Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1595

3차원 벡터 시각화를 활용한 효과적인 위험 수준 평가*

이 주 영,† 조 인 현, 이 재 희, 이 경 호‡
고려대학교 정보보호대학원

Effective Risk Level Assessment Using Three-Dimensional Vector Visualization*

Ju-young Lee,† In-hyun Cho, Jae-hee Lee, Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

위험분석은 위험을 허용 가능한 수준으로 관리하기 위한 방안을 수립하는 데 활용된다. 이러한 위험관리 의사결정에 있어서 위험의 시각화는 중요하다. 그러나 기존의 위험 시각화 방식은 위험의 요소들을 고려하여 입체적으로 위험을 시각화하는 데 있어서 한계를 지닌다. 본 논문에서는 기밀성, 무결성, 가용성 측면에서 개별적 혹은 종합적으로 위험을 표현할 수 있는 개선된 위험도 3차원 시각화 방법을 제시한다. 제안된 방법을 기업의 위험분석 평가에 적용하여 유효성을 검증한다. 제안된 시각화 방법은 내부통제를 위한 정보보호 의사결정 과정에 효과적으로 활용될 수 있다.

ABSTRACT

Risk analysis is utilized in devising measures to manage information security risk to an acceptable level. In this risk management decision-making, the visualization of risk is important. However, the pre-existing risk visualization method is limited in visualizing risk factors three-dimensionally. In this paper, we propose an improved risk visualization method which can facilitate the identification of risk from the perspective of confidentiality, integrity, and availability respectively or synthetically. The proposed method is applied to an enterprise's risk analysis in order to verify how effective it is. We argue that through the proposed method risk levels can be expressed three-dimensionally, which can be used effectively for information security decision-making process for internal controls.

Keywords: Risk Analysis, Information Security Decision Making, 3-dimensional Visualization

I. 서 론

기업의 비즈니스 형태가 다양해지고 광범위해지고 있다. 이에 따라 위험관리는 기업을 운영하는데 있어서 더욱 중요한 분야가 되었다. 기업의 위험이 관리되지 않았을 경우 기업뿐만 아니라 비즈니스와 관련된 여러 이해관계자 및 고객들까지도 상당한 피해를 볼 수 있다. 따라서 기업의 위험을 분석하고 합당한 보안 대책을 세우는 것이 매우 중요하다. 또한 다양한 위험을 미리 분석하여 보완 대책을 세우고 효율적, 효과적으로 위험을 관리해야 한다. 위험관리란 위험과 연관하여 조직을 지휘하고 관리하기 위해 조정되는 활동이다. 효과적인 위험관리를 위해서는 체계적이고 구체적인 위험분석을 실시하여야 한다. 위험분석은 자산의 가치와 손실을 측정하여 위험을 평가하는 일련의 과정이다. 이 결과를 가지고 기업은

Received(09. 30. 2015), Modified(10. 22. 2015), Accepted(10. 23. 2015)
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2015년 고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음
† 주저자, juyounglee1027@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

위험을 수용 가능한 수준으로 감소시키기 위하여 적절한 보호대책을 마련하고 우선순위에 따라 실시한다. 이를 통하여 인력과 비용의 과도하거나 과소한 투자를 예방한다.[1] 위험분석을 미흡하게 실시하면 취약점과 위협에 대한 우선순위가 제대로 설정되지 않아 보호대책을 비효율적으로 수행하게 된다. 또한 보호대책은 상황과 시기에 따라 달라지므로 기업의 위험을 수용 가능한 수준으로 유지하기 위하여 지속적인 관리가 필요하다. 본 논문에서는 위험도를 기밀성, 무결성, 가용성 측면에서 각각 산정하고 3차원 벡터 다이어그램을 활용하여 위험을 계량화하여 식별한다. 이렇게 각 측면으로 산정된 위험을 이용하여 보다 정밀하게 보호대책을 수립하고 의사결정을 수행할 수 있도록 한다.

II. 선행연구

2.1 위험분석방법론

정보기술 보안관리를 위한 국제 표준 지침인 ISO/IEC 13335-1에서는 위험분석 전략을 크게 4가지로 분류하고 있다[2]. 베이스라인 접근법(Baseline Approach)은 모든 시스템에 대하여 표준화된 보안대책의 세트를 체크리스트 형태로 제공하고, 이 리스트에 있는 구현대책의 구현유무를 판단한다. 비정형 접근법(Informal Approach)은 구조적인 방법론에 기반을 두기보다는 경험자의 지식을 사용하여 위험분석을 수행한다. 상세위험분석(Detailed Risk Analysis)은 기존의 정립된 모델에 기초하여 자산, 위협, 취약성 분석을 수행하고 위험을 평가한다. 복합 접근법(Combined Approach)은 고위험 영역을 식별하여 이 영역은 상세위험분석을, 그 외의 영역은 베이스라인 접근법을 사용한다.

위험분석을 할 때 사용하는 평가 방법에는 정성적, 정량적인 방법으로 나누어볼 수 있다.[3]. 정성적인 방법(ISO/IEC-13335-3부, BS-7799, CSE, OCTAVE[4][24],CRAMM[5], CONTROL-IT, auditMASTERPLAN)은 정량적인 방법에 비해 평가기간이 짧고 단순하지만 평가 근거의 객관성이 부족하다. 정량적인 평가 방법(RiskCALC, HAWK)은 정보시스템의 규모가 커질수록 위험분석 및 평가에 상당히 많은 시간이 소요되며, 위험분석 및 평가의 모든 구성요소를 정량적 수치로 표현하기가 매우 어렵다. 현재는 정성적인 방법이 널리 사용되고 있다.

