Journal of The Korea Society of Computer and Information
Vol. 24 No. 8, pp. 77-85, August 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.08.077

Safe Web Using Scrapable Headless Browser in Network Separation Environment

Won-chi Jung*, Jeonghun Park*, Namje Park**

Abstract

In this paper, we propose a "Safe Web Using Scrapable Headless Browse" Because in a network separation environment for security, It does not allow the Internet. The reason is to physically block malicious code. Many accidents occurred, including the 3.20 hacking incident, personal information leakage at credit card companies, and the leakage of personal information at “Interpark”(Internet shopping mall). As a result, the separation of the network separate the Internet network from the internal network, that was made mandatory for public institutions, and the policy-introduction institution for network separation was expanded to the government, local governments and the financial sector. In terms of information security, network separation is an effective defense system. Because building a network that is not attacked from the outside, internal information can be kept safe. therefore, "the separation of the network" is inefficient. because it is important to use the Internet's information to search for it and to use it as data directly inside. Using a capture method using a Headless Web browser can solve these conflicting problems. We would like to suggest a way to protect both safety and efficiency.

▸Keyword: Separation of the network, Headless browser, network security, captured Web, safe web

I. Introduction

3.20 해킹사태, 카드사 개인정보 유출, 쇼핑몰 개인정보 유출 등 사고 많은 정보보안 사고가 발생하였으며, 이를 통해 많은 피해자가 속출하였다. 국민적인 관심과 불안감이 높아졌다. 대부분의 업무는 인터넷을 통해 이루어지고 있으며, 공격자는 항상 인터넷과의 접점을 공격하고자 한다. 이런 환경에서 정보보안 강화를 위해 망분리라는 개념을 도입하여, 업무를 사용하는 업무망과 인터넷을 활용하는 인터넷망(혹은 외부망)을 물리적으로 원천 차단하는 정책을 만들게 되었으며, 금융권, 공공기관 또는 국가기관 등 보안이 필요한 곳은 내부 업무망을 인터넷망을 의무적으로 분리하여 해킹이나 악성코드 등의 공격을 원천적으로 차단하는 정책을 도입하게 되었다[1-2].

망 분리 환경에서 업무망과 인터넷망은 분리되어 있으므로, 업무망 단말은 인터넷에 직접 접속할 수 없다. 인터넷 자료가 필요한 경우 담당자는 인터넷망 단말을 이용하여 인터넷 자료를 검색한 후 필요한 일부 정보를 저장하여, 보안USB(보안적으로 인가된 장치) 혹인 망간 자료전송 시스템을 이용하여 안전성 조치를 확인 한 후 업무망에서 이용하여야 한다.

망분리를 적용하기 위해서는 커다란 두 가지 벽이 존재한다.

• First Author: Won-chi Jung, Corresponding Author: Namje Park
*Won-chi Jung (jwonchi@jdcenter.com), Dept. of Convergence Infor. Security, Graduate Sch., Jeju Natl. University
*Jeonghun Park (jeonghun.park@telefield.com), Dept. of Conv. Infor. Security, Graduate Sch., Jeju Natl. University
**Namje Park (namjepark@jejunu.ac.kr), Dept. of Computer Education, Teachers College, Jeju Natl. University
• Received: 2019. 07. 15, Revised: 2019. 08. 12, Accepted: 2019. 08. 12.
• This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) [2019-0-00203, The Development of Predictive Visual Security Technology for Preemptive Threat Response]. And, this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (NRF-2019R1I1A3A01062789)

첫 번째는 많은 예산이 확보의 어려움이다. 단말 관점에서 망분리는 2개의 PC를 지급해야 하기 때문에 모든 사무직원에게 기존에 지급된 PC외에 1대를 더 지급 해야 한다. 또, 단말 노드부터 내부 인트라넷 까지 분리되어야 하기 때문에 연결된 네트워크 장비가 두 배로 필요며, 내부 관리 서버나 정보보호 장비, 정책서버, 배포서버 등 접점 관리가 필요한 장비는 기존 장비 외에 추가로 필요하기 때문에, 장비를 도입하고 운용하는 인력까지 따진다면 기존까지 구축한 정보시스템 및 네트워크 도입비용의 상당부분이 재투자 되어야 하는 상황이기 때문에 기존 정보화 혹은 정보보안 예산과 비한다면, 상당한 예산이 확보 필요하다. 두 번째는 임직원의 변화관리의 어려움이다. 인터넷을 통해 다양한 정보를 활용하여 내부 문서를 작성하고, 외부 메일을 통해 편하게 공유를 했다면, 변화된 환경에서는 제한적이고 불편한 절차를 거쳐서만 인터넷 정보가 활용이 가능하다. 정보보안 담당은 이런 변화 관리를 위해 많은 노력을 펼치지만 새로운 정책에 따른 갈등은 심화되는 양상을 보인다.

본 논문에서 제안하고 하는 내용은 정보보안 담당자와 불편을 호소하는 임직원 사이에서 업무망 및 인터넷망이 서로 분리된 망 분리 환경에서 인터넷을 이용하는 방법을 제안하여, 차단의 관점이 아닌 활용의 관점에서 최근 기술을 활용한 방안을 제시하고자 한다.

II. Preliminaries

2. Related works

2.1 Examples of Korea Domestic Hacking

쇼핑몰에서 근무하는 직원은 업무 시간에 사내 PC에서 웹메일을 접속 후, 동생이 보내 온 메일에 '우리가족' 이라는 첨부가 있었으며, 이 첨부파일은 스크린세이버 실행파일이 있었다. 가족의 메일이라 의심 없이 첨부 파일을 실행하였으나, 실행된 스크린세이버 파일에는 (그림1)과 같이 'ielowutil.exe' 악성파일이 숨겨져 있었으며 파일이 실행과 같이 악성파일은 PC에는 설치된다.

