情報保護學會論文誌
第19卷 第4號, 2009. 8

# 심리적 보안관점에서의 사이버범죄 프로파일링

임 채 호,[1†] 김 지 영,[2‡] 최 진 혁[3]
[1]NHN(주), [2]NHN Business Platform(주), [3]한국기업보안협의회

# Profiling of Cyber-crime by Psychological View

Chaeho Lim,[1†] Jeeyoung Kim,[2‡] Justin Jin-Hyuk Choi[3]
[1]NHN Corporation, [2]NBP Corporation,
[3]Korea Corporate Security Managers' Council

요 약

사이버범죄는 인터넷 가상공간이 사회 전반으로 광범위하게 확대되면서 공격 기술력을 과시하려던 의도에서 최근에는 영리와 일반적인 목적의 범죄로 변화하고 있다. 신택스(Syntax) 기반의 탐지 분석이 가능한 네트워크 및 시스템 공격이 아닌 시맨틱(Semantic) 기반으로 수동적인 탐지와 대응을 요하는 콘텐츠 이상의 공격에 의한 인터넷 사기와 명예훼손, 개인정보 침해, 저작권 침해 등이 일어나고 있다. 시맨틱 기반의 범죄는 컴퓨터 이용자, 즉 인간의 내면적인 취약성을 이용하는 심리적 요인에 근거한다. 이 논문에서는 공개된 사이버범죄를 분석 후 사회적 영향력과 기술적 영향력으로 분류하고 사이버범죄의 심리적 관점에서의 프로파일링 방안을 연구하여 사이버범죄를 그 발생 수에 의하여 분류하였고, 이를 통하여 결국 범죄의 분석과 대응에 소요되는 시간을 줄이는 계기가 될 수 있음을 보이고 있다.

ABSTRACT

Internet is in rapid growth from technology to total social environment, so technical and syntax based cyber crime is evolved but also psychological and semantic based one is showing. In this paper, we analyze the cyber-crime cases announced by police, then classify it into social and technical influence. After that, we study the profiling method on psychological view point of cyber-crimes. We expect that it is possible to classify cyber-crimes into the categories rapidly and take less time to analyze and response.

**Keywords:** Cyber-crime, Social engineering, Psychological view

## I. 개 요

인터넷 강국인 우리나라는 인터넷 해킹이 1990년 초부터 매우 활발하였으며, 2000년 초부터는 본격적인 악성코드의 천국으로 발전하였다. 그리고 사이버범죄가 본격적인 사회문제가 되기 전인 2000년 초반, 경찰청에서는 사이버테러대응센터를 설립하여 본격적으로 사이버범죄에 대한 대응을 시작하였다[1].

역대 사이버범죄는 해커들을 컴퓨터 도사라고 지칭할 정도로 기술력이 매우 뛰어난 사람이 저지르는 하이테크 범죄였으나, 현재는 인간 심리나 내면의 정신적인 취약성을 공격하는 사회공학적 사기에 의한 범죄가 늘고 있으며 이러한 변화는 주로 돈을 벌려는 경제적 목적에 의한 것이다[2-4].

개인정보 침해는 개인정보 자체가 돈으로 환매할 수 있으므로 범죄자의 손쉬운 범행 목적이 되었고, 그 범죄에 필요한 기술적 방안은 타인을 매수하거나 고용하면서 해결되기도 한다. 결국 범죄자의 의도에 따라 필요한 기술은 어디서나 누구나 고용할 수 있는 상황으로 변한 것이다[5].

사이버범죄를 수사해야 하는 사법당국도 그 동안은 기술적 기반을 확보하려고 노력하였고, 이제는 충분할

접수일(2009년 1월 2일), 수정일(2009년 5월 22일), 게재확정일(2009년 7월 28일)
† 주저자, chlim@nhn.com
‡ 교신저자, jy.kim@nhn.com

정도가 되었다. 하지만, 사이버범죄의 유형이 변하면서 이제는 심리, 즉 사기기법에 의한 범죄를 더욱 분석 조사해야만 범죄사회의 급격한 변화에 대응할 수 있게 되었다.

이 논문에서는 경찰청 사이버테러대응센터에서 보고한 사이버범죄 중 심리적 요인에 의한 범죄를 대상으로 사이버범죄의 '일반' 범죄 중 사회적 영향력을 기준으로 분류하여 이러한 심리적 요인에 의한 범죄도 기술력을 응용할 뿐이라는 관점에서 사이버범죄의 프로파일링 모델을 제안한다. 이 모델을 적용한 분석결과를 통해 기술적 범죄 보다 시맨틱 범죄가 더욱 많음을 증명하고자 한다.

## II. 사이버범죄 현황

### 2.1 사이버범죄의 정의

사이버범죄는 "컴퓨터 통신 등을 악용하여 사이버 공간에서 행하는 범죄로 인터넷과 같은 정보 통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 한 사이버 공간을 이용하여 공공복리를 저해하고, 건전한 사이버 문화에 해를 끼치는 행위이다. 사이버범죄는 짧은 시간 안에 불특정 다수에게 많은 악영향을 미친다. 그러나 사이버 공간이라는 특성상 정보 발신자의 특정이 어렵고, 전자 정보의 증거 인멸 및 수정이 간단하기 때문에 범죄 수사에 어려움이 많다.

범행 목적에 따라 사이버 테러형 범죄와 일반 사이버범죄로 나뉜다. 사이버 테러형 범죄는 해킹, 컴퓨터 바이러스와 같은 유형의 범죄이고 일반 사이버범죄는 사이버 명예훼손과 전자상거래 사기, 개인정보 침해, 불법 사이트 개설, 디지털 저작권 침해 등을 말한다. 사이버범죄는 국내·국외에서 동시에 발생할 수 있는 특성이 있는데, 이에 대처하기 위해 국가 간 법·제도의 상이성을 초월한 국제적인 형사 사법의 규칙도 필요하다[6]."

