바이러스 차단 인프라 구조에 관한 연구

노시춘* · 김수희** · 김귀남***

요 약

virus 방역 체계 관리는 network infra 구조관리, traffic 소통경로관리, 방역 zone 설정, gateway구간 방역관리이다. 본 논문은 일반적인 방역체계 구조의 성격과 취약점을 진단하고 이를 개선할 수 있는 대책으로서 개선된 방역체계를 설계하였다. 또한 설계된 방역체계와 configuration, mechanism하에서는 어느 정도의 개선효과 나타나고 있는지 분석하였다. 개선된 다단계 방역체계 하에서는 gateway 단계에서 불필요한 mail을 걸러줌으로서 server에 주는 부하는 감소하며 virus wall상의 CPU 부하의 감소와 virus 치료율의 상승으로 송신 적체 건수는 감소하고 시스템 process수는 증대하고 있다.

A study on an Infrastructure for Virus Protection

Si-Choon Noh* · Su-hee Kim** · Kuinam J. Kim***

ABSTRACT

Virus protection infrastructure managementis network infrastructure management, traffic route management, virus protection zone expansion, and virus protection management for gateway area. This research paper provides a diagnosis of characteristics and weaknesses of the structure of existing virus protection infrastructure, and recommends an improved multi-level virus protection infrastructure as a measure for correcting these weaknesses. Improved virus protection infrastructure filters unnecessary mail at the gateway stage to reduce the load on server. As a result, numberof transmission accumulation decreases due to the reduction in the CPU load on the Virus wall and increase in virus treatment rate.

Key words : Virus Protection Infrastructure

* 남서울대학교

** 호서대학교 컴퓨터공학부 컴퓨터공학전공

*** 경기대학교 정보보호기술공학과

1. 서 론

오늘날 computer virus는 기술적으로 더욱 지능화되고 있고 파괴력 또한 더욱 강화되는 추세이며, 형태적으로는virus와 worm의 다양한 조합형으로 진화하고 있다. 날로 강력해지는 computer virus는 고속화, global화한 초고속 network 인프라를 타고 순식간에 확산되므로서 파괴력과 위험성은 가공할 수준에 이르고 있다.

virus 침투시의 일반적인 대처는 먼저 신종 virus 대응 vaccine을 개발하여 viruswall상에 장착된 engine을 update하는 것이다. 이 방법이 기술적으로서는 유일한 대처방안 이지만 이 방법은 사실 문제를 원천적으로 해결하는 방식은 아니다. 그보다는 virus를 근본적으로 차단할 수 있는 기술이 개발되어 virus 위협을 항구적으로 제거하는 것이 인류의 큰 염원중의 하나이다.

그러나 유감스럽게도 가까운 장래에 이 같은 염원이 실현되기는 불가능 해 보인다. 지금 virus 오염현장에서는 확산된 virus를 서버와 pc 단위에서 수동적으로 삭제를 계속하여 감염숫자를 점차 줄여나가는 방법으로 방역에 임하고 있다.

이 같은 방법들은 기술적 대처가 아니라 방역체계와 관리를 통한 해결방식이다. 본 연구는 오늘날의 방역체계환경에서의 방역인프라구성에 관한 것이다. 즉 virus 공격패턴에 대응할 수 있는 방역인프라는 어떤 구조로 구성되어야 하는가에 대한 대안을 제시하기 위한 것이다.

이를 위해 널리 사용되고 있는 일반적인 방역체계 구조의 성격과 취약점을 진단하고 이를 개선할 수 있는 대책으로서 개선된 방역체계를 설계하였다. 또한 설계된 방역체계와 configuration, mechanism하에서는 어느 정도의 개선효과 나타나고 있는지를 분석하였다. 제안된 방역전술 기본사항은 변화된 공격패턴에는 변화된 방어전술체계가 필요하다는 것이다.

오늘날의 virus 방역전술핵심은 침투 virus의 기술적 다양성과 침투패턴의 가변성에 대응하여 방역체계 또한 가변적이고 유연성을 확보한 다단계 방역체계로의 전환이 첫번째의 관건이 되어야 함을 이 연구를 통해 설명하고자 한다.

2. 관련 연구

2.1 Infection Mechanism

2.1.1 침투대상자원

virus방역체계 구축 시 감염경로 파악은 무엇보다도 우선되어야 할 첫 번째 과제이다. 알려진대로 virus는 감염 이후 실행 될 경우에만 피해를 유발시키기 때문에 virus 침투가능성이 있는 취약점을 먼저 파악해야 한다.

