Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.1, Feb. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.147

발전된 보안 시각화 효과성 결정 모델

이 민 선,† 이 경 호‡
고려대학교 정보보호대학원

Decision Model of the Effectiveness for Advanced that Security Visualization

Min-Sun Lee,† Kyung-Ho Lee‡
Graduate School of information Security, Korea University

요 약

IT 환경의 변화 속에서 다양한 서비스와 기기의 출현으로 인하여, IT 규모의 증가와 더불어 데이터의 복잡도가 높아지면서 많은 조직에서 보안 상황 인지를 위한 대량의 데이터 분석 및 처리에 어려움을 겪고 있다. 이에, 조직의 위험관리에 있어서 보안 상황의 인지와 대응이 늦어지는 문제의 해결을 위해, 시각화를 통한 보안 상황 인지 효과의 향상을 제안한다. 이를 위해, 본 연구에서는 시각화와 관련한 다양한 관점에서의 선행 연구를 통해 사용자 유형, 상황 인지 단계, 정보 시각화의 속성 등을 고려하여 효과적 시각화를 위한 평가 요인과 대안을 선정하고 AHP 계층 모델을 수립하였다. 이를 토대로, 다 기준 의사결정 문제의 해결을 위한 AHP 기법을 활용하여 효과적 시각화를 위한 요인과 요인별 대안의 중요도를 산정함으로써, 시각화의 목적 및 사용자 유형에 따라 보안 상황의 인지 효과를 향상할 수 있는 시각화 방안을 제시하고자 한다.

ABSTRACT

With the advent of various services and devices in the change of IT environment, increasing the complexity of the data, and increasing scale of IT, Many organizations are experiencing the difficulty of analyzing and processing with a large amounts of data for security situations awareness. Therefore, propose the enhancement of security situational awareness through visualization in order to solve the problems of slow response and security situational awareness in organizational risk management. In this paper, we selected the evaluation factors and alternatives for effective visualization by considering user type, situational awareness step, and information visualization attributes through various studies on visualization. And established AHP layer model. Based on this, by using the AHP method for solving the problem of multi-criteria decision making, by calculating the factors for effectively visualizing and the importance of alternative by factor, try to propose a visualization method that can improve the effectiveness of the security situational awareness according to the purpose of visualization and the type of user.
Keywords: Security Visualization, Situational Awareness, AHP, MCDM, Network Security

I. 서 론

1.1 연구 배경 및 목적

IT 기술은 비즈니스 요구와 결합하여 빠르게 변화하며 급속한 성장을 이루고 있고, 이러한 성장의 이면에는 다양한 서비스와 기기의 출현과 함께 엄청난 트래픽과 데이터의 증가가 수반되고 있다. 이와 더불어 IT 환경에 대한 공격 기술도 함께 고도화 되면서 보안 위협이 증가하고, 이로 인한 대규모 보안 사고

Received(12. 06. 2016), Modified(12. 26. 2016), Accepted(12. 29. 2016)

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

들이 연이어 발생하면서 효과적 공격 방어를 위한 다양한 방법에 대한 요구도 함께 증가하고 있다.

이처럼, IT 발전에 따른 규모와 복잡도의 증가로 인해 대량의 데이터 분석에 어려움을 겪고 있는 다수의 조직들은 보안 위협을 탐지하고 대응하는 데에 더 집중해야만 한다. 대량의 로그 데이터 속에서 모든 데이터를 살펴보는 것에는 제약이 따르기 때문에, 시각화의 기술적인 요소와 더불어 데이터를 요약하고, 한 눈에 살펴볼 수 있도록 돕는 시각화 방법론적 요소의 중요성이 커지고 있다[1].

위와 같은 이유들로, 시각화 기반의 분석 기술이 더욱 주목 받게 되면서 시각화는 상황 인지와 더불어 효과적인 보안 위협의 탐지 및 대응을 위한 주요 방안으로 정보보호 분야에서 이슈가 되고 있다.

상황 인지(situational awareness)란 "주변에서 진행되고 있는 또는 발생하고 있는 무언가를 알고, 알고 있는 범위 내에서 중요한 것이 무엇인지를 아는 것"[2]을 말하며, '인식(perception)', '이해(comprehension)', '예측(projection)'의 3단계로 이루어진다[2][3]. 상황 인지 기술은 대규모 네트워크에서의 보안 위협 발생 시, 여러 관점에서 발생하는 보안 이벤트들 사이의 관계에 기초하여 전체적인 네트워크 보안 상황을 효과적으로 판단[4]하는 데 활용할 수 있다.

시각화(visualization)는 사용자에게 더 효율적으로 정보를 전달하기 위하여 그래픽 요소를 활용하여 데이터가 정보로서 의미가 생성되도록 직관적으로 형상화 하는 것[5]을 말하며, 대량 정보의 '인식'과 '이해'에 효과적인 방법으로 알려져 있다. 이와 같은 시각화 기반의 분석 기술은 실시간으로 발생하는 보안 이벤트를 즉각 처리하여 관리자가 방대한 양의 데이터를 빠르게 이해하는 것을 가능하게 해주며 알려지지 않은 이상 패턴을 표현해 줌으로써 관리자가 신속하게 상황에 대처할 수 있도록 도와준다[6].

본 연구는 대규모의 복잡한 환경 속에서 발생 가능한 다양한 보안 상황을 효과적으로 탐지 및 대응하기 위해, 시각화를 이용하여 보안 상황 인지 효과의 향상 방안을 제시하는 데 그 목적이 있다.

이와 관련하여, 정보보호 분야에서 선행된 시각화 연구들을 살펴보면 색상, 형태 등 시각화의 특정 구성 요소들을 활용하여 보안 위협 또는 상황(이벤트)의 탐지를 위한 시각화 시스템의 설계 및 구현에 중점을 두고 있음을 알 수 있다. 이러한 연구들은 대체로 보안 위협 또는 상황의 탐지 여부로 그 효과를 입증하고 있으나, 대규모 네트워크와 같은 복잡한 환경에서 실제 보안 상황이 발생하는 경우에는 해당 시각화 패턴을 식별하기 어렵거나 필요한 정보가 충분히 제공되지 않는 등의 문제가 발생하여 시각화의 효과가 충분히 검증되지 않는 경우가 발생한다. 이를 통해, 실제 보안 업무에서의 활용 목적과 대상, 상황 인지 단계의 특성 등에 따라서 구현된 시각화(요소)의 효과는 다르게 나타날 수 있음을 알 수 있다.

이에, 본 연구에서는 시각화 구현 요소의 선택에 있어서 시각화의 목적과 대상, 상황 인지 특성 등을 고려하여 최적의 시각화 요인이 선정될 수 있도록 보안 시각화 효과성 결정 모델을 제시함으로써, 향후 정보보호 분야에서 연구될 보안 시각화 시스템의 구현 시 실질적인 효과성 향상에 기여하고자 한다.

1.2 연구 방법과 구성

본 연구에서는 상황 인지 및 시각화와 관련한 선행 연구를 기반으로 '효과적 정보 시각화를 위한 평가기준'을 선정하고, AHP(Analytic Hierarchy Process) 기법을 이용하여 도출된 중요도에 따라 주요 요인과 대안을 최종 선정함으로써, 보안 상황 인지 효과의 향상을 위한 시각화 방안을 제시 한다.

이를 위해, '효과적 정보 시각화를 위한 평가기준'을 바탕으로 수립된 AHP 모델을 이용하여 국내 금융, 통신, 공공, 교육, 서비스 등 5개 분야 9개 조직의 보안 업무 관련자 24명을 대상으로 설문조사를 수행하였다. 이 중 유효성 평가를 통과한 7개 조직 20명에 대한 설문결과를 바탕으로 보안 모니터링 업무 관리자 및 운영자, 보안전문가(컨설턴트) 그룹으로 구분하여 사용자 유형별 시각화 특성을 분석한다.

