情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

계층분석과정을 이용한 융합보안을 위한 물리 보안 이벤트 활용: 정보 보안 중심*

강 구 홍,[1†‡] 강 동 호,[2] 나 중 찬,[2] 김 익 균[2]
[1]서원대학교 정보통신공학과, [2]한국전자통신연구원

Utilization of Physical Security Events for the Converged Security using Analytic Hierarchy Process: focus on Information Security*

Koohong Kang,[1†‡] Dongho Kang,[2] Jung Chan Nah,[2] Ikkyun Kim[2]
[1]Dept. of Information and Communication Engineering, Seowon University,
[2]Network System Security Team, ETRI

요 약

최근 물리보안과 정보보안으로 양분화 되어 있는 영역자체가 융합되고 있는 추세이며, 이러한 융합의 중심에 있는 것이 융합보안관제이다. 그러나 이러한 추세에도 불구하고, 융합보안을 위한 이들 두 영역의 보안 이벤트를 어떻게 활용할 것인지에 관한 구체적인 솔루션은 찾아볼 수 없다. 본 논문에서는 물리 보안 이벤트를 활용하여 정보 보안의 효율을 향상시킬 수 있는 정보보안 오브젝트-기반 접근법을 제안한다. 또한, 계층분석과정(Analytic Hierarchy Process)을 이용하여 확장성을 고려한 많은 양의 물리 보안 이벤트의 의미 있는 이벤트 조합을 찾는 체계적인 방법을 제안한다. 특히, 출입통제시스템과 영상감시 시스템에서 발생되는 물리보안 이벤트를 이용해 컴퓨팅 시스템 접근 정보보안 효율성 향상을 위한 구체적인 실현 과정을 기술하였다.

ABSTRACT

Today's security initiatives tend to integrate the physical and information securities which have been run by completely separate departments. That is, the converged security management becomes the core in the security market trend. However, to the best of our knowledge, we cannot find any solutions how to combine these two security events for the converged security. In this paper, we propose an information security object-driven approach which utilizes the physical security events to enhance and improve the information security. For scalability, we also present a systematic method using the analytic hierarchy process finding the meaningful event combinations among the large number of physical security events. In particular, we show the whole implementation processes in detail where we consider the information security object 'illegal computing system access' combined with two physical security devices - access controller and CCTV+video analyzer system.

Keywords: Converged Security, Physical Security, Information Security, Security Event Correlations

접수일(2011년 11월 21일), 수정일(2012년 4월 9일), 게재확정일(2012년 4월 19일)
* 본 논문은 2011년 지식경제부 산업원천기술개발사업(산업시설 정보자산 보호용 공간연동 침입 탐지 및 대응기술 개발)의 위탁과제로 지원된 연구임.
† 주저자, khkang@seowon.ac.kr
‡ 교신저자, khkang@seowon.ac.kr

I. 서 론

보안이란 국가, 개인, 기업의 유.무형 자산 및 인적 자원의 안전과 보호를 의미하며, 보안 산업이란 이를 위한 보안제품을 생산하거나 보안 서비스를 제공하는 산업을 의미 한다[1]. 보안 산업은 출입통제, 주차시설 관리, CCTV, 그리고 영상보안 등 물리적 환경에서 이루어지는 물리 보안(Physical Security) 산업과 오늘날 정보화 사회의 근간을 이루고 있는 컴퓨터와 네트워크를 보호하는 정보 보안(Information Security) 산업으로 양분화 되어 발전되어 왔다. 범죄, 테러, 재난 예방을 위한 물리 보안의 경우, 9.11 테러 이후 테러 및 범죄예방을 위해 스마트카드와 접목한 출입통제시스템과 CCTV를 중심으로 한 영상보안시스템에 대한 수요가 폭발적으로 증가하고 있으며 다양한 위험상황에 보다 효과적으로 대처하기 위해서 이들 물리 보안 장치들은 사고 대응 중심에서 사전 예방 중심으로 진화하고 있다. 뿐만 아니라 단순 영상감시가 아닌 상황인지 기능을 제공하는 영상감시 시스템, 얼굴이나 지문 등으로 사람을 식별하는 바이오인식 등 물리적 보안기술에 대한 관심이 한층 고조되고 있다[3]. 한편, 새로운 정보기술이 등장함에 따라 조직의 정보자산에 대한 위협 역시 다양해지고 있으며, 정보유출 등의 사건/사고에 따른 피해규모는 조직의 존폐에 영향을 줄 만큼 증가하고 있다[4]. 따라서 개인, 기업, 그리고 국가는 자신의 정보와 컴퓨팅 환경을 보호하기 위해서 방화벽, 침입탐지시스템, 안티 바이러스 제품 등 다양한 정보 보안 솔루션들을 구축하고 있다[2].

현재 대부분의 조직들은 물리 보안과 정보 보안이 두 개의 독립적 조직에 의해 운영되고 관리되어 오고 있다. 즉 조직 내 시설 관리부서는 직원 배지(badging process) 관리와 빌딩 내 출입문 관리, 그리고 화재와 CCTV와 같은 재난과 관련된 물리 보안 장치들을 관리한다. 한편 이들 시설 관리부서와는 독립적으로 전산부서는 조직 내 정보보호를 위해 다양한 정보 보안 장치들을 운영하게 된다. 그러나 최근 물리보안과 정보보안으로 양분화 되어 있는 영역자체가 융합되고 있는 추세이며, 이러한 융합의 중심에 있는 것이 융합보안관제이다. 융합보안관제는 출입통제시스템, CCTV 등 개별적으로 운영되고 관리되어 왔던 물리보안영역과 IT 통합보안관제시스템을 하나의 관리범위 안으로 통합함으로써 보안 관리의 체계성을 확보하고 각각의 보안체계의 취약점을 상호 보완함으로써 정보 유출 및 침입사고를 획기적으로 예방, 차단, 차후 추적 등을 가능하게 해준다. 그러나 이러한 융합보안에 대한 필요성과 요구가 매우 활발하게 논의되고 있으나 아직 융합보안을 위한 구체적 표준, 프레임워크, 혹은 개발된 융합 보안 장비를 찾아보기는 불가능한 실정이다. 뿐만 아니라, 융합보안 개념조차 아직 정확하게 하나로 정의되지 못하고 있다. 본 논문에서는 융합보안의 협의의 의미로 사용 되고 있는 '물리 보안 이벤트를 활용하여 정보 보안의 효율을 향상' 시킬 수 있는 구체적인 방법을 제안한다. 즉 물리 보안 장치에서 발생하는 이벤트를 적극 활용할 경우, 정보 보안에서 검출하게 되는 각종 공격의 탐지율과 오탐율을 향상시킬 수 있을 것으로 기대된다.

물리 보안 장치에서 발생하는 매우 다양한 이벤트를 정보 보안에 사용하기 위해서는 이들 물리 보안 이벤트의 조합들을 분석해 정보 보안에 활용될 수 있는 의미 있는 이벤트 조합을 선택해야 한다. 앞에서 언급된 물리 보안 장치들이 발생하게 될 이벤트 수가 n 개라고 가정하면 2^n 개의 이벤트 조합을 고려해야 한다. 따라서 엄청난 수의 이벤트 조합을 고려해야 하기 때문에, 우리는 체계적인 이벤트 상관분석(event correlation analysis)을 통해 의미 있는 이벤트 조합을 선택할 수 있는 방법을 강구하여야 한다. 본 논문에서는 계층분석과정(AHP: Analytic Hierarchy Process) 기법을 이용하여 물리 보안 이벤트의 의미 있는 이벤트 조합을 찾는 방법을 제안한다. 또한 물리 보안 이벤트들의 발생 순서에 따른 이벤트 효과 변화를 반영하기 위해 시간 연관성(temporal correlation)을 나타내는 2진 쌍대 시간 행렬을 제안하였다. 특히 2개의 물리보안 장치를 적용한 구체적인 적용 사례를 보임으로써 제안된 기법의 구현 가능성을 보였다.

