8

산업기밀 정보유출방지와 개인정보보호의 현황과 전망

닉스테크 ▌안 홍 기

급격한 정보사회로의 변화에 따라 기업에서의 정보보안은 필수항목으로 떠오르고 있다. 정보보안 중에서 기업이 보유하고 있는 기밀정보의 유출방지는 기업의 흥망을 좌우 할 정도로 주요관심사가 되었다. 이에 따라 필자는 2007년도 정보보호 시장에서의 주요 이슈사항을 분석해 보고 그 중에서도 기업의 주요 관심사인 산업기밀 정보유출 현황과 솔루션 동향에 대해서 자세히 살펴보겠다. 더불어 작금의 핫 이슈로 떠오르고 있는 개인정보유출 현황과 솔루션 동향에 대해서도 살펴보겠다.

1. 2007년 정보보호 시장동향

한국정보보호진흥원(KISA)의 '2006 국내 정보보호 산업 통계조사'에 따르면 2006년 국내 정보보호 시장규모는 7천348억원이며 2009년 1조원을 돌파할 것으로 전망하고 있다(표 1, 2 참조).

IDC 자료에 따르면 전세계 보안시장규모는 2005년 328억달러에서 2010년 670억달러를 예상, 연평균 16%의 고속성장을 달성할 것으로 전망했다.

국가정보원과 정보통신부가 정한 2006년 정보보호 10대 이슈를 보면 개인정보보호 관심 증대, 금전적 이익취득을 위한 보안위협의 증가, 기업 핵심기술 유출방지 관심 고조, 정보보호 관련 법제 강화, 보안 취약점을 이용한 제로데이(Zero-day) 공격 증가, 사이버 침해행위의 지능화 및 고도화, 디지털콘텐츠와 VoIP 정보보호 부상, 국제상호인정협정(CCRA) 가입, 유비쿼터스 보안 필요성 대두, 정보보호분야 국제위상 제고이다.

2007년도의 보안시장 특징을 살펴보면 과거 해커의 자기과시성 공격, 항의성 공격에서 금전을 노리는 공격으로 성향이 변화하고 있다는 것이다. 이러한 변화는 개인사용자들의 직접적 피해를 유발 할 뿐만 아니

표 1 시스템 및 네트워크 정보보호제품 분야 매출 전망, 2006. 11, KISA

[단위 : 백만원]

구분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
침입차단 (방화벽시스템)	89,108	94,554	104,896	115,075	125,107	135,006	144,787	8.43
침입방지시스템(IPS)	62,406	71,469	80,532	59,595	98,658	107,721	116,784	11.01
보안관리	87,957	101,038	112,519	122,767	132,049	140,562	148,455	9.12
가상사설망(VPN)	53,776	54,558	64,340	69,622	74,904	80,186	85,468	8.03
인증제품	56,736	42,691	56,202	68,015	78,981	89,321	99,123	9.75
Anti-Virus	57,935	68,671	79,681	90,083	100,185	110,386	121,232	13.10
Anti-Spam	10,756	15,438	18,715	21,010	22,616	23,740	24,527	14.73
보안운영체제(Secure OS)	28,652	29,144	29,636	30,128	30,620	31,112	31,604	1.65
PC보안	29,500	32,662	35,824	38,986	42,148	45,310	48,472	8.63
컨텐츠 보안	27,329	32,554	37,779	42,202	46,624	51,047	55,469	12.52
공개키기반구조(PKI)	16,085	17,735	19,385	21,035	22,685	24,335	25,985	8.32
접근관리	11,221	9,087	11,378	13,510	15,501	17,363	19,110	9.28
무선/모바일 보안	2,516	3,646	4,776	5,906	7,036	8,166	9,296	24.34
바이오인식제품	43,195	46,725	51,697	55,864	59,629	63,192	66,655	7.50
기타제품	6,251	5,210	6,329	7,142	7,739	8,186	8,528	5.31
합 계	583,423	625,182	713,689	790,940	864,482	935,633	1,005,495	9.45

표 2 정보보호산업의 매출 전망, 2006. 11, KISA

[단위 : 백만원]

