情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

프록시 서비스를 통한 범죄 위협과 프라이버시 보호에 관한 연구

강 신 범,† 이 상 진,† 임 종 인
고려대학교 정보보호대학원

A Study on the Criminal Threat and Privacy Protection with a Proxy Service

Shin-Beom Kang,† Sang-Jin Lee,‡ Jongin Lim
Korea University

요 약

인터넷 사용자와 정보서비스 제공자 사이의 권리 침해 행위의 예방을 위해 행위자들의 본인확인제와 활동에 사용된 개인정보의 수집이 이뤄지고 있다. 하지만 인터넷 사용상의 익명성 보장을 요구하는 개인들의 권리와 규제 법률의 집행 사이의 논쟁은 지속되고 있다. 다양한 기술적 목적으로 사용되는 프록시 서버(Proxy Server)의 특성을 이용해 인터넷 상의 익명성을 확보하려는 우회접속 사용자가 늘어나고 있지만 이에 대한 제도적 관리체계나 사용자들을 보호할 제도적 장치는 미미하다. 본 연구에서는 프록시 서버를 이용한 우회접속 서비스가 갖는 사이버범죄 위협과 프라이버시 보호를 위한 필요성에 대해 논하고 비례성 고찰을 통해 공익과 제한되는 개인의 권익 사이에 균형을 위해 필요한 제도적 보완책을 제안한다.

ABSTRACT

Internet service provider is able to collect personal information to prevent the violations of the rights of service providers and customers using internet. But there are still many debates going on between a personal privacy and a regulation. Proxy servers are used in various technical purposes include bypass access. Although the proxy server users are increasing but there are not any proper institutional mechanisms and regulations to protect users. In this study, we discuss the two sides of a proxy service includes its privacy protection function and the cyber-crime threat and propose supplementary measures to mediate between the interests of public and private.

Keywords: Personal Information Protection and Security, Proxy Service, Cyber Criminal Threat, Security Policy

I. 서 론

인터넷 사용자에 대한 본인확인제도는 이용자 및 정보통신서비스 제공자의 자기책임성 확보를 통한 권리 침해 행위의 예방을 위해 도입되었다. 비슷한 목적으로 정보통신서비스 제공업자들은 서비스 사용자들의 로그인 및 댓글 등과 같은 활동에 사용된 컴퓨터의 IP 정보를 수집한다. 인터넷 사용자에 대한 본인확인제도나 개인정보를 수집하여 이용자와 서비스 제공자의 권리 침해로 인한 피해 방지와 신속한 피해구제를 위한 조치들은 점점 강화되고 있는 추세이다. 반면에 인터넷 사용상의 익명성을 보장받기 위한 사용자들의 노력도 증가하고 있다. 대표적인 현상으로 사용자들의 인터넷 접속 정보를 수집하는 통신사업자들에게 자신

접수일(2011년 6월 11일), 수정일(2011년 8월 16일), 게재확정일(2011년 9월 30일)
† 주저자, shinbeom@korea.ac.kr
‡ 교신저자, sjlee@korea.ac.kr

의 IP 정보를 숨기기 위해 프록시 서버를 이용한 우회 접속을 들 수 있다. 이러한 프록시 서비스는 인터넷 사용자 및 통신사업자의 권리 침해 방지를 위한 규제 정책과 사용자들의 개인정보 보호 및 익명성 보장이라는 권리가 충돌하는 영역에서 적정한 제도적 관리 없이 방치되고 있다.

본 연구에서는 프록시 서비스를 이용하는 사용자의 권리와 관련 서비스에 대한 제도적 현황을 살펴보고 프록시 서비스가 갖는 양면성에 따른 비례성 고찰을 토대로 프록시 서비스가 사이버범죄 위협 관리와 프라이버시 보호를 위한 규제대상이 됨을 보이고 이에 따른 개선점과 대응책을 제시한다.

II. 프록시 서비스

2.1 프록시 서버 및 서비스 형태

프록시 서버는 자신을 통해 컴퓨터나 네트워트가 다른 네트워크나 컴퓨터에 간접적으로 접속할 수 있게 함으로써 접속을 시도한 클라이언트와 최종 접속된 서버 사이에 중계역할을 수행하는 기능을 갖는다. 대부분 프록시 서버는 중계되는 데이터를 캐쉬로 저장하는 등의 전후처리 기능을 통해 클라이언트와 서버간의 통신에 부가적인 기능을 제공하는 장점이 있지만 중계서버를 통해 접속되는 경우 직접 접속되는 경우보다 통신 속도 저하와 같은 단점도 있다. 이러한 프록시 서버가 인터넷 사용상의 익명성을 위해 사용되는 이유는 중계서버의 특성상 접속을 시도하는 클라이언트의 IP 등과 같은 개인정보가 프록시 서버를 통해 중계역할을 수행하는 도중 변경되어 최종 통신서비스 제공자의 서버에 사용자 컴퓨터의 IP 등과 같은 정보가 노출되지 않기 때문이다.

인터넷 사용자에게 익명성을 제공하기 위해 사용되는 프록시 서비스 유형은 다음과 같이 분류될 수 있다.

