情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

통신분야 조기경보시스템의 프레임워크

구 자 현*

요 약

본 연구는 망의 가용성이나 보안성을 확보하는 것이 중요한 통신사업자들에게 전국적인 IT 인프라에서 발생하는 해킹이나 기타 보안 위협에 따른 피해를 최소화하고, 위협에 대해서 능동적으로 방어하기 위하여 구축하는 조기경보시스템에 대한 연구이다. 이러한 조기경보시스템을 구축함으로서 해킹, 바이러스, 웜 등의 다양한 전자적인 침해사고 등의 이벤트를 수집, 분류하고 빠른 시간 안에 대응할 수 있는 시스템을 갖추게 된다. 본 연구는 통신사업자가 조기경보시스템(EWIS : Early Warning Information System)을 구축하기 위해서 필요한 프레임워크를 제시하는데 있다.[1]

Ⅰ. 서 론

최근 인터넷의 급속한 확산과 정보통신 기술의 발달은 정치, 경제, 사회, 문화 전반을 획기적으로 변화시키고 있으며 우리의 생활도 많은 변화와 함께 정보화로 인한 편리함을 누리고 있다. 이렇게 온라인화가 진전되면 될 수록 이러한 정보통신의 기본 인프라를 제공하는 통신사업자의 책무가 무거워 지고 있다고 할 수 있다. 예전의 통신사업자는 회선이나 장비의 이중화를 통하여 안정성을 확보하는 것을 주요한 고려 요소로 보았다면 요즘에는 개인정보나 신용카드, 인터넷 뱅킹 정보 등을 불법적으로 획득하거나[2] 다양한 해킹이나 서비스 거부공격 (DoS : Denial of Service; 이하 "DoS"라 한다) 등의 전자적인 침해사고로 인한 네트워크의 폭주 및 심지어는 네트워크의 장애로 인하여 통신사업자 네트워크의 안정성에 심각한 영향을 주고 있다.[3,4]

이에 통신사업자의 네트워크 전체에 대해서 전자적인 침해사고에 대한 조기경보 시스템을 구축하여 망의 안정성이 침해를 받기 전에 미리 대처 할 수 있는 시스템의 구축이 필요하겠다. 이러한 조기경보시스템을 이용하여 조직의 정보보호 담당자가 자신이 보유한 네트워크 및 시스템 자산에 대한 공격이 발생 할 경우 전체 네트워크 및 시스템으로 피해가 확산되기 전 조기에 위협의 규모를 판단하고 대처 방법을 찾을 수 있어야 하겠다.

본 논문에서는 통신사업자 네트워크에 행해지는 전자적인 침해사고에 대한 공격평가와 조기경보가 가능한 조기경보시스템의 설계와 기능에 대한 개념을 논의한다. 본 논문의 구성은 다음과 같다. 2장에서는 조기경보시스템의 정의 및 현재 구축되어 있는 조기 경보시스템의 구축 사례 등을 살펴보고 3장에서는 조기경보시스템을 구성하는 기본적인 프로세스에 대해서 도출하고 4장에서는 조기경보시스템을 구성하는 전체 프레임워크와 프레임워크를 구성하는 각 세부 구성 요건을 제시하고 5장에서는 실제 사례를 적용하여 조기경보시스템의 프레임워크를 구성하는 각 세부 구성요소들이 단계별로 어떻게 적용되는지를 실제 대응 사례 등을 통하여 살펴본다.

Ⅱ. 조기경보시스템의 정의 및 구축 사례

조기경보시스템의 프레임워크를 설계하기 전 조기경보시스템의 정의나 현재 초기에 구축되고 있는 여러 분야의 조기경보시스템 구축사례를 살펴본다.

1. 정의

조기경보 시스템은 바이러스나 웜(Worm)과 같은 전자적인 침해사고에 대한 정보를 수집, 분석하여 이

* (주) 데이콤 보안기술팀 (k55k559@chol.com)
한국정보보호학회 조기경보시스템연구회 WG11 "대형 Test-Bed 연동을통한 신규 취약점/제품/기술 평가" 운영자

를 통해 예측되는 공격을 미연에 파악하여 문제가 확산되기 전 해당 기관이나 사용자들이 취약점과 위협을 사전에 제거할 수 있도록 정보를 제공하는 역할을 수행하는 체계를 말한다.

