韓國컴퓨터情報學會 論文誌
第16卷 第12號, 2011. 12.

2011-16-12-5-3

# 국가 정보보호 지수 산출을 위한 OLAP 데이터베이스 시스템의 구축

최 정 우*, 최 인 수**

# Development of an OLAP Database System for Calculating National Information Security Index Numbers

Jung-Woo Choi *, In-Soo Choi **

## 요 약

UN, OECD, ITU 등 국제기구들은 정기적으로 정보 정책을 수립하고 평가하는데 활용하기 위한 목적으로 정보화 지수를 발표한다. 정보화 지수는 국가의 정보 정책의 수행능력을 평가하고 미래에 진행할 정부의 정보화 프로젝트를 선택하기 위한 기준으로서 활용된다. 정보 시스템이 고도화됨에 따라 이와 더불어 정보보안 역시 그 중요성이 부각되고 있는 실정이고, 이에 따라 국가 정보보호 지수의 산출이 필요하게 되었다. 정보 보안 지수는 특정 그룹의 정보 보안의 특성을 가장 명확하게 표현하는 공식 수치 값이며, 이는 정부의 정보 보안 정책을 결정하는데 이용된다. 국가 정보보호 지수를 산출하는 데에는 현재 설문지 조사방법이 사용되고 있는데, 이 방법으로는 충분한 통계자료를 확보하기 어려우며 그 자료의 신뢰성 또한 높지 않다는 문제점이 존재한다. 본 연구에서는 이를 해결하기 위해 기존의 설문지 조사방법이 아닌 개별 기업의 정보보호 수준에 관한 원시데이터를 정확하게 수집할 수 있는 새로운 방법을 제시하고, 다음으로 원시데이터를 근간으로 하여 머크로 데이터를 얻어 정책 의사결정을 할 수 있는 OLAP 데이터베이스 시스템을 구축하는 것에 목적을 두고 있다. 현 OLAP 체제에서는 모든 계층구조 스키마가 분배적으로 되는 경우에만 제대로 집계데이터를 구할 수 있기 때문에 본 연구에서는 사례의 비 분배적 계층구조 스키마를 분배적 스키마로 변환하여 국가 정보보호 지수를 산출하는 OLAP 데이터베이스 시스템을 구축하였다. 본 연구에서 제안하는 방법은 구현의 관점과 스키마 설계의 관점에서 볼 때에 유용한 방법이 되리라 생각한다.

▸ Keyword : 정보보호지수, 설문지 조사, 계층구조 스키마, 합계가능, 분배적, 비분배적, OLAP 데이터베이스 시스템

## Abstract

UN, OECD, ITU and other international organizations regularly announce ISI (Information

• 제1저자 : 최정우 • 교신저자 : 최인수
• 투고일 : 2011. 09. 27, 심사일 : 2011. 10. 04, 게재확정일 : 2011. 10. 08.
* 숭실대학교 대학원 산업·정보시스템공학과 박사 과정 (In a Ph.D. program of Industrial & Information Systems Engineering, Soongsil Univ.)
** 숭실대학교 산업·정보시스템공학과 교수 (Professor of Industrial & Information Systems Engineering, Soongsil Univ.)

Society Index) to utilize in establishing and evaluating information policies. ISI is utilized as important data for countries to evaluate their information policy performance and select future projects. As the advancement of information systems, the importance of information security has been emerged. Accordingly, NISI (National Information Security Index) has been required. NISI number is the most clearly figure to express the characteristics of a particular group's information security. It can be utilized in determining information security policies. Currently, questionnaire method has been used to calculate NISI number. But there is an absolute lack of statistical data, and the reliability of surveyed statistical data is problematic. The objective of this paper is to show how to collect precise micro data of each company's information security index numbers, and to develop an OLAP database system which calculating NISI numbers by using those micro data. In this process of the survey, we presented the technique to collect the data more systematically, and to analyze the data without using questionnaire method. OLAP architecture performs only well on the facts that are summarizable along each dimension, where all hierarchy schemas are distributive. Therefore we transformed the non-distributive hierarchy schema into the distributive hierarchy schema to implement OLAP database system. It is thought that this approach will be useful one from an implementation and schema design point of view.

▸ Keyword : Information Security Index, questionnaire, Hierarchy schema, Summarizable, Distributive, Non-distributive, OLAP database system

## Ⅰ서 론

오늘날 정보화의 고도 진전에 따라서 개인과 기업이 인터넷과 정보기술을 활용하고 의존하는 정도가 급속도로 높아지고 있다. 그러나 이러한 정보화의 고도 진전에 수반되어 정보보호 측면에서 해킹이나 컴퓨터 바이러스 등의 부작용도 날로 증가되어서 사회전반에 막대한 경제적 손실을 낳고 있는 것도 현실이다. 따라서 세계 최고의 인터넷 인프라를 자랑하며 인터넷에 대한 의존도가 높은 우리나라는 기술적, 정책적으로 이러한 부작용에 대한 보다 철저한 대처가 필요한 상황이다[1].

먼저 기술적으로 대처하기 위해서는 국내 개별 기업의 정보보안 상태에 대해, 다른 말로 하면 국내 개별 기업의 정보보호 수준에 대해 정확하게 이해할 필요가 있다. 현재 많은 기업이 자사의 시스템 및 네트워크를 악의적인 공격으로부터 보호하기 위해 네트워크, 시스템, 애플리케이션, 데이터베이스 등에 각종 보안 솔루션과 관련 기술을 도입하고 운영하고 있는데, 이에 대한 실태조사를 정부에서는 기업설문조사방법을 통해 수행해왔고, 이 설문조사 결과를 기업의 정보보호 수준 평가와 국가정책 개발의 기초자료로 활용하고 있다. 그러나 설문지를 통한 위와 같은 조사방법은 현재 널리 행하여지고 있는 방법이기는 하지만 그 정확성에는 한계가 있다[2],[3].

설문지 조사방법에서는 해당 응답자가 자의적 판단에 의하여 해당 질문의 내용을 정리하고 판단하여 그 결과 값을 기입하게 되는데 이때 이 결과 값이 왜곡되고 변조될 가능성이 있다. 왜냐하면 객관적인 사실 값이 기록되어야 함에도 불구하고, 응답자의 자의적 판단에 따른 결과 값이 기록되기 때문이다. 즉 사실을 정량화하고 표준화하는 권한의 주체가 설문의 응답자가 되기 때문에 사실이 왜곡되고 변조된다는 뜻이다. 설문지 방법을 통한 조사로는 국내 개별 기업의 정보보호 수준에 관한 데이터, 즉 원시데이터(micro data)를 정확하게 수집할 수 없는 한계가 있음을 알 수 있다.

다음으로, 정부가 정보보호 관련 예산을 어느 정도 확보해야 하는지, 정보보호교육과 홍보활동을 어떻게 추진해야 하는지와 같은 정책적인 대처를 하기 위해서는 우선적으로 개별기업의 정확한 실태조사가 이루어져야 한다. 개별기업 데이터 즉, 원시데이터를 모아 머크로 데이터(macro data)를 얻음으로써 정책 의사결정을 하게 되는데 여기서 원시데이터를 설문지 조사방법을 통해 수집할 경우 이 원시데이터는 상술한 바와 같이 왜곡되고 변조될 수 있으며 결과적으로 머크로 데이터까지도 왜곡되고 변조되어 효과적인 정책의사결정을 하지 못하게 된다.

본 연구에서는 먼저 설문지 조사방법이 아닌 개별기업의 정보보호 수준에 관한 원시데이터를 정확하게 수집할 수 있는 새로운 방법을 제시하고, 다음으로 원시데이터를 근간으로 하

여 머크로 데이터를 얻어 정책의사결정을 할 수 있는 OLAP(online analytical processing) 데이터베이스 시스템을 구축하는 것을 목적으로 하고 있으며, 이는 구현의 관점과 스키마 설계의 관점에서 볼 때에 유용한 방법이 되리가 생각된다.

