[5C-107]

보조기억매체를 이용한 비밀 유출방지 대책

Protection Mechanism of Critical Information by Portable Storage Media

김현중[1], 김인중[1], 정윤정[1], 박진섭[2]
HyunJung Kim[1], InJung Kim[1], YoonJung Jung[1], JinSeop Park[2]
국가보안기술연구소[1], 대전대학교[2]
NSRI[1], Daejon University[2]

ABSTRACT

정보통신망에서 소통 및 처리되고 있는 전자자료의 유출경로는 정보통신망, 전자파, 보조기억매체 등 크게 3가지로 분류할 수 있다. 첫째 정보통신망의 경우 외부자의 해킹 또는 내부자가 고의적인 외부 유출이 이에 해당되는데 이에 대한 대책은 가장 활발하게 진행되고 있으며 또한 수법도 점차 지능화되어가고 있다. 둘째 전자파에 의한 유출은 원거리에서 복원기술이 용이하지 않아 현재 선진각국에서 관심을 가지고 있는 분야이며 방어기술 또한 초기 단계에 있다. 마지막으로 보조기억매체를 이용한 자료유출은 가장 원시적이고 간편한 전자유출 방법이지만, 기술적 대책을 포함하여 인적보안 등의 관리적 대책이 필요하다.

본 논문에서는 국방, 외교, 금융 등 민감한 정보의 안전성 및 신뢰성을 확보하기 위하여 개인 사용자가 사용하고 있는 각종 보조기억매체에 대한 보호 대책을 제시하고자 한다.

1. 서 론

비밀자료, 민감한 정보를 유통하는 정보통신망은 외부 이용자, 내부 사용자, 개발자 등으로부터 접근권한의 차등화를 통해 보호되어야 한다. 특히 외부 해킹으로부터의 차단과 내부 사용자로부터의 접근제어가 무엇보다도 중요하다. 먼저 외부 해킹에 대한 보호에 있어서는 비밀 정보가 저장되어 있는 내부 서버를 잘 관리해야 하는 데, 내부 서버에 대한 보안대책은 업무 목적이외의 기능 및 프로그램을 제거하고, 보안정책의 임의변경 금지, 일반사용자 계정 존재 여부 확인 및 환경 설정시 접근 허용 모드의 적합한 설정 등이 필수적이다. 내부 사용자로부터의 보호를 위해서는 내부 통제 직원의 직무를 분리하거나 확인·승인 절차를 강화하고, 보조기억매체를 통한 비밀 정보 복사 및 이동시 담당 부서장 및 책임자의 승인을 받도록 해야 한다. 또한, 주기적인 로그 분석을 통하여 불법 접근이 이루어졌는지를 점검하는 것도 필수적이다. 하지만 가장 중요한 것은 보조기억매체에 저장되어 있는 각종 비밀 데이터에 대한 관리이다. 보조기억매체 운용상의 관리 미숙으로 인하여 도난 및 유출이 발생하는 경우가 다수 있다. 이런 보조기억매체를 통한 자료유출로 인하여 조직에 상당한 피해 영향을 미치게 할 뿐 아니라, 실제 자료 유출자를 색인하는 것도 어려운 현실이다.

이에 본 논문은 보조기억매체내의 각종 비밀 자료에 대한 보호대책을 제시하고, 도난 및 매체에 대한 분실시 일어날 수 있는 전자자료 유출을 방지할 수 있는 관리 및 기술적 방안을 제시하기로 한다. 이를 통해서 보조기억매체에 대한 관리를 용이하게 하고 보조기억매체에 보관된 전자자료에 대한 신뢰성을 확보함으로써 보조기억매체를 이용한 국방 및 패쇄망의 비밀 자료 유통 방안에 대하여 제시하고자 한다.

2. 정보통신망의 환경분석

요즘 국방, 외교, 금융 등 민감한 자료를 유통하는 정통신망도 산하기관이나 상급기관과의 연동이 고려되고 있다. 하지만 연동에 따른 가장 큰문제점은 비밀이 유통되어야 하므로 물리적인 연결 및 연동은 많은 제약요소를 가지고 있다. 다만, 부분적으로 비밀을 소통할 수 있도록 비밀자료를 암호화하여 저장/관리하고 각종 시스템에 대한 침해사고를 예방하기 위하여 관련 보호시스템의 구축 등 환경에 따른 최선의 보호대책을 강구하고 제한적으로 비밀을 소통하고 있다고 판단된다.

또한 이러한 민감한 정보통신망에서도 대부분 보조기억매체를 사용하는데, 이런 보조기억매체를 이용한 자료복사 및 유출 등 위협요인이 상존하고 있어서 민감한 정보통신망에서 유통되는 전자문서 및 자료에 대한 유출방지 대책이 시급한 실정이다. 특히 보조기억매체는 설치가 용이하고 소형화, 대용량화, 고속화 및 소형화가