연구총서 10-07

K O R E A N I N S T I T U T E O F C R I M I N O L O G Y

사이버안전체계 구축에 관한 연구

A Study on the Construction of Efficient System for Safe Cyberspace

강석구 · 윤해성 · 박영우 · 김민호 · 권헌영 · 김도승 · 김기범

KIC 한국형사정책연구원
Korean Institute of Criminology

▌강석구

한국형사정책연구원 연구위원, 법학박사

▌윤해성

한국형사정책연구원 부연구위원, 법학박사

▌박영우

한국인터넷진흥원 전문위원

▌김민호

성균관대학교 법학전문대학원 교수

▌권헌영

광운대학교 법과대학 교수

▌김도승

한국법제연구원 산업경제법제연구실 부연구위원

▌김기범

경찰청 사이버테러대응센터 경감

발간사

정부는 성숙한 세계국가로 도약하기 위하여 사이버 안전 확보를 국정과제로 삼는 한편, 통합적 안전체계 구축을 위하여 노력하고 있습니다. 저희 한국형사정책연구원도 정부의 이러한 정책기조에 발맞추어 주요 정보통신기반시설 및 공공과 민간 부문의 정보시스템을 보호하기 위한 형사정책적 대안을 제시함으로써 실효적인 사이버안전정책 수립에 기여하고자 합니다.

그런데 인터넷과 모바일로 대변되는 정보통신기술의 급속한 발달과 정보화의 정착에 따라 우리 사회 역시 21세기 고도 지식정보화 사회로 변모하게 되었지만, 이러한 지식정보화의 허점을 악용하여 해킹, 컴퓨터 웜·바이러스, DDoS 공격 등과 같은 공격적 사이버침해도 증가하고 있습니다. 더욱이 최근의 사이버침해는 단순한 자기과시형에서 벗어나 금전적인 이득추구형으로 변질되고 있으며, 개인정보의 대량유출 및 유출된 정보의 암거래도 성행하고 있습니다.

심각한 수준이라고 단정하기에는 아직 이르지만, 사이버공간 속에 우리가 이룩하고 축적한 수많은 업적과 정보들은 사이버공간이라는 가상의 공간을 바탕으로 하기 때문에 사소한 침해에도 취약할 수 있습니다. 더욱이 우리는 2009년 7월에 DDoS 공격이라는, 네트워크 트래픽을 기계적으로 증가시키는 단순한 공격에도 청와대 등 주요 사이트가 일시적으로 마비된 경험이 있고, IT선진국인 미국 국무부의 주요 외교문서가 고스란히 외부로 유출된 사례를 목격한 바 있습니다. 이는 미리 대책을 마련해두지 않는다면 어떠한 문명국가도 사이버침해로부터 자유롭지 못함을 의미합니다.

이에 형사정책 분야의 유일한 국책연구기관인 저희 한국형사정책연구원에서는 사이버안전 분야의 저명한 학자와 실무가를 공동연구자로 모시고, 다양한 방향에서 종합적·입체적 연구를 진행하여 사이버안전을 확보하기 위한 여러 대안을 마련하게 되었습니다. 법학적 방법론에 의한 연구라는 한계성은 가지지만 이 연구에서 제안한 범국가적 사이버위험 관리방안이나 제반 인프라 구축방안, 사이버 수사체계 정비방

안 등이 사이버안전 확보를 위한 국가사이버안전정책 수립에 기여하기를 바라며, 이 연구가 사이버안전 분야에 대한 형사정책적 연구의 초석이 될 것이라고 기대합니다.

끝으로, 만만치 않은 분야에 대한 연구임에도 충실하게 연구를 수행해준 강석구 연구위원과 윤해성 부연구위원의 노고를 치하하며, 바쁘신 와중에도 고견을 아낌없이 내어주신 성균관대학교 김민호 교수, 광운대학교 권헌영 교수, 한국인터넷진흥원 박영우 박사, 한국법제연구원 김도승 박사, 경찰청 김기범 경감께 감사드립니다.

2010년 12월

한국형사정책연구원
원장 김 일수

CONTENTS

국문요약 ····· 13

제1장 서론 ····· 23

제1절 연구의 목적 ····· 25

제2절 연구의 범위와 내용 ····· 28

제3절 연구의 방법 ····· 30

제2장 사이버안전의 이론적 고찰 ····· 33

제1절 사이버침해의 의의 ····· 35

1. 개 관 ····· 35

2. 다른 개념과의 구분 ····· 37

제2절 사이버침해의 유형 ····· 39

1. 의 의 ····· 39

2. 기존의 유형 분류 ····· 40

3. 사이버침해 유형 ····· 53

제3절 사이버침해 유형별 대응전략 개관 ····· 57

1. 사이버전 ····· 59

2. 사이버테러 (주요정보통신기반시설 보호) ····· 59

3. 일반 정보시스템 및 정보 침해 ····· 63

제3장 우리나라 사이버안전체계의 현황 ····· 65

제1절 사이버안전 관련 법제 ····· 67

1. 법제형성의 연혁 ····· 67

2. 사이버안전 관련 처벌규정 ····· 69
3. 사이버안전 업무수행의 법적 근거 ····· 79
제2절 국가정보원의 사이버침해 대응체계 개관 ····· 80
1. 국가사이버안전관리 체계 ····· 80
2. 위협정보 탐지 및 대응활동 ····· 85
3. 사이버위협 경보 및 대응 ····· 89
4. 사고조사 및 복구 ····· 101
5. 향후 과제 ····· 110
제3절 방송통신위원회의 사이버침해 대응체계 개관 ····· 114
1. 서 설 ····· 114
2. 방송통신위원회 사이버침해 대응체계의 법적 근거 ····· 115
3. 주요 정책 ····· 122
4. 인터넷침해대응센터 ····· 125
5. 분석 및 평가 ····· 126
제4절 경찰청의 사이버침해 대응체계 개관 ····· 127
1. 사이버수사의 법적 근거 ····· 127
2. 경찰청의 사이버범죄 대응전략 ····· 128
3. 경찰청의 사이버수사조직 ····· 130
4. 경찰청의 사이버수사활동 개관 ····· 131
5. 평가 및 개선방안 ····· 139
제5절 사이버침해 대응 국제협력체계 개관 ····· 149
1. 국제공조 관련 조약 및 법률 ····· 149
2. 국제기구 및 핫라인 운영현황 ····· 152
3. 수사기관 간 국제협력 활동 ····· 154
4. 평가 및 개선방안 ····· 155

제4장 주요국의 사이버안전체계 분석 ····· 159

제1절 미국의 사이버공격 대응체계 ····· 162

1. 개 관 ····· 162
2. 조직체계 ····· 165
3. 법제도 체계 ····· 169
제2절 영국의 사이버공격 대응체계 ····· 177
1. 개 관 ····· 177
2. 조직체계 ····· 178
3. 법제도 체계 ····· 182
제3절 독일의 사이버공격 대응체계 ····· 184
1. 개 관 ····· 184
2. 조직체계 ····· 185
3. 법제도 체계 ····· 188
제4절 프랑스의 사이버공격 대응체계 ····· 190
1. 개 관 ····· 190
2. 조직체계 ····· 191
3. 법제도 체계 ····· 196
제5절 일본의 사이버공격 대응체계 ····· 198
1. 개 관 ····· 198
2. 조직체계 ····· 201
3. 법제도 체계 ····· 205
제6절 비교법적 고찰의 시사점 ····· 207
1. 대응 조직 및 전략 측면 ····· 208
2. 법제도 측면 ····· 211

제5장 우리나라 사이버안전의 실태 ····· 213
제1절 사이버안전의 실태 ····· 215
1. 유형별 사이버침해 현황 ····· 215
2. 분야별 사이버침해 안전 실태 ····· 230
3. 향후 전망 ····· 237

제2절 사이버안전에 관한 전문가인식 ····· 240
1. 조사 개요 ····· 240
2. 사이버안전에 관한 전문가 인식조사의 주요 결과 ····· 243
3. 전문가 인식조사의 시사점 ····· 248

제6장 사이버안전체계의 구축방안 ····· 253
제1절 사이버안전체계 구축의 기본방향 ····· 255
1. 문제의 소재 ····· 255
2. 사이버안전정책 수립의 주요 쟁점 ····· 258
3. 사이버안전정책 수립의 현실적 한계 ····· 260
제2절 사이버위험 관리방안 ····· 262
1. 사이버위험 관리체계 설계의 전제조건 ····· 262
2. 재난관리체계와의 연계방안 ····· 264
3. 국가사이버위기 관리방안 ····· 267
4. 사이버안전 관련 제반 인프라 구축을 위한 제언 ····· 272
제3절 사이버 수사체계 정비방안 ····· 275

제7장 결 론 ····· 277

참고문헌 ····· 283

ABSTRACT ····· 297

부록 1. 국가사이버안전관리규정 ····· 303
부록 2. 국가사이버위기 관리법(안) ····· 311
부록 3. 사이버침해 사고 예방 및 대응 기법 ····· 318
부록 4. 전문가인식조사 응답 주요 내용 ····· 333

표 차례

〈표 1〉 경찰청 사이버테러대응센터의 사이버침해 유형 분류 ····· 41
〈표 2〉 한국인터넷진흥원 인터넷침해대응센터의 사이버침해 유형 분류 ····· 42
〈표 3〉 국가정보원 사이버안전센터의 사이버침해 유형 분류 ····· 43
〈표 4〉 국가정보원 사이버안전센터의 안보위해공격 유형 분류 ····· 43
〈표 5〉 국가정보원 사이버안전센터의 사고유형 분류 ····· 44
〈표 6〉 미국 국토안보부의 사이버보안 사고 유형 분류 ····· 45
〈표 7〉 독일 연방정보기술보안청의 정보시스템 위협행위 유형 분류 ····· 46
〈표 8〉 일본 JPCERT/CC의 컴퓨터 보안 인시던트 유형 분류 ····· 47
〈표 9〉 본 연구에서의 사이버침해 유형 분류 기준 ····· 57
〈표 10〉 주요 정보통신기반시설 지정 기준 ····· 61
〈표 11〉 분야별 주요 정보통신기반시설 현황 ····· 61
〈표 12〉 국가사이버안전업무 관련 법률 및 규정 ····· 69
〈표 13〉 단계별 법적 근거 ····· 86
〈표 14〉 사이버위협 경보 수준 ····· 91
〈표 15〉 사이버안전 전담조직 현황 ····· 98
〈표 16〉 사고조사 및 복구체계 ····· 102
〈표 17〉 증거확보 및 보존요령 ····· 107
〈표 18〉 피해복구 절차 ····· 109
〈표 19〉 법률별 대상 및 소관부처 ····· 112
〈표 20〉 사이버공격수단 및 단계별 피해 ····· 112
〈표 21〉 국가사이버위기 관리체계 구축시 국가정보원의 역할 ····· 113
〈표 22〉 정보보호지침의 포함 사항 ····· 117
〈표 23〉 보호조치의 구체적인 내용 ····· 118
〈표 24〉 주요 사이버 공격 일지 ····· 123
〈표 25〉 사이버범죄 신고민원 접수현황 ····· 133
〈표 26〉 디지털증거분석 실적 ····· 135

〈표 27〉 시기별 사이버 침해의 특징 ····· 217
〈표 28〉 사이버 위협 패러다임의 변화 ····· 217
〈표 29〉 국가사이버안전센터 공공기관 침해사고 신고처리 통계(연도별) ····· 219
〈표 30〉 인터넷침해대응센터 침해사고 신고처리 통계(연도별) ····· 221
〈표 31〉 인터넷침해대응센터 해킹신고처리 통계(연도별) ····· 222
〈표 32〉 인터넷침해대응센터 해킹신고처리 통계(피해기관별) ····· 223
〈표 33〉 국가사이버안전센터 공공기관 해킹신고처리 통계(연도별) ····· 225
〈표 34〉 국가사이버안전센터 공공기관 해킹신고처리 통계(피해기관별) ····· 225
〈표 35〉 인터넷침해대응센터 웜·바이러스 감염신고처리 통계(연도별) ····· 227
〈표 36〉 국가사이버안전센터 공공기관 악성코드 감염 신고처리 (연도별) ····· 228
〈표 37〉 국가사이버안전센터 공공기관 악성코드 감염 신고처리 통계(피해기관별) ····· 229
〈표 38〉 국내·외 주요정보통신기반시설 제어시스템 피해사례 ····· 232
〈표 39〉 2006~2009년 정부 공공부문 침해사고 현황 ····· 234
〈표 40〉 2007년 공공분야 사이버 침해사고 발생 현황 ····· 236
〈표 41〉 전문가 인식조사 설계표 ····· 241
〈표 42〉 전문가 인식조사 주요 설문내용 ····· 242
〈표 43〉 정보화 예산 대비 정보보호 예산 비율 ····· 274

그림 차례

[그림 1] 주요 정보통신기반시설 보호계획 수립 절차 ····· 62
[그림 2] 국가사이버안전 관리체계 ····· 81
[그림 3] 사이버 위협 단계별 발령경보 ····· 88
[그림 4] 평시 업무흐름 체계도 ····· 95
[그림 5] 사고조사 업무흐름 체계도 ····· 102
[그림 6] 프랑스 사이버 보안 관련 국가적 조직체계 ····· 191
[그림 7] 프랑스 DCSSI 조직도 ····· 192
[그림 8] 정보통신기반보호를 포함한 재난·안전관리 체계 ····· 266

국문요약

1. 연구의 의의

가. 연구의 배경

2009년에 발생한 '7·7 DDoS 공격 사태'를 비롯하여 최근 해킹, DDoS 공격 등 사이버침해에 따른 위험이 증가하고 있다. 특히 최근의 사이버침해 사고는 주민등록번호, ID, 비밀번호 등 개인정보를 유출하여 금전적 이익을 추구한다는 점에서 종전보다 위험성이 증가하고 있고, 유출된 개인정보의 암거래까지 성행하고 있어 문제라고 할 것이다. 이와 함께 공공부문의 주요 정보통신기반시설을 대상으로 하는 사이버침해도 증가 추세이며, 특히 국가기관을 대상으로 하는 해킹은 매년 300% 내외로 증가하는 추세이기 때문에 사이버공격에 의한 국가기능 마비 우려도 증대되고 있다. 예컨대 2009년 발생한 '7·7 DDoS 공격'에 의하여 청와대, 금융기관 등 주요 사이트가 일시적으로 마비된 바 있으며, 대응책 마련에도 불구하고 금년 역시 동일시기에 재발한 바 있다. DDoS 공격의 경우 악성코드에 감염된 좀비 PC를 이용한다는 점에서 신속하고 효과적인 대응이 어렵다는 한계도 나타낸다.

이에 대응하여 정부는 '정보화촉진기본법'을 '국가정보화기본법'으로 전면개정하고, '국가사이버안전관리규정'을 보완하는 등 사이버위기관리 관련 법제를 전면적으로 점검하였으며, 민간분야는 한국인터넷진흥원 인터넷침해대응센터가, 국가·공공분야는 국가정보원 국가사이버안전센터가, 국방분야는 국방부 사이버사령부가 전담하는 민·관·군 종합대응체계도 현재 구축하고 있다. 다만 정부가 사이버침해 내지 사이버공격에 대응한 법제도를 대폭적으로 손질했음에도 불구하고 물리적·기술적·제도적 한계 등으로 인하여 사전예방이나 범인 추적은 제대로 이뤄지지 못하였고, 국민과 정부의 불안감은 여전히 지속되었다.

나. 연구의 목표 및 방법

이 연구는 이러한 사이버침해 내지는 사이버공격, 더 나아가 이로 인해 촉발된 사이버위기에 대응한 사이버안전체계 구축을 목표로 한다. 이를 위하여 이 연구는 전문분야가 다른 연구자들과 역할을 분담하여 연구를 진행하였으며, 방법론상 법학적 방법론을 채택하되 이를 유형적 고찰, 현황 분석, 비교법적 고찰, 실증적 고찰로 구분하여 다각적·입체적으로 분석하고자 하였다.

2. 사이버안전의 이론적 고찰

가. 사이버침해의 의의

이 연구에서 '사이버침해'란 "사이버공간(인터넷)을 통하여 정보시스템·네트워크에 침입 또는 이를 교란·마비·파괴하거나 정보를 누출·훼손·왜곡전파하는 행위 또는 그 결과"라고 할 수 있으며, 정책적 또는 법적 가치판단이 아닌 객관적·사실적으로 접근한 개념이다.

나. 사이버침해의 유형

사이버침해 유형은 공격 수법과 피해를 기준으로 분류하는 것이 정석이나, 안전실태 파악과 대응전략을 수립하는 데 있어서는 공격 수법과 피해, 공격 대상, 공격자 등을 종합적으로 고려하여 사이버전(戰), 사이버테러(주요 정보통신기반시설 침해), 일반 정보시스템 및 정보 침해로 구분하는 대분류가 기술적 세분류보다는 유용할 것이다.

다. 사이버침해의 유형별 대응전략

사이버전(戰)은 국제법에서 논의되어야 할 사안으로서, 현재는 사이버전 선전포고 시점의 불명확성, 적대국 불확실성, 여러 나라를 거치는 라우팅 경로에 따른 국제적

협조 근거 부재 등이 주요 문제점으로 지적되고 있으므로 근원지, 동기, 대상을 명확하게 밝힐 수 있는 국제 조약, 국제 협약 등이 마련되어야 한다. 또한, 국가적으로 중요한 정보시스템 및 정보통신망과 같은 주요 정보통신기반시설에 대한 사이버테러의 경우 취약점 분석·평가, 보호대책 및 보호계획의 수립 등의 조치가 필요하다. 이밖에 사이버 침해사고 대응의 실효성을 거두기 위해서는 민간부문에 대한 정보보호 인식 제고와 좀비PC 제거 등의 노력이 요구된다.

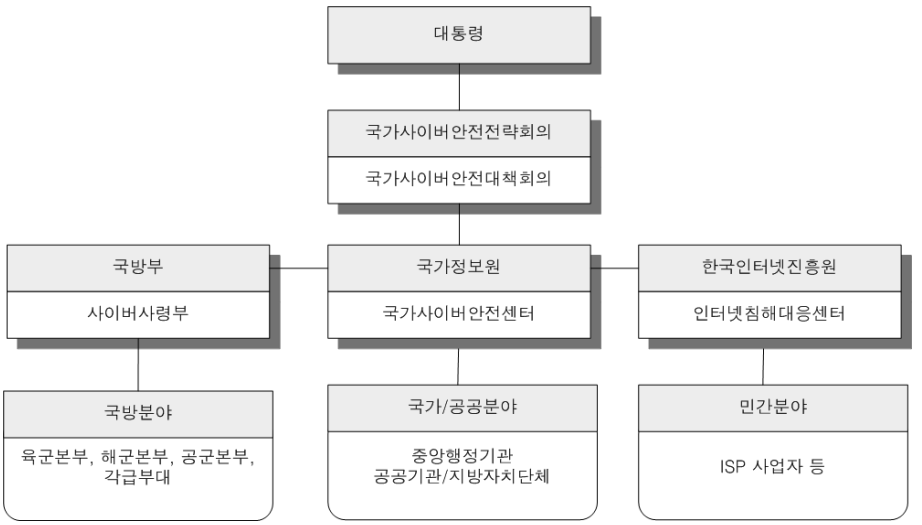
3. 우리나라 사이버안전체계의 현황 분석

가. 사이버안전 관련 법제

사이버안전 관련 근거법률로는 국가정보화기본법, 정보통신기반보호법, '정보통신망 이용촉진 및 정보보호 등에 관한 법률', 전자정부법, 국가정보원법 등이 있고, 이밖에 보안업무규정, 정보 및 보안업무 기획조정 규정, 국가사이버안전관리규정, 국가위기관리기본지침, 국가정보보안기본지침 등이 마련되어 있다. 처벌법규는 형법 이외에도 정보통신기반보호법 등 특별법에 산재하여 있다.

나. 국가정보원의 사이버침해 대응체계

국가사이버안전체계는 '국가사이버안전관리규정'에 의해 정부가 국가안보차원의 사이버위협에 대한 대응을 보다 강화하여 국가 인터넷망의 전자적 침해사고 조기탐지 및 피해확산 방지를 위해 구축한 범국가적 체계로서, 한국인터넷진흥원의 '인터넷침해대응센터'가 민간분야를 담당하고, 국가안전보장회의(NSC) 사무처 주관 하에 범정부적 차원에서 출범한 국가정보원 소속의 '국가사이버안전센터'(NCSC)가 공공분야를 담당하며, 국방정보본부 산하의 '사이버사령부'가 군 분야를 담당하는 민·관·군 종합 대응체계이다.



〈그림〉 국가사이버안전 관리체계

국가정보원 소속의 국가사이버안전센터는 사이버공격에 대한 국가차원의 체계적인 대응을 위해 2004년 2월 설립된 기관으로서, 정보통신망에 대한 24시간 사이버 위협정보를 수집·분석·전파하는 국가 종합상황실을 운영하면서 각종 사이버공격에 대한 예방·대응활동과 피해확산 방지에 주력한다. 또한, 국가·공공기관 등 공공분야를 대상으로 사이버위협에 대한 수준별 경보발령 등 각종 사이버공격에 대응하고, 24시간 네트워크 보안관제를 통해서 사이버위협 정보를 수집·분석하여 각급기관에 전파하며, 침해사고 발생 시 긴급대응·조사 및 복구를 지원하고 유관기관과의 정보협력을 강화하고 있다.

다. 방송통신위원회의 사이버침해 대응체계

방송통신위원회는 구 정보통신부의 통신정책 및 통신규제기능과 방송위원회의 방송정책 및 방송규제기능을 통합하여 2008년 출범한 대통령소속 중앙행정기관으로서, 현 정부 출범 초기부터 안전하고 건전한 방송통신 이용환경 조성을 위하여 2008년 7월 인터넷정보보호 종합대책을 수립하고 침해사고 대응, 개인정보 보호, 유해정보 대응, 정보보호 기반조성 등의 4대 분야별 대책 50개를 선정하여 추진 중이다. 다만

2008년 출범 초기에 방송통신위원회는 주로 방송정책과 통신정책의 융합 및 산업적·진흥적 관점의 정책에 집중하는 모습을 보여 왔지만, 2009년 7·7 DDos 공격 이후 사이버침해 대응이 주요 정책이슈로 부상하면서 최근 '인터넷침해대응센터'를 중심으로 하여 정보보호에 관한 정책대응이 크게 강화된 것이 특징적이다.

라. 경찰청의 사이버침해 대응체계

경찰청은 수사국 내에 사이버테러대응센터를 두고, 사이버테러의 탐지, 추적수사 및 경보 등 조치, 사이버테러 관련 수사기법의 연구·개발 및 국제경찰기구 등과 협력, 사이버범죄의 수사 및 지도, 디지털매체 등 증거분석 업무를 수행하고 있다. 또한, 경찰청은 중앙단위에 별도의 수사조직을 운영하고 있는데, 주로 사이버테러 대응, 국제공조수사를, 지방청은 개인정보 유출, 음란·도박사이트 단속 등 인지수사를, 경찰서는 인터넷 사기, 사이버명예훼손, 디지털 저작권 침해, 음란물 유포 등을 수사하고 있다.

마. 사이버침해 대응 국제협력 체계

국제공조 관련 조약으로는 유럽평의회 사이버범죄 조약, UN 반초국가조직범죄 조약이, 법률로는 국제형사사법공조법이 시행되고 있다. 또한, 사이버침해와 관련한 국제공조네트워크로는 인터폴의 '사이버수사 핫라인', G8의 '24/7 네트워크', 일본 경시청의 '사이버범죄 기술정보네트워크'(CTINS)가 가동되고 있다.

4. 주요국의 사이버안전체계에 관한 비교법적 고찰

가. 미 국

미국은 국토안보부(DHS)를 중심으로 대통령직속 주요기반보호 협의회(PCIPB), 연방수사국(FBI) 국가기반보호센터(NIPC) 등이 운영되고 있고, 이들은 애국법, 국토안보법, 관리예산처 지침, 사이버보안연구개발법, 컴퓨터보안법, PDD-63(중요기반시설

보호), HSPD-63(국내 사고관리) 등에 기반하여 활동하고 있다. 이 밖에도 사이버보안법안, 국가자산으로서 사이버공간 보호법안 등이 의회에 계류 중이다.

나. 영 국

영국의 사이버안전체계를 보면, 네트워크 및 정보보호 정책은 내각부 산하의 정보보증 중앙지원국(CSIA)에서 정보보호 관련 활동에 대해 정부전체를 조정하며, 통상산업부(DTI), 외무부 산하 정부통신총국(GCHQ)·통신전자보안단(CESG) 및 내무부 보안정보부(M15) 산하 국가기반보호센터(CPNI) 등이 국가전반에 걸친 정보보호 기관으로서 역할을 수행하고 있다. 또한, 조사권한규제법(RIPA), 컴퓨터부정사용법, 대테러 범죄 및 안전 보장법 등으로 해커와 바이러스 유포자를 처벌하고 있으며, 스팸규제는 프라이버시법리와 전기통신지침 등으로 이루어지고 있다.

다. 독 일

독일의 사이버안전은 '연방정보기술안전청설치법'(BSIG)에 의해 설립된 연방정보기술안전청(BSI) 및 연방통신망청법상의 연방통신망청(BNetzA)이 주로 담당하고 있다. 또한, 독일은 정보보안을 통해 정보통신기술의 신뢰를 조성하고 정보사회의 기회를 최대한 이용하기 위해 독일 자체의 정보보안 가이드라인을 제정하여 시행하고 있다.

라. 프랑스

프랑스는 중앙정보시스템보안국(DCSSI) 내에 프랑스 정부 CERT인 CERTA를 구축, 운영하고 있으며, 사이버보안운영센터를 구축하여 각급기관에 사이버위협정보를 제공하고 있다. 또한, 프랑스는 사이버 보안을 국가 안보의 문제로 인식하여 총리실 직속의 국방사무국(SGDN)으로 하여금 사이버 보안을 담당하도록 하고 있다.

마. 일 본

일본은 전체적으로 내각관방을 중심으로 경찰청·방위청·총무성·경제산업성이

각각 정보보호정책을 추진하는 시스템을 갖추고 내각관방이 각 부처를 총괄·조정하는 역할을 담당하고 있다. 각 부처별로는 일본 경찰청은 2001년 사이버포스(Cyber Force)를 창설하여 하이테크범죄 예방에 주력하고 있고, 방위청은 2003년 '방위물자 조달에 관한 정보보호기본방침'을 수립하여 조달업무에 관한 정보시스템과 DB 등의 보안대책을 추진하고 있으며, 총무성은 2002년 인터넷사업자(ISP)를 중심으로 '인터넷침해사고 정보공유분석센터'를 설립하여 인터넷 해킹 등에 대비하고 있다.

5. 우리나라 사이버안전 실태에 관한 실증적 고찰

가. 우리나라 사이버침해의 실태

사이버침해의 위해 및 피해 가능성은 계속해서 높다고 할 수 있다. 이는 사이버침해 행위자들이 고도의 전문성을 갖고 있으며, 배후에 범죄조직이 있는 경우가 많기 때문이다. 또한, 공격 대상이 될 수 있는 시스템과 정보도 많아졌다. 이는 전자정부, 전자상거래 그리고 최근의 모바일 오피스 혹은 스마트 오피스 등의 추진으로 더욱 심화되고 있다. 한편, 사이버침해는 피해자가 공격 및 피해 사실을 알지 못하는 경우가 많고, 특히 기업의 경우 이를 알더라도 신용훼손을 우려하여 신고하지 않는 경우가 많기 때문에 각종 통계를 통해 알 수 있는 공격 및 피해보다 훨씬 많은 공격 및 피해가 발생하고 있다고 본다.

유형별로 살펴보면, 해킹 접수·처리건수는 2005년까지 크게 증가(33,633건)하다가 2006년 이후 상당히 감소하는 추세였으나(2008년도 15,940건), 2009년에 7·7 DDoS 공격 등의 영향으로 소폭 증가하였으며(21,230건), 스팸릴레이, 단순침입시도, 홈페이지 변조가 주를 이루고, 피싱경유지로 악용되는 경우는 감소하고 있다. 웜·바이러스 신고건수는 2009년 10,395건으로 2008년 대비 22.7% 증가하였고, 특정 온라인 게임의 계정정보 탈취를 목적으로 하는 온라인게임 해킹의 신고 건수가 10.8%로 가장 높은 비율을 차지하였다. DDoS 공격의 경우 2009년 7월 7일부터 9일까지 3차례에 걸쳐 국내 주요 공공기관과 이용자 방문이 많은 포털, 금융 사이트 등 총 26곳을 공격한 사례가 보고되었고, 이해관계가 없는 국내 PC 1만 2,000여대와 해외

PC 8,000여대가 공격에 이용되었다고 한다.

나. 사이버보안실무자 대상 전문가 인식조사

공공기관 및 민간기관의 사이버정보보안 실무책임자 25명을 대상으로 하여 전문가 인식조사를 실시한 결과, '안전' 또는 '위기'에 대한 판단에 오류가 있을 경우 불요불급한 업무 마비와 사회구성원의 불편, 나아가 국민의 불안감을 증폭하거나 국력 낭비만을 초래할 우려가 있음에도 실무상 '안전'이나 '위기'를 판단할 구체적 기준이 미흡하고, 영리를 추구하는 기업의 속성상 민간기업이 이윤창출과 거리가 있는 고비용의 정보보안시스템을 제대로 구축하기란 현실적으로 무리가 있으며, 민간분야 정보보호가 취약할 수밖에 없는 현실에서 인터넷실명제 등 본인확인제의 확대는 사이버안전을 위협하는 환경을 더욱 조장할 수 있고, 법제도를 정비함에 있어 흔히 제기되는 사이버침해행위에 대한 가중처벌방안은 그 효과도 의문이지만 전문가들이 인식하는 가장 효과적인 대응수단도 아니라는 점 등을 시사점으로서 도출하였다.

6. 사이버안전체계의 구축방안

가. 사이버안전체계 구축의 기본방향

사이버안전정책은 정보통신 및 정보저장 방식의 급변 및 다변화, 정보보안의 기술적·경제적 한계, 사이버공격 추적·수사의 현실적 한계 등을 고려하는 한편, 다음에 열거하는 쟁점을 참고하여 수립하여야 할 것이다.

(1) 국가안보와 직결된 보다 높은 수준의 위험에 대해서는 중앙통제방식이 적절하다고 판단되지만, 이를 준전시상황으로 보아야 할지, 위기상황으로 보아야 할지, 재난상황으로 보아야 할지에 대해서는 보다 논의할 필요가 있다.

(2) 위기에 이르지 않는 위험 또는 일상적인 위험에 대해서는 분산관리방식이 적절하다고 판단되지만, 어느 기관이 어떤 역할과 기능을 분담해야 할지는 보다 논의가 필요하고, 어느 정도를 '안전' 또는 '위기'라고 판단할지 그 구체적 기준 마련에 대해서도 연구가 필요하다.

(3) 사이버안전 문제는 민간분야과의 협력, 나아가 국가 간의 협력이 필요한 사안이라고 판단되지만, 민간분야와 협력해야 할 경우 경제적 부담 및 상황인식의 차이를 고려해야 할 것이며, 국가 간의 협력의 경우 실효성 확보를 위한 고민이 요구된다.

(4) 사이버안전을 확보하기 위해서는 정보화정책와 정보보안정책 간의 차별성 확보 및 인터넷건전성과 사이버안전성이라는 상반된 가치의 조화가 필요하다고 판단된다. 다만 양자를 모두 규제하는 것은 적절치 않으므로 어느 쪽을 규제하고 자율에 맡길지에 대한 논의가 필요하다.

(5) 사이버수사의 실효성을 확보하기 위해서는 초동수사의 실효성을 확보하는 것이 가장 중요하고, 이를 위해서는 초동수사의 관할을 현실에 부합되게 조정할 필요가 있다고 판단된다. 다만 사이버공격의 경우 '수사'보다는 '방어'와 '피해복구'가 우선할 수 있다는 점에 유의해야 한다.

(6) 사이버안전 관련 조직과 인력, 권한과 예산을 조정할 필요가 있다고 판단되며, 이를 위해서는 법제 정비가 필요할 수 있다. 다만 무조건적인 확대 내지 행정권한 강화는 적절하지 못하다고 판단되며, 보안기술 개발과 같은 공공인프라 구축에 지원이 집중될 필요가 있다.

나. 범국가적 사이버위험 관리방안

사이버위험의 정도를 측정할 수 있고 사이버위험 대응체계를 차별화할 수 있다는 전제에서 범국가적 사이버위험 관리체계 구축을 위한 종합적인 대안으로서 재난상황을 전제한 행정안전부 중심의 '재난관리체계와의 연계방안'과 사이버위기상황을 전제한 국가정보원 중심의 '국가사이버위기 관리방안'을 제시하였다.

'재난관리체계와의 연계방안'은 사회 인프라의 마비로 인한 피해를 재난으로 보고 관리한다면 해당 사회 인프라의 기능 수행에 중요한 역할을 하는 정보통신기반시설도 재난관리의 내용에 포함하여야 한다는 전제에서, 융합 시대에 맞게 현행 정보통신기반시설 보호체계를 재난관리체계와 연계, 통일시키자는 제안이며, '국가사이버위기 관리방안'은 국가사이버위기를 효과적으로 예방·대비하고 대응·복구하기 위해서는 국가가 직접 나서서 자원을 기획·조직·조정·통제할 필요가 있다는 전제에서, '국가사이버위기 관리법'(안)을 바탕으로 하여 새로운 범국가적 사이버위기관리

체계를 갖추자는 제안이라고 할 것이다.

참고로, 사이버위험 관리체계를 범국가적으로 구축할 필요가 있더라도 이는 필요한 최소한의 범위에서만 허용되어야 할 것이며, 사이버안전환경 구축을 위해서는 제반 인프라 확충도 중요하므로 전문인력 양성 및 확보, 관련 연구·개발 증진, 적절한 정보보호 예산의 확보, 불요불급한 개인정보 수집·보관의 최소화 등의 대안도 함께 제시하였다.

다. 사이버수사체계 정비방안

초동수사의 중요성을 감안할 때 경찰청의 사이버수사체계를 사후 추적수사에서 사전탐지 및 조기대응 체제로 전환할 필요가 있으며, 이와 함께 사이버범죄 수사 대응 및 대응 관련 법규 정비 필요성, 주요 기반시설 사이버침해 피해에 대한 수사기관 고발 의무화, 한국인터넷진흥원의 WHOIS 정보 정확성 제고의 필요성, 전담조직 위상 강화, 민간 IT전문가 경찰관 특채 확대, 사이버테러 전문수사관 양성 등 사이버수사 전담조직 및 전문성 확보방안, 사이버치안 거버넌스 강화 등 유관기관 및 민간분야 협력방안, 사이버범죄 예방에 관한 수익자 부담원칙 도입방안 등의 방안을 제시하였다.

제1장
서론

01 서론

제1절 연구의 목적

한국통신이 최초로 인터넷 상용서비스를 개시한 1994년 6월 이후 고작 16년여의 시간밖에 지나지 않았지만, 인터넷 보급 이후 우리 사회는 그 이전에 상상했던 수준 이상으로 정보통신 환경의 급변(急變)을 경험하게 되었다. 문서작업과 게임기 정도로만 활용되던 거대한 애물단지 데스크탑 컴퓨터는 랩탑, 노트북, 태블릿 등으로 점차 크기가 작아지더니 이제는 바지주머니 속에 쏙 들어오는 모바일 스마트폰으로 진화하였고, 이른바 유비쿼터스(Ubiquitous) 환경 구축이 진전됨에 따라 정치, 경제, 사회, 문화 등의 다양한 컨텐츠뿐만 아니라 전자상거래, 금융서비스, 행정민원서비스 등의 용역서비스까지도 장소와 시간에 구애받음 없이 자유롭게 이용할 수 있게 되었다. 이처럼 정보통신기술의 급속한 발달은 우리가 상상 속에서만 꿈꾸던 일들을 현실로 만들어가고 있고, 우리 사회의 거의 모든 영역에서 변화와 편익을 실현해나가고 있다. 그래서 오늘날을 '고도 지식정보화 사회의 도래'라고 표현해도 무방할 것이다.

그런데 정보통신기술의 획기적 발전과 이에 따른 지식정보화의 급속한 진전이 우리 사회에 변화와 편익을 실현하기도 했지만, 새롭고 편리한 만큼 이러한 문명이기에 대한 우리 사회의 의존도도 급속히 높아져만 갔다. 익명성이 특징인 사이버공간에서 이용자의 실명(實名)과 주민등록번호는 필요불가결한 신원확인 도구가 되었고, 종래 중요한 재산권 행사에서 본인확인을 위해 반드시 요구되었던 인감(印鑑) 역시

점차 공인인증서로 대체되고 있다. 실명, 주민등록번호, 공인인증서 등을 활용한 전자상거래 등이 활성화되고, 온라인을 기반으로 하는 사회·경제 활동이 오프라인을 기반으로 하는 활동 못지않게 늘어갔다. 종이를 기반으로 하는 문서들도 상당 부분 전자문서로 대체되었고, 이는 행정문서라고 하여 예외는 아니었다. 오히려 공공분야의 지식정보화는 세계 어느 나라에 뒤지지 않을 정도로 신속하고 광범위하게 진행되었다. 이로 인해 국민들이 인터넷 도입 이전에 비하여 보다 높은 편익과 자유를 향유할 수 있게 된 것도 분명하다.

그러나 정보통신기술의 획기적 발전과 이에 따른 지식정보화의 급속한 진전이 순기능만 가져온 것은 아니고, 급속한 변화에 따른 새로운 불안요소도 만들어냈다. 익명성의 배후에 숨은 비방과 욕설·성희롱, 인터넷의 전파성에 편승한 정치적 포퓰리즘, 타인의 창의(創意)와 노력에의 무임승차, IT 문맹층, 노인·청소년을 대상으로 한 사기와 협잡, 사이버공간에서의 아바타 살해와 폭력성 등 고대사회의 혼돈상태가 현대사회의 사이버공간에 재현되고 있다. 더욱이 이러한 혼돈은 사이버공간에만 머무는 것이 아니라 이제는 현실공간에도 많은 영향을 미치고 있지만, 시공간의 제약을 받지 않는 인터넷의 특성상 현실권력의 개입에는 한계가 나타나고 있다.

또한 정보통신기술이 획기적으로 발전한 만큼, 한편으로는 정보통신을 침해하는 기술 역시 획기적으로 발전하였다. 해킹과 바이러스로 대별되던 침해기술은 이제 이름조차 알지 못하는 다양하고 창의적인 기법으로 진화하였고, 범죄수법의 진화속도를 수사기법이 쉽게 따라갈 수 없듯이 침해를 방비하기 위한 보안기술의 개발 역시 침해기법의 진화속도를 쫓아가지 못하고 있다. 더욱이 수많은 개인정보와 영업비밀 등이 인터넷에 방치되어 있는 한, 이를 수집하고 이를 통해 수익을 창출하고자 하는 시도는 쉽게 근절되지 못할 것이고, 지금 이 순간에도 계속되고 있을 것이다.

그런데 몇몇 범죄가 창궐한다고 하여 곧 국가와 사회가 붕괴되고 인류가 멸절하는 것은 아닐 테지만, 사이버공간 속에 우리가 이룩하고 축적한 수많은 업적과 정보들은 사이버공간이라는 가상(假想)의 공간을 바탕으로 하기 때문에, 즉 언제라도 허물어질 수 있는 사상누각(砂上樓閣)과 다름이 없기 때문에 사소한 침해일지라도 이를 제대로 방어하지 못한다면 망실(亡失)의 위험에 처할 수 있음도 부인할 수는 없다. 특히 인터넷에 대한 의존도가 비약적으로 높아진 오늘날, 사이버공간의 해체는 이와 연계된 현실 속 지식정보 기반의 붕괴 또는 사회통제 체제의 붕괴로 이어질 수 있기

때문에 결코 가볍게 다룰 문제가 아니다. 실제 최근의 이라크전에서도 경험하였듯이 현대전(現代戰)은 정보통신 기반의 타격을 최우선 목표로 하여 전개되는 양상을 나타내고 있다. 그래서 사이버공간을 형성하고 지지(支持)하는 시스템과 네트워크 등의 안전성을 확보하는 일이 국정(國政)의 최우선과제 중 하나가 될 수밖에 없음은 지극히 당연한 귀결이라고 할 것이다.

다만 2009년 7월, 청와대 등 우리나라의 주요 사이트를 일시적으로 마비시킨 '7·7 DDoS 공격' 사례에서도 경험하였듯이 네트워크 트래픽을 증가시키는 지극히 원시적이고도 단순한 공격에도 우리의 최첨단 보안시스템이 무력해진 바 있고, 정부 차원에서 이에 대한 대비책을 다양하게 마련했음에도 불구하고 금년 동일시기에 재발하였음을 감안한다면 사이버공간, 그리고 이를 형성하고 지지하기 위해 전 세계에 퍼져있는 네트워크의 안전성 확보가 결코 일국(一國)의 노력만으로 달성될 성질의 것이 아니라는 사실도 분명하다. 더욱이 최근 미국 국무부의 주요 외교문서 12만 건이 위키리크스(wikileaks.ch)로 유출된 사례는 어떠한 문명국가도 사이버침해 내지 공격으로부터 자유롭지 못함을 시사한다.

그래서 이 연구는 사이버공간, 그리고 이를 형성하고 떠받치는 시스템과 네트워크의 안전성 확보를 위한 형사정책 분야의 대안을 발굴하기 위하여 기획되었다. 물론 형사정책적 연구는 범죄의 원인과 실태, 범죄자의 특성 등을 분석하여 범죄를 예방하고 범죄자를 단죄함으로써 법과 정의를 바로 세우는 것을 목표로 하기 때문에 사이버침해나 사이버공격과 같은 시공간(時空間)을 초월한 범죄에 대한 효과적인 대안을 제시함에는 한계가 있을 수 있으나, 법학적 방법론에 따라 사이버침해 내지 사이버공격을 유형화하고, 유형별 또는 기능별 실태와 대응현황을 체계적으로 정리해둠으로써 이 연구뿐만 아니라 후속 연구의 기초자료로서 활용될 수 있는 기반을 조성하는 한편, 다른 분야에서 소홀히 다루기 쉬운 법적·제도적 맹점과 한계에 초점을 맞춤으로써 기술적으로 극복하기 힘든 여러 문제들을 제도적으로 보완하는 합리적 대안 내지 화두(話頭)를 제시하고자 한다.

제2절 연구의 범위와 내용

이 연구는 사이버공간(cyberspace)의 안전성을 확보하기 위하여 그 기반시설인 시스템과 네트워크를 보호하기 위한 체제를 구축하는 것을 목표로 한다. 그렇기 때문에 이 연구는 일반적인 사이버범죄가 아니라 시스템과 네트워크에 침입하거나, 이를 교란·마비·파괴하거나, 시스템에 축적된 정보를 누출·훼손·왜곡전파하는 행위를 대상으로 한다.

이와 관련하여 이러한 행위를 실무상 '사이버침해'라고 표현하기도 하고, '사이버공격'이라고 표현하기도 한다. 또한 사이버침해 또는 사이버공격으로부터 시스템 및 네트워크를 보호하는 행위를 '사이버보안'이라고 표현하기도 하고, '사이버안전'이라고 표현하기도 한다. 이처럼 이들 행위를 나타내는 용어가 실무상으로 통일되지는 못했지만, 인터넷이 보급된 것이 그리 오래되지 않은 일이며 관련 제도 정비가 아직도 진행 중임을 감안한다면 용어가 일관되지 못함은 아직은 불가피하다고 할 것이다. 그래서 이 글에서는 용어를 인위적으로 통일시키지 않고, 사안에 따라 보다 적절한 용어를 선택하여 사용한 점을 미리 밝힌다.

이 연구는 이러한 전제에서 사이버침해, 사이버공격 및 사이버안전 문제에 접근하였고, 법학적 방법론을 바탕으로 전문분야가 다른 공동연구자들과 역할을 분담하여 다음과 같이 논의를 전개하였다.

먼저, 제2장에서는 '사이버안전의 이론적 고찰'을 행하였는데, 제1절에서는 사이버침해의 의의를, 제2절에서는 사이버침해의 유형 분류를 다루었다. 이 두 절은 이 연구의 기초연구로서의 성격을 가진다. 또한, 이러한 유형 분류를 바탕으로 제3절에서 사이버침해 유형별 대응전략을 개관하였다. 제2장의 내용은 한국인터넷진흥원의 박영우 전문위원이 주로 집필하였다.

제3장에서는 '우리나라 사이버안전체계의 현황'을 살펴보았는데, 우선 제1절에서는 사이버안전 관련 법제를 법제형성의 연혁, 사이버안전 업무수행의 법적 근거, 사이버침해 관련 처벌규정 등으로 나누어 살펴보았다. 이 내용은 한국형사정책연구원 윤해성 부연구위원을 중심으로 실무연구진이 함께 집필하였다.

이 중 형사정책적으로 보다 심도 있는 분석이 필요한 국가정보원, 방송통신위원회, 경찰청 등 3개 기관의 사이버침해 대응체계에 대해서는 절을 바꾸어 각각 살펴

보았는데, 먼저 국가정보원의 사이버침해 대응체계에 대해서는 제2절에서 국가사이버안전관리 체계, 위협정보 탐지 및 대응활동 체계, 사이버위협 경보 및 대응체계, 사고조사 및 복구체계 등을 개관하였는데, 성균관대학교 김민호 교수를 중심으로 실무연구진이 함께 집필하였다. 방송통신위원회의 사이버침해에 대해서는 제3절에서 법적 근거, 주요 정책, 인터넷침해대응센터, 분석 및 평가로 나누어 살펴보았고, 광운대학교 권헌영 교수가 주로 집필하였다. 경찰청의 사이버침해 대응체계에 대해서는 제4절에서 사이버수사의 법적 근거, 사이버범죄 대응전략, 사이버수사조직, 경찰청의 사이버수사활동 등을 살펴보았고, 이 밖에 제5절에서는 사이버수사 관련 국제협력체계를 개관하였다. 제4절과 제5절의 내용은 경찰청의 김기범 경감이 주로 집필하였다.

제3장에서 우리나라의 현황을 살펴보았으므로 제4장에서는 미국, 영국, 독일, 프랑스, 일본 등 주요국의 사이버안전체계를 조직체계와 법제도를 중심으로 비교법적으로 고찰하였다. 사이버침해 대응체계 구축을 위한 나름의 노력은 모든 나라에서 발견되지만, 특히 미국은 책임과 권한이 여러 부처에 분산됨으로 인해 발생하는 정책의 혼선을 방지하고 모든 역량을 한 곳에 집중하기 위해 국토안보부(DHS)의 창설로 대표되는 효율적인 대응체계를 마련한 것으로 평가되므로 중점적으로 살펴보았다. 제3장의 내용은 한국법제연구원의 김도승 부연구위원이 주로 집필하였고, 이 중 수사제도 관련 내용은 김기범 경감이 보완하였다.

대안을 개발하기 위해서는 법제도뿐만 아니라 실태에 대한 분석도 중요하다. 이에 제5장에서 '우리나라 사이버안전의 실태'를 살펴보고자 하였는데, 국가통계를 중심으로 우리나라의 유형별, 분야별 사이버침해 내지 사이버안전 실태를 제1절에서 살펴보았으며, 이 내용은 박영우 전문위원이 주로 집필하였다. 제2절에서는 자체적인 전문가인식조사를 바탕으로 하여 사이버안전에 관한 전문가인식을 분석하였는데, 조사는 조사전문기관인 (주)리서치21에서 전담하는 한편, 결과 분석과 관련해서는 (주)리서치21의 백온유 선임연구원이 초안을 집필하고, 한국형사정책연구원의 강석구 연구위원이 이를 보완하였다. 다만 전문가인식조사의 시사점과 관련한 내용은 강석구 연구위원이 단독으로 정리하였다.

이상의 논의를 바탕으로 제6장에서 '사이버안전체계의 구축방안'을 제시하였는데, 이와 관련해서는 미리 밝혀두어야 할 사항이 있다. 이 연구는 당초 3개년 장기연구로

서 기획되어 사이버침해 유형별, 유관부처별 및 국가별 대응체계를 분석하고(1년차), 사이버안전 관리·검증을 위한 지표를 도출하며(2년차), 최종적으로 종합적·범국가적인 사이버안전체계 구축방안을 제시하는(3년차) 것을 목적으로 하였다. 그래서 금년은 사이버안전체계 구축에 관한 종래의 여러 논의와 제도를, 사실(fact) 및 실태(reality)를 중심으로 분석·정리함으로써 후속연구를 위한 기초자료를 축적하는 것을 단기목표로 삼았다. 다만 당초의 연구계획과 달리 차년도 이후의 후속연구를 진행하지 않기로 결정함에 따라 부득이하게 1년차 연구의 불완전한 성과만을 바탕으로 사이버안전체계 구축방안을 제시할 수밖에 없고, 이 때문에 구체적인 대안 제시보다는 다른 후속연구를 위한 화두(話頭) 제시에 초점을 맞추었다. 이러한 내용을 집약한 '사이버안전체계 구축의 기본방향'은 연구책임자인 강석구 연구위원이 집필하였다.

구체적 대안으로서는 제2절에서 '사이버위험 관리방안'을 '재난관리체계와의 연계방안', '국가사이버위기 관리방안'을 중심으로 제안하였고, '사이버안전 관련 제반 인프라 구축을 위한 제언'을 더하였다. 또한, 제3절에서 '사이버 수사체계 정비방안'을 소개하였다. 집필은 박영우 전문위원, 김민호 교수, 김기범 경감 등 공동연구진이 제안한 초안을 바탕으로 강석구 연구위원과 윤해성 부연구위원이 수정·보완하는 방식을 취하였다.

제3절 연구의 방법

법학적 방법론을 바탕으로 하는 연구인 만큼 국내외의 문헌연구 및 전문가·실무가 자문의 방법을 중심으로 연구를 진행하였으나, 사이버안전 내지는 사이버침해·사이버공격이라는 용어 자체가 신조어(新造語)인 것처럼 이 분야에 대한 논의나 관련 법제도 역시 역사가 일천하여 방법론상 이를 이론적 고찰, 현황 분석, 비교법적 고찰, 실증적 고찰로 구분하여 다각적·입체적으로 분석하고자 하였다. 이론적 고찰은 사이버안전 관련 유개념의 구별, 유형론 등을 중심으로, 현황 분석은 소관부처별 내지 기능별 대응체계 분석, 유형별 대응전략 분석, 법령 분석 등을 중심으로, 비교법적 고찰은 미국, 영국, 독일, 프랑스, 일본 등 선진제국의 사이버침해 대응체계 분석을 중심으로, 실증적 고찰은 유형별 내지 분야별 사이버침해 실태 분석, 전문가 인

식조사를 중심으로 하여 진행하였다.

전문가 인식조사를 위하여 공공과 민간 분야의 사이버보안 실무담당자를 대상으로 '심층면접조사'라는 질적 연구방법도 병행하였는데, 이 연구에서 차용한 심층면접조사라는 연구방법은 단순히 현상이나 실태에 대한 질적 접근을 위해 수행한 것이라기보다는 국민의식조사를 실시하기에 앞서 사이버안전정책 분야에 대한 이해도를 제고하기 위한 탐색적 연구방법의 일환으로서 수행한 것이라고 할 것이다.

제2장

사이버안전의 이론적 고찰

02
사이버안전의 이론적 고찰

제1절 사이버침해의 의의

1. 개 관

현대 정보사회는 수많은 컴퓨터 시스템이 서로 연결되어 이루어진 네트워크를 통해 행정, 기업, 교육, 거래 기타 다양한 사회 활동을 영위하고 있다. 컴퓨터 시스템 네트워크로 만들어진 영역을 사이버공간(Cyberspace; 가상공간)이라고 한다. 사이버공간은 중요한 사회생활 공간이라고 할 수 있으며, 이를 지탱하는 것은 바로 각 컴퓨터 시스템과 네트워크(통신망)이다. 만일 국가, 기업 혹은 개인에게 있어 중요한 기능을 하는 컴퓨터 시스템과 네트워크가 내·외부 공격으로 훼손, 마비되는 경우 해당 국가, 기업 혹은 개인에게 중대한 피해가 발생하게 된다. 따라서 사이버공간을 구성하는 컴퓨터 시스템과 네트워크의 안전에 대한 침해(사이버침해)[1]는 영토·영해·영공 침해 못지않게 현대 정보사회의 안전에 대한 심각한 위협이라고 할 수 있다.

그러나 사이버침해는 정부내 조직 또는 업무를 나타내는 데 많이 사용되고 또 각종 언론에서 널리 사용되고 있음에도 불구하고 이 용어 또는 개념에 대해 구체적으

1) '침해'는 사전적으로 "침범하여 해를 끼침"을 말하며, 법령에서도 '사생활의 침해', '인권의 침해', '일조권의 침해' 등 권리 또는 이익과 관련하여 일반적으로 사용한다. 또한, '사이버침해'라고 하면 사이버공간에서 보호받아야 하는 각종 권리 또는 이익에 대한 침해를 포괄하게 된다. 그러나 본 연구에서는 컴퓨터 시스템과 네트워크의 안전을 침해하는 행위를 가리키는 개념 또는 용어로 제한적으로 사용하기로 한다.

로 정의된 바는 없다.[2] 유사한 개념으로 사이버공격과 전자적 침해가 사용되고 있으며, 이에 대해서는 각각 다음과 같이 정의하고 있다.

사이버공격(Cyberattack)은 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 누출·훼손·왜곡전파 하는 모든 공격행위를 말한다.[3] 또 전자적 침해는 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.[4] 사이버공격과 전자적 침해 모두 ① 정보시스템 혹은 정보를 대상으로 하고(대상), ② 해킹·컴퓨터바이러스·서비스방해·전자기파 등 전자적 수단을 이용하며(수단), ③ 정보시스템 자체 또는 정보에 피해를 야기하는(효과) 점에서 동일하다고 할 수 있다.

더 나아가 사이버침해를 "정보시스템을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 및 고출력전자기파 등에 의하여 정보시스템을 공격하는 일체의 행위"[5] 라고 하여 사이버공격, 전자적 침해 및 사이버침해를 동일한 개념으로 보기도 한다. 따라서 사이버침해, 사이버공격 및 전자적 침해는 뉘앙스의 차이는 있으나[6] 동일한 개념으로 이해할 수 있다.

이상의 논의를 토대로 정리하면 사이버침해는 사이버공간(인터넷)을 통하여 정보시스템·네트워크에 침입 또는 이를 교란·마비·파괴하거나 정보를 누출·훼손·왜곡전파하는 행위 또는 그 결과라고 할 수 있다.[7] 경우에 따라서는 사이버공간(인터

2) 2010년 6월 23일 네이버 기사검색에서 "사이버침해"로 검색한 기사의 수가 1,725건임(중복기사 포함). 그러나 정보보호기술 전문용어 표준(한국정보통신기술협회 정보통신단체표준 TTAS.KO-12.0002/R1, 1998.11.25 제정 2003.10.24 개정)과 사이버보안 개요(한국정보통신기술협회 정보통신단체표준 TTAE.IT-X1205, 2009.12.22 제정)에는 사이버침해 또는 유사한 용어에 대한 정의규정을 두고 있지 않다.

3) 공성진의원 대표발의 '국가사이버위기 관리법안'(2008.10.28 발의, 의안번호 1619) 제2조 제1항 제1호. '국가사이버안전관리규정'(대통령훈령 제222호, 2005.1.31 제정 2008.8.18 개정)도 사이버공격을 유사하게 정의하고 있다(제2조 제2호 : "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다).

4) 정보통신기반보호법 제2조 제2호.

5) 이필중, 전산보안개론 & 전산시스템보안 강의자료, 2005. http://islab.postech.ac.kr/class/e472&i560/2005/data/1_2.pdf.

6) 침해는 공격 자체를 의미하기도 하지만 공격의 결과인 피해 상황을 의미하기도 한다.

7) 사이버침해와 인터넷을 통하지 않고 고출력 전자기파를 사용하여 직접 정보시스템 등을 공격하는 경우를

넷)을 통하지 않고 전자기파 등을 사용하는 경우를 제외하여 사이버공간(인터넷)을 통한 사이버공격 또는 전자적 침해만을 사이버침해로 볼 수도 있다.

2. 다른 개념과의 구분

사이버침해와 관련한 연구에서는 사이버침해를 비롯해 사이버범죄, 사이버테러, 사이버보안, 사이버안전 등 여러 가지 용어 또는 개념을 사용하고 있다. 본 연구의 대상과 범위를 정확히 하기 위하여 먼저 사이버침해와 이들이 어떻게 다른지 살펴본다.

먼저 사이버범죄(Cybercrime)는 컴퓨터기술과 정보통신기술이 조성하는 사이버공간에서 발생하는 범죄,[8] 무수히 많은 인터넷사이트들과 그것들을 서로 연계시키는 컴퓨터연결망(인터넷)을 범행의 수단, 표적 혹은 무대로 삼는 범법사례[9] 등 컴퓨터 혹은 인터넷과 관계된 범죄를 말한다. 이는 초기인 1980년대 단순한 파일손괴나 개인정보 유출 등 컴퓨터(전산정보처리조직)를 이용하거나 이를 대상으로 하는 범죄(컴퓨터범죄)에서 시작하여, 1990년대 전자상거래로 대표되는 인터넷의 상업적 활용으로 인터넷사기, 음란물유포 등 인터넷을 통한 범죄(인터넷범죄), 2000년대 개인 블로그, 온라인게임 등의 등장으로 프라이버시침해, 아이템절도 등 사이버공간에서 행해지는 범죄(사이버범죄)로 발전하였다. 정보기술의 발달과 융합[10]으로 사이버공간이제 더 이상 현실공간(real space)과 분리되어 독립적으로 존재하지 않는다. 따라서 사이버범죄도 그 개념이나 내용이 확정적이지 않고 계속하여 변화, 발전하고 있다. 그러나 사이버범죄로 언급되는 새로운 유형의 범죄 형태를 포괄하는 적절한 법적 개념은 현재까지 존재하지 않는다. 개념 정의 자체의 어려움과 함께, 아직도 이러한 유형의 불법행위들은 기본 범죄분류의 범주 안에서 해결되고 있다는 것이기도 하고, 종합적·일반적인 규정이 존재하지 않다는 것을 반증하는 것이기도 하다.[11] 따라서

포괄하여 '전자적 침해'라 할 수 있다(정보통신기반 보호법 제2조 제2호).

8) 조병인/정진수/정완/탁희성, 앞의 보고서, 15-18쪽.

9) 조병인/정진수/정완/탁희성, 앞의 보고서, 19-20쪽.

10) 스마트 그리드(Smart Grid), 사물통신망(Internet of Things), 클라우드 서비스(Cloud Services) 등.

11) 김성룡, RFID/USN 기술의 활용과 관련한 형사법적 문제점, 인터넷법률, 통권 제45호, 2009. 1, 55쪽

모든 사이버침해가 반드시 사이버범죄로 규정되지는 않는다.

사이버범죄와 함께 가장 일반적으로 사용되는 용어 또는 개념이 사이버테러(Cyberterror)이다. 경우에 따라서는 사이버범죄와 사이버테러가 동의어로 사용되기도 한다. 그러나 사이버테러는 국가·사회적으로 공포 내지 불안을 조성하기 위한 컴퓨터시스템 운영방해, 정보통신망 침해 또는 전자적 침해행위로서, '한 사회나 국가에 공포심 내지 불안감을 조성할 수 있는 정도'에 도달하여야만 사이버테러라고 할 수 있다.[12]

사이버보안(Cybersecurity)은 사이버침해(전자적 침해) 혹은 사이버공격으로부터 정보시스템 및 정보를 안전하게 보호하는 것을 말한다. 이는 정보보호(Information Security)와 동일한 의미로 사용하기도 한다. 최근에는 사이버보안 또는 정보보호와 동일한 의미에서 사이버공격으로부터 국가정보통신망을 보호하는 것을 가리켜 "사이버안전"이라는 용어를 사용하기도 한다.[13] 사이버보안 혹은 사이버안전은 컴퓨터 혹은 인터넷과 관계된 보안 혹은 안전이나 이를 추구하는 것을 말한다. 따라서 앞에서 말한 사이버범죄, 사이버테러, 사이버공격, 사이버침해가 컴퓨터 혹은 인터넷과 관계된 위협 혹은 위험을 의미하는 데 반해 사이버보안 혹은 사이버안전은 이를 예방 혹은 방지하는 것을 의미하는 점에서 차이가 있다.

요컨대 사이버침해는 사이버테러 또는 사이버범죄와 같이 국가안보 또는 범죄와 같은 정책적 또는 법적 가치판단이 아닌 객관적, 사실적으로 접근한 개념이다. 따라서 사이버침해가 경우에 따라서는 국가안보 또는 범죄의 가치판단에 따라 사이버테러 또는 사이버범죄가 될 수 있을 것이다.

이하.

12) 백광훈, 사이버테러리즘에 관한 연구, 한국형사정책연구원, 2001.12. 62-63쪽; 최정호, "사이버테러리즘의 변천방향과 한국의 대응", 2008 국방안보학술회의, 159-160쪽; Samuel C. McQuade, III, Encyclopedia of Cybercrime, 2009, 55쪽. 따라서 일반 사이버범죄를 주로 다루는 기관에 대하여 '사이버테러대응센터'라는 명칭을 붙이는 것은 적절하지 않다고 생각한다.

13) 국가사이버안전관리규정 제2조 제3호 : "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다. 이밖에 "사이버안전"이라는 용어를 사용하는 예로는 '교육사이버안전센터운영규정', '국토해양 사이버안전센터 운영규칙', '방송통신 사이버안전센터 운영규칙', '보건복지 사이버안전센터 운영규칙', '산업자원 사이버안전센터 운영규칙' 등 사이버안전센터 운영규칙들이 있다.

제2절 사이버침해의 유형

1. 의 의

사이버침해는 사이버공간(인터넷)을 통하여 정보시스템·네트워크에 침입 또는 이를 교란·마비·파괴하거나 정보를 누출·훼손·왜곡전파하는 행위라고 정의할 수 있다.

초기에는 공격수법이나 동기가 비교적 단순하였다. 해킹이나 바이러스 제작 기술을 익힌 사람이 자신의 실력을 과시하기 위해 특정 시스템을 해킹하여 정보를 훔쳐보거나 홈페이지에 특정한 메시지를 올리는 경우가 많았다. 그리고 이러한 능력을 가진 해커 그룹은 비교적 소수에 불과하였다. 따라서 사이버침해의 유형도 해킹, 컴퓨터바이러스 유포에 불과하였다.

그러나 최근 사이버침해는 공격수법의 지능화·다양화·복합화, 파일공유·메일·P2P 등을 통한 다른 시스템으로의 빠른 전파, 사회공학적 기법과 다양한 기술적 방법이 결합된 사이버공격 도구 출현, 침입차단시스템·침임탐지시스템 등 정보보호시스템을 우회 또는 무력화하는 공격 출현, 보안취약점이 공개되는 당일 이를 이용하는 공격도구 출현(제로 데이 공격), 역연결(Reverse Connection)을 이용하여 원격제어하는 악성코드 출현, 금전적 이득을 위해 개인정보를 유출하는 공격 출현 등의 특징을 보인다.[14] 따라서 사이버침해는 공격의 주체, 공격의 동기(또는 목적), 공격의 대상, 공격의 수단·방법, 공격의 효과(또는 피해) 등에 따라 그 형태가 매우 다양해지고 있다.

이와 같이 다양하고 복잡한 사이버침해에 효과적으로 대응하기 위해서는 각각의 사이버침해 유형별 실태와 특성을 정확히 분석·이해하고 이에 맞추어 적절한 대응전략을 수립하고 실행하는 것이 필요하다. 그리고 사이버침해의 실태와 특성을 정확히 분석하기 위해서는 개별 침해(행위)에 대한 분석과 함께 개별 침해(행위) 간의 공통점과 차이점 등을 파악하여야 한다. 이를 위해서는 먼저 개별 사이버침해(행위)에 대한 합리적인 기준을 마련하여 유형화하

14) 국가사이버안전센터, 국가사이버안전매뉴얼, 2005. 10, 56쪽.

는 것이 필요하다.

2. 기존의 유형 분류

가. 국 내

사이버침해의 유형과 관련하여 국내에서는 주로 사이버침해의 수단 또는 수법과 피해를 중심으로 분류하고 있다.[15]

먼저 '경찰청 사이버테러대응센터'는 정보통신망 자체를 공격대상으로 하는 불법 행위로서 해킹, 바이러스유포, 메일폭탄, DoS공격 등 전자기적 침해장비를 이용하여 컴퓨터시스템과 정보통신망을 공격하는 행위를 사이버테러형 범죄로 분류하고, 이를 해킹(단순침입, 사용자 도용, 파일등 삭제와 자료유출, 폭탄메일)과 악성프로그램으로 구분한다.[16]

해킹은 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해행위로서, 사용하는 기술과 방법 및 침해 정도에 따라 ① 단순침입, ② 사용자도용, ③ 파일 등 삭제변경, ④ 자료유출, ⑤ 폭탄스팸메일 및 ⑥ 서비스거부공격으로 구분한다. 그리고 악성프로그램은 정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작·유포되는 모든 실행 가능한 컴퓨터 프로그램으로, 리소스의 감염 여부, 전파력 및 기능적 특징에 따라 ⑦ 바이러스, ⑧ 웜 및 ⑨ 스파이웨어 등으로 구분한다.

15) 주로 실무적인 관점에서 유형 분류가 이루어지고 학술적인 분류는 제대로 이루어지지 않고 있다.

16) http://www.netan.go.kr.

표 1 경찰청 사이버테러대응센터의 사이버침해 유형 분류

유 형	침해 행위	내 용
해킹	단순침입	정당한 ① 접근권한 없이 또는 허용된 접근권한을 초과하여 ② 정보통신망에 침입 하는 것 ① 접근권한 : 행위자가 해당 정보통신망의 자원을 임의로 사용할 수 있도록 하는 권한 ② 정보통신망에 침입한다 : 행위자가 해당 정보통신망의 자원을 사용하기 위해서 거쳐야 하는 인증절차를 거치지 않거나 비정상적인 방법을 사용해 해당 정보통신망의 접근권한을 획득하는 것. 즉 정보통신망의 자원을 임의대로 사용할 수 있는 상태가 되었을 때 침입이 이루어진 것이라고 할 수 있음
	사용자도용	정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 것 ※ 개념상으로만 보면 단순침입의 한 가지 유형에 해당하지만 사용자 도용이 차지하는 부분이 많아 별도로 구분
	파일등 삭제와 자료유출	정보통신망에 침입한 자가 행한 2차적 행위의 결과로, 일반적으로 정보통신망에 대한 침입행위가 이루어진 뒤에 가능함
	폭탄메일	메일서버가 감당할 수 있는 한계를 넘는 많은 양의 메일을 일시에 보내 장애가 발생하게 하거나 메일내부에 메일 수신자의 컴퓨터에 과부하를 일으킬 수 있는 실행코드 등을 넣어 보내는 것. 서비스거부공격의 한 유형
	서비스거부공격	정보통신망에 일정한 시간 동안 대량의 데이터를 전송시키거나 처리하게 하여 과부하를 야기시켜 정상적인 서비스가 불가능한 상태를 만드는 일체의 행위
악성 프로그램	트로이목마	프로그램에 미리 입력된 기능을 능동적으로 수행하여 시스템 외부의 해커에게 정보를 유출하거나 원격제어기능 수행. 트로이목마처럼 유용한 유틸리티로 위장하여 확산되기 때문에 감염사실 알아채기 어려움
	인터넷웜	시스템 과부하를 목적으로 이메일의 첨부파일 등 인터넷 이용하여 확산됨. 확산시 정상적인 파일이 이메일에 첨부되기도 하기 때문에 개인정보 유출의 위험 내포
	스파이웨어	공개프로그램, 쉐어웨어, 평가판 등의 무료 프로그램에 탑재되어 정보를 유출시키는 기능이 있는 모든 종류의 프로그램

또한, '한국인터넷진흥원 인터넷침해대응센터'는 침해사고를 ① 웜·바이러스, ② 해킹, ③ 악성 봇(Bot)으로 분류하고, ② 해킹을 다시 스팸 릴레이, 피싱 경유지, 단

순침입시도, 홈페이지 변조, 기타 해킹으로 나눈다.[17]

표 2 한국인터넷진흥원 인터넷침해대응센터의 사이버침해 유형 분류

유 형	침해 행위	내 용
웜바이러스	웜	독립적으로 자기복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 코드
	바이러스	컴퓨터 프로그램이나 메모리에 자신 또는 자신의 변형을 복사해 넣는 악의적인 명령어들로 조합하여 불특정 다수에게 피해를 주기 위한 목적으로 제작된 모든 컴퓨터 프로그램 또는 실행 가능한 코드
해킹	스팸릴레이	스팸 메일 발신자 추적을 어렵게 하기 위하여 타 시스템을 스팸 메일발송에 악용
	피싱경유지	정상적인 웹서버를 해킹하여 위장사이트를 개설한 후, 인터넷 이용자들의 금융정보 등을 빼내는 신종 사기수법으로 Bank Fraud, Scam이라고도 함
	단순침입시도	시스템에 침입하려고 시도하거나, 취약점 정보의 수집을 위해 스캔하는 등의 행위
	홈페이지변조	–
	기타 해킹	–
악성봇	봇(Bot)	운영체제 취약점, 비밀번호의 취약성, 웜바이러스의 백도어 등을 이용하여 전파되며, 해킹명령 전달 사이트와의 백도어 연결 등을 통하여 스팸메일 전송이나 DDoS 공격에 악용이 가능한 프로그램 또는 실행 가능한 코드

'국가정보원 사이버안전센터'는 사이버공격을 수법에 따라 ① 악성코드공격, ② 서비스거부공격, ③ 비인가접근공격, ④ 복합구성공격의 4가지로 분류한다.[18]

17) 한국인터넷진흥원 인터넷침해대응센터, 인터넷 침해사고 동향 및 분석 월보, 2010.4; 방송통신위원회·행정안전부·지식경제부, 2010 국가정보보호백서, 2010.4, 29쪽 이하.

18) 국가사이버안전센터, 국가사이버안전매뉴얼, 2005.10, 56-57쪽.

표 3 국가정보원 사이버안전센터의 사이버침해 유형 분류

유형 (침해 행위)	내 용
악성코드공격	컴퓨터바이러스, 웜, 트로이목마, 백도어, 봇(BOT), 스파이웨어 등 악성코드가 사용자의 동의없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 컴퓨터를 오작동시키고 네트워크를 마비시키는 행위를 말한다.
서비스거부공격	시스템에 과도한 부하(負荷)를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 행위를 말한다.
비인가접근공격	네트워크, 시스템, 응용프로그램, 데이터 기타 정보자원 등에 인가받지 않은 자가 논리적 혹은 물리적으로 불법 접근하는 행위를 말한다.
복합구성공격	위의 악성코드공격, 서비스거부공격, 비인가접근공격 등의 요소를 복합적으로 이용하는 공격행위를 말한다.

또한, 국가정보원 사이버안전센터는 국가안전보장 또는 국가이익에 큰 피해를 유발할 우려가 있는 사이버공격으로서 국가정보원장이 별도로 분류한 것을 '안보위해공격' 으로 별도로 규정하고 있다.[19)]

표 4 국가정보원 사이버안전센터의 안보위해공격 유형 분류

유형	내용
국가기밀에 속하는 문서 · 자재 · 시설 · 지역 등을 대상으로 한 공격	국가정보원법 제3조 및 보안업무규정에 따른 국가기밀에 속하는 문서 · 자재 · 시설 · 지역 및 이를 관리하는 인원을 대상으로 한 사이버공격
반국가단체, 국제범죄조직 및 테러단체에 의한 공격	국가보안법 제2조에 따른 반국가단체, 국가정보원법 제3조에 따른 국제범죄조직 및 테러단체에 의하여 수행되는 사이버공격
국가안전보장 관련 주요정보통신기반시설을 대상으로 한 공격	'정보통신기반 보호법' 제7조 제2항에 따른 국가안전보장 관련 주요정보통신기반시설 및 이를 관리하는 인원을 대상으로 한 사이버공격
국가핵심기술을 대상으로 한 공격	'산업기술의 유출방지 및 보호에 관한 법률' 제9조에 따른 국가핵심기술 및 이를 취급하는 인원을 대상으로 한 사이버공격

19) '국토해양 사이버안전센터 운영규칙' 제4조 제1항 제3호. '방송통신 사이버안전센터 운영규칙' 제4조 제4호.

한편, 국가정보원 사이버안전센터는 사고 유형의 경우 다음 표와 같이 주로 피해를 기준으로 분류하고 있다.[20]

표 5 국가정보원 사이버안전센터의 사고유형 분류

기 호	사고 유형	설 명
A	경유지 악용	타기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹흔적 또는 해킹툴이 설치되어 타시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단송신된 흔적이 발견되었을 경우
C	단순침입 시도	지속적인 스캐닝 공격이 발생할 경우
D	웜바이러스 피해	기관내의 PC에서 웜바이러스가 발견되었을 경우
E	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
F	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능할 경우
G	서비스거부공격 피해	불특정 다수의 IP로부터 접속시도 또는 대량 트래픽이 일시에 유입될 경우
H	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

나. 국 외

국외의 경우에도 정보보호 기관·단체, CERT 등 사이버침해 대응조직들이 실무적인 관점에서 사이버침해에 해당하는 행위를 분류하고 있다. 그러나 이들 기관의 유형 분류는 역사적, 기술적인 이유에서 자신의 소관 업무를 중심으로 매우 제한적으로 파악, 분류하고 있는 한계가 있다.

미국의 경우 국토안보부의 US-CERT는 사이버보안 사고를 ① 비인가접근공격, ② 서비스거부공격, ③ 악성코드, ④ 부정사용, ⑤ 스캔·탐지 기타 접속시도로 분류한다.[21]

20) 국가사이버안전센터, 상황통보양식의 사고 유형 목록 참조.

21) US-CERT QUARTERLY TRENDS AND ANALYSIS REPORT(Volume 4, Issue 1, June 16, 2009). 보고유형의 하나로 '조사(Investigation) 필요'도 있으나, 이는 보고기관이 추가 조사가 필요하다고 판단한 악성 혹은 비정상 행위로서 사이버보안 사고의 유형으로 보기에는 부적절하여 제외하였다.

표 6 미국 국토안보부의 사이버보안 사고 유형 분류

유형 (침해 행위)	내 용
비인가접근공격 (Unauthorized Access)	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
서비스거부공격 (Denial of Service)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
악성코드 (Malicious Code)	Successful installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are not required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
부정사용 (Improper Usage)	A person violates acceptable computing use policies.
스캔·프로브·접속시도 (Scans, Probes, or Attempted Access)	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

독일의 경우 '연방정보기술보안청'(Bundesamt für Sicherheit in der Informationstechnik; BSI)이 정보시스템에 대한 위협을 ① 악성프로그램(바이러스, 웜, 트로이목마, 봇, 스파이웨어), ② DoS공격, ③ 스팸메일, ④ 봇넷, ⑤ ID도용, ⑥ 사기 웹서비스, ⑦ 전파훼손(Kompromittierende Abstrahlung), ⑧ 내부위협(내부행위자, 오류, 과실)으로 분류한다.[22] 특히 독일의 경우 외부위협 뿐만 아니라 내부위협도 포함하고 있다는 점에 특색이 있다.

22) Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, Januar 2009, SS.20-32.

표 7 독일 연방정보기술보안청의 정보시스템 위협행위 유형 분류

유 형	침해 행위	내 용
악성 프로그램	바이러스	–
	웜	–
	트로이목마	–
	봇	–
	스파이웨어	–
DoS공격		–
스팸메일		–
봇넷		–
ID도용		–
사기 웹서비스		–
전파 훼손		Derart informationsbehaftete Störemissionen
내부위협	내부행위자	내부직원에 의한 정보절취(경제적 동기 혹은 복수)
	오류	–
	과실	–

일본의 경우 '내각관방 시큐리티센터'(内閣官房情報セキュリティセンター; NISC), 경찰청, 정보처리추진기구(情報処理推進機構; IPA) 등 사이버침해 대응조직들은 사이버침해의 개념 및 분류를 사용하고 있지 않다. 다만 경찰청이 사이버범죄를 ① 부정엑세스금지법위반, ② 컴퓨터・전자적기록대상범죄(전자계산기사용사기, 전자적기록부정작출・훼기 등, 전자계산기손괴 등 업무방해), ③ 네트워크이용범죄(사기〈옥션이용사기〉, 아동매춘・아동포르노법위반〈아동포르노〉, 아동매춘・아동포르노법위반〈아동매춘〉, 만남주선사이트규제법위반, 청소년보호육성조례위반, 음란물반포 등, 기타〈저작권법위반, 상표법위반, 상기 이외〉)로 분류하고 있으나, 사이버침해의 유형 분류로는 보기 어렵다.

한편 IPA와 JPCERT/CC가 사이버침해와 관련한 유형분류를 하고 있다. IPA가 해킹・바이러스 신고・상담과 대책 차원에서 크게 ① 바이러스, ② 부정엑세스(해킹),

③ 봇으로 분류하고 있다. JPCERT/CC는 '인시던트 보고 가이드라인'(2004. 6. 7)에서 컴퓨터 보안 인시던트[23]를 ① 프루프, 스캔, 기타 의심스러운 액세스, ② 서버 프로그램의 부정 중계, ③ 송신 헤더를 사칭한 전자메일의 배송, ④ 시스템에의 침입, ⑤ 서비스 운용 방해로 연결되는 공격, ⑥ 기타의 6개 유형으로 분류하고 있다.

표 8 일본 JPCERT/CC의 컴퓨터 보안 인시던트 유형 분류

유형	침해 행위	내용
프루프, 스캔, 그외 의심스러운 액세스 [Scan]	HTTP 서버의 약점 탐색	서버 프로그램 버전의 체크 등
	FTP 서버에의 로그인의 시도	(미수에 끝난 것)
	웜의 감염의 시도	(미수에 끝난 것)
서버 프로그램의 부정 중계 [Abuse]	메일 서버의 부정 중계	
	프록시 서버의 부정 중계	
송신 헤더를 사칭한 전자메일의 배송 [Forged]	대량의 에러 메일의 수신	
	SPAM 메일의 송신 바탕으로 사용	
시스템에의 침입 [Intrusion]	시스템에의 침입이나 변조	백 도어의 설치
	DDoS용 프로그램의 설치	
	웜의 감염	
서비스 운용 방해로 연결되는 공격 [DoS (Denial of Service)]	네트워크의 폭주(혼잡)에 의한 방해	대량의 ICMP 패킷의 수신
	서버프로그램의 정지	Web 서버에의 대량의 액세스
	OS의 정지나 재가동	
기타 [Other]	SPAM 메일의 수신	
	컴퓨터바이러스의 감염	바이러스에 감염한 메일의 수신

23) 컴퓨터 보안 인시던트란 "정보시스템의 운용에 있어서 보안상의 문제로 파악할 수 있는 사상"으로, 실제로는 영향이 발생하고 있지 않은 사상이어도 어떠한 영향을 받은 의심이 있거나 방치해 두면 보안상의 영향이 생길 우려가 있는 경우라면 컴퓨터 보안 인시던트라고 파악한다(동 가이드라인 1.2).

다. 종래의 분류 이론

학술적인 관점에서는 국내보다는 국외에서 사이버침해의 유형 분류가 활발하게 이루어지고 있으며, 주로 사이버침해의 수단 또는 수법과 피해를 중심으로 기술적으로 분류하고 있다.

노르웨이의 셰르란 박사(Maria Kjaerland)는 사이버범죄 행위자와 희생자에 초점을 맞춰 컴퓨터범죄 프로파일링과 관계된 CERT의 사이버침입(cyber-intrusions) 유형 분류를 제안하였다.[24] 셰르란 박사는 연구에서 패싯(facet) 이론과 작동(Operation) 방법, 대상(Target), 출처(Source) 및 영향(Impact)을 고려한 다차원척도법(multidimensional scaling; MDS)을 사용하여 사이버공격을 분석하였고, 각 패싯은 고유한 설명(exhaustive description)을 갖는 다수의 요소를 포함하고 있다고 한다. 셰르란 박사는 이 패싯들을 사용하여 상업 침해사고와 정부 침해사고를 비교하며, 공격이 일어난 이유와 공격이 시작된 출처를 밝히기 위하여 공격자의 동기에 유형분류의 초점을 맞춘다. 이러한 유형 분류는 공격 개시를 파악하는 데 사용할 수 있는 수법에 대해 보다 자세한 내용을 제공하지 않으면서 작동 방법에 대한 고차원적인 시각을 제공하는 점에서 다소 한계가 있다.

뉴질랜드의 헌트 교수(Ray Hunt)와 한스먼 연구원(Simon Hansman)은 네트워크와 컴퓨터 공격을 포섭하는 전체적인 분류를 제공하는 4개의 고유 영역을 갖는 유형 분류를 제안한다.[25] 이들의 유형 분류는 컴퓨터와 네트워크 보안뿐만 아니라 공격 기술과 관련한 언어의 일치를 개선하는 데 도움이 된다. 공격 벡터라는 첫 번째 특성은 공격을 분류하는 데 사용되며, 두 번째 특성은 공격 대상을 분류하고, 세 번째 특성은 취약성 분류번호 혹은 후술하는 하워드 박사의 유형 분류에서의 기준으로 구성된다. 네 번째 특성은 관계된 폭발력 또는 효과에 집중하며, 각 특성 내에서 공격에 대한 상세한 내용을 제공하기 위해 다양한 수준의 정보가 제공된다. 다만 이들은 자신들의 유형 분류에서 한계라고 할 수 있는 혼합형 공격의 분류를 개선하기 위

24) Kjaerland, M., "A taxonomy and comparison of computer security incidents from the commercial and government sectors", Computers and Security 제25권 제7호, 2006, 522-538쪽.

25) Hansman, S. & R. Hunt, "A taxonomy of network and computer attacks", Computers & Security 제24권 제1호, 2005, 1-13쪽.