## II 관련 연구

### 1. 국내 기업의 정보보호 실태조사 현황

국내 민간기업의 정보보호 정책 및 조직 구성 현황, 역기능 대응실태와 정보화 역기능 피해현황 등을 종합적으로 파악함으로써 국내 기업의 정보보호 수준을 측정 하고 정보보호 관련 정책 수립의 기초자료로 활용하기 위해 한국정보보호진흥원에서는 2001년부터 매년 정보보호 실태조사를 실시하여 왔다. 2011년에는 방송통신위원회와 한국인터넷진흥원(KISA)에서 우리나라의 전반적인 정보보호 수준을 평가 산출한 『2010년 정보보호지수』를 발표한 바 있다.

정보보호 실태조사의 실시목적은 국내기업의 정보보호 현황 조사를 통해 국내 정보보호 수준평가 및 정책개발의 기초자료로 활용하기 위함에 있으며, 또한 정보보호 관련 세부지표의 지수 산출의 기초 데이터로 활용함에 있다. 실태조사의 결과는 국가정보보호백서, 한국인터넷백서 등에 소개되고 있다. 종사자수 5인 이상의 네트워크 구축 사업체 6,529개를 2010.9.1~2010.10.31까지 약 2달간 전산담당자 및 총무담당자를 대상으로 하여 방문 면접 조사를 실시한 것이 2010년 기업 정보보호 실태조사이다[4].

정부는 상기 조사에서 수집된 데이터를 기초로 하여 표 1의 정보보호 지표의 분류 체계에 따라 각 지표의 지수를 산출하고 있다. 정보보호라는 대분류 지표는 정보보호 기반 지표와 정보보호 환경지표로 중분류 되고 있으며, 이 중 정보보호 기반 지표는 백신이용률, 보안패치 설치률, 공인인증서 보급률, 방화벽(Firewall) 보급률, 침입탐지/차단시스템(IDS/IPS) 보급률, 보안서버 보급률 등 총 6개의 세부 지표로 분류되고, 정보보호 환경 지표는 정보보호 예산 비율, 정보보호 전문 인력 비율, 국민 보안의식 수준 등 총 3개의 세부 지표로 분류되고 있다.

이러한 정보보호실태조사와 정보보호 지수 산출결과를 토대로 하여 정보보호 관련 예산을 확보하고, 정보보호 인식제고를 위한 교육을 실시하고, 홍보 활동 등의 추진계획을 수립하며, 국가보안정책을 수립하고 있으며, 정보보호 취약계층에 대한 관련 지원을 강화하고 보안수준을 향상시킬 수 있는 방안을 마련하고 있다.

표 1. 정보보호 지표의 분류
Table 1. A Classification of Information Security Indices

| 대분류 지표 | 중분류 지표 | 세부 지표 |
|---|---|---|
| 정보보호 | 정보보호 기반 | 백신 이용률 |
| | | 패치 설치률 |
| | | 공인인증서 보급률 |
| | | Firewall 보급률 |
| | | IDS/IPS 보급률 |
| | | 보안서버 보급률 |
| | 정보보호 환경 | 정보보호 관련 예산 비율 |
| | | 정보보호 전문인력 비율 |
| | | 국민의 보안의식 수준 |

### 2. 설문지 조사방법의 한계

전술한 바와 같이 해당 기업체의 전산 또는 총무 담당자들이 작성한 설문지에 근거하여 여러 지수를 산출하고 있는데, 이때 사용한 설문지 중 정보보호 기반지수 산출용 2010년도 설문지를 살펴보면 표 2 와 같다.

문12 귀 사(귀 기관)에서 현재 운영 중인 정보보호 제품은 다음 중 어떤 것이 있습니까?

표 2. 기업정보보호 실태조사를 위한 설문지 양식
Table 2. A Questionnaire for the Survey of Company Information Security

| 구분 | 제품명 | 사용여부 | | | |
|---|---|---|---|---|---|
| (가) 접입차단 시스템 | 1. 웹 방화벽 | □ | (사) Anti Virus | 1. Virus 백신 | □ |
| | 2. 네트워크(시스템) 방화벽 | □ | | 2. Anti 스파이웨어 | □ |
| | 3. PC 방화벽 | □ | | 3. Anti 피싱 | □ |
| (나) 접입방지 시스템 | 1. 접입방지시스템(IPS) | □ | (아) Anti Spam | 1. 스팸차단 S/W | □ |
| | 2. 접입탐지시스템(IDS) | □ | (자) 보안 운영체제 | 1.보안운영체제(Secure OS) | □ |
| | 3. Ddos 차단시스템 | □ | (차) 통합 PC보안 | 1. PC보안(내부정보유출방지) | □ |
| (다) 통합보안 시스템 | 1. 통합보안시스템(UTM) | □ | | 2. 보안 USB | □ |
| (라) 보안관리 | 1. 기업보안관리(ESM) | □ | (카) DB/컴텐츠 보안 | 1. DB 보안 | □ |
| | 2. 위협관리시스템(TMS) | □ | | 2. DB 암호 | □ |
| | 3. 패치관리시스템(PMS) | □ | | 3. 디지털저작권관리(DRM) | □ |
| | 4. 자산관리시스템(RMS) | □ | (타) 공개키 기반구조 | 1. 공개키기반구조(PKI) | □ |
| | 5. 로그 관리/분석 툴 | □ | (파) 접근관리 | 1. 네트워크 접근제어(NAC) | □ |
| | 6. 취약점 분석 툴 | □ | | 2. 통합접근관리(EAM) | □ |
| (마) 가상사설망 | 1. 가상사설망(VPN) | □ | | 3. 싱글사인온(SSO) | □ |
| (바) 인증제품 | 1. 보안 스마트카드 | □ | | 4. 통합계정관리(IM/SAM) | □ |
| | 2. H/W 토큰(HSM) | □ | (하) 기타 | 1. 무선랜인증(WLAS) | □ |
| | 3. 일회용비밀번호(OTP) | □ | | 2. 기타 | □ |
| | 4. 바이오인식시스템 (Biometrics) | □ | | | |

표 2 설문지의 2010년도 응답결과는 그림 1과 같다[4]. 그림 1(a)에서는 전체 6,529개의 조사기업 중 87.1%의 기업 Virus 백신 제품을 사용하고 있다는 것을 나타내고 있고, 그림 1(b)에서는 서버 보유사업체 중 76.0%가 웹방화벽 제품을 사용 하고 있다는 것을 설명하고 있다.


그림 1. 정보보호제품 사용현황
Fig. 1. Usage Rate of Information Security Solutions
(a) All Participants
(b) Server Operating Participants

설문조사용 설문지 작성에는 다음과 같은 점을 고려해야 한다. 첫 번째로 설문 응답자의 정보인지 가능성에 대한 고려가 필요하다. 설문내용을 응답자가 잘 모르는 경우는 엉뚱한 응답을 얻을 가능성이 높기 때문이다. 두 번째로 응답의 난이도를 적절히 고려해야 한다. 응답자가 정보를 가지고 있더라도 응답을 하기 위해서 시간적으로 많은 노력이 필요하면 응답을 회피하거나 무성의한 응답을 할 가능성이 높다. 세 번째로 응답자의 정보제공 가능성에 대한 예측이 필요하다. 회사 기밀이 공개되는 것을 두려워하여 응답을 회피하거나 거짓 응답을 할 가능성이 존재하기 때문이다. 설문결과의 정확성과 무결성을 확보하기 위해서는 위와 같은 사항들을 고려해야만 한다[5],[6].

