情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

사이버 위협 사전인지를 위한 위협 정량화 기술

김 기 영*, 임 선 희**, 김 종 현***

요 약

최근 고도의 지능적인 대량 공격이 지속적으로 발생하고 있으며, 다형성 악성코드 공격 증가로 인하여 개인과 기업 및 국가 기반시설까지 사이버위협에 노출되고 있다. 현재, 국가차원의 대응센터에서는 이러한 위협 대응을 위해 공격 위험도를 CVSS(Common Vulnerability Scoring System) 취약점 등급시스템으로 점수화하여 단계적으로 경보를 발령한다. 하지만 현재의 경보발령 체계가 공격이 이루어진 후 사후 대책으로 제공되고 있어, 공격발생 전에 공격 징후를 포착하거나 공격량 예측과 같은 전역 네트워크 차원의 위협에 대한 대응 기술은 미비하다.

본 논문에서는 최근 봇넷 기반의 공격들이 많아지고 있는 상황에서 봇넷을 네트워크 위협 전조증상으로 정의하고, NCSC(National Cyber Security Center), KrCERT와 같은 국가기관의 경보등급 산정체계를 기반으로 전역차원의 예·경보 발령 및 공격량 예측 시스템에 대해 연구한다.

Ⅰ. 서 론

최근 급증하는 사이버 위협으로 인한 피해가 다양한 분야로 확산되고, 공격발생 후 피해규모 파악의 어려움 뿐만 아니라 2차 연계 공격 및 지연된 대응에 따른 추가적인 피해발생이 더욱더 심각한 문제로 대두되고 있다[1,2,3].

각 정보보호 관련 기관에서는 사이버 위협의 실시간 대응을 위하여 개별 네트워크 및 독립된 기관 차원이 아닌 협력대응기반의 기술을 제공하고 있으며, 각 기관 자체적인 고유 사이버 위협 예·경보 체계를 제공하고 있다[4, 5, 6]. 사이버 위협에 체계적으로 대응하기 위하여 공격에 대한 위협 또는 제공서비스 전체의 위험수준을 평가하고, 단계적인 경보 발령이 요구된다. 위험도 등급, 공격량 산정, 각 기관별 경보 수준을 기반으로 사이버위협에 효과적으로 대처함으로써 위협을 조기에 차단하고 공격발생의 확산을 최소화 하고 공격 위협요인 도출이 가능하다.

이러한 대응 방법은 공격이 발생 후에 사후 대처 방안으로 보다 효과적인 대응을 위해 공격발생 전 공격 징후를 포착하거나 공격 발생을 예상, 공격량을 예측 기술이 필요하다. 하지만, 전역 네트워크 차원의 위협에 대한 예측 기술을 통해 사전에 위협에 대한 대응기술은 현재 미비한 상태이다.

본 논문에서는 사이버 위협의 사전 인지를 위해 기존의 봇넷 연구들을 기반으로 도출된 공격의 위협요인을 특징화하여 기존 예·경보 발령체계를 기반으로 전역차원의 보안 모니터링 기술에 대해 연구한다. 이러한 연구는 공격 발생전에 사이버위협에 대한 전조증상들을 분석하고 예상되는 공격량을 측정함으로써 보다 효과적으로 대처할 수 있다.

Ⅱ. 관련연구

2.1. 국내 예·경보 발령 체계

현재 국내에서 자체적으로 예·경보 발령체계를 갖는 기관은 국가·공공분야의 국가정보원, 민간분야의 인터

본 연구는 방송통신위원회 정보보호 원천기술개발 사업의 일환으로 수행하였음. [2012/10912-06002, 전역적 협력기반의 통합보안제어 시스템 개발]
* 한국전자통신연구원 사이버융합보안연구단 (kykim@etri.re.kr)
** 한국전자통신연구원 사이버융합보안연구단 (capsunny@etri.re.kr)
*** 한국전자통신연구원 사이버융합보안연구단 (jhk@etri.re.kr)

넷 침해대응사고 대응지원센터, 국방 분야의 국방정보전 대응센터 등이 있다. 또한, 안철수 및 하우리 등에서는 망 전역에 대한 예·경보 체계 제공이 어렵기 때문에 개별 위협에 대한 상세한 정보와 대응 솔루션을 제공하고 있다[4, 11, 12].