2.1.1 유·무료 프록시 서버를 이용한 브라우징

HTTP나 SOCKS 프로토콜을 지원하는 프록시 서버로써 대부분의 웹 브라우저의 프록시 설정을 통해 무료 또는 유료로 이용이 가능해 가장 쉽게 사용자들이 이용할 수 있는 서비스 형태이다. 프록시 서버를 이용하는 사용자들의 익명성을 보장하지만 무료로 운영되는 서버의 경우 서비스 이용자에 비해 시스템 투자가 이뤄지지 않아 적정한 QoS를 보장받지 못하며 보안정책 등이 제대로 적용되어 운영되고 있지 않은 경우 외부 공격자에 의해 관리 권한이 탈취된 상태에서 중계 서버를 통해 전달되는 사용자들의 정보가 악용될 가능성도 있다.

2.1.2 웹 기반 프록시 사이트 이용

서버 기반의 스크립트 기술을 이용한 CGIProxy, PHProxy와 같은 프로그램을 이용해 구축된 프록시 서비스로 사용자들은 별도의 설정 없이 브라우저를 통해 해당 프록시 서버 사이트를 방문하여 최종 목적 사이트의 URL을 입력하면 원하는 사이트에 익명으로 접속할 수 있다. 서비스를 위한 설정 변경이나 설치가 필요 없기 때문에 사용이 용이하지만 원하는 사이트를 서버 기반의 스크립트 기술로 표현하는 과정에서의 오류가 발생하거나 원래 의도와 다른 결과를 전달받을 수도 있다.

2.1.3 프록시 네트워크 이용

FreeNet, I2P와 같은 P2P 네트워킹 또는 암호화 통신을 이용하는 네트워크형 프록시로 네트워크 안에 존재하는 사용자들에 대해 익명성이 보장된다. 네트워크 안에서 익명성을 보장하기 위해 특정 프로그램을 설치하며 라우터가 생성한 터널(tunnel)을 통해 메시지를 전달하는 방식으로 동작한다. 데이터를 전송하기 전에 라우터 정보를 조회하여 데이터의 전송 루트를 결정하기 때문에 터널의 길이를 사용자가 결정하여 익명성이나 성능 등을 조절할 수 있다.

2.1.4 프록시 클라이언트를 사용하는 형태

클라이언트 기반의 프록시 프로그램은 대부분 브라우저나 네트워크의 자동화된 프록시 설정 기능을 제공하며 실시간으로 최적의 프록시 서버를 이용할 수 있도록 관리해 준다. 단순하게 프록시 설정을 대신해 주는 프로그램에서부터 수집된 프록시 서버들의 QoS를 테스트하여 최적 상태의 서버 리스트를 운영하거나 유료 프록시 서버로의 접속을 위한 기능 등을 포함하고 있는 경우도 있다. 사용자 PC에 별도의 프로그램이 설치되어 네트워크 설정을 조작하기 때문에 배포자에 대한 완벽한 신뢰가 없다면 프록시 서비스의 결과는 물론 사용자 PC에 대한 보안도 보장할 수 없다.

2.2 프록시 서비스 현황

인터넷 사용의 익명성을 보장하기 위해 운영되는 프록시 서버가 모두 무료로 운영되지는 않는다. 대부분의 유료 프록시 서버는 월정액 개념의 비용을 지불한 회원들로 구성된 폐쇄 그룹으로 운영되며 부가적으로 프록시 서비스를 제공하는 업체가 관리하는 프록시 서버들의 상태를 조회하여 일정 수준의 QoS를 관리해주는 클라이언트 프로그램을 제공한다. 프록시 서버의 정확한 현황을 확인하기 위한 데이터를 산출하기는 매우 어렵다. 산업적으로도 협회나 인증을 위한 기관이 존재하지 않아 관리 체계가 매우 취약하고 전 세계적으로 개인이나 단체들에 의해 무료로 운영되는 다수의 프록시 서버들은 산발적인 운영이 이뤄지고 있어 실제 존재 여부조차 파악하기 힘들다. 최소한의 현황 파악을 위해 대표적으로 운영되는 프록시 클라이언트 프로그램의 스캔 기능을 이용해 스캔 당시 운영 중인 프록시 서버가 329,326대(2011년 5월, Proxy Swicher 스캐너 집계 기준)에 이른다는 것을 알 수 있었다.

III. 프록시 서비스에 대한 비례성 원칙 고찰

비례성 원칙은 보통 '목적과 수단의 관계'로 이해된다. 즉, 선택된 수단은 그 수단에 의하여 추구되는 목적과 서로 이성적 관계가 있어야 한다는 것이다[1]. 그리고 '비례'는 선택한 수단이 처음에 의도한 목적의 달성에 적합하고, 필요하며 균형을 이루어야 한다는 것을 그 내용으로 한다[2]. 프록시 서비스 역시 인터넷 사용에 있어 개인의 익명성 보장을 위한 수단으로써 그 의도한 목적의 달성 과정상에 사이버범죄 위협을 조장할 수 있는바 둘 사이의 비례성 검토를 통한 고찰이 필요하다.

3.1 프록시 서비스와 개인정보 보호

3.1.1 개인 정보 보호의 의의

개인정보에 대한 정의는 여러 형태가 존재하나 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 6호에서는 개인정보를 "생존하는 개인에 관한 정보로서 성명·주민등록 번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다."고 정의하고 있다. 이는 보호되어야 할 개인정보로 성명, 주민등록 번호와 같은 직접식별 개인정보는 물론 다른 정보와 결합하여 용이하게 식별가능한 개인정보 모두를 포함한다는 의미이다.