다음 2장에서는 선행 연구를 통해 상황 인지 및 시각화에 대한 개념과, 다양한 보안 시각화 기술의 장단점 및 효과적 시각화 방안의 평가기준에 대해 살펴보고, 3장에서는 AHP 기법을 통해 효과적 정보 시각화 요인과 요인별 대안의 중요도를 평가하여 분석 결과를 검토한다. 마지막 4장에서는 본 연구의 결론과 연구를 수행함에 있어서 도출된 한계점을 바탕으로 향후 발전 방향을 제시한다.

II. 선행 연구 검토

2.1 상황 인지

2.1.1 상황 인지의 단계 및 정의

상황 인지 분야의 저명한 과학자인 Mica R. Endsley는, 상황 인지에 대해 시간과 공간의 체적을 가진 환경 요소를 인식하여 그 의미를 이해하고 가까운 미래의 그 상태를 예측하는 것[2]이며, 이는 '인식', '이해', '예측'의 3단계로 이루어진다고 하였다.

Fig. 1.[7]에 보이는 것처럼 상황 인지 과정의 각 단계별 특징을 살펴보면, 1단계 '인식'은 환경 속에서 반드시 알아야 하는 요소들을 앎을 의미하는 것이고, 2단계 '이해'는 그들이 인식한 요소들을 결합하고 통합하여 그들의 목표를 중점으로 의미를 도출하는 것이다. 마지막 3단계 '예측'은 미래에 예상되는 사건들을 미리 투사하는 개체의 능력으로 다음 행동 단계의 결정을 돕는다[3].

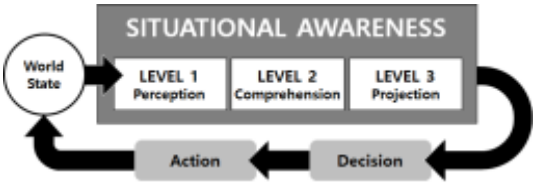

Fig. 1. Situation awareness is the key to good decision making[7]

2.1.2 네트워크 보안 상황 인지와 시각화

네트워크에서 보안 위협이 발생하는 경우, 운영자들이 보안 상황을 인지하는 데 있어서, 효과적인 '인식'과 '이해'는 이를 바탕으로 다가올 미래의 상황을 '예측'하게 함으로써 적시에 적절한 의사 결정을 통해 미리 대응할 수 있도록 하는데 도움이 된다. 때문에 보안 상황 인지의 효과성 향상을 위해 상황 인지의 세 단계를 기반으로 하나 이상의 단계에 시각화를 적용하는 방법이 있다. 시각화는 효율성과 직관성 향상의 대표적인 방법[8]으로 네트워크에서 보안 상황 인지를 위해 적용하게 된다면, 대량의 로그 데이터를 실시간으로 시각화 하여 네트워크 관리자에게 관련 정보를 쉽고, 빠르며, 정확하게 전달할 수 있게 된다. 네트워크 보안 상황 인지를 위한 시각화 기술에는 크게 네트워크 패킷 또는 트래픽 정보를 표현하여 이상 상황을 판단하는 기술과, 침입탐지시스템(IDS:Intrusion Detection System)이나 방화벽(FW:FireWall) 등과 같은 보안장비들에서 발생하는 보안 경보를 표현 및 분석하는 기술들이 있다[9].

2.2 시각화

2.2.1 시각화 단계 및 정의

위키피디아에 따르면, 데이터 시각화(data visualization)는 데이터 분석 결과를 쉽게 이해할 수 있도록 시각적으로 표현하고 전달되는 과정을 말하며, 데이터 시각화의 목적은 도표(graph)라는 수단을 통해 정보를 명확하고 효과적으로 전달하는 것이라고 정의하고 있다. 데이터 시각화는 미적 형태와 기능성 두 가지를 모두 포괄하는 것으로 대개 데이터들의 연결과 그룹핑을 표현하는데 초점을 둔다[10]. ETRI(신희숙 외)의 연구[11]에 따르면, 데이터 시각화가 이루어지기 위해서는 정보 조직화 단계, 정보 시각화 단계, 상호 작용 단계를 거치게 되며, 각 단계는 다음과 같은 특성을 갖는다.

① 정보 조직화 단계
: 사용자의 정보 인지에 관여하며, 데이터를 분류하고 배열하고 조직화하여 질서를 부여함

② 정보 시각화 단계
: 사용자의 정보 지각에 관여하며, 보다 효율적인 정보 전달을 위해 시각, 청각 등의 감각 기관에 최적의 자극을 제시하는 방법을 찾음

③ 상호 작용 단계
: 정보와 사용자 간의 상호 작용 측면의 사용자 경험을 디자인하며, 정보의 인지적 요인뿐만 아니라 지각적 요인을 함께 활용하고, 정보 시각화 단계와 밀접하게 연동됨

위와 같이 시각화 과정의 단계별 특성을 살펴봄으로써 정보 시각화가 상황 인지 과정에서 '인식'과 '이해'에 영향을 미치고, 더불어 정보 시각화 결과를 바탕으로 상호 작용을 유도함으로써 지각적 요인을 활용, '예측'을 통한 의사결정에 도움을 줄 수 있음을 확인할 수 있다.

2.2.2 정보 시각화의 기본 속성

정보 시각화의 기본 속성은 내용(content), 구조

(Structure), 형식(Form)의 세 가지 요소로 구성된다. 이 세 가지 요소는 정보디자인을 위해 반드시 포함 되어야 하는 기본 요소이면서 목적하는 의도에 맞춰 방법적으로 구사하고 조합할 수 있는 유기성을 가지고 있으며, 이러한 성질을 이용하여 내용, 구조, 형식을 유기적으로 조정하면 어떠한 수준의 조직화와 컨트롤이 가능하다는 것을 확인할 수 있다[12].

2.2.3 정보 시각화 방법

Nathan Yau[13]의 저서 Visualize This에서는 정보 시각화 방법을 시간, 분포, 관계, 비교, 공간을 기준으로 분류하고 있으며, 그의 저서에서 제시된 차트와 그래프의 쓰임새를 바탕으로 정리한 정보 시각화 방법은 아래 도표와 같다.
Table 1[13].에서 보다시피, 5가지 정보 시각화 방법을 이용하면 통용되고 있는 대부분의 차트와 그래프 유형을 분류할 수 있으며, 각 기준별 시각화 방법의 특징은 다음과 같다.

① 시간 시각화
: 시간에 따라 진행되는 변화 또는 트렌드를 추적하는 데 주로 사용하며, 시간의 전후 관계를 파악하면 값의 의미를 더욱 명확하게 이해할 수 있음
② 분포 시각화
: 분포 시각화에서 가장 중요한 것은 분포 정도이며, 분포 데이터들은 부분을 전부 합하면 1 또는 100%가 되므로, 전체 관점에서 부분 간 분포 비율 보여줌
③ 관계 시각화
: 데이터 간의 상관관계를 알게 되면 특정 값의 변화를 통해서 다른 값의 변화를 예측할 수 있으므로, 여러 변수 간의 상관관계 표현을 위해 활용함
④ 비교 시각화
: 여러 변수들의 데이터 비교가 가능하며, 변수들 간의 상대적 가치 비교, 집단적 성향 및 유사도 등을 표현함
⑤ 공간 시각화
: 지도상의 한 위치를 다른 위치와 비교하여 표현할 수 있으며, 하나의 지도는 시간상의 한 순간을 반영하고 있으나 여러 장의 지도를 이용하면 여러 시간의 표현이 가능함

Table 1. Information visualization method[13]

Division	Key visualization methods
Time	Bar graph, stacked bar graph, point graph
Distribution	Pie chart, donut chart, tree map, cumulative continuous graph
Relation	Scatter plot, bubble chart, histogram
Compare	Heat map, star chart, parallel coordinate system, multidimensional scaling
Space	Map mapping

각각의 시각화 방법들은 표현하고자 하는 대상 정보의 내용과 목적에 따라 적절한 유형을 선택하여 시각화를 구현할 수 있으며, 대규모 네트워크에서의 효과적 보안 상황 인지를 위한 시각화 방법으로는 대상들 간의 위치적 특성을 고려한 공간 시각화, 보안성 상태의 비교 시각화, 상관관계를 통한 변화 예측 등이 필요함을 알 수 있다.

