情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

인터넷 침해사고 조기탐지 및 대응 체계 운영 현황

정 태 인*, 강 준 구*, 이 두 원**

요 약

인터넷침해사고대응지원센터(KISC)에서는 2003년 1월 25일에 있었던 인터넷의 접속 불능 사태의 재발을 방지하기 위하여 기존의 한국정보보호진흥원(KISA)내의 해킹바이러스 상담지원센터를 확대 개편하여 KISC를 개소하여 운영하고 있다. 본 고에서는 KISC 개소 1주년을 맞이하여 운영현황 및 주요 인터넷 침해사고 대응 사례를 살펴보고, 개선점을 찾고자 한다.

Ⅰ. 서 론

2003년 1월 25일은 한국의 인터넷사에서 큰 의미를 가지는 사건이 발생한 날이다. 핵전쟁 발생시 네크워크의 지속적인 운용을 목적으로 설계된 인터넷이지만, TCP/IP 프로토콜 자체의 취약성과 그 취약성으로 인해 인터넷이 마비될 수 있다는 가능성은 계속 지적되었다. 그러한 가능성이 한국에서 현실로 나타난 것이 바로 슬래머 웜에 의한 인터넷 마비 사태였다. 이 사태를 통해 전국적인 규모에서 인터넷 트래픽을 모니터링하여 이상 징후를 탐지하고, 이를 신속히 전파 및 대응하여 인터넷이 마비되는 사고를 재발해야겠다는 필요성이 커지게 되었다. 이러한 필요성에 따라서 기존에 한국정보보호진흥원(KISA : Korea Information Security Agency)내 해킹바이러스 상담지원센터를 확대·개편하여 2003년 12월 17일 한국인터넷침해사고대응지원센터(KISC : Korea Internet Security Center)를 개소하였다. 본고에서는 KISC의 운영 1주년을 맞이하여, 운영 체계 및 현황을 살펴보고 주요 침해사고에 대하여 어떻게 대응하였는지 사례를 살펴보겠다. 또한 향후 KISC의 보다 효율적인 운영을 위하여 어떠한 개선사항이 필요한지를 도출하고자 한다.

Ⅱ. 본 론

1. KISC 연혁

1.1 해킹바이러스 상담지원센터

1996년 한국정보보호센터 설립과 함께 만들어진 해킹바이러스 상담지원센터에서는 해킹이나 바이러스로 인해 피해를 입은 사용자들이 전화(02-118)나 메일(cert@certcc.or.kr)로 문의하는 경우, 대응 방법이나 시스템 복구 방법을 알려주는 역할을 주로 수행하였다. 또한 국내외 보안권고문(security advisory)을 수집·분석하여 국내 전파가 필요한 경우에 메일(sec-info@cert.certcc.or.kr)이나 홈페이지 게시를 통하여 전파하였다. 한편 주요 해킹 및 바이러스 사고에 대해서 사고 노트(incident notes)를 작성하여, 사고의 원인을 분석하고 재발 방지를 꾀하였다. 또한 신고된 해킹, 바이러스 사고 건수를 수집·분석하여 매월 '해킹바이러스 통계 및 분석 월보' 통계보고서를 작성·배포하고 있다. 이 보고서는 해킹, 바이러스에 관해 신뢰할 수 있는 현황 자료를 제공하는 역할을 수행하고 있다. 이와 같이 해킹바이러스 상담지원센터는 주로 개별 시스템이나 일반 사용자들의 보호에 중점을 두고 운영 되었다.

* 한국정보보호진흥원 인터넷침해사고대응지원센터 ({tijung, jgkang}@kisa.or.kr)
** 정보통신부 기반보호대응팀 (smiledwlee@mic.go.kr)

1.2 한국인터넷침해사고대응지원센터

한국인터넷침해사고대응지원센터(KISC)는 1996년부터 한국정보보호진흥원내에 운영하던 해킹바이러스 상담지원센터를 확대 및 개편하여 2003년 12월 17일 개소하였다. KISC의 목적 및 주요 업무는 다음과 같다.