인터넷을 사용하는 동안 정보통신서비스 제공자에게 수집될 수 있는 개인정보는 약관 동의를 통한 직접식별 개인정보는 물론 서비스 개선이나 마케팅 용도를 위해 수집되는 개인 컴퓨터의 IP주소와 같은 정보도 포함된다. 문제는 인터넷 상의 다양한 곳에 노출되어 있는 정보를 결합하여 분석하여도 상당한 수준으로 용이하게 개인식별이 가능하다는 점이다.

프록시 서비스는 이러한 인터넷 환경에서 자신의 컴퓨터 정보 즉, IP 정보를 프록시 서비스 제공자의 정보나 기타 정보로 대체하여 정보통신서비스 제공자에게 접속할 수 있도록 해 주기 때문에 결과적으로 자신의 개인식별이 용이하지 않게 하여 개인정보의 노출을 보호할 수 있는 도구가 된다.

3.1.2 개인정보의 자기결정권

개인정보자기결정권이란 개인정보에 대한 포괄적 제어권이 그 정보의 주체에게 있으며 개인정보가 활용되고 있는 사실에 대한 알권리를 포함한다. 인터넷 발달과 함께 정보통신서비스 제공자들의 증가는 정보요구를 증대시켜 개인정보의 수집·처리가 증가되고 있다. 개인정보자기결정권에 대한 헌법상의 명확한 규정이 없기 때문에 헌법 제10조의 인간의 존엄과 가치 규정을 통하여 개인정보자기결정권이 보장되어야 한다는 견해가 있다. 현대 사회에서 개인의 존엄을 보장받기 위해서는 자신의 개인정보를 제어할 수 있는 권리가 반드시 필요하다는 점을 들어 헌법 제17조의 사생활의 비밀·자유조항의 소극적 권리보다 헌법 제10조에 의한 적극적 권리로 이해되어야한다는 주장이다[3].

인터넷 사용자로서의 개인정보자기결정권의 행사는 정보통신서비스 제공자들의 약관 고지를 통한 동의 후 사용 수준 보다 더 적극적인 개인정보에 대한 제어권을 행사할 수도 있다. 문제는 대부분의 인터넷 사용자들은 자신의 개인정보가 특정 서비스를 제공 받는 동안 어떻게 활용되고 있는지 제대로 인식하지 못하는데 있다. 최근 사례에서도 애플사의 아이폰 제품이 개인의 위치정보를 축적하고 있다는 의혹이 제기되어 방송통신위원회가 조사에 나서기도 했다. 이에 대해 애플

측은 해당 제품이 개인정보인 사용자들의 위치를 추적하고 있지 않지만 통신 서비스의 효율을 위해 사용자 위치 주변의 와이파이 존과 기지국에 관한 데이터베이스를 유지해왔을 뿐이라고 해명했다[4]. 사례처럼 개인정보자기결정권의 올바른 행사를 위해서는 개인이 자신의 개인정보가 어떻게 활용되고 있는지를 인지하지 못한다면 사후 대처 이외의 다른 방법이 없다. 때문에 인터넷 사용자는 프록시 서비스를 이용해 개인 컴퓨터의 IP 정보와 같은 개인정보를 원천적으로 수집할 수 없는 상태로 서비스에 접속하여 개인정보가 활용될 필요가 있는 경우 개별적 접근을 허가하는 방식으로 개인정보자기결정권을 강화시킬 수 있다.

3.1.3 프록시 서비스와 프라이버시 보호

헌법재판소는 2005년 7월 2일 소위 NEIS 사건에서 "인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장되는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다."[5] 고 판시함으로 개인정보에 대한 자기결정권의 헌법적 보장을 명시하였다. 그럼에도 해당 사건의 경우 "졸업생의 성명, 생년월일, 졸업일자를 시스템에 수록한 행위는 개인정보자기결정권을 침해하지 않는다"며 합헌 결정을 내렸다.

결국 우리 헌법 제10조, 제17조에 의해 자신의 개인정보자기결정권이 보호됨은 인정되나 개인정보가 개인정보자기결정권의 보호범위에 해당하는지는 개인정보의 보유목적과 수집된 정보가 개인의 인격과 얼마나 밀접한 연관이 있는지 등이 고려되어야 함을 시사한다. 즉, 프록시 서비스를 이용해 자신의 IP 정보에 대한 제어권을 행사하는 행위가 개인정보자기결정권의 보호범위에 해당하는지 여부도 역시 해당 정보를 수집 및 보유하려는 정보통신서비스 제공자의 목적과 해당 정보가 가지는 개인의 인격과의 연관성 등에 비추어 판단되어야 함을 알 수 있다.

