Journal of Digital Contents Society Vol. 11 No. 1 Mar. 2010(pp. 79-89)

DDoS 대응 지표 프레임워크 개발

이연호*, 김범재**, 이남용***, 김종배****

요 약

날로 지능화되고 고도화되어가는 DDoS 공격과 같이 증가하는 사이버 위협으로부터 자산을 보호하기 위해서 정부와 기업들은 서둘러 DDoS 대응 시스템을 구축하고 있다. 그러나 아직까지도 정보보호 시스템은 지난 2009년 7월7일에 발생한 7.7 DDoS 공격과 같은 사회적 사건의 발생이나, 직접적인 피해의 사례가 발생하였을 때에만 단기적으로 이슈가 될 뿐, 이를 위한 지속적인 투자에는 여전히 소극적이라는 것이 일반적인 인식이다.

이는 정보보호 시스템의 특성상 사건이 발생하기 전에는 그 효과를 인식하기 어렵고, 사건이 발생한 경우에는 침해 또는 방어라는 결과에 대한 이분법적인 방식의 성패 판단만 있을 뿐, 이것의 효과와 효율에 대한 상세하고 객관적인 측정의 기준이 없기 때문이다. 비록 최근에는 정보보호관리체계에 대한 평가나 인증 작업이 진행 중이나, 이는 정보보호관리시스템에 대한 일반적인 지침이나 기준만을 제시하고 있어, 그 결과로는 조직의 정보보호관리체계 개선이나 향상이 쉽지 않다는 문제가 있다.

따라서 본 논문에서는 DDoS 대응 체계에 대한 상세하고 객관적인 측정이 가능하도록, 대응 전략 및 프로세스별로 주요 지표들을 개발하기 위한 프레임워크를 제시한다.

The framework to develop main criteria for a DDoS correspondence

Yeon-ho Lee*, Beom-Jae Kim**, Nam-Yong Lee***, Jong-Bae Kim****

Abstract

The government and companies build a DDoS correspondence system hastily to protect assets from cyber threats. It has become more and more intelligent and advanced such as DDoS attack. However, when outbreaks of the social incidents such as 7.7 DDoS attack(2009.7.7) or cases of the direct damage occurred, information security systems(ISS) only become the issue in the short term. As usual, sustained investment about ISS is a negative recognition.

Since the characteristic of ISS is hard to recognize the effectiveness of them before incidents occurs. Also, results of incidents occurred classify attack and detection. Detailed and objective measurement criterion to measure effectiveness and efficiency of ISS is not existed. Recently, it is progress that evaluation and certification about for the information security management system(ISMS). Since these works propose only a general guideline, it is difficult to utilize as a result of ISMS improvement for organization.

Therefore, this paper proposes a framework to develop main criteria by a correspondence strategy and process. It is able to detailed and objective measurements.

Keywords : DDoS, Information Security System, Correspondence Strategy, Framework

1. 서론

최근 들어 서비스공격(Denial of Service, 이하 DoS)이나 분산서비스공격(Distributed Denial of Service, 이하 DDoS)이 날로 증가하고 있다. 지난 2009년 7월 7일 한국과 미국의 정부기관, 금융기관, 인터넷서비스 업체 등 약 46개 사이트를 대상으로 이뤄진 DDoS 공격은 한동안 우리 기억 속에 잊혀진 인터넷 보안의 중요성을 다시 일깨워주는 계기가 된 큰 사건이라고 할 수 있

※ 제일저자(First Author) : 이연호
접수일:2010년 02월 16일, 완료일:2010년 03월 31일
* 숭실대학교 대학원 컴퓨터학과 박사과정
bren1199@naver.com
** 숭실대학교 대학원 컴퓨터학과 박사과정
*** 숭실대학교 컴퓨터학부 교수
**** (주)이엔터프라이즈 (교신저자)
▣ 본 논문은 숭실대학교 교내연구비 지원으로 수행됨

다. 더욱 심각한 것은 이러한 DDoS 공격의 기법이 갈수록 진화하고 고도화되고 있다는 점이다[2].

정부와 기업들은 이번 피해를 계기로 다시 한번 보안 인프라 확충의 필요성을 느꼈으며 양적인 발전보다는 질적인 발전을 위해 정부 차원의 관련 정책 수정 및 마련, IT 서비스 업체에 대한 지원 등으로 보안 인프라 후진국이라는 불명예를 씻어내기 위해 다각적인 노력을 기울이고 있다. 7.7대란이후 정부는 예산을 대폭 증액하여 “해킹 바이러스대응 고도화”라는 큰 주제 하에 범정부 DDoS 대응체계구축사업을 각 부처별로 발주하여 추진하고 있으며, 정보보호업무에 장비와 소프트웨어 도입 등의 노력을 기하고 있다. 또한, ISP 등 민간 기업들도 방송통신위원회/한국인터넷진흥원(KISA)[8]의 지휘 하에 대응체계를 점검하고 장비 및 솔루션, 인력 등을 보강하며 이전에 비해 많은 노력을 기울이는 것은 주지의 사실이다.

그러나 아직까지도 정보보호 시스템은 사회적 사건의 발생이나, 해당 조직에 대한 직접적인 피해의 사례가 발생하였을 때에만 단기적으로 이슈가 될 뿐, 이를 위한 지속적인 투자에는 여전히 소극적이라는 것이 일반적인 인식이다. 이는 정보보호 시스템의 특성상 사건이 발생하기 전에는 그 효과를 인식하기 어렵고, 사건이 발생한 경우에는 침해 또는 방어라는 결과에 대한 이분법적인 방식의 성패 판단만 있을 뿐, 이것의 효과와 효율에 대한 상세하고 객관적인 측정의 기준이 없기 때문이다.

비록 최근에는 정보보호관리체계에 대한 평가나 인증 작업이 진행 중이나, 이는 정보보호관리시스템에 대한 일반적인 지침이나 기준만을 제시하고 있어, 이를 통해 정부기관이나 기업의 DDoS 대응 체계가 어느 정도의 수준으로 구축되어 관리되어지는지, 또 대응 체계의 구축이 침해 대응에 얼마나 효과적인지 그 성과를 정량적으로 측정할 수 있는 지표로 활용하기는 어려운 실정이다.