국가사이버안전센터의 경우 국가·공공기관이 사이버안전 및 정보보안 관련 업무를 전담하고 있으며 국가 전 분야에 걸쳐 사이버위협요소 평가를 진행하고 있다. 사이버 공격의 파급영향, 피해규모 등을 고려하여 심각, 경계, 주의 및 관심 등의 4단계 경보를 발령하고 있다[4, 11].

인터넷침해사고 대응지원센터(KrCERT)의 경우 인터넷 침해사고의 조기탐지, 분석, 예·경보 전파를 통해 피해확산방지와 상시적인 정보공유를 위한 민간부문 침해사고 대응지원센터로 역시 4개 등급 기준 발령기준을 제시하고 있다. 국방정보전대응 센터의 경우 체계 및 존재 여부가 비공개로 진행되고 있다[4,12].

그림 1은 국가 사이버 안전에 관한 국가적 조직체계의 확립을 목적으로 제정된 '국가 사이버 안전 관리규정' 체계를 나타낸다. 그림 2는 국가사이버안전센터의 경보 5단계를 나타낸다[4].

국외의 발령체계의 경우도 국내와 유사하다. 시만택에서는 Critical/Warning/Managed/Locked/Unmanaged 등급을 제공하고. 트래드마이크로는 Server/High/Elevated/Normal 보안등급으로 제공한다.

각 기관에서 제공하고 있는 사이버위협 경보체계는 발생된 공격에 대하여 보안이벤트 정보를 통합하여 대략 5단계(정상/관심/주의/경계/심각)로 분류하고 관리자에게 보안수준 보고 및 대응을 제공하도록 하고 있다.

〔그림 1〕 국가 사이버 안전관리체계

〔그림 2〕 국가사이버안전센터 사이버위협 경보 5단계

2.2. 네트워크 위협 대응기술 현황 및 한계점

다양한 사이버 공격 및 위협에 대해서 기존 IDS(Intrusion Detection System), IPS(Intrusion Protection System), ESM(Enterprise Security Management) 및 TMS(Threat Management System)/RMS와(Risk Management System) 같은 네트워크 보안시스템이 네트워크 위협대응을 위한 보안 시스템으로 적용되어 왔다.

하지만, 취약성을 공격하는 exploit 코드 발생 시간에 비해 해당 취약성공격에 대한 탐지 시그니처 생성 및 배포, 적용시간이 길어짐에 따라 제로데이 공격 위험에 노출될 가능성이 점점 더 높아지고 있다[8]. 뿐만 아니라 지금까지 이들 대부분이 이미 공격이 진행된 후 탐지된 보안이벤트 정보를 기반으로 공격확산을 차단하는데 중점을 두고 있어 이미 발생한 공격의 확산을 개별 ISP 및 기관, 보안시스템에서 탐지하여 각 기관 관리자에게 수동적 차단을 제공하기에는 많은 비용과 시간이 할애되어야 하고, 급속한 공격의 확산차단에는 한계를 보이고 있다.

2.3. 기존 사이버 위협 예·경보 기술

지금까지 네트워크 공격 발생 전 위협 예측 기술로는 패킷단위로 측정된 트래픽 특성을 분석하여, 시계열 모형 적용 및 마코브 체인 모델 적용을 통한 예측 모델이 주를 이루었다. 특히, 트래픽 양 및 분포를 측정하여 이상트래픽을 탐지하여 예측하는 것이 대다수이다.

하지만, 공격을 예측하기 위하여 위협요인 추출을 위

한 패킷의 특징들을 기반으로 연관성을 정의하기는 어렵다. DDoS(Distributed Denial of Service) 공격을 예측하기 위한 네트워크 트래픽 볼륨 기반으로 베이지안 추론이론 적용 기술도 연구되었으나, 공격의 시작 기준 정의 등에 대한 문제점 등이 있다[9, 10].