2. 구축사례

데이콤의 경우 바이러스나 웜에 대한 피해를 조기에 감지하고 대응하기 위하여 전 세계적인 위협정보 및 이상 포트 변동정보를 제공해 주는 위협정보제공 사업자의 정보 및 자체 통신 네트워크에 구축되어 있는 이상 트래픽 탐지 시스템을 통해서 발생하는 이벤트 정보를 가공하고 최신 취약점 데이터베이스와의 연동을 통하여 알려지지 않은 최신 취약점에 의해서 공격을 받는지 등을 신속하게 파악하여 보안 담당자 및 해당 통신망을 이용하는 고객들에게 사전에 경보할 수 있는 초기단계의 조기경보시스템을 구축하여 운영하고 있다.

한국 정보보호진흥원의 인터넷침해사고 대응지원센터의 경우 정보통신망이용촉진 및 정보보호 등에 관한 법률에 의해서 현재 주요 ISP, IDC, 보안 관제업체로부터 수집되는 위협정보 및 트래픽정보 등을 수집하여 민간기관에 대해서 조기경보 할 수 있는 체계가 구축되어 있다.[5]

III. 조기경보시스템을 구성하는 세부 프로세스

조기경보시스템을 구성하는 세부 프로세스로 "스캔 및 탐지", "취약점 인지", "위협·취약점 분류 및 분석", "경보 및 관리"와 "조치"의 5단계로 구분할 수 있다.

1. 스캔 및 탐지

네트워크 및 시스템의 위치나 기능에 따라 트래픽을 모니터링 하는 프로세스로 전체 조기경보시스템 구성요소중 입력부분에 해당된다.

2. 취약점 인지

스캔 및 탐지 등의 실시간 모니터링을 통하여 해킹이나 악의적인 코드, 바이러스 등을 탐지하는 프로세스를 말한다. 이 단계에서는 탐지된 이상트래픽이 이미 구축되어 있는 취약점 데이터베이스와 비교하여 신규 취약점인지 이미 알려진 취약점인지를 빨리 파악하는 것이 중요하다.

3. 위협·취약점 분류 및 분석

탐지된 취약점을 이벤트화하여 위협 및 취약점 정도를 그룹별로 분류하고 위협의 종류 및 경중을 분석하는 프로세스로 위협 및 취약점의 분류(classification) 및 위험의 영향도 (risk impact)를 종합적으로 판단하는 것이 중요하다.

