논문 2009-1-10

P2P프로그램을 통한 한국과 일본의 정보유출 현황 및 대책 연구

A Study on the Information Effluence State and Measure by Peer-to-Peer Programs in Korea and Japan

김완수*, 김식**

Wan-Soo Kim, Shik Kim

요 약 네트워크 인프라의 확충과 인터넷 활용 증대로 한국과 일본에서 P2P프로그램 사용이 활성화되고 있으며 이를 통한 정보유출 문제가 증대되고 있다. 본 연구는 두 국가에서 P2P를 통해 유출되고 있는 자료들을 수집하여 심각성을 확인하였고, 어떤 대책이 수립되고 적용되었는가를 연구하였다. 또한 대책 적용 시기별 유출된 자료를 수집하여 대책의 실효성을 검증하였다. 두 국가 모두 개인정보 유출이 발생되고 있었지만, 특히 일본의 경우 개인정보 뿐만 아니라 기업, 행정기관, 군 등 광범위한 범위에서 많은 자료들이 유출되고 있음을 확인했다. 정보유출 대책으로 한국은 개인 및 P2P서비스 업체를 중심으로 대응방안이 시행되고 있으며, 일본은 각 기관별 업무지침, 조직관리, SW개발 및 보급, HW보급 등 다양한 방안을 시행하고 있다. 본 연구를 통해 일본이 한국보다 정보유출 문제가 심각하며, 이에 대한 대책도 잘 수립되고 적용되고 있음을 확인했다. 따라서 일본의 P2P프로그램을 통한 정보유출 대책을 타산지석으로 삼는다면 한국의 정보유출 문제를 미연에 방지할 수 있으리라 기대한다.

Abstract Information Effluence leaks are caused by the wide use of the P2P program in Japan and Korea lead by the increase of internet use and network infrastructure expansion. This research confirms the seriousness of the data collected from the P2P leaks of the two countries and furthers its study by researching how countermeasures are applied. The effectiveness is verified by collecting data according to countermeasure applied periods. Both countries had information leaks, but in the case of Japan, not only personal information leaks but corporation, administrative agency, military, and others in a wide range as well. As a countermeasure against information effluence, Korea is enforcing counter plans mainly against the P2P service businesses and for Japan, various plans are taken such as business guides for each agency, organization management, SW development and supply, HW supply, and ect. The leaks in Japan were more severe than the ones in Korea but they had well planned countermeasures that were applied. Therefore if the Japanese countermeasure on information effluence of P2P programs is taken as a lesson, Korea can prevent the problem of leaks beforehand.

Key Words : P2P, 정보유출, Winny, Share

Ⅰ. 서 론

인터넷 사용자들 상호간에 정보를 공유하기 위한 P2P 프로그램은 성능 향상을 목적으로 구조설계, 사용자인증, 네트워크 구현기술, 트래픽, 공유방식, 검색알고리즘 등을 중심으로 연구되고 있으며, 피해에 대한 연구는 저작권 및 개인정보유출에 초점을 두고 있다. 최근 P2P프로그램을 통해 발생되는 피해는 저작권 문제 뿐 만아니라

*정회원, 세명대학교 전산정보학과
**정회원, 세명대학교 정보통신학부
접수일자 2008.12.10, 수정완료 2009.2.9

개인정보유출을 넘어 기업의 비밀문서나 군사비밀문서 유출 등 심각한 상태이다. 이러한 사례는 한국 및 일본에서 모두 발생되고 있지만 일본의 경우 특정 P2P프로그램을 대상으로 하는 바이러스의 확산으로 더욱 심각하게 정보유출 사건이 발생되고 있음을 본 연구를 통해 확인하였다. 한국의 P2P프로그램 정보유출 및 대책에 대한 연구는 2004년 정보보호진흥원의 「개인정보 유출 사례 검토 및 대책」, 정보통신부의 2005년 「개인정보보호 수칙 마련」 및 2007년 금칙어 적용 등으로 일본의 다양한 정보유출대책에 비해 미비한 실정이다. 이와 같은 이유로 두 국가의 P2P프로그램을 통한 정보유출 문제점, 특징, 대책을 연구하기 위해 2006년 1월부터 2008년 6월까지 일본 P2P프로그램을 중심으로 정보유출 현황, 대책, 대책 적용시기별 정보유출 추이를 연구하여 대책의 실효성을 검증하였고, 한국에서 시급히 적용해야할 대책을 제시하였다.