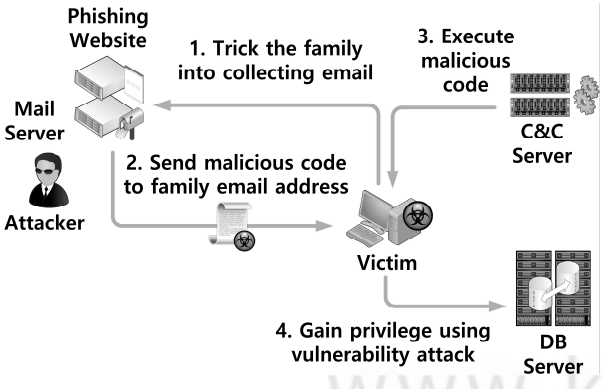

Fig. 1. Information Leakage Through Hacking Mail

이 악성코드는 공격자의 명령제어(Command and Control, C&C) 서버와 통신을 수행한다. 해당 직원은 PC에서 파일공유 서버로 악성코드가 전이 되었으며, 또 다시 파일공유 서버를 경유하여 여러 PC로 악성코드가 확산되었으며, 이와 같이 내부정보를 수집했다. 수집된 내부 정보를 활용하여 개인정보 취급자 PC를 장악하였으며, 이를 통해하여 회사 DB서버로 접근, 그 이후 다른 직원 PC를 이용, 회사DB로부터 개인정보를 외부로 유출 하였다[3-4]. 이 쇼핑몰 업체가 망분리가 되었다면, 해킹메일에 의한 악성코드는 PC 제어권을 빼기었을 지라도 내부 DB를 통한 개인정보 유출사건으로 확대 진행 되지 않았을 것이다.

2.2 Data Exchange System and Design

자료교환 체계에 관한 연구는 다양한 방법으로 진행 되어 왔으며, 이중 일부는 현재까지 살아남는 방식이 되었다. 연구를 살펴보자면, PC를 이용하여 네트워크 중앙에 VM이 탑재된 서버에 접속하여 Server-Client 방식의 응용프로그램을 활용하여 데이터를 저장하여 자료를 교환하는 일련의 방식을 SBC(Server Based Computing) 기반의 자료교환의 체계라고 하며, 이 방식은 서버의 중앙 집중 관리로 통제가 비교적 수월하게 가능하다. 서버로 집중 된 자료는 서버가 탈취될 경우 해당 자료 침해가 발생할 수 있는 단점이 존재한다.

중앙화된 서버의 하이퍼바이저에 유저별 사용자 운영체제를 VM에 연결하여 사용자의 운영체제를 구동하여 사용자 PC에 설치된 클라이언트 프로그램을 이용하여 서버를 통해서 구동되며 이를 네트워크를 통해 이용하는 방식이 서버-데스크톱 가상화 기반의 자료교환 체계라고 한다. 이 방식은 중앙서버가 가상화를 구동할 때 허가된 ActiveDirectory를 승인하는 방식으로 사용자에게 인증된 영역을 사용할 수 있도록 부여하는 방식이다. 장점으로는 클라이언트가 다양한 PC, 운영체제 등을 활용하여 동일한 환경에서 사용할 수 있는 장점이 존재하고, 업그레이드 등 자원관리와 PC 고장 등 물리적인 파손이나 자료 손실 위험에서 다른 방식보다 안전하다고 할 수 있다. 하지만, 사용자가 급증하는 경우 자원을 분할 해 사용하기 때문에 성능저하가 불가피하며, 이를 해결하기 위해서는 서버 증설 등 큰 비용이 수반되기 때문에 예측하여 운영하기 어려운 부분이 있다. 이런 서버-데스크톱 가상화 기반의 자료교환 체계는 현재 운영되는 논리적 망분리의 기원이 된다고 볼 수 있다[5-6].

이밖에, 외부망, 내부망 사이에 공유 스토리지를 이용한 물리적으로 분리된 망 사이에 다른 네트워크(제어망)를 설정하여, 정의된 스토리지 전송 경로를 TCP/IP 등 알려진 통신체계가 아닌 양방향으로 연동을 실시간으로 해주는 방식을 이용하는 스토리지 기반의 자료교환 체계가 있으며, 장점으로는 TCP/ IP 통신을 기반으로 물리적으로 완전히 차단되어 외부망 해커의 공격에 침범 당해도 내부 시스템은 안전하게 보호할 수 있으며, 게이트를 단순화 하여, 입구 등 에서 바이러스, 악성코드 차단 등 정보보안 장비를 총력하여 보안 체계를 구축할 수 있다. 단점으로는 실시간으로 전송받을 수 없는 불편이 존재한다[7-8].

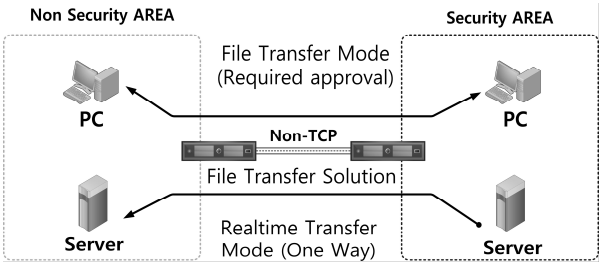

Fig. 2. Network DataTransfer System scheme

공공기관 등에 공유된 망분리 가이드라인을 살펴보면, (그림 2)와 같이 이중 일부는 발전되어 현재 공공기관에서 사용하는 자료교환 시스템의 체계와 설계의 밑바탕이 된 것을 볼 수 있다. 공유 스토리지를 이용한 자료교환 체계는 중계시스템을 활용한 현재의 망간 자료전송이 되었으며, 일방향 전송장치(스트리밍 장비)로 현재 망간 통신이 필요한 서버사이에 사용되고 있다.

2.3 Efficient Network Eeparation Scheme in Network Eparation Environment

업무망과 인터넷을 분리한 기관은 해킹에 의한 자료유출 및 침해사고에 상당한 정보보안 관점에서 성과를 보이고 있으나, 사용자에 대한 불편이 가중되어, 업무의 효율적인 부분에 있어서는 회의적이다. 안전한 정보시스템 네트워크 분리 모델을 수립하기 위해서 업무망과 외부망은 망간자료전송, 일방향 전송장치를 제외하고는 어떤 통신도 허락하지 않는다는 것이다.

