Journal of KIIT. Vol. 6, No. 6, pp. 101-112, Jun. 30, 2018. pISSN 1598-8619, eISSN 2093-7571 101
http://dx.doi.org/10.14801/jkiit.2018.16.6.101

NFS를 이용한 효율적인 논리적 망 분리 시스템 구현 : 공공기관 중심으로

조성호*, 최진탁**

Efficient Implementation of Logically Separated Network System Using NFS : Focused on Public Institutions

Sung-Ho Cho*, Jin-Tak Choi**

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future Planning (NRF-2017R1A2B4005185)

요 약

공공기관과 기업에서 인터넷과 인트라넷을 이용하여 업무의 효율성을 증대시키고 있다. 내부 정보 유출 및 개인정보 보호를 위해 다양한 보안 장비들을 도입하고 있으나, 점차 발전되어 가는 해킹 및 보안 위협 요소에 대해 방어가 늦어지고 있다. 외부 네트워크와 상시 연결되어 있다는 사실이 보안의 가장 큰 위협요소이기도 하다. 근본적으로 인터넷과 인트라넷을 분리하여 상호 연동할 수 없게 하는 망 분리의 필요성이 여기에 있다. 현재 물리적인 망 분리와 논리적인 망 분리 등의 선행연구가 지속되어 있기는 하나, 각기 장단점이 있다. 물리적 망 분리는 구조 변경이 어렵기 때문에 논리적 망 분리에 대한 연구가 활발하다. 본 논문에서는 기존 논리적 망 분리와는 방법을 달리하여 네트워크 파일 시스템을 이용한 논리적 망 분리 시스템을 제안한다.

Abstract

Public institutions and companies are increasing their efficiency by using the Internet and Intranet. We have introduced a variety of network security solution to protect internal information leakage and privacy, but we are delaying defenses against hacking and security threats. The fact that it is always connected to an external network is the biggest security threat. This is basically the necessity of separating the Internet and the intranet from each other and making it impossible to interoperate with each other. Although previous studies such as physically separated network and logically separated network have been continuing, Each has advantages and disadvantages. Since Physically separated network is difficult to change the architecture of network, logically separated network is actively researched. In this paper, we propose a logically separated network system using Network File System, which is different from existing logically separated network method.

Keywords
separated network, logically separated network, network file systems, network security

* 인천대학교 컴퓨터공학과
- ORCID: https://orcid.org/0000-0002-1871-0268
** 인천대학교 컴퓨터공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-1606-3626

· Received: May 08, 2018, Revised: Jun. 19, 2018, Accepted: Jun. 22, 2018
· Corresponding Author: Jin-Tak Choi
Dept. of Computer Engineering, Incheon National University, 119, Academi-ro, Incheon, Republic of Korea,
Tel.: +82-32-835-8493, Email: choi@inu.ac.kr

Ⅰ. 서 론

공공기관에서는 각종 대민서비스를 인터넷을 이용하여 서비스하고 있으며, 개인정보를 많이 취급하고 있다. 특히, 교육공공기관은 학사정보 및 건강정보 등의 학생 개개인의 신상정보를 관리하고, 대학입시에 반영하기 때문에 무엇보다도 개인정보보호의 중요성이 크다. 현재 주요 보안침해요소가 다양화되고 그에 따른 대비책이 세워지는 시기가 늦기 때문에 근본적으로 예방할 수 있는 시스템 구축이 상시 논의되고 있다. 기본적인 네트워크 보안 및 웹 보안 등은 방화벽이나 침입탐지 시스템 등의 기술적 발달로 어느 정도 예방이 가능하지만, 실제 외부로 개인정보 등의 유출이 발생하는 큰 이유는 업무담당자의 개인 PC등에 웜, 트로이 목마 등이 설치되어 외부로 정보가 반출될 수 있고, 이는 바이러스 백신 등으로 차단이 가능하지만 메일이나 메신저 등으로 첨부파일을 통하여 감염이 되는 사례에 대해서는 취약한 부분이 있다.

정부는 이러한 공공기관의 보안 취약점을 해결하기 위한 근본적인 대책으로 망 분리에 대해 가이드라인을 책정하고, 해킹 등 주요 사이버공격으로부터 국가 기밀 등 중요자료의 유출을 차단하고 있다. 망분리 구축 가이드라인에 따르면 물리적 망 분리 방법과 논리적 망 분리 방법의 두 가지 방법을 예시하고, 이를 뒷받침할 기억매체 관리시스템, PC보안 시스템 등의 추가 보안시스템에 대한 부분이 언급되어 있다.

