KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2021 KISA REPORT

volume 12

www.kisa.or.kr

CONTENTS

ISSUE I. 디지털

01 **차기 정부의 IT 정책에 바라는 것**
[한상기/ 테크프론티어 대표]

02 **빅테크 기업 규제의 방향성**
[최호섭/ IT칼럼니스트]

03 **무한경쟁 OTT 시장 라운드1 전망**
[최홍규/ EBS 연구위원]

ISSUE II. 정보보호

04 **소프트웨어 보안 관점에서 본 미국 사이버보안 행정명령과 우리의 대응방안**
[이태준/ 고려대학교 컴퓨터보안연구실 연구원]

05 **정보시스템의 상시 모니터링을 위한 SCAP과 도구에 대한 소개**
[안효범/ 공주대학교 인공지능학부 교수]

ISSUE III. 개인정보보호

06 **개인정보 정책에서 증거기반(evidence-based)의 규제의 필요성**
[이진규/ 네이버주식회사 이사]

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.

차기 정부의 IT 정책에 바라는 것

한상기 (stevehan@techfrontier.kr)

테크프론티어 대표

대선이 가까워지면서 차기 정부의 정책에 대해 많은 의견들이 나온다. 정책도 공약의 모습으로 나오고 있고, 정부 산하 연구 기관에서도 여러 보고서를 만들고 전문가 의견을 수렴하는 중이다.

다음 정부가 추진할 정책 하나 하나에 어떤 의견을 얘기하는 것보다, 그동안 여러 정책 입안이나 추진 과정에 참여했던 사람으로 앞으로 지켰으면 하는 몇 가지 기본 원칙을 말하고자 한다.

첫째, 도전적인 과제를 몇 년 먼저 앞서서 기획했으면 한다. 최근 차세대 인공지능 기술 확보를 위해 2022년부터 총사업비 3018억원을 투입한다는 발표가 있었다. 이 과제의 기획과 예타 통과를 하느라 몇 년이 걸렸다. 세부적인 내용을 보면서 안타까운 점은 모두 좋은 도전이고 연구 가치가 많은 분야인데 왜 이것을 몇 년 전에 시작하지 못했을까 하는 점이다. 우리가 인공지능 국가 전략을 발표한 것이 2019년 12월이다. 2022년부터 향후 5년동안(왜 5년인지는 다 아실 것이라 생각한다) 하겠다는 또 하나는 신뢰할 수 있는 인공지능이다. 모두 다 5년 전에는 시작 했어야 하는 연구 과제들이라고 생각한다.

좀 더 과감히 도전 목표를 세우고 빠른 기획과 도전이 이루어지지 않으면, 예산 확보 시간을 감안하면 이미 많은 연구가 진행되거나 연구 흐름이 바뀐 상황에서 과거의 연구 주제나 방식을 유지하게 된다.

세밀한 과제 계획을 세우는 것 보다는 도전적 목표를 세우고 다양한 연구 접근 방식, 좀 더 획기적인 시도를 할 수 있게 하는 것이 이제 필요한 시점이라고 생각한다. 예를 들어 미국 DARPA는 하나의 주제에 대해 각자의 연구 방식을 제안하고 적절한 연구 제안을 모두 승인해서 여러 가지 방식의 연구가 다 이루어지게 한다. 대표적인 것인 설명가능 인공지능 (XAI)에 대한 연구 지원이다.

둘째, 새로운 정책을 발표할 때는 과거에 진행한 연관 정책의 상호 연결 관계를 보여주고, 이 정책이 어떤 배경과 과거 결과를 바탕으로 나왔는지 알려줘야 한다.

유럽이나 미국의 국가 정책을 보면, 새로 발표하는 정책의 배경과 주요 내용 요약이 명확하게 앞에 나오는 것과 함께, 이 정책 이전에 같은 주제의 정책과 관계, 다른 정책과 이 정책과의 연관성 등이 나온다.

모든 자료는 관련 링크가 있거나, 정책 소개 문서에 하이퍼링크로 연결되어 이 정책이 어떤 정책을 계승하거나 관련 법이 무엇인지, 연관 정책과는 얼마나 다르거나 서로 다른 역할이 있는지를 알게 한다.

특히 문제가 심각한 것은 우리 정책 발표에는 그냥 이번 정책만 나온다. 마치 하늘에서 새로운 정책이 뚝 떨어져 나온 것 같다. 과거 정책의 결과를 어떻게 계승하는 것인지 또는 부족했던 점을 어떻게 보완하고자 하는지에 대해 하나도 알 수가 없다. 그 자리에 오래 있었던 사람만이 알지만, 순환 보직으로 그 내용을 숙지하는 공무원도 별로 없다.

모든 정책 문서에는 정책이 발전해 온 이력을 남겨야 하고, 모든 정책 내용은 HTML로 웹에 제공해야 한다. 유럽 연합, 미국, 캐나다 등은 다 그렇게 되어 있는데 우리는 HWP 파일이나 PDF 파일의 형태도 되어 있어 내용에 대한 검색도 안 된다. 그나마 주요 정책이 올라온 게시판에는 올해 발표한 정책도 몇 개 없다. 나머지는 보도자료로 찾아야 한다.

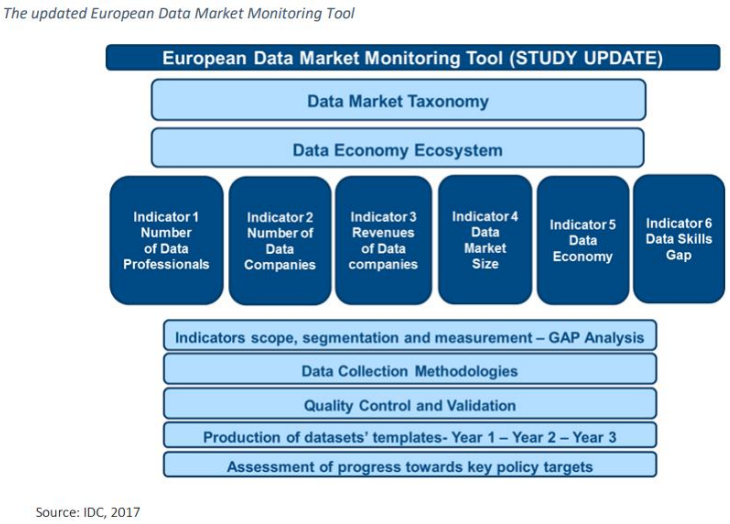
예를 들어 유럽 연합의 인공지능에 대한 접근 방식이라는 웹 페이지에 접속하면 이전에 공개한 문서에 대한 링크, 관련 문서로 안내하는 링크, 집행위가 제공하는 내용, 지금까지 이 결과가 나오게 된 과정이 날짜 별로 보이며 관련 문서와 웹 페이지 링크가 모두 공개되어 있다. 그것이 월드와이드 웹이며 인터넷의 의미인데, 우리는 대부분 아직도 PC 통신 시대의 게시판 구조나 문서 저장소로 이용할 뿐이다.

셋째, 정책 추진 성과를 올바르게 평가하기 위한 도구 개발을 처음부터 해야 한다. 2019년 1월 데이터와 인공지능 경제 활성화 정책 발표했을 때 우리의 목표가 데이터 시장 규모 30조원에 AI 유니콘 기업 10개 육성이었다. 2019년 12월 인공지능 국가 전략에서는 2030년 지능화 경제 효과 455조원, 빅데이터 45,000종 개발이다. 인재 양성도 매년 각 분야마다 몇 십 만명을 내세운다.

2016년 3월에 당시 미래창조과학부가 발표한 지능정보산업발전전략에서 내세웠던 투자 금액이나 각종 프로젝트, 계획이 도대체 어떻게 추진되고 결과가 나왔으며, 이후 정부에서 인공지능 전략에 반영된

내용이나 변경된 사항이 무엇인지 왜 아무도 평가와 분석을 하지 않는 것일까? 왜 정부 부처의 정책은 리뷰와 평가 분석 대상이 아닌 것일까?

어떤 정부 정책의 성과를 어떤 기준과 방식으로 측정할 것인지, 매년 목표 달성은 얼마나 했고, 미흡한 부분이 무엇인지를 알려면 정책 성과를 모니터링할 수 있는 도구가 있어야 한다. 아래 그림은 유럽이 데이터 경제 정책을 추진하면서 동시에 그 성과를 어떻게 측정할 것인지에 대한 연구 분야이다.



[그림 1] 유럽의 데이터 시장 모니터링 도구 [출처: IDC]

넷째, 모든 정책 문서는 완전한 문장의 형식으로 작성하자. 더 이상 요약형의 개조식 문장을 공식 문서에서 사용하지 말자. 개조식 문장은 비문인 경우도 많고, 정확한 표현이 무엇인지 알기 어려울 때도 있으며, 원본이 있고 요약하는 것이 아니라 처음부터 개조식으로 작성한 문서는 그 정책의 철학과 내용을 제대로 이해하기 어렵게 만든다.

소준섭 전 국회도서관 조사관이 한겨레 신문에 기고한 글에서 '개조식 문장은 그 자체로 완성되지 못한 문장으로서 비문이다. 그러므로 당연히 문장간 논리적 연관성을 확인하기 어렵고 주어가 생략되면서 공직사회의 폐단인 책임회피의 방편으로 이용될 소지가 적지않다'고 비판했다.[1] 게다가 이 역시 일본의 잔재라고 보는 사람이 많다.

선진국의 정책 문서는 모두 완전한 문장으로 기술되어 있으며, 맨 앞에 정책의 배경과 의미를 요약한 개요(Executive Summary)를 포함시켜 이 정책에 대해 빠르게 이해할 수 있도록 돕고 있다. 우리는 그런 부분조차 글머리 기호를 포함한 개조식 문장을 사용함으로써 다중의 해석을 용인하고 있다. 도대체 왜 이렇게 하자는 것인지 알 수가 없다. 정 안된다면 정책안의 맨 앞의 한 페이지는 완전한 문장으로 정책의 의미와 추진 배경을 제대로 설명하기 바란다.

1) 한겨레, "[왜냐면] 일제식 종결 문장투 '~함' 이젠 고치자," 2021년 9월 8일

다섯째, IT 기술이 갖는 사회적 영향과 우리가 준비해야 하는 규범과 제도에 대해 전문적으로 지속적 연구를 하자. 소셜미디어, 사물 인터넷, 빅데이터, 인공지능 모두 사회와 개인에게 미치는 영향이 지대한 분야지만, 관련 연구를 지원하고 정책을 얘기하면서 그로 인한 사회적 임팩트나 함의에 대한 연구는 간헐적으로 여기 저기에서 산발적으로 연구가 나올 뿐이다.

전문성을 가진 집단이나 연구소를 통해서 지속적으로 연구를 추진하고 영향력 분석을 해야 한다. 그때그때마다 과제를 발주하고 여기 저기의 연구 그룹에게 과제를 주는 방식으로는 의미 있는 정책 연구 결과를 얻기 힘들다.

필자가 기고한 다른 글에서 '인공지능 사회 연구소의 필요성'을 제안한 것이 그런 이유 때문이다.[2] 미국이나 영국은 이미 기존에 기술과 사회 문제나 인류의 미래에 대한 연구소들이 있고 새로운 기술에 의한 영향력 분석이나 사회적 이슈를 연구하는 그룹이 생기면 바로 연구소를 수립하고 여러 기관과 공동 연구를 추진한다.

전문 그룹은 네트워크형으로 연결되고 펠로우 제도를 이용해 다른 곳에서 근무하는 전문가나 학자를 연구에 투입해서 몇 년 동안 지속적인 연구를 진행하고 이에 대한 공론장을 만들어 낸다. 물론 민간 재단에서도 자금 지원하는 경우도 많다. 이제 크게 성장한 국내 IT 기업들이 이런 연구 재단이나 연구소 설립에 적극 참여하고 공동 연구를 지원할 때가 되었다고 생각한다. 이를 차기 정부에서 정책적으로 유도하고 지원해서 좀 더 전문 연구 그룹이 만들어지게 해야 한다.

마지막으로 정책에는 유행적인 마케팅 용어 사용을 멈췄으면 한다. 메타버스를 예로 들면, 메타버스의 정의나 개념이 아직도 진화 중이고 메타버스는 단지 결과물을 의미하는 용어일 수 있다. 정부가 정책에 이런 단어를 사용하는 것은 정말로 최소화해야 한다. 그 대신에 공간 인터넷이나 공간 컴퓨팅이라는 보다 본질적인 단어를 사용하는 것이 오히려 더 기본적인 연구를 추진한다는 의미를 줄 수 있다.

민간에서 마케팅 용어로 사용하거나 아직 개념이 불투명한 용어는 기업이 의도적으로 사용할 수 있어도 정부의 정책에서는 최소화해야 한다. 정부 연구 정책은 마케팅용으로 하는 것이 아니기 때문이다.

이제는 선진국답게 기술 개발 정책과 관련 사회적 이슈 분석 연구 방법에 대한 기본 원칙을 다시 한번 정립했으면 한다. 인터넷 강국이라고 하면서 인터넷의 기본 원칙을 지키지 않고 있고, 문서는 숨어 있어서 검색도 되지 않으며, 성과에 대한 양적/질적 평가를 위한 체계가 없었다고 생각한다. 이제는 유럽연합이나 미국, 영국이 하는 방식을 따라가는 것이 필요하며, 다음 정부가 제일 먼저 해야 할 일이라고 생각한다.

2) 한상기, "인공지능 사회 연구소의 필요성," ICT Insight, 한국방송통신전파진흥원, 2021년 7월

빅테크 기업 규제의 방향성

최호섭 (work.hs.choi@gmail.com)

IT컬럼니스트

빅테크 규제는 어디로 가고 있나. 기업도, 소비자도 웃을 수 있어야

지난 한 해 논란이 됐던 ICT 관련 이슈를 꼽자면 '구글 갑질 방지법', '넷플릭스 무임승차 방지법', 'n번방 방지법' 등의 이름으로 대표되는 규제들이 떠오른다. 각자 이유나 목적은 다르지만 이 정책들은 특정 서비스에 대한 규제를 목적으로 하고 있다. 그리고 대체로 그 대상이 되는 기업이나 서비스도 정해져 있다.

물론 실제로 해당 법안에 기업의 이름이 직접 쓰여서 통과되는 것은 아니다. 대부분의 법들은 '전기통신사업법 개정안'이나 '정보통신망법 개정안' 등의 이름으로 입법 절차가 이뤄진다. 하지만 이 이름만으로는 어떤 내용인지 알 수 없기 때문에 해당 법안의 취지나 목적을 잘 드러내기 위해 별칭을 정하는 것이 일반적이다. 그리고 기업과 관련된 정책들은 해당 기업의 이름을 따서 직관적으로 법안의 방향성을 설명되곤 한다. '구글의 마켓 플랫폼 갑질을 막겠다', 혹은 '넷플릭스가 인터넷 망을 무임 승차하지 못하게 규제한다'라는 내용이 이름에 담기는 것이다.

하지만 이 규제들이 적절하게, 또 모두가 합리적이라고 받아들일 수 있는지는 조금 다른 문제다. 인터

넷은 세상을 더 단순하게 연결하고 있지만, 그 영향력은 더 복잡하게 엮이고 있다. 각 국가의 문화, 환경, 규제와 복잡하게 얽히면서 이전의 가치관으로 해결되지 않는 문제들이 늘어나는 것이다. 규제의 목적과 방향이 옳은지 생각해봐야 할 필요가 있다.

ICT 규제의 역할과 필요성

ICT와 관련된 규제의 적지 않은 부분이 해외 기업들과 관련되어 있다. 여전히 ICT와 관련된 기술들의 중심은 미국의 실리콘밸리와 연결되어 있고, 이 기업들이 내놓는 제품과 서비스들은 전 세계적으로 큰 영향력을 내기 때문에 우리나라도 직접적으로 영향을 받는 경우가 많다. 특히 국내의 다른 서비스들과 충돌을 일으키기도 하고, 때로 독점적 영향력을 바탕으로 한 부작용도 일어난다.

이 때문에 모든 분야에서 법과 제도를 통한 적절한 규제는 반드시 마련되어야 한다. 특정 사안이 문제를 일으키면 아무리 좋은 상품이라고 하더라도 해당 기업의 잘못된 부분을 바로잡는 것은 국가가 해야 하는 부분이다. 국내 기업 뿐 아니라 글로벌 기업이라고 하더라도 국가 시스템은 사회적 합의를 거친 규제로 우리 환경에 맞는 제품과 서비스가 이뤄지도록 할 권한과 의무가 있는 것이다.

다른 한편으로는 여전히 국내 특정 산업의 보호를 목적으로 규제가 이뤄지는 부분도 없지 않다. 우리나라 경제 구조의 중심이 되는 제품과 서비스들이 적지 않고, 지금도 꾸준히 늘어가고 있기 때문에 적어도 국내에서 경쟁력을 갖고 성장할 수 있는 환경이 이뤄지도록 국가 시스템이 돕는 것도 자연스러운 일이다.

대부분의 국가들은 자유무역을 이야기하지만 실질적으로는 보호무역을 적절히 섞어서 정책을 세운다. 받아들일 것은 받아들이고, 내어줄 것은 내어준다는 계산인 셈이다. 각 국가별로 꼭 지켜내야 하는 것들, 이는 산업이나 경제구조 뿐 아니라 문화와 정서, 통념까지 연결될 수 있다.

과거에는 무역 규제로 대부분의 것들이 해결되었다. 농산물부터 일본 음악은 유통도, 방송도 안 됐다. 하지만 인터넷은 국경을 넘어 더 많은 것들을 전 세계로 유통하고 있다. 한창 세계를 달구고 있는 K-팝도, 또 K-드라마도 그 배경에는 실시간으로 콘텐츠를 실어 나르는 인터넷이 있다.

인터넷 플랫폼 비즈니스는 점차 전 세계를 하나로 연결하고 있다. 넷플릭스를 통해 전 세계 사람들이 '오징어 게임'에 열광하고, 유튜브를 통해 뉴욕에서 열리는 쇼케이스를 전 세계가 동시에 시청한다.

규제의 방향성, 특정 기업보다 시장 전체로 시야 넓혀야

최근 IT 관련 규제들에서 부쩍 눈에 띄는 것은 특정 기업의 이름이다. 구글 갑질 방지법, 넷플릭스 무임승차 방지법을 대표적으로 들 수 있다. 물론 이 법안에 실제로 기업의 이름이 들어가는 것은 아니다.

예를 들어 넷플릭스 무임승차 방지법은 넷플릭스가 국내에 데이터센터를 따로 마련하지 않은 탓에 통신망 사업자들은 해당 데이터를 일본을 비롯한 해외에서 끌어 와야 하고, 이는 곧 국가간 망 이용에 대한 부담으로 이어졌다.

통신사들의 해법은 여러가지가 있었는데, LG유플러스는 일찍부터 넷플릭스와 제휴를 통해서 국내에 캐시 서버를 두는 방법을 택했다. KT는 상대적으로 용량이 넉넉한 해외 접속망을 통해 서비스를 제공했다. 하지만 SK브로드밴드는 해외 접속망의 부담을 함께 나누는 방법을 택했다. 넷플릭스 때문에 해외망의 부담이 늘었으니 망 이용과 확장 등에 드는 비용 명목으로 넷플릭스가 망 이용 대가를 따로 치러야 한다는 것이었다.

