)**

구글사의 안드로이드, 리눅스 계열의 LiMo 및 스마트폰과 PDA의 운영체제로 이용되는 소프트웨어 플랫폼

◆ **개인위치정보 자기제어 시스템**

이용자가 자신의 위치정보를 확인할 수 있는 대상·시간·장소·방법 등을 단말기 또는 서비스 상에서 스스로 설정할 수 있도록 하는 시스템

◆ **단축 URL(Short Uniform Resource Locator)**

긴 인터넷 상의 파일주소(URL)를 모바일에서 이용하기 쉽도록 짧게 줄인 파일주소

◆ **디지털 워터마킹**

디지털 콘텐츠에 저작권 정보, 사용자 정보 등의 특정 정보, 즉 워터마크를 콘텐츠 자체에 삽입하고 추출하는 기술

◆ **매쉬업 (Mash-up)**

웹서비스 업체들이 제공하는 각종 콘텐츠와 서비스를 융합하여 새롭게 만든 웹서비스 또는 제작 행위

◆ **멀티미디어메시지 (MMS)**

기존 단문 문자 서비스(SMS)의 문자 위주의 서비스를 개선하여 사진, 동영상 또는 매우 긴 문장의 송·수신을 지원해주는 문자 서비스

◆ **모바일 IPTV**

각종 콘텐츠를 IP 방식으로 전송하는 기존 IPTV 기술에 무선 및 이동성 기술을 확장하여 이동단말을 통해 TV를 시청하는 새로운 서비스

◆ **모바일 VoIP**

초고속인터넷망을 기반으로 하는 유선 VoIP와 달리 Wi-Fi, WIBRO, 이동통신 3G 망 등을 이용하는 서비스

◆ **모바일 앱스토어 (App Store)**

모바일 기기에서 이용되는 앱의 제작 및 판매를 제공하는 모든 서비스를 지칭

◆ **모바일 오피스**

시간과 장소에 구애받지 않고 사무실 밖에서 회사 업무를 처리하는 시스템

◆ **모바일 클라우드**

IT자원을 필요한 만큼 빌려 쓰고 요금을 지불하는 클라우드 컴퓨팅이 모바일 영역까지 확대된 개념

◆ **문자메시지 (SMS)**

Short Message Service, 단문 문자 서비스이며 휴대폰(스마트폰) 사용자간 음성 통화 대신 간단한 내용의 문자를 통하여 의사소통을 할 수 있도록 제공되는 서비스

◆ **백도어 (Backdoor)**

침입자가 시스템에 침입한 후 자신이 원할 때 침입한 시스템을 재침입하거나 권한을 쉽게 획득하기 위해 만들어 놓은 일종의 비밀 통로

◆ **봇넷 (Botnet)**

IRC 망에 연결되어 있으면서 감염된 봇들로 구성된 네트워크

◆ **블루투스 (Bluetooth)**

근거리(10m ~ 100m)에서 개인간 파일, 정보 전송 및 음향기기 제어에 이용되는 무선통신 프로토콜

◆ **사회공학적기법 (Social Engineering)**

특정 환경에서 사용자로부터 특정 행위(접속, 실행 등)를 이끌어 낼 수 있도록 조작된 문구 및 콘텐츠를 전달(이메일, 메신저, 메시지 등)하는 기법

◆ **서비스 거부 공격 (Denial of Service)**

컴퓨터 시스템의 특정 부분을 지속적으로 공격하여 해당 자원에 대한 서비스를 더 이상 받지 못하도록 하는 공격 기법

◆ **스마트 TV**

TV에 OS가 설치되어 TV시청, 앱 설치, 게임, 웹서핑 등 다양한 서비스를 제공하는 차세대 TV 환경

◆ **스마트그리드 (Smart Grid)**

기존 전력망에 정보통신 기술을 사용하여 전력 공급자와 소비자가 양방향으로 정보를 교환하여 에너지 효율을 최적화하는 인프라

◆ **스마트 라이프 (Smart Life)**

스마트러닝(Learning), 스마트홈, 스마트카의 확산 등 삶속에서 ICT기술의 융합으로 나타날 편리하고 효율적인 생활상을 지칭

◆ **스마트사이어티 (Smartciety)**

Smart+Society의 합성어로 스마트폰 등 각종 스마트기기로 대화와 소통이 이루어지고 업무처리, 학습, 진료 등 사회 전반에 스마트 기술이 활용되는 사회를 지칭

◆ **스마트워크 (Smart Work)**

종래의 사무실 근무를 벗어나 언제 어디서나 효율적으로 일할 수 있는 업무 개념으로 모바일 기기를 이용해 업무를 수행할 수 있는 모바일 오피스, 영상 회의 시스템 등을 활용하는 원격근무, 재택근무 등이 포함

◆ **스마트패드 (Smart-pad)**

스마트폰과 PC·넷북의 장점을 갖춘 멀티미디어 디바이스로서 태블릿PC, 미디어 태블릿, 스마트북 등 다양한 명칭으로 호칭

◆ **스팸 (SPAM)**

광고를 목적으로 불특정 다수에게 전송되는 문자 메시지, 이메일 또는 게시판 글

◆ **악성코드 (Malicious Code)**

시스템을 파괴하거나 정보를 유출하는 등 악의적 활동을 수행하도록 의도적으로 제작된 코드

◆ **안드로이드 (Android)**

구글사의 휴대폰용 OS·미들웨어·응용프로그램을 한데 묶은 소프트웨어 플랫폼

◆ **암호화 (Encryption)**

데이터의 비밀성(기밀성) 유지를 위해 암호 알고리즘과 키를 사용하여 평문을 암호문으로 변환하는 과정

◆ **앱 게놈 프로젝트 (App Genome Project)**

일정 대상을 선정해 해당 앱의 기능적 특성, 보안위협 등을 상세 분석하여 앱의 악성행위 수행 여부 등을 파악하고자 하는 프로젝트

◆ **와이브로 (Wibro)**

대한민국 삼성전자와 한국전자통신연구원이 개발한 무선 광대역 인터넷 기술로서 고속 데이터 통신을 위한 무선 인터넷 접속 규격

◆ **와이파이 (Wi-Fi)**

AP(Access Point)가 제공되는 위치를 중심으로 무선랜(802.11) 서비스를 지원하기 위해 제공되는 무선 인터넷 프로토콜

◆ **원클릭 보안설정**

이용자들이 쉽게 무선 AP에 보안설정 강도를 높일 수 있도록 암호화 수준 (WEP→ WPA2)을 자동 변환시키는 프로그램

◆ **웜 (Worm)**

스스로를 복제하는 컴퓨터 프로그램으로 바이러스와는 다르게 숙주를 필요로 하지 않고 독자적으로 실행되며 일반적으로 대역폭을 잠식하는 것과 같은 방법으로 네트워크를 손상시키는 악성 프로그램의 한 종류

◆ **위치기반(LBS) 모바일 광고**

모바일 기기를 소지한 가입자의 현재 위치를 기지국 등을 통해 파악한 뒤 맛집 등 맞춤형 지역광고를 내보내는 것

◆ **위피 (WIPI)**

Wireless Internet Platform for Interoperability, 이동통신사간 상이한 모바일 플랫폼을 표준화시켜 국내 공통 휴대인터넷 플랫폼.

◆ **윈도우즈 폰 (Windows Phone)**

MS사의 새로운 모바일 OS로 기존의 윈도우즈 모바일과는 다른 UI 등 새로운 개념의 OS를 표방

◆ **인증 (Authentication)**

일반적인 인증의 의미는 참이라는 근거가 있는 무언가를 확인하거나 입증하는 행위

◆ **좀비 (Zombie)**

인터넷 상에서 악성코드로 인해 좀비처럼 작동하는 컴퓨터 및 시스템

◆ **코드 서명 (Code Signing)**

개발된 프로그램이나 콘텐츠의 신뢰성을 높이기 위해 공신력 있는 기관에서 발급하는 프로그램에 대한 확인

◆ **탈옥 (jail break)**

애플社 아이폰의 하드웨어(hardware)와 소프트웨어(software) 사이에 잠금장치를 해제(해킹)하는 행위

◆ **트윗 (Tweets)**

트위터에 글을 올리는 것을 의미

◆ **팔로워 (Followers)**

팔로잉과 반대 개념으로 내 글을 읽고 싶어 구독 신청한 사람을 의미

◆ **팔로잉 (Following)**

내가 추종하는 사람, 즉 자신이 구독 신청한 트위터 사용자 수를 의미

◆ **패치**

이미 발표된 소프트웨어 제품에서 발견된 사소한 기능 개선 또는 버그나 오류 등을 수정하기 위해 개발자(개발 회사)가 내놓는 업데이트 프로그램

◆ **펄토셀 (Femtocell)**

100조분의 1을 의미하는 펄토(femto)와 이동전화 커버리지 단위인 셀(cell)의 합성어로 가정 등 실내에서 사용되는 10mW이내의 초소형 이동통신 기지국

◆ **푸시(Push)형 광고**

웹상의 정보를 서버가 이용자에게 밀어주는 '푸시 기술(push technology)'을 이용해 사용자에게 콘텐츠(광고 포함)를 제공하는 것

◆ **피싱 (Phishing)**

개인정보(Private data)를 낚는다(fishing)라는 의미의 합성어로, 불특정 다수에게 메일을 보내 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 금융정보 등을 빼내는 신종사기 수법

<부 록>

1. 스마트폰 이용자 10대 안전수칙
2. 스마트폰 정보보호 주체별 역할(요약)
3. 국내외 주요 모바일 악성코드 사례
4. 알기 쉬운 무선랜 보안 안내서

(부록 Ⅰ) 스마트폰 ‘이용자 10대 안전수칙’

< ‘이용자 10대 안전수칙’ 및 요약설명 >

① 의심스러운 애플리케이션 다운로드하지 않기

- 스마트폰용 악성코드는 위·변조된 애플리케이션에 의해 유포 될 가능성이 있으므로 의심스러운 애플리케이션의 다운로드 자제

② 신뢰할 수 없는 사이트 방문하지 않기

- 의심스럽거나 알려지지 않은 사이트를 방문할 경우 정상 프로그램으로 가장한 악성프로그램이 사용자 몰래 설치될 수 있으므로, 신뢰할 수 없는 사이트 방문 자제

③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

- 멀티미디어메세지(MMS)와 이메일의 첨부파일 기능은 악성코드 유포 수단으로 사용되는 경우가 많으므로 발신인이 불명확하거나 의심스러운 메시지 및 메일은 열어보지 말고 즉시 삭제 필요

