CERT팀 구축 및 운영 가이드

2001. 12. 6

정현철, hcjung@certcc.or.kr
하도윤, dyha@certcc.or.kr
박유리, yrpark@certcc.or.kr

1. CERT구축의 역사와 배경

1988년 11월, 인터넷의 전신이라고 할 수 있는 ARPANET은 "Morris 웜" 이라고 불리는 첫 자동화된 네트워크 보안사고를 당했다. 코넬 대학의 Robert T. Morris라는 학생이 몇몇 취약점 중의 하나를 찾아서 이를 이용해서 다른 시스템에 접속하고, 자신을 복사하는 프로그램을 만들었다. 최초의 원본 코드와 복사본은 ARPANET내의 다른 컴퓨터에 대해 무한정 이와 같은 행동을 반복하였다. 이것이 세계 최초의 "자기 복제기능을 가진 네트워크 공격 도구"로써 이러한 종류의 악성프로그램(Malicious Code)를 인터넷 웜이라고 부르고 있다. 이 웜은 많은 시스템 자원을 사용하여 공격당한 컴퓨터가 더 이상 정상적으로 동작할 수 없도록 하였다. 그 결과 당시 ARPANET에 연결되어 있던 미국의 컴퓨터들 중 약 10% 정도가 동시에 중지되었다.

하지만, 이 사고에 대한 대응은 피해를 당한 기관마다 독립적으로 이루어지고, 조정되지 않아서 똑같은 노력이 중복되고, 해결책이 서로 상충하였다.

이 사건이 발생된지 몇 주 후에 인터넷 보안 사고와 취약점 분석 배포를 위한 조정자 역할을 수행하기 위해서 미 국방성의 지원하에 CERT/CC가 조직되었다.

세계 최초의 CERT팀이 생성되는 순간이다.

미국의 CERT/CC가 만들어진 후, 각각의 목적과 임무를 가진 사고대응팀들도 크게 증가하였다. 하지만 각국의 사고대응팀들은 언어와 사간대역의 차이 등으로 인해 각 팀간의 상호대응이 원활히 이루어지지 못했다. 이러한 가운데 1989년 10월, DEC VMS 시스템을 공격 타겟으로 하는 "WANK 웜"이 계기가 되어 각 팀들간의 커뮤니케이션과 협력의 필요성이 대두되었다.

이러한 문제로 인해 1990년 국제사고대응팀협의회(FIRST)가 결성되었다. 2001년 현재 FIRST에는 전세계 100여개 이상의 사고대응팀이 가입하여 정보교류를 하고 있다.

국내에서는 1996년 한국정보보호진흥원 내에 CERTCC-KR이 설립되었고, 1999년 FIRST에 가입함으로써 한국을 대표하는 사고대응팀으로 활동하고 있다. 또한 국내 침해사고대응팀간의 정보 교류, 기술 공유 등의 협조체제를 통하여 국내 침해사고 예방 및 확산 방지를 도모

하기 위하여 한국침해사고대응팀협의회(CONCERT)를 구성하였다. 2001년 현재 망사업자, 연구소, 대학 등 108개 기관이 CONCERT에 가입되어 있다.

하지만, 국내 일선기관의 사고대응체계는 아직 대단히 미비하다고 볼 수 있다.

일례로 지난 2000년 초, 국내의 모대학이 해킹을 당한 후 국외 사이트를 공격시도한 사건이 계기가 되어, 국외의 몇몇 주요 메일링 리스트에서 한국의 인터넷 보안 현실에 대한 혹평들이 올라온 적이 있다.

다음은 메일링리스트에서 외국 네티즌들 사이에 오고간 이야기 중의 일부이다.

- *누구 한국으로부터 해킹사고에 대한 답변을 받은 사람 있나요?*
- *한국인들은 영어도 읽을 줄 모르거나 아니면 보안에 전혀 신경을 쓰지 않거나 둘 중에 하나다.*
- *한국에 있는 시스템들이 손쉬운 타겟이 되는 것은 확실히 문제이다.*
- *그들이 답장을 하지 않을지 모르지만 그들의 네트워크에 관한 문제의 심각성을 알릴 필요가 있다.*
- *한국 특히 교육기관이 전세계의 cracker 들에게 사실상 열려져 있다.*

외국인들의 많은 이야기들 중에 주목해야할 것은 한국이 보안이 허술하다는 것 보다는 오히려 해킹사고 관련하여 국내 연락처를 찾기 힘들고, 사고메일을 보내도 전혀 응답이 없다는 것에 대해서 더 문제제기를 하고 있다. 즉, 국내 기관들에서 사고대응이 이루어지고 있지 않다는 것을 많이 이야기하고 있었다.

사실, 국내 정보통신 운영기관에서 사고대응을 위한 전담조직이 갖추어진 곳이 그렇게 많지 않다. 대부분은 인력과 예산의 문제로 인해 대응이 이루어지고 있지 않고 있다.

그렇지만, 최근의 인터넷 환경의 변화는 각 기관에서 어떤 형태로든 사고대응팀의 구축이 필요하게 되어 가고 있다. 최초의 사고대응팀인 미국 CERT/CC가 탄생하게 된 계기가 된 "Morris 웜"과 유사하게 최근에 Ramen 웜, Li0n 웜, Adore 웜, Sadmind/IIS 웜, Code Red 웜 등 다양한 웜들이 출몰하고 있어, 그 어느 때 보다 사고대응팀간의 정보교류가 필요하게 되었다. 또한, CERTCC-KR에 접수되는 해킹사고가 '97년 64건, '98년 158건, '99년 572건, '00년 1,943건, '01년 11월 현재 4,949건으로 매년 3배 이상 가파른 증가세를 보이고 있어 CERTCC-KR에 의한 직접적인 사고대응이 한계에 다다르고 있다.

이러한 환경의 변화는 이제 국내 정보시스템 운영기관에서도 사고대응팀의 조직화를 요구하고 있다. 물론, 각 기관에서 가용한 인력과 예산, 그리고, 기관의 성격에 따라 사고대응팀의 구축형태와 제공되는 서비스가 달라질 수 있다.

본 고에서는 일반적으로 CERT팀 구축에 필요한 요소들과 CERT팀에서 제공되어야 하는 서비스에 대해서 알아보도록 한다.

본 고에서 사용되는 CERT(Computer Emergency Response Team), CSIRT(Computer Security Incident Response Team), IRT(Incident Response Team) 등의 용어들은 모두 침해사고대응팀으로 해석될 수 있다.

2. CERT팀 구축

본 장에서는 사고대응팀을 운영하기 위해 필요한 요소들과 사고대응팀 운영에 필수적인 기초정책, 연속성보장(continuity assurance), 보안 관리, 팀원관리 등 4가지 운영 이슈에 대해 알아보도록 한다.

2.1 CERT팀 운영에 필요한 요소들

2.1.1 업무계획 수립

먼저 CERT팀의 업무시간을 어떻게 할 것인지를 결정하여야 한다. 오전 9시에서 오후 6시까지 정상적인 근무시간에만 서비스를 제공할 것인지 아니면 365일 24시간 서비스를 제공할 것인지를 결정하여야 한다. 해킹사고는 근무시간, 근무외 시간을 구분하지 않고 발생되므로 가능한 24시간 비상연락될 수 있는 체제를 유지하는 것이 바람직하다. 하지만, 24시간 근무인력이 투입될 경우 많은 인력과 예산이 투입되는 것에 비해 업무의 효율성이 저하될 수도 있으므로 팀의 성격에 따라 결정하여야 한다.
일반적으로 정상적인 근무시간과 정상 근무외 시간의 업무계획도 달리 짜여져야 한다. 즉, 근무교대, 정상근무외 시간의 인력배치(경비원이나 상담서비스를 담당하는 상담원처럼), 백업 등을 고려하여야 한다.

