Journal of Knowledge Information Technology and Systems(JKITS), Vol. 9, No. 6, pp. 805~819, December 2014

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Study on the Improvement of Security Monitoring in the Separate Network Environment

Chang-Woo Han[1], Huy Kang Kim[1], Eunjin Kim[*2]

[1]*Graduate School of Information Security, Korea University*
[2]*Department of International Industrial Information, Kyonggi University*

ABSTRACT

Internal network connected to the internet are vulnerable to external attack. A consensus of awareness of that problem are spreading. As solutions to that problem, To prevent any damage on the system in the organization, The network separation obligation are spreading. Even if the intranet operates as a closed network by separating the internet can not be guaranteed to be secure. Security threats posed by malicious code are still present, such as stuxnet which works on control network that operates on a closed network. User carelessness, internet connect by intranet PC due to malicious intent, information leakage through the USB, an influx of malicious code to intranet, and using a technique for transferring data between separate networks without the use data transmission system for secure data transfer can be transferred uncontrolled data between internet and intranet. Also, even if network separation is completed insider threat is still present. Network separation made a difference of the traffic form occurring in each of the network, and the characteristics of the security log was affected. Accordingly, separately many researching for the internet about malicious traffic detection, need a plan that can effectively detect anomalies in the security log occurring in the interanet. In this study, Analysis of the characteristics of the security log occurring in physically separate the network environment focusing on the interanet and proposes a model for efficiently performing the security control.

KEYWORDS: Network Separation, Security Monitoring and Control, Log Analysis

ARTICLE INFO: Received 17 November 2014, Revised 12 December 2014, Accepted 12 December 2014.

1. 서 론

[*]Corresponding author is with the Department of International Industrial Information at kyonggi University, Gwanggyosan-ro 154-42, Yeongtong-gu, Suwon-si, Gyeonggi-do, 443-760, Korea

E-mail address: ejkim777@kgu.ac.kr

인터넷을 통한 보안 위협이 커짐에 따라 인터넷을 기반으로 업무 환경을 구축해 왔던 공공기관 및 기업들은 다양한 보안 위험에 직면하게 되었다. 인터넷으로 연결된 업무망이 외부의 공격에 직접 노출됨에 따라 내부의 중요 자료가 외부로 유출되는 등 보안관련 피해가 발생하고 있는 것이다.

이에 대한 보안 방안으로 인터넷망을 통한 보안 위협에 내부 업무망의 노출을 최소화하는 망분리가 적극 논의, 의무화되고 있다[1]. 망분리는 다양한 형태의 사이버공격과 새로운 악성코드 증가에 따른 정보유출 사고, 외부 침투에 따른 업무 손실, 업무망에 대한 사고 발생 위협의 증가가 예상되는 가운데 망분리가 의무적으로 요구되는 공공기관 및 기업 뿐 아니라 이외의 기업 및 조직에서도 시스템 구축 시 보편적으로 채택될 것으로 전망된다.

정부는 개인정보 유출을 근절하기 위한 보안대책으로 '12년 8월 17일 개정 공표한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」에 개인정보처리시스템에 접근하는 컴퓨터 등의 외부 인터넷망 차단(망분리) 조항을 신설, '13년 2월부터 일정 규모 이상의 기업은 망분리를 의무적으로 도입하도록 하였다.

금융위원회는 전자금융거래가 증가함과 함께 보안위협 또한 증가함에 따라 보안 대응체계를 강화하기 위해 종합적인 개선대책을 마련하여 '13년 7월 「금융전산 보안 강화 종합대책」을 배포하였다. 대책의 주요 내용 중에 금융전산에 대한 망분리를 의무화, 「금융전산 망분리 가이드라인」에 따라 전산센터를 시작으로 망분리가 순차적으로 추진될 예정이다.

이에 앞서 국가기관에서는 2006년 6월 '해외발 국가기관 해킹실태 및 대처방안'의 일환으로 국가기관 업무 전산망과 인터넷 분리 방침을 대통령에게 보고하였고, 이에 따라 2007년부터 시작된 국가기관 망분리 시범사업을 시작으로 현재까지 많은 국가기관이 업무 전산망과 인터넷을 분리하여 운영하고 있다.

망분리란 업무망과 외부 인터넷망을 2중으로 운용하는 방식으로, 기술적으로는 물리적 망분리와 논리적 망분리로 나눌 수 있다. 물리적 망분리는 업무용과는 별도로 인터넷망을 위한 네트워크를 구축하고 인터넷 접속을 위한 PC도 물리적으로 분리하는 방식을 말한다. 이 방식은 높은 보안성을 가지고 있으나, 많은 비용을 필요로 하고 개인당 2대의 PC를 사용함에 따른 사용자의 업무 효율성이 저하되는 단점을 가지고 있다. 물리적 망분리 방식은 업무상 불편함에도 불구하고 높은 보안 수준이 요구되는 대부분의 국가기관이나 공공기관에서 채택하고 있는 방식이기도 하다. 논리적 망분리는 물리적으로 같은 공간에 존재하는 자원을 가상화 방법으로 분리함으로써 서로 접근하지 못하도록 구성하는 방법이다. 이 방식은 기존 자원을 그대로 사용하여 도입 비용이 낮고 사용자는 하나의 PC로 업무를 할 수 있어 업무 효율성은 높다. 하지만, 물리적 망분리에 비해 상대적으로 안정성이 떨어지는 단점은 있다[2][3].

업무전산망을 물리적 또는 논리적 망분리를 통해 인터넷과 분리하여 폐쇄망으로 운영한다고 해서 보안성이 보장되는 것은 아니다. 폐쇄망으로 운영하는 제어망에서도 Stuxnet 등과 같은 악성코드로 인한 보안위협은 여전히 존재하고, 사용자 부주의 및 악의적인 의도에 의한 업무망 PC의 인터넷 사용, 보조 기억매체를 통한 정보유출 및 업무망으로의 악성코드 유입 그리고 업무망과 인터넷망간에 안전한 자료 전송을 위한 자료 전송 시스템을 사용하지 않고 분리된 네트워크 간에 자료를 전송할 수 있는 기술을 사용하여 통제되지 않는 데이터가 업무망과 인터넷망 사이로 전송될 수 있다. 또한 망분리를 했다고 하더라도 내부자로부터의 보안위협은 여전히 존재한다.

내부자 위협은 현재 혹은 이전 직원, 계약자 또는 조직의 네트워크, 시스템 또는 데이터에 접근 권한이 있거나 있었던 외부 사업 파트너가 조직의 정보나 시스템의 기밀성, 무결성, 가용성에 부정적인 영향을 주는 방법으로 접근하여 의도적으로 권한을 초과하여 사용하거나 잘못 사용하는 것을 말한다[4]. 내부자의 사기, 지적 재산의 절도, 고의적인 업무 방해, 스파이 행위와 같은 위협은 망분리가 이뤄졌다고 해서 해당 위협이 해소되는 것은 아니다.

