

2020 vol.3

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA REPORT

CONTENTS

ISSUE

- 01 사회적/물리적 거리두기가 IT 산업과 사회에 미치는 영향과 주요 이슈
[한상기/ 테크프론티어 대표]
- 02 감염병예방방법의 정보공개 규정 살펴보기 - 공공의 건강 및 안전, 그리고 프라이버시의 균형
[이진규/ 네이버주식회사 개인정보보호책임자(이사)]
- 03 원격근무, 회사를 떠나 일한다는 것
[최호섭/ 디지털 칼럼니스트]
- 04 코로나19 확산에 따른 비대면 원격수업에 대한 단상
[윤대균/ 아주대학교 소프트웨어학과 교수]
- 05 비대면 협업툴의 미디어적 필수 요건에 대하여
[최홍규/ EBS 연구위원]
- 06 코로나19가 앞당긴 원격 사회 이후 사이버 대피 공간을 위한 가상현실의 역할
[최필식/ 기술작가]

TREND

- 07 RSAC 2020 - 보안 트렌드 살펴보기
[송혜인/ 한국인터넷진흥원 보안산업단 해외사업팀장]
- 08 연합학습으로 AI 빅브라더 문제 해소
[유성민 /IT 칼럼니스트]
- 09 미국과 영국의 드론 대응(Ant-drone) 정책 및 전략 추진동향
[이응용/ AI&security 애널리스트]
- 10 중국 “네트워크 안전등급 보호 제도” 개요 및 관련 국가표준 제정 동향
[정연수/ 한국인터넷진흥원 연구위원]
- 11 광주의 미래 - 인공지능 기반 산업융합 집적단지 조성사업
[나종희/ 광주대학교 컴퓨터공학과 교수]
- 12 미래인터넷 기술 성공의 핵심 포인트, 보안
[김대엽/ 수원대학교 정보통신학부 교수]

KISA 주요 활동 안내

- 01 민간 500대 웹사이트 플러그인 개선 실적 및 웹 표준 전환 지원사업 안내
- 02 개인정보보호 국제협력센터 안내

KISA Report의 내용은 한국인터넷진흥원의 공식 견해와 다를 수 있습니다.

주제 제안 및 정기 메일 신청 | kisareport@kisa.or.kr

인터넷 정보보호 관련 이슈, 현안 등 궁금한 내용을 보내주시면 선별 후 보고서 주제로 선정됩니다.

또한, KISA Report 온라인 서비스 제공을 원하실 경우 신청해주시면 매월 받아보실 수 있습니다.

중국 “네트워크 안전등급 보호 제도” 개요 및 관련 국가표준 제정 동향

정연수 (meet@kisa.or.kr)

한국인터넷진흥원 연구위원

네트워크 안전등급 보호 제도

■ 제도 개요

중국은 네트워크를 중요도에 따라 보호수준을 다르게 적용시키는 <네트워크 안전등급 보호 제도>의 시행을 준비하고 있다. <네트워크 안전법> 제21조에서는 “국가는 네트워크 안전등급 보호 제도를 시행한다. 네트워크 운영자는 네트워크 안전등급 보호 제도의 기준에 따라 안전보호 의무를 이행하여 네트워크가 방해, 파괴 또는 비인가 방문을 차단하도록 보장하고, 네트워크 데이터의 유출 또는 도난, 변조를 방지한다.”라고 <네트워크 안전등급 보호 제도>의 시행을 명문화하고 있다. 중국 공안부는 동 제도의 시행을 위하여 <네트워크안전등급보호조례>¹⁾의 제정을 추진하는 한편, 관련 표준을 제·개정 하고 있다. 그러나 <네트워크 안전등급 보호 제도>는 새로운 제도는 아니라 2007년부터 시행해오던 <정보시스템 안전등급 제도>를 기존의 정보시스템 위주에서 클라우드 컴퓨팅, 빅데이터, 사물인터넷, 모바일인터넷 등으로 확대한 것이다. 기존의 <정보시스템 안전등급 보호 제도>와 구별하기 위하여 <네트워크 안전등급 보호 제도>를 <안전등급 보호제도 2.0(Cybersecurity Classified Protection 2.0)>이라고도 부른다.