미국의 사이버범죄수사국이 규정한 사이버범죄는 1)컴퓨터 침해, 2)패스워드 불법거래, 3)저작권 침해(소프트웨어, 영화, 음악), 4)업무상 비밀의 절도, 5)상표위조, 6)통화위조, 7)아동 포르노그라피 또는 착취, 8)메일 연계를 갖는 아동 착취, 9)인터넷 사기, 10)인터넷을 통해 타인을 괴롭히는 행위, 11)인터넷 폭탄 협박, 12)인터넷 상에서 폭발물·무기 거래 등으로 분류한다[7].

국내 경찰청 및 검찰청의 분류는 [표 1]과 같다[1].

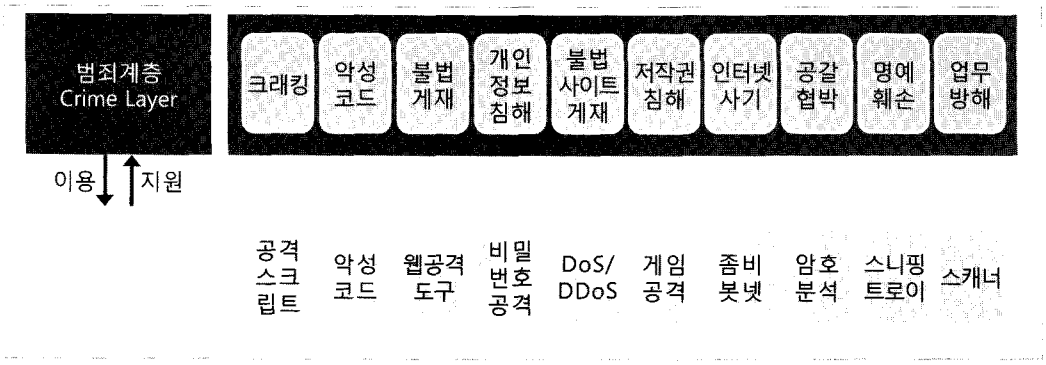
### 2.2 사이버범죄와 기술

사이버범죄는 기술적인 능력을 가진 해커나 크래커 집단이 아닌 금전적 목적의 범죄자나 범죄 집단에 의한 행위의 결과물로 변하고 있으며, 기술적 능력을 가진 집단은 범죄자들의 하수인에 불과한 경우가 늘고 있다[8].

사이버범죄 유형과 여기에 사용되는 기술력의 유형

[표 1] 경찰청·검찰청의 사이버범죄 분류

| 구분 | 사이버범죄 | 설명 |
|---|---|---|
| 테러형 | 해킹 | 컴퓨터 시스템 불법 침입, 파괴 등에 의한 크래킹, 중요 정보의 위변조 및 삭제 유출 |
| | 악성코드 | 사회 기반시설에 대한 사이버 테러, 바이러스 유포, 메일폭탄 등을 이용한 기반시설의 정보통신시스템 파괴 |
| 일반형 | 불법자료 게재 | 음란·폭력물 게시 유통 |
| | 개인정보침해 | 공공·개인정보 오남용, 인터넷을 이용한 신용 정보 및 공공 정보의 유출 |
| | 인터넷범죄 | 스토킹, 인터넷 스와핑, 매매춘, 사기, 도박 |
| | 불법복제 | 지적 재산권 침해, 소프트웨어, 웹 콘텐츠, 인터넷의 전자문서 무단전제·도용 |
| | 전자상거래 침해 | 전자상거래 상의 문서 위변조, 허위정보 입력 |
| | 인터넷 사기 | 통신을 이용한 사기, 물품 판매 사기 |
| | 명예훼손 | 공인에 대한 명예훼손, 악성루머 유포 |
| | 협박·공갈 | 부당 이익 추구를 위한 협박, 공갈 |




〔그림 1〕 범죄와 기술

은 〔그림 1〕과 같다.

예를 들어, 보이스피싱, 개인정보유출, 금융기관 해킹, 온라인 게임머니 해킹, DDoS 공격으로 인한 협박, 스팸메일 등 전형적인 금전을 노린 범죄이며 대다수가 기술자를 이용한 사례들이다[1].

- 맥마피아는 조직폭력단이 국제화되고 있음을 상기시키며, 보이스피싱 사기를 하고 청소년들에게 해킹기술을 학습시키고 있다[9].
- 국내 대부업체는 국내 인터넷을 해킹한 중국 해커로부터 개인정보 900만 건을 사들여 대출 권유 스팸 전화를 시도하였다.
- 2008년 3월, 국내 모 증권회사 등 국내 기업 7개 업체에 트래픽 과부하를 통해 서비스를 방해, 정지시키고 이를 미끼로 협박하여 550만 원의 돈을 뜯어내었다.
- 인천 모 저축은행을 해킹한 J모 씨와 공모한 국내 일당을 구속하였는데 이들은 970만 건의 개인정보를 유출하였다.

### 2.3 사이버범죄의 변화

이러한 사이버범죄와 심리적 관점을 바탕으로 새롭게 개인정보보안과 사이버범죄를 보기 시작한 모델이 소개되었고 이를 〔표 2〕에서 설명하고 있다. 이는 ISO/OSI 7계층 구조처럼 보안을 7개 계층적 모델로 소개하고 기술적 관점만이 아닌 심리적 계층에 의한 사이버범죄를 모두 소개한 것이다[10].

