전 세계 정부의 디지털 주권으로의 전환

공공 부문 조직을 위한 새로운 생존 전략

미국 외 지역의 공공 부문 조직들에 디지털 주권은 단순한 규제 체크리스트를 넘어 생존 전략으로 그 의미가 확대되었습니다. 각국 정부는 이제 주권을 확보하거나 관할 법규를 준수하는 것만으로는 충분하지 않다는 사실을 깨닫고 있습니다. 이러한 새로운 디지털 주권의 목표를 전략적 자율성이라 부릅니다. 이는 외부 지원이 중단되거나 글로벌 공급망에 차질이 생기더라도 중요 서비스를 독립적으로 운영,·혁신, 유지 관리할 수 있는 역량을 의미합니다.

최근 유엔무역개발회의(UNCTAD) 리포트에 따르면, "개인정보 보호 및 데이터 보호 법률을 보유한 국가 중 79%가 디지털 주권에 대해 우려하고 있습니다."[1] 각국 정부는 폐쇄적인 독점 시스템에 내재된 종속성을 더 이상 무시할 수 없는 상황에 직면했습니다. 전략적 자율성으로의 전환은 다음과 같은 3가지 요소에 영향을 받습니다.

- **지정학적 리스크:** 평시에는 글로벌 하이퍼스케일러에 대한 의존이 큰 문제가 되지 않을 수 있습니다. 그러나 분쟁 상황에는 외부 지원에 대한 의존이 치명적인 취약점이 됩니다. 물리적 파괴 또는 인터넷 서비스 장애로 클라우드에 의존하는 운영이 마비됩니다. 각국은 국제적 협력이 불가능하거나 신뢰할 수 없는 상황에서도 독자적으로 행동할 수 있는 역량을 갖추어야 합니다. 그러려면 연결이 차단되거나, 중단되거나, 간헐적이거나, 대역폭이 제한된(Denied, Disrupted, Intermittent, and Limited, DDIL) 환경에서도 운영 가능한 시스템이 필요합니다. 이를 통해 국가가 글로벌 인터넷과 단절되더라도 국방 지휘 통제 시스템부터 긴급 행정 서비스에 이르는 핵심 임무 기능들이 중단 없이 운영될 수 있도록 보장해야 합니다.
- **사이버 복원력:** 국가 지원을 받는 사이버 공격이 갈수록 정교해지고 있으며, 그 빈도와 영향력 또한 확대되고 있습니다. 주권이 확보되면 에너지 그리드, 의료 체계, 국방 시스템 네트워크와 같은 중요 인프라가 외부 간섭과 공급망 파괴 공작에 대응하여 복원력을 유지할 수 있습니다. 사이버 공격의 리스크에는 데이터 도난뿐만 아니라 전송 중인 소프트웨어 업데이트에 악성 코드를 삽입하는 행위도 포함됩니다. 정부 기관은 주권 보장을 필요로 합니다. 즉, 해외의 첩보 활동을 방지하기 위해 소프트웨어 공급망의 무결성을 독자적으로 검증하고, 시스템이 손상되지 않았음을 확인할 수 있는 역량을 갖추어야 합니다.
- **경제적 경쟁력:** 각국 정부가 디지털 주권을 국가 안보의 초석으로 간주하는 경향이 점차 뚜렷해지고 있습니다. AI 개발과 데이터 거버넌스를 현지화함으로써 미래 경제 성장의 동력을 외부 감독이 아닌 국가 관할권 내에 유지할 수 있습니다. 해외의 블랙박스 AI 모델에 의존할 경우 지적재산권과 문화적 관련성을 잃게 될 수 있다는 우려가 커지고 있습니다. 각국은 전략적 자율성을 바탕으로 디지털 역량을 구축하여 국내 혁신 에코시스템을 육성할 수 있고, 디지털 혁신으로 창출되는 경제적 가치를 국가 경제 내에 유지할 수 있습니다.

1 "전 세계 데이터 보호 및 개인정보 보호 법률." UNCTAD, 2026년 2월 17일.

글로벌 수요와 지역적 현실

통제권 확보는 전 세계적으로 공통된 요구사항이지만 글로벌 공공 부문이 직면한 구체적인 영향과 장애물은 지역에 따라 현격한 차이를 보입니다.

