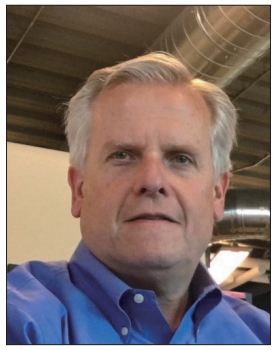
DX 시대, 네트워크 옵저버빌리티 확보 위한 10가지 방법

네트워킹 데이터 관리 중앙화·클라우드 네트워크 모니터링 등으로 네트워크 통제력 확보



케빈 우드(Kevin Wood) 켄틱 제품 마케팅 책임자
(번역·감수: 조인호 시엔스 리드 기술 매니저)
kevin@kentik.com

네트워크 모니터링을 효율적으로 하기 위해서는 아키텍처의 복잡도나 네트워크 구성의 변경 속도와 무관하게 모든 네트워크에서 발생하는 문제에 대해 빠르게 자동으로 대처할 수 있어야 한다. 이에 기존 SNMP 기반 모니터링 도구는 최신 네트워크 흐름 분석에 적합하지 않으며, 인공지능·머신러닝 기술이 접목된 '옵저버빌리티'가 필요하다. 〈편집자〉

디지털 혁신, 클라우드 마이그레이션, SaaS 등 하이브리드 클라우드 환경으로의 전환에 따라 IT 인프라 환경이 더욱 복잡해지고 다양해지는 변화를 겪고 있다. 클라우드 네이티브 아키텍처(Cloud Native Architecture)와 모든 것을 클라우드로 운영하는 체제로의 전환은 다양한 유형의 장비와 네트워크 구조를 급격하게 증가시켰으며, 이 모든 장비와 네트워크는 IT 부서가 네트워크 모니터링의 일부로 관리하게 됐다.

동시에 클라우드 환경은 다양한 리소스(클라우드 공급자 네트워크, ISP, CDN 인프라 및 SaaS 애플리케이션 등)와 그 종속성이 상호 작용해 복잡한 네트워크 환경을 구성하게 되는 방식을 이해할 수 있어야 한다.

그러나 네트워크 성능에 대한 편협한 시각을 가진 고립된 벤더 종속적 플랫폼이 확산됐고, 네트워크에 대한 IT 조직의 통제력은 예전보다 취약해졌다. 대신 고도의 가용성과 지연시간을 보장하며 탁월한 고객 경험을 제공해야 한다는 압박은 그 어느 때보다 증가하고 있는 상황이다.

네트워크 옵저버빌리티 등장

지난 10년간 데이터 과학과 분석 도구는 더욱 발전했으며, 많은 고립된 포인트 솔루션이 시대에 뒤떨어진 것이 됐다. 이제는 머신러닝(ML)과 인공지능(AI) 기술을 접목해 데이터 소스를 결합하고 실행 가능한 새로운 솔루션이 제공되고 있다.

이러한 현대적인 접근 방식의 솔루션을 '옵저버빌리티(Observability)' 솔루션이라 한다. 옵저버빌리티는 모니터링의 진화된 개념으로 기업이 이용하는 전체 시스템에 대한 가시성을 확보하는 것을 의미한다.

네트워크 옵저버빌리티는 다양한 데이터 소스를 사용해 네트워크 내부에서 일어나는 일과 네트워크의 내부 상태가 해당 비즈니스의 목표와 사용자 경험에 미치는 영향을 이해한다. 이는 네트워크상의 예측 가능한 문제를 분석하고 해석하기보다는 그저 찾아내는 것에 국한된 네트워크 모니터링을 훨씬 뛰어넘는 접근 방식이다.

IT 조직은 네트워크 옵저버빌리티를 통해 네트워크의 성능과 가용성 등의 문제를 파악할 수 있을 뿐만 아니라 근본적인 원인까지 정확하게 분석할 수 있다. 실제

로 기업들이 클라우드로 더 많은 워크로드를 옮기면서 네트워크 성능 모니터링이 더 복잡해졌는데, 옵저버빌리티는 이러한 환경에 대해 가시성을 제공하고 효과적으로 문제를 찾아 해결해 줄 수 있게 도와준다.

이번 글에서는 IT 조직이 네트워크 옵저버빌리티 개념을 이해하는데 도움이 되도록 디지털 트랜스포메이션(DX) 시대에 네트워크 옵저버빌리티 확보를 위한 10가지 팁을 알아본다.

