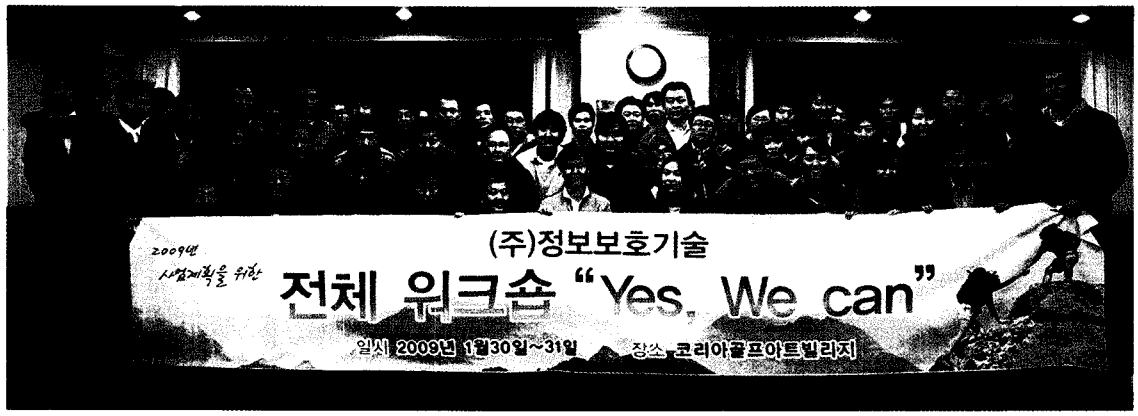
위협 수집기, TMS

국내 정보보호 기업의 약 60%는 벤처 창업 붐이 최고조에 달했던 1999년~2003년 사이에 설립됐다. '정보보호기술' 역시 약 10년 전인 2000년에 창업한 기업 중 하나다. 2000년 전후로 국내 IDS 시장이 활성화되던 당시 '테스(TESS) IDS'로 정보보호 제품을 선보인 정보보호기술은 기술력을 바탕으로 비교적 짧은 시간 내 정보보호 분야에서 탄탄한 기반을 다지게 된다. IDS를 통해 시장 점유율을 높이던 정보보호기술은 2004년 자체 IDS 개발 기술을 바탕으로 당시에는 생소했던 '위협관리시스템'을 내놓으며 신선한 바람을 일으켰다.

보안산업의 새로운 분야로 떠오른 위협관리시스템은 사후 대응이 아닌 위협요소에 대한 사전대응을 목표로 한 예/경보 시스템. 정보보호기술의 위협관리시스템 'TESS TMS(Threat Management System)'은 기존 IDS가 가진 분석기능과 모니터링 기능에서 출발했다.

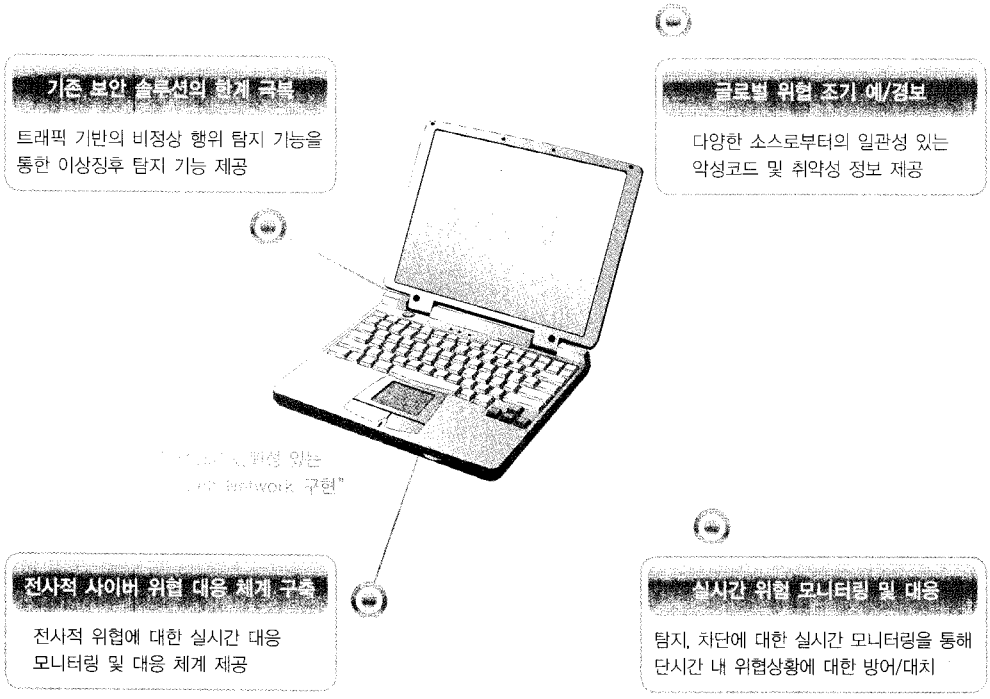
글 **김지숙** | 정보보호기술 과장 _ nanook5@infose.co.kr



