

# 정보보호제품 품질 평가 모델에 관한 연구

윤형득,<sup>1\*</sup> 이경호<sup>2\*</sup><sup>1</sup>한국산업기술시험원, <sup>2</sup>고려대학교 정보보호대학원

## Quality Evaluation Model on Information Protection Product

Hyung-Deuk Yoon,<sup>1\*</sup> kyung-ho Lee<sup>2\*</sup><sup>1</sup>Korea Testing Laboratory, <sup>2</sup>Korea University

### 요약

기업의 정보보호활동 예산 중 정보보호제품 구매가 가장 큰 비중을 차지하고 있다. 그러나 정보보호제품을 객관적으로 비교하기 위해 적용되어야 하는 평가요소와 평가모델이 없어 제품 선택에 어려움을 겪고 있다. 따라서 본 연구에서는 정보보호제품 고유의 품질 특성을 연구하고 그에 따른 평가 요소들을 선정한다. 선정된 평가 요소들을 분석하여 중요도에 따른 가중치를 부여한 품질 결정 모델을 제시한다. 대상은 네트워크 정보보호제품으로 제한하여 분석하였고 모든 정보보호제품으로 확대하여 적용할 수 있다.

### ABSTRACT

The purchase of information protection products accounts for the largest portion of corporate information protection activity budgets. However, there are no evaluation factors and evaluation models that should be applied to objectively compare information protection products, and therefore, product selection is difficult. Therefore, in this study, we study the inherent quality characteristics of information security products and select evaluation factors accordingly. The selected evaluation factors are analyzed and a quality determination model is given by weighting according to importance. The target is limited to the network information protection product and can be extended to all information protection products.

**Keywords:** Information Protection Product, Quality Evaluation Model, Quality factor, AHP

## 1. 서론

해마다 보안사고가 늘어나고 있으며 사고 유형도 다양해지고 있다. 기업체는 이에 대한 피해를 최소화하기 위해 정보보호관리체계 인증 등, 관리체계를 비롯하여 보안관제 서비스, 정보보호제품 구매 등 다양한 방법을 통하여 노력하고 있으며 이에 따라 기업체에서 사용하는 정보보호 예산도 매년 증가하고 있다. 2016년 정보보호실태조사[1]에 따르면 전체 사업체에서 정보보호관련 예산을 편성한 사업체는 32.5%

이며 정보보호 예산을 별도로 편성한 사업체에서는 정보보호의 방법으로 주로 정보보호제품 구입(42.9%)에 가장 많은 예산을 편성하였다. 그 중에서도 특히 네트워크 보안 제품군(82.4%)을 주로 사용하는 것으로 [Fig.1]과 같이 발표하고 있다. 또한 2016년 국가정보보호백서[2]에서도 네트워크 보안이 차지하는 비중이 26.0%로 다른 콘텐츠 정보 유출 방지(13.4%)나 보안관리(10.7%)에 비해 높은 것으로 나타났다. 즉 정보보호를 위해 노력하는 많은 기업들이 정보보호제품 구입을 통해서 정보보호를 실현하고자 노력하고 있다. 그러나 외산 제품과 서비스를 구매하는 이유에 대한 답변으로는 보안성능 및 서비스 품질이 우수하기 때문이라는 답변이 42.3%로 가장 높게 나타났다. 또한 95%의 미국 기업들은 IT

Received(10. 16. 2017), Modified(11. 13. 2017),  
Accepted(11. 13. 2017)

\* 주저자, secupia@nate.com

† 교신저자, kevinlee@korea.ac.kr(Corresponding author)

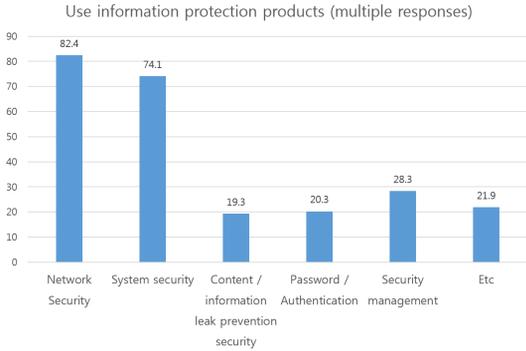


Fig. 1. Information protection product use ratio

보안상품 판매 기업들이 제품과 서비스에 대한 품질 보증을 받고 싶다고 응답했고, 88%가 만약 이렇게 보장 서비스를 제공하는 업체가 있다면 협력기업을 바꾸겠다고 했다[3]. 정보보호의 수준을 높이기 위한 기업체의 노력에 정보보호제품 구매가 가장 큰 비중을 차지하고 있지만 품질에 대한 측정 모델이 존재하지 않아 구매 후 제품에 대해 품질을 만족도는 떨어졌다. 성장하는 정보보호제품의 시장에서 지속적인 기능의 안정성과 성능의 우수성 등 품질은 향후 제품의 경쟁력을 위한 필수적인 요소이다.

품질에 대한 의미는 시간이 지나면서 발전해 왔다. American Society for Quality에서는 품질이란 개인이나 부문별로 자체 정의가 있는 주관적인 용어이며 제품에 대한 요구사항, 기대에 대한 충족과 같은 개인의 정의하고 있는 양적, 질적인 관점의 결합으로 정의하고 있다. Crosby[4]는 어떠한 요구사항이 있고 해당 제품이 그 요구사항에 준수하는 것으로 품질을 판단한다고 정의하고 있으며 Juran[5]은 제품의 특성이 고객의 요구사항을 만족시키고 고객에게 제품에 대한 만족을 제공하는 것으로 정의하고 있다. 따라서 품질 결정을 위한 모델을 연구함에 있어서 연구 대상 제품을 필요로 하는 사용자의 요구사항이 무엇인지를 파악하고 분석하는 것을 토대로 평가모델을 제시하려 한다.

본 논문에서는 구성은 다음과 같다. 제 2장에서는 네트워크 정보보호제품의 특성에 대해 연구하고 평가 모델을 제시한 선행 연구들을 조사한다. 제 3장에서는 평가 모델에 사용된 평가 요소를 구분하고 평가 요소 별 사용된 표준을 연구하여 각 표준 간 유사 평가 항목을 배제한 평가요소를 선정한다. 제 4장에서는 선정된 평가요소에 대해 AHP(Analytic Hierarchy Process) 기법을 적용한 설문분석을

통해 평가 요소 간 가중치가 부여된 평가 모델을 제시한다. 마지막으로 5장에서는 연구의 결론과 시사점을 기술한다.

