융합보안관제 시스템의 효율성 향상을 위한 이벤트 분류 및 처리에 관한 연구

김 성 일*, 김 종 성*

요 약

글로벌 IT 시장조사기관인 IDC의 조사에 따르면 국내 융합보안 시장은 2010년 기준으로 1조 7,000 억 원 규모였으며, 이후 매년 32%씩 성장해서 2018년에는 12조 8,000 억 원 규모가 될 것으로 전망하고 있다. 이처럼 전 세계적으로 융합보안의 중요성은 증가하고 있다. 기존의 융합보안관제 솔루션은 다양한 솔루션시스템(방화벽, 네트워크 침임 탑지 시스템 등) 및 장비들(CCTV, Access Control System 등)로부터 수집된 데이터를 기반 하여 이벤트를 발생시키고, 이를 보안관제 요원들이 상황을 판단 및 조치하는 방식으로 구성되어 있다. 하지만 최근 IoT 산업의 발전으로 IoT 장비들의 수가 급격히 증가하고 있고, 이러한 장비들이 보안관제에 사용될 수 있음에 따라 발생할 수 있는 이벤트의 양 역시 증가할 것이다. 물론 많은 이벤트들을 통해 보다 더 많은 상황에 대한 판단 및 조치를 할 수 있는 이점은 있지만, 반대로 너무 많은 이벤트들을 처리해야 하는 부담감 역시 존재한다. 따라서 본 논문에서는 융합보안관제 시스템에서 발생 할 수 있는 이벤트들을 3가지 종류로 구분 짓고, 효과적으로 이벤트들을 분류 및 처리할 수 있는 모델을 제안하여 융합보안관제 시스템의 효율성을 향상시키고자 한다.

A Study on Classification and Processing of Events to Improve Efficiency of Convergence Security Control System

Kim Sung Il*,Kim Jong Sung*

ABSTRACT

According to a research by global IT market research institute IDC, CSIM(Converged Security Information Management) market of Korea was estimated to be 1.7 trillion KRW in 2010, and it has grown approximately 32% every year since. IDC forcasts this size to grow to 12.8 trillion KRW by 2018. Moreover, this case study exemplifies growing importance of CSIM market worldwide. Traditional CSIM solution consists of various security solutions(e.g. firewall, network intrusion detection system, etc.) and devices(e.g. CCTV, Access Control System, etc.). With this traditional solution, the the data collected from these is used to create events, which are then used by the on-site agents to determine and handle the situation. Recent development of IoT industry, however, has come with massive growth of IoT devices, and as these can be used for security command and control, it is expected that the overall amount of event created from these devices will increase as well. While massive amount of events could help determine and handle more situations, this also creates burden of having to process excessive amount of events. Therefore, in this paper, we discuss potential events that can happen in CSIM system and classify them into 3 groups, and present a model that can categorize and process these events effectively to increase overall efficieny of CSIM system.

Key words : Convergence Security, Security Management System, Event Classification

접수일(2017년 8월 24일), 수정일(1차: 2017년 9월 23일), 게재확정일(2017년 9월 27일)

* SK / 융합서비스개발그룹
** SK / 융합서비스개발그룹

1. 서 론

최근 다양한 분야에서 융합보안관제의 필요성이 증가하고 있다. 융합보안관제는 범죄 예방, 교통 관리, 공항, 철도, 관공서와 같은 중요 시설 및 공장과 연구시설의 보호 등 여러 분야에서 활용이 되고 있으며, IoT 기술의 발전에 따라서 다양하고 폭 넓은 정보를 바탕으로 더 많은 분야에서 활용될 수 있을 것이다. 이와 관련해서 IDC(International Data Corporation)에서는 융합보안 시장의 성장 가능성을 높게 예측했으며, 국내 융합보안 시장은 2010년 약 1조 7,000 억 원으로 정보보안시장 규모인 1조 3,000 억 원을 넘었으며 2018년까지 연평균 32% 성장하여 12조 8,000억 원에 이를 전망이라는 조사 결과를 발표했다[1].

기존의 물리보안관제 시스템은 다양한 이기종 장비들 (CCTV, Access Control System, Fire Alarm System 등)으로부터 오는 데이터들 중 비정상적인 데이터를 시스템에서 판단하여 사람에게 이벤트로 알림으로써 처리하는 방식이다. 마찬가지로 정보보안관제 시스템에서는 정보유출, 해킹 등과 같은 네트워크 공격을 시스템에서 감지하여 사람에게 알림으로써 처리하는 방식이다. 물리보안, 정보보안 그리고 두 가지 영역을 동시에 담당하는 융합보안에 있어서 중요한 요소 중 한 가지는 보안관제를 수행하는 사람이다. 따라서 관제를 수행하는 사람에게 많은 이벤트들을 효과적으로 분류하여, 어떤 이벤트가 발생했는지, 해당 이벤트의 중요도나 정확성은 얼마나 되는지를 잘 알려주는 것이 중요하다.