넷플릭스는 오픈커넥트 기반의 캐시 서버를 계속 제안하면서 망 사용료를 낼 수 없다는 입장을 지켰고, 둘 사이의 갈등은 몇 년을 이어왔다. 결국 이 문제가 공론화되면서 '해외 기업이 국내 기업들이 깔아 놓은 인터넷 망을 무료로 쓰고 있다'는 문제가 국회로 넘어갔다.

이는 구글을 비롯한 해외 인터넷 서비스들과 오랫동안 얽혀 있던 문제이기도 하다. 이 기업들이 아무 제한 없이 국내에서 간단히 비즈니스를 시작하고, 쉽게 돈을 벌어간다는 것이다. 인터넷 망 사용료는 국내 인터넷 기업들은 대부분 지불하고 있는 별도의 요금인데, 해외 기업들이 이를 빗겨가고 있다는 '역차별' 논란으로도 이어진다. 하지만 이는 인터넷을 바탕으로 비즈니스를 하는 기업들의 기본 환경과 관련이 있는 문제다. 인터넷의 망 중립성을 비롯한 데이터 패킷 전송 역무라는 인터넷 망 사업자의 책임과도 연결되는 다소 복잡한 문제다.

조금 더 단순하게 보자면 이 상황은 인터넷 초기부터 당연하게 이어져 온 망 사용료 제도가 더욱 글로벌로 확장된 인터넷 환경과 어긋나기 시작하면서 이를 다시 가다듬는 과정이 필요한 단계라고 볼 수 있다. 조금 더 폭넓게 보자면 인터넷 망 사업자와 인터넷 서비스 제공 업체들 사이의 균형을 잡고, 해외 기업들이 일정한 기준을 바탕으로 국내 기업이 억울하다고 느끼지 않을 적절한 해법이 필요한 문제였다. 네이버가 1년에 700억원씩 망 이용료를 낸다는 자료도 공개됐는데, 국내 기업도 이에 대해 통신사와 적절한 답을 찾아낼 필요가 있는 셈이다.

하지만 법안의 이름이 지어지는 과정부터 진행 절차는 이 법의 목적이 단순히 넷플릭스를 규제하기 위해서 만들어진다는 뒷맛이 남아있다. 구글 플레이스토어의 결제 수수료가 부당하고, 외부의 자체 결제 방법을 선택하지 못하는 것을 '갑질'로 규정한 전기통신사업법 제50조 개정안도 다르지 않다.

이 법은 구글의 마켓에서 앱이나 콘텐츠를 판매하면 30%의 수수료를 내야 한다는 부분에서 출발했다. 구글 뿐 아니라 애플 등 대부분의 앱 마켓 수수료는 30%, 즉 콘텐츠 공급자와 유통사 사이의 7:3 비율로 정해져 있다. 애플이 앱스토어를 내놓으면서부터 이어져 오던 암묵적인 규칙이다. 이를 벗어나기 위해 구글 플레이스토어를 벗어난 외부 결제가 적지 않게 이뤄졌는데, 구글이 이를 차단하겠다고 밝히면서 '갑질' 논란이 일어나기 시작했다.

30%의 수수료부터 결제 방법까지 도마에 올랐고, 결국 구글은 연간 매출 100만 달러, 우리돈으로 약 11억원까지는 수수료를 절반인 15%로 낮추는 안을 내놓았다. 하지만 국회는 양보 없이 결제 수단의 강제도 법으로 막아냈다. 적어도 구글 플레이스토어는 이제 앱 내에서 구글 플레이스토어의 결제 방법을 쓰지 않아도 된다.

이 역시 단순히 결제 방법을 강제하는 갑질이라고 단순화해서 보기는 어렵다. 구글플레이를 비롯한 앱 마켓은 콘텐츠 유통 플랫폼이다. 앱과 콘텐츠를 인터넷을 통해 전 세계로 유통해주는 서비스다. 막대한 용량의 데이터 파일을 전송하고, 보안, 마케팅, 홍보, 기술지원 등 다양한 서비스가 뒤따르게 된다. 그에 대한 수수료가 플랫폼의 등장 당시에는 30% 정도로 설계된 것이다. 구글이나 애플이 마켓을 열던 시기만 해도 절반이 넘는 수수료를 내는 유통 시장도 적지 않았기 때문에 30% 수수료는 만족도가 높았던 것도 사실이다. 무엇보다 기존의 분산된 유통 구조보다 일관된 플랫폼에서 전 세계 이용자들에게 같은 경험을 주는 이 시장에 만족을 느끼고, 수수료에 대해서도 당연하게 받아들여지는 경향도 있었다.

하지만 시장이 커지고, 모바일 관련 콘텐츠 매출 규모가 폭발적으로 성장하면서 일관된 수수료에 대해 기업들로서는 부당하다고 느낄 만한 부분도 있다. 큰 수수료에 대한 목소리는 에픽게임즈를 비롯해 많은 기업들이 지속적으로 내고 있고, 마찰과 분쟁, 그리고 협의가 곳곳에서 반복되고 있다.

우리나라는 이에 대해 특정 기업이 마켓을 독점한다는 관점에서 바라보는 분위기가 적지 않다. 국내에 구글 플레이스토어에 대응하는 원스토어가 있고, 국내의 많은 게임 기업들이 수수료에 대한 불만을 갖고 있기도 하다. 구글의 마켓을 견제하기 위해 여러 규제들이 한번에 쏟아졌고, 그 중에서 수수료 인하, 외부 결제 허용, 모든 앱은 국내에 서비스되는 모든 스토어에 등록 같은 문제들이 법으로 고민됐다.

그러자 가장 큰 수혜자로 꼽히던 원스토어가 구글을 비롯한 스토어의 규제에 대해서 우려하고 있다는 이야기가 나오기도 했다. 구글의 플랫폼 규제는 결국 국내 다른 기업에게도 영향을 끼칠 수 있다는 것이다. 수수료를 낮추고, 외부 결제를 푸는 것은 구글만이 아니라 원스토어에게도 똑같은 조건이기 때문이다. 기본적인 수익 구조를 바꾸면 플랫폼의 가장 중요한 지속 가능성에 대한 확신도 떨어지게 마련이다.

이 역시 조금 더 치밀하게 시장 구조와 현실성을 반영했으면 하는 아쉬움이 남는 부분이다. 자칫 이 법안들의 기본이 구글만 보고 만들었다는 지적을 받을 수도 있기 때문이다.

세계적으로 커지는 빅테크 규제, '해외기업이니까…'보다 '국내 이용자 위해서' 되어야

빅테크 규제에 대한 목소리는 세계적으로 커지고 있다. 이미 구글세로 불리는 글로벌 기업들의 형평성 있는 과세는 오랫동안 많은 국가들이 고민해 왔고, 조세 회피처나 규제를 넘나드는 여러 가지 방법들을 제도권 안으로 끌어들이는 방안들이 자리를 잡아 가고 있다.

유럽연합의 일반개인정보보호법(GDPR) 같은 규제 역시 이 빅테크 기업들이 전 세계의 인구를 대상으

로 개인정보를 다루는 방법과 가이드라인을 상세하게 정해두면서 큰 파장이 일었다. 하지만 이 규제들을 통해서 온라인의 조세 국경, 그리고 개인정보 보호에 대한 기준점이 생겨났고, 큰 틀에서 빅테크 기업들도 흐름을 따라가는 중이다.

그럴수록 온라인은 더 많은 다양성과 예측불허의 신기술을 통해 복잡성을 더해가게 마련이다. 앱 마켓 규제 역시 다음 논란 거리로 도마에 올라 와 있던 주제다. 우리나라의 사례를 바탕으로 다른 나라들도 플랫폼 기업들의 규제를 고민하고 있다.

하지만 규제의 방법은 조금 더 신중하고, 큰 그림이 필요해 보인다. 넷플릭스 무임승차 방지법은 모호한 규제로 기업간의 갈등을 씻어내기는 커녕 여전히 이어지는 논란으로 남아 있다. 해당 법의 무기력함도 지적된다. 구글의 수수료 논란도 기업들이 모두가 반기기만 하는 주제가 아니다. n번방 방지법의 핵심 법안인 정보통신망법 및 전기통신사업법 개정안 역시 그 중심에는 텔레그램이라는 규제의 목적지가 있었지만 결과적으로는 해당 법으로 텔레그램을 뒤져볼 수는 없었다. 대신 국내 메신저 기업들의 검열 논란이 튀어 나왔다.

인터넷의 규제는 그 어떤 규제보다 어려울 수밖에 없다. 기술적으로, 때로는 법적으로 근거를 마련하기 어려운 부분이 너무 많기 때문이다. 그래서 기본적인 정책 기조를 세우고, 그에 맞춰 더 치밀하고 정교하게 법안이 만들어지고, 엄격하게 시행되어야 한다.

한편으로는 규제가 그 안에는 '해외 기업이 국내에서 쉽게 큰 돈을 벌어간다'는 감정적인 요소가 비치는 부분도 있다. 국내 산업을 보호하고, 우리 환경에 더 맞는 서비스들을 키우기 위한 적절한 규제는 필요하지만 특정 기업에 대한 차별이 눈에 띄는 것은 바람직하지 않다. 또한 갈등이 무역이나 통상 문제로 이어질 수 있다. 국내 기업들 역시 시장이 국내에만 머무르는 것이 아니기 때문이다. 글로벌 플랫폼을 타고 세계 시장을 만나는 것이 당연한 일이 됐고, 우리나라 기업들이 글로벌로 손꼽히는 플랫폼 사업을 하기도 한다.

자칫 국내의 규제들이 기업들에게 해외에서 차별을 만들어낼 여지가 될 수도 있고, 규제 안에서 글로벌 스탠더드의 경험을 놓칠 가능성도 있다. 국내의 플랫폼 기업들도 글로벌 기업들에 뒤지지 않을 뿐 아니라, 오히려 국내 시장에서는 이용자들의 입맛을 더 잘 맞출 수 있다는 것이 늘 경쟁력으로 언급되곤 한다. 경쟁력과 적절한 규제가 함께 갈 수 있는 방법이 고민되어야 한다.

그 사이에 이용자들은 가려지는 부분도 있다. 위치 정보법을 비롯해서 적지 않은 규제들이 해외 기업에는 진입장벽으로, 국내 기업에는 역차별로 이야기된다. 그 사이에 이용자들은 해당 서비스에서 소외되곤 한다. 국가가 기업을 규제하는 가장 중요한 원칙은 이용자 보호에 있어야 한다. 우리도 전 세계 사람들과 같은 서비스를 이용할 수 있는 권리가 있다. 시장보다 이용자가 중심에 놓인다는 기본 원칙이 규제 전반에 놓여야 할 것이다.

무한경쟁 OTT 시장 라운드1 전망

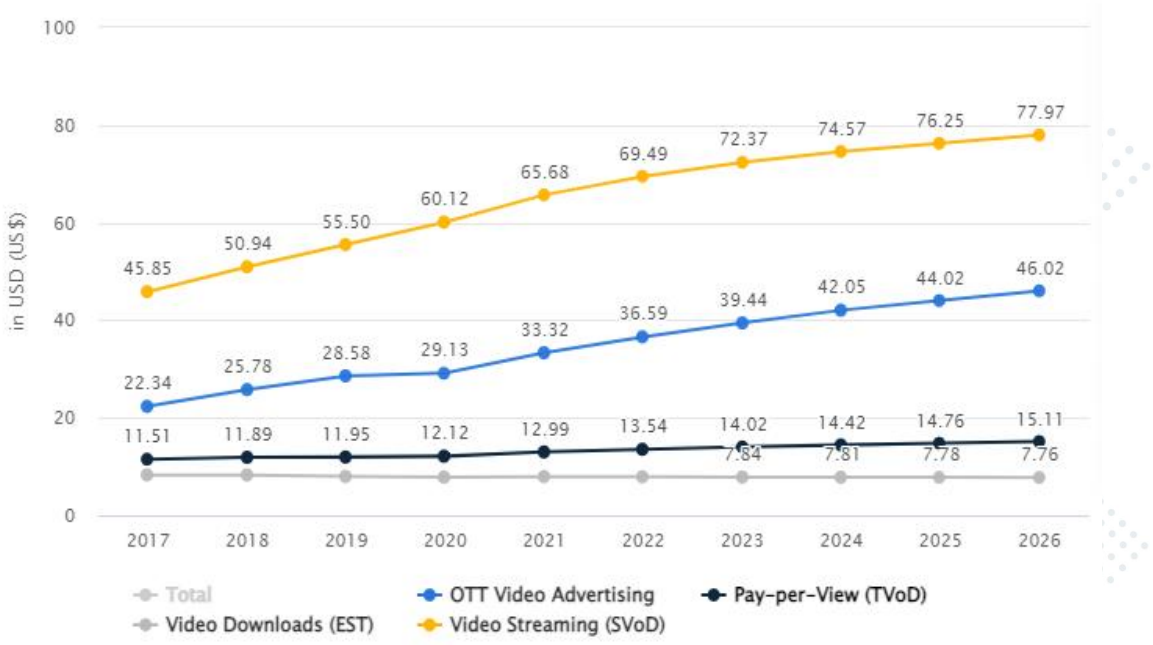
최홍규 (think.bc399@gmail.com)

EBS 연구위원 / 미디어학 박사

지속 성장하는 OTT, 경쟁자들은 353조를 향한 오징어 게임 중

각종 통계지표를 제공하는 스태티스타(statista)에서 발표한 자료를 보자. 글로벌 시장에서 동영상 OTT(Over The Top) 시장의 수익은 2021년도에 무려 1,780억5천만 달러에 이를 것으로 예상한다. 한화로는 211조2,741억3천만 원쯤 되는 액수다. 2021년부터 시작하여 2026년까지 총 5년이라는 시간 동안 매출 성장률은 10.84% 정도 되고 이러한 매출이 누적되어 2026년에 이르러 추산되는 동영상 OTT 시장의 규모는 2,979억1천5백만 달러에 이를 것으로 예측된다. 결과적으로 2026년에 이르러 전 세계 동영상 시장의 규모는 한화 353조 원이 넘는 규모가 될 것으로 가늠되고 있다.

수익의 규모로 볼 때, 구독 서비스를 제공하는 서비스 영역인 SVOD(Subscription Video On Demand)의 이용자당 평균 수익 규모가 가장 크고, 다음으로 광고를 기반으로 하는 동영상 서비스, 다음으로 시청 콘텐츠 당 이용료를 지불하는 PPV(Pay-per-View) 서비스가 그다음 순이다. 구독 서비스로 지불하는 비용이 상대적으로 높아서 나온 당연한 결과이지만, 이로써 향후 광고기반 서비스보다 구독기반의 광고프리 형태 서비스가 지속하여 성장할 것이라는 예측이 가능하다.



[그림 1] 글로벌 OTT 시장의 이용자당 평균 수익(ARPU)[3)]

이처럼, 동영상 기반의 OTT 시장은 지속하여 성장하고 있고 그중에서도 구독기반 서비스가 더욱 성장할 것이라는 예측이 지배적이다. 지금으로부터 14년 전 넷플릭스(Netflix)가 인터넷 기반의 스트리밍 서비스를 제공하기 시작했고, 이 시점인 2007년부터 동영상 기반 OTT 서비스가 하나의 미디어 제공 유형으로 자리 잡기 시작했다. OTT 시장은 그로부터 20년간 지속적인 성장세를 이어가며 거대한 산업 영역으로 자리를 잡아갈 것이다!

처음에는 넷플릭스가 스트리밍 기반의 동영상 서비스나, OTT 서비스의 대명사와 같은 서비스였다. 하지만 글로벌 서비스로는 넷플릭스, 디즈니플러스(Disney+), 아마존 프라임 비디오(Amazon Prime Video), HBO 맥스(HBO Max)가 시장에서 두각을 보이고 국내에서는 웨이브(wavve), 티빙(TVING), 왓챠플레이(Watcha Play), 시즌(seezn) 등이 서로 경쟁을 하면서 이제는 글로벌 OTT 시장이 포화상태에 이르렀다.

여기서 포화상태라는 것은 소비자 숫자의 포화를 말한다. 동영상 OTT 서비스라는 큰 돔(dome) 같은 공간에 이용자들이 들어올 만큼 들어왔고, 이 OTT 시장의 돔 안에 더 많은 이용자를 수용할 수 없게 되었다. 따라서, 사업자 간에 서로 이용자를 뺏고 빼앗기는 게임이 시작된 것이다. 최종 승자가 되기 위한 경쟁이 본격화된 것이다. 최종 승자는 더 많은 이용자를 확보할 수 있게 된다. 물론 이용자 취향이 더욱 세분화하는 요즘의 세상에서는 OTT 사업자로서 승자가 하나라도 그 혼자만 살아남을 수는 없게 될 가능성이 있다. 이용자 취향별로 서비스가 존재해야 하므로.

3) https://www.statista.com/outlook/amo/media/tv-video/ott-video/worldwide#global-comparison

2021년은 경쟁자 모두 링 위에 오를 준비를 마친 시기

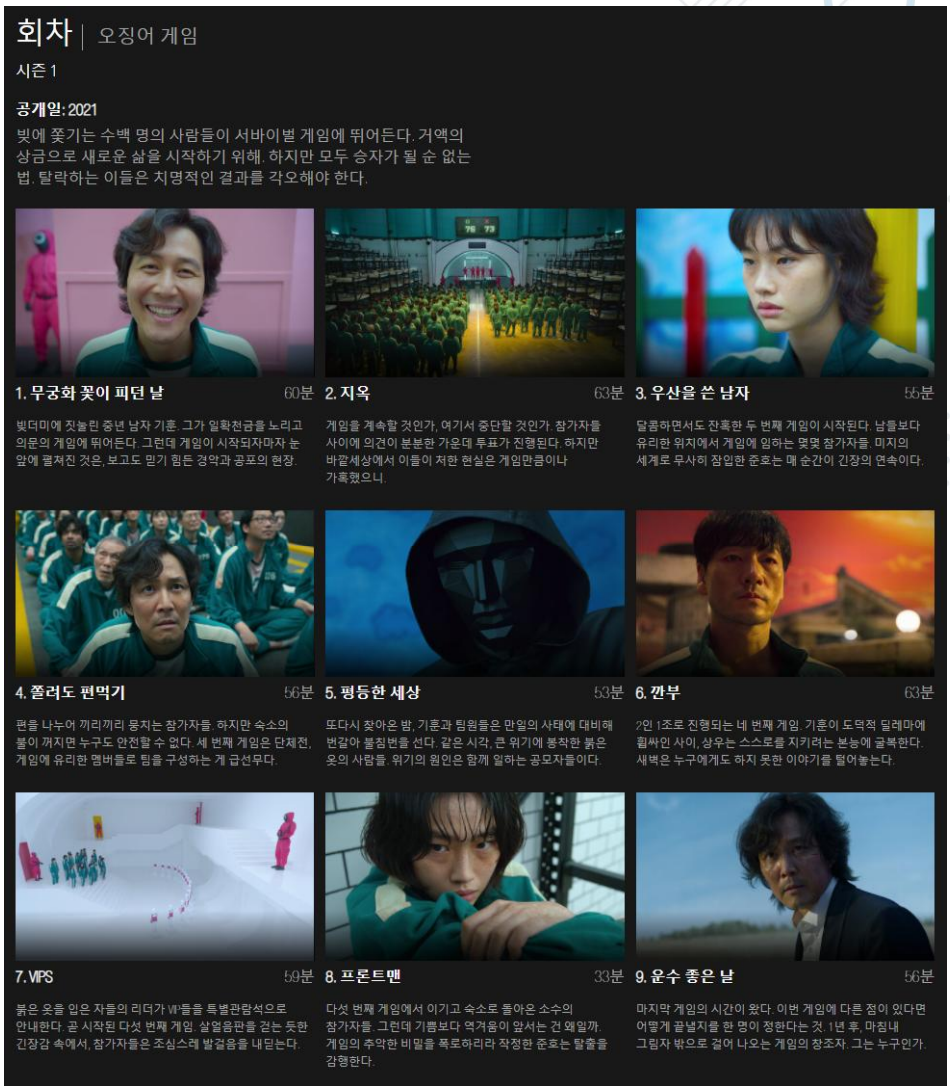
2021년은 시장에 들어오겠다고 말한, 소위 플랫폼을 제공하겠다고 발표한 사업자들은 모두 링 위에 올라선 상태라고 할 수 있다. 글로벌 시장에서는 넷플릭스(2007년)뿐만 아니라 아마존(2018년), 페이스북(2018년)에 이어 애플(2019년), 디즈니(2019년), 컴캐스트(2020년), HBO(2020년)까지 가세했으니 말이다. 국내에서도 지상파 3사(KBS, MBC, SBS)의 연합체인 웨이브(2019년), 유료방송사인 CJ ENM과 JTBC가 협력한 티빙(2020년)까지 합세했으니 이제 동영상 OTT 시장은 진정한 경쟁의 장이 마련된 셈이다.