따라서 DDoS 대응 체계에 대한 상세하고 객관적인 측정의 지표가 요구되나, 이러한 지표들은 DDoS 대응 전략 및 절차를 비롯한 종합적인 대응 체계의 수립을 전제로 하고 있고, 개별 조직의 전반적인 분석을 통해 최종적으로 선정되어져야 한다. 또한, 지표는 현재의 상태에 대한 측정이 목적이 아니라, 궁극적으로는 그 결과를 통해 조직 조직의 정보보호관리체계 개선이나 향상을 위한 가이드라인으로서의 역할을 수행하여야 하기 때문에 다양한 사례의 분석을 통해 보다 일반화된 기준의 마련이 선행되어야 한다.

본 논문에서는 이러한 시도를 위한 첫 번째 과제로 각 조직들이 DDoS 대응 체계를 구축하는데 있어서 참조할 수 있는 대응 전략 및 프로세스 모델을 제시하고, 구축한 대응 체계의 수준과 성과 측정을 위한 지표 개발의 절차와 지침을 중심으로 한 프레임워크를 제시한다.

본 논문은 다음과 같이 구성되어 있다.

먼저 2장에서 DDoS의 공격 및 차단 기술을 살펴보고 정보보호관리체계 측정 및 평가를 위한 기존의 연구를 분석한다. 3장에서는 DDoS 대응 프로세스 및 지표 프레임워크를 제시하고, 4장 결론에서 이에 대한 간략한 평가 및 향후의 방향을 제시한다.

2. 관련연구

2.1. DDos의 공격 및 차단 기술

DDoS 공격은 ‘해커가 감염시킨 개인용 컴퓨터(PC) 또는 서버를 공격하여 특정 시스템의 자원을 고갈시킴으로써 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법‘으로 정의된다[3][10]. 이러한 DDoS 공격에 대응하기 위해서는 개개의 보안 기술 개발도 중요하지만, 최종적으로는 전체가 통합적으로 동작하여, 유기적인 대응을 수행할 수 있어야만 DDoS 공격을 효과적으로 차단할 수 있게 된다[2].

이러한 측면에서 공격 프로세스를 공격발생이전/공격간/공격발생이후의 3단계로 구분하고, 각 단계별 DDoS 대응 요구사항과 정보통신망 환경 전체를 고려한 DDoS 공격 대응기술의 요구사항을 정리하면 다음과 같다[1][9].

<표 1> DDoS 공격단계별 대응기술 요구사항

단계	구분	방안
공격 발생 이전 단계	공격 agent 개발단계대응	• 법안 개정을 통해 공격 agent 개발/배포 방지 노력
	공격 agent 전파 단계	• 동적 악성 프로그램 분석기술 개발 • 수집된 악성 프로그램 송수신 정보 공유를

	대응(네트워크상에서 송수신되는 실행파일들을 탐지/재구성/분석을 통한 공격 agent 여부 판단)	통한 국가 차원의 DDoS 조기 경보 체계 구축 • 실행파일들의 신뢰성 판단을 위한 객체 인증(Object Authentication) 기술 개발 • 사용자의 의도와 관계없이 설치 되는 실행파일 탐지, 보고, 제거기술 개발 • 취약한 웹사이트를 허니넷 내에 위치시켜 공격 agent를 수집
	공격 agent 제어단계대응	• 다양한 형태의 C&C 서버 접근 방식을 분석하고, 이를 탐지할 수 있는 기술을 개발 • 공격 agent가 어떤 접속규격에 의해 C&C 서버로 접근하는지를 분석하여 C&C 서버로 접근하는 연결 요청을 특정한 대응 시스템으로 유도하고, 해당 접속규격에 맞춰 공격 agent 자체를 제거하도록 명령을 내릴 수 있는 관련 기술을 개발
공격 발생 단계	백본 네트워크 레벨대응	• 백본 네트워크를 모니터링하고 공격의 징후를 탐지하기 위해 백본 네트워크상에서 송수신되는 모든 네트워크 트래픽을 수집하여 분석할 수 있는 DDoS 장비 개발
	Edge네트워크 레벨대응	• 응용 프로그램의 트래픽 특성 분석을 통한 응용 계층 DDoS 공격 탐지 기술 ● Edge 네트워크 레벨에서 좀비PC를 네트워크에서 분리시킬 수 있는 방안
	공격대상서버 레벨대응	• 네트워크 인터페이스 카드 내에 H/W로 구현되어, 자체 CPU를 이용한 공격 탐지 및 차단을 수행함으로써 서버의 성능 저하는 발생하지 않으면서 공격을 차단할 수 있는 기술 개발
	통합분석레벨 대응(공격발생 시 전역네트워크상에서 발생하는 다양한 보안이벤트들을 수집하여 통합분석,활용)	• DDoS 공격 관련 정보들을 수집하고, 이를 자동화된 방법으로 통합 분석하여 신속히 공격을 탐지, 정보를 전달하고, 좀비PC, 공격 agent 유포시스템, C&C서버 그리고 공격자의 위치를 추적할 수 있는 국가차원의 통합관제시스템을 법적 제도적 지원하에 정부기관에 의해 관리 운영
공격 발생 이후 단계	-	• 공격에 사용된 시스템들을 추출하여 해당 시스템에서 공격 agent를 제거하고, 취약점이 존재하는 경우, 이를 제거 • 수집된 공격 agent를 상세하게 분석하여, C&C 서버 및 공격 agent 유포지를 알아내어, 해당 서버 및 유포지로 접근을 시도하는 네트워크 트래픽에 대해 블랙홀 라우팅(Blackhole Routing) 혹은 싱크홀 라우팅(Sinkhole Routing) 등의 기법을 적용하여, 접근제어 및 공격 agent의 자동 삭제 • 시도된 공격의 핵심 특징을 추출하여 향후, 동일한 공격이 발생하는 경우에는 신속히 탐지 및 차단할 수 있는 시그니처를 생성하고 이를 배포

물론, 이러한 대응체계를 구현하기 위해서는 기술적인 문제뿐만 아니라, 법적 제도적 문제가 해결되어야 한다[5]. 이러한 대응체계에서는 다수의 서로 다른 관리망 내의 다양한 데이터들이 통합 DDoS공격 대응관제체계 하에 수집되어 동시에 분석되어져야 하는데, 이를 위해서는 다수의 관리망들이 동일한 인터페이스 또는 프로토콜을 이용하여 정보를 제공할 수 있어야 한다. 이를 위해서는 제공하는 정보의 형태 및 내용 등에 대한 규정과 실제 정보 전달을 위해 필요한 프로토콜의 표준화 등 법적/제도적으로 해당 정보들을 제공하도록 해야만 통합 대응이 가능해 지는 것이다[7].

