Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.341

DEA-SBM 모형을 이용한 대기업 계열사 보안관리 체계 효율성 분석

정 혁,[1†] 이 경 호[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

Efficiency Analysis of Security Management System of Affiliates of Conglomerate Using DEA-SBM Model

Hyuk Jung,[1†] Kyung-ho Lee[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

우리나라 대기업은 계열사를 포함한 그룹 전체의 경쟁력 및 기술력을 향상시키고 시너지를 제고하기 위해 서로 정보를 공유하고 인력을 파견하는 등 협력관계를 강화하고 있다. 이에따라 그룹 전체의 정보보호 수준을 높이기 위해 만전을 기하고 있으나 계열사, 협력회사를 우회한 정보유출 사고가 지속적으로 발생하고 있다. 또한 모회사에서 실시하는 계열사의 보안관리 체계 평가결과와 실제 보안수준에 대한 실효성 문제가 제기되어 왔다. 또한 각 회사에서는 보안관리를 위해 투입할 수 있는 자원이 한정되어 있어 그 어느때보다 효율적인 보안관리 체계가 필요한 시점이다. 본 연구에서는 철강분야 기업 계열사의 보안관리 체계 운영의 효율성을 DEA-SBM 모형을 이용하여 검토하고, 분석 결과를 토대로 보안관리 수준 제고를 위한 개선방안을 제시하고자 한다.

ABSTRACT

Conglomerates are strengthening cooperative relations by sharing information and dispatching manpower with each other to improve the overall competitiveness and technology of the group, including affiliates, and to enhance synergy. As a result, we are making every effort to increase the level of information protection of the entire group, but information leakage accidents that bypass affiliates and partner companies continue to occur. In addition, the results of the evaluation of the security management system of affiliates conducted by the parent company and the effectiveness of the actual security level have been raised. In addition, each company has limited resources that can be put into security management, so it is time for an more efficient security management system than ever before. In this study, the efficiency of operating the security management system of affiliates of steel companies is reviewed using the DEA-SBM model, and based on the analysis results, improvement measures to improve the level of security management are suggested.

Keywords: DEA(Data Envelopment Analysis), Security efficiency, Security management system

I. 서 론

우리나라는 기술적, 경제적 가치가 높은 기술을 국가핵심기술로 지정하여 보호하고 있으며, 현재 반도체, 자동차 등 12개 분야 71개 기술이 이에 해당한다. 국가핵심기술을 취급하는 회사는 산업기술의 유출방지 및 보호에 관한 법률이 요구하는 보호조치를 해야 하며, 정부기관으로 부터 주기적으로 국가핵

Received(02. 08. 2022),Modified(03. 29. 2022), Accepted(03. 29. 2022)

† 주저자, omote81@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

심기술의 보호조치가 적절한지 평가를 받고 있다. 이렇듯 국가핵심기술을 취급하는 기업들은 해당 기술을 보호하기 위해 관리적·물리적·기술적 보호를 위한 보안관리 체계를 구축하여 운영하는 등 기술정보 보호에 만전을 기하고 있다. 그럼에도 불구하고 국가핵심기술을 포함한 산업기술의 유출사고는 지속적으로 발생하고 있다. 2016년 이후 5년 6개월 동안 기술유출 사건이 111건 발생하였으며 그 중 반도체·디스플레이 등 국가핵심기술유출은 35건이 발생하였다. 분야별로 전기전자 분야 41건, 디스플레이 17건, 조선 14건, 자동차 8건, 정보통신 8건, 기계 8건 등 이며, 111건 가운데 중소기업에서 적발된 사례가 66건, 대기업 36건, 대학·연구소 8건, 공공기관 1건으로 나타났다 [1]. 핵심 기술정보 보호를 위해 기업들은 자체 보안관리 체계를 강화하는 것 뿐만 아니라 관련 계열사, 협력사 등의 보안관리수준을 높이기 위해 노력하고 있다. 대기업들은 기술개발 및 상용화를 위해 연구개발, 설계 및 제작 등 여러 역할을 수행하는 계열회사를 두고 있으며, 기술 경쟁력을 제고하기 위해 계열사간 협력관계를 강화하고 있다. 정보활용의 개념이 하나의 기업을 넘어 계열회사까지 확장되어 정보 활용과 정보 보호의 개념이 그룹차원으로 확장되었다. 이에따라 대기업 모회사에서는 각 계열사의 보안관리 체계를 점검하고 수준을 주기적으로 평가하는 등 그룹 전체의 보안관리 수준을 향상시키고자 노력하고 있다. 하지만 이러한 노력에도 불구하고 기술유출 사고는 지속적으로 발생하고 있어, 모회사에서 실시하는 계열사의 보안관리 체계 수준 평가결과와 실제 정보보호 수준에 대한 실효성에 대한 문제가 제기되어 왔다. 또한 기업 내에서는 일반적으로 보안수준 향상시키고 보안관리 체계를 보다 효율적으로 운영하기 위해서는 보안 인력, 예산 등 투입요소를 증가시켜야 한다고 여겨왔다. 하지만 기업별로 투입할 수 있는 자원이 한정되어 있기에 보안 분야 또한 그 어느때보다 효율적인 관리체계가 필요하다는 목소리가 나오고 있다.

본 연구에서는 대기업 계열사의 기술자료 보호를 위한 효율적 보안관리 체계 운영 방안을 평가하고 효율성 측정 결과를 통해 보안관리의 비효율성을 분석하였으며 그 결과를 토대로 각 기업별 보안관리 체계 효율성 향상을 위한 개선 방안을 제시하고자 한다. 이를 위해 철강분야 대기업 계열사를 대상으로 해당 모델을 적용하여 그 유효성을 입증하였다.

II. 이론적 배경 및 선행연구

2.1 계열사 보안관리 체계 수준진단 개요

그룹 전체의 경쟁력 강화 및 시너지 제고를 위해 계열사 간의 기술정보 및 중요 경영정보의 공유가 활발히 이루어지고 있다. 생성된 정보를 활용하고 보호해야 하는 주체는 정보를 생성한 회사에 한정되는 것이 아니라 정보를 공유받아 활용하는 회사로 그 범위가 넓어진 것이다. 하지만 그룹 내 각 회사의 규모와 특성에 따라 보안의 중요도에 대한 인식의 차이, 보안관리 수준을 유지 및 향상시키기 위해 투입하는 자원의 종류와 양의 차이로 인해 각 회사별 보안관리 체계의 수준에는 차이가 있다. 이에따라 대기업 모회사에서는 주기적으로 각 계열사의 보안관리 체계 수준을 평가하고 개선방안을 마련하는 등 그룹 전체의 보안관리 체계 수준을 향상시키기 위해 노력하고 있다.