Ⅲ. 네트워크 위협 사전인지를 위한 정량화

본 장에서는 네트워크 위협 대응기술의 한계점을 극복하기 위하여 공격 발생 전 사전인지를 위한 위협 정량화에 대해 연구한다.

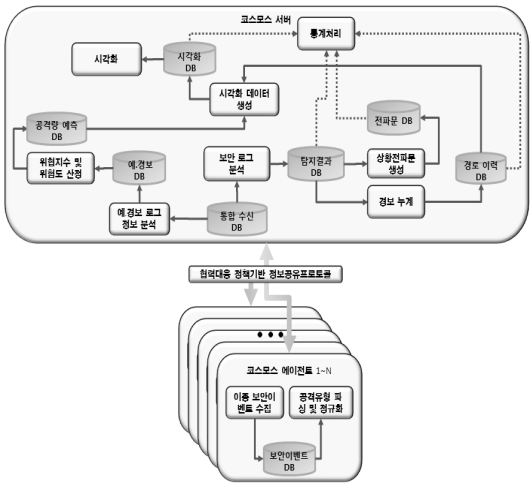
본 논문에서는 사이버 위협의 전조증상으로 최근 지능적이고 대량의 공격의 수단으로 많이 사용되고 있는 봇넷(Botnet)을 기반으로 한다.

봇넷은 악성코드 봇(Bot)에 감염된 다수의 컴퓨터들이 네트워크로 연결되어 있는 형태로서 실제 감염된 봇들에게 공격 명령을 내리는 봇마스터(Bot Master), 명령 및 제어 메시지를 전달하는 C&C 서버, 악성코드 봇(Bot)에 감염되어 공격자로부터 제어를 받는 좀비(Zombie)PC들로 구성된다. C&C서버와 좀비PC들은 명령 및 제어 메시지를 송수신하기 위해 연결을 시도하는데, 기존의 방법인 봇 프로그램에 하드코딩된 IP주소를 할당하는 방식이 탐지가 용이함에 따라 도메인주소를 할당하여 DNS(Domain Name System) 서비스를 이용한 봇넷들로 진화하고 있다[16].

본 논문에서는 좀비PC가 질의하는 DNS 트래픽을 분석하여 탐지된 의심 도메인의 IP 및 의심 도메인에 접속하는 좀비PC들의 접속행위를 통해 위험도를 산정하고 공격량에 대해 예측한다.

3.1. 협력대응정책기반 통합보안제어 프레임워크 (COSMOS 시스템)

통합보안제어 프레임워크(COoperative Security MOnitoring System, COSMOS)는 통합보안제어 서버, 다수의 에이전트(1~n) 및 서버와 에이전트 간 정보전달을 위한 보안정보 공유프로토콜로 구성된다. 그림 3과 같이 통합보안제어 서버는 다수의 에이전트로부터 수집된 이종보안로그 정보, 의심도메인/IP/접속리스트/추적로그, 이벤트 분석, 경보계산, 통계처리 및 네트워크 위협 사전 인지를 위한 예·경보 기능을 제공한다. 다수의



〔그림 3〕 협력대응기반 통합보안제어 프레임워크 구성

에이전트는 각 ISP에서 제공되는 이종보안장비의 정보를 실시간으로 수집하여 표준포맷으로 정규화 및 축약 기능을 제공한다. 특히, 기존의 상용제품에서의 수집기능은 초당 2천건~7천건 정도인데 반해, COSMOS 에이전트 시스템은 이종보안 이벤트 수집을 1만건 이상으로 처리한다. 보안정보 공유프로토콜은 IETF의 표준화 그룹에서 정의하고 있는 IDMEF(Intrusion Detection Message Exchange Format), IODEF(Incident Object Description Exchange Format) 및 RID(Real-time Inter_network Defense) 프로토콜 표준을 적용한다[13, 14, 15]. 표준프로토콜을 기반으로 이종보안이벤트 정보가 손실 없이 실시간으로 전달한다.