Ⅱ. 본 론

한국의 인터넷 인프라가 일본보다 발전하였으며, 인터넷 활용 인구비율도 높다고 인식하는 사람들이 많이 있다. 그러나 2008년 3월 18일 일본 총무성에서 작성한 IT 선진국들의 정보통신인프라에 대한 비교를 수행한 보고서 「일본의 ICT 인프라에 관한 국제 비교 평가 리포트[1]」에서 평가 결과 일본 1위, 한국 2위, 핀란드 3위, 스웨덴 4위, 네덜란드가 5위를 차지했다. 일본의 인터넷 이용자수도 꾸준히 증가하여 2007년 3월 3세 이상 일본 인구 1억2,454만 명 중 8,226.6만 명으로 66.1%가 되었다[2]. 과거 한국의 인터넷으로 인한 사회문제가 다른 나라의 모델이 되었지만, 이제는 한국도 일본, 핀란드, 스웨덴, 네덜란드 등의 인터넷 문제를 이해해야 한다.

1. P2P프로그램의 사용 현황

일본에서 주로 사용하는 P2P프로그램은 그림 1과 같이 Winny[4]이고, 사용률은 27.0%를 차지하고 있다. 2위는 Limewire[5], 3위는 WinMX[6]이다. 주로 사용하고 있는 일본의 P2P프로그램은 약 9가지이며 10%이상의 이용자가 사용하고 있는 P2P프로그램은 5가지이다.

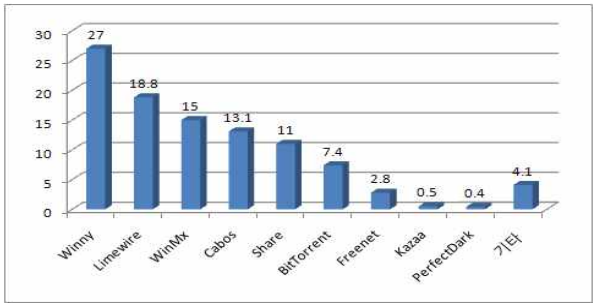

그림 1. 일본의 P2P프로그램 사용 현황
Fig 1. Present conditions of Japan's P2P program.

성·연령별로 40대 남성과 10대 여성은 Limewire을 가장 많이 이용했고, 기타 인원은 Winny를 가장 많이 이용하고 있다[7].

한국에서 많이 사용하는 P2P프로그램은 2008년 7월 현재 프루나[8], 파일구리[9], 소리바다[10], 피디팝[11], 몽키3[12], 엔피[13], 당나귀[14] 등이 있다. 프루나는 25.35%, 파일구리는 24.47, 소리바다는 19.77%의 점유율로 3개의 P2P 프로그램이 약 70% 점유율을 차지하고 있다[15].

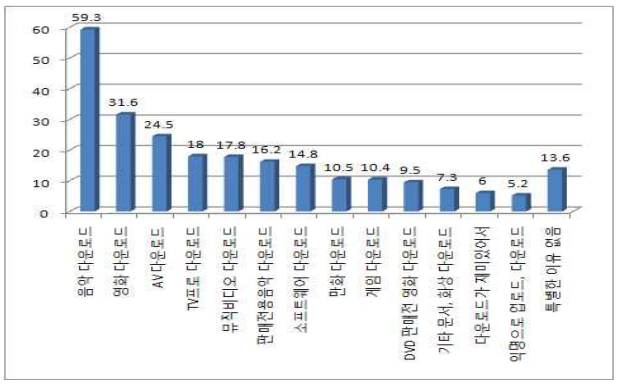

그림 2. 일본의 P2P프로그램 사용 목적
Fig 2. Purpose of Japan's P2P usage.

일본의 「파일교환소프트웨어의 이용에 관한 조사 앙케이트 조사보고서[7]」에 의하면 P2P프로그램을 이용하는 목적은 그림 2와 같이 무료 음악, 영화, AV, TV 프로그램, 뮤직비디오, 소프트웨어, 만화, 게임 등을 다운로드하기 위해서였다. P2P프로그램을 사용하는 가장 큰 이유는 무료음악 다운로드가 사용 목적의 60%에 해당하였다. 30~40대 남성의 경우 영화 보다는 무료AV를 다운로드 받기 위해 P2P프로그램을 사용하고 있었다. 다운로드 받은 경험도 음악 파일이 78.2%로 가장 높게 나타났으며, 영상파일은 66.8%로 나타났다. 자신의 파일을 P2P프로그램에 공유하는 사용자는 35.8%였으며, 남성이 여성보

다 공유 경험이 높았다. 또한 공유하고 있는 음악 파일은 평균 112.4개, 영상 파일은 86.3개였다. P2P프로그램 사용에 문제가 있다고 생각하는 사람은 15.6%밖에 되지 않았으며, 앞으로도 P2P프로그램을 사용하겠다는 사용자는 35.5%로 나타났다.