## II. 선행연구

### 2.1 네트워크 정보보호제품의 특성

네트워크 정보보호제품의 품질 모델을 결정하기 위해서는 전통적인 품질에 대한 정의를 기반으로 네트워크 정보보호제품에 대해 소비자가 원하는 요구사항을 도출하는 것이 필요하다. 따라서 네트워크 정보보호제품의 품질을 정의하기에 앞서 네트워크 정보보호제품에 대해서 조사하였다. 정보보호제품이라 함은 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 총칭한다[6]. 이러한 정보보호제품을 형태로 분류하면 네트워크 정보보호제품군, 정보보호 기반 제품군, 컴퓨팅 정보보호제품군으로 분류된다. FW(FireWall), IPS(Intrusion Prevention System), IDS(Intrusion Detection System) 등은 네트워크 정보보호제품으로 분류되며 스마트카드, 전자여권 등은 정보보호 기반 제품군으로, 보안 USB, DB 접근통제 제품 등은 컴퓨팅 보호제품 유형으로 분류된다. 이는 정보보호제품의 정의에 기술된 요구사항을 제공하는 환경에 대한 구분으로 볼 수 있다. 본 논문에서 다루게 되는 네트워크 정보보호제품은 트래픽에 대한 제어를 중심으로 하는 제품으로 정보보호를 위한 관리적·기술적 수단이 네트워크를 통해 이루어지는 특성을 가지고 있다. 즉 소비자의 품질에 대한 요구사항을 만족시키기 위해서는 네트워크를 통한 트래픽 처리의 품질이 바탕이 되어야 하고 더불어 정보보호의 특성에 따른 품질이 모두 보장되어야 한다.

### 2.2 품질 평가 모델에 대한 선행 연구

FW, IDS, IPS 등의 네트워크 정보보호제품 품질 측정과 관련하여 다양한 연구가 진행되었으며 관련한 선행 연구에서 제시한 품질 결정 모델들을 조사하였다. 이하용 등[7,8]은 IDS와 IPS 각각의 성능 평가 모델을 제시하면서 ISO/IEC 15408[9]과 ISO/IEC 9126[10]에 근거하여 평가 모델을 제시하였다. 이종민[11]은 보안소프트웨어 제품에 대해

서 ISO/IEC 15408과 ISO/IEC 9126 기반으로 하고 새로운 시험항목을 제시하여 평가 모델로 제시하였다. 윤여웅 등[12]도 정보보호제품 품질평가를 위한 품질 모델 연구에서 정보보호제품에 대한 평가 기준인 ISO/IEC 15408과 소프트웨어 품질 평가 기준을 제시하고 있는 ISO/IEC 9126을 모델로 하여 품질평가를 위한 모델을 제시하였다. 네트워크 정보보호제품을 포함한 전체 정보보호제품에서는 국내 및 국외에서 ISO/IEC 15408 기반의 CC 평가가 일반적으로 많이 사용되고 있다. 그러나 앞선 연구에서 ISO/IEC 15408에 ISO/IEC 9126의 평가 모델을 적용한 것은 보안성에 맞춰진 평가 모델만으로 기능성, 사용성, 호환성 등의 소프트웨어적 특성에 대한 평가가 부족하다고 연구하였기 때문이다. 따라서 본 논문에서도 네트워크 정보보호제품의 평가 모델의 평가 요소에 ISO/IEC 15408과 ISO/IEC 9126 기반의 평가 요소들을 사용하고 ISO/IEC 9126의 경우 ISO/IEC JTC1/SC7 WG6에서 IEC 25000 시리즈로 개편하였기 때문에 본 논문에서는 개편된 버전인 ISO/IEC 25023[13]을 사용하기로 한다.

평가 모델을 제시한 선행 논문 중 앞서 살펴본 두 가지 표준외의 다른 방법론을 제시한 논문을 살펴보면 전용회[14]는 IPS 성능평가 방안에서 HTTP 트래픽, 프로토콜 혼합 트래픽, 응답시간 등 네트워크 성능 부분을 포함하여 탐지엔진, 안전성, 신뢰성 등 소프트웨어적 특성과 보안특성을 평가 요소로 제시하였으며 이춘성[15] 등은 DDos 대응장비 시험의 시험방안 연구에서 RFC 3511[16]을 참고하여 침입 방지 시스템의 유효성 평가에 적용하였다. 또한 Niemann[17] 등은 네트워크 필터의 성능 평가를 위해 RFC 3511을 이용한 Throughput을 평가요소로 사용하였으며 Sheth[18]는 방화벽 제품에 대한 평가 방법에서 기능적 요소로 Application Intelligence, Firewall Management와 네트워크 요소로 Throughput, HTTP Throughput, Concurrent Connections, Connections per Second를 평가 요소로 선정하였다. Lyu[19] 등은 HTTP 등의 트랜잭션 평균시간, 지연 시간 등을 평가 요소로 사용하였다. 정태인[20] 등은 정보보호제품 성능시험 동향 분석에서 상기 선행연구와 다른 네트워크 기반의 RFC 3511 등을 기준으로 국제 시험기관에서 평가가 진행되고 있음을 조사하였다. 특히 NSS Labs, Tolly Group 등의 주요 시험기관에

Table 1. Precedent research for selection criteria of research

Quality characteristics	Standard	Precedent research
Security quality	ISO/IEC 15408	Lee Ha-Yong [7,8] Lee Jong-Min[11] Yun Yeo-Wung[12]
Software quality	ISO/IEC 9126	
Network quality	RFC 3511	Jeon Yong-Hee.[14] Lee Chun Seong[15] Niemann[17] Sheth[18] Lyu[19] Jung Tae-In[20] TTA[21]

서는 크게 효율성을 포함한 기능시험 항목과 네트워크 성능 부분, 보안성능 부분에 대해 시험을 진행하고 있다고 조사하였다. 정보통신단체표준으로 사용되고 있는 TTA 표준의 네트워크 보안 장비에 대한 성능 측정 방법[21]은 RFC 3511을 그대로 적용하고 있다. 상기 선행 연구는 RFC 3511 등 네트워크 특성에 따른 품질 평가 요소를 주요 평가 모델로 사용하고 있는 것을 확인할 수 있다. 또한 4절의 정보보호 전문가의 설문조사 결과를 보면 소프트웨어 품질보다 네트워크 품질이 더 중요하다고 응답하였으며 네트워크 품질의 중요성과 정보보호 품질에 대한 중요도의 차이가 많지 않다. 즉 네트워크 품질이 전체 제품의 품질에 많은 영향을 미치는 것을 확인할 수 있으며 이에 따라 네트워크 품질에 대한 평가 요소도 포함하여 평가 모델을 제시하도록 한다.

이에 따라 본 논문에서는 네트워크 품질, 소프트웨어 품질, 정보보호 품질의 3가지 요소를 기반으로 평가 요소를 정의하기로 한다.