표 2의 설문문항은 해당 기업이 도입하고 있는 정보보호제품의 종류와 효과를 알아보기 위한 문항이다. 설문 응답자가 자기 기업이 도입하고 있는 제품이 있으면 이를 기입하는 방식인데 이와 같은 경우 상술하였던 첫 번째 경우인 설문 응답자의 정보인지 가능성에 대한 고려가 필요하다. 설문 응답자는 해당 설문 문항에 대한 모든 내용에 정확한 답변을 할 수 있는 기반지식을 보유하고 있어야 정확한 답변을 할 수 있다. 표 2의 설문 항목에 따르면 각 보안기능을 담당하는 제품 보유의 여부에 대하여 설문 응답자는 해당 내용을 기입하여야 하는데 이때 설문 응답자가 답변하기에 어려운 문제점이 하나 존재한다. 근래에는 보안제품의 제공기능이 다양화, 다변화되는 추세이다. 즉 통합보안제품이나 다기능을 제공하는 제품들이 많이 등장하고 있다는 뜻이다. 응답자가 이러한 다기능 제품에 대한 충분한 인식을 하지 못하면 표 2에서의 해당 기능을 정확하게 기입할 수 없게 된다.

두 번째로 응답의 난이도 부분에 대해 고려하여 볼 때, 설문 응답자는 해당 기업의 전체 보안제품 리스트를 가지고 있지만 각 제품의 명칭만으로는 해당 제품의 전체 기능을 알지 못 하는 경우도 있다. 이런 경우에는 전체 보안제품 리스트와 각 제품별 설명서, 매뉴얼 등을 면밀히 숙지하여야만 정확한 설문의 응답이 가능할 것이며, 이러한 과정을 번거롭고 힘들게 느끼는 설문 응답자들은 자연스레 응답을 회피하거나 무성의하게 응답할 가능성이 높아지게 된다.

마지막으로 응답자의 정보제공 가능성에 대한 예측부분을 고려하여 볼 때, 설문의 응답자가 기업의 보안제품에 대한 항목은 곧 기업의 보안척도로 비추어질 것이라 판단하여 사실의 내용보다 부풀려 설문에 응하거나, 또는 이와는 반대로 기업의 비밀에 속하는 내용이라 자의적으로 판단하여 응답 자체를 회피하거나 축소하여 설문에 응할 가능성도 존재한다.

이와 같은 여러 단점을 보완하기 위해서 본 연구에서는 설문지 조사방안 대신 개별 기업이 정부기관에 보고하는 보안제품보유목록 만으로 해당 기업 전체 정보보안 기능을 조사할 수 있는 방안을 제시하고 있다. 먼저 국내 모든 보안제품에 대한 기능을 명세화 한다는 가정 하에, 이 기능 명세를 활용하여 개별 기업이 보유하고 있는 보안 제품의 기능에 관한 정확한 원시 데이터를 수집하고 있다. 이러한 원시 데이터를 근

간으로 하여 개별기업이나 기업군의 정보보호 성취도와 같은 머크로 데이터를 얻어 정책 의사결정을 할 수 있는 OLAP 데이터베이스 시스템을 구축하고자 하는 것이다. 이하 장에서는 OLAP 데이터베이스 시스템의 설계와 구현에 대하여 기술하고자 한다.

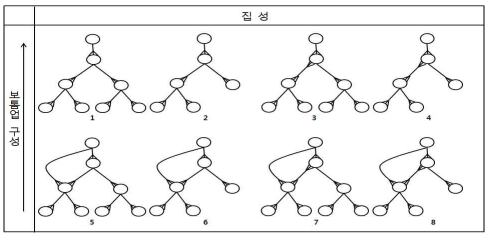
## III 정보보호 지수 산출을 위한 OLAP 시스템 설계

### 1. 계층구조 스키마의 분류

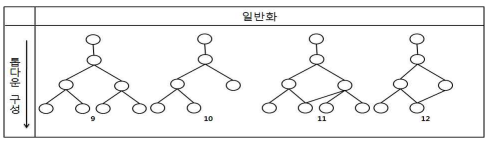
데이터 큐브(data cube)는 집계(summarization) 데이터 자체인 여러 큐브 뷰(cube view)가 모인 것인데, 여기서 큐브 뷰는 해당 차원 모두에 걸쳐 각 차원의 수준을 조합시켜서 얻게 되는 격자점에서 집계한 데이터로 형성되게 된다. OLAP 지향 다차원 데이터 모델(multidimensional data models)에서의 각 차원에는 해당 차원의 수준들을 DAG(directed acyclic graph)로 표현한 어떤 구조가 있기 마련인데, 이러한 구조를 계층구조 스키마라 부른다. 계층구조 스키마에 있는 각 수준에는 여러 개의 멤버가 있을 수 있으며, 이들 멤버 간에는 부모/자식 관계(child/parent relation)가 맺어져 있다[7-9].

OLAP에서 일컫는 합계가능조건(summarization conditions)이란 어떤 하나의 큐브 뷰를 다른 여러 큐브 뷰로 부터 정확하게 이끌어 낼 수 있는 조건을 말하는데, 이러한 합계가능조건을 만족시키기 위해서는 데이터 큐브가 분배적(distributive)이 되어야만 한다. 좀 더 구체적으로 말할 것 같으면, 계층구조 스키마가 분배적이어야 한다는 뜻이다[10-12].

현 OLAP 체제에서는 모든 계층구조 스키마가 분배적으로 되는 경우에만 제대로 집계 데이터를 구할 수 있는데[13], 실제로 실세계를 개념화할 때에는 서로 다른 여러 종류의 비분배적 계층구조 스키마가 발생하게 된다. 저자들의 이전 연구[14]에서는 실세계를 개념화할 때 발생하는 모든 계층구조 스키마를 일반화(generalization)에서 4가지, 집성(aggregation)에서 8가지의 총 12가지 계층구조 스키마로 분류한 바 있다. 이 중, 집성에서의 8개 계층구조 스키마는 한 개의 분배적 계층구조와 일곱 개의 비분배적(non-distributive) 계층구조 스키마로 분류되어 있다(그림 2 참조).




(a) ID1, ID2, ID3, ID4, ID5, ID6, ID7, ID8




(b) ID9, ID10, ID11, ID12

그림 2. 계층구조 스키마

Fig. 2. Hierarchy Schemas

### 2. 차원 테이블의 설계

본 연구에서는 정보보호 지표체계 중 정보보호 기반 분류의 세부 지표에 관한 지수 산출을 할 OLAP 시스템을 설계하고 구현하고자 한다. OLAP 시스템을 구현하자면 여러 차원 테이블을 설계해야 하는데, 본 연구에서는 FUNCTION 차원 테이블, PRODUCT 차원 테이블, COMPANY 차원 테이블, TIME 차원 테이블과 같은 4개의 차원 테이블을 설계하고 있다(표 4, 표 5, 표 6, 표 7 참조).

표 3. 정보보안제품의 분류

Table 3. Classification of Information Security Products

| 대분류 | 소분류 | 기호 | 세부 항목 |
|---|---|---|---|
| 정보보안 제품 | 네트워크 보안 | A | 1. 웹방화벽 |
| | | | 2. 네트워크(시스템) 방화벽 |
| | | | 3. 침입장비시스템(IPS) |
| | | | 4. DDoS 차단 시스템 |
| | | | 5. 통합보안시스템(UTM) |
| | | | 6. 가상사설망(VPN) |
| | | | 7. 네트워크접근제어(NAC) |
| | | | 8. 무선/모바일 보안 |
| | 시스템 보안 | B | 1. PC 방화벽 |
| | | | 2. Virus 백신 |
| | | | 3. Anti 스파이웨어 |
| | | | 4. Anti 피싱 |
| | | | 5. 스팸차단 S/W |
| | | | 6. 보안운영체제 |
| | 컨텐츠/정보유출 방지보안 | C | 1. DB 보안 |
| | | | 2. DB 암호 |
| | | | 3. PC 보안 |
| | | | 4. 보안 USB |
| | | | 5. 디지털저작권관리(DRM) |
| | 암호/인증 | D | 1. 보안스마트카드 |
| | | | 2. H/W토큰(HSM) |
| | | | 3. 일회용비밀번호(OTP) |
| | | | 4. 공개키기반구조(PKI) |
| | | | 5. 통합접근관리(EAM) |
| | | | 6. 싱글사인온(SSO) |
| | | | 7. 통합계정관리(IWIAM) |
| | | | 8. 공인/사설 인증 툴 |
| | 보안관리 | E | 1. 기업보안관리(ESM) |
| | | | 2. 위험관리시스템(TMS) |
| | | | 3. 패치관리시스템(PMS) |
| | | | 4. 자산관리시스템(RMS) |
| | | | 5. 로그 관리/분석 툴 |
| | | | 6. 취약점 분석 툴 |
| | 기타 제품 | F | 1. 기타 |