〔표 2〕의 모델을 바탕으로 구체적인 위협 사례와 대책을 보면 〔표 3〕과 같다.

〔표 2〕와 〔표 3〕을 보면 지금까지의 해킹 등 기술적 요인에 의한 사이버범죄뿐만 아니라, 스팸, 인터넷 사기, 피싱 등 사회공학적 기법에 기반한 범죄도 충분히 고려하였음을 알 수 있다.

3계층인 OS/애플리케이션 이하의 위협들은 주로 기술을 기반으로 한 위협으로 기존에 이미 잘 알려진 공격의 하나로써 판단할 수 있다. 그러나 콘텐츠 이상은 새로운 형태의 공격이며 스팸, 산업스파이, ID도용, 개인정보 침해, 피싱, 파밍, 인터넷 사기 등은 일

〔표 2〕 심리적 관점을 추가한 보안 7계층 모델

| 계층 | 계층 이름 | 속성 | |
|---|---|---|---|
| 7 | 심리계층(Psychological) | 인식 | 사람의 취약성을 이용한 범죄 |
| 6 | 관습계층(Custom, Habit) | 행위관습 | |
| 5 | 운영관리계층(Operation) | 규칙 | |
| 4 | 콘텐츠계층(Contents) | 데이터 | 외부에서 파악하기 어려움 |
| 3 | OS/애플리케이션계층(Application) | 소프트웨어 | |
| 2 | 하드웨어계층(Hardware) | 소프트웨어 | 외부에서 쉽게 파악할 수 있음 |
| 1 | 물리계층(Physical) | 물리적 보안 | |

〔표 3〕 보안 7계층 모델의 위협 및 사례

| 계층 | 위협 사례 | 대책 |
|---|---|---|
| 심리 | 피싱, 파밍, 인터넷사기 | 홍보/교육, 인식 제고 |
| 관습/<br>습관 | ID 도용, 파밍,<br>XSS 등 | 인식 제고,<br>디지털 서명 등 |
| 운영<br>관리 | DoS, 스팸, 사보타지,<br>산업스파이, 랜썸웨어 | 필터링, OPSEC,<br>사법, 정책 등 |
| 콘텐츠 | 스니퍼, 스팸,<br>스파이웨어, 컨텐츠<br>위변조 등 | 필터링, 암호화, 콘텐츠<br>감시, 호스트기반 IDS<br>등 |
| OS/<br>애플리케<br>이션 | DOS, Attack Script,<br>봇넷, 루트킷, 제로데이<br>공격 | 방화벽, Anti-Virus,<br>N-IDS, IPS, Patch<br>& Auto Patch 등 |
| 하드웨어 | 부당접근/훼손/<br>위변조 등 | 경계보안, 훼손방지,<br>포장 |
| 물리 | 시건장치<br>훼손/도난/파괴 | CCTV 감시, 경보,<br>경보 알림 |

부 기술적인 사항을 이용하기도 하지만 근본적인 내용은 심리적 기법을 이용한 사회공학적 공격이 범죄의 대부분을 차지함을 보여준다〔11-15〕.

## 2.4 심리적 관점에서의 보안

심리적 관점에서의 보안을 보는 시각은 브루스 슈나이어 박사의 논문에는 수학적 통계를 바탕으로 한 '현실성(Reality)'과 사람에 따라 다른 심리적 느낌으로 보안을 판단하는 '감각성(Feeling)' 간의 차이를 역설하였다〔16〕.

하지만 이 논문에서는 논리적 관점의 보안을 심리전 혹은 심리전쟁과 사회공학적(Social Engineering) 측면에서 보고자 한다. 심리전쟁은 사람의 마음을 공격하는 전쟁으로 사람의 정신과 감정에 자극과 충격을 줌으로써 군인들의 사기를 저하시켜 전쟁에서 우위를 점하려는 목적이 있다〔17〕.

유사한 개념으로 사회공학적 공격도 사람의 심리적 취약성을 이용한다〔18〕. 케빈 미트닉은 "상대방을 속여 원하는 정보를 얻어내는 것"으로 정의한 바 있으며〔19〕, 속임수 및 트릭을 이용하여 중요 정보를 획득하고, 타인에 대한 신뢰를 이용한 인간본성 자체의 취약성을 이용하여 특정 조직의 기술적·물리적 보안장벽을 가장 손쉽게 무력화할 수 있는 방법이다〔20〕. 다음과 같은 요소들이 이용된다〔21〕.

- 특권(Authority) : 특정 사람의 신분 및 직권에 대한 신뢰
- 친분(Liking) : 자신이 좋아하는 사람에 대한 신뢰(평소 친분이 두터운 사람)
- 보답(Reciprocation) : 자신을 도와 준 사람에 대해 도움을 주려는 경향
- 규율(Consistency) : 구두상의 정책 및 규칙들에 대해 상대방이 따르도록 한 후 비밀번호 및 기타 중요 정보 예측
- 설문(Social Validation) : 일반적으로 공인된 형태의 설문 조사를 통하여 상대방으로부터 중요 정보 획득
- 결핍(Scarcity) : 특정 대상에 대한 일정 및 수량 한정 이벤트를 통한 사용자 심리 동요 이용

현재 벌어지고 있는 인간의 심리적 취약성을 이용한 대표적인 위협은 다음과 같은 것이 있다.

