

DEA 모형을 이용한 주요정보통신기반시설 취약점 분석·평가의 효율성 분석

선종욱,^{1†} 이경호^{2*}
^{1,2}고려대학교 (대학원생, 교수)

Analysis of Efficiency of Major Information and Communication Infrastructure Analysis and Evaluation Methods Using DEA Model

Jong-wook Sun,^{1†} Kyung-ho Lee^{2*}
^{1,2}Korea University (Graduate student, Professor)

요 약

오늘날 국가 기반시설의 전자적 침해 행위에 의한 정보통신 인프라의 교란 및 마비가 위협 요소로 대두되고 있다. 이에 정부는 주요 기반시설의 정보시스템 및 제어시스템을 보호하기 위해 주요정보통신기반시설 취약점 분석·평가 제도를 정기적으로 시행하고 있으며 이를 효율적으로 운영하기 위해 매년 늘어난 인적·물적 자원을 투자하고 있다. 그러나 이러한 정부의 노력에도 불구하고 국가 기반시설을 대상으로 한 침해사고가 지속해서 발생함에 따라 정보보호 기반마련을 위한 정부의 자원 투입이 정보보호 활동 결과 산출에 미치는 영향도가 떨어져 평가체계가 효율적이지 못하다는 의문이 제기되고 있다. 따라서 본 연구에서는 주요정보통신기반시설 취약점 분석·평가 제도의 효율적 운용 여부를 DEA 모형을 이용해 검토하고, 분석된 결과를 바탕으로 정보보호 수준 제고를 위한 개선방안을 제안하도록 한다.

ABSTRACT

Today, disturbance and paralysis of information and communication infrastructure by electronic infringement of national infrastructure is emerging as a threat. Accordingly, the government regularly implements the vulnerability analysis and evaluation system of major information and communication infrastructure to protect the information system and control system of major infrastructure, and invests increased human and material resources every year to efficiently operate it. However, despite the government's efforts, as infringement accidents and attempts targeting national infrastructure continue to occur, the government's resource input to prepare the information protection foundation has little effect on the information protection activity result calculation, making the evaluation system not efficient. The question arises that it is not. Therefore, in this study, we use the DEA model to review the efficient operation of the vulnerability analysis and evaluation system for major information and communications infrastructure, and suggest improvement measures to enhance the level of information protection based on the analyzed results.

Keywords: DEA(Data Envelopment Analysis), Security efficiency, Major information and communication infrastructure

I. 서 론

오늘날 인터넷 및 정보통신기술(ICT)의 발전으로 에너지·정보통신·금융·정부 주요시설 등 국가 기반시설의 사이버 의존도가 높아지면서 전자적 침해행위에 의한 정보통신 인프라의 교란 및 마비가 위협 요소로 대두되고 있다. 이에 대해 실제로 2013년 3.20 전산대란, 6.25 사이버 테러, 2014년 한국수력원자력 해킹 공격, 2018년 한국국제협력단 해킹 등 국가 주요 기반시설을 대상으로 한 침해사고 발생뿐만 아니라 사이버 공격 시도 역시 2016년 이후 2020년 6월까지 기관별로 투자진흥공사 1327건, 산업기술시험원 765건, 에너지공단 725건, 가스공사 561건, 한국수력원자력 364건, 강원랜드 356건, 한전 203건, 산업부 94건, 연도별로 2016년 3,725건, 2017년 3025건, 2018년 2582건, 2019년 2488건, 2020년 6월까지 1019건, 총 12,849건으로 집계되는 등 위협이 끊이지 않고 있다[1][2].

이에 정부는 주요 기반시설의 정보시스템 및 제어 시스템을 보호하기 위한 활동의 근거로서 정보통신기반보호법을 제정(2001년)하였으며, 이에 대한 활동으로서 주요정보통신기반시설 취약점 분석·평가 제도를 정기적으로 시행하고 있다. 주요정보통신기반시설 취약점 분석·평가는 대상기관의 관리적, 물리적, 기술적 분야의 취약점을 점검하고 보호대책 수립하는 절차로 구성되어 있으며 정부는 이를 안정적이고 효율적으로 운영하기 위해 매년 늘어난 인력과 예산을 투입하고 있다[3].

그러나 이러한 정부의 의지와 노력과는 다르게 주요정보통신기반시설 취약점 분석·평가를 위한 투자가 매년 늘어나고 있음에도 불구하고 침해사고 및 침해시도가 지속해서 발생함에 따라 정보보호 기반마련을 위한 자원의 투입이 취약점 평가 점수를 포함한 정보보호 활동의 결과 산출에 미치는 영향도가 떨어져 평가체계가 효율적이지 못하다는 의문이 제기되고 있다.

따라서 본 연구에서는 DEA 모형을 이용하여 주요정보통신기반시설 취약점 분석·평가 체계의 효율성을 분석하고, 결과를 바탕으로 주요정보통신기반시설 취약점 분석·평가 대상기관의 정보보호 수준 제고를 위한 개선방안을 제안하도록 한다.