본 연구는 효율적인 융합보안관제 시스템을 구성하기 위해서, 각 장비와 시스템으로부터 전달되는 이벤트들을 효율적으로 분류하고 처리하는 모델을 수립하는 것이 목적이다.

제 2장에서는 보안관제의 정의 및 필요성과 보안관제시스템에 대한 개요를 살펴보고, 제 3장에서는 이벤트 분류 및 처리 모델을 설계하며, 제 4장에서는 적용 예시를 통한 기대 효과를 정리한다. 마지막으로 제 5장에서는 연구 결과를 정리한다.

2. 관련 연구

2.1 보안관제의 정의 및 필요성

보안관제는 증가하는 보안위협으로부터 보호 대상을 효율적으로 보호하기 위해 감시 및 제어하는 일련의 과정을 통칭하며 크게 ① 물리보안, ② 정보보안, ③ 융합보안으로 구분된다.

물리보안, 정보보안, 융합보안의 정의 및 대표 제품은 <표 1>에서 볼 수 있고, 효과적이고 효율적인 보안을 위해서는 물리보안과 정보보안을 모두 포함하는 융합보안이 필요함을 알 수 있다[3].

과거에는 정보보안의 중요성으로 인해 물리보안의

<표 1> 지식 정보 보안 산업 기술 분류

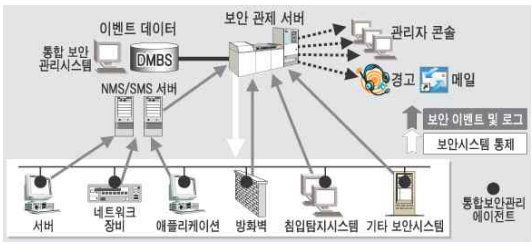
구분	정의	대표 제품
물리보안	개인의 신변 안전 및 주요 시설물의 안전한 관리 환경 구축을 위한 개인 식별, 영상 감시, 재난·재해 방지 등을 위한 보안 기술	출입통제, 영상 감시 솔루션, 지능형 카메라, 바이오 인식 등
정보보안	컴퓨터 또는 네트워크상의 정보의 훼손·변조·유출 ① 공통 기반 보안: 암호, 인증 ② 네트워크·시스템보안: 사이버 침해 대응 등 ③ 응용·서비스보안: IT서비스 등	방화벽, 안티바이러스, 포렌식 툴, 디지털 포렌식 툴, DDoS 대응 장비 등
융합보안	정보 보안과 물리 보안 간의 융합 또는 IT기술과 타 산업간 융·복합 시에 발생되는 보안 위협을 해결하기 위한 보안 기술	차량 블랙박스, u-헬스케어, 보안 장비, 스마트 미터 보안칩

중요성을 낮게 보는 경향이 있었으나, 최근 가장 기초가 되는 물리보안이 취약하면 다른 보안들의 안정성도 보장할 수 없다고 인식되기 시작했다. 실제로 2014년 초에 발생한 모 카드사의 개인정보유출 사고는 데이터를 지키는 보안시스템의 문제라기보다는 협력사 직원이나 내부 직원에 의한 유출 때문에 발생한 문제였다[4].

이처럼 보안사고는 보안시스템 뿐만 아니라 사람에 의해서도 발생할 수 있으며 이는 곧 기업의 정보 유출이나 개인정보 유출 등 큰 사회적 이슈를 일으킬 수 있다. 이에 따라 효율적인 융합보안관제 시스템을 통한 자산 및 정보 보호가 중요해지고 있다.

2.2 보안관제 시스템

보안관제 시스템은 등록되어 있는 장비들로부터 수집된 데이터와 그 외 서버나 어플리케이션의 로그(Log) 데이터를 수집하여, 정상 이벤트와 비정상 이벤트로 분류한다. 비정상 이벤트의 경우 시스템 화면이나 유·무선으로 보안관제 요원에게 알리는 기능을 수행한다. 일반적인 보안관제 시스템의 구성도는 (그림 1)과 같으며 실질적으로 해당 이벤트에 대한 조치는 관제요원이 수행한다[5].