유럽, 중동, 아프리카(EMEA) 및 캐나다

EMEA 지역의 주요 갈등은 첨단 기술에 대한 요구와 비유럽연합 공급업체에 대한 의존성 사이의 긴장에 있으며, 이는 정부를 관할권 리스크, 특히 미국이 제정한 해외 데이터 합법적 활용 명확화법(CLOUD Act)이나 해외 정보 감시법 1978(FISA)과 같은 역외 적용법 관련 법률에 노출시킵니다.

유럽 정부 기관들은 프랑스의 SecNumCloud와 같은 국가 의무 사항과 더불어 사이버 보안을 위한 EU의 NIS2, 운영 회복탄력성을 위한 디지털 운영 복원력법(DORA) 등 엄격하고 복잡한 규제에 직면해 있습니다. 국방 인프라는 여전히 파편화되어 있으며, 북대서양조약기구(NATO) 내 상호운용성 격차로 인해 데이터 교환이 지연되는 상황입니다. 또한 각국은 주권 기반 환경을 운영하는 데 필요한 보안 승인을 받은 인력이 극심하게 부족한 상황에 직면해 있습니다. 캐나다는 지리적으로 북미에 있으나 노후화된 인프라로 인해 발생하는 문제들에 있어서는 EMEA 지역과 비슷합니다. 캐나다 국방부는 CSNI(Consolidated Secret Network Infrastructure)의 파편화된 구조와 더불어 현대적인 역량 도입을 지연시키는 관료적 장애물로 인해 어려움을 겪고 있습니다. 이러한 수준의 위험으로 인해 정부 기관들은 민감한 데이터를 외국의 법적 간섭으로부터 격리하고 있고 자체적인 역량 구축을 통해 소프트웨어 격차를 해소하고 있습니다.

아시아 태평양(APAC)

APAC 지역은 기술적 자립성을 실현하기 위한 엄격한 보호주의적 의무 사항과 높은 수준의 컴플라이언스를 강조하는 것이 특징입니다.

- **데이터 현지화:** 중국, 인도, 인도네시아와 같은 국가들은 중요 데이터를 전적으로 자국 영토 내에 보관하도록 요구하는 등 엄격한 데이터 현지화를 시행하며, 글로벌 퍼블릭 클라우드의 활용을 제한합니다.
- **고도의 책임성:** 싱가포르의 경우 공직자가 데이터 오용 또는 오배치 시 형사 처벌을 받는 등 엄격하고 철저한 보안 표준을 시행하고 있어 위험을 회피하는 조달 문화가 형성되고 있습니다.
- **국내외 요구 사항:** 주권적 통제권을 보장하기 위해 글로벌 기술을 현지 기업을 통해 공급하는 '글로컬(glocal)' 파트너십 모델에 대한 선호도가 매우 높습니다.

APAC 국가들은 해외 의존도를 낮추기 위해 자체 역량을 개발하는 데 집중하고 있으며, 디지털 주권을 지정학적 취약점에 대응하는 방패로 간주하고 있습니다.

중남미(LATAM)

LATAM 지역의 현대화는 운영 연속성에 영향을 받으며, 정책보다는 구조적 불안정성으로 인해 지체되는 경우가 많습니다.

- **불안정성과 불연속성:** 빈번한 정권 교체와 경제적 변동성은 불확실한 지정학적 상황 속에서 장기적인 IT 계획 수립과 다년도 조달 계약 체결을 어렵게 만드는 요인이 되고 있습니다.
- **내부 안보에 대한 포커스:** LATAM 국방 기관들은 국경 보호나 마약 단속과 같은 내부 안보를 우선시하며, 대규모 전략적 인프라보다는 민첩한 감시 툴을 선호합니다.[2]

2 "국가 본토 및 서반구 중심의 새로운 미 국방부 전략," DefenseNews, 2025년 9월 25일.

- **조달 리스크:** 공공 조달 과정의 비효율성과 부패 리스크는 기술 예산의 실질적 가치를 하락시킵니다. 따라서 국가가 높은 비용의 경직된 독점 벤더에 종속되지 않으면서, 예산 삭감과 정치적 변화에도 견딜 수 있는 경제적이고 개방적이며 유연한 시스템이 필요합니다.

디지털 주권에 대한 Red Hat의 접근 방식

전 세계 공공 기관들이 성공을 거두기 위해서는 앞서 언급한 다양한 차원에서 주권 문제를 해결해야 합니다. Red Hat은 이러한 각 요소를 파악할 수 있는 툴과 에코시스템을 제공합니다.

