情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

보안 솔루션의 상호 연동을 통한 실시간 협력 대응 방안 연구*

김 지 훈,† 임 종 인, 김 휘 강‡
고려대학교 정보보호대학원

Collaborative security response by interworking between multiple security solutions*

JiHoon Kim,† Jong In Lim, Huy Kang Kim‡
Graduate School of Information Security, Korea University

요 약

자동화 툴로 인해 악성코드의 수가 기하급수적으로 증가하고 있을 뿐만 아니라 최근 보안 대응 체계를 우회하는 지능화된 악성코드의 출현으로 기업에 막대한 피해가 발생하고 있다. 기존 보안 대응 체계만으로는 나날이 고도화·지능화되는 보안 위협을 방어하는데 한계가 있음을 시사한다.

이에 보안 대응 체계 내의 각 보안 솔루션의 진단율 향상을 통한 전반적인 보안 위협 방어 수준 강화가 요구되고 있다. 개별 보안 솔루션의 탐지·방어 기술 진화, 보안 솔루션 간의 조합 구성을 통해 공격 대응력을 향상시켜 나감과 동시에, 보안 솔루션 간에 진단율 향상에 필요한 중요 정보를 실시간 공유하고, 해당 정보를 기반으로 한 다양한 보안 대응 기술 연구 개발이 시급하다.

본 논문에서는 지금까지의 인터넷 서비스 보안을 위한 보안 솔루션의 연동 구성 방식에 대한 연구 사례를 살펴보고, 그 한계점을 도출하여 지능화되고 있는 보안 위협에 대한 실시간 대응 개선을 위한 보안 솔루션 간의 상호 연동을 통한 유기적인 협력 기술 및 대응 방안을 제안하고자 한다.

ABSTRACT

Recently, many enterprises are suffering from advanced types of malware and their variants including intelligent malware that can evade the current security systems. This addresses the fact that current security systems have limits on protecting advanced and intelligent security threats.

To enhance the overall level of security, first of all, it needs to increase detection ratio of each security solution within a security system. In addition, it is also necessary to implement internetworking between multiple security solutions to increase detection ratio and response speed.

In this paper, we suggest a collaborative security response method to overcome the limitations of the previous Internet service security solutions. The proposed method can show an enhanced result to respond to intelligent security threats.

Keywords: Collaborative, security response, security solutions

접수일(2012년 10월 9일), 수정일(1차: 2012년 12월 4일, 2차: 2012년 12월 24일), 게재확정일(2013년 1월 28일)

* 본 연구는 한국연구재단(KRF-20110005499)과 지식경제부 및 정보통신산업진흥원의 "대학 IT연구센터 육성·지원사업(NIPA-2012-H0301-12-3007)"의 연구결과로 수행하였습니다.

† 주저자, smallj@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr

I. 서 론

유무선 환경의 통합, 웹 서비스 플랫폼의 진화 등 IT 시스템이나 인터넷 환경이 발전할수록 보안 위협의 공격 기술과 주요 확산 경로도 점차 복잡다단해지게 된다. 새로운 시스템을 개발하거나 인프라를 구축할 때 보안이 함께 고려되지 못하고 보안 취약점을 내재한 체 서비스화 되어 공격의 희생양이 되는 일도 비일비재하다. 공격자는 공격 성공 가능성을 높이기 위한 방법으로 다양한 공격무기를 동시에 탑재하고 활용하기도 한다. 해킹 기술들은 점차로 지능화, 악성화되고 있으며 자기 은폐, 난독화 기법의 활용을 통해 손쉽게 발각되지 않거나 신속한 대응 및 치료가 어렵게 만들기도 한다. 7.7 DDoS 및 3.4 DDoS 공격 등 2차례에 걸친 사이버 테러 발생의 영향으로 주요 정보기관, 금융기관, 포털 인터넷 사이트가 마비되는 등 사이버 보안의 중요성이 크게 대두되고 있다.

2011 국가정보화백서[1]에 따르면, 주요 국가 전산망에 대한 해킹 등 사이버침해 범죄건수가 2010년 기준 18,237건으로 2009년에 비해 10.2% 증가한 것으로 보고되었다. 단순한 보안 정책과 단일 보안 솔루션만으로는 사이버 테러 대응에 대처하기에 역부족이다. 백신 솔루션, 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS) 등 기존 보안 솔루션들의 개별적인 대응 기술이나 보안 솔루션의 단순한 조합 형태만으로는 더욱 지능화되고 다양화된 보안위협을 적절히 대응 하는 데 한계를 보이고 있다.

본 논문에서는 보안 솔루션 간의 유기적인 상호 연동을 통해 지능화된 보안위협에 대해 효과적인 대응이 가능하도록 하는 실시간 협력 대응 기술에 대해 연구를 진행하였다. 2장에서는 관련 연구로 인터넷 서비스 보안을 위해 그동안 진행되어 온 보안 솔루션의 연동 구성 및 협력 대응 프레임워크 연구에 대한 사례를 살펴보고 기술의 현황과 한계점에 대해 기술한다. 3장에서는 앞서 도출된 한계점을 극복하고 개선할 수 있는 보안 솔루션 간의 상호 연동을 통한 실시간 협력 대응 기술을 제안한다. 4장에서는 제안한 실시간 협력 대응 기술에 대한 실험 및 결과를 기술하며, 마지막으로 5장에서는 결론을 맺는다.

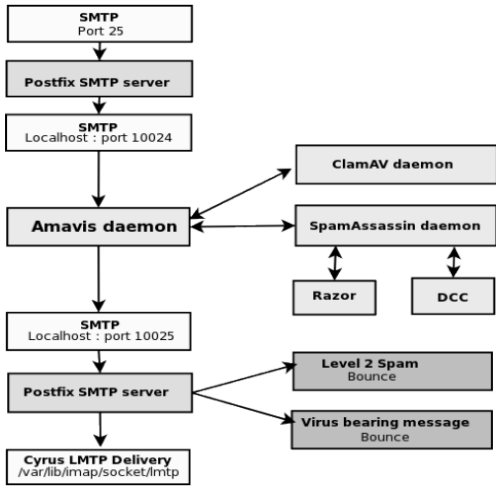
II. 연동 기술 모델 동향

인터넷 서비스 보안 기술은 가장 큰 보안 위협 중 하나로 손꼽히는 악성코드에 대응하기 위해 발전해왔다 해도 과언이 아니다. 악성코드의 전파를 차단하기 위해 사용되어 온 가장 효과적인 방법으로 인터넷 프락시 서버 (혹은 게이트웨이) 상에서 다양한 보안 솔루션을 연동하는 기술이 활용되어 왔다. 불건전한 이메일 컨텐츠 유통 차단을 위해 이메일 프락시 서버를 중심으로 스팸 솔루션, 백신 솔루션 등이 연동되었고, 웹을 통한 악성코드 유입 차단을 위해 웹 프락시 서버를 중심으로 유해사이트 차단 솔루션, 백신 솔루션 등이 연동 운영되고 있다.