■ 1단계 – SaaS 기반 네트워크 옵저버빌리티 수용

전통적인 네트워크 모니터링 도구는 어플라이언스 기반 솔루션으로 온프레미스 환경에 구축됐다. 이는 IT 조직이 유지·관리해야 하는 자산이 추가된다는 의미와 같다. 이러한 솔루션은 확장이 어려우며 인프라에 대한 대규모 투자가 선행돼야 한다.

오늘날의 네트워크 관리 어플라이언스는 시대에 뒤떨어지고 있다. IT 관리 전략을 현대화하려면 최소한의 노력으로 모든 네트워킹 자산을 실시간 모니터링하고, 유연하게 확장 가능한 SaaS 기반 네트워크 관찰 솔루션으로 마이그레이션해야 한다.

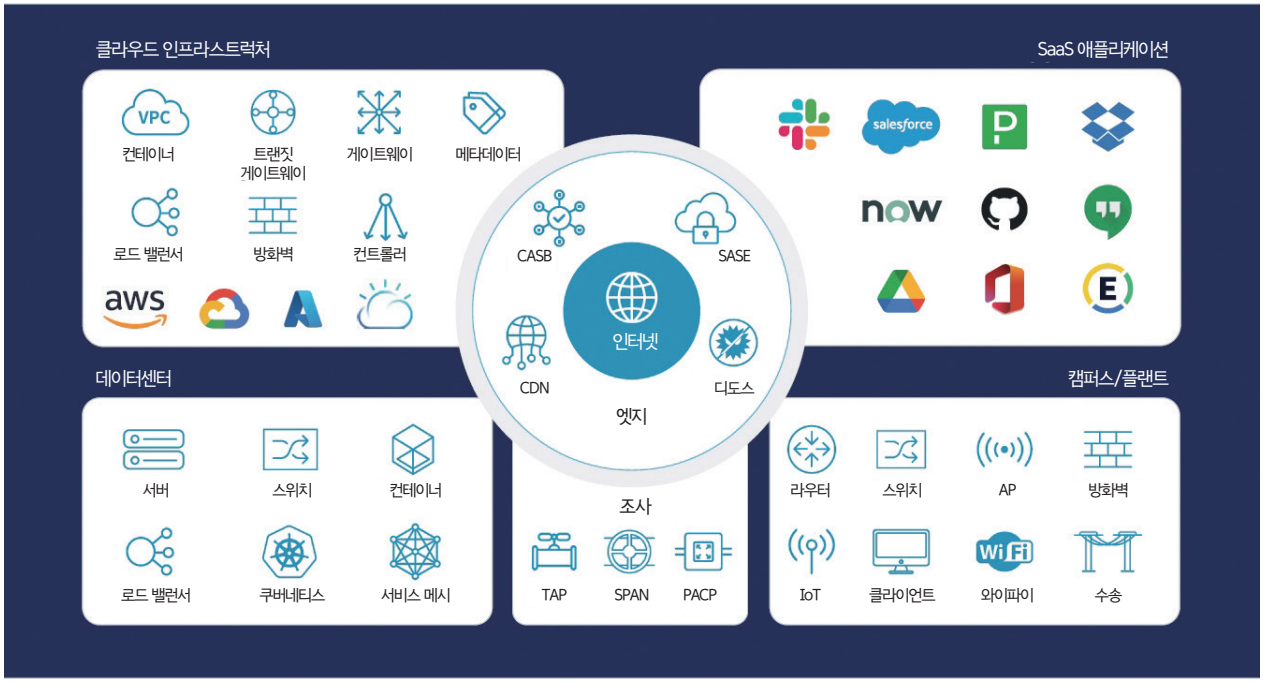
네트워크 옵저버빌리티를 위한 SaaS 기반의 솔루션은 사용량만큼 지불하면 되며, 유연한 확장이 가능하다. 물리적인 어플라이언스로 모니터링하기 어려웠던 클라우드 환경의 장비까지 쉽게 연결할 수 있으며, 네트워크의 범위와 복잡도 증가에 맞춰 원활한 확장이 가능하다.