데이터 주권과 AI

Red Hat은 중요 데이터와 AI 모델에 대한 완전한 제어권과 자율성의 기준을 이해하여 국경 내의 데이터 레지던스와 현지 법률에 부합하는 거버넌스를 보장합니다. 정부 기관은 자체 모델과 학습 데이터에 대한 소유권을 유지하여 외국이 통제하는 모델에 대한 애플리케이션 프로그래밍 인터페이스(API) 액세스에 의존하지 않고 현지화된 인프라에 배포하여 운영하는 소버린 AI 전략을 이행해야 합니다. Red Hat® OpenShift® AI를 사용하면 데이터가 있는 곳에 소버린 AI 기능을 배포할 수 있습니다. Red Hat은 기밀 컴퓨팅 기술로 사용 중인 데이터를 보호하여 데이터 위치 및 액세스에 대한 제어권을 부여하며, 이를 통해 EU AI 법과 같은 규제의 컴플라이언스를 보장합니다.

기술 주권

장기적인 독립성을 확보하고 제약 없는 애플리케이션 이동성을 보장하기 위해서는 특정 공급업체의 인프라나 독점 소프트웨어에 종속되지 않고 워크로드를 실행할 수 있는 역량이 필요합니다. 정부는 오픈 표준과 이식 가능한 컨테이너 플랫폼을 도입하여 벤더 종속성을 방지해야 합니다. 클라우드 공급업체의 정책이 변경되거나 지정학적 긴장이 고조되는 경우 리팩토링 없이 워크로드를 다른 인프라로 마이그레이션할 수 있습니다. Red Hat은 오픈소스 표준을 통해 벤더 종속성을 완화합니다. Red Hat의 플랫폼은 여러 하드웨어 아키텍처(x86, Advanced RISC Machine(ARM), RISC-V)를 지원하므로 국가 시스템이 외부 종속성과 무관하게 독자적인 일정에 맞춰 진화하고 업데이트할 수 있습니다.

운영 주권

정부 기관은 연결이 해제된 상황에서도 생존하고 운영될 수 있도록 중요 IT 운영에 대한 완전한 행정 권한과 독립성을 유지해야 합니다. 국방 및 중요 인프라는 운영 복원력을 우선시해야 합니다. 이러한 인프라에는 전시 상황을 고려한 재해 복구 계획을 자동화하고, 지원 및 운영이 보안 승인을 받은 현지 시민 인력에 의해 관리되도록 보장하는 것이 포함됩니다. 예를 들어 Red Hat은 검증된 현지 시민 인력(예: EU 내 인력)이 제공하는 기술 지원인 'Confirmed Sovereign Support'를 제공하여 지원 담당자가 액세스하는 어떠한 데이터도 해당 관할권을 벗어나지 않도록 합니다. 또한 Red Hat Ansible® Automation Platform이 복원력을 자동화하여 연결이 해제된(DDIL) 환경에서도 신속한 복구와 패치를 제공합니다.

검증 주권(assurance sovereignty)

디지털 시스템과 프로세스의 무결성, 보안 및 신뢰성을 독자적으로 검증함으로써 정부 기관은 계속해서 규제를 준수할 수 있습니다. 정부 기관은 맹목적 신뢰에서 벗어나 검증 가능한 신뢰로 전환해야 합니다. 이러한 전환을 위해서는 소프트웨어 공급망에 대한 엄격한 감사와 공통 평가 기준, 연방 정보 처리 표준(FIPS), NIS2 등과 같은 표준에 대한 컴플라이언스를 입증할 수 있는 능력이 필요합니다. Red Hat은 암호화 서명과 출처 검증이 완료된 소프트웨어와 SBOM(Software Bill of Materials)이 포함된 신뢰할 수 있는 소프트웨어 공급망을 제공하여 정부 기관이 모든 구성 요소를 감사하고 악성 코드의 삽입을 방지하도록 지원합니다. 이러한 안전 조치는 정부 기관이 EU 사이버 복원력 법과 같은 새로운 법적 의무 사항들을 준수하는 데 도움이 됩니다.