- 피싱 및 보이스피싱, 파밍 : 금융기관을 사칭한 메일이나 전화를 통한 공공기관 및 폭력배 사칭, DNS 사기 등
- 스팸 : 스팸 필터링 도구를 회피하기 위한 제목, 송신자 등의 변화
- 인터넷 사기 : 인터넷 물품 판매 사기, 사이버 앵벌이 등
- 악성코드 : 첨부파일 보기를 유도하기 위한 트로이목마, 스파이웨어 등
- 악의적 콘텐츠 게재 : 모욕을 위한 악의적 콘텐츠나 댓글 게재
- 콘텐츠 신뢰도 약화를 노린 공격 : 클릭(Click) 오남용 등

그러므로 현재 나타나고 있는 사이버범죄의 양상을 보면, OS/애플리케이션 계층까지의 특징이 콘텐츠 이상의 계층으로 변화하고 있음을 알 수 있다.

(1) Syntax는 자동 점검 가능 -> Semantic은 수동 점검 필요
(2) 기술적 공격 -> 사회공학적 사기 공격, 기술적 사항 포함하여 시도
(3) 기술적 지식 필요 -> 범죄자들이 기술자를 활용
(4) 기술적 만족 -> 돈을 노린 범죄자의 한탕주의

그러므로 최근의 양상을 볼 때 보안 기술을 가진 사람들은 범죄의 하수인으로 전락할 가능성이 매우 높아진 상태이며, 심지어는 '맥마피아'라는 신조어가 나타나 국제적인 범죄 집단이 하수인들에게 해킹 기법 등을 교육시키고 있는 것으로 나타나기 시작하였다[9].

### 2.5 정보전 맥락에서의 사이버범죄

정보전에 대한 이론의 창시자는 공격기법 분류를 물리적 공격, 신택스기반 공격, 시맨틱 혹은 인지기반 공격으로 분류한 바 있다[22].

시맨틱 공격은 컴퓨터 사용자의 심리를 직접 공격하는 것이다[23]. 시맨틱 공격에 대한 대응은 정보 및 보안공학에 있어 중요한 역할을 할 것이며 정보검색이나 문서검색 방식은 추적기능을 포함하도록 개발하여 과학자나 법률 전문가의 요구에 부응할 수 있어야 하고 문서들은 과학적 사실이나 법적 증서를 제시할 수 있도록 명확히 표현되어야 한다.

정보 및 정보보안과학에는 데이터 마이닝, 시각화, 링크 분석 기술 등이 필요하며 이러한 분석환경에는 공격이 발생할 때 자동으로 경고를 발생할 수 있는 시맨틱 해킹 대응 툴과 분석가가 신속히 관련 자료를 분석할 수 있는 메커니즘이 요구된다[24].

## III. 사이버범죄 프로파일링 모델

### 3.1 사이버범죄 프로파일링 관련 연구

사이버범죄에 대한 프로파일링은 컴퓨터 범죄에 대한 분류, 컴퓨터 범죄의 증거분석 등의 컴퓨터 포렌식에서 활용하고 있으며 미국 FBI나 사이버범죄에서의 분류 방법이 다르다. 어떤 연구인들은 포렌식 증거 관리 시스템을 제안하면서 디지털 증거의 무결성을 보장하기 위한 시스템을 발표하기도 하였다[25].

### 3.2 사이버범죄의 기본적 분류

경찰청 사이버테러대응센터의 분류에 의하면 사이버범죄는 '테러형'과 '일반형'으로 나뉜다. 각 유형에 속한 범죄의 종류는 [표 4]와 같다.

위 분류에 따르면 사이버범죄는 크게 1)심리적 분석, 즉 사회공학적 사기 범죄에 대한 일반적인 수사, 조사, 분석 등이 요구되는 범죄와, 2)기술적으로 숙련된 범죄에 대한 기술적인 분석, 대응이 요구되는 범죄로 나누어진다.

[표 4] 사이버테러대응센터의 사이버범죄 분류

| 분류 | 사이버범죄 | 속성 |
|---|---|---|
| 테러형 | 해킹 | - 기술적 접근 요구됨<br>- 분석대응 시간 필요 |
| | 악성프로그램 | |
| 일반형 | 사기(통신, 게임) | - 사회공학적 사기<br>- 기술적기법을 응용하기도 함<br>- 조사 분석에 많은 시간을 요하지 않음 |
| | 불법복제 (음란물, 프로그램) | |
| | 불법·유해사이트 (음란, 도박, 폭발물, 자살) | |
| | 명예 훼손 | |
| | 개인정보 침해 | |
| | 사이버 스토킹 | |
| | 사이버 성폭행 | |
| | 협박·공갈 | |

이 프로파일링 모델에서는 크게 기술적 분석과 심리적 분석의 2가지 방법으로 사이버범죄의 축을 두고 분석하는 모델을 제안하는데 심리적 분석은 사회적인 영향을 얼마나 주는가에 따라 판단한다.

### 3.3 사이버범죄 프로파일링 관련 연구

기술적 영향력은 침입, 크래킹과 악성코드로 나뉘고, 봇넷(Botnet)을 구축하고 운영하여 개인정보 침해, DDoS 공격 등이 가능한 악성코드가 영향력이 더욱 크다.

기술적 사이버범죄의 성격은 [표 5]와 같다.