A 철강 회사에서는 매년 계열사의 보안관리 체계의 수준을 진단하고 평가하여 각 회사의 최고경영자에게 그 결과를 피드백하고 개선결과를 확인하는 활동을 하고 있다. 보안관리 체계의 수준 진단은 체크리스트 기반으로 수행하며, 평가에 사용되는 체크리스트는 국정원에서 국가핵심기술 취급사를 대상으로 하는 진단 체크리스트 내용 중 회사 보안관리에 필요한 필수사항만을 사내 전문가 집단에 의해 도출되었으며 매년 대내외 사항을 반영하여 검토되고 있다. 또한, 정보보호 관리가 보안담당자 활동에서 머무르지 않도록 보안관리 체계 수준평가 결과는 한해 계열사의 최종 경영평가에 반영하고 있다. 보안관리 체계 수준 진단을 위해 매년 초 각 계열사 별 진단 일정 및 계획을 수립하여 안내하며 진단 일정이 확정되면 각 계열사에 진단 기준과 상세 항목이 담긴 진단 체크리스트를 보낸다. 계열사에서는 현장 진단 당일 항목별로 증빙할 수 있는 자료를 찾아 제시하고 그에 따라 수준진단을 이행하고 결과를 산출한다. 최종 평가 결과 및 보완해야 할 사항에 대해 진단 후 2주 내 계열사에 제공하며 계열사에서는 보완 계획을 수립 후 1주 내로 회신하며, 보완결과는 차년도 보안관리 체계 수준평가 방문 시 확인한다. 보안관리 체계 진단 체크리스트는 각 회사의 관리적, 물리적, 기술적 보안관리 수준을 종합적으로 평가할 수 있도록 6개 분야, 50개 항목으로 구성되어 있다.

Table 1. Security Management System Evaluation Checklist

Sortation	Number of Items
Security Policy Management	9
Activities to raise awareness of industrial security	9
Human Resource Management	6
Information Asset Management	5
Security Restricted Area Management	5
Information System Management	13
Security Audit Activitis	3

각 항목별 점수는 별도 가중치 없이 5점을 부여하며 항목별 점수를 합산하여 평균 값을 구한 후 백분율 점수로 환산하여 최종 점수를 산정하고 있으며, 점수 산정 방법은 (식 1)과 같다.

$$\frac{\sum_{n=1}^{50} x_n}{50} \times 5 \quad (1)$$

〈 x_n = 항목 점수〉

본 연구에서는 계열사를 대상으로 하는 일반적인 보안관리 체계 효율성 평가 모델을 철강회사 모기업인 A사에서 2021년에 시행한 계열사 보안관리 체계 수준진단 평가 결과에 적용하여 계열사 간 보안관리 체계의 상대적 효율성을 측정하고자 한다.

2.2 효율성의 개념

효율성은 일반적으로 제한된 투입 자원을 활용하여 산출물을 최대화하는 기술을 의미한다[2]. 즉, 투입요소의 사용량에 따른 산출물의 생산량의 비율을 의미하는 것으로, 어떤 투입요소를 선정하느냐에 따라 산출요소의 효율성 결과가 달라지며 생산 조직의 능력, 외부 환경 등이 효율성에 영향을 미친다[3]. 효율성을 측정하는 방법으로 절대적인 측정과 상대적인 측정 방법이 있다. 조직의 보안관리 체계 수준을 평가하고 조직 간 효율성을 비교분석하는데 있어 투입대비 산출요소의 비율에 따른 절대적인 효율성 측정보다는 비교 대상의 조직 중 가장 효율성이 높은 것과 그 외의 조직 간의 효율성을 측정하는 상대적 효율성의 관점을 적용하는 것이 효과적일 것으로 판단된다.

상대적 효율성은 최고의 효율성 측정치와의 상대적인 비율로, 가장 높은 효율성을 1로 표준화하여 나타냈을 때의 상대적인 비율로 표현된다[4].

효율성을 측정하는 방법으로 모수적 측정과 비모수적 측정 방법을 들 수 있다. 전통적으로 많이 사용되는 모수적 방법으로 비율분석, 회귀분석을 들 수 있는데, 비율분석은 어디에서 비효율이 발생하는지 파악하기 어려우며, 기업 전체의 효율성을 파악하기 어렵다는 한계점이 있으며, 회귀분석 방법은 어떤 부분에 어느 정도의 비효율이 있는지 파악하기 어렵다는 한계점이 있다. 이에 반해 비모수적 방법인 DEA는 비효율의 원인을 세분화하여 분석이 가능하며, 효율성 개선을 위한 여러 방안을 제시할 수 있어 상대적 효율성 측정 방법으로 널리 사용되고 있다[5].

2.3 DEA 모형

비모수적 효율성 측정 방법인 DEA(Data Envelopment Analysis)는 선형계획법에 근거한 효율성을 측정하는 방법이다. 통계적으로 구체적인 함수 형태를 정한 뒤 효율성을 측정하는 회귀분석법과 달리 평가대상의 투입 및 산출요소 간의 정보를 이용하여 효율적 프론티어를 도출 후 평가하는 대상이 해당 프론티어 라인으로부터 얼마나 떨어져 있는지를 측정하여 비효율성을 측정하는 방법이다[6]. 효율성의 측정 대상을 의사결정단위(DMU : Decision Making Unit)라고 하며, DMU의 효율성 측정 점수 1의 의미는 가장 효율성이 높다는 것을 의미하며 1 미만의 DMU는 모두 비효율적인 것으로 평가 할 수 있다.

DEA 모형은 Farrell의 연구를 바탕으로 Charnes, Cooper & Rhodes(1978)가 제시한 CCR 모형과, Banker, Charnes & Cooper가 제시한 BCC 모형이 가장 일반적으로 사용되고 있다. CCR 모형은 효율성을 측정하는데 있어 규모에 따른 효과를 고려하는 규모수익불변(CRS : Constant Return to Scale)을 가정하며, BCC 모형은 규모수익가변(VRS : Variable Return to

Scale)을 가정한다. 효율성을 측정할 때 투입요소와 산출요소 중 어떤 요소를 고정한 후 나머지 요소의 비효율성을 파악하느냐에 따라 구분할 수 있는데, 투입량은 변화시키지 않고 산출량을 비례적으로 얼마나 확대시킬 수 있는지를 평가하는 산출지향적 모형(Output-oriented)과 생산된 산출량은 그대로 두고 투입량을 얼마나 비례적으로 감소시킬 수 있는지 평가하는 투입지향적 모형(Input- oriented)로 나눌 수 있으며[6], 투입요소와 산출요소 중 어느 쪽이 통제 가능한지 판단하여 적합한 모형을 이용해야 한다.