3.2 프록시 서비스와 범죄 위협

3.2.1 사이버범죄 특성

실제 세계의 범죄는 근접성(proximity), 크기(scale), 물리적 제약(physical constraints) 그리고 유형(pattern)이라는 특징을 가지고 있다[6]. 하지만 사이버범죄의 경우 피해자와 가해자 사이의 물리적 제약이 약하고 네트워크에 연결된 컴퓨터를 통해 예상할 수 없는 크기의 범죄도 가능하다. 또한, 인터넷을 이용한 범죄의 경우 한 국가의 경계 안에만 머무르지 않고 경계를 넘나드는 경우가 일반적이다[7]. 이러한 사이버범죄의 특징들로 인해 실제 세계의 범죄에 대한 수사 방식이 사이버범죄의 수사에 효과적이지 않을 수 있다. 사이버범죄의 경우 범행이 이뤄지는 공간이 가상화 되어 있고 인터넷을 이용한 네트워크형 범죄의 경우 익명 서비스가 제공되는 공간이기 때문에 가해자에 대한 단서를 찾기 위해서는 서비스 제공자의 시스템 로그 정보에 크게 의존할 수 밖에 없다.

소규모의 사이버범죄 수준을 넘어 사회 안전이나 국가안보를 위협할 수 있는 사이버 테러 수준의 범죄는 그 자체가 독립된 공격으로도 사용될 수 있지만 전통적인 테러나 전쟁의 예비행위로서 수행되기도 쉽다는 특성을 보유한다[8]. 이러한 사이버범죄의 특성은 그에 대한 대응이 매우 신속하고 효과적으로 이루어질 필요성이 있음을 보여준다. 반대로 공격자의 입장에서는 물리적 제약이 약하고 근접성이 떨어지는 사이버범죄의 특성을 이용해 보다 효과적인 피해를 입히기 위해 필요한 것은 최대한의 활동 시간이며 사이버범죄 행위 이후 자신을 향한 수사 활동에 대한 혼선과 지연을 위해 해당 시간 동안의 행위에 있어서의 익명성은 필수적이라 할 수 있다.

3.2.2 익명성의 효과

인터넷 상에서 일어나는 사이버범죄와 잘못된 정보 전달과 같은 사용자 행동은 인터넷 상에서 제공되는 익명성과 관련이 있다[9]. Wallace에 의하면 사람들

은 다른 사람들이 자신이 누구인지 알아낼 수 없다고 생각할 때 억제되지 않은 방법으로 행동하는 것이 익명성이라고 하였으며 이것이 가능한 곳에서 긍정적이거나 부정적인 방법으로 풀려는 경향이 있다고 말했다[10]. Suler는 사이버 공간 내 익명성의 효과에 대하여 의견을 자유롭게 표현하고 도덕적 구속력이 적어져 보다 개방적인 태도를 가지게 되는 "양성적 탈억제성 효과"(benign disinhibition effect)뿐 아니라 다른 한편으로 개인의 정체가 뚜렷이 드러나는 현실 세계에 비해서 개인의 행동에 대한 책임을 묻거나 강제력을 동원할 수 없어서 발생하는 각종의 "악성적 탈억제성 효과"(toxic disinhibition effect)도 두드러지게 나타남을 말하였다[11]. 국내의 경우에도 익명표현의 자유에 대한 침해 문제가 있지만 익명성을 이용한 인터넷의 역기능을 해소하기 위해 인터넷 본인확인제가 광범위하게 적용되어 시행되고 있다. 한국청소년정책연구원의 보고서에 따르면 우리나라 중고생 30.4%가 "댓글을 통해 남의 사생활을 폭로하는 것을 본적이 있다"고 응답했고 성희롱을 목격한 청소년도 27.0%에 이르는 것으로 나타났다. 문제해결 방안으로 "모든 사이트에 실명제를 도입해야 한다"는 제시어에 응답자 21.4%가 '매우 그렇다'고 답했고, 14.3%는 '약간 그렇다', '보통'이라는 응답은 31.7%, 반대의 견으로 '아닌 편이다'와 '전혀 아니다'를 합쳐 32.6%에 그쳤다[12].

3.2.3 사이버범죄 위협

우리나라의 사이버테러대응센터 발표 자료를 보면 2003년 68,445건의 사이버범죄 발생 이후 2010년 122,902건에 이르기까지 사이버범죄는 꾸준히 증가되는 추세이다. 관련법규 또한 "정보통신망 이용촉진 및 정보보호등에 관한 법률"외에 16개 법률이 존재하고 각각 적용법규들도 개정 등을 통해 강화되고 있다. 정보통신서비스 사업자의 경우 사이버범죄의 예방을 위해 제도적 보호조치를 취하고 있지만 이러한 조치가 모든 경우의 위협을 제거하거나 예방하지는 못한다. 이는 사이버범죄가 갖는 사회적·기술적 특성에 기인하는데 무엇보다도 익명성과 비대면성을 기반으로 한 발각과 원인규명의 곤란성과 관련이 있다[13].