구분	2005년	2006년	2007년	2008년	2009년	2010년	2011년	CAGR(%)
시스템 및 네트워크 정보보호 제품	583,423	625,182	713,689	790,940	864,482	935,633	1,005,495	9.50
정보보호 서비스	97,282	109,610	123,053	136,495	149,938	163,380	176,823	10.47
합 계	680,705	734,792	836,742	927,435	1,014,420	1,099,013	1,182,318	9.64

라 기업의 기밀정보취득을 노리는 타깃 공격으로 인해 기업의 지적 재산이 위협 받을 수 있는 변화로 지적된다. 이에 따른 2007년 정보보호시장의 주요 솔루션으로 NAC(Network Access Control)와 개인정보보호가 화두가 될 것으로 전망되고 업체 동향으로는 대형 기업의 보안업체 인수와 마이크로소프트의 보안시장 진출을 들 수 있겠다.

2. 산업기밀 정보유출 현황

지금까지의 보안기술이 바이러스나 해킹 등과 같은 외부로부터의 위협에 대응할 수 있는 네트워크 보안이 대부분이었으나, 최근의 보안기술은 기업내부의 기밀정보 유출에 대응할 수 있는 보안으로 영역을 확장하고 있다. 기업의 내부정보 등이 이메일, 인스턴트 메시징 서비스, P2P 등을 통하여 의도적으로 또는 부주의로 인하여 무분별하게 유통됨으로써 심각한 정보유출이 우려되고 있고, 여러 손실 유형 가운데 내부정보 유출에 따른 경제적 손실이 가장 많은 부분을 차지하고 있으며, 최근 중국, 일본, 미국 등 경쟁국가 및 경쟁기업에 의한 불법기술유출이 증가하는 추세이다. 특히, 스파이웨어가 경제적 목적으로 개인정보와 기업기밀 탈취 수단으로 악용되는 사례가 증가하고 있으며, 2003년 이후 국내에서 제조업체들의 핵심기술이 중국 등 해외로 유출되거나 공공기관이나 통신, 온라인 쇼핑몰, 의료기관 등의 개인정보 유출, 이동통신사의 고객 정보가 유출되는 사고들이 잇따라 발생하고 있다. 특히 기업에게 있어서 기밀정보, 핵심기술, 개인정보 등 내부 정보나 고객정보 등의 유출피해는 경제적 손실, 고객 손해배상 뿐만 아니라 대외 인지도 및 주가 하락, 기업 브랜드 이미지 추락 등의 기업 활동에 심각한 피해를 줄 뿐만 아니라 기업의 생존에도 위협을 줄 수 있다. 2003년부터 2006년 12월까지 최근 4년간 총 92건이 적발, 업계 추산 약 96조원의 손실이 발생하였다(표 3, 4 참조).

기업규모별로 볼 때 대기업은 보안전담부서를 두고 기밀정보유출방지를 위한 각종 솔루션 도입과 보안관리규정을 두어 대비를 하고 있으나 자금과 인력부족으로 인한 보안투자에 소홀 할 수 밖에 없는 중소, 벤처기업은 내부로부터의 정보유출이 심각한 상태이다. 또한 핵심기술의 유출경로로 내부직원에 의한 유출이 91%에 달할 정도로 가장 큰 비중을 차지하고 있다.

표 3 연도별 기술유출 적발추이, 2007, 국가정보원

년도	건수	예상피해액(조원)
'03	6	13.9
'04	26	32.9
'05	29	35.5
'06	31	13.7
합 계	92	96

표 4 기업의 주요 정보유출 사고

년 도	사건 사고
07. 05	게임 L의 영업기밀 일본 유출
07. 05	무선통신 원천기술 미국유출 기도
07. 05	K자동차 핵심기술 중국유출 중 검거
06. 03	S사 휴대폰기술 카자흐스탄 유출 기도
06. 01	TFT-LCD 컬러필터기술 중국유출 기도
05. 07	고성능 세톱박스기술 해외 유출 기도
05. 07	반도체 제조공정 기술 해외 유출 기도
04. 11	TFT-LCD 제조기술 해외 유출 기도
04. 06	바이오 환경기술 해외 유출 기도
98. 06	S사 64M D 메모리 대만 유출

3. 산업기밀 정보유출방지 솔루션 동향

이러한 시장 요구에 따라 보안 업체들은 내부정보유출방지에 대한 보안 체계 구축 방법론과 제품들을 출시하고 있다. 이들 보안체계와 제품은 네트워크 단과 호스트 단에서 기밀 콘텐츠의 내용을 분석하여 유기적으로 대응함으로써 감지 장치의 고지능화를 실현하였고, 이를 통해 기존의 정보보호 제품들보다 한 단계 진화된 방식을 선보이고 있다.