서론에 이어, 제2장에서는 정보 보안에 활용된 이벤트 상관분석에 관한 기존 방법과 연구 동기를 기술하고, 제3장에서는 물리 보안 이벤트의 상관분석에 사용할 계층분석과정에 대해 간략히 설명한다. 제4장에서는 본 논문에서 제시하는 융합보안을 위한 정보보안 오브젝트 기반의 물리보안 이벤트 활용 기법을 설명하고, 제5장에서는 물리 보안 장치인 출입통제시스템과 영상감시 시스템에서 발생되는 물리 보안 이벤트를 이용해 서버 컴퓨팅 시스템 접근 정보보안 효율 향상 방안에 대해 구체적인 예를 제시한다. 마지막으로 제6장에서 결론 및 향후 연구 방향에 대해 기술하였다.

II. 연구 배경

2.1 기존 이벤트 연관성 분석(Event Correlation) 기술

이벤트 연관성 분석 기술은 처음에는 비즈니스 성능 관리 혹은 네트워크 장애 관리 분야에서 다양한 형태로 연구되어 왔으나 최근에는 네트워크 보안 관리 및 침입탐지와 같은 다양한 응용분야로 확대되고 있다[5,6]. 정보 보안 산업 분야에서, "엔터티(entities) 사이의 관계를 설정하거나 혹은 발견하는" 것으로 정의되는 연관성 분석 기술은 다양한 발신지로부터 수집되는 정보를 조합하여 위협을 확인하고 분석하는 과정의 효율을 개선하기 위해 사용되고 있다[7,8]. 연관성 분석 기술은 네트워크 보안에 관련된 대량의 이벤트 정보를 운용자가 수작업으로 처리할 수 없는 문제를 해결하기 위한 정보 관리 기술로서 또 한편으로는 독립적으로 발생한 다수의 이벤트 정보 간의 연관 관계를 분석함으로써 보안 침해 사건의 근본적인 원인을 규명하기 위한 지식 창조 프로세스로 적용되고 있는 상황이다. 만약 우리가 이러한 기술을 활용하지 않을 경우, 무수히 많은 네트워크 이벤트로 인하여 정말 의미 있는 중요한 이벤트를 놓치게 된다. 뿐만 아니라 시스템 관리와 로그 파일 분석에서도 이벤트 상관분석 기술이 적용되고 있다. 많은 컴퓨터와 네트워크 장비들은 자신에게서 발생되는 이벤트를 로그로 저장한다. 이렇게 저장된 이벤트들은 특정 운영체계, 응용, 그리고 네트워크 컴포넌트에 따라 고유한 의미를 가지게 된다. 한편, 이들 IT 제품들이 공격을 받게 되면, 이들 이벤트 로그 정보로부터 공격의 원인을 분석해 향후 이들 공격으로부터 안전하게 보호한다.

정보 보안 산업 분야에서 연관성 분석 기술은 이벤트의 발신지에 따라 두 가지, 즉 시간(temporal) 연관성과 공간(spatial) 연관성 분석 기술로 구분된다. 시간 연관성 기술은 일정 시간대에서 이벤트 시퀀스의 연관성을 분석하게 된다. 즉 학습을 통해 정의된 정상적인 이벤트 모델로부터 수집된 이벤트 시퀀스가 얼마나 차이가 나는지를 확인하거나 혹은 이미 잘 알려진 공격들이 가지는 이벤트 시퀀스 규칙(rule)을 확인하게 된다. 학습기반의 시간 연관성 분석 기법은 일반적으로 정상적인 이벤트의 특징들을 학습하게 된다. 이렇게 학습된 정상적인 모델로부터 심각한 변화가 일어나면 침입이 의심되며 다양한 방법으로 공격을 검출하게 된다. 규칙 기반 시간 연관성 기법은 서로 다른 시간대에서 이벤트 시퀀스를 비교할 규칙들을 정의해 둔다. 이러한 이벤트 시퀀스는 정상적인 행위, 혹은 공격 행위에 대해서 정의해 둔다. 공간 연관성 분석 기법은 보안 진단을 위해 다양한 위치에서 발생되는 이벤트 분석 기술에 초점을 맞춘다. 이러한 이벤트들은 다양한 시간대에서 분산되어 발생될 수 도 있다. 연관성 분석 엔진으로 입력되는 정보들은 저수준(low level)에서 검출되는 원시 이벤트 (raw events)이거나 혹은 오디트(audit data)로부터 발생되는 고수준(high level) 경고 이벤트도 될 수 있다. 저수준의 원시 이벤트는 파일 시스템 업데이트, 네트워크 패킷, 그리고 시스템 콜 들을 포함한다. 고수준 경보들은 침입탐지시스템으로부터 발생되는 이벤트를 포함한다. 대부분의 공간 연관성 분석 기술들은 고수준의 이벤트에 초점을 맞추고 있다. 한편, 통계적 방법과 룰-기반 방법이 사용된다. 저수준의 이벤트 레코드와 비교해 고수준의 이벤트 수는 확연히 줄어든다. 따라서 고수준의 이벤트를 다루는 것은 복잡도에서 매우 유리하게 되지만 지협적으로 관찰되는 이벤트로는 침입을 검출할 수 없는 경우가 발생되기도 한다.

2.2 연구 동기

현재 활발하게 논의되고 있는 융합보안은 단순한 보안 이벤트의 디스플레이 통합화나 관리 체계의 단일화 수준에 머물러 있다. 따라서 진정한 융합보안의 효과를 얻기 위해서는 이 두 영역의 보안 이벤트들을 어떻게 상호 연동하여 보다 높은 수준의 보안 정보를 만들어 낼 것인가에 대한 구체적인 방법이 제시되어야 한다. 그러나 앞에서 언급한 바와 같이 보안 분야에서 적용된 이벤트 연관성 분석기술은 정보보안 분야에서만 이용되어 왔다.

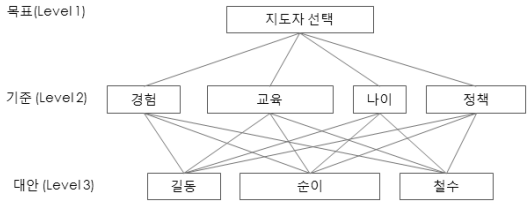
오늘날 물리보안 장치들은 보안 영역 내 접근제한 수단 및 관련 정보를 제공한다. 예를 들어, 출입문통제시스템은 해당 출입문을 통해 비인가 받은 사람이 해당 보안 영역 내로 접근하는 것을 감시는 것이고 영상감시 시스템 역시 해당 보안 연역 내 비정상적인 객체를 탐지해 해당 보안 영역 내 접근을 제한하는 것이다. 따라서 해당 보안 영역 내에 우리가 보호해야할 컴퓨팅 시스템이 존재한다면 물리보안 장치에서 제공하는 다양한 이벤트 정보들은 컴퓨팅 시스템을 보호하기 위한 정보보안에 적극 활용할 필요가 있다. 보다 구체적으로는, 이러한 목적을 위해 다음과 같은 두 가지 방법으로 접근할 수 있다. 첫째, 물리보안 이벤트

와 정보보안 이벤트 사이 일대일 상관관계에 의한 매우 직접적이며 분명한 융합보안 시나리오를 작성하는 것이다. 예를 들어, 물리보안이 제공하는 접근제한 영역 내에 존재하는 않는 사용자(물리보안 이벤트)에 의해 로컬 시스템 로그-온(정보보안 이벤트) 이벤트가 발생하는 경우 매우 강력하고 확실한 정보보안 경고 메시지를 발생시킬 수 있다. 두 번째, 물리보안 이벤트가 만들어 내는 다양한 이벤트 조합들을 간접적으로 정보보안에 활용하는 방안이다. 예를 들어, 물리보안 장치에서 발생된 이벤트들이 해당 보안 영역 내 심각한 수준의 위험 즉 외부의 침입 가능성을 경고한다고 가정하면 해당 컴퓨팅 시스템의 각종 정보보안 이벤트들은 평소와는 다르게 감시되고 처리되어야 할 것이다. 상기 첫 번째 접근 방법은 두 영역 이벤트 조합에 대한 일대일 대응에 의한 단순 처리 과정을 통해 얻을 수 있는 간단한 문제임으로 본 논문에서는 상기 두 번째 접근 방법인 간접적인 물리보안 이벤트 활용 문제만 다루기로 한다. 본 저자들이 알고 있는 범위 내에서는, 이러한 시도는 본 논문이 최초임을 밝힌다.