이런 체계를 구축하기 위해서는 망을 분리하기 전 모델 수립이 필요하다. 예를 들어, 국가정보통신망과 연결을 해야하는 기관인 경우는 망을 1단계 : 업무망, 2단계 : 국가정보통신망, 3단계 인터넷 망으로 구성하는 것이 적합하며, 감시제어를 위한 통제(SCADA, Supervisory Control And Data Acquisition)가 필요한 경우는 SCADA 망을 별도로 구성해야 한다. 네트워크 분리를 위한 프로세스는 우선 정보시스템 식별이 필요하다. 보유하고 있는 정보시스템을 성격에 따라 대민서비스를 위한 정보시스템, 내부 업무를 위한 정보시스템 영역, 정보보호를 위한 영역, 네트워크나 서버 등 인프라 관리를 필요한 영역으로 분리할 필요가 있다. 특히 기업의 업무 특성상 주요정보를 다루는 정보시스템, 개인정보를 다루기 위한 개인정보처리시스템은 별도로 구분하여 정보시스템을 분류하는 것이 우선적으로 선행되어야 한다. 이를 통해 식별되고 분류된 정보시스템을 안전하게 구분지어 망분리를 수행 할 영역을 나누어야 한다. 식별된 정보시스템을 등급으로 분류하고, 기관의 예산과 상황에 맞게 몇 개의 영역으로 나눌지를 결정해야 한다. 특히 정보시스템이 활용되는 영역과 중요도, 가치는 영역을 분류하는 중요한 기준이 된다[9-14].

이렇게 결정된 영역에 인터넷 허용여부를 다시 결정해야 한다. 크게 나누면 인터넷이 허용된 외부망과 인터넷이 허용되지 않은 내부망으로 구분된다. 여기에 위에서 정한 영역을 추가하여 나누는 방식으로 네트워크 분리 설계 방안을 설계 한다. 기관의 업무효율성, 업무적절성에 따라 외부망을 1개 이상 분리할 수도 있고, 내부망을 국가정보통신망 사용 여부나 기타 사유로 한 개 이상 분리하는 설계를 진행 할 수 있다. 이 밖에도 효과적인 망분리를 수행하기 위해서는 사전에 고려해야 하는 사항들이 추가적으로 존재한다[11-12,15-16].

첫째, 망분리 사업 추진 전 기관내부 조직원의 공감대가 필요하다. 망분리는 기관 정보보안 담당자가 정보보호를 위한 모든 행위가 이행되고, 집중되는 단계이며, 이에 따른 책임도 집중 되어 있다. 둘째, 기관에 적합한 망분리 방식을 선정하는 것이다. 적합한 망분리 선정을 위해 정보보호의 3요소(기밀성, 무결성, 가용성)를 기준으로 하여 자산의 가치를 분석하여 분리 방식을 정할 필요가 있다. 셋째, 정보시스템 접점을 완벽하게 차단하여야 한다. 완벽한 네트워크 분리 완성을 위해 정보시스템 망분리를 하여야 한다. 일반적으로 피씨나 말단 노드의 분리만을 고려하는 경우가 있는데 정보시스템, 네트워크, 정보보호시스템은 분리되어 망분리의 차단 효과를 완벽하게 구축해야 한다. 넷째, 정보시스템간 어플리케이션에 대한 기능 및 구조의 검토가 필요하다. 수신된 사용자의 요청을 처리하고 응답하기 위해서는 다양한 응용어플리케이션이 필요하며, 이들은 다양한 프로토콜과 호환성을 담보하여야 한다. 이를 해결하기 위해서 다양한 프로토콜과 API가 망간 자료전송 시스템이나 일방향 전송장치로(스트리밍 장비)로 정상적인 연계가 되는지 확인이 필요하며, 보안적으로 안전한지 검증이 필요하다. 다섯째, 내부 사용자의 무선 인터넷 및 매체제어 통제 대책 마련이다. 대다수의 망분리 사업은 유선망을 이중으로 구성하는 방안에 중점이 되어있다. 하지만 매체나 무선망을 통제할 수 없다면 외부 위협은 망분리 이전과 동일하게 존재한다. 불법적인 매체의 차단을 위해서는 물리적인 USB 포트 차단 방식과 소프트웨어 방식인 매체제어 솔루션을 이용한 차단 그리고 무선망 차단을 위해서는 다양한 형태의 무선카드를 연결할 수 없는 구조를 만들고 업무공간에서 WIPS(Wireless Intrusion Prevention System)등을 설치하여 차단하는 등의 통제 수단이 사전에 고려되어야 한다.

III. The Proposed Scheme

3. Technical analysis constituting network separation

3.1 Separate network from network and end node viewpoint

망분리는 네트워크를 업무망과 인터넷망으로 분리하여 사용목적에 따라 독립적으로 네트워크를 구성하는 것을 말한다. 망을 분리하는 방법은 크게 물리적으로 독립적인 네트워크를 구성하는 방법과 SBC(Server Based Computing), CBC(Client Based Computing)등 논리적으로 네트워크를 구성하는 방법으로 나뉘며 각 방법의 특징은 (그림3)처럼 명확한 차이를 가지고 있다.

우선 물리적 방법은 고전적인 네트워크 구성을 N개가 아닌 2N개의 형태로 만들어 각 목적에 맞는 별도의 네트워크를 통해 업무 혹은 인터넷을 쓰는 방식으로 목적별로 필요한 영역 네트워크를 구성할 물리적인 네트워크 자원과 물리적인 단말장치가 필요하다. 물리적 필요공간을 많이 차지하며, 비용도 가장 많이 필요하지만 정보보안 관점에서 가장 안전한 망분리 방법이다. 즉 완전히 독립된 네트워크 구조를 사용하고 별도의 PC를 통해 해당 네트워크만 이용하여 망간의 간섭이 없는 독립적인 구조이다. 앞에서 언급한 비용 및 공간의 제약은 기술의 발전에 의해 비용은 절감되고 장비 및 PC의 공간이 줄어들고 있기 때문에 많은 부분에서 해소 될 전망이다[17-21].

논리적 망분리는 많은 방식이 있으나 대부분 현재 사용하고 있는 단말과 연결되어 있는 네트워크를 그대로 이용하며 해당 단말의 OS를 가상화 하여 사용하는 CBC 방식과 단말이 접속하는 서버를 통해 망분리를 사용하는 SBC 방식이 보편적이다. VDI 또한 서버를 통한 가상데스크탑으로 망분리를 하지만 SBC는 서버의 리소스를 완전하게 이용하고 중앙집중식으로 관리가 가능하다는 점이 다르다[22-29].