해서는 추가적인 작업이 필요함을 인정하며, 이외에도 이들의 유형 분류는 공격으로부터 시스템을 보호하는데 도움이 되는 정보를 취득하는 것을 막는 '취약성 정보의 부족' 에 따른 한계를 가진다.

미국의 미르코비치 박사(Jelena Mirkovic)와 레이어 박사(Peter Reiher)는 공격 및 방어 전략을 분류하기 위한 목적으로 분산 서비스거부 공격과 방어 메커니즘의 복합적인 유형 분류를 제시한다.[26] 이들의 연구는 공격 전략의 특성에 집중하며, 여기서 전략은 대응수단을 마련하는 데 필수적이다. 이들의 분산 서비스거부 공격 유형 분류는 자동화 정도, 사용하는 약점, 출처주소의 유효성, 공격율 역학(Attack Rate Dynamics), 정의 가능성, 지속되는 에이전트 세트, 희생자 유형 및 희생자에 대한 영향으로 분류된다. 이러한 유형 분류는 이용, 희생자에 대한 영향과 분산 서비스거부 공격의 이용과 관계된 특징을 검사하는 데 사용된다. 이들은 활동 수준, 협력 정도 및 전개 위치로 이루어지는 DDoS 방어의 유형 분류를 개발하였고, 하나의 유형 분류 안에서 DDoS 공격과 방어의 유형 분류를 결합하여 위협에 대한 커뮤니케이션을 가능하게 함으로써 해결책을 논의하기 위한 연구자들 간의 협력을 제고하였다.

미국의 러프 박사(Daniel Lough)는 VERDICT(validation exposure randomness deallocation improper conditions taxonomy)라는 공격 중심의 유형 분류를 제안한다.[27] 여기서 러프 박사는 부적절한 확인(Validation), 부적절한 노출(Exposure), 부적절한 무작위성(Randomness), 부적절한 자원 재분배(Deallocation) 등 4가지의 주요 보안 실패 요인에 주목한다. 러프 박사는 이들 4가지 특성에 공격으로 부적절한 조건이 된다고 생각하여 "부적절한(Improper)"이란 접두사를 붙이는 한편, 부적절한 확인은 부적절하게 확인하거나 물리적 보안을 포함하여 구속받지 않는 데이터를 말한다고 한다. 또한, 노출은 직접 혹은 간접으로 취약성을 이용하는 데 사용될 수 있는 정보의 부적절한 노출을 의미하며, 무작위성은 암호의 기본을 다루며 무작위성의 부적절한 이용을 의미하고, 자원 재분배는 쓰레기통 뒤지기를 포함하여 정보의 부적절한 파괴 혹은 데이터의 잔여를 의미한다고 한다. 러프 박사는 취약성을 하나의 체

26) Mirkovic, J. & P. Reiher, "Taxonomy of DDoS Attack and DDoS Defense Mechanisms". In ACM CCR, 2004. 4.

27) Lough, D., "Taxonomy of Computer Attacks with Applications to Wireless Networks," Virginia Polytechnic Institute and State University 박사학위논문, 2001.

계 안에서 기술하기 위해 이들 특성 중 하나 이상을 사용하는데, 헌트 교수와 한스먼 연구원은 러프 박사의 유형 분류를 CERT와 같은 지식집단이 일상적인 공격을 분류하고 조언을 하는 데 도움이 되는 적절한 정보가 결여되어 있다고 표현한다. 또한, 러프 박사의 유형 분류는 웜, 트로이목마, 바이러스 등의 공격 유형에 대한 분류가 결여되어 있다.

미국의 하워드 박사(John Howard)는 변화된 상태를 야기할 의도로 특정 목표를 향한 공격인 사건(events)에 따라 공격을 분류하는 침해 유형분류(incident taxonomy)를 제안한다.[28] 하워드 박사는 공격을 포함하는 모든 단계와 공격이 전개되는 방법에 초점을 두며, 공격은 공격자가 허용되지 않은 결과를 얻기 위해 취하는 5개의 논리적 단계로 이루어진다고 한다. 이들 단계는 수단(tools), 취약성(vulnerability), 행위(action), 목표(target) 및 허용되지 않은 결과(unauthorized result)로 구성되는데, 여기서 수단은 공격을 수행하는 데 사용하는 장치·방법이고, 취약성은 공격을 수행하는 데 사용하는 약점(exploit)의 종류이다. 행위는 공격자가 공격을 수행하는 데 사용한 방법(즉, Probe, Scan, Authenticate 등)을 말하며, 목표는 공격으로 훼손시키려고 시도하는 의도를 말한다. 허용되지 않은 결과는 공격으로 야기된 변화 상황을 말한다. 하워드 박사의 유형 분류는 사이버침해에 대한 유익한 기준선을 제공했지만, 공격에 대한 깊이 있는 통찰에 필요한 세부정보를 결여하였다는 한계가 있다.

이밖에 미국의 농예 교수 연구진(Nong Ye, Clark Newman, Toni Farley)은 사이버공격 분류를 위한 시스템-오류-위험(System-Fault-Risk; SFR) 프레임워크를 제안한 바 있는데, 이는 시스템 엔지니어링, 오류 모형(fault modeling) 및 위험 평가(risk-assessment)에서의 이론을 결합한 과학적 토대에 근거를 두고 있다고 할 것이다. 또한, 시몬스 교수 연구진(Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu)은 사이버공격을 파악하고 방어하는데 도움이 되도록 AVOIDIT(attack vector, operational impact, defense, information impact, and target)라 부르는 사이버공격 유형 분류를 제안하고 있다.[29] 이들은 공격의 성격을

28) Howard, J. D. & Thomas A. Longstaff, “Common Language for Computer Security Incidents”, Technical report, Sandia National Laboratories, 1998.

특징짓기 위하여 ① 공격 벡터에 의한 분류(classification by attack vector), ② 공격 목표에 의한 분류(classification by attack target), ③ 작용효과에 의한 분류(classification by operational impact), ④ 정보효과에 의한 분류(classification by informational impact) 및 ⑤ 방어에 의한 분류(classification by defense) 등 5가지 주요 분류요소를 사용한다. 5번째 범주인 방어에 의한 분류는 네트워크 관리자에게 공격을 완화 또는 구제하는 방법에 대한 정보를 제공하는 데 사용하며, 다른 유형 분류와 달리 이들의 분류는 최근 크게 증가하고 있는 혼합형 공격을 효율적으로 분류할 수 있다.

라. 기존 유형 분류의 문제점

기존 유형 분류의 가장 큰 문제점은 사이버침해를 단순히 취약점 혹은 기술적 공격수법만으로 유형을 분류한다는 것이다. 이에 따라 공격자, 공격 목표(대상), 효과(피해) 등 사이버침해의 특성을 규정하고 대응책을 마련하는 데 중요한 요소들이 상당 부분 배제되고 있다. 이러한 문제는 특히 국내에서 행해지는 유형 분류에서 두드러진다고 할 수 있다.

첫째, 공격자의 특성, 의도 등 대응에 있어 중요한 요소들이 배제된다. 공격자가 내부자, 내국인 혹은 외국인이냐, 개인이냐 집단이냐에 따라 대응이 다를 수 있음에도 이러한 중요한 요소가 유형 분류에서 배제되어 있다. 공격자 및 이러한 공격의 의도는 사전 혹은 사고발생 즉시 알기는 어렵다. 그러나 이를 사이버침해의 유형에서 고려하지 않는다면 그 대응은 단순히 기술적 차원에 그치게 되어 종합적인 대응을 하지 못하는 문제가 생길 수 있다. 독일의 보고서에서도 외국 정보기관에 의한 자국 기업 및 기관에 대한 전자적 공격의 종류와 공격자에 대한 정보를 다루고 있는 실정이다.[30]

둘째, 공격 목표(대상)가 배제된다. 공격 대상이 국가기관 혹은 사회인프라인가, 아니면 기업 혹은 개인인가에 따라 대응이 달라질 수밖에 없다. 공격 대상에 따라

29) Simmons, C., Charles Ellis, Sajjan Shiva, Dipankar Dasgupta & Qishi Wu, AVOIDIT : A Cyber Attack Taxonomy, 2009. 8.

30) 독일 연방 및 주 헌법수호청(Verfassungsschutzbehörden)의 연차보고서 참조.

공격 수단이나 방법이 크게 다르지는 않으나 이에 따른 대응이나 침해 발생에 따른 후속조치 등에 있어서 큰 차이가 있을 수 있기 때문이다.

셋째, 국가·사회·개인 차원에서 공격으로 인한 효과(피해)가 배제된다. 오늘날 정보시스템은 인터넷을 중심으로 상호 연계되어 있다. 또한 정보시스템의 기능 마비는 다른 영역에서의 재해를 발생시킬 수도 있다. 따라서 각각의 침해가 국가, 사회 또는 개인 차원의 것인지가 중요한 의미를 갖는다.

다른 한편으로 지나치게 기술적으로 요소를 세분화하는 것은 사이버침해에 대한 국가 차원의 대응전략을 수립하는 데 장애가 될 수 있다. 이는 사이버침해 수법의 하나인 악성프로그램의 경우 대부분 모듈 형태로 구성되고 여러 가지 침해 기능을 함께 갖고 있기 때문인데, 예컨대 트로이목마가 백도어와 스파이웨어 기능을 갖고 또 키로거를 이용하여 감염된 시스템을 고의로 봇넷에 접속시킬 수도 있기 때문이다.[31] 또한 사이버범죄의 유형 분류를 전적으로 수용하는 것도 적절하지 않다. 사이버범죄의 유형은 우선 사이버침해 중 범죄로 규정된 일부만 대상으로 하고 피해 법익에 따른 구분을 중심으로 하기 때문에 행위 자체의 특성을 충분히 파악하지 못하기 때문이다.

요컨대 단일한 지표만으로 사이버침해를 분류하는 것은 바람직하지 않다고 할 수 있다. 이러한 이유에서 국외의 유형분류나 많은 연구가 매우 다양한 요소들을 포함하려고 애쓰고 있음을 볼 수 있다. 그러나 지나치게 세분화되고 많은 수의 유형은, 본 연구와 같이 국가 차원에서 사이버침해 안전실태 분석과 대응전략을 수립함에 있어서는 오히려 불필요하게 많은 비용과 시간을 소모하게 되어 적절한 대응을 곤란하게 할 수 있다. 따라서 본 연구에서는 기술적인 세분류보다는 연구의 목적에 맞게 대응전략의 수립·이행을 결정하는 데 중요한 요소를 기준으로 사이버침해를 분류할 필요가 있다.

31) Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, 2009. 1, 20쪽.

3. 사이버침해 유형

가. 분류 기준

본 연구는 당초 사이버침해 유형별, 유관부처별 및 국가별 대응체계를 분석하고(1년차), 사이버안전 관리·검증을 위한 지표를 도출하며(2년차), 최종적으로 종합적·범국가적인 사이버안전체계 구축방안을 제시하는(3년차) 것을 목적으로 하였다. 그래서 사이버침해의 유형은 앞서와 같이 기술적 분류를 중심으로 하기보다는 행위자, 목적, 공격대상, 피해 등 사회적, 거시적인 관점을 기본으로 분류하고 이에 기술적 특성을 고려하는 것이 적절할 것으로 본다. 그렇게 함으로써 각 사이버침해 유형을 기초로 유관부처별 및 국가별 대응체계를 비교·분석하는 것이 가능하고 또 사이버안전 관리·검증을 위한 지표를 도출할 수 있을 것이기 때문이다.

그렇다면 어떤 요소들을 사이버침해의 유형 분류기준으로 할 것인가. 기본적으로 사이버침해는 대상, 공격 그리고 피해(결과)를 핵심 요소로 한다. 앞에서 살펴본 바와 같이 기존의 유형 분류는 이 가운데 공격 요소를 그 수법을 중심으로 기술적으로 분류하였다. 따라서 이러한 유형 분류에 기초한 대응책 또한 기술 중심적이라는 한계를 가질 수밖에 없다. 그러나 유형 분류에서 침해의 핵심 요소인 대상, 공격 그리고 피해를 모두 고려할 수 있다면 이에 기초한 대응책 또한 포괄적일 수 있다.

먼저 대상을 기준으로 하면 특정 정보시스템을 파괴·마비하거나 복수의 정보시스템 특히 네트워크를 파괴·마비시키거나 또는 DB 등 정보를 유출하는 사이버침해 유형이 있을 수 있다. 각각의 대상은 가치에 따라 그 보호수준이 달라지게 된다.[32] 이는 크게 SCADA, 망, DB, 단말로 분류할 수 있다. 그러나 이보다는 주요 정보통신기반시설과 일반 시스템으로 분류하는 것이 타당하다고 본다.

다음으로 공격을 기준으로 하면 이는 기존의 사이버침해 유형 분류를 활용할 수 있다. 수법에 따라 해킹, 악성코드 유포, 서비스거부공격, 봇, 기타 유형으로 분류할 수 있을 것이다. 공격 대상 및 목적에 따라 이들 수법 중 하나가 사용되거나 혹은 둘 이상이 함께 사용될 수 있을 것이다.[33] 따라서 대응책 차원에서는 수법 자체 보

32) 예컨대 '주요정보통신기반시설'의 경우 그 국가적·사회적 중요성 때문에 다른 정보시스템과 달리 특별한 보호조치를 하고 있다.

다는 대상 및 피해를 중심으로 하여 포괄적으로 살펴보는 것이 바람직하다.

끝으로 피해를 기준으로 하면 정보시스템 또는 네트워크의 파괴, 마비, 훼손 그리고 정보의 유출, 훼손으로 분류할 수 있다. 그러나 이는 해당 정보시스템, 네트워크 및 정보에 대한 일차적인 피해에 불과하여, 실제 이들 피해는 다른 정보시스템 및 네트워크의 기능이나 서비스에 장애를 초래함으로써 국가 또는 사회의 전체 혹은 일부에 큰 피해를 가져올 수도 있다. 따라서 국가 차원의 사이버침해 대응책과 안전체계를 연구하는 데 있어서는 그 피해를 단순히 개별 정보시스템 또는 네트워크 단위에서 살펴볼 것은 아니다. 따라서 피해를 기준으로 한 사이버침해 분류도 다른 정보시스템 및 네트워크에의 영향이나 국가 또는 사회 전체의 영향 정도를 따질 필요가 있다.

이외에도 행위자(개인, 조직·단체, 국가), 공격 근원지(국내, 국외) 등을 분류 기준으로 들 수 있다. 유형 분류에서는 이를 기준으로 살펴보지 않는다. 행위자나 공격 근원지의 차이가 사이버침해의 유형 분류에서 결정적인 요소는 아니기 때문이다. 그러나 대응전략에서는 이들이 중요한 고려 사항이므로 이를 고려하여 살펴본다.

나. 각 기준에 따른 세부 분류

(1) 공격수법 및 피해를 기준으로 한 분류

사이버침해는 전통적으로 공격수법을 기준으로 하는 경우 해킹, 악성코드 유포, 서비스거부 공격, 기타 유형으로 분류할 수 있다.

해킹은 네트워크, 시스템, 응용프로그램, 데이터 기타 정보자원 등에 인가받지 않은 자가 논리적 혹은 물리적으로 불법 접근하는 행위를 말한다.

악성코드 유포 공격은 컴퓨터바이러스, 웜, 트로이목마, 백도어, 봇(BOT), 스파이웨어 등 악성코드가 사용자의 동의 없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 컴퓨터를 오작동시키고 네트워크를 마비시키는 행위를 말한다.

33) 대개 특정 수법은 특정한 피해를 발생시킨다. 예컨대 해킹에 의해서는 시스템 파괴나 정보 유출을 초래하는 것과 같다. 그러나 하나의 수법은 다른 행위를 위한 수단에 불과한 경우가 많으므로 이를 주의할 필요가 있다.

서비스거부 공격은 시스템에 과도한 부하(負荷)를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 행위를 말한다.

기타 공격 유형은 위의 악성코드공격, 서비스거부공격, 비인가접근공격 등의 요소를 복합적으로 이용하는 공격행위를 말한다.

(2) 공격대상을 기준으로 한 분류

사이버침해는 대상을 기준으로 하는 경우 주요정보통신기반시설에 대한 사이버침해와 일반 정보시스템에 대한 사이버침해로 분류할 수 있다. 이러한 분류는 과학적이기 보다는 현실적인 이유에서 필요하다.

현재 국가 주요정보통신기반시설은 '정보통신기반보호법', '국가사이버안전관리규정'(2005.1.31 제정, 대통령훈령 제141호; 2008.8.18 일부개정, 대통령훈령 제222호), '국방정보화 기반조성 및 국방정보자원관리에 관한 법률'(2010.2.4 제정, 법률 제9995호) 등에 의해 특별한 보호체계를 갖고 있다. '정보통신기반보호법'은 주요정보통신기반시설에 대해, 또 '국가사이버안전관리규정'은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대해, '국방정보화 기반조성 및 국방정보자원관리에 관한 법률'은 국방정보통신망에 대해 전자적 침해 즉, 사이버침해로부터 보호하기 위한 특별한 체계를 마련하고 있다. 즉 분야별 특성에 맞게 사이버침해로부터 주요정보통신기반시설을 보호하도록 하고 있는 것이다.

또한 최근 전세계적으로 큰 문제를 일으키는 스턱스넷(Stuxnet)[34]이 발전소·공항·철도 등 기반시설의 파괴하는 특정한 목적으로 제작된 악성프로그램이라는 점에서도 분야별 특성에 맞는 보호대책의 필요성이 강조될 수 있다.

(3) 공격자를 기준으로 한 분류

사이버침해는 행위자를 기준으로 하는 경우 개인, 범죄집단, 국가로 구분할 수 있

34) 스턱스넷(Stuxnet)은 발전소, 공항, 철도 등 기간시설을 파괴할 목적으로 제작된 바이러스로 2010년 6월에 처음 발견되었다. 네트워크 연결 없이 USB로도 목표 컴퓨터에 쉽게 설치되며, 독일 Siemens의 공업시설 원격제어용 소프트웨어인 PLC 추적 및 새로운 명령을 통해 전력량, 수압, 온도, 밸브개폐 등 SCADA 시스템의 파괴를 유발한다.

다. 전통적으로는 개인 혹은 소수에 의해 해킹, 악성코드 유포 등 사이버침해가 이루어졌으나, 최근 들어서는 범죄집단이 경제적 이득을 목적으로 하거나 국가가 정치적·군사적 목적으로 조직적으로 사이버침해를 하는 경우가 많아지고 있다.

특히 우리나라와 같이 금융 등 경제활동의 많은 부분이 사이버공간에서 이루어지는 경우 범죄집단이나 적대 국가 또는 세력에 의한 사이버침해의 위험이 매우 높다고 할 수 있다. 그리고 각 행위자의 특성에 따라 공격 대상이나 그 피해가 달라질 수 있다. 따라서 행위자는 사이버침해의 성격을 이해하고 적절한 대응책을 마련하는 데 있어 중요한 의미를 갖는다.

(4) 공격 근원지를 기준으로 한 분류

사이버침해의 공격 근원지에 대한 자료(해킹, 악성코드, 스팸메일 등)를 살펴보면 국내 보다는 주로 해외 그리고 특정 국가에 집중되는 것을 알 수 있다.[35] 따라서 공격 근원지도 사이버침해 유형을 분류하는 데 중요한 항목으로 넣을 수 있다.

다. 연구대상인 사이버침해 유형

이상에서 기본적인 사이버침해 유형은 공격 수법과 피해를 기준으로 분류하여야 하겠으나, 안전실태 파악과 대응전략을 수립하는 데 있어서는 공격 수법과 피해, 공격 대상, 공격자 등을 종합적으로 고려할 때 사이버전, 사이버테러(주요 정보통신기반시설 침해), 일반 정보시스템 및 정보 침해로 대별(大別)한다. 이러한 대분류가 앞의 기술적 세분류보다는 공격 대상, 공격자, 피해 등을 모두 포괄할 수 있어서 향후 국가 차원의 정책 분석 및 대응책 마련에 오히려 적합하기 때문이다.

35) 보안전문업체인 시만텍에서 매년 반기별로 180개국 이상을 대상으로 조사·발표하는 사이버 공격 근원지 국가순위에서 중국이 수위를 차지하고 있다. 또한 2007년 KISA가 수행한 침해사고 현장·원격 기술지원 총 76건 중 중국발 해킹사고는 28건으로 전체 기술지원 건수의 37%를 차지하였으며, 중국발 해킹사고의 경우 개인정보 유출을 목적으로 서버를 해킹하는 경우가 다수였다.

표 9 본 연구에서의 사이버침해 유형 분류 기준

유형	공격자	공격 대상	공격 수법	파해	공격 근원지
사이버전	국가	○ 군사시설 ○ 기반시설	모든 수법	국가기능 및 전행수행력 파훼	국외
사이버테러	국가 테러단체	○ 군사시설 ○ 기반시설	모든 수법	사회기능 마비 및 공포	국내 국외
정보시스템 및 정보 침해	범죄단체 개인	○ 일반 정보시스템 ○ 정보	모든 수법	특정 업무 마비 및 정보 유출	국내 국외

제3절 사이버침해 유형별 대응전략 개관

우리나라의 경우 국가사이버안전센터(NCSC)가 2004년에 설립된 이후 사이버안보 분야에 대한 정책 및 업무를 강력하게 추진하고 있으며 가시적인 성과도 이루었다. 민·관·군 등 3원화 체계를 통해 공공분야는 국가정보원 국가사이버안전센터와 행정안전부 정부통합전산센터에서 사이버안전 업무를 수행한다. 국방 분야는 국방정보본부 예하의 사이버사령부에서 수행하고 있으며,[36] 민간분야는 한국인터넷진흥원의 인터넷침해사고대응지원센터와 금융결제원의 금융 ISAC, 코스콤의 증권 ISAC에서 맡고 있다.

범국가적인 사이버안전체계 확립 및 기관 역할 조정 심의를 살펴보면, 국가사이버안전관리 규정 및 국가사이버안전 메뉴얼에 따른 경보발령, 대응 기술 등이 수록되어 있다. 국방의 경우에는 인포콘을 4단계로 발령할 수 있도록 되어있다.

현재 정부는 방송통신위원회에서 정보통신망법을 통해 침해사고 대응, 개인정보보호, 스팸에 대한 업무를 수행하고 있다. 행정안전부는 국가정보화기본법과 정보통신기반보호법을 통해 기반시설 지정 및 관리, 정보화촉진 계획 수립, 정보보호시스템

36) 기무사령부의 국방정보전대응센터에서 수행하던 사이버안전 업무를 사이버사령부에 이양해 통합. http://news.mk.co.kr/v2/view.php?year=2010&no=711898&sID=302.

인증 평가 등을 수행하고 있다. 행정안전부의 공공기관 개인정보보호법에서는 공공기관 개인정보 보호에 대한 업무를, 지식경제부에서는 정보통신산업육성법을 통해 정보산업 촉진 등을 수행하고 있다. 하지만 사이버안보와 관련하여 이원화되어 있는 업무로 인하여 실제 심각한 사이버 공격이 발생한다면 이에 대응할 수 있는 조직이 없는 상태이다.

사이버안보 전략 중에서 가장 중요한 역할을 차지하는 기관이 국방 분야이다. 이미 국가적으로 많은 해킹 사고가 발생하고 있으며, 우리 군도 해킹으로 인한 보안사고가 많이 발생하고 있다. 이러한 해킹 사고는 결국 사이버전으로 발전하게 되고 필요시 해당국과의 분쟁을 넘어 전쟁으로 확산될 수 있는 불씨를 만들게 된다. 하지만 한국의 국방 분야 정보보안 정책 및 기술은 주변 정세에 발맞추어 정립되어 있지 못하다. 군사보안업무시행규칙에 따른 보안정책은 아직까지도 관리적·물리적인 보안정책에 의존하고 있으며, 정보보안 및 사이버보안과 관련한 정책은 매우 제한적으로 제시되고 있는 실정이다. 특히 각종 정보보안관련 사고 발생 시 이에 대한 대응 및 정보작전에 필요한 정보보안의 교리가 아직도 구축되어 있지 않는 상태이다. 이에 대한 대책으로 국방정보보호훈령이 있으나 사이버안보와 관련한 책임 및 처벌 규정이 미약하여 실효성이 적은 상황이다. 실제로 취약점 분석 및 평가, 개인정보보호 관련 조항, 침해사고 예방 및 대응에 대한 업무 절차와 기준만을 규정하고 있고 사이버전에 발생하는 경우 대응할 수 있는 교전 수칙 및 우리 군이 적의 서버 및 기반시설에 대한 원천지 대응에 대한 명확한 규정이 내포되어 있지 않았다.

다만 2010년 2월에 제정된 '국방정보화 기반조성 및 국방정보자원관리에 관한 법률'에서 국방정보에 대한 평시 또는 비상사태 등 상황별 침해대응체계를 구축하고, 국방정보보호대응체계의 효율적인 구축·운용을 위하여 국방사이버안전 전담기관을 설치·지정하여 침해·위협 정보기술의 동향조사 및 분석, 침해된 정보의 유통 또는 유통시도에 대한 감시체계의 구축, 침해·위협에 대한 역추적 등 대응기술의 개발 등을 수행할 근거를 일부 마련하였다.[37]

37) '국방정보화 기반조성 및 국방정보자원관리에 관한 법률'[법률 제9995호, 2010.2.4, 제정] 제21조(국방정보침해에 대한 대응); 동 시행령[대통령령 제22559호, 2010.12.29. 제정] 제16조(국방사이버안전 전담기관).

1. 사이버전

사이버전은 말 그대로 전쟁·전투이다. 따라서 그 주체가 국가 혹은 고도로 조직화된 단체이다.

사이버전은 국제법에서 논의되어야 할 사안이다. 즉, 세계 각국은 국내에서 발생한 사이버 위협의 대처를 위한 법률 체계를 갖고 있지만, 타국과의 공조는 당사국들 간의 개별 사안이다. 현재는 사이버전 선전포고 시점의 불명확성, 적대국 불확실성, 여러 나라를 거치는 라우팅 경로에 따른 국제적 협조 근거 부재 등이 주요 문제점으로 지적되고 있다. 현 사이버전의 형태는 국경이 없고, 국가안보를 위협할 수 있다는 이유로 국제 법으로 규정해야 한다는 논의가 활발히 이루어지고 있는데 근원지, 동기, 대상을 명확하게 밝힐 수 있는 국제 조약, 국제 협약 등이 마련되어야 한다.[38]

2. 사이버테러 (주요정보통신기반시설 보호)

가. 의 의

국가 기반시설을 연결하고 각 정보시스템에 영향을 주는 정보통신기반시설의 광범위한 침해사고는 국가 전반의 장애를 초래할 수 있다. 이러한 배경으로 정보통신기반시설 보호를 사회·경제의 안정과 발전을 위한 핵심요소로 인식하여, 정부는 2001년 '정보통신기반보호법'을 제정하는 등 대응체계를 구축하였다. 이에 따라 국가적으로 중요한 정보시스템 및 정보통신망을 주요정보통신기반시설로 지정하여 취약점 분석·평가, 보호대책 및 보호계획의 수립 등의 조치로 각종 전자적 침해사고를 사전에 예방하고 유사시 적절한 대응 및 복구를 할 수 있는 토대를 마련하였다.

38) 손영동 외, "해외 주요국의 사이버 안보 정책분석 및 강화방안", IT 정보경영학회지 제1권 제1호, 2008. 5, 72쪽.

나. 정보통신기반보호 제도

2001년 '정보통신기반보호법'이 제정된 이래 해킹, 컴퓨터바이러스, 기타 악성프로그램 유포를 비롯한 전자적 침해행위의 수법이 급속히 발전함에 따라 그 피해도 증가하고 있다. 이러한 현실에 비추어 주요정보통신기반시설을 신속하고 효과적으로 보호하기 위하여 위원회의 구성·운영을 실질적으로 변경하고 주요정보통신기반시설 지정권고와 이행여부 확인근거를 신설하는 등 현행제도의 운영과정에서 나타난 미비점을 개선·보완할 필요성이 제기되었다.

행정안전부는 관계기관과 함께 각계 의견수렴 등을 통하여 정보통신기반보호법 개정작업에 착수하여 2007년 12월 개정을 완료하였다. 2009년에는 실효성 있는 정보통신산업 진흥정책을 추진할 수 있도록 '정보통신산업진흥법'이 제정됨에 따라 정보통신기반보호법의 정보보호컨설팅전문업체 조항이 이관되어 정보통신산업진흥법상에 지식정보보안컨설팅전문업체로 변경 반영되었다. 또한 지식정보 보안산업 육성은 지식경제부가 담당하게 됨에 따라 지식정보 보안컨설팅 전문업체 관련 업무도 지식경제부에 이관되었다.

다. 주요정보통신기반시설 지정

주요정보통신기반시설의 지정 대상은 국가·공공기관 뿐 아니라, 민간이 운영·관리하는 정보통신기반시설을 포함하며, 사이버침해행위 발생 시 국가안보, 국민의 기본생활 및 경제안정에 중대한 영향을 미치게 되는 국가안전보장·행정·국방·치안·금융·방송통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템과 정보통신망이 해당된다.

각 중앙행정기관의 장은 소관분야의 정보통신기반시설 중에 해당 관리기관이 수행하는 업무의 중요성 등 5가지 기준에 의하여 전자적 침해로부터 보호해야 할 필요가 있다고 인정되는 시설에 대하여 주요정보통신기반시설로 지정할 수 있다.

표 10 주요 정보통신기반시설 지정 기준

구분	지정 기준
1	· 해당 관리기관이 수행하는 업무의 국가 사회적 중요성
2	· 관리기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3	· 다른 정보통신기반시설과의 상호 연계성
4	· 침해사고가 발생한 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5	· 침해사고의 발생가능성 및 복구의 용이성

2001년 7월 정보통신기반보호법의 시행 이후 주요정보통신기반시설로 지정된 시설은 1차 2001년 4개 부처 23개 시설, 2차 2002년 5개 부처 66개 시설, 3차 2004년 (구)정보통신부 소관 7개 시설, 4차 2005년 중앙선거관리위원회 소관 1개 시설, 5차 2006년 (구)정보통신부 소관 5개 시설, 6차 2007년 3개 부처 10개 시설, 7차 2008년 2개 부처 8개 시설, 2009년에는 4개 부처 21개 시설이 지정되었다. 2010년 1월 현재 10개 관계중앙행정기관 90개 관리기관 126개 기반시설이 지정·관리되고 있다.

표 11 분야별 주요 정보통신기반시설 현황

행정	방송통신	금융	에너지	건설교통	사회복지	기타
행정업무시스템 등	인터넷 접속망 등	인터넷뱅킹 시스템 등	SCADA 시스템 등	운항 관리 시스템 등	보험관리 시스템 등	보험 전산망 등

※ 출처 : 행정안전부 내부자료, 2010년 2월(국가정보보호백서 2010, 81쪽에서 재인용)

라. 취약점 분석·평가

해당 관리기관은 주요정보통신기반시설로 지정 후 6개월 이내에 취약점 분석·평가를 실시해야 한다. 관리기관은 단기적으로 주요정보통신기반시설의 신규 취약점을 제거하고, 장기적으로는 침해사고 발생 시 파급효과를 분석하여 경제적이고 실효성 있는 보호대책을 수립하기 위하여 취약점 분석·평가를 수행한다.

취약점 분석·평가는 매 2년마다 정기적으로 취약점 분석·평가를 수행하고 있으며, 중간연도에는 간이 취약점 분석·평가를 수행하고 있다. 서비스의 확대와 신규

위협의 증가에 따라 취약점의 분석·평가의 주기를 2년에서 매년 실시할 필요성이 제기되고 있다. 정보통신기반보호법 제9조에 따라 관리기관은 '취약점 분석·평가 전담반'을 구성하여 소관시설에 대한 취약점 분석·평가를 수행하거나 한국인터넷진흥원, 정보공유·분석센터, 지식정보 보안컨설팅 전문업체, 국가보안기술연구소가 할 수 있다.

마. 주요정보통신기반시설 보호대책 및 계획의 수립·시행

주요정보통신기반시설을 관할하는 관계중앙행정기관의 장은 정보통신기반보호법에 따라 매년 소관분야 주요정보통신기반시설에 관한 보호계획을 수립·시행하여야 한다. 보호계획은 주요정보통신기반시설을 관리하는 기관에서 제출한 보호대책을 종합·조정하여 작성되며, 관계중앙행정기관의 장은 다음 연도의 보호계획을 정보통신기반보호위원회에 제출하여 심의를 받는다. 위원회에 제출된 보호계획은 심의 과정을 통해 종합·조정하도록 하고 있다.

주요정보통신기반시설에 대한 취약점 분석·평가부터 보호계획의 수립과 그 시행까지의 일련의 과정을 도식화하면 다음과 같다.

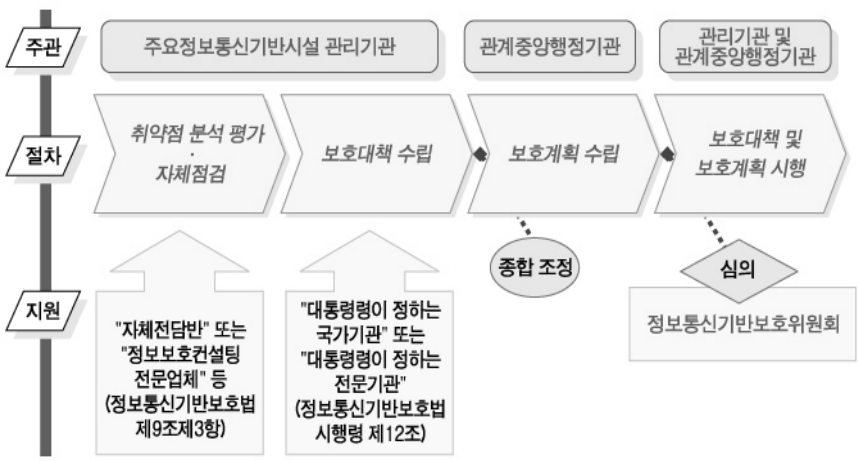


그림 1 주요 정보통신기반시설 보호계획 수립 절차

관리기관에서는 매년 주요정보통신기반시설에 대한 보호대책을 수립하여 관계중앙행정기관에 제출한다. 2001년 정보통신기반보호법 시행 이후, 2002년도에 최초로 총 17개 관리기관에서 총 23개 시설에 대하여 보호대책을 제출한 것을 시작으로 매년 소관 주요정보통신기반시설에 대한 보호대책을 제출하고 있다. 2008년도에는 총 73개 관리기관에서 총 101개 시설에 대한 보호대책을 제출하였다. 2009년도에는 78개 관리기관에서 109개 시설에 대한 보호대책을 제출하였다.

바. 주요정보통신기반시설 이행점검

2007년도에 정보통신기반보호법을 개정하여 2007년 이후에 수립된 보호대책에 대해 행정안전부장관 등이 관리기관에서 작성한 보호대책의 이행 여부를 확인할 수 있도록 하는 등 사후 관리를 강화하였다.

3. 일반 정보시스템 및 정보 침해

최근 공공 및 민간부문에서 일어나는 침해사고의 대부분이 민간의 홈페이지 및 개인 PC가 원인이 되어 발생하므로 민간부문의 정보보호는 국가 정보보호의 기반이 된다.

최근 사이버 공격은 취약한 홈페이지 및 좀비화된 PC에 의해서 이루어지며, 인터넷의 특성상 공공과 민간의 구분은 의미가 없다. 민간부분의 웹서버와 PC가 좀비화되거나, 경유지가 되는 이유는 상대적으로 보안에 취약하기 때문이며, 국내 PC의 약 96% 이상이 민간소유 PC이다. 따라서 민간부문에 대한 정보보호 인식 제고와 좀비 PC 제거 등의 노력 없이는 사이버 침해사고 대응의 실효를 거둘 수가 없으므로, 국가 차원의 침해사고 예방 및 대응을 위해서는 공공 부문과 더불어 민간 부문의 정보보호에 대한 투자 및 인력 확보가 반드시 필요하다. 민간 부문에서 백신 S/W를 사용하지 않거나, 검사를 제대로 수행하지 않아 악성코드 감염위험이 있는 PC는 2009년 현재 491만여대(개인 357만여대, 사업자 134만여대) 이상으로 민간 부문 전체 PC(3,112만여대)의 15.8%를 차지한다. 이는 2007년 7·7 DDoS 침해사고에 동원된

좀비 PC(11만 5천여대)의 약 43배에 해당한다.[39]

최근에는 해킹·바이러스·스팸·개인정보 유출 등 다양한 사이버 위협이 금전 탈취 등을 위해 연계·결합되는 추세이다.

39) 배성훈, '7·7 DDoS 사고' 대응의 문제점과 재발방지 방안, 현안보고서 제48호, 국회입법조사처, 2009. 12. 1, 19쪽.

제3장

우리나라 사이버안전체계의 현황

03 우리나라 사이버안전체계의 현황

제1절 사이버안전 관련 법제

1. 법제형성의 연혁

2003년 초 참여정부는 국가안보차원의 사이버테러 대응역량을 강화하기 위한 논의가 확산되자 (구)한국정보보호진흥원(KISA)의 인터넷침해사고대응지원센터[40]와 국가정보원의 국가사이버안전센터, 국방부의 정보전대응센터[41] 등 사이버안전기관들을 설립, 국가안보회의(NSC) 중심의 대비체계를 마련한데 이어 2005년에는 '국가사이버안전전략회의' 및 '국가사이버안전센터' 설립·운영 등 사이버안전 조직 운영에 대한 사항을 체계적으로 정립한 '국가사이버안전관리규정'(대통령훈령 제267호)을 제정함으로써[42] 국가사이버안전센터를 구심점으로 하는 국가사이버안전관리체계와 '국가위기관리기본지침'(대통령훈령 제229호)에 의한 국가안보회의 주관의 국가위기·재난관리체계를 구축하였다.[43]

---

40) 현재, 한국인터넷진흥원 '인터넷침해대응센터'로 변경.

41) 현재, 국방부의 '사이버사령부'로 변경.

42) <부록 1> 국가사이버안전관리규정 참조.

2007년에는 '전자정부법'의 일부 규정을 수정하는 한편, 행정정보에 대한 보안을 강화하여 (구)행정자치부장관을 위원장으로 하는 '전자정부서비스보안위원회'를 구성하고, 각급 기관은 국가정보원장이 안전성을 확인한 보안조치를 시행토록 하였으며, 국가정보원장이 보안조치 이행여부를 확인할 수 있게 하였다. '정보통신기반보호법'도 국가정보원장과 행정안전부장관이 주요기반시설에 대한 보호대책의 이행여부를 확인할 수 있게 개정하였다.

2008년에는 현 정부가 들어서면서 '정부조직법' 개정으로 정보통신부가 폐지되고, 정보통신부 사무가 행정안전부와 방송통신위원회, 지식경제부 등으로 이관되면서 정보보호 관련 행정부처의 명칭도 변경되어 정보보호 추진체계가 대폭 변화되었다. 동시에 '국가사이버안전관리규정'도 개정되어 '국가사이버안전전략회의' 위원[44]에 교육과학기술부·지식경제부·보건복지부·국토해양부의 차관과 금융위원회 부위원장이 추가되어 외교·행정·국방·금융·통신·과학연구·에너지·교통·교육·보건의료 등 국가 10대 핵심전산망을 관장하는 중앙행정기관들을 국가사이버안전 정책결정에 참여하게 하였다.

2009년 이후에는 정보보호에 관한 국가·사회적 관심이 제고됨에 따라 정보화관련법 개정 및 정보보호 강화 등 법률의 정비가 활발히 이루어졌다. 즉, '정보화촉진기본법'이 '국가정보화기본법'으로 명칭과 규정이 전면 개정되었고, 7·7 DDoS 사태로 인한 후속조치로서 2010년 1월 국회에서 '국방정보화 기반조성 및 국방정보자원관리에 관한 법률'이 제정되었고, 국방정보본부에 '사이버사령부'를 신설하여 정보사령부, 제777부대 등과 함께 배속되었다.[45]

2010년 4월에는 '국가사이버안전관리규정'을 보강하여 각급 기관에 보안관제센터 구축, 대책기구 구성 등 DDoS사태 시 제기된 문제점에 대한 보완 규정이 신설되었다. 즉, '국가사이버안전관리규정' 제10조의2를 신설하여 각급 기관의 장은 보안관제

43) '국가사이버안전관리규정' 제정 전에는 국가안보회의(NSC) 사무처가 적극 참여하여 기관간 조정자적 역할을 수행하였다.

44) 변경된 국가사이버안전전략회의 위원 : 교육과학기술부차관, 외교통상부차관, 법무부차관, 국방부차관, 행정안전부차관, 지식경제부차관, 보건복지부차관, 국토해양부차관, 대통령실 외교안보수석비서관, 방송통신위원회 상임위원, 금융위원회 부위원장, 국가정보원장 및 국가정보원 제3차장 등.

45) 2010 국가정보보호백서, 2010. 5. 171쪽 참조.

센터 설치를 의무화하고, 센터를 설치하지 못할 경우 타 기관에 관제업무를 위탁하게 하였다. 또한, 사이버공격 정보를 수집·탐지할 경우 국가정보원장 및 관계기관에 제공하도록 하고, 보안관제센터를 운영하는 기관은 보안관제 전담직원을 상시 배치하되 필요할 경우에는 전문업체로부터 인력을 파견받을 수 있게 하였다. 한편, 국가정보원장이 필요할 경우에는 범정부적 '사이버위기대책본부'를 구성하여 사이버공격에 대한 원인분석, 사고조사, 긴급대응, 피해복구를 위해 합동조사팀 등을 설치, 운영토록 하였다(국가사이버안전관리규정 제13조).[46]

표 12 국가사이버안전업무 관련 법률 및 규정

구 분	법률 및 규정 명칭	목 적	소관기관
법 률	국가정보화기본법 및 동법 시행령	정보화촉진	범정부
	정보통신기반보호법 및 동법 시행령	기반시설 보호	행정안전부
	정보통신망이용촉진 및 정보보호 등에 관한 법률	침해사고 대응	방송통신위
	전자정부법 및 동법시행령	전자정부 구현	행정안전부
	국가정보원법, 보안업무규정, 정보 및 보안업무 기획조정 규정	각급기관 보안업무	국가정보원
대통령	국가사이버안전관리규정	사이버안전	범정부
훈령	국가위기관리기본지침 (33개분야 중 사이버안전 포함)	위기재난 관리	범정부
지침	국가정보보안기본지침	정보보안	국가정보원

2. 사이버안전 관련 처벌규정

사이버안전을 확보하고 사이버침해에 대응하기 위하여 형법과 관련 특별법에 다양한 벌칙규정이 마련되어 있는데, 이를 구체적으로 살펴보면 다음과 같다.

46) 대통령훈령 제267호, '국가사이버안전관리규정' 일부 개정령, 관보 제17238호, 2010. 4. 16, 4-5쪽.

가. 형법상 사이버침해 관련 처벌규정

사이버침해행위가 형법에 저촉되는 경우로는 종래 공무상 비밀표시무효죄(제140조 제3항), 공용서류 등 무효죄(제141조 제1항), 공전자기록위작·변작죄(제227조의2), 사전자기록위작·변작죄(제232조의2), 업무방해죄(제314조 제2항), 비밀침해죄(제316조 제2항), 권리행사방해죄(제323조), 재물손괴죄(제366조) 등의 성립이 문제될 뿐이었다. 이는 전자기록 등 특수매체기록을 대상으로 하는 범죄이기 때문에 해석상 사이버침해행위가 범죄태양에 당연히 포섭될 수밖에 없다.

그러나 사이버침해의 외연(外延)이 1995년 형법개정 당시에 예상했던 수준을 넘어서서 사이버테러, 사이버전(戰) 개념으로까지 확장되면서 이제는 형법상 외환유치죄(제92조), 시설파괴이적죄(제96조), 간첩죄(제98조), 외국에 대한 사전죄(제111조), 외교상 비밀누설죄(제113) 등의 성립까지도 검토할 필요가 있다. 예컨대 외환유치죄(제92조)는 외국과 통모하여 대한민국에 대하여 전단을 열게 하거나 외국인과 통모하여 항적함으로써 성립하는 범죄인데, 사이버전(戰)을 광의(廣義)의 전투행위로 파악할 수 있다면 외환유치죄 성립을 긍정할 수 있다. 마찬가지로 사이버전 수행과정에서 적국을 위하여 군용 정보통신시스템이나 네트워크를 사용할 수 없게 한 경우에는 시설파괴이적죄(제96조)가 성립할 수 있다. 형법 제111조의 '사전'(私戰) 개념에 사이버전 또는 사이버테러가 포섭될 수 있다면 외국에 대한 사전죄(제111조)가 성립할 수 있을 것이며, 사이버전의 수행과정이 아니더라도 적국을 위하여 해킹 등을 통하여 국가기밀을 탐지·수집하고 이를 누설한다면 간첩죄(제98조)가 성립할 수 있음도 물론이다. 나아가 외교상 비밀의 경우 외교상 비밀누설죄(제113)가 적용될 것이다.

사이버침해 개념의 외연 확장은 교통방해죄(제185조, 제186조), 일수죄(제177조) 등 공공의 안전을 침해하는 범죄의 해석·적용에까지 영향을 미치게 되었는데, 예컨대 시스템이나 네트워크를 교란하여 신호체계를 마비시킨다거나, 가로등, 등대 등을 꺼지게 한 경우 교통방해죄(제185조, 제186조)의 성립이, 시스템이나 네트워크를 교란하여 댐이나 저수지의 수문을 개방하여 강물을 범람하게 한 경우 일수죄(제177조)의 성립이 문제될 수 있을 것이다.

나. 특별법상 사이버침해 관련 처벌규정

(1) 정보통신기반보호법

정보통신기반보호법은 전자적 침해행위에 대비하여 주요 정보통신 기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다(동법 제1조). 여기서 '정보통신 기반시설'이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호의 규정에 의한 정보통신망을 말하며, '전자적 침해행위'라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다(동법 제2조 참조).

주요 정보통신 기반시설의 보호 및 침해사고에 대응하기 위하여 이 법은 ① 접근권한을 가지지 아니하는 자가 주요 정보통신 기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위, ② 주요 정보통신 기반시설에 대하여 데이터를 파괴하거나 주요 정보통신 기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위, ③ 주요 정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위를 하여(동법 제12조 참조) 주요 정보통신기반시설을 교란·마비 또는 파괴한 자에 대하여 10년 이하의 징역 또는 1억원 이하의 벌금에 처하고 있으며(동법 제28조 제1항), 미수범도 처벌하고 있다(동법 제28조 제2항).

(2) 공공기관의 개인정보보호에 관한 법률

'공공기관의 개인정보보호에 관한 법률'은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다(동법 제1조). 여기

서 '개인정보'란 생존하는 개인정보에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보[47]를 말한다(동법 제2조 제2호).

이 법은 개인정보의 보호를 위하여 공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 말소한 행위에 대해서는 10년 이하의 징역에, 개인정보의 업무처리를 위탁받아 그 업무에 종사하거나 종사하였던 자가 직무상 알게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용한 행위에 대해서는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하고 있다(동법 제23조 참조).

(3) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

'정보통신망 이용촉진 및 정보보호 등에 관한 법률'은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다(동법 제1조). 여기서 '정보통신망'이란 전기통신사업법 제2조 제2호[48]에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체제를 말하며, '개인정보'란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보를 말한다.

'정보통신망 이용촉진 및 정보보호 등에 관한 법률'은 개인정보 및 정보통신망을 보호하기 위하여 ① 이용자의 동의를 받지 아니하고 개인정보를 수집한 행위, ② 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 행위, ③ 개인정보를 이용하거나 제3자에게 제공한 자

47) 당해 정보만으로도 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다. 이하 같다.

48) 전기통신사업법 제2조 제2호. "전기통신설비"란 전기통신을 하기 위한 기계·기구·선로 또는 그 밖에 전기통신에 필요한 설비를 말한다.

및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 행위, ④ 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 행위, ⑤ 이용자의 개인정보를 취급하고 있거나 취급하였던 자가 이용자의 개인정보를 훼손·침해 또는 누설하는 행위, ⑥ 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 행위, ⑦ 정보통신서비스 제공자 등은 오류정정의 요구를 받으면 지체 없이 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알려야 하는데, 이를 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 행위, ⑧ 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집하는 행위, ⑨ 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 악성프로그램을 전달 또는 유포하는 행위, ⑩ 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 행위, ⑪ 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하는 행위에 대하여 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하고 있다(동법 제71조 참조). 이와 관련하여 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하는 행위의 미수범은 처벌하며, 기망하여 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여 다른 사람의 개인정보를 수집하는 행위, 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용하는 행위는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고 있다(동법 제72조 참조).

참고로, 정보통신서비스 제공자 등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영, 접속기록의 위조·변조 방지를 위한 조치, 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치, 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 등 기술적·관리적 조치를 하여야 하며, 이에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손하거나, 방송통신위원회의 명령을 위반하여 정보통신망의 접속기록 등 관련 자료를 보전하지 아니하거나, 속이는 행위로 정보통신망을 통하여 다른 사람의 정보를 수집하거나 다

른 사람이 정보를 제공하도록 유인한 경우에도 2년 이하의 징역 또는 1천만원 이하의 벌금에 처하고 있다(동법 제73조 참조).

(4) 주민등록법

'주민등록법'은 시·군·구의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것을 목적으로 하는데(동법 제1조), 사이버침해와 관련해서는 ① 거짓의 주민등록번호를 만드는 프로그램을 다른 사람에게 전달하거나 유포하는 행위(동법 제37조 제4호), ② 법률에 따르지 아니하고 영리의 목적으로 다른 사람의 주민등록번호에 관한 정보를 알려주는 행위(동법 제37조 제9호), ③ 다른 사람의 주민등록번호를 부정하게 사용하는 행위(동법 제37조 제10호)에 대하여 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하고 있다.

(5) 통신비밀보호법

'통신비밀보호법'은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다(동법 제1조). 이 법은 사이버침해와 관련하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인 간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취한 경우(동법 제16조 제1항 제1호, 제3조, 제14조) 10년 이하의 징역과 5년 이하의 자격정지에 처하고 있다. 대화비밀을 침해하거나 통신비밀을 침해하여 지득한 통신 또는 대화의 내용을 공개하거나 누설한 경우(동법 제16조 제1항 제2호, 제16조 제2항-제4항, 제11조)도 마찬가지이다.

(6) 산업기술의 유출방지 및 보호에 관한 법률

'산업기술의 유출방지 및 보호에 관한 법률'은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함을 목적으로 한다(동법 제1조). 이 법은 산업기술을 외국에

서 사용하거나 사용되게 할 목적으로 절취·기망·협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개하는 행위에 대하여 10년 이하의 징역 또는 10억원 이하의 벌금에 처하고 있는데(동법 제36조 제1항 참조), 사이버침해의 경우도 포함된다고 할 것이다.

(7) 전자서명법

'전자서명법'은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다(동법 제1조). 여기서 '전자문서'라 함은 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말하며, '전자서명'이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

전자서명법은 가입자의 신청 없이 가입자의 전자서명생성정보를 보관하거나 전자서명생성정보의 보관을 신청한 가입자의 승낙 없이 이를 이용하거나 유출한 행위, 타인의 전자서명생성정보를 도용 또는 누설한 행위, 타인의 명의로 공인인증서를 발급받거나 발급받을 수 있도록 한 행위에 대하여 3년 이하의 징역 또는 3천만원 이하의 벌금에 처함으로써 사이버침해에 대비하고 있다.

(8) 전자무역 촉진에 관한 법률

'전자무역 촉진에 관한 법률'은 전자무역의 기반을 조성하고 그 활용을 촉진하여 무역절차의 간소화와 무역정보의 신속한 유통을 실현하고 무역업무의 처리시간 및 비용을 절감함으로써 산업의 국제경쟁력을 높이고 국민경제의 발전에 이바지함을 목적으로 한다(동법 제1조). 여기서 '전자무역'이라 함은 '대외무역법' 제2조 제1호의 규정[49]에 의한 무역의 일부 또는 전부가 전자무역문서에 의하여 처리되는 거래를

49) 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. "무역"이란 다음 각 목의 어느 하나에 해당하는 것(이하 "물품등"이라 한다)의 수출과 수입을 말한다.

말하며, '전자무역 기반시설'이라 함은 정보통신망을 통하여 무역업자와 무역유관기관을 체계적으로 연계하여 전자무역문서의 중계·보관 및 증명 등의 업무를 수행하는 정보시스템을 말한다(동법 제2조 참조).

사이버침해와 관련하여 이 법은 전자무역기반사업자·전자무역전문서비스업자·무역업자·무역유관기관의 컴퓨터파일에 기록된 전자무역문서 또는 데이터베이스에 입력된 무역정보를 위조 또는 변조하거나 위조 또는 변조된 전자무역문서 또는 무역정보를 행사하는 행위, 전자무역기반사업자의 컴퓨터 등 정보처리장치에 거짓 정보 또는 부정한 명령을 입력하여 정보처리가 되게 하는 등의 방법으로 증명서를 발급하는 행위에 대하여 1년 이상 10년 이하의 징역 또는 1억원 이하의 벌금에 처하고 있으며(동법 제30조 참조), 전자무역기반사업자·전자무역전문서비스업자·무역업자·무역유관기관의 컴퓨터파일에 기록된 전자무역문서 또는 데이터베이스에 입력된 무역정보를 훼손하거나 그 비밀을 침해한 행위, 업무상 알게 된 전자무역문서 또는 무역정보에 관한 비밀을 누설하거나 도용한 행위에 대해서는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하고 있다(동법 제31조 참조).

(9) 물류정책기본법

'물류정책기본법'은 물류체계의 효율화, 물류산업의 경쟁력 강화 및 물류의 선진화·국제화를 위하여 국내외 물류정책·계획의 수립·시행 및 지원에 관한 기본적인 사항을 정함으로써 국민경제의 발전에 이바지함을 목적으로 한다(동법 제1조). 여기서 '물류'란 재화가 공급자로부터 조달·생산되어 수요자에게 전달되거나 소비자로부터 회수되어 폐기될 때까지 이루어지는 운송·보관·하역 등과 이에 부가되어 가치를 창출하는 가공·조립·분류·수리·포장·상표부착·판매·정보통신 등을 말한다.[50]

가. 물품

나. 대통령령으로 정하는 용역

다. 대통령령으로 정하는 전자적 형태의 무체물(無體物)

50) 물류정책기본법에서는 단위물류정보망과 종합물류망을 구축하고 있는데, '단위물류정보망'이란 기능별 또는 지역별로 관련 행정기관, 물류기업 및 그 거래처를 연결하는 일련의 물류정보체계를 말하며, '종합물류정보망'이란 단위물류정보망을 종합적으로 연계하여 구성한 물류정보체계라고 정의하고 있다(제2조 참조).

사이버침해와 관련하여 이 법은 종합물류정보망 또는 물류기업, 물류관련기관 및 물류 관련 단체가 대통령령으로 정하는 물류정보에 관한 전자문서를 위작 또는 변작하거나 위작 또는 변작된 전자문서를 행사하는 행위에 대해서는 10년 이하의 징역 또는 2억원 이하의 벌금에 처하고 있고, 미수범을 처벌하고 있다(동법 제71조 제1항). 또한, 종합물류정보망 또는 국가물류통합데이터베이스에 따라 처리·보관 또는 전송되는 물류정보를 훼손하거나 그 비밀을 침해·도용 또는 누설하는 행위에 대해서는 5년 이하의 징역 또는 1억원 이하의 벌금에(동조 제2항), 종합물류정보망 또는 국가물류통합데이터베이스의 보호조치를 침해하거나 훼손한 행위에 대해서는 3년 이하의 징역 또는 5천만원 이하의 벌금에(동조 제3항), 전자문서 또는 물류정보를 공개하는 행위에 대해서는 3천만원 이하의 벌금에 처하고 있다(동조 제6항).

(10) 전자정부법

'전자정부법'은 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정함으로써 전자정부를 효율적으로 구현하고, 행정의 생산성, 투명성 및 민주성을 높여 국민의 삶의 질을 향상시키는 것을 목적으로 한다(동법 제1조). 여기서 '전자정부'란 정보기술을 활용하여 행정기관 및 공공기관의 업무를 전자화하여 행정기관 등의 상호 간의 행정업무 및 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.

사이버침해와 관련하여 이 법은 행정정보의 처리업무를 방해할 목적으로 행정정보를 위조·변경·훼손하거나 말소하는 행위에 대해서는 10년 이하의 징역에(동법 제76조 제1항), 행정정보 공동이용을 위한 정보시스템을 정당한 이유 없이 위조·변경·훼손하거나 이용하는 행위, 행정정보를 변경하거나 말소하는 방법이나 프로그램을 공개·유포하는 행위에 대해서는 5년 이하의 징역 또는 5천만원 이하의 벌금에(동조 제2항), 공개하여서는 아니 되는 행정정보를 정당한 이유 없이 누설하는 행위, 직무상 알게 된 비밀을 누설하거나 도용하는 행위에 대해서는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고 있다(동조 제3항 제1호 및 제5호).

(11) 신용정보의 이용 및 보호에 관한 법률

‘신용정보의 이용 및 보호에 관한 법률’은 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모하며 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 하는데(동법 제1조), 여기서 ‘신용정보’란 금융거래 등 상거래에 있어서 거래 상대방의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보를 말한다.

신용정보회사 등은 ① 국가의 안보 및 기밀에 관한 정보, ② 기업의 영업비밀 또는 독창적인 연구개발 정보, ③ 개인의 정치적 사상, 종교적 신념, 그 밖에 신용정보와 관계없는 사생활에 관한 정보, ④ 확실하지 아니한 개인신용정보, ⑤ 다른 법률에 따라 수집이 금지된 정보, ⑥ 그 밖에 대통령령으로 정하는 정보 등을 수집·조사하여서는 아니 되며, 신용정보전산시스템의 정보를 변경·삭제하거나 그 밖의 방법으로 이용할 수 없게 한 자 또는 권한 없이 신용정보를 검색·복제하거나 그 밖의 방법으로 이용한 경우(동법 제19조 제1항) 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고 있다(동법 제50조 제2항).

(12) 공직선거법

‘공직선거법’은 대한민국 헌법과 지방자치법에 의한 선거가 국민의 자유로운 의사와 민주적인 절차에 의하여 공정히 행하여지도록 하고, 선거와 관련한 부정을 방지함으로써 민주정치의 발전에 기여함을 목적으로 한다(동법 제1조). 사이버침해와 관련하여 이 법은 선거운동정보를 전송하는 자가 수신자의 수신거부를 회피하거나 방해할 목적으로 기술적 조치를 한 경우, 행위주체를 불문하고 숫자·부호 또는 문자를 조합하여 전화번호·전자우편 등 수신자의 연락처를 자동으로 생성하는 프로그램 그 밖의 기술적 장치를 이용하여 선거운동정보를 전송한 경우는 1년 이하의 징역 또는 100만원 이하의 벌금에 처하고 있다(동법 제255조 제4항).

3. 사이버안전 업무수행의 법적 근거

국가사이버안전은 국가기밀과 군사·외교정보를 포함한 국가안보정보는 물론 산업기밀 정보 등까지도 함께 보호하는, 국익과 직결된 업무로서 국민의 안전한 삶에 직접적인 영향을 미치고 있다. 그렇기 때문에 우리나라의 사이버안전은 '정부조직법'을 비롯한 다양한 법률에 기반하여 다양한 기관들이 분야별로 분담하여 업무를 수행하고 있는 바, 주로 국가정보원, 방송통신위원회, 행정안전부, 지식경제부가 각각 기능별로 업무를 담당한다.[51]

국가정보원은 정부조직법 제15조에 의거하여 대통령소속 하에 국가안전보장과 관련되는 정보·보안 및 범죄수사에 관한 사무를 담당할 목적으로 각급 기관에 대한 정보 및 보안업무의 기획, 조정업무(국가정보원법 제3조)를 수행한다. 또한, 국가안전보장회의법 제10조에 의거하여 국가안보와 관련된 국내외 정보를 수집·평가, 이를 회의에 보고한다. 나아가 '정보및보안업무기획조정규정', '보안업무규정'에 의거하여 각급 기관에 대한 보안업무를 수행하고, '국가사이버안전관리규정'에 의거하여 사이버 안전정책 총괄 및 위협정보 수집·분석, 대응 업무를 수행한다.

행정안전부는 정부조직법 제29조에 의거하여 전자정부 및 정보보호업무, 그리고 다른 중앙행정기관의 소관에 속하지 않는 사무를 처리하고 있으며, '행정안전부직제령'이 정한 국가기반시설 보호업무와 한국정보화진흥원에 대한 관리감독, 정부통합전산센터 운영 및 '중앙행정기관 사이버침해사고 대응센터', 개인정보보호업무 등을 수행한다.

방송통신위원회는 (구)정보통신부의 업무를 계승한 대통령소속 기관으로서 별도의 '방송통신위원회 설립 및 운영에 관한 법률'에 의해 운영된다. 따라서 '방송통신위원회직제령'에 의거하여 방송통신보안, 통신비밀보호, 네트워크의 안전 확보, 침해사고 대응 및 정보통신망 안전진단, 암호정책 업무를 수행하며 '국가사이버안전관리규정' 제11조(경보발령)에 의거하여 사이버공격 시의 경보업무를 취급한다.

지식경제부는 2008년부터 (구)정보통신부에서 소관해온 정보보호제품의 안전기준 제정 및 제품 평가 업무와 인증기관 지정업무 등 주로 정보보호 산업의 육성업무를

51) 2009 국가정보보호백서, 148쪽.

수행한다. 즉, 지식경제부직지령 제16조(기술표준원 직무)에 의거하여 정보보호산업 지원 및 적합성 평가분석 등의 행정사무를 수행한다. 또한, 정보통신망법에 의거한 정보보호제품 인증기관 지정업무도 수행한다.

이하에서는 우리나라의 사이버침해 대응체계를 보다 심도 있게 분석하기 위하여 국가사이버안전관리체계를 중심으로 한 국가정보원의 사이버침해 대응체계, 방송통신위원회의 사이버침해 대응체계 및 경찰청의 사이버침해 대응체계로 구분하여 살펴보기로 한다.

제2절 국가정보원의 사이버침해 대응체계 개관

1. 국가사이버안전관리 체계

국가사이버안전체계는 '국가사이버안전관리규정'에 의해 정부가 국가안보차원의 사이버위협에 대한 대응을 보다 강화하여 국가 인터넷망의 전자적 침해사고 조기탐지 및 피해확산 방지를 위해 구축한 범국가적 체계이다.[52] 한국인터넷진흥원의 '인터넷침해대응센터'가 민간분야를 담당하고, 국가안전보장회의(NSC) 사무처 주관 하에 범정부적 차원에서 출범한 국가정보원 소속의 '국가사이버안전센터'(NCSC : National Cyber Security Center)가 공공분야를 담당하며, 국방정보본부 산하의 '사이버사령부'가 군 분야를 담당하는 민·관·군 종합 대응체계이다.

52) 2009 국가정보보호백서, 10쪽.

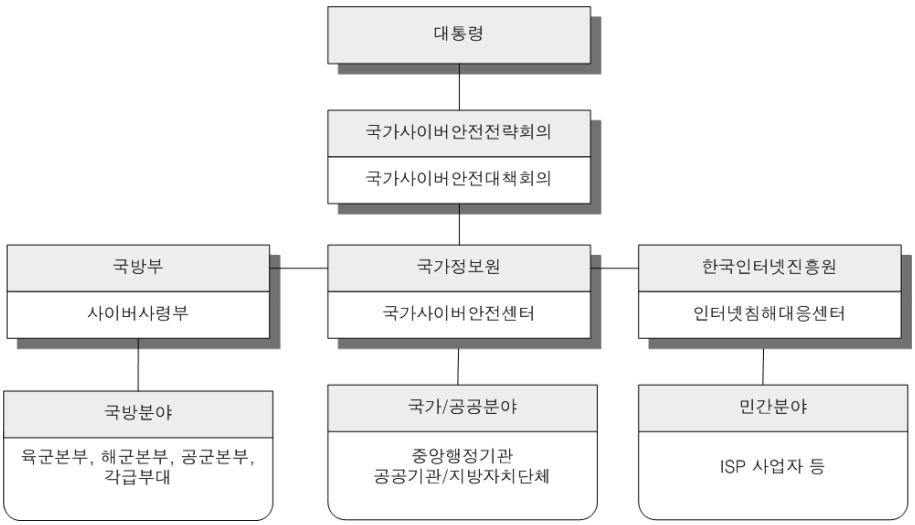


그림 2 국가사이버안전 관리체계

여기에는 2004년 7월 제정된 '국가위기관리기본지침'과, 이를 근거로 핵심기반 분야에 사이버안전을 포함시켜 2004년 9월 마련된 '사이버안전분야 위기관리표준매뉴얼'에 적용되는 위기관리 차원의 사이버위기관리도 포함된다.[53]

공공분야는 '국가사이버안전센터'에서 국가사이버안전관리규정에 따라 사이버위협정보 수집, 분석을 위하여 보안관제시스템을 운용하고 국가전산망에 대한 사이버침해에 대응, 복구지원 활동, 사이버안전 정책결정 등 범정부차원에서 국가사이버안전업무에 대한 총괄 조정 역할을 수행한다.[54]

국방분야의 사이버안전업무는 국방부가 국가사이버안전관리규정에 근거하여 수행

53) 2004년 이후 중국 발 국가기관 해킹사고가 계속 증가되면서 정부는 NSC중심의 비상시 사이버위기관리업무와 보안기관으로서 국가정보원이 평상시 수행하는 사이버안전업무를 일원화할 필요성이 대두되자, 이와 같은 해킹사고의 공간인 인터넷이 민·관·군 영역을 구분할 수 없을 뿐만 아니라 사전 예방활동을 통하여 피해를 미연에 방지하는 것이 중요한 문제로 제기되면서 각각의 분야와 기관을 막론하고 정보공유 등 업무협조가 절실히 요구되었다. 따라서 노무현대통령은 2004년 '국가차원에서 사이버안전업무를 총괄하는 기관을 정하고 이를 규범화 할 것'을 지시하였다. 이를 계기로 국가정보원장을 의장으로 외교통상부, 법무부, 국방부, (구)행정자치부, (구)정보통신부, 국가안전보장회의 사무처 등의 차관급을 위원으로 하는 '국가사이버안전전략회의'의 설치, 유관기관간 정보공유 및 업무협조 강화 등을 명시한 '국가사이버안전관리규정'을 제정, 시행하게 되었다.

54) 2007 국가정보보호백서, 49쪽.

한다. 예전에 정보본부 산하 '사이버사령부'를 통하여 독자적으로 수행하며, 각급부대 정보통신망에 대한 안전성 확인, 경보발령, 사고조사 및 관련 정보 통보 등이 별도로 이루어졌다.[55]

하지만 국방부는, 최근 국방정보화 기반조성 및 국방정보자원관리에 관한 법률 제정을 통해 국방사이버안전 전담기구를 설치 국방정보침해 대응 기술 개발, 정보보호 협력체계 구축 등을 마련하였다. 이 국방사이버안전 전담기관은 국방통합보안관제 및 위협정보를 수집, 분석하고 사이버 위기 대응 전문기관 등과 협력할 수 있도록 했다. 이 규정에 따라 사이버안전 전담기관을 설치할 수 있도록 되어 있으나 현 사이버사령부를 지정하는 방식으로 진행될 것으로 예상되고 있다. 사이버사령부는 2010년 1월 국방부 정보본부 산하에 창설되었으며, 육·해·공군별로 운영중인 CERT(침해사고대응팀)간의 정보 공유 및 주의사항 종합분석, 진단 등의 임무를 수행하고 있다. 이에 따라 사이버사령부가 상당부분 사이버안전 전담기관과 역할이 유사한 만큼 신설보다는 지정하는 방식으로 진행된다고 볼 수 있다.

민간분야의 사이버안전활동은 정보통신망법[56]에 따라 방송통신위원회가 정보보호 지침을 정하여 고시하고 정보보호안전진단 수행기관을 관리 감독하며, 정보보호 관리체계 인증업무를 수행한다. 이에 따라 한국인터넷진흥원[57] 소속의 '인터넷침해대응센터'를 통하여 민간분야 정보통신망 침해사고에 관한 정보의 수집, 전파, 침해사고의 예보, 경보, 침해사고에 대한 긴급조치 등 각종 대응업무를 수행한다. 한편, ISP 등 주요 정보통신사업자와 집적정보통신시설사업자는 침해사고가 발생하면 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다.[58]

---

55) '국가사이버안전관리규정' 제18조는 국방분야의 안전성확인, 경보발령, 사고통보, 사고조사 등을 국방부장관이 수행토록 위임되어 있다.

56) '국가사이버안전관리규정'은 대통령훈령이므로 각급기관만 해당하고, 금융·통신 등 민간분야에는 적용되지 않는다.

57) 한국정보보호진흥원의 인터넷침해사고대응지원센터가 한국인터넷진흥원 인터넷침해대응센터로 명칭이 변경되었다. 인터넷 침해대응센터는 침해사고 대응단, 침해예방단으로 구성되어 있다. 24시간 365일 인터넷 침해사고에 대한 조기탐지, 분석, 필요시 경보 발령을 통해 피해확산 방지를 위한 노력과 118상담센터 운영 및 스팸과 컴퓨터 바이러스로 인한 인터넷 이용시 발생할 수 있는 불편한 사항을 해소하기 위하여 기술적인 지원을 실시하고 있다. 특히, 분산서비스거부공격(DDoS)과 좀비 PC로 인한 인터넷 침해사고의 확산을 최소화하기 위하여 이에 대한 집중적인 노력을 수행하고 있다. 또한 해킹 악성코드 동향 파악, 인터넷침해사고에 대한 대응방안 수립과 기술의 지원, 국내외 보안전문기관과 신속한 공동대응체계를 운영하여 인터넷 침해사고 예방과 대응을 위한 다양한 활동을 전개해 나가고 있다.

가. 국가사이버안전전략회의

국가사이버안전전략회의(이하 "전략회의"라 한다)는 '국가사이버안전관리규정' 제6조에 의거 설치된 우리나라 사이버안전의 최고 정책기구로서 국가사이버안전과 관련된 사항을 심의한다. 전략회의 의장은 국가정보원장이 되며, 위원은 교육과학기술부·외교통상부·법무부·국방부·행정안전부·지식경제부·보건복지부·국토해양부 차관과 외교안보수석 비서관, 방송통신위원회 상임위원, 금융위원회 부위원장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 구성된다. 전략회의는 국가사이버안전체계의 수립 및 개선에 관한사항, 국가사이버안전 정책 및 기관간 역할조정에 관한 사항, 대통령 지시사항에 대한 조치 방안, 그밖에 전략회의 의장이 부의하는 사항 등을 다룬다.

나. 사이버안전 대책회의

사이버안전전략회의의 효율적인 운영을 위하여 동 전략회의 산하에 국가사이버안전대책회의(이하 "대책회의"라 한다)를 두고 있다. 대책회의 구성은 국가정보원의 사이버 안전업무를 담당하는 차장이 의장을 맡고 있으며, 위원은 전략회의 위원이 속하는 기관의 실·국장급 공무원이 맡고 있다. 대책회의는 '국가사이버안전관리규정' 제7조에 의거 국가사이버안전관리 및 대책방안, 전략회의의 결정사항에 대한 시행방안, 전략회의로부터 위임받거나 전략회의 의장으로부터 지시받은 사항, 그리고 그밖에 대책회의 의장이 부의하는 사항 등에 대해 심의한다.[59]

다. 국가정보원

국가정보원은 국가정보원법, 보안업무규정, '정보 및 보안업무 기획조정규정'과 '정보통신기반보호법', '전자정부법' 등 관련 법규에 의해 국가 정보보안업무의 기획·조정 및 보안정책 수립 시행 등 국가공공기관에 대한 정보보안업무를 담당하고 있다. 특히 '국가사이버안전관리규정'에 의거 사이버안전정책 및 관리에 대해 국가정

58) 2007 국가정보보호백서, 11쪽.

59) 2007 국가정보보호백서, 49쪽.

보원장이 관계 중앙 행정기관의 장과 협의, 이를 총괄·조정[60]하는 등 국가사이버안전관리업무를 수행하는 전담기관이다. 국가정보원은 1998년부터 국가·공공기관을 대상으로 정보통신보안대책을 지원, 해킹·컴퓨터바이러스 유포 등 사이버 공격에 대한 예방·복구는 물론, 국가보안목표시설에 대한 보안측정, 국가안보관련 정보통신기반시설의 보호업무, 국가·공공기관용 암호장비 등 보안시스템의 개발·보급, 보호시스템의 인증업무 등을 수행하여 왔다. 산하에 '국가사이버안전센터'를 두고 사이버안전정책 수립, '국가사이버안전전략회의' 운영 및 국가정보통신망 및 시스템의 안전성 확인업무를 수행한다.

라. 국가사이버안전센터

국가정보원 소속의 국가사이버안전센터(National Cyber Security Center : NCSC)는 사이버공격에 대한 국가차원의 체계적인 대응을 위해 2004. 2월 설립된 기관으로서 정보통신망에 대한 24시간 사이버 위협정보를 수집·분석·전파하는 국가 종합상황실을 운영하면서 각종 사이버공격에 대한 예방·대응활동과 피해확산 방지에 주력한다. 또한 국가·공공기관 등 공공분야를 대상으로 사이버위협에 대한 수준별 경보발령 등 각종 사이버공격에 대응하고 24시간 네트워크 보안관제를 통해서 사이버위협 정보를 수집·분석하여 각급기관에 전파한다. 한편, 침해사고 발생 시 긴급대응·조사 및 복구를 지원하고 국방부, 법무부, 행정안전부, 지식경제부, 방송통신위원회, 경찰청 등 물론 해외 유관기관과의 정보협력을 강화하고 있다. 또한 범정부차원에서 사이버위협 정보의 공유, 수준별 경보 심의 등의 업무협조를 위하여 관계 기관에서 파견된 공무원들로 구성된 '협력관실'을 운영하고 있다. 아울러 국가사이버안전매뉴얼의 작성·배포, 사이버공격으로 인하여 발생한 사고의 조사 및 복구지원 등 업무를 수행한다.

60) '국가사이버안전관리규정' 제5조(국가사이버안전정책 및 관리) : 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다.

2. 위협정보 탐지 및 대응활동

가. 보안관제

최근 사이버위협은 단순한 웜·바이러스 유포에서 탈피, 각종 악성코드를 결합한 웹 해킹, 대규모 네트워크를 이용한 DDoS 공격, 무선인터넷 해킹 등 다양한 형태로 발전함에 따라 사이버피해를 최소화하기 위해서는 국가전산망에 대한 이러한 침입시도를 미연에 탐지하는 활동이 중요하다.[61] 우리나라에서는 1999. 9. 21일부터 '안랩 코코넛'이 민간업체를 대상으로 보안관제를 시작한 이래, 아직까지 보안관제(모니터링)의 개념에 관한 명확한 정의 없이 주로 TMS(Threat Management System), ESM(Enterprise Security Management) 등 센서(NIDS)를 사용, 사이버위협정보를 탐지하고 있다. 민·관·군에서도 '보안관제'라는 용어를 사용한다.[62] 국가 공공기관의 보안관제는 최초 2002. 12월 금융결제원의 금융ISAC이 18개 시중은행에 대한 관제를 시작, 2004년 출법한 국가사이버안전센터가 국가 차원의 종합 보안관제기능을 수행하고 있다.

국방분야의 경우, '사이버사령부'에서 국방부와 군부대 등 군의 인터넷 홈페이지를 대상으로 보안관제·분석업무를 수행하며 민간분야는 '인터넷침해사고대응센터'에서 국내 인터넷에 대한 보안관제를 실시하고 있다. 동 센터는 주요 통신사업자 및 관제업체의 네트워크 정보를 실시간으로 제공 받아서 신규 출현 웜·바이러스의 위험도를 분석, 홈페이지를 통하여 국민들에게 대응방법을 전파한다.

2008. 2월에는 교육사이버안전센터가 개소, 전국 초·중·고 등 교육과학기술부 산하 각급학교 및 교육청으로부터 사이버위협정보를 수집하고, 행정안전부도 전자정부 통합망과 16개 광역시 도를 비롯한 지방자치단체 등에 대한 보안관제를 실시한다. 또한 외교부는 외교통신망에 대해서 보안관제를 실시하는 등 각급기관에서 부문관제센터들이 설립, 운용하고 있다.

보안관제는 행정·국방·외교·금융·보건·교육·교통 등 공공부문 관제센터와 한국전력 및 KT·데이콤 통신가입자 대상의 에너지·금융 등 민간부문 관제센터로

61) 보안관제와 관련된 내용은 2006 국가정보보호백서, 111-112쪽 참조.

62) 김영진, "국가전산망 보안관제업무의 효율적 수행방안에 관한 연구", 정보보호학회지, 2009. 2.

구분한다. 지방자치단체를 비롯한 지방교육청 및 경찰청 본부와 지방경찰청 경찰서 및 한국전력공사와 전력거래소, 특허청, 관세청, 한국수자원공사, 국세청, 국회, 방위사업청 등 단위별 보안관제센터로 구분하여 구축되고 있다.

표 13 단계별 법적 근거

구분	주요내용	법적 근거	
		관련 법규	세부 내용
예방 활동	안전성 확인	전자정부법	제27조 정보통신망 등의 보안대책 수립·시행, 안전성확인
	보호제품 사용 – 적합성 검증 – 평가 인증	동법시행령	제35조 전자문서의 보관·유통관련보안조치
		정보화촉진기본법	제15조 정보보호시스템에 관한 기준 고시 등
		동법시행령	제16조 정보보호시스템의 보완 등
		정보보안기본 지침	제91조 도입, 검증필 정보보호제품 사용, 보안적합성 검증요청
	취약점 분석	전자정부법	제27조 정보통신망 등의 보안대책 수립·시행
	평가	전자정부법 시행령	제35조 전자문서의 보관·유통 관련 보안조치
		사이버안전 관리규정	제8조 국가사이버안전센터 ①항, 제9조 안전대책의수립·시행
		정보보안 기본지침	제105조 정보보안측정 ①항
	국제 협력	사이버안전 관리규정	제8조 국가사이버안전센터, 제14조 전문기관간협력, 제16조 인력양성
탐지	보안 관제	사이버안전 관리규정	제11조 경보발령, 제12조 사고통보 및 복구, 제14조 전문기관간 협력 등
	예경보 발령	사이버안전 관리규정	제11조 경보발령 ①항, 제12조 사고통보 및 복구 ①항
복구	사고조사 복구	사이버안전 관리규정	제13조 사고조시 및 처리, 제14조 전문기관간 협력, 제15조 연구개발
		정보보안 기본지침	제107조 정보보안사고 처리 및 조사

현재 우리나라 보안관제의 법적근거는 '국가사이버안전관리규정'(대통령훈령제267호) 제8조 제2항 3호 및 제15조 제1항, 제10조의2를 통하여 사이버위협 탐지를 위한 보안관제를 실시한다. 동 규정은 2010. 4월 일부개정, 제10조의2를 신설하여 모든 중앙행정기관과 지방자치단체, 그리고 공공기관에서 관제센터 운영을 의무화하고, 이를 운영하지 못하지 못하는 경우에는 위탁관제를 할 수 있게 하였다.[63]

나. 예·경보 발령 및 전파

사이버공격을 적시에 탐색, 차단하기 위해 각종 위협정보의 흐름을 실시간 관제하여 보안 위해요인 및 공격유형 등을 종합분석하고 위협징후가 포착되면, 예·경보를 발령한다. '국가사이버안전관리규정' 제11조에 의거 국가정보원장은 사이버공격의 파급영향, 피해규모 등을 고려하여 〈그림 4〉과 같이 국가차원에서 관심·주의·경계·심각 등 수준별 경보를 발령한다.

63) 제10조의2(보안관제센터의 설치 운영) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지 분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 설치 운영하여야 한다. 다만, 보안관제센터를 설치 운영하지 못하는 경우에는 다른 중앙행정기관(국가정보원을 포함한다)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치 운영하는 보안관제센터에 그 업무를 위탁할 수 있다. ② 보안관제센터를 설치 운영하는 기관의 장은 수집 탐지한 사이버 공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다. ③ 보안관제센터를 설치 운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다. ④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 지식경제부장관이 지정하는 보안관제전문업체의 인원을 파견 받아 보안관제업무를 수행하도록 할 수 있다. 이 경우 보안관제전문업체의 지정 관리 등에 필요한 사항은 지식경제부장관이 국가정보원장과 협의하여 정한다. ⑤ 제1항의 보안관제센터의 설치 운영 및 제2항의 사이버공격정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.

그림 3 사이버 위협 단계별 발령경보

출처 : 국가정보원 국가사이버안전센터(www.ncsc.go.kr)

민간분야는 방송통신위원회가 경보를 발령하며, 공공분야는 국가사이버안전센터가 각급기관 정보통신망을 관제, 사이버공격 징후를 탐지, 위험도와 피해규모 등을 고려, 사이버위협 단계별 경보를 발령한다. 경보는 단계별 주요 대응내용과 함께 정상(Green), 관심(Blue), 주의(Yellow), 경계(Orange), 심각(Red)등 수준별로 하고 발령은 주로 정보보안 담당자와 비상연락망을 통해 SMS나 E-mail을 통해 전파한다.

다. 사고조사 및 복구

해커의 공격으로 국가·공공기관에서 사이버침해사고가 발생할 경우, 피해확산 차단을 위해 원격, 또는 직접 사고기관을 방문하여 사고조사 및 긴급 대응업무를 수행하는데,[64] 이는 '국가사이버안전관리규정'에 근거한다. 국가·공공기관에서 피해신고

64) 사고조사 및 복구와 관련한 내용은 2006 국가정보보호백서, 114쪽 참조

가 있거나 해킹기록 사이트(Zone-H 등)를 통해 사고를 인지하면, 현장에 직접 출장 조사 또는 원격조사 등을 통해 사고 내용을 확인, 복구하여 정상상태로 복원시키고 사고원인을 분석, 사고재발 및 확산 방지를 위한 보안대책을 지원한다. 또한 사고조사에서 공격자가 내국인으로 밝혀지면, 수사기관에 이첩하여 수사를 의뢰하고 외국인일 경우에는 당사국 사이버안전기관에 통보한다.

