

2021년은 중견기업의 클라우드 및 SaaS 도입 원년

기술 투자를 통해 효율성, 수익성, 보안 등 대폭 강화



DG의 새로운 연구 결과에 따르면 중견기업들은 전혀 없는 변화의 시대를 클라우드 기술로 헤쳐 나가고 있다고 합니다. 이는 클라우드가 급변하는 비즈니스 목표에 적응하는 동시에 조직을 혁신하는 데 필요한 유연성을 갖추고 있기 때문입니다. 많은 사람들이 재택근무를 계속하고 있으므로 앞으로 한동안은 이러한 유연성이 필수 조건이 될 것입니다.

IDG와 시스코는 기업, 특히 직원 수 100~999명인 중견기업이 어떻게 적응하고 있는지 정확하게 파악하기 위해 IT 구매를 담당하는 비즈니스 리더들을 대상으로 향후 구매 예정인 제품과 구매 이유, 조달 관련 문제, 팬데믹으로 인한 계획 변경 등에 대한 설문조사를 실시했습니다. 이 백서에서는 그 결과를 정리합니다.

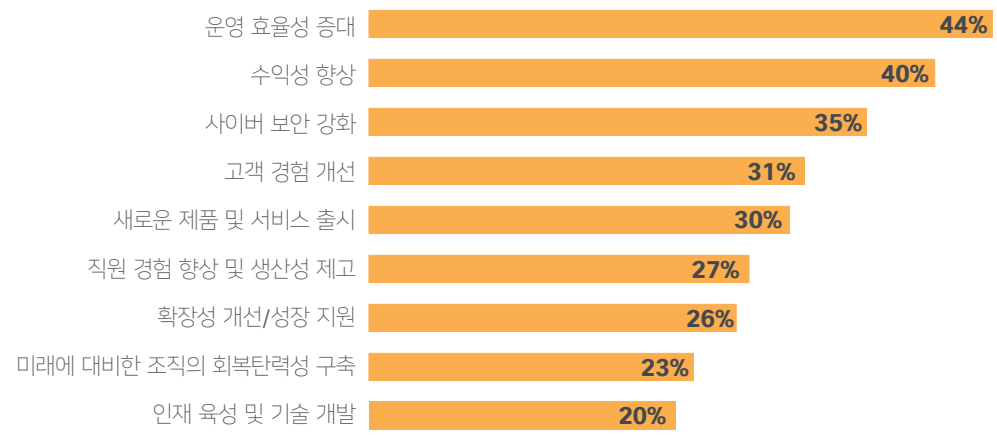
투자 촉진 요인

중견기업은 전반적으로 운영 효율성을 높이고 이를 바탕으로 수익성을 개선할 필요가 있다는 것이 이번 조사에서 드러났습니다. 또한 중전보다 훨씬 강력한 보안 기능도 필요합니다. 그리고 이 세 가지 목표는 기술을 통해 달성할 수 있습니다.

하지만 역설적으로 기술은 효율성과 수익성 실현을 가로막는 가장 큰 장애물이자 보안 업그레이드의 걸림돌이기도 합니다. 조사 대상 기업 중 절반 정도가 사일로화된 레거시 시스템으로 인해 어려움을 겪고 있는 것으로 밝혀졌습니다. 또한 조사 대상 기업 중 3분의 2가 두 곳 이상의 사무실을 지원해야 한다고 답변한 것으로 보아 이것은 여러 위치에서 발생하는 문제입니다.



그림 1 2021년 이후의 주요 비즈니스 목표



출처: IDG

사이버 보안, 클라우드, 하드웨어에 우선적으로 투자할 계획이라는 답변에서는 기업들이 생각하는 투자 효과의 순위를 엿볼 수 있습니다. 그리고 이 모든 것을 아우르는 제1의 목표는 44%의 중견기업 리더들이 언급한 바와 같이 지금 같은 혼란의 시대에 운영 효율성을 높여야 한다는 것입니다.

1위에 필적하는 2순위 목표는 수익성 향상(40%)이었습니다. 효율성을 높이면 수익이 늘어나기 때문입니다. (그림 1 참조)

시스코 중견·중소기업 및 커머셜 부문의 글로벌 CTO인 Nick Chrissos는 "비용 절감과 생산성 증대는 모든 비즈니스의 기본"이라고 강조하면서, 중견기업의 사이버 보안 위험이 증가하고 있다고 설명합니다. "일반적으로 보안은 모든 비즈니스의 필수 요소지만, 지난 몇 년간 중견기업을 노리는 공격이 점점 늘고 있습니다."