TMS, 위협관리시스템

기존 침입탐지 및 방지제품인 IDS/IPS는 외부에서 내부로 유입되는 사이버 공격에만 초점을 맞춰 개발 운영된다. 하지만 최근 사이버 위협은 '내부 → 내부'로, '내부 → 외부' 등 방향성을 가리지 않을 뿐 아니라, 단순 패턴 매칭으로는 사이버 공격을 감지하기가 더 어려워지고 있다. 이 같은 위협에 대응하기 위해 2004년을 전후로 글로벌/로컬 위협을 상관분석하고, 단순 패턴 탐지 방식이 아닌 정규식 표현(PCRE : Perl Compatible Regular Expressions)과 같은 고도화된 탐지 기법 등을 적용해 사이버 위협에 대응하는 새로운 방식이 등장하기 시작했다.

만약 위협을 사전에 인지하지 못하고 피해가 발생된 이후 조치가 이뤄질 경우, 피해복구에 대한 대응조치 지연 및 복구비용은 기하급수적으로 증가할 것이다. 반대로, 잠재적인 위협요인을 조기에 감지하고 대응해 발생한 위협을 완화시키거나 확산을 막을 수만 있다면 IT 자산의 피해는 최소화될 수 있다.



▲ 테스 TMS의 주요 기능

그런데 소수의 보안 관리자가 많은 그리고 복잡한 정보 시스템과 네트워크에 출현하는 모든 위협을 판단하고, 또 위협이 내부의 보호자산에 미치는 영향을 단일 솔루션으로 분석하기란 현실적으로 불가능에 가깝다.

때문에 잠재 위협을 사전에 알리는 위협관리시스템이 갖춰야 할 첫번째 조건은 국내외 각종 위협 정보들과 실제 보호대상 인프라에 미치는 영향을 상관분석해 현재 그리고 미래의 위협을 예측하는 것이다. 위협관리시스템은 바로 위협의 발견, 위협의 활성화, 위협의 확산에서 소멸단계까지의 라이프 사이클을 관리하는 역할을 수행한다.