4. 경보 및 관리

이벤트에 따른 위험도를 미리 정의된 위기 경보체

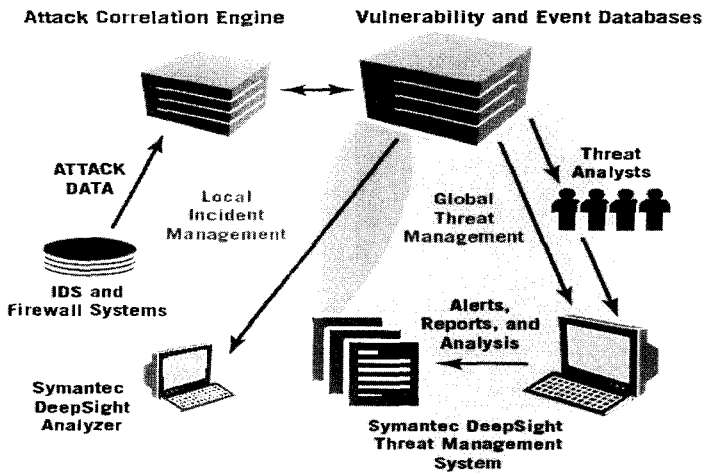

그림 1. 조기 예·경보시스템 구축 구성도

계에 따라 공지 및 대응을 하는 프로세스다. 현재 국가사이버 안전센터의 사이버위기 경보단계에 의하면 국가적으로 5단계의 경보단계를 갖고 있다. 첫째, "심각"단계(Red)는 국내·외 대규모 피해 발생, 기간망 전체에 대한 위협, 국가적 차원에서 네트워크 사용 불가능 및 공동 대처할 필요성이 있는 상황으로 정의 하고 있으며, 둘째, "경계"단계(Orange)는 복수 통신사업자 또는 기간망의 피해 발생, 주요 정보시스템 공격으로 피해 발생, 웜·바이러스 출현 등 대규모 피해 발생, 상황 해결을 위하여 다수 기관의 협조가 필요한 상황으로 정의하고 있으며, 셋째, "주의"단계(Yellow)는 바이러스나 해킹의 출현으로 일부 피해가 발생하거나 이상 징후의 예상·감지, 시스템의 악의적 도용 또는 정보시스템 전반에 걸쳐서 보안태세를 강화할 필요성이 있는 상황으로 정의하고 있으며, 넷째, "관심"단계(Blue)는 심각한 컴퓨터 웜이나 바이러스 및 해킹 기법의 출현 및 신종 사이버위협 출현으로 인한 피해 발생 가능성의 증대 및 해외에서 피해가 확산된 사이버 위협의 국내 유입 가능성의 증대로 정의하고 있으며 마지막으로 "정상"단계(Green)는 전 분야에 걸쳐서 정상적이며 위협도가 낮은 웜이나 바이러스 등이 발생하거나 위험도가 낮은 해킹기법이나 보안취약점이 발표되는 시기로 정의하고 있다.[6]

5. 조치

미리 정의된 위협에 따른 조치 방법에 따라 프로세스 재이행 및 위협에 대한 리포팅, 이벤트 데이터베이스 저장 및 분류, 해당 위협에 대한 네트워크 및 시스템 자원에 대한 보호대책을 수행하는 단계이다.

Ⅳ. 조기경보시스템 프레임워크

이 장에서는 조기경보시스템을 구성하는 상세 프레임워크에 대해서 구체적으로 살펴본다. 조기경보시스템은 선행단계로서 해킹 및 위협에 대한 정확한 분류(Classification)가 매우 중요하다. 네트워크 및 시스템 상에 위협을 가져다 줄 수 있는 모든 해킹 및 위협관련 정보에 대해서 인지를 하고, 이를 바탕으로 각각의 성격에 따른 정확한 분류가 선행되어야 하며 이러한 체계는 신규 취약점 및 해킹에 대해서도 지속적으로 유지되어야 한다.

조기경보시스템은 크게 센서, 데이터 & 이벤트 처리 단계, 상관관계 분석엔진(Correlation Engine), 경보 및 이벤트(Alert & Event) 데이터베이스, 신뢰할 수 있는 외부자료 처리(Public Resource Handling), 콘솔(Console) 등의 6단계로 구분할 수 있다.

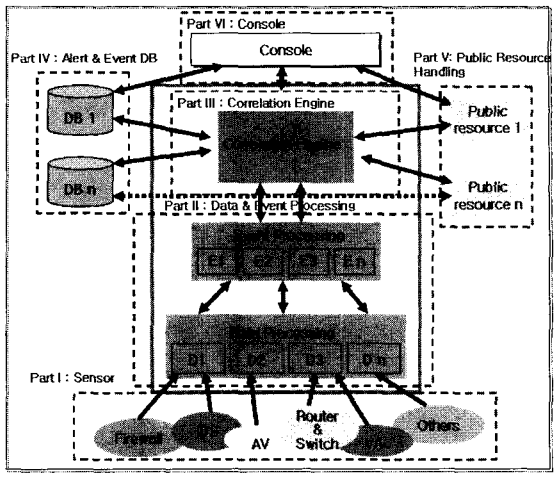

그림 2. 조기경보시스템 프레임워크

1. 센서 (Sensor)

해킹이나 위협이 네트워크 상에 침투될 때 네트워크에 존재하는 여러 장비에서 해당 징후가 포착될 수 있고 조기경보시스템의 예측 및 탐지율을 극대화하기 위해서는 이러한 Sensing기능을 하는 장비들이 유기적으로 연동이 되어야 한다. Sensing을 위해서는 방화벽이나 침입탐지시스템 (IDS : Intrusion and Detection System, 이하 "IDS"라고 한다) 뿐이 아니라 라우터나 스위치류 등에서 나오는 이벤트 정보 및 초당 패킷전송율 (PPS : Packet per Second) 등 다양한 디바이스를 이용하여 이상 트래픽을 Sensing할 수 있어야 한다.