3.1 네트워크 기반 솔루션

이메일, 웹, IM, P2P 등의 다양한 채널을 통하여 전달되는 outbound 트래픽을 모니터링 하여 허가받지 않은 내부정보 전달을 확인하는 기능을 제공하는 게이트웨이형 솔루션이다. 대부분의 경우 방화벽 뒷단에 네트워크 스니퍼가 설치되어 outbound 네트워크

트래픽을 모니터링 하는 구조이며, 스니퍼에서 TCP 세션을 재조립하고 분석하여 사전에 정의된 룰이나 정책에 기반을 두어 내부정보를 탐지한다. 그 외에 하나의 전용 채널(대부분 이메일)을 검사하고 차단하기 위하여 프록시를 사용하기도 한다.

또한 웹방화벽 제품이 국내에 상륙한 지도 만 3년이 흘렀다. 아직은 초기 시장으로, 올해까지는 제품이 알려지고 있는 인식 단계나 도입기라는 시각이 지배적이다. 이에 내년부터는 웹 방화벽 시장이 성장가도를 달릴 것이란 게 업계 관계자들의 예측이자 '희망사항'이다. 최근 잇따른 웹 해킹 사건으로 웹 방화벽에 대한 관심이 부쩍 높아진게 그 근거다. 하지만 제품 테스트에서 도입 결정까지 오랜 시간이 걸릴 뿐 아니라, 실제 솔루션 운영이 녹록치 않아 담당자들이 제품을 선뜻 구매하지 못하고 있는 것 또한 엄연한 현실이다. 성능과 기능 등 제품 개선도 해결할 숙제다.

3.2 데스크탑 기반 솔루션

데스크탑 사용자의 정책위배 여부를 제어하여 정보유출을 방지하는 솔루션이며, 사용자 정책 위배 여부는 네트워크 관련 정책위배 여부(이메일에 파일 첨부, IM 메시지 등)와 데스크탑 정책위배 여부(프린팅, USB로 파일복사, CD 굽기) 등을 포함한다. 데스크탑 기반 서비스 전문업체로서 국내는 닉스테크, 잉카인터넷, 세이프존 등이 있고, 해외는 Verdays, Orchestria, Oakley Networks, Onigma 등이 있다. USB, PCMCIA, printer, DC/DVD, Firewire, Infra Red 등 데스크탑에서의 인터페이스를 제어하는 종단 보안솔루션을 제공하는 Safend, Control Guard, Lambda DSS, SecureWave, Sen-force, Smartline, Reflex Magnetics 등의 업체도 포함되나, 속성상 기밀유출방지 솔루션이라고 할 수 없다. 이는 inbound, outbound 위협에 대처하기 위하여 무선(무선 단말을 통한 정보유출)과 주변장치(USB를 통한 바이러스 감염)에 대한 사용정책을 정립하기 위한 것이라고 보는 것이 타당하다.

4. 개인정보 유출 현황

정부가 2003년부터 5년간에 걸쳐서 추진하고 있는 전자정부 31대 과제가 금년에 마무리 되면서 일반 국민들의 인터넷을 통한 대 정부 업무처리(전자민원G4C, 조달G2B 등)가 증가추세에 있고, 민간에서의 인터넷 생활화(인터넷 뱅킹, 인터넷 증권거래, 쇼핑몰 등)에 따른 상거래도 폭발적인 증가 추세에 있다.

이러한 인터넷을 통한 업무처리와 상거래에 있어서 하드웨어의 발전으로 인하여 이동형 저장매체의 보급이 대중화 및 대용량, 소형화로 변해감에 따라 중요한 기업의 정보나 개인의 정보가 외부로 유출될 가능성이 점차 높아지고 있다. 실제로 일반 개인들을 소비자로 하는 기업(통신사업자, 은행, 쇼핑몰 등)이나 일반 개인들을 회원 형식으로 관리하는 기업(인터넷 포털사이트, 인터넷 게임 업체 등)에서의 개인정보 유출 사고가 매년 증가 추세에 있다.