2.1.2 전화통신 시스템

전화, 팩스, 휴대폰, 호출기, 자동응답기 등 전통적인 통신수단을 모두 포함한다. 통신방식은 팀의 임무와 서비스의 특성에 의존한다. 전화로 서비스를 이용하려고 할 때 4번 연속 통화가 되지 않는다면 이용자는 불쾌감을 느낄 수 있고, 긴급한 상황에서는 15분 이내에 연락이 오지 않는다면 불쾌감을 느낄 수 있으므로 신속한 연락이 될 수 있도록 하여야 한다.
또한, 전화번호는 서비스를 받는 기관이나 사람들이 암기하기 쉬운 특수 번호를 사용하는 것이 바람직하다. 가령 한국정보보호진흥원 해킹바이러스상담지원센터의 경우 02-118을 사용하고 있어 비상시에도 누구나 도움을 요청하기 편하다. 그리고, 휴일이나 근무시간 이외의 경우라고 하더라도 휴대폰을 Open하고 있어 직접적인 통화가 가능하도록 하는 것이 바람직하다.

2.1.3 전자우편(E-mail)

전자우편은 비동기적으로 정보를 교환하는 쉬운 기술이고, 수신된 전자우편의 우선순위에

따라 사용자들이 더 효율적으로 업무를 처리할 수 있다. 사실 대부분 전화통화로 소비하는 시간보다 적게 소모되나, 직접 통신을 대체하기는 힘들다.
그러나, 해킹사고의 경우 관련된 로그 등을 필요로 하는 경우가 많기 때문에 전화통신보다 많이 사용되고 있다. 또한 국제적인 해킹사고 처리의 경우에도 서로 다른 시간대에 직접적인 통화가 힘들므로 전자우편을 이용한 사고관련 정보를 교환하는 경우가 대부분이다.
따라서, 각 팀에서는 RFC2142에서 권과하고 있는 보안 메일계정 즉, security, cert, abuse 등을 사용하는 것이 바람직하다. 또한 사고관련 기관의 정보 및 관련 로그 등 중요 정보를 주고받을 경우 PGP 등을 사용하여 암호화하거나 신원확인을 위한 서명을 하는 것이 바람직하다.
다음은 호주 AUSCERT로 부터 접수된 해킹사고관련 E-mail의 예이다.

Subject: (AUSCERT#32978) Possible unauthorised connection attempts *from* your site
Date: Fri, 28 Sep 2001 09:46:16 +1000 (EST)
From: AusCERT Probe Reporter <probe-reply@auscert.org.au>
Reply-To: probe-reply@auscert.org.au
To: cert@cert.certcc.or.kr, abuse@abcd.co.kr
CC: auscert@auscert.org.au

Hi,

I am a member of the Australian Computer Emergency Response Team (AusCERT).
AusCERT provides technical information and liaison for computer security incidents within Australia and New Zealand. AusCERT provides services similar to the CERT Coordination Center that you may be familiar with.

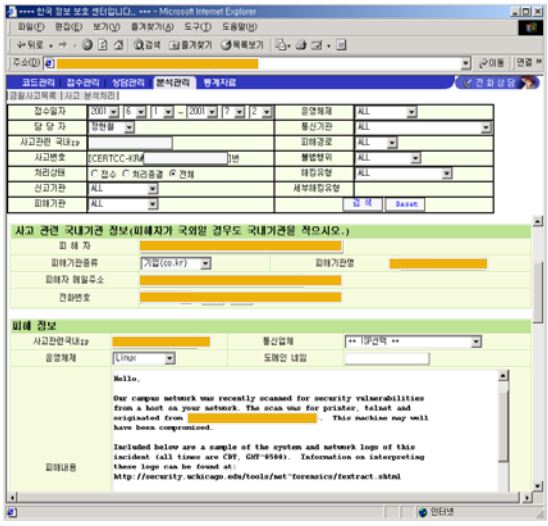
We have received a report of unauthorised connection attempts from your site. If you are not the correct person to be dealing with this incident, could you please contact the appropriate person with the details and inform us.

Please find the original message enclosed at the end of this email.

> source: xxx.xxx.245.12
> port: tcp 111
> timezone: GMT+0000 (Zulu Time)
>
> Logs:
> Name: xxx-xxx-245-12.rev.abcd.co.kr
> 20010927T045752 tcp xxx.xxx.245.12:4956 -> xxx.xxx.216.47:111
> 20010927T045801 tcp xxx.xxx.245.12:1311 -> xxx.xxx.223.34:111
> 20010927T045806 tcp xxx.xxx.245.12:1346 -> xxx.xxx.230.238:111
> 20010927T045807 tcp xxx.xxx.245.12:4157 -> xxx.xxx.234.227:111
> 20010927T045812 tcp xxx.xxx.245.12:1663 -> xxx.xxx.238.197:111
> 20010927T045813 tcp xxx.xxx.245.12:4300 -> xxx.xxx.243.6:111
> 20010927T045826 tcp xxx.xxx.245.12:3060 -> xxx.xxx.6.200:111
> 20010927T045827 tcp xxx.xxx.245.12:3523 -> xxx.xxx.7.10:111
> 20010927T045827 tcp xxx.xxx.245.12:3905 -> xxx.xxx.7.178:111
> 20010927T045829 tcp xxx.xxx.245.12:4942 -> xxx.xxx.10.203:111
> 20010927T045830 tcp xxx.xxx.245.12:3064 -> xxx.xxx.13.193:111
> 20010927T045837 tcp xxx.xxx.245.12:2405 -> xxx.xxx.19.0:111
> 20010927T045907 tcp xxx.xxx.245.12:4388 -> xxx.xxx.58.36:111

2.1.4 업무 관리 도구

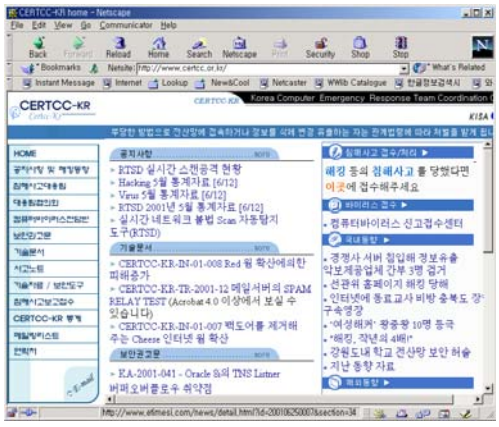
과도한 업무량과 교대 근무자가 있는 운영 환경에서는 업무흐름과 진행중인 업무를 수행하는데 도구의 사용이 필수적이다.
CSIRT은 전체업무에 사고, 요구사항, 분석 업무 등을 추가하고 검색해서 수정할 수 있는 데이터베이스 기반의 업무관리 소프트웨어가 필요하다. 모든 처리되는 정보를 모으고 각각 상호연결을 위해 전자우편, 웹, 전화 시스템을 통합하는 것이 필요하다.
(그림 1)은 CERTCC-KR에서 운영 중인 해킹바이러스 관리시스템으로 웹, 전자우편, 전화를 통해 접수되는 해킹바이러스 사고를 통합하여 관리하고, 정보의 검색, 분류, 통계자료작성에 활용하고 있다.