논리적 망분리 방안에서는 물리적으로 동일한 네트워크를 사용하는 방법으로 보안장비에서 인터넷망과 업무망의 트래픽이 분리되지 않고 혼재되어 탐지되나, 물리적 망분리 방안에서는 물리적으로 2개의 네트워크가 생성되어 인터넷망에서는 주로 인터넷 관련 트래픽이 발생하게 되고, 업무망에서는 내부 업무 관련 트래픽이 대부분 발생하게 된다. 보안장비도 인터넷망과 업무망에 별도로 구축하여 운영하게 됨으로써 해당 네트워크 별로 발생하는 트래픽 형태로 달라지고 따라서 발생하는 보안로그의 특성도 달라진다.

물리적 망분리 이후의 폐쇄망인 업무망에서 발생하는 보안로그의 양이 망분리 전보다 줄어들기는 하겠지만 여전히 많은 보안로그가 발생한다. 이렇게 수많은 보안로그에서 유해한 이벤트를 찾아내고 효과적으로 관리하기란 쉬운 일이 아니다.

이에 본 논문에서는 먼저 망분리에 관련한 일반적인 현황을 정리하고, 침입탐지와 관련된 연구와 상대적으로 많은 연구가 이뤄진 외부와의 연결이 없는 폐쇄망인 제어망에 대한 보안위협과 탐지와 관련된 문헌연구 그리고 물리적 망분리가 된 기관의 업무망에서 발생하는 보안로그 분석을 통해 효율적으로 유해 트래픽을 탐지할 수 있는 방안을 제시하고자 한다.

2. 업무전산망 분리환경

2.1 물리적 네트워크 분리 방안

물리적 네트워크 분리 방안은 인터넷과 업무 전산망을 분리하는 방안 중에서 개념적으로 명확한 방안이다. 업무 전산망이 인터넷과 물리적으로 단절되어 있어 인터넷을 통한 사이버공격은 물론 정보 유출도 원칙적으로 차단이 가능하다는 장점이 있다. 인터넷과 물리적으로 분리된 업무 전산망을 구축하기 위해서는 별도의 네트워크를 구축해야 하며, 사용자 PC의 운용형태에 따라 아래와 같은 3가지 방안으로 구분할 수 있다.

2.1.1 두 대의 PC를 이용한 네트워크 분리

두 대의 PC를 이용한 네트워크 분리는 인터넷용과 업무용으로 분리된 네트워크에 인터넷 PC와 업무 PC를 각각 접속하여 물리적으로 업무영역과 인터넷을 분리하는 방식이다. 이 방안은 명확한 개념의 망분리 방안으로 가장 안전한 업무 환경을 제공한다는 장점이 있는 반면, 네트워크 구축과 PC 구입 등의 도입 비용과 유지보수 비용이 많이 발생하고 업무 효율이 상대적으로 떨어지는 단점이 있다. 이 방안에서 발생할 수 있는 보안 위협요소로는 업무 PC와 인터넷 PC간 자료 이동과정, 사용자 부주의 및 악의적 의도에 의한 업무 전산망의 PC가 인터넷에 연결되어 사용될 경우 그리고 보조기억매체를 통한 정보 유출 및 보조 기억매체의 악성코드 감염으로 업무 전산망에 해당 악성코드가 유입될 수 있다.

위와 같은 보안 위협을 줄이기 위해 보조기억매체의 물리적 이동 및 사용을 통제하고, 분리된 네트워크에 연결하기 위한 커넥터를 구분하여 사용함으로써 업무 PC가 인터넷에 연결 되는 것을 방

지해야 하며 업무망에 별도의 패치관리서버와 백신엔진 업그레이드 서버 등을 운용하여 업무망의 안전성과 보안성을 강화할 수 있다. 망간 자료이동 시 불편함을 최소화하기 위해 안전성을 확보한 자료전송 시스템을 운용하는 것이 필요하다.

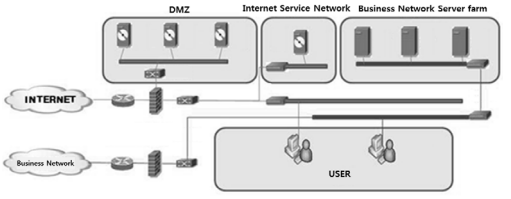

그림 1. 2대의 PC를 이용한 네트워크 분리 구성도
Figure 1. Network separate structure using two PC

2.1.2 망 전환 장치를 이용한 네트워크 분리

PC에 하드디스크 및 랜카드를 별도로 설치하고, 망 분리 전환 장치를 이용하여 업무용 모드와 인터넷 모드로 전환하는 방식이며, 망분리 전환 장치를 통해 사용자가 PC 운용환경을 선택하도록 하여 업무망과 인터넷을 물리적으로 분리하는 방식이다.

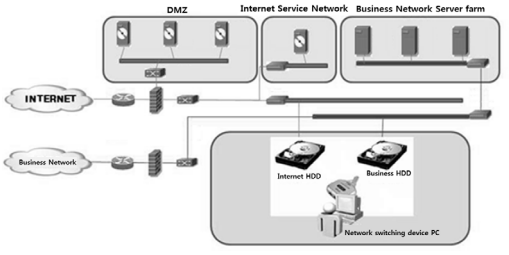

그림 2 망 전환 장치를 이용한 네트워크 분리 구성도
Figure 2 Network separate structure using network switch device

이 방안의 장점은 PC 2대 이용방안에 비해 구축과 운영비용이 절감되면서 비슷한 수준의 보안성을 제공하고 효율적인 공간 활용이 가능하다. 반면에 별도의 네트워크 구축에 따른 비용이 발생하고, 망 전환 시 재부팅이 필요해 사용이 불편하다는 단점이 있다. 망 전환 장치를 이용하는 네트워크 분리방안의 보안 위협요소와 해소 방안은 2대의 PC를 이용하는 방안과 유사하다.

2.1.3 멀티 PC를 이용한 네트워크 분리

한 대의 PC를 업무용으로 활용하고, 인터넷은 별도 접속장치를 통하여 호스트 PC에 접속하여 처리함으로써 기존 터미널 방식의 작업환경을 소규모 단위로 운영하는 형태이다. 이 방안은 장점은 망 전환 장치 이용방안과 마찬가지로 PC 2대 이용방안에 비해 구축과 운영비용이 절감되면서 비슷한 수준의 보안성을 제공하고 효율적인 공간 활용이 가능하다. 단점으로는 모든 사용자의 동시 접속 시 속도 저하가 발생 가능하고, 대규모 기관에 적용 시 관리 부담이 증가한다. 이 방안 또한 별도의 네트워크 구축에 따른 비용이 발생한다. 멀티 PC를 이용 방안도 앞 두 가지 방안의 보안 위협요소와 해소방안과 유사하다.