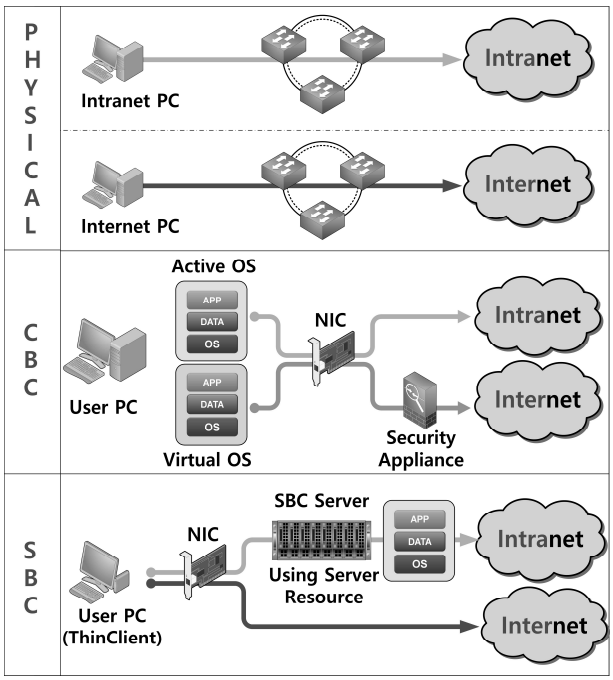

Fig. 3. Network DataTransfer System scheme

3.2 NAC(Network Access Control)

망분리 형식과 관계 없이 NAC는 필수 솔루션이다. NAC는 'Network Access Control'의 약자로 '네트워크 접근제어 및 네트워크 접근통제'라고도 한다. NAC(네트워크 접근제어)는 (그림4)와 같이 제어를 위해 특정 프로토콜들을 사용하여 사용자의 PC 즉 '앤드포인트(Endpoint)'가 내부망 네트워크에 처음 접근시도를 하면, 기존 내부망에 피해를 끼치지 않도록 접속하는 보안 정책들을 적용할 수 있게 하는 네트워크 솔루션이다. 이를 통해 인가되지 않은 장비나 PC는 내부로 들어왔을 때 인가의 과정을 걸쳐야 네트워크를 사용할 수 있다. 명칭에서도 나타나듯이 정책에 따라 서버나 앤드 포인트의 접근을 통제하고 제어한다.

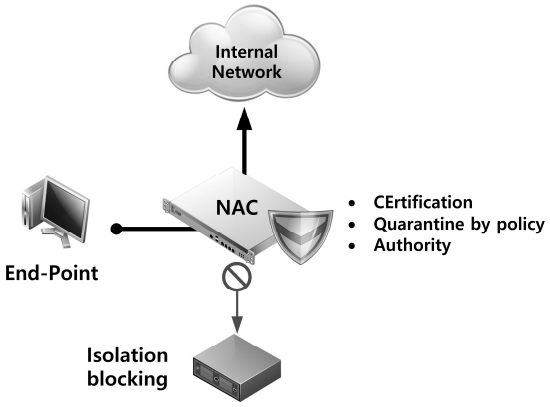

Fig. 4. NAC(Network Access Control) scheme

내부망 접근 전 장비 혹은 PC의 안전 검사를 실시하고 내부망 접근 후에도 어떤 영역으로 접근하는지 가능한 범위와 가능한 역할을 부여할 수 있다. 방식은 크게 네트워크 방식과 Agent 방식으로 운용되고 병행하여 사용 할 경우 효과적인 통제를 수행할 수 있다. 대부분 네트워크 방식의 NAC는 ARP 프로토콜을 이용하여, NAC장비가 Gateway로 착각하게 만들어 인가 여부를 확인하고 통신제어의 역할을 실시한다.

Agent 방식의 NAC는 관리서버로부터 내려받은 정책을 사용자의 정보보호 레벨에 맞게 통제를 실시하며, 특히 앤드포인트의 검염소 역할을 수행 한다. 물리적 업무망 접속을 시도하는 경우에 차단을 수행하기 위해 필수적인 솔루션이라고 할 수 있다. NAC가 없다면 물리적 망분리를 수행하는 기관에서 외부망 PC와 업무망 PC의 네트워크를 바꿔 접속을 시도하는 경우를 효과적으로 막을 수 없다.

3.3 Media control system

정보보안담당자가 필수로 관리해야 할 부분이 바로 매체제어이다. 다양한 매체로 대용량의 파일과 정보를 공유하는 것은 높은 업무 효율을 가져올 수는 있지만 악성코드가 감염되거나 많은 중요한 정보가 유출되는 등 그만큼 취약한 부분이 있다. 망분리를 수행 했을지라고 매체를 제어하지 않는다면 매체를 통한 자료 유출을 막을 수 없기 때문에 안전하지 않다.

두 개의 PC의 양쪽 USB를 연결하여 PC간 통신을 하는 방법도 존재하기 때문에 매체제어는 망분리의 필수 조건이다. 매체제어 방법은 물리적인 제어방법과 소프트웨어 방식으로 나눌 수 있다. 물리적인 방식은 PC를 케이지 같은 곳에 넣어 정보보안 담당자가 열쇠를 가지고 있어, 키보드 마우스 교체 등 특별한 경우가 아니면 매체에 접근하지 못하게 하는 방법이다.

