JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 6 : 1249~1254 Jun. 2014

동적인 ICT 생태계에 따른 전자정부 보안대책 연구

정영철[1] · 배용근[2*]

Study on Security Measures of e-Gov with Dynamic ICT Ecosystem

Young-chul Choung[1] · Yong-Guen Bae[2*]

[1]Department of Computer Engineering, Chosun University, Gwangju 230-7381, Korea
[2*]Department of Computer Engineering, Chosun University, Gwangju 230-7381, Korea

요 약

ICT 환경 변화에 따라 개인 및 기업에 대한 보안의 위협은 날로 증가하고 있다. 최근에 해킹기법의 고도화가 진행되고 있고, 해킹의 상업적 서비스로 발전하고 있는 ICT 환경에서 지속적으로 해킹이 증가 추세에 있다. 이에 따라 사이버 침해 사례의 특징 분석이 필요하다. 또한 우리는 전자정부 1위 국가의 위상에 맞는 안전한 전자정부서비스 구현이 실현되기 위해서 정부의 역할로서 정책적으로 전자정부 보안 대책이 필요하다. 따라서 본 논문에서는 사이버 침해 사례를 통해 그 특징을 분석하고, 전자정부 보안 대책을 고찰하여 정책적인 제안사항을 제시하였다.

ABSTRACT

As ICT ecosystem changes, security-related threat on individuals and corporations has increased. With the recent sophistication of hacking strategy, hacking serves commerce and its scale becomes larger than ever. Accordingly, the analysis on cyber intrusion is required. As a number one electronic government around the world, the government's role for security solution for realization of safe electronic government. This manuscript analyzes cyber intrusion cases, speculates the government's measures and suggests political recommendation for the current phenomena.

키워드 : ICT 생태계, 전자정부, 봇넷, 맬웨어, 보안대책

Key word : ICT Ecosystem, e-Government, Botnet, Malware, Security Measures

접수일자 : 2014. 04. 21 심사완료일자 : 2014. 05. 14 게재확정일자 : 2014. 05. 26

*** Corresponding Author** Yong-Guen Bae(E-mail:ygbae@chosun.ac.kr, Tel:+82-62-230-7707)
Department of Computer Engineering, Chosun University, Gwangju 230-7381, Korea

Open Access **http://dx.doi.org/10.6109/jkiice.2014.18.6.1249** print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

ICT 생태환경은 동적으로 불가측하게 진화하고 있다. 이에 따라 스마트 시대에 걸 맞는 전자정부 패러다임의 변화는 시대적 소명과 우리나라가 글로벌 경쟁국가에서 선도적 역할을 할 수 있는 중요한 기회인 것이다. 이를 위해서는 정부는 끊임없이 정책적으로 연구투자하고, ICT의 급속한 발전에 따라 전자정부의 개방성, 다양성, 안전성, 경제성 등을 수용할 수 있는 스마트 전자정부로의 새로운 요구사항에 대비하여야 할 것이다.

따라서 대국민 및 기업의 웹 환경 변화에 따른 정부의 역할로서 스마트한 정부 구현을 위한 전자정부 서비스 활성화를 위해 보다 안전한 전자정부 서비스 전략을 수립하고, 이의 정책방향으로 전자정부 보안대책 방안을 제시할 필요가 있다.

본 논문에서 동적인 ICT 생태계에 안전한 전자정부 서비스 구현을 위해서 Ⅱ절에서 ICT 국내외 생태환경의 보안 위협요소 증가 요인을 살펴보고, Ⅲ절에서 지속적인 해킹 증가추세에 따른 해킹기법의 고도화와 해킹의 다양한 상업적 서비스로 발전하는 사이버침해 특징을 분석하며, Ⅳ절에서는 최근의 사이버침해 사례에 따른 보안대책과 정부의 역할로서 전자정부 보안대책을 고찰하여 이의 정책방향으로 본 연구내용을 제안하였다.