■ 2단계 – 네트워킹 데이터 관리 중앙화

최신 네트워크 인프라를 관찰하기 위해서는 외부 서비스(SaaS 애플리케이션 및 클라우드 서비스), 온프레미스 기반 인프라, 가상 인프라, 사설 네트워크 및 공용 네트워크 등 다양한 소스에서 나온 데이터를 수집하고 분석할 수 있어야 한다.

이러한 모든 데이터를 효율적으로 분석하려면 실시간 분석이 가능해야 하며, 경고를 실행하는 중앙 로그 수집 데이터베이스(DB)에 저장해야 한다. 데이터 중앙화 및 통합이 제대로 시행되지 않으면 자동화된 분석 작업의 효율이 떨어질 뿐 아니라 네트워크 이슈를 심층적으로 파악하기 어렵다. 결국 네트워크 옵저버빌리티 도구는 서로 다른 소스에서 데이터를 수집하고 이를 필요한 만큼의 분석 작업을 수행할 수 있는 중앙의 통합 저장소에 보관할 수 있어야 한다.

〈그림 1〉 켄틱 옵저버빌리티 도구는 다양한 네트워킹 데이터 수집·분석이 가능하다



켄틱(Kentik)은 네트워크 성능 데이터를 일반 옵저버빌리티 도구와 결합할 수 있도록 도움을 준다. 예를 들어 켄틱 데이터는 뉴렐릭(New Relic)의 옵저버빌리티 플랫폼에서 유용하게 활용 가능하다.

■ 3단계 – 메타데이터·태그 활용

분석가들은 인덱싱 검색을 위한 컨텍스트를 제공하기 위해 네트워크 옵저버빌리티 데이터에 메타데이터와 태그를 적용할 것을 권장한다. 일반적으로 태그를 지정하거나 기타 메타데이터를 컨텍스트화하는 작업은 네트워크 옵저버빌리티 도구가 데이터를 변환해 분석을 준비하는 과정에서 수행된다.

물론 데이터에 수동으로 태그를 적용할 수도 있다. 그러나 대규모의 효율적인 운영을 위해서는 소스, 데이터 유형 또는 데이터와 연결된 엔드포인트와 같은 요소를 토대로 데이터에 자동으로 태그를 지정하는 네트워크 옵저버빌리티 도구가 필요하다.

켄틱은 네트워킹 데이터에 ▲애플리케이션 ▲디바이스 ▲인터페이스 ▲자율 시스템 번호(ASNs) ▲국가 ▲AWS 리전 ▲BGP 패스(BGP path) ▲도시 ▲연결 타입(Connectivity type) ▲넥스트홉 ASNs(Nexthop ASNs) ▲프로토콜 ▲공급자(Providers) ▲사이트(Sites) ▲트래픽 프로필(Traffic profile) 등과 같은 태그를 자동으로 적용한다.

■ 4단계 – 벤더 중립 체제 구축

네트워크 옵저버빌리티 도구는 벤더 친화적인 방식으로 네트워크를 관찰하도록 설계돼야 한다. 이는 네트워크 아키텍처가 수정되고, 새로운 클라우드 서비스 및 공급자 선택이 이뤄지는 등 다양한 작업이 진행되는 과정에서 IT 조직의 옵저버빌리티 전략이 계속 진화할 수 있도록 하는 유일한 방법이다. 여러 벤더 독립적인 모니터링 솔루션을 조율하는 방식은 효과가 없다.

벤더 중립적이라는 것은 독점적인 데이터 수집 또는 모니터링 프레임워크 대신 표준화된 개방형 프로토콜을 토대로 네트워킹 데이터를 수집하는 것을 의미한다. 더불어 모든 클라우드 공급자, ISP 및 애플리케이션 유형과 통합할 수 있는 능력을 의미하기도 한다. 형식, 유형, 소스에 관계없이 네트워킹 데이터를 분석하고 관리하는데 일관된 접근 방식을 취할 수 있어야 한다.