먼저 FUNCTION 차원 테이블은 2010 국내 정보보안산업 실태조사[15]에서의 정보보안 제품의 분류(표 3 참조)를 기반으로 하여 설계하였다. 왜냐하면 이 분류는 한국인터넷진흥원이 국내 모든 보안제품을 대상으로 한 최근의 제품 분류이기 때문이다. 표 3에 표 3에서의 기타항목을 제외한 33개 세부항목을 잎멤버(leaf member) 즉 Level3의 멤버로 삼고, 상위 Level2 수준을 추가함으로써 본 연구의 FUNCTION 차원 테이블을 설계하였다(표 4 참조). FUNCTION 차원 테이블의 Level3는 제품이 아닌 기능으로 되어 있음에 유의하기 바란다. 이 이유는 많이 공급되고 있는 다기능 제품을 처리하기 위해서 이다. 본 연구에서는 FUNCTION 차원 테이블의 Level3를 기능 단위로 삼고, 이 Level3와 제품을 연계시키는 방법을 통해서 다기능 제품에서의 문제를 해결하고 있다. 본 연구에서는 FUNCTION 차원 테이블의 Level3와 제품을 그림 4와 같이 연계시키고 있다. 각 보안 제품은 33개의 기능 중 한 개 이상의 여러 기능을 갖게끔 연계 시킨 것을 그림 3의 점선 안에 표시하였다. 여기서 PRODUCT : FUNCTION의 최대 카디널 수는 N:M이다. 이 N:M의 최대 카디널 수를 1:N으로 변환시킴으로써, 즉 분배적 계층구조 스키마로 변환시킴으로써 본 연구에서의 OLAP 시스템을 구현시키고자 하는 것이다. 이 구현과정을 Ⅳ장에서 기술하고자 한다.

나머지 PRODUCT 차원 테이블, COMPANY 차원 테이블, TIME 차원 테이블은 다음과 같다.

PRODUCT(ProductID, ProductName, Manufacturer)

COMPANY(CompanyID, CompanyName, IndustryType)

TIME(TimeID, Quarter, Year)

표 4. FUNCTION 차원 테이블
Table 4. FUNCTION Dimension Table

| Function ID | Level3 | Level2 | Level1 |
|---|---|---|---|
| 1 | Web Firewall | 내/외부 보안 | 네트워크보안 |
| 2 | System Firewall | 내/외부 보안 | 네트워크보안 |
| 3 | IPS | 내/외부 보안 | 네트워크보안 |
| 4 | Anti-DDoS | 내/외부 보안 | 네트워크보안 |
| 5 | UTM | 내/외부 보안 | 네트워크보안 |
| 6 | Wireless Security | 내/외부 보안 | 네트워크보안 |
| 7 | VPN | 접근통제 | 네트워크보안 |
| 8 | NAC | 접근통제 | 네트워크보안 |
| 9 | ESM | 관제시스템 | 보안관리 |
| 10 | TMS | 관제시스템 | 보안관리 |
| 11 | PMS | 관제시스템 | 보안관리 |
| 12 | RMS | 관제시스템 | 보안관리 |
| 13 | 로그관리/분석툴 | 분석툴 | 보안관리 |
| 14 | 취약점 분석툴 | 분석툴 | 보안관리 |
| 15 | DB 보안 | DB 유출방지 | 컨텐츠/정보유출방지 보안 |
| 16 | DB 암호화 | DB 유출방지 | 컨텐츠/정보유출방지 보안 |

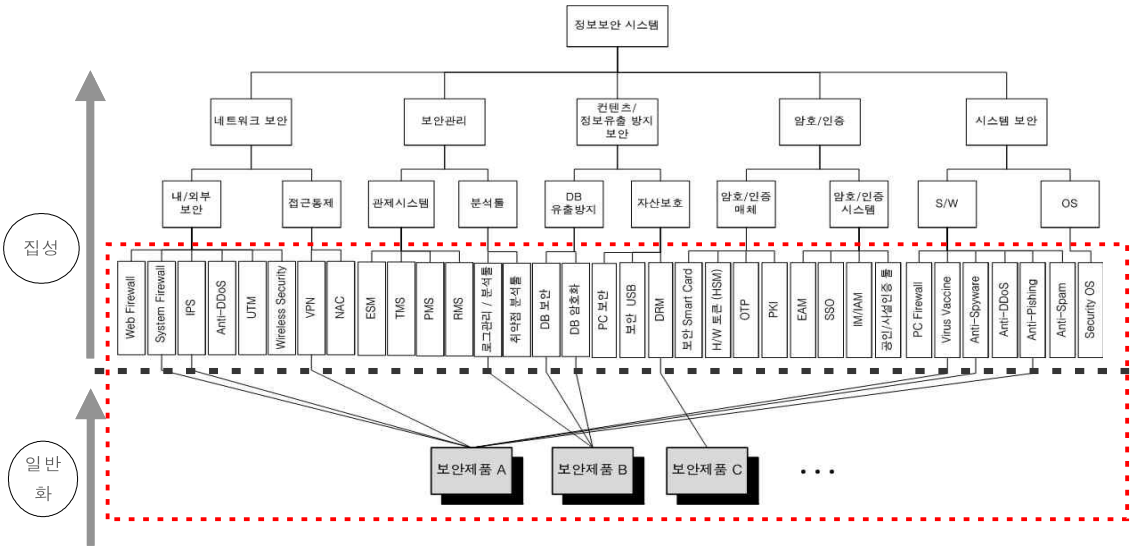



그림 3. 기능의 집성 계층과 제품의 포괄적 일반화 계층의 연계
Fig. 3. Connection of the Function Aggregation Hierarchy and the Inclusive Product Generalization Hierarchy

| | | | |
|---|---|---|---|
| 17 | PC 보안 | 자산보호 | 컨텐츠/<br>정보유출방지 보안 |
| 18 | 보안 USB | 자산보호 | 컨텐츠/<br>정보유출방지 보안 |
| 19 | DRM | 자산보호 | 컨텐츠/정보유출방지<br>보안 |
| 20 | 보안<br>SmartCard | 암호/인증매체 | 암호/인증 |
| 21 | H/W<br>토큰(HSM) | 암호/인증매체 | 암호/인증 |
| 22 | OTP | 암호/인증매체 | 암호/인증 |
| 23 | PKI | 암호/인증매체 | 암호/인증 |
| 24 | EAM | 암호/인증<br>시스템 | 암호/인증 |
| 25 | SSO | 암호/인증<br>시스템 | 암호/인증 |
| 26 | IM/IAM | 암호/인증<br>시스템 | 암호/인증 |
| 27 | 공인/사설인증 툴 | 암호/인증<br>시스템 | 암호/인증 |
| 28 | PC Firewall | S/W | 시스템보안 |
| 29 | Virus Vaccine | S/W | 시스템보안 |
| 30 | Anti-Spyware | S/W | 시스템보안 |
| 31 | Anti-Pishing | S/W | 시스템보안 |
| 32 | Anti-Spam | S/W | 시스템보안 |
| 33 | Secure-OS | OS | 시스템보안 |

표 5. PRODUCT 차원 테이블
Table 5. PRODUCT Dimension Table

| ProductID | ProductName | Manufacturer |
|---|---|---|
| 1 | Ksign SWAT | 케이사인 |
| 2 | Ksign Mobile | 케이사인 |
| 3 | PETRA | 신시웨이 |
| 4 | XecureDB | 소프트포럼 |
| 5 | INISAFE Mail PKI | 이니텍 |
| 6 | INISAFE Web | 이니텍 |
| 7 | INISAFE Net | 이니텍 |
| 8 | TrustWeb | 비씨큐어 |
| 9 | TrustXML | 비씨큐어 |
| 10 | sysKeeper PKI | 티맥스소프트 |
| … | … | … |
| 223 | Vforce NAC | 넥스지 |