2.2 보안의 특성

정보보안은 인가되지 않은 접근, 사용, 공개, 중단, 수정 및 파괴를 하는 행위로부터 정보를 방어하는 방법이다. 정보는 크게 기밀성, 무결성, 가용성의 측면에서 고려된다. 기밀성은 인가되지 않은 개인, 단체, 프로세스에게 노출되거나 제공되지 않아야 하는 속성이다. 무결성은 데이터의 전체 생명주기에 걸쳐 정확성과 완전성을 보증하고 유지하는 것을 의미한다[6]. 이것은 데이터가 승인되지 않거나 알아챌 수 없는 방법으로 변조되지 않아야 하는 것이다. 가용성은 필요할 때 정보에 접근하여 이용 가능해야 하는 특성으로 시스템에 대한 서비스 거부 공격 등을 방지하는 것을 포함한다[7-10].

2.3 위험의 요소들 및 평가방법

자산은 비즈니스와 연관을 가지며 사고 및 사건 발생 시 영향을 받을 수 있는 모든 것이다. 위험 평가를 실시함에 있어서 자산의 범위를 정하는 것은 구체적인 위험도 산정을 위해 중요한 부분이다[11]. 취약성은 공격자에 의해 악용될 수 있는 자산이나 인프라의 설계 구현 또는 운영의 모든 약점이다. 이러한 약점은 건물 특징, 장비의 특징, 직원의 행동, 사람의 위치, 인사 관행 등에서 발생할 수 있다. 위협은 자산에 손해 또는 손실을 야기할 수 있는 잠재적인 모든 상황, 사건을 의미한다. 위험의 분석에서 위협은 자산에 해를 입힐 수 있는 행위를 수행하는 공격자의 능력과 의도의 분석에 기초한다[12].

김성원 외(2007)에 따르면 위험의 구성요소를 자산, 취약성, 위협으로 보고 이들을 어떻게 구성하고 평가하는가에 따라 AVR(ISO/IEC 13335-3부 방법을 이용한 자산-취약성 기반), AVTR(BDSS, HWAK 방법의 자산-취약성-위협 기반), ATVR(OCTAVE, NIST SP800-30, CRAMM, BDSS, CISSP 방법을 이용한 자산-위협-취약성 기반), TVR(SSE-CMM, CA), GAO3, 에너지성-SRAG 방법의 위협 기반) 및 기타(ISO/IEC TR 13335-1부, Open Framework)의 7가지로 기존 위험분석 및 평가방법을 분류하고 있다[13]. 최근 위험분석 및 평가 방법의 연구는 ATVR 유형의 프로세스로 수행되고 있으며 이와 같은 위험분석 및 평

가 방법은 자산기반의 프로세스를 가진다[14].

AVTR방법에서 사용되는 주요 평가방법은 CRAMM, OCTAVE, NIST SP800-30, BDSS 등이 있다. CRAMM은 자산에 대한 영향도를 정한 후 각각의 위협을 정하고 위협에 대한 취약성을 정한다. 이렇게 정해진 영향도와 취약성을 곱하여 나온 값을 위험으로 본다[15]. OCTAVE는 시나리오 기반으로 조직의 운영상에서 나타날 수 있는 위험들을 분석하는 방법론이다.[16], NIST SP800-30은 위험관리과정을 정보시스템 개발 라이프사이클에 적용시키기 위한 프레임워크이며, 9가지 단계로 위험을 평가한다. 위험레벨을 위협의 발생가능성과 영향도를 곱해서 위험을 산정하는 방법이다[17]. BDSS는 사전확률에 조건부확률을 적용시켜 예측의 정확도를 높이는 베이시안 메소드를 의사결정 과정에 적용시킨 모델이다[18].

2.4 위험 시각화 및 벡터의 활용

위험을 시각화하는 것은 위험 평가와 효과적인 의사결정을 위해 사용될 수 있다. 시각화는 위험을 평가하고 식별하는데 중요한 역할을 할 수 있다[28]. 시각화를 함으로써 위험에 대한 정보를 직접적으로 전달할 수 있으며 이는 위험을 수치화하는 방법과도 연결될 수 있다[29]. 또한 시각화는 단순히 데이터 결과를 보는 것보다 집중하는 효과와 더불어 적은 인지적 노력으로 위험을 인식할 수 있도록 한다[30]. 위험을 시각적으로 보여주는 방법은 위험의 효과, 크기, 가능성, 시간에 따른 변화, 위험 비교 등에 따라 다르게 표현된다. 시각화를 통해 위험에 대한 단순 전달이 아니라 위험 정보를 통한 상호작용을 획기적으로 높일 수 있기 때문에 위험을 시각화하여 위험평가에 활용하는 것은 매우 중요하다. 2.2절에서 설명한 위험분석 방법들은 각각의 평가값들을 매트릭스화 시켜 이차원적으로 시각화를 하여 위험 평가에 이용하고 있다. 이러한 위험 시각화 방식은 위험의 요소들을 고려하여 입체적으로 위험을 시각화하는 데 있어서 한계를 지닌다. 이차원으로 표현되는 시각화 방식은 위험도 분포의 다양한 측면을 인지하기 어렵고 위험도가 의미하는 바를 분석적으로 들여다보기 힘든 한계점이 있다. 이러한 한계점은 결과적으로 위험관리 의사결정시에 좁은 시각을 가지고 임하게 되므로 적절한 위험관리 방안 수립 및 의사결정이 이루어지기 위해서는 다차원적인 접근을 통해 효과 및 정확성을 향상시켜야 한다. 따라서 본 논문에서는 기밀성, 무결성, 가용성을 개별적 혹은 종합적인 측면에서 위험을 식별할 수 있도록 벡터를 사용하여 3차원으로 위험을 시각화한다. 정윤정 외(2005)[27]은 NASA Space Program[31]에서 위험 관리에 사용하는 비선형 방법을 사용하여 자산을 평가하는데 벡터를 활용하였다. 벡터를 사용함으로써 자산의 특징에 따른 중요성을 파악하고 자산의 위험을 명확히 평가할 수 있도록 하였다. 본 논문에서는 자산뿐만 아니라 위험 또한 기밀성, 무결성, 가용성 측면에서 산정되게 하여 위험을 다차원적인 관점에서 접근하여 식별할 수 있는 3차원 벡터를 활용한 시각화 방법을 제시한다. 이 방법은 효과적인 위험관리 계획 수립 및 의사결정에 도움이 될 수 있다.