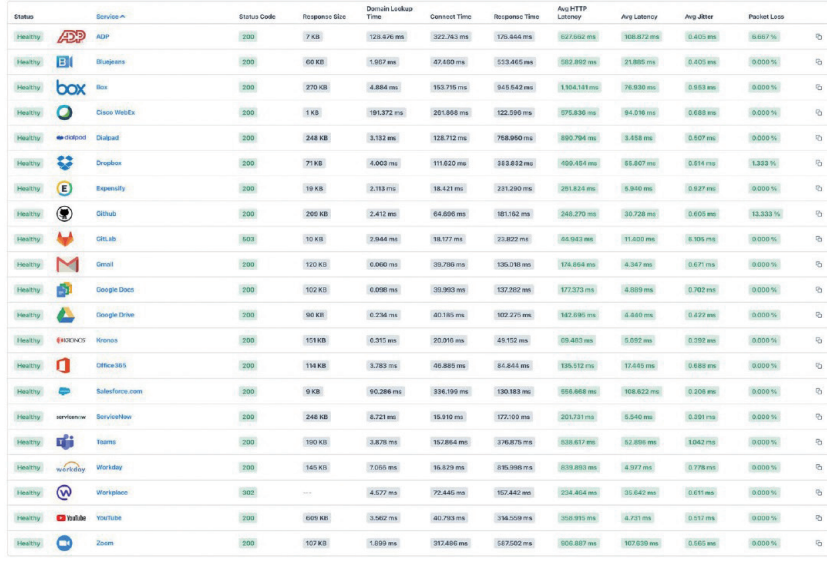
■ 5단계 – SaaS 애플리케이션 네트워크 성능 모니터링

보통 네트워크 관리 시 SaaS 애플리케이션을 간과하기 쉽다. 일반적으로 SaaS 제조사가 SaaS 애플리케이션을 대신 관리해 주기 때문이다.

그러나 네트워크 성능 모니터링 관점에서 볼 때, SaaS 문제는 사용자 경험을 심각하게 저하시킬 수 있다. SaaS 애플리케이션의 연결 오류나 응답 속도, DNS 성능 등과 같은 문제가 SaaS 애플리케이션 문제인지, ISP 또는 내부 네트워크 문제인지 즉시 확인할 수 있어야 한다.

SaaS 네트워크 성능 모니터링으로는 SaaS 제조사의 환경에 직접 액세스 할 수 없는, 다시 말해 네트워크에 대한 데이터를 직접 수집할 수 없다는 문제가 있다. 켄틱은 수십 개의 주요

〈그림 2〉 켄틱은 다양한 SaaS 애플리케이션 성능을 모니터링한다



SaaS 애플리케이션 상태를 실시간으로 추적하는 모니터링 에이전트를 운영하며 이를 글로벌 네트워크로 배포함으로써 이러한 문제를 해결할 수 있다.

켄틱 포털의 SaaS APPs 성능 항목을 통해 조직의 내부 사용자들이 사용 중인 SaaS 애플리케이션 및 플랫폼에 성능 문제가 발생하는지 즉시 확인할 수 있다. 이를 통해 사용자 경험 문제의 근본 원인이 네트워크 내부에 있는지 아니면 외부에 있는지 파악할 수 있다.

■ 6단계 – 클라우드 네트워크 모니터링

클라우드 공급자 환경의 네트워킹 문제는 SaaS 네트워킹 성능 문제와 마찬가지로 사용자에게 심각한 문제가 될 수 있다. 이러한 문제를 방지하려면 자체 네트워크 인프라에 대한 모니터링에 사용되는 깊이와 세분성을 동일하게 적용해 공용 클라우드 네트워크 및 트래픽 흐름을 모니터링해야 한다.

클라우드 공급자의 네트워크, 인터넷 및 자체 온프레미스 네트워크 리소스 간의 관계를 추적하는 켄틱 맵은 이러한 가시성을 제공한다. 켄틱 맵은 이러한 모든 네트워킹 구성 요소의 토폴로지를 보여주며, 패킷이 공용 클라우드 영역, VPC, 서브넷 및 게이트웨이에 걸쳐 어떻게 이동하는지, 이러한 흐름이 사용자 환경의 네트워크 성능 및 사용자 경험에 어떠한 영향을 미치는지 파악할 수 있게 해준다.

■ 7단계 – 외부 네트워크 경로 분석

SaaS 애플리케이션이나 퍼블릭 클라우드 환경과 같은 외부 리소스에서 네트워크 문제를 감지하는 것은 사용자 경험을 최적화할 수 있지만, 나머지 문제는 감지하는 것만으로는 해결할 수 없다. 외부 네트워크에서 트래픽이 어떤 경로로 라우팅되는지, 네트워크 문제 발생 시 누구에게 연락해야 하며 어떻게 트래픽을 다시 라우팅하는지 정확하게 알아야 한다.