④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기

- 단말기를 분실 혹은 도난당했을 경우 개인정보 유출 및 악성코드 설치 방지를 위하여 단말기 비밀번호 설정 필요

⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기

- 악성코드 감염 가능성을 줄일 뿐만 아니라 단말기의 불필요한 배터리 소모를 막기 위해서는 블루투스 등 무선 인터페이스는 사용 시에만 활성화

⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기

- 이상증상 발생 시 스마트폰 매뉴얼에 따라 조치하며 조치 후에도 이상증상이 지속될 경우 악성코드에 의한 감염 가능성이 있으므로 백신 프로그램을 통한 단말기 진단 및 치료 필요

⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기

- 스마트폰용 악성프로그램은 특정 프로그램이나 파일에 숨겨져 유포될 수 있으므로, 프로그램 및 파일 다운로드 · 실행 시 스마트폰용 백신프로그램으로 바이러스 유무 검사 후 사용

⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기

- 스마트폰과 PC간 데이터 백업, 복사, 전송 등의 작업수행 과정에서 PC에 숨어있는 악성코드가 스마트폰으로 옮겨질 수 있으므로 PC에 대한 백신 프로그램 설치 및 정기점검 필요

⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기

- 스마트폰 플랫폼 구조를 변경(예: Jailbreak) 사용할 경우, 기본적인 보안기능 등에 영향을 주어 문제가 발생할 수 있으므로 이용자 스스로 구조 변경 자제

⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

- 해커들은 보안 취약점을 이용하고 다양한 공격기법을 사용하고 있으므로 이용자는 자신이 사용하는 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하여 사용

(부록 II) 스마트폰 정보보호 주체별 역할 (요약)

1. 이동통신서비스 사업자

① 모바일 악성코드 대응방안 수립 및 이행

- 모바일 악성코드의 감염으로 인한 이용자 피해를 최소화하고 서비스에 영향을 미치지 않도록 침해 대응체계 수립 및 이행 필요

② 사고접수 및 처리절차 수립

- 스마트폰 분실 및 도난 사고, 악성코드에 의한 침해사고 접수·처리를 위한 고객 대응 매뉴얼 마련 및 효과적 대응을 위한 유관기관으로의 정보·전파 공유

③ 악성코드 조기경보 서비스 제공

- 신규 모바일 악성코드의 출현 및 악성코드에 의한 피해 접수 시, 정보보호알림이 서비스(KISA 및 이통사 공동 제공)에 가입한 고객을 대상으로 악성코드 증상, 대처방안 등의 관련 내용 통보

④ 악성코드 감염 이용자 대상 서비스 이용 제한 기준 마련

- 스마트폰 악성코드 감염 이용자 대상 서비스 이용 제한 기준(본인 동의 절차 포함) 및 대응 프로세스를 마련하고 해당 사항을 이용 약관에 반영

⑤ 중요 S/W 패치 및 업데이트 서비스 지원

- 국가적·사회적 이슈가 되어 선제적 대응이 필요하다고 판단되는 스마트폰 악성코드에 대해서는 정부와 협의하여 이통사 포털 또는 앱스토어를 통한 전용백신 무료 배포

⑥ 안티스팸 서비스 제공

- 공개되거나 자체 분석한 스팸 발송번호에 대해 서버차원의 근원적 차단을 지원하고, 스팸메시지를 통해 전달되는 모바일 악성코드의 특성을 고려, 메시지 패턴분석을 통한 스팸 발송현황 탐지 서비스 지원을 고려하는 한편, 신고·접수된 스팸 발송번호 등을 등록하여 관리하는 방안 마련

⑦ 스마트폰 원격 제어 서비스 제공

- 단말기 제조사와의 협력을 통해 분실 및 도난당한 스마트폰에 대해 중요한 정보를 원격으로 삭제하거나 사용을 불가능하게 할 수 있는 서비스 제공 방안 검토

⑧ 단말기 보안설정 정보 제공

- 스마트폰 개통 시 가입축하 및 공지 메시지에 '스마트폰의 안전한 이용에 관한 내용 또는 관련 홈페이지 주소(URL)' 제공 방안 검토(관련 홈페이지는 방통위·KISA가 제공)

⑨ 네트워크 및 서버 관리

- 외부 공격으로부터 이통사 네트워크와 서버를 보호하기 위한 보안시스템 구축 및 발생 가능한 공격 정보의 사전 파악을 통한 원활한 운용성 확보

⑩ 모바일 악성코드 테스트 망 지원

- 국내 모바일 정보보호 분야 발전 및 관련업체의 효과적인 보안솔루션 개발 지원을 위해 테스트용 연구실 및 실험 장비 지원 고려

⑪ WAP Push 서비스 관리

- 스마트폰 단말기 이용자를 보호하기 위하여 가급적 특수한(관리적) 용도로만 WAP Push 서비스(Service Loading)를 제공하거나 Service Indication(Callback URL) 형태로 대체하는 방안 고려

⑫ 공조체제 유지

- 동종업체, 백신사, 단말기 제조사 및 정부기관과 긴밀한 협력 관계를 유지하여 모바일 악성코드와 관련한 정보 공유 및 침해사고 발생 시의 효과적 대응책 마련 필요

2. 스마트폰 단말기 제조사

① 단말기 잠금 기능 강화

- 이용자의 피해를 최소한으로 줄이기 위해 스마트폰 단말기 잠금 기능을 강화(4자리 이상 패스워드 자리 수 설정, 특수문자 및 영문자 사용 등)하는 방안 고려

② 블루투스 연결 가능 목록 관리 기능 제공

- 많은 이용자들이 블루투스 기능을 미사용할 시에도 활성화 상태를 유지하는 경우가 많기 때문에 블루투스 기능 활성화 상태에서 이용자가 사전에 연결 가능 목록에 등록한 단말기만 연결이 가능하도록 하는 기능 제공

③ 데이터 암호화 제공

- 이용자 정보보호 차원에서 개인 프라이버시와 관계가 있는 중요 파일(전화번호, 이메일, SMS 등)에 대한 데이터 암호화 모듈의 탑재 고려

④ 데이터 및 시스템 백업·복구 기능 제공

- 스마트폰 분실 및 손상으로 인한 신규제품 구입 시 이용자의 애플리케이션 재설치, 데이터 복구 등에 소요되는 시간을 절약할 수 있도록 스마트폰에 저장된 시스템 및 이용자 데이터 손실 이전 상태로 복원할 수 있는 백업 및 복구 기능 제공 고려

⑤ 데이터 및 시스템 접근 제어

- 스마트폰 내에 저장된 민감한 정보를 별도의 저장 영역에 보관하고, 패스워드 등 이용자 인증을 통해 접근을 허용하는 파일 접근 제어기능 구현 필요

⑥ 안티스팸 기능 제공

- 전화번호를 숨기거나 변조하며, 메시지 필터링을 우회하기 위해 특정 문자를 삽입하여 전송하는 우회적인 스팸에 대한 차단 및 제거 기능 검토

⑦ 안전성 검사 강화

- 스마트폰 침해사고로 인한 피해를 최소화할 수 있도록 단말기 출시 전, 다양한 응용 애플리케이션을 설치한 상태에서 다각적인 방법으로 단말기의 안전성을 검증하는 방안 마련

⑧ 단말기 보안설정 매뉴얼 제공

- 단말기 매뉴얼을 통해 기본 기능에 포함된 보안 기능에 대한 정보를 제공하고, 필요시 이용자가 손쉽게 단말기 보안설정 정보를 이용할 수 있도록 홈페이지를 통해 분실·도난, 악성코드 피해사례와 그에 대한 대처방법 등을 안내

⑨ 악성코드 샘플 확보 협력

- 악성코드로 인한 감염이 의심되는 스마트폰의 A/S 접수 시, 샘플 확보를 위해 백신사와 협력하고, 관련내용을 즉시 유관기관에 전파

⑩ 신속한 보안패치 및 업데이트 제공

- 스마트폰 OS 및 기본 프로그램의 취약점 발견 및 인지 시, 이에 대한 패치를 신속히 확보하고 S/W 업데이트 제공 방안 마련

⑪ 공조체제 유지

- 동종업체, 백신사, 이동통신사 및 정부기관과 긴밀한 협력 관계를 유지하여 모바일 악성코드와 관련한 정보 공유 및 침해사고 발생 시의 효과적 대응책 마련 필요

3. 모바일 백신 및 보안솔루션 사업자

① 신속한 악성코드 샘플 확보

- 이동통신사, 단말기 제조사 등과의 유기적 협력 관계 구축을 통한 신속한 악성코드 샘플 확보

② 모바일 환경을 고려한 백신 개발

- 다양한 스마트폰 운영체제를 감안하여야 하며, 저전력·저용량의 모바일 환경에 최적화 할 수 있도록 백신 연구 및 개발

③ 신속한 백신 업데이트

- 스마트폰 이용자 보호를 위해 신규 악성코드에 대한 신속한 백신 업데이트를 제공해야 하며, 업데이트는 PC 동기화, 무선망 및 이통망 등 다양한 인터페이스를 통해 가능하도록 지원(비상시 이용자가 이통망을 사용할 수밖에 없는 상황을 고려하여 이통사와의 협력을 통해 이용자 보호방안 마련)

④ 악성코드 정보 제공

- 백신프로그램은 악성코드 탐지 및 치료뿐만 아니라 악성행위(정보유출, MMS 무단 전송 등)에 대한 상세 정보 제공을 통해 이용자 스스로 피해여부를 확인하고 추가피해를 예방할 수 있도록 지원

⑤ 다양한 보안솔루션의 연구·개발

- 일반 이용자를 위한 안티스팸, 안티바이러스, 방화벽 등의 솔루션은 물론, 비즈니스 업무 수행자를 위한 VPN, 인증, DRM 등의 보안솔루션에 대한 지속적 연구 개발을 통해 스마트폰 서비스의 확산·발전에 노력

⑥ 공조체제 유지

- 동종업체, 이동통신사, 단말기 제조사 및 정부기관과 긴밀한 협력 관계를 유지하여 모바일 악성코드와 관련한 정보 공유 및 침해사고 발생 시의 효과적 대응책 마련 필요

4. 정부기관(방송통신위원회 및 KISA)

① 민·관 협의체 구성 및 지원

- 모바일 악성코드에 대한 정보 공유 및 침해사고 대응을 위한 민·관 협의체 구성·지원 및 정기적인 협력회의를 통한 모바일 보안 이슈 점검 및 협력체계 강화

② 이용자 보안인식 제고

- 스마트폰 이용자가 모바일 악성코드를 인지하고 대응할 수 있도록 인터넷을 포함한 각종 매체와 오프라인 세미나를 통해 다양한 정보 및 자료를 제공하여 이용자 보안인식 제고

③ 모바일 위협정보 수집 및 악성코드 분석·채집기술 개발

- 국내·외 주요 해킹·보안 관련 기관들과 정보 공유를 통해 모바일 위협정보를 조기 감지하여 전파 및 데이터베이스화하고 이용자가 스마트폰 악성코드 감염여부를 인지할 수 있는 기술적 판단방법 및 악성코드 분석·채집기술 개발 필요