• Users Computer

desktop의 local drivers가 모든 종류의virus공격에 취약하다. virus 감염은 floppy drive, email, 인터넷 downloads, 여러 종류의 macro-enabled application 등을 통해 local drive로 침투한다. 그뿐만 아니라 file server, HTTP based web traffic, FTP based file 전송, CD-ROOMS, synchronised PDA data등이 이곳으로 수신된다.

• Local File Server

File server의 종류는 application, file print server등으로 분류되는데 다양한 types의 viruses의 저장과 증식장소로서 악용되기가 매우 쉽고 약간의 침투기술만으로도 다양한 virus type의 숙주로서 악용될 소지가 많다. 대부분 file과 print server는 필요 시 desktop을 통해 사용자가 접속해오는 files을 단지 보관만 하고 있을 뿐이다. 그런데 바로 이 자원들이 virus code에게는 저장과 증식에 적합한 무대를 제공하게 되는 것이다.

• Email SMTP 서버

email server는 네트워크 gateway에 배치되어

내부 시스템으로 유입,유출되는 email traffic을 처리한다. Email Server는 SMTP, Lotus Notes/Domino, Microsoft Exchange 같은 protocol지원을 받는다. Email traffic은 내부 system으로의 최대의 virus 침투경로로 알려지고 있다. 일단 감염된 email document가 SMTP email gateway를 통과하면 전 조직의 desktop에 감염이 발생한다.

• Email 수신서버

email 수신서버는 email header의 "to:"에 기록된 수신자 주소 정보를 검색한 후 mail의 내용을 mail box에 저장하는 역할을 하는 server이다. SMTP gateway를 통과한 data 뿐만 아니라 internet 내부 유통경로를 통해 mail box에 수신된 정보는 오염될 수 있는 위험성이 매우 높은 취약한 곳이다. mail box에 이미 저장되어 있는 letter들은 scanning 기법이 적용되기가 어렵고 사용자에 의해 file forward, open, reply, use등 어떤 경우의 사용에도 감염된다.

2.1.2 Virus 활동개시 요인

각종 *infection* 경로로 *target system*내에 침투에 성공한 악성 code는 사용자의 실행과 동시에 활동을 개시한다. 잠복한 virus를 잠에서 깨워 행동에 나서도록 하는 활성화 요인은 가장 전통적인 방식인 오염된 저장매체와 프로그램의 사용에서부터 감염된 email, 오염된 공유파일사용, 오염된 WEB Server 사용 등으로 점차 다원화 되고 있다.

• 저장매체 사용시

제작 시 virus에 오염된 각종 CD_ROM, Diskette을 computer에 장착하고 실행 시에 잠복한 virus는 활동을 개시한다.

• Application 프로그램 사용시

불법 제작된 프로그램을 read할 경우 프로그램의 일부 embeded 된 virus module, 또는 routine에 의해 활동이 개시된다.

• Email사용시

email에 첨부된 readme.exe 를 실행 시 감염된다.

outlook Express의 경우 보안 patch를 안 했을 경우에는 '미리보기'를 click 하는 것 만으로도 감염된다.

• 공유 file 사용시

read/write 권한이 공유된 시스템 file이 오염될 경우 실행 시 감염을 일으킨다.

• WEB사용시

IIS취약점을 이용하여 오염된 web server를 patch하지 않을 경우 IIS web server 사용시 감염된다. 감염된 web server의 'HTML', 'HTM', 'ASP' file 실행 시 감염된다.

