융합보안관제시스템 개선에 관한 연구

이동휘* · 하옥현**

요 약

국가정보원 자료에 의하면, 산업기술 유출로 인한 피해액은 수십 조원에 이르고 있고, 피해유형은 내부자 유출, 공동연구, 해킹, 불법유출, 위장합작 등으로 나눌 수 있으나 그 중 80%가 물리적인 보안과 연계된 내부자 유출로 나타나고 있다. IT와 비IT의 융합이 가속화되고 영역간의 경계 및 구분이 불명확해지면서 정보보호산업은 점차 지식정보보안산업으로 확대되는 개인정보보호중심으로 지속적으로 성장해왔으나, 향후 정보보호산업은 IT 보안기술 및 제품간 융합, IT 보안과 물리 보안간 융합, IT 융합산업보안으로 집중된다. 본 논문에서는 기업 정보유출 방지를 위해서 논리적 보안과 물리적 보안이 모두 동일 수준에서 관리 되어야 하며, 특히, 물리적인 보안시스템(출입통제시스템, 영상보안시스템 등)과 IT 통합보안관제시스템의 융합으로 외부 공격 및 내부자 유출의 예방, 차단, 분석의 시너지효과를 극대화 할수 있는 융합보안관제시스템 개선 모델을 제안 한다.

A study on Improved Convergence Security Monitoring System model

DongHwi Lee* · Ok Hyun Ha**

ABSTRACT

According to the NIS, damages due to leaking industrial technology are reaching tens of trillion won. The type of damages are classified according to insider leaks, joint research, and hacking, illegal technology leaks and collaborated camouflaged. But 80% of them turned out to be an insider leak about connecting with physical security. The convergence of IT and non IT is accelerating, and the boundaries between all area are crumbling. Information Security Industry has grown continuously focusing Private Information Security which is gradually expanding to Knowledge Information Security Industry, but Information Security Industry hereafter is concentrated with convergence of IT Security Technology and product, convergence of IT Security and Physical Security, and IT convergence Industry Security. In this paper, for preventing company information leaks, logical security and physical security both of them are managed at the same level. In particular, using convergence of physical security systems (access control systems, video security systems, and others) and IT integrated security control system, convergence security monitoring model is proposed that is the prevention of external attacks and insider leaks, blocked and how to maximize the synergy effect of the analysis.

Key words : Convergence Security, Enterprise Security Management, Event Monitoring

접수일(2011년 10월 10일), 수정일(1차: 2011년 10월 15일), 게재확정일(2011년1 10월 18일)

* University of Colorado Denver, Dept. of Computer Science and Engineering
** 호남대학교 경찰법행정학부 (교신저자)

1. 서 론

국가정보원 자료에 의하면, 산업기술 유출로 인한 피해액은 수십 조원에 이르고 있고, 피해유형은 내부자 유출, 공동연구, 해킹, 불법유출, 위장합작 등으로 나눌 수 있으며, 그 중 80%가 물리적인 보안과 연계된 내부자 유출로 나타나고 있음. 향후 10년간 피해액은 5,000조 이상에 이를 것으로 예상 되며, 융합보안 관제 제품의 개발로 내부유출 피해를 줄일 수 있는 계기가 되며, 국가 산업기술의 파수꾼 역할을 기대하고 있음.

IT와 비IT의 융합이 가속화되고 영역간의 경계 및 구분이 불명확해지면서 정보보호산업은 점차 지식정보보안산업으로 확대되는 개인정보보호중심으로 지속적으로 성장해왔으나, 향후 정보보호산업은 IT 보안기술 및 제품간 융합, IT 보안과 물리 보안간 융합, IT 융합산업보안을 골자로 하는 지식정보보안산업으로 확대됨.

산업보안 기술유출 방지를 위해서는 논리적 보안과 물리적 보안을 모두 동일 수준에서 관리 되어야 하며, 특히, 물리적인 보안시스템(출입통제시스템, 영상보안시스템등)과 IT 통합보안관제시스템의 융합으로 외부공격 및 내부자 유출의 예방, 차단, 분석의 시너지효과를 극대화 할 수 있음.