2.1 인터넷 서비스 보안 강화를 위한 연동 기술

2.1.1 이메일 프락시 연동 기술

2000년대 들어, 마이둠 (Win32/Mydoom), 넷스카이 (Win32/Netsky), 베이글 (Win32/Bagle) 등의 이메일 웜이 성행하면서 이메일을 통한 악성코드 전파가 많은 피해를 입히게 되자, 이메일 프락시 상에서 이메일로 전파되는 악성코드를 차단하기 위해 백신 솔루션과의 연동이 자연스럽게 진행되었다. 또한, 봇넷 혹은 자동화된 공격 도구에 의한 피싱·스팸 메일 발송으로 인해 금전적인 피해가 유발하게 되면서, 스팸 차단 솔루션과의 연동으로 이어지게 되었다[2]. 아래 [그림 1]의 연동 구성은 메일러(Mail Transfer Agent)와 백신 및 스팸차단 기능을 갖는 보안솔루션들과의 고성능 인터페이스를 제공하는 Amavis 데몬[3]을 통해 이루어진다.



[그림 1] 이메일 프락시 서버와 보안 솔루션 연동

2.1.2 웹 프락시 연동 기술

〔표 1〕은 2010년 ~ 2012년에 발생한 웹을 통한 악성코드 유포에 활용된 주요 취약점들이다. 이러한 취약점들은 '공다팩', '블랙홀' 등의 웹 익스플로잇 툴킷 (Web Exploit Toolkit) 에 포함되어 다수의 악성코드 유포지를 생산하고 악성코드 감염에 악용되고 있다. 웹을 통한 악성코드 유입을 방지하기 위해, 웹 프락시 서버 구축을 통해 웹 트래픽을 중앙 통제할 수 있도록 하고, 유해사이트 차단 솔루션, 백신 솔루션과의 연동을 통해 웹 보안을 강화해 나가고 있다〔4〕. 아래 〔그림 2〕의 연동 구성은 웹 트래픽 상에 흐르는 유해 컨텐츠 유입을 방어하기 위해 백신 및 유해사이트 차단 기능을 갖는 보안 솔루션과의 연동 기술을 제공하는 웹 프락시 서버인 Squid Proxy cache〔5〕를 통해 이루어지며, 웹 프락시 서버와 백신 솔루션 간의 연동을 위해 ICAP 프로토콜(Internet Content Adaption Protocol)〔6〕이 지원하고 있다.

〔표 1〕 웹을 통한 악성코드 유포에 활용되는 주요 취약점

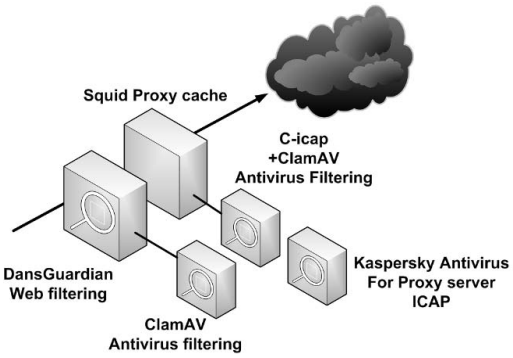
벤더	CVE 정보	취약성 정보
MS	CVE-2012-0003 CVE-2012-0004	윈도우 미디어 취약점
Adobe	CVE-2011-2110	플래시 취약점
MS	CVE-2011-1255	Internet Explorer 취약점
Adobe	CVE-2010-2884	플래시 취약점
MS	CVE-2010-1885	윈도우 도움말 및 지원 센터 취약점

2.2 기존 연동 기술의 한계점 및 제안의 필요성

앞서 살펴본 주요 인터넷 서비스 보안 강화를 위한 연동 기술을 정리해보면 〔표 2〕와 같다. 프락시 서버 중심으로 다수의 보안 솔루션을 연동함으로써, 보다 다양한 보안 위협에 대응하고 있다.

그러나, 현존하는 프락시 서버와 보호 솔루션의 연동 모델은 개개의 보안 솔루션의 서비스 목적에 따라 방어할 수 있는 보안 위협의 유형을 늘리는 정도에 그치고 있다. 보안 솔루션 간의 협력 대응 모델의 부재로 그 이상의 시너지 효과를 기대할 수 없어, 지능화된 보안위협에 대해 효과적으로 대응하기에는 어려움이 따른다.

본 논문에서 제안하고자 하는 주요 기술을 통해 기존의 보안 솔루션 연동 기술이 갖는 기술적 한계점을 보완하고 개선하며 아래와 같은 목적에 부합하였다.



〔그림 2〕 웹 프락시 서버와 보안 솔루션 연동

① 알려지지 않은 보안위협에 대한 대응 방안 마련
② 보안 대응 체계를 구성하는 보안 솔루션 간의 단순 조합 구성의 연동 방식을 넘어, 실시간으로 보안 솔루션 간에 필요 정보를 서로 공유하여 보안 솔루션의 진단율 향상을 도모함으로써 전반적인 보안 대응 체계의 방어 능력 향상시킬 수 있는 유기적 연동 구조로 개선
③ 보안 대응 체계를 구성하는 보안 솔루션이 생산하는 다양한 정보를 가공하여 미처 파악하지 못하였거나 새롭게 출현한 보안 위협에 대한 조기 대응 및 사전 대응력 개선