- 목적
  - 침해사고 예방을 위한 기술지원
  - 실질적인 침해사고 대응 및 분석, 피해 복구 기술 지원
  - 국내 전산망 침해사고대응팀들간 협조 체제(CONCERT) 운영 지원
  - 침해사고 대응을 위한 단일 창구 운영
  - 그밖의 침해사고 예방 활동
- 업무
  - 침해사고 예방을 위한 기술지원
  - 전산망 보안 기술 지침 개발 및 보급
  - 기술 세미나 지원
  - 침해사고의 접수
  - 전산망 보안 침해 사고 진단 분석 지원
  - CONCERT 사무국 운영
  - FIRST 활동 참여
  - FIRST 제공 정보의 공유
  - 사고 통계 및 분석 결과 배포
  - 국내 유관 기관 협력

KISC는 기존의 1개 팀 규모로 운영하던 상담지원센터를 3개 팀 규모로 확대하였으며, 국내 인터넷 서비스 제공 사업자(ISP), 집적정보통신시설사업자(IDC) 등으로부터 침해사고 관련정보를 제공받아 모니터링할 수 있는 법적인 근거를 확보하였다.

제공받은 관련정보는 외부에 공개되지 않도록 각별히 보안에 주의하며, 24시간 침해사고 징후를 모니터링하는데 활용하고 있다. 이러한 모니터링을 성공적으로 수행하기 위해서, 센터는 정보제공기관에서 인터넷 상황에 관계없이 안정적으로 관련정보를 제공받기 위하여 전용회선 및 데이터 송수신 서버를 구축하였다. 또한 수집된 다양한 1차 정보(raw data)로부터 실제 침해사고 이상 징후를 탐지할 수 있는 시스템을 개발하였다.

한편 이상 징후 탐지시 신속하게 ISP, IDC 등에 이상 징후를 전파하여, 피해의 예방 및 확산 방지가 가능하도록 주파수 공용 통신(TRS), 단문 메시지 서비스(SMS), 메신저 등 연락체계 및 시스템을 구축하였다. 또한 국내외 관계기관과도 공동 대응 체계를 구축하고 정기적으로 공동 대응 훈련 등을 통해 대응 능력을 제고하고 있다.

2. KISC 운영 체계

2.1 KISC 구성

KISC는 초기 개소시 분석대응팀, 네트워크모니터링팀, 대응협력팀의 3개 팀이었으나, 2005년 조직개편을 통해서 5개 팀으로 변경되었다. 각각의 팀은 센터의 목적과 업무의 특성을 충분히 반영하여, 팀간 시너지 효과를 높일 수 있도록 구성되었고, 각기 수행하는 업무는 다음의 표와 같다.

표 1. KISC 팀별 업무

팀명	업무
분석기술팀	o 신규 취약성 및 웜·바이러스 동향 조사 o 취약성 검증 및 분석 보고서 작성 o 웜·바이러스 분석
상황관제팀	o ISP 네트워크 및 국내외 주요 사이트 모니터링 o 정보수집 개소 확대 및 정보공유 o 침해사고 초동대응 및 해킹·바이러스 예·경보 발령
해킹대응팀	o 해킹 기법 및 국내외 동향조사 o 시험망 운영을 통한 해킹사례 분석 o 침해사고 긴급대응 및 기술지원
대응협력팀	o FIRST 및 국가 CERT 협력 o APCERT, CONCERT 사무국 운영 o 국내외 침해사고 E-Mail 접수 및 처리
스팸대응팀	o 불법스팸대응 정책지원 o 불법스팸관련 실태조사 및 대응 o 불법스팸관련 신고 접수

2.2 KISC 업무

KISC의 운영은 크게 4 단계로 나눌 수 있다. 각처에서 관련정보를 제공받아 수집서버에 저장하여 이상 징후를 탐지하는 ① 수집·탐지단계, 수집된 데이터를 전문가 시스템이나 통계분석시스템을 통하여, 취약점, 공격코드, 영향력을 평가하는 ② 분석·협의 단계, 일정 수준이상의 위험도를 가지는 바이러스·웜 및 취약점의 경우, 대응요령 및 관련 정보를 ISP, IDC, 일반사용자들에게 전파하는 ③ 전파·발령 단계, 대응요령에 따라 각 기관이나 사용자들이 대응하고 피해 발생시 이를 복구하는 ④ 대응·복구 단계이다.