2.2.4 정보 시각화 표현 요소

정보 시각화 분야의 전문가인 Jacques Bertin은 명도(value), 색상(color), 질감 (texture), 형태(shape), 위치(position), 방향(orientation), 크기(size)의 7가지 요소[14]를 정보 시각화 표현을 위한 요소로 정의 하였고, 각 요소들의 주요 속성은 아래와 같다.

① 명도
: 명도는 그 값에 따라 구체적인 위계질서를 가지므로, 이러한 속성을 적용해 단계적 특성이나 상태를 표현한다[14]. 명도의 높고 낮음은 색상보다 명시성에 더 큰 영향을 주므로 사용자는 명도 대비를 쉽게 인지할 수 있다.

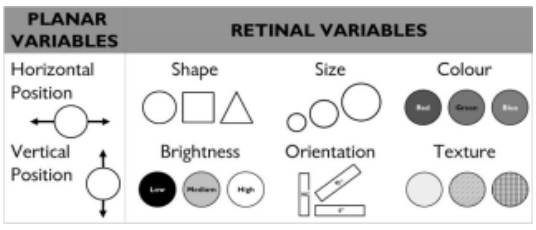

Fig. 2. Jacques Bertin's Visual variables[15]

② 색상
: 색상은 각 정보를 특성별로 구분하기에 유용하며[14], 색상 변화로 순서와 위계를 나타내기도 하고 핵심이 되는 데이터를 색의 특성으로 강조하기도 한다[5]. 중요한 요소에 색상 하나를 적용하면 정보 탐색에 걸리는 시간을 크게 단축할 수 있지만, 색상이 7개를 넘어가게 되면 정보를 탐색하는데 어려움이 생기고[16], 정보 전달 기능이 저하될 수 있다[17]. 색상은 수치 표현에는 적합하지 않다.

③ 질감
: 정보 표현을 위한 2차원적 형태에서의 질감은 촉감이 아닌, 우리 눈에 보이는 느낌으로 시각을 통해 촉감을 불러일으키는 시각적 질감을 의미한다[5]. 동일한 색과 형태에서 질감을 다르게 하면 시각적으로 강조 효과를 줄 수 있다.

④ 형태
: 특정 정보를 형태적 요소로 해석한 후 구체적 이미지로 표현한 것으로, 형태를 이용하면 설명적, 상징적인 정보를 전달할 수 있게 된다[18]. 형태를 구분하는 것은 색상이나 크기의 인지에 비해 어려우며, 형태만으로 큰 대비 효과를 주기가 어려우므로 색상이나 크기 등의 요소와 같이 활용해야 한다.

⑤ 위치
: 위치를 활용한 표현은 조형 요소 간의 상대적인 관계에 의해 내용이 전달될 수 있도록 하는 것으로, 위치 변수는 정보의 이해에 매우 중요한 역할을 하게 된다[18]. 크기와 함께 정량적 표현이 가능하며, 정보의 상하구조를 효과적으로 전달할 수 있다.

⑥ 방향
: 사용자 시선의 움직임과 같은 방향에 의한 정보 시각화는 주로 사건의 진행이나 물리적 현상의 진행 방향을 그래프나 다이어그램 등으로 표현한다[19].

⑦ 크기
: 크기는 가장 널리 이용하는 시각 표현 중 하나다. 크기를 이용하면 영역에 대한 정량적 표현이나 상태 표현이 가능해 한 눈에 정보 간 특성을 인지할 수 있게 된다[14]. 크기는 순서로 구분할 수도 있기에, 양과 중요도를 표현하는데 유용하게 사용할 수 있다.

위와 같이 7가지 시각화 표현 요소의 속성을 살펴본 결과, 명시성이 높은 요소인 명도와 색상, 우선순위의 표현과 강조 효과가 있는 요소인 색상과 크기, 상대적 관계 표현과 네트워크의 물리적 위치 파악이 가능한 요소인 위치 등은 네트워크에서의 보안 상황 인지 효과 향상에 적합한 표현 요소임을 알 수 있다.

2.3 보안 시각화 관련 연구

데이터 시각화, 정보 시각화라는 개념과 함께 보안 분야에서의 시각화 역시 이미 오래전부터 지속적으로 연구되고 있는 분야이다. 보안 시각화 연구는 보안상의 특성이나 시각화 목적에 따라 다양하게 구분되어 질 수 있다.

Hadi Shiravi 외[20]의 네트워크 보안을 위한 시각화 시스템 조사 연구에 따르면, ① Host/Server Monitoring, ② Internal/External Monitoring, ③ Port Activity, ④ Attack Patterns, ⑤ Routing Behavior 의 5가지 사용 유형에 따라서 보안 시각화를 분류하였다. 각 시각화 방안은 시각화 기술과 데이터 소스의 유형에 따라 다양한 형태의 시각화 시스템으로 구현될 수 있음을 보여주고 있다.

장범환 등[9]에 의하면, 네트워크 보안 상황인지를 위한 보안 이벤트 시각화 기술에는 크게 네트워크의 패킷 또는 트래픽 정보를 표현하여 이상 상황을 판단하는 것과, 보안장비들에서 발생하는 보안 경보를 표현 및 분석 하는 기술이 있다. 이는 대상 이벤트의 종류에 따른 분류 방식으로 각각의 장단점을 살펴보면, 네트워크 트래픽 시각화의 경우 알려지지 않은 공격 패턴 검출에 용이하지만 방대한 이벤트를 처리해야 하는 단점이 있으며, 보안 경보 시각화의 경우에는 여러 보안 상황을 표현할 수 있으나 알려지지 않은 공격을 탐지하는 데에는 한계가 있다고 한다.

박재범 등[4]은 네트워크 보안 상황 인지를 위한 여러 가지 유형의 시각화 시스템들을 보안 상황 인지의 '이해'와 '식별'의 관점에서 분석하였으며, 각 시각화 시스템들의 장점을 종합한 결과를 살펴보면 ① 하나의 화면에서 전체 네트워크 상황을 관찰 할 수 있도록 하여 '식별'에 도움을 주며, ② 도형, 색상, 명암을 활용하여 '식별'과 '이해'를 쉽게 하고, ③ 기본 화면에 보여주는 정보를 최소화 하여 '식별'을 효과적으로 하되 ④ '이해' 단계를 위하여 필요시 더욱 상세한 정보를 얻을 수 있는 단계적 시각화를 제공한 점 등

으로 요약하였다.

이동건 등[8]은 VAST Challenge 2012 우수 연구들에서 제시하는 시각화 방법과 보안과 관련하여 여러 분야에서 연구되고 있는 다양한 시각화 연구들을 살펴본 결과, 기존 연구들에서는 위치정보, parallel coordinates 등 다양한 시각화 전략 또는 도구들이 사용된 것을 확인 할 수 있었지만, 다수의 연구들이 다양한 시각화 요소 중 형태적인 파악을 통한 시각화에 많이 집중되어 있음을 알 수 있다고 분석하였다.

2.4 효과적 정보 시각화 평가기준 선정을 위한 연구

에드워드 터프티(Edward Tufte)[16]는 7가지 정보 시각화의 원칙으로 시각적 비교의 강화, 인과관계의 표현, 다중 변수의 표시, 텍스트·그래픽·데이터를 한 화면에 조화롭게 배치하는 화면 구성, 콘텐츠의 질과 연관성 및 진실성 확보, 시간이 아닌 공간에 따른 배치 등을 제시하였다.

오병근 외[5]는 정보 시각화의 효과로 정보의 직관적 이해, 동시에 많은 데이터를 차별적으로 제시, 어려운 지각적 추론 가능, 정보에 감성을 부여하여 흥미를 유발, 문자보다 친근하고 쉽게 접근, 정보들의 관계와 차이를 명확하게 표현, 정보의 입체적 표현(위계) 등을 제시 하였다.