표 6. COMPANY 차원 테이블
Table 6. COMPANY Dimension Table

| Company ID | CompanyNam e | industryType |
|---|---|---|
| 1 | A | agriculture/fisheries |
| 2 | B | manufacturing |
| 3 | C | construction |
| 4 | D | wholesales |
| 5 | E | retail trade |
| 6 | F | lodging/restaurant |
| 7 | G | transportation |
| 8 | H | networking |
| 9 | I | financial/insurance |
| 10 | J | real estate/lease |
| 11 | K | etc. |
| … | … | … |
| 26 | Z | construction |

표 7. TIME 차원 테이블
Table 7.TIME Dimension Table

| TimeID | Quarter | Year |
|---|---|---|
| 1 | 1 | 2009 |
| 2 | 2 | 2009 |
| 3 | 3 | 2009 |
| 4 | 4 | 2009 |
| 5 | 1 | 2010 |
| 6 | 2 | 2010 |
| 7 | 3 | 2010 |
| 8 | 4 | 2010 |

# Ⅳ OLAP 시스템의 구현

## 1. 분배적 계층구조 스키마로의 변환

본 연구에서는 PRODUCT : FUNCTION = N : M인 계층(그림 4 참조)을 현 OLAP 체제 하에서 구현시키고자 한다. 그림 4의 계층구조 스키마는 계층구조 ID 3에 해당한다(Ⅲ장 1절 참조). 이 비분배적 계층구조 스키마인 ID 3을 분배적 계층구조 스키마인 ID 1로 변환시켜야만 현 OLAP 체제에서 구현시킬 수 있는데, 이 변환과정을 그림 5를 예로 들어 설명하고자 한다.

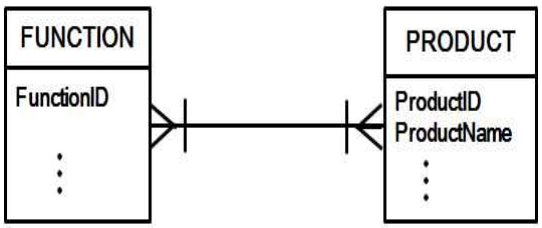



그림 4. 단일경로-비직립성-대칭 집성계층(계층 ID 3)
Fig. 4. A Single-Path, Non-Strict, Symmetric Aggregation Hierarchy

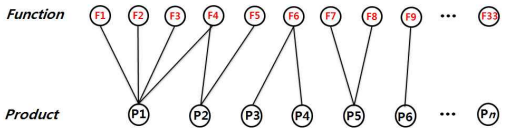



그림 5. 다 대 다 관계
Fig. 5. Many-to-Many Relationship

그림 5에서 다기능 제품을 살펴 볼 것 같으면 P1 제품은 F1, F2, F3, F4의 4가지 기능을 갖고 있고, P2 제품은 F4, F5의 2가지 기능을, P5 제품은 F7, F8의 2가지 기능을 갖고 있다. 이 경우를 일반화 계층 개념으로 볼 때에는 계층구조 ID 11인 포괄적 일반화 계층이 된다(그림 6 참조)[16].

본 연구에서는 이러한 포괄적 일반화 계층 ID 11을 한 개의 제품을 그 제품이 갖고 있는 기능별로 여러 개의 제품으로 분할시킴으로써 계층 ID 1인 분배적 계층으로 변환시키고 있다.

P1 제품은 P1_F1, P1_F2, P1_F3, P1_F4의 4개의 제품으로, P2 제품은 P2_F4, P2_F5의 2개의 제품으로, P5 제품은 P5_F7, P5_F8의 2개의 제품으로 분할시키고 있다(그림 7 참조). 그림 7에서 볼 것 같으면 FUNCTION : PRODUCT = 1 : N임을 확인할 수 있을 것이다. 이러한 변환 과정을 그림 3에 접목시키면 그림 8과 같은 분배적 계층구조 스키마를 얻게 된다.

본 연구에서는 FUNCTION 차원 테이블의 Level3 보안지표의 지수(index number : IN)를 편의상 표 8과 같이 정하고 있음을 밝힌다. 그림 7의 P1_F1 제품 밑에 8이라는 숫자가 기입되어 있는 데, 이 숫자는 표 8의 web firewall의 지수 8을 의미한다.

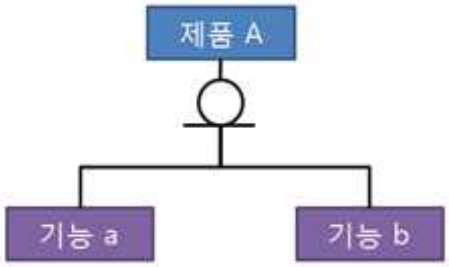



그림 6. 포괄적 일반화 계층
Fig. 6.An Inclusive Generalization Hierarchy

표 8. 33개 잎멤버 지수
Table 8. Index numbers of 33 Leaf Members

| | level1 | IN | level2 | IN | level3 | IN |
|---|---|---|---|---|---|---|
| 1 | 네트워크보안 | 100 | 내/외부보안 | 50 | web firewall | 8 |
| 2 | | | | | System Firewall | 8 |
| 3 | | | | | IPS | 8 |
| 4 | | | | | Anti-DDoS | 8 |
| 5 | | | | | UTM | 10 |
| 6 | | | | | Wireless Security | 8 |
| 7 | | | 접근통제 | 50 | VPN | 25 |
| 8 | | | | | NAC | 25 |
| 9 | 보안관리 | 100 | 관제시스템 | 50 | ESM | 12.5 |
| 10 | | | | | TMS | 12.5 |
| 11 | | | | | PMS | 12.5 |
| 12 | | | | | RMS | 12.5 |
| 13 | | | 분석툴 | 50 | 로그관리/분석툴 | 25 |
| 14 | | | | | 취약점 분석툴 | 25 |
| 15 | 컨텐츠/정보유출방지 보안 | 100 | DB 유출방지 | 50 | DB 보안 | 25 |
| 16 | | | | | DB 암호화 | 25 |
| 17 | | | 자산보호 | 50 | PC 보안 | 17 |
| 18 | | | | | 보안 USB | 16 |
| 19 | | | | | DRM | 17 |
| 20 | 암호/인증 | 100 | 암호/인증 매체 | 50 | 보안 SmartCard | 12.5 |
| 21 | | | | | H/W 토큰(HSM) | 12.5 |
| 22 | | | | | OTP | 12.5 |
| 23 | | | | | PKI | 12.5 |
| 24 | | | 암호/인증 시스템 | 50 | EAM | 12.5 |
| 25 | | | | | SSO | 12.5 |
| 26 | | | | | IM/IAM | 12.5 |
| 27 | | | | | 공인/사설인증 툴 | 12.5 |
| 28 | 시스템보안 | 100 | S/W | 50 | PC Firewall | 10 |
| 29 | | | | | Virus Vaccine | 10 |
| 30 | | | | | Anti-Spyware | 10 |
| 31 | | | | | Anti-Pishing | 10 |
| 32 | | | | | Anti-Spam | 10 |
| 33 | | | O/S | 50 | Secue OS | 50 |
| | 합계 = | 500 | 합계 = | 500 | 합계 = | 500 |

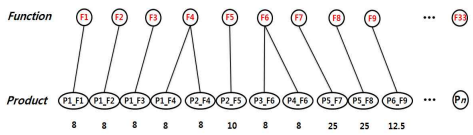



그림 7. 일 대 다 관계
Fig. 7. One-to-Many Relationship

이하 그림 8의 분배적 계층구조 스키마 개념을 사실 테이블을 활용하여 실제로 구현시키는 방법을 설명하고자 한다.

