Information Systems Review
Vol. 22, No. 2 May 2020 http://dx.doi.org/10.14329/isr.2020.22.2.201

침해사고 통계 기반 정보보호 투자 포트폴리오 최적화: 유전자 알고리즘 접근법

Optimization of Information Security Investment Portfolios based on Data Breach Statistics: A Genetic Algorithm Approach

임 정 현 (Jung-Hyun Lim) 충북대학교 대학원 경영정보학과 석사
김 태 성 (Tae-Sung Kim) 충북대학교 경영정보학과 교수, 보안경제연구소장, 교신저자

요 약

정보보호는 기업의 운영과 고객의 신뢰를 보장하는 필수요소이며 침해사고 예방을 통해 불확실한 피해를 완화시킬 수 있기 때문에 적절한 정보보호 대책의 선택과 적정투자 수준을 결정하는 것이 중요하다.

본 연구는 다양한 산업군에 속해있는 기업에서 정보보호 대책 투자에 활용할 수 있는 예산 범위에서 구성할 수 있는 최적의 정보보호 대책 포트폴리오 구성뿐만 아니라, 각 대책의 적절한 투자 수준에 대한 의사결정 지원 모델을 제시한다. 이를 위하여 산업군별 침해사고 유형 통계를 분석하고 유전자 알고리즘을 활용하여 최적 정보보호 대책 투자 포트폴리오를 도출한다. 도출된 모델을 기존 유전자 알고리즘을 이용한 정보보호 대책 투자 최적화 모델과 비교하고 기업 대상 설문 조사를 통하여 실제 사례를 분석한다.

키워드 : 정보보호 투자, 유전자 알고리즘, 투자 최적화, 침해사고 통계

Ⅰ. 서 론

정보통신기술의 발전으로 정보보호의 대상이 기존 정보통신기기에서 주변 모든 사물로 확대되고 그 피해 범위 또한 확대될 것으로 보인다. 따라서 정보보호를 고려하지 않은 정보통신기술의 안정적인 발전과 진화는 불가능할 것으로 보인다(과학기술정보통신부, 2019). 정보보호 위협의 고도화·지능화에 따라 정보보호의 중요성을 인식하고 각 조직에서 정보보호 예산을 수립하고 있으나 IT 예산 중 정보보호 예산이 차지하는 비율은 높지 않다. 2018년 정보보호 실태조사에 따르면 경영진의 정보보호 중요성 인식은 90.2%로 전년 대비 2.8% 증가하였다(과학기술정보통신부, 2019). 하지만, 2017년 1년간 IT 예산 중 정보보호 또는 개인정보보호 예산을 편성한 사업체는 36.2%로 전년 대비 11.9% 감소하였으며 IT 예산 중 정보보호 예산이 차지하는 비율은 1% 미만이 25.2%, 1~5%는 9.2%, 5% 이상은 1.7%에 불과했다. 2017년 침해사

† 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2018S1A5A2A01039356).

고를 경험한 사업체의 비율은 2.2%로 나타났으며 2019년 국내 사업체 중 2.3%가 침해사고를 경험했다고 응답하여 침해사고는 꾸준하게 발생하고 있는 것으로 나타났다(한국인터넷진흥원, 2018). 따라서 정보보호 의사결정 과정에 대한 다양한 접근 방법을 통해 정보보호 수준의 향상과 정보자산의 보호가 필요하다(김종기, 김지윤, 2018).

정보보호는 기업의 운영과 고객과의 신뢰를 보장하는 필수요소이며 적절한 정보보호 대책의 선택은 적정투자 수준을 결정하고, 기업 운영비용을 최소화할 수 있는 가이드라인을 제공한다(공희경 등, 2008). 또한, 적절한 정보보호 대책은 침해사고 사전 예방을 통해 불확실한 피해를 완화시킬 수 있다(Benaroch, 2018).

본 연구는 정보보호 침해사고를 대응하기 위한 정보보호 투자 의사결정 지원 모델을 제안한다. 침해사고에 대한 정의와 산업군별 침해사고 유형 통계분석을 수행하고, 산업군별 최적 정보보호 대책 포트폴리오를 구성한다. 이를 통해 정보보호 투자에 대한 가이드라인을 제시하고 기업의 정보보호 의사결정을 지원하는데 도움이 되고자 한다.

기존의 유전자 알고리즘을 이용한 최적 정보보호 대책 포트폴리오 구성 관련 연구에서는 정보보호 대책 도입여부만을 고려하였기 때문에 각 대책에 대한 적절한 투자 수준을 결정하는데 어려움이 있었다(Gupta *et al.*, 2006; 김길환 등, 2018).

본 연구의 구성은 다음과 같다. 제Ⅰ장에서는 연구의 배경과 필요성, 연구 목적과 구성을 제시함으로써 본 연구의 의도를 설명한다. 제Ⅱ장은 문헌연구로 정보보호 투자 효과 예측과 관련한 연구와 유전자 알고리즘을 활용한 정보보호 투자 포트폴리오 구성에 관한 연구를 고찰한다. 제Ⅲ장에서는 연구에 활용되는 연구 데이터와 최적화 탐색 기법을 설명한다. 제Ⅳ장에서는 기존 유전자 알고리즘을 활용한 정보보호 투자 최적화 알고리즘과 본 연구에서 제시한 알고리즘과의 성능을 비교하고 산업군별 실제 사례에 모델을 적용한다. 제Ⅴ장 결론에서는 연구의 결과 및 시사점을 설명하고 연구의 한계점과 향후 연구방향을 제시한다.

Ⅱ. 문헌고찰

정보보호 투자 효과를 예측하거나 정보보호 최적 포트폴리오를 구성하고 가치를 평가하는 연구는 이전부터 꾸준히 진행되고 있다. Bodin *et al.*(2005)은 AHP 평가 방법을 사용하여 정보보호 시스템 개선을 위한 대안을 평가하는 기준을 제시하였으며, 정보보호 투자 의사결정 지원 모델을 제시하였다. Gordon and Loeb(2002)은 정보보호 투자의 적정 수준에 대한 연구를 수행하였으며 정보보호에 대한 투자가 일정 수준을 넘어서면 투자 효과는 감소한다는 결과를 도출하였다. 양원석 등(2009)은 대기행렬을 활용하여 정보보호 대책 포트폴리오에 대한 가치를 평가하였다. 보안 위협은 하드웨어 대체, 데이터 복구, 작업 유실에 따른 피해를 발생시킨다고 가정하였으며, 정보보호 대책 포트폴리오 구성에 따른 보안시스템 구축 투자비, 작업 복구 비용, 하드웨어 대체 비용에 대한 변동비와 고정비를 고려하여 정보보호 대책 포트폴리오의 손익을 계산하였다. Cavusoglu *et al.*(2004)은 게임이론을 이용한 보안투자 의사결정을 평가하기 위한 포괄적인 모델을 제시하였으며 게임이론을 활용하여 기업과 해커 간의 전략적 상호작용을 분석하였다. Kumar *et al.*(2008)은 정보보호 대책 포트폴리오를 평가하는 모델을 제시하였다. 정보보호 포트폴리오의 가치는 비즈니스 환경, 위협 환경, 포트폴리오 특성에 따라 달라질 수 있다는 점을 모의실험을 통해 제시하였다. Cavusoglu *et al.*(2005)은 게임이론을 활용하여 해커와 기업 간의 상황을 모델링하고 기능설정(configuration)에 따른 IDS(Intrusion Detection System) 가치의 차이를 분석하였다. Fielder *et al.*(2016)은 게임이론과 조합최적화를 활용하여 중소기업 정보보호 대책 의사결정 모델을 제시하였다. Biermann *et al.*(2001)은 IDS에 대한 다양한 접근 방식을 비교하여 최적 시스템에 대한 표준을 제시하고 다양한 환경에서의