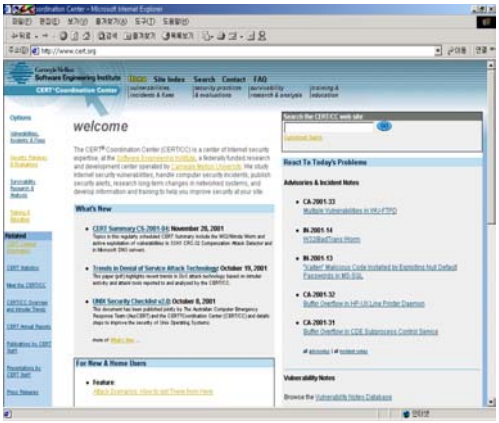
(그림 1) CERTCC-KR 해킹바이러스 관리시스템

2.1.5 홈페이지

웹은 현재 정보교류를 위해 가장 많이 사용되고 있다. 대부분의 상업 보안사이트와 다른 사고대응팀간에도 대부분 웹을 지원한다. 이런 사고대응팀의 웹서버나 다른 공개용 정보시스템은 비인가된 사용자의 조작으로부터 안전하게 관리되어야 한다. 침입차단시스템으로 보호하고, Tripwire나 MD5 같은 도구를 이용하여 주기적으로 무결성 점검을 할 필요도 있다. 사고대응팀의 공개 서버들은 해커들이 가장 해킹하고 싶어하는 시스템 중의 하나임을 명심하여야 한다.
(그림 2)는 CERTCC-KR의 홈페이지(www.certcc.or.kr)로 보안권고문, 기술문서, 사고노트 등의 최근 해킹바이러스 관련자료를 배포하고, 사고접수 창구역할을 한다. (그림 3)은 미국 CERT/CC 홈페이지(www.cert.org)이다.



(그림 2) CERTCC-KR 홈페이지



(그림 3) 미국 CERT/CC 홈페이지

2.1.6 IP 주소와 도메인네임

보안상 이유로 다른 모든 네트워크로부터 내부 네트워크를 분리하고, 사고대응팀에 할당된 IP 주소공간을 스스로 관리할 필요가 있다. 보안을 향상시키기 위해서 상위기관과 다른 주소 블록을 사용하거나 사설 주소(예를 들면, 10.0.0.0)나 NAT 혹은 모든 외부접속을 침입차단시스템에서 차단하는 등 다양한 방법으로 보안을 강화하여야 한다.
DNS(도메인 네임서버)에서는 특정 호스트에서 운영되는 운영체제 종류와 같은 민감한 정보와 모든 내부 호스트의 완전한 리스트를 제공해서는 안된다.

2.1.7 네트워크와 호스트 보안

IR 서비스를 하는 내부컴퓨터, 네트워크, 연결된 다른 네트워크의 환경설정이 안전해야 하고 공격에 보호되어야 한다. 내부 네트워크를 분리하고 외부로부터의 침입에 대해 침입차단시스템으로 보호한다. 최소한 두 개의 분리된 망이 존재해야 한다. 즉, 모든 서비스 업무를 수행하고 데이터가 저장되는 운영 네트워크와 비록 각종 취약점에 대한 테스트를 할 수 있는 테스트베드가 필요하다.

침입차단시스템 선택은 예산의 영향을 받을 것이다. 일반적으로 dual-screened 침입차단시스템이 보다 나은 보안레벨을 제공한다. CSIRT 이 운영하는 시스템은 항상 보안 패치와 최신 업데이트를 유지하여야 하며, Wrapper 나 다른 로깅도구로 사용자 식별을 하여 침입시도를 예방하여야 한다.
서비스거부 공격은 팀 업무에 지장을 초래할 수 있으므로 대책을 세워야 한다. 하나 이상의 네트워크 서비스 제공자에게 네트워크를 연결함으로써 문제를 해결할 수 도 있다. 또한 주요 네트워크 서비스가 막혀지더라도 이메일과 같은 최소한의 통신대책을 강구하여야 한다.

2.2 정책 및 지침

2.2.1 행동준칙(Code of Conduct)

행동준칙은 조직의 사명과 특성에 부합되도록 어떻게 행동해야 하는지를 기술한 전반적인 규칙의 집합이라고 할 수 있다. 행동준칙은 기관내 모든 스탭(스탭들의 태도)에게 적용된다. 행동준칙은 어떤 상황에서 어떻게 대처를 하고, 어떤 상호작용을 해야 하는지에 대해서 기본적인 지시를 제공한다. 팀 대내외적으로 어떤 상호작용을 해야 하는지도 기술한다.

다음은 한국정보보호진흥원 CERTCC-KR의 정책 개요이다.

Ⅰ. IRT 임무 및 구성

1. IRT 임무
2. 침해사고의 범위
   - 2.1 침해사고의 정의
   - 2.2 침해사고의 종류
3. 인력 구성 및 역할
   - 3.1 침해사고대응지원팀장
   - 3.2 침해사고 접수 담당
   - 3.3 침해사고 처리 담당

Ⅱ. 침해사고 접수 및 처리

1. 침해사고 접수
   - 1.1 침해사고 접수 수단
   - 1.2 국내 침해사고 접수
   - 1.3 국외 침해사고 접수
   - 1.4 침해사고 접수 처리
   - 1.5 바이러스 사고 접수
2. 침해사고 분석 및 처리
   - 2.1 지원 범위
   - 2.2 현장 지원 업무
   - 2.3 관련기관 연락업무
   - 2.4 침해사고 분석
   - 2.5 침해사고 처리
3. 사후 조치
   - 3.1 피해기관 보안 조치
   - 3.2 사후 침해사고 분석

Ⅲ. 침해사고 정보 관리

1. 인적 관리
2. 안전한 전자메일 사용
3. 기록 및 보관
4. 정보의 중요성에 따른 처리
5. 정보 공개

Ⅳ. 해킹기법 시험· 분석, 대책

1. 보안권고문 및 기술문서
2. 해킹기법 시험·분석
3. 해킹방지기술 연구

Ⅴ. 대외 업무

1. 조직내 각 IT 담당자
2. 관련 대외기관 담당자
3. CONCERT / 수사기관

Ⅵ. 내부 보안

1. 출입통제
2. 시스템 및 네트워크 보안
3. 재해 대책

2.2.2 정보 카테고리 정책

CSIRT는 정보의 카테고리 정책이 있어야 한다. 정보 카테고리 정책 없이는 CSIRT 팀원 각자 자신이 이해하는 카테고리에 정보를 저장하고 구별하지 않으려고 할 것이다. 개인적인 인지의 차이로 일관되지 못하는 결과를 초래하고 적절하지 못한 서비스를 제공할 수 있으므로, 카테고리의 가이드라인이 필요하다.

카테고리 정책의 복잡성과 사이즈는 팀의 임무와 구성원에 의존한다. 예를 들면 가장 간단한 경우는 민감한 정보와 일반정보로 나눌수 있을 것이다. 일반 정보는 공개적으로 취급되는 반면 민감한 정보는 특별히 주의해서 취급되어야 한다.

조금 더 정교한 스킴의 경우 팀내 내부정보와 동료 팀과 업무협조를 위해 알려야 할 필요가 있는 정보 마지막으로 외부에 공개할 정보로 카테고리를 정의할 수 있을 것이다.

2.2.3 정보 공개 정책

CSIRT의 경우 가장 중요한 이슈중의 하나는 다른 팀이나 이용자로부터 어떻게 신뢰를 얻고 이떻게 품위를 유지할 것인지에 노력할 필요가 있다. 신뢰와 존경없이 팀이 제 역할을 하지 못할 것이고 마지못해 정보를 보고할 것이다. 사고대응실무와 그에 상관된 정보공개 정책을 정의하는 것이 중요하다. 그런 정책없이 CSIRT 스탭은 전화에 답변하고 메일을 처리하는데 무엇을 언제 말해야 하는지 가이드가 없을 것이다.