마이클 윌슨(Micheal Wilson) 외[21]는 흥미유발, 사용자 필터링 기능, 읽기 쉽고 식별하기 편한 시각적 구조와 계층 형태, 목적에 맞는 메타포 활용, 메시지 강조, 사용자의 정보 구성 통제, 일관성 등을 시각 디자인 원칙으로 제시하였다.

위에서 언급한 국내·외 시각화 전문가들이 제시한 시각화 관련 원칙과 효과 등에 대한 연구를 바탕으로 정보 시각화 관련 특성을 비교·분석한 결과는 Table 2.와 같다. 에드워드 터프티[16], 오병근[5], 마이클 윌슨[21]이 제시하는 시각화 원칙을 보안 시각화의 관점에서 검토하여 총 13개의 원칙을 도출하였다. Table 2.는 좌의선[17]이 제시한 효과적 시각화 평가 기준을 일부 참고하였으나, 도출된 기준 원칙의 수와 비교 결과에서 차이가 있음을 밝혀둔다.

Table 2.를 살펴보면, 총 13개 원칙 중 9개의 원칙을 효과적 정보 시각화의 평가 요소로 선별한 것을 알 수 있다. 해당 요소는 선행연구 결과를 바탕으로 도출된 여러 원칙들 중에서 공통적으로 언급된 '명확성', '직관성', '상관관계', '다중변수', '화면구성', '콘텐츠', '계층표현'의 7가지 원칙을 우선 선별하고, 보안 시각화 관련 연구 결과를 토대로 보안 상황 인지의 특성을 고려하여 '추론가능성', '확장성'을 추가로 선별하였다. 이 과정에서 공통으로 선택된 '흥미유발'과 '메타포'의 경우 정보 디자인(인포그래픽) 평

Table 2. Comparison of effective information visualization principles[17]

Principle	Edward Tufte [16]	Byungkeun Oh [5]	Micheal Wilson [21]	frequency	Selection
Clarity	V	V	V	3	O
Intuitiveness	V	V	V	3	O
Correlation	V	V		2	O
Multiple variable	V	V		2	O
Screen composition	V	V	V	3	O
Contents	V		V	2	O
Hierarchical representation		V	V	2	O
Possibility of reasoning		V		1	O
Scalability			V	1	O
Interesting		V	V	2	X
Metaphor		V	V	2	X
Quantitative property	V			1	X
Communication			V	1	X

가에 주로 적용되는 항목으로 보안 시각화의 효과성 평가에는 해당 요소를 반영 하지 않았다.

2.5 선행 연구와의 차이점

앞에서 살펴본 바와 같이 기존의 보안 시각화 관련 연구들은 시각화의 일부 구성 요소들을 적용하여 트래픽의 이상, 보안 장비의 경보, 공격 패턴 발생 등 특정 보안 위협 또는 상황을 중점적으로 표현하는 시각화에 집중하였고, 탐지 여부를 중심으로 그 효과성을 입증하였다. 이러한 시각화 방안들은 실제 보안 업무에 적용 시 여러 변수들로 인하여 그 효과가 충분히 입증되지 못하는 경우가 발생하는데, 이는 시각화의 목적 및 대상 등에 따라 시각화 구현에 적용된 특정 구성 요소의 효과에 차이가 있음을 시사한다.

본 연구는 특정 시각화 시스템을 제시하는 것이 아닌, 시각화 시스템의 구현 과정에서 구현 목적과 대상, 상황 인지 특성 등을 고려하여 주요 시각화 요인을 선정하는 보안 시각화 효과성 결정 모델을 제시한다는 점에서 다른 연구들과의 차별점이 있다.

다음 장에서는, AHP 기법을 이용하여 효과적 보안 시각화를 위한 평가 요인을 선정하고, 사용자 유형에 따른 각 요인별 중요도를 평가하여 주요 우선순위를 도출함으로써, 보안 상황 인지 효과의 향상을 위한 시각화 요인과 대안을 제시하고자 한다.

III. 효과적 보안 시각화를 위한 요인 분석

이번 장에서는 선행 연구를 바탕으로 '보안 상황 인지 효과 향상을 위한 시각화(이하, 효과적 보안 시각화)' 평가기준을 선정·정의하고, AHP(Analytic Hierarchy Process) 기법을 적용하여 중요도 평가를 수행하며, 주요 시각화 요인과 대안을 최종 선정함으로써 효과적 보안 시각화 방안의 기틀을 마련하고자 한다.

3.1 효과적 보안 시각화 방안 결정을 위한 방법론

AHP는 Satty[22]가 개발한 의사결정 기법으로, 복수의 대안에 대한 복수의 평가기준이 존재하는 다기준 의사결정(MCDM : Multiple Criteria Decision Making) 문제를 해결하기 위한 대표적인 기법으로, 다양한 유형의 의사결정 문제에 폭넓게 활용되어 왔다[23]. 본 연구에서 효과적 보안 시각화를 위한 주요 요소의 선정에 활용하는 AHP는 목표, 평가요인, 대안으로 이루어지는 계층 모델을 정의하고, 쌍대비교(pairwise comparison) 방식을 통해 각 계층별 의사결정 요인들 간의 중요도를 평가

Table 3. Effective Security Visualization Evaluation Criteria

Criteria	Sub Criteria	Definition
Expression method	Clarity	When presenting a lot of data at the same time, it is clearly expressed so that the user can easily recognize it.(discrimination)
	Intuitiveness	Express to intuitively understand the information provided (emphasis)
	Harmonic	To place text, graphics, and data on one screen in a harmonious
Commnuni-cation contents	Usefulness	Provide useful information for security situation awareness (content - quality of information)
	Diversity	Provide multiple variables on one screen (multiple variables - amount of information)
	Correlation	It is possible to recognize interrelationships based on the information provided (causality, correlation, difference, etc.)
Work efficiency	Priority grasp	It is possible to identify the hierarchy through visualization information (hierarchical representation - prioritization)
	Corresponding prediction	It is possible to predict the response by knowing the relationship between the information provided (possibility of reasoning)
	Extension funtion	It is possible to provide additional information step-by-step in accordance with user's needs in addition to the information provided (Scalability)

하여 최종 우선순위를 도출한다.

3.2 효과적 보안 시각화 방안 도출 절차

AHP는 계층 모델 구축, 쌍대비교, 부분 우선순위 도출, 일관성 평가, 최종 우선순위 도출 및 대안 선택의 5단계로 이루어진다[23]. 각 단계별 주요 수행 내역은 아래와 같다.

① 사전 분석
: 효과적 보안 시각화 평가기준 수립을 위한 선행 연구 및 평가요소 선별
② 평가 요인 선정 및 계층 모델 수립
: 사전 분석 결과를 바탕으로 최종 평가기준(요인) 선정 및 AHP를 이용한 계층 모델의 수립
③ 설문조사 및 유효성 평가
: 앞 단계에서 수립된 AHP 계층 모델을 바탕으로 설문 조사를 실시하고, 결과 데이터의 유효성을 평가
④ 평가 요인별, 대안별 가중치 도출
: 사용자 유형에 따른 3개 그룹으로 나누어 각각의 평가 요인별, 대안별 중요도를 평가하여 최종 가중치를 도출
⑤ 효과적 보안 시각화 방안 선정
: 최종 도출된 결과 값을 이용하여 중요 평가 요인 및 대안을 바탕으로 효과적 보안 시각화 방안을 선정

3.3 효과적 보안 시각화 평가 요인의 선정

앞서 살펴 본 Table 2.에서 선행 연구들의 비교·분석 결과를 바탕으로 효과적 정보 시각화를 위한 총 9가지 평가 요소들을 최종 선별하였다. 이를 근거로 시각화 구성의 3 요소인 형식, 내용, 구조를 상위 평가 기준으로 하여 Table 3.과 같이 효과적 보안 시각화를 위한 평가 기준을 제안한다. 다만, Table 3.에 명시된 각 평가 요인들의 명칭은 Table 2.에서 최종 선별된 9개 원칙의 명칭을 각 요인별 특성과 대표성 및 보안 상황 인지 효과를 고려하여 일부를 수정한 결과이다.