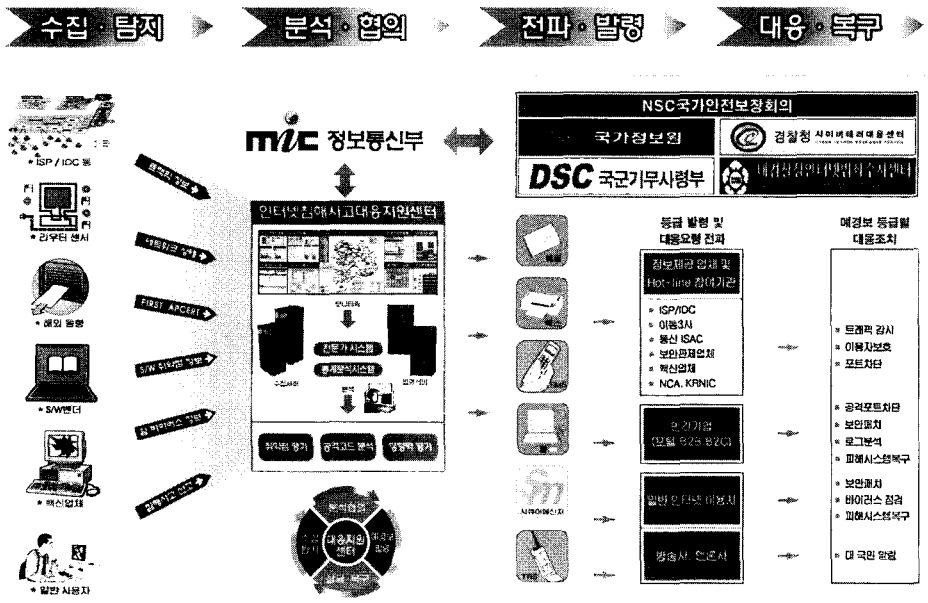

그림 1. KISC 운영 체계

① 수집 · 탐지 단계

KISC는 '정보통신망이용촉진및정보보호등에관한법률'에 근거하여 해당 기관으로부터 침해사고 관련정보를 제공받고 있다.

- 침해사고 관련정보 제공기관
  · 주요정보통신서비스제공자(ISP)
  · 집적정보통신시설사업자(IDC)
  · 주요정보통신기반보호시설
  · 보안관제업체
  · AS 번호를 할당받은 자
  · 바이러스 백신 제조자

- 침해사고 관련정보
  · 침해사고의 유형별 통계
  · 당해 정보통신망의 소통량 통계
  · 접속경로별 이용통계 등

또한 KISC는 공격 정보를 수집하기 위한 에이전트를 개발하여 전국 주요 지점에 설치하였다. 에이전트는 ADSL 등 실제 인터넷 이용자 환경과 유사한 환경에 설치되어 있어, 이용자들이 직면하고 있는 보안위협을 효과적으로 모니터링할 수 있다.

이 외에도, MS, Cisco 등과 협력체계를 구축하여 주요 보안 취약점이 발견되었을 경우, 관련 정보를 공유하여 신속한 패치 개발을 돕고, 패치 검증 시험 등을 통해 오류를 최소화하도록 상호 협력하고 있다.

최근의 해킹, 웜 · 바이러스의 경우, 국경과 상관없이 전세계적으로 동시에 전파 및 발생되는 경우가 많다. 따라서 해외 주요 보안 사이트와 메일링 리스트 가입을 통해서 주요 보안 정보를 획득하고 국외 동향을 파악하는 작업도 지속적으로 수행하고 있다.

② 분석 · 협의 단계

위의 수집 · 탐지 단계를 거쳐서 다양한 출처로부터 수집된 정보는 모두 KISC의 데이터베이스에 저장된다. 그러나 이러한 정보는 단지 쌓아두는 것만으로는 효과가 없다. 다양한 1차 정보(raw data)로부터 얼마만큼 효과적으로 침해사고 이상 징후를 분석할 수 있는지 여부가 관건이다. 이러한 분석을 위해서는 축적된 통계정보를 사용하여 추이를 분석하고 각각의 독립된 정보들간의 관계를 파악하는 전문가 시스템, 통계분석 시스템이 필요하다. KISC에서는 이러한 시스템을 자체 개발하였으며, 판단 기준값들을 지속적으로 조정하여 판단의 정확성을 높이고 있다.