④ 모바일 콘텐츠 안전성 확보 방안 검토

- 모바일 콘텐츠 시장의 활성화를 유지하면서 이용자를 보호할 수 있는 모바일 콘텐츠 안전성 검증 체계 구축 필요

⑤ 모바일 인터넷 고충 처리

- 다양한 모바일 기기를 통해 무선인터넷을 이용하는 개인이 겪을 수 있는 개인정보 침해, 금전적 피해 및 이로 인한 고충들을 처리하는 창구를 마련하여 문제 상담, 민원 처리, 필요시 정책 마련

⑥ 모바일 시큐리티 전문인력 양성 및 교육 강화

- 모바일 보안 분야의 국내 기술력을 확보하기 위해 기존 인력의 심화 교육 및 재교육을 통해 전문 인력을 양성하고 주기적인 개발자 윤리 교육으로 건전한 애플리케이션 개발·이용 환경 조성

⑦ 모바일 인터넷 환경에서의 보안강화 법제 개선

- 해킹, 이용자 개인정보 유출 등 모바일 인터넷 정보보호 이슈에 대응하기 위한 구체적인 조치 마련 및 법·제도 체계 정비

⑧ 안전한 이용을 위한 모바일 단말·인프라·서비스 보안 기술 개발 장려

- 스마트폰 등 모바일 기기의 안전한 이용 환경 조성을 위해 모바일 단말 및 플랫폼 보호 기술 개발, 모바일 인터넷 침해사고 대응 기술 및 콘텐츠 보호 기술 개발, 모바일 이용자 프라이버시 보호 기술 개발 등 지원

⑨ 모바일 서비스 침해예방 및 대응체계 구축

- 모바일 웹사이트 취약점 점검 강화 및 개방형 앱스토어를 통해 유포되는 모바일 악성코드 조기 탐지·차단 등의 침해예방 및 대응체계 마련

⑩ 모바일 보안위협 국제 대응 공조체제 마련

- 글로벌화되고 있는 사이버 위협에 대해 국외 유관기관과의 협력체계를 구축하여 모바일 보안 이슈에 대한 정보 공유 및 핫라인을 통한 침해사고 공동대응

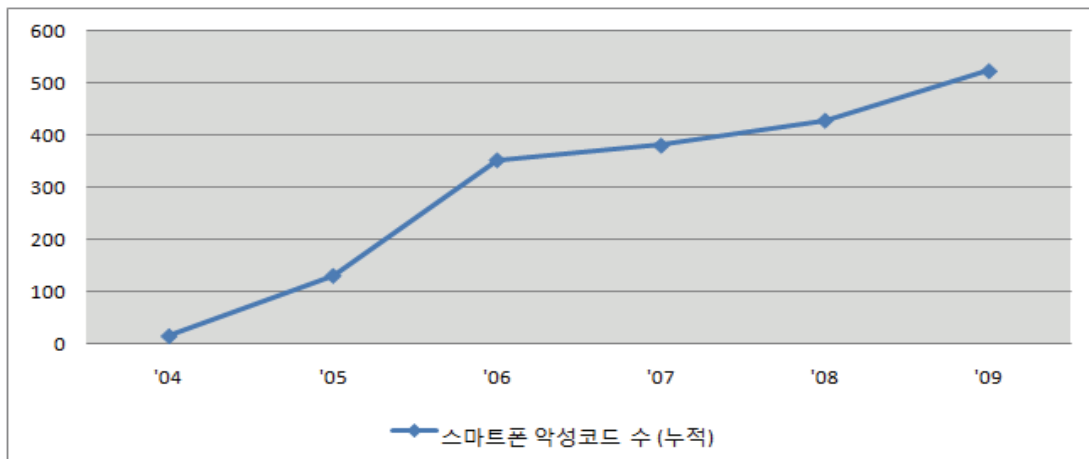
(부록 III) 국내외 주요 모바일 악성코드 사례

1. 해외 악성코드 발생 현황

- '09년 6월까지 발견된 스마트폰 악성코드는 총 524종이며, 증가추세 및 국내외 보도 자료를 볼 때 '10년 2/4분기 기준 약 600여 종으로 추정

※ '09년 6월 이후 스마트폰 악성코드 관련 공식 통계는 발표되지 않고 있음

- 최초의 스마트폰 악성코드는 Cabir로 '04년 8월 필리핀에서 발견



<전세계 스마트폰 악성코드 발견 수(누적), 출처: SMobile Systems>

- 스마트폰 악성코드의 약 60%는 트로이 목마(Trojan)이며 스파이웨어, 웜, 바이러스의 형태를 지님
- ※ 스마트폰 악성코드 중 95%이상이 심비안 OS(국내 보급률 미미함)에서 발생
- 해외에서 발생한 모바일 악성코드 중 95% 이상이 심비안 OS를 탑재한 스마트폰을 대상으로 동작하며,
- 개인정보 유출 · 이용자 부정요금 발생 · 단말기 이용 방해 · 단말기 무단 설정 변경 등과 같은 침해 사례 발생 가능
- ※ 현재까지 구체적 피해사례가 보고된 바는 없음
- 모바일 악성코드 별 피해유발 형태
- ※ ()안은 악성코드 명, 스마트폰 OS명

① 개인정보 유출 유형

- **(PBStealer, Symbian)** 전화번호부 압축 프로그램을 가장한 악성코드로 단말기에 저장된 전화번호를 외부 단말기로 유출시키는 피해 유발
- **(Arifat, Symbian)** 블루투스를 통하여 감염되는 악성코드로 MSN으로 위장하여 사용자의 아이디와 패스워드를 훔쳐 특정 번호로 SMS를 보내는 피해 유발
- **(FlexiSpy, 윈도우모바일)** 사용자의 통화 기록과 SMS 발송 정보를 수집하고 해당 정보를 특정 서버에 전송하는 악성코드로 SMS를 통하여 감염
- **(InfoJack, 윈도우모바일)** 인터넷 다운로드를 통하여 감염되며, 단말기의 시리얼 정보나 운영체제 정보를 송신하고, 인증 받지 않은 파일을 설치하는 악성코드

② 이용자 부정요금 피해 발생 유형

- **(Mosquit, Symbian)** 고액의 비용을 청구하는 서비스 전화번호 리스트를 포함하고 있어, 단말기 사용자 몰래 SMS 메시지를 해당 전화번호로 보냄으로써 고액의 서비스 이용료를 부과시키는 악성코드
- **(CommWarrior, Symbian)** 단말기 주소록에 있는 모든 연락처에 MMS 메시지를 발송함으로써 고액의 서비스 이용료를 부과시키는 악성코드
- **(RedBrowser, Symbian)** SMS를 무료로 전송할 것처럼 속이고, 실제로는 프리미엄 서비스가 되는 특정번호에 SMS를 무작위로 발송시키는 악성코드
- **(Allcano, Symbian)** 사용자의 휴대폰이 수신, 발신하는 SMS 문자를 특정번호로 전송시키는 악성코드
- **(Flocker, Symbian)** ICQ프로그램(메신저 채팅프로그램)으로 가장하여 실행을 유도하고 실행 후에는 프리미엄 서비스를 제공하는 특정 번호에 무작위로 문자를 발송 하게 하는 악성코드

③ 단말기 이용 방해 유형

- **(BlankFont, Symbian)** 감염된 단말기의 폰트 파일 사용을 불가능하게 하여 이용자가 글자를 읽지 못하도록 방해하는 악성코드
- **(Stealwar, Symbian)** 블루투스를 통해 감염되며 과도한 블루투스 트래픽을 생성하여 단말기 배터리를 빠르게 소모시키는 악성코드
- **(Palm/Phage, Palm OS)** Palm OS를 대상으로 하는 악성코드로 감염된 파일을 실행하면 설치된 프로그램이 실행되지 않는 피해 유발
- **(ikee worm, Jailbreaken iPhone OS)** 무선랜을 통해 감염되며, 'Together Forever'를 부른 가수 릭애슬리(Rick Astley)사진과 'ikee is never going to give you up' 이라는 문구가 나타나고, 다른 아이폰에 전파를 시도하는 악성코드
- **(Duh worm, Jailbreaken iPhone OS)** 무선랜을 통해 감염되어 무선 환경에서 botnet 형태로 운영되며 명령 서버를 통해 좀비 스마트폰을 원격제어할 수 있는 악성코드

④ 단말기 설정 무단 변경 유형

- **(Bootton, Symbian)** 단말기에 설치된 응용 프로그램의 아이콘을 변경하고 전화통화 외의 다른 기능은 사용하지 못하도록 하는 악성코드
- **(Skull, Symbian)** 감염된 단말기의 시스템 애플리케이션을 다른 파일로 교체함으로써 단말기를 사용할 수 없게 하며 단말기 내의 모든 애플리케이션 아이콘을 해골 이미지로 변경시키는 악성코드
- **(Palm/Vapor, Palm OS)** 실행되면 단말기 내의 모든 프로그램의 아이콘을 사라지게 하는 악성코드

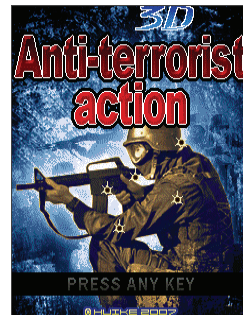
2. 국내 악성코드 발생 현황

- 국내 스마트폰 악성코드는 지난 4월 최초로 발생하였으며, 방통위에서 구성·운영 중인 '스마트폰 정보보호 민·관 합동대응반'의 사전 점검을 통해 발견·조치

- (악성코드 발생) '10. 4월 국내 최초로 국제전화 무단발신을 유발하는 악성코드 발생
 - ※ 해외(영국)에서 '국제전화 무단발신을 유발하는 윈도우 모바일 기반의 악성코드'가 발견됨에 따라 민·관 합동 대응반이 국내 유포여부를 점검(4.16~20)하는 과정에서 발견
- (악성코드 대응) '스마트폰 정보보호 민·관 합동대응반'에서 해당 사안을 사전에 탐지하고, 악성코드(WinCE/Terdial) 게임 차단, 백신개발 등을 통해 확산 방지 조치('10.4.21)
 - 이동통신 3사는 악성코드에 감염된 가입자를 파악하여 개별 SMS 연락 및 전화통화를 통해 전용백신을 제공하였으며,
 - 이동통신사, 스마트폰 제조사, 백신사 홈페이지 등에 악성코드 발생 및 대처 방안(전용 백신 배포)에 대한 보안 공지물 게시

< 참고자료 >

- 테러리스트 다이얼(WinCE/TerDial)
 - : 지난 4월 19일, 윈도우모바일 운영체제를 탑재한 스마트폰을 대상으로 한 국내 최초 스마트폰 악성코드로,



- '3D Anti Terrorist Action'이라는 3D Anti Terrorist Action 게임 캡처 화면 스마트폰 게임에 악성코드가 숨겨져 있으며, 게임이 설치되는 시점에 스마트폰을 감염시키고 국제전화 무단 발신을 시도
- 당시, 국내 스마트폰 가입자 약 160여만명 중 약 150여명 (0.01%)이 악성코드에 감염되었으나 민관 합동대응반의 신속한 대응으로 과금 피해사례는 발생하지 않았음

(부록 IV) 알기 쉬운 무선랜 보안 안내서

1 무선랜 사용하기



무선랜이란?