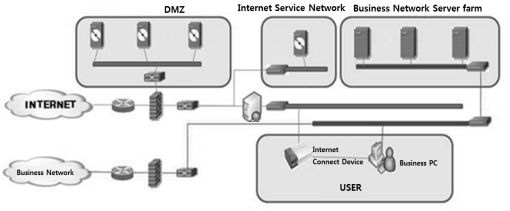

그림 3 멀티 PC를 이용한 네트워크 분리 구성도
Figure 3 Network separate structure using multi-PC

2.2 논리적 네트워크 분리 방안

논리적 망분리는 인터넷망과 업무망을 분리할 때 별도의 네트워크를 구축하지 않고 논리적으로 네트워크를 분리하는 방식을 말한다. 이 방법은 실제로 존재하지 않는 가상의 망을 구축해야하기 때

문에 다양한 가상화 기술 및 보안 기술을 사용한다. 물리적 네트워크 분리 방안에 비해 상대적으로 안전도가 떨어지는 단점이 있지만, 1대의 PC에서 인터넷 이용과 내부업무 수행이 동시에 가능하기 때문에 효율성이 높다. 논리적 망분리 방식으로는 서버 기반 가상화와 PC 기반 가상화 등 2가지 방식이 있다.

2.2.1 서버 기반 가상화(SBC)

서버기반 가상화(SBC, Server-Based Computing)는 사용자가 PC에서 수행했던 응용프로그램 실행, 자료저장 등 모든 작업을 터미널을 통해 서버에서 실행되는 컴퓨터 환경을 말한다. 인터넷 접속 시 기존 인터넷 PC를 활용하고, 업무망은 SBC 환경을 위한 전용 에뮬레이터를 사용하여 업무자료 유출을 차단할 수 있다. 이 방안의 장점은 물리적 망분리 방식 대비 네트워크 구축 및 시스템 도입비용을 절감할 수 있다. 단점으로는 응용 프로그램 획일화로 업무가 불편할 수 있는 등 제한적인 업무에 적합한 구조로 다양한 프로그램 실행이 불가능하다.

2.2.2 PC기반 가상화

PC기반 가상화(CBC, Client-Based Computing)는 업무용 PC에 가상화된 인터넷 영역을 생성한 후 가상화 영역에서 실행되는 프로그램만 인터넷 접속이 가능하도록 하며 네트워크를 논리적으로 분리하는 방식이다. 인터넷 접속은 보안 게이트웨이를 이용해 구축한 가상사설망(VPN)을 통해 개별적이고 논리적인 통신채널을 이용한다. 이 방안의 장점은 망분리 방식 중 구축비용이 가장 저렴하다. 단점은 다양한 PC환경에 대한 호환성에 대한 검토가 필요하다.

3. 관련 연구

3.1 침입탐지 관련 연구

일반적인 침입 탐지 기법은 이미 알려진 공격의 특징을 패턴화하여 해당 공격과 일치하는 트래픽을 탐지하는 오용탐지(misuse detection)기반 방식과 일반적인 패킷 크기에 대한 기준선 또는 일반적인 상태와 비교하여 비정상인 트래픽을 탐지하는 이상증후 탐지(anomaly detection) 기반 방식으로 분류되고 있다. 오용탐지 방식에 사용되는 모델로는 전문가 시스템(Expert System), 시그니처 분석, 페트리넷(Petri-net), 상태전이분석(state transition analysis), 신경망 그리고 유전 알고리즘 등이 있고, 이상증후 탐지 방식에는 통계적 방법, 전문가 시스템, 신경망, 컴퓨터 면역학, 데이터마이닝, 기계학습 등의 모델이 있다[5].

위의 탐지방법에 더해 산업공학과 열역학 등 타 학문의 방법론을 보안에 적용하여 공격 탐지에 활용하는 연구들이 다수 있다. 인가된 내부자에 의한 Anomaly를 효율적으로 진단하기 위해 R(Recency), F(Frequency), M(Monetary)의 3가지 Factor를 이용하여 사용자의 패턴을 진단하는 RFM 기반 user profile 분석기법이 있다. 이를 보안에 응용하여 네트워크 프로토콜의 분포, 프로토콜별 목적지 포트 분석, 패킷 사이즈 분석을 통하여 각 시스템과 네트워크의 Profile을 제어망에 적용하는 방안[6]과 함께, RFM 분석기법과 병행하여 데이터의 용이한 시각화를 위해 통계적 공정관리(SPC, Statistical Process Control)에서 사용하는 관리도(Control Chart)를 이용한 사용자 패턴 변화를 탐지하는 방법이 있다. 이를 네트워크 트래픽에 적용하여 네트워크 프로토콜의 분포, 프로토콜별 목적지 포트, 프로토콜별, 포트별 패킷 사이즈 등이 일반적으로 정규분포를 따른다고 가정하여 시스템의 변동 상

황이 정상인지 비정상적인지를 관리도(Control Chart)를 이용하여 관리상한(upper control limit)과 관리하한(lower control limit) 영역을 벗어난 경우 이상 징후로 판단하는 방법론을 제시[6]하였다.

열역학에서 사용되는 시스템 내의 무질서의 정도를 측정하는 수치인 엔트로피 개념이 있다. 이를 네트워크에 적용하여 시스템과 주변 환경의 물질 분포에 급격한 변화가 나타나면 엔트로피가 증가한다는 열역학이론을 활용, 네트워크에 이상 징후 발생 시 패킷의 이동에 따른 패킷역학의 변화에 따른 엔트로피가 증가하게 된다. 이와 같은 개념에 착안하여 이상 징후를 야기하는 공격자를 파악하기 위해 IP를 이용하여 시스템(내부 네트워크)와 주변 환경(외부 네트워크)을 구분하고, 이상 징후의 공격대상 서비스를 파악하기 위해 포트번호를 이용하여 시스템과 주변 환경을 구분한 다음, 이상 징후의 출현시간을 파악하기 위해 엔트로피를 주기적으로 측정하고 관찰하여 효율적인 이상 징후 탐지 알고리즘을 제안[7]하였다.

기존 보안 솔루션을 활용하여 공격을 효율적으로 탐지하고 검증하기 위한 연구들로는 데이터 마이닝을 이용한 공격탐지 방안으로, 공격자의 로그인 시도 시, 계정 차단 및 정상사용 여부에 대한 임계치를 두고 데이터마이닝을 거쳐 위협 가능성에 대한 알람이 울리게 하여 장기적으로 시도되는 공격에 대하여 데이터를 분류, APT 공격과 같은 앞으로 일어날 수 있는 공격 징후를 탐지할 수 방안을 제시[8]하였다.

