논문 2019-1-10 http://dx.doi.org/10.29056/jsav.2019.06.10

사이버안전에 대한 국민인식 조사 연구

윤영선*† , 안개일**

A Survey on Public Awareness of Cyber Security

Young-Sun Yun*† , Gae-il An**

요 약

본 연구에서는 사이버안전에 대한 설문조사를 통하여 인터넷 사용 환경의 파악, 국민들이 노출되기 쉬운 사이버 위협, 불안감을 느끼는 분야, 건전성을 해치는 콘텐츠 등에 대한 국민인식을 조사하였다. 그 결과, 국민들이 많이 노출되었다고 생각하는 사이버위협과 불안정도가 높은 사이버위협에 대한 분석을 진행하였으며, 인터넷 사용 환경, 불건전 콘텐츠에 대한 생각, 예방주체 및 방법 등을 파악하였다. 조사결과는 사이버안전 분야의 융합 연구 아이템을 기획할 때 참조해야할 요구사항을 도출할 수 있도록 그 결과를 분석하고, 그 활용방안을 제시하였다.

Abstract

In this study, we surveyed the public awareness about cyber security. Through the survey, we found the awareness for cyber threats that are easily exposed to the public, the one is felt anxiety by the people, and harmful contents in the online. As a result, we analyzed the various cyber threats, and found the internet usage environments, thoughts on unhealthy contents, person in charge of prevention and its methods. The results of the study can be considered as the bases of the extracting requirements for designing convergence research items in the cyber security, and they also suggested its utilization.

한글키워드 : 사이버안전, 국민인식, 설문조사, 사이버위협, 불건전콘텐츠

keywords : cyber security, public awareness, survey, cyber threats, harmful contents

1. 서 론

최근 인터넷과 정보통신의 발전으로 인하여 거의 대부분의 국민이 항상 인터넷과 연결되어 있다고 할 수 있다. 2018년 통계의 경우 하루에 1회 이상 인터넷을 이용하는 비율은 95.3%, 주 평균 이용시간은 16시간 30분으로 집계되었다. 또한 전체 가구 중 94.9%가 스마트기기를 보유하고 있으며, 데스크톱 소유가구가 56.3%, 노트북 소유가구가 34.2%로 나타났다. 만 3세 이상 인구의 89.6%가 스마트폰을 사용하고 있으며, 90.4%가 모바일 인터넷 사용자로 집계되었다[1]. 특히 4차 산업 혁명에 대한 관심이 증가하면서 사람과 사람, 사람과 사물, 사물과 사물 간에 교환되는 정보를 통하여 기존의 방식으로 해결하기 어려웠

* 한남대학교 정보통신공학과
** 한국전자통신연구원 정보보호연구본부
† 교신저자: 윤영선(email: ysyun@hnu.kr)
접수일자: 2019.06.01. 심사완료: 2019.06.11.
게재확정: 2019.06.20.

던 많은 문제가 인공지능 및 빅데이터 이론 등의 도움으로 쉽게 해결되고 있다. 그러나 이런 기술들이 악용되어 완전히 새로운 방식의 사이버 공격이 발생할 가능성이 높아져서 사이버 보안이 더욱 중요해졌다. 그러나 국내의 경우 스마트폰과 인터넷의 사용률이 기하급수적으로 증가한 반면, 사이버 보안(안전)에 대한 국민 개인의 인식과 예방 대응조치는 여전히 상대적으로 미흡한 것으로 나타났다. 2012년 미국의 Microsoft사의 “Security Intelligence Report”에 의하면 우리나라 악성코드 감염률은 전 세계 1위로 사이버 침해에 매우 취약한 상태를 보이고 있으며[2], 통신기기의 발달로 인하여 다양한 연결 장치 및 방법들의 취약점을 공격하여 개인정보를 탈취하는 사이버 공격 및 위협은 지속적으로 증가하고 있다.