<정보시스템 안전등급 보호 제도>와 ,네트워크 안전등급 보호 제도> 구분

구 분	정보시스템 안전등급 보호 제도 (안전등급 보호제도 1.0)	네트워크 안전등급 보호 제도 (안전등급 보호제도 2.0)
시행근거	<ul style="list-style-type: none"> ▶ 컴퓨터 정보시스템 안전 보호 조례 (국무원령) ▶ 정보안전등급 보호 관리방법(고시) 	<ul style="list-style-type: none"> ▶ 네트워크안전법 제21조 ▶ 네트워크안전등급보호조례(의견수렴안)

1) 공안부는 한국의 대통령령에 해당하는 국무원령인 <네트워크안전등급보호조례> 의견수렴(안)을 발표(2018. 6. 27.)하였고, 현재는 공포 절차를 준비 중에 있다.

시행년도	2007년도	시행 준비 중
적용대상	▶ 컴퓨터 정보시스템	▶ 컴퓨터 정보시스템. ▶ 클라우드 컴퓨팅 ▶ 빅데이터 ▶ 사물인터넷 ▶ 모바일인터넷
관련 표준	▶ 정보시스템 안전등급 보호 기본요구(GB/T 22239-2008) ▶ 정보시스템 등급 보호 보안 설계 기술 기준(GB/T 25070-2010) ▶ 정보시스템 등급 보호 평가요구(GB/T 28448-2012) ▶ 정보시스템 안전보호 등급구분 준칙(GB 17859-1999) 등	▶ 네트워크 안전등급 보호 기본요구(GB/T 22239-2019) ▶ 네트워크 안전등급 보호 안전설계 기술요구(GB/T25070-2019) ▶ 네트워크 등급 보호 평가요구(GB/T 28448-2019) 등

[출처: 한국인터넷진흥원 자료]

■ 네트워크 안전등급 부여 방법 및 절차²⁾

〈네트워크 안전등급〉은 국민·조직의 합법적 권익, 공공이익·사회질서, 국가안전에 미치는 피해의 정도를 감안하여 보호대상(객체)과 침해정도에 따라 다음과 같이 5개 등급으로, 등급에 따라 각기 보호수준과 방법을 다르게 적용하도록 하고 있다.

- 제1급 : 네트워크 손상 시 관련된 국민과 조직의 합법적 권익에 손해를 끼치나, 국가 안전과 사회 질서, 공공이익을 해치지 않는 일반적인 네트워크
- 제2급 : 네트워크 손상 시 관련된 국민과 조직의 합법적 권익에 심각한 손해를 끼치거나, 사회질서와 공공이익에 손해를 끼치나, 국가안전을 해치지 않는 네트워크
- 제3급 : 네트워크 손상 시 관련된 국민과 조직의 합법적 권익에 특별히 심각한 손해를 끼치거나, 사회질서와 공공이익에 심각한 손해를 끼치거나, 혹은 국가안전에 해치는 중요 네트워크
- 제4급 : 네트워크 손상 시 사회질서와 공공이익에 특별히 심각한 손해를 끼치거나, 국가안전에 심각한 피해를 끼치는 특별히 중요한 네트워크
- 제5급 : 네트워크가 손상되면 국가안전에 특별히 심각한 피해를 끼치는 극도로 중요한 네트워크

2) 네트워크 안전등급 부여 방법 및 절차는 <네트워크안전등급보호조례(의견수렴안)> 및 중국 국가표준인 <정보시스템 안전보호 등급구분 준칙(GB 17859-1999)>에 기술되어 있다. <정보시스템 안전보호 등급구분 준칙>에 기술되어 있는 등급구분 방법은 <네트워크 안전등급>을 구분할 때도 적용되고 있다.

중국의 네트워크 안전등급

침해대상	대상에게 미치는 침해정도		
	일반손해	심각한 손해	특별히 심각한 손해
국민, 법인 및 기타 조직	제1급	제2급	제3급
사회질서 및 공공이익	제2급	제3급	제4급
국가안전	제3급	제4급	제5급

[출처 : 네트워크안전등급보호조례 초안]

〈안전등급〉을 결정하는 절차는 ① 네트워크 운영자는 자체적으로 외부 자문을 받아 사업 기획 및 설계 단계에서 네트워크안전등급을 판단하여 주무 부처(주무 부처의 지방조직 포함)에 제시한다. ② 주무 부처가 판단하여 등급을 승인한다. 승인을 받는 과정에서 등급이 상향 조정되기도 하고, 유사 업무시스템이라 할지라도 주무 부처 또는 지방에 따라 등급이 달라질 수 있다. ③ 2급 이상으로 승인되면 해당 네트워크 운영자는 현급 이상의 공안기관에 신고(备案)를 하여야 한다. ④ 네트워크 기능과 서비스 범위, 서비스 대상 및 처리하는 데이터에 중대한 변화가 발생한 경우 안전등급을 변경해야 한다.