[그림 2] 디즈니플러스에 공개된 '완다비전'[4]

무엇보다 콘텐츠 최강자인 디즈니플러스의 동영상 OTT 시장 참여는 큰 충격이었다. 너무나 많은 히어로물과 명작 애니메이션을 보유한 디즈니였으므로 콘텐츠를 중심으로 시장에서 행사할 영향력이 클 것으로 여겨졌기 때문이다. 디즈니라고 하면 전통과 역사를 지니는 콘텐츠 제작 그룹으로서의 이미지가 있어 그들이 제공하는 플랫폼은 다를 것이라는 이용자들의 기대감이 있었다.

시장에서 가입자 수로 절대적 우위에 있었던 넷플릭스마저 경계감을 드러내면서 디즈니가 시장에서 가할 영향력은 더욱 크게 느껴졌던 것이 사실이다. 넷플릭스에서 디즈니 콘텐츠가 대거 빠져나가게 되면서, 디즈니가 넷플릭스의 존재감마저 지워버리는 것이 아닌가 싶었다. 하지만, 그렇지 않았다.

4) https://www.disneyplus.com

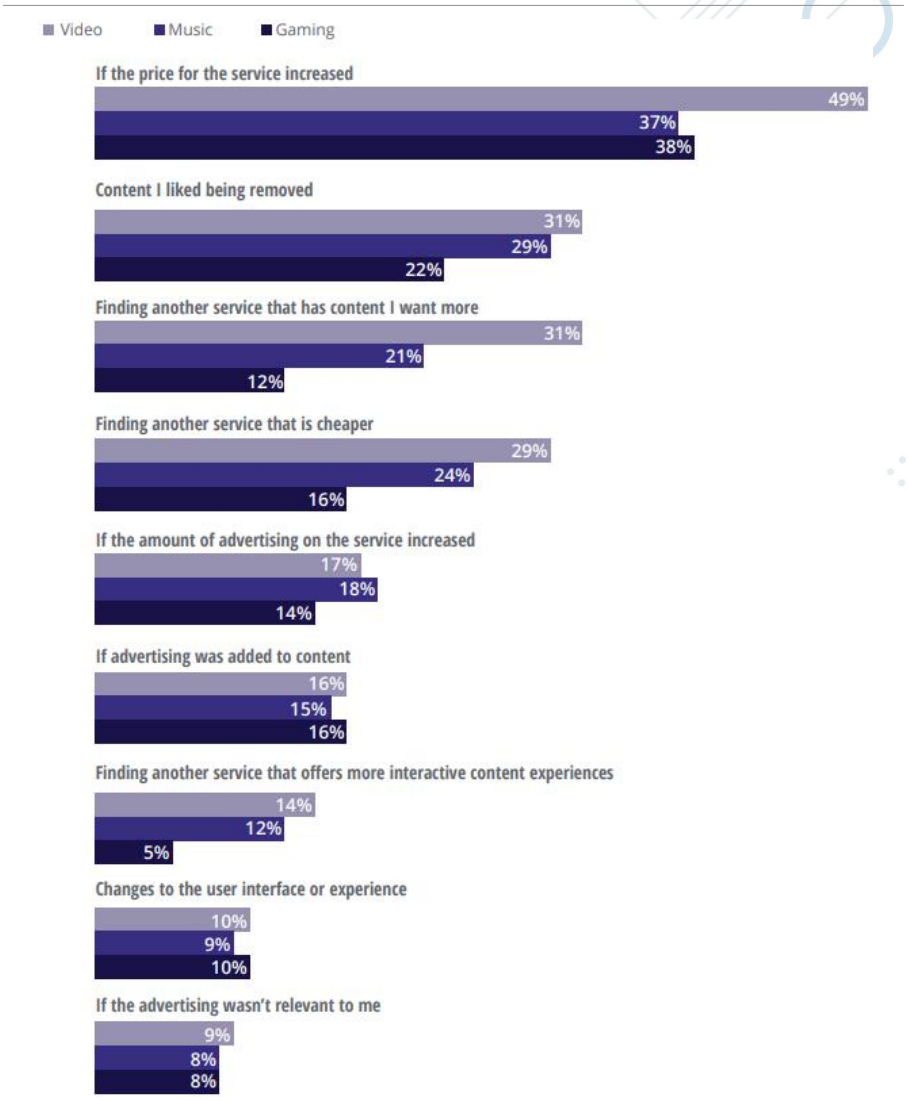


[그림 3] 넷플릭스에서 큰 화제를 낳은 시리즈 '오징어 게임'[5)]

넷플릭스는 '오징어 게임'이라는 대한민국 감독이 만든 콘텐츠를 서비스 전면에 앞세워 가까스로 시장에서 버티는 모양새다. 아직까지도 서양인들에게는 콘텐츠에 있어서 변방인 대한민국, 이 대한민국에서 만든 콘텐츠에 전 세계는 열광했다. 덕분에 넷플릭스는 코로나19로 인한 비대면 환경에 입은 수혜를 이어갈 수 있었다.

코로나19가 확산하기 직전까지도 동영상 기반의 OTT 시장은 한동안 쟁쟁한 사업자들이 대거 등장하며, 레드오션으로 구획화되는가 싶었다. 하지만, 코로나19는 기존 미디어 시장의 이용자들을 OTT 서비스로 끌어들이는 효과를 낳았고 덕분에 시장은 활력있는 경쟁환경이 갖춰질 수 있었다.

5) https://www.netflix.com/kr/title/81040344



[그림 4] 어떠한 경우에 서비스를 바꿔 이용하는가에 대한 설문결과[6)]

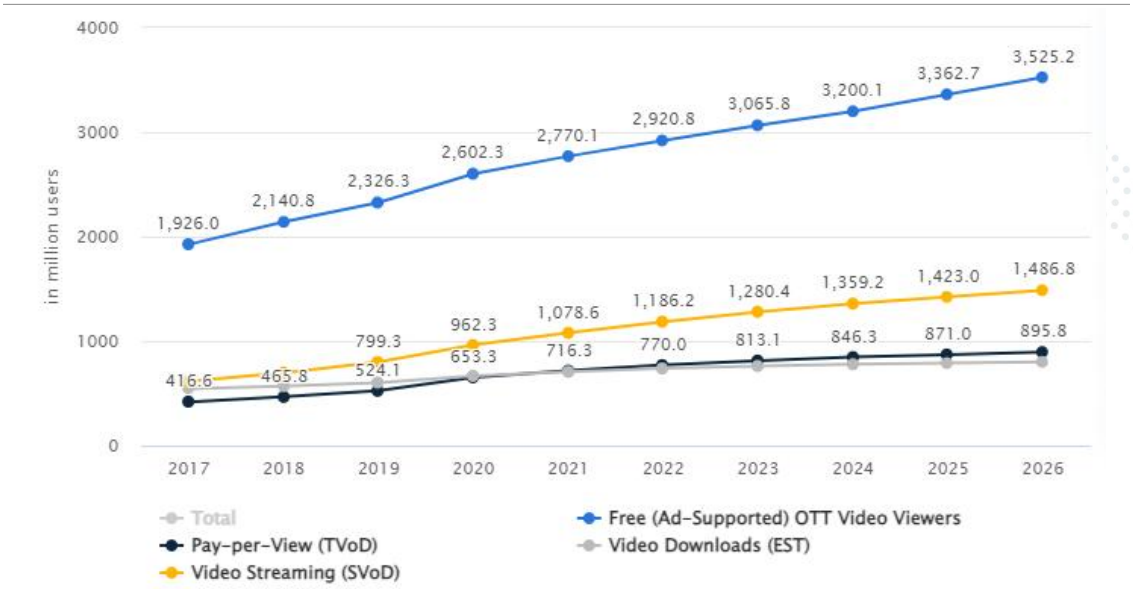
동영상 OTT 시장의 경우 이용자는 대개 가격이 올랐을 때, 가입된 서비스를 해지하고 새로운 서비스에 가입할 확률이 높다. 다음으로 보고 싶은 콘텐츠가 없을 때도 서비스를 갈아탈 확률이 높게 나타난다(위의 그래프). 그래서인지, 광고나 서비스 인터페이스도 가입에 영향을 미치지만. 무엇보다 이용자에게는 OTT 서비스를 선택하는 요인으로 가격과 콘텐츠와 관련한 요인들이 가장 많이 꼽힌다.

2021년까지 거대 기업들이 대거 진출한 OTT 시장이 아직도 알 수 없는 경쟁 시장으로 남아있는 이유가 여기에 있다. 시장에 참여한 어느 사업자도 가격을 낮출 수 있을 정도로 규모가 있는 사업자들이다. 또한, 콘텐츠를 무한정 생산할 수 있을 정도로 자금력이 있는 사업자들이 대부분이기 때문이다. 결국, 규모의 경제라는 답이 정해져 있는 OTT 시장에서 남다른 전략으로 이용자를 사로 잡아야 시장에서 승기를 잡아갈 수 있다는 것이다.

6) https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html

진정한 라운드1, 2022년에 살아남아야 진정한 강자

OTT를 구독 서비스로 한정하지 말고 살펴보면, 시장에서 구글의 유튜브가 1위다. 글로벌 OTT 시장에서 이용자 수 추이를 봐도 광고기반의 동영상 시청자들의 숫자가 가장 많아질 것으로 예측된다. 이용자 수를 중심으로 보면 유튜브에게 구독 서비스 분야 최강자인 넷플릭스나 여타 구독 서비스들이 명함을 내밀기 힘들다. 광고기반의 동영상 OTT 영역은 유튜브로 인해 아직도 많은 이용자 수를 보유하고 있다.

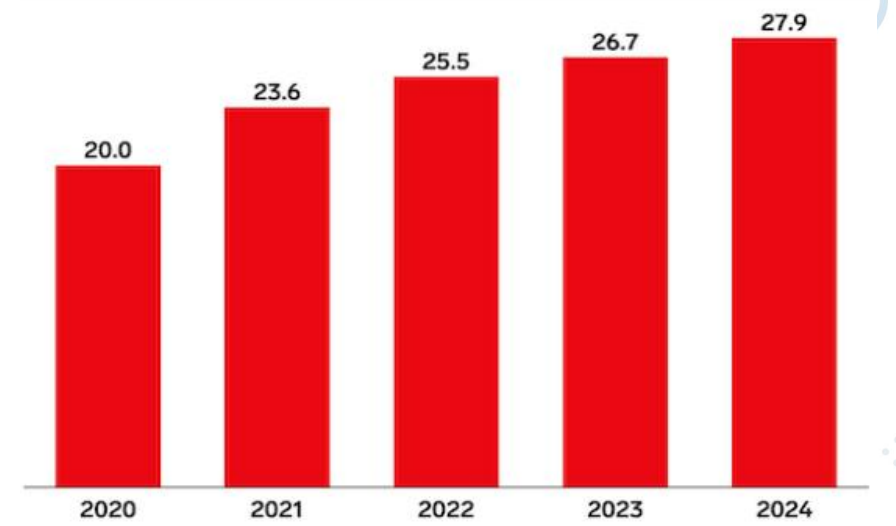


[그림 5] 글로벌 OTT 분야별 이용자 수 추이(단위: 백만 명)[7)]

전 세계 동영상 OTT 사업자들의 수익 순위를 굳이 따져도 알파벳(Alphabet, Inc.), 아마존(Amazon.com, Inc.), 애플(Apple, Inc.), AT&T(AT&T, Inc.), 컴캐스트(Comcast Corp.), 아이치이(iQIYI, Inc.), 넷플릭스(Netflix, Inc.), 텐센트(Tencent Holdings Ltd.), 월트디즈니(The Walt Disney Co.), 워너미디어(Warner Media, Llc) 순서다. 구글의 알파벳이 1등이다. 그래서 유튜브는 2021년 구독 서비스 경쟁에 치열하게 뛰어들지 않은 사업자인 것처럼 보인다.

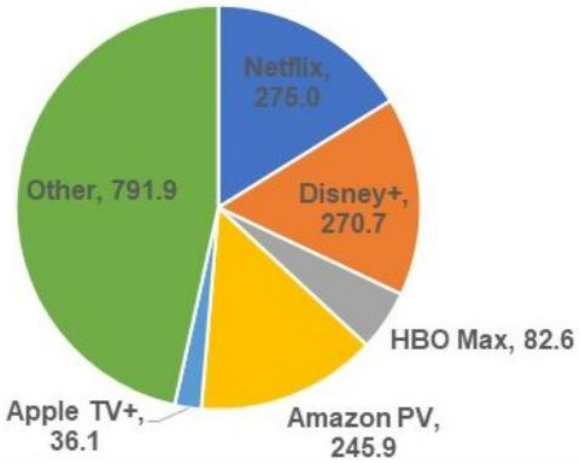
하지만 그렇지도 않다. 유튜브의 구독 서비스인 유튜브 프리미엄 서비스는 이미 미국 내에서만도 2천 3백만 명 이상에 달할 정도의 가입자 수 규모를 보인다. 2026년까지 지속하여 성장할 것이라는 예측도 있다. 물론, 가입자 수로만 따지면 넷플릭스를 비롯한 구독 서비스에 비해 낮은 수준이라고 할 수 있지만, 유튜브는 아직 본격적으로 구독 서비스 가입자를 늘려나갈 전략을 펴지 않은 것으로 보이며 앞으로의 행보는 알 수 없다.

7) https://www.statista.com/outlook/amo/media/tv-video/ott-video/worldwide#global-comparison



[그림 6] 2024년까지 미국 내 유튜브 프리미엄 가입자 수 전망(단위: 백만)[8)]

그럼, 다시 유튜브를 빼고 구독 서비스를 중심으로 시장을 살펴보자. 여전히 넷플릭스가 강자일까? 이 또한, 그렇지 않다. 구독 서비스 시장은 치열한 경쟁 상태이므로 2026년이 지나면 디즈니플러스가 넷플릭스를 앞설 것이라는 전망도 나오고 있다. 2020년과 2021년에 넷플릭스가 얻은 특수는 코로나19로 얻은 행운의 특수요. 오징어 게임이라는 넷플릭스 역사상 최고의 콘텐츠로 평가받은 콘텐츠가 등장했기 때문에 가능했던 특수지, 이것이 오래 못 갈 것이라는 전망도 등장하는 것이다.



[그림 7] 2026년까지 구독형 OTT 서비스 가입자 수 전망(단위: 백만)[9)]

2022년은 코로나19라는 특수가 사라져가는 시기이고, 시장에 처음 등장한 사업자들이 시장에 적응을 마치고 맞는 시기이다. 2022년에 두각을 보이는 사업자가 결국 시장에서 향후 10년을 버틸 사업자가

8) https://www.emarketer.com/content/youtube-premium-will-accrue-us-subscribers-by-year-end-2021
9) https://www.digitaltvnews.net/?p=37411

될 것이라고 본다.

2년 전 디즈니가 OTT 시장에 등장한다고 했을 때, 필자와 함께 사람들이 디즈니에 걸었던 기대감은 절반은 맞고 절반은 틀렸다. 디즈니가 그간 시장에 적응했던 시기였으므로 겪었던 시행착오도 있었을 것이다. 유튜브도 마찬가지다. 유튜브가 구독과 광고 사이에서 사업모델을 고민하는 동안에 구독 서비스 영역은 급성장했다. 유튜브는 그간 이렇게 성장한 시장을 뒷짐 지고 지켜보지만은 않았을 것이다. 전략적 고민들이 그간 축적되었을 것이다. 전 세계적으로 분리된 시장으로 보여서 그렇지, 중국의 OTT 시장도 무시할 수준은 아니다. 글로벌 시장에서는 변방이지만, 우리나라 OTT 시장도 무려 '오징어 게임'이라는 콘텐츠를 만들어낼 수 있는 만큼의 저력이 있는 시장이다.

2022년은 그야말로 무한경쟁이 가능한 OTT 시장의 라운드1이 될 것이다. 머니게임으로 점철될 경쟁시장이 될 것이 뻔하다. 벌써 국내외의 OTT 콘텐츠 제작시장에서는 몇천억은 우습고 '조' 단위의 투자가 보통 수준으로 언급되고 있다. 살기 위해서 이겨야 하는 시장이 아니라, 이겨야 살아갈 수 있는 시장. 포화한 가입자 수를 누가 더 많이 확보하느냐의 땅따먹기 시장. 그 치열한 경쟁의 서막이 2022년 드디어 열린다. 이용자들은 OTT의 신작을 기다리듯 지켜보면 된다. 그리고 좋은 서비스 하나를 선택해 가입하면 된다. 물론, 마음에 안 들면 해지하고 다른 서비스에 가입하면 된다. 라운드1은 그렇게 진행된다.

소프트웨어 보안 관점에서 본 미국 사이버보안 행정명령과 우리의 대응방안

이태준 (tjlee@korea.ac.kr)

고려대학교 컴퓨터보안연구실 연구원

* 공동저자:
이희조 (고려대학교 교수, heejo@korea.ac.kr)
박춘식 (고려대학교 연구교수, cspark14@hanmail.net)

제1장 서론

2021년 5월 12일, 미국 바이든 행정부는 『국가의 사이버보안 향상에 관한 행정명령(EO 14028) (2021)』을 내렸다. 이는 최근 콜로니얼 파이프라인 공격이나 솔라윈즈 공급망 공격과 같은 **대규모 사이버 공격 사례가 등장하여 사이버보안의 필요성이 증가**했기 때문이다. 이러한 악성 사이버 공격이 공공부문, 민간 부문을 넘어 개개인의 보안과 프라이버시까지 위협한다고 미국 정부는 판단한 것이다.

