Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.181

금융회사 망분리 정책의 효과성 연구

조 병 주,† 윤 장 호, 이 경 호‡
고려대학교 정보보호대학원

Study of effectiveness for the network separation policy of financial companies

Byeong-joo Cho,† Jang-ho Yun, Kyeong-ho Lee‡
Korea University, Graduate School of Information Security

요 약

과거 금융권은 고객 및 외부기관과의 연계업무 연속성을 위하여 외부 인터넷망과 내부 업무망을 통합 운영하였다. 그러나 이러한 환경은 악성코드의 유입을 통한 외부 공격 및 정보유출에 대한 위험을 내포하고 있어 금융감독 당국으로부터 보다 근본적인 기술적·관리적 보호대책이 요구되었다. 금융권은 인터넷을 통한 악성코드 감염, 해킹공격 등의 위협으로부터 IT자산을 보호하고, 고객의 개인정보 및 금융거래정보 등 중요정보의 유출을 차단하기 위하여 금융감독당국의 가이드라인에 따라 업무망과 인터넷망을 분리하고, 기존 환경 하에서 정의되었던 보안정책을 망분리 이후 환경에 맞게 재구성하고 있다. 본 연구는 망분리가 적용된 금융회사의 구축사례와 운영현황을 통하여 악성코드 유입 부분에 대한 망분리 정책의 효과를 살펴보고, 모든 경로의 악성코드 유입이 차단되었는지 확인하였다. 연구결과 망분리 이후에도 이동식 저장매체를 통한 악성코드의 감염경로가 완전히 차단되지 않았음을 확인하였다. 이에 따라 망분리 효과를 극대화할 수 있는 이동식 저장매체의 통제 등의 효율적인 보안정책을 제시하고자 한다.

ABSTRACT

Financial industries have operated internal and external network with an unified system for continual business process of customers and other organizations in the past. The financial supervising authority requires more technical and managerial protecting policy to financial industries related to the exposure as danger of external attacks or information leakage. Financial industries performed network separation into internal business and external internet networks for protecting IT assets from malware infection accessing internet or hacking attacks and prohibiting leakage of customers' personal and financial information following financial supervising authority and redefine security policy to fit on network separated-condition. In this study, effectiveness for network separation policy was examined on malware inflow and verified that malware inflow in all routes can be blocked by the policy with analyzing operration data of a financial company, estimating network separation. Result of this study proves that malware infection route by portable storages was not completely blocked even on adapting network-separated condition. As a solution for this, efficient security policy would be suggested in this paper as controlling portable storages for maximizing effectiveness of network separation.

Keywords: Network separation, Network separation policy, effectiveness for Network separation policy

접수일(2014년 11월 14일), 수정일(2014년 12월 15일), 게재확정일(2014년 12월 15일)

† 주저자, bangjour@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

I. 서 론

최근의 금융거래는 인터넷 뱅킹을 비롯한 전자상거래가 활성화 되었으며, 무선인터넷을 이용한 스마트뱅킹 등은 급속히 성장하고 있다. 그러나 최근 금융권을 대상으로 한 사이버 공격은 지속적으로 증가하고 있으며, 특히 특정 목표에 대한 지능형 지속위협(APT, Advanced persistent threat) 공격과 악성코드가 결합된 복합적인 신규 공격 패턴이 증가하고 있다. 일부 금융회사에서 발생한 3.20 금융전산 사고 역시 내부시스템에 접근이 가능한 내부 업무PC, 운영단말기 등이 인터넷을 통하여 악성코드에 감염되어 정보유출 및 자료파괴를 초래하는 해킹 공격의 경로로 이용되었다. 이에 금융위원회는 「금융전산 보안강화 종합대책」을 마련하여 기존의 보안솔루션으로 대응하기 어려운 신규 보안위협을 사전에 차단하기 위하여 전산센터에 대해서는 2014년도말까지 내부 업무망과 외부 인터넷망을 원천적으로 차단하는 물리적 망분리를 의무화하고, 본점 및 영업점에서는 선택적·단계적으로 적용하도록 망분리 구축을 의무화 하였다[1]. 또한 2012년 8월 17일 개정된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(약칭 정보통신망법) 에서는 개인정보의 보호조치로 개인정보의 불법적인 접근을 차단하기 위하여 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷 망을 차단하도록 의무화 하였다[2]. 이는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위한 강력한 보호조치로써, 정보통신 서비스 제공자인 금융회사는 기술적·관리적 조치를 다하기 위하여 의무적으로 망분리를 구축하여야 한다.

금융회사의 망분리 구축을 위해서는 해당 금융회사의 인원, 네트워크 구성, 통신장비 현황, 통신회선 내역 및 대고객 서비스 제공 현황 등의 특성을 고려한 면밀한 현황 분석이 필요하다. 또한 보안성, 성능, 편의성, 도입비용 등을 고려한 금융회사에 적합한 망 분리 방식을 선택하고 망 분리 구축이후의 효과적인 운영을 위한 보안정책 수립이 필요하다.

본 논문에서는 망분리 방식의 장단점을 비교하고 금융회사의 망분리 구축사례와 운영현황을 통하여 망분리 구축 효과를 검증하고, 망분리 이후의 효율적인 정책방안을 제시한다. 논문의 세부구성은 다음과 같다. 2장에서는 망분리의 목적과 망분리 방식의 장단점을 비교하고 3장에서 금융회사의 망분리 구축사례를 분석한다. 4장에서는 망분리 운영 현황을 분석하여 망분리 정책의 효과성을 검증하고, 망분리 이후의 보안정책에 대한 개선방안을 제안한다. 5장에서는 요약 및 향후 연구 방향을 제시한다.

II. 관련연구

2.1 망분리 목적과 적용 대상

최근 발생하고 있는 APT 형태의 공격은 공격자들이 내부 직원들의 PC에 악성코드를 배포한 후, 내부망으로 악성코드를 퍼뜨려 인터넷 망을 통해 해당 PC를 제어하고, 시스템 관리자의 패스워드 및 권한 등을 탈취하는 방법을 이용하고 있다. 3.20 금융전산 사고도 마찬가지로 APT 형태의 사이버 테러였다. 전통적인 보안 솔루션으로는 방화벽, 침입차단시스템(IPS), 유해 사이트 차단 시스템, 안티바이러스 등이 있으나, 이들만으로는 더 이상 고도로 지능화된 APT에 대응할 수 없다.

이에 따라 업무를 수행하는 업무망과 인터넷망을 완전히 분리함으로써 인터넷을 통한 악성코드 전파 및 해킹이 업무 인프라에는 영향을 미치지 않도록 하기 위한 방법이 논의되고 있다.