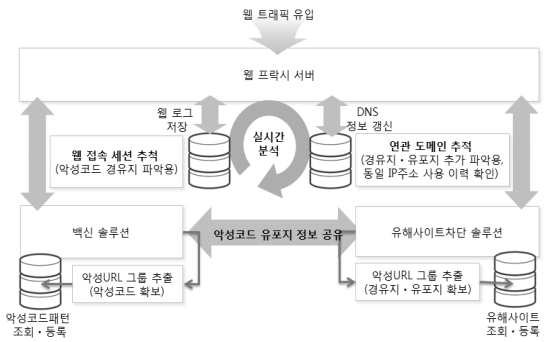
〔표 2〕 연동 기술의 한계점

연동 기술	한계점
이메일 프락시 + 스팸차단, 백신	• 알려지지 않은 보안 위협에 대한 대응이 어려움 • 다양한 우회 기법 (실행압축, 난독화, 은폐기법, 이미지 스팸 등)의 존재로 탐지를 회피할 수 있음
웹 프락시 + 유해사이트 차단, 백신	• 알려지지 않은 보안 위협에 대한 대응이 어려움 • 다양한 우회 기법의 존재로 탐지를 회피할 수 있음 • 보안 솔루션 간의 정보 공유 과정이 없어, 악성코드 및 유해사이트 정보를 연결 짓기 어려움 • 유해사이트 접근 시도 차단을 통해 악성코드 유입을 차단할 수는 있으나, 해당 사이트로부터 유포되는 새로운 악성코드 샘플을 수집하는 기능이 존재하지는 않음 • 특정 사이트의 알려진 악성코드 유입을 차단할 수는 있으나, 동일 사이트로부터 알려지지 않은 악성코드 유입시 효과적이고 신속한 대응이 어려움 (분석가 개입 필요, 분석 등으로 시간 소모)

III. 실시간 협력 대응 기술 제안

3.1 실시간 협력 대응 기술 프레임워크

본 장에서는 기존 연동 기술로 구현된 환경 하에서 앞서 도출된 한계점을 보완하고 개선할 수 있도록 보안 솔루션 간의 유기적인 상호 연동을 통한 실시간 협력 대응 기술을 제안하고자 한다. 〔그림 3〕의 실시간 협력 대응 기술 프레임워크를 구성하는 주요 세부 기술에 대한 설명은 〔표 3〕과 같다.



〔그림 3〕 실시간 협력 대응 기술 프레임워크

구현된 환경은 모든 웹 트래픽을 웹 프락시 서버인 Squid Proxy cache〔5〕를 통해 흐르도록 구성하였고, 웹 프락시 서버와 백신 솔루션인 ClamAV〔7〕 및 유해사이트차단 솔루션인 squidGuard〔8〕 간의 기존 연동 기술을 사용하였다.

웹 프락시 서버와 연동하는 보안 솔루션 단에서, 이미 알려진 악성코드 및 유해사이트에 대한 탐지・차단 이벤트가 발생한 경우 타 보안 솔루션이 해당 이벤트를 참조할 수 있도록 하는 보안 이벤트 공유 설정을 정의하였다.

또한, 웹 접속 세션 추적 기술을 추가 적용하여 새롭게 발견된 악성코드 유포지와 연관된 악성코드 경유지 파악이 가능하게 하여 동일한 경유지를 통해 새롭게 변경되는 악성코드 유포지를 조기에 탐지・차단할 수 있도록 하였다.

더 나아가 연관 도메인 추적 기술을 추가 적용하여 기존에 미처 발견하지 못한 유해사이트와 악성코드를 파악할 수 있도록 하였을 뿐만 아니라, 웹 프락시 서버를 통해 새롭게 접근 시도 되는 모든 웹 사이트에 대한 연관 도메인 추적을 통해 블랙리스트화된 유해사이트와 동일한 IP주소를 사용하는 알려지지 않은 새로운 유해사이트 및 악성코드에 대한 대응이 가능하도록 하였다. 새롭게 파악된 악성코드 및 유해사이트 정보를 기반으로 웹 프락시 서버와 연동된 개별 보안 솔루션은 각자 자신에 맞는 대응 패턴을 신속하게 제작・ 차단 적용하도록 하는 실시간 협력 대응 기술을 적용하였다.

〔표 3〕 실시간 협력 대응 프레임워크의 세부 기술

세부 기술	설명
보안 이벤트 정보 공유 설정	악성코드 유포지 정보를 보안 솔루션 상호간 공유한다. • 보안 솔루션에 의해 악성코드 유포지가 확인된 경우, 해당 악성코드 유포지 정보를 포함하는 탐지・차단 이벤트를 발생시키고, 이를 통해 타 보안 솔루션이 활용할 수 있도록 한다.
웹 접속 세션 추적	악성코드 경유지 정보를 추적한다. • 웹 프락시 서버의 모든 웹 접속 로그를 데이터베이스화 한다. • 보안 솔루션에 의해 악성코드 유포지가 확인되는 경우, 웹 접속 로그 추적을 통해 악성코드 유포지와 연결된 악성코드 경유지 정보를 추적하여 새로운 악성코드 경유지를 탐지하고 블랙리스트로 표기한다.
연관 도메인 추적	연관된 유해사이트 정보를 추적한다. • 웹 프락시 서버를 통해 접속하는 모든 웹 사이트 도메인명과 IP 주소를 데이터베이스화 한다. • 악성코드 경유지・유포지로 확인될 경우, 동일 IP 주소 기반으로 연관된 도메인 정보를 추적하여 블랙리스트로 추가 표기한다. • 접속 시도되는 모든 웹사이트에 대한 IP 주소와 블랙리스트화된 악성코드 경유지・유포지의 IP 주소의 일치를 확인하여 새로운 유해사이트를 탐지하고 블랙리스트로 표기한다.
보안 솔루션 대응	새롭게 발견된 악성코드 및 유해사이트를 신속하게 차단 적용한다. • 백신 솔루션은 새로운 악성코드를 즉시 차단 적용한다. • 유해사이트 차단 솔루션은 새로운 유해사이트를 블랙리스트로 즉시 차단 적용한다.

3.2 실시간 협력 대응 기술 구현 및 적용

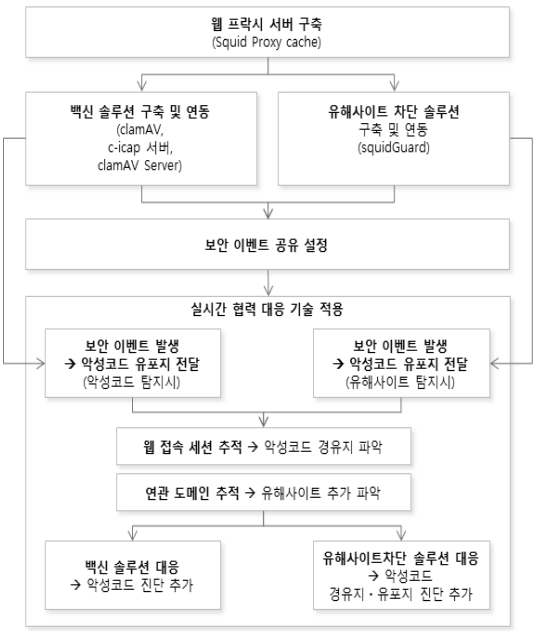
실시간 협력 대응 기술의 활용도를 높이기 위해 〔표 4〕의 널리 사용 중인 오픈 소스를 이용하여 기존의 웹 프락시 서버 기반의 보안 솔루션 연동 기술을

적용한 기본 환경을 구성하였다. 해당 오픈 소스들은 설치가 쉽고, 다양한 솔루션과의 연동 모델이 이미 존재하여 확장성이 뛰어나다.

