情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

# 보안과 비즈니스 요구, 그리고 시각화(Visualization)

이 용 균*

요 약

정보의 시각화 연구는 결국 비즈니스와 연결되어 있다. 수많은 정보들로부터 비즈니스를 지켜내기 위한 거시적 관점의 시각화 요구를 충족하기 위한 노력이 필요하다. 기업의 다양하고 방대한 양의 위협정보들을 경영자의 의사결정과 행동에 옮길수 있도록 지원하는 수단으로서의 시각화 요구사항들을 살펴보고자 한다.

## Ⅰ. 서 론

비즈니스의 환경이 급속하게 변화하고 있다. 기업들은 자신들의 비즈니스가 어떻게 수행되고 있는지를 확인하기 위해 다양한 노력을 통하여 정보에 접근하고 분석하며 공유해 왔다. 비즈니스 인텔리전스(BI)는 개인들에게 다양한 원천으로부터 수집된 정보뿐만 아니라 분석 및 통계 예측 툴에서 얻은 정보를 제공하고 있다. 이런 결과로 보다 나은 운영 성과를 이끄는 향상된 의사결정이 가능해졌다. 즉, 비즈니스에 있어서의 거래 시스템들(transactional systems)에 의해 유지관리 되는 방대한 양의 데이터를 경영자에게 행동에 옮길 수 있는 정보로 전환하는데 도움을 주어 왔다.

한편 보안은 단순히 기술적인 요인이 아니라 기업의 흥망을 좌우할 수도 있는 엄청난 파괴력으로 등장하고 있다. 비즈니스를 위한 데이터 보호에 엄청난 비용과 노력이 소요될 수도 있는 지금의 보안 환경에서 기업들은 중대한 도전에 직면해 있다. 즉, 기업의 애플리케이션과 데이터베이스, 기타 일상적 기업 활동에 필수적인 비즈니스 자산에 영향을 미치는 모든 보안 문제들을 미리 처리하고 예방적으로 관리해야만 하며, 단편적인 보안 데이터를 통합, 정리하여 실질적인 BI로 활용할 수 있어야 한다. 또한, HIPAA (Health Insurance Portability and Accountability Act), 사베인스-옥슬리 법안 (SarbanesOxley Act), 신바젤협약 (Basel II), 세이프하버 가이드라인 (Safe Harbor) 등을 비롯한 여러 가지 관련 법규를 준수해야만 한다. 가장 중요한 것은 기업 환경 전반에 걸쳐 위험을 완화하는 한편으로 비용을 절감하고 운영 효율을 제공함으로써 비즈니스의 연속성을 보장하는 것이다.

이 같은 도전에 대응하기 위해서는 이제까지와는 다른 새로운 접근방식이 요구된다. 기업의 비즈니스 자산을 보호하는 다양하고 이질적인 요소들을 모아서 관리가 용이한 하나의 포괄적 솔루션으로 통합하는 새로운 보안 관리 모델이 필요한 것이다. 끊임없이 변화하는 보안 환경에서 새로운 보안 관리 모델은 비즈니스 요구에 부합하는 보안 관리가 가능하도록 예방적 관리와 실시간 대응을 요구한다.

기업의 조직 구조나 구체적인 비즈니스 모델에 따라 복잡한 보안 환경을 정확하게 이해하여 단순한 보안 데이터를 실질적인 정보로 바꾸고 중대한 문제에 대해 신속하게 해결방안을 도출하며 도출된 방안에 따라 예방적이고 적극적인 조치를 취하여 전사적 자산과 정보를 보호해 나가야 한다.

포괄적인 보안 관리를 통해 비용 절감, 시스템 중단 감소, 생산성 제고, 준법 경영 보장 등, 다양한 효과를 기대할 뿐 아니라 적시에 적절한 의사결정을 내릴 수 있는 방안 중 하나가 바로 실시간적인 정보 상황의 시각화가 아닌가 싶다.