물리적 망 분리의 경우 업무용 PC와 인터넷용 PC를 따로 이용하고, 그에 따른 네트워크 시설이 새로이 추가 구축되어야 하며, 보안시스템 역시 추가 구축되어야 한다. 네트워크 연결의 접점이 없기 때문에 가장 확실한 망 분리의 수단이다. 그러나 기존의 네트워크 구축비용만큼의 비용이 추가 시설되고 단말기 역시 추가로 구성되기 때문에 엄청난 비용의 발생이 가장 큰 문제이다. 또한, 에너지 사용량이 두 배로 확장되어 정부의 Green IT 정책과 병행하기에는 어렵다는 딜레마에 빠진다. 인터넷용 PC에서 생산한 문서를 업무용 PC에서 이용하기 위해 보안 USB를 이용해야 하기에 업무연속성이 떨어지고 생산량이 떨어진다는 단점도 있다. 이를 보완하기 위하여 사용자 PC환경만 망 전환 장치를 이용하는 방법이 있다. NIC(Network Interface Card)만 추가로 설정하여 외부 망 및 내부 망을 망 전환 스위치를 이용해 1대의 PC로 인터넷 망과 업무 망을 사용하는 방법이다. 이 역시도 물리적인 네트워크를 새로 구축하는 비용이 추가로 필요하고, 망 전환 시 재부팅을 해야 하는 단점이 있어 업무의 연속성이 떨어진다. 또 다른 방법으로 멀티 PC를 이용한 망분리 방법도 있다. 업무용 네트워크는 현재 네트워크로 이용하고, 추가로 인터넷 네트워크를 사용하는 PC를 따로 구축하여 호스트-클라이언트 방식으로 인터넷을 이용할 때는 인터넷 호스트 PC에 접속하여 사용하는 방법이다. 네트워크 구축비용은 상대적으로 적어지지만, 각 부서단위별로 호스트 PC 구축비용이 들고, 호스트 PC의 보안에 따라 부서별 업무용 PC의 보안 상태가 정해진다는 단점이 있다[1].

물리적 망 분리를 구축하기에 어려운 두 가지 큰 요건을 업무 연속성 저하와 큰 비용의 발생으로 볼 수 있다. 특히, 공공기관에서는 관리 주체에 따라 예산편성이 이루어지며, 물리적 망 분리는 이 부분에 대해 자유로운 선택이 되기 어렵다. 네트워크 공사가 필요한 시설비, 추가 단말PC의 필요에 의한 자산취득 비, 정보보안 용역에 대한 운영비 등으로 나뉘어져 사업을 추진하기 어려운 부분이 있다. 논리적 망 분리의 기본적인 설계는 “모든 PC가 악성코드에 감염되어 있다”는 가정 하에서 출발한다. 물리적 망 분리와 논리적 망 분리 시스템의 경우 이 기본 원칙을 준수하고 있다. 따라서 본 연구 역시 기본적인 보안지침과 가이드라인을 준수하는데서 시작한다. 논리적 망 분리 시스템이 구축되는 가장 큰 요인은 물리적 망 분리 시스템에 비해 관리가 쉽고, 막대한 인프라 비용이 소요되지 않는다는 점이다. 1인당 PC보급비용, 네트워크 인프라 구축비용, 상용 S/W 도입비용을 감안하면 논리적 망 분리 시스템이 해결점이 될 수 있다. 현재까지 구축된 논리적 망 분리 시스템은 가상화에 기반한 제품들이 많다. 이는 상용 S/W도입비용에서 자유로울 수가 없다. 서버에 업무 망을 구축해도 사용자가 클라이언트로 접속해서 서버의 자원을 쓸 때, 서버에 상용 S/W 라이선스가 도입되어 있어야 한다.

표 1. 물리적 망 분리 방안
Table 1. Methods of physically separated network

Physically separated network	Function	Considerations
Using 2 PCs	Completely isolate network physically to ensure business network integrity	Network and terminal costs are doubled
Using network separation switching device	Using a network-to-PC switch in a single PC secure work safely	Degraded business continuity when switching network
Using multiple network PC	Physical separation security and transition effects on a single PC	Security Dependent on Internet Host-PC

클라이언트 기반 컴퓨팅에 가상화를 구현하여 VPN으로 망을 분리할 때에도 사용자 PC내의 가상화 O/S환경에서 상용 S/W라이선스가 도입되어야 한다.

이를 감안하여 사용자 PC의 물리적 자원과 S/W 사원을 가지고 업무 망을 이용하고, 인터넷 환경을 할 수 있는 논리적 망 분리 시스템을 구현하는 것이 본 연구의 목적이다.

본 연구에서는 NFS(네트워크 파일 시스템)에 기반한 논리적 망 분리 방안을 제안하고자 한다. 망 분리 사업의 가장 큰 어려움인 비용 절감부분과 업무 연속성 부분을 개선하고, 어느 정도의 보안 안정성을 확보하는데 그 목적이 있다고 하겠다.

기존 가상화 기반의 논리적 망 분리가 아닌 네트워크 웹하드 S/W인 ClouDoc제품을 기반으로 논리적 망 분리의 관련 연구에 대해 알아보고, 문제점을 보완할 수 있는 부분을 고려한다.

사용자 입장에서 망 분리 시스템 이용에 대한 기초나 응용 교육 없이도, 기존 업무를 보던 익스플로러 기반의 업무환경을 지원한다. 업무 연속성을 위해 기존의 물리적 망 분리의 단점이었던 재부팅이나 가상화 기반 논리적 망 분리의 접속허용 및 해제에 대한 부분을 배제할 수 있도록 한다. 관리자 입장에서는 생성된 데이터의 공유 및 권한 설정, 인사이동이 있을 시에 해당 업무 폴더의 사용자 재지정 등의 업무처리를 지원한다.

보안에 치우친 망 분리 시스템이 외려 업무의 질적 저하를 일으키는 문제점을 보완하고, 업무연속성을 중시하게 되면 안전성이 떨어지는 부분의 경계점을 충분히 숙지하고, 사용자와 관리자 모두를 충족하고 망 분리 가이드라인을 준수할 수 있는 논리적 망 분리 시스템 구축이 본 연구의 핵심이라고 하겠다.