미래창조과학부에서는 사이버안전을 사이버공격으로부터 정보통신망을 보호하여 정보통신망과 정보의 기밀성, 무결성, 가용성 등 안정성을 유지하는 상태라고 정의하고 있다. 여기에서 사이버공격은 해킹, 컴퓨터바이러스, 서비스방해, 전자기파 등 전자적 수단에 의하여 정보통신망을 침입, 교란, 마비, 파괴하거나 정보통신망을 통해 보관 유통되는 전자문서, 전자기록물을 위조, 변조, 유출, 훼손하는 일체의 공격행위를 말한다[3]. 사이버안전이라는 용어는 2003년 1.25 인터넷 대란으로 인하여 국가 정보기반시설에 대한 국가안보차원의 대응체계 구축 필요성이 제기되었고, 그 과정에서 사이버안전이라는 용어가 등장하였으며, 보안 (security)이라는 용어대신 포괄적 개념의 안전 (safety)이라는 용어가 사용되기 시작하였다[4]. 따라서 사이버안전 (cyber safety)은 사이버보안 (cyber security)과 동일한 의미이며, 정보통신 기술을 매개로 개인, 기업, 정부기관의 취약점을 공격하여 인간의 생명과 정신, 그리고 물리적 자산을 위협하는 공격으로부터 방어하는 전략을 의미한다[5].

본 논문에서는 최근 여러 사건·사고들을 통하여 관심과 경각심이 증가되고 있는 사이버 위협과 관련된 사이버안전에 대한 국민인식 조사를 통하여, 국민들이 노출되기 쉬운 사이버위협(cyber threat)을 파악하고 분석한다. 또한 이들 결과를 이용하여, 사이버위협을 예방하는 사이버안전 분야의 융합 연구 아이템을 기획할 때 참조해야할 요구사항을 도출할 수 있는 기본 분석 자료를 제공하며, 활용 및 요구사항을 제시하였다.

2. 보안 위협과 사이버안전

일반적인 정보보호는 보안 위협 수준을 기준으로 정보보안, 사이버보안, 그리고 사이버안보로 구분한다. 정보보안(information security)은 정보의 비밀성, 무결성, 가용성을 유지하기 위해 권한 없는 사용자로부터의 정보의 유출, 훼손, 변조를 예방하고 대응하는 전략이다. 사이버보안은 ICT (Information & Communication Technology) 기술을 매개로 개인, 기업, 정부기관의 취약점을 공격하여 인간의 생명과 정신 그리고 물리적 자산을 위협하는 공격으로부터 방어하는 전략을 의미한다. 사이버안보 (cyber defense)는 국가의 안보를 위협하는 사이버공격으로부터 국가를 방어하는 전략이다[5]. 과거에는 정보보안과 물리적보안의 상관관계가 명확하지 않았으나, 최근에는 사이버공간에서의 오류 또는 피해가 물리적 공간으로 전이되는 예를 쉽게 볼 수 있다. 2018년 발생한 OO통신의 화재와 OOO의 클라우드 공간의 오류는 사이버 공간이 물리적 공간에 끼친 영향과 물리적인 통신 오류가 온라인으로 연결된 많은 서비스의 피해를 가져온 것으로 볼 때 서로 밀접한 관계를 가지고 있으며, 특정 서비스나 공간의 피해는 상호 의존적임을 알 수 있다. 따라서 양적, 질적으로 변화하는 보안 위협 및 공격

에 대한 대응은 기존과 다른 방식으로 전개되어야 하며, 이를 위하여 새로운 방식의 보안 위협에 대한 국민의 의식, 기술 수준, 위협, 피해의 유형 등을 파악할 필요가 있다. 표 1은 보안위협에 따른 개인, 기업, 국가별 피해 유형을 정리한 것이다.

표 1. 보안위협에 따른 피해유형[6]
Table 1. Security threats and their damages[6]

보안위협	피해 유형 (개인, 기업, 국가)
정보 유출	[개인] 개인데이터, 생체정보 유출 [기업] 고객정보 유출, 기업 기밀정보 유출 [국가] 국가정보, 군사정보 유출, 국가기반시설정보 유출
경제적 피해	[개인] 단말기 오작동, 데이터삭제, 암호화 등 사용불가 [기업] 기업전산망, 시스템 오작동, 마비 [국가] 국가기반시설 마비, 재난사고 유발
정신적 피해, 사회 건전성 위협	[개인] 인신공격(사이버 왕따, 댓글, 가짜뉴스 등) [기업] 기업이미지 하락 [국가] 사회갈등, 대립, 혼란조성, 건전성 훼손(불법, 유해정보 유통)
생명 위협	[개인], [기업] 개인 및 고객의 생명위협 [국가] 국가를 향한 사이버테러 위협