제 2장의 국내외 관련 기술의 현황을 통해서 보안관제의 종류와 방법에 대한 변천과정을 살펴보고 제 3장에서는 융합보안관제 모델을 설계하고 제 4장에서는 관련 내용을 검증하고, 5장에서는 파급효과와 논문에 한계에 대해 논 한다.

2. 관련 연구

2.1 보안관제의 개념

지금 까지 전산망 보안관제에 관해 법 규정이나 학술적으로 개념 정의가 되어 있지 않은 실정이다.

사전적 의미는 컴퓨터의 프로그램 수정 중 일어날 수 있는 여러 가지 오류에 대비하기 위한 감시활동이라고 설명되어 있으며[1], 외국의 경우에는 보안관제에 관해 네트워크 트래픽 분석도구를 이용하여 24시간 서버와 네트워크를 통해 통신한 방대한 데이터에서 잠재적인 침입자의 공격시도를 규명하는 일련의 행위[2]라고 정의한 바 있다.

국내의 정보유출 방지를 위한 노력은 문서보안, USB보안, 매체제어, 안티바이러스, 방화벽 등 사이버 분야에서의 단위 솔루션 제품에서 시작되고 있으나, 여전히 네트워크 수준의 사이버 보안 차원에서의 관리가 주를 이루고 있음. 관리적 차원에서는 아직 초기 단계의 기술 적용과 제품의 사업화 단계이어서 목표 시스템과의 직접적 경쟁관계에 있는 제품은 뚜렷하게 발생하지 않고 있다.

2.2 융합보안의 개념

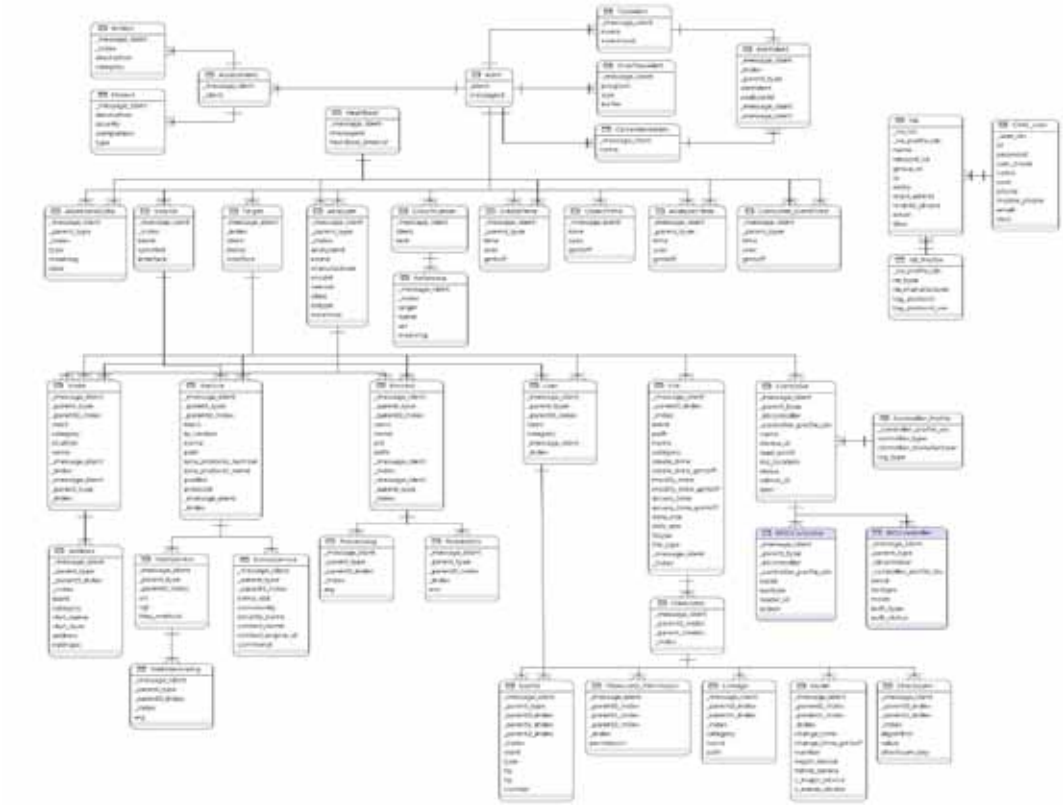
현재 융합보안에 대한 정의는 국제적으로 표준화되지 않았지만, 다양한 연구기관에서 제시되고 있다. 우선 ASIS(American Society for Information Science)에서는 “융합”에 대한 정의를 “기업 내에 존재하는 비즈니스 기능과 프로세스 사이의 상호 의존성 및 보안위험을 식별하고, 이를 적절하게 관리할수 있는 비즈니스 솔루션을 수립하는 것”[3]이라고 정의 하고 있다[4].