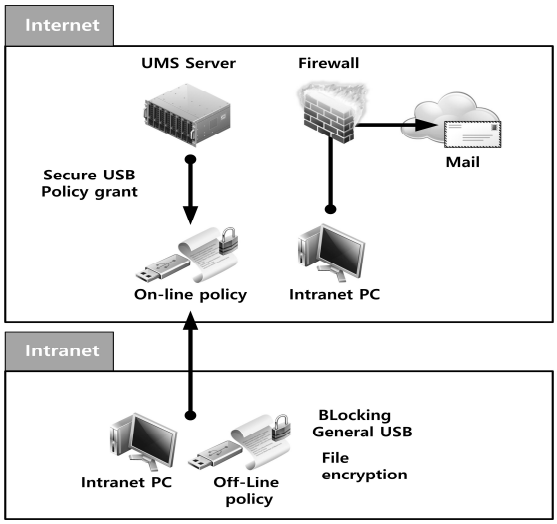

Fig. 5. Media control system scheme

또한, USB를 물리적으로 파손시키거나 제거금지 스티커로 붙이는 방법도 존재한다. 소프트웨어 방식은 (그림5)와 같이 Agent 방식으로 PC에 접근하는 매체를 차단하는 방식이다. 매체제어는 보안 USB와 같이 도입하여 업무망과 외부망 사이의 자료를 보안 USB를 통해 허용하는 방법을 정책적으로 허용 할 수 있다.

3.4 Network connection solution

망연계 솔루션은 망분리가 구축된 환경에서 업무망과 외부망 사이에 서로 다른 네트워크망간 실시간 데이터 연계(Streaming, 그림6-상단), 파일전송(File Transfer, 그림7-하단) 서비스를 정보보안 정책에 맞게 구성하여 안전하게 망간 데이터 전속을 할 수 있는 환경을 제공할 수 있는 솔루션이다.

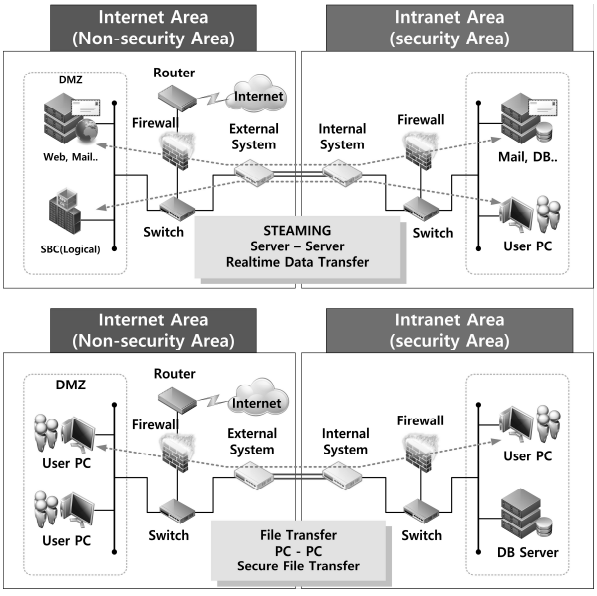

Fig. 6. (top) Streaming system scheme / (bottom) File transfer scheme

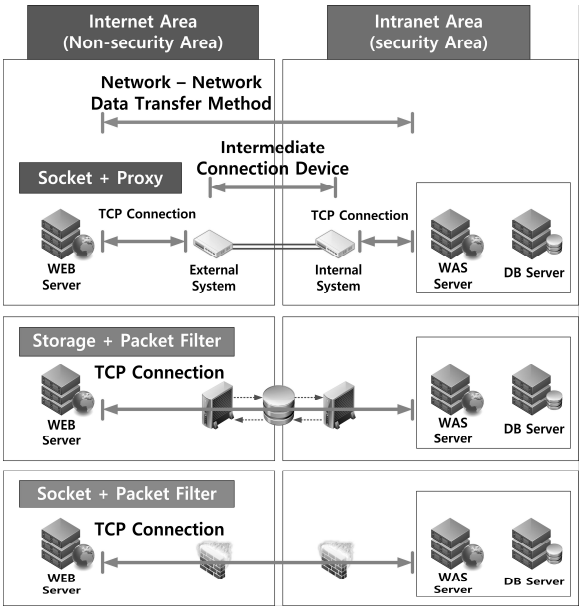

Fig. 7. Streaming and File transfer control mechanism

솔루션의 구성은 크게 두 가지 방법으로 존재하는데 (그림7)과 같이 서버와 서버를 실시간으로 연계하는 스트리밍(Streaming) 서비스가 존재한다. 안전성을 확보하기 위해 단방향 암호화 통신 (Outbound Session을 이용) 방식을 사용한다. 또한 White List 방식을 통해 유요한 접근 IP, Port만 연결을 허용하도록 구성이 되어있다. 파일전송(File transfer) 방식은 결재를 통해 인가된 반출자료를 반입, 반출하는 것을 의미한다. 반입 반출 시는 백신이나, APT솔루션을 통해 숨겨진 악성코드 등을 검사하거나, 실행이 가능한 확장자(exe, msi, scr) 등을 제한하는 정책을 적용하여 운영 할 수 있다.

3.5 Headless Browsing technology

일반적인 웹 브라우저는 웹페이지의 결과를 모니터에 뿌려 사용자가 웹을 인식하도록 한다. 브라우저는 어떤 화면을 어떻게 구성할지를 웹 서버로부터 HTML, CSS 등 파일을 불러와서 화면을 구성하는 역할을 수행하게 된다. 헤들리스(headless) 브라우저 기술은 header없이 수행되는 즉 창이 없는 브라우저라고 이해하면 적절하다. 일반적으로는 검색엔진 등이 사이트 정보를 파악하고 수집하기 위해 Crawling을 수행할 경우에 많이 이용하며, 자동화된 웹의 브라우징 컨트롤을 목적으로 한다. 헤들리스 브라우저를 컨트롤 하기 위한 기술로는 Webkit 기반의 phantom.js, casper.js 가 있으며, Jsdom 기반의 zombie.js, Gecko를 기반으로 한 slimer.js 등이 있으며, 헤들리스 브라우저를 옵션으로 사용할 수 있는 구글 크롬의 Headless Chrome 등이 있다.

이런 기술을 이용한다면, (그림8)과 같이브라우저 구동 없이 웹의 특정 정보를 추출하거나 전체 페이지를 원하는 전자문서로 캡처하여 저장하는 것이 가능하다.