한편 KISC에서는 OS, 네트워크 장비 플랫폼별로 분석실을 구성하여 다양한 웜 · 바이러스, 취약성 등을 신속하고 정확하게 분석하고 있다.

이렇게 통계정보 분석과 동작·영향 분석을 수행하여, 웜·바이러스, 취약성이 네트워크에 미치는 영향, 공격접근 용이성, 전파력, 관련기관 평가 등을 종합적으로 고려하여 점수를 산정한다. 산정된 점수에 따라 필요시 예·경보를 발령하는 등 대응방법을 결정하게 된다.

또한 인터넷 위협에 효과적으로 대응하기 위해서는 관계 기관과의 협의가 필수적이다. 즉, 특정 웜·바이러스가 국내에서 발견되었을 경우, 샘플을 신속히 확보하여 국내 백신제조업체에 전달하여 백신 제작을 독려하고, 해외의 피해 현황 및 대응 방안 등을 공유하고 있다. 국제적으로 공조가 필요한 Bot이나 피싱 사고의 경우, 중간 경유지나 숙주 서버의 IP를 확인하여 국외 ISP나 침해사고대응팀(CERT)에 요청하여 차단하고 있다.

③ 전파·발령 단계

KISC 설립 이전에는 주요 웜·바이러스, 보안 취약점이 발견되면 주로 이메일(sec-info), 홈페이지 공지, 시큐어 메신저 등을 주요 전파수단으로 활용하였다. 그러나 1.25 슬래머 웜과 같이 인터넷에 장애가 발생하는 경우에는 이러한 전파 수단으로는 신속하게 관련 ISP, IDC 등에 전파가 어려웠다. 따라서 인터넷 이외의 통신을 이용한 전파 수단의 확보가 필요하였다. 따라서 비상시 연락하여 조치가 가능한 각 ISP, IDC 등의 정보보호 담당자 목록을 확보하여, 유선전화, FAX, 휴대폰, TRS 등으로 비상연락망을 구성하였다. 특히 동시에 여러 명에게 상황을 전파할 수 있는 TRS 연락 체계를 구축하고 매일 네트워크 관련 특이사항을 점검하고 있어, 비상시 즉시 활용할 수 있는 체계를 갖추고 있다.

또한 일반 인터넷 이용자, 민간기업 등에 예·경보 및 관련 정보를 전파하기 위하여 SMS 연락체계를 갖추었다. KISC 홈페이지를 통하여 신청한 사람에게는 예·경보와 주요 정보보호 정보를 문자 메시지로 송신해주는 서비스를 무료로 제공하고 있다.

특히 네트워크나 시스템 관리자들이 아닌, 일반 사용자들의 대응이나 조치가 필요한 경우에는 방송사, 신문사 등의 언론기관에 보도자료 배포 등을 통하여 대국민 홍보를 하고 있다.

④ 대응·복구 단계

인터넷에 영향을 미치는 웜·바이러스의 경우 특정 IP나 포트 등을 사용하는 경우가 많다. 이러한 경우, 각 ISP, IDC 등에서 해당 IP나 포트를 차단하여 효과적으로 악성 트래픽을 차단할 수 있다. 그러나 다수의 사용자들이 동시에 사용하는 인터넷의 특성상, 일부 사용자에게 특정 서비스의 사용이 불가능해지는 등 불편이 발생할 수 있다. 따라서 이러한 조치의 경우에는 신중하게 판단하여야 하며, 다수의 사용자들의 인터넷 사용을 위해 발생하는 불편을 감수할 수 있는 법·제도적 근거와 사용자들의 인식 제고가 필요하다.

한편, 특정 웜·바이러스는 자신의 네트워크나 시스템에서는 완전히 치료가 되었으나, 보안 취약점을 조치하지 않는 경우, 다른 네트워크나 시스템을 통해 재감염될 가능성이 있다. 따라서 단순히 웜·바이러스의 치료뿐만 아니라 보안 취약점의 패치 등을 통하여 재발을 방지하는 조치가 필요하다.