Ⅱ. ICT 생태환경

2.1. 국내외 ICT 환경변화

ICT의 발전은 우리에게 많은 문명의 이기를 가져다준다. 최근 급속히 확산되고 있는 개방형 컴퓨팅 환경으로 보안의 우려사항이 심각한 상황이 되고 있다. 우리나라의 전자정부는 발전적인 추진에 있어서 개인정보보호와 정보보안의 인프라 강화에 초점을 맞출 필요성이 있다.

UN은 행정전산망 구축에 있어서 응용시스템 구축 순으로 추진된 전자정부 사업에 대해 우리나라 전자정부 성숙단계를 최고수준인 5단계 통합처리를 2년 연속 세계1위 국가로 평가하고 있다[1].

표 1. UN 전자정부 평가결과
Table. 1 Evaluation results of e-Gov by UN

구 분		2005	2008	2010	2012
전자정부 발전지수		5위	6위	1위	1위
	온라인 서비스	0.97 (4위)	0.82 (6위)	1.00 (1위)	1.00 (1위)
	정보통신 인프라	0.67 (9위)	0.69 (10위)	0.64 (13위)	0.83 (7위)
	인적자본	0.97 (14위)	0.98 (10위)	0.99 (7위)	0.94 (6위)
온라인 참여지수		0.87 (5위)	0.98 (2위)	1.00 (1위)	1.00 (1위)

이와 같은 수준에 걸 맞는 전자정부 이념을 달성하기 위해서는 전자정부를 추진할 때 성숙도 제고를 위한 보완사항으로 정부부처 위주의 정보화에서 대국민 및 기업 중심의 통합서비스로 전환하고, 중앙・지방정부의 통합적으로 연계된 대국민 및 기업 밀착형 서비스를 개발하며, 정보보안 및 표준화 등 전자정부의 기본 인프라 강화가 중요한 사항으로 지적되고 있다. 또한 세계 전자정부 주요한 전망 중에 정부의 보안침해 사건의 증가로 안전한 정보관리 투자 필요성이 제기되고 있다. 따라서 전자정부는 새로운 디지털 시대에 대비한 행정시스템의 변화를 위한 대응에 힘을 써야할 것이다.

2.2. 보안 위협 증가

정부의 행정정보 디지털화, DB화의 가속화에 따른 정보의 복제 가능성이 증가하고 있으며, 정보시스템 연계 및 정보 유통 증가에 따른 권한관리의 필요성이 증가하고 있다. 최근 중국의 자국내 컴퓨터 및 인터넷 보급률 증가에 따라 국내 중국발 해킹, 바이러스, 스팸메일 등 사이버공격이 지속적인 증가 추세에 있다. 또한 ICT의 빠른 발전과 디지털 융합 증가에 따른 ICT 의존도의 증가와 신규 보안 취약점의 증가를 보이고 있다. 특히 개인정보・프라이버시 침해로 인한 피해 유형으로 사업자의 관리소홀로 인한 개인정보 유출이 심각하게 나타나고 있다[2].

Ⅲ. 사이버침해 특징 분석

정보보안의 위험분석은 위험관리 부분에서 가장 중요한 역할인 위협 및 취약성 분석에 대해 강조 하고 있다[3].

본 논문의 사이버 침해에 대한 특징의 위험분석에서 취약성 분석 방법론으로 그 사이버 침해 특징을 분석하였다.

3.1. 해킹기법 고도화

유명세를 떨친 Botnet의 일종인 Strom Worm의 주요 기능인 스팸메일 발송, 백도어, 바이러스 전파, DDoS 공격 기능 등은 프로그래밍 기법의 발달에 따른 해킹기법이 고도화 되고 있다. 또한 불특정 다수에 대한 공격보다 상대적으로 성공률이 매우 높은 Botnet과 Social Engineering 기술의 결합 현상이 나타나고 있다.

또한 최근 안랩은 'APT 방식의 악성코드 고도화와 표적확대', '전자금융 사기와 사이버범죄의 산업화', '악성코드 유포 방법의 다양화와 고도화', '윈도우 XP 지원 종료에 따른 보안 위협 증가', '특정 표적을 노린 소규모 모바일 악성코드 등장' 등 고도화된 보안 위협요소를 발표하였다[4].

