

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.

미래인터넷 기술 성공의 핵심 포인트, 보안

김대엽 (daeyoub69@suwon.ac.kr)

수원대학교 정보통신학부 교수

인터넷의 한계

1970년대부터 개발된 인터넷은 다양한 온라인 서비스의 기반 기술로 폭넓게 활용되면서 기술적 측면과 아울러 산업적 측면에서도 그 중요성이 지속해서 증가해 왔다. TCP/IP 기술연구와 함께 초기 인터넷 기술의 주요 목표는 원거리에 있는 기기 사이에 안전한 네트워크 채널을 생성하고 관리하는 것이었다. 그러나 유/무선을 이용하는 다양한 기기의 급속한 보급과 콘텐츠 서비스의 폭발적인 증가와 같은 현상을 초기 인터넷 개발자들은 고려하지 못했다. 이와 같은 인터넷 사용 증가는 네트워크 병목과 기기의 빈번한 이동으로 인한 서비스 지연을 일으키고 있으며, 이를 해결하기 위하여 물리적으로 네트워크 설비를 확충하려는 노력이 계속되고 있지만, 비용 문제와 함께 이와 같은 설비 확충이 늘어나는 네트워크 수요 요구를 충족시키기 힘들 것이라는 것이 일반적인 예상이다¹⁾²⁾. 또한, 취약한 보안 구조로 인하여 서비스 거부 공격과 같은 다양한 해킹 공격의 대상이 되고 있다.

네트워킹 패러다임의 변화

인터넷을 활용하는 기기와 콘텐츠의 폭발적인 증가 추세는 앞으로도 지속할 것으로 예상하며, 이로 인한 문제들을 근본적으로 해결하려는 움직임이 2010년 이후로 계속되고 있다. 이와 같은 해결 방안으로 제안된 기술 중 하나가 정보중심 네트워킹 아키텍처(Information Centric Networking Architecture, ICN) 기술이다.

주요 ICN 기술은 사용자가 요구하는 콘텐츠를 빠르고 효율적으로 사용자에게 제공하는 것을 목표로 한다. 앞서 언급한 것처럼 기존 인터넷 기술의 주요 목적이 기기 사이의 안전한 네트워크 채널을 구축하는 것이었다면, 주요 ICN 기술은 기기가 아닌 사용자가 요청한 콘텐츠와 사용자를 연결하는 것을 주목적으로

1) <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html>

2) <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1955935>

한다. 그러므로 기존 인터넷 기술이 기기의 식별자와 위치에 기반을 둔 네트워킹 기술이라고 한다면, 주요 ICN 기술은 콘텐츠의 식별자와 위치에 기반을 둔 네트워킹 기술이라 할 수 있다.

이러한 목적을 실제 구현하기 위하여 주요 ICN 기술들은 콘텐츠의 생성자(Original Creator/Publisher/Provider)가 제공하는 콘텐츠 외에 네트워크에 산재되어 있는 콘텐츠의 복사본(Cache)을 활용하는 방안을 모색한다. 콘텐츠 캐시는 다른 사용자의 요청 때문에 이전에 배포된 콘텐츠일 수도 있고, 네트워크 사업자 또는 콘텐츠 서비스 사업자가 운영하는 콘텐츠 서버에 저장된 콘텐츠일 수도 있다. 콘텐츠 캐시를 활용한 네트워킹 기술은 기존 P2P 네트워킹 기술이나 CDN 기술에서도 이미 활용되고 있는 방법이다. 그러나 ICN 기술은 콘텐츠 캐시 활용 기술을 일반적인 네트워크 플랫폼을 통하여 제공한다는 점에서 기존 P2P/CDN과 차별화된다고 할 수 있다. 표1은 주요 ICN 기술들의 특징을 요약하여 설명 한다³⁾.