KISC는 홈페이지를 통하여 효과적으로 웜·바이러스의 재감염을 방지하고 해킹당한 시스템을 복구하고 백도어 등의 취약점을 제거하는 방법을 공지하고 있다.

3. 주요 대응 현황

3.1 웜·바이러스 예·경보

예보발령 주요 웜·바이러스로는 MyDoom, Bagle, rbot(악성 Bot) 및 PeepView 트로이잔, Santy 등이 있었으며, 15건의 예보 가운데 언론보도자료를 배포한 경우는 5건이었으며, 8건에 대해서는 악성코드를 상세분석하여 동작 및 감염원리, 발생하는 네트워크 트래픽 등에 대한 분석보고서를 홈페이지를 통하여 배포하여 일반인에게 주의를 촉구하였다.

2004년도 웜·바이러스 예·경보 발령 목록은 다음과 같다.

3.2 보안권고문 예·경보

예보발령 주요 보안 취약점은 MS ASN.1 처리모듈 취약점, 그래픽 이미지 모듈 버퍼오버런 취약점 등 MS 운영체제관련 취약점, CheckPoint Firewall-1의 HTTP Security Server, ISS 일부 제품군 PAM 보안취약점 등 보안제품 관련 취약점, Cisco SNMP 메시지 처리모듈 취약점 등 네트워크 장비관련 취약점 등 다양하였다.

22건의 예보 가운데 특히, PKI 인증서 처리와 관련이 있는 것으로 알려진 MS ASN.1 모듈 취약점의 경우 해당 취약점과 국내공인인증체계와 연관성이 적

표 2. 웜·바이러스 예·경보 목록

번호	일시	제목	홈페이지	메일	SMS	보도자료	기술문서
1	01.19	Win32.Bagle 웜	O	O	O		
2	01.21	SPYBOT.S 웜	O	O	O		
3	01.27	MIMAIL.R 웜	O	O	O		O
4	01.29	WORM_MY DOOM.B	O	O	O	O	
5	02.19	WORM_NET SKY	O	O			
6	03.18	Bagle.P	O	O	O	O	O
7	03.19	Win-Trojan.Onban.24576	O	O	O		
8	03.20	W32.Witty 웜	O	O	O		
9	03.26	Bagle.U 웜	O	O	O		O
10	04.02	Win32/Agobot.gen.worm	O	O			O
11	04.29	Win32/Agobot.Worm.ali	O	O	O		O
12	04.30	rbot(Agobot 변종)	O	O	O	O	O
13	05.01	w32.Sasser 웜	O	O	O	O	O
14	06.19	PeepView 트로이잔	O	O			O
15	12.23	santy.A 웜	O	O	O	O	

표 3. 보안권고문 예·경보 목록

번호	일시	제 목	홈페이지	메일	SMS	보도자료	기술문서
1	01.14	MDAC 함수의 버퍼 오버런으로 인한 코드 실행 문제	O	O	O		
2	01.14	H.323 메시지 프로세싱의 취약점	O	O			
3	02.05	checkpoint firewall-1 HTTP Security Server 취약점	O	O	O		
4	02.06	Checkpoint VPN-1 Server, VPN Client 버퍼오버플로우 취약점	O	O			
5	02.12	ASN.1의 취약점으로 인한 코드 실행 문제	O	O	O	O	
6	03.10	Microsoft Outlook 2002의 취약점으로 인한 코드 실행 문제	O	O	O		
7	03.11	MSN Messenger의 취약점으로 인한 정보 공개 문제	O	O	O		
8	03.20	ISS 제품군의 PAM Buffer Overflow 취약점	O	O	O		
9	03.29	시스코 취약점관련 공격가능코드 공개	O	O	O		
10	04.06	인터넷익스플로러의 CHM처리에 대한 취약점	O	O	O		
11	04.06	IE 기반의 웹메일 서비스의 Cross Site Scripting 취약점	O	O	O		
12	04.08	Cisco WLSE, HSE 디폴트 계정 취약점	O	O	O		
13	04.12	시스코 LEAP관련 공격도구 Asleap 공개	O	O			
14	04.14	MS04-011 14가지 윈도우즈 취약점에 대한 패치	O	O	O		
15	04.14	MS04-012 4가지 윈도우즈 취약점에 대한 패치	O	O			
16	04.14	MS04-014 마이크로소프트 Jet Database Engine (Jet) 취약점	O	O			
17	04.22	TCP 취약점(BGP의 경우 주의 요함)	O	O	O		
18	04.22	Cisco SNMP 메시지 처리 취약점	O	O			
19	05.12	Help and Support Center 취약점으로 원격코드 실행	O	O			
20	05.13	IEEE 802.11 무선프로토콜의 서비스거부공격 취약점	O	O			
21	09.15	[MS04-028] GDI+ 버퍼 오버런 취약점 패치권고	O	O			
22	10.13	MS Windows JPEG 처리(GDI+)용 보안 업데이트 재배포 등 8개 취약점	O	O			