III. 위험분석 방법 및 평가 기준의 사례

위험 시나리오를 산정하는 방법은 OCTAVE[16], BS7799[25], ISO/IEC 27001[26], ISACA에서 사용하는 방법 등이 있으며 위험 구성요소들을 파악하고 위험 시나리오를 구성한다. 본 논문에서는 ISACA의 위험 시나리오 구성 방법을 참고하여 위험분석을 하는데 이용하였다[20]. 본 장에서는 3.1절에서 위험 시나리오 도출을 위한 위험 구성요소들을 설명하고 3.2절에서는 식별된 위험 구성요소 및 위험 시나리오를 기반으로 자산, 위협, 취약성을 평가하기 위한 기준 및 방법을 설명한다.

3.1 ISACA 시나리오 기반 위험분석

위험 시나리오를 위험분석에 유용하게 사용하기 위해서는 위험 구성요소들을 고려해야 한다[20]. 자산(Asset)은 비즈니스에 영향을 주거나 사건에 영향 받을 수 있는 모든 가치 있는 것들이다. 위협원(Actor)은 위협을 일으키는 주체이다. 위협원은 내부자(내부직원, 아웃소싱 직원, 경비, 청소부 등)또는 외부자(경쟁업체, 해커, 외부인 등)로 나눠 볼 수 있다. 위협원은 동기(잠재적 이익, 접근권한)와 능력(기술적 능력, 지식, 자원, 기회)을 기반으로 내부자, 외부자의 위협원을 평가 할 수 있다. 위협 유형(Threat Type)은 사건(Event)의 본질로 볼 수 있다. 위협 유형은 악의적, 사고, 에러, 장애, 자연재해, 외부 요건)으로 구분 지을 수 있다. 사건은 정보의 유출이나 변조, 시스템의 침해, 도난, 파괴와

같은 발생의 유형이다. 마지막으로 시기(Time)은 사건을 탐지하기 위한 시간, 사건이 발생되는 시기 또는 지속 되는 시간 등이다. 위험 시나리오 구성요소를 참고하여 식별된 자산에 대한 위협원, 위협 유형, 사건, 시기를 결정하고, 이를 기반으로 위험 시나리오를 구성한다. 각 구성요소를 산출하여 위험 시나리오를 구성하는 것은 대상 자산에 대해 발생할 수 있는 다양한 위협들을 효과적으로 산출해낼 수 있다[21].

3.2 평가 기준

위험분석방법은 앞에서 언급한 AVR, AVTR, ATVR, GACO3등 다양한 방법들이 존재한다. 위험분석을 수행하는데 있어 다수의 위험분석방법들은 위험과 관련된 각 요소들을 매트릭스화 시켜 나름의 기준을 가지고 위험도를 산정하고 있으며 위험 구성요소들을 나타내는 인자의 수와 결과의 표현방식에 차이가 있다. 본 논문에서는 객관적인 위험분석을 위해 자산, 위협, 취약성을 평가하기 위하여 TRA(Threat and Risk Assessment)방법의 평가 방법을 참고하였다. TRA는 적절하고 비용효과적인 보안통제를 수립하고 위험을 허용가능 수준으로 관리할 수 있도록 적절한 통제방안의 제시 및 보안에 합리적인 의사결정을 할 수 있는 위협 및 위험 평가 방법론이다[22][25]. 자산과 위협은 기밀성, 무결성, 가용성 (이하 CIA) 각각의 측면에서 평가한다. 기밀성 측면에서의 위협은 유출, 노출, 도청, 스니핑, 트래픽 분석 등이 있다. 무결성 측면에서는 정보의 변조, 삭제, 중간자 공격, 위장, 재사용공격, 부인 등이 포함된다. 가용성 측면에서는 서비스 장애 또는 DoS, DDoS 공격 등이 평가의 고려대상이다. 각각의 측면에서 금액, 인적, 기업, 명성, 경쟁구도 사이에서의 침해를 받는 정도에 대하여 평가한다.

3.2.1 자산 가치 평가 방법

자산은 기업마다 매우 다양 및 상이하며 비즈니스 유형, 자산의 특징 및 종류에 따라 자산의 가치는 달라질 수 있다. 자산의 종류는 크게 정보 자산, 문서, 소프트웨어, 물리적, 인적, 회사의 명성, 서비스 등으로 구분될 수 있다[25]. 자산의 식별은 위험 구성요소들을 식별하고 위험 시나리오를 도출하여 위험을 도출하는데 있어 그 시작점이라 할 수 있으므로 자산의 식별은 위험분석 프로세스에서 중요한 부분을 차지한다. 자산 가치 평가는 [Table 1]을 참고하여 CIA측면으로 각각 평가한다[27].