ICN 기술 특성

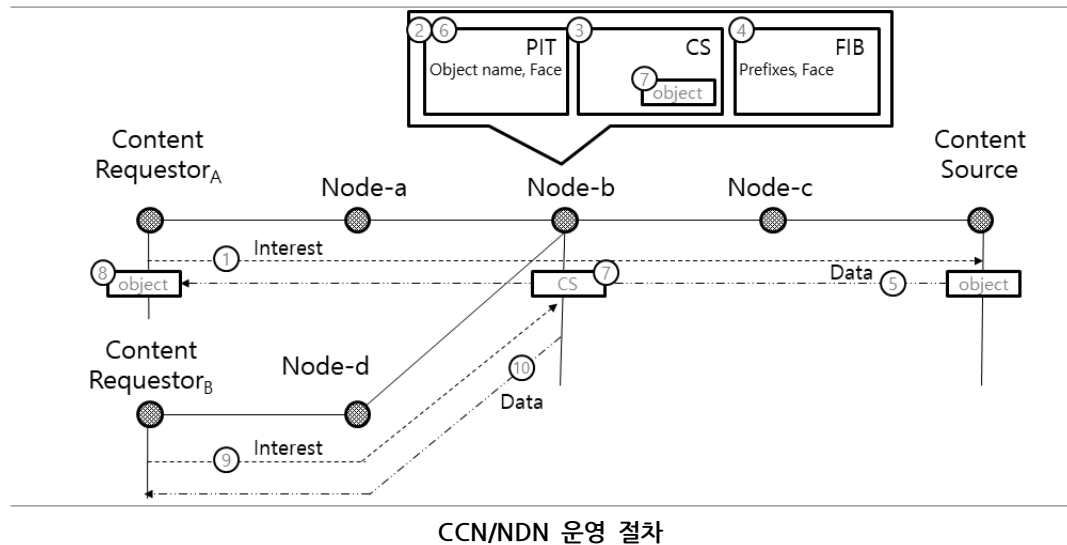
| | DONA | CCN/NDN | PSIRP | NetInf |
|-------------------------|----------------------|----------------------|-----------------------------------|------------------------|
| Namespace | Flat | Hierarchical | Flat | Flat |
| Integrity | Signature | Signature | Signature | Signature |
| Routing Content Request | Name-based | Name-based | Name Resolution System | Name Resolution System |
| Routing Content | Reverse request path | Reverse request path | Source routing using Bloom filter | Reverse request path |

콘텐츠 중심 네트워킹

ICN 기술들은 콘텐츠 캐시를 활용하는 방법에 따라 크게 두 가지 종류로 구분해서 생각할 수 있다. 첫 번째 종류는 콘텐츠 서버를 운영하고, 사용자가 콘텐츠를 요청하는 메시지를 생성하면, 해당 사용자에게 가장 빠르고 효율적으로 콘텐츠를 제공할 수 있는 콘텐츠 서버를 식별하여 사용자에게 이를 알려줌으로써 사용자가 콘텐츠 서버로부터 콘텐츠를 수신할 수 있도록 하는 기술이다. 이와 같은 ICN 기술은 Name Resolution System (NRS) 운영이 필요하다. 두 번째 종류는 네트워크 노드들에 콘텐츠를 임시 저장할 수 있는 기능을 구현한 후, 콘텐츠가 사용자에게 전송될 때 콘텐츠 전송에 이용된 네트워크 노드가 해당 콘텐츠를 임시 저장한 후, 이처럼 저장된 콘텐츠 캐시를 다른 사용자가 요청할 때, 네트워크 노드가 콘텐츠 캐시를 이용하여 직접 응답하는 기술이다. 후자와 같은 ICN 기술을 콘텐츠 중심 네트워킹(Content-centric Networking, CCN) 또는 콘텐츠 이름에 기반을 둔 네트워킹(Named Data Networking, NDN)이라 한다⁴⁾. 그림1은 CCN/NDN의 운영 절차를 설명한다.

3) https://www.os3.nl/_media/2018-2019/courses/an/an2019-icns.pdf

4) <https://dl.acm.org/doi/10.1145/1658939.1658941?CFTOKEN=33230744&CFID=515870947>



CCN/NDN은 사용자가 생성한 콘텐츠 요청 메시지와 응답 메시지를 각각 Interest와 Data라고 표기한다. 사용자 A가 생성한 Interest가 네트워크 a, b, c를 통해서 콘텐츠 원제작자에게 전송되면, Interest가 전송된 네트워크 경로의 역순으로 Data가 전송된다. 이 때, 네트워크 노드 c, b, a는 차례로 Data를 임시 저장한다. 이후, 사용자 B가 같은 콘텐츠를 요청하기 위해 Interest를 생성/전송하면, Interest가 전송되는 경로 상의 네트워크 노드 b가 캐시를 활용하여 사용자 B에게 직접 응답할 수 있다. 이와 같은 네트워크 캐시를 활용하여 Interest/Data를 효과적으로 처리하기 위하여 CCN/NDN은 기존 인터넷에서 사용하는 IP 주소와 같은 호스트 식별 정보 대신에, 계층적으로 구성된 콘텐츠 이름을 패킷 주소로 활용하고 이를 기반으로 Interest를 라우팅 한다.