〔표 4〕 기술 구현에 이용된 오픈 소스 목록

오픈 소스	최신 버전	설 명
Squid Proxy cache〔5〕	3.2.0.16	웹 프락시 서버
ClamAV〔7〕	0.97.5	백신 솔루션
ClamAV-Server〔9〕	0.97.5	백신 서비스 (데몬)
SquidClamAV〔10〕	6.8	C-IAP서버의 백신 프로그램 서비스 호출 모듈
C-ICAP〔11〕	0.2.1	ICAP 프로토콜 지원 서버
squidGuard〔8〕	1.5-beta	유해사이트 차단 솔루션

또한, 기존 기술의 한계점을 보완하고 개선하기 위해 연구된 보안 이벤트 공유 설정 및 웹 접속 세션 추적, 연관 도메인 추적, 보안 솔루션 대응을 포함하는 실시간 협력 대응 기술을 추가 구현하여 〔그림 3〕의 기술 프레임워크가 〔그림 4〕의 기술 흐름도에 따라 동작하도록 하였다.



〔그림 4〕 실시간 협력 대응 기술 흐름도

3.2.1 보안 이벤트 공유 설정

개별 보안 솔루션에서, 유해사이트 혹은 악성코드를 탐지하였을 경우 발생되는 보안 이벤트는 연동하는 웹 프락시 서버의 로그를 통해 실시간 협력 대응 파트너 솔루션에게 공유되도록 하였다. 공유되는 보안 이벤트의 형식은 〔표 5〕, 〔표 6〕과 같다.

〔표 5〕 보안 이벤트 주요 형식

포 맷	설 명
%{%Y-%m-%d %H:%M:%S}tl	DATE (탐지 시간)
%〉a	IP Address (탐지된 클라이언트 IP 주소)
%〉p	Port (탐지된 클라이언트 Port 주소)
%rm	Method (웹 요청 메소드)
%ru	URL (요청된 URL 정보)

〔표 6〕 URL(%ru)의 세부 형식

항 목	설 명
Redirect_URL	차단시, 유도(Redirect)할 웹페이지 ex) http://www.ahnlab.com/kr/site/product/productView.do?prodSeq=8
by_detect	보안이벤트를 공유한 보안 솔루션 표식 ex) by_detect=squidGuard or by_dtect=clamAV
url	차단된 요청 URL 주소

아래 〔그림 5〕와 같이, 백신 솔루션 (by_detect=clamAV)이 악성코드 qaz2.exe를 탐지한 경우 미리 정의한 보안 이벤트 형식에 따라 악성코드 유포지 xx.xiumaa.com 정보가 공유되고 아래 〔그림 6〕과 같이, 유해사이트차단 솔루션 (by_detect=squidGuard)이 유해사이트 ddd.mhyddrrd.com을 탐지한 경우 미리 정의한 보안 이벤트 형식에 따라 해당 유포지를 통해 유입 시도된 악성코드 bq6.exe 의 정보

```
2012-11-16 20:58:37|111.2.0.87|1084|211.233.80.29|80
|www.ahnlab.com|/kr/site/product/productView.do?prodSeq=8&
by_detect=clamAV&?url=http://xx.xiumaa.com/010/qaz2.exe&so
urce=111.2.0.87&user=-&virus=stream:%20Win.Trojan.Chiviper
(aaef43be52f8b197349a314ab8ecc915:53248)%20FOUND|GET|http:
//www.ahnlab.com/kr/site/product/productView.do?prodSeq=8&
by_detect=clamAV&?url=http://xx.xiumaa.com/010/qaz2.exe&so
urce=111.2.0.87&user=-&virus=stream:%20Win.Trojan.Chiviper
(aaef43be52f8b197349a314ab8ecc915:53248)%20FOUND|-|104744|
```

〔그림 5〕 백신 솔루션(clamAV)에 의해 공유된 악성코드 유입 차단 보안 이벤트

```
2012-11-16 22:41:54|111.2.0.87|3685|211.233.80.29|80
|www.ahnlab.com|/kr/site/product/productView.do?prodSeq=8&
by_detect=squidGuard&url=http://ddd.mhyddrrd.com/ckr/bq6.e
xe|GET|http://www.ahnlab.com/kr/site/product/productView.d
o?prodSeq=8&by_detect=squidGuard&url=http://ddd.mhyddrrd.c
om/ckr/bq6.exe|-|104744|0
```

〔그림 6〕 유해사이트차단 솔루션(squidGuard)에 의해 공유된 악성코드 유포지 접근 차단 보안 이벤트

가 공유된다.

즉, 개별 보안 솔루션에서 각각 기진단되어 발생한 보안 이벤트 정보의 실시간 공유를 통해 기존에 알려지지 않은 유포지 xx.xiumaa.com 과 악성코드 bq6.exe를 새롭게 파악할 수 있게 된다. 이 정보는 보안 솔루션에 신속하게 진단 추가 되어 동일 유포지 및 악성코드에 대한 사전 예방 효과를 기대할 수 있다.

3.2.2 웹 접속 세션 추적 기술

악성코드 유포지 탐지시, 접속한 사용자의 웹 접속 세션을 추적하여 악성코드 유포지와 연관된 악성코드 경유지를 파악하였다. 이를 위해 웹 프락시 서버를 통한 모든 웹 접속 기록은 데이터베이스화 하고, 접속 시도한 클라이언트의 접속 시간대, IP 주소, 세션 Port 등의 정보를 기반으로 악성코드 경유지를 파악한다.