오픈소스를 통한 전략적 자율성

Red Hat은 유연하고 개방적인 기반을 바탕으로 당면 과제들을 해결하며, 공공 기관에 경직된 격리가 아닌 더 넓은 선택권과 강력한 제어권을 부여합니다. 이러한 유연한 접근 방식은 단일 공급업체만으로는 디지털 주권 문제를 해결하기 어렵다는 사실을 잘 보여줍니다. Red Hat은 다양한 인프라 공급업체와 클라우드 영역에 걸쳐 소버린 클라우드를 구축할 수 있는 선택권을 제공하여 단일 솔루션의 한계를 극복합니다.

Red Hat은 30년 이상 보안 및 컴플라이언스 요건이 가장 엄격한 조직들을 대상으로 신뢰할 수 있는 엔터프라이즈 오픈소스 솔루션을 제공해 왔습니다. 엔터프라이즈 오픈소스는 단순한 기술이 아니라 정부 기관이 진정한 디지털 주권과 전략적 자율성을 실현하기 위해 갖추어야 할 필수 아키텍처 기반입니다. 폐쇄적이고 불투명한 시스템에 의존하며 맹목적 신뢰를 요구하는 독점 벤더들과 달리 Red Hat은 정부 기관이 외부에 의존하지 않고 자체적으로 디지털 운명(Digital Destiny)에 대한 통제권을 유지할 수 있도록 지원합니다. 이러한 개방적 접근 방식은 글로벌 공공 부문이 네트워크의 전술적 엣지부터 소버린 AI에 이르기까지 글로벌 혁신의 속도를 제어할 수 있도록 지원하는 동시에 워크로드의 이식성과 복원력을 보장합니다. 또한 오픈소스 접근 방식은 벤더 종속성과 기술적 노후화의 리스크로부터 미션 크리티컬 운영을 보호합니다. Red Hat은 오픈소스 기술을 기반으로 EU 등의 지역에서 통용되는 '오픈 기본'(default to open)' 원칙을 따르고 있습니다. 이러한 모델의 사용은 단일 벤더에 대한 의존을 방지하고 코드 검사 및 수정을 허용하므로 국가 안보와 신뢰에 필수 요소가 되고 있습니다.

- **투명성 및 신뢰**

  Red Hat의 오픈소스 모델은 100% 투명성을 제공하므로 정부 기관은 소스 코드를 검사하고 보안성을 검증하며 소프트웨어 공급망을 감사할 수 있습니다. 이러한 감사 가능성은 EMEA 및 APAC 지역의 검증 요건을 충족하는 데 있어 매우 중요한 요소입니다. 나아가 Red Hat은 EU 사이버 복원력 법과 같은 새로운 법적 의무 사항을 준수할 수 있도록 출처 검증과 암호화 서명이 완료된 소프트웨어를 제공합니다.

- **운영 주권 및 현지 지원**

  Red Hat은 관할권 리스크를 해결하기 위해 인프라 운영 주체에 대한 제어 역량을 지원하여 운영 주권을 실현합니다.

  - **주권 지원:** 앞서 언급했듯이 Red Hat은 EU 내에서 검증된 EU 시민권자만이 기술 지원이 제공되도록 하는 'Confirmed Sovereign Support'를 EU에서 제공합니다. 이러한 기술 지원을 통해 지원 담당자가 접근하는 어떠한 데이터도 해당 지역을 벗어나지 않도록 보장할 수 있습니다.
  - **현지 에코시스템:** 현지의 인증된 클라우드 공급업체들로 구성된 Red Hat 파트너 에코시스템은 엄격한 국가별 데이터 레지던스 법률을 충족하는 소버린 클라우드 역량을 제공합니다.

- **기술 독립성**

  오픈 하이브리드 클라우드 전략은 온프레미스, 프라이빗 클라우드, 전술적 네트워크 엣지, 에어갭(air-gapped) 환경 등 여러 환경에서 워크로드가 실행되도록 지원합니다.

  - **이식성:** 이식성은 공공 부문, 특히 LATAM 및 APAC 지역의 정부 기관들이 가장 우려하는 벤더 종속성을 예방하기 위한 기반입니다. 해당 지역에서 워크로드와 데이터를 효율적으로 마이그레이션할 수 있는 역량은 기술 공급업체의 교체가 필요할 수 있는 정치적 또는 경제적 변화와 같은 지정학적인 변동에 대한 효율적 대응과 서비스 연속성을 보장하기 위한 필수 요건입니다.
  - **연결이 해제된 운영:** 국방 기관의 경우 Red Hat Device Edge와 Red Hat OpenShift 같은 Red Hat 솔루션을 사용해 연결이 끊긴 DDIL 환경에서 시스템을 자율적으로 구동함으로써 특정 클라우드의 연결이 불가능한 상황에서도 임무를 이어 나갈 수 있습니다.