한국의 경우 10대 이상의 인터넷 사용자 중 60%가 P2P프로그램을 사용하고 있으며, 사용 목적은 그림 3과 같이 음악파일 공유가 38.9%, 영화파일 공유 35.0%, 프로그램공유가 12.0%를 차지했다[16]. 한국과 일본 모두 음악파일 및 영화, 프로그램 공유를 위한 목적으로 P2P프로그램을 사용하고 있었으며, 한국에 비해 일본은 성인물 공유 목적이 높게 나타났다.

그림 3. 한국의 P2P프로그램 사용 목적
Fig 3. Purpose of Korea's P2P usage.

2. P2P프로그램을 통한 정보유출

가. P2P프로그램을 통한 정보유출 원인

일본에서 2003년 8월 Antinny라는 웜이 등장했다. Antinny는 가짜 에러 메시지를 표시하고, 자신을 자동으로 작동하도록 Windows 설정을 변경하고 자신을 복제하였다. 복제된 Antinny는 자동으로 자신을 공개해서 Winny네트워크에 감염 대상을 확대하였다. 2004년 3월에는 Antinny의 아종인 Antinny.B가 등장하였다. 지속적으로 Antinny의 아종들이 등장했고, Winny로 다운로드한 파일로 Antinny 및 그 아종들의 웜에 감염되는 사건이 발생되면서 감염 컴퓨터 내부의 비공유 파일들이 유출되기 시작했다. 이러한 웜은 기업의 업무자료, 채팅기록, 메일, 사진, 비밀번호 등 다양한 정보들을 유출시켰다. 정보유출의 가장 큰 원인은 특정 P2P프로그램을 대상으로 하는 웜들이 모든 파일을 공유할 수 있게 드라이브 속성을 변경하여 사용자의 의도와 다르게 모든 파일들을 공유시켰기 때문이다. 초기의 웜은 컴퓨터 화면을 캡쳐하는 수준에서 점차 새로운 기능의 아종들이 등장하였다. 이러한 바이러스 중에 가장 유명한 것은 Antinny 바이러스와 그 아종들로 「불알바이러스(キンタマウイルス)」라고 통칭하고 있다. Winny네트워크에서 활동중인 웜은 여러 가지가 존재하고 계속 아종들이 발생되고 있다. 정보유출 사건으로 유명한 Antinny의 아종은 표 1과 같다.

표 1. Antinny 웜의 아종
Table 1. Antinny subspecies of worms.

웜	내 용
Antinny	-´03.8, 감염되면 가짜 에러 메시지를 표시하고 자신을 자동으로 작동하도록 Windows의 설정변경 및 자신을 복제 - 복제된 자신을 자동으로 공개해서 Winny 네트워크에 송신함으로써 감염대상 확대
Antinny.B	-´04.3, 자신을 메모장 아이콘으로 표시 - 자기 자신을 Windows의 Temporary에 svhost.exe로 복사 - 시스템 폴더에 <랜덤한 파일명>.exe 형식의 파일을 작성하여 서비스 프로세스에 상주시킴
Antinny.G	-´04.3, Winny를 악용해서 개인정보를 흘뿌리는 최초의 폭로형 바이러스 - 감염된 PC에서 사용자명이나 메일주소 등 개인정보를 훔쳐 Winny 네트워크에 송신
Antinny.K	-´04.4, Antinny.G의 아종, 수법은 거의 비슷, 수집한 개인정보를 ACCS[17] 웹사이트에 송신
Antinny.L	-´04.5, Antinny.G의 아종 - 수법은 유사하지만 작성하는 파일이나 복제파일명이 다르며, 사용자 개인정보를 텍스트파일로 만들고, 컴퓨터 화면을 캡처하여 ZIP파일에 모아 Winny네트워크에 송신
Nullpos	-´04.8, Antinny와 다른 계통의 Winny 관련 바이러스 - 부적절한 폴더에 파일을 풀어버리는 취약성을 악용
Antinny.AA, Antinny.C	-´05.6 - 정보유출의 위험도가 높음 - Antinny.G의 기능에 쿠키, 메일, 엑셀, 워드 등 다양한 데이터 유출
EXponny	-´06.3, Winny의 설정을 변경해 PC 전체의 하드디스크드라이브를 업로드 폴더로 공개
Antinny.BF	-´06.4, - Outlook Express의 inbox.dbx나 folder.dbx 를 ZIP파일로 만들어 유출