최적 IDS의 선택과 조합 방법을 제시하였다. Nespoli *et al.*(2018)은 현재까지 정보보호 대책 최적화 분야에서 다루었던 다양한 최적화 방법론들을 비교하기 위한 기준을 제시하고 분석하였다. Kong *et al.*(2012)은 BSC 관점에서 정보 보안 투자의 영향에 대한 실증 분석을 수행하였다.

Gupta *et al.*(2006)은 정보보호 대책의 운영비용과 취약점을 최소화하기 위해 유전자 알고리즘을 활용하여 최적의 보안 포트폴리오를 구성하였다. 취약점 20개를 7가지 범주로 분류하였으며 13개의 일반적인 정보보호 대책을 정의하였다. 취약점이 가진 특성과 정보보호 대책을 이진표현으로 나타내었으며 취약점이 가진 특성과 정보보호 대책을 매칭하여 잔여 취약점과 운영비용을 최소화하는 최적 정보보호 대책 포트폴리오를 구성하였다. 김길환 등(2018)은 침해사고의 발생 빈도, 평균 피해액, 정보보호 대책 평균 투자비용, 방어비율의 점추정치를 산정할 수 있다고 가정하여 침해사고와 정보보호 대책을 설정하였다. 정보보호 대책의 도입여부에 따라 침해사고에 의한 피해액을 산정하여 정보보호 대책 운영비용과 침해사고에 의한 피해액을 최소화하는 정보보호 대책 포트폴리오를 유전자 알고리즘을 활용하여 구성하였다.

기존의 정보보호 대책 포트폴리오 최적화 연구에서는 임의로 생성된 침해사고를 대상으로 최적 정보보호 대책 도입여부를 구성하였다. 실제 정보시스템 이용 현황에 적용가능한 최적의 정보보호 대책 포트폴리오를 구성하는데 한계가 있다. 본 연구에서는 산업군별 침해사고 데이터 통계를 이용하여 다양한 산업군에서의 정보보호 대책에 대한 구성을 최적화하고 각 대책에 대한 적정 투자 수준에 대한 의사결정 지원 모델을 제시한다.

Ⅲ. 연구 모형

3.1 연구 데이터

침해사고 데이터 통계에 기반한 정보보호 투자 포트폴리오 최적화 연구를 진행하기 위해서 먼저 침해사고와 정보보호 대책에 대한 데이터를 수집하였다.

침해사고 공격기법들은 Verizon 2019 보고서와 안랩 보안용어사전(안랩, 2019), OWASP 웹 응용 프로그램 공격 Top 10(OWASP, 2019)을 참고하였다(<표 1> 참고).

〈표 1〉 침해사고 공격기법

기법 구분	세부 기법 구분
사이버 스파이	피싱
	백도어
	멀웨어
웹 응용 프로그램 공격	SQL 인젝션
	취약한 인증
	민감한 데이터 노출
	XML 외부 개체
	취약한 접근 통제
	잘못된 보안 구성
	크로스 사이트 스크립트
	안전하지 않은 역직렬화
	알려진 취약점이 있는 구성요소 사용
	불충분한 로깅과 모니터링
오류	민감한 데이터 전달 오류
	데이터 게시 오류
	잘못된 서버 구성
권한 남용	승인되지 않은 접근
	악의적 사용

침해사고 데이터는 41,686 건의 보안 사고를 분석하여 산업군별 보안사고와 데이터 유출 유형 통계를 제공하는 2019 Data Breach Investigations Report를 참고하였다(Verizon, 2019). 해당 보고서에는 IT, 공공, 헬스케어, 제조 등 9개의 산업군으로 구분하여 통계를 제공하고 있다. 본 연구에서는 그 중에서 공공, IT서비스 2가지 산업군을 선정하여 적용한다.

정보보호 대책에 대한 정의는 안랩 보안용어사전(안랩, 2019), 펜타시큐리티 홈페이지(펜타시큐

리티, 2019), 정보보호개론 서적(양대일, 2016)을 참고하였으며 정의를 바탕으로 정보보호 대책별 방어 가능한 침해사고를 도출하였다(<표 2> 참고).

IT 서비스 산업군 침해사고 유형 통계에서는 오류, 웹 어플리케이션 공격, 사이버 스파이가 높은 비율을 차지하는 것으로 나타났으며 공공 산업군 침해사고 유형 통계에서는 사이버 스파이, 오류, 권한남용, 웹 어플리케이션 공격 순으로 비율이 높게 나타났다(<표 3> 참고).

〈표 2〉 정보보호 대책별 방어 가능한 침해사고

대책 구분	방어 가능한 침해사고
방화벽	취약한 접근통제, 승인되지 않은 접근
웹방화벽	SQL 인젝션, 취약한 인증, 민감한 데이터 노출, 취약한 접근 통제, XML 외부 개체, 크로스 사이트 스크립트, 불충분한 로깅과 모니터링, 승인되지 않은 접근
안티 바이러스	멀웨어
IDS	취약한 접근통제, 승인되지 않은 접근
IPS	취약한 접근통제, 불충분한 로깅과 모니터링, 승인되지 않은 접근
정보보호 교육	민감한 데이터 전달 오류, 데이터 게시 오류, 피싱, 악의적 사용
보안 관제 서비스	불충분한 로깅과 모니터링, 취약한 접근통제, 승인되지 않은 접근
보안 컨설팅 서비스	백도어, SQL 인젝션, 취약한 인증, 민감한 데이터 노출, XML 외부 개체, 취약한 접근통제, 잘못된 보안 구성, 크로스 사이트 스크립트, 안전하지 않은 역직렬화, 알려진 취약점이 있는 구성요소, 잘못된 서버 구성

〈표 3〉 산업군별 침해사고 유형

산업 구분	공격 기법	빈도(%)
IT 서비스	오류	42
	웹 어플리케이션 공격	29
	사이버 스파이	13
공공	사이버 스파이	42
	오류	18
	권한남용	12
	웹 어플리케이션 공격	10

3.2 정보보호 투자 포트폴리오 최적화 모형

정보보호 투자 포트폴리오 최적화 모형은 임정현, 김태성(2019)의 모형을 활용하였다.