우리나라 또한 소프트웨어 보안 문제에서 자유롭지 않다. 소프트웨어에 국경이 없는 만큼 해외소프트웨어의 취약점이 국내에 영향을 끼칠 수 있으며 반대의 경우도 마찬가지이다. 소프트웨어 공급망을 통해 전세계가 연결되어 있기 때문에 **미국의 행정명령을 통해 나온 규제에서 국내 기업도 자유로울 수 없는 것**이다.

많은 국내 소프트웨어 기업들은 소프트웨어 제품의 구현을 중심으로 하는 프로세스를 가지고 있다. 근래의 사이버보안 요구사항은 소프트웨어 개발부터 유통까지 공급망의 모든 과정을 대상으로 하기 때문에 이에 대비하기 위해서는 많은 비용과 시간을 들여 근본적인 체질 개선을 해야 한다. 이번 행정명령과 같은 **변화를 미리 파악하고 대비하지 않으면 이후에 더 큰 비용**으로 돌아올 수 있다.

본 문서는 소프트웨어 제품을 개발하는 기업에서 행정명령의 요구사항에 맞추기 위해 무엇을 준비해야 할지 살펴보기 위해 작성되었다. 행정명령 중 소프트웨어 보안에 대한 부분인 4절의 내용과 연관된 문서들, 그리고 국내의 소프트웨어 보안 관련 정책을 분석하여 앞으로 **국내 기업에서 소프트웨어 제품 보안 요구사항에 어떻게 대비해야 할지 점검**하고자 한다.

제2장 미국 사이버보안 행정명령

이번 행정명령은 앞으로의 사이버보안 위협에 맞서기 위해 시행되는 조치로 총 11절로 구성되어 있다.

- 1절 방침(Policy)
  - ■ 행정명령의 배경과 목적에 대해 설명
- 2절 위협 정보 공유 과정의 장애물 제거
- 3절 연방 정부 사이버보안의 현대화
- 4절 소프트웨어 공급망 보안의 강화
- 5절 사이버안전심의회(Cyber Safety Review Board)의 설치
- 6절 연방 정부의 사이버보안 취약점과 사고 대응 전략 표준화
- 7절 연방 정부 네트워크에서 사이버보안 취약점과 사고 검출 개선
- 8절 연방 정부의 조사 및 복구 능력 향상
- 9절 국가안보시스템
- 10절 용어 정의
- 11절 일반적인 규정(General Provisions)

행정명령의 1절에서는 **연방 정부와 민간 부문의 협력을 강조**하고 있다. 안전한 사이버 공간을 만들기 위해 연방 정부는 사이버 공격을 방어, 탐지 및 대응하기 위한 노력을, 민간 기업은 끊임없이 변화하는 위협 환경에 적응하며 자사 제품이 안전하게 구축 및 운용되고 있는지 확인해야 한다는 것이다. 최종적으로 디지털 인프라에 대한 신뢰를 구축하여 국가 및 경제의 안전을 보장하는 것을 목표로 한다.

행정명령 4절 '소프트웨어 공급망 보안의 강화'는 소프트웨어 개발 및 유통 과정에서의 보안 강화에 대

해 다룬다. 내용을 보면 보안 강화를 위한 지침 발행, 가이드라인 공표 등 어떤 기관이 언제까지 무엇을 수행해야 하는지를 지시하는데, 그 안에서 **소프트웨어 제품 개발 기업에 요구되는 사항**들을 볼 수 있다.

제3장 소프트웨어 공급망 보안의 강화 (행정명령 4절)

행정명령 4절은 총 24항으로 구성되어 있으며, 각 항은 어떤 기관이 언제까지 무엇을 해야 하는지를 지시한다. NIST 등 각 부처와 기관은 행정명령의 내용에 따라 보안 강화를 위한 지침 발행, 주요 소프트웨어의 정의 공표 및 보안 지침 발행, 소프트웨어 라벨링 등 필요한 조치를 수행해야 한다. 각 항의 세부 내용과 기한은 Appendix A를 통해 확인할 수 있다.

[그림 1]은 행정명령 4절 중 소프트웨어 제품을 개발하는 기업에서 대응해야 할 항목들을 시간 순으로 정리한 것이다. 크게 주요 소프트웨어 관련, SBOM 관련, 소프트웨어 테스트 관련, 가이드라인 및 지침 관련으로 나눌 수 있다.

[표 1] 소프트웨어 제품 개발 기업 관점 타임라인

가) '주요 소프트웨어(critical software)' 관련

'주요 소프트웨어'는 연방 정부에서 사용하는 주요 소프트웨어 제품에 대한 보안 기준을 개발하기 위해 행정명령에서 도입한 개념으로, 일반적인 의미의 주요 소프트웨어와 구분하기 위해 EO-주요(EO-Critical) 소프트웨어라 한다. **EO-주요 소프트웨어로 지정된 소프트웨어는 연방 정부가 소프트웨어를 구매 및 관리하는 방법을 포함하여 추가적인 활동**을 필요로 한다. 따라서 서비스하고 있는 소프트웨어 제품이 EO-주요 소프트웨어에 해당되는지 알아보고, EO-주요 소프트웨어를 위한 보안 조치를 적용해야 한다.

NIST에서 공표한 EO-주요 소프트웨어의 정의에 따르면, EO-주요 소프트웨어란 다음 속성들 중 하나 이상을 포함하는 소프트웨어 혹은 그러한 소프트웨어를 직접적으로 포함하는(direct dependencies) 소

프트웨어를 의미한다.

- 상승된 권한으로 작동되거나 권한을 관리하는 소프트웨어
- 네트워크 및 컴퓨팅 자원에 직접적으로, 혹은 권한을 부여받아 접근할 수 있는 소프트웨어
- 운용 기술이나 데이터로의 접근을 제어하기 위해 설계된 소프트웨어
- 신뢰와 직결되는 기능을 수행하는 소프트웨어
- 권한 있는 접근(Priviliged Access)으로 신뢰 경계 밖에서 운용되는 소프트웨어

NIST는 소프트웨어 시장의 규모, 범위 및 복잡성과 정부 내에서 필요한 인프라를 감안하여 EO-주요 소프트웨어의 공급망 보안 강화를 단계적으로 접근하기로 하였다. 행정명령을 처음 적용하는 단계에서는 스탠드얼론 및 온프레미스 소프트웨어를 중심으로 하고, 그 이후에 클라우드 기반 소프트웨어나 펌웨어, OT 분야의 소프트웨어 등을 포함시키는 것을 권장하였다. 첫 적용 범위에 해당되는 소프트웨어의 예비 리스트를 보면 **운영체제, 웹 브라우저, 방화벽, 원격 취약점 검사 소프트웨어 등 광범위한 소프트웨어가 EO-주요 소프트웨어에 해당**된다.

배포되는 방식과 무관하게 EO-주요 소프트웨어에 정의에 해당되는 제품은 모두 EO-주요 소프트웨어이다. 오픈소스 소프트웨어 또한 예외가 아니다. EO-주요 소프트웨어의 정의에 해당되는 오픈소스 소프트웨어를 컴포넌트로 사용하는 경우 이를 개발 프로세스에 포함시켜 요구사항을 준수해야 한다. 임베디드 소프트웨어나 펌웨어 또한 EO-주요 소프트웨어에 해당될 수 있다.

EO-주요 소프트웨어에 해당되는 소프트웨어 제품을 개발하는 기업은 **EO-주요 소프트웨어에 대한 보안 조치를 제품에 적용**해야 한다. 보안 조치에 대한 지침은 기존에 발행된 여러 보안 관련 문서를 기반으로 하는데, 그 중 NIST의 Cybersecurity Framework와 SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations를 우선적으로 참조하여 만들어졌다.

지침은 다섯 가지 목표와 그에 맞는 조치로 구성되어 있으며, 간략한 내용은 다음과 같다.

1. EO-주요 소프트웨어를 인증되지 않은 접근 및 사용으로부터 보호

(1) 다중 요소 인증 사용
(2) EO-주요 소프트웨어 및 플랫폼에 접근하는 각 서비스를 고유하게 식별 및 인증
(3) 네트워크 기반 관리를 위한 권한 있는 접근(privileged access) 관리 원칙 준수
(4) 적절한 경계(boundary) 보호 기법 사용

2. EO-주요 소프트웨어에서 사용되는 데이터의 CIA 보호

(1) 데이터 인벤토리 설정 및 유지 관리
(2) 데이터 및 자원에 대한 세분화된 접근 제어 사용

(3) 민감한 데이터에 대한 암호화를 통해 저장된 데이터 보호

(4) 상호 인증 및 민감한 데이터 통신 암호화를 통해 전송 중인 데이터 보호

(5) 데이터 백업, 백업 복구 실행 및 데이터 복구 준비

3. EO-주요 소프트웨어 플랫폼과 해당 플랫폼에 배포된 소프트웨어를 식별하고 관리하여 악용 방지

(1) 소프트웨어 인벤토리 설정 및 유지 관리

(2) 패치 관리 방법 적용

(3) 구성 관리 방법 적용

4. EO-주요 소프트웨어와 관련된 위협과 사고에 대한 빠른 발견, 대응, 회복

(1) 보안 관련 이벤트를 기록하기 위한 로깅 설정

(2) 지속적인 보안 모니터링

(3) 엔드포인트 보안 보호 기법 적용

(4) 네트워크 보안 보호 기법 적용

(5) 모든 보안 운용 담당자 및 사고 대응 팀 구성원 교육

5. EO-주요 소프트웨어의 보안을 담당하는 사람의 이해와 능력을 강화

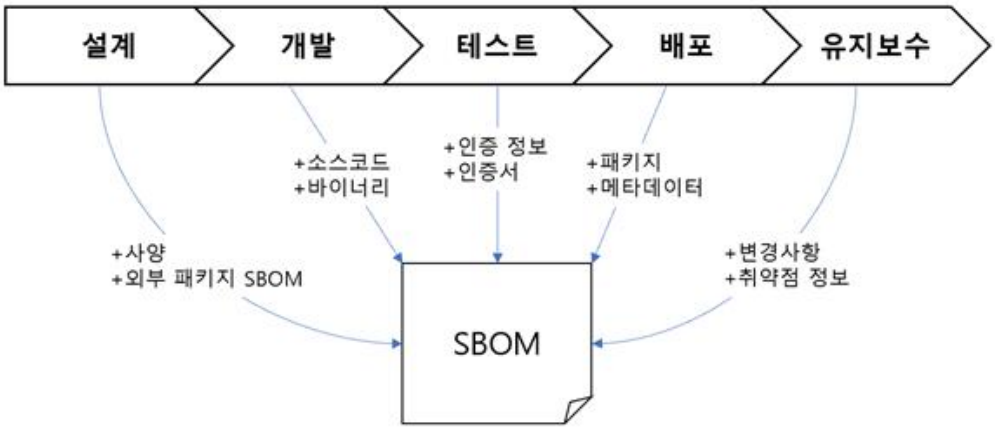
(1) 모든 EO-주요 소프트웨어 사용자 교육

(2) 모든 EO-주요 소프트웨어 및 플랫폼 관리자 교육

(3) 보안 인식 활동 자주 수행

나) SBOM 관련

SBOM은 Software Bill of Materials의 준말로 **소프트웨어를 빌드하기 위해 사용된 여러 컴포넌트에 대한 내용과 공급망 관계를 형식에 맞춰 기록하는 것**을 의미한다. 식품의 성분표와 비슷한 역할을 한다고 볼 수 있다. SBOM은 소프트웨어 제품을 생산, 소비, 운용하는 자가 공급망에 대해 더 깊이 이해하고, 알려진 혹은 새로운 취약점과 위협을 추적할 수 있게 한다. 특히 알려진 취약점의 확산을 저지하는 데 효과적이다.



[그림 1] 소프트웨어 개발 주기에 따른 SBOM 정보

SBOM은 소프트웨어가 어떤 패키지를 포함하는지, 어떤 코드와 파일로 구성이 되는지, 어떤 인증을 받았는지 등 소프트웨어에 대한 자세한 정보를 포함해야 한다. [그림 1]은 소프트웨어가 개발되는 주기의 각 단계가 SBOM에 어떻게 반영되는지를 나타낸 그림이다. SBOM은 소프트웨어를 설계하는 단계부터 배포되기까지 고려되어야 하며, 배포 이후 유지보수 단계에서도 소프트웨어의 변경사항과 취약점 등 위험 관련 정보가 지속적으로 반영, 배포되어야 한다.

행정명령에 의해 NTIA에서 SBOM의 최소 요소를 공표하였다. SBOM의 최소 요소란 취약점 관리, 라이선스 등 기본적인 SBOM의 활용에 필요한 최소 요소를 의미한다. 공표된 최소 요소는 크게 세 부분으로 필수적인 항목, 자동화, 관행과 절차로 구성되어 있다. 필수적인 항목은 SBOM이 어떤 정보를 담아야 하는지를, 자동화는 SBOM 생성이 자동화되어야 한다는 것을, 관행과 절차는 SBOM을 어떻게 관리하고 운영해야 하는지를 담고 있다.

필수적인 항목의 경우 각 컴포넌트에 대해 추적하고 관리해야 하는 기본 정보를 지정한다. 기본 정보는 컴포넌트 공급자명, 컴포넌트명, 컴포넌트 버전, 컴포넌트 식별을 위한 기타 고유 식별자, 의존 관계, SBOM 데이터 작성자, 타임스탬프로 총 7가지 항목으로 구성되었다.

자동화의 경우 SBOM을 생성하고 처리하기 위한 **데이터 형식을 SPDX, CycloneDX, SWID의 세 가지로 제한**하고 있다. 리눅스 재단의 SPDX는 Software Package Data Exchange의 준말로, 오픈소스 라이선스 관리를 중심으로 컴포넌트 관련 정보를 교환할 수 있는 SBOM 표준이다. OWASP의 CycloneDX는 오픈소스 컴포넌트에 대한 취약점 식별, 라이선스 관리 등을 위해 개발된 보안 취약점 중심의 SBOM 표준이다. NIST의 SWID는 Software Identification의 준말로, 소프트웨어 수명 주기 전반에 걸쳐 소프트웨어 인벤토리 자동화 및 관리를 하기 위해 개발된 SBOM 표준이다.

*P1, P2, P3는 소프트웨어에 포함된 패키지를 의미함

[그림 2] SBOM 자동 생성 과정

예시로 SPDX는 SBOM Generator를 제공하여 SBOM을 자동 생성할 수 있게 한다. [그림 2]는 패키지 P1, P2, P3를 포함하고 있는 소프트웨어에 SBOM Generator를 사용했을 때 SBOM 파일이 생성되는 과정을 나타낸 것이다. SBOM Generator는 Composer, Maven, NPM, PIP 등의 패키지 매니저를 지원하며 입력된 소프트웨어가 어떤 하위 패키지를 포함하고 있는지 정보를 추출하여 이를 SBOM으로 만든다.

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: spdx-sbom-generator
DocumentNamespace: http://spdx.org/spdxpackages/spdx-sbom-generator--57918521-3212-4369-a8ed-3d681ec1d7a1
Creator: Tool: spdx-sbom-generator-XXXXX
Created: 2021-05-23 11:25:29.1672276 -0400 -04 m=+0.538283001

##### Package representing the Go distribution

PackageName: go
SPDXID: SPDXRef-Package-go
PackageVersion: v0.46.3
PackageSupplier: NOASSERTION
PackageDownloadLocation: pkg:golang/cloud.google.com/go@v0.46.3
FilesAnalyzed: false
PackageChecksum: TEST: SHA-1 224ffa55932c22cef869e85aa33e2ada43f0fb8d
PackageHomePage: pkg:golang/cloud.google.com/go@v0.46.3
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageLicenseComments: NOASSERTION
PackageComment: NOASSERTION