2.2 Protection Mechanism

2.2.1 Anti-virus software

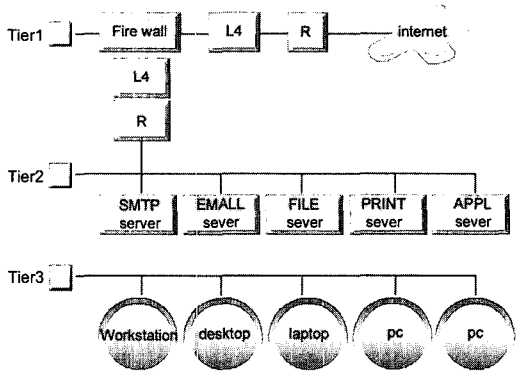
방어 mechanism은 anti-virus technologies, protection infrastructure, management등 3개의 분야로 나누어진다. virus 진단과 삭제에 사용되는 software인 scanner는 사용자가 직접 가동하거나 또는 on. access 방식으로 run하여 scanning을 수행한다. 오늘날의 scanner는 DOS.exe - FILE, Windows NW/PE files등 여러 종류의 실행 file, Mime-encoded file format등의 분석이 가능하다. 스캐닝툴은 file이 drive에 기록될 때 virus감염여부를 사전 check한다. 이 기법은 방역조치를 아직 수행하지 않은 사용자들이 desktop의 home directory에 위험한 file을 저장하지 않도록 해준다. 또 하나의 방법은 file이 server로부터 읽혀올 때의 virus 스캐닝이다. 이 방법은 미 방역된 사용자들이 감염되지 않도록 해주는 중복 방역장치이기도 한다.

2.2.2 Viruswall

viruswall은 원래 anti-virus software를 의미하는 것으로서 시스템에 유입 되는 emails 과 첨부물을 scan한다. 원래 의미에 불구하고 오늘날에는 virus 차단을 목적으로 배치된 software 또는 software와 hardware 말한다. 즉, software만으로 network gateway 장비에 장착되거나 또는 전용 server 상에 software를 탑재하는 방식이다. Viruswall은 내부에서 외부로 또는 외부에서 내부로 통과하는 traffic을 검색하여 virus 가 첨부된 packet 여부를 진단하고, 만약 virus가 발견되면 치료 후 통과 또는 drop 시킨다. Anti-virus product 제조사들은 gateway 장비의 software에 virus 차단기능 module을 삽입하거나 또는 기존의 virus scanner 제품을 설치하여 virus wall을 구성한다. Gateway software에 삽입되는 anti-virus software와 scanner의 차이점은 전자는 통과하는 traffic을 packet 단위로 filtering 하면서 진단과 치료, drop을 수행하는 방식이고, 후자의 경우는 filtering이 아닌 packet sniffering 방식의 traffic monitoring 기법이 주로 사용된다.

2.2.3 Protection Infrastructure

방역인프라는 network gateway 구간, server 구간, client 구간으로 3단계로 계층화 되어 있다. Network intranet이나 LAN 규모에 따라서 외부네트워크와 exit point에 virus wall을 설치한다. Intranet 구조가 본사-지사-지점으로 계층화되고 내부 pc 자원이 통상 500대 이상 규모일 경우 virus wall을 배치하는데 배치방식은 fire wall에 내장시키거나 또는 viruswall 전용서버를 두는 방법이다. Gateway 구간에 virus wall을 설치하는 이유는 관문 1개소에서 내부 network 전체자원에 대한 통제가 가능하고 firewall의 packet filtering 기능과의 combination을 통해 강력한 차단기능이 가능하기 때문이다. network 규모가 소규모 일 경우는 PC 단위로 방역을 실시한다.



(그림 1) 일반구조 Protection infrastructure

2.2.4 방역절차

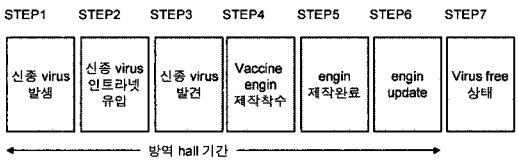
virus에 대한 대응절차는 우선 보고된 virus를 file system을 통해 signature를 추출한 뒤 이를 분석하여 대응 vaccine engine을 개발, 오염system의 virus wall engine을 update한다. Virus wall에서는 통과 traffic에 대한 packet 단위 scanning을 실시하여 virus에 감염된 packet의 virus를 치료하거나 또는 drop 한다. 만약 gateway에 virus wall을 확보하지 않은 소규모 네트워크 시스템일 경우에는 개별 pc 단위로 vaccine을 download하여 engine을 update 한다. 지금 일반적인 virus 방역방식은 1차 방역망인 virus wall을 통과한 virus를 서버나 pc 자원에서 제거작업으로 2차 방역을 실시하여 감염된 IT 자원숫자를 점차 줄여나가는 것이다. 사실, 이 방식은 기술적인 대처라기보다는 방역체계와 management를 통해 문제를 해결하는 방식이다. 따라서 virus 방역 시 1차 방역망이 뚫린 이후의 2차 방역 의존도는 날로 더 높아지고 있고 인트라넷의 경우 내부에 침투한 virus 소멸 때까지 1

차, 2차, 다단계 방역의 중요성은 거의 유일한 해법이 되고 있다.