2.2. 정보보호관리체계 측정 및 평가 방법

정보보호 평가 측면에서 기존 연구의 내용들은 크게 두 가지 접근방법에 의해 구분된다.

첫 번째는 TCSEC(Trusted Computer System Evaluation Criteria), ITSEC(Information Techn-ology Security Criteria) 등과 같이 제품이나 시스템의 보안 기능과 성능 측면을 중심으로 하는 평가 체계이다. 이러한 기존의 평가기준이 주로 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성 면에서 제약을 받고 있다[6].

두 번째는 BS7799[13][14]와 같이 관리적 측면을 중심으로 한 평가 체계이다. 특히, BS7799는 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다. 따라서 BS7799 표준은 지침과 권고안의 성격을 갖으며, 관리적 측면을 중심으로 한 평가 체계여서, 정보보호 관리를 위한 지침으로는 적합할 수 있지만 그 자체로서는 평가대상 조직의 정보보호관리체계 개선이나 향상이 쉽지 않다는 문제가 있다[4].

한편, 현재 정보보호관리 국제 표준인 ISO/IEC TR 13335 GMITS(Guidelines for the Management of IT Security)[15][16][17][18]에서는 정보보호관리 프로세스를 중심으로 14개의 절차를 제시하고 있다[6].

<표 2> 정보보호관리 프로세스

영역	프로세스
IT 보안목적, 전략과 정책	IT 보안목적과 전략
	조직의 IT 보안 정책
위험 분석	상위수준 위험분석
	상세 위험분석 계획수립 및 승인
	자산식별 및 가치 평가
	위협 평가

	취약성 평가
	위험 평가
IT 보안의 구현	보안대책의 구현
	보안인식제고 교육 및 훈련
	IT 시스템 승인
사후조치	보안 준거성 확인
	모니터링
	사고처리
	변화통제

정보보호관리를 위해서는 조직의 정보보호 관리체계의 구축과 더불어, 현재 작동중인 정보보호관리체계에 대한 정확하고 지속적인 측정 및 평가 작업이 필요하다. 이러한 측정과 평가 작업을 통해서 조직은 현재 자신의 정보보호관리체계 수준과 필요한 요구사항들을 파악할 수 있고, 이를 바탕으로 조직의 정보보호관리체계에 대한 지속적인 개선이 가능하다.

또, 중요한 정보자산을 보호하기 위한 정보보호관리체계방법론으로 현재 ISO 27001[12]이 국제표준으로 제정되어 가장 널리 사용 되고 있다. 이와 유사한 개념으로는 SP800-53[11], COBIT4.x[19] 등 국가와 조직별로 다양한 모델이 응용되어 사용되고 있다.

이상에서 살펴본 기존의 표준 및 모델들은 일반적이며 범용적인 특성을 가지고 있어, 표준을 적용하기 위한 구체적인 방법론과 분석방법을 제공하고 있지는 않다.

3. DDoS 대응 프로세스 및 지표 프레임워크

3.1. DDoS 대응 체계 모델

DDoS 공격 기술은 끊임없이 진화하고 있기 때문에 이에 대해서 기술적으로 완벽한 방어 방법을 제시하기는 어렵다. 결국 다양한 공격 위협에 대해서 신속하고 효과적으로 대응 할 수 있는 체계와 프로세스를 구비하고 변화하는 공격 유형에 대한 지속적인 학습을 통해 스스로를 진화시키는 노력이 필요하다. 이를 위해 두 가지 관점에서 대응체계를 구축해야 한다.

첫째, 공격자의 공격전략, 기법, 피해영향도 및 각 사이트 별 대응기법을 상세히 분석한 후, 현 문제점을 도출하여 사이트의 가용성을 확보할 수 있는 효과적인 대응체계를 구축해야 한다.

둘째, 장비중심의 일차원적 대응을 탈피하여, 정책, 대응기술, 용량증설이 조화를 이루는 전방위적 DDoS 방어 아키텍처 수립을 통해 지속적 대응체계를 구축해야 한다.

이러한 관점에서 DDoS 대응 전략을 수립하기 위한 절차와 항목을 정리하면 아래의 <표 3>과 같다.

<표 3> DDoS 대응 전략 수립 절차

단계	세부 절차 및 항목
비즈니스 요구사항 검토	• 비즈니스 연속성 측면에서의 요구사항 분석 • 주요 부서의 부서장 및 실무진 측면에서의 요구사항 분석
대응체계 범위 정의	• 사업 목표 및 업종 특성 등을 분석 • 요구사항을 반영하여 주요 방어 대상 정의
공격 유형 식별	• DDoS 공격 형태별 위협 피해 정도 식별
인프라 및 용량 분석	• 인프라 구성 및 장비 운영 현황 파악 • 방어 대상에 대한 가용성 측면에서의 현 용량 지표산정 및 측정
관리적 운영형태 분석	• 관리적 측면에서의 운영 형태 분석(프로세스, 정책 등)
용량 계획 수립	• 공격에 대한 일정 위협 수준이상 방어가 가능하도록 공격방어용 용량 증강 계획 수립
인프라 강화 체계 수립	• 공격 형태에 따른 네트워크 장비, 보안장비 및 서버 강화, 지역 내 분산대응 및 지역적 분산대응 인프라 강화방안 수립
위협 단계별 대응체계 수립	• 위협 단계별 공격 대응을 위한 정책, 프로세스, R&R 수립
사후 관리	• 지속적인 관리 및 대응

또, DDoS에 대한 효과적 대응을 위해서 아래의 <표 4>에서 보는 바와 같이 공격탐지에서부터 사고 대응에 이르기까지의 대응 체계 및 절차를 사전에 마련하여야 한다.