국방분야는 '사이버사령부'에서 실시하고 민간분야는 '인터넷침해대응센터'(KISA)가 담당, 보안업체 및 ISP 등과 협조하고 APCERT·FIRST 등과도 협조, 국제적 대응을 위한 창구역할을 수행한다. 또한 '정보통신기반보호법' 제16조 제1항과 제4항에 의거,[65] 은행분야의 경우, 금융결제원의 금융ISAC에서, 증권분야의 경우 코스콤의 증권ISAC에서, 정보통신분야는 통신정보공유분석협회(TISAA)에서 각각 소관분야별 사고가 발생 시 초동 사고조사는 물론, 피해방지 조치와 함께 복구 등 사고 대응 관련 기술을 지원한다.

3. 사이버위협 경보 및 대응

가. 개 요

사이버위협에 대한 예방 및 대응은 정상 단계에서의 평시 예방활동과 경보발령 단계에서의 대응활동으로 구분한다.

정상 단계는 국내·외에서 신종 웜·바이러스나 해킹기법 및 보안취약점 등이 발견되었으나 그 피해가 미미하여 사이버공간상에서 국가경제·사회 등 제반활동이 정상적으로 이루어지고 있는 상태이다.

경보발령 단계는 사이버위협으로 인해 사고가 발생하거나 피해발생 가능성이 있어 경보를 발령한 상태로서, 사이버위협 수준에 따라 관심·주의·경계·심각의 4단계로 구분한다.

65) 정보공유분석센터(ISAC : Information Sharing & Analysis Center). ISAC 설립의 법적 근거는 '정보통신기반보호법' 제16조 제1항("정보통신기반시설을 보호하기 위하여 다음 각 호 업무를 수행하는 자는 정보공유·분석센터를 구축·운영할 수 있다. 제4항 : 정부는 제1항 각호의 업무를 수행하는 정보공유·분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있다.")이다.

나. 사이버위협 경보

사이버위협 경보체계[66]는 정보통신망에 대한 사이버공격 징후를 포착하였거나 사이버공격 발생이 예상되는 경우, 그 위협 또는 위험의 수준을 평가하여 단계적으로 경보를 발령함으로써 사이버안전을 확보하기 위한 대응체계이다.

사이버위협 경보가 필요한 이유는 각급기관이 경보 수준에 따라 사이버위협에 효과적으로 대처함으로써 사고를 예방하고 피해를 최소화할 수 있다. 또한 사이버위협 경보를 주시함으로써 사이버공격에 의한 피해 확산 및 동일 공격의 재발을 방지한다. 사이버위협 경보 수준에 적합한 대응 요령을 제시, 체계적이고 일관되게 대응하게 함으로써 국가적 혼란과 비효율성을 제거할 수 있다. 그리고 사이버위협 상황을 국민에게 전파함으로써 대국민 경각심 촉구 및 사이버안전 활동에의 참여를 유도할 수 있다.

정부는 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를 발령한다. 경보 발령 절차는 다음과 같다.

국가·공공분야는 국가정보원장, 국방분야는 국방부장관, 민간분야는 방송통신위원장 또는 한국인터넷진흥원 인터넷침해대응센터에서 사이버위협 경보를 발령하며, 국가차원에서의 효율적인 경보 업무를 수행하기 위하여 관련정보를 경보발령 전에 상호 교환한다.

경계 또는 심각 경보를 발령하거나 경보 수준을 조정하는 경우에는 국가안전보장회의 사무처와 사전 협의한다.

국가정보원장은 중앙행정기관의 장에게 경보내용을 전파하고, 각 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장에게 경보내용을 전파한다. 이 경우 국가사이버안전센터는 경보 수준별 대응책 등이 포함된 '사이버위협 경보문'을 홈페이지(http://service.nis.go.kr)에 게시하고, 전자우편, SMS, FAX 등을 통해 각급기관에 전파한다.

66) 국가사이버안전매뉴얼은 2005년에 제정된 이후 개정이 되지 않았다. 따라서 사이버 위협 경고 및 대응과 관련된 조직과 임무가 상당수 변경됨에 따라 현 조직과 직무분장에 맞추어 내용을 정리하였다.

표 14 사이버위협 경보 수준

구분	내 용
심 각 (Red)	o 국가적 차원에서 네트워크 사용 불가능 o 핵심 기반 시설·시스템 대상 피해 발생 o 지역적 · 부분적 피해 발생, 전국적 확산 가능성 증대 o 국가적 차원에서 공동 대처 필요. 즉각 대응 태세 돌입
경 계 (Orange)	o 복수 정보통신 서비스 제공자(ISP)망 또는 기간망에 피해 발생 o 웜·바이러스 등 악성코드의 급속한 확산으로 대규모 피해로 발전 가능성 증가 o 피해가 여러 곳에서 분산 발생하여 다수 기관의 공조 대응이 필요한 경우 대비 계획 점검
주 의 (Yellow)	o 위험도가 높은 웜·바이러스, 취약점, 해킹기법 출현으로 피해 발생 o 네트워크 트래픽이 급격히 증가하여 피해의 범위가 다수 시스템 또는 조직에 해당하는 경우 o 국가 정보시스템 전반에 대한 보안취약점 발견 o 시스템이 악의적 목적으로 도용 ※ 협조 체계 가동
관 심 (Blue)	o 위험도가 높은 웜·바이러스, 취약점, 해킹기법 출현으로 피해 발생 가능성 증대 o 비인가접근, 서비스거부공격 등의 침입시도 흔적 다수 발생 o 해외 피해확산 등 사이버위협의 국내 유입 가능성 증대 ※ 징후 활동 감시

사이버사령부는 각급부대의 부대장에게 경보내용을 전파하고, 인터넷침해대응센터는 민간분야 정보통신 서비스 제공자(ISP)를 대상으로 경보내용을 전파한다.

사이버위협 경보발령시 각급기관은 사고 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 뒤 '경보 대응조치 서식'에 의거 국가정보원에 통보한다.

국가사이버안전센터는 민·관·군 사이버안전 전문기구로부터 사이버공격으로 인한 사고현황 및 조치사항을 통보받아 총괄 관리하고, 범정부차원의 대응이 요구되는 경보(심각단계)의 경우에는 사이버안전 현황을 종합하여 국가사이버안전전략회의에 보고한다.

(1) 경보수준별 대응요령

사이버위협 경보수준은 관심·주의·경계·심각의 4단계로 나뉜다. 각급기관은 국가정보원으로부터 경보발령을 접수한 경우에는 본 장에 수록된 경보수준별 대응요령

을 수행하여야 한다. 단, 예방 및 대비 활동은 경보 등급에 상관없이 항시 수행한다.

(2) 관심단계 대응요령

요주의 웜·해킹기법 및 보안취약점 발표시 모니터링을 강화한다. 새로운 보안취약점이 발표되거나 위험도가 높은 웜·해킹기법에 대한 피해 발생 가능성이 높은 상태이므로 지속적으로 모니터링 하여 피해 발생 여부를 체크하고 위기징후를 감시한다. 해외에서 피해가 확산되는 경우 사이버위협의 국내 유입가능성이 높아지므로 이에 대한 감시를 철저히 한다.

또한 국가사이버안전센터의 보안권고문 등 보호대책을 이행한다. 국가사이버안전센터에서 제공하는 보안권고문은 일정수준 이상의 위험성을 갖고 있는 웜·바이러스, 보안취약점, 해킹기법 등 사이버위협 요소에 대한 특성과 적절한 대응방법을 제공하고 있으므로 이에 따라 보호대책을 이행한다.

그리고 불필요한 서비스를 차단한다. 업무 수행에 반드시 필요한 서비스를 제외한 일반적인 시스템 서비스에 대해서는 해당 프로세스의 실행을 중지시키거나 서비스 포트를 차단하여 취약점에 대한 위협을 최소화한다.

다음으로 라우터, 스위치, 침입차단시스템 차단규칙을 점검한다. 라우터의 CAR(Committed Access Rate), ACL(Access Control List) 설정 내용과 스위치, 침입차단 시스템의 IP주소 또는 포트번호에 대한 허용 및 차단 규칙을 확인한다. 서비스 포트를 허용할 때는 서비스를 제공하는 특정 포트만을 허용하도록 설정하였는지 점검한다.

(3) 주의단계 대응요령

사고발생시 연락체계를 점검한다. 각급기관은 사이버위협 경보 발령 시 업무흐름체계도에 따른 연락체계를 확인한다. 각급기관은 기관 내에서 사용 중인 정보보호시스템, 네트워크 장비 등 시스템 및 프로그램을 제공한 업체 간의 연락체계를 점검한다.

그리고 공격대상 시스템, 서비스포트, 스캐닝활동에 대한 감시를 강화한다. 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 공격대상이 될 수 있는 시스템, 서비스 포트번호 등을 예상한다. 공격대상 시스템의 IP주소 또는 공격대상

서비스 포트번호의 차단 상태를 확인한다. 침입차단시스템, 침입탐지시스템 등을 이용하여 공격대상 시스템, 서비스 포트번호 등에 대하여 모니터링을 강화한다.

다음으로 웜·바이러스, 해킹 등 악성코드의 예상 유입경로를 차단한다. 악성코드의 유입경로가 이메일의 첨부물을 통한 것인지, 웹 사이트의 이동코드를 통한 것인지, 특정한 소프트웨어의 배포를 통한 것인지를 판단한다. 이메일이나 웹을 통해 악성코드에 감염될 경우, 침입차단시스템, 침입탐지시스템, 이메일 서버 및 클라이언트 프로그램, 웹 프록시 서버 등에 차단규칙을 추가한다. 특정 소프트웨어 배포를 통해 악성코드에 감염될 경우 해당 소프트웨어를 설치하여 해지하고 추가적인 설치를 금지한다.

기관별 자체 긴급대응반 가동을 준비한다. 사전에 조직된 위기대처 및 사고대응을 위한 긴급대응반에 대한 비상연락망의 인원 및 연락처를 점검하여 최신내용으로 갱신한다. 마지막으로 긴급대응반원을 비상소집한다.

(4) 경계단계 대응요령

사이버안전 전문기구 전파사항 이행여부를 재확인한다. 사이버안전 전문기구, 정보통신 서비스 제공자(ISP), 백신업체에서 제공하는 사이버위협에 대한 대응요령을 모두 이행하고 있는지 재확인한다.

서비스거부공격 발생시 차단규칙을 재설정한다. 서비스거부공격에 대한 이상 징후를 포착한 경우 정보보안담당관(자)은 신속하게 라우터, 침입차단시스템 등의 차단규칙을 재설정하여 공격의 진행을 차단하여야 한다.

다음으로 중요 자료를 백업한다. 중요 자료를 갖고 있는 서버 및 예상 가능한 피해대상 서버의 자료를 백업하여 네트워크와 단절된 안전한 곳에 보관한다. 공격 IP·포트 등에 대한 모니터링과 시스템 취약점 점검을 강화한다. 악성코드, 취약점, 공격도구 등에 대한 분석정보에 따른 공격대상 시스템의 IP 주소 또는 공격대상 서비스 포트번호의 차단 상태를 수시 확인한다. 침입차단시스템, 침입탐지시스템 등을 이용하여 취약점을 재점검하여 발견된 취약점을 제거한다.

피해발생 가능성이 높은 네트워크는 단절한다. 서비스거부공격 및 웜 발생을 확실하게 예상할 수 있거나 내부 시스템 및 네트워크에 대규모 피해 확산을 예상할 수

있는 경우, 기관장의 승인을 받고 물리적인 케이블 분리 등을 통해 피해대상 네트워크를 단절한다.

기관별 자체 긴급대응반을 가동한다. 피해가 예상되거나 피해상황 추이에 따라 긴급대응반을 투입, 즉각적인 시스템복구를 실시하고 피해확산 차단조치를 취한다.

(5) 심각단계 대응요령

민·관·군 합동조사팀과 복구지원팀의 임무수행을 지원한다. 합동조사팀은 사이버위협에 대한 철저한 원인 분석을 통해 피해규모 및 적절한 대응 방법 등을 제시하고 복구지원팀은 사이버위협에 대한 피해를 최소화하기 위해 임무를 수행한다. 피해를 당한 해당 기관의 정보보안담당관(자)은 사고와 관련된 데이터뿐만 아니라 데이터백업 및 로그관리 등 사고조사 및 복구에 필요한 자료를 제공한다.

경보발령 공격대상 서비스 포트를 차단한다. 악성코드, 취약점, 공격도구 등에 대한 분석정보가 발표될 경우, 라우터에서 CAR조정 및 ACL을 추가설정 하거나 스위치 및 침입차단시스템의 차단규칙을 추가설정 하여 공격대상 서비스 포트를 차단한다.

서비스거부공격 등에 의한 대규모 피해발생 가능성이 높아질 경우, 사전에 해당 공격에 관련된 패킷차단 협조를 가입한 정보통신 서비스 제공자(ISP)에 요청한다.

피해발생 가능성이 높은 네트워크를 단절한다. 서비스거부공격 및 웜 발생을 확실하게 예상할 수 있거나 내부 시스템 및 네트워크에 대규모 피해 확산을 예상할 수 있는 경우, 기관장의 승인을 받고 물리적인 케이블 분리 등을 통해 피해대상 네트워크를 단절한다.

기관내 PC 사용 최소화를 권고한다. 기관내 PC 사용을 최소화하여 만약에 발생할 수 있는 잠재적인 사고를 미연에 방지한다.

다. 평시 예방활동

(1) 평시 업무흐름 체계

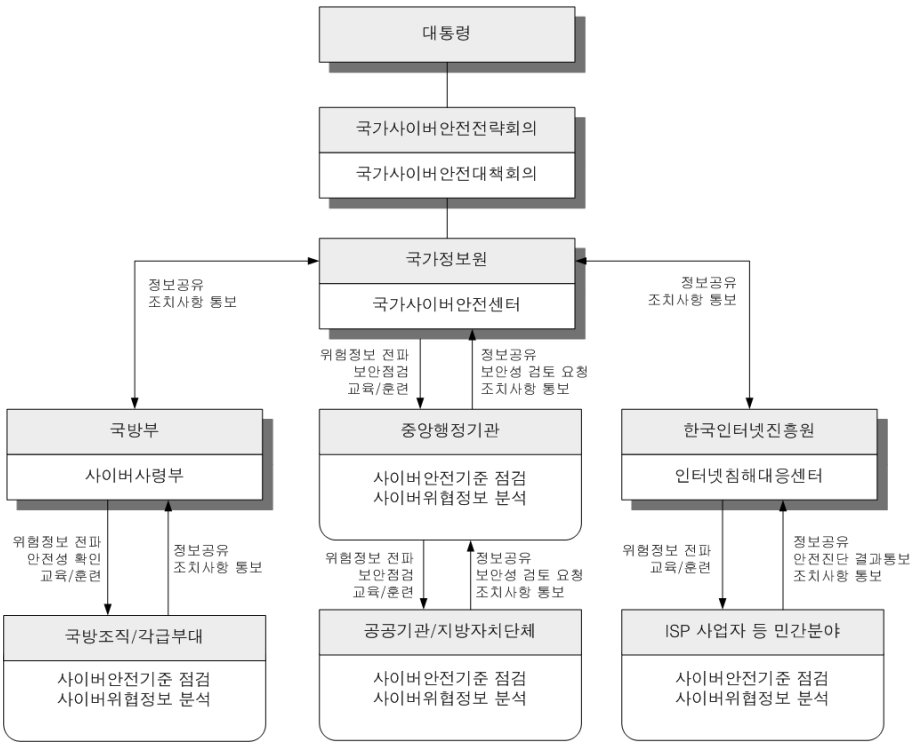


그림 4 **평시 업무흐름 체계도**

평시 민·관·군 분야별 주관기관[67] 및 사이버안전 전문기구[68]는 다음의 임무를 수행한다. 분야별 주관기관은 소관분야 실정에 맞는 보안관리 기준을 수립한다. 국가정보원과 국방부는 사이버안전대책의 이행여부 등 소관분야 정보통신망에 대한 안전성을 확인한다. 방송통신위원회는 정보통신서비스와 집적정보통신시설을 대상으로 안전진단을 실시한다.

국가정보원은 중앙행정기관의 정보통신망 안전성을 확인할 수 있고, 지방자치단체

67) 분야별 주관기관 : 국가정보원, 국방부, 방송통신위원회.

68) 사이버안전 전문기구 : 보안관제, 침해사고대응, 정보공유분석 등 사이버안전 업무를 전담하는 기구.

및 공공기관의 정보통신망에 대한 안전성 확인은 관계 중앙행정기관의 장과 협의하여 수행할 수 있다. 각 분야 사이버안전 전문기구는 24시간 사이버공격 및 위협 징후 감시, 침해사고대응, 정보공유분석 등의 업무를 수행한다.

평시 각급기관은 다음의 임무를 수행한다. 각급기관의 장은 사이버위협으로부터 관할 정보통신망의 보호를 위해 정기적으로 보안점검을 시행한다. 각급기관은 정보통신망 신·증설 등 정보화 사업 추진 시 자체 보안대책을 강구하고 국가정보원에 보안성 검토를 의뢰한다. 각급기관은 대규모 사이버공격 발생 시 신속하고 효과적으로 대응하기 위하여 정보보안 전문인력으로 자체 긴급대응반을 구성한다. 각급기관의 장은 보안실무자로부터 국가 사이버안전에 위협을 초래할 수 있는 정보를 보고받은 경우, 관련 사항을 국가사이버안전센터로 신속하게 통보한다.

(2) 예방활동

국가정보원은 중앙행정기관과 소속 및 산하기관에서 활용 가능하도록 보안관리 기준을 포함한 '국가사이버안전매뉴얼'을 작성하여 배포한다. 중앙행정기관은 국가사이버안전매뉴얼을 바탕으로 해 기관의 실정에 맞게 보안관련내규(지침)에 반영하거나 소관분야 안전대책을 수립하고, 이를 소속 및 산하기관에 배포하여 사용토록 한다. 중앙행정기관의 소속 및 산하기관은 관계 중앙행정기관의 보안관련내규(지침) 또는 안전대책에 따라 자체 안전대책을 수립·시행한다. 중앙행정기관은 소관분야 보안관련내규(지침)를 제·개정하거나 안전대책을 수립한 경우에는 국가정보원에 그 1부를 통보하여야 한다.

안전성 확인 및 정기점검 시행과 관련하여 중앙행정기관은 자체 수립한 안전대책에 따라 소관분야 정보통신망에 대한 안전성과 안전대책 이행여부에 대해 정기점검을 실시한다. 소속 및 산하기관은 자체적으로 정보통신망에 대한 안전대책의 적절성 여부 등에 대해 정기적으로 점검을 실시한다. 국가정보원은 관계 중앙행정기관과 협의하여 사이버안전대책 이행 여부와 정보통신망의 안전성을 확인한다.

안전성 확인의 시정 조치와 관련해서 국가정보원은 각급기관에 대한 정보통신망의 안전성과 안전대책 이행여부에 대해 확인을 실시한 경우에 필요한 시정조치를 권고할 수 있다. 해당 중앙행정기관은 국가정보원이 제시한 시정 권고사항에 대해 조

속히 조치를 취하고, 그 결과를 국가정보원장에게 통보한다. 국가정보원은 관계 중앙행정기관과 협의하여 시정권고 사항에 대한 이행 여부를 확인할 수 있다.

(3) 위협정보 수집·분석 및 전파

위협정보 공유체계 구축을 위하여 국가정보원은 국가차원의 사이버위협을 총괄 수집·분석·전파하는 체계를 구축 운영한다. 각급기관은 국가차원의 사이버위협 정보가 종합될 수 있도록 사이버위협 정보수집 시스템의 연동을 지원한다. 국가정보원은 사이버위협 정보수집 시스템을 연동한 기관을 대상으로 보안관제 정보공유 등을 위해 협의체(회의체)를 운영한다.

사이버위협 정보 수집을 위하여 국가사이버안전센터는 사이버위협 정보 또는 이상징후 정보 등과 같은 다양한 위협정보를 수집하기 위해 국가 주요 전산망을 대상으로 24시간 사이버공격 및 위협 징후를 모니터링 한다. 국방분야는 사이버사령부, 민간분야는 인터넷침해대응센터가 담당 보안관제를 통한 위협감시와 함께 국가정보원은 국내외 다양한 경로를 통해 오프라인 상의 사이버위협에 대한 정보를 파악한다.

각급기관은 보안관제시스템 또는 오프라인 등을 통해 사이버위협 정보를 인지한 경우에는 초동조치 후 국가사이버안전센터에 신속히 통보한다. 국가사이버안전센터는 분야별 수집된 통계자료를 기반으로 분석한 후에 그 결과를 관계기관에 정기적으로 전파한다.

사이버위협 정보 대응책 작성·배포를 위하여 국가정보원은 국가·공공기관에서 많이 사용되는 프로그램에 대한 보안취약점이 발표되거나, 웜·바이러스 출현 시에는 '보안권고문' 또는 '취약점 분석정보'를 작성하여 배포한다. 정부는 국가의 사이버안전을 위해 필요한 경우 민·관 합동으로 전용백신 또는 보안프로그램을 제작하여 배포한다. 각급기관은 보안권고문 또는 취약점 분석정보를 바탕으로 보안업데이트 및 대응조치를 수행하고, 기관 내부에 배포한다.

사이버위협 인지 또는 사고 발생시 신고 및 조사를 위하여 각급기관은 국가사이버안전센터와 위협정보 전파 및 사고신고 연락체계를 구성하여 유지해야 한다. 사고 발생 시에 각급기관은 국가사이버안전센터 홈페이지의 '사이버침해사고 신고' 메뉴를 이용하거나 국가사이버안전센터에 통보한다.

국가 기밀문서가 저장된 정보시스템에 해킹 사고가 발생했을 경우에는 의무적으로 신고해야 한다.

(4) 사이버안전 관련기관과 정보공유

사이버안전 전문기구와의 정보공유 및 공조체계를 위하여 국가사이버안전 정책 수립 및 제도 개선 등을 협의하기 위해 관련회의를 운영한다. 국가사이버안전전략회의는 년 1회 이상, 국가사이버안전대책회의는 년 2회 이상(상·하반기), 국가사이버안전실무회의는 월 1회 이상 개최한다. 각급기관은 국가사이버안전전략회의 및 대책회의 위원으로 참여하거나 상정안건이 있는 경우에는 국가정보원과 협의한다. 국가정보원은 사이버안전 전문기구와 협력체계를 유지하고 관계전문가 회의를 개최한다. 사이버안전 전문기구 현황은 다음과 같다.

표 15 사이버안전 전담조직 현황

구 분	기 능	전 담 조 직	소 관 분 야
주관 기관	보안관제 · 침입사고대응 · 정보공유분석	국가사이버안전센터 (국가정보원)	국가공공
		사이버사령부 (국방부)	군
		인터넷침해대응센터 (한국인터넷진흥원)	민간
유관 기관	부문별 보안관계	전자정부통합관제센터 (행정자치부)	전자정부
		과학기술정보보호센터 (과학기술부)	과학기술
		금융결제원	은행
		한국증권전산	증권
수사 기관	사이버범죄 수사	사이버테러대응센터	경찰청
		인터넷범죄수사센터	대검찰청

수사기관은 수사과정에서 다음의 경우에는 국가정보원에 관련자료를 제공, 보

안대책 수립과 보안조치를 강구토록 지원한다. 침해사고 경유지 또는 피해범위에 국가·공공기관이 포함되거나, 피해가 국가 전반에 걸쳐 파급될 가능성이 있다고 판단되는 사건을 조사한다.

외국의 사이버범죄 수사기관 등으로부터 국가·공공기관의 정보통신망에 대한 침해사고와 관련되어 공조수사를 요청받은 사건이나 외국의 수사기관에 공조수사를 요청한 사건을 조사한다.

국가정보원과 각급기관 간의 정보공유를 위하여 국가정보원은 국가·공공기관 정보보안담당관(자)에게 사이버위협 정보를 제공하기 위해 '정보공유시스템'(http://is.ncsc.go.kr)을 운영한다. 정보공유시스템은 보안뉴스, 보안권고문, 웜·바이러스 정보, 사고처리 결과 및 통계 등 제공한다. 각급기관의 정보보안담당관(자)은 정보공유시스템에 가입하고 관련정보를 주기적으로 확인한다. 가입 시에는 정보공유시스템 이용신청서를 국가사이버안전센터에 제출한다.

(5) 정보통신망에 대한 보안성 검토 및 보안측정

정보통신망 보안대책 수립 및 보안성 검토와 관련하여 각급기관은 정보통신망 신·증설 등 정보화 사업을 추진하는 경우 자체적으로 보안대책을 수립한다. 각급기관은 자체 수립한 보안대책의 적절성 여부에 대해 국가정보원에 보안성검토를 요청한다. 국가정보원은 각급기관이 요청한 보안대책에 대한 보안성을 검토하여 적합한 대책을 제시한다.

정보통신 안전진단 및 보안측정의 실시를 위하여 국가정보원은 국가·공공기관의 정보통신망 및 국가보안목표시설에 대한 보안측정을 실시한다.

(6) 사이버안전에 대한 교육 홍보 및 훈련 등

각급 기관은 사이버위협에 대비하여 정기적인 교육 및 훈련을 통해 소속직원의 보안의식을 제고하고, 보안관리 요령을 전파한다.

국가정보원은 각급기관 정보보안담당관(자)을 대상으로 국가 정보보안 설명회를 실시하고, 사이버안전관련 전문기술 전수를 위해 국가정보대학원에 사이버테러 대응 관련 교육과정을 개설·운영한다.

대국민 보안의식 제고를 위하여 산·학·연의 연계를 통하여 정보보호 전문인력 양성을 촉진하고 보안관련 캠페인을 통하여 대국민 보안의식을 고취시키기 위해 노력한다. 국가정보보안협의회, 한국정보보호학회, 한국사이버테러정보전학회, 정보보호실천협의회 등 단체를 적극 활용하여 사이버안전에 대한 인식을 제고시킨다.

사이버공격 대응훈련과 관련하여 국가정보원은 사이버공격 발생 시 효율적으로 대응하기 위해 범국가적 차원의 사이버전 모의훈련을 실시한다. 사이버전 모의훈련은 경보발령 상황접수 및 전파, 침투공격 및 방어, 메일 열람, 사고신고 및 조치 등 사이버안전업무 전반을 대상으로 하며, 모의훈련용 측정기술은 개발계획을 수립하여 확보한다. 국가정보원은 비상기획위원회, 국가안전보장회의사무처, 국방부 등과 협의하여 모의훈련 기간·대상기관·훈련방법 등 범정부적 모의훈련 계획을 수립하고 시행한다. 각급기관은 사이버전 모의훈련을 통해 발견되지 않았던 새로운 취약점이나 관리가 허술했던 부분을 찾아내고 이를 보완하기 위하여 적극 협조한다. 각급기관은 당해 기관의 보안취약성을 진단하기 위해 필요한 경우 국가정보원에 수시 모의훈련 실시를 요청할 수 있으며, 국가정보원은 특별한 사정이 없는 한 이에 적극 협조한다.

(7) 기본점검 활동

사이버위협 동향 파악을 위하여 국가사이버안전센터 등 사이버안전 전문기구 및 보안업체의 홈페이지를 수시방문, 관련내용을 파악한다. 또한 국내외 언론의 사이버위협 관련 보도를 주시한다.

그리고 주요 정보시스템을 정기적으로 점검한다. 웹서버, 메일서버 등의 정보시스템이 정상적으로 운영되는지 또는 불법침입자에 의한 중요 데이터의 파괴 및 위·변조가 발생되었는지 여부를 정기적으로 점검한다. 업무와 관련 없는 P2P 등의 인터넷 연결 프로그램 사용 자제한다. P2P 등의 파일공유프로그램은 웜이나 트로이목마 등과 같은 악성프로그램을 전파할 가능성이 있으므로 가급적 사용을 자제하도록 한다.

백신 탐지 패턴 및 소프트웨어 보안패치 업데이트를 실시한다. 악성프로그램의 특성은 계속적으로 변하기 때문에 백신프로그램의 엔진은 항상 최신버전으로 업데이트한다. 사용 중인 소프트웨어의 보안패치사항이 발표된 경우 해당패치를 수행하여 취약점을 최소화하도록 노력한다.

네트워크 트래픽량 변화를 모니터링한다. 라우터, 침입탐지시스템 등을 이용하여 트래픽량이 급증하는지를 지속적으로 모니터링한다. 네트워크 트래픽량 모니터링을 통해 서비스거부 공격, 웜 확산 등의 이상 징후 발생 여부를 관찰한다.

출처가 불분명한 이메일은 삭제한다. 출처가 불분명한 이메일을 통해 웜·바이러스가 감염될 우려가 있으므로 의심되는 이메일은 열지 않고 삭제한다. 사용자가 이메일의 미리보기만 하더라도 악성코드가 사용자 PC에 사용자도 모르는 사이에 설치될 우려가 있으므로 미리보기 기능을 삭제한다.

폴더 및 파일 공유 사용을 자제한다. 자료 교환 등을 위해 사용하는 컴퓨터 폴더 및 파일 공유를 통해 사이버공격이 발생될 우려가 있으므로 폴더 및 파일 공유 사용을 지양한다. 복잡한 패스워드를 사용하고 주기적으로 변경한다. 컴퓨터의 불법적인 접근을 방지하기 위해 유추하기 힘든 복잡한 패스워드를 사용하며, 반드시 특수문자를 포함하도록 한다. CMOS 패스워드, 계정 패스워드, 화면보호기 패스워드, 공유 패스워드, 네트워크 접근 등 컴퓨터에서 사용하는 패스워드는 월 1회 이상 주기적으로 변경한다.

4. 사고조사 및 복구

가. 사고조사 및 복구체계

사고조사라 함은 사이버공격으로 인해 발생한 정보통신망 보안사고 또는 사이버안전사고의 원인을 분석하고 피해범위 확인 및 재발방지 대책을 수립하기 위한 일체의 행위이다.

사이버위협 경보가 심각 수준으로 발령된 경우에는 범정부적으로 구성된 합동조사팀·복구지원팀과 연계하여 사고조사 및 피해복구를 수행하며, 해당기관의 장은 이에 필요한 인력 및 관련 자료를 지원한다.

자체적으로 사고원인 규명, 공격자 추적, 공격 증거확보 등의 조사를 실시하거나 피해를 복구할 때에는 절차에 따라 실시하며 사고조치결과를 작성·유지한다. 사고조사 결과, 범죄 혐의가 있다고 판단되는 경우 해당기관의 장은 국가정보원장에게

통보하고 국가정보원장은 해당기관의 장과 협의하여 수사기관장에게 통보한다.[69]

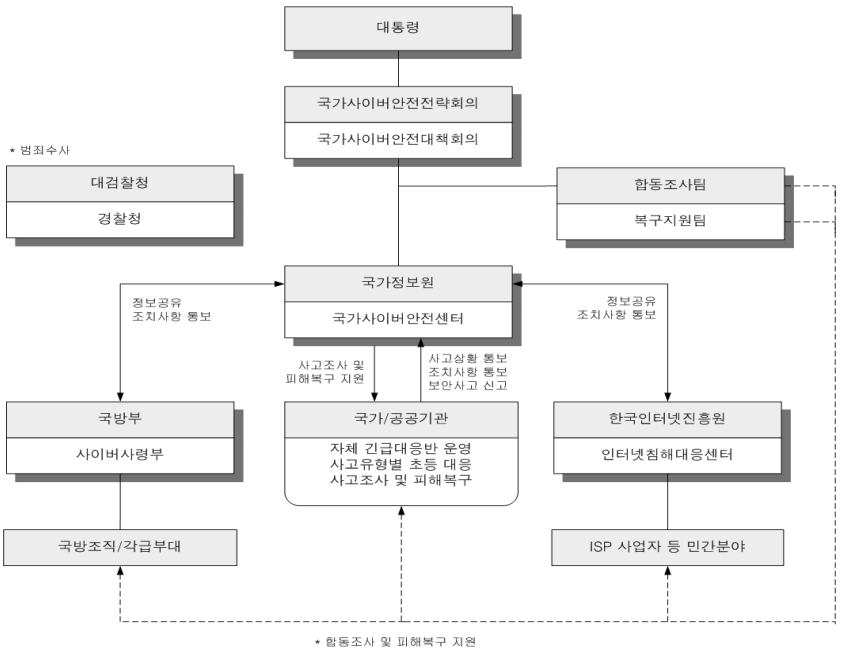


그림 5 사고조사 업무흐름 체계도

표 16 사고조사 및 복구체계

단계	수행	내용
1단계	사고신고 초동대응	사고신고 및 초동대응
2단계	증거확보 및 보존	증거자료 백업
3단계	사고조사	공격유형별 사고조사 : 원인 규명 및 공격근원지 추적 필요시 합동조사팀 연계 조사 범죄혐의여부 판단 : 필요시 수사기관(사이버범죄수사센터, 사이버테러대응센터) 연계 조사
4단계	피해복구	피해복구
5단계	보고서 작성	사고 조치결과 통보 : '사고처리결과보고서' 작성 '사고처리결과보고서'는 초동조치, 증거확보, 사고조사, 피해복구결과, 합동조사 및 피해복구팀 연계 조사내용을 기술

69) 기술적인 사고조사 방법과 관련하여 '부록 3. 사이버침해 사고 예방 및 대응 기법' 참조.

나. 사고조사 및 복구 요령

(1) 사고 신고

1) 보안사고가 발생한 기관의 장 또는 사고를 범하였거나 이를 인지한 자는 지체 없이 사고의 일시·장소·사고내용 및 현재 취하고 있는 조치를 국가정보원에 통보하여야 한다.
2) 각급기관의 장은 정보보안사고가 발생한 때에는 즉시 피해를 최소화하도록 조치를 취하고 이를 국가정보원장에게 통보하여야 한다.
3) 정보통신보안 사고 발생 시에는 사고일시 및 장소, 사고개요, 사고자 및 관계자의 인적사항과 함께 조치내용을 통보한다.
4) 사이버 침해사고와 관련해서 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체 없이 그 사실을 국가정보원장에게 통보하여야 한다.
5) 중앙행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체 없이 그 사실을 국가정보원장에게 통보하여야 한다. 다만 국방분야의 경우에는 관련 내용을 국방부장관에게 통보하고, 국방부장관은 국가안보에 필요하다고 판단되는 경우에는 관련내용을 국가정보원장에게 통보하여야 한다.
6) 공공기관 및 지방자치단체의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 관계 중앙행정기관의 장에게 통보하고, 관계 중앙행정기관의 장은 이를 지체 없이 국가정보원장에게 통보하여야 한다.
7) 국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우 관계 중앙행정기관의 장에게 관련 사실을 통보하고 사고조사를 실시한다.

(2) 사고조사의 실시

1) 국가정보원장은 각급기관에서 발생한 비밀의 누설 또는 분실과 국가중요시설 및

장비의 파괴, 보호구역에 대한 불법침입 등 보안사고에 대하여 전말조사를 실시한다.

2) 보안사고 전말조사는 각급기관의 업무용 PC에 불법침입이 발생하여 대외비 이상의 비밀자료가 유출된 경우에도 해당된다.
3) 보안사고는 이에 대한 전말조사가 종결될 때까지 공개하여서는 아니된다.
4) 국가정보원장은 정보통신보안사고가 발생한 때에는 사고조사를 실시한다. 다만, 경미한 사고의 경우에는 해당 기관의 장에게 사고조사를 위임할 수 있다.
5) 국가정보원장은 국가·공공기관에 대한 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 해당기관의 장이 자체적으로 조사하게 할 수 있다.
6) 국가·공공기관에 대한 사이버공격이 ① 대외비 이상의 비밀자료를 입력, 출력, 열람에 활용되거나 과거에 활용된 이력이 있는 업무용 PC에 저장된 자료유출을 목적으로 하는 사이버공격, ② 대외비 이상의 비밀자료를 입력, 출력, 열람하는 업무를 현재 수행 또는 과거에 수행했던 공무원 또는 임직원의 업무용 PC에 저장된 자료유출을 목적으로 하는 사이버공격에 해당되는 경우 보안사고에 준하여 사고조사를 실시한다.
7) 국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있다.
8) 국가정보원장은 사고조사 시 원인 분석을 위하여 필요하다고 인정하는 때에는 국가·공공기관의 장에게 정보통신망의 접속기록 등 관련 자료의 제공 및 피해시스템에 잔존한 해킹프로그램의 채증 등 증거확보를 요청할 수 있으며, 이 요청 절차는 그 취지에 대한 구두설명 또는 그 취지가 요약된 전자우편으로 갈음할 수 있다.
9) 요청받은 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.
10) 국가정보원장은 직무를 수행함에 있어서 필요한 협조와 지원을 관계 국가기관 및 공공단체의 장에게 요청할 수 있다.
11) 공공기관의 컴퓨터에 의하여 처리되는 개인정보 중 국가안전보장과 관련된 정보분석을 목적으로 수집 또는 제공요청되는 개인정보의 보호에 관하여는 동법을

적용하지 아니한다.

12) 사고조사에 대한 실무 지원은 국가·공공기관의 정보보안담당관 또는 정보보안 실무자가 수행하는 것을 원칙으로 한다.

13) 국가정보원장은 교육기관에 발생한 사고에 대하여 사고조사 업무의 전부 또는 일부를 국가보안기술연구소장에 위임할 수 있다. 이 경우 당해 교육기관의 장은 특별한 사유가 없는 한 국가보안기술연구소가 수행하는 사고조사에 협조하여야 한다.

14) 국가정보원장 또는 국가보안기술연구소장은 제출받은 자료 및 조사를 통하여 알게 된 정보를 사고의 원인분석 및 대책마련 외에는 이를 사용하지 못하며 사고조사가 종료된 후에는 즉시 파기하여야 한다.

15) 정보통신망운용기관의 장은 사이버 경보가 발령되었을 때에 경보발령과 관련된 사고 대응을 위해 긴급대응반을 운영할 수 있다.

16) 정보통신망운용기관의 긴급대응반장은 사이버공격으로 인한 사고의 발생 또는 징후 발견 시 피해 최소화 조치를 취해야 한다.

17) 각급기관의 긴급대응반장은 정보보안담당관이 겸임하는 것을 원칙으로 한다.

18) 국가·공공기관의 긴급대응반장은 정보보안담당관이 겸임하는 것을 원칙으로 하며, 긴급대응반원은 정보보안실무자를 중심으로 편성한다.

19) 국가정보원장은 사이버공격으로 인하여 국가·공공기관에 발생한 사고에 대하여 경미한 사고라고 판단되는 경우에는 해당기관의 장이 자체적으로 조사하게 할 수 있으며, 해당 기관의 장은 정보보안담당관 또는 긴급대응반장으로 하여금 자체 사고조사를 수행하게 할 수 있다.

20) 국가·공공기관의 장은 자체 사고조사를 완료한 후 사고대응조치 서식에 의하여 사고조치결과보고서를 작성, 유지하고, 사본 1부를 국가정보원장에게 통보한다.

21) 정보통신서비스제공자 등 정보통신망을 운영하는 자는 침해사고가 발생한 때에는 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다.

(3) 범정부 합동조사 및 복구지원팀

1) 국가정보원장은 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우에는

관계 중앙행정기관의 장과 협의하여 범정부적 합동조사 및 복구지원팀을 구성·운영할 수 있다.

2) 국가정보원장은 합동조사 및 복구를 위하여 관계 중앙행정기관의 장에게 필요한 인력 및 관련 자료의 지원을 요청할 수 있다.
3) 합동조사 및 복구지원팀은 국가정보원, 국방부, 방송통신위원회 소속 공무원으로 구성하되 필요시 대검찰청과 경찰청 소속 공무원 및 산·학·연 정보보호전문가를 참여시킬 수 있다.
4) 각 분야별 합동조사 및 복구지원팀의 주관은 국가정보원(공공), 국방부(국방), 방송통신위원회(민간)가 담당하며, 복수분야에서 발생된 사고에 대해서는 국가사이버안전대책회의에서 주관을 담당할 기관을 결정한다.
5) 국가정보원은 간사기관으로 합동조사 및 복구지원팀 운영을 총괄 지원하고, 조사결과를 국가사이버안전대책회의 및 전략회의에 보고한다.

(4) 수사와의 관계

1) 국가정보통신망에 대한 사이버공격과 관련한 수사사항에 대하여 해당 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 해당 정보를 국가정보원장에게 통보하여야 한다. 이 경우 수사결과를 대외에 공표시 사전에 국가정보원장과 협의하여야 한다.
2) 국가정보원장은 사이버공격으로 인하여 국가·공공기관에 발생한 사고에 대하여 조사한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다.

(5) 사고 조사결과

1) 국정원장은 보안업무규정에 의한 전말조사를 실시한 경우 그 결과를 해당기관의 장에게 통보한다. 조사결과를 통보받은 기관의 장은 조사결과에 대하여 필요한 조치를 하여야 한다.
2) 정보통신보안 사고관련자는 보안업무규정의 징계기준에 의거 징계토록 하며, 징계결과에 대해 국정원장에게 통보하여야 한다.

3) 국가정보원장은 관련정보를 제공받은 경우에는 대응에 필요한 조치를 강구하고 그 결과를 정보를 제공한 해당기관의 장에게 통지한다.
4) 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통함에 있어서는 위조·변조·훼손 또는 유출 방지를 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 한다.
5) 국가정보원장은 보안사고의 전말 조사결과에 의하여 비밀의 효력의 정지 또는 취소 등의 필요한 조치를 취한다.

표 17 증거확보 및 보존요령

단계	수행	내 용	
1단계	증거자료 백업	피해 장비(컴퓨터)의 백업파일 생성 : 로그자료, 프로세스 정보, 네트워크 연결상태, 파일 시스템 정보 주의사항 : 피해 장비의 전원차단 실시 등 운영 장비 정지로 사고원인의 증거 발견이 불가능해지지 않도록 주의해야 한다.	
2단계	컴퓨터 하드웨어 파악	윈도우 시스템	'내 컴퓨터' 등록정보를 이용, 하드웨어 정보파악
		유닉스/리눅스 시스템	dmesg 명령어 이용, 하드웨어 정보파악
3단계	해당 S/W 파악	윈도우 시스템	제어판의 프로그램 추가/삭제 기능을 통해 시스템에 설치된 프로그램 현황을 파악 주의사항 : 레지스트리(Registry) 정보를 통해 세부 사항도 확인해야 한다.
		유닉스 시스템 리눅스 시스템	운영체제에 맞는 명령어를 사용하여 파악 Linux : RPM (RedHat Package Manager) 명령 실행 Solaris(SUN O/S) : pkgadd, pkgrm, pkginfo 명령 실행 HP-UX : swinstall 명령 실행 SCO OpenServer : pkgadd, pkgrm, custom 명령사용 FreeBSD : pkg_add, pkg_delete, pkg_info 명령사용
4단계	파일목록 작성 및 조사	윈도우 시스템	모든 파일의 검색 : 모든 파일을 볼 수 있도록 검색옵션을 선택하고 탐색기를 사용하여 전체 파일 현황을 파악 특정 파일의 검색 : 특정 파일을 볼 수 있도록 검색옵션을 선택하고 탐색기를 이용, 특정 파일 현황을 파악
		유닉스 시스템 리눅스	모든 파일의 검색 'ls' 명령어를 사용하고 '-a' 또는 '-al' 옵션을 사용하여 전체 파일의 목록 확인

단계	수행	내 용	
		시스템	특정 파일의 검색 'find' 명령어를 사용하여 특정파일의 위치를 확인
5단계	증거자료 추출	증거자료 백업매체 : '원본'과 동일한 형태, 동일 모델로 보관 증거자료 추출분석 : 원본 같은 이미지 복사본을 사용 하드웨어적 이미지 복사 : Encase등과 같은 하드디스크 복사기로 복사 (고가의 정밀수사에 사용) 소프트웨어적 복사 : '고스트' 프로그램 사용 증거자료 분석환경 : 컴퓨터 범죄 환경과 동일하게 준비 (예 : 동일 환경의 하드웨어 준비 등)	
6단계	증거자료 분석확보	일반적 문서파일 : 특정 키워드가 포함된 문서 검사 회계 파일 : 사용한 회계용 프로그램 파일 분석 DB 파일 : 원본 DB 무결성 검사, DB 구조, 테이블 구성 조사	

(6) 사이버공격 유형별 사고조사 요령

1) 악성코드 분석 및 추후 사고조사를 위해 악성코드 사본을 수집하여 보존한다.
2) 수집된 악성코드를 국가사이버안전센터에 통보한다.
3) 사후 법적 증거로 활용하거나 상황보고 및 사고 처리 활동에 대한 사후 검토를 위해 악성코드로 인한 사고 발생시 대응요령 수행 내역에 대한 기록을 유지한다.
4) 스니퍼와 같은 트래픽 분석 도구를 이용하여 감시되는 트래픽으로 부터 공격 근원지를 식별한다.
5) 라우터의 트래픽 분석기능과 스위치의 MAC 주소 테이블을 이용하여 서비스거부 공격의 공격자를 추적한다.
6) 정보통신 서비스 제공자(ISP)에게 공격자 추적을 요청한다.
7) 서비스거부공격이 호스트를 손상시킨 방법을 파악한다.
8) 시스템 및 네트워크의 대량 로그 엔트리를 분석한다.
9) 피해시스템과 동일 IP대역을 사용하고 있는 컴퓨터의 로그를 조사한다.
10) MRTG와 같은 네트워크 트래픽 모니터링 도구를 이용하여 복구활동이 시작되기 전까지 꾸준한 네트워크 모니터링을 실시한다.
11) 네트워크 모니터링으로 후속 공격 발생시, 서비스거부공격 발생시 대응요령을 이용하여 공격자를 추적하고 추가적인 증거를 확보한다.
12) 침입탐지시스템, 침입차단시스템, 피해시스템의 로그 등과 같은 사고 관련 로그

및 증거 자료를 확보한다.

13) 침입사실을 확인하기 위하여 lsof(유닉스용) 또는 fport(윈도우즈용)와 같은 도구를 이용하여 열려진 포트와 매칭하는 프로세스를 찾아낸다.

14) 사고기간 중 전산실, 사무실 등의 출입통제시스템의 로그를 확보한다.

15) 복합구성공격에 의하여 사고가 발생한 경우 일어난 사고 각각에 대해 사고조사를 수행한다.

표 18 피해복구 절차

단계	수행	내 용	
1단계	피해복구 범위결정	단순데이터 복구	피해사고가 발생한 시스템의 데이터만 손상이 발생
		소프트웨어 복구	피해사고가 발생한 시스템의 프로그램 및 운영체제에 단순 오류 발생
		시스템 재설치	피해사고가 발생한 시스템의 운영체제에 복구 불가능한 심각한 오류 발생
		하드웨어 교체	피해사고가 발생한 시스템의 하드웨어의 손실 발생
2단계	피해복구 우선순위 결정	피해복구 대상 시스템이 두개 이상인 경우, 이들 대상에 대한 복구 우선 순위화 즉시 조치해야 할 복구 내용과 중장기적인 계획에 의해서 수행해야 할 복구 내용 결정	
3단계	피해 복구	단순데이터 복구	피해사고 발생 전에 백업하였던 데이터로 복구
		소프트웨어 복구	백신 프로그램을 이용한 악성코드 탐지 및 치료 SW 패치를 이용한 공격에 이용된 취약점 제거 응용프로그램 재설치 운영체제 CD를 이용한 운영체제 복구
		시스템 재설치	운영체제 CD를 이용한 운영체제 재설치 필요한 응용프로그램 설치 먼저 백업한 자료를 이용한 데이터 복원 시스템을 완료 후 정상상태 복귀 확인
		하드웨어 교체	파손된 하드웨어 부품 교체
4단계	사후 관리	시스템 재개 후 일정기간 동안 모니터링 재개 피해복구에 관한 보완 보고서 작성 및 일정기간동안 시스템 및 네트워크의 주기적인 재점검 사건처리에 대한 회의 개최 책임부과 여부 검토	

5. 향후 과제

가. 국가 사이버안전 관련 법제 정비 필요성과 방향

지금 우리는 인터넷으로 대표되는 유무선 네트워크 사회 속에서 살고 있다. 이러한 현상은 농업혁명, 산업혁명에 이어 가히 정보통신혁명이라 부를 수 있을 만큼 현재를 살고 있는 우리에게 많은 긍정적 영향을 끼치고 있다. 반면, 정보통신혁명은 우리에게 '사이버공간'(cyberspace)이라는 새로운 개념적 공간과 '현실세계'(real world)와의 상호연관성을 더욱 강하게 하고 있으며, 이러한 상호연관성으로 말미암아 사이버공간에 대한 침해행위가 현실세계에 대한 치명적인 위협요소로 작용할 수 있는 개연성을 낳고 있다.

1996년부터 국가경쟁력 제고를 위하여 정보화를 추진한 결과, 우리나라는 세계 최고 수준의 정보통신인프라를 구축하고 국가 사회 전반의 정보화 추진 및 IT산업의 국가 주력산업 등장 등 정보강국의 지위를 확보할 수 있게 되었다. 그러나 사이버공간의 새로운 위협요소에 대해서는 단편적이고 산발적인 법규정만으로는 대응하기 어려운 문제점도 나타나게 되었다. 그래서 이러한 사이버공간의 침해행위가 가지는 위협성에 대하여 국가차원에서 보다 효율적으로 대응하기 위하여 2001년부터 '정보통신기반보호법'이 제정·시행하고 있지만, 지난 2003년 1월 25일 발생한 인터넷 침해사고를 통하여 기존의 주요 정보통신기반시설 중심의 사이버테러 대응체계의 미비점 및 새로운 체계 정비의 필요성을 인식하게 되었고, 국가안전보장의 확보라는 새로운 각도에서 국가차원의 사이버테러 대응체계의 구축·운영방향을 모색하게 되었다. 그 결과, 국가안전보장회의를 중심으로 하는 '국가사이버테러대응체계'를 구축하게 되었고, 이를 위해 '사이버안전정책조정회의'가 국가안전보장회의(NSC) 산하에 신설되었으며, 범 국가차원에서 사이버테러에 체계적으로 대응하기 위하여 '국가사이버안전센터'가 설립되었다. 또한, 민간부문과 국방부문의 사이버테러 대응을 위하여 '인터넷침해대응센터'와 '사이버사령부'가 설립되었다.

이번에 마련된 대응체계의 핵심은 사이버공간을 침해하는 위협요소로부터 국가사이버안전을 확보하기 위하여, 사이버테러 대응을 위한 상설기구를 설치하고, 대응기구 및 관련기관 사이에 정보를 공유하며 이를 국가사이버안전센터를 통하여 종합·

분석·판단하게 하는 것이다. 그리고 국가차원의 예·경보를 내림으로써 외부로부터의 사이버공격을 예방하고, 피해발생시 관련기관 합동으로 피해에 대한 신속한 복구 및 효율적 지원을 가능하게 한 것이라는 점이다. 다만 이번에 구축된 국가 사이버테러 대응체계는 관련 조직과 기능의 정비라는 측면에서는 매우 긍정적이며 진일보한 것이라고 할 수 있지만, 국가차원의 사이버테러 대응체계가 효율적으로 가동하기 위해서는 관련 대응기구의 실질적 권한확보와 예산확보 등 관련 정책의 구속력 확보를 위해서는 법제도적 정비가 뒷받침되어야 할 것이다.

법제도 정비는 다음과 같은 방향에서 이루어져야 할 것이다. 첫째, 산발적인 기관별 사이버테러 대응정책 추진의 문제점을 극복하기 위하여 노력하고 있는 미국과 일본의 사이버안전 정책 추진 현황의 예에서 보듯이, 국가사이버테러 대응 활동의 중심역할 수행을 위한 조직 및 체계에 관한 법적 지위를 확보하여야 한다. 둘째, 관련기관 간 정보공유 및 예·경보체계와 관련된 법제정비가 필요하다. 예컨대 사이버테러 대응기구들 간 정보공유의 법적 근거 확보 및 해당 정보의 오·남용을 막기 위한 제도적 장치가 필요할 것이고, 사이버공격 위협에 대응하기 위한 국가차원의 예·경보체계의 도입·시행에 관한 사항이 규정되어야 할 것이다. 셋째, 국가사이버안전을 위한 중장기적 관점에서의 정책과 기술에 대한 연구 및 핵심 기술 확보를 위한 예산지원 등에 관한 규정이 필요할 것이다. 넷째, 국가차원의 사이버테러 대응을 위해서는 고도의 숙련된 전문인력이 필요한 각급기관에 효율적으로 배치되어야 한다는 점을 감안할 때, 이에 대한 효과적인 지원도 이루어져야 할 것이다. 다섯째, 국제협력 강화에 관한 것이다. 사이버테러는 공간의 제약성이 없다는 특성을 가지고 있으므로 다수 국가의 공동 대응 노력이 절실히 필요한 만큼 실질적 협력체계를 구축하는 것은 중요한 의미를 가진다고 할 수 있다.

나. 사이버 공격에 대한 위기관리체계 구축의 필요성

현재까지 사이버 위기 대응과 관련된 업무는 소관부처별로 이루어졌으며, 각 부처의 업무범위는 정보자산과 기반시설에 대한 침해사고 대응 및 복구에 한정되고 있다.

표 19 법률별 대상 및 소관부처

법률명	대상	소관부처
정보통신기반보호법	주요 정보통신기반시설	행정안전부
정보통신망 이용촉진 및 정보보호 등에 관한 법률	ISP 및 민간통신시설	방송통신위원회
재난 및 안전관리기본법	자연재해 및 기타 물리적 사고	행정안전부

따라서, 제어시스템이나 주요 정보통신기반시설로 지정되지 않은 시스템은 현행 법체계로는 보호할 수 없어 사이버 공격에 무방비로 노출되어 있다. 종합적이고 체계적인 대응이 이루어지고 있지 않아 새로운 국가안보위협으로 떠오르고 있는 것이다. 특히 전력, 가스, 상하수도, 통신 등 각종 기반시설을 통제하는 제어시스템이 해킹을 통해 가동 중단 및 기능 마비 사태가 발생할 수 있다. 그 예로, 2003년 1월에 발생한 전국적인 규모의 국가 주요 통신망 마비 사태, 2004년 6월 중국발 국가기관 해킹사건, 2007년 5월 러시아발 에스토니아 정보통신망 마비시도, 2008년 8월 러시아발 그루지아전 등의 주요사건들을 통해 이미 사이버 공격이 국가·사회적으로 파급력이 막대하여 새로운 국가 안보의 위협 요인으로 대두되고 있다는 것을 잘 보여주고 있다. 현대의 사이버 위기는 바로 국가적인 위기인 것이다.

표 20 사이버공격수단 및 단계별 피해

사이버공격수단	1차피해	2차피해
해킹 컴퓨터 바이러스 서비스 방해 전자기파	국가기밀자료절취	
	국가기반 시설 전산망파괴	댐 SCADA해킹 → 홍수피해
		원자력발전소 SCADA해킹 → 핵폭발

이미 사이버공격은 국가안보의 새로운 위협요인으로 대두되었으나 민·관 분야별 구분대처로 인하여 한계성에 직면하고 있다. 2008년 8월 그루지아 사태 때 사이버 전쟁의 위력이 여실이 증명이 되었는데, 러시아 해커들이 그루지아 대통령실, 정부기관, 군부대, 은행, 통신, 교통, 등의 국가 전산망을 초토화 시켜 그루지아는 전쟁

발발 6일 만에 완전 항복을 선언하였다. 또한, 우리나라 국회, 해양경찰청, 국방연구원, 원자력연구소 등 주요 국가기관이 무더기로 해킹을 당했던 적이 있었는데, 그 발신지가 중국으로 밝혀졌으나 북한의 정예 사이버 부대의 소행으로 의심되고 있는 것이 사실이다. 동시다발적인 사이버 공격으로 전기, 상하수도, 통신 등 30%가 수개월동안 마비되는 경우 그 피해는 대형 허리케인 40~50개와 맞먹는 피해가 발생하는 것으로 조사되었으며, 이미 미국에서는 2007년 3월 사이버 공격으로 인하여 전력발전기에 장애가 발생할 수 있다는 시나리오를 공개하였다.

이러한 상황에서 대응의 신속성이 미흡하고 컨트롤타워(control tower)가 없는 현 체계는 피해를 더욱 확대시킬 뿐이다. 따라서 새로운 사이버위기관리체계를 갖출 필요가 있으며, 이를 뒷받침할 법률 제정이 시급하다. 이를 위해서는 사이버 위기를 국가차원에서 체계적으로 관리할 수 있는 제도와 구체적인 방법 및 절차가 정립되어야 한다.

참고로, 사이버위기는 태풍과 같은 자연재해로부터 오는 재난이 아니라 국가혼란 등의 목적을 가진 특정인이나 집단에 의하여 이루어지기 때문에 국가 안보차원에서 접근이 필요하다. 또한, 국가적 사이버위기관리체계를 구축한다고 해서 국가정보원의 권한이 확대되는 것이 아니라 오히려 타 정부부처 및 기관의 자율성이 강화될 수 있고, 사이버위기경보의 발령에 따라 사이버 위기대책본부가 구성되어도 현재의 조직과 인력이 그대로 위기관리 업무를 수행하므로 조직 확대 또는 권한 강화 등의 우려는 없을 것으로 판단된다.

표 21 국가사이버위기 관리체계 구축시 국가정보원의 역할

	주요활동	현행	구축 후
평시	계획 및 지침	책임기관에 배포	좌동
	확인점검평가	모든 기관에서 수행	중앙행정기관에서 수행
	정보 탐지	책임기관으로부터 취합	좌동
	정보 분석	취합 정보의 분석 및 대책수립	좌동
	지원	정보분석에 따른 대책의 이행	좌동
위기시	경보발령	공공부문	공공 및 민간부문
	사고조사 및 사후처리	대부분의 사고	중대한 사고
	비상기구 운영	중대한 상황시 운영	좌동

제3절 방송통신위원회의 사이버침해 대응체계 개관

1. 서 설

방송통신위원회는 기존 정보통신부의 통신정책 및 통신규제기능과 방송위원회의 방송정책 및 방송규제기능을 통합하여 2008년 출범한 대통령소속 중앙행정기관으로서, 공공부문의 행정안전부, 국방 분야의 국방부, 산업분야의 지식경제부, 형사사법 분야의 검찰·경찰 등과 더불어 방송통신 분야의 사이버침해 대응에 일익을 담당하고 있다. 특히 정보통신부의 전통에 따라 온라인 정보보호, 사이버침해 대응, 개인정보침해 대응 등에 전문성과 풍부한 경험을 축적한 부처라는 대표적 상징성도 함께 가지고 있다.

그러한 상징성에 걸맞게 방송통신위원회는 이명박 정부 출범초기부터 안전하고 건전한 방송통신 이용환경 조성을 위하여 2008년 7월 인터넷정보보호 종합대책을 수립하고 침해사고 대응, 개인정보 보호, 유해정보 대응, 정보보호 기반조성 등의 4대 분야별 대책 50개를 선정하여 2008년부터 2010년까지 역점 추진 중이다.[70]

그 세부사업으로는 인터넷 침해사고의 예방과 대응 강화를 위해서 국내 인터넷 이상 징후 365일 24시간 상시 모니터링 및 초동 대응, 온라인 배포 프로그램(Active X) 취약점 위협 예방 조치, 허위스파이웨어 제거 프로그램 실태조사, 악성 봇 감염률 감소를 위한 피해 예방 활동, ISP·IDC·C쇼핑몰 등 주요 정보통신서비스제공자 대상 안전진단 시행 등이 있으며, 또한 신규 서비스에 대한 보안 강화를 위해 VoIP(인터넷전화), IPTV, 무선 랜 등 신규 서비스에 대한 보안 가이드라인 및 침해대응 기술을 개발하고, VoIP 보안통신, 세션 제어 기술의 산업체 기술이전 및 상용화를 통한 산업 활성화 유도 등의 사업을 추진 중에 있다.

한편, 정보보호 취약계층 지원을 위해 웹 취약점 점검서비스, 공개 웹 방화벽 기술지원, PC 원격점검 서비스 등을 시행하였으며, 중·소규모 IT 서비스 기업의 보안수준 강화를 위하여 취약점 점검, 위험관리, 보호대책 수립 등 기술지원을 추진하는가 하면, 2009년 7·7 DDoS 침해사고로 인해 정보보호 관련 법의 제·개정이 활발

70) 2010 국가정보보호백서, 8-10쪽.

한 가운데 악성코드 전파의 숙주로 악용되는 좀비PC의 발생 및 확산을 막기 위해 '악성프로그램 확산 방지 등에 관한 법률', 일명 좀비 PC법의 제정 작업을 추진하는 등 사이버침해에 대응하기 위한 활발한 정책 사업을 수행하고 있다.

이하에서는 방송통신위원회를 중심으로 한 사이버침해 대응체계를 법적근거와 주요 정책을 위주로 살펴보기로 한다.

2. 방송통신위원회 사이버침해 대응체계의 법적 근거

가. 조직법적 근거

방송통신위원회는 '방송통신위원회 설치 및 운영에 관한 법률'에 따라 대통령 소속으로(법§ 3①) 설치된 중앙행정기관(법§ 3②)으로서 1) 방송에 관한 사항, 2) 통신에 관한 사항, 3) 전파연구 및 관리에 관한 사항과 기타 작용법규의 사항을 소관사무로 하고 있다.(법§ 11①) 또한 방송통신위원회에는 '방송통신위원회와 그 소속기관 직제(대통령령)' 에 따라 이용자 네트워크국을(영§ 13①), 이용자 네트워크국에 네트워크 안전과 등 사이버침해 대응체계 관련 업무조직을 설치하고 있고(영§ 13③), 개인정보보호에 관하여는 개인정보 보호과를, 불법정보대응 등에 관하여는 사이버윤리팀을 설치(영§ 13③)하고 있는 바, 구체적인 사항은 네트워크 안전과장의 업무와[71] 개인정보 보호과장의 업무에서[72] 잘 드러난다.

71) '방송통신위원회와 그 소속기관 직제' 제13조 제12항
1. 방송통신망의 안전성·신뢰성 확보를 위한 종합대책의 수립 및 관련법령 제·개정
2. 방송통신망상의 서비스 보호 관련 지침 수립
2의2. 방송통신망의 서비스 보호 관련 기술개발 및 기술기준 제정
3. 방송통신망의 안전성 점검·평가 및 관련지수 개발, 통계조사
4. 방송통신망 침해사고 대응체계 구축·운영
5. 방송통신망 침해사고 관련정보 수집·전파, 예·경보 발령
6. 악성 프로그램 기준 제정 및 실태조사
7. 광대역 통합망 등 융합 네트워크 보호체계 개발
8. 유·무선 네크워크 안전관리대책 수립
9. 삭제 <2008.7.3>
10. 방송통신 분야에서 암호이용정책의 수립 및 이용활성화에 관한 사항

한편, 전파분야에 대해서는 방송통신위원회 소속기관으로 전파연구소와 중앙전파관리소를 설치(영§ 14, 영§ 16)하여 보안, 통신보안과 전파침해에 대응하고 있다.

나. 작용법적 근거

조직법과는 달리 방송통신위원회의 사이버침해대응 업무에 관한 작용법적 근거는 대표적으로 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)'에서 논의되고 있다.

정보통신망법은 '침해사고'에 대해 "해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서

11. 정보보호 안전진단 종합계획 수립, 안전진단 수행기관 관리 및 제도 운영
12. 정보보호관리체계인증 종합계획 수립, 인증기관 지정 및 제도 운영
13. 방송통신망 보호 관련 공공기관·법인·단체 등의 육성·지원
14. 위원회 소관 주요 정보통신 기반시설 보호에 관한 사항

72) '방송통신위원회와 그 소속기관 직제' 제13조 제13항

1. 방송통신망에서 개인정보보호에 관한 기본정책의 수립 및 관련법령 제·개정
2. 인터넷서비스 개인정보보호에 관한 대책 수립
3. 개인정보보호 신뢰지수 개발 및 통계조사
4. 방송통신사업자의 관리적·기술적 개인정보보호조치 기준 제정
5. 방송통신사업자 개인정보보호 사전영향평가제도 운영
6. 방송통신서비스 개인정보 침해대책 수립
7. 방송통신망에서 개인영상정보 보호대책 수립·추진
8. 방송통신서비스제공자의 개인정보 실태점검 기획·조사
9. 법 위반 사업자 제재 및 위반내용 공표
10. 방송통신망에서의 개인정보 침해 구제
11. 방송통신망에서 개인정보취급방침의 전자적 표시수단 개발·보급
12. 방송통신망에서 개인식별수단의 개발·보급
13. 방송통신망에서의 개인정보보호 기술적 대책 수립 및 기술 연구
14. 방송통신망에서의 개인정보보호 교육 및 홍보
15. 개인정보보호 유관단체 지원 및 인증마크 보급 확산
16. 위치정보 사업자 인·허가 및 보호정책 수립
17. 위치정보 품질 개선 및 법 위반 사업자 제재
18. 위치정보서비스 개발·보급 및 기술 표준의 보급·확산
19. 위치정보이용 활성화에 관한 기본계획의 수립 및 법제도에 관한 사항
20. 방송통신 분야에서 보안서버의 적용 및 확산에 관한 사항.

비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다"고 규정하여 사이버침해행위의 개념을 명문화하고 있으며(§ 2⑦), 이에 대응하기 위하여 '정보통신망의 안전성 및 신뢰성 제고'에 관한 사항을 행정안전부, 지식경제부, 방송통신위원회에 맡기고,(§ 4⑧) 이를 국가정보화기본계획과 연계하도록 규정하고 있다.(§ 4③) 따라서 방송통신위원회는 주로 통신사업자를 비롯한 온라인서비스사업자에 대한 사이비침해대응 계획의 수립 및 집행업무를 수행하는 것으로 파악할 수 있다.

구체적인 업무수행의 법적근거로서 방송통신위원회는 정보통신서비스제공자가 준수할 정보보호조치 및 안전진단의 방법·절차·수수료에 관한 '정보보호지침'의 제정권을 보유하고 있다.(망법§ 45①, ②) 아래 표는 정보보호 지침의 포함사항과 그 구체적인 내용이다.

표 22 정보보호지침의 포함 사항 (망법§ 45③)

1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치 2. 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치 3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치 4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

※ 비고 1. "서비스수준협약"은 SLA(Service Level Agreement)를 말한다.
2. "DMZ"는 Demilitarized Zone을 말한다.
3. "DNS 서버"는 Domain Name System 서버를 말한다.
4. "DHCP 서버"는 Dynamic Host Configuration Protocol 서버를 말한다.
5. "DB 서버"는 Data Base 서버를 말한다.
6. "ACL"은 Access Control List를 말한다.
7. 2.2.7~2.2.11의 사항은 2.2.1~2.2.6에 해당하는 설비에 적용된다.

표 23 보호조치의 구체적인 내용 (방송통신위원회 고시 제2008-12호)

구 분			세부조치사항
1. 관리적 보호조치	1.1. 정보보호 조직의 구성운영	1.1.1. 정보보호조직의 구성	▸ 정보보호책임자, 정보보호관리자, 정보보호담당자로 구성된 정보보호조직을 운영
		1.1.2. 정보보호책임자의 지정	▸ 침해사고 발생시 긴급조치 권한을 행사할 수 있는 자로 지정
		1.1.3. 정보보호조직 구성원의 역할	▸ 정보보호책임자는 정보보호 업무와 조직을 총괄 지휘 ▸ 정보보호관리자는 정보보호 업무의 실무를 총괄하고 관리 ▸ 정보보호담당자는 정보보호 업무의 분야별 실무를 담당
	1.2. 정보보호 계획 등의 수립 및 관리	1.2.1. 정보보호방침의 수립·이행	▸ 정보보호 목표, 범위, 책임 등을 포함한 정보보호 방침(policy) 수립 ▸ 최고경영층(임원급 이상)의 승인
		1.2.2. 정보보호 실행계획의 수립·이행	▸ 정보보호방침을 토대로 예산, 일정 등을 포함한 당해 연도의 정보보호 실행계획을 수립 ▸ 최고경영층이 실행계획을 승인하고 정보보호책임자가 추진 상황을 매 반기마다 점검
		1.2.3. 정보보호 실무지침의 마련·준수	▸ 정보통신설비 및 시설에 대한 관리적·기술적·물리적 보호조치의 구체적인 시행 방법·절차 등을 규정한 정보보호 실무지침을 마련 ▸ 정보보호책임자가 실무지침을 승인하고 관련 법·제도, 설비의 교체 등 변경 사유가 발생할 경우 보완하여 관리
	1.3. 인적 보안	1.3.1. 내부인력 보안	▸ 임직원의 전보 또는 퇴직시 즉시 관련 계정 등에 대한 접근 권한을 제거 ▸ 임직원에게 정보보호 인식을 제고할 수 있는 홍보(정보보호 실천수칙 보급 등)를 실시 ▸ 정보보호조직의 구성원 및 정보보호와 관련된 업무에 종사하는 자에게 정기적으로 정보보호교육 실시
		1.3.2. 외부인력 보안	▸ 자사 직원이 아닌 자를 업무에 활용할 경우 보안서약을 징구
		1.3.3. 위탁운영 보안	▸ 전산업무를 외부에 위탁할 경우 보안계약서 또는 서비스수준협약등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무 중단에 따른 비상대책' 등을 반영
	1.4. 이용자 보호	1.4.1. 정보보호 정보제공	▸ 이용자에게 침해사고 예·경보, 보안취약점, 계정·비밀번호 관리방안 등의 정보를 지속적으로 제공
	1.5. 침해사고 대응	1.5.1 침해사고 대응계획의 수립 · 이행	▸ 침해사고 정의 및 범위, 대응체계(보고 및 조치 체계), 대응 방법 및 절차, 복구 방법 및 절차, 증거자료 수집 및 보관 등을 포함한 침해사고 대응계획을 마련·시행

구 분			세부조치사항
	1.6. 정보보호 조치 점검	1.6.1. 보호조치의 자체 점검	▸ 정보보호관리자는 매년 동지침 및 정보보호실무지침의 기준에 따라 자체적으로 정보보호 현황을 점검
	1.7. 정보자산 관리	1.7.1 정보통신설비 및 시설의 현황 관리	▸ 정보통신망 구성도를 마련하고 변경사항이 있을 경우 보완관리 ▸ 정보통신설비 및 시설의 목록(용도 및 위치 등 포함) 작성관리
2. 기술적 보호조치	2.1. 네트워크 보안	2.1.1. 트래픽 모니터링	▸ 네트워크 모니터링 도구를 이용하여 백본망, 주요노드 및 외부망과 연계되는 주요회선의 트래픽 소통량을 24시간 모니터링
		2.1.2. 무선서비스 보안	▸ 무선랜서비스, 무선인터넷서비스를 제공할 경우에는 사용자인증, 데이터암호화 등 보안조치를 마련
		2.1.3. 정보보호시스템 설차운영	▸ 외부망과 연계되는 구간에 침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설차운영
	2.2. 정보통신설비 보안	2.2.1. 웹서버 보안	▸ 외부에 서비스를 제공하는 웹서버는 단독서버로 운영하고 DMZ에 설치
		2.2.2. DNS서버 보안	▸ 과부하에 대비한 부하분산 대책을 마련 ▸ 설정파일 백업 실시
		2.2.3. DHCP서버 보안	▸ 과부하에 대비한 부하분산 대책을 마련 ▸ 설정파일 백업 실시 ▸ IP 할당 상황 등에 대한 로그기록 유자관리
		2.2.4. DB서버 보안	▸ 내부망에 설치 ▸ 외부망에서 직접 접속할 수 없도록 네트워크를 구성
		2.2.5. 라우터/스위치 보안	▸ ACL 등의 접근제어 기능을 적용할 수 있는 설비를 사용
		2.2.6. 정보보호시스템 보안	▸ 이상징후 탐지를 알리는 경고 기능을 설정하여 운영 ▸ 정보보호시스템 보안기능(비정상 트래픽 차단 등)의 정상 작동 여부를 주기적으로 점검(월 1회 이상)
		2.2.7. 취약점 점검	▸ 연 1회 이상 취약점 점검을 실시하고 발견된 취약점을 보완
		2.2.8. 접근통제 및 보안설정 관리	▸ 인가된 자만 접속할 수 있도록 설정하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드 등을 사용하도록 하여 인가 절차를 강화 ▸ 불필요한 프로토콜 및 서비스 제거 등 보안설정
		2.2.9. 관리자 계정의 비밀번호 관리	▸ 관리자 계정의 비밀번호는 8자리 이상으로 설정. 단, 설정 가능한 자리수가 8자리 미만일 때는 설정 가능한 최대의 자리수로 설정 ▸ 최소 3개월에 1회 이상 비밀번호 변경

구 분			세부조치사항
		2.2.10. 로그 관리	▸ 최소 1개월 이상 로그기록 유자관리(정보보호시스템은 3개월)
		2.2.11. 보안패치 관리	▸ 보안패치 정보를 주기적으로 입수하고 적용 ▸ 주요 보안패치에 대해서는 적용일 등 패치정보를 기록관리
		2.2.12. 백업 및 복구	▸ 주요정보를 주기적으로 백업 ▸ 백업 담당자, 백업 및 복구 방법·절차주기 등을 기록관리
3. 물리적 보호조치	3.1. 출입 및 접근 보안	3.1.1. 정보통신 시설의 출입접근 통제	▸ 비인가자가 출입할 수 없도록 잠금장치를 설치 ▸ 출입자의 출입기록을 1개월 이상 유지·보관
	3.2. 부대 설비 및 시설 운영·관리	3.2.1. 백업설비 및 시설설차운영	▸ 주요정보를 백업하여 보관할 수 있는 백업설비 및 시설을 설차운영

방송통신위원회는 사업자에 대한 정보보호지침과는 별도로 이용자가 준수하여야 하는 이용자 정보보호기준제정권도 보유하고 있으나(망법§ 47의3①), 이에 대한 특별한 실효성 확보수단은 미비하다는 점에서 일정한 한계가 있다 할 것이다. 또한 이외에도 방송통신위원회는 IDC에서 중대 침해사고 시 그 서비스의 전부 또는 일부를 중단시킬 수 있고(망법§ 46의2①3), 정보보호안전진단 결과 정보보호조치 개선이 필요한 경우 그 명령권을 발동할 수 있으며(망법§ 46의3), 정보보호 관리체계 인증 업무를 수행하는 등(망법§ 47), 다양한 정보보호 업무를 수행하고 있다.

방송통신위원회의 사이버침해 대응체계에 대해서 우리가 눈여겨보아야 할 내용은 정보통신망법 제48조가 핵심적인 것으로서, 여기에서는 각 항별로 정보통신망 무단침입죄, 정보통신망 장애발생죄, 악성프로그램 유포죄의 구성요건을 규정하고 각각 3년 또는 3천만원(§ 72①), 5년 또는 5천만원(§ 71)의 형벌을 부과하고 있는데, 결국 이와 같은 형사벌을 정보통신망법에 규정함으로써 방송통신위원회의 행정적 대응체계와 수사기관의 사법적 대응체계가 상호 연계·공조될 수 있는 기반을 마련하고 있는 것이다.

방송통신위원회가 사이버침해에 행정적으로 대응하고 있는 체계는 그 침해사고의

대응권한을 보유하고 있음에서 명확히 드러나고 있다.[73] 물론 기술적인 전문성을 보다 제고하기 위하여 인터넷 및 정보보호에 관련 국내에서 가장 전문성이 있는 것으로 평가받고 있는 한국인터넷진흥원에 그 업무의 전부 또는 일부를 위탁하고 있는 것도 눈여겨보아야 할 사항이다. 당해 침해사고 대응체계에 따라 주요정보통신서비스제공 및 집적 정보통신시설 사업자 등 일정 의무자는 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 방송통신위원회나 한국인터넷진흥원에 제공하여야 한다.(망법§ 48의2②)[74]

한편, 정보통신망법은 방송통신위원회의 침해사고의 대응과 더불어 민간부문에 대해서도 침해사고대응에 조력하도록 의무를 부과하고 있는데, 정보통신서비스 제공자, 집적 정보통신시설 사업자는 침해사고가 발생하면 즉시 그 사실을 방송통신위원회나 한국인터넷진흥원에 그 사고를 신고할 의무를 부과하고 있다.(망법§ 48의3①)[75]

---

73) 정보통신망법 제48조의2(침해사고의 대응 등) ① 방송통신위원회는 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다.
1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 대통령령으로 정하는 침해사고 대응조치

74) 동법 동조 ② 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 방송통신위원회나 한국인터넷진흥원에 제공하여야 한다.
1. 주요정보통신서비스 제공자
2. 집적정보통신시설 사업자
3. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자

③ 한국인터넷진흥원은 제2항에 따른 정보를 분석하여 방송통신위원회에 보고하여야 한다.

④ 방송통신위원회는 제2항에 따라 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있다.

⑤ 방송통신위원회나 한국인터넷진흥원은 제2항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다.

⑥ 방송통신위원회나 한국인터넷진흥원은 침해사고의 대응을 위하여 필요하면 제2항 각 호의 어느 하나에 해당하는 자에게 인력지원을 요청할 수 있다.

75) 제48조의3(침해사고의 신고 등) ① 다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다. 이 경우 '정보통신기반 보호법' 제13조 제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다.

또한 방송통신위원회는 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관 합동 조사단을 구성하여 그 침해사고의 원인을 분석(망법§ 48의4 ②)하고 이를 위한 자료보전명령권(동조③), 자료제출 요구권 등(동조④)을 보유하고 있는 것도 정보통신망법이 방송통신위원회를 중심으로 사이버 침해대응을 위해 마련하고 있는 주요 제도 중 하나이다.

3. 주요 정책

가. 개 관

방송통신위원회는 대통령 직속기관으로서 미국의 연방통신위원회(FCC)와 같이 방송·통신정책을 총괄할 기구 마련의 필요성에 따라 이명박 정부 초기 출범하였다. 그동안 방송계와 정보통신계의 대립으로 지지부진했던 방송통신 융합산업과 서비스를 본격적으로 추진하기 위한 정권의 의지가 담겨 있었던 만큼 정보통신부에서 관장해온 통신·주파수 정책, 개인정보 및 인터넷 정책, 방송위에서 다뤄온 방송 심의 등 규제 정책 등을 총괄하도록 한 것이다. 따라서 2008년 출범 이후 줄곧 방송통신위원회는 주로 방송정책과 통신정책의 융합 및 산업적·진흥적 관점의 정책에 집중하는 모습을 보여 왔다.

그러나 2009년 DDos 공격[76] 이후 사이버침해 대응이 주요 정책이슈로 부상하면

1. 정보통신서비스 제공자
2. 집적정보통신시설 사업자

② 방송통신위원회나 한국인터넷진흥원은 제1항에 따라 침해사고의 신고를 받거나 침해사고를 알게 되면 제48조의2제1항 각 호에 따른 필요한 조치를 하여야 한다.

76) 2009년 7월 3차례에 걸쳐 분산서비스 거부(Distributed Denial of Service : DDoS) 공격이 발생하였다(국내 22개 사이트 및 미국 14개 사이트).
분산서비스 거부(Distributed Denial of Service : DDoS) 공격은 인터넷 서비스를 제공하는 기업(기관)의 운영서버(웹서버, DNS 서버 등) 와 네트워크 장비(라우터, 스위치 등) 에 임의의 조작된 공격성 트래픽을 전송하여 시스템 자체를 지연 또는 마비시켜서 이용자들이 인터넷 서비스를 이용할 수 없는 상황을 만들며, 대규모의 사이버공격 및 사이버테러의 대부분이 이와 같은 DDoS 방법으로 행해지고

서 2010년 사이버침해 등 정보보호에 관한 정책대응이 크게 강화된 것이 특징이다.

표 24 주요 사이버 공격 일지

발생시기	내 용	비 고
2000년	미국 야후, 아마존, CNN 등 주요사이트 DDoS 공격 및 해킹으로 서비스 일시 중단	첫 대규모 DDoS 공격
2001년	한국정보보호센터, 국내 서버에 DDoS용 프로그램 확산 경고	–
2001년	Windows NT 및 Windows2000의 보안 취약점을 이용해 전파되는 백악관 사이트 공격용 인터넷 웜 '코드 레드(Code Red)' 출현 및 확산.	이틀만에 전세계에서 30만대 이상 감염돼 26억달러 손실 추정.
2001년	님다(Nimda) 웜 발견 및 확산으로 국내 인터넷 접속지연	–
2002년	미국 DNS 루트서버 13대에 DDoS 공격으로 평소 10배가 넘는 트래픽 발생	–
2003년	정통부, 국내 컴퓨터시스템 경유한 국제 해킹 급증으로 긴급경보 발령	–
2004년	SCO, MS 웹사이트에 대한 DDoS 공격	SMTP엔진, 이메일, P2P 파일을 통한 전송, 전세계 439억달러 피해 추정, SCO 웹사이트 다운으로 대체사이트 운영
2009년	국내 DDoS 사이버 대란 (7·7 인터넷대란)	주요 정부기관 및 언론사이트, 포털사이트 서비스장애, PC 손상 1500대

나. 2010년 안전한 사이버세상 구현정책[77]

(1) DDoS 등 사이버공격 대응역량 강화

상술한 바와 같이 출범초기의 방송통신위원회의 업무는 2009년 DDoS 사건을 계기로 사이버공격 대응역량 강화에 크게 집중되었다. 특히 정부의 강력한 의지에 따라 장비 및 인력이 보강되었으며, 인터넷침해대응센터(KISC)의 노후한 대응시스템을

있다.

77) 방송통신위원회, 2010년 업무계획 available at http://www.kcc.go.kr/user.do?page=P04010500&dc=K04010503(2010.9.1 방문).

업그레이드하고 악성코드 분석 등의 전문인력을 대폭 보강하는데 약 120억 원의 예산을 투입하였다. 이는 DDos 공격이 비교적 큰 규모로 진행될 수 있었던 이유가 일반 이용자의 PC가 악성코드에 감염되어 공격에 가담되었던 사실을 인지한 정책적 대응이라 할 것이다.[78] 또한 민간부문에 악성코드 탐지 점검대상 웹사이트를 대폭 확대(15만개 → 100만개)하고 영세 중소기업을 위한 DDoS 긴급대피소를 구축하는데 약 80억 원의 예산을 투입하기도 하였다.