*n*개의 보안 침해사고 유형과 기업이 보유하고 있는 *m*개의 정보보호 대책이 존재한다고 할 때, 본 연구에서는 *n*개의 보안 침해사고 유형을 산업군별 통계를 활용해 생성하고, 정보보호 대책의 속성을 객관화 할 수 있다고 가정하였다. 각 변수에 대한 설명은 다음과 같다.

v_{id}: 보안 침해사고 i의 평균 피해액
v_{il}: 침해사고 i의 수준
v_{ip}: 침해사고 i의 공격 목표
c_{il}: 정보보호 대책 i의 수준
c_{iL}: 강화된 정보보호 대책 i의 수준
c_{ip}: 정보보호 대책 i의 방어 가능한 공격 기법
c_{iu}: 정보보호 대책 i의 강화 비용
d_i: 침해사고 i로 인한 피해액
d: 총 피해액
i: 투자금액
λ: 평균 피해액 조절 계수(0.2)

정보보호 대책의 강화비용은 현재 보유하고 있는 대책을 구입하는데 현재까지 투입된 총 누적비용을 수준으로 나눈 값으로 정의한다. 이때 침해사고 i = 1, …, n이고, 정보보호 대책 j = 1, …, m이다. 침해사고 수준 v_{il}은 취약점의 주요 특징을 파악하고 심각도를 반영하는 수치를 산출하는 CVSS(Common Vulnerability Scoring System)를 참고하여 정의하였다(Houmb and Franqueira, 2009). CVSS 점수는 0.1부터 10까지 정의되어 있으나 본 연구에서는 계산의 편의를 위해 1부터 10까지의 정수(10단계)로 정의하였다. 정보보호 대책의 수준은 0(도입예정)부터 10까지의 정수로 대책의 수준을 객관화할 수 있다고 가정하고 설정하였다. 기존 연구들에서는 침해사고와 정보보호 대책의 관계를 -1, -0.5, 0, 0.5, 1의 5단계 점수로 정의하였

지만(Gupta *et al.*, 2006; Viduto *et al.*, 2012) 본 연구에서는 침해사고 수준(10) 단계와 정보보호 대책 수준(11) 단계의 차이를 이용하여 관계를 정의하였다. 침해사고의 수준 v_{il}과 정보보호 대책 c_{il}의 수준은 다음과 같다.

$$v_{il}=\begin{cases}1 \text{ 수준}\\ \vdots\\ 10 \text{ 수준}\end{cases} \qquad c_{il}=\begin{cases}0 \text{ 도입예정}\\ \vdots\\ 10 \text{ 도입 수준}\end{cases}$$

기업이 보유한 정보보호 대책이 결정되면 침해사고 *i*에 의한 피해액 d_i와 전체 침해사고에 대한 총 피해액 d는 다음과 같이 정의할 수 있다.

$$d_i=\begin{cases}(v_{il}-c_{jl})v_{id}\lambda\,, \text{if } v_{il}>c_{jl}\\ 0 \qquad\quad, \text{if } v_{il}\leq c_{jl}\end{cases}$$

$$d=\sum_{i=0}^{n}(v_{il}-c_{jl})v_{di}\lambda$$

여기서 *j*는 침해사고 *i*의 공격목표와 매칭되는 대책을 말한다. 또한, 평균 피해액 조절 계수 λ(0.2)는 침해사고 v_i 발생 시 최대 피해액과 최소 피해액의 중간값이 침해사고 *i*의 평균 피해액 v_{id}과 같아지도록 하는 계수이다. v_i 발생 시 최대 피해액은 침해사고 수준 v_{il}이 10이고 정보보호 대책 c_{jl}이 0인 경우이며, 최소 피해액은 0인 경우이다.

정보보호 투자를 통해 대책이 강화된 이후의 피해액 d_i와 주어진 투자금액과 강화비용에 관한 제약식은 다음과 같이 정의하였다.

$$d_i=\begin{cases}(v_{il}-c_{jl})v_{id}\,, \text{ if } v_{il}>c_{jL}\\ 0 \qquad\quad, \text{ if } v_{il}\leqq c_{jL}\end{cases}$$

$$\text{제약식: } \sum_{i=0}^{m}(c_{iL}-c_{il})c_{iu}<i$$

본 연구에서 정보보호 투자 최적화 문제는 주어진 투자금액 내에서 기업이 보유하고 있는 정보보호 대책들을 강화하고 침해사고로 인해 발생할 수 있는 총 피해액을 최소화하는 것이 목표이다.

3.3 최적해 탐색 방법

본 연구에서 유전자 알고리즘을 최적해 탐색 방법으로 선정한 이유는 대책의 수준이 0부터 10까지로, 최적해 탐색 범위가 최대 11^m개이며 대책의 범위 또한 소프트웨어, 하드웨어, 교육 및 훈련, 서비스로 모든 대책을 포함하기 때문에 모든 범위를 탐색하기에 어려움이 있다. 이러한 한계를 해결하기 위해 메타 휴리스틱 방법 중 유전자 알고리즘을 선택하였다.

유전자 알고리즘을 활용하기 위해서는 해를 유전자로 표현하는 방식, 해의 적합도를 평가하는 적합도 함수, 초기 인구 생성, 선택, 교차 방법, 변이에 대한 설계가 필요하다.

정보보호 대책은 도입예정인 대책을 포함하여 수준을 0부터 10까지 정의하였다. 따라서 해를 표현하는 유전자는 각 자리가 0부터 10 사이의 값인 길이가 m인 정수표현(integer representation)이다. 대책 조합의 수준을 해로 표현한 예시는 <표 4>와 같다.

〈표 4〉 대책 조합을 표현하는 예시

	안티바이러스	방화벽	웹 방화벽	정보보호 교육	관제서비스
수준	4	5	2	6	8

초기해 생성은 기업의 객관화된 대책 수준을 기준으로 제한된 투자금액 안에서의 무작위 투자가 이루어진 경우의 수를 모집단 개수만큼 생성하는 방식을 사용한다. 초기해는 다음 세대 생성을 위한 해집단으로 초기해 생성 이후 유전자 연산에 따라 다음 세대의 해집단을 생성한다.

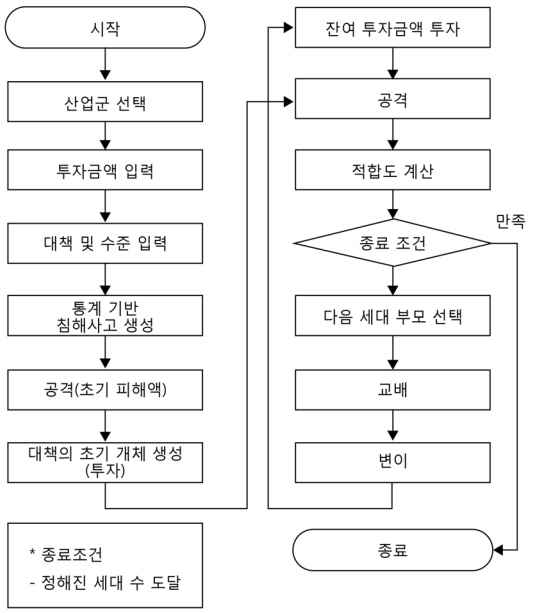
선택은 엘리트 유전자(적합도가 높은 유전자)를 선별하는 과정으로서 이전세대에서 개체를 선택하여 다음 세대를 구성한다. 본 연구에서는 순위 선택(rank selection) 방법을 사용하여 적합도가 높은 유전자를 선택한다. 적합도는 피해액이 가장 적은 유전자를 구별하기 위해 설정하였다.