<표 4> DDoS 대응 체계 및 절차

단계	체계 및 절차
DDoS 공격 탐지	• 센서 장비 및 외부 경고 수집으로 탐지 - Sensor : DDoS 솔루션, FW, WAF, IDS 등 - 외부 경고 : KISA, ISAC, CERT, ISP 등
위험수준 정의 및 분석	• 위험대상장비에 대한 위험수준 정의 • 위험수준판단 : 트래픽부하, 세션접속수준 • 정상수준정의 : 평균 1~3개월 동안 평균치 선정
상황 전파	• 위험수준에 따라 담당자 및 관계자에게 상황전파 - 비상연락망에 따라 담당/관계자에 상황전파 - 방법 : SMS, e-mail, 유무선 전화 - 관계자 : KISA, CERT, ISP, IDC 등
침해 사고 대응	• 공격수준에 따른 대응 절차 진행 - 피해상황 파악(접속장애, 시스템 오류 등) - 공격유형분석(TCP, HTTP, 네트워크) - 공격지 분석 및 차단 절차

또한, 하나의 DDoS 장비로 모든 DDoS 공격을 막을 수는 없기 때문에 조직내에 존재하는 보안 장비들의 유기적인 관리를 통해 통합적으로 대응을 해야 한다. 방화벽에서 IP/Port 차단, IDS/IPS에서 최신 패턴 탐지, 스위치 장비에서 트래픽 분산, 서버 보안 툴에서 악성코드/취약점 탐지, 클라이언트 백신에서 바이러스/웜 치료 등 사내 보안 장비 간 소통을 통해서 통합 관리해야 한다. 이러한 관점에서 공격 유형별 대응 정책을 수립하고 각 시스템에 적용하여 DDoS 공격대응 맵을 구성, 관리하는 예를 제시하면 <표 5>, <표 6>과 같다.

<표 5> 공격 유형별 대응 맵

DDoS공격유형			A	B	C	D	E	F	G	H
논리공격	호스트	TearDrop		√			√			
		Bonk		√			√			
		LandAttack		√			√			
		WinNuke		√			√			
		PingofDeath		√			√			
대역폭소진공격	ICMP	DirectFlooding	√							
		BroadcastFlooding	√							
	UDP	DNSUDPFlooding	√							
		DNSQueryFlooding	√							
		DNSReplyFlooding	√							
		FraggieAttack	√							
	TCP	SYNFlooding			√					
		ACKFlooding					√			
		MalformedFlagFlooding					√			
자원소진공격	어플리케이션	GETFlooding			√	√			√	√
		CCAttack			√	√			√	√
		CircleCCAttack			√	√			√	√
		SlowrisAttack			√				√	√
	호스트	SYNFlooding				√			√	√
침해시도	호스트	InjectionAttack						√		√
		XSSAttack						√		√

(범례) A: Router(ISP), B: Router(Border), C: DDoS 차단장비, D: QoS, E: Firewall, F: IPS, G: Reverse Proxy, H: Web Server

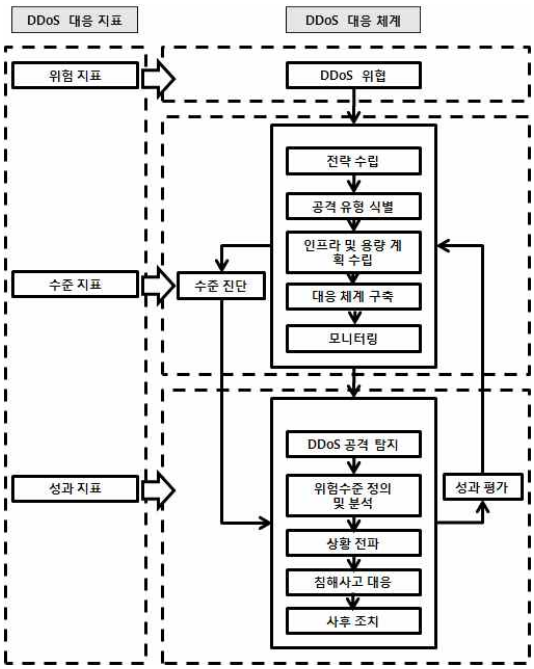
<표 6> 구성 요소별 대응 전략

구분	공격 유형	공격 특징 방어 전략
Router<ISP>	• 네트워크(ICMP) : Direct Flooding, Broadcast Flooding • 네트워크(UDP) : DNS UDP Flooding, DNS Query Flooding, DNS Reply Flooding, Fraggie Attack	• 대역폭소진공격 - 회선의 대역폭 증가 - 동일 N/W을 사용하는 모든 서비스에 장애가 발생 됨
		• RateLimit설정 - ICMP 및 UDP 사용량에 근거하여 일정범위를 넘어서는 패킷 발생 시 인터넷 통신 병목구간인 경계라우터에 도달하기 전 ISP 라우터에서 Null0 Routing 처리함
Router<Border>	• 호스트 : Tear Drop, Bonk, Land Attack, WinNuke, Ping of Death	• 논리공격 - 논리적 오류를 이용한 공격 - 피해 서버의 오작동 유발
		• BOGON차단설정 - IP Spoofing 대응 • 비정상패킷차단 - 라우터에서 비정상 패킷을 받아들이지 않도록 설정
DDoS차단장비	-	-
		• DDoS 차단 장비 內 시스템 방어기능을 활용하여 구별 가능한 시그니처가 있는 공격 및 과다 HTTP 공격을 차단하고 트개픽 현황을 모니터링 함
QoS	-	-
		• IP 접속 평판 통해 Loyalty가 있는 정상 사용자의 가용성을 보장함
방화벽	• 네트워크(TCP) : ACK Flooding, Malformed Flag Flooding	• 비연결성TCPFlooding공격 - 비연결성 TCP Flooding 공격은 UDP 및 ICMP Flooding 공격과는 다르게 상태정보를 인지하는 못하는 라우터 장비 등에서 방어가 불가능하여, 외부 경계구간을 넘어 방화벽 앞 단까지 도달함
	• 호스트 : Tear Drop, Bonk, Land Attack, WinNuke, Ping of Death	• TCP프로토콜상태인식검사기능 - 방화벽의 TCP 프로토콜 상태인식 검사기능을 사용하여 차단
IPS	• 침해시도 : XSS, Injection Attack 등(웹서버 대상의 공격 방어)	• DDoS공격발생중침해시도 - DDoS 공격과 침해를 동시에 시도함 - DDoS 공격 중에는 과다 트래픽으로 인해 IPS의 침해방지/탐지 기능이 일부 소실될 수 있음
		• 장비기능의집중화 - DDoS 공격 발생 시에도 DDoS 트래픽은 타 장비에서 차단하며 IPS는 XSS 등 침해시도에 대한 방어/탐지에 모든 리소스를 집중함
웹서버	• 어플리케이션 : HTTP Get Flooding, CC Attack, Circle CC Attack, Slowris Attack	• httpd 과다 접속 공격 대상 시스템만 피해
	• 호스트 : SYN Flooding	
	• 침해시도 : XSS, Injection Attack 등	• 서버에서 제공하는 SYNCookie 기능 사용 - SYN Cookie 적용시 실제 가용성 테스트 필요 (웹접속 속도 등) - HTMLRedirection 초기 페이지 구성