정보통신망법과 전자금융감독규정은 망분리 대상의 범위와 적용 방식에 있어서 Table 1.과 같은 기준을 제시하고 있다. 정보통신망법 시행령에서는 사업자의 부담을 고려하여 개인정보 유출 위험도가 높은 개인정보취급자의 컴퓨터로 한정하여 대상 사업자가 스스로 망분리 대상이 되는 개인정보 취급자의 수를 줄이도록 하였다. 금융 감독당국은「금융전산 보안강화 종합대책」을 통하여 카드사 정보유출과 과거 해킹사고 등에서 드러난 문제점에 대한 근본적이고 종합적인 재발방지 방안으로 금융회사의 내부통신망과 연결된 내부업무용시스템을 망분리 대상으로 정하고 이행여부에 대한 점검을 강화하였다.

2.2 망 분리 방식

망분리란 업무망과 인터넷망을 분리하여 두 영역이 서로 접근할 수 없도록 차단하는 것으로 전산망을 분리하는 방식은 물리적 망분리와 논리적 망분리로 구분할 수 있다.

2.2.1 물리적 망분리 방식

물리적 망분리 방식은 통신망, 장비 등을 물리적으

Table 1. Comparing standards of network separation policy

divisions	information and communication network law	electronic finance supervision regulations
network seperation relavant business operation	• more than a million users per a day in average whose personal informations were stored and manged in companies' data systems for 3 monthes comparing to the last 3 months in last year • the total sales value is over 10 billion in the previous year in the information and communication province	• financial companies and electronic financial business operators performing electronic financial transactions
subject of application	• personal information managers	• system for business
sphere of application	• personal information downloaders • personal information processors • personal information provisionning supervisors	• internal business systems, connected internal network • information system in personal computing terminal units, connected directly for managing, developing, protecting as purpose.
application method	• network isolation in physically or logically	• the computation centers' networks are obligatory isolated physically • the head quarters and branches are optionally serviced in isolated networks physically

로 이원화하여 인터넷망과 업무망의 접근경로를 차단하고 각 망에 접속하는 PC도 물리적으로 분리한다. 물리적 망분리는 물리적으로 인터넷망과 내부 업무망이 연결되어 있지 않기 때문에 높은 보안성을 갖고 있다. 그러나 물리적 망분리는 별도의 망을 구축해야 하기 때문에 추가적으로 PC, 네트워크 장비 등의 인프라 구축이 필요하므로 도입비용이 많이 들며, PC 2대를 사용함으로써 업무 효율성을 저하시키는 단점을 가지고 있다[1].

2.2.2 논리적 망분리 방식

논리적 망분리는 물리적 망분리의 여러 가지 단점을 보완하기 위한 방법으로 물리적으로 동일한 자원을 가상화 기법으로 분리함으로써 상호간에 접근이 차단되도록 구성하는 방법이다. 논리적 망분리는 기존의 자원을 그대로 사용하고 추가 도입 장비를 최소화하여 도입 비용이 낮고 사용자는 하나의 PC로 업무처리를 할 수 있어 업무 효율성이 높은 장점이 존재한다. 그러나 물리적으로 내부 업무망과 인터넷망이 연결되어 있기 때문에 격리성이 상대적으로 낮아 일정수준의 격리성을 보장하기 위해서는 높은 가상화 기술력이 요구되는 단점이 있으며 가상화 기술의 보안 위협에 대한 검토가 필요하다. 논리적 망분리 방식으로는 가상화 기술을 이용한 서버기반 논리적 망분리 방식 (SBC, Server-Based Computing) 또는 PC기반 논리적 망분리 방식 (CBC, Client-Based Computing)을 이용한다.

서버기반 논리적 망분리는 인터넷망 접근을 위한 서버팜과 업무용 사용자 컴퓨터를 분리하는 방법 또는 업무망 접근을 위한 서버팜과 인터넷 PC를 분리하는 방법을 사용한다[5].

PC 기반 논리적 망분리는 사용자 컴퓨터의 영역을 분리하여 업무 영역의 인터넷 접근을 차단한다. 접속 컴퓨터의 운영체제 및 응용프로그램을 가상화 하여 사용자 컴퓨터에 인터넷에 접속하기 위한 가상화 영역을 구성한다[5].

2.2.3 망분리 구축시 고려사항

이은배는 물리적 망분리만을 통한 내부 정보 유출 및 악성코드 방지는 어려우며, 추가적인 정보 유출 방

지를 위한 솔루션의 도입 또는 보호 방안을 마련해야 하며, 업무 자료의 암호화 및 사용자 인증, 보안 정책 관리에 대한 추가적인 보호 방안이 마련되어야 하고, 물리적 망분리 적용시 업무PC의 관리 소홀에 따른 바이러스 감염이나 이동식 저장장치 등을 통한 유출가능성의 위험과 논리적 망분리시 가상화 기술에 대한 호환성 문제 등에 대한 고려가 필요성을 제시하였다[6]. 망분리 방식에 따른 장단점은 Table 2.에서 기술한 바와 같다.

금융회사는 보안성, 성능, 편의성, 도입비용 등을 고려하여 해당 금융회사에 적합한 망분리 방식을 선택하여야 할 것이다.

2.2.4 망간 자료 이동

업무망과 인터넷망을 분리할 경우 인터넷에서 획득한 정보를 업무망으로 전송하거나 업무자료의 외부 반출 등 분리된 전산망간에 자료이동이 요구되는 경우가 있다. 이 경우 보조저장매체, 망연계 시스템 등을 이용하여 데이터를 전달할 수 있을 것이다. 금융회사는 업무망과 인터넷망간 안전한 자료 전송체계를 구축하고 망분리의 보안성 및 업무 효율성 저하를 막기 위한 관리적 보호조치 등의 보안대책을 수립하고 시행하여야 한다. 사용자 환경에서 개인정보취급자는 데이터 전달 과정의 불편함을 느낄 것이다. 따라서 개인정보취급자는 불편을 해소하기 위해 보안정책에 반하는 행동을 할 수 있으므로, 개인정보관리책임자는 망분리의 보안성 및 업무 효율성 저하를 막기 위한 관리적 보호조치를 취하여야 한다[4].

Table 2. Comparing pros and cons in physical and logical network separation[6]

division	system	pros	cons
physical network separation	using 2 different PCs	• highly secure	• high cost(networks, PCs) • Increase the space and energy consumption • security management is required for additional equipment
	network switching devices used	• highly secure • suitable for limited office space	• high cost(networks, PCs) • declining work effiency(user hostile as reboot)
logical network separation	Internet network separation based on server virtualization	• user control and management policy to be applied in batches • mininization malware infections	• high cost • internet traffic in crease as mass transactions • compatibility of security programs should be reviewed
	biz. network separation based on server virtualization	• centralized management of business data course preventing internal information leakage • user control and management policy to be applied in batch	• high cost • biz. network traffic increase as mass transactions • compatibility of security programs should be reviewed
	internetnetwork separation based on terminalserver	• integrate security managing would be possible for setting security level of terminal servers	• high cost • internet traffic increase as mass transactions • countermeasures to vulnerabilities and malware infections are required
	Internet network separation based on PC virtualization	• user control and management policy to be applied in batches • low cost	• compatibility of security programs should be reviewed • other network equipment are needed