3.2. 해킹의 상업적 서비스로 발전

최근 사이버 침해는 금전적 목적을 위한 개인정보 해킹, 경쟁기업에 대한 기밀정보 요구 등 해킹이 상업적으로 발전되고 있는 경향이 있으며, 해커의 조직화 경향을 나타내고 있다. 국제적으로 사이버 범죄와 관련하여 맬웨어(Malware)의 판매, DDoS 공격, 스팸메일 발송, 애드웨어 설치, 해킹 등의 상업적 서비스가 제공되고 있다.

TREND MICRO 보고서에 따르면 2013년부터 금전적인 이익으로 이어질 수 있는 개인정보와 금융정보를 얻기 위한 사이버공격과 악성코드의 활동이 두드러지고 있다는 분석을 한다[5].

3.3. 지속적 해킹 증가추세

최근 웜・바이러스에 대한 피해 현황을 분석하면 PC 생존기간은 최단시간이 4초로 조사되고 있다. 예루살렘 바이러스는 전세계 전파시간이 3년이 걸렸지만 슬래머는 수분내에 전세계에 전파 되었다. 또한 신규 취약점을 이용한 해킹 가능성의 제기와 공개된 취약점에 대한 지속적인 해킹이 증가 추세에 있다. 2013년에는 여러 데이터 유출 사고가 있었다. Evernote는 해커들이 정보 액세스 권한을 확보할 수 있다는 사실을 알게 된 이후 5천만 사용자들에게 로그인 자격증명을 재설정하도록 요청하였다. LivingSocial 정보유출 사고로 인해 5천만 사용자의 자격 증명 정보가 노출된바 있고, Yahoo Japan 사고로 인해 2천2백만 사용자 아이디가 공개 되었다[6].

최근 MS의 윈도우XP에 대한 기술지원 종료는 개인정보보호 및 중소기업의 보안 취약점에 대한 심각성이 우려되고 있다.

표 2. 윈도우XP 이하 버전 사용현황
Table. 2 Usage of WindowsXP version below

구분	전체	윈도XP 이하	비율(%)
PC	688,929대	162,480대	23.6
CD/ATM	87,082대	81,929대	94.1
합계	776,011대	244,409대	31.5

(표 2)와 같이 2014년 4월 8일까지 예상되는 윈도우 XP 이하 버전 사용비율은 31.5%에 해당되고 있다. 업무용 PC 23.6%, CD/ATM 94.1%가 윈도우XP 이하 버전을 사용하는 것으로 조사되고 있다[7]. 당분간 윈도우 XP 이하 버전의 컴퓨팅 환경은 개인 및 중소기업 등에서는 예산 사정상 사용이 지속될 것이다. 이처럼 윈도우XP를 그대로 쓰는 것은 해커에게 무방비로 문을 열어주는 것이나 다름없다.

이와 같은 사이버 침해 사례에 대한 대형 사건과 MS의 기술 지원종료에 따른 윈도우XP의 취약점이 예상되는 가운데 지속적으로 해킹의 증가추세는 매우 우려되는 현상으로 전망된다.

Ⅳ. 전자정부 보안대책

4.1. 침해 사례와 보안대책

네트워크의 접근성이 쉬어짐에 따라 최근 중국측 해커들이 기업의 직원들에게 해킹프로그램을 내장한 대량 메일을 발송하여 직원들이 메일을 확인한 순간 관리자 확인 자료가 해커에게 유출되어 기업의 서버에 접속

해 기업의 고객정보를 유출하는 사례이다. 기업은 다양한 보안 솔루션이 설치되어 있음에도 불구하고 웜・바이러스가 첨부된 메일을 내부직원이 읽을 경우 보안시스템이 무방비 상태가 되어 내부의 중요한 정보가 유출될 가능이 있다[8].