이 중 본 논문에서 관심을 가지고 있는 사이버안전에 대한 보안위협을 살펴본다. 사이버안전이란 해킹으로부터 컴퓨터내의 정보 및 비 정보 자산을 보호하는 행위를 말한다. 4차 산업혁명시대에 사이버안전을 위협하는 대표적인 요소로는 IoT 공격이 있다. 4차 산업혁명시대에는 IoT 기기의 보급 확산에 비례하여 사이버 공격으로 인한 피해가 함께 증가할 전망이다. 과거에는 인터넷에 연결된 기계가 주로 PC에 국한되어 있었고, PC를 이용하여 직접 또는 간접 공격, 매개체 등의 방법으로 정보의 훼손 및 탈취 등의 사례가 종종 발생하였다. 그러나 모든 사물이 인터넷에 연결되는 4차 산업 혁명 시대에는 모든 기기가 공격의 매개체가 될 가능성이 존재한다. 시장조사기관 Erricson에 의하면 IoT 기기의 보급률은 2015년 약 46억 개에서 2021년 약 160억 개에 이를 것이며, 연평균 23%의 시장 성장률을 보일 것으로 예상된다. 그런데 IoT기기는 오픈소스를 활용하는 특징 등으로 인해 보안 취약성이 높을 뿐 아니라 공격에 쉽게 노출되어 있다. 이런 약점 등으로 인하여 IoT는 앞으로 사이버 공격의 표적이 될 가능성이 높다. 특히 IoT가 사이버공간과 현실공간 (물리적공간)의 경계선에 위치한다는 특징 때문에 단말기와 사이버세계에 한정되었던 사이버 공간의 대상이 인체, 물리적자산 등의 현실 세계로 확대될 가능성이 높아졌다[5]. IoT 공격 이외에도 가짜뉴스, 사이버폭력, 불건전 콘텐츠, 악성코드감염 등 많은 요소가 사이버안전을 위협하고 있다. 최근에는 인간의 감정이나 인지적 과정에 개입하여 현실적인 이득을 취하는 새로운 위협도 등장하고 있다.

사이버공격의 동향을 살펴보면 2000년 이후로 무차별적으로 배포되어 시스템의 동작을 불안정하게 하는 바이러스나 웜의 공격은 감소한 반면, 개인정보 유출이나 APT를 이용하여 지속적으로 특정 대상을 공격하는 것과 서비스 거부 공격을 통한 시스템이나 통신망의 마비에 대한 공격은 증가하고 있다[7]. 국내의 경우에도 2003년 1월 이후 총 36건 이상의 사이버 공격 및 침해가 확인되었다[8]. 그 이후에도 안전 및 다양한 생활과 밀접한 사이버 공격 및 통신망 안전사고 등이 발생하고 있다. 표 2에서 보는 바와 같이 2003년 이후부터 2018년 6월까지 보고된 정보 보안 사고의 유형을 분석하면 개인정보 유출이 26건, 사이트/전산망 마비가 6건, 금융자산탈취 등이 4건으로 집계되었다.

사고 유형을 살펴보면, 개인정보 유출이 압도적으로 많으며, 사이트 마비, 그리고 최근의 가상화폐 유출 등이 증가되는 것을 알 수 있다. 개인정보 유출의 경우 기업들이 저장하고 있는 고객

표 2. 정보 보안 사고 유형별 분류
Table 2. Types of information security accidents

사고 유형	건수	내용
개인정보 유출	26	기업
사이트/전산망 마비	6	기관, 기업
금융자산탈취	4	가상화폐유출

정보 등이 유출되어 기업의 책임이나 보안 대책이 중요하다는 것을 알 수 있다.

