입법기관의 보안성 평가와 정보보호 인식 연구

남원희* · 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study on Evaluation of Information Security Awareness and Security Level about Legislative Authority

Won-hee Nam* · Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

E-mail : *dlbongmt@na.go.kr · *prof1@paran.com

요 약

최근 7.7 DDoS 사건과 해킹 사건 등으로 정보보호에 관한 중요성이 대두되고 있고, 정보보호 관련 법률이 국회에서 논의되고 있다.

본 연구에서는 입법지원 기관인 국회사무처를 중심으로 인터넷 네트워크와 사용 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 기밀성, 가용성, 무결성 등의 보안기준에 따라 파악하고, 이를 분석한다. 또한, 인터넷 네트워크와 사용 시스템 등을 주로 이용하는 입법 지원기관인 국회사무처 직원들의 정보보호에 대한 인식 및 정보보호에 관한 행동지침 준수에 대한 설문조사를 하고, 이에 대한 분석을 한다. 이를 통하여 입법지원기관의 보안 현황을 분석하고, 사회적인 책임기관으로서 역할을 고취시키고자 한다.

ABSTRACT

7.7 DDoS incident due to recent events and the emerging importance of privacy and Privacy laws are being discussed in the National Assembly.

In this study, Legislative Assembly Secretariat support organization focused on using the system, such as the Internet network and the administrative, technical and physical security elements on the status of confidentiality, availability, integrity and security criteria to identify and follow and We are analyzing. In addition, the Internet, including network and use the system primarily for use, Legislative support agency, The National Assembly Secretariat staff awareness about information security and privacy on the survey for compliance with codes of conduct and We are analyzing. Through this analysis of legislative support agencies' security status, and social responsibility as an institution will wish to encourage the role.

키워드

정보보호, DDoS, 보안성 평가, 입법기관, 보안기준

Ⅰ. 서 론

IT강국인 대한민국의 입법기관인 국회는 많은 부분이 전자화 되어 있으며 입법관련 많은 정보들이 DB화 되어 관리□지원되고 있다. “세계 최초로 국회 본 회의장을 첨단 디지털 국회로 바꾸었고, 시각과 청각 장애 의원들을 위한 시설도 설치해 주목 받기도 했다”[1].

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

국회의 특성상 국민을 위한 많은 정보의 제공을 목적으로 하고 있는 국회 네트워크 시스템은 개방성을 가질 수밖에 없을 것이며, 개방성은 외부의 불법적인 해킹에 노출이 되는 취약점을 안고 있다.

그림 1. 인터넷의사중계시스템

최근 7.7DDoS 공격사건[3]에서 문제가 되었듯 정보장애, 개인정보 유출이 빈번하게 발생되고 있다. 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.

본 논문은 입법지원기관인 국회사무처 직원들의 정보보호 인식에 관한 조사를 한다. 또한 국회사무처의 H/W, S/W적인 관리적, 기술적, 물리적 보안시스템에 대한 시설과 정보보호 제도의 준수 및 보안 시스템 운용에 대한 분석과 평가를 하여 본다.

본 연구의 결과는 국회의 보안에 대한 기초자료로 활용되어 국가의 사이버침해 등에 능동적으로 대처할 수 있는 방안을 마련하는 초석이 될 것이다.

II. 관련연구

2.1. 정보통신기반 보호법과 해킹 공격

표 1. 7.7 DDoS 공격에 의한 국내 피해사항

구분	일자	피해사이트				계
1차	7.7.18:00 ~ 7.8.18:00	청와대 국방부	옥션, 조선일보, 네이버, (메일)		외통부, 국회, 한나라당, 농협, 신한은행, 외환은행, 네이버(블러그)	12
2차	7.8.18:00 ~ 7.9.18:00	청와대 국방부		전자민원 G4C 다음(메일) 파란(메일) 국민은행	기업은행, 하나은행, 우리은행, 국가사이버안전센터, 알툴즈, 안철수 연구소	15
3차	7.9.18:00 ~ 7.10.18:00			다음(메일) 파란(메일) 국민은행		7

정보통신기반보호법을 기본으로 대통령인 정보통신기반보호법시행령 및 부령인 정보통신기반보호법시행규칙과 각 부처 또는 지자체에서 각종 조례 및 지침을 제정□이용하고 있다.