Winny네트워크에 유출된 정보는 캐시를 보관·유지하는 컴퓨터가 존재하는 한 지속적으로 Winny네트워크상에 상주한다[18]. 따라서 Winny사용자의 데이터를 모두 삭제하지 않는 한 유출된 정보를 삭제하거나 회수하는

것이 불가능하다. 이 점이 Winny에서 정보유출로 인한 파급효과가 큰 이유이다. 일본 P2P프로그램 사용 순위와 상이하게 Winny와 Share에서 정보유출이 많이 발생하고 있는 이유는 두 P2P프로그램의 취약점을 이용한 바이러스의 생성 및 확산이 원인이 되었음을 알 수 있었다.

나. P2P프로그램을 통한 정보유출 사례

한국에서 P2P프로그램을 통해 유출되는 대부분의 정보는 개인정보가 가장 많았다. 정보통신부 정보보호기획단 정보윤리팀의 2007년 11월 P2P 개인정보 관련 자료[19]에 의하면 표 2와 같이 프루나, 동키호테, 파일비, 파일구리 등을 통해 2007년 7월까지 많은 수의 성명, 주민등록번호, 주소, 연락처 등 2가지 이상의 정보가 포함된 개인정보가 유출되었음을 확인할 수 있었다.

표 2. 한국의 P2P네트워크에서 개인정보 유출 건수
Table 2. The number of information effluence cases from the Korean P2P network.

시기	프루나	동키호테	파일비	파일구리	위디스크	엔피
´06.11	4,496	6,357	2,397	1,948	1,740	836
´07.3	56	27,199	20,787	19,839	114	668
´07.5	31	2,981	195	-	397	-
´07.7	280	14,445	12,694	119	-	-

그림 4은 2008년 7월 파일구리를 통해 이력서 정보를 검색한 결과이다. 개인정보보호를 위해 “이력서” 단어검색은 수행되지 않도록 되어 있었지만, "력서"란 검색어를 통해 이력서 관련 정보 641개를 검색할 수 있었다. 또한 일부 파일에서는 이력서 작성자의 주민등록번호 및 이력정보를 확인 할 수 있었다.

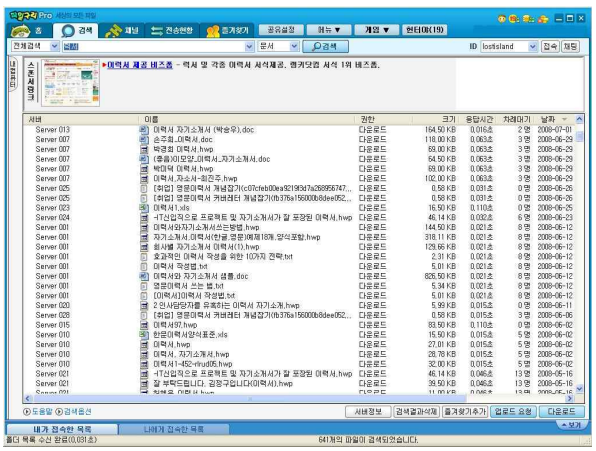

그림 4. 파일구리를 통한 이력서 정보 검색
Fig 4. Resume information search from Fileguri.

일본의 경우 P2P프로그램을 통한 정보유출은 민간 기업이나 개인에게만 국한되지 않고 일본 우정공사, 형무소, 재판소, 원자력 발전 시설, 지방 자치단체 등 관공서 및 경찰, 자위대에서도 발생하였다. 정보유출의 가장 큰 이유는 내부정보나 개인 업무자료를 자택으로 이동하여 바이러스에 감염된 컴퓨터에서 업무를 수행했기 때문이다. 자택의 개인 컴퓨터는 가족구성원 누구나 사용가능하기 때문에 아이들 또는 방문자에 의해 자신도 모르는 사이에 바이러스에 감염될 확률이 높다.