■ 안전등급에 따른 보호의무³⁾

〈안전등급〉 2급~4급에 해당하는 네트워크 운영자는 “네트워크 일반 보안의무”⁴⁾를 이행하여야 한다. 특별히 안전등급이 3급 이상인 경우는 “네트워크 일반 보안의무”를 이행 하는 것 이외에도 ① 네트워크 안전관리조직의 확립, 네트워크가 변경되거나 네트워크 접속 및 유지관리 조직이 변경될 경우 단계별 승인 시스템을 구축, ② 네트워크 안전보호를 위한 총괄 계획과 전략을 수립하고, 기술 전문가의 검토를 거쳐 확정, ③ 네트워크 안전관리를 책임지는 핵심 인력에 대한 신원조사를 실시, ④ 네트워크 설계, 건설, 운송 및 기술 서비스를 제공하는 기관과 인원에 대한 안전 관리, ⑤ 네트워크 운영상태와 네트워크 트래픽, 사용자 행동, 보안사고 등을 모니터링하고 분석하는 네트워크 안전관리 플랫폼을 구축하고, 중요 네트워크 장비와 시스템에 대한 백업 및 복구 조치를 실시 등의 추가 조치를 하여야 한다.

또한, 안전등급이 3급 이상인 경우에는 연 1회 외부전문기관으로부터 네트워크 안전등급 테스트평가를 실시하고 그 결과를 공안기관에 보고하여야 하며, 공안기관은 제3급 이상의 네트워크 운영자에 대해 1년에 최소 1회의 안전검사를 실시한다. 제2급 내지 제4급에 해당하는 네트워크운영자는 서비스 플랫폼의 운영 정비를 반드시 중국에서 실시하는 것을 원칙으로 하며, 상용 암호제품의 조달 및 사용은 국가암호관리국(OSCCA)⁵⁾의 <상용암호제품사용관리규정>에 따른 인증된 제품만 사용할 수 있다. 한편 안전등급 1급의

3) 안전등급에 따른 보호의무는 국가표준 “네트워크 안전등급 보호 기본요구(GB/T 22239-2019)에 기술되어 있다.
4) “네트워크 일반 보안의무”의 주요내용은 네트워크 안전관리제도와 운영매뉴얼 수립과 보안 책임자 지정, 네트워크 침해 방지를 위한 기술조치의 이행, 네트워크 운영상태와 보안사고 모니터링, 데이터 백업과 암호화 조치의 이행 등이다.
5) 국가암호관리국(OSCCA : State Cryptography Administration Office of Security Commercial Code Administration)은 국무원 소속 장관급 행정부처이면서도 중앙공산당 직속의 <중공암호영도소조판공실>과

보호요건은 “네트워크 일반 보안의무”를 참조하여 자발적으로 시행하고, 안전등급 5급에 대한 보호요건은 공개하고 있지 않다.

네트워크운영자가 이러한 절차와 보호기준을 지키지 않을 경우에는 먼저 시정명령을 받게 되고, 시정명령을 이행하지 않거나 네트워크 보안에 피해를 주는 결과가 발생할 경우 1만~10만 위안(170만 원~1700만 원)에 해당하는 벌금을 받게 된다.

〈네트워크 안전등급 제도〉와 〈핵심 정보 인프라 시설〉의 구분

〈네트워크 안전법〉 제31조에서는 “국가는 공공통신과 정보서비스·에너지·교통·수리·금융·공공서비스·전자정부 등 중요 산업과 영역, 그리고 기타의 일단 파괴·기능 상실·데이터 유출이 발생하면 국가 안전·국가경제와 국민 생활·공공이익에 중대한 손상을 줄 수 있는 〈핵심 정보 인프라〉에 대하여, 〈네트워크 안전등급 보호 제도〉에 기초하여, 중점 보호를 실행한다.”라고 규정하고 있다. 여기서 언급하고 있는 〈핵심 정보 인프라 시설〉⁶⁾과 〈네트워크 안전등급 제도〉를 구분할 필요가 있다.