교배는 이전 세대에서 선택된 엘리트 유전자들이 부모가 되고 부모의 유전자를 사용하여 하나 이상의 자손을 생성하는 연산으로, 본 연구에서는 한 지점 교차(one point crossover) 방식을 사용하였다. 한 지점 교차 방식은 한 개의 교차 포인트가 선택되면 교차 포인트를 기준으로 교배를 진행하는 방식이다.

돌연변이는 유전자 세대 반복을 통해 얻어지는 해가 해공간의 제한성을 극복하고 새로운 탐색 해들을 얻는 연산이다. 돌연변이 연산 방식 중 스왑 변이(swap mutation)와 무작위 리셋(random resetting)을 사용하며, 스왑 변이 방법은 무작위로 염색체의 두 위치를 선택하고 값을 교환하는 방식이고 무작위 리셋 방법은 허용된 집합의 값을 무작위로 선택된 유전자에 할당하는 방식이다.

본 연구에서는 제한된 투자금액 내에서 최적해를 도출하기 때문에 초기 랜덤하게 생성한 정보보호 대책 조합에서 가장 피해액이 적은 대책(엘리트 유전자)을 선택한다. 엘리트 유전자를 교배 연산하여 생성한 다음 정보보호 대책 조합 세대 중 투자금액을 넘어선 유전자를 제외하였다. 투자금액을 초과한 유전자는 다음 세대 유전자로 적합하지 않기 때문에 본 연구에서는 교배 후 생성된 유전자 중 적합한 유전자를 선별하고 모집단 개수에서 모자란 개수만큼 무작위 리셋 변이 방식을 활용하여 돌연변이를 생성한다. 또한, 스왑 변이 확률을 정의하여 확률만큼 변이를 추가 생성한다. 돌연변이 생성 또한 제한된 투자금액을 초과하지 않는 유전자를 선별한다.

본 연구의 유전자 알고리즘 흐름도는 <그림 1>과 같다. 유전자 알고리즘을 통한 해 탐색은 정해진 세대 수에 도달하게 되면 종료한다.



〈그림 1〉 정보보호 대책 포트폴리오 최적화 알고리즘 흐름도

Ⅳ. 수치 예제

4.1 기존 유전자 알고리즘과의 비교

김길환 등(2018)에서는 정보보호 대책의 도입여부에 따라 침해사고에 의한 피해액을 산정하여 정보보호 대책 운영비용과 침해사고에 의한 피해액을 최소화하는 정보보호 대책 포트폴리오를 유전자 알고리즘을 활용하여 구성하였다. 알고리즘 비교에서는 대책의 도입여부를 고려한 알고리즘과 도입 수준을 고려한 알고리즘 사이의 피해액을 비교한다.

김길환 등(2018)에서는 n개의 보안 침해사고 유형과 m개의 정보보호 대책이 존재하고, 침해사고 평균 피해액, 침해사고 발생률, 정보보호 대책 운영비용, 정보보호 대책 방어비율의 점추정치를 산정할 수 있다고 가정하였다.

d_i: 침해사고 i로 인한 피해액
p_i: 한 기간 동안 보안 침해사고 i 발생률
c_j: 한 기간 동안 정보보호 대책 j 운영비용
q_{ij}: 정보보호 대책 j의 침해사고 i 방어비율
r_i: 침해사고가 피해로 이어지는 비율
$y_i(x)$: 침해사고에 의한 피해액 기대치

정보보호 대책 j의 도입여부 x_j, 침해사고가 피해로 이어지는 비율 r_i, 침해사고에 의해 발생하는 피해액 기대치는 다음과 같다.

$$x_j = \begin{cases} 1, \text{정보보호 대책 } j \text{ 도입} \\ 0, \text{정보보호 대책 } j \text{ 미도입} \end{cases}$$

$$r_i = \prod_{j=1}^{m} (1-q_{ij})^{x_j}$$

$$y_i(x) = d_i p_i r_i = d_i p_i \prod_{j=1}^{m} (1-q_{ij})^{x_j}$$

본 연구와 동일한 환경에서의 결과를 위해 침해사고에 의해 발생하는 피해액의 기대치를 수정하여 두 알고리즘에서의 피해액이 동일하도록 설정하였다. 평균 피해액 조절 계수 μ, 침해사고 발생률과 침해사고가 피해로 이어지는 확률 $p_i r_i$, 침해사고에 의해 발생하는 피해액 기대치 $y_i(x)$는 다음과 같이 수정하였다. μ는 평균피해액 조절 계수로 침해사고 발생 시 최대 피해액과 최소 피해액의 중간값이 침해사고의 평균 피해액과 같아지도록 하는 값이다.

μ : 평균 피해액 조절 계수(2)

$$p_i r_i = (v_{il} - c_{il}) \times 0.1, \text{ if } v_{il} > c_{il}$$

$$y_i(x) = \begin{cases} x=0, d_i(v_{il}-c_{il}) \times 0.1\mu, & \text{if } v_{il} > c_{il} \\ x=1, \quad 0, & \text{if } v_{il} < c_{il} \end{cases}$$

성능 비교에서 침해사고는 특정 산업군 통계를 활용하지 않고 공격대상, 수준, 평균피해액을 무작위로 1,000개 생성하였으며, 정보보호 대책은 대책의 수, 방어대상, 강화비용을 임의의 값으로 설정하였다. 기존 알고리즘에서의 강화비용은 도입여부만을 고려하기 때문에, 기존 알고리즘의 도입비용과 본 연구의 강화비용에 차이가 발생한다. 따라서 기존 알고리즘에서 정보보호 대책 도입 시 발생하는 도입비용은 본 연구 알고리즘에서 수준을 0에서 10까지 강화하는 비용으로 설정하였고 두 알고리즘을 비교하기 위해 정보보호 대책은 모두 미도입 상태(수준 0)로 가정하였다. 성능 비교를 위해 설정된 침해사고 및 정보보호 대책 속성값들은 <표 5>, <표 6>, <표 7>과 같다.

투자금액은 과학기술정보통신부와 한국인터넷진흥원에서 중소기업 정보보호 컨설팅 및 솔루션 구입비용으로 기업에게 제공하는 지원 금액인 1,000만 원을 최소금액으로(한국인터넷진흥원, 2019), 최대 5,000만 원까지 차등을 두었다.