표 3은 내각관방정보시큐리티센타(NISC)에서 「2005년 3월~2006년 3월까지 정보유출현황」을 조사한 결과이다[20]. 전체 112건의 정보유출이 발생되었으며, 지방자치단체 관련 정보 및 민간정보가 다수 유출 된 것을 확인할 수 있었다.

표 3. 2005.3~2006.3월까지 일본의 정보유출 현황
Table 3. The status of information effluence in Japan from 2005.3 to 2006.3.

분류	정보유출 건수(공개)
민	59
관	44
군	9

일본 행정기관의 정보유출 발표자료 뿐만 아니라 본 연구를 위해 2006년 1월~2008년 6월까지 일본 P2P프로그램을 통한 정보유출 자료를 수집한 결과 417건을 수집할 수 있었다. 또한 행정기관의 발표자료 및 언론기사로 공개되지 않은 유출정보를 70건이나 수집할 수 있었다. 수집결과를 민·관·군으로 분류한 결과는 표 4와 같다.

표 4. 2006.1~2008.6월까지 일본의 정보유출 현황
Table 4. The status of information effluence in Japan from 2006.1 to 2008.6.

분류	정보유출 건수(공개)	정보유출 건수(비공개)	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 등

이 유출되었음을 확인하였다. 행정기관은 업무문서, 직원 정보, 개인신상정보, 경찰의 수사정보, 전과자 및 피해자 정보, 건강보험가입자정보 등이 유출되었음을 확인하였다. 군 유출정보로는 군사자료, 군인 신상정보, 부대 배치도 및 무기제원, 훈련정보 등이 유출되었음을 확인하였다. 2008년 1월~2008년 6월까지 민간분야 23건, 국가행정기관 9건 등 정보유출은 계속되고 있음을 수집결과를 통해 확인 하였다. 그러나 자위대의 정보유출 건수는 수집결과 그림 5와 같이 현저히 감소되었고, 2006년 3월 이후 유출정보를 수집한 결과 지속적으로 감소 추세인 것을 확인하였다. 또한 일본 내각관방정보시큐리티센타의 발표 자료를 통해 민·관·군 모두 정보유출 현황은 지속적으로 감소하고 있음을 확인할 수 있었다.

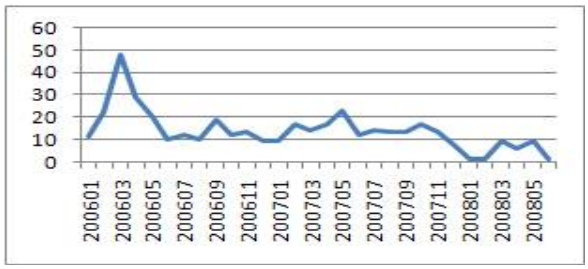

그림 5. 일본 P2P프로그램 전체 자료 유출 추이
Fig 5. The transition of the whole data exposed in Japan's P2P program.

3. 정보유출 대책

가. 일본의 P2P프로그램 정보유출 대책

2007년 5월 내각관방정보시큐리티센타의 「일본의 정보시큐리티 정책 방향성」 발표에서 자택에 허가되지 않은 정보가 반입되는 문제가 표면화 되었다. 직장내 컴퓨터 부족을 이유로 개인컴퓨터를 반입하여 사용하는 관습이 문제가 되고 있음을 인식했고, 이러한 사유로 정부의 비밀문서 및 군 비밀문서가 다수 유출되었음을 확인하였다. 이러한 문제를 해결하기 위해 일본 정부는 2005년 12월 정부기관 정보 시큐리티 대책 통일 기준을 결정했고, 2006년 2월 「제 1 차 기관 정보 시큐러티 기본계획」 결정하였다. 2006년은 정보보안에 대한 일본의 전략적 정책 실시의 시발점이 되었다. 일본의 정보보안 관련 시책은 Winny 대책 뿐 만 아니라 여러 가지 위협으로부터 정보를 지키는 것이었으며, 정보 등급설정으로 기밀성의 확보, 완전성의 확보, 가용성의 확보 대책을 실시하는 것이었다. P2P프로그램을 통한 정보유출이 사회 이슈화가 됨에 따라 일본 P2P프로그램 사용자의 의식도 변화되었다. P2P프로그램을 통한 정보유출로 인해 야후재팬에서는 2006년 3월 P2P 정보유출 뉴스 전용 게시판[21]을 개설하였으며, 동년 3월 마이크로소프트, 시만텍, 트렌드마이크로, NTT에서는 P2P프로그램을 통한 정보유출 주의를 발표하였다. 이러한 P2P프로그램을 통한 정보유출로 인한 사회적 이슈화 및 관심에 따라 2007년 「파일교환 소프트웨어에 의한 정보유출에 관한 조사[22]」에서 P2P프로그램 이용자 중 90% 정도가 보안대책을 실시하였다. 대책의 주요 내용은 백신을 사용하거나 의심되는 확장자는 다운로드할 경우 주의하며, P2P프로그램 전용컴퓨터를 사용하는 것이었다. 2007년 5월 총무성 내각관방정보시큐리티센타의 「일본의 정보시큐리티 정책 방향성 발표」에서 과거 사용자가 P2P프로그램 사용을 중지 한 이유에 대한 설문 조사결과 「보안, 바이러스가 걱정」이라는 항목이 2005년부터 2007년까지 약 30%이상을 차지하며 3년간 1위를 차지하였다. 일본 정부기관 및 자위대의 정보유출 대책을 이해하기 위해 일본 언론사의 정보유출 관련 기사를 조사한 결과 표 5와 같다. 일본 정부는 다양한 업무지침 발표와 정보유출 방지를 위한 SW를 개발하고 보급하였다. 자위대는 일본 정부기관 보다 더 강력히 정보유출 대책을 수립하여, 업무용도의 개인 PC 사용을 금지하기 위해 PC를 보급하고, 인력관리 및 조직을 개선하였다. 자위대의 정보유출 대책은 표 6과 같다.

표 5. 일본 정부기관의 정보유출 방지 주요 대책
Table 5. Important measures taken by the Japanese government agency to prevent information effluence.

분류	일 시	기 관	대 책
업무 지침	´06.2.22	법무성	자택 PC의 업무파일 삭제 지시
SW 도입	´06.4.20	내각 관방	Winny 대책 소프트웨어, 산관학 팀에서 개발 결정
업무 지침	´06.5.4	총무성	Winny를 통한 정보유출 방지를 위해 직장 외에서 Winny 접속 규제 지침 마련
SW 도입	´06.5.26	문부 과학성	정보유출방지를 위해 문부과학성에서 안전성을 높이는 소프트웨어 개발 착수
SW 도입	´06.9.1	총무성	파일 교환 소프트웨어의 정보유출을 방지하기 위해 신기술 개발 착수
SW 도입	´07.3.9	경찰청	정보유출 대책을 위해 모든 PC에 암호 소프트웨어 설치

SW 도입	´07.4.27	내각 관방	정부의 보안 계획에 의거 정보누설 방지 신시스템 개발
SW 도입	´07.6.8	NICT[23]	보안사고 대책 기술 「NICTER」 공개
업무 지침	´07.6.22	경찰청	경시청의 정보유출로 인해 개인 PC 긴급 점검 지시
업무 지침	´07.8.3	총무성	개인정보 유출 사건으로 일본 우정공사에서 재발 방지책 총무성에 보고
업무 지침	´07.12.7	IPA	IPA 경고,「Winny를 사용하는 한 정보유출은 없어지지 않는다」

표 6. 일본 자위대의 정보유출 방지 주요 대책
Table 6. Important measures taken by the Japanese Self-Defense Forces to prevent information effluence.

분류	일 시	기 관	대 책
업무 지침	´06.3.2	방위청	개인 사용 목적의 PC로 비밀정보 취급 전면 금지
HW 교체	´06.3.9	방위청	정보유출방지를 위해 관비로 PC 7만대 지급 계획 발표
SW 도입	´06.3.30	방위청	자료 암호화, 외부 정보유출 대책 실시
HW 교체	06.4.20	방위청	정보누설방지대책으로 Winny가 동작하지 않는 PC 56,000대 지급
SW 도입	´07.1.26	방위성	Winny 정보유출 방지 소프트웨어´07. 4월 도입 발표 ※´07.1.9 방위성 승격
인력 관리	´07.5.18	방위성 방위상	방위상이「부하 전원에게 개별 면담」지시
인력 관리	´07.6.29	해상 자위대	외국인 배우자가 있는 대원은 정보부서에서 타부서로 발령
업무 지침	´07.8.3	방위성	내부 고발 제도 개정, 정보유출 대책 강화
조직 개선	´07.8.3	방위성	정보유출방지 강화를 위해 정보보전대 본부 설치
조직 개선	´08.1.18	방위성	정보유출대책회의 개최
조직 개선	´08.5.2	방위성	사고방지기술본부대책회 설치