물리보안 이벤트와 정보보안 이벤트의 상호 연관성을 도출하고 입증하는 것은 현장 실험을 통해 얻어진 실제 자료를 바탕으로 이루어질 수 있는 문제이다. 즉 해당 보안 영역이 물리보안 위험 정도에 따라 정보보안 위험에 어떤 상관관계를 가지며 어떤 수준의 영향을 미칠 것인지는 해당 보안 영역의 환경 및 보안 관리자의 판단에 따라서 많은 차이를 보일 것이다. 예를 들어, 출입문통제시스템(물리보안 장치)이 출입문열림지속(물리보안 이벤트) 이벤트를 발생시켰다고 가정하면 현재 발생된 물리보안 이벤트를 어떤 정보보안 시나리오와 상호 관계를 맺을지는 보안 관리자의 판단에 좌우되며 또한 이들 물리보안 이벤트 조합의 중요도는 해당 물리보안 영역 내 존재하는 인가받은 사람의 수와 해당 물리보안 영역의 크기 등 다양한 물리보안 영역 환경에 따라 달라진다. 따라서 본 논문에서 물리보안 이벤트와 정보보안 이벤트의 상호 연관관계를 입증하는 문제를 다루는 것이 아니라 보안 관리자의 관심 대상이 되는 임의의 정보보안 관점(이하, 정보보안 오브젝트라 칭함)에서 의미 있는 물리보안 이벤트 조합을 찾기 위한 체계적인 방법을 제시하는 것이다.

III. 계층분석과정(AHP: Analytic Hierarchy Process)

AHP는 복잡한 의사결정(decision problem)을



〔그림 1〕 4개의 기준(criteria)과 3개의 대안(alternatives)로 이루어진 AHP의 계층구조 〔9〕

조직화하고 분석하는 구조화된 기술이다. 수학적 그리고 심리적 학문에 기반한 Thomas L. Satty에 의해 1970년대에 개발된 AHP는 이 후 기업, 산업, 그리고 교육 등 여러 분야에서 의사결정을 위해 사용되어 왔다〔9,10〕. AHP 사용자는 먼저 자신의 의사결정 문제를 계층화시켜 더욱 이해하기 쉬운 형태의 문제로 재구성하여야 한다. 즉 계층의 각 레벨을 일반적인 것으로부터 보다 자세한 세부 문제로 계층을 확대해 나가는 것이다. 결국, 이러한 계층적 구조는 의사 결정 문제를 보다 쉽게 풀어갈 수 있도록 문제를 보다 명료하게 보이도록 한다. 다음 〔그림 1〕에서 보여 지듯이, AHP 계층구조는 의사결정 목표(goal), 이들 목표에 도달하기 위한 대안(alternatives), 그리고 이들 대안과 목표를 연결하는 기준(criteria)의 그룹으로 이루어진다.

일단 계층적 구조가 완성되면, 의사 결정은 각 대안들의 쌍대비교(pairwise comparisons)을 통해 계층의 각 노드들에 대한 수치적 스케일을 결정할 수 있게 된다. 즉 AHP의 가장 큰 특징은 평가를 절대평가가 아닌 일대일 비교에 의한 상대평가에 근거하여 행한다는 것이다. 그리고 각 기준들 역시 중요도에 따라 목표에 대해 쌍대 비교를 수행한다. 쌍대비교에 사용되는 척도는 인간이 느낄 수 있는 차이를 최대한도로 반영할 수 있는 범위를 요구한다. 1965년 밀러의 심리학실험에서 "인간은 7개의 대상을 혼동이 없이 동시에 비교가 가능하다"라는 결과로부터 척도의 범위는 1에서 9까지의 수 또는 이의 역수들로 한다 (〔표 1〕 참조)〔12〕.

이러한 비교들은 수학적으로 처리되고 각 대안에 대한 가중치(weight)가 결정된다. 이러한 가중치는 각 기준 내에서 대안들이 가지는 상대적 중요도를 나타낸다. 즉 AHP는 이러한 평가들을 문제를 처리하고 비교하기 위해 사용될 수 있는 값으로 변환한다. 이러한 값들을 각 계층에서의 대안의 가중치(weight) 혹은 우선순위(priority)라고 부른다.

〔표 1〕 비교 스케일

언어적 판단	계량적 점수 부여
극단적 선호	9
중 간	8
매우 강하게 선호	7
중 간	6
강하게 선호	5
중 간	4
약간 선호	3
중 간	2
동일하게	1

쌍대비교와 우선순위 과정은 다음과 같다. n 개의 요소들을 각각 $A_1, A_2, \cdots, A_n$이라 하고 각 요소들의 가중치를 $w_1, w_2, \cdots, w_n$이라고 가정한다. 이제 이들 각 요소들에 대한 쌍대비교로부터 얻어진 결과를 다음 식 (1)과 같은 비교행렬(comparison matrix) A로 표현한다.

$$A = \begin{bmatrix} w_1/w_1 & w_1/w_2 \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 \cdots & w_2/w_n \\ \cdots & \cdots \cdots & \cdots \\ w_n/w_1 & w_n/w_2 \cdots & w_n/w_n \end{bmatrix} \quad (1)$$

쌍대비교에 의해 비교행렬 $A=(a_{ij})$ 가 이루어지면, $a_{ii}=1(i=1,2,\cdots,n)$ 이고 $a_{ji}=1/a_{ij}$ 인 역수행렬(reciprocal matrix)이 된다. 이 행렬에 상대적 중요도를 나타내는 열벡터(column vector) $W^T=(w_1, w_2, \cdots, w_n)$을 곱한 결과는 식 (2)와 같은 관계식을 성립한다. 따라서 상기 식 (2)에서 우리는 행렬 A의 특성방정식의 고유치(eigenvalue)가 산출되는 과정에서 가중치 W를 유도할 수 있게 된다. 이때 행렬 A가 완전한 기수적 일관성 (cardinal consistency)이 있다면, 특성방정식의 근 $\lambda_i(i=1,2,\cdots,n)$는 가장 큰 근($\lambda_{\max}$) 하나만이 n의 값을 가지며, 나머지 근들은 모두 0이 된다〔9,10〕. 한편, 쌍대비교 행렬을 만들 때 논리적 모순의 정도를 검증하기 위해 기수적 일관성을 측정해 볼 필요가 있다. 즉 쌍대비교에 의해서 얻어진 행렬 A에 요소 a_{ij}가 w_i/w_j 값을 갖고 있다면 기수적 일관성, 즉 $a_{ij} \cdot a_{jk} = a_{ik}$ 가 성립되는 경우 $\lambda_{\max}=n$이 되며, 일관성에서 벗어나는 편차를 측정하는 $\lambda_{\max}-n$ 으로 알 수 있다. 따라서 일치되는 정도를 지수로 나타낸 것을 일관성지수(consistency index: CI)로 정의하며 다음 식 (3)과 같이 정의된다.