융합보안의 비용을 효율적으로 관리하기 위하여 COSO online에서는 전통적인 위험관리 기능을 통합하는 것으로 여기서 통합이란, 인적자원 보안, 사업 연속성, 재난 복구, 위험 관리 등을 논리적, 물리적으로 통합하는 것을 의미한다[5].

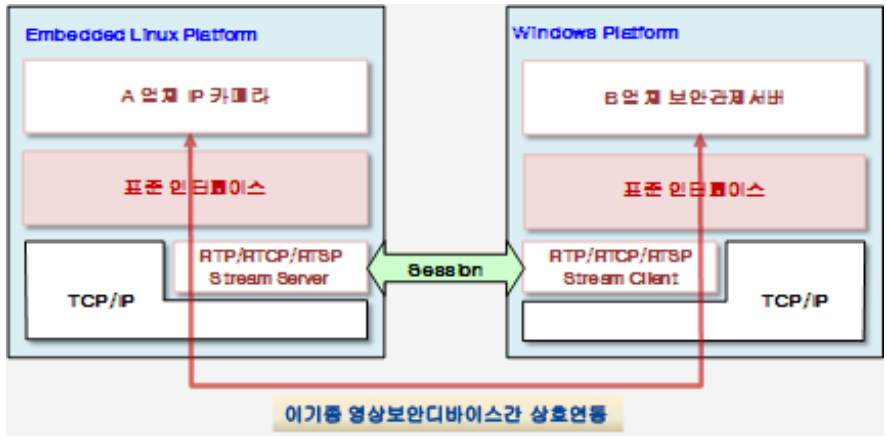
2.3 국내외 현황

상용화 제품의 부재로 인하여, 삼성전자, LG전자와 같은 국내 대기업에서는 정보유출 방지를 위해 높은 수준의 비용을 독자적인 시스템으로 시스템을 구축하고 있음. 사이버 보안관제와 같이 행정분야, 공공분야, 민간기업, 연구소, 국방 분야에서 사용될 수 있는 상용화 제품이 필수적이다.

국외에서는 산업시설의 신뢰성 향상을 위해 이미



(그림 1) 연동설비 보안이벤트 로그속성 설계서



(그림 2) 영상보안디바이스의 표준 인터페이스 탑재로 인한 상호운용 구성도

상용화 제품들이 출시하고 있으며, 물리적 보안시장의 새로운 수요를 창출하고 있다.

- CA사에서는 물리보안제품과 IT보안제품을 통합하여 보안상황을 수집, 분석, 관리하는 eTrust20/20 솔루션을 개발하였음
- GE-Security사는 물리보안과 IT보안기능을 통합한 융합보안제품인 Facility Commander 개발하였음
- AESRM(Alliance for Enterprise Security Risk Management)에서는 IT보안, 물리보안, 인력 및 자산 등에 대한 기업보안 등을 통합 관리하기 위한 기술을 연구하고 있음
- Fuji Xerox사에서는 IT보안과 물리보안을 통합한 AWILS 보안관제솔루션을 개발하였음
- ArcSight사에는 ESM(Enterpise Security Management)과 CCTV시스템이 융합된 산업보안 솔루션을 개발하였다[6].