2.3 방역누락요인

오늘날 적용하고 있는 protection infrastructure에서는 다음과 같은 방역누락요인이 존재한다.

- A형 : vaccine engine 개발 기간 중 감염확산. virus발생시, vaccine engine 개발 착수 후 개발완료, 장착시간까지 신종 virus는 이미 무력화된 네트워크 방어망을 통과하여 인트라넷의 각종 감염대상자원에 침투한다. 적어도 이 개발 기간 중은 아무런 방어장치가 없는 무방비 상태이다.



(그림 2) virus 방역누수 발생 과정도

- B형 : gateway 구간에서의 트래픽 처리 누락.네트워크상의 gateway에서 packet filtering 과정의 virus 치료 및 차단 시 traffic 처리 매커니즘상 시스템 별로 차이가 있지만 기능과 성능별로 일정량의 처리누락이 발행한다. 이는 Giga bits 속도로 통과하는 packets에 대해 sniffering 방식의 packet inspection은 처리지연과 data loss가 일정부분 발생하기 때문이다.
- C형 : gateway 구간에서의 web traffic 감염.gteway에서의 virus검색은 통상 SMPT 프로토콜을 사용하는 email packet 을 대상으로 함. 그 이유는 전통적으로 email virus 통한 침투가 virus의 초기부터 pattern 이었으므로 기술개발이 집중되었고 email 이외의 모든 service에 대한 검색과 치료는 network performance상 성능저하를 야기할 수 있기 때문이다. 그러나 HTTP traffic이 월등하게 증대되고 있는 현재의 환경에서 web 감염은 해결해야 할 최대의 현안이다.
- D형 : 인트라넷 내부에서의 저장 매체를 통한 감염인트라넷 내부시스템에서의 오염된 CD, floppy disk를 통한 감염은 gateway 구간방역과 전혀 무관하게 발생된다. 이 경우 감염숙주는 물론 server 또는 pc이다. 이 매체를 통한 감염은 또한 일단 감염 후 worm virus의 경우 내부번식, 복제를 반복 함으로서 gateway상의 방역 mechanism을 위주로 하고 있는 일반적 방역체계에서 가장 큰 취약점으로 대두 되고있다.
- E형 : 인트라넷 내부전파와 확산 'A'~'D'형 유형요인으로 인트라넷 내부로 침투한 virus는 내부감염, 복제, 확산을 계속한다. 확산된 worm virus는 내부간 유통감염을 계속하는 한편 outbound traffic을 급증 시킴으로 gateway상 session을 증가시키고 gateway를 무력화 시킴으로 네트워크 전체를 마비시킬 수 있다.

2.4 방어 mechanism상의 문제점

첫째, server, PC로 분리된 2원화 방역방식은 방역 zone을 server, pc로 제한 시키므로서 network상 유통되는 virus에 대한 차단기능이 없다. 무엇보다도 1차 방어망을 통과했거나 내부감염으로 server, pc에 잠복한 virus의 인트라넷 내부 확산 시 현재와 같은 server, pc를 대상으로 하는 수동적인 삭제방식 방역체계로는 근본적 해결이 어렵다.

둘째, Network traffic은 TCP/IP 서비스 별로

특성이 상이하고, 침투 pattern 이상이 하나 vaccine에 의한 획일화 된 단일방식 치료는 다양한 침투에 효과적 차단이 되지 못한다.

셋째, 기존의 방역체계는 전통적으로 email virus 방역대책에 초점을 맞춤으로서 email 이외의 타 virus 경로에 대한 효과를 발휘하지 못한다.

- Web 감염
- File 공유감염
- CD-ROM, Diskette 등 내부 매체감염
  불법제작 프로그램 감염

넷째, 기존의 client 방역은 troyan horse등 최근 기승을 부리는 악성 code 감염여부를 진단하고 치료 하는데는 효과를 나타내지만, 인터넷에 접속한 상태에서 공격용 packet이 유입되거나 hacking 기술을 동반한 형태로 접속해오는 virus 움직임에 대한 감시기능이 없어 불안한 상태이다.

다섯째, 방역 infra 관리측면에서 필요시마다 solution 도입, 설치로 대응하고 있으나 종합적인 infra 관리가 이루어지지 못한다. 각종 server, pc, application과 network은 유기적으로 연결되어있다. 따라서 각 application에 대한 개별적인 방역으로는 점차 지능화 하는 virus를 막기란 쉽지않다.