〈핵심 정보 인프라 시설〉은 〈네트워크 안전등급〉을 받은 네트워크 중에서 에너지, 통신, 국방, 은행 등과 같이 〈핵심 정보 인프라 시설 안전 보호 조례(안)〉에서 정하는 특별한 기준에 해당하는 경우에 각 부처 및 성으로부터 한번 더 〈핵심 정보 인프라 시설〉로 지정받게 된다. 지정된 〈핵심정보 인프라시설〉은 〈네트워크 안전등급 제도〉의 등급에 해당하는 보호조치들을 기본적으로 하면서, ① 개인정보와 중요정보를 중국내에 보관해야 하고, 만약에 해외로 제공할 경우 안전성 평가를 진행, ② 네트워크 제품 및 서비스 구매 시 국가보안심사를 받거나 강제성 안전인증(CCIS)받은 제품을 사용 등을 준수하여야 한다. 만약 〈핵심 정보 인프라 시설〉 운영자가 이러한 보호기준을 지키지 않을 경우에는 먼저 시정명령을 받게 되고, 시정명령을 이행하지 않거나 네트워크 보안에 피해를 주는 결과가 발생할 경우 10만~100만 위안(1700만 원 ~1억7천만 원)에 해당하는 보다 강화된 벌금을 받게 된다. 또 특정한 경우에는 영업중지, 홈페이지폐쇄, 영업허가 취소와 같은 보다 강도 높은 제재를 받게 된다.

네트워크 안전등급 보호 제도 관련 표준 현황

■ 중국 정보보호 표준화 추진체계

중국 표준화의 방법과 절차를 정하고 있는 법규는 〈표준화법〉이지만, 정보보호 분야의 표준화를 직접적으로 명시하고 있는 것은 〈네트워크 안전법〉이다. 〈네트워크 안전법〉에서는 “국가는 네트워크 보안 표준체계를 구축하고 보완하여야 한다.(제15조)”, “네트워크 제품, 서비스는 관련 국가표준의 강제성 기준에 부합

동일한 조직이다. 즉, 2개의 조직은 명칭만 다를 뿐 하나의 조직이다.

6) <핵심 정보 인프라 시설> 제도는 한국의 “정보통신기반보호법”에 따른 정보통신기반시설과 유사한 제도로 볼 수 있다.

해야 한다.(제22조)”, “네트워크 핵심장비와 네트워크 보안 전용제품은 국가표준의 강제성 기준에 따라 자격이 있는 기관의 안전인증에 통과 또는 안전시험기준에 부합된 후에야 판매 또는 제공이 가능하다.(제23조)” 등과 같이 국가표준을 준수하도록 하는 규정을 두고 있다.

〈네트워크 안전법〉 규정에 따라 2016년에 〈국가표준화관리위원회(SAC : Standardization Administration of China)⁷⁾와 〈국가인터넷정보판공실⁸⁾은 〈중앙 네트워크 안전 및 정보화 위원회⁹⁾의 승인을 거쳐 〈국가 네트워크 보안 표준화 업무 강화에 관한 의견〉을 발표하였다. 동 의견에서는 네트워크 보안 표준화 추진을 위하여 〈전국정보보호표준화기술위원회(全国信息安全标准化技术委员会, CITS; China Information Security Standardization Technical Committee)¹⁰⁾로 하여금 〈국가표준화관리위원회〉의 지도 아래, 〈국가인터넷정보판공실〉의 총괄 조율과 네트워크 보안 관련 주무부처(공안부, 공업정보화부 등)의 지원을 받아 정보보안 표준을 담당하도록 강조하고 있다. 즉, 네트워크 보안표준을 제정함에 있어 〈전국정보보호표준화기술위원회〉는 〈국가인터넷정보판공실〉과 〈국가표준화관리위원회〉의 지도를 받도록 명문화하고 있는 것이다.

■ 안전등급 제도 시행을 위한 국가표준 제정 현황

2019년 12월 까지 제정된 정보보호 국가표준(GB)¹¹⁾은 242건(폐지 14건 포함)이다. 228건 중 〈네트워크 안전등급 보호 제도〉의 시행을 위하여 제정된 표준은 다음 〈표〉와 같은 7건이다.

중국의 네트워크 안전등급 제도 관련 국가표준 현황

표준번호 (시행일)	주요 내용
GB/T 22239-2019 (2019/12/1)	<p>〈 정보보호기술 - 네트워크 안전등급 보호 기본요구(GB/T 22239-2008 대체) 〉</p> <p>* 네트워크보안 등급보호의 제1급에서 제4급까지 등급보호 대상의 보안 일반 요구와 보안 특별 요구를 규정함. 등급 분류의 비암호 관련 대상의 보안 건설과 감독관리에 적용됨.</p> <p>* 네트워크 보안등급보호 개요 : 등급보호대상, 등급별 보안보호능력, 일반 보안요구사항과 특별 보안요구사항</p> <p>* 1~4급, 등급별 보안요구사항 : 일반 보안요구사항, 클라우드컴퓨팅, 모바일인터넷, 사물인터넷, 산업제어시스템 등 특별 보안요구사항</p>
GB/T 25070-2019	〈 정보보호기술 - 네트워크 안전등급 보호 안전설계 기술요구(GB/T25070-2010 대체) 〉

7) 중국 표준화 업무를 총괄하는 조직이지만 실제 존재하는 조직은 아니다. 장관급 조직인 <국가시장감독관리총국>은 표준화 관련 업무를 수행할 때 대외적으로 <국가시장감독관리총국>이 아닌 <국가표준화관리위원회>라는 명의를 사용한다. 표준화 관련 업무는 <국가시장감독관리총국>의 부국장(차관급)중 1명이 관장한다.

8) <국가인터넷정보판공실>은 국무원 소속의 장관급 행정부처이다. 그러나 중앙공산당에 설치된 <중앙 네트워크 안전 및 정보화 위원회 판공실>과는 이름만 다를 뿐 동일 조직이며, 국무원이 아닌 중앙공산당의 통제를 받는다.

9) 시진핑 국가주석이 위원장이며, 중앙공산당에 설치된 위원회이다. 동 위원회의 “의견”이라는 형식은 중국 정보 보호 및 정보화 분야의 정책 결정 및 집행에 있어 중요한 기준이 된다.

10) <https://www.tc260.org.cn/>

11) GB는 國家(Guójia) 標準(Biāozhǔn)의 중국어 표기법(병음) 앞 글자를 딴 약자이다.

표준번호 (시행일)	주요 내용
(2019/12/1)	<ul style="list-style-type: none"> * 네트워크보안 등급보호 제1급에서 4급까지 등급보호 대상의 보안 설계 기술 요구를 규정함. 운영사용 기관, 네트워크보안 기업, 네트워크서비스 기구 등이 네트워크보안 등급보호 보안기술 방안의 설계와 실시를 진행하도록 지도하는데 적용되고 또한 네트워크 보안 직증 부문이 감독, 검사, 지도를 진행하는 근거가 될 수 있음. * 네트워크보안 등급보호 보안기술 설계 개요 : 일반 등급보호 보안기술설계구조, 클라우드컴퓨팅, 모바일상호연결, 사물인터넷, 산업제어 등 등급보호 보안기술설계구조 * 1급~4급 등급별 시스템 보안보호환경설계 : 설계목표, 설계정책, 설계기술요구
GB/T 28448-2019 (2019/12/1)	<p>〈 정보보호기술 - 네트워크 등급보호 평가요구(GB/T 28448-2012 대체) 〉</p> <ul style="list-style-type: none"> * 서로 다른 급의 등급보호 대상의 보안 테스트평가 일반 요구와 보안 테스트평가 추가 요구를 규정함. 보안 테스트평가 서비스 기구, 등급보호 대상의 운영사용 기관 및 주관 부문이 등급보호 대상의 보안 상황에 대하여 보안 테스트평가를 진행하는데 적용되고 지침을 제공함. 또한 네트워크 보안 직증 부문이 네트워크보안 등급보호 감독검사를 진행할 시에 참고로 적용됨. * 등급 테스트평가 개요 : 등급 테스트평가 방법, 개별 항목 테스트평가와 전체 테스트평가 * 1급~4급: 등급별 보안테스트평가 일반 요구, 클라우드컴퓨팅, 모바일상호연결, 사물인터넷 등 특별 요구
GB/T 28449-2018 (2019/7/1)	<p>〈 정보보호기술 - 네트워크 등급보호 평가절차 가이드 〉</p> <ul style="list-style-type: none"> * 네트워크보안 등급 보호 테스트평가의 업무 과정과 테스트평가 활동 및 그 업무의 임무를 규정함. 테스트평가 기구, 등급분류 대상의 주관 부문 및 운영사용 기관이 네트워크보안 등급보호 테스트평가 업무를 전개하는데 적용됨. * 등급테스트평가 개요 : 등급테스트평가 과정, 위험, 위험회피 * 테스트평가 준비, 편제, 현장, 보고 등 활동
GB/T 36958-2018 (2019/7/1)	<p>〈 정보보호기술 - 네트워크 안전등급 보호 안전관리센터 기술 요구사항 〉</p> <ul style="list-style-type: none"> * 네트워크보안 등급보호 보안관리센터의 기술 요구를 규정함. 보안개발 업체와 운영 기관이 본 표준의 요구에 의거해 보안관리센터를 설계, 건설, 운영하는데 적용됨. * 보안관리센터 개요 : 전체 설명, 기능 설명 * 2급~4급 보안관리센터 기술 요구 : 기능, 인터페이스, 자체 보안 등 요구
GB/T 36959-2018 (2019/7/1)	<p>〈 정보보호기술 - 네트워크 등급보호 평가기구의 능력요구와 평가규범 〉</p> <ul style="list-style-type: none"> * 네트워크보안 등급보호 테스트평가 기구의 능력 요구와 평가 규범을 규정함. 네트워크보안 등급보호 테스트평가 기구가 되거나 또는 더 높은 등급의 테스트평가 기구가 되려고 하는 능력 건설, 운영 관리, 자격 평가결정 등 활동에 적용됨. * 테스트평가기구 능력 요구 : 테스트평가기구 등급분류, 등급평가인원 등급분류, 1급~4급 등급별 테스트평가기구 능력 요구 * 테스트평가기구 능력 평가 : 평가 절차, 최초 평가, 기간 평가, 능력 재평가를 기술함

표준번호 (시행일)	주요 내용
GB/T 36627-2018 (2019/4/1)	<p>〈 정보보호기술 - 네트워크 안전등급 보호 평가기술 가이드 〉</p> <p>* 네트워크 공격의 정의, 속성, 다차원의 묘사 방법을 규정함. 네트워크 운영자가 네트워크 건설, 운영유지, 관리 시 보안에 대한 설계와 평가를 진행하는데 적용됨.</p> <p>* 개요 : 등급 분류, 등급 선택</p> <p>* 등급 테스트평가 요구 : 검사 기술, 식별 및 분석 기술, 취약점 검증 기술</p>

[출처 : 중국 국가표준공개시스템, <http://openstd.samr.gov.cn/>]






[참고문헌]

1. 중국 공안부, 네트워크안전등급보호조례 초안 발표, 한국인터넷진흥원, 인터넷 법제동향 제130호, 2018년 7월
2. ICT 표준화 추진체계 분석서, 한국정보통신기술협회, 2010년
3. 정보통신표준화 추진체계 분석서 : 국가 및 주요표준화기구, 한국정보통신기술협회, 2005년
4. 중화인민공화국 표준화법
5. 중화인민공화국 네트워크 안전법
6. 중국 국가표준화관리위원회 홈페이지, <http://www.sac.gov.cn/>
7. 중국 국가표준공개시스템 홈페이지, <http://openstd.samr.gov.cn/>
8. 중국 전국정보보호표준화기술위원회, <https://www.tc260.org.cn/>

< KISA 주요 활동 안내 >

민간 500대 웹사이트 플러그인 개선 실적 및 웹 표준 전환 지원사업 안내

□ 플러그인이란?

- (정의) 보안, 결제, PC제어 등 웹 브라우저*에서 지원하지 않는 기능을 사용하기 위해 PC에 설치하는 별도 프로그램(액티브X, 실행파일 등)
 - * 이용자가 PC, 스마트폰 등에서 웹사이트를 볼 수 있게 해주는 응용프로그램으로  인터넷 익스플로러(IE),  크롬,  파이어폭스,  사파리,  오페라 등 종류 다양
- (용도) 인터넷에서 **이용자 편의 서비스**(결제, 금융이체 등)나 **보안 서비스**(공인인증서, 보안3종(키보드보안, 백신, 방화벽)) 등을 제공

□ 플러그인 개선 필요성

- ① (국민 불편) 웹사이트 접속 시 플러그인을 설치해야 하고, 이 과정에서 여러번 웹 브라우저가 재시작 되면서 국민 불편 초래
- ② (보안성) 다양한 웹사이트의 플러그인 강제 설치에 따라 생긴 이용자의 무의식적인 설치 습관으로 인해 악성코드 유포 등의 경로로 활용
- ③ (플랫폼 종속) 실행파일은 다양한 웹브라우저(크롬, 사파리 등)에서 동작하는 반면, 액티브X는 MS社 웹브라우저인 인터넷익스플로러(IE)에서만 동작

□ 민간 500대 웹사이트(국민 83% 이용) 플러그인 개선 실적

- (플러그인 수) '17년 대비 **액티브X 82.3% 감소, 실행파일 81.8% 감소**

구 분	'17년	'18년	'19년
액티브X 개수	810개	510개 (△37.0%)	143개 (△82.3%)
실행파일 개수	1,456개	290개 (△80.1%)	265개 (△81.8%)
합 계	2,266개	800개 (△64.7%)	408개 (△82.0%)

< 플러그인 개선 방향 >

- ◆ (액티브X) 웹 표준 등 솔루션으로 대체하여 제거 ⇒ '19년말까지 82.3% 제거
- ◆ (실행파일) ▲웹 표준 솔루션으로 대체 가능한 것은 제거, ▲불가능한 것*은 웹서비스 프로세스 개선(설치없는 간편결제, 앱카드 등)을 통해 설치 최소화

* 실행파일 265개 중 98%(보안 프로그램 등 총 260개, 이 중 200개가 금융 관련) 차지('19년)

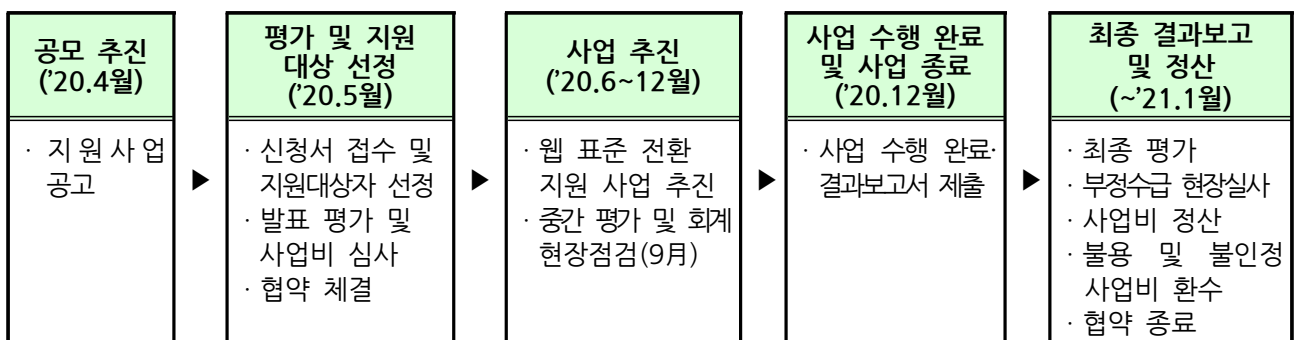
□ 웹 표준 전환 지원사업 안내

**2020년 민간 500대 웹사이트 액티브X 개선 관련
정부 지원사업이 종료될 예정입니다!!**

○ (사업분야) 민간 500대 웹사이트* 액티브X 개선 지원사업

* 민간 500대 웹사이트 목록은 HTML5 기술지원센터(koreahtml5.kr)에서 확인 가능

○ (사업기간) 약 6개월('20. 6월~12월 예정)



※ 상기 일정은 사정상 변동 될 수 있음

○ (사업예산) 총 1,000백만원(정부지원금 상한액* 존재)

* 기업당 정부지원금 상한액이 존재하며, 상세내용은 한국인터넷진흥원 홈페이지(www.kisa.or.kr)의 사업 공고문('20.4월 공고 예정) 참조

○ (사업목적) 민간 500대 웹사이트에서 사용 중인 액티브X의 웹 표준(불가피할 경우 실행파일) 전환을 통해 국민들의 웹사이트 이용 편의 제고

○ (참여대상) 민간 500대 웹사이트 운영기업 또는 국내 민간 500대 웹 사이트가 보유한 액티브X 개선(웹 표준 또는 실행파일)이 가능한 기업

○ (지원방식 및 기준) 한국인터넷진흥원 및 참여기업 매칭방식으로 진행

전체사업비 중 자체부담금 기준	자체부담금 중 현금부담 기준
<ul style="list-style-type: none"> ■ (대기업) 최소 50% 이상 ■ (중견) 최소 40% 이상 ■ (중소) 최소 25% 이상 <p>※ 비영리기관 및 연구개발서비스사업자 자체부담금 없음</p>	<ul style="list-style-type: none"> ■ (대기업) 최소 40% 이상 ■ (중견) 최소 26% 이상 ■ (중소) 최소 20% 이상 <p>※ 비영리기관 및 연구개발서비스사업자 해당사항 없음</p>

○ (문의처) 한국인터넷진흥원 인터넷기반조성팀 html5@kisa.or.kr

개인정보보호 국제협력센터 안내

개인정보보호 국제협력센터는 “해외 침해사고 발생 시 내국민 피해구제 및 해외 진출 기업에 글로벌 개인정보 규제 정보 제공”을 위하여 개소(‘17.10, www.privacy.go.kr/pic)

□ 제공 서비스

- **(해외 국가 정보)** 9개국(미국, 일본, 중국, 영국, 독일, 호주, 캐나다, 싱가포르, 베트남) 개인정보 보호 법률, 행정, 피해구제, 사건 사례, 동향 정보 제공
- **(해외 민원 제기 절차)** 12개국(그리스, 뉴질랜드, 미국, 싱가포르, 아일랜드, 영국, 일본, 중국, 캐나다, 프랑스, 호주, 홍콩) 개인정보 감독 기구에 개인정보보호 유출 등 관련 민원을 신청할 수 있도록 step-by-step 가이드 제공
- **(해외 법제 자료)** 유럽(EU GDPR, 영국, 독일, 체코), 아시아(중국, 일본, 싱가포르, 베트남), 북미(미국, 캐나다) 권역별로 개인정보보호 관련 법령, 가이드라인 등을 원문과 한글 번역 자료 제공



□ 향후 계획

- **(이벤트)** '20년 상반기 중 “해외 개인정보보호 무엇이든 물어보세요!” 이벤트를 개최하여 해외 개인정보보호 이슈 분석, 관련 법률 번역 신청을 받고, 추첨을 통해 기프티콘 증정 예정
※ KISA SNS 채널(Facebook, Twitter, Blog, 카톡 채널)을 이용하여 이벤트 안내

개인정보보호 국제협력센터는 이용자들의 의견을 항상 경청하고 있습니다.
홈페이지 개선 의견은 이메일(iprivacy@kisa.or.kr)로 보내주세요.

2020 Vol.1

이슈&트렌드

CES 2020 - 인공지능과 로봇의 만남: 더 많은 시간이 필요
CES 2020 행사에서 가장 핫(hot)했던 제품
CES 2020 서비스화 되는 모빌리티
CES 2020 뷰티테크(Beauty Tech) 화두는 인공지능과 개인화
CES 2020에서 PC의 변화
CES 2020에서 살펴보는 슬립테크 동향
온라인 데이터에서 나타난 “CES 2020” 관심도와 그 내용들
CES 2020 스케치: 모든 것에 테크를 붙인 CES의 뒷담화
미국의 의료분야 데이터사이언스 및 인공지능 정책 동향
개인정보 유출 통지·신고 제도의 개선 검토

2020 Vol.2

이슈&트렌드

인공지능과 데이터 분석으로 질병 확산을 예측할 수 있는가?
코로나 바이러스와 개인정보 활용에 대한 소고
데이터와 헬스케어의 진화
EU의 5G 네트워크의 위험 완화를 위한 조치 방안
데이터 3법 개정의 주요 내용과 전망
국내외 중소기업 정보보호 지원 정책 분석 및 개선 검토
일본 IoT 보안정책 동향 분석 및 시사점





발 행 일	2020년 3월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 ICT미래연구소
편 집	(주) 해리