### 2.3 의사결정 모델

제품 간의 품질을 비교하기 위해서는 평가 항목이 동일하더라도 차이를 둘 수 있는 요소가 필요하다. 즉 동일한 기능이나 다른 기능 간의 중요성을 비교할 수 있는 요소가 필요하며 본 논문에서는 평가 요소에 대한 가중치를 결정하여 상대적으로 중요항목에 더 높은 점수를 부여할 수 있는 모델을 만들고자 한다. 이에 따라 먼저 품질 평가 요소를 선정한 후 평가 항

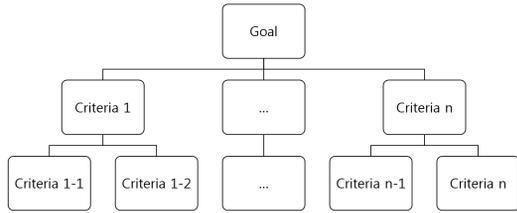


Fig. 2. AHP Model

목간의 비교 우선순위와 가중치를 부여하기 위해 AHP(analytic hierarchy process) 모델을 사용하여 각 항목에 가중치를 부여하려 한다. AHP는 T. L. Saaty[22,23]에 의해 제안된 의사결정 모델이다. 의사 결정을 위해 구성 요소를 계층으로 세분화 하여 요소 간 이원비교를 통해 가중치를 부여하여 최종 목표에 대한 의사결정을 하는 방식으로 평가자의 지식, 경험 등을 이용하는 방식이다. AHP 모델은 복잡한 의사결정 문제를 작은 특성들로 구분하여 계층적 구조화를 통해 순차적인 접근 과정을 거쳐 최종적으로 의사결정을 하도록 지원한다. 또한 AHP기법은 일관성비율(Consistency Ratio, CR)을 기준으로 설문 응답의 신뢰도를 측정할 수 있는 특성을 갖고 있기 때문에, 의사결정자의 논리적 일관성 유지 여부를 확인 할 수 있으며 논리적이고 합리적인 의사결정 과정에 대한 신뢰성을 높일 수 있다. 정보보호 분야에도 이석원[24]은 금융회사에서 서버 특수 계정 운영방식에 적합한 방법을 결정하기 위해 AHP 모델을 사용하였고 윤석웅[25] 등은 VoIP 정보보호 점검항목의 중요도 분석에 AHP 모델을 사용하였다.

AHP 모델은 어떠한 선택에 있어서의 우선순위를 파악하고 평가 요소의 가중치 부여를 통해 평가대상을 객관적으로 판단하는데 적합한 방법으로 보이며 소프트웨어 분야 및 정보보호 분야에서도 적절한 평가방법으로 사용되어졌다. 따라서 네트워크 정보보호 제품 평가요소 선정에 평가요소 이원비교를 통한 평가 항목의 우선순위 결정에 적합한 모델이라고 판단하였고 우선순위 비교에 따라 가중치를 부여한 평가 모델을 제시하려 한다.

### III. 평가 모델의 품질 요소 분석

#### 3.1 정보보호 품질요소 분석

정보보호제품 평가를 위한 방법으로 사용되는

ISO/IEC 15408은 보안감사, 통신, 암호지원, 사용자 데이터 보호, 식별 및 인증, 보안관리, 프라이버시, TSF 보호, 자원활용, TOE 접근, 안전한 경로/채널의 기능 클래스로 분류되어 있다. 이러한 11개의 클래스 구분은 정보보호제품에서 많이 사용되는 기능요구사항들을 분류해 놓은 것이다. 각 제품 유형별로 필요한 기능요구사항은 달라 질 수 있으며 제품에 적합한 기능요구사항을 이용하거나 새로 정의하여 사용할 수 있다. 각 제품들은 동일 제품유형에 대한 필요한 기능요구사항을 템플릿 형태로 정의한 문서인 PP(Protection Profiles)를 이용할 수 있다. 본 논문에서는 네트워크 정보보호제품 유형에 해당하는 PP[26~32]를 분석하여 네트워크 정보보호제품에 적용 가능한 공통 보안요구사항을 도출하여 평가 요소로 사용하고자 한다.

IT보안인증사무국[33]에 게재된 네트워크 정보보호제품 PP는 FW, IPS, VoIP FW(Voice over Internet Protocol FireWall), VPN(Virtual Private Network), 네트워크 장비, 네트워크 자료유출방지, 무선침입방지로 총 7가지이며 이들 PP를 분석한 결과 [Table 2]와 같이 모두 공통적인 보안요구사항 클래스를 사용한다. 각 클래스는 사용자 관점에서 필요로 하는 보안기능에 대한 요구사항이 기재되어 있으며 각 클래스는 다양한 기능요구사항을 정의하고 있는 패밀리를 포함하고 있다. 9개의 클래스를 살펴보면 다음과 같은 기능요구사항을 제공한다. 먼저 보안감사 클래스는 모든 보안 행동에 관련된 정보의 인식, 기록, 저장, 분석을 포함하며 발생 내용과 책임소재를 결정할 때 활용될 수 있다. 암

Table 2. SFR Class used for Network Information Protection Product PP

PP	SFR Class
IPS	(1) Security Audit (2) Cryptographic support (3) User Data Protection (4) Identification and Authentication (5) Security Management (6) Protection of the TSF (7) TOE Access (8) Trusted Path/Channels
VoIP FW	
VPN	
FW	
Network Device	
Network DLP	
WIPS	

호 지원 클래스는 암호키 관리 및 암호 연산을 다루고 있으며 하드웨어, 펌웨어, 소프트웨어로 구현될 수 있다. 사용자데이터보호 클래스는 사용자 데이터와 직접적으로 관련된 보안속성뿐만 아니라 유입, 유출, 저장하는 동안 제품 내의 사용자 데이터를 다룬다. 식별 및 인증 클래스는 사용자의 신원을 설정하고 증명하기 위한 요구사항을 다룬다. 보안관리 클래스는 보안속성, 기능 등을 관리하는 것을 다룬다. 서로 다른 역할 관리와 능력의 분리 같은 역할들의 상호작용이 명세될 수 있다. TSF(TOE Security Functionality) 보호 클래스는 보안 기능을 구성하는 메커니즘의 무결성과 관리에 관련된 기능요구사항 패밀리와, 보안기능과 관련된 데이터의 무결성에 대한 기능요구사항을 포함한다. TOE(Target Of Evaluation) 접근 클래스는 사용자 세션 설정을 통제하기 위한 기능요구사항을 명세한다. 안전한 경로/채널 클래스는 사용자와 제품 기능간의 신뢰된 통신 경로와 제품 기능과 다른 신뢰된 IT 제품 간의 신뢰된 통신 채널에 관한 요구사항을 정의한다.