정보통신기반보호법이 발효된 뒤에도 2009년 7월 7일 표 1과 같은 DDoS 공격에 의한 국내 피해사이트가 발생하였다. PC손상 피해는 총 1,466건 접수: 7.10(금) 396건, 7.11(토) 209건, 7.12(일) 441건, 7.13(월) 337건, 7.14(화) 70건, 7.15(수) 13건이다[4].

2.2. 정보보호의 3요소

그림 2처럼 정보보호를 위해서는 최소한 정보보호의 3요소[5]를 갖추어야만 한다.

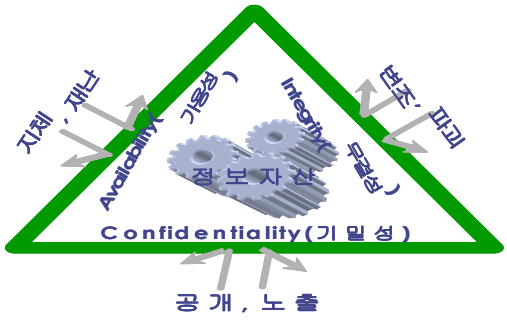

그림 2. 정보보호의 3요소

2.3. 보안성평가(기준)

표 2는 기관별 보안성 평가기준을 나타내고 있다.

표 2. 기관별 보안성 평가 기준

기관	보안성 평가 기준
국제표준 (기준)	- ISO/IEC 17799
	- ISO/IEC TR 13335 (GMITS)
행정안전부	- 정보통신기반보호법
금융감독원	- IT 경영평가지침 - 전자금융안전대책
한국인터넷진흥원	- 정보보호관리체계 인증심사기준
한국전산원	- 정보시스템 보안/통제 감리지침 연구 (1998) - 분야별 세부 감리지침
한국정보시스템 감리인협회	- 정보시스템 운영/보안 감리지침 연구 (2002)

III. 입법기관 정보보호 보안성 분석

국회 및 소속기관은 「전자정부법」 제56조에 따라 보안대책을 의무적으로 수립□시행하도록 하고 있다. 그러나 이를 위한 기본적인 원칙이 규정되지 않아 체계적인 보안정책이 수립되지 못하고 있으며, 이러한 결과 사전적 정보보호를 위한 기본조치 및 교육이 제대로 수행되지 못하고 있

고, 사후적으로는 침해사고에 대한 소속 기관 간 협조가 이루어지지 않는 등 많은 문제점을 노출하고 있다.

본 연구에서는 국회사무처[6]의 정보보호 현황을 그림 3처럼 관리적, 기술적, 물리적 보안 현황[7]을 파악하고 분석하였다.

그림 3. 관리적, 기술적, 물리적 보안 요소

3.1. 관리적 정보보호 현황

국회사무처 경우 「정보통신기반 보호법」에 의한 「주요정보통신 기반시설」로 지정되어 매년 「주요정보통신 기반시설 보호대책」(법 제6조)을 수립하여 「정보통신기반보호위원회」(법 제3조)의 승인을 받고 있으며, 「정보통신기반 보호법 시행령」 제17조에 따른 정보보호컨설팅을 2년마다 실시하고 있는 등 「정보통신기반 보호법」에 따른 정보보호 업무를 실시하고 있다.

2008년 8월 11일 시행된 국가정보원 「국가 정보보안 기본지침」에 헌법기관이 제외되어 국회사무처□도서관□예산처□조사처의 경우 정보보호 관련 규정이 없는 상황이다.

국회는 소관 주요정보통신기반시설의 취약점을 분석 평가하고 물리적 기술적 대책을 포함한 보안관리대책을 수립하여 향후 국회정보시스템의 안정성 및 신뢰성을 제고하고자 아래와 같이 관리적인 정보보호 활동을 하고 있다.