따라서 보안대책으로 각급 기관들은 메일을 통한 웜・바이러스 해킹이 위험성을 인식하고 개인 PC에 대해 최신의 보안패치 설치, 웜・바이러스 백신 프로그램을 설치하여 보안을 강화하고 출처가 불분명한 메일의 경우 즉각 삭제조치를 수행하는 것이 최선이다.

에스토니아 전자정부 서비스 마비사례로서 2007년 4월 27일 에스토니아 수도인 탈린 중심부에 있는 구소련의 전승 기념물을 국군묘지로 옮기는 것에 불만을 품고 러시아와 사이버 전쟁이 시작 되었다. 처음에는 러시아 정부에 연결된 컴퓨터가 정부・방송・은행 등의 전산망을 공격하였으나 Botnet이 설치된 전세계의 수십만대의 컴퓨터를 사용하여 다각적인 공격을 수행하였다. 당시 100만대 이상의 컴퓨터가 사용된 것으로 알려졌으며 에스토니아 전자정부가 마비되는 결과를 초래하였다[8]. 이러한 사이버 침해 사례의 적절한 보안대책으로 Botnet을 이용한 DDoS 공격에 대해 상시 모니터링 체계 구축과 빠른 대응체계 구축이 필요하다. 이를 위해 DDoS 공격에 악용되는 악성코드의 추가적인 유포를 차단하고, 이미 감염된 컴퓨터에 공격자가 공격명령을 전달하지 못하도록 조치하는 것이 중요하다.

따라서 국내의 경우 Botnet 등이 감염되지 않도록 보안패치와 웜・바이러스 점검 수행을 위한 주기적인 교육・홍보를 실시하고 정보보호 사각지대에 대한 지원체계가 필요하고, 또한 국외 DDoS 공격에 대한 국제적 공조체계가 필요하다.

4.2. 정보보안 환경구축 필요성

컴퓨터 악성 프로그램의 피해는 날로 커져가고 있는 실정이며, 컴퓨터 바이러스는 정보화 사회에서 나타난 대표적인 사회적 문제를 야기하고 있다. 2007년에 발생한 Storm 바이러스는 10개월 동안 전 세계 5,000만 대의 컴퓨터에 전파하여 커다란 피해를 준 사례이다. 이러한 바이러스들에 의한 피해는 2010년대에 접어들면서 컴퓨터 바이러스는 점차 줄어든 대신 그 자리를 악성 프로그램이 대신하고 있으며, 엄청난 경제적 손실뿐만 아니라 사회 안전망까지 위협하게 되고 사이버테러와 같은 심각한 문제들을 야기 시킨다.

정보화 사회에서 정보는 중요한 역할을 하고 있다. 인터넷 상의 정보를 기반으로 더욱 유익하고 새로운 정보를 생성하게 되며, 이는 우리 삶의 질을 높이는 결과를 가져오기도 한다. 반면에 주민등록번호, 은행예금계좌, 신용카드정보 등의 중요한 정보의 유출, 그리고 해킹에 의한 정보유출은 우리들이 잘못된 정보의 관리로 인해 많은 피해와 이로 인한 사회적 문제가 발생하고 있다. 이를 방지하기 위해서 평소에 정보보안에 대하여 숙지하고 있어야 하며, 개인 컴퓨터 및 자신이 관리하는 정보시스템을 외부의 침입자로부터 보호하는 인식과 정보보안 생활수칙을 정하는 것이 바람직하다[9].

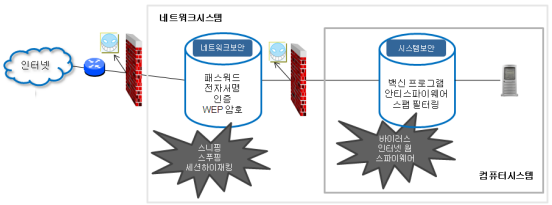

그림 1. 정보보안 환경 구조
Fig. 1 Structure of information security environment

따라서 물리적으로 정보보안 환경을 갖추어 외부로부터 네트워크의 접근에 다중의 정보보호를 위한 네트워크 보안요소를 강화하여 대국민 및 기업이 안전하게 생활할 수 있는 정부의 지원이 절실하다. 이것이 행정의 이념으로서 전자정부 서비스 목표를 달성하는 정보보안 환경구축인 것이다.