2.4 DEA-SBM(Slack Based measure) 모형

DEA 모형을 통해 효율성이 가장 높은 프론티어를 파악할 수 있으며 비효율적인 DMU는 어떤 원인에 의해 비효율성이 나타났는지 규모의 문제인지 파악할 수 있다[8]. 하지만 기존의 DEA 모형은 효율성 측정시 잔여분이 존재하여 비효율적인 상태임에도 효율성 값이 1로 계산되어 효율적인 DMU로 판명될 수 있는 문제가 발생할 수 있다. 예로 <그림 1>에서 투입요소 X1과 X2에 따른 산출요소의 효율성 측정시 일반적인 방사형 모델인 DEA 모형에서는 원점 O를 지나는 효율적 프론티어 상에 위치한 DMU들을 효율적이라고 판단한다. 즉, B와 C는 모두 효율적 프론티어 상에 존재하므로 B, C 모두 효율적인 상태로 판단하게 된다. 하지만 X2의 투입량은 동일하지만 X1의 투입량은 B가 C보다 적으며, 그 크기만큼의 투입요소의 여유분(Slacks)이 존재한다는 것 확인할 수 있음에도 이를 구분할 수 없다는 한계점이 존재한다[9]

반면 비방사형 모형은 방사형 모형에서 지적된 여유분(Slacks)을 포함하여 효율성을 측정하여 여유분이 모두 0인 경우에 가장 효율적인 상태로 판단한다. 이에 따라 보다 일반적인 DEA 모형보다 합리적으로 효율성을 측정할 수 있는 방법으로 볼 수 있다.

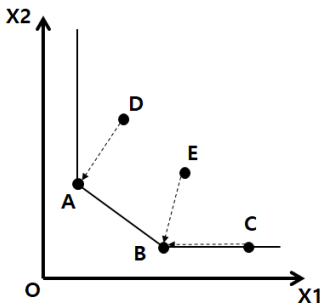

Fig. 1. Non-radial DEA Model

Tone(2001)은 이와 같은 문제점을 보완하고자 잔여기준모형(SBM : Slack-Based Model)을 제안하였으며, 이의 기본적인 수식은 식(2)와 같다.

$$Min\rho_{k^0} = \frac{1-\frac{1}{m}\sum_{i=1}^{m}(\frac{s_i^-}{x_{ik^0}})}{1+\frac{1}{s}\sum_{r=1}^{s}(\frac{s_r^+}{y_{rk_0}})}$$

Subject to

$$x_{ik^0} = \sum_{k=1}^{n} x_{ik}\lambda_k + s_i^-,\ y_{rk^0} = \sum_{k=1}^{n} y_{rk}\lambda_k - s_r^+$$

$$\lambda_k,\ s_i^-,\ s_r^+ \geq 0,\ \forall k, i, r \qquad (2)$$

효율성 척도인 ρ_{k^0} 는 0과 1사이의 값으로 이 값이 1일때, 투입요소의 잔여물 벡터인 s_i^-와 산출요소의 잔여물 벡터인 s_r^+이 모두 0이 될 때 효율적인 상태가 된다. 이렇듯 SBM 모형은 투입 및 산출요소의 잔여분이 모두 0일 때에만 효율적인 상태로 판명하게되어 DEA 모형의 문제점을 보완할 수 있게 되었으며[10], 기존 DEA 모형보다 더 정확하게 DMU의 효율성을 판단하는 기법으로 사용되고 있다[11].

2.5 선행연구 고찰

본 연구의 방향을 설정하고, 연구 목적에 맞는 최적의 변수 설정을 위해 DEA 또는 DEA-SBM 모형을 활용한 조직의 효율성 및 보안관리 효율성 평가를 진행하였던 선행 연구에 대해 조사하였다.

최원녕 등[12]은 민간 기업들의 정보보호 활동에 대한 효율성을 평가하고자 총 15개 DMU를 대상으로 AHP와 DEA 모형을 활용하여 효율성을 분석하였다. 투입요소는 정보보호부문 투자액과 정보보호부문 전담인력 수를 사용하였고 산출요소로는 정보보호 관련 인증평가 점검 건수와 정보보호를 위한 활동 건수를 사용하였다. 이를 통해 상대적으로 정보보호 활동의 효율성이 높은 기업을 선별하고 비효율적인 기업을 대상으로 효율성을 향상시킬 수 있는 방안을 제

시하였다.

김인환[13]은 DEA 모형을 활용하여 자동차 도급업체 36개사를 대상으로 기술자료 보안관리 체계 효율성을 분석하고 이를 향상시키기 위한 개선방향을 제안하고자 하였다. 매출액, IT 투자예산, 전체 임직원 수를 투입요소로, 보안담당자 수, 기술자료 보안 시스템 수, 기술자료 관련 보안수준진단 점수를 산출요소로 설정하였으며, 승용·상용·설비 업체 등 기업의 특성별로 효율성을 분석하였다.

신영진[14]은 DEA 모형을 활용하여 25개 공공기관의 개인정보관리의 효율성을 분석하였다. 투입요소로는 개인정보관리예산, 개인정보관리인력, 정보보호교육현황을, 산출요소로는 개인정보자료관리현황, 홈페이지정보관리현황, 개인정보보호시스템운영, 개인정보관리시스템통제를 선정하고 요소들간의 효율성을 측정하였다.

이태휘 등[15]은 비방사적 DEA 모형인 DEA-SBM 모형을 활용하여 외항해운기업의 경영효율성을 분석하고 시사점을 제시하였다. 총 DMU는 18개로, 투입변수로는 비유동부채, 법인세 비용, 자본을, 산출변수로는 매출액을 선정하였다.

김재원[8]는 DEA-SBM 모형을 이용하여 연구장비산업의 경영 효율성을 분석하여 연구장비산업의 육성을 위한 정책 수립의 중요한 정보를 제공하였다. 총 12개의 DMU를 대상으로 분석을 수행하였으며 투입요소는 총자산, 연구개발비, 종사자수를 선정하였고, 산출요소는 매출액을 선정하였다.

박현준 등[16]은 국내 로봇기업 32개사를 대상으로 DEA-SBM 모형을 활용하여 경영 효율성을 분석하였다. 투입요소로는 인건비, 경상연구개발비, 유형자산, 무형자산을 선정하였으며, 산출요소는 매출액을 선정하였다.