보안관제 및 대응 활동의 효율성 강화를 위해 공격에 대한 실증적 분석에 기반을 두어 해킹 시도와 관련된 실제 트래픽 정보를 수집하고, 수집된 데이터를 토대로 필수요소 및 2차 보조요소 값을 분류한다. 그런 다음 해당 트래픽 정보에 대하여 정·오탐 유무를 분석하고 확인한 후 예외처리 여부를 결정하는 등의 검증절차를 통해 보안이벤트를 자동으로 분석하고 공격 여부를 자동으로 검증하는 방안을 제안[9]하였다.

최근의 보안관제 기술의 동향은 수많은 데이터로부터 가치를 추출하고 결과를 분석하는 빅데이터라는 기술과 접목되면서, 다양한 소스로부터 정보를 통합하고 상호연관성을 갖는 상황(Context)정보 분석 및 모니터링으로 유용한 정보를 찾아낼 수 있는 기술적 개념과 방법론인 시큐리티 인텔리전스(Security Intelligence)로 발전하고 있다[10].

3.2 제어망에 대한 보안위협 탐지

일반적으로 제어망은 하나의 독립적인 망으로 외부와의 연결이 단절되어 운영된다. 이런 제어망의 특성이 망분리가 이뤄진 업무망의 특성과 유사한 형태를 가지고 있다. 제어망에서 이상 징후 탐지와 관련된 연구들을 살펴보는 것은 업무망에서 유해한 트래픽을 분류해 내는데 도움이 될 수 있을 것이다.

제어시스템 환경에서는 시스템 동작 패턴 또는 네트워크 통신 트래픽이 규칙적이기 때문에 제어시스템의 정상적인 특성을 Whitelist로 나타내고 이를 통해 이상 징후를 탐지하는 것이 효과적일 수 있다. 이와 관련한 연구들로 주요 프로토콜을 중심으로 정상 트래픽을 생성하고 이를 통해 알려지지 않은 트래픽에 대하여 비정상 트래픽으로 간주하고 공격으로 방안으로, 제어망으로 들어오는 패킷들은 Whitelist 기법을 적용한 검사를 받게 되며 이를 통해 비정상적 행위를 탐지할 수 있다. 이때 정상 행위에 대하여 사전에 프로파일링한 결과를 바탕으로 이상 징후 탐지를 하는 방안을 제시[11]하였다. 다른 연구에서는 Whitelist 기반 이상 징후 탐지 모델을 제시하기 위해 제어시스템 환경에서 발생할 수 있는 공격 및 오동작 유형을 분류하고, 이를 탐지하기 위해 네트워크 계층(Network

Layer), 프로토콜 명세 계층(Protocol Specification Layer), 제어 메시지 계층(Control Message Layer), 통계 계층(Static Layer)의 4계층으로 이루어진 Whitelist를 제시하고 이를 통해 세분화된 검사와 이상 징후 유형에 대한 정보를 제공하는 방안을 제안[12]하였다.

제어망은 가용성을 침해할 위험이 있는 조치사항을 대체할 수 있는 대응 모델을 마련하고, 운영환경의 특수성에 기인한 제약사항에 위배되지 않는 보안모델을 수립하는 것이 중요하다. 효과적인 이상 징후 탐지를 위해 네트워크 트래픽을 조사하고, 이를 분석하는데 있어 앞서 살펴보았던 RFM분석기법과 통계적 공정관리(SPC) 기법을 제어망에서 발생한 네트워크 데이터에 적용하여, 발생한 데이터의 특성이 장기간 변함없이 거의 동일한 패턴이 존재하기 때문에 이상증후 측정이 가능함을 분석을 통하여 고찰함으로서, 제어망에서의 침입탐지 및 대응에 대한 의사결정이 가능한 분석 및 대응 모델을 제시[13]하였다.

제어망에서의 침입탐지와 관련된 다른 연구로는 이상증후 탐지기법 중 네트워크 트래픽이 일반적으로 가지고 있는 통계적 특성인 자기 유사성(self-similarity)을 이용하는 방법이 있다. 자기 유사성이란 서로 다른 스케일에서 보았을 때 동일하게 보이거나 동일하게 행동하는 것이 유사한 현상을 말한다. 시간당 패킷의 개수(PPS, Packet Per Second), 시간 당 패킷의 크기(BPS, Byte Per Second), 프로토콜 그리고 동일한 근원지 주소(source address), 목적지 주소(destination address), 포트 번호(port number), 평균 패킷 사이즈(average packet size) 등을 갖는 패킷의 집합인 플로우(flow)와 같은 네트워크 트래픽의 여러 요소를 분석하여, 해당 네트워크 환경의 특성을 잘 설명할 수 있는 측정 메트릭(metric)을 지정하여 측정한 다음, 이를 통해 다양한 공격을 탐지할 수 있다. 제어망의 경우 일정하고 규칙적인 네트워크 트래픽 형태를 갖는다는 특성에 착안하여, 제어망에서 네트워크 트래픽의 자기 유사성을 측정하면 자기 유사성이 극히 높은 상태로 유지됨을 알 수 있고, 자기 유사성의 변화가 공격의 증후를 감지하는 지표가 될 수 있으므로 이를 활용한 침입탐지 방법론을 제안[14]하였다.

4. 망분리 환경에서의 보안로그 특성

4.1 전산망 운영 현황

제어망을 운영하는 기관에서 인터넷과 단절된 업무 전산망을 분리하여 운영할 경우 그림4와 같이 인터넷망, 업무망 그리고 제어망으로 크게 3가지로 분류할 수 있다. 각 망별 특성을 살펴보면, 우선 인터넷망은 외부 통신망과 연결이 되어 기존 업무 전산망이 분리되기 전의 특성을 그대로 가지고 있게 된다.

각종 설비를 제어하고 감시하는 시스템과 그 부속시설을 일컬어 제어시스템이라 하며, 이러한 제어시스템이 존재하는 정보통신망은 보통 외부와 단절되어 운영되며 이렇게 폐쇄망 형태로 운영되는 망을 제어망이라고 한다[15].