4.3. 보안대책 제안

행정이념을 달성하기 위해 대국민 및 기업에 대한 전자정부 서비스는 기술적인 보안성, 안정성, 확장성이 보장된 전자정부 통신망을 구성하여 품질이 보장된 정보통신 서비스를 제공함으로서, 정보공유 및 유통 활성화로 정부 부처간 협업형 전자정부 구축을 목표로 하고, 신기술 출현, 통신환경 변화 등에 따른 국가기관의 신규 수요를 효율적으로 수용할 수 있도록 확장성을 갖도록 하는 전자정부의 역할이 필요하다[10].

따라서 전자정부는 정부의 서비스를 5any(anywhere, anytime, anynetwork, anydevice, anyservice) 형태로 빠르고 쉽게 대국민 및 기업이 만날 수 있는 국민의 국민

에 의한 전자정부를 구현할 수 있는 스마트 정부를 위해서 전자정부 서비스 활성화를 위해 보다 안전한 보안대책이 필요하다. 그러므로 논거한 보안대책으로 다음과 같이 제안한다.

첫째, 중국・인도 등 개발도상국에 의한 사이버 대응체계를 정비하고 전담인력을 확보하여야 한다. 중국・인도에 대한 사이버 침해 대응을 위한 전담인력을 상시 확보하고 국가간 사이버 침해사고 발생에 대비하여 공동 대응체계의 구축이 필요하다.

둘째, 신규 보안 취약점에 대한 지속적인 연구와 투자가 필요하다. 웹 프레임워크인 XpressEngine, Adobe 제품군 등 정보통신 신규 보안의 취약점에 대한 지속적인 연구를 위해 산・학・연 공동연구센터의 설립이 필요하다.

셋째, 해킹기법의 고도화와 소셜 엔지니어링 공격의 결합에 따른 정보보안 인식제고 교육 강화 및 대응체계를 정비하여야 한다. 피싱, Botnet, 웜・바이러스로 인한 중요정보 유출과 DDoS 공격 및 해킹 등을 미연에 방지하기 위해 대국민 및 기업 교육・홍보를 강화하고 기본적인 정보보안 솔루션 도입 의무화를 추진하여야 한다.

넷째, 해킹의 상업적 서비스에 대응한 법체계 강화와 국내외 협업체계 강화가 필요하다. 해킹을 상업적인 서비스로 이용할 경우 강한 처벌규정으로 Malware 산업을 초기에 근절하고 국가간 공조 체제를 강화하여 Malware 산업에 대한 국제적 대응 체계를 구축할 필요가 있다.

다섯째, 개인정보보호, 정보보안, 표준화 등 전자정부의 기본 인프라에 대한 지속적인 투자 강화가 필요하다. 미국은 IT 투자예산 중 10% 이상을 정보보안에 투자한 반면, 우리나라의 경우 2011년 정보화 예산 3조 3,023억원 중에서 정보보호 예산이 차지하는 비율은 6.2%에 불과하다. 따라서 전자정부 1위국가로서 정부의 역할은 향후 정보보안 인프라 강화를 위해 선진국 수준의 예산 확보가 절실히 필요하다.

Ⅴ. 결 론

지식정보화 시대의 진화로 국내외 ICT 환경 패러다임은 많은 변화를 가져왔다. 거치성 컴퓨팅 시대에서 이동성과 소형의 편리성이 강조된 컴퓨팅 구현이 가능한 스마트 기기의 시대가 도래 하였다. 이와 같이 ICT 생태계 변화의 개방성으로 개인 정보보호 및 정보보안에 대한 기대와 실천적인 보안강화의 필요성이 중요한 이슈가 되고 있다.

