일본의 P2P프로그램 정보유출 현황 및 대책 연구

김완수*, 김식**
*세명대학교 전산정보학과
**세명대학교 정보통신학부
e-mail:virtuews@freechal.com

A Study on Information leak state and measure by Peer-to-Peer Program in Japan

Wan-Soo Kim*, Sik Kim**
*Dept. of Computer and Information Science, Se-myung University
**School of Information and Communication Systems, Se-myung University

요 약

P2P프로그램에 대한 연구는 정보공유 및 성능 향상을 초점으로 많은 연구가 진행되어 왔다. 그러나 P2P 프로그램의 정보유출 문제에 대한 원인분석 및 대응방안에 대한 연구는 미비한 실정이다. 일본은 2004년부터 P2P프로그램을 통한 정보유출 사건이 빈번히 발생하고 있다. 이와 같은 이유로 본 연구는 일본의 P2P 프로그램을 통한 정보유출 현황, 원인, 대응방안을 연구했다. 정보유출 현황을 조사하기 위해 정보유출에 관련된 언론기사를 수집했고, 일본 P2P프로그램으로부터 유출되고 있는 정보를 30개월간 수집했다. 정보유출 원인을 이해하고 대응방안을 파악하기 위해서 일본 P2P프로그램의 사용현황, 정보유출 사례, 정보유출 원인, 일본 정부·기관·기업·군의 대응방안을 조사하고 분석했다. 유출된 정보를 수집한 결과 개인 신상정보, 기업, 관공서, 군 등의 내부 자료를 수집할 수 있었으며, 유출 정보로 인한 사회적 심각성을 이해할 수 있었다. 또한 일본 민·관·군의 정보유출 대응방안이 실효성을 거두고 있는가를 검증하기위해서 유출정보를 지속적으로 수집하였다. 그 결과 대응방안 적용 시점부터 유출정보가 급격히 감소했음을 확인했다. 이러한 연구 결과는 타 국가의 P2P프로그램을 통한 정보유출 대응방안수립에 도움이 될 것이다.

1. 서 론

많은 도구들과 시스템들은 인간 생활의 편리를 위해 만들어 지고 운용되지만 어느 순간 순기능이 역기능으로 변화되기도 한다. 인터넷 사용자들 상호간에 정보를 공유하기 위한 P2P프로그램도 역기능을 포함하고 있다. P2P프로그램을 이용하여 다른 사람의 정보를 훔치거나 유출시키기 위해 바이러스를 만들고, 위장된 프로그램이나 문서에 유해코드를 삽입하여 바이러스를 확산시키기도 한다. 일본에서는 특정 P2P프로그램을 대상으로 하는 바이러스의 확산으로 정보유출 사건이 빈번히 발생되고 있다. 이러한 정보유출의 원인은 무엇이며, 유출되고 있는 정보들은 무엇이 있으며, 대책은 어떻게 수립되었고, 효과가 있었는가를 이해하기 위해 연구를 수행했다. 본 연구 결과를 통해 일본의 P2P프로그램을 통한 정보유출 원인 및 대책을 이해할 수 있을 것이며, 한국에서 발생될 P2P프로그램을 통한 정보유출 대책 수립에 방향을 제시할 수 있을 것이다.

2. 본 론

2008년 3월 18일 일본 총무성에서 작성한 IT 선진국들의 정보통신인프라에 대한 비교를 수행한 보고서 "일본의 ICT 인프라에 관한 국제 비교 평가 리포트[1]"의 평가 결과 1위 일본, 2위 한국, 3위 핀란드, 4위 스웨덴, 5위는 네덜란드가 차지했다. 일본의 인터넷 이용자 수도 꾸준히 증가하여 2007년 3월 3세 이상 일본 인구 1억2,454만명 중 8,226.6만명이 인터넷을 사용하였고, 비율도 66.1%가 되었다.[2] 이와 같이 일본의 인터넷 사용자 수는 지속적으로 증가하고 있으며, P2P프로그램 사용도 증가하고 있다. 일본의 P2P프로그램 사용이 증가되면서 한국보다 정보유출 문제가 심각하게 발생 되었으며, 정보유출은 사회적 문제가 되었다. 본 연구는 일본 P2P프로그램 사용자들의 특징, 사용현황, 정보유출 원인, 대책을 조사하고 직접 수집한 결과를 분석하여 대책의 효율성을 확인했다.