Table 1. Asset Valuation Criteria

Rating	Description
5	Breach could result in high-dollar losses, or in exceptionally grave injury to an individual's or the organization's: well-being; reputation; privacy; or competitive position, and the business process will fail
4	Breach could result in very serious loss or injury, and the business process could fail
3	Breach could result in serious loss or injury, and the business process could be negatively affected
2	Breach could result in minor loss or injury
1	Breach could result in little or no loss or injury

3.2.2 위협 평가 방법

위협은 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자로 정의되며 위험분석 방법론마다 다양한 위협의 목록을 제시하고 있다. 위협의 유형은 자산에 영향을 미치는 방식을 규정하며 그 위협에 대응하기 위한 대책 선정에도 영향을 미친다. 본 논문에서 제시하는 방법에서는 다양한 위협원 및 위협 유형 등을 식별하여 기밀성, 무결성, 가용성의 측면에서 요구성 정도를 평가하였다.[25]

위협원은 고의나 실수로 취약점을 이용하여 자산에 해를 가하는 주체를 뜻한다. 위협원은 동기와 능력에 따라 평가될 수 있다. 여기서 동기란 위협원에게 주어지는 잠재적 이익, 위협원이 접근 가능한 자원을 고려하여 평가된다. 동기는 자연적이거나 임의로 일어나는 현상에 대해서는 고려되지 않는다. 한편, 능력이란 위협원이 취약점을 이용하여 자산에 대해 성공적으로 공격을 수행할 수 있는 능력으로서, 기술적 능력, 지식, 자원, 기회 등으로 구분 된다[25].

[Table 2]를 기초로 능력과 동기를 고려하여 [Table 3]과 같은 매트릭스를 얻을 수 있다. 이렇

게 표현된 매트릭스의 각 등급에 따른 요구성 정도는 〔Table 4〕와 같다. 이를 기반으로 위협을 CIA 측면에서 각각 평가한다.

Table 2. Threat Agent Capability and Motivation Ratings

Capability	Rating	Motivation
Highly capable. Has knowledge, skills and resources to mount an attack	3	Highly motivated. Almost certain to attempt an attack
Moderate capability. Has knowledge, skills to mount attack, lacking in some resources Or, lacking some knowledge but has sufficient resources to mount an attack	2	Moderate level of motivation. Would act if prompted, or provoked
Little or no capability to mount an attack	1	Little or no motivation. Not inclined to act

Table 3. Threat Agent Rating Combinations

Capability Rating	Motivation Rating		
	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5

Table 4. Overall Threat Agent Ratings

Rating	Description
5	Highly capable and motivated.
4	Highly capable, moderate level of motivation Or, moderate capability, highly motivated
3	Highly capable, little or no motivation. Or, little or no capability, highly motivated, Or, moderate capability, moderate level of motivation
2	Little or no capability, moderate level of motivation. Or, moderate capability, little or no motivation
1	Little or no capability or motivation

3.2.3 취약성 평가 방법

취약성은 그 자체로 피해를 야기하지는 않으며 공격에 의해 피해를 입을 수 있는 자산에 대한 조건의 집합 또는 조건이다.

TRA 방법에서는 취약성 평가에 하나 또는 그 이상의 위협 사건의 발생으로부터 기인한 영향의 심각성 및 손실에 대한 잠재적인 노출을 고려한다. 취약성 평가는 〔Table 5〕에서처럼 심각성과 노출을 고려하여 〔Table 6〕와 같은 매트릭스를 얻을 수 있다. 매트릭스에서의 1~5 등급에 따른 요구성 정도는 〔Table 7〕과 같으며 이를 이용해 취약성 정도를 평가한다.

Table 5. Vulnerability Rating

Severity	Rating	Exposure
High severity. Few resources to exploit with significant potential for loss	3	High exposure. Affects a majority of system components.
Moderate severity. Significant resources to exploit with significant potential for loss. Little resources to exploit with moderate potential for loss	2	Moderate Exposure. Can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities
Minor severity. Significant resources to exploit with little potential for loss	1	Minor exposure. Effects tightly contained. Does not increase the probability

Table 6. Vulnerability Rating Combinations

Severity Rating	Exposure Rating		
	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5

Table 7. Overall Vulnerability Ratings

Rating	Description
5	Highly exposed, high severity.
4	Highly exposed, moderate severity; Or, moderate exposure, high severity.
3	Highly exposed, minor severity; Or minor exposure, high severity; Or moderate exposure, moderate severity.
2	Minor exposure, moderate severity; Or moderate exposure, minor severity.
1	Minor exposure, minor severity.

IV. 개선된 위험도 시각화 방법

본장에서는 평가된 자산, 위협, 취약성을 기반으로 위험도를 산정하는 방법과 3차원 다이어그램의 활용을 설명한다. 3차원으로 표현되는 요소들은 위험분석의 여러 기준들에서 일반적으로 사용되는 기밀성, 무결성, 가용성이다. 위험이 세 가지 측면으로 산정됨으로써 각 측면에 특화된 위험 관리 계획이 수립될 수 있다. 따라서 본 논문에서는 기밀성, 무결성, 가용성 측면으로 평가하여 위험 또한 각 측면으로 산정될 수 있도록 하였다. 4.1절에서는 3차원 벡터를 이용하여 위험을 시각화하고, 4.2절에서는 위험 산정 방법을 설명한다. 마지막으로 4.3절에서는 제시하는 방법으로 자동차대여사업 기업의 위험분석 평가 자료를 재평가하여 그 유효성을 점검한다.