선 연결없이 인터넷을 이용할 수 있게 해주는 무선인터넷 이용환경을 의미하며, 흔히 와이파이(Wi-Fi)라고도 합니다.

※ 무선인터넷 기술은 와이브로, 3G 휴대폰(HSDPA 등), WLAN(Wireless LAN) 등이 있으며, 무선랜은 WLAN 기술을 이용한 서비스를 지칭합니다.



와이파이(Wi-Fi) : 국제 비영리단체인 WiFi Alliance에서 무선랜 표준인 802.11x 규약을 준수하여 무선랜 관련 장치와 연동됨을 보증함을 의미하는 인증마크를 의미합니다.

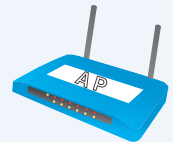


무선랜을 만들거나 사용하려면 무엇이 필요한가요?

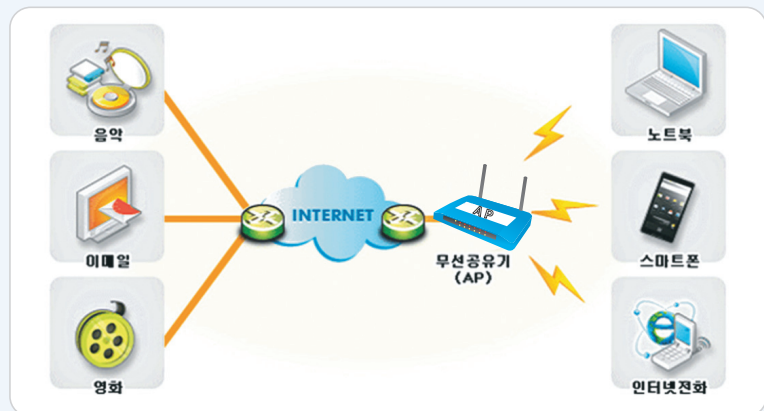
무선랜을 사용하기 위해서는 기본적으로 무선 AP와 무선 단말기(노트북, 스마트폰 등)가 필요합니다.



무선 AP(Access Point) : 무선공유기라고도 불리는 무선 AP는 인터넷 회선(유선랜, 와이브로 등)과 연결하여 무선랜 환경을 만들어주는 장치입니다.



●●● [무선공유기를 이용한 무선랜 환경의 예]





무선랜은 어디에 있나요?

우리 주변에서는 다음과 같은 무선랜 환경을 흔히 볼 수 있습니다.



개인이 구매·설치하여 이용하는 무선랜



인터넷 전화 설치시 제공되는 무선랜



공공시설에서 고객편의 제공을 위해 운영하는 무선랜



통신 사업자가 서비스 제공을 위해 구축한 무선랜

! 위와 같이 일반 이용자를 대상으로 하는 무선랜 환경 외에도 기업 등에서 내부 업무용으로 사용하기 위해 구축하는 무선랜도 있습니다.

2 무선랜 보안이 중요해요

 무선랜은 선 연결 없이 자유롭게 접속할 수 있으므로 악의적인 목적을 가진 사용자가 접속하여 개인정보 유출 등 다양한 보안 위협을 발생시킬 수 있습니다.

 **무선랜 이용자의 중요한 정보가 유출될 수 있습니다.**

- 보안이 설정되지 않은 무선랜으로 인터넷을 이용할 경우 악의적인 목적의 사용자가 접속하여 비밀번호 등 개인의 중요한 정보를 유출할 수 있습니다.

●●● [무선랜을 통한 개인정보 유출]



 **인터넷전화도 도청될 수 있습니다.**

- 보안이 설정되어 있지 않거나 취약한 무선 AP에 접속하여 인터넷전화를 이용할 경우 통화내용이 도청될 수 있습니다.

●●● [무선랜을 통한 도청]

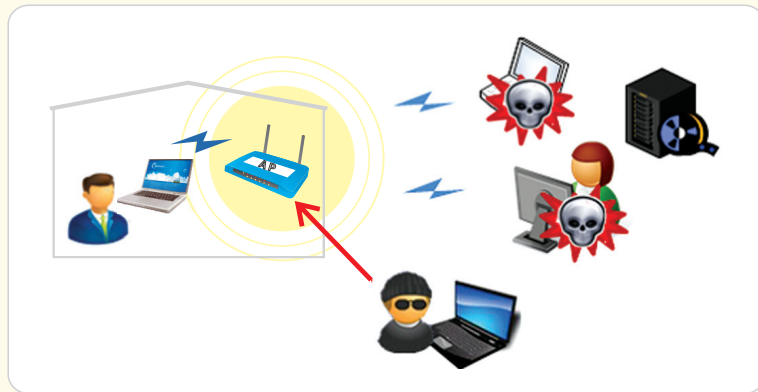




자신의 무선 AP가 악의적으로 이용될 수 있습니다.

- 보안설정이 되어 있지 않거나 미흡한 경우 자신의 무선 AP가 해킹, 불법 다운로드 등에 악용될 수 있습니다.
- 또한, 바이러스, 악성코드 등을 유포하는 경유지로 활용될 수 있습니다.

●●● [무선랜을 통한 불법다운로드, 악성코드 유포]



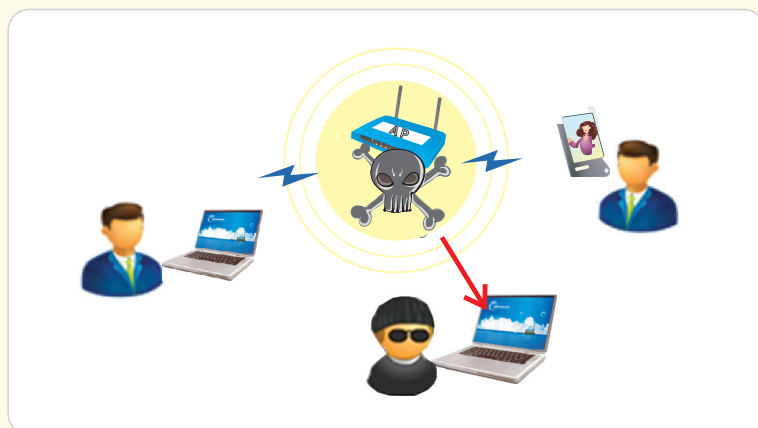
악의적인 목적으로 설치된 무선랜에 접속되어 개인정보가 유출될 수 있습니다.

- 해커가 개인정보 탈취등을 목적으로 구축한 무선랜에 접속할 경우 사용자의 개인정보가 유출될 수 있습니다.



Evil Twin : 이용자의 개인 정보를 수집하기 위해 정상 무선랜으로 위장 설치된 무선 AP

●●● [불법 무선랜 이용에 따른 개인정보 유출]



3 무선랜 안전 이용 수칙



무선랜 안전 이용 수칙을 준수하여 안전하게 무선랜을 이용할 수 있습니다.



- 1 무선공유기 사용시 보안기능 설정하기
- 2 무선공유기 패스워드 안전하게 관리하기
- 3 사용하지 않는 무선공유기는 꺼놓기
- 4 제공자가 불분명한 무선랜 이용하지 않기
- 5 보안설정 없는 무선랜으로 민감한 서비스 이용하지 않기
- 6 무선랜에 자동 접속 기능 사용하지 않기
- 7 무선공유기의 SSID를 변경하고 숨김 기능 설정하기



알기쉬운
무선랜 보안
안내서 << >>

4 무선랜 안전 이용 수칙 따라하기



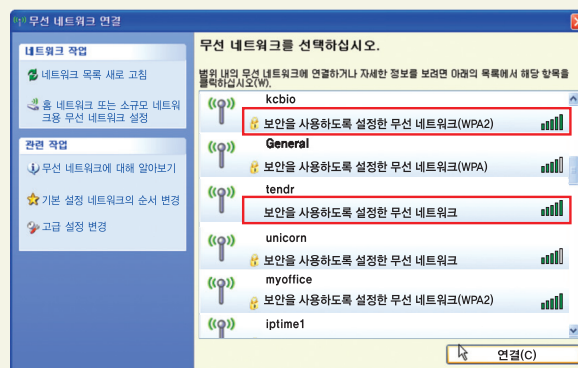
무선랜 안전 이용 수칙은 어떻게 사용할까요? 아래의 방법대로 따라하면 손쉽고도 안전하게 무선랜을 이용할 수 있습니다.

수칙 ① 무선공유기 사용시 보안기능 설정하기

무선공유기 사용 시 암호화/인증 등 보안기능을 설정하지 않으면 외부인이 무단으로 본인의 무선랜을 사용할 수 있으며, 이러한 경우 인터넷 속도가 느려지거나 개인정보 유출 등 해킹사고가 발생할 수 있습니다. 또한, 기업 내에서 보안기능 없는 무선랜을 사용하는 경우 사내 네트워크에 접근경로를 제공하여 해킹 등에 악용될 수 있습니다.

노트북에서 무선랜 보안설정 확인하는 방법

●●● [windows XP]



●●● [window 7]



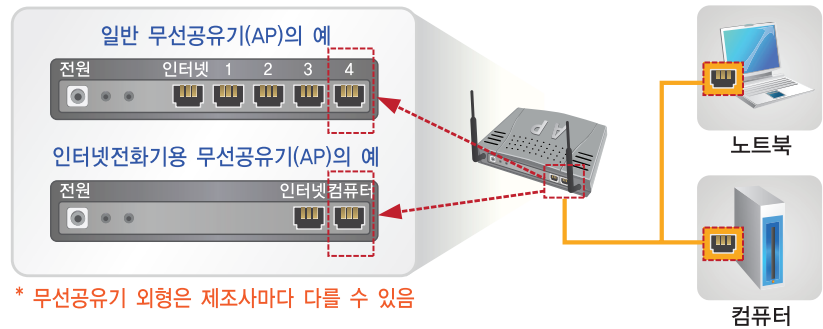
무선공유기 사용 시
암호화/인증 등 보안기능을
설정하지 않으면
해킹 대상이 됩니다.



알기쉬운 무선랜 보안 안내서 <<>>

● 노트북에서 무선랜 보안설정 확인하는 방법

① 무선공유기와 컴퓨터 또는 노트북을 연결합니다.



② 무선공유기 관리화면으로 접속합니다.