Chrissos는 그 이유가 오늘날 사이버 범죄자들이 일종의 악성코드 경제에서 얻은 자금으로 규모가 작은 기업을 정밀하게 공격하기 때문이라고 주장합니다. 이 지하 세계에서는 이제 무기화된 소프트웨어 툴을 공격자에게 판매하는 범죄 조직까지 생겨났습니다. 예를 들어 개발자는 기술력이 떨어지는 사기꾼에게도 RaaS(Ransomware-as-a-Service) 방식으로 악성코드 라이선스를 판매할 수 있습니다. 이들은 악성코드로 보안에 철저하지 못한 피해자를 공격해서 금전을 갈취하려고 합니다.

효율성, 수익성, 보안 같은 기본적인 요구 사항을 해결한 기업 중 31%는 뒤이어 고객 경험 개선을 위한 IT 투자를 생각하게 됩니다. McKinsey 보고서에 따르면, 뛰어난 고객 경험은 상당한 매출 증대와 비용 절감을 촉진하여 효율성 및 수익성 목표에 보탬이 될 수 있다고 합니다.

발전의 걸림돌

기술 도입 여정을 시작한 기업에서 가장 먼저 넘어야 할 중요한 장애물은 바로 구형 시스템과 데이터 액세스 문제입니다. 비즈니스 목표를 달성하려 애쓰는 기업의 49%가 데이터 사일로화를 유발하는 레거시 시스템을 가장 큰 장애물로 꼽았습니다.

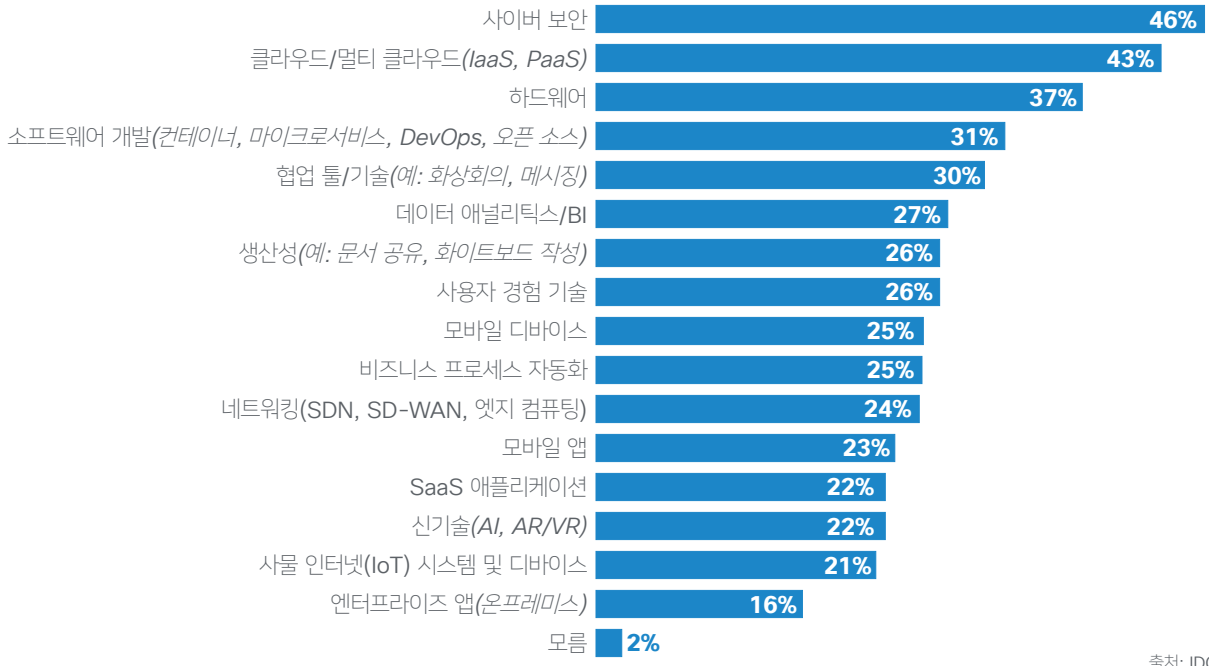
요즘처럼 혼란스러운 시대에는 놀랄 일도 아니지만, 38%의 응답자들은 팬데믹과 정치·경제적 상황 같은 외부 요인을 기술 도입을 가로막는 장애물 2위로 선정했습니다. 이어서 예산 및 금전적 제약(36%)과 인적 자원 문제(30%)가 그 뒤를 바짝 쫓고 있습니다.