아래 〔그림 7〕과 같이, 웹 접속 세션 추적 기술을 통해 유해사이트 ddd.mhyddrrd.com를 통해 유포된 악성코드 bq6.exe 가 악성코드 경유지 ly.nhyujmds.com로부터 비롯된 공격임을 파악할 수 있어 알려지지 않은 보안 위협에 대한 대응력을 한층 강화하는 데 도움을 준다.

```
2012-11-20 20:20:11|http://ly.nhyujmds.com/xrly/swfobject.js
2012-11-20 20:20:12|http://ly.nhyujmds.com/xrly/jpg.js
2012-11-20 20:20:14|http://ly.nhyujmds.com/xrly/iLyfoO2.html
2012-11-20 20:20:44|http://ddd.mhyddrrd.com/ckr/bq6.exe
```

〔그림 7〕 웹 세션 추적 기술을 통한 악성코드 경유지 파악

3.2.3 연관 도메인 추적 기술

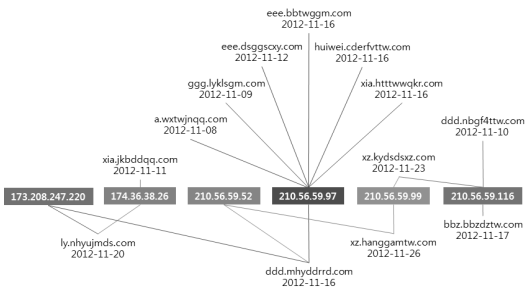
악성코드 유포지 탐지시, 동일 IP 주소를 사용한 적 있는 유해사이트를 추가 파악하였다. 이를 위해 웹 프락시 서버를 통해 접근한 적 있는 모든 웹 사이트 도메인에 대해 지속적으로 IP 주소 조회 결과 (DNS Lookup)를 갱신하여 데이터베이스화 하고, 악성코드 유포지의 IP 주소 일치 여부를 기반으로 미처 발견하지 못하였거나 새롭게 확인된 웹 사이트의 유해 여

```
210.56.59.50|173.208.247.220|210.56.59.92|173.208.247.217|210.5
6.59.52|182.16.9.122|210.56.59.97|210.56.59.99|182.16.7.10|182.
16.9.196|173.208.189.171|182.16.9.125|210.56.59.86|173.208.247.
197|173.208.247.195|174.36.138.26|173.208.247.196|210.56.59.74|
180.178.38.245|182.16.9.197|210.56.59.116|210.56.59.91|NULL
ddd.mhyddrrd.com|huiwei.cderfvttw.com|xia.htttwwqkr.com|ggg.lyk
lsgm.com|xia.jkbddqq.com|ly.nhyujmds.com|xz.kydsdsxz.com|eee.bb
twggm.com|ddd.nbgf4ttw.com|xz.hanggamtw.com|a.wxtwjnqq.com|eee.
dsggscxy.com|bbz.bbzdztw.com|NULL
```

〔그림 8〕 연관 도메인 추적을 통한 유해사이트 파악 I

부를 파악한다.

위 〔그림 8〕과 같이, 연관 도메인 추적 기술을 통해 악성코드 경유지 ly.nhyujmds.com 과 악성코드 유포지 ddd.mhyddrrd.ciom 이 사용해왔던 IP 주소 목록을 기반으로 추적하여 연관된 도메인들을 추가적으로 파악한다. 아래 〔그림 9〕는 추적된 도메인-IP 주소 간의 연관성을 쉽게 확인할 수 있도록 도식화한 것이다. 유해사이트 도메인명 아래에 WHOIS 정보를 통해 확인된 도메인 생성일자를 기재하였다. 시간이 흐름에 따라 공격자가 새로운 유해사이트를 지속적으로 생성하여 악성코드 유포 공격에 이용하더라도 본 연관 도메인 추적 기술을 통해 효과적인 대응이 가능하게 되어 알려지지 않은 보안 위협에 대한 대응력을 한층 더 강화할 수 있다.



〔그림 9〕 연관 도메인 추적을 통한 유해사이트 파악 II

또한, 새롭게 접근 시도되는 모든 웹 사이트들의 유해 여부를 파악하는 데에도 본 기술을 효과적으로 활용될 수 있어 알려지지 않은 보안 위협- 유포지 및 유포되는 악성코드 - 에 대한 대응을 가능하게 한다.

3.2.4 보안 솔루션 대응 기술

앞서 설명한 보안 솔루션 간의 보안 이벤트 (악성코드 유포지 정보) 공유, 웹 세션 추적 및 연관 도메인 추적 기술을 통해 파악한 알려지지 않은 새로운 악성코드 및 유해사이트 정보를 보안 솔루션에 진단 추가하여 차단 적용함으로써 본 논문에서 제안하는 보안 위협에

대한 실시간 협력 대응 체계가 비로소 마련된다.

아래 〔그림 10〕은 새롭게 파악된 악성코드 유포지로부터 악성코드를 다운로드하여 백신 솔루션에 진단 추가하는 대응 과정을, 〔그림 11〕은 새롭게 파악된 악성코드 경유지·유포지 정보를 유해사이트차단 솔루션에 진단 추가하는 대응 과정을 보여주고 있다.

```
$wget       = '/bin/wget -O realtime.ex_ '.$real[1];
system($wget);
$sigtool    = '/bin/sigtool --md5 realtime.ex_ >> /var/lib/clamav/realtime.hdb';
system($sigtool);
system('clamscan --remove=yes realtime.ex_');
```

〔그림 10〕 백신 솔루션 대응 과정

```
open(SG_D, '>> /usr/local/squidGuard/db/malware/domains');
print SG_D "$malsite[1]\n";
system('/usr/local/bin/squidGuard -C all');
system('/usr/sbin/squid -k reconfigure');
close(SG_D);
```

〔그림 11〕 유해사이트차단 솔루션 대응 과정

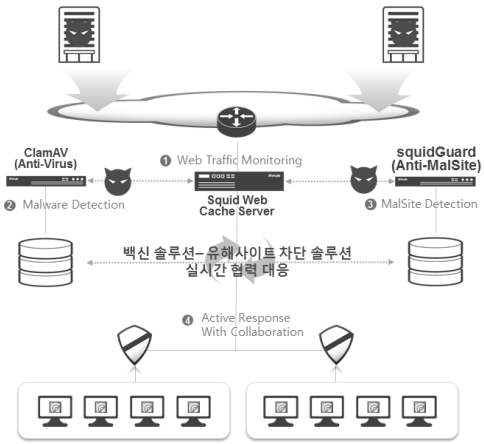
IV. 실험 및 평가

이번 장에서는 본 논문에서 제안하고 있는 보안 솔루션의 상호 연동을 통한 실시간 협력 대응 기술 평가를 위해 일정 기간 동안 인터넷 상에서 실제 발생한 악성코드 유포 공격을 대상으로 기존 연동 기술과 제안된 실시간 협력 대응 기술에 대한 악성코드 유입 차단 실험을 진행하였다. 본 실험의 결과로, 제안된 기술 적용을 통해 새롭게 발견되는 악성코드 및 유해사이트에 대한 즉각적인 실시간 협력 대응이 가능함을 증명하였고, 보안 솔루션들의 단순 조합 형태의 기존 방식에서는 크게 기대할 수 없었던 알려지지 않은 보안 위협에 대한 신속한 조기 대응 및 사전 예방 효과를 확인할 수 있었다.

