입법기관의 보안강화를 위한 Cloud 네트워크 분석 및 보안 시스템 연구

남원희* · 박대우**

A Study on Cloud Network and Security System Analysis for Enhanced Security of Legislative Authority

Won-Hee Nam* · Dea-Woo Park**

요 약

3.4 DDoS 사건과 농협 해킹사건 등으로 국가기관의 정보보호에 관한 중요성이 대두되고 있고, 정보보호 관련 법률이 국회에서 논의되고 있다. 하지만 국회사무처의 정보보호컨설팅 결과 61.2점으로 매우 낮게 평가 되었으며, H/W, S/W분야의 평가에서도 보안성이 취약한 것으로 나타났다. 본 논문은 입법지원 기관인 국회와 국회사무처의 네트워크와 컴퓨터 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 분석한다. 그리고 입법지원 기관이 갖추어야 할 네트워크와 시스템을 위한 물리적 네트워크 분리, DDoS 공격 대응, Virus 공격 대응, 해킹 공격 대응 및 중요 시스템 보안과 사이버침해대응센터를 위한 설계와 연구를 통해서 기밀성, 가용성, 무결성, 접근제어, 인증 등의 보안평가기준에 따라 분석을 한다. 본 연구를 통해 입법지원기관의 보안 강화를 위한 자료와 보안관련법 제정을 위한 기초자료를 제공하고자 한다.

ABSTRACT

National institutions on the importance of information security is being recognized, information security laws are being discussed in Congress 3.4 DDoS incident and Nonghyup hacking, etc. However, National Assembly Secretariat when the results of the Information Security Consulting has been assessed very low 61.2 points, evaluation of hardware and software in secure areas were vulnerable. This paper, the legislative support agencies National Assembly and National Assembly Secretariat on the network and computer systems, and managerial, technical and physical security elements are analyzed for the status. And network should have the legislative support agencies and system for the physical network separation, DDoS attack response, Virus attack response, hacking attacks response, and Cyber Emergency Response Team/Coordination Center for Cyber infringing design and research through the confidentiality, integrity, availability, access control, authentication and security analysis is based on the evaluation criteria. Through this study, the legislative support agencies to strengthen the security of data and security laws enacted to provide the basis for.

키워드

입법기관, 보안평가기준, 공격 대응, 보안 시스템, 사이버침해대응센터

Key word

Legislative Agencies, Security Evaluation Standards, Attack Response, Security Systems, Cyber Emergency Response Team/Coordination Center

* 정회원 : 호서대학교 벤처전문대학원 IT응용기술학과(제1저자)
** 종신회원 : 호서대학교 벤처전문대학원 IT응용기술학과
(교신저자, prof1@paran.com)

접수일자 : 2011. 05. 27
심사완료일자 : 2011. 05. 27

Ⅰ. 서 론

대한민국의 입법기관인 국회는 많은 부분이 전자화 되어 있으며 입법관련 많은 정보들이 DB화 되어 관리되고 있다. IT강국인 대한민국의 국회로서, 국회 본 회의장을 세계 최초로 첨단 디지털 국회로 바꾸었고, 시각과 청각 장애 의원들을 위한 시설도 설치하였다[1].

국회홈페이지를 통해서 국회에서 진행되는 모든 회의록을 PDF 형식으로 확인할 수 있고, 국회의 본회의・예결위・상임위 및 주요 청문회・공청회, 국정감사 등에 대해 인터넷 생중계로 볼 수 있으며, 관련자료 또한 디지털 파일 형태로 제공 받을 수 있다[2].

국회의 특성상 국민을 위한 많은 정보의 제공을 목적으로 하고 있는 국회 네트워크 시스템은 개방성을 가질 수밖에 없으나, 개방성은 외부의 불법적인 해킹[3]에 쉽게 노출이 되는 취약점을 안고 있다.

최근 7.7DDoS 공격사건에서 문제가 되었듯 정보장애, 개인정보 유출이 빈번하게 발생되고 있다[4]. 또한 국회 네트워크의 개방적 특성상, 국회의원 및 그 보좌진 등에 대해서도 무차별 해킹과 정보침해 사례들이 발생할 수 있으며, 또한 입법기관인 국회의 행정을 주관하는 국회사무처에서 국회의 보안에 대한 책임을 가져야만 한다.