2.4 영상보안시스템용 표준 인터페이스 개요

현재 다양한 제작 업체에 의해서 개발된 영상보안 디바이스들은 업체별 서로 다른 인터페이스를 가지며, 자체 개발된 프로토콜을 사용하고 있는데, 이러한 문제로 인하여 이기종 영상보안 디바이스간 연동이 어려운 상황이다. 예를 들어, 하나의 영상보안관제서버에서 여러 IP 카메라로 수집된 영상을 동시에 관제하기 위해서는 동일한 제조사에서 제작되고 동일한 프로토콜이 탑재되어 있는 IP 카메라들만 연동할 수 있다. 따라서, 서로 다른 제조사에서 제작된 영상보안디바이스들간의 상호 연동 및 상호 운용성을 제공하기 위해서는 표준화된 인터페이스의 정의가 필요하다. 다음 (그림 2)은 제조사가 서로 다른 영상보안디바이스에 표준 인터페이스 규격에서 정의한 표준 인터페이스의 탑재로 인한 상호연동 구조를 보여준다[7].

3. 융합보안관제 모델

물리적인 보안시스템(출입통제시스템, 영상보안시스템등)과 IT 통합보안관제시스템의 융합으로 기업의 위험관리 및 보안관리를 통하여 내부자 유출을 획기적으로 예방, 차단, 사후추적 등이 필요하다.

- 기존 물리적보안과 IT보안인력의 추가적인 확충이 없어도 단시간 내에 체계적인 융합보안관리 프로세스 확립이 가능해져 전문 조직 체제를 상시 운영하는 효과를 기대할 수 있음
- 네트워크로 전송되는 패킷에 대해 실시간으로 사용자 바이오정보를 투명(transparency)하게 삽입하고 인증하여 데이터 전송 시 산업기술 내부 정보가 외부로 유출되는 것을 방지하는 자동화된 네트워크 이벤트 정보의 생성이 가능하다.

3.1 융합보안설비 보안이벤트의 공통사항을 고려한 표준 포맷 정의

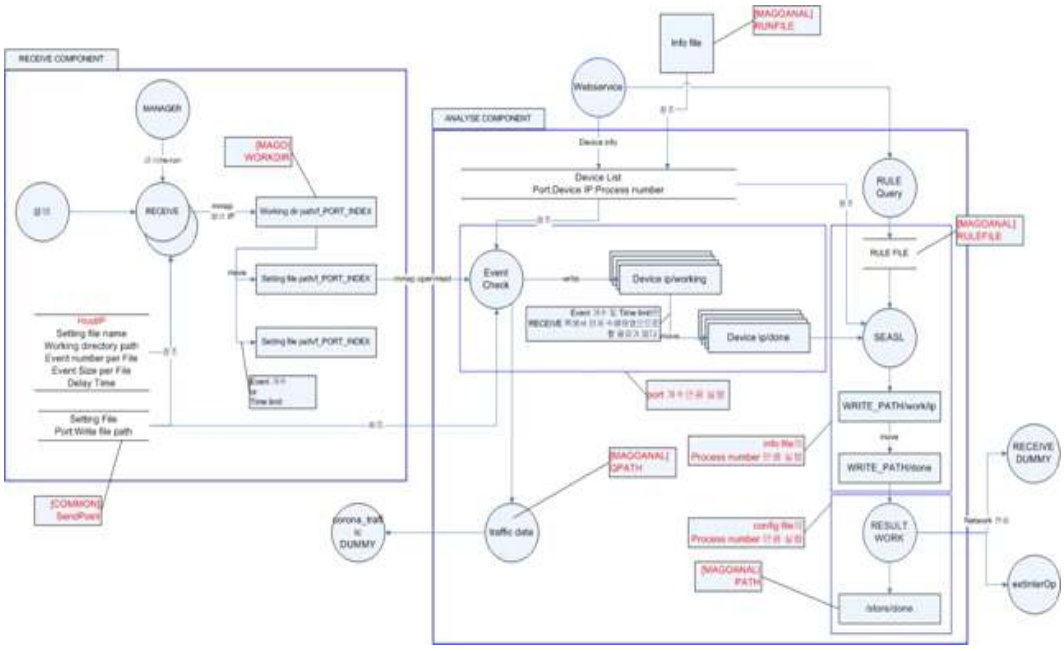
a. 정보보호설비 별 상이한 보안이벤트의 역할 및 이벤트의 파라미터 정의
  - 보안이벤트의 상호 참조 분석이 가능하도록 이벤트 공통 형식 정의
  - IDMEF(Intrusion Detectin Message Exchange Format)의 기반하에 출입통제 및 융합보안설비 수용토록 정의함