II. 이론적 배경 및 선행연구

2.1 주요정보통신기반시설 취약점 분석·평가

주요정보통신기반시설 취약점 분석·평가는 악성코드 유포, 해킹 등 사이버 위협에 대한 취약점을 관리적·물리적·기술적으로 분석 및 평가·개선하는 제도로서 대상기관의 정보보호 수준 향상을 그 목적으로 한다[4]. 취약점 분석·평가의 수행 주체, 수행 절차, 수행 방법 및 결과 도출의 과정은 다음과 같다.

취약점 분석·평가 수행 주체는 대상기관이 구성한 자체 전담반이 직접 수행하거나, 또는 한국인터넷진흥원과 같은 전문기관, 정부에서 지정한 정보보호 컨설팅 전문서비스 기업 등의 외부기관을 통해 수행할 수 있다. 그러나 대부분 대상기관에서는 전문성을 높이기 위해 외부기관을 통한 취약점 분석 평가를 수행하고 있으며 외부수행인력과 대상기관의 보안담당자가 상호협력하여 취약점 분석·평가를 수행하게 된다.

취약점 분석·평가를 수행하는 세부 절차는 세부 계획수립, 자산식별 및 유형별 그룹화, 세부 취약점 점검항목을 통한 취약점 분석 수행, 위험등급 부여, 개선 방향 수립 순으로 진행되며, 특히 마스터플랜 수립을 통한 개선 방향 수립의 경우 다음 연도 기관의 소요 자원 할당의 근거가 된다.

한편 주요정보통신기반시설 취약점 분석·평가의 대상기관은 공공분야 141개와 관리기관 265개 시설, 민간분야 91개와 관리기관 149개 시설 등 총 414개의 기관을 지정·관리 중이며, 취약점 분석·평가를 위한 세부 점검항목은 관리적 분야 113개, 물리적 분야 18개, 기술적 분야 347개의 세부 점검항목으로 구성되어 있다[6].

2.2 효율성의 개념과 측정

효율성(efficiency)의 개념은 이제까지 많은 학자에 의해 다양한 의미로 해석됐으며 이와 유사한 개념으로는 효과성(effectiveness)이 있으나 본질적인 의미는 서로 다르다[6]. 효율성은 일반적으로 한정적인 투입자원을 사용하여 산출물을 극대화하는 기술을 의미한다[7]. 반면 효과성은 일반적으로 미리 설정해 놓은 목표를 달성했는지에 중점을 두는 개념이다[8]. 즉, 목표 달성을 위한 한정된 자원의 활용은 효율성이고 목표를 달성했는지의 정도는 효과성이라고 해석할 수 있다.

효율성을 측정하는 방법은 절대적 측정 방법과 상대적 측정 방법이 있다. 절대적 효율성 측정 방법은 조직의 투입요소를 물리적인 단위나 모종의 비율로써 표현하는 방법을 나타내며 상대적 효율성 측정 방법은 여러 조직의 효율성을 비교하여 상대적으로 최고 수준의 비율을 나타내는 조직을 표준으로 상대적 비율을 측정하는 방법이다[9]. 일반적인 상대적 효율성 측정 방식을 수식으로 표현하면 식(1)과 같다.

$$\text{효율성} = \frac{\text{산출물(Output)}}{\text{투입물(Input)}} \quad (1)$$

2.3 DEA 모형

2.3.1 DEA 모형의 이해 및 특징

DEA 모형은 Farrell, Charnes, Cooper, Rhodes[10][11][12] 등에 의해 고안된 효율성 분석모델로서 선형계획법에 근거한 효율성 측정 방법을 사용한다. 이는 비율분석, 회귀분석, 생산함수분석과 같은 모수적 측정 방법과는 달리 기존의 생산성 측정 방법의 문제점들을 극복한 비모수적 측정 방법을 말한다. DEA 모형은 효율성 평가대상인 DMU(Decision Making Unit)의 투입요소와 산출요소를 활용하여 경험적 효율 프론티어(frontier)를 구성한 후, 각 DMU가 효율적인 프론티어 라인으로부터 떨어진 거리를 측정함으로써 상대적 효율성을 측정하는 방법이다[13]. 이때 산출요소의 가중치 합을 투입요소의 가중치 합으로 나눈 값을 효율성 값으로 정의하는데 단일 DMU에 대해 효율성 수치가 1인 경우 해당 DMU는 효율적이라고 하고, 1 미만이면 비효율적이라고 한다[14].

DEA 모형은 현재까지 많은 모델이 개발되었으나 Charnes, Cooper, Rhodes(1978)가 개발한 CCR 모형과 Banker, Charnes, Cooper(1984)가 개발한 BCC 모형을 가장 널리 사용하고 있다. 또한 두 모형은 투입요소와 산출요소 중 어느 부분에 초점을 두느냐에 따라 투입지향, 산출지향으로 구분할 수 있으며 투입지향 모형은 산출요소의 수준을 유지하면서 투입량을 비례감소 시키는 모형이고, 산출지향 모형은 투입요소의 수준을 유지하며 산출량을 비례증가 시키는 모형이다[15].