하지만 국회사무처의 정보보호컨설팅 결과 61.2점으로 공공기관의 보안성 평가 중에서도 매우 낮게 평가되었다. 또한 H/W, S/W분야의 평가에서도 보안성이 취약한 것으로 나타났으며, 특히 정보보호 인식과 행동지침 준수 설문조사에 비추어 국회사무처 직원의 정보보안 인식과 행동지침 준수 정도는 낮은 것으로 평가되었다.

본 논문은 입법지원기관인 국회사무처의 인터넷 네트워크와 사용 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 기밀성, 가용성, 무결성 등의 보안기준에 따라 파악하고, 이를 분석한다. 그리고 입법지원 기관이 갖추어야 할 인터넷 네트워크에서 물리적 네트워크 분리, DDoS 공격 대응, Virus 공격 대응, 해킹 공격 대응을 통한 중요 시스템 보안 및 사이버침해대응센터를 위한 설계와 연구를 한다.

본 연구의 결과는 입법기관인 국회와 연관기관의 보안에 대한 기초자료로 활용되어, 국가 사이버침해와 외부의 해킹 공격 등에 능동적으로 대처할 수 있는 방안을 마련하는 초석이 될 것이다.

Ⅱ. 관련 연구

2.1. 보안시스템

컴퓨터 시스템과 네트워크의 중요 정보 자원을 공격자로부터 보호하고 안전한 인터넷에 사용을 하기 위한 시스템을 보안시스템이라 한다.

따라서 침해가 발생하지 않도록 서버, 네트워크를 방어하는 역할을 하여야 하며, 보안 관리자는 보안시스템으로부터 침입자 또는 침입을 시도하는 공격자에 대한 정보를 확인할 수 있고, 공격에 대응하여, 중요정보자원을 안전하게 관리할 수 있어야 한다[5].

- Virus Wall은 시스템에 감염되는 Virus와 악성코드를 검색하고 검색된 Virus를 치료 할 수 백신을 갖춘 정보보호시스템이다.
- 침입차단시스템(Firewall)은 방화벽으로 외부 네트워크로부터 불법적인 침입으로부터 내부 네트워크를 보호하기 위하여 게이트웨이에 설치되는 접근제어, 패킷필터링, NAT을 수행하는 정보보호 솔루션이다[6].
- 내부 네트워크에서 발생하는 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 침입탐지시스템(Intrusion Detection System)이 있다.
- 가상사설망(Virtual Private Network)은 기존의 인터넷 망을 이용해 터널링과 암호화를 수행하는 전용망과 같이 사용 할 수 있는 시스템이다.
- IDS에서 탐지된 비정상적인 트래픽을 중단시키는 공격 중단 기능, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 침입방지시스템(Intrusion Prevention System)[5]이 있다.
- 침입차단시스템, 침입탐지시스템, 가상사설망 등의 보안 솔루션의 패킷을 통합 관리하는 통합관제시스템(Enterprise Security Management)은 보안솔루션 간의 네트워크보안 정책을 수립할 수 있는 통합보안관리 시스템이다.

2.2. 보안평가기준과 보안요소

보안강화를 위해 접근제어, 사용자인증, 가용성, 보안성, 기밀성 등 보안평가기준을 마련하여 등급에 맞는 보안시스템과 보안인적자원을 확보하도록 하여야 한다.

컴퓨터 범죄의 80% 이상이 인적 소행으로 나타나고 있어, 내부의 운영요원과 사용자에 대한 보안교육과 ID 및 패스워드의 인증 관리 부여체계 확립과 생성 관리를 통해, 전자서명과 지문인식 등 사용자보안을 강화하고, 사용자 정보의 보안 관리와 보안정책 변경체계를 정립시킨다.

2.3. Cloud Computing

사용자가 언제 어디서나 인터넷 접속을 통하여 IT 자원을 제공받는 주문형 IT 서비스를 뒤미한다. Cloud Computing 서비스는 인터넷의 급속한 확산과 웹 2.0 진화에 따른 IT 환경의 확장 요구에 부응하여 등장했다. Cloud 서비스는 IT 자원을 '개별소유 방식에서 공유방식으로 전환해 관련 비용을 절감하고, 업무의 시간적 · 공간적 제약을 없앰으로써 업무방식도 변화시켰다. 정부와 기업의 Cloud 서비스 도입 확대로 Cloud 서비스의 전 세계 시장규모가 2009년 796억 달러에 달했으며, 2014년에는 3,434억 달러로 연평균 34%씩 급성장할 것으로 예상된다[7].