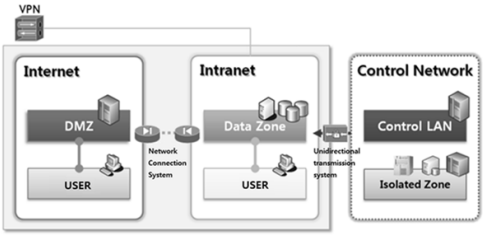

그림 4. 전산망 분리 구성도
Figure 4. Network separation structure

감시 네트워크와 제어 네트워크가 초기에는 분

표 1. 전산망 형태에 따른 특성 비교
Table 1. Compare each network characteristics

division	Internet	Intranet	Control
N/W Periodic replacement	Relatively short period of time (3~6year)	Relatively short period of time (3~6year)	Long-term use (10~20year)
N/W Performance conditions	Real-time Non-real-time	Real-time Non-real-time	Real-time Critical response time
Availability	Allowable service delay	Allowable service delay	stop/delay non-Allowable
Network structure	Open	Closed	Closed
Security policy	confidentiality, integrity, availability, etc.	confidentiality, integrity, availability, etc.	Availability First
Topology	Centralized	Centralized	Distributed structure

리되어 운영되었으나, 현재는 통합화되고 있는 추세이다. 제어망의 일부 데이터가 단방향 전송시스템을 통해 업무망으로 전송되는 것을 제외하고는 제어망으로 데이터가 유입되는 경로는 거의 없다. 제어시스템은 자동화된 제어 기능을 제공하기 위해 중단 없이 안정적으로 수행하는 것을 일차적인 목적으로 설계되어 있으며, 운영·관리의 목적 또한 시스템 오류를 모니터링하고 안정성을 저해하는 요소를 차단하는 것을 기본으로 시스템의 가용성을 확보하는데 우선을 두고 있다. 각종 계측 제어 설비들은 기본적으로 일반 IT설비에 비해 수명주기가 길고, 실시간 응답을 요구하며, 제어시스템 전용 프로토콜을 사용하고 있다.

외부 인터넷과 차단되어 운영되는 업무망의 경우 제어망과 유사한 특성을 가지고 있다. 다만 제어망의 경우 시스템이 발생시키는 데이터가 대부분인 반면 업무망의 경우 직원들의 내부 업무를 위해 사용하는 데이터가 다수를 차지하고 있다. 외부망과의 연결은 제어망에서 단방향 전송시스템을 통해 업무망으로 유입되는 데이터, 망연계시스템을 통해 업무망과 인터넷망 간에 자료가 전달되고 그리고 외부 사용자를 위해 VPN을 사용해 내부 업무망에 연결되는 정도이다. 위와 같은 망분리가 이뤄진 기관의 망 구성과 각 망별 특성을 비교하면 아래와 같다.

4.2 망분리 후 업무전산망 보안 로그 특징

물리적 망분리가 이뤄진 인터넷과 분리된 폐쇄망인 업무전산망의 보안 로그를 분석하면 발생하는 데이터의 변동이 크지 않고, 제어망과 유사하게 일정한 패턴을 갖고 있음을 확인할 수 있었다. 실험에 사용한 데이터는 산업통상자원 사이버안전센터의 회원기관 중 물리적 망분리가 이뤄진 기관의 침입차단 시스템에서 생성된 4주간의 데이터를 활용하였다.

망분리 이후의 보안로그를 살펴보기 전에 조직 내부 업무와 인터넷을 함께 사용하는 기관과 망분리가 이뤄진 기관의 업무전산망에 대한 보안로그에 대한 특성을 4주 동안 발생한 데이터에 대해 비교해 보았다. <표 2>는 인터넷과 내부 업무를 함께 사용하는 3개 기관과 망분리가 이뤄진 3개 기관의 업무전산망에서 발생하는 전체 보안로그에 대해 Protocol별 탐지되는 패킷 크기의 평균과 표준편차와 Protocol별 탐지되는 비율에 대한 평균과 표준편차를 나타내고 있다. 6개 기관에서 공통적으로

표 2. 망분리 유무에 대한 Protocol별 탐지되는 패킷 크기의 평균과 표준편차, Protocol별 탐지되는 비율에 대한 평균과 표준편차
Table 2. Each protocol average size, Standard deviation and average ratio, standard deviation of Detect Packet According to the network separation

Division	protocol	Detect Packet average Size(byte)	Detect Packet Size Standard deviation	Detect average Ratio	Detect Ratio Standard deviation
Internet-A	TCP	357	52.56	49.66%	18.13%
Internet-A	UDP	202	109.89	40.50%	21.09%
Internet-A	ICMP	101	3.42	9.83%	3.93%
Internet-A	ESP	2974	174.27	0.02%	0.01%
Internet-B	TCP	920	107.37	68.33%	23.57%
Internet-B	UDP	733	370.85	30.80%	23.77%
Internet-B	ICMP	114	4.73	0.87%	0.30%
Internet-C	TCP	932	82.23	45.06%	14.43%
Internet-C	UDP	990	400.19	54.50%	14.48%
Internet-C	ICMP	949	87.03	0.45%	0.26%
Intranet-D	TCP	145	2.22	89.73%	1.46%
Intranet-D	UDP	284	25.17	6.49%	0.69%
Intranet-D	ICMP	9108	497.33	3.32%	0.71%
Intranet-D	OSPF	14411	505.93	0.46%	0.08%
Intranet-E	TCP	154	7.59	25.26%	1.27%
Intranet-E	UDP	830	26.11	71.45%	1.27%
Intranet-E	ICMP	796	147.61	3.29%	0.27%
Intranet-F	TCP	764	37.07	87.63%	2.43%
Intranet-F	UDP	835	147.20	9.92%	3.46%
Intranet-F	ICMP	441	275.50	2.45%	2.23%

탐지되는 Protocol인 TCP, UDP, ICMP에 대해 망분리 유무에 따른 차이가 발생하는지 살펴보았다. 일부 기관에서만 탐지되는 ESP, OSPF 등의 Protocol이 존재하지만 망분리 유무에 대한 특성 비교에 활용하기엔 부족하였다.

망분리 유무와 상관없이 탐지되는 보안로그의 Protocol중에서 TCP와 UDP가 전체의 약 90%를 차지하고 있어서, 망분리에 따른 특성을 비교하기에는 두 개의 Protocol이 해당 특성을 잘 대변한다고 생각된다. 통계집단 단위의 계량적 특성값에 관한 산포도를 나타내는 표준편차를 이용해 비교, 분석해 보면 Protocol별 탐지되는 패킷의 크기에 대한 표준편차와 Protocol별 탐지되는 비율에 대한 표준편차를 비교하면 망분리된 기관의 업무전산망의 표준편차가 조직 내부 업무와 인터넷을 함께 사용하는 기관의 표준편차에 비해 작은 것을 확인할 수 있었다. 그 의미는 폐쇄망으로 운영하는 망분리된 기관의 업무전산망에서 보안로그는 그 변동 폭이 적다는 것을 알 수 있다. 특이한 점으로는 어떤 기관에서는 1%도 탐지되지 않긴 하지만, ICMP Protocol의 경우에는 망분리된 기관의 업무전산망에서 탐지되는 패킷의 크기에 대한 표준편차가 상대적으로 크게 나타났다. 또한, 특징적으로 많은 차이가 발생하는 특성으로 가장 많이 발생한 근원지 주소(source address) IP와 목적지 주소(destination address) IP간에 발생한 트래픽이 탐지

되는 개수의 변화였다. 망분리된 업무전산망의 보안 로그의 경우에는 탐지되는 IP 주소의 쌍이 지속적으로 탐지되는 반면에, 조직 내부 업무와 인터넷을 함께 사용하는 기관에서는 도표나 그림으로 도식화하기 힘들 정도로 그 변화가 크게 나타났다.