4.1 실험 환경

실제 인터넷 상에서 발생한 총 118회의 악성코드 유포 공격을 〔그림 12〕의 구현된 실험망 환경으로 유입 시도하여 실험을 진행하였다. 실험에 사용된 악성코드 및 유해사이트에 대한 〔표 7〕의 실험 데이터 셋은 공격자가 다양한 악성코드 경유지·유포지를 지속적으로 생성하여 악성코드를 무차별적으로 고객 시스템을 감염시키는 데 활용하는 최근의 지능화된 공격 형태와 악성코드마다 서로 다른 횟수로 중복 유입 시도 되는 실제 공격 특징이 반영되어 있다.

인터넷으로부터의 악성코드 유입 차단을 위해 〔그림 12〕의 실험망 환경의 각 구성요소는 논문에서 제안하고 있는 실시간 협력 대응 기술의 〔그림 3〕 프레임워크와 〔그림 4〕 흐름도에 따라 동작하도록 〔표 8〕



〔그림 12〕 실험망 환경

〔표 7〕 실험 데이터 셋 현황

모니터링 기간	2012년 11월 07일 ~ 2012년 11월 21일
유입 시도	총 118번의 악성코드 유입시도
악성코드 경유지	37개 사이트
악성코드 유포지	14개 사이트
악성코드 수	41종의 신종/변형 악성코드

〔표 8〕 실험망 환경에서의 실시간 협력 대응 기술의 동작

프레임워크 기술	구성요소별 동작 설명
기존 연동 기술 동작	① 웹 프락시 서버인 Squid Proxy cache는 모든 웹 트래픽을 모니터링 한다. ② 백신 솔루션인 clamAV는 알려진 악성코드 유입을 차단한다. 실제 실험에서는 글로벌 백신 솔루션 5종을 병행 진단하여 한 개 이상의 솔루션에서 진단할 경우 실험망 환경의 백신 솔루션인 clamAV에서 진단할 수 있도록 미리 진단 추가해 두었다. ③ 유해사이트차단 솔루션인 squidGuard는 유해사이트 접근 시도를 봉쇄하여 악성코드 유입을 차단한다.
제안된 실시간 협력 대응 기술 동작	④ 악성코드 유입 탐지시, 보안 솔루션 간 악성코드 유포지 정보를 포함한 보안 이벤트를 공유하여 개별 보안 솔루션이 악성코드 및 악성코드 유포지를 진단 추가한다. 또한, 웹 접속 세션 추적 및 연관 도메인 추적을 통해 새롭게 파악된 추가적인 악성코드 및 악성코드 경유지 정보를 추가 진단한다.

과 같이 기술 구현・적용하였다.

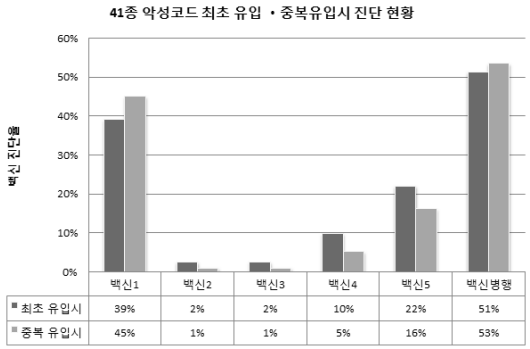
4.2 기존 연동 기술의 악성코드 유입 차단 실험

4.2.1 웹 프락시 서버와 백신 솔루션의 단순 연동

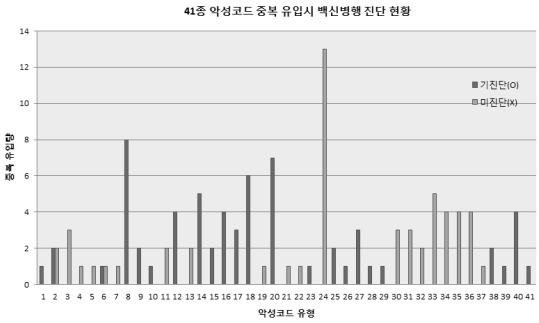
〔표 7〕의 실험 데이터 셋, 41종의 악성코드가 다양한 경유지・유포지를 통해 총 118회 실험망으로 유입될 당시의 백신 솔루션의 진단 현황을 조사하였다. 악성코드별 최초 유입시 (총 41회) 진단 현황과, 중복 유입시 (총 118회)에 대한 글로벌 백신 솔루션 5종의 개별 진단현황과 병행 운영시의 진단 현황은 아래 〔그림 13〕과 같이 약 50% 수준의 진단으로 지속적으로 변형되어 유포되는 악성코드 유입시 효과적인 사전 예방이 어려움을 알 수 있다. 각 백신의 진단율이 다르게 나타난 이유는 샘플 수집 능력과 휴리스틱 진단 기능의 차이에 따른 것으로 풀이된다.

〔그림 13〕의 실험 결과에서, 악성코드의 최초 유입과 중복 유입시 백신 진단율 차이는 기진단・미진단되는 악성코드의 중복 유입량의 차이에 따른 영향으로 확인되었다. 기진단되는 악성코드의 유입량이 많을수록 진단율이 상승하며, 미진단되는 악성코드의 유입량이 많을수록 진단율은 하락한다.

또한, 백신마다 최초 유입과 중복 유입시의 진단율 특징이 다르게 나타나는 이유는 악성코드별로 중복 유입 시도 횟수가 다른 실제 인터넷 환경에서의 공격 특징이 〔표 7〕의 실험 데이터 셋에 반영된 것이라 할 수 있다. 위 〔그림 14〕은 41종 악성코드의 중복 유입시 백신병행 진단 현황을 나타낸 것이다.



〔그림 13〕 악성코드 유입별 백신 진단 현황



〔그림 14〕 악성코드 중복 유입시 백신병행 진단 현황

4.2.2 웹 프락시 서버와 유해사이트차단 솔루션의 단순 연동

총 11개 사이트에서 제공하는 유해사이트 도메인 정보를 유해사이트차단 솔루션에 적용하여 악성코드 유포지 접근 시도에 대한 차단을 진단한 결과, 악성코드 유입 이전에 단 한 건의 차단도 발생되지 않았다. 이러한 결과는 〔표 9〕의 공격 패턴의 분석을 통해 충분한 설명이 가능하다.