1 바탕화면의 웹 브라우저(ex. 인터넷 익스플로러 실행)



2 http://192.168.?.? 입력 (설정화면 IP주소)

※ 설정화면IP주소는
제품마다 다를 수 있습니다.
상세내용은 제품 메뉴얼을
참고하세요.

제품별 설정화면 IP 주소	
디링크	192.168.0.1
링크시스	192.168.1.1
아이피타임	192.168.0.1
유니콘정보시스템	192.168.123.254
애니게이트	192.168.10.1
한국쓰리콤	192.168.1.1

3 무선공유기 설정 초기화면 접속

기본정보	
인터넷 정보	
인터넷 연결상태	정상적으로 연결됨
인터넷 연결방식	고정 IP 연결
네트워크 정보	
내부 IP 주소	192.168.0.2 ~ 192.168.0.254
DHCP	DHCP 동작 중
무선 서비스 정보	
SSID	HomeAP
보안설정	암호화 미사용



③ 무선공유기 관리화면에서 보안기능을 설정 합니다.

1

기본 설정

- ▶ 상태 보기
- ▶ 자동 설정
- ▶ 수동 설정

고급 설정

- ▶ ID 선택
- 무선보안설정**
 - 무선 보안 설정
 - 무선 고급 설정
 - WPS
- ▶ 트래픽 제어
- ▶ 보안 설정
- ▶ 부가 기능
- ▶ 관리자
- ▶ 상태 정보

2 암호를 통한 보안 설정을 선택

보안 설정 ☒ 암호를 통한 보안설정

3 암호는 WPA2를 선택

암호 설정 ☐ WEP ☐ WPA ☒ WPA2

※ 제품에 따라 WPA는 WPAPSK, WPA2는 WPAPSK2로 표기될 수 있습니다.

보안설정	암호알고리즘	보안강도
WEP	RC4	낮음
WPA	RC4(TKIP)	보통
WPA2	AES	높음

4 암호알고리즘은 AES를 선택한 후 비밀번호를 입력

Algorithms ☐ TKIP ☒ AES

공유키(비밀번호)

☞ 무선 AP에서 제공하는 인증/암호 기술은 보안 강도에 따라 WEP, WPA, WPA2가 있으며, 안전한 이용을 위해 WPA2 설정을 권고합니다.



알기쉬운
무선랜 보안
안내서 <<>>

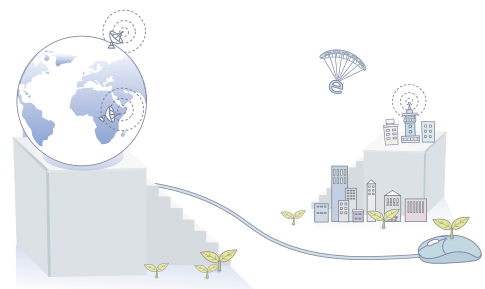
수칙 ② 무선공유기 비밀번호 안전하게 관리하기

무선공유기에 설치된 초기 비밀번호는 공개되어 있어 타인이 쉽게 접속할 수 있으므로 반드시 변경 후 사용해야 합니다. 또한, 설정한 비밀번호는 주기적으로 변경하고 추측하기 쉽거나 7자리 이하의 짧은 비밀번호는 사용하지 않아야 합니다.

● 안전한 비밀번호 관리 방법

- ▶ 무선AP의 비밀번호는 안전한 비밀번호 생성방법에 따라 생성합니다.
- ▶ 초기 설정된 무선 AP의 비밀번호는 빠른 시간 내에 새로운 비밀번호로 변경합니다.
- ▶ 무선 AP의 비밀번호는 주기적으로 변경합니다.
- ▶ 비밀번호 변경은 이전에 사용하지 않은 새로운 문자열로 변경합니다.
- ▶ 무선랜의 비밀번호가 제3자에게 노출되지 않도록 합니다.
- ▶ 제 3자에게 비밀번호를 유추할수 있는 정보, 힌트를 제공하지 않습니다.
- ▶ 제 3자에게 비밀번호가 노출된 경우, 즉시 새로운 비밀번호로 변경합니다.

※ 안전한 비밀번호 생성방법은 “비밀번호 선택 및 이용 안내서”를 참조하세요
(<http://www.118.or.kr> 의 자료실 참조)





수칙 ③ 사용하지 않는 무선공유기는 꺼놓기

사용하지 않는 무선공유기를 켜 놓을 경우 외부인이 불법다운로드, 해킹등에 악용할 수 있고 전력이 낭비될 수 있으므로, 사용하지 않는 무선공유기는 꺼놓아야 합니다.

● 무선공유기의 전원을 끄는 방법

●●● [무선공유기 전원을 끄거나 케이블을 분리합니다.]

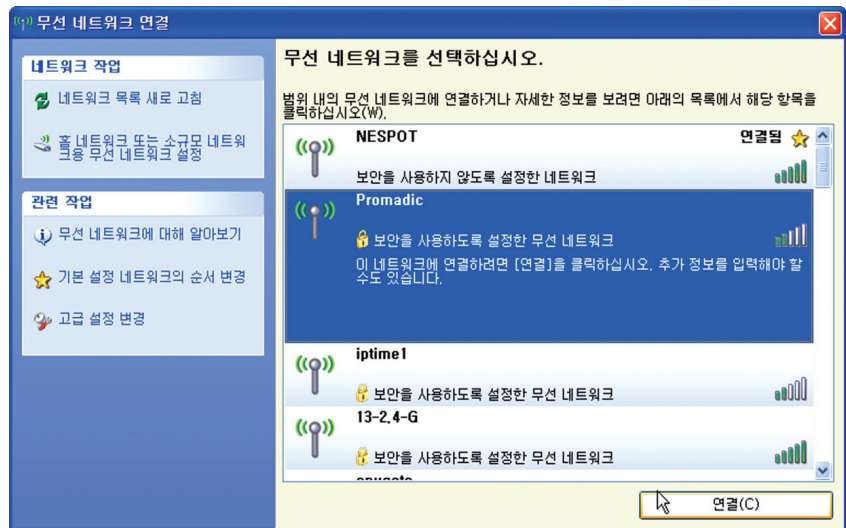


알기쉬운 무선랜 보안 안내서 <<>>

수칙 ④ 제공자가 불분명한 무선랜 이용하지 않기

개인정보 유출 등을 위해 악의적인 목적으로 설치한 무선공유기를 이용할 경우 개인정보가 쉽게 유출될 수 있습니다. 부득이 외부에서 무선랜 이용이 필요할 경우 본인이 잘 알고 있거나, 무선랜 이용 장소에서 제공자가 확인된 무선랜 만을 이용해야 합니다.

무선네트워크 연결 화면에서 무선랜 이름(SSID)으로 자신이 알고있는 무선랜인지 여부를 확인할 수 있습니다.



④ 제공자가 분명한 무선랜의 예

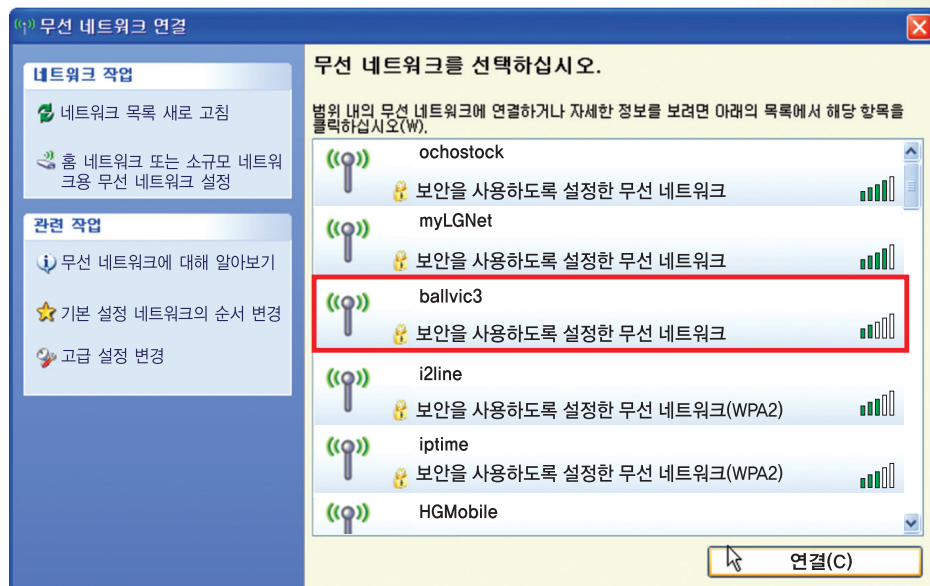
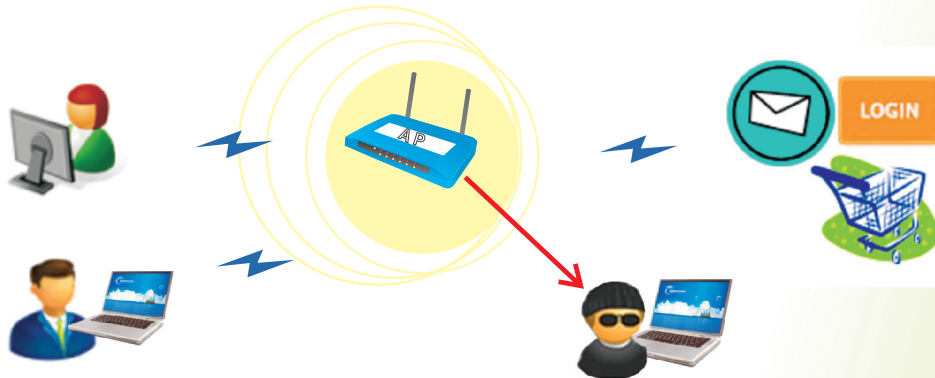
- ① 통신사, 지자체에서 제공하는 무료 와이파이존
예) KT의 QOOKnSHOW, ollehWiFi, SKT의 SKT-Tspot, LGU+의 U+ Wi-Fi100 등
- ② 커피숍 호텔 등에서 제공하는 무선랜
예) 커피숍, 호텔 등에서 유료 또는 무료로 제공하는 무선랜
- ③ 자신의 집에 설치된 인터넷전화기용 무선랜
예) KT_WLAN, myLGnet-xxx, 등
- ④ 자신이 설치했거나 기업에 설치된 사설 무선랜



수칙 ⑤ 보안설정 없는 무선랜으로 민감한 서비스 이용하지 않기

보안설정이 없는 무선랜의 경우 이용자의 접속행위, 개인정보 등이 유출될 수 있습니다. 부득이 무선랜 이용이 필요할 경우 금융거래, 기업업무, 로그인이 필요한 서비스, 개인정보를 입력하는 서비스 등 민감한 서비스는 가급적 사용하지 않아야 합니다.