인적 자원 문제에는 기술 격차도 포함됩니다. 세계 경제 포럼(World Economic Forum)이 최근 보고서에서 밝혔듯이, 팬데믹 이전에도 시급한 과제였던 인력 및 기술 부족 문제는 당분간 전 세계 기업들의 발목을 잡는 요인으로 남을 것입니다. 기술 발전으로 인해 업무가 변경되면서 직원들 역시 업무 중단의 고통을 겪고 있습니다.

기술 부족 문제는 다른 기업 못지 않게 중견기업에도 큰 영향을 미칩니다. 중견기업들은 기술 격차 때문에 비즈니스 목표 달성이 지연되고 있다며 고충을 토로했습니다. IDG 설문조사에서 평균적인 IT 조직의 IT 직원 수는 25명 미만인 것으로 나타났습니다. 절반 정도(43%)는 IT 직원 수가 10명 미만이었으며, 독립된 IT 부서가 아예 없는 경우도 일부(5%) 있었습니다.

상황이 이런 만큼, 중견기업의 41%가 기술 구현 작업을 외부 업체에 맡기고 있다는 사실은 전혀 놀랍지 않습니다.

그림 2 주요 기술 투자 분야



출처: IDG

기술 우선순위

중견기업 IT 리더와 비즈니스 리더의 68%는 2020년을 돌아보면서, 팬데믹 기간 중 클라우드에서 애플리케이션과 데이터를 사용하는 경우가 늘었다고 밝혔습니다. 클라우드 사용이 줄었다고 밝힌 응답자는 10%에 불과했습니다. 지역 봉쇄와 재택근무 조치가 장기화되면서 예상했던 일이지만 업종, 지역, 회사 규모를 불문하고 설문조사에 참여한 모든 기업에서 이러한 증가 추세를 보였습니다.

조사 대상 기업의 78%는 클라우드의 유형을 결정할 때도 팬데믹의 영향을 고려했다고 밝혔습니다. 여기에서도 마찬가지로 팬데믹의 영향은 업종, 지역, 회사 규모를 가리지 않았습니다. 설문조사에 참여한 회사 중 절반 이상(56%)이 팬데믹 기간 중 소프트웨어 투자를 늘릴 계획이었다고 밝혔습니다.

업계 관계자들은 더 광범위한 인력의 분산 운용을 포함하여 팬데믹으로 인한 변화가 대부분 그대로 유지될 것이라고 전망합니다. 중견기업의 리더들은 이러한 점을 분명히 인식하고 있으며, 2021년에 소속 조직에서 어떤 유형의 기술을 구매할 계획인지 상세히 알려 주었습니다.

조사에서 밝혀진 2021년의 주요 투자 분야 3가지는 보안(46%), 클라우드(43%, 멀티 클라우드 설정 및 SaaS 포함), 하드웨어(37%)였습니다. (그림 2 참조)

거의 모든 중견기업(95%)이 2021년에는 하나 이상의 클라우드 구축 모델을 활용할 것이라고 답했습니다.

- 중견기업 리더의 57%는 하나 이상의 프라이빗 클라우드를 구현할 계획입니다.
- 51%는 퍼블릭 클라우드를 사용할 예정입니다.
- 33%는 하이브리드 퍼블릭/프라이빗 클라우드 전략을 구현할 것입니다.

2020년 현재 기업에서 사용 중인 애플리케이션 셋 중 하나(30%)는 SaaS 모델의 클라우드에 의존하고 있습니다.

클라우드 보안에 쏠리는 관심

응답자 중 절반 이상(51%)이 클라우드 소프트웨어에 기대되는 가장 큰 이점으로 데이터 보안 강화를 꼽았습니다. 이어서 49%의 응답자들이 선택한 생산성 증대가 클라우드의 이점 2위를 차지했습니다. 그리고 애플리케이션 성능 향상(38%), 비용 절감(35%) 등이 뒤를 이었습니다.