본 논문의 구성은 다음과 같다. 2장은 관련연구로 기존 논리적 망 분리 시스템의 구성과 단점, 보완할 점에 대한 부분에 대해 기술하고, 업무 연속성을 위한 스토리지 기반의 연동 시스템 구축 연구내용에 대하여 논한다. 3장에서는 NFS를 이용한 논리적 망 분리 시스템의 기본 설계와 방향에 대해 소개한다. 4장에서는 구체적인 NFS를 이용한 논리적 망 분리 시스템의 네트워크 락(Network-Lock)기능과 그 기능의 개발 명세에 대해서 기술하고, 적용된 결과에 대해 논한다. 마지막으로 5장에서는 결론에 대해 기술하고 본 연구의 기대효과와 문제점, 향후 연구에 대하여 제시한다.

II. 관련 연구

2.1 논리적 망 분리 시스템

앞서 서론에서 물리적 망 분리 시스템의 종류와 고려사항에 대해 다루어 보았다.

비용적인 문제와 전력소비, 업무효율성 저하 등의 문제로 논리적 망 분리 시스템이 대안이기는 하나, 각기 장단점이 있기 때문에 선택 시 단점을 보완할 수 있는 시스템으로 많은 연구가 필요하다[2][3].

현재 논리적 망 분리 시스템은 가상화 기반으로 두 가지로 분류될 수 있다. 서버기반의 망 분리(Server Based Computing)와 클라이언트 기반의 망 분리(Client Based Computing)이다.

표 2. 물리적 및 논리적 망 분리 장·단점
Table 2. Pros and cons of physically separated network and logically separated network

Division	Physically separated	Logically separated
Advantages	· Gain visibility · High use recognition rate · Ensure the safety of the internal network by the complete network separation	· One PC per user · GreenIT
Disadvantages	· Two PCs per user · Reduced work efficiency · High costs · GreenIT policy reversal	· Lack of reliability of virtualization · Violation of S/W license policy · Fifficulty handling multiple virtual servers

2.1.1 SBC 논리적 망 분리 시스템

가상 머신을 탑재한 서버에 접속하여 내부 업무 망을 사용하고 인터넷을 사용할 시에는 기존 PC는 환경과 동일하게 이용하는 방식이다. VMware와 같은 가상머신을 탑재한 서버를 중앙에 두고 각 사용자 PC가 중앙 서버에 접속하여 업무 망을 이용한다. 서버시스템 유지관리 효율성이 높으며, 서버에 생성된 문서는 서버에서만 보관되어 외부 유출의 위험성 또한 적다[5]. 물리적인 네트워크 증설비용은 없으나, 가상화 S/W와 가상화 서버에 설치되는 응용 S/W라이선스에 들어가는 비용이 매우 크다. 또한, DDos에 취약하며, 공공기관 특성상 공문에 의해 답변 자료가 몰리는 경우 다수의 이용자가 이용하게 되면 속도가 느려지는 문제점이 있을 수 있다.

2.1.2 CBC 논리적 망 분리 시스템

개인 PC의 H/W 사양이 고도화되면서 쓰이기 시작한 방법이다. SBC 기반의 논리적 망 분리 시스템과 비슷하게 가상화 기반에서 동작하지만 개인별 데스크탑 PC에서의 가상화 방법이다. NIC를 두 개 사용하여 분리된 망으로 연결하는 방법이 있고, VPN을 이용하여 내부 망으로 접속함으로써 망 분리를 하는 방법이 있다. 전자의 경우에는 물리적 망 분리의 범주에 들어간다. 데스크톱 OS를 가상화 하여 Host OS와 Guest OS를 구성하여 각각의 영역에 다른 네트워크를 설정한다[4]. 서버 구축에 도입되는 비용은 없으나, 가상화 S/W나 개인 PC상 OS마다 설치되어야 하는 응용 S/W 라이선스에 대해 논란의 소지가 있으며, 응용 S/W의 충돌 현상이 잦다. 또한, 본 연구에서 제시되는 논리적 망 분리 시스템보다는 상대적으로 도입 및 관리비용이 많이 든다.

2.2 NAS를 이용한 NFS 연동

본 연구는 웹하드 S/W인 ClouDoc을 기반으로 한다. 형태는 SBC기반의 논리적 망 분리 시스템이지만, 근본적 설계가 다르다. 가상화 서버에 접속하는 것이 아닌 웹하드 S/W 관리서버에 접속하여 NFS가 개인 PC에 마운트 되는 것과 네트워크 락(Network-Lock) 설정의 서비스만 이용한다. 따라서 문서의 저장 및 액세스 부분이 SBC기반 논리적 망 분리 시스템과 같이 다수의 사용자가 몰릴 때 성능문제가 될 수 있다.

개인 사용자별 볼륨을 할당하는데 있어서 SAN을 고려해 볼 수 있지만, SAN Network를 별도로 구축하는데 엄청난 비용이 발생하고, 개인별 볼륨을 할당하는데 있어서 관리적 어려움이 발생한다. 기존 물리적 망 분리 및 SBC 기반의 논리적 망 분리 시스템에서 업무효율성의 문제가 있었다. 업무 문서를 생성하기 위해 인터넷 자료들이 상당수 필요하나 사용자 입장에서 공유하기 위해 보안 USB를 이용한 물리적 복사작업이 시간을 많이 낭비하고, 생산성을 저하시키는 요인이 되었다. 이를 해결하기 위하여 업무 망과 인터넷 망을 보안 정책에 위배되지 않게 데이터만 연동할 수 있는 연구가 진행되었으며, NAS를 이용한 방법이 연구되었다. 읽기/쓰기 권한을 망 접속 상태에 따라 차별적으로 부여하여 연동하는 방법이다[5]-[7]

기존에 NAS가 많이 쓰이지 않았던 이유는 네트워크 대역폭이 작다는 약점이 있어서였다. 수십 명 이상의 동시 접속자 처리 시 1Gbps의 대역폭으로는 이를 감당하기 어려웠지만, 본 연구에서는 웹하드 S/W와 NAS간의 네트워크 구성을 10Gbps로 설정하여 이러한 문제를 해결하고자 하였다.