(2) 신규서비스 대응체계 구축

신규융합서비스에 대한 침해사고 대응강화도 방송통신위원회의 주력 정책의 하나로 볼 수 있다. 신규융합서비스에 대한 안정성 확보는 산업경쟁력 강화와 신성장 동력 창출이라는 정부 경제정책기조 달성을 위해 당연한 대응이라 할 것인 바, 구체적으로는 인터넷전화(VoIP), 인터넷TV(IPTV), 무선인터넷 등에 대한 침해사고 대응체계를 마련하는가 하면(2010.10월), 클라우드 서비스 및 미래 인터넷서비스 등 차세대 인터넷 기반서비스에 대한 사전 보안체계를 강구한 것이 주요 내용이다(2010.12월).

(3) 이용자 보호 강화

한편, 방송통신위원회는 이용자에게 안전한 정보통신환경을 제공하기 위한 정책도 추진하였다. 특히 이용자PC에 대한 신속한 감염 확인과 치료를 위해 감염PC 알림서비스와 전용백신 보급체계를 마련하는데 약 40억 원의 예산을 투입하는 한편, 이용자들이 TV, 포털 등을 통해 인터넷 위협정보를 적시에 제공받을 수 있도록 정보보호 예보지표를 개발하는데 약 14.9억 원의 예산을 투입하였다.

78) 실제로도 민간부문의 경우 인터넷사용자 3,500만명, PC 3천만대, 서버 570만대, IP 7,200만개 등으로 전체 사이버영역의 97% 이상을 차지하고 있다. 반면 공공부문의 경우 PC 130만대, 서버 수만대로 DDos 공격과 같이 일반이용자가 공격에 노출되거나 가담할 경우 피해는 기하급수적으로 늘어나게 된다.

4. 인터넷침해대응센터

방송통신위원회의 사이버침해 대응정책을 살펴봄에 있어서 이를 위한 주요 추진 주체를 빼놓을 수 없을 것이다. 실무적이고 전문적으로 사이버침해에 대응하기 위하여 마련된 대표적인 사례로 '인터넷침해대응센터'가 있다.[79)]

인터넷침해대응센터는 국내 인터넷망의 상시 모니터링을 통하여 취약점, 웜·바이러스 등 보안위협 및 인터넷 이상 징후를 조기에 탐지한 후 분석·경보발령을 통하여 인터넷 침해사고를 사전에 예방하고 피해확산을 방지하는 역할을 수행하고 있다. 특히, 국내 정보통신 서비스제공자(ISP), 백신업체, 보안관제업체 등과 상시적인 정보공유, 신속한 공동대응을 통하여 침해사고로 인한 사회적·경제적 손실을 최소화하고, 이용자가 신뢰하고 사용할 수 있는 안전한 인터넷 서비스 환경을 구축하는 것이 주된 임무인데, 이러한 인터넷침해대응센터는 민간 부문의 인터넷 침해사고에 대응하고, 보안업체, 인터넷 서비스사업자 등과 협조체제를 구축하며, 국제적 침해사고 대응을 위한 창구역할을 수행하기 위하여 2003년 12월 한국인터넷진흥원(KISA) 내에 설치된 것이다.

인터넷침해대응센터의 주요업무를 분설하면 다음과 같다. 첫째, 침해사고에 따른 조기대응을 강화하기 위해 종합상황실을 운영하여 KT, SK브로드밴드 등 국내 주요 통신사업자 및 관제업체의 네트워크 정보를 실시간으로 제공받아 365일 24시간 이상 징후를 모니터링 하는 한편, DDoS, 홈페이지 변조사고 등 주요 해킹사고의 사고접수·처리 및 주요 해킹사고, 웜·바이러스 감염 등에 대한 대국민 상담과 기술지원을 수행한다.

둘째, 악성코드가 은닉되어 유포되는 홈페이지를 사전에 탐지하여 해당기관 및 업체에게 실시간 통보하여 피해를 최소화하는 등 초동대응을 담당하고, 발생한 인터넷 침해사고에 효과적으로 대응하기 위해 신규 출현 취약점과 웜·바이러스에 대한 정보를 수집하며, 확산 가능성, 영향력 등의 위험도를 객관적인 지표로 평가하여 심각성 수준에 따른 민간분야 위기경보를 발령하여 신속한 상황전파가 이루어지도록 하는 업무를 수행한다.

79) 2010 국가정보보호백서, 10쪽.

셋째, 인터넷 이상 징후 상시모니터링 및 대응을 통한 선제적 침해사고 예방 및 피해확산방지 노력과 함께 KrCERT(www.krcert.or.kr) 홈페이지에 최신 보안동향 및 침해사고 통계분석 정보를 제공함으로써 정부의 정보보호 정책수립 지원 및 대국민 보안인식을 제고하는가 하면, 마지막으로 아시아·태평양지역 침해사고 대응팀 협의회(APCERT) 및 인터넷침해사고대응 국제기구(FIRST) 등의 국제기구 참가를 통해 국제 정보교류의 창구 역할도 수행하고 있다.

5. 분석 및 평가

이상의 사항을 분석하여 보면, 방송통신위원회는 사이버 침해사고에 대응하여 기존의 역량을 유지발전 시키고 있고, 새로운 침해사고나 위험요소에 대응하기 위한 노력을 기울이고 있음을 알 수 있다. 또한 경험을 바탕으로 하여 실질적인 정보보호 전문기관인 인터넷진흥원을 산하기관으로 운영하면서 국가적 대응체계의 일익을 확실히 담당하고 있다.

그러나 정부정책의 조직적, 체계적 운용과 신속한 대응을 위하여서는 몇 가지 지적할 만한 사항이 있다. 이는 현 정부 들어서 IT정책 추진체계를 개편하면서 빚어지는 혼선으로부터 비롯된다.

실제로 "현재 국가사이버안전센터, 국방정보전대응센터, 인터넷침해사고대응센터 등 분야별로 사이버테러에 대응하고 있는 것은 비효율적 … 각 센터운영을 위한 전문인력이 부족하고 각 센터간 정보공유와 협조체제가 미미하며 실무리더기관이 부재한 실정…"[80]이라는 비판의 목소리가 현장에서 제기되고 있다.

여기에는 두 가지 문제점이 존재한다. 하나는 IT정책에서 정보보호의 중요성이 인정됨에도 불구하고 IT정책은 여전히 물량 투입의 정보화정책을 중심으로 운용된다고 하는 점이다. 즉, 예산과 조직이 많이 투입되는 정보화분야에서는 이에 대한 기관간 경쟁이 치열하고 그에 따라서 조직개편에서 정리하는 작업과 체계화하는 작업이 정보보호 분야에 비해 상대적으로 우선 조정되는 경향을 띤다. 그러나 국가적으로

80) 한국정보사회진흥원, "CIO 리포트" 제5호(2008. 9), 5쪽; 김귀남 교수 인터뷰 내용에서 인용.

볼 때 정보보호에 관한 종합조정은 정보화보다 국익의 입장에서 볼 때 훨씬 중요한 이슈라는 지적이 가능하다.

또 하나는 국가안보를 중심으로 하는 정보보안과 전자정부나 금융 및 상거래 등 일상적인 정보보호에 관한 조직체계적 정리가 부족한 문제이다. 국가안보에 관한 사항을 다루는 분야와 전자정부, 공공부문 정보보호, 금융·상거래 등 일반 정보보호는 그 정책 목표와 내용이 다르게 나타날 수밖에 없는 분야이다. 이에 대한 체계적 대응이나 조직적 역할분담이 부족한 상태에서 동시 다발적으로 시스템에 대한 침해사고가 발생하자, 정책적 혼선을 야기하는 것이다.

이에 대한 우선적 대응방안으로는 국가 전체의 정보보호정책체계를 바로 세우는 작업이 필요하다. 종합적·체계적 정보보호 정책의 목표를 설정하고 이에 대응하는 국가 정책역량을 결집할 수 있는 리더십을 마련하여야 한다. 국가안보 사이버대응을 위한 체계를 대통령실로부터 지휘할 수 있는 종합지휘감독체계를 중심으로 하여 부처간 협의회와 부처별 역할을 분명히 정리하면 공동 대응센터의 운영 등 실무적 정책이 뒤 따를 수 있다. 이를 위하여 정보보호 정책을 체계적으로 운용하기 위한 법제도적 개선이 뒷받침되어야 함은 물론이다.

제4절 경찰청의 사이버침해 대응체계 개관

1. 사이버수사의 법적 근거

경찰의 범죄예방 및 수사 활동의 근거는 경찰법, 경찰관직무집행법 그리고 형사소송법에서 찾을 수 있다. 경찰법 제3조에는 국가경찰의 임무로 "국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압 및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 임무로 한다"고 규정되어 있으며, 경찰관직무집행법 제2조 제1호에 경찰관의 직무는 "범죄의 예방·진압 및 수사" 등을, 형사소송법 제196조에는 "사법경찰관은 검사의 지휘를 받아 수사를 하여야 한다"라고 적시하고 있다. 경찰청과 그 소속기관 직제(대통령령 제22459호) 제12조 수사국 업무에는 경찰수사 업무에 관한 기획·지도·조정 및 통제, 범죄수사의 지도 및 조정, 범죄의 수

사에 관한 사항을, 제15조 보안국 업무에는 간첩 등 보안사범에 대한 수사의 지도·조정, 간첩 등 중요방첩수사에 관한 업무, 중요 좌익사범의 수사에 관한 업무 등이 규정되어 있다.

경찰청과 그 소속기관 직제 시행규칙(행정안전부령 제165호)에는 수사국내에 사이버테러대응센터를 두도록 하고 있다. 동 규칙 제9조 제9항에 따라 사이버테러대응센터는 ① 사이버테러의 탐지, 추적수사 및 경보 등 조치, ② 사이버테러 관련 수사기법의 연구·개발 및 국제경찰기구 등과 협력, ③ 사이버범죄의 수사 및 지도, ④ 디지털매체 등 증거분석 업무를 담당한다.

2. 경찰청의 사이버범죄 대응전략

가. 1997년 컴퓨터범죄 수사기능 강화방안

경찰청은 1995년 해커수사대 창설 후 총 4회에 걸쳐 종합대책을 마련하여 사이버범죄 또는 사이버테러에 대한 대응전략을 수립하여 추진해 왔다.

1997년 '컴퓨터범죄 수사기능 강화방안'을 수립하여 1995년부터 경찰청 외사관리관실에서 운영되어 왔던 '해커수사대'와 형사국 지능과에 소속되어 있는 사이버수사 전담요원을 통합하여 형사국 지능과 소속의 컴퓨터범죄수사대로 수사체제를 일원화하였고, 이후 1999년에 사이버범죄수사대로 확대 개편하였다. 지방청과 경찰서에 전담요원을 지정하여 운영하고, 경찰수사연수원에 컴퓨터범죄 수사과정을 신설하여 전문 수사요원 양성을 위한 기반을 마련하였다. 사이버수사조직은 사이버범죄가 컴퓨터가 발달한 외국에서 먼저 이슈화되었고, 인터폴 및 선진국으로부터 공조수사 요청이 들어오면서 자연스럽게 외사관리관실에서 시작된 것으로 추정된다.

나. 2000년 사이버테러 대책보고서

2000년에는 미국 CNN, YAHOO, E-BAY 등이 공격[81]을 당하자 우리나라에서도

81) 캐나다 경찰은 '마피아 보이'란 별명을 가지고 있는 15세 소년을 범죄용의자로 특정하여 사건발

국가안보 차원의 대응을 위해 국무총리실 주관으로 범정부적 '사이버테러 방지대책'을 추진하였고, 그 일환으로 경찰청에서도 '사이버테러 대책보고서'를 마련하였다. 당초 경무관을 책임자로 총 128명 규모의 사이버테러대책단을 신설하고, 소속 하에 협력운영팀, 신고·경보센터, 수사팀, 수사기법개발팀 등 4개 팀으로 구성하고자 하였으나 최종적으로는 총경을 책임자로 72명 규모의 사이버테러대응센터로 출범하게 되었다. 당시에 처음으로 민간 IT 전문가를 경장급의 사이버수사요원으로 특채하는 제도를 도입하여 현재까지 이르고 있다.

다. 2004년 사이버치안역량 강화방안

지식정보 기반사회에 대비하여 미래형 수사조직 모델을 구축하기 위하여 '21세기 첨단 디지털 시대 사이버치안역량 강화방안'을 수립하였다. 주요 내용은 첫째 최첨단 디지털 수사기반 확보 차원에서 디지털증거센터 설치·육성, 둘째 미래형 조직모델 구축에서 경무관을 책임자로 하는 4과 체제(107명)의 대응조직 창설, 사이버테러와 일반사이버범죄 개념 분리 대응, 실효성 있는 전문인력 관리방안 마련, 셋째 전략적 사이버치안 활동 전개 차원에서 중장기 사이버치안 전략 수립, 국제사회 리더로서 위상 제고, 국제수준의 법·제도 개선 등을 골자로 하고 있다. 또한, 서울 등 주요 3개 지방청에 사이버범죄수사과 신설, 현장 수사관과 증거분석 수사관으로 인력양성 이원화, 사이버수사요원 특채제도 정례화, 사이버수사요원 인사관리 규정 제정 등 다양한 정책이 제시되었다.

라. 2009년 사이버테러 종합대책

2009년에는 7·7 DDoS 사건을 계기로 '사이버테러 종합대책'을 수립하였다. 종합대책은 전담조직 확대, 전문인력 확보 및 양성, 첨단시설 및 장비도입, 유관기관 및 민간협력, 국제협력 강화 등 5개 분야 28개 과제를 포함하고 있는데, 주요내용은 경무관을 책임자로 하는 120명 규모의 '사이버범죄수사단' 창설, 핵심인력 양성과정 개

생 약 1달 여만에 검거하여 해킹혐의로 기소하였다(매일경제 인터넷판, "CNN 사이트 해커 용의자 체포…15세 캐나다인 '마피아보이'" 제하 보도, 2000. 4. 20일자).

발·운영, 악성코드 분석대회 개최, 디지털증거센터 구축, 해킹·악성코드 분석실 설치, 사이버테러 신고보상금제 도입, 사이버테러 전문위원회 도입, 인터폴 사이버범죄 아카데미 창설, 인터폴 내 경찰관 파견 등이다. 종합대책은 종전의 조직인력 중심이 아닌 각종 제도 도입, 국제기구 유치, 국제협력 강화, 첨단시설·장비 확충 등 사이버테러 수사를 위한 인프라 확충에 중점을 두었다.

3. 경찰청의 사이버수사조직

경찰청 사이버수사조직의 역사는 1995년 외사관리관실 외사3과 '해커수사대', 1997년 형사국 지능과 '컴퓨터범죄수사대', 1999년 수사국 지능과 '사이버범죄수사대', 2000년 수사국 소속 사이버테러대응센터로 확대되어 오늘에 이르고 있다. 지방청은 2000년에 전국적으로 사이버범죄수사대를 창설하였고, 2007년에 전국 경찰서 1급지에 사이버범죄수사팀을 설치하여 전국적인 수사체제를 구축하였으며 현재 사이버수사 전담인력 1천명 시대를 목전에 두고 있다.

경찰청 사이버테러대응센터의 사무는 경찰청 사무분장 규칙(경찰청 훈령 제593호) 제27조에 규정되어 있다. 사이버협력운영팀(동조 제1항)은 ① 사이버범죄·테러 종합대책 수립, ② 사이버수사 교육 및 전문가 특채, ③ 사이버수사 예산 및 장비관리, ④ 유관기관·민간업체 등과 협력 및 홍보, ⑤ 국제기구 및 외국과의 협력 및 공조활동, 사이버기획수사팀(동조 제2항)은 ① 사이버범죄 예방 및 단속대책 수립, ② 사이버범죄 수사지도 및 조정, ③ 사이버범죄 신고·상담 및 초동조치, ④ 사이버범죄 사이트 관련 대응조치, 사이버테러수사팀(동조 제3항)은 ① 해킹, DDoS 공격 등 중요 사이버범죄 수사, ② 국내·외 사이버테러 첩보수집 및 대응, ③ 사이버테러 국제공조 수사, 디지털포렌식팀(동조 제4항)은 ① 디지털포렌식 기획, ② 디지털포렌식 및 사이버수사 기술지도, ③ 디지털매체 증거분석 및 분석기법 연구·개발, ④ 해킹·악성코드 등 분석 및 기법 연구·개발, ⑤ 네트워크 추적 등 사이버수사기법 연구·개발, ⑥ 사이버수사 시스템 관리 및 개발 업무를 담당한다.

경찰청은 중앙단위에 별도의 수사조직을 운영하고 있는데, 주로 사이버테러 대응, 국제공조수사를, 지방청은 개인정보 유출, 음란·도박사이트 단속 등 인지수사를, 경

찰서는 인터넷 사기, 사이버명예훼손, 디지털 저작권 침해, 음란물 유포 등을 수사하고 있다.

4. 경찰청의 사이버수사활동 개관

가. 전문인력 채용 및 양성

(1) 민간 IT 전문가 경찰관 특채

2000년 사이버테러대응센터를 창설할 때, 수사를 전공한 경찰관에게 IT기술을 가르칠 것인지, IT 기술을 전공한 경찰관에게 수사를 가르칠 것인지에 대해 고민에 빠졌다. 전자를 선택하면 내부 인력에 대한 교육훈련을 강화해야 하고, 후자를 선택하면 IT기술 전공자가 부족한 만큼 외부에서 인력을 충원해야 한다는 결론에 도달하게 된다. 결국 컴퓨터·전산은 전문성이 깊고, IT기술의 발달이 매우 빠르기 때문에 비전공자의 캐치업(Catch-up)에는 한계가 있으며, 설령 내부 인력이 전산·컴퓨터 전공자라 하더라도 현장경험이 없다면 수사의 전문성을 높이는 것이 곤란하다고 판단하여 민간 IT 전문가를 특채하기도 결정하였다. 이렇게 도입된 사이버수사요원 특채제도는 민간 IT 분야에서 3년 이상 근무한 경력자 등을 대상으로 ① 해킹·악성코드 분석, ② 디지털 포렌식, ③ 시스템·네트워크 엔지니어링, ④ 데이터베이스, ⑤ 무선통신, ⑥ 프로그래밍 등 6개 분야로 구분하여 매년 경장급으로 20여명을 선발하고 있다. 사이버수사요원 특채자들은 2000년부터 2009년까지 매년 15~48명씩 총 209명이 임용되어 현재 전국 경찰관서에서 사이버수사 및 디지털 포렌식 분야를 주도하고 있다. 2006년부터는 사회적 약자 배려 차원에서 '장애인 경찰공무원 채용계획'에 따라 매년 사이버수사요원 특별채용 시 장애인 1~2명씩을 선발하여 현재 총 7명이 근무하고 있다. 재미있는 현상은 미국에서는 수사기관에 있는 경찰관들이 대우가 좋은 민간으로 이직하고 있어 전문성 확보에 어려움을 겪고 있는 반면, 우리나라에서는 IT 경험을 가지고 있는 30대~40대의 숙련된 엔지니어들이 고용이 불안한 민간보다는 연봉은 작지만 안정적인 공직을 선호하고 있어 특채제도를 통해 우수인력이 유입되고 있다는 점이다.

(2) 연구직 특채

경찰관인 사이버 특채자는 IT기술 분야 전문인력이지만 승진 등의 요인에 의해 경찰관서 간, 부서 간 인사발령이 잦고, 수사업무에 전종하고 있어 해킹·DDoS 공격 등 전문기술에 대한 심도 있는 연구를 진행하는데 한계가 있다. 이러한 문제를 해결하기 위해 2006년에 박사급 등으로 연구직 공무원을 채용하였고, 해킹·악성코드 분석, 디스크 복구 및 분석, 모바일 포렌식, 물리적 복구, 압수수색 지원 및 첨단 수사기법 개발 등의 업무를 수행하고 있다. 또한 새로운 기술을 즉시 흡수하기 위하여 일반계약직도 선발하여 운영하고 있다.

(3) 교육기관 직무교육

경찰수사연수원에서는 사이버범죄수사과정(90명), 디지털증거분석전문과정(40명), 해킹범죄수사전문과정(20명) 등 총 3개 과정 연간 150명을 교육하고 있다.[82] 사이버범죄수사과정은 사이버수사요원을 대상으로 컴퓨터·네트워크 기초, 인터넷추적기법, 디지털증거 압수수색 절차, 사이버범죄 판례연구, 유형별 수사기법, 공판정진술요령 등 28개 과목을 가르치고 있다.

해킹범죄 수사전문과정은 Buffer overflow 이해, Anti-reversing 이해, packing과 unpacking, 악성코드 및 무선해킹 분석실습 등 24개 과목 140시간을 교육하며, 디지털증거분석전문과정은 파일시스템 분석, 휘발성 증거수집분석, 증거분석 소프트웨어(Encase) 이용한 분석기법, 증거능력 관련 형소법 연구, 휴대정보기기 분석기법 등 총 22과목 140시간을 교육하고 있다. 특히 디지털증거분석전문과정과 해킹범죄수사전문과정은 이수 후 일정한 자격시험을 거쳐 전문가 인증을 수여하는 제도를 운영하고 있다.

경찰대학에서는 경감, 경정, 총경급 기본교육과정에서 중간간부로서 기본 소양을 갖출 수 있도록 사이버범죄수사에 대한 교육을 실시하고 있고, 경찰대학생을 대상으로 사이버법과 사이버범죄수사론을 가르치고 있다.

중앙경찰학교에서는 사이버수사요원으로 특채된 경찰관을 대상으로 총 24주간 교

82) 경찰청, 2010년 경찰교육훈련계획.

육을 실시하고 있다. 중앙경찰학교는 경찰관으로서 기본소양을 교육하는 기관으로서 경무, 생활안전, 수사, 경비훈련, 교통, 정보·보안, 체포술 등 총 32개 과목을 가르치고, 사이버수사요원 특채자에게는 사이버범죄의 법률, 수사기법 등 과정특화 수업에 23시간을 할애하고 있다.

(4) 국내외 민간위탁교육

경찰수사연수원에서는 사이버범죄 수사요원을 양성하는 교육인 반면, 민간위탁교육은 사이버테러 핵심인력을 양성하기 위한 교육이다. 민간위탁교육은 크게 해킹·악성코드 분석, 디지털증거분석 등 2개 과정에 연간 70~100명을 실시하고 있으며 일부는 미국 등 해외 교육기관에 파견을 보내어 악성코드 분석, 디지털포렌식 기법을 학습하도록 하고 있다.

나. 신고접수 및 단속체계

(1) 사이버범죄 24시간 접수 체제 운영

경찰청에서는 사이버범죄 신고민원 시스템(www.ctrc.go.kr)과 신고전화(02-3939-112)를 운영하고, 컴퓨터를 전공한 수사경험자를 전담요원으로 배치하여 24시간 신고민원을 접수하고 있다. 신고민원은 2008년 151,432건, 2009년 158,511건, 2010년 9월 현재 128,951건으로 증가 추세에 있고 인터넷사기와 해킹·악성코드 범죄가 가장 많은 비중을 차지하고 있다.

표 25 사이버범죄 신고민원 접수현황

(단위 : 건수)

구 분	총 계	해킹 악성코드	인터넷 사기	불법 사이트	개인정보 침해	사이버 폭력	디지털 저작권
2008년	151,432건	43,954건	50,362건	5,492건	27,659건	22,541건	1,424건
2009년	158,511건	43,800건	69,974건	6,516건	22,763건	13,975건	1,483건
2010.9월	128,951건	37,841건	57,031건	5,296건	16,864건	10,833건	1,086건

(2) 다수 피해사건 책임수사관서 지정제도 운영

사이버범죄는 짧은 시간에 대수의 피해자가 발생하고 피해의 확산속도가 빠르며 관할이 중복되는 경우가 많다. 악성 프로그램이 유포될 경우 순식간에 수 만명이 감염될 수 있고, DDoS 공격으로 인한 피해도 전국적으로 다수의 시스템에서 발생할 수 있다. 이러한 관할의 중복 문제를 해결하기 위해서 특정 경찰관서를 지정하여 수사하도록 하는 책임 수사관서 제도를 운영하고 있다. 대상범죄는 주로 악성 프로그램 유포, DDoS 공격, 인터넷사기, 특정 저작물 유포 등이 여기에 해당한다.

(3) 각급 관서별 특화된 단속활동 전개

매년 사이버범죄에 대한 정밀한 분석을 통하여 범죄발생이 급증하거나 사회적으로 이슈가 되는 범죄에 대한 특별단속을 실시하고 있다. 경찰청에서는 주로 해킹·DDoS·봇넷 등 기술적 전문성을 요하는 사건과 국제공조와 관련된 사건을 수사하고, 지방청에서는 해킹, DDoS, 악성 프로그램 유포범죄 뿐만 아니라 음란·도박사이트 등에 대한 인지위주의 수사활동을 전개하며, 경찰서에서는 사이버명예훼손, 디지털저작권, 개인정보침해, 인터넷사기 등에 대한 수사를 하고 있다.

다. 첨단시설 및 장비 확충

(1) 디지털증거분석실

정보통신기술(IT)이 보편화 되면서 범죄수사에서 디지털증거는 점차 중요해지고 있다. 컴퓨터·휴대폰·CCTV 등 디지털기기에 저장된 각종 정보는 용의자 추적단서, 범행증거를 발견하는데 결정적인 역할을 하고 있다. 해킹·개인정보 유출 등 사이버범죄뿐만 아니라 살인, 성폭력, 불법선거, 뇌물, 변사, 실종 등 모든 범죄수사에 활용되면서 디지털증거분석 매체수는 계속하여 증가하고 있다.

표 26 디지털증거분석 실적

(단위 : 매체수)

구 분	2005년	2006년	2007년	2008년	2009년	2010.10월
매체수	274건	1,849건	2,930건	4,272건	5,547건	4,412건

디지털증거가 휘발성과 가변성이 강하다는 점과, 공판중심주의 강화, 배심제 도입 등 사법환경의 변화 등을 감안할 때 법정에서 디지털증거의 증거능력에 대한 다툼은 계속하여 증가할 것이다. 최근 대법원은 일명 일심회 사건에서 법원감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 증거능력을 인정할 수 있다고 판시한 바 있다.[83]

이에 따라 경찰청은 2004년과 2010년 두 번에 걸쳐 디지털증거분석실을 확충하였고, 전국 지방청에는 2007년부터 2009년까지 3년간 총 23억원을 투입하여 디지털증거분석실을 구축하여 전문역량을 확충하였다. 이곳에서는 하드디스크, USB, CCTV 등의 디지털매체에 대한 분석 활동을 지원하고 있다. 그러나 아직까지 우리나라에는 디지털증거분석 프로그램의 신뢰성을 평가할 수 있는 인증제도나 조작자의 전문적인 기술능력을 검증할 수 있는 자격제도가 정착되어 있지 않아 신뢰성과 전문성을 제도적으로 증명하는 데는 한계가 있다.

(2) 해킹·악성코드 분석실

해킹·DDoS 공격이 국가안보를 위협함에 따라 공격도구나 악성코드를 분석하여 공격구조, 공격루트, 피해양태를 밝혀내고 공격진원지를 신속하게 역추적하여 용의자를 검거하거나 공격을 차단하는 것이 중요해지고 있다. 최근 스마트폰의 급속한 확산과 더불어 모바일 악성코드가 등장하면서 공격의 위험성은 더해가고 있다.

경찰청에서는 이에 따라 해킹·악성코드 분석실을 구축 중에 있으며 이를 통하여

83) 대판 2007. 12. 13, 2007도7257 판결.

악성코드 수집, 분석, 검증, 관리를 통하여 각종 공격에 적극 대응할 수 있는 기반을 마련하고 있다. 공격에 대한 재연을 위하여 피해 시스템과 유사한 시스템을 구축하고 폐쇄된 네트워크를 설계하여 해킹·악성코드가 실제 환경에서 어떻게 동작하는지 악성코드의 감염경로, 피해 정도는 어느 정도 인지를 확인할 수 있도록 하였다. 재연과 동시에 영상으로 촬영하여 법정에 증거를 제출할 수 있는 체계도 갖출 예정이다. 또한 수집된 해킹도구, 악성코드를 데이터베이스화하여 추후 동일하거나 유사한 악성코드 발견 시 동일범 소행를 판단하고, 용의자 검거 시 여죄 추궁의 증거로 활용할 수 있도록 할 계획이다.

(3) 모바일 분석실

휴대폰에 이어 스마트폰의 보급이 급속도로 확산됨에 따라 신종범죄의 발생에 대한 많은 우려가 제기되고 있다. 특히 모바일 기기에는 동영상이나 사진, 문자메시지, 통화내역, 스케줄 관리, 주소록, 이메일 등 다양한 정보가 수록되어 있어 범죄수사에도 매우 중요한 단서가 되고 있으며, 범행대상이 되었을 경우에는 개인의 프라이버시 침해 등에 있어서 큰 피해를 안겨주게 된다. 스마트폰을 대상으로 한 악성코드가 등장하여 통화를 불가능하게 하거나, 자동적으로 전화를 걸어 과금을 발생시키거나 스마트폰에 대한 DDoS 공격 등 다양한 범죄 시나리오가 등장하고 있다. 사전에 이러한 범죄에 대응하기 위하여 모바일 분석실을 구축하여 각종 휴대폰, 스마트폰에 대한 데이터 획득, 악성코드 분석, 데이터 복구 등에 관한 장비를 도입하고 기법연구를 계속 진행하고 있다. 모바일 분석실은 휴대폰·스마트폰을 분석하면서 계속되는 통신행위로 인하여 데이터가 변경되는 것을 막기 위하여 전파차폐 시설을 설치하여 무결성을 최대한 보장하고 있다.

라. 유관기관 및 민간 협력

(1) 경찰관 파견제도

유관기관 협력체제를 유지하기 위하여 그동안 국정원 국가사이버안전센터와 한국인터넷진흥원에 경찰관을 파견하여 왔으나 최근에는 모두 중단되었다. 정보통신망법

과 국가사이버안전관리규정에서 해킹·DDoS·피싱 피해 발생시 방통위·국정원에 신고토록 의무화함에 따라 양 기관에 사고 정보가 집중되고 있어 범죄수사와 연계하기 위해서는 파견이 절실히 필요하다. 특히, 방통위(한국인터넷진흥원)는 개인정보·스팸·피싱(메신저 등) 등 일반적인 사이버범죄에 대한 신고상담을 접수받고 있어 경찰 업무와도 매우 밀접하다. 2009년에 국회·언론에서 '7·7 DDoS' 등 사이버테러에 대한 기관간 정보공유가 미흡하다는 지적에 따라, 유관기관에 경찰관파견을 다시 추진할 필요가 있다.

(2) 사이버침해사고 통보제도

정보통신망법상 정보통신서비스 제공자는 한국인터넷진흥원 등에 침해사고(제56조), 속이는 행위로 인한 타인의 정보수집행위(제71조제2항), 개인정보 누출사실(제91조제1항) 등을 신고하도록 의무화하고 있다. 정보통신기반보호법 제13조에도 관리기관의 장은 침해사고가 발생하여 소관 주요 정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원에 그 사실을 통지하도록 규정하고 있다. 관련범죄는 명백한 불법행위로 특성상 피해가 광범위하고 확산속도가 빠르므로 피해 차단을 위한 조치와 함께 수사기관의 신속한 수사착수가 필요하다.

그러나 우리나라에서는 유관기관에 접수된 침해사고가 수사기관의 수사 착수 연계되는 경우가 많지 않은데, 이는 관계기관의 이해부족, 피해자의 수사 기피, 수사기관의 업무량 한계 등 다양한 이유가 복합적으로 작용하고 있기 때문이다. 우리나라뿐만 아니라 미국에서도 보안사고가 발견하더라도 법집행기관에 잘 신고하지 않고 있고, 심지어 수사기관에 신고 되었을 때의 불편함, 곤란한 상황이 생길 수 있음을 이유로 사회적 책임이 있는 침해사고 대응기관이 범죄인 침해사고를 알았을 때도 수사기관에 통보조차 하지 않는 경우도 적지 않다.[84]

미군의 경우 보안 사고를 중요도에 따라 10가지 카테고리로 분류하고 국방부 대응팀이 사고를 탐지한 경우 상위 4개 카테고리에 해당하면 즉시 수사기관에 통보하

84) 이동희 등, 앞의 보고서, 19쪽.

고 이 경우에도 원활한 수사를 위해 증거훼손을 방지하기 위한 피해시스템의 처리요령 등 처리절차에 대한 엄정한 규정을 가지고 있어서 유기적인 협력 체제를 유지[85] 하고 있는데, 이는 우리나라에 주는 시사점이 크다고 할 것이다. 또한 미국 법무부 내 'Computer Crime and Intellectual Property Section Criminal Division'이 펴낸 "Prosecuting Computer Crimes"의 Appendix B : Best Practices for working with companies에는 인터넷서비스 제공업자와의 협조적 형성에 대한 논의를 적고 있는데 ① 피해자로서의 서비스제공업자의 권리보호, ② 고위 매니저와의 상의, ③ 정보기술 스태프와의 상의, ④ 회사에의 피해 최소화, ⑤ 언론과의 관계 조정, ⑥ 수사의 진행 상황을 회사에게 필요한 범위 내에서의 공지, ⑦ 사전 협조 관계 구축(서비스 제공업자들이 신용도 하락을 우려하여 신고를 기피하는 현상 극복) 등을 유의할 사항으로 나열하고 있는데,[86] 우리나라에서 발전방안을 마련하는 데 있어 반드시 고려해야 할 항목들이다.

(3) 민간분야와 협력체제

사이버범죄에 대응하기 위하여 ISP·IDC·포털·금융 등 각종 민간사업자와 한국디지털포렌식학회, 한국정보보호학회, 한국침해사고대응팀협의회와도 기술자문, 세미나 개최 등을 통해 긴밀한 협력 체제를 유지하고 있다. 경찰은 수사과정에서 취득한 각종 보안 취약점을 민간에 피드백하여 추가적인 피해발생을 차단하고, 민간은 수사기관에 전문기술에 대한 자문을 제공함으로서 범죄를 근절하는 등 상호간 긴밀히 협력하고 있다.

경찰청에서는 더 나아가 사이버치안에 대한 국민의 공감과 사회적 관심을 고조시키고 민간 분야의 적극적인 참여를 유도하기 위하여 2008년부터 대한민국 사이버치안대상을 제정하여 일반인 및 경찰관을 대상으로 정부포상을 수여하고 있다.

85) 이동희 등, 앞의 보고서, 19쪽.

86) 이창수, "초국가적 사이버범죄에 대한 국제공조 활성화 방안과 그 선결과제", 형사법의 신동향 제21호, 2009. 9, 144쪽.

(4) 사이버명예경찰 '누리캅스'

인터넷 특성상 경찰력만으로는 사이버범죄 예방 및 단속에 한계가 있다고 판단하고, 부족한 경찰력을 보완하기 위해 인터넷에 관심이 있는 네티즌을 상대로 '누리캅스'로 위촉하여 사이버범죄에 대한 신고제보기반을 확충하였다. 누리캅스는 누리꾼의 '누리'와 'Cops(경찰)'의 합성어로 사이버명예경찰을 의미한다. 2007년 제1기가 출범한 이래 올해 제4기에 이르고 있고, 현재 전국적으로 약 884명이 활동하고 있다. 이보다 발전된 프로그램으로 미국에서는 INFRAGARD 프로그램을 운영하고 있는데 이는 사이버공격에 대한 정부와 민간부분에 정보를 제공하거나 경고를 해주는 역할을 하며, 미국에 적대적인 행위를 저지하기 위한 정보를 공유하기 위하여 기업, 대학, 정부기관 및 기타 기관들로 구성된 FBI와 민간부문의 협력체이다.[87]

5. 평가 및 개선방안

가. 사후 추적수사에서 사전탐지 및 조기대응 체제로 전환

(1) 유관기관간 사이버침해 초동조치 협력 강화

사이버침해에 대한 예방·사후복구는 국정원, 방송통신위원회, 행정안전부에서 담당하고, 수사기관은 경찰청과 대검찰청에서 담당하고 있다. 사이버공격에 관해서는 정보통신망법, 정보보호기반보호법, 전자정부법, 국가사이버안전관리규정(대통령령) 등 다수의 법률이 규제하면서 기관 간 임무가 중첩되는 경우가 발생하기도 한다. 따라서 다양한 기관이 존재하고 있음에도 실제 사이버위기가 발생하였을 경우 각 기관의 책임과 역할이 불분명하다.[88] 사이버공격이 국가안보에 대한 위협이 될 수 있는 '가능성'이 있다고 하여 사이버공격에 대한 사전·사후적 대응 전부를 국가안보의 차원에서 접근할 수는 없다. 민주사회에서 국가안보 기타 공익에 대한 위협을 빌미로

87) 현대호, "미국의 사이버위기 관련 법제의 현황과 전망", 법학논총 제33권 제1호, 2009, 5쪽 (http://www.infragard.net 참조).

88) 김도승, 앞의 글, 36쪽.

시민의 기본권을 부당하게 침해할 수 없고 문제의 핵심은 위협의 '실존성'에 있다.[89] 사이버테러는 정치·사회적 동기가 파악되어야 하고, 사이버전은 공격을 감행하는 국가가 특정되어야 하는데 추적과 조사를 선행하지 않고는 알아낼 수 없다.

정보화시대 이전에 물리적 범죄의 문제는 많은 부분을 법집행기관에서 담당하였고, 그렇지 않은 경우에도 영역간의 역할분담은 상대적으로 용이하였지만 사이버공간에서 불법행위는 다양한 방식으로 접근이 가능하며 기존의 대응방식으로는 한계가 있다.[90] 그러나 경찰은 범죄의 의심이 있다면 국가적인 문제인지 사적인 문제인지 혹은 테러 공격인지 금전적 이익 목적인지 심지어 국가정보를 탈취하기 위한 것인지 등에 관계없이 개입이 정당화되기 때문에 사고대응에 있어 정당성을 가질 수 있다.[91]

따라서 경찰은 사건 초기에 더욱 적극적으로 참여하여 사실관계를 정확히 밝히는 노력을 하고, 밝혀진 사실을 유관부서에게 적시에 통보하여 필요한 조치를 취할 수 있도록 긴밀한 협력 체제를 구축해야 한다. 이를 위해 침해사고 대응기관 간 사고의 중요도·시급성에 따라서 상호간 통보할 수 있는 프로세스를 만들고, 수사기관은 증거가 훼손되는 것을 미연에 방지하기 위하여 피해시스템에 대한 증거 취급요령을 제공할 필요가 있다.

(2) 사이버 공격정보 분석을 통한 사전탐지·조기대응 역량 확충

2003년 1·25 대란은 당시 어떠한 국가기관도 이를 사전에 탐지하지 못했고, 경찰청에서도 미국, 호주 경찰청 등과 공조수사를 진행했지만 용의자를 추적하는데 실패했다. 2004년 국가기관 해킹사건은 방위산업체 관계자의 신고로 수사가 시작되었으나 이미 국가기관은 모두 해킹 피해를 당한 상태였고 중국 측의 비협조로 용의자를 검거하지도 못했다.

2009년 7·7 DDoS 사건 역시 국가정보원, 방송통신위원회, 한국인터넷진흥원 등에서 사전에 탐지하지 못했고, 추후 경찰의 수사결과에 의해 공격지를 중국 소재 북한 체신성 산하기관으로 밝혀냈지만 여전히 용의자는 검거하지 못하고 있다. 최근에

89) 이동희 외, 앞의 보고서, 18-19쪽.
90) 이동희 외, 앞의 보고서, 19쪽.
91) 이동희 외, 앞의 보고서, 19쪽.

우리나라에서 발생한 사건 전부는 수사기관을 비롯하여 침해사고 대응기관을 불문하고 모두 사전에 탐지하지 못했고, 이로 인하여 사고 발생시 각 기관에서 제각각 대응하면서 많은 혼란과 문제점이 야기되었다.

따라서 앞으로는 유관기관과 정보교류, ISP의 이상 트래픽 분석, 해킹·DDoS 공격정보 분석, 국제사회 해킹조직 동향, 해킹·악성코드 유포실태, 세계 각국의 수사조직과 정보교류 등을 통해 사이버공격을 사전에 탐지할 수 있는 역량을 확충하고 사이버공격정보에 대한 분석활동과 이에 대한 구체적인 정보수집 방법에 대해 고민을 해야 한다.

나. 사이버범죄 수사 및 대응 관련 법규 정비

(1) 사이버범죄 처벌법규 정비

우리나라는 1995년 형법개정을 통해 컴퓨터범죄에 대처할 수 있는 규정을 신설하였지만, 이러한 규정들은 분명 은행의 대형 컴퓨터와 같이 독립된 컴퓨터 환경을 전제로 한 것이었고 지금은 그 당시 입법자가 예상하지 못했던 새로운 상황이 전개되어 버렸다.[92]

우리나라는 컴퓨터 이용의 역기능에 대처하기 위한 방안으로 각 부처별로 상황에 따라 필요할 때마다 특별법을 제정하는 방법을 선택했다.[93] 그 이유는 그간 정책입안자 및 입법자가 사회 현실의 변화에 따라 새로이 등장하는 범죄현상에 대해 충분한 형법이론적·형사정책적 고민 없이 진압위주의 강경한 법정책 기조 위에 임기응변식으로 손쉽게 법을 만들어 적용해온 데에 있다.[94] 이러한 정부의 대처방법은 각 법률간 형벌의 불균형, 법체계상의 문제, 다수의 유사한 규정이 여러 법률에 산재되어 있는 문제점 등을 야기하였다.[95]

미국, 독일, 영국 등 선진 각국은 대체로 기본적으로 형법에 의하여 컴퓨터범죄를 규율하고, 새로운 범죄에 대해 형법에 보충하는 입법정책을 펴고 있다. 다만 미국의

92) 이정훈, "사이버범죄에 관한 입법동향과 전망", 사이버커뮤니케이션학보 통권 제20호, 2006. 4, 234쪽.
93) 유석준, 앞의 글, 1쪽.
94) 서보학, "인터넷상의 정보유포와 형사책임" 형사정책연구 제12권 제3호, 2001 가을, 10쪽.
95) 유석준, 앞의 글, 2쪽.

경우에는 OECD의 권고를 받아 들여 데이터의 비밀성, 무결성, 가용성을 보호하고, 해킹이나 바이러스 유포 등 행위로부터 국가정보기반시설을 보호하기 위해 1996년 국가정보기반보호법(NII)를 제정하였다.[96]

실무적으로는 해킹, DDoS, 피싱, 악성프로그램 유포와 관련된 범죄는 모두 정보통신망법, 정보통신기반보호법으로 처벌하고 있고, 형법에 규정되어 있는 전자기록 비밀침해죄(제316조 제2항), 전자기록 손괴죄(제366조), 컴퓨터 업무방해죄(제314조 제2항), 공전자기록 위작·변작죄(제227조의2), 사전자기록 위작·변작죄(제232조의2), 공무상 비밀침해죄(제140조 제3항) 등은 거의 활용되지 않고 있다.

사이버범죄에 대한 형법규정에 대한 정비방안은 사이버범죄 처벌규정을 하나의 특별법으로 제정하는 방안[97]과 처벌규정을 원칙적으로 형법에 두고 특별한 이유가 있는 경우에만 예외적으로 특별법에 규정하는 방안[98]이 제시되고 있다.[99] 형법 전에 규정되어야 한다고 주장하는 근거는 수범자가 금지된 내용을 용이하게 인식할 수 있어야 규범준수가 가능[100]하고, 사이버범죄에 대한 처벌이 특별한 것이 아니라 일반적이라는 것을 국민들에게 인식시킬 수 있으며 이를 통해 일반 예방적 기능이 더 효과를 나타낼 수 있기 때문이다. 또한, 해당 행위에 대한 처벌의 정도를 다른 범죄들과 비교·검토함으로써 처벌범위에 대한 정당성을 획득하고 다른 범죄와의 체계와 형평성을 유지할 수 있기 때문이다.[101] 만약 사이버범죄에 대한 특별법을 제정할 경우에는 오프라인 범죄체계와 균형, 첨단기술의 특성을 고려한 절차법적 조항 신설, 온라인 서비스제공자의 책임조항 신설, ISP에 대한 정보통신망에 대한 기술적 대응장치 의무화, 보호관찰·사회봉사명령·수강명령 제도 도입 등을 고려해야 할 것이다.[102]

96) 유석준, 앞의 글, 19쪽.

97) 원혜욱, "인터넷범죄의 특징과 범죄유형별 처벌조항", 형사정책연구 제11권 제2호, 2000, 113쪽; 곽병선, "사이버범죄 예방을 위한 법제도적 해결방안 - 가칭 '사이버범죄 특별법' 제정 논의를 중심으로 -", 원광법학 제24권 제3호, 2008, 128-136쪽.

98) 강동범, 앞의 글, 54쪽; 오영근 "인터넷범죄에 관한 연구", 형사정책연구 제14권 제2호, 2003, 330쪽 참조.

99) 전지연, "사이버범죄의 과거, 현재 그리고 미래", 형사법연구 제19권 제3호, 2007 가을, 24쪽.

100) 강동범, 앞의 글, 46쪽.

101) 전지연, 앞의 글, 25쪽.

102) 곽병선, 앞의 글, 132-136쪽.

사이버범죄의 태양은 이미 상당 부분 유형화 되어 형법 전에 포함시키는데 기술적인 문제가 없어 보이고, 다른 범죄와 형량에 대한 균형을 맞추기 위해서라도 원칙적으로 형법에 두어야 하고,[103] 특별법에 두어야 할 필요성이 있는 경우에만 예외적으로 특별법을 제정·개정하는 바람직해 보인다. 어떠한 경우이든 보호법익과 법정형 및 용어에 있어 기존 형벌법규와의 체계성을 잃지 않도록 하여야 함은 당연하다.[104]

(2) 주요 기반시설 사이버침해 피해에 대한 수사기관 고발 의무화

형사소송법 제234조 제2항에 공무원은 그 직무를 행함에 있어 범죄가 있다고 사료하는 때에는 고발하여야 한다고 규정하고 있으므로 침해사고에 대하여 공무원이 이를 통보하지 않은 것은 형사소송법 위반이라고 볼 수 있다.[105] 국가사이버안전관리규정(대통령훈령 제222호) 제13조에서 국가정보원장은 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다고 선택사항으로 규정되어 있으나, 이는 대통령령으로 법률인 형사소송법과 대등한 지위에 있다고 볼 수 없다. 정보통신기반보호법 제13조에 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원에 그 사실을 통지하여야 한다고 규정되어 있다.

따라서 일반적인 해킹, DDoS 공격 등은 예외로 하더라도 국가기관 및 공공기관, 주요기반시설에 대한 사이버공격으로 인한 피해가 발생할 경우에는 수사기관에 통보하는 것을 의무화할 필요가 있다. 특히 정보통신기반보호법 제8조에 따른 주요 정보통신기반시설 즉, 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 등에 대해서는 반드시 수사기관에 고발하도록 의무화하여야 한다.

103) 오영근, 앞의 글, 330쪽.
104) 강동범, 앞의 글, 50쪽.
105) 이동희 외, 앞의 보고서, 39쪽.

(3) 한국인터넷진흥원의 WHOIS 정보 정확성 제고

현재 PC방에 할당된 IP정보를 WHOIS상에서 조회할 경우 PC방에 대한 정확한 위치가 나타나지 않고 있다. 따라서 범죄 용의자를 신속하게 검거할 수 없게 되고, 용의자는 이를 알고서 PC방에서 계속 범행을 하게 되는 악순환이 반복되고 있다.

PC방과 같은 공개된 장소의 IP주소는 한국인터넷진흥원에서 제공하는 WHOIS 정보에 정확하게 등록할 필요가 있고, 인터넷주소자원에관한법률을 개정하여 이를 의무화할 필요가 있다. ISP업체들은 PC방 IP가 공개될 경우, ISP간 영업 마케팅 경쟁이 일어날 수 있다고 우려하고 있으나, 범죄수사의 관점에서 바라볼 때 그리 큰 문제는 아니며 더 나아가 우리사회의 안전망을 확보하기 위해서라도 반드시 개선되어야 한다. PC방 IP 주소 정보의 정확성 문제는 꼭 수사기관만의 문제는 아니고, 민간에 있어서도 PC방에서 갑작스런 해킹공격을 받을 경우에 IP 위치를 조회하여 공격을 차단시킬 수 있기 때문에 민간의 공격차단 등 자율적인 문제 해결에도 기여하게 된다.

(4) 디지털증거 압수수색 및 증거처리 관련 법률정비

우리나라 형사소송법에서 압수수색 대상과 이를 수집하기 위한 영장의 발부기준 등에 관한 제반규정은 1954년 제정 당시 이후 현재까지 단 한차례도 변경되지 않았다.[106] 이로 인하여 디지털 증거에 대한 법률적 정비는 매우 늦어지고 있다. 다행히 국회 조영택 의원 대표 발의안, 이종걸 의원 대표 발의안, 박영선 대표 발의안, 이주영 의원 대표 발의안 등이 제출되어 국회 차원에서 논의가 전개되고 있다.[107]

형사소송법과 통신비밀보호법과 규제대상에 대한 재정립, 디지털증거의 대물적 강제처분 대상여부, 전자우편의 압수수색 기간설정, 원격지 압수수색 문제, 저장매체의 물리적 압수원칙이 아닌 복제·출력을 우선적인 원칙으로 하는 문제, 디지털증거 보

106) 설민수, "인터넷서비스제공자를 통해서 본 제3자 보유정보에 대한 영장주의의 실효성", 법조 제635호, 2009. 8, 165쪽.

107) 2009. 12. 7. 조영택 의원 대표발의(의안번호 6880); 2009. 5. 13. 이종걸 의원 대표발의(의안번호 4839); 2009. 6. 23. 박영선 의원 대표발의(의안번호 5246); 2009. 4. 1. 이주영 의원 대표발의(의안번호 4366).

전명령 및 제출명령 제도, 디지털증거의 전문법칙 등 증거능력, 위법수집 증거능력 등 많은 논점들에 대한 정리가 필요하다.

다. 사이버수사 전담조직 및 전문성 확보

(1) 전담조직 위상 강화

현재의 과 단위의 조직을 국 단위로 격상시키고 책임자의 계급도 경무관급 이상으로 격상시키는 방안을 생각할 수 있고, 각 지방청에도 총경급 간부를 책임자로 임명함으로써 신속한 공조체제를 유지하도록 하여야 한다.[108] 경찰청은 1995년 이후 꾸준히 전담조직과 인력을 확충하였으나, 여전히 부족하다. 2003년 1·25 대란을 계기로 국정원은 국가사이버안전센터를 창설하였고, 2009년 7·7 DDoS 사건을 계기로 국방부는 사이버사령부를 창설하였음에도 불구하고, 경찰청은 관련범죄가 계속하여 급증하고 있음에도 2000년에 창설한 조직을 그대로 유지하고 있다.

국제해커에 대한 동향, 공격정보 분석 및 기법탐구, 네트워크 추적기법 연구, 국제적 봇넷 범죄 척결을 위한 국제사회 커뮤니티 활동 등 새로운 업무를 수행하기 위해서라도 조직 확충이 필요하다. 이번 G20 정상회의를 기점으로 2012년 핵안보 정상회의 등 국제회의가 계속하여 개최될 경우 사이버테러에 대한 위협이 더욱 증대할 것이며, 국가차원의 스마트 그리드[109]가 보편화되면 해킹공격은 단순히 시스템, 네트워크에 머물지 않고 스마트폰을 넘어 전기자동차, 전기, 가스, 텔레비전 등 모든 영역으로 급속하게 확대될 것이다. 이러한 업무를 효율적이고 선제적으로 수행하기 위해서 조직의 위상은 강화되어야 한다.

108) 우제태, "사이버 범죄의 대응방안에 관한 연구", 경찰연구논집 제1호, 한국경찰이론과실무학회, 2007, 181쪽.

109) 스마트그리드란 기존 전력망(발전→송배전→판매)에 정보기술(IT)을 접목하여 전력공급자와 소비자가 양방향으로 실시간 정보를 교환하여 에너지 효율을 최적화하는 차세대 전력망이다(F. Sissine, "Energy Independence and Security Act of 2007 : A Summary of Major Provisions", CRS Report for Congress, 2007. 12. 참조).

(2) 민간 IT 전문가 경찰관 특채 확대

경찰청은 그간 민간 IT 전문가를 경찰관과 연구직으로 특채하여 전문인력을 확보하였고, 수사경과제와 임용 후 사이버수사부서에서 5년간 의무 복무하도록 하여 기술에 대한 전문성을 축적하였다. 이들의 전문성을 바탕으로 2004년 국가기관 해킹사건, 2009년 7·7 DDoS 사건 모두 외부 전문가의 도움 없이 자체적인 기술역량으로 공격 진원지를 밝혀낼 수 있었다.

그러나 첨단 IT 기술이 급속도로 발전함에 따라 갈수록 고도의 전문인력이 필요하게 되는데 현행 경장급 특채만으로는 한계가 있다. 단계적으로 특채계급을 경사, 경위급까지 상향시켜 고급인력을 꾸준히 특채해야 한다.

현재 사이버특채자가 약 209명이 근무하고 있지만 전국 경찰관서에 모두 배치하기 위해서는 아직도 많은 인력이 필요한 만큼 채용인원을 매년 20명 수준에서 대폭 늘려 선발하여 전국 경찰관서에 배치하여야 한다.

민원인은 수사관이 컴퓨터에 대한 전문지식이 없다는 이유만으로 컴퓨터 능력뿐만 아니라 수사능력까지도 인정하지 않기 때문에 기술 전문성을 가지고 있는 수사관을 최대한 배치하여야 한다.

(3) 사이버테러 전문수사관 양성

그간 경찰수사연수원 교육과정과 국내외 민간위탁교육으로 수사요원의 전문성은 충분히 확보하였으나, 사이버테러 수사를 위한 고도의 기술인력을 체계적으로 양성하는 데는 미흡했다. 사이버테러 수사를 위해서는 IT기술, 외국어, 범죄수사에 대한 전문성을 모두 가지고 있어야 하는데 아쉽게도 경찰청에는 그러한 능력을 가지고 있는 수사 인력이 많지 않다. 사이버테러는 기본적으로 국제공조를 전제로 하는 수사활동으로 해킹·DDOS 공격 등 기술 분야에 대한 전문성이 없거나 외국어 능력이 부족할 경우 신속한 수사 활동을 전개하는데 한계가 있다.

따라서 사이버테러 전문수사관을 양성하기 위해서는 해외 위탁교육 등 중장기 전문교육을 통하여 우수인력을 적극 양성하고, 필요시에는 국내 대학에 맞춤형 석사과정을 개설하여 필요한 분야에 대해 체계적이고 종합적인 교육이 이루어질 수 있도록 해야 한다. 또한 최근 UN·OECD·ITU·인터폴 등 국제기구에서 사이버범죄·테러

에 대한 논의가 증가하고 있으므로 한국경찰을 대표하여 의사결정에 참여할 수 있도록 국제 사이버범죄 전문가를 양성하는 것도 중요하다.

라. 유관기관 및 민간분야 협력

(1) 유관기관 경찰관 파견제도

과거에는 국정원과 한국인터넷진흥원에 경찰관이 파견을 나가서 수사기관에서 협조할 사항, 신고 받은 사건에 대한 법률검토 및 경찰통보에 대한 판단 등의 역할을 수행했으나 현재는 파견관이 없어 유관부처와의 협력이 과거만 같지 않다. 사이버테러는 발생 초기에 공격자를 신속하게 추적하는 것이 어렵고 누구의 소행인지에 대한 판단이 쉽지 않아 수사기관인 경찰의 역할이 중요하다. 따라서 국정원 국가사이버안전센터, 방통위의 한국인터넷진흥원뿐만 아니라 행정안전부 정부통합전산센터, 국방부 사이버사령부 등으로 경찰관을 파견시켜 유관부처 간 정보교류를 활성화해야 한다.

(2) 민간의 신고기피 해소방안 강구

민간기업은 수사기관에 신고하였을 경우 언론보도로 인한 기업의 이미지, 신뢰도 하락을 우려하고 있기 때문에 사이버범죄에 대한 피해를 받았을 때 신고를 기피하고 있다. 그러나 불이익이 형사사법이 의도하는 공적이익보다 크지 않다면 사법정의 실현에 협력해야 하는 것이 건전한 시민의식이다.[110] 프라이버시와 보이지 않는 자산에 대한 침해가 있기 때문이다. 경찰에서는 민간에 대한 수사과정에서 확보한 정보제공을 하나의 서비스로 개발하여 제공하고, 민간에서는 이를 활용하여 추가적인 범죄가 발생하지 않도록 조치해야 할 것이다.

(3) 사이버치안 거버넌스 강화

사이버범죄 예방은 경찰 혼자서만 할 수 없다. 사이버범죄 예방은 무엇보다도 시스템 정책 및 보안에 대한 의사결정권자의 역할이 매우 중요하다. 시스템의 운영방

110) 이동희 외, 앞의 보고서, 20쪽.

식을 개선함으로써 많은 범죄를 예방하고, 용의자를 검거할 수 있다. 범죄예방 주체를 수사기관에서 ISP, IDC, 포털, 금융 등 다양한 사업자까지 포함한 사이버치안 거버넌스를 강화할 필요가 있다. 실례로 인터넷 게시판에 악성코드를 올릴 때 IP를 표시하게 하거나, 메신져 피싱에서 외국 IP에서 접속한 경우 경고창이 뜨도록 하거나 네이트온 등 특정계정에 ID가 다중으로 접속될 경우 알림이 되도록 하는 것이 좋은 예라고 할 것이다.

민간 참여를 적극적으로 유도하기 위하여 경찰에서 보유하고 있는 각종 통계와 정보 제공을 적극적으로 하고, 대한민국 사이버치안대상과 같은 민간의 참여를 유도할 수 있는 인센티브 제도를 지속적으로 개발해야 한다.

최근 미국 FBI에서 개최한 ICCS 2010에서는 구글, Facebook, Paypal 등의 관계자들은 주제발표를 통해 자신의 회사에 제공하는 서비스를 설명하고, 이를 활용하여 어떠한 범죄가 일어날 수 있는지, 수사할 때 구글이 어떠한 정보를 제공해 줄 수 있는지, 수사상 어떠한 팁이 있는지 등에 대해서 설명하고 경찰의 적극적인 수사를 요청하였다.[111] 우리나라도 이처럼 민간기업과 밀접하게 관계하면서 사이버범죄를 근절해 나갈 필요가 있다.

(4) 사이버범죄 예방에 관한 수익자 부담원칙 도입

해킹범죄의 경우 개인은 ID 도용이지만, 기업은 시스템 다운이나 마비의 피해가 발생할 수 있고, 피싱도 개인이 아닌 기업을 상대로 하고 있다. 심지어 명예훼손의 경우도 과거에는 개인을 대상으로 하였지만, 최근에는 기업뿐만 아니라 촛불집회와 천안함 침몰사건 등까지 확산되고 있다. 저작권의 피해자도 기업이고, DDoS 공격의 피해자도 기업이다. 수사기관의 사이버범죄에 대한 대응전략 종전에 포괄적 국민들의 개념에서 특정화된 기업 중심으로 기업의 서비스를 분석하고 그 서비스에 따른 범죄발생요인을 파악하는 것도 중요하다.

사이버범죄에 대한 이론연구와 각급 형사사법기관의 감사활동에 대한 기업의 지

111) 미국 FBI 및 포담대학의 주관으로 개최된 2010년 ICCS 행사에서 구글사의 Trust & Safty Manager인 Cory Louis가 “How do criminals make money from Google?”이라는 제목으로 발표한 내용을 요약하였다(경찰청 내부자료 활용).

원이 확대되어야 할 것이다.[112] 물론 범죄수사와 예방활동에 관한 예산은 국가가 전담하는 것이 원론적으로 옳다. 그러나 국가의 재정상태로 인하여 예산확보가 쉽지 않고, 국민들의 조세부담을 늘려야 하는 문제가 발생할 수 있으므로 수익자 형태의 구조가 있는 분야에 대해서는 민간의 비용지원을 이끌어 내는 것도 하나의 방법이다. 단순 수익자 개념이 아니라 기업수익의 원천이 되는 고객보호 차원에서 수익자의 비용부담을 요구할 수 있을 것이다. 수혜자가 비용을 부담하는 조건의 용역경비 사업이 번창하고 있음을 상기하면 기업이 수사기관의 활동비를 분담하는 방안이야말로 기업의 미래와 안전을 보장받는 지름길로 여겨진다.[113] 우리나라에서는 온라인 게임회사에 의한 각종 ID 도용, 아이템 거래 등의 범죄에 대해서 수익자 부담 원칙을 적용해 해서 운영해 볼 수 있을 것이다.

제5절 사이버침해 대응 국제협력체계 개관

1. 국제공조 관련 조약 및 법률

가. 유럽평의회 사이버범죄 조약

유럽평의회(The Council of Europe)는 1980년경부터 사이버범죄의 문제점을 인식하고 연구를 진행해 왔고, 2001년 6월 22일 제50차 유럽 형사문제위원회에 사이버범죄 조약이 제출되어 승인을 받아 2001년 11월 8일 각료위원회에서 최종적으로 채택[114]되었고, 전문과 실체법·절차법, 국제공조 등 총 4개장 48개 조문으로 구성되어 있다.[115]

동 조약은 ① 컴퓨터 시스템·네트워크 및 정보의 오용뿐만 아니라 기밀성, 무결성, 가용성을 침해하는 행위 등을 범죄화하여 사이버범죄로부터 사회의 안전을 도모

112) 우제태, 앞의 글, 187쪽.
113) 조병인 외, 사이버경찰에 관한 연구, 한국형사정책연구원, 2000, 179쪽.
114) 유석준, "사이버범죄에 대한 외국의 입법례", 영산법률논총 제5권 제1호, 2008. 9, 18쪽.
115) 유석준, 앞의 쪽.

하고, ② 정보기술의 개발과 이용에 대한 법적 보호를 더욱 강화하고 나아가 사이버범죄에 관한 국가 간 및 기업 간 상호협력을 제고하며, ③ 사이버범죄에 대한 효과적인 처벌을 위하여 형사사건에 있어서 신속하고 원활한 국제공조 방안을 마련하고, ④ 국내적·국제적 차원에서 사이버범죄 행위에 대한 수사, 기소 및 탐지를 지원하는 동시에 신속하고 공정한 국제협력을 의무화함으로써 동 범법행위를 효과적으로 대응하며, ⑤ 컴퓨터 시스템이나 자료와 관련된 범죄의 효과적인 수사 및 기소를 위해 기존의 형사사법공조조약이나 범죄인인도조약을 보충하고, 사이버범죄의 전자증거 수집을 지원하기 위한 목적으로 제정되었다. 현재 프랑스, 이탈리아, 노르웨이, 미국 등 총 23개국이 가입서명 및 비준까지 완료하였고, 일본, 러시아, 영국, 캐나다 등 23개국은 서명을 하였으나 아직 비준절차를 완료하지 못한 상태에 있다.[116] 현재 우리나라는 동 조약에 가입할 필요성은 공감하고 있으나 동 조약의 요구에 따르기 위해 실체법과 절차법에서 많은 문제를 해결해야 하므로 아직까지 가입하지 못하고 있다.

나. UN 반초국가조직범죄 조약

UN의 반초국가범죄 조약(United Nations Convention Against Transna-tional organized Crime)은 현재 가입 및 비준절차를 완료한 국가만 해도 147개 국가에 달하고 있다. UN 반초국가조직범죄 조약에 의하면 규율대상이 되는 조직범죄를 ① 3인 이상이 ② 직·간접적인 경제적·유형적 이득을 얻을 목적으로 ③ 하나 또는 그 이상의 중범죄[117] 또는 조약이 정하는 범죄[118]를 저지르기 위하여 ④ 일정기간 이상 유지되는 집단을 의미한다고 규정하고 있다.[119] 해킹·DDoS 공격등은 조직범죄의 성향을 띠고 있고, 협박·공갈을 수반하면서 경제적 이익을 목적으로 하고 있어 반초국가범죄라고 정의할 수 있다. 법정형을 보더라도 정보통신망법 제71조 제9호

116) 이창수, 앞의 글, 108쪽.

117) United Nations Convention Against Transnational organized Crime, Article 제2조 (b)에 이하면 중범죄(Serious Crime)라 함은 법정 최고형이 징역 4년 이상으로 구성된 범죄를 의미한다.

118) 조약이 정하는 범죄란 본 조약이 가입 당사국들을 상대로 반드시 형사처벌 규정을 두도록 강제한 범죄로서 ① 범죄조직에의 참가, ② 자금세탁, ③ 부패범죄, ④ 사법방해 등 4개 조항이 있다.

119) United Nations Convention Against Transnational organized Crime, Article 2(a).

악성 프로그램을 전달 또는 유포한 자, 동조 제10호 정보통신망에 장애를 발생하게 한 자(DDoS 공격), 동조 제11호 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자(해킹) 등은 모두 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있어 동 조약에서 말하는 중범죄의 개념에 포함된다.

따라서 사이버범죄 근절을 위한 유럽평의회의 사이버범죄 조약 가입이 실체법, 절차법 개정을 수반해야하는 문제가 있어 일정한 시간이 필요하다면 UN의 반초국가조직범죄 조약에 가입하는 방안을 검토해 볼 수 있을 것이다.

다. 국제형사사법공조법

국제형사사법공조법 제1조에는 형사사건의 수사 또는 재판과 관련하여 외국의 요청에 따라 실시하는 공조 및 외국에 대하여 요청하는 공조의 범위와 절차 등을 정함으로써 범죄를 진압하고 예방하는 데에 국제적인 협력을 증진함을 목적으로 한다고 규정하고 있다. 동법 제5조에서는 공조의 범위는 ① 사람 또는 물건의 소재에 대한 수사, ② 서류·기록의 제공, ③ 서류 등의 송달, ④ 증거 수집, 압수·수색 또는 검증, ⑤ 증거물 등 물건의 인도, ⑥ 진술청취, 그 밖에 요청국에서 증언하게 하거나 수사에 협조하게 하는 조치로 한정하고 있고, 동법 제29조~31조에서 사법경찰관은 검사에게 신청하여 법무부장관에게 공조요청서를 송부하고, 법무부장관은 외교통상부장관에게 송부하여 외국에 송부되도록 규정하고 있다. 다만, 공조요청 절차가 복잡한 점을 감안하여 제38조에 국제형사경찰기구와(인터폴)의 협력에 관한 사항을 규정하고 있다. 즉, 행정안전부장관은 국제형사경찰기구로부터 외국의 형사사건 수사에 대하여 협력을 요청받거나 국제형사경찰기구에 협력을 요청하는 조치를 취할 수 있고 구체적으로 ① 국제범죄의 정보 및 자료 교환, ② 국제범죄의 동일증명 및 전과조회, ③ 국제범죄에 관한 사실 확인 및 그 조사를 할 수 있다고 규정하고 있다.

해외에서 공격하는 해킹, DDoS 범죄에 대한 용의자를 추적하기 위해서는 관련 당사국과 긴밀한 협력체제가 필요하다. 해킹, DDoS 범죄의 용의자는 고도의 지능범으로 자신의 접속흔적으로 모두 삭제하기도 하고, 각종 시스템 접속기록과 서비스 사용기록이 일정한 시간이 지나면 소멸되는 경우가 있어 용의자에 대한 즉각적인 추적이 중요하다. 이러한 시급성에도 불구하고 국제형사사법공조법은 복잡한 공조절차

를 규정하고 있어 사이버범죄를 수사하는데 있어서는 적합하지 않다는 비난을 받고 있다. 따라서 국제형사경찰기구와의 교류할 수 있는 범위를 정보 및 자료교환, 사실 확인 및 조사 등으로 한정하지 말고 일정한 범위 내에서 범죄수사까지 진행할 수 있도록 확대할 필요가 있다.

2. 국제기구 및 핫라인 운영현황

가. 인터폴 사이버수사 핫라인

인터폴은 1979년 프랑스 파리에서 열린 제3차 인터넷사기에 관한 인터폴 심포지움을 통해 컴퓨터범죄 대응과 형사법적 규제 문제를 제기한 최초의 국제기구 중 하나이다. 인터폴 사무국에서 사이버범죄를 담당하는 부서는 특수범죄 및 분석국(Specialized Crime & Analysis) 재정범죄 및 하이테크범죄과(Finalcial and High-tech Crime : FHC)의 정보기술범죄반(Information Technology crime)이다. 인터폴은 세계의 사이버범죄 수사관들이 신속하게 연락을 취할 수 있도록 '국가별 중앙 조회처(National Central Reference Points : NCRPs)를 구성하여 운영하고 있다. 각 국가별 정보교류는 국가별 중앙사무국(National Central Bereau)에 설치된 인터폴 전용망인 I-24/7을 통해 연결하는 것이 원칙이나, 사이버범죄는 그 특성을 고려하여 예외적으로 수사부서 간 직접적인 연결을 할 수 있도록 하였다. 현재 인터폴은 '재정 및 하이테크분과'에서 매년 사이버수사 핫라인을 갱신하면서 운영하고 있고, 우리나라를 비롯하여 총 128개국이 활동하고 있다. 로널드 노블 인터폴 사무총장은 2007년 12월 인도에서 열린 제7차 국제 사이버범죄 컨퍼런스에서 기존의 사이버범죄 대응을 위한 연락체계인 NCRPs와 G8의 24/7 연락망, 유럽평의회 사이버범죄협약의 따른 연락체계 등을 통합하여 인터폴 통신망인 I-24/7을 통해 연결하는 글로벌 사이버범죄 수사 네트워크의 구축과 함께 경찰 등 법집행관의 전문성 향상을 위한 교육의 강화, 민간과의 긴밀한 협력 등을 촉구하면서 글로벌 혹은 지역별 범죄방지센터의 설립에 대한 추진 의지를 피력하였다.[120]

120) 이동희 외, 앞의 보고서, 75-76쪽 참조.

나. G8 24/7 네트워크

주요 8개국 정상회담인 G8은 일찍이 1997년 하이테크 범죄에 관한 하부위원회를 설치하면서 사이버범죄에 대한 논의를 본격화하였다.[121] G8에는 초국가적 사이버범죄의 수사와 관련하여 회원국 수사기관이 7일/24시간, 항상 협조하는 것을 목적으로 하는 24/7 네트워크를 구축하여 운영하고 있다. 이는 G8에서 파생된 컴퓨터범죄 소회의에서 비롯된 것으로서 1998년부터 구체화되기 시작하였는데 우리나라를 비롯하여 총 49개국이 가입되어 있다.[122] 이 제도는 공식 국제사법공조 절차가 외교채널 등을 거치면서 상당한 시간이 걸리는 단점이 있어 초국가적 사이버범죄의 수사에는 적합하지 않다는 반성 아래 비공식적인 방법(전화, 이메일, 팩스)으로 상대국가에 대하여 사법공조 요청을 하고, 공식적인 절차는 나중에 취하게 됨으로써 신속성을 확보할 수 있다는데 그 취지가 있다.[123] 현재 50개국 가량이 참여하고 있는데 국내에서는 대검찰청에서 유일하게 가입하고 있어 경찰에서 단말기를 가지고 있는 인터폴의 I-24/7 네트워크와의 중복 문제나 분산된 접근방식으로 인한 문제 등이 야기되기도 한다.[124]

다. 일본 경시청의 CTINS

일본 경시청은 아시아 14개국을 대상으로 '사이버범죄 기술정보네트워크(CTINS)' 구축하여 매년 자국의 부담으로 회원국 경찰관을 초청하는 등 아시아 지역의 국제협력을 위해 적극 노력하고 있고, 아태 지역의 사이버범죄 통계, 대응전략, 국제협력 방안 등에 대한 다양한 컨텐츠를 제공하고 있다. 그러나 참여국의 동의나 결의에 의해 결성된 것이 아니고 일본 주도로 만들어져 다른 국제협력망에 비하여 상대적으로 구속력이 약하고, 다른 아시아 국가의 경우에도 인터폴망, G8 24/7망 등을 활용하고 있어 활용성이 떨어진다. 특히, 우리나라는 사이버범죄 관하여 일본과 국제공조가 많지 않고, 다양한 인적 네트워크가 이미 구성되어 있어 CTINS 망의 활용성은 매우 낮다.

121) 이동희 외, 앞의 보고서, 61쪽.
122) 이창수, 앞의 글, 125쪽.
123) 이창수, 앞의 글, 126쪽.
124) 이동희 외, 앞의 보고서, 63쪽.

3. 수사기관 간 국제협력 활동

가. 주요국과 협력약정(MOU) 체결

경찰청에서는 국제협력의 필요성이 증대됨에 따라 각국 경찰청 간 범죄수사 등 포괄적 협력약정을 체결하기 시작하였는데, 이는 1996년 중국 공안부를 시작으로 러시아, 일본, 몽골, 인도네시아, 베트남, 태국, 호주, 뉴질랜드, 필리핀, 싱가포르, 요르단, 카타르, 멕시코, 이탈리아 등 15개국과 체결하였다. 이와 별도로 영국, 프랑스, 미국, 독일 등 4개국과는 각국 경찰청 사이버수사부서간 체결하여 사이버범죄 관련 정보 공유 및 기술교류, 심포지엄 및 국제회의 상호초청, 사이버범죄 공조수사 적극 협력 등 다양한 협력활동을 하고 있다. 프랑스와는 2003년 이래 매년 양국이 상호 방문하면서 사이버수사 기법, 사이버범죄 동향, 국제협력 방안 등을 긴밀하게 논의하였고, 2010년에는 한·미 사이버수사 워킹그룹을 창설하여 제1회 회의를 미국에서 개최하기도 하였다.

나. 인터폴 주관 교육 프로그램 운영

인터폴 아·태지역 사이버수사교관 양성 워크숍(TTI)은 한국경찰청과 인터폴이 공동으로 창설하여 2002년부터 매년 1~2회씩 각 회원국을 순회하면서 개최하고 있다. 교관단은 한국, 홍콩, 일본, 인터폴 소속의 수사관 또는 증거분석관으로 구성하고, 대상자는 동남아시아 등이 주류를 이루고 있다. 인터폴 아·태지역 디지털 포렌식 워크숍(TTF)은 일본경찰청의 제안으로 2007년부터 인터폴과 공동으로 개최하고 있다. 이를 통해서 아·태지역 사이버수사경찰관간 인적 네트워크를 구축하여 향후 국제공조수사가 필요할 경우에 해당국가의 협력창구로서 적극적인 협력을 기대할 수 있게 되었다. 이러한 교육 프로그램은 교육이수 후에 별도의 시험을 통하여 교관 자격에 대한 인증서를 수여하고 있다.

다. 개도국 수사기법 전수교육 사업

지난 7·7 DDoS 사건에서도 여실히 드러났듯이 사이버공격은 선진국보다는 국제

협력과 시스템 보안이 상대적으로 미흡한 개도국의 서버를 활용할 가능성이 높아 개도국과 국제협력이 매우 중요하다. 이에 경찰대학에서는 매년 국제협력단(KOICA)와 공동으로 '국제 사이버범죄 교육과정'을 개설하여 개도국 IT전문가 20여명 초청하여 교육을 실시하고 있다. 참석자는 경찰관을 비롯한 법집행기관 종사자, IT 관련부처 공무원, 민간 전문가 등 매우 다양하다. 이와 별도로 2006년에는 베트남에 사이버범죄 교관단을 파견하여 사이버수사기법에 대한 교육을 실시하였고, 2008년에는 멕시코 연방경찰청의 요청에 따라 사이버범죄 법률, 대응정책, 인터넷추적 및 포렌식 기법에 대한 교육을 실시하기도 하였다. 2009년에는 카타르 정부의 요청에 의해 교관을 파견하였고, 2010년에는 코스타리카 경찰의 요청에 의해 교관을 파견할 계획이다.

4. 평가 및 개선방안

가. 국제기구·협력대상국 다변화 및 사이버범죄 방지조약 가입

사이버범죄는 국경을 초월하여 발생하기 때문에 특정 국가의 법률제정과 노력만으로는 범죄를 예방하고 수사하고 처벌하는데 한계가 있다.

경찰은 그동안 인터폴과 세계 각국에 파견된 경찰 주재관을 활용하여 국제협력을 진행하여 왔으나 만족스럽지는 못했다. 최근 UN, OECD, ITU, G8 등 각종 국제기구에서도 사이버범죄에 대한 거대한 담론이 구체적으로 논의되고 있으므로 국제협력의 채널을 다변화하여 국제사회 사이버범죄 근절을 위한 노력을 게을리 해서는 안 될 것이다. 그간 국제협력은 선진국 중심으로 정보 및 기술교류를 중심으로 이루어졌다. 그러나 7·7 DDoS 사건 발생시에는 파키스탄, 과테말라, 그루지아 등 개도국 및 후진국의 서버를 다수 이용해서 공격했다. 이는 개도국의 서버의 보안관리가 허술하여 장악이 쉽고, 반대로 우리나라와 개도국의 경우에는 상호간에 국제협력이 잘 되지 않을 것이고, 개도국의 경우 현지 수사관의 전문성 저하로 인해 원활한 국제협력이 되지 않을 것까지 고려했다고 볼 수 있다. 따라서 다변화하고 개도국에 대한 교육지원도 적극적으로 지원할 필요가 있다.

또한, 국제사회가 공통적으로 해악이라고 인식하는 범죄행위를 사전에 예방하고

진압하기 위해서는 세계 각국은 조약에 의해 특정의 행위를 범죄로 규정·처벌할 근거를 만들고 그 조약의 시행을 위한 자국의 현실에 맞는 각각의 국내법을 제정하여 조직적이고 체계적인 수사절차를 종합적으로 정비하여야 할 것이다.[125]

나. 국제공조 수사에 앞서 국제정보공조 활성화

그간 국제협력은 송환·출국금지 등 사후적 검거·집행 등에 초점이 맞추어져 있었으나, 사이버범죄는 초기에 실시간으로 협력하지 않으면 용의자를 특정할 수 없어 이후의 국제공조수사는 사실상 무의미하다. 나라마다 로그기록을 남기는 기준이 다르고, 일정시간이 경과할 경우 용의자들이 증거를 은닉할 수 있기 때문에 신속한 국제공조가 필요하다. 외국의 경우에도 PC방, 도서관 등 공공장소에서 컴퓨터를 사용할 경우 실시간 검거체제가 확립되지 않으면 검거할 수가 없다. 따라서 국제협력에 있어서 수사기관 간 긴밀한 협력체제가 매우 중요해지고 있다. 향후 사이버범죄가 계속 증가하고, 각 나라마다 이로 인하여 심각한 사회문제에 봉착할 경우 각국 간의 협력은 지금보다 훨씬 밀접해 질 것이다.

국가간 수사공조는 사람이나 자료를 다른 나라에 보내야 하는데 자국민 불인도, 정치범 불인도 등의 원칙 때문에 절차가 번거롭고, 내용에도 제한이 따른다. 이런 까닭에 범죄인인도조약이나 형사사법공조조약이 체결된 상태에서도 공조실적이 미비하다. 반면 정보공조는 사람이나 증거자료를 넘겨주지 않기 때문에 상대적으로 절차가 간편하고, 개인의 불이익과는 거리가 멀어 비공식적인 공조의 여지도 매우 넓다. 따라서 공조의 신속성이 요구되는 상황에서는 개인의 친분을 이용한 공조도 가능할 수 있다. 경찰이 정보공조기능을 지속적으로 확대해 나가야 한다.[126] 다만, 정보공조로 할 수 있는 것이 무엇인지에 대한 고민이 필요하다. 실제 2009년에 IT기업을 해킹한 후 협박하여 금품을 갈취하고자 했던 독일 해커를 검거하는 과정에서 외국에 가입된 도메인 정보를 조회하여 검거한 사건이 좋은 예가 되겠다.

125) 정정일, "사이버범죄에 대한 국제적 대응방안", 경호경비연구 제10호, 2005, 350쪽.

126) 우제태, 앞의 글, 188쪽.

다. 인터폴 사이버범죄 센터 창설

우리나라가 사이버치안 강국으로서 지속적으로 리더 역할을 하기 위해서는 개발도상국에 사이버수사 기법과 대응 시스템을 전수하고, 전문인력을 양성할 수 있는 국제 사이버범죄 대응기구를 창설할 필요가 있다.[127] 소위 '사이버 범죄꾼'들로부터 이제 막 IT기반 시설을 구축하는 단계인 개발도상국의 피해를 최소화해주는 울타리 역할이나 IT범죄 대응 시스템을 구축해 주는 역할을 맡을 경우 국제사회의 발전에 기여할 수 있을 것이다. 세계 최고로 평가받는 '사이버수사' 분야를 국제적 브랜드화 하여 한국경찰 내에 인터폴 소속 국제기구 창설을 추진할 필요가 있다. 이는 개도국 등 대상 사이버수사 교육훈련 과정을 운영, 사이버테러 대응을 위한 국제협력망 확충 및 국제사회에 기여할 것으로 보인다. 주요 기능은 사이버범죄 관련 교육훈련, 기술지원, 조사연구, 국제협력활동을 수행할 예정이다. 이는 2008년 3월에 인터폴 사무총장, 한국내 '반(反)사이버범죄 교육센터' 창설을 제안하면서 시작되었고, 2009년 10월경 '사이버테러 종합대책' 속에 국제기구 유치를 포함함으로서 경찰청의 사업추진이 공식화되었다. 현재 연구용역을 완료하고 경찰청 안을 마련 중에 있으며 행정안전부, 기획재정부, 외교통상부 등 유관기관과 협의를 거쳐 인터폴 총회 승인을 거치고, 국내 비준조약을 통과함으로써 최종적으로 완성될 것으로 보인다.

127) 정정일, 앞의 글, 349쪽.