사이버범죄에 대한 위협이 현실화 된 경우 증거인멸의 용이성에 따라 신속한 증거 확보가 중요하다. 정보통신서비스 사업자의 경우 이를 가정하여 상당히 방대한 시스템 로그를 기록하고 유지한다. 보안 관제 서비스를 위해 전문업체에 위탁 관리를 맡기거나 방화벽·침임탐지시스템을 운영하고 데이터베이스의 정보암호화 및 권한관리솔루션을 운영하는 비용은 모두 서비스 비용의 상승을 초래한다. 기업의 내부 시스템을 익명 사용자들로부터 보호하고 사이버범죄의 예방 효과 및 신속한 대응을 위해 프록시 서비스를 통한 접속을 아예 차단하는 정책을 운영할 경우 접속 IP가 호스트네임을 가지거나 알려진 유·무료 프록시 서버들의 IP 대역 또는 가상 IP를 사용한 경우까지 모두 접속이 제한되는 경우도 있다. 하지만 대다수의 서비스 업체는 소수일지라도 일부의 정상사용자들에게 서비스 장애가 예상된다는 이유로 적극적인 대응을 회피하는 경우가 많다.

프록시 서비스를 이용하거나 접속 컴퓨터의 IP주소를 변조하는 사용자들이 많을 경우 1차적인 위협 대응에 어려움이 있다. 사이버범죄의 특성상 물리적 제약이 약하고 동시적인 발생이 가능하기 때문에 한명의 해커가 다수의 IP를 이용해 범죄 위협을 일으키는 경우 실질적인 가해자 1인을 검거하기까지 시간과 비용적인 소모가 많다. 또한, 사고 발생시 로그 분석 결과에 의존하여 진행되는 포렌식 과정에서도 IP 정보의 신뢰성은 매우 중요하기 때문에 이를 보장할 수 없을 경우 추가적인 시간 투입과 비용이 발생하게 된다. 또한, 프록시 서비스를 이용하는 사용자들이 늘어나게 되면 정보통신서비스를 제공하는 기업의 내부 비용은 증가된다. 대부분의 침입탐지시스템은 일반적인 프록시 접속을 경고보다는 낮은 주의 수준으로 기록하고 있으며 특정 프록시 툴을 이용한 변조된 HTTP 요청 등을 위협으로 기록하고 있다. 또한, 내부적으로 서비스 최적화나 개인 맞춤형 서비스 등과 같이 약관 동의를 얻어 제공되는 서비스의 경우 서비스 접속자의 IP 정보가 활용되거나 접속 로그에 대한 분석 작업이 수행되는데 프록시 서비스를 통한 접근의 경우는 프로그램에서 예외처리 되거나 오류를 발생시킬 수도 있다.

프록시 서비스를 이용하는 사용자들에게도 추가적인 사이버범죄 위협이 존재한다. 악의적인 프록시 서버는 운영 중 접속한 사용자와 최종 접속 대상 사이트 사이의 데이터를 불법 수집하거나 이를 변조하여 위장하거나 피해를 야기할 수 있다. 또한, 이미 해커에 의해 관리자 권한이 탈취된 프록시 서버에 접속하여 서비스를 이용하는 순간 악성 코드나 봇넷 등에 감염되어 자신의 컴퓨터가 좀비PC화 될 수 있는 위협은 상존한다. 서버 사이드 방식으로 프록시 서비스를 제공하는 경우에도 마찬가지로 웹 플랫폼을 이용한 악성코

드 유포의 위협은 상존한다. 이러한 위협에 주의를 기울여야 할 이유는 프록시 서비스가 가지는 익명성 제공이 사회공학적 기법으로 이용되어 보다 효과적으로 공격이 이뤄질 수 있다는 점이다. 사회공학적 기법을 이용한 공격 방식에서 가장 많이 사용되는 것은 '이메일'을 이용한 피싱 또는 악성코드 감염 공격이다. 악의적인 공격자라 하더라도 수신자가 기대하는 가치를 이용해 보다 쉽게 공격자가 원하는 행동을 유발시킬 수 있다. 프록시 서비스 역시 무료로 운영되거나 명확한 운영주체가 고지되지 않은 경우라 할지라도 사용자들은 자신들의 기대가치인 우회 접속을 위해 쉽게 해당 서버를 이용하도록 자신의 컴퓨터 설정을 변경하게 된다.

3.3 비례성 고찰 결과

개인정보보호를 위한 제어권 차원에서의 프록시 서비스 사용과 이에 따른 사이버범죄 위협과의 비례성 고찰 결과를 정리하면 다음과 같다.

가. 개인 사용자의 PC를 식별할 수 있는 IP 정보는 다른 정보와 결합하여 용이하게 개인 식별이 가능한 개인정보로써의 의미를 갖는다.

나. 개인정보의 자기결정권은 헌법 제10조의 인간의 존엄과 가치 규정을 통하여 보장되어야 한다.

다. 개인정보자기결정권이 보장된다 하더라도 개인정보의 수집 목적과 해당 정보가 가지는 개인의 인격과의 연관성 등에 비추어 판단되는 것이 옳다.

라. 사이버범죄는 실제 세계의 범죄와 다르게 시·공간적 무제한성과 광역성, 증거인멸의 용이성, 비대면성, 익명성과 같은 특징을 갖는다.

마. 사이버 공간에서의 익명성은 "양성적 탈억제성 효과"와 "악성적 탈억제성 효과"를 두드러지게 한다.

바. 프록시 서비스가 제공하는 익명성은 사이버범죄의 익명성과 비대면성을 기반으로 한 발각과 원인규명의 곤란을 높인다.

정리를 통해 현행 프록시 서비스가 양성적 산업 영역으로 들어오기 위해서는 사용자들의 개인정보보자기결정권을 보장하되 사이버범죄의 위협을 조장하거나 관련 비용을 증대시키지 않도록 적정한 규제와 제도적 관리 체계가 필요함을 알 수 있다.