정부・국민・기업은 기존의 거치성의 컴퓨터 기반 서비스를 이동성, 개방성, 다양성, 경제성 등을 지원하는 컴퓨팅 이용환경의 변화를 요구하고 있으며, 모바일 확산으로 네트워크, 서비스, 콘텐츠 등 ICT 산업분야 전반으로 성장의 견인 역할을 하고 있다. 이에 따라 정부는 끊임없이 정책적으로 전자정부의 안전성을 위해 연구 투자하고, ICT의 급속한 발전으로 인한 전자정부의 새로운 요구사항에 대비하여야 할 것이다.

본 논문에서 공공성이 보장된 정부 구현을 위해 먼저 ICT 국내외 생태환경의 보안 위협요소 증가 요인을 고찰하였고, 지속적인 해킹 증가추세에 따른 해킹기법 고도화의 사이버침해 특징을 분석하였으며, 끝으로 최근의 사이버침해 사례에 따른 보안대책과 정부의 역할로서 전자정부 보안대책을 고찰하여 전자정부 정책방향으로 연구내용을 제안하였다.

결론적으로 본 논문의 동적인 ICT 생태계에 따른 전자정부 보안대책 연구에 의한 정책적 제안은 결국 전자정부 정책과제 활용가치로 인해 정부 혁신과 대국민 삶의 질을 향상시킬 수 있는 행정의 궁극적인 목적 실현의 최적 수단으로 활용되어 행정이념이 추구하는 지식정보와 민주적 가치가 구현되기를 기대한다.

감사의 글

본 연구는 2013년도 조선대학교 연구비의 지원에 의하여 이루어진 연구로서, 대학본부에 감사드립니다.

REFERENCES

[1] UN E-Government Survey 2012, Printed at the United Nations, New York, ISBN : 978-92-1-123190-8, pp. 10-11,

February 2012. Available: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf
[2] NIA, “National Information White Paper,” pp.548-549, 2013.
[3] H. B. Jang, S. J. Rim, “Information Security Management and Policy”, KR: Kihanjae Pub., ch.1, pp.18, 2009.
[4] oKISA, “Cyber Security Issue”, pp.51, Feb. 2014. Available: http://www.dt.co.kr/contents.html?article_no=2014013020199607860003
[5] TREND MICRO, “Threat Report and Forecast,” pp.1-6, Jan.2014. Available: www.trendmicro.co.kr/.../rpt-cashing-in-on-digital-information-kr.pdf
[6] TREND MICRO, “Became blurred boundaries,” *2014 security predictions report*, Available: www.trendmicro.co.kr/.../rpt-trend-micro-security-predictions-for-2014-and-beyond_1212_kr.pdf
[7] Korea Financial Services Commission, “financial company corresponding status with end of Windows XP technology support,” *Press release*, pp.2, Mar. 2014. Available: www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=2&sch1=&sword=&r_url=&menu=7210100&no=29760
[8] G. S. Cha, “Security measures of the e-government according to analysis of trends in recent security incidents,” *e-Government Focus*, No. 06, pp.19-23, 2008.
[9] Y. C. Choung, Y. G. Bae, “The Era of Computer Understanding of Convergence,” KR: Humanscience Pub., ch.10, pp.315-316, 2014.
[10] Y. C. Choung, Y. G. Bae, “m-Gov strategy and policy challenges with ICT ecosystem changes,” *Journal of KIICE*, vol. 17, no. 7, pp. 1533, Jul. 2013.

정영철(Young-Chul Choung)

1987년 조선대학교 행정학 학사
2003년 조선대학교 전자공학 석사
2007년 조선대학교 정보통신공학 박사
현재 제이앤아이코리아 연구소장, 조선대학교 컴퓨터공학과 외래교수
※관심분야 : 정보통신 정책, 전자정부, 네트워크 및 보안, 융복합 응용

배용근(Yong-Guen Bae)

1984년 조선대학교 컴퓨터공학사
1987년 조선대학교 대학원 공학석사
1993년 원광대학교 대학원 공학박사
현재 조선대학교 컴퓨터공학과 교수
※관심분야 : 마이크로프로세서, 프로그래밍 언어, ICT 정책