보안 패러다임의 변화

호스트 중심의 전통적인 인터넷은 호스트 식별/인증과 호스트 간 통신채널 보안을 근간으로 보안 프레임워크를 구축하고 있다. 호스트 중심의 보안 프레임워크는 특정 호스트와의 네트워크 채널 생성 및 관리가 주요 목적인 전통적인 인터넷에 매우 적합한 방법이었다. 그러나 주요 ICN 기술들은 사용자에게 콘텐츠를 제공할 수 있는 호스트가 네트워크에 다수가 존재하고, 가변적일 수 있으므로 기존의 호스트 중심의 보안 체계를 그대로 적용할 수 없다. 특히 CCN/NDN의 경우, 콘텐츠를 제공하는 네트워크 노드를 사용자가 식별할 수 없으므로, 사용자와 콘텐츠 제공자 사이에 기존의 식별/인증/접근통제와 같은 보안 기술을 적용하는 것이 매우 어렵다.

그러므로 ICN 기술에 맞는 새로운 보안 체계를 구성하는 것이 매우 중요하다. 표 2는 ICN 기술에 적용 가능한 다양한 공격들을 요약하고 있다⁵⁾.

5) <https://ieeexplore.ieee.org/abstract/document/7009958>

ICN ATTACKS VS. SECURITY REQUIREMENTS (H: HIGH; M: MEDIUM; L: LOW; BLANK: NO IMPACT)

| Attack | Confidentiality | Integrity | Availability | Privacy |
|------------------------|-----------------|-----------|--------------|---------|
| Watchlist | L | | L | H |
| Sniffing | L | | L | H |
| Source | | | L | |
| Flooding | | | M | |
| Timing | | | M | |
| Jamming | | | L | |
| Hijacking | L | | L | |
| Interception | L | | | M |
| Time Analysis | | | | M |
| Packet Mistreatment | | H | M | |
| Breaching signer's Key | H | H | | H |
| Unauthorized Access | M | M | | |

이와 같은 공격들은 콘텐츠 식별자 및 캐시 이용과 같은 ICN이 가진 몇 가지 주요 특징에 기인한 것들이다. 그러므로 이러한 특징들을 더 안전하고 효율적으로 구현하기 위하여 다음과 같은 요구사항들에 대한 필수적인 고려가 필요하다.

- 콘텐츠 식별 정보 인증 기술: 콘텐츠 캐시를 효율적으로 이용하기 위하여 주요 ICN 기술들은 콘텐츠 식별 정보를 패킷 헤더에 삽입하여 패킷 라우팅에 활용한다. 콘텐츠 식별 정보를 위/변조할 경우 악성 콘텐츠를 유포하는 방법으로 악용될 수 있다. 그러므로 콘텐츠 식별 정보와 콘텐츠를 페어링 하는 기술이 고려되어야 한다.

- 콘텐츠 인증 기술: 사용자에게 콘텐츠를 제공하는 호스트/노드가 네트워크에 다수가 존재하며, 사용자는 실제 자신에게 콘텐츠를 제공한 호스트/노드를 식별할 수 없는 경우도 많으므로 이와 같은 특징을 악용하여 콘텐츠를 위/변조하려는 다양한 공격이 가능하다. 그러므로 사용자가 콘텐츠를 수신한 후, 해당 콘텐츠의 위/변조 여부를 포함한 무결성 확인이 가능해야 한다. 일부 ICN 기술은 전자서명 기술을 활용하여 콘텐츠 생성자가 해당 콘텐츠에 자신의 전자 서명을 첨부하는 것을 추천하고 있다. 그러나 ICN 기술이 서비스/애플리케이션 계층의 기술이 아닌 네트워크 계층의 일반화된 플랫폼을 제공하는 기술임을 고려할 때 전자서명 기반의 콘텐츠 인증을 적용하기 위해서는 글로벌한 PKI 시스템 구축과 같은 추가적인 문제를 양산할 수 있다.

- 안전한 패킷 라우팅 기술: 콘텐츠 식별자 정보를 기반으로 패킷을 라우팅하기 위하여 ICN 기술은 NRS 시스템 운영이 필요하거나 네트워크 노드의 FIB 테이블 운영이 필요하다. 그러나 네트워크를 통해 배포되는 콘텐츠의 양을 고려할 때, 기존 호스트의 IP 주소를 기반으로 운영하는 DNS나 FIB 테이블과 비교하면 이와 같은 시스템은 매우 많은 양의 정보를 관리해야 한다. 이 경우, 서비스 지연의 주요 요인이 될 수 있으며, 기존 인터넷에서와같이 서비스 거부 공격의 주요 공격 목표가 될 수도 있다. 또한, CCN/NDN의 경우, Data 전송을 위해 각각의 네트워크 노드가 관리하고 참조하는 PIT 정보를 대상으로

플러딩 공격이 가능하며, 이 경우 Data는 사용자에게 전송되지 않고 폐기된다. 그러므로 공격에 사용되는 Interest를 식별하고 처리하기 위한 Interest 인증과 같은 별도의 패킷 인증 기술도 고려되어야 한다.