b. IDMEF 기반의 이벤트 파라미터 표준화 정의
  - (그림 1)은 각 연동설비의 로그속성에 대한 설계서의 일부이다.
  - 정보설비/정보보호설비/문서유출/출입통제/자산관리 의 이벤트의 내용을 포괄적으로 수용할 수 있는 공통 포맷 정의

3.2 CCTV 연동 표준화 프로토콜 분석

a. 정보유출 및 침해사고의 발생 시 관제시스템에서 영상정보와 이벤트 연계 모니터링을 위한 프로토콜 분석
  - CCTV 영상정보 실시간 전송을 위한 인터페이스
  - CCTV 제어를 위한 제어 인터페이스 분석

b. CCTV NVR/DVR 연동
  - (그림 2)는 영상보안 디바이스와 관제서버간의 인터페이스 상호운용 구성도를 나타낸다.
  - 다양한 상호 연동 인터페이스에 대한 정의가 이루어지고 있음. 단, 개발 목표 시스템은 이벤트 분석시스템과 연계하여 실시간 영상정보 요구를 위



(그림 3) 보안이벤트 수집부 다중프로세서

한 정보 Relay와 사고 추적분석 기능 연계를 위한 과거의 영상정보조회 구현을 위한 기능을 확인하고 이를 활용함. CCTV의 최소한의 국제/국내 표준을 만족하는 제품을 대상으로 함.

3.3 보안이벤트 수집을 위한 멀티프로토콜 지원 이벤트수집 어뎁터

방화벽, 가상사설망, 침입탐지시스템, 침입방지시스템, WEB보안, 통합위협관리시스템, 출입통제시스템, 자산관리시스템, 생체인식시스템 등에서 발생되는 로그 자료는 보안 문제를 일으키는 원인과 이에 대한 해결방안을 제시할 수 있는 근거 자료로써, 이의 효과적인 분석을 통하여 각종 침해사고 발생 시 원인 파악과 명확한 책임 소재를 입증하고, 내부자 또는 비인가자에 의한 불법적인 접근 시도와 악의적인 침입흔적을 파악, 보안정책 수립 자료로 활용함으로써 침해사고를 사전 예방하고 보안관리의 전체적인 효율성을 확보 할 수 있다.

통합 상관 분석 장치는 단일 장비의 로그만을 분석하는 것이 아니라 여러 설비/제조사 이기종 간의 로그를 상관분석 하여 효율적인 보안관리 기능을 제공하는 시스템이다.

로그 수집장치는 정보보호설비들이 제공하는 SYS LOG, SNMP, Binary Format, XML같이 다양한 형식과, 보안 설비별/제조사별로 상이한 전달 방식으로 제공되는 로그를 수집하는 기능을 제공한다.

로그 수집 장치는 아래그림과 같이 프로토콜 별로 로그를 수진하는 Adaptor부분과 전달로그 내용을 분석하는 Format Parser부분 전달된 로그를 IDMEF형태로 변환하는 IDMEF Converter부분으로 구성되어 있다.

a. 기능

- 다중 프로토콜 지원
- 다양한 정보설비 연동 지원 (정보설비, 자산관리, 출입통제 등)
- 정보설비의 보안이벤트 전송기능이 부재한 경우 Agent 소프트웨어를 통한 수집 반영

(그림 4) 융복합 통합보안이벤트 수집

b. 보안이벤트 수집부

(그림 3)은 보안이벤트 수집부 다중프로세서를, (그림 4)는 융복합 통합이벤트 수집 구조를 나타낸다.

