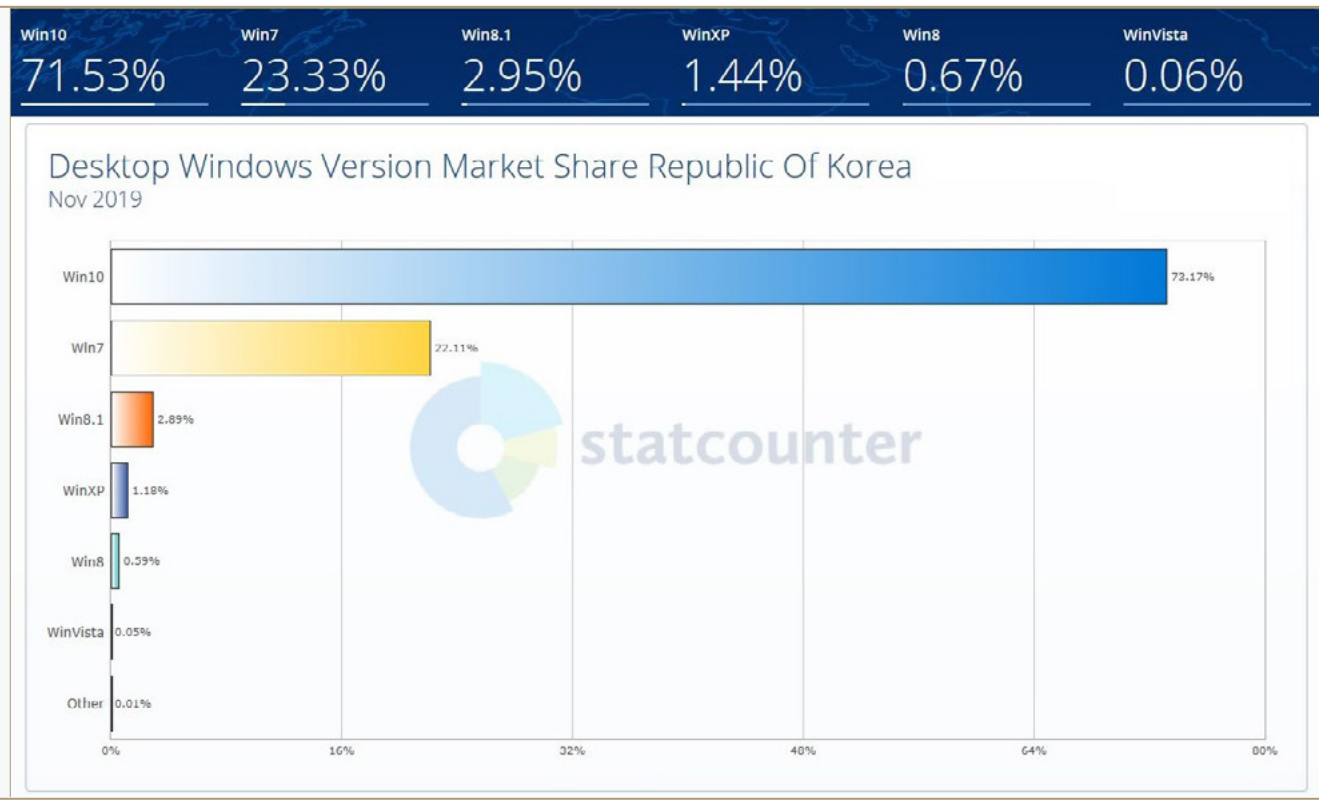
IT & LIFE

윈도우7 지원 종료 코앞, 지금 챙겨야 할 것은?

2020년 1월 14일, 윈도우7의 지원이 종료된다. 왠지 '2020년'이라고 하면 먼 미래의 일 같이 느껴지지만, 이제 딱 한달 남았을 뿐이다. 현재 적지 않은 수의 기업과 대다수 공공기관에서는 윈도우7을 사용 중인 것으로 알려져 있다. 특히 일반 기업에서는 예산이나 업무 공백 등의 이유로 당장 윈도우7을 다른 운영체제로 교체하기 어려운 실정이다. 한달 앞으로 '윈도우7 지원 종료'의 의미와 보안 담당자들이 확인해야 할 부분은 무엇인지 살펴본다.