제4장

주요국의 사이버안전체계 분석

04
주요국의 사이버안전체계 분석

세계 각국은 사이버전 전담부대를 창설하는 등 사이버공격 대응능력을 국가 및 국방 핵심전략으로 추진하고 있으며, 특히 중국은 인민해방군에 6천여 명 규모의 해킹 조직을 운영하고 있고 미국은 2001년 이후 국방부와 주요 정부기관 웹사이트에 해커가 침입, 기밀문서가 유출되는 사건이 빈발하자 중국정부를 배후로 지목하고 사이버 보안을 더욱 강화하여 최근에는 사이버전에 대비한 가상공격 체계를 수립한 것으로 알려졌다. 또는 미 공군은 4대 편대로 구성된 사이버사령부를 신설해 적의 통신시스템을 교란하거나 데이터 패킷을 파괴하는 등 사이버 공격 정예부대로 양성하겠다는 의지를 표명하기도 하였다. 이는 그동안 미 정부가 사이버전 전략을 방어위주로 일관해온 데서 선회, 이제는 선제공격을 취할 수 있음을 공개적으로 시사한 것이어서 더욱 주목되는 부분이다. 종합적으로 볼 때 우리나라에서도 그동안 발전된 정보인프라를 안전하게 보호하고 국가가 지향하는 미래 유비쿼터스 사회로의 진전과정에서 제기되는 물리적 공격위협에 못지않게 사이버공격 위협의 심각성 등 현대 사회의 안보환경을 직시하고 이와 관련된 법률과 대응체계를 확립할 필요성이 크다.[128]

128) 이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구", 국가정보연구 제1권 2호, 2008. 12, 55쪽.

이에 본 연구는 사이버침해를 효과적으로 대응하기 위한 법제도 및 정책적 과제를 살펴보기 위한 논의의 기초로 주요국의 사이버공격 대응체계에 대해 살펴보기로 한다.

제1절 미국의 사이버공격 대응체계

1. 개 관

미국은 1970년대부터 이미 사이버공격의 심각성을 인식하고 대책을 세우고 법적 장치를 마련하기 시작하였으나, 사이버테러리즘에 대한 구체적인 대응책이 나타나게 된 것은 1991년 걸프전 당시 미 국방부의 사이트가 사이버테러리스트에 의해 해킹당한 사실이 상원 청문회를 통해 밝혀진 이후로 알려진다. 또한 미국 정부는 사이버위협에 대응하기 위하여 클린턴 행정부 시절 '대통령지시'(Presidential Decision Diretive 63)로 주요기반보호정책 등 사이버보안의 기초를 확립하였다. 즉, 사이버침해 대응과 관련된 국가정책은 사이버위협에 대한 위기감의 확산에 따른 국가주요기반보호의 필요성이 제기되어 1995년 주요기반보호위원회(PCCIP : President's Commission on Critical Infrastructure Protection)보고서에 근거한 대통령지시(Presidential Decision Diretive 63)가 1997년 발표되면서 시작되었다.

1997년 6월 국가안보국(NSA : National Security Agency)이 미국의 주요 기관의 컴퓨터 보안상태 점검을 위해 태평양사령부 지휘통제소를 메일 폭탄(Mail Bomb) 등으로 가상 공격하였는데, 중앙컴퓨터시스템이 파괴되어 위성과 군사시설 등에 대한 통제 불능 상태에 빠지고 저장된 국방기밀들이 해킹당하는 결과가 초래되어 큰 우려를 낳았다. 이에 국가 주요기반시설에 대한 사이버위협에 대응하기 위한 계획이 각계의 의견수렴을 거쳐 2000년 1월 '정보시스템 보호를 위한 국가계획'(National Plan for Information System Protection)[129]으로 발표되어 국가 주요기반보호를 위한 체

129) 이 국가계획은 크게 사이버위협에 대한 대비와 예방, 탐지와 대응, 안전한 기반구축 등으로 이루어져 있으며 이에 기초하여 연방침입탐지네트워크(FIDNET : Federal Intrusion Detection NETwork)가 운영되고 있다. 이 FIDNET의 목적은 주요 기반구조자산과 공유된 상호의존성을 확인하고 취약성을

계적인 전략개발이 주로 연방정부를 중심으로 이루어지기 시작했다. 특히, 이러한 미국의 사이버침해 대응체계는 2001년 9·11 테러를 계기로 급속한 진전을 이루게 되는 바, 2003년 3월 기존의 22개 다른 연방기관과 프로그램 및 기관들을 연방재난관리청(FEMA)과 함께 통합하여 국토안보부(DHS : Department of Homeland Security)를 신설하고 국가의 재난관리 및 국토안보 업무를 총괄하는 등 9.11 테러는 미국의 안보체계를 전면 재편하는 일대 전기가 되었다. 미국은 9.11 이후에 물리적인 공격과 더불어 사이버공격을 포함한 테러리스트의 위협과 공격으로부터 미국의 안전을 보장하기 위한 조치를 추진하였고, 이를 위해 총괄부서로서 국토안보부를 신설하고, 사이버안보 담당 대통령 특별 보좌관, 국가기반자문회의, 주요기반보호대통령협의회 등을 조직하였다. 이처럼 책임과 권한이 여러 부처에 분산됨으로 인해 발생하는 정책의 혼선을 방지하고 모든 역량을 한 곳에 집중하기 위해 국토안보부(DHS)의 창설로 대표되는 효율적인 대응체계를 마련한 것은 미국의 사이버안보전략이 갖는 가장 큰 의의로 평가된다.

무엇보다 미국은 연방정부만으로는 더 이상 사이버위협에 대응키 어렵다는 인식하에 관련 업계의 협조를 비롯한 모든 국민의 적극적 참여와 국제적인 협조가 절실하게 요구된다는 점을 주목하였다. 이에 2002년 9월 18일 '사이버안보국가전략'(National Strategy to Secure Cyberspace)[130]의 초안을 발표하고 사이버공간에의 의존성 심화와 새로운 취약성의 발견 및 네트워크의 글로벌화 등에 따라 증대되는 사이버위협에의 지속적인 대응과 국가 차원의 위험관리의 중요성을 강조하였다. 이후 사이버안보국가전략은 수차례의 의견수렵과정을 거쳐 2003년 2월 14일 최종적으로 확정되었는 바, 사이버안보를 국가의 주요기반시설의 보호에 한정하지 않고 기존의 개념을 확장한 국가안보차원에서의 사이버안보의 중요성을 재확인하고 주요기반시설 및 핵심자산에 대한 물리적 보호전략과 양축을 이루게 되었다.[131] 사이버안보 국가전략에서 미국은 사이버안보는 국민의 참여 없이 연방정부만으로 수행할 수 없

제안하며, 침입행위의 실시간 탐지와 이에 대한 신속한 대응으로 주요 정보시스템 보안을 위한 견고한 기초(Strong Foundation)를 구축하는 것이다.

130) Whitehouse(2003.2), The National Strategy to Secure Cyberspace.

131) Whitehouse(2003.2), The National Strategy for The Physical Protection of Critical Infrastructure and Key Asset.

는 매우 어려운 과제이므로 사이버안보에 대한 인식제고와 교육훈련, 기술개발과 취약성 해결 등으로 시장의 활성화, 정보의 공유와 운영계획의 수립 등 민간부문과 공공부문 간의 긴밀한 체계구축을 최우선 원칙으로 제시하고 있다. 또한 사이버위협의 동적 특성을 고려하여 사이버위협에 유연하게 대응하고 책임과 의무를 명확히 하며 지속적인 정책의 필요성을 제시하고, 국가 간의 정보공유, 취약성 감소노력, 사이버테러리즘 대응을 위한 국제적인 협력체계 구축의 필요성을 강조하고 있다. 2008년 1월에는 부시 대통령이 "NSPD-54/ HSPD-23"을 승인함으로서 이를 바탕으로 한 '국가사이버보안종합전략'(CNCI : Comprehensive National Cyber Security Initiative)이 수립되었다. 이는 신 사이버보안을 위해 결정한 비밀정책으로, 지금까지는 각각의 침입사고에 대한 사후 대응에 비중이 높았다면, 이제 사전대응 체계 구축으로 사이버안보를 달성하겠다는 의지를 나타내고 있다.[132]

오바마 행정부가 수립된 이후에도 역시 사이버보안은 중대한 정책이슈로 주목받게 되었으며, 이는 오바마 대통령이 취임 후 60일 이내에 기존 연방 사이버보안 정책에 대한 검토와 향후 전략 수립을 위한 보고서 제출을 국가안보이사회(NSC) 등 관련기관에 요청한데서도 이 같은 의지를 짐작할 수 있다. 이에 따라 최근 2009년 5월말에는 ① 백악관, 연방차원 등 최상위 리더십에 따른 정책 추진, ② 보안교육, 전문 인력 양성 등 디지털 국가를 위한 역량 제고, ③ 민·관 협력을 위한 파트너십 구축 등 사이버보안 책임 분배, ④ 효율적인 정보 공유 및 대응 능력 강화, ⑤ 보안 강화를 위한 혁신 촉진 등을 내용으로 하는 '사이버공간 정책 리뷰'(Cyberspace Policy Review : Assuring a Trusted and Resilient Information and Communications Infrastructure)[133]를 발표하였다. 동 보고서에서는 단기실행계획(10개) 및 중기실행계획(13개)을 제시하고 있으며, 특히 단기실행계획 첫 번째로 국가사이버보안 정책 추진을 총괄할 사이버보안책임관을 임명할 것을 제안하고 있다. 이에 오바마 대통령이 선거 공약에서부터 우선과제로 강조해 온 사이버보안에 대한 실질적인 정책 실현을 위한 범부처간 조정자로서 요구되는 직제의 필요성에 따라 이른바 사이버 차르(Cyber

132) "The Murky Waters of the White House's Cybersecurity Plan", July 23, 200 : http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm.

133) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Czar)로 불렸던 사이버보안조정관을 2009년 12월 22일 임명하였다.[134] 사이버보안조정관은 미국 국가안전보장회의(NSC)에 상주하면서 대통령과 NSC에 정기적으로 보고하며, 미군과 민간기관의 연방정부 사이버보안 정책 마련을 위한 자문관으로 역할을 수행하고 있다.

특히, 최근 2010년 5월 27일 오바마 정부는 출범 후 처음으로 국가안보의 현황과 지향점을 공개 발표한 국가안보전략(NSS : National Security Strategy)에서 사이버보안의 의미와 향후 정책 방향을 중요한 전략으로 다루고 있다. 즉, 국가안보와 공공안전 및 국가경제에 위협을 주는 사이버공간에서의 불법행위와 테러, 해킹 등을 안보 이슈로 인식하여 디지털 인프라를 국가의 주요 자산으로 관리하겠다는 의지를 천명하였다. 이를 위해 관련 인력과 기술부문의 투자를 과감하게 늘리고, 공공·민간·학계 등 관련 부문 파트너십을 강화하는 방향으로 사이버보안 강화정책을 펼칠 것임을 밝혔다.[135] 이처럼 미국은 사이버보안과 관련한 정책을 추진하는데 있어 가장 의욕적이고 강력하게 추진하고 있는 대표적인 나라로 평가되며 이는 우리나라 사이버보안 대응체계 구축에 있어 시사하는 바가 크다고 할 것이다.

2. 조직체계

가. 국토안보부(DHS)

미국은 911테러 이전에도 테러 방지를 위한 노력을 계속하여 왔으나 기능이 여러 기관들로 분산되어 효과적이고 유기적으로 대응하기 위한 총괄기구의 도입의 필요성이 제기되었다. 이에 2002년 6월 부시 미국 대통령이 상원에 제출한 '국토안보법(안)'을 계기로 2003년 3월 정식 출범한 국토안보부(DHS)를 중심으로 테러방지 및 자연재해, 재해 등을 총집결시킨 총체적 재해·재난 관리체계를 구축하였다.

국토안보부는 기존의 대통령 자문기구 성격의 '국토안보국'을 격상시킨 것으로, 국

134) 오바마 대통령은 초대 사이버보안조정관으로 약 40여 년간 미국 사이버보안 관련 공공 및 민간부문의 최고경력자로 평가되는 하워드 슈미트를 임명하였다.

135) http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

토안보부의 편입되는 기구들에는 세관, 이민국, 해양수비대, 교통보안국, 연방재난관리청(FEMA) 등 22개 기관에 이른다.[136]

국토안보부는 미국에 대한 공격을 막고, 국토의 위협과 테러에 대한 취약점을 축소시키며, 테러리스트에 의한 공격으로 발생된 피해복구 지원 및 위험 최소화를 위한 임무를 수행한다. 즉, 국토안보부의 임무에는 ① 미국의 핵심 자원과 주요기반시설을 보호하기 위한 종합적인 국가전략 개발, ② 주요기반시설에 대한 공격에 대응한 위기관리 기능 수행, ③ 주요정보시스템 마비에 대비한 긴급복구와 관련 민간 및 정부기관 기술지원, ④ 다른 연방기관들과 협력하여 주정부, 민간부문, 학계, 공공, 일반국민 등을 대상으로 하는 경부 발령과 정보보안 대책 및 자문 제공, ⑤ 다른 기관과 연계하여 국가안보에 관한 새로운 과학적 지식과 기술 연구개발 수행 및 재정지원 등이 있다. 국토안보부는 연방정부의 정보보호 정책을 실시할 책임을 지고 있으며, 이를 규정한 것이 2003년 2월에 제시된 '사이버공간 보안 국가전략'(National Strategy to Security Cyberspace)이다. 이는 연방정부의 각 기관이 완수해야 할 정보보호의 포괄적인 틀을 제시하고 있다.[137]

국토안보부의 장은 대통령이 임명하고 상원이 인준하는데, 국토안보부 장관은 국방장관이나 법무장관과 같은 지위로, 미국 내 재난안보와 관련한 모든 정보에 접근할 수 있는 권한을 가지고 있으며, 여기에는 사법당국과 정보기관, 기타 정부기관의 자료는 물론 미국의 인프라 및 기타 취약대상과 관련한 정보도 포함된다.

국토안보부는 2005년 조직개편을 통해 정보보호와 관련되어 국토안보부 장관에게 국토안보와 관련된 현안에 대해 자문하는 국토안전보장자문위원회(HSAC : Homeland Security Advisory Council)와 국토안보부 장관과 대통령에게 공공 및 민간영역의 주요 기반시설의 보안과 관련된 사항을 자문하는 국가기반시설자문위원회(NIAC : National Infrastructure Advisory Council)가 설립되었다.[138] 이후 국토

136) 국토안보부는 직원 18만 명 이상, 연간 예산 400억 달러의 막대한 인적·물적 기반을 토대로 국경경비, 재난 및 화생방 공격대비 활동, 과학기술 확보, 정보 분석, 이민관리, 사이버 보안 등의 활동을 수행한다. 사이버테러리즘을 포함한 모든 대테러 활동 임무는 민·관·군의 모든 기반산업과 관련되어 상호 영향을 미치기 때문에 기존 행정부처나 정보기관 중 특정 1개부서가 맡기에는 너무 방대한 범위라고 판단하였기 때문에 모든 관련 조직, 법령 및 예산을 통합·정비하여 국토안보부를 신설한 것이다.

137) http://www.dhs.gov/xprevprot/programs/gc_1158611596104.shtm.

138) Congressional Research Service(2005).

안보부는 2006년 4월 부시 대통령이 서명하고 2007년 3월 1일부터 효력이 발생된 포스트-카트리나위기관리개혁법(the Post-Katrina Emergency Management Reform Act)[139]에 의하여 일부 조직적 변경이 있었고, 연방재난관리청(FEMA : Federal Emergency Management Agency) 또한 재조직되었다.[140]

국토안보부는 유비쿼터스 시대를 대비하기 위해 핵심 정보보호전략으로서 국토안보 대통령령 7호(HSPD-7)를 근거로 국가기반구조와 주요자원(CI/KR : Critical Infrastructure/Key Resource)보호를 개선하기 위해 2006년 6월 '국가기반보호계획'(NIPP : National Infrastructure Protection Plan)을 발표하였다. 이 계획에는 국가기반구조와 주요자원 보호 프로그램을 구현하기 위한 보안 협력모델 수립, 장기적 위험 감소 프로그램 실행, 국가기반구조와 주요자원 보호를 위한 자원의 효율적 사용 극대화 등을 담고 있다. 이를 위해 에너지, 물, 식량, 의료, 교통 및 정보통신과 같은 국가의 핵심자산 및 자원을 보호하기 위한 민간부문과의 협력관계를 규명하는 프레임워크를 포함하고 있다. 동 계획에서 국토안보부는 기반구조부문조정위원회(SCC : Sector Coordinating Council) 및 정부부처조정위원회(GCC : Government Coordinating Council)를 운영하고, 핵심 기반구조의 소유자와 운영자에게 정보를 제공할 수 있는 프로토콜을 구현할 것을 밝히고 있다.

나. 대통령직속 주요기반보호 협의회(PCIPB)

'대통령직속 주요기반보호 협의회'(PCIPB : President's Critical Inftrastructure

139) 포스트-카트리나위기관리개혁법(the Post-Katrina Emergency Management Reform Act)은 국토안보부 내의 새로운 리더십 정립과 기능 조정, 재난관리청(FEMA)의 기능 추가, 그리고 기존 국토안보법의 수정을 가져왔다. 즉, 동법은 재난관리청(FEMA)에 준비국(Preparedness Directorate)의 기능을 이관시켰고, 기존의 준비국은 국가보호프로그램국(NPPD: National Protection and Programs Directorate)으로 개명되었다. 국가보호프로그램국(NPPD)은 기반보호실(OIP:Office of Infrastructure Protection), 사이버보안통신실(OCS&C: Office of Cyber Security and Communications), 위험관리분석실(ORM&A: Office of Risk Management and Analysis), 정부간프로그램실(OIP: Office of Intergovernmental Programs), 그리고 미국방문실(US-VIST)로 구성되어 있다. http://www.dhs.gov/xabout/structure/gc_1169243598416.shtm.

140) 즉, 미국 역사상 가장 참혹한 자연재난이었던 2005년 허리케인 카트리나 대응에서 나타난 문제점들을 치유하기 위하여 좀 더 강한 사전준비 임무를 포함하여 실질적인 재난관리 권한을 FEMA에 부여하였다. http://www.fema.gov/about/history.shtm.

Protection Board)는 긴급대비통신을 포함한 주요기반에 대한 정보시스템 및 동 시스템을 지원하는 물리적 시설에 대한 프로그램 조정 및 정책 제안 등을 위해 대통령 행정명령에 의해 9·11테러 이후에 창설되었다. PCIPB는 미국의 비상통신망을 포함한 주요기반의 정보시스템을 지원하는 물리적 자산의 안전을 확보하여 미국의 국민, 경제, 정부업무 및 국가안보를 보호하기 위해 설립한 최고정책기관으로서 주요기반 보호정책을 효과적으로 집행하고 강화할 수 있는 조직이다. PCIPB는 국무장관, 재무장관, 국방장관, 법무장관, 상무장관, 보건인적서비스장관, 교통장관, 에너지장관, CIA국장, 합참의장, 연방재난관리국(FEMA) 국장, 조달청장, OMB국장, OSTP(Office of Science and Technology Policy) 국장, 대통령비서실장, 국가경제위원회 의장, 대통령안보담당보좌관 등 정부 관련조직의 고위관리로 구성되어 있는 바, 그 위상을 가늠케 하고 있다. 협의회는 필요한 경우 실무위원회 또는 지원위원회를 둘 수 있는 바, 현재 민간분야 및 주정부·지방정부 위원회, 행정부 정보시스템보안위원회, 국가보안시스템위원회, 침해대응조정위원회, 물리적 보안위원회, 기반상호관계위원회, 국제문제위원회 등 다양한 실무위원회를 두고 있다.

동위원회는 2003년 2월 미국의 정보통신기반을 보호하기 위한 「사이버공간 보안 국가전략(National Strategy to Security Cyberspace)」을 수립하여 사이버안보를 위한 전략적 목적[141]과 국가전략 수립의 원칙[142] 및 국가적 우선순위[143]를 기초로 전략을 구체화하고 있다.

다. 미국의 사이버수사조직

1988년 클린턴 대통령에 의해 연방수사국(FBI)에 국가기반보호센터(National Infrastructure Protection Center : NIPC)를 설치하였고,[144] 2002년 11월 국토안보

141) 미국의 주요기반시설에 대한 사이버공격 예방, 사이버공격에 대한 국가적 취약성 감소, 사이버공격 발생 시 피해와 복구시간의 최소화 등이다.

142) 국가적 노력(모든 국민의 참여), 프라이버시와 국민의 자유보호, 규제와 시장지배력, 책임소재(국토안보부의 역할), 유연성 확보, 중장기 계획 수립 등이다.

143) 사이버안보를 위한 우선순위(Critical Priorities)는 국가사이버안보대응 시스템, 국가사이버안보 위협 및 취약성 축소 프로그램, 국가 사이버안보 인식 및 프로그램, 정보의 사이버공간 보호, 국가안보 및 국제 사이버안보 협력 등이다.

법을 제정하여 FBI의 국가기반보호센터(NIPC), 국방부의 국가통신시스템(NCS), 상무부의 주요기반보장국(CIAO) 등의 기관에 속한 직무와 인적자원, 권한과 책임이 국토안보부로 이관되었으며, 국토안보부가 각종 테러리즘과 관련된 모든 정보를 수사기관과 법집행기관으로부터 제공받을 수 있게 되었다.[145] 이와 별도로 현재 FBI에는 사이버범죄를 전담하는 사이버범죄수사부(Cyber Division) 소속에 운영지원과, 사이버범죄과, 컴퓨터침입범죄과, 특수기술응용과, 능력개발 및 대외협력과 등 5개과를 두고 있고, 주요 22개 도시에 사이버 테스크 포스 조직을 별도로 운영하고 있다. 컴퓨터침입범죄과는 해킹수사를 전담하는 '컴퓨터침입범죄수사계'와 사이버테러를 전담하는 '대태러/방첩 컴퓨터침입수사계', 공격정보 분석을 전담하는 '사이버정보계'로 구성되어 있다.[146]

3. 법제도 체계

가. 애국법

애국법(USA PATRIOT ACT of 2001)은 9·11테러 직후 계속되는 테러 위협에 대응하기 위한 수사력 강화와 국가안보 확립을 목적으로 한 법률로서 주요내용을 살펴보면 종래 법집행기관의 용의자 관련 전화번호 기록 권한을 인터넷이나 휴대전화를 포함한 전자통신으로 확대하고 DCS1000[147] 등에 의한 IP주소 등을 기록한다. 동법은 법집행기관과 정보기관 간의 정보 수집 및 공유체계에 구조적·법적인 제약을 해소시킴으로써 대테러 기관간 협력을 강화시킨 것이다. 이를 위해 테러 혐의자에 대한 감청 허용요건과 영장주의를 완화하고 테러조직과 관련된 은행계좌나 자산의 동결 등을 규정하였다.[148] 또한, 테러범죄자들이 미국으로 입국하는 것을 막고 미국

144) 민경식 외, "주요국 정보보호 동향조사 2007-유비쿼터스 시대의 정보보호 정책을 중심으로", 한국정보보호진흥원, 2006, 28-29쪽.

145) 김도승, "사이버위기 대응을 위한 법적과제", 방송통신정책 제21권 17호, 2009. 9, 46쪽.

146) 경찰청에서 2009년에 수립한 "사이버테러 종합대책" 참고.

147) Carnivore라 불리며, 미국 연방수사국(FBI)이 사이버 범죄 예방을 위하여 1999년 개발한 이메일 감시시스템을 말한다.

내 테러용의자들의 추방을 쉽게 하기 위하여 구금 및 추방의 요건을 대폭 완화하는 한편, 테러행위에 대한 처벌도 크게 강화 하였다. 즉, 이전의 경우 사이버테러시 초범은 5년 이하의 징역, 상습범에게는 10년 이하의 징역이 최고형이었지만, 이 법은 보호되는 컴퓨터에 손해를 가한 해커에 대한 최고 형량을 초범 10년, 상습범 20년까지 상향조정하였을 뿐만 아니라 국방이나 국가안보와 관련한 컴퓨터에 피해를 야기한 경우에는 손실을 증명할 수 없어도 처벌할 수 있도록 하였다.

이후 2006년 개정된 애국법은 애국법의 개선 및 권한 재부여 법(USA PATRIOT Improvement and Reauthorization Act of 2005)과 애국법의 부가적 권한 재부여에 관한 수정안(USA PATRIOT Act Additional Reauthorizing Amendment Act of 2006)의 두 개의 법률로 구성되어 있다. 개정 법률은 9·11 테러 이후 연방당국에 주어진 광범위한 감시와 수사권한을 대부분 유지하고 있으며 2005년 말 효력이 완료되어 있던 16개 조항 중에서 14개 조항을 영구 법제화하고 2개 조항은 2009년 12월 30일 까지 4년 연장돼 효력을 가지게 되었다.[149]

나. 국토안보법

2002년 6월 6일 부시 대통령은 미국 내 테러대책을 총괄하는 국토안보부의 창설을 제안하였고, 2002년 11월 국토안보법(Homeland security Act of 2002)[150]을 제정하여 이에 대한 법적 근거를 확보하였다.[151] 국토안보법은 포괄적인 테러리즘으로부터 미국의 전체 국가기반을 보호하기 위해서 제정된 법으로서 총 17장으로 구성되어 있는데 특히 사이버안보와 관련된 규정으로는 제2장의 정보분석 및 기반시설 보호(IAIP : Information Analysis and Infrastructure Protection)에 관한 규정과 제

148) 미국 연방법전 제18권 제1030조.

149) http://www.usdoj.gov/olp/pdf/usa_patriot_improvement_and_reauthorization_act.

150) http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm.

151) 국토안보법은 테러리즘에 관해 "인명에 위험하거나 주요기반시설 또는 핵심자원을 파괴할 잠재적인 행위와 미국의 모든 주 또는 기타 세부 행정구역의 형법에 대한 위반행위를 포함하고, 일반국민을 협박하거나 위압하려는 의도, 협박이나 위압을 통하여 정부정책에 영향을 미치고자 하는 의도, 대량파괴, 암살 또는 납치 등을 통하여 정부의 업무수행에 영향을 미치고자 하는 의도를 나타낸다"고 정의하고 있다. Homeland security Act of 2002, SEC. 2. DEFINITIONS (15).

10장의 정보보안(Information Security)에 관한 규정이 대표적이다.

제2장은 FBI의 국가기반보호센터(NIPC), 국방부의 국가통신시스템(NCS), 상무부의 주요기반보장국(CIAO) 및 에너지부의 국가기반시뮬레이션 및 분석센터와 에너지안보 및 보장 프로그램, 총무성(GSA)의 연방컴퓨터 사고대응센터(FedCIRC) 등의 기관에 속한 직무 등이 국토안보부로 이관하도록 규정함으로써, 국토안보부가 각종 테러리즘과 관련된 모든 정보를 수사기관과 법집행기관으로부터 제공받을 수 있게 하여 명실공히 사이버공격 대응을 위한 총괄기관으로서 기능할 수 있는 법적 근거를 제공한다. 특히 제2장 SEC.225는 2002년 하원 통과 후 상원에서 폐기된 '사이버보안강화법'(Cyber Security Enhance-ment Act of 2002)이 국토안보법에 포함되어 통과된 것으로, 양형위원회 관련 내용, 긴급 공개 예외, 선의의 예외규정, 불법장치의 인터넷광고, 강화된 벌칙, 프라이버시 보호 등이 규정되어 있다. 특히 사이버공격자가 고의 또는 부주의로 법률을 위반하여 심각한 신체적 상해를 유발하거나 시도하는 경우나, 공격자가 고의 또는 과실로 사망을 유발하거나 유발하고자 시도하는 경우 등에 관하여 벌금과 징역형을 병과할 수 있게 하는 등 처벌수위를 대폭 강화하고 있다.

'연방정보보안관리법'(FISMA : Federal Information Security Management Act of 2002)으로도 불리는 제10장은 연방을 지원하는 주요 정보자원에 대한 보호 및 통제를 위한 포괄적인 프로그램을 제공하고 고도로 네트워크화된 국가기반의 보안을 위하여 민간 부문의 국가기관 전체의 정보보안 노력을 조정하여 사이버위협에 대해 효과적으로 대응할 수 있도록 국토안보부가 정부 전체를 관리·감독하도록 하고 있다.[152] 연방정보보안관리법은 국립표준기술연구소(NIST)에 정보보안 정책, 절차, 그리고 실무뿐만 아니라 정보시스템을 보호하기 위한 표준과 가이드라인 대응에 관한 기관들에게 기술적인 지원을 제공하는 임무까지 부여하고 있다.

미국의 정보보호 관련 각 정부기관의 개별적인 과제의 예산은 연방정보보안관

152) 연방정보보안관리법은 2002년 11월에 만료 폐기된 정부정보보안개혁법(Government Information Security Reform Act of 2000)의 한시법 조항을 삭제하고, 전자정부법 2002(e-Government Act of 2002)의 제3장 정보보안에 삽입된 법이다. 연방정보보안관리법의 목적은 연방정부의 운영 및 자산에 대한 정보보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크 제공, 국가보안 및 법집행기관 전반에 걸친 관련 정보의 보안 위험에 대한 효율적인 관리 및 통제방안 제공 그리고 연방정부 정보 및 정보시스템 보호를 위한 최소한의 통제 및 유지 방안 개발 등에 있다.

리법(FISMA)에서의 정보보호의 정의를 사용하고 있는데, 동법에서의 정보보호에 대한 정의는 “정보 및 정보시스템의 가용성, 무결성, 기밀성을 제공하기 위해 불법적인 접근, 이용, 공개, 변형, 파괴로부터 보호하는 것”이라고 되어 있다.[153]

최근에는 미국 연방 사이버보안을 향상시키기 위해 연방정보보안관리법을 개정하였는데(2010.5.28), 이를 통해 대통령실에 사이버공간보호국(NOC : Nati-onal Office for Cyberspace)을 구축하고 상원의 승인을 받은 책임자를 둘 예정이다. 이로써 백악관은 정부기관 내 사이버보안을 더욱 직접적으로 통제할 수 있을 것으로 기대하고 있다. 사이버공간보호국(NOC)은 연방 사이버보안 실무 이사회(Federal Cybersecurity Practice Board)의 지원을 받아 사이버보안에 관한 정책과 절차를 도출한다.[154]

다. 관리예산처 지침

미국 연방정부의 컴퓨터보안을 포함한 정보자원관리의 중심기관은 ‘관리예산처’(OMB : Office of Management and Budget)이다. OMB는 연방정보보안 정책에 필요한 최소한의 통제장치들을 수립하여 각 정부기관들이 정보보안에 관한 책임을 지도록 요구하고 각 기관들의 정보보안 프로그램과 기관관리통제시스템을 상호 연계시키고 있었다. 관리예산처는 정보자원의 관리와 정보보안에 있어 요구되는 임무수행에 필요한 사항들을 기술한 지침(Circular A-130)을 발표하였다. OMB Circular A-130의 〈부록Ⅲ〉 연방정보자원보안(Security of Federal Automated Information Resources)은 연방정보보안정책에 필요한 최소한의 통제장치들을 수립하고, 각 기관들이 정보보안에 대한 책임을 지도록 하면서 각 기관 정보보안프로그램과 관리통제시스템을 상호연계시키도록 규정하고 있다. 세부내용에 따르면 관리예산처는 연방정보자원보안정책을 총괄 및 감독하며 상무부, 특히 국립표준기술연구소(NIST : National Institute of Standards and Technology)는 보안관련 표준 및 지침을 개발

153) http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf.

154) NOC의 주요 역할은 기본적인 사이버보호를 위한 최소한의 보안통제, 보안통제를 위한 효과성 측정, 보안통제를 충족하기 위해 정부기관들이 사용한 상업적 제품 및 서비스를 위한 기준, 보안통제의 결점에 대한 해결방법, 정보보안 문제에 대한 업계 및 외국과의 협력 등이다.

하고 인사관리처(OPM : Office of Personal Management)는 정보보안교육 및 훈련을 지원하고 각 기관의 침해사고 대응 및 취약성 정보공유 및 조정 등을 포함한 기타 기관들의 역할을 규정하고 있다.[155]

그러나 OMB의 지침 성격을 가진 Circular A-130으로는 급증하고 있는 새로운 보안침해 및 기술에 대하여 충분한 대응을 할 수 없다는 인식하에 보완의 필요성이 제기됨에 따라 2000년 10월 정보보안 프로그램 관리와 평가측면을 강조하는 '정부정보보안개혁법'(Government Information Security Reform Act)이 제정된 것이다. 연방정부의 정보보안관리 강화의 필요성은 계속되었는데 정부정보보안개혁법이 2002년 10월까지 유효한 한시법적 형태를 가지고 있음에 따라 정부정보보안개혁법을 영구화할 수 있는 방안으로 2001년 11월 국토안보법의 일부로서 연방정보보안관리법(FISMA)이 제정되었다.[156]

라. 사이버보안연구개발법

2002년 11월 27일에 제정된 '사이버보안연구개발법'(Cyber Security Research and Development Act of 2002)의 주요 내용은 국립과학재단(NSF)과 국립표준기술원(NIST)에 새로운 연구 프로그램을 신설하는 것이다. 이에 따라 국립과학재단에 사이버안보 관련 연구개발의 혁신을 위한 연구센터(Institute for Security Technology Studies)와 장학금 제도를 신설하고 국립표준기술원에 정부·연구계·산업계의 연구보조금 프로그램을 신설하였다.[157]

마. 컴퓨터보안법

미국의 정보보호관련 최초법률로서 1987년 제정된 '컴퓨터보안법'(Computer Security Act)은 미국국립표준기술연구소(NIST)를 중심으로 정부에서 사용되는 컴퓨터보안에 기준 프로그램을 제공함과 동시에 연방정부 컴퓨터시스템의 운용에 관계되

155) http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.

156) http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

157) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ305.

는 정부 관련자의 교육을 목적으로 한다.

바. 기타 대통령령

대통령령으로는 클린턴 대통령이 최초로 공표한 PDD-63(중요기반시설 보호)와 2003년 2월 부시 대통령이 발표한 '국토안보대통령명령 제63호'(HSPD-63 : 국내 사고관리) 등이 있다.[158]

대통령령 제3호 '국토안보경보시스템'(HSPD-3 : Homeland Security Adv-isory System)은 2002년 3월에 테러 위험과 관련된 정보를 공유하고 이를 사전에 경고할 수 있는 시스템 창출을 규정하고 있다.[159]

대통령령 제5호 '국내 사고관리'(HSPD-5 : Management of Domestic In-cidents)는 2003년 2월에 미국 내 사고 발생 시 정부 간 및 민간영역과의 효율적 협력을 통해 관리할 수 있도록 그 체계를 정하고 있다. 특히, 동명령에 따라 국토안보부는 연방 국내사고 관리의 총책임자로 지명되었으며 테러 공격, 주요 재난 발생 등과 같은 비상사태의 예방, 준비, 대응 및 복구를 위한 연방자원 배분 및 업무조정의 책임을 부여받았다.[160]

대통령령 제7호 '주요기반 식별, 우선순위 설정 및 보호'(HSPD-7 : Critical Infrastructure Identification, Prioritization, and Protection)는 2003년 12월에 테러 행위로부터 보호해야 할 주요 기반시설 및 자산을 식별하고 보호활동의 우선순위를 설정하며 보호활동을 수행할 수 있는 프레임워크 구성을 규정하여 국토안보부 및 연방과 지방정부 등 기반시설 보호를 위한 참여자들의 책임과 역할을 정하고 있다.[161]

대통령령 제8호 '국가준비'(HSPD-8 : National Preparedness)는 2003년 12월에 미국의 테러활동에 대한 예방, 보호, 대응 및 복구를 강화할 수 있는 준비태세 강화 정책을 수립하도록 규정하고 있다.[162]

---

158) 국가 사이버안전을 위한 대통령 명령으로는 국가안보를 위한 대통령명령(NSPD)과 국토안보를 위한 대통령명령(HSPD)이 있다.

159) Homeland Security Presidential Directive-3 : http://www.fas.org/irp/offdocs/nspd/hspd-3.htm.

160) Homeland Security Presidential Directive-5 : http://www.fas.org/irp/offdocs/nspd/hspd-5.html.

161) Homeland Security Presidential Directive-7 : http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

162) Homeland Security Presidential Directive-8 : http://www.fas.org/irp/offdocs/nspd/hspd-8.html.

그 외 대통령령 제23호 및 제54호(HSPD-23/NSPD-54)는 2008년 1월에 연방정부 사이버보안에 대해 커다란 전략적 변화를 꾀하고자 미국 정부 전산망을 적극적으로 감시하는 정책을 수립하도록 규정하고 있다. 동 명령에 따라 국토안보부 내에 국가 사이버안전센터(NCSC : National Cyber Security Center)가 설립되었으며 국가 사이버 안전 센터의 미션은 연방 기관들 간의 협력을 통해 사이버 위협으로부터 미국 정부의 컴퓨터와 통신 시스템을 보호하는 것으로 알려지고 있다.

사. 2009 사이버보안법안

앞서 설명한 바와 같이 오바마 행정부는 2009년 '사이버공간 정책 리뷰'를 발표하고 국가사이버보안 정책 추진을 총괄할 사이버보안책임관(사이버 차르)을 임명하는 등 강력한 사이버보안 체계 확립을 위한 노력을 경주하고 있다. 이와 같은 오바마 행정부의 의지에 의회는 그에 상응하는 제도적 근거를 마련하기 위한 입법적 조치로 화답하고 있다. 즉, 민주당 상원의원 록펠러와 공화당 상원의원 스노위는 사이버 보안에 관한 포괄적 입법조치로서 '사이버보안법(안)'(Cybersecurity Act of 2009)을 국회에 제출(2009.04.01)하였다.

이 법안은 국가사이버안보 정세를 안정화하기 위한 전례가 없는 대응책으로 백악관 자문기구로 외부 전문가로 구성된 사이버안보 고문 위원단의 창설, 상무부 아래 실시간 정보시스템 마련 등의 내용을 담고 있는 것으로 알려졌으며, 크게 ① 연방정부 내 사이버안보 프로파일의 대폭적인 확장 및 사이버 관련 정부 기능 및 권한의 능률 강화, ② 국민 인식 촉진 및 인권 보호, ③ 사이버안보에 있어 정부와 민간 분야의 관계 재설정, ④ 장기적인 해결책 개발을 위해 사이버안보의 혁신과 창의력 촉진 등의 내용을 담고 있다.[163] 그런데 법안의 내용에는 인터넷 정보의 열람 내지 압수에 있어 영장주의가 제한되는 등 기본권 제한에 관한 사항도 포함되어 미국 내 기업, 시민단체 등은 프라이버시침해, 기업 활동 간섭 규제 등의 문제로 반발하고 있다. 사이버보안 비상사태 발생 시, 사고의 긴급한 해결을 위해 국민의 기본권을 제한하는 수준을 어느 정도까지 용인할 수 있을지에 대한 논란이 계속될 전망이다.[164]

163) 상세는 http://www.govtrack.us/congress/bill.xpd?bill=s111-773 참조.

164) 우리의 경우, '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조의3에서는 중대한 침해사고가

동 법안이 제정될 경우에 사이버보안에 관한 기본법적 지위를 지닐 것으로 예상되는 바, 귀추가 주목된다.

아. 국가자산으로서 사이버공간 보호법안

최근에는 상원 국토안보위원장인 Joe Lieberman 의원이 2010년 6월 16일 발의한 대통령에게 강력한 인터넷 통제권을 부여하는 것을 골자로 한 '국가 자산으로서 사이버공간 보호법안'(PCCNAA : Protecting Cyberspace as a Asset Act of 2010, S.3480)이 논란의 대상이 되고 있다. 동 법안은 크게 5개의 장으로 구성되어 있다. 즉, 제1장에서는 '사이버공간 정책실'(Office of Cyberspace Policy)의 설립과 구성, 역할 등을 규정하고 있으며, 제2장에서는 '국가 사이버보안 통신센터'(Natinal center for Cyberscurity and Communication)에 관하여, 제3장에서는 연방 정보 보안 관리를 위한 정책조정에 관하여, 제4장에서는 보안인력 양성을 위한 사항에 관하여 인력의 평가, 인력계획, 사이버보안 직업의 분류, 고용효과 측정, 교육 및 훈련, 인센티브 등 상세한 규정을 마련하였으며, 제5장에서 사이버보안 연구 및 개발, 조달 권한 등에 관하여 규정하고 있다.[165]

동 법안은 사이버보안 비상 상황 하에서 발동되는 대통령의 인터넷 통제권에 민간시스템의 인터넷 트래픽을 제한 또는 차단하는 내용이 포함돼 있다. 또 대통령실 내에 '사이버공간 정책실'을, 국토안보부에 '국가 사이버보안 통신센터'(NCCC)를 설치하도록 하고 있다. 특히 NCCC는 민간 부문의 웹사이트, 브로드밴드 사업자 등의 보안 상태를 모니터링 하는 권한을 갖는다. 인터넷서비스업체, 통신회사 등 정보통신 기반시설에 속하는 회사뿐 아니라 검색엔진 및 소프트웨어 업체들도 이 센터의 긴급조치에 즉각 협조해야 한다고 규정하고 있다.

무엇보다 동 법안은 사이버보안 비상상황(Cybersecurity emergency)하에서 발동되는 대통령의 인터넷 통제권에는 민간 시스템의 인터넷 트래픽을 제한하거나 차단하는 권한을 포함하고 있다. 이 때문에 동 법안 상의 긴급권이 사적 영역의 인터넷

발생할 경우, ISP가 이용자에게 보호조치를 취하도록 요청하고, 이용자가 이행하지 아니하는 경우에 해당 정보통신망을 통한 접속을 일시적으로 제한할 수 있다고 규정하고 있다.

165) 상세는 http://www.govtrack.us/congress/bill.xpd?bill=h111-5548 참조.

까지 차단할 수 있으며 개인의 프라이버시를 심각하게 침해할 수 있다는 비난에 직면하고 있는 바, 향후 동법안의 귀추가 주목된다.

제2절 영국의 사이버공격 대응체계

1. 개 관

영국은 기술적인 측면에서 미국과 함께 사이버안보 분야를 선도하고 있는 국가 중 하나이다. 영국 정부의 정보보호에 대한 노력은 법률에 의한 행위규제 보다 일반 국민에게 정보침해에 대한 의식을 제고하고 사전적 대처 방안계획과 실행 역할에 중점을 두고 있다. 조사권한규제법(RIPA), 컴퓨터부정사용법, 대테러 범죄 및 안전 보장법 등으로 해커와 바이러스 유포자를 처벌하고 있으며, 스팸규제는 프라이버시법리와 전기통신지침 등으로 이루어지고 있다.

영국은 정보통신 환경 변화와 이에 따른 정보보안 환경 변화에 적극적으로 대처하고 있으며, 이에 따라 정보보안과 관련한 입법 활동도 비교적 활발한 국가 중 하나이다.[166] 영국은 EU의 기본적 정보보안 및 개인정보보호 방침을 자국 법으로 수용하는데 적극적이며 미국·EU 등 타 국가들이 주도적으로 추진하는 정보보안 정책들을 받아들이고 있다. 정보보안과 관련해서 영국은 사이버범죄를 처벌할 수 있는 법률을 중심으로 상당히 적극적으로 관련 법률과 제도를 발전시켜왔으며, 특히 EU의 각종 지침을 자국 법으로 현실화시켜 국제적으로도 정보보안을 선도하고 있다.[167]

166) 이연수 외, 앞의 글, 76쪽.

167) 유럽 연합(EU : European Union)의 정보보안 관련 지침으로는 개인정보나 프라이버시를 안전하게 보호하고 통신네트워크의 안전성을 확보하는 것을 목적으로 하는 EU의 정보보호기본법에 해당하는 '프레임워크 지침'(Directive 2002/21/EC)이 대표적이며, 그 밖에 '안전한 인터넷 사회-대화, 협력 및 부권'(Communication from the Commission, 2006.5.31), '유럽 네트워크 및 정보보안 기구(ENISA : Europe Network and Information Security Agency) 설립에 관한 규칙'(Regulation(EC) No 460/2004), '사이버범죄방지조약'(Convention on Cyber Crime), '통신네트워크에 관한 데이터보존 지침' 등이 있다. 상세는 이연수 외, 앞의 글, 72-74쪽 참조.

영국의 사이버안전체계를 보면, 네트워크 및 정보보호 정책은 내각부 산하의 정보보증 중앙지원국(CSIA : Centeral Sponsor for Information Assurance)에서 정보보호 관련 활동에 대해 정부전체를 조정하며, 통상산업부(DTI : Department of Trade and Industry), 외무부 산하 정부통신총국(GCHQ : Government Communications Head Quarters)·통신전자보안단(CESG : Communications Electronics Security Group) 및 내무부 보안정보부(M15) 산하 국가기반보호센터(CPNI : Center for the Protection of National Infrastructure) 등이 국가전반에 걸친 정보보호 기관으로서 역할을 수행하고 있다.

정보보증중앙지원국(CSIA)에서는 2007년 국가정보보안정책(A National Information Assurance Strategy)을 발표하여, 기관의 효율적인 위협정보 관리를 위해 임원급의 책임과 의무를 강조하는 한편, 전문 기술인력 양성 및 홍보 정책을 추진하고 있다. 내각부는 정부기관의 보안정책을 확산시키기 위한 '정보보호 기본정책'(HMG Security Policy Framework, 2008년 12월) 등 정보보호 관련 정책을 발표한 바 있다.

2. 조직체계

가. 국가기반보호센터(CPNI)

국가기반보호센터(CPNI)는 국가보안국 산하의 '국가보안권고센터'와 '국가기반시설보안조정센터'(NISCC : National Infrastructure Security Co-ordina-tion Centre)[168], 정보인증에 대한 국가기술을 담당하던 CESG 등을 통합하여 2007년 2월 새로이 창설된 기관이다. 미국의 국토안보부와 유사하게 물리적 보안과 사이버공간 보안을 통

168) NISCC는 과거 영국의 대표적인 사이버 테러 및 전자침해사고에 대응 기관이었다. 영국 내각장관(Home Secretary)은 정부부처·기관 및 민간 분야 조직을 대상으로 전자적 공격으로부터 국가주요기반시설(Critical National Infrastructure)을 보호하기 위하여 1999년 12월 20일 NISCC를 창설하였다. NISCC의 주요 업무는 주로 통신, 에너지, 금융, 교통, 중앙정부, 상하수도, 보건서비스, 비상시태 서비스 등 국가주요기반시설(CNI : Critical National Infrastructure)을 위한 주요한 IT시스템 보호를 책임졌다. 기존 NISCC는 CPNI로 흡수되어 컴퓨터 네트워크 보안업무를 수행하고 있으며, NSAC는 인원 및 시설보안 업무를 담당하는 등 영국은 새로 발족된 CPNI를 통하여 물리적 보안과 사이버보안을 융합적으로 수행한다는 측면에서 미국의 국토안보부 설립취지와 유사한 것으로 평가된다.

할하는 CPNI는 영국 국가기간망 관련 공공기관 및 기업체에 보안자문 등 서비스를 제공하며 이러한 활동을 통해 주요 국가기반시설에 대한 테러위협을 사전에 차단하기 위해 노력하는데, 여기에는 다수의 정부부처와 기관이 공동으로 참여하고 있으며 해당시설과 관련된 민·관 조직의 정보·인적·물적 보안에 대한 종합적인 보안권고 활동을 수행한다.[169]

CPNI는 영국과 해외의 컴퓨터사고대응팀(CERT, Computer Emergency Response Team), 정보공유분석센터(ISAC, Information Sharing and Analysis Centre) 및 WARP(Warning, Analysis and Reporting Points) 회원사간에 정보공유를 하고 있다. CPNI는 국가주요기반시설 시스템을 운영하고 있는 회사를 직접적으로 조정하고 있으며, CPNI가 직접 일대일로 접촉할 수 없는 회사들에 대해서는 자문을 제공할 수 있는 CERT의 설립을 적극 권고하고 있다.

나. 오프콤(Ofcom)

Ofcom(Office of Commincations)은 통신영역에서 콘텐츠 및 기반시설의 전 영역을 규율한다. 이는 과거에는 다수의 내각 각부의 책임권한에 속하여 이 관련부서들을 감독하는 독립된 Commons Select Committee의 책임영역이었던 것을 통합한 것이다.[170] 2003년 통신법 제3조는 Ofcom의 주된 임무는 통신관련 문제에 있어서 시민의 이익을 추구하고, 관련시장에서 적절한 경우 경쟁을 촉진함으로써 소비자들의 이익을 추구하는 것이다.[171] Ofcom의 주된 의사결정기관은 이사회이며, 이사회는 집행부서와 비상임구성원들로 구성되어 있다. 수석 임원진으로 구성되어 Ofcom의 방향을 설정하고 조직의 관리 감독 책임을 지는 실행위원회를 두고 있으며, Board로부터 일부 권한을 위임받은 위원회(Committee)들과 자문기구를 두고 있다.[172]

169) http://www.cpni.gov.uk/About/whatWeDo.aspx.

170) 한국정보보호진흥원, 각국의 정보보호법제 및 집행체계에 관한 연구, 2007. 12, 51-52쪽.

171) Ofcom의 임무는 ① 전자기장주파수의 최적 이용확보, ② 광범위한 전기통신서비스가 국내 전역에서 이용 가능하도록 확보, ③ 광범위한 고질의 티비 및 라디오 서비스를 확보, ④ 방송에 있어서 다양성의 유지, ⑤ 시청자들을 유해내용으로부터 보호, ⑥ 시청자들을 불공정성 또는 프라이버시 침해로부터 보호 등이다.

172) http://www.ofcom.org.uk/about/how-ofcom-is-run.

다. 통상산업부(DTI)

민간분야에서는 통상산업부(DTI, Department of Trade and Industry)가 정보보안의 중요성에 대한 인식제고와 '정보보안관리에 대한 표준'(BS 7799)의 사용 권장 등을 통해 정보보안 향상에 노력하고 있다. 통상산업부에서는 기업들에게 정보보안 관리에 관한 좋은 방식을 권장하고 국내외 차원에서 정보보호를 개선하기 위해 필요한 체계적 정책을 제공하는 것을 임무로 한다.

라. 정부통신총국(GCHQ)

외무부 산하 영국의 통신정보기관으로서 전자기파, 음향, 기타 설비물로부터 나오는 방사물, 암호화된 물건 등과 같이 정보자료와 관계되거나 이로부터 생산되는 정보를 획득·처리하고 있다. 또한 정보수집, 암호해독, 통·번역, 전산망 상의 정보해독, 해독을 위해 수집된 정보를 국방부 소속 국방정보요원 등 전문가 집단에게 제공하는 한편 암호관련 정책을 수립하여 지원하고 있다.

마. 전자통신보안그룹(CESG)

영국 전자통신보안그룹(CESG : Communication-Electronics Security Group)은 정부통신총국(GCHQ)에 소속되어 있으며, 정보보증(IA, Informa-tion Assurance)을 담당한다. CESG는 정보공유를 안전하게 할 수 있는 환경을 만드는 것을 목적으로 하며 정부부처 및 공공기관 그리고 군을 대상으로 하지만 다양한 민간 회사들에게도 관련서비스를 제공해준다. 특히 전력·수도·보건 등 중요한 기반시설과 공공시설들이 주요 대상이 된다.[173] 영국의 정보보호 관련 정책 및 지침 수립을 지원하고 각 부처 정보보호정책 실행에 필요한 기술자문 및 솔루션도 제공한다. CESG 산하 응용보안기술부는 200년 초에 정부 서비스 분야에서 새롭게 부상하는 IT기술에 대처하고 영국의 주요 국가기반자원을 보호하기 위한 목적으로 구성되어 새롭게 개발되는

173) http://www.cesg.gov.uk/policy_technologies/index.shtml.

기술들의 특징과 장점 및 제한성에 대한 지식과 이를 이해하는 영역까지 업무를 확장하였다. 이러한 방법을 통해 영국정부는 진행 중인 각종 IT사업에서 즉시적인 단기권고, 협의업무와 전자정부구현 및 안전한 인터넷 공간을 유지하기 위한 활동을 수행하고 있다.

바. 국립 하이테크범죄대책단(NHTCU)

국립하이테크범죄대책단(NHTCU, National Hi-Teck Crime Unit)은 지난 2001년 4월 컴퓨터 범죄수사를 목적으로 창설되었으며, 2000.11 영국의 내무장관이 의회에 보고한 국가하이테크범죄전략이 계기가 되었다.[174] NHTCU는 영국에서 발생하거나 영국에 영향을 미치는 모든 인터넷 범죄및 하이테크 범죄를 담당하며 NISCC · UNIRAS뿐만 아니라 미국의 NIPC(National Infrastru-cture Protection Center)와도 업무 공조를 하고 있다. 또한, 정부와 기업간 협력관계를 증진시키기 위해 노력하고 있는데, 새로운 전자범죄에 대항하기 위해 기업의 기밀성 유지를 위한 강령(Confidentiality Charter) 등을 발표한 바 있다. 주요 임무는 심각하거나 조직화된 하이테크 범죄에 대항하기 위한 대응활동 지원, 국가기반시설에 대한 모든 심각한 위협에 대한 수사, 전략적인 위협성 평가업무 수행, 법 집행업무지원 및 공동대응, 법 집행기관 및 사업자들에게 조언 제공 등이다.

사. 영국의 사이버수사조직

2001년 4월 컴퓨터 범죄수사를 목적으로 영국 경시청 소속 국립하이테크범죄국(National Hi-Tech Crime Unit : NHTCU)을 창설하였고, 하부조직은 범죄수사부, 정보부, 전자증거부, 기술지원부 등 4개의 부로 구성되어 있다. 범죄수사부는 조직화되거나 심각한 하이테크 범죄를 수사하고 법원 지원을 담당하며 정보부는 영국의 모든 법집행기관과 정보기관들을 위하여 전략적·전술적 정보를 제공한다. 전자증거부 NHTCU에 의해 수행되는 하이테크 범죄수사를 위한 포렌식 기술을 지원하고, 기술지원부는 법원이나 정부를 위한 기술지원과 컨설턴트를 담당한다. 이후 2005년에 심

174) http://en.wikipedia.org/wiki/National_Hi-Tech_Crime_Unit.

각하게 조직화된 범죄 및 경찰법(The Serious Organised Crime and Police Act 2005)에 근거하여 2006년에 NHTCU의 조직을 흡수한 중대조직범죄수사청(SOCA : The Serious Organised Crime Agency)이 창설되었다. SOCA는 내무부에 의해 지원되지만 운영은 독립적인 비정부 공공조직으로 집행기관이다.[175]

그러나 SOCA가 국가적 사무에 전념하여 민생과 관련된 사이버범죄에 대한 전국적 대응을 제대로 수행하지 못하게 되자 오히려 민간기업의 계속된 요구로 2008년에 경찰 중앙전자범죄대책단(PCeU)을 설립하게 되었다.[176]

3. 법제도 체계

가. 대테러범죄 및 안전보장법

영국은 기존의 테러방지법이 전시에 준한 임시적 성격을 띤 법이기 때문에 강력한 제재조치를 가지고 있었고, 이는 인권침해의 가능성이 높다는 비판을 받았다. 이러한 문제점을 해결하기 위하여 영국은 2000년 7월 20일 새로운 테러법(Terrorism Act 2000)을 제정하여 2001년 2월 19일부터 시행하게 되었다. 이 법은 기존의 테러가 북아일랜드 사태에 초점을 맞춘 임시법적 성격을 가진 것인데 비해 영구적인 성격의 법으로 대체하였다는데 의미가 있다. 이 법은 민사적 입증책임의 분배의 원칙에 따른 테러단체 통화의 압수와 금융기관에 대한 테러수사 목적의 예금계좌 확인 요구권을 신설하는 등 테러에 대한 수사권을 강화하고 처벌을 위한 절차상 특례를 인정하였다. 또한 범위를 넓혀 영국을 기반으로 자행되는 모든 국제 테러활동에 대해 단속을 가능하도록 하였다. 이와 같이 북아일랜드 문제에 대응하기 위하여 테러대책을 수립하고 있었으나 9·11 테러가 발생하면서 이러한 수단 외에 테러를 방지하기 위한 강력한 법적인 대책을 수립하였다.

2001년 12월 14일 제정된 '대테러범죄 및 안전보장법'(Anti-terrorism, Crime and Security Act 2001)은 미국의 9·11테러 이후 테러 대응을 위해 필요한 여러 테러대

175) 이재은, 앞의 글, 78쪽 참조.

176) 이동희/장윤식/김석범/표창원, "국제 사이버범죄 아카데미 모델개발(중간보고서)", 경찰청, 2010, 36쪽.

책 관련 내용을 포함하고 있다. 14개 장으로 이루어져 있으며 테러리스트 자산, 동결명령, 인종 및 지역간 문제(racial hatred), 경찰권한, 항공기보안, 데이터보안 등을 규정하면서, 테러범죄자에 대한 자산동결, 출입국관리, 병원체 및 독극물 통제, 통신자료 취득 등에 관한 기존의 규정을 개정하여 테러에 관한 수사권을 강화하고 있다. 정보보호 관련 주요 내용으로는 동법 제11편에 통신 데이터(전화, 인터넷 및 우편내용 등) 보전을 위한 권한 관계를 규정하고 있다.[177]

나. 조사권한규제법

총 5개장으로 구성된 '조사권한규제법'(RIPA : Regulation of Investigatory Power Act of 2000)은 통신감청을 위한 것으로서 인터넷이나 컴퓨터 암호화기술의 발전과 더불어 일반인을 모니터하기 위한 기술을 기반으로 하는 법이다. 영국정부는 이 법을 통해서 기업이나 개인에게 암호 키를 강제적으로 개시시키는 권한을 영국 경찰에게 부여하는 준비를 진행하고 있다.[178]

다. 컴퓨터부정사용방지법

컴퓨터부정사용방지법(Computer Misuse Act 1990)은 ① 허가받지 않고 컴퓨터 자료에 접근하는 행위(동법 제1조), ② 추가적인 범죄행위를 실행하거나 그 실행을 돕기 위한 목적으로 허가받지 않고 접근하는 행위(동법 제2조), ③ 허가받지 않고 컴퓨터의 자료를 변경하는 행위(동법 제3조) 등을 처벌하고 있다. 즉, 모든 컴퓨터 소프트웨어의 불법복제금지 등 비인가자에 의한 컴퓨터 접속을 금지하고 있는데, 여기에는 일반인의 취미활동이나 테스트를 위한 접속도 포함되어 이를 위반하는 경우 6개월의 구금, 혹은 5000파운드의 벌금형을 부과한다.

또한 사기 및 도용 등 범죄를 목적으로 한 비인가된 접속을 금지하며, 범죄를 목적으로 한 행위에 해킹을 포함하고 있어 이를 위반한 경우 5년간 구금 혹은 벌금형을 부과한다. 뿐만 아니라 이 법에 의해 바이러스 등의 유포행위를 포함, 컴퓨터 소

177) 상세는 http://www.legislation.gov.uk/ukpga/2001/24/contents.

178) 이연수 외, 앞의 글, 76쪽.

프트웨어나 데이터에 대한 불법 수정행위를 금지하며 이를 위반한 경우 5년간 구금 혹은 무한대의 벌금형이 부과될 수 있다.[179]

라. 정보보안관리에 대한 표준(BS 7799)

1995년 정보자산을 체계적이고 표준적인 관리지침 및 방법에 따라 관리할 목적으로 영국 표준기관(BSI : British Standard Institution)이 '정보보안관리에 대한 표준'(BS 7799 ; British Standard for Information Security Management)을 제정하였다. 동 표준은 Part 1과 Part 2로 구성되어, Part 1은 조직에서 정보보호관리 체계를 수립하기 위한 지침으로 활용할 목적으로 2000년 12월에 국제표준인 ISO/IEC 17799로 채택되었다. Part 2는 정보보호관리체계의 규격(Specification)을 제시하는 인증 심사 시 활용되는 지침과 설명을 통해 정보보안 관리시스템의 모델을 지원해 주는 내용으로 2005. 10월에 역시 국제표준인 ISO/IEC 27001로 채택되었다.

제3절 독일의 사이버공격 대응체계

1. 개 관

일반적으로 독일에서 IT 의존적 중요기반시설의 안전 및 보안개선의 필요성 인식과 필요조치 실행 의지는 서서히 지속적으로 높아가고 있다. 특히 미국의 9·11 사건 이후 막연한 절박감을 가지게 되어 국제적 협력에 관심을 기울이고 있다. 독일의 사이버안전체계는 '연방정보기술안전청설치법'(BSIG : BSI-Erri-chtungsgesetz)에 의해 설립된 연방정보기술안전청(BSI : Bundesamt für Sicherheit in der Informaion stechnik) 및 연방통신망청법상의 연방통신망청(BNetzA)이 주로 담당하고 있다. 1991년에 설립된 내무부 산하 '연방정보기술안전청'은 실질적인 국가 사이버안전업무를 총괄하는 기관으로서 정보기술을 적용했을 때 야기되는 보안위험을 연구하고 보안조치, 정보기술보안을 위한 기술적 방법과 장치는 물론, 정보기술 시스템 및 그

179) 이연수 외, 앞의 글, 77쪽.

구성요소에 대한 검사·평가를 위한 기준·방법 및 도구를 개발하여 정보기술 시스템 및 그 구성요소의 보안을 검사·평가하여 보안인증서를 부여하고 있다. 한편, 경찰 및 형사소추기관의 법적 임무를 지원하며, 테러활동 감시 등 정보활동을 통하여 수집한 첩보를 활용, 평가하는 작업을 지원함과 동시에 정보기술보안 문제 발생 시 생산자와 유통자 및 사용자에게 자문 등의 임부를 수행하기도 한다.[180] 독일은 정보보안을 통해 정보통신기술의 신뢰를 조성하고 정보사회의 기회를 최대한 이용하기 위해 독일 자체의 정보보안 가이드라인(IT-Grundschutz-die Basis für IT-Sicher-heit)을 제정하여 시행하고 있다.

독일은 미래사회에서의 정보보호 및 정보보안에 대한 중요성을 깨닫고 1991년에 BSI를 창설하여 상당한 예산 및 인력투자를 해 왔다.[181] 독일의 경우 정보보안을 위해 국가적 차원에서 상당한 지원을 하고 있고 사경제 분야에 있는 기업도 점차 정보보안과 관련한 책임의 중대성을 인식하고 대비책을 마련하는 과정에 있다.

2. 조직체계

독일은 미국이나 중국처럼 사이버공격과 관련 심각한 상황에는 이르지 않았으나 국가적으로는 이에 대한 대응을 위해 조직 체계를 비교적 상세하게 구분하여 역할과 책임 분담을 분명히 하고 있다. 사이버안보와 관련해서는 주로 연방정보기술안전청(BSI)에서 담당하고 추적수사와 디지털증거분석 등은 연방범죄수사청(BKA)[182]에서

180) 국가사이버안전센터, Monthly 사이버시큐리티 7월호, 2007. 7 참조.

181) BSI, Zertifizierte IT-Sicherheit, 17쪽 이하.

182) 독일의 비스바덴(Wiesbaden)에 위치하고 있는 독일 연방범죄수사청(BKA)은 1951년에 설립되었으며, 간첩수사, 테러·마약·위조지폐·조직범죄 및 국민 경호업무를 담당하고 있다. 연방수사청(BKA)는 주의 범죄수사청(LKA)와는 독립적인 조직으로서 협력관계에 있다. 연방범죄수사청(BKA)은 연방범죄수사청법(BKA-Gesetz)에 의해 설립되었다. 연방범죄수사청은 국제협력국(IK), 조직·일반범죄국(SO), 종합 범죄경찰업무·자문감식국(ZD), 범죄기술국(KT), 총무관리국(ZV), 정보기술·IT국(IT), 범죄연구소(KI), 국가보안국(ST), 경호국(SG) 등으로 구성되어 있다. 연방범죄수사청(BKA)은 독일 경찰의 정보와 커뮤니케이션의 중앙기관이다. 범죄수사청(BKA)은 경찰기관으로서 기본적인 경찰업무는 주의 범죄수사청(LKA)에서 수행하고, 연방의 연방범죄수사청(BKA)은 기본법에 규정된 국가안보와 관련된 특정분야의 업무 만을 수행한다. 구체적으로 연방범죄수사청(BKA)은 ① 정보에 관한 업무 [“정보수집”(Informationssammlung), “정보평

담당하고 있다.

가. 연방정보기술안전청(BSI)

연방정보기술안전청(BSI : Bundesamt für Sicherheit in der Information-stechnik)은 1950년대 설치된 '중앙암호제도실'이 그 전신으로서 연방 행정정보의 안전성 및 고유직무와 국외 비밀정보의 수집 분석 등 업무를 수행해 왔다. 연방정보기술안전청(BSI)은 독일 연방 내무부 산하의 국가기관으로서 실무상 정보통신의 안전 영역에 대한 관할권을 가진 가장 중요하고 독보적인 독립된 국가 정보보안기관으로 연방기관에 대한 정보보안 업무를 수행한다. 1987년에는 컴퓨터 안전성을 그 관할범위에 포함시킨데 이어 업무범위 확대 등 기관의 중요성을 고려하여 1989년에 '중앙정보기술안전실' 로 명칭을 변경하고 업무영역도 종래의 협소한 국가적 사무의 범위를 넘어 정보기술의 사법적 적용 및 안전성에 이르기까지 포괄적인 업무를 담당하였다. 이어 연방정보기술안전청설치법(BSIG, 1991)에 의해 내무부장관 관할 하의 연방상급 관청으로 승격되었다.[183] 동법에서는 평가·인증업무는 물론, 정보통신기술 시스템의 연구와 개발, 그리고 정보통신시스템 및 내용의 심사를 통한 안전성 위험 조사 및 정보통신시스템 안전성 검사, 평가와 인증서의 발급, 정보통신시스템의 허가를 비롯하여 국가기관 및 민간기관에 대한 기술지원 및 자문을 제공토록 규정하고 있다.[184]

연방정보기술안전청(BSI)은 행정국과 1국, 2국, 3국의 4개국으로 되어 있다. 1국

가"(Informationsauswertung) 및 "정보조정"(Informationssteuerung)], ② 전자수사(elektronische Fahndung)와 정보시스템(Informationssystem)의 구축, ③ 범죄인식서비스(Erkennungsdienst), ④ 본질적인 범죄기술(wesentliche Kriminaltechnik) 업무, ⑤ 아동포르노범죄(Kinderpornografie), ⑥ 범죄정책(Kriminalstrategie)업무 등을 수행하고 있다. 특히 테러·간첩사건의 경우에는 연방검찰(GBA)의 수사지휘하에 연방범죄수사청이 전담하고, 주 범죄수사청은 극히 예외적인 경우에 한해 연방검찰의 수사지휘를 받아 수사에 참여하게 된다. 다만 구체적인 범죄사건이 아닌 시위·데모 등 예상되는 위협에 대한 예방활동은 검찰의 수사지휘를 받지 아니하고 전적으로 경찰의 업무범위에 속한다. 독일 테러방지기관에 대한 상세는 경찰청, 외국의 대테러·안전활동, 1999; 국가정보원, 5개국의 국가 대테러 대응체제비교, 2000; 국회도서관 입법전자정보실, 일본의 테러대책특별조치법, 국회도서관, 2001 등 참조.

183) 이렇듯 독일은 사이버안전기관의 설립 근거와 조직의 활동사항을 법률로 규정하고 있는데 반하여, 우리의 경우 대통령 훈령인 '국가사이버안전관리규정'에 근거하고 있는 바, 유관기관간의 협조를 유인하는데 한계가 지적된다(이연수 외, 앞의 글, 83쪽).

184) http://www.bsi.de/bsi/index.htm.

에는 전략 어플리케이션부와 인터넷 보안부가 있다. 2국에는 네트워크 보안부, 암호기술·기반기술부가 있다. 그리고 3국에는 대도청기술부와 일반 IT 보안부가 있다. 정보통신기술에 대한 보안취약성연구, 정보통신시스템의 보안성 시험·평가를 하며, 경찰 등 관련기관에 조언을 한다. 물리 수학 컴퓨터전문가 등 총 350여 명의 인원이 연 600억 원의 예산을 사용하면서 사이버안보를 위해서 공공과 민간부문을 지원하고 있다. BSI의 기능 및 주요업무는 ① 인터넷 보안에 대한 평가와 인증, ② 컴퓨터 긴급구조팀 및 바이러스 센터 관리, ③ 네트워크 보안, 암호술, 공공 핵심 기반시설 보호, ④ 중요 정보통신기반시설 보안 등이다.

나. DFN-CERT

정보통신기반구조 사고 대응을 위해서 독일의 연구 네트워크를 위한 컴퓨터긴급대응팀인 DFN-CERT(Digital Freedom Network Computer Emergency Response Team)을 운영하고 있는데, 이는 사이버사고 처리, 사건 처리에 필요한 기술적 지원, 관련 정보의 수집·제공, 취약성 분석 등의 업무를 수행한다. IT 네트워크와 시스템에 대한 공격의 사례가 증가하는 것은 컴퓨터 및 네트워크보안에 관련된 문제를 해결하기 위한 중앙조정 기관이 필요하다는 것을 보여주고 있다. 독일 CERT는 예방 및 대응 기능을 수행하고 있다. 예방의 측면에서 IT보안에 대한 질문에 답하고 제품에 대한 취약성을 경고하고 보안과 관련된 사건에 대해 정보를 제공한다. 아울러 사고의 경우, 시스템의 복구를 지원한다. 독일 CERT는 연방정부와 일부의 민간 사용자에게 서비스를 제공한다.

다. 독일의 사이버수사조직

독일은 연방수사청(BKA)에 중대범죄조직국 소속으로 총 4개의 계로 구성된 하이테크·컴퓨터 범죄과를 두고 있다. 1계는 행정관리, 국제 워킹그룹 활동, 2계는 범죄정보 및 전략분석, 국제공조 24/7 네트워크, 3계는 인터넷 모니터링, 4계는 사이버수사 전담 체계로 구성되어 있다. 국제협력 활동과 실시간 국제공조 기능을 분리하여 운영하고, 범죄정보 및 전략분석 등 사이버테러에 대한 정보분석 기능을 별도로

운영하고 있다. 인터폴 국가중앙사무국(NCB), 유로폴 연락국(NLO), G8 경찰협력, UN 마약 및 범죄예방기구(UNDCCP) 등과 다양한 국제협력 활동을 전개하고 있다.

독일은 유럽평의회의 사이버범죄 방지협약의 이행 등을 위해 2007년 8월 컴퓨터 범죄 대응을 위한 제41차 형법 개정법률을 발효함에 따라 사이버범죄의 규율에 관한 국제적인 표준으로 인정받고 있고, 사이버범죄 영역에서의 국제협력뿐만 아니라 국내 입법상의 모델로서도 중요한 의미를 가지는 국가[185]로 평가되고 있다.

3. 법제도 체계

가. 정보통신법(TKG)

2004년 제정된 정보통신법(TKG : Telekommunikationsgesetz)은 정부기관이 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해 인터넷통신 사업자와 정보통신서비스 제공하는 모든 책임자에게 고객 정보에 대한 정부의 접근 요청시 이를 지원해 주도록 하고 있으며, 이러한 데이터는 정부의 감시기관이 직접 접근할 수 있도록 규정하고 있다.[186]

제7장(비밀, 정보보호 및 공공안전)에서 특히 공공안전을 위해 사업자들이 긴급전화가 가능하도록 할 의무, 기술적 보호대책과 감시가 가능한 방법을 마련할 의무 및 정보제공 의무를 지게 하여 국가 본연의 기능을 수행할 수 있도록 사업자 등에 대한 자료요구 권한, 사업자들의 관련 시설지원 의무 등을 구체화하고 있다. 한편 '정보보안책임자'를 임명하여 '정보보안에 관한 계획'을 수립하여 정보보안계획의 내용과 유지는 연방통신망청의 통제를 받도록 제도화되어 있다.[187]

185) 오병두, "독일의 컴퓨터범죄 대응을 위한 제41차 형법개정법률 : 배경, 내용 및 시사점", 형사법연구 제19권 제3호, 2007 가을, 895-896쪽 참조.

186) 정보보안과 관련하여 개인정보보호에 대해서는 '연방데이터보호법(BDSG)'이 규율하고 일반적인 우편, 통신, 전화 등과 관련한 정보보안은 2004년 제정된 정보통신법이 다루고 있다.

187) 기타 상세한 내용은 한국정보보호진흥원, 앞의 보고서, 107쪽 및 117-126쪽 참조.

나. 국제테러대책법

독일은 유럽에서 가장 먼저 테러범죄자를 처벌하기 위한 법적 조치를 강구하여 실체법적 측면에서 테러범죄의 처벌범위를 확대하고 형량을 높이는 한편, 절차법상으로는 테러범죄자인 피의자 또는 피고인의 권리 및 수형자로서의 권리를 현저히 제한하는 특칙을 규정하였다. 1971년 테러가 형법[188]에 규정되기 시작한 이래 본격적인 입법적 조치가 취해지기 시작한 것은 1976년 4월 22일의 제14차 형법개정에서였다. 독일에서 테러와 관련하여 처벌되는 행위는 1976년 대테러 법에 의하여 테러단체를 조직하는 행위가 처벌대상이 되었다. 이는 범죄단체조직에 대한 특별구성요건으로서의 성격을 지닌다. 이는 사전에 테러를 막는다는 전략에 기인한 것으로 독일의 테러전략의 중심적인 조항이다. 독일정부는 2001년 9·11 테러를 계기로 한층 강화된 테러대책을 수립하였는데, 그 주요 내용은 테러대책을 위한 재정확보, 법 개정을 통한 효율적인 테러기관의 권한 강화, 신원확인, 주요시설의 보안 강화 등이다. 이에 따라 국제테러대책법(Gesetz zur Bkämpfung des internationlen Terrorismus)이 제정되어 2002년 1월 1일부터 발효되었다. 그 주요내용은 외국 테러단체에 대한 처벌의 확장이었다.

다. 연방정보기술안전청설치법(BSIG)

연방정보기술안전청설치법(BSI-Errichtungsgesetz)은 정보통신 안전영역에 있어서

188) 테러의 개념에 대해서는 현재까지 국제적으로 공인된 개념이 정립되어 있지 않으나 현방헌법보호청(BfV)에서는 "테러란 정치적 목적을 달성하기 위해 지속적으로 추구되는 활동으로 생명·재산 등을 위협하는 범죄행위 중 형법 제129a조 제1항에 명시되어 있는 범죄 또는 그와 같은 범죄행위의 구성에 도움을 주는 부수적 행동을 말한다"고 개념정의하고 있다. 이러한 테러개념을 살펴보면 먼저 정치적 목적이라 함은 독일의 자유민주적 기본질서를 와해시키고 사회적 변혁을 유도하려는 목적이 있는 경우를 말한다. 여기서 말하는 이념이란 정치·경제·사회·종교 등 어떠한 것이라도 이 개념에 포섭된다. 가장 전형적인 경우는 극좌세력의 사회주의 혁명이나 극우세력의 신나치주의 재건, 이슬람근본주의 등이다. 둘째, 조직적 활동이란 장기간에 걸쳐 조직적으로 활동함을 말한다. 따라서 살인·폭력·방화 등 테러의 범위에 해당한다고 할지라고 즉흥적 인 행동을 "테러"의 범위에 해당하지 않는다. 셋째, 형법 제129a조의 중대한 범죄행위해 해당하여야 한다. 독일 형법 제129a조 제1항에는 살인·납치·폭파 등의 범죄를 저지르거나 자금지원을 통하여 범죄행위를 지원하는 행위를 테러에 해당한다고 보고 있다.

가장 대표적인 기관인 연방정보기술안전청의 설립 근거법이다. 동법에서는 평가·인증업무는 물론, 정보통신기술 시스템의 연구와 개발, 그리고 정보통신시스템 및 내용의 심사를 통한 안전성 위험 조사 및 정보통신시스템 안전성 검사, 평가와 인증서의 발급, 정보통신시스템의 허가를 비롯하여 국가기관 및 민간기관에 대한 기술지원 및 자문을 제공토록 규정하고 있다.[189)]

제4절 프랑스의 사이버공격 대응체계

1. 개 관

프랑스는 선진적으로 정보화가 진행된 서유럽의 다른 국가와 비교할 때 상대적으로 정보화가 늦은 나라였다. 1990년대 중반까지만 해도 프랑스는 이웃 선진유럽국가에 비하여 행정의 정보화뿐만 아니라 사회 전체의 정보화가 뒤져 있었다고 평가된다. 그러나 1998년 이후 매우 의욕적이고 계획적으로 정보화를 추진하고 있는 것으로 알려진다.

프랑스는 중앙정보시스템보안국(DCSSI) 내에 프랑스 정부 CERT인 CERTA를 구축 운영하고 있으며 사이버보안운영센터를 구축하여 각급기관에 대한 사이버위협정보를 제공하고 있다. 아울러 프랑스 정부는 사이버보안위기관리체계를 수립하여 경계 수준을 5단계로 분류하고 DCSSI로 하여금 각 경계단계에 따른 일련의 사이버보안 기능적 조치를 수행하도록 하고 각 정부부처로 하여금 사이버보안조치를 실행하도록 하고 있다.

이렇듯 프랑스는 사이버 보안을 국가 안보의 문제로 인식하여 총리실 직속의 국방사무국(General Secretariat of National Defense : SGDN)으로 하여금 사이버 보안을 담당하도록 하고 있다. 즉 1996년 1월 29일에 발표된 프랑스 법령 96-67은 국방사무국으로 하여금 정보 시스템 보안(Information Systems Security)에 대한 책임을 부담하도록 명확하게 규정하고 있다. 또한 2001년 7월 31일에 발표된 프랑스 법령

189) http://www.bsi.de/bsi/index.htm.

2001-693은 국방사무국내에 중앙정보시스템보안국(Central Directorate for Security of Information Systems : DCSSI)을 설립하여 사이버 공간과 프랑스 정보 시스템에 대한 보안을 수행하고 신뢰할 수 있는 정보화 사회를 조성하도록 하고 있다.

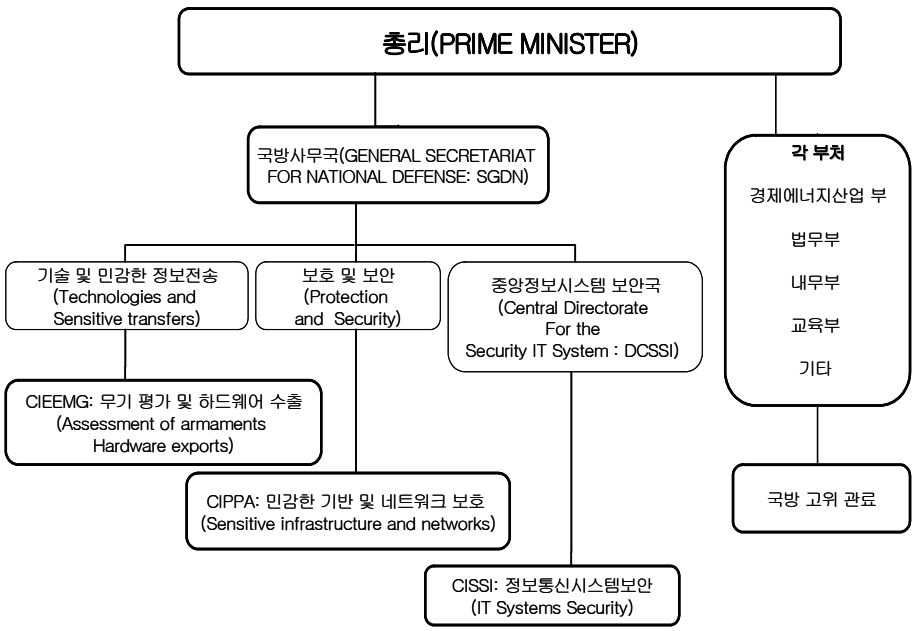


그림 6 프랑스 사이버 보안 관련 국가적 조직체계

2. 조직체계

가. 총리실 중앙정보시스템보안국(DCSSI)

2001년 5월, 총리 국방담당보좌관(SDGN : Secrétaire Générale de la Defense Nationale) 산하의 '중앙정보시스템 안전대책실'을 '중앙정보시스템보안국'(DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information)으로 확대 개편하였다. DCSSI의 전략적 주요 목표는 프랑스 주요 국가기반시설 정보시스템의 안전 확보와 정보사회의 발전을 촉진하기 위한 신뢰받는 환경조성이라고 할 수 있으며 그

임무는 ① 정보시스템안보관련 정부정책 입안 및 부처업무 조정, ② 국내외 정보·통신보안분야 규제 및 허가 등 업무, ③ 정부기관 정보시스템 위협에 대한 전반적 평가 및 예방·대책지원, ④ 정보통신보안분야 과학기술적 전문지식의 개발, ⑤ 정보보안에 관한 인식확산과 훈련 등이다.[190]

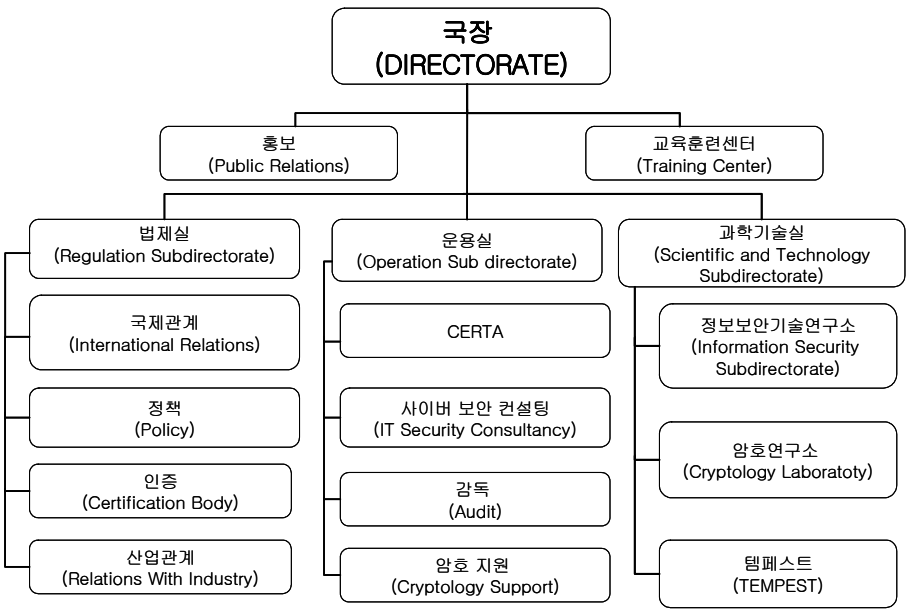


그림 7 프랑스 DCSSI 조직도

DCSSI는 법제실, 운용실 및 과학기술실로 구성되어 있다. 법제실은 DCSSI의 국제관계, 정책, 인증 및 산업관계 부서로 구성되어 있다. 법제실은 국제관계와 산업분야에 대한 업무를 수행하며, 정보보안 분야에서의 DCSSI 규칙을 작성, 실시하고 인증업무를 수행한다. 운용실은 통신 및 정보보안 분야에서의 프랑스 정부의 정책시행을 지원한다. 운용실은 프랑스 정부 CERT인 CETRA를 운영하고 있으며, 정보보안 분야에서 정부의 다른 기관들을 지원하고, 정부의 정보보안시스템을 조사·평가하고, 정부기관 내부에서의 암호사용을 감독한다. 과학기술실은 정보기술, 통신보안, 암호화의 분야에서 프랑스 정부를 대표하고 DCSSI의 정책실행을 기술적으로 지원한다.[191]

190) http://www.ssi.gouv.fr/en/dcssi/index.html.

프랑스 정부는 '사이버보안 경보 및 위기관리'를 위하여 인식제고, 위협·사고·취약성 분석, 적절한 사이버보안조치 선정 및 각 부처 자체 사이버보안 조치를 포함한 사이버보안조치의 실행 등 4단계를 수립하고 있다. 또한 사이버보안경계계획을 수립하여 경계 수준을 5단계로 분류하고, DCSSI로 하여금 각 경계단계에 따른 일련의 사이버보안 기능적 조치를 수행하도록 하며 각 정부부처로 하여금 사이버보안조치를 실행하도록 하고 있다.

또한 사이버위협에 대한 프랑스 정부의 계획-VIGIPIRATE(IT 보안 측면) 및 PIRANET 계획을 조정하기 위하여 '사이버보안운영센터'(ITSOC : IT Security Operation Center)를 DCSSI 내에 설립하였다. 사이버보안운영센터는 기술적 활동, 조정 활동 및 커뮤니케이션 활동을 주요 임무로 수행하고 있다. DCSSI의 사이버보안운영센터는 프랑스 정부 CERT인 CERTA를 통하여 다양한 통로로 사이버위협 정보와 대응을 위한 관련 정보를 수집하여 이를 프랑스 정부부처들에게 제공하고 있으며, 프랑스 정부부처들로부터 사이버위협정보 등을 제공받고 있다. 또한 사이버보안운영센터는 사이버보안통합 및 부처의 조정을 통하여 사이버위협 관련 정보를 파악하고 있다. 사이버보안운영센터는 프랑스 정부 CERT인 CERTA와 사이버보안 통합 및 부처조정을 통하여 파악한 사이버위협정보를 각급기관의 고위관리들에게 제공하고 있다.[192]

나. 국방사무국(SGDN)

프랑스 국방사무국은 국내외 안보 문제에 관하여 책임을 부담하고 있다. 국방사무국은 프랑스 총리의 직접적인 명령을 받고 있으며 사이버보안 및 주요기반보호와 관련된 정부 부처들의 활동을 조정하고 있다. 1996년 1월 29일에 발표된 프랑스 법령 96-67은 국방 사무국으로 하여금 정보 시스템 보안(Information Systems Security)을 완수하는 책임을 규정하고 있으며 2001년 7월 31일에 발표된 프랑스 법령 2001-693은 중앙정보시스템보안국(the Central Directorate for Security of

191) http://www.ssi.gouv.fr/site_article18.html.

192) 오일석 외, "미국과 프랑스 정부의 사이버조기 경보 체계", 정보보호학회지 제15권 제1호, 2005. 2, 6쪽.

Information Systems : DCSSI)을 창설하도록 규정하고 있다. 국방사무국은 국방 분야 및 민간분야 관련 정보통신기술의 보안에 중점을 두면서 국방정책 및 보안정책의 과학·기술적 혁신에 대하여도 책임을 부담한다. 이와 관련하여 국방사무국은 DCSSI와 긴밀하게 협력하고 있다.[193]

다. 국립경찰 정보통신기술범죄수사부(OCLCTIC)

경찰청 형사국 산하에 1994.6. 창설된 정보통신기술범죄단속반(BCRCI : la Brigade Centrale de Répression de la Criminalité Informatique)을 2000.5. 형사국 재정경제국(SDAEF) 산하 중앙정보통신기술범죄대응센터(OCLCTIC : l 'Office Central de Lutte contre la Criminalité liée aux Tsechnologies de l'Information et de la Communication)로 확대 개편하였으며[194], 산하에 19개 지방수사대(Section Economique et Financière)가 편제되어 정보화범죄전문수사관이 배치되어 있다. 군인경찰·세관·기타 관련부처 등 정보통신기불범죄 관련 범정부적으로 취합 수사한다. OCLCTIC의 권한들은 사이버분야의 새로운 테크놀로지와 관련된 특수한 범죄들의 사법상 처리를 담당하고 국제적 협력담당이며 G8·Europol·Interpol·유럽위원회 등 여러 국제조직들과 전략적 과제에 참여하고 있는 것으로 알려져 있다.[195]

라. 컴퓨터긴급대응센터(CERTA)

CERTA는 프랑스에 있는 여러 CERT들 중의 하나로 1999년 1월 19일 정보사회를 위한 관계위원회(CISI : Comité Interministériel pour la Société de l'Information)의 결정[196]으로 1999년 10월에 발족되었다. 프랑스 행정 분야를 관장하고 있으며

193) Myriam Dunn, Isbelle Wigert, Internation CIIP Handbook 2004-Critical Information Infrastructure Protection, CRN, Center for Security Studies at ETH(Swiss Federal Institute of Technology), 2004. 오일석 외, 앞의 글, 5쪽에서 재인용.

194) Décret n.2000-405 du 15 mai 2000. 하옥현, 국가 사이버안보체계 구축 전략, 고려대학교 박사학위논문, 2004, 159쪽에서 재인용.

195) http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcpj/cyber-criminalite.

196) "프랑스 정부의 컴퓨터 시스템 침입에 대한 활동을 강화하고 조정하기 위하여 프랑스 정부는 컴퓨터 공격을 탐지하고 관련 문제를 해결하기 위한 지원 및 경보 팀의 창설을 결정한다"고 하는 1999년 1

소프트웨어 및 하드웨어 취약성 개선과 같은 기술적 혁신 지속, 프랑스 정부 정보시스템 내에서 발생하는 컴퓨터 침해사고에 대한 해결 및 프랑스 정부가 제공하는 서비스의 신뢰성 형성 및 관리를 그 주요 임무로 하고 있다. 프랑스 정부 CERTA의 두 가지 주요 목적은 다음과 같다. 첫째는 정보시스템보안(SSI : Sécurité des Systèmes d'Information)과 관련된 취약점탐지와 사고의 해결(la détection et la résolution des incidents)을 보장하는 것이고 둘째는 미래의 사고에 대비책(moyens permettant de prévenir et de prémunir contre de futures incidents)을 지원하는 것이다. 위의 두 목표를 달성하기 위하여 기술적 모니터링(veille technologique)과 신뢰체계를 구축(mise en place d'un réseau de confiance)하며 사고해결(résolution d'incident)을 위해 상담·지원하는 것을 임무로 한다.[197]

CERTA는 사이버 조기 경보 및 대응을 위하여 경고(AVIS : Advisories), 경보(ALERTES : Alerts), 상세정보(NOTES D'Information : Information Notes) 및 권고(RECOMMANDATIONS : Recommendations)를 제공하고 있다.[198] CERTA는 해커들이 아이폰, 아이패드, 아이팟 등 애플 제품에서 사용자 정보를 빼내고 통화를 도청할 수 있다고 밝힌 바 있다.[199]http://www.reseau-certa.org/index.php

---

월 19일 CISI(Comite Interministeriel pour la Societe de l'Information) 결정을 말한다. http://www.certa.ssi.gouv.fr.

197) http://www.reseaucerta.org.

198) AVIS는 취약성에 대한 간단한 정보 제공 및 취약성의 결과 및 보호수단 관련 정보(일반적으로 정보보호 관련 기업의 패치)를 제공하는 것이고, ALERTES는 패치가 아직 발표되지 않았거나 긴급한 조치가 필요한 경우 제공되는 경보이며, NOTES D'Information은 사이버보안 관련 주요 문제에 대한 상세한 설명을 제공하는 것이고, RECOMMANDATIONS은 조직 차원의 상세한 보호 수단을 제공하는 것이다(오일석 외, 앞의 글, 6쪽).

199) CERTA는 두 가지 보안 결함을 지적했다. 첫 번째 문제는 해커들이 악성코드를 설치해 놓은 PDF파일을 아이폰 사용자가 열어볼 때 생긴다. 이때 악성코드가 사용자의 아이폰에 심어질 수 있다. 두 번째 결함은 아이폰 부품 중에 데이터 에러가 발생하면 해커들이 아이폰을 더 잘 통제할 수 있게 된다는 것이다. 두 가지 결함이 합쳐지면 해커들은 연락처, e메일, 문서, 카메라, 녹음기 등 모든 정보에 접근할 수 있다고 경고했다. http://www.reseaucerta.org/index.php.

3. 법제도 체계

가. 형법상 정보화범죄 관련 규정

프랑스의 경우 사이버공격 내지 사이버테러 대응과 관련한 별도의 법제는 마련되어 있지 않다. 다만, 사이버공격은 형법에서 정보화범죄(사이버범죄)에 대한 규정으로 이를 규율하고 있는 실정이다.[200]

형법 제323조 이하에서 정보통신시스템 침해행위로 ① 데이터베이스시스템에 무단접속(제323-1조), ② 작동방해(제323-2조), ③ 혼란야기(제323-3조), ④ 시스템내 위장정보 삽입, 제거 및 변조(제323-4조), ⑤ 상기 범죄를 위해 공모 또는 조작에 참여(제323-6조, 제323-7조), ⑥ 사이버범죄 미수 및 법인에 대한 처벌규정 등을 두고 있다.

프랑스 법학계에서는 사이버공격 대응을 위한 강력한 법체계 확립을 주장하는 논의는 거의 찾기 어렵고, 오히려 후술하는 '정보화와 자유에 관한 법률'(Loi ju 6 janvier 1978 relative à l'Informatique et la Liberté)에서 보는 바와 같이 개인의 자유와 프라이버시 보호에 보다 비중을 두고 있는 것으로 이해된다.

나. 프랑스 안전한 디지털경제를 위해 2004년 6월 21일 제정된 법률 제2004-575호

프랑스 안전한 디지털경제를 위해 2004년 6월 21일 제정된 법률 제2004-575호(Loi n 2004-575 du 21 juin 2004 pour la confiance dans l'économie numrique)에서는 기존 형사법의 사이버범죄 관련 개정을 규정하고 있다. 즉, 제2장(사이버범죄 방지)에서 형사소송법 제56조와 제94조 및 제97조에 있어 물건, 문서 등에 "디지털 정보"를 추가하고, 디지털 정보의 압수 등을 신설함을 규정하고 있다. 아울러 프랑스법상 사이버범죄처벌 규정인 형법 제323-1조, 제323-2조, 제323-3조 등의 형량을 상향조정하였다.

200) 정보자동처리시스템에 대한 침해에 대한 형사적 제재에 대한 상세한 내용은, 한국정보보호진흥원, 앞의 보고서, 16-18쪽 참조.

다. 정보화와 자유에 관한 법(개인정보보호법)

개인정보에 관한 관계인의 권리는 1978년에 제정된 정보화와 자유에 관한 법률(Loi ju 6 janvier 1978 relative à l'Informatique et la Liberté)에 의해 일반적으로 인정되었다. 즉, 동법은 사회의 정보화 발전이 개인의 사생활, 기본권 및 인간의 정체성의 보호에 대해 야기하였던 위험에 대응하기 위하여 제정된 법률이다. 동법에 의해 17명의 위원으로 구성된 독립행정기관인 국가정보처리와자유위원회(CNIL : la Commission Nationale de l'Information et des Libertés)를 설립하고 개인정보보호 활동을 해오고 있다.[201] 사이버테러리즘 등의 처벌과 관련하여 독립된 법규는 없으나 현행 형법 규정(§ 421)에 의하여 테러행위를 개인 또는 단체가 공포 또는 위협을 통해 중대한 공공질서 혼란야기 행위로 규정하고 제323조에 규정된 정보통신시스템 침해행위[202]를 테러행위에 포함시키고 있다.

2006년 1월 23일자로 반테러법이 통과됨에 따라 '정보처리와 자유에 관한 법률' 을 수정하게 되었다. 즉, CNIL의 정보활동 중 국가 안보와 관련한 사항에 대한 활동을 제한하게 된 것이다. 1978년 1월 6일 법률은 CNIL의 자문을 거치지 않은 채 2006년 1월 23일 법률('반테러법')에 의해 개정되었다. 개정된 1978년 1월 6일 법률 제30조는 CNIL에 전달되는 답변서가 "국가의 안녕, 국방 및 공안과 관련된 데이터베이스(fichier)에 대한 것일 경우에는 통상 포함하여야 하는 모든 정보를 포함시키지 않을 수 있다"라고 규정하고 있다. 위의 답변서가 최소한 포함하여야 하는 정보처리업무와 정보의 내용은 꽁세이데따가 CNIL의 심의를 거쳐 데크레(décret)로 정하도록 법률은 규정하고 있다. CNIL의 권한을 제한하는 법률의 개정은 1978년 1월 6일 법률을 대폭 수정한 2004년의 개정 이전에도 이루어진 적이 있다. 이러한 개정은 1979년 12월 28일 데크레에 의해 구체화되었으나, 이러한 규정들은 위 법률에 대한 개정을 내용으로 하는 법률안이 제출됨으로 인해 시행되지는 않았었다. 의회는 이 법률안에서 "망각"(태만, 불이행 : 'OUBLI')의 문제를 제기하면서 국가의 기본적 이익에 대한 방어를 위해 필수적인 조치들을 무력화하지 않기 위해 이러한 '생략'에

201) CNIL은 정보처리로 인한 기본권 침해의 위험에 대응하여 사생활과 기본권을 보호하는 것을 주된 임무로 한다. CNIL의 임무에 관한 상세는 한국정보보호진흥원, 앞의 보고서, 29-30쪽 참조.

202) 한국정보보호진흥원, 앞의 보고서, 18쪽.

대한 규정을 수정하는 것이 필요하다고 보았다. 그러나 CNIL의 "국방 비밀"에 이르는 정보도 다루어야 하는 위원회 위원들과 인력들은 이 법률에 의해 업무상 비밀에 구속된다는 점을 주목할 필요가 있다. 뿐만 아니라 위원회에 송부되는 정보에서 국가의 기본적 이익이 문제될 때는 공중에 공개되지 않는다.[203]

라. 전자통신법

공중전자통신부문의 규제는 전자통신담당장관 및 우편통신규제청에 의하여 국가의 이름으로 행해진다(전자통신법 제32-1조 제1항). 망의 호환성 및 안전성 유지, 망 표준화, 그 밖의 위해방지를 위한 각종의 규제 등 전자통신망에 대한 기술규제는 우편통신규제청이 행한다.

온라인상의 공동통신역무에 대한 접근을 제공하는 활동을 하는 자 등 전자통신사업자는 모든 트래픽관련 정보를 삭제하거나 익명화할 수 있으며, 이 경우 전자통신법 제34-1조의 규정에 따른다. 형사범죄에 대한 수사, 확인 및 소추를 위한 필요가 있는 경우 사법수사기관이 행하는 것을 조건으로 일정 범위의 기술적 데이터를 삭제하거나 익명화하는 작업은 연기될 수 있으며, 이 경우 그 기간은 최대 1년을 넘지 못하도록 하였다.

제5절 일본의 사이버공격 대응체계

1. 개 관

일본은 이미 과학·기술 선진국으로서 첨단 정보통신기술 능력을 갖추었지만 사이버공격 대비능력은 막강한 경제력과 첨단기술력에 비추어 다소 뒤떨어져 있는 것으로 알려지고 있다. 이제 일본은 사이버공격에 대응하기 위한 다양한 대책을 마련해 나가고 있다. 일본에서는 아직까지 심각한 사이버테러리즘은 발생하지 않고 있으나,

203) La CNIL s'est prononcée sur les articles de l'avant-projet de loi relatif à la lutte contre le terrorisme concernant : http://www.cnil.fr.

최근 들어 해킹 사례와 컴퓨터범죄가 급증하고 있다. 이에 대한 대책과 사이버테러리즘을 미연에 방지하기 위해 통상산업성 주관으로 국민생활과 직결된 전력, 석유산업 등의 컴퓨터 네트워크 현황을 분석하고 사이버테러리즘 가이드라인을 작성하는 등 적극적인 대응에 나서기 시작했다. 2001년 1월, 일본 정부의 웹사이트들과 민간 웹사이트들이 외부의 무차별 공격에 순식간에 다운당할 정도로 일본의 사이버공격에 대한 취약성은 잘 알려져 있다. 또한 사이버공간 상에서 일본의 난징대학살을 비난하는 중국인들의 시위의 일환으로 일본정부의 웹사이트가 무차별 공격을 받자 일본정부는 방위청을 선두로 본격적으로 시작하였다.

일본은 정부기관인 관방성 주도하에 사회기반 및 생산설비에 대한 사이버테러리즘대책을 수립 시행하였다. 1997년 8월, 정부 주도하에 정보보안대책실을 설치하고 국가적 정보보안대책을 추진하여 대규모 공장설비 네트워크의 보안대책위원회를 구성하여 네트워크 보호기술 및 운영체제의 표준화를 추구하고 보안수준을 향상시키기 위해 필요한 대책을 제안하였다.

1999년 9월 관방성·경찰청·방위청·금융감독청 등 13개 기관의 국장급으로 정보보안관계부처 회의체인 정보보안관련성청국장회의를 구성하고, 2003년을 목표로 해커대책등기반정비행동계획을 수립 발표하였다.[204]

2000년 12월 '중요 인프라의 사이버 테러 대책에 관한 특별 행동 계획'(重要インフラのサイバーテロ對策に係る特別行動計劃)을 발표하고 정부의 내각관방을 중심으로 관·민의 긴밀한 협력 하에 이 계획을 실시하기로 하였으며 민간의 주요 인프라 사업자 등도 이 계획을 토대로 자율적인 대책을 강구하도록 하였다.

미국의 9·11 사고 이후에는 사이버테러리즘 대책 강화 등을 중점 추진사항으로 하여 사이버테러 특별행동계획과 그 후속조치를 마련하는 등 진일보한 대책을 서둘러, 2002년 4월 e-Government 사이버공격에 대한 정보공유와 사이버테러리즘에의 긴급대응을 임무로 하는 NIRT(National Incident Response Team)를 설치하였고, 경

204) 2000.1. 발표한 주요 내용은 ① 보안평가제도 도입, ② 정보수집 및 긴급대응을 위해 정부 부처간 연락체계 구성, ③ 2000.4. 금융·정보통신 등 중요분야 선정, ④ '민관 정보교환을 위한 연락회의' 설치, ⑤ 2000.12. '사이버테러에 관한 특별행동계획' 마련 및 각 부처의 종합적이고 체계적인 정보보안대책이 추진 가능하도록 '정보보안정책에 관한 가이드라인' 제정, ⑥ 2002년까지 각 성청별 세부가이드라인을 제정하는 것이다.

찰청 산하에 전문 기술가들로 サイバーフオース(Cyber Force)를 구성하였다. 2003년 10월 국가정보보안종합전략을 수립·발표하고 내각관방의 사이버테러리즘 대응 조직과 역할을 강화하였으며 민·관 공동 감시체제인 정보방위센터 설치를 추진하고 있다.

2006년 2월 내각관방에서는 국가 전반의 정보보호 요구에 대응하기 위해 '제1차 정보보호 기본계획'을 수립하여 추진하였다. 정부·지방공공단체, 주요 인프라, 민간(개인 및 기업)을 대상으로 '정보보호 기본계획'의 주요 대책을 2006년에서 2008년까지 3년간 추진하였으며, 정부·지방공공단체, 주요 기반, 기업, 개인 영역으로 구분하여 'Secure Japan 200X'를 수립하고 실행성과를 평가하고 있다. 또한, 총무성에서는 u-Japan 정책을 통해 정보화 역기능에 관한 100대 과제를 정리한 'ICT 안심·안전 21 전략'을 추진 중에 있다. 경제산업성에서는 정보보호 위협에 대한 국제적 대응, 국제경쟁력 강화 기반 마련, 국내외 다양화된 환경변화 대응을 위한 글로벌 정보보호전략을 추진 중에 있는 바, 이처럼 일본은 정보통신강국답게 국가기관협의체를 구성하여 사이버테러리즘에 대치하고 미래의 사이버전(Cyber-Warface)에 대비하기 위하여 체계적인 정보보안대책을 마련하고 있는 것으로 평가된다. 최근 2009년 2월에는 '2차 정보보호 기본계획'을 마련하였다. 제2차 계획은 2009년도부터 2011년도까지 3년간을 대상으로 일본 전체 정보보안 문제에 대한 대책을 추진하기 위한 계획이며, '고품질, 고신뢰성, 안전안심'을 추구하는 일본모델을 구현하고 "새로운 민관 협력 모델"의 구축을 목표로 함을 명시하였다.

최근 2010년 7월 일본정부 '정보 보안 정책 회의'는 각 부 부처가 실시하는 보안 대책을 정리한 계획 '정보 시큐리티 2010'(情報セキュリティ2010)을 결정했다. '정보 시큐리티 2010'은 2010년에서 2013년도에 이르는 4개년 계획으로 수립되었다. '국민을 지키기 정보 보안 전략'에서는 2014 년까지 정보 보안에 대한 국민의 불안을 해소, 2020 년까지 세계 최첨단의 '정보 보안 선진국'을 실현하는 것을 목표로 각 기관이 2010~2011년도에 실시하는 196개의 시책을 제시하고 있다. '정보 시큐리티 2010' 시책의 내역은 대규모 사이버 공격에 대한 대처, 정보 보안 정책의 강화 시책, 대규모 사이버 공격에 대한 대처 시책으로는 적절한 초동 대처를 위해 내각 관방에 태세를 정비하고 훈련을 실시하거나, 방위성에 사이버 기획 조정관 (가칭)을 배치하는 것이 평소의 정보 수집 공유 체제 구축 강화 등이 있다.[205] 구체적인 시책으로 각 행정 기관의 최고 정보 보안 책임자(CISO)에 의한 '정보 보안 대책 추진회

의'를 설치하거나 범정부 정보 수집 분석 시스템의 충실 강화, 핵심 인프라 기반 강화, 클라우드화에 대응하는 정보 보안 확보 정책의 검토, (가칭) 정보 보안 안심 창구 검토, 사이버 범죄에 적절히 대처하는 법 정비의 추진 등을 들 수 있다. 또한 2009 년도의 년도 계획 '보안 Japan 2009'에 포함된 시책의 실시 상황에 대해서는 212 시책 중 176 시책(83.0%)은 예정대로 추진되고 나머지 시책에 대해서도 25 시책(11.8%)은 수개월 이내에 완료 11 시책(5.2%)은 향후 활동을 통해 달성 전망으로 알려져 있다.

2. 조직체계

일본의 사이버테러리즘 대응 조직은 내각관방 정보시큐리티대책추진실(情報セキュリティ對策推進室), 내각 고도정보통신네트워크사회추진 전략본부(高度情報通信ネットワク社會推進戰略本部), 경찰청, 총무성, 경제산업성 및 일본컴퓨터긴급대응센터(JPCERT/CC) 등 민간기관으로 구성되어 있다. 일본은 전체적으로 내각관방을 중심으로 경찰청·방위청·총무성·경제산업성이 각각 정보보호정책을 추진하는 시스템을 갖추고 내각관방이 각 부처를 총괄·조정하는 역할을 담당하며 각 부처와의 연대협력은 물론 '긴급대응지원팀'(NIRT)으로 하여금 전자정부의 정보보호와 주요 인프라 사이버테러 대책을 마련하고 정보보호 정책보좌관을 민간전문가로 임명하고 있다. 각 부처별로는 일본 경찰청은 2001년 4월부터 Cyber Force를 창설, 하이테크범죄 예방에 주력하고 있고, 방위청은 2003년 10월 '방위물자 조달에 관한 정보보호기본방침'을 수립, 조달업무에 관한 정보시스템과 DB 등의 보안대책을 추진하고 있으며, 총무성은 2002년 7월 인터넷사업자(ISP)를 중심으로 "인터넷침해사고 정보공유분석센터"를 설립, 인터넷 해킹 등에 대비하고 있다.[206]

205) 정보 보안 정책 강화 시책은 국민을 지키는 정보 보안 기반의 강화 (102 시책), 국가 이용자 보호 강화 (29 시책), 국제 협력 강화 (15 시책), 기술 전략의 추진(24 시책), 정보 보안에 대한 제도 정비(7 시책) 등이다. http://www.nisc.go.jp/conference/seisaku/index.html#seisaku24.

206) 한국정보보호진흥원, 앞의 보고서, 204-212쪽.

가. 내각관방 정보시큐리티대책추진실

정보시큐리티대책추진실은 인터넷의 급속한 이용확대 등 국민생활의 IT발전에 따른 부정엑세스(부정アクセス), 컴퓨터 웜바이러스 확산 등에 대처하기 위해 2000.2월 내각관방장관 산하에 설치되었다. 주요 역할은 각 정부부처와의 협력을 도모하고 민관 전문가로 구성된 비상근팀의 조언을 받아 전자정부의 정보보호 확보 및 중요인프라 사이버테러 대책 등 민·관의 정보보호확보를 위한 정책추진을 총괄·전담하고 있다. 또한, 내각총리대신 산하 내각 '고도정보통신네트워크사회추진 전략본부'(IT전략본부)에 설치된 정보시큐리티대책추진회의와 민간전문가로 구성된 정보시큐리티전문조사회의 사무국을 담당하면서 각 부처 업무조정을 하고 있다.

'전자정부의 정보시큐리티확보를 위한 액션플랜'(2003. 10. 정보시큐리티대책추진회의 결정) 을 근거로 전자정부나 민간 중요인프라 사업자 등의 정보시스템에 대한 사이버테러 등 국민생활에 중대한 영향을 줄 우려가 있는 정보보호에 관련사항에 대해 각 성(省)·청(廳)의 정보보호 대책 입안시 이에 대한 필요한 조사·조언 등을 실시하기 위해 2002년 4월 긴급대응지원팀(NIRT, National Incident Response Team)을 설치하였다. 인력구성은 민관 컴퓨터 보안전문가 17명으로 구성되며 총괄·지도는 독립행정법인 '통신총합연구소'의 '비상시(非常時) 통신그룹장'이 담당하고 있다. 그 주요 활동 상황은 사이버공격 등으로 전자정부·중요인프라사업자 등의 정보시스템에 관한 장애가 발생하거나 장애 발생이 예상되어 정부차원의 위기관리대응이 필요한 정보시큐리티 관련 사안에 대한 대응활동을 하고 있다.

정보보호시책의 시행에 대하여 중장기적 관점에서 조언을 하고 중요 인프라 방호를 위한 사이버테러 대책을 강구하기 위해 정보시큐리티대책추진실 산하에 전문가조사팀을 설치하였다. 주요 추진실적으로는 2000년 12월 '중요인프라의 사이버테러대책에 관한 특별행동계획'(重要インフラのサイバーテロ對策に係る特別行動計劃)을 발표, 사이버테러 등 정보통신네트워크, 정보시스템을 이용한, 국민생활이나 사회경제활동에 중대한 영향을 끼칠 가능성이 있는 어떠한 공격으로부터도 중요인프라를 방호하기 위한 정책을 심의·수립하였다.

정보통신기술의 활용에 따라 세계 규모로 진행중인 급격하고도 대폭적인 사회경제구조의 변화에 신속 정확하게 대응할 필요성을 고려, 고도정보통신네트워크사회의

형성에 관한 시책을 신속하고도 중점적으로 추진하기 위해 2001년 1월 '고도정보통신네트워크사회형성기본법'에 근거하여 내각에 '고도정보통신네트워크사회추진전략본부'(高度情報通信ネットワク社會推進戰略本部 : 이른바 "IT전략본부")를 설립하였다.[207] IT 전략본부는 고도정보통신네트워크사회 형성에 관한 중점계획을 작성, 그 시행을 추진하며, 그 외 고도정보통신네트워크사회의 형성에 관한 중요시책을 심의하고 이를 위해 사안별 민·관전문가를 소집, '전문조사회'를 운영한다.

'시큐리티대책추진회의'는 내각관방 부장관을 의장, 내각위기관리감을 부의장으로 하여 정부부처 국장급으로 구성되며, 정보보호 대책추진을 전담하고 있으며, '정보시큐리티전문조사회'는 민간전문가들로 구성되어 민관분야의 정보보호 대책 추진에 관한 사항의 조사, 검토를 전담하고 있다. '각부처 정보화총괄책임자(CIO) 연락회의'는 2003년 7월 '전자정부구축계획(안)'과 관련 공공 앙케이트 조사를 실시한 바 있으며, 'IT 전략의 향후 바람직한 방향에 관한 전문조사회'를 수시 운영하고 '평가전문조사회'는 "e-Japan전략Ⅱ"에 관한 정부의 추진상황 평가 등을 수행한다.

나. 경찰청 사이버포스센터(Cyber Force Center)

일본 경찰청에서는 컴퓨터 기술 및 전기기술을 악용하는 하이테크범죄가 급증함에 따라 이에 적절히 대처하기 위해 1998년 6월 하이테크범죄대책 중점추진 프로그램을 공표했다. 1999년 4월 경찰청에 기술대책과를 신설하고 1개월 후 동경 경시청에 하이테크범죄대책센터를 개설하였다. 선진국에 비해 뒤늦은 1999년 8월, '부정액세스금지에 관한 법률'(不正アクセス行爲の禁止等に關する法律)을 제정하여 타인의 ID, 패스워드를 도용하여 컴퓨터에 접속하는 행위 등을 2000년 2월부터 단속하고 있으나 최고형이 징역 1년 이하로 형량이 가벼워 억제효과는 크지 않았다.[208] 2001년 4월 악질적인 사이버테러리즘에 대응하기 위해 약 60명의 기술자로 사이버포스(サイバ-フオ-ス)라는 특별팀을 구성하여 동경도내의 민간빌딩에 있는 사이버포스센터 등 전국 57개소의 거점으로 경찰네트워크에 대한 해킹행위를 24시간체제를 감시하고

207) http://www.kantei.go.jp/jp/singi/it2/index.html.

208) 正アクセス行為の禁止等に関する法律平成11年法律第128号) : http://www.kantei.go.jp/jp/singi/it2/hourei.

있다. 하이테크범죄·사이버테러를 예방하고 피해확대를 방지하기 위해 2001년 경찰청 정보통신국 사이버테러대책기술실에 설치되었으며 범죄수사 등의 지원을 위해 동경에 센터를 두고 오사카·나고야·히로시마·후쿠오카·센다이·삿포로·사이타마·타카마츠 등 전국 8개 관할 경찰국내에도 설치되었다. 전국 경찰기관에 설치되어 있는 인터넷 접속점의 IDS를 24시간 감시하여 관련정보를 수집·분석하는 관제장비인 '검지(檢知) 네트워크시스템'을 운영하여 사이버테러 조기탐지 및 긴급대응업무와 함께 관련분야 연구개발과 전문인력에 대한 교육훈련을 실시하고 있다. 또한, 긴급출동차량에는 현장활동에 필요한 각종 분석컴퓨터, 백업장치, 과학수사장비, 자가발전기 등을 구비하여 활동하고 있다.

다. 일본의 사이버수사조직

일본은 하이테크범죄·사이버테러를 예방하고 피해확대를 방지하기 위해 2001년 정보통신국 사이버테러대책기술실을 설치하였고, 범죄수사 등의 지원을 위해 동경에 센터를 두고 오사카·나고야·히로시마·휴쿠오카·센타이·삿포로·사이타마·타카마츠 등 전국 8개 관할 경찰국 내에도 설치하였다.[209] 경찰청은 기획·조정·지원만 담당하고 실제 사이버테러 전담수사는 동경경시청 '하이테크범죄종합대책센터'('99년 설립)에서 처리하고 있으며, 일반적인 사이버범죄에 대한 직접수사는 47개 도도부현(지방청)에서 담당하고 있다. 정보통신국 첨단범죄기술과에는 디지털증거분석센터, 사이버포스센터가 있다. 특히, 사이버포스센터는 1999년 하이테크 범죄대책에 관하여 도도부현 경찰을 기술적으로 리드하는 국가적 센터로 육성하기 위하여 설치되었다.[210]

일본은 아시아 지역에서 유일한 G8 회원국으로서 1998년 창설한 'G8 High-Tech Crime Sub Group'에 참여하여 국제사회의 사이버범죄 근절을 위한 정책결정에 주도적으로 참여하고 있고, 2001년부터 현재까지 인터폴 사무총국에 사이버수사업무를 담당하는 재정 및 하이테크분과(FHT)에 경찰관을 파견하고 있다. 아시아 14개국이 참여하는 '사이버범죄 기술정보네트워크'(CTINS)를 구축하였고, 참여국을 매년 초청하여 국제회의를 주관하는 등 아시아 지역 국제협력을 위해 많은 노력을 경

209) 이재은, 앞의 글, 82쪽.

210) 김재광/김정임, "일본의 사이버위기 관련 법제의 현황과 전망", 법학논총 제33권 제1호, 55-56쪽.

주하고 있다. 또한, 우리나라가 2002년에 '인터폴 아·태지역 사이버수사 교관양성과정'(TTI)을 개설하자 일본은 2007년부터 '인터폴 아·태지역 디지털 포렌식 교관양성과정'(TTF)을 개설하는 등 한국과 일본은 국제사회에서 사이버범죄 대응에 관한 주도권을 확보하기 위해 보이지 않는 경쟁을 하고 있다.

3. 법제도 체계

가. 전기통신사업법

전기통신사업법(電気通信事業法)은 1984년 12월 법률 제86호로 제정되어 최근 2006년 6월 법률 제50호로 개정되었는 바, 이 법은 전기통신사업의 공공성에 비추어 적정하고 합리적인 운영을 꾀함과 동시에 그 공정한 경쟁을 촉진하고 전기통신서비스의 원활한 제공을 확보하여 이용자의 이익을 보호하는 한편, 전기통신의 건전한 발달 및 국민편의를 도모하여 공공복리를 증진하는 것을 목적으로 하고 있다.

나. 고도 정보통신 네트워크 사회 형성 기본법

고도 정보통신 네트워크 사회 형성 기본법(高度情報通信ネットワーク社会の形成に関する基本方針を定めた法律)은 일명 'IT기본법'이라고 하며 이 법은 사이버안전 측면에서 최근 문제가 되고 있는 정보통신 네트워크 안전성 확보를 위하여 국민이 안심하고 네트워크를 이용하기 위한 네트워크 안전성 및 신뢰성 확보 등에 관한 조치가 선행되어야 함을 규정하고 있다(제21조). '고도 정보통신네트워크 사회 추진전략 본부'로 하여금 정보통신 네트워크의 안전성 및 신뢰성 확보 시책에 대한 중점 계획을 작성토록 하는 등 우리의 국가정보화기본법과 유사한 지위를 지닌다.

다. 테러방지법제

9·11테러 이후 일본에서는 2개의 국제적인 조약이 시행되었으며, 이에 대해 구체적인 입법을 한 바 있다. 그 중 하나는 '폭탄테러방지조약'의 이행입법인 '테러리

스트에 의한 폭탄사용의 방지에 관한 국제조약의 체결에 따른 관계법령의 정비에 관한 법률'이다. 이 법이 제정됨에 따라 '폭발물단속벌칙', '방사선동위원소에 의한 방사선장애 방지에 관한 법률' 등 관련 규정에 국외범에 대한 처벌규정을 신설하게 되었다. 둘째로 일본에서는 '생물병기금지법'을 개정하여 생물병기 또는 독소병기를 사용하여 생물체, 독소로 국민을 위협하는 행위나 독극물을 발산시키는 행위 이외에도 이러한 독극물을 부주의하게 발산시켜 생명 등에 위험을 발생하게 한 행위에도 가벌성을 인정하고 있다. 셋째, '화학병기금지법'을 개정하여 화학병기를 사용하여 독성물질 등을 반산시키는 행위와 아울러 이것을 부주의하게 발산시켜 생명 등에 위험을 발생하는 경우에도 처벌하도록 규정하고 있다. 넷째, '핵원료물질·핵연료물질·원자로 규제에 관한 법률' 등을 개정하여 핵원료물질과 핵연료물질에 오염된 물질을 함부로 취급함으로써 방사선을 방사시켜 생명·신체·재산에 위협을 발생시킨 행위 역시 처벌하도록 하고 있다. 그 밖에도 '테러자금공여방지조약'의 이행입법으로 '금융기관본인확인법'과 '테러자금공여처벌법'을 제정함과 아울러 '외환 및 외국무역법'을 개정함으로써 테러단체에 자금이 전달되는 것을 원천적으로 차단하고 있다. 즉 이 법들에 의하여 공중이나 국가를 대상으로 한 테러를 위한 자금의 제공·수집을 처벌하고 제공자금을 몰수할 수 있도록 하고 있다.[211]

9·11 테러 이전에는 일본의 테러범죄에 관한 법적 정의 규정은 없었다. 다만 실무상으로 "테러리즘이란 널리 공포 또는 불안을 느끼게 함으로써 그 목적을 달성하기 위하여 행하는 극좌 기타의 주장에 근거한 폭력주의적 파괴활동"이라고 정의하고 있었다(경찰청조직령 제17조의 2). 또한 그러한 테러리즘이 외국인 또는 외국에 활동의 본거지가 있는 일본인에 의해서 행해지는 경우를 국제테러리즘이라고 한다. 따라서 중핵파 등 국내의 극좌폭력집단이 외국에서 테러사건을 감행하여도 여기서 말하는 국제테러리즘의 범주에 속하지 않았다고 한다. 그러나 9·11 테러 이후 테러특별조치법을 제정하여 자위대의 활동 범위를 타국 영토까지 확대하고, 자위대의 전투시 해외 파견을 처음으로 허용하는 등 적극적인 대응을 하고 있으며, 정부차원의 테러방지 대책이 추진되는 등 적극적인 움직임을 보이고 있다. 즉 2001년 11월 2일

211) 이상 일본의 대테러관련 법제에 관해서는 조성용, "일본의 테러관련 법제연구", 대구법학 제6호, 2003, 22-23쪽 참조.

미군 주도의 테러 보복공격을 자위대가 후방 지원하기 위한 '테러대책특별조치법'을 제정하고, 일본 내 미군 시설 등을 자위대가 경비할 수 있도록 한 '자위대법개정안'과 의심 선박에 대한 선체 사격을 허용하는 '해상 보안청법 개정안'도 통과시켰다. 이 법의 제정과 관련하여 해외에 자위대를 파견하는 행위가 전쟁포기를 선언하고 있는 헌법의 규정(일본 헌법 제9조)에 위배되는 것이 아닌가 하는 점에 대하여 많은 논쟁이 있었다.

테러특별조치법은 2년간의 한시법으로 자위대의 활동 범위를 타국 영토까지 확대하고, 자위대의 전투 시 해외 파견을 처음으로 허용한 것이 특징이다. 또한 자위대법과 해상보안청법을 개정하면서 주로 경찰관직무집행법의 범위 내에서 사용되던 자위대원과 해상보안청 직원의 무기사용 범위를 완화하였으며(특별조치법 제12조), 자위대의 정보수집 권한 강화 및 주요시설 경호를 위한 출동권한 부여 등을 통하여 테러행위에 대한 신속하고 적극적인 대응이 가능하도록 제도 변화를 두었다.

제6절 비교법적 고찰의 시사점

앞서 미국, 영국, 독일, 일본, 프랑스 등 다양한 나라의 사이버공격 대응체계 현황을 살펴보았다. 그 중에서 사이버공격을 국가적으로 중대한 위협요인으로 인식하고 가장 활발하게 대응체계를 구축하고 있는 나라로 꼽히는 미국의 사례는 우리에게 주는 시사하는 바가 크다. 즉, '전자정부법'의 일부인 '연방정보보안관리법'에 따라 각 연방기관은 예산절차의 일환으로서 관리예산처에 정보보호 대책의 상황을 보고하도록 하여 정보보호 정책과 예산을 연계시킨 형태로 분석된다. 관리예산처(OMB)는 직접 정보보호조치를 집행하지는 않지만 '연방정보보안관리법'에 근거하여 전자정부에서 각 연방기관의 정보보호조치를 감독하고 이를 예산집행 등에 반영함으로써 공공부문 정보보안 일반에 대한 실질적인 평가 역할을 수행함으로써 사이버보안 확립에 기여한다. 한편 국토안보부는 '국토안보법'에 근거하여 공공과 민간부문 전체에 걸쳐, 그리고 물리적 위협이든 사이버공격이든 그 형태를 막론하고 보호조치를 총괄적으로 집행한다. 국토안보부는 연방정부의 정보보호 정책을 실시할 책임을 지고 있으며, 이것에 대한 실례로, 2002년에 발표된 '국토안보 국가전략'에서 국토안보부의 주

요기반시설 보호를 총괄하는 역할을 명시한 점, 2003년에 제시된 '사이버공간 보호를 위한 국가전략'에서는 연방정부의 각 기관이 완수해야 할 정보보호의 포괄적인 틀을 제시한 점, 2004년부터 '국가 사고 관리 시스템'을 통한 사고대응단일 체계 수립 및 표준화된 관리 계획을 제시한 점 등을 언급할 수 있다. 또한 국토안보부는 '국가 대응 프레임워크', '국가기반보호계획', '국가 사이버공간 대응 시스템', '사이버 위험 관리 프로그램' 등의 전략과 프로그램의 진행으로 사이버 공격을 예방하고 대응하기 위한 실질적인 조치들을 수행하고 있으며 최근의 경우 "국가 사이버보안 종합전략"에 의해 미국 정부 전산망을 적극적으로 감시하는 임무를 맡아 사이버침해사고에 대한 사후 대응측면보다는 '사전' 대응체계를 수립하는데 중요한 역할을 담당하고 있음을 알 수 있다. 아래에서는 미국의 사례가 우리에게 주는 시사점을 대응조직 및 전략측면과 법체계 측면으로 나누어 살펴본다.

1. 대응 조직 및 전략 측면

미국의 사이버안보전략이 갖는 가장 큰 의의는 기존에 책임과 권한이 여러 부처에 분산됨으로 인해 발생하는 정책의 혼선을 지양하고 모든 역량을 한 곳에 집중하여 국토안보부(DHS)의 창설로 대표되는 보다 효율적인 대응체계를 마련한 것이다. 또한 국방부문이 평시에 민·관 부문과 밀접하게 관계하고 있어 유사시 적극 개입할 수 있는 협력체계를 유지하고 있다. 정부기관과 민간에서 CERT와 ISAC을 운영하고 국방부는 CERT를 운영하여 민·관·군이 상호 공조하는 CERT와 ISAC 위주로 정보보안 정책을 추진하고 있다. 그러나 국가의 주요기반시설을 사이버공격으로부터 방어하고자 하는 다양한 노력은 국토안보부의 리더십 부재, 민간부문의 참여를 유도할 수 있는 구체적인 유인책의 결여, 추진 프로그램의 운용을 위한 재원의 부족, 정부기관 간의 적절한 역할 분담 등 해결되어야 할 많은 과제도 남아 있는 것으로 지적된다.[212] 미국의 정보우위에 대한 노력은 정보우위의 유지 및 강화 전략(Information Hegemony Mainte-nance Strategy)으로 요약될 수 있다. 현재 미국의

212) 하옥현, 앞의 글, 145쪽.

군사적 압도에도 불구하고 미국에 도전할 수 있는 다른 국가들의 존재를 부인하기 어려워, 미국이 전통적인 병력유지에 많은 고정비용과 투자를 해야 하지만 새로운 도전국들은 정보기술력 향상에 집중투자를 하여 단기간 내에 미국을 따라 잡을 수 있다는데 미국의 고민이 있다. 아울러 이러한 미국의 전략에 중국은 비대칭위협전략(Asymmetreic Threat Strategy)으로 나가려는 경향을 보이고 있는 상황에서 이러한 강대국들의 사이버안보강화전략이 다른 국가들에게 어떤 영향을 미칠지 면밀히 검토하고 대응할 필요가 있다. 미국의 이러한 일련의 노력은 우리에게 많은 시사점을 제공해주고 있다.

앞서 살펴본 해외 체계를 통해 알 수 있듯이, 미국, 독일, 프랑스 등은 사이버 전담 조직이 존재하고 있고, 일본과 영국의 경우에는 우리나라와 같이 부문별로 기관이 존재하고는 있으나 이를 조정하기 위한 센터 내지 위원회가 존재하고 있다는 것을 알 수 있다. 그러나 현재 우리나라의 사이버 위기 대응기관으로는 국가정보원의 국가사이버안전센터, 국방부의 사이버사령부, 방송통신위원회(산하 한국정보보호진흥원)의 인터넷침해사고대응지원센터를 주축으로 대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 국가보안기술연구소, 정보공유분석센터(ISAC)등으로 다양하게 존재하고 있으나 이들 간의 협력체계를 뒷받침할 법체계가 미비하고 사이버침해 발생 시 신속하고 강력하게 이를 대응할 체계가 미흡한 실정으로 개선이 필요함을 알 수 있다. 한편, 미국, 독일 및 영국, 일본 등의 경우 이미 국가사이버위기 관리 체계에 대한 정립을 끝낸 수준으로 인력 및 기술개발 보완 등의 활용 및 안정화 단계에 진입했다고 볼 수 있다. 그러나 IT 선진국이라고 불리우는 우리나라의 경우 IT산업 발전 속도는 이들 선진국을 능가하고 있으나, 국가사이버위기 관리 체계는 이제 갓 체계 정립 단계에 있다고 볼 수 있다. 따라서 향후 국가사이버위기 관리 체계 강화 방안 마련이 요구된다. 또한 사이버침해에 효과적으로 대응하기 위한 연구개발도 소홀할 수 없다. 미국은 '2001. 9·11 동시다발테러' 이후 사이버보안을 연방정부 R&D 분야에서 최우선 프로그램 중 하나로 선정하고 연구개발 정책을 강화하고 있다.[213] 즉, 사이버보안연구개발법(2002년)을 제정하였고, 이어서 국가 사이버공간 방어전략(2003년)·사이버보안우선순위의 위기(2005), 연방 사이버보안 및 정보보증

213) 이재은 외, 국가사이버위기 관리 체계 강화 방안에 관한 연구, 국가보안기술연구소, 2008, 97-99쪽.

연구개발 계획(2006년) 등을 발표하였음은 우리에게 시사하는 바가 크다 할 것이다. 연방정부의 사이버보안 R&D에의 참여는 연구개발 감독 및 조정, 비공식 정책조정지원, 핵심 연구수행 및 기금출연의 형태로 이루어지고 있다. 우리나라도 관련 법제의 정비와 더불어 조직구성 및 예산 확보 등 국가 사이버보안 R&D 정책을 강화할 필요가 있다.

사이버침해 대응을 위한 특징 중 하나는 국제 협력 및 공조의 강화 필요성이라 할 것이다. 기존 테러리즘이 교통과 정보통신의 발전 등으로 국제화되어 가는 추세에서 테러리즘을 사전에 차단하기 위해서는 무엇보다 국제적인 정보의 공유가 필요하다. 우리나라는 2004년도에 국가사이버안전센터와 미국, 영국, 독일, 프랑스 등 주요국가의 사이버안전 담당기관과 사이버 위협정보를 공유하고 향후 침해사고 발생시 공동 대응키로 하는 등 국제적인 협력관계를 강화하고 있으나, 국내·국제를 망라한 입체적 대테러 네트워크를 구축해야 한다. 21세기 들어 과학·교통·통신의 발달과 함께 세계화·정보화 물결이 맞물리면서 국제테러조직들도 전 세계적인 테러 네트워크를 구축하고 점조직화하고 있다. 그러므로 이에 대응하기 위해서는 국내·국제적인 대테러 네트워크 구축이 불가결하다. 특히, 사이버테러의 경우는 점점 더 국제적인 공조와 네트워크구축이 요구되고 있으므로 이에 대한 적절한 대응과 대책이 강구되어야 할 것이다.

한편 미국의 경우 최근 IT 예산은 상대적 증가세가 둔화되었지만 꾸준히 증가하는 추세이며, IT예산 대비 정보보호 예산은 지속적으로 증가하였고, 2006년부터 2009년까지 최근 4년간 평균 9%로 나타나고 있다. 그러나 우리의 정보화 예산은 2009년 7·7 DDoS 침해사고 이후 일시적으로 약 5% 증가하였으나, 2011년 예산감액이 예상되고 있는 실정이다. 즉, 7·7 DDoS 침해사고 이후 8.2%까지 상승한 정보보호 예산비율은 2011년 다시 6.2%로 감소할 것으로 예상되어 정보보호 선진국인 미국에 비해 미흡한 상황이다. 우리나라의 정보보호 관련 예산은 지난 4년(2007년~2010년) 평균 약 5.25% 수준에 머무르고 있는 실정이다.[214] 미국의 경우 침해사고 발생 유무에 관계없이 침해사고 발생에 대비하여 꾸준하게 정보보호에 예산을 투자하고 있는 반면 우리나라의 경우는 사고가 발생한 후에야 그것도 일회성으로 예산

214) 국회 입법조사처, 국가정보보호 정책현안과 개선방안, 2010. 10, 25쪽.

투자가 이루어지고 있으며, 그나마도 사고에 대한 관심이 잦아든 이후에는 다시 이전 수준으로 감액되고 있는 상황이다. 실효적이고 강력한 사이버공격 대응체계를 구축하기 위해서는 향후 보다 장기적인 예산계획에 따른 지속적인 정보보호 예산 투자가 이루어져야 할 것임은 물론이다.

2. 법제도 측면

사이버대응 법제와 관련하여 9·11 테러 이후 UN 안보리는 결의안 1368호와 1373호를 통해 회원국들에게 강력한 대테러법을 제정할 것을 촉구하였다. 그리고 이러한 UN의 요구에 부응하여 대부분의 국가가 테러에 대비하기 위한 각종 제도를 정비하고 있다. 즉, 미국은 애국법과 국토안보부법을 제정·시행 중에 있고, 영국은 기존의 반테러법을 대폭 강화하였다. 독일 또한 기존의 보안관련 법률을 새로운 테러 위협상황에 적응토록 개정하는 것을 목적으로 하는 테러대책법을 제정하였으며, 일본과 프랑스도 테러대응을 위한 특별법을 제정하여 이에 대응하고 있다. 우리나라도 2002년 9월까지 대테러법을 제정하겠다는 보고서를 UN에 제출하였고 2001년 11월 정부안을 마련하여 국회에 제출하였으나 논란만 거듭하다 2004년 5월 국회회기 종료와 함께 법안이 폐기되고 말았다. 그리고 논란이 되었던 시민단체의 인권보호 조항 등이 많이 수정 보완되어 17대 국회에서도 3건의 테러방지법안이 재발의 되었으나, 결국 결실을 보지 못하였다.[215] 그러나 국가의 대테러활동의 법적인 체계를 구축하고 대테러 활동의 투명성 보장은 물론 국제사회와의 협력체제의 강화가 필요한 시점에서 테러방지법의 필요성은 인정된다 할 것이고, 특히 사이버테러에 효율적으로 대응하기 위한 사이버 테러 관련규정의 정비 혹은 별개의 법률로서의 사이버테러 관련 법령의 정비도 논의되어야 할 것이다.[216]

---

215) 테러대응체계의 확립과 대테러활동 등에 관한 법률안(공성진 의원 대표발의), 테러방지 및 피해보전 등에 관한법률안(조성태 의원 대표발의), 테러예방 및 대응에 관한 법률안(정형근 의원 대표발의) 등이다. 국가보안기술연구소, 국가 사이버위기 관리 체계 강화방안에 관한 연구, 2008, 97-99쪽 참조.

216) 마침 이와 관련해서는 2008년 10월 28일 의원입법으로 '국가 사이버위기관리법안'(공성진 의원 대표발의)이 발의되어 보다 이에 대한 활발한 논의가 진행될 것으로 기대된다. 특히, 현재 대통령 훈령에

근거한 국가사이버안전센터에 대한 법적 근거를 담은 동 법안의 주요내용은 다음과 같다. ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제4조). ② 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련정보를 상호 공유하기 위하여 민·관 협의체를 구성·운영할 수 있음(안 제5조). ③ 국가정보원장은 국가사이버위기 관리종합계획을 수립하고 이에 따라 위기관리기본지침을 작성하여 책임기관의 장에게 배포하고, 책임기관의 장은 세부지침을 수립·시행하여야 함(안 제6조). ④ 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조). ⑤ 책임기관의 장은 사이버공격을 탐지하여 사이버위기 발생 가능성을 조기에 차단·예방하는 등 피해를 최소화하기 위하여 신속한 대응조치를 취하여야 함(안 제9조). ⑥ 책임기관의 장은 사이버공격으로 인해 피해가 발생한 경우에는 자체 사고조사를 실시하고, 그 결과를 관계 중앙행정기관의 장 및 국가정보원장에게 통보하여야 하며, 국가정보원장은 필요한 경우에 직접 사고조사를 실시할 수 있음(안 제10조). ⑦ 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취해야 함(안 제12조). ⑧ 정부는 심각단계의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등을 위하여 관계 기관 및 전문인력이 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제13조). ⑨ 관계 중앙행정기관의 장 및 국가정보원장은 사이버위기관리에 필요한 기술개발·국제협력 등 필요한 시책을 추진할 수 있음(안 제14조 및 제16조). ⑩ 정부는 사이버공격 기도에 관한 정보를 제공하거나 사이버공격을 가한 자를 신고한 자에 대하여 포상금을 지급할 수 있음(안 제18조). ⑪ 직무상 비밀을 누설한 경우에는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 보안관제센터를 구축하지 아니한 경우에는 2천만원 이하의 과태료에 처할 수 있음(안 제19조 및 제20조).

제5장

우리나라 사이버안전의 실태

05 우리나라 사이버안전의 실태

제1절 사이버안전의 실태

이 절에서는 앞의 제2장 제2절에서 살펴본 사이버침해 유형 분류 가운데 공격 수법과 피해를 기준으로 각 유형별로 그 발생원인 및 피해양상, 발생빈도 및 유형간 발생비중, 피해규모 등을 분석하고, 이를 토대로 유형별 위험도 및 고위험군 침해유형을 파악하여 본다. 그 다음으로는 대응전략 수립과 관계하여 분야별 사이버안전 실태를 살펴본다.

1. 유형별 사이버침해 현황

가. 의 의

기술의 급속한 발전으로 사이버침해의 양태와 행위 및 행위자 유형도 크게 달라졌다. 개인 컴퓨터의 출현은 전체 침해 과정을 1명 혹은 2명의 전문가 수중에 놓이게 만들었는데, 예를 들면 한때 세상을 공포에 떨게 했던 '해킹'이 있다. 더 최근에는 '플러그 앤 플레이' 및 '클라우드' 컴퓨팅 시스템으로 인해 컴퓨터 운영체제에 관

한 전문지식의 필요성이 극적으로 감소했다. 전문지식의 필요성 부재와 온라인을 통한 침해 이익의 잠재성 증가가 결합하면서, 기밀성과 수익(범죄 경영 윤리에 있어) 극대화의 욕구가 도덕성과 윤리적 해커들의 기술적 허세를 바꾸어 놓았다.[217]

따라서 사이버침해는 양적인 면과 질적인 면에서 모두 이제 새로운 위협 단계에 들어섰다고 할 수 있다.[218] 인터넷에서 악성프로그램의 수가 크게 증가하고 있어 2초마다 새로운 변종이 나타나고 있으며, 유니트 공법 식으로 산업적으로 만들어지고 있다. 동시에 점점 더 지능적인 공격기술과 광범위한 공격능력을 가진 매우 성숙한 악성 프로그램을 발견할 수 있다.

또한 사이버침해의 위해 및 피해 가능성은 계속해서 높다고 할 수 있다. 이는 사이버침해 행위자들이 고도의 전문성을 갖고 있으며 또 배후에 범죄조직이 있는 경우가 많기 때문이다. 오늘날 사이버침해 행위자는 더 이상 단독으로 행동하지 않으며, 취약점을 찾고 악성코드를 제작하며 절취한 데이터를 처리하는 일련의 가치형성 사슬을 갖는 분업화·조직화된 네트워크에 속해 있는 경우가 많다. 이들 범죄조직은 국경을 초월해서 해커나 바이러스 제작자와 협력하여 고도로 전문적으로 일하고 인터넷에서 사이버침해를 저지르는 데 필요한 악성프로그램 및 인프라를 갖추고 있다.[219] 그리고 사이버침해는 공격자가 변화된 기술조건에 빠르게 적용하여 놀라운 혁신능력을 보여주므로 대단히 역동적이라고 할 수 있다.

다른 한편으로 공격 대상이 될 수 있는 시스템과 정보가 많아졌다. 이는 전자정부, 전자상거래 그리고 최근의 모바일 오피스 혹은 스마트 오피스 등의 추진으로 더욱 심화되고 있다. 한편 사이버침해는 피해자가 공격 및 피해 사실을 알지 못하는 경우가 많고 또 특히 기업의 경우 이를 알더라도 신용훼손을 우려하여 신고하지 않는 경우가 많다.[220] 따라서 각종 통계를 통해 알 수 있는 공격 및 피해보다 훨씬

217) David Wall/백지나(역), "정보화시대의 유비쿼터스 범죄 : 사이버범죄의 이해와 규제", 형사정책연구 제19권 제4호(통권 제76호), 2008 겨울호, 9쪽.

218) 미하엘 항에(Michael Hange) 독일 연방정보기술보안청장이 2010년 5월 12일 "Cybercrime – eine globale Gefahr?" 콘퍼런스에서 언급하였다 : Wirtschaftskonferenz 2010 von BKA und BSI zum Thema "Cybercrime – eine globale Gefahr?"
https://www.bsi.bund.de/cln_174/ContentBSI/Presse/Pressemitteilungen/BKA_IuK-Kriminalitaet_120510.html <2010년 5월 17일 방문>

219) David Wall/백지나(역), 앞의 글, 9쪽.

많은 공격 및 피해가 발생하고 있다고 본다.

표 27 시기별 사이버 침해의 특징

시 기	공격 수법	공격자	공격 대상	피 해	비 고
90년대	해킹, 바이러스	개인	일반 정보시스템	특정 업무 마비 및 정보 유출	LOVE 바이러스
2003년	버퍼 오버 플로우	개인 범죄집단	도메인 서버	인터넷 마비 및 공포	1.25 인터넷침해사고
2009년	DDoS	테러집단 적대국가	국가 정보시스템	특정 업무 마비 및 정보 유출	7·7 DDoS 공격
2010년	Stuxnet	테러집단 적대국가	원전 등 기반시설	사회기능 마비 및 공포	–

표 28 사이버 위협 패러다임의 변화

구 분		2005년 이전	2005년 이후
인터넷 환경		개별망 기반의 국지적 서비스, 상호작용이 적은 정적(靜的)인 웹1.0	방송통신 융합, 디지털 컨버전스, 상호작용이 많은 동적(動的)인 웹2.0
주요 사이버 위협 유형		해킹, 인터넷 웜, DoS(서비스거부공격), 이메일 스팸	해킹, 스파이웨어, 봇넷, DDoS(분산서비스거부공격), 휴대폰 스팸
공격 목적		호기심자기과시, 서비스 가용성 침해	데이터 탈취를 통한 금전적 이득, 불법 유해정보 유포, 저작권 침해
주체별 보안 이슈	국가	기반시설, 국지적 네트워크 보안	All-IP망 기반 범국가적 인프라 보호
	기업	웹사이트 변조, 서비스 장애	이용자정보 및 내부정보 유출
	개인	피해자	피해자인 동시에 가해자

공공부문의 경우 2004년도에 국가·공공기관에서 총 3,970건의 해킹·바이러스

220) 사이버침해는 해당 범죄가 실제로 발생하였으나 수사기관에 인지되지 않거나 수사기관에 인지되어도 용의자 신원미파악 등 문제가 해결되지 않아 공식적 범죄통계에 집계되지 않은 암수범죄(暗數犯罪)로 볼 수 있다.

등 침해사고가 신고되었으며, 2003년도 1,323건에 비해 3배 이상 증가하였다. 이는 보안취약요인 또는 해커의 증가 때문이 아니라 2004년 2월 국가사이버안전센터 개소로 사고인지가 신고 위주에서 24시간 보안관제에 의한 능동적인 탐지로 전환된 데에 따른 것으로 파악되고 있다. 2004년도 침해사고 현황을 살펴보면 크게 두 가지 특징을 발견할 수 있는데 첫째, 초·중·고·대학 등 교육기관을 제외한 국가·공공기관의 사고발생 비율이 2003년도에 비해 16배로 현저히 증가하였으며 둘째, 웜 바이러스 감염피해가 해킹관련 사고건수를 추월한 것이 그것이다. 2005년도에 발생한 공공분야 해킹 및 웜·바이러스 사고건수는 4,549건으로 2004년도 3,970건에 비하여 16% 증가하였다. 2006년에 발생한 공공분야 해킹관련 및 바이러스 사고건수는 4,286건으로 2005년 4,549건에 비하여 263건(-5.8%) 감소하였다. 사고유형별로는 악성코드 감염사고가 가장 많았으며 사고 기관별로는 지자체에서 가장 많은 사이버 침해사고가 발생하였다. 2007년에는 공공분야 사이버 침해사고가 배 가까이 늘었고 지방자치단체와 교육기관들의 보안 취약성은 오히려 악화된 것으로 나타났다. 2007년 공공분야 사이버 침해사고 건수를 취합한 결과, 전체 공공기관에서 발생하는 사이버 침해사고 건수는 총 7,588건으로 전년도의 4,286건에 비해 크게 증가한 것으로 나타났다. 2008년에는 경유지 악용과 자료훼손 및 유출 유형은 증가하였으며, 특히 자료훼손 및 유출 유형은 전년 대비 448% 급증한 789건이 발생하였다. 공공분야 사이버 침해 사고가 급증한 것은 날로 지능화되고 있는 사이버 공격의 진화 속도를 사이버 보안이 따라가지 못한 것으로 해석할 수 있다. 특히 지방자치단체와 교육기관을 타깃으로 한 사이버 침해사고 발생 건수가 급증하였다. 2007년 지자체에서 발생한 사이버 침해사고 건수는 총 3,827건으로 전년도의 1,470건에 비해 3배 가까이 늘었고 교육기관도 1,464건에서 2,148건으로 약 50% 증가하며 기관 중 2번째로 높은 사고 발생률을 보였다.

표 29 국가사이버안전센터 공공기관 침해사고 신고처리 통계(연도별)

연도	2004	2005	2006	2007	2008
악성코드 감염	2,287	2,504	2,548	6,194	5,655
경유지 악용	378	1,214	1,316	767	984
홈페이지변조	297	687	253	379	228
자료훼손유출	126	87	123	176	789
단순침입시도	570	–	–	–	–
기타	312				
계	3,970	4,492	4,117	7,340	6,867

※ 2005년부터는 단순침입시도를 침해사고 유형에서 제외

민간부문의 경우 한국정보보호진흥원 인터넷침해대응센터에서 접수·처리한 민간부문 침해사고 통계를 분석한 결과 과거 국내의 주요 사이버침해사고 경향은 주로 대학 내 전산망에 대한 침입이나 PC통신환경에서 단순한 개인 ID에 대한 침해사고가 주류를 이루었다. 그러나 초고속인터넷 등 인터넷 보급이 확대되고 온라인 게임, 인터넷 뱅킹 등 인터넷을 이용한 서비스 이용이 증가하면서 이들을 대상으로 하여 금전적인 이익을 추구하는 범죄형 해킹이 증가하고 있으며, 해킹에 사용되는 공격툴 및 공격 기법들이 인터넷을 통해 널리 공개되어 해킹에 가담하는 공격자들의 연령층도 다양화되고 있다. 해킹사고는 점차 증가하고 있는 추세이며 그 원인은 다음과 같이 분석할 수 있다. 첫째, 정보시스템의 활용도 증가 및 인터넷 등 네트워크를 통한 상호 연결의 증가를 들을 수 있다. 즉, 각 정보시스템들은 내부적으로 근거리통신망(LAN)에 의해 서로 연결되어 있고, 또한 인터넷에 연동되어 전세계 어디든지 시간과 공간에 구애됨이 없이 정보를 교환하며 각종 서비스를 제공받을 수 있게 되었다. 반면 네트워크화의 진전에 따라 적법한 내부 사용자뿐 아니라 전세계의 어느 사용자라도 내부 시스템에 불법적으로 접근할 가능성이 높아진 것이다. 둘째, 해커들 간의 자유로운 정보 교환을 들 수 있다. 해커들은 보통 자신들의 홈페이지를 만들어서 해킹기술을 공개하고 있어 누구나 해킹 정보를 쉽게 구할 수 있다. 과거에는 인터넷을 이용하는 국내 몇몇 대학들의 전유물로 여겨지던 네트워크 침입 등의 해킹기술이 모

든 기관 및 개인의 컴퓨터들이 인터넷에 연동됨에 따라 해킹 정보사이트를 통해 일반인까지도 해킹 기술을 쉽게 습득할 수 있는 환경이 조성된 것도 한 원인이라 볼 수 있다. 셋째, 정보시스템 관리자의 기술적 역량 부족 및 정보보호에 대한 인식 부족을 그 원인으로 들 수 있다. 정보시스템을 공격하고자 하는 수많은 해커들은 공격기술에 심취해서 공격을 시도하고 있지만, 정보시스템 관리자는 기관의 수많은 시스템을 관리와 고유 업무에 많은 시간을 빼앗겨 정보보호에 신경 쓰기가 쉽지 않다. 또한 정보보호 인식이 확산되어 침해사고에 적극적으로 대처하려고 하여도 관련 지식의 부재로 실천이 어려웠던 점 등을 들 수 있다.

2005년 민간부문 해킹사고 처리 건수는 33,633건으로 전년도에 비하여 38% 증가한 반면 웜·바이러스 신고는 85% 감소하였다. 민간부문 침해사고의 주요특징은 크게 두 가지로 요약 될 수 있는데, 첫째는 2004년에 비하여 Netsky, Bagle 등과 같이 전파력이 강한 대량 이메일 발송 웜의 출현이 2005년도에 상대적으로 적었다는 점이며 둘째, 과거 지적 호기심이나 언론의 조명을 받기 위한 단순 웜·바이러스 제작, 유포 등의 침해사고 형태가 감소하고 금전적 이익을 목적으로 하는 피싱, 게임 ID/비밀번호를 갈취해 가는 악성코드 유포 등 특정 목적에 의한 의도적 침해가 증가하였다는 점이다. 2006년도 민간부문 침해사고 통계를 분석한 결과 해킹사고 접수·처리는 26,808건으로 전년(33,633)대비 20.3% 감소하였으며, 웜·바이러스 피해신고는 총 7,789건으로 전년(16,093)대비 51.6% 감소하였다. 특히 웜·바이러스 피해신고가 전년대비 크게 감소한 주요원인은 NetSky, Bagle 웜과 같은 대량 이메일 발송 웜의 출현 및 피해가 감소하였기 때문인 것으로 파악되었다. 해킹사고의 경우 전체건수에 있어서는 전년도에 비하여 감소하였으나 최근 사이버침해사고는 피싱, 온라인 게임 ID/비밀번호를 유출하는 트로이잔 유포 등 금전적 이익을 목적으로 행해진다는 점에서 위험성은 오히려 과거에 비하여 증가하고 있다고 할 수 있다.

2007년도 해킹사고 접수·처리는 21,732건으로 전년(26,808건) 대비 18.9% 감소하였으며, 웜·바이러스 피해신고는 총 5,996건으로 전년(7,789건)대비 23.0% 감소하였다. 특히 웜·바이러스 피해신고가 전년대비 크게 감소한 주요원인은 NetSky, Bagle 웜과 같은 대량 이메일 발송 웜의 출현 및 피해가 감소하였기 때문인 것으로 파악되었다.

2008년도 방송통신위원회에서 접수·처리한 민간부문 침해사고 통계를 분석한 결

과 웜·바이러스 신고건수는 총 8,469건으로 2007년(5,996건)에 비하여 41.2% 증가하였으며 해킹사고 접수·처리 건수는 총 15,940건으로 2007년(21,732건)에 비하여 26.7% 감소하였다.

2009년 한 해 동안 방송통신위원회에서 접수·처리한 민간부문 침해사고 통계를 분석한 결과, 웜·바이러스 신고건수는 총 10,395건으로 2008년(8,469건)에 비하여 22.7% 증가하였으며, 해킹사고 접수·처리 건수는 총 21,230건으로 2008년(15,940건)에 비하여 33.2% 증가하였다.

표 30 인터넷침해대응센터 침해사고 신고처리 통계(연도별)

연도		2004	2005	2006	2007	2008	2009	2010(9월)
웜바이러스		107,994	16,093	7,789	5,996	8,469	10,395	12,580
해킹		29,109	33,633	26,808	21,732	15,940	21,230	11,844
	스팸릴레이	3,297	6,334	14,055	11,668	6,490	10,148	3,689
	피싱경유지	220	1,087	1,266	1,095	1,163	988	746
	단순침입시도	–	–	3,711	4,316	3,175	2,743	3,155
	홈페이지변조	4,812	16,692	3,206	2,293	2,204	4,320	2,134
	기타	20,780	9,520	4,570	2,360	2,908	3,031	2,120
악성 봇		–	18.8%	12.5%	11.3%	8.1%	1.0%	0.6%

* 2004년 및 2005년의 경우 단순침입시도의 분류가 없고 일반해킹으로 분류

나. 해 킹

해킹은 네트워크, 시스템, 응용프로그램, 데이터 혹은 기타 자원 등에 인가를 받지 않은 자가 논리적 혹은 물리적으로 불법 접속하는 공격을 말한다.[221]

한국인터넷진흥원 인터넷침해대응센터가 접수·처리한 민간부문 침해사고 통계[222]를 분석한 결과 해킹사고 접수·처리는 2005년까지 크게 증가(33,633건)하다 2006

221) "비인가접근공격"이라 하기도 한다(국가사이버안전매뉴얼, 57쪽).

222) 매월 발간되는 '인터넷침해사고 동향 및 분석 월보'를 분석.

년 이후 상당히 감소하였다. 2007년도는 21,732건으로 2006년(26,808건)에 비하여 18.9% 감소하였고, 2008년도는 15,940건으로 2007년(21,732건)에 비해 크게 감소하였다. 2009년에 7·7 DDoS 공격 등의 영향으로 다시 증가하였는데(21,230건), 침해사고 유형별로는 스팸릴레이, 단순침입시도, 홈페이지 변조가 주를 이루고, 피싱 경유지로 악용되는 경우는 감소하고 있다.

표 31 인터넷침해대응센터 해킹신고처리 통계(연도별)

연도	2004	2005	2006	2007	2008	2009	2010(9월)
스팸릴레이	3,297	6,334	14,055	11,668	6,490	10,148	3,689
피싱경유지	220	1,087	1,266	1,095	1,163	988	746
단순침입시도	–	–	3,711	4,316	3,175	2,743	3,155
홈페이지변조	4,812	16,692	3,206	2,293	2,204	4,320	2,134
기타	20,780	9,520	4,570	2,360	2,908	3,031	2,120
계	29,109	33,633	26,808	21,732	15,940	21,230	11,844

※ 2004년 및 2005년의 경우 단순침입시도 및 기타의 분류가 없고 일반해킹으로 분류

또 피해 기관별로는 아래 표와 같이 기타(개인)가 차지하는 비율이 가장 많고, 다음으로 기업, 대학 순으로 나타났다. 민간 부문의 경우 개인이 차지하는 비율이 2008년 74.1%, 2009년 76%로 매우 높은데, 이는 개인 인터넷 이용자의 PC가 사이버침해에 악용되는 경우가 많기 때문으로 분석된다.[223]

223) 2010 국가정보보호백서, 32쪽

표 32 인터넷침해대응센터 해킹신고처리 통계(피해기관별)

연도	2005	2006	2007	2008	2009	2010(9월)
기업	11,166	3,689	3,039	3,344	4,185	4,100
대학	714	1,094	1,121	603	598	187
비영리	1,932	714	273	173	239	181
연구소	26	16	5	2	1	0
네트워크	1,898	307	133	0	1	0
기타(개인)	7,283	20,988	17,161	11,818	16,206	7,376
계	23,019	26,808	21,732	15,940	21,230	11,844

※ 기관 분류기준 : 침해사고 관련 도메인이나 IP를 기준으로 기업(co,com), 대학(ac), 비영리(or,org), 연구소(re), 네트워크(ne,net), 기타(pe 또는 ISP에서 제공하는 유동IP 사용자)로 분류

과거 해킹이 자기 과시나 네트워크 마비가 목적이었다면, 최근에는 개인정보 탈취나 금품 갈취 등 범죄형 해킹이 증가하는 추세이다. 2007년 개인정보 탈취 등을 목적으로 하는 해킹시도(4,316건)가 전년대비 16.3% 증가한 사실이 이를 뒷받침한다.

한편 공공부문의 경우 2004년도에 국가·공공기관에서 총 3,970건의 해킹·바이러스 등 침해사고가 신고되었으며, 2003년도 1,323건에 비해 3배 이상 증가하였다. 이는 보안취약요인 또는 해커의 증가 때문이 아니라 2004년 2월 국가사이버안전센터 개소로 사고인지가 신고 위주에서 24시간 보안관제에 의한 능동적인 탐지로 전환된 데에 따른 것으로 파악되고 있다. 2004년도 침해사고 현황을 살펴보면 크게 두 가지 특징을 발견할 수 있는데 첫째, 초·중·고·대학 등 교육기관을 제외한 국가·공공기관의 사고발생 비율이 2003년도에 비해 16배로 현저히 증가하였으며 둘째, 웜바이러스 감염피해가 해킹관련 사고건수를 추월한 것이 그것이다.

2005년도에 발생한 공공분야 해킹 및 웜·바이러스 사고건수는 4,549건으로 2004년도 3,970건에 비하여 16% 증가하였다. 사고 유형별로는 웜·바이러스 감염사고가 55%로 가장 많았으며 사고기관별로는 교육기관이 56%로 가장 많은 사이버 침해사고가 발생하였다. 2005년도에 발생한 침해사고의 유형별 분포를 보면 웜·바이러스 감염사고가 2,504건이 발생하여 전체의 55%를 차지, 전년에 이어 가장 심각한 사이

버위협이 되었으며 경유지악용이 1,214건(27%)으로 두 번째 위협으로 나타났다. 그 밖에 홈페이지 변조 687건(15%), 자료훼손 및 유출 87건(2%) 순으로 나타났다.

2006년에 발생한 공공분야 해킹관련 및 바이러스 사고건수는 4,286건으로 2005년 4,549건에 비하여 263건(-5.8%) 감소하였다. 사고유형별로는 악성코드 감염사고가 가장 많았으며 사고 기관별로는 지자체에서 가장 많은 사이버 침해사고가 발생하였다. 사고유형별 분포를 보면 악성코드 감염, 경유지 악용, 홈페이지 변조, 자료 훼손 및 유출 순으로 점유되었다. 2006년은 전자우편이나 보안에 취약한 홈페이지를 통한 정보절취형 악성코드가 유포되는 형태의 해킹이 기승을 부렸는데, 이는 해킹의 목적이 과거 호기심이나 실력과시에서 사용자의 개인정보를 악용하는 금전적 이득 추구로 변질되었기 때문이다. 이에 대응해서 관계기관은 탐지기술의 고도화, 최신 패치 기술개발 등 사이버 보안분야의 노력이 이어지고 있지만, 악성코드에 백신탐지 우회 기술이 적용되는 등 사이버 위협수준이 날로 심각해지고 있어 앞으로 악성코드 감염 사고가 이어 질 것으로 보인다.

2007년에는 공공분야 사이버 침해사고가 배 가까이 늘었고 지방자치단체와 교육기관들의 보안 취약성은 오히려 악화된 것으로 나타났다. 2007년 공공분야 사이버 침해사고 건수를 취합한 결과, 전체 공공기관에서 발생하는 사이버 침해사고 건수는 총 7,588건으로 전년도의 4,286건에 비해 크게 증가한 것으로 나타났다. 2008년에는 경유지 악용과 자료훼손 및 유출 유형은 증가하였으며, 특히 자료훼손 및 유출 유형은 전년 대비 448% 급증한 789건이 발생하였다.

공공분야 사이버 침해 사고가 급증한 것은 날로 지능화되고 있는 사이버 공격의 진화 속도를 사이버 보안이 따라가지 못한 것으로 해석할 수 있다. 특히 지방자치단체와 교육기관을 타깃으로 한 사이버 침해사고 발생 건수가 급증하였다. 2007년 지자체에서 발생한 사이버 침해사고 건수는 총 3,827건으로 전년도의 1,470건에 비해 3배 가까이 늘었고 교육기관도 1,464건에서 2,148건으로 약 50% 증가하며 기관 중 2번째로 높은 사고 발생률을 보였다.

표 33 국가사이버안전센터 공공기관 해킹신고처리 통계(연도별)

연 도	2004	2005	2006	2007	2008
경유지 악용	378	1,214	1,316	767	984
홈페이지변조	297	687	253	379	228
자료훼손·유출	126	87	123	176	789
단순침입시도	570	–	–	–	–
계	1,371	1,988	1,692	1,322	2,001

※ 2005년 이후 단순침입시도의 분류가 없어짐

또한, 피해 기관별로는 아래 표와 같이 교육기관이 차지하는 비율이 가장 많고, 다음으로 지자체, 산하기관 순으로 나타났다. 공공 부문의 경우 교육기관이 차지하는 비율이 매우 높은데, 이는 교육기관의 PC가 사이버침해에 악용되는 경우가 많기 때문으로 분석된다.

표 34 국가사이버안전센터 공공기관 해킹신고처리 통계(피해기관별)

연도	2004	2005	2006	2007	2008
국가기관	798	94	124	105	294
지자체	701	161	221	229	571
연구소	155	70	147	47	102
교육기관	1,537	1,483	973	622	609
산하기관	558	158	218	254	232
기타	221	22	9	65	193
계	3,970	1,988	1,692	1,322	2,001

※ 경유지 악용, 홈페이지 변조, 자료훼손 및 유출을 해킹 유형으로 포함(2004년도의 경우 이외에 웜바이러스 감염, 기타 유형까지 해킹사고에 포함하여 처리)

다. 악성코드 유포

민간 부문의 경우 웜·바이러스 감염피해가 2004년 2,287건으로 전체 침해사고의 58%를 차지하여 2003년도의 29%에 비해 2배 이상 증가하였다. 2004년도에 처음으로 웜·바이러스 감염사고가 해킹사고 건수를 추월하게 되었다. 특히, 웜·바이러스 감염사고 가운데 감염 후 스스로 익명의 IRC(Internet Relay Chat) 서버 등에 접속하여 공격자의 명령에 따라 원격 작동하는 '봇' 계열의 웜·바이러스 및 보안시스템을 우회할 수 있는 전자우편 유포형 웜·바이러스가 피해의 대부분을 차지하였다.

2005년 국내 민간부문에 접수된 웜·바이러스 피해신고는 총 16,093건으로, 2004년에 비하여 85% 감소(107,994 → 16,093)하였다. 2005년에는 2004년에 주로 기승을 부렸던 Netsky, bagle, Dumaru 등 대량 이메일 발송 웜의 출현 및 피해건수가 상대적으로 적었기 때문이며, 최근에는 기존의 지적 호기심이나 일반인의 주목을 끌기 위한 웜·바이러스의 유포보다는 특정대상, 특정목적을 가지고 행해지는 해킹의 형태로 변하고 있기 때문인 것으로 보인다.

2006년 국내 민간부문에 접수된 웜·바이러스 피해신고는 총 7,789건으로, 2005년 16,093건에 비하여 51.6% 감소하였다. 2006년에 웜·바이러스 신고건수가 전년도에 비하여 크게 감소한 것을 알 수 있는데 주요 감소 원인으로는 2004년 이후 NetSky, Bagle 웜 변종과 같은 대량이메일 발송 웜의 출현이 2006년에도 지속적으로 감소하였기 때문이다. 물론 게임 ID/비밀번호 등을 유출하는 트로이목마 계열의 악성코드 유포는 증가하고 있으나 이러한 악성코드는 주로 자체 전파능력이 없기 때문에 전체 신고 건수는 감소하였다.

2007년 한 해 동안 웜·바이러스 신고건수는 5,996건으로 월 평균 499.7건에 해당하며, 2006년(7,789건) 대비 23.0% 감소한 수치다. 주요 감소 이유로는 Netsky, Bagle과 같은 이메일 바이러스로 인한 피해신고가 올 들어 크게 감소하였기 때문이다. 반면 웹 사이트를 통하여 감염되는 악성코드 의한 피해신고가 증가하였으나 자체 전파력이 없어 전체 건수는 전년도에 비하여 감소한 것으로 파악되었다. 2008년의 경우 2008년 한 해 동안 웜·바이러스 신고건수는 8,469건(월 평균 705.7건)으로 2007년(499.7건) 대비 41.2% 증가하였다. 이는 지난 2007년 9월 이후 증가하기 시작한 특정 온라인 게임의 계정정보 탈취를 목적으로 하는 ONLINEGAMEHACK,

KORGAMEHACK 등의 신고건수가 2007년 1,060건(17·7%)에서 '08년 1,895건(22.4%)으로 전체 피해신고 건수 및 차지하는 비중 모두에서 크게 증가한 것이 주요 원인으로 파악되었다. 이 외에도 전년에 이어 자체 전파력은 없으나 주로 웹사이트 등을 통해 감염되어 추가적인 악성코드를 다운로드하는 AGENT, XEMA 및 USB 이동식 저장장치를 통하여 전파되는 AUTORUN이 지속적으로 확인되었으며, 위조된 ARP Reply 패킷을 통한 통신 데이터의 유출 및 변조, 허위 광고나 경고 메시지 등을 통해 사용자의 클릭 및 결제를 유도하는 등의 피해사례가 특징적이라 할 수 있다.