- SYSLOG, SNMP, DBMS, Agent Program 의 다수의 수집 프로토콜 지원
- 보안이벤트의 IDMEF 기반 표준화 정의서를 바탕으로 보안이벤트의 정규화 처리 수행 및 실시간 통계 처리
- 초당 12,000 events/sec의 목표 달성

3.4 각종 정보보호설비 및 출입통제 보안이벤트 시뮬레이터

분석시스템의 수집처리 성능, 정규화처리 성능 및 분석처리 성능을 점검

- 융합보안관제시스템의 시험환경을 위한 다양한 네트워크 정보보호설비, 출입통제, 자산관리 시스템 등의 이벤트 생성기 개발
- 다양한 설비와 이들의 로그이벤트의 동시 생성, 분석시스템의 연관분석 기능 확인 가능

○ 이벤트 생성기

- 다양한 정보보호설비 및 융합보안설비의 이벤트 생성기
- 임의의 침해사고 시나리오의 생성 지원

3.5 융합보안관제시스템 설계

a. 기본 핵심 설계 내용

- 다양한 정보보호설비의 이벤트 수집, 실시간 분석과 모니터링
- 보안이벤트, 분석이벤트의 공간 식별과 CCTV 연계 실시간 모니터링
- 식별 이벤트와 CCTV 영상정보의 사후 추적 모니터링

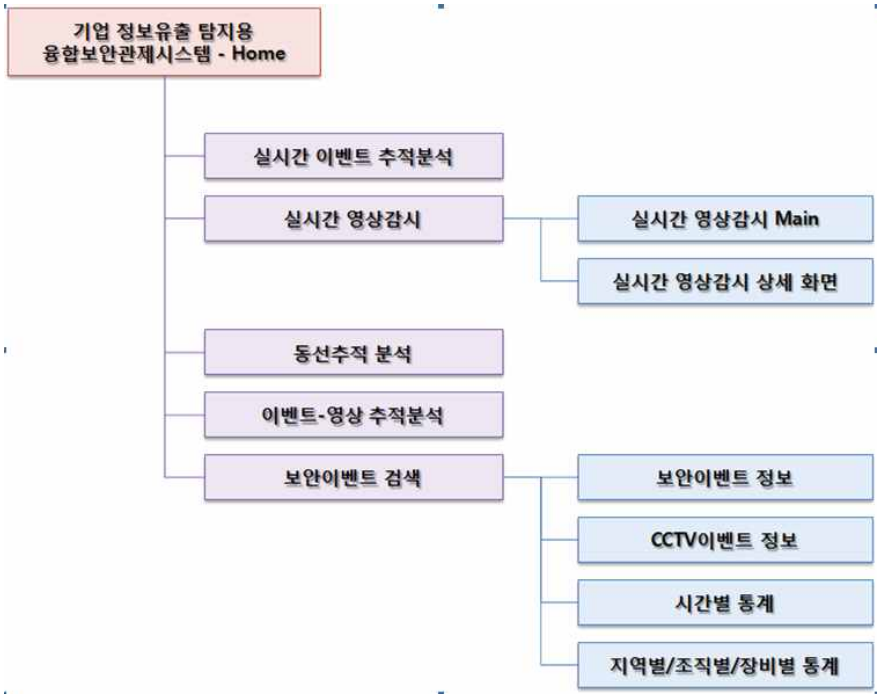
b. 사용자 화면 설계 및 기본 구현

- 실시간 이벤트 감시 및 영상감시 화면
- 실시간 이벤트 분석화면
- 보안이벤트 검색/조회 화면
- 평면도상의 정보자산 관리 및 동선추적분석 화면
- 이벤트/분석결과 영상 추적분석 화면