사이버 안전이란 조직이나 기구가 아니며, 단일한 그룹에 의하여 보장될 수 있는 것이 아니다. 다시 말하면 사이버 안전은 온라인 관련 기술을 사용하는 사람이라면 누구나 가지고 있어야 할 책임, 즉 일종의 사고방식이다[9]. 따라서 사이버 안전을 유지하기 위해서는 모든 국민이 자신이 사용하는 기기의 보안을 유지하며, 그렇지 않은 경우 주위 사람, 직장, 정부 등 모두에게 위험을 준다는 경각심을 가져야 한다. 물론 기존의 조직이나 기관이 사이버 안전을 위하여 국민들에게 홍보와 교육을 통하여 국민이 자신의 역할을 다 할 수 있도록 지원할 수 있지만, 국민의 인식 제고 확대를 위해서는 다방면으로 지원 가능한 융합 연구 항목을 선정하고 지원할 토대를 구축하여야 한다.

3. 설문문항 구성

3.1 설문문항 구성 원칙

사이버 안전에 대한 국민 인식을 설문조사하기 위하여 시민단체 및 사이버 안전 전문가와의 지속적인 회의를 통하여 설문 조사 방법 및 설문 방향 등에 대하여 논의하였으며, 국내외 사례를 통하여 설문 문항을 구성하였다.

IT 지식과 전문 지식이 없을 수도 있는 일반 국민들을 대상으로 실시하는 설문조사이기 때문에, 설문 문항이 너무 많거나 전문적인 지식을 요하는 문항의 경우 중간에 포기하는 경향이 있다. 따라서 설문 문항을 국민들의 지식과 상관없이 통계를 얻을 수 있는 평이한 문장들로 구성하였다. 다만 사이버 안보/보호와 정보 보안 등이 IT를 접하지 않는 사람들인 경우에는 거부감이 발생할 수 있기 때문에 최신 용어나 전문 용어의 경우 별도로 설명 문장을 추가하는 것이 바람직하다는 의견을 반영하였다.

3.2 설문문항 구성 방법

시작단계에서 설문조사 대행업체를 통하여 설문 문항을 제시하고 실시하는 방안을 고려하였으나, 설문 문항의 수가 제한적이고 모바일 폰을 이용하여 설문 당 리워드를 받는 형태의 설문 방법으로 설문에 대한 객관성을 답보하기 힘들어, 직접 구글 설문지를 이용하여 설문을 구성하였다.

설문을 시작하기 전 사이버 안전에 관한 설문조사 안내 및 통계법에 따른 비밀 준수에 대하여 설명하였으며, 설문의 진행상황을 확인할 수 있도록, 전체 페이지와 현재 페이지를 표시하였고 설문을 마지막까지 진행하도록 장려하기 위하여 마지막 페이지에 이름과 연락처를 입력받아, 성의껏 설문을 답변한 사람에게 쿠폰을 발송하도록 하였다.

총 20개의 섹션 (페이지)으로 설문을 구성하였으며 1개의 섹션에 3개 이상의 설문 문항이 포함되지 않도록 하였다. 설문자의 선택에 따라 설문 문항 바로가기를 지정하였으며, 선택된 사항과 관련성이 없는 문항의 경우 설문에 표시하지 않도록 하였다. 국내·외 참고문헌과 사이버 안전 전문가, 그리고 설문조사 전문가의 의견을 반영하여 최종적으로 완성된 설문 문항은 표 3과 같이 구성하였다.

표 3. 설문 문항 구성 및 내용
Table 3. Questionnaire items and contents

분류		문항 수	내용
설문자 분포 조사		4	성별, 연령대, 학력, 직업 조사
사이버안전 관련문항	PC 운영체제	1	윈도우즈 버전, 맥, 리눅스 등 조사
	휴대폰 운영체제	3	안드로이드, 아이폰 버전 조사
	사이버 안전 중요도	1	사이버/온라인 안전 중요도
	사이버 공격 노출도	2	사이버 공격/위협 노출정도/순위
	사이버 위협 불안감	2	사이버 위협 불안감/순위
	악성코드 감염/대처	3	악성코드 감염 여부 및 대처 방안
	건전성 침해 관련	4	사이버 건전성 침해 및 예방책
	사이버 위협 보호주체	1	사이버 범죄/위협에서 사용자 보호 주체
	인터넷/컴퓨터 사용 시 예방 및 보호대책	3	인터넷/컴퓨터 사용 시 보호 방법 및 정도
합 계		24	