III. NFS를 이용한 논리적 망 분리 시스템

3.1 주요 연구 내용

NFS를 이용한 효율적인 논리적 망 분리 시스템 구현을 위해 다음과 같은 몇 가지 과제를 설정한다.

첫째로, 가상화에 기반을 두지 않는다. 본 연구 목적의 중요한 부분은 비용 절감이다. 가상화 자체가 논리적으로 2대의 운영체제를 이용하고, 망을 분리하여 독립적인 기기를 운영하는데 기반을 두고 있기 때문에, 상용 S/W 라이선스 정책에서 자유로울 수 없다.

다음으로, 업무 망에 연결되었을 때에는 인터넷 연결이 끊어지고, 인터넷을 쓸 때에는 업무 망에 접속이 불가한 환경을 만들 수 있다. 이 가정으로 1대의 PC자원으로 2개의 네트워크를 쓸 수 있다는 가설이 세워진다. 또한, 악성코드에 감염되었어도 업무망을 쓰는 동안은 인터넷 연결이 되지 않아 외부로 자료유출이 되지 않는다고 볼 수 있다.

업무용 데이터는 보안시스템 내부에 있는 스토리지에 저장하고, 사용자 PC에는 어떠한 업무용 자료를 남겨두지 않는다는 대전제를 세운다. 여기에서 NFS를 이용하는 당위성이 나온다. NAS 스토리지에 각 사용자별 계정을 만들어 관리서버에서 관리하고, 스토리지의 데이터는 사용자의 로컬 디스크에 저장을 시키지 않도록 한다. 업무 망을 이용할 때에는 사용자의 로컬 디스크는 쓰기가 금지되며, NAS에 설정된 “세이프드라이브”에만 쓰기가 허용된다.

사용자 PC가 세이프 드라이브에 로그인을 하면 인터넷이 차단되고, 업무자료를 사용자 PC에 있는 응용 S/W를 이용해 생성, “세이프드라이브”에 저장하면서 업무 시스템을 활용한다. 이후 로그아웃 시 사용자 PC에 업무자료가 저장되는 Cookie, 임시파일등을 삭제하고, 인터넷을 허용한다. 사용자 PC에는 기본적인 백신 및 키보드 보안 프로그램이 탑재되어야 하며, “세이프드라이브”는 메인 보안시스템 내부에 위치하여 외부 해킹 공격으로부터 보호되어야 한다.

3.2 사용자 환경에서의 구현 방법

표 3. 운영환경 및 구현방법
Table 3. Operating environments and implementation methods

Division	Implementation
Security features	· The data transmission between the PC and the server and the file storage in the system are applied to the cryptographic module verified by the NIS ✓Restrict access by administrator or hacker · Temporary file / Intermediate save automatically in PC when connecting to system Creation of security area for file / cache file, deletion of area or discretionary access when disconnection · Provides general internet blocking function excluding network bandwidth (IP based) specified by the administrator when accessing the system
Availability Coherence	· Install related S/W on two servers · Maintain file integrity when a user fails in connection state (editing of file, etc.)
User support	· Announcements, FAQs, Q / A (simple inquiries, improvement requirements, etc.), online help
Admin function	· Maintain management records of top and middle managers · Provide new user subscription UI, approve and manage · Multilevel, Hierarchical (departmental, etc.) administrator designation / authorization / release · Specification of export allowable IP band · Manage site (IP, URL, etc.) to allow / block users when accessing the system · Taking into consideration the transfer of personnel, etc., · Access records, Display (daily / monthly / yearly) statistics, capacity utilization rate per user, report output (graph usage etc.) · Adjust capacity allocated per user / group · Real-time monitoring of system load ratio (CPU / Memory / storage / traffic, current users, etc.) · Various log management function

기본방향은 업무 생산성 유지를 위해 기존 PC사용 환경에 최대한 친숙하게 구현하여야 한다. 시스템에 저장된 파일의 다운로드 후 접근 방식이 아닌 직접 접근하여 응용 S/W와의 호환성을 가진다.

시스템 접속에서의 보안은 Key-Logging방지 프로그램 작동 하에 ID+기관고유 PKI인증서를 사용하여 접속환경을 구현하였고, 기존 사용자 PC에 운영 중

인 백신 프로그램의 최신 버전 적용 여부, 실시간 감시 상태 여부를 확인하도록 하였다. 구체적인 운영환경 및 구현 방법은 표 3과 같다.

보안성 여부에서 사용자가 자료공유를 원할 경우 생성한 폴더를 다른 사용자에게 Read-Only, Read-Write등의 권한별 공유 설정/해제하도록 한다. 자료 반출은 관리자가 허용한 IP 대역에서만 반출이 가능하도록 하며, 로컬 드라이브나 사용자의 메신저 메일 등으로 반출할 경우 관리자 승인 절차 경유하고, log로 기록이 남도록 한다. 접근기록은 각 파일별 접근 기록 및 통계를 낼 수 있고, 접근자의 PC IP, 이용자 ID가 포함된 세부적인 내용으로 기록을 남기도록 한다.