개인정보는 이름, 주민등록번호 등 '신분정보'에서 건강상태, 병력 등을 알 수 있는 '심신정보', 경제상황, 개인의 사상이나 신조, 정치성향 등을 알 수 있는 '내면의 비밀정보'까지 범위가 확대되고 있는 추세다. 지문, 홍채, DNA 등 '생체정보'와 휴대전화 위치정보, 네트워크 정보까지 새로운 유형의 개인정보까지 속속 나타나고 있다.

한국정보보호진흥원(KISA)의 '2006 개인정보분쟁조정사례집'에 따르면 2005년 신고·접수된 개인정보 침해사례가 18,206건에서 2006년에 23,333건으로 28% 증가했다. 2006년의 침해사례 유형별로는 주민등록번호 도용이 10,835건으로 전체의 46%를 차지했고, 신용정보 침해, 동의 없는 정보수집의 순이었다.

최근에 발생한 주요 개인정보 유출 사고사례를 보면 점차 공공, 민간의 구분 없이 대형화 하고, 개인정보가 그 가치에 따라 거래되고 있다는 데 심각성이 있다.

- 리니지2 개인정보 유출. "위자료 10만원씩 줘라" (2006. 1. 26 / 이데일리)
  서울중앙지법 형사항소1부(한호형 부장판사)는 "개인정보를 담은 파일인 '로그파일'을 암호화 하지 않아 개인정보가 노출됐다"며 온라인 게임 '리니지'의 운영업체인 엔씨소프트에 1인당 10만원씩 지급하라는 판결을 함.
- LG전자 공채 지원자 100여명. 16일쯤 집단소송…. 1인당 2000만원 배상 요구(2006. 10. 3/국민일보)
  소송대리인인 김연호 변호사는 "LG전자는 채용사이트가 뚫려 응시자들의 개인정보가 불특정 다수에 의해 무작위로 이용될 수 있는 위험에 처하게 한 데 대해 책임져야 한다".
- 90만명 주민번호 인터넷 떠돌아… 정통부, 개인정보 삭제 요청(2006. 8. 2 / 경향신문)
  90만명이 넘는 한국인의 주민등록번호가 인터넷상에 나돌고 있는 것으로 확인됐다. 정보통신부는 1일 정보검색사이트 '구글'의 데이터베이스에서 지난달 24일부터 5일간 주민번호를 검색한 결과 6,337개 웹사이트에의 49,583개 페이지에서 90만

3665명의 주민번호가 노출된 것으로 나타났다고 밝혔다(중략).

- 771만명 개인정보 시중에 불법유출(2006. 4. 4/ 매일경제)
  국내 인터넷 가입자 1240만명 중 62.2%에 달하는 771만명(KT, 하나로통신, 두루넷, 온세통신 등 국내 4대 인터넷 서비스 업체의 가입자 정보) 개인정보를 시중에 불법 유출시킴.

이에 따라 정보통신부는 2005년 3월 '개인정보의 기술적 · 관리적 보호조치 기준'을 시행한 이래 2005년 9월 '초고속인터넷사업자 개인정보보호 조치 시행' 및 2006년 4월 '공공기관 홈페이지를 포함한 10만개 웹사이트에 대한 개인정보 노출실태 집중 점검'하여 수사의뢰 등의 조치를 취하였고 최근 2007년 4월부터 6월까지 '공공기관 홈페이지 개인정보 노출 정밀 재점검'을 실시하였다.

인터넷 상에서 명의도용 등 주민번호의 불법 수집 · 사용으로 인하여 발생하는 문제점을 해결하기 위하여 2005년에 주민번호 대체수단인 아이핀(i-pin)을 마련한 바 있다. 또한 2006년 12월 개인정보를 취급하는 웹사이트에서 개인정보를 암호화하여 안전하게 전송하는 보안서버를 의무적으로 구축하도록 하는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 의한 '개인정보의 기술적 · 관리적 보호조치 기준'을 개정하기도 했다. 국회에는 3개의 개인정보보호법[안]이 상정되어 심의 중에 있다.