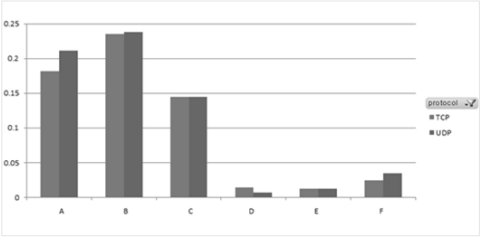

그림 5. 망분리 기관과 분리되지 않은 기관의 Protocol별 탐지되는 비율에 대한 표준편차 비교
Figure 5. Comparison of standard deviation for detect ratio

물리적 망분리가 이뤄진 기관의 업무전산망에서 발생하는 보안로그의 특성을 자세히 알아보기 위해 업무전산망에서 발생한 보안로그(침입차단 시스템)에 대해 탐지된 전체 탐지건수의 합계, 탐지된 이벤트의 트래픽 합, 프로토콜별 탐지건수, 많이 탐지되는 Top 10에 대한 탐지패턴별 탐지건수 합, 탐지되는 패킷의 크기별 탐지건수 합 마지막으로 근원지 주소(source address) IP와 목적지 주소(destination address) IP간 탐지된 이벤트의 4주간 데이터에 대한 변동 추이를 분석하였다.

위에서 분류한 특징별 탐지되는 추이를 살펴보면 변동 폭이 적고 주기별 거의 동일하게 탐지됨을 알 수 있었다. 이는 망분리가 이뤄진 업무전산망의 네트워크 트래픽의 특성이 제어망과 유사함을 의미한다. 물론 위에서 언급한데로 제어망은 시스템이 발생시키는 데이터가 일정하고 규칙적인 형태로 나타나는 반면에, 업무망은 장비 관리를 위한 네트워크 트래픽이 있겠지만 대부분은 직원들의 내부 업무를 위해 사용한 트래픽이 다수를 차지하고 있다. 그럼에도 불구하고 보안장비에서 탐지되는 망분리가 이뤄진 업무전산망의 보안로그는 일정한 형태를 나타내고 있음을 알 수 있다.

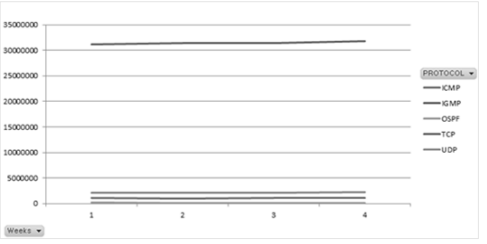

그림 6. Protocol 별 탐지건수 합계 변화
Figure 6. Changes of total detect count

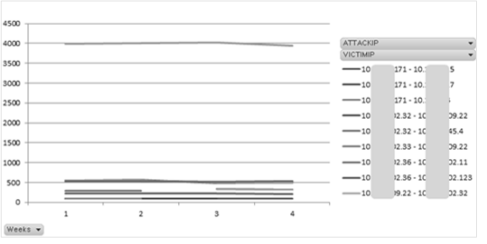

그림 7. 탐지되는 이벤트 중 Top10에 해당하는 “Source IP-Destination IP” 간 탐지된 패킷의 평균 크기 변화
Figure 7. Changes of Detect Packet average size in Top 10 Source IP-Destination IP

5. 망분리 환경에서의 보안관제 효율화 방안

5.1 망분리 환경에서 이상 징후 탐지 모델

이상 징후를 탐지하는 방법은 앞서 살펴본 바와 같이 크게 두 가지로 분류할 수 있다. 네트워크의 일반적인 패킷 크기에 대한 기준선 또는 일반적인 상태와 비교하여 비정상인 트래픽을 탐지하는 이상증후탐지(anomaly detection) 기법과 이미 알려진 공격의 특징을 패턴화하여 해당 공격과 일치하는 트래픽을 탐지하는 오용탐지(misuse detectin or

signature based detection) 기법이다.

본 연구에서는 망분리 환경에서 업무전산망의 대한 보안로그에 대해 효과적으로 이상 징후를 탐지하기 위해, 기존에 운영하고 있는 보안장비(침입차단시스템)에서 탐지되는 패턴에 기반을 둔 오용탐지 기법에 추가하여, 많은 보안로그가 지속적으로 발생하는 상황에서 효과적으로 이상 징후를 판별하기 위한 관제모델을 제안한다. 앞서 살펴본 바와 같이 망분리 후 폐쇄망으로 운영되는 업무전산망의 특징이 제어망과 같이 유사하다는 점을 확인, 선행연구에서 살펴본 통계적 공정관리(SPC) 기법과 Whitelist 기반 이상 징후 탐지 기법을 업무전산망의 보안로그 데이터에 적용하기 적합하다고 판단하였다.

SPC기법을 <표 3>에서와 같이 Protocol 별 공격 시도에 따른 탐지 회수와 탐지된 Packet의 평균 크기, Protocol 별 목적지 포트로 발생한 공격 탐지 회수와 탐지된 Packet의 평균 크기, Protocol 별 탐지된 패킷의 크기에 따른 공격 탐지 회수 등이 일반적으로 정규분포를 따른다고 가정하여 매일 생성되는 보안로그에 적용하였다. 다만 업무 전산망은 직원들의 내부 업무를 위해 사용하는 트래픽이 많으므로, 근무일과 휴일을 구분하여 적용하였다. 정규분포를 따르는 이벤트라면 데이터는 $\mu \pm 2\sigma$ (μ는 평균, σ는 표준편차) 범위 내에 있는 95%에 분포하게 된다. 이를 기준으로 관리상한(upper control limit)을 $\mu + 2\sigma$로, 관리하한(lower control limit)을 $\mu - 2\sigma$로 잡은 뒤, 이 영역을 벗어난 경우 이상 증후로 판단할 수 있을 것이다.

Whitelist 기반 이상 징후 모델은 여러 가지가 있을 수 있겠지만, <표 4>와 같이 망분리된 업무 전산망에 적용하기에는 기관에서 사용 및 관리되는 내부 IP 대역, 주로 통신하는 출발지 IP와 목적지 IP 대역, 특정 서비스 포트를 사용하는 client_ip / server_ip / server_port 등을 선정할 수 있을 것이다.