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-go
```

[그림 3] SPDX SBOM Generator 사용 결과 예시

[그림 3]은 SBOM Generator를 통해 생성된 SPDX 형식의 실제 SBOM 파일 예시이다. SPDX의

SBOM은 spdx와 json 형식으로 사용할 수 있다. 그림을 자세히 보면 사용된 SPDX의 버전, 라이선스, 포함된 패키지의 이름과 버전 등 자세한 정보가 담겨있다. SPDX 포맷은 문서 생성 정보, 패키지 정보, 파일 정보, 스니펫 정보, SPDX 외 라이선스 정보, (SPDX 문서 간) 관계 정보, 주석으로 이루어지는데, 이를 알려진 취약점을 발견하거나 라이선스를 관리하기 위해 활용할 수 있다.

다) 소프트웨어 테스트 관련

소프트웨어의 제품이 안전하다는 것을 검증하기 위해서는 소프트웨어 테스트가 불가결하다. 현재 사용되는 테스트 방법은 위협 모델링, 자동화 검사, 정적 및 동적 분석 등으로 다양하기 때문에 어느 정도의 테스트를 거쳐야 소프트웨어가 충분히 안전한지 판단하기가 어렵다. 이번 행정명령에서는 **소프트웨어 검증에 권장되는 최소 기준을 마련**하여 소프트웨어 생산자가 자체적인 검증 프로세스를 만들 수 있도록 돕고자 한다.

행정명령으로부터 60일 이내, NIST에서 소스 코드 테스트의 최저 기준에 대한 가이드라인을 공표하게 된다. 자발적인 가이드라인이기 때문에 의무적으로 준수할 필요는 없지만 추후 의무 사항이 될 가능성이 있으므로 미리 대비해두는 것이 좋을 것이다. 공표된 테스트 종류에는 위협 모델링, 자동화 검사, 코드 정적 분석, 동적 분석, 구성요소 검사, 버그 수정이 있다.

테스트 종류	설명
위협 모델링	시스템을 추상화하여 잠재적인 공격자와 그들의 목표 및 방법, 잠재적인 위협을 설계 단계에서 미리 발견하는 방법
자동화 검사	소프트웨어 테스트를 자동화하여 워크플로우나 이슈 추적 과정에 통합하는 방법
정적 분석	코드 스캐너를 사용하여 버그를 발견하거나 하드코딩된 비밀 정보가 있는지 검토하는 방법
동적 분석	블랙박스 테스팅을 하거나 퍼징, 웹앱 스캐너를 사용하는 등 프로그램이 실행되는 동안 분석하는 방법
구성요소 검사	소프트웨어에 포함된 라이브러리, 패키지 등에 존재하는 알려진 취약점을 탐지하는 방법
버그 수정	발견된 치명적인 버그를 최대한 빨리 수정하는 방법

위협 모델링이란 시스템을 분석하여 잠재적인 위협을 식별하는 것을 의미한다. 자동화 검사는 자동화된 검사를 지속적으로 수행하는 것이다. 정적 분석은 소스코드를 직접 분석하는 것이고, 동적 분석은 코드가 실행되는 환경에서 분석하는 것이다. 구성요소 검사는 소프트웨어에 포함된 라이브러리, 패키지, 서비스 등 컴포넌트가 가지고 있는 알려진 취약점을 검사하는 것이다. 버그 수정은 치명적인 버그를 최대

한 빨리 수정하는 것을 의미한다. 각 테스트의 세부 내용은 Appendix B를 통해 확인할 수 있다.

라) 가이드라인 및 지침 관련

행정명령 4절의 가장 핵심적인 산출물은 공급망 보안 강화를 위한 가이드라인과 실행 지침이다. 가이드라인은 4절의 요구사항들을 만족시킬 수 있게끔 만들어지고, 지침은 가이드라인을 기반으로 만들어진다. 지침에는 안전한 소프트웨어 개발 환경, 코드의 완전성을 확보하기 위한 자동화 도구 도입, SBOM 제공, 안전한 소프트웨어 개발 방법에 대한 적합성 증명 등 공급망 보안을 강화하기 위한 내용이 포함된다.

예비 가이드라인과 관련된 내용의 경우 NIST에서 개발 중인 SP 800-161 Rev. 1 (2nd Draft)의 Appendix F에 수록되었다. SP 800-161은 시스템과 조직을 위한 사이버보안 공급망 위험 관리 실행 지침에 대한 문서이다. SP 800-161 문서의 Appendix F의 내용을 보면 행정명령을 통해 나온 '주요 소프트웨어의 정의' 등 산출물들의 내용에 대한 정리와 그 내용이 SP 800-161과 어떻게 연결이 되어있는지 확인할 수 있다.

실행 지침의 경우 기존에 NIST에서 개발한 SSDF (Secure Software Development Framework)를 행정명령의 요구사항에 맞게 업데이트하는 것으로 대신한다. SSDF는 SDLC에 통합할 수 있는 고수준의 안전한 소프트웨어 개발 지침 모음으로 총 43개의 보안 조치로 구성되어 있다. 보안 조치는 조직에서 준비해야 하는 조치, 소프트웨어 보호를 위한 조치, 안전한 소프트웨어 생산을 위한 조치, 취약점 대응을 위한 조치의 네 종류로 구성되어 있다. 행정명령 내용을 반영한 SSDF 1.1 버전이 배포되었으며, 행정명령의 요구사항과의 연결은 SSDF 문서의 Appendix A에 수록되어있다.

제4장 우리나라의 대응방안

국내의 경우 2021년 2월 발표된 'K-사이버방역 추진전략'에서 공급망 보안을 강화하기 위한 정책을 제시한 바 있다. 해당 정책에 따르면 주요 SW업체에 단계별 보안진단 및 조치 지원, 중소 SW업체에 자가 보안 진단 도구 및 가이드 보급, 주요 SW서비스 기업에 개발환경 보안점검 지원 및 공급망 검증 체계 구축, 공급망 보안점검 기준 및 점검도구 개발이 이루어진다고 한다.

위 내용에 따라 올해 8월 과학기술정보통신부 주관으로 '소프트웨어 개발 보안 허브'가 개소된 바 있다. 중소기업에 소프트웨어 개발보안을 적용하여 공급망 공격을 예방하겠다는 것이다. 소프트웨어 개발 보안 활성화를 위해 보안약점 진단, 개발자 대상 교육 등의 사업이 추진된다. 아쉬운 점은 보안약점 진단이 정적분석에 한정되어 있고, **국내 개발보안이 시큐어코딩으로 한정**된 경우가 많다는 것이다.

[표 2] 미 사이버보안 행정명령과 K-사이버방역 추진전략 비교

사이버보안 행정명령	내용	K-사이버방역 추진전략
'주요 소프트웨어' 대상 보안 조치 지침 발행,	**보안 조치**	다중이용공공서비스 분야 주요 SW 업체 대상 단계별 보안진단·조치 지원
SBOM 최소 요소 공표	**SBOM**	해당 없음
소프트웨어 검증 최소 기준 공표	**소프트웨어 테스트**	중소 SW 업체 대상 자가 보안 진단 도구 및 가이드 보급
공급망 보안 강화를 위한 가이드라인 및 지침 발행	**가이드라인 및 지침**	융합산업 분야별 보안 가이드라인 및 표준 보안모델 마련

[표 2]를 보면 미 사이버보안 행정명령과 K-사이버방역 추진전략이 공급망 보안 문제에 접근하는 방식의 차이를 볼 수 있다. 행정명령은 공급망 보안에 필요한 부분을 체계적으로 문서화하여 기업에서 직접 적용할 수 있게끔 한다. K-사이버방역 추진전략은 정부기관의 개입을 통해 주요 SW업체나 중소 SW업체를 대상으로 보안 관련 지원을 한다. 즉 **행정명령이 기업의 근본적인 체질 개선을 통해 보안을 강화하려 한다면 K-사이버방역 추진전략은 대응 체계 강화를 통해 보안을 강화**하려 한다는 것이다.

행정명령을 통해 연방 정부에 납품되는 모든 소프트웨어와 그 컴포넌트의 보안에 요구사항이 생기는 만큼 국내 기업에 영향이 존재할 수밖에 없고, 현재 국내의 보안 정책만으로는 새롭게 만들어지는 국제적 보안 기준을 만족하기 어려운 것이 사실이다. 또한 공급망 보안은 최종 소프트웨어가 만들어지는 모든 과정에 대한 보안을 의미하기 때문에 국제적 요구사항에 직면했을 때 반영하기에는 시간이 부족할 수 있다. 따라서 행정명령에 따라 공표되는 **가이드라인, 지침 등을 잘 파악하여 미리 국제적 요구사항에 맞춰 준비하는 것이 필수적**이라고 볼 수 있다.

가) '주요 소프트웨어(critical software)' 관련

우선 서비스 중이거나 개발 중인 소프트웨어 제품이 **EO-주요 소프트웨어에 해당되는지 확인**해야 한다. 공표된 EO-주요 소프트웨어의 정의가 광범위한 종류의 소프트웨어를 포함하고 중요한 소프트웨어를 직접적으로 포함하고 있는 소프트웨어도 EO-주요 소프트웨어가 되는 만큼, 소프트웨어 제품이 EO-주요 소프트웨어에 해당될 가능성이 높다고 볼 수 있다. 만약 **제품이 EO-주요 소프트웨어에 해당된다면 EO-주요 소프트웨어를 위한 보안 조치를 제품에 적용**해야 한다.

NIST에서 제시한 EO-주요 소프트웨어의 예시에 의하면 인증 관련 소프트웨어, 운영체제, 브라우저, 보안 관련 소프트웨어, 네트워크 관련 소프트웨어 등이 EO-주요 소프트웨어에 해당될 수 있다. 물론 미국 정부에 납품하거나 납품하는 소프트웨어에 관련될 일이 없다면 이를 EO-주요 소프트웨어에 해당되지 않으므로 EO-주요 소프트웨어를 위한 보안 조치를 꼭 적용하지 않아도 된다.

나) SBOM 관련

그리고 SBOM을 도입해야 한다. SBOM은 알려진 취약점을 제거할 뿐 아니라 라이선스 리스크를 방지하는 데에도 도움이 된다. 안전한 소프트웨어 생태계 조성을 위해서도 SBOM은 필수적이다. SBOM의 최소 요소를 공표하면서 사용 가능한 SBOM의 데이터 형식이 **SPDX, CycloneDX, SWID tags의 세 가지**로 명시되었으므로 이 중 **하나를 채택하는 것으로부터 SBOM 생성 및 관리를 시작**할 수 있을 것이다.

다) 소프트웨어 테스트 관련

소프트웨어 제품을 적절히 테스트하는 것도 중요한 부분이다. 공표된 소프트웨어 테스트 최소 기준에서는 총 12가지 방식의 테스트 방식을 제안하고 있는데, 기업마다 보유한 보안 역량에 차이가 있으므로 모든 방법을 적용하기 어려울 수 있다. 그런 경우 **자동화 검사나 코드 스캐너, 구성요소 검사와 같이 비교적 적용하기 용이한 방법부터 단계적으로 적용**해보는 방식으로 접근할 수 있을 것이다. 참고로 최소 기준 가이드라인 문서를 보면 각 방법과 관련된 보충 자료가 있으므로 이를 참고해볼 수 있다.

라) 가이드라인 및 지침 관련

무엇보다도 공급망 보안 강화를 위한 **가이드라인과 실행 지침을 준수**해야 한다. NIST의 SSDF를우선적으로 적용할 수 있다. 개발 환경을 안전하게 만들어야 하고, 코드의 무결성 유지와 취약점 발견을 위한 자동화 도구를 도입해야 하며, SBOM을 제공해야 하고, 취약점 공개 프로그램에 참여해야 하는 등 행정명령의 여러 요구 사항들이 SSDF에 포함되었다. 문서에서 제안하고 있는 보안 조치가 43개 정도로 많기 때문에 **어떤 조치가 이미 적용되어 있는지, 어떤 조치부터 적용하면 좋을지 분석하여 단계적으로 적용**하는 것을 권한다.

제5장 결론

이번 사이버보안 행정명령이 여러 방면으로 많은 내용을 담고 있지만, 자세히 살펴보면 기존에 이미 존재하던 관행, 기준, 표준을 활용하여 재구성한 부분이 많다. 다만 기존에 **권장 사항 정도로 존재하던 개념들이 행정명령을 통해 필수적으로 요구되는 사항이 될 수 있다**는 점에서 의의가 있다고 볼 수 있다.

국내의 경우 이번 행정명령의 요구사항을 100% 만족하고 있는 기업은 많지 않을 것으로 예상이 되고 있는 상황이다. 미국에서 나온 행정명령이지만, 소프트웨어의 국경이 모호한 시대인 만큼 **국내 기업에도 영향**을 끼칠 것임은 자명한 일이다. 다행히 행정명령이 발령된 지 오래 되지 않았고, 아직 진행 중이기 때문에 지금부터 대비한다면 **대비할 시간은 충분**하다.

소프트웨어 제품의 구현에 집중하다 보면 보안에 소홀해지곤 한다. 당장 눈에 보이지 않는 위험에 대

한 지불을 꺼리는 것이다. 솔라윈즈 공급망 해킹 사건을 보면 알 수 있듯이 공급망 공격은 큰 파급력을 가지고 있다. 소프트웨어 제품에 있는 **작은 취약점이 돌이킬 수 없는 피해**를 낳을 수 있다는 것이다. 이번 행정명령이 국내에서도 **보안을 중요시하는 문화**가 자리잡는 계기가 될 수 있을 것으로 생각된다.

참고문헌

1. Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021). https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

2. NIST. (2021) Definition of Critical Software Under Executive Order (EO) 14028. https://www.nist.gov/document/white-paper-critical-software-enhancing-security-software-supply-chain

3. NIST. (2021) Security Measures for “EO-Critical Software” Use Under Executive Order (EO) 14028. https://www.nist.gov/document/security-measures-eo-critical-software-use-under-executive-order-eo-14028-pdf-version

4. The United States Department of Commerce. (2021) The Minimum Elements For a Software Bill of Materials (SBOM). https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

5. NIST. (2021) Guidelines on Minimum Standards for Developer Verification of Software. https://www.nist.gov/document/document-developer-verification-software

6. NIST. (2021) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-161r1-draft2

7. NIST. (2021) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. https://doi.org/10.6028/NIST.SP.800-218-draft

8. 과학기술정보통신부. (2021) K-사이버방역추진전략 발표. https://www.msit.go.kr/bbs/view.do?sCode=user&mPid=112&mId=113&bbsSeqNo=94&nttSeqNo=3179937

9. 과학기술정보통신부. (2021) 소프트웨어 개발보안 시대 활짝 열렸다. https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeqNo=3180584

10. 이희조, "오픈소스 SW 공급망 공격 대응기술 동향", 금융보안원-전자금융과 금융보안, Vol. 26, pp. 13, Nov. 23. 2021.

Appendix A

- 사이버보안 행정명령 4절 세부 항목

항	기간	책임	협력	내용
(a)	해당 없음	해당 없음	해당 없음	개요
(b)	30 일 이내	상무부-NIST	해당 없음	(e)에 맞는 기준, 도구 및 모범 사례 특정을 위한 의견 수집
(c)	180 일 이내	NIST	해당 없음	공급망 보안 강화를 위한 예비 가이드라인 공표
(d)	360 일 이내	NIST	해당 없음	(c)의 가이드라인의 검토, 보완 절차를 포함한 추가 가이드라인 공표
(e)	(c)로부터 90 일 이내	상무부-NIST	적절한 기관	공급망 보안 강화를 위한 실행 지침 발행 *지침에 포함될 기준 포함
(f)	60 일 이내	상무부	통신정보담당차관보, 미국통신정보국	SBOM 의 최소 요소 공표
(g)	45 일 이내	상무부-NIST	국방부-NSA, 국토안보부-CISA, OMB, 국가정보장실	'중요한 소프트웨어'의 정의 공표
(h)	(g)로부터 30 일 이내	국토안보부-CISA	상무부-NIST	사용 중 혹은 발주 단계인 소프트웨어 중 '중요한 소프트웨어'에 해당되는 제품 목록 특정 후 각 부처에 제공
(i)	60 일 이내	상무부-NIST	국토안보부-CISA, OMB	'중요한 소프트웨어'의 보안조치에 대한 지침 발행
(j)	(i)로부터 30 일 이내	OMB-전자정부국	해당 없음	각 부처가 (i)의 지침을 준수하기 위한 조치
(k)	(e)로부터 30 일 이내	OMB-전자정부국	해당 없음	명령 이후 조달된 소프트웨어에 대해 각 부처가 (i)의 지침을 준수하도록 요구하기 위한 조치
(l)	(k) 이후	각 기관	해당 없음	(k)의 요구사항 준수 연장 요구
(m)	(k) 이후	각 기관	해당 없음	(k)의 요구사항 면제 요구
(n)	1 년 이내	국토안보부	국방부, 법무부, OMB, OMB-전자정부국	(g)~(k)의 요구사항을 소프트웨어 공급자가 준수하고, 준수하고 있음을

				설명하는 것을 요구하는 계약언어 FAR Council 에 권고
(o)	(n) 이후	FAR Council	해당 없음	(n)의 권고 검토 후 FAR 개정
(p)	(o) 이후	각 부처	해당 없음	(o)의 FAR 개정 이후, 개정된 FAR 을 만족하지 않는 소프트웨어를 계약에서 삭제
(q)		OMB-전자정부국	해당 없음	명령 이전에 개발 및 조달된 소프트웨어를 채용하고 있는 기관에 (k)의 요구사항을 준수할 것을 요구
(r)	60 일 이내	상무부-NIST	국방부-NSA	소프트웨어 소스 코드 테스트의 최저 기준에 대한 가이드라인 공표
(s)		상무부-NIST	적절한 기관	기존 소비자용 제품의 라벨링 프로그램을 참고하여 대중에게 IoT 기기와 소프트웨어 개발 관행에 대한 보안을 교육하기 위한 파일럿 프로그램 개시
(t)	270 일 이내	상무부-NIST	연방거래위원회, 적절한 기관	소비자용 라벨링 프로그램을 위한 IoT 사이버보안 기준 특정
(u)	270 일 이내	상무부-NIST	연방거래위원회, 적절한 기관	안전한 소프트웨어 개발 관행이나 소비자용 라벨링 프로그램의 기준 특정
(v)	해당 없음	해당 없음	해당 없음	파일럿 프로그램은 OMB Circular A-119 및 NIST Special Publication 2000-02 에 준거해야 함
(w)	1 년 이내	NIST	해당 없음	파일럿 프로그램 검토 및 유효성 평가, 개선 방안 도출하여 APNSA 에 보고