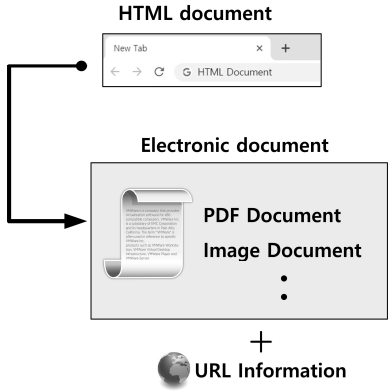

Fig. 8. Web Scraping with a headless Browser

IV. Proposal for improvement of network separation for user convenience

4. Suggestion of user convenience improvement in network separation environment

4.1 Analysis of internet usage requirement in business network

망분리가 구축되어있는 기관에서는 업무망과 외부망이 분리되어있기 때문에 해킹이나 악성코드 등의 공격을 원천적으로 차단하고는 있지만, 망 분리 환경에서 업무망과 외부망은 분리되어 있으므로, 업무망 PC에서 인터넷에 접속할 수 없다. 인터넷에 있는 정보를 업무에 활용하기 위해서는 기관에 맞는 망분리 정책을 따라야 한다. 자료교환 시스템이 구축되어 있는 기관은 인터넷 자료를 다운로드 받아 자료교환을 통해 업무망으로 전달하고 전달받은 자료를 업무망에서 열어 업무자료에 활용한다. 인터넷에 존재하는 한, 두 가지 자료를 활용할 경우는 정보보안을 준수하고 따르지만, 인용해야 할 자료가 다양하고 많은 자료로 요구 될 때 불편함이 존재하며, 정보보안 담당자와 임직원간의 갈등의 요소가 된다. 본 논문을 통해 제안하고자 하는 것은 업무망에서 망분리의 원칙을 위배하지 않고 인터넷을 사용하는 방법이다.

4.2 Use secure web network in the proposed network separation environment

지금까지 망분리의 주요 개념과 자료교환을 위해 필요한 기술들을 살펴보았다. 잠깐 정리해보면, 업무망과 외부망이 단절되어야 하며, 이중 외부망에서만 인터넷이 사용가능해야 한다. 업무망은 안전성의 이유로 인터넷이 차단된 상태에서 회사의 업무를 한다. 하지만 5G가 도입되고 인터넷을 통한 정보를 얻고 이를 업무에 활용할 경우가 많으며, 업무특성에 따라 이런 경우가 더 많은 회사나 직군이 존재 한다. 회사의 특성이나 일부 부서 혹은 직무 담당자의 업무 효율성을 이유로 인터넷을 열어주거나 외부망 PC에 문서편집기를 설치하는 것은 회사의 전체적인 보안 수준을 내려야 하기 때문에 조심스럽게 접근할 필요가 있다. 주목할 부분은 망분리 정책에서 망연계 솔루션과 망간 자료전송 시스템을 이용한 문서 파일의 전송은 허용하고 있다는 점이다. 이를 활용하여 망분리 된 기관 업무망에서 안전하게 웹을 사용하는 방안을 제안하고자 한다.

업무망 단말(Intranet PC)은 접속하고자 하는 사이트의 인터넷 주소를 기 정의된 망간 자료전송방법을 통해 인터넷망 단말(Internet PC)로 전달한다. (그림9)를 참고하자면, 업무망 단말(Intranet PC)과 인터넷망 단말(Internet PC) 사이에 직접적인 통신은 불가능하므로, 업무망 단말(Intranet PC)은 앞에서 설명한 자료전송시스템을 이용하여 인터넷 주소를 외부망 단말로 전달한다.

인터넷 주소는 URL(Uniform Resource Locator) 주소 또는 IP(Internet Protocol)주소 등 인터넷 접속에 사용될 수 있는 모든 종류의 주소를 의미하며, 전송을 위해 프로토콜을 별도로 정의할 수 있다. 인터넷망 단말(Internet PC) 은 자료전송시스템을 통해 전달받은 인터넷주소를 기초로 해당 사이트에 접속하여 데이터를 스크래핑한다.

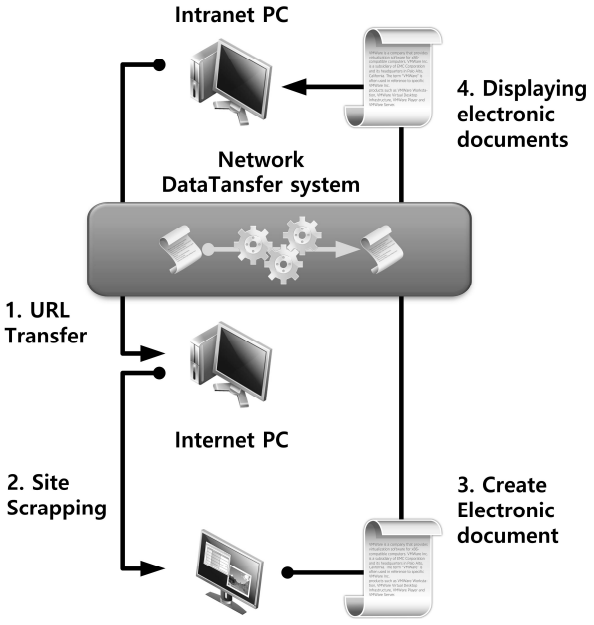

Fig. 9. Safe Web Using Scrapable Headless Browser in Network Separation Environment

(그림10)과 같이, 인터넷 주소가 'www.google.com'이면. 인터넷망 단말에 있는 에이전트가 헤들리스 브라우저를 호출하여 해당 사이트의 구성을 PDF 등 전자문서로 변경하고 저장하며, 이 과정을 사이트 스크래핑(Site Scrapping)이라고 한다. 브라우저를 통한 웹 서피은 악성코드가 포함된 경우 PC를 감염시켜 침해사고 등 피해가 예상되지만 전자문서로 캡처된 웹은 브라우저에서 열릴지라도 악성코드는 작동할 수 없는 상태가 된다. 이렇게 악성 코드 등이 존재할 수 없는 전자문서 형태로 변환한 파일(PDF, 혹인 이미지)을 자료교환을 통해 내부로 전송한

다. 이 방법을 이용하면, 보안을 지켜야 하는 보안 담당자와 자료를 효율적으로 이용하고자 하는 불편을 호소하는 임직원 사이의 갈등의 틈새를 줄일 수 있다.