Ⅲ. 입법기관의 네트워크 및 보안시스템 분석

3.1. 네트워크와 시스템 분석

입법기관의 네트워크는 국회, 국회사무처, 국회도서관, 법제처 등으로 구성되어 있으며, 그림 1의 국회 정보공개시스템처럼 상호 연결이 되어 있다.

또한 국회사무처, 국회도서관, 국회예산정책처, 국회입법조사처의 4개 기관이 정보공개 청구에 대한 상태를 조회하며 정보공개 업무를 총괄하는 기능을 가지도록 구성되어 있다.

입법기관 네트워크는 그림 2의 국회 본회의장 네트워크처럼 각각의 입법기관 내부 시스템들과 연결되어 있다.

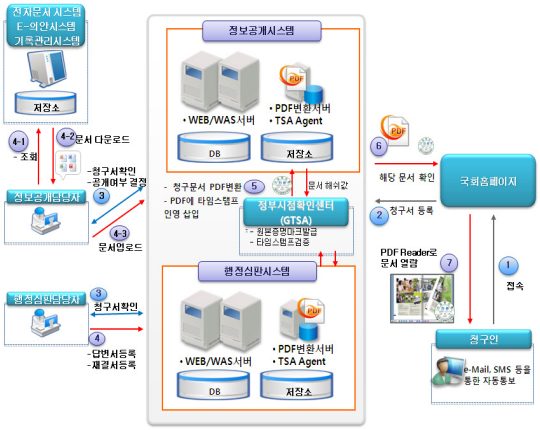

그림 1. 국회 정보공개시스템의 연결
Fig. 1. Connection of National Assembly Information Open System

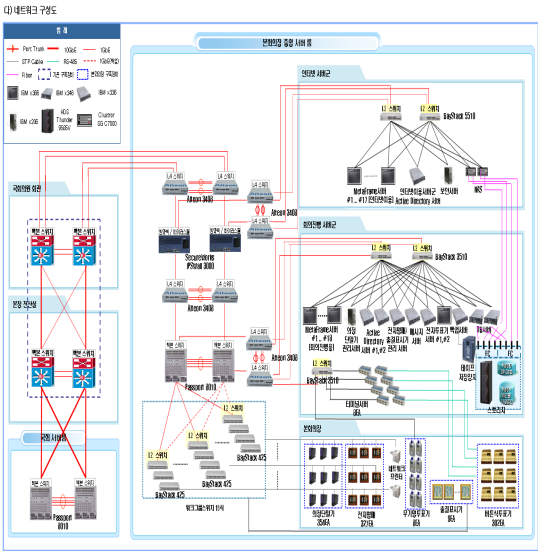

그림 2. 국회 본회의장 네트워크 구성
Fig. 2. Network configuration of National Assembly Main Chamber

입법기관의 시스템은 국회도서관 정보시스템 , 입법지식 DB 시스템, 국회도서관 홈페이지 시스템, 국회사무처 시스템 및 법제처 법령정보센터 시스템으로 구성되어 있다.

3.2. 홈페이지 분석

입법기관은 각각의 홈페이지를 구축하여 독립적으로 관리되고 있으며, 국회 입법정보는 국회 도서관과 국회 전자도서관을 통해 일반에게 공개되고 있다. 예를 들면 국회도서관의 홈페이지는 주요정보서비스, 각종 서비스 안내, 주요 공지사항, 행사 안내 등 대국민 정보 서비스 제공하며 보면 다음과 같이 구성되어 있다.

- 웹서버 : WebtoB 4.1.2.0, JEUS 5.0.0.26
- 검색엔진 : K2 Toolkit(ver.6)
- DBMS : Informix 11.50
- 검색시스템 : 웹검색
- 원문제공도구 : 국회도서관 통합뷰어
- 개발언어 : Java, PHP

그림 3의 국회 전자도서관 시스템 구성처럼 국회 전자도서관 시스템 - 도서관업무 통합관리 시스템 - 국회도서관 홈페이지 - 법률도서관 시스템의 각각 홈페이지는 서로 연결되어 있는 것으로 파악되었다.