### 3.2 소프트웨어 품질요소 분석

소프트웨어 분야에 대한 품질의 정의는 기능적 요구사항이나 명세를 기초로 주어진 디자인을 얼마나 잘 준수하는지를 평가하는 기능적인 품질과 SW가 요구사항에 따라 정확하게 만들어 졌는지에 대한 구조적 품질로 구분할 수 있다. ISO/IEC 25000[34]에서 SW 품질과 관련하여 6가지의 분야를 정의하고 있으며 선행 연구에서 사용된 ISO/IEC 25023을 살펴보면 소프트웨어 제품의 품질 평가에 필요한 평가 항목과 각 항목의 상세 평가 방법을 기술하고 있다. 평가 항목은 기능적질성, 신뢰성, 호환성, 사용성, 효율성, 보안성, 유지보수성, 이식성의 8가지로 분류하였고 이를 다시 부특성으로 세분화하여 품질 모델을 정의하고 있다. 8가지의 평가 항목은 각각 부특성 항목들을 가지고 있으며 각 부특성의 세부 평가를 통해 수치화하여 품질을 결정할 수 있다. 예를 들어 신뢰성의 부특성으로 성숙도, 가용성, 결함 허용, 복구 가능성을 가지며 각각의 부특성 평가를 통해 신뢰성 항목의 점수를 결정할 수 있다. 기능적질성은 운영 중에 기능의 정확한 동작, 외부 시스템과의 상호운용 등의 속성 등을 측정하는 것이며 신뢰성은 규정된 조건에서 성능 수준을 유지할 수 있는 소프트웨어 제품의 능력을 정량적으로 측정하는 것이

다. 호환성은 동일한 하드웨어 또는 소프트웨어 환경을 공유하면서 제품, 시스템 또는 구성 요소가 다른 제품 또는 구성 요소와 정보를 교환하고 필요한 기능을 수행 할 수 있는 정도를 측정하며 사용성은 규정된 조건에서 사용되는 경우에 사용자에게 의해 이해 및 학습이 쉽고, 사용의 편리성 등에 대한 능력을 측정한다. 또한 효율성에서는 소프트웨어를 포함한 컴퓨터 시스템의 시간적 반응 및 사용되는 자원을 적절하고 효율적으로 운영하는지 여부를 측정하고 보안성에서는 제품 또는 시스템이 정보 및 데이터를 보호하는 정도를 측정한다. 유지보수성은 소프트웨어가 수정되거나 관리될 때 소프트웨어를 포함하는 시스템, 사용자 또는 유지관리자들의 활동에 관한 속성 등을 측정하고 이식성은 소프트웨어가 새로운 환경에서 사용될 때 적응 및 설치 등에 대한 속성들을 측정한다.

### 3.3 네트워크 품질요소 분석

RFC 3511은 가장 오래된 네트워크 정보보호제품의 하나인 방화벽을 기반으로 한 평가 요소를 나타내고 있다. RFC 3511은 L1~L3에 대한 평가 요소인 IP Throughput, Latency와 Concurrent TCP Connection Capacity(이하 'CC'라 한다.), Maximum TCP Connection Establishment Rate(이하 'CPS'라 한다.), Maximum TCP Connection Tear Down Rate, HTTP Transfer Rate, Maximum HTTP Transaction Rate(이하 'TPS'라 한다.) 등 L4~L7에 대한 평가 요소를 포함하여 Denial Of Service Handling, Illegal Traffic Handling, IP Fragmentation Handling 등 방화벽 자체의 기능 요구사항에 대한 평가 요소도 포함되어 있다. IP Throughput과 Latency는 네트워크상에 초당 데이터를 보낼 수 있는 양과 데이터를 송신한 후 수신까지의 지연시간을 측정한다. CC는 동시에 서비스에 사용할 수 있는 커넥션 수를 측정하며 CPS는 동시에 접속할 수 있는 커넥션 수를 측정한다. TPS는 커넥션 당 여러 개의 트랜잭션이 발생할 수 있으며 동시에 접속할 수 있는 트랜잭션 수를 측정한다. Maximum TCP Connection Tear Down Rate는 동시에 서비스에 접속한 커넥션을 종료하는 수를 측정하는 평가 요소이다. 이들 모두 네트워크 환경에서만 사용되는 품질 평가 요소이다.

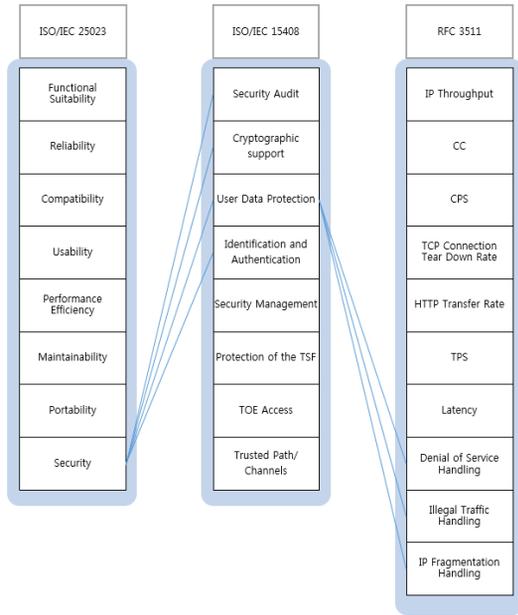


Fig. 3. Comparison of similar quality factors

### 3.4 유사 품질요소 분석

각각의 표준에는 각 제품의 특성에 따른 평가 요소를 선정하고 있기 때문에 다른 표준들에서 유사한 평가 요소들을 찾을 수 있다. 이를 독립적인 평가요소로 선정하게 되면 설문을 통한 가중치 부여 시 중복하여 가중치를 부여받게 되어 본 내용에서는 각각의 표준에서 유사한 항목을 분석하여 동일 평가요소로 분류하고자 한다. 먼저 ISO/IEC 25023에 기술된 보안성 항목을 살펴보면 기밀성, 무결성, 부인 방지성, 책임추적성, 인증성에 대한 평가 방법을 설명하고 있다. 보안성 항목은 이전 버전의 ISO/IEC 9126에서 기능성의 세부 항목으로 정의되어 있었으나 소프트웨어의 보안성이 중요 항목으로 인식 품질 특성으로 추가되었다. ISO/IEC 15408은 인가되지 않은 노출 및 변경, 사용능력 손실로부터 비밀성, 무결성, 가용성 측면의 정보보호를 다룬다고 기술되어 있으며 구체적으로 살펴보면 다음과 같다. 보안감사 클래스에서는 사용자 신원 측면에서 감사대상 사건의 책임추적성에 대한 요구사항을 다루고 있으며 통신 클래스에서는 발신/수신 부인방지에 대해 기술하고 있다. 사용자 데이터 보호 클래스에서는 저장된 데이터의 무결성과 사용자 데이터의 무결성을 기술하고 있으며 전송 데이터의 기밀성에 대해서도 기술하

고 있다. 식별 및 인증 클래스에서는 사용자 식별 및 인증에 대해서 다루고 있다. 즉 ISO/IEC 25023의 보안성 항목은 (Table 3)과 같이 ISO/IEC 15408의 기능요구사항에 모두 포함될 수 있다. 다음으로 RFC 3511의 Denial Of Service Handling, Illegal Traffic Handling, IP Fragmentation Handling 항목을 살펴보면 방화벽 제품의 기능에 대한 평가 요소로 사용되고 있다. 이 3가지 항목에 대해 방화벽 PP[32]에서 동일한 항목을 분석해 보면 사용자 데이터 보호 클래스의 IFC(정보흐름통제 정책), IFF(정보흐름통제 기능) 패밀리에서 주체로/주체로부터의 정보흐름을 유발하는 모든 오퍼레이션에 대하여 정보흐름통제를 강제해야 한다고 기술되어 있어 다른 보안 요구사항과 함께 ISO/IEC 15408의 사용자 데이터 보호 클래스에 포함되어 질 수 있다.