■ 취약점 진단 및 대응방안 수립.
- 기반보호시설에 대한 환경 및 자산 분석.
- 취약점 점검 및 위험도 분석(약 30개 국회웹 호스팅 사용 의원홈페이지 포함).
- 정보보호 관리체계 수립.
- 보안 정책 및 절차 제 개정.

■ 정보보호 마스터플랜 작성
- 수행과제 도출 및 우선순위 결정.
- 과제별 조직/예산/일정 계획 수립.
- 보안관제센터 운영방안 및 서비스수준지표(SLA) 도출.

3.2. 기술적 보안 현황

인터넷망과 업무용 망 분리 등 기술적 보안 현황은 다음과 같다.

표 3. 국회사무처 기술적 보안 현황

내 용	규 격	수 량
듀얼 PC	- PC 모듈 2식	2,691식
패치관리 솔루션	- 라이선스 추가구매	4,500User
IP관리 솔루션	- 라이선스 추가구매	3,500User
백본 스위치	- CPU 모듈 2식 - 48포트 광 모듈 2식	4식
워크그룹스위치	- 10/100/1000 48포트	75식
내부정보 유출방지 솔루션	- DLP	8,500User
보조기억매체 관리 솔루션	- 관리서버	2식
	- 관리매니저	2식
	- Client 에이전트	6,500식
케이블 포설	- 광케이블	300코어
	- UTP	3,200회선

3.3. 물리적 보안 현황

인터넷망과 업무용 망 분리 등 기술적 보안 현황은 다음과 같다.

■ 설비 현황
○ 규모
- 면적 : 00평(회관 0평)
- 설비관리시스템[FMS] 운영
- 소화설비 완비/안전 진단 실시 후 장비배치

○ 전원설비
- 비상전원과 일반전원 분리공급
- UPS 6조[회관 1조], AVR 1조 & 인입 전력 565KVA

○ 공조설비
- 항온항습기 13대[회관 1대]: 197.5RT[회관 5RT]

○ 보안시스템
- 지문인식시스템
- 무인카메라
- 24시간 감시

■ 서버 및 저장장치
○ 서버 장비(총 187대)

구분		보유대수	주요모델
IBM	중대형	15대	-
	소형	2대	-
SUN	중대형	49대	-
	소형	3대	-
기타	중대형	6대	-
	소형	112대	-

○ 통합저장장치: 50TB (Rald 1+0.5)
○ 통합백업장치: 500TB(25 Drive 1300 slot)

■ 네트워크
○ 인터넷전용선

구분	회 선	규격(M)
본청	2회선	100
	1회선	300
의원회관	1	300
기자망	1	60

○ 장 비

구분	대수
라우터	5식
백본	15식
스위치(L4/L2)	345식
무선AP	64식

3.4. 보안성 평가

정보보호 수준평가에 대한 국내 기준은 국정원 「국가사이버안전메뉴얼 제5장」에 의한 평가 방법과 한국인터넷진흥원의 「정보보호 안전진단 기준 체크리스트」에 의한 평가 방법이 있으며, 국제적으로는 ISO27001 Information Security Management Requirements에 따른 평가 방법 등이 있다.

3.4.1. 정보보호 수준 평가

국회사무처의 경우 2009년도에 실시한 정보보호컨설팅 결과[8] ISO 기준 적용시 61.2점으로 평가 되었으며, 표 1처럼 “보안 정책”분야와 “사업연속성 계획”분야에서 많이 부족한 것으로 평가되었다.

표 4. ISO27001 기준 국회사무처 정보보호수준

영역	국회사무처
5. 보안 정책	20.0
6. 보안 조직	71.1
7. 자산 분류 및 통제	65.8
8. 인적 보안	79.1
9. 물리적, 환경적 보안	61.3
10. 통신 및 운영 관리	72.3
11. 접근 통제	51.8
12. 시스템개발 및 유지보수	73.2
13. 보안사고 관리	72.1
14. 사업연속성 계획	25.5
15. 준거성	80.5
평균	61.2

3.4.2. 공공기관과 보안성 평가 비교

2008년도에는 59개 정부기관과 16개 광역자치단체를 대상으로 보안정책□문서관리□정보통신망 보호대책 등 8개 분야 135개 항목에 대해 정보보안 관리실태를 평가하였다.