이후 인사이동 및 업무분장에 변화가 있을 경우 자료 인계에 대해서 특정 사용자에게만 인계될 수 있도록 한다. 이외에도 관리자가 지정한 정책, 권한 등을 실시간 적용하도록 하며, PC의 일반 저장장치에 업무용 자료를 저장하지 않도록 강제화 정책을 구현한다.

IV. NFS를 이용한 논리적 망 분리 시스템 구현을 위한 개발 명세 및 수행 결과

4.1 네트워크 락(Network-Lock) 기능 개요

관리자가 설정한 네트워크 차단 정책을 통하여, 업무 PC는 인터넷을 차단하거나, 업무 망을 차단한다. 사용자는 두 차단 모드 간 전환을 통해 필요한 업무를 수행한다. 각 업무 PC에 설치된 Agent(NDIS Filter Driver)는 통신 패킷의 IP 정보를 바탕으로 해당 통신을 차단/ 허용할 것인지 판별한다. 이는 기존 연구되었던 트래픽 분석을 기반으로 하여 공격 트래픽 탐지 시 파티션 게이트웨이(Partition Gateway)에게 망 분리를 통보하는 LNP(Logical Network Partition)기법과 유사하다[8].

네트워크 락이 동작하는 데 있어서, 내부업무 시스템을 사용할 수 있는 네트워크 환경을 내부 망이라 정의하고, 관리자는 내부 망으로 허용할 복수의 IP 대역과 도메인을 관리한다.

또한, 인터넷을 이용 가능한 네트워크 환경을 외부 망이라 정의하고, 관리자는 외부 망 모드에서 차단할 복수의 IP대역과 도메인을 관리한다.

4.2 네트워크 락 시스템 구성도

네트워크 락 기능과 관계된 클라이언트 모듈의 시스템 구성도는 그림 1과 같다. 네트워크 락 모듈 설치가 완료되면 위 시스템에서 NDIS Intermediate Filter Driver가 동작한다.

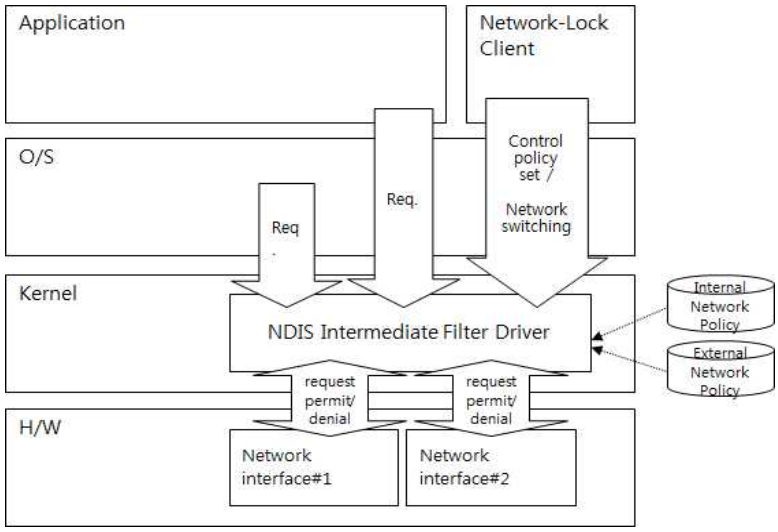

그림 1. 네트워크-락 클라이언트 모듈
Fig. 1. Client module of network-lock

일반 응용 프로그램, 운영체제에서 통신이 발생하면 H/W에 전달되기 전에 네트워크 락 모듈에 의하여 내부망/외부망 정책을 적용받게 된다. 네트워크 락 클라이언트는 내부 망/외부 망 전환을 설정할 수 있으며, 네트워크 락 모듈에 내부 망/외부 망 정책 설정을 할 수 있다. 네트워크를 모니터링하여 통신 패킷을 관리자가 설정한 정책에 따라 차단/허용하고, 사용자의 망 전환 요청에 따라, 내부 망 정책 또는 외부 망 정책이 설정된다. 이때, 내/외부 망 정책을 로컬에 캐시 형태로 저장 관리하여 윈도우 재시작 후 외부 망이 기본으로 설정되도록 한다.

4.3 망 모드 전환 작업

내부 망 모드에서 외부 망 모드 전환 시 수행되는 프로세스는 ClouDoc의 문서를 열고 있는 편집 애플리케이션을 종료하고서야 외부 망 연결모드로 전환이 가능하고, 강제 프로세스를 종료하기 보다는 사용자가 각 프로세스를 종료하게 유도하고, 종료된 프로세스는 목록에서 자동 삭제되도록 처리한다.

이후 ClouDoc 드라이브의 마운트를 해제하고, 클립보드 내용을 초기화 한 후 인터넷 임시 폴더를 삭제하는 프로세스로 이루어진다.

4.4 상황별 이용 형태 결과

사용자 관점에서의 상황별 이용형태 결과는 다음과 같다. 윈도우 로그인 후 바로 외부 망 모드로 진행되며, 마지막 외부 망 정책을 적용받는다. 이때 사용 가능한 디스크는 로컬디스크이다.

외부 망 상태에서 내부 망 로그인 진행시 로컬디스크의 인터넷 캐시영역은 초기화되며, ClouDoc프로그램상의 세이프드라이브에 접속이 진행된다. 지속적으로 서버에서 주기적으로 정책을 받게 되고, 외부 망 자료를 카피하기 위한 클립보드는 초기화시키지 않는다. 내부 망 상태에서 외부 망으로 전환시에는 ClouDoc프로그램상의 세이프드라이브는 마운트 해제되며, 인터넷 캐시와 자료의 반출을 막기 위해 클립보드 역시 초기화시킨다. 이 프로세스에서도 주기적으로 서버에서 정책을 받아 진행한다.

표 4. 상황별 이용 형태
Table 4. Situation type of network switching

Status		User action	Required action	Applied network state	Available disk	Internet cache initialize	Clip-board initialize	Remarks
Windows Login		-	-	External network	Export disk	-	-	At logon, it goes to external network mode and applies the last external network policy.
External network mode	Before Login	Login progress	-	Internal network	NFS On/Offline temporary disk Export disk	Remove	-	Server periodically receives policy
		Internal network switching	Login required	Internal network	NFS On/Offline temporary disk Export disk	Remove	-	Server periodically receives policy
	After login	Logout progress	none	External network	Export disk	-	-	-
		Internal network switching	none	Internal network	NFS On/Offline temporary disk Export disk	Remove	-	Server periodically receives policy
Internal network mode	Before login	n/a	n/a	n/a	n/a	n/a	n/a	n/a
		n/a	n/a	n/a	n/a	n/a	n/a	n/a
	After login	Logout progress	Exit the program that is using the NFS file	External network	Export disk	Remove	Remove	-
		External network progress	Exit the program that is using the NFS file	External network	Export disk	Remove	Remove	Server periodically receives policy

사용자 관점에서 상황별 이용 형태는 표 4와 같다.

사용자가 외부 망 사용 시 웜이나 랜섬웨어 등에 감염될 수 있다. 3.2절에서 기본적으로 백신 및 키보드암호화 프로그램이 사용자 PC에 있고 주기적으로 업데이트 여부를 확인하고 있다. 백신 등에서 감염되었다고 판명되는 단말기는 내부 망으로 접속을 할 수 없다. 안전한 타 사용자의 PC에 기관고유 PKI인증서를 복사하여 이용하여야 한다. 내부 망 자료는 원천적으로 관리자의 승인 없이는 반출이 불가능하며, 내부 망 접속 시에는 개인 PC의 디스크에 쓰기가 금지된다. 외부 망 모드 시에는 내부 망의 NFS 연결이 끊어지므로 신종 멀웨어나 APT 공격에도 안전하다. 감염된 PC가 내부 망 자료를 전송하려 해도 외부 망이 끊어져 있는 상태여서 전송이 불가능하며, 별도의 파일을 만들어 저장했다가 차후 전송하려 해도 개인 PC의 로컬 디스크에 저장이 불가능한 상황이므로 자료 반출의 우려가 없다.

4.5 테스트

표 5와 같이 사용자 환경과 관리자 환경에서 테스트 하였다. 각 상황 분류 별 확인 방법을 통해 테스트 내용과 같이 운영하였고, 업무상 필요한 모든 내용을 만족하였다. 개인 PC와 문서 중앙화 되는 NFS간의 연계 문제로 백신 프로그램과 키보드 보안, 로그인시 공인인증서 관리 등이 연계되어야 하며, 각 솔루션을 모니터링 하여 내부 망 모드를 허가 또는 거부의 판단을 내려야 하는 것이 중요한 핵심이다. 전체 시스템 관리자는 그 허용 범위에 대해 지속적으로 판단하여 가장 업무에 적합하도록 정책 설정을 하여야 한다.

표 5. 테스트 리스트
Table 5. Test list

Category			Checking method	Test contents
Main	Middle	Small		
User environment	Connecting and disconnecting the system	ID+EPKI certificate-based login	Login	Do I need a certificate in addition to my login ID?
				Does it print an error message when login fails? Is the content of the message appropriate?
		Check the vaccine program	Login	Is the login successful only when a vaccine is installed and real-time monitoring is enabled?
				Does it print an error message when login fails? Is the content of the message appropriate?
	Access UI	Windows explorer	Install and run the client for Windows (Not applicable to Information Protection Manager)	Is the Cloudoc disk mounted as a local drive? (eg.X: \)
			Delete files on Cloudoc disk	Is the deleted file moved to its own trash when deleting the file?
	Search	Search file name	Explorer Basic Search	When searching by file name, is the data in Cloudoc disk normally searched?
	Document version	Version control	Editing Save and right-click an Office document and then manage the file →Version control -OfficeWord,Excel,PowerPointFile	If you click restore at any time, will the restore file be created normally?
		Delete drafts	Check for storage data	Are the temporary files deleted after a set period of time?
	Share data	Shared folder	Right-click the folder and set the share and license	Can I share private folders with other departments or individuals?
				Does the permissions of the shared folder apply normally?(eg, read only, read / write, etc.)

User environment	Export data	Export allowed IP	Information Protection Manager → DiskLock → Set export IP	Is it possible to apply for export only in the allowed IP band?
		Via approval procedure	Right-click the file and apply for export	If you fill out the title and contents in the application for exporting documents, select the approver, decide the export period, and apply for the export, can you apply normally?
		View export status	System tray rightclock → Document export status	Can I retrieve the history of the document export request and the history of the request?
	Access record	Access record	Information Protection Manager → Security → Log Search	Can I view the file-by-file access history for the central document?
	Data transferr	Data transfer	Web page → Login → Transfer data	Is the data transferred to the personal documents to be handed over after approval?
	Network separation	External network	Agent login → widget is in external network mode	Is it possible to access other than the limited IP area?
		Internal network	Switch from widget to internal network mode	Is it possible to access only the IP areas that are allowed access?
		Process termination	Open the central document in the internal network → Click the external network in the widget → End process window	Does the process termination window work normally when switching modes?
		Delete clipboard	Copy file or text contents from internal network → Switch to external network → Paste	Are the copied contents or files copied in external network mode?
		Delete internet cache	Use the Internet in the internal network → Switch the external network → Check the Internet cache folder	Are cache files stored in the Internet cache folder deleted?
	Remarks	Malware defense	Set up WhiteList for Central document folder with DiskLock policy settings	Is Central Disk accessible to applications files allowed by the DiskLock policy?
		Policy and permissions real-time application	System Tray Right-click → Refresh Policy	Are the policies and permissions specified by the administrator (after the cache update) applied to the user immediately?
		Install Agent for PC	Click Web Page → Login → Install button	Is the Agent program installed normally?
		Update Agent for PC	Agent login	Do you check for the latest version and update automatically?
		Prohibit local storage of business material	Attempt to save forbidden documents through policy	Do not store Do application documents are stored on a PC local disk?
Intallation and operating environment	Security features	Data transfer encryption	Check packets with TCP / IP capture program	Is the central server communication in SSL?
		Encrypt system save files	Open the secure+ extension file on the server.	Is the file encrypted so that it can not be checked?
		Restricted viewing of administrator files	Service Manager → Agent Login → Check the files in Central Document.	Can the service administrator check the list of users' files?
		Delete temporary save file	Switch between internal and external network mode → Check the files in the Internet temporary folder.	Are the files in the Internet temporary folder deleted?

Intallation and operating environment	Security features	Saving prohibited/ saving off setting	Information Protection / Service Manager → DiskLock → Console Execution → Edit Policy, Apply Policy	Is the policy set by the administrator well applied to the user? (Test after policy cache update and policy refresh)
		Block the specified out-of-network Internet	Internal network mode → Allowed IP area site connection	Is the allowed IP area site accessible?
			Internal network mode → Access permitted IP area sites	Is site blocking for unauthorized IP areas blocked?
	Ensure availability consistency	Server redundancy	Open the central document → Exclude user-connected servers from L4	Is the open document stored on the central server?
	User support	Notice	Service manager → board management → notice registration	Can the user see the notices registered by the service manager?
		FAQ	Service Manager → Board management → FAQ Registration	Can the user see the FAQ registered by the service administrator?
		Q&A	User → Customer Support → Q&A Registration	Can the administrator view the Q&A registered by the user?
			Service manager → Board management → Q&A confirmation and registration	Can you confirm the answer after registering Q&A?
	Administrator function	Management activity record	Information Protection Manager → Security → Security Log → Search Log → Set Permissions	Is it possible to check the history of operations such as entering, modifying, and deleting permissions?
			Information Protection Manager → Security → Security Log → Log Search → History of Member Information	Can I check the history of membership creation, withdrawal, information viewing, and change?
		Administrator IP login restrictions	Information Protection Manager → Security → IP Authentication → Create IP Certificate	Is it possible to login to the administrator only in the allowed IP band?
		Sign up and approve new users	Web page → Member registration, Service manager → Member search → Subscription processing	Is the subscription and approval normal?
		Assigning a Folder Manager by Department	Service manager → Agent login → Select department folder Right click → Folder manager	Does the granted privilege apply to the user?
		IP area assignment allowed for export	Information Protection Manager → DiskLock → Set export IP	Is it possible to set the exportable IP area?
		Manage sites to allow and block during system access	Service Manager → Network Lock → Console Execution	Is it possible to register IP areas allowed in internal network mode?
				Is it possible to register the IP area to be blocked in the external network mode?
		Take over data arguments	Service Manager → Member Management → Member Search → Select Data Transfer Target	Is the data transfer to a specific user successful?

Intallation and operating environment	Administrator function	View access history	Information Protection Manager → Security → Security Log → Log Search → File Access	Are upload, download, deletion, name change, move, log-in history normally displayed?
		View resource status	Service Manager → Statistics → Resource Status	Is resource utilization of storage, users, and departments properly viewed?
		View user subscription status	Service Manager → Statistics → Subscription Status	Are the daily and monthly subscription statuses displayed normally?
		View usage status	Service Manager → Statistics → Usage Status	Is the usage status by time, day, and month normally displayed?
		Assignment capacity adjustment	Service Manager → Organizational Chart Management → Edit → Start the whole organization chart editor Right-click the department → Manage the department chart	Is the capacity of the department box adjusted normally?
			Service Manager → Organizational Chart Management → Edit → Start the whole Organization Chart Editor Right-click → Properties → Change Capacity	Is the user's personal document capacity adjusted normally?
		System Notice Registration	Service manager → board management → announcement registration	Is the notice properly registered?
		Real-time monitoring of system load ratio	Run service status check	Is there a notification email when there is a problem with the service status?
		Various log management function	Information Protection Manager → Security → Security Log → Log Settings	Do you log a file that corresponds to the minimum file size at which you want to log?
				Do you record logs that are set to log to the log destination?
				Do you record logs set to log in authentication log?
				Are logs that are older than the log retention period deleted?
Special condition	Other performance	Coping with temporary connection load	Block access of large amount of disk I / O programs such as vaccines	Are programs causing large I / O blocked access to the central disk?