마이크로소프트(Microsoft, 이하 MS)는 지난 2009년 10월 22일에 윈도우7을 출시할 당시 '10년 동안 제품 지원을 제공하겠다'고 밝혔다. 10년의 지원 기간이 종료되면 최신 기술과 새로운 환경을 지원하는 데 투자를 집중할 수 있도록 윈도우7 지원을 중단할 것이라고 오래 전부터 공언해 온 것. 따라서 윈도우7 운영체제(OS)를 이용하고 있는 기업에서는 내년 1월부터 윈도우를 업그레이드하거나 아예 다른 운영체제로 갈아타야 한다.

국내 PC 4대 중 1대가 여전히 윈도우7을 사용하고 있는 것으로 알려져 있다. 또, 글로벌 시장조사 기관 스탯카운터(Statcounter)에 따르면, 2019년 11월 기준 국내에서 이용 중인 윈도우OS 버전 중 윈도우7 이용율은 22.11%에 달한다.



▲ 국내 윈도우 OS 버전별 점유율 (*출처: Statcounter.com)

전체 윈도우OS 중 윈도우10 점유율이 70% 이상을 차지하고 있지만, 지원 종료가 예정된 윈도우7을 비롯해 이미 지원이 종료된 XP 등도 여전히 사용되고 있다는 것은 우려되는 부분이다. 다행인 것은 상대적으로 윈도우7 이용 비율이 높은 편으로 알려진 공공 분야의 윈도우7 교체 작업이 속도를 내고 있다. 지난 5월 행정안전부의 발표에 따라 공공기관의 인터넷망에 개방형OS 도입을 추진 중이다.

'윈도우7 지원 종료'의 진짜 의미는?

많은 사람들이 궁금해하는 것 중의 하나는 "윈도우7을 계속 쓸 수 없냐"는 것이다. 결론부터 말하면, 쓸 수 있다. 다만, 여러 가지 제약과 위험이 따른다.

지원 종료 후에도 윈도우7을 사용할 경우, 가장 큰 제약 사항은 '호환성'이다. 현재 MS를 비롯해 대다수의 소프트웨어 업체들은 윈도우10을 기준으로 소프트웨어 제품을 개발하고 있다. 즉, 앞으로 윈도우7을 계속 사용한다면 인터넷 이용부터 PC 작업이 수월하지 않을 수 있다는 뜻이다.

그러나 더 큰 문제는 '보안'이다. 랜섬웨어를 비롯해 각종 악성코드에 의한 피해가 확산될 때마다 보안 업체와 관련 기관에서 강조하는, 뻔하지만 가장 중요한 보안 수칙이 바로 '사용 중인 운영체제나 소프트웨어의 보안 패치 적용'이다. 대부분의 악성코드가 운영체제나 소프트웨어의 취약점을 이용하기 때문이다. 이와 관련해 MS는 윈도우 OS와 MS오피스 등 소프트웨어의 취약점 패치를 정기적으로 배포하고 있다.

'지원 종료'는 바로 이 보안 패치와 밀접한 관련이 있다. 윈도우7의 지원이 종료된다는 것은 이후 윈도우7과 관련된 취약점이 발견되더라도 보안 패치를 제공하지 않을 수도 있다는, 즉 업데이트되지 않는다는 의미다. 취약한 운영체제를 업데이트하지 않은 채 사용할 경우 랜섬웨어 등 악성코드를 비롯해 각종 사이버

위협에 고스란히 노출되기 십상이다.

만약 내년 1월 이후 취약점이 발견된 윈도우7 기반의 PC가 해킹되면 워너크라이 랜섬웨어 사태보다 심각한 피해가 발생할 수 있다는 게 전문가들의 공통된 목소리다. 지난 2017년 나타난 워너크라이 랜섬웨어는 윈도우 운영체제의 알려진 취약점을 이용해 감염·확산되었는데, 당시 사태의 심각성을 인지한 MS는 이례적으로 이미 기술 지원이 종료된 윈도우X 등에 대한 긴급 보안 패치를 배포했다.

워너크라이 랜섬웨어는 유럽의 이동통신사 텔레포니카, 영국의 국민건강서비스, 페덱스, 도이체반, 러시아 내무부와 방위부, 러시아 통신사 메가폰 등 전 세계 약 150개국에서 30만 대가량의 PC를 감염시켰다. 그 중에서도 영국의 보건부는 특수 목적 시스템의 운영체제가 바뀌면 사용 중인 소프트웨어를 처음부터 다시 개발해야 한다는 점 때문에 운영체제 업그레이드를 미루다 워너크라이 랜섬웨어에 심각한 피해를 입은 것으로 알려졌다. 이처럼 윈도우7은 언제 터질지 모를 보안의 시한폭탄이 되었지만 개인을 비롯해 기업의 보안 불감증은 여전하다고 전문가들은 지적하고 있다.