나. 한국의 P2P 정보유출 대책

한국은 표 7과 같이 2004년 10월 한국정보보호진흥원 개인정보보호팀의 「P2P를 통한 개인정보 유출 사례 검토 및 대책[24]」으로 법·제도적 대응 방안, 교육, 홍보방안이 실행되었다. 2005년 9월에는 정보통신부 개인정보보호전담팀이「P2P 개인정보보호 수칙[25]」을 마련했고, 2006년 11월부터는 개인정보가 유출된 P2P 사이트에 117개 금칙어 처리 및 공유자에게 삭제를 요청하였다. 일본의 정보유출대책을 살펴본 결과 한국보다 다양한 대책들이 수립된 것을 확인하였다. 일본의 P2P프로그램을 통한 정보유출 대책이 한국보다 발전한 것은 P2P프로그램으로 인한 정보유출 문제가 심각하게 발생되고 있기 때문일 것이다. 2007년 정보통신부는 프루나, 동키호테 등 개인정보가 유출된 9개 사이트에 대해 금칙어 처리를 요청했지만 이력서 검색에 무력한 것을 확인하였다. 또한 일본의 개인컴퓨터 사용금지를 위한 컴퓨터 보급, 정보유출 방지를 위한 전문 SW의 개발, 파일 암호화, 업무 자료의 반출 금지, 인력관리, 조직개선 등의 노력에 비한다면 한국의 P2P프로그램을 통한 정보유출 대책은 미흡한 수준이라 판단된다.

표 7. 한국의 정보유출 방지 주요 대책
Table 7. Important measures taken by the Korea to prevent information effluence.

분류	일 시	기 관	대 책
홍보	´04.10	정보보호 진흥원	P2P를 통한 개인정보 유출 사례 검토 및 대책 홍보
수칙 발표	´05.9	정보 통신부	P2P 서비스 제공자가 취해야 할 보호조치 및 이용자가 지켜야할 개인정보보호 수칙 발표
처리 요청	´06.11	정보 통신부	9개 P2P 서비스 제공자에게 117개 금칙어 처리 요청
처리 요청	´07.3	정보 통신부	개인정보 공유자에게 이용을 제한하는 “3진 아웃제” 시행을 사업자에게 요청

다. 정보유출 대책방안 제시

일본의 정보유출 대책은 많은 비용과 지침으로 해결방안을 제시하였고 본 연구에서 정보유출 수집결과를 통해 그 실효성이 확인되었다. 일본에서 P2P프로그램을 통한 정보유출의 가장 큰 원인은 P2P프로그램 관리주체의 부재이며, 소스공개에 의한 바이러스 생성 및 확산이었다. Winny와 Share가 P2P프로그램 사용 순위와 상이하게 정보유출이 심각한 이유도 두 P2P프로그램을 대상으로 만들어진 바이러스 때문이었다. 한국의 경우 많이 사용되는 P2P프로그램이 상업적 목적으로 만들어 졌고 관리주체가 있었기에 현재까지 특정 P2P프로그램을 대상

으로 만들어진 바이러스 및 정보유출 문제는 심각하게 발생되지 않고 있다. 그러나 악의적 사용자에 의해 공유되는 문서나 프로그램에 악의적 코드를 삽입한다면 개인 및 기업의 소중한 정보가 유출될 소지는 한국에서도 다분하다. 따라서 한국의 P2P프로그램에 가장 시급하게 적용해야 할 대책은 공유되는 정보의 바이러스 내포 유무를 탐지할 수 있도록 P2P프로그램 관리주체에 의한 백신 적용을 의무화하고, 취약점을 관리주체가 사전에 탐지하고 수정하며, 기밀문서 및 업무자료를 처리하는 컴퓨터에서는 P2P프로그램 설치를금지하고, 네트워크를 통한 P2P프로그램 사용무력화를 수행하는 것이 최우선의 방법 일 것이다.

Ⅲ. 결 론

P2P프로그램을 통한 정보유출은 한국 및 일본에서 모두 발생되고 있음을 확인했으며, 특히 일본의 경우 정보유출 피해가 심각함을 언론정보와 수집결과를 통해 확인하였다. P2P프로그램을 통해 발생할 수 있는 정보유출은 사용자의 P2P프로그램 작동 미숙도 원인이 되고 있지만, 원인의 대부분은 특정 P2P프로그램에 정보유출을 유발시키는 악성 바이러스 및 웜에 의해 발생되었음을 일본의 사례를 통해 확인하였다. 다수 인터넷 사용자들이 자신의 컴퓨터 및 P2P프로그램이 안전할 것이라는 믿음을 갖고 있지만, P2P프로그램을 통해 공유되고 있는 다양한 프로그램과 파일들은 악의적인 프로그래머가 개발한 악성코드에 의해 감염되어 있는 경우가 많은 것이 현실이다. 신종 바이러스에 의해 감염된 문서나 파일들은 백신에 의해 발견 및 치료되지 않는 경우가 많기 때문에 정보유출 문제는 지속적으로 발생될 것이다. 한국의 경우 개인정보 유출에 관점을 두고 정보유출 대책이 이루어지고 있으며, P2P프로그램 서비스회사와 개인이 정보유출 대책을 시행하게 하고 있다. 이에 반해 일본은 P2P프로그램의 바이러스 대응을 위한 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 있다. 정보유출 대책의 실효성은 본 연구를 통해 효과를 거두고 있음을 확인할 수 있었다. 한국의 경우 비밀문서나 기업의 중요한 내부문서가 유출되는 사례가 일본보다 적게 발생되고 있지만 일본의 정보유출 사례와 대책, 본 연구에서 제시한 정보유출 방지 대책을 반영한다면 P2P프로그램으로 인한 피해를 사전에 예방할 수 있을 것이다. 향후 본 연구결과를 통해 P2P프로그램으로 인한 정보유출 피해가 감소되길 기대한다.

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] 財團法人インターネシト協會 監修, インターネット白書2007, Impress R&D, pp.31, 2007.7

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

[4] 金子勇(Kaneko Isamu), Winnyの技術, ASCII, pp.39-81, 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, 日本ｷ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), pp.4-13, 2007.12

[8] 푸르나, http://www.pruna.com

[9] 파일구리, http://www.fileguri.com

[10] 소리바다, http://www.soribada.com

[11] 피디팝, http://www.pdpop.co.kr

[12] 몽키3, http://www.monkey3.co.kr

[13] 엔피, http://www.enppy.com

[14] 당나귀, http://www.edonkeyp2p.com

[15] 랭키닷컴, http://www.rankey.com, P2P프로그램 점유율, 2008.7.8

[16] 전자신문, 엠브레인, 국내 파일공유(P2P) 이용 현황 및 전망 조사, pp.1-4, 2008.3.25

[17] ACCS(Association of Copyright for Computer Software-社団法人コンピュータソフトウェア著作權協會), http://www2.accsjp.or.jp

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

[19] 안덕기, P2P 개인정보 관련, 정보통신부 정보보호기획단 정보윤리팀, pp.1-2, 2007. 11. 20

[20] 內閣官房情報セキュリティセンた(NISC), 我が國

の情報セキュリティ政策の方向性, 2007.5
[21] http://dailynews.yahoo.co.jp/fc/domestic/winny/
[22] 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, 株式會社日立製作所, pp9, 2007.12.21
[23] NICT(情報通信研究機構- National Institute of Information and Communications Technology), http://www.nict.go.jp
[24] 안준모, P2P를 통한 개인정보 유출 사례 검토 및 대책, 한국정보보호진흥원 개인정보보호팀, pp.5-7, 2004. 10.5
[25] 조정현, P2P 개인정보보호 수칙 마련, 정보통신부 보도자료, pp3, 2005.9.20

저자 소개

김 완 수(정회원)

- 1999년 세명대학교 전사정보학과 학사.
- 2001년 세명대학교 전산정보학과 석사.
- 2009년 세명대학교 전산정보학과 박사과정수료.

<주관심분야 : 보안, 통신, 분산처리>

김 식(정회원)

- 1979년 경북대학교 컴퓨터공학과 학사.
- 1991년 Texas A&M Univ. 컴퓨터공학 석사.
- 2004년 오카야마 현립대학, 정보통신학과 박사.
- 1993년~현재 세명대학교 정보통신학과 교수.

<주관심분야 : 분산처리, 임베디드공학, 통신>