1.1 Sensing 장비

보안장비류 - 방화벽, IDS, 위협관리시스템(TMS : Treat Management System, 이하 "TMS"라고 한다), 바이러스 백신, 침입방지 시스템 (IPS : Intrusion and Prevention System, 이하 "IPS"라고 한다) 등의 보안 이벤트 로그 등이 있다.

네트워크장비류 - 라우터나 스위치 등의 네트워크 장비에서 나오는 이벤트 로그 및 SNMP(Simple Network Management Protocol)를 이용한 트래픽 정보나 포트 up/down 정보 및 SMS(Server Management System)에서 발생하는 이벤트 로그 등이 있다.

2. 데이터 & 이벤트 프로세싱 (Data & Event Processing)

데이터 & 이벤트 프로세싱은 Part1 Sensor 로부터 올라오는 모든 보안 취약점 및 위협 데이터를 모아서 분류 및 그룹화 하여 조기경보를 제공하는 기본 이벤트로 정의를 한다. 이벤트는 수집(Collect), 제거(Filter), 공고화(Consolidate), 표준화(Normalize), 집합(Aggregation), 확장(Enrich) 등의 처리를 거쳐서 원하는 결과 값을 도출하게 된다.

2.1 수집 (Collect)

센서로부터 데이터를 수집하는 단계로 데이터가 누락되지 않도록 설계되어야 한다.

2.2 제거 (Filter)

수집된 데이터 중 정상적인 데이터와 분석할 만한 가치가 있는 이상 데이터로 구분할 수 있어야 한다.

2.3 공고화 (Consolidate)

분석할 만한 데이터를 그 특성에 따라 미리 정의해 둔 해킹 및 위협 구분 기준에 맞게 분류하고 공고화 하여야 한다. 때에 따라서는 동일한 위협요인이 동시에 여러 카테고리에 속할 수도 있다.

2.4 표준화 (Normalize)

공고화(Consolidate)된 데이터를 발생시간, 피해정도, 공격 형태, 공격 대상 등을 기준으로 표준화한다.

2.5 집합 (Aggregation)

표준화된 데이터를 같은 이벤트로 표현 될 수 있는 형태로 구분하여 표시한다. 예를 들어 특정 포트를 이용한 웜 공격이 발생할 경우 공격자 및 공격 대상에 상관없이 하나의 이벤트로 표시할 수 있다.

2.6 확장 (Enrich)

집합(Aggregation)된 이벤트 중 비슷한 유형 및 변종 등을 묶어서 강조하여 최종적으로 처리해야할 하나의 큰 이벤트로 표현해 낸다.

3. 상관관계 분석 엔진 (Correlation Engine)

네트워크 및 시스템 상의 위협을 예측하는 엔진이며, Part II 데이터 & 이벤트 프로세싱에서 정의 및 확장된 이벤트와 Part IV Alert & Event 데이터베이스의 최신 취약점 정보간의 상관관계를 정의하고 조기경보 할 수 있는 정보를 제공한다. 분석된 정보는 다시 Part IV Alert & Event 데이터베이스에 저장 관리한다.

4. Alert & Event 데이터베이스

이상 데이터와 이벤트간의 상관관계 분석 결과 및 외부의 위협과 취약점 정보를 분석하고 저장 관리하게 된다. 정적인 분석을 위하여 분석된 정보에 대한 Query-based 데이터베이스화 하며, 동적인 분석을 위하여 실시간 이벤트 및 해킹 위협을 분석 저장하기 위하여 저용량의 데이터는 메모리상에 Cache-based 데이터베이스를 이용하며 고용량의 데이터는 하드드라이브 상의 Query-based 데이터베이스로 이분화 하여 저장한다.

5. Public Resource Handling

통신망 사업자들이 운용하는 네트워크에 대한 데이터 및 이벤트뿐만이 아니라 국내외의 공신력 있는 보안 취약점 및 위협 서비스 정보 제공업체들과의 교류