테스 TMS의 센서 및 위협분석시스템 – 테스 TAS 장비 ▶

TMS와 UTM의 만남

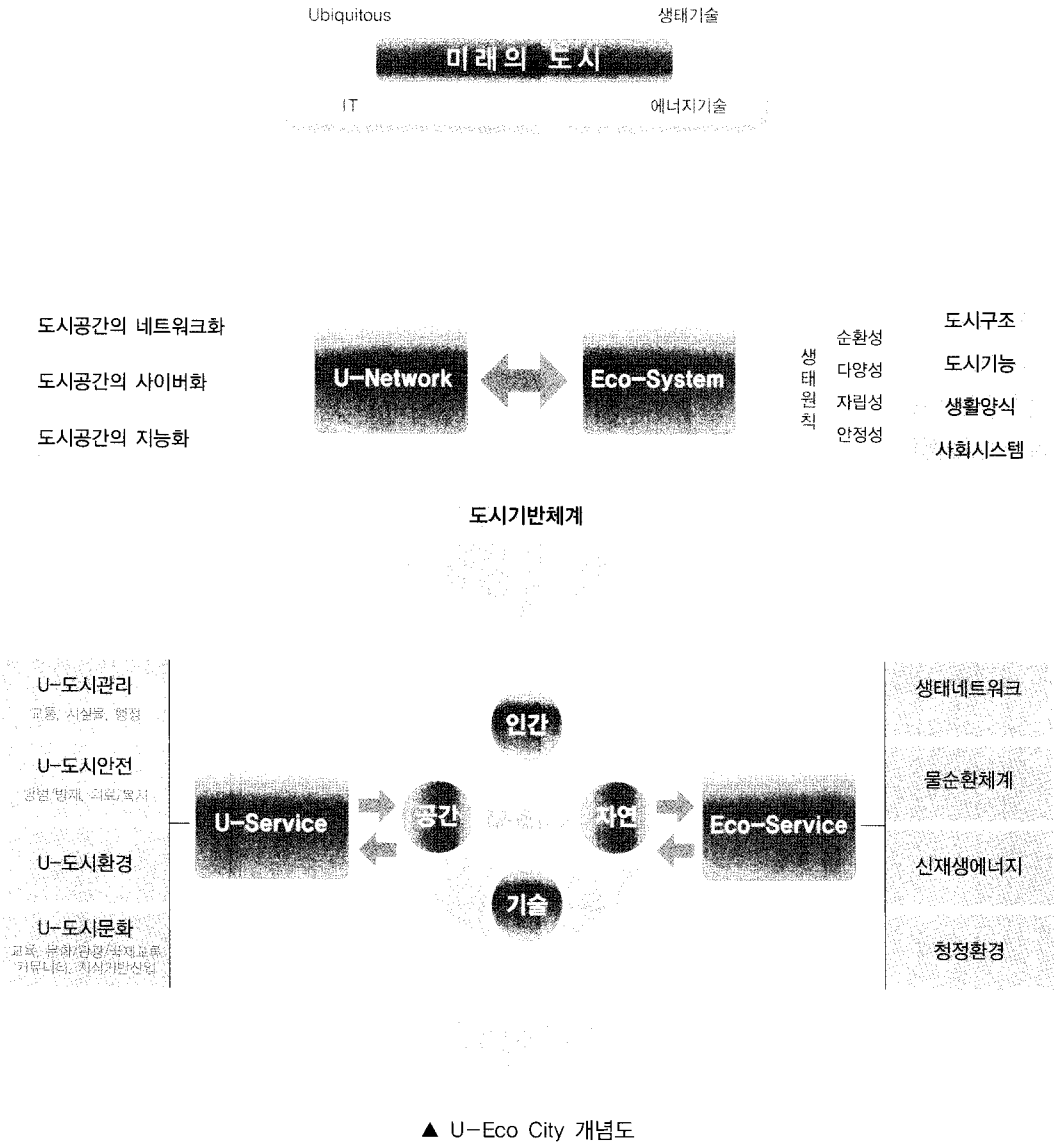
이런 사전 조기 예/경보 기능에 대한 관심이 높아짐에 따라 정보보호기술 TMS은 현재 국가 기간망을 비롯해 청와대, 국정원, 행정안전부, 외교통상부, 국토해양부, 보건복지부, 국방부 등 주요 정부부처의 보안관제 센터에서 통합보안 관제 시스템으로 활용되고 있다. 공공기관 뿐만 아니라, 내부 정보유출 방지가 필요한 민간기업 등에서도 제품 도입이 이뤄져 내부와 외부를 넘나드는 위협에 대처하고 있다.

특히, 지난 2008년에는 대형 기관 관리자들의 요구를 충족시켰던 모니터링 기능과 TMS의 주요 기능을 UTM 솔루션과 접목시키는데 성공, 중소 규모의 기업과 관공서에게까지 TMS의 기능을 제공할 수 있게 됐다.

TMS과 UTM의 연계는 본사와 지사의 관계에서 큰 장점을 지니고 있다. 가령, TMS를 구축한 본사가 지사에 구축된 UTM 장비를 통합적으로 모니터링하면서 조직 전체의 보안위협 현황을 모니터링할 수 있으며, 긴급 상황발생 시에는 실시간 차단정책을 적용할 수 있게 된다.

또한, 최근 건설교통부의 R&D VC-10 프로젝트 중 미래형 첨단 친환경 도시 'U-Eco City' 사업 수주를 통해 TMS 제품과 그 기술력을 유비쿼터스 사업에 직접적으로 응용 가능하게 됐고, 이를 발판으로 국내 네트워크 보안사업이 유비쿼터스 시장으로 진입하는 교두보를 확보했다.

◀ 정보보호기술 '테스 UTM' 500 장비



▲ U-Eco City 개념도

이와 같은 사업영역 확대를 바탕으로 정보보호기술은 기존 '테스 TMS'를 통해 유선 환경에 대한 보안 위협을 해소하는 것은 물론, 최근에 이슈가 되는 무선, USN 환경에 대비하기 위해 무선분야에 적용할 수 있는 TMS를 개발하고 있다. 이 같은 전략은 정보보호기술의 기술을 바탕으로 '유+무선' 모든 인프라에 대한 사이버 위협을 분석, 대응하겠다는 의지인 셈이다. **S**