(x)	1 년 이내	상무부	적절한 기관	진척 상황 검토 및 추가 조치를 설명한 보고서를 대통령에게 제출

Appendix B

- Recommended Minimum Standard for Vendor or Developer Verification of Code The following are recommended minimums for verification of code by developers.

Technique Class	Technique	Description & Reference to Recommended Minimums Document
Threat modeling	Threat modeling helps identify key or potentially overlooked testing targets.	Section 2.1. Threat modeling methods create an abstraction of the system, profiles of potential attackers and their goals and methods, and a catalog of potential threats. Threat modeling can identify design-level security issues and help focus verification.
Automated testing	As testing is automated, it can be repeated often, for instance upon every commit or before an issue is retired.	Section 2.2. Automated testing can run tests consistently, check results accurately, and minimize the need for human effort and expertise. Automated testing can be integrated into the existing workflow or issue tracking system.
Code-based (static) analysis	Use a code scanner to look for top bugs.	Section 2.3. Static analysis tools can check code for many kinds of vulnerabilities and for compliance with the organization's coding standards. For multi-threaded or parallel processing software, use a scanner capable of detecting race conditions.
	Review for hardcoded secrets.	Section 2.4. Heuristic tools can be somewhat effective checking for hardcoded passwords and private encryption keys since functions or services taking these as parameters have specific interfaces.
Dynamic analysis (i.e., run the program on test cases)	Run with built-in checks and protections.	Section 2.5. Programming languages, both compiled and interpreted, provide many built-in checks and protections.
	Create "black box" test cases.	Section 2.6. "Black box" tests can address functional specifications or requirements, negative tests (invalid inputs and testing what the software should not do), denial of service and overload attempts, input boundary analysis, and input combinations.
	Create code-based structural test cases.	Section 2.7. Code-based, or structural, test cases are based on the implementation, that is, the specifics of the code. Code-based test cases may also come from coverage metrics.
	Use test cases created to catch previous bugs.	Section 2.8. Test cases which have been created to specifically show the presence (and later, the absence) of a bug can be used to identify issues in the absence of more general "first principles" assurance approaches for detecting bugs.
	Run a fuzzer.	Section 2.9. Fuzzers can try an immense

		number of inputs with minimal human supervision. The tools can be programmed with inputs that often reveal bugs, such as very long or empty inputs and special characters.
	If the software might be connected to the Internet, run a web app scanner.	Section 2.10. If there is a network interface, use a dynamic security testing tool (e.g., web application scanner) to detect vulnerabilities.
Check included software	Use similar techniques to gain assurance that included libraries, packages, services, etc. are no less secure than your code.	Section 2.11. Use the verification techniques recommended in this section to gain assurance that included code is at least as secure as code developed locally. The components of your software must be continually monitored against databases of known vulnerabilities; a new vulnerability in existing code may be reported at any time.
Fix bugs	Fix critical bugs that are uncovered.	Correct critical bugs as soon as possible and make process improvements necessary to prevent such bugs in the future, or to at least catch them earlier in the development process.

정보시스템의 상시 모니터링을 위한 SCAP과 도구에 대한 소개

안효범 (hbahn@kongju.ac.kr)

공주대학교 인공지능학부 교수

정보시스템에 대한 상시 모니터링을 통해 보안체계를 유지하는 것은 중요한 정보보호 활동 중에 하나의 작업이다. 상시 모니터링을 통해, 정보시스템에 대한 취약점을 발견할 수 있고 빠르게 대처할 수 있는 정보보호체계를 구성할 수 있게 된다. 그러나, 대부분의 기업들은 침입을 방어하는 입장에서 정보보호체계를 유지하려는 특성을 가진다. 즉, 사고가 발생했을 때, 정보보호를 위한 대응체계를 가동하게 된다. 적극적인 정보보호 활동을 수행하기 위해서는 상시 모니터링을 할 수 있는 표준이 필요하며, 이를 위한 도구가 필요한데, 이 논고에서는 상시모니터링을 위한 표준으로 제시되고 있는 SCAP(Security Content Automation Protocol)에 대한 구성을 알아보고, 검증에 사용될 수 있는 도구들에 대하여 소개한다.

1. 보안 표준화 및 자동화 동향

보안 자동화(security automation)는 특정 공통 보안 기능을 수행하기 위해 표준화된 규격 및 프로토

콜을 사용하는 것으로 취약성 평가 소프트웨어를 예로 들 수 있다. 취약성 평가 소프트웨어는 각 정보시스템에 대해 검사를 수행하여 패치되지 않거나 잘못된 보안 구성 설정(운영체제와 설치된 소프트웨어의 환경설정파일)여부와 같은 일련의 취약성을 확인한다. 보안 자동화 기술은 자산 관리(asset management), 구성 관리(configuration management), 취약점 관리(vulnerability management)가 상호 작용하면서 시스템을 효과적으로 관리하고 모니터링 할 수 있다.

각 보안 자동화 기술 구성요소는 개별적으로 사용할 때 유용하지만 취약점을 검증과 보고를 하기 위한 여러 표준을 함께 사용하면 큰 이점을 갖게 된다. 많은 기업과 벤더는 이러한 표준을 결합하고 구성요소가 함께 작동할 수 있도록 하는 방법을 보안 자동화 프로토콜(security automation protocol)로 정의해 왔다. 하나의 표준은 여러 프로토콜에서 사용되며 각 프로토콜은 특정 목적을 위해 구성요소들이 함께 사용되는 방법을 정의함으로써 구성요소 표준을 기반으로 한다. 보안 자동화 프로토콜 중 가장 잘 알려진 것은 SCAP이다. SCAP은 현재 버전이 1.3까지 NIST SP-800-125 Revision3에서 정의하고 있다.

2. SCAP의 구성 및 구조

SCAP은 컴포넌트 명세(component specification)들의 다중-목적 프레임워크이다. 컴포넌트 명세는 자동화된 환경설정, 취약점 그리고 패치 검사, 보안성 측정(security measurement) 그리고 기술적 제어를 위한 내부통제(compliance) 활동들을 지원한다[10]. SCAP 1.3은 5가지의 범주에 대하여 20개의 컴포넌트로 구성되어 있다. [표 1]은 SCAP의 5가지의 범주에 대하여 요약을 하였다.

언어 범주에서는 SCAP에서 사용되는 표준 어휘들과 보안 정책을 표현하기 위한 규칙들, 기술적 검사 메카니즘 그리고 수행된 결과들을 제공한다. 보고 형식 같은 경우에는 표준화된 형식으로 수집된 정보를 표현하기 위한 필수적인 구조를 제공한다. 식별 체계에서는 표준 식별 형식을 사용하여 소프트웨어 제품, 취약점 그리고 환경설정 아이템들 같은 주요 개념들을 식별하기 위한 방법들을 제공한다. 측정과 스코어링 시스템에서는 보안 약점(예를 들면, 소프트웨어 취약점과 보안 환경설정 이슈들) 중의 특정 특성들을 평가하기 위하여 참조된다. 무결성에서는 SCAP의 내용들과 결과의 무결성을 보존하기 위하여 사용된다.

10) D. Waltermire, S. Quinn, H. Booth, K. Scarfone, and D. Prisaca, “The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3,” NIST Special Publication 800-126. Revision 3, National Institute of Standards and Technology, February 2018.

[표 1] SCAP 버전 1.3의 5가지의 범주와 포함된 구성요소

카테고리	구성요소	설명
언어 (language)	XCCDF (Extensible Configuration Checklist Description Format)	보안 체크리스트/벤치마크 작성 및 평가 결과 보고용 언어로, 보안 검증 항목에 관한 내용을 작성하는 데 사용되며 검증 이후 해당 검증 결과를 표현하는 언어
	OVAL (Open Vulnerability and Assessment Language)	시스템 구성 정보 표현, 시스템 상태 평가 및 평가 결과 보고를 위한 언어로, XML 형식으로 구성
	OCIL (Open Checklist Interactive Language)	다른 데이터 수집 노력으로 만들어진 기존의 데이터 저장소 또는 사용자로부터 정보를 수집한 데이터를 나타내는 언어
보고 형식 (reporting format)	ARF (Asset Reporting Format)	자산(asset)에 대한 정보의 전송 형식 및 자산과 보고서 간의 관계를 표현하기 위한 형식
	AI (Asset Identification)	자산(asset)에 대한 알려진 식별자 및 알려진 정보를 기반으로 자산을 고유하게 식별하기 위한 형식
식별 체계 (identification scheme)	CPE (Common Platform Enumeration)	하드웨어, 운영 체제, 애플리케이션의 명명 및 사전으로, SCAP에서는 해당 플랫폼이 무엇인지에 대한 명시를 위해 CPE 이용
	CCE (Common Configuration Enumeration)	보안 관련 소프트웨어 결함의 명명 및 사전으로, SCAP에서는 보안 관련 시스템 설정 항목을 확인하기 위해 CCE 이용
	CVE (Common Vulnerabilities and Exposures)	소프트웨어 보안 구성의 명명 및 사전으로, 제품의 취약점에 대해 고유 식별 번호 'CVE 식별 번호'를 부여함으로써 정보 간의 상호 참조 및 연결에 CVE 사용
	SWID (Software Identification)	소프트웨어 식별자 및 관련 메타데이터를 나타내기 위한 형식
측정 및 채점 시스템 (measurement and scoring system)	CVSS (Common Vulnerability Scoring System)	소프트웨어 결함 취약성의 상대적 심각도를 측정하기 위한 시스템
	CCSS (Common Configuration Scoring System)	시스템 보안 구성 문제의 상대적 심각도를 측정하기 위한 시스템
무결성 (integrity)	TMSAD (Trust Model for Security Automation Data)	다른 보안 자동화 규격에 적용되는 공통 신뢰 모델에서 디지털 서명을 사용하기 위한 규격

SCAP은 보안취약점에 대한 점검을 수행하고 평가하기 위한 일관된 방법을 제공하기 위해

열거(enumeration), 언어(language), 위험측정(risk measurement)의 세 가지 종류의 자동화 표준을 사용한다[11].

가) 열거 표준 (Enumeration Standards)

보안 열거(enumeration) 표준은 보안 자동화 요소에 대한 명명법이며 해당 명명법을 사용하여 표현된 항목의 사전도 제공한다. 가장 널리 사용되는 보안 열거 표준은 CVE(Common Vulnerabilities and Exposures)로, 공개적으로 발표된 소프트웨어 취약성에 대한 고유 식별자를 제공한다. CVE는 식별자는 취약점 스캐너 및 침입 탐지 시스템 등에서 취약점을 참조할 때 사용되며 소프트웨어 판매 회사들은 제품의 새로운 취약점에 대한 권고 사항을 발행할 때 CVE 식별자를 포함한다. CVE와 유사한 열거 표준으로 CCE(Common Configuration Enumeration)와 CPE(Common Platform Enumeration)가 있다. CCE는 특정 운영체제의 개별 구성 설정과 같은 소프트웨어 보안 구성 문제에 대한 고유 식별자를 제공하며, CPE는 하드웨어, 운영체제 및 응용 프로그램 버전에 대한 고유 식별자를 제공한다.

나) 언어 표준 (Language Standards)

보안 언어 표준은 보안 정책, 보안 검사 목록(checklist), 개별 보안 항목에 대한 검사를 수행하는 메커니즘과 같은 보안 정보를 표현하기 위해 표준화된 어휘 및 규칙을 제공한다. 앞서 소개한 열거 표준을 통해 검사할 항목을 지정할 수 있는 경우, 언어는 일련의 검사를 프로파일에 제시하거나 해당 검사를 수행하는 데 사용된 기술적 메커니즘에 대해 제품에 규정함으로써 검사 방법을 자세히 설명한다.

(1) 체크리스트 언어 표준

체크리스트 언어 표준은 체크리스트 작성 및 실행에 사용되며 대표적으로 XCCDF(Extensible Configuration CHecklist Description Format)가 있다. XCCDF는 가장 많이 사용되는 보안 체크리스트 언어지만 보안 목적이 아닌 체크리스트 작성 및 실행에도 사용될 수 있을 만큼 유연하다.

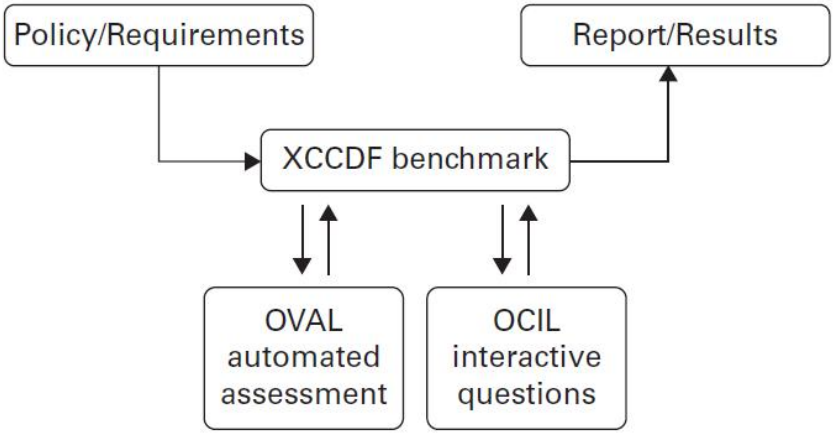
(2) 검사 언어 표준

검사를 위한 언어 표준은 보안 설정 확인, 알려진 취약점 검색, 패치 여부 확인, 컴퓨터에서 기타 정보 수집과 같은 보안 검사를 수행하기 위해 설계되었으며 대표적으로 OVAL(Open Vulnerability and Assessment Language)이 있다. OVAL은 개별 보안 검사와 검사 결과 보고 시 사용된다. 개별 OVAL 검사를 직접 평가할 수도 있지만, 전체 검사 목록을 단일 XCCDF 체크 리스트로 컴파일하고 XCCDF가 필요한 OVAL 테스트를 호출하도록 하는 것도 가능하다.

OCIL(Open Checklist Interactive Language)은 OVAL을 보완하기 위해 추가로 만들어진 보안 언어 표준이다. 다른 자료수집 작업을 통해 사용자나 기존 데이터 저장소로부터 정보를 수집하는 검사를 나타