위에 언급한 두 가지 방법이 효과적이긴 위해서는 부서 이동 후 이전 부서의 공용 프린터 서버 IP 설정으로 인해 발생하는 트래픽 등 업무와 무관하게 발생하는 트래픽의 발생 원인을 제거하여 통신망의 부하를 경감하기 위한 노력과, 장비 관리 등의 목적으로 지속적으로 발생하는 NMS 트래픽 등의 정상 트래픽은 보안장비에서 예외 처리하고, 탐지 현황을 분석하여 보안장비에서 탐지되는 패턴의 임계치를 조정하여 관리해야하는 보안로그를 줄여 보안장비의 탐지 효율성을 강화할 필요가 있다. 예외처리 해야 할 대상 선정은 앞장에서 살펴본 바와 같이 지속적으로 탐지되는 "Source IP-Destination IP"에 대해서 발생 원인을 분석하면 될 것이다.

표 3. SPC 기법 적용 패턴
Table 3. Detect model using SPC techniques

tuple	abnormal symptoms
Protocol	detect count
	detected packet average size
Protocol Destination Port	detect count
	detected packet average size
Protocol Detect Packe size	detect count

표 4. 업무 전산망의 Whitelist
Table 4. Whitelist of intranet

Whitelist Object	Tuple
Approved IP	Used and managed IP List
Approved Communication IP List	Communication is permitted Source and Destination IP List
Approved Sercies	Servies is permitted Client IP list/ Server IP/Server Port

5.2 방법론 적용

본 논문에서 제안한 모델의 유효성을 검증하기 위해 망분리된 실제 업무전산망의 보안로그에 이를 적용하는 것과 가상으로 망분리된 업무전산망과 유사한망을 구축하여 적용하는 것을 계획하였다. 실제 망분리된 업무전산망 보안로그에 적용하기 위해 산업통상자원 사이버안전센터 회원기관 중 물리적 망분리가 이뤄진 2개 기관의 주말을 제외하고 업무일 기준으로 2주간의 데이터를 중심으로 분석하였다.

SPC기법을 적용한 각 기관마다 protocol별 탐지된 패킷의 평균 크기 변화와 탐지건수 합계 변화, protocol별 destination port 번호마다 탐지된 패킷의 평균 크기 변화와 탐지 건수 합계 변화 그리고 protocol별 사용하는 탐지 패킷의 크기에 따른 탐지 건수 합계 변화를 살펴보았다. 아래의 그림에서와 같이 요일을 기준으로 매일 탐지되는 트래픽의 분포가 $\mu \pm 2\sigma$ 기준으로 관리상한과 관리하안 내에 데이터가 포함됨을 알 수 있었다. 이와 같이 발생하는 보안로그 데이터가 큰 변화를 보이지 않고 있음을 알 수 있었다. 탐지되는 보안로그가 관리도를 벗어날 경우 이는 이상 증후로 판단할 수 있을 것이다.

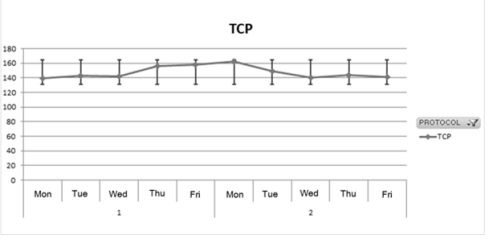

그림 8. SPC기법을 적용한 A기관의 탐지된 패킷의 평균 크기 변화
Figure 8. Changes average size of detected packet using SPC techniques

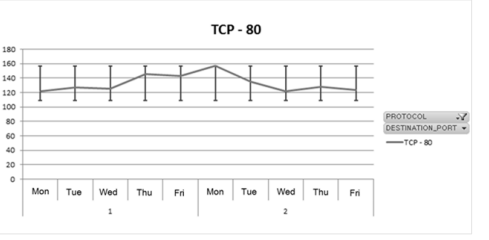

그림 9. SPC기법을 적용한 TCP 목적지 80번 port로 탐지된 패킷의 평균 크기 변화
Figure 9. Changes average size of detected packet for TCP 80 port using SPC techniques

분석기간 동안 해당 기관들의 업무전산망에서 발생하는 보안로그가 비교적 큰 변화가 없어 이상증후를 발견해 내지 못하였다. 이상증후가 발견될 때까지 분석기간을 연장하기 어려운 상황에서 방법론을 다시 한 번 검증하기 위해 인터넷에 연결되지 않은 소규모 네트워크를 구축한 뒤 네트워크 트래픽이 침입차단시스템을 통과하도록 구성하여 제시한 모델의 유효성을 검증하였다.

가상 실험에는 open Source 서비스거부 공격 툴인 'UDP Unicorn'을 사용하였다. 해당도구는 garbage 데이터와 함께 UDP 패킷을 지속적으로 발생시키는 도구이다. 본 연구에서 제시한 방법을 실험 데이터에 적용한 결과 공격 툴이 트래픽을 발생시킬 경우 <그림 10>과 같이 탐지건수와 탐지된 패킷의 크기의 변화가 발생, 이를 통해 이상증후를 판별할 수 있었다.

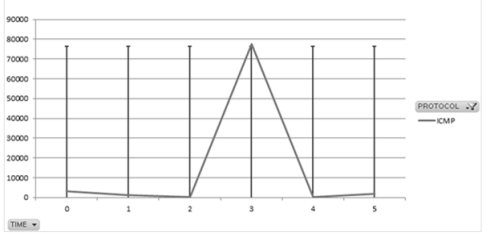

그림 10. 탐지된 패킷 평균 크기 변화
Figure 10. Changes average size of detected packet

6. 결 론

본 연구에서는 망분리 이후 업무전산망의 보안장비에서 탐지되는 이벤트의 패턴이 제어망과 유사한 패턴을 가지고 있음에 착안하여 업무전산망에서 효율적으로 이상 징후를 판단할 수 있는 방법론을 제안하였다. 업무전산망을 인터넷과 분리하여 폐쇄망으로 운영한다고 모든 보안위협이 사라지는 것이 아닌 만큼 망분리 이후에도 업무전산망에 대한 보안위협 요소에 대한 관심이 필요하다. 앞서 살펴본 바와 같이 내부자의 보안위협 등 보안위협은 여전히 존재하겠지만, 외부로부터의 보안위협은 상대적으로 경감되었으므로 기존에 일반적인 open network에서의 침입탐지 또는 보안관제 방법론을 적용하기 보다는, 본 논문에서 제시하는 방법론을 사용하면 보안관제 효율성을 높일 수 있을 것이다.