평가 결과, 전체 평균 점수가 2007년 보다 7.5점 상승한 87.51점(100점 만점)이었다. 중앙행정기관의 경우 90점 이상을 받은 기관이 21개, 80점 이상에서 90점 미만인 기관이 31개, 80점 미만인 기관이 7개 기관으로 나타났다.

해킹메일 차단, 홈페이지를 통한 개인정보 노출 방지 대책 수립 및 바이러스 백신 프로그램 설치 등은 대부분 잘하고 있는데 반해 무선랜 무단사용 점검, 보직변경 직원 대상 보안조치와 정보보호 예산 확보 등은 미흡했다[9].

Ⅳ. 정보보호인식과 행동지침 준수 분석

4.1. 정보보호인식 평가

4.1.1. 정보보호 인식 평가 항목

① 본인이 취급하는 입법정보의 중요도의 정도를 파악하고 있는가?
② 보안 관련 부서에서 보낸 보안관련 공지를 확인하는가?
③ 악성코드 및 바이러스에 대비하여 백신프로그램 등을 얼마나 자주 사용 하는가?
④ 보안 패치 메일 등을 확인하고 실행 하는가?
⑤ 정보보호 관련 직원 교육에 참여 빈도는?

4.1.2. 정보보호 행동지침준수 평가 항목[10]

① 자신의 이용자계정(ID)을 타인에게 빌려 주거나 타인의 이용자계정(ID)을 사용해서는 안된다.
② 비밀번호(Password)는 누구에게도 알려주거나, 알 수 있게 관리하여서는 안 된다.
③ 개인정보는 개인의 매우 중요한 정보재산이므로 소중하게 취급하여야 한다.
④ 전자상거래정보 및 개인정보를 제공할 때에는 반드시 상대 사이트의 이용약관이나 개인정보 보호방침 등을 반드시 읽어보고 개인정보 관리정책을 확인한다.
⑤ 각종 인터넷 검색 정보 및 E-mail(전자우편) 정보는 다른 사람에게 노출 또는 유출될 수 있음을 명심하고 암호화하여야 한다.
⑥ 중요한 파일은 암호화하여 저장하고, 만일의 경우를 대비하여 백업을 받아 보관해 놓는다.
⑦ LAN 이용자는 가능한, 디렉토리를 공유하지 않도록 하며, 불가피하게 공유할 경우에는 암호를 설정한다.
⑧ 공공장소에서 컴퓨터를 사용하던 중에 자리를 일시적으로 비울 경우를 대비하여 암호화한 화면보호기를 설정한다.
⑨ 개인정보침해, 해킹, 컴퓨터 바이러스 감염 등 각종 침해사고에 대비해 대처방법을 미리 알아둔다.

4.2. 정보보호인식 설문조사 및 평가

4.2.1. 직원 정보보호 인식

표 5. 국회사무처 직원 정보보호 인식 설문조사

구 분	ⓐ 매우	ⓑ 상당	ⓒ 보통	ⓓ 약간	ⓔ 전혀	계
정보보호 인식 정도	7.6%	21.8 %	42.6 %	23.2 %	4.8%	100 %
정보 중요도 정도	12	17	42	25	4	100
보안관련 공지 확인	6	30	49	14	1	100
백신프로그램등 사용	6	30	49	14	1	100
보안 패치 메일 실행	11	25	51	11	2	100
정보보호 교육 참여	3	7	22	52	16	100

*조사대상 : 국회사무처 직원, ◇조사 및 수거 : 2010. 3. 16(화) ~ 22(월), ◇개별 발송 e-mail , ◇조사자 : 호서대학교벤처전문대학원 박사과정 남원희 ◇총 1,350명 중 150명 발송 이 중 112명 답변 하였다.