공격자는 효율적인 악성코드 유입 성공을 위해 특정 악성코드 경유지・유포지를 지속적으로 생성하고 짧은 기간 동안만 활용하는 패턴을 반복적으로 보였다. 기존의 유해사이트에 대한 대응이 진행되기 이전에 새로운 경유지・유포지를 생성하여 공격을 진행하

〔표 9〕 도메인 생성 후 단기간 활용의 공격 패턴 분석

유해사이트명	도메인 생성시점 (UTC)	도메인 공격 활용 기간 (UTC+9)	
b.xiangzitao.com	2012-11-05	2012-11-07 ~ 2012-11-09	6일
qq.xiama1q.com	2012-11-08	2012-11-09 ~ 2012-11-10	2일
eee.dsggscxy.com	2012-11-12	2012-11-12 ~ 2012-11-17	6일
xx.xiumaa.com	2012-11-16	2012-11-16 ~ 2012-11-18	3일
ddd.mhyddrrd.com	2012-11-16	2012-11-16 ~ 2012-11-21	6일
ndtw.wmdottw.com	2012-11-17	2012-11-17 ~ 2012-11-18	2일
xx.wtxty.com	2012-11-16	2012-11-18 ~ 2012-11-19	6일
sb.rnmmb.com	2012-11-20	2012-11-21 ~ 2012-11-21	1일

는 것이다.

4.3 제안된 기술의 악성코드 유입 차단 실험

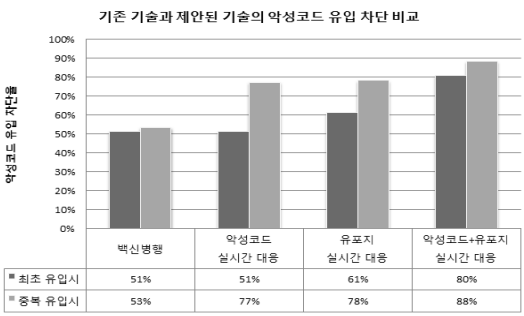
제안된 실시간 협력 대응 기술의 실험은 〔표 10〕의 평가 항목 및 방법을 통해 진행되었다. 본 실험은 기존 연동 서비스 방식을 기본 구성으로 유지하며 추가적인 연동을 통한 실시간 협력 대응 기술 - 보안 이벤트 공유 설정, 보안 솔루션 대응 - 의 구현·적용을 통해 지능화된 악성코드의 유입의 효과적인 차단을 검증하는 데 그 목적이 있다.

〔표 10〕 제안된 실시간 기술의 평가 항목 및 방법

실험 항목	세부 내용	평가 방법
보안 이벤트 정보 공유	악성 코드 실시간 대응	다음 유형의 악성코드 유입 차단율을 평가한다. • 알려진 악성코드 유입 차단 • 유해사이트차단 솔루션에 의해 공유된 악성코드 유포지 정보로부터 악성코드 획득·진단 추가하여 동일 악성코드 유입 차단
	악성 코드 유포지 실시간 대응	다음 유형의 악성코드 유입 차단율을 평가한다. • 알려진 악성코드 유포지 접근을 차단 • 백신 솔루션에 의해 공유된 악성코드 유포지 정보로부터 악성코드 유포지 획득·진단 추가하여 동일한 악성코드 유포지 접근 차단

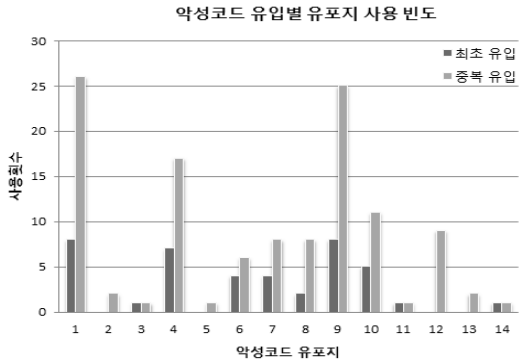
아래 〔그림 15〕와 같이, 보안 솔루션 간의 보안 이벤트 공유를 통한 실시간 대응 기술의 적용으로 악성코드 유입 차단율은 기존 단순 연동 기술의 차단율에 비해 개선되었다.

〔그림 15〕의 실험 결과에서, 악성코드의 최초 유입과 중복 유입시 차단율 차이는 제안된 기술을 통해 새롭게 진단 추가되는 악성코드 유포지 사용빈도, 악성코드와 유포지 간의 연관성, 그리고 악성코드의 중복 유입량에 따른 영향으로 확인되었다.



〔그림 15〕 제안된 기술의 악성코드 유입 차단율 개선 현황

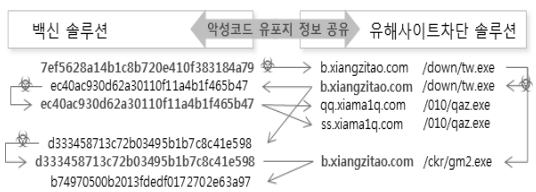
아래 〔그림 16〕은 41종 악성코드의 최초 유입 및 총 118회 중복 유입시의 유포지 사용빈도를 나타낸 것이다. 기진단되는 유포지 사용빈도가 높을수록 유입 차단율이 상승하고, 미진단되는 유포지 사용빈도가 높을수록 유입 차단율은 하락한다.



〔그림 16〕 악성코드 유입별 유포지 사용 빈도

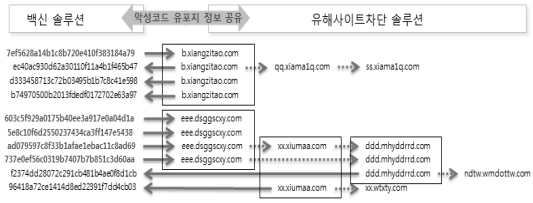
아래 〔그림 17〕은 본 실험을 통한 실시간 협력 대응 사례를, 〔그림 18〕은 본 실험에서 확인된 동일 악성코드를 유포하는 새로운 도메인들의 연관 관계를 나타낸다. 백신 솔루션과 유해사이트차단 솔루션 간에는 악성코드 유포지 정보를 실시간으로 공유한다.