3. 개선체계

3.1 설계방향

변화하는 virus 공격 pattern에는 변화된 방역 전술이 적용되어야 한다. 이를 위해 infrastructure를 새로운 요구에 부응할 수 있도록 수정하고, infra와 technology를 효율적으로 combine한다. 그 내용은 infra 구조단계 재 설정, 감염경로별 차별화방역, scanning tool의 효율적 배치를 통한 real-time 방역체계 구성 등으로 요약된다. 개선된 체계에서는 network infra 구조. traffic소통경로 방역 zone, gateway 구간 방역방법, server 방역방법, anti-virus software 구성 등에서 개선방식을 적용한다.

3.2 제안구조 내용

3.2.1 protection infrastructure 재구성

exit point에서부터 firewall 구간, server 구간, client 구간으로 3단계로 계층화된 구조에 web traffic, email traffic filtering을 위한 gateway구간과 내부네크워크 virus wall 구간을 추가하여 5단계의 방어층을 구성한다. Gateway 방역구간을 추가하는 이유는 Web traffic이 급증하는 과정에서 virus 유입 또한 크게 증가함으로서 일반적인 수준의 방역으로는 소기의 차단효과를 얻을 수 없기 때문이며 SMPT gateway 또한 다량 email 유입의 대표적 통로로서 방역 gateway구간으로 재설정하여 network 진입 전에 차단할 필요가 있다. 내부 네트워크 virus wall은 일단 침투된 virus의 내부유통을 차단하는 기능으로 새로운 방역층을 설정한다.

3.2.2 Traffic 소통경로 재설정

Network Traffic을 경로에 따라 채널종류별로 2개 채널로 구분하고 그에 따라 protection infra 구조를 단계화 한다. 구분되는 traffic 경로는 내부 internet 구간과 DMZ 구간이다. 먼저 내부 internet 구간은 외부 접속점에서 최종 사용자까지이며 Exterior Router → Web switch → Firewall → Web switch → Interior Router → Servers → Client 이다. DMZ구간은 외부 접속점에서 DMZ 내에 수용된 각종 server 구간 까지로서 Exterior Router → Web switch → Firewall → Web switch → DMZ → Servers 까지이다.

〈표 1〉 Traffic 소통경로표

구 간	Routing	Load Balancing	Paket Filtering	Virus checking	Load balancing	Routing	destination
Intranet	Exterior router	Layer 4 switch	Firewall	Firewall	Layer4 switch	Interior router	Intranet
DMZ	Exterior Router	Layer4 switch	Firewall	Firewall	Layer4 switch		DMZ

3.2.3 Gateway level 방역 실시

gateway level은 mail gate, web gate/internet proxy가 있다. virus 방역에는 오염 site로부터 유입되는 traffic filtering이 매우 중요하다. virus 감염으로부터 data를 보호하기 위해서는 virus가 네트워크상 핵심 중요정보에 도달하기 전에 실시하는데 web traffic과 SMTP traffic을 대상으로 한다. 통계에 의하면 일반적으로 전체 traffic에서 차지하는 비중은 web traffic이 80%, SMTP traffic이 10%로 나타난다. 따라서 이 두 개 종류의 traffic에 대해 사전방역을 실시하는 방안은 virus 차단과 performance 향상 두 가지 측면에서 매우 긴요하다.

Gateway 방역의 기본 기능은 filtering 기능이다. gateway에서 적용할 수 있는 filtering 종류는 virus filtering, contents filtering, email filtering, file filtering, spam filtering등으로 구분할 수 있다. virus filtering은 packet 단위로 virus 감염여부를 점검 삭제하며 Contents filtering은 email의 제목과 본문내용에서 특정 keyword가 발견되는 경우 이를 차단하는 기능이다. Email filtering은 email 통과허용 size를 제한하는 기능이며, file filtering은 특정 첨부 file명이나 확장자를 미리 검사해 차단하는 기능이다. 그리고 지속적으로 발송되어 오는 mail을 차단하는 기능이다.