DEA 모형은 다수의 투입 및 산출변수를 고려하여 변수 간 사전 가중치를 결정하거나, 연계된 특정

형태의 함수관계를 규정할 필요가 없는 장점이 있다. 이러한 장점은 업무적 특성상 목표를 가격으로 환산하기 어려워 계량적 분석이 어려운 공공기관의 효율성을 측정하는 데 적합한 특징이 있어 관련된 많은 연구에서 사용되었다[13].

2.3.2 CCR 모형의 특징 및 이해

CCR 모형은 분석대상인 DMU의 투입과 산출이 정비례 관계에 있는 불변규모수익(Constant Return to Scale, CRS) 상태를 가정하고 효율성을 분석하는 모형으로 기술적 효율성과 규모의 효율성이 모두 포함된 지표이다. 따라서 CCR 모형은 규모의 편차가 큰 다수의 DMU 분석 시 효율적 프론티어를 참조하는 과정에서 규모의 차이로 인한 문제점이 발생하는 문제점이 존재한다[16]. 한편 주어진 투입 수준을 고정하고 산출물을 극대화하는 CCR 모형을 수식으로 표현하면 식(2)과 같다.

$$\begin{aligned} \text{Min} h_0 &= \frac{\sum_{i=1}^m v_i x_{io}}{\sum_{r=1}^s u_r y_{ro}} \\ \text{s.t.} \quad \frac{\sum_{i=1}^m v_i x_{ij}}{\sum_{r=1}^s u_r y_{rj}} &\leq 1, \quad j = 1, \dots, n \\ u_r &\geq \epsilon > 0, \quad r = 1, \dots, s \\ v_i &\geq \epsilon > 0, \quad i = 1, \dots, m \end{aligned} \quad (2)$$

한편, 위의 식(2)에서 각각의 변수가 의미하는 내용은 다음과 같다. 변수 h_0 는 DMU의 효율성을 나타내며, 변수 v_i 는 i 번째 투입요소의 가중치, 변수 u_r 는 r 번째 산출요소의 가중치, 변수 x_{ij} 는 DMU j 의 i 번째 투입요소량, 변수 y_{rj} 는 DMU j 의 r 번째 산출요소량을 나타낸다. 또한, 변수 n 은 DMU의 수, 변수 m 은 투입요소 수, 변수 s 은 산출물의 수를 각각 나타낸다.

2.3.3 BCC 모형의 특징 및 이해

BCC 모형은 앞서 살펴본 CCR 모형의 단점을 보완하기 위해 CCR 모형을 완화하여 가변규모수익(Variable Return to Scale, VRS)을 가정하고

불록성 필요조건을 추가한 모형으로 순수 기술적 효율성만을 나타내는 지표이다. 그러나 BCC 모형 또한 효율성 분석 시 상대적으로 규모가 큰 DMU의 개수가 작으면 다수의 DMU가 효율적으로 나타나는 문제점이 존재한다. 한편 주어진 투입 수준을 고정하고 산출물을 극대화하는 BCC 모형을 수식으로 표현하면 식(3)과 같으며 각각의 변수가 의미하는 내용은 Table 3.를 참고한다.

$$\begin{aligned} \text{Min} h_0 &= \frac{\sum_{i=1}^m v_i x_{io} + v_o}{\sum_{r=1}^s u_r y_{ro}} \\ \text{s.t.} \frac{\sum_{i=1}^m v_i x_{ij} + v_o}{\sum_{r=1}^s u_r y_{rj}} &\leq 1, \quad j=1, \dots, n \\ u_r &\geq \epsilon > 0, \quad r=1, \dots, s \\ v_i &\geq \epsilon > 0, \quad i=1, \dots, m \end{aligned} \quad (3)$$

2.3.4 규모의 효율성의 특징 및 이해

규모 효율성은 비효율성의 원인이 비효율적인 운영에 의한 것인지, 아니면 규모에 의한 것인지, 혹은 둘 다에 의한 것인지 확인할 수 있다[17]. 규모의 효율성을 측정하는 방법은 CCR 모형의 효율성 수치와 BCC 모형의 효율성 수치의 비율로 확인할 수 있으며 이를 수식으로 표현하면 식(4)와 같다.

$$SE = \frac{\theta_{ccr}^*}{\theta_{bcc}^*} \quad (4)$$

2.4 선행연구 검토

본 연구에서는 DEA 모형을 통한 공공기관의 효율성 분석을 어떠한 방식으로 진행하였는지에 대한 연구내용과 분석에 필요한 변수선정에 관한 선행연구를 진행하였다.

신영진[9]은 공공기관의 개인정보를 효과적으로 관리하기 위해 국가행정기관, 지방자치단체 교육기관 등 총 25개 DMU를 대상으로 효율성 분석을 하였다. 투입요소는 개인정보 관리예산, 개인정보 관리인력, 정보보호 교육 현황을 사용하였고 산출요소로는 개인정보 관리현황, 홈페이지 정보관리 현황, 개인정

보보호 시스템 운영, 개인정보 관리시스템 통제를 사용하였다.