5. 개인정보보호 솔루션 동향

이렇듯 기업의 개인정보를 보호하기 위해서는 규정 제정, 조직과 개인정보 관리자 선정 등의 내부 제도적인 측면과 개인정보 관리 시설로의 접근을 통제할 수 있는 물리적 조치 및 내부직원 교육, 임직원 보호 관리 등의 기반 체계가 수립되어야 하고, 기업 내부의 개인정보 유출을 예방하고 대응할 수 있는 소프트웨어적인 시스템 구축이 선행되어야 한다.

이에 발맞추어 국가에서는 개인 정보보호 법제 제정, PETS (privacy enhanced technology) 개발 지원, 한국형 P3P 개발 지원 등의 사업을 추진하고 있으며, 사회적으로도 개인정보 침해예방 및 대응에 대한 관심이 고조되고 있고, 기술적인 면에서도 개인정보 보호기술 개발 및 연구가 활발히 진행 되고 있다.

기존 국내의 개인정보 유출방지 시스템의 문제점은 크게 3가지로 나눌 수 있다. 보호 대상 선정의 문제, 검사 지점 범위의 문제, 검사 수준의 문제이다.

첫 번째로 보호 대상 선정의 문제는 기존의 개인정보보호 시스템은 기업망 중앙의 보안 서버에 기밀 데이터를 취합해서 저장해두고 취합된 데이터(구조화된 데이터)에 대해서만 접근제어, 감사작업을 수행하였다. 하지만 기업이나 기관에서 개인정보의 80% 이상이 각각의 개인용 호스트에 구조화되지 않은(비구조화) 데이터 형태로 저장되어 있다. 이들 데이터에 대한 유출방지 방안의 개발이 요구되는 시점이다.

두 번째로 검사 지점 범위의 문제는 기존의 방식은 크게 보안 게이트웨이를 통한 네트워크 단에서의 차단 방식과 개인용 호스트의 I/O를 감시하는 데스크탑 지점에서의 차단 방식으로 나뉠 수 있다. 지금까지 국내 업체에서는 두 방식을 모두 지원하면서 하나의 프레임워크로 지원하는 경우가 없었는데 완벽한 기밀 차단을 위해서는 모든 채널에 대한 감시가 요구되므

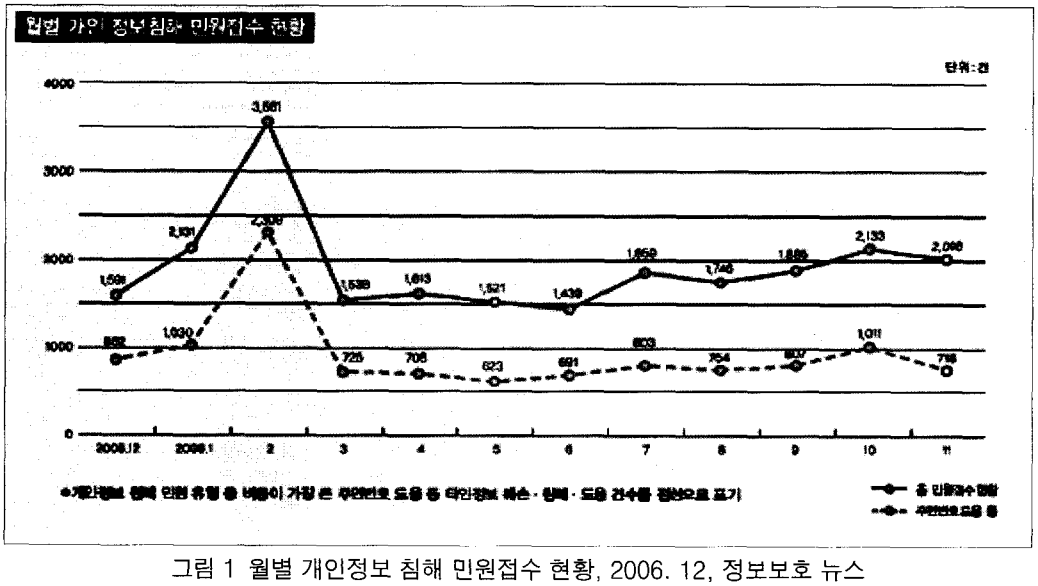

그림 1 월별 개인정보 침해 민원접수 현황, 2006. 12, 정보보호 뉴스

로 두 가지 방안 모두를 유기적으로 결합하는 프레임 워크의 개발이 필요하다.