2009년 한 해 동안 웜바이러스 신고건수는 10,395건(월 평균 866건)으로 2008년(월 평균 706건) 대비 22.7% 증가하였다. 2008년과 마찬가지로 특정 온라인 게임의 계정정보 탈취를 목적으로 하는 온라인게임 해킹의 신고 건수가 10.8%로 가장 많은 비율을 차지하였다. 자체 전파력은 없으나 주로 웹사이트 등을 통해 감염되어 추가적인 악성코드를 다운로드하는 웜바이러스인 에이전트가 10.5%로 그 뒤를 이었다. 이외에 USB 같은 이동형 저장매체를 통해 전파되어 보안 설정을 변경, 인터넷 장애를 유발하는 CONFICKER 및 그 변종이 다수 발견되었고, 개발환경 내 특정 소스에 코드를 삽입하는 새로운 전파 기법이 사용된 INDUC, 국내외적으로 교묘해진 사회공학적 악성코드 유포 수단으로 허위 백신SW, 동영상 플레이어 등을 가장하여 사용자에게 클릭 및 결제를 유도하는 등 피해 사례가 특징적이라 할 수 있다.

봇(Bot)은 운영체제 취약점, 비밀번호 취약성, 웜·바이러스의 백도어 등을 이용하여 전파되며, 명령 전달사이트와의 백도어연결 등을 통하여 스팸메일 전송이나 DDoS 공격에 악용 가능한 프로그램 또는 실행가능한 코드를 말한다.

표 35 인터넷침해대응센터 웜·바이러스 감염신고처리 통계(연도별)

연도	2004	2005	2006	2007	2008	2009	2010(9월)
웜바이러스	107,994	16,093	7,789	5,996	8,469	10,395	12,580
악성 봇	-	18.8%	12.5%	11.3%	8.1%	1.0%	0.6%

※ 악성 봇은 전 세계 악성 Bot감염 추정 PC 대비 국내 감염률

공공부문의 경우 2004년 웜·바이러스 감염피해가 2,287건으로 전체의 58%를 차

지하여 2003년도의 29%에 비해 2배 이상 증가하였다. 따라서 2004년도에 처음으로 웜·바이러스 감염사고가 해킹사고 건수를 추월하게 되었다. 특히, 웜·바이러스 감염사고 가운데 감염 후 스스로 익명의 IRC(Internet Relay Chat) 서버 등에 접속하여 공격자의 명령에 따라 원격 작동하는 '봇' 계열의 웜·바이러스 및 보안시스템을 우회할 수 있는 전자우편 유포형 웜·바이러스가 피해의 대부분을 차지하였다.

2005년 웜·바이러스 감염사고 건수는 웜·바이러스 감염사고가 2,504건이 발생하여 전체의 55%를 차지, 전년에 이어 가장 심각한 사이버위협이 되었다. 웜·바이러스 감염사고는 2004년에 이어 1위의 사이버 위협이 되고 있지만 발생빈도가 감소하였다.

2006년에도 악성코드 감염사고가 가장 많았으며 전자우편이나 보안에 취약한 홈페이지를 통한 정보절취형 악성코드가 유포되는 형태의 침해사고가 기승을 부렸는데, 이는 과거 호기심이나 실력과시에서 사용자의 개인정보를 악용하는 금전적 이득 추구로 변질되었기 때문이다.

2007년과 같이 2008년에도 웜·바이러스 감염 유형이 대부분의 건수를 차지하고 있으며 전체 침해사고의 71%를 차지하고 있다.

표 36 국가사이버안전센터 공공기관 악성코드 감염 신고처리 (연도별)

연도	2004	2005	2006	2007	2008
악성코드 감염	2,287	2,504	2,548	6,194	5,655

공공기관별 2007년 대비 악성코드 감염사고 발생 건수를 분석하면 2007년과 같이 지자체와 교육기관의 감염사고 발생 건수가 가장 많았다. 그러나 2007년 대비 국가기관에서 발생한 감염사고가 2008년에는 63.3% 증가한 813건으로 급증하였다.

표 37 국가사이버안전센터 공공기관 악성코드 감염 신고처리 통계(피해기관별)

연도	2005	2006	2007	2008
국가기관	231	316	498	813
지자체	599	1,233	3,583	2,443
연구소	109	110	145	698
교육기관	1,058	489	1,504	1,210
산하기관	506	396	448	418
기타	1	4	16	73
계	2,504	2,548	6,194	5,655

※ 2004년도의 경우 이외에 웜바이러스 감염, 기타 유형까지 해킹사고에 포함하여 처리

라. 서비스거부 공격

서비스거부 공격(Denial of Service attack)은 시스템에 과도한 부하를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 행위를 말한다. 특히 최근 큰 피해를 일으키고 있는 분산 서비스거부 공격(Distribute Denial of Service attack)은 여러 대의 PC가 한 번에 특정 사이트에 접속하는 해킹 방식의 하나다. 트래픽이 많아지면 과부하가 걸려 사이트가 마비된다. 이는 내부의 정보를 빼내기 위한 것이 아니라 단지 다른 사람들이 이용하지 못하도록 방해하는 방법이다. 보통 좀비PC 한 대에서 발생하는 총 트래픽은 54.2kbps로 좀비PC에 크게 무리를 주지 않는 수준이다. 따라서 본인도 모르게 해커가 마음대로 조종할 수 있다.

2009년 7월 7일부터 9일까지 세 차례에 걸쳐 국내에서 발생한 DDoS공격은 국내 주요 공공기관과 이용자 방문이 많은 포털, 금융 사이트 등 총 26곳을 공격해서 페이지를 열 수 없게 만들었다.

국가정보원은 정부문서가 유출되거나 업무가 마비되는 등의 피해는 전혀 없었다고 밝혀, DDoS공격 의도에 대한 궁금증을 더욱 증폭시켰다. 안철수연구소는 동시다발적으로 주요 사이트를 공격한 것과 국내 사이트에 대해 24시간 단위로 공격 목표를 바꿨다는 점을 들어 국내 사이트에 대한 정보가 풍부하고 치밀한 사전준비가

있을 것으로 분석했다. 주요 사이트가 소화할 수 있는 트래픽의 양을 정확히 예측했기 때문이다.

1차 공격 이후 국가정보원은 악성 프로그램 샘플을 분석한 결과 공격할 대상 26개 기관의 IP를 발견했다. 또 과도한 트래픽을 유발하는 특징이 있으며, 국내 주요 사이트의 접속장애 현상이 발생하는 등 사안의 심각성을 감안해 사이버 위기경보 단계를 '주의'로 올렸다.

1, 2차 공격을 받은 기업들은 트래픽을 분산시키기 위해 서버와 회선을 늘리고, 공격 목표가 된 인터넷주소를 살짝 바꾸는 편법까지 동원해 피해를 최소화하려고 노력했다.

1차 공격이 끝난 직후 국가정보원이 집계한 조사에 따르면 아무런 이해관계가 없는 국내 PC 1만 2000여대와 해외 PC 8000여대가 DDoS공격에 이용되었다. 악성코드는 이메일 첨부파일이나 출처가 분명하지 않은 액티브X, USB 드라이브 등에 침투해 이용자들에게 접근했다. 파일이 받아진 뒤에는 윈도우 서비스 형태로 등록되어 PC 시작과 함께 자동으로 실행되었다. 이후 일정한 시각에 좀비PC가 특정 사이트에 한꺼번에 접속해 사이트를 마비시킴으로써 7·7 대란이 일어났다.

마. 기타 공격

최근에는 악성코드 공격, 서비스거부 공격, 해킹 등의 요소를 복합적으로 이용하는 공격도 등장하고 있다. 봇 계열의 악성코드가 서비스거부 공격을 수행하거나 해킹을 위한 피싱 등의 경우가 이에 해당하며, 복합구성공격이라 하기도 한다.[224]

2. 분야별 사이버침해 안전 실태

가. 사이버전

사이버전과 관련하여서는 우리나라가 직접 공격 및 피해를 입은 사례는 알려진

224) 국가사이버안전매뉴얼, 57쪽.

바가 없다. 수년 전 일본과의 독도 관련 사이버 공격은 사이버전이라고 하기는 어렵다. 그러나 외국의 경우 실제 사이버전이 발생한 사례가 다수 알려진 바 있다.

1991년 미국은 걸프전 당시 컴퓨터 바이러스를 이용하여 이라크 방공망을 마비시켰다. 1999년 유고 내전에서 정부군은 코소보와 전쟁에서 영국 기상시스템을 마비시켜 나토군이 공습을 취소하도록 하였다. 실제로 공군의 공습은 기상 장교의 승인에 따라 이루어지는 데, 기상악화 및 환경변화에 따라 전투기가 발진을 하는 데 있어 기상 장교가 승인을 하지 않으면 공습이 취소된다. 2001년 중국은 미국 전투기와의 하이난 섬 인근 충돌로 인하여 미 정부기관에 대한 전산망 공격을 수행하였다. 실제 해커들의 소행으로 판명되었으나, 배후에 중국정부가 있다는 증거를 확보하지는 못했다. 2003년 미국은 다시 이라크 전쟁을 수행 하였는데, 이 당시에도 사전에 이라크 통신망을 교란하여 마비시켰다. 2007년 6월에 발생한 에스토니아와 러시아간의 사이버전에서는 에스토니아 수도 탈린에 있던 소련군 동상이 철거되자 대통령궁, 정부부처, 정당, 금융기관 등을 대상으로 대규모 사이버공격이 행해져 2개월간 행정업무가 마비되는 등 혼란이 야기되었다. 이후 나토는 에스토니아가 다시 사이버공격을 당하지 않게 하기 위하여 에스토니아에 ENISA 산하 사이버안전센터를 설립하였다. 에스토니아도 재발방지를 위하여 유럽 최초로 사이버 안보 전략을 수립하여 운영 중에 있다. 이후, 소련은 에스토니아에서 얻은 교훈을 토대로 그루지아와 사이버전을 수행하였다. '남오세티아'를 둘러싼 영토분쟁으로 무력충돌이 확산된 그루지아 주요 정부 인터넷사이트가 러시아 비지니스 네트워크(RBN : Russian Business Network)로부터 수차례 무차별 DDoS 공격으로 정부기관 사이트가 초토화 되었다. 최근 중국, 러시아는 군사·정치적 우위를 점하고자 상대국의 약점을 이용한 비대칭적 사이버 공격을 수행하고 있다. 특히, 중국은 사이버 공격이 고난도 해킹이 아니어도 근원지 추적이 불가능하고, 상대국의 네트워크 의존도가 높아 피해 확산이 용이하며, 국제법 미비로 국가 간 수사협조 및 사이버전(戰) 방어를 수행할 공조 체계가 어렵다는 것을 간파하여 물리적인 군사력과 함께 사이버 군사력을 확대해 나가고 있다.[225]

북한과 같은 가난한 국가들은 소수의 엘리트 전사를 통해 선진국의 우수 정보시스

225) 김인중, "사이버범죄 추적·수사기법과 문제점 분석", '사이버안전 확보를 위한 바람직한 연구방향'(전문가초청 워크숍 자료집), 한국형사정책연구원, 2010. 6. 16, 42쪽.

템을 교란할 수 있도록 사이버 훈련을 시키고 있다.[226] 따라서 북한과 군사적으로 대치하고 있는 우리나라의 경우 사이버전의 발생 위험이 매우 높다고 할 수 있다. 이외에도 중국 및 일본과의 역사적 이해관계 및 영토 문제로 인해 분쟁이 본격화할 경우 이들 국가 혹은 그 일부세력에 의해 사이버전이 발생할 가능성도 배제할 수 없다.

나. 사이버테러(주요 정보통신기반시설 침해)

국가의 주요 인프라 및 서비스가 정보통신시설로 연계되어 이러한 시설에 대한 사이버 침해행위, 시스템 장애 등이 행정, 방송통신, 에너지, 물류, 금융 등 다른 분야에 연쇄적으로 파급되어, 개별 시스템의 장애가 전체시스템에 미치는 영향이 매우 커질 수 있다. 특히 국가 기반시설을 연결하고 각 정보시스템에 영향을 주는 정보통신기반시설의 광범위한 침해사고는 국가 전반의 장애를 초래할 수 있다. 이러한 제어시스템을 포함한 정보통신시설의 사고는 석유, 환경, 원자력, 전력, 수자원 등 다양한 분야에서 발생하고 있으며, 인명을 포함하여 대규모의 피해를 야기한다.

표 38 국내·외 주요정보통신기반시설 제어시스템 피해사례

시 기	발생국	피해내용	비 고
'99년	미국	· 워싱턴주 올림픽 파이프라인사의 석유 송유관 제어시스템 DB 수정 후 송유관이 폭발 · 3명 사망, 피해액 4,500만 달러, 786만 달러 벌금 부과 · http://seattletimes.nwsource.com/html/opinion/2009319747_guest10goltz.html	석유
'00년 4월	호주	· 퀸즈랜드주 오폐수 처리 제어시스템을 전직 직원이 무선통신 해킹 · 3달 동안 46차례에 걸쳐 오폐수 방출 · http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_ revenge_sewage/	환경
'03년 1월	미국	· 미국 오하이오주의 Davis-Besse 원자력 발전소의 사설컴퓨터 네트워크에 슬 래머웜이 침투 · 안전 감시시스템이 5시간 동안 정지 · http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html	원자력
'03년 1월	한국	· ISP의 DNS 등이 슬래머 웜에 감염 · 수시간 동안 인터넷 접속 마비 · http://www.krcert.or.kr/index.jsp	통신

226) 김인중, 앞의 쪽.

시 기	발생국	피해내용	비 고
'03년 8월	미국	· 동부지역의 철도신호시스템이 소빅-F 웜에 감염 · 수 시간 동안 운행 중단 · http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml	교통
'07년 3월	미국	· DHS 주관 미국 발전소 제어시스템을 모의해킹 · 발전기 가동 사이클을 변경하여 발전기 파괴 · http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnn STCText	전력
'07년 8월	미국	· 전직 직원이 캘리포니아주의 TCCA 운하 제어시스템에 악성프로그램을 설치 · 운하 운영 마비 · http://www.computerworld.com.au/article/198630/insider_charged_hacking_california_canal_system/	수자원
'08년 1월	폴란드	· 14세 소년이 TV 리모컨을 개조하여 트램 교차로를 불법 조작 · 4대의 트램 탈선 및 12명 부상 · http://www.telegraph.co.uk/newSWorldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html	교통
'08년 5월	미국	· 회계감사원(GAO) 주관 미국 최대 국립전력회사인 TVA사 제어시스템을 모의해킹 · 발전소 제어시스템 침투 성공 · http://www.cnn.com/2008/US/05/21/cyber.attack/index.html	전력
'09년 8월	러시아	· 수력발전댐의 터빈 제어시스템 장애 · 발전기 터빈 폭발, 75명 사망 · http://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_hydro_accident	수자원

※ 국가정보보호백서 2010, 77쪽에서 인용

사이버전에 비해 주요정보통신기반시설 등을 대상으로 하는 사이버테러는 상당히 빈발하고 있다고 할 수 있다. 공공부문의 경우 2006년부터 2009년까지 해킹 및 웜·바이러스 감염 등의 사이버 침해사고는 총 30,498건이 발생하였으며, 그 중 지방자치단체가 12,762건 41.85%로 제일 높았으며, 교육기관, 산하기관, 국가기관 순이다.[227] 해킹과 관련하여 교육기관이 2006년부터 2009년까지 총 9,170건 중 30.3%인 2,779건으로 가장 많은 침해사고가 발생하였으며, 그 다음으로 지방자치단체, 국가기관, 산하기관 순이다. 주목할 점은 2009년의 경우 국가기관이 1,172건으로 제일

227) 배성훈, 앞의 글, 8-9쪽. 2009년 사이버침해사고 데이터 분류기준이 변경되어 경유지 악용, 홈페이지 위·변조, 자료훼손 및 유출, 기타 부분이 해킹으로 통합되었으며, 기관 구분에서도 연구기관과 산하기관을 산하기관으로 통합하였다.

높았으며, 증가율 면에서 매년 300% 가까운 증가세를 보인다는 것이다. 이는 국가기관의 중요 정보를 노리는 해킹시도가 잦아지고 있다는 것으로 해석할 수 있다. 또 웜·바이러스 관련하여 총 21,328건 중 50.8%인 10,839건으로 지자체가 가장 높았으며, 다음으로 산하기관, 교육기관, 국가기관 순이다.

표 39 2006~2009년 정부 공공부문 침해사고 현황

구분		웜바이러스 감염	해킹				합계
			경유지 악용	홈페이지 변조	자료훼손 및 유출	기타	
2006년	국가기관	316	59	16	49	16	456
	지자체	1,233	162	38	21	16	1,470
	연구기관	110	125	5	17	3	260
	교육기관	489	821	145	7	2	1,464
	산하기관	396	146	49	23	6	620
	기타	4	3	–	6	3	16
	합계	2,548	1,316	253	123	46	4,286
2007년	국가기관	498	29	21	55	22	625
	지자체	3,583	94	111	24	15	3,827
	연구소	145	20	8	19	6	198
2007년	교육기관	1,504	513	91	18	22	2,148
	산하기관	448	85	143	26	4	706
	기타	16	26	5	34	3	84
	합계	6,194	767	379	176	72	7,588
2008년	국가기관	813	67	23	204	80	1,187
	지자체	2,443	224	64	283	53	3,067
	연구소	698	31	6	65	18	818
	교육기관	1,210	454	82	73	48	1,867
	산하기관	418	104	36	92	22	672
	기타	73	104	17	72	88	354
	합계	5,655	984	228	789	309	7,965

구분		웜바이러스 감염	해킹				합계
			경유지 악용	홈페이지 변조	자료훼손 및 유출	기타	
2009년	국가기관	562	1,172				1,734
	지자체	3,580	818				4,398
	교육기관	784	503				1,287
	산하기관	1,972	681				2,653
	기타	33	554				587
	합계	6,931	3,728				10,659
계	국가기관	2,189	1,813				4,002
	지자체	10,839	1,923				12,762
	교육기관	3,987	2,779				6,766
	산하기관	4,187	1,740				5,927
	기타	126	915				1,041
	합계	21,328	9,170				30,498

※ 국가정보원 외, 국가정보보호백서, 2007년부터 2010년까지 내용을 재구성 (배성훈, 9-10쪽에서 재인용)

2007년 국가사이버안전센터가 접수·처리한 침해사고를 분석한 결과 공공부문 침해사고는 전년에 비하여 2배 가까이 늘었고 지방자치단체와 교육기관들의 보안취약성은 오히려 악화된 것으로 나타났다. 지난해 공공부문 사이버침해사고 건수를 취합한 결과, 전체 공공기관에서 발생하는 사이버침해사고 건수는 총 7,588건으로 전년도의 4,286건에 비해 크게 증가한 것으로 나타났다.

국가·공공부문 사이버침해사고가 급증한 것은 날로 지능화되고 있는 사이버공격의 진화속도를 사이버보안이 따라가지 못한 것으로 해석할 수 있다. 특히 자치단체와 교육기관을 목표로 한 사이버 침해사고 발생 건수가 급증하였다. 2007년 지방자치단체에서 발생한 사이버침해사고 건수는 총 3,827건으로 2006년의 1,470건에 비해 3배 가까이 늘었고 교육기관도 1,464건에서 2,148건으로 약 50% 증가하여 기관 중 2번째로 높은 사고 발생률을 보였다.

표 40 2007년 공공분야 사이버 침해사고 발생 현황

기관	웜바이러스 감염	경유지악용	홈페이지 변조	자료훼손 및 유출	기타	합계
국가기관	408	29	21	56	22	625
지자체	3,583	94	111	24	15	3,827
연구소	145	20	8	19	6	198
교육기관	1,504	512	91	18	22	2,148
산하기관	448	86	143	26	4	706
기타	16	26	5	34	3	84
합계	6,194	767	379	175	72	7,588

※ 출처 : 국가사이버 안전센터(2008.2)

한편 2008년에 국가사이버안전센터에서 접수·처리한 침해사고를 분석한 결과 전년 7,588건수 대비 4.96% 증가한 7,965건인 발생하였다. 국가·공공부문 침해사고 유형들을 살펴보면 전년과 같이 웜·바이러스 감염 유형이 대부분의 건수를 차지하고 있으며 전체 침해사고의 71%를 차지하고 있다. 침해 유형별로 2007년과 비교하면 웜·바이러스 감염 사이버 침해 사고는 감소하였으나 경유지 악용과 자료훼손 및 유출 유형은 증가하였다. 특히 자료훼손 및 유출 유형은 2007년 대비 448% 급증한 789건이 발생하였다.

공공기관별 전년 대비 사이버 침해사고 발생 건수를 분석하면 2007년과 같이 지자체와 교육기관을 목표로 한 사이버 침해사고 발생 건수가 가장 많았다. 그러나 전년 대비 국가기관에서 발생한 사이버 침해사고가 89.9% 증가한 1,187건으로 급증하였다. 웜·바이러스 감염사고의 기관별 발생비율을 살펴보면, 지방자치단체가 전체 악성코드 감염사고의 43%를 차지하였다. 이는 2007년 지자체의 웜·바이러스 비율인 54.8%보다 감소된 수치로 해당 기관에 대한 지속적인 웜·바이러스 감염예방 조치에 기인한 것으로 보인다.

다. 민간부문 정보시스템 및 정보 침해

2008년도 방송통신위원회에서 접수·처리한 민간부문 침해사고 통계를 분석한 결

과 웜·바이러스 신고건수는 총 8,469건으로 2007년(5,996건)에 비하여 41.2% 증가하였으며 해킹사고 접수·처리 건수는 총 15,940건으로 2007년(21,732건)에 비하여 26.7% 감소하였다.

3. 향후 전망

국가사회 시스템이 네트워크로 연결되고, 지식정보의 가치가 커지면서 정보보호가 국가경쟁력의 핵심요소로 자리 잡아가고 있는 반면, 국가기관·첨단기업의 중요자료 절취 시도, 해킹, 개인정보 유출 피해 등 인터넷 침해사고가 지속적으로 증가함에 따라 국민과 기업의 경제적 피해 및 심리적 불안뿐 아니라 국가 시스템의 마비 가능 등 정보위험사회로의 진입에 대한 우려 또한 확산되고 있다. 국가사이버안전센터, 인터넷침해대응센터 등의 사이버침해 신고처리 내용을 살펴볼 때 향후 사이버침해 전망은 다음과 같다.

첫째, 응용프로그램 취약점을 노리는 홈페이지 은닉 악성코드의 위협이 지속될 것이다. 2009년도에도 취약한 홈페이지를 통한 악성코드 은닉이 전파경로의 주요 수단으로 많이 이용되었으며 그 자체로서 악성행위를 수행하기 보다는 추가적인 악성코드를 다운로드하거나 생성하는 유형이 다수를 차지하였다. 이제 홈페이지 해킹은 악성코드 삽입, 홈페이지에서 관리하는 기업의 주요 정보, 개인정보 탈취 등을 위한 경유지 형태로 정착이 되었다. 특히 이러한 악성코드가 로컬 시스템에 설치된 소프트웨어(Flash, PDF, MS보안 취약점 등)의 취약점을 악용하는 사례가 50% 이상을 차지하는 것으로 나타났다. 이는 최근 인터넷을 통한 전자문서 교류나 멀티미디어 콘텐츠 사용이 급증하면서 해커들의 관심이 취약점에 대한 보안이 강화된 운영체제를 이용하기 보다는 다수의 사용자들이 보유하고 있는 소프트웨어에 대한 공격으로 전환될 수 있다는 점을 시사하고 있다.[228)]

둘째, 금전적 이익을 취득할 목적의 악성코드의 위협도 지속될 것이다. 기업을 대상으로 금전적인 이익을 목적으로 분산서비스거부공격 협박을 시도하고 이에 응하지

228) 국가정보보호백서 2010, 26-27쪽

않을 경우, 실제로 공격을 시도하는 사례가 2009년에도 다수 발생하였다. 이는 주로 고가의 DDoS(분산서비스거부, Distributed Denial of Service) 방어장비를 구축하기 어려운 기업을 대상으로 발생하고 있으며, 과거의 특정 형태의 사이트에 대한 공격에서 탈피하여 여행사, 호스팅 업체 등 일반 사업체를 대상으로 공격범위가 확대되고 있다. 이러한 분산서비스거부공격에는 넷봇(NetBot)을 이용하여 제작된 악성코드들이 많이 악용되고 있다. 최근에는 운용중인 게임 프리서버를 중심으로 보복성 공격이나 프리서버의 마스터로부터 아이템 유포를 요구하는 등의 DDoS 공격을 수행해주는 전문 카페들이 활성화되어 있어 네트워크상의 트래픽을 유발시키는 신고가 다수 접수 되었다. 특히, 7·7 DDoS 침해사고는 평소의 공격대상과는 다르게 주요 정부기관도 포함되어 있어, DDoS 공격이 기존의 금전적인 이득을 위한 단순공격에서 사회혼란을 유발시킬 수 있는 공격으로 변모될 수 있음을 보여주는 대표적 사례이다.[229]

셋째, 사회적인 이슈·이벤트를 악용한 악성코드의 유포이다. 2009년에는 마이클 잭슨 사망, 오바마 미국 대통령 당선, 전(前) 대통령들의 연이은 서거 등 국내·외적으로 사회적인 이슈가 많았으며, 이러한 사회적인 이슈는 악성코드 및 스팸 제작자들에게 더 없는 기회로 악용되어 발렌타인·화이트데이, 크리스마스 등 일련의 이벤트 등과 함께 인터넷 이용자를 현혹(사회공학적인 기법)시키기 위한 소재로 많이 악용되었다. 더불어 트위터, 페이스북 등 커뮤니티형 웹서비스인 소셜 네트워크(SNS, Social Network Service)를 통한 전파, 그리고 피싱사이트 및 합법적인 기관을 가장한 접속 유도 등의 방법으로 고도화되고 있는 실정이다.[230]

넷째, 분석지연을 위한 고도의 분석방해 기술의 접목이다. 7·7 DDoS 침해사고를 유발한 악성코드는 미리 정해진 시나리오를 기반으로 공격을 수행하는 형태로서 기존의 명령제어 서버(C&C, Command and Control) 접속 후 명령을 전달받는 유형에 비해 대응 및 조치가 어려웠다. 이와 같은 특정 시간에 정해진 악성행위를 수행하는 시한폭탄(Time-Bomb) 형태의 악성코드에서 적당한 공격 시점을 알아낸 후 대응하는 일련의 과정은 분석시간 지연을 유발시킬 수 있다. 또한 최근의 악성코드

229) 국가정보보호백서 2010, 27-28쪽

230) 국가정보보호백서 2010, 28쪽

는 여러 가지 악성행위를 포함하고 있으며 분석도구 우회, 가상머신 탐지, 압축(Packing) 적용 등을 통하여 분석을 어렵게 하고 있다.[231]

다섯째, 악성코드 대량생산을 위한 자동화된 도구의 이용이다. 최근 인터넷으로부터 악성코드 생산 시 기반이 될 수 있는 정보를 손쉽게 획득하여 이를 재배포 할 수 있는 기회가 많아졌다. 지난 11월 아이폰 악성코드가 한 달 사이에 3종이 발생한 것도 한때 최초 아이폰 악성코드의 소스코드가 공개되었던 것에 기인한 것으로 판단된다. 더불어 인터넷 전화감청 바이러스(Skype Trojan)도 공개된 적이 있어 향후 인터넷상의 무수한 악성코드 정보를 활용한 변종 발생 가능성이 높아지고 있다. 여기에 2008년 넷봇(NetBot)을 이용하여 DDoS 에이전트를 손쉽게 제작할 수 있는 도구의 상업적 판매에 이어 2009년에도 "풍운"이라는 DDoS 공격도구가 인터넷에 공개되어 분산서비스거부공격에 악용되었다. 위 두 가지 도구는 사용자 인터페이스(UI)를 제공하여 손쉽게 이용할 수 있는 기회를 제공하였고 기존의 악성코드 제작을 위해 소요되는 시간을 단축시켜 악성코드의 대량 생산이 가능한 환경을 조성한 대표적인 예라고 할 수 있다. 이로써 변종 악성코드의 출현 주기가 짧아져 이에 대한 대응에는 어려움이 있다고 할 수 있다.[232]

여섯째, 해외발 해킹 등 사이버침해의 증가이다. 온라인 게임 아이템을 사고 파는 문화적 특성, 마케팅을 위한 주민번호 수요가 많고, 시스템이 취약한 우리나라를 노린 해외발 해킹이 증가하고 있다. 특히 해외로부터의 해킹시도 중 중국발이 전체의 33%~53%를 차지한다. 중국 해커들이 이용하는 해킹 툴이 1,000개가 넘는 등 중국 해킹기술이 발전하고 있으며, 한국과 문화적 동질성이 있다는 점이 중국발 해킹의 증가 원인으로 보인다. 한편 한류(韓流)와 외국인과의 인적교류 등으로 중국 외 지역으로부터의 사이버침해 위협도 증가할 것으로 예상된다.

231) 앞의 쪽.

232) 국가정보보호백서 2010, 28-29쪽.

제2절 사이버안전에 관한 전문가인식

1. 조사 개요

가. 조사 목적

본 조사는 사이버안전에 대한 전문가들의 인식 전반에 대한 심층면접을 통하여 관련 정보(data)를 수집하여, 추후 본 내용과 관련 있는 조사 및 정책의 기초 자료를 제공하는데 목적이 있다. 이를 위하여 공공기관 및 민간기관의 사이버정보보안 실무책임자를 대상으로 하여 전문가 인식조사를 실시하였다.

다만 전문가인식조사는 당초 2년차 연구의 일환으로 계획되었던 국민의식조사의 사전조사 내지는 예비조사로서 실시하였기 때문에 설문조사보다는 심층면접조사의 기법을 활용하였다. 따라서 조사의 결과는 사이버정보보안 분야의 전문가인식을 참고하는 정도로 연구에 활용하면 족하며, 전문가 중 극히 일부에 편중된 조사이므로 이것이 전문가 전체의 의견이거나 국민일반의 의견이 아니라는 점을 미리 밝혀둔다.

나. 조사 설계

사이버안전에 관한 전문가인식조사는 공공기관 및 민간기관의 사이버정보보안 실무책임자를 대상으로 하여 2010년 11월중 2주간에 걸쳐 구조화된 설문지를 이용한 1:1 전문가 심층면접 인터뷰기법으로써 실시하였다. 대상자는 관련 협회원의 정보를 중심으로 하여 무작위로 선별하였고, 사이버보안 분야의 특수성을 감안하여 공공과 민간의 비율은 4:1로 정했다. 조사설계 및 조사실시는 조사전문기관인 (주)리서치21에서 담당하였다.

표 41 전문가 인식조사 설계표

조사 대상	사이버 안전에 대한 국가기관 및 민간 기관 전문가
조사 방법	구조화된 설문지를 이용한 1:1 전문가 심층 인터뷰 (In Depth Interview)
조사 규모	25명
조사 대상	사이버 안전에 대한 국가기관 및 민간 기관 전문가
조사 내용	1. '사이버안전' 및 '사이버위기'에 대한 용어의 인식 및 이해 2. 사이버 안전을 위협하는 위협요인 및 위협요인에 대한 사전 예방방안이나 사후 대응방안 3. 사이버 공격 또는 사이버 침해에 의한 국가기밀 유출 가능성 4. 외국과 우리나라의 인터넷 사이트 가입요건에서의 개인정보 유출 가능성 5. 사이버안전체계 구축이 필요하다면, 특정부처를 중심으로 한 강력한 중앙통제방식과 적정소관별 분산관리방식의 비교 6. 사이버위기 발생 시 가장 중요한 초동조치
조사 기간	2010년 11월 11일 ~ 11월 23일

다. 주요 설문내용

전문가 인식조사는 다음과 같은 6개의 화두와 15개의 주요 설문을 중심으로 진행되었다. 전문가의 보다 차원 높은 응답을 이끌어내기 위하여 설문에 대한 응답에는 가급적 그러한 응답을 하게 된 이유도 함께 밝히도록 하였다. 이러한 설문에 대한 구체적 응답내용은 비공개를 요구한 경우를 제외하고는 관련 후속연구의 기초자료로서 보다 활용될 수 있도록 〈부록 4〉에 따로 소개하였다.

표 42 **전문가 인식조사 주요 설문내용**

연번		설문내용
1	0	– ‘사이버안전’이란 말을 들어본 적 있는지? – 있다면, 어떤 의미로 이해하고 있는지? – 그렇다면 여기서 ‘안전’이란 어느 정도의 보호를 의미하는지? (정도 1 ~ 100%)
	1	흔히들 ‘사이버위기’라는 말도 자주 사용합니다. – 여기서 ‘사이버위기’란 말을 들어본 적 있는지? – 있다면, 어떤 의미로 이해하고 있는지? – 그렇다면 여기서 ‘위기’란 어느 정도의 침해 내지 위험성을 의미하는지? (정도 1~100%)
2	0	– 시스템 및 네트워크의 안전성 확보에 한하여 ‘사이버안전’이라고 이해한다면, 사이버 안전을 위협하는 위협요인으로 가장 중요한 것은? (대내 & 대외) – 그러한 요인이 왜 중요하게 다루어져야 하는지?
	1	– 그러한 중요 위협요인에 대한 사전 예방방안이나 사후 대응방안이 마련되어 있는지? (기술적 & 제도적) – 사전 예방방안이나 사후 대응방안이 마련되어 있지 않다면, 효과적인 방안으로 생각할 수 있는 것은?
	2	– 그러한 중요 위협요인에 대하여 형벌을 마련하거나, 현행보다 더욱 무겁게 처벌한다면 효과적일 것이라고 생각하는지? – 효과적이거나, 효과적이지 않다면 그 이유는? – 형벌이 효과적이려면 어떻게(또는 어느 정도로) 처벌해야 하는지?
3	0	– 사이버 공격 또는 사이버 침해에 의하여 국가기밀이 유출될 가능성이 일반적으로 보아 높은 수준인지? – 높다면(또는 낮다면) 그 이유는?
	1	– 사이버 공격 또는 사이버 침해에 의하여 개인정보가 유출될 가능성이 일반적으로 보아 높은 수준인지? – 높다면(또는 낮다면) 그 이유는?
	2	– 사이버 공격 또는 사이버 침해에 의하여 공공분야에서 국가기밀이 유출될 가능성이 높은지, 아니면 민간분야에서 개인정보가 유출될 가능성이 높은지? (양자 비교 요망) – 그 이유는?
	3	– 사이버 공격 또는 사이버 침해에 의한 공공분야의 국가기밀 유출과, 민간분야의 개인정보 유출 중에서 어느 쪽이 피해가 클 수 있다고 생각되는지? (양자 비교 요망) – 그 이유는?

연번		설문내용
4	0	외국사이트의 경우 가입요건으로 (본인이 직접 확인할 수 있는) 정확한 메일주소만을 요구하는 경우가 많습니다. 그래서 전자상거래를 제외하고는 개인정보 유출사고가 발생하기 어렵습니다. 반면 우리나라의 경우 악성댓글, 사이버모욕 등을 방지하기 위하여 인터넷실명제 또는 제한적 본인확인제를 실시함에 따라 가입시 주민등록번호와 같은 개인정보를 요구하는 경우가 많습니다. – 어느 경우가 더 안전하다고 생각하는지? 그 이유는? – 그리고 어느 경우가 더 바람직하다고 생각하는지? 그 이유는?
	1	– '건전한 인터넷문화 조성'과 '사이버 안전성 확보' 모두 중요한 가치이겠지만, 둘 중 무엇이 더 중요한 가치라고 생각하는지? – 그 이유는?
5	0	– 사이버안전체계 구축이 필요하다면, 특정부처를 중심으로 한 강력한 중앙통제방식과 적정소관별 분산관리방식 중 어느 경우가 더 효과적이라고 생각하는지? 그 이유는? – 강력한 중앙통제방식이 효과적이라고 한 경우 어느 부처를 중심으로 하는 것이 가장 효과적인지? 그 이유는?
	1	– 사이버안전체계 구축이 필요하다면, 특정부처를 중심으로 한 강력한 중앙통제방식과 적정소관별 분산관리방식 중 어느 경우가 더 바람직하다고 생각하는지? 그 이유는? – 강력한 중앙통제방식이 바람직하다고 한 경우 어느 부처를 중심으로 하는 것이 가장 바람직한지? 그 이유는?
	2	사이버 안전성 확보를 위하여 노력하는 정부부처로서 검찰청, 경찰청, 국가정보원, 국방부, 방송통신위원회, 법무부, 행정안전부 등이 있다면(가나다순. 열거하지 않은 부처도 포함 가능), – 이를 중요도 순서대로 나열하면? (3가지만)
6	0	– 사이버위기 발생 시 초동조치로서 가장 중요한 것은? – 그 이유는?

2. 사이버안전에 관한 전문가 인식조사의 주요 결과

가. '사이버안전' 및 '사이버위기'에 대한 용어의 인식 및 이해

'사이버안전' 또는 '사이버위기'란 말을 들어본 적이 있는지, 있다면 어떤 의미로 이해하고 있는지에 대해서 응답자 전원이 '사이버 위기'라는 말을 들어본 적이 있다고 응답하였다. '사이버위기'란 "시스템 및 네트워크를 통한 공격받을 가능성 및 공격으로 인해 피해를 입을 가능성이 있는 것(외부자의 공격)"(10명), "사이버 공간에서 국가·개인적 측면이나 권한이 없는 사람들에게 정보가 유출되는 것"(7명)의 의미로 이해하고 있다고 응답하였다. 그러나 '사이버안전'에 대해서는 일치되는 의견이 많지 않아 각자 이해하는 바가 다르다는 인상을 받았다. 이밖에 "사이버 테러, 인터

넷 루머, 비방, 시위 및 서비스 차단, 중지 위변조 등의 행위", "여러 가지 IT기술을 통해 일어날 수 있는 역기능", "해킹 바이러스 유포 등 시스템 제약을 가하는 부분 및 산업전반에 침투할 수 있는 국가적 위기"를 의미한다는 응답도 있었다.

그렇다면 여기서 '위기'란 어느 정도의 침해 내지 위험성을 의미하는지에 대해 응답자 중에 사이버 위기의 침해 내지 위험성은 "30% 정도"(3명), "50%"(3명), "60%"(3명), "80%"(3명), "90% 이상"(3명), "표현하기 어려움"(3명) 등으로 고르게 응답하였다. 이는 사이버위기의 판단을 위하여 실무계에서 통용되는 기준이 아직 없음을 나타내는 것이다.

나. 사이버 안전을 위협하는 위협요인 및 사전예방·사후대응 방안

시스템 및 네트워크의 안전성 확보에 한하여 '사이버안전'이라고 이해한다면, 사이버 안전을 위협하는 위협요인으로 가장 중요한 것은 무엇이라 생각하는가에 대해, 대내적으로는 응답자 중 7명이 "직원들이 정보를 빼돌리는 경우"라고 답했으며, "사람들의 잘못된 인식"(3명), "보완수칙을 지키지 않은 것"(4명) 등이 사이버 안전을 위협하는 위협요인이라고 답하였다. 대외적으로는 응답자의 15명이 "해커침입"이라고 응답하였고, "잘못된 시스템"(3명)이라는 응답도 있었다. 그 외에도 "정보유출"을 응답한 응답자도 있었다.

이러한 내용이 중요하게 다뤄져야 하는 이유로는 "정보 유출이 되면 안되므로"(12명)라는 응답이 가장 많았으며, "국가 및 기업의 주요 기능 마비"(4명) 때문이라는 응답도 적지 않았다. 기타 답변으로는 "사회의 큰 문제로 발전될 수 있다"는 응답도 있었다.

또한, 그러한 중요 위협요인에 대한 사전 예방방안이나 사후 대응방안이 마련되어 있는지에 대해 응답자 중 10명이 "제도적 방안"이 마련되어 있다고 응답하였고, 응답자의 11명이 "기술적 방안"이 마련되어 있다고 응답하였다. 만약 사전 예방방안이나 사후 대응방안이 마련되어 있지 않다고 가정할 때 효과적인 사전 예방방안이나 사후 대응방안으로는 "보안시스템 구축"(6명), "사이버 안전센터 구축"(6명), "보안지침 교육"(5명), "PC점검"(3명)으로 응답을 하였다.

그러한 중요 위협요인에 대하여 형벌을 마련하거나, 현행보다 더욱 무겁게 처벌한

다면 효과적일 것이라고 생각하는지에 대해 응답자의 12명이 “형벌이 효과가 있을 것이라고 생각해서”라고 응답하였고, “효과적이라고 생각하지 않음”(8명), “효과는 모르겠음”(5명)의 순으로 응답자들이 응답을 하였다. 형벌이 보다 효과적이려면 어떻게 처벌해야 하는지에 대해서는 응답자의 11명이 “의식수준을 높이는 게 필요하다”고 가장 많은 응답을 하였고, “현행보다 엄중한 형벌이 필요하다”(8명)는 응답도 많았다. 기타 응답으로는 “형벌의 세분화”, “인사 불이익 및 연봉감소” 등의 응답이 있었다.

다. 사이버 공격 또는 사이버 침해에 의한 국가기밀 유출 가능성

사이버 공격 또는 사이버 침해에 의하여 국가기밀이 유출될 가능성이 “높다고 생각한다”(14명), “외부적 공격에 유출될 가능성이 적다”(10명) 등으로 응답하였다.

외부적 공격에 유출될 가능성이 높다고 응답한 이유로는 “정보보호 마인드가 낮음”, “사이버침해 기술의 고도화” 순으로 응답을 하였으며, 유출된 가능성이 낮다고 응답한 이유로는 “외부의 공격에 대응하려는 시스템이 준비되어 있어서”, “인터넷망과 업무망이 분리되어 있어서”의 순으로 응답하였다.

사이버 공격 또는 사이버 침해에 의하여 개인정보가 유출될 가능성이 ‘높다’라고 응답한 응답자들은 그 이유에 대해 “보안시스템이 취약함”, “사용자의 개인 정보 요구”, “시스템화를 위한 투자가 현실적으로는 어려움” 등으로 응답하였고, ‘낮다’고 응답한 이유에 대해서는 “시스템적인 보호장치와 통제를 받고 있기 때문에”라고 응답을 하였다.

사이버공격 또는 사이버침해에 의하여 공공분야에서 국가기밀이 유출될 가능성이 높은지, 아니면 민간분야에서 개인정보가 유출될 가능성이 높은지에 대해 ‘공공분야가 더 유출될 가능성이 높다’라고 응답한 이유로는 “정보의 접근성이 용이함”, “공격 및 침해를 입었을 때 방지하는 시스템의 미비”, “개인정보 유출은 (이미) 많이 일어났으므로”로 총 3명의 응답자가 답하였다. ‘민간분야에서 개인정보가 유출될 가능성이 더 높다’고 응답한 이유로는 “공격 및 침해를 입었을 때 방지하는 시스템의 미비”, “보안에 취약한 업체 많음”, “시스템화를 위한 투자의 어려움”, “정보보호에 대한 의식 낮음” 등 기타 의견으로 21명의 응답자가 답하였다.

사이버공격 또는 사이버침해에 의한 공공분야의 국가기밀 유출과, 민간분야의 개

인정보 유출 중에서 어느 쪽이 피해가 클 수 있다고 생각되는지에 대해 '공공분야의 국가 기밀 유출의 피해가 더 클 것이다'고 응답한 이유로는 "국가정보 유출 피해 큼"(10명), "파급효과가 더 크다"(6명), "국가 위협과 연관되므로"(5명) 등으로 총 22명의 응답자가 답하였고, '민간분야의 개인정보 유출의 피해가 더 클 것이다'라고 응답한 이유로는 "공격 및 침해를 입었을 때 방지하는 시스템의 미비"(1명)로 응답하였다. '둘 다 비슷하다'는 응답자는 "피해의 기준에 따라 다르다"(2명)고 응답하였다.

라. 인터넷 사이트 가입 시 개인정보 유출 가능성

외국사이트의 경우 가입요건으로 본인인지 여부를 직접 확인할 수 있는 정확한 메일주소만을 요구하는 경우가 많아 전자상거래를 제외하고는 개인정보 유출사고가 발생하기 어려운 반면, 우리나라의 경우 악성댓글, 사이버모욕 등을 방지하기 위하여 인터넷실명제 또는 제한적 본인확인제를 실시함에 따라 가입 시 주민등록번호와 같은 개인정보를 요구하는 경우가 많은데, 이 둘 중 어느 경우가 더 안전하다고 생각하는지에 대해 '우리나라에 비해 외국이 더 안전하다'고 응답한 응답자는 15명, '외국에 비해 우리나라가 더 안전하다'고 응답한 사람은 12명, '비교가 불가능하다'는 응답이 2명이었다.

그 이유로서는 "외국의 간단한 정보가 더 안전하다"(12명)라고 응답을 하였고, '우리나라가 더 안전하다'라는 응답은 "메일을 통한 개인확인은 아직 어렵다"(3명), "본인확인 측면에서 주민등록번호가 필요하다"(3명)으로 응답을 하였고, '비교가 불가능하다'라고 응답한 이유로는 "외국은 주민등록번호가 없으므로 환경적인 측면이 다르기 때문에"라고 응답하였다. 그리고 어느 경우가 더 바람직하다고 생각하는지에 대해서는 "메일을 통한 본인 확인"(8명), "개인정보의 간소화"(5명), "PIN값 등을 이용한 회원가입"(4명)이 바람직하다고 응답을 하였다.

'건전한 인터넷문화 조성'과 '사이버 안전성 확보', 둘 중 무엇이 더 중요한 가치라고 생각하는지에 대해 '사이버안전성 확보가 더 중요한 가치이다', '건전한 인터넷 문화 조성이 더 중요한 가치이다'고 각각 11명씩 응답하였으며, '둘 다 중요하다'고 3명이 응답을 하였다. '사이버 안전성 확보가 더 중요한 가치이다'라고 응답한 이유로는 "사이버 안전성을 확보해야 건전한 인터넷 문화가 조성될 수 있을 것이므로"(5

명)라는 응답이 가장 많이 나왔으며, '건전한 인터넷문화 조성이 더 중요한 가치이다'라고 응답한 이유로는 "건전한 문화가 조성되면 인터넷 사용에 문제가 없을 것"(3명), "건전한 인터넷 문화가 조성되면 자연스럽게 사이버안전이 확보가 될 것이며 안전할 것이다"(2명), "건전한 문화가 형성되면 여러 가지 부작용이 해소될 것이므로"(2명)의 순으로 응답하였다. 4-0 설문과 4-1 설문은 서로 대응하는 설문으로서 주민등록번호 활용 필요성을 묻는 설문이다.

마. 사이버안전체계 구축 시 중앙통제방식과 분산관리방식의 비교

사이버안전체계 구축이 필요하다면, 특정부처를 중심으로 한 강력한 중앙통제방식과 적정소관별 분산관리방식 중 어느 경우가 더 효과적이라고 생각하는지에 대해서 '강력한 중앙통제방식이 더 효과적이다'(11명), '적정소관별 분산관리'(9명), '혼합형'(5명)으로 응답을 하였다.

'중앙통제방식이 더 효과적이다'라고 응답한 이유로는 "중앙에서 통제 및 관리를 하는 것이 효과적일 것 같다"(4명), "비용적인 문제에서"(2명), "일관성 있게 특정기관에서 중심되어야 함"(2명)의 순으로 응답하였다.

'적정 소관별 분산관리가 더 효과적이다'라고 응답한 이유로는 "각 분야별로 관리하는 것이 효과적"(2명), "중앙에서 통제하면 각 분야의 특성에 맞는 관리 및 통제가 어려움"(2명), "통제 시스템이 특정하게 드러나면 사이버 침해의 주요 표적이 될 수 있음"(2명) 등으로 응답하였고, '혼합형'은 "중앙통제방식 밑에 적정소관별 관리통제방식 병행"(4명)과 "인력 및 전문성을 다 확보하기 어렵기 때문에 각기 특성에 맞게 관리가 효과적"(1명)이라고 응답하였다.

사이버안전체계 구축이 필요하다면, 특정부처를 중심으로 한 강력한 중앙통제방식과 적정소관별 분산관리방식 중 어느 경우가 더 바람직하다고 생각하는지에 대해 '특정부처를 중심으로 한 강력한 중앙통제방식이 더 바람직하다'고 응답자 중 10명이 응답하였다. 그리고 특정부처로는 "국가정보원"(5명), "행정안전부"(2명), 기타의 순으로 응답하였다. '사이버 안전성 확보를 위하여 노력하는 정부부처'를 중요도 순서대로 선택하게 한 질문에 대해서는 '국가정보원'이 1순위로 22명의 응답자가 선택하였고, '행정안전부'(20명), '방송통신위원회'(14명), '경찰청'(10명)의 순으로 응답하

였다.

일부 전문가, 특히 공공기관 종사자를 대상으로 한 인식조사이기 때문에 5번 설문의 조사결과에 큰 의미를 부여할 필요는 없다. 또한, 정부 조직구조는 가변적이기 때문에 현행 체제를 고수할 필요는 없으며, 동일한 설문을 국민의식조사에 반영할 경우 전혀 다른 결과가 도출될 수 있다. 더욱이 중앙통제방식을 도입할 경우 특정 행정부처보다는 청와대나 국무총리실의 역할이 보다 중요해질 것이기 때문에 행정부처 간의 선호도 분석에 큰 의미를 부여할 필요도 없다. 다만 공공기관의 사이버정보보안 사무에 국가정보원이 상당 부분 관여해왔다는 점을 감안할 때 공공기관 사이버보안 실무자들은 사이버정보보안 분야에 대한 국가정보원의 기여도와 노력을 어느 정도 인정해주고 있는 것으로 추정할 수 있다.

바. 사이버위기 발생 시 가장 중요한 초동조치

사이버위기 발생 시 가장 중요한 초동조치로 '긴급 전파'(또는 정보공유)(10명)가 필요하다고 응답한 응답자가 많았으며, 그 이유로는 "확산 방지 차원(대응체계 구축)에서"(4명), "대응 체계 구축"(3명), "원인분석을 통한 원인 파악(자료 확보)이 필요함"(3명)이라고 응답하였다.

3. 전문가 인식조사의 시사점

이상과 같이 전문가 인식조사 결과를 살펴보았는데, 표본 자체가 크지 않고 응답자의 주관이 상당히 개입되어 있으며 공공기관 종사자에 편중된 결과이기 때문에 이것이 곧 '전문가그룹의 다수의견'이라고는 말하기 어렵다. 그래서 이 연구에 있어서도 이들 의견은 참고사항으로만 활용할 뿐이지 전적으로 수용하지는 않았다. 그러나 우리나라 주요 기관의 사이버정보보안 실무책임자를 면접한 결과이기 때문에 우리나라 사이버안전정책의 결정에 소용될 만한 내용이 있을 것이라고 판단된다. 특히 개개의 의견에는 응답자의 주관이 상당 부분 개입되어 있지만, 전체를 일관하는 공통분모 또는 조사과정에서 확인할 수 있던 사항 등은 하나의 '시사점'으로서 참고할

만한 가치가 있을 것이다.

가. 사이버위기 판단기준의 미비

어떤 사안들을 종합하여 '안전하다', '안전하지 않다', 더 나아가 '위기에 처했다'라는 판단은 누구라도 쉽지 않을 것이다. 더욱이 이러한 판단을 내릴 책임이 있는 입장에서는 더욱 그러할 것이다. 그러다 보니 큰일이 아닌데도 '위기'라고 호도하여 불요불급한 업무 마비와 구성원의 불편만을 초래할 수도 있고, 정작 위기상황을 미리 예측하지 못하여 낭패를 볼 수도 있을 것이다. 이는 굳이 사이버안전에 국한되는 문제는 아니기 때문에 어느 분야라도 사정은 크게 다르지 않을 것이다.

물론 이러한 사정은 사이버안전 관련 개념 이해도를 확인하기 위한 〈설문 1〉의 조사결과에서도 그대로 드러난다. 예컨대 '사이버안전' 및 '사이버위기'는, 어쩌면 '동전의 양면'이라고 할 수도 있는 상호 밀접한 개념임에도 불구하고 전문가그룹의 대부분은 전혀 별개의 의미로 이해하고 있고, 안전도나 위험도를 판단할 수 있는 일관된 기준을 제시하지 못하고 있다고 판단되었다.

이는 실무상 '안전'이나 '위기'를 판단할 구체적 기준이 아직 존재하지 않는 것으로 이해할 수 있는데, 이러한 판단기준이 제대로 마련되지 못한다면 사소한 불안요소의 출현에 범국가적인 대응시스템이 가동되어 불요불급한 행정낭비 내지 국력낭비를 초래할 수도 있다. 그렇기 때문에 적어도 어느 정도를 안전하다고 할 것인지, 또는 어느 정도를 위기라고 할 것인지 정도는 그 판단기준을 정할 필요가 있고, 이를 위해서는 사이버안전 또는 사이버위기와 관련된 지표를 개발하여 안전도 내지 위험도를 가능한 한 계량화할 필요가 있다.

나. 형벌효과에 대한 막연한 인식

사이버침해나 사이버공격의 경우 시스템과 네트워크를 교란하기 때문에 이에 대한 사전예방이나 사후대응이 중요하다. 사후대응 역시 '수사'와 '문책'보다는 '방어'와 '복구'에 보다 무게가 실리는 것도 당연할 것이다. 〈설문 2〉에 대한 전문가들의 인식 역시 관련 시스템이나 제도에 관한 사항에 초점을 맞추고 있다고 판단된다. 형

벌의 최후수단성을 굳이 논하지 않더라도 형벌을 효과적인 대안으로 제시한 경우는 없었고, 행위자를 체포하여 엄벌한다고 하여 '방어'와 '복구'의 효과가 발생하는 것도 아니다.

하지만 행위자를 추적하여 색출하고 이를 법에 따라 처벌하는 것은 재발방지를 위해서는 중요하다. 다만 사이버안전 분야의 특성상 '방어'와 '복구'에 치중하느라 행위자를 추적하지 못하거나 증인 및 증거를 확보하지 못한 경우가 적지 않아 실제로 처벌되는 경우가 많지 않을 뿐이지 사이버침해 또는 사이버공격에 대응해서는 앞서 살펴본 바와 같이 이미 엄중한 형벌체계를 갖추고 있다. 결국 우선순위의 차이일 뿐이지 이것만으로 곧 형벌이 효과 있거나 없음을 판단하기는 어려울 것이다.

그런데 〈설문 4-3〉에 대하여 응답자의 다수(12명)는 형벌이 효과 있을 것이라고 응답하였고, 이 중 8명은 현행보다 엄중한 형벌이 필요하다고 인식하고 있었다. 그러나 형의 경중을 불문하고 형벌제도 자체가 전문가들이 인식하는 효과적인 사후대응수단에 포함되지 못하는 만큼 가중처벌이 필요하다는 응답 자체를 신뢰하기 어렵고, 현행 형벌제도조차 충분히 활용되지 못하는 상황에서 중형(重刑)의 효과성은 더욱 신뢰하기 어려울 것이다. 따라서 형벌효과에 대해서는 그 존부를 단언할 수 없으나, 적어도 전문가들이 인식하는 가장 효과적인 대응수단은 아니라고 결론지을 수 있을 것이다.

다. 민간분야 정보보안시스템 구축의 한계 노정

사이버침해 내지 사이버공격은 시스템 또는 네트워크 자체의 교란을 목적으로 하는 경우도 많지만, 시스템 또는 네트워크에서 관리하는 고급정보를 대상으로 하는 경우도 많다. 이러한 고급정보로는 공공분야에서는 국가기밀이 대표적일 것이고, 민간분야에서는 개인정보와 영업비밀을 생각해볼 수 있을 것이다. 〈설문 3〉은 고급정보 중 어느 쪽이 사이버침해나 사이버공격에 취약한 것인지를 묻는 질문이다.

이에 대하여 전문가의 대부분은 민간분야의 개인정보 유출 쪽이 공공분야의 국가기밀 유출 쪽보다 취약하다는 인식을 가지고 있었다. 그 이유로는 민간분야의 경우 정보보안에 투자하지 않거나 이에 대한 인식이 부족하다는 의견을 제시하였다. 상식적으로 판단하더라도 기업이 영리를 추구하는 것은 당연한 것이고, 일부 기업을 제

외하고는 전자상거래에 종사하는 대부분의 기업이 영세하다는 점을 감안하면 영리를 추구하는 기업의 속성상 이윤창출과는 거리가 있는 고비용의 정보보안시스템 구축에 투자하기를 기대하는 것은 다소 무리가 있다.

그래서 민간분야의 정보보안시스템이 공공분야의 정보보안시스템보다 취약한 것은 필연적일 수밖에 없고, 어떠한 강제수단을 동원하더라도 이러한 한계를 극복하기란 간단치 않을 것이라고 생각한다. 따라서 정책설계에 있어서도 기업의 투자부담에 대한 고려가 필요하다고 생각한다.

라. 본인확인제도의 역기능 완화 필요

악성댓글, 사이버모욕 등을 방지하고 건전한 인터넷문화를 조성한다는 명분으로 마련되었던 인터넷 실명제와 본인확인제 등은 반세기 가까이 시행되어 온 우리나라의 주민등록제도를 배경으로 한다. 대한민국 내에 거주하는 우리나라 국민인 이상 누구라도 주민등록번호가 부여되어 있기 때문에 이용자의 실지명의와 주민등록번호의 대조만으로 손쉽게 본인확인이 가능하기 때문이다. 또한, 우리나라가 다른 어떤 나라보다도 빠르게 전자상거래가 발전할 수 있었던 것도 주민등록번호라는 강력한 본인확인 수단의 존재를 배경으로 한다.

그런데 우리나라에서 주민등록번호는 사이트 회원가입이나 전자상거래뿐만 아니라 거의 모든 법률관계에서 본인확인을 위한 가장 기본적인 정보로서의 역할을 수행해 왔기 때문에 실명과 주민등록번호만 가지고 있다면 할 수 있는 일이 의외로 많다. 그래서 몇 가지 개인정보만 더 수집하여 조합한다면 사이버공간뿐만 아니라 현실에서도 본인 행세가 그다지 어렵지 않게 된다. 따라서 범죄를 획책하는 무리들이 주민등록번호 등의 개인정보 수집에 관심을 갖게 되는 것은 누구라도 짐작할 수 있을 것이다. 실제로 IDC는 세계적으로 개인정보 암거래 시장이 2005년 7억 1,400만 달러에서 2010년 16억 달러에 이를 것으로 예측하고 있을 정도로 현재 인터넷상의 개인정보 노출에 따른 경제적 피해가 엄청나며, 향후 그 규모가 더 커질 것으로 예상된다.[233] 그런데도 우리나라 대부분의 사이트는 회원가입 시에 주민등록번호 등 개인

233) 정교일 외, 훤히 보이는 정보보호, 전자신문사, 2008, 221쪽.

정보를 요구하고 있고, 정부는 인터넷실명제 등을 명분으로 하여 이러한 환경을 더욱 조장하고 있다.

그래서 주민등록번호 수집과 관련한 이러한 문제들에 대한 전문가그룹의 인식을 조사하기 위하여 〈설문 4〉가 제공되었고, 조사에 응한 전문가그룹의 과반수 내지 그 이상은 이러한 문제에 대한 근본대책이 필요함을 어느 정도 공감하고 있다고 판단된다.

제6장

사이버안전체계의 구축 방안

06 사이버안전체계의 구축방안

제1절 사이버안전체계 구축의 기본방향

1. 문제의 소재

이상과 같이 사이버안전, 사이버침해, 사이버공격 등과 관련하여 이를 유형별로, 또는 소관부처별로, 국가별로 살펴보았고, 제도적인 측면과 현상적인 측면으로도 나누어보았다. 이를 통하여 개별 연구진이 도출한 문제점과 대안은 다음과 같다.

분류이론을 바탕으로 유형별 고찰을 시도한 박영우 전문위원은 사이버전이 발발할 경우 이에 대응할 수 있는 교전수칙이 미흡하고, 적의 서버 및 기반시설에 대한 원천지 대응 근거규정이 부족함을 지적하는 한편, 근원지, 동기, 대상 등을 명확히 밝힐 수 있는 국제조약 내지 국제협약 등을 마련하기 위한 노력이 지속되어야 함을 문제제기하였다. 또한, 공공 및 민간부문에서 발생하는 침해사고의 대부분이 민간의 홈페이지 및 개인PC의 취약점을 이용하기 때문에 민간부문의 정보보호에 대한 투자 및 인력확보가 필요함을 역설하였다.[234]

234) 이 글, 제2장 제3절 '사이버침해 유형별 대응전략 개관' 참조.

또한, 박 위원은 국가통계를 바탕으로 유형별, 분야별 안전실태를 점검하는 과정에서 향후 응용프로그램의 취약점을 노리는 홈페이지 은닉 악성코드 및 금전적 이득 취득 목적의 악성코드에 의한 위협이 여전히 지속될 것으로 판단하는 한편, 마이클 잭슨 사망, 오바마 대통령 당선 등 사회적 이슈·이벤트를 악용한 악성코드 유포 가능성이 높아질 것으로 전망하였다. 또한, 미리 정해진 시나리오에 따라 공격한 7·7 DDoS 침해사고와 같이 분석지연을 위한 고도의 분석방해 기술을 접목하거나 악성코드의 대량생산을 위하여 자동화된 도구를 이용하는 경우도 증가할 것으로 예측하였다. 해외발 사이버침해의 경우도 한류(韓流)와 같은 외국과의 문화교류가 증가함에 따라 사이버침해 위협도 함께 증가할 것으로 예측하였다.[235]

사이버안전 관련 법제를 분석한 윤해성 부연구위원은 사이버침해의 외연이 1995년 형법개정 당시 예상했던 수준을 넘어서서 사이버테러, 사이버전 개념까지 확장되면서 내란, 외환죄와 관련한 종래의 형법해석론이 한계에 직면했음을 지적하는 한편, 교통방해, 일수 등 공공안전과 관련해서도 새로운 해석이 필요함을 지적하였다.[236]

국가사이버안전센터를 중심으로 하여 국가정보원의 사이버침해 대응체계 현황을 분석한 김민호 교수와 실무연구진은 사이버안전 관련 법제정비 및 사이버공격에 대응한 위기관리체계 구축의 필요성을 지적하였다. 이들은 법제정비와 관련해서는 대응활동의 중심역할 수행을 위한 조직·체계의 법적 지위 확보, 관련기관 간 정보공유 및 예·경보체계 관련 법제 정비, 중장기적 관점에서의 연구 및 이를 위한 예산 지원, 고도의 숙련된 전문인력 확보를 위한 노력, 실질적 국제협력 강화의 필요성 등을 제기하였고, 위기관리체계 구축과 관련해서는 컨트롤타워(control tower)의 구축 및 구체적 절차 정립의 필요성을 제기하였다.[237]

방송통신위원회의 사이버침해 대응체계 현황을 분석한 권헌영 교수는 정보화만큼 정보보호도 중요한 이슈이므로 이에 대한 정비와 조정이 필요하며, 국가안보를 중심으로 하는 정보보안과 전자정부, 전자상거래 등 일반분야의 정보보호는 그 정책목표와 내용이 다르기 때문에 정책 역시 차별화되어야 한다는 전제에서 국가 전체의 정

235) 이 글, 제5장 제1절 3. '향후 전망' 참조.
236) 이 글, 제3장 제1절 2. '사이버안전 관련 처벌규정' 참조.
237) 이 글, 제3장 제2절 5. '향후 과제' 참조.

보보호정책체계를 바로세우기 위해서는 대통령실에서 직접 지휘할 수 있는 종합지휘감독체계를 중심으로 하여 부처간 협의회에 부처별 역할을 정리할 필요가 있음을 역설하였다.[238]

경찰청의 사이버침해 대응체계와 사이버침해 대응 국제협력체계 현황을 분석한 김기범 경감은 사이버공격이 국가안보에 대한 위협이 될 수 있다는 가능성만으로 사이버공격에 대한 사전·사후적 대응 전부를 국가안보 차원에서 접근하는 것은 적절하지 못하고 중요 사이버위기 위기 시에 정보보안 담당부처가 이를 사전에 탐지하지 못했던 사실을 지적하면서 경찰청의 사이버 수사체계를 사후 추적수사에서 사전탐지 및 조기대응 체제로 전환할 필요가 있음을 주장하였다. 특히 사이버침해 초동수사의 중요성을 강조하며, 유관기관간 사이버침해 초동조치에 있어 협력 강화 필요성을 제기하였다. 또한, 김 경감은 사이버범죄 수사 대응 및 대응 관련 법규 정비 필요성을 제기하는 한편, 주요 기반시설 사이버침해 피해에 대한 수사기관 고발 의무화와 한국인터넷진흥원의 WHOIS 정보 정확성 제고의 필요성을 제기하였으며, 이 밖에도 전담조직 위상 강화, 민간 IT전문가 경찰관 특채 확대, 사이버테러 전문수사관 양성 등 사이버수사 전담조직 및 전문성 확보방안, 사이버치안 거버넌스 강화 등 유관기관 및 민간분야 협력방안, 사이버범죄 예방에 관한 수익자 부담원칙 도입방안, 국제정보공조 활성화 등 국제협력 및 공조수사 역량 확충방안 등을 제안하였다.[239]

미국, 영국, 독일, 프랑스, 일본 등 주요 국가의 사이버공격 대응체계 현황을 분석한 김도승 부연구위원은 사이버공격을 국가의 중대 위협요인으로 인식하고 가장 활발하게 대응체계를 구축하고 미국의 사례를 모범사례로 제시하면서, 우리나라의 경우 책임과 권한이 여러 부처에 분산됨에 따라 발생하는 정책의 혼선을 지양하기 위해서는 기관간 협력체계를 뒷받침할 법체계를 마련할 필요가 있음을 주장하는 한편, 침해사고 발생 유무에 관계없이 꾸준하게 정보보호 예산에 투자하는 미국과 달리 사고발생 후 일회성 예산 투자가 이루어지는 우리나라의 현실을 지적하면서 관련 예산 확보 등 국가사이버보안 R&D 정책을 강화할 필요가 있음을 역설하였다. 또한, 김 위원은 국제테러주직들조차 전세계적인 테러 네트워크를 구축하고 점조직화하는 현

238) 이 글, 제3장 제3절 5. '분석 및 평가' 참조.

239) 이 글, 제3장 제4절 5. '평가 및 개선방안' 및 제5절 4. '평가 및 개선방안' 참조.

실을 지적하면서 국내·국제적 대테러 네트워크 구축 및 관련 법제도 정비 필요성을 제기하였다.[240]

공공기관 정보보안실무자를 대상으로 전문가 인식조사를 수행한 조사결과를 분석한 강석구 연구위원은 '안전' 또는 '위기'에 대한 판단에 오류가 있을 경우 불요불급한 업무 마비와 사회구성원의 불편, 나아가 국민의 불안감을 증폭하거나 국력낭비만을 초래할 우려가 있음에도 실무상 '안전'이나 '위기'를 판단할 구체적 기준이 미흡하다는 사실을 지적하는 한편, 영리를 추구하는 기업의 속성상 민간기업이 이윤창출과 거리가 있는 고비용의 정보보안시스템을 제대로 구축하기란 현실적으로 무리가 있으므로 정책설계에 있어 기업의 투자부담에 대한 고려 필요성을 제기하였다. 또한, 민간분야 정보보호가 취약할 수밖에 없는 현실에서 인터넷실명제 등 본인확인제의 확대는 사이버안전을 위협하는 환경을 더욱 조장할 뿐이므로 이에 대한 근본대책이 필요한 점과, 법제도를 정비함에 있어 흔히 제기되는 사이버침해행위에 대한 가중처벌방안은 그 효과도 의문이지만 전문가들이 인식하는 가장 효과적인 대응수단도 아니라는 점을 지적하였다.[241]

종합적인 대안으로서의 '사이버위험 관리체계 구축방안'은 후술하겠지만, 이상과 같이 연구진 각자의 역할분담에 따라 발굴해낸 문제점과 대안을 사이버안전정책 수립의 기초자료로서 소개하였다. 이하에서는 사이버안전정책 수립에 있어서의 주요 쟁점과 고려하여야 할 현실적 한계에 관하여 기술하고자 한다.

2. 사이버안전정책 수립의 주요 쟁점

살펴본 바와 같이 사이버안전체계의 구축과 관련해서는 수개월간 함께 연구해온 연구진 간에도 생각이 다르고, 시각의 차이가 있다. 그래서 이를 통일적인 대안으로 종합하여 제시하기에는 다소 무리가 있기 때문에 일단 공통분모 내지는 공통관심사를 중심으로 사이버안전정책 수립을 위한 주요 쟁점을 이끌어내어 정리해보았다.

240) 이 글, 제4장 제6절 '비교법적 고찰의 시사점' 참조.

241) 이 글, 제5장 제2절 3. '전문가 인식조사의 시사점' 참조.

첫째, 국가안보와 직결된 보다 높은 수준의 위험에 대해서는 중앙통제방식이 적절하다고 판단된다. 다만 이를 준전시상황으로 보아야 할지, 위기상황으로 보아야 할지, 재난상황으로 보아야 할지에 대해서는 보다 논의할 필요가 있다. 경우에 따라 중심기관이 다를 수 있기 때문이다.

둘째, 위기에 이르지 않는 위험 또는 일상적인 위험에 대해서는 분산관리방식이 적절하다고 판단된다. 다만 어느 기관이 어떤 역할과 기능을 분담해야 할지는 보다 논의가 필요하고, 어느 정도를 '안전' 또는 '위기'라고 판단할지 그 구체적 기준 마련에 대해서도 연구가 필요하다.

셋째, 사이버안전 문제는 민간분야와의 협력이 필요한 사안이라고 판단된다. 나아가 국가 간의 협력도 중요하다고 판단된다. 다만 민간분야와 협력해야 할 경우 경제적 부담 및 상황인식의 차이를 고려해야 할 것이며, 국가 간의 협력의 경우 실효성 확보를 위한 고민이 요구된다.

넷째, 사이버안전을 확보하기 위해서는 정보화정책과 정보보안정책 간의 차별성 확보 및 인터넷건전성과 사이버안전성이라는 상반된 가치의 조화가 필요하다고 판단된다. 다만 양자를 모두 규제하는 것은 적절치 않으므로 어느 쪽을 규제하고 자율에 맡길지에 대한 논의가 필요하다.

다섯째, 사이버수사의 실효성을 확보하기 위해서는 초동수사의 실효성을 확보하는 것이 가장 중요하고, 이를 위해서는 초동수사의 관할을 현실에 부합되게 조정할 필요가 있다고 판단된다. 다만 사이버공격의 경우 '수사'보다는 '방어'와 '피해복구'가 우선할 수 있다는 점에 유의해야 한다.

여섯째, 사이버안전 관련 조직과 인력, 권한과 예산을 조정할 필요가 있다고 판단된다. 이를 위해서는 법제 정비가 필요할 수 있다. 다만 무조건적인 확대 내지 행정권한 강화는 적절하지 못하다고 판단되며, 보안기술 개발과 같은 공공인프라 구축에 지원이 집중될 필요가 있다.

이상과 같은 주요 쟁점을 고려하여 사이버안전체계를 구축해야 할 것이고, 그 구체적인 대안을 다음 절에서 제시하고자 한다. 다만 실효적인 사이버안전 정책 수립을 위해서는 후술하는 사이버안전 문제를 둘러싼 현실적 한계도 함께 고려해야 할 것이다.

3. 사이버안전정책 수립의 현실적 한계

사이버안전 문제는 과학기술 및 통신환경의 급격한 변화에 따라 21세기 들어 부각된 사안이고 여전히 제반 환경이 급변하는 분야이기 때문에 사이버안전 분야의 정책결정자는 최신기술과 동향을 따라잡지 못한 경우가 적지 않을 것이고, 그것은 이 연구를 수행한 연구진의 경우도 예외가 아니다. 그렇기 때문에 피상적이거나 도식적인, 그래서 현실과 동떨어진 결론을 도출할 가능성이 크기 때문에 다른 정책분야보다 고민의 폭이 클 수밖에 없다. 이러한 현실적 한계로서 고려할 만한 사항은 다음과 같다.

가. 정보통신 및 정보저장 방식의 급변 및 다변화

종래 인터넷 위주의 정보통신 방식이 최근 모바일, WiFi, DMB, 블루투스 등으로 다변화하는 추세이며, 이에 따라 사이버공격 경로도 다변화되어 종래 인터넷 위주의 정보보안정책은 한계에 봉착할 수밖에 없다. 또한, 종래 하드디스켓, USB 위주의 정보저장 방식 역시 메일, 웹하드, 웹드라이버, SD카드, Micro SD 카드 등으로 다변화하는 추세이기 때문에 종래 USB 위주의 보안정책도 한계에 봉착했다고 판단할 수밖에 없다.

특히 향후 모바일 또는 블루투스 방식의 정보교환이 일반화될 것을 감안한다면 공공PC 역시 이들 방식에 개발될 수밖에 없고, 이와 같이 공공분야의 정보환경이 변화할 경우 현재 공공분야에 적용되는 USB 위주의 통제적 보안정책은 정보유출에 무력할 뿐만 아니라 공공분야의 의사소통에 저해요인으로 남을 수밖에 없을 것이다.

나. 정보보안의 기술적·경제적 한계

인터넷사이트에 회원가입할 경우 이메일주소 등 단순한 개인정보만을 요구하는 외국과 달리 우리나라의 경우 주민등록번호, 휴대전화번호, 주소 등 법률관계와 직결된 민감한 개인정보를 요구하는 경우가 많다. 따라서 이에 따라 외국의 경우보다 높은 수준의 보안기술이 요구되나, 보안기술의 발전속도는 필연적으로 정보통신기술의 발전속도를 따라가지 못할 수밖에 없으므로 어떠한 보안대책에 의하더라도 정보

유출 시 피해규모가 심각할 수밖에 없고, 이러한 환경변화에 대응하려면 더 많은 비용, 시간, 예산, 인력 부담을 감수해야 할 수밖에 없다.

또한, DDoS(서비스분산) 공격의 경우 공격에 비례하여 네트워크 대역폭을 늘리거나 서버를 분산시키는 임시방편 외에는 원천적 방어기술을 아직 확보하지 못한 상태이므로 DDoS 공격에 대한 효과적 방어기술을 개발하지 못하는 한, 사이버안전체계 구축 등 제도 개선만으로는 대응에 한계가 있을 수밖에 없다. 나아가 DDoS 공격의 경유지로 활용되는 좀비(악성코드 감염) PC의 치료를 위해서는 이용자의 협조가 필요하나, 인권옹호를 별론으로 하더라도 그 많은 PC의 이용자를 파악하여 협조요청하는 것은 현실적으로 무리가 따를 수밖에 없다.

다. 사이버공격 추적·수사의 한계

사이버공격의 경우 '수사'보다는 '방어'와 '피해복구'가 우선할 수 없다는 점을 별론으로 하더라도, 장소적 제약을 받지 않는 네트워크의 특성에 따라 해킹, 웜·바이러스, DDoS 공격 등의 발원지 내지 경유지 추적이 어려울 수밖에 없고, 특히 기관(수사기관, 국방부, 국가정보원 등) 간의 업무관할에 따라 해외발 공격의 경우 관할 소재가 명확해질 때까지 경찰청 등 수사기관의 즉시대응이 더욱 어려워질 수밖에 없다. 또한, 수사개시를 위해서는 범죄구성요건 위반, 피해발생 등 범죄혐의 확인이 필요하나, 초동수사 지연에 따라 범인 추적, 증거 확보 실패가능성이 높을 수밖에 없다. 나아가 공격세력 추적·수사에 실패하여 이들을 색출해내지 못할 경우 재발가능성도 증가할 수밖에 없다.

한편, 수사기관의 경우 수사기술에 우위를 가지고는 있으나, 보안기술에 대한 전문성은 타 기관에 비하여 취약할 수밖에 없으므로 전문성을 확보한 타 기관의 협조도 고려해야 할 것이다.

제2절 사이버위험 관리방안

1. 사이버위험 관리체계 설계의 전제조건

가. 사이버위험의 측정가능성

먼저 '사이버위험'이란 용어는 학계나 실무에서 통용되는 용어가 아니라 사이버안전체계 구축방안 도출을 위하여 임의로 만들어낸 연구목적의 용어란 점을 미리 밝힌다. 이 글에서 '사이버위험'이란 '사이버안전'에 대비되는 개념으로서, 사이버침해 또는 사이버공격에 의하여 발생할 수 있는 위험 또는 그 정도를 의미한다고 이해하면 될 것이다.[242] 사이버위험은 양(量)과 질(質)로 나타낼 수 있기 때문에 그 정도인 '위험도'로도 표현할 수 있고, 사이버위험도는 사이버안전도와 서로 대응하는 개념이 된다. 따라서 사이버위험도를 측정하기 위해서는 '사이버위험'의 측면으로 접근하여도 되지만, '사이버안전'의 측면으로 접근하여도 무방하다.

하지만 어느 쪽으로 접근하건 간에 사이버위험도를 측정할 수 있어야만 위험도를 기준으로 사이버위험을 구분할 수 있다. 만일 사이버위험을 위험도에 따라 객관적으로 구분해낼 수 없다면 그다지 위험도가 높지 않은 사안에 대하여 범국가적인 대응을 하여 국력을 낭비하거나, 위험도가 매우 높은 사안을 간과하여 국가적인 위기를 초래할 수 있기 때문에 사이버위험의 측정가능성은 매우 중요한 사안이 된다. 또한, 사이버위험을 분류할 수 있어야만 위험도에 따른 차별적 대응이 가능하게 되고, 후술하는 '사이버위험 관리방안'이 의미를 가질 수 있을 것이다.

참고로, 사이버위협 수준에 따른 단계적 경보발령체계는 이미 시행되고 있다.[243] 다만 여기서 말하는 '위험도', '국가적 차원', '전국적', '대규모', '다수', '일부', '장애', '우려' 등의 개념이 지나치게 추상적이고 포괄적이어서 이러한 기준이 실무에서 제대로 활용되고 있는지 의문이 아닐 수 없다. 그래서 사이버안전 또는 사이버위험의 정도를 객관적으로 측정할 수 있는 도구가 아직까지는 충분히 개발되지 못하였다

242) 이 연구에서 사이버위기나 사이버안전성과 같이 학계나 실무계에서 통용되는 용어를 굳이 활용하지 않은 것은 이들 개념에는 이미 다른 목적의 가치가 포함되어 있어 오해의 소지가 있기 때문이다.

243) 이 글, 제3장 제2절 2. 나. '예·경보 발령 및 전파' 참조.

고 추정할 수밖에 없다.

결국 일정 수준 이상의 사이버위험에 한하여 범국가적인 위험관리체계를 가동시키고자 한다면, 이에 앞서 사이버위험도를 측정할 수 있는 객관적 도구부터 개발하여야 할 것이다. 다만 이 연구는 법학적 방법론을 바탕으로 하기 때문에 사이버위험도와 같이 계량적이고도 전문적인 결과물을 도출하기에는 적절치 않으므로 사이버안전지표 개발 등 사이버위험도 측정과 관련한 사항은 향후 다른 분야의 연구과제로 수행할 필요가 있을 것이다.

나. 사이버위험 대응체계의 차별가능성

위험도가 높지 않은 사이버위험이나 일상적인 위험의 경우에는 당해 기관 내지 소관부처의 대응만으로도 충분히 방어할 수 있을 것이다. 문제는 고위험군 침해에 대한 방어인데, 사이버침해 내지 사이버공격을 위험도를 기준으로 구분하여 고위험군 침해를 추출해낼 수 있다고 하더라도 이에 대한 대응을 어떻게 또는 어느 기관에서 할 것인지는 전혀 차원이 다른 문제이다. 또한, 고위험군 침해가 발생한 경우 이를 준전시상황으로 보아야 할지, 재난상황으로 보아야 할지, 위기상황으로 보아야 할지에 대해서도 따져볼 필요가 있다. 컨트롤 타워를 어느 기관이 맡게 될지는 별론으로 하더라도 준전시상황으로 파악할 경우 국방부가, 재난상황으로 파악할 경우 행정안전부가, 위기상황으로 파악할 경우 국가정보원이나 방송통신위원회와 같은 정보보안 또는 정보화의 주무부처가 주축기관이 될 수밖에 없기 때문이다.

어느 경우이건 간에 고위험군 침해에 대한 신속한 대응체계가 제때 가동되지 못한다면 사태가 복구할 수 없는 심각한 상황으로 악화될 수 있고, 고위험군 침해에 대해서는 보다 집약적이면서도 차별적인 대응전략이 요구되기 때문에 범국가적 위험관리체계 구축 및 위험관리기관 사전지정은 시급한 과제에 속한다. 현재도 민간분야, 국가·공공분야, 국방분야로 구별하여 사이버위기 대응기구를 마련하고 있지만, 이처럼 침해 또는 피해의 성질을 기준으로 하여 분야를 나눌 경우 침해주체가 불분명하거나 피해대상이 복합적일 경우에는 이를 명확하게 구분해내어 역할을 분담하기란 생각보다 간단치 않을 것이기 때문이다. 이는 대응의 주체를 결정함에도 마찬가지이기 때문에 어떠한 체계가 적절하고 보다 현실에 부합되는지에 대해서는 향후 심도

있는 논의가 필요할 것이다.

이 글에서도 그 대안을 모색하고자 하나, 준전시상황을 전제한 대안은 본 연구에서 제시하기에는 적절치 않으므로 재난상황을 전제한 '재난관리체계와의 연계방안'과 사이버위기상황을 전제한 '국가사이버위기 관리방안'을 각각 소개하고자 한다. 다만 연구진 간에 의견이 합일되지 못한 사안이므로[244] 가급적 이들 방안을 제안자의 의견을 존중하여 소개하되 이에 대한 논평은 별도로 하지 않고자 한다.