[표 5] 기술적 사이버범죄의 성격

| 기술적 사이버범죄 | 영향력 순위 | 비고 |
|---|---|---|
| 해킹 (Hacking) | 2 | 주로 1 대 1 해킹, 신기술 발전 가능 |
| 악성코드 (Malware) | 1 | 봇넷 이용으로 다양, 복잡한 공격 |

### 3.4 사이버범죄의 기본적 분류

주로 기술이 그다지 크게 요구되지 않는 '일반형' 범죄이므로 특별한 기술이 없어도 일반적인 범죄 수사를

〔표 6〕 논리적 사이버범죄별 영향력

| 논리적 사이버범죄 | 영향력 순위 | 비고 |
|---|---|---|
| 사기(통신, 게임) | 2 | 전 국민을 상대로 한 사기 만연 가능 |
| 불법복제(음란물, 프로그램) | 6 | 기업과 경제에 대한 영향력 |
| 불법·유해사이트(음란, 도박, 폭발물, 자살) | 3 | 전 국민을 상대로 한 영향력 발휘 가능 |
| 명예 훼손 | 5 | 명예훼손 대상에 따른 영향력 |
| 개인정보 침해 | 1 | 정보유출 건수 많고, 사후 범죄 예상 |
| 사이버 스토킹 | 7 | 국민 개인에 대한 영향력 |
| 사이버 성폭행 | 8 | 국민 개인에 대한 영향력 |
| 협박·공갈 | 4 | 주요 기업 및 개인에 대한 영향력 |

하였던 인력으로 충분히 조사 분석이 가능하다. 하지만 사회적, 심리적인 영향력이 얼마나 되는지 충분히 파악하여야 적절한 대응이 가능하다. 예를 들어 '명예훼손'이라는 범죄는 미미한 범죄의 하나이지만, 주요 인사에 대한 명예 훼손은 정책적인 변화를 불러오고 국민에 대한 심리적 충격이 매우 클 수도 있다.

논리적 사이버범죄의 영향력은 〔표 6〕과 같다.

### 3.5 사이버범죄의 기본적 분류

사이버범죄에 대한 프로파일링은 범죄에 사용된 기법의 분류를 사전에 해 두어 향후 나타나는 사이버범죄를 수사할 경우 소요되는 수사 인력의 수와 경력을 미리 예측할 수 있고, 범죄의 변화를 통계 분석하여 사이버 수사에 대한 중장기 계획을 수립할 수 있게 한다. 이 논문에서 목표로 제시한 심리적인 측면을 반영하여 일반범죄로 분류된 사이버범죄를 세분화하려고 한다.

이를 공식화된 코드로서 다음과 같은 규칙을 정한다.

$$CCP = K \cdot T\ [Description]$$

| | |
|---|---|
| CCP | Cyber Crime Profile |
| K | Cyber Crime Classification |
| T | Technically, time required |
| Description | Description of Cyber Crime in Brief |

사이버범죄 종류는 정의된 바에 의하면 10가지이나 경찰청에서는 이를 8가지로 분류하여 발생 및 검거 현황을 분석하고 있다. 분류 유형은 1)해킹, 2)바이러스, 3)사기(통신, 게임), 4)폭력(명예훼손, 성폭력 등), 5)개인정보 침해, 6)불법사이트 운영, 7)불법복제 판매, 8)기타이다.

이 논문에서는 이 현황의 분류를 기준으로 K 값을 구성하며, 기술력의 적용 유무에 따라 각 유형을 두 가지로 나눈다. 사이버테러대응센터 홈페이지(www.netan.go.kr)에 공개된 '주요 사건'을 범죄의 유형 및 기술력의 유무로 분류하면 아래의 〔표 7〕과 같다.

## IV. 프로파일링 결과 적용 및 분석

사이버범죄의 유형별 발생 현황을 보면 기술력이 필수로 요구되는 테러형 범죄보다, 심리적인 요소를 이용한 일반형 범죄가 월등히 높다. 〔표 8〕은 2008년의 경찰백서에 나타난 사이버범죄의 유형별 검거 현황이다(단위 : 건수)〔26〕.

전체 건수에 대한 테러형 범죄와 일반형 범죄의 비율은 〔그림 2〕와 같다.

이 논문에서 제시한 프로파일링 모델은 발생 비율이 월등히 높은 일반형 사이버범죄를 대상으로 하므로 80% 이상의 범죄에 대한 상세 분류를 제공할 수 있다. 또한 이를 통하여 다음과 같은 응용과 적용사항이 기대된다.

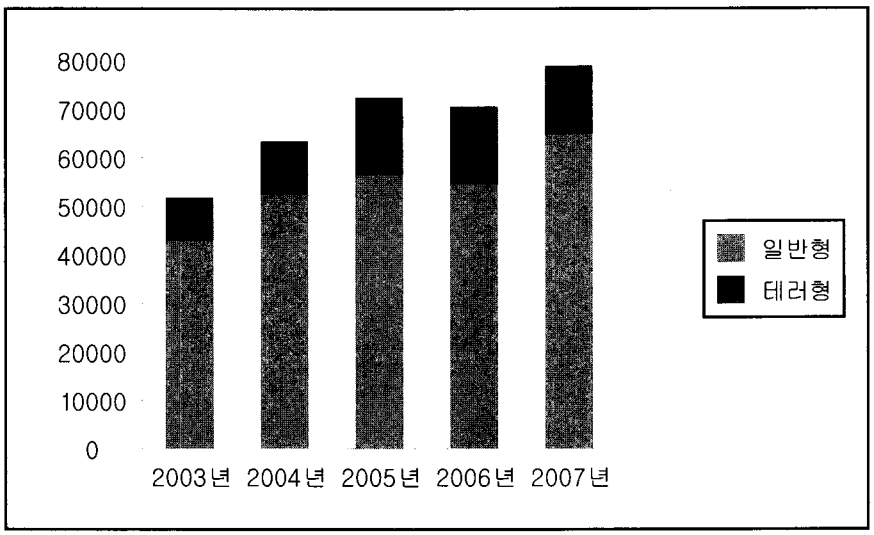
- 사이버범죄의 신속한 분류 및 코드화를 통한 자료의 통합적 축적 및 활용
- 일반범죄와 테러형범죄 발생 비율의 꾸준한 분석을 통한 사고분석의 효율적 대응
- 통계 분석 및 관리를 통한 국가적 사이버범죄 동향 예측 가능
- 공공기관 및 일반 기업에서 사이버범죄 예방 분석 자료로서 활용