2.3 금융전산 망분리

금융회사의 전산망은 일반적으로 내부 업무를 처리하는 정보처리시스템 영역, 내부 직원 PC 영역, 고객에게 전자금융거래서비스를 제공하거나 내부 직원의 웹 페이지 접근, 이메일 등을 이용할 수 있는 DMZ 영역 등으로 구성되어 있다. 업무망과 인터넷망을 구분하기 위해 백본 스위치, 침입차단시스템 등으로 이용하고 있으나. 대부분 내부 직원이 사용하는 PC는 업무망과 인터넷망에 동시 접속할 있도록 구성되어 있다. 따라서 내부 직원 PC에는 악성코드 감염 등의 외부 침해에 대응하기 위한 백신 프로그램 등이 설치되며 내부 정보 유출 방지를 위해 정보처리시스템 영역으로의 접근통제 정책 설정, USB 등 보조기억장치 제어, 문서 암호화 등의 보안 솔루션이 운영되고 있다. 그러나 이러한 네트워크 구성은 최근 고도화·지능화된 사이버 공격의 증가로 내부 직원 PC가 악성코드에 감염되거나 접근통제 정책의 예외 처리 등으로 인한 금융전산 사고 발생 시 그 피해가 확산될 수 있는 구조적인 위험성을 가지고 있다.

2.3.1 금융전산 보안 위협분석

최근의 금융사고를 살펴보면 내부직원의 PC가 인터넷망과 업무망을 동시에 접속할 수 있는 구조의 금융전산 망에서 악성코드에 감염된 직원의 PC에 의해 서버시스템 파괴 등 금융서비스 장애가 발생하였다[1]. 이에 금융감독당국은 전자금융거래의 보안성 강화 및 해킹 방지를 위해 전자금융거래법, 전자금융감독규정, 금융회사 정보기술(IT)부문 보호업무 모범규준 등의 법·제도를 마련하였다.

금융위원회는 금융전산 망분리 가이드에서 금융회사의 사고사례를 통하여 Table 3.과 같이 보안위협의 유형과 취약점에 관한 현황을 제시하고 있다.

이익준은 전자금융거래에 있어서의 보호대상 및 정보흐름을 Table 4.와 같이 정리하고 이에 따라 Table 5.의 전자금융감독규정에서 지정하는 5대 위협을 기반으로 보호 대상 및 정보 흐름 상에서 발생 가능한 보안위협을 식별하였다[7].

2.3.2 금융전산 망분리 보안정책

「국가기관 망분리 구축 가이드」에서는 망분리에 따른 필수 보안프로그램으로 보조기억매체 관리시스템,

Table 3. current status of threats for banki information system

security threats	vulnerabilities
leaking information	possibly access to internal network from external internet network
IT service paralyzing	possibly outflowing or accessing internet of server managing laptops
IT service obstacles	groupware server or patch managing system as accessible from external internet area.

Table 4. Subject to protect and flow of information[7]

division	details
subject to protect	• confidential information (computing source,documents) PCs, terminals, ATMs applications, web, security device, network, server, DB
flow of information	• accessing to Internal network from external internet • accessing to external internet network to internal network

Table 5. 5major security threats on electronic finance supervision regulations [7]

security threats	details
unauthorized access	connection of unauthorized user without permission
elevation of authority	general users acquired Root authority
outflowing of information	leaking of valuable information such as personal information or confidential information
forgery information	deformation of valuable information such as personal information or confidential information
damaged information	delete or destroy and make information in disuse

네트워크 접근제어(NAC: Network Access Control) 시스템, PC보안 및 PMS(Patch Man-

agement System)의 도입을 제시하고 구성요소와 고려사항에 대하여 기술하였다. 또한 보조적으로 보안 메일시스템 구축과 업무 및 인터넷 프린터 공유에 대한 원칙을 제시하였다. 금융위원회에서 제시한 망분리 보안 가이드라인 기본원칙을 살펴보면 다음의 Table 6.과 같다.

Table 6. Basic principles of banking network system seperation [1]

division	basic principles
pc security management	devide PCs into internal and internet network and managing
using internet mail	private mail accounts should be possibly accessed only in separate external internet network
controlling patch managing system	patch managing system should be operated in separate division from external internet area.
network Access control	unauthorized devices as PCs, laptops etc should be controlled preventing from accessing to internal network
managing auxiliary storages	limied portable storages as USB, CD, portable disks can be permitted to use
data transmission between networks	transfering data from business PCs to internet or real-time business-linked open sever to biz server is possible for operating
managing external devices as printers	external devices as printer should operate in devided into internal and external network

2.4 망분리 동향

국내 금융회사에서 선택하는 망분리 방식을 살펴보면 Fig.1.에서와 같이 물리적 망분리보다는 논리적 망분리 방식을 선호하는 것을 알 수 있다.

이는 금융회사 경우 영업점의 수와 근무 직원수가 많아 물리적 망분리를 적용하기 어렵고, 망분리 도입이 의무사항으로 금융회사의 업무 효율 및 매출에 기여하는 것이 아니기 때문에 상대적으로 저렴하고, 빠른 시간내에 쉽게 이행할 수 있는 방식을 선호하기 때문으로 분석된다[7].

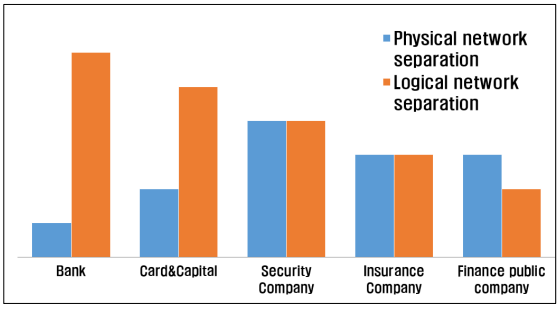

Fig.1. financial companies' decision on physical/ logical network separation

2.5 선행연구와의 차이점

본 논문은 첫째, 기존의 연구에서 다루지 않았던 금융기관의 망분리 구축 및 운영 사례에 관하여 연구를 하였다. 둘째, 망분리가 적용된 경로구간별로 운영현황에 대한 분석을 실시하였고, 셋째, 기존의 망분리 방식 및 구축 기법에 대한 기술적 관점 또는 망분리 이후의 보안위협에 관한 분석 및 대책 제시 등의 정책적 관점의 연구와 달리 망분리의 적용사례의 실증연구를 통한 효과성 관점의 분석과 개선방안을 제시한다는 점에서 차이가 있다.

III. 금융회사의 망분리 구축사례 분석

2.4와 같이 금융권에서 망분리 방식으로 선호하는 CBC방식의 논리적 망분리를 구축한 A금융사의 적용사례를 통하여 금융권의 실제 구현된 망분리 운영사례를 분석하였다.

3.1 A금융사의 망분리 구축사례

A금융사는 국내 최대의 점포수와 임직원을 보유하고 있는 대형 금융회사로 2014년 1월 금융권 최초로 PC기반의 논리적 망분리 시스템을 전사적으로 구축하였다.