[출처: 전자신문 ET통계 2005.01.07]

(그림 1) 보안관제시스템 구성도

하지만 기존에 데이터를 발생시킬 수 있는 장비들의 수가 IoT 산업의 발전으로 점차 매우 빠른 속도로 늘어나고 있다. 한국과학기술정보연구원의 조사 결과에 의하면 인터넷에 연결 가능한 다종다양한 기계 및 통신장비 등, 사물(things)은 (그림 2) 그래프에서 볼 수 있듯이 2010년 약 40억 개, 2012년 약 150억 개에서 2020년에는 800억 개까지 증가하여 사물인터넷 인프라의 급격한 확대를 예고하고 있다[6].

(그림 2) IoT에 연결 가능한 사물 증가 추이

이처럼 무수히 많은 장비들로부터 들어오는 데이터들에 대해 효율적으로 보안관제를 수행하기 위해서는 이벤트들을 효과적으로 분류 및 처리할 수 있는 모델이 필요하다.

3. 이벤트 분류 및 처리 모델

융합보안관제 시스템은 다양한 보안 솔루션 시스템(이하, 하부 시스템) 및 장비들로부터 데이터를 수집하고 이를 기반으로 이벤트를 발생시킨다. 발생된 이벤트의 경우 보안관제 시스템이 자동으로 처리하거나, 관제 요원에 의해서 원격 또는 현장에서 처리하게 된다. 하부 시스템 및 장비가 많아질수록 서버로 수신되는 데이터들이 많아지고, 이에 따라 발생하는 이벤트의 수가 증가하게 된다. 기존의 융합보안관제와 관련된 연구에서는 이벤트들의 수집 방법의 효율성 상승 및 이벤트들의 종류에 따라 분류하는 방법에 관한 연구가 대부분이었다[7][8].

효율적인 관제를 위해서는 수집되는 데이터를 바탕으로 단순히 데이터의 종류(영상 데이터, 센서 데이터 등)만으로 이벤트를 분류 하는 것이 아니라, 그러한 이벤트들의 상위 개념의 이벤트를 정의 및 분류해서 처리를 할 수 있도록 해야 한다.

본 장에서는 이벤트 분류 방법 및 분류된 이벤트 처리 방법에 대해서 알아본다.

3.1 이벤트 분류

이벤트는 융합보안관제 시스템에서 업무의 기본이 되는 단위이다. 융합보안관제 시스템의 대부분의 업무는 이벤트로부터 시작 된다. 따라서 이벤트를 효과적으로 분류하는 것만으로도 융합보안관제 시스템의 효율성을 향상 시킬 수 있다.

본 연구에서는 이벤트를 3가지로 분류한다.

① 일반 이벤트

② CEP(Complex Event Processing) 이벤트

③ SOP(Standard Operating Procedures) 이벤트

3.1.1 일반 이벤트

일반 이벤트는 하나의 장비 또는 하부 시스템으로부터 수신된 정보를 바탕으로 발생되는 단일 이벤트로, 그 예시는 다음 <표 2>와 같다.

<표 2> 일반 이벤트 예

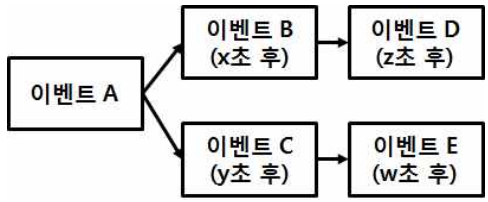
장비/하부시스템	송신 데이터	발생 이벤트
CCTV	물체 감지	물체 감지
	네트워크 끊김	CCTV 네트워크 연결 끊김
	연결 상태 양호	없음
출입문	출입문 열림	없음
	출입문 닫힘	없음
	출입문 비정상 개폐	비정상 개폐
네트워크 방화벽	이상 징후 탐지	방화벽 공격
연기 감지 센서	연기 감지	화재 징후 감지
불꽃 감지 센서	불꽃 감지	화재 징후 감지
…	…	…

<표 2>에서 볼 수 있듯이 장비 또는 하부 시스템은 보안관제 시스템에게 다양한 데이터를 송신한다. 보안관제 시스템에서는 수신하는 데이터를 모두 이벤트로 발생시키는 것이 아니라 해당 정보들로부터 관제에 필요한 데이터들만 선별하여 이벤트로 등록해서 관제에 사용한다. 관제를 수행하는 목적, 적용 장소에 따라서 이벤트로 등록되는 항목들을 다르게 설정 된다.

일반 이벤트가 발생하면 관제 시스템에 알람이 발생하고 시스템마다 등록된 프로세스에 따라 관제요원이 처리하게 된다.

3.1.2 CEP 이벤트

CEP(Complex Event Processing) 이벤트는 다양한 종류의 이벤트들로부터 발생되는 복합 이벤트이다.