3.2. DDoS 대응 지표 개발을 위한 프레임워크

3.2.1. DDoS 대응 지표 프레임워크

앞 절에서 제시한 DDoS 대응 체계 및 프로세스 모델을 참조로 구축된 대응 체계를 측정하기 위해서 사용할 수 있는 지표는 성과지표, 위험지표, 수준지표 등으로 세 가지 관점에서 설계할 수 있는데, 본 논문에서는 이러한 관점에서 DDoS 대응 체계 모델과 프로세스 측면으로 매핑되는 대응 지표의 프레임워크를 (그림 1)과 같이 제시한다.



(그림 1) DDoS 대응지표 프레임워크

실제로 측정을 위한 지표를 만들기 위해서는 가능한 한 많은 지표 풀(pool)을 만들어야 하며, 지속적인 측정과 피드백을 통해서 정제, 개선되어야 한다.

지표 후보들은 실행항목들에 대한 책임과 시기, 결과 등이 명시되어 있는 조직의 정보보호정책을 통해 선정하거나, 조직의 정보보호업무를 입력-처리-출력 형식으로 정의되는 상세 수준의 프로세스로 분해하여 각 프로세스별 처리시간, 비용, 출력물의 양과 질, 비율 등을 통해 만들 수 있다.

본 연구에서 제시한 지표 프레임워크는 DDoS 대응 프로세스 모델을 기준으로 위험 지표, 수준 지표, 성과 지표라는 세 가지 관점에서 지표 개발의 틀을 구성하고 있다. 각각의 관점에서 지표 개발의 프레임워크를 정의하면 다음과 같다.

먼저, 위험지표는 ERM(Enterprise Risk Management) 등과 같은 위험관리 기법에 의해 제시된 개념으로 현재의 상황을 대변해주는 요소이며, 외부적인 요인에 의한 지표이다. 이에 대한 예로는 침해사고 발생비율, 주간 네트워크 공격 발생 건수처럼 개별 조직 차원에서 통제 불가능한 외부 위협 수준이나 가까운 미래에 있을 위험에 대한 경보 등이 포함가능하다. 따라서 아래의 (그림 2)와 같이 개별 조직의 입장에서는 측정과 통제보다는 정보의 수집과 분석이라는 관점에서 바라보아야 한다. 조직 내에서 직접 위험지표를 만들 경우 기존의 정보보호위험분석 결과나 개인정보영향평가 등에서 도출된 위험 리스트를 활용할 필요가 있다.

(그림 2) 위험 지표 프레임워크

다음으로, 수준지표는 표준의 관점에서 볼 때의 수준을 의미하는 것으로 ISO 27001이나 ISMS의 GAP 분석 점수, SSE-CMM과 같은 성숙도 점수 등이 여기에 해당된다.

(그림 3) 수준 지표 프레임워크

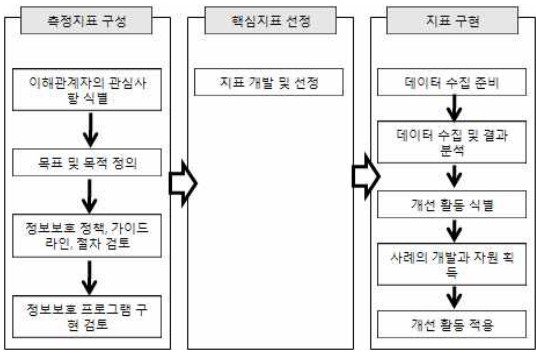
DDoS 대응과 같은 정보보호 업무에 대한 객관적인 성과관리는 다른 어떤 업무 보다 어렵고 까다롭다. 성과관리나 효율성 측면의 고려를 하기 위해서는 정확한 측정지표를 설정하고 이를 구현하는 방법이 중요하다.

성과지표는 BSC(Balanced Score Card), 6시그마 등 전통적인 경영이론과 기법을 통해서 발전해온 영역이다. 보안패치 비율이나 대응 처리 시간, 정보보호교육 이수 비율 등이 해당될 수 있으며 수행하는 해당업무 자체의 효율성 및 이행의 정도를 설명하는 요소이다.

(그림 4) 성과 지표 프레임워크

3.2.2. DDoS 대응 지표 개발 프로세스

대응 지표 개발의 첫 번째 단계는 측정지표의 구성이다. 측정지표 풀을 구성하기 위해서는 공개된 지표들을 가져오거나 업무에서 직접 도출할 수 있다. 공개된 지표로서 참조할 수 있는 자료들은 NIST SP 800-55[20], ISO 27004(WD)[21]와 같은 자료나 관련 표준문서 또는 서적을 들 수 있다. 하지만 이런 방법들은 자신의 회사에 직접 적용하기 어려우며, 시도하더라도 효과가 적을 수 있기 때문에 더 좋은 방법은 자신의 업무와 조직의 환경으로부터 직접 지표를 이끌어내는 것이다.