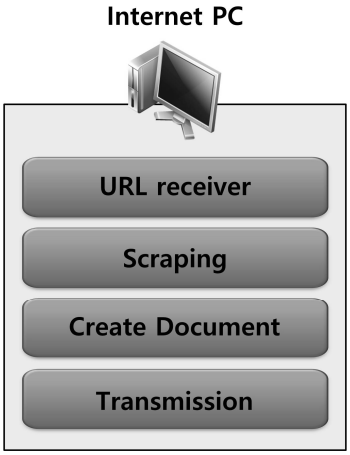

Fig. 10. Features Required for Internet PC Agent

V. Suggestions for Administrators

5.1 A Study on the Direction of Information Security

정보보안 담당자의 역할은 크게 두 가지로 나누어 볼 수 있다. 첫 번째는 관리의 영역이다. 주기적으로 네트워크, 서버, 정보보호 제품에 이상한 계정은 없는지, 적용된 정책이 과도하지는 않은지, 허가받지 않은 권한이나 계정이 생성된 것이 있는지 끊임없이 살펴보고 점검하고, 임직원과 경영진에게 정보보안에 대한 관심을 제고하여 능동적인 정보보안 체계를 확립해 나가는 과정이 필요하다. 두 번째는 기술적 보안영역이다. 외부로부터 공격을 차단하기 위해 기술적으로 대응하는 영역으로 흔히 정보보안 제품인 방화벽, IPS(Intrusion Prevention Systems), IDS(Intrusion Detection System), APT(Advanced Persistent Threat) 대응 솔루션, 백신, DRM(Digital Rights Management) 등등 많은 보안 솔루션이 기술적인 영역의 역할을 수행하는 수행체계이다.

네트워크를 망분리 하는 정책은 두 번째인 기술적 보안영역에 해당한다. 기술적으로 원천적인 망을 분리해서 보안을 강화하는 방식이다. 하지만 이를 통해 기술적 보안영역에서의 성과는 존재하지만 관리적 보안을 수행하기에는 어려움이 생긴다. 관리적 보안은 타 부서와 그 소속 임직원의 협조가 절대적으로 필요하다. 그런데 망분리 같은 대규모 작업을 통해 기술적 영역의 보안체계를 변경하면, 수년, 아니 수십년동안 일해 온 직원들의 반발이 거세며, 이런 급진적인 변화는 불만을 폭주 시키게 만들어 결론적으로 관리적 보안을 약화 시키는 원인이 될 수 있다. 해킹기술의 진화에 맞춰 정보보호 기술은 발전하였으며, 정보보호 기술의 발전이 소속 직원을 불편하게 만들 수 있다. 더 큰 피해를 막기 위한 선제적 조치임을 강조해도 현장에서 업무하는 정보보안 담당자는 감정노동에 시달리게 된다. 이런 시점에서 정보보안의 안전성을 그대로 유지하면서 편의성을 제고하는 연구나 발명이 앞으로 많이 수행되기를 희망한다.

5.2 Administrative Recommendations on the proposed network separation

망분리를 하기 위해서는 막대한 예산이 투입되고 네트워크 서버팜, PC 등 대부분의 모든 것에 수정이 필요하기 때문에 어려운 결정을 해야 한다. 현장에서 경험을 바탕으로 이러한 망분리 정책에 대한 반발을 잠재우기 위한 방법을 고안하게 되었다.

다양한 자료교환, 망연계 솔루션이 존재한다. 이런 다양한 제품이 동일하게 업무망에서 안전한 웹을 이용하기 위해서는 망연계를 통한 웹 브라우징을 위한 프로토콜을 만들 필요가 있다. 그리고 프로토타입의 코드를 작성하고 공개하여, 정보보호 시스템을 만드는 많은 업체가 써드파티로 참여하여 지속적으로 편의성을 주는 방향으로 진화되길 바란다. 또한, 정보보안이 직원의 편의를 고려하고 연관된 시스템을 이용할 경우 정보보안 체계의 준수율과 임직원이 느끼는 정보보안 안전성 평가 등은 다음 연구를 통해 분석할 필요가 있다.

VI. Conclusions

중요자료유출을 방지하기 위한 망분리 사업들이 공공기관을 중심으로 진행되었으며, 기술적인 운영 문제점도 많았지만 많은 부분은 해결해 나가면서 발전해 가고 있다. 특히 보안 USB를 통해 망간 자료 전송을 하거나, 공유 스토리지를 활용한 자료교환 체계는 구조적인 취약점으로 인해 유명무실 해지고 있어, 현재 공공기관에서는 실시간 데이터 연계(Streaming), 파일 전송(File Transfer) 시스템을 구축하여 운영하고 있다.

정보보안의 중요한 역할이 차단이라는 것은 누구나 알고 있다. 하지만, 이 제안을 통해 “정보보안과 효율성은 반비례” 라고 주장하는 속언에 반발하고 싶으며 정보보안 담당과 소속 직원 서로가 서로를 이해하고 배려하는 마음으로 정보보안기술이 발전해야 하고, 이런 방향이 궁극적으로는 소속직원의 적극적인 보안 동참으로 유도되어 관리적 보안 성과로 이어질 것이다.

REFERENCES

[1] Eun-hye Han, In-seok Kim, “Efficient Operation Model for Effective APT Defense,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 27, Issue 3, pp. 501-519, June 2017.

[2] D. Lee, N. Park, "Electronic identity information hiding

methods using a secret sharing scheme in multimedia-centric internet of things environment," Personal and Ubiquitous Computing, Vol. 22, Issue 1, pp. 3-10, Feb. 2018.

[3] Ji-Sang Lee, Jung-Eun Jee, Yong-Tae Shin, "A Study on Network Partition to Cope with Cyber Attack," Proceedings of the Korean Information Science Society Conference, Korean Information Science Society, pp. 313-315, June 2011.

[4] N. Park and M. Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment," Cluster Computing, Vol. 17, Issue 3, pp. 653-664, Sep. 2014.

[5] Jungeun Jee, Sangji Lee, Sungryoul Lee, Byungchul Bae, Yongtae Shin, "A Logical Network Partition Scheme for Cyber Hacking and Terror Attacks," Journal of KISS : Information Networking, Vol. 39, No. 1, pp. 95-101, Feb. 2012.