〈표 5〉 시나리오 1: 대책 6개, 투자금액 1,000만 원

초기 피해액 : 32,112,168				투자금액 : 10,000,000		
구분	대책1	대책2	대책3	대책4	대책5	대책6
수준	0	0	0	0	0	0
방어대상	1	2	3	4	5	6
강화비용	50만 원	30만 원	10만 원	20만 원	10만 원	40만 원

〈표 6〉 시나리오 2: 대책 8개, 투자금액 3,000만 원

초기 피해액 : 42,613,576					투자금액 : 30,000,000			
구분	대책1	대책2	대책3	대책4	대책5	대책6	대책7	대책8
수준	0	0	0	0	0	0	0	0
방어대상	1	2	3	4	5	6	7	8
강화비용	10만 원	20만 원	40만 원	100만 원	200만 원	5만 원	30만 원	50만 원

〈표 7〉 시나리오 3: 대책 6개, 투자금액 5,000만 원

초기 피해액 : 31,403,910				투자금액 : 50,000,000		
구분	대책1	대책2	대책3	대책4	대책5	대책6
수준	0	0	0	0	0	0
방어대상	1	2	3	4	5	6
강화비용	50만 원	100만 원	200만 원	400만 원	200만 원	200만 원

〈표 8〉 시나리오 1 결과

구분		대책1	대책2	대책3	대책4	대책5	대책6	잔여금액
1	수준	4	9	10	10	10	3	100,000
2	수준	0	1	1	0	1	1	1,000,000

〈표 9〉 시나리오 2 결과

구분		대책1	대책2	대책3	대책4	대책5	대책6	대책7	대책8	잔여금액
1	수준	9	9	8	6	5	10	10	9	100,000
2	수준	1	1	1	1	0	1	1	1	4,500,000

〈표 10〉 시나리오 3 결과

구분		대책1	대책2	대책3	대책4	대책5	대책6	잔여금액
1	수준	8	10	3	0	7	8	0
2	수준	1	0	0	0	1	1	5,000,000

성능 비교 실험들의 결과는 <표 8>, <표 9>, <표 10>과 같다. 구분 1은 본 연구에서 제안하는 알고리즘, 구분 2는 김길환 등(2018)에서 사용한 알고리즘을 뜻한다.

성능비교 실험들을 종합적으로 분석한 결과는 <표 11>과 같다. 투자 효율은 투자대비효과(ROI, Return on Investment)를 활용하였다. ROI는 투자 전략을 비교하는데 자주 사용되며 기업의 투자 의사결정을 지원한다(Sonnenreich, 2006). Benefit은 정보보호 대책 투자로 인한 피해액 감소이고, Cost는 정보보호 대책 투자비용이다.

$$ROI(\%) = \frac{Benefit - Cost}{Cost} \times 100$$

총 3회의 성능비교 결과, 본 연구에서 제시된 알고리즘이 3회 모두 더 많은 피해액 감소를 보였고, 3회 중 2회의 ROI가 더 높게 측정되었다.

〈표 11〉 성능비교 종합 분석

구분		대책 투자비용(원)	피해액 감소(원)	ROI (%)
시나리오1	1	9,900,000	27,513,372	178
	2	9,000,000	22,642,378	152
시나리오2	1	29.900.000	39,618,746	33
	2	25,500,000	37,902,881	49
시나리오3	1	50,000,000	22,673,498	-55
	2	45,000,000	16,622,902	-63

4.2 투자 예산 의사결정

본 연구의 모형은 정보보호 투자의 최적 규모에 대한 의사결정에 활용될 수 있다. 정보보호 투자 규모 의사결정에 대한 실험 환경은 <표 12>와 같고, 여러 회 실험을 반복하여 다양한 ROI 수치를 도출하였다(<표 13> 참고).

정보보호 투자 규모 의사결정에 대하여 실험한 결과, 투자금액이 850만 원과 900만 원일 때 가장 높은 ROI 수치를 보였다. 투자비용 대비 피해액 감소를 고려하였을 때, 최적의 투자 규모에 대한 의사결정을 지원할 수 있다.

4.3 IT 중소기업 A 사례

IT 중소기업 A의 정보보호 투자 현황을 설문을 통해 수집하여 본 연구의 모델을 적용하였다. 해당 중소기업의 정보보호 투자 현황은 총 7개의 기존 정보보호 대책과 1개의 도입예정인 대책으로 구성되어 있었다, 금년 정보보호 예산은 2,000만 원이다.

가격(Price)은 정보보호 대책을 구입하는데 현재까지 투입된 총 누적비용을 뜻하며 수준(Level)은 완벽한 보안 수준 대비 보유하고 있는 대책의 상대적인 수준을 뜻한다. 본 연구에서의 강화비용은 각 정보보호 대책을 구입하는데 현재까지 투입된 총 누적비용을 수준으로 나눈 값으로 가정한다. <표 14>를 활용하여 본 연구 모델에 적용 가능한 속성값들을 구성하였다. <표 15>의 강화비용의 단위는 백만 원이다.

침해사고는 Verizon 보고서의 통계에 기반하여 IT 산업군 침해사고 유형 1,000개를 생성하였으며,

〈표 12〉 정보보호 투자예산 의사결정: 실험 환경

투자금액 : 미정						
구분	대책1	대책2	대책3	대책4	대책5	대책6
수준	0	0	0	0	0	0
방어대상	1	2	3	4	5	6
강화비용	50만 원	30만 원	10만 원	30만 원	20만 원	40만 원

〈표 13〉 정보보호 투자예산 의사결정: 실험 결과

투자예산	대책 투자비용	피해액 감소	ROI(%)
800만 원	7,900,000	22,583,722	186
850만 원	**8,500,000**	**24,633,447**	**190**
900만 원	**8,900,000**	**25,805,843**	**190**
1,000만 원	10,000,000	27,416,273	174
1,300만 원	12,900,000	28,270,193	119
1,500만 원	14,800,000	31,743,430	114

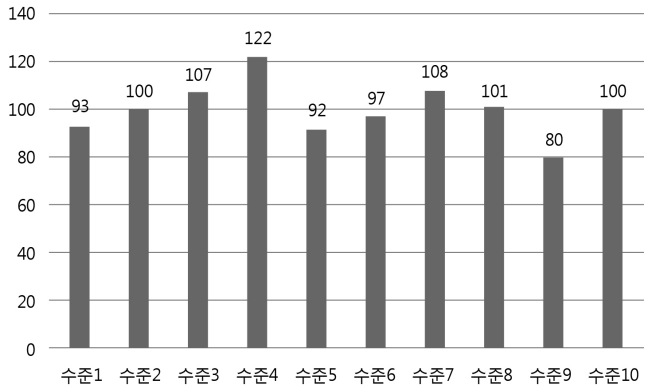
〈표 14〉 IT 중소기업 A 사례: 정보보호 투자 현황

P/L: Price/Level(Price 단위: 백만 원)

대책1 (P/L)	대책2 (P/L)	대책3 (P/L)	대책4 (P/L)	대책5 (P/L)	대책6 (P/L)	대책7 (P/L)	대책8 (P/L)
안티 바이러스 (3/7)	보안 컨설팅 (15/7)	방화벽 (10/8)	IPS (15/8)	웹 방화벽 (15/8)	정보보호교육 (10/5)	보안 관제 서비스 (50/8)	정보 보호 교육2 (0/0)