(그림 5) 지표 개발 프로세스

이해관계자의 관심사항 식별 : 지표에 대해서 관계자들과 그들의 관심사항을 식별하는 것이다. 조직에 소속된 모든 사람은 보안에 대해서 이해관계자가 될 수 있지만 위치에 따라서 그 정도는 다르다. 기관 대표자, CIO, 정보시스템/네트워크 관리자, 정보보호 엔지니어 등은 주요 관련자라고 볼 수 있다. 또한 CFO, 교육/훈련기관, 인력관리 및 인사 분야 등도 보안이 주 업무는 아니지만 자체 업무에 정보보호가 관련되는 부관계자라고 할 수 있다. 이러한 관계자들은 각각의 역할과 직위 등에 따라 보안에 대한 관심과 중점 사항이 다르다.

목표 및 목적 정의 : 특정 정보 시스템에 대한 정보보호 대책을 가이드 할 수 있는 정보보호시스템의 성능 목적 및 목표를 식별하고 문서화 하는 것이다.

정보보호 정책, 가이드라인, 절차 검토 : 조직의 정책과 절차에 대한 베이스라인으로, 정보보호 목표와 목적을 달성하기 위한 보안 대책, 요구사항, 기술들에 대한 구현 방법을 기술한다.

정보보호 프로그램 구현 검토 : 기존의 지표와 지표를 유도하는데 사용되는 관련 자료를 검토한다. 검토 후에는 적용가능한 정보가 추출되어야 하고, 지표 개발과 데이터 수집을 지원하는 적절한 구현 증거가 식별되어야 한다. 여기에 참고할만한 지표들은 시스템 보안 계획/정보보호 관련 활동에 대한 추적 정보(침해사고 보고서, 시험, 네트워크 관리, 감사로그 등)/위험평가 및 침투시험 결과/인증 문서/지속적인 모니터링 결과/비상계획(Contingency plans)/형상관리 계획/훈련 결과 및 통계 등이다.

다음 단계는 위에서 선택한 지표 풀에서 핵심적인 지표를 도출하는 과정으로 이는 DDoS 대응 업무에 대한 성과와 보상을 위해서 공식적으로 인정되는 지표의 포트폴리오를 구성하는 것이다.

지표 개발 및 선정 : 조직에서는 지표 개발 동안의 반복성을 보장할 수 있도록 표준화된 형태로 지표를 문서화하여야 한다. 여기에는 지표를 수집, 분석, 보고하는데에 요구되어지는 상세한 사항들이 제공되어야하며, <표 7>과 같은 예를 기준으로 할 수 있다.

<표 7> 지표 템플릿 예

필드	자료
식별자	지표의 추적 및 정렬을 위해 사용되는 유일한 식별자
목적	전략적 목적
지표	측정에 대한 설명으로 '퍼센트', '갯수', '빈도', '평균' 등
유형	지표가 구현, 효과성/효율성, 영향 등인지에 대한 구분
공식	지표의 수학적인 표현값에 대한 계산
목표	지표에 대한 만족도 등급에 대한 목표
구현내용	특정 지표에 대해서 지표 계산, 수행된 활동의 타당성, 불만족스러운 이유 등
빈도	얼마나 자주 자료가 수집되고, 분석되고, 보고되는지를 나타냄
책임부서	주요 참여자들을 표시 : 정보 소유자, 정보수집자, 정보사용자 등
자료소스	지표를 계산하는데 사용되는 자료의 위치
보고포맷	지표에 대한 보고 포맷 : 파이 차트, 라인 차트, 바 그래프, 기타 포맷 등

또, 지표들의 우선순위를 판단하여 선정하는데, 기존의 정책과 절차를 준수하여 작업하게 되면 도출 가능한 지표들이 방대하기 때문에 참여자당 2~3개 정도의 높은 우선순위를 갖는 지표들을 선택하는 것이 중요하다.

그리고 지표들은 성능 목표를 설정하는 것이 중요한데, 각각의 특성에 따라 정량적 또는 정성적인 분석을 통하여 적용가능한 지표의 성능을 설정하여야 한다.

일단 지표가 선정되면 이는 성능을 측정하거나 만족시키지 못한 이유를 규명하거나 개선을 위해서만이 아니라 일관성 있는 정책 구현을 촉진시키고, 효율적인 정보보호 정책 변경을 하며, 목표나 목적의 재정의와 함께 지속적인 개선을 위해서도 사용되어야 한다. 따라서 지표 개발 및 선정의 과정은 내부에서 지속적인 피드백이 필요한 활동이다.

핵심지표를 도출을 마친 후에는 실제 지표를 구현하는 단계로 측정을 실행하기 위한 체계를 구축한다. 성공적인 실행을 위한 고려사항으로는 측정주체, 측정 주기, 측정 데이터의 위치, 수집 방법, 검증 방법 등에 대한 검토가 있으며, 이 항목들은 지표 측정 절차나 지표 정의 문서에 반영되어야 한다. 각 과정의 상세 내용은 다음과 같다.

데이터 수집 준비 : 지표 프로그램 구현 계획을 수립하는 것이다. 계획에는 계획의 대상/데이터 수집, 분석, 보고의 책임을 포함한 측정의 역할과 책임/특정 조직의 구조, 과정, 정책 및 절차에 맞춰진 지표 수집, 분석 및 보고 절차/이해관계자들 간의 상세한 협조 사항/자료 수집이나 추적 도구의 개발 또는 선정/지표 요약 보고서 형태/지속적인 모니터링을 위한 규정 등이 포함된다.

데이터 수집 및 결과 분석 : 이 단계에서는 지표 구현 계획에서 정의된 절차에 따라 지표 자료를 수집, 통합하고 분석 및 보고에 적합한 형태(예를 들면, 데이터베이스 또는 스프레드시트)로 저장한다. 수집된 지표 데이터는 목표와의 비교를 통해 갭 분석을 수행하고 실제와 원하는 성능간의 갭을 식별함으로서 성능이 낮은 원인과 개선이 필요한 부분을 정의한다.

개선 활동 식별 : 앞 단계에서 분석된 갭을 해결하기 위한 로드맵이 될 수 있는 계획을 개발하는 단계이다. 계획을 위해서는 원인요소나 결과에 기초한 개선 활동의 범위(체계의 구성이나 변동, 스태프들에 대한 교육이나 훈련, 보안장비의 구입, 보호 정책의 변동 등)를 결정하고, 전체적인 위험완화 목표에 기반을 둔 개선 활동 우선순위를 결정하여야 한다. 개선 활동은 대개 단일한 성능에 영향을 주지만, 경우에 따라서는 문제에 비해서 해결 비용이 너무 높을 수도 있다. 따라서, 개선 활동 비용에 대해서는 오름차순, 활동의 효과(impact)에 대해서는 내림차순으로 정리하는 방법을 통해 전체 비용-이익 분석을 수행하여 우선순위 목록에서 가장 상위에 있는 실용적인 개선 활동을 선택한다.