3.2.4 내부 network 유통 virus 방역 실시

client용 vaccine은 pc의 virus를 차단하나 server에 잠복해있는 mail의 첨부 file에 대해서는 검사하지 못한 채 server의 DB가 감염될 경우 전체 network에 치명적인 결과를 초래한다. 널리 배치된 많은 수의 client에 대한 개별적인 방역보다는 server 단위에서 관리하고 방역을 수행하는 server 차원방역이 효과적이며 매우 강력하다고 할 수 있다. 특히 intranet 내부에 침투하여 확산되는 virus 박멸 대책으로서 server 단위에서의 방역은 대단히 중요한 의미를 갖는다. 내부네트워크 유통경로상의 Virus 차단을 local five server의 전단에 별도의 Virus wall system을 설치하거나 각 server상에 software embed ded 방식의 scanner를 장치한다.

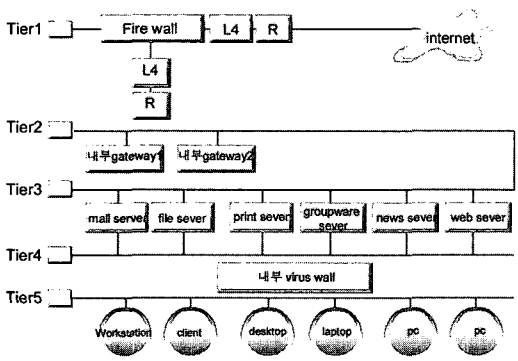
설치된 vaccine enqine에 의해서 각종 virus의 내부 유통에 server 전단에서 다시 한번 virus가 차단된다.

Vaccine enqine 설치 방법은 독립된 server 형태로 하거나 software module 삽입의 방법을 각 site의 실정에 맞게 custimizing 하여야 한다. 이렇게 장치된 virus wall은 file wall의 virus wall과 gateway level 방역과 comination을 통해 내부유통경로상의 virus 차단이 가능하다. Server level 방역대상 자원은 local file server의 범위에 있는 Application server, file server, print serer이다.

〈표 2〉 개선체계내용

구 분	일 반 구 조	개 선 구 조	내 용
Network infra 구조 재구성	◦ 수직구조 - firewall - server - clients ◦ 2단계 또는 3단계 차단구조	◦ 수직, 수평혼성 - firewall - gateway - servers - 내부 네크워크 - clients ◦ 5단계 차단구조	Gateway level 신설 수평구조로 전환
Traffic 소통경로 재설정	모든 Traffic 단일경로소통	◦ gateway 구간 경로설정	Web switch로 traffic 분리
방역대상 zone 확대	◦ email 경로위주 ◦ email 이외 모두 수동방역	◦ 저장매체 ◦ 공유폴더 ◦ 뉴스그룹 ◦ web경로 ◦ email 경로 ◦ 내부네트워크 유통경로	각종 자원을 방역 zone에 편입
gateway 구간방역 실시	Firewall 상에서 email virus 차단	1차 : firewall 2차 : gateway	Web swith로 Traffic 분리
내부 network level 방역실시	◦ Server방역, 미실시, 또는 수동방역	◦ Server 진출입구간에 virus wall 배치 ◦ server별 scanning실시	별도의 virus wall 설치

3.3 시스템 개선구조도



(그림 3) 개선된 protection infrastructure

◦ intra 구조는 2단계차단 또는 3단계차단에서 5단계 차단 방식으로 변경하고 gateway level에서 전체 server에 대한 filtering과 방역실시

◦ internet traffic 소통경로는 traffic 유형별로 분리하여 차별화 방역실시

◦ local file server 진출입 구간 virus wall 배치로 network 유통 virus 방역

◦ gateway 하부구조인 client level에 대하여 real-time 방역 network를 구성

4. 성능분석

4.1 분석환경

설계된 구조 중 모든 항목의 성과측정이 현실적으로 어렵기 때문에 측정이 가능한 부분을 대상으로 성능을 측정했다. 개선된 구조하에서 가장 큰 변경이 가해진 부분이 Web traffic 분야와 mail traffic 분야로 대표될 수 있지만 측정 가능 부분으로서는 gateway 방역 성과의 mail 시스템 상에서의 virus 차단성과에 관한 것을 선정했다. Mail virus를 기준으로 방역성과를 측정한 이유는 전체 virus중mail virus 점유비가 80%이상으

로서 대표성을 갖는다는 것과 또 하나는 email 이외에 다른 traffic의 경우는 개선 전후의 data 채집이 이루어지지 않아 비교가 불가능하다는 것이다. 본 측정에 사용된 테스트용 mail system의 제원은 virus wall 시스템은 E3500 기종으로, CPU는 400Mhz*6, Memory는 6 Giga이며 software는 secureworks의 virus wall제품임.