〔그림 17〕에서, 최초 유입된 악성코드(md5:-7ef5628a14b1c8b720e410f383184a79)는 백신 솔루션에 의해 기진단되고, 새로운 유포지 도메인 정보 b.xiangzitao.com 은 유해사이트차단 솔루션에 진단 추가된다. 이후 해당 도메인을 이용하는 유포지 접근은 차단되며, 새로운 악성코드는 신속하게 수집되어 백신 솔루션에 진단 추가된다. 동일 악성코드를 유포하는 새로운 유포지 도메인 qq.xiama1q.com과 ss.xiamalq.com 도 신속하게 진단 추가된다. 제안된 기술에 의해 진단 추가되는 악성코드와 유포지가



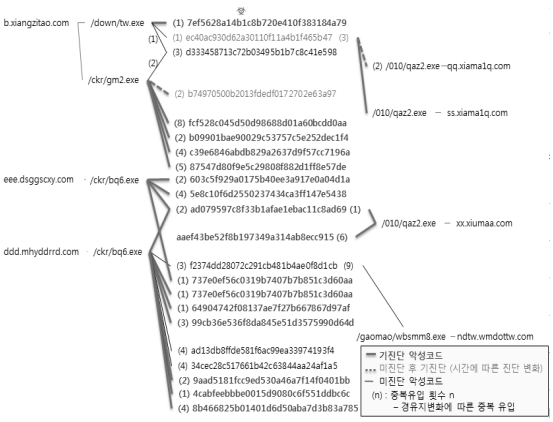
〔그림 17〕 즉각적인 실시간 협력 대응 사례

많아질수록 유입 차단율은 상승한다. 또한 새롭게 기진단되는 악성코드의 중복 유입량이 많을 수록 유입 차단율은 상승한다.



〔그림 18〕 동일 악성코드와 유포지 도메인들의 연관 사례

아래 〔그림 19〕는 유입시간에 따른 유포지 및 악성코드의 변화, 그리고 중복 유입량을 쉽게 확인할 수 있도록 〔표 7〕의 실험데이터의 일부를 표현한 것이다.



〔그림 19〕 시간에 따른 유포지 · 악성코드 변화

공격자는 체계적인 악성코드 유포 환경을 갖추고 있으며, 이를 통해 유포지 및 악성코드를 반복 사용하고, 일정 시간 후에는 또다른 정보로 변경시키며 지속적으로 악성코드 유포 공격을 전개하고 있음을 파악할 수 있다.

본 실험을 통해 제안된 보안 이벤트 공유를 통한 실시간 협력 대응 기술의 적용으로 새로운 보안 위협에 대한 신속한 대응이 가능하며, 보안 솔루션의 진단율 향상 및 보안 대응 체계의 대응력을 강화시킬 수 있음을 확인할 수 있었다. 공유된 보안 이벤트 내의 악성코드 유포지 정보를 통해 새로운 악성코드 및 악성코드 유포지를 진단 추가함으로써 개선된 효과를 볼 수 있었고, 악성코드 및 유포지 실시간 대응을 함께 적용할 경우 보다 큰 개선 효과를 얻게 되었다.

V. 결 론

단순히 보안 솔루션들의 기능을 묶어 서비스하는 기존의 단순 조합 구성 형태의 기존의 연동 서비스 방식에서는 지능화된 보안 위협 공격 - 백신 차단 우회를 위해 신종·변형 악성코드 생성 후 단기간 활용, 유해사이트 차단 우회를 위해 새로운 도메인 생성 후 단기간 활용 등의 반복적인 공격 패턴 사용 - 에 대해 효과적인 대응이 어려움을 확인할 수 있었다.

본 논문을 통해 제안된 실시간 협력 대응 기술은 보안 솔루션 상호 간의 보안 이벤트를 지속적으로 공유를 통해 상호 간의 진단률 향상을 도와 악성코드 유입 차단율이 기존 단순 연동 방식에 비해 개선됨을 입증함으로써 실시간 협력 대응의 신속한 조기 대응 및 사전 예방 효과를 확인할 수 있었다. 또한, 제안한 기술의 실제 활용도를 높이기 위해 시장에서 오랫동안 검증된 오픈 소스를 중심으로 구현하였고, 특히 연동 기능이 뛰어난 무료 웹 프락시 서버인 Squid의 사용과, 사용자 정의 패턴을 직접적으로 반영할 수 있는 무료 유해사이트차단 솔루션인 squidGuard와 무료 백신 솔루션인 clamAV를 사용함으로써, 보안 위협에 스스로 적극적으로 대응할 수 있는 구현 모델을 제시하였다.

향후 다양한 보안 솔루션 간 상호 연동에 대한 추가 연구를 통해 시스템, 네트워크 전방위적 실시간 협력 대응 체계의 모범이 될 수 있도록 지속적인 연구를 진행해 나갈 것이다.

참고문헌

〔1〕 행정안정부, “2011 국가정보화백서,” pp. 47, 2011년 8월

〔2〕 Timothy Vismor, ″Mail Server Implementation,“ pp. 11, June. 2011.

〔3〕 amavisd-new, “High-performance interface between mailer (MTA) and content checkers: virus scanners, and/or SpamAssassin,” http://www.ijs.si/software/amavisd/

〔4〕 Artica Open Source Project, ″What filters can be added in order to scan contents,″ http://www.artica.fr/index.php/artica-a-system/56-web-filtering/146-what-filters-can-be-added-in-order-to-scan-contents, April. 2009.

〔5〕 Squid, "Caching proxy for the Web supporting HTTP, HTTPS, FTP, and more," http://www.squid-cache.org/
〔6〕 J. Elson and A. Cerpa, "Internet Content Adaptation Protocol (ICAP)," RFC 3507, April 2003.
〔7〕 ClamAV, "Open source (GPL) antivirus engine designed for detecting Trojans, viruses, malware and other malicious threats," http://www.clamav.net/
〔8〕 squidGuard, "URL redirector used to use blacklists with the proxysoftware Squid," http://www.squidguard.org/
〔9〕 ClamAV-Server(daemon), http://www.clamav.net/
〔10〕 SquidClamav, "Antivirus for Squid Proxy based on the Awards winnings ClamAV anti-virus toolkit," http://squidclamav.darold.net/index.html
〔11〕 C-ICAP, "Implementation of an ICAP server," http://c-icap.sourceforge.net/

〈著者紹介〉

김 지 훈 (JiHoon Kim) 정회원
2000년 2월: 충남대학교 정보통신공학과 졸업
2000년 3월~2004년 10월: PSINet Korea 및 아이네트호스팅 재직
2004년 10월~현재: 안랩 시큐리티대응센터(ASEC) 분석2팀장
2007년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 네트워크 보안, 개인정보보호, 디지털포렌식, 융합기술보안 등

임 종 인 (Jong In Im) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 2월~2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌식