

보안'USB All Guide

공공기관 및 기업 보안 담당자를 위한 핸드북





국가정보원
보안적합성 검증필

국가정보원 보안적합성 검증필

DefConTM Secure USB
국가정보원 보안관리지침에 따른

가장 편/리/한 솔루션



LG 그룹



국세청



병무청



(구)정보통신부
(현)지식경제부

실제크기 : 480mm × 180mm



주 세이퍼존

[서울본사] 서울시 강남구 삼성동 109-18번지 경희빌딩 2층
[대전지사] 대전광역시 서구 둔산동 1457 둔산현대아이텔 13층

고객지원센터 : 1577-3110

TEL : 02.525.1410

FAX : 02.525.1411

[http:// www.saferzone.com](http://www.saferzone.com)



국가정보원
보안적합성 검증필



한국정보통신기술협회
GS인증



중소기업청
벤처기업인증



기술신용보증기금
우량기술기업선정



한국산업기술진흥협회
연구소인정



SAFE USB⁺

국가 / 기업의 핵심자료 유출에 대한
걱정을 아직도 하십니까?

국정원 인증지침에 따른 닉스테크의 보조 기억매체
관리 시스템 (SAFE USB⁺)로 해결 하십시오.

국가정보원 USB 메모리 등 보조기억매체 보안관리지침에 의거하여
제품 개발을 하였으며, 분실시 보안 USB 사용시스템 정보추출기능, 일반
USB도 사용 등록 후 이용가능, 타 저장매체 통제기능(CD-RW, FDD,
PDA, 시리얼포터 등) 등 기존 보안 USB와 차별화된 기능을 제공하여
기업 및 공공기관의 정보유출을 방지할 수 있습니다.

주요기능

1. 사용자 식별 인증 기능
2. 지정데이터 암호 / 복호화 기능
3. 저장된 자료의 임의 복제 방지기능
4. 분실시 저장데이터의 보호를 위한 삭제 기능 지원
5. 매체 제어 기능

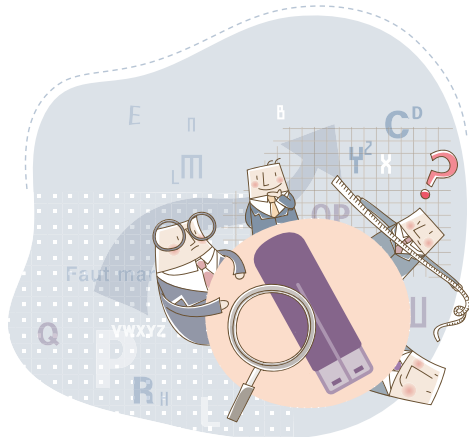
보안 USB+ 협력업체

(주)씨맥스아이엔티 02-521-5174 / (주)키스톤테크놀로지 02-2203-7134 / (주)유네시스 02-2192-3655 / (주)솔디엔아이 02-720-7821 /
(주)엘아이텍 031-478-3599 / (주)네트웍시스템 061-287-0365 / 신한포토닉스(주) 062-949-7107 / 싸이버테크(주) 062-676-2100 /
(주)가희아이티 055-326-4700 / 전북네트웍스(주) 063-838-3006 / (주)티아이에스 033-651-4364

Contents

I. 보안USB 개요

- 006 내부정보 유출방지와 보안USB의 필요성
이동식 저장매체 '보안' 이 필수
- 008 보안USB 시장 현황과 전망
공공시장 석권위한 경쟁 치열할 듯
- 010 보안USB 효율적 활용 방법
보안USB 도입하면 정보유출문제 해결되나?
- 012 보안USB 제품동향
정보유출방지와 매체 통합관리에 효과적
- 014 보안USB 도입시 고려사항
각각의 사용 환경에 적합한 제품 도입해야
- 016 해외 데이터 유출방지 시장 동향
급부상하는 해외 데이터 유출방지 시장



III. 업체별 보안USB 기능 및 특징

- 040 비앤비솔루션, SeProS
- 044 닉스테크, SafeUSB+
- 048 세이퍼존, DefCon Secure USB
- 052 엔트랙커, NTRACKER USB Enterprise
- 056 비젯, Safe USB
- 060 코디아, Secure-i
- 064 솔루션어소시에이트, IGM-Public
- 068 디지털센스, Infosecure-USB



II. 보안USB 활용

- 020 보안USB란?
보조기억매체 관리시스템 '보안USB'
- 022 보안USB의 필요성과 도입효과
정보의 보안과 관리에 효과적
- 024 바람직한 보안USB의 활용 방안
사용특성에 맞는 보안USB 도입해야
- 026 성공적인 보안USB 구축방안
효율성·타당성 충분한 검토 필요
- 028 보안USB 시장현황과 전망
보안USB 초기 시장, 시행착오 우려
- 030 내부정보 유출방지와 보안 USB
내부정보 유출방지에 적극 활용
- 032 <구축사례 1> 경찰청내부 및 원격 업무에 최적화
- 033 <구축사례 2> 편의성과 안정적인 커스터마이징 제공
- 034 <구축사례 3> 정보유출 방지 및 체계적 이력 관리
- 036 <구축사례 4> 안정성과 확장성 고려한 시스템 구축

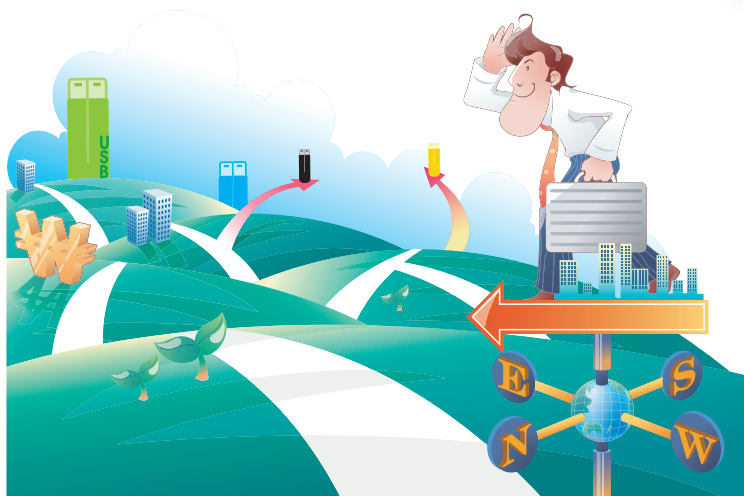


IV. 정보유출과 기업 보안

- 074 <Column> 잇따른 기술유출사건에 대한 단상
- 075 <Column> 보안담당자들이여, 위험을 수치화하라
- 076 <산업보안 X-파일> USB를 이용한 정보유출 사례
- 080 <특별기고> 기술보호(산업보안)에 대한 오해와 착각

V. 부록

- 088 개인정보 관련 법규
 - 공공기관의 개인정보 보호에 관한 법률 시행령
 - 공공기관의 개인정보 보호에 관한 법률
 - 정보통신망법
- 095 주요 정보보호관련 유관기관 및 단체
- 096 국내 주요 보안USB 업체 현황



월간 **정보보호21c** 별책

발행일 2008년 4월 25일

발행처 (주)인포더 (121-600) 서울 마포우체국 사서함 2호

출력 엔테크 인쇄 씨엔씨 미디어



보안뉴스

www.boannews.com

지금 **보안뉴스**에 접속하면
당신의 보안이 **업그레이드**됩니다!!

차별화된 보안전문 뉴스 제공

개인 정보보호와 사이버 침해사고를 비롯한 'IT보안', 기업의 성패를 좌우하는 '기업보안', 일상생활 속의 안전을 위한 '생활 보안'에 이르기까지
보안이슈 총망라.

국내 대표 포털사와 뉴스검색 제휴 체결

국내 대표적 포털인 네이버, 다음 등과 뉴스검색 제휴를 통해 보안뉴스의
최신 콘텐츠와 뉴스 검색.



I. 보안USB 개요

- 006 이동식 저장매체 '보안' 이 필수
- 008 공공시장 석권위한 경쟁 치열할 듯
- 010 보안USB 도입하면 정보유출문제 해결되나?
- 012 정보유출방지와 매체 통합관리에 효과적
- 014 각각의 사용 환경에 적합한 제품 도입해야
- 016 급부상하는 해외 데이터유출방지 시장



이동식 저장매체 ‘보안’이 필수

근본적 보안 대책도 뒷받침 돼야 효과 크다

월간 정보보호21c 편집팀

최근 저장매체의 다양화(FDD, CD-RW, PDA, USB, MP3 등 이동형 저장매체)로 인해 내부자에 의한 정보유출 사고가 증가하고 있다. 또한 USB와 같은 이동성 저장매체의 사용도 급증하면서 정보유출의 사전 예방 및 매체에 대한 통합관리의 필요성이 제기되고 있다.

물론, 현재 말단 저장 디바이스로 CD, DVD, USB, SD카드 등이 많이 활용되고 있기에 보안을 필요로 하는 것은 비단 USB에 한정되는 것만은 아니다. 그러나 여러 디바이스 중에도 특히 일반적으로 보편화 되어 있는 USB는 많은 데이터를 손쉽게 이동·저장할 수 있기에 많이 활용되고 있고 향후 수 년간은 상승세를 이어갈 것으로 예상되고 있다.

코디아 고병수 대표는 “사내 혹은 사외에서 USB의 활용이 많은 이유는 데이터의 간편한 이동성과 편리성 그리고 저렴한 가격이 매력적인 요소로 작용하고 있기 때문이다. 그러나 최근에 발생하는 많은 정보유출 사건에 있어 CD, DVD 및 USB는 가장 많이 활용되는 도구기 때문에 말단 미디어에 보안솔루션을 적용할 필요가 높아졌다”고 설명했다.

특히 USB는 휴대가 편리한 작은 사이즈임에도 대용량을 저장할 수 있고 매년 급격히 하락하는 메모리의 영향으로 휴대저장매체로서 급격한 상승세를 그리는 추세다. 그러나 많이 활용되는 도구인 만큼 외부로의 정보유출을 막기 위한 적극적인 노력이 절실한 현재에 USB를 비롯한 말단 미디어의 제어와 관리는 반드시 해결해야 할 과제다.

이와 관련해서 엔트랙커의 최상백 전무는 “USB메모리의 보급이 빠르게 확산되면서 사용자가 급격히 늘었다. 사용자가 증가함에 따라 USB메모리를 통해 이동되는 정보량도 자연히 증가하게 된다”며 “문제는 회사 및 관공서의 기밀문서가 아무런 반·출입 기록도 없이 자유롭게 담당자의 손으로 유출되어 해외로 팔리고 있다”고 지적했다. 이렇게 유출된 정보는 은밀히 거래되며 해외로까지 팔려나가고 있고 대부분 기밀등급도 높은 편이어서 철저한 보안관리가 필요하다는 것이다.



필수적인 보안 솔루션

1인 1컴퓨터시대에 살고 있는 요즘 컴퓨터는 생활의 필수품이

며 사무실에서는 모든 자료의 저장고로 갈수록 데이터가 쌓이게 되지만 이들 데이터의 물리적 이동 대부분이 USB메모리에 의해 이루어져 편리함과 더불어 자료 유출의 위험이 되고 있다. 특히 USB 등을 통한 개인정보의 무차별적 유포와 특허기술, 연구자료, 국가 기밀문서의 유출이 무분별하게 이뤄지고 있어 기업의 존폐 위기와 국가적 손실로 이어지고 있다.

비젯 이기철 본부장은 “최근 포스코 강판 기술의 중국 경쟁사 유출, 팬택 휴대폰 기술 유출, 현대차 차제 기술 등 외국 및 경쟁사 등에 중요한 기술 등이 불법적으로 유출됨에 따라 국가 및 기업 경쟁력에 큰 타격을 받고 있다”며 “이러한 현실에서 보안USB의 등장은 중요 정보에 대한 합법적인 프로세스를 통한 정보 보호 및 반출의 흐름이 유기적인 형태로 이뤄지므로 현재 상황에서 가장 필요한 보안솔루션”이라고 강조했다.

솔루션어소시에이트 이흥진 부장은 “보안USB는 도난 또는 분실에 대한 대책으로는 최선의 대책임에는 틀림없으나 내부정보의 부정유출을 방지하기 위해서는 보안USB 이 외에도 여타의 보조 기억매체 및 노트북 등에 대한 사용통제 및 반·출입통제 등 보다 근본적인 정보유출 방지대책이 충분히 뒷받침 되어야 할 것”이라고 덧붙였다.

정보유출방지를 위해서는 보안USB의 도입뿐만이 아니라, 보안에 대한 인식제고와 함께 각각의 보안 시스템이 서로 유기적으로 구동될 수 있도록 하는 것도 중요하겠다.

한편 최근에 각 공공기관과 기업 등에서 개인정보보호와 내부정보 유출방지는 이제 더 이상 미룰 수 없는 과제가 됐다. 이는 특히 올해 정보보호 담당자들에게 아주 중요한 정보보호 이슈 중에 하나다. 지난 한 해 동안 국내 대기업의 첨단 핵심 기술이 해외로 유출되는 사건들이 잇따랐고 올해에도 대기업과 옥션, 다음 등 대형 온라인 쇼핑몰과 포털 사이트, 그리고 금융권 등에서 개인정보 유출사고가 터지면서 내부정보보호와 개인정보보호에 대한 중요성과 관심은 갈수록 증대되고 있다. 이에 따라 내부의 핵심 기술을 비롯해 고객의 개인 정보 등 주요 정보자산을 지킬 준비가 되지 않으면 살아남기 힘들다는 인식도 점차 확산되고 있다.

국가정보원에 따르면 2003년부터 2007년 사이 적발된 기술 유출사건만 124건에 이르며 그 피해액은 170조원에 달하는 것으로 나타났다. 특히 2007년 한 해 피해액만 80조원에 육박하는 것으로 조사됐다. 특히 이 같은 보안 사고의 80% 이상이 외부인이 아닌 전, 현직 내부 직원에 의한 것이며, 유출방법은 이동식 저장매체나 CD복사, 이메일, 웹하드 등을 이용해 유출한 것으로 밝혀지면서 기업들은 더욱더 내부정보 유출방지 및 데이터 보안에 촉각을 곤두세우고 있는 만큼 보안 USB도 내부정보 유출방지를 위한 중요한 솔루션으로 그 역할이 크다고 할 수 있다. 15

공공시장 석권위한 경쟁 치열할 듯

고객 요구에 적합한 시스템 구축이 성공 좌우

월간 정보보호21c 편집팀



앞으로 보안USB의 공공기관 공급이 더욱 활발해질 전망이다. 그동안 국가정보원 보안적합성 검증 필요 학습고대해 오던 보안USB 업체들의 숨통이 트였다. 이번에 보안적합성을 통과한 업체는 모두 6개 업체로 지난 4월 7일 세이퍼존, 닉스텍, 브레인즈스퀘어, 솔루션어소시에이트, 아이티네이드 등 5개 업체가 인증을 받았고 지난 15일에는 엔트랙커가 인증을 받았다.

이번에 추가로 인증을 받은 제품은 세이퍼존 'DefCon Secure USB', 닉스텍 'SafeUSB+', 브레인즈스퀘어 'RSM System, SecureDrive', 솔루션어소시에이트 'IGM-Public', 엔트랙커 NTRACKER USB Enterprise, 아이티네이드 'USB Management System' 등이다.

올 4월부터 국가기관은 내부 정보유출을 방지하기 위해 의무적으로 보안USB를 도입해 사용해야 한다. 하지만 여전히 보안USB에 대한 정확한 개념도 모르는 지방자치단체도 많아 업체를 선정하는데 제대로 된 정보가 없다는 지적도 나오고 있다.

이전에 보안적합성을 통과한 업체는 비엔비솔루션 'SeProS', 엘립시스 '유토큰 콤보', 테크모아 'FX-USB' 등 3개 제품이다. 이번에 통과한 6개 회사를 합하면 현재까지 총 9개 업체 제품들이 올해 공공시장 보안USB 시장을 놓고 일전을 펼칠 전망이다. 또한, 현재 비젯, 코디아, 잉카인터넷, 디지털센스 등의 업체 제품이 인증 심사중이다.

업계 관계자는 "올해 상반기와 하반기까지 공공시장 도입이 활발하게 이루어질 것"이라며 "그 이후 기업시장에서도 도입이 늘어날 전망이다. 앞으로 계속해서 경쟁체제가 더욱 치열하게 전개될 것"이라고 말했다.

보안적합성 인증업체 위주로 경쟁

닉스텍 함재춘 차장은 "올해 보안USB 시장 규모는 약 300억원 규모로 예상된다. 4월 15일 현재 국정원 보안적합성 인증업체는 9군데, 하지만 향후 인증업체가 더 증가할 것이며 인증업체 위주로 시장경쟁이 치열해질 것"으로 전망했다. 또한 올 하반기부터는 업체 수가 급감할 것으로

보이며 4월 이후에는 재구매 수요가 한풀 꺾일 것으로 예상했다. 아울러 치열한 가격인하 및 국정원 인증을 획득하지 못한 업체의 경우 공공시장에서의 위치가 여의치 못할 것이라는 전망을 내놴다.

향후 공공기관의 보안USB 사용은 점차 정보보호가 중시되는 통신업종이나 금융권, 의료 분야 등을 포함해 일반 기업으로까지 그 여파가 이어질 것이라는 점을 감안하면 보안USB 인증 획득 여부는 시장 선점 효과 및 추후 사업 존속성 여부로까지 이어질 수 있다는 것.

코디아 고병수 대표는 “현재 여러 보안관련 업체들이 국가정보원의 기준에 맞춰 제품 개발과 공공기관 시장공략에 적극 나서고 있고 올해 4월과 9월을 기점으로 시장이 급격히 확대될 것으로 기대 된다”고 밝혔다. 그는 또 “이는 비단 국가 및 공공기관에 그치지 않고 금융권을 비롯한 일반 대기업과 연구소 등으로까지 확대되어 말단 디바이스의 보안의 중요성을 인식하고 실천해 나가는 계기가 될 것”이라고 덧붙였다.

엔트랙커의 최상백 전무는 “현재 USB의 KS마크라고 할 수 있는 국정원 검증필 제품이 몇 개 되지 않고 오히려 지난 4월 15일 인증을 받기 전까지 엔트랙커에서 실제 납품 운영중인 기관이 제일 많다는 것은 검증필이라는 허울과 실제 보안USB 운영에는 괴리가 있다는 점은 인정해야 한다”고 설명했다.

그는 또 향후 시간이 지나 보안USB를 도입한 기관이 늘어나고 실제 운영 주체의 입소문과 추천이 타 기관과 시장에 가장 큰 영향을 줄 것이라며 각기 다른 특성을 가진 3~5개 정도의 업체 정도가 살아남아 경쟁하는 구도가 될 것으로 예상했다.

비젯 이기철 본부장은 “보안 USB는 시장 개척을 하는 다른 솔루션에 비해서는 쉽게 수익 창출을 할 수 있는 이점이 있다”며 “하지만 고객의 요구에 따라 개발한 솔루션이 아니라 공공기관과 기업 등의 정보 유출로 인한 피해의 심각성을 국가에서 먼저 인식하고 이를 해결할 수 있는 방안에서 출발했기 때문에 시장을 확대하는 데에는 한계가 있다”고 밝혔다. 그러나 국가 및 기업, 나아가서는 개인에게도 필요한 솔루션으로 인식됨에 따라 그 시장은 무궁무진할 것이며 타 시스템과의 연계를 통한 발전 가능성이 충분히 있을 것으로 예상했다.

솔루션어소시에이트 이홍진 부장은 “공공기관의 보안USB 도입이 의무화됨에 따라 공기업을 포함한 전체 공공시장의 규모는 3년간 약 1,200억원 정도로 올해엔 약 300억원, 2009년도 약 600억원, 2010년도 300억원 규모”로 전망했다. 그러나 그는 업체간 저가경쟁으로 치닫는 경우에는 시장규모가 2/3로 줄어들 것으로 내다봤다. 한편 그는 “민수시장은 공공시장과는 달리, 보안USB 제품보다는 내부정보유출방지 솔루션을 더 선호하기 때문에 보안USB 시장이 쉽게 형성되지 않을 것이지만 투자가 용이한 금융권이나 일부 대기업을 중심으로 한 시장은 점진적으로 형성될 가능성이 크다”고 말했다. ⑮

보안USB만 도입하면 정보유출문제 해결되나?

다른 보안 시스템이나 솔루션을 함께 운용해야

월간 정보보호21c 편집팀

보안USB만 도입하면 정보유출 문제는 해결될까? 솔루션어소시에이트 이흥진 부장은 “정보유출을 방지하기 위해서는 보안USB 외에도 다른 보안 시스템이나 솔루션을 함께 운용해야 하는데, 마치 보안 USB만 도입하면 모든 보안문제가 해결되는 것처럼 착각할 정도로 업체의 홍보나 언론의 보도기사가 홍수를 이루어 고객에게 오해를 불러일으킬 소지가 있다”고 말했다. 이 외에도 수많은 업체가 개발경쟁에 뛰어들어 가격경쟁이 심화되면 제살을 깎아먹는 출혈 경쟁도 우려했다. 또한 코디아 고병수 대표는 “CD 및 USB를 서버와 연동함으로써 사용자 권한을 제어하고 관리하여 기존 보다는 더 높은 보안성을 실현하고자 하는 것이 현재의 말단 미디어 보안의 주류다”며 “대부분 서버와 연동이 되지 않을 경우는 사용할 수 없기에 안전하다고 볼 수는 있으나 말단 미디어의 특성상 서버와 연동이 되지 않는 외부에서 많이 활용되는 USB는 서버와 연동이 되지 않는 오프라인에서는 사용하기가 무척 불편하게 되어있다”고 설명했다.

그는 “이에 따라 서버와 연동이 되지 않는 곳에서도 발군의 보안실력을 발휘할 USB가 필요하고 서버의 인증을 통해 외부에 데이터가 이동이 되었거나 열람되어졌을 때 열람된 PC에 열람된 데이터의 임시파일이 남기 때문에 정보가 유출될 가능성이 상당히 높다고 볼 수 있어 임시파일을 남기지 않기 위해서는 USB 자체에 뷰어가 반드시 탑재되어야만 한다”며 자사 제품의 특성을 강조했다.

엔트랙커의 최상백 전무는 “국정원 보안적합성 검증필을 통과한 업체의 제품들이 각각의 특성과 가격 등이 차이가 있어 도입 기관의 담당자들도 기준을 잡지 못하고 있다”며 “검증필 업체 중에는 보안USB를 납품한 사이트가 거의 없는 업체도 있기 때문에 실제로 인증만 믿고 선불리 도입한 기관은 많은 시행착오를 겪을 수도 있다”고 지적했다.

이와 관련해 닉스텍 함재춘 차장은 “공공기관 및 산하단체에서는 올해 4월부터 보안USB를 의무적으로 사용해야하나 지방자치단체의 경우 국정원의 지침이 잘 전달되지 않아 보안USB 도입의 필요성을 못 느끼고 있는 상태”라며 “또 각 기관의 예산 배정이 이미 끝났고 보안USB 도입을 위한 추가 예산을 승인해 주지 않아 보안USB 도입을 하고 싶어도 할 수 없는 기관이 있다는 것도 문제”라고 말했다.

또한 비젠텍의 이기철 본부장은 “현재 보안USB는 국정원 지침을 기준으로 솔루션 개발이 이뤄짐에 따라 고객사를 대상으로 한 시스템의 획일화에서 벗어나 경쟁력을 갖추기 위해 다양한 기능을 탑재하기 시작했다”며 “실제로 PC보안, PMS, 백신 등 다양한 기능을 탑재해서 추진하고 있으나 이러한 부가적인 기능으로만 경쟁력을 강화하는데 한계가 있다”고 말했다. 고객 환경에 맞는 컨설팅 및 커스터마이징 능력이 선행되어야만 고객이 만족할 수 있는 시스템을 완성할 수 있지만 현재로서는 이러한 부분에 대해서는 아직까지 시간이 더 필요하다는 것이다. ①



정보유출 방지와 매체 통합관리에 효과적

정보유출 방지대책 마련은 대·내외적 신뢰 향상에 기여

월간 정보보호21c 편집팀

보안USB에 있어 국정원 ‘USB 메모리 등 보조기억매체 관리지침’에 의한 사용자 식별 및 인증 기능, 지정 데이터 암호·복호화 기능, 저장된 자료의 임의 복제 방지 기능, 분실시 저장 데이터의 보호를 위한 삭제 등 4가지 주요 기능은 필수 사항이다.

닉스테크 함재춘 차장은 “이러한 기능 외에 저장 매체 제어 기능(FDD, CD/DVD-R/W, PDA, USB용 저장장치 등), 사용자 입장에서 필요한 매체 사용 통계 보고서 기능 등을 추가해 차별화 했다”며 “이러한 보안 USB의 도입은 공공기관과 기업 등에서 정보유출로 인한 물질적 피해를 최소화한다. 정보 유출의 사전 예방이 가능하며 매체에 대한 통합관리로 중요정보의 유출을 방지할 수 있다”고 말했다.

코디아 고병수 대표는 보안USB는 국정원 지침에 의한 기본 기능 외에도 타 PC에서 열어본 파일의 데이터가 임시파일(Tempfile)에 남지 않는 기능과 데이터가 저장된 USB를 패스워드와 함께 상대방에게 전달해도 데이터를 열어볼 수만 있고 인쇄와 PC로 복사, 화면캡처 등을 방지할 수 있는 기능을 추가했다는 것이 특징이라고 말했다. 그는 “이 외에도 USB에 자체뷰어가 탑재되어 있어 서버와의 연동이 필요 없이 USB자체로 보안시스템이 구동되기 때문에 PC의 프로그램에 의존하지 않고 열람할 수가 있으나 이 기능은 타 보안USB에 없는 중요한 기능으로 보안성을 강화했다”고 강조했다.

보안USB 하면 일반적으로 비밀번호를 입력하는 정도의 기능을 상상하지만 실제 가장 중요한 기능은 무분별한 USB 사용을 통제하는데 있다. 엔트랙터 최상백 전무는 “보안USB가 필요하게 된 가장 중요한 이유 중 하나가 관리되지 않는 보조기억매체로 인한 정보 유출, 특히 내부자에 의한 정보유출을 방지하는 것이기 때문에 사용한 USB메모리의 모든 사용이력과 반·출입에 대한 통제 기록이 남아야 된다는 것”이라고 설명했다.

비젯 이기철 본부장은 “특히 보안USB 도입은 조직 내부 업무에 필요한 중요한 정보에 대한 불법적인 외부 유출 방지로 대내외적인 신뢰도 확보할 수 있으며 수작업 형태로 진행된 업무에 대한 시스템 구축으로 업무 효율 향상과 업무 연속성 기대할 수 있다”고 보안USB의 도입 효과를 설명했다. 그는 또 “중요 정보에 대한 악의적인 접근에 대해 체계적인 관리가 가능해 업무 투명성을 유지할 수 있고 인사DB, 그룹웨어 등 다양한 솔루션과의 연동이 가능해 업무 편의성 및 확장성에 기여한다”고 덧붙였다.

기본 기능 외에 차별화로 승부

현재 보안USB 제품으로 출시 또는 광고하는 제품은 비엔비솔루션 ‘SeProS’, 세이퍼존 ‘DefCon Secure USB’, 닉스테크 ‘SafeUSB+’, 솔루션어소시에이트 ‘IGM-Public’, 엔트랙터

NTRACKER USB Enterprise, 비젯 'SafeUSB', 코디아 'Secure-i', 디지털센스 'Infosecure-USB', 잉카인터넷의 '엔프로텍트 XTICK', 아이티네이드 'USB Management System', 코스콤 '시큐유에스비(SecuYouSB)' 블루젠의 'VX세이프, 엘립시스 '유토콘 콤보', 테크모아 'FX-USB', 브레인즈스퀘어 'RSM System' 과 'SecureDrive' 등이 있다.

이들 제품 중에서 4월 15일 현재까지 국정원의 보안적합성 인증을 받은 제품은 비앤비솔루션, 닉스테크, 세이퍼존, 엔트랙터, 솔루션어소시에이트, 브레인즈스퀘어, 테크모아, 엘립시스, 아이티네이드 등의 9개 제품이며, 비젯과 코디아, 디지털센스, 잉카인터넷 등의 제품은 현재 인증 심사 중이다. 이들 각 제품들의 기능은 단순한 국정원에서 제시한 보안 지침에 의한 필수 기능에다가 통합 PC 보안과의 연동, 바이러스 백신 탑재 등과 차별화된 기능을 추가해 더욱 확대된 방향으로 출시되고 있는 추세다.

특히 엔트랙터측은 최근 이슈가 되고 있는 보안 USB는 크게 4가지 형태로 나누었다. 첫 번째는 보안USB를 처음부터 개발한 엔트랙터 주식회사의 경우처럼 보안 USB의 기능에 중점을 둔 제품으로 매체 자체의 안정성과 사용자 로그 전송 기능 등이 이미 1년여 간 시장에서 검증되어 왔다는 것을 장점으로 내세웠다. 그리고 두 번째로 통합PC보안 업체들인 세이퍼존, 닉스테크, 잉카 등의 제품들은 USB 매체 보다는 PC단에서 국정원 지침 기능의 대부분을 구현한 제품들이다. 세 번째는 생체 인식 기능을 탑재하는 등 하드웨어적으로 보안USB 기능을 구현한 비앤비솔루션 등의 제품을 들었고 마지막 네 번째는 금융기관 등에서 공인인증서용으로 사용되던 토큰에서 파생된 제품군인 엘립시스의 제품을 꼽았다.

각각의 제품들은 장·단점이 있지만 대부분 전용 USB를 개발하는 것에 초점을 두었다. 처음에는 많이 보급되어 있는 일반 USB를 보안USB화하는데 시간을 소비한 업체들이 일부 있었으나 보안USB 시장의 태동 이유가 편리성 보다는 보안에 무게를 두었기 때문에 일반USB의 보안USB화는 보안에 허점을 드러낼 수 밖에 없다고 설명했다. 이에 따라 일단 전용USB를 채용한 업체들이 제품의 안정성과 가격, 그리고 제품의 간편한 구성 등으로 좀 더 나은 보안환경에 초점을 맞출 것으로 전망했다.

기존의 일반 USB에 비밀번호 설정기능 또는 지문인식 기능을 탑재한 보안USB는 단순한 보안기능 수준으로, 일반 사용자들이 쉽게 보안을 설정할 수 있는 제품이었다. 코디아 고병수 대표는 "Secure 시리즈와 같이 USB에 비밀번호 설정은 물론 수납되는 모든 데이터는 자동으로 암호화 압축됨과 동시에 뷰어의 탑재로 템프파일 보안 및 해킹차단 등의 보안과 편리기능을 더욱 강화한 제품도 좋은 평가를 받았다"고 설명했다.

특히 최근에는 서버와의 연동을 통해 사용자 제한, USB의 중앙관리 시스템을 구축해 더 적극적인 USB보안이 서버보안 및 PC보안 전문 업체 등을 통해 연구 개발되고 있다는 것. 현재의 국가정보원의 기준을 적용한 서버연동 시스템은 다양한 곳에서의 활용도가 낮아 국방과 민간기업, 그리고 설계분야 등에서 다양하고 세분화된 제품화가 이루어 질 것으로 예상했다.

이렇게 다양한 사용 환경에 따라 현재 보안USB의 기술은 초기의 단순한 솔루션 개발 수준에서 벗어나 타 시스템과의 연동, 자체 애플리케이션 기능, 관리 방식 등 다양한 형태에서 고객의 요구에 적합하도록 한 단계 더 업그레이드된 기능의 솔루션 개발에 박차를 가하고 있는 추세다. ⑮

각각의 사용 환경에 적합한 제품 도입해야

기능과 비용 등 꼼꼼히 따져라

월간 정보보호21c 편집팀

최근 발표된 보안USB 제품의 기능은 대부분 대동소이하다. 따라서 보안USB를 도입하고자 하는 기관과 기업에서는 필수 기능 이외에 부가적으로 어떤 기능을 제공하는지, 또 사용자가 요구하는 기능을 얼마나 수용해줄 수 있는지를 잘 판단해야 한다. 닉스테크의 함재춘 차장은 “특히 보안SI의 능력이 있느냐, 없느냐도 도입시 고려해야 할 중요한 부분으로 생각된다”고 말했다. 또한 그는 보안USB는 소프트웨어와 하드웨어가 같이 들어가는 만큼 유지보수도 중요한 부분이라고 덧붙였다.

아울러 코디아의 고병수 대표는 보안 USB 도입을 위한 제품 선정시에는 “USB 저장장치를 PC와 연결해 통신 할 경우 입력한 비밀번호가 PC에서 확인되는 것은 물론이며 암호화되지 않고 평문으로 전송돼 해커의 스니핑 공격에 무방비로 노출될 수 있기 때문에 비밀번호를 설정할 때 해쉬함수를 이용해 저장되는 제품인지, 또 외부에서 많이 활용되는 USB의 특성을 고려해 USB드라이브 자체에도 보안기능이 있는 것이 더욱 안전하고 오프라인에서도 사용될 수 있는지, 그리고 외부에서 열람하더라도 외부 PC에 템프 파일이 남지 않는 제품인지를 고려해야 한다”고 강조했다.

또한 엔트랙터 관계자는 “특히 공공기관의 경우 제품의 안정성과 운영 노하우가 필수적이며 과도한 도입단가가 문제가 될 수 있어 제품의 기능과 가격 등을 꼭 확인하고 도입해야 한다”며 “USB 매체의 경우 경박단소의 경향으로 내구성이 떨어지는 단점을 고려해야 하고 가급적이면 적당한 가격에 운영 노하우가 풍부한 제품을 선택하는 것이 좋다”고 밝혔다.

비젯의 관계자는 공공기관의 경우에는 조직에서 관리해야 하는 중요한 정보 및 자료들이 있는지, 중요 정보에 대한 외부 반출이 빈번하게 발생하는지, 중요 정보 분실시 업무에 영향을 끼치는지, 사용자별 정보 이력 관리의 필요성이 있는지, 이동식 저장 디스크에 대한 제어가 필요한지 등을 고려해야 한다고 말했다. 아울러 금융권과 대기업의 경우에는 중요 기술 및 자료에 대한 보호의 필요성이 있는지, 외부로 반출된 자료가 경쟁사에 넘어갈 경우 회사에 영향을 끼치는지, 중요 자료가 담긴 이동식 디스크 분실 시 업무에 지대한 영향을 끼치는지, 정보 접근에 관해 내·외부로 구분하여 정책을 수행할 필요성이 있는지 등을 고려한 도입을 권장했다.

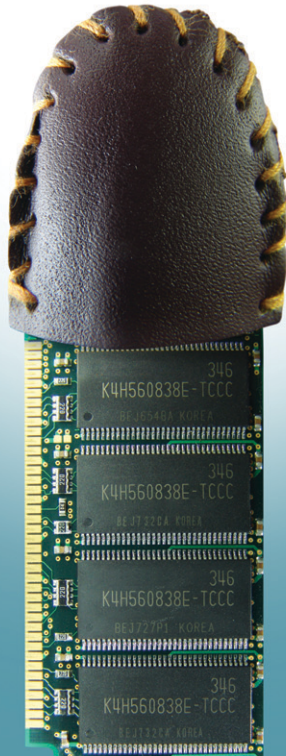
한편 솔루션어소시에이트의 관계자는 공공기관에서는 기존에 개인별로 보유하고 있는 USB를 보안 USB로 전량 교체하지 않고도 국정원의 보안안관리지침을 준수하면서 사용할 수 있는 방법은 없는 지, 여타 보조기억매체의 통제는 어느 수준까지 가능한 지, 운영성에는 문제가 없는 지 등을 확인할 필요가 있다고 말했다.

그는 또 “금융권 등 대기업의 경우 보안 USB 자체의 기능보다는 본래의 목적인 내부정보유출방지를 위한 기능이 얼마나 완벽히 구현되어 있는 지를 확인할 필요가 있다”며 “예를 들면 PC 내 데이터를 노트북이나 외장 SCSI Disk Driver로 복사하는 경우 차단이 가능한지, PC 내 설계도면 등의 이미지 데이터를 CD-ROM(DVD)에 복사했을 때 차단이 가능한지, USB를 읽기만 허용하고자 하는 경우에는 시행 가능한지 등 보안의 무결성에 대해 반드시 확인할 필요가 있다”고 설명했다. ①

nisc 국가정보원 산업기밀보호센터

개발 못지않게 중요한 것이 **보안**입니다!

어떤 기술을 개발했느냐 보다
어떻게 지키느냐가 중요합니다.
보안에 대한 투자는
일류기업으로 가는 지름길입니다.



www.nisc.go.kr
산업기밀 보호상담은 국번없이 **111**

급부상하는 해외 데이터 유출방지 시장

기대와 관심만큼 실제 기술은 아직 미성숙 단계

월간 정보보호21c 편집팀

정부 주도로 사용이 의무화되어 시장이 형성되고 있는 우리나라와는 달리 해외, 특히 북미 지역에는 별도의 '보안 USB' 라는 개념을 찾아보기는 힘들다. 물론 별도의 명칭만 존재하지 않을 뿐, 이미 그들 지역에서는 USB 내에 보안 기능을 탑재해 왔다.

그러나 다른 보안 관련 시장에 비해 데이터 유출방지 시장의 규모가 아직 크게 확대되지 않은 까닭에 우리나라에 비해 해외 시장에서는 손쉽게 데이터를 이동할 수 있는 USB에 대한 보안에 비중을 덜 두고 있는 것으로 이해할 수 있을 것이다.

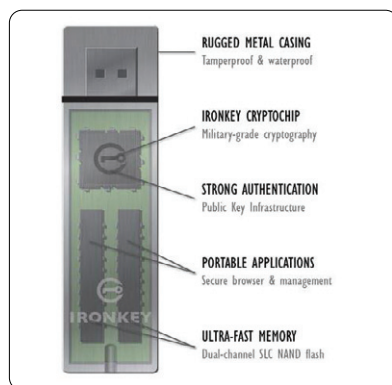
세계적인 IT 전문지 테크타겟의 닐 로이터(Neil Roiter)는 최근 네트워크에서 엔드포인트로 초점이 변화하면서 데이터 유출방지(DLP : Data Loss Prevention) 시장이 진화하고 있고, 특히 대기업이 DLP 기술 업체들을 인수함으로써 통합되고 있다며 'DLP의 시대가 왔다'고 평가했다.

그러나 문제는 대부분의 사용자들이 DLP가 일반적으로 구현하기가 어렵고 고비용이 요구된다고 생각된다는 것으로, 데이터 유출방지 제품에 대한 과대 선전에도 불구하고 실제 기술은 아직 성숙하지 않았다는 것을 의미한다. 그러나 비록 관련 시장의 성장이 급격한 상승 속에 다소 주춤

던 것은 사실이지만 최근 데이터 유출방지가 하나의 시장으로 성숙하고 있는 조짐이 보인다.

Enterprise Strategy Group이 보안 전문가를 대상으로 그들이 데이터를 보호하는 이유에 대해 조사한 결과, 응답자의 72%는 정부 규제를, 62%는 지적 자산에 대한 관심을 원인으로 들었다. 또한 53%는 업계 규정과 더 나은 기업 거버넌스를 원인으로 꼽았다. 즉, DLP 제품을 구매하는데 있어 기업의 이윤 이상으로 중요한 동기로, 그것이 고객 정보를 포함하고 있는 데이터의 침해 공개를 강제하고 있는 법률과 관련된 규제 준수는 북미 시장 등에서 데이터 유출방지 시장의 성장 가능성을 밝게 하고 있는 것이다.

또한, 최근 독자들을 대상으로 분야별 최고의 보안 제품을 선정(Readers' Choice Award)한 미(美) 인포메이션 시큐리티(Information Security)지는 '아직 독자적인 시장 분야로 구분할 만큼의 반응이 충분하지는 않다'면서도 보안 톨의 존재가 중요하게 부각되고 있다고 평가하며 급부상하



고 있는 3개의 시장으로 데이터 유출방지(DLP)를 제일 먼저 언급했다.

또한, 연이어 발생한 노트북을 포함한 여러 모바일 장치들과 관련된 데이터 유출 사건들의 결과로 모바일 장치 암호화 제품이 상당한 관심을 끌고 있다고 평가했다.

한편, 액세스 거버넌스 회사 Aveksa의 부사장 브라이언 클리어리(Brian Cleary)는 채널웹(www.crn.com)과의 인터뷰를 통해 “위기 관점에서 모든 것(데이터)을 분류해야만 한다”며 “이러한 통제가 자리 잡게 되면 데이터 유출의 가능성이 실질적으로 줄어든 것”이라고 말했다. 또한 채널웹의 스테파니 호프만(Stefanie Hoffman)은 기업들이 2008년에

보안 위험 평가와 관리에 상당한 투자를 할 것이라는 보안 전문가들의 말을 인용하며 DLP 업체들은 기업들이 가장 민감한 정보들을 어디에 두어야 하는지, 회사에서 어떤 정보가 누구에게로 빠져나가는 지 알 수 있도록 도와주는 툴을 도입하게 될 것으로 ‘2008년 내부정보유출방지 시장의 경향(Data Loss Prevention Trends To Watch In 2008)’을 예측했다.

그러나 앞서 언급했던 것처럼 DLP 시장이 다시금 주목받고 있다는 것과는 별도로 북미 시장에는 이미 데이터 유출을 방지하기 위한 USB 제품들로 유명한 업체들이 있다. 특히 USB 플래시 디바이스 제조업체이자 데이터 보호와 암호화 업계의 선두 업체인 아이언키(IronKey)는 군용 수준의 보안을 제공한다고 평가받고 있다.

이 업체는 처음부터 안전한 플래시 드라이브로 만들기 위해 설계되었고 현재 군용 수준의 암호화, 자가 파괴 시퀀스, 온라인 보안 저장소, 스텔스 브라우징 기술, 자가 학습 패스워드 관리, 방수 및 형태 조작방지 요소 등을 포함한 고급 기능을 보유하고 있다고 공언하고 있다. 아이언키는 최근 유명 대외 홍보업체와 파트너십을 맺고 적극적인 마케팅에 나서고 있다.

또한, 지난 3월에는 디지털 미디어용 메모리 제품 글로벌 업체 렉사 미디어(Lexar Media Inc.)와 기업용 중앙 관리의 모바일 접근 보호 솔루션 업체 레드캐논 시큐리티(RedCannon Security Inc.)가 렉사의 프리미엄 JumpDrive USB 플래시 드라이브 라인에 통합 원격 접근 및 데이터 보호 추가와 더불어 판매 및 배급에 관한 협약을 발표했다.

렉사는 “레드캐논의 기술을 우리의 JumpDrive USB 플래시 드라이브에 접목할 수 있게 되어 대단히 만족스럽게 생각한다”며 “이 제품들은 기업과 일반 고객들에게 모바일로 작업하는 직원들에 관한 더 나은 강력한 솔루션을 제공한다”고 설명했다. 



SPY 그들의 위장술

“자랑스런 우리의 첨단기술,
우리 손으로 지켜야 할 때입니다.”

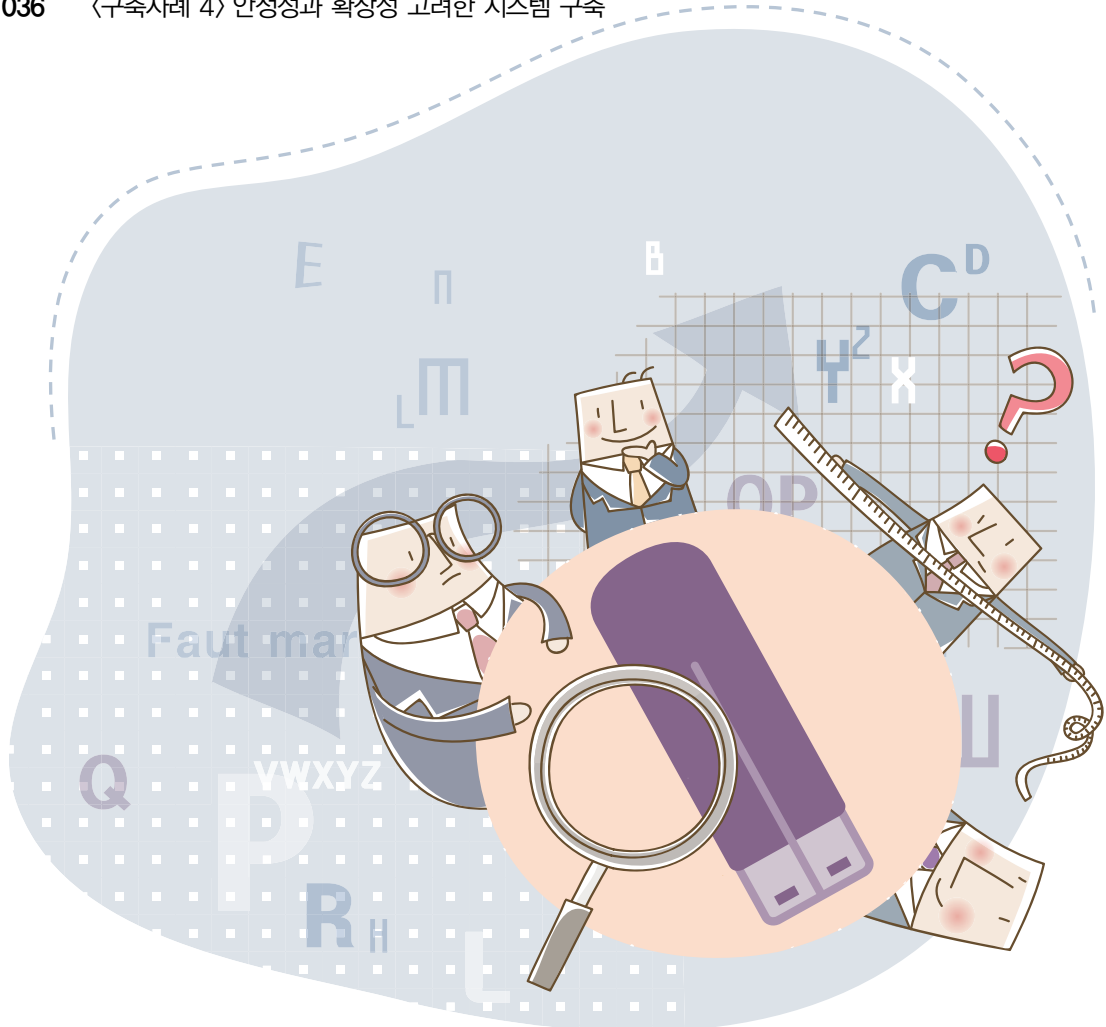
한순간의 무관심과 부주의로
우리의 첨단 산업기술이 유출 될 수 있습니다.

산업기밀 보호상담은 국번없이 111
www.nisc.go.kr

nisc 국가정보원 산업기밀보호센터

Ⅱ. 보안USB의 활용

- 020 보조기억매체 관리시스템 '보안USB'
- 022 정보의 보안과 관리에 효과적
- 024 사용특성에 맞는 보안USB 도입해야
- 026 효율성·타당성 충분한 검토 필요
- 028 보안USB 초기 시장, 시행착오 우려
- 030 내부정보 유출방지에 적극 활용
- 032 <구축사례 1> 경찰청내부 및 원격 업무에 최적화
- 033 <구축사례 2> 편의성과 안정적인 커스터마이징 제공
- 034 <구축사례 3> 정보유출방지 및 체계적 이력 관리
- 036 <구축사례 4> 안정성과 확장성 고려한 시스템 구축



[보안USB란?]

보조기억매체 관리시스템 ‘보안USB’

글 · 김대봉 세이프존 전략기획마케팅부 부장(kimdb@saferzone.com)

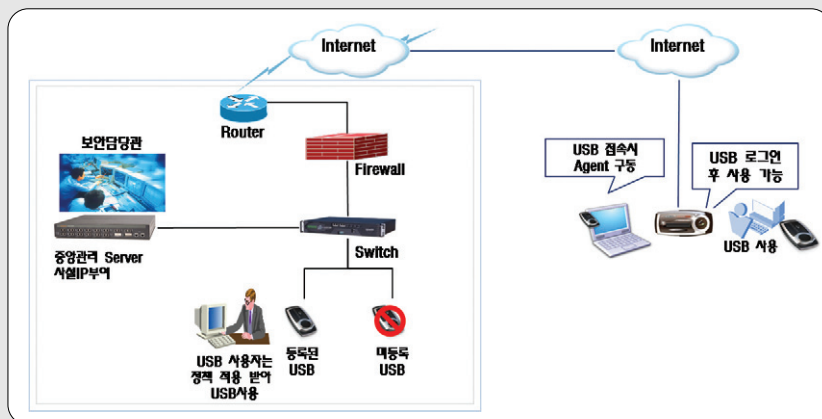
최근 IT기술의 발전에 따라 데이터의 저장 관리를 위한 메모리수단은 다양한 형태로 발전되고 있으며 일반 하드 디스크 드라이브(HDD)부터 외부 메모리수단 CD, DVD, 메모리스틱(카드) 등 비교적 소용량으로부터 기존의 하드 디스크 드라이브의 용량을 넘어서는 고용량의 외부 메모리 장치까지 다양하게 상용화되고 있다.



그중에서도 근래에는 소형이라 휴대하기 편리하고 PC의 USB포트에 간단히 장착하여 사용 가능한 USB메모리가 대중적으로 사용되고 있다. USB(Universal Serial Bus)는 개인용 컴퓨터(PC)와 주변 장치를 접속하는 Bus 규격을 말하는 것으로 일반적으로 외부 메모리 장치와의 인터페이스수단을 간단하게 USB라고 호칭하고 있다.

이와 같은 USB는 PC를 열지 않고 장치를 컴퓨터에 쉽게 연결할 수 있도록 하는 장치를 말한다. USB는 표준 포트와 플러그 조합을 사용하여 프린터, 모뎀, 스캐너, 디지털 카메라 장치를 연결한다. 이 Bus의 장점은 장치를 쉽게 추가하거나, 삭제하거나, 옮길 수 있는 기능을 제공하는 것으로 USB 포트를 이용하게 되면 키보드, 조이스틱, 스캐너, 모뎀 등을 연결하기 위해 필요하던 각 장치간의 인터페이스를 내장하지 않아도 된다. 이로 인한 부가 비용이 PC의 제조 단가를 줄일 수 있으며 새로운 디바이스의 연결이 용이하고 하드웨어적인 호환성 문제를 쉽게 해결할 수 있다는 장점이 있어 일반적으로 사용되고 있다.

이와 같은 USB를 이용하여 PC에 연결하여 사용하는 외장 메모리수단이 USB메모리 스틱이며 이를 간단하게 USB 또는 USB메모리라고 호칭하고 있다. 근래에는 반도체 기술의 발달로 인해 고용량의 USB메모리스틱이 제공되고 있다. 따라서 손쉽게 데이터를 옮길 수 있음은 물론 대용량의 파일까지 쉽게 이동시킬 수 있는 USB의 특성을 감안하면 기업 및 기관 내부에서 심각한 보안 문제를 고려하지



▲ 보안USB 구축 구성도

않을 수 없다. 이에 국가정보원은 2007년 1월에 ‘USB메모리등 보조기억매체 보안관리지침’에 의해 2008년 3월 31일까지 보안적합성 검증필 한 제품을 도입하도록 권고하고 있다. 국가정보원 지침 ‘USB메모리등 보조기억매체 보안관리지침’에는 사용자 인증 및 식별기능, 지정데이터의 암호·복호화 기능, 저장된자료의 임의복제 방지 기능, 분실시 지정데이터 보호를 위한 삭제기능 등의 4가지 필수 기능을 요구하고 있다.

이와 같은 USB메모리 수단을 사용함에 있어서의 보안관리를 수행할 수 있도록 하는 보안 USB메모리 관리 시스템과 이를 구현하기 위한 USB메모리는 USB메모리 내에 저장되는 데이터의 관리 및 사용관리를 위한 프로그램(Agent program)을 내장시키고 이의 프로그램과 정보를 교류하여 USB의 사용 제한 및 사용이력 등을 관리할 수 있는 서버시스템을 구성하여 네트워크상의 PC에서 사용되는 USB메모리의 관리가 가능하도록 하는 것이다. 즉, 이로써 기업 또는 관공서 등에서 내부 데이터의 관리 및 유출 등을 방지할 수 있도록 하는 보안 USB메모리와 보안 USB메모리 관리 시스템을 의미한다.

보안USB메모리 관리 시스템은 내부 네트워크망 및 인터넷과 같은 외부 네트워크 망을 통해 연결되는 다수의 PC에 연결해 사용되는 USB메모리를 관리하기 위한 서버 시스템으로 구성된다. 또한 서버 시스템은 USB메모리 관리프로세스를 포함하는 외장 메모리관리 프로그램이 탑재된 서버와 USB메모리 관리제어정보(관리자 정책결정), 등록된 USB메모리 정보, USB메모리의 사용내역, 저장된 데이터가 저장된 데이터 베이스를 포함하여 구성되고 서버시스템에 등록된 USB메모리는 서버 시스템으로부터 제공된 USB메모리의 관리를 위한 에이전트 프로그램이 설치된 것을 특징으로 한다.

따라서 관공서 또는 기업내부의 데이터 반입·반출에 대한 통제가 용이하며 내부 보안 데이터의 외부 유출로 인한 손실을 방지할 수 있게 된다. 이와 같은 보조기억매체 관리시스템이 내부정보 유출로 인한 기업의 막대한 R&D 투자금과 이에 따른 천문학적인 손실금액을 예방하여 국가 정보유출 방지 산업에 많은 도움되어 IT 산업의 발전과 국가 경쟁력이 한층 높아지길 바란다. 

정보의 보안과 관리에 효과적

글 · 안흥기 닥스텍 기술연구소 상무(hkahn@nicstech.com)

지난해 대한상공회의소에서 실시한 ‘국내기업의 기밀유출 대응실태’ 조사결과 보고서에 따르면 내부 직원이 기밀유출을 시도할 경우 성공 가능성을 묻는 질문에 ‘기밀유출이 가능하다’는 응답이 59.7%, ‘적발되거나 원천적으로 불가능하다’는 응답이 40.3%로 유출이 가능하다는 답변이 훨씬 높게 나오는 놀라운 결과치를 보여주었다.

한 조사기관에 따르면 최다 기업정보유출 경로는 USB가 1위를 차지하고 있으며 회사 메일이 2위, 개인 웹 메일이 3위를 차지했다는 조사결과도 있었다. 지난해 모 외국어 고등학교 입시부정 역시 선생님들이 시험문제를 USB에 담아서 외부로 유출하는 사례도 있었다.

수많은 방법 중에서 이처럼 보안USB가 화제인 이유는 무엇일까? 휴대용 메모리 스틱은 속도가 빠르고 대용량이며 사용하기가 간단하면서도 작은 크기로 휴대성이 높은 장점이 있어 최근 가장 보편적인 휴대용 저장 장치가 됐다. 이러한 장점으로 인해 내부 기밀자료의 외부유출의 매체로 악용되는 사례가 크게 증가하고 있으며 USB시장 역시 매년 빠른 속도로 급성장하고 있다.

그렇다고 USB 사용 자체를 모두 차단하는 정책은 현실적이지 못하기에 등록된 USB만 사용하고 사용자의 인증을 거치고 암호화 로깅, 외부에서의 적법한 사용 그리고 분실 시의 데이터 처리 등 꾸준하게 고객의 요구들이 존재해 왔다.

이에 국정원은 지난해 초(2007년) 국가 공공기관의 기밀유출 방지를 위해 ‘USB메모리 등 보조기억매체 보안관리 지침’을 발표하고 1년간의 유예기간을 거쳐 각급 공공기관들은 올해 4월부터 보안USB를 의무적으로 사용해야 한다. 국정원 지침에 따르면 보안USB는 다음과 같은 4가지 필수기능을 만족해야 한다.

- 사용자 식별 · 인증기능
- 지정데이터 암호 · 복호화 기능
- 저장된 자료의 임의 복제 방지기능
- 분실 시 저장데이터의 보호를 위한 삭제 기능

관리체계 동반돼야 효율적

국정원이 제시하는 보안USB 지침은 사실 ‘보안USB’ 자체 도입 · 운영보다는 ‘관리체계’와 동반되어 운영되어야 한다. 이는 사용신청, 반출신청, 회수 또는 분실까지 여러 단계의 절차를 거쳐야 되며 그 단계는 관리 사이클을 이루며 지속적으로 수행되어야 한다.

다음의 간단한 시나리오를 통해 보안USB 도입에 따른 변화된 업무환경을 예상할 수 있다.

- 지식경제부에 근무하는 사원 K씨는 보안USB사용을 위해 매체제어 사용 신청 시스템에 접속 한 후

팀장에게 보안USB를 1개 신청한다.

- 사원 A씨의 팀장은 메일을 통해 신청여부를 확인하고 신청 시스템에 접속 한 후 미리 일괄 신청한 보안USB 중 1개를 A에게 배포한다. 배포가 완료되면 해당 신청 건을 완료 처리한다.
- 사원 A씨는 해당 보안USB로 회사의 중요정보를 저장하고 사용하며 허가되지 않은 다른 USB는 사내에서 사용이 차단된다.
- A씨가 내일 지방으로 출장이다. 자신의 노트북은 지참하지 않고 보안USB에 중요 자료를 저장하여 내려갈 계획이다.
- 출장기간 동안 보안USB 사용을 위해 팀장에게 보안USB의 외부반출 사용을 신청한다. 이때 사유와 사용기간을 적는다.
- 사원 A씨의 팀장은 메일을 통해 신청여부를 확인하고 신청 시스템에 접속 한 후 외부반출 신청을 승인한다.
- 해당 신청 건에 대해서 보안담당관이 한 번 더 승인절차를 거쳐야 하는데, 이때 USB내의 파일들을 외부로 복사 금지 옵션을 걸지 않고 OTP(One Time Password)를 설정한다. 해당 OTP는 A의 메일로 자동 전송된다. 참고로 보안담당관은 OTP입력 회수 제한을 설정할 수 있다. 이는 보안USB 분실 시를 대비하는 것이다.
- A씨는 출발 전 신청 건의 처리여부를 확인하면 실시간으로 A의 보안USB에 설정 치와 OTP값이 입력된다. A는 필요한 파일을 보안USB에 저장하고 해당 파일은 실시간 자동 암호화된다.
- A씨는 출장지에서 해당 OTP를 입력하고 보안USB에서 자료를 이용하여 업무를 본다. 이때 자료의 사용 내역은 보안USB 자체에 로깅되며 회사 복귀 시 자동으로 서버에 전송된다.

위의 내용은 공공기관에서 보안USB 도입시 바뀌는 업무환경을 간단하게 정리해보았다. 그렇다면 보안USB를 어디서 구매할 수 있을까? 보안USB 제공업체는 기존 PC보안 업체와 기타 보안 업체로 구분될 수 있다. 기존 PC보안 업체가 개발한 보안USB는 매체제어 관리시스템과 외부반출 관리시스템 등의 기존 보안관리시스템과 융합된 관리체계를 제공하는 이점이 있다. 예를 들면 닥스텍의 통합 PC보안 제품과 보안USB를 동시에 구매할 경우 통합보안관리가 가능하다는 장점이 있다.

한편, 기타 보안업체는 기본적인 기능을 충실히 따르며 USB분실 시 추적 기능과 같은 부가적인 기능들을 장점으로 내세우고 있다. 고객의 관점에서 기술적으로 기존 보안에이전트와의 충돌여부와 관리적으로는 보안USB 외로 기타 매체에 관한 제어를 어떻게 가져갈 것인지에 대해서 고려해야 한다. 또한 업체 선정시 사후관리가 가능한 업체인지도 꼼꼼히 따져봐야 할 것이다.

결론적으로 보안USB를 도입함으로 얻을 수 있는 장점은 무엇일까? 크게 두 가지를 꼽을 수 있다.

첫째, 관리적 측면에서 보조기억장치의 등록으로 구역 내 사용현황 파악이 용이하며 분실에 따른 정보 유출 방지, 보안정책 수립 및 시행의 효율적 관리체계 구축이 가능하다.

둘째, 보안성 측면에서는 USB를 통한 문서유출 경로 차단, USB 이용 내역 기록, 미등록 보조기억장치 사용 차단이 가능 하다.

보안USB는 여러모로 편리한 관리적 장점을 제공하고 있다. 그렇지만 보안에 있어 가장 중요한 점은 정보를 이용하는 사람에게 있다는 것을 잊어서는 안될 것이다. ⑩

사용특성에 맞는 보안USB 도입해야

글 · 한오석 비앤비솔루션 부장(foryou@bnbsol.net)

USB메모리 등 보조기억매체는 휴대가 간편하고 사용이 편리해짐에 따라 누구나 쉽게 사용하게 되면서 보안사고도 빈번해지고 있다. 근래 기업뿐만이 아니라 국가의 중요 정보도 USB메모리 등 보조기억매체에 무단으로 저장, 사용하여 뜻하지 않게 유출되는 사례가 발생하고 있어 보안USB의 사용이 시급히 요구되고 있다.

보안USB의 선택

보안USB 시장의 성장과 더불어 업체들 간에 너도 나도 보안USB라는 명칭을 붙여 제품을 출시하면서 보안관계자들을 유혹하고 있어 보안관계자들은 범람하는 보안USB에 대하여 옥석을 가려 선택할 수 있어야 하겠다.

보안USB의 선택에 있어서 가장 중요한 첫번째 기준은 국정원의 보안적합성 검증 통과여부의 확인이다. 현재 시장에는 2007년 9월 비앤비솔루션의 'SeProS'를 필두로 4월 15일 현재까지 약 9개의 업체가 국정원 보안적합성 검증을 통과한 제품을 출시하고 있다.

두 번째로 검토해야 할 부분은 대부분의 업체가 대동소이한 기능을 구현하고 있으므로 특허 등록과 같이 기술적 우위와 지적재산권 침해에 따른 분쟁의 소지를 해소한 제품을 선택하여야 한다. 마지막으로 보안관리 기능에 있어서 얼마만큼 보안관리자 입장에서 프로그램을 구현했는지를 살펴야 한다. 보안USB의 다양한 기능을 일목요연하게 관리할 수 있도록 시스템화 되어 있어야 실질적이고 효과적인 보안 관리가 가능할 것이다.

보안USB의 활용

국정원 지침에 의하면 공공기관에서는 보안USB를 일반용, 비밀용, 공인인증서보관용으로 구분하여 관리해야 한다. 일반용에는 일반자료만 저장되어야 하고 캐비닛 등에 안전하게 보관하여야 한다. 비밀용은 대외비를 포함해서 비밀등급별로 구분하여 보안USB를 각각 마련해야 하며 비밀자료와 동일하게 이중 캐비닛 또는 금고에 보관해야 한다. 공인인증서용에는 공인인증서 이외의 자료를 저장해서는 안 된다. 또한 모든 USB메모리 등 보조기억매체는 용도별로 구분하여 각각의 관리대장을 두어 관리되어야 한다.

보안USB를 분실했을 경우에는 즉시 보안관리 책임자에게 분실보고를 하여 보조기억매체 관리시스템에서 분실 USB에 저장된 중요자료를 원격으로 삭제하거나 분실 USB의 무단사용을 차단시키도록 조치를 취하여야 한다.

개인이 기존에 사용하던 USB의 경우에도 보조기억매체 관리시스템에 등록 후 사용할 수 있지만 공인인증서용으로만 사용해야 한다. 보안USB의 세부 기능은 제조사에 따라 기능과 편의성에 차이가 있을 수 있으므로 구매 전 각 기관의 사용 특성에 적합한 업체의 보안USB를 선택해야 한다. ①

산업기밀 보호상담은 국번없이 111
www.nisc.go.kr

보안이 열리면 미래는 잠깁니다

산업기술 유출은 기업 및 국가
경제에 커다란 손실을 가져옵니다.
우리가 개발한 기술을 우리가 지키지 못하면
기업의 성장도, 국가의 미래도 없습니다.



nis 국가정보원 산업기밀보호센터

효율성 · 타당성 충분한 검토 필요

글 · 김승현 비젯 영업부 부장(rainbowni@bizet.co.kr)

국가정보원은 지난 2007년 1월 ‘USB메모리 등 보조기억매체 보안관리지침’을 발표하고 공공기관을 대상으로 3월부터 1년 동안 일반USB와 보안USB를 자유롭게 사용할 수 있도록 했다. 하지만 유예기간이 끝나는 3월 31일 이후에 USB 사용시 반드시 보안USB를 사용하도록 하고 있다.

현재는 공공기관을 대상으로 의무도입이 되고 있으며 금융권, 기업 등에서도 보안USB 도입 추진이 활성화될 것으로 예상됨에 따라 한층 시장이 확대될 것으로 보인다. 국정원은 보안USB의 필수 보안 기능으로 사용자 식별 · 인증 기능, 지정데이터 암호 · 복호화기능, 저장된 자료의 임의복제방지 기능, 분실 시 데이터 보호를 위한 삭제 기능 등 네 가지 보안 기능을 충족해야만 한다.

결론적으로 공공기관들은 국정원 지침에 따라 보안USB를 도입할 경우 필수 보안 기능을 충족해야 하며 구축 완료 후 적합성 검증을 받아야만 한다. 보안USB는 국가 및 기업, 나아가서 개인에 이르기

까지 그 활용도가 높아지고 있으며 조직 및 개인 정보에 대한 관리에 이르

기까지 그 범위가 매우 광범위하게 적용될 수 있다. 특히 경쟁사 혹은 타인에게 획득되었을 경우, 보안USB메모리가 아닌 일반USB메모리라면 자료 유출로 인한 피해는 경제적인 측면 물론 다방면으로 그 영향을 받을 수 있다.

그러므로 보안USB로서의 기능을 갖추고 있어야 분실되거나 타인에 의해 의도적으로 획득되었다고 하더라도 보안화되어 있으므로 USB메모리 내에 저장된 중요 정보가 외부로 유출되거나 혹은 복사되는 것에 대한 근원적으로 방지할 수 있을 것이다.

보안USB는 기존에 각광받던 FDD, CD-ROM, 이동식 하드디스크 등의 저장매체에 비해 이동성과 휴대성 측면에서 매우 뛰어나고 가격도 저렴해 그 활용도는



| 성공적인 보안USB 시스템 구축을 위한 체크리스트

✓ 보안USB 시스템 구축 타당성 검토

- 시스템 구축에 따른 명확한 목표 설정 및 타당성 확보
- 시스템 확장성, 편의성, 보안성 등 여러가지 측면에서 구축 필요성 검토
- 시스템 운영 전담 인력 확보 가능 여부 판단
- 문서 및 데이터에 대한 등급별 보안 정책 필요 가능 여부 파악
- 내부 정보에 대한 외부 정보로의 활용도 수준 파악
- 저장 매체에 대한 현황 및 활용도 파악

✓ 효율적인 보안USB 시스템 구축시 고려사항

- 시스템 구축에 따른 업무 연속성 및 효율성이 확보되어야 한다.
- USB 등 보조기억매체관리지침에 따른 시스템 구축 여부에 대해 결정한다.
- 인사DB, SSO, 그룹웨어 등 타 시스템과의 연동이 필요할 경우, 가능한지에 대해서 검토해야 한다.
- 보안USB를 제외하고 모든 타 저장매체에 대한 제어 정책이 필요한지 정의한다.
- 3계층 구조(정보보호담당관-부서책임자-취급자) 관리시스템에서 2계층 혹은 다른 형태의 구조로의 변경에 대한 커스터마이징이 가능한지 파악해야 한다.
- 보안USB메모리의 배포 정책-전체 조직원 혹은 필요한 부서별, 조직별 인원-을 결정한다.

✓ 성공적인 보안USB 시스템 구축 방안

- 도입전에 개발사와의 충분한 구축 방안에 대한 논의를 한 후 진행해야 한다(구축 시 고려사항에 대한 체크리스트 작성 필요).
- 보안USB 관리시스템 구축 후 서버-PC Agent-보안USB메모리 등 전체 시스템에 대한 충분한 테스트를 거쳐 안정화 단계를 수행한다.
- 보안USB 시스템과 연동하는 타 시스템(인사DB, SSO, 그룹웨어, DRM 등)과의 연동 테스트를 진행하고 필요한 부분에 대한 커스터마이징을 통해 안정화시킨다.
- 국정원에서 요구하는 필수 기능에 대한 테스트를 통해 제대로 작동하는지를 검증한다.
- USB관리시스템에서 로그 모니터링, 리포팅 기능이 제대로 구현되는지 확인한다.
- 업무 추가 및 변경에 맞춘 신속한 업그레이드 기능을 제공하는지 확인한다.
- 정기적인 시스템 점검 통한 업무 연속성 및 확장성을 항상 확보할 수 있도록 한다.

매우 높아지고 있다. FDD는 저장용량의 한계가 있고 CD-ROM은 한 번 저장하면 재사용이 어렵지만 보안USB는 읽고 쓰기 기능을 제한 없이 사용할 수 있으므로 타 매체에 비해 우수한 장점을 갖고 있다.

보안USB는 기존 일반USB에서 발생할 수 있는 정보 유출 문제에서 완전하게 벗어날 수 있다. 사용자 본인에 대한 식별과 인증을 받지 않고는 정보 저장 및 반출이 불가능하고 분실하였다 하더라도 원격에서 완전삭제 및 데이터 삭제가 가능해 중요 정보에 대한 유출로부터 완벽한 보호 체계를 갖출 수 있게 됐다.

이와 같이 3가지 조건에 대한 점검 사항 및 구축 요인을 검토해서 보안USB도입을 통해 충분히 효과를 확보할 수 있다면 구축하는 편이 나을 것이다. 크게 3가지 조건으로 구분해서 체크리스트를 작성했지만 이 외에도 구축 전 검토해야 할 사항이 많다. 하지만 이 정도 수준에서 충분한 시간을 두고 검토한다면 투자한 만큼의 효과를 얻을 수 있을 것으로 판단된다. **15**

보안USB 초기 시장, 시행착오 우려

글 · 임종규 엔트랙커 대표(info@ntracker.net)

최근 이슈가 되고 있는 보안USB는 기능별로 크게 4가지 형태로 나뉘어 진다.

첫 번째는 보안USB를 처음부터 개발한 엔트랙커의 경우처럼 보안USB의 기능에 중점을 두는 경우이다. 이는 매체 자체의 안정성과 사용시 로그 전송 기능 등이 이미 1년여 간 시장에서 검증되어 왔다는 강점이 있다. 두 번째 경우는 통합PC보안 업체들인 세이퍼존, 닉스텍, 잉카 등의 제품이고 이들 제품은 USB매체 보다는 PC단에서 국정원 지침 기능의 대부분을 구현한다. 세 번째 경우는 생체 인식 기능을 탑재하는 등 하드웨어적으로 보안USB 기능을 구현한 비앤비솔루션의 제품을 들 수 있겠고, 네 번째 경우는 금융기관 등에서 공인인증서 용으로 사용되던 토큰에서 파생된 제품군인 엘립시스 제품을 꼽을 수 있겠다.

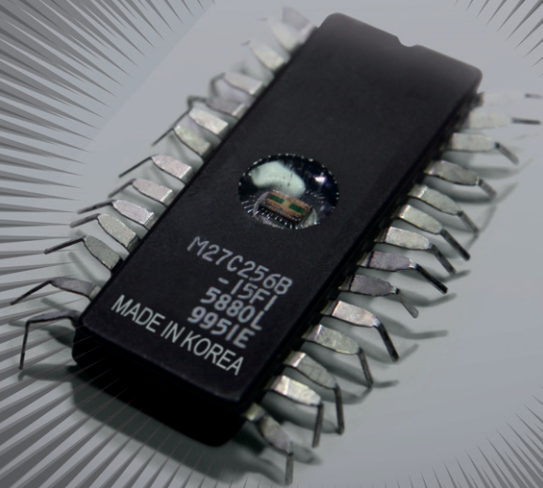
이들 제품들은 각각의 장·단점이 있겠지만 대부분이 전용 USB를 개발하는 것에 초점을 두고 있다는 점이 고무적인 현상이다. 처음에는 많이 보급되어 있는 일반 USB를 보안USB로 개발하는데 시간을 소비한 업체들이 일부 있었으나 보안USB 시장의 태동 이유가 편리성 보다는 보안에 무게를 두기 때문에 일반 USB의 보안USB화는 보안에 허점을 드러낼 수 밖에 없다고 보여진다.

일단 전용 USB를 채용한 업체들이 제품의 안정성과 가격 그리고 제품의 간편한 구성 등으로 좀 더 나은 보안 환경을 꾸려가는 가에 초점을 맞출 것으로 보인다. 현재 보안USB의 가장 큰 문제는 역시 인증이다. 보안USB에 대한 국정원의 보안적합성 검증필을 득한 회사가 4월 15일 현재까지 9개 업체로 선택의 폭이 넓지 않다는 점이 큰 문제며 검증필을 통과한 업체들 또한 일정한 기준 없이 각각 개발한 관계로 가격과 방식 등이 너무 상이해 도입 기관 담당자들이 갈피를 잡지 못하고 있다. 또 검증필 업체 중에는 보안USB를 납품한 사이트가 거의 없는 업체도 있기 때문에 실제로 인증만 믿고 선불리 도입한 기관은 많은 시행착오를 겪을 수도 있다는 것을 염두에 두어야 한다.

현재 보안USB 시장은 이제 막 태동기에 접어들었다고 봐야 할 것이다. 보안USB의 KS마크라고 할 수 있는 국정원의 보안적합성 검증필 제품이 몇 개 되지 않고 오히려 지난 4월 15일 엔트랙커가 국정원의 인증을 받기 전까지도 실제 납품 운영중인 기관이 제일 많다는 것은 검증필이라는 형식적인 허울과 실제 보안USB 운영에는 어느 정도 괴리가 있다는 점은 인정해야 한다.

최근 먹거리가 크게 줄어든 IT보안 업계에 있어서 보안USB 만큼 쉽게 시장에 진입할 수 있는 아이템이 몇 개 나 될 것인가 할 정도로 시장에 진입한 업체가 많아서 초기에는 많은 시행착오를 겪을 것이라는 것은 공통된 견해였지만, 이제 조금 시간이 지나 도입한 기관이 늘어나고 실제 운영 주체의 입소문과 추천이 타 기관과 시장에 가장 큰 영향을 줄 것으로 예상되며 각기 특성을 가진 3개 업체 정도가 살아남아 경쟁하는 구도가 될 것으로 예상된다. **IS**

산업기밀 보호상담은 국번없이 111
www.nisc.go.kr



핵심 기술이 빠져나가고 있습니다

한번 빠져나간 기술은 다시 되돌아오지 않습니다.
기술 유출이 이어지면 우리의 산업기반이 뿌리째 흔들릴 수 있습니다.

nisc 국가정보원 산업기밀보호센터

내부정보 유출방지에 적극 활용

글 · 최주호 디지털센스 대표이사(bksnchoi@unietel.co.kr)

그 동안 정보시스템이 개인용 컴퓨터의 사용, 각 컴퓨터의 네트워크로 연결, 데이터 구축, 정보의 공유 및 활용 단계를 거쳐 발전해왔다. 이 과정에서 축적된 다량의 정보와 보안이 요구되는 파일들이 외부로부터 침입과 내부자에 의해 외부로 유출되는 위험성이 높아지고 있다.

특히 다양한 휴대용 저장장치나 인터넷 통신 등의 발전은 내부 정보의 유출 위험이 높아지고 있는 시점에서 보안USB는 정보유출에 대한 보안 인식을 높일 수 있고 금융권, 기업 등에 미칠 영향이 매우 클 것으로 예상된다. 휴대용 저장장치에 대해 일반 USB에 일부 보안기능이 포함된 소프트웨어를 이용해 보안 기능을 이용했지만 보안 취약점이 노출된 부분이 많았다. 또한 공공기관에는 기밀자료를 제외하고는 정보의 유출을 방지할 수 있는 영역이 작았다고 생각해 네트워크를 통한 침입방지 등에 비중을 높여 보안시스템을 구축하고 운영했다.

축적된 내부 정보는 안전하게 보관하고 이동시킬 수 있어야 하며 저장된 파일을 활용할 수 있어야 한다. 이러한 측면에서 보안USB는 외장형HDD, CD-RW/DVD 등 휴대형 저장장치를 이용한 정보유출방지에 대한 보안 필요성을 인식시켰고 더 나아가 사용자 컴퓨터에 대한 종합적인 정보유출방지로 발전시킬 수 있는 계기가 됐다.

현재 인증된 제품의 보안USB의 기능을 분석하면 보안USB에 파일을 저장할 때 암호화 상태로 저장되게 함으로써 USB 분실시 저장된 파일의 내용에 대한 접근을 제한하거나 파일 내용의 정보 노출을 방지할 수 있는 기능을 요구하고 있다. 또한 분실시 관리 서버에 등록하면 원격으로 파일의 삭제 기능을 구현토록 함으로써 분실된 USB에 저장된 파일에 대한 2중, 3중 보안장치를 만들어 놓은 것이다. 이러한 기능은 USB에 저장된 파일에 대해서 분실에 대한 보안성을 강조한 결과이고 저장된 파일에 대한 가용성 측면에서는 매우 제한적이다. 보안USB의 사용시 고려할 사항 중 첫 번째는 USB에 파일을 저장할 때 Explorer창을 이용하는 경우 Drag&Drop, Copy&Paste, Save 또는 Save as의 방법이 있으나 USB에 파일을 저장시 암호화 상태로 저장하려면 Save 또는 Save as의 방법은 사용할 수 없다는 점이다. Save나 Save as로 파일 저장시 모든 파일을 자동 암호화할 수 있는 방법이 제공되지 못하기 때문이다. 둘째는 USB에 저장된 파일을 열어 보거나 수정하기 어렵다는 점이다. 암호화된 파일을 열거나 수정을 위해서는 메모리상에서 복호화하거나 암호화된 파일을 복호화해 USB에 저장한 후 파일열기 후 수정할 수 있어야 하지만 평문 상태로 파일을 보안USB에 저장할 수 없어 파일의 열기와 수정이 제한될 수 밖에 없다는 점이다.

일부 제품에는 일반영역과 보안영역으로 구분하여 일반영역에 복호화해 평문파일을 저장한 후 다시 보안영역에 암호화 저장하는 방식을 이용하고 있지만 사용자가 보안파일을 일반영역에 저장하는 경우 정보가 노출될 수 있는 위험을 가지고 있다. 비밀문서의 파일은 당연히 보안USB에 저장 및 이동해야 하지만 수정과 편집이 가능한 일반문서를 보안USB에 저장하는 경우에는 활용에 많은 제한이 있을 것으로 예상된다.

셋째는 보안USB 저장장치 이외의 외장형HDD, CD-RW/DVD, 캠코더, 디지털카메라, PDA 등을 이용하여 파일 유출하는 경우 여전히 보안 취약점을 가지고 있다는 문제다. 현재의 보안USB 분실시 정보유출 방지 목적에 중점을 둔 보안방책으로 전제하고 향후 정보유출을 방지할 수 있는 방안을 다음과 같이 제안 한다.

종합적인 정보유출방지 솔루션으로 발전

첫째는 사용자의 컴퓨터에 저장된 파일에 대한 유출방지 방법이 더욱 필요하다는 점이다. 1차적으로는 사용자의 컴퓨터와 서버에 저장된 파일에 대한 유출방지 방법이 강구되어야 할 것이다. 사용자 컴퓨터에 보안시스템이 설치되어 파일의 유출 내용에 대해 로그를 생성하거나 유출을 방지할 수 있는 보안방법이 요구된다. 비 등록 저장장치를 통해 파일이 유출되는 경우 유출로그를 생성하거나 파일의 저장·복사를 금지 할 수 있도록 해 사용자 컴퓨터에 대한 파일유출을 방지할 수 있는 보안시스템 필요하다.

이러한 방법은 사용자 컴퓨터에 보안 에이전트(Agent)가 설치되어야 요구되는 기능을 구현할 수 있다. 보안USB와 에이전트가 연동되면 다양한 보안 기능의 구현이 가능하므로 이를 발전시켜야 한다. 둘째는 사용자 컴퓨터에 대한 통합 유출방지 시스템이 필요하다는 점이다. 사용자의 컴퓨터에 저장된 파일이 외부로 유출되는 경로는 크게 저장장치, 인터넷을 포함한 통신, 종이 문서로 인쇄할 수 있는 프린터, 기타 사무기기 등을 이용하는 방법이 있어 이에 대한 종합적인 유출방지시스템이 필요하다는 점이다. 최근에는 Wibro/HSDPA 등의 이동통신을 이용해 사무실내에서 손쉽게 정보를 유출할 수 있어 이에 대한 보안 방책이 필요하게 됐다.

셋째는 보안USB의 경우 보안문서 등 보안등급이 높은 파일을 저장할 수 있는 보안USB와 일반문서와 공인인증서 등을 사용할 수 있는 보통이나 낮은 보안등급의 보안USB로 구분하여 사용자의 활용성을 높일 수 있는 방안이 필요하다는 점이다.

현재의 보안USB는 보조저장장치 중 가장 많이 사용하고 있는 USB에 대한 보안방법을 제시하고 있지만 다른 저장장치에 대해서도 보안 기능의 적용이 필요하다. 보안USB가 향후 사용자 컴퓨터에 대한 종합적인 정보유출방지 솔루션으로 발전할 수 있는 계기가 되어 국가나 기업이 많은 비용과 투자로 구축된 정보나 중요자료가 유출되어 발생할 수 있는 손실을 예방 하고 사회적인 문제가 될 수 있는 위험요소를 최소화 시켜 안전한 경영활동에 기여할 것으로 기대된다. ⑬

경찰청 내부 및 원격 업무에 최적화

글 · 한오석 비앤비솔루션 부장(foryou@bnnbsol.net)

경찰청은 국정원 보안적합성 검증을 통과한 보안 USB를 도입한 국내 최초의 기관이다. 경찰청은 업무 특성상 USB메모리 등 보조기억매체의 활용이 내·외부에서 빈번하게 이루어지고 있어 특히 보안 사고에 대한 대책마련이 시급한 기관이었다.

실제로 군·경찰 등에서 중요자료가 유출되어 신문·방송 등의 언론에 기사화 되어 사회적 파장을 일으킨 사례도 발생했다. 이처럼 보조기억매체에 대한 보안대책이 시급했던 경찰청에서는 중소기업청에 구매조건부 신제품 개발사업으로 보안USB의 개발을 의뢰했고, 이에 국가정보통신망의 보안장비 개발 전문업체로써 기술적인 노하우를 확보한 비앤비솔루션이 중소기업청 과제 수행을 위한 주관기업으로 선정됐다.



경찰청에서는 2006년 10월 비앤비솔루션의 'SeProS(씨프로스)'를 경찰청의 보조기억매체 관리시스템으로 시범 적용했다. 경찰청의 전산 네트워크는 내부망과 외부망으로 구성되어 있어 각각의 망에 보조기억매체 보안관리시스템을 구축하여 경찰청은 내부에서 뿐만이 아니라, 일선 경찰 업무 중 외부에서 원격으로 이루어지는 업무에 대해서도 보안대책을 강구했다.

경찰청에서는 2006년 12월까지 시범사업을 통해 사용자 편의와 관리자 편의, 관리 기능 강화 등 경찰청 보안관리 업무에 최적화된 시스템이 되도록 수정, 보완을 진행했다. 이로써 'SeProS'는 시스템의 안정화와 보조기억매체에 대한 보안기능의 최적화를 확보할 수 있는 계기가 됐다.

경찰청에서는 2007년부터 본격적인 보조기억매체 관리시스템을 도입하여 2008년 현재 각 지방청뿐만 아니라 일선 지구대까지 보조기억매체 보안관리시스템을 적용하여 보안에 만전을 기하고 있다. 보조기억매체 보안관리 시스템에 대해 경찰청 본청 각국·관에 배포 후 사용자 설문조사 결과 시스템의 성능이 우수하다는 평가가 93%에 이르렀고 전국적으로 시행되어야 한다는 의견이 대다수를 차지했다.

경찰청에서는 본 시스템을 도입 후 단 1건의 보안사고도 발생하지 않아 보안관리의 효과가 입증되었으며 정보보안에 대한 사용자들의 인식제고에도 큰 몫을 했다.

경찰청 관계자는 보조기억매체에 의한 보안사고는 뜻하지 않은 곳에서 발생하게 되므로 단순히 교육과 단속으로만 사고를 예방하기는 한계가 있어 반드시 보조기억매체 보안관리시스템을 구축해야 실질적인 보안관리가 가능하다고 강조하고 있다. 15

편의성과 안정적인 커스터마이징 제공

글 · 임종규 엔트랙커 대표(info@ntracker.net)

보안USB 시장이 태동한 이유 중의 하나가 2006년 말에 방위사업청 소속 해군 중령이 택시에 두고 내린 USB메모리 때문에 벌어진 소동 때문이라는 이야기가 있다.

이 소동 때문에 이들 기관의 보안담당자들은 보안강화 방안을 모색하던 중 그 당시 보안USB를 국내에서 유일하게 출시하고 있었던 엔트랙커를 찾게 되었고 엔트랙커와 협상을 진행하면서 보안의 취약점을 완벽하게 보완할 수 있다는 확신을 갖고 도입을 결정했다.

초기 도입 후 엔트랙커 연구원과 보안 담당자들간의 적극적인 협의로 솔루션은 예상 보다 훨씬 빠르게 안정화에 들어갔고 솔루션 안정성이 인정되자 해군본부 는 해병대뿐만 아니라 전부대로 확대 보급했다. 이후 방위사업청 역시 전체 부서로 확대 도입했다. 도입 후 각 기관의 담당자들은 생각보다 솔루션 사용이 어렵지 않고 커스터마이징도 안정적으로 이루어져 흡족해했다.

엔트랙커가 방위 사업청과 해군본부 전체에 자사의 보안USB를 운영한지가 벌써 1년이 훨씬 지났다. 더구나 두 기관에서 운영 중인 보안USB의 수량은 현재까지 보급된 타사 보안USB 전체 수량보다도 몇 배가 많다는 것을 자부하며 보안USB의 원조임을 강조하고 있다. 물론 많은 시행착오도 겪었지만 이것이 현재 엔트랙커 USB의 안정성과 효율성의 밑거름이 되었다고 한다.

그리고 중앙부처 중 비밀문서 생성이 가장 많은 기관 중 하나인 통일부 전체에 보안USB를 납품해 안정적이고 효율적으로 운영하면서 보안적합성 검증을 신청했다. 타사들이 샘플링이나 무상 기증을 통해서 보안적합성 신청을 한 것과는 조금 다른 경우다.

최근 제 17대 대통령직 인수위원회에도 보안USB를 납품했다. 나라의 5년 대계와 중요한 정보들이 수많은 인수위의 각 분과 별로 커스터마이징되어 엔트랙커 USB를 통해 사고 없이 관리되기도 했다. 이 외에도 국군정보 사령부, 한미연합사, 국가 비상 기획위원회 등 보안이 중요시 되는 기관들에 납품됐다. 엔트랙커가 보안적합성 인증이 나오지 않은 상태에서도 꾸준한 매출을 기록하고 있었던 것이 바로 이러한 탄탄한 기존 구축 경험에서 비롯된 것이다. 특히 기관의 보안 담당자들은 USB메모리 300개, 에이전트 500개 기준으로 3,000~4,000만원 정도로 예상되는 도입비용에 비해 30~50% 정도 저렴하다는 것에도 만족스럽게 생각하고 있다. 한편, 엔트랙커는 지난 4월 15일 국정원 보안적합성 인증을 받았다.

그리고 각종 이동식 저장매체를 통한 정보 유출 방지를 위해 이들 매체 통제에 강력한 성능을 갖는 RSC라는 에이전트 프로그램을 가지고 있으며 이 또한 납품 실적이 1만8천 라이선스가 넘어 풍부한 운영 노하우를 가지고 있다는 것이 장점이다. **15**



정보유출 방지 및 체계적 이력 관리

글 · 김승현 비젯 영업부 부장(rainbowni@bizet.co.kr)

비젯은 보안USB 전문개발 업체로 업무 연속성 및 편의성에 초점을 맞춰 시스템을 개발했다. 보안솔루션의 기본 컨셉인 보안에 대해서도 충분히 고려한 설계를 통해 완성도 높은 시스템을 구현했다.

비젯의 'SafeUSB'는 지난해 1월 국가정보원에서 발표한 'USB 등 보조기억저장 매체 관리 지침'에 부합하는 시스템으로 개발됐다. 이

지침은 4월부터 시범적으로 시행됐으며 1년 동안 공공기관을 대상으로 시범서비스를 거쳐 일반USB 환경에서 보안USB 환경으로 전환하도록 권고했으며 올해 4월부터 의무적으로 도입해서 사용해야 한다.

국정원에서 요구하는 필수기능인 사용자 식별 및 인증, 지정 데이터 암호·복호화, 저장 데이터 임의복제 방지, 분실 시 저장 데이터 원격 파괴 등의 4가지 기능을 충족하는 동시에 시스템의 효율성을 극대화하는 인터넷 역기능에 대응할 수 있는 백신 기능과 공인인증서 저장이 가능한 스마트카드 기능을 추가했다.

부가적으로 제공하는 기능은 타사와는 차별되는 요소로 시스템 도입 시 상당한 효과를 볼 수 있을 것으로 예상하고 있다. 비젯은 보안USB의 중요성이 확대됨에 따라 공공기관을 대상으로 한 제품 설명 및 영업을 수행했으며 다양한 고객들을 만나면서 고객의 정확한 요구사항을 파악할 수 있는 계기를 마련했다.

그 중에서도 보안USB 시스템을 의무적으로 도입기로 한 A국립대학교에 SafeUSB시스템을 구축했다. 이 대학은 SafeUSB 시스템에 대한 전사적인 체계를 구축하는 것을 목표로 본격적인 구축을 진행했다. 하지만 진행되는 과정에서 전체 시스템 구축으로 인한 구성원의 반발 및 안정화 단계에 대한 시간의 필요성을 인식하고 단계별 구축으로 방향을 수정하여 진행했다.

지난 1월부터 시스템 구축을 수행했으며 업무 협의 및 컨설팅, 사전 테스트를 통해 안정화를 확보한 이후에 시스템을 본격 가동했으며 총 4주의 시간이 소요됐다. 이번 시스템 구축으로 보안USB를 제외한 일반USB 및 이동식저장디스크, FDD, CD-ROM 등을 완벽하게 차단함에 따라 정보유출의 위험으로부터 벗어날 수 있게 됐다. 또 외부사용에 대한 신청-허가 단계를 지침에 따라 중요 정보에 대한 외부 사용 이력 관리가 가능해져 효과적인 정보 활용 빈도 및 모니터링이 가능하게 됐다.

결론적으로 업무 환경에 부합하는 SafeUSB 시스템을 구축함으로써 중요 정보에 대한 유출을 원천적으로 방지하고 업무에 대한 연속성을 확보할 수 있게 됐으며 다양한 정보에 대한 효율적인 모니터링



이 가능해져 업무 효율성을 한층 강화할 수 있게 됐다.

원천적인 정보유출 방지에 적합

이번에 구축한 SafeUSB 시스템은 경기 김포 외고 시험 문제 사전 유출 피해, 포스코 강판 제조 핵심 기술 중국경쟁사 유출 피해, 현대기아차 차체조립기술 중국경쟁사 유출 피해, 첨단 휴대폰 기술정보 유출 피해발생, 삼성전자



TFT·LCD 핵심 기술 유출 미수 등 예전부터 최근에 이르기까지 발생한 정보유출로 인한 피해를 원천적으로 방지할 수 있는 환경을 구현할 수 있다는데 그 의의를 두고 있다.

무엇보다도 조직 내부의 중요한 정보 유출로 인한 피해가 커지고 있으며 대부분 내부 사용자에 의한 발생빈도가 높다는 점에서도 발 빠르게 구축을 추진한 요인으로 작용했다. 이처럼 이 대학은 이번 시스템 구축으로 다양한 효과를 얻고 있다. 특히 논문과 특허 등 원천 자료에 대한 USB 등의 이동식 저장장치를 통한 외부 반출 시 모니터링을 통한 정보 흐름을 한눈에 파악할 수 있게 됐다.

또 허가된 보안USB메모리를 사용하고 허가받지 않은 일반USB는 사용할 수 없으므로 정보 매개체의 일원화로 체계적인 관리가 가능해졌다. 중요자료가 담겨있는 USB 분실시 유선상 혹은 온라인상으로 담당자에게 신고하면 원격에서 USB 차단 및 메시지 생성, 완전 삭제 등 3가지 단계로 차단 설정이 가능하므로 정보 유출을 방지할 수 있다는 것이 장점이다.

이러한 장점들이 있는 반면에 단점도 있다. 특히 보안시스템 도입에 따른 거부감에 대해서는 단계적인 구축방안으로 해결하고 있다. 또 사용자 환경의 변화로 인해 업무 체계에 대한 교육 및 홍보가 필요한데 이에 대해서는 기존 시스템 환경에서 변화를 최소화할 수 있는 시스템 구축으로 업무 연속성을 유지하고 있다.

무엇보다 중요한 것은 항상 새로운 시스템을 구축하면서 발생할 수 있는 문제에 대한 준비 자세가 필요하고 무리하게 전체 시스템을 변경하기 보다는 사용자 환경에 맞게 단계별로 시스템을 구축하는 것이다. 이럴 경우 상당 시간이 소요되기는 하지만 시스템 완성도 및 안정화 측면에서는 매우 효율적인 효과를 얻을 수 있다.

이번에 구축한 SafeUSB 시스템은 A대학의 환경에 대한 요구를 충분히 수용하고 사전에 업무 협의를 통해 시스템 정의를 내림으로써 주어진 영역 내에서 최상의 효율을 얻을 수 있게 됐다는 것이 큰 특징이다. 15

안정성과 확장성 고려한 정보보안

글 · 조상구 코디아 이사(wildjoe@kodia.co.kr)

정보화시대에 있어서 핵심기술의 정보보안은 회사의 운명을 좌우한다. 정부 및 공공기관뿐만 아니라 대소를 막론하고 많은 기업들이 보안에 대해 신경을 곤두세우고 있다. 다양한 노력을 기울였음에도 불구하고 정보가 유출되는 것을 막을 수 있는 방법이 여의치 않아 방관할 수밖에 없는 처지이기도 했고 완성도 높은 보안시스템을 구축하기 위해 엄청난 투자비용과 사용자의 불편함을 감수해야만 했었다. 그리고 정보유출을 막기 위해 서버보안, 네트워크보안, PC보안, 문서보안 등 다양한 노력과 전력투구를 했음에도 불구하고 여기저기 날아다니는 집나간 정보를 바라보며 안타까워할 수밖에 없는 노릇이었다. 그러나 정작 그 정보들의 유출경위를 추적해보면 안방의 두터운 금고에서 나간 것 보다는 부뚜막이나 사랑방 그리고 대문 앞 등에서 흘러나간 정보의 비율이 높다는 것을 부정할 수 없다. 왜냐하면 정보를 나만 혼자 보며 사업을 영위해 갈 수 없기 때문이다. 이에 USB 및 기타 말단 미디어의 보안의 중요성을 인식해야 한다.



문서, 동영상 등의 USB보안(Secure-i)

대전의 H연구소에서는 매년 기술세미나를 개최하고 회원으로 가입한 참석자들에 한해 발표 자료를 배포하는데 이 자료에는 회원들에게 만큼은 알려줘야 할 중요한 기술정보가 동영상과 함께 들어 있었다. 요즘에는 워드뿐만 아니라 동영상, 음악, 사진 등이 곁들여 있어서 CD로 전달했다.

그러나 문제가 발생했다. 이전까지는 자료를 종이문서로 배포했기 때문에 설령 복사되어 전파되었더라도 정보유출에는 한계가 있었다. 그러나 자료를 받은 한 회원이 지인에게 자료를 건네주고 이 지인은 인터넷을 통해 이 자료를 배포하는 바람에 어디서나 구할 수 있는 자료가 돼버렸다.

이에 H연구소는 CD to CD, CD to 하드디스크의 불법복제를 방지할 수 있는 코디아의 Secure-i CD를 도입했고 회원들에게 안심하고 자료를 배포할 수 있었다. 더구나 H연구소의 연구원들이 다양한 곳에서 강의를 할 때 타인의 PC로 기존의 USB를 활용할 경우 강의 후 USB를 빼와도 그 PC에 템프 파일이 남아서 불안했고 강의 중 휴식시간에도 USB의 분실 내지는 불법복제에 신경이 쓰였었는데 Secure-i USB를 활용하면서 그러한 문제까지도 해결됐다.

카드데이터 USB보안(Secure-CAD)

조선업계에서 특수선분야에서 세계 선두를 달리고 있는 D조선이 선박을 건조해 선박과 함께 인도하

는 사양서 및 설계관련 자료는 DVD로 약 7장 정도로, 선주에게 인도된 정보가 누출될 가능성에 대해서 고민하고 있었다.

설계도면의 경우 Multi-TIFF DWG Image PDF 등의 다양한 포맷의 도면을 구현하고 대형 사이즈의 출력 및 출력 허용여부 선택, 설계도면의 확대 축소가 자유로운 D조선은 설계도면 관련 세부 희망사항을 만족하면서도 완벽한 정보보안을 할 수 있는 솔루션을 찾고 있었다.

Secure-CAD는 그러한 요구에 맞춰 기존의 보안기능의 CD 및 USB에 설계도면 전용뷰어를 개발하여 탑재함으로써 고객의 요구에 부응할 수 있었고 선주에 전달되는 자료뿐만 아니라 사내·외에서 보관 또는 이동되는 정보데이터를 안전하게 보호할 수 있었다. 이에 다양한 분야에서 활용되고 있는 CAD도면의 보안에 적극 활용될 것으로 기대하고 있다

서버 연동형 USB보안(Secure-Network Control)

세계적인 철강회사 P사는 사내정보 보안을 구축하면서 회사 내·외부에 데이터를 전달하는 이동성이 높은 말단 미디어의 특성을 감안하여 USB사용자 식별 및 인증, 회의 및 세미나시 복제방지 및 정보유출방지, 대외 제출용의 보안강화를 위한 솔루션 개발을 추진했다.

코디아는 외부에서의 사용률이 높은 USB의 보안 완성도를 높이기 위해 Secure-i USB 자체에 전용뷰어를 탑재했는데 그것은 외부에서 USB내의 데이터를 볼 수는 있어도 인쇄, 화면캡처 등을 방지할 수 있는 기능을 구현했다. P사의 경우 이러한 기능을 연동시킴으로서 USB 사용자 관리를 철저히 하고 USB가 외부에서 사용되더라도 정보유출을 차단할 수 있는 시스템을 구축했다. 특히 서버보안에서 발군의 실력을 자랑하는 I사와의 공동개발에 의한 뛰어난 중앙관리 기능으로 안정적이고 확장성 있는 제품을 개발할 수 있었다.

국가정보원의 보조기억매체 관리 및 지침에 따른 사용자 식별 인증 기능, 지정데이터 암호·복호화, 저장된 자료의 임의 복제 방지 기능, 저장데이터의 보호를 위한 삭제기능을 만족시키면서도 P사 고유의 특성을 잘 살린 시스템구축 솔루션이라 할 수 있다.

이러한 보안USB의 도입에 있어서 고려해야할 가장 중요한 포인트는 운영시의 안정성과 향후 변화가 고객의 요구에 따른 확장성이다. 이는 실적으로 증명된 회사의 제품이어야 정보의 효과적인 관리와 보호가 가능해 진다는 것이다. 최근 국정원이 제시한 기능을 충족한 다양한 제품들이 쏟아져 나오고 있고 각 공공기관을 중심으로 도입이 확대되고 있기에 보안USB는 차후 정보유출방지에 꼭 필요한 솔루션으로 자리매김할 것이며 아울러 한국이 말단 디바이스 보안의 강국이 될 것으로 확신한다. ⑮

www.nisc.go.kr

산업기밀 보호 상담은 국번없이 111



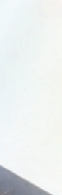
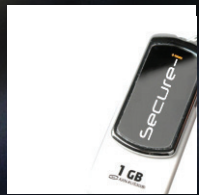
기술유출로부터 안전해야 국가경쟁력이 커집니다!

기업도산의 위기까지 불러오는 핵심기술 유출,
산업기술 보호는 국가경쟁력의 첫걸음입니다.

nisc 국가정보원 산업기밀보호센터

국내 출시된 주요 업체 보안USB 솔루션의 기능과 특징

비엔비솔루션 SeProS | 닉스테크 SafeUSB+ | 세이퍼존 DefCon Secure USB
엔트랙커 NTRACKER USB Enterprise | 비젯 SafeUSB | 코디아 Secure-i
솔루션어소시에이트 IGM-Public | 디지털센스 Infosecure-USB



비엔비솔루션 SeProS



비엔비솔루션은 지난 2006년 경찰청의 개발 의뢰로 중소기업청 구매조건부 신제품개발사업의 일환으로 보안USB의 개발을 추진, 같은 해 9월에 개발을 완료했다. 개발 완료 후 경찰청에 시범사업으로 납품되어 같은 해 12월까지 3개월간 다양한 현장적용 검증절차를 거쳐 가장 안정화된 보안USB 시스템을 구현했다. 현재 경찰청에서는 전국의 지방경찰청을 비롯해 일선 지구대까지 보급하여 활발하게 사용하고 있으며 'SeProS' 도입 후 단 한 건의 유출사고도 발생하지 않고 있다.

사용자 및 관리자 편의 중심 보안 강화

'SeProS'는 관리자 기능을 강화하기 위해 보안USB 제품으로는 유일하게 USB 제품 표면에 제품 시리얼 번호를 조각해 넣었으며 제품 시리얼 번호는 관리자 프로그램과 연동해 관리기능을 한 층 강화했고 관리자가 손쉽게 USB의 사용현황을 파악할 수 있도록 했다. 또한 분실 등에 대비해 수요처의 로고와 습득신고 전화번호를 수요처의 요구에 따라 제품표면에 조각하여 공급하고 있다. 이처럼 고객의 요구사항에 유연하게 대응할 수 있게 된 원인은 보안USB를 외주생산 없이 비엔비솔루션의 자체 공장에서 직접 생산하기 때문에 가능하게 됐다.

또한 사용자 편의뿐만 아니라 관리자 중심의 사용 편리성을 극대화했다. 관리자 프로그램은 웹으로 제공되며 관리자는 한 눈에 사용현황을 파악할 수 있도록 했다. 관리자는 마스터 관리자와 단위별 관리자를 두어 관리 단위별 보안관리가 가능하여 실질적이고 효과적인 보안관리체계를 구축할 수 있도록 유도하고 있다. 특히 통계 레포트 기능을 추가하여 사용자 및 보안USB 사용 현황을 통계 데이터로 쉽게 파악할 수 있도록 했다.

이 외에도 보안USB의 플래시메모리 보안영역을 숨김으로 처리하여 전용프로그램 사용 및 인증 없이는 보안영역에 저장된 파일의 목록조차 볼 수가 없도록 구현되어 보안성을 강화했다. 또한 전용 파일

탐색기의 자체 파일시스템을 개발하여 사용함으로써 플래시 메모리가 USB에서 분리되어도 메모리에 액세스할 수 없어 메모리에 저장된 데이터에 접근이 불가능하게 했다.

SeProS에 저장되는 모든 데이터는 암호화되어 저장 되므로 삼중사중으로 보안기능을 구현하여 어떠한 불법적인 시도에도 데이터 유출을 방지할 수 있어 그 보안성이 탁월하면서도 사용자에게는 불편을 느끼지 않게 한 점이 특징이다.

SeProS의 주요 특징

● 별도의 프로그램 없이 PC매체 제어 가능

국정원의 보조기억매체 보안관리지침에 명시된 주요기능을 완벽하게 수행할 뿐만 아니라 추가의 프로그램 구입 없이 HDD, FDD, CD-ROM, IEEE 1394, Parallel, Network 등의 매체제어 기능을 동시에 제공함으로써 PC 매체제어를 위한 별도의 소프트웨어 구매비용을 절감할 수 있게 했다.

● KISA 비밀번호 생성규칙 준수

서버인증방식으로 사용자 식별코드 및 비밀번호를 'SeProS' 서버에 저장하고 서버와 에이전트 PC 간의 통신 패킷을 암호화하여 보안성을 강화했다. 'SeProS' 서버에 저장되는 비밀번호는 8자리 이상으로 기호, 문자, 숫자를 조합해야 하고 연속된 문자, 숫자의 사용을 금지하는 KISA의 비밀번호 생성 규칙을 준수하고 있다.

● 서버&에이전트 프로그램 기능

'SeProS'의 보안정책 설정은 부서별, 지역별뿐만 아니라 동일 부서 내에서도 개인별로 차등화 하여 설정할 수 있어 사용자의 보안등급에 따라 효과적인 보안관리가 가능하도록 했다. 'SeProS' 에이전트 프로그램이 사용자 PC에 설치된 이후에는 사용하고자 하는 모든 휴대용 저장매체는 서버에 등록해야 사용자 PC에 접근할 수 있어 USB 등 미등록 휴대용 저장매체에 의한 불법적인 정보유출을 차단할 수 있다.

에이전트 프로그램이 설치되면 'SeProS' 보안USB뿐만 아니라 시중에서 구입하는 일반 USB에 저장되는 데이터도 모두 암호화되어 저장되므로 무단 반출에 의한 정보유출은 원천적으로 예방할 수 있도록 했다. 또 분실했을 경우에도 여러 단계의 안전절차에 의해 데이터가 유출될 우려는 없으며 사용자의 분실보고에 의해 무단사용자의 IP를 추적할 수 있어 분실된 보안USB를 회수할 수 있고 불법적인 사용에 대한 문제를 해결할 수 있다.

특히 보안USB는 분실 등에 의한 불법 사용으로 5회 이상 서버인증에 실패할 경우에는 보안유지를 위해 보안USB의 상태가 ON-Line뿐만 아니라 OFF-Line에서도 보안USB에 저장된 모든 데이터는 강제로 삭제되고 복구할 수 없도록 했다. 'SeProS' 서버에는 모든 사용 로그가 저장되어 주요 데이터의 이동경로를 파악할 수 있고 보안USB 또는 일반USB에 저장된 파일정보를 로그로 관리하도록 했다. 또한 각종 보조기억매체 관리대장을 국정원 지침에서 정한 양식대로 출력할 수 있어 보안관리 및 보안감사 등에 대비하여 보안관리자의 편의를 도모했다.

● 보안USB의 Off-line 사용 지원 및 USB 내 작업 기능

또한 사용자 편의를 위하여 보안USB의 반출기능 구현으로 반출승인이 된 보안USB는 외부에서 On/Off-line 구분 없이 사용할 수 있도록 하였다. 이때 사용된 내역은 보안USB 자체에 로그를 저장하며 반입 후에는 서버에 외부에서 사용한 로그내역을 자동으로 보관하도록 하여 보안관리를 강화했다. 특히 보안USB에 암호화되어 저장된 파일을 PC로 이동하지 않고 보안USB 내에서 복호화하여 작업이 가능하며 재 암호화하여 보안USB에 저장할 수 있어 PC에 작업 파일의 흔적을 남기지 않아 그 보안성이 탁월하다.

● 생체인증 기능 추가

지문, 얼굴 등 생체인증 기능을 별도의 추가 비용 없이 구현하여 사용자의 보안등급 및 저장 데이터의 비밀 등급에 따라 선택적으로 사용할 수 있게 설계되어 그 보안성을 극대화했다. 이처럼 'SeProS'는 국가정보통신 보안장비를 개발, 생산하는 보안장비 전문 방위산업체의 기술 노하우로 개발된 제품으로써 경쟁사 대비 사용자 및 관리자 편의성과 보안성에 큰 차별화를 두고 있다.

| 비엔비솔루션

최근 보조기억매체의 후대가 간편해지고 사용이 보편화됨에 따라 국가 및 기업, 개인의 기밀정보 유출 사례가 빈번하게 발생하고 있어 사회적·경제적으로 파장이 일고 있다. 정부에서도 전자정부 구현을 위해 보조기억매체에 대한 보안대책이 시급하게 요구되고 있어 정부 및 공공기관에서의 보안USB 사용이 강조되고 있다.

비엔비솔루션(정연택 대표)은 보안USB 시장에 가장 먼저 진출해 2008년 3월 현재 경찰청을 비롯해 노동부, 특허청, 부산시교육청, 모 기관의 연구소, 한국인터넷진흥원, 군위군청 등 다양한 국가기관 및 공공기관에 보안USB를 납품하고 있다. 이 기업은 지난 2003년 8월 삼성전자의 보안·암호장비 사업부에서 분사하여 설립된 회사로써 군, 경찰, 정부기관 및 공공기관 등에서 사용하는 국가정보통신 보안장비를 전문으로 개발·생산하는 방위산업체다. 이 기업에서 개발·생산하는 보안장비는 국가정보통신망의 핵심 보안장비로써 안정적인 정보통신 보안체계 확립과 운영에 일익을 담당하고 있다. 'SeProS'는 이러한 국가용 통신보안장비를 개발, 생산하면서 축적된 암호화 기술과 네트워크 보안기술을 기반으로 개발되어 경쟁사 대비 특히 우수한 보안성을 확보하고 있다.

특히 2007년 9월 국내 최초로 국가정보원의 보안USB 보안적합성 검증을 필함으로써 대내·외적으로 그 기술력과 보안성을 공인 받았다. 국가정보원의 보안적합성 검증제도는 전자정부구현을 위한 행정업무등의 전자화촉진에 관한 법률 등 관계법규에 의거하여 국가 및 공공기관에 도입하는 정보보호제품의 보안적합성과 안전성을 사전에 검증함으로써 국가정보통신망의 보안수준을 제고하기 위해 시행하는 제도이다.

또한 이 제품은 보조기억매체 보안관리시스템과 관련해 3건의 특허등록을 완료했다. 본 특허에는 보안USB 서버와 에이전트 PC, 보안USB 간의 매체 등록, 인증, 폐기 등의 기능과 보안등급 검토, 보안정책 실행, 데이터의 암호화, 보안USB의 위치추적과 데이터의 원격삭제 기능이 포함되어 등록됐다. 따라서 'SeProS'는 서버인증 방식을 채택한 유사 제품의 난립을 방지하고 지적재산권의 권리를 확보함으로써 고유의 기술력을 보호받을 수 있을 뿐만 아니라 사용자에게도 지적재산권에 대한 분쟁의 소지를 해소했다.

www.bnbsol.com / 02-801-0199

국/내/최/초

국정원 보안적합성 검증 통과 진짜 보안USB “씨프로스”

보안적합성 검증,
빨리 통과하고 늦게 통과하는 데에는 다 이유가 있습니다.



비엔비솔루션(주)는 삼성전자(주)에서 분사한
보안장비 전문 방위산업체 입니다.

보조기억매체 보안 관리시스템 “SeProS” 특허등록



“씨프로스”의 보안USB는 특허등록으로 권리를
보호받고 있습니다. 본 특허를 침해한 유사
제품을 사용할 경우 불이익을 받을 수 있습니다.

대한민국 정보보안! 비엔비솔루션(주)이 새롭게 지켜가겠습니다.

닉스테크 SafeUSB+



닉스테크의 SafeUSB+는 사용자의 식별인증기능, 지정데이터 암호·복호화 기능, 저장된 자료의 임의 복제방지기능, 분실시 데이터의 보호를 위한 삭제기능 등 국정원의 지침에 따라 만든 제품이다. 타 회사 제품과의 차별성이 있다면 매체제어기능을 추가했다는 것이다. 사용자의 정책 설정에 따라 CD/RW, 이동형저장장치, PDA 등의 제어가 가능하다. 또 일반 USB를 사용하고자 하는 기관의 요구에 맞게 등록 후에 일반 USB도 사용할 수 있으며 일반 USB는 읽기만 가능하게 하고 쓰기는 차단하는 기능 등, 도입하고자 하는 기관의 특성에 맞도록 유연하게 구성할 있다.

통합 PC 보안노하우로 시스템 안정성 확보

2001년도부터 개발 및 판매한 통합 PC 보안의 경험을 바탕으로 한 'SafeUSB+'는 국정원 보안관리 지침이 발표되기 전부터 보안USB와 흡사한 기능을 사이트 요구에 의해서 개발 납품했다. 이 제품은 보안USB의 필수기능을 제외하고라도 사이트에서 다년간 검증된 통합 PC 보안 제품의 기능을 많이 접목하여 'SafeUSB+'를 구매하면 통합 PC 보안 기능을 함께 사용할 수 있다는 장점을 가지고 있다.

인증번호 기반의 보안 기능 강화

장치 인증 번호를 입력하기 전까지 사용자가 사용하는 일반 영역은 Hidden영역으로 보호됨으로 장치 인증 번호의 인증 없이는 이미 저장된 파일의 읽거나 새로운 파일의 쓰기를 할 수 없게 구현되어 있다. 장치 인증 번호로 인증을 받은 후 사용하는 경우에도 모든 데이터가 국정원에서 권고하는 ARIA_256 알고리즘으로 자동 암호화되어 저장된다. 또한 사용자가 입력한 장치 인증 번호와 Random Key를 바탕으로 하는 'PKCS#5 패스워드 기반의 암호 인증' 방식을 따라서 장치 인증 번호는 해킹할 수 없게 구현되어 있다.



장치 인증 번호는 8자리 이상으로 문자, 숫자를 조합해야 하고 연속된 문자, 숫자의 사용을 금지하는 비밀번호 생성규칙을 따르고 있다. 그리고 자동으로 암호화된 문서 중에서 사용자가 원하는 파일들에 한해서 본인만의 비밀번호 설정으로 또 다시 암호화를 할 수 있다. 이는 만일의 경우 내/외부에서 보안USB를 분실하거나 비밀번호를 유출하더라도 파일단위의 암호화가 되어있으므로 다른 사용자가 복호화할 수 없도록 구현이 되어있다.

아울러 사용자 PC에 설치되는 Agent 프로그램은 시중에서 사용하고 있는 프로세스 Kill 프로그램으로는 Kill할 수 없는 방법으로 Agent의 프로세스를 보호함으로 사용자가 정상으로 설치된 Agent 프로그램을 불법적으로 Kill 또는 삭제를 할 수 없게 되어 있으므로 보안 기능이 탁월하며 관리 측면에서도 편리하게 관리를 할 수 있다.

권한에 따른 관리 프로그램

각 사용자의 권한에 따른 관리 프로그램을 제공하고 있다. 이는 정보보안담당관/관리책임자/취급자의 3단계 권한을 두어 각 사용자의 권한에 맞게 UI 제공하여 사용자 편의성에 중점을 두었



으며 도입기관의 조직 구성에 따라 각 사용자의 권한을 변경하여 사용할 수 있게끔 하여 조직 구성에 따른 유동성도 배려했다. 특히 정보보안담당관은 관리 시스템의 모든 상태를 한 눈에 파악할 수 있게 하는 현황리스트 조회 및 각종 통계 리포팅 기능 등으로 관리시스템의 손쉬운 관리 및 개인별/부서별/파일별 보안USB 및 매체 사용 통계 자료를 얻을 수 있다.

이 외에도 도입 기관의 요구에 따라서 제품에 도입 기관의 로고와 습득시 연락처, 제품 시리얼 번호 등사용자가 원하는 내용을 제품에 포함시킬 수 있으며 통합 PC 보안의 매체 제어 기능 제공과 더불어 외부에서도 사용하도록 하는 외부 반출 승인 기능과 사용자가 언제 어떻게 얼마만큼의 정보를 이동시켰는지 알 수 있는 일일보안지표를 판단할 수 있는 통계 자료도 제공된다.

| 닉스테크

닉스테크(박동훈 대표)는 지난 1995년 설립 이후 다양한 기업용 S/W를 개발해 왔으며 현재는 명실상부한 대표적인 통합PC보안 솔루션기업으로 거듭나면서 향후 소프트웨어 서비스 기업으로 변신하기 위해 현재 정보보안서비스, e-비즈니스, IT서비스 등 특화된 수익모델로 초석을 다지고 있다.

제품으로는 보안USB 관리솔루션 SafeUSB+, 통합PC 보안관리 솔루션 SafePC Enterprise를 국내에 공급하고 있다. 이 외에 포티넷 등 외산 보안제품을 공급하고 있다. 통합PC보안 솔루션 SafePC 엔터프라이즈는 2001년 처음 출시 이후 현재 공공기관, 일반기업분야에서는 타 PC보안업체 비해 가장 많은 래퍼런스를 보유 명실상부한 1등 제품이라고 할 수 있다. SafePC 엔터프라이즈는 GS인증, 국정원 보안검도필, 신SW대상, NEP인증 제품이다.

또한 지난해 하반기에는 최근 이동형저장장치, 특히 USB를 통한 정보유출이 사회의 큰 이슈가 되고 있다. 이에 발 맞춰 국정원 지침에 따라 최적화된 기능을 첨가한 보조기억매체관리솔루션 SafeUSB+를 출시했다. 현재 국정원 보안성 검토필 인증을 받아 본격적으로 제품을 판매하고 있다.

SafeUSB+의 차별화된 기능으로는 통합PC보안제품에 들어가 있는 매체제어 기능이 들어가 있으며 보고서통계기능을 통해 개인별, 부서별, 파일별로 일일 사용 현황을 파악할 수 있어 업무에 효율적이다. 특히 안전모드에서 사용이 가능하며 에이전트에 설치되는 프로세스 Kill 방지 기능이 들어가 있다. 기존 통합PC보안고객의 경우는 보안USB에 이진트가 필요 없이 업그레이드만을 통해서 편리하게 제품구매가 가능하다는 것도 장점이다.

닉스테크는 현재 중소기업용 대상 통합PC보안제품을 상반기 내에 출시 예정이며 특히 올해 공공기관의 보안USB의 의무구매 등으로 SafeUSB+의 매출이 크게 상승할 것으로 기대하고 있다. 2008년에는 120억원의 매출을 달성하는데 무난할 것으로 전망하고 있다.

www.nicstech.com / 02-3497-8900



SAFEUSB⁺

국가 / 기업의 핵심자료 유출에 대한
걱정을 아직도 하십니까?

국정원 인증지침에 따른 닉스테크의 보조 기억매체
관리 시스템 (SAFE USB⁺)로 해결 하십시오.

국가정보원 USB메모리 등 보조기억매체 보안관리지침에 의거하여
제품 개발을 하였으며, 분실시 보안USB 사용시스템 정보추출기능, 일반
USB도 사용 등록 후 이용가능, 타 저장매체 통제기능(CD-RW, FDD,
PDA, 시리얼포터 등) 등 기존 보안USB와 차별화된 기능을 제공하여
기업 및 공공기관의 정보유출을 방지할 수 있습니다.

주요기능

1. 사용자 식별 인증 기능
2. 지정데이터 암호 / 복호화 기능
3. 저장된 자료의 임의 복제 방지기능
4. 분실시 저장데이터의 보호를 위한 삭제 기능 지원
5. 매체 제어 기능

보안USB+ 협력업체

(주)씨맥스아이앤티 02-521-5174 / (주)키스톤테크놀로지 02-2203-7134 / (주)유네시스 02-2192-3655 / (주)솔디엔아이 02-720-7821 /
(주)엘아이텍 031-478-3599 / (주)네트웍시스템 061-287-0365 / 신한포토닉스(주) 062-949-7107 / 싸이버테크(주) 062-676-2100 /
(주)가희아이티 055-326-4700 / 전북네트웍스(주) 063-838-3006 / (주)티아이에스 033-651-4364

세이퍼존 DefCon Secure USB



최근 IT산업의 발전으로 메모리의 경박단소화에 따른 보조기억매체의 소형화, 대용량화에 의해 사용자의 PC에 저장되어 있는 자료를 보조기억매체를 통해 외부로 유출되는 것을 방지하며 이를 체계적으로 관리하고 모니터링 할 수 있는 시스템의 필요성과 함께 보조기억매체 관리는 필수적인 보안요소로 자리매김하고 있다. 보조기억매체 관리시스템인 DefCon Secure USB는 국가정보원의 'USB 등 보조기억매체 보안관리지침'을 만족하며 보조기억매체로의 데이터유출을 철저히 제어함과 동시에 관리자 및 사용자 중심의 설계로 업무의 연속성을 유지할 수 있다. 이 제품은 사용자인증 및 식별기능 지정데이터 암호·복호화 기능 저장된 자료의 임의 복제 방지기능 분실시 데이터 보호를 위한 삭제기능 등이 4가지 필수 기능을 모두 충족하고 있다. 이 기능 외에도 다수의 PC보안 솔루션의 구축경험과 고객지원 노하우를 바탕으로 한 안정성과 타 저장매체(무선랜, 블루투스, CD-RW 등)를 통제 및 로깅할 수 있으며 일반 USB도 사용 등록 후 이용이 가능하며 모듈 추가로 PC보안으로의 확장 구현이 가능하고 웹기반의 UI와 관리자 중심의 플렉스 기반 레포트도 지원된다.

따라서 이 제품은 보조기억매체를 효율적으로 관리하고 인증된 보조기억매체에 대한 사용과 사용내역을 보관함으로써 정보관리의 투명성 및 안정성을 제공하고 있다.

DefCon Secure USB의 주요 특징

● 사용자식별 및 인증기능

사용자 식별은 보조기억매체 등록 시 서버에 기존 인사DB와 연동된 정보와 매칭해 식별하며 인증은 USB를 접속하면 패스워드 로그인 기능을 통해 인증하며 패스워드는 암호화 된 형태로 USB보안영역에 저장된다.

● 저장데이터 암호화기능

보조기억매체로 파일 복사/이동시 선택적 또는 강제적으로 파일을 암호화 한다. 암호화는 PW 지정과 파일 암호화의 2단계 구조를 지원하며 Agent가 설치되어 있지 않은 PC에서는 암호화된 파일이 복호화되지 않는다.

● 저장된 자료의 임의복제 방지기능

보조기억매체에 저장된 파일은 임의적으로 복제할 수 없고 사용자의 인증절차를 거쳐야만 복제를 할 수 있다. 또한 복제된 내역에 대해서는 USB의 보안영역에 로그를 저장하고 있어 서버와 통신시 로그가 서버로 저장된다.

● 분실시 데이터 보호를 위한 삭제기능

보조기억매체 분실시 삭제는 2가지 프로세스로 구현한다. 서버와 통신이 되는 지역에서는 관리자의 분실등록으로 데이터를 원천 삭제할 수 있으며 오프라인이나 통신이 되지않는 지역에서는 패스워드 실패 횟수에 따른 삭제를 구현한다.

● 모니터링 기능

보조기억매체 관리시스템의 사용로그 저장은 용도변경이력, 사용이력, 파일접근 로그로 구분되며 모든 로그는 실시간으로 통신하여 저장 된다.

● 국정원 별지서식 지원 기능

보조기억매체관리시스템인 'Defcon Secure USB'는 웹2.0 플렉스 기반으로 개발되어 컬럼의 수정 및 형식을 자유롭게 웹 상에서 설정하며 엑셀파일로의 저장이나 출력을 구현한다.

● 다중 보조기억매체 제어 기능

PC에 고정장착된 보조기억매체 장치(FDD, CDRW, DVD RW)는 보안정책 및 관리자의 승인 절차에 따라 사용한다. 이동식 저장매체(외장형 디스크, USB메모리, 플래시메모리)는 USB 시리얼 번호 및 사용자등록 후 보안정책에 따라 사용 보조기억매체의 반출은 승인 후 반출하여 사용할 수 있으며 승인되지 않은 보조기억매체는 사용금지 된다.