DEA 모형의 사용은 공통된 특성을 가진 집단 내 DMU 간의 경영 효율성을 측정하는 용도로 많이 사용되고 있다. 이를 위한 투입요소는 주로 인건비, 개발비 등의 비용요소와 DMU의 규모를 산정할 수 있는 인원, 자본규모 등을 선정하고 있으며, 산출요소는 객관적 성과지표로 볼 수 있는 매출액을 선정하였다. DEA 모형은 동일 특성 집단 내 DMU 간의 관리적 효율성을 평가하는 용도로도 사용되고 있었으며, 보안 및 개인정보 관리의 효율성 측정을 위한 투입요소로는 IT/보안 예산, 보안 시스템 수, 정보보호 교육현황 등을, 산출요소로는 주로 보안 관리 수준 평가와 관련된 지표를 선정하고 있다. 이는 경영효율성 측정과 관리적 효율성 측정 두 경우 모두 투입요소와 산출요소를 선정할 때에는 둘 사이에 유의미한 상관관계가 있는 요소를 선정하고 있음을 알 수 있다.

III. 연구 방법

3.1 연구 설계

본 연구는 대기업 모회사에서 그룹 전체의 보안관리 수준을 향상시키기 위해 계열사의 보안관리 체계의 효율성을 분석하여 보안관리 체계가 비효율적인 계열사를 대상으로 개선방안을 제시하는데 그 목적이 있다. 상대적 효율성 측정은 앞서 언급한 것처럼 모수적 접근방법인 회귀분석법, AHP 등을 이용할 수 있겠으나, 보안관리 체계의 수준 및 보안관리 효율성의 정도와 그에 영향을 미치는 요인간의 상관관계를 통계적으로 명확히 설명하기 힘들며 여러가지 투입 및 산출요소를 고려하여 효율성을 측정하기 어렵다는 점을 고려하여 보았을때, 본 연구에는 비모수적 접근방법이 적합하다고 판단된다.

또한 상대적 효율성 측정을 위한 비모수적 접근방법 중 대표적으로 사용되는 기본적인 DEA 모형을 활용하기보다 잔여분(Slacks)까지 고려한 DEA-SBM 모형을 활용하므로써 DMU 간의 보다 더 정확한 상대적 효율성을 평가하고자 하였다.

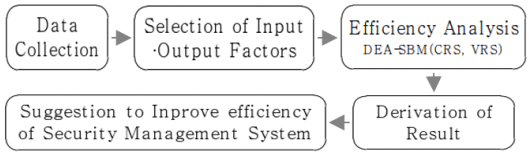

Fig. 2. Efficiency Analysis Model

3.2 의사결정단위(DMU) 선정

DEA 모형을 이용하여 DMU의 효율성을 측정할 때 적절한 DMU의 개수를 선정할 때 몇 가지 적절한 방법이 제안되어 왔다. 첫째, 연구에서 분석대상이 되는 DMU는 투입요소와 산출요소 합의 3배 이상으로 선정해야 한다[17]. 둘째, 투입요소와 산출요소의 곱의 이상으로 DMU를 선정해야 한다[18]. 본 연구의 분석대상이 되는 19 개의 DMU는 앞서 제시된 분석조건을 만족한다고 볼 수 있다.

분석 대상이 되는 19개 계열사는 규모와 업의 특성에 따라 구분하였다. 먼저 규모에 따른 분류는 현 대기업, 중견기업, 중소기업 분류 기준인 매출규모나 자산 규모 등에 따른 분류보다, 임직원 수에 따른 기업 분류 기준에 따라 대기업(종업원 수 1,000명 이상), 중견기업(종업원 수 300명 이상 1,000명 미만), 중소기업(종업원 수 300명 미만)으로 분류 하였다. 또한 본 연구는 국가 핵심기술을 취급하는 철강 대기업 모회사의 계열사에 대한 보안관리 체계에 대한 효율성을 평가하는 것으로 계열사 특성에 따라 분류할 수 있는데, 모회사의 중요 기술 또는 경영정보를 활용하여 사업을 영위하는 핵심 계열사와 모회사의 복지, 자재구매 등 기업 운영을 보조하는 성격의 일반 계열사로 구분할 수 있다.

Table 2. DMU Classification

DMU	Scale	Importance
DMU1	Conglomerate	Core
DMU2	Middle Market ENT	Core
DMU3	Conglomerate	Core
DMU4	Small ENT	General
DMU5	Conglomerate	Core
DMU6	Middle Market ENT	Core
DMU7	Small ENT	Core
DMU8	Small ENT	General
DMU9	Small ENT	General
DMU10	Conglomerate	Core
DMU11	Middle Market ENT	General
DMU12	Small ENT	General
DMU13	Conglomerate	Core
DMU14	Middle Market ENT	Core
DMU15	Middle Market ENT	General
DMU16	Middle Market ENT	General
DMU17	Small ENT	General
DMU18	Conglomerate	General
DMU19	Small ENT	General

3.3 투입 및 산출요소

DEA 모형을 활용하여 계열사의 보안관리 체계의 효율성을 측정하는데 있어 적절한 투입요소와 산출요소를 선정하는 것이 매우 중요하다. 본 연구는 2021년 한해동안 철강업 모회사의 계열사를 대상으로 한 보안관리 체계 현장진단 평가 및 인터뷰 결과를 토대하고 앞서 살펴본 선행연구 조사를 참고하여 투입요소와 산출요소를 선정하였다.

3.3.1 투입요소 선정

투입요소로는 한해 동안의 IT 예산과 보안담당자 수, 보안담당자 전문성 향상 활동 수를 각각 선정하였다.

IT 예산은 IT 및 보안시스템 구축 및 운영, 각종 보안 활동에 필요한 근본적인 요소이다. 다만, 규모가 큰 회사일 수록 IT 예산의 규모가 클 수 밖에 없기에 규모에 따른 투입요소의 절대적 편차를 없애기 위해 IT 예산 금액을 전체 임직원 수로 나눈 1인당 IT 예산 금액을 투입변수로 선정하였다.

보안담당자는 회사 보안관리 활동을 수행하는 주체로서 중요 기술정보를 보호하기 위한 가장 기초가 되는 요소이다. 보안담당자 수의 산출은 보안 전담 인력인 경우는 1, IT 업무와 겸임일 경우 0.5, 재무, 총무, 인사 등 3가지 이상의 업무를 겸임하고 있을 경우 0.3으로 계산하였으며, 보안담당자의 수 또한 회사 규모에 따른 편차를 없애기 위해 임직원 100명당 보안담당자 수로 환산하여 최종 투입요소로 선정하였다.

회사 보안활동의 수준은 보안담당자의 전문성 수준과 비례한다고 볼 수 있다. 이에 따라 한 해 동안 보안 전문성을 높이기 위한 전문 교육, 세미나, 자격취득 등의 활동 이력을 종합한 보안담당자 전문성 향상 활동 건수를 투입요소로 선정하였다.