● 보안이 설정되지 않은 무선랜 이용에 따른 개인정보 유출 화면



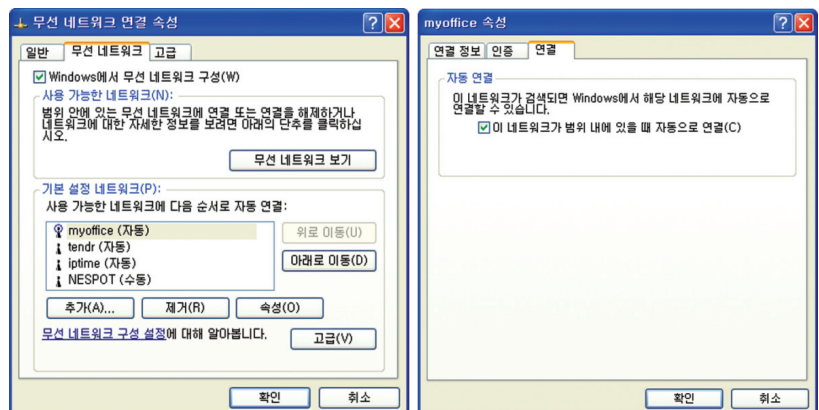
알기쉬운 무선랜 보안 안내서 <<>>

수칙 ⑥ 무선랜에 자동 접속 기능 사용하지 않기

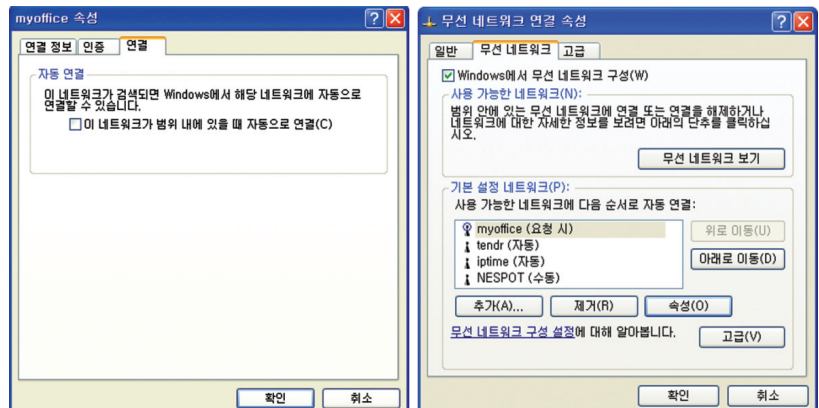
무선단말기에는 한번 접속한 무선랜에 자동으로 접속하는 기능이 있습니다. 무선랜 이름은 관리자가 임의로 변경가능하기 때문에, 해커가 잘 알려진 무선랜을 가장하여 자동접속 기능을 통해 이용자의 접속을 유도할 경우 개인정보 유출 등의 위험에 노출될 수 있습니다. 따라서, 무선랜의 자동접속기능은 끄고, 기존 접속한 무선랜 리스트는 주기적으로 지워야 합니다.

Windows XP에서 자동접속 해지 및 접속리스트 삭제

▶ [시작] → [설정] → [네트워크 연결] → [무선네트워크 연결] → [무선 네트워크] → [속성] → [연결] → 자동연결 체크해제



▶ [시작] → [설정] → [네트워크 연결] → [무선네트워크 연결] → [무선 네트워크] → 해당 무선랜 선택 → [제거]

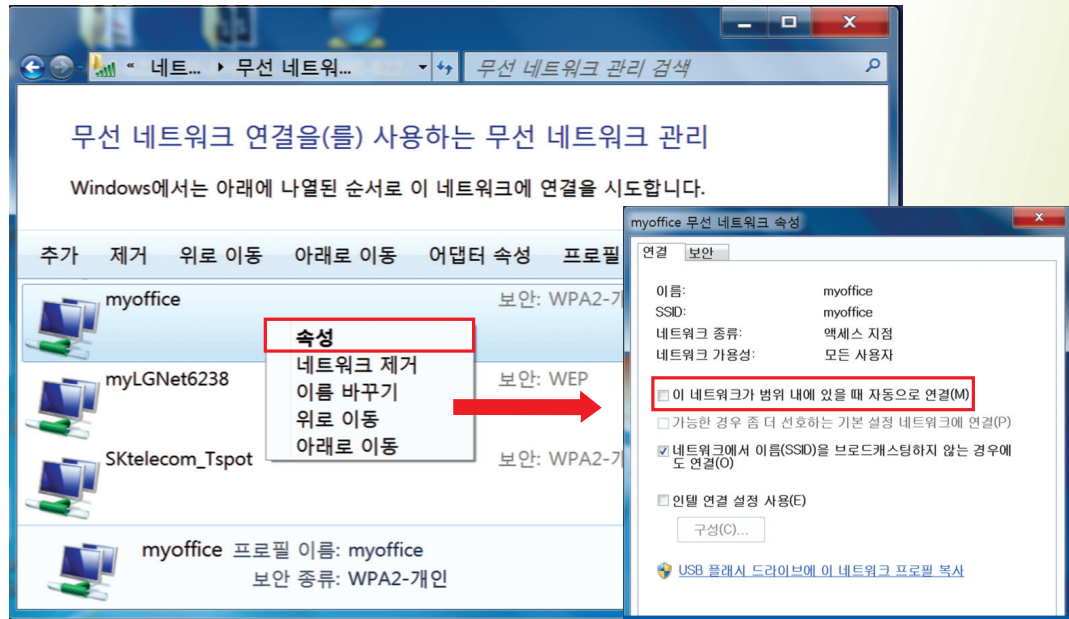




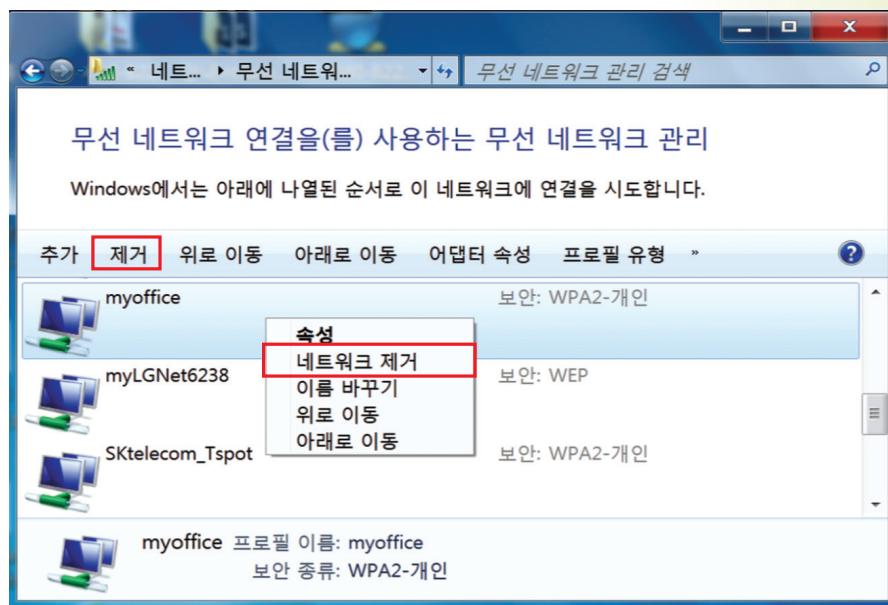
Windows 7에서 자동접속 해지 및 접속리스트 삭제



- ▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] → [무선 네트워크 관리] → 해당 무선랜 우클릭 → [속성] → 자동연결 체크 해제



- ▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] → [무선 네트워크 관리] → 해당 무선랜 선택 → 제거



알기쉬운
무선랜 보안
안내서 <<>>

수칙 ⑦ 무선공유기의 SSID를 변경하고 숨김 기능 설정하기

SSID(Service Set IDentification)란 무선랜을 구분하기 위한 이름입니다. SSID 숨김은 SSID 보안설정과 함께 사용 되어 보안성을 높이는 기능입니다. SSID를 숨김으로 할 경우 외부인은 해당 무선랜이 존재하는 지 알 수 없으므로 무선랜을 이용할 수 없어 해킹, 정보유출을 예방할 수 있습니다.

무선네트워크 이름(SSID) 변경 및 숨김 기능 설정 방법

① 무선공유기의 관리화면에 접속합니다.

※ 무선공유기 관리화면에 접속하는 방법은 “수칙①, 무선공유기 사용시 보안기능 설정하기” 를 참조하세요

② 무선 네트워크 설정 화면에서 SSID를 변경하고, 숨김기능을 체크 합니다.

●●● [무선 네트워크 SSID 이름변경 및 숨김기능 설정화면]



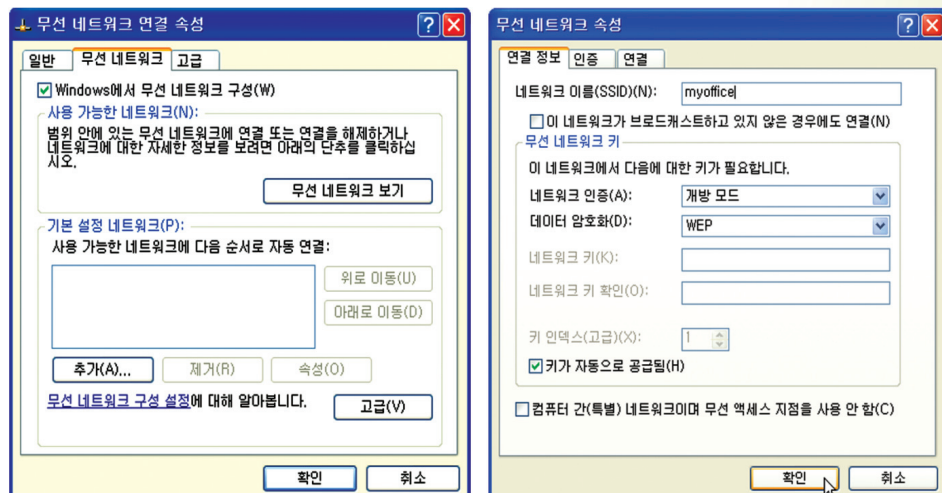
● SSID가 숨김으로 설정된 경우 접속 방법

- ▶ SSID가 숨겨져 있는 경우, 직접 SSID를 입력해야 합니다.