3.4 효과적 보안 시각화 - AHP 계층 모델 정의

선행 연구에서 정리한 정보 시각화의 속성, 정보 시각화 방법, 정보 시각화 표현 요소 등에 대한 내용은 시각화 자체를 구성하는 기본 요소들에 대한 연구 결과이다. 이러한 구성 요소들을 기반으로 구현된 시각화의 효과를 측정하기 위해서는 시각화를 통한 특

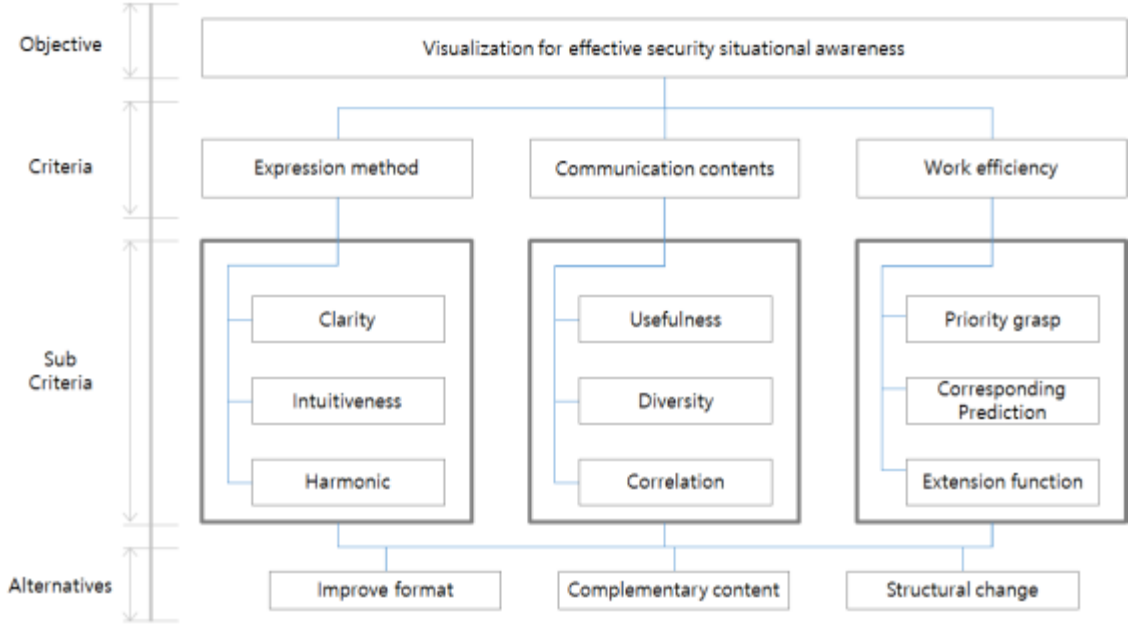

Fig. 3. AHP layer model for effective security visualization

정 목적의 달성 여부 혹은 목표 달성의 정도에 따라 그 효과를 평가할 수 있으므로, 본 연구에서는 보안 상황 인지를 그 목적으로 하여 '인식', '이해', '예측'의 관점에서 시각화의 효과성을 분석하고자 한다. 이에 Table 3.에서 제시된 상위평가요인의 도출 시, 보안 상황 인지 각 단계와의 관련성을 고려하여 인식=표현방식, 이해=전달내용, 예측=업무효율의 세 가지 상위평가기준을 선정하였다. 상위평가기준인 '표현방식'의 하위평가기준은 명확성, 직관성, 조화성이고, '전달내용'의 하위평가기준은 유용성, 다양성, 연관성, '업무효율'의 하위평가기준은 순위파악, 대응예측, 확장기능이다. 또한, 최종 의사결정 사항인 대안은 정보 시각화의 기본속성인 내용, 구조, 형식을 기반으로 내용보완, 구조변경, 형식개선을 선정하였다.

본 연구에서 Table 3.을 바탕으로 구축한 AHP 계층 모델은 Fig. 3.과 같으며, 보안 상황 인지 효과 향상을 위한 시각화 방안의 선정을 목적으로 한다. AHP를 이용한 분석은 3개의 상위평가기준 간 쌍대비교, 각 상위평가기준에 해당하는 하위평가기준 간의 쌍대비교를 통해서 평가 요인별 최종 가중치를 도출하고, 9개 하위평가기준에 대한 3가지 대안 간 쌍대비교를 통해서 각 대안의 우선순위를 도출한다.

3.5 설문 조사 및 유효성 평가

Table 3.의 효과적 보안 시각화 평가기준 및 Fig. 3.의 AHP 계층 모델을 기반으로 설문지를 작성하여 보안 모니터링 업무 관리자 및 운영자, 보안 전문가로 구성된 3개 유형의 사용자 그룹을 대상으로 9점 척도를 이용한 쌍대비교 평가 방식의 설문지를 배포하고 회수하였다.

쌍대비교를 이용한 평가 방식의 경우, 도출된 가중치가 논리적으로 일관성을 유지하는지를 검증하는 것이 중요하다. 이에 Saaty[22]가 제시한 '일관성 비율(CR : Consistency Ratio)'을 사용하여 설문 결과의 유효성을 판단한다. Saaty[22]는 일관성 비율이 0.1 이하일 때 쌍대비교행렬이 일관성이 있다고 하였다. 설문 결과, 일관성 비율이 0.1 미만일 경우 일관성을 유지한다고 판단하여 분석대상에 포함하고, 일관성 비율이 0.1 이상인 설문의 경우에는 일관성이 결여되어 합리적 판단에 적합하지 않으므로 분석대상에서 제외하였다[24]. 그 결과, 회수된 24부 중 일관성 비율이 0.1 미만으로 평가된 설문은 총 20부 이다. 3개 유형의 사용자 그룹 기준으로는 관리자 8부, 운영자 8부, 보안 전문가 4부가 유효한 설문으로 분류되었다. 복수의 설문 분석 및 평가 시에는 AHP의 특성인 역수성 유지를 위해 기하평균(geometric mean)을 사용하는 것이 일반적이며, 본 연구에서는 설문의 분석 및 평가를 위해 Expert Choice 2000 교육용 소프트웨어를 이용하였다.

3.6 평가 요인별, 대안별 우선순위 도출

Fig. 3.의 AHP 계층 모델을 적용하여 설문을 수행하고, 일관성 비율 0.1 미만의 유효한 설문지를 토대로 결과를 분석하였다. 설문 결과는 총 3개의 그룹으로 나누어 분석을 실시하였다. 그룹의 구성은 사용자 유형에 따라 분류하였으며, 'Group1'은 보안 모니터링 업무 관리자, 'Group2'는 보안 모니터링 업무 운영자, 'Group3'은 보안 전문가(컨설턴트)로 구성하여 사용자 유형에 따른 효과적 보안 시각화의 요인을 분석하였다.

Table 4.는 AHP 계층 모델을 이용하여 쌍대비교 분석을 통해 도출된 결과를 사용자 그룹 기준으로 정리하여 각 상위, 하위 평가 요인별 가중치와 최종 가중치 및 우선순위를 도출한 결과이다. 각 평가 요인별 최종 가중치는 상위 평가 요인의 가중치와 해당 하위 평가 요인별 가중치의 곱으로 산정하였다. 최종 가중치는 결과적으로 상위 평가 요인별 가중치가 각 해당 하위 평가 요인의 가중치에 영향을 미치게 되므로 각각의 하위 평가 요인별 최종 가중치를 이용하여 전체 하위 평가 요인별 우선순위를 도출하게 된다.

Table 5.는 각 사용자 그룹을 기준으로 Table 4.에서 도출된 평가 요인별 최종 가중치를 바탕으로, 각 하위 평가 요인별로 3가지 대안의 우선순위를 산출한 결과이다. 이 종합 산출 결과들을 토대로 상위 평가 기준 및 각 사용자 그룹 단위로도 대안의 우선순위를 도출 할 수 있다. 다음은 Table 4.와 Table 5.를 토대로 각 사용자 그룹별 분석 결과를 정리한 내용이다.