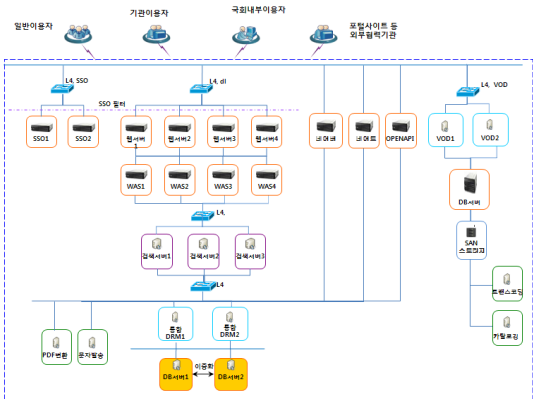

그림 3. 국회 전자도서관 시스템 구성
Fig. 3. Configuration of National Assembly Electronic Library System

3.3. 보안 내용 분석

- 웹 접근성 준수 : 웹 표준의 적용 및 관련 지침 준수를 통하여 웹 접근성 적용하며, '인터넷 웹 콘텐츠 접근성 지침(국가표준, '05.12)' 준수 및 적용하고, '웹 접근성 향상을 위한 국가표준 기술 가이드라인('09.03)과 '한국형 웹 콘텐츠 접근성 지침 2.0' 및 W3C 표준 준수하고 있다.
- 접속 이력 기록 : 시스템 접속 ID, 접속일시 및 로그아웃 일시, 접속 IP 등을 기록하고 있다.
- 인증 : 접속 시에는 대한 본인 확인(공인전자서명, G-pin 인증) 후 온라인 서비스 이용 가능하다.
- 암호화 : 주민등록번호, 비밀번호 등의 개인정보는 암호화하여 DB에 저장하며, 이에 대한 암호화. 복호화 방안을 구체적으로 명시하고 있다.
- 정보보호 : 국회사무처에서 제시하는 「국회정보시스템 보안가이드라인」, 「웹 어플리케이션 보안 개발 가이드라인」을 준수하고 있다.

3.4. 내용 분석에 따른 개선 검토

- 목표시스템 부합성 - 기능 및 성능 충족도를 감안하여 통합 목표시스템을 구성하여야 한다.
- 홈페이지는 국내, 국외의 표준을 준수하도록 개선되거나 새로 개발되어야 한다.
- 최신 기술을 적용하여야 한다.
- 향후 국회의 발전방향을 고려한 단계별 확장성 및 발전방향을 반영하여야 한다.
- 외부의 DDoS 공격이나 해킹 공격 등을 대비한 안정성을 강화한 대용량 트래픽 수용 및 보안 네트워크와 보안 시스템에 대한 장비를 구성하여야 한다.
- 보안장비는 CC인증 및 국정원 인증 장비와 보안 솔루션으로 하여야 한다.

Ⅳ. 입법기관의 보안강화를 위한 Cloud 네트워크 및 보안시스템 연구

4.1. 네트워크 보안 강화

4.1.1. 물리적 네트워크(업무망, 인터넷망) 분리

그림 4처럼 내부 망 분리는 논리적 망 분리로 구성한다. 서비스 연계 영역 부분은 DDoS방어장비, IPS, 침입차단시스템, VPN, ESM, TMS(Threat Management System), 웹방화벽 등 네트워크 보안 시스템 각각에 랜카드 2개 이상의 내·외부 네트워크 접점을 분리하여 접근제어, 사용자인증, 보안성을 강화한다.

또한 L4스위치, L2스위치, 프락시(Proxy), 콘텐츠 필터링, White/Black List 활용 보안 정책 서버 등을 구성하

여 외부의 공격으로부터 가용성과 보안성을 확보하고 VPN을 이용한 내부, 외부 DB자료의 암호화 전송과 접속을 통해 기밀성 한다.