3.3.2 산출요소 선정

산출요소로는 IT 예산, 보안담당자 등 앞서 선정한 투입요소를 활용하여 회사의 기술 정보를 보호하기 위한 관리체계의 수준을 파악할 수 있는 보안관리 체계 수준진단 평가 항목 중 기술정보보호와 직접적으로 연관이 있는 항목(19개)의 평가 점수를 선정하였다.

Table 3. Input and Output Factors

Category	Details
Input Factors	The number of security personnel per 100 employees.
	Activities to strengthen the expertise of security personnel.
	IT budget per employee.
Output Factor	The results of the evaluation of the technical information management system.

IV. 연구 결과

본 연구에서는 DEA-SBM 모형을 활용하여 규모수익불변의 가정(CRS)과, 규모수익가변의 가정(VRS)을 분석하였다.

4.1 효율성 분석 결과

4.1.1 SBM (CRS) 효율성 측정 결과

〈표 4〉는 SBM(CRS) 모형을 활용하여 상대적 효율성을 분석한 결과이다. 총 19개의 DMU 중 6개의 DMU가 100% 효율성을 나타냈으며 평균 77%, 최솟값은 42%으로 나타났다. 상대적 효율성 분석과 함께 비효율적 집단에 대해서는 벤치마킹 할 수 있는 효율적 집단을 제시하여 비효율적인 부분을 개선할 수 있게 되었다. 예를 들어 58%의 효율성을 나타내는 DMU2는 DMU14를 참조하여 효율성을 개선할 수 있을 것이다. 참조된 횟수가 많은 DMU 일수록 상대적으로 효율성이 높은 집단으로, DMU4와 DMU13이 총 7번 참조되어 상대적으로 가장 효율적인 집단으로 판단할 수 있다.

Table 4. SBM(CRS) Efficiency Analysis

DMU	SBM(CRS)	Reference
DMU1	72%	6,13
DMU2	58%	14
DMU3	61%	14
DMU4	100%	4
DMU5	82%	6,13
DMU6	100%	6
DMU7	55%	13
DMU8	55%	4
DMU9	42%	4
DMU10	68%	4,13
DMU11	66%	4,13
DMU12	99%	4,13,16
DMU13	100%	13
DMU14	100%	14
DMU15	100%	15
DMU16	100%	16
DMU17	51%	4
DMU18	62%	15
DMU19	85%	14,15

Table 5. Input Values

DMU	The Numer of Security personnel per 100 employess	The Number of Activities to strengthen the expertise of security personnel	IT budget per employees (million won)
DMU1	0.1624	4	2.9
DMU2	0.4	3	4.9
DMU3	0.1242	5	6.2
DMU4	0.7246	1	1
DMU5	0.2094	3	2.3
DMU6	0.1214	4	0.6
DMU7	0.3247	3	5.3
DMU8	0.9804	1	18.3
DMU9	0.7895	3	6.5
DMU10	0.2852	2	4.3
DMU11	0.3311	2	4.3
DMU12	0.4054	1	3.9
DMU13	0.0939	2	2.8
DMU14	0.0829	4	0.3
DMU15	0.0378	2	5.2
DMU16	0.1163	1	7.4
DMU17	1	1	7.4
DMU18	0.0903	2	10.5
DMU19	0.0549	3	2.9

〈표 5〉는 최초 각 DMU 별 투입요소의 투입량을 나타내는 것이며, 〈표 6〉은 SBM(CRS) 모델을 활용한 효율성 분석 결과 효율성을 최적화 하기 위한 목표값으로 삼아야 할 투입량을 나타내는 것이다. 예를 들어 DMU5는 효율성을 높이기 위해 100명당 보안인력의 수를 0.2명에서 0.1명으로 줄이고 1인당 IT 예산을 2백3십만원에서 2백1십만원으로 줄일 필요가 있으며, DMU7은 효율성을 높이기 위해 100명당 보안인력의 수를 0.32명에서 0.14명으로 줄이고, IT 예산은 5백3십만원에서 4백2십만원으로 줄일 필요가 있다. 이는 〈표 7〉의 참조집단(Reference) 정보와 함께 비효율성이 나타나는 투입요소의 개선활동을 수행하는 자료로 활용할 수 있다.

Table 6. Input Target Value according to SBM(CRS) Efficiency Evaluation

DMU	The Numer of Security personnel per 100 employess	The Number of Activities to strengthen the expertise of security personnel	IT budget per employees (million won)
DMU1	0.13	4	1.1
DMU2	0.14	3	4.2
DMU3	0.1	5	0.37
DMU4	0.72	1	1

DMU	The Numer of Security personnel per 100 employess	The Number of Activities to strengthen the expertise of security personnel	IT budget per employees (million won)
DMU5	0.11	3	2.12
DMU6	0.12	4	0.6
DMU7	0.14	3	4.2
DMU8	0.72	1	1
DMU9	0.79	1.09	1.09
DMU10	0.11	2	2.79
DMU11	0.11	2	2.79
DMU12	0.41	1	3.76
DMU13	0.09	2	2.8
DMU14	0.08	4	0.3
DMU15	0.04	2	5.2
DMU16	0.12	1	7.4
DMU17	0.72	1	1
DMU18	0.04	2	5.2
DMU19	0.05	2.71	1.88

Table 7. SBM(CRS) Efficiency analysis by company size

Sortation	DMU	SBM(CRS)	Reference
Conglomerate	DMU1	72%	6,13
	DMU3	61%	14
	DMU5	82%	6,13
	DMU10	68%	4,13
	DMU13	100%	13
	DMU18	62%	15
Middle Market ENT	DMU2	58%	14
	DMU6	100%	6
	DMU11	66%	4,13
	DMU14	100%	14
	DMU15	100%	15
	DMU16	100%	16
	DMU19	85%	14,15
Small ENT	DMU4	100%	4
	DMU7	55%	13
	DMU8	55%	4
	DMU9	42%	4
	DMU12	99%	4,13,16
	DMU17	51%	4

4.1.1.1 규모에 따른 SBM(CRS) 효율성 분석

〈표 7〉은 상대적 효율성 평가 결과를 계열사 규모별로 구분한 것으로 대기업군은 총 6개 DMU 중 1개의 DMU가 효율성 100%로 분석되었으며 평균 74%의 효율성을 나타내고 있다. 중견기업의 경우 총 7개의 DMU 중 4개의 DMU에서 효율성 100%가 나타났으며 평균 87%의 효율성을 나타내고 있다. 마지막 중소기업의 경우 총 6개의 DMU 중 1개의 DMU에서 효율성 100%를 나타났으며 평균 67% 효율성을 나타내고 있었다.