특히, 서버에서 발령된 예·경보 및 공격상황 정보가 대상 네트워크에 20분 이내 동기화 되도록 자동대응 메커니즘을 제공한다.

3.2. COSMOS 경보체계

사이버 위협 경보 체계는 사이버 공격 발생이 예상되는 경우에 그 위협 또는 위험의 수준을 평가하여 단계적으로 경보를 발령하여 사이버 안전을 확보하고자하는 일련의 체계 또는 시스템으로 정의되어 있다. KISC(Korea Internet Safety Commission)에서는 전체 위험도를 공격자체 위험도, 사고현황, 피해확산 가능성, 피해기관 중요도, 피해시스템 중요도, 트래픽 이상 유·무, 피해복구 난이도 등으로 분류한다. 분류된 각 항목마다 자체 기준점수를 할당하고, 해당 이벤트가 발생한

공격상황의 심각도에 따라 점수를 할당한다.

전역차원의 통합보안제어를 위하여 COSMOS 시스템에서의 경보체계는 구축된 보안 시스템들의 이벤트정보가 제공하는 개별 공격에 대한 위험도 값을 해당 장비제공위치 및 접속점으로 분류하여 균등하게 4개구간으로 할당한다. 또한, 1일 동안 발생한 이벤트 빈도를 균등하게 4개구간으로 분배하여 사고현황 값을 할당한다. 피해기관 중요도 및 피해시스템 중요도 역시 주요 ISP의 공격피해 여부, 주요 네트워크 장비 및 서버 장비, 혹은 개인 이용자의 공격 여부에 따라 4개의 구간으로 분할하여 점수를 할당한다. 그 외 BPS/PPS 증가율을 산정하여 점수를 배정하고, 서비스 중단 필요성 유·무에 따라 난이도 점수까지 할당한다.

본 시스템은 실제 운영 시에 참조 값을 관리자가 임의적으로 할당가능하며, 기본적으로 제공된 최소구간의 공격과 최대구간의 공격 위험도, 횟수, 중요도를 균등하게 분할하여 기본 설정 값으로 제공하도록 한다.

그림 4는 통합보안제어 시스템 경보체계에서 위험도 산정을 위해 공격상황에 맞게 분류하고, 분류된 항목마다 위험도에 따른 점수를 할당한 예이다.

마지막으로 각 공격 당 발생한 보안 이벤트 분류 항목 당 할당 점수를 합산하여 100점 만점 기준으로 위험도를 산정한다.

구분	배점	평가항목	세부배점
공격 위협도	30	AID : 21 ~ 24 (DDoS 대응장비 #1 App. 공격 : GetFlooding~In-CompleteGet)	30
		AID : 13 ~ 18 ISP #1(CPFINFlooding~Bandwidth)	25
		AID : 0 ~ 12 (DDoS 대응장비 #1 Net. 공격 : TCP SYN Flooding~TCP Flooding)	20
		AID : 24이상(Unknown Attack)	15
사고현황(1일 보안이벤트발생빈도)	20	300회~	20
		100회~300회	15
		11회~100회	10
		1회~10회	5
피해기관 중요도	10	주요 ISP, IDC, 주요정보통신기반시설 등	10
		중소규모 ISP(SO, RO 등) 또는 IDC 등	7
		주요 기관(관공서, 금융기관, 포털사이트 등)	5
		일반 기업, 대학, 일반기관 등	3
		개인 이용자(인터넷사용자), PC방 등	2
피해시스템 중요도	10	네트워크 장비(AR, DR, BR 등)	10
		중요 서버 장비(DNS, 메일, 전자거래, DB, 주요기관 웹서버 등)	7
		주요기관 업무용 또는 금융거래 PC 등(중요자료 노출 가능)	5
		개인용 또는 일반 서버 장비(웹서버, 호스팅서버 등)	2
		개인용 PC	1
트래픽 이상유무	20	BPS 증가율 30~50%(10)	10
		BPS 증가율 50%이상(20)	20
		PPS 증가율 : 30~50%(3), 50~100%(7), 100~150%(10)	3/5/7/10/
		PPS 증가율 : 150~200%(15), 200%이상(20)	15/20
피해 복구 난이도	10	서비스 중단 필요	10
		서비스 중단 필요 없음	1
총계	100		