대부분의 팀들은 모든 정보를 엄격히 보안을 유지하며 보고하고 팀원 범위 외에는 정보를 공유하지 않는다. 이런 가이드라인의 예외로 경향이나 통계를 목적으로 하거나 사이트나 정보를 공개하는 기관이거나 다른 기관에 연관된 기관의 경우는 예외다.(사고와 관련된 다른 사이트, 법적으로 공개, 사고 대응을 위해 다른 대응팀과 협조할 때)

2.2.4 언론 정책

언론정책이 있는 것이 좋다고는 확신할 수는 없다. 비록 상세한 정보 배포 정책이 있더라도, 언론을 상대하는 것은 힘들다. 가장 중요한 이슈는 언론 관련기관에 주요한 인터페이스를 어디로 할 것인가 하는 것이다. CSIRT를 내부나 외부로 할 것인가? CSIRT팀이나 관련된 팀들이 하는 고도의 기술과 민감한 데이터를 다루는 팀은 외부 언론 담당자가 있는 것이 바람직하다. 그러면 언론 담당자는 민감한 데이터가 없거나 접근할 수 없고, 언론정책과 정보 공개에 따라서 언론에 배포할 내용만을 숙지하면 된다.

2.2.5 보안정책

우선 CSIRT와 유사한 기관은 근본적으로 공격에 취약한 네트워크 환경이라고 간주해야 한다. 또한 CSIRT는 공격자가 좋아하는 공격대상이고, 중요한 위험요소를 명확히 해야한다. 공격을 자주 받는 팀은 대응능력이 떨어지고, 신속한 조치와 전문적인 대응을 할 수 없으면 신뢰성을 잃게 된다. 보안정책은 팀 컴퓨터, 네드워크와 다른 네트워크 연결등 모든 면을 고려하여야 한다.

- 물리적 보안
- 복구 계획(백업 등)
- 로컬 네트워크 보안
- 로컬 정보 보안

- 외부 통신 보안
- 로컬 보안 사고 처리
- 재난 대비, 비즈니스 연속성

2.2.6 인적 실수에 대한 정책

인간은 누구나 실수를 저지를 수 있다. CSIRT 스탭도 역시 인간이기에 실수를 범할 수 있다. 그들이 취급하는 정보에 대한 책임성과 고강도의 스트레스를 받는 환경에서 누구나 실수에 취약할 수 있다. 인적 실수 정책은 사람에 의해 발생하는 피해를 최소화할 수 있다. 이 정책은 스탭 멤버가 실수를 하였다면 좋지 못한 결과를 가져온다는 것을 명확히 해주어야 한다. 훈련이나 교육도 실수를 최소화할 수 있는 방안이다.

2.3 연속성 보장

일관된 연속성과 신뢰할 수 있는 서비스는 CSIRT의 성공적인 운영의 필수요소이다. 이것은 일관성에 의해서 인식된 능력과 팀의 신뢰레벨에 직접적인 영향을 미친다. 연속성 보장은 업무흐름 관리, 시간외 적용범위, 사이트외 적용범위 등 운영면에서 많은 중요한 일반적인 운영 이슈이다.

연속성을 위협할 수 있는 요인으로는 시간부족, 사원의 가용성 침해, 근무교대 전환, 기반요소 침해 등의 단기 위협요소들과 자금부족, 운영인력 부족 등의 중·장기적인 위협요소들이 있을 수 있다.

o 업무흐름 관리
IR 연속성 문제는 지속적으로 팀원들이 변화하는 근무조건(근무교대, 휴일, 업무순환, 이직)에서 오랜 기간동안 많은 문제를 취급하는 IR 팀들간에 발생될 수 있는데, 모든 문제, 사고, 인위 정보나 취약성에 관한 정보 등을 팀원이 언제든지 이용할 수 있어야 한다.

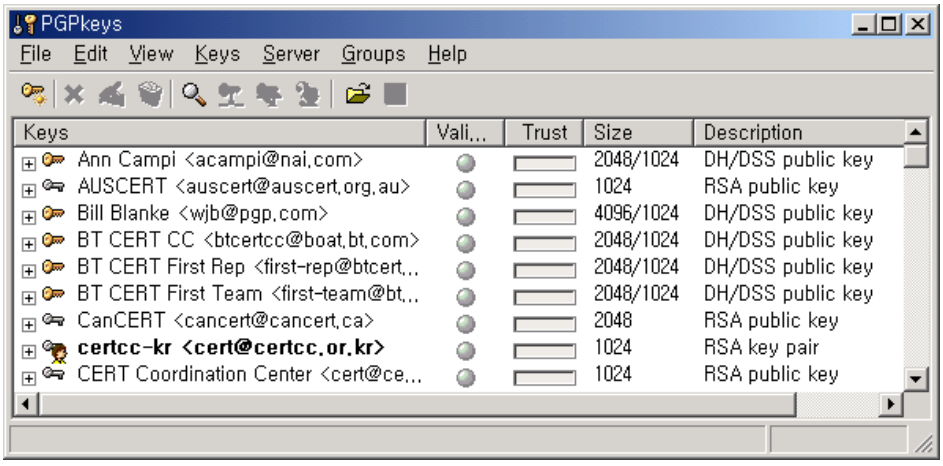
o 근무시간외 범위
업무 외 시간에 핫라인 호출시 누가 응답할 것인가에 대한 대책이 필요하다. 근무중인 팀원, 다른 스탭 멤버 혹은 음성메일 같은 응답서비스, 경비원, 통신회사에서 제공하는 콜센터 등 다양한 방법이 있을 수 있다.
업무 외 시간 호출에 대해서 휴대폰 등 핫라인 번호로 연결할 수 있지만 최소한의 숙직 근무자가 있는 것이 바람직하다.

o 근무지 외 범위
업무시간에 컨퍼런스 참석 등으로 인해 외부에 있을때 긴급상황이 발생할 수도 있는데, 이런 경우도 근무외 시간과 유사하게 정상적인 서비스가 지원되어야 할 것이다.

2.4 보안관리

2.4.1 암호와 전자서명 사용

암호도구의 사용은 모든 CSIRT에서 사용되어져야만 한다. 팀 내에서 컴퓨터 시스템 데이터를 보호하고 안전하지 못한 네트워크로 전송을 할 때 암호화를 사용한다. 팀과 기업 협력사간에 DES나 PGP 같은 일반적인 암호툴로 민감한 데이터(사고분석, 새로운 공격기법이나 동향 등)를 안전하게 통신할 수 있다.
CERTCC-KR에서도 국제간의 해킹사고에 대한 정보를 제공할 때 가장 많이 이용하는 통신수단이 전자우편이며, 사고기관 등 중요한 데이터를 포함한 정보를 주고받을 경우에는 PGP를 이용하여 암호화하고 있다.
(그림 4)는 PGP 키 목록으로 국외 CERT팀들의 공개키와 CERTCC-KR의 개인키/공개키 등을 볼 수 있다.



(그림 4) PGP Key 목록

다음 문서는 PGP를 설치하고 운영하는데 도움을 줄 수 있다.
http://www.certcc.or.kr/tools/PGP.html

그리고, CERTCC-KR의 PGP 공개키는 다음에서 구할 수 있다.
http://www.certcc.or.kr/teampub.txt

2.4.2 침입차단시스템과 네트워크 보안

이상적으로 팀의 네트워크는 잘 설계된 침입차단시스템으로 다른 네트워크와 분리된다. 다른 네트워크는 팀의 주 기관을 포함한다. 침입차단시스템은 완전한 솔루션은 아니고 네트워크를 통과하는 것에 대해 적절한 인증과 허가를 필요로 한다. 하지만 의심스러운 행위에 대해서 규칙적으로 로그화일을 점검하지 않는다면 침입차단시스템도 무의미하다.