표 5에 의하면, 국회사무처 직원들의 정보보호 인식 정도는 상당 이상이 29.4%, 약간 이하가 28%, 보통으로 인식하는 정도가 42.6%로 그 정도가 높은 편은 아닌 것으로 조사되었다. 특히 정보보호 교육 참여가 보통 이상이 32%로 매우 취약한 것으로 나타났다.

4.2.2. 정보보호 행동지침에 대한 준수 정도

표 6. 국회사무처 직원 정보보호 행동지침 준수 설문조사

구 분	ⓐ 매우	ⓑ 상당	ⓒ 보통	ⓓ 약간	ⓔ 전혀	계
정보보호 행동지침 준수 정도	11.6 %	20.8 %	31.9 %	29.5 %	6.2 %	100 %
이용자계정(ID) 관리	20	27	37	11	5	100
Password 관리	21	36	28	13	2	100
개인정보 취급(소중)	20	28	34	14	4	100
이용약관 등 개인정보 관리정책 확인	4	13	56	21	6	100
E-mail 암호화 전송	3	8	22	55	12	100
중요파일 암호화, 백업 보관	21	31	29	12	7	100
LAN 이용자 디렉토리 암호 설정	4	10	28	50	8	100
암호화한 화면보호기 설정	6	22	24	39	9	100
침해사고 대처방법 숙지	5	12	29	51	3	100

표 6에 따르면, 정보보호 행동지침 준수 정도는 상당 이상 32.4%, 약간 이하 35.7%, 보통으로 인식하는 정도가 31.9%로 그 정도가 낮게 나타났다. 이용자 계정 관리, Password 관리, 개인정보 취급, 중요파일 암호화 백업 보관 등은 보통 이상이 71%~85%로 양호하게 나타났으나, E-mail 암호화 전송, LAN 이용자 디렉토리 암호 설정, 침해사고 대처 방법 숙지 준수 정도는 33%~46%로 저조하게 나타났다.

Ⅴ. 결 론

국회사무처의 정보보호컨설팅 결과 61.2점으로 매우 낮게 평가 되었다. 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 연구결과 국가 주요기관인 입법기관의 정보보호를 위해서는 첫째, 지속적인 직원 정보보호 중요성 인지교육과 행동지침 인식의 활성화가 필요하다. 둘째, 연속적 계획에 의한 물리적 정보보호 기능 확충과 중요 정보에 대한 외부 접근 차단을 위한 내부서버와 외부 접속 서버의 분리가 요구되며, 중요 데이터에 대 한 백본망 등의 구축이 시급하다. 셋째, 정보보안을 위한 조직화된 정보보안관제센터 등의 운영이 필요하다. 넷째, 입법기관 정보보안을 위한 국회정보보안 관련 근거 법규 제정이 요구된다.

향후 연구로는 국회사무처에 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] [창간1주년 특별 인턴뷰] 김원기국회의장 , 데일리서프라이즈, 박영일기자 2005. 11. 6.
[2] 인터넷의사중계시스템, http://assembly. webcast.go.kr/, 2010. 4.
[3] 배성훈, “7.7 DDoS 사고 문제점과 재발방지 방안”, 국회입법조사처, 2009. 12.
[4] 방송통신위원회, 국회 국정감사 제출자료, 2009. 10.
[5] 백성주, “정보시스템 운영/보안 감리지침연구”, 한국정보시스템감리인협회, 2002.
[6] 국회소속기관은 국회사무처, 국회도서관, 구회예산정책처, 국회입법조사처가 있으며, 예산 등 기본적인 사항은 국회사무처 중심으로 이루어지므로 연구의 편의상 국회사무처를 대상으로 하였다
[7] 국회사무처, 2010년도 입법정보화 업무현황, 2010. 3.
[8] 정보보호행동지침, 정보통신부 한국정보보호센터, 2004. 11.
[9] 국회사무처, 2009년도 정보보호컨설팅 결과 보고서, 2009. 12.
[10] 국가정보원, 국가정보보호백서 2009. 4.