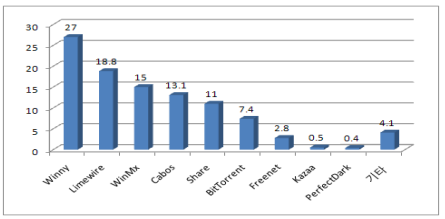
2.1 P2P프로그램

P2P(Peer-to-Peer Network)는 네트워크 구성에 참여하는 컴퓨터들의 능력과 대역폭의 성능에 의존하여 구성되는 통신망이다. 순수 P2P 파일 전송 네트워크는 클라이언트나 서버의 개념이 없이 동등한 계층 노드들이 서로 클라이언트와 서버 역할을 동시에 수행하게 된다. 이러한 P2P 네트워크 기술은 1999년 6월 Napster[3]로부터 시작되었다. P2P는 중앙 중재자형 P2P 동작방식과 순수 P2P 동작 방식이 있다. 중앙 중재자형 P2P 동작방식은 공유 자료를 P2P프로그램 사용자가 공유하지만, 자료검색을 하기 위해서는 정보목록을 유지하는 서버가 필요하다. 순수 분산형 P2P 동작방식은 P2P프로그램 사용자의 컴

퓨터를 이용하여 자료공유 및 검색을 수행하는 방식이다. P2P프로그램은 동작방식에 따라 개발되고 사용되고 있으며, 현재까지 연구의 초점이 되어왔다.

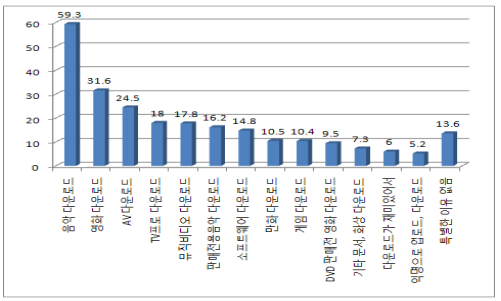
2.2 일본의 P2P프로그램 사용현황

일본에서 주로 사용하는 P2P프로그램은 (그림 1)과 같이 Winny[4]이고, 사용률은 270%를 차지하고 있다. 2위는 Limewire[5], 3위는 WinMX[6]이다. 주로 사용하고 있는 일본의 P2P프로그램은 약 9가지이며 10%이상의 이용자가 사용하고 있는 P2P프로그램은 5가지이다. 성·연령별로 40대 남성과 10대 여성은 Limewire을 가장 많이 이용했고, 기타 인원은 Winny를 가장 많이 이용하고 있다.



(그림 1) 일본의 P2P프로그램 사용 현황

일본의 "파일교환소프트웨어의 이용에 관한 조사 앙케이트 조사보고서[7]"에 의하면 P2P프로그램을 이용하는 목적은 (그림 2)와 같이 무료 음악, 영화, AV, TV 프로그램, 뮤직비디오, 소프트웨어, 만화, 게임 등을 다운로드하기 위해서였다. 그 중 P2P프로그램을 사용하는 가장 큰 이유는 무료음악 다운로드가 사용 목적의 60%에 해당했다. 30~40대 남성은 무료 AV를 다운로드 받기 위해 P2P프로그램을 사용하고 있었다. 다운로드 받은 경험도 음악파일이 78.2%로 가장 높게 나타났으며, 영상파일은 66.8%로 나타났다.