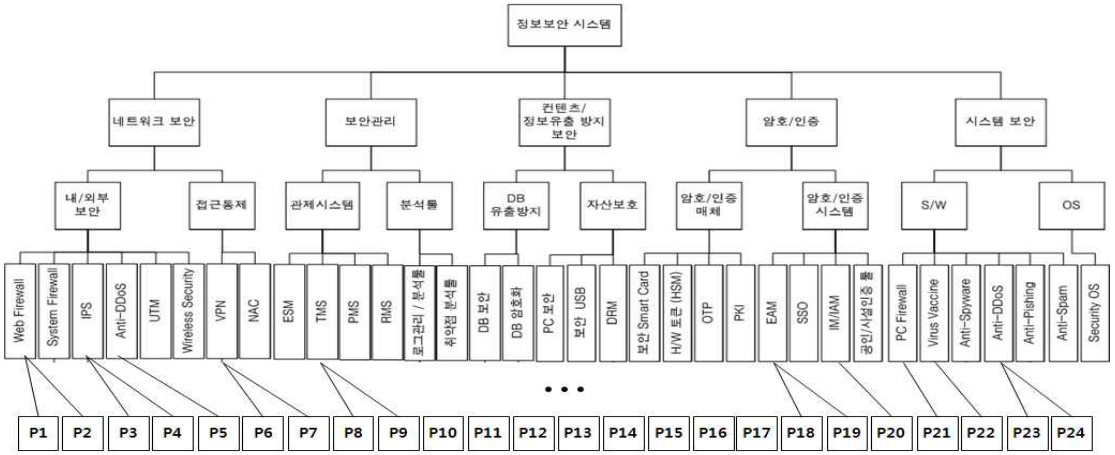



그림 8. 분배적 계층구조 스키마
Fig 8. A Distributive Hierarchy Schema

## 2. 사례 OLAP 큐브의 구현

본 연구에서 사례로 삼고 있는 보안지수 큐브의 스타스키마를 살펴보면 그림 9와 같다. 그림 9에서의 FUNCTION 차원 테이블, PRODUCT 차원 테이블, COMPANY 차원 테이블, TIME 차원 테이블은 각각 표 4, 표 5, 표 6, 표 7과 같다.

표 9의 보안지수 사실 테이블을 예로 하여 분배적 계층구조 스키마 개념을 구현시키는 방법을 설명하고자 한다. 표 9에서 FactID 52,53,54를 보면, 제품 102가 각각 기능 28,29,30을 갖고 있음을 알 수 있다. 보안지수 사실 테이블의 Security Index Number1(SecurityIN1) 측정값으로 제품 102, 기능 28의 경우 10(표 8의 PC firewall 지수), 제품 102, 기능 29의 경우 10(표 8의 Virus Vaccine 지수), 제품 102, 기능 30의 경우 10(표 8의 Anti-Spyware 지수)을 책정함으로써 분배적 계층구조 스키마 개념을 구현시켰다.

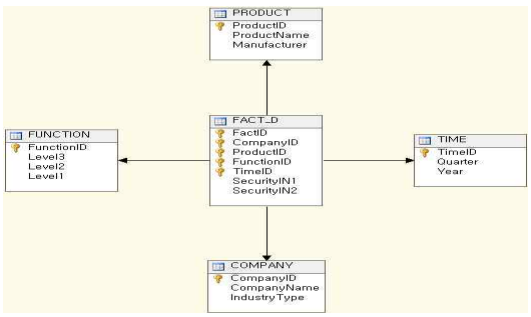



그림 9. 보안 지수 큐브의 스타 스키마
Fig. 9. Security Index Number Cube Star Schema

표 9. 보안 지수 사실 테이블
Table 9. Security Index Number Fact Table

| FactID | Company ID | ProductID | Function ID | TimeID | SecurityI N1 | SecurityI N2 |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 23 | 7 | 12.5 | 12.5 |
| 2 | 1 | 2 | 23 | 7 | 12.5 | 12.5 |
| 3 | 1 | 3 | 15 | 7 | 25 | 25 |
| 4 | 1 | 3 | 16 | 7 | 25 | 25 |
| 5 | 1 | 28 | 19 | 7 | 17 | 17 |
| 6 | 1 | 46 | 4 | 7 | 8 | 8 |
| 7 | 1 | 69 | 2 | 7 | 8 | 8 |
| 8 | 1 | 69 | 7 | 7 | 25 | 25 |
| 9 | 1 | 75 | 5 | 7 | 10 | 10 |
| 11 | 1 | 95 | 3 | 7 | 8 | 8 |
| 12 | 1 | 122 | 6 | 7 | 8 | 8 |
| 10 | 1 | 149 | 1 | 7 | 8 | 8 |
| 13 | 2 | 1 | 23 | 7 | 12.5 | 12.5 |
| 14 | 2 | 2 | 23 | 7 | 12.5 | 12.5 |
| 15 | 2 | 3 | 15 | 7 | 25 | 25 |
| 16 | 2 | 3 | 16 | 7 | 25 | 25 |
| 20 | 2 | 101 | 28 | 7 | 10 | 10 |
| 21 | 2 | 101 | 29 | 7 | 10 | 10 |
| 17 | 2 | 139 | 18 | 7 | 16 | 16 |
| 19 | 2 | 145 | 32 | 7 | 10 | 10 |
| 22 | 2 | 145 | 32 | 7 | 10 | 10 |
| 18 | 2 | 162 | 33 | 7 | 50 | 50 |
| 46 | 9 | 6 | 23 | 7 | 12.5 | 12.5 |
| 47 | 9 | 7 | 23 | 7 | 12.5 | 0 |
| 51 | 9 | 8 | 27 | 7 | 12.5 | 12.5 |
| 38 | 9 | 12 | 15 | 7 | 25 | 25 |
| 39 | 9 | 12 | 16 | 7 | 25 | 25 |
| 40 | 9 | 27 | 17 | 7 | 17 | 17 |
| 42 | 9 | 28 | 19 | 7 | 17 | 17 |
| 26 | 9 | 47 | 4 | 7 | 8 | 8 |
| 24 | 9 | 68 | 2 | 7 | 8 | 8 |
| 29 | 9 | 68 | 7 | 7 | 25 | 25 |
| 27 | 9 | 80 | 5 | 7 | 10 | 10 |
| 25 | 9 | 95 | 3 | 7 | 8 | 8 |
| 52 | 9 | 102 | 28 | 7 | 10 | 10 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 53 | 9 | 102 | 29 | 7 | 10 | 10 |
| 54 | 9 | 102 | 30 | 7 | 10 | 10 |
| 55 | 9 | 106 | 31 | 7 | 10 | 10 |
| 50 | 9 | 110 | 26 | 7 | 12.5 | 12.5 |
| 28 | 9 | 123 | 6 | 7 | 8 | 8 |
| 41 | 9 | 129 | 18 | 7 | 16 | 16 |
| 32 | 9 | 141 | 9 | 7 | 12.5 | 12.5 |
| 56 | 9 | 145 | 32 | 7 | 10 | 10 |
| 23 | 9 | 150 | 1 | 7 | 8 | 8 |
| 57 | 9 | 189 | 33 | 7 | 50 | 50 |
| 49 | 9 | 192 | 25 | 7 | 12.5 | 12.5 |
| 48 | 9 | 196 | 24 | 7 | 12.5 | 12.5 |
| 43 | 9 | 198 | 20 | 7 | 12.5 | 12.5 |
| 45 | 9 | 204 | 22 | 7 | 12.5 | 12.5 |
| 44 | 9 | 205 | 21 | 7 | 12.5 | 12.5 |
| 35 | 9 | 213 | 12 | 7 | 12.5 | 12.5 |
| 36 | 9 | 217 | 13 | 7 | 25 | 25 |
| 37 | 9 | 217 | 14 | 7 | 25 | 25 |
| 33 | 9 | 219 | 9 | 7 | 12.5 | 0 |
| 34 | 9 | 219 | 10 | 7 | 12.5 | 12.5 |
| 58 | 9 | 220 | 3 | 7 | 8 | 0 |
| 59 | 9 | 220 | 4 | 7 | 8 | 0 |
| 60 | 9 | 220 | 8 | 7 | 25 | 0 |
| 61 | 9 | 220 | 14 | 7 | 25 | 0 |
| 30 | 9 | 223 | 8 | 7 | 25 | 25 |
| 31 | 9 | 223 | 11 | 7 | 12.5 | 12.5 |

SecurityIN1 측정값은 동일 기능을 수행할 수 있는 이종 제품을 1개 이상 추가로 보유하고 있을 경우에 대한 측정값 즉, 예비제품 보유률을 포함한 값이며, 각 회사의 진정한 정보보호 지수를 산출은 동일 기능의 중복 보유에 따른 측정값의 중복 산정을 제외한 Security Index Number2(SecurityIN2)라는 측정값 컬럼을 통해 가능하다. SecurityIN2 컬럼에서는 한 회사가 동일 기능을 발휘하는 제품을 여러 개 가지고 있을 경우 하나의 제품만 지수를 인정하고 나머지 제품의 지수는 인정하지 않는다.