〔표 7〕 사이버범죄 유형별 발생 사례

| 분류코드 | 코드 | 사례 |
|---|---|---|
| Privacy 개인정보 | P | 〔2008/04/16 - 텔레마케팅 업체에 개인정보유출 피의자 등 검거〕<br>대형할인점에서 경품응모권 등으로 모은 개인정보 3만여 건을 고객의 동의 없이 텔레마케팅 업체에 넘겨주었다. |
| | PT | 〔2008/03/13 - PC 100만 대 감염, 12억 회 불법 광고한 일당 검거〕<br>PC 사용자의 ID, 비밀번호 등 개인정보를 빼내 자동으로 인터넷 사이트에 접속하는 글을 게시하는 기능을 수행하는 악성코드를 정상적인 프로그램으로 속여 국내 주요 포털사이트 게시판에 유포하고, 감염된 PC 100만여 대에서 개인정보를 유출하고, 12억 2천 회에 걸쳐 중국에 개설한 도박 사이트를 광고하였다. |
| Fraud 사기 | F | 〔2008/04/13 - 5억 5천만 원 쇼핑몰 사기 피의자 검거〕<br>사기쇼핑몰 '인더드림'을 개설·운영하면서, 인터넷 가격비교 사이트에 에어컨 등 가전제품을 최저가로 판매한다고 허위 광고하고 물품 대금을 입금한 피해자 875명으로부터 약 5억 5,900여만 원을 교부 받아 편취한 혐의이다. |
| | FT | 〔2007/10/30 - 악성프로그램 유포 및 사기 피의자 검거〕<br>2005년부터 2년 여간 악성 바이러스 치료 프로그램에 바이러스를 몰래 첨부하여 이용자의 동의 없이 622만 대의 컴퓨터에 무단 배포하고, 배포된 바이러스 및 감염되지 않은 정상 파일을 치료해 준다고 속여 126만 명으로부터 93억 원 상당을 편취한 혐의이다. |
| Violence 폭력 | V | 〔2005/02/23 - 타인 비방 메신저 대화명, 모욕죄 해당〕<br>피의자는 모 컴퓨터 관련 업체에 고용된 지 20여 일만에 해고되자 이 회사 대표에게 욕설 내용의 메신저 대화명을 사용하고, 인력채용 사이트 게시판에 해직된 회사를 비방하는 글을 올린 혐의 등으로 기소됐다. |
| | VT | 〔2008/07/25 - '미래에셋' 공격프로그램 제작 유포자 등 검거〕<br>지난 3월부터 포털사이트 게시판을 통하여 특정 사이트를 대상으로 대량의 데이터를 일시에 전송함으로써 시스템을 마비시키는 '분산서비스거부(DDoS)공격' 프로그램을 제작·유포하여 1만여 대의 컴퓨터를 감염시키고, 감염 컴퓨터를 해외에서 원격으로 관리·조종할 수 있는 원격제어 시스템까지 갖춘 '공격네트워크(봇넷 : Botnet)'를 구축한 후, 해외 공범들에게 제공하였다.<br>미래에셋증권 사이트를 공격하고 공격을 중지하는 조건으로 2억 원을 요구하는 등 국내 인터넷 쇼핑몰 등 7개 업체로부터 550만 원을 갈취하였다. |
| Illegal 불법 사이트 | I | 〔2008/04/30 - 불법 환전사이트 운영자 등 91명 검거〕<br>온라인 게임머니 환전사이트를 불법으로 운영하면서 게임머니를 구매하여 되파는 수법으로 약 85만 회에 걸쳐 총 850여억 원 상당의 불법 거래를 하였다. |
| | IT | 〔2008/03/13 - 청부 해킹 피의자 등 검거〕<br>피의자들은 포털사이트 내 해킹 관련 카페 회원으로 활동하면서 '해킹을 해준다.'고 게시글을 올려, 이를 보고 의뢰한 자에게 일정 금액을 받고 해킹을 하였는데, 각종 사이트에 ID와 Password 찾기 기능을 악용하여 타인의 비밀번호를 무단 침해하거나 인터넷사이트의 암호화된 비공개 게시판글 내용을 권한 없이 지득하였다.<br>의뢰자는 자신이 근무하는 회사 업종 관련, 공정거래위원회 사이트 비공개글 내용 파악, 애인의 싸이월드 접속 비밀번호 파악 등을 요청하였다. |
| Copyright 불법 복제 | C | 〔2008/01/29 - 기업형 파일공유사이트 운영업체 일당 검거〕<br>합법적인 것처럼 속여 7개의 국내 유명 파일공유사이트를 운영하면서, 유료회원 66만여 명을 대상으로 음악 파일 등 저작물 310만여 개와 포르노 동영상 2만여 건을 판매, 유포하였다. |
| | CT | 〔2002/12/26 - 경쟁업체 해킹, 수억 원대 디지털콘텐츠 유출사범 검거〕<br>인터넷상에서 디지털 음악악보를 유료로 제공하는 경쟁업체 B사의 서버에 불법적으로 침입하여 수시로 매출현황, 회원수, 단가, 업데이트 현황 등 회사 기밀을 열람하고, 회사의 중요 자산인 음악 악보 파일 약 3천 개(시가 3억 원 상당)를 유출하여 그 중 일부를 직접 제작한 것처럼 속여 서비스를 제공하였다. |
| Hacking 해킹 | H | -- |
| | HT | 〔2004/03/04 - 사상 최대 4,300여 서버시스템(국내) 무차별 해킹 당해!〕<br>최근 국내에서 일어난 해킹사건을 추적하던 중 해외 해커들의 공격루트를 발견, 수사한 결과 국내 약 4,300여 서버시스템이 이곳을 경유지로 사용한 20여 명의 해커들에 의해 피해를 당한 것으로 파악되어 추적 중에 있다고 밝혔다. 단일 사건으로는 해커 수사상 최대 규모이다. |
| Mal Code 악성코드 | M | -- |
| | MT | 〔2002/12/26 - 사이버테러형 웜바이러스 제작자 및 언론기관 홈페이지 해킹사범 등 무더기 검거〕<br>멜리사 바이러스보다 더 큰 전파력과 매달 31일에 전 시스템을 파괴하는 무서운 파괴력을 가진 국내 최초의 사이버테러형 웜바이러스(I-Worm.Win32.White)를 제작, 유명 사이트를 통해 유포시킨 서모군(15세)을 검거하였다. |
| Else 기타 | E | 〔2003/10/02 - 뒷돈 주고 인터넷 골프예약 사실로 밝혀져 피의자 검거〕<br>대중(퍼블릭) 골프장의 인터넷 예약시스템에 피의자가 개발한 프로그램을 사용하여 1년 6개월간 560여 명에 대하여 2,370여 건을 1회에 4-6만 원씩 받고 인터넷 예약대행을 함으로써 총 1억 원의 부당이득을 취하고 A골프클럽 인터넷 예약시스템에 장애를 발생하게 하여 업무를 방해하였다. |