4. 설문조사 결과 및 활용방안

4.1 설문조사 실시

설문기간은 2019년 4월30일부터 5월 15일까지 약 2주간에 걸쳐 구글 설문지를 이용하여 설문을 실시하였다. 2개 학회 회원 대상 약 550명, 대전 소재 H 대학교 공식 홍보 페이스북 팔로워(Follower) 20,724명, 지인들의 단체 채팅방 참가자 약 2~300명, 개인 페이스북 친구 약 1,000명에게 홍보하였으며, 약 1.2% 정도의 응답률을 보인 총 282명의 설문 응답을 얻었다. 282명의 응답자 수는 모집단을 22,500~23,000 명으로 가정하였을 경우 95% 신뢰수준에 5.8%의 표본오차로 산출되었다.

4.2 설문조사 결과

설문 응답자는 총 282명으로 남자 185명, 여자 97명, 연령대는 20대 39%, 30대 10.6%, 40대 13.5%, 50대 31.6%의 분포를 보였다. 학회 회원들의 경우 대학졸업자가 많고 주 응답자가 연구하는 사람들이기 때문에 50대 응답자가 많았으며, 대학교의 팔로워는 주로 대학생 위주로 구성되어 20대 비중이 높은 것으로 파악되었다. 응답자의 구성 분포는 표 4와 같다.

표 4. 설문응답자 분포
Table 4. Distribution of questionnaire responder

구분	응답 분포
성별	남자 185명(65.6%), 여자 97명(34.4%)
연령대	20대(39%), 30대(10.6%), 40대(13.5%), 50대(31.6%)
학력	고졸(27%), 대졸(31.7%), 대학원졸 이상(40.2%)
직업	대학생(26.7%), 대학원생(7.5%), 전문직(33.5%), 사무직(21%)

사이버 안전에 관한 설문조사는 인터넷 접속에 사용하는 컴퓨터 또는 모바일 기기의 질문으로부터 사이버 안전에 관한 노출, 불안, 예방 등의 응답을 수집하였다. 각 응답에 대한 대표적 응답 구성 및 분석 내용을 표 5에 정리하였다.

표 5. 사이버안전 관련 설문 결과 및 분석
Table 5. Results and analysis of cyber security related questions