● 에이전트 보호기능

관리자에게 권한을 부여 받지 않은 사용자는 보안 에이전트를 임의로 삭제 및 정지를 할 수 없다. 작업관리자를 이용하여 프로세스를 중지하려 해도 프로세스 감춤 기능으로 사용자가 에이전트의 프로세스를 확인 할 수 없게 하며 여러 방법을 이용하여 삭제 시도한 내역에 대하여 실시간으로 모니터링을 지원한다.

● 원본 저장 기능 및 반출 승인

보조기억매체로 복사/이동되는 파일의 원본저장기능을 통해 사후감사의 명확성 및 투명성을 극대화시킨다. 한편 보조기억매체의 반출은 승인 후 반출하여 사용할 수 있으며 미승인 된 보조기억매체는 사용금지 된다.

● 제품 구성과 구축

'DefCon Secure USB'는 중앙관리서버 소프트웨어, 에이전트, 소프트웨어, 보안전용 USB로 구성되며 중앙관리서버는 정책관리, 모니터링 Agent는 정책적용, 사용자식별 보안전용 USB는 사용자인증, 암호화, 데이터삭제 등을 수행한다.

중앙관리서버는 내부망에 구성하며 별도의 인증서버 없이 USB의 자체인증만으로 사용을 할 수 있어 서버의 장애(정전/재해 등)가 발생하여도 업무의 연속성을 유지할 수 있다.

DefCon Secure USB의 특 · 장점

● 통합보안관리

모든 추가 기능들을 단일 Agent에 Plug-In방식으로 추가하여 구현 함으로써 P C의 부하를 최소화 할 수 있으며 통합보안관리를 실현할 수 있다.

● 연동성

ESM, 백신로그 및 다양한 솔루션과의 연동을 통해 관리자의 편의성을 증대 및 보안 시너지 효과 극 대화를 이룰 수 있다.

● 안정성

8년간의 수많은 구축 경험 및 노하우를 통한 기존 애플리케이션과의 충돌없이 구축 될 수 있는 안정 된 솔루션이다.

● 확장성

자산관리, 출력물보안, 인터넷 모니터링 시스템과의 확장성을 제공하여 온라인을 통한 정보 유출뿐만 아니라, 오프라인을 통해서 정보가 유출되는 것을 방지 할 수 있다.

● 편리성

웹기반의 UI와 관리자 중심의 플렉스 기반 레포트도 지원되어 추가 작성없이 보고서를 출력할 수 있다.

| 세이퍼존

세이퍼존(권창훈 대표)은 2001년 창립이후 우리나라 정보보안 전문기업으로서의 사회적 역할과 의무를 위해 최선을 다하고 있는 젊은 기업이다. 설립 초부터 기술연구소를 창설하여 기술연구기반의 기업으로 성장하고 있으며 기술신 용보증으로부터 우량기술기업으로 인정받았고 PC보안솔루션인 DefCon(데프콘)으로 벤처기업 인증, GS인증을 획득 하여 공공기관 일반기업 부분에서 다른 경쟁사에 비해 많은 레퍼런스를 확보했다.

또한 제품의 우수성을 인정받아 KT와 협력하여 2005년부터 약 2년간 준비한 PC보안 솔루션으로 기업 내에 설치된 PC보안 중앙관리 시스템에 대한 관제 시스템으로 시스템정보 · 네트워크정보 · 서비스정보 · 침입탐지정보 등 각종 로그 취합 및 분석을 통한 사전 장애발생 방지 시스템 및 원격장애 처리 시스템을 구축했다. 아울러 데프콘은 각 기 업내 내부정보유출을 원천 차단하여 기업내 기술 및 노하우 유출에 따른 재정적 손실을 보호하는 솔루션으로 2007 년 5월에 출시되어 현재 콜센타를 담당하고 있다.

이에 2007년 상반기부터 국가정보원 USB메모리 등 보조기억매체 보안관리 지침에 의거한 DefCon Secure USB(보안USB 솔루션)를 개발, 2008년 4월에는 국정원 보안적합성 검증을 획득했다. DefCon Secure USB는 지 침의 필수 기능인 사용자 식별인증, 데이터 암호화, 임의복제 방지, 분실시 데이터 삭제 이외에도 데이터 이동시 파일원본 저장지원, 외부에서의 데이터 이동시 로그 모니터링, 국정원 리포팅 웹에서의 완벽자동 지원 등의 관리자 편리성의 추가기능도 함께 제공한다. 그동안 국내 PC보안 시장을 주도해 온 업체로서 기업시장에서 높은 시장 점유 율로 다년간의 경험과 노하우를 기반으로 보안USB 시장에서도 많은 레퍼런스를 확보해 기업시장에서 오랫동안 안 정성이 검증된 제품으로 고객서비스를 최우선으로 고객사에 최선의 서비스를 제공할 방침이다.

www.saferzone.com / 02-525-1410



국가정보원
보안적합성 검증필

국가정보원 보안적합성 검증필

DefConTM

Secure USB

국가정보원

보안관리지침에 따른

가장 편/리/한 솔루션



LG 그룹



국세청



병무청



(구)정보통신부
(현)지식경제부

실제크기 : 480mm × 180mm



|주 세이퍼존

[서울본사] 서울시 강남구 삼성동 109-18번지 경희빌딩 2층
[대전지사] 대전광역시 서구 둔산동 1457 둔산현대아파트 13층

고객지원센터 : 1577-3110

TEL : 02.525.1410

FAX : 02.525.1411

[http:// www.saferzone.com](http://www.saferzone.com)



국가정보원
보안적합성 검증필



한국정보통신기술협회
GS인증



중소기업청
벤처기업인증



기술신용보증기금
우량기술기업선정



한국산업기술진흥협회
연구소인증

엔트랙커 NTRACKER USB Enterprise



NTRACKER USB Enterprise는 USB를 이용한 내부자의 정보 유출을 사전에 방지하며 분실·도난 시 추적 회수가 가능하고 원격 삭제 및 메시지 전송 기능을 가진 이동식 저장매체 정보 보안 통제관리 시스템이다. 엔트랙커USB 전용 서버 프로그램과 각 PC에 인스톨하는 에이전트 프로그램인 RSC, 엔트랙커 보안USB메모리로 구성된다.

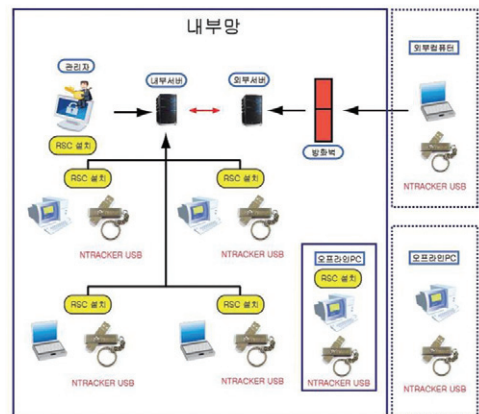
제품의 특징을 살펴보면 기본적으로 엔트랙커 USB는 내부자 정보유출 방지를 위해 서버의 통제를 받는 내부 IP대역에서만 USB를 사용하도록 하고 외부에서는 아예 사용이 불가능하도록 설계 되어 있다.

물론 관리자가 승인을 한 경우에는 외부에서도 별도의 프로그램이나 에이전트의 설치 없이 편리하게 사용 할 수 있고 이 경우에도 관리자에 의해 통제가 되기 때문에 USB 본연의 기능을 충실히 살리면서도 내부자 정보유출 방지가 확실하게 된다는 점이 큰 특징 중의 하나다.

로그 정보로 사용시 추적 기능 작동

또 서버로 로그정보를 보내는 보안프로그램 기능이 USB자체에 임베디드 되어 있으며 이 프로그램의 효율성에 대해서는 삼성전자노트북 SENS의 전 모델 탑재로 타사와 비교해서 시장에서 충분히 검증 받았다는 점이 특징이다. 즉 모든 보안

■ 시스템 구성도





USB 접속 기록이 실시간으로 서버로 전송되며 오프라인일 경우에는 일단 USB에 접속기록을 유지한 후 온라인 될 때 서버로 전송하도록 설계 되어 언제 어디서 사용하든지 추적 기능이 작동 된다.

해의 사용 접속 기록도 100% 전송된다는 것이 특징이다. 간혹 관리 서버의 이전이나 유지보수를 위해 서버 작동을 멈출 경우에도 개별 보안

USB들은 정상 작동하여 업무의 연속성을 제공하며 보안을 유지시킨다.

요즘 들어 한참 강조 되고 있는 주기적인 비밀번호 변경 문제에 있어서도 엔트랙커 보안USB시스템은 원격 메시지 송신 기능을 이용하여 사용자에게 비밀번호 변경을 수시로 알려 주며 강제 할 수도 있어 보안 관리자의 시름을 덜어 주고 있다. 또한 자료 유출과 더불어 자료유실에도 상당한 신경을 쓴 흔적이 보인다.

일단 엔트랙커에서는 그 동안 풍부한 운영경험에서 배운 점이라며 USB매체 자체의 내구성을 가장 강조하고 있다. PC와 접속 커넥터부분과 파일이 전송 중임을 알리는 LED기능이 상당히 안정적으로 작동 하며 파일 소실 가능성을 줄이고 있고 잘못 된 비밀번호 5회 입력 시에도 바로 삭제에 들어가지 않고 일단 잠금 모드를 거쳐 삭제하도록 해서 많은 시간과 노력을 들인 자료의 유실 방지에도 만전을 기하고 있다. USB 바이러스 감염 방지 기능도 당연히 들어가 있으며 국가정보원 보안적합성 지침 기준에도 완벽히 부합하는 제품이다.

NTRACKER USB Professional

분실 추적의 원천 기술이 임베디드되어 기존 USB메모리와 똑같이 사용하면서도 안전하고 강력한 보안 기능을 탑재한 획기적인 개인용 보안USB메모리다. 컴퓨터 연결시 사용 정보 로그를 등록된 이메일로 전송, 폴더 단위 암호·복호화로 안전하게 데이터 보존, 사용자 인증과 사용자 영역 보안유지 등이 제품의 주요기능이며 보안기능은 사용자가 동작을 정지하거나 삭제 불가능한 임베디드 영역에 솔루션이 탑재되어 있다.



NTRACKER Notebook

NTRACKER프로그램이 설치된 노트북이 분실, 도난 당한 후 네트워크에 연결되면 변경된 네트워크 정보를 미리 설정해 놓은 개인 이메일로 발송한다. 이 정보를 바탕으로 분실 또는 도난 당한 노트북의 위치 정보를 경찰을 통해 확인하고 추적할 수 있다. 이 제품은 컴퓨터를 훔친 혹은 습득한 사람 임의 대로 삭제할 수 없도록 만들어져 있다.

하드디스크 BIOS Setup에서 CD-ROM 부팅금지를 지정할 경우 디스크 포맷으로부터 프로그램을 보호하고 한 번 설치 후 자동으로 동작하여 사용자는 별다른 조작 없이 기능이 작동된다. 현재 삼성전자 노트북 SENS전모델에 엔트랙커 솔루션이 기본 탑재 되어 판매되고 있다. 이 외에도 중소기업을 위한 NTRACKER USB Premium 제품은 서버 없이 보안USB메모리를 사용 할 수 있어서 경제적 부담도 덜 수 있다.

| 엔트랙커

엔트랙커(임종규 대표)는 2004년 12월 설립, NTRACKER Notebook 출시와 더불어 추적 및 회수 솔루션에 대한 특허를 출원하고 기반 기술을 바탕으로 다양한 소프트웨어 출시와 함께 사업화에 힘써 왔다.

엔트랙커는 Network의 N과 Tracker의 합성어로 네트워크상의 추적 기술을 의미하는 회사의 이름처럼 전 세계가 하나의 거대한 네트워크로 연결된 21세기에 오히려 더 많이 발생하고 있는 고가 정보기기의 분실 도난과 각종 중요 정보 유출 등 허술하기 짝이 없는 보안현실을 개선하고자 도난 분실 시 회수 가능성 높이는 추적 기술과 정보보호 솔루션을 개발하여 왔다.

장기적으로는 전체 모바일 기기의 분실 추적 솔루션 상용화가 목표라고 한다. 처음으로 개발되어 시중에 출시된 NTRACKER Notebook은 삼성전자 SENS노트북 전 기종에 기본사양으로 탑재 출시되어 호평을 받고 있던 최근 노트북 수요가 급증하면서 분실 도난 또한 급증해 이 솔루션에 대한 관심이 커지고 있다.

그리고 NTRACKER USB Enterprise 제품은 각 공공기관 및 연구소 등에서 이동식 저장매체들로 발생하고 있는 보안의 취약성 등을 미리 파악하고 개발된 것으로 국가정보원의 지침이 있기 1년여 전부터 상용화에 성공해서 이미 시장을 선점한 효과를 톡톡히 누리며 막 태동기에 있는 보안USB 시장에서 분실 추적의 원천기술을 바탕으로 확고 부동의 업계 1위를 고수하고 있다. 또한 국가정보원 보안적합성 인증을 획득함으로써 명실공히 보안USB 전문 기업으로의 위상을 인정받았다.

아직 미공개인 Mobile NTRACKER 상용화라는 비장의 카드를 가지고 미래 IT환경구현, 최고의 보안 기술 개발, 고객과의 공동 이익 추구 달성을 목표로 엔트랙커는 인간과 자연 그리고 과학이 조화롭게 어울리는 세계를 꿈꾸며 항상 새로운 정보를 적극적으로 받아들이고 인간의 이로움을 먼저 생각하는 기업으로 기억되기 위해 기술정진에 최선을 다하고 있다.

www.ntracker.net / 1544-3773

국가정보원
보안적합성
검증 필

국내 최초 보안USB 상용화

풍부한 운영 노하우 | 시스템 안정화 시간 최소화 | 기존 보안 환경에 유연한 대응

NTRAKCER USB Enterprise

압도적인 상용 사이트로 평가받고
합리적 도입 가격으로 보답합니다.

내부자 정보 유출 더 이상 없습니다!!



엔트랙커(주)

서울특별시 구로구 구로동 26번지 신도림포스빌 916호

고객지원센터 : 1544-3773 Tel : 02-860-5767

info@ntracker.net www.ntracker.net

Real Tracking
High Security

효율성과 편의성에서 최적화된 솔루션

비젯 SafeUSB



'SafeUSB'는 국가정보원 지침에 맞춰 개발되었으며 백신, 스마트카드 등 다양한 기능을 탑재, 고객의 요구조건에 가장 적합한 솔루션이 될 수 있도록 설계됐다.

SafeUSB는 3계층(관리/정책 시스템, PC Agent, SafeUSB)로 구성되어 있으며 업무 효율성 및 편의성 측면에서 가장 적합한 운영 구조를 제공하고 있다. 현재 사용되고 있는 USB는 정보의 저장 및 복사, 이동이 자유로우며 가격하락으로 인해 개인당 다수의 USB메모리를 갖고 있는 경우가 많다. USB 용량도 기존의 128MB, 256MB에서 1GB, 2GB메모리 등으로 용량이 증가되고 있으며 최대 16GB까지 사용이 가능해졌다.

이렇듯 USB메모리의 활용도가 높아짐에 따라 개인정보는 물론 기업정보, 기술정보 등 국가경쟁력 차원에서 중요한 정보에 대한 접근이 용이해지고 저장, 복사, 이동이 다양해져 경쟁사 혹은 경쟁국가에 중요정보 유출로 인한 피해사례가 증가하고 있다.

백신기능과 스마트카드 기능 추가

SafeUSB는 사용자 식별·인증 기능, 지정데이터 암호·복호화 기능, 저장된 자료의 임의 복제방지 기능, 분실 시 저장데이터의 보호를 위한 삭제 기능 등 국가정보원 지침에서 요구하는 4가지 필수 기능을 보유하고 있다. 이를 통해 중요 정보 유출방지를 사전에 차단할 수 있으며 한층 강력한 기업 경쟁력을 창출할 수 있는 기반을 제공하고 있다. 또한 SafeUSB는 경쟁우위와 타사 제품과의 차별성을 위하여 백신(바이러스 방역)기능과 가상 스마트카드 기능을 부가기능으로 제공하고 있다.

SafeUSB에서 제공하는 바이러스 방역시스템은 휴대형 바이러스 백신으로써 USB메모리의 연결만으로 바이러스 감염으로부터 사용자의 데이터를 보호하는 기술이다. 휴대형 바이러스 백신은 탑재된 USB메모리는 물론 연결된 PC 전체에 대해서 실시간 감시는 물론 바이러스 검사, 치료 및 자동업데



이트 기능까지 제공한다. 또한 SafeUSB는 공인인증서를 관리하기 위한 별도의 보안구조를 보유하고 있다. 이는 USB메모리기반의 가상 스마트카드 시스템으로써 별도의 스마트카드나 리더기의 연결 없이 SafeUSB의 연결만으로 스마트카드의 보안기술을 바탕으로 공인인증서를 관리하는 기술이다. 비췌은 이 기능들에 대한 원천기술을 확보하고 상용화시켰으며 이미 국내 특허 등록은 완료하고 PCT 국제특허 출원과 미국 및 일본 국제특허도 출원했다. 따라서 SafeUSB를 통해 정보유출방지는 물론 바이러스 감염피해 방지와 강력한 공인인증서 관리구조를 제공함으로써 중요 정보에 대한 보안을 한층 강화했다.

특히 타 경쟁사와는 달리 PKI 등 인증분야 개발 시작으로 사용자 인증 및 식별에 대한 상당한 개발 경험과 구축경험을 기반으로 보안성과 편의성을 극대화한 것이 장점이다. 이 회사는 국내 KT와 일본 NTT 도코모 커뮤니케이션 등의 대형 업체와의 협력을 통해 인증 및 보안 시스템을 개발·공급했다. 아울러 인사DB, SSO, 그룹웨어, PMS, PC보안, 미디어보안 등 타 시스템과의 연동이 용이해 업무 정의에 따라 시스템을 확장하거나 독립적으로 활용할 수 있도록 했으며 USB메모리 기반 시스템 개발 및 애플리케이션 기능의 탑재로 효율적인 솔루션으로 인정받고 있다.

SafeUSB의 주요 특징

● 인증 및 식별

장치고유정보, 장치암호, 사용자암호 등 3단계 인증 체계를 적용하여 분실 및 도난으로 인한 사용자

의 정보 유출 또는 악의적인 의도로 획득한 경우에도 등록된 사용자가 아니라면 인증 시스템을 통과 해서 사용자 식별 후 권한을 확보하는 것이 불가하다.

● 보안성

Volume 단위의 전체 암호·복호화와 사용자 선택에 의한 지정파일 암호화로 사용자 환경변화를 최소화하고 악의적인 정보유출을 원천적으로 차단할 수 있으며 사용자 PC로의 데이터 이동 시 보안이 유지된 상태를 유지할 수 있다.

● 사용자 편의성

일반적으로 사용하는 웹사이트와 동일한 형태를 유지하고 있으므로 사용자 계정 정보를 통해 손쉽게 접근이 가능하며 필요한 등급의 보안USB 신청을 통해 승인 및 배포 단계를 거쳐 사용할 수 있다. 분실 시에도 온라인 분실 접수를 통해 장치에 대한 차단 및 원격 파괴가 용이하다.

● Value-added feature

백신기능을 USB저장매체에 탑재함으로 저장매체의 보호뿐 아니라, 사용하는 PC까지도 바이러스로부터 보호 체계를 구현했다. 또 스마트카드 기능은 USB저장장치를 이용해 별도 장치 없이 스마트카드 수준의 보안을 제공해 안전성 높은 공인인증서 관리 체계를 제공한다.

| 비젯

보안USB 개발 전문업체인 비젯(장건 대표)은 지난 2003년 3월에 설립, 이후 2004년에 법인 체제로 전환하고 전문 개발업체로의 위상을 확장해 나가고 있다. 이 기업은 국정원이 지난해 1월 발표한 'USB 등 보조기억저장매체 관리 지침'에 부합하는 시스템인 'SafeUSB'와 USB 기반 PKI기반 보안 및 바이러스 백신, 스마트카드 시스템을 개발하고 국내 시장은 물론 대만, 프랑스, 일본 등 글로벌 시장에 진출해서 괄목할만한 성장을 하고 있다.

특히 USB메모리를 근간으로 하고 있으며 다양한 메모리 기반에서 보안 및 인증 솔루션을 개발하고 있다. 실제로 스마트카드 기반 사용자 인증 및 PC 보안 시스템, USB Drive 기반 사용자 인증 및 통합보안 시스템, USB Drive 기반 Dynamic loading Virus Vaccine, 중앙제어식 PC 방화벽, 중앙제어식 사용자 인증시스템 기반 PC 보안시스템 등을 통해 시장 공략을 본격화하고 있다.

지난 4년 동안 비젯은 특화된 솔루션과 핵심 역량을 갖춘 아이템을 개발하고 상품화하고 있다. 이와 함께 고객들의 요구사항에 부합하는 개발 아웃소싱 프로젝트도 다수 진행하고 있다. 현재 핵심 제품에 대한 특허 확보 및 신규 시장 발굴과 진입에 나서고 있으며 전 세계 시장을 대상으로 한 솔루션 개발에 박차를 가하고 있다.

비젯은 '개발 완료 이후 시장 공략'이라는 원칙을 철저히 지켜 나가고 있다. 이에 따라 개발 중인 제품에 대해서 영업을 시작하는 형태가 아닌 제품 개발 완료 이후 시장 공략을 해나감으로써 고객의 요구에 가장 부합하는 솔루션을 제공하는데 최선을 다하고 있다. 올해를 개발 전문 보안업체로서의 위상을 다지는 동시에 공공기관을 중심으로 의무 도입되는 보안USB 시장에서 SafeUSB의 우수성을 통해 리딩 기업의 위상을 확보하는데 주력할 방침이다.

www.bizet.co.kr / 02-380-3377

내부정보 유출이 걱정되십니까?

엄격한 보안관리 철학과 풍부한 기술개발경험으로 자신있게 선보입니다.



※ 제조사의 사양에 의해 제품디자인은 변경될 수 있습니다.

USB메모리기반 정보유출방지시스템
SafeUSB

※ 국가정보원 보안USB관리지침 충족

- 2007년 1월1일 국가정보원의 중앙행정기관 지방자치단체 및 각급기관에 대한 "USB등 보조기억매체 보안관리지침" 발표
- 2008년 4월1일부터 해당기관은 보안관리지침에 따른 기능을 포함한 보안USB메모리만을 사용하여 함

검증된 기술, 풍부한 국내외 개발 경험!

인정받는 기업, 주목받는 기술!

금융정보보안 / 삼성증권, 한화증권, 농협 등

삼성증권 : 이동식장치 기반의 휴대형 백신 및 사용자 인증 온라인 증권거래시스템 공급
한화증권 : 이동식 장치기반의 온라인증권거래 시스템 공급
농협 : Flash 메모리 기반 사용자인증시스템 공급

공공정보보안 / 근로복지공단, 토지개발공사, 국방연구원 등

근로복지공단 : 보안성향화사업 사용자인증시스템 공급
토지개발공사 : 키보드 해킹방지 시스템 공급
국방연구원 : 스마트카드 기반 사용자인증시스템 공급

의료정보보안 / 서울대병원, 국군병원, 동국대 한방병원 등

서울대병원 : 의료정보시스템용 전자서명 장치 공급
서울대분당병원 : 의료정보시스템용 사용자인증장치 공급
국군병원 : 의료정보시스템용 사용자인증장치 공급
동국대 한방병원 : 의료정보시스템용 사용자인증장치 공급

해외개발&공급 / 미국, 일본, 아시아, 유럽, 남미, 아프리카 등

미 국 Fingersystem Inc. : USB메모리백신 공급계약 체결, PC Club USB 메모리백신 공급
일 본 Intelligent Wave Inc. : 보안USB메모리 공급계약 체결,
NTT Communication 공식제품 등록
독 일 Conard International GmbH사 : USB메모리 수출
프랑스 Paris SUD사 : USB메모리 백신 수출
브라질 SUN S/A사 : 보안USB 메모리 공급
핀란드 Lyco Oy사 : Guardians for SmartDrive 공급
남아공 Titatrad Electric & Electronics : 지능형 USB메모리 공급
대 만 Opiron : USB메모리백신 및 보안USB공급
싱가폴 MI ASSEMBLY PTE LTD. 외 : USB메모리백신 및 보안USB공급

인증



중소기업청
벤처기업

중소기업청
수출유망중소기업

중소기업청
기술혁신형 중소기업

중소기업청
기술혁신형 중소기업

특허



특허 제 10-0645604호 악성코드 및 바이러스 치료시스템 및 치료방법

특허 제 10-0713128호 바이러스 방역 장치 및 시스템

특허 제 10-0720374호 스마트유아보호장치 및 그를 이용한 소프트웨어 스마트카드 시스템 및 서비스제공방법

특허 제 10-0753641호 휴대형 저장장치를 이용한 온라인 증권거래 장치

WINNER



TECH TEN 2005 WINNER
(USA)

미래를 함께 할 인재를 찾습니다

자세한 내용은 홈페이지를 참고하십시오

www.bizet.co.kr

모/집/분/야 : 웹프로그래머(ASP)
응용프로그래머
웹디자이너



강력한 보안 기능으로 다양한 활용

코디아 Secure-i



코디아의 Secure 시리즈의 CD 및 USB는 강력한 보안성과 함께 다양한 분야에서 활용되도록 CD, USB, 서버연동 버전 등으로 구성되어 있다. 특히 CD의 경우는 일본 리코사에서 개발 생산된 것으로서 100년 이상의 보존력과 CD 한 면에 CD-ROM과 CD-R로 구성되어 있는 세계에 유일한 하이브리드 CD로서 강력한 보안력을 갖고 있다.

Secure-i CD

기존의 비밀번호를 설정하는 수준의 보안USB는 개발되어 있으나 사용자가 저장하는 파일을 USB에서 복제방지 할 수 있는 기능이 적용된 사례는 'Secure-i'가 처음이다. 또한 보안성과 더불어 편리성도 매우 강화된 것이 장점이다. 자체 뷰어를 내장하고 있어서 아래한글, 파워포인트나 엑셀, 훈민정음, PDF 등등의 해당 문서 프로그램이 PC에 설치되어 있지 않아도 복제방지된 문서의 열람이 가능하도록 설계됐다. 이 보안 멀티뷰어는 출장이나 외부기업 방문시 자료 열람에 아주 편리하다. 또한 저장되는 모든 파일에 대해 자동으로 압축·암호화한다.

보안 기능으로는 USB에 비밀번호 설정, 저장 파일의 복사·인쇄·캡처 방지, 저장되는 데이터의 자동 암호화, 키보드 통제, Temp File 통제 기능이다. 전용뷰어 지원파일은 MS Office, PDF, Text File, Image File, 아래한글, 훈민정음, MPEG1 VIDEO·AUDIO 등이다.

Secure-i USB

타사 제품의 경우 USB 구동, 압·복호화, 관리 애플리케이션이 서버에 탑재되어 있어서 서버와 연결되지 않을 경우는 USB가 제 기능을 발휘하지 못한다. 그러나 코디아 Secure-i는 서버연동의 모든 관리기능이 가능하며 이와 동시에 중요한 애플리케이션이 USB 자체에 탑재되어 있어서 USB와 서버



가 연동될 때 발생 가능한 해킹으로부터 피해를 최소화 하면서 서버와 연동되지 않는 오프라인에서도 강력한 기능을 발휘할 수 있다는 것이 특징이다.

또 데이터의 장기 보관, 타인에게 데이터를 전달할 경우, 서버연동 보안USB와 똑같은 기능을 하는 CD(데이터 보존력 100년 이상)를 보유하고 있어 보안CD가 USB보다 저렴하게 활용될 수 있다.

국정원의 보조기억매체 보안관리지침에 따른 기능 이외에도 타 PC에서 열어본 파일이 임시파일(Tempfile)에 데이터가 남지 않고 데이터가 저장된 USB를 패스워드와 함께 상대방에게 전달해도 데이터를 열어볼 수만 있고 인쇄, PC에 Copy, 화면캡처 등을 방지할 수 있다.

USB에 자체뷰어가 탑재되어 있어 흔히 사용되고 있는 프로그램은 PC의 프로그램에 의존하지 않고 열람할 수가 있어 해외 출장 등 뷰어가 없는 곳에서도 열람이 가능하다. Secure-i의 기능은 모두 같다. 쓰기 지우기가 가능하며 용량은 1, 2, 4G 등 자유롭게 선택할 수 있다.

Secure-NC(서버 버전)

Secure-i의 기능에 서버와 연동함으로써 기존의 Secure-i의 기능 외에 USB 사용 등록 및 관리, USB 사용자 관리 및 통제, USB 분실·도난시 추적 관리, 데이터 유효기간 설정, 불법 유출 방지·삭제 등 관리의 기능이 있다.



Secure-CAD CD

Secure-CAD는 설계도면 전용 보안 CD로서 CD내에 CAD관련 자체 뷰어를 내장하고 있어서 CAD 전용 지원파일들이 해당 문서 프로그램이 PC에 설치되어있지 않아도 복제 방지된 문서의 열람이 가능하도록 설계됐다. 복잡하고 다양한 CAD관련 데이터를 안전하게 이동, 보관할 수 있으며 자체 CAD뷰어로 수납된 데이터를 자유롭게 볼 수 있다.

보안 기능으로 USB에 비밀번호 설정, 저장 파일의 복사·인쇄·캡처 방지, 저장되는 데이터의 자동 암호화, 키보드 통제, Temp File 통제 기능 등이 있다. CAD전용 지원파일은 dxf, dwg, plt, hgl, rtl, hg, plo, hp, hp1, hp2, hpg, hpgl, hpgl2, gl2, prn, spl, svg, cgm, gif, jpg, jpeg, bmp, emf, wmf, ico, png, dib, pbm, pcx, ghw, ppm, tif 등이다.

Secure-CAD USB

Secure-i의 기능은 모두 같으며 쓰기 지우기가 가능하다. 용량은 1, 2, 4G등 자유롭게 선택할 수 있다.

Secure-CADi USB

Secure-CAD와 Secure-i의 기능을 동시에 넣음으로서 CAD 도면과 일반 문서를 동시에 열어볼 수 있는 뷰어를 탑재한 보안USB다. 상기의 전용뷰어 지원파일과 CAD전용 지원파일을 모두 지원하는 제품이다.

| 코디아

코디아(고병수 대표)는 2003년 일본의 리코사와 하이브리드 CD 공동개발, 공동판매계약을 맺고 Security CDR이라는 제품을 국내 및 해외에 판매를 추진했다. 지금까지 Hybrid CD내에서 외부 프로그램 지원 없이 독자적으로 기능 가능한 압축암호화 솔루션 및 복호화 솔루션의 개발과 Multi-Media, MS Office, Image, PDF, 한글 등 다중 포맷 지원 가능한 전용 뷰어 및 컨트롤 박스 등을 개발해왔다. 이 외에도 포토샵의 편집 기능까지 구현 가능한 전자앨범 솔루션과 Source Multi Use가 가능한 실시간 매체 제작 시스템 등을 개발했다. CD의 강력한 보안력으로 다양한 분야에서 콘텐츠를 보호를 필요로 하는 곳에 활용되어 왔으며 정부, 공공기관, 대기업 및 연구소 등에서의 정보유출방지에 큰 역할을 해왔다. 코디아는 USB 및 서버연동버전의 출시로 말단 디바이스의 정보보호에 더욱 기여하게 될 것으로 전망하고 있다.

보안USB Secure 시리즈는 CD보안에서 출발하여 약 7년간 한국과 해외에서 판매되어 보안성과 실용성에 대해 입증되어 왔고 그동안 고객의 다양한 요구에 대응해서 버전 업이 되어왔기에 고객의 니즈를 정확하게 파악하고 제품화했다고 볼 수 있다.

차별화 기능으로서 일반적인 제품의 경우 USB 구동, 암호화, 관리 어플리케이션이 서버에 탑재되어 있어서 서버와 연결되지 않을 경우는 USB가 제 기능을 발휘하지 못하지만 코디아의 제품의 경우는 서버연동의 모든 관리기능도 가능함과 동시에 중요한 어플리케이션이 USB자체에 탑재되어 있어서 USB와 서버가 연동될 때 발생 가능한 해킹으로부터 피해를 최소화 하면서 서버와 연동되지 않는 오프라인에서도 강력한 기능을 발휘할 수 있다는 것이 특징이다. 또한 데이터의 장기 보관시 또는 타인에게 데이터를 전달할 경우 서버연동 보안USB와 똑같은 기능을 하는 CD(데이터 보존력 100년 이상)를 보유하고 있어 보안 CD가 USB보다 데이터의 장기보관용으로 저렴하게 활용될 수 있다.

www.kodia.co.kr / 02-568-5744



USB · CD 보안의 최강자!!

강력한 보안성과 더불어 사용자의 편리성을 갖춘 신개념의 저장매체!!



◎ 코디아의 Secure Series

Secure-i : 문서, 동영상, 이미지, 음악 전용(CD, USB)

Secure-CAD : 캐드파일 전용(CD, USB)

Secure-CADi : 캐드파일, 문서, 동영상, 이미지, 음악전용(CD, USB)

Secure-NC(network Control) : 국가정보원 보안관리지침에 최적화된 솔루션

◎ 코디아 Secure Series의 특징

저장된 문서 및 각종 데이터 등의 복사, 인쇄, 캡처를 방지를 선택할 수 있고, 열람시 Temp파일을 남기지 않기 때문에 당신의 소중한 정보를 안전하게 지켜줍니다. 각종 뷰어의 탑재로 해당문서 프로그램이 PC에 없어도 문서 열람이 가능합니다.

DIGITAL COMMUNICATION

KODIA

(주)코디아
www.kodia.co.kr

서울시 송파구 방이동 22번지 대우유토피아 1505호
TEL : 02) 568-5744, FAX : 02) 568-5895
E-mail : cowboy@kodia.co.kr

고객의 요구에 따른 경제적 USB관리 솔루션

솔루션어소시에이트 IGM(Inner Guard Master)-Public



솔루션어소시에이트의 IGM-Public은 국가정보원의 'USB 등 보조기억매체 보안관리지침'을 반영하고 지침의 효율적 운영 및 비용절감을 가능케 하는 공공기관용 IGM 버전으로 제품기획 단계부터 내부자에 의한 외부로의 정보유출방지라는 보안 목표를 명확히 설정하고 그에 상응하는 전문화된 통합솔루션을 컴포넌트별로 개발해 차별화된 기술을 구현했다는 것이 특징이다.

특히 보안의 무결성 지향 Architecture를 채용해 외부로부터의 해킹에 의한 정보유출방지에서 출발한 여타 대다수의 유사 솔루션이 파일 시스템 레벨에서의 매체제어 아키텍처를 채용함으로써 FDD, CD-ROM, 외부 Disk(USB)에 한정하여(CD-ROM의 경우는 Image Data의 차단도 불가) 제어를 할 수 있는 반면에 이 회사의 솔루션들은 드라이버 레벨에서의 매체제어 아키텍처를 채용함으로써 FDD, CD-ROM, USB는 물론, IEEE1394, SCSI, PCMCIA, Net-Disk, 적외선 Port, Serial, Parallel 등 PC에 접속이 가능한 모든 Device를 완벽히 제어하는 기능을 구현했다는 것이 장점이다. 또 안전모드에서의 정상동작, 클라이언트 에이전트에 대한 사용자의 임의 삭제나 정지 불가조치, 윈도우 복원 방지조치 기능 등 제품 자체의 취약점 위협요인을 완벽히 제거했다.

이 외에도 이 회사는 하드웨어 비용 최소화 지향 아키텍처를 채용해 가능한 한 소프트웨어적으로 해결하는 접근방식을 채용함으로써 고객의 솔루션도입 예산 절감에 크게 기여를 하고 있다는 것이 장점이다. 아울러 통합화 지향 아키텍처를 채용해 선 통합화 구성 설계, 후 컴포넌트별 제품개발 방식을 채용함으로써 고객의 여건상 순차 도입 시에도 One-Console, One-Agent체계로 시스템을 운영할 수 있다는 것도 특징이다.

내부정보 유출방지시스템 기반의 솔루션

솔루션어소시에이트의 IGM-Public은 고객의 입장에서 개발된 경제적인 USB관리 솔루션으로 고객

이 기존에 보유하고 있는 USB에 대해서도 국가정보원의 USB 등 보조기억매체 보안관리지침의 4가지 필수기능을 구현함으로써 보안USB는 필수가 아니라 고객의 사정에 따라 선택할 수 있다. 예를 들어 기밀용 또는 일반 자료용은 IGM-USB+(보안USB)를 구입하고 개인소지가 허용된 인증서용 USB는 기존에 보유한 USB를 그대로 사용할 수 있는 등의 선택이 가능하다.

이 제품은 처음부터 내부정보 유출방지시스템 기반의 솔루션이다. 보안USB를 구입했다고 해서 보조기억매체에 대한 보안의 무결성이 보장되는 것은 아니다. 최근 들어 USB의 보급이 급속히 확산되어 사용이 보편화 된 것은 사실이지만 USB도 단지 보조기억매체 중 하나이며 따라서 여타 모든 보조기억매체의 사용도 완벽히 통제할 수 있어야 내부정보유출을 방지할 수 있다.

IGM-Public은 이미 일본 및 국내 시장에 판매 중에 있는 기업용 내부정보유출방지 전문 솔루션인 IGM을 공공기관에 맞게 업그레이드한 행정정보유출방지 솔루션이다. 아울러 행정정보 유출방지에 필요한 모든 기능이 이미 만들어진 솔루션이다.

프린터 출력자료의 Water Marking 기능을 이용하면 인쇄자료의 외부유출 시 추적관리가 용이하며 노트북의 반·출입관리 및 외부통제 기능을 이용하면 노트북을 통한 자료유출도 방지하고 노트북의 반·출입 현황을 쉽게 파악할 수 있다.

또한 네트워크 제어 옵션기능을 구입하면 인터넷을 통한 외부로의 정보유출도 사전에 통제할 수 있다는 점이 이 제품의 특징이다.

IGM-Public의 주요 특징

● 관리 및 USB 사용통제 기능

조직 및 사용자관리, 부서별 관리책임자의 권한설정관리, PC 자산현황관리 (H/W 및 S/W) 및 클라이언트 에이전트(Agent) 설치현황 및 보조기억매체 현황 관리가 가능하다.

또 보안USB(IGM-USB+)는 물론, 보유하고 있는 일반USB도 국가정보원의 USB 등 보조기억매체 보안관리지침에 따른 식별/인증, 지정 데이터의 암호화, 저장자료의 임의 복제방지 및 분실시 저장데이터 보호 기능이 있다.

이 외에도 USB 사용등록, USB 사용 PC 제한, 조직 내 또는 조직간 USB 저장자료 수합 기능, USB 일시 점검, 특정 지정 파일의 USB 저장금지, 지정횟수 이상 인증실패시 저장데이터 삭제 및 잠금, USB 반출시 기한설정, 반출정책을 통한 외부에서의 USB 사용통제, 오프라인에서의 USB 식별·인증, USB 불용매체관리, USB 출력 데이터의 해킹 감시 기능 등을 추가했다.

● 타 보조기억매체 사용통제 기능

개인별·그룹별·조직별 또는 PC별 구분하여 정책적용, 모든 보조기억매체의 통제(FDD, CD-ROM, IEEE1394, Serial, Parallel, IRDA, Net-Disk, SCSI, 와이브로, 블루투스 등) 및 읽기만 허용, 쓰기 허용, 차단 등으로 세분화했다.

그리고 프린터 사용통제 및 인쇄물 추적관리 기능을 추가해 개인별·그룹별·조직별 또는 PC별로 구분하여 정책적용과 Local·Network 프린터 사용통제 및 인쇄물의 워터마킹 기능과 노트북 반출

신청 및 승인, 반출정책을 통한 외부에서 보조기억매체 사용통제, 노트북 반입신고, 노트북 반·출입 현황관리 기능 등이 있다.

● 감사·보고서 기능

접속일시, 접속자명, 접속시스템 현황관리, 모든 보조기억매체로의 출력 기록관리, USB메모리의 원본 File의 PC(폴더 숨김) 또는 서버저장, USB메모리 인증실패시 실패기록관리, USB메모리의 반·출입 파일 목록 비교·관리 기능과 보안관리지침에 명시된 관리대장 양식의 확인 및 출력이 가능하다.

● Agent 보호 기능

프로세스 정지 또는 서비스 삭제 방지, 안전모드에서의 매체제어, 윈도우 복구를 통제하고 삭제를 방지 할 수 있으며 네트워크 사용통제 기능을 추가해 개인별·그룹별·조직별 또는 PC별 구분하여 정책적용, SMTP Mail 및 첨부 File 전송통제, HTTP Mail 및 첨부 File 전송통제, MSN-Messenger 및 첨부 File 전송통제, FTP 전송통제, HTTPS 전송통제, Web-Site 접근제한, Network 공유 Folder 접근제한, Packet Size 제한 전송통제가 가능하다.

| 솔루션어스시어이트

솔루션어스시어이트(전응희 대표)는 내부정보유출방지 및 IT 인프라관리 Package S/W 개발 전문회사로써 지난 2003년도에 회사 설립과 동시에 일본 후지전기IT솔루션 주식회사와 제품개발 및 판매에 관한 전략적 파트너십을 체결하고 일본시장을 집중 공략해 왔다. 지난 2006년 하반기부터는 국내 시장에도 진출해 제품을 판매해 오고 있다. 이 회사는 제품기획단계에서 '내부자에 의한 외부로의 내부정보유출방지'라는 보안목표를 명확히 설정하고 그에 상응하는 전문화된 통합솔루션을 컴포넌트 별로 개발해 왔다. 이는 애당초 '외부에서 내부로의 해킹방지'라는 목표로 개발된 제품을 트렌드에 따라 판매를 목적으로 일부 매체제어기능을 보완한 기존의 짜깁기식 제품과는 달리, 보안의 무결성 및 시스템 통합성 측면에서 확실히 차별화했다. 또한 글로벌 S/W 꿈의 실현을 목표로 제품 사양, 품질 및 서비스에서 고객으로부터 사랑을 받기 위해 최선을 다하고 있는 작지만 강한 기업이다. 일본에서의 제품경쟁력을 보다 강화하고 미국 시장에도 진출해 2013년에는 Package S/W 분야에서 수출 1위를 달성함으로써 명실상부하게 글로벌 S/W화를 실현을 목표로 부단한 노력을 하고 있다.

www.sa-inter.com / 031-751-8321

“현장의 소리” 로 개발된 행정정보유출방지 솔루션

@IGM-Public

국가정보원 보안적합성 검증필



매체제어 기반의 보안USB관리 솔루션 입니다. (노트북, 통신 제어 포함)

- ◆ 기존에 보유하고 계신 USB도 보안USB 처럼 사용하실 수 있습니다.
- ◆ 자매품 IGM-USB+ (보안 USB) 는 필요 수량만 구입하시면 됩니다.

제품구입문의

개발사  (주) 솔루션어소시에이트

경기도 성남시 수정구 복정동 694-5 야정빌딩 3층

TEL : 031-751-8321 FAX : 031-751-8323

수도권총판 : (주)헤음시스템 TEL : 02-2027-3325

호남권총판 : (주)모든아이티 TEL : 02-598-5002

디지털센스 Infosecure-USB



보안USB와 USB관리서버로 구성된 Infosecure-USB에는 기본 기능인 사용자인증에 의한 보안 영역으로의 로그인, 파일 저장시 암호화, USB내 저장된 파일의 임의 복제 방지, 보안USB 분실시 저장 파일의 원격 삭제 기능이 있다.

사용자 인증은 세션키에 의해 암호화로 보안이 유지되는 통합관리 서버와의 통신으로 인증절차가 수행되고 파일 암호키는 세션 기간 동안만 유효하게 하여 보안성을 강화했다. 보안 알고리즘은 국정원이 권고하는 ARIA 256비트 블록 암호화 알고리즘을 채택하고 있으며 보안USB내에 파일을 저장하면 자동으로 암호화되어 저장된다. 또 인증을 받지 않은 사용자가 보안USB로 파일을 복사하거나 보안USB내의 파일을 타 저장장치로 복제하는 것을 방지한다.

보안성 강화 · PC 사용현황 로그 관리

파일 암호키는 통합관리서버에서 보안USB를 발급할 때 유일하게 부여되며 파일을 실제로 암호화할 때 사용되는 키는 이 키와 사용자 패스워드를 결합하여 이용함으로써 암호키가 파악된 경우라도 파일을 복호화할 수 없게 해 보안성을 강화했다.

보안USB는 사용자 컴퓨터에 플러그인 되는 순간 사용자명, 컴퓨터 명 및 OS, IP주소 등의 사용자 컴퓨터 자원현황과 보안USB의 ID등 기본정보를 통합관리서버로 송신하여 사용현황에 대한 로그를 저장하고 통합관리서버가 사고 USB여부를 미리 판단하여 분실 USB의 경우 사용자의 로그인 시도와 관계없이 USB내에 저장된 파일을 자동으로 삭제하는 등의 보안 기능을 수행할 수 있다.

또 사전식 공격에 대비하여 일정 횟수 이상의 로그인 패스워드 오류 또는 사용자 인증 오류가 발생하면 보안USB는 스스로 파일 자동삭제를 수행함으로써 타인에 의한 도용의 위험을 방지하도록 했다.

USB관리 서버는 보안USB의 구입, 등록, 사용변경, 폐기 등의 모든 관리 내용을 포함하고 있다. 보안

USB 이 외의 CD-ROM, 외장형HDD 등에 대한 보조저장장치의 등록 및 관리를 포함하고 있어 자산 관리까지 가능하다. 보안USB가 컴퓨터에 접속시 접속로그를 전송 받아 추적이 가능하며 서버와 접속되지 않은 상태에서 파일의 복사한 내용의 로그를 보관한 후 서버와 접속시 로그를 전송한다.

저장장치에 대한 구입 현황, 등록관리, 변경 이력 등을 관리하며 재물조사, 부서 변경에 따른 인수인계 등을 지원할 수 있는 기능을 포함하고 있어 관리 기능이 매우 우수하다. 이러한 내용을 DB에 저장하여 다양한 검색을 통하여 통계와 현황을 분석할 수 있으며 현황 집계, 보고서, 대장관리 등의 다양한 출력물을 제공한다. 또한 데이터는 Excel이나 WORD, PDF 파일 형태로 제공할 수 있어 필요시 보고서를 편집할 수 있어 관리가 용이하다.

Infosecure-Enterprise

또한 보안USB와 보안Agent, 그리고 통합관리서버로 구성된 정보유출방지 시스템 Infosecure-Enterprise는 보안Agent에 의해 보안USB와 미등록 보조저장장치와 구별하여 관리가 가능하다. 미등록 USB, CD-R/W, 외장형HDD 등을 이용하여 파일유출시 원천적으로 차단하고자 하는 경우에 저장장치에 제어를 설정함으로써 파일 복사를 방지하고 등록된 저장장치만 파일복사를 허용한다.

보안정책을 모니터링으로 설정하는 경우에는 파일을 복사하는 경우에 반출 및 유출 파일에 대한 로그를 생성하여 보안관리 서버에 전송함으로써 보안감사 근거를 확보할 수 있다.

정보 유출 · 반출시 로그 생성 · 관리

유출 · 반출시 생성된 로그는 보안USB와 미등록 저장장치를 구분할 수 있어 정확히 유출의 경로와 내용을 파악할 수 있다. 사용자 컴퓨터 내에 저장된 파일이 보안USB, 일반USB, CD-R/W, 외장형HDD, FDD에 반출이나 유출되는 경우에 저장장치별로 구분하여 언제, 누가, 어떤 파일을, 어디로, 복사했는지에 대한 로그를 생성함으로써 정확한 유출 근거를 관리할 수 있다.

통합관리 서버는 사용자에게 설치된 Agent에 보안정책을 설정하여 전달한다. 보안정책은 기관전체, 부서별, 개인별, 장치별로 구분하여 설정할 수 있어 기관별 보안정책을 쉽게 적용할 수 있다. 보안Agent에서 생성된 로그를 통합관리 서버에서 수신하여 유출 · 반출된 내용을 실시간으로 모니터링할 수 있으며, 로그에 대해 다양한 조건 검색이 가능하다.

제품의 주요 특징

보안USB를 포함한 CD-ROM, USB, 외장형HDD 등의 저장장치를 통한 유출방지와 e-mail, Web Mail, Web Hard, Messenger, P2P 등의 인터넷을 통한 유출방지, 프린터를 통한 유출방지에 대한 통합 유출방지 기능을 제공하고 있다.

또한 Agent방식으로 노트북, Wibro, 무선랜 등에 대한 유출방지 기능이 있다. 보안 Agent가 사용자 컴퓨터에 설치되어 운영되어 노트북 컴퓨터와 같이 사외로 반출되어 유출되거나 Wibro/HSDPA와 같이 이동통신을 통해 파일 유출시에도 보안이 가능해 보안 취약부분을 최소화 할 수 있다.

또 파일이 저장장치로 유출되는 경우에 언제, 어디에 있는 어떤 파일이 어디로 복사되었는지 로그를 생성하며 필요시 유출파일을 사본화하여 유출된 파일의 내용을 알 수 있다. 인터넷 통신을 통해 파일 전송시에는 송신자 주소, 수신자 주소, IP, 제목, 본문, 첨부파일 등에 대해 로그를 생성하고 실시간으로 모니터링 할 수 있다.

아울러 보안프로그램 설치에 따른 사용자 컴퓨터의 속도나 불편없이 사용할 수 있어야 하므로 안정적인 시스템이 필수적이다. 특히 시스템 후킹에 따른 사용자 컴퓨터의 속도저하 등의 문제가 없으며 대규모 적용 및 운영사태가 있어 안정적인 시스템 운영을 지원한다. 한편 다수의 사용자 컴퓨터를 관리하기 위해 보안정책을 설정하는데 기관별, 부서별, 개인별, 장치별로 구분하여 정책 적용이 용이하며 관리자 화면도 사용에 편리하다. 또 다양한 로그 검색 기능과 보고서용 출력물을 제공하고 있어 보안 관리자의 관리가 용이하다.

| 디지털센스

디지털센스(최주호 대표)는 2002년 1월에 정보유출방지 전문업체를 목표로 설립하였다. 정보보호 분야는 초기에 바이러스 백신에서 출발하여 네트워크 보안 분야가 성장하였지만 향후에는 정보화 시스템 구축과 축적된 데이터에 대한 보호가 필수적이며 특히 내부정보 유출에 대한 보안 요구가 커 질것으로 예상된다. 이에 따라 이 기업은 최고의 솔루션을 제공할 수 있는 전문회사로 성장을 목표로 하고 있다. 그동안 개발한 제품은 통합정보유출방지 시스템인 'Infosecure-Enterprise', 노트북 유출방지 제품인 'Infosecure-GateGuard', 보안USB관리를 위한 'Infosecure-USB', 파일보안을 위한 'infosecure-FileKeeper' 등을 출시했다. 이러한 제품은 자체 기술에 의해 개발했고 난이도가 높은 파일시스템 드라이버와 네트워크 드라이버 기술을 확보하여 가장 안정적이고 보안성이 높은 기능을 구현할 수 있게 됐다. 특히 통합유출방지시스템(Infosecure-Enterprise)은 저장장치, 인터넷, 프린터를 통한 정보유출을 통합적으로 관리할 수 있는 제품이다.

또한 파일시스템과 네트워크 드라이버를 핵심기술의 바탕으로 End Point인 사용자 컴퓨터에 대한 종합관리가 가능한 제품을 지속적으로 개발할 계획이다. 단기적으로는 보안USB를 포함하여 외장형HDD, CD-ROM/DVD등에 대한 유출방지와 통합관리가 가능한 제품을 개발하고 중기적인 목표는 정보유출방지의 한 축인 PC DRM, 다양한 자원을 관리할 수 있는 시스템관리, 비인자자의 접근을 통제하는 네트워크 통제 제품 등을 출시해 정보유출에 대한 통합관리가 가능한 제품을 개발하고 정보유출방지 전문 업체로서 성장한다는 목표를 세우고 있다.

www.digitalsense.co.kr / 02-3473-7760

InfoSecure-Enterprise

통합정보유출방지 시스템

서버나 사용자 컴퓨터에 저장된 파일이 저장장치, 인터넷, 프린터를 통하여 외부로 유출을 방지하는 시스템



유출방지 대상

저장장치 - FDD, HDD, CD/DVD, USB 등
인터넷 - 유선, 무선, 이동통신(WIBRO) 등
프린터 - 기본, 네트워크 프린터

주요기능

모니터링 - 유출로그 생성 및 실시간 모니터링
사본화 - 유출파일의 사본 저장
유출방지 - 복사금지, 전송차단, 인쇄제한
워터스탬프 - 출력정보 및 이미지 인쇄

디지털센스 제품군

InfoSecure-Enterprise(통합 유출방지) / InfoSecure-Device(저장장치 유출방지) / InfoSecure-Internet(인터넷 유출방지)
InfoSecure-USB(보안USB) / InfoSecure-GateGuard(노트북 유출방지)



Digital Security
(주)디지털센스

서울시 서초구 방배동 1001-1 KT서초지사 501호
Tel : 02-3473-7760 Fax : 02-3473-7720
E-mail : admin@digitalsense.co.kr

●Security Book



월간 정보보호 21c

최신 보안 트렌드와 심층적인 분석 기사를 통해 보안 산업을 이끌어가고 있는 월간 정보 보호 21c는 기업의 핵심 경쟁력인 '정보'를 보호하기 위한 최신·최적의 해법을 제시한다. 특히 세계적인 IT 전문지 美 Tech Target의 'Information Security' 기사를 독점 제 공함으로써 산업 전반에 걸친 해외의 최신 IT관련 이슈를 전달해 국내 IT 산업이 세계적인 추세를 놓치지 않도록 하는데 기여한다. 또한, 온라인 보안뉴스(www.boannews.com)와 연계하여 현장의 보안 관리자들이 즉각적으로 반응할 수 있도록 실질적인 도움을 주는 지침서 역할을 하며, 보안의식 제고와 의식 향상을 통해 미래지향적인 보안문화 형성에 앞 장서고 있다.



월간 시큐리티월드

월간 시큐리티월드는 일반인들이 생활 속에서 접하게 되는 개인의 신변안전과 재산보호 등 각종 보안문제를 비롯하여 기업의 재산과 정보를 보호하는 기업보안, 그리고 국가간의 산업 스파이 문제 등의 산업보안에 이르기까지 보안에 대한 모든 정보를 제공하는 보안종합 전문지이다. 국내 최고 권위를 자랑하는 보안 전문지로 국내외 최신 제품과 최근 기술동향 및 시장동향을 신속, 정확하게 전달하여 국내 보안 산업 발전에 이바지하고 있다. 또한 오프라인은 물론, 온라인(www.secuinfo.com)을 통한 양방향 커뮤니케이션으로 독자에게 한층 더 가깝게 다가가고 있다.



기업보안 관리전략(최 태 익박사)

기업경영에 있어 화두는 단연 위기관리이다. 그러나 글로벌화로 인해 기업 환경이 급변하고 있는 현실에도 불구하고 기업경영에 있어서의 위기관리에 관한 전문서적은 여전히 자연재난과 보험 산업, 위험관리에 치중해있다. 즉, 이미 기업의 가장 큰 자산인 핵심 기술이 유출되는 사고가 빈번함에도 불구하고 보안측면에서 기업자산에 대한 리스크 관리를 다룬 전문서는 찾아보기 힘든 것이 현 실정이다. 이런 시점에서 국내에서는 최초로 CPP 국제 보안관리 자격증을 취득한 최선태 박사가 대기업은 물론, 중소기업의 보안관리자뿐만 아니라 모든 직원들이 손쉽게 읽을 수 있고 실무 관리업무에 활용할 수 있는 기업보안 관리전략을 발간했다.



시큐리티 시스템 개론(안창훈 외)

보다 전문화, 체계화된 보안 시스템의 구축과 운영은 최적의 보안 시스템 선정과 활용이 전제되어야 한다. 이러한 고객의 요구를 좇아 시큐리티 시스템 개론은 '최적 보안 시스템 도입과 활용'을 중심으로 이론적 기초와 실무를 체계화, 집대성한 보안 총서이다. 특히 보안관련 기초이론에 입문하고자 하는 경보·경비·경찰유관 학과 강의로서는 물론 경비지도사 자격증 대비용 수험서, 보안장비 제조·공급업체를 비롯, 일반 기업체나 금융권, 정부공공기관 등 보안 관리자 활용서 등으로 폭넓게 필독될 수 있도록 최신 보안 시스템의 A to Z를 소개한 보안 시스템 활용 및 실무 지침서라 할 수 있다.

IV. 정보유출과 기업 보안

- 074 <Column> 잇따른 기술유출사건에 대한 단상
- 075 <Column> 보안담당자들이여, 위험을 수치화하라
- 076 <산업보안 X-파일> USB를 이용한 정보유출 사례
- 080 <특별기고> 기술보호에 대한 오해와 착각



잇따른 기술유출사건에 대한 단상

글 · 권준 월간 시큐리티월드 취재팀장(joon@infothe.com)

기술유출방지의 핵심은 결국 기업 임직원의 마음을 잡는 일이다.
그리고 이것은 기술개발 인력을 비롯한 임직원들에게
얼마나 공정한 보상체제를 제시하느냐에 달려있다.

첨단 조선기술유출 무더기 적발, PDP 기술유출시도 발생, 상하이차의 쌍용차 기술유출 의혹, 국내 반도체 업계 기술유출논란 등등.

최근 언론지상을 가득 메운 기술유출관련 사건소식들이다. 국가 차원에서의 경각심이 높아지고 기업들의 보안의식 또한 점차 향상되고 있다는 요즘 기술유출관련 사건들이 봇물 터지듯 발생하는 이유는 무엇일까? 그리고 어떻게 해야만 기술유출의 본질적 문제에 접근할 수 있을까?

최근 기술유출사건이 잇따라 발생되고 매스컴에 보도되는 이면에는 앞서 언급했듯 정부, 기업, 시민, 언론 등 사회 모든 구성원들이 기술유출에 대해 이제야 비로소 심각하게 인식하고 있다는 반증이라고 본다. 과거에는 대부분의 기술유출이 유출자만 아는 행위로, 더구나 그것이 범죄인지도 모르게 행해졌고 피해 기업들조차 쉬쉬하며 넘어가곤 했다. 그러나 관련법과 제도가 정비되고 사회구성원들의 감시망이 제대로 작동되면서 그동안 음지에서 비밀리에 행해졌던 기술유출이 하나 둘씩 포착되기 시작했다는 생각이다.

그러나 아마 우리가 발견해내지 못하고 지나쳐버린 기술유출사례는 적발된 사례보다 훨씬 더 많을 것이 자명하다. 그렇기에 지금 이 상황을 오히려 기회로 삼아야 한다. 이렇듯 이슈로 부각돼 사회 전반적인 관심이 높을 때에 지속적인 문제제기가 이루어져야만 기술유출의 본질적 문제에 보다 가깝게 접근하고 해결책에 대한 공감대를 확산시킬 수 있기 때문이다.

기술유출방지의 핵심은 결국 기업 임직원의 마음을 잡는 일이다. 그리고 이것은 기술개발 인력을 비롯한 임직원들에게 얼마나 공정한 보상체제를 제시하느냐에 달려있다. 기술유출 가능성이 있다고 감시를 강화하기에 앞서 직원들이 애사심을 갖고 업무에만 매진할 수 있도록 물질적·정신적 여건을 조성해주는 일이 선행되어야 하는 것이다. ⑬



보안담당자들이여, 위험을 수치화하라!

글 · 김용석 월간 시큐리티월드 취재기자(sw@infothe.com)

유능한 보안담당자라면 경영진을 설득하고 이해시킬 수 있어야만 한다.
이때 반드시 필요한 것은 눈에 보이지 않는 위험을
그래프나 숫자 등으로 수치화해야 한다는 것이다.

‘꿈은 높는데, 현실은 시궁창이야’라는 표현이 있다. 국내 기업체에 종사하는 보안담당자들은 기자를 만나면 항상 하는 말이다. 해외기업들에 비해 국내기업들은 보안업무에 대해 별 대수롭지 않게 생각한다는 것. 이런 현상은 국내 보안담당자들의 위상과도 연결될 수 있기 때문에 이들에게는 심각한 문제로 받아들여지고 있다. 이렇듯 보안담당자들의 꿈과 현실 사이에도 큰 괴리가 존재하고 있는 것이다.

물론 국내 기업의 환경은 선진국의 그것과는 다른 부분이 존재한다. 경제성장을 목표로 ‘속도’를 최우선시 했던 우리네 정서는 어쩌면 보안과는 맞지 않는 것이었을지 모른다. 또 그동안 지켜야 할 것보다는 남의 정보를 얻어야 하는 경우가 많았던 기업들의 입장에서도 보안은 먼 이야기일 수밖에 없었다. 하지만 이제 시대가 바뀌었고 우리가 지켜야 될 기술도 과거에 비하면 엄청나게 많아졌다. 시대가 변하면 사고도 바뀌어야 한다고 했다. 이제는 보안체계를 강화하기 위한 특단의 대책을 세워야 할 때가 된 것이다. 하지만 불행하게도 아직 과거 생각에 사로잡혀 있는 경영진들이 많다는 것은 보안체계를 강화하는데 어려움으로 작용하곤 한다.

보안체계를 강화하는 것은 보험과도 같은 것이다. 하지만 언제 일어날지 모를 위험에 대비하기 위해 당장 투자를 시행해야 하는 것은 경영진에게 있어 어려운 선택일 수밖에 없다. 그런 이유 때문에 보안체계를 적당한 수준에서 마무리하거나, 또는 아예 투자자체를 꺼려하는 경우가 발생하는 것이다. 따라서 유능한 보안담당자라면 이러한 경영진을 설득하고 이해시킬 수 있어야만 한다. 이때 반드시 필요한 것은 눈에 보이지 않는 위험을 그래프나 숫자 등으로 수치화해야 한다는 것이다. 눈에 보이지 않는 위험과 눈으로 직접 보이는 위험은 체감온도부터 다르기 때문에 경영진을 설득하는데 유용하게 쓰일 수 있다. 가령 현재 자사에서 보유하고 있는 기술의 값어치를 책정해 기술의 중요성을 이해시킨다거나 혹은 보안 시스템 투자대비 얻을 수 있는 이익을 계산해 수치로 보여주는 것이야말로 보안의 중요성을 경영진에게 인식시킬 수 있는 가장 큰 자극제가 될 수 있다.

백번의 말보다 한번의 행동이 더 중요하다는 말이 있다. 보안체계 강화가 중요한 것은 누구나 아는 사실이지만, 그것이 왜 중요한지에 대해서는 그 누구도 자세히 설명해주지 않는다. 위험을 수치화하고, 또 그것을 대비함으로 인해 얻을 수 있는 이익을 수치화하는 것이야말로 말이 아닌 행동이지 않을까. 보안담당자들이 가슴 깊이 새겨보길 바란다. ⑮

USB를 이용한 정보유출 사례

89조원

이 작년 한 해동안의 국내 기술의 해외 유출로 인한 피해액이다. 이것은 전년 대비 7배 가까이 증가한 액수다. 다음 사례들은 최근 발생한 기술유출 사례에 관한 내용이다.

Case #01

2008년 신기술 셋톱박스 빼돌린 업체 간부들 적발

디지털방송에 쓰이는 고화질 영상저장 녹화 신기술 셋톱박스를 빼돌려 중국으로 넘기려던 첨단기술 유출사범 11명이 경찰에 적발됐다. 셋톱박스(set-top box)는 디지털방송 신호를 압축한 형태로 받아 TV 등 디스플레이에 전송하는 디지털 미디어 기기로 국내 수출 규모는 1조 1천억원이며, 무엇보다 국내 업체가 전 세계 시장의 20%를 점유하고 있을 만큼 자랑스러운 IT 신기술이다.

셋톱박스 개발·판매업체 A사의 조직관리부장으로 근무하던 D씨는 기술개발팀장이던 E씨 등과 공모, 지난해 2월부터 3개월 동안 셋톱박스 관련 핵심 기술을 USB와 노트북에 몰래 담아 빼돌렸다. D씨 등은 이후 A사를 퇴사한 뒤 같은 해 5월 B사를 설립, 중국 현지 생산업체 C사에 셋톱박스 기술을 넘기려고 시도했으나 국가정보원으로부터 김씨 등의 범행에 대한 첩보를 넘겨받은 경찰이 다행스럽게도 셋톱박스 시제품이 중국에서 만들어지기 직전 이들을 검거했다.

경찰 관계자는 “이 셋톱박스 기술이 중국으로 유출됐을 경우 향후 5년간 1조 5,000억원 이상의 피해가 발생하고 국내 셋톱박스 업체는 경쟁력을 상실해 줄 도산할 위험에 처했을 것으로 분석됐다”고 말했다. 한편, 경기경찰청 외사과는 부정경쟁 방지 및 영업비밀보호법 위반 혐의로 D씨(42)를 구속하고 E씨 등 관련자 10명을 불구속 입건했다.

Case #02

2008년 자동차 핵심기술, 중국 유출 시도

국내 자동차 기업에서 근무하던 A씨는 사무실 동료들이 모두 자리를 비운 점심 식사시간을 틈타 동료의 컴퓨터에 USB메모리를 연결, 회사의 중요 데이터를 다운 받았다. 다운 받은 데이터는 B사의 25년 노하우가 그대로 축적된 자료로, 얼핏 보면 대수롭지 않은 기술일지 모르지만 자동차 업계 사이에서는 일급 기밀 중 하나에 속하는 것이었다.

다시 자신의 자리로 돌아온 그는 이메일을 통해 후배 C에게 자신이 빼낸 정보의 일부를 전달했고 후배 C는 그것을 가지고 중국의 자동차 회사와 거래를 시도했다. 곧 나머지 자료를 실수 없이 중국으로 갖고 온다는 조건 하에 이사금으로 채용해 준다는 확답을 받을 수 있었던 C는 그러나 선배 A가 국정

원의 수사망에 포착돼 결국 중국으로의 출국 직전, 공항에서 체포됐다. 메일을 통해 자료를 전달한 것이 화근이 돼 발각된 것이다.

B사의 기술이 모두 중국에 유출됐을 경우 2010년까지 중국 자동차 시장에 서만 4조 7,000억원의 시장잠식이 예상될 뿐 아니라, 중국 자동차 회사의 기술력 축적에 따른 시장잠식으로 세계시장에서는 22조 3,000억원의 매출 손실이 예상됐다. 또한 중국의



자동차관련 기술이 현재 우리와 5~7년의 기술격차를 보이고 있지만 2010년에는 1.5년 이내로 크게 줄어들 것으로 분석됐다.

이 사건은 국내 자동차 업계의 허술한 보안 시스템을 또다시 드러낸 실례로 같은 사무실 동료라 할지라도 마음대로 타인의 컴퓨터를 볼 수 있다는 것, 덧붙여 USB메모리 등과 같은 간단한 저장장치만으로도 쉽게 자료를 유출할 수 있다는 것 자체가 국내 자동차 업계의 보안 취약점을 그대로 반영한 것이라 할 수 있다.

Case #03

2008년 폐기물 처리기술 유출 시도

산업 폐기물 처리업체 A사의 전직 간부 B씨는 지난해 9월 회사를 퇴사하면서 자신의 노트북과 USB에 1GB 용량의 공정설계자료 279개를 다운받아 저장한 후 이를 고액의 연봉을 받는 조건으로 경쟁회사인 호주의 산업 폐기물 처리업체에 넘기려했다.

그러나 폐기물 재처리 공정기술 같은 첨단기술은 국가가 직접 관리하는 것으로 이 업체의 기술 또한 산업자원부가 첨단기술로 지정해 이미 특별관리하고 있었다. 따라서 경찰이 사전에 이러한 움직임을 포착할 수 있었으며, 반면 이를 알지 못한 B씨는 경찰의 신중한 조사 끝에 산업기술의 유출방지 및 보호에 관한 법률 위반혐의로 체포됐다.

B씨는 해당 기술과 관련된 기밀파일 270여개를 자신의 인터넷 웹하드에 올려놓는 것만으로 거의 모든 기술을 확보할 수 있었다. 그러나 더욱 놀라운 점은 B씨가 대범하게도 A사를 사직한 뒤에도 몇 차례 더 A사를 방문해 휴대용 USB로 또 다른 기술을 빼돌릴 수 있었다는 점이다.

이 사건에서는 특히 A사의 보안체계가 문제점으로 지적됐다. 아무리 산업자원부가 첨단기술로 지정해 특별관리를 해준다고 할지라도 기본적인 보안체계는 A업체 스스로 구축해야 마땅하다. 하지만 웹하드를 이용한 기술유출이 이뤄졌다는 점, 그리고 퇴사 후 USB를 이용한 기술유출이 이뤄졌다는 점은 어떠한 변명도 용납될 수 없는 허술한 보안체계였다고 할 수 있다.

덧붙여 퇴사 후 마음대로 회사에 출입할 수 있었던 것도 퇴직자 관리가 얼마나 엉망으로 이뤄지고 있

있는지를 여실히 보여주는 사건이었다. B씨가 유출하려 한 TSL공법 기술 개발 비용은 340억원에 불과하지만 라이선스 손실과 프로젝트 수행, 상용화, 잔재물 처리를 통한 수익 등을 감안할 경우 5년간 1조 원가량의 경제적 손해가 발생할 수 있는 것으로 알려졌다.

한편, 기술개발실장으로 근무하던 B씨는 회사에서 진행한 인사에 불만을 품고 퇴직하면서 해당 기술을 해외 경쟁사인 호주 C주식회사에 고액의 연봉을 받는 조건으로 유출키로 결심한 것으로 알려졌다.

Case #04

2008년 휴대폰 배터리기술 유출, 공항서 체포

휴대폰 배터리를 전문으로 개발·생산하던 업체 A사의 이사 B씨와 연구원 C씨가 공모해 핵심 기술을 유출하고 D사를 설립했다. 전직 A사의 이사 B씨는 회사의 전반적인 경영 노하우와 파트너 업체들과 관련된 영업 관련 리스트를, 연구원 C씨는 제품 생산 기술에 따른 기밀사항을 빼내는데 주력했다.



B씨는 직원들이 전부 퇴근한 시

간을 노려 자신의 컴퓨터에 담겨져 있는 관련 비밀문서를 USB메모리에 저장했는데 USB메모리의 용량이 부족해 더 이상 저장할 공간이 없을 경우 인터넷 웹하드에 저장하는 방법까지 서슴지 않았다. 연구원 C씨도 이와 비슷한 방법으로 자신의 연구 자료를 빼돌릴 수 있었다. 이들은 A업체가 보안 시스템이 사실상 전무하다는 점을 노려 이렇듯 대담한 방법들을 동원해 기술유출에 성공할 수 있었다. 결국 이들 두 사람은 그들이 원하는 모든 자료를 취한 후, 사직서를 제출했고 D사를 설립하기에 이르렀다.

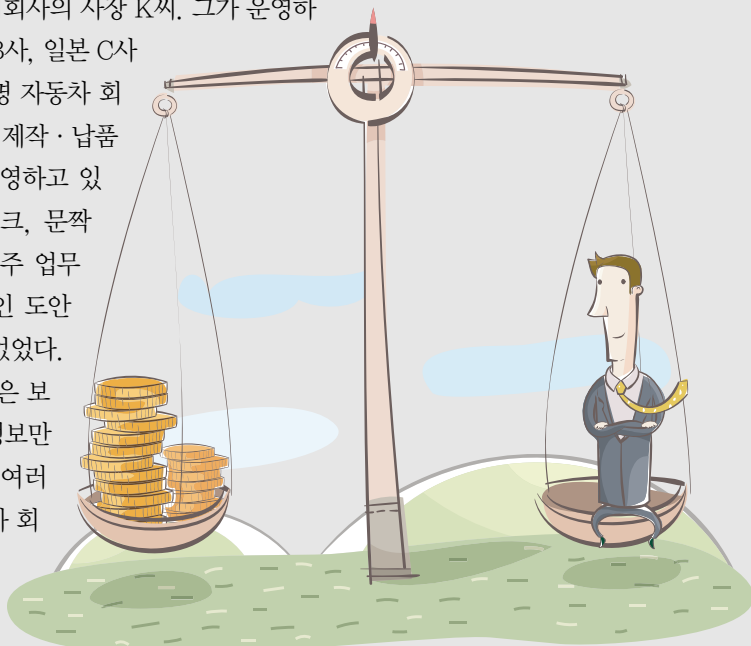
이미 기술 자료와 영업 자료가 모두 구비된 D사는 빠르게 업계에 정착할 수 있었다. 특히 그들은 A사의 기술로 만든 제품을 A업체의 협력사들에게 값싼 가격에 제의했다. 그러나 이와 같은 행각은 그리 오래가지 않았다. A사의 파트너사 중 하나가 A업체의 기술과 너무나 흡사한 D사의 휴대전화 배터리를 보고 A사에 이 사실을 알렸기 때문이다. A사는 즉각 경찰에 신고 했고 경찰은 은밀히 수사를 진행했다.

수사망이 좁혀오자 이들 두 사람은 해외로 도피를 시도했으나 공항에서 경찰에 붙잡히고 말았다. 수사결과 이들이 빼돌린 산업기밀은 A사의 연구개발비와 향후 판매 손실 등을 합쳐 3,700억원에 달한 것으로 밝혀졌다.

Case #05

2007년 자동차 금형기술 유출사건

설립한지 13년째인 자동차 금형 벤처회사의 사장 K씨. 그가 운영하고 있는 회사는 국내 A사와 미국의 B사, 일본 C사 등 이름만 들어도 알만한 국내외 유명 자동차 회사와의 계약을 통해 자동차 부품을 제작·납품하는 업무를 맡고 있었다. K씨가 운영하고 있는 업체는 자동차의 보닛이나 트렁크, 문짝 등 자동차 금형을 생산해내는 것이 주 업무였기 때문에 차량의 전체적인 디자인 도안과 같은 자료는 필수적일 수밖에 없었다. 일반적으로 대부분의 자동차 회사들은 보안을 이유로 하청 업체에는 일부 정보만을 제공해주기 마련이지만 K씨는 여러 해 동안 다져온 '신의'를 통해 자동차 회사들의 높았던 '보안장벽'을 조금씩 허물어갈 수 있었다.



그러던 중 금형기술을 유출하는 조건으로 엄청난 대가를 지불하겠다는 제의를 받게 된 K씨는 망설이던 끝에 욕심을 이기지 못하고 자사가 보유하고 있는 여러 자동차 회사들의 금형정보를 유출하기에 이르렀다. K씨는 공조가 없으면 일이 어렵다는 생각으로 핵심직원 5명을 추가로 섭외해 그들과 함께 일을 도모했다.

이들은 우선 첨단 산업기밀인 자동차 금형 설계 2D, 3D 파일이 들어있는 핵심 데이터베이스(시가 3,000억원 상당)를 내장용 하드디스크와 USB 및 보조기억 매체 등을 이용해 마치 업무상 취급하는 것처럼 가장한 후 유출행위를 벌여나갔다. 그러나 보다 완벽한 범죄를 위한 2차 작업으로 이 기술을 도용해 다른 동종 업체를 창업하는 과정이 필요했다. 이렇게 해야만 표면상으로 문제가 없는 정보유출이 가능하고 또 혹시 있을지 모를 수사망을 피할 수도 있었기 때문이다. 결국 또 다른 업체를 창업한 이들은 본격적으로 자신들이 보유한 핵심 자동차 금형기술을 해외로 빼돌리기 시작했다.

하지만 이들의 범죄 행각은 그리 오래가지 못했다. K씨가 대표이사로 있는 회사의 직원 중 한명이 뭔가 이상한 낌새를 눈치 채고 경찰에 제보했기 때문이다. 이 제보는 최근 중국의 자동차시장에서 국내 차량을 본따 만든 일명 '짝퉁' 차량을 조사하는 검찰 내 특별팀으로 넘겨졌고 이들은 곧바로 용의자들의 주변인물 조사와 지속적 탐문 수사, 은행계좌 추적, 통화내역 발취 등을 통해 이름뿐인 또 다른 업체를 발견할 수 있었다. 또한 중국 상해의 S자동차 사와 대만 F자동차사 등지에 납품한 회계서류 등을 분석하는 작업이 이루어졌으며 이런 과정을 통해 이들의 범죄 행각은 세상에 낱알이 드러나게 됐다. ⑮

기술보호에 대한 오해와 착각



선진국 어느 나라를 막론하고 산업스파이로 인한 첨단기술유출로 고민하지 않는 곳은 없다. 또한, 냉전 시대의 정치·군사 첩보수집과 국가보안에 전념하던 각국의 정보기관은 첨단기술 첩보와 경제정보 수집에 주력하고, 산업스파이 방어를 국가안보차원에서 접근하고 있는 실정이다. 국제환경과 정치·경제적인 변화, 그리고 과학기술의 발달로 인해 산업보안의 개념에서부터 보호대상, 보호주체의 가치관 등이 변하는 과도기적 단계에 와 있다. 이러한 상황에서 산업보안에 대한 정부와 기업, 근로자, 그리고 국민들의 오해를 바로잡아야 우리나라 산업보안 수준이 한 단계 업그레이드 될 수 있을 것으로 본다.

글 · 김종길 한국산업보안연구원 원장(antispy@paran.com)

[정부의 오해와 착각]

오해와 착각 1 : 기술유출의 근본원인에 대한 시각 차이

기술유출과 관련한 보도를 보면 첨단기술이 외국으로 유출됐다는데 초점이 맞추어져 있어 일반인들은 마치 외국기업이나 외국인이 우리 기업에 침입해 기술을 훔쳐가는 것으로 오해하는 경우도 가끔 있다. 또한, 우리나라 경제에 큰 도움이 되는 첨단기술 유출을 차단함으로써 몇 십 조원의 손실을 막았으며 유출한 자는 매국노나 간첩에 버금가는 범죄인으로 매도하는 경우가 많다. 더욱이 산업기술유출방지법 시행규칙에 산업기술을 유출하는 자를 신고하는 자에게 1억원의 보상금을 줄 수 있게 규정하고 있는 등 간첩신고에 버금가는 상금을 주고 있기도 하다.

그러나 기술을 유출하는 자가 내부직원이고 같은 직장의 동료일 경우가 많기 때문에 기술유출을 방지하기 위해 직장동료를 범죄자로 신고하도록 유도하는 것이 과연 최선의 접근방법인지는 한번 고려해야 할 문제라고 생각한다.

기술유출의 80% 이상이 임직원 또는 퇴직자인 상황에서 해당기술을 취급하고 있는 자가 왜 기술을 유출하고 있는지에 대한 근본적인 원인을 밝히고 이에 대한 대응책을 마련하는 것이 정부가 최우선적으로 지향해야 할 정책이라고 할 수 있다.

현재 우리나라는 국가경제기반인 첨단기술을 개발한 자와 이를 효과적으로 활용해 기업과 국가경제에 크게 이바지하는 자에 대한 보상규정이 매우 미흡하다. 즉, 첨단기술 개발자에 대한 보상과 명예, 기술보호수당의 장기지급 등이 요구되고 있는 것이다. 그러나 보상능력이 없는 중소기업은 정부차원의 적극적인 대응책 없이는 내부자의 기술유출을 방지하거나 유출사건의 감소를 기대하기 매우 어렵다.

기술유출사건의 발견을 위한 보상이 아니라 첨단기술 개발자와 관리자의 기술유출을 원천적으로 예방하는 데 초점을 맞추지 않으면 임직원 등 내부자의 기술유출을 막을 수 없는 것이 현실이다.

오해와 착각 2 : Global 시대 폐쇄적 기술보호만이 능사는 아니다

미국의 퀄컴사는 CDMA 원천기술 특허를 보유하고 이를 공개해 우리나라에 매년 약 4,000억원에 이르는 로열티를 받아가고 있다. 이러한 글로벌 시대에 자국 내 기술보호만이 최선이라는 편협된 사고

에서 벗어나야 한다. 글로벌 스탠더드를 확보하기 위해서는 특허를 확보해 널리 공개해야 하고 세계시장을 석권하기 위해서는 다양한 전략을 수립해 기술 이전은 물론 외국진출을 위한 투자도 보장해야 한다.

하물며 국내 기업이 외국법에 의하여 설립한 외국지사에도 기술이전을 제한하는 것이 국제적인 대기업 육성과 외국시장 확보, 그리고 글로벌 경영 차원에서 과연 적절한 정책인지 생각해야 할 문제이다. 필자의 견해로는 기술 공개와 외국 진출에 대해 자율성을 보장하는 대신 외국진출



기업의 기술보호 기법 및 수준을 높일 수 있도록 정

부에서 정책적인 지원을 하는 것이 바람직하다고 본다. 선진국의 경우 M&A에 의한 기술유출을 방지하기 위해 각종 법률을 제정해 시행중이다. 미국은 1988년부터 시행하는 엑슨-플로리오(Exon-Florio) 법에 의하여 첨단기술을 보유한 기업은 외국기업의 M&A를 제한할 수 있고 일본은 2005년부터 황금주(주요 의사결정에 대해 거부권 행사가 가능한 주식) 도입 등을 골자로 한 'M&A 방어지침'을 마련하고 있으나 우리나라는 첨단기술 보유업체에 대한 외국기업의 M&A를 통한 기술유출에 대응할 수 있는 법적 제도가 아직 없는 형편이다.

합법적인 기술이전은 국내 경제에 미치는 영향을 고려하여 민간단체의 자율적인 조정기구를 두어 스스로 판단하게 하되 정부 관계자는 해당기구의 동등한 멤버로 참가해 의견을 개진하는 정도에 그치는 것이 바람직하다고 본다.

오해와 착각 3 : 기술보호가 IT 보안만으로 가능하다?

우리나라의 정보통신기술과 IT 보안 수준은 세계적이다. 이로 인해 IT 보안관련 국책연구기관, 협회도 여럿 있고 이에 따라 IT 보안 업체 역시 포화상태라 할 수 있다. 따라서 기술보호 또는 산업보안의 실천방안이 정보보호 또는 IT 보안이 전부인양 착각할 만큼 보편화되어 있으나 중소기업의 경우 기술과 재정적인 문제로 IT 보안으로 기술보호를 하기에는 여러 가지로 한계가 있다.

오늘날 사무환경 인프라가 IT 기반으로 이루어져 있는 등 국민생활에 절대적인 영향을 미치고 있으므로 IT 보호를 위한 기술적 또는 물리적인 안전대책을 강구하는 것은 너무나 당연하다. 그러나 중소기업이나 국민의 대다수는 오히려 정보통신의 발달에 정비례하여 정보화의 역기능에 시달리고 있고 전 세계 해커들의 경유지로 활용되는 등 부작용도 만만치 않은 게 사실이다.

이와 관련해 대기업의 경우는 정보보호를 위한 많은 솔루션이 있으므로 이를 활용하여 기술정보를 충분히 보호할 수 있다. 그러나 중소기업은 기술보호를 위해 다양한 보안 솔루션을 도입할 재정적인 능력도 없고 만약 솔루션을 지원한다 해도 기술적으로 운영할 능력과 전문가를 확보할 여력이 없는 상황이다. 필자가 강연을 다니다 보면 중소기업에 대해 정부에서 2,000여만원 상당의 보안 솔루션을

지원했지만 기술 및 관리상의 문제로 제대로 활용하지 못한 업체를 여럿 볼 수 있었다.

중소기업이 서버나 하드디스크에 첨단기술정보를 저장해 두고 어설픈 IT 보안정책을 바탕으로 해당 기술을 보호한다는 것은 현실적으로 무리라고 볼 수 있다. 그러나 정부가 이를 권장하고 지원하고 있으므로 중소기업으로 하여금 IT 보안으로 핵심기술 보호가 가능하다고 믿도록 하는 것이 오히려 기술보호에 허점이 되고 있는 것이다. 그렇기에 기업규모와 업종, 그리고 상황에 알맞은 맞춤형 기술보호 대책이 더욱 절실하다.

오해와 착각 4 : 기술유출에 따른 손실과 중요성에 비해 처벌이 미약하고 온정적이다?

언론에서 첨단기술의 해외유출로 인한 손실이 최대 몇 조원에 이른다고 보도하고 있으나 실제 처벌되는 내용을 보면 너무 온정적이고 관대하다는 사실을 알 수 있다. 사법 연감에 따르면 '부정경쟁방지 및영업비밀보호에관한법률' 위반으로 기소된 사건 중에 2004년 1심 판결을 받은 138명 중 유기징역을 받은 사람은 10명(7.2%)이었고 2005년 1심 판결이 내려진 130명 가운데 실형을 선고받은 사람은 11명(8.4%)에 불과했다.

이러한 첨단기술의 해외유출이 국가경제를 뒤흔드는 사건이고 엄청난 손실이 예상되는 사건임에도 처벌이 미약하거나 또는 대개가 집행유예로 선고되는 것은 미온적인 판결이며 기술유출 예방 측면에서도 바람직하지 않다는 견해가 많다. 이러한 생각도 관련기관과 언론이 사건을 피상적이고 감정적으로 보도하는 경향에서 비롯된 오해라고 할 수 있다.

기술유출 사건은 은밀하게 이루어질 뿐 아니라 기술정보의 원본에 아무런 손상 없이 정보통신이나 기타 저장매체로 유출되는 등 증거인멸이 용이하기 때문에 사전에 충분한 보호조치 없이는 기술유출사건의 증거확보에 어려움이 많다. 또한, 증거확보를 위한 증인도 직장동료이거나 동종업계의 선후배 등이 대부분이라 온정적인 증언을 피할 수 없으므로 범죄를 성립시킬 수 없는 경우도 많다. 따라서 보안담당자가 사전에 기술적인 보호조치와 관련된 전문적인 지식과 경험이 없으면 기술유출에 대한 증거확보가 대단히 어려운 것이다.

특히, 영업비밀 침해와 관련된 범죄 구성요건으로 기업의 해당기술이 철저히 보호되고 있는 비밀이라는 것이 전제조건으로 붙는다. 그러나 중소기업은 사전에 철저하게 기술보호를 하지 않는 경우가 많으므로 기술을 유출한 사실이 있음에도 이를 처벌할 수 없는 경우도 발생하는 것이다. 또한, 기술유출 사건은 범인이 내부직원으로 과학자 또는 기술자이며, 본인들이 별다른 죄의식 없이 유출하는 초범인 경우가 대부분이다. 비록 기술을 부정하게 취득했다라도 외국으로 유출되지 않은 경우에 형사처벌이 미흡한 것을 두고 온정주의라고만 매도할 수는 없다.

엄중한 처벌도 물론 중요하다. 그러나 사전에 기술 가치를 객관적으로 평가해 그 평가기준을 바탕으로 철저한 보호대책을 마련해야만 기술유출사건의 핵심을 파악하지 못하는 피상적인 접근에서 오는 오해와 착각에서 벗어날 수 있다.

[기업경영진의 오해와 착각]

보호할 기술은 무형인데, 유형의 물질보호에 중점을 두고 있다

지난해 초 미국의 블루킹스 연구소는 오늘날 기업의 가치 가운데 약 70%가 눈에 보이지 않는 지적재산이라고 발표한 바 있다.

특히, 마이크로소프트사의 가치 가운데 무형의 지적재산이 95%, 나이키는 86%, 코카콜라사는 77%이고 무형의 지적재산 가치가 1982년에는 전 기업의 평균 38%이었던 것이 오늘날은 평균 70%로 약 2배에 가까운 가치로 증가한 것으로 조사됐다.

그러나 우리나라는 아직도 눈에 보이는 물리적인 재산인 30%를 보호하기 위하여 울타리 및 CCTV 설치, 출입통제, 인적경비 등 유형의 물질을 보호하는데 초점이 맞추어져 있고 기업가치의 70%에 이르는 무형의 지적재산 보호에는 소홀한 상황이다.

이는 경영환경은 급변하는데 경영진의 인식은 아직 산업사회의 보안수준을 벗어나지 못하고 있기 때문이다. 이에 경영진들은 보호해야할 정보의 가치와 유출의 근본원인을 정확히 인식하고 정보사회에 걸 맞는 기술보호 대책을 마련할 필요가 있다.

무형기술은 지금도 은밀히 유출되고 있다

산업기술은 외부침입을 막는 울타리와 CCTV, 출입통제 시스템이 존재하더라도 통신선, E-mail, 팩스, 전화, 도청 등을 통해 유출자 이외에는 아무도 모르게 유출될 수 있다. 특히, 임직원의 CD, USB, 휴대폰 카메라 등을 통해 저장, 복사 또는 촬영할 수 있는 정보가 무형이기 때문에 발견하는데 어려움이 많다.

이렇듯 시대변화에 따라 보호의 대상과 가치가 변화하므로 보호대상인 지적재산의 특징과 유출경로를 정확히 파악하여 이를 보호하는데 초점을 맞추어야 한다. 일례로 중소기업의 경우 때로는 고전적인 문서형태로 보호하는 것이 오히려 기술보호가 용이하고 경제적인 수 있다.

시대와 지역에 따른 맞춤형 보안이 필요하다

1990년대 초 미국의 유명한 보안업체인 P사와 C사가 국내에 진출했으나 사업에 실패하고 철수한 적이 있다. 우리나라의 사회 현실과 국민정서, 그리고 기업문화가 미국과 판이하게 달랐기 때문이다. 월마트가 우리나라에서 철수한 이유도 우리 국민의 정서를 깊이 이해하지 못한 까닭이다. 기업보안은 시대와 문화수준, 국민정서에 따라서 접근방법에 차이가 날 수밖에 없다.

일례로 총기소지를 허용하고 마약사용 및 테러 등에 고심하는 미국의 경우 경영자와 근로자의 신변안전, 기업(상점)의 총기강도, 근로자의 마약복용 및 대테러 대응 등이 기업보안 및 안전관리 측면에서 주요 이슈가 되지만 우리나라의 현실과는 동떨어질 수밖에 없는 것이다.

또한, 기업도 사회 안전의 일익을 담당하므로 이를 산업보안이라 확대해석하는 선진국 또는 외국의 Skill이나 Tool을 우리나라에 바로 적용하는 것이 기업현실과 국민정서에 맞지 않았기에 외국의 유명한 보안업체인 P사와 C사가 철수할 수밖에 없었던 것이다.

기술보호는 해당국가의 정치·경제적 상황과 사회 환경, 그리고 기업 현장에서의 현실적인 문제가 이론보다 앞서기 때문에 국가와 기업의 특성을 고려한 맞춤형 보안이 가장 바람직하다.

우리 기업의 실정과 인식수준에 맞지 않게 산업보안을 확대 해석하는 접근방법은 IT 보안이 산업보안의 전부인양 착각하고 오해하는 것과 다를 바 없다. 국내 대기업과 중소기업의 현실에서 가장 심각한 기술유출문제를 시급히 해결해야 하는 것이 산업보안에 있어 최우선적이고 현실적인 문제인 것이다.

기술보호 담당자도 본능과 욕구를 지닌 사람이다

기업이 보유한 첨단기술을 철저히 보호하면서 독점 사용하거나 다른 기업에 합법적인 기술이전을 통해 로열티를 받으면 그 기업은 성장할 수 있다.

이러한 첨단기술은 기업의 소유이고 이를 보호하는 것은 기업을 대표하는 대표이사의 책임이다. 그러나 첨단기술은 기업경영진과 임직원간의 첨예한 이해관계가 상충됨에도 불구하고 현실적으로 근로자가 첨단기술을 보호·관리하고 있다. 자본주의 시장경제가 지배하는 경쟁사회에서 근로자도 인간이고 본능적 욕구를 가진 평범한 사람인데 이들에게 별다른 동기부여 없이 聖人의 禁慾(기술보호, 유출방지의무)을 강요하는 것이 과연 바람직한 것인지 깊이 생각해볼 필요가 있다.

고용은 불안하고 인간의 수명은 연장되고 있다. 또한 기술자의 유동성은 높아지고 헤드헌트 사의 난립, 그리고 경쟁업체의 우수인력 확보전략 등으로 고급인력의 이동과 기술유출의 유혹은 갈수록 증가하고 있다. 이는 굶주린 고양이에게 생선가게를 맡겨 놓고 생선을 먹지 말기를 바라는 것과 같은 상황이다.