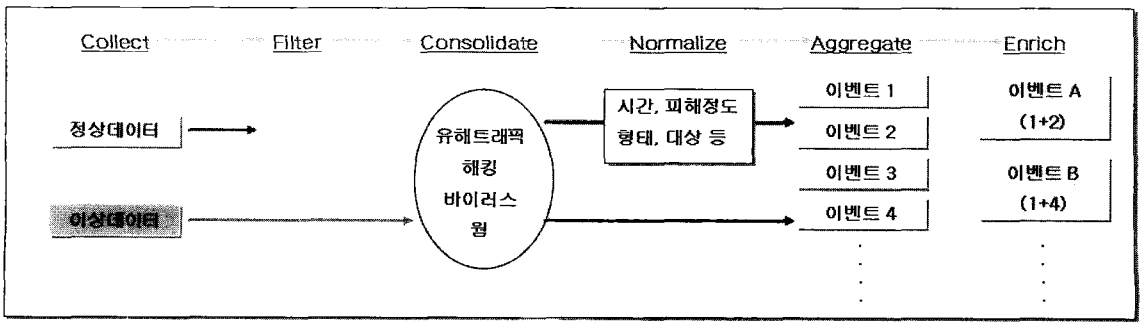

그림 3. 데이터 & 이벤트 프로세싱

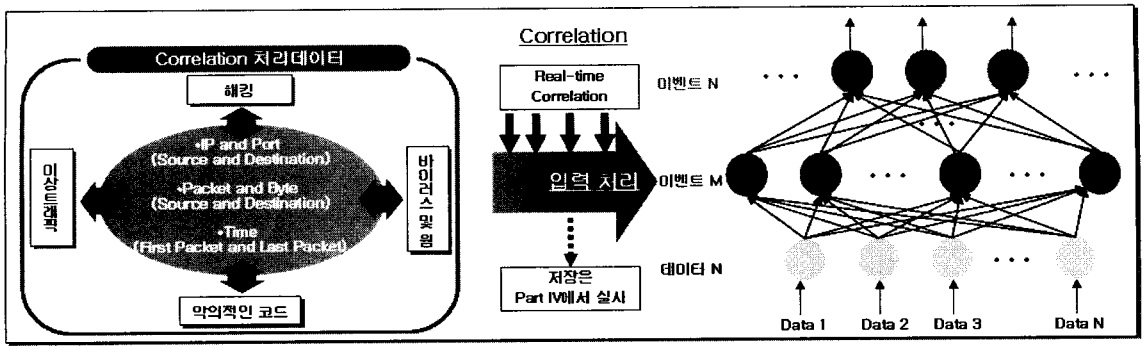

그림 4. 상관관계 분석 엔진 처리도

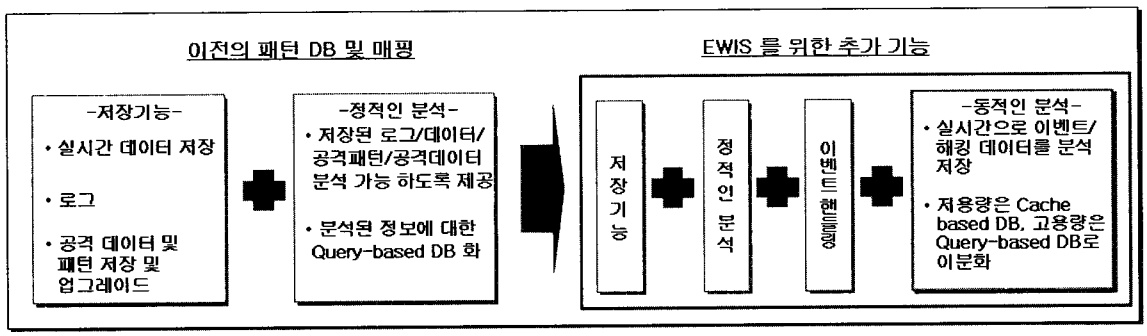

그림 5. Alert & Event 데이터베이스 구성도

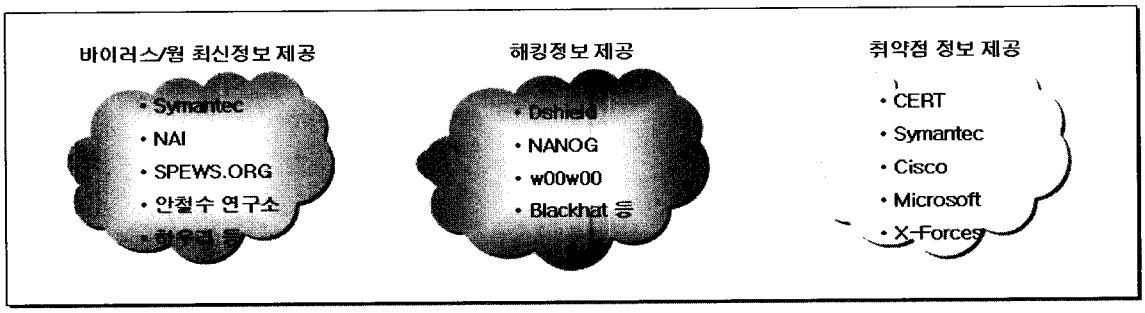

그림 6. 위협 및 취약점 정보를 공유하거나 분석을 제공하는 Resource 들

및 분석을 공유하여 조기경보시스템의 정확성을 향상시키는데 사용해야한다. 이러한 조기경보시스템은 또 다른 조기경보시스템의 Public Resource 로서 역할을 수행할 수 있으며 통신사업자는 해당 통신망을 이용하는 개별 고객에 대해서 Public Resource로서의 역할을 제공해야 한다.

6. 콘솔 (Console)

콘솔은 각 단계에서 처리한 결과 및 정보를 실시간으로 한 화면으로 Visual하게 보여주며, 조기경보에 따른 대응 및 조치도 함께 관리하는 종합 상황 모니터링 도구이다. 콘솔의 주요기능으로는 User Interface를 통하여 센서들의 현재 상황을 종합적으로 관리하거나, 전체 관리하는 현재 위험 등급을 자동으로 계산하여 표시해주고, 최신 취약점 및 악성코드 정보 등을 제공하고, 각종 통계 기능을 제공하거나, 리포팅 기능 및 Alarm기능을 통해서 운용자가 편리하게 조기경보시스템을 이용할 수 있도록 구성하여야 한다.