〔표 8〕 2008년 경찰백서의 사이버범죄 검거 현황

| 구분 | 계 | 테러형 범죄 | | 일반형 범죄 | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 해킹 | 바이러스 | 통신사기 게임사기 | 명예훼손 성폭력 등 | 개인정보 침해 | 불법사이트 운영 | 불법복제 판매 | 기타 |
| '03년 | 51,722 | 8,844 | 47 | 26,875 | 2,976 | 2,015 | 1,719 | 677 | 8,569 |
| '04년 | 63,384 | 10,955 | 38 | 30,288 | 3,751 | 2,065 | 2,410 | 1,244 | 12,633 |
| '05년 | 72,421 | 15,831 | 43 | 33,112 | 6,338 | 2,889 | 1,850 | 1,233 | 11,125 |
| '06년 | 70,545 | 15,934 | 45 | 26,711 | 7,109 | 2,327 | 7,322 | 2,284 | 8,813 |
| '07년 | 78,890 | 13,988 | 49 | 28,081 | 9,164 | 3,741 | 5,505 | 8,167 | 10,195 |




〔그림 2〕 사이버범죄 유형별 발생 비율

## V. 결 론

사이버범죄의 프로파일링을 위하여 먼저 다음을 분석하였다.

- 현재(2008년 12월) 사이버범죄의 정의와 유형들을 살펴보았다.
- 최근 사이버범죄는 범죄자가 기술자를 하수인으로 이용하고 있음을 알았다.
- 심리적인 보안이 사기를 치는 사회공학적, 시맨틱 공격과 유사한 상황임을 보였다.
- 사람의 심리적인 취약성을 이용한 범죄로서 콘텐츠, 운영관리, 습관 및 심리계층 등을 보이는 계층적 모델을 보여주고 사례를 보였다.

사이버범죄의 프로파일링을 정의하기 위하여 경찰청 사이버테러대응센터의 각종 사례를 바탕으로 사이버범죄를 1)개인정보 침해, 2)인터넷 사기, 3)사이버 폭력, 4)불법사이트 개설, 5)불법복제, 6)해킹, 7)악성코드 유포, 8)기타로 분류하여 보았다.

이 프로파일링 기법을 바탕으로 그 동안 경찰청에 신고된 사건을 분석한 결과, 신택스 점검 위주의 기술적 범죄 수사보다는 시맨틱 위주의 비자동적인 수사가 더욱 요구됨을 알 수 있었다. 또한, 시맨틱 위주의 수사는 범죄 사실의 내용과 의미를 파악하여야만 분석이 가능한 심리적 요인이 매우 크게 반영된 사이버범죄이고 이러한 범죄는 매우 급격히 증가함을 알 수 있었다.

이는 경찰청 사이버테러대응센터가 기술도 필요한 요소이기는 하지만 사이버범죄의 심리적, 사회공학적 사기에 노출된 수많은 국민에게 경찰의 많은 수사 경

험과 사고 조사에 의한 사이버범죄 수사가 매우 적절하게 다가서고 있음을 직간접적으로 증명한다.

이 논문에서 제안하는 프로파일링 기법은 사이버범죄 유형을 잘 분류하여, 실무 부서에서 수사를 할 경우 빠르고 적절한 인력 배치 등을 가능하게 할 것으로 판단한다. 또한, 향후 나타날 새로운 형태의 사이버범죄뿐 아니라 좀 더 구체적인 실무나 다른 속성에 의한 분류도 가능할 것으로 본다. 또한 향후 보다 구체적이고 세부적인 분류도 요구되고 분류된 사이버범죄 간의 상관관계 분석, 행위자 및 의도 등에 대한 프로파일링도 중요할 것이다.

## 참 고 문 헌


[1] 경찰청 사이버테러대응센터(NETAN), http://www.netan.go.kr/index.jsp

[2] KISA, "2006 정보시스템 해킹·바이러스 현황 및 대응," pp. 5-6, 2006년 12월.

[3] Symantec, "Underground economy July 07~June 08," pp. 1-2, Nov. 2008.