A금융사는 망분리 방식을 가상화 기술로 PC영역을 논리적으로 분리하는 PC기반의 논리적 망분리 방식으로 채택하고 10개월간의 구축기간을 통하여 본점 및 영업점에서 사용중인 약 30,000대의 업무용PC에 대하여 망분리 시스템 구축을 완료하였다.

A금융사는 망분리 추진 시 구축범위를 해당 금융사

뿐만 아니라 그룹 계열사를 포함하는 전체 업무용PC로 정하였다. 구축 당시 업무용 PC의 표준 OS 가 기술지원 서비스가 종료되는 이슈로 인하여 표준OS의 업그레이드 전환작업이 진행되고 있는 특수한 상황이었다. 이에 망분리 솔루션을 업무용 PC에 적용하는 이행방식은 망분리 소프트웨어를 추가적으로 배포하여 설치하는 방식이 아닌 OS교체작업과 병행진행하는 PC초기화 방식의 마스터링 설치 방식으로 진행되었다. 이때 클라이언트 PC의 가상화 구현을 위한 PC의 저장공간을 확보하기 위하여 하드디스크 드라이브의 C드라이브의 용량을 40GB이상으로 설정하고 초기화가 진행되었다. 다만 기존 업무데이터의 보관과 관리 효율성을 위하여 하드디스크의 물리적 초기화 방식은 고려하지 않았으며 논리적으로 파티션을 분할하여 기존 데이터를 이동 보관하도록 사전 조치하였다.

3.2 망분리 보안정책 분석

A금융사는 망분리 구축 후 내부 업무 자원을 보호하기 위하여 업무망에서의 인터넷 접속 차단정책을 적용하였다. 이를 위하여 망분리 설치PC는 업무영역에서의 인터넷 망 접속은 차단하고, 인터넷영역에서만 인터넷 사이트가 접속되도록 조치하였으며, 망분리 미설치 PC의 인터넷 사용을 전면 차단하고 블룸버그, 로이타, 특정 공공기관 등의 업무상 예외대상으로 요청된 경우에 한하여 해당 사이트만 제한적으로 허용하였다. 또한 내부업무용 전용기기인 자동화기기, 순번대기기 등의 경우에는 인터넷 접속을 전면 차단하였다. 이에 따른 PC 인터넷 보안정책은 다음 Table 7.과 같다.

3.3 망분리 예외 정책 분석

A금융사는 전산센터의 경우 물리적 망분리 이전까지 논리적 망분리를 한시적으로 적용하였으며, 외주인력의 인터넷 사용을 전면적으로 금지하고 망분리 적용대상에서 제외하였다.

망분리 미적용 PC는 인터넷 사용이 불가하도록 통제하나 업무 목적상 필요한 경우에는 보안부서의 승인하에 특정 인터넷 사이트만 제한적으로 허용하였다. 망분리를 적용하지 않는 경우의 예외PC는 Table 8.의 기준과 같이 망분리 예외대상 기준을 정리하여 관리하고 있다. 예외PC의 허용사례를 살펴보면 망분리 솔루션의 지원이 불가한 문제로 설치 또는 운영이 불가하여 업무연속성을 보장하기 위하여 불가피하게 예외가 적용되는 경우에 해당되었다.

Table 7. Internet security policy of network separated PCs.

division	external internet	internal network
using internet	• permitted access to internet sites with exception(limitation:obscene, gamble, securities, arcade games, web hard) • using webmail, preventing private mails	• open a company online bangking site • limited websites could be accessable after accreditation of security department (ex. Cretop, korea financial telecommunications & clearing institute governmental site etc.)
internal business	• blocking to access internal business system	• authorized to access internal business system
editing files	• file viewer only	• creating and editing files
copy/ paste	• copy and paste of text in documents to internal area	• interdiction copy and paste of text in documents to external internet area
file delivery	• setting a limit on transferring files between two network sections: under 10 files, under 100MB • searching personal information in transferred files from internal to external network	
limit users	• outsourcing staff could access to only internal network in need. (accessible internet with accreditation of security department) • IT professionals are prohibited accessing usual web sites, except internal mailings, online banking service important terminals, treat sensitive informations(DB account or system administrator) are blocked internet access approval is required before transferring files between networks	

Table 8. standard of exception PCs in network separation

division	details
standards for exception cases of network separation	exclusive PC as a connector to specific agencies PC needs editing during connecting web sites PCs using specific programs accessing relevant organization sites
managing exception cases	exceptional PC as a connector could ristrictly accessible to permitted websites and internal network (internet access is allowed at network linkage system)

A금융사의 망분리 보안정책과 예외정책에 따라 클라이언트 기기의 망분리 적용현황을 정리하면 Table 9.와 같다.

Table 9. current status of client PCs' network separation

division	subject	internet use
PCs network separation	• PCs in headquater deputies and branches	• available only at virtual internet network
PCs, unseperated in network	• PCs for outsourcing staff • Important terminals	• blocking internet use
exception PCs in network separation	• exceptional PCs in business (bloomburg, Reuters, particular organizations)	• specific web sites for relevant business (network linkaged)
exclusive machine for internal use	• ATMs, coin exchange machines, etc	• blocking internet access
PCs only for internet use	• PCs for customers in branches • PCs for internet use in headquaters	• allowance based on whitelist • peoridical PC initializa-tion

3.4 망연계 정책 분석

A금융사는 망분리 후 내부영역에서의 인터넷 접근이 차단되었으며 메일의 본문에 외부 이미지 및 동영상 등의 링크가 보이지 않게 되었다. 내부영역에서 접근한 인트라넷 content중 외부 이미지 및 동영상 등의 링크가 보이지 않게 되었고, 내부영역의 프로그램 및 개발환경 등에서 외부로 접속이 필요하거나 외부 라이브러리를 연결하는 경우 연결이 되지 않는다. 하지만 이러한 변화에 따르는 업무상의 문제점을 망연계 시스템을 통하여 연계하여 줌으로서 업무의 연속성을 유지할 수가 있도록 하였다. A금융사에서는 다음의 Table 10.의 체크리스트를 망연계 서비스 정책을 결정하는데 사용하는 판단 기준으로 사용하고 있다.

Table 10. standard of network linkage service policy(check list)

division	object
newly adapted system	• organizing the sysem excluding connection to external network and internet section
previously adapted system	• changing previous system after verifying of disconnect to external internet network
common terms	• necessity of network linkage service • business services • point exact destination IP, port

IV. 금융전산 망분리 효과성 분석

금융회사는 망 분리 구축으로 내부 네트워크망과 외부 네트워크망을 분리함으로써 악성코드 감염과 APT 공격 등 외부 해킹의 위협에 효과적으로 방어할 수 있는 체계를 구축하였다. 많은 비용과 시간의 투자로 구축한 망분리를 통해서 얻고자 하였던 목적과 기대 효과가 달성되었는지를 살펴볼 필요가 있다. 본 절에서는 망분리 도입 후의 잔존 위협에 대해 살펴보고 망분리의 효과성을 검증하려 한다.