정보 시각화(Information Visualization)는 비즈니스 인텔리전스 분야에서, 프리젠테이션 및 분석을 위한 중요한 역할을 담당 해왔다. 시각화에 대한

* ㈜이글루시큐리티 연구소장

사례들은 확실히 인기를 끌고 있다. 우리의 뇌는 시각 패턴들을 이해하는데 직관적이다. 그리고 패턴들은 관계를 설명한다. 뿐만 아니라, 관계에 대한 이해(고객 서비스와 고객 충성도 사이의 관계, 제품의 품질과 판매와의 관계 등)는 의사 결정을 이끌어 낼 수 있다. 따라서 정보 시각화를 올바르게 사용한다면 주요 비즈니스 관계를 이해하기 위한 능력을 향상시킬 수 있고 올바른 의사 결정을 할 수 있다.

## Ⅱ. 무엇을 보여줄 것인가?

오늘 신문에는 도대체 몇 개의 정보가 있을까? 기사 수만큼이라고 가정할 수 있을까? 내가 지금 읽고 있는 책에는? 장이나 절의 수 만큼 많은 기사의 단위가 있을까? 범위를 좁혀서 오늘 신문에 실려 있는 기사 하나에는 얼마나 많은 단위의 정보가 담겨 있을까?

정보경제학(Information Economics)에서는 정보가 경영에 있어서 어떻게 의사결정에 영향을 미치는지 연구해 왔다. 즉 가지고 있는 정보의 양 또는 질이 의사결정에 어떤 영향을 미칠까 라는 것이다. 이걸 알아 보는 가장 쉬운 방법은 특정한 정보를 가지고 있는 사람과 그렇지 못한 사람이 어떻게 다르게 행동하느냐를 비교연구해 보는 것이라고 한다. 이 특정한 정보는 어떻게 적시에 적합한 방법으로 제공되어야 하는데, 최근의 보안환경에 이보다 더 적용 가능한 모델이 있을까?

사실 기업 보안의 가장 어려운 문제 중 하나는 수많은 멀티벤더 보안 장치 및 시스템에서 발생하는 대량의 경보를 관리하는 것이다.

다양한 종류의 물리적 보안 및 IT 보안 시스템, 플랫폼, 애플리케이션 등이 쏟아내는 엄청난 양의 보안 데이터로 인해 이를 관리하기 위해 소요되는 비용은 크게 증가하고 있다. 각각의 보안 시스템과 플랫폼 및 애플리케이션은 제각기 정보를 생성하는 방식, 생성된 정보를 제공하는 포맷, 정보를 저장하는 장소와 보고 대상이 저마다 모두 다르다. 이처럼 상호 호환이 불가능한 이질적 보안 기술에서 쉴새 없이 쏟아져 들어오는 보안 데이터는 보안 정보의 과부하로 이어지고 비즈니스 운영에 부정적 영향을 미친다. 정보를 통합하고 관리할 수 있는 방법이 없다면, 이와 같은 파편화된 접근 방식은 결국 이중의 수고와 보안 비용 상승, 취약한 보안 모델 및 감사 기능의 실패를 초래할 뿐이다.

시각화는 정보경제학의 관점에서 볼 때 이러한 질문들에 대해 대답해 줄 수 있는 현실적 대안으로 주목받는 것은 어쩌면 당연한 일 일수도 있다. 그러면 시각화를 통해서 무엇을 보여 줄 것인가? 비즈니스를 위협하는 여러요소들의 변화추이에 따라 무엇을 보여줄 것인가에 대한 대답도 변화하고 있다.

큰 유형별 추이를 보면 위협요소의 민감도에 따라 이 변화의 흐름을 읽어볼 수 있다.

① 나의 비즈니스를 어디서 언제 누가 주로 이용하는가?
② 어떤 방법으로 악의적인 목적으로 접근 하는가?
③ 네트워크의 상황은 어떠한가?
④ 주요 자산과 그에대한 위협요소와의 종합적인 상관성은 어떠한가?
⑤ 내부정보의 유출을 종합적으로 감시할 수 있는가?

이러한 여러가지 요구는 수많은 정보로부터 실제적인 보안 위협을 나타내는 몇 가지 메시지를 구분하고, 이 메시지에 우선 순위를 부여하여 경영층에게는 경영지표(대쉬보드 등)의 형태로 실무자에게는 보안상황을 인지할 수 있는 실물의 형태로 보여주어야 할 것이다.