4.1 3차원 벡터를 이용한 위험 시각화

3차원으로 표현된 위험은 집중적으로 통제를 해야 하는 측면을 식별하기에 용이하다. 위험은 하나의 시나리오, 한 자산 또는 전체 자산에 대한 위험을 나타낼 수 있다. (a)를 보면 V1, V2는 위험에 대한 유형(벡터의 방향)을 나타낸다. 각각의 위험은 벡터 V와 공간을 고려하여 벡터의 방향에 따라 어떤 측면의 위험이 집중적으로 통제되어야 하는지 식별할 수 있다. 또한 (b)를 보면 위험은 DoA공간을 비롯하여 〔C, I, A, (C, I), (C, A), (I, A), (C, I, A)〕라는 8가지의 공간으로 범주화할 수 있다.

이 8가지의 공간 속에서 3차원 상에 표현된 위험은 벡터 V의 방향성에 따라 어떤 공간속에 위험이 포함되는지 식별할 수 있다. DoA 공간은 위험이 통제가 잘 되고 있거나 수용할 수 있는 부분이며, 그 외의 공간들에 대해서는 벡터의 방향을 기반으로 위험이 어떤 공간에 포함되는지를 식별한다.

4.2 3차원 시각화를 위한 위험 산정 방법

본 절에서는 3.2절에서의 평가기준을 이용하여 도출된 자산, 위협, 취약성을 평가하고 CIA 측면으로 위험을 산정하는 방법을 설명한다. 행렬로 이루어진 수식을 이용하여 위험을 CIA 각 측면으로 산정할 수 있다. 산정된 위험도는 3차원으로 표현하여 집중적으로 관리해야하는 측면을 식별할 수 있고 위험 관리 방안을 수립하는데 의미 있게 사용될 수 있다.

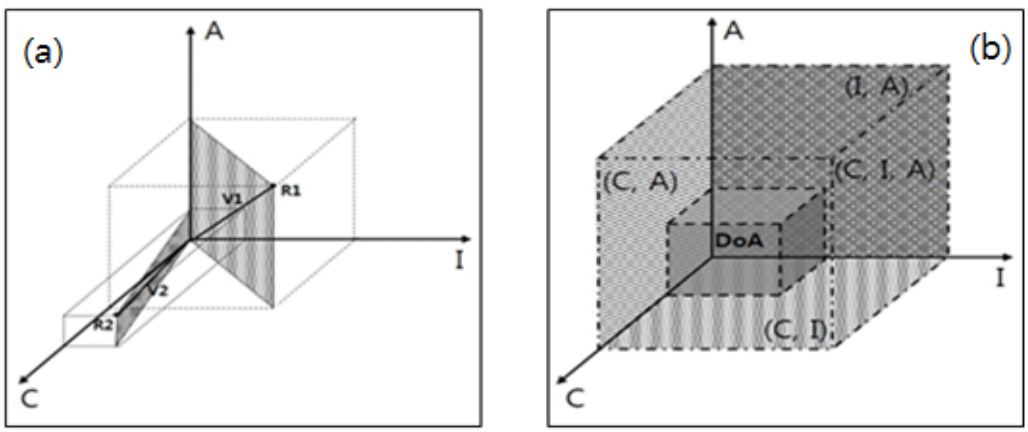


Fig. 1. Risk Identification Through 3-Dimensional Vector

$$[R_{C_i}R_{I_i}R_{A_i}] = \nu A T = \nu[a_{C_i}a_{I_i}a_{A_i}]\begin{bmatrix} t_{C_i} & 0 & 0 \\ 0 & t_{I_i} & 0 \\ 0 & 0 & t_{A_i} \end{bmatrix} \quad (1)$$

- $A = [a_{C_i}\ a_{I_i}\ a_{A_i}]$: 자산의 가치
- $T = \begin{bmatrix} t_{C_i} & 0 & 0 \\ 0 & t_{I_i} & 0 \\ 0 & 0 & t_{A_i} \end{bmatrix}$: 위협 수준
- $\nu = Vulnerability$: 취약성 수준

CIA 측면의 위험은 각각 최소 1~ 최대 125의 값을 가지며 각 측면으로 정해진 DoA와 비교를 통해 DoA를 상회하는 위험을 식별할 수 있다. 산정된 위험은 또한 〔Table 8〕과 같이 각 측면의 위험 정도 또는 벡터량을 계산하여 해당 위험의 위험 정도를 알 수 있다. 또한 각 측면의 위험은 원점에서 좌표까지의 거리가 해당 위험의 위험량(벡터량)이 된다.

$$R_D = \sqrt{R_{C_i}^2 + R_{I_i}^2 + R_{A_i}^2} \quad (2)$$

위험량 R_D는 최소 $1.7(\fallingdotseq \sqrt{1^2+1^2+1^2})$, 최대 $216(\fallingdotseq \sqrt{125^2+125^2+125^2})$ 사이의 값을 가지며 〔Table 8〕와 같이 값의 범위에 따라 위험 정도를 나타낼 수 있다. 위험은 그 정도에 따라 Very High ~ Very Low의 5가지 위험 정도로 분류해 볼 수 있다.

이 정도를 기반으로 DoA를 정하고 산정된 위험 정도와 비교하여 고위험군을 식별해낼 수 있으며 위험의 우선순위를 매겨 관리할 수 있다.