“클라우드를 소비 모델로 이용하면 하드웨어에 투자하거나 소프트웨어를 설치하지 않고도 구축할 수 있습니다. 이렇게 빠른 구축 속도는 정말 큰 장점입니다.” – Nick Chrissos, 시스코 중견·중소기업 및 커머셜 부문 글로벌 CTO

한편 설문조사 응답자의 53%는 2021년에 다른 어떤 SaaS 솔루션보다 클라우드 기반의 보안 투자에 집중할 계획이라고 밝히면서 클라우드에 강력한 지지를 보냈습니다.

그 다음으로 우선순위가 높았던 SaaS 투자 대상은 1위와 큰 격차를 보였습니다. 예를 들어 웹 앱 및 스토리지(두 가지 모두 응답자의 35%가 선택)를 구축하겠다는 계획은 SaaS 우선순위 목록에서 공동 2위를 차지했습니다. 문서 및 스프레드시트 같은 생산성 앱이 3위에 올랐고(33%), 4위는 협업 툴(29%)이었습니다. 보안 문제의 경우, 중견기업 IT 및 비즈니스 관리자의 약 절반(48%)은 보안 기능을 별도로 구매해야 하는 전용 솔루션보다 보안이 기본으로 내장된 번들형 SaaS 솔루션을 선호하는 것으로 나타났습니다. 독립형 SaaS 솔루션 구축을 선호한다고 응답한 비율은 31%에 그쳤습니다.

설문조사 응답자들이 말하는 보안 기능이 통합된 번들형 소프트웨어의 장점은 다음과 같습니다.

- 더 쉬운 유지 보수 및 문제 해결
- 더 쉬운 설정
- 더 우수한 사용자 경험

SaaS 솔루션을 구매하는 대부분의 조직(56%)에서는 레거시 시스템으로 인한 과제를 안고 있기 때문에 SaaS 솔루션 지원을 위해 환경을 변경하는 대신 기존 환경에 솔루션을 이식하고자 합니다.

결론

효율성, 생산성, 보안을 향상할 방법을 모색하던 중견기업들은 사상 초유의 상황에 대응하면서 작년 한 해를 보냈습니다. 그 과정에서 중견기업은 현재 구축 가능한 기술 중 가장 강력한 톨로 눈길을 돌렸습니다. 바로 IT 리더와 비즈니스 리더의 95%가 2021년의 우선 투자 대상으로 선택한 클라우드 및 SaaS 솔루션입니다.

Chrissos는 이렇게 설명합니다. "아키텍처로서 클라우드는 탁월한 이점이 있습니다. 클라우드를 도입하는 즉시 위치에 구애받지 않아도 됩니다. 그리고 클라우드를 소비 모델로 이용하면 하드웨어에 투자하거나 소프트웨어를 설치하지 않고도 구축할 수 있고요. 이렇게 빠른 구축 속도는 정말 큰 장점입니다."

Chrissos는 클라우드에는 당연히 다른 방식의 보안이 필요하다는 경고도 잊지 않습니다. "모든 직원이 사무실에서 근무하고 애플리케이션이 데이터 센터에 있을 때는 장벽을 둘러싸서 전부 보호하면 됩니다." 하지만 여러 팀이 여러 장소에서 근무하는 지금, 기업에 필요한 것은 원격 근무자를 위해 설계된 클라우드 중심 보안이라고 Chrissos는 말합니다. 보안 기능이 통합된 SaaS 애플리케이션은 이 부분에서 진가를 발휘하며, 따라서 중견 기업은 이에 대한 투자 계획을 세우고 있습니다.

귀사와 같은 중견기업에서 클라우드를 활용하여 더 적극적으로 수익성을 향상하는 방법을 알려 드리겠습니다. 시스코의 [중견기업 비즈니스 솔루션](#)에 대해 알아보세요.

설문조사 정보

IDG는 2020년 11월 12일부터 11월 23일까지 직원 수 100~999명의 민간 기업에서 IT 구매를 담당하는 기술 리더 및 비즈니스 리더 650명을 대상으로 설문조사를 실시했습니다.

조사 대상 업종에는 금융 서비스, 제조업, 소매업, 전문 서비스가 포함되었습니다.

응답자의 소속 기업은 미주(미국 200명, 캐나다 50명, 브라질 50명, 멕시코 50명), 유럽(영국 50명, 독일 50명, 프랑스 50명), 아시아 태평양(오스트레일리아 50명, 인도 50명, 일본 50명) 지역에 소재하고 있습니다.