$$\begin{bmatrix} w_1/w_1 & w_1/w_2 \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 \cdots & w_2/w_n \\ \cdots & \cdots \cdots & \cdots \\ w_n/w_1 & w_n/w_2 \cdots & w_n/w_n \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ \cdots \\ w_n \end{bmatrix} = n \begin{bmatrix} w_1 \\ w_2 \\ \cdots \\ w_n \end{bmatrix} \quad (2)$$

$$CI = \frac{\lambda_{\max} - n}{n-1} \quad (3)$$

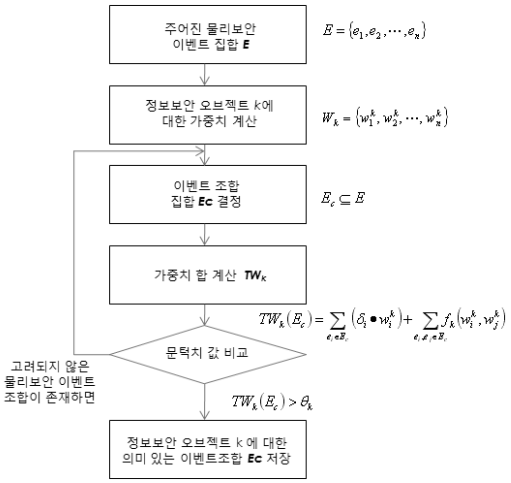
한편, 상대적 중요도를 평가할 때 얼마나 일관성을 가지고 평가를 진행하였는지 확인할 필요가 있다. 이를 위해 일관성지수 CI를 경험적 자료로 얻어진 평균 무작위 지수(random index: RI)로 나눈 일관성비율(consistency ratio: CR)로 검정할 수 있으며, Satty는 CR의 값이 10% 이내인 경우에만 서수적 순위에 무리가 없는 신뢰할 수 있는 결과라고 하였다. 표본 500개로부터 RI를 구하여 평균을 구한 결과 행렬의 크기가 4이면 0.90 그리고 7이면 1.32로 조사되었다〔12〕. 따라서 행렬의 크기가 5이상 이면 통상보다 엄격한 CI 값 10%를 기준으로 일관성 검증을 실시하여 평균 RI 값을 구하는 부담을 제거할 수 있다. 본 논문의 제5장 적용 사례에서도 CI 값을 사용하였음을 밝힌다.

IV. 융합보안을 위한 정보보안 오브젝트 기반 접근법

4.1 물리보안 이벤트 조합 생성

서론에서 설명한 바와 같이 물리보안 장치에서 발생되는 이벤트의 수가 n 개라고 가정하면, 2^n 개의 이벤트 조합이 가능하게 되며 이들 이벤트 조합 중에서 어떤 물리보안 이벤트 조합들을 정보보안 영역에서 활용할지 결정해야 한다. 그러나 n 이 클 경우 모든 물리보안 이벤트 조합을 고려한다는 것은 쉽지 않다. 따라서 우리는 물리보안과 정보보안 사이의 이벤트 연관성 분석을 통해 정보보안에서 사용하게 될 의미 있는 물리보안 이벤트 조합을 결정할 수 있는 체계적인 방법이 필요하다. 〔그림 2〕는 본 논문에서 제시하는 물리보안 이벤트 조합을 찾는 연관성 분석 과정을 나타낸다.

먼저, 물리보안 이벤트 셋 $E=\{e_1, e_2, \cdots, e_n\}$ 가 주어지고, 우리의 관심 대상인 정보보안을 기준으로 구체적인 목표 즉 오브젝트(object)를 결정한다. 또한 다수의 정보보안 오브젝트 셋 $O=\{o_1, o_2, \cdots, o_x\}$을 가정한다. 예를 들어, 컴퓨팅 시스템 침입, 컴퓨터 파일 시



〔그림 2〕 물리-정보 보안 이벤트 연관성 분석 알고리즘

스템 공격, 그리고 네트워크 공격 등을 정보보안 주요 오브젝트로 설정할 수 있다. 이들 정보보안 오브젝트 o_k $(k=1,2,\cdots,x)$ 를 기준으로 물리보안 이벤트들의 가중치(혹은 중요도)를 결정한다. 즉 각 물리보안 이벤트들은 해당 정보보안 오브젝트에 대한 가중치 값 $W_k=\{w_1^k,w_2^k,\cdots,w_n^k\}$를 갖게 된다. 본 논문에서는 제3장에서 설명한 AHP를 통해 이들 물리보안 이벤트 가중치 값을 결정한다. 이제 정보보안 오브젝트 o_k 에 대해 임의의 물리보안 이벤트 조합 $E_c(\subseteq E)$가 의미 있는 이벤트 조합이 될 수 있는 가능성을 나타내는 결정값(decision value) $TW_k(E_c)$를 다음 식 (4)와 같이 구한다.

$$TW_k(E_c)=\sum_{e_i\in E_c}(\delta_i\bullet w_i)+\sum_{e_s e_j\in E_c}f_k(w_i,w_j), \tag{4}$$

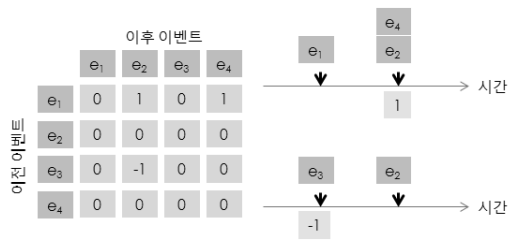
$$\delta_i=\begin{cases}+1 & \text{if } e_i\Uparrow o_k\\ -1 & \text{if } e_i\Downarrow o_k\end{cases}$$

여기서, δ_i는 E_c에 속한 물리보안 이벤트 e_i가 o_k에 긍정적(positive) 관계를 가지면 +1을 갖고, 반대로 부정적(negative) 관계를 가지면 -1을 갖게 되는 임펄스 함수이다. 따라서 식 (4)의 $TW_k(E_c)$ 는 해당 물리보안 이벤트 조합에 포함된 각 이벤트의 단순 가중치 합(simple additive weight method)을 구한 후, 해당 물리보안 이벤트 조합에 포함된 임의의 두 이벤트 e_i와 e_j가 갖는 정보보안 오브젝트 o_k에 대한 쌍대 상관 함수 (pairwise correlation function) $f_k(w_i,w_j)$를 고려한다. 여기서 $f_k(w_i,w_j)$는 다음 식 (5)와 같이 이벤트 e_i와 e_j 의 시간 연관성(temporal correlation)에 의해 결정된다. 정보보안 오브젝트 o_k 조건에서 먼저 발생된 이벤트 e_i가 뒤에 발생된 이벤트 e_j의 효과를 변화 $(e_i\xrightarrow{k}e_j)$ 시키거나, 혹은 이와는 반대로 먼저 발생된 이벤트 e_i 의 효과가 변화 $(e_i\xleftarrow{k}e_j)$ 될 수 있다.