11) S. Radack, "Security Content Automation Protocol (SCAP): Helping Organizations Maintain and Verify the Security Of Their Information Systems", ITL Bulletin, September 2010.

내는 언어로 설문 형식의 보안 평가를 수행할 수 있는 언어다. 예를 들어 OCIL을 사용하여 사용자에게 보안 관련 질문을 할 수 있다. OVAL과 마찬가지로 OCIL 설문지도 개별적으로 호출하거나 XCCDF 체크리스트로 호출할 수 있다. 단일 XCCDF 체크 리스트는 OCIL 설문지와 OVAL 검사 및 기타 검사 언어 표준을 모두 호출할 수 있으며, 모든 검사 결과를 포함하는 단일 보고서를 작성할 수 있다. [그림 1]과 같이 XCCDF는 OVAL 및 OCIL과 연계하여 필요한 검사를 수행하고 검사 결과를 반환한다.



[그림 1] XCCDF, OVAL, OCIL의 상호 작용

(3) 이벤트 언어 표준

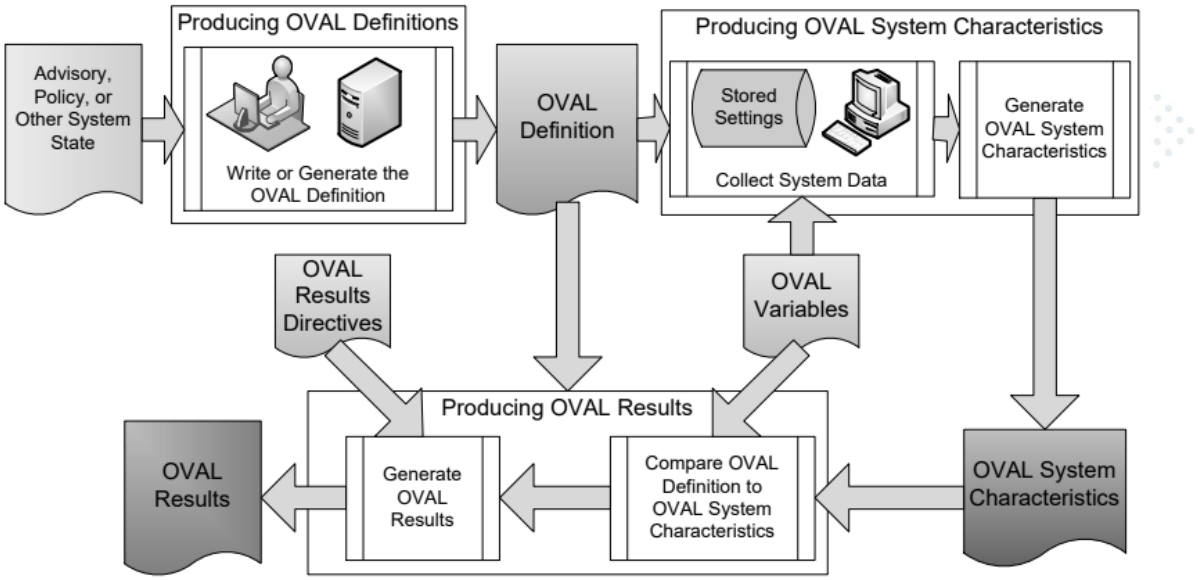
이벤트 언어 표준은 보안 이벤트를 포함하여 컴퓨터 이벤트의 특성을 문서화하는 데 사용되며, 특히 로그 파일에서 표준화된 형식으로 표현될 수 있다. 관련 이벤트 언어 표준으로 이벤트 필드 사전을 포함하는 CEE(Common Event Expression)가 있다. CEE는 주목할 만한 이벤트가 발생했다고 보고하는 공통 언어를 제공하고 이벤트를 알아야 하는 사람들, 공유하는 방법을 정의하고, 수신 시스템이 이벤트를 해석하는 방법을 설명한다. 이를 통해 보안 자동화 커뮤니티가 효과적으로 정보를 공유할 수 있도록 돕는다.

(4) 자산 언어 표준

자산 언어 표준은 컴퓨터, 네트워크, 소프트웨어 및 하드웨어를 포함한 다양한 자산(asset)과 관련된 정보를 문서화하기 위한 프레임워크를 제공한다. 자산 식별(Asset Identification, AI) 표준을 사용하면 표준화된 표현을 사용하여 자산을 고유하게 식별할 수 있다. AI의 보완적 표준인 자산 보고 형식(Asset Reporting Format, ARF)은 표준화된 보고 형식과 자산에 대한 정보를 한 컴퓨터에서 다른 컴퓨터로 전송할 수 있는 방식으로 표현하는 방법을 정의한다. 이를 통해 보안 정보를 포함한 자산에 대한 정보를 보고할 수 있다.

3. 보안 평가를 위한 OVAL에 대하여

OVAL(Open Vulnerability and Assessment Language)은 컴퓨터 시스템의 상태를 평가하고, 취약점을 보고하는 과정을 표준화하기 위하여 생성된 국제 정보보안 커뮤니티 표준으로, 시스템 관리자가 로컬 시스템상에서 시스템이 가지고 있는 특성 및 설정 정보들을 기반으로 취약점을 찾아내고, 평가하는 과정을 거칠 수 있도록 한다. OVAL 언어는 시스템의 설정 정보를 수집하여 보안 정책을 준수하는지 테스트한 뒤 결과를 XCCDF 컴포넌트로 넘기는 등 실질적으로 시스템을 평가하는 과정에 쓰이는 언어이며, 그러한 점에서 SCAP 컴포넌트들 중 가장 중요한 역할을 하는 컴포넌트로 결론 지을 수 있다.



[그림 2] OVAL 언어 작동 과정

OVAL을 이용하여 시스템을 평가하는 프로세스는 그림 36에서 나타나듯 크게 세 단계로 구분된다. 평가하고자 하는 시스템의 설정 파일과 경로를 확인한 뒤, 수집하고자 하는 객체와 해당 객체의 상태를 OVAL 코드로 작성한다. 보안 스캐너 내에서 작성된 OVAL 코드를 이용하여 객체를 수집하고, 수집된 객체의 존재 여부나 상태를 이용하여 평가를 수행한다. 평가된 결과는 보안 스캐너에 의해 기본적으로 OVAL Results라는 XML 파일로 작성되며, 해당 결과를 XCCDF 컴포넌트에 넘겨 테스트 결과를 최종적으로 보고하여 시각적으로 리포트를 표현하는 과정을 거친다.

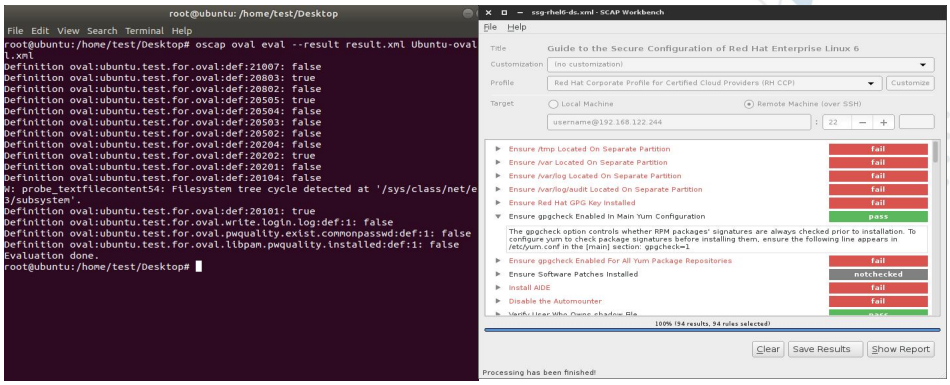
4. SCAP을 이용하는 보안 모니터링 도구 및 모듈[12)]

시스템이 알려진 위협 및 취약점에 대응하는 것은 필수적이고 지속적인 프로세스이며, 대응하기 위한

12) https://csrc.nist.gov/Projects/scap-validation-program/validated-products-and-modules

보안 정책을 마련하고, SCAP을 이용하여 시스템 구성요소를 점검하는 모니터링 과정이 필요하다. 이에 SCAP 보안 프로토콜의 사양을 기반으로 한 보안 자동화 모니터링 도구들이 출시되었으며, 도구들은 작성된 SCAP 문서를 기반으로 취약점 및 시스템 객체를 식별하고, 시스템의 보안 정책 준수 여부를 평가 및 보고한다.

가. OpenSCAP



[그림 3] OpenSCAP을 이용하여 테스트하는 모습

OpenSCAP은 Redhat 사에서 주도하여 개발되고 있으며, SCAP 프로토콜 사양을 이용하여 시스템을 감사하기 위한 보안 스캐너로서 개발되고 있는 오픈소스 프로젝트이다[13]. OpenSCAP에서 지원하는 OSCAP 프로그램은 대표적인 보안 스캐너로 시스템의 보안 구성 설정을 확인하고, SCAP 표준 및 사양을 기반으로 하는 규칙을 사용하여 시스템의 손상 징후를 검사할 수 있다. 기본적으로 XCCDF, OVAL와 같은 SCAP 컴포넌트들을 결합한 벤치마크 문서를 바탕으로 시스템의 보안 정책 준수 여부를 평가하며, OVAL 인터프리터(Interpreter)의 역할 또한 수행한다. OpenSCAP 도구는 크게 네 가지의 도구로 나뉘어 지원한다.

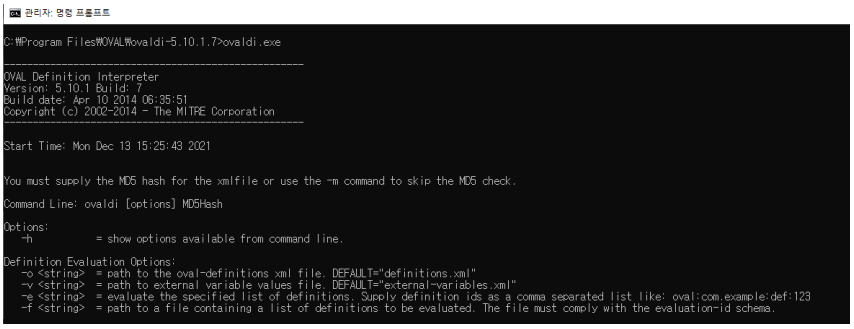
- **OpenSCAP Base** : OpenSCAP Base는 SCAP을 이용하여 시스템의 구성 및 취약성 스캔을 수행하는 커멘드라인 도구(OSCAP)이다. SCAP 표준 XML 스키마에 따라 SCAP 컨텐츠를 검증하며, 이를 바탕으로 시스템 평가를 수행한다.
- **OpenSCAP Deamon** : 백그라운드에서 실행되는 데몬 서비스이며, 지정된 일정에 따라 기계와 컨테이너를 평가한다. 특정 정책에 대해 시스템을 지속적으로 평가하거나 혹은 일회성 평가를 할 수 있다.
- **OpenSCAP WorkBench** : OpenSCAP Base보다 기능이 제한적이나, 그래픽으로 제공되는 유틸리티이므로 쉽게 시스템을 평가할 수 있다.
- **OSCAP-SSH** : 네트워크를 통해 원격 컴퓨터를 스캔하고, 결과를 수집할 수 있다.

OpenSCAP 제품군은 기본적으로 로컬 시스템상에서만 시스템을 스캔하고 평가하므로 해당 플랫폼

13) OpenSCAP User Manual, https://github.com/OpenSCAP/openscap/blob/maint-1.3/docs/manual/manual.adoc

에 대한 OpenSCAP 빌드가 필요하며, OSCAP-SSH도 원격 시스템에 설치되어 있어야 하므로 OpenSCAP 내에서 평가 가능한 플랫폼이 유닉스, 리눅스 및 윈도우로 한정되는 한계점을 가진다. NIST에서 인증받은 오픈소스 프로젝트이므로 기존 OVAL 사양에 없는 새로운 테스트 추가 및 다양한 플랫폼 확장 작업이 이뤄지고 있어 현존하는 SCAP 보안 모니터링 도구 중에서 가장 발전 가능성이 큰 도구이다[14]. 또한, OpenSCAP은 C언어로 작성되어 스캔 속도가 타 제품군과 비교하여 빠른 장점을 지니고 있다. 평가 결과의 경우, XML 파일 또는 HTML 보고서로 출력하여 시스템의 전반적인 평가 결과를 확인할 수 있다.

나. OVAL Interpreter (ovaldi)



[그림 4] OVAL 인터프리터의 옵션을 확인하는 모습

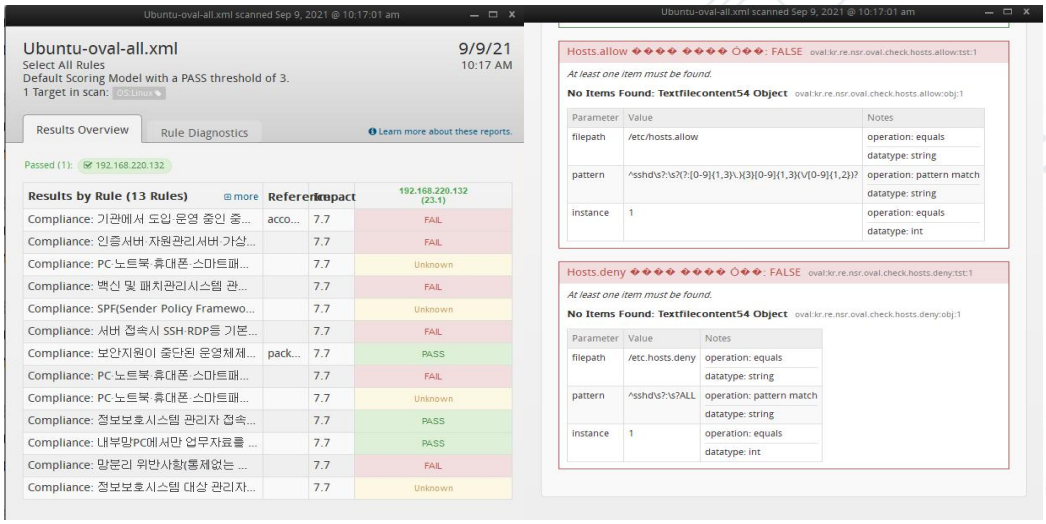
OVAL 인터프리터(ovaldi)는 MITRE 사에서 개발한 프로그램으로 OVAL 커뮤니티에 OVAL 언어의 오픈소스 레퍼런스 구현을 제공하기 위해 개발된 프로젝트이며, OpenSCAP과 마찬가지로 로컬 시스템에서 보안 관련 구성 정보를 수집하고, 취약점 및 구성 문제에 대한 정보를 분석하여 분석 결과를 보고한다. 문제는 SCAP 컴포넌트 중에서 오직 OVAL만 지원하는데, OVAL 중에서도 개발 우선순위 지정으로 인해 필요에 따라 테스트에 대한 개발을 추진하여 모든 테스트를 지원하지 않는다[15]. 플랫폼 또한 윈도우즈 및 일부 유닉스에 크게 초점이 맞춰져 있어 그 외의 플랫폼에서의 평가가 불가하며, 오픈소스 프로젝트임에도 불구 2014년 이후 활발한 기능 추가 작업이 이뤄지고 있지 않다.

다. jOVAL : Continuous Monitoring

jOVAL 제품군은 Java 언어로 작성되었으며, SCAP 벤치마크 문서를 이용하여 플랫폼의 기기들을 원격으로 평가할 수 있는 다중 플랫폼 구성 컴플라이언스 스캐너이다. SCAP 컴포넌트들 중에서도 OVAL의 경우 최신 버전만 지원하는 대신 해당 OVAL 언어 버전에서 지원할 수 있는 모든 테스트를 이용할 수 있는 특징이 있으며, 타 도구들과 비교하여 원격 시스템에 jOVAL이 설치되어 있지 않아도 SSH

14) Add support for FreeBSD, derived from https://github.com/OpenSCAP/openscap/pull/1574
15) OVAL Community, “Supported tests”. https://sourceforge.net/p/ovaldi/wiki/Supported%20tests/

통신을 이용하여 모든 시스템 플랫폼에 대해 SCAP 평가를 원격으로 진행할 수 있는 장점이 있다.



[그림 5] jOVAL 프로그램을 이용하여 테스트한 결과

jOVAL Professional 제품의 경우 원격을 스캔하면 SCAP 평가결과가 '$scan_data' 디렉터리 내에 ARF(Asset Report Format) 리포트 형식으로 저장되며, ARF로 보고된 결과를 프로그램 내에 나타낸다. jOVAL 프로그램으로 HTML 리포트를 생성하지는 못하나, 대신 수집된 시스템 객체 및 평가결과를 프로그램 내의 평가결과 및 상세지표로 자세히 나타내어 평가의 근거를 쉽게 확인할 수 있다.

jOVAL 회사는 2011년 창업 이래 오픈소스를 상업화시킨 이후 SCAP의 문법 개정 및 jOVAL의 플랫폼 확장을 위해 노력해왔으나, 2021년 12월 Aritic Wolf 사에 편입되어 현재는 jOVAL의 상업적 구매 가능 여부를 알 수 없다.

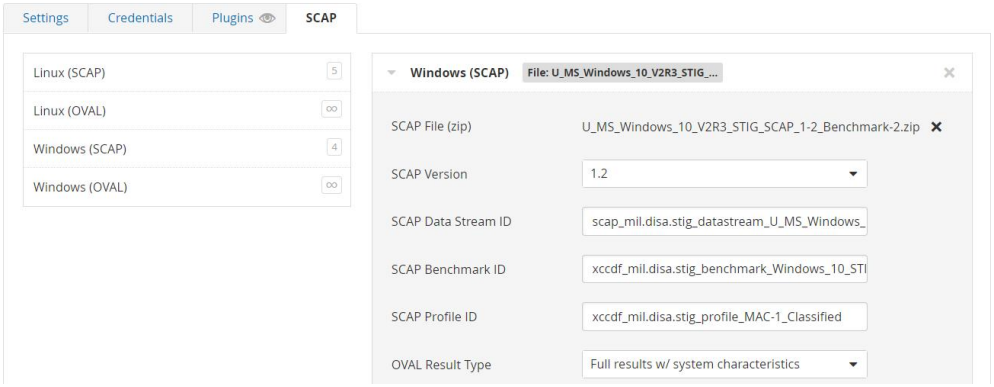
라. Nessus Professional

Nessus Professional은 SSH 통신을 통해 IT 네트워크 내 시스템들의 구성요소를 원격 스캔하고, 평가하는 웹 기반 보안 스캐너이다. SCAP 스캔을 비롯하여 멀웨어 스캔, 네트워크 스캔 등 미리 구성된 450개 이상의 시스템 스캔 템플릿(Templete)을 갖추고 있어 취약점 발생 지점을 다양한 스캔을 통해 파악할 수 있고, 취약점 정보를 플러그인(Plug-in) 형태로 저장되어, 플러그인을 가져다 사용함으로써 일부 취약점 평가를 신속하게 수행할 수 있는 특징을 지니고 있다[16].

SCAP 평가의 경우 'Advanced Scan' 또는 'SCAP and OVAL Auditing' 템플릿을 이용하여 할 수 있으며, SCAP 벤치마크 문서와 OVAL XML 문서 중 하나를 택하여 평가를 진행할 수 있다. 라이브 결과를 보여줄 수 있는 장점을 지니나 SCAP 버전의 경우 SCAP 1.0~1.2 버전까지만 지원하며, Ubuntu

16) Tensible, Nessus Professional Datasheet. https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/PDFs/Tenable/Tenable-Nessus-Professional-052421-Datasheet.pdf

커널과 같은 일부 리눅스는 해당 템플릿에서 평가를 진행할 수 없는 한계점이 존재한다. 또한, SCAP 또는 OVAL 파일을 이용하여 평가할 시 평가하고자 하는 파일을 zip 확장자로 압축하여 업로드해야 하며, SCAP 파일을 첨부했을 시 SCAP Data Stream ID, SCAP Benchmark ID, SCAP Profile ID를 일일이 지정해야 하는 불편함을 지닌다.



[그림 6] Nessus Professional를 이용하여 스캔을 진행하는 모습

정리한 SCAP 보안 모니터링 도구들의 특징을 총합하여 정리한, 대표적인 모니터링 도구들의 특장점 비교 현황을 [표 2]에 나타냈다.

[표 2] SCAP 보안 모니터링 도구들의 기능 비교표

	OpenSCAP	ovaldi	jOVAL	Nessus
SCAP 벤치마크 문서 평가 가능 여부	O	X	O	O
원격 평가 가능 여부	△ (로컬 시스템에 설치되어야 함)	X	O	O
스캔 속도	1~5초 이내	1~5초 이내	10~20초	30초 이상
다운로드 가능 여부	O	O	X	O
리포트 가능 포맷	XML, HTML	XML, HTML	ARF	.

그 외에도 SCC (SCAP Compliance Checker) , IBM BigFix Compliance, McAfee Policy Auditor 등이 있다.

5. 결어

운영체제 및 각 소프트웨어들은 유닉스나 리눅스 계열에서는 설정파일을 가지고 있고 윈도우즈에서는 레지스터리에 설정 정보들을 포함하게 된다. 이러한 설정 정보를 이용하여 운영체제나 소프트웨어들이 갖는 취약점(일반적으로 패치인 경우)을 파악할 수 있다. 이러한 취약점들은 NCP(National Checklist Program)[17]에 보고 되고 있으며, 각 목표 시스템에 따라 분류하여 XCCDF 또는 SCAP 1.3 content 형식으로 제공하고 있다. 국내에서도 SCAP과 같은 상시모니터링을 위한 체계를 갖도록 하는 연구가 필요하고 이를 통해 소프트웨어를 생산하는 기업은 취약점을 제공하고, 일반 기업에서는 정보시스템의 취약점을 모니터링할 수 있는 체계를 통해 상시 보안 취약점에 대한 적극적인 대책을 강구할 수 있도록 하는 제도적인 변화가 요구된다.

17) https://ncp.nist.gov/repository

개인정보 정책에서 증거기반(evidence-based)의 규제의 필요성

이진규 (lee.david@navercorp.com)

네이버주식회사 개인정보보호책임자 (이사)

들어가며

[사례 1] 개인정보위원회 및 보험업계에 따르면 올해 7월 말 기준 개인정보 손해배상책임보험에 가입한 사업자는 8,435곳이다. 제도 도입 당시 방송통신위원회가 대상사업자 규모를 18만3,300사로 추정했던 점을 감안하면 가입률이 5%에도 미치지 못한다. 보험상품이 나온지 2년 가량 되었으나 보험금 지급 사례가 전무(全無)하다.[18)]

[사례 2] 금융데이터거래소의 출범 1년 즈음에 확인한 누적 거래량은 2,100여 건, 유료거래는 약 90건(총 12억원, 전체 거래 대비 4% 수준)으로 확인된다.[19)] 금융데이터 거래소는 '20년 5월 출범 당시 '데이터 3법 시행 시점인 20년 8월 이후가 터닝포인트가 될 것이다.'라고 예상했으나, 등록된 데이터와

18) 대한금융신문, "의무보험인데 가입자 파악도 못하는 '개인정보보험'", 2021. 11. 25., URL: http://www.kbanker.co.kr/news/articleView.html?idxno=201755

19) 아이뉴스24, "[리딩금융인] 임구락 데이터혁신센터장 "데이터 거래시장, 올해가 변곡점"", 2021. 5. 11., URL: https://www.inews24.com/view/1365763

유료 수요는 기대와 달리 초라한 수준이다.[20]

[사례 3] 정부는 QR코드 기반의 '방역패스'를 올해 12월에 전격 시행했으나, 접속량 예측에 실패하여 서버 운영에 문제점을 드러내며 '먹통 사태'에 대한 비난을 받아야 했다. 시행 둘째날인 12월 14일 점심 시간대엔 약 150만건의 QR코드 예방접종 검증이 이뤄졌는데, 이는 7일 같은 시간대(약 46만건)의 사용량을 3배 이상 상회하는 수준이었다.[21]

[사례 4] 공정거래위원회는 전자상거래법 개정을 통해 온라인 사업자가 맞춤 광고를 하는 경우 그 내용과 방법을 사전에 소비자에게 고지하고 맞춤 광고 수신 여부를 개별 소비자가 선택할 수 있도록 하겠다 밝혔다. 그런데, 이로 인한 광고 매출 감소 효과는 총 1~2조에 달하는 것으로 추정되고, 이로 인해 중소상공인의 틈새시장 확보가 어려워져 대규모 사회적 손실(롱테일 경제 타격)이 예상된다는 주장이 제기되었다. 맞춤 광고에 대한 실태 조사를 통해 데이터를 확보·분석해 개인정보 활용 및 보호에 대한 경제성 분석 연구를 추진 필요성이 제기되지만 정부는 여전히 법 개정을 추진할 것으로 알려지고 있다.[22]

상기 [사례 1~3]은 정책적 실패 또는 준비 미흡으로 평가받는 사안인데, 한 가지 공통점이 있다. 정부가 사전에 데이터 증거를 기반으로 정책을 수립하는 경우 발생을 피할 수 있었던 정책이라는 점이다. [사례 4]는 규제의 영향을 받는 시장이 '정책에 관련된 데이터를 모아 증거 기반으로 접근하면, 당면한 문제를 보다 합리적으로 해결할 수 있다.'라는 주장을 내세우고 있는 것으로, 향후 규제당국의 대응이 주목되는 사안이다.