V. DoS 공격에 대한 조기경보시스템 대응 사례

DoS나 분산서비스 거부공격(DDoS, Distribute Denial of Service ; 이하 "DDoS"라 한다)에 대한

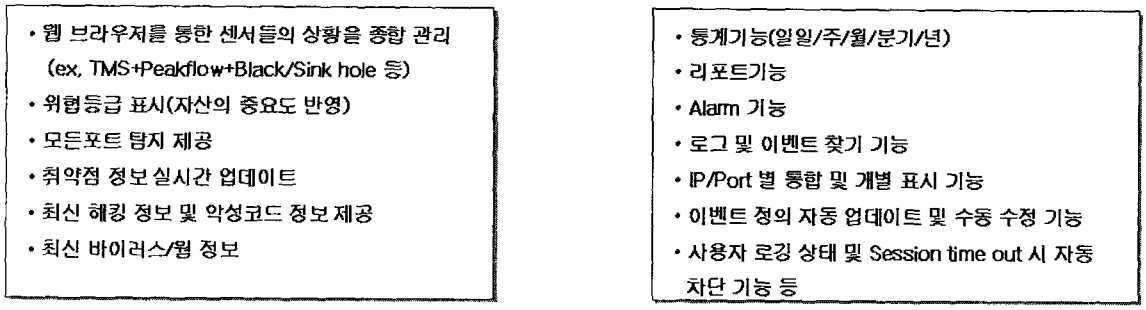

그림 7. 콘솔의 주요 기능

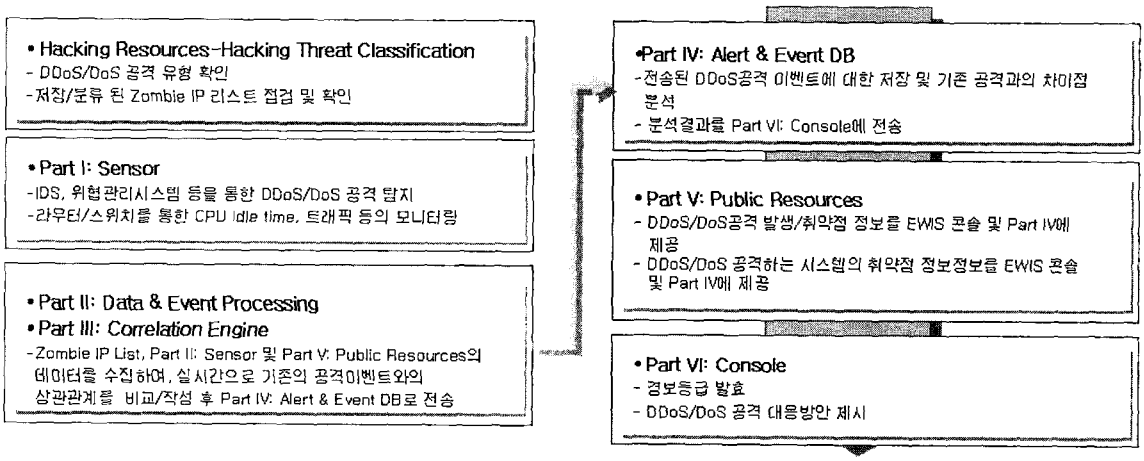

그림 8. DoS/DDoS 발생에 대한 조기경보시스템 프레임워크 가동 및 처리내용

조기경보시스템의 대응 내용은 먼저 사전단계로 Hacking Resource & Threat Classification에 따라서 DoS의 공격유형을 확인하고, Part I "센서"단계에서는 침입탐지시스템, 위협관리시스템 및 라우터나 스위치 등의 CPU 부하율 및 트래픽의 상태를 모니터링하고, Part II "데이터 & 이벤트 처리" 및 Part III "상관관계 분석엔진" 단계에서는 공격자 IP정보 및 기존의 공격이벤트와의 상관관계를 비교하여 그 결과를 Part IV "경보 및 이벤트 데이터베이스"로 전송하여 저장한다. 이러한 이벤트는 동시에 Part VI "콘솔"로 전송하여 적절한 경보 등급을 발효하거나 능동적인 대응 방법을 제시하여 운용자가 쉽게 처리할 수 있도록 도와준다.

Ⅵ. 결 론

통신분야의 조기경보시스템은 운용하는 망의 안정성 및 보안성을 확보하기 위하여 반드시 필요한 요소라고 할 수 있다. 우리나라의 경우 인터넷침해사고 대응지원센터에서 각 통신사업자의 중요노드에 대해서 유해트래픽 정보나 트래픽 통계정보 등을 수집하여 전국적인 조기경보체계를 구축하려고 하는 시도가 있다. 