본 연구에서 활용한 실제 보안 로그에서는 분석기간의 한계로 제시한 방법론을 해당 데이터에 적용한 결과 실제 유해 트래픽을 분류해 낼 수는 없었다. 향후에는 제시한 방법론을 지속적으로 적용 운영하고, 그와 더불어 업무와 무관한 발생하는 트래픽에 대한 발생원인 제거, 유해 트래픽은 아니지만 지속적으로 탐지되는 이벤트에 대한 예외처리 등을 관리, 정비 후 본 방법론의 효과성이나 탐지의 정확도를 다시 검증해볼 필요가 있을 것이다.

References

[1] *Internet and information security top 10 issues in 2014*, KISA, 2014.

[2] *Building guide for network separation and data sharing system*, Ministry of Knowledge and Economy Cyber Security Center, 2012.

[3] *Separate network solutions suitable for our company?*, AhnLab Security Magazine Monthly Ahn, 2011.

[4] Insider Threat, http://www.cert.org/insider-threat

[5] ByungHa Choi, *An analysis of intrusion detection techniques assorted by malicious traffic directions*, KOREA INFORMATION SCIENCE SOCIETY, Vol. 39 No. 1A, pp. 57-59, Jun. 2012.

[6] Huy Kang Kim, *Host based intelligent IDS with RFM analysis methodology*, thesis for a Master degree, KAIST, Dec. 1999.

[7] Chan-Kyu Han, and Hyoung-Kee Choi, *An anomalous event detection system based on information theory*, Journal of KIISE, Vol. 36 No. 3, pp. 173-183, 2009.

[8] Kim min jun, and Kim gui nam, *A study of mining ESM based on data-mining*, Convergence security journal, Vol. 11 No. 6, pp. 3-8, 2011.

[9] Kyu-il Kim, Hark-soo Park, Ji-yeon Choi, Sang-jun Ko and Jung-suk Song, *An auto-verification method of security events based on empirical analysis for advanced security monitoring and response*, Journal of The Korea Institute of Information Security & Cryptology, Vol. 24, No. 3, pp. 507-522, Jun. 2014.

[10] Hyugeun Sin, and Gicheol Kim, *A study of security control technology trends survey and the next generation of security control framework*, Review of KIISC, Vol. 23(6), dec. 2013.

[11] DongHwi Lee, and KyoungHo Choi, *A study of an anomalous event detection using white-list on control networks*, Jouranl of Information and Security, Vol. 12(4), pp. 77-84, Sep. 2012.

[12] Hyunguk Yoo, Jeong-Han Yun, and Taeshik Shon, *Whitelist-based anomaly detection for industrial control system security*, THE JOURNAL OF KOREA INFORMATION AND COMMUNICATIONS SOCIETY, Vol. 38(8), PP. 641-653, Aug. 2013.

[13] Wanjib Kim, Huy Kang Kim, Kyungho Lee, and Heung Youl Youm, *Risk analysis and monitoring model of urban SCADA network infrastructure*, Journal of the Korea Institute of Information Security and Cryptology, Vol. 21(6), PP. 67-81, Dec. 2011.

[14] Pauline Koh, Hwa Jae Choi, Se Ryoung Kim, Hyukmin Kwon, and Huy Kang Kim, *Intrusion detection methodology for SCADA system environment based on traffic self-similarity property*, Journal of the Korea Institute of Information Security and Cryptology, Vol. 22(2), pp. 267-281, Apr. 2012.

[15] *ICT principles of electric power*, Kepco KDN, 2014.

망분리 환경에서의 보안관제 효율화 방안 연구

한창우[1], 김휘강[1], 김은진[2]
[1]*고려대학교 정보보호대학원*
[2]*경기대학교 국제산업정보학과*

요 약

인터넷과 연결된 내부 업무망이 외부 공격에 취약하다는 문제점에 대한 인식이 확산되고 있다. 그에 대한 해결방안으로 조직 내 시스템의 피해를 예방하기 위해 내부 업무망과 외부망(인터넷망)을 분리해 운영하도록 하는 망분리 의무화가 확산되고 있다. 업무전산망을 망분리를 통해 인터넷과 분리하여 폐쇄망으로 운영한다고해서 보안성을 보장받을 수는 없다. 폐쇄망으로 운영하는 제어망에서도 Stuxnet 등과 같은 악성코드로 인한 보안위협은 여전히 존재하고 있고, 사용자 부주의 및 악의적인 의도에 의한 업무망 PC의 인터넷 사용, 보조 기억매체를 통한 정보유출 및 업무망으로의 악성코드 유입 등의 보안위협이 있다. 그리고 업무망과 인터넷망간에 안전한 자료 전송을 위한 자료 전송 시스템을 사용하지 않고도 분리된 네트워크 간에 자료를 전송할 수 있는 기술을 사용하여 통제되지 않는 데이터가 업무망과 인터넷망 사이로 전송될 수 있다. 또한 망분리를 했다고 하더라도 내부자로부터의 보안위협은 여전히 존재한다. 하지만, 여전히 망분리는 정보유출 방지와 침해사고 예방 등을 위한 효과적인 대안으로 많은 조직에서 도입하고 있다. 망분리는 인터넷망과 업무망에서 발생하는 트래픽 형태의 차이를 가져왔고, 각 망의 보안로그의 특성에도 영향을 미치게 되었다. 이에, 많은 연구가 이뤄진 인터넷망과는 별도로, 업무전산망에서 발생하는 보안로그에 대해 효율적으로 이상 징후를 탐지할 수 있는 방안을 필요하다. 본 연구에서는 물리적으로 망이 분리된 환경에서 발생하는 보안로그의 특징을 업무전산망을 중심으로 분석하고 효율적으로 보안 관제를 수행하기 위한 방안을 제시하고자 한다.

감사의 글

본 논문은 미래창조과학부 및 정보통신산업진흥원의 '지식정보보안인력양성 최고정보보안전문가 과정' 사업의 연구결과로 수행되었음(과제번호 : NIPA-H2012-13-1002).

Chang Woo Han received the bachelor's degree in the Department of Industrial & System Engineering from Changwon National University in 2001. He has worked as assistant manager at Kepco KDN since 2001. He has worked at ministry of trade, industry & energy cyber security center since

2008. He has been a student in Graduate School of Information Security in Korea University since 2013. His current research interests include Information Security, cyber attack detection, digital forensics.

E-mail address: onechang@korea.ac.kr

Huy Kang Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1998. He received the M.S. degree in Industrial & Systems Engineering from KAIST in 2000. He worked as Technical Director at NC soft from 2004 to 2010. He received the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2009. He has been a professor in the Department of Information Security at Korea University since 2010. His current research interests include Online game security, network security, network forensic, IDS, botnet detection.

E-mail address: cenda@korea.ac.kr

Eun jin Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1999. He received the MS degree and the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2001 and 2007, respectively. He has been a professor the in Department of International Industrial Information at kyonggi University since 2008. His current research interests include Management information systems, security economics.

E-mail address: ejkim777@kgu.ac.kr