구분	응답 분포	결과 분석
운영체제	윈도우즈 10(70.5%), 윈도우즈 7/8(17.1%), 맥(5.3%), 윈도우즈 XP이하(3.2%)	. 윈도우즈 계열이 약 90%를 보이고 있으며, 최신 운영체제인 윈도우즈 10이 70.5%를 보임 . 컴퓨터를 사용하지 않거나 운영체제버전을 모르는 응답자 존재
인터넷 연결 휴대용기기	안드로이드(63.7%), 아이폰계열(34.9%), 사용하지 않음 (1.4%)	. 전 국민을 대상으로 하는 비율보다 아이폰 비율이 높음
안드로이드 기기의 운영체제	안드로이드9(38.5%), 안드로이드8(17.9%), 안드로이드7(8.9%), 모름(30.2%)	. 최신 운영체제의 비율이 약간 높음 . 모른다고 응답한 비율이 전체 1/3을 차지함
아이폰 계열의 운영체제	iOS12(62.%), iOS11(7.1%), iOS10(7.1%), iOS6/7/8(13.3%), 모름(9.2%)	. 최신 운영체제의 비율이 상대적으로 높음 . 모른다고 응답한 비율이 약 10%임
사이버안전의 중요성	매우 그렇다.(68.7%), 그렇다(23.8%), 보통이다(5.3%)	. 인터넷을 사용하는 대부분이 중요하다고 응답 . “아니다/전혀 아니다”의 응답분포는 인터넷을 적게 사용하는 응답자로 추정
사이버위협의 노출정도	개인정보탈취(3.12/1.18†), 불건전콘텐츠(2.95/1.32), 사이버사기(2.91/1.20), 악성코드감염(2.84/1.14)	† 평균/모집단 표준편차 표시 . 체감하는 사이버 공격 빈도수 정도를 나타냄 . 개인정보탈취, 불건전콘텐츠, 사이버사기 순
사이버위협의 노출순위	개인정보탈취, 악성코드감염, 불건전콘텐츠	. 과거 사이버 공격 발생 양상과 비슷한 분포를 보임 . 발표된 사이버 공격이 반영된 것으로 파악됨
사이버위협의 불안정도	개인정보탈취(3.70/1.14†), 악성코드감염(3.46/1.17), 사이버감시(3.35/1.22), 사이버사기(3.34/1.17), 인터넷장치(3.29/1.18)	† 평균/모집단 표준편차 표시 . 노출정도보다 불안정도의 점수가 높음 . 사이버감시, 사이버사기, 인터넷장치의 불안정도 높음 . 서비스거부, 사이버폭력의 경우 성인이거나 직업군에 따라 낮은 분포를 보이는 것으로 판단됨
사이버위협의 불안순위	개인정보탈취, 악성코드감염, 인터넷장치해킹	. 인터넷장치 해킹에 대한 불안감이 높음 . 제조사의 업데이트나 지속적인 지원이 필요함
악성코드 감염경험	있다(40.2%), 없다(59.8%)	. 상대적으로 악성코드 감염경험이 많음 . 타 조사와 비교할 때 감염비율은 증가 경향
악성코드 감염대처	백신프로그램 설치/업데이트(36.3%), 악성코드 제거프로그램 사용(33.6%), 컴퓨터수리점(12.4%), 컴퓨터교체/초기화(11.5%)	. 악성 백신/제거 프로그램 이용 (70%) . 스스로 대처함 (81.5%) . 랜섬해커에게 돈을 준 경우 있음 . 무시 (4.4%)
악성코드 감염책임	본인/사용자 (57.3%), 악성코드제작자(60.9%), 포털운영자(30.2%), 인터넷공급자(22.8%), 보안업체(23.5%)	. 법적 책임은 악성코드제작자이지만, 사용 책임은 본인/사용자로 해석 . 포털운영자, 인터넷공급자의 경우 악성코드 관리 책임이 있다고 생각 . 영리적 목적의 보안업체에 신속성, 정확성, 예비/방지 요구

표 5. 사이버안전 관련 설문 결과 및 분석 (계속)
Table 5. Results and analysis of cyber security related questions (continued)

구분	응답 분포	결과 분석
건전성 침해 경험	있다(44.8%), 없다(55.2%)	. 악성코드와 비슷한 분포지만 불건전성 콘텐츠 노출 빈도가 조금 더 높음
건전성 침해 대처	무시(80.2%), 지인상담(8.7%), 신고(6.3%)	. 피해사항이 미비하거나 건전성 침해 경험이 없는 응답자가 무시를 선택한 것으로 판단 . 불건전 콘텐츠의 경우 개인대상이며, 자신이 조심하면 피해가 발생하지 않는다고 느끼는 경향이 있는 것으로 판단
건전성 침해 예방 활동	신고및처벌강화(50.2%), 불건전 콘텐츠/서비스 차단(40.2%)	. 불건전 콘텐츠의 경우 위법성이 높기 때문에 법이나 규제를 통하여 차단/금지 . 법/규제로 통제되지 않는 경우 ISP가 차단하는 것을 원함
사이버 위협 보호 주체	본인/사용자 (61.2%), 포털(31%), 정부(28.5%), 보안업체(31.8%), ISP(20.6%)	. 사용자 스스로 자신을 보호해야 함 . 포털은 콘텐츠 관리, 정부는 법/규제를 통한 보호, ISP는 기술적 보호, 보안업체는 악성코드 예방 등으로 해석
인터넷 브라우저 적용 기능	스크립트 차단/관리(37.7%), 광고차단기능(32.4%), 사용하지않음(29.2%)	. 30%의 사용자가 전혀 보호하지 않고 있기 때문에 이들을 대상으로 보호 정책 마련 필요
사이버위협 예방행동	보안 프로그램 설치/업데이트(73%), 운영체제 보안업데이트(68.7%), 방화벽/네트워크 관리(50.2%), 암호변경(48%), 데이터백업(42.3%)	. 높은 차원의 예방을 위해서는 별도로 보안프로그램을 설치/운용 . 보안 프로그램 외에도 운영체제에서 제공하는 기본기능을 이용해서도 보호 가능 판단 . 사이버 공격 피해를 가정하여 데이터백업 필요
사이버위협 보호조치 않는 이유	해당사항없음(59.4%), 보호방법을 모름(11.4%), 사용이 불편(8.9%), 비용문제(6.8%)	. 보호방법을 모른 경우에는 자동 설치 및 업데이트 환경 필요 . 비용문제를 해결하기 위하여 저비용 또는 무료의 보안프로그램 배포 필요 . 중복 설치, 비표준 보안프로그램 등으로 인한 성능저하 등이 발생