이러한 조기경보시스템이 좀 더 효율적으로 운용되기 위해서는 조기경보시스템에서 발생된 전자적인 침해사고를 자동적으로 처리해줄 수 있는 침해사고 처리 시스템 및 현재의 통신망 전체에 대한 위험도 및 대응방안을 결정해 주고 적절한 대응방법을 도출해 낼 수 있는 의사결정시스템 및 침해사고대응시스템 등에 대한 연구가 병행되어야 한다.

참 고 문 헌

[1] 최운호, "국가 조기경보시스템 활성화를 위한 제안", 월간사이버시큐리티, 국가사이버안전센터 2004.5
[2] 국가사이버안전센터, "2003년도 국내 전산망 침해사고 사례분석", 2004
[3] 정관진, 이희조, "인터넷 웜과 바이러스의 진화와

전망", 정보처리학회지, 제10권 제2호 pp. 27-37, Mar 2003.
[4] 구자현, "인터넷기반구조의 취약성 분석 및 개선 방안", 제 9회 정보보호심포지움, 2004
[5] 인터넷침해사고 대응지원센터,"조기경보시스템 체계", http://krcert.or.kr
[6] 국가사이버안전센터, "사이버 위기경보 체계", http://ncsc.go.kr
[7] 박종성, 최운호, 문종섭, 손태식, "자동화된 침해사고대응시스템에서의 네트웍 포렌식 정보에 대한 정의", 한국정보보호학회 논문지, 2004. 4.
[8] 전규삼, 최운호,"자동화된 침해대응시스템에서 Web을 기반으로한 로봇에이전트에 대한 연구" 한국정보보호학회 하계학술대회, 2004년
[9] 김현상, 이상진, 최운호, 임종인 "자동화된 침해사고 대응시스템에서의 디지털증거 수집", 한국정보보호학회 하계학술대회, 2004년

〈著 者 紹 介〉

구 자 현 (Koo Jahyun)
정회원

1998년 2월 : 한양대학교 전자공학과 졸업
1998년 3월~현재 : (주) 데이콤 선임연구원
〈관심분야〉 정보보호, 네트워크 보안, 통합보안장비, 조기경보, BcN