Table 8. Degree Classification of Risk

Degree	R_D	C	I	A
Very High	174~216	101~125		
High	131~173	76~100		
Medium	88~130	51~75		
Low	45~87	26~50		
Very Low	1.7~44	1~25		

4.3 개선된 위험 시각화 방법 적용사례

본 절에서는 연 매출 1조 700억원, 종업원 수 1,408명, 국내 1위를 차지하고 있는 자동차대여사업 종 기업의 위험분석 평가 자료를 기반으로 제안하는 위험도 산정 방법을 적용하여 CIA 각각의 측면으로 위험도를 산출하고 제시된 방법의 유효성을 점검한다. 〔Table 9〕은 대상 자산(고객정보 DB Data)에 대하여 앞에서 언급한 위험 구성요소들을 식별하고 자산, 위협, 취약성을 평가하여 위험도를 산정한 것이다.

4.3.1 위험분석 프로세스

위험분석 프로세스의 진행과정을 좀 더 자세히 설명한다.

1) 자산에 대하여 위협원, 위협 유형, 행위, 발생 시기를 식별
2) 식별된 위험 구성요소들을 기반으로 위험 시나리오 도출
3) 위험구성요소들과 시나리오를 기반으로 자산, 위협을 CIA측면으로 평가
4) 취약성 평가
5) 평가값을 기반으로 제시한 위험도 산정식을 이용하여 위험도 산정
6) 3차원 다이어그램을 활용한 위험의 식별 및 대응 방안 수립

〔Table 9〕는 위험분석 프로세스에서 1)~5)까지를 나타내며 다음의 4.3.2에서 3차원 벡터를 이용하여 위험을 시각화하고 DoA와의 비교를 통해 통제되어야 하는 위험을 식별하는 방법을 설명한다.

4.3.2 위험 시각화

〔Table 9〕의 위험분석 결과를 3차원으로 표현하여 위험을 식별한다. 이후 DoA를 벗어나는 위험들을 식별하고 대응방안을 모색할 수 있다. 〔Fig. 2.〕는 〔Table 9〕에서 산정된 위험을 3차원으로 표현한 것이다.

이렇게 좌표로 나타낸 위험들은 벡터의 방향성을 이용하여 DoA를 상회하는 위험이 어떤 측면에 대해서 취약한지 식별할 수 있다.

자산 '고객정보 DB Data'에 대한 위험은 8가지 시나리오별로 산정되었으며 3차원으로 표현하면 〔Fig. 2.〕과 같으며, DoA속의 위험들은 위험을 수용하거나 위험이 잘 관리되고 있음을 의미한다. 또한

Table 9. Risk Assessment Result

Asset	Actor	Threat Type	Event	Time	Scenario	Asset			Threat			Vulnerability	Risk		
						C	I	A	C	I	A		C	I	A
DB Data	Internal	Deliberate	Leakage	Off-Hour	1	5	4	3	5	4	3	5	125	80	45
	Internal	Mistake	Leakage	Working hour	2	5	4	3	5	4	3	3	75	48	27
	Internal	Mistake	Modify	Ongoing	3	4	5	3	4	5	4	3	48	75	36
	Internal	Deliberate	Unauthorized Access	Off-Hour	4	4	4	5	4	4	3	4	64	64	100
	External	Deliberate	Leakage, Unauthorized Access	Ongoing	5	5	4	5	5	4	3	5	125	80	125
	Internal	Mistake	Leakage	Ongoing	6	5	4	3	5	4	3	4	100	64	36
	External	Deliberate	Modify, Unauthorized Access	Ongoing	7	4	5	5	4	5	3	5	80	125	100
	External	Mistake	Leakage	Ongoing	8	5	4	3	5	4	3	3	75	48	27

벡터를 이용하여 DoA와 공간으로서 위험을 식별하면 〔Fig. 3.〕과 같다. 좌표로 표현된 각 위험은 〔Fig. 3.〕과 같이 벡터의 방향성을 이용하여 위험을 더욱 가시적으로 식별할 수 있다.

본 논문에서는 DoA를 각 측면에 대해 80으로 가정하였다. DoA값과 CIA측면으로 산정된 위험값을 비교해 보면 〔Table 10〕과 같이 DoA를 상회하는 위험들을 식별할 수 있다. CIA 각 측면에서 DoA를 상회하는 측면을 음영처리해보면 위험 S1, S4, S5, S6, S7이 식별된다. 또한 수식(2)를 통해 각 위험의 위험량을 가지고 〔Table 8〕을 이용해 식별된 각 위험의 위험 정도 또한 알 수 있다.

식별된 위험들을 살펴보면 High, Very High의 고위험 정도를 가지는 위험들이 식별되었고, 식별된 각 위험들의 CIA 측면에 대해 공간을 범주화해보면 위험 S1, S5, S6의 경우는 〔기밀성(C)〕을, S4는 〔가용성(I)〕, S7은 〔무결성과 가용성(I, A)〕을 집중적으로 고려하여 대응방안을 수립해야 함을 알 수 있다. 기존의 위험 분석 결과는 〔S1, S2, S6, S7,