4.1.1.2 특성에 따른 SBM(CRS) 효율성 분석

〈표 8〉은 계열사 특성별 상대적 효율성을 평가한 결과로 효율성의 정도와 참조 집단을 나타내고 있다. 핵심 계열사(Core) 총 9개 중 3개의 DMU에서 상대적 효율성 100%가 나타났으며, 평균 77% 효율성으로 나타났다. 일반 계열사(General)의 경우 총 10개의 DMU 중 3개의 DMU에서 효율성 100%가 나타났으며, 평균 76% 효율성을 나타내고 있었다.

Table 8. SBM(CRS) Efficiency analysis by characteristics

Sortation	DMU	SBM(CRS)	Reference
Core	DMU1	72%	6,13
	DMU2	58%	14
	DMU3	61%	14
	DMU5	82%	6,13
	DMU6	100%	6
	DMU7	55%	13
	DMU10	68%	4,13
	DMU13	100%	13
	DMU14	100%	14
General	DMU4	100%	4
	DMU8	55%	4
	DMU9	42%	4
	DMU11	66%	4,13
	DMU12	99%	4,13,16
	DMU15	100%	15
	DMU16	100%	16
	DMU17	51%	4
	DMU18	62%	15
	DMU19	85%	14,15

4.1.2 SBM(VRS) 효율성 분석 결과

이번 연구에서는 규모수익불변을 가정한 CRS 모형과 더불어 규모수익가변을 가정한 VRS 모형을 활용하여 순수기술효율성을 측정하였다. 이는 투입량에 따라 산출량이 일정하게 증가하지 않고 변화가 있다는 것을 가정하므로 기술정보 보안관리 체계의 효율성을 분석하는데 있어 보다 현실성이 있다고 판단된다.

〈표 9〉는 SBM(VRS) 모형을 활용하여 상대적 효율성을 분석한 결과이다. 총 19개의 DMU 중 11개

Table 9. SBM(VRS) Efficiency Analysis

DMU	SBM(VRS)	Reference
DMU1	100%	1
DMU2	74%	3
DMU3	100%	3
DMU4	100%	4
DMU5	100%	5,6,13
DMU6	100%	6
DMU7	64%	5,6,13
DMU8	55%	4
DMU9	42%	4
DMU10	69%	4,6,13
DMU11	67%	4,6,13
DMU12	100%	12
DMU13	100%	13
DMU14	100%	14
DMU15	100%	15
DMU16	100%	16
DMU17	51%	4
DMU18	62%	15
DMU19	100%	19

의 DMU가 100% 효율성을 나타냈으며 평균 83%, 최소값은 42%으로 나타났다. SBM(CRS) 분석 결과와 동일하게 비효율적 집단에 대해서는 벤치마킹 할 수 있는 효율적 집단을 제시하였고, 〈표 15〉에서 효율성을 높이기 위한 투입량의 목표치를 제시하여 비효율적인 부분을 개선할 수 있게 하였다.

Table 10. Input Target Value according to SBM(VRS) Efficiency Evaluation

DMU	The Numer of Security personnel per 100 employess	The Number of Activities to strengthen the expertise of security personnel	IT budget per employees (million won)
DMU1	0.16	4	2.9
DMU2	0.34	3	1.77
DMU3	0.12	5	6.2
DMU4	0.72	1	1
DMU5	0.21	3	2.3
DMU6	0.12	4	0.6
DMU7	0.17	3	2.06
DMU8	0.72	1	1
DMU9	0.72	1	1
DMU10	0.13	2	2.63
DMU11	0.13	2	2.63
DMU12	0.41	1	3.9
DMU13	0.09	2	2.8
DMU14	0.08	4	0.3
DMU15	0.04	2	5.2
DMU16	0.12	1	7.4
DMU17	0.72	1	1
DMU18	0.04	2	5.2
DMU19	0.05	3	2.9

4.1.2.1 기업 규모에 따른 SBM(VRS) 효율성 분석

〈표 11〉 SBM(VRS) 효율성 분석 결과를 기업 규모별로 구분하여 나타낸 것이다. 대기업은 총 6개의 DMU 중 3개의 DMU에서 100%의 효율성을 나타냈으며, 평균 88%의 효율성을 나타내고 있다. 중견기업의 경우 총 7개의 DMU 중 5개의 DMU에서 100% 효율성을 나타내고 있으며, 평균 92% 효율성을 나타내고 있다. 중소기업의 경우 총 6개의 DMU 중 2개의 DMU에서 100% 효율성을 나타내고 있으며 평균 69%의 효율성을 나타내고 있다.

Table 11. SBM(VRS) Efficiency analysis by company size

Sortation	DMU	SBM(VRS)	Reference
Conglomerate	DMU1	100%	1
	DMU3	100%	3
	DMU5	100%	5,6,13
	DMU10	69%	4,6,13
	DMU13	100%	13
	DMU18	62%	15
Middle Market ENT	DMU2	74%	3
	DMU6	100%	6
	DMU11	100%	14
	DMU14	67%	4,6,13
	DMU15	100%	15
	DMU16	100%	16
	DMU19	100%	19
Small ENT	DMU4	64%	5,6,13
	DMU7	100%	4
	DMU8	55%	4
	DMU9	42%	4
	DMU12	100%	12
	DMU17	51%	4

4.1.2.2 특성에 따른 SBM(VRS) 효율성 분석

〈표 12〉은 계열사 특성별 SBM(VRS) 효율성 분석 결과를 구분한 것이다. 핵심(Core) 계열사는 총 9개의 DMU 중 6개의 DMU에서 효율성 100%가 나타났으며, 평균 90%의 효율성을 나타내고 있는 반면, 일반(General) 계열사의 경우 10개의 DMU 중 5개의 DMU에서 100% 효율성이 나타났으며 평균 78%의 효율성이 나타났다.

Table 12. SBM(VRS) Efficiency analysis by characteristics

Sortation	DMU	SBM(VRS)	Reference
Core	DMU1	100%	1
	DMU2	74%	3
	DMU3	100%	3
	DMU5	100%	5,6,13
	DMU6	100%	6
	DMU7	64%	5,6,13
	DMU10	69%	4,6,13
	DMU13	100%	14
	DMU14	100%	14
General	DMU4	100%	4
	DMU8	55%	4
	DMU9	42%	4
	DMU11	67%	4,6,13
	DMU12	100%	12
	DMU15	100%	15
	DMU16	100%	16
	DMU17	51%	4
	DMU18	62%	15
	DMU19	100%	19

Table 13. SBM(VRS) Input Target Value of Core Company

DMU	The Numer of Security personnel per 100 employess	The Number of Activities to strengthen the expertise of security personnel	IT budget per employees (million won)
DMU1	0.16	4	2.9
DMU2	0.34	3	1.77
DMU3	0.12	5	6.2
DMU5	0.21	3	2.3
DMU6	0.12	4	0.6
DMU7	0.17	3	2.06
DMU10	0.13	2	2.63
DMU13	0.09	2	2.8
DMU14	0.08	4	0.3