(그림 2) 일본의 P2P프로그램 사용 목적

자신의 파일을 P2P프로그램에 공유하고 있는 일본 P2P프로그램 사용자는 35.8%였으며, 남성이 여성보다 공유경험이 높았다. 또한 공유하고 있는 음악 파일은 평균 112.4개, 영상 파일은 86.3개였다. 공유를 위한 파일을 작성한 사용자는 25.7%였으며, 음악파일이 19.3%, 영상파일 9.8%, 음악파일은 여성이, 영상파일은 남성이 작성 경험이 많았다. 사용 소프트웨어는 Winny, Share 사용자가 상대적으로 많은 것이 특징이었다. P2P프로그램 사용에 문제가 있다고 생각하는 사람은 15.6%밖에 되지 않았으며, 앞으로도 P2P프로그램을 사용하겠다는 사용자는 35.5%로 나타났다. 이러한 통계로 부터 P2P프로그램을 통한 정보유출이 지속될 것임을 예측할 수 있다.

2.3 P2P프로그램을 통한 정보유출

2.3.1 정보유출 원인

일본에서 2003년 8월 Antinny라는 웜이 등장했다. Antinny는 가짜 에러 메시지를 표시하고, 자신을 자동으로 작동하도록 Windows 설정을 변경하고 자신을 복제했다. 복제된 Antinny는 자동으로 자신을 공개해서 Winny 네트워크에 감염대상을 확대했다. 2004년 3월에는 Antinny.B가 등장했다. 이후 지속적으로 Antinny의 아종들이 등장했고, Winny로 다운로드한 파일로 Antinny 및 그 아종들에 감염되는 사건이 발생되었다. 감염된 컴퓨터는 기업의 업무자료, 개인의 채팅기록, 메일, 사진, 패스워드 정보 등 다양한 정보들을 유출시키고 있다. 정보유출의 가장 큰 원인은 웜들이 모든 드라이브 속성을 변경하여 사용자의 의도와 다르게 모든 파일들이 공유되었기 때문이다. 야마다 얼터너티브(山田オルタナティブ) 웜은 컴퓨터를 HTTP 서버로 만들어, 컴퓨터 자료 전체를 인터넷에 공개했으며, 웜에 감염된 사람들 상호간에 HTTP 링크로 상호 접속하는 기능이 추가되었다. 이러한 바이러스 중에 가장 유명한 것은 Antinny와 그 아종들로 「불알 바이러스(キンタマウイルス)」라고 통칭하고 있다. 바이러스 이름이 「불알 바이러스」로 붙여진 것은 컴퓨터 화면을 캡처해서 그 화상을 업로드하거나 컴퓨터의 파일을 정리해 업로드하는 파일명이 「[キンタマ]*.확장자」와 같이 붙여졌기 때문이다. Winny네트워크에서 활동 중인 웜은 여러 가지가 존재하고 현재도 계속 발생하고 있다. Winny로 정보유출이 되면 회수가 불가능한 것이 또 하나의 큰 특징이다.[8] 한번 Winny네트워크에 유출된 정보는 캐시를 보관·유지하는 컴퓨터가 존재하는 한 계속적으로 Winny네트워크상에 상주한다. 따라서 유출된 정보를 삭제하는 것은 Winny사용자의 데이터를 모두 삭제하지 않는 한 결국 불가능하다. Winny 이외에도 Share에서 웜으로 인해 정보유출이 발생되고 있다. 일본 P2P프로그램 사용 순위와 상이하게 Winny와 Share에서 정보유출이 많이 발생하고 있는 이유는 두 P2P프로그램의 취약점을 이용한 웜의 생성 및 확산이 이유가 되었음을 확인 할 수 있었다.

2.3.2 정보유출 사례

P2P프로그램을 통한 정보유출은 민간 기업이나 개인에게 국한되지 않고 일본 우정공사, 형무소, 재판소, 원자력 발전소, 지방 자치단체, 관공서 및 경찰, 자위대에서도 발생했다. 정보유출의 가장 큰 이유는 기밀정보나 개인 업무자료를 자택의 개인 컴퓨터에서 작업을 하고 저장하는 과정

에서 바이러스에 감염되었기 때문이다.

<표 1> 2005년 3월~2006년 3월까지 일본의 정보유출 현황

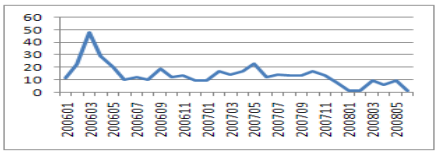
분류	정보유출 건수
민	59
관	44
군	9

<표 1>은 내각관방정보시큐리티센타(NISC)에서 2005년 3월부터 2006년 3월까지 정보유출현황[9]을 조사한 결과이다. 전체 100건의 정보유출이 발생되었으며, 지차체 관계 정보 및 민간정보가 다수 유출 된 것을 확인할 수 있었다. 정보유출 현황을 확인하기 위해 일본 언론사의 정보유출 기사를 수집한 결과 417건의 유출사고가 있었다. 언론기사의 유출정보를 수집하기 위해 2006년 1월부터 2008년 6월까지 Winny와 Share를 사용하여 유출 정보를 수집했다. 수집된 결과 중 언론기사로 공개되지 않은 정보를 70건이나 수집할 수 있었다. 이 결과를 민·관·군으로 분류한 결과는 <표 2>와 같다.

<표 2> 2006년 1월~2008년 6월까지 일본의 정보유출 현황

분류	정보유출 건수 (언론 공개)	정보유출 건수 (언론 미공개)	합계
민	286	36	322
관	85	10	95
군	14	19	33

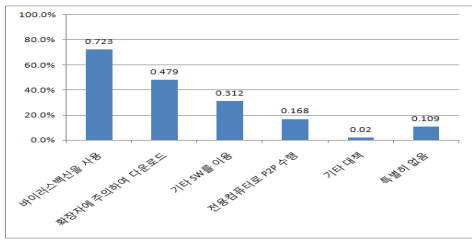
P2P를 통한 정보유출 중 민간분야는 기업의 고객정보, 기업 내부정보, 직원정보가 많았으며, 학교의 경우 졸업생 및 재학생 관련 신상정보, 병원정보로는 환자정보 등이 유출되었다. 일본 행정기관의 경우는 내부문서 및 업무문서, 직원정보, 국민들의 개인신상정보, 경찰의 수사 정보, 전과자 및 피해자 정보, 건강보험가입자 정보 등이 유출되었으며, 군 유출정보로는 자위대 군사자료, 군인 신상정보, 부대 배치도 및 무기제원, 훈련정보 등이 유출되었다. 2008년 1월부터 2008년 6월까지도 민간분야 23건, 국가행정기관 9건 등 정보유출은 계속되고 있다. 그러나 일본 자위대의 정보유출 건수는 (그림 3)과 같이 현저히 감소되었고, 2006년 3월 이후 유출정보를 수집한 결과 지속적으로 감소 추세인 것을 확인할 수 있었다. 또한 일본 내각관방정보시큐리티센타(NISC)의 발표자료를 통해 민·관·군 모두 정보유출 현황은 지속적으로 감소하고 있음을 확인할 수 있었다.



(그림 3) 일본 자위대 정보유출 현황

2.4 정보유출 대책

2007년 5월 내각관방정보시큐리티센타(NISC)의 "일본의 정보시큐리티 정책 방향성" 발표에서 자택에 허가되지 않은 정보가 반입되는 문제가 표면화 되었다. 직장 내부에서 컴퓨터 부족을 이유로 개인 컴퓨터를 반입하여 사용하는 관습이 문제가 되고 있음을 인식했고, 이러한 사유로 정부의 비밀문서 및 자위대 비밀문서가 다수 유출되었음을 확인했다. 문제 해결을 위해 일본 정부는 2005년 12월 정부기관 정보 시큐리티 대책 통일 기준을 결정했고, 2006년 2월 "제1차 기관 정보 시큐리티 기본계획" 결정했다. 일본의 정보보안 관련 시책은 Winny 대책뿐만 아니라 여러 가지 위협으로부터 정보를 지키는 것이었으며, 정보의 등급설정으로 기밀성의 확보, 완전성의 확보, 가용성의 확보 대책을 실시하는 것이었다. 민·관·군에서 정보유출에 대한 수많은 대책이 수립되었으며, P2P프로그램을 통한 정보유출의 사회 이슈화에 따라 일본 P2P프로그램 사용자의 의식도 변화되었다. P2P프로그램을 통한 정보유출이 사회로부터 주목을 받게 되면서 야후 재팬에서는 2006년 3월 P2P 정보유출 뉴스 전용 게시판[10]을 개설하였으며, 동년 3월 마이크로소프트, 시만텍, 트렌드마이크로, NTT에서는 P2P프로그램을 통한 정보유출 주의를 발표했다. 이러한 P2P프로그램을 통한 정보유출이 사회적 이슈화 및 관심을 받음에 따라 2007년 파일교환 소프트웨어에 의한 정보유출에 관한 조사[11]에서 P2P프로그램 이용자 중 90% 정도가 보안대책을 실시했다. (그림 4)와 같이 바이러스 백신을 사용하거나 의심되는 확장자는 다운로드할 경우 주의하며, P2P프로그램 전용컴퓨터를 사용하는 사용자 보안대책을 수립했다.



(그림 4) 2007년 일본 P2P프로그램 사용자의 보안 대책

2007년 5월 총무성 내각관방정보시큐리티센타(NISC)의 일본 정보시큐리티 정책 방향성 발표에서 과거 사용자가 P2P프로그램 사용을 중지 한 이유에 대한 설문 조사결과 "보안, 바이러스가 걱정"이라는 항목이 2005년부터 2007년까지 약 30%이상으로 3년간 1위를 차지했다. 일본 정부기관 및 자위대의 정보유출 대책을 조사하고 분석하여 <표 3>과 같이 일본 정부의 정보유출 대책을 정리했다. 일본 정부는 다양한 업무지침 발표와 정보유출 방지를 위한 SW를 개발했고, 조직 개선을 통해 정보유출 대책을 수행했다. 자위대는 일본 정부기관 보다 더 강력히 정보유출

대책을 수립했다. 업무용도의 개인 컴퓨터 사용을 금지하도록 하였으며, 이를 위해 컴퓨터를 보급하고, 인력관리 및 조직개선, SW도입, 업무지침을 수행했다. 자위대의 정보유출 대책은 <표 4>와 같이 요약했다. 이러한 자위대의 정보유출 대책은 (그림 3)과 같이 2006년 3월을 기점으로 효과를 거두고 있음을 확인할 수 있다.

<표 3> 일본 정부기관의 정보유출 방지 주요 대책

분 류	일 시	기 관	대 책
업무지침	´06.2.22	법무성	자택 PC의 업무파일 삭제 지시
SW도입	´06.4.20	내각 관방	Winny 대책 소프트웨어, 산관학 팀에서 개발 결정
업무지침	´06.5.4	총무성	Winny를 통한 정보유출 방지를 위해 직장 외에서 Winny 접속 규제 지침 마련
SW도입	´06.5.26	문부 과학성	정보유출방지를 위해 문부과학성에서 안전성을 높이는 소프트웨어 개발 착수
SW도입	´06.9.1	총무성	파일 교환 소프트웨어의 정보유출을 방지하기 위해 신기술 개발 착수
SW도입	´07.3.9	경찰청	정보유출 대책을 위해 모든 PC에 암호 소프트웨어 설치
조직개선	´07.4.27	내각 관방	정부의 보안 계획에 의거 정보누설 방지 신시스템 개발
SW도입	´07.6.8	NICT [12]	보안사고 대책 기술 「NICTER」 공개
업무지침	´07.6.22	경찰청	경시청의 정보유출로 인해 개인 PC 긴급 점검 지시
업무지침	´07.8.3	총무성	개인정보 유출 사건으로 일본 우정공사에서 재발 방지책 총무성에 보고
업무지침	´07.12.7	IPA	IPA 경고,「Winny를 사용하는 한 정보유출은 없어지지 않는다」