Table 3. Comparison of ISO / IEC 25023 security detail with ISO / IEC 15408 class

ISO/IEC 25023 Security Details	ISO/IEC 15408
Confidentiality	FDP
Integrity	FDP
Non-repudiation	FCO
Accountability	FAU
Authenticity	FIA

### 3.5 품질 평가 요소

상기 유사 품질요소 분석을 통해 중복되는 평가요소를 배제하고 각 표준에서 기술된 평가요소를 모두 품질 평가요소로 선택하기로 한다. 하나의 표준에서 각기 다른 평가요소들은 상호 보완적인 측면을 가지고 있기 때문에 각 표준의 평가요소의 재분배나 추가, 삭제 없이 사용하였다. 이에 따라 상위 정보보호 품질에 대한 [Table 4]와 같이 분류하고 정의하였으며 하위 품질 평가요소는 정보보호 품질 8가지, 소프트웨어 품질 7가지, 네트워크 품질 7가지로 정의하였다.

Table 4. Contents of Quality characteristics

Quality characteristics	Contents
Security quality	The impact of security related items such as traffic analysis, encryption, identification and authentication on network information protection products
Software quality	The impact of quality on software protection requirements such as functionality and compatibility on network information protection products
Network quality	Influence of throughput, CPS, TPS on network information protection products

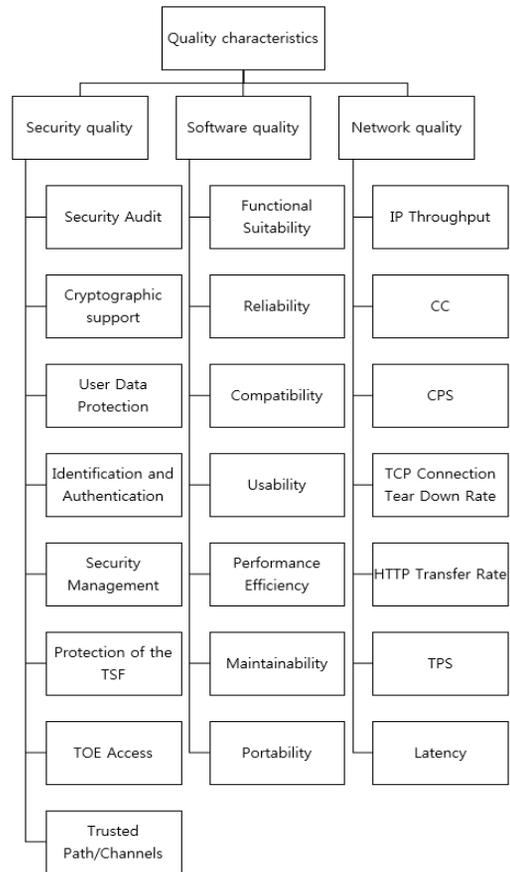


Fig. 4. Network information protection AHP model for product quality evaluation

#### IV. 실증 분석

##### 4.1 전문가 설문 분석

품질 결정을 위한 AHP 계층도는 [Fig.4]와 같다. 첫 번째 정보보호 품질, 소프트웨어 품질, 네트워크 품질 측면에서 구성된 상위 평가 요소에 하위 22개의 평가 요소로 구성하였다. 선정된 평가기준을 기준으로 구성된 모델에 따라 2017년 9월 18일에서 9월 27일까지 총 10일에 걸쳐 설문조사 방식을 통해 전문가의 의견을 수렴하였다. 특정 분야에 한정적인 의견수렴을 배제하기 위해 연구기관, 공공기관, 기업 등의 다양한 업종과 책임자 및 실무자 등 다양한 위치의 전문가로부터 의견을 받았고 네트워크 정보보호제품 기획/운영/관리에서 테스트 평가에 이르는 다양한 전문가의 의견을 [Table 5]와 같이 수집하였다. 설문에 따른 결과 분석은 신뢰성을 높이기 위해 [Table 6]과 같이 일관성 비율(Consistency Ratio, C.R.)을 조사하였고 C.R.이 0.1이하인 평가 항목에 대해서만 결과로 사용하였다. 일관성 비율은 일관성 지수(Consistency Index, C.I.)에 난수지수(Random Index)로 나눈 값으로써, C.R.이 작을수록 일관성이 있다. 또한 응답자 간 의견에 대한 오차를 줄이기 위해 각 설문자의 결과는 기하 평균(geometric mean)을 사용하였다.

먼저 대분류 간 비교에서는 0.47로 정보보호 품질

Table 5. Respondent's baseline data

Category	Content	Count
Organization	University/Research institute	3
	Government/Public institutions	6
	Enterprise	13
	Hospital	1
Career	0~5 years	6
	5~10 years	3
	More than 10 years	14
Number of Network Information Protection Product	0~10 things	7
	10~50 things	12
	More than 50 things	4