(그림 5)는 융합보안관제시스템 기본 메뉴트리를 나타낸다

c. DB 및 GUI 화면 설계

- 로그수집엔진 구조 설계



(그림 5)] 융합보안관제시스템 기본 메뉴트리

(그림 6) 융합보안관제시스템 전체 GUI 구성도

- DB 설계서 (환경설정, 통계테이터 관리, 이벤트 데이터관리)
- 문서보안, USB보안, 프린트 Fax 출력물보안, E mail 보안, 출입문보안 등 정보유출탐지 및 출입통제 요소의 통합 이벤트 관리가 적용된 화면 구성
- IT기반의 다양한 정보유출방지 솔루션과 출입통제, 권한관리의 보안이벤트를 상호참조 분석하여 정보유출/보안위배 사항에 대한 패턴 정의 및 실시간 감시가 가능한 화면
- GIS 정보 (지형, 건물) 표시 - 무인 감시/관제 패널
  * 건물의 층간 평면 모델링 화면
  * 동적 Object 설정 기능이 추가되는 지형지물 표시 화면
- 정보유출 탐지 이벤트에 대한 공간인지 및 동선 추적 시각화 분석 표시
  * 시간추이에 따른 이벤트의 도식화 출력 및 출입자 동선 정보의 시각화 처리
  * 건물 평면도에서의 이벤트 정보를 참조한 유출자 동선 시각화 화면
  * 물리적 동선 출력 - 공간적 이동 경로를 출력
  * 논리적 동선 출력 - 원격으로 자산 접근, 사용시에 그 사용 이력을 논리적으로 출력

(그림 6)은 융합보안관제시스템 전체 GUI 구성도를 나타낸다.

- CCTV/출입통제 화면 구성 - 출입통제, IP카메라, 안면인식 기능 동적 연결 (자산 유출입 관리)
  * 보안이벤트와의 CCTV와의 연계를 통한 보안위배사항 및 행위에 대한 직관적 상황 모니터링 화면 구성
  * 보안이벤트 발생시점의 CCTV 조회 영상 출력 기능

4. 보안이벤트 수집 처리 성능 측정

기존 보안관제시스템의 성능을 기준으로, 융합보안관제서비스에서 처리 프로세스의 속도를 측정하여 본 연구의 검증을 하였다.

초당 이벤트	7000	8000	9000	10000	11000	12000	13000	14000
예정 초1	42.86	37.50	33.33	30.00	27.27	25.00	23.08	21.43
소요 초1	43.00	37.00	33.00	28.00	30.00	25.00	24.00	26.00
push1	4.63	4.25	4.36	4.50	4.81	5.93	5.63	5.19
recv1	46.67	34.91	31.44	27.53	25.83	26.82	21.52	19.22
par1	20.23	19.87	21.25	18.79	28.58	20.91	22.70	25.45
초당 처리량1	6976	7588.1	7687.9	7753.29	7785.00	7760.00	7841.00	7887.46

<표 1> 처리프로세스 1

초당 이벤트	7000	8000	9000	10000	11000	12000	13000
예정 초	42.86	37.50	33.33	30.00	27.27	25.00	23.08
소요 초	42.00	36.00	34.00	29.00	28.00	25.00	23.00
push10	5.80	6.00	6.28	6.61	7.03	7.32	7.55
recv10	41.78	36.88	34.22	29.78	28.14	26.29	23.66
par10	3.16	3.22	3.14	3.07	3.20	3.09	3.12
초당 처리량10	7,000	7980.33	8845.53	9990.83	10714.29	12000.00	13043.48

<표 2> 처리프로세스 10

첫 번째로 각 측정결과를 수신후 처리하기 위한 처리 프로세스로 전달되는 과정에서 성능검증을 통해 분석한다.

(그림 7) 시뮬레이터 구성

(그림 7)은 성능평가 방법 구조 이며, 각각 시뮬레이터 설비 : 이벤트 생성 시뮬레이터, corona_mago : 이벤트 수집 프로세스, corona_magolyse : 이벤트 처리 프로세스를 나타낸다.

(그림 7)의 구조에서와 같이 시뮬레이션 결과 <표 1>은 초당 이벤트 수에 따른 처리량을,<표 2>는 같은 방법의 10번째 프로세스를 보여준다.