윈도우7이라는 시한폭탄…..해법은?

결과적으로 안전한 업무 환경을 유지하고자 한다면 윈도우10으로 업그레이드하는 것이 바람직하다. 그런데, 다른 대안은 없을까? 일각에서는 리눅스 등 개방형 운영체제를 대안으로 평가하고 있다. 윈도우 보안 취약점을 해소하는 한편 윈도우의 종속성에서 탈피해 비용 절감까지 가능하다는 게 이들의 판단이다.

정부는 공공기관의 윈도우7 PC를 윈도우10으로 교체하는데 7800억 원에 달하는 비용이 소요될 것으로 예상, 이를 줄이기 위해 윈도우10 대신 개방형OS를 단계적으로 도입한다는 계획이다. '개방형OS'란 오픈소스 소프트웨어인 리눅스(Linux) 기반으로 개발하고 소스 프로그램을 공개하는 운영체제(OS)를 말한다.

행안부는 개방형OS 가이드라인 마련과 함께 OS를 비롯한 각종 업무용 애플리케이션을 빌려 쓰는 DssS(클라우드에서 서비스형 데스크톱) 도입 방안을 올해 안에 수립할 계획이다. 해외에서도 공공기관에서 우분투 기반의 공개용 운영체제를 비롯해 공개용 오피스 프로그램 등을 도입해 비용을 절감한 사례가 보고되고 있다.

또한 한컴의 개방형 운영체제인 구름(Gooroom)이나 티맥스의 공개용 티맥스OS, 정보통신산업진흥원(NIPA)의 하모니카OS, 화웨이의 훙멍OS 등 글로벌 IT기업들도 잇따라 윈도우를 대체할 수 있는 개방형 운영체제 개발에 나서고 있어 주목된다.

개방형 운영체제 및 프로그램 도입의 결림돌 역시 호환성이다. 대부분의 기업용 소프트웨어 및 서비스가 윈도우 기반으로 제작되고 있기 때문이다. 다행스럽게도 최근 국내외 주요 소프트웨어 업체들이 멀티OS 기준으로 호환성을 확대하고 있는 추세다. 또 일부 개방형OS 업체는 윈도우 환경에서 기본적으로 사용하던 기능들을 선택적으로 설치해 사용할 수 있도록 하고 있다. 행안부에서도 개방형OS의 단계적 도입·확산을 목표로, 인터넷망 PC에 개방형OS를 선도입하면서

주요 SW의 호환성 검토 및 확보를 중점 추진한다는 계획이다. 또 민·관 협의체를 구성하고 SW 업체들의 개방형OS 호환성 확보를 촉진하고 있다.

그러나 개방형OS도 윈도우 운영체제와 마찬가지로 악성코드 등 보안 위협으로부터 자유로울 수 없다. 이와 관련해 안랩은 최근 개방형OS 기반의 업무용 PC 전용 보안 솔루션인 V3 Desktop for Linux를 출시했다. V3 Desktop for Linux는 리눅스 기반의 개방형OS에 최적화된 PC 보안 솔루션으로, 구름(Gooroom), 티맥스OS(TmaxOS), 하모니카(HamoniKR) 등 다양한 개방형OS를 지원한다.

당장 갈아탈 수 없다면 '이것'만이라도 확실하게!

당장 윈도우10으로 업그레이드하거나 개방형OS로 대체할 수 없는 경우라면 어떻게 해야 할까? 개인 사용자와 달리 특히 중소기업이나 생산시설 등 특수한 환경에서는 비용 외에도 여러가지 이유로 운영체제를 업그레이드하거나 교체하기가 쉽지 않다. 그렇다면 일단 지금까지 배포된 윈도우7 관련 보안 패치라도 빠짐없이 적용하도록 하자. 상당수의 악성코드나 사이버 공격은 알려진 취약점을 이용하고 있기 때문에 배포된 패치만 모두 적용해도 사전 예방에 큰 도움이 된다.

모든 PC를 일일이 확인하기 어렵다면 패치 관리 솔루션을 이용해 전사 시스템에 윈도우7의 보안 패치 적용 여부를 확인하고 조치할 수 있다. 안랩 EPP 패치 매니지먼트(AhnLab EPP Patch Management)는 중앙에서 전 시스템의 패치 현황을 한 번에 확인하고 조치할 수 있을 뿐만 아니라 윈도우7 및 윈도우XP 등의 보안 패치를 손쉽게 적용할 수 있는 기능을 제공하고 있다.