## 3. 결과 및 분석

표 9와 그림 10에서와 같이 SecurityIN1, SecurityIN2 두 개의 측정값 컬럼이 있는데, SecurityIN1은 예비제품 보유률을 나타내고 SecurityIN2은 정보보호 지수를 나타낸다.

그림 10의 보안 지수 큐브에서는 2010년 3사분기 시점(TimeID 7)에서의 A 기업, B 기업, I 기업의 정보보호 지수를 나타내고 있다. 먼저 SecurityIN2 측정값을 살펴보면, A 기업의 경우에는 총합계 점수가 167이며 따라서 전체 정보보호 지수는 167/500 즉 백분율로 환산하면 33.4% 이다. 그리고 level2의 내/외부 보안 범주에서 총점 50점 기준으로 50점 모두를 부여 받고 있기 때문에 내/외부 보안 범주에서는 100%의 정보보호 지수를 나타내고 있으며, 접근통제 보안 범주에서는 총점 50점 기준으로 25점 즉 50%의 정보보호 지수를 나타내고 있다. B 기업의 경우에는 총 합계 점수가 181점이며 따라서 전체 정보보호 지수는 181/500 즉 36.2% 이다. 그리고 level1의 시스템 보안, 암호/인증, 컨텐츠/정보유출방지 보안의 4개 범주에서 총점 100점 기준으로 각각 90, 25, 66점을 획득하고 있기 때문에 각 범주에서 90%, 25%, 66%의 정보보호 지수를 나타내고 있다. I 기업의 경우에는 총합계 점수가 500이며 따라서 전체 정보보호 지수는 500/500 즉 100%의 정보보호 지수를 나타내고 있다.

두 번째로 기능의 예비제품 보유률을 나타내는 SecurityIN1 측정값을 살펴보면 I 기업의 경우, 총합계 점수가 591점으로 전체 33개 기능의 총합계 500점 보다 높게 산정되어 있다. 그 이유는 표 9의 데이터 항목 중 I 기업이 동일 기능의 이종 제품을 보유하고 있기 때문이라 분석할 수 있다.

TIME 계층 3

| Level1 | Level2 | Level3 | Product Name | Company Name A Security IN1 | A Security IN2 | B Security IN1 | B Security IN2 | I Security IN1 | I Security IN2 | 총합계 Security IN1 | 총합계 Security IN2 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ⊟ 네트워크보안 | ⊟ 내/외부 보안 | ⊟ Anti-DDoS | WeGuardia™ DDoS V1.0 | | | | | 8 | 8 | 8 | 8 |
| | | | Tipping Point | | | | | 8 | 0 | 8 | 0 |
| | | | Safezone XDDoS V3.0 | 8 | 8 | | | | | 8 | 8 |
| | | | 합계 | 8 | 8 | | | 16 | 8 | 24 | 16 |
| | | ⊟ IPS | SNIPER IPS V6.0.v | 8 | 8 | | | 8 | 8 | 16 | 16 |
| | | | Tipping Point | | | | | 8 | 0 | 8 | 0 |
| | | | 합계 | 8 | 8 | | | 16 | 8 | 24 | 16 |
| | | ⊟ System Firewall | SECUREWOKRS V5.2 | 8 | 8 | | | | | 8 | 8 |
| | | | SecuwaySuite 6000 V3.0 +IPS | | | | | 8 | 8 | 8 | 8 |
| | | | 합계 | 8 | 8 | | | 8 | 8 | 16 | 16 |
| | | ⊟ UTM | SECUREWORKS | | | | | 10 | 10 | 10 | 10 |
| | | | TESS UTM V4.5 | 10 | 10 | | | | | 10 | 10 |
| | | | 합계 | 10 | 10 | | | 10 | 10 | 20 | 20 |
| | | ⊟ Web Firewall | SECUI NXG W V2.0 | | | | | 8 | 8 | 8 | 8 |
| | | | WAPPLES v3.0 | 8 | 8 | | | | | 8 | 8 |
| | | | 합계 | 8 | 8 | | | 8 | 8 | 16 | 16 |
| | | ⊟ Wireless Security | AirFront v4.5 | | | | | 8 | 8 | 8 | 8 |
| | | | PPX-AnyLink v4.0 | 8 | 8 | | | | | 8 | 8 |
| | | | 합계 | 8 | 8 | | | 8 | 8 | 16 | 16 |
| | | 합계 | | 50 | 50 | | | 66 | 50 | 116 | 100 |
| | ⊟ 접근통제 | ⊟ NAC | Vforce NAC | | | | | 25 | 25 | 25 | 25 |
| | | | Tipping Point | | | | | 25 | 0 | 25 | 0 |
| | | | 합계 | | | | | 50 | 25 | 50 | 25 |
| | | ⊟ VPN | SECUREWOKRS V5.2 | 25 | 25 | | | | | 25 | 25 |
| | | | SecuwaySuite 6000 V3.0 +IPS | | | | | 25 | 25 | 25 | 25 |
| | | | 합계 | 25 | 25 | | | 25 | 25 | 50 | 50 |
| | | 합계 | | 25 | 25 | | | 75 | 50 | 100 | 75 |
| | 합계 | | | 75 | 75 | | | 141 | 100 | 216 | 175 |
| ⊟ 보안관리 | ⊞ 관제시스템 | | | | | | | 62.5 | 50 | 62.5 | 50 |
| | ⊞ 분석툴 | | | | | | | 75 | 50 | 75 | 50 |
| | 합계 | | | | | | | 137.5 | 100 | 137.5 | 100 |
| ⊞ 시스템보안 | | | | | | 90 | 90 | 100 | 100 | 190 | 190 |
| ⊞ 암호/인증 | | | | 25 | 25 | 25 | 25 | 112.5 | 100 | 162.5 | 150 |
| ⊞ 컨텐츠/정보유출방지 보안 | | | | 67 | 67 | 66 | 66 | 100 | 100 | 233 | 233 |
| 총합계 | | | | 167 | 167 | 181 | 181 | 591 | 500 | 939 | 848 |

그림 10. 보안 지수 큐브
Fig. 10. Security Index Cube

표 9와 그림 10에서와 같이 I 기업은 Anti-DDoS, IPS, NAC, ESM, PKI, 취약점분석 툴의 총 6개 항목에서 각각 동일 기능의 이종 제품을 보유하고 있기 때문에 각각의 기능에 대하여 200%의 예비제품 보유율을 가지고 있음을 분석할 수 있다. 표 9에서 음영으로 표시한 FactID 30, 33, 47, 58, 59, 60, 61 항목이 예비 제품이 됨을 알 수 있다.