경영자의 직무유기로 선량한 근로자를 산업스파이로 만들고 있는 건 아닌지 곰곰이 생각해봐야 한다. 경영자가 술선수범하여 기술보호에 앞장서야 하고 첨단기술 개발자에 대한 적절한 보상대책이 절실한 이유다. 많은 기업에 출강해보면 경영진의 참석률이 3%에 불과하다. 경영자는 기술보호가 근로자의 뒤편인양 착각하고 있는 것이다.

기술유출은 영원히 계속될 것이다

기술이 외국에 유출되는 경우보다 국내기업 간에 유출되는 경우가 많고 더구나 발견되지 않는 사건이 80% 이상이라는 것이 외국전문가들의 주장이다. 기술보호관련 산업분야는 엘빈 토플러의 예언처럼 21세기에 가장 큰 성장산업이며 이는 유출사건 또한 점차 증가한다는 사실을 전제하는 것이다.

기술유출 사건은 일시적인 문제가 아니라 보다 더 좋은 제품과 서비스를 바라는 인간의 욕망이 있고 경쟁업체가 있는 한 영원히 지속될 것이 분명하다. 따라서 이에 대한 대응책도 물리적인 보안장비의 설치나 유출자 처벌, 그리고 유출행위의 신고자에 대해 포상금을 지급하는 것만으로 문제가 해결되지는 않을 것이다.

국민의 기술보호에 대한 인식수준이 꾸준히 높아지고 기업의 윤리경영과 근로자의 직업윤리를 향상시키지 않으면 어려운 것이다. 따라서 초·중·고등학교 등 공교육 차원에서 기술보호의 중요성에 대한 국민들의 인식 수준을 높이는 교육이 필요하며 대학에서는 전문교육을 통해 기술보호 전문가를 양성하는 일이 중요하다.

사건에 대한 은폐와 無대응은 기술유출을 조장한다

기술유출은 80% 이상이 내부직원에 의해 발생되므로 유출자의 은폐는 너무나 당연하지만 이를 인지

한 관리자도 사건을 은폐하고자 하는 속성이 있다. 더욱이 기술유출사건은 당사자 이외는 발견이 매우 어렵다. 설사 기술유출의 정황이 포착돼도 기술정보의 원본에 아무런 손상이 없으므로 관리자나 경영자가 증거를 확보하기가 어렵고 만약 사건의 전모를 파악했다 하더라도 관리자는 문책의 두려움으로, 그리고 경영자는 기업이미지 손상 및 주가하락을 두려워하므로 사건을 은폐하기 위해 모든 노력을 경주하게 된다.

이는 사건에 연루된 자에 대한 아무런 징계나 사법처리 등을 하지 않은 사례가 상공회의소 조사에서는 47.6%, 한국산업기술진흥협회 조사에서는 33.3%에 이른 것으로 조사된 것에서도 짐작할 수 있다. 사건에 대해 아무런 책임을 묻지 않는 것은 결국 기술유출에 대한 경각심을 흐리게 하여 다른 직원도 기술유출의 유혹에 빠질 수 있게 된다. 따라서 기술유출사건이 발생했을 경우 관련자들에게 반드시 엄정한 책임을 물어야 한다.

보안은 엘리트가 담당해야 할 전문분야다

고전적인 의미의 산업보안은 회사의 건물과 물자를 보호하기 위하여 경비원이 출입을 통제하고 울타리를 튼튼히 하여 외부침해를 막으면 되는 물리적 보안 위주였다. 그러므로 예비군이 설치된 직장은 예비군 중대장이 겸직하거나 곧 퇴직할 직원 또는 능력이 부족한 직원이 담당하는 업무로 치부하는 경우가 많았다.

그러나 오늘날 기업의 지적재산권 및 기술보호는 그 보호대상의 특징과 다양한 유출경로로 인해 기업경영과 IT 보안 등에 대한 전문적인 지식을 갖춘 전문가가 아니면 기술보호업무를 수행하기가 불가능하다. 또한, IT 보안이나 물리적 보안 분야를 전공한 사람이라도 좀더 폭 넓은 지식을 쌓아 시대변화에 따른 다양한 보안지식을 갖추는 필요가 있다.

기술보호 시스템이 철저히 구축돼 있거나 담당자의 능력이 탁월할 경우 기술유출을 조기에 발견할 수 있어 사건이 많이 발생하는 것으로 착각할 수 있으나 이는 기술보호체계가 우수한 업체의 초기 현상이다. 다시 말하면 기술유출을 발견할 능력이 있기 때문에 발견된다는 얘기다. 기술보호 시스템이 존재하지 않고 담당자의 능력이 부족하면 사건을 발견할 수 없으므로 사건이 없는 것으로 착각하고 있는 것이다.

[근로자의 오해와 착각]

직업윤리와 준법정신이 미흡하다

미국은 법적으로 개인의 자유와 권리가 철저히 보장되지만 개인적인 문제 즉, 기업과 근로자간의 대등한 입장에서 작성한 계약(고용계약, 비밀유지서약)은 반드시 지킨다.

선진국은 고용의 유동성이 매우 높으나 내부자의 기술유출사건은 50% 이하에 불과하다. 반면, 우리나라의 경우 내부자의 기술유출사건은 80% 이상이다. 이는 선진국의 경우 직업윤리의식과 준법정신이 강하고 자기가 서명한 비밀유지계약을 철저히 준수하기 때문이다.



미국은 고용계약 등에는 근무시간에 사적인 업무를 인정하지 않으므로 회사의 PC로 개인의 사무를 처리할 경우 약 25% 정도의 기업은 면직을 하고 75% 정도는 징계를 하는 것으로 조사된 바 있다. 이는 우리나라 기업 근로자의 근무행태로 본다면 상상하기 어려운 상황이다.

우리나라 근로자는 공적인 업무와 사적인 업무의 구분이 명확하지 아니하고 직업윤리의식이 미흡한 것이 사실이다. 이에 기업은 윤리경영을 시행하고 근로자는 회사를 위하여 책임과 의무를 다하는 직업윤리를 갖추어야만 한다.

자신이 개발·관리하는 기술은 회사기술이다
우리나라는 국가공무원과 지방공무원 및 국립학교 교사의 직무발명은 국가와 지방자치단체 또는 학교단체에 귀속되며 그 발명에 대한 보상규정과 금액을 법령으로 규정하고 있다. 그러나 기업 종업원의 직무발명은 근원적으로는 종업원의 귀속을 원칙으로 하고 있으나, 기업이 사전에 회사에 귀속한다는 예약승계규정을 둔 경우는 기업에 귀속할 수 있도록

규정하고 있다.

발명에 대한 권리를 회사로 귀속시킬 경우 보상을 하도록 직무발명관계규정에 명시하는 등 발명진흥법이 대폭 개정되기도 했다.

2007년 6월에 진행된 중소기업청과 산업기술진흥협회의 조사에 의하면 중소기업의 연구개발성과에 대한 금전적 보상은 16.7%, 비금전적 보상 시스템 운영은 21.5%, 양 시스템을 모두 운영하는 업체가 26.9%에 이르는 등 보상 시스템을 갖춘 업체가 65.1%이고, 보상 시스템이 없는 기업이 34.9%로 나타났다.

성과보상의 지급방법에 있어서는 특허출원, 등록, 실시보상, 처분보상 시에 일시적 보상은 물론, 그 기술이 회사이익에 기여하는 동안은 그 이익의 일부를 장기적으로 기술보호수당으로 지급하는 것이 가장 바람직할 것으로 본다. 이러한 방법으로 정당한 보상을 받은 발명기술의 경우 종업원이 해당기술의 유출을 방지하는데 적극적으로 참여하는 것이 바로 직업윤리인 것이다. 15

V. 부록

088 개인정보 관련 법규

공공기관의 개인정보 보호에 관한 법률 시행령

공공기관의 개인정보 보호에 관한 법률

정보통신망법

095 정보보호관련 유관기관 및 단체

096 국내 주요 보안USB 업체 현황



개인정보 관련 법규

공공기관의 개인정보 보호에 관한 법률 시행령

제3조 (단순 업무 처리를 위한 행위)

법 제2조 제3호 단서에서 “대통령령이 정하는 행위”라 함은 다음 각호의 1에 해당하는 행위를 말한다.

1. 문서 또는 도면의 내용만을 기록하는 행위
2. 문서 또는 도면의 내용을 전기통신의 방법으로 전달하기만 하는 행위
3. 인쇄물을 제작하기 위한 행위

제10조 (개인정보의 안전성 확보 등)

1. 보유기관의 장은 법 제9조의 규정에 의한 개인정보의 안전성 등을 확보하기 위하여 입출력자료 · 전산기기 · 전산실 등의 관리에 관하여 행정자치부령이 정하는 바에 따라 필요한 조치를 취하여야 한다.

〈개정 1999.1.29〉

2. 공공기관의 장은 개인정보의 처리를 다른 공공기관 또는 관련 전문기관에 위탁하는 때에는 행정자치부령이 정하는 바에 따라 개인정보의 보호에 필요한 조치를 취하여야 한다.

〈개정 1999.1.29〉

제12조 (처리정보의 제공제한)

1. 보유기관의 장은 처리정보를 통신망을 이용하여 다른 기관에 제공하는 경우에는 제공하는 처리정보의 항목을 한정하고 그 위를 넘어서 처리 정보를 이용할 수 없도록 필요한 조치를 취하여야 하며, 제11조제2항 각호의 사항을 행정자치부장관등에게 통보하여야 한다.

〈개정 1999.1.29〉

2. 보유기관의 장은 제1항의 규정에 의하여 처리정보를 제공받은 기관이 법 제10조제3항의 규정에 의한 제한이나 요청사항을 이행하지 아니하는 때에는 즉시 처리정보의 제공을 중지하여야 한다.

제19조 (대리인의 범위)

- ① 법 제16조의 규정에 의하여 대리청구를 할 수 있는 자는 의정대리 정보주체로부터 위임을 받은 수임인
- ② 유기관의 장은 특별한 사유가 있는 때에는 제1항의 규정에 의한 대리인의 범위를 행정자치부장관과 협의하여 따로 정할 수 있다.

〈개정 1999.1.29〉

공공기관의 개인정보 보호에 관한 법률

제2조 (정의)

이 법에서 사용하는 용어의 정의는 다음과 같다. [개정 2007.5.17] [[시행일 2007.11.18]]

1. “공공기관”이라 함은 국가행정기관·지방자치단체 그 밖의 공공단체중 대통령령이 정하는 기관을 말한다.
2. “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명 주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.
3. “처리”라 함은 컴퓨터 폐쇄회로 텔레비전 등 정보의 처리 또는 송수신 기능을 가진 장치(이하 “컴퓨터 등”이라 한다)를 사용하여 정보의 입력 저장 편집 검색 삭제 및 출력 기타 이와 유사한 행위를 하는 것을 말한다. 다만, 문장만을 작성하는 등의 순업무처리를 위한 행위로서 대통령령이 정하는 행위를 하는 것을 제외한다.
4. “개인정보파일”이라 함은 컴퓨터 등에 의하여 처리할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 자기테이프 자기디스크 등 전자적인 매체에 기록된 것을 말한다.
5. “처리정보”라 함은 개인정보파일에 기록되어 있는 개인정보를 말한다. 5의2. “폐쇄회로 텔레비전”이라 함은 정지 또는 이동하는 사물의 간접 영상 및 이에 따르는 음성·음향 등을 특정인이 수신할 수 있는 장치를 말한다.
6. “보유”라 함은 개인정보파일을 작성 또는 취득하거나 유지관리하는 것 (개인정보의 처리를 다른 기관 단체등에 위탁하는 경우를 포함하되, 다른 기관 단체 등으로부터 위탁받은 경우를 제외한다)을 말한다.
7. “보유기관”이라 함은 개인정보파일을 보유하는 기관을 말한다.
8. “정보주체”라 함은 처리정보에 의하여 식별되는 자로서 당해 정보의 주체가 되는 자를 말한다.

제3조의2 (개인정보보호의 원칙)

- ① 공공기관의 장은 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 아니된다.
- ② 공공기관의 장은 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 한다.
- ③ 공공기관의 장은 개인정보관리의 책임관계를 명확히 하여야 한다.
- ④ 공공기관의 장은 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다.

[본조신설 2007.5.17] [[시행일 2007.11.18]]

제4조 (개인정보의 수집)

① 공공기관의 장은 사상·신조등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나, 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.

② 공공기관의 장은 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서(「전자정부법」제2조제5호에 따른 전자문서를 포함한다. 이하 같다) 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인 할 수 있도록 안내하여야 한다. 다만, 제6조제3항 각 호의 어느 하나에 해당하는 개인정보파일을 보유할 목적으로 개인정보를 수집하는 경우에는 그러하지 아니하다.

[신설 2007.5.17] [[시행일 2007.11.18]]

제6조 (개인정보파일의 보유·변경시 사전협의)

① 공공기관의 장이 개인정보파일을 보유하고자 하는 경우(다른 공공 기관으로부터 처리[[정보를 제공받아]]보유 하고자 하는 경우를 제외한다)에는 다음 각 호의 사항을 행정자치부장관과 협의하여야 한다. 다음 각 호의 어느 하나에 해당하는 사항을 변경하고자 하는 경우에도 또한 같다.

[개정 1999.1.29, 2007.5.17] [[시행일 2007.11.18]]

1. 개인정보파일의 명칭
2. 개인정보파일의 보유목적
3. 보유기관의 명칭
4. 개인정보파일에 기록되는 개인 및 항목의 범위
5. 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭
6. 개인정보파일의 열람예정시기
7. 열람이 제한되는 처리정보의 범위 및 그 사유
8. 그 밖에 대통령령이 정하는 사항

② 중앙행정기관의 장이 아닌 공공기관의 장은 제1항에 따라 협의를 하고자 하는 경우에는 관계 중앙행정기관의 장을 거쳐 관련 서류를 제출하여야 한다.

[신설 2007.5.17] [[시행일 2007.11.18]]

③ 제1항의 규정은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 이를 적용하지 아니한다.[개정 2007.5.17] [시행일 2007.11.18]

1. 국가의 안전 및 외교상의 비밀 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 조세법처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보파일
4. 삭제 [2007.5.17] [[시행일 2007.11.18]]

5. 삭제 [2007.5.17] [[시행일 2007.11.18]]

6. 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일

7. 삭제 [2007.5.17] [[시행일 2007.11.18]]

8. 그 밖에 이에 준하는 개인정보파일로서 대통령령이 정하는 개인정보파일

④ 다른 법률에 관계 중앙행정기관의 장으로 하여금 공공기관의 개인정보파일의 보유기준을 정하도록 규정되어 있는 경우에는 제1항에 불구하고 그 보유기준에 관한 협의로 제1항에 따른 협의를 갈음한다. 이 경우 행정자치부장관과의 협의는 관계 중앙행정기관의 장이 행한다.

[신설 2007.5.17] [[시행일 2007.11.18]]

⑤ 행정자치부장관은 제1항 또는 제4항에 따라 협의를 하는 경우로서 개인정보의 보호를 위하여 필요하다고 인정하는 때에는 제20조에 따른 공공기관개인정보보호심의위원회에 협의사항에 관하여 심의를 요청할 수 있다.

[신설 2007.5.17] [[시행일 2007.11.18]]

[본조제목개정 2007.5.17] [[시행일 2007.11.18]]

제7조의2 (개인정보보호방침)

①보유기관의 장은 다음 각 호의 내용이 포함된 개인정보보호 방침을 정하여야 한다.

1. 제6조의제1항 각 호의 사항. 다만, 같은 조 제3항 각 호의 개인정보 파일에 관한 사항을 제외한다.

2. 제20조의2에 따른 개인정보관리책임관의 성명·소속·부서·직위 및 전화번호 그 밖의 연락처

3. 인터넷 홈페이지 접속정보파일 등 인터넷 홈페이지를 통하여 수집되는 개인정보의 보호에 관한 사항

4. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② 보유기관의 장은 제1항에 따라 개인정보보호방침을 정한 경우에는 그 내용을 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

[본조신설 2007.5.17] [[시행일 2007.11.18]]

제9조 (개인정보의 안전성확보등)

① 공공기관의 장은 개인정보를 처리하거나 개인정보파일을「전자정부법」제2조제7호에 따른 정보통신망(이하“정보통신망”이라 한다)에 의하여 송수신하는 경우 개인정보가 분실 도난 누출 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 강구하여야 한다.

② 공공기관의 장은 개인정보의 처리에 관한 사무를 다른 공공기관 또는 관련 전문기관에 위탁할 수 있으며, 이 경우 개인정보가 분실 도난 유출 변조 또는 훼손되지 아니하도록 안전성 보에 필요한 조치를 취하여야 한다.

[신설 2007.5.17] [[시행일 2007.11.18]]

③ 2항에 따른 위탁 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

[신설2007.5.17] [[시행일 2007.11.18]]

④ 공공기관의 장은 제2항에 따라 개인정보의 처리에 관한 사무를 위탁하고자 하는 경우에는 관보 또는 인터넷 홈

페이지 등을 통하여 미리 그 사실을 공개하여야 한다.

[개정 2007.5.17] [[시행일 2007.11.18]]

⑤ 공공기관으로부터 개인정보의 처리를 위탁받은 자에 대하여도 제1항의 규정을 준용한다.

제10조 (처리정보의 이용 및 제공의 제한)

① 기관의 장은 다른 법률에 따라 보유기관내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니된다.

[개정 2007.5.17] [[시행일 2007.11.18]]

② 유기관의 장은 보유목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한하여야 한다.

[신설 2007.5.17] [[시행일 2007.11.18]]

③ 보유기관의 장은 제1항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다.

[개정 99.1.29, 2007.5.17] [[시행일 2007.11.18]]

1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 처리정보를 보유목적 외에 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조에 따른 공공기관개인정보보호심의위원회의 심의를 거친 경우.
3. 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우
4. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우
6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우
7. 법원의 재판업무수행을 위하여 필요한 경우
8. 삭제

[2007.5.17] [[시행일 2007.11.18]]

④ 보유기관의 장은 제3항제2호 내지 제7호의 규정에 의하여 처리정보를 정보주체외의 자에게 이용하게 하거나 제공하는 때에는 처리정보를 수령한 자에 대하여 사용목적 · 사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성확보를 위하여 필요한 조치를 강구하도록 요청하여야 하며, 이러한 요청을 받은 정보수령자는 처리정보의 안전성 확보를 위한 조치를 취하여야 한다.

[개정 2007.5.17] [[시행일 2007.11.18]]

⑤ 보유기관으로부터 처리정보를 제공받은 자는 보유기관의 동의 없이 당해 처리정보를 제3자에게 이용하게 하거나 제공하여서는 아니 된다.

[개정 2007.5.17] [[시행일 2007.11.18]]

⑥ 보유기관의 장은 제3항제2호 내지 제5호 및 제7호에 따라 보유목적 외의 목적으로 이용하게 하거나 제공하는 경우에는 그 이용 또는 제공의 법적 근거·목적 및 범위 등에 관하여 필요한 사항을 정보주체가 쉽게 확인할 수 있도록 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

[개정 2007.5.17] [[시행일 2007.11.18]]

제10조의2 (개인정보파일의 파기)

① 보유기관의 장은 개인정보파일의 보유목적 달성 등 당해

개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 제1항에 따라 개인정보파일을 파기한 경우 보유기관의 장은 개인정보파일을 파기한 사실을 관보 또는 인터넷 홈페이지 등에 공고하여야 한다. 다만, 파기한 개인정보파일이 제6조제3항 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

③ 개인정보파일의 파기방법, 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2007.5.17] [[시행일 2007.11.18]]

제11조 (개인정보취급자의 의무)

개인정보의 처리를 행하는 공공기관의 직원이나 직원이었던 자 또는 공공기관으로부터 개인정보의 처리업무를 위탁 받아 그 업무에 종사하거나 종사하였던 자는 직무상 알게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니된다.

제14조 (처리정보의 정정 및 삭제 등)

① 제12조에 따라 본인의 처리정보를 열람한 정보주체는 보유기관(다른 기관으로부터 처리정보를 제공받아 보유하는 기관을 제외한다.

이하 이조에서 같다)의 장에게 문서로 당해 처리정보의 정정 또는 삭제를 청구할 수 있다. 다만, 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있는 경우에는 그 삭제를 청구할 수 없다.

[개정 2007.5.17] [[시행일 2007.11.18]]

② 보유기관의 장은 제1항의 규정에 의한 정정 또는 삭제청구를 받은 때에는 처리정보의 내용의 정정 또는 삭제에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다.

[개정 2007.5.17] [[시행일 2007.11.18]]

제15조 (불복청구)

① 제12조제1항 및 제14조제1항에 따른 청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또

는 이익의 침해를 받은 자는 「행정심판법」으로 정하는 바에 따라 행정심판을 청구하거나 「행정소송법」으로 정하는 바에 따라 행정소송을 제기할 수 있다.

② 제1항에 따라 행정심판을 제기하는 경우 국가행정기관 및 지방자치단체 외의 공공기관의장의 처분 또는 부작위에 대한 재결청은 관계 중앙행정기관의 장으로 한다.

[전문개정 2007.5.17] [[시행일 2007.11.18]]

[본조제목개정 2007.5.17] [[시행일 2007.11.18]]

③ 보유기관의 장은 제2항의 규정에 의한 조사를 함에 있어 필요한 때에는 당해 청구인으로 하여금 정정 또는 삭제 청구사항의 확인에 필요한 증빙자료를 제출하게 할 수 있다.

[개정2007.5.17] [[시행일 2007.11.18]]

[본조제목개정 2007.5.17] [[시행일 2007.11.18]]

정보통신망법

제24조 제4항

이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니된다.

제50조의7

① 누구든지 인터넷 홈페이지 운영자 또는 관리자의 명시적인 거부 의사에 반하여 영리목적의 광고성 정보를 인터넷 홈페이지에 게시하여서는 아니된다.

② 인터넷 홈페이지 운영자 또는 관리자는 제1항의 규정에 위반하여 게시된 영리목적의 광고성 정보에 대하여 삭제하는 등의 조치를 할 수 있다.

정보통신망법 제30조

② 이용자는 정보통신서비스제공자등에 대하여 자신의 개인정보에 대한 열람 또는 개인정보를 이용하거나 제3자에게 제공한 내역을 요구할 수 있고, 자신의 개인정보에 오류가 있는 경우에는 그 정정을 요구할 수 있다.

④ 정보통신서비스제공자등은 제2항의 규정에 의하여 열람·내역 또는 정정요구를 받은 경우에는 지체 없이 필요한 조치를 취하여야 한다.

⑤ 정보통신서비스제공자등은 제2항의 규정에 의하여 오류의 정정요구를 받은 경우에는 그 오류를 정정할 때까지 당해 개인정보를 제공 또는 이용하여서는 아니된다.

⑥ 정보통신서비스제공자등은 이용자로부터 제1항 및 제2항의 규정에 의한 동의의 철회, 개인정보의 열람 또는 정정의 요구를 받은 경우에는 제22조 및 제23조의 규정에 의하여 개인정보를 수집하는 방법보다 쉽게 할 수 있도록 필요한 조치를 취하여야 한다.

● 주요 정보보호 유관 기관 및 단체

국가보안 기술연구소	www.nstri.re.kr
	042-870-2114
	대전시 유성구 가정로 138

국가정보보안 연합회	www.nisa.or.kr
	042-870-2114
	대전광역시 유성구 유성우체국 사서함 1호

국방부	www.mnd.go.kr
	02-748-1111
	서울시 용산구 이태원로 22번지

대검찰청	www.spo.go.kr
	02-3480-2000
	서울시 서초구 서초 3동 1730-1

방송통신위원회	www.bcc.go.kr
	02-750-1114
	서울시 종로구 세종로 20 (세종로100번지)

산업기밀보호센터	www.nisc.go.kr
	111(상담전화)

전자서명인증 관리센터	www.rootca.or.kr
	02-405-5114
	서울시 송파구 중대로 135 IT 벤처타워

지식경제부	www.mke.go.kr
	1577-0900
	경기도 과천시 관문로 88 정부과천청사

한국과학기술 정보연구원	www.kisti.re.kr
	042-869-1234
	대전시 유성구 과학로 335

한국산업기술 보호협회	www.kaits.or.kr
	02-6009-8530
	서울시 강남구 역삼동 701-7 한국기술센터 15층

한국생산기술 연구원	www.kitech.re.kr
	041-589-8114
	충남 천안시 입장면 흥천리 35-3

한국전자인증	www.crosscert.com
	1566-0566
	서울시 서초구 서초동 1674-4 하림빌딩 7층

한국정보문화 진흥원	www.kado.or.kr
	02-3660-2500
	서울시 강서구 공항로 188

한국정보보호 진흥원	www.kisa.or.kr
	02-405-5114
	서울시 송파구 중대로 135 IT 벤처타워

한국정보사회 진흥원	www.nia.or.kr
	02-2131-0114
	서울시 중구 청계천로 14

한국정보시스템 감사통제협회	www.isaca.or.kr
	02-786-2179
	서울시 금천구 가산동 371-28 우림라이온스밸리 C동 1106호

한국CISSP협회	www.cisspkorea.or.kr
	02-2142-0011
	서울시 송파구 가락동 78번지 정보통신 벤처센터 서관 11층

국가사이버 안전센터	www.ncsc.go.kr
	02-557-0716
	서울시 강남구 역삼동 736-1 한솔빌딩 9층

국가정보원	www.nis.go.kr
	111(콜센터)/02-3412-3800

금융보안연구원	www.fsa.or.kr
	02-6919-9114
	서울시 영등포구 여의도동 36-1번지 삼성생명빌딩 15층

대한민국전자정부	www.egov.go.kr
	02-2100-4040

사이버경찰청	www.npa.go.kr
	02-363-0112
	서울시 서대문구 의주로 91 미근동 209

외교통상부	www.mofat.go.kr
	02-2100-7999
	서울시 종로구 세종로 37

중소기업청	www.smba.go.kr
	1357
	대전시 서구 선사로 139

특허청	www.kipo.go.kr
	1544-8080
	대전시 서구 선사로 139

한국벤처기업협회	www.venture.or.kr
	02-8900-6000
	서울시 구로구 구로3동 222-12 마리오타워 8층

한국산업보안 연구원	www.antispy.or.kr
	02-584-0052
	서울시 서초구 양재동 16-2 미래빌딩 4층

한국소프트웨어 진흥원	www.software.or.kr
	02-2141-5000
	서울시 송파구 중대로 113 (가락본동 79-2)

한국전자통신 연구원	www.etri.re.kr
	042-860-6114
	대전광역시 유성구 가정로 138

한국정보보호 산업협회	www.kisia.or.kr
	02-2142-0900
	서울시 송파구 가락동 78번지 IT 벤처타워

한국정보보호학회	www.kiisc.or.kr
	02-564-9333
	서울시 강남구 역삼동 642-6 성지하이츠3차 909호

한국정보산업 연합회	www.fkii.or.kr
	02-780-0201
	서울시 마포구 상암동 1605 누리꿈스퀘어 비즈니스 타워

한국침해사고 대응지원팀	www.krcert.or.kr
	118
	서울시 송파구 중대로 135 IT벤처타워

행정안전부	www.mopas.go.kr
	02-2100-3399
	서울시 종로구 세종로 55 정부중앙청사

● 국내 주요 보안USB 업체 현황

비앤비솔루션 (대표 정연택)	제품명	SeProS
	웹사이트	www.bnbsol.net
	연락처	02-801-0199
	주소	서울시 구로구 구로동 197-28 E&C벤처드림타워 6차 808호
닉스테크 (대표 박동훈)	제품명	SafeUSB+
	웹사이트	www.nicstech.com
	연락처	02-3497-8900
	주소	서울시 서초구 양재동 275-5 태석빌딩 15층
세이프존 (대표 권창훈)	제품명	DefCon Secure USB
	웹사이트	www.saferzone.com
	연락처	02-525-1410
	주소	서울시 강남구 삼성동 109-18 경희빌딩 2층
엔트랙커 (대표 임종규)	제품명	NTRACKER USB Enterprise
	웹사이트	www.ntracker.net
	연락처	1544-3773
	주소	서울시 구로구 구로동 26 신도림포스빌 916호
비젯 (대표 장건)	제품명	SafeUSB
	웹사이트	www.bizet.co.kr
	연락처	02-380-3377
	주소	서울시 마포구 상암동 DMC 산학협력연구센터 14층
코디아 (대표 고병수)	제품명	Secure-i
	웹사이트	www.kodia.co.kr
	연락처	02-568-5744
	주소	서울시 강남구 삼성동 165-4 계명빌딩 3층
솔루션어소시에이트 (대표 전용희)	제품명	IGM(Inner Guard Master)-Public
	웹사이트	www.sa-inter.com
	연락처	031-751-8321
	주소	경기도 성남시 수정구 복정동 694-5 야정빌딩 3층
디지털센스 (대표 최주호)	제품명	Infosecure-USB
	웹사이트	www.digitalsense.co.kr
	연락처	02-3473-7760
	주소	서울시 서초구 방배3동 1001-1 KT서초지사 501호

보안적합성 검증필 엔트랙커 보안USB

17대 대통령직인수위원회

통일부

대한민국 해군

방위사업청

국방기술품질원

해병대

국가비상기획위원회

국군정보사령부

한미연합사

인천해양수산청

장성군청

한옥 테크노글라스

삼익 THK

대웅제약

영주시청

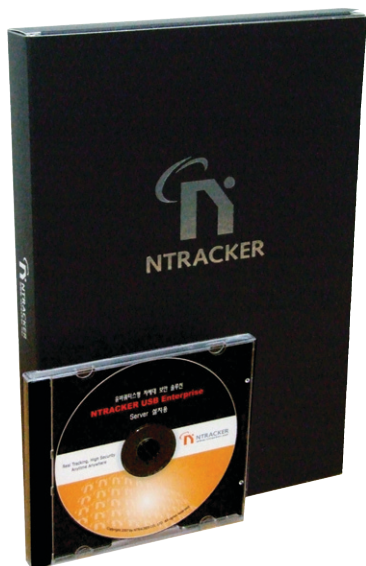
⋮

2008년 3월 현재



믿음과 신뢰를 드립니다.

보안 USB 핵심기능 누구도 따라올 수 없습니다.



Powerful **Security**
Anytime Anywhere!!

- Easy Control, Easy Use!
- Plug & Play
- Windows 2000/XP/Vista

국/내/최/초

국정원 보안적합성 검증 통과 진짜 보안USB “씨프로스”

보안적합성 검증,
빨리 통과하고 늦게 통과하는 데에는 다 이유가 있습니다.



비엔비솔루션(주)는 삼성전자(주)에서 분사한
보안장비 전문 방위산업체 입니다.

보조기억매체 보안 관리시스템 “SeProS” 특허등록



“씨프로스”의 보안USB는 특허등록으로 권리를
보호받고 있습니다. 본 특허를 침해한 유사
제품을 사용할 경우 불이익을 받을 수 있습니다.

대한민국 정보보안! 비엔비솔루션(주)이 새롭게 지켜가겠습니다.