3.6.1 그룹 1 - 관리자 그룹 분석 결과

Table 4.의 Group1을 살펴보면, 상위평가기준의 중요도는 전달내용(0.395), 업무효율(0.368), 표현방식(0.237) 순으로 분석되었다.

그 중 상위평가 가중치가 높은 순으로 하위평가기준의 가중치를 살펴보면, 첫 번째 전달내용은 연관성

Table 4. Weights by Criteria

division	Criteria	Weight	Sub Criteria	Weight	Final Weight	Priorities
Group1 (Manager)	Expression method	0.237	Clarity	0.450	0.107	5
			Intuitiveness	0.371	0.088	6
			Harmonic	0.179	0.042	8
	Commnunication contents	**0.395**	**Usefulness**	**0.377**	**0.149**	**3**
			Diversity	0.102	0.040	9
			Correlation	**0.521**	**0.206**	**1**
	Work efficiency	0.368	Priority grasp	0.338	0.124	4
			Corresponding prediction	**0.470**	**0.173**	**2**
			Extension function	0.193	0.071	7
Group2 (Operator)	**Expression method**	**0.462**	**Clarity**	**0.530**	**0.245**	**1**
			Intuitiveness	**0.374**	**0.173**	**3**
			Harmonic	0.096	0.044	8
	Commnunication contents	0.161	Usefulness	0.481	0.077	5
			Diversity	0.106	0.017	9
			Correlation	0.413	0.066	6
	Work efficiency	0.378	**Priority grasp**	**0.545**	**0.206**	**2**
			Corresponding prediction	0.288	0.109	4
			Extension function	0.167	0.063	7
Group3 (Consultant)	Expression method	0.303	**Clarity**	**0.584**	**0.177**	**2**
			Intuitiveness	0.179	0.054	7
			Harmonic	0.237	0.072	6
	Commnunication contents	0.287	**Usefulness**	**0.524**	**0.150**	**3**
			Diversity	0.102	0.029	9
			Correlation	0.375	0.108	5
	Work efficiency	**0.410**	Priority grasp	0.363	0.149	4
			Corresponding prediction	**0.530**	**0.217**	**1**
			Extension function	0.108	0.044	8

(0.521), 유용성(0.377), 다양성(0.102) 순으로 나타났으며, 두 번째 업무효율은 대응예측(0.470), 순위파악(0.338), 확장기능(0.193) 순으로 평가되었고, 세 번째 표현방식은 명확성(0.450), 직관성(0.371), 조화성(0.179) 순으로 도출되었다.

Table 4. Group1의 각 평가 요인별 최종 가중치 산정 결과를 살펴보면 연관성, 대응예측, 유용성이 상위 3개의 평가 요인으로 분석되었다.

Table 5. Group1 관점에서의 대안의 최종 우선순위는 내용보완(0.421), 구조변경(0.299), 형식개선(0.280)으로 도출되어 내용보완이 가장 적합한 대안으로 평가되었으며, 상위 3개 평가 요인인 연관성, 대응예측, 유용성에 따른 대안도 모두 내용보완이 적합한 것으로 나타났다.

3.6.2 그룹 2 - 운영자 그룹 분석 결과

Table 4.의 Group2를 살펴보면 상위평가기준의 중요도는 표현방식(0.462), 업무효율(0.378), 전달내용(0.161) 순으로 분석되었다.

그 중 상위평가 가중치가 높은 순으로 하위평가기준의 가중치를 살펴보면, 첫 번째 표현방식은 명확성(0.530), 직관성(0.374), 조화성(0.096)순으로 평가되었고, 두 번째 업무효율은 순위파악(0.545), 대응예측(0.288), 확장기능(0.167) 순으로 나타났으

Table 5. Weights by alternatives

Criteria	Sub Criteria	Group1 (Manager)				Group2 (Operator)				Group3 (Consultant)			
		Final Weight	Alternatives			Final Weight	Alternatives			Final Weight	Alternatives		
			Format	**Contents**	Structure		**Format**	Contents	Structure		Format	Contents	**Structure**
Expression method	Clarity	0.107	0.036	0.039	0.032	**0.245**	0.094	0.054	**0.097**	**0.177**	0.025	0.075	**0.077**
	Intuitiveness	0.088	0.031	0.036	0.020	**0.173**	**0.094**	0.027	0.052	0.054	0.015	0.013	0.026
	Harmonic	0.042	0.018	0.013	0.011	0.044	0.015	0.010	0.019	0.072	0.032	0.021	0.019
	Total	0.237	0.086	0.088	0.063	0.462	0.203	0.092	0.168	0.303	0.072	0.109	0.122
Commnunication contents	Usefulness	**0.149**	0.026	**0.090**	0.033	0.077	0.018	0.039	0.020	**0.150**	0.017	**0.101**	0.033
	Diversity	0.040	0.009	0.022	0.010	0.017	0.004	0.008	0.005	0.029	0.003	0.014	0.012
	Correlation	**0.206**	0.043	**0.087**	0.076	0.066	0.007	0.028	0.032	0.108	0.017	0.039	0.052
	Total	0.395	0.078	0.199	0.118	0.161	0.029	0.075	0.057	0.287	0.037	0.153	0.097
Work efficiency	Priority grasp	0.124	0.051	0.030	0.044	**0.206**	**0.078**	0.062	0.065	0.149	0.046	0.025	0.077
	Corresponding prediction	**0.173**	0.045	**0.084**	0.044	0.109	0.036	0.041	0.032	**0.217**	0.023	**0.099**	0.096
	Extension function	0.071	0.021	0.021	0.029	0.063	0.015	0.019	0.029	0.044	0.006	0.017	0.021
	Total	0.368	0.117	0.134	0.117	0.378	0.129	0.122	0.127	0.410	0.075	0.140	0.194
Final weight of alternatives			0.280	**0.421**	0.299		**0.361**	0.288	0.351		0.185	0.402	**0.414**
Final priority of alternatives			3	**1**	2		**1**	3	2		3	2	**1**

며, 마지막 전달내용은 유용성(0.481), 연관성(0.413), 다양성(0.106) 순으로 도출되었다.

Table 4. Group2의 각 평가 요인별 최종 가중치 도출 결과를 살펴보면 명확성, 순위파악, 직관성이 상위 3개의 평가 요인으로 분석되었다.

Table 5. Group2 관점에서 대안의 최종 우선순위는 형식개선(0.361), 구조변경(0.351), 내용보완(0.288)으로 도출되어 형식개선이 가장 적합한 대안으로 평가되었으며, 상위 3개의 평가 요인을 기준으로 각 요인별 대안을 살펴보면 명확성은 구조변경, 순위파악과 직관성은 형식개선이 적합한 대안으로 도출되었다.

3.6.3 그룹 3 - 전문가 그룹 분석 결과

Table 4.의 Group3을 살펴보면 상위평가기준의 중요도는 업무효율(0.410), 표현방식(0.303), 전달내용(0.287) 순으로 분석되었다.

상위평가기준의 가중치 순서별로 하위평가기준의 가중치를 살펴보면, 첫 번째 업무효율은 대응예측(0.530), 순위파악(0.149), 확장기능(0.044) 순으로 평가되었고, 두 번째 표현방식은 명확성(0.584), 조화성(0.237), 직관성(0.179)순으로 나타났으며, 마지막 전달내용은 유용성(0.524), 연관성(0.375), 다양성(0.102) 순으로 도출되었다.

위 Table 4. Group3의 각 평가 요인별 최종 가중치 도출 결과를 살펴보면 대응예측, 명확성, 유용성이 상위 3개의 평가 요인으로 분석되었다.

Table 6. Factor analysis results by user group

Division	Criteria (Top1)	Sub Criteria (Top3)	Priority alternatives by Sub Criteria
Group1 (Manager)	Communication contents	Correlation	Complement the contents
		Corresponding prediction	Complement the contents
		Usefulness	Complement the contents
Group 2 (Operator)	Expression method	Clarity	Change of structure
		Priority grasp	Improvement of format
		Intuitiveness	Improvement of format
Group 3 (Consultant)	Work efficiency	Corresponding prediction	Complement the contents
		Clarity	Change of structure
		Usefulness	Complement the contents

Table 5. Group3 관점에서의 대안의 최종 우선순위는 구조변경(0.414), 내용보완(0.402), 형식개선(0.185)으로 도출되어 구조변경이 가장 적합한 대안으로 평가되었으며, 상위 3개의 평가 요인을 기준으로 각 요인별 대안을 살펴보면, 대응예측과 유용성은 내용보완, 명확성은 구조변경이 적합한 대안으로 도출되었다.