2.4.3 로컬 호스트에 대한 원격 접속

집이나 이동 컴퓨터에서 작업시 전자우편이 있는 로컬시스템과 업무흐름 관리 툴에 접근할 수 있게하기 위해 특별한 주의가 요구된다. 일회용 패스워드에 의한 강력한 인증과 SSH 등을 이용한 암호화 통신이 요구된다.

2.4.4 물리적 보안

CSIRT가 자체 물리적 보안에서 모든 면을 구현하는 권한을 가지지 않을 수도 있다. 물리적 보안은 대개 상위 기관에 의해서 구현되고 있지만, 가능하면 CSIRT의 요구조건을 충족해야 한다. 잠금 정책, 문서정리 정책, 인가된 사용자와 방문객 점검 등도 고려하여야 한다.

2.4.5 재해 대책

파괴적인 네트워크 침입, 파괴, 화재나 다른 자연 재해 등 예상하지 못한 재앙의 경우 우선순위와 재해를 피해갈 수 있는 절차(무엇을 먼저 하고 누구에게 연락할 것인지)가 있어야 한다.

2.4.6 내부 보안사고 처리

대부분의 CSIRT에서는 내부 보안사고에 관해서는 내부적으로 조용히 처리하고자 할 것이다. 하지만, 사고가 외부 기관들과 연관되어 다른 사람들이 사고에 대해서 인식할 필요가 있을 경우에는 정보를 공개하여야 한다.

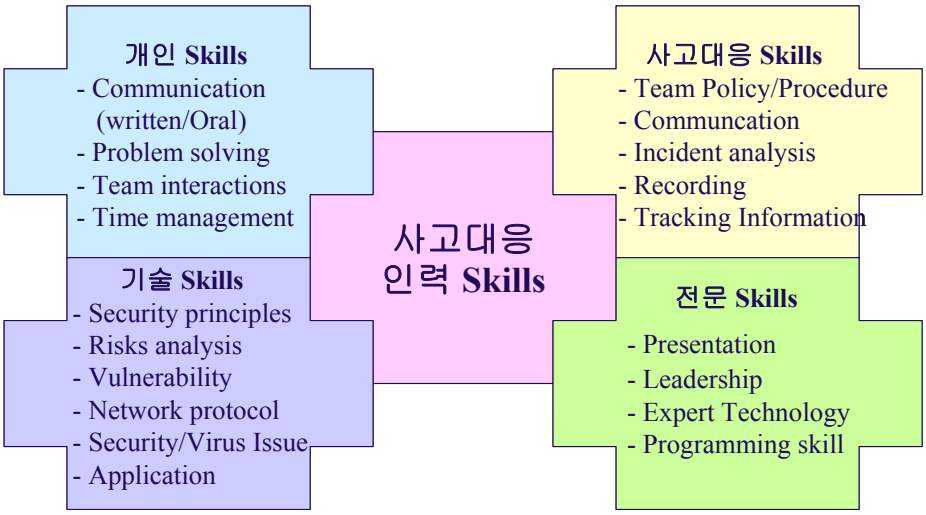
2.5 직원 관리

업무처리시 팀의 정책 및 절차를 효과적으로 수행하는 것은 전적으로 스탭의 능력과 신뢰성에 의존하게된다. 그러므로 CSIRT 스탭은 서비스 운영과 임무를 효과적으로 수행하는데 중추적인 역할을 한다.

2.5.1 사고대응팀 직원의 자질

대부분의 사람들이 CSIRT 스탭의 기술적인 경험을 가장 중요하게 생각할 수 있다. 기술적인 경험이 중요한 요소지만 중요한 판단 기준은 개인의 의지와 고객 및 다른 CSIRT와 업무협조시 절차 준수 능력이다. 고용시 기술적인 경험이 덜 하더라도 좋은 인간관계와 대화능력을 가진 사람을 고용하여 CSIRT 특정 기술을 교육하는게 더 바람직하다.

일반적으로 사고대응을 위한 전문인력은 (그림 5)와 같이 다양한 기술과 능력이 요구된다.



(그림 5) 사고대응 인력의 자질

사고대응 인력은 전문적인 기술력 뿐만 아니라 다음과 같이 유연한 대인관계 능력도 요구된다.

- 명확한 규정이 없거나, 스트레스를 받고 있거나 힘든 경우 효율적이고 타당한 판단을 할 수 있는 상식
- 다른 팀이나 의뢰자와 효율적인 구어, 문어 대화 능력
- 언론이나 협력기관 등 다른 기관과의 절충 능력
- 정책과 절차를 따르는 능력
- 지속적인 교육 의지
- 스트레스와 업무 부하를 견딜 능력
- 팀 업무협조
- 팀 명성과 품위를 지킬수 있는 품위
- 실수를 인정하는 태도
- 새로운 상황에서 효율적인 사고처리를 위한 문제해결 능력
- 일의 우선 순위를 관리할 수 있는 시간 관리 능력

기술적인 측면에서 각 사고 처리자는 기본적인 기술의 이해와 개인은 그들의 전문성에 기초를 두어야 하는데, 아래는 사고처리자가 갖추어야할 기술적인 요소들이다.

- 일반적인 데이터 네트워크(전화, ISDN, X.25, PBX, ATM, 프레임 릴레이)
- 인터넷
- 네트워크 프로토콜(IP, ICMP, TCP, UDP)
- 네트워크 기반 요소(라우터, DNS, 메일서버)
- 네트워크 응용프로그램, 서비스와 관련된 프로토콜(SMTP, HTTP, FTP, TELNET)
- 기본 보안 원칙
- 컴퓨터와 네트워크 위험 및 위협
- 보안 취약성과 관련된 공격(IP 속이기, 스니퍼와 컴퓨터 바이러스)

- 네트워크 보안 이슈(침입차단시스템 혹은 가상사설망)
- 암호 기술, 전자서명, 해쉬 알고리즘
- 사용자와 시스템 관리자 측면의 호스트 시스템 보안(백업, 패치)

2.5.2 입사와 퇴사 절차

CSIRT에서 취급하는 정보의 중요성 때문에 새로운 팀원의 입사와 팀을 떠나는 팀원에 대한 특별한 절차가 중요하다. 새로운 팀원은 상위기관에서 요구된 어떤 표준 근로 계약과 함께 CSIRT의 계약 동의가 필요하다. CSIRT의 동의서는 정보공개부터 네트워크 연결과 언론매체와의 범위를 포함한다. CSIRT 팀원의 퇴사에 앞서 퇴사절차와 다른 CSIRT 팀원과의 조치가 선행되어야 할 것이다. 퇴사 절차는 아래사항을 포함한다.

- 패스워드 변경
- 물리적인 보안 장비와 다른 미디어 반납(전화, 호출기, 백업장비)
- 키 반납
- 과거 실적 검토
- 퇴사자의 숙지사항 주지
- CSIRT 업무 관련자에게 통보
- 개인 연락처 기록

2.5.3 팀원 교육

팀원 교육은 새로운 팀원이 그들의 직무를 수행하기 위해 필요한 기술을 습득하거나 팀원 개인 발전을 위한 역량 강화와 새로운 기술과 공격자의 경향을 파악하는 전반적인 기술향상을 위해 필요하다. 팀의 전체적인 교육을 검토할 때 팀 전체의 일반적인 기술뿐만 아니라 각 팀원의 특성화된 기술을 구분하는 것이 중요하다.

교육과정에 아래에 열거된 항목이 포함되어야 한다.