〔그림 4〕 통합보안제어 경보 체계 할당(예)

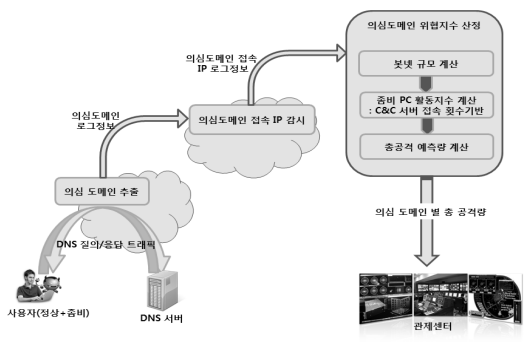
대부분의 위험도 산정시 기준으로 제시했던 기본점수를 기반으로 5단계로 분류하며, 표 1과 같이 합산 위험도점수에 따라 정상, 관심, 주의, 경계 및 심각으로 할당한다

3.3. 네트워크 위협 사전인지 및 분석기술

기존의 네트워크 위협 기술은 네트워크에서 발생한 트래픽 양 및 여러 ISP에서 제공되는 네트워크 보안 장비의 이벤트 로그양 등을 기준으로 통계적인 기법으로 공격 발생 후 대응하는 기술들이 대부분이다.

하지만, 주기적으로 접속하는 행위탐지, 트래픽 볼륨 및 이벤트 로그양의 변화로만 가지고 실제 공격 가능성에 대한 예측은 개연성이 모호할 뿐 아니라 사후 처리 방식을 기반으로 하여 예측기술로는 한계를 가지고 있다.

본 논문에서는 네트워크 위협 사전인지를 위해 전역 네트워크 차원의 C&C 서버 탐지 및 모니터링으로 감염된 좀비 PC 규모를 예측하고, 좀비 PC와 C&C 서버 간의 트래픽을 모니터링하여 좀비 PC 활동성을 통해 공격 규모 및 자산 손실에 대한 예측을 제공하는 기술에 대해 연구한다. 그림 5는 DNS트래픽 분석을 통해 탐지된 C&C 서버와, 이를 접속하는 좀비 IP를 모니터링한 후 통합보안제어 서버 시스템으로 관련 정보를 전달하는 과정을 나타낸다.



〔그림 5〕 DNS트래픽 분석기반 의심도메인 및 좀비 활동성 분석을 통한 위협지수 선정

〔표 1〕 통합보안제어 위험도 산정 등급

경보	정상	관심	주의	경계	심각
위험도 점수	50점 이하	51~60	71~8	81~90	90이상

의심도메인 위협지수 산정을 위하여 DNS트래픽 분석을 통해 의심 도메인 즉 C&C 서버 탐지 기술[16] 및 탐지된 C&C 서버를 국제관문국 네트워크 IX(International eXchange) 구간의 모니터링 정보가 통합보안제어 서버 시스템으로 제공되어야한다.

3.4. 네트워크 위협 사전인지 및 공격량 예측

본 논문에서는 탐지된 도메인 별 예상 공격량 산정을 위하여 네트워크 위협 요소를 아래와 같이 3개의 항목으로 정의한다.