〈표 15〉 IT 중소기업 A 사례 속성표

	대책1	대책2	대책3	대책4	대책5	대책6	대책7	대책8
대책 유형	안티 바이러스	보안 컨설팅	방화벽	IPS	웹 방화벽	정보보호 교육	보안관제 서비스	정보보호 교육
수준	7	7	8	8	8	5	8	0
강화비용	0.4	2.1	1.3	1.9	1.9	2	6.3	2



〈그림 2〉 IT 중소기업 A 사례: 침해사고 수준 분포

앞서 정의한 정보보호 대책별 방어 가능한 침해사고를 활용하여 본 연구의 모형을 적용하였다. 생성된 1,000개의 수준은 <그림 2>, 공격유형은 <표 16>으로 나타내었다. 생성된 침해사고 1,000개의 피해액의 평균은 한국 기업 데이터 유출사고 평균 피해액 31억 원으로 설정하였다(Ponemon Institute, 2018).

본 연구에서는 높은 대책의 수준은 낮은 수준의 침해사고를 완벽히 방어한다고 가정한다. 각 침해사고의 공격기법과 정보보호 대책의 방어 가능한 공격기법을 매칭하여 침해사고의 수준이 정보보호 대책의 수준보다 높을 경우 수준 차에 따라 초기피해액을 산정한다. 초기 피해액 산정 이후 유전자 알고리즘을 활용하여 기업의 정보보호 예산 범위에서 각 대책의 수준을 강화시키며 피해액이 가장 적은 대책 조합을 구성한다.

입력된 정보보호 대책과 침해사고에 대한 초기 총 피해액은 1,795,394,310원이다. 피해액을 줄이기 위해 유전자 알고리즘을 활용하여 정보보호 대책의 수준을 정보보호 투자 예산을 활용하여 강화하였다. 유전자 알고리즘을 활용하기 위해 해를 표현하는 자료구조는 0부터 10까지, 길이가 대책의 개수인 정수표현을 활용하였으며, 정보보호 대책 조합의 경우의 수인 초기 인구 집단 개수는 40개로 설정하였다.

각 세대별 인구 집단에서 엘리트 유전자를 선택하는 개수는 6개로 설정하였고, 교배는 한 지점 교차 방법, 변이는 두 가지 연산(랜덤 리셋, 스왑 변이)을 조합하였다. 본 연구의 모델에서는 기업의 정보보호 투자 예산 안에서의 투자라는 제약조건이 존재하기 때문에 교배 연산 시, 정보보호 투자 예산을 초과하는 대책의 조합들은 제거하였고, 초기 인구 집단 개수인 40개만큼 부족한 인구를 무작위 리셋 방법으로 돌연변이를 발생시켰다. 스왑 변이 방식은 20%의 확률로 두 개의 유전자를 교환하는 방법을 사용하였다. 변이 또한 기업의 정보보호 예산을 초과하지 않는 범위에서 돌연변이를 발생시켰다.

〈표 16〉 IT 중소기업 A 사례: 침해사고 공격기법 분포

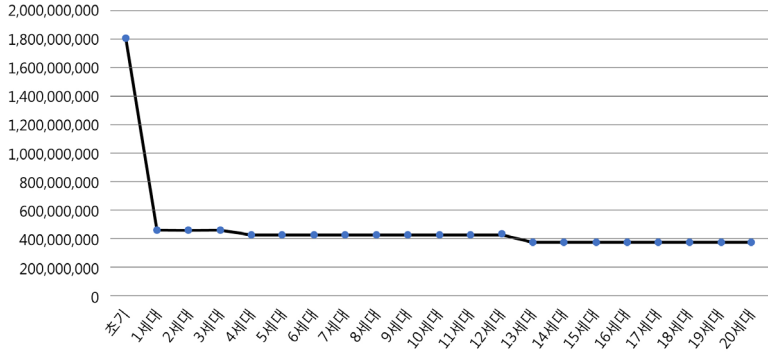
구분	공격기법	개수(개)
오류	민감한 데이터 전달 오류	170
	데이터 게시 오류	171
	잘못된 서버 구성	170
웹 어플리케이션 공격	SQL 인젝션	34
	취약한 인증	34
	민감한 데이터 노출	34
	XML 외부 개체	34
	취약한 접근통제	34
	잘못된 보안 구성	34
	크로스 사이트 스크립트	33
	안전하지 않은 역직렬화	33
	알려진 취약점 구성요소	33
	불충분한 로깅, 모니터링	33
사이버 스파이	피싱	51
	멀웨어	51
	백도어	51
합계	1,000	

최적해 탐색 과정에서 각 세대별 최소 피해액의 변화를 <그림 3>으로 나타내었다. 기업의 정보보호 예산 내에서의 투자와 초기 정보보호 대책의 수준 이하의 해 탐색은 제외하였기 때문에 최적해는 모두 20세대 이내에서 탐색되었다. IT 중소기업 정보보호 현황에 대한 최적해는 <표 17>과 같다. A 기업 정보보호 예산 2,000만 원을 모두 투자하였고, 최적 정보보호 대책 조합은 초기 총 피해액을 투자 이전의 1,810,466,740원에서 투자 이후에 380,208,890원으로 1,430,257,850원 만큼 감소시켰다.

4.4 공공기관 B 사례

공공기관 B의 정보보호 투자 현황을 설문을 통해 수집하여 본 연구의 모델을 적용하였다. 해당 공공기관의 정보보호 투자 현황은 소프트웨어 제품군, 하드웨어 제품군, 보안 관제 서비스, 정보보호 컨설팅으로 구성되어 있었다. 2019년 정보보호 예산은 39,200만 원이다(<표 18> 참고).

공공기관 B의 정보보호 투자 현황을 본 연구 모델에 적용하기 위해 소프트웨어 제품군과 하드웨어 제품군에 대한 대책을 임의로 설정하였다.



〈그림 3〉 IT 중소기업 A 사례: 각 세대별 최소 피해액 변화

〈표 17〉 IT 중소기업 A 사례: 최적 정보보호 대책 구성

		안티 바이러스	보안 컨설팅	방화벽	IPS	웹 방화벽	정보보호 교육	보안관제 서비스	정보보호 교육	피해액(원)
기존	수준	7	7	8	8	8	5	8	0	1,810,466,740
최적해	수준	7	7	8	8	8	7	8	8	380,208,890

각 제품군의 투자비용과 수준의 평균을 고려하여 소프트웨어 제품군은 안티 바이러스로 구성하였으며, 하드웨어 제품군은 방화벽, 웹방화벽, IPS로 구성하였다. 투자 금액은 2019년 정보보호 예산 중 절반인 19,600만 원을 사용하였다(<표 19> 참고).