3.7 분석 결과의 요약

본 연구에서는 보안 시각화 방안의 개선을 위해, AHP 기법을 활용하여 효과적 보안 상황 인지를 위한 시각화 요인을 분석하였다. 요인 분석은 설문을 통해 총 3개 그룹으로 나누어 수행하였으며, Table 6.은 각 사용자 그룹별 주요 분석 내용을 요약한 결과이다. Table 6.의 Group1, Group2, Group3을 살펴보면 각 사용자 그룹별로 도출된 주요 평가 요인 및 대안이 서로 다르게 나타난 것을 확인할 수 있다. 이와 같은 결과를 보안 상황 인지와 연결하여 분석해 보면, 첫 번째 관리자 그룹은 전달내용을 효과적 시각화의 주요 평가 요인으로 선정하였으며, 이를 통해 관리자 그룹에서 시각화를 통해 얻고자 하는 주요 효과가 보안 상황의 '이해'에 중점을 두고 있음을 알 수 있다. 두 번째 운영자 그룹은 표현방식을 주요 평가 요인으로 선정하였으며, 연관된 하위평가 기준들의 Top3 항목을 살펴보면 명확성, 순위파악, 직관성으로 이는 보안 상황의 '인식(식별)'이 운영자 그룹에서 가장 중요한 요인임을 알 수 있다. 세 번째 보안 전문가(컨설턴트) 그룹에서는 업무효율이 주요 평가 요인으로 도출되었으며, 대응예측이 가장 높은 가중치의 하위평가 요인으로 분석되어, 보안 상황 인지 단계 중 '예측'이 전문가 그룹에 가장 효과적인 시각화 요인임을 알 수 있다.

위의 분석 결과에 따르면 보안 상황 인지 효과의 향상을 위한 시각화 요인은 관련 업무 사용자의 유형에 따라서 상황 인지의 특정 단계와의 관련성이 매우 높음을 알 수 있으며, 이를 통해 각 사용자 유형에 따른 별도의 시각화 방안이 필요함을 시사하고 있다.

3.8 보안 시각화 요인 및 대안 적용 예시

Table 7.은 다양한 시각화 이미지들을 제공하고 있는 'SecViz[25]'와 'D3.js[26]'에서 몇 가지 시각화 사례들을 분석하여, 각 사례별로 시각화를 구성하는 요소인 형식(표현요소)과 구조(방법), 그리고 이

Table 7. (Security) Visualization case analysis [25][26]

Case	Alternatives		Sub Criteria
	Format	Structure	
1	value position	Space	Intuitiveness Correlation Priority grasp
2	value	Compare	Clarity Intuitiveness Correlation Priority grasp
3	color shape position size orientation	Compare	Clarity Intuitiveness Usefulness Diversity Correlation Corresponding -prediction

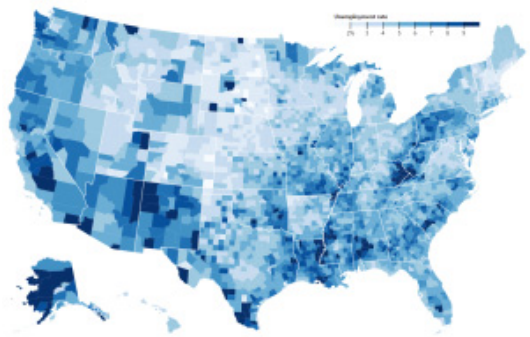

Fig. 4. Visualization Case1.[27]

와 관련된 시각화의 평가 요인을 정리한 결과이다.

보안 시각화의 효과성 향상을 위한 평가 요인 및 대안의 중요도 분석 결과에 따라 결정된 시각화 방안이 실제 시각화 시스템의 구현 시에 어떻게 적용되고 영향을 미칠 수 있는지, Table 7.의 분석 결과를 바탕으로 다음의 각 사례에 적용되어 있는 시각화 구성 요소(대안)와 관련된 시각화 평가 요인의 상호 관계를 살펴보고자 한다.

Fig. 4.[27]의 Case1은 명도와 위치의 형식을 이용하여 공간(지도) 구조 위에 시각화를 구현한 사례이다. 이 경우, 명도를 통해 위계·상태(순위)를 표현하였고, 공간의 특성을 통해 지역별 분포를 쉽게 인식할 수 있으며, 이를 통해 지역별 순위 분포를 파악하고, 지역 간 혹은 상태별 연관성을 인지할 수 있다. 다만, 지도를 이용한 특성으로 인해 실제 지역의 물리적 크기에 따라 대상 지역을 구분하기 때문에, 대상 식별을 위한 명확성 표현에는 적합하지 않다.

Fig. 5.[28]의 Case2는 Case1과 동일하게 명

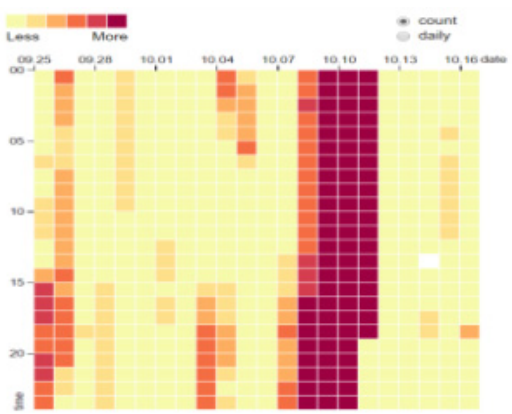

Fig. 5. Visualization Case2.[28]

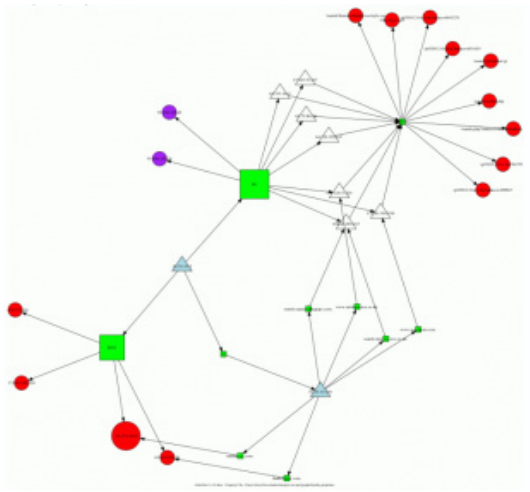

Fig. 6. Visualization Case3.[29]

도와 위치 형식을 이용하고 있으나, 비교의 특성을 갖는 히트맵 구조 위에 시각화를 구현한 사례이다. 히트맵은 일정 간격의 크기로 된 트리맵 구조로 각 표현 대상의 식별에 용이하여 명확성 확보에 적합하다. Case2 는 Case1 과 마찬가지로 명도를 이용한 순위 표현이 가능하며, 시간에 따른 분포 특성을 통해 연관성 파악이 가능하다.

Fig. 6.[29] Case3은 색상, 형태, 위치, 크기, 방향의 5가지 형식을 이용하고 있다. 형태를 이용하여 출발지와 목적지를 구분하고, 색상을 이용하여 공격 유형을 표현하며, 위치 및 방향을 이용하여 네트워크 내에서의 특성 및 상대적 관계 파악을 용이하게 하였다. 이러한 복합적 형식이 다차원 구조 위에 구현되어 있으며, 다수의 요소로 복잡하게 구현되어 있으나, 명확성, 직관성, 유용성, 다양성, 연관성 및 대응예측이 가능하다. 다만, 다수의 공격 발생 시 공격 패턴의 증가로 명확성과 직관성 등이 저하될 수 있다.