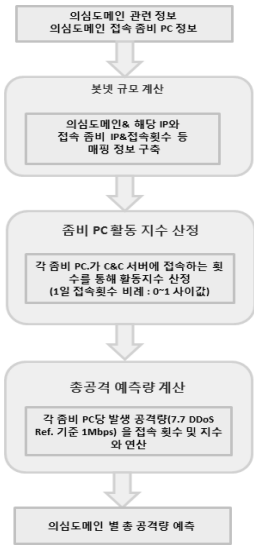
- 의심 도메인 별 위협등급 : 봇넷 규모 계산에 의하여 등급이 산정되며, 1일 기준으로 5단계로 균등하게 등급을 부여한다. 단 예외 상황 발생 시 관리자가 임의로 변경 및 재 할당 가능하다.
- 좀비 PC활동지수 : 좀비 PC 활동 지수를 좀비 PC가 C&C 서버에 접속하는 횟수로 산정한다. 즉, 좀비 PC가 C&C 서버에 접속하는 횟수로 활동지수가 산정되며 1일 기준으로 5단계로 균등하게 등급을 부여한다. 단 예외 상황 발생 시 관리자가 임의로 변경 및 재 할당 가능하다.
- 좀비 PC 당 위협별 공격규모 : 좀비 PC 분석정보 기반 발생 공격량을 할당한다. 기존 발생 공격을 참조하여 할당한다.

도메인 별 예상 공격량 산정을 위하여 정의된 위협요소를 다음과 같이 정의한다.

*도메인 별 예상 공격량 = 의심 도메인 별 위협등급 * 좀비 PC 활동 지수 * 좀비 PC 당 위협별 공격 규모*

공격량 산정은 그림 6에서 기술한 프로세스대로 제공된다.

예를 들어, A.com, B.com, C.com 이라는 3개의 의심도메인이 탐지되었을 때, A.com의 좀비 PC 공격건수가 10,000개, B.com의 좀비 PC의 공격건수가 5,000개, 그리고 C.com가 10,000개의 경우, 위협등급은 가장 많은 좀비 PC를 공격건수를 갖는 A.com과 C.com을 기준으로 가장 위협한 등급으로 산정되고, B.com이 두번째 위협한 등급으로 산정된다. 좀비 PC 활동지수의 경우, 각 좀비 PC가 C&C 서버에 접속하는 횟수를 1일



〔그림 6〕 의심도메인별 공격량 예측 및 총공격량 예측 프로세스

기준으로 균등하게 분할하여 0에서부터 1까지 0.2, 0.4, 0.6, 0.8, 1 이렇게 5단계 값으로 할당한다. A.com이 가장 많이 접속했으며, 1일 15회 접속했다면 활동지수 1, B.com이 6회 접속했다면 활동 지수값은 0.6이 된다. A.com 도메인의 예상 공격량을 예측하기 위하여 최소 공격량을 기준으로 위의 등급에 따라 산정해보면, 10,000(공격건수)*1.0(활동지수)*1Mbps(좀비PC당 예측 공격량 : 최소 1Mbps, 최대 10Mbps)로 10Gbps의 공격량을 예측할 수 있다. A.com이 10Gbps공격량을 예측하고, B.com이 3Gbp를 C.com이 2Gbps의 공격량을 예측한다면 총 공격 예측량 예측이 가능하다. 여기에서 최소공격량 예측은 10Gbps이지만, 최대공격량을 기준으로 한다면 100Gbps까지 예측할 수 있어서, 공격량 예측시 10~100Gbps까지 범위로 예보발령이 가능하다.

여기에서 탐지된 임의의 의심도메인에 대하여 수십 Gbps의 공격이 예측된다는 발령을 그림 6과 같은 과정을 통하여 해당 네트워크에 전파할 수 있게 된다. 공격량 예측 발령은 기존 상황전파문의 형식을 따른다.

Ⅴ. 결 론

지금까지 사이버테러 대응을 위한 NCSC 및 KrCERT와 같은 국가기관 중심의 대응체계 및 위험도 산정 등에 대해 알아보고, 기존 기술의 한계를 극복하기

위한 방안으로 전역 네트워크 차원의 통합보안제어 시스템 대응체계 및 위험도 산정, 공격량 예측 기술에 대해 연구하였다.