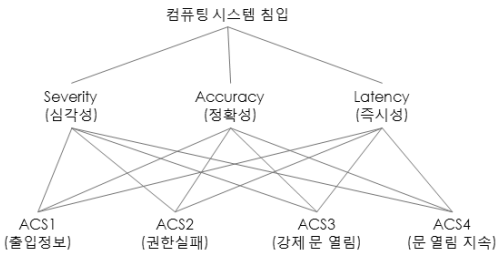
$$f_k(w_i,w_j)=\begin{cases}g_k(w_j) & \text{if } e_i\xrightarrow{k}e_j\\ g_k(w_i) & \text{if } e_i\xleftarrow{k}e_j\\ 0 & otherwise\end{cases} \tag{5}$$

여기서, 함수 $g_k(w)$는 이벤트 가중치 w에 대한 가중치 변화의 정도를 나타내며 다양한 함수를 적용할 수 있다. 예를 들어, 두 이벤트의 시간 연관성 효과는 주어진 정보보안 오브젝트 o_k에 대해 $TW_k(E_c)$ 값을 증가시킬 수 도 있으며 혹은 반대로 감소시킬 수 도 있다. 본 논문에서는 단순 2진 부정적(negative) 시간 연관성 효과만을 고려한 $g_k(w)=-w$ 관계식을 사용한다. 즉 $e_i\xrightarrow{k}e_j$ 의 경우, 물리보안 이벤트 e_j의 가중치 w_j가 물리보안 이벤트 e_i에 의해 무시되고, 반대로 $e_i\xleftarrow{k}e_j$의 경우, 물리보안 이벤트 e_i의 가중치 w_i가 물리보안 이벤트 e_j에 의해 무시된다. 〔그림 3〕은 4개의 물리보안 이벤트에 대한 $f_k(w_i,w_j)$를 2진 쌍대 시간 연관성 행렬 (Binary Feature Pairwise Temporal Correlation Matrix)로 나타내었다. 〔그림 3〕의 행렬 엔트리가 1인 경우 $e_i\xrightarrow{k}e_j$를 나타내고, 행렬 엔트리가 -1인 경우 $e_i\xleftarrow{k}e_j$를 각각 나타낸다.

최종적으로, 〔그림 2〕에서 $TW_k(E_c)$ 가 정보보안 오



〔그림 3〕 2진 쌍대 시간 연관성 행렬 예



〔그림 4〕 출입통제기 물리보안 이벤트이 가중치 결정을 위한 AHP 계층도

브젝트 o_k 의 문턱치 값 θ_k 보다 크면 E_c 는 정보보안 오브젝트 o_k에 대한 '의미 있는 물리보안 이벤트 조합'이 된다. 이때 θ_k 값 설정은 제안된 기법의 성능에 중요한 역할을 할 것으로 예상되며, 제5장 적용 사례를 통해 설정 방법에 대한 아이디어를 제공한다.

4.2 AHP를 통한 물리보안 이벤트 가중치 결정

〔그림 4〕는 물리보안 이벤트들에 대한 중요도를 나타내는 가중치 계산을 위한 AHP의 계층도를 보여준다. 그림에서 보듯이, 레벨 2의 기준은 각 물리보안 장비를 기준으로 사용하거나 혹은 보안 특징을 기준으로 사용할 수 있다. 예로서, 물리보안 장비를 기준으로 사용할 경우, 출입통제기, CCTV 및 영상분석 장치, 혹은 바이오 인식 장치 등이 된다. 만약 보안 특징을 기준으로 사용할 경우 주어진 정보보안 오브젝트에 영향을 미치는 특징, 예를 들어 물리보안 이벤트가 해당 정보보안 오브젝트에 미치는 영향의 정도를 나타내는 심각성(severity), 이벤트의 사용 가능성(availability), 이벤트의 정확성(accuracy), 그리고 이벤트의 반응 시간을 가늠할 수 있는 즉시성(latency) 등이 사용될 수 있다. 한편 본 논문에서는 AHP의 대안인 물리보안 이벤트의 쌍대비교 행렬을 만들 때 〔표 1〕에 나타난 비교 스케일을 사용하였다.

V. 적용 사례

본 장에서는 하나의 정보보안 오브젝트 '컴퓨팅 시스템 침입'을 정하고, 이 오브젝트에 대해 물리보안 이벤트를 어떻게 활용할 것인지에 관해 다룬다. 먼저 하나의 물리보안 장치(출입통제기)에서 발생되는 이벤트를 활용하는 예와 두개의 물리보안 장치(출입통제기와 영상감시 시스템)를 사용하는 환경에서의 적용 사

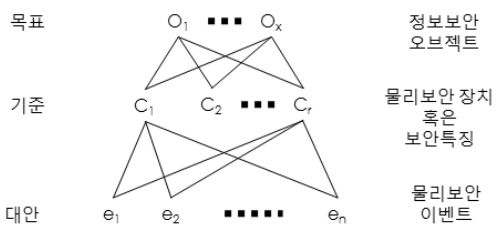
〔표 2〕 물리보안 이벤트

장치	이벤트	설명
출입 통제기	ACS1(e1)	허가 받은 정상적인 인원의 입.출입 정보 획득
	ACS2(e2)	일정 횟수 이상의 권한 실패
	ACS3(e3)	강제로 출입문 열림
	ACS4(e4)	일정 시간 문 열림이 지속
영상 분석기 CCTV	VAS1(e1)	객체 출입 정보 획득
	VAS2(e2)	침입 검출
	VAS3(e3)	위장된 객체 검출
	VAS4(e4)	제한 지역 내 배회
	VAS5(e5)	시그널 이상 (낮은 가시성 등)

례를 각각 설명한다. 다음 〔표 2〕는 출입통제기와 영상감시 시스템에서 발생되는 가장 대표적인 물리보안 이벤트를 나열하였다. 물론 이러한 이벤트 이외에도 다양한 물리보안 이벤트가 존재할 수 있으나 본 논문에서는 설명의 편의성을 위해 이들 이벤트들만 고려한다.

5.1 적용 사례 1

오늘날 우리가 사용하는 대부분의 출입문 통제기는 RFID 기술을 적용한 스마트카드를 이용해 출입자 정보를 획득하고 이더넷을 이용한 네트워킹 기능을 제공함으로써 원격에 있는 관리자가 해당 보안 영역 내 출입자들을 모니터링하게 된다〔11〕. 우리가 정한 정보보안 오브젝트에 대해서 이들 출입통제기 물리보안 이벤트의 가중치를 결정하기 위해 〔그림 5〕와 같은 AHP의 계층도를 사용한다. 그림에서 보듯이, AHP 기준으로 심각성, 정확성, 그리고 즉시성을 사용하였으며 각 레벨에서의 쌍대 행렬은 다음 〔표 3〕과 같이 결정하였다. 〔표 3〕에서 보듯이, 물리보안 이벤트를 고려할 때 기준으로 물리보안 이벤트의 심각성을 가장 중요하게 고려했으며, 다음으로는 이벤트의 정확성을



〔그림 5〕 물리보안 이벤트 가중치 결정을 위한 AHP 계층도

〔표 3〕〔그림 5〕 출입통제기 물리보안 이벤트의 가중치 결정을 위한 AHP의 쌍대비교 행렬 (S; 심각성, A: 정확성, L: 즉시성)

S	e1	e2	e3	e4
e1	1	5	1/5	1/3
e2	1/5	1	1/9	1/7
e3	5	9	1	3
e4	3	7	1/3	1

A	e1	e2	e3	e4
1	1	5	1	3
2	1/5	1	1/7	1
3	1	7	1	5
4	1/3	1	1/5	1

L	e1	e2	e3	e4
e1	1	3	1	7
e2	1/3	1	1/7	3
e3	1	7	1	7
e4	1/7	1/3	1/7	1

	S	A	L
S	1	3	5
A	1/3	1	3
L	1/5	1/3	1

꼽았다. 그러나 AHP 레벨2 기준의 종류와 이들에 대한 쌍대비교행렬은 보안 관리자에 의해 결정될 것이며 적용 환경에 따라 다른 값을 가질 수 있다. 한편, AHP의 레벨3 물리보안 이벤트에 대한 쌍대비교행렬은 〔표 3〕과 같이 결정했으며, 이들 쌍대비교행렬을 기준으로 계산된 각 이벤트의 가중치들은 〔표 4〕와 같다. 〔표 4〕에서 보듯이 이들 각 가중치들의 CI 값들이 10% 미만으로 나타났음으로 쌍대비교행렬 결정에 대한 만족할 만한 수준으로 판단의 일관성을 보장받은 것으로 볼 수 있다. 한편 〔표 3〕에서 결정한 레벨2 기준에 대한 쌍대행렬로부터 계산된 가중치는 심각성이 0.64, 정확성이 0.57, 그리고 즉시성이 0.103으로 조사되었고, 이러한 가중치 값들을 사용하여 〔표 4〕의 최종 물리보안 이벤트의 가중치가 결정되었다. 이때 레벨2 기준의 쌍대비교행렬 CI는 0.0194로 조사 되었다.

