국회 네트워크 분리에 따른 보안 USB 메모리의 사용 문제점 및 보안 대책 연구

남원희* · 박대우*

*호서대학교 벤처전문대학원

A Study on Security Police against Problem of Using Secure USB according to National Assembly Network Separation

Won-Hee Nam* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : dlbongmt@na.go.kr · prof_pdw@naver.com

요 약

정부의 행정기관과 사법기관들은 정보보안을 위해서 네트워크 분리와 CERT를 구축하여 활용하고 있다. 하지만 입법부는 기본적인 보안시스템만을 갖추고 있어, 상대적으로 보안 취약점이 많다. 본 논문에서는 입법부인 국회와 국회사무처, 국회도서관에 대한 정보보안을 위한 연구를 한다. 국회 정보보안을 위한 네트워크 구성을 외부의 인터넷과 직접 연결된 인터넷 네트워크와 내부 업무 네트워크로 분리하는 것이다. 네트워크 분리에 따른 자료의 이동은 보안USB 메모리를 이용하는데, 사용자가 불편한 문제점을 가지고 있다. 문제점 분석과 보안USB 메모리 사용에 대한 보안 취약성 문제를 연구를 한다. 이를 개선하기 위한 사용자의 효율성 및 대책과 보안성을 강화하는 방안에 대해 연구한다.

ABSTRACT

The administration of government agencies and Law enforcement agencies is utilize. that network separation and Establish CERT for network security. However, the legislature has a basic security system. so a lot of relative vulnerability. In this paper, study for security National Assembly and the National Assembly Secretariat, at Library of National Assembly on legislative National Assembly for information security and network configuration, network and external Internet networks is to divide the internal affairs. Network separation in accordance with the movement of materials to use secure USB memory, the user has the uncomfortable issues. Problem analysis and security vulnerabilities on the use of USB memory is study the problem. User efficiency and enhance security.

키워드

National Assembly Security, Network Separation, Secure Universal Serial Bus, Vulnerability

Ⅰ. 서 론

대한민국을 대상으로 한 2009년 3.4 DDoS 공격 사건과 2011년 7.7 DDoS 공격 사건 및 검찰의 수사 발표가 있었던 농협 해킹사건 등으로 국가와 공공기관의 정보보호에 관한 중요성이 대두되고 있다.

하지만 정보보호 관련 법률이 국회에서 논의되고 있는 기관인 국회사무처의 정보보호컨설팅 결과는 61.2점으로 매우 낮게 평가 되었으며, H/W, S/W분야의 평가에서도 보안성이 취약한 것으로 나타났다[1].

저자들은 이전 논문[1]에서 국회와 국회사무처의 네트워크와 컴퓨터 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 분석하였으며, 입법지원 기관이 갖추어야 할 네트워크와 시스템을 위한 물리적 네트워크 분리, DDoS 공격 대응, Virus 공격 대응, 해킹 공격 대응 및 중요 시스템 보안과 사이버침해대응센터[2]를 위한 설계와 연구를 통해서 기밀성, 가용성, 무결성,

접근제어, 인증 등의 보안평가기준에 따라 분석을 하였다.

최근 국회와 국회사무처, 국회도서관에서는 네트워크와 시스템 보안성을 강화하기 위하여 물리적 네트워크 분리를 실행하고 있다. 이 결과 물리적 네트워크 분리에 따르는 보안성은 강화 되었으나, 국민들에게 서비스하는 공공기관인 국회의 업무 성격상 인터넷 네트워크에서 자료 사용이 많아 불편성과 비효율성이 늘어나고 있다.

행정업무를 처리하기 위해서, 인터넷 네트워크와 행정업무 네트워크에서 보안 USB 메모리를 사용하여, 정보자료의 이송과 보안을 실행하여야 하는데, 여기에 따르는 업무 사용자들에 대한 불편함이 나타나게 되어 사용자들의 불만이 폭주하게 되었다. 또한 이러한 불편함에 대한 일시적 적용으로 보안USB 메모리가 보안성을 보장하지 못하는 방향으로 사용이 왜곡되고 있는 문제점도 있다.

따라서 국회의 물리적 네트워크 분리를 실행으로 인한 보안USB 메모리 사용의 불편함을 분석하고, 불편함을 해소하면서 효율성을 강구할 할 수 있는 대책과 보안성 강화를 위한 방안에 대한 연구가 필요하다.

Ⅱ. 관련연구

2.1 물리적 네트워크 분리

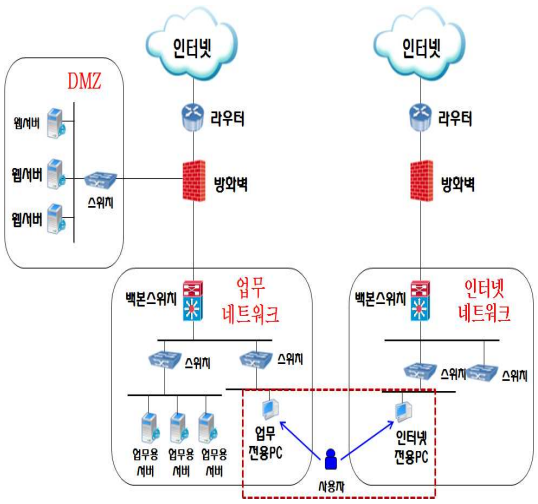

그림 1. 물리적 네트워크 분리

그림 1은 물리적 네트워크 분리를 나타낸 그림이다. 행정안전부의 정보통신보안업무규정에 의하면“제35조 (상용망 등 외부망 연동) ⑦ 행정기관의 장은 비밀을 취급하는 정보통신망 또는 제21조제1항의 규정에 따른 기반시설의 네트워크는 상용망과 분리·운용하여야 한다”[3].라고 되어 있다.

2.2 소프트웨어 기반 보안USB 시스템

USB 메모리 매체 내에 저장된 데이터를 보호하고 PC 상에서 USB 메모리 매체 사용을 통제하기 위해 소프트웨어로 구현된 보안USB 시스템을 의미한다.

보안USB 시스템은 그림 2와 같이 보안USB 시스템 운영환경에서 보안기능을 수행한다. 첫째, 보안USB 시스템은 USB 메모리 매체 내에 저장된 데이터가 노출되는 것을 보호한다. 둘째, 보안USB 시스템은 PC 상에 저장된 데이터를 USB 포트에서 비인가 보조기억매체를 통한 유출을 보호한다.

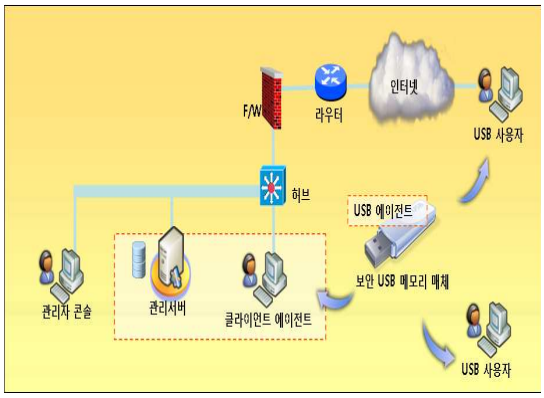

그림 2. 보안USB 시스템 운영환경

보안USB 시스템은 관리서버, 클라이언트 에이전트, USB 에이전트로 구성된다.

* 관리서버는 관리자가 요청하는 사항을 수행하고 USB 메모리 매체에 대한 등록, 폐기 등 USB 접근통제 목록을 관리하고, 읽기, 쓰기 등을 포함하는 USB 기능목록을 관리하고, 관리자의 보안역할을 관리한다. 관리서버는 조직에서의 USB 메모리 매체 반입 및 반출을 승인할 수 있다. 관리서버는 소프트웨어로 구현되어야 한다. 관리자가 설정하는 대부분의 정보들은 관리서버에 저장된다. 관리서버는 클라이언트 에이전트 감사기록 및 USB 메모리 매체 감사기록을 관리하고 관리자의 요청사항을 수행한다.

* 클라이언트 에이전트는 USB 포트에서 비인가 보조기억매체를 통한 PC의 데이터 유출을 보호하기 위하여 클라이언트 에이전트는 클라이언트 에이전트가 설치된 PC의 USB 포트에서 비인가 보조기억매체의 사용을 통제한다. 클라이언트 에이전트는 관리 서버로부터 통제를 받아 USB 메모리 매체의 반입 및 반출을 승인할 수 있다. 클라이언트 에이전트는 보안사건 발생 시 감사기록을 생성할 수 있으며 관리서버로 전송한다. 클라이언트 에이전트는 소프트웨어로 구현되어야 한다.

* USB 에이전트는 사용자에 대한 식별 및 인

증을 수행하고 USB 메모리 매체에 저장되는 데이터를 암호화한다. USB 에이전트는 비 인가된 사용자로부터 USB 데이터 유출을 방지하기 위하여 USB 데이터에 대한 접근통제를 수행한다. USB 에이전트는 보안사건 발생 시 감사기록을 생성하고 저장할 수 있으며 관리서버로 전송한다. USB 에이전트는 소프트웨어로 구현되고 보안 USB 메모리 매체에 탑재되며 PC에서 동작된다 [4].

Ⅲ. 네트워크 분리에 따른 보안 USB 메모리의 사용 문제점 분석

3.1 네트워크 분리와 보안USB 메모리 사용

그림 3과 같이 국회 네트워크를 외부 인터넷 네트워크와 연결된 인터넷 네트워크와 내부 업무 네트워크와 연결된 내부 네트워크로 물리적인 네트워크 분리를 하여, 외부로부터 해커의 공격이나, 침해사고로부터 내부 네트워크와 시스템의 보안성을 강화할 목적으로 수행한다.

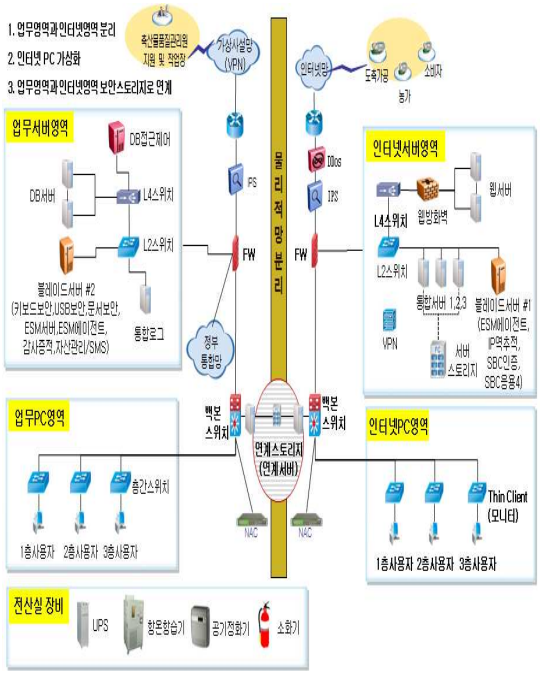

그림 3. 국회의 네트워크 분리 구성도

물리적인 네트워크 분리를 하면 업무를 위하여 외부의 인터넷 네트워크에서의 정보 자료의 송수신과 인터넷 접속이 제한되어 업무에 불편을 초래한다.

특히 국회도서관에서는 업무의 많은 부분이 인터넷 네트워크와의 연결에서 이루어져 심각한 내부 업무 사용자의 반발과 불편함을 호소하였다.

이러한 물리적인 네트워크 분리에 따르는 정보자료의 단절 및 이용 불편을 해소하기 위한 방안 중의 하나가 보안USB 시스템이다. 보안USB 시스템은 인터넷 네트워크에서의 정보자료를 업무 네트워크로 이송하거나, 내부 업무 네트워크에서 인터넷 네트워크에 자료를 메일로 전송하거나, 이송하는 데 사용된다.

3.2 보안USB 메모리 사용자 불편 분석

실제 국회 인터넷 네트워크 PC에서 내부 업무 네트워크 PC로 자료 이송을 위하여 보안 USB 메모리를 사용하여 정보자료를 전송하는 프로세스를 분석 해 보았다. 자료 이송 프로세스는 자료 검색과 작성 → 대상 정보 저장 → 보안USB 삽입 → 보안USB 인증 → 정보 저장 → 보안USB 삽입→ 정보 이송 인증→ 백신검사 및 정보 이동 → 정보 메일에 첨부 → 정보 전송 등 9~10단계를 거쳐야 한다.

보안USB 메모리를 사용하는 국회사무처나 국회도서관의 일반 업무 담당자가 프로세스를 수행할 때, 약 10M byte 정보 전송에 적게는 2~3분, 많게는 10분~20분 이상이 소요되며, 승인이 늦어지는 경우 대기시간으로 인한 업무 공백과 수작업에 의한 정보자료 이동업무에 대한 불편으로 정보자료 이송 수행을 미루는 사태도 발생하는 것으로 조사 되었다.

또한 보안USB 관리시스템 및 전용 클라이언트 프로그램의 오류 또는 장애가 발생 할 시에는 보안USB와 메모리 사용에 제약이 발생한다.

또한 업무 담당자들은 보안USB 메모리를 개인별로 관리해야 하며, 보안USB 메모리 저장 공간을 확보하기 위해 주기적으로 저장된 자료를 선별하고 삭제해야 하는 불편함이 발생하고 있다.

3.3 보안 USB 메모리의 취약점 분석

또한 보안USB 메모리를 통한 업무 프로세스에서 보안 취약점으로는, 보안USB 메모리를 개인이 관리하다 보니, 반출•입 절차에 대한 관리와 통제가 어렵고 부실해서, 업무 사용자가 임의로 데이터를 유출하는 것이 가능하다.