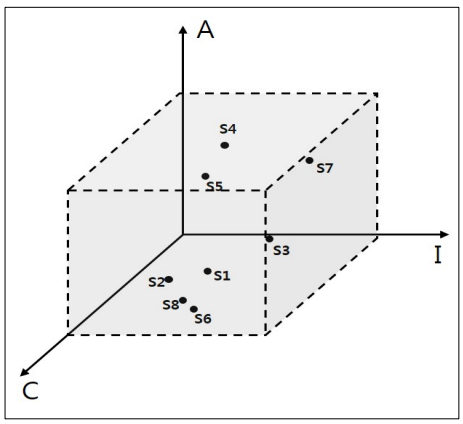


Fig. 2. Risk Calculation Result

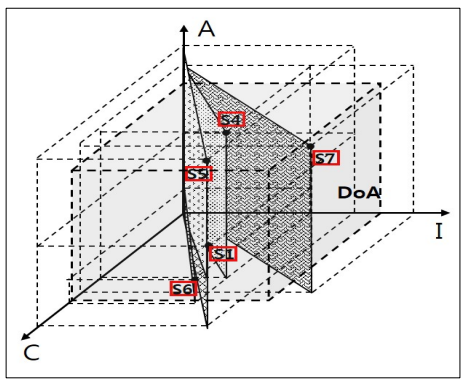


Fig. 3. Risk Identification Using Vector

S8]이 고위험군으로 산정되었다. 반면 재평가된 위험에서는 [S2, S8]이 고위험군에서 제외되어야 함을 알 수 있다. 따라서 의사결정자는 두가지 위험에 대하여 인력이나 비용 효과적인 관리계획을 수립할 수 있음을 알 수 있다. 의사결정자는 벡터량을 이용한 위험량 뿐만 아니라 CIA 각 측면으로 산정된 위험을 고려하여 구체적인 위험 관리 계획을 세울 수 있다. 이렇게 CIA 각 측면으로 산정된 위험을 통해 중점적으로 통제되어야 하는 측면에서 위험 구성요소들을 기반으로 수립되는 위험 관리 계획은 구체적이며 효과적이다. 결과적으로 적절한 위험의 분석은 정보보호 의사결정에 있어 도움을 줄 수 있다.

Table 10. Comparison with DoA

No	DoA	C	I	A	R_D	Degree
S1	80	125	80	45	155	High
S2		75	48	27	93	Medium
S3		48	75	36	96	Medium
S4		64	64	100	134	High
S5		125	80	125	194	Very High
S6		100	64	36	124	High
S7		80	125	100	178	Very High
S8		75	48	27	93	Medium

V. 결론 및 향후 과제

본 논문에서는 CIA 측면에서 자산과 위협을 각각 평가하고, 취약성을 고려하여 정교하게 위험도를 산정하고 이를 3차원으로 시각화하여 위험을 식별, 식별된 위험을 기반으로 효율적인 위험관리방안을 수립할 수 있는 개선된 3차원 시각화 방법을 제시하였다. 위험 구성요소 및 위험 시나리오를 식별 및 도출하는 것은 자산, 위협 및 취약성을 구체적으로 평가하는데 사용된다. 이를 기반으로 CIA 각 측면의 위험을 산정한다. 이렇게 산정된 위험도는 3차원 좌표로 표현할 수 있다. 3차원으로 표현된 위험도는 2차원적으로 보는 것보다 입체적이고 가시적으로 위험을 파악하고 대응 방안 수립에 용이하다. 3차원 벡터를 활용한 방법은 [Fig. 4.]의 위험분석 프로세스에서 위험 평가 부분에 적용할 수 있다.

3차원으로 위험을 시각화해봄으로써 위험 분포의 다양한 측면을 식별할 수 있으며 이는 의사결정에 있어 위험을 넓은 시각으로 볼 수 있도록 한다. 또한 위험도를 CIA 각 측면에서 개별적 혹은 종합적으로 분석해볼 수 있다.

3차원 상에 표현된 각 위험들은 벡터를 이용하여 어떤 측면을 집중적으로 고려해야 하는지 알 수 있으며 DoA 공간과 비교를 통해 통제를 해야 하는 위험들을 식별할 수 있다. 식별된 위험들은 공간에 따라 그룹핑을 하여 각 그룹에 대한 개별적인 통제방안을 수립할 수도 있다. 또한 3차원 상에서는 위험 시나리오별 위험, 자산별 위험, 전체 위험 총량 등을 산정하는 것이 가능하며 위험을 다양한 관점에서 접근하는 것이 가능하다. 이러한 3차원을 이용한 위험분석은 다양성 및 분석적인 관점에서 효과적인 위험 통제 방안 수립과 더불어 의사 결정자의 효과적인 정보보호 의사결정에 도움을 줄 수 있다.

향후 3차원 좌표로 표시한 위험도의 기울기를 고려하여 전체 위험도에서 기밀성, 무결성, 가용성이 차지하는 비율을 계산하는 방법론을 제시하고, 3차원으로 표시된 위험도를 RMS(Risk Management System) 솔루션에 적용하는 방안 모색 등 제시한 방법을 시스템화 시켜 실제 위험분석에 적용해 볼 수 있는 연구가 필요하다.

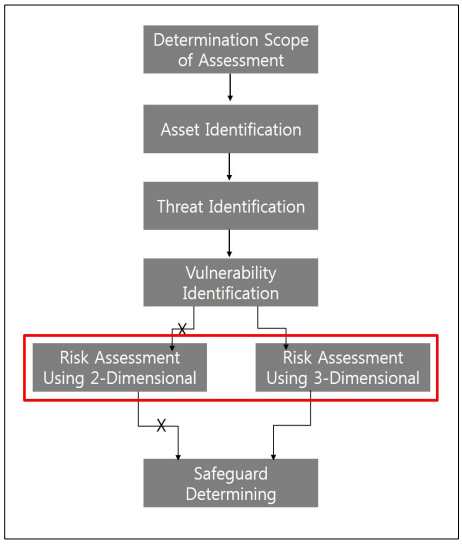


Fig. 4. Risk Analysis Process

References

[1] ISACA (2006), "CISA Review Manual 2006. Information Systems Audit and Control Association," p. 85. ISBN 1-933284-15-3.

[2] ISO/IEC 13335-1 : 1996, "Guidelines for the Management of Security - Part 1 : Concepts and Models of IT Security," 1996.