<표 4> 일본 자위대의 정보유출 방지 주요 대책

분 류	일 시	기 관	대 책
업무지침	´06.3.2	방위청	개인 사용 목적의 PC로 비밀 정보 취급 전면 금지 실시
HW교체	´06.3.9	방위청	정보유출방지를 위해 관비로 PC 7만대 지급 계획 발표
SW도입	´06.3.30	방위청	Winny 문제로 자료 암호화, 외부 정보유출 대책 실시
HW교체	´06.4.20	방위청	정보누설방지책으로 Winny가 동작하지 않는 PC 56,000대 지급
SW도입	´07.1.26	방위성	Winny 정보유출 방지 소프트웨어´07. 4월 도입 발표 ※07.1.9 방위청에서 방위성 승격
인력관리	´07.5.18	방위성 방위상	정보유출로 인해 방위상이「부하 전원에게 개별 면담」지시
인력관리	´07.6.29	해상 자위대	해상자위대 기밀 데이터 유출 방지를 위해 외국인 배우자가 있는 대원은 정보부서에서 타부서로 발령 지시
업무지침	´07.8.3	방위성	내부 고발 제도 개정, 정보 유출 대책 강화
조직개선	´07.8.3	방위성	정보유출방지 강화를 위해 정보보전대 본부 설치
조직개선	´08.1.18	방위성	정보유출대책회의 개최
조직개선	´08.5.2	방위성	사고방지기술본대책회의 설치

3. 결론

본 연구를 통해 일본 P2P프로그램 현황, 사용용도, 정보유출 현황·원인·대책을 살펴보았으며, 정보유출 피해가 심각함을 언론정보와 수집결과를 통해 확인 할 수 있었다. 다수 인터넷 사용자들이 자신의 컴퓨터 및 P2P프로그램이 안전할 것이라는 믿음을 갖고 있지만, P2P프로그램을 통해 공유되고 있는 다양한 프로그램과 파일들은 악의적 프로그래머가 개발한 악성코드에 의해 감염되어 있는 경우도 발생되고 있다. 최근에 만들어진 웜에 의해 감염된 문서나 파일들은 백신에 의해 발견 및 치료되지 않기 때문에 정보유출 문제는 지속적으로 발생되고 있다. 일본은 P2P프로그램의 바이러스 대응을 위해 백신개발, 정보유출 언론홍보, 교육확대, 개인컴퓨터를 통한 업무금지, 업무용 컴퓨터 보급 확대, 정보유출 방지 전문 프로그램 개발, 파일 암호화, 업무 자료의 반출 금지 정책 수립, 인력관리, 조직개선 등의 노력을 수행하고 있음을 확인했다. 정보유출 대책은 정보유출 기사 및 유출된 정보를 수집한 결과 자위대의 경우 2008년 이후 단 1건의 정보유출도 없었다. 이러한 결과는 일본 관·군의 P2P프로그램을 통한 정보유출 대책이 효과를 거두고 있음을 증명하고 있다. 앞으로 한국의 P2P프로그램을 통한 정보유출 현황 및 대책을 조사하고 한국과 일본의 정보유출 원인, 대책에 대한 차이점을 연구할 것이다. 이러한 연구결과는 다른 국가 및 한국에서 발생될 정보유출 원인 및 대책 수립에 도움이 될 것이다.

참 고 문 헌

[1] 總務省, 日本のＩＣＴインフラに關する國際比較評価レポート概要, 2008. 3

[2] Impress R&D, インターネット白書, 31페이지, 2007. 7. 1

[3] Napster, http://free.napster.com

[4] 金子勇(Kaneko Isamu), Winnyの技術, 2005. 10

[5] Limewire, http://www.limewire.com

[6] Winmx, http://win-mx.cool.ne.jp

[7] 社団法人コンピュータソ1フトウェア著作權協會, 社団法人日本レコード協會, 日本ﾌ國際映畵著作 權協會, ファイル 交換ソフトの利用に關する調査 アンケート調査報告書(概要版) , 2007. 12

[8] IPA(정보처리추진기구), http://www.ipa.go.jp

[9] 內閣官房情報セキュリティセン(NISC), 我が國の情報セキュリティ政策の方向性, 2007.5

[10] http://dailynews.yahoo.co.jp/fc/domestic/winny/

[11] 株式會社日立製作所, 2007 年ファイル交換ソフトによる情報漏えいに關する調査, 2007. 12. 21

[12] NICT(National Institute of Information and Communications Technology - 情報通信研究機構), http://www.nict.go.jp