또한 접근통제를 위한 승인체계가 갖추어져 있지 못해서, 이동성이 쉬운 보안USB 분실 시에 취득자에 의한 고의적인 바이러스 감염으로 인한 네트워크와 시스템에 대한 바이러스 확산 문제가 있다.

또한 보안USB 클라이언트 소프트의 무력화와 정보자료에 악성코드를 은닉하여, 내부 업무 네트워크의 감염으로 인한 정보 유출과 백도어를 발생시켜, 내부 네트워크에 대한 해킹공격의 위험 등의 취약점이 분석되고 있다.

Ⅳ. 보안USB 메모리 사용의 불편 대책 및 보안성 강화 방안

물리적인 네트워크 분리로 인한 내부 업무 네트워크와 외부 인터넷 네트워크의 정보자료의 이송과 연동 문제를 위해서는 다음과 같은 불편 대책이 필요해 보인다.

또한 국가정보원이 제시한 '국가·공공기관 내부 네트워크와 인터넷 간 안전한 자료 전송 보안 가이드라인'을 준수하도록 시스템을 구축하여 운영하여야 한다.

4.1 보안USB 메모리 사용의 불편 대책

우선 내부 네트워크와 외부 네트워크의 연계 스토리지를 활용하여 보안 USB 메모리의 9~10단계로 이루어진 정보자료를 전송하는 프로세스를 줄여야 한다.

또한 인증과 승인 시스템을 체계화하여 실시간으로 승인, 결재되면서, 취약점 점검과 바이러스 검사 등이 이루어지면서, 감사기록 등이 저장되는 시스템으로 바뀌어야 한다.

이 결과로 인한 업무 네트워크와 인터넷 네트워크에서 메일 및 정보자료의 전송 구현이 쉽게 이루어지는 효율성을 갖추어야 한다.

4.2 보안성 강화 방안

물리적인 네트워크 분리로 인한 내부 업무 네트워크와 외부 인터넷 네트워크의 정보자료의 이송과 연동 문제를 위해서는 보안성 강화를 위한 대책은 다음과 같다.

* 업무 네트워크와 인터넷 네트워크 간 정보자료의 상호 전송시스템을 구축하여 상시 보안시스템을 유지한다.

* 업무 네트워크와 인터넷 네트워크 간 정보자료의 상호 전송을 할 때에는 공인인증서에 의한 사용자 인증 및 보안 등급에 따라 암호화 전송과 무결성 검증, NAT등을 이용한 접근통제 및 로그 감사기록의 실시간 저장 시스템을 구축하고, CERT와 연계하여 상시 보안시스템을 유지한다.

* 업무 네트워크에서 인터넷 네트워크로 정보자료의 전송 시에는 실시간 승인 시스템을 구축하도록 한다.

* 업무 네트워크와 인터넷 네트워크 간 전송된 정보자료에 대한 모든 로그기록을 보관 관리하여 감사기록의 보관과 포렌식 자료로 활용 할 수 있도록 한다.

* 업무 네트워크와 인터넷 네트워크 간 정보자료의 전송 시 악성코드와 바이러스를 실시간으로 검사하여 차단하고 백신으로 치료하도록 한다.

Ⅴ. 결론

본 논문에서는 입법부인 국회와 국회사무처, 국회도서관에 대한 물리적인 네트워크 분리에 따른 보안USB 메모리 사용에 있어서 사용자의 불편한 문제점을 분석하였다. 또한 보안USB 메모리 사용에 대한 보안 취약성 문제를 연구를 하여, 이를 개선하기 위한 사용자의 효율성 및 대책과 보안성을 강화하는 방안에 대해 연구하였다.

향후 연구는 보안USB 메모리 사용에 대한 대책 수립한 후에 실시간 전보전송 보안 시스템에 대한 검증과 보안성을 검증하는 연구가 필요하다.

참고문헌

[1] 남원희, 박대우, "입법기관의 보안강화를 위한 Cloud 네트워크 분석 및 보안 시스템 연구," 한국해양정보통신학회논문지, 제15권 6호, 2011년 6월.

[2] 김선태, 박대우, 전문석, "정량적 침해사고 관리를 위한 Security Ticket 기반의 CERT/CC 설계 및 관리," 한국컴퓨터정보학회논문지, 제12권 제4호, 2007년 9월.

[3] "제35조(상용망 등 외부망 연동)," 정보통신 보안업무규정, 행정안전부, 2009년 6월.

[4] 최희봉, 나학연, 박종욱, "소프트웨어 기반 보안USB 시스템 보호프로파일," 국가보안기술연구소, V1.0, 2010년 4월.