음을 알리는 내용의 보도자료를 배포하여 일반인이 안심하고 공인인증서를 사용할 수 있도록 하였다.

2004년도 보안취약점에 대한 예·경보 발령 목록은 다음과 같다.

3.3 사고노트

사고노트란 KISC에 접수되는 해킹사고를 처리하는 과정에서 다른 기관이 유사한 피해를 당하지 않도록 사고의 원인 및 대응 방안을 서술한 문서다.

2004년도 사고노트 목록은 다음과 같다.

표 4. 사고노트 목록

번호	일시	제목
1	03.06	개인 PC를 이용한 스팸메일 발송 분석보고서
2	06.14	Phishing Site 사고 분석보고서

3.4 2004년 기술문서

기술문서란 최신 해킹기술에 대하여 직접 시험 분석한 공격기술 및 보안대책을 서술한 문서다.

2004년도 기술문서 목록은 다음과 같다.

표 5. 기술문서 목록

번호	일시	제목
1	01.20	와레즈(컨텐츠 불법유통 사이트)등으로 악용되는 윈도우즈 해킹피해 대책
2	02.13	MyDoom.A와 Doomjuice 웜 분석 및 대응
3	03.19	Bagle 웜(변종P/R) 분석 보고서
4	03.29	Bagle.U 웜 분석보고서
5	04.06	AgoBot계열 웜 분석 보고서
6	04.30	Agobot(rbot) 웜 최신 변종 분석 보고서
7	05.03	Sasser 웜 분석 보고서
8	05.22	Bobax.c 분석보고서
9	06.29	Peep Trojan 분석 보고서
10	06.30	관리자를 위한 악성적프로그램 분석방법
11	08.18	Ratos 27136 웜/바이러스 분석 보고서
12	09.03	kerberos 5 implementation 취약점
13	09.07	Trojan에 의한 정보유출 사전예방을 위한 개인 방화벽 활용
14	09.07	Microsoft Windows XP 서비스 팩(SP) 2 영향 분석
15	09.10	MyDoom.18200 웜/바이러스 분석보고서
16	09.30	분산 서비스 거부 공격 차단 및 분석 기술
17	11.04	Bagle.AM 웜/바이러스 분석 보고서
18	11.18	IE 등 인터넷 탐색기의 URL Spoofing 취약점
19	12.20	악성 Bot 특성 분석을 통한 탐지 및 대응책

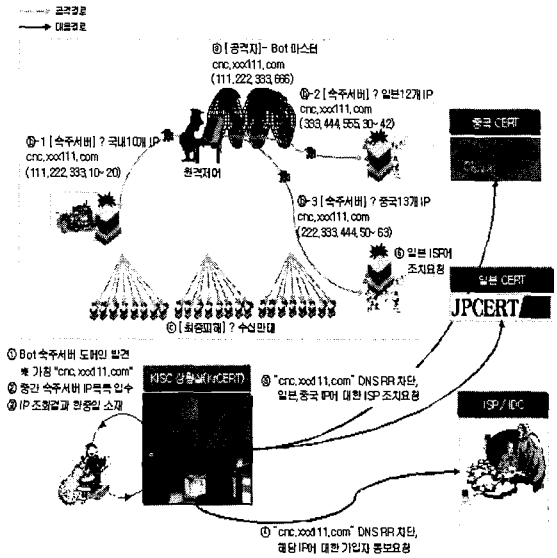

그림 2. 모의훈련 개념도

3.5 한중일 공동 모의 훈련

KISC는 국내 ISP, IDC 등과 공동으로 분기별로 가상 시나리오에 기반한 공동 대응 훈련을 시행하고 있으며, 2004년 12월에는 한국, 중국, 일본 및 국내 5개 주요 ISP 등이 참여하여 한중일 공동 대응 훈련을 진행하였다.