[6] D. Lee and N. Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance," International Journal of Supercomputing, pp. 1-16, 2016.

[7] Sung-hoon Lee, "A Study on Separate Plan of Efficient Information System Network in Partitioned Network Environment," http://www.riss.kr/link?id=T12468570, pp. 12-33, June 2011.

[8] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia," Electronics, Vol. 8, No. 4, pp. 412, Apr. 2019.

[9] Mi-hwa Lee, Ji-won Yoon, "A Study on Detection Method of Multi-Homed Host and Implementation of Automatic Detection System for Multi-Homed Host," Journal of the Korea Institute of Information Security and Cryptology, Vol. 28, No. 2, pp. 457-469, Apr. 2018.

[10] N. Park and N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," Sensors, Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[11] Seung Jae Jeon, Hun Yeong Kwon, "Public Enforcement and Private Enforcement of Technical and Organizational Measures for Protecting Personal Information," Journal of Law & Economic Ragulation, Vol. 11, No. 2, pp. 269-291, Dec. 2018.

[12] Namje Park, Hyo-Chan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment," Security and Communication Networks, Vol. 9, Issue 6, pp. 500-512, April 2016.

[13] Jin-Woo Park, Hong-Ki Min, Hwanyong Lee, "A Study of Data Exchange System to Prevent Information Leakage Between Intra-Network and Inter-Network," Korea Computer Graphics Society, pp. 156-157, July 2017.

[14] D. Lee, N. Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment," Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[15] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)," International Journal of Distributed Sensor Networks, Vol. 2016, Article ID 2965438, 3 pages, 2016.

[16] Youn-seo Jeong, Ki-Dong Nam, "An Investigation of Network Separation Solution for Government Network," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 1125-1126, June 2011.

[17] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment," Advanced Web and Network Technologies, and Applications, LNCS, Vol. 3842, pp. 741-748, Jan. 2006.

[18] Donghyeok Lee, Namje Park, "ROI-based efficient video data processing for large-scale cloud storage in intelligent CCTV environment," International Journal of Engineering & Technology, Vol. 7, No. 2.33, pp. 151-154, Mar. 2018.

[19] Namje Park, Donghyeok Lee, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment," Personal and Ubiquitous Computing, Vol. 22, Issue 1, pp. 3-10, Feb. 2018.

[20] Donghyeok Lee, Namje Park, "A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance," Journal of the Korea Institute of Information Security and Cryptology, Vol. 28, No. 2, pp. 417-428, Apr. 2018.

[21] Namje Park, "Information Exchange between VTSCs for Secure Next-generation Vessel Traffic System," International Information Institute (Tokyo). Information, Vol. 20, Iss. 2B, pp. 1309-1316, Feb. 2017.

[22] Donghyeok Lee, Namje Park, "A Proposal of Privacy-Enhanced Deduplication Technique in a Cloud Environment," The Journal of Korean Institute of Information Technology, Vol. 16, No.5, pp. 91-102, May 2018.

[23] Jinsu Kim, Sangchon Kim, and Namje Park, "Access

Control Masking Mechanism to Dynamic Image Identification Information," The Journal of Korean Institute of Information Technology, Vol. 17, No. 7, pp. 95-101, Jul. 2019.

[24] Donghyeok Lee, Namje Park, "Institutional Improvements for Security of IoT Devices," Journal of the Korea Institute of Information Security & Cryptology, Vol. 27, No. 3, pp. 607-615, June 2017.

[25] Jinsu Kim, Sangchon Kim, and Namje Park, "Face Information Conversion Mechanism to Prevent Privacy Infringement," The Journal of Korean Institute of Information Technology, Vol. 17, No. 6, pp. 115-122, June 2019.

[26] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission ," Electronics, Vol. 8, No. 7, pp. 735, June 2019.

[27] Jinsu Kim, and Namje Park, "Inteligent Video Surveilance Incubating Security Mechanism in Open Cloud Environments," The Journal of Korean Institute of Information Technology, Vol. 17, No. 5, pp. 105-116, May 2019.

[28] Jinsu Kim, and Namje Park, "Development of a board game-based gamification learning model for training on the principles of artificial intelligence learning in elementary courses," Journal of The Korean Association of Information Education, Vol. 23, No. 3, pp. 229-235, June 2019.

[29] Namje Park, "Privacy-Enhanced Deduplication Technique in Closed Circuit Television Video Cloud Service Environment," International Journal of Engineering & Technology, Vol. 7, No. 3.24, pp. 321-325, Oct. 2018.

Authors

Won-chi Jung received the BSc degree in Computer Science from Soongsil University, Korea, in 2008. He is currently a Master's student in Department of Convergence information Security, Graduate School at Jeju National University since 2018. Won-chi Jung works for JDC(Jeju Free International City Development Center, public institution) as an information security officer since 2014. And he was senior programmer of the Platform Development Team of the SK company for 4 years. He is concerned in the information security technology, Web Services Security, Big Data and Blockchain.

Jeonghun Park received the BSc degree in Computer Science from Korea National Open University, Korea, in 2017. He is currently a Master's student in Department of Convergence information Security, Graduate School at Jeju National University since 2018. Jeonhun Park is a network expert. He has been managing the National Information and Communication Network of Jeju Special Self-Governing Province for 13 years. He has been researching various technologies for efficient management of national information and communication networks. He is concerned in networks, access control and network policy settings.

Namje Park received the BSc degree in information industry from Dongguk University, Korea in 2000, and received his M.E. and Ph.D. degrees in Information Engineering from Sungkyunkwan University in 2003, and 2008 respectively. Prof. Namje Park is a Professor of Department of Computer Education in Teachers College at Jeju National University since 2010.He has been serving as a Research Scientist of Arizona State University since 2010. Prior to joining the researcher at ASU, he had worked as a post-doc at University of California, Los Angeles for 1 year. And he had an appointment as the senior engineer of the information security research division of the Electronics and Telecommunication Research Institute for 6 years. He is concerned in the information security technology field for the mobile environments, IoT system, Smart Grid, Mobile XML Security, Web Services Security, Ubiquitous computing including Sensor Network and a variety of cryptographic technologies. He has many talks related in mobile and information security technologies.