네트워크 위협 사전인지 정보 정량화 정보추출을 위한 의심도메인 탐지 엔진 구현을 위하여 1,000여개의 시스템으로 구성된 중규모 네트워크에서 최신 봇넷을 감염시켜, 이를 수집 및 분석하였다. 또한, 실 ISP의 트래픽을 적용하여 전역 네트워크 차원의 통합보안제어 시스템에서의 위협 사전 인지 기술을 검증하였다.

향후 상용제품으로 제공되려면 단기간의 적용가능성 검증을 위한 데이터 뿐 아니라 장기간의 ISP 실 데이터 적용 및 검증 과정이 필요하다.

참고문헌

[1] IDG Tech Report, “은밀하고 끈질긴 위협 APT의 이해”, 2011년 12월.

[2] 잉카인터넷 대응팀 http://erteam.nprotect.com/251,

[3] 시만텍, 인터넷 보안 위협 보고서 제17회, 2012년

[4] KISA 안내.해설 제2010-13호, 침해사고대응팀(CERT) 구축/운영 안내서. 2010년 1월.

[5] 2012년 국가 정보보호백서

[6] 최석우, “블랙리스트 접근 트래픽 감시를 통한 봇 탐지 방법‘, KNOM Review, Vol. 13, No. 1

[7] 기동진, 조성제, IIS, 제1권 제2호 2010년 11월 pp.130-147, 국가 DB 기반의 국내외 보안 취약점 관리체계 분석

[8] 정일안, 오진태, 장종수, “보안 정보 공유 기술 및 표준화 동향,” 전자통신동향분석, 23권 4호, pp. 30-38, Aug. 2008.

[9] R. Villamarín-Salomón,J. C. Brustoloni, “Bayesian bot detection based on DNS traffic similarity”, in Proceedings of the 2009 ACM symposium on Applied Computing, 2009, pp. 2035–2041.

[10] L. Bilge, E. Kirda, C. Kruegel,M. Balduzzi, “EXPOSURE: Finding malicious domains using passive dns analysis”,Proceedings of the Annual Network and Distributed System Security. 2011년 2월

[11] 국가사이버안전센터, http://www.ncsc.go.kr/

[12] 인터넷침해대응센터, http://www.krcert.or.kr/

[13] H. Debar, D. Curry and B. Feinstein, “The Intrusion Detection Message Exchange Format (IDMEF)”, IETF, RFC 4765, March 2007.

[14] R. Danyliw, J. Meijer, Y. Demchenko, “The-Incident Object Description Exchange Format,”IETF, RFC 5070, Dec. 2007.

[15] K. M. Moriarty, “Real-time Inter-network Defense,” IETF, RFC 6045, Nov. 2010.

[16] S.H Kim, J. Cho, J.H Kim, B.G Lee, Feature Seclection with PCA based DNS Query for Malicious Domain Classification“, Proceedings of the KIPS, Vol. 1, No. 1, pp 55-60, Oct. 2012.

〈著者紹介〉

김 기 영 (Kiyoung Kim)

1988년 : 전남대학교 전산 통계학과(학사)

1993년 : 전남대학교 전산통계학과(석사)

2002년 : 충북대학교 전자계산학과(박사)

1988년 2월~현재 : 한국전자통신연구원 융합보안연구팀 책임연구원

<관심분야> 네트워크보안, 임베디드 보안 OS 및 모바일 보안기술 등

임 선 희 (Sun-Hee Lim)

1999년 2월 고려대학교 컴퓨터학과 학사

2005년 2월 고려대학교 대학원 정보보호학과 공학석사

2010년 8월: 고려대학교 대학원 정보보호학과 공학박사

2010년~현재: 한국전자통신연구원 선임연구원

<관심분야> 무선이동통신보안, 정보보호, 사이버보안, 융합보안기술

김 종 현 (Jong-Hyun Kim)

2000년 오클라호마주립대 컴퓨터학과공학석사

2005년 오클라호마주립대 컴퓨터학과공학박사

2005년~현재 한국전자통신연구원 선임연구원

<관심분야> 정보보호, 사이버보안, 역추적기술