4.1 테스트 환경

CPU : Intel(R) Xeon(TM) 8 CPU
메모리 :8257240kB
측정장비 : 브레이킹포인트 (BPS 10K)
장비 : 융합보안관제 프로토타입

4.2 테스트 실행환경

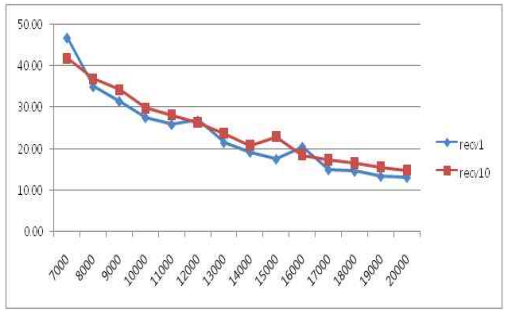
시뮬레이터 설비 : 이벤트 생성 시뮬레이터
corona_mago : 이벤트 수집 프로세스
corona_magolyse : 이벤트 처리 프로세스

4.3 테스트 조건

① UDP 60003 port 사용.
② 시뮬레이터 설비 1대당 초당 2,500 건 발생.
③ 수신 데이터 생성 파일에 저장될 최대 건수 10000 설정.
④ 시뮬레이터 설비 개수를 추가하며 초당 이벤트 발생건수를 늘려 테스트한다.

4.4 테스트 결과

현재 기관에서 활용 가능한 통합보안관제시스템의 처리용량의 목표를 초당 12,000 events/sec로 잡고 테스트 하였다.



(그림 8) 테스트 결과 그래프

<표 3> 테스트 최종결과 표

설비수	초당이벤트발생수	수집부 평균 처리 속도	ma_mago CPU 사용
16	40,000	12,701events/sec	11%

최종테스트 결과 (그림 8), <표 3>과 같이 융합보안관제서비스 조건에 부합하는 결과가 나왔다.

5. 결 론

'광역화', '통합화', '융합화'로 대변되는 사회적인 트렌드에 맞추어 국가에서는 보안분야에서도 통신상의 정보보호 뿐만 아니라 생활 속의 지식정보보안의 중요성을 강조하고 있으며, 이종산업 간 융합 현상이 가속화됨에 따라 정보보호 분야의 융합에 대한 적극적인 지원을 표명하고 있다. 그러므로 본 연구는 각종 소요설비 및 솔루션에 대한 과도한 투자 및 이의 관리 부담을 해소할 수 있으며, 상시 운영을 위한 비용을 최소화 할 수 있는 융합보안관제 모델을 연구하였다.

참고문헌

[1] 김영진외 3명, “국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구”, 정보보안학회논문지, 2009.2

[2] R. Bejtlich, "Tao of Network security monitoring, the beyond intrusion Detection:What is Network Security monitoring, Addison wesley professional, pp40-41, July 2004

[3] Deloitte, "The Convergence of Physical and Information Security in the context of enterprise Risk Management", The Alliance for Enterprise Security Risk Management, 2007

[4] 김정덕외 2명, “융합보안의 개념 정립과 접근방법”, 정보보안학회지, 2009.12

[5] Scalet S.D., "Convergence: Case Study“, COSO online, 2005

[6] 삼성SDS, “융합 보안 시장에 대한 보고서”, 2010

[7] TTAK.KO-12.0117, 영상보안시스템들 간의 상호연동을 위한 인터페이스, 2009.12.22.

[저 자 소 개]

이 동 휘 (DongHwi Lee)

2000년 경기대학교
컴퓨터과학과(이학사)
2003년 경기대학교
정보보호기술공학과
(공학석사)
2006년 경기대학교
정보보호학과
(정보보호학박사)
2011년~현재 University of Colorado Denver, Dept. of Computer Science and Engineering

email : dhclub@naver.com

하 옥 현 (Ok Hyun Ha)

1978년 성균관대학교
정치외교학과(정치학사)
1980년 서울대학교
행정대학원(행정학석사)
1998년 프랑스 사회과학대학원
(EHESS) 박사과정
(DEA 취득)
2005년 고려대학교
정보보호대학원(공학박사)
2008년~현재 호남대학교
경찰법행정학부 교수

email : okclub@empal.com