韓國 컴퓨터情報學會 論文誌
第12卷 第4號, 2007. 9.

2007-12-4-2-8

침해사고 대응을 위한 서비스 제어전략에 관한 연구

신영선*, 박진섭**, 박정진***, 이희성**

A study of service control strategies against infringement accidents

Young-sun Shin*, Jin-sub Park**, Jung-jin Park***, Hee-sung Lee***

요 약

네트워크의 방대화로 인해 온라인 게임, 인터넷 뱅킹 등 인터넷을 이용한 서비스 이용이 증가하고 있는 반면, 이에 대한 역기능으로 웜/바이러스는 물론 해킹에 이르기까지 통신망 서비스를 위협하는 각종 공격이 증가하고 있다. 이러한 각종 공격으로 인해 심각한 피해가 발생함에 따라 이에 대응하기 위해 국가적 차원에서 대응체제를 구축하여 대응하고 있다. 그러나 1.25대란과 같은 국가적 차원의 비상사태 발생시 네트워크망 또는 시스템이 어떠한 침해사고가 발생하고 있는지에 대한 분석을 수행하는 동안 급속도로 전파되어 심각한 피해를 당할 수 있어 효과적인 대응 전략이 필요하다.[1] 따라서 본 논문에서는 통신망에 발생하는 침해사고 유형을 분석하고 대응하기 위한 체크리스트를 제시하고 국가적 차원의 대규모 침해사고 발생시 서비스를 제어하기 위한 전략을 제시한다.

Abstract

With the construction of vast networks, Internet based services such as online games and Internet banking are steadily increasing. As dysfunctions of the trend, various threats from worms/viruses to hacking are proliferating and new types and variations of worms/viruses are emerging. In response to the problems, telecommunication carriers and the government are establishing systems to cope with infringement accidents and resultant damages. However, in case of nationwide emergencies like the 1.25 Accident, infringement may spread rapidly while analyzing what kind of infringement it is and that may result in enormous losses. Thus, the paper purposed to analyze the states of infringement accidents occurring at each network and coping methods and checklist, based on the results, and to propose strategies for controlling services in case of large scale infringement accidents.

▸ Keyword : service strategies, infringement accidents, checklist

• 제1저자 : 신영선
• 접수일 : 2007. 8.24, 심사일 : 2007. 9.7, 심사완료일 : 2007. 9.20
* 대전대학교 컴퓨터공학과 박사수료 ** 대전대학교 컴퓨터공학과 교수
*** 대전대학교 컴퓨터공학과 박사과정

Ⅰ. 서 론

각종 응용서비스 및 다양한 업무가 네트워크를 중심으로 이루어짐에 따라 네트워크는 점점 더 복잡해지고 방대해지고 있다. 이로인한 역기능으로 온라인 게임 및 인터넷 뱅킹 등 인터넷을 이용한 서비스 이용이 증가하면서 금전적인 이익을 추구하는 범죄형 해킹이 증가하는 등의 침해사고도 계속적으로 증가하고 있다.[2]

계속적으로 증가하는 다양한 침해사고에 대응하기 위해 각 통신사업자 및 국가차원에서의 일반화된 침해사고 대응 방법을 제시하고 있으나 1.25대란과 같이 짧은 시간안에 침해사고가 발생하여 순식간에 네트워크와 시스템을 마비시키는 침해사고에 대해서는 근본적인 대책이 되지 못하고 있다. 특히 서비스를 지속적으로 제공해야 하는 통신사업자에게는 침해사고로 인한 서비스 중단시 예상되는 손실과 법적 책임 사항등 다양한 문제가 발생하게 될 것이다.

이러한 문제 발생에 신속히 대응하고 피해를 최소화 하는 것이 통신사업자 및 국가차원의 중요한 쟁점이 될수 있다. 즉, 어떠한 상황에서도 서비스 사용을 중단시키게 되는 문제가 발생하여서는 안되며, 1.25대란과 같은 국가적 차원의 침해사고 발생시 피해를 최소한으로 줄이기 위한 제도가 필요하다.

따라서 본 논문에서는 빠른 시간안에 전파되는 침해사고 발생에 대해 대응하기 위하여 기존의 침해사고 대응 절차를 분석하고 서비스 제어 전략을 포함한 새로운 침해사고 대응 절차를 제시한다. 또한 침해사고 대응시 요구되는 서비스 제어 전략과 침해사고 유형별 체크리스트를 제시하여 긴급한 침해사고 발생시 대응할 수 있도록 한다.

Ⅱ. 관련연구

1. 국내 침해사고 현황 분석

1.1 침해사고 발생 원인

일반적인 침해사고는 대부분 DDOS공격과 패스워드 추정과 같은 아주 간단하면서도 쉽게 발생한다. 대부분의 공격은 프로토콜에 대한 취약점등 네트워크상의 취약점을 이용하여 발생하는 것으로 이에 대해 탐지하고 대응하기 위한 방법들이 지속적으로 연구되고 있다.[3][4][5]

이러한 노력에도 불구하고 침해사고가 매년 증가하고 발생하는 이유를 몇 가지로 살펴 볼 수 있다.

첫째, 각종 인터넷 전자상거래의 발전으로 인해 개인 정보를 유출하는 보안사고가 발생하고 있는 것이 현실이나 대부분 이러한 보안사고의 문제점을 인식하지 못하고 있으며, 기본적인 지식 역시 부족한 상황이다.

둘째, 인터넷에 공개된 해킹 기술을 인터넷 이용자 누구나 쉽게 구할 수 있게 되었다. 인터넷을 이용하여 방대한 자료를 공유할 수 있으며, 쉽게 해킹 기술을 습득하여 악의적인 목적으로 사용할 수 있다. 또한 침해사고가 발생한 네트워크 망에만 영향을 주는 것이 아니라 망과 망간의 침해사고가 쉽게 전파되어 그 피해손실은 증가하게 된다.

셋째, 정보시스템 관리자의 기술적 역량 부족 및 정보보호에 대한 인식 부족이다. 통신사업자별로 정보보호 업무를 수행하고 그에 적절한 보안 전문가 및 책임자를 두어 관리하고 있다. 그러나 침해사고가 발생하여 고객 서비스에 영향을 줄 수 있는 경우라 하더라도 관리자의 소신에 맞추어 대응을 하기에는 불가능한 현실이다.

이와 같이 침해사고 증가 원인은 다양하게 발생하고 있으며 이러한 원인을 분석하고 침해사고의 패턴을 조사하여 정형화된 틀이 제시가 되어야 할 필요가 있다.

1.2 침해사고 현황

인터넷 서비스를 제공하는 유선/무선 사업자와 국가기관에서는 각종 통계 자료를 수집·분석하여 침해사고에 대응하고 있다. 국내에서는 한국정보보호진흥원에서 인터넷침해사고대응센터를 중심으로 인터넷 침해사고 조기 탐지, 분석, 경보를 통해 피해 확산 방지와 상시적인 정보 공유 및 신속한 공동 대응 체계 운영을 통해 정보통신망의 신뢰성을 확보하고 있다.[2]

대부분의 침해사고는 포트를 통해 전파되고 이에 대한 대응으로 포트 즉, 서비스를 차단하게 된다. 이러한 침해사고를 발생시키는 포트들에 대한 현황을 표 1에서 나타내고 있다.[6]

표 1. 침해사고 발생포트 Top10
Table 1. infringement accident occurring port

포트	관련 취약점 및 Bot
80	WebDAV
135	DCOM, DCOM2
139	NetBios, Brute force login attempts
445	LSASS

901	NetDevil
903	NetDevil2
1023	Sasser Backdoor
1025	DCOM
1234	Subseven
1433	MS SQL Login Brute force

일반적으로 표 1에 나타낸 포트별 취약점을 이용하여 각종 침해사고가 발생하게 되면 각 통신사업자들은 포트별 취약점을 분석 한 후 서비스 포트에 대한 차단 여부를 결정하게 된다.

표 2는 이러한 포트를 이용한 공격으로 인해 발생되어지는 포트별 해킹 트래픽 점유율이다. 이는 실제 모기업의 특정 월의 유해 트래픽 발생량을 나타낸 것으로 전체의 42.47%를 차지하고 있다.

표 2. 특정달의 포트별 공격률
Table 2. Port hit ratio

포트	해킹트래픽에 대한 공격률	전체 트래픽에 대한 공격률
80번	20.3	11.8
0번	9.3	3.85
6667번	3.9	2.28
53번	3.5	2.04
135번	1.7	0.99
1433번	0.8	0.46
1027번	0.7	0.4
5900번	0.5	0.29
3410번	0.4	0.23
771번	0.37	0.21

이중 해킹 트래픽이 전체 트래픽의 41%를 차지하고 있으며, 유해 트래픽을 발생시키는 포트 중 80번 포트로 인한 공격이 전체의 49%를 차지하고 있는 것으로 분석되었다.

표 2의 포트별 공격률을 기반으로 well-known 포트와 non well-known 포트의 공격비율을 표 3과 같이 도출하였다.

표 3. Well-Known 포트의 공격 비율
Table 3. hit ratio of well-Known port

포트	공격률
80번	49.0
0번	22.5
6667번	9.3
53번	8.4
135번	4.1
1433번	2.0
1027번	1.6
5900번	1.2
3410번	1.0
771번	0.9

표 3에서 well-known 포트에 대한 공격이 전체의 84.9%를 차지하고 있는 것을 볼 수 있다. 이를 통해 알 수 있듯이 침해사고 발생시 서비스 차단 및 미차단에 대한 신중한 결정이 필요하다.

현재는 포트를 대상으로 한 침해사고 발생시 포트차단 또는 미차단시 발생할 수 있는 피해에 대한 법적 차원의 근거가 미비하여 관리자로 하여금 빠른 대응 및 복구를 수행할 수 없는 것이 현실이다.

이로인해 급격히 피해가 확산될 수 있으므로 긴급상황에 적절한 대응체계가 필요하며, 법적 차원에서의 서비스를 제어하기 위한 전략이 필요하다.

2. 침해사고 대응절차

2.1 침해사고 대응 절차 분석

인터넷 침해사고의 피해범위가 네트워크로 확대되어 침해사고 발생시 국가적인 비상상황으로 확산될 가능성이 커짐에 따라 인터넷 침해사고를 국가적인 차원에서 체계적으로 관리해야 할 필요성이 대두되고 있으며 인터넷 침해사고에 신속하고 효율적으로 대응할 수 있도록 예·경보 등급체제가 시행되게 되었다.

또한 각 통신사별로 침해사고 발생시 시스템 및 네트워크망에 피해를 주는 정도에 따라 예·경보를 단계별로 구분하여 대응 및 대책 수립을 수행하고 있다. 대체적으로 유사한 대응 절차를 수립하고 있으며, 정상적인 네트워크 운영시 사내망과 사외망, 라우터 및 주요 시스템에 대한 유해 트래픽 모니터링과 웜·바이러스 관리 및 백신 소프트웨어 설치 등의 업무를 수행하게 된다.[7][8]

그림 1은 현재 침해사고 발생시 대응하기 위한 일반적인 침해사고 대응 절차이다.

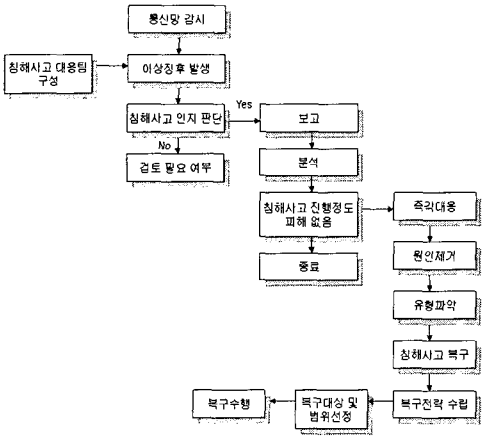

그림 1. 침해사고 대응 절차
Fig 1. Incident response procedure

그림 1의 침해사고 대응절차는 통신망에 이상징후가 발생하게 되면 기업의 규모 및 특성에 따라 대응할 수 있는 침해사고 대응팀을 구성하고 침해사고를 분석하여 서비스 제공에 어느 정도의 피해를 주는지를 판별하도록 한다. 이는 침해사고 발생시 침해사고에 따른 대응 복구를 수행할 때 어느 정도의 심각도를 가지고 있는 침해사고 인지를 판단하고 적절한 대응 체제를 구축하기 위함이다.

이러한 일반적인 침해사고 대응 절차는 이상징후 발생후 판단하고 검토하고 보고한 후 대응하는 단계까지 여러 단계를 수행하게 되는데 일반적인 침해사고 대응절차 단계에서는 인지-분석-대응-사후관리 단계로 구성되어 있다. 이러한 절차는 하나의 그물처럼 이어져 있는 통신망에 침해사고가 발생 할 경우 짧은 시간안에 통신망 전체에 전달되어 1.25 대란과 같은 결과를 가져오게 된다.

이러한 4단계에 기반을 두어 본 논문에서는 긴급한 침해사고 발생시 대응절차를 제시하고 침해사고 발생을 인지, 분석, 대응, 관리하기 위한 침해사고 유형별 체크리스트를 4단계로 제시한다.

III. 네트워크 침해사고 발생시 서비스 제어 전략

1. 서비스 차단의 효과성 및 문제점

국가적 차원의 관점에서 서비스의 원활한 제공은 정보시스템에 의존하고 있는 현실에서 가장 중요한 문제로, 안정적인 서비스를 제공하기 위해 국가적 차원의 각종 규정 및 법제도를 마련하고 있다.

1.25대란과 같은 침해사고가 발생하게 되면 짧은 시간안에 국가망 전체를 마비시켜 엄청난 피해를 가져올 수 있기 때문에, 신속한 침해사고 대응이 가장 중요하다. 일반적으로 침해사고가 발생하게 되면 침해사고 대응 절차에 따라 수행하게 되고 대응방법 중 하나로 서비스 차단을 통해 쉽고 빠르게 네트워크망을 통해 전파되는 공격을 차단하게 된다.

그러나 서비스 포트에 대한 차단이 간단하고 신속한 대응 방법이지만 서비스 차단으로 인해 큰 피해가 발생할 수 있기 때문에 중요한 논점이 될 수 있다. 즉 ISP의 인터넷 공격으로 인한 대응을 위해 서비스 포트 차단이라는 문제는 신속한 공격 포트 차단을 통한 인터넷 위협 방지라는 측면과 사용중인 가입자 서비스의 일방적인 차단이라는 측면에서 양면성이 존재하는 민감한 문제이다.

이러한 논쟁에 대한 사례를 그림에서 제시하였다. Blaster웜이 발생하였을 때 확산 방지를 위한 서비스 차단 여부에 대해 문제가 발생하였고, 이에 대한 서비스 차단 및 해제 내역과 발생되어진 문제점이다.

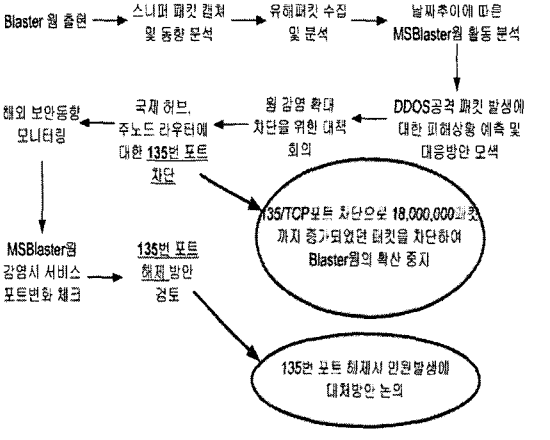

그림 2. Blaster웜 확산 방지를 위한 서비스 차단 및 해제 내역
Fig 2. details of service interception and remove for check the Blaster worm spread

그림 2의 Blaster 웜에 대한 대응은 웜 출현을 인지하고 대응·복구까지의 시간을 최소 1시간~2시간 정도의 시간을 소요하게 되는데, 이 시간동안 가장 중점을 두어야 할 사항은 서비스 차단으로 인해 발생되어지는 효과성과 문제점이다.[6]

이 시간 안에 인지-분석-대응 단계까지 이루어지는데 침해사고를 인지한 담당자가 인지 및 대책 회의, 대응까지의 시간으로 일반적인 침해사고 대응 절차를 따르고 있다.

그러나 1.25대란과 같은 침해사고의 경우 30분내에 모든 네트워크의 상태가 마비되는 대규모의 침해사고가 발생할 수 있어 빠른 침해사고 대응과 서비스를 효율적으로 제어하기 위한 절차가 요구된다.

따라서 일반적인 침해사고 대응 절차 방법외에 서비스 또는 포트를 차단하는 등의 긴급한 침해사고에 대응하기 위한 절차를 수립하여야 하며, 각종 분석 자료 및 과거 경험을 바탕으로 법적 제도하에 서비스를 제어하기 위한 제도가 필요하다.

2. 서비스 제어를 위한 침해사고 대응 절차

본 절에서는 일반적인 침해사고 대응절차를 분석하고 긴급한 침해사고 발생시 대응하기 위한 서비스 제어 측면의 침해사고 대응 절차를 제시한다. 또한 서비스 제어 전략과 침해사고 발생시 대응을 위한 대응 체크리스트를 제시한다.

2.1 일반적인 침해사고 대응 절차

일반적으로 통신망에 침해사고가 발생하게 되면 국정원 및 KISA, 각 통신업체들의 관제 센터로부터 각종 정보가 수집되고, 침해사고 전파에 따른 대응을 위해 침해사고 정도에 따라 예보/경보 단계를 KISA에서 발령하게 된다. 그 후 긴급조치 및 대응 조치 수행을 위해 KISA가 각 통신업체에 지시하게 되고 원인분석 후 법적 조치를 찾게 되는 절차를 수행한다.

그림 3은 법에서 제시하고 있는 일반적인 침해사고 대응 절차이다.

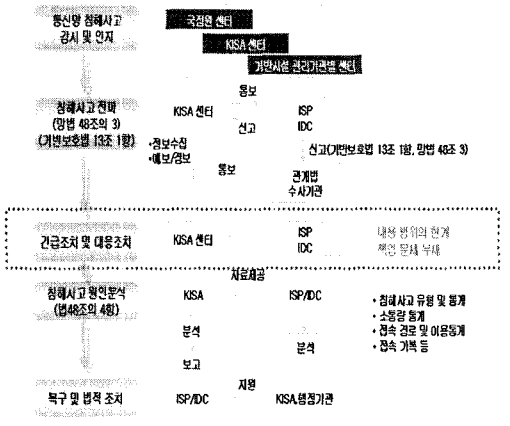

그림 3. 기존의 침해사고 대응 절차
Fig 3. A existing of incident response procedure

그림 3의 일반적인 침해사고 대응절차의 문제점은 1.25 대란과 같은 긴급한 침해사고 발생시 긴급조치 및 대응 조치시 내용 범위 및 대응 후 책임 문제에 대한 명확한 내용이 언급되지 않고 있다.

또한 각 통신사업자 별로 서비스 제공의 중단 시간이나 원인에 따라 사용자 이용 약관에 배상기준을 제시하고 있으나 국가적 차원의 법적/제도적 기반이 뒷받침 되지 않으므로 배상에 대한 문제도 거론되고 있다.

따라서 일반적인 침해사고 대응 절차의 문제점을 보완하여 국가적 차원의 긴급한 침해사고가 발생하였을 책임 및 범위 부여에 대한 문제와 여러 단계의 보고 및 승인 과정에 의해 발생되는 문제점을 보완하여 서비스를 제어하기 위한 대응절차가 필요하다.

2.2 긴급한 침해사고 발생시 서비스 제어를 위한 대응절차

기존의 침해사고 대응 절차는 여러 단계의 보고와 대책회의로 인한 대응시간 지연과 대응 범위의 한계 및 모호한 책임부여 등 긴급한 침해사고 발생에 대한 대응으로 인해 여러 가지의 문제가 발생할 수 있다.

이러한 문제점을 최소화하기 위해 본 논문에서는 그림 4와 같이 긴급한 침해사고 발생시 서비스 제어를 목적으로 하는 침해사고 대응절차를 제시하였다.

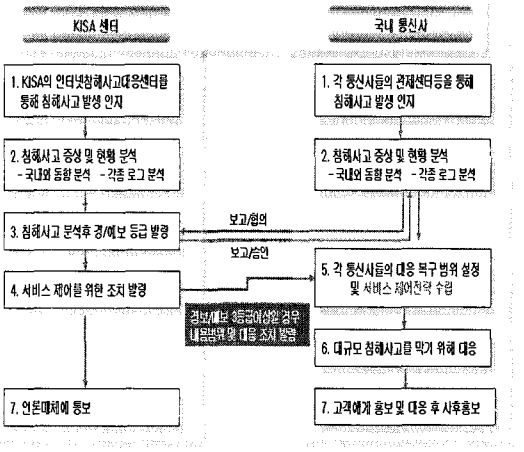

그림 4. 대규모 침해사고시 서비스 제어 시나리오
Fig 4. service strategies scenario against large scale infringement accidents.

그림 4에서 보는 바와 같이 침해사고가 발생하면 침해사고 발생을 인지하고 분석을 통해 예보/경보 등급을 발령한

다. 그 후 4단계에서 서비스 제어를 위한 조치를 발령하게 되는데 이때 각 침해사고의 심각도에 따라 침해사고 대응 범위 및 서비스 제어 전략에 대한 권한 위임 여부를 결정하게 된다.

본 논문에서는 경보/예보 등급이 3단계 이상일 경우 대응을 위한 대책 회의 및 보고단계를 생략하고 침해사고에 대응하기 위한 권한을 해당 통신업체에 위임하도록 제시하였다.

긴급한 침해사고 발생시 서비스 제어를 위한 대응절차 적용시 기존의 침해사고 대응 절차에 비해 여러 가지 면에서 문제점을 해결할 수 있다.

우선 권한을 위임 받은 통신업체는 서비스 제어로 인해 발생할 수 있는 피해를 예측하고 서비스 차단 여부를 결정하여 신속히 대응할 수 있도록 한다.

또한 서비스 차단 여부 결정시 발생한 침해사고 유형별 체크리스트 적용과 서비스 제어 전략을 수립하여 대응하도록 한다. 이러한 긴급한 침해사고 발생시 본 논문에서 제시한 서비스 제어 목적의 대응절차에 적용하면 여러단계의 승인으로 인해 발생할 수 있는 문제점과 책임상의 문제를 통신사업자에게 위임함으로써 해결할 수 있다.

이때 중요한 것은 통신사업자가 서비스를 제어하기 위한 목적으로 주요 서비스 포트를 차단할 경우 과거의 충분한 데이터 수집과 침해사고 유형에 대한 명확한 분석이 뒷받침되어야 한다.

본 논문에서 제시하고 있는 긴급한 침해사고 발생시 서비스 제어를 위한 대응절차는 일반적인 침해사고 대응절차와는 다르게 발생한 침해사고가 국가차원의 큰 위협을 줄 수 있을 정도의 심각도를 갖을 경우 사고 대응방법 및 서비스 제어시의 모든 권한을 위임토록 하는 방안을 제시하였다. 이로 인해 기존의 문제점인 서비스 제어로 인한 책임소재 문제와 사고 대응범위의 모호함을 해결할 수 있다.

이를 위해 우선적으로 침해사고 유형을 빠르게 분석하여 대응하기 위한 체크리스트를 제시하였다. 또한 대응 방법 및 서비스 제어시의 권한 위임으로 인해 발생되어지는 차후 문제점을 법/제도적 차원에서 보호할 수 있는 방안을 제시하였다.

2.3 침해사고 유형 분류 및 침해사고 체크리스트

본 논문에서 제시하는 체크리스트는 각종 침해사고 사례를 분석하고 침해사고 유형을 분류하여 각 단계별 사항을 정립하기 위한 것으로 침해사고 대응 목적의 체크리스트이다.

공격 유형별로 일반적인 침해사고 대응 절차의 단계인 인지단계-분석단계-대응단계-관리단계의 4단계로 침해사고 유형별 체크리스트를 작성하였다.

침해사고 유형을 정의하는 이유는 침해사고 유형에 따라 분석 방법과 대응 절차가 다를 수 있으므로 침해사고 진단 및 대응 절차를 명확하게 분석하고 신속한 대응을 하기 위함이다.[9][10]

그림 5는 본 논문에서 제시한 침해사고 유형과 체크리스트 점검 단계이다. 본 논문에서 제시한 침해사고 유형은 통신망에 발생할 수 있는 공격들로 한정하였다.

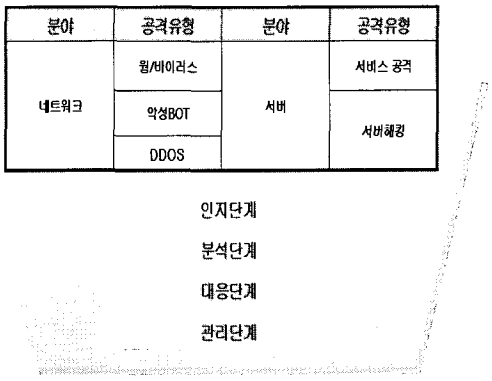

그림 5. 침해사고 유형 분류
Fig 5. classification of Incident type

침해사고 유형별 체크리스트는 네트워크 분야와 서버 분야로 구분하여 제시하고 분야별 공격 유형에 따른 체크리스트를 작성하였다. 또한 각 공격 유형별로 다음 4단계의 기준에 적합한 체크리스트 항목을 제시하였으며 각 단계는 침해사고 대응 절차를 바탕으로 도출하였다.

- 인지단계

각 통신사업자들의 보안관제 센터로부터 수집된 자료를 기반으로 하고 국내외 보안 동향과 KISA의 인터넷침해사고 대응센터의 현황 시스템을 통해 이상징후를 판단한다.

- 분석단계

각 공격 유형에 따라 보안동향과 보안관제 센터의 자료를 분석하여 공격 패턴 및 트래픽 분석, 포트 분석을 수행한다.

- 대응단계

침해사고 유형을 분석하여 해당 대응 절차를 수행한다. 또한 침해사고의 원인을 제거 한 후 조치 여부를 확인하고 그 결과를 관리하여 유사 침해사고 발생시 신속하게 대처할 수 있도록 한다.

- 관리단계

대응 단계 후 트래픽을 모니터링 하고 지속적인 관리를 수행한다.

표 4는 본 논문에서 제시하는 침해사고 유형별 체크리스트 중 웜/바이러스에 대한 체크리스트이다.

침해사고 유형별 체크리스트는 제시한 4단계 기준에 맞추어 작성하였으며, 체크리스트를 통해 침해사고 발생시 인지-분석-대응-관리 단계를 거쳐 침해사고를 파악하고 대응 할 수 있다.

표 4. 웜/바이러스에 대한 체크리스트
Table 4. Checklist for Worm/Virus

침해사고 유형		
구분	내용	
인지	보안동향	- 국내외 보안동향 분석
	통신업체	- 침해모니터링 및 보고 - 보안장비 관리
	공동대응	- 트래픽 동향 - 웜/바이러스 발생 동향
분석	-이상프로세스나 시스템 속도 저하 발견 -각종 보안 장비에 대한 로그 분석 및 시간대별 트래픽 상태 분석 -임계치 초과 이벤트 분석	
대응	-예/경보 단계에 적합한 공동 대응체계 구축 -웜/바이러스 사고 수준에 따른 경보 -라우터 및 주요 네트워크 장비에 대한 차단 -보안취약점 패치 적용 -홈페이지에 웜/바이러스 발견 및 패치 홍보	
관리	-웜/바이러스 신고건수 통계 -보안시스템 모니터링 -최신 백신 및 백신 업데이트	

2.4 서비스 제어를 위한 보안 법/제도 차원의 보완

침해사고 발생시 대응 및 조치에 관한 사항으로 망법 제48조 1항 3,4호에서 침해사고 긴급조치를 수행해야 하며, 대통령령이 정하는 침해사고 대응 조치를 수행하게 되어 있다. 그러나 이러한 법적 문구가 긴급한 상황에 대처하기 위한 기준은 되지 못한다. 즉, 이러한 법적 조항은 다음과 같은 모호성을 갖고 있다.

첫째, 긴급조치의 내용과 한계가 명확하지 않다.
1.25 대란과 같은 국가적 비상사태 발생시 긴급조치를 수행하였을 때 그 후에 발생할 사용자들의 민원과 피해에 대해 언급하지 않고 있으며, 어느 범위까지의 긴급조치를 요하는지에 대해서도 명확하지 않다.

둘째, 긴급 조치의 실질적 실행 방법이 구체화 되어 있지 않다. 이에 대한 실행 방법을 국가적 차원의 대규모 침해사고시 대응 규정을 제시할 필요가 있다.

셋째, 긴급 조치의 수행 주체가 명확하지 않다. 현재 KISA에서 조치 명령을 내리면 긴급 대응을 수행하는 기관은 각 통신사업자들이다. 이러할 경우 그 책임이 명확하지 않아 책임 논란이 일어날 수 있다.

넷째, 대통령이 정하는 침해사고 대응 조치의 내용이 명확하지 않다. 일정한 범위를 제시하거나 그렇지 못할 경우 권한 자체를 각 통신사업자들에게 넘기는 방법이 필요하다.

본 논문에서는 긴급한 침해사고 대응시 서비스 제어를 위한 전략을 법/제도적 측면과 침해사고 대응 주체인 통신사 차원의 보완 사항을 제시하였다.

2.4.1 법/제도적 측면의 보완

법/제도적 측면의 보완 필요성은 현재 국가적 차원의 대규모 침해사고가 발생하게 되면 각 통신사업자는 국가망의 안정적인 운영을 위해 실질적인 대응 업무를 수행하게 된다.[10][11] 그러나 그에 대한 명확한 대응 내용 및 권한 부여의 의미가 모호하여 피해손실이 발생하였을 경우 대응할 여지가 없다. 따라서 이러한 법/제도적 측면을 보완하여 통신사업자와 국가는 책임 있는 운영과 서비스를 제공하는 사용자로 하여금 혼란을 겪지 않도록 해야 한다.

본 논문에서는 법/제도적 측면의 보완 사항을 다음과 같이 제시하였다.

① 침해사고 발생시 인터넷침해사고대응센터에서는 침해사고를 인지하고 현황을 분석해야 한다.
- 국내외 보안 동향 분석 및 국가의 네트워크 운영상황, 신종/변종 형태의 각종 침해사고 유형들 대해 빠르게 인식하고, 각 통신사업자 역시 주요 시스템 한 철저한 분석이 뒷받침 되어야 한다.

② KISA는 통신사로부터 침해사고 증상 및 현황을 보고 받고 협의해야 한다.
- KISA는 침해사고 발생시 통신사업자로부터의 각종 정보에 대한 보고를 통하여 통신사업자와의 협의를 통해 신속한 대응 방안을 제시해야 한다.

③ 침해사고 발생시 통신사업자에게 침해사고 예보/경보 등급을 발령한다.
- 국가적 차원의 침해사고 발생은 예보/경보 등급 3단계 이상으로 정하고 통신사업자에게 대응 조치를 발령해야 한다.

④ KISA는 침해사고 대응 업무에 대해 통신사에게 대응 업무를 승인하도록 한다.
- 각 통신사업자들에게 국가적 차원의 침해사고 대응을 위한 업무를 위임하여 통신사업자로 하여금 책임 있는 운영을 하도록 해야 한다.

⑤ 서비스 제어로 인해 발생 할 수 있는 민원 대응 방책을 수립한다.
- 민원에 대응하기 위해 홍보문안 및 대응 요령을 작성하여 배포한다.
- 홈페이지를 통한 서비스 제한을 안내한다.

2.4.2 통신사 차원의 보완

관리기관 자체 이용약관 보완의 필요성은 현재 통신사업자의 이용약관에 다음 사항과 같은 서비스 중지 및 손해배상, 면책사항에 대해 제시하고 있으나, 서비스 중지 시간에 따른 배상 내용 및 세부적인 사항이 제시되어 있지 않다.
따라서 기존의 사용자 이용약관에 대한 보완책은 다음과 같다.

① 침해사고 경보/예보 등급이 3,4 등급일 경우 관리기관은 일정기간 서비스를 중단한다.
- 앞에서 제시한 대규모 침해사고 대응 절차에 따라 KISA는 경보/예보 등급이 3,4 등급일 경우 통신사업자에게 대응 조치를 발령하고 일정기간 서비스 중단을 통해 침해사고 전파를 단절시키도록 한다.

② 침해사고 대응을 위한 서비스 제어 전략을 수립하여 KISA에 보고한다.
- 통신사업자는 침해사고 대응 후 서비스 제어 사항을 KISA에게 보고하고 피해손실 및 규모를 분석해야 한다.

③ 서비스 제어 후 고객에게 홈페이지를 통해 홍보해야 한다.
- 서비스 중단시 고객에게 사전에 통보하게 되어 있으나 국가적 차원의 비상사태 발생시에는 사후 홈페이지를 통해 홍보하여 서비스를 중단 할 수 밖에 없었던 사항을 공지해야 한다.

IV. 서비스 제어전략 시나리오 예시

본 절에서는 제시한 긴급한 침해사고 발생시 대응절차에 따라 서비스를 제어하기 위한 서비스 제어 전략 시나리오를 제시한다.

그림 6은 긴급한 침해사고 발생시 서비스 제어를 위한 시나리오로써 3단계로 구성하였다.

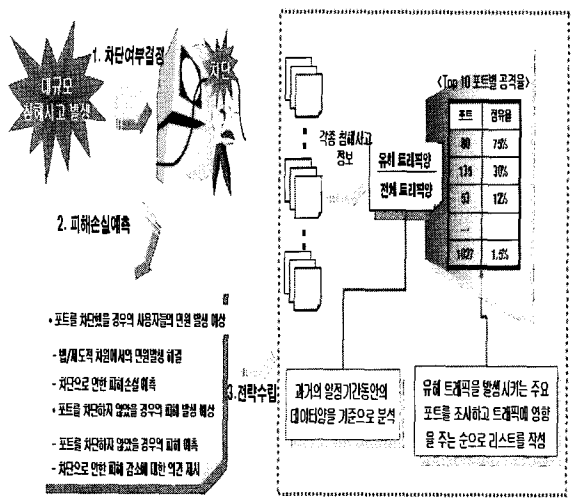

그림 6. 서비스 제어 전략 수립을 위한 방법
Fig 6. methods for service strategies

첫 번째 단계는 예보/경보 3단계 이상의 침해사고가 발생하게 되면 각 통신사의 관리자들은 KISA의 보호조치 발령으로 인해 차단할 것인지 차단하지 않을 것인지에 대해 결정한다.
차단 여부에 대한 결정은 일괄적으로 처리되어지는 문제는 아니다. 즉, 침해사고 발생상황 및 대응은 과거 자료와 경험을 통해 대응할 수 있으나, 차단 여부를 결정하기 위한 기준은 과거 일정기간동안의 데이터와 전문가의 경험을 통해 수립되어야 한다.
두 번째 단계는 차단하였을 때와 하지 않았을 때의 피해손실을 예측해야 한다. 이는 침해사고 대응 후 서비스를 지속적으로 제공받지 못하여 이용약관에 어긋나거나 이로 인해 발생한 피해에 대해 국가 또는 통신사가 그에 대한 책임을 질 수 있는지 여부에 대한 것으로 민감한 논의 쟁점이 될 것이다.

따라서 두 번째 단계에서는 표 5와 같이 피해손실을 예측하는 내용에 대해 분석해야 한다.

표 5. 포트차단에 따른 피해 예측 내용
Table5. damage subject for port

포트를 차단 했을 경우의 민원발생 예상	- 법·제도적 차원의 민원발생 해결 - 차단으로 인한 피해손실 예측
포트를 차단 하지 않았을 경우의 민원 발생 예상	- 포트를 차단하지 않았을 경우의 피해손실 예측 - 차단으로 인한 피해감소에 대한 의견 제시

세 번째 단계는 이러한 피해손실 예측 단계 후 전략을 수립하게 되는데 각종 침해사고 정보를 수집하여 침해사고가 발생하였을 때 공격포트가 된 포트들의 점유율을 계산한다.

각 포트별로 과거의 일정 기간 동안의 데이터양을 기준으로 분석하고 유해트래픽을 발생시키는 주요 포트를 조사하고 트래픽에 영향을 주는 순으로 리스트를 작성하도록 한다. 결과적으로 서비스 제어 전략의 3단계를 통해 침해사고 발생에 따른 피해를 최소화 하고 지속적으로 서비스를 제공할 수 있다.

V. 결론

현재 국내 주요 침해사고는 웜, 바이러스, 해킹등으로 인한 피해가 증가하고 있다. 이러한 역기능에 대응하기 위해 각 통신사별로 자사의 기술과 침해사고 대응 절차를 수립하여 적절한 대응을 수행하고 있지만 효과성과 효율성을 고려한 대응책을 적용하기에는 어려운 점이 있다.

본 논문에서는 일반적인 침해사고 대응절차를 분석하고 긴급한 침해사고 발생시 서비스를 제어하기 위한 긴급한 침해사고 발생시의 대응절차를 제시하였다.

또한 침해사고 발생시 이에 대한 발생원인 및 현황을 분석하고 유형별 침해사고를 두 가지 분야 즉, 네트워크와 서버분야로 분류하여 체크리스트를 작성하였다. 체크리스트는 인지단계, 분석단계, 대응단계, 관리단계 4단계에 걸쳐 네트워크 상에 침해사고 발생시 대응할 수 있는 체크리스트를 작성하였다.

마지막으로 네트워크상에 침해사고가 발생하였을 경우 어떤 대응책을 적용해야 하는지, 누가, 얼마나 오랜시간 단절을 해야 하는지에 대한 효과성을 고려한 서비스 제어 전략을 제시하였다.

결과적으로 본 논문에서 제시한 긴급한 침해사고에 대응하기 위한 절차를 통해 기존의 대응절차에서 발생되는 책임여부 및 대응시간의 문제를 해결할 수 있다. 또한 이러한 문제를 해결함으로써 피해를 최소화 할 수 있는 서비스 제어 전략을 수립할 수 있다.

향후 본 연구에서 제시한 침해사고 대응절차를 기반으로 하여 실제적인 대응 사례에 대한 연구가 필요하다.

참고문헌

[1] 인터넷 대란에 대한 정책적 대응방향, 국가보안기술연구소, 2003

[2] 인터넷 보안 동향 보고서, 2004.8

[3] 정태명, 인터넷 침해사고 원인과 대책, 한국정보처리학회지,Vol.10 No.2, 2003.

[4] 서정택, 정보통신망 취약점 분석평가 방법론, 한국정보보호학회 Vol.13, No5, 2003

[5] 최운호, 자동화된 침해사고 대응 시스템에서의 안전하고 합법적인 ISP의 IP 정보제공방안, 한국정보보학회, Vol.15,No.1, 2005

[6] 웜 분석 결과 보고서, 침해사고대응협력팀, 2003.9

[7] 정태인, 인터넷침해사고 조기탐지 및 대응 체계 운영 현황, 한국정보보호학회, 2005

[8] 이미정, 한승환, 사이버공간에서의 국가안보위협 요인 및 대책 방안, 국방대학교 안보문제 연구소, pp35~69, 2005.

[9] 네트워크 침해사고 대응을 위한 체크리스트 개발, 연구보고서, 성균관대학교, 2004.7

[10] Nyanchama,M., Information Security Management Enterprise Vulnerability Management and Its Role in Information Security Management ,Vol.14, No3, ACM, 2005

[11] Hone. K., "Information Security Policy What Do International Information Security Standards Say?", Computers and Security, Vol.21,No5, 2002

저 자 소 개

신영선

2004년 대전대학교 대학원 컴퓨터공학과 석사
2007년 대전대학교 대학원 컴퓨터공학과 박사수료
현재 (주)유비엔씨 기술연구소 연구원
관심분야 : 정보보호, 보안평가

박진섭

2003~현재 : 정보보호 전문업체 기술위원
2000~2005 : 정보보호컨설팅전문업체 기술심의위원회 위원장
2007~현재 : 대전대학교 공과대학장
관심분야 : 정보보호, 보안관리

박정진

2003~2004 (주)니츠 정보보호기술연구소 전임연구원
2007년 현재 (주)유비엔씨 기술연구소 선임연구원
2007년 현재 대전대학교 컴퓨터공학과 대학원 박사과정
관심분야 : 개인정보보호, 시스템 및 네트워크 보안

이희성

2000년 대전대학교 대학원 컴퓨터공학과 석사
2002~2005 국방부 연구개발관실 기술개발관리과
2006년~현재 대전대학교 컴퓨터공학과 대학원 박사과정
2006~현재 방위사업청 통합사업관리 T/F
관심분야 : 개인정보보호, 보안관리, ITA