경로 분석(Path Analytics)은 이러한 가시성을 제공한다. 경로 분석은 추적 경로를 사용해 퍼블릭 인터넷과 같이 제어할 수 없는 네트워크의 트래픽 흐름을 분석하고 네트워크 각각의 경로별 다양한 서비스 공급자를 파악할 수 있다.

켄틱 신세틱스(Kentik Synthetics)의 패스 뷰(Path View) 메뉴는 이러한 가시성을 제공한다. 패스 뷰는 외부 네트워크의 홉 및 물리적 거리에 대한 데이터를 표시하며, 다양한 관점으로 외부 네트워크 경로를 분석해 시간순으로 경로가 어떻게 변경되는지 알려준다.

■ 8단계 – 네트워크 선제적 테스트

현대적인 네트워크 관리는 문제 발생 후에 조치하는 것 이상을 의미한다. 문제가 무엇인지 알 수 없거나 틀린 가정 하에 문제를 파악한다면 이미 그 자체로도 어려움을 겪게 될 것이다.

네트워크 관리는 네트워크를 지속적으로 테스트해 선제적인 조치를 취할 수 있어야 하며, 최종사용자에게 영향을 미치기 전에 사전에 문제를 파악할 수 있어야 한다. 이를 위한 가장 바람직한 방법은 테스트 시나리오 에뮬레이션(emulation)을 위한 신세틱 트래픽(Synthetic Traffic)을 생성하는 것이다.

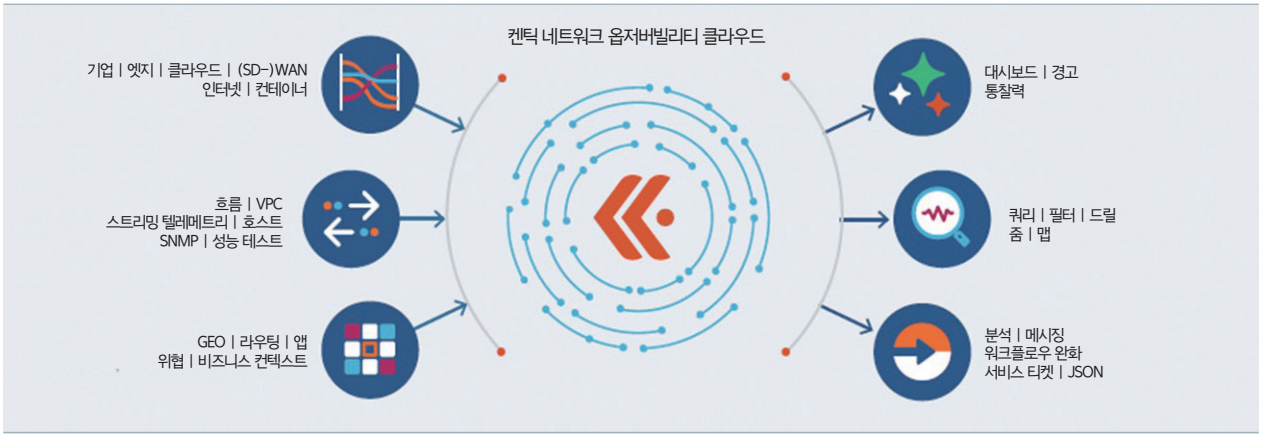
이러한 테스트는 페이지 로드 시간, 지터(Jitter), 패킷 손실, DNS 응답속도 및 API 요청 성능과 같은 네트워크 성능의 다양한 측면을 분석할 수 있어야 하며, 정확하게 분석해야 한다. 특히 사용하는 CDN 트래픽이나 요청이 시작된 지리적 위치 등의 구체적인 조건, 요소들을 토대로 네트워크 성능에 대해 평가할 수 있어야 한다.

켄틱 신세틱스는 페이지 로드 테스트를 통해 포괄적이고 세밀화된 테스트 기능을 제공해 네트워크 인프라에 대한 선제적 테스트를 쉽게 할 수 있다. 켄틱을 사용하면, SaaS 애플리케이션 성능, 주요 클라우드 네트워크, BGP 경로 및 DNS 성능을 모니터링하는 다양하고 종합적인 선제적 테스트 기능을 추가 비용 없이 바로 이용할 수 있다. 자체 네트워크에 대한 사용자 정의 테스트 라이브러리도 제공한다.