- 새로운 기술 발전
- 내부 팀 정책과 절차
- 침입기술의 이해와 식별
- 관련 사이트와 통신
- 사고분석
- 사고기록 유지
- 팀 조직
- 업무 로드 분산과 조직화

2.5.4 직원 유지

경험이 풍부한 CSIRT 팀원은 많지 않고, 임금도 비싸다. 그래서 시간을 투자해서 선별하고,

고용하고, 교육시키는 것이 그들의 이직을 막는데 중요하다. 이직의 주된 두가지 이유는 과다한 업무량과 적은 급여이다.
높은 급여는 사람들의 관심을 끌기에 충분하다. 반면에 업무 만족도와 개인 성장 가능성을 제시함으로서 그들을 머물게 할 수도 있다. 팀은 근무환경뿐만 아니라 고급 팀원이 있는 팀 환경을 만듬으로써 이직을 막을 수 있다.

3. CERT팀에서 제공되는 서비스

3.1 사고대응팀 형태별 제공되어야 하는 서비스

정책과 지침 개발을 용이하게 하기 위해 CSIRT는 목적의 명확한 정의가 필요하다. 사고대응팀의 규모나 설립 목적에 따라 제공되어야 하는 서비스도 다를 수 밖에 없다. [표1]은 사고대응팀의 형태에 따라서 제공되어야 하는 서비스들을 정의하고 있다.

CSIRT 형태	임무(Mission)	가능한 사고대응 서비스 목적
국제 조정 센터	다른 CSIRT들의 조정자 역할을 통하여 컴퓨터 보안 위협을 전망하는 지식 베이스를 보유한다.	-전 세계의 CSIRT와의 조정기능을 통하여 컴퓨터 사고대응을 지원하기 위한 기술적인 지원을 제공한다. -사고대응활동을 통하여 현재 일어나고 있거나 잠재적인 침입자의 위협을 찾아내고 기술적인 상세설명을 문서화한다. 침입자의 위협에 대해 탐지, 예방, 복구할 수 있는 정보를 만든다.
국가 팀	컴퓨터 보안 위협에 대한 국가 연락처 역할을 유지하고 해당 국가의 시스템에서 공격하거나 목표가 되는 사고들을 줄이고자 하는 임무를 가진다.	-해당 국가에서 발생되는 컴퓨터 보안사고에 대한 기술적 지원을 제공한다. -취약점에 대한 탐지, 예방, 복구에 대한 기술적인 정보를 제공한다. -국가 법 집행기관의 연락책 역할을 한다.
네트워크 서비스 제공자 팀	고객들에게 접속을 위한 안전한 환경을 제공한다. 고객들의 컴퓨터 보안사고와 관련하여 효과적인 대응을 제공한다.	-컴퓨터 보안사고 대응을 위한 기술지원을 제공한다. -네트워크 인프라의 보안을 보장해 준다. -국가 팀들의 연락책 역할을 수행한다.
IT 공급자	해당 제품의 보안을 개선한다.	-취약점들에 대응하기 위한 기술적인 지원을 제공하고 CSIRT들과 협력하여 사고의 근본 원인을 분석한다. -취약점을 발견해 내고 새로운 패치를 만들어 낸다.
기업	기업의 정보인프라의 보안을 강화하고 침입의 결과로 발생되는 손실의 위협을 최소화한다.	-기업내의 시스템/네트워크 관리자와 사용자들에게 사고대응 센터 역할을 수행한다. -사고 시스템을 격리시키고 침입자의 위협으로부터 복구하기 위해 on-site 기술지원을 제공한다.

[표 1] 사고대응팀 형태에 따른 서비스의 목적

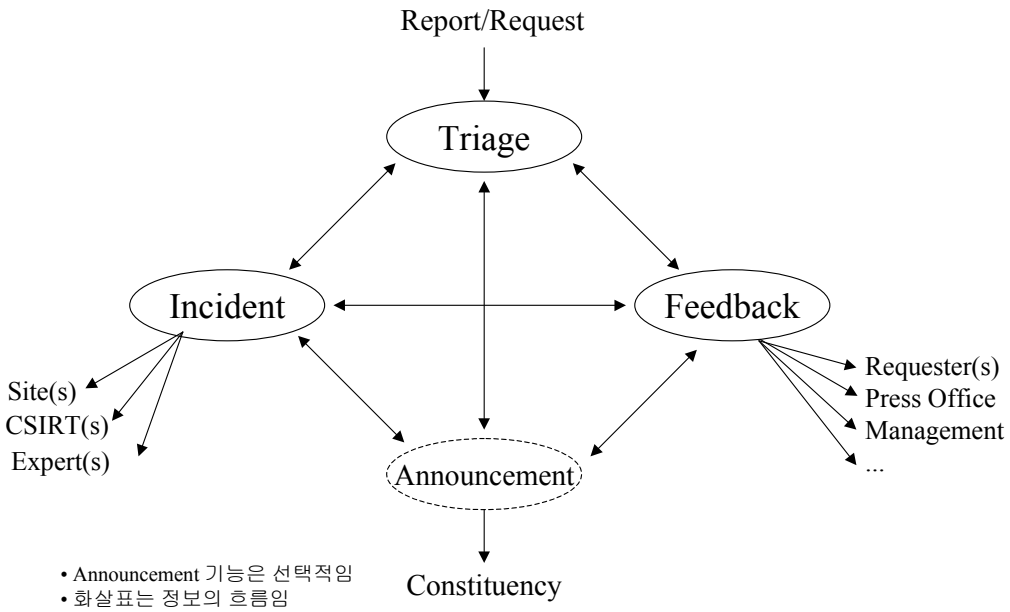
3.2 일반적인 서비스 개요

사고대응팀에서 제공되는 서비스는 크게 두가지로 나눌 수 있다. 첫 번째 서비스는 실시간으로 제공되어야만 하는 서비스로써 "사고대응(Incident Response)" 서비스이다. 이는 사고대응팀에서 반드시 제공되어야 하는 서비스이다. 두 번째 서비스는 "사전 활동(Proactive Activities)"으로써 이는 모든 사고대응팀에서 반드시 제공해 줄 필요는 없으며, 인력과 기술력에 따라 선택적으로 제공할 수도 있다.

"사고대응" 서비스는 일반적으로 사고 리포트를 접수하여 다른 사고대응팀이나 ISP들 또는 다른 사이트들과 협력하여 이 사고를 지원하는 업무라고 할 수 있다. 또한, 사고를 당한 사이트가 복구할 수 있도록 돕는 업무도 "사고대응" 서비스에 속할 수 있지만 이 또한 모든 사고대응팀에서 반드시 필요한 것은 아니고 선택적이다.

"사전 활동"은 일반적으로 취약점, 패치정보 또는 대응책을 제공하는 등의 정보제공 서비스나, 보안교육, 제품 평가, 사이트 보안 감사 및 컨설팅 등의 업무가 여기에 속할 수 있다.

사고대응팀에서 제공되어야 하는 서비스를 좀 더 세분화 하면 "사고대응" 서비스에는 선별(triage), 사고(incident) 기능으로 나눌 수 있고, "사전 활동"에는 알림(announcement)와 피드백(feedback) 기능으로 나눌 수 있다. 많은 CSIRT 팀들은 (그림 3)과 같은 기능 설계와 일치하지만 각 기능을 구현데 있어서는 상당히 다를 수 있다. 이러한 차이점은 사고대응팀의 자금, 가능한 전문가, 또는 조직 구조와 같은 요소들에 의해 나타난다.