[4] ZDNet Korea, "해킹의 프로화 「명예보다 돈이 좋아」," http://www.zdnet.co.kr/ArticleView.asp?artice_id=00000039131366, 2004년 11월.

[5] 행정안전부 개인정보과, "개인정보 이해와 해설," pp. 3-11, 2008년 6월.

[6] 네이버 백과사전, 두산 백과사전, http://100.naver.com/100.nhn?docid=775269

[7] U.S. Department of Justice, Computer Crime & Intellectual Property Section, http://www.cybercrime.gov/index.html

[8] Sophos, "Security threat report: 2009 - State-sponsored cybercrime," p. 13, Dec. 2008.

[9] 윤희영, "국경 없는 조폭 맥 마피아," 디지틀 조선일보, http://news.chosun.com/site/data/html_dir/2008/05/26/2008052601148.html, 2008년 5월.

[10] G. Takama, M. Association, and Papan, "Security, Privacy Data Protection, and Perspectives of Counter Cyber Crime," CodeGate Conference, Seoul, pp. 64-66, Apr. 2008.

[11] M. Allen, "Social Engineering," SANS, pp. 2-8, June 2006.

[12] 국가사이버안전센터(NCSC), "인터넷 신종 사기 기법, 파밍(Pharming)," http://www1.ncsc.go.kr(동향분석정보 #44), 2005년 3월.

[13] A. Litan, "Increased Phishing and Online Attacks Cause Dip in Customer Confidence," Gartner, http://www.gartner.com/DisplayDocument?doc_cd=129146, June 2005.

[14] G. Conti, "Countering Denial of Information Attacks," Blackhat 2005 & Defcon 13, http://www.defcon.org/html/defcon-13/ dc13- speakers.html#Conti, July 2005.

[15] G. Conti and M. Ahamad, "A Framework for Countering Denial of Information Attacks," IEEE Security & Privacy November/December 2005, vol. 5, no. 6, pp. 50-56, Nov. 2005.

[16] B. Schneier, "The Psychology of Security," http://www.schneier.com/essay-155.html, Jan. 2008.

[17] 이대원, "정훈 교육과 심리전," 육군 제132호, pp. 22-30, 2005년 7월.

[18] J. Kee, "Social Engineering: Manipulating the Source," SANS, pp. 5-7, Apr. 2008.

[19] K. Mitnick, The Art of Deception, John Wiley & Sons Inc., Oct. 2003.

[20] H. Kratt, "The Inside Story: A Disgruntled Employee Gets His Revenge," SANS, pp. 6-7, Dec. 2004.

[21] M. Libicki, "The Mesh and the net: Speculations on armed conflict in an age of free silicon," McNair Paper no. 28, National Defense University, 1994.

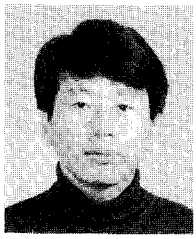
[22] Cybenko, A. Giani, and P. Thompson, "Cognitive Hacking: A Battle for the Mind," IEEE Computer, vol. 35, no. 8, pp. 50-56, Aug. 2002.

[23] P. Thompson, Semantic Hacking and Intelligence and Security Informatics, Springer Berlin/Heidelberg, Jan. 2003.

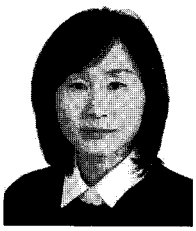
[24] K.K. Arthur, M.S. Oliver, H.S. Venter, and J.H.P. Eloff, "Consideration Towards

a Cyber Crime Profiling System," The third International Conference on Availability, Reliability and Security, IEEE, pp. 1388-1393, Mar. 2008.
[25] 경찰청, 2008 경찰백서, pp. 138-141, 2008년 9월.

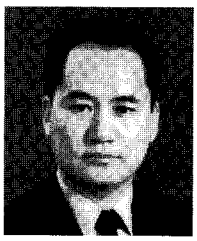
## 〈著者紹介〉



임 채 호 (Chae Ho Lim) 종신회원
1986년 2월: 홍익대학교 전산학과 학사
1990년 2월: 건국대학교 전산학과 석사
2001년 2월: 홍익대학교 전자계산학과 박사
1986년 ~ 1995년: KIST SERI 선임연구원
1996년 ~ 2000년: 한국정보보호진흥원 책임연구원
2001년 ~ 2004년: KAIST 전산학과 초빙교수
2004년 ~ 2005년: 시큐리티맵(주) 대표이사
2006년 ~ 현재: NHN(주) 수석연구원
2009년 현재: 한국정보보호학회 부회장
〈관심분야〉 정보보안



김 지 영 (Jee Young Kim) 정회원
1998년 2월: 홍익대학교 컴퓨터공학과 학사
2001년 2월: 홍익대학교 전자계산학과 석사
2009년 현재: NHN Business Platform(주) IT보안실
〈관심분야〉 정보보안



최 진 혁 (Jin Hyuk Choi) 정회원
1987년 2월: 국립경찰대학교 행정학과 학사
1993년 2월: 연세대학교 행정대학원 행정학 석사
1995년 2월: 영국 University of Kent 국제관계론 석사과정 수료
2009년 2월: 용인대학교 경호학과 박사과정 수료
1987년 ~ 1998년: 경찰청 인터폴(INTERPO:L)/해커수사대
1998년 ~ 2005년: 한국IBM(주) Security Program Manager
2005년 ~ 2009년: NHN(주) Global Security & Risk Management
2009년 현재: 한국기업보안협의회 부회장 & 한국산업보안연구학회 국제이사
UN 사이버범죄 방지를 위한 가상포럼 국제컨설턴트그룹 인프라 담당 의장
〈관심분야〉 정보보안