〔그림 6〕은 출입통제기 물리보안 이벤트에 대한 2진 쌍대 시간 연관성 행렬을 보여준다. 〔그림 6〕에서 보듯이 우리가 방어하는 물리보안 영역의 크기에 따라서 행렬의 값은 변화될 수 있음을 보여 준다. 예를 들어, 개인연구실 규모의 좁은 보안영역 내 출입통제기의 경우 ACS1(e1 출입정보) 이벤트는 해당 보안영역 내에 정상적인 출입권한을 가진 사용자가 존재하는

〔표 4〕 출입통제기 물리보안 이벤트의 가중치

이벤트	심각성	정확성	즉시성	최 종
ACS1	0.123	0.373	0.361	0.2117
ACS2	0.037	0.076	0.107	0.0542
ACS3	0.567	0.456	0.483	0.5298
ACS4	0.273	0.095	0.049	0.2041
CI	0.0581	0.0157	0.0433	

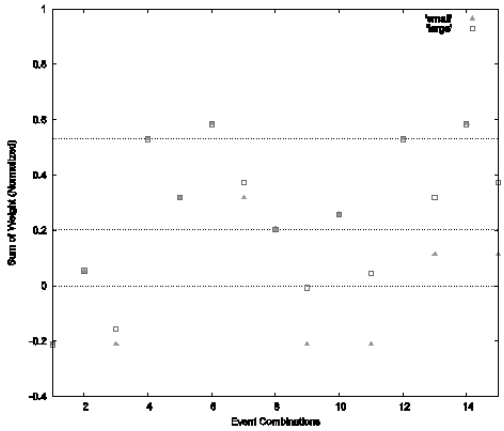
〔그림 6〕 출입통제기 물리보안 이벤트 2진 쌍대 시간 연관성 행렬 예 (보안 영역 규모에 따른 변화)

것을 의미하며, 따라서 ACS2(e2 출입 권한 실패) 그리고 ACS4(e4 문열림 지속) 이벤트들은 더 이상 이벤트로서 의미를 가지지 못함을 보인다(〔그림 6〕 참조). 이와 반대로 빌딩 내 출입통제기와 같은 큰 규모의 보안영역 내에서는 좁은 보안영역 내에서 해석되었든 이와 같은 두 이벤트 간의 시간 연관성 분석이 더 이상 유효하지 않게 된다. 물론 이러한 두 이벤트 간 시간 연관성 분석 (〔그림 6〕의 2진 쌍대 시간 연관성 행렬 값)은 AHP의 쌍대비교행렬과 마찬가지로 보안 환경에 따른 보안 관리자의 판단에 의해 결정될 값들임을 기억해야 한다.

〔그림 7〕은 〔표 4〕와 〔그림 6〕과 같이 구한 출입통제기의 물리보안 이벤트 가중치와 이들 이벤트 간의 2진 쌍대 시간 연관성 행렬을 기준으로 식 (4)를 이용해 모든 가능한 이벤트 조합에 대한 결정값을 보여준

〔표 5〕 출입통제기 물리보안 이벤트 조합과 문턱치 값에 따른 이벤트 조합 셋 (S: 좁은 보안 영역, L: 넓은 보안 영역)

조합	이벤트				threshold (문턱치 값)					
	e1	e2	e3	e4	0.0		0.2		0.52	
					S	L	S	L	S	L
1	√									
2		√			√	√				
3	√	√								
4			√		√	√	√	√	√	√
5	√		√		√	√	√	√		
6		√	√		√	√	√	√	√	√
7	√	√	√		√	√	√	√		
8				√	√	√	√	√		
9	√			√						
10		√		√	√	√	√	√		
11	√	√		√		√				
12			√	√	√	√	√	√	√	√
13	√		√	√	√	√		√		
14		√	√	√	√	√	√	√	√	√
15	√	√	√	√	√	√		√		
δ	-1	1	1	1						



〔그림 7〕 출입통제기 물리보안 이벤트 조합의 결정값 $TW_k(E_c)$

다. 이때 2진 쌍대 시간 연관성 행렬을 적용하기 위해서는 물리보안 이벤트의 발생순서가 중요하며, 본 적용 사례에서는 하나의 물리보안 이벤트 조합 내에 복수의 이벤트가 존재할 경우 시간 순서상에서 이벤트 1, 2, 3, 그리고 4의 순서로 발생된다고 가정한다. 〔그림 7〕의 x 축에 나타난 이벤트 조합 번호는 〔표 5〕와 같다.

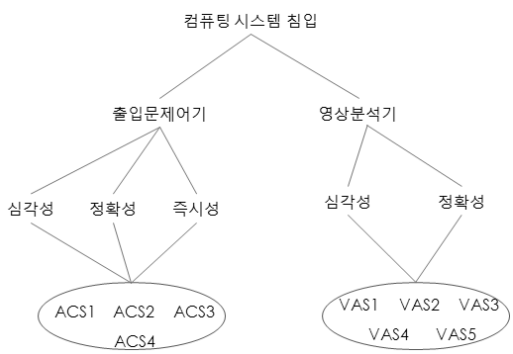
〔표 5〕에서 보듯이, 출입정보 획득 이벤트(e1 혹은 ACS1)는 우리가 정한 정보보안 오브젝트에 대해 '부정적 관계 ($\delta=-1$)'를 가진다. 즉 정상적인 사용자가 해당 보안영역 내에 존재한다는 사실은 영역 내 존재하는 컴퓨팅 시스템들이 외부 침입자로부터 접근될 가능성이 떨어진다는 것을 의미한다. 반대로 출입 시도 실패 이벤트(e1 혹은 ACS2), 강제문열림 이벤트(e3 혹은 ACS3), 그리고 문열림지속 이벤트(e4 혹은 ACS4)는 정보보안 오브젝트에 대해 '긍정적 관계 ($\delta=1$)'를 가진다. 〔그림 7〕로부터 우리가 정한 정보보안 오브젝트에 관한 이들 물리보안 이벤트의 의미 있는 조합을 선택하기 위해, 세 가지 종류의 문턱치 값을 설정 후 이 값보다 큰 결정값을 가지는 물리보안 이벤트 조합들을 좁은 보안 영역과 넓은 보안 영역으로 구분해 〔표 5〕에 나타내었다. 문턱치 값은 물리보안 이벤트 중에서 가장 큰 가중치를 갖는 값을 조건1로 선택하고 두 번째 큰 가중치 값을 조건2, 그리고 0을 조건3으로 각각 설정한 후 시험하였다. 우리가 이미 쉽게 예상할 수 있었듯이, 문턱치 값이 올라갈수록 의미 있는 물리보안 이벤트의 조합 수는 줄어들고, 그리고 보안 영역이 넓어질수록 우리가 고려해야할 보안 이벤트 조합 수는 늘어난다.

〔표 6〕〔그림 8〕 영상감시 시스템의 물리보안 이벤트의 가중치 결정을 위한 AHP의 쌍대비교 행렬

	심각성(severity)					정확성(accuracy)				
	e1	e2	e3	e4	e5	e1	e2	e3	e4	e5
e1	1	1/7	1/5	3	1	1	1/2	4	2	3
e2	7	1	3	6	4	2	1	5	2	3
e3	5	1/3	1	4	2	1/4	1/5	1	1/3	1/4
e4	1/3	1/6	1/4	1	1/3	1/2	1/2	3	1	1/2
e5	1	1/4	1/2	3	1	1/3	1/3	4	2	1

5.3 적용 사례 2

본 절에서는 출입통제기와 영상감시 시스템이 해당 보안 영역 내에 함께 존재하는 환경에서 이들 물리보안 이벤트를 정보보안 오브젝트 '컴퓨팅 시스템 침입'에 활용하는 방안을 설명한다. 구현에 필요한 모든 과정은 앞 절에서 설명한 적용 사례 1과 동일하기 때문에 자세한 설명은 생략하고 영상감시 시스템과 관련된 주요 데이터와 결과 중심으로 설명한다 (출입통제기 관련 파라미터는 적용 사례 1에서 구한 값들을 변경 없이 사용한다). 〔그림 8〕은 출입통제기와 영상감시 시스템의 물리보안 이벤트 가중치를 결정하기 위한 AHP 계층도를 보여준다. AHP 레벨 2 기준으로는 이들 물리보안 장치를 선택했으며, 이들 기준에 대한 가중치는 0.6 (출입통제기)과 0.4 (영상감시 시스템)로 각각 결정했다. 적용 사례 1에서 설명한 바와 같이 이러한 가중치 결정은 보안 관리자에 의해 결정되는 파라미터임을 밝힌다. 본 논문에서는 하드웨어적으로 보다 안정적이며 정확한 정보를 제공할 수 있는 출입통제기를 영상감시 시스템과 비교해 높은 가중치를 부여하였다.



〔그림 8〕 출입통제기와 영상감시 시스템의 물리보안 이벤트 가중치 결정을 위한 AHP 계층도

〔표 7〕 영상감시 시스템의 물리보안 이벤트의 가중치 (영상감시 시스템 AHP 레벨3 기준 심각성 가중치: 0.6, 정확성 가중치: 0.4)

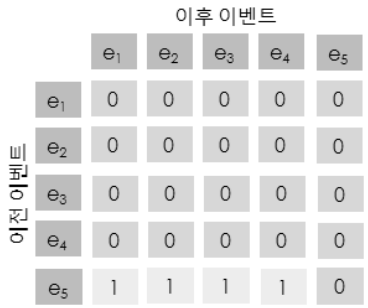
이벤트	심각성	정확성	레벨3
VAS1	0.087	0.281	0.1646
VAS2	0.502	0.371	0.4496
VAS3	0.253	0.052	0.1726
VAS4	0.047	0.129	0.0798
VAS5	0.110	0.165	0.1320
CI	0.0665	0.0618	

〔표 6〕은 〔그림 8〕에서 보인 AHP 계층도에서 레벨4에 해당하는 영상감시 시스템의 물리보안 이벤트의 가중치를 결정하기 위해 정한 쌍대비교행렬을 보여주며, 〔표 7〕은 이들 쌍대비교행렬을 이용해 〔그림 8〕의 레벨 3에서 결정된 각 물리보안 이벤트의 가중치 값들이다. 이때 레벨 3 기준의 가중치는 각각 0.6 (심각성)과 0.4(정확성) 결정하였다. 〔표 8〕은 〔표 4〕와 〔표 7〕에서 얻어진 각 물리보안 이벤트 가중치를 기준으로 〔그림 8〕 레벨 2의 가중치를 고려해서 최종 결정된 물리보안 이벤트 가중치를 보여준다. 한편, 영상감시 시스템의 2진 쌍대 시간 연관성 행렬은 〔그림 9〕와 같다. 〔그림 9〕에서 보듯이 영상감시 시스템의 영상시그널 이상 이벤트(e5 혹은 VAS5)가 발생될 경우, 뒤이어 발생되는 모든 영상감시 시스템 물리보안 이벤트 효과는 무시된다.

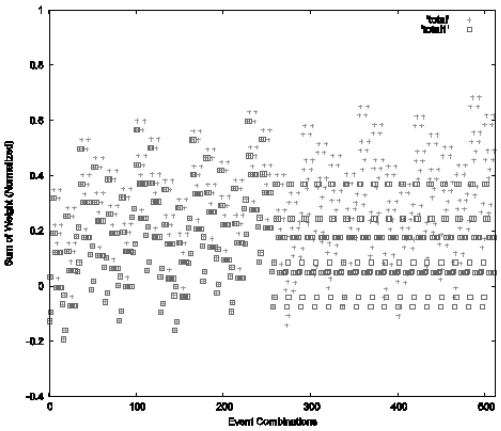
〔그림 10〕은 출입통제기와 영상감시 시스템의 물리보안 이벤트 조합에 따른 결정값 식 (4)의 $TW_k(E_c)$를 보여준다. 이때 이벤트 조합번호는 이벤트 수가 모두 9개임으로 1에서 511까지 가능하며, 출입통제기 이벤트 e1이 LSB(Least Significant Bit), 그리고 영상감시 시스템 e5가 MSB(Most Significant Bit)가 되는 9비트 2진수로 나타내었다. 앞에서 설명한 바와 같이, 물리보안 이벤트 2진 쌍대 시간 연관성

〔표 8〕 출입통제기 및 영상감시 시스템의 물리보안 이벤트의 가중치 (AHP 레벨2의 출입통제기 가중치: 0.6, 영상시스템 가중치: 0.4)

이벤트	가중치	이벤트	가중치
ACS1	0.1270	VAS1	0.0658
ACS2	0.0325	VAS2	0.1798
ACS3	0.3179	VAS3	0.0690
ACS4	0.1225	VAS4	0.0319
		VAS5	0.0528



〔그림 9〕 영상감시 시스템 물리보안 이벤트 2진 쌍대 시간 연관성 행렬 예



〔그림 10〕 출입통제기와 영상감시 시스템 물리보안 이벤트 조합의 결정값 $TW_k(E_c)$ (+ 표시: 경우 1, □ 표시: 경우 2)

행렬에 의해서 이벤트 조합 내에 복수의 이벤트가 존재할 경우 이벤트 발생순서가 중요하다.

〔그림 10〕에서는 두 가지 순서 조합에 대한 결과만을 보인다. 첫 번째 시간 순서 조합 (경우 1)은 출입통제기 이벤트 e1, e2, e3, e4, 그리고 영상감시 시스템 이벤트 e1, e2, e3, e4, e5 순이고, 이와 정반대인 두 번째 시간 순서 조합 (경우 2)는 영상감시 시스템 e5, e4, e3, e2, e1, 그리고 출입통제기 e4, e3, e2, e1 순이다. 〔그림 10〕에서 두 번째 이벤트 시간 순서 조합의 경우, 이벤트 조합 번호 256부터 일정한 패턴을 보이는 이유는 〔그림 9〕에서 설명한 바와 같이 영상감시 시스템의 이벤트 e5에 의해 뒤 이어 발생되는 영상감시 시스템 이벤트들이 모두 무시되기 때문이다. 한편, 문턱치 값을 출입통제기 이벤트 e3 (혹은 영상감시 시스템 이벤트 e2) 의 가중치로 잡을 경우, (경우 1)은 88 (혹은 193) 개의 이벤트 조합이,

그리고 (경우2)는 217 (혹은 354) 개 이벤트 조합이 각각 의미 있는 이벤트 조합으로 등록되었다.