박태형[18]은 공공부문 정보보호 조직의 수준 제고를 위한 정책 개선 방향을 제시하기 위해 중앙행정기관, 광역 시도 등 총 36개의 DMU를 대상으로 효율성 분석을 수행하였다. 투입요소는 정보보호인력, 정보보호예산을 사용하였고 산출요소로는 보안 인식 교육 횟수, 외부교육 횟수, 외부교육 인원 비율을 사용하였다.

정명수[19]는 공공기관들의 개인정보보호 활동과 기반마련에 대한 효율성을 분석하고, 도출된 효율성을 개인정보보호 관리수준 진단 결과에 반영하여 진단 결과의 효과성과 효율성을 높이기 위한 새로운 모델을 제안하였다. 산하기관, 기초자치단체, 지방공기업 등 26개 DMU를 대상으로 효율성 분석을 수행하였으며, 투입요소는 전체 예산, 전체 직원을 사용하였고, 산출요소는 전담예산, 예산편성 수, 관리수준 점수를 사용하였다.

이홍재 등[15]은 공공부문 국가기관, 공공기관, 교육기관 등 기관유형별 개인정보보호 효율성을 분석하고, 결과를 토대로 정책적 개선사항을 제시하였다. 총 12개의 DMU를 대상으로 효율성 분석을 수행하였으며, 투입요소는 개인정보보호 담당자 수, 개인정보보호 예산을 사용하였고, 산출요소는 제3자 위반 사례 없음, 수집목적 외 위반사례 없음, 민감정보 수집 위반사례 없음을 사용하였다.

김인환[6]은 자동차 도급업체를 대상으로 기술자료 보안관리체계에 대한 효율성을 분석하고, 결과를 평가 결과에 반영하여 개선 모델을 제시하였다. 자동차 업계 도급회사의 1차 부품 및 설비 36개 DMU를 대상으로 승용·산업·설비 특성별로 구분하여 효율성 분석을 수행하였으며, 투입요소는 매출액, IT 투자 예산, 전체 임직원 수를 사용하였고, 산출요소는 보안담당자 수, 보안시스템 수, 보안수준 진단 점수를 사용하였다.

선행연구 검토 결과 공통적인 내용은 다음과 같다. 첫째, 분석대상인 DMU는 같은 업종이거나 같은 목적을 가진 조직에서 선정되었다. 이는 효율성 분석에 타당성이 보장될 수 있도록 같은 성질의 자료를 사용해야 하기 때문이다. 둘째, 연구를 위해 사용한 DEA 모형은 대부분 CCR 모형과 BCC 모형이다. 이는 대상기관의 규모의 차이에서 발생하는 비효율의 원인 및 정도를 파악하기 위해 규모 효율성 분석을 수행하기 위함으로 볼 수 있다. 셋째, 투입요소

선정에 대한 정확한 기준 연구는 없으나 투입요소에는 대부분 공통으로 인력과 예산을 변수로 선정하고 있다. 이는 모든 조직의 운영에 인력과 예산이 기본 요소이며, 산출물을 생산하는데 필수요소이기 때문이다. 넷째, 객관적으로 판단할 수 있는 산출요소를 선정하고 있다. 이는 효율성 평가 결과의 정확성을 확보해야 하기 때문이다.

III. 연구 방법

3.1 연구의 틀

본 연구는 주요정보통신기반시설 취약점 분석·평가 대상기관의 효율성을 분석하고 이를 바탕으로 개선방안을 제시하는 데 그 목적이 있으며, 효율성 분석의 관점을 대상기관의 투자 예산·인력 대비 정보보호 예산, 보안 평가 점수 비율의 관점으로 두고 있다. 이는 곧 정보보호 기반마련과 정보보호 활동 측면의 효율성 분석을 뜻한다.

효율성 분석을 위한 DEA 모형으로는 이론적 배경과 선행연구 검토에서 언급한 내용을 근거로 산출지향 CCR 모형과 산출지향 BCC 모형을 사용하며, 두 모형의 단점을 극복하기 위한 규모 효율성 분석을 동시에 진행하도록 한다. 또한, 투입요소와 산출요소 간 상관분석을 추가로 수행함으로써 정보보호 기반마련에 따른 활동이 효율적으로 이뤄지고 있는지 분석하고, 이를 바탕으로 개선방안을 제시하도록 한다.

3.2 투입요소 및 산출요소 선정

선행연구에 따르면 DEA 모형을 이용한 효율성 분석 시 투입요소, 산출요소 선정에 따라 결과가 크게 달라지므로 연구목적에 적합한 변수 요소 선정이 매우 중요하다[20]. 따라서 이러한 선행연구를 반영하여 선정한 투입요소 및 산출요소는 아래와 같다.