해외, 특히 유럽연합이나 미국에서 특정 규제에 관한 논의가 '개시'되면 국내에선 벌써 법제화가 진행되는 경우가 다수 있다. 특히, 개인정보에 관한 규제는 전 세계의 "가장 강한 규제의 합집합"을 가장 빠르게 만들어낸 것으로 평가받고 있기도 하다. 현재 국회에 제출된, 정부가 발의한 개인정보보호법 개정안은 기존의 규제가 모자랐던 듯, 유럽연합 GDPR에 있는 규제를 추가로 받아들이는 동시에 기존의 규제를 더욱 강화하는 조치를 반영한 법조항을 다수 포함하고 있다(예: 전체 매출액 기반의 과징금, 개인정보분쟁조정위원회의 조사권 확보 등). 그런데, 이와 같은 신규 정책들이 법제에 반영될 때, 국내의 환경과 데이터 처리 맥락을 충분히 고려하여 도입되는 것인지는 명확하지 않다. 특히, 데이터를 중심으로 하는 증거 기반(evidence-based)의 논거가 제시되어 검토되고 있는지는 좀처럼 확인이 되지 않는다. 해외의 사례나, 규제 추가(강화)의 당위만 반복적으로 제시되고 있는 것이다.

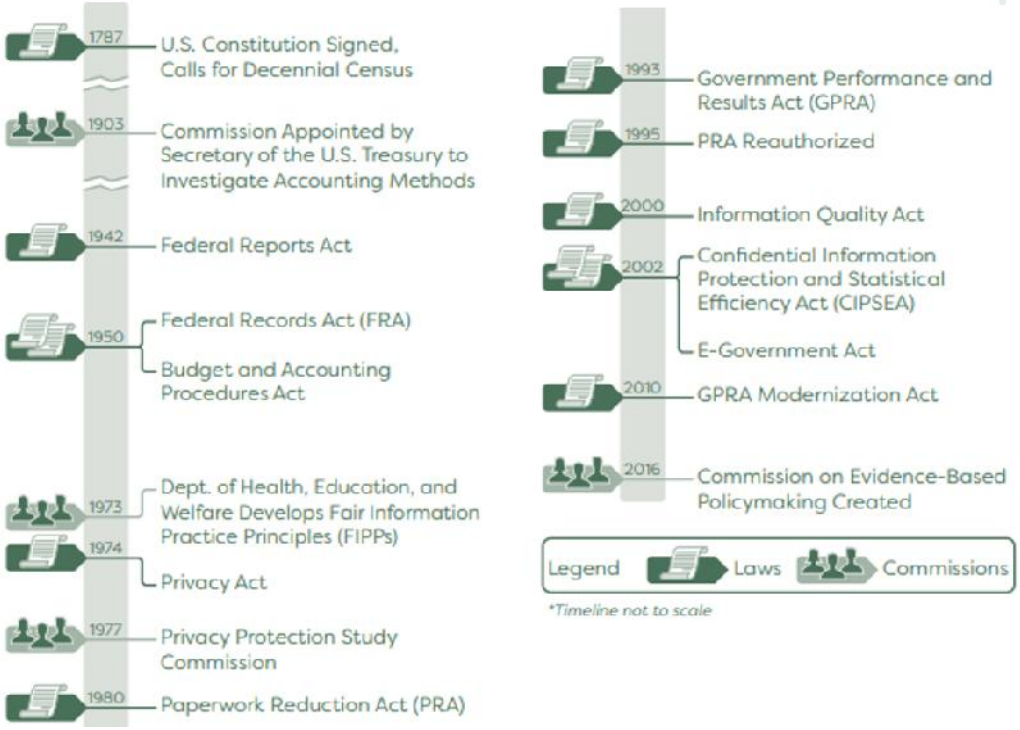
이 글은 개인정보 관련 규제를 도입할 때, 증거기반 정책수립의 필요성에 대해 화두를 던지고자 하는 목적으로 작성되었다.

---

20) BIKorea, "<초점>금융데이터 거래소 출범 3개월 성과를 보면…", 2020. 8. 11.,
URL: http://www.bikorea.net/news/articleView.html?idxno=27619
21) 경향신문, "접속량 예측 실패에 "서버 운영 문제" 남 탓…불신 키운 정부", 2021. 12. 14.,
URL: https://www.khan.co.kr/national/health-welfare/article/202112142100005
22) 뉴스토마토, "(시론)맞춤 광고와 개인정보 보호", 2021. 12. 21.,
URL: http://www.newstomato.com/ReadNews.aspx?no=1094739

증거기반 정책수립을 위한 법률적 토대

미국에는 「증거기반 정책수립 기초법 2018(Foundations for Evidence-Based Policymaking Act of 2018)」 이라는 연방법이 있다. 이것은 〈증거기반 정책수립 위원회(U.S. Commission on Evidence-Based Policymaking(2017))〉가 제시한 여러 제언을 받아들여 법제화 한 것으로서, 1) 정책 생성을 위한 증거 및 데이터의 활용을 향상시키고, 2) 연방 평가 활동을 의무화하며 3) 연방 데이터 관리를 개선하는 것 등을 목적으로 한다. 총 5편 제44편으로 구성된 이 법률은 연방 기관이 정책을 수립할 때 고려해야 할 증거기반 접근방식에 대한 기반을 제공한다.[23]



[그림 1] 미국 내 증거 형성 시스템 주요 마일스톤[24] (출처: 증거기반 정책수립 위원회)

이 법률에 의하면 정부 기관은 매년 미국 관리예산실(OMB, Office of Management and Budget)과 의회(National Assembly)에 정책 질의를 식별하고 대응할 '체계적 계획서'를 제출해야 하는데, 계획서에는 다음의 내용이 반드시 포함되어야 한다.[25]

---

23) Library of Congress, "H.R.4174 - Foundations for Evidence-Based Policymaking Act of 2018", introduced on Oct. 31, 2017, URL: https://www.congress.gov/bill/115th-congress/house-bill/4174

24) 해당 마일스톤은 증거기반 정책수립 위원회가 대통령에게 제출한 'The Promise of Evidence-Based Policymaking' 보고서에 수록된 것(p. 13)을 편집하여 수록한 것이다. 해당 리포트는 다음 링크에서 확인할 수 있다.
보고서 내려 받기: https://bit.ly/3moXc0A

25) The CIO Council, "Foundations for Evidence-Based Policymaking Act of 2018", last visited on Dec. 20. 2021, URL: https://www.cio.gov/policies-and-priorities/evidence-based-policymaking/

- 정책수립을 지원할 증거 개발을 위한 질의 문항
- 정책수립에서 증거 사용을 촉진하기 위해 기관이 수집, 이용, 취득할 의향이 있는 데이터
- 정책수립을 지원할 증거 개발에 사용될 수 있는 방법론 및 분석적 접근법
- 정책수립을 지원할 증거 개발에 대한 도전적 과제

  (관련 정보에 접근함에 있어 도전이 되는 법적 또는 다른 유형의 제한을 포함)
- 증거 형성 활동을 조정하기 위한 고위직 평가 담당관(Evaluation Officer) 및 통계적 정책, 기술, 절차에 관한 조언을 제시할 수 있는 통계적 전문지식을 보유한 담당관의 지정

이 법률은 하위법령으로 「공공정부 데이터법(OPEN Government Data Act)」와 「비밀정보보호 및 통계효율법(confidential Information Protection and Statistical Efficiency Act of 2018)」를 두고 있는데, 전자는 대통령실 직속 예산관리실장으로 하여금 연방정부 지침에 따라 실행 가능한 범위의 전략적 정보자원 관리 계획을 수립 및 관리하도록 하는 내용을, 후자는 증거 구축 활동을 촉진하고 효율적 통계 활용을 위해 연방 정부의 비밀정보 접근 가이드를 수립하는 동시에 통계 거버넌스를 정비하는 내용을 담고 있다. 특히, 전자는 연방 정부가 보유하고 있는 데이터 자산을 파악하고 공개의 우선순위 평가를 거쳐 최종적으로 '연방 데이터 목록(Federal Data Catalogue)'을 대중에게 공개하도록 하고 있다.[26]

[그림 2] 증거기반 정책수립의 6대 행동 방식 (출처: Urban Institute)[27]

우리나라에선 「데이터기반행정 활성화에 관한 법률(이하 "데이터기반행정법")」이 지난 2020년 6월에 제정되었다. 우리 데이터기반행정법은 데이터기반행정에 관해 법으로 정한 사항을 심의·조정하기 위하

26) 한국정보화진흥원, "Global Open Data, Now[오픈데이터 해외주요동향, 2019 Vol. 12]",
URL: https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=27974&bcIdx=20968&parentSeq=20968
27) Urban Institute, "Improving Evidence-Based Policymaking: A Review", April 2021,
URL: https://www.urban.org/sites/default/files/publication/104159/improving-evidence-based-policymaking.pdf

여 행정안전부장관 소속으로 데이터기반행정 활성화 위원회를 두고(제5조), 행정안전부 장관으로 하여금 데이터기반행정 활성화를 위한 기본계획을 3년마다 수립하도록 하고 있다(제6조). 공공기관의 장은 해당 기관의 데이터기반행정 활성화에 관한 업무를 총괄하는 책임관을 임명해야 하며(제19조), 책임관은 데이터기반행정에 관한 업무를 담당한다. 또한, 공공기관의 장으로 하여금 공동활용의 필요가 있다고 인정하는 데이터를 '데이터통합관리 플랫폼'에 등록하도록 하며(제8조), 이외의 데이터에 대해서는 공공기관의 장이 타 기관에 요청, 제공할 수 있는 근거(제10조 내지 제13조)도 마련하고 있다. 공공기관의 장은 데이터기반행정 추진 현황, 데이터 연계·제공 및 공동활용 성과 등 데이터기반행정의 실태를 대통령령으로 정하는 바에 따라 자체적으로 점검하고, 그 결과를 행정안전부장관에게 제출해야 한다(제22조). 심지어, 우리나라 데이터기반행정법은 민간에서 생성, 취득하여 관리하는 데이터를 제공하여 줄 것을 요청할 수 있는 근거 규정(제14조)도 보유하고 있다.

데이터기반행정법에 의거하여, 정부는 올해 〈제1차 데이터기반행정 활성화 기본계획〉을 수립, 공개했는데, 해당 계획에선 ①데이터 통합관리기반 구축으로 데이터 공동활용 ②데이터기반 행정 활성화를 위한 제도 확립 ③지능형 서비스 제공을 위한 데이터 분석·지원 ④데이터기반의 일하는 방식으로 혁신 등의 추진 전략을 제시했다. 특히, 네번째 전략에 해당하는 데이터 기반의 일하는 방식과 관련하여, ▲정책의 수립·집행·평가 전 과정에 데이터 기반행정의 접목의 강화 ▲정부기관내 데이터기반행정 역량 강화 등의 세부 접근법을 제시하면서, 미국의 연방 데이터 전략을 벤치마킹하여 '데이터역량강화 가이드라인'을 마련, 배포할 예정이라 밝혔다.[28]

[그림 3] 데이터기반행정 비전 및 추진전략 (출처: 행정안전부)

그런데, 미국의 증거기반 정책수립 기초법과는 달리 우리 법은 데이터 목록을 대중에 공개하도록 하는 규정은 찾아볼 수 없다. 또한, 국회에 관련 정보를 정기적으로 제출하여야 하는 의무도 없다. 더군다나 데이터기반행정 활성화를 위한 기본계획은 매 3년마다 수립하고 있어 데이터 환경의 변화에 맞춘 신속하고 유연한 대응도 기대하기 어려운 것으로 평가된다. 법이 정하는 바에 따라 민간 데이터를 정부에 제

28) 행정안전부, "[보도자료] 데이터로 국민체감형 공공서비스 새롭게 설계한다. 「제1차 데이터기반행정 활성화 기본계획(2021~2023)」 확정발표", 2021. 2. 20.
URL: https://www.mois.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_00099440YjMv4Uf&fileSn=0

공하도록 요청할 수는 있으나, 민간 데이터의 절대 다수에 해당하는 개인정보에 대해서는 개인정보보호법에 따르도록 하고 있는 규정(제4조)에 따라, 이를 정부의 데이터기반행정에 활용할 수 있는 방법도 요원하다.

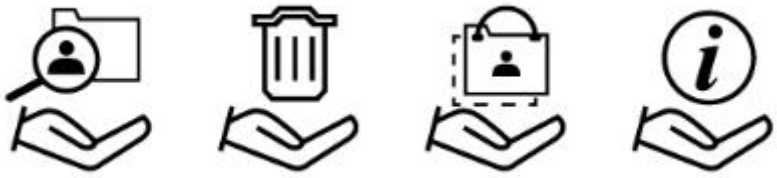
결국 법의 형식적 구성의 완성도 내지 미국 법제와의 유사성에 비하여 실질적 효과성이 매우 떨어질 수밖에 없는 내용으로 인해 이 법제가 의도한 기능을 제대로 할 수 있을 것인지에 대한 의구심이 제기될 수밖에 없다. 가장 문제가 되는 것은, 데이터기반행정을 활성화하기 위한 '인센티브 체계'가 거의 갖춰져 있지 않아서, 데이터기반 행정을 통한 증거기반 규제 마련에 나설 동인이 거의 없다는 점이다. 데이터기반 행정이 본격적으로 자리를 잡을 때 까진 더 많은 시간이 필요할 것으로 예상되는 까닭이 여기에 있다.

증거기반 규제의 필요성

데이터, 특히 개인정보와 관련하여 증거기반 규제가 필요한 지점은 매우 다양하게 존재한다. 예를 들면, 우리나라에는 해외에서 찾아보기 어려운 매우 지엽적인 '중요내용 강조표시' 규제가 존재하는데, 정보주체에게 동의를 받을 때, 법이 정한 일부 '중요한 내용'은 폰트의 크기, 색상, 형태(굵기) 등의 방식으로 강조하여 표시하여야 한다는 것이다. 이는 '중요한 내용이 정보주체에게 보다 잘 인식될 수 있도록 하여' 정보주체가 개인정보 처리에 대한 동의를 할 때, 중요 내용을 확인할 수 있도록 하겠다는 정책적 취지에서 시작된 것이다.

그런데, 전 세계적으로 이와 같은 규제는 찾아보기 어렵다. 절대 다수의 개인정보 처리가 발생하는 온라인, 특히 모바일 환경에서 해당 규제를 준수하기 위해 디자인적으로 매우 선호되지 않는 방식으로 주요 내용을 강조하고 있어 디자이너들의 원성이 높다(미적으로 완성도가 높지 않은 UI가 형성될 뿐만 아니라, CSS의 통일성 내지 단순함을 유지하기 어렵다는 불만 등). 가장 큰 문제점은, 중요한 내용을 강조하여 표기하였다고 하여 정보주체가 이를 보다 명확히 인식하고 동의를 표할 것이라는 '데이터 기반의 증거'가 제시된 적이 없다는 것이다. 중요 내용이 강조된 동의문을 읽었을 때, 기존의 일반적 동의문과 비교하여 중요한 내용을 보다 명확히 인식했는지에 대한 실험을 하지 않았기 때문이다. 증거 없이 만들어낸 대표적인 '자판기식 규제'의 사례라 할 수 있다.

오히려 해외에서는 Icon 기반으로 중요한 내용을 표시하는 방식에 대한 다양한 실험이 진행되고 있고, 그에 관한 데이터가 정책 형성의 증거로 활용될 수 있는 수준에 이르고 있다. 다양한 유형(크기, 표시, 색상 등)의 아이콘이 이용자 프라이버시 인식에 어떻게 작용하는지를 디자인과 심리의 관점에서 분석하여 정보주체의 통제권 행사에 가장 적극적으로 기여할 수 있는 아이콘을 선정할 수 있는 수준까지 다다른 것이다.



[그림 4] GDPR에 의한 정보주체의 권리를 상징하는 아이콘 셋 (출처: Univ. of Luxemburg)[29]

이와 같은 사례 외에도 증거 기반으로 규제를 형성해야 할 필요성은 적지 않다. 우선 규제 측면에서의 사대주의를 탈피해야 한다는 명제가 있다. 최근 유럽에서 논의되는 인공지능(AI), 디지털 서비스 및 시장에 대한 규제 법안(DMA, DSA)에 따라 우리나라에서도 플랫폼 규제 이야기가 다수 나오고 있다. 이들 법안에는 당연하게도 개인정보에 직접 또는 간접적으로 영향을 미치는 규제들이 다수 포함되어 있다. 유럽연합이 미국기반의 테크 플랫폼에 지배된 기술환경적 맥락을 전혀 고려하지 않은 채, 우리나라에도 유럽연합에서 논의되는 규제 방식을 무비판적으로 도입하려는 '규제 사대주의'가 다시금 고개를 들고 있는 것이다. 이와 같은 규제 사대주의는 ▲탈맥락적 논의를 통한 '몸에 맞지 않는' 규제의 형성 ▲상호운영성을 고려하지 않은 채, 형식(틀) 위주 규제의 도입 ▲규제 도입 취지를 벗어나 규제를 통해 달성하고자 하는 목적의 상실 등으로 인해 매우 다양한 사회적 문제점을 양상하는 원인이 된다는 것은 기존의 규제 형성 체계를 통해 수없이 반복적으로 경험했다.

둘째는 사회적 갈등 해소의 필요성이다. 최근 개인정보보호법 제2차 개정안에 반영된 '전체 매출액 기반' 과징금 부과와 관련하여 정부, 시민사회, 산업계의 갈등이 평행선을 달리고 있다. 정부는 의도적이고 반복적으로 대규모의 개인정보 사고를 저지르지 않는 이상 기존과 특별히 달라질 것이 없다고 하지만, 산업계에선 매우 예외적 사례를 들면서 특정 기업의 경우 조 단위의 과징금 부과도 가능하다며 의견이 대치하고 있다. 이와 같은 상황에서 정부가, 기존의 과징금 부과 사례를 기반으로 개정법 규정이 적용되었을 때, 어느 수준의 과징금이 발생 수 있는 것인지에 대한 '시뮬레이션 결과'를 제시한다면 현재와 같은 논란은 피할 수 있을 것이다. 필요한 데이터가 존재함에도 이를 입증하지 않는 상황에서 피규제자의 신뢰를 기대할 수는 없을 것이다.

셋째는 법제 재편에 소요되는 사회적 에너지와 리소스를 절약할 수 있다는 점이다. 잘 못 형성된 비증거 기반의 법제를 재편하기 위해선 기존의 법제가 잘 못 형성되었다는 점을 입증하고, 새로운 규제에 대한 효과성을 새롭게 입증해야 한다. 최초 잘 못 설계한 규제에 대한 책임, 그리고 규제 재설계에 필요

29) 이 그림은 GDPR에 의한 정보주체의 권리를 나타내는 것으로, 아래의 손은 '권리'를 나타내며, 손 위의 아이콘들은 권리의 유형(좌측부터 열람권(access), 삭제권(erasure), 이동권(data portability), 정보제공권(information))을 나타낸다. 이에 대한 보다 자세한 설명은 다음 논문을 참고할 수 있다. - Arianna Rossi, Gabriele Lenzini, "Making the case for evidence-based standardization of data privacy and data protection visual indicators", 2020. 2. 21., Vol. 8 No. 1 (2020): Special Issue on "Visual Law", URL: https://ojs.law.cornell.edu/index.php/joal/article/view/103/96

한 사회적 합의 등에 소요되는 사회적 자원의 낭비는 증거기반 규제 형성으로 사전에 예방할 수 있다. 시간이 경과하고, 환경이 변화함에 따라 기존의 규제 효과가 기대 수준을 밑돌게 되더라도, 초기에 제대로 갖춰 놓은 증거기반의 프레임워크에 새로운 '정책적 변수'를 적절히 입력하는 경우 규제의 초점을 다시 맞추는 것은 크게 어렵지 않다. 법제 재편에 소요되는 사회적 에너지와 리소스를 대폭으로 감소시킬 수 있는 것이다.

나가며

휴리스틱(huristics)에 의해 한번 잘 못 형성된 법규제가 사회에 미치는 악영향을 개선하기 위해서는 수 년의 시간과 상상하기 어려운 수준의 사회적 자원이 소모된다. 기존에 선진국을 따라서 '패스트 팔로어(fast follower)'방식으로도 사회적 변화를 법제도로 규율할 수 있었다면, 전 세계적으로 주목받는 선진국의 일원으로서 전 세계에 규제 모범을 보이기 위해서는 한시바삐 증거기반의 규제체계로 이동해야 한다.

▲신규 규제 필요성/효과성(기대효과) 대해서는 반드시 데이터 기반 증거 제시하여 검증받도록 하고, ▲형성된 규제에 대해서는 데이터 기반의 효과성 평가를 정기적으로 수행하도록 하며, ▲규제 효과성 예측과 엇나가는 결과 발생 시, post mortem을 수행하는 것을 의무화하는 등의 조치가 반드시 필요하다. 특히, 데이터 기반 경제의 시대에 본격 진입하여 선도 국가로서 지위를 탄탄하게 하기 위해서는 더 이상 주목 구구식의 규제 형성은 허용되어서는 안된다. 아울러, 형식에 치중한 데이터기반행정법의 실질을 강화하기 위한 사회적 논의도 본격적으로 시작해야 할 것이다.

"증거없이 규제없다."는 간단하지만, 미래를 밝힐 원칙을 세워야 한다.

발 행 일	2022년 1월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 미래정책연구실 정책분석팀
편 집	㈜ 해리

본 내용의 무단 전재를 금하며, 가공·인용할 때는 반드시 출처를 「한국인터넷진흥원(KISA)」이라고 밝혀 주시기 바랍니다.

KISA Report의 내용은 한국인터넷진흥원의 공식 견해와 다를 수 있습니다.