사례의 개발과 자원 획득 : 지금까지의 과정을 통해 결정했던 것들에 대한 자원을 예산에 반영하여 획득해야 한다. 이전의 과정을 통하여 분석한 보고서는 예산을 지원받을 수 있는 증거가 된다.

개선 활동 적용 : 적용에서는 보안 프로그램이나 기술, 관리부분에 대한 보안 정책 등에 대한 개선 활동을 포함한다. 개선 활동에 대해서 관리하고 문서화함으로써 수정 활동과 개선사항에 대해서 더 좋은 효과를 기대할 수 있다.

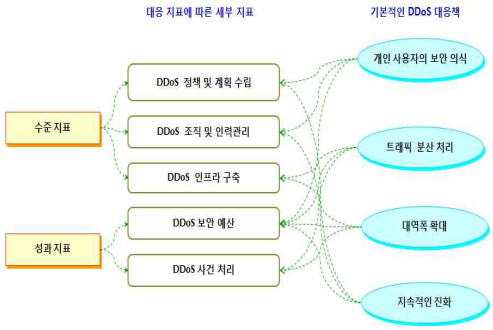
지금까지 정의한 지표 개발과 적용을 위한 활동들은 데이터를 모으고, 분석하고, 보고하는 실행과 관리의 지속성이 유지되어야 그 성과를 보장받을 수 있다. 진척상황에 대해서 모니터링 하고 수정 활동을 지속하는 것은 정보 시스템 보호 정책의 정상적인 구현과 관리에 영향을 준다. 또한, 많은 빈도와 수량의 지표들은 계획되지 않은 행동을 하거나 요구한 행위를 하지 않을 때, 체계를 바탕으로 하여 진로를 빠르게 수정함으로써 문제를 회피할 수 있게 해준다.

4. 대응 지표 도출

본 연구는 일부 지표들을 도출하고 이를 제안한다. 제안하는 지표는 완전한 것이 아니며 DDoS 특징에 적합하게 커스터마이즈한 것이다. 2009년 7월 7일 발생한 DDoS 공격을 통해 확인된 기본적인 4가지 DDoS 대응책은 다음과 같다. 첫째, 개인 사용자의 보안 의식을 통해 좀비 PC의 가능성을 제거한다. 둘째, 트래픽의 분산처리 능력을 높여 공격시 많은 양의 트랙픽을 우회시켜야 한다. 셋째, 대역폭을 확대시켜 공격에 대한 서비스 중단을 미연에 방지해야 한다. 넷째, 지속적인 진화, 즉 지속적인 투자와 DDoS에 대한 예방을 통해 대응 대비 효과를 높여야 한다.

기본적인 4가지 대응책들을 측정할 수 있도록 본 논문에서 제안한 수준/ 성과 대응 지표 수준에 적합한 세부 지표를 도출하여 이를 맵핑해야 한다.

이러한 특징들을 맵핑하고, 각 지표에 적합한 세부지표 및 측정식을 다음과 같이 도출할 수 있다. 본 연구에서 제안한 세부지표와 측정식은 DDoS의 대응 체계를 측정하기 위한 일부분이며 완전한 대응 지표를 개발하기 위해서 계속 연구를 진행하고 있다.



(그림 6) 대응 지표에 따른 세부 지표 도출

<표 8> 수준 대응 지표에 따른 세부지표와 측정식

대응 지표 분류	세부 지표	측정식
수준 대응 지표	DDoS 정책 및 계획 수립	DDoS 관련 규정 절차의 수립 여부의 진행율
		DDoS 관련 대응 절차의 수립 여부의 진행율
	DDoS 조직 및 인력관리	DDoS 대응 관련 전담인력 비율
		DDoS 대응 관련 규정 절차의 공유 여부
	DDoS 인프라 구축	트래픽 감시 도구의 유무
		개인 PC에 대한 보안 프로그램 설치 여부
		DDoS 대응 도구의 유무
		네트워크 대역폭 확대 비율
성과 대응 지표	DDoS 보안 예산	투자할 수 있는 예산의 비율
		DDoS 보안교육에 투자한 비율
	DDoS 사건 처리	사건 발견시점에서 대응까지 걸린 시간
		DDoS 공격으로 인한 물리적 피해 정도
		트래픽 분산 시점까지 걸린 시간

도출한 세부지표와 측정식을 본 연구에서 제안한 프레임워크에 대응하기 위해 제안한 템플릿에 맞게 제안한다. <표 9>는 DDoS 정책 및 계획 수립 지표에 대한 예이다.

<표 9> DDoS 정책 및 계획 수립 지표

필드	자료
식별자	DDoS 정책 및 계획 수립
목적	DDoS에 대응하기 위한 정책과 계획이 사전에 수립되어 있는 정도를 판단하기 위함
지표	DDoS 관련 규정 절차의 수립 여부의 진행율, DDoS 관련 대응 절차의 수립 여부의 진행율
유형	규정 절차와 대응 절차의 구현 여부를 판단
공식	DDoS 정책 및 계획 수립 = (DDoS 관련 규정 절차의 수립 여부의 진행율 +DDoS 관련 대응 절차의 수립 여부의 진행율) / 2
목표	지표에 대한 결과값이 높을수록 DDoS에 대한 조직의 정책 및 계획 수립이 잘 되어있다고 판단한다.
구현내용	보안 담당자의 주관적인 판단으로 조직의 DDoS 절차 수립 여부를 판단함
빈도	분기별로 정책 및 계획에 대한 수립을 판단해야 함
책임부서	보안 책임자 및 관리자
자료소스	DDoS 정책수립서와 계획서의 존재유무와 진행 사항으로 판단
보고포맷	바 그래프로 표현하며, 이를 통해 지속적인 개선 여부도 체크할 수 있음

5. 결론

'측정하지 못하면 관리할 수 없다'는 말은 이제 IT분야의 업무에 있어서도 피할 수 없는 말이 되었다. 정보보안 업무에서도 객관적 지표를 통해서 업무성과를 평가받는 대상에서 더 이상 예외일 수 없다.