세 번째로 검사 수준의 문제는 내부정보 유출감시 모듈의 지능이 얼마나 높은가의 문제이다. 기존의 방식은 등록된 보호 정보에 대해서 현재 유출되는 문서가 일치하는지 여부만을 검사하는 단순 비교 방식이었다면 미래의 감시모듈은 등록된 보호 정보가 일부 변형되더라도 탐지가 가능해야 하고 등록되지 않은 비구조화 문서에 대해서도 보호정보 여부 검사가 가능해야 한다.

현재 개인정보를 보호하기 위한 여러 가지 법제도적 대책과 기술이 연구 개발되고 있는데, 전문 연구단체에서 정의한 개인정보 침해기술과 개인정보 보호기술은 아래와 같다.

5.1 개인정보 침해 기술(Privacy Invading Tech-nology: PIT)

침해 기술	방 법
TCP/IP 주소	TCP/IP 주소의분배 및 관리체계 특성 때문에 인터넷 이용시 TCP/IP 주소를 추적하여 이용자 신원을 확인하는 것은 용이.
도메인 네임	e-mail의 출처를 확인하는 것은 매우 간단하며, 누구나 ISP 정보와 e-mail 이용자의 ID를 알 수 있음. ISP는 이용자의 ID를 이용하여 이용자의 계정을 확인.
Processor Serial Number(PSN)	Intel사는 자사가 개발하는 Pentium III 칩에 고유의 프로세서 일련번호(Serial Number)를 부여하여, 인터넷에 접속하는 특정 컴퓨터의 이용자의 신원정보와 연결시켜 전자 상거래에 있어서 인증 목적으로 이용.
IPv6	IPv6의 계획은 인터넷상의 모든 장치에 고정된 주소를 할당하는 것으로, IPv6의 새로운 주소는 하드웨어 속에 내장될 것이고, 추적 가능한 정보를 포함하게 됨. 이것은 마치 영구적인 쿠키를 심는 것과 동일한 개념.
쿠키(Cookie)	쿠키 파일을 이용하여 인터넷 이용자의 신원을 쉽게 파악할 수 있음. 두 가지 방식으로 첫째, 쿠키는 로그인 정보(예컨대 이름, 주소, 비밀번호 등)를 불러내는 데에 사용될 수 있다. 둘째, 쿠키에 담긴 정보와 마케팅 데이터베이스에 있는 이용자의 이름, 주소, 이전의 소비정보 등을 상호 비교함으로써 이용자의 신원 확인 가능.
웹 버그(Web Bug)	웹 버그는 온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출해 가거나 심지어 이용자의 시스템을 파괴할 수도 있는 기술임. 웹 버그는 Web Page에 심어 놓은 매우 작은 그래픽이미지 파일로, 통상 해당 Web Page의 바탕화면과 같은 색을 지니기 때문에 육안으로는 거의 보이지 않음.
스파이웨어(Spyware)	무료 또는 유료로 배포되는 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭하는 것으로, 해당 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑 할 때 이용자의 개인정보나 온라인 활동 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전송하는 것이 주된 기능.
고성능스파이웨어 (Sophisticated spyware) 기술	스파이웨어 기법이 한 단계 진보된 기법으로, 스파이웨어를 탐지하기 위해 사용되는 백신이나 안티 스파이웨어 솔루션 등을 우회하기 위해, 스파이웨어를 통해 수집된 정보를 작은 크기로 나누어 컴퓨터의 파일 시스템상에 보이지 않는 틈새공간(Slack Space)에 임시 저장한 다음, 특정 시간대에 내외부의 특정인에게 전송하는 방법을 이용함. 이러한 기법은 정부의 수사기관에서 범죄자의 감시 및 경쟁사에 대한 정보 수집, 국가간첩정보 수집에 이용된 사례가 있음.
WLAN 환경	WLAN 사용자가 액세스 포인트에 접속할 때, 해커가 가상의 액세스포인트를 이용하여 사용자의 중요한 개인정보를 모니터링 하게 됨.
웹메일의 첨부화일 유출	웹메일 첨부파일 유출기법은 기존 e-mail이나 웹메일을 모니터링하여 데이터를 유출하는 방식에서 한 단계 진화하여, 웹메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀 정보를 유출하는 데 사용됨.
Staganography	이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부할 수 있는 스테가노그래픽 기법이 확산될 전망이다. 이 기법은 오시마빈라덴이 알카에다 조직원과의 연락을 위해 사용된 것으로 보고되면서 널리 알려짐.
접속 세탁 (Connection laundering)	접속 세탁 기법은 해커들이나 해커 그룹간 공간 창조를 통해, 해커 역추적 경로 파악을 어렵게 만드는 것으로, 해커가 여러 국가를 경유하여 해킹 할 경우, 중간 단계에서 해커 그룹이 운용하는 가명경로(anonymizer)를 거쳐 해커에 대한 역추적이 불가능하게 하는 방법임.
위치측정 정보 침해	GPS 또는 휴대전화의 위치 측정 내용을 인터넷을 통해 확인할 수 있게 되어, 개인의 위치정보가 유출되어 개인의 신변에 위협이 될 수 있음.