■ 9단계 – 넷옵스 수용

현재 네트워크 관리 조직은 독립적으로 업무를 진행할 수 없다. 네트워크 운영팀, 서버 운영팀, 개발자, 데브옵스(DevOps) 팀은 물론 기타 이해관계자들과 지속적으로 소통하고 협업해야 한다. 서로 다른 팀이 협업하며 네트워크와 기타 IT 업무가 상호 보완적으로 운영될 수 있도록 하려면 협업 전략이 반드시 필요하다.

〈그림 3〉 켄틱 네트워크 옵저버빌리티 클라우드 구성



넷옵스(NetOps)는 이러한 협업을 가능하게 하는 네트워크 관리 접근 방식이다. 네트워크 엔지니어와 기타 기술 이해 관계자는 옵저버빌리티처럼 네트워크 운영팀과 개발자 및 데브옵스 팀 모두에게 중요한 공유된 방법론을 활용해 동일한 언어를 사용하고 공통의 목표를 향해 노력해야 한다.

켄틱은 네트워크 옵저버빌리티 데이터를 켄틱에서 뉴렐릭, 스플렁크(Splunk), 프로메테우스(Prometheus)와 같은 데브옵스 옵저버빌리티 및 경고 도구로 전송하는 켄틱 파이어호스(Kentik Firehose) 등의 도구를 통해 넷옵스 운영 환경을 지원한다. 모든 이해관계자가 동일한 데이터로 작업하면 네트워킹이 더 광범위한 IT 목표에 어떻게 부합하는지 이해하는 능력을 최적화할 수 있다.

넷옵스와 데브옵스의 협업을 위해 켄틱은 켄틱 랩스(Kentik Labs)라는 개발자 커뮤니티를 구축해 오픈소스 네트워킹에 대한 정보를 공유하고 있다. 켄틱 랩스는 켄틱 파이어호스와 같은 일련의 오픈소스 프로젝트를 제공해 오늘날 네트워크 모니터링 기술에 존재하는 경계를 허무는데 일조한다. 이러한 오픈소스 프로젝트는 네트워크에서 발생되는 모든 문제에 대해 관측 가능하게 만들 때 필요한 정보를 누구에게나 공유될 수 있도록 커뮤니티를 활성화하고 있다.

■ 10단계 – 네트워크 관리 위한 AI옵스 수용

AI옵스(AIOps)는 AI와 머신러닝을 사용해 복잡한 IT 운영을 자동화할 수 있는 능력을 의미하며, 최근 몇 년 동안 IT 분야에서 화제가 되고 있다. 그러나 AI옵스는 단순히 일반적인 IT 운영 작업만을 위한 것은 아니며, 네트워크 관리에서 여전히 효과적일 수 있다.

켄틱과 같은 도구로 복잡한 네트워킹 데이터 세트에 대한 AI 기반 분석을 수행하면 엔지니어가 스스로 감지할 수 없는 문제를 파악할 수 있다. 또 복잡한 다계층 네트워크 내에서 성능 문제의 원인을 보다 신속하게 찾아낼 수도 있다.

네트워크 실시간 파악·제어 권한 확보

오늘날의 네트워크는 불과 2~3년 전과도 확연히 다르게 변화하고 있다. 가상 네트워크 인프라 환경으로의 변화 및 클라우드로의 전환은 기존 네트워크 기술과 도구가 현재의 IT 인프라 환경의 네트워크 성능 문제를 신속하게 감지하고 완화하기에 더 이상 충분하지 않다는 것을 의미한다.

해결 방안은 기존 네트워크 모니터링 기술에서 최신 네트워크 옵저버빌리티 기술로 전환하는 것뿐이다. 켄틱과 같은 플랫폼을 사용하면 엔지니어가 소유하고 있는 리소스와 외부 제조사가 제공하는 리소스를 포함해 모든 네트워킹 리소스 및 자산을 실시간으로 파악할 수 있다.

이를 통해 IT 조직은 네트워크 리소스에 대한 제어 권한을 확보할 수 있다. 또 조직의 네트워크 관리 전략이 비즈니스의 진행에 따라 지속적으로 진화하고 확장할 수 있다는 확신을 얻을 수 있다.