〈표 18〉 공공기관 B 사례: 정보보호 투자 현황

P/L : Price/Level(Price 단위: 백만 원)

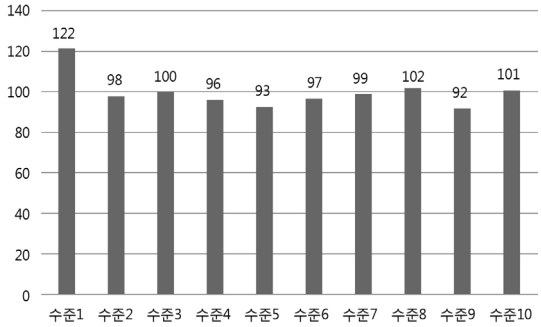
대책1 (P/L)	대책2 (P/L)	대책3 (P/L)	대책4 (P/L)
소프트웨어 (40/5)	하드웨어 (300/5)	보안 관제 서비스 (12/5)	정보보호 컨설팅 (40/5)

침해사고는 Verizon 보고서의 통계에 기반하여 공공 산업군 침해사고 유형 1,000개를 생성하였으며, 앞서 정의한 정보보호 대책별 방어 가능한 침해사고를 활용하여 본 연구의 모형을 적용하였다. 생성된 1,000개의 수준은 <그림 4>, 공격유형은 <표 20>으로 나타내었다. IT 산업군 수치예제와 동일하게 생성된 침해사고 1,000개의 피해액의 평균은 한국 기업 데이터 유출사고 평균 피해액 31억 원으로 설정하였다(Ponemon Institute, 2018).

〈표 19〉 공공기관 B 사례 속성표

	대책1	대책2	대책3	대책4	대책5	대책6
대책 유형	방화벽	웹 방화벽	안티 바이 러스	IPS	보안 관제 서비스	정보 보호 컨설팅
수준	4	5	5	6	5	5
강화 비용	15	24	8	20	2.4	8

IT 산업군의 사례와 동일하게 각 침해사고의 공격기법과 정보보호 대책의 방어 가능한 공격기법을 매칭하여 침해사고의 수준이 정보보호 대책의 수준보다 높을 경우 수준 차에 따라 초기 피해액을 산정한다. 초기 피해액 산정 이후 유전자 알고리즘을 활용하여 기업의 정보보호 예산 안에서 각 대책의 수준을 강화시키며 피해액이 가장 적은 대책 조합을 구성한다.



〈그림 4〉 공공기관 B 사례: 침해사고 수준 분포

입력된 정보보호 대책과 침해사고에 대한 초기 총 피해액은 529,440,690원이다. 피해액을 줄이기 위해 유전자 알고리즘을 활용하여 정보보호 대책의 수준을 투자 예산을 활용하여 강화하였다.

〈표 20〉 공공기관 B 사례: 침해사고 공격기법 분포

구분	공격기법	개수(개)
사이버 스파이	피싱	166
	멀웨어	167
	백도어	167
오류	민감한 데이터 전달 오류	73
	데이터 게시 오류	73
	잘못된 서버 구성	74
권한 남용	승인되지 않은 접근	75
	악의적 사용	75
웹 어플리 케이션 공격	SQL 인젝션	13
	취약한 인증	13
	민감한 데이터 노출	13
	XML 외부 개체	13
	취약한 접근통제	13
	잘못된 보안 구성	13
	크로스 사이트 스크립트	13
	안전하지 않은 역직렬화	13
	알려진 취약점 구성요소	13
	불충분한 로깅, 모니터링	13
합계	1,000	

〈표 21〉 공공기관 B 사례: 최적 정보보호 대책 구성

		방화벽	웹방화벽	안티 바이러스	IPS	보안관제 서비스	정보보호 컨설팅	피해액 (원)
기존	수준	4	5	5	6	5	5	529,440,690
최적해	수준	4	8	10	7	10	10	39,645,450

공공기관 정보보호 현황에 대한 최적해는 <표 21>로 나타내었다. 최적 정보보호 대책 조합은 초기 총 피해액 529,440,690원에서 39,645,450원으로 489,795,240원 만큼 피해를 감소시켰으며 정보보호 투자 예산 19,600만 원 중 1,200만 원을 제외한 18,400만 원을 사용하였다.

Ⅴ. 결 론

본 연구에서 정보보호 최적화 시스템을 개발하기 위해 조합유전자 알고리즘을 선택하고 JAVA 프로그래밍 언어로 구현하였다. 기존 정보보호 대책 포트폴리오 최적화 연구는 대책 도입여부만을 고려하였고(Gupta *et al.*, 2006; 김길환 등, 2019), 가상의 침해사고 데이터를 사용한 한계점이 있었다. 본 연구에서는 이러한 한계점을 극복하기 위해 정보보호 대책 도입여부 뿐만 아니라 도입 수준을 고려하였고, 실제 침해사고 데이터 통계를 활용하여 최적 정보보호 대책 포트폴리오를 구성하였다. 본 연구에서 제시된 알고리즘을 활용하면 정보보호 초기 투자뿐만 아니라 기존에 보유하고 있는 정보보호 대책에 대해서도 수준을 강화할 수 있는 투자 방법을 도출할 수 있다.

김길환 등(2018)의 정보보호 투자 최적화 연구에 사용된 유전자 알고리즘과 본 연구 알고리즘을 비교해본 결과 정보보호 대책 투자로 인해 전체적인 피해액 감소는 본 연구 알고리즘을 적용한 경우에 크게 나타났고, 3회중 2회의 ROI 수치도 높았다. 정보보호 대책 비용은 정보보호 제품 구입비용과 정보보호 서비스 이용비용으로 나눌 수 있다. 정보보호 제품의 경우 초기 구입비용 이후의 비용은 추가로 발생하지 않으며 정보보호 서비스 비용은 초기 서비스 도입비용 이후의 비용이 발생한다는 특징이 있다. 본 연구의 결과는 초기 투자 또는 추가 투자, 제품 구입 또는 서비스 이용 등 다양한 관점에서의 정보보호 투자 의사결정에 활용할 수 있다. 침해사고 발생 통계를 활용하여 산업군별로 실제 적용가능한 최적 투자 포트폴리오를 도출한 것도 본 연구의 주요 성과이다.

다양한 제약조건이 있는 문제를 해결하기 위해 유전자 알고리즘 변이 방법을 조합하여 해결함으로써 보다 복잡한 문제를 본 연구 알고리즘을 활용하여 해결할 수 있을 것이라 기대한다.

본 연구에서는 실제 침해사고 데이터 통계를 활용하여 정보보호 대책 도입여부 뿐만 아니라 각 대책에 대한 투자 수준 의사결정을 지원하였지만 다음과 같은 후속 연구가 가능할 것이다.

첫째, 모든 침해사고와 대책들의 수준을 객관화하여 수치로 나타낼 수 있으며 높은 수준의 대책은 낮은 수준의 침해사고를 완벽히 방어한다고 가정하였다. 향후 연구에서는 일부 기술적인 정보보호 대책들의 성능을 활용하여 구체적으로 침해사고와 대책의 수준을 정의할 필요가 있다.