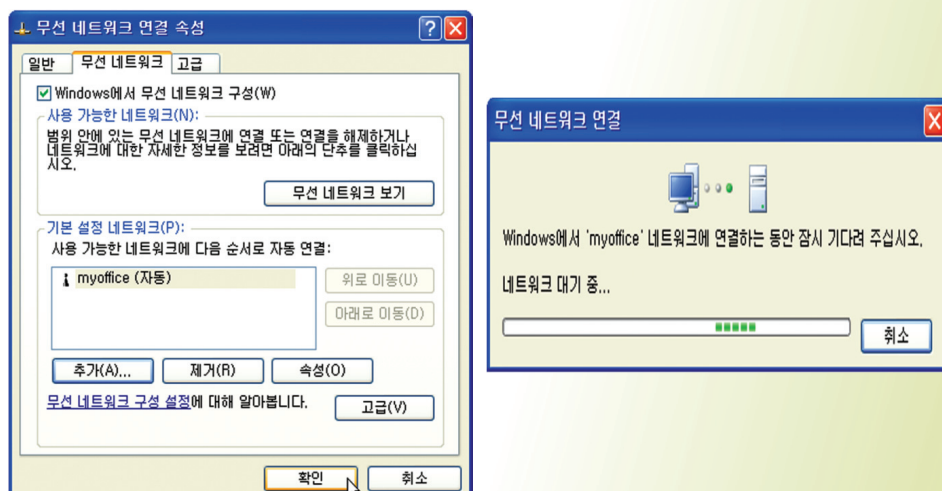
① Windows XP

- ▶ [시작] → [설정] → [네트워크 연결] → [무선네트워크 연결] → [고급 설정 변경] → [무선네트워크 탭] → [추가]
- ▶ [네트워크 이름(SSID)] 입력 및 [이 네트워크가 브로드캐스트 하고 있지 않은 경우에도 연결] 클릭, 인증/암호화, 암호키 입력

●●● [숨김 설정된 무선랜에 접속하기 위한 화면]



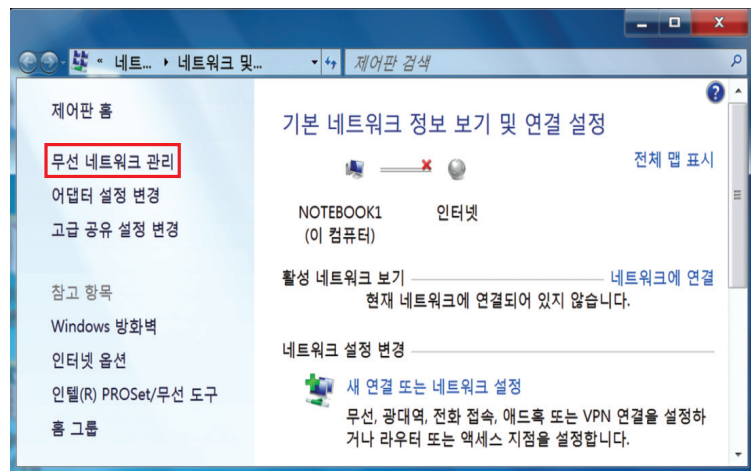
●●● [무선 네트워크 추가 화면, 접속되는 화면]



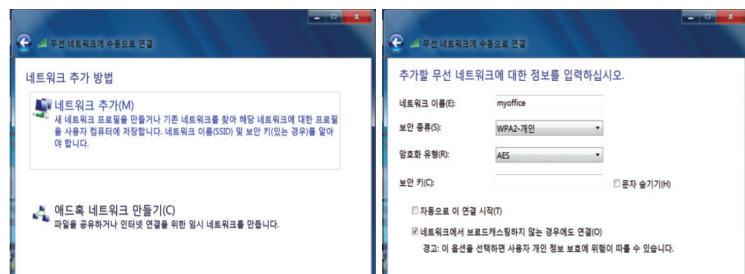
알기쉬운 무선랜 보안 안내서 <<>>

② Windows 7

- ▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] → [무선 네트워크 관리] → [추가]



- ▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] →





③ 스마트폰

●●● [숨김 설정된 무선랜에 접속하기 위한 화면]



●●● [아이폰에서 수동으로 무선랜 설정하는 화면]



[첨부 1] 무선랜 관련 사업자 · 제조사 문의처



무선랜 관련 서비스를 제공하는 통신사업자

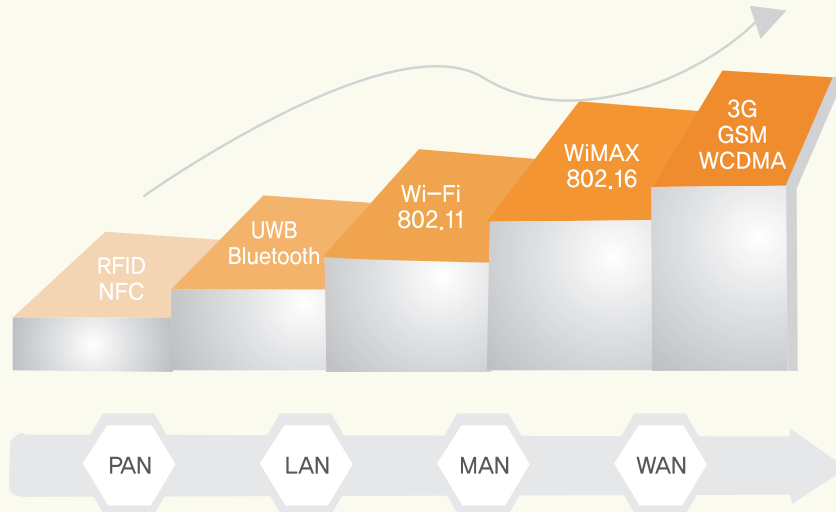
사업자	홈페이지	연락처	주요서비스
KT	http://www.kt.com	100	Qook-허브, Qook-인터넷전화, 네스팟, QOOKnSHOW, KT-에그 등
SKB	http://www.skbbroadband.com	106	anyway, SK_WLAN 등
SKT	http://www.sktelecom.com	02-1599-0011	T 와이파이존 등
LGU+	http://www.lguplus.com	02-1544-0010	LG U+ ACN, LG U+ 070 등

무선공유기를 제조하는 제조사



제조사		홈페이지	연락처	주요모델
국내	Airband	http://www.airband.co.kr	070-7759-8555	AWR-11N, AWR-MIMO, AWR-54G
	AnyGate	http://www.anygate.co.kr	02-566-3879	RG-5300A, RG-5500A, RG-5300N, RG-5500N, XM-3100N, XM-3300N, 등
	엑슬러	http://www.axler.co.kr	02-703-1303	LGI-IP10000N, LGI-IP10000N PLUS, LGI-IP9500S, LGI-IP6000T, 등
	CREWAVE	http://www.crewave.com	031-420-0990~2	CW-1100AP 등
	Danbi	http://www.dan-bi.com	1588-6076	Danbi
	FREEO	http://www.freeo.co.kr	1577-7107	FN151, FN301, FL15U, FR101
	iptime	http://iptime.co.kr	1544-8695	N1, N608, N6004, N104M, N604M, N6004M, G104i 등
	MODAFUN	http://www.modafun.com	0505-656-1380	PWR MD-760NI
	NEPLE	http://www.neple.co.kr	1544-9586	G101, G101Y, N101, N202
	NetTop	http://www.nettop.co.kr	1577-2940	NTP-N4, NTP-N6, NTP-NP 150, NTP-NV120, NTP-NV150
	NEXT	http://www.ez-net.co.kr	02-715-0372	NEXT-N1104, NEXT-640MIMO, NEXT-1004N 11N, NEXT-WR54G 등
	UNICORN	http://www.eunicorn.co.kr	1588-2713	AP-150R, DW-2200N, WB-1100NR, WB-3300NR, MW-9000N 등
	Windy31	http://www.windy31.co.kr	070-7018-0024	windy31
	ZIO	http://www.izio.co.kr	1588-1696	ZIO-1500N, FX11s, V11, Q11, Z11 등
국외	3COM	http://www.hp.com	080-698-0880	A7700, A8700, A9100, A9500 등
	ASUS	http://support.asus.com	02-718-0164	RT-N11
	BELKIN	http://www.belkin.com/kr	00798-8521-9469	N+_F5D8232-4, N+_F5D8235-4
	BUFFALO	http://www.buffalotech.co.kr	02-2057-2094~5	WCR-GN, WHR-G300N, WHR-G300N V2 등
	D-Link	http://www.d-link.co.kr	02-890-3540~4	DWL-3200AP, DWL-8200AP, DWL-8500AP, DWL-8600AP 등
	imation	http://www.imation.co.kr/imation.php	1544-9152	R104G, R104N
	levelone	http://global.level1.com	080-087-0001	WAP-3010, WAP-3100
	CISCO	http://cisco.com/kr	080-808-8082	WRT110, WRT120N, WRT160N, WRT160NL, WRT320N, WRT610N 등
	NETGEAR	http://www.netgear.co.kr	080-638-4327	WG 602

[첨부 2] 무선랜 기술 표준



- PAN : Personal-area networks
- LAN : Local-area networks
- MAN : Metropolitan-area networks
- WAN : Wide-area networks

무선랜 기술 표준

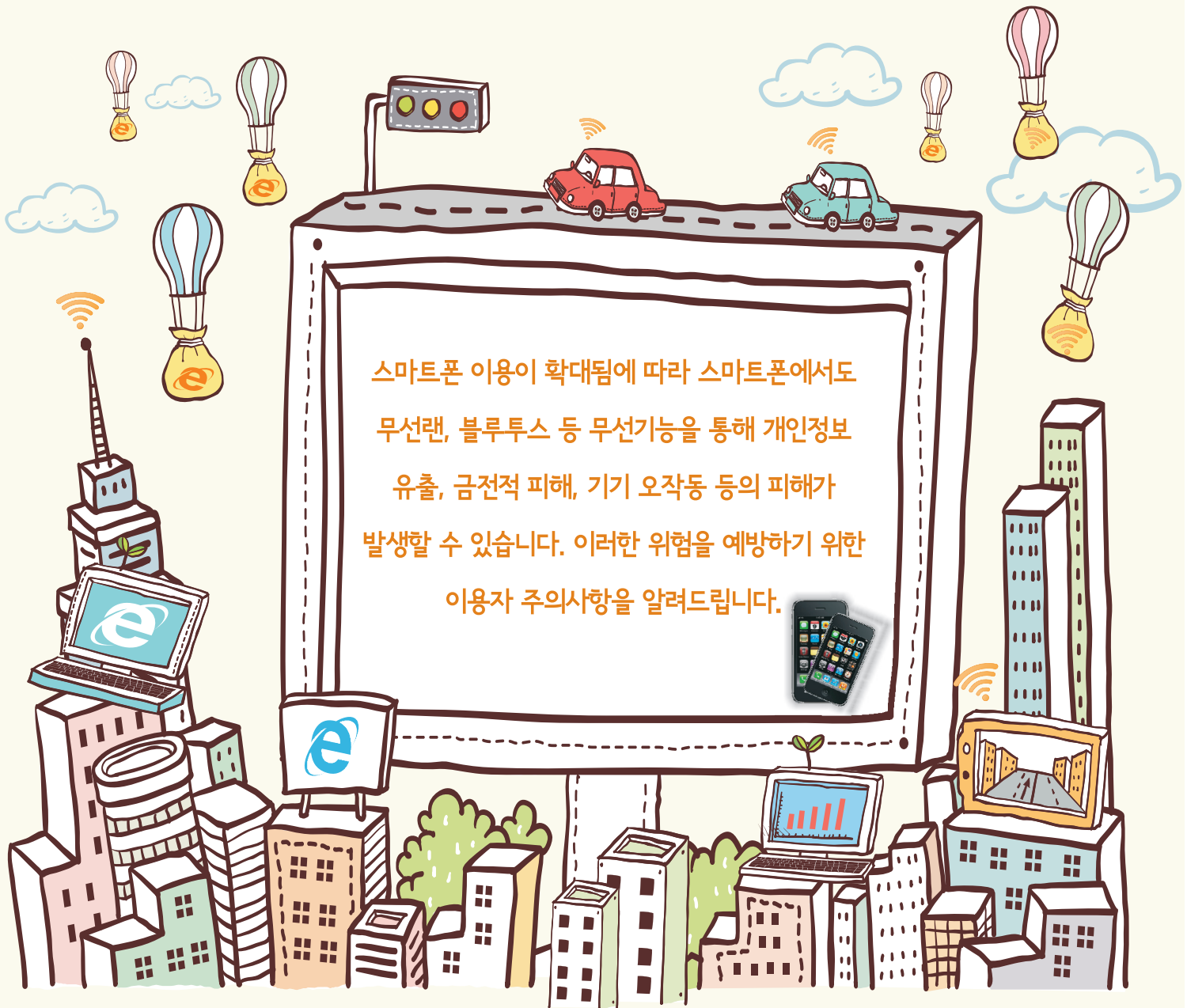
무선랜 표준	표준 제정시기	주파수대역	데이터속도(최대)	서비스 범위(실내)
802.11	1997	2.4GHz	2 Mbps	20M
802.11a	1999	5GHz	54 Mbps	35M
802.11b	1999	5GHz	11 Mbps	35M
802.11g	2003	2.4GHz	54 Mbps	35M
802.11n	2009	2.4 / 5GHz	540 Mbps	70M