이 모의훈련은 한중일 국가 CERT간 대응협력체계 점검, KISC 자체 상황대응절차 숙련도 측정, 개선사항 도출을 위해 실시되었다. 한국에서는 KISC와 5개 주요 ISP 사업자(KT, 하나로, 데이콤, 두루넷, 드림라인)가 참여하고, 일본(JPCERT), 중국(CNCERT)이 참여하였다.

훈련에서 사용한 시나리오는 다음과 같다.

- 악성 Bot의 중간숙주 서버 도메인에 대한 3국 동시 차단
- 인접국(중국, 일본) 트래픽 이상 징후를 통한 국내 웜 유입(확산) 방지

이렇게 국내가 아닌 인접국 3개국이 참여한 공동 대응 훈련은 세계 최초로 시도된 것이었으며, 향후 이러한 훈련을 정례화하고 참여 국가를 확대하여 대응능력과 체계를 강화할 예정이다.

3.6 웜·바이러스 대응 사례

3.6.1 Mydoom 웜

Mydoom 웜은 2004년 2월 발생하였으며, 이메일

을 통하여 감염되고, 감염 후에는 대량 메일을 발송하고 특정 사이트에 분산 서비스 거부 공격(DDoS)을 하는 특징을 가지고 있다.

KISC의 대응 내역은 다음과 같다.

표 6. Mydoom 웜 대응 내역

일시	대응내역
01.28	o MyDoom 출현 인지 o 관련포트 트래픽 이상 징후 모니터링 o 영향력 및 위험성 분석
01.29	o 예보 발령 o 주요 ISP에 1차 상황 전파문 발송 o 홈페이지에 대응 조치법 게시
01.31	o 2차 상황 전파문 발송
02.02	o MyDoom.B 영향력 및 위험성 분석
02.02	o 3, 4차 상황 전파문 발송
02.11	o MyDoom.Juice 영향력 및 위험성 분석
02.11	o 5차 상황 전파문 발송
02.13	o MyDoom 계열 웜 종합 분석 보고서 웹 게시

영문 제목의 이메일로 전파되는 특징과 KISC의 신속한 대응에 힘입어, 전 세계적으로 200만대 이상의 PC가 감염되었으나, 국내에서는 700건의 감염이 발생하였다.

3.6.2 Sasser 웜

Sasser 웜은 '04년 4월에 발표된 MS 취약성(MS 04-011)을 이용한 웜으로, 취약성 발표후 1개월 후에 발생하였다. 이 웜은 LSASS 취약점 패치가 안 된 시스템을 TCP 445 포트로 스캔후 공격하여 관리자 권한을 획득한다. 관리자 권한 획득후에는 추가적인 웜파일을 다운로드하여 설치하고 계속적으로 공격대상을 찾는 특성을 가지고 있다.

KISC의 대응 내역은 다음과 같다.

표 7. Sasser 웜 대응 내역

일시	대응내역
05.01	o Sasser.A 출현 인지 o 관련 포트 트래픽 이상 징후 모니터링 o 웜 영향력 및 위험성 분석 o 예보 발령 및 주요ISP에 1차 상황 전파문 발송
05.02	o Sasser.B 출현 인지 o 위험성 분석 o 2차 상황 전파문 발송[관련 포트 차단 권고]
05.03	o 분석 보고서 홈페이지 게재 o 3차 상황 전파문 발송
05.04	o 4차 상황 전파문 발송[Sasser.D 주의]

웜 자체에 프로그램 오류가 있고, 웜을 다운로드 받는 사이트를 신속히 차단한 결과, 국외에서는 美 델타 항공에서 6시간 동안 애틀랜타행 항공 이착륙 지연, 핀란드 삼포 은행의 백신 프로그램 설치에 따른 업무 중단, 대만 우체국 400여 지점의 업무 중단 등이 발생하였으나, 국내에서는 피해가 미비하였다.