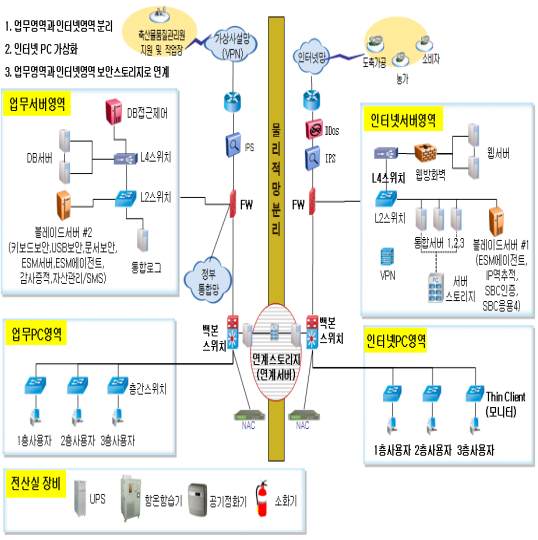

그림 4. 네트워크 분리 시스템 구성도
Fig. 4 Consist of Network Isolation System

4.1.2. 네트워크 DDoS 공격 대응

네트워크 DDoS 공격이 실시되면 L4스위치, L2스위치로 네트워크 트래픽 가용성을 확보하고, 공격감지 및 차단을 실시간으로 공격대응을 하기 위한 DDoS 공격 대응 시스템을 준비한다. DDoS 공격의 좀비PC(Zombi PC)가 추가적으로 감염되는 것을 차단하고, 연속적인 서비스 거부공격이 자동으로 탐지되고, DDoS의 숙주가 되는 봇넷(Botnet)시스템을 자동으로 차단 및 악성코드 전파를 위하여 주변시스템으로 웜 및 ARP Spoofing을 이용한 전파 공격시도를 차단한다.

DDoS 공격패킷에 대한 트래픽을 네트워크 앞단과 중간단으로 우회하고, DDoS 공격 차단과 동시에 실시간으로 공격 패킷을 수집하고 국정원 등 정보보호센터와 연계하여 DDoS 공격 사이버 대피소로 연결 설정하면서, 공격로그는 DDoS 공격 CERT기관과 협조하여 로그 분석 및 공격 근원지 및 좀비PC 차단에 대한 로그 기록을 감사기록으로 보관한다.

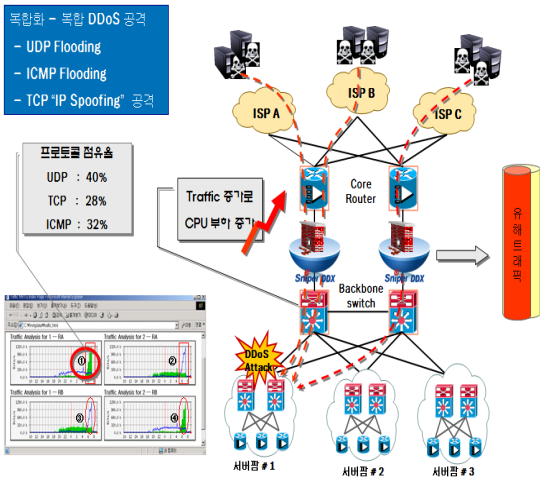

그림 5. DDoS 공격대응
Fig 5. DDoS attack response

4.1.3. Virus 공격 대응

네트워크와 시스템에 대한 Virus 공격 대응을 위해 컴퓨터 시스템을 감염시키는 Virus, Worm, 트로이목마, Zeroday Attack, 스파이웨어, 애드웨어, 루트킷, 해킹도구 등 다양한 악성코드를 이용한 Virus로부터 시스템을 보호하고, 새로운 Virus의 증상은 즉시 CERT/CC 등과 협조하여 실시간 Virus 코드 분석이나, 리버스 엔진니어링을 통해 백신을 생산하고, 백신의 업데이트로 Virus 동작중지 및 삭제를 통한 악성코드를 탐지 및 차단하며, 로그는 저장하여 관리하도록 한다.

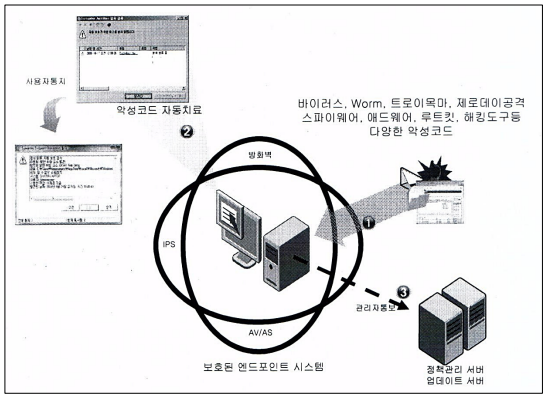

그림 6. Virus, Worm 등 악성코드 차단관리
Fig 6. Virus, Worm etc. malware protection management

4.2. 해킹 공격 대응

- 사용자 인증기능은 네트워크와 시스템에 접근하는 모든 사용자가 접근제어와 사용자 보안 인증을 받기 위해 공인인증 및 대체 인증을 받도록 하며, ID, 패스워드의 보안관리가 필요하다.
- PC 보안점검 및 조치를 주기적으로 실시한다. 백신과 보안패치 설치 및 최신상태 유지, 필수/비인가 SW 설치 여부 등 사용자 단말기 상태 조사 및 자동설치, 설치유도 가능하도록 한다.
- 네트워크 접근 제어 기능을 보안등급에 따라 실시하여, 유/무선 환경에서의 인가되지 않은 사용자 및 장비에 대해 탐지 및 차단하도록 한다.
- 비정상 트래픽 제어 기능은 사용자 단말에서 발생하는 p2p, 불법 인스턴트 메시지 포함한 이상 트래픽에 대한 탐지 및 차단이 가능하도록 한다.

4.3. 인적 보안 강화

CSO(Chief Security Officer), 사이버침해대응센터(CERT/CC) 책임자와 부서의 보안책임자는 사용자에 대한 보안서약서 집행, 정보보호 교육 및 수시/정기 보안점검 등을 실시하여야 하며, 특히 보안 점검관리업체에서는 철저히 계획에 의한 수행을 해야 한다.

문서 및 전산자료 보안을 위해 정보통신망 구성도, 정보시스템 구성도, 용역사업 산출물 및 개인정보 등은 비공개 자료로 분류하여 관리해야 한다.

최근 문제가 되고 있는 외부 용역 업체의 사업기간 중 과업수행에 필요한 전산장비인 PC. 노트북. 디지털복합기의 무단 반입과 출입을 금하며, 내부에 사용시에는 완전히 포맷하고 내부에서 다시 정상 보안 프로그램을 셋팅하여 사업에 참여하고, 과업 후에 포맷하여 보안관리를 준수한다. 사업 참여 인력은 외장형 HDD, USB 및 CD/DVD 등의 보조기억 매체를 사용 할 수 없다. 필요시 통합센터의 사전 승인을 거쳐야 한다.

4.4. 중요 시스템 보안 강화

국회사무처의 중요 자료인 DB에 대한 보안 강화를 위하여 DB 암호화를 한다. DB 암호화는 국정원에서 CC 인증을 받은 국가용 암호제품으로 제공해야하며, DBMS 내 중요 데이터를 칼럼 단위로 선택적 암호화 기능을 제공한다. 초기 및 운영 중 암호화 적용시 서비스가 중단되지 않아야 한다. 암호화 후 Index검색 기능을 통한 암호화 적용 후 Application 성능이 보장 되어야 한다. 암호화, 복호화 시 시스템 부하를 최소화 하여야 한다. DBMS 이중화(RAC, HA) 및 분산 Application 환경을 지원한다. 다양한 암호화 알고리즘(SEED, 3DES, AES, ARIA, SHA1)을 제공하여야 한다.

4.5. Cloud 네트워크 컴퓨팅 보안

국회사무처에 Private Cloud 네트워크와 Cloud시스템을 설치하여, 전국의 국회의원의 사무소 및 국회 내부의 본관, 국회도서관, 국회사무처, 의원회관에 대한 Cloud 서비스를 실시한다.

Cloud 서비스를 통해 국회 관련 사용자는 Private Cloud에다 VPN 기능을 추가하여 국내, 지방, 해외에서 Cloud 서비스 통합센터에 보안접속이 가능하다. 이때 Cloud 네트워크 컴퓨팅 패킷에 대한 실시간 모니터링과 접근제어, 사용자 인증을 통해 자료의 무결성, 기밀성 보안성을 확보한다.

4.6. 사이버침해대응센터 구축

사이버침해대응센터의 통합보안관제 시스템은 국회에서 생성되는 이벤트 모니터링 및 지방과 해외에서의 침해등급 산정, 사고접수 및 대응 조치 이력 등을 종합적으로 관제 할 수 있는 침해분석대응 기반 구축하여야 한다.