IV. 개선점 및 대응 방안

프록시 서비스에 대한 고찰을 통해 사용자 보호 및 개인정보보호 측면에서의 대응책과 사이버범죄의 예방 및 위협 관리 측면에서의 적정한 규제와 대응책이 필요함을 지적했다.

4.1 사용자 보호 측면에서의 개선점

프록시 서비스를 운영하기 위해 제작된 소프트웨어는 사용자들에게 직접적인 UI를 제공하는 접점으로써 또한 이를 이용하는 사용자들에게 해당 소프트웨어 기술은 디지털 규제자로서 사이버범죄에 있어 법률보다 더 강력하며 잘못된 구조에 대한 통제뿐만 아니라 만들어 놓은 구조안에서 벌어지는 행동을 형성할 수 있기 때문에 중요한 의미를 갖는다[14]. 따라서 관련 소프트웨어를 제작하는 경우 단순 기능 구현 뿐만 아니라 사회공학적 고려가 필요하다.

자동화된 프록시 서버 설정 프로그램의 경우 개인의 익명성 확보를 위한 사용 도구라기보다는 특정한 목적을 위한 사전 준비 도구로써의 의미가 크다. 순간적이고 지속적으로 프록시 서버를 갱신하며 사용하는 사용자의 컴퓨터가 통신서비스를 제공하는 시스템 입장에서는 로그 분석의 난해성을 가중시키는 존재로써 기업의 서비스 비용을 증가시킬 수 있다.

"정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제48조제3항은 "누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다." 라고 규정하고 있다. 또한 동법 제48조제2항은 "누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다."라고 규정하고 있기 때문에 개인의 익명성을 보장받기 위한 목적이라 하더라도 그 행위의 결과로 인해 정보통신시스템이나 정보통신망의 안정적 운영을 방해하지 않아야 한다. 또한, 이러한 프로그램을 제작 판매하는 경우 이와 같이 해당 프로그램에 대한 주의사항을 소비자들에게 사전 고지하여 소프트웨어의 잘못된 사용으로 인한 피해 예방을 위해 노력해야 한다.

프록시 클라이언트 프로그램 판매업자의 경우 유료로 운영되더라도 비용을 지불한 소비자와 실제 프록시 서비스를 제공하는 프록시 서버 사이의 중개역할을 담당하는 업체 특성을 이용해 법적 책임을 회피할 여지가 크기 때문에 소비자 권익보호를 위해서라도 자동화

된 프록시 서버 설정 프로그램을 유통하는 사업자를 통신판매업자로 규정하는 등의 적법한 관리규제가 필요하다.

4.2 개인정보보호 측면에서의 개선점

유·무료 프록시 서버를 운영하는 개인이나 기업을 대상으로 해당 서비스를 이용하는 개인들의 프라이버시가 안전하게 보호되고 있는지 검토될 필요가 있다. 사용자의 컴퓨터와 방문하고자 하는 사이트 사이의 트랜잭션 정보들이 악의적인 프록시 서버를 통해 수집되거나 위·변조 될 수 있기 때문에 사용자들의 주의가 필요하다.

현행 제도에서는 프록시 서버를 운영하는 사업자에 대해 정보보호안전진단과 같은 침해사고 예방조치를 권고할 수도 없다. 사업자의 적절한 보호조치와 운영관리를 위해서는 예방적 정보보호조치 이행이 반드시 필요하지만 프록시 서비스는 보호조치 의무 대상 범주에 명시되어 있지 않다[15]. 이러한 경우 많은 사용자들이 이용하는 프록시 서비스의 경우라도 보호조치 시행을 위한 근거가 없어 정작 서비스를 통해 개인정보 보호를 원했던 사용자들의 심각한 침해를 야기할 수 있다. 프록시 서비스에 대한 실태 조사를 통해 보호조치 시행이 필요한 규모의 사업체들은 적법한 제도적 예방조치를 취할 수 있도록 관리되어야 한다.

4.3 프록시 서비스 운영 측면에서의 개선

사이버범죄의 예방적 효과 및 사후 신속한 대응 및 복구를 위해 정보통신서비스 제공업자들의 내부감사 및 로그기록은 매우 중요하다. 정보통신서비스제공자는 "전기통신사업법" 제2조제1항제1호의 규정에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. 통신비밀보호법 제2조제11호에서는 전기통신사업자가 준수해야 할 "통신사실확인자료" 즉, 전기통신사실에 관한 자료에 대해 정의하고 있다.

통신사실확인자료에 포함되는 정보[16]

가. 가입자의 전기통신일시

나. 전기통신개시·종료시간

다. 발·착신 통신번호 등 상대방의 가입자번호

라. 사용도수

마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료

바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료

사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

또한 동법 시행령 제41조제2항에서는 통신사실확인자료 중 각목에 따른 보관기간을 정의하고 있다. 프록시 서비스 사업자에게 해당될 수 있는 마목과 사목의 경우 해당 정보의 보관기간을 3개월 이상으로 규정하고 있다. 이같은 조치는 사이버범죄의 발생 이후 적법 절차를 통한 통신사실확인자료 요청에 대응하여 원활한 수사를 진행할 수 있도록 한다. 하지만 대부분의 프록시 서비스 운영업체의 경우 이러한 의무 조치를 이행하지 않거나 할 수 없을 정도로 영세하며 제도적 기반도 취약하다. 이러한 상황은 피해 사업자들의 사이버범죄 대응에 대한 비용을 증가시키고 수사에 가장 중요한 초기 증거확보를 어렵게 하기 때문에 반드시 제도적 규제가 시행되어야 한다.