위와 같은 시각화 사례별 분석 결과를 통해 시각화의 구성 요소(대안)들이 시각화에 미치는 영향을 살펴봄으로써, 시각화의 평가 요인과 대안 간의 관련성을 미리 예측해 볼 수 있다.

IV. 결론 및 한계

4.1 결론

시각화는 내용(content)과 구조(Structure), 형식(Form) 이라는 세 가지 속성을 이용하여 목적에 맞게 조직화하는 과정이라고 할 수 있다[12]. 때문에, 정보를 어떻게 조직화 하는가에 따라서 정보를 바라보는 관점이 달라지고, 이러한 관점의 차이에 따라서 정보가 전달하는 메시지는 달라지게 마련이다. 이는 곧, 보안 상황의 인지에 있어서 관련 정보의 조직화 방법에 따라 정보에 대한 '인식(식별)'과 '이해'의 효과가 달라지고, '인식(식별)'과 '이해'의 관점에 따라 '예측'의 방향이 달라지므로, 결과적으로 의사결정에 중요한 영향을 미치게 됨을 의미한다.

대규모 네트워크와 같은 복잡한 환경에서의 보안 상황 인지는, 대상의 규모와 복잡도, 사용자 유형 및 상황 인지 단계별 특성들이 복합적으로 작용하기에 시각화의 목적과 시각화를 구성하는 요인들에 따라서 보안 상황 인지 효과가 크게 달라질 수 있다. 이에, 본 연구에서는 사용자 유형과 보안 상황 인지 단계에 따른 특성을 고려하여 효과적 보안 시각화를 위한 요인과 요인별 대안의 선정이 가능하도록 AHP 계층 모델을 설계하였다. 기존의 보안 시각화 연구들은 대부분 특정 보안 위협이나 이벤트 탐지를 위한 시각화 표현에 초점을 맞추어 개별적인 요인 분석 결과에 따라 구현되었으며, 이러한 경우 여러 가지 환경 변수에 따라 해당 시각화의 효과성이 충분히 발효되지 않는 경우가 발생할 수 있다.

본 연구에서는 시각화의 구현에 있어서 사용자의 유형과 상황 인지 단계에 따른 시각화의 목적을 고려한 시각화 요인의 분석이 가능하도록 보안 시각화 효과성 결정 모델을 제시하고, 시각화의 목적에 적합한 주요 요인과 해당 요인의 구현을 위한 시각화 구성 요소 간의 균형점을 찾을 수 있도록 의사 결정을 도움으로써, 시각화를 통한 보안 상황 인지 효과를 향상 할 수 있는 방안을 제시하였다.

4.2 한계 및 향후 발전 방향

본 연구에서는 효과적 시각화 방안에 대한 실제 시스템을 구현한 것이 아니라, 요인 분석 결과를 바탕으로 효과성 개선을 위한 시각화 요인(방안)을 제시하는 연구였기에, AHP 계층 모델 설계 시 3계층으로 제한하여 효과적 시각화를 위한 주요 요인과 대안의 중요도만을 분석하였다. 때문에, 시각화의 구성요소인 내용, 형식, 구조와 관련하여 보다 구체적인 시각화 기법들의 제시에 어려움이 있었다. 향후에는, AHP 외에 더 효율적인 의사결정 기법의 적용을 검토하고, 실제 시각화의 구현에 좀 더 구체적인 개선 방안의 제시가 가능할 수 있도록 각 대안을 중심으로 상세 구현 방법 혹은 세부 구성 요소들과의 관련성을 고려하여 추가 연구를 수행한다면 보안 시각화 구현 시 보다 큰 실질적 효과의 향상을 기대할 수 있다.

References

[1] Gwang-sun Choi, "Bigdata Visuali- zation", Korea Society of Computer Information, 21(1), p33-43, Jun. 2013

[2] Mica R. Endsley. "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors, vol. 37, No.1, pp. 32-64. Mar. 1995

[3] A. D'Amico and M. Kocka, "Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned," Proc. of VizSEC'05, IEEE, pp. 107-112, Oct. 2005.

[4] Jea-beom park, "Design and implementation of the honeycomb structure visualization system for the effetive security situational awareness of large-scale networks", Korea Institute of Information Security & Cryptology, 24(6), p1197-1212, Dec. 2014

[5] Byungkeun Oh, "Textbook of Information Design", AhnGraphics, 2008

[6] Jae-Ho Lee, "Decision Support System to Detect Unauthorized Access in Smart Work Environment", Korea Institute of Information Security and Cryptology, 22(4), p797-808, Aug. 2012

[7] Mica R. Endsley, "Situation awareness : State of the art", IEEE, p1-4, 2008

[8] Dong-gun Lee, "Study on security log visualization and security threat detection

using RGB Palette", Korea Institute of Information Security & Cryptology, 25(1), p61-73, Feb. 2015
〔9〕 Beom-Hwan Chang, "Security situation awareness technology using security event visualization", Korea Institute of Information Security & Cryptology, 16(2), p18-25, Apr. 2006
〔10〕 Jisun Lee, "A Study on Visualizing Method and Expression of Information Design for Big Data", Basic Design & Art, 14(3), p261-269, Jun. 2013
〔11〕 Heesook Shin, "Information visualization technology and information expression technology for the visually impaired", Electronics and Telecommunications Trends, 28(1), Feb. 2013
〔12〕 Jinkon Kim, "A Study for Foundation Properties of Information Visualization in Information Design", Digital Design, 9(3), p313-324, Jul. 2009
〔13〕 Nathan Yau, "Visualize This", John Wiley & Sons Inc, P1-358, 2011
〔14〕 Jacques Bertin, Graphics and Graphic Information Processing, Walter de Gruyter, p.205-227, 1981
〔15〕 Jacques Bertin, "Semiology of Graphics: Diagrams, Networks, Maps.", Univ. of Wisconsin Press, Madison, 1983
〔16〕 Alan Cooper, "About Face3 - Interaction design completed with persona", acorn publishing, p461, 2010
〔17〕 Yi Xuan Zuo, "A Study on the Effective Communication of Information Visualization", Digital Design, 14(3), p8-94, Jul. 2014
〔18〕 Eunhee Cho, "Image-based Visualization of Realtime Numeric Data on a Smartphone", Digital Design, 11(4), p91-100, Oct. 2011
〔19〕 Junghyun Lee, "Case study on design of theme park sign system through graphic elements of information visualization", Hanyang University Industrial Design Academy, p23-27, 2009
〔20〕 Hadi Shiravi, "A Survey of Visualization Systems for Network Security", IEEE Transaction on Visualization and Computer Graphics, vol.18, No.8, p1313-1329, Aug. 2012
〔21〕 Michael Wilson&Anthony Conway, "Enhanced Interaction style for User Interfaces", IEEE Computer graphics and Applications. Vol.11 No.2, pp.79-90., 1991
〔22〕 Saaty T. L., "The Analytic Hierarchy rocess," McGraw-Hill, New York, 1980.
〔23〕 Sang-Pil Shin, "An analytic hierarchy process (AHP) approach to selection of implementation mode of mobile office system", Korea Management Engineers Society, 18(2), p105-119, Jul., 2013
〔24〕 Suk-Won Lee, "Decision Making Model for Selecting Financial Company Server Privilege Account Operations", Korea Institute of Information Security & Cryptology, 25(6), p1607-1620, Dec. 2014
〔25〕 SecVIz, http://secviz.org/
〔26〕 D3.js, https://github.com/d3/d3/wiki/Gallery
〔27〕 D3.js, "Choropleth", http://bl.ocks.org/mbostock/4060606
〔28〕 D3.js, "Days-hours Heatmap", http://bl.ocks.org/oyyd/859fafc8122977a3afd6
〔29〕 SecVIz, "Zomvie network activity repre-sentation by Dorothy", http://secviz.org/content/zombie-network-activity-representation-dorothy

〈저자소개〉

이 민 선 (Min-Sun Lee) 정회원
2000년 2월: 수원대학교 전자계산학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 및 개인정보보호 GRC, 보안아키텍처, 네트워크보안, 보안시각화

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
2011년 9월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책