Table 14. SBM(VRS) Input Target Value of General Company

DMU	The Numer of Security personnel per 100 employess	The Number of Activities to strengthen the expertise of security personnel	IT budget per employees (million won)
DMU4	0.72	1	1
DMU8	0.72	1	1
DMU9	0.72	1	1
DMU11	0.13	2	2.63
DMU12	0.41	1	3.9
DMU15	0.04	2	5.2
DMU16	0.12	1	7.4
DMU17	0.72	1	1
DMU18	0.04	2	5.2
DMU19	0.05	3	2.9

4.1.3 규모의 효율성 측정

규모의 효율성을 측정한 결과 대기업은 평균 86%, 최솟값 61%를 나타냈으며 2개의 DMU에서 100% 효율성을 보였다. 중견기업의 경우 평균 95%, 최솟값 78%의 효율성을 나타냈으며 4개의 DMU에서 100%의 효율성을 보였다. 중소기업의

Table 15. Scale Efficiency Analysis

DMU	SBM(CRS) Efficiency	SBM(VRS) Efficiency	Scale Efficiency
DMU1	72%	100%	72%
DMU2	58%	74%	78%
DMU3	61%	100%	61%
DMU4	100%	100%	100%
DMU5	82%	100%	82%
DMU6	100%	100%	100%
DMU7	55%	64%	86%
DMU8	55%	55%	100%
DMU9	42%	42%	100%
DMU10	68%	69%	99%
DMU11	66%	67%	99%
DMU12	99%	100%	99%
DMU13	100%	100%	100%
DMU14	100%	100%	100%
DMU15	100%	100%	100%
DMU16	100%	100%	100%
DMU17	51%	51%	100%
DMU18	62%	62%	100%
DMU19	85%	100%	85%

경우 평균 67%, 최솟값 86%를 나타냈으며, 4개의 DMU에서 100%의 효율성을 보였다. 계열사 특성별로는 핵심 계열사의 경우 평균 85%, 최솟값 61%를 나타냈으며 3개의 DMU에서 100% 규모 효율성이 나타났다. 일반 계열사는 평균 98%, 최솟값 85%를 나타냈으며 7개의 DMU에서 100% 규모의 효율성이 측정되었다. 상세 결과는 〈표 15〉과 같다.

4.1.4 효율성 분석 결과 소결

본 연구에서는 일반 DEA 모형의 한계점을 극복하고 보다 정확한 상대적 효율성 평가를 하고자 DEA-SBM 모형을 활용하여 기술효율성(CRS), 순수기술효율성(VRS)을 분석하고 이 두 가지 결과를 토대로 규모 효율성을 평가하였다. 〈표 16〉를 살펴보면 기업의 특성 및 규모에 따른 효율성 평가 결과는 규모수익가변를 가정한 경우 평균적인 효율성이 높은 것으로 나타났다. 이는 규모에 따른 효율성보다 투입요소를 산출요소로 보다 효율적으로 전환한 순수기술효율성에 의한 결과로 규모효율성 평가 결과에서도 볼 수 있듯이 보안관리 체계의 효율성은 규모의 영향을 받는 다는 것을 알 수 있다.

효율성 평가 결과 비효율적으로 운영되고 있는 회사는 분석결과 제공되는 참조 기업과 투입요소들의 목표 투입량을 참고하여 효율성을 개선할 필요가 있다. 일반적으로 보안관리 체계의 수준을 향상시키기 위해서는 보안관리에 필요한 보안담당자, 관련 예산 등을 늘려야 한다고 생각할 수 있으나, 다른 기업들과 상대적인 보안관리 체계 효율성을 평가한 결과 오히려 투입요소가 과다하여 효율성이 떨어지는 경우가 다수 발견되었다. 보안관리 체계 효율성 제고를 위해 보안담당자는 직원 수 대비 적절한 수준으로 유지하고 IT 및 보안 인프라 또한 비용 효율화를 할 필요가 있다.

Table 16. Aaverage Efficiency Measurement

Sortation		Average efficiency		
		SBM (CRS)	SBM (VRS)	Scale
Character	Core	77%	90%	86%
	General	76%	78%	98%
Size	Congl.	74%	88%	86%
	Middle	87%	92%	95%
	Small	67%	69%	97%

V. 결 론

5.1 연구결과 종합

본 연구는 대기업의 계열사 보안관리 평가체계에 대한 효율성을 분석하고 이를 바탕으로 개선방안을 제시하는 데 목적이 있다. 이를 위해 철강분야에 해당 모델을 적용하여 유효성을 확인하였으며, 연구의 대상인 19개 계열사의 기술정보 보안관리 체계 평가에 대한 효율성 분석 결과는 다음과 같다.

첫째, SBM(CRS) 효율성 분석에서 총19개 대상 중 78%의 DMU에서 비효율성이 나타났으며, SBM(VRS) 효율성 분석에서 42%의 DMU에서 비효율성이 나타났다. 이는 현 수준의 보안관리 체계를 유지하는데 있어 투입요소의 절감을 통해 보다 효율성을 높일 수 있음을 뜻한다. 초경쟁의 기업환경에서 비용절감은 중요한 경쟁력이다. 보안관리 체계를 효율적으로 운영하기 위해 보안인력과 예산을 확충시키는 것보다 자원의 효율적 투입을 검토해야 한다는 것을 이번 연구를 통해 확인하였다.

둘째, 계열사 특성에 따른 SBM(CRS) 분석 결과 핵심 계열사의 효율성은 평균 77%, 일반 계열사의 효율성은 평균 76%로 나타났으며, SBM(VRS) 분석 결과 핵심 계열사의 효율성은 평균 90%, 일반 계열사의 효율성은 평균 78%로 나타났다. 핵심 계열사는 일반 계열사에 비해 보안관리 수준이 높게 관리되고 있으며 보다 효율적으로 운영되고 있음을 나타내는 것으로, 국가핵심기술보안을 취급하는 제조업, 연구개발업종의 핵심 자회사는 일반 자회사에 비해 보호해야할 자산의 중요성이 높기 때문인 것으로 판단된다. 하지만, 계열사간 실시간으로 정보가 공유되고 시스템이 연결되어 있는 환경에서 보안 사고는 약한 고리에서 발생할 수 있기에 그룹 전체의 보안관리 수준을 높이고 운영 효율성을 향상시키기 위해서는 일반 계열사의 보안관리에 관심을 가질 필요가 있음을 알 수 있다.