(그림 3) 사고대응팀이 제공하는 서비스 관계

3.3 선별 기능

연락의 단일 창구 역할을 제공하고, IR 서비스를 위해 들어오는 정보를 접수(accepting), 수집(collecting), 정렬, 전달하는 기능을 제공한다. Tracking 번호가 새로운 사건에 할당된다. triage 기능은 문서보관, 전송, 또는 장치변화 등과 같은 추가적인 절차도 담당한다.
이 기능의 목표는 IR 서비스의 모든 정보는 적당한 재분배와 서비스 내에서 처리되기 위해 email, fax, 전화, 우편 등 집수 수단에 상관없이 단일한 창구를 통하는 것을 보장하는 것이다.

triage 기능을 지원해주고, 다른 단계에서 정보의 질을 향상시키는데 도움을 줄 수 있는 수단이 할당번호(tracking number), 표준화된 보고형식, 미리 등록된 연락처(pre-registration of contacts) 등이 있다.

3.3.1 할당번호 사용

만약 한 팀이 할당번호 체계를 사용하고 다른 사람들이 이 번호를 차후의 모든 대응에서 사용하도록 한다면, triage 과정은 대단히 편리하게 될 것이다. 할당번호는 email의 제목이나 Fax의 표지 또는 정해진 음성 메시지에 쉽게 사용될 수 있다.

할당번호는 IR 서비스의 각 기능에서 사건을 추적하는데 사용되어져야 한다. 각기 다른 서비스에는 다른 prefix가 사용되어야 한다. 외부와의 통신에서는 할당번호의 일부에서 해당 팀 소유의 번호임을 알려야만 한다. Feedback, incidents 그리고 announcement는 자신의 고유한 할당번호를 가져야만 한다. 예를들어, CERT/CC는 prefix 식별자로 incident에는 CERT#를 feedback에는 CERT-INFO#를 할당번호로 사용한다.

할당번호 요구사항의 가장 기본은 유일해야 한다는 것이다. 일반적으로 팀들은 할당번호의 번호체계로 미리 정의된 정수의 범위를 사용한다.
DFN-CERT는 1에서 65,535 사이의 번호를 사용하고, 한번 할당된 번호는 재사용하지 않는다. 한국정보보호진흥원 CERTCC-KR의 경우, 해킹사고에 CERTCC-KR#YYMMxxxx와 같은 사고번호를 부여하고 있다.

할당번호는 팀의 외부 통신에 사용되기 때문에 공개 정보로 간주되어야 하고 호스트나 도메인 이름 등과 같이 민감한 정보가 포함되어 공개되어서는 않 된다. 할당체계에서 다른 민감한 정보 즉, 보고된 숫자, 속성, 사건의 범위를 가리키는 정보를 포함하지 않기 위해서 난수생성 기법이 사용되기도 한다.

3.3.2 표준화된 보고 양식의 사용

표준화된 보고양식은 완전하고 적당한 정보를 제공하는 것을 용이하게 한다. 이러한 용이성은 새로운 보고에 대한 시기적절한 인식과 적당한 기능으로의 정보 전달, 차후의 진행을 좀 더 쉽게 할 수 있도록 한다. triage 기능과 incident 기능 자체 모두를 지원하기 위해 incident 보고 양식이 일반적으로 요구된다.

- 보고하는 사이트와 이 사고와 관련되어 통신하는 다른 집단들의 연락 정보
- 사고와 관련된 호스트의 이름과 네트워크 주소
- 사고에 대한 설명
- 사고와 관련된 세부 로그(time-zone 정보 포함)
- 이미 할당되었다면 그 할당번호

다음은 CERTCC-KR에서 사용하고 있는 침해사고 접수 양식이다.

신고기관 정보							
기관 이름							
신고자 이름							
전화번호							
E-mail							
호스트 정보							
IP주소							
호스트명							
운영체제							
사고에 대한 설명							
사고발견 경위, 피해현황 등							
유관기관 신고여부							
신고하지 않음		검찰청		경찰청		국가정보원	

[표 2] CERTCC-KR의 사고접수 양식

3.3.3 미리 등록된 연락처

보고 양식의 사용과 더불어 팀 관할구역의 크기와 속성에 따라 triage 기능에 도움이 되는 정보를 미리 받아두는 것도 가능하다. 이 과정은 다른 집단 즉, 다른 CSIRT들이나 법집행 기관 등의 정보로 확대할 수도 있다. 유용한 사전등록 항목은 다음과 같다.

- 신뢰된 연락처와 관련 연락정보(최소한 일년마다 주기적으로 검증되어야 한다.)
- 정보 공개 제한
- 정보교환을 위한 암호화와 사인을 위한 키들

3.4 사고 기능

컴퓨터 보안 사고라고 의심되거나 확실한 사건에 대해서 지원하고, 가이드를 제공한다.
"대응(response)"라는 말의 정의는 팀의 사고에 대한 정의와 개별 팀의 IR 서비스의 목적에 따라 팀마다 대단히 다양하다. 또한 다른 요소들도 고려해야 될 사항들이 있는데 가장 중요한 것이 특정 사고 양식에 우선순위와 관련된 사이트의 연관관계를 고려하는 것이다.
이 기능의 목표는 컴퓨터 보안사고 보고에 대한 대응을 제공해 주는 것으로 최소한 보고처(Reporting point), 분석(Analysis), 통지(Notification) 등 세 가지 속성들을 제공해주어야 한다.

사고 기능	사례
보고처	- 관할구역에 영향을 미치는 보고를 수신하여 처리하고, 관할구역 내의 관련 사이트들에게 전달한다. - 관할구역으로부터의 보고를 처리하고, 관련 사이트나 외부 CSIRT 등 관련기관에 전달한다.
분석	- 로그파일 분석 - 영향을 받는 사이트 파악 - 기술문서나 권고문을 알림 - 기술적인 지원 제공 - 임시대책이나 해결책 제공 - 현장 지원 제공
통지	- 적당한 연락처를 제공하거나 연락하는데 도움이 되는 자료를 알림 - 적당한 연락처 목록을 제공 - 사고와 관련된 다른 집단과 연락업무를 수행 - 관련된 다른 집단과 법 집행기관과의 연락업무를 수행

[표 3] 사고 기능 속성별 사례

사고분석은 다음의 두 가지로 분류할 수 있다.

○ 단일사고 내에서의 분석
특정 사고를 고려한 분석으로써 일반적인 형태는 아래와 같다.
- 로그파일 분석
- 공격자의 행위에 의해 남겨진 자료(artifact) 분석
- 사고가 발생된 소프트웨어 환경 분석
- 사고 내의 web-of-trust 분석

○ 사고간의 분석
사고간의 관계를 고려한 분석으로써, 진행중인 사고의 구조 분석이라고 할 수 있다. 이 분석은 일치하거나 관련이 있는 공격자의 출처를 가진 별개의 사건들 사이의 연관성을 찾기 위해서이다.

3.5 알림 기능

현재의 위협들과 이러한 위협을 방어하기 위한 절차, 그들에게 보고된 최신 공격 동향에 대한 정보를 작성·배포하는 기능이다.
Announcement는 진행중인 활동의 특정 형태와 관련된 단기 정보를 제공하는 것에서부터 인식과 시스템 보안을 강화할 수 있는 장기 정보를 제공하는 것에 이르기까지 다양한 형태가 있다.

■ Heads-up
일반적으로 짧은 메시지 형태를 취하고, 상세한 정보가 불가능할 때 사용한다. 가까운 미래에 중요할 것 같은 무엇인가에 대한 정보를 제공하는 것을 목적으로 한다.

■ Alert
경보는 최근의 공격, 계속되는 침입, 새로운 취약점에 대한 정보를 단기 통지이다. 사고노트(Incident Notes), 취약점노트(Vulnerability Notes) 등이 경보에 속한다.

■ Advisory
권고문은 인식을 높이거나 사고를 피하는데 도움을 줄 수 있는 문제점들과 해결책들에 대한 중장기 정보이다. CERT 권고문을 예로 들 수 있다.