본 논문에서는 정보보호 분야 중 특히 지금까지 이슈가 되고 있는 DDoS 공격에 대한 대응 전략 및 절차를 중심으로 한 대응 모델을 제시함으로써 종합적인 DDoS 대응 체계의 수립에 참조할 수 있게 하였다. 또, DDOS 대응체계를 정량적으로 측정함으로써 우선순위와 효과에 대한 철저한 관리를 위한 지표의 체계와 개발 절차에 대한 프레임워크를 제시하였다.

본 연구에서 제시한 프레임워크는 궁극적으로는 DDoS 대응체계의 수준지표, 위험지표, 성과지표를 개발하기 위한 공통적인 프로세스와 지침들을 제공하고자 하였기 때문에, 지표를 실제로 개발할 때에는 각 영역들의 특성에 따라 지표의 내용이 달라질 수 있다. 즉, 수준지표는 성숙도의 개념을 추가로 고려하여야 하고, 위험지표는 개별 조직 보다는 국가적인 차원에서 고려하여야 한다. 또한, 성과지표는 투자 대비 효과라는 측면에서 접근하여야 한다. 그러나, 각각의 지표를 개발하기 위한 전략과 방법론은 본 연구에서 제시한 프레임워크를 모델로 참조하는 것이 효율적이다.

제안한 대응 지표는 DDoS의 공격 특징의 일부분에 대한 것만을 도출한 것이다. 현재 지표에 대한 연구가 진행 중이며, 추후 지표에 대한 심층적인 연구를 통해 효과적으로 DDoS 대응을 평가할 수 있는 구체적인 지표들을 개발해야 한다.

참 고 문 헌

[1] 최양서, 오진태, 장종수, 류재철, "분산서비스거부(DDoS) 공격 통합 대응체계 연구", 정보보호학회논문지, 제19권 제5호, 2009.10.

[2] 인터넷침해사고대응지원센터, "국내 주요 사이트 대상 분산서비스거부공격 분석보고서", 한국정보보호진흥원, 2009. 7.

[3] 구자현, "서비스 거부 공격(Denical of Service)의 유형 및 대응", 주간기술동향, 통권 1377호, 2008.12.

[4] 이희명, 임종인, "기업의 정보보호수준 측정모델 개발에 관한 연구", 한국정보보호학회논문지, 제18권 제5호, 2008.10.

[5] 한국침해사고대응협의회, "All about DDoS 기술세미나", 2008

[6] 나윤지, 조영석, 고일석, "기업의 정보보호 수준 평가를 위한 평가지표", 정보.보안 논문지 제6권 제3호, 2006. 9.

[7] 유황빈, 김경탁, 윤창표, "해킹바이러스연구 최종보고서 - 서비스거부공격 위협분석 및 대응체계 연구", 한국정보보호센터, 2000. 12.

[8] 한국인터넷진흥원 ((구)한국정보보호진흥원), KISA, http://www.kisa.or.kr

[9] Peng, T., Leckie, C., and Ramamohanarao, K., "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Comput. Surv. 39, 1, Article 3, April 2007.

[10] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM

SIGCOMM Computer Communication Review, Volume 34, Issue 2, pp. 39-53, April 2004.
[11] SP800-53(Rev.2) : Recommended Security controls for Information Security, 2007. 10, NIST
[12] ISO/IEC27001 : 2005(FDIS) Information Security Management System Requirements
[13] BS7799 Part 1 "Information Security Management - Code of practice for information security management", BSI, 1999
[14] BS7799 Part 2 "Information Security Management - Specification for information security management", BSI, 1999
[15] ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 1 - Concepts and Model", 1997
[16] ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 2 - Managing and Planning IT Security", 1998
[17] ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 3 - Techniques for the Management of IT Security", 1998
[18] ISO/IEC JTC1/SC7/WG1 "Guidelines for the Management of IT Security(GMITS) : Part 4 - Selection for Safeguard", 1999
[19] Information Systems Audit and Control Association, "COBIT, Management Guideline, 3rd Edition", 2000
[20] SP800-55(Rev.1) : Performance Measurement Guide for Information Security, 2008. 7, NIST
[21] ISO/IEC27004(WD) : 2008(FDIS) Information security management measurements

이 연 호

1988. 2 : 서울산업대학교 전자계산학과(공학사)
1991. 8 : 한양대학교 대학원 전자계산학전공(공학석사)
2007. 2 : 숭실대학교 대학원 컴퓨터학과(박사과정수료)
1988년 ~ 현 재 : 행정중심복합도시건설청(과장)
관심분야 : U-city, 컴퓨터보안

김 범 재

1988년 3월:서울대학교 독어독문학과 학사
2000년 8월:연세대학교 산업대학원 전자계산전공 석사
2005년 9월~현재 숭실대학교 대학원 컴퓨터학과 박사과정
1992년 7월~1995년 2월 (주)쌍용컴퓨터
1995년 3월~현재 한국 HP(공공사업본부 e-Gov't 사업부장 이사)
관심분야 : 멀티캐스트, 그룹통신, 인터넷 보안, 이동 인터넷 통신

이 남 용

1993년 : 미시시피주립대학 경영정보학과(경영학박사)
1979년~1983년: 국군정보사령부 정보처 정보시스템분석 장교
1983년~1999년:한국국방연구원 정보체계연구부장
1999년~현재:숭실대학교 컴퓨터학부 교수
관심분야 : 소프트웨어테스팅, 시스템엔지니어링

김 종 배

1996년 : 서울시립대학교 경영학사
2002년 : 숭실대학교 정보과학대학원 (공학석사)
2006년 : 숭실대학교 대학원 (공학박사)
2001년~현 재: (주)이엔터프라이즈 대표이사
2004년~2006년: 남서울대학교 컴퓨터학과 겸임교수
2006년~현 재: 서울여자대학교 컴퓨터학부 겸임교수
2009년~현 재: (사)해킹보안협회 학술연구위원장
관심분야 : 오픈 소스 소프트웨어, 정보보호(Personal Information), 유비쿼터스 컴퓨팅 등