## Ⅲ. 어떻게 보여줄 것인가?

정보시각화는 정보검색과 관련하여 대량의 부정확한 정보에서 이용자가 요구하는 정보의 내용을 파악하기 쉽게 시각적으로 정리하여 표현하는 기법이다. 이때 정보의 재조직 및 시각적 표현 방식은 스크린이라는 제한된 영역에서 이루어지게 되므로, 이러한 제한된 공간을 어떻게 잘 활용하는가는 어떻게 이용자의 요구에 잘 부응하는 방식으로 조직되는가와 더불어 시각화 기법의 효용성을 결정하는 요소가 된다. 이러한 시각화 기법은 전달되는 정보의 종류와 정보를 처리하는 방법에 따라 분류될 수 있다.

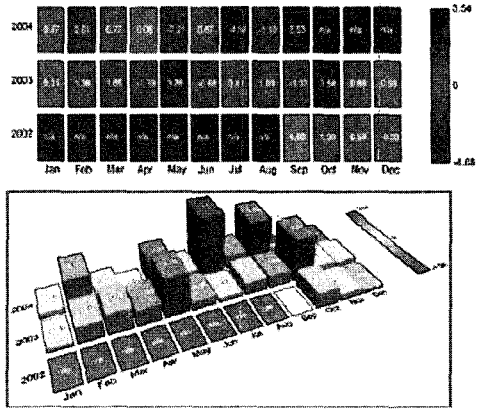
전달되는 데이터의 종류에 따라 텍스트를 주로 하는 1차원 데이터, 직사각형 등의 다각형 중심의 2차원데이터, 건축물이나 분자 구조와 같은 실세계의 개체를 표현하는 3차원 데이터, 개체들 사이의 계층구조를 표현하는 트리 구조데이터, 개체들 사이의 상호관계를 나타내는 네트워크 구조 데이터 등으로 나누어서 시각화 기법이 각각 다른 종류의 데이터에 따라 강조해야 하는 부분이 달라야 할 것이다. 1차원 데이터의 경우 시각화에 있어서 고려사항은 색깔, 크기, 폰트 등이며, 2차원 데이터는 인접 개체, 개체들 사이의 경로, 그리고 개체의 개수 등이 고려되어야 한

다. 3차원 데이터를 다룰 때 고려할 사항으로는 시각화 기법에서 이용자가 자신의 위치를 파악하도록 하는 것이 중요하며, 데이터를 처리하는 연산에 따라 시각화 기법을 나눌 수 있다. 이를 살펴보면 전체 정보공간의 개요를 제공하는 overview, 특정부분을 더 깊이 관찰하기 위한 zoom, 관심 대상에서 제외되는 개체를 제거하는 filter, 최종의 관심 대상을 선택한 경우 그 대상의 세부적인 사항에 대한 정보를 얻고자 할 때 사용되는 details-on-demand, 개체들 사이의 상호 관련성을 알아보고자 하는 relate, 이용자의 요구를 기록하고 저장해서 나중에 다시 조회하도록 하는 history등이 있다.

Jacob Nielson(1993)은 열 가지의 구체적인 항목으로 구성된 휴리스틱 평가방법을 개발하여 인터페이스의 이용성 평가에 사용할 수 있도록 소개하였는데, 이것을 어떻게 시각화할 것인지에 사용하여도 유용하리라 생각된다. Nielson에 의하여 제시된 휴리스틱은 다음의 〔표 1〕과 같다.

### 3.1 정보의 다차원 표현의 시각화

보여주어야 할 정보의 종류에 따라 어떤 방법을 사용했는지에 따라 그 효과가 다르게 나타나게 된다. 아래 그림에서와 같이 동일한 정보를 2차원의 매트릭스에서 3차원의 막대바를 사용하여 더욱 효과적인 정보의 시각화를 표현할 수 있다.

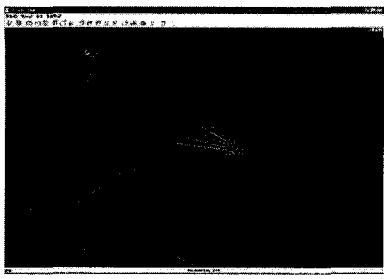


### 3.2 정보의 실시간 변화의 시각화

다음 그림은 대량의 정보에 대한 실시간 변화추이를 의미있는 도형이나 선으로 표현하여 상황을 인지할 수 있는 시각화 표현으로 많이 사용되는 방법으로 X,Y,Z 축을 이용한 선이나 점의 분포를 활용한 예이다.