(그림 3) CEP 이벤트 정의 예시

(그림 3)은 CEP 이벤트 정의의 한 예시이다. CEP 이벤트는 (그림 3)에서 볼 수 있듯이 단순 이벤트들의 조합으로 정의 할 수 있다. (그림 3)에서 정의된 CEP 이벤트의 경우, 다음 ①, ② 경우에 대해서 동일한 CEP 이벤트로 간주된다.

① 이벤트 A가 발생한 후 x초 후, 이벤트 B가 발생하고, z초 후 이벤트 D가 발생

② 이벤트 A가 발생한 후 y초 후, 이벤트 C가 발생하고, w초 후 이벤트 E가 발생

이처럼 여러 이벤트들의 발생 경우의 수를 묶어 하나의 CEP 이벤트로 정의할 수 있기 때문에 장비나 하부 시스템으로부터 수신되는 데이터의 활용 범용성을 높일 수 있다.

CEP 이벤트는 크게 2가지 역할을 수행할 수 있다.

첫째, 보다 정확한 상황 판단을 할 수 있도록 도와준다. 하부 시스템 또는 장비에서 보안관제 시스템으로 전달하는 데이터들 중 일부는 장비의 오작동이거나, 실제로 위협이 발생하지 않은 상태일 수도 있다. 이러한 상황을 보다 정확하게 알기 위해서는 유사한 기능을 수행하는 관련 장비들의 데이터들 함께 참조하면 이벤트의 정확성을 높일 수 있다. 예를 들어 화재 감지의 경우 불꽃 감지 센서, 연기 감지 센서, 온도 감지 센서 등과 같은 연관 장비들의 알람을 함께 수신해서 화재를 판단한다면 관제 시스템의 효율 및 정확도

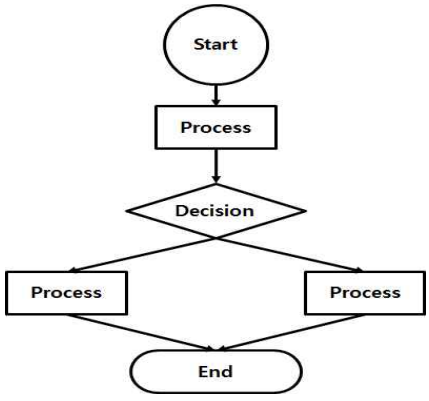
가 상승한다.

둘째, 이기종 시스템 및 장비로부터 발생하는 이벤트로부터 새로운 상황에 대한 이벤트를 발생시킬 수 있다. 예를 들어 서버가 있는 구역을 관제하는 CCTV에 사람의 움직임이 포착되고, 이어서 보안 시스템에서 비 인가된 네트워크 접근이 탐지 된다면, 이는 정보 유출과 관련된 사고라는 CEP 이벤트로 정의 할 수 있을 것이다.

이처럼 CEP 이벤트는 각각 연관성이 있거나 혹은 없는 일반 이벤트들을 기반으로 새로운 종류의 이벤트를 발생시킬 수 있기 때문에, 폭 넓은 관제를 할 수 있도록 도와준다.

3.1.3 SOP 이벤트

SOP(Standard Operating Procedures) 이벤트는 일반 이벤트 또는 CEP 이벤트들 중 표준 운영 절차에 따라서 처리해야할 이벤트들이다. SOP 이벤트들은 (그림 4)와 같은 절차에 의해서 처리된다. 각 이벤트들은 처리 성향에 따라 더 단순하거나, 복잡한 처리 절차에 따라 대응 할 수 있도록 설정할 수 있다. 보안관제 시스템에 등록된 일반 이벤트 및 CEP 이벤트 중 SOP 절차에 따라서 처리해야 할 이벤트들은 SOP 이벤트로 등록해서 처리한다.

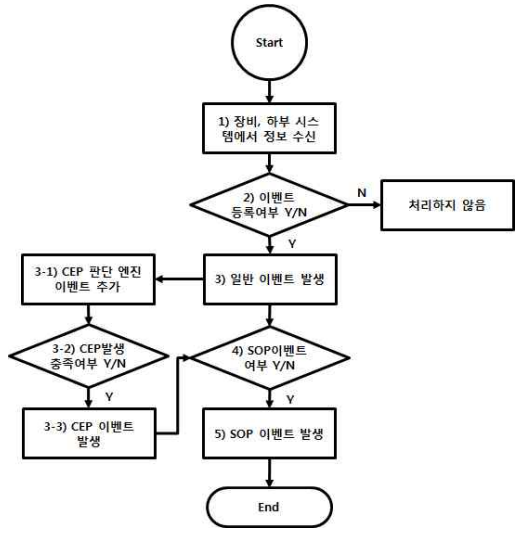


(그림 4) SOP 다이어그램 예시

SOP 이벤트는 처리해야 할 절차가 명확하며, 상황에 따른 가이드가 되므로, 긴급 상황이나 중요도가 높은 이벤트를 처리함에 있어서 대응 절차가 누락되지 않도록 무결성을 높여줄 수 있다. 또한 대응 절차가 시스템에 이미 반영되어 있으므로, 조치 효율성을 높일 수 있다.