5.3 정보보안 해석

5.1절과 5.2절을 통해 정보보안 오브젝트 '컴퓨팅 시스템 침입'에 대한 의미 있는 물리보안 이벤트 조합을 구했다. 결국 이러한 물리보안 이벤트 조합들은 우리가 정한 정보보안 오브젝트에 관하여 훨씬 높은 발생 가능성을 객관적 지표로 제공하는 것으로 볼 수 있다. 한편 정보보안에 관련된 다양한 이벤트들이 존재한다. 예를 들어, 방화벽 혹은 침입탐지 시스템 등과 같이 정보보안에 직접 관련된 장치에서 발생되는 각종 이벤트들과 일반 컴퓨팅 시스템에서 발생되는 이벤트 로그 등이 있다. 이들 정보보안 이벤트 중에서 '컴퓨팅 시스템 침입'이라는 오브젝트에 관련된 이벤트가 발생되고 이 오브젝트에 관련된 의미 있는 물리보안 이벤트 조합이 동시에 존재한다면, 관련 정보보안 이벤트는 훨씬 높은 수준의 보안 경보로 취급되어야 할 것이다. 예를 들어, 윈도우즈 혹은 리눅스 서버에서 발생되는 '프로그램 설치' 로그 정보보안 이벤트가 앞에서 구한 물리보안 이벤트 조합과 함께 발생하게 되면, 매우 심각한 수준의 정보보안 이벤트로 처리되어야 할 것이다.

VI. 결론

몇 년 전만해도 산업보안의 중심은 물리보안이 대부분이었다. 그러나 오늘날 정보화 사회의 도래와 함께 정보보안의 중요성은 물리보안과 동등한 수준에서 논의되고 있다. 융합보안은 기존에 분리 운영되어 왔던 물리보안과 정보보안을 하나의 프레임워크 안에서 통합 운영함으로써 효율을 극대화하고자 함이다. 그러나 이러한 활발한 토의에도 불구하고 어떻게 융합할 것인지에 대한 구체적인 실현 방안이 존재하지 않는 실정에 있다. 본 논문에서는 정보보안 오브젝트 기반 접근법을 제시하고 물리보안 이벤트를 정보보안 오브젝트에 어떻게 활용할지에 대한 구체적인 구현 방법을 제시하였다. 특히 AHP를 이용해 물리보안 이벤트를 정보보안 관점에서 정량화시키고, 물리보안 이벤트들의 시간 연관성(temporal correlation)을 나타내는 2진 쌍대 시간 행렬을 제안하였으며 이를 기반으로 모든 물리보안 이벤트 조합을 고려해 해당 정보보안 오브젝트에 의미 있는 이벤트 조합을 선택할 수 있는 방법을 제안하였다. 제안된 방법이 비록 융합보안을 위한 최적의 시스템이라고 판단하기에는 다소 무리가 있으나, 물리보안 이벤트를 어떻게 정보보안 분야에 활용할 수 있을지에 대한 구체적인 실현 방안을 최초로 제안했다는 점에 의미가 있다고 본다.

향후 연구 방향으로는 정보보안 오브젝트를 '파일 시스템 공격', '네트워크 공격', 그리고 '시스템 공격' 등 보다 구체적으로 세분화시키고 실제 산업 현장에서 얻어진 물리보안 이벤트를 모두 적용하여 실험하는 단계로 나아가는 것이다. 뿐만 아니라, 융합보안을 위해 정보보안 장치의 이벤트를 물리보안 이벤트와 직접 연동시키는 저수준(low level) 연동방안도 강구할 예정이다.

참고문헌

〔1〕 최진묵, 권정옥, "융합보안시장 동향 보고", Samsung SDS Journal of IT Services, 7(2), pp. 13-29, 2010년 9월.

〔2〕 H. Debar, M. Sacier, and A. Wespi, "Towards a taxonomy of intrusion-detection system," Computer Networks, vol. 31, no. 8, pp. 805-822, April 1990.

〔3〕 한종옥, 조현숙, "영상보안시스템 기술 동향", 정보보호학회지, 19(5), pp. 29-37, 2009년 10월.

〔4〕 김정덕, 김건우, 이용덕, "융합보안의 개념 정립과 접근방법", 정보보호학회지, 19(6), pp. 68-74, 2009년 12월.

〔5〕 S.K. Chen, J.J. Jeng, and H. Chang, "Complex Event Processing using Simple Rule-based Event Correlation Engines for Business Performance Management," Proceedings of E-Commerce Technology/ The 8th IEEE International Conference on and Enterprise Computing, E-Commerce, and E-Services, pp. 100-102, June 2006.

〔6〕 이수형, 방효찬, 장범환, 나중찬, "효과적 보안상황 분석을 위한 보안 이벤트 처리", ETRI 전자통신동향분석, 22(1), pp. 59-72, 2007년 2월.

〔7〕 Y. Xie, "A Spatiotemporal Event Correlation Approach to Computer Security," Ph.D Dissertation, Dept. of CS, Carnegie Mellone University, May 2005.

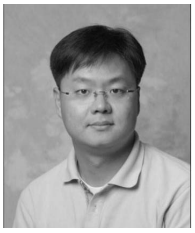
〔8〕 A. Muller, Event "Correlation Engine," Master's Thesis, Dept. of IT and EE, Swiss Federal Institute of Technology Zurich, Aug. 2009.
〔9〕 Thomas L. Saaty and L.G.Vargas, Prediction, Projection and Forecasting, Kluwer Academic Publishers. April 1991.
〔10〕 Thomas L. Saaty, "Relative Measurement and Its Generalization in Decision Making Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors The Analytic Hierarchy/Network Process," RACSAM (Review of the Royal spanish Academy of Sciences, Series A. Mathematics), vol. 102, no. 2, pp.251-318, Feb. 2008.
〔11〕 Suprema Inc., BioStar SDK Reference Manual, http://www.supremainc.com/ 고객지원 다운로드, 2010.

〈著者紹介〉

강 구 홍 (Koohong Kang) 정회원
1985년 8월: 경북대학교 전자공학과 학사
1990년 2월: 충남대학교 전자공학과 석사
1998년 2월: 포항공과대학교 전자계산학과 박사
1985년 9월~1999년 3월: 한국전자통신연구원 선임연구원
2002년 5월~2003년 12월: 한국전자통신연구원 초빙연구원
2008년 1월~2009년 2월: Purdue University Visiting Scholar
2000년 9월~현재: 서원대학교 교수
〈관심분야〉 성능평가, 컴퓨터 네트워크, 네트워크 보안

강 동 호 (Dongho Kang) 정회원
1999년 2월: 한남대학교 컴퓨터공학과 학사
2001년 2월: 한남대학교 컴퓨터공학과 석사
2001년 3월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 데이터 통신, 네트워크 보안, 보안 관제

나 중 찬(Jung Chan Nah) 정회원
1986년: 충남대학교 계산통계학과 졸업
1989년: 숭실대학교 전자계산학과 석사
2004년: 충남대학교 컴퓨터과학과 박사
1989년~현재: 현재 한국 전자통신연구원 책임연구원
〈관심분야〉 네트워크 보안, 보안 상황인지, 스마트그리드 보안, 산업제어망 보안



김 익 균 (Ikkyun Kim) 정회원
1994년 2월: 경북대학교 컴퓨터공학과 학사
1996년 2월: 경북대학교 컴퓨터공학과 석사
2009년 2월: 경북대학교 컴퓨터공학과 박사
1996년~1999년 한국전자통신연구원 연구원
1999년 2월~2001년 6월: (주)팍스콤 선임연구원
2004년 6월~2005년 7월: 미국 Purdue University Visiting Scholar
2001년~현재: 한국 전자통신연구원 책임연구원, 네트워크시스템보안연구팀 팀장
〈관심분야〉 클라우드 컴퓨팅, 컴퓨터 네트워크, 네트워크 보안