4. 개선 사항

KISC의 1년간의 운영 경험에 비추어 보면, 주요한 웜·바이러스 등에 대하여 성공적으로 대응하였지만, 아직도 개선해야할 부분은 많이 있다.

현재 KISC에서 특정 IP나 포트 차단을 각 ISP나 IDC 등에 권고하는 경우, 비교적 신속하게 차단이 되는 상황이다. 그러나 차단 권고는 FAX나 메일 등을 통해서 이루어지고 있어서, 실제 담당자가 수신후 권고의 적절성 여부를 판단하여 조치하기까지는 적지 않은 시간이 소요된다. 따라서 전파속도가 상당히 빠른 웜·바이러스의 경우 대응이 늦어지는 사태가 생길 수 있다. 따라서 ISP나 IDC에서 보안 정책 서버(security policy server)를 운영하여, 중앙에서 보안 정책을 변경하면 하부 라우터, 침입차단시스템 등에 일괄적으로 적용할 수 있는 시스템을 구축할 필요가 있다. 이 경우, KISC의 권고가 표준화된 보안 정책의 형식을 이용하면, 보다 신속한 대응이 가능할 것이다.

또한 네트워크 환경은 기존의 PC나 서버뿐만 아니라, 다양한 정보단말기가 연결되는 유비쿼터스 환경으로 변하고 있다. 유비쿼터스 환경에서는 휴대폰, PDA, 정보가전 등의 다양한 단말기가 연결되고, 이동성을 보장해주는 Ad-hoc 네트워크가 사용된다. 따라서, 이러한 다양한 환경을 고려하여 단말기나 네트워크의 종류에 관계없이 모든 네트워크의 정상적인 운용을 보장하기 위하여, 이상 징후를 모니터링 할 수 있도록 시스템 업그레이드가 필요하다.

Ⅲ. 결 론

지금까지 KISC의 운영 현황, 체계 및 주요 대응 사례를 살펴보았다. 그러나 완벽한 대응 체계를 구축하기 위해서는 1회성으로 센터를 설립하고 설치된 시스템으로 운영을 지속하는 것만으로는 충분하지 않다. 급변하는 보안 환경에서 새롭게 나타나는 보안 위협에 대해 지속적인 분석을 통해서 시스템에 필요한 부분들을 추가하고 기존의 모듈을 개선하는 노력을 계속하여야 한다. 또한 인터넷을 사용하는 일반

사용자들의 보안 의식이 성숙하여, 침해사고 징후를 발견하면 즉시 KISC로 신고할 수 있는 분위기가 만들어져야 할 것이다. 즉, 특정 조직이나 센터에서 정보보호를 전담하는 것이 아니라, 인터넷을 사용하는 모든 사용자들이 생활속에 정보보호를 실천하는 환경이 되어야 할 것이다.

참 고 문 헌

[1] 한국정보보호진흥원, "2004 정보시스템 해킹·바이러스 현황 및 대응", 한국정보보호진흥원, 2004
[2] 한국정보보호진흥원, http://www.krcert.or.kr, 한국정보보호진흥원, 2004

〈著 者 紹 介〉

정 태 인(Jung, Tae In)
1998년 2월 : 한양대학교 전기공학과 졸업
2000년 2월 : 한국과학기술원 전기및전자공학과 석사
2000년 1월~2001년 6월 : 데이콤 근무
2001년 7월~현재 : 한국정보보호진흥원 근무
〈관심분야〉 네트워크, 정보보호

강 준 구(Kang, Jungu)
1996년 2월 : 고려대학교 통계학과 졸업
1997년 6월 : 미국 IELI 졸업
1997년 6월~1999년 11월 : (주)디비뱅크 근무
2001년 12월 : 영국 버밍엄대학 컴퓨터공학 석사
2002년 1월~현재 : 한국정보보호진흥원 근무
〈관심분야〉 정보보호, 소프트웨어공학, MIS

이 두 원(Lee, Doo Won)
2004년 9월 : 중앙대학교 영어영문학과 졸업
2004년 12월~현재 : 정보통신부 정보화기획실 정보통신기반보호대응팀 근무
〈관심분야〉 정보보호