Table 6. Consistency ratio of respondent

Respondent	Quality characteristics			Security quality			Software quality			Network quality		
	Max Eigenv alue	C.I.	C.R.	Max Eigenv alue	C.I.	C.R.	Max Eigenv alue	C.I.	C.R.	Max Eigenv alue	C.I.	C.R.
P1	3.00	0.00	0.00	8.09	0.01	0.01	8.14	0.19	0.14	11.71	0.79	0.58
P2	3.00	0.00	0.00	8.25	0.04	0.03	8.78	0.30	0.22	8.11	0.19	0.14
P3	3.04	0.02	0.04	9.06	0.15	0.11	7.20	0.03	0.02	7.20	0.03	0.02
P4	3.15	0.08	0.15	10.13	0.30	0.22	8.82	0.30	0.22	8.67	0.28	0.21
P5	3.20	0.10	0.19	8.68	0.10	0.07	8.21	0.20	0.15	7.71	0.12	0.09
P6	3.00	0.00	0.00	8.44	0.06	0.04	7.06	0.01	0.01	7.08	0.01	0.01
P7	3.00	0.00	0.00	8.30	0.04	0.03	7.35	0.06	0.04	7.79	0.13	0.10
P8	3.00	0.00	0.00	11.18	0.45	0.32	7.20	0.03	0.02	7.26	0.04	0.03
P9	3.00	0.00	0.00	8.86	0.12	0.09	7.65	0.11	0.08	7.66	0.11	0.08
P10	3.43	0.21	0.41	9.99	0.28	0.20	8.23	0.21	0.15	9.64	0.44	0.33
P11	3.04	0.02	0.04	9.46	0.21	0.15	8.39	0.23	0.17	9.11	0.35	0.26
P12	3.00	0.00	0.00	8.11	0.02	0.01	7.00	0.00	0.00	7.06	0.01	0.01
P13	3.00	0.00	0.00	8.07	0.01	0.01	7.46	0.08	0.06	7.00	0.00	0.00
P14	3.00	0.00	0.00	8.25	0.04	0.03	7.39	0.07	0.05	7.81	0.14	0.10
P15	3.00	0.00	0.00	8.33	0.05	0.03	7.12	0.02	0.02	7.26	0.04	0.03
P16	3.01	0.00	0.01	8.68	0.10	0.07	7.54	0.09	0.07	7.77	0.13	0.10
P17	3.02	0.01	0.02	8.56	0.08	0.06	7.29	0.05	0.04	7.32	0.05	0.04
P18	3.07	0.04	0.07	8.30	0.04	0.03	7.74	0.12	0.09	7.69	0.12	0.09
P19	3.00	0.00	0.00	8.87	0.12	0.09	7.29	0.05	0.04	7.96	0.16	0.12
P20	3.00	0.00	0.00	8.09	0.01	0.01	7.13	0.02	0.02	7.11	0.02	0.01
P21	3.09	0.04	0.08	8.25	0.04	0.03	7.44	0.07	0.05	7.76	0.13	0.09
P22	3.01	0.00	0.01	9.28	0.18	0.13	7.55	0.09	0.07	7.43	0.07	0.05
P23	3.01	0.00	0.01	8.44	0.06	0.04	7.12	0.02	0.02	7.45	0.08	0.06

(0.47)이 가장 높은 것으로 나타났다. 제품의 기능성에 따른 소프트웨어 품질(0.15)보다는 네트워크 특성의 품질(0.38)에 대한 순위가 더 높게 나타났으며 정보보호 품질과는 큰 차이가 없는 것으로 나타나고 있다. 정보보호 품질의 세부 품질 요소들 사이의 비교 우선순위는 네트워크 정보보호제품에서 송/수신 데이터의 제어를 다루고 있는 사용자데이터 보호가 가장 우선순위가 높은 것으로 나타났다. 또한 대분류에서 보인 결과와 유사하게 보안관리 등의 기능 관련 중요도가 낮게 평가되고 식별 및 인증, TSF 보호 기능 등에 더 우선순위를 두어 자산 보호 관점에서의 보안성에 더 높은 품질을 기대한다고 답변하였다.

소프트웨어 품질에서는 사용자의 요구사항에 따라 기능이 정확히 구현되고 신뢰되는지를 평가하는 기능

적설성과 신뢰성이 가장 우선순위를 보였다. 또한 정보보호제품의 특성상 한번 설치되면 변경관리가 쉽지 않기 때문에 이식성은 낮은 순위에 기록되었다.

네트워크 품질에서는 HTTP Transfer Rate, CPS, TPS 등이 상위에 기록되어 있으며 사용자가 체감할 수 있는 사용자 단의 성능이 가장 중요하다고 응답하였다.

설문 조사의 분석 결과 평가 요소들에 대한 중요도 우선순위를 파악할 수 있었고 이를 토대로 대분류와 소분류의 가중치의 곱으로 각 소분류의 가중치를 구할 수 있다. 전체 가중치를 [Table 7]과 같이 비교한 결과 사용자 데이터 보호, HTTP Transfer Rate, TSF 보호, TPS 등의 순위로 나타났다. 또한 가중치에서 1 순위를 기록한 HTTP Transfer

Table 7. Analysis results of Main Category and Sub Categories

Quality characteristics	Weight (Ranking)	Sub Categories	Weight (Ranking)	Total Weight	Total Ranking
Security quality	0.47(1)	Security Audit	0.11(4)	0.0517	9
		Cryptographic support	0.08(7)	0.0376	16
		User Data Protection	0.25(1)	0.1175	1
		Identification and Authentication	0.13(3)	0.0611	5
		Security Management	0.07(8)	0.0329	16
		Protection of the TSF	0.14(2)	0.0658	3
		TOE Access	0.11(4)	0.0517	9
		Trusted Path/Channels	0.11(4)	0.0517	9
Software quality	0.15(3)	Functional suitability	0.29(1)	0.0435	13
		Reliability	0.29(1)	0.0435	13
		Compatibility	0.09(4)	0.0135	19
		Usability	0.11(3)	0.0165	18
		Performance efficiency	0.08(6)	0.012	21
		Maintainability	0.09(4)	0.0135	19
		Portability	0.05(7)	0.0075	22
Network quality	0.38(2)	IP Throughput	0.15(4)	0.057	7
		CC	0.13(6)	0.0494	12
		CPS	0.14(5)	0.0532	8
		TCP Connection Tear Down Rate	0.07(7)	0.0266	17
		HTTP Transfer Rate	0.18(1)	0.0684	2
		TPS	0.17(2)	0.0646	4
		Latency	0.16(3)	0.0608	6

rate는 Portability 항목에 비해 15배가 높은 가중치를 보여주고 있다. 이는 보안제품의 특성에 맞게 사용자 데이터 보호, TSF 보호 등의 주요 보안 기능과 HTTP Transfer Rate, TPS 등의 사용자 측면의 품질이 가장 중요하다는 것을 보여준다.