[3] Artur Rot, "IT Risk Assessment: Quantitative and Qualitive Approach," Proceedings of the World Congress on Engineering and Computer Science, Oct 22-24, 2008, San Francisco, USA

[4] Christopher Alberts, Audrey Dorofee, James Stevens and Carol Woody, "Introduction to the OCTAVE®," Aug. 2003.

[5] Yazar and Zeki, "A qualitative risk analysis and management tool-CRAMM," SANS InfoSec Reading Room White Paper (2002).

[6] Boritz and J. Efrim, "IS Practitioners' Views on Core Concepts of Information Integrity," International Journal of Accounting Information Systems. Elsevier. Retrieved 12, Aug. 2011.

[7] ANNEX TO NISTISSI No. 4011, INFORMATION SYSTEMS SECURITY : A COMPREHENSIVE MODEL

[8] Loukas, G. and Oke, G., (September 2010) [August 2009]. "Protection Against Denial of Service Attacks: A Survey," Comput. J. 53 (7): 1020 - 1037. doi:10.1093/comjnl/bxp078.

[9] ISO 7498-2, Information processing Systems - Open Systems Interconnection - Basic Reference Model -Part 2 : Security Architecture

[10] NIST SP. "800-33, Underlying Technical Models for Information Technology Security." National Institute for Standards and Technology (2001)

[11] Rainer Jr, Rex Kelly, Charles A. Snyder, and Houston H. Carr., "Risk analysis for information technology," Journal of Management Information Systems (1991): 129-147.

[12] Cox Jr and Louis Anthony Tony. "Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks." Risk Analysis 28.6 (2008): 1749-1761.

[13] Sung won Kim, Hui young Kim, Young chan Kwon, Ho sang Yun and Chul ho Kim, "Risk analysis and assessment Methodology Research for network based Real-time Risk Management," KCC, vol. 34, no. 1.

[14] Kwo-jean Farn et al., "A study on information security management system evaluation-assets, threat and vulnerability," Computer Standards & interfaces 26 (2004) 501-513.

[15] Hank Marquis, "10 Steps to Do It Yourself CRAMM," vol.4.50, December 17, 2008.

[16] Caralli and Richard A., et al., "Introducing octave allegro: Improving the information security risk assessment process," No. CMU/SEI-2007-TR-012. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2007.

[17] NIST, SP. "800-30 Risk Management Guide for Information Technology Systems," National Institute for Standards and Technology (2002).

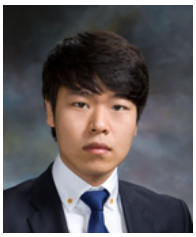
[18] Ferson and Scott. "Bayesian methods in risk assessment," Technical report for the Waste and Storage Unit, Service Environnement & Procédés, Bureau de Recherches Géologiques et Minières, France. Available at: www. ramas. com/bayes. pdf, 2003.

[19] ISACA. "The it practitioner guide. Technical report," ISACA, USA, 2009

[20] Inhyun Cho and Jaehee Lee, "Study on

scenario-based Personnel Risk Analysis," Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 12 (January 15, 2015)
[21] CSE, RCMP. "Harmonized Threat and Risk Assessment (TRA) Methodology," TRA-1 Date: October 23 (2007).
[22] ISO27k implementer's forum,"Matrices for Asset Valuation and Risk Analysis," www.ISO27001security.com, 2009.
[23] Christopher Alberts and Audrey Dorofee, "OCTAVESM*Threat Profiles," Software Engineering Institute Carnegie Mellon University's White Paper.
[24] "Threat risk assessment working guide," 1999, Government of Canada, Communications Security Establishment, p 73.
[25] British Standards Institute (BSI), "Information security management systems - part 3: Guidelines for information security risk management," BSI Standard 7799-3:2006, 2006.
[26] Brewer and David. "An Introduction to ISO/IEC 27001: 2013," London: Bristish Standards (2013).
[27] Chung, Yoon Jung, et al. "Security risk vector for quantitative asset assessment," Computational Science and Its Applications-ICCSA 2005. Springer Berlin Heidelberg, 274-283.
[28] Eppler, Martin J., and Markus Aeschimann. "A systematic framework for risk visualization in risk management and communication," Risk Management 11.2 (2009): 67-89.
[29] Lipkus, Isaac M., and J. G. Hollands. "The visual communication of risk," Journal of the National Cancer Institute. Monographs 25 (1998): 149-163.
[30] Smerecnik, Chris MR, et al. "Understanding the positive effects of graphical risk information on comprehension: measuring attention directed to written, tabular, and graphical risk information," Risk analysis 30.9 (2010): 1387-1398.
[31] Dezfuli, Homayoon, et al. "NASA Risk Management Handbook. Version 1.0," (2011).

〈저자소개〉



이 주 영 (Ju-Young Lee) 학생회원
2012년 2월: 단국대학교 멀티미디어공학과 졸업
2014년 3월~현재: 고려대학교 금융보안학과 석사과정
〈관심분야〉 금융보안, 위험관리, 위험분석, 정보보호컨설팅

조 인 현 (In-Hyun Cho) 학생회원
2013년 7월: 고려대학교 지리교육과/국제학부 졸업
2014년 9월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 사이버보안, 내부자보안, 시스템보안

이 재 희 (Jae-Hee Lee) 학생회원
2015년 2월: 고려대학교 물리학과 졸업
2015년 9월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 전자공학, 통신공학

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 교수
〈관심분야〉 위험관리. 정보보호컨설팅. 정보보호 및 개인정보보호정책