둘째, 정보보호 대책의 수준 강화 비용에 대해서 정의할 필요가 있다. 본 연구의 모델에서는 대책에 대한 초기 구입비용과 운영비용을 구분하지 않았기 때문에 초기 구입비용과 운영비용을 고려하면 보다 현실적인 정보보호 대책 투자 의사결정을 지원할 것으로 기대한다.

참 고 문 헌

[1] 공희경, 전효정, 김태성, “AHP를 이용한 정보보호투자 의사결정에 대한 연구”, *Journal of*

Information Technology Applications & Management, 제15권, 제1호, 2008, pp. 139-152.

[2] 과학기술정보통신부, *2018 정보보호실태조사*, 2019.

[3] 김길환, 양원석, 김태성, "유전자 알고리즘을 이용한 정보보호 대책 투자 포트폴리오의 최적화", *한국통신학회논문지*, 제43권, 제2호, 2018, pp. 439-451.

[4] 김종기, 김지윤, "정보보호 의사결정에서 정보보호 침해사고 발생가능성의 심리적 거리감과 상대적 낙관성의 역할", *Information Systems Review*, 제20권, 제3호, 2018, pp. 51-71.

[5] 안랩, 보안용어사전, 2019.11.19, Available at https://www.ahnlab.com/kr/site/main.do.

[6] 양대일, *정보보호개론*, 한빛아카데미, 2016.

[7] 양원석, 김태성, 박현민, "확률모형을 이용한 정보보호 투자 포트폴리오 분석", *한국경영과학회지*, 제34권, 제3호, 2009, pp. 155-163.

[8] 임정현, 김태성, "정보보호 대책 수준을 고려한 정보보호 투자 최적화: 유전자 알고리즘 접근법", *한국IT서비스학회지*, 제18권, 제5호, 2019, pp. 155-165.

[9] 펜타시큐리티, 2019.11.19, Available at https://www.pentasecurity.co.kr/.

[10] 한국인터넷진흥원, 중소기업 정보보호컨설팅 지원사업, 2019. 11. 25, Available at http://www.smb.isconsulting.kr.

[11] 한국인터넷진흥원, *2017 정보보호실태조사*, 2018.

[12] Benaroch, M., "Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making", *Information Systems Research*, Vol.29, No.2, 2018, pp. 315-340.

[13] Biermann, E., E. Cloete, and L. M. Venter, "A comparison of intrusion detection systems", *Computers & Security*, Vol.20, No.8, 2001, pp. 676-683.

[14] Bodin, L. D., L. A. Gordon, M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process", *Communications of the ACM*, Vol.48, No.2, 2005, pp. 78-83.

[15] Cavusoglu, H., B. Mishra, and S. Raghunathan, "A model for evaluating IT security investments", *Communications of the ACM*, Vol.47, No.7, 2004, pp. 87-92.

[16] Cavusoglu, H., B. Mishra, and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture", *Information Systems Research*, Vol.16, No.1, 2005, pp. 28-46.

[17] Fielder, A., E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol.86, 2016, pp. 13-23.

[18] Gordon, L. A. and M. P. Loeb, "The economics of information security investment", *ACM Transactions on Information and System Security*, Vol.5, No.4, 2002, pp. 438-457.

[19] Gupta, M., J. Rees, A. Chaturvedi, and J. Chi, "Matching information security vulnerabilities to organizational security profiles: A genetic algorithm approach", *Decision Support Systems*, Vol.41, No.3, 2006, pp. 592-603.

[20] Houmb, S. H. and V. N. Franqueira, "Estimating ToE risk level using CVSS", *2009 International Conference on Availability, Reliability and Security, IEEE*, 2009, pp. 718-725.

[21] Kong, H. K., T. S. Kim, and J. Kim, "An analysis on effects of information security investments: A BSC perspective", *Journal of Intelligent Manufacturing*, Vol.23, No.4, 2012, pp. 941-953.

[22] Kumar, R. L., S. Park, and C. Subramaniam, "Understanding the value of countermeasure portfolios in information systems security", *Journal of Management Information Systems*, Vol.25,

No.2, 2008, pp. 241-280.

[23] Nespoli, P., D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, “Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks”, *IEEE Communications Surveys Tutorials*, Vol.20, No.2, 2017, pp. 1361-1396.

[24] OWASP Top Ten Project, 2019.11.15, Available at https://www.owasp.org.

[25] Ponemon Institute, *2018 International Data Breach Statistics*, 2018.

[26] Sonnenreich, W., J. Albanese, and B. Stout, “Return on security investment (ROSI)-a practical quantitative model”, *Journal of Research and Practice in Information Technology*, Vol.38, No.1, 2006, pp. 45.

[27] Verizon, *2019 Data Breach Investigations Report*, 2019.

[28] Viduto, V., C. Maple, W. Huang, and D. LóPez-PeréZ, “A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem”, *Decision Support Systems*, Vol.53, No.3, 2012, pp. 599-610.

Information Systems Review
Volume 22 Number 2
May 2020

Optimization of Information Security Investment Portfolios based on Data Breach Statistics: A Genetic Algorithm Approach

Jung-Hyun Lim* · Tae-Sung Kim**

Abstract

Information security is an essential element not only to ensure the operation of the company and trust with customers but also to mitigate uncertain damage by preventing information data breach. Therefore, It is important to select appropriate information security countermeasures and determine the appropriate level of investment.

This study presents a decision support model for the appropriate investment amount for each countermeasure as well as an optimal portfolio of information countermeasures within a limited budget. We analyze statistics on the types of information security breach by industry and derive an optimal portfolio of information security countermeasures by using genetic algorithms.

The results of this study suggest guidelines for investing in information security countermeasures in various industries and help to support objective information security investment decisions.

Keywords: Information Security Investment, Genetic Algorithm, Optimization of Investment, Statistics of Vulnerabilities

* Master Student, Department of MIS, Chungbuk National University
** Corresponding Author, Professor, Department of MIS, Chungbuk National University

◐ 저 자 소 개 ◑

임 정 현 (lowly13@naver.com)

충북대학교 컴퓨터공학과에서 학사 학위를 취득하고, 충북대학교 경영정보학과 석사를 취득하였다. 주요 관심 분야는 정보통신과 정보보호 분야의 정책 및 투자, 경영과학, 개인정보보호이다.

김 태 성 (kimts@cbnu.ac.kr)

한국과학기술원 산업경영학과에서 박사를 취득하고, 한국전자통신연구원 정보통신기술경영연구소에서 근무한 후, 현재 충북대학교 경영정보학과에서 교수로 재직하고 있으며 보안경제연구소 소장을 맡고 있다. University of North Carolina at Charlotte과 Arizona State University에서 Visiting Professor와 Visiting Scholar로 각각 근무하였다. 국내외 경영과학, 정보통신, 정보보호 관련 학술지 및 학술대회에서 논문을 발표하였으며, 주요 관심 분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.

논문접수일 : 2020년 03월 01일 **게재확정일 : 2020년 03월 17일**
1차 수정일 : 2020년 03월 12일