4.3 활용 및 요구사항

사이버 안전에 관한 설문지에 대하여 응답자의 분포를 제외하고, 사이버 안전관련 질문 20개에 대한 분석을 진행하였다. 분석 과정은 설문결과를 분석하고, 전문가들과의 자유스러운 의견개진을 통하여 유추 또는 추정 분석들이 추가되었다. 이들 분석을 종합적으로 정리하여 그 활용방안을 다음과 같이 제시하였다.

- 사이버 안전을 유지하기 위한 일차 보호 주체는 사용자이기 때문에, 컴퓨터나 인터넷의 이용 시 자신의 행동에 따른 책임을 느끼고 사이버 위협으로부터 컴퓨터나 인터넷 연결기기, 저장된 데이터를 보호할 수 있도록 홍보/계도 및 관련 정책을 수립한다.
- 컴퓨터 이용 시 운영체제에서 제공하는 기본 보호/보안 기능을 이용하고 관련 지침을 준수하는 것만으로도 대부분의 사이버 위협을 예방할 수 있으므로 관련 기능을 잘 사용할 수 있는 환경을 지원한다.
- 인터넷 포털이나 인터넷 통신망 제공자는 사용자의 파일들에 대하여 악성코드 등에 대하여

속도 저하 없이 검출하는 기법 등을 통하여 사용자가 악성코드 등에 쉽게 노출되지 않도록 예방 조치를 취한다.

- 국내 컴퓨터 운영체제의 분포는 90%정도가 윈도우즈 계열이며, 이중 70%정도가 최신 운영체제인 윈도우즈 10을 사용하고 있기 때문에, 그에 맞는 보안 정책 및 프로그램을 지원한다.
- 보안 업데이트가 중지된 제품의 경우, 다른 사용자의 피해를 최소화하기 위하여 업데이트 또는 저비용의 안전 운영체제(예; 리눅스) 등으로 이전을 홍보/계도화 하고 사용 환경을 지원한다.
- 휴대용 기기의 경우 안드로이드와 아이폰의 비율이 7:3정도이지만, 각 운영체제의 다양성이 존재하고, 운영체제의 버전을 모른다는 응답이 많아 제조 모델에 따른 보호 대책 등이 강구되어야 한다.
- 사이버 위협의 노출과 불안 정도는 개인정보탈취와 악성코드감염에 대한 순위가 높으며, 공격빈도도 많기 때문에 중점적으로 관련 정책 및 기술 지원을 통하여 보호한다.
- 불건전 콘텐츠에 대한 노출 정도가 증가하고 있기 때문에, 인터넷 서비스 제공자나 포털 서비스 업체들의 협조를 통하여 노출 수위와 범위를 제한한다.
- 최근 인터넷 장치의 해킹에 대한 우려가 높아지고 있기 때문에, 제조사의 보안 업데이트 지원과 단종된 제품에 대한 보호/보안 조치나 지원책을 마련해야 한다.
- 인터넷 사용 시 사이버 위협/공격에 대한 보호/예방책을 수립하지 않는 이유로, 비용의 증가, 성능의 하락, 신뢰성의 문제가 대두되기 때문에 국민 서비스의 일환으로서 저비용의 악성코드 백신/치료/제거 프로그램을 배포하고, 각 보안 프로그램에서 대한 성능 및 신뢰성을 검증하는 정책을 지원한다.
- 각 보안프로그램이 중복되어 설치되어 프로그램간의 충돌, 중복 기능 등으로 인한 성능하락, 사용이 불편하여 표준화된 비중복 보안프로그램의 제공이 필요하다.