투입요소로는 대상기관의 규모를 확인할 수 있도록 IT 예산과 IT 인력을 각각 선정한다. IT 예산은 정보보호에 필요한 시스템 구축, 컨설팅, 정보보호 전담인력 확보 등 정보보호 체계를 마련하기 위한 근본적 요소로 판단되어 투입요소로 선정하였다. 한편 IT 인력은 DEA를 통한 효율성 분석 시 대부분의 연구에서 공통으로 투입요소에 포함되는 요소이며, 대상기관의 IT 인력 규모에 따라 정보보호 기반을 위한 전담인력 할당 정도를 확인할 수 있는 근본 요

소로 판단되어 투입요소로 선정하였다.

산출요소로는 대상기관의 정보보호 기반마련을 위한 활동 의지를 확인할 수 있도록 정보보호 예산, 기술적 분야의 시스템별 취약점 분석·평가 수준 점수를 각각 선정한다. 정보보호 예산은 IT 예산 및 인력 대비 어느 정도 수준의 전담 예산을 투자했는지 확인하는 지표로서 산출요소로 선정하였다. 기술적 분야의 시스템별 취약점 분석·평가 수준 점수는 정보보호 기반마련과 활동을 통해 얻은 최종적인 산출물로, 해당 기관이 어느 정도 수준의 정보보호 체계를 갖췄는지를 확인하기 위한 산출요소로 선정하였다.

본 연구에서 산출요소는 주요정보통신기반시설 취약점 분석·평가 점수의 관리적, 물리적 분야의 평가 점수를 제외한 기술적 분야의 일부 평가 점수만을 선정하였다. 해당 사유는 타 시스템(보안장비, 제어시스템, PC, WEB, 모바일, 클라우드 시스템)의 평가 점수는 DMU로 선정된 대부분 기관에서 100% 수준을 나타내거나, 해당 시스템이 일부 기관에만 존재하여 평가 점수가 존재하지 않아 효율성 분석 요소로서의 변별력이 없다고 판단되었기 때문이다. 한편 선정된 투입요소와 산출요소를 표로 나타낸 결과는 Table 1.와 같다.

Table 1. Input and output factors

Category	Detail of Factors
Input factors	IT Budget(hundred millions)
	Number of IT employees
Output factors	Information protection budget(hundred millions)
	Server vulnerability score
	Network vulnerability score
	DBMS vulnerability score

3.3 의사결정단위(DMU) 선정

선행연구에 의하면 DEA 모형을 통한 효율성 분석 시 효율성의 과대측정을 예방하기 위한 적절한 DMU 개수를 선정하는 세 가지 방법이 있다. 이는 각각 투입요소 개수와 산출요소 개수 합의 3배 이상으로 선정하는 방법[12], 투입요소 개수와 산출요소 개수의 곱 이상으로 DMU를 선정하는 방법[21],

투입요소 개수와 산출요소 개수 합의 2배 이상으로 DMU를 설정하는 방법[22]이다. 따라서 본 연구에서는 선정된 변수의 개수와 선행연구에 근거하여 두 번째와 세 번째 방법으로 연구를 진행한다.

한편 효율성 분석을 위한 DMU 선정은 2010년부터 2018년 사이의 주요정보통신기반시설 대상기관(전국 시·도 교육청, 지방자치단체, 정부산하기관, 공기업 등) 중 관련 자료수집이 가능한 14개 기관으로 선정하였으며 해당 자료는 기재부의 공공기관 경영정보 공개시스템, 대상기관에 정보공개요청, 인터뷰 내용을 근거로 수집하였다.

IV. 연구 결과

4.1 DEA 효율성 분석 결과

4.1.1 CCR 효율성 분석 결과

CCR 모형을 통한 효율성 측정 결과 14개의 DMU 중 총 7개의 DMU가 효율성 100%로 분석되었으며, 최소값 17.2%, 표준편차 34.6%로 분석되었다. 100%의 효율성을 보이지 못한 7개의 DMU 효율성 점수의 평균은 전체 평균보다 23.4% 낮은 53.3%였으며, 최소 17.2%, 최대 93.3%, 표준편차 39.5%로 분석되었다. CCR 모형을 통한 효율성 분석 상세 결과는 Table 2.와 같다.

Table 2. CCR Efficiency Result

DMU	CCR Efficiency	DMU	CCR Efficiency
DMU01	100%	DMU08	92.8%
DMU02	100%	DMU09	20.5%
DMU03	100%	DMU10	88.4%
DMU04	100%	DMU11	93.2%
DMU05	100%	DMU12	17.2%
DMU06	41.0%	DMU13	100%
DMU07	20.5%	DMU14	100%

4.1.2 BCC 효율성 분석 결과

BCC 모형을 통한 효율성 측정 결과 14개의 DMU 중 총 8개의 DMU가 효율성 100%로 분석되었으며, 최소값 82.9%, 표준편차 0.06%로 분석되었다. 100%의 효율성을 보이지 못한 6개의

Table 3. BCC Efficiency Result

DMU	BCC Efficiency	DMU	BCC Efficiency
DMU01	100%	DMU08	92.8%
DMU02	100%	DMU09	96.0%
DMU03	100%	DMU10	96.9%
DMU04	100%	DMU11	100%
DMU05	100%	DMU12	88.9%
DMU06	82.9%	DMU13	100%
DMU07	87.2%	DMU14	100%

DMU 효율성 점수의 평균은 전체 평균보다 5.3% 낮은 90.8%였으며, 최소 82.9%, 최대 96.9%, 표준편차 5.4%로 분석되었다. BCC 모형을 통한 효율성 분석 상세 결과는 Table 3.와 같다.