프록시 서비스 운영상의 미숙이나 제도적 기반의 취약을 이유로 이러한 기본적 조치들이 간과되어서는 안 된다. 이는 영리나 범죄를 목적으로 송신인의 전화번호를 변작하거나 거짓으로 표시할 수 없게 하고 있는 전기통신사업법의 해석에 따라 프록시 서비스 제공자의 목적을 재해석해야 하는 부담이 있다. 송신인의 전화번호와 컴퓨터 사용자의 IP정보와의 등치관계에 대해서는 법리해석이 따라야겠으나 서비스 제공 목적의 위법성에 대해서는 논란의 여지가 있다.

4.4 사이버범죄 예방적 측면에서의 개선

통신비밀보호법 제13조(범죄수사를 위한 통신사실확인자료제공의 절차)의 규정에 의거 검사 또는 사법경찰관은 수사 또는 형의 집행을 위해 필요한 경우 전기통신사업자에게 통신사실확인자료의 열람이나 제출을 요청할 수 있다. 하지만 즉시 수사 또는 형집행을 위한 상황은 아닐지라도 예방적 조치를 위해 통신사실확인정보가 요구되는 경우가 있다.

미국의 경우에는 국가기관의 행위가 개인의 '프라이버시에 대한 합리적인 기대(reasonable expectation of privacy)'를 침해하지 않는 경우에는 영장 없이도 수색이 가능하며[18], 수사기관의 영장 없는 수색은 개인의 프라이버시를 침해하지만, 영장요구의 예외에

의한 수색은 '합리적일 경우에는 수색이 가능하다'고 [19] 판시하고 있다. 국내의 경우 인터넷 본인확인제와 같은 제도를 통해 익명성에 기댄 사이버범죄 위협에 대한 예방적 조치를 취하고 있다. 인터넷 본인확인제가 헌법에서 금하고 있는 검열에 해당한다는 주장이 있지만 헌법재판소는 "검열은 행정권이 주체가 되어 사상이나 의견이 발표되기 이전에 예방적 조치로서 그 내용을 심사, 선별하여 발표를 사전에 억제하는, 즉 허가받지 아니한 것의 발표를 금지하는 제도를 뜻한다"고 판시한 바 사전적 내용 심사에 속하지 않는 인터넷 본인확인제를 검열이라고 볼 수 없을 것이다[20].

서비스 사업자가 자사의 시스템 보호와 내부 관리 규정에 따라 프록시 서비스를 이용한 사용자들을 제한하거나 예방적 활동을 위해 프록시 서비스 사용자의 로그를 요청하는 경우 현행법상 영장 없이는 불가능하다. 하지만 지속적인 IP 변경을 통해 공격을 시도하는 공격자를 색출하여 다수의 정상적인 사용자의 권리 침해 위협을 예방할 수 있다면 사이버범죄의 특수성과 합리적인 개인정보보호 기대수준에 따라 신속한 대응이 가능할 수 있도록 제도적 개선이 요구된다.

4.5 사이버범죄의 관할권 측면에서의 개선

프록시 서비스 제공업체들이 사용하는 IP 대역의 주소지가 우리나라가 아닌 국외지인 경우가 많다. 사이버범죄의 특성상 공간의 제약이 약해 행위지가 국내외를 넘나드는 경우가 많다. 우리나라는 사이버범죄의 국제적 분쟁과 관련하여 현행법에 근거하여 국제형사재판관할권을 확정한다. '범죄지'란 행위자가 범죄를 실행한 장소는 물론, 구성요건에 해당하는 결과가 발생하였거나 행위자의 표상에 따라 발생하였으리라고 추측되는 장소면 족한 것으로 보고 있다[21]. 따라서 국내에 거주하는 행위자가 국내 인터넷서비스를 이용하여 범죄행위를 하는 경우 뿐 아니라 외국에 거주하는 자가 외국의 인터넷서비스를 이용하여 우리나라에서 범죄행위의 결과를 발생시킨 경우에도 속지주의를 적용하여 우리 형법을 적용할 수 있을 것이다.

사이버범죄 대응의 국제적 공조를 위해 현재 유럽평의회 회원국뿐만 아니라 미국, 일본, 캐나다 등 40여개국이 서명한 "사이버범죄 협약"이 발효 중이다. 협약은 사이버범죄의 실체적 구성요소를 명확히 하고 이를 국내법에 반영하도록 한다. 이러한 국제적 협약 가입은 물론 사이버범죄에 대한 효율성을 높이기 위해서는 해당 국가들의 수사기관간의 협력 협정서가 효과적일 것이다. 결국 사이버범죄에 현실적으로 대처하기 위해서는 외국인의 국외범에 대하여 행위지를 근거로 하는 행위지법을 우선적으로 적용하되, 관련국간의 국제적인 협력을 필요로 한다[22].