5.2 개인정보 보호기술 (Privacy Enhancing Tech-nology: PET)

보호 기술	방 법
P3P (Platform for Privacy Preference)	P3P는 W3C(World Wide Web Consortium)에서 개발한 개인정보보호 표준 기술 플랫폼으로서 웹 사이트에서 이루어지는 데이터 처리에 관한 표준을 제시하고 있음. P3P의 목표는 웹 사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨주는 것이며, 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어졌음.
프라이버시 정책 생성 (Privacy Policy Statement Generator)	OECD가 1980년에 발표한 '프라이버시 보호 및 개인정보의 국가간 유통에 관한 지침에 따라 개발되었고, 프라이버시 정책문구를 자동적으로 생성하는 기능을 가지고 있음. 특히, 정보보호 생성 소프트웨어가 요구하는 절차에 따라 실제 운영중인 개인정보 보호방침을 입력하면 해당기업이나 조직의 개인정보 보호방침 문구를 HTML 문서로 자동 작성하여 출력하는 기능을 갖고 있음.
쿠키 관리 (통제)	이용자로 하여금 언제 쿠키가 자신의 컴퓨터에 저장되는지를 결정하게 함으로써 쿠키의 수용 여부를 결정하고 관리하도록 하며, 개별적인 쿠키에 저장된 정보가 무엇인지를 판단할 수 있는 방법으로, 개인에게 자신의 컴퓨터에 저장된 쿠키에 대해 통제권을 주는 방법임.
암호화 소프트웨어 (Encryption Software)	암호화 소프트웨어는 암호화를 통해 자신의 전자 메일 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공함. 암호화가 이루어지면 오직 그 당사자만 암호화된 정보에 대한 디지털 키를 가지고 그 정보를 열람하며, 디지털 키는 브라우저, 생체인증, 스마트카드 등과 결합하여 생성됨.
익명화 (anonymizers)	익명화는 클라이언트와 웹 사이트간에 중재자 역할을 수행함으로써 이용자가 익명으로 웹을 서핑하도록 하는 서비스를 제공함. 일반적으로 익명화 서비스는 웹 사이트가 방문객의 IP 주소를 식별하거나 쿠키를 개인의 컴퓨터에 저장하는 것을 막아줌으로, 소비자가 웹을 브라우징 하거나 보내는 이가 누구인지 알 수 없도록 익명화된 메일을 보낼 때 유용함. 그러나 이러한 기능은 반대로 개인화된 서비스나 온라인 계정관리, 과거의 구매기록 보관 또는 열람 등에 대한 특정한 기능을 사용할 수 없게 함.

참고문헌

[1] 국가정보원, "2007 국가정보보호백서"

[2] 한국정보보호진흥원, "2006 국내 정보보호산업 통계조사"

[3] 한국소프트웨어산업협회, "제3회 공공기관 개인정보보호 컨퍼런스"

[4] 한국정보보호진흥원, "SIS2007(제12회 정보보호 심포지움)"

안 흥 기

1989~1998 (주)삼테크 네트워크사업부 기술팀장
1999~2001 (주)농심데이타시스템 정보보호팀 사업팀장
2001~현재 닉스테크(주) 기술연구소 소장
E-mail : hkahn@nicstech.com