4.1.3 규모 효율성 분석 결과

규모 효율성 측정 결과 14개의 DMU 중 총 7개의 DMU가 100%로 분석되었으며, 최소값 19.4%, 표준편차 33.6%로 분석되었다. 100%의 효율성을 보이지 못한 7개의 DMU 효율성 점수의 평균은 전체 평균보다 28.7% 낮은 49.8%였으며, 최소 19.4%, 최대 93.3%, 표준편차 34.8%로 분석되었다. 한편 규모 효율성을 통한 분석 상세 결과는 Table 4.와 같다.

Table 4. Scale Efficiency Result

DMU	CCR E.	BCC E.	Scale E. (CCR E./BCC E.)
DMU01	100%	100%	100%
DMU02	100%	100%	100%
DMU03	100%	100%	100%
DMU04	100%	100%	100%
DMU05	100%	100%	100%
DMU06	41.0%	82.9%	49.5%
DMU07	20.5%	87.2%	23.5%
DMU08	92.8%	92.8%	100%
DMU09	20.5%	96.0%	21.4%
DMU10	88.4%	96.9%	91.4%
DMU11	93.2%	100%	93.3%
DMU12	17.2%	88.9%	19.4%
DMU13	100%	100%	100%
DMU14	100%	100%	100%

4.2 DEA 효율성 분석 결과 소결

앞선 연구 결과에서 CCR 모형과 BCC 모형을 통해 각각 기술효율성, 순수 기술효율성을 분석하고, 이를 활용한 규모 효율성을 분석하였다. 그 결과 비효율적으로 분석된 대상기관은 순수 기술적인 요인보다는 규모적 요인에 의한 것임을 알 수 있었으며 이를 개선하기 위해 투입요소를 줄이거나 산출요소를 늘리는 방법을 택할 수 있다. 그러나 공공기관의 특성상 정해진 투입요소의 조절이 탄력적이지 못하므로 산출요소를 극대화하는 방향으로 개선방안을 모색해야 한다고 보인다.

4.3 상관관계 분석 결과 및 소결

본 연구에서는 주요정보통신기반시설 취약점 분석·평가 대상기관의 효율성 분석을 위한 투입요소와 산출요소의 상관관계 분석을 통해 투입과 산출이 어떤 관계에 있는지 분석하여 정보보호 기반마련에 따른 활동의 효율성을 확인하였다.

Table 5.을 참고하면 투입요소(① IT 예산, ② IT 직원)와 산출요소(③ 정보보호 예산, ④ 서버 평가 점수, ⑤ 네트워크 평가 점수, ⑥ DBMS 평가 점수) 간 상관관계가 모든 요소에 대해 정비례하지 않으며 통계적으로 유의미한 상관관계가 아님을 알 수 있다. 이는 정보보호 기반마련을 위한 인력과 예산의 투입이 정보보호 활동 측면으로서의 산출로 효율적이지 못한 것으로 해석할 수 있다.

Table 5. Correlation Analysis

Variables	①	②	③	④	⑤
① IT Budget					
② IT Employee	.80**				
③ Infosec budget	.67**	0.42			
④ Server	-0.16	0.01	0.31		
⑤ network	-0.1	-0.12	0.22	0.52	
⑥ DBMS	.55*	0.25	.66*	-0.03	0.2

p < 0.01(2-tailed).**
p < 0.05 level(2-tailed).*

V. 연구 결론

5.1 연구 요약

본 연구는 주요정보통신기반시설 취약점 분석·평가 대상기관의 정보보호 기반마련에 따른 활동 측면의 효율성에 문제를 제기하고 이에 대한 검증을 통하여 정보보호 수준 제고를 위한 정책적 개선방안을 제안하는 것을 목적으로 시작하였다.

이를 위해 먼저 연구의 목적을 구체화하기 위해 주요정보통신기반시설 취약점 분석·평가와 DEA 모형에 대한 이론적 검토를 수행하였으며, 연구와 관련된 개념을 분석하고 설명하기 위해 DEA 모형을 통한 공공부문의 효율성 분석에 대한 선행연구 검토를 진행하였다. 그리고 연구의 틀을 통해 효율성 분석의 관점과 사용할 DEA 모형, 투입 및 산출요소와 DMU 선정 사유, 자료를 수집한 방법 등에 대해 논의하였다.

연구 결과를 중심으로 더욱 구체적으로 정리된 내용은 다음과 같다.

첫째, 주요정보통신기반시설 취약점 분석·평가 대상기관의 CCR, BCC, 규모 효율성 분석을 수행한 결과, CCR 분석에서는 반수 이상 기관이 비효율적인 것으로 나타났으며 비효율성 평균이 53.3%로 나타났다. BCC 분석에서는 CCR 분석에 비해 다소 적은 6개 기관이 비효율적인 것으로 나타났으며 평균 비효율성은 90.8%인 것으로 나타났다. 또한, 이들을 활용한 규모 효율성 분석에서는 CCR 분석과 마찬가지로 반수 이상의 기관이 비효율적인 것으로 나타났으며 평균 비효율성은 49.8%였다.

둘째, 투입요소와 산출요소 간 상관관계 분석을 수행한 결과, 투입요소인 (IT 예산 및 IT 인력)과 산출요소인 (정보보호 인력 및 각 보안 평가 점수)가 모든 상관관계에 있어 정비례하지 않았으며 통계적으로도 유의미한 상관관계를 나타내지 않았다.

5.2 연구의 결론 및 개선방안

본 연구로 확인한 주요정보통신기반시설 취약점 분석·평가 대상기관의 비효율성 원인을 고찰하면 아래와 같은 해석이 가능하다.

첫째, DEA 모형을 통한 주요정보통신기반시설 취약점 분석·평가의 효율성을 분석한 결과, 반수 이상의 대상기관이 비효율적인 수준으로 나타났다. 이

는 정보보호 기반마련을 위한 정보보호 활동의 효율성이 미비함을 의미하며 이러한 문제점을 개선하기 위해 투입량 조절 또는 산출량 조절 중 한 가지를 선택할 수 있다. 그러나 앞서 언급한 정부 기관 특성상 투입량 조절을 통한 개선 방법은 적합하지 않다. 이에 본 연구에서 제안하는 개선방안은 투입의 질적인 개선을 통한 산출량 극대화 방식이다. 실제로 여전히 많은 공공기관에서 비전공자를 정보보호 담당자로 임명하고 있으며 이 또한 대부분 순환보직과 겸직을 통한 임시보직인 경우가 많다. 이러한 보안담당자의 비전문성은 낮은 업무 이해도와 책임 의식 결여로 인한 보안사고를 초래할 수 있다. 따라서 이러한 문제를 조직의 환경적·구조적 개선을 통한 높은 수준의 보안 전문 인력을 운용함으로써 개선할 수 있다.

둘째, 투입·산출요소 간 상관관계를 분석한 결과 통계적으로 유의미하지 않았다. 이는 투입과 산출이 정비례하지 않다는 것을 의미하며 대상기관의 취약점 분석·평가 활동이 비효율적인 것으로 해석할 수 있다. 따라서 이러한 문제를 해결하기 위해 투입에 대한 산출 왜곡을 최대한 줄일 수 있는 환경을 구성할 필요가 있으며 이는 평가항목의 재구성을 통한 평가 점수의 효과성 향상으로 개선할 수 있다. 실제로 대상기관의 취약점 분석·평가 진행 시 평가 점수를 산출하는 과정에서 특정 시스템을 대상으로 한 평가항목이 존재하지 않아 모든 대상에 동일한 평가기준을 적용하지 못해 평가점수가 실제 보안수준을 반영하지 못하는 경우가 많다. 따라서 이러한 문제에 대해 실제 보안수준을 평가점수에 효과적으로 반영할 수 있는 개선된 평가항목과 평가방법을 개발함으로써 대상기관의 효율성을 높일 수 있다.

5.3 연구의 한계 및 향후 연구

본 연구는 DEA 모형을 통한 보안수준 평가의 적절성 분석 측면에서 의미 있는 연구라고 보이나 다음과 같은 한계점을 가질 수 있다.

첫째, DEA 모형은 효율성 차원의 성과를 평가하는 모델로 일정 수준 이상의 기본상태를 유지해야 하는 보안수준 평가에 적용하는 것은 그 한계가 있다. 둘째, DEA 모형은 상대적 효율성 평가 방법이기 때문에 모든 기관을 대상으로 한 전체적인 해석이 어렵다. 셋째, DEA 모형 자체의 특성으로 변수의 선택에 있어 본 연구에 쓰인 요소 외에 정보보호 조직에서 활용하는 추가 요소가 존재할 수 있다. 넷째, 투

입에 대한 산출 효율성이 높은 개선된 구체적 평가 모델을 도출하지 못하였다.

위에서 언급한 연구의 한계점을 보완하기 위해 향후 연구에서는 더욱 충분한 자료확보와 다양한 요소 분석이 추가로 수행되어야 하며, 이를 바탕으로 시기별·특성별·규모별 요건을 충족하여 더욱 다양한 관점에서의 효율성 분석을 수행해야 한다. 추가로 주요정보통신기반시설 취약점 분석·평가의 효율성 제고와 연계된 구체적인 평가 모델 개발에 관한 연구를 진행할 필요가 있다.