■ For Your Information
중장기 정보로써 권고문과 유사하지만 포괄적인 독자들 즉 이러한 주제를 처음 접하거나 관리자층, 언론 매체와 같은 사람들을 대상으로 좀더 짧고 기술적이지 못한 문서이다. CIAC 노트가 여기에 속한다.

■ Guideline
기본 지식을 가진 사람이 시스템 및 네트워크 보안을 개선할 수 있도록 이끄는 일련의 절차를 기술한 문서이다. "Site Security Handbook[RFC 2196]"과 "CERT Security Improvement Modules"들이 여기에 속한다.

■ Technical Procedure
전문가 집단을 독자층으로 하는 좀더 기술적으로 상세한 지침을 말한다. "Problems With The FTP PORT Command"와 같은 CERT Tech Tips가 여기에 속한다.

3.6 피드백 기능

특정한 사고와 직접적으로 관련이 없는 사건에 대해서 feedback을 제공한다. Feedback은 명확한 요구에 의해서 일어날 수도 있고, (연차보고서와 같이)정기적으로 또는 케이스별로 요구되지 않고서도 제공될 수 있다.

사고대응을 위해 반드시 필요한 것은 아니지만 사고대응업무와 직접적으로 무관한 요청이나 이슈들도 팀에 요구된다. 이러한 요청들과 이슈들을 무시하게되면 팀에 대한 평판과 관할구역 내의 사람들이 팀을 대하는 태도가 나빠질 수도 있다. 따라서 모든 CSIRT들은 이러한 요청들에 어느 정도 수준으로는 피드백을 제공할 필요가 있다.

다음은 일반적으로 접수되는 요청들이다.

■ 일반적인 컴퓨터 보안 요청
일반적으로 사고예방 차원에서의 정보를 찾거나 만일 사고가 발생했을 때 CSIRT와 어떻

게 연락할 수 있는지에 대한 문의이다.

■ 언론 요청

일반적인 보안 기사나 특정 사고에 관련된 이야기의 소재를 찾고자하는 언론사 기자로부터의 요청이다. CSIRT는 팀의 정보공개 정책을 침해하지 않는 범위내에서 언제든 언론에 대응할 수 있도록 준비하여야 한다.

■ 그외의 요청과 이슈들

피드백을 바라는 다른 요청과 이슈들도 있다. 가령 컨퍼런스에서 강사 지원을 요청하거나 팀에서 만든 자료를 사용할 수 있도록 허락을 요청할 경우도 있다. 이러한 요청들은 팀에 대한 인식을 개선하는데 도움을 줄 수 있으므로 무시해서는 않 된다. 연차 보고서와 같은 명확히 피드백이 요구되지 않는 이슈들도 이 분류에 속한다.

■ 들어줄 수 없는 요청(out-of-scope requests)

이러한 요청들은 팀에 의해 제공되는 IR 서비스에서는 지원하지 않는다. 하지만 FAQ를 참조하거나 범위 밖의 요청에 대한 정책을 일러주는 것이 그 요청을 단순히 무시하는 것보다는 바람직하다.

요청에 대한 응답은 개별적으로 처리될 수도 있지만 시간이 많이 소모될 수 있다. 따라서, 자주 요청되는 문의들에 대해서는 FAQ(Frequently Asked Questions)를 만들고, 접수되는 요청들에 대해 적당한 문서를 복사하거나 어디에 있는지 가르쳐줌으로써 간단하게 처리할 수 있다.

4. 결론

급증하는 해킹사고와 하루가 다르게 발전하는 해킹기술은 각 정보시스템 운영기관에서 사고대응을 하기 위한 전담조직이나 인력을 요구하고 있다.

국내의 경우 초고속 인터넷 망 보급률이 세계 몇 위라는 등 네트워크 인프라 구축에는 성공하였지만, 이 인프라를 안전하게 보호하기 위한 대책이 마련되어 있지 않은 실정이다. 국내 보안산업의 활성화로 인해 이제 웬만한 기관에는 Firewall이나 IDS와 같은 보안장비를 갖추게는 되었지만, 실제 이를 운영하고 사고가 발생했을 때 대응할 수 있는 인력이 대단히 부족한 실정이다. 이로 인해 해외 네티즌으로부터 한국의 보안 후진성에 대해 질타받기도 한다.

본 고에서는 해킹사고 대응을 위한 사고대응팀을 구축하고 운영하는데 필요한 요소들과, 사고대응팀에서 제공되어야 하는 서비스들에 대해서 알아보았다.

본 고에서 살펴본 사고대응팀 운영을 위한 요소들과 서비스들은 각 팀의 인력, 자금력, 팀의 목적 등에 따라 달라질 수 있다. 인터넷 서비스를 제공해주는 ISP의 경우에는 CERT팀을 구축하여 고객들에게 안전한 네트워크 인프라를 제공하고, 고객의 침해사고관련 지원을 해주어야만 한다. 하지만, 작은 기업에서 해당 기업내의 보안만을 담당한다고 할 경우에는 CERT팀과 같이 거창한 전담조직을 둘 필요까지는 없을 것이다.

그렇지만, 조직의 규모나 목적에 상관없이 반드시 갖추고 있어야 할 것이 있다.

그것은 대내외적으로 침해사고와 관련된 정보를 주고받을 수 있는 공식적인 채널이 마련되어 있어야 한다는 것이다. RFC2142에서는 보안과 관련한 메일 주소를 다음과 같이 사용하기를 권고하고 있다.

security@domain.name	보안관련 사고 담당자 메일 주소
cert@domain.name	보안관련 사고 담당자 메일 주소
abuse@domain.name	네트워크 오용 담당자 메일 주소

최근 국내침해사고대응팀협의회(CONCERT, CONsortium of CERTs)를 통하여 국내 CERT팀을 활성화시키고, 팀들간의 네트워크를 구축하려고 노력하고 있다.
하지만 아직 CEO의 인식부족, 예산 및 인력 부족 등 다양한 이유로 인해 각급 기관의 CERT팀이나 보안전담자가 조직적으로 활동하고 있지 못한 실정이다.
그렇지만, 최근 CodeRed, Nimda 등 대규모 피해를 입히고 있는 해킹바이러스의 사례는 각 기관에 사고대응 전담팀의 필요성을 다시금 일깨워주고 있다. 최초의 CERT팀인 미국 CERT/CC가 발족하게된 계기도 최초의 인터넷 웜인 "Morris 웜"의 발생에 의해서 였다. 최근 각종 인터넷 웜이 우후죽순으로 발생되고 있는 인터넷 환경에서는 신속한 정보교류와 상호대응이 무엇보다 요구된다.
이제 우리나라도 네트워크 인프라의 수준에 걸맞는 보안수준과 사고대응체계를 갖추어야 할 때라고 생각된다.

참고문헌

[1] Moria J. West-Brown 외, Handbook for Computer Security Incident Response Teams(CSIRTs), 1998

[2] Security of the Internet, http://www.cert.org/encyc_article/tocencyc.html

[3] AirCERT Background and Motivation http://www.cert.org/kb/aircert/motivation.html

[4] Expectations for Computer Security Incident Response (RFC 2350) (www.ietf.org), http://www.ietf.org/rfc/rfc2350.txt

[5] Forming an Incident Response Team (www.auscert.org.au) http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html

[6] Avoiding the Trial-by-Fire Approach to Security Incidents (interactive.sei.cmu.edu) http://interactive.sei.cmu.edu/Columns/Security_Matters/1999/March/Security.mar99.htm

[7] NIST Incident Handling Information and Publications (csrc.nist.gov) http://csrc.nist.gov/topics/inchand.html

[8] CERT/CC, http://www.cert.org

[9] CERTCC-KR, http://www.certcc.or.kr