셋째, 계열사의 규모별 효율성 분석 결과 CRS, VRS 모두 중견기업, 대기업, 중소기업 순으로 효율적으로 운영되고 있음을 확인하였다. 이는 규모가 작은 중소기업은 투입량을 효율적으로 관리하여 보안관리 체계의 운영 효율성을 높여야 하며, 규모가 큰 대기업 이라고 해서 보안관리 체계의 운영을 효율적으로 하는 것은 아님을 시사하고 있다.

5.2 한계점 및 향후 연구 방향

본 연구는 DEA-SBM 모형을 활용한 대기업 계열사의 보안관리 체계 평가의 효율성 분석 측면에서 실질적인 의미있는 연구 결과를 도출하였다. 그럼에도 불구하고 다음과 같은 한계점이 존재한다. 먼저, 본 연구 대상의 범위가 19개 계열사로 국한되어 있으며 한해 동안의 투입 및 산출 데이터를 활용하였다는 점에서 연구 결과의 실뢰도를 높이기 위해 보다 더 많은 시계열 데이터를 수집하여 분석 필요가 있다. 또한 본 연구는 대기업의 계열사를 대상으로만 분석하였지만, 그룹 전체의 보안관리 체계 효율성 향상에 도움이 되기 위해서 그룹의 개념에 포함되는 해외법인, 협력회사, 고객사 등 보다 광범위한 대상으로 추가적인 연구가 진행되어야 할 것으로 판단된다.

상대적 효율성 측정에 있어 투입요소와 산출요소의 선택이 매우 중요하며, 특히 산출요소와 통계적 유의성이 높은 투입요소를 선택했을때 효율성 측정 결과의 신뢰도가 높아질 수 있는 만큼 보다 다양한 투입 및 산출요소를 선정하여 효율성을 평가 후 결론을 도출할 필요가 있다.

본 연구는 정보보호 수준 평가 점수라는 산출요소를 도출함에 있어 어떻게 투입요소를 효율적으로 구성할 것인가 하는 내용으로, 정보보호 수준 평가 점수가 그 회사의 절대적인 정보보호 수준을 나타내는 것은 아니다. 보안사고 예방과 정보보호 수준 향상을 위해서는 투입요소의 효율적 배분도 중요하며, 회사 상황에 맞춘 보안 Risk 평가 기반인 DoA(Degree of Acceptance)를 고려하여 투입요소 크기의 정도를 결정해야할 필요가 있다.

References

[1] Sedaily, "national core technology leaks", https://www.sedaily.com/NewsVIew/22OZZFATQB, Jan. 2022.

[2] Sang-gyu Woo and Woo-yeol Jeong, "Efficiency assessment university operating system using DEA," Proceedings of the 2015 Summer Academic Presentation of the Korean Society for Government Studies, 2015(6), pp. 279-299, Jun. 2015

[3] S.W.Hwang, D.H.Ahn, S.H.Choi, S.H.Kwon and D.P.Chun, "Efficiency of National R&D Investment," Science and Technology Policy Institute, 2009(24), pp. 1-316, Dec. 2009

[4] Ji-Hyun Baek, "Efficiency Analysis of Defense Industry Company Using DEA and Super-SBM," Journal of the Korea Academia-Industrial Cooperation Society, 21(8), pp. 130-139, Aug. 2020

[5] Buyng-Cheol Kim, "A Comparative Study on Measuring Work Efficiency of DEA, Ratio Analysis and Regression Analysis," Journal of CEO and Management Studies, 22(3), pp. 175-188, Oct. 2019.

[6] Gui-ryong Ha and Suk-bong Choi, "A study on the efficiency of Korean steel industry using a DEA model: focused on technological innovation aspects." Enture Journal of Information Technology, 11(2), pp. 7-20, Aug. 2012.

[7] Suh, Chang Juck and Lee, Jeong Sik, "The Evaluation of Relative efficiency on the Electronic Corporaion Retail Shop Using Data Envelopment Analysis," Journal of Korea Service Management Society, 15(1), pp. 243-268, Mar. 2014

[8] Kim, Jae-won, "Analysis on management efficiency of research equipment industry using DEA-SBM," The journal of Industrial Innovation Study, 37(4), pp. 25-46, Dec. 2021

[9] Kim, Sung-moon and Ha, Hun-Koo, "Analysis of Efficiency and Determinants on the Efficiency of Major Logistics Companies in Korea," Journal of Transport Research, 24(3), pp. 17-26, Jul. 2017

[10] Honggyun Park, "The efficiency of e-Logistics on the Global Logistics Providers Using the SBM Model," Journal of Korea Port Economic

Association, 27(4), pp. 37-49, Dec. 2011
〔11〕 Dong-gi Yum and Hyeon-dae Shin, "Relative Efficiency or Research and Development Business Foundations through Data Envelopment Analysis," Korean Journal of Public Administration, 51(1), pp. 293-319, Mar. 2013
〔12〕 Won-Nyeong Choi, Woo-Je Kim and Kwang-Ho Kook, "An Evaluation of the Efficiency of Information Protection Activities of Private Companies," Journal of convergence security, 18(5), p. 25-32, Dec. 2018
〔13〕 In-hwan Kim and Kyngho-Lee, "Evaluation Model of the Contracting Company's Security Management Using the DEA Model," 27(3), p. 687-704, Jun. 2017
〔14〕 Young-Jin Shin, "Evaluation of private information security in public sector," Korean Association for Local Government Studies, 18(1), p. 87-106, Mar. 2006
〔15〕 Tae-Hwee Lee and Gi-Tae Yeo, "Efficiency Analysis of Ocean Shipping Lines Using Non Radial DE Model," Journal of Korea Port Economic Association, 31(1), pp. 37-49, Mar. 2015
〔16〕 Park, Hyun Jun, Ha, Jeong-Seok, Kang, Yeon Ji, Shim, Woo-Jung, "A Study on the Analysis of Management Efficiency of the Korean Robotics Industry Using DEA-SBM," Journal of Industrial Innovation Study, 33(2), pp. 25-48, Jun. 2017
〔17〕 R. D. Banker, A. Charnes, and W. W. Cooper, "Some models for estimation technical and scale inefficiencies in data envelopment analysis," Management Science, vol. 30, no. 9, pp. 1078-1092, Sep. 1984.
〔18〕 A. Boussofiane, R. G. Dyson, and E. Thanassoulis, "Applied data envelopment analysis," European Journal of Operation Research, vol. 52, no. 1, pp. 1-15, May 1991.

〈저자소개〉

정 혁 (Hyuk Jung) 정회원
2007년 2월: 전남대학교 전자컴퓨터정보통신공학부 학사 졸업
2021년 3월~현재: 고려대학교 정보보호대학원 석사과정
2006년 12월~현재: 포스코 정보보호부서 근무
〈관심분야〉 정보보호 및 개인정보보호정책, 정보보호관리체계, 위험관리

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책