#### 4.2 평가 모델

전문가의 의견을 반영하여 가중치를 부여한 평가 모델은 각 평가 항목에 대한 점수를 산출하여 합산한 결과를 제품의 품질로 결정한다. [Table 7]에 기술된 내용과 같이 각 품질 평가 요소의 평가 결과 값에 Total Weight를 곱하여 합한 값으로 제품의 품질을 객관화한다. 세부적인 평가 적용방법을 살펴보면 먼저 ISO/IEC 15408의 요구사항을 평가하기 위해 평가방법론인 ISO/IEC 18045[35]는 해당 기능에 대한 요구사항을 바탕으로 설계, 구현, 기능

및 취약성 시험 등을 통해 평가를 수행하고 있다. 그리고 현재 ISO/IEC 15408에 따른 CC인증제도 상에서는 해당 요구사항의 만족 여부에 대한 판단만 이루어지고 있으며 각 기능에 대한 가중치는 부여하고 있지 않다. 따라서 현재 제도상에서 본 평가 모델을 사용한다면 해당 기능에 대한 적합 여부에 따라 0점 또는 1점을 부여할 수 있다. 다음으로 ISO/IEC 25023을 살펴보면 각 세부 항목마다 만족여부에 따른 점수화를 할 수 있다. 예를 들어 기능적결성의 항목 중 기능적 정확성에서 정확한 결과를 제공하는 기능의 수(X)에 대해 (1-부정확한 기능의 수/전체 기능의 수)의 방법으로 항목의 점수를 수치화한다. ISO/IEC 25023을 기반으로 한 평가 완료 후 본 모델을 적용하면 해당 항목에 받은 점수에 항목의 중요도의 가중치를 곱하여 제품의 품질을 계량화 할 수 있다. 네트워크 품질의 경우 제안서 등에서 수용 가능한 품질의 수준을 결정하는 경우가 있고 이에 대해

Table 8. Evaluation model application example

Sub Categories	Weight	A	B
SECURITY AUDIT	0.0517	1	1
Cryptographic support	0.0376	1	1
USER DATA PROTECTION	0.1175	1	1
IDENTIFICATION AND AUTHENTICATION	0.0611	1	1
SECURITY MANAGEMENT	0.0329	1	1
PROTECTION OF THE TSF	0.0658	1	1
TOE ACCESS	0.0517	1	1
TRUSTED PATH/CHANNELS	0.0517	1	1
Functional suitability	0.0435	1	1
Reliability	0.0435	1	0.78
Compatibility	0.0135	0.9333	1
Usability	0.0165	1	0.59
Performance efficiency	0.012	0.57.19	1
Maintainability	0.0135	0.50	1
Portability	0.0075	1	0.3533
IP throughput	0.057	1	1
CC	0.0494	1	1
CPS	0.0532	1	1
TCP Connection Tear Down Rate	0.0266	1	1
HTTP Transfer Rate	0.0684	1	1
TPS	0.0646	1	1
Latency	0.0608	0	1
Total( $\sum(\text{Weight} * \text{Score})$ )		0.9264	0.9788

가중치를 부여하는 방식이 있는 경우도 있다. 수용 가능한 품질의 수준 결정에서는 0점 또는 1점을 부여한 후 각 항목에 가중치를 부여할 수 있으며 품질 수준에 따른 가중치 부여 방식을 적용한 후 각 품질 요소에 대한 가중치를 추가로 곱하여 전체 품질을 표현할 수 있을 것이다.

본 평가 모델을 실제 제품 평가에 적용하면 CC인증, GS인증, 성능 평가를 각각 완료 후, [Table 8]의 각 항목 점수를 기입하면 제품의 품질에 대한 점수를 확인할 수 있다. A, B 두 제품에 대한 평가 결과를 보면 CC인증에서는 모든 항목을 반드시 만족하여야 하므로 인증이 완료된 제품의 항목 점수는 1이 된다. GS 인증 결과 각 항목 점수는 각 항목의 하위 부특성 평가 결과를 토대로 결정지어 진다. 기능 적절성은 두 제품 모두 만족하며 신뢰성 등 나머지 6개의 평가 요소에서는 각기 다른 점수를 획득하였다. 네트워크 성능의 경우 Latency를 제외한 모든

항목의 최소 성능 기준치를 통과하였고 A 제품의 경우 Latency가 성능 기준치에 들지 못하여 0점을 획득하였다. 결과적으로 A 제품(0.9264)과 B 제품(0.9788)의 비교에서는 B가 더 우수한 제품으로 결정된다. 더 간단한 예시를 들면 모든 부분에서 1점을 획득한 A, B의 두 제품이 있다고 가정하자. A 제품은 HTTP Transfer Rate에서 0.5점을 획득하고 B 제품은 Security Management에서 0점을 획득하였다더라도 품질 결정 모델에서는 HTTP Transfer Rate의 상대적 중요도에 따라 B제품의 Total Score가 더 높다.

## V. 결 론

제품의 품질에 대해서 결정을 한다는 것은 많은 어려움이 따른다. 각 업체의 이해관계를 비롯하여 평가 대상 업체들은 유리한 항목에 따라 평가를 받고

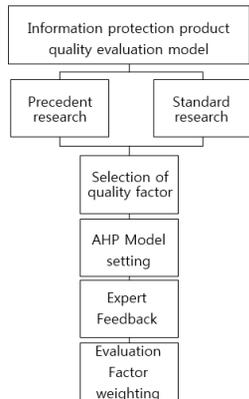


Fig. 5. Information protection product quality evaluation model selection procedure

싶어 하는 것은 어쩌면 당연한 이치다. 여러 논란에도 불구하고 표준, 제도 등 다양한 분야에서 이를 위한 노력을 기울이고 있는 것은 사용자 위주의 시장과 무관하지 않으며 사용자 요구사항에 적합한 제품을 찾기 위한 노력 때문이다. 현재 국내에서 ISO/IEC 15408기반의 CC인증과 ISO/IEC 25023 기반의 GS 인증, RFC 3511의 일부 요소를 사용한 BMT 등을 통해서 고객의 요구사항에 대한 품질을 유지하기 위해 노력하고 있다. 그러나 각각의 평가 활동마다 태생적인 특징으로 인해 정보보호 측면, 소프트웨어 측면, 네트워크 측면에서 일부 미흡한 부분이 있으며 BMT를 제외하고는 인증에 초점이 맞춰져 있어 동일 인증 제품에 대해서 좀 더 우수한 제품을 고르는 쉽지가 않다. 또한 기존의 평가 모델은 정보보호, 소프트웨어, 네트워크 측면의 품질 중 한, 두 가를 기준으로 평가 모형을 제시하는데 비해 이 연구에서는 세 가지 측면을 모두 평가 요소에 사용하여 연구하였고 AHP 기법을 이용한 설문을 토대로 일관성이 결여된 의견을 배제하여 전문가의 의견을 수렴하여 포괄적이고 신뢰성 있는 모델을 제시하였다. 또한 국가정보화 기본법(GS 인증), 소프트웨어산업진흥법(CC 인증), 정보보호산업의 진흥에 관한 법률(성능 평가) 등 국내에서 제도화 되어 있는 평가, 인증 제도를 활용할 수 있어 각기 평가된 제품의 결과를 이용할 수 있는 모델을 제시하였다. 과연 우리가 필요로 하는 제품이 무엇인지, 또는 제품유형에 대해서 과연 이러한 제품은 어떠한 기능이 중요하고 어떠한 요소가 더 중요시 되어야 하는지에 대한 내용을 찾기가 쉽지 않아 구매자의 입장에서는 항상 고민

일 것이라고 생각된다. 본 연구에서는 이러한 고민을 바탕으로 네트워크 정보보호제품의 품질을 결정하기 위해 필요한 요소들을 선행 연구를 통해 찾고 계량화한 평가 요소 가중치 부여에 전문가의 의견 수렴을 통하여 전문성 부여하였다. 또한 비밀관성을 갖는 의견은 배제하여 품질 결정 모델에 사용하여 신뢰성을 높이기 위해 노력하였으며 현재 많이 사용되고 있는 분야의 표준을 이용하였다. 본 논문이 작성된 순서는 [Fig.5]와 같고 동일한 과정의 연구를 통해 다양한 제품 유형에 대한 품질 결정모델을 만들 수 있다. 또한 현재 만들어진 모델을 기반으로 평가 요소 추가/변경/삭제를 할 수 있으며 가중치 부분에서 더 다양한 전문가와 벤더의 의견을 수렴하여 정교한 모델을 만들 수 있을 것으로 생각된다.