3.2 이벤트 분류 모델

다수의 하부 시스템 또는 장비로부터 전달되는 데이터를 바탕으로 일반 이벤트, CEP 이벤트 그리고 SOP 이벤트로 분류를 할 수 있는 모델의 알고리즘은 (그림 5)와 같다.



(그림 5) 이벤트 분류 모델의 알고리즘

(그림 5)에서 제시한 알고리즘에 대한 상세 설명은 다음과 같다.

1) 장비 및 하부 시스템에서 융합보안관제 시스템으로 데이터를 전송한다.

2) 융합보안관제 시스템은 수신한 데이터로부터 사전에 이벤트로 정의된 정보들인지 판단 한 후 이벤트로 등록되어 있을 경우 처리하지 않으며, 이벤트 일 경우 3번 과정을 수행한다.

3) 이벤트로 등록되어 있는 데이터에 대해서 일반 이벤트를 발생시킨다. 동시에 3-1 과정을 수행한다.

4) 3번에서 발생한 일반 이벤트가 SOP 이벤트로 등록되어 있는지 판단한다. SOP 이벤트로 등록되어있지

않으면 추가적인 처리를 하지 않는다.

5) 3번에서 발생한 일반 이벤트가 SOP 이벤트로 등록되어 있었다면, SOP 이벤트를 발생시킨다. 그 이후 표준 처리 절차에 따라서 이벤트를 처리하도록 한다.

3-1) 3번에서 발생한 일반 이벤트를 CEP 판단 룰 엔진에 추가한다.

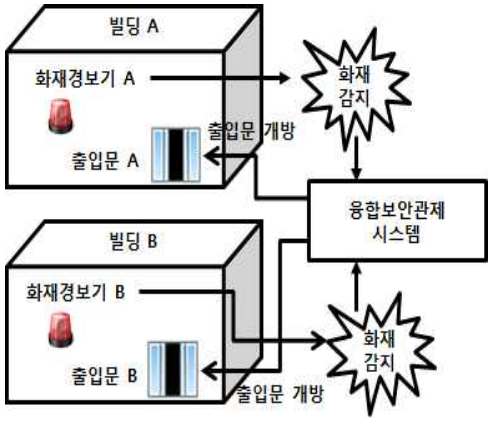
3-2) 룰 엔진에서 새로 추가된 이벤트가 CEP 정의에 등록되어있는 조건을 충족시켜서, CEP 이벤트가 발생하는지 확인한다. 충족되는 CEP 이벤트가 없을 경우 데이터만 유지하고 추가적인 처리를 하지 않는다.

3-3) CEP 이벤트 기준을 충족하면 CEP 이벤트를 발생시킨다. 해당 CEP 이벤트가 SOP 이벤트로 등록되어있는지 확인하기 위해 4번 SOP 이벤트 판단 여부를 수행하며 이후 과정은 일반 알람과 같다.

3.3 이벤트 처리 모델

융합보안관제 시스템은 발생한 이벤트들에 대해서 관제 요원이 조치를 취하고 그에 대한 로그(Log)를 기록하는 방식으로 이벤트를 처리한다.

정형화된 이벤트의 경우 이벤트에 대한 조치 내용이 유사하다. 따라서 이벤트에 대한 조치 과정 중 일부를 자동으로 수행할 수 있도록 시스템을 설계한다면, 이벤트에 대한 대처를 신속하게 할 수 있다. 이러한 자동 조치 기능은 각 하부 시스템 및 장비와 연계 될 수 있도록 시스템을 설계해야 한다.



(그림 6) 자동 조치 모델 예시

예를 들어 화재관련 자동 조치 모델은 (그림 6)과 같이 설계할 수 있다. 빌딩 A에 설치되어 있는 화재경보기 A에서 화재를 감지했을 때, 해당 장비에 설정되어 있는 자동 조치 내용이 출입문 A의 개방이라면, 관제요원이 이벤트를 확인하고 조치하기 전에 자동으로 출입문을 개방되므로, 인명피해를 최소화 할 수 있다. 같은 방식으로 화재경보기 B에 대해서도 자동 조치 모델을 등록 할 수 있다.

자동 조치가 시스템에 의해서 수행된 이후에 처리 과정은 관제 요원이 수행을 한다. 자동 조치만으로 이벤트에 대한 처리가 충분할 경우 이벤트를 조치 완료로 처리해서 이벤트에 대한 처리를 마무리한다. 추가적으로 조치가 필요한 경우에는 수동으로 조치를 취한다. 발생하는 이벤트들 중에서 SOP 이벤트의 경우 시스템에서 자동으로 대처 가이드를 제공하며, 각 단계별로 관제요원이 사전에 정의된 업무 처리 방식을 따라 이벤트에 대한 처리를 완료한다.

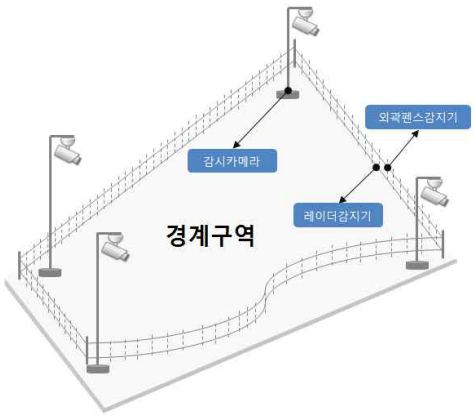
이벤트에 대한 처리가 끝나면 관제 요원은 보안관제 시스템에서 해당 이벤트의 조치 상태를 완료로 설정해서 발생한 이벤트와 관련된 업무를 종료한다.

4. 적용 예시 및 기대 효과

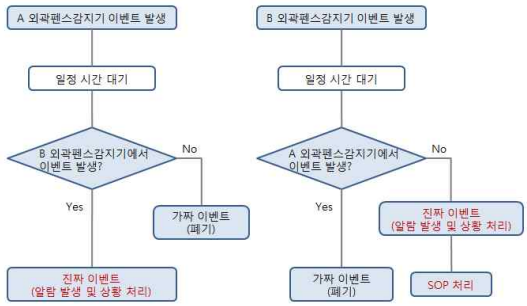
3장에서 언급한 관제 이벤트 분류 및 처리 모델을 현업에 적용한 예시를 통해 그 기대 효과를 알아본다.

4.1 외곽경계 시스템에서의 적용 예시

외곽경계 시스템의 정의를 요약하면 특정 영역의 침입을 감지하기 위한 시스템을 말하고 이는 물리보안 관제 영역의 일부에 속한다. (그림7)처럼 경계구역을 기준으로 경계 부근에 외곽펜스가 설치되어 있고 외곽펜스에는 외곽펜스감지기, 레이더감지기가 설치되어 있으며 경계구역 내에는 곳곳을 감시할 수 있는 감시카메라가 위치 해 있다. 특히 감시카메라는 경계구역 내 전체를 커버할 수 있도록 PTZ(Pan, Tilt, Zoom) 동작을 지원하는 카메라가 설치되어 있다.



(그림 7) 외곽경계 시스템 구성도



(그림 8) 시간 간격 기반 CEP 처리 흐름도

외곽경계시스템은 구축 특성 상 외각펜스를 설치할 수밖에 없고, 그 외각펜스는 외부 환경과 바로 연결되어 있으므로 곳이므로 외부의 간섭에 의해 이벤트가 발생할 가능성이 높다. 그러므로 이벤트에 대한 처리가 필수적으로 필요하다.

최초 외곽경계시스템에서는 외곽펜스감지기에서 이벤트가 발생 할 경우에 대한 대처 방안만 적용하여 운영했다. 그런데 이벤트가 발생해서 현장을 가보니 바람이 불어서 휘날리는 낙엽에 의한 감지이거나, 멧돼지, 고라니 등 산짐승들에 의한 이벤트 등 가짜 이벤트가 대부분이었다.

이를 개선하기 위해 외곽펜스이벤트가 발생할 때 해당 지역의 영상을 볼 수 있도록 감시카메라를 설정하였으나, 이 역시 이벤트가 발생할 때마다 관리자가 영상을 통해 진짜 이벤트인지 가짜 이벤트인지 구별을 해야 한다는 수고가 발생했다.

이 역시 개선이 필요하기 때문에 해당 외곽경계시스템에 CEP 이벤트 모델을 도입하였고, 여러 상황을 기반으로 설계하였다. 예를 들어 두 이벤트간의 시간 간격을 기반으로 진짜 이벤트와 가짜 이벤트를 구별하는 기능은 (그림 8)과 같이 설계하였다.

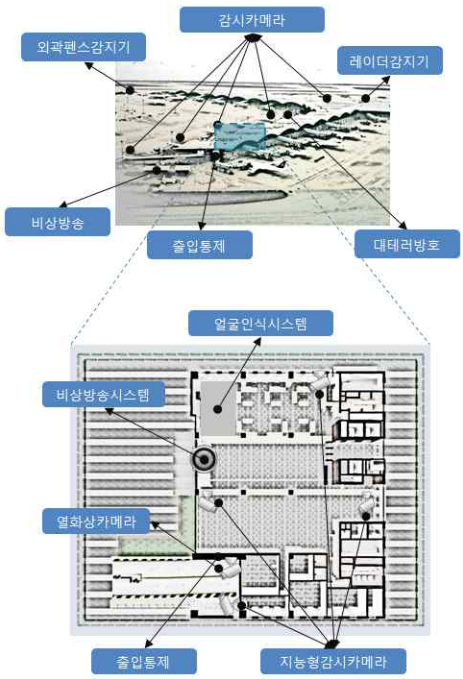
(그림 8) 에서는 A 이벤트 발생 후 일정 시간 후에도 B 이벤트가 발생하면 진짜 이벤트이지만, B 이벤트 발생 후 일정 시간 후에 A 이벤트가 발생하면 가짜 이벤트임을 나타내고 있다.

4.2 공항보안관제 시스템에서의 적용 예시

공항보안관제 시스템의 정의를 요약하면 공항과 같은 사회간접자본(SOC) 시설의 내·외부적인 위협(불법 침투, 입국, 테러, 파괴 등)으로부터 사용자의 안전과 시설을 보호하는 시스템을 말하며 이는 융합보안관제 영역의 일부에 속한다.

(그림 9)처럼 시설물을 제외한 기준으로 경계 부근에 외곽펜스가 설치되어 있고 외곽펜스에는 외곽펜스 감지기, 레이더감지기가 설치되어 있으며 경계구역 내에는 곳곳을 감시할 수 있는 감시카메라가 위치 해 있다. 또한 시설물 내에는 출입통제장치, 지능형 영상 감시 장치, 얼굴인식장치, 비정상 행위 탐지 장치, 열 감지 장치 등 의심되는 사용자를 분별하는 시스템이 구축되어 있다. 또한, 비상통신 시스템, 비상방송 시스템, 경보기, 대테러방호 등 위협상황 발생 시 사용자들에게 알리고 사용자들을 보호하는 시스템도 구축되었다. 이렇게 수많은 장치들이 복합적으로 구축되어 있다.

이러한 공항보안관제시스템은 특성 상 이벤트가 발생할 경우 정해진 조치법에 따라 운용을 해야 한다. 예를 들어, 지능형 영상 감시 장치를 통해 비정상적인 행위를 하는 사용자를 발견하거나 얼굴인식장치를 통해 위험인물을 발견할 경우 근처 출입통제의 게이트를 OFF 시키고, 관련 감시 카메라를 해당 지점을 볼 수 있도록 PTZ 제어 한 후 보안경비대에 비상통신 시스템을 통해 유·무선으로 상황을 알리고 비상방송 시스템을 통해 사용자들에게 알림으로써 향후 발생할 수 있는 위협을 최소화해야 한다.



(그림 9) 공항보안관제 시스템 구성도

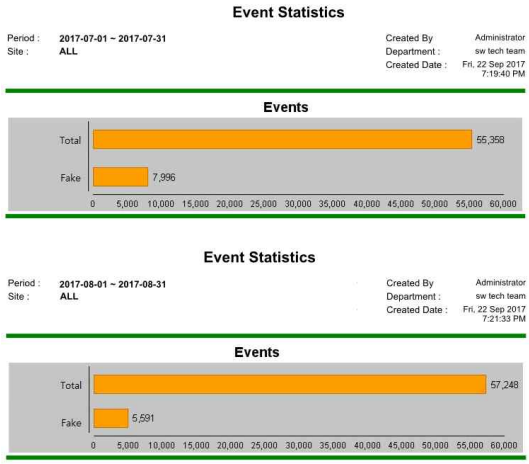
이렇듯 일련의 처리 프로세스가 정해져 있는데, 이를 관제요원이 이벤트가 발생할 때 마다 매뉴얼을 참조하거나 모든 매뉴얼을 미리 숙지한다는 것은 어려운 것이 현실이다. 그러므로 이러한 일련의 처리 과정을 SOP 로 정의하고, 이를 보안관제 시스템에 적용해서 이벤트 발생 시 관제요원이 등록된 SOP 이벤트 처리 절차에 따라 조치할 수 있도록 하였다.

4.3 기대 효과

위의 예시와 같은 상황에서 이벤트들에 대한 CEP 이벤트처리 모델과 SOP 이벤트 모델을 적용한다면, 불필요한 관제를 줄여서 관제의 효율성을 높일 수 있다. 특히 SOP 이벤트를 정의함에 따라 이벤트 처리 과정의 누락을 방지하고 어떠한 관제 요원이 관제를 하더라도 일관성 있는 업무 처리가 가능해지므로, 이벤트 처리의 효율이 높아지게 된다.

(그림 10)은 실제로 해외 T국가에 구축한 보안관제 시스템에서의 CEP 도입 전 후 1개월간의 이벤트 통계 보고서이다. (그림 10)에서 볼 수 있듯이, CEP 이벤트를 정의하지 않고 운영된 7월 한 달간 집계된 전체이벤트 중 가짜 이벤트의 비율은 약 14%(7,996/55,358)이다. 이후 CEP 이벤트 정의를 적용한 8월 한 달간 집계된 전체 이벤트 중 가짜 이벤트의 비율은 약 9%(5,591/57,248)이다. 이를 기반으로 CEP 도입 전 후 가짜 이벤트의 비율이 약 5% 감소되었음을 알 수 있다.

이처럼 상황에 대한 정확한 판단 및 발생한 이벤트의 효율적 처리는 결과적으로 융합보안관제 시스템의 전체적인 성능을 향상시킬 수 있을 것이다.



(그림 10) 공항보안관제 이벤트 보고서

5. 결 론

국가, 기업 그리고 개인의 자산과 정보를 보호하고 안전을 보장하기 위해서, 융합보안관제의 중요성 및 수요가 점점 증가하고 있다. 또한 IoT 장비의 증가와 새로운 보안 문제들이 계속해서 대두됨에 따라 융합보안관제 시스템이 처리해야하는 문제의 종류와 데이터의 양은 이전과 비교가 안 될 정도로 많아지고 있다.

본 연구에서는 융합보안관제의 핵심인 문제 상황에 대해서 높은 정확도의 이벤트를 발생시키는 것과 발생한 이벤트에 대해서 효율적이고 완벽하게 대처할 수 있도록, 이벤트 분류 방법 및 처리 모델을 제시했다.

그러나 시스템이 자동으로 이벤트 분류 및 처리 절차를 등록할 수 없기 때문에 제안된 모델을 잘 활용하기 위해서는 융합보안관제 분야에 대한 지식과 경험

이 필요하다. 누적된 지식과 경험을 바탕으로 본 연구에서 제안한 모델을 적용한다면, 융합보안관제 시스템의 정확성, 처리 속도 등에 향상을 통해 효율성 증가를 기대할 수 있을 것이다.

참고문헌

[1] 한국인터넷진흥원, 국내외지식정보보안동향, 2012.
[2] 박시장, 박종훈, “국내 보안관제 체계의 현황 및 분석”, 한국전자통신학회 논문지, Vol 9, No.2, 2014
[3] 물리보안과 정보보안이 만나 “융합보안” 으로 진화하다, LG CNS IT Solutions/Security blog, 2015
[4] 대한민국의 정보보안 사고 목록, Wikipedia
[5] 보안관제시스템 구성도, 전자신문, 정보통신 ET 통계, 2015
[6] 한국과학기술정보연구원, 유비쿼터스 및 초연결사회 구현을 위한 사물인터넷(IoT) 산업동향, 2015
[7] 하옥현, “산업보안을 위한 융합보안관제시스템에 관한 연구”, 한국융합보안학회 논문지, 제9권 4호, 2009
[8] 고근호, 이성렬, 안성진 “산사물인터넷 환경에서의 보안 관제 방향에 관한 연구”, 한국융합보안학회 논문지, 제15권 5호, 2015.

〔저자소개〕

김 성 일 (Sung-Il Kim)
2014년 2월 서강대학교 컴퓨터공학과 (공학학사)
2016년 2월 서강대학교 컴퓨터공학과 (공학석사)
2016년 ~ 현재 (주) SK 선임연구원
email : joongjum@sk.com

김 종 성 (Jong-Sung Kim)
2004년 2월 한국외국어대학교 정보통신공학과 (공학학사)
2006년 2월 한국외국어대학교 정보통신공학과 (공학석사)
2006년 (주)네이버시스템
2016년 ~ 현재 (주) SK 수석연구원
email : ziippy@sk.com