V. 결 론

본 연구에서는 프록시 서비스의 개인정보 보호적인 측면과 사이버범죄 위협적인 측면에 대한 고찰을 통해 관련 사업과 서비스 기술에 대한 사용자 보호 및 개인정보보호 측면에서의 대응책과 사이버범죄의 예방 및 위협 관리 측면에서의 대응책을 도출하였다. 프록시 서비스가 개인의 개인정보자기결정권에 대한 권리행위로 사용될 수도 있지만 사이버범죄의 특성과 정보통신서비스 제공업자들의 예방적 권리 보호를 위해서 범죄 위협이 높은 행위에 대한 기술적 제어가 필요하고 산업적으로도 프록시 서비스를 사용하는 개인들의 범죄 위협 노출을 예방하기 위한 보호조치가 요구된다. 또한, 사이버범죄 발생 후 신속한 증거확보와 정확한 대응을 위한 국제적 협력체계를 구축하는 것도 매우 중요하다. 이를 통해 보다 효과적이고 공익에 부합하는 프록시 서비스 운영이 가능해 짐을 보여줬다. 향후 프록시 서비스에 대한 기술적 사례분석을 통해 범죄 위협이 높은 행태의 활동을 사전에 차단하고 정보서비스제공 시스템을 보호할 수 있는 기술적 연구가 필요해 보인다.

참고문헌

[1] Katharina Sobota,, Das Prinzip Rechtsstaat. Verfassungs- und verwaltungsrechtliche Aspekte, Mohr Siebeck, pp. 244, 1997.

[2] 김일수 외 공편, 법치국가와 형법, 세창출판사, pp. 46, 1998.

[3] 김철수, 헌법학 개론, 박영사, pp. 569, 2003.

[4] 연합뉴스, 애플·구글, 방통위에 위치정보 답변서 제출, 2011년 5월 13일.

[5] 헌법재판소, 2003헌마282, 425(병합), 2005년 7월 21일.

[6] Susan W. Brenner, "Cybercrime: re-thinking crime control strategies," Crime Online, Willan Publishing, pp. 14, 2007.

[7] Eric Hilgendorf/이원상(역), "유럽차원에서의 인터넷 형법 조화의 문제와 경향". 비교형사법 연구,

제8권 제2호, pp. 227-268, 2006년 12월.
〔8〕 백광훈, 사이버테러리즘에 관한 연구, 한국형사정책연구원, pp. 70, 2001.
〔9〕 David Davenport, "Anonymity on the Internet: Why the Price May Be Too High," Communications of the ACM, Vol. 45, No. 4, April 2002.
〔10〕 Wallace, P. M., "The Psychology of the Internet," 황상민 역, 에코 리브르, 2001.
〔11〕 John Suler, "The Online Disinhibition Effect," The Psychology of Cyberspace, Vol. 7, No. 3, pp. 321-326, July 2003.
〔12〕 한국청소년정책연구원, "인터넷 댓글에서의 청소년 인권침해 현황과 대응방안", 2008년 12월.
〔13〕 허만형, 사이버범죄에 대한 국가의 정책적 대응방안, 사이버커뮤니케이션학보 pp. 226-263, 2000년 11월.
〔14〕 David Wall, 정보화시대의 유비쿼터스 범죄, 형사정책 연구, 백지나 역, 한국형사정책연구원, pp. 11, 2008.
〔15〕 방송통신위원회. 한국인터넷진흥원, 정보보호 안전진단 해설서, pp. 29, 2010년 3월.
〔16〕 통신비밀보호법 제2조 제11호 가목부터 사목.
〔17〕 전기통신사업법 제100조.
〔18〕 Illinois v. Andreas, 463 U.S. 765, 771, 1983.

〈著者紹介〉

강 신 범(Shin-Beom Kang) 정회원
1997년 2월: 전북대학교 정보통신공학과 졸업
1999년 2월: 전북대학교 정보통신공학과 공학석사
2012년 2월: 고려대학교 정보보호대학원 공학박사
현재: (주)티앤에스 대표이사
소프트포럼 기술개발실장 / 전략기획본부장, 국정원 CA 보호프로파일 개발 연구위원, 국내 최초 인터넷뱅킹 시스템 개발 및 상용화, KTH 신사업전략팀장 / 금융사업TF장
〈관심분야〉 정보보호정책, 암호 프로토콜, 금융보안시스템, 통신공학 등

이 상 진(Sang-Jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 졸업
1989년 2월: 고려대학교 수학과 이학석사
1994년 8월: 고려대학교 수학과 이학박사
1989년 10월~1999년 2월: ETRI 선임연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 정교수
고려대학교 디지털포렌식연구센터 센터장, 한국디지털포렌식학회 편집이사, 세계포렌식경진대회 2년 연속 세계1위, 경찰청 휴대폰증거분석협의체 자문위원 등
〈관심분야〉 대칭키 암호, 정보은닉, 디지털포렌식 등

임 종 인(Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
1986년 3월~2001년 1월: 고려대학교 자연과학대학 정교수
2001년 2월~현재: 고려대학교 정보보호대학원 원장
대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 방송통신위원회 인터넷협의회 운영위원 등
〈관심분야〉 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등