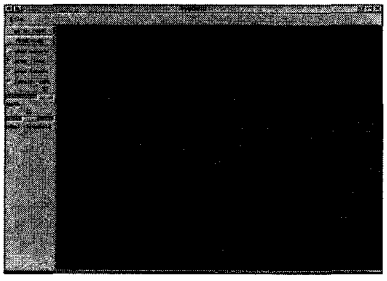
〔표 1〕 Nielson의 휴리스틱

| | |
|---|---|
| 휴리스틱-1 | 심미적이고 최소한의 설계 (Aesthetic and minimalist design) - 자주 이용되는 필요한 정보만으로 구성된 단순한 인터페이스인가 |
| 휴리스틱-2 | 시스템과 실제상황의 일치정도(Match between system and the real world) -이용자가 이해하기 쉬운 단어와 문장으로 표현 되었는가 |
| 휴리스틱-3 | 기억보다는 인식에 의존(Recognition rather recall) - 필요한 모든 기능이 쉽게 눈에 띄도록 구성 되었는가 |
| 휴리스틱-4 | 일관성과 표준화(Consistency and standards) - 같은 단어, 상황 등이 일관성 있게 사용 되었는가 |
| 휴리스틱-5 | 시스템 상황의 가시성(Visibility of system status) - 시스템이 이용자 요구를 처리 중이라는 표시를 해 주고 있는가 |
| 휴리스틱-6 | 시스템 조작의 용이성(User control and freedom) - 이용자가 길을 잃었을 때 원점으로 바로 전환할 수 있도록 해 주고 있는가 |
| 휴리스틱-7 | 이용자 수준에 맞는 인터페이스(Flexibility and efficiency of use) - 초보자, 전문가 등 이용자 수준에 맞추어 바로가기 등의 기능을 지원하고 있는가 |
| 휴리스틱-8 | 오류진단 및 처리(Help users recognize, diagnose, and recover from errors) - 이용자가 이해하기 쉬운 표현으로 오류에 대한 정보를 제공하고 처리방안을 제공하고 있는가 |
| 휴리스틱-9 | 오류방지(Error prevention) - 오류를 처음부터 방지할 수 있는 체계를 갖추었나 하는 것으로 이것은 발생한 오류에 대처하는 것보다 더 중요함 |
| 휴리스틱-10 | 매뉴얼 및 도큐멘테이션(Help and documentation) - 이용자의 작업을 지원하도록 적절한 표현과 양의 도큐멘테이션이 있는가 |



### 3.3 정보의 검색결과 시각화

다음 그림은 정보의 검색결과를 트리 형태로 시각화한 전형적인 사례이다.



## Ⅳ. 결 론

우리는 비즈니스에 있어서 가장 중요한 것은 적시에 적절한 사람에게 알맞은 정보를 제공하는 것이라고 믿고 있다. 비즈니스의 환경이 어떻게 변화하더라도 비즈니스 사용자들이 갖고 있는 기대는 순간적인 정보에서부터 최신의 정보까지 '적시의 정보'에 대한 기대는 늘어가고 있다. 분명한 것은 비즈니스에 있어서 정보의 가치는 더욱 중요해지고 있으며, 이를 종합적으로 분명하게 시각화해야 하는 것은 피할 수 없는 대세라는 것이다.

정보 시각화의 방향은 데이터, 사용자, 복잡성 세 가지 차원들에서 효과적으로 확장할 수 있어야 한다. 결국 사용자에게는 어떻게 보여질 것인가에 대한 View의 관점이지만 통상 분석되는 데이터양이 수백 기가에서 테라바이트까지 분석 가능한 엔진의 구조 또한 중요한 연구분야 이기도 하다.

정보 특히 보안의 시각화 연구는 상대적으로 해외에 비해서 수준도 낮으며, 연구 역사도 일천하다. 하지만 최근의 시각화에 대한 뜨거운 관심을 지속하기 위한 끊임없는 열정과 방법들이 시도되기를 기대한다.


### 〈著 者 紹 介〉

**이 용 균 (Lee Yong-Gyun)**

1986년 인하대학교 전자계산학과 졸업
2006년 고려대학교 정보보호대학원 석사 4학기 재학중
2000년~현재 이글루시큐리티 보안연구소 연구소장
관심분야 : 통합보안관리, 공격수준 평가, 보안상황 시각화