4.1 망분리 이후의 보안위협 및 위험요인

A금융사의 구축사례를 분석해 보면 논리적 망분리 대상 PC에서 업무 영역과 인터넷(가상) 영역으로 분

리하였음에도 불구하고 인터넷이외의 외부접점을 통한 악성코드 감염, 정보 유출 및 권한 상승, 망분리 예외 PC를 통한 업무망으로의 불법접속 등의 잔존하는 위협이 여전히 존재하였다. 망분리 효과를 무력화 시킬수 있는 보안위협의 유형을 3가지로 분류하였다.

- 망간 자료전송 시스템을 통한 악성코드의 유입
- 보조저장매체 등 다양한 외부접점을 통한 업무망의 악성코드 감염
- 망분리 정책 예외구간에서의 인터넷접속을 통한 업무망의 악성코드 감염

망간 자료 전송 시 정상적인 망 연계 과정을 거치더라도 감염된 악성 파일이 망 자료전송 시 적용되는 백신 검사 등의 각종 보안 기능들을 우회하도록 견고하게 제작되어질 경우 공격에 취약할 수 있다.

업무 이외의 용도로 사용되는 보조기억장치를 업무망에서 사용할 경우 외부 경로를 통해 감염 및 유입된 악성 파일이 사용자의 부주의 등으로 인하여 인터넷망에서 실행, 복사 될 수 있다. 이러한 부분은 결과적으로 신뢰할 수 없는 경로를 통하여 들어온 파일이나 기타 해킹에 대한 안전성을 보장할 수 없는 파일이 무분별하게 내부망에 유입되는 부분을 차단하기 위한 망분리 개념의 일부를 무력화시킬 수 있으며 이를 통하여 여러 가지 해킹 위협이 발생할 가능성이 존재한다.

대외계, 국제금융 등 업무상의 목적과 망분리 구축 환경의 제약사항을 이유로 망분리 시스템을 경유하지 않도록 예외가 허용되었거나 망분리가 적용되지 않은 사용자의 업무망은 인터넷 직접 접속을 통한 악성코드 감염 및 해킹 공격의 대상이 된다.

A금융사의 경우 망분리 시스템을 구축한 후 망연계 시스템을 적용하여 파일의 망간이동시 통제할 수 있도록 승인절차를 운영중이다. 또한 USB등 이동식저장매체를 통한 문서이동을 금지하고 필요시 반출권한을 승인절차에 따라 부여하도록 통제하고 있다. 이에 따라 정보의 망간이동에 따른 유출방지 대책 및 이동식 저장매체를 통한 반출입 이력이 망분리 이후에만 생성되어 관리되어진 상황으로 망분리 전후를 비교분석이 불가하여 금번 효과성 연구 대상에서는 정보유출에 대한 분석은 제외하였다.

4.1.1 악성코드 감염추이 분석

Fig.2.에서 나타나듯이 A금융사의 악성코드 탐지 건수는 2014년 1월을 기점으로 현저히 감소하여 약 800건 이상이던 탐지건수가 약 200개로 줄어들었다. 신종 악성코드는 백신 프로그램에서 탐지를 못할 수도 있는 점을 감안하더라도 약 70% 이상 악성코드 탐지건수가 감소하였다. 하지만 Fig.2.은 망분리를 적용하였음에도 불구하고 악성코드의 유입을 절대적으로 막을 수 없다는 점도 시사하고 있다.

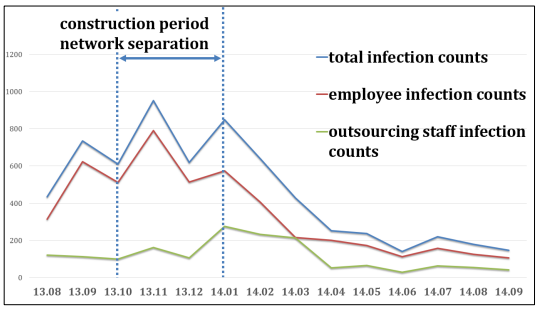

Fig.2. malware infection status changes of the company A

망분리 구축이 완료된 2014년 1월 이후 3개월 정도의 안정화 기간을 감안하더라도 2014년 4월 이후에도 여전히 지속적으로 악성코드가 유입되고 있다. 이는 일정 부분은 망분리가 매우 효과적 일수 있지만 특정한 부분은 망분리의 영향을 크게 받지 않는 것일 수 있음을 나타낸다. 그래프 상에서 특이할 만한 점은 내부직원의 악성코드 감염수는 전체적인 감염추이와 동일한 흐름을 보이는 반면에 외주인력의 감염수는 망분리 이전과 이후가 거의 변동성이 없다는 사실이다. 이는 A금융사의 경우 망분리 이전부터 외주인력에 대해 전면적인 인터넷 차단 정책을 적용하고 있었고, 망분리 이후에도 해당 정책을 유지하여 인터넷 영역을 분리하는 망분리의 영향을 받지 않아 악성코드의 감염율에는 차이를 보이지 않은 것으로 분석된다. 결국 인터넷 차단정책이 적용된 외주인력 업무영역의 감염은 인터넷 접속이 아닌 외부접점을 통한 감염으로 발생되는 부분으로 판단되며, 망분리 구축의 효과가 없거나 존재하더라도 아주 낮다고 볼 수 있다.

4.1.1.1 망간 자료전송을 통한 악성코드 유입 분석

Fig.3.에서 A금융사의 망분리 후 가상 인터넷영역의 악성코드 감염수가 유의할 만한 수준으로 증가되지 않고 낮은 수준으로 유지되고 있음을 알 수 있다.

또한 Table 11.에서와 같이 망연계시스템이 구축 완료된 2014년 4월 이후 매월 일정한 양의 망간 자료 이동이 있었음에도 인터넷영역의 악성코드 감염수가 증가 하지 않았음을 알 수 있다.

이는 A금융사의 망간 자료이동시 보안정책에 기인한다고 볼수 있을 것이다. A금융사는 망간 자료전송시 책임자의 승인절차를 추가하고 이동하는 파일의 개인정보의 보유여부를 검사하여 본부승인을 득하도록 하였으며, 인터넷 영역과 업무망 영역의 접점에서 실행파일에 대한 악성코드 감염여부를 이동전후에 실시하는 등 망간 자료전송시 보안정책을 강화하였다.

또한 인터넷 영역의 악성코드 감염율이 낮은 이유는 망분리 이후에도 인터넷 영역에서 접속가능한 사이트를 제한적으로 허용하는 정책을 적용하였기 때문이다. 따라서 망간 자료이동시 악성코드 유입의 경우에는 망분리 정책에 따른 차단효과를 부정할 만한 위협을 찾을 수 가 없었다.

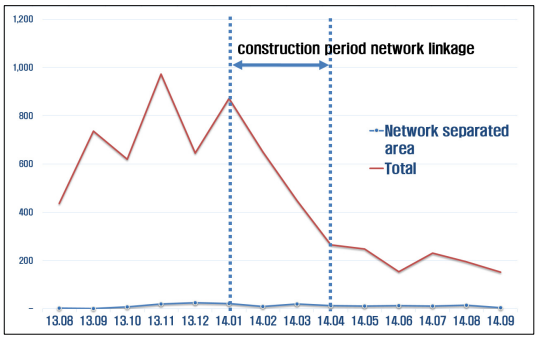

Fig.3. malware infection status changes in external internet network, / Company A

Table 11. status of transferring data between separated networks

year/ month	transferring counts between networks	infection counts in internet area
2014.04	91,000	13
2014.05	75,179	11
2014.06	77,576	13
2014.07	82,657	11
2014.08	71,751	15
2014.09	73,922	4

4.1.1.2 보조기억장치를 통한 악성코드 감염 분석

Fig.4.를 통하여 A금융사의 USB저장매체(이하 USB)를 통한 반출거래수의 추이를 분석해보면 망분리 이후에도 USB의 사용이 증가하였음을 알 수 있다.

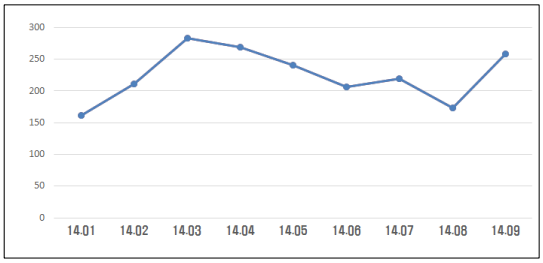

Fig.4. changes of data exporting transaction using USB

A금융사의 보조기억장치를 통한 악성코드의 감염 현황은 Fig.5.과 같다. 추이를 분석하여 보면 망분리 적용기간 동안 USB의 사용량이 증가함에 따라 악성코드 감염이 급속히 증가하였음을 알 수 있었다.

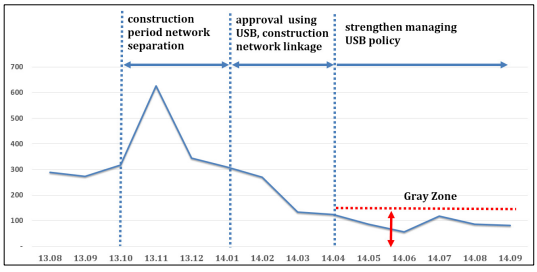

Fig.5. changes of malware infection counts on USB, company A

A금융사는 망분리가 구축됨에 따라 고객정보유출을 방지하기 위하여 2014년 1월 이후 업무용 PC에서의 USB 등 보조기억장치의 사용을 통제하고 필요시 책임자의 승인을 득하여 사용권한을 부여받도록 보안정책을 강화하였다. 그 결과 USB의 사용량의 감소되었고 악성코드의 감염율이 저하되는 효과를 보였다. 또한 2014년 4월 USB관리를 위하여 지정된 USB만 사용하도록 정책이 강화시행되었으나 2014년 4월이후부터는 감소세가 지속되지 못하고 USB의 악성코드 감염율이 일정구간 유지 되고 있다. 이는 망분리 이후에도 USB에 의한 악성코드 감염이 완전히 제거 되지 못하였음을 알수 있다.

USB의 악성코드 감염수의 추이는 A금융사의 전체 악성코드 감염수의 변동추이와 유사한 유형으로 나타나고 있는 바 A금융사가 망분리 이후 제거되지 못한 악성코드의 대부분이 USB를 통한 악성코드 감염수이기 때문이다. 이를 통해 망분리의 효과는 USB의 이용을 제거하지 못하면 낮다는 점을 확인할 수 있다.

Fig.6.은 인터넷을 전면 차단하여 망분리를 적용하지 않는 PC기반의 내부업무 전용기기(이하 내부전용기기)와 외주인력의 보조기억장치를 통한 악성코드 감염현황이다. 외주인력의 경우 망분리 적용기간동안 급격하게 USB감염이 증가하였음을 알 수 있다. 이는 풍선효과가 발생하여 망분리 시 정보이동이 USB사용으로 대체되어 일시적으로 나타나는 현상으로 보인다.

또한 내부전용기기의 경우에는 지속적으로 유지보수 업체에서 사용하는 USB를 통하여 지속적으로 악성코드가 검출되었는 바 2014년 5월이후 내부전용기기의 악성코드 검출시 현업부서에 대한 사유서의 징구 등의 관리활동을 강화하였다. 이에따라 내부전용기기의 감염수가 급격하게 감소하였음이 확인되는바 USB 사용에 대한 관리활동의 중요성과 효과성을 나타낸다고 할 수 있다.

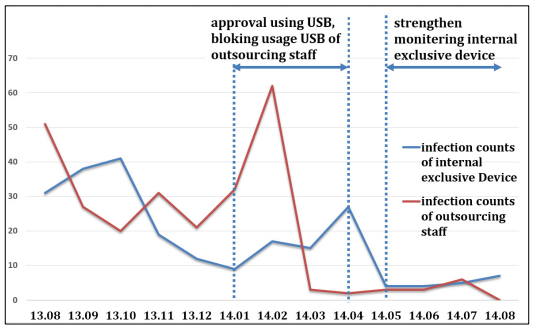

Fig.6. changes of malwere infected counts on devices, unseparated in network

4.1.1.3 인터넷 접속을 통한 악성코드 감염 분석

A금융사는 망분리 이후 망분리시스템을 적용 않는 PC는 인터넷을 차단하도록 하였으나 업무상의 사유로 업무의 연속성을 유지하기 위하여 부득이 하게 망분리를 적용하지 않는 일부 업무용PC의 인터넷접속을 허용하는 예외정책을 적용하고 있다. 이러한 예외의 경우는 해당 업무에서 접속이 필요한 목적지 IP를 특정하여 해당 사이트와 내부망 영역만 접속이 허용된다. 하지만 결국 망분리를 하였음에도 예외정책으로 접속이 가능해진 인터넷 사이트를 통한 알려지지 않은 악성코드 유입에는 자유로울 수 없다. 업무망을 인터넷망과 원천적으로 분리하기 위한 망분리의 기술적 관점에서는 망분리를 하지 않은 것과 같은 동일하므로 망분리 효과를 무력화 시킬 수 있다고 판단된다.

A금융사는 Table 12.에서와 같이 접근이 허용된 인터넷사이트를 통하여 유입되는 파일을 분석하여 바이러스 백신으로 검출되지 않는 신종 악성코드에 대하여 대응하고 있다.

Table 12. state of countermeasures to unknown malwere

year / month	total inflow files	suspicious file analysis	new type of malware
2014. 2	871,184	1,098	40
2014. 3	950,586	857	10
2014. 4	725,135	524	15
2014. 5	567,356	427	26
2014. 6	612,760	228	9
2014. 7	654,489	534	9
2014. 8	571,305	228	2
2014. 9	595,282	280	5

4.2 망분리 효과 분석 변수 설정

본 논문에서는 A금융사의 구축사례를 통하여 망분리 적용에 대한 효과성을 악성코드의 감염율로 확인하기 위하여 악성코드의 감염에 영향을 미치는 변수들을 사례를 통하여 도출하였고, 각 변수들이 감염율에 영향을 주는 정도가 다를 수 있다는 가정하에 분석을 수행하였다. 우선 잔존위협이 어느 부분에 의해서 존재하는지를 알기위해서 여러 가지 변수를 추출하여 상관계수를 도출하였다. 1차적으로 망분리 이후에 데이터가 크게 변동된 변수들을 1차 의심경로로 선별하였다. 그 중 망분리와 관련 없는 독립적인 변수들을 추출하여 과연 어떠한 관계가 있는지 분석해 보았다.

4.2.1 자료의 수집 및 분석방법

연구를 위한 자료는 A금융사의 최근 1년 동안의 사용자PC와 자동화기기의 악성코드 감염현황과 USB 저장매체의 사용량 측정을 위한 USB 사용권한승인 건수를 확인하였다. 이를 확인해보니 실제로 망분리가

실시된 2014년부터 약 USB의 사용권한승인이 10 ~ 40 배 이상 증가 된 것으로 확인되었다. 이는 망분리의 실시로 악성코드의 유입이 인터넷이 아닌 USB를 통해서 유입되는 것으로 예상된다. 하지만 정상적인 USB사용 승인건과 악성코드의 유입경로로 활용된 USB사용을 구분하기 위하여 Table 13.의 USB 반출현황을 수집하였다. USB반출현황 건수와 악성코드 탐지건수 데이터의 상관도 분석 및 산점도는 SPSS 21(Statistical Packages for Social System)을 사용하였으며 상관 분석시 적용된 상관계수는 Pearson 상관계수이다.

Table 13. permission counts of authority on using USB

year/ month	permission counts
2013.10	13
2013.11	53
2013.12	202
2014. 1	2,504
2014. 2	5,288
2014. 3	3,480
2014. 4	3,369
2014. 5	2,780
2014. 6	2,058

4.2.2 상관분석

다음 Table 14.는 의심경로중 하나인 USB의 분석 현황이다.

Table 14. detected malware counts on USB

year/ month	malware detected counts in total	malware detected counts on USB	rate
2013.10	611	317	51%
2013.11	953	626	65%
2013.12	620	344	55%
network seperation			
2014. 1	850	310	36%
2014. 2	640	270	42%
2014. 3	428	134	31%
2014. 4	252	125	50%
2014. 5	237	86	36%
2014. 6	140	57	40%

USB의 경우 전체 악성코드 탐지건수가 줄어들면서 USB에 의한 탐지 건수도 줄어들었지만 여전히 전체 탐지 건수의 약 40%가 USB로 인한 감염으로 꽤 많은 비중을 차지하였다. 망분리를 실시하였는데도 불구하고 보조기억장치로 인하여 꾸준히 악성코드가 탐지되는 원인을 파악하기 위해 USB사용승인 및 반출건수에 대해여 전체 악성코드 탐지건수에 대비하여 상관계수를 도출해 보았다. 도출된 Table 15.에 의하면 2014년 1월 망분리가 적용된 시점을 기점으로 급격히 USB의 반출건수가 증가됨을 확인 할 수 있다. 상관계수 또한 음의 상관계수로 -0.653 이라는 매우 큰 음의 상관계수를 가지고 있다.

Table 15. exporting data on USB correlation analysis

year/ month	total malware detected counts	exporting counts of USB
2013.10	611	11
2013.11	953	8
2013.12	620	15
2014. 1	850	161
2014. 2	640	211
2014. 3	428	283
2014. 4	252	269
2014. 5	237	241
2014. 6	140	206
correlation coefficient	-	-0.653

Fig.7.의 경로별 악성 코드 탐지 현황을 살펴보면 망분리 이후에도 가장 많은 탐지 경로를 보이고 있는 것은 보조기억장치임을 알 수 있다.

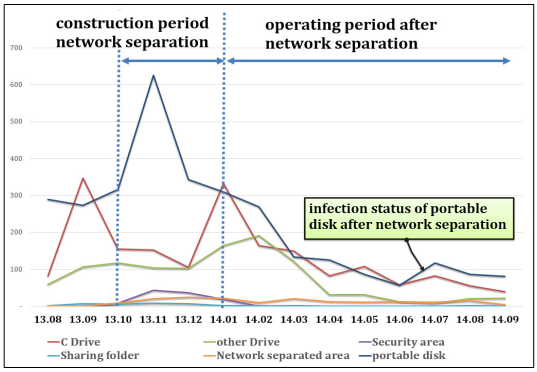

Fig.7. chages of malware infection on path by type, company A

이는 망분리 이후에 원활한 인터넷을 사용 할 수 없는 PC관리자가 외부 인터넷에서 받은 파일을 보조기억장치에 저장하여 업무에 사용함으로써, 결국 사용자의 관리적 소홀로 인하여 유입된 경로로 볼 수 있다.

4.2.3 망분리 이후 잔존위협별 대응방안

4.1.1 에서도 확인했듯이 보안 침해 사고유형에 대한 근본적인 처방이 망분리 만이라고는 생각할 수 없다. 웜바이러스 감염과 경유지 악용에 대한 대응은 물리적으로 망을 분리하더라도 파일이동에 따른 감염이 발생할 수 있기 때문에 PC내 백신이나 보안 툴과 같은 소프트웨어적인 보안과 함께 접근하는 것이 근본적인 해결책이라 할 수 있다. 본 논문에서는 Table 16.과 같이 USB뿐만 아니라 다양한 잔존위협들을 파악하였고 망분리 이후에 존재하는 잔존위험에 대한 대응방안 또한 제시한다.

홈페이지 변조 침해 사고의 경우는 금융회사 내 임직원이 사용하는 내부 웹사이트를 변조하는 것이 아니라 고객서비스를 대상으로 공격하는 것이기 때문에 금융회사의 PC활용을 위한 망분리 에서는 효과가 없다. 자료훼손 및 유출 사고와 관련하여 PC내 트로이 목마와 같은 도구가 PC내 파일을 인터넷을 경유하여 외부로 전송하는 유형이 있을 수 있으나 이는 망분리만을 통해서 막을 수 있는 것은 아니다.

망분리 정책으로 대응할 수 없는 감염경로에 중점을 두고 보안정책을 수립한다면 이는 망분리를 더욱 효과적으로 활용 할 수 있는 정책의 기반이 될 것으로 보인다. 또한 망분리 이후의 잔존위협에 적절하게 대응하기 위해서는 현재 의 외부 인터넷망에 집중된 관제중심의 대응환경에서 내부망 중심으로 망분리 보안정책의 변화가 필요하다.

V. 결론 및 향후 연구방향

5.1 연구 결론 및 의의

본 연구는 망분리 구축이 외부의 불법적인 접근을 통한 악성코드 유입을 차단하여 내부정보의 유출을 차단하고자 하는 기본목적의 관점에서 유의한지의 효과성 분석에 중점을 두었다.

금융권의 망분리 방식으로 가장 많이 구축되는 PC기반의 논리적 망분리 환경을 살펴보았으며 분리된 망간 자료의 공유를 망연계 구축 환경을 고려하였다. 또한 망분리와 망연계의 적용에 있어 고려해야할 기본적인 원칙과 보안요건을 살펴보고 망분리 구축이후의 남아있는 보안위협에 대한 분석을 통하여 보안정책의 개선방향도 제시하였다

망분리 이후 적용된 보안정책에 대한 효과성을 운영현황을 통해 분석한 결과 망분리 효과를 무력화 시킬 수 있는 보안 위협에 대한 3가지의 분석결과를 도출하였다.

첫째, 망연계 등 망간 자료전송을 통한 악성코드의 유입차단에 있어서 일반적으로 구축의 효과가 있음을 확인하였다. 다만, 사용자에 대한 전면적인 인터넷 차단 정책을 운영하는 경우에는 망분리의 효과가 유의하지 않았다.

둘째, 망분리가 적용된 PC의 경우 인터넷 접속을 통한 악성코드 감염 방지 효과가 있음을 확인하였다. 다만, 업무상의 필요로 망분리 정책을 예외적용하는 PC가 존재할 경우 시스템 전체적인 관점에서 망분리 효과가 무력화 될 가능성이 존재하였다.

셋째, 이동식저장매체 등의 외부접점을 통한 업무망의 악성코드 감염이 망분리 이후에도 완전히 제거되지 못하였음을 확인하였다. 이는 이동식 저장매체에 대한 대책은 망분리 적용만으로는 효과를 기대할 수 없음을 나타낸다. 이는 망분리 구축효과를 얻기 위해서는 이동식 저장매체 사용에 대한 지속적인 통제 및 관리활동이 필수적인 보안정책 요건임을 입증해 주고 있다.

연구결과 금융회사의 전산망 환경에서 망분리가 인터넷 등 외부로부터의 보안위협에 대한 대응방법으로 매우 강력한 대책이고 효과가 큰 것만은 분명하다. 그러나 원천적인 보안 전략이라고 기대했던 망분리 또한 그리 안전하지는 못했다. 망을 분리하였다고 해서 외부로부터의 모든 보안위협을 완전하게 예방할 수 없다는 것이 실제 적용사례로부터 확인되었다.

망분리 구축으로 금융회사들은 외부의 공격위협에 대한 기술적인 환경과 보안정책을 보유하게 되었지만 제대로 된 관리적 보안대책 없이 운영된다면 그 효과를 보장할 수 없게 된다. 결국에는 망분리 대상을 줄이기 위하여 개인정보취급자에게 불필요하게 부여된 접근권한을 회수하는 등의 조치를 통하여 근본적인 위험을 줄이기 위한 노력을 기울여야 할 것이다. 본 논문은 이론적으로 제시되었던 망분리 보안정책과 각종 보안위협에 대한 이슈들이 실제 구축 사례를 통하여 확인되었고 보다 구체화 되었다는 점에서 의의를 둘 수 있을 것이다.

Table 16. countermeasures by remaining threats after network separation

inflow path	subject	threats	weak points	countermeasures
WEB	headquarters, branches	inflow of malware in internal area, transffering data between networks	Unknown malware	〔basic actions〕 IPS,vaccine, detecting system for zombiePC, APT response system 〔additional actions〕 import malware total inspection system to the connected points to internal network
	PCs and devices in branches (minwon24, other 53 websites, 21 IPs)	threats of download malware from polluted network linkage sites to internal area		
	exceptional users (partial headquarter department, overseas branches)	malware inflow by accessing websites		
WEB mail	headquarters, branches	malware inflow by accessing websites		
	exceptional users (partial headquarter department, overseas branches)	malware inflow from attachments to emails		
USB CD-ROM	all users	malware inflow from authorized users	Unknown malware	〔basic action〕 Data loss prevention, vaccine 〔additional actions〕 import malware total inspection system to the connected points to internal network
wireless LAN (WI-FI)	headquarters, branches	connecting up internal to external networks with wireless devices	using wireless LAN devices, uninstalling NAC	〔basic actions〕 W-IPS,NAC 〔additional actions〕 managerial control

5.2 연구의 한계 및 향후 연구 방향

망분리의 구축사례와 관련된 국내 및 해외의 연구가 아직 활발하지 못하여 관련한 연구가 부족하여 사례 비교하여 분석하지는 못하였다.

향후 망분리의 구축효과에 대한 다양한 효과성 분석과 새로운 기법을 적용한 연구사례가 발표되어 본 논문의 연구결과에 대한 비교연구가 이루어지기를 기대한다.

또한 향후 연구에서는 의무적으로 물리적 망분리 방식으로 구축될 금융권의 전산센터의 운영사례에 대한 분석을 통하여 논리적 망분리 방식으로 적용된 본점 및 영업점의 운영사례와 비교 분석하여 망분리 방식별 효과성과 개선방안에 대한 연구가 이루어 질 수 있을 것이다. 아울러 2007년부터 망분리를 적용해온 국가기관 및 공공기관과 금융권의 물리적 망분리와 논리적 망분리의 구축사례 비교를 통한 망분리 정책을 분석하는 연구가 진행 될 필요가 있을 것이다.

References

〔1〕 Financial services commission, “guidelines for separating financial network system,“ Sep.2013

〔2〕 Korea communication commission, “regulations for promoting information communication network and information security,” pp.5-6, Aug.2014

〔3〕 Korea communication commission, “tandards on technical and managing protective action for personal information,” pp. 1-4, Aug.2012

〔4〕 Korea communication commission, "Manuals of standards on technical and managing protective action for personal information," pp. 48-49, Sep.2012
〔5〕 KISA, "guidelines for blocking external internet network", Feb.2013
〔6〕 Lee, Eun Bae, Kim, Yeong Ki, "Study of information security in network seperated enviroment," pp.6-8, Feb.2010
〔7〕 Lee, Ig Jun, "A Study on the Security Policy for Logical Separation of the Banking Network System," pp. 6-8 Dec.2013
〔8〕 Digital Daily, "similar rates of financial companies decision of network separation with logical or physical," http://www.ddaily.co.kr/news/article.html?no=108084, Aug.2013
〔9〕 Ministery of security and public administration, "Guidelines for setting network separation of govermental organzations," May.2008
〔10〕 Ji,JeongEun, "Logical network separation against cyber hecking or terror attacks," The Korean Institute of Infomation Scientists and Engineers, Feb.2012
〔11〕 Financial security agency, "guidelines for separating financial network system"
〔12〕 Joosam Lee, "A Study on Designating the Solution for Deployment of an Efficient Partitioned Network," Dankook University, Jun.2013

〈저자소개〉

조 병 주 (Byoeng Joo Cho) 정회원
1999년 2월: 단국대학교 전산통계학과 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 위험관리, 정보보호관리체계, 보안아키텍쳐

윤 장 호 (Jang Ho Yun) 정회원
2012년 8월: 고려대학교 정보수학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융보안, 위험관리, 정보보호컨설팅

이 경 호 (Kyung Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험관리. 정보보호컨설팅. 정보보호 및 개인정보보호정책