V. 결 론

본 논문에서는 기존 물리적 망 분리와 논리적 망 분리 방식을 발전시키지 않고, 네트워크 파일 시스템을 이용하여 논리적으로 망 분리를 구현하였다. 물리적 망 분리에는 새로운 추가 네트워크 구축과 단말기를 추가 구성하는데 엄청난 예산이 소요되며, 새 단말기에 응용 프로그램을 설치하는데에도 많은 비용이 든다. 기존 논리적 망 분리의 경우에도 로컬과 가상화 망 분리 영역에서 응용 프로그램의 라이선스를 따로 비용 지불을 해야 하기 때문에 많은 예산이 소요된다.

NFS를 이용한 논리적 망 분리에서는 기존 단말기에서 응용프로그램은 그대로 사용하고, 가상화 영역 없이 업무 망 저장공간과 인터넷 사용 저장공간을 분리할 수 있기 때문에 응용 프로그램 사용 측면에서 매우 효율적이다. 사용자 입장에서는 드라이브만 추가 마운트 되기 때문에 큰 환경변화가 없어 매우 친숙하게 적응 할 수 있다. 업무용 디스크 공간 확장 시 물리적 드라이브를 추가하지 않고 관리자에게 연락하여 허용 용량만 권한 설정을 해주면 되기 때문에 확장도 용이하다. 가상화를 쓰지 않는 논리적 망 분리는 상용 S/W추가 라이선스를 구매할 필요가 없으며, 가상화에 따른 PC 리소스를 쓰

지 않기 때문에 쾌적한 단말기 성능을 유지할 수 있다. 사용 공공기관 인사이동시 같은 기관 내 부서 이동의 경우 단말기를 이동하지 않고도 관리자에 의한 업무 폴더 변경만으로 연속성이 이루어질 수 있다. 많은 장점이 있으나, 몇 가지 풀어야 할 문제점이 있다. 같은 상용 S/W를 이용하여 생성하는 업무문서의 저장영역이 틀리기 때문에 상용 S/W 실행 시 최근 문서 검색에서 오류 발생의 경우가 있다. 이는 로컬디스크와 세이프 드라이브 영역이 망 전환에 따라 마운트 유무가 결정되는 근본적인 문제로 업무 적응의 문제이다. 또한, 부서별 VLAN 구성에 따라 장시간 이용 시 연결이 끊어지는 문제가 발생하기도 한다. 본 연구를 적용할 네트워크 환경에서는 VLAN구성이 아닌 단일 네트워크로 구성된 기관에서는 보다 효과적으로 이용할 수 있다. 사용자의 자료공유 문제가 있다. 가장 많은 불편함을 호소하는 부분이므로, 개선의 여지가 있다. 기존 보안 USB를 이용하는 경우 업무 효율성이 저하되므로, 외부 망 자료를 내부 망에서 이용할 수 있는 공유 영역을 지정하고, 이를 보안적으로 관리 할 수 있는 방법에 대한 연구가 추가적으로 필요하며 본 논문의 향후 과제로 한다.

References

[1] T. H. Im, K. S. Park, E. J. Lee, and W. H. Park, "A study on network disconnect technology for information leakage protection", Korean Journal of Industrial Security, Vol. 5, No. 1, pp. 97-109, Feb. 2015.

[2] S. C. Park, I. S. Jang, J. Y. Lee, B. C. Kim, M. S. Lee, D. H. Hyun, and D. W. Chung, "Security association and testbed implementation fo separated business and organizational networks", The Institute of Electronics Engineers of Korea-Telecommunications, Vol. 48, No. 12, pp. 42-53, Dec. 2011.

[3] I. W. Joe and S. S. Lee, "Design and implementation of storage-based data sharing system in the separate network environment", The Journal of the Korean Institute of Communication Science, Vol. 36, No. 5, pp. 477-483, May 2011.

[4] Y. H. Lee and S . J. Yoo, "The Construction of logical, physical network separation by virtualization", Convergence Security Journal, Vol. 14, No. 2, pp. 25-33, Mar. 2014.

[5] M. S. Kim, S. I. Shin, D. H. Lee, and K. N. Kim, "A study on NAS-linked network seperation system using AHP", Convergence Security Journal, Vol. 13, No. 3, pp. 85-90, Jun. 2013.

[6] Curtis, P. W, "Using SANs and NAS", O'Reilly, Cambridge, U.S.A, 2002.

[7] G. A. Gibson and R. V. Meter, "Network attached storage architecture", Communication of the ACM, Vol. 43, No. 11, pp. 37-45, Nov. 2000.

[8] J. E. Jee, S. J. Lee, S. R. Lee, B. C. Bae and Y. T. Shin, "A logical network partition scheme for cyber hacking and terror attacks", Journal of KISS : Information Networkung, Vol. 39, No. 1, pp. 95-101, Feb. 2015.

저자소개

조 성 호 (Sung-Ho Cho)

2001년 2월 : 고려대학교 화학과(이학사)
2012년 2월 : 인천대학교 정보기술대학원(공학석사)
2000년 11월 ~ 현재 : (주)휴먼 이사
관심분야 : SI, NI, Computing 등

최 진 탁 (Jin-Tak Choi)

1977년 2월 : 동국대학교 수학과(공학사)
1982년 8월 : 동국대학교 전자계산학과(공학석사)
1991년 2월 : 경희대학교 전자공학과(공학박사)
2018년 6월 현재 : 인천대학교 컴퓨터공학과 교수
관심분야 : 데이터베이스, 정보보호, 암호학, 전산통계