## V 결론

본 연구에서는 설문지 조사방법을 사용하지 않고 개별기업의 정보보호 수준에 관한 원시데이터를 정확하게 수집할 수 있는 새로운 방법을 제시하였으며, 이는 수집된 원시데이터를 근간으로 하여 머크로 데이터를 얻어 정책의사결정을 할 수 있는 OLAP 데이터베이스 시스템을 구축함으로써 가능하였다. OLAP을 분석 시스템으로 채택한 이유는 정형화된 분석기준과 reporting을 지양하기 위해 OLAP이라는 분석 시스템을 통해 단순히 수집된 데이터를 통해 현황을 reporting하는 과거의 분석기법이 아닌 생산된 통계를 다양하게 분류하고 조회할 수 있으며, 비정형 분석기준으로 관련 통계의 분석이 가능하도록 구현하기 위함이다. 본 연구의 기법을 적용하여 구축된 OLAP 데이터베이스 시스템을 사용하면 개별 기업의 보안지수와 예비 보안제품의 보유률을 표현하고 더 나아가서는 국가 전체의 보안지수도 산출해 낼 수 있음을 확인하였다. 또한 이전 연구에서 보였던 바와 같이, 현 OLAP 체제에서는 모든 계층구조 스키마가 분배적으로 되는 경우에만 제대로 집계데이터를 구할 수 있기 때문에 본 연구에서는 사례의 비 분배적 계층구조 스키마를 분배적 스키마로 변환하여 OLAP 데이터베이스 시스템을 구축하는 과정을 다음과 같이 보였다.

먼저, 단일기능의 제품만이 존재한다는 가정에서 벗어나 다 기능의 제품을 정확하게 분류하기 위해 국내 모든 보안제품에 대한 기능을 명세화 하여 전체 보안 기능을 33개의 세부 기능으로 분류하고 분야별로 계층화 하였다. 그리고 이 기능명세를 활용하여 개별 기업이 보유하고 있는 보안 제품의 목록만으로 해당 기능에 관한 정확한 원시 데이터의 수집을 가능케 하였다.이 때의 수집된 원시데이터를 통해 머크로 데이터를 얻어내기 위해 계층구조 ID 3에 해당하는 PRODUCT : FUNCTION = N : M인 비분배적 계층구조를 일반화 계층 개념에서의 계층구조 ID 11인 포괄적 일반화 계층으로 변환하였다. 그리고 분류된 각 33개의 기능에 보안 지수를 할당하여 표현함으로써 현 OLAP 체제 하에서 구현 가능한 분배적 계층구조 스키마인 ID 1로 변환할 수 있었다.

위와 같은 과정을 본 연구에서는 통해 기존의 기업 정보보호 실태조사의 사례를 OLAP 데이터베이스 시스템으로 구축하였으며, 이와 같은 방법을 통해 기존의 설문조사기법 보다 더욱 정확한 데이터를 얻어 해당 조사에서 분석된 결과치의 무결성을 보장할 수 있었다. 그 이유는 특정 응답자의 지식기반에 의존한 데이터가 아닌 실제 사실 값을 기반으로 한 조사, 분석 기법이기 때문이며, 사례의 OLAP 데이터베이스 시스템을 구축하기 위해 정보보안 제품과 정보보안 기능과의 관계를 표현한 계층구조 스키마를 OLAP 체제에서 구현 가능하도록 변환하였기 에 가능하였다.

이와 같은 조사, 분석기법은 각 기업들이 국가 정보보안 지수를 조사하는 정부의 해당 기관에 정기적으로 해당 기업이 보유하고 있는 정보보안 제품의 리스트를 보고,갱신 하여야 하며, 국내의 모든 보안제품의 기능명세가 작성되어져야 한다는 전제가 필요하다. 향후 해당 정부기관이 제도적으로 이와 관련한 규정을 제정한다면 보다 정확하고 효율적인 국가 정보보호 지수의 산출을 기대할 수 있을 것이다. 2008년 통계개발원이 발간한 국제공동연구보고서인 “국가통계 제도의 발전”에서 정확하고 신뢰성 있는 통계를 생산하기위한 기반구축에 대한 중요성을 강조하고 있듯이 본 연구의 결과물이 제도적으로 정착되기 위한 각 기업들의 정보보안 제품 보고체계와 국내 보안제품들의 기능 명세화 체계의 정립이 필요하다고 생각되며 이에 관련한 연구가 필요다고 생각된다.

## 참고문헌

[1] Korea Communication Commission(KCC), Korea Information Security Agency(KISA), “2008 Informat ion Security Survey in Korea”, KOSIS, 2008

[2] Taell Kim, JuHyun Seo “A Critical Review of Survey Method in Public Policy Studies”, Journal of Korea Public Administration, Vol. 32, No. 3, pp. 199-215, 1998

[3] MinAh Kang, KyungAh Kim, “Handling of Missing Data in Public Policy Studies“, Journal of Korea Public Administration, Vol. 40, No. 2, pp.31-52, 2006

[4] Korea Communication Commission(KCC), Korea Information Security Agency(KISA), “2010 Information Security Survey in Korea, KOSIS, 2011

[5] Willem E. Saris, Irmtraud N. Gallhofer “Design, Eva

luation, and Analysis of Questionnaires for Survey Research," John Wiley & Sons, pp.35-44, 2007

[6] Robert M. Groves, Floyd J. Fowler Jr., Mick P. Coup er, James M. Lepkowski, eleanor Singer, Roger Tourangeau, "Survey Methodology SE," John Wiley & Sons, pp.300-312, 2009

[7] SeHyeon Jang, HanJu Yu, and InSoo Choi, "Design of a Hierarchical Dimension of the Bill of Materials Type", KSCI, Vol. 11, No. 4, pp. 244-250, Sept ember. 2006.

[8] Carlos A. Hurtado, and Alberto O. Mendelzon. Jensen, "Reasoning about Summarizability in Heterogeneous Multidimensional Schemas", LNCS 1973, pp. 375 - 389, 2001.

[9] J. Gray, A. Bosworth, A. Layman, and H. H. Pirahesh, "Data cube : A relational operator generalizing group-by, cross-tab and sub-totals", In Proceedings of the 12th IEEE-ICDE Conference, New Orleans, Los An-geles, USA, 1996.

[10] Robert S. Craig, Joseph A. Vivona, and David Ber kovitch, "Microsoft Data Warehousing : Building Distributed Decision Support Systems," pp. 59-66, John Wiley & Sons, 1999.

[11] Carlos A. Hurtado, and Alberto O. Mendelzon. Jensen, "Reasoning about Summarizability in Heterogeneous Multidimensional Schemas", LNCS 1973, pp. 375 - 389, 2001.

[12] SeungHyun Lee, DuckSung Lee and InSoo Choi, "Applying an Aggregate Function AVG to OLAP Cubes", KSCI, Vol. 14, No. 1, pp. 217-228, Janu ary. 2009.

[13] Svetlana Vinnik, and Florian Mansmann, "From Analysis to Interactive Exploration: Building Visual Hierarchies from OLAP Cubes", LNCS 3896, pp. 496-514, 2006.

[14] Mihwa Oh, ManMo Hwang, JungWoo Choi and InSoo Choi, "An Approach to Navigating Data Cubes with a Hierarchical Visualization Technique", KSCI, Vol. 16, No. 2, pp. 290-305, February. 2011.

[15] Knowledge Information Security Industry Ass ociation(KISIA), Korea Information Security Agency(KISA), "2010 Information Security Indust ry Markets and Trends in Korea", KOSIS, pp. 10, 2010.12

[16] David M. Kroenke, "Database Processing," PEARSON, pp. 174-188, 2011.

## 저 자 소 개

**최 정 우**

1999 : 숭실대학교 산업·정보시스템공학과 공학사

2002 : 숭실대학교 산업공학과 공학석사

현 재 : 숭실대학교 대학원 산업 정보시스템공학과 박사과정

관심분야 : MIS, DW, OLAP

Email : fantom119@naver.com

**최 인 수**

1985 : 서울대학교 산업공학과 공학박사

현재 : 숭실대학교 산업·정보시스템공학과 교수

관심분야 : MIS, DW, OLAP

Email : ischoi@ssu.ac.kr