4.2 Mail virus 방역 성과

〈표 3〉 개선구조 성과 측정치

구 분	개선전	개선후	비 고
Virus wall CPU 부하	순간최대 100%	순간최대 60%	
바이러스 치료 실패후 메일수	10%	3%	
송신적체/ 대기(일간)	5600개	500개	
시스템 최대 프로세스수	3.000개	10.000개	

개선구조 성과 측정결과

◦ virus wall CPU 부하

virus로 인하여 mail virus wall CPU는 부하 수준이 순간 최대 100%까지 상승함으로서 process 처리지연이 발생하고 이로 인해 email 송신지연이 발생했다. 개선된 구조에서는 virus차단에 의해 virus wall 부하가 60% 이하로 안정되었다.

◦ virus 치료실패 mail

virus 급증에 따라 virus 치료에 실패하여 virus 감염 mail이 mail 서버로 전송되는 mail이 10% 수준에 이르렀으나 구조개선후 비율이 3% 이내로 감소했다.

◦ email 송신적체

virus wall 부하가 중시 전송대기 mail 건수가 일간 최대 56000건에 이르렀다 virus wall 부하 경감 시 전송대기 mail 숫자는 현저히 감소했다.

◦ 시스템 최대 process수

전송적체로 시스템 CPU의 성능이 저하 됨 으로서 최대 process수는 3,000개 수준으로 하향 조정이 불가피 했다 그러나 시스템 구조개선후 process수는 10,000개로 정상수준에 도달했다.

5. 결 론

본 논문에서는 날로 위협강도가 높아지는 오늘날의 virus 침투 pattern에 대처하기 위한 방안으로서 infrastructure 구성 측면에서 개선된 효율적 model을 연구하였다. 그 방법론은 protection infrastructure 재구성, traffic 소통경로 재설정, gateway level 방역실시, 내부 network 유통 virus 방역, 방역 zone 확대로 요약된다. 효과적인 virus 차단을 위해서는 infrastructure 개선과 scanning tool의 combination을 통한 종합적인 접근이 오늘날의 virus 침투 환경에 대비한 유일한 대안임을 강조한다. 본 논문에서 제안하는 방법론은 그러나 virus를 항구적으로 퇴치 할 수 있는 근본적인 기술적 대처 방법이 아직 개발되지 못하고 있는 환경에서의 대안으로서 infrastructure 구성을 통한 해법을 모색하는 것으로서 항구적인 방역 기술 개발만은 숙제로 남겨두고 있는 것이다. Virus 방역 infra 구축은 지속적인 사고와 계획을 전제한 시스템적 접근이 필수 요소이다. 방역 architecture의 성공 여부는 infra에 대한 지속적인 개선, 유지보수, 관리에 달려있는 것이다.

참 고 문 헌

[1] Willam Stallings, "Network and Internetwork Security". Prentice Hall, 1995.

[2] J. Hruska, "Computer Virus and Anti-virus Warfare" Ellis Horwood, 1992.

[3] P. Denning "Computer Under Attack In-

truders, Worms and Virus", Addison-Wesley, 1990.
[4] F. Cohen, "A short Course on Computer Viruses", ASP Press, 1990.
[5] Bruce Schneier, "Applies Cryptography", Wiley, Second Edition, 1996.
[6] http://www.dreamedianet.co.kr/protect/right1.htm.
[7] http://msdn.microsoft.com.
[8] http://www.snut.ac.kt.

노 시 춘

1992년 고려대학교 경영대학원 경영정보학과 석사
2003년 경기대학교 대학원 정보보호기술공학과 박사
1970년~2004.12 KT IT본부시스템보안부장 및 충청전산국장 역임
2005.3~현재 남서울대학교 교양과정부 교수

김 수 희

1986년 University of Georgia 전산학과 (MS)
1988년 University of Georgia 수학과 (MA)
1993년 University of South Carolina 전산학과(Ph.D.)
1993년~1994년 Benedict College 조교수
1994년~현재 호서대학교 컴퓨터공학부 컴퓨터공학전공 교수

김 귀 남

미국 캔자스대학 수학과 (응용수학사)
미국 콜로라도주립대학 통계학과(통계학 석사)
미국 콜로라도주립대학 기계산업공학과 (기계산업공학과박사)
현재 경기대학교 정보보호기술공학과 주임교수