## References

- [1] Information security survey(Corporate sector), Ministry of Science, ICT and Future Planning, Dec. 2016
- [2] National Information Protection White Paper, NIS, Apr. 2016
- [3] <http://www.boannnews.com/media/view.asp?idx=52750>
- [4] Crosby and Philip B, "Quality is free: The art of making quality certain.", Signet, 1980.
- [5] Juran, Joseph, and A. Blanton Godfrey, Quality handbook, 5th Ed, McGraw-Hill, pp. 173-178, 1999.
- [6] Regulations for the evaluation and certification of information protection products, Ministry of Science and ICT, Sep. 2017
- [7] Ha-Yong Lee and Hyo-Sik Yang, "Convergence Performance Evaluation Model for Intrusion Protection System based on CC and ISO Standard," Journal of Digital Convergence, 13(5), pp. 251-257, May. 2015.
- [8] Ha-Young Lee and Hae-Sool Yang, "Quality Evaluation Model for Intrusion Detection System based on Security and Performance," Journal of Digital

- Convergence, 12(6), pp. 289-295. Jun. 2014
- [9] ISO and I.E.C, "Information Technology - Security techniques - Evaluation criteria for IT security," ISO/IEC 15408, 2012
- [10] ISO and I.E.C, "Software engineering - Product quality," ISO/IEC 9126, 2003
- [11] Lee Jong-Min, "Investigation in Evaluation Matrix for Security Software Product," Proceedings of the Korean Information Science Society Conference, 33(2C), pp 427-432, 2006.
- [12] Yun, Yeo-Wung and Sang-Ho Lee, "A Study on the Quality Model and Metrics for Evaluating the Quality of Information Security Products," Journal of the Korea Institute of Information Security and Cryptology, 19(5), pp 131-142, Sept. 2009
- [13] ISO and I.E.C, "Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Measurement of system and software product quality," ISO/IEC 25023, 2016
- [14] Yong-Hee Jeon, "Technical analysis and evaluation of intrusion prevention system," REVIEW OF KIISC, 15(2), pp 63-73, Apr. 2005
- [15] Lee Chun Seong, Kim Young Deok, Jang Woong, and Lee Keun Ku, "A Study on the Testing Methodology and Test Cases for DDoS Protection Appliance," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp 537-538, 2011
- [16] Hickman, B., Newman, D., Tadjudin, S., and Martin, T, "Benchmarking methodology for firewall performance. No. RFC 3511", April 2003
- [17] Niemann, Raik, Pflingst, Udo, and Göbel, Richard, "Performance Evaluation of netfilter: A Study on the Performance Loss When Using netfilter as a Firewall", Jan. 2015
- [18] Sheth, Chirag, and Rajesh Thakker, "Performance evaluation and comparative analysis of network firewalls.", ICDeCom, International Conference on. IEEE, pp 1-5, Feb. 2011
- [19] Lyu, Michael R. and Lorrien KY Lau., "Firewall security: Policies, testing and performance evaluation," Computer Software and Applications Conference, COMPSAC 2000. The 24th Annual International. IEEE, 2000
- [20] Tae-In Jung, Jin-Ho Kim, Young-Nyuo Shin, and Hee-Un Park, "Analysis of information protection product performance test trend," REVIEW OF KIISC, 12(5), pp 62-69, Oct. 2002
- [21] TTA, "How to measure performance for network security appliances", TTAS.KO-12.0044, Dec. 2006
- [22] T.L. Saaty, "The Analytic Hierarchy Process," McGraw Hill, 1980
- [23] T.L. Saaty, "How to Make a Decision: The Analytic Hierarchy Process," European Journal of Operation Research, 1990
- [24] Suk-Won Lee and Kyung-Ho Lee, "Decision Making Model for Selecting Financial Company Server Privilege Account Operations," Journal of the Korea Institute of Information Security & Cryptology, 25(6), pp 1607-1620, Dec. 2015
- [25] Seokung Yoon, Haeryong Park, and Hyeong Seon Yoo, "Factor analysis of VoIP Security Checklists using AHP," Journal of the Korea Institute of Information Security & Cryptology, 22(5), pp 1115-1122, Sept. 2012
- [26] NIS, Firewall Protection Profile V1.0, Jun. 2016
- [27] NIS, VoIP Firewall Protection Profile V1.0, Jun. 2016
- [28] NIS, Virtual Private Network Protection Profile V1.0, Jun. 2016
- [29] NIS, Intrusion Prevention System

- Protection Profile V1.0, Jul. 2017
- [30] NIS, Network Device Protection Profile V1.0, Jun. 2016
- [31] NIS, Network Data outflow prevention Protection Profile V1.0, Jul. 2017
- [32] National Intelligence Service, Wireless intrusion prevention system Protection Profile V1.0, Aug. 2017
- [33] <http://www.itscc.kr/>
- [34] ISO and I.E.C, "Information technology - Service management -," ISO/IEC 25000, 2012
- [35] ISO and I.E.C, "Information technology - Security techniques - Methodology for IT security evaluation," ISO/IEC 18045, 2012

### 〈저자소개〉



윤 형 득 (Hyung-Deuk Yoon) 정회원  
 2005년 8월: 경희대학교 컴퓨터공학과 졸업  
 2006년 10월~2011년 6월: 한국인터넷진흥원 선임연구원  
 2011년 6월~현재: 한국산업기술시험원 선임연구원  
 <관심분야> 정보보호, 위협관리, 네트워크 정보보호



이 경 호 (Kyung-Ho Lee) 중신회원  
 1989년 8월: 서강대학교 수학과 학사  
 1997년 8월: 서강대학교 정보통신대학원 석사 졸업  
 2009년 8월: 고려대학교 정보경영대학원 박사 졸업  
 1994년 2월~2013년 12월: 삼성그룹, 네이버(주), 시큐베이스 등 근무  
 2011년 9월~현재: 고려대학교 정보보호대학원 조교수, 부교수  
 <관심분야> 위협관리, 정보보호 컨설팅, 정보보호 및 개인정보보호정책