References

- [1] Union News, "More than 10,000 hacking attempts for the Ministry of Industry and affiliated organizations in 5 years", <https://www.yna.co.kr/view/AKR20201009019800003>, Oct. 2020
- [2] ZDNet Korea, "Korea International Cooperation Agency hacked 7,000 personal information leaked", <https://zdnet.co.kr/view/?no=20180626085457>, Jun. 2018
- [3] Public institution management information disclosure system, "Status of employees of public institutions" <http://www.alio.go.kr/statisticsStat7.do>, Jun. 2021
- [4] Ministry of Science and ICT Notice No. 2021-28 (2021).
- [5] NIS, et al National Information Protection White Paper", Jun. 2020
- [6] In-hwan Kim and Kyung-ho Lee, "Evaluation Model of the Contracting Company's Security Management Using DEA Model," M.S. Thesis, Korea University, Aug. 2017
- [7] 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, pp.

- 279-299, Jun. 2015
- [8] Sung-min Park, Heon Kim and Dong-hyun Baek, "Evaluation of R&D projects in electric power industry with efficiency and effectiveness," *Journal of IE Interfaces*, 22(3), pp. 192-204, Sep. 2009
- [9] Young-jin Shin, "Personal information protection analysis efficiency analysis in public sector," *Journal of Local Government Studies*, 18(1), pp. 87-106, Mar. 2005
- [10] M.J. Farrell, "The measurement of productivity efficiency," *Journal of the Royal Statistical Society*, vol. 120, no. 3, pp. 253-290, Mar. 1957
- [11] A. Charnes, W.W. Cooper, and E. Rhodes, "Measuring the efficiency of decision making units," *European Journal of Operational Research*, vol. 2, no. 6, pp. 429-444, Nov. 1978
- [12] 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.
- [13] Jung-dong Lee and Dong-hyun Oh, *Efficiency Analysis Theory: DEA: Data Envelope Analysis*, IB Book, Seoul, 2010.
- [14] Sung-mook Lim, "A Method for Selection of Input-Output Factors in DEA," *Journal of IE Interfaces*, 22(1), pp. 44-55, Dec. 2009
- [15] Hong-jae Lee, Mee-kyung Park and Yong-jin Cha, "Evaluation of personal information protection efficiency by type of institution in the public sector," *Korean Journal of Policy Analysis and Evaluation*, 26(4), pp. 163-188, Dec. 2016
- [16] Bong-young Hong, "The comparison between CCR and BCC model," *The Journal of the Institute of Social Science*, 12(1), pp. 17-22, Feb. 2005
- [17] Seung-hyun Ban and Dong-hun Han, "An efficiency analysis of Korean software companies using DEA," *The e-Business Studies*, 15(3), pp. 197-213, Jun. 2014
- [18] Tea-hyoung Park, Ki-chan Yoon, Sin-yong Moon, and Jong-in Lim, "Evaluating the efficiency of information security organizations in public sector using DEA models," *Journal of the Korea Institute of Information Security & Cryptology*, 20(6), pp. 209-220, Dec. 2010
- [19] Myung-su Jung and Kyung-ho Lee, "A Study on personal information protection management assessment method by DEA," *Journal of Korea Institute of Information Security & Cryptology*, 25(3), pp. 691-701, Jun. 2015
- [20] Konshik Kim, "Analyzing the technical efficiency of Korean engineering and construction firms after the financial crisis," *Korean Journal of Construction Engineering and Management*, 6(1), pp. 151-161, Feb. 2005
- [21] 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
- [22] B. Golany and Y. Roll, "An application procedure for DEA," *OMEGA International Journal of Management Science*, vol. 17, no 3, pp. 237-250, Dec. 1989
- [23] Kyung-joo Lee, Jung-lo Park and Jae-jun Kim, "Management Efficiency Prediction Model for the Korean Construction Firms Using DEA-Logit Methodology," *Journal of the*

- architectural institute of Korea structure&Construction, 28(11), pp. 167-174, Nov. 2012
- [24] Yong-hwan Lim, "Analyzing the Efficiency of Defense Basic Research Projects using DEA," Journal of Korean Industry-Academic Technology Society, 21(7), pp. 517-524 Jul. 2020
- [25] Kyoung-soo Seo and Hyun-mi Ahn, "Urban railway train operation efficiency studies using DEA," Proceedings of the Fall Conference of the Korea Railroad Association, pp. 446-459, Oct. 2016
- [26] Dong-gi Ryum and Hyun-dae Shin, "Evaluation of the relative efficiency of industry-academic cooperation groups using data envelope analysis (DEA)," Administrative Thesis, 51(1), pp. 293-319, Mar. 2013
- [27] Young-kyu Lee and Jee-ho Bang, "A Study on Improvement of Vulnerability Checklist for the Critical Information and Communication Infrastructure Management/Physical field," M.S. Thesis, Konkuk University, Nov. 2017

〈저자소개〉



선 중 욱 (Jong-wook Sun) 정회원
 2014년 8월: 광운대학교 컴퓨터소프트웨어학과 졸업
 2014년 11월: ㈜에스피에이스
 2016년 5월: ㈜파수닷컴
 2019년 10월~현재: 정보보호컨설팅 프리랜서
 2018년 8월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
 <관심분야> 위협분석, 정보보호컨설팅, 정보보호 및 정보보호정책



이 경 호 (Kyung-ho Lee) 정회원
 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> 위협관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책