● 캐시 관리 정책: 네트워크를 통해 배포되는 콘텐츠의 양은 앞으로도 지속해서 증가할 것이다. 그러므로 콘텐츠 캐시를 관리하는 시스템과 네트워크 노드의 저장 공간에 대한 플러딩 공격이 가능하다. 또한 캐시의 저장 위치는 네트워크 성능에 직접적인 영향을 줄 수 있으므로 효율적으로 캐시를 관리하는 기술이 고려되어야 한다.






● 프라이버시: 일부 ICN 기술은 가독성이 있는 콘텐츠 식별 정보를 사용한다. 이 경우, 콘텐츠 생성자의 정보가 그대로 유출될 수 있으며, 사용자 주변 네트워크를 모니터링 함으로써 사용자의 콘텐츠 이용에 대한 정보도 수집/분석할 수 있다. 그러므로 콘텐츠 식별자에 대한 블라인딩 기술이 요구된다. 또한 콘텐츠 캐시를 이용하기 때문에 콘텐츠 생성자가 콘텐츠 배포를 제어할 수 없다. 이 경우, 생성자가 실제로 배포한 콘텐츠를 회수하거나 삭제할 수 없으므로 심각한 프라이버시 침해의 요인이 될 수 있다. 그러므로 콘텐츠 캐시에 대한 추가적인 접근통제 기술이 고려되어야 한다.

현재 미래 인터넷 기술은 안전성과 효율성 함께 고려하여 연구가 진행되고 있다. 미래 인터넷 기술이 실제 적용되기 위해서는 기존 인터넷을 기반으로 구축된 시스템과 서비스를 전반적으로 교체해야하기 때문에 가까운 시일 내에 적용될 수는 없을 것으로 예상하나, 대형 네트워크 장비 업체에서도 이미 캐시 관리 기능을 네트워크 장비에 구현하는 것을 고려하고 있으며, MEC 기술에서도 캐시를 활용하는 방안이 계속 논의되고 있으므로 점진적으로 네트워크 패러다임은 ICN이 추구하는 방향으로 변해갈 것이다. 그러나 이와 같은 연구 개발이 유럽과 미국을 중심으로 진행되고 있어 한국을 포함한 아시아 국가들의 연구는 매우 미진한 상태라 할 수 있다. 그러므로 미래 인터넷을 선도하기 위해서는 기술 격차를 줄이기 위한 정책 수립이 요구된다.

< 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)

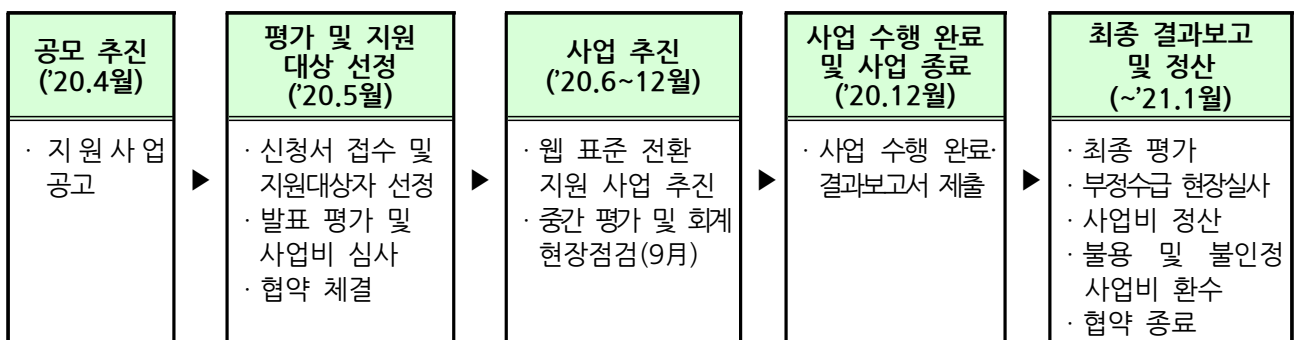
□ 웹 표준 전환 지원사업 안내

**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 |