5. 결 론

본 논문에서는 사이버 안전 분야에서 국민생활문제 해결을 위하여 시급한 문제와 국민들의 의식 수준을 파악하여 국민들 스스로 사용 환경에 대한 보안을 유지하고 안전한 사이버 생활을 영위할 수 있도록 지원할 수 있는 기초 정보를 제공하기 위하여 사이버 안전에 관한 국민 인식을 조사하고 분석하였다.

사이버 안전에 대한 국민인식 조사를 위하여 국내·외 문헌을 조사하고, 심도 있는 의견을 수집하기 위한 전문가 그룹 자문 회의 등을 통하여 설문 문항을 구성하였고, 다양한 각도에서 분석을 진행하였으며, 활용 및 요구사항을 제시하였다. 제안된 활용 및 요구사항을 통하여 국민 모두가 스스로 사이버안전을 지켜서 건전한 콘텐츠와 서비스가 유통되는 사이버 세상이 되길 기대한다.

이 논문은 2018년도 한국전자통신연구원의 지원을 받아 수행된 연구임(EA20184053, 사이버 안전에 대한 국민 인식 분석 및 활용 컨설팅).

참 고 문 헌

[1] 과학기술정보통신부, 한국인터넷진흥원, “2018 인터넷이용실태조사”, 2019. https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw11241&artId=1643636

[2] 사이버안전 확보 기본 계획, 경찰청 사이버안전국, 2014. http://cyberbureau.police.go.kr/bureau/cyber_plan.pdf
[3] 미래창조과학부 사이버안전센터 운영규정, Jun. 5, 2013. https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw352&artId=1974356
[4] 이연수, 이수연, 윤석구, 전재성, “주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구”, 국가정보연구, 제1권 2호, pp. 35-116, 2009. http://www.kanis.or.kr/sample/board_view.php?bbs_id=magazine_search&kbbs_doc_num=13&page=11
[5] 송근혜, 이승민, “4차 산업혁명과 보안 패러다임 변화”, 정보통신기술진흥센터 주간기술동향 1847호, pp.16-27, May 2018. http://www.itfind.or.kr/publication/regular/weeklytrend/weeklymailzine/view.do?boardParam1=1028&boardParam2=1020
[6] 이승민, 송근혜, “정보보호동향 및 보안위협 분석”, ETRI Insight Report 2017-27, DOI: https://doi.org/10.22648/ETRI.2017.B.000042
[7] 박순태, 2013년 주요 침해사고 사례와 대응, 해킹방지워크샵, Dec. 4, 2013. http://www.kisa.or.kr/uploadfile/201312/201312041443047984.pdf
[8] 위키피디아, 대한민국의_정보_보안_사고_목록, Retrieved May 15, 2019. https://ko.wikipedia.org/wiki/대한민국의_정보_보안_사고_목록
[9] J. I. James, “사이버안전(Cybersecurity)란 무엇인가?”, Mar. 25, 2013. http://dfire.ucd.ie/

저 자 소 개

윤영선(Young-Sun Yun)

1990.2 KAIST 전산학과 졸업
1992.2 KAIST 전산학과 석사
2001.2 KAIST 전산학과 박사
2006.4-2007.2 한국전자통신연구원 초빙연구원
2012.8-2013.7 University of Washington 방문학자
2001.3-현재 : 한남대학교 교수
<주관심분야> 음성인식, 음성변환, 화자인식, 인공지능, 내장형시스템 등

안개일(Gae-il An)

1993.2 충남대학교 컴퓨터공학과 졸업
1995.2 충남대학교 컴퓨터공학과 석사
2001.8 충남대학교 컴퓨터공학과 박사
2006.7-2007.6 미국 Security University 박사후연구원
2001.8-현재 : 한국전자통신연구원 책임연구원
<주관심분야> 네트워크 보안, 네트워크 시뮬레이션, 모바일 디바이스 보안