무선랜 보안기술 표준

설정 방식	보안기술	인증	암호화
개인 모드 (Personal-mode)	WEP	PSK	RC4 (64bit/128bit)
	WPA	PSK	RC4-TKIP
	WPA2	PSK	AES-CCMP
엔터프라이즈 모드 (Enterprise-mode)	WPA	IEEE 802.1X/EAP	RC4-TKIP
	WPA2	IEEE 802.1X/EAP	AES-CCMP

[첨부 3] 스마트폰 안전하게 이용하기



※ 안전한 스마트폰 이용에 대한 세부 내용은 “스마트폰 안전이용 수칙” 을 참조하세요
(<http://www.118.or.kr> 의 자료실 참조)



의심스러운 애플리케이션은 다운로드하지 않습니다.

신뢰할 수 없는 사이트는 방문하지 않습니다.

발신인이 불명확하거나 의심스러운 메시지 및 메일은 삭제합니다.

비밀번호 설정 기능을 이용하고 정기적으로 비밀번호를 변경합니다.

블루투스 기능 등 무선인터페이스는 사용 시에만 켜놓습니다.

이상증상이 지속될 경우 악성코드 감염여부를 확인합니다.

다운로드한 파일은 바이러스 유무를 검사한 후 사용합니다.

PC에도 백신 프로그램을 설치하고 정기적으로 바이러스를 검사합니다.

스마트폰 플랫폼의 구조를 임의로 변경하지 않습니다.

운영체제 및 백신 프로그램을 항상 최신 버전으로 업데이트 합니다.

‘스마트 모바일 시큐리티 종합계획’ 집필 및 자문 위원

1. 종합계획 집필위원

기관명	소속	직책	성명	기관명	소속	직책	성명
방송통신위원회	네트워크정책국	국장	황철중	한국인터넷진흥원	인터넷정책단	단장	원유재
방송통신위원회	네트워크정보보호팀	팀장	박철순	한국인터넷진흥원	정책연구팀	팀장	황성원
방송통신위원회	네트워크정보보호팀	사무관	엄지현	한국인터넷진흥원	정책연구팀	책임	이종화
방송통신위원회	네트워크정보보호팀	사무관	김신겸	한국인터넷진흥원	정책연구팀	주임	지순정
방송통신위원회	네트워크정보보호팀	사무관	배영식	한국인터넷진흥원	해킹대응팀	선임	전은국
방송통신위원회	네트워크정보보호팀	사무관	구교영	한국인터넷진흥원	미래인터넷팀	팀장	김주영
방송통신위원회	네트워크정보보호팀	사무관	이상국	한국인터넷진흥원	미래인터넷팀	선임	김종표
방송통신위원회	네트워크정보보호팀	주무관	김양근	한국인터넷진흥원	무선인터넷팀	팀장	백종현
방송통신위원회	네트워크정보보호팀	주무관	이재곤	한국인터넷진흥원	무선인터넷팀	수석	박순태
방송통신위원회	네트워크정보보호팀	주무관	홍성준	한국인터넷진흥원	융합보호R&D팀	팀장	정현철
방송통신위원회	네트워크정보보호팀	주무관	김인회	한국인터넷진흥원	융합보호R&D팀	파트장	임채태
방송통신위원회	네트워크기획보호과	과장	허성욱	한국인터넷진흥원	코드분석팀	팀장	전길수
방송통신위원회	네트워크기획보호과	사무관	최승만	한국인터넷진흥원	코드분석팀	선임	서승현
방송통신위원회	개인정보보호윤리과	과장	김광수	한국인터넷진흥원	웹보안지원팀	팀장	서진원
방송통신위원회	개인정보보호윤리과	사무관	김지원	한국인터넷진흥원	웹보안지원팀	수석	박성우
방송통신위원회	네트워크윤리팀	팀장	엄 열	한국인터넷진흥원	스팸대응팀	팀장	노명선
방송통신위원회	네트워크윤리팀	사무관	박승철	한국인터넷진흥원	스팸대응팀	책임	권현오
방송통신위원회	인터넷정책과	과장	홍진배	한국인터넷진흥원	개인정보보호기획팀	팀장	박찬기
방송통신위원회	인터넷정책과	사무관	양기성	한국인터넷진흥원	개인정보보호기획팀	책임	윤권일
방송통신위원회	지능통신망팀	팀장	김정렬	한국인터넷진흥원	법제분석팀	팀장	이창범
방송통신위원회	지능통신망팀	사무관	양충식	한국인터넷진흥원	KISA아카데미팀	팀장	김창현
방송통신위원회	스마트워크전략팀	팀장	김꽃미음	한국인터넷진흥원	홍보팀	팀장	유진호
방송통신위원회	스마트워크전략팀	사무관	김순철	한국인터넷진흥원	인터넷윤리팀	팀장	강안구
한국전파진흥원	방통위 정보보호PM	PM	정경호	한국전자통신연구원	휴먼인식기술연구팀	팀장	김정녀
한국전파진흥원	방통위 정보보호PM	선임	유종호	한국전자통신연구원	인프라보호연구팀	팀장	서동일

2. 종합계획 자문위원

기관명	소속	직책	성명	기관명	소속	직책	성명
KAIST	시스템공학과	교수	김세현	SKT	정보보호팀	매니저	김인호
성균관대학교	정보통신공학부	교수	정태명	KT	정보보호팀	부장	이상훈
고려대학교	정보통신공학부	원장	임종인	KT	정보보호팀	부장	박상수
고려대학교	정보통신공학부	교수	이동훈	KT	정보보호팀	차장	유기무
충남대학교	컴퓨터공학	교수	류재철	LGU+	정보보안팀	부장	문영식
순천향대학교	정보보호학	교수	염홍열	LGU+	정보보안팀	부장	박민호
순천향대학교	정보보호학	교수	이임영	팬택	SW개발	주임	김성진
선문대학교	컴퓨터정보학	교수	박정호	SGA	-	주임	한인회
충북대학교	경영정보학	교수	김태성	하우리	보안대응센터	팀장	김정수
성균관대학교	컴퓨터공학	교수	김승주	잉카인터넷	시큐리티대응센터	차장	문종현
서울여자대학교	정보보호학	교수	박춘식	이스트소프트	보안대응팀	팀장	박정철
서울여자대학교	정보보호학	교수	김형중	안철수연구소	-	상무	조시행
중앙대학교	정보시스템학	교수	김정덕	안철수연구소	서비스개발팀	팀장	최은혁
성균관대학교	정보통신공학	교수	정진욱	소만사	-	전무	최일훈
금융보안연구원	정보보안본부	본부장	성재모	지란지교	연구소	소장	윤두식
ETRI	융합기술연구부문	부문장	손승원	SK컴즈	정보보호팀	팀장	하중수
SKT	정보보호팀	팀장	이기혁	법무법인 광장	-	변호사	고환경
SKT	정보보호팀	매니저	최준섭				

※ 이외에도 ‘인터넷 정보보호 협의회’, ‘스마트폰 정보보호 민·관 합동대응반’, ‘모바일 시큐리티 포럼’, ‘미래융합 IT서비스 보안연구회’ 등의 위원들도 자문에 참여

네트워크정책국 주요 정책추진 현황

1. 방송통신경쟁력 강화 및 융합서비스 활성화를 위한 **방송통신망 중장기 발전계획**(‘09.1.30)
2. 모바일 인터넷활성화 추진계획(‘09.3.11)
3. 인터넷상 주민등록번호 대체수단 이용 활성화 기본계획(‘09.3.31)
4. Giga 인터넷 활성화를 위한 **Giga 인터넷도입 추진계획**(‘09.4.30)
5. 이동통신사업자 개인정보 관리체계 자율개선계획(‘09.5.1)
6. 무선 인터넷활성화 추진계획(‘09.9.29)
7. 사물통신 기반구축 기본계획(‘09.10.14)
8. **2009년 스팸방지 종합대책**(‘09.10.16)
9. 클라우드컴퓨팅 활성화 종합계획(‘09.12.30)
10. 스마트모바일 강국 실현을 위한 **무선 인터넷활성화 종합계획**(‘10.4.21)
11. **미래인터넷 추진전략**(‘10.5.19.)
12. LBS산업육성 및 사회안전망 고도화를 위한 **위치정보 이용활성화계획**(‘10.6.10)
13. **스마트워크 인프라 고도화 및 민간 활성화 계획**(‘10.7.20)
14. 차세대 인터넷주소(IPv6) 추진계획(‘10.9.15.)
15. 인터넷광고 시장 활성화 종합계획(‘10.10.14)
16. 개인정보보호 관리체계 인증제 도입(‘10.11.15)
17. 스마트 모바일 오피스 추진계획(‘10.11.23)
18. 스마트 모바일 시큐리티 종합계획(‘10.12.24)