Red Hat은 정부 기관이 불확실성 속에서도 생존하고, 신뢰할 수 있는 데이터 보안을 제공하며, 국가 기능을 지속할 수 있는 소버린 클라우드를 구축할 수 있도록 개방형 기반을 제공합니다.

- **소버린 AI**

  각국 정부가 AI를 탐색하고 확장해 나감에 따라 Red Hat은 소버린 AI를 구축할 수 있는 플랫폼을 제공하고 있습니다. 이를 통해 각국은 모델과 학습 데이터에 대한 소유권을 유지할 수 있으며, 외국에서 통제하는 모델에 대한 API 액세스 방식에 의존하지 않고 현지화된 인프라에 직접 배포함으로써 EU AI 법과 같은 규정을 준수할 수 있습니다.

공공 부문에 Red Hat을 사용해야 하는 이유

Red Hat은 공공 부문의 신뢰를 받는 파트너로서 미국 행정부 부처 100%에 도입되었으며[3], NATO 및 전 세계 국방부에서도 널리 사용되고 있습니다. Red Hat 라이센싱 모델과 오픈 표준에 대한 강력한 의지는 정부 기관이 특정 벤더에 영구적으로 종속되지 않는 구조를 만들어 줍니다. 조직은 소프트웨어를 무기한으로 사용하고 유지 관리할 권리를 보유하므로 벤더 로드맵 변경이나 지정학적 제약으로부터 장기적 투자를 보호할 수 있습니다.

특히 국방 분야를 중심으로 지출이 증가함에 따라 Red Hat 솔루션 및 서비스 포트폴리오에 투자함으로써 가시적인 ROI(투자수익률)를 달성할 수 있습니다. NATO 회원국들이 약속한 국방비 지출이 두 배로 증액되어 2035년까지 국가 GDP의 5% 수준에 도달할 전망입니다.[4] 정부 기관은 단일 플랫폼으로 표준화함으로써 파편화된 기존 시스템을 유지 관리하는 데 따른 비용을 새로운 임무 수행 역량을 창출하는 분야로 전환하여 운영 비용과 총소유비용(TCO)을 획기적으로 절감할 수 있습니다.

시작을 위한 다음 단계

- 글로벌 공공 부문의 Red Hat에 대해 자세히 알아보고 Red Hatter에게 문의하세요.
- 조직의 디지털 주권 상태를 평가하고 싶으신가요? 이 블로그 포스트를 읽고 시작해 보세요.

3 Red Hat 고객 데이터, 2025년 9월.

4 "국방 지출과 NATO의 5% 증액 약속." NATO, 2025년 12월 18일.

Red Hat 소개

Red Hat은 세계적인 엔터프라이즈 오픈소스 소프트웨어 솔루션 공급업체로서 커뮤니티 기반의 접근 방식을 통해 신뢰도 높은 고성능 Linux, 하이브리드 클라우드, 컨테이너 및 쿠버네티스 기술을 제공합니다. 또한 Red Hat은 고객이 클라우드 네이티브 애플리케이션을 개발하고, 신규 및 기존 IT 애플리케이션을 통합하고, 복잡한 환경을 자동화하고 관리할 수 있도록 지원합니다. Fortune 선정 500대 기업이 신뢰하는 어드바이저인 Red Hat은 전 세계 고객에게 권위 있는 어워드를 수상한 지원, 교육 및 컨설팅 서비스를 제공하여 모든 산업 분야에서 개방형 혁신의 이점을 실현할 수 있도록 최선을 다하고 있습니다. Red Hat은 기업, 파트너, 커뮤니티로 구성된 글로벌 네트워크의 허브 역할을 하며 고객들이 성장하고, 확장하고, 디지털 미래에 대비할 수 있도록 지원합니다.

www.facebook.com/redhatkorea
구매문의 02-6105-4390
buy-kr@redhat.com

www.redhat.com/ko
#3613114_0326

Copyright © 2026 Red Hat LLC. Red Hat, Red Hat 로고, Ansible 및 OpenShift는 미국과 그 외 국가에서 Red Hat 또는 계열사의 상표이거나 등록 상표입니다.