사이버침해대응센터는 정보자산 및 취약점 연동, 위험지표 및 수준지표의 평가와 관리 및 사고접수 단위로 위험등급 산정 및 기관 위험등급 산정 등의 종합적이고 체계적인 위험관리 체제 기반 구축하여야 한다.

사이버침해대응센터에서는 서버 등 중요정보자산에 대한 실시간 모니터링을 통해 트래픽을 감시하고 실시간 바이러스 스캔을 통해 바이러스 감염 여부를 탐지하고, 치료하고, 파일에 암호화 전송을 하여 무결성 검증을 위한 백업을 하게 된다.

접근제어는 Cloud 서비스 통합센터와 국회의 모든 서버에 자료를 열람하는데 보안 등급을 적용하여 자료를 관리해야 한다. 보안 등급을 통한 접근제어에서 공인인증서를 통한 사용자 인증을 통해 사용자의 신분과 보안 등급에 맞는 자료에 대한 읽기, 쓰기, 실행의 권한을 행사하게 된다.

V. 결 론

본 논문은 입법지원 기관인 국회와 국회사무처의 컴퓨터 시스템과 네트워크의 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 분석하였다. 분석 후에 입법지원 기관이 갖추어야 할 인터넷 네트워크에서 물리적 네트워크 분리, DDoS 공격 대응, Virus 공격 대응, 해킹 공격 대응을 통한 중요 시스템 보안 및 사이버침해대응센터를 위한 설계와 연구를 하여 기밀성, 가용성, 무결성, 접근제어, 인증 등의 보안평가 기준에 따라 파악하였다. 본 연구를 통해 입법지원기관의 보안 강화를 위한 자료를 제공하고, 정보보안을 위한 관련 근거 법규가 제정 되었으면 한다.

향후 연구로는 국회사무처 직원들의 정보보호 인식에 관한 조사와 H/W, S/W적인 관리적, 기술적, 물리적 보안시스템에 대한 시설과 정보보호 제도의 준수 및 보안 시스템 운용에 대한 분석과 평가를 하여, 직원들에 대한 보안교육과 현장의 보안 의무 사항 준수 지침을 만들어 실시한 후에 결과에 대한 분석이 필요하고, 이 결과를 통해 정보보호 관련법을 제・개정하는 것에 대한 연구가 필요하다.

참고문헌

[1] Young-Il Park, [Anniversary of founding a special interview] Won-Ki Kim Chairman, *Daily Seoprise*, Nov. 2005.

[2] Internet Broadcasting System, http://assembly.webcast.go.kr/, April 2010.

[3] Dea-Woo Park, Moon-Suk Jun, "The Analysis of New Video Conference System for Secure Communications," *Journal of International Transaction on Computer Science and Engineering,* Vol.2, No.1, pp.200-214, March 2005.

[4] Wan Choung, "A Study on Victims and Legal Response against the Internet DDoS Attack," vol.18, no.1, pp.207-228, 2010.

[5] Dea-Woo Park, Seung-In Lim, "A Study of the Intelligent Connection of Intrusion prevention System against Hacker' Attack," *Journal of The Korea Society of Computer and Information*, vol.11, no.3, pp.351-360, 2006.

[6] Dea-Woo Park, Woo-Sik Jung, "The study of performance evaluation between 32bit and 64bit K4 Firewall System," vol.8, no.1, Mar. 2003.

[7] 최우석, "클라우드 컴퓨팅 서비스 전개와 시사점," SERI 경영 노트, 제67호, 2010.

저자소개

남원희(Won-Hee Nam)

1987년 서울시립대학교 경영학과(경영학사)
2004년 경희대학교 법학대학원 공법학과 (법학석사)
2009년~현재 호서대학교 벤처전문대학원 IT응용기술학과 (박사과정)
현재 국회사무처 지식경제위원회 부이사관
※관심분야 : 개인정보보호법, IT Convergence, 정보보호, 네트워크 보안

박대우(Dea-Woo Park)

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과(공학박사)
2006년 정보보호진흥원(KISA) 선임연구원
2007년~현재 호서대학교 벤처전문대학원 조교수
※관심분야 : 정보보호, 유비쿼터스 네트워크 및 보안, 보안시스템, CERT/CC, Forensic, Hacking, VoIP보안, 이동통신 및 WiBro 보안