2. 재난관리체계와의 연계방안

융합 시대에 맞게 현행 정보통신기반시설 보호체계를 재난관리체계와 연계, 통일시키는 것이 필요하다.[245] '재난 및 안전관리 기본법'은 재난을 국민의 생명·신체 및 재산과 국가에 피해를 주거나 줄 수 있는 ① 자연현상(태풍·홍수·호우·강풍·풍랑·해일·대설·낙뢰·가뭄·지진·황사·적조 등)으로 인하여 발생하는 재해, ② 화재·붕괴·폭발·교통사고·화생방사고·환경오염사고 등으로 인한 피해, ③ 국가기반체계(에너지·통신·교통·금융·의료·수도 등)의 마비로 인한 피해, ④ 전염병 확산 등으로 인한 피해로 규정한다(동법 제3조 제1호). 특히 국가기반체계는 에너지, 정보·통신, 교통·수송, 금융, 보건·의료, 원자력, 환경, 식용수 등 그 기능이 마비될 경우 국민의 생명과 재산 및 국가경제에 심각한 영향을 미칠 수 있는 물적·인적·서비스·환경 체계이다. 따라서 이러한 사회 인프라의 마비로 인한 피해를 재난으로 보고 관리한다면, 해당 사회 인프라의 기능 수행에 중요한 역할을 하는 정보통신기반시설도 재난관리의 내용에 포함하여야 한다. 다만 사회 인프라 별로 또 사회 인프라의 구성요소마다 위협이 상이하므로 그에 대한 대응은 달라질 수밖에 없을 것이다. 이때 정보통신기반시설의 경우 전자적 침해행위가 중요한 위협요소가 될 수 있다.

244) '재난관리체계와의 연계방안'은 박영우 전문위원이, '국가사이버위기 관리방안'은 김민호 교수와 실무연구진이 제안하였다.

245) 이와 관련한 내용은 박영우, 융합 시대의 정보통신기반시설 보호, 정보보호21c, 2010년 8월호, 52쪽 이하에서 재인용.

정보통신기반시설 보호와 재난관리체계의 주요 연계방안은 다음과 같다. 첫째, 기본계획을 연계하여야 한다. '재난 및 안전관리 기본법'은 관리대상인 재난의 하나로 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비를 들고 있으며, 전자적 침해행위로 인한 주요정보통신기반시설의 파괴 혹은 기능 마비는 통신 등 특정한 국가기반체계 즉 사회 인프라의 기능 마비를 초래하거나 더 나아가 금융 등 다른 사회 인프라의 기능 마비를 가져올 수도 있다. 따라서 재난관리계획의 수립에서 주요 정보통신 기반시설 보호를 포함하거나 또는 주요 정보통신 기반시설 보호계획과 연계하는 것이 바람직하다. 국가안전관리 기본계획은 각종 재난 및 사고로부터 국민의 생명·신체·재산을 보호하기 위하여 국가의 재난 및 안전관리의 기본방향을 설정하는 '최상위 계획'이다. 따라서 국가안전관리 기본계획에 주요 정보통신 기반시설 보호계획을 반영 혹은 연계시키는 것은 당연한 논리라고 할 수 있다. '재난 및 안전관리 기본법'은 국가기반체계의 보호를 위하여 2007년부터 국가기반시설을 지정, 관리하도록 규정하고 있으므로, 주요 정보통신 기반시설 보호계획을 국가기반시설 지정, 관리와 통합 혹은 연계할 수 있다.

둘째, 추진체계와 관련하여서는 주요 정보통신 기반시설 보호체계를 '재난 및 안전관리 기본법'에 따른 국가기반시설 보호체계와 연계하는 것이 바람직하다. 앞에서 살펴보았듯이 주요 정보통신 기반시설은 독립한 사회 인프라가 아니며, 사회 인프라의 기능 수행에 핵심적인 역할을 하는 전자적 제어·관리시스템 및 정보통신망이다. 또한 주요 정보통신 기반시설을 포함하는 사회 인프라는 대개 국가기반시설에 해당한다고 볼 수 있다. 주요정보통신기반시설이 관계되는 업무로 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등을, 국가기반시설이 관계되는 국가기반체계로 에너지·통신·교통·금융·의료·수도 등을 드는 데서 공통점을 찾을 수 있다. 그리고 전자적 침해를 '정보재난'으로 이해할 수 있으며, '재난 및 안전관리 기본법'의 국가기반체계의 마비는 그 주요 정보통신 기반시설에 대한 의존 때문에 전자적 침해를 포함하지 않으면 완전하게 이해할 수 없다. 따라서 주요 정보통신 기반시설 보호체계도 재난 및 안전관리체계 내에서 국가기반시설 보호의 일환으로 운영되는 것이 타당하다. 이러한 맥락에서 국가기반시설의 지정, 재난관리 교육·훈련, 위기관리 매뉴얼 정비·보완 등 국가기반시설의 관리가 해당 시설의 주요 정보통신 기반시설 보호와 연계되도록 하여야 한다. 이러한 점에서 우선 '정보통신기반보호법'에 따

른 정보통신기반보호위원회를 '재난 및 안전관리 기본법'에 따른 중앙안전관리위원회의 분과위원회 중 하나인 국가기반체계보호대책위원회에 통합하는 것이 바람직하다. 다만, 주요정보통신기반시설의 경우 해킹·컴퓨터바이러스 등 전자적 침해행위가 주요한 위협이므로 자연재해, 화재, 전염병 등에 대한 대응체계와 같이 전자적 침해에 맞는 예방, 대응 및 복구 등 조치가 이루어질 수 있도록 체계와 제도가 정비되어야 할 것이다.

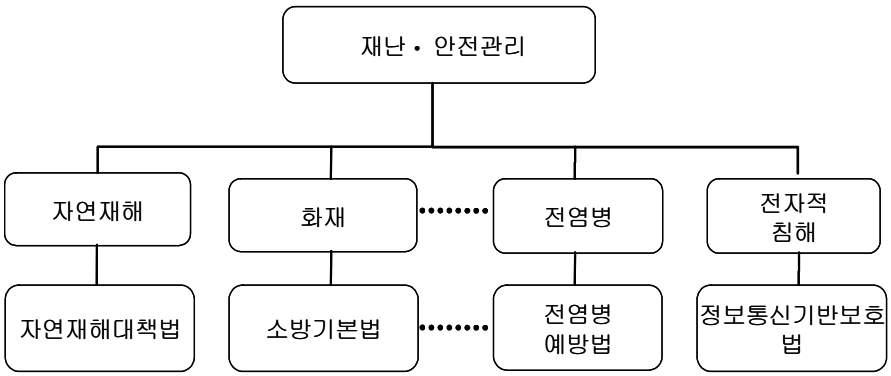


그림 8 정보통신기반보호를 포함한 재난·안전관리 체계

셋째, 대응 및 복구대책을 연계하여야 한다. 전자적 침해와 다른 재해·재난은 그 위협의 성격이 다르므로 그 예방, 대응 및 복구 수단도 다를 수밖에 없다. 따라서 전자적 침해에 대해서는 어느 정도 독립한 조직과 체계를 필요로 한다. 그러나 전자적 침해라 할지라도 그로 인한 주요정보통신기반시설의 마비가 해당 국가기반시설 혹은 더 나아가 다른 국가기반시설의 마비를 초래할 수 있다. 따라서 대응 및 복구 차원에서는 주요정보통신기반시설의 마비로 인한 해당 국가기반시설 및 다른 국가기반시설에의 영향을 고려하여야 한다.

요컨대 고도 정보사회 및 융합 시대에는 사회 인프라의 대부분이 정보통신 인프라에 절대적으로 의존한다. 따라서 전통적인 재난·재해 뿐만 아니라 전자적 침해행위에 의해 해당 정보통신 인프라의 파괴 혹은 기능 마비를 가져올 수 있고, 이는 궁극적으로 정보통신 인프라에 의존하는 사회 인프라의 파괴 혹은 기능 마비를 초래할 수 있다. 따라서 현재와 같이 사회 인프라에 대한 재난관리체계를 전통적인 재난·

재해와 전자적인 침해로 분리하여 운영하는 것은 바람직하지 않으며, 양자를 통합하여 통일된 재난관리체계를 구축하는 것이 필요하다.

3. 국가사이버위기 관리방안

가. 국가사이버위기 관리의 필요성과 목적 확립

현재까지 우리나라에는 국가사이버위기 관리와 관련된 통합법적 성격을 지닌 개별 법률이 없는 상태이다.[246] 따라서 개별 법률에서 규정하고 있는 사이버 위기에 관한 다종다양한 내용을 총괄 관리할 수 있는 법률이 필요하다. 특히 민간 기업 및 개인에 대한 사이버위기는 물론 국가·사회적으로 중요한 기능을 수행하는 핵심기반 마비와 관련된 사이버 위기관리를 위한 체계 구축이 필요하다.

또한 국가사이버위기 관리는 궁극적으로 국가 및 지역 사회를 구성하는 개인, 조직, 기업, 공공기관, 정부기관 등이 각각의 수준에 맞는 사이버 위기관리 체계를 이룰 때에 비로소 국가사이버위기 관리가 가능하다는 점을 전제로 한다. 국가사이버위기 관리의 가장 기본적 이념은 국가를 구성하는 최소 단위인 국민의 사이버상 안전 확보뿐만 아니라 국가·사회적으로 중요한 기능, 시스템, 시설 등을 보호하기 위하여 사이버위기를 관리하는데 있다. 또한 국가사이버위기 관리는 개인을 포함하는 개별 국가 구성요소의 안전뿐만 아니라 국가사회 전반에 대한 위협을 가져오는 사이버 위

246) 국가사이버위기 관리에서 사용하는 용어를 정의하면 다음과 같다. 첫째, 국가사이버위기는 "정보통신기술을 통해 국민의 생명과 재산 및 건강, 국가의 주권과 영토, 그리고 국가를 구성하는 정치·경제·사회·문화 체계 등 국가의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태"로 정의할 수 있다. 이러한 국가사이버위기의 정의는 다음의 내용을 포함한다. 우선, 국가사이버위기의 정의에는 컴퓨터나 인터넷, 모바일 통신, 무선 망 등의 포괄적 의미의 정보통신 기술을 활용하는 것들이 모두 포함된다. 둘째, 국가사이버위기에는 정보통신 기술을 활용하여 국민생활안전에 대한 위협, 국가의 주권 및 영토 등 전통적 안보에 대한 위협, 국가 핵심기반에 대한 위협 등을 모두 포함한다. 셋째, 국가 핵심기반, 즉 금융·교통·전력·정보통신·에너지·원자력·댐·주요산업단지·공중보건 마비의 경우에는 정보통신 기술을 활용함으로써 온라인 및 오프라인 상에서의 시스템, 시설, 기능의 마비를 가져올 수 있는 상황을 모두 포함한다. 넷째, 이외에도 현재의 과학 기술이나 인지 능력의 한계로 말미암아 사이버 위기로 인식하지 못하지만 향후 국민의 생명과 재산을 위협하거나 국가의 안전을 정보통신 기술을 이용하여 위협할 수 있는 신종 사이버 위기를 고려해야 한다.

기 상황의 예방과 대비, 대응, 복구를 통해 국가사회의 사이버 기능과 시스템, 시설이 보호될 수 있도록 해야 한다.

나아가 국가사이버위기 관리는 국가사이버위기를 효과적으로 예방·대비하고 대응·복구하기 위하여 국가가 자원을 기획·조직·조정·통제하는 과정으로서 다음과 같은 단계 및 활동으로 구성되어야 한다. ① 예방 단계는 국가사이버위기 요인을 사전에 제거하거나 감소시킴으로써 국가사이버위기의 발생을 억제하거나 방지할 수 있어야 하며, ② 대비 단계는 국가사이버위기 상황 하에서 수행해야 할 제반 사항을 사전에 계획·준비하고 교육·훈련을 실시하여 국가사이버위기에 대한 대응 능력을 높임으로써 국가사이버위기 발생에 즉각적으로 대응할 수 있는 태세를 강화시킬 수 있어야 하고, ④ 대응 단계는 국가사이버위기가 발생한 경우 국가의 자원과 역량을 효율적으로 활용하고 신속하게 대처함으로써 사이버 위기로 인한 직·간접적 피해를 최소화하고 2차적인 국가위기 및 국가사이버위기의 발생 가능성을 감소시킬 수 있어야 하며, ④ 복구 단계는 국가사이버위기로 인해 발생한 피해를 국가사이버위기 발생 이전의 상태로 개량 복구함으로써 재발하지 않도록 할 수 있어야 할 것이다.

나. 국가사이버위기 관리의 기본방향 및 책무 확립

국가사이버위기 관리에 있어서 국가사회를 구성하는 개인, 조직, 기업, 공공 및 정부 기관은 국가사이버위기 관리의 기본 방향을 다음과 같이 설정하여 시행하는 것이 효과적이다. 첫째, 국가사이버위기 관리 정책은 국민의 생명과 재산 및 건강을 보호하고, 국가의 주권·영토 및 국가핵심기반의 안전 확보를 그 목적으로 하여야 한다. 둘째, 국가사이버위기가 발생하지 않도록 하기 위한 사전 예방 위주의 위기관리 정책을 수립하여야 한다. 셋째, 국가사이버위기 관리 기능 수행은 정부기관뿐만 아니라 시민사회단체 및 민간기업의 적극적 참여와 협력을 기반으로 하고, 필요하다고 인식하는 경우에는 공동으로 기능을 수행하여야 한다. 넷째, 정부와 시민사회단체 및 민간 기업은 국가사이버위기 관리의 지속적인 발전을 위하여 노력하여야 한다. 다섯째, 국가는 각종 유형별 국가사이버위기를 관리하기 위하여 국제적 협력 체계를 구축하여야 한다. 여섯째, 국가사이버위기 관리는 국민과 국가의 안전 확보를 위해 국내 및 해외의 사이버 위기에 대한 관리 활동이 적용되어야 한다.

국가사이버위기 관리의 효과적 수행을 위하여 다음과 같은 책무가 부과되어야 한다. 첫째, 국가는 국가사이버위기 관리의 발전과 이를 통한 국가의 종합적 사이버 안전 확보를 위한 종합적인 정책을 세우고 추진하여야 한다. 둘째, 중앙정부 및 지방자치단체, 공공기관 및 주요 민간 기업들은 특성을 고려하여 국가사이버위기 관리 계획을 수립하고 추진하여야 한다. 셋째, 정부, 기업, 시민사회단체 그 밖에 조직들은 각종 국가사이버위기를 적극적으로 예방하고 대비하여야 하며, 국가사이버위기 발생 시에 효율적으로 대응·복구하는데 필요한 기획, 조직, 조정, 통제 기능을 수행하여야 하며, 제반 국가사이버위기 관리 정책을 수립하고 집행·평가하기 위한 계획을 수립·시행하여야 한다. 넷째, 정부는 국가사이버위기 관리 정책의 효과성과 효율성 증진을 위하여 국가사이버위기 관리 정책의 형성, 집행, 평가 그 밖에 활동 과정에 민간 전문가 또는 관련 단체 등이 참여하도록 하고 일반 국민의 다양한 의견을 모을 수 있는 방안을 마련하여야 한다.

다. 국가사이버위기 관리의 조직체계 구축

현재 우리나라는 국가사이버위기 관리에 관한 개별 법률들이 산재되어 체계화되어 있지 못하며 법률 간의 협력 및 연계도 제대로 이루어지지 못한 실정이다. 따라서 전통적 안보 차원, 국가 핵심기반 차원, 국민생활 안전 차원 등에서의 국가사이버위기를 포괄할 수 있는 기준이 되는 법률의 제정을 통하여 국가사이버위기 관리와 관련된 법률을 체계화하는 것이 요구된다.

이와 함께 지금까지는 각 기관간 역할이나 국가 차원의 대응체계를 고려하지 않고 소관부처 중심으로 업무수행이 이루어져 정보공유와 업무 협조에 있어서도 소극적일 수밖에 없었고, 사이버 테러리즘으로 인한 침해사고와 관련한 민간기업의 정보제공, 정보보호안전진단 등 침해사고 최소화 방안이 미흡하였다. 이러한 문제점들을 개선하고 실질적인 대응 업무를 마련하고 정착시키기 위해서는 관련 법제도의 개선이 필요하다.

또한, 국가사이버위기 관리의 효율적이고 효과적인 수행을 위해서는 국가사회 전반의 국가사이버위기 관리의 기준과 새로운 모범을 제시하는 한편, 각 부처 및 국가사회의 구성요소들에 대해 국가사이버위기 관리 정책을 집행할 수 있는 국가사이버

위기 관리 조직체계를 구축하는 것이 요구된다. 즉, 정부는 국가사이버위기 관리에 관한 주요 정책의 심의 및 기획·조정, 통합된 국가사이버위기 관리의 기능을 수행하기 위하여 훈령으로 설립되어 있는 '국가사이버안전센터'의 법적 지위를 마련하는 것이 필요하다. 국가사이버위기와 관련된 정보의 종합적 수집, 분석, 처리의 종합적 기능을 수행하고 각 정부 및 공공 기관을 통할하며 민간부문과의 협조체계 구축을 수행한다.

새롭게 구성되는 국가사이버위기 관리 조직은 다음 기능을 수행하는 것이 필요하다. 첫째, 국가사이버위기 관리에 관한 중요 정책의 심의 및 총괄·조정, 둘째, 국가사이버위기 관리 체계 및 경보·연습·평가 등 제도의 구축에 관한 기획 및 조정, 셋째, 국가사이버위기 관리 기관이 수행하는 위기관리 업무의 협의와 조정, 넷째, 국가사이버위기 발생 시 통합 대응 기능의 수행 및 조정, 다섯째, 국가사이버위기 발생 이전에 이를 예방하기 위한 정책의 수립·집행 및 조치 사항, 여섯째, 국가사이버위기의 발생에 따른 각 기관별 소관 업무와 관련되는 응급대책의 수립·시행, 일곱째, 국가사이버위기 발생으로 인한 피해 복구 및 안정화 대책 등이 그것이다.

라. 국가사이버위기 관리의 교육·훈련·연습 체계 구축

국가사이버위기에 효율적으로 대응하기 위해서는 사이버상에서의 정보통신 기술을 활용할 수 있는 전문적이고 기술적인 지식과 응용 능력을 지녀야 할 뿐만 아니라 사이버범죄 및 테러리즘이라고 하는 보안 분야의 전문적인 이해도 지녀야 한다. 각 기관별 사이버위기대응센터 및 사이버범죄 수사기관의 전문 인력은 공공분야, 민간분야, 그리고 국방분야 모두 부족한 실정이다. 따라서 국가 핵심기반과 관련된 국가기간전산망을 사이버 상에서 안전하게 운영하기 위해서는 보안시설과 장비에 대한 지속적인 투자와 함께 관련 인력에 대한 지속적인 교육과 훈련, 연습을 실시해야 하는 한편, 전문성을 확보하기 위한 노력을 기울여야 한다. 즉, 전문적인 교육·훈련·연습을 통해 빠른 기술적인 변화를 보충하도록 해야 하며, 시스템을 운영하는 직원의 전문성을 최대한 보완해주는 것이 필요하다.

마. 국가사이버위기 경보체계 구축

과거에는 국가적인 사이버위기가 발생한 후 효과적인 위기관리를 위해 사후 위기관리에 중점을 두는 경향이 있었으나, 최근에는 위기 징후를 사전에 탐지하여 사이버 위기 발생을 사전에 방지하는 사전 조기 경보·사전 위기관리의 운용이 중요시되고 있다. 각종 국가사이버위기로 인하여 국민과 국가의 안전에 피해가 예상되는 경우 국가사이버위기 관리 관련 기관들로 하여금 필요한 조치를 취하게 하기 위하여 국가사이버위기 경보를 발령하는 것이 필요하다. 즉, 국가사이버안전센터는 국가사이버위기 발생의 징후가 식별되거나 발생이 우려되는 경우에 국가사이버위기 관리 기관들이 사전에 필요한 조치를 취할 수 있도록 국가사이버위기경보를 발령해야 한다.

따라서 국가사이버안전센터는 국가사이버위기 경보의 발령에 따른 국가사이버위기 관리 기관별 조치 사항의 이행 실태를 점검하고, 필요하다고 인정하는 경우에는 국가사이버위기 관리 기관의 관계 직원의 출동 또는 물자 및 지정된 장비·인력의 동원 등 필요한 조치를 취할 수 있어야 한다.

바. 국가사이버위기사태 선포체계 구축

정부는 각종 국가 사이버위기로 인하여 국민과 국가의 안전에 중대한 영향을 미치거나 당해 사이버 위기의 효과적인 수습 및 복구를 위하여 특별한 조치가 필요하다고 인정되는 경우에는 국가사이버위기사태를 선포할 수 있어야 한다.

사. 국가사이버위기 관리 평가체계 구축

국가사이버안전센터는 국가사이버위기 관리 기관의 정책 및 활동에 관하여 평가를 함으로써 국가사이버위기 관리의 효과성 확보를 위하여 노력하여야 한다. 이러한 사이버 위기관리 평가의 기본 내용은 다음과 같다. 첫째, 국가사이버위기를 예방하기 위한 정책의 수립·집행 및 조치 사항, 둘째, 국가사이버위기의 발생에 따른 대응 조치와 이에 필요한 대비 활동, 셋째, 국가사이버위기 발생으로 인한 피해 복구 및 안정화 대책, 넷째, 국가사이버위기 유형별 관리 정책 및 관리 체계, 규정 등이다.

국가사이버안전센터는 평가 결과를 국가사이버위기 관리 정책에 반영하고, 필요하

다고 인정하는 경우에는 국가사이버위기 관리 기관의 장에게 시정조치나 보완을 요구하는 것이 필요하다.

4. 사이버안전 관련 제반 인프라 구축을 위한 제언

이상과 같이 사이버위험 관리체계 구축을 위한 서로 다른 2개의 대안을 살펴보았는데, 이러한 대안들의 공통점은 제한된 고위험상황에서 국가의 역할을 강조하고 있다는 점이다. 그러나 현재의 보안기술 내지 보안정책으로는 정보통제에 한계가 있고, 중앙집중적 통제정책의 실시는 IT 산업 발전을 저해하거나 이용자 불편만 초래할 소지가 있다는 점에 유의할 필요가 있다. 또한, 사이버안전체계를 구축하고자 하는 지금의 논의는 7·7 DDoS 공격사태로 인하여 촉발되었는데, 현재의 사이버공격 방어기술 내지 보안정책으로는 DDoS 공격의 대응에 한계가 있을 수밖에 없고, 기술개발 외에 유효한 대안이 없다는 점에도 유의하여야 할 것이다.

따라서 경우에 따라서는 국가기관 주도의 통제(control)정책보다는 이용자인 국민과 이용자와 전문성을 확보한 민간 보안업체(예 : 안철수연구소, 하우리)의 자율적 협력을 이끌어낼 수 있는 정책이 보다 효과적일 수 있기 때문에 사이버위험 관리체계를 범국가적으로 구축할 필요가 있더라도 이는 필요한 최소한의 범위에서만 허용되어야 할 것이다. 나아가 사이버위험 관리체계를 구축·운용하여 한때의 고위험상황을 잘 넘기는 것도 중요하지만, 평소에 다음과 같은 제반 인프라를 충실하게 구축해두는 것도 중요할 것이다.[247]

가. 전문인력 양성 및 확보

사이버위험 관리는 공공과 민간 분야에서의 전문인력 확보와 전문성 향상이 그 핵심요소로 제시되고 있다. 이러한 전문 인력을 양성하는 방법으로 국가가 직접 사이버 위험관리 전문기관을 운영하는 방안과, 대학이나 연구소 또는 정부가 인정하는

247) 가안 및 나안은 김민호 교수와 실무연구진이, 다안은 박영우 전문위원이, 라안은 강석구 연구위원이 제안하였다.

기관을 교육기관으로 지정하거나 협약을 통하여 전문인력의 양성기관으로 지정하는 방안을 생각해볼 수 있다.

나. 관련 연구·개발 증진

사이버 위험관리와 관련된 문제점을 해결하고 예방하며 효율적으로 대응하기 위해서는 많은 인력과 예산을 투입해서 연구하고 분석하여 문제점 발견과 개선 방안 도출을 위해 노력해야 한다. 이러한 노력을 통해 예방 효과를 높이고 대형 사이버위기 발생 시의 혼란과 무질서를 조금이라도 줄이는 것이 위험관리의 접근 방식이다.

이에 국가는 사이버위기에 대한 정확한 원인의 진단과 분석, 교훈의 도출 등을 위하여 사이버위기 발생 시에 관련된 다양한 학문분야별 전문가들을 공동으로 파견하여 각종 사이버위기 사례에 대한 전문가들의 연구와 분석, 관련 자료의 수집·정리·보존이 함께 이루어지도록 노력하여야 한다. 사이버위기 유형 중 빈번하게 발생하는 위기의 원인 분석 및 개선방안, 관련된 자료의 종합 DB 구축, 기술 지원 등의 사업을 추진하기 위하여 국책연구기관 등의 적극적 활용이 필요할 것이다.

다. 적절한 정보보호 예산의 확보

적절한 정보보호 예산이 확보되어야 한다. 사이버침해의 예방 및 대응은 손만 가지고 할 수 있는 것이 아니다. 사이버침해가 정보기술과 장비를 이용하므로 이에 대응하기 위해서는 기술 및 장비가 필요하다. 미국의 경우 최근 IT 예산은 상대적 증가세가 둔화되었지만 꾸준히 증가하는 추세이며, IT예산 대비 정보보호 예산은 지속적으로 증가하였고, 2006년부터 2009년까지 최근 4년간 평균 9%로 나타난다. 미국의 경우, 정보보호에 대한 장기적인 정책과 지속적인 정보보호 예산 투자를 통해 침해사고에 대비하고 있음을 알 수 있다.

그러나 국내 정보화 예산은 2009년 7·7 DDoS 침해사고 이후 일시적으로 약 5% 증가하였으나, 2011년 이후 예산감액이 예상되고 있다. 7·7 DDoS 침해사고 이후 8.2%까지 상승한 정보보호 예산비율은 2011년 다시 6.2%로 감소할 것으로 예상되어 정보보호 선진국인 미국에 비해 크게 미흡한 상황이다. 우리나라의 정보보호 예산비율은 지난 4년(2007년 ~ 2010년) 평균 약 5.25% 수준에 그치고 있다.

표 43 정보화 예산 대비 정보보호 예산 비율

(단위 : 억원)

구분	정보화예산	정보보호예산 비율
2007년	34,104	2.9%
2008년	34,062	4.7%
2009년	31,378	5.6%
2010년	32,867	8.2%
2011년(안)	33,023	6.2%

※ 자료 : 국회예산정책처[국가정보화사업 평가], 2010년 8월
기획재정부 제출자료, 2010년 10월 1일 (배성훈, 26쪽에서 재인용)

미국의 경우 침해사고 발생 유무에 관계없이 침해사고 발생에 대비하여 꾸준하게 정보보호에 예산을 투자하고 있다. 반면 우리나라의 경우는 사고가 발생한 후에야 일회성으로 예산 투자가 이루어지고 있으며, 그나마도 사고에 대한 관심이 잦아든 이후에는 다시 이전 수준으로 감액되고 있는 상황이다. 국가적인 침해사고를 예방하고 효과적으로 대응하기 위해서는 장기적인 예산계획에 따른 지속적인 정보보호 예산 투자가 이루어져야 한다. 사안이 발생한 경우에만 일회성으로 증가하는 예산은 오히려 사업의 지속성 및 연속성을 저해하며, 중장기 전략을 무용지물로 만들어버릴 가능성이 있다.[248]

라. 불요불급한 개인정보 수집·보관의 최소화

사이버안전성 확보를 위해서는 사후적 위험관리도 중요하겠지만, 피해규모 최소화를 위한 사전적 예방조치도 중요할 것이다. 그런데 사이버침해 또는 사이버공격에 의한 민간분야의 피해가 큰 것은 우리나라 사이트 운영자의 불요불급한 개인정보 수집관행 때문인 것으로 판단되므로 개인정보 유출에 대비한 대책이 필요하다고 판단된다.

특히 주요한 인증수단으로 활용되는 주민등록번호의 경우 이를 안전하게 보호하

248) 배성훈, 앞의 글, 25-26쪽.

지 않으면 명의가 도용되어 사회생활에 지장을 줄 수 있기 때문에 보안기술 내지 환경이 취약한 사이트의 경우 인터넷실명제 적용대상이 아닌 이상 이메일 외의 본인확인 정보 수집을 가능한 한 제한하고, 기(旣)수집 개인정보의 폐기를 명함으로써 피해유발요인을 최소화할 필요가 있다.

제3절 사이버 수사체계 정비방안

사이버 수사체계 정비와 관련해서는 이 글 제3장 제4절에서 경찰청의 사이버침해대응체계를 분석하는 과정에서 대안을 이미 제시한 바 있다. 그 개요를 정리하면 다음과 같다.[249]

첫째, 사후 추적수사에서 사전탐지 및 조기대응 체제로 전환할 필요가 있으며, 이를 위해서는 사이버침해 초동조치에 있어 유관기관 간 협력을 강화하고, 사이버 공격정보 분석을 통한 사전탐지 및 조기대응 역량을 확충하여야 한다.

둘째, 사이버범죄 수사 및 대응 관련 법규를 정비할 필요가 있는데, 이를 위해서는 사이버범죄 처벌법규 정비, 주요 기반시설 사이버침해 피해에 대한 수사기관 고발 의무화, 한국인터넷진흥원의 WHOIS 정보 정확성 제고, 디지털증거 압수수색 및 증거처리 관련 법률정비 등의 조치가 수반되어야 할 것이다.

셋째, 사이버수사 전담조직 및 전문성이 확보될 필요가 있는데, 이를 위해서 전담조직의 위상이 제고되어야 하고, 민간 IT 전문가 경찰관 특채 확대, 사이버테러 전문수사관 양성 등의 조치가 병행되어야 할 것이다.

넷째, 유관기관 및 민간분야와 수사기관 간의 협력이 강화될 필요가 있는데, 이를 위해서는 유관기관 경찰관 파견제도가 활성화되고, 민간의 신고기피를 해소하고 사이버치안 거버넌스를 강화할 수 있는 방안이 마련되어야 할 것이다. 또한, 사이버범죄 예방에 관한 수익자 부담원칙이 도입될 필요도 있을 것이다.

이들 개선방안 중 중요하지 않은 것은 없겠지만, 사이버침해나 사이버공격이 발생한 경우 대상기관의 입장에서는 '방어'와 '피해복구'에 치중할 수밖에 없어 결국 '수

249) 자세한 내용은 이 글, 제3장 제4절 5. '평가 및 개선방안' 참조.

사'를 위한 증거확보에는 소홀해지기 쉽기 때문에 사이버수사의 체계정비를 위해서는 '초동수사의 시기(始期) 단축'이 가장 핵심적인 과제로 될 수밖에 없다. 특히 수사기관, 국방부, 국가정보원 등 기관 간의 업무관할에 따라 공안사범, 사이버전(戰), 일반범죄 여부를 따질 동안 수사 개시가 지연될 가능성이 높고, 이러한 판단이 쉽지 않은 해외발 공격의 경우 경찰청 등 수사기관의 즉시대응이 어려운 문제가 있다.

따라서 수사개시를 위해서는 범죄구성요건 위반, 피해발생 등 범죄혐의에 대한 신속한 확인이 필요하므로 침해의 법적 성격을 불문하고 공격성 침해가 발생한 경우 특정 기관에 우선조사권을 부여하되, 관할이 확정된 때에는 즉시 이관토록 할 필요가 있을 것이다. 이를 위해서는 유관기관 간의 협력체계 구축이 필수적이므로 사이버위험 관리체계를 구축하여야 할 경우 초동수사기관의 지정에 관한 사안도 함께 논의되어야 할 것이다.

제7장

결 론

07 결 론

2009년에 발생한 '7·7 DDoS 공격 사태'를 비롯하여 최근 해킹, DDoS 공격 등 사이버침해에 따른 위험이 증가하고 있다. 특히 최근의 사이버침해 사고는 주민등록번호, ID, 비밀번호 등 개인정보를 유출하여 금전적 이익을 추구한다는 점에서 종전보다 위험성이 증가하고 있고, 유출된 개인정보의 암거래까지 성행하고 있어 문제라고 할 것이다. 이와 함께 공공부문의 주요 정보통신기반시설을 대상으로 하는 사이버침해도 증가 추세이며, 특히 국가기관을 대상으로 하는 해킹은 매년 300% 내외로 증가하는 추세이기 때문에 사이버공격에 의한 국가기능 마비 우려도 증대되고 있다. 예컨대 2009년 발생한 '7·7 DDoS 공격'에 의하여 청와대, 금융기관 등 주요 사이트가 일시적으로 마비된 바 있으며, 대응책 마련에도 불구하고 금년 역시 동일 시기에 재발한 바 있다. DDoS 공격의 경우 악성코드에 감염된 좀비 PC를 이용한다는 점에서 신속하고 효과적인 대응이 어렵다는 한계도 나타낸다.

이에 대응하여 정부는 '정보화촉진기본법'을 '국가정보화기본법'으로 전면개정하고, '국가사이버안전관리규정'을 보완하는 등 사이버위기관리 관련 법제를 전면적으로 점검하였으며, 민간분야는 한국인터넷진흥원 인터넷침해대응센터가, 국가·공공분야는 국가정보원 국가사이버안전센터가, 국방분야는 국방부 사이버사령부가 전담하는 민·관·군 종합대응체계도 현재 구축하고 있다. 다만 정부가 사이버침해 내지 사이버공격에 대응한 법제도를 대폭적으로 손질했음에도 불구하고 물리적·기술적·제도적 한계 등으로 인하여 사전예방이나 범인 추적은 제대로 이뤄지지 못하였고, 국민

과 정부의 불안감은 여전히 지속되었다.

이 연구는 이러한 사이버침해 내지는 사이버공격, 더 나아가 이로 인해 촉발된 사이버위기에 대응한 사이버안전체계 구축을 목표로 한다. 이를 위하여 이 연구는 전문분야가 다른 연구자들과 역할을 분담하여 연구를 진행하였으며, 방법론상 법학적 방법론을 채택하되 이를 유형적 고찰, 현황 분석, 비교법적 고찰, 실증적 고찰로 구분하여 다각적·입체적으로 분석하고자 하였다.

이론적 고찰은 분류이론을 바탕으로 진행하였으며, 그 결과 사이버전이 발발할 경우 이에 대응할 수 있는 교전수칙이 미흡하고, 적의 서버 및 기반시설에 대한 원천지 대응 근거규정이 부족한 문제를 도출하였으며, 민간부문의 정보보호에 대한 투자 및 인력확보가 필요하다는 대안을 제시할 수 있었다. 또한, 형법해석론을 바탕으로 사이버안전 관련 법제를 분석한 결과, 사이버침해의 외연이 1995년 형법개정 당시 예상했던 수준을 넘어서서 사이버테러, 사이버전 개념까지 확장되면서 내란, 외환죄와 관련한 종래의 형법해석론이 한계에 직면했으며, 교통방해, 일수 등 공공안전과 관련해서도 새로운 해석이 필요하다는 문제를 도출할 수 있었다.

현황분석은 국가정보원, 방송통신위원회, 경찰청 등 주요 소관부처의 사이버침해 대응체계 현황을 중심으로 진행하였으며, 이 중 국가정보원의 대응체계 현황분석 결과를 바탕으로 하여 대응활동의 중심역할 수행을 위한 조직·체계의 법적 지위 확보, 관련기관 간 정보공유 및 예·경보체계 관련 법제 정비, 중장기적 관점에서의 연구 및 이를 위한 예산 지원, 고도의 숙련된 전문인력 확보를 위한 노력, 실질적 국제협력 강화, 범국가적 위기관리체계 구축 등의 대안을 제시하였다. 또한 방송통신위원회의 대응체계 현황분석 결과를 바탕으로 하여 정보화와 정보보호 행정의 정비와 조정, 국가안보를 중심으로 하는 정보보안정책과 전자정부, 전자상거래 등 일반분야의 정보보호정책의 차별화, 대통령실을 중심으로 하는 종합지휘감독체계 구축 등의 방안도 제시하였다.

한편, 경찰청의 대응체계 현황분석 결과를 바탕으로 하여 침해사고 대응기구와 경찰 간의 정보교류를 활성화할 수 있는 협력모델 구축, 사후추적 수사에서 사전탐지·조기대응 사이버수사체제 전환, 사이버침해 예방을 위한 경찰청 및 지방청의 전담조직과 기능 확충, 민간의 IT전문인력 특채 등 전문성 제고, 사이버범죄 처벌법규 정비, 형사소송법상 디지털 증거 관련 규정 개정, 민간의 신고기피 현상을 해소하는 방안

개발, 학계, 민간, 업체, 시민단체 등이 모두 참여한 사이버치안 거버넌스 체계 구축 등의 대안을 제시하였다. 이와 관련하여 사이버수사 관련 국제협력 현황을 분석하였고, 그 결과를 바탕으로 국제사회에서 사이버범죄 근절을 위한 책임 있는 역할을 수행하기 위하여 인터폴 사이버범죄 센터를 창설하는 방안 등도 함께 제안하였다.

비교법적 고찰은 미국, 영국, 독일, 프랑스, 일본 등 주요 국가의 사이버공격 대응체계 현황을 중심으로 진행하였고, 그 중 대응체계 구축에 있어 모범사례라고 할 수 있는 미국의 경우와 우리나라의 경우를 비교한 결과, 정책의 혼선을 지양하기 위해서는 기관 간 협력체계를 뒷받침할 법체계 마련 필요성, 국가사이버보안 R&D 정책을 강화 필요성, 국내·국제적 대테러 네트워크 구축 및 관련 법제도 정비 필요성 등의 시사점을 도출하였다.

실증적 고찰은 국가통계 분석과 전문가 인식조사로 진행되었다. 국가통계를 바탕으로 유형별, 분야별 안전실태를 점검한 결과, 응용프로그램의 취약점을 노리는 홈페이지 은닉 악성코드 및 금전적 이득 취득 목적의 악성코드에 의한 위협 지속, 사회적 이슈·이벤트를 악용한 악성코드 유포 가능성 증가, 분석지연을 위한 고도의 분석방해 기술 접목, 악성코드의 대량생산을 위하여 자동화된 도구 이용 증가, 해외발 사이버침해 위협 증가 등의 위험을 전망하였다. 또한, 공공기관 정보보안실무자를 대상으로 실시한 전문가 인식조사 결과, 실무상 '안전'이나 '위기'를 판단할 구체적 기준 미흡, 민간분야에서 고비용 정보보안시스템 구축의 현실적 어려움, 인터넷 실명제 등 본인확인제의 확대에 따른 사이버안전 위협환경 조성가능성 증가, 중대사이버침해 가중처벌방안의 비효율성 등의 시사점을 제시하였다.

나아가 사이버위험의 정도를 측정할 수 있고 사이버위험 대응체계를 차별화할 수 있다는 전제에서 범국가적 사이버위험 관리체계 구축을 위한 종합적인 대안으로서 재난상황을 전제한 행정안전부 중심의 '재난관리체계와의 연계방안'과 사이버위기상황을 전제한 국가정보원 중심의 '국가사이버위기 관리방안'을 제시하였고, 사이버안전환경 구축을 위한 제반 인프라 확충을 위하여 전문인력 양성 및 확보, 관련 연구·개발 증진, 적절한 정보보호 예산의 확보, 불요불급한 개인정보 수집·보관의 최소화 등의 대안도 함께 제시하였다. 이밖에 사이버 수사체계 정비와 관련해서는 경찰청 대응체계 현황분석을 바탕으로 한 대안을 제시하는 한편, 초동수사 실효성 확보를 위한 초동수사기관 일원화 문제를 제기하였다.

이상과 같이 사이버안전체계 구축을 둘러싼 여러 논의와 대안들을 살펴보았지만, 사이버안전 문제는 과학기술 및 통신환경의 급격한 변화에 따라 21세기 들어 최근에야 부각된 사안이고 여전히 제반 환경이 급변하고 있기 때문에 급격한 변화에 따른 불안감과 미지(未知)의 위험에 대한 위기감이 적지 않은 것이 사실이다. 다만 최첨단 분야의 현상에 대한 논의이고 관련 제도와 기술이 충분하게 갖추어진 상황은 아니지만, 제반 인프라를 공고히 갖추고, 학계와 실무계에서 현실감 있는 다양한 연구와 정책개발을 통하여 국가적 위기라는 극히 예외적인 한계상황에 대한 현명한 대처법을 하나하나 개발해나가다 보면 국민과 정부가 가진 불안감과 위기감은 어느 정도 해소될 수 있을 것으로 기대한다.

참고문헌

Ⅰ. 국내문헌

강동범, “정보통신망법상 사이버범죄처벌규정의 검토”, 인터넷법률 제39호, 법무부, 2007.

_____, “사이버범죄 처벌규정의 문제점과 대책”, 형사정책 제19권 제2호, 한국형사정책학회, 2007.

_____, “사이버범죄와 형사법적 대책”, 형사정책연구 제42호, 한국형사정책연구원, 2000.

강 형 외, “사이버테러에 따른 경제적 피해규모 산정을 위한 모델 연구”, 정보·보안논문지 제9권 제3호, 한국사이버테러정보전학회, 2009.

곽병선, “사이버범죄 예방을 위한 법제도적 해결방안 - 가칭 ‘사이버범죄 특별법’ 제정논의를 중심으로 -”, 법학연구 제24집 제3호, 원광대학교 법학연구소, 2008. 9.

경찰청, 미래비전 2015, 2009. 10.

_____, 경찰 미래발전전략, 2009. 5.

_____, 경찰백서, 2005~2009.

국가정보원, 국가정보보호백서, 2004/2006/2007/2008/2009.

_____, 국가사이버안전메뉴얼, 2005. 10.

국가안전보장회의, 국가위기관리에 관한 법제화 방안, 2006.

국가보안기술연구소, 국가 사이버위기 관리 체계 강화방안에 관한 연구, 2008.

_____, 각국의 정보보안 관련법제, 2006.

국가사이버안전센터, Monthly 사이버시큐리티 7월호, 2007. 7.

국회입법조사처, “7·7 DDOS 사고” 대응의 문제점과 재발방비 방안, 2009.

권문택, “국가사이버안전관리 조직의 통합적 체계구축에 관한 연구”, 정보·보

안논문지 제9권 제3호, 한국사이버테러정보전학회, 2009.

_____, “사이버테러정보전 전문인력 양성 및 관리 방향에 대한 연구”, 정보보증논문지 제5권 제3호, 한국사이버테러정보전학회, 2005.

김귀남, “국가 사이버전 대비방안 연구”, 정보·보안논문지 제6권 제4호, 한국사이버테러정보전학회, 2006.

김도승, 사이버공간에서의 경찰법이론에 관한 연구, 성균관대학교 박사학위논문, 2009.

_____, “사이버공간에서 경찰책임의 법적 구조와 특징”, 토지공법연구 제46집, 한국토지공법학회, 2009. 11.

_____, “사이버위기 대응을 위한 법적 과제 : 미국의 사이버위기 대응체계 현황과 시사점을 중심으로”, 방송통신정책 제21권 17호, 정보통신정책연구원, 2009. 9.

김민식 외, “통합적 사이버 위기관리 체계의 필요성에 관한 연구 : 미국과 한국의 제도 및 정책 비교를 중심으로”, 정보·보안논문지 제9권 제1호, 한국사이버테러정보전학회, 2009.

김석훈 외, “통합보안관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구”, 정보보증논문지 제5권 제2호 , 한국사이버테러정보전학회, 2005.

김성규, “인터넷과 형법”, 인터넷법률 제26호, 법무부, 2004.

김연수, 사이버범죄 총람, 법률미디어, 2002.

김열수, 21세기 국가위기관리체계론(한국 및 외국의 사례비교연구), 오름, 2005.

김영란, “사이버범죄조약 대응을 위한 일본의 형사법개정안 연구”, 치안정책연구 제19호, 치안정책연구소, 2005.

김영진 외, “국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구”, 정보보호학회논문지 제19권 제1호, 2009. 2.

김영환, “사이버범죄에 대한 국가적 대응체계 구축의 이론적 함의 : 사이테러형 범죄를 중심으로”, 한국컴퓨터정보학회논문지 제63호, 2009. 6.

김인중 외, “사이버테러리즘의 변화 : 자생적테러와 대응방안”, ICCSA 2007, LNCS(SCI-E), 2007. 8.

_____, “대규모 네트워크시스템을 위한 시변 위험분석과 피해산정 연구”, ICCSA 2005, LNCS(SCI-E), 2005. 5.

_____, “피해 수준과 피해 진행 분석을 위한 정보시스템 모델링 연구”, ICCSA 2006, LNCS(SCI-E), 2006. 5.

김재광/김정임, “일본의 사이버위기 관련 법제의 현황과 전망”, 법학논총 제33권 제1호, 2009.

김재권, “사이버 테러 범죄수사를 위한 Forensics 기법 연구”, 한세대학교 박사학위논문, 2007.

김정규, “사이버 테러리즘의 위험성 증가에 따른 국가위기관리 차원의 대처방안 : 사이버 범죄의 대응과 연계하여”, 국가위기관리연구 제1권, 충북대학교 국가위기관리연구소, 2007.

김준호(역)/Ulrich Sieber(저), “전세계 사이버 공간상의 복합성에 대한 대처방안 : 컴퓨터관련형법의 조화”, Law & technology 제5권 제4호, 서울대학교 기술과법센터, 2009.

김학신, “Computer Forensics를 통한 디지털 범죄수사에 있어 기본권 보호에 관한 연구”, 성균관대학교 박사학위논문, 2008.

김현곤/이재은/장윤식/김기범/민경식/김인호/박영우/이혜정/김은정, 미래형사이버범죄 대응전략 연구, 한국정보화진흥원, 2009. 12.

류인모, “정보보안을 위한 형법적 대응 : 해킹범죄를 중심으로”, 인천법학논총, 1998.

민경식 외, 주요국 정보보호 동향조사 2007 - 유비쿼터스 시대의 정보보호 정책을 중심으로, 한국정보보호진흥원, 2006.

박동균, “북한의 사이버 테러공격 가능성 및 대비전략”, 국가위기관리학회보 제1권, 2009. 12.

_____, “한국 경찰의 위기관리능력 제고방안 : 미국과 일본 사례의 교훈을 중심으로”, 한국공안행정학회보 제18호, 2004.

박영우, “사이버범죄방지협약의 국내법적 수용문제”, 정보보호학회지 제13권 제5호, 2003. 10.

박윤해, “컴퓨터범죄에 관한 연구”, 법학논집 제16집, 숭실대학교 법학연구소,

2006.
박준석, “한국에서의 사이버 범죄 규율의 현황과 제언”, Law & technology 제5권 제3호 , 서울대학교 기술과법센터, 2009.
박창욱, “경찰의 사이버범죄에 대한 효율적 대응방안에 관한 연구”, 한국컴퓨터정보학회논문지 제53호, 2008.
박희영, “독일의 사이버범죄방지조약의 비준에 관한 법률(上)”, 법제 제616호, 법제처, 2009.
_____, “독일의 사이버범죄방지조약의 비준에 관한 법률(下)”, 법제 제617호, 법제처, 2009.
_____, “사이버범죄방지조약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향”, 인터넷법률 제46호, 법무부, 2009.
_____, “독일에 있어서 사이버범죄 관련 입법 및 판례의 최근 동향”, 법제 제612호, 법제처, 2008.
_____, “독일의 컴퓨터 범죄 방지를 위한 제41차 형법 개정법”, 법제 제600호, 법제처, 2007.
_____, “독일에 있어서 사이버범죄의 형사법적 대응에 관한 최근 동향”, 인터넷법률 제35호, 법무부, 2006.
_____, “인터넷에서 형법의 장소적 적용범위 : 속지주의와 편재주의를 중심으로”, 인터넷법률 제26호, 법무부, 2004.
_____, “사이버범죄방지조약의 발효와 한국 형법의 대응법규”, 인터넷법률 제23호, 법무부, 2004.
방송통신위원회, 인터넷 정보보호 종합대책, 2008. 7. 22.
방송통신위원회/행정안전부/지식경제부, 2010 국가정보보호백서, 2010. 4.
배문범, “가상공간에서의 범죄의 의미와 유형분류에 관한 연구”, 대학원논문집 제30집, 동아대학교 대학원, 2005.
배성훈, ‘7·7 DDoS 사고’ 대응의 문제점과 재발방지 방안, 현안보고서 제48호, 국회입법조사처, 2009. 12. 1.
_____, 국가 정보보호 정책현황과 개선방안, 현안보고서 제93호, 국회입법조사처, 2010. 10. 20.

백광훈, “사이버범죄의 개념과 용어의 문제”, 형사정책연구소식 제68호, 한국형사정책연구원, 2001.

_____, 사이버테러리즘에 관한 연구, 한국형사정책연구원, 2001. 12.

_____, 사이버범죄에 대한 ISP의 형사책임에 관한 연구, 한국형사정책연구원, 2003.

서보학, “인터넷상의 정보유포와 형사책임”, 형사정책연구 제12권 제3호, 한국형사정책연구원, 2001. 9.

설민수, “인터넷서비스제공자를 통해서 본 제3자 보유정보에 대한 영장주의의 실효성”, 법조 제635호, 2009. 8.

손경한/박진아, “사이버 불법행위에 대한 국제적 규제”, 법학논문집 제31집 제1호, 중앙대학교 법학연구소, 2007.

손영동, I war(사이버 냉전 시대 국가는 어떻게 생존하는가?), 황금부엉이, 2010.

손영동 외, “국가사이버위협에 대응하기 위한 정보보안 정책 연구”, ISP 2009, 2009. 8.

_____, “해외 주요국의 사이버 안보 정책분석 및 강화방안”, IT 정보경영학회지 제1권 제1호, 2008. 5.

신각철, 컴퓨터범죄론, 법영사, 1996.

신동일, “사이버범죄에 대한 글로벌 대응”, 법죄방지포럼 제20호, 한국범죄방지재단, 2007.

안경옥, “사이버범죄의 현황과 대응방안”, 경희법학 제38권 제1호, 경희대학교 법학연구소, 2003.

안철현, “국가 위기관리 개념의 변화와 위기관리 체계의 구축방향”, 비상기획보 제73호, 2005.

양근원, “주요 국가들의 사이버테러 범죄 대응 1”, 수사연구 제244호, 수사연구사, 2004.

_____, “주요 국가들의 사이버테러 범죄 대응 2”, 수사연구 제246호, 수사연구사, 2004.

_____, “각국의 사이버범죄 대응 절차법 1”, 수사연구 제247호, 수사연구사,

2004.
_____, “각국의 사이버범죄 대응 절차법 2”, 수사연구 제251호, 수사연구사, 2004.
_____, “각국의 사이버범죄 대응 절차법 3”, 수사연구 제252호, 수사연구사, 2004.
_____, “사이버테러 현황 및 사례”, 정보통신윤리 제57호, 정보통신윤리위원회, 2004.
오병두, “독일의 컴퓨터범죄 대응을 위한 제41차 형법개정법률 : 배경, 내용 및 시사점”, 형사법연구 제19권 제3호, 2007. 9.
오영근, “인터넷범죄에 관한 연구”, 형사정책연구 제14권 제2호, 한국형사정책연구원, 2003. 6.
오원이/김연수/홍승희/정완/양희인, 사이버범죄 국내외 동향 및 방지를 위한 정책적 개선방안, 한국정보문화진흥원, 2005. 3.
오일석 외, “미국과 프랑스 정부의 사이버조기 경보 체계”, 정보보호학회지 제15권 제1호, 2005. 2.
오태곤, “국제범죄 대응을 위한 국제형사경찰기구의 강화방안”, 법학연구 제18집, 정문사, 2005.
_____, “국가간 사이버범죄 대응체계 구축에 관한 연구 : 글로벌 거버넌스적 측면에서”, 한국컴퓨터정보학회논문지 제35호, 한국컴퓨터정보학회, 2005.
_____, “사이버테러리즘의 대응방안에 관한 연구”, 한국콘텐츠학회논문 제5권 제3호, 한국콘텐츠학회, 2005.
우제태, “사이버 범죄의 대응방안에 관한 연구”, 경찰연구논집 제1호, 한국경찰이론과실무학회, 2007.
우형진, 넷 전쟁과 인터넷 보안군, SERI 연구에세이, 삼성경제연구소, 2007.
園田壽, “일본의 사이버범죄와 형사법제”, 공익과 인권 제4권 제2호, 서울대학교 공익인권법연구센터, 2007.
원혜욱, “인터넷범죄의 특징과 범죄유형별 처벌조항”, 형사정책연구 제11권 제2호, 한국형사정책연구원, 2000. 6.

유백준, “사이버범죄의 수사상 문제점과 대책에 관한 연구”, 조선대학교 박사학위논문, 2008.

유석준, “사이버범죄에 대한 외국의 입법례”, 영산법률논집 제5권 제1호, 영산대학교 법률교육연구원, 2008.

유진호/지상호/송혜인/정경호/임종인, “인터넷 침해사고에 대한 피해손실 측정”, 정보화정책 제15권 제1호, 2008년 봄.

이경렬, “디지털 정보 관련 압수수색 규정 도입을 위한 전제적 고찰”, 성균관법학 제21권 제2호, 성균관대학교 법학연구소, 2009.

이경재, “정보화사회에서의 형법적 규제”, 법학연구 제17권 제1호, 충북대학교 법학연구소, 2006.

이동희 외, 국제 사이버범죄 아카데미 모델 개발, 경찰청, 2010.

이보영, “사이버 공간에서의 형법의 임무와 과제”, 법학연구 제36편, 2009. 11.

이상원, “사이버 범죄에 관한 토론문”, Law& Technology:기술과 법에 관한 전문학술지 제5권 제3호, 서울대학교 기술과법센터, 2009.

이상호, “사이버전의 실체와 미래 사이버공격 대응방안 : 7·7사이버공격의 교훈과 대책”, 시대정신 제44호, 시대정신, 2009.

이수현, “인터넷 범죄의 실태와 대응방안”, 법학논고 제25집, 경북대학교 법학연구소, 2006. 12.

이연수, “국가정보의 보호를 위한 사이버안전 법 제도 연구 - 국가 정보보안 법제를 중심으로”, 고려대학교 박사학위논문, 2010. 9

이연수 외, “주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구”, 국가정보연구 제1권 2호, 2008. 12

이원상(역)/Eric Hilgendorf(저), “유럽차원에서의 인터넷 형법 조화의 문제와 경향”, 비교형사법연구 제15호, 한국비교형사법학회, 2006.

이윤호, “e-테러리즘의 효율적 통제방안”, 한국경호학회지 제20호, 2009.

이재은, “국가 사이버위기 관리체계 강화 방안에 관한 연구”, 한국위기관리논집 제4권 제2호, 2008. 12.

이재은 외, 재난관리론, 대영문화사, 2006.

_____, 국가사이버위기 관리 체계 강화 방안에 관한 연구, 국가보안기술연

구소, 2008.

이재은/양기근/류성일, “국가사이버위기 관리체계 강화방안에 관한 연구”, 한국위기관리논집 제4권 제2호, 2008. 12.

이재은/장윤식/김기범/민경식/김인호/박영우/이혜정/김은정, 미래형 사이버범죄 대응 전략연구, 한국정보화진흥원, 2009. 12.

이재진/오태곤, “컴퓨터범죄의 대책에 관한 연구”, 사회과학연구 제31호, 조선대학교 사회과학연구소, 2004.

이정훈, “사이버범죄에 관한 입법동향과 전망”, 사이버커뮤니케이션 학보 제20호, 사이버커뮤니케이션학회, 2006. 12.

_____, “Cyber범죄조약에 대처한 실체법적 대응방안 모색 : 최근 일본의 하이테크범죄에 대한 입법동향을 검토하며”, 중앙법학 제7집 제1호, 중앙법학회, 2005.

이창범, “유럽연합의 정보보안 및 개인정보보호 법제 현황”, 인터넷법률 제38호, 법무부, 2007.

이창수, “초국가적 사이버범죄에 대한 국제공조 활성화방안과 그 선결과제”, 형사법의 신동향 제21호, 대검찰청, 2009.

이창우 외, “통합보안 관리를 위한 침입대응 시스템 설계”, 정보보증논문지 제5권 제2호, 한국사이버테러정보전학회, 2005.

이필중, 전산보안개론 & 전산시스템보안 강의자료, 2005.
http://islab.postech.ac.kr/class/e472&i560/2005/data/1_2.pdf

임병락, “사이버범죄의 학제간 연구를 위한 이해의 기초 : 형법상 규제를 중심으로”, 한국컴퓨터정보학회논문지 제13권 제3호, 한국컴퓨터정보학회, 2008.

임병락/오태곤, “우리 사이버범죄 대응 절차의 문제점에 관한 연구 : 미국의 사이버범죄대응절차법을 중심으로”, 한국컴퓨터정보학회논문지 제11권 제4호, 한국컴퓨터정보학회, 2006.

임종인, 경찰의 차세대 디지털 포렌식 기반 구축방안, 치안정책연구소, 2008.

장광수, “DDos 공격 대응현황 및 대책”, 디지털행정(제113호), 행정안전부 정보화인력개발과, 2009.

전 웅, 국가정보와 안보정책, 한국국제정치학회, 1997.

전지연, “사이버공간에서 형법적 적용범위의 수정·제한”, 법조 제566호, 법조협회, 2003.

_____, “사이버범죄의 과거, 현재 그리고 미래”, 형사법연구 제32호, 한국형사법학회, 2007.

정교일/이병천/진승헌, 훤히 보이는 정보보호, 전자신문사, 2008.

정국환/유지연, 디지털재난 그 의미와 대응의 새로운 패러다임, KISDI 이슈리포트, 2009.

정 완, “사이버범죄의 방지를 위한 국제협력방안”, 형사정책연구 제70호, 한국형사정책연구원, 2007.

_____, “사이버범죄의 주요동향과 형사정책적 과제”, 형사정책연구(제71호), 한국형사정책연구원, 2007.

_____, “사이버범죄의 현상”, 형사정책 제19권 제2호, 한국형사정책학회, 2007.

_____, “사이버범죄의 실태와 동향 및 대응책”, 홍익법학 제10권 제1호, 홍익대학교 법학연구소, 2009.

정윤정/김인중/이철수/임을규/원동호, “기상 예측시스템을 이용한 온라인 침해 예측시스템 설계”, ICCSA 2006, LNCS(SCI-E), 2006. 5.

정정일, “사이버범죄에 대한 국제적 대응방안”, 경호경비연구 제10호, 2005.

정준현, “국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구”, 미국헌법학회, 2009. 9.

정준현/김귀남, “사이버테러 대응체제와 법치주의”, 정보보증논문지 제4권 제3호, 한국사이버테러정보전학회, 2004.

정태석/설동훈, 사이버범죄와 보안의식, IT의 사회·문화적 영향 연구 : 21세기 한국 메가트렌드 시리즈 04-26, 정보통신정책연구원, 2004. 2.

정혜욱, “사이버 범죄와 관할”, 법학논문집 제31집 제2호, 중앙대학교 법학연구소, 2007.

조광래, “정보환경변화시대의 사이버테러 양상 및 대응체계에 관한 연구”, 경호경비연구 제9호, 한국경호경비학회, 2005.

조병인, 사이버경찰에 관한 연구, 한국형사정책연구원, 2000.

조병인/정진수/정완/탁희성, 사이버범죄에 관한 연구, 한국형사정책연구원, 2000. 12.

조성택, “사이버테러의 추세와 관련법·제도에 관한 고찰 : 해킹범죄를 중심으로”, 한국테러학회보 제1권(창간호), 2008.

조호대, “사이버 테러리즘 현황과 정책적 대응”, 한국위기관리논집 제4권 제1호, 위기관리 이론과 실천, 2008.

_____, “사이버테러 대응 방안에 관한 연구”, 한국위기관리논집 제2권 제1호, 2006.

조호대/박동균/조현빈, 사이버침해사고 예방 및 대응을 위한 법·제도적 개선방향, 국회입법조사처, 2007.

조호대/신동일, “공공 및 민간부문의 사이버침해사고 현황분석에 따른 대응방안”, 한국콘텐츠학회논문지, 제9권 제1호, 2009.

주승희, “사이버범죄와 국제형법:추상적 위험범의 범죄지 및 형법 제6조의 적용범위를 중심으로”, 형사정책연구 제63호, 한국형사정책연구원, 2005.

최영호, 컴퓨터와 범죄현상, 컴퓨터출판사, 1995.

최영호, 정보범죄의 현황과 제도적 대처방안, 크라운출판사, 1998.

최정호, “사이버테러리즘의 변천과 법률적 대응”, 경찰학연구 제18호, 경찰대학, 2008.

_____, 사이버테러리즘의 변천방향과 한국의 대응, 2008 국방안보학술회의 발표자료.

최해필, “사이버 시대 군 사이버 전력의 강화방안 연구”, 건양대학교 박사학위논문, 2007.

최호진, “새로운 해킹기법과 관련된 형법적용의 흠결과 해결방안”, 형사정책연구 제72호, 한국형사정책연구원, 2007.

하옥현, “국가 사이버안보체계 구축 전략”, 고려대학교 박사학위논문, 2005.

한국법제연구원, 정보보안관련 법제의 문제점과 개선방안, 2007.

한국인터넷진흥원, 2009 정보보호 실태조사, 2010.

한국인터넷진흥원 인터넷침해대응센터, 인터넷 침해사고 동향 및 분석 월보, 2010. 4.

한국정보보호진흥원, 각국의 정보보호법제 및 집행체계에 관한 연구, 2007.

_____, 미국 사이버범죄 실태조사, 2005.

한국정보사회진흥원, 2007~2010 국가정보화 백서, 2007/2010년.

한국형사정책연구원, 컴퓨터 범죄에 관한 연구, 1993.

허진경, “테러형 사이버범죄와 침해사고 대응”, 한국테러학회 학술회의 자료집, 2009.

현대호, “미국의 사이버위기 관련 법제의 현황과 전망”, 법학논총 제33권 제1호, 2009.

홍승희, “유비쿼터스환경과 사이버범죄”, 형사정책연구 제17권 제3호, 한국형사정책연구원, 2006. 9.

Ⅱ. 외국문헌

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, Januar 2009.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2009_pdf.pdf?__blob=publicationFile

Brenner, Susan W., Cybercrime and the U.S. Criminal Justice System, Global Perpectives in Information Security : legal, social, and international issues, John Wiley & Sons, 2009.

Congressional Research Service, Department of Homeland Security Reorganization : The 2SR Initiative, 2005.

Council of Europe/Economic Crime Division, Guidelines for the cooperation between law enforcement and internet service providers in the investigation of cybercrime, 2008. 4.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf

Harley, Brian, A Global Convention on Cybercrime?, 2010. 3. 23.

http://www.stlr.org/2010/03/a-global-convention-on-cybercrime

Hunton, Paul, The growing phenomenon of crime and the internet : A cybercrime execution and analysis model, Computer Law & Security Review 25, 2009.

Ifrah, Laurence, Cybercrime : current threats and trends, 2008. 3.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study1-d-provisional%20_13%20Mar%2008.pdf

ITU, Understanding Cybercrime : A guide for developing countries (Draft), 2009. 4.
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

Jakobsson, Markus & Zulfikar Ramzan, Crimeware : Understanding New Attacks and Defendses, Addison Wesley Professional, 2008.

Kiefer, Kimberly, Stephen Wu, Ben Wilson & Randy Sabett, Information Security : A Legal, Business, and Technical Handbook, ABA, 2004.

Lewis, James A., The “Korean” Cyber Attacks and Their Implications for Cyber Conflict, Center for Strategic and International Studies, 2009. 10.
http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf

McAfee, Virtual Criminology Report 2009, Virtually Hear : The age of Cyber Walfare, 2009.

Taylor, Digital Crime and Digital Terrorism, Prentice Hall, 2006.

Ye, Nong, Clark Newman & Toni Farley, A System-Fault-Risk Framework for cyber attack classification, Information Knowledge Systems Management 5, 2005/2006.

Whitehouse, National Strategy for Trusted Identities in Cyberspace(NSTIC)-Creating Options for Enhanced Online Security and Privacy(Draft), 2010. 6.

_____, The National Strategy for The Physical Protection of Critical Infrastructure and Key Asset, 2003.

_____, The National Strategy to Secure Cyberspace, 2003.

Wilson, C., Botnets, Cybercrime, and Cyberterrorism, 2008.

情報處理推進機構, 情報セキュリティ白書 2010 - 廣まる脅威·多様化する攻撃、求められる新たな情報セキュリティ對策 -, 2010.8.27.

Ⅲ. 관련 사이트

한국 경찰청 사이버테러대응센터 : http://www.netan.go.kr

한국 국가기록원 : http://www.archives.go.kr

한국 국가정보원 국가사이버안전센터 : http://www.ncsc.go.kr

한국 국가정보원 IT보안인증사무국 : http://www.kecs.go.kr

한국 국방부 국방정보전대응센터 : http://www.dsc.mil.kr

한국 한국인터넷진흥원 인터넷침해사고대응센터 : http://www.krcert.or.kr

한국 한국정보사회진흥원 : http://www.nia.or.kr

미국 국토안보부 : http://www.dhs.gov

미국 법무부 컴퓨터범죄및지적재산국 : http://www.cybercrime.gov

미국 백악관 : http://www.whitehouse.gov

영국 국가기반보호센터 : http://www.cpni.gov.uk

영국 국립 최첨단범죄 수사단 : http://www.nhtcu.org

영국 컴퓨터침해사고 대응팀 : http://www.uniras.gov.uk

영국 통신-전자보안그룹 : http://www.cesg.gov.uk

독일 연방정보기술안전청 : http://www.bsi.bund.de

프랑스 중앙정보시스템보안국 : http://www.ssi.gouv.fr

일본 경찰청 : http://www.npa.go.kr/cyber

일본 경찰청 사이버포스 : http://www.cyberpolice.go.jp/cyberforce

일본내각관방정보보안센터 : http://www.nisc.go.jp

일본 방위성 : http://www.mod.go.jp

일본 총리실 : http://www.kantei.go.jp

Abstract

A Study on the Construction of Efficient System for Safe Cyber space

Kang, Seok Ku · Yoon, Hae Sung · Park, Young-Woo
Kim, Min Ho · Kwon, Hun Yeong · Kim, Do Seung · Kim, Gi Bum

These days, risks of hacking, DDoS attack and other cyber trespass including so called '7·7 DDoS' in 2009 are increasing. In particular, the cyber trespass has disclosed an individual's resident registration number, ID and password, etc to pursue monetary benefit to increase risk more than before, and personal information disclosed has been secretly sold to produce problems. And, cyber trespass against information and communication infrastructure of public organizations is increasing: In particular, hacking against government organization is increasing approximate 300% every year to be likely to paralyze government organizations. For instance, 7·7 DDoS attack in 2009 temporarily paralyzed important web sites of Cheongwadae and financial organizations, and similar cyber attack occurred during same time period this year despite countermeasure. DDoS makes use of zombie PC that has been given malicious codes: So, prompt and effective action cannot be taken.

The government reenacted the Act on Information Promotion to enact the Act on Government Information and to supplement the regulations of government cyber safety control and to check overall legal systems of cyber risk control: And, the Internet Trespass Counteraction Center of the Korea

Internet Security Agency(KISA) controlled private areas, and the Government Cyber Safety Center of the National Intelligence Service(NIS) did government and public organizations and the Cyber Headquarters of the Ministry of Defence did defense areas so that general counteraction system of government, military and private area has been established. Even if the government greatly revised legal system against either cyber trespass, it could not prevent crimes nor detected criminals because of physical, technical and systematic limitations: As a result, not only people but also the government felt uneasy continuously.

The purpose of this study was to build up cyber safety system against cyber crisis that was made because of cyber trespass, cyber attacks and associated crisis. The author researched by sharing roles with other researchers and adopted law methodology and investigated types, current status, comparison and empirical status in multi-sided and three dimensional way.

The theoretical investigation was done based on theory of classification: As a result, fighting rules against cyber war were not enough and counteraction against source of enemy's server and infrastructure was not good. So, the study argued that investment and manpower were needed to protect information at private areas. And, the study investigated legal system of cyber safety based on interpretation of criminal law. The cyber trespass expanded concept of cyber terror and cyber war to exceed level at the enactment of criminal law in 1995, so that conventional interpretation of the criminal law concerning civil commotion and foreign invasion had limitation and new interpretation on traffic obstruction and other public safety was needed.

This study investigated status of counteraction system of cyber trespass of government organizations such as National Intelligence Service (NIS), Korea Communications Commission and Police Agency, etc. Based on analysis on counteraction system of NIS, the study examined legal status of organizations and systems that could play an important role at counteraction, and suggested sharing of information between concerned organizations, improvement of legal

system of forecast and alarm system, researches from point of view of mid-term and long-term and support of budget, recruitment of experienced professionals, actual international cooperation, and build up of national crisis control system, etc. And, based on analysis on counteraction system of Korea Communications Commission, the study suggested improvement and coordination of information, improvement and adjustment of information protection administration, national security oriented information security policy and electronic government, differentiation of information protection policy of e-commerce and other general areas and build up of general command and supervision system based on the President Team.

On the other hand, based on analysis on counteraction system, the study suggested build up of cooperative model of information exchange between counteraction organization of trespass accident and police agency, preliminary detection of follow-up investigation, conversion into early action cyber investigation system, expansion of organization and functions of policy agency as well as local policy agency that could prevent cyber trespass, recruitment of private IT professionals, improvement of punishment laws and regulations of cyber crimes, revision of digital evidence related laws and regulations of the Criminal Procedure Act, development of the program that could solve phenomenon that civilians were reluctant to report, and build up of public security and cyber governance system that university, citizens and non-government organizations, etc. The study investigated international cooperation of cyber investigation. Based on the analysis result, the study suggested establishment of interpol cyber crime center that could play a role at removal of cyber crime in international society. The study investigated counteraction system against cyber attack in advanced countries such as the United States, the UK, Germany, France and Japan by using comparative method. The study compared counteraction system of the United States that was a model case with that of Korea: Legal system that could support

cooperative system between organizations should be made to avoid disturbance of the policy, and R&D policy of national cyber security should be strengthened and local and international anti-terror network should be established and legal system needed to improve it. The empirical analysis investigated national statistics as well as professionals' cognition. The study investigated actual conditions of safety by each type and area based on national statistics: For instance, malicious code hidden of homepage that attempted to attack application programs, threat by malicious code that aimed at obtaining of monetary benefits, distribution of malicious codes by using social issue and events, technology that could prevent high level of analysis, automation tools that could produce large quantity of malicious code, and threat of cyber trespass from foreign countries, etc. And, the study investigated cognition of working staffs of information and security of public organizations to find out problems: for instance, low standards deciding upon either safety or crisis at practical affairs, difficulties at build up of high cost information security system at private sector, environment that could threaten cyber safety in accordance with use of Internet real name identification system and other identification system, and inefficiency of weighted punishment against critical cyber trespass, etc.

Furthermore, degree of cyber risk could be tested to differentiate counteraction system of cyber risks. The study suggested ‘national cyber crisis control’ based on NIS subject to not only 'connection program with national disaster control system' but also cyber crisis environment to build up national cyber risk control system. And, to build up cyber safety environment and expand infrastructure, the study suggested training and recruitment of professionals and experts, research and development, budgeting for information protection, and lessening of collection and storage of unnecessary personal information. The study suggested cyber investigation system based on policy agency's analysis on counteraction system, and raised problem of unification of

first investigation on-the-spot that could attain efficiency.

The study examined discussion and alternatives to build up cyber safety system. In the 21st century, cyber safety has been important because of rapid change of scientific technology and communication environment. And, uneasiness and unknown risks exist because of rapid changes of environment. State-of-the-art area was discussed and associated systems and technologies were not equipped enough. The university and practical working groups should research and develop policies to find out intelligent counteractions on exceptional limitation one by one to overcome uneasiness and crisis of both people and the government.

부록

부록 1. 국가사이버안전관리규정

[시행 2010. 4.16] [대통령훈령 제267호, 2010. 4.16, 일부개정]

제1조(목적) 이 훈령은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다.

제2조(정의) 이 훈령에서 사용하는 용어의 정의는 다음과 같다. 〈개정 2008.8.18〉

1. “정보통신망”이라 함은 「전기통신기본법」 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. “사이버공격”이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.
3. “사이버안전”이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.
4. “공공기관”이라 함은 다음 각목의 기관을 말한다.
   가. 「공공기관의 운영에 관한 법률」 제5조에 따라 지정된 공기업 또는 준정부기관인 공공기관
   나. 「공공기관의 운영에 관한 법률」 제5조에 따라 지정된 기타공공기관 중 「정부출연연구기 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따른 연구기관

다. 「초·중등교육법」 및 「고등교육법」에 따른 국·공립학교

라. 그 밖에 다른 법령의 규정에 의하여 설립된 공공기관 중 제6조의 규정에 의한 국가사이버안전전략회의에서 정보통신망의 안전성 확보가 필요하다고 지정한 기관

제3조(적용범위) 이 훈령은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대하여 이를 적용한다. 다만, 「정보통신기반보호법」 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대하여는 적용하지 아니한다.

제4조(사이버안전 확보의 책무) ① 중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임이 있으며 이를 위하여 사이버안전업무를 전담하는 전문인력을 확보하는 등 필요한 조치를 강구하여야 한다.

② 관계 중앙행정기관의 장은 소관 공공기관 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 전문인력의 확보 등 필요한 조치를 강구하도록 하여야 한다.

제5조(국가사이버안전정책 및 관리) 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다.

제6조(국가사이버안전전략회의) ① 국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의(이하 "전략회의"라 한다)를 둔다.

② 전략회의의 의장은 국가정보원장이 된다.

③ 전략회의의 위원은 교육과학기술부차관·외교통상부차관·법무부차관·국방부차관·행정안전부차관·지식경제부차관·보건복지부차관·국토해양부차관·대통령실 외교안보수석비서관·방송통신위원회 상임위원·금융위원회 부위원장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 한다. 〈개정 2008.8.18, 2010.4.16〉

④ 전략회의는 다음 각호의 사항을 심의한다.

1. 국가사이버안전체계의 수립 및 개선에 관한 사항
2. 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항
3. 국가사이버안전 관련 대통령 지시사항에 대한 조치방안
4. 그 밖에 전략회의 의장이 부의하는 사항

⑤ 전략회의의 구성·운영 등에 관하여 필요한 사항은 전략회의의 의장이 따로 정한다.

제7조(국가사이버안전대책회의) ① 전략회의의 효율적인 운영을 위하여 전략회의에 국가사이버안전대책회의(이하 "대책회의"라 한다)를 둔다.

② 대책회의의 의장은 국가정보원의 사이버안전업무를 담당하는 차장이 되며, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 한다.

③ 대책회의는 다음 각호의 사항을 심의한다.

1. 국가사이버안전 관리 및 대책방안
2. 전략회의의 결정사항에 대한 시행방안
3. 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항
4. 그 밖에 대책회의의 의장이 부의하는 사항

④ 대책회의의 구성·운영 등에 관하여 필요한 사항은 대책회의의 의장이 따로 정한다.

제8조(국가사이버안전센터) ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 "사이버안전센터"라 한다)를 둔다.

② 사이버안전센터는 다음 각호의 업무를 수행한다.

1. 국가사이버안전정책의 수립
2. 전략회의 및 대책회의의 운영에 대한 지원
3. 사이버위협 관련 정보의 수집·분석·전파
4. 국가정보통신망의 안전성 확인
5. 국가사이버안전매뉴얼의 작성·배표
6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원
7. 외국과의 사이버위협 관련 정보의 협력

③ 국가정보원장은 사이버안전센터의 업무 수행과 관련하여 필요하다고 인정하는 경우에는 관계 중앙행정기관의 장에게 소속 공무원 및 전문요원의 파견을 요청할 수 있다.

제9조(사이버안전대책의 수립·시행 등) ① 중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 한다.

② 관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 사이버안전대책을 수립·시행하도록 할 수 있다.

③ 국가정보원장은 제1항 내지 제2항의 규정에 의한 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼을 작성 배포할 수 있다. 다만, 국가사이버안전매뉴얼을 작성하는 경우에는 미리 관계 중앙행정기관의 장과 협의하여야 한다.

④ 국가정보원장은 제1항 내지 제2항의 규정에 의한 사이버안전대책의 이행여부 등 정보통신망에 대한 안전성을 확인할 수 있으며 필요하다고 인정하는 경우에는 해당 중앙행정기관의 장에게 시정 등 필요한 조치를 권고할 수 있다. 다만, 지방자치단체 및 공공기관의 정보통신망에 대한 안전성 확인은 관계 중앙행정기관의 장과 협의하여 수행한다.

제10조(사이버공격과 관련한 정보의 협력) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가정보원장에게 통보하여야 한다.

② 국가정보원장은 제1항의 규정에 의하여 관련 정보를 제공받은 경우에는 대응에 필요한 조치를 강구하고 그 결과를 정보를 제공한 해당기관의 장에게 통지한다.

제10조의2(보안관제센터의 설치·운영) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 설치·운영하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 다른 중앙행정기관(국가정보원을 포함한다)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다.

② 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다.

③ 보안관제센터를 설치·운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다.

④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 지식경제부장관이 지정하는 보안관제전문업체의 인원을 파견받아 보안관제업무를 수행하도록 할 수 있다. 이 경우 보안관제전문업체의 지정·관리 등에 필요한 사항은 지식경제부장관이 국가정보원장과 협의하여 정한다.

⑤ 제1항의 보안관제센터의 설치·운영 및 제2항의 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.

[본조신설 2010.4.16]

제11조(경보 발령) ① 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를 발령할 수 있다. 다만, 민간분야에 대하여는 방송통신위원회위원장이 경보를 발령하며, 국가정보원장과 방송통신위원회위원장관은 국가차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 발령 전에 상호 교환하여야 한다. 〈개정 2008.8.18〉

② 제1항의 규정에 의하여 경보를 발령하였을 때에는 관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장에게 이를 신속히 전파하고 적절한 조치를 취하여야 한다.

③ 국가정보원장은 사이버공격이 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우에는 대통령실의 국가위기상황업무를 담당하는 수석비서관과 협의하여 심각 수준의 경보를 발령할 수 있다. 〈개정 2008.8.18〉

④ 국가정보원장은 제1항의 규정에 의한 경보 발령에 필요한 정보를 관계 중앙행정기관의 장에게 요청할 수 있다. 이 경우 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제12조(사고통보 및 복구) ① 중앙행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체없이 그 사실을 국가정보원장에게 통보하여야 한다.

② 공공기관 및 지방자치단체의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 관계 중앙행정기관의 장에게 통보하고, 관계 중앙행정기관의 장은 이를 지체없이 국가

정보원장에게 통보하여야 한다.

③ 국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 제1항 및 제2항의 규정에 의한 통보를 받은 때에는 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있으며, 요청받은 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제13조(사고조사 및 처리) ① 국가정보원장은 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 해당 기관의 장이 자체적으로 조사하게 할 수 있으며, 이 경우 해당 기관의 장은 사고개요 및 조치내용 등 관련 사항을 국가정보원장에게 통보하여야 한다.

② 국가정보원장은 제1항의 규정에 의하여 조사한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다.

③ 국가정보원장은 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우에는 관계 중앙행정기관의 장과 협의하여 범정부적 사이버위기 대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다. 〈개정 2010.4.16〉

④ 사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위하여 대책본부 내에 합동조사팀 등 필요한 하부기구를 둘 수 있다. 이 경우 하부기구의 구성·운영 등에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다. 〈신설 2010.4.16〉

⑤ 국가정보원장은 제4항에 따른 사고조사 및 피해복구 등의 조치를 위하여 관계 중앙행정기관의 장에게 필요한 인력·장비 및 관련 자료의 지원을 요청할 수 있다. 〈개정 2010.4.16〉

제14조(전문기관간 협력) ① 사이버안전업무를 전담하는 전문기구를 운영하는 기관은 국가사이버안전업무를 효율적으로 수행하기 위하여 다음 각호의 사항을 상호 긴밀히 협력하여야 한다.

1. 사이버위협 관련 정보의 탐지 및 정보공유체계의 구축·운영
2. 사이버안전 관련 정보의 분석·전파

3. 사이버안전 위해 요소에 대한 조치방안
4. 공격기법 분석 및 공격차단 등 대응방안
5. 그 밖에 경보의 수준별 세부 대응조치 등 필요한 사항

② 사이버안전센터장은 제1항의 규정에 의한 전문기구를 운영하는 기관간 협력을 원활하게 하기 위하여 관계전문가 회의를 소집할 수 있다.

제15조(연구개발) ① 국가정보원장은 국가사이버안전에 필요한 기술개발과 기술수준의 향상을 위하여 필요한 시책을 추진할 수 있다.

② 중앙행정기관의 장은 공공분야의 사이버안전 관련 기술의 확보를 위하여 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항의 규정에 의하여 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소로 하여금 관련 연구개발을 수행(연구개발을 위하여 보안관제업무를 수행하는 것을 포함한다)하게 할 수 있다. 〈개정 2010.4.16〉

③ 제2항의 규정에 의한 사이버안전에 필요한 기술의 연구개발에 관한 세부사항은 국가정보원장이 따로 정한다.

제16조(인력양성 및 교육홍보) ① 관계 중앙행정기관의 장은 사이버안전의 기반 조성에 필요한 기술인력을 양성하고 국민의 인식제고를 위하여 다음 각호의 시책을 강구하여야 한다.

1. 사이버안전 관련 전문기술인력의 확보 및 양성
2. 사이버안전 교육프로그램의 개발 및 투자
3. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항

② 국가정보원장은 관계 중앙행정기관의 장이 사이버안전과 관련한 전문인력의 양성, 교육 및 홍보를 위하여 필요한 지원을 요청하는 경우 이에 대하여 지원할 수 있다.

제17조(예산) 중앙행정기관의 장은 소관분야와 관련된 사이버안전대책의 수립·시행에 필요한 재정상의 조치를 강구하여야 한다.

제18조(안전성 확인 등에 대한 특례) ① 제9조, 제11조 내지 제13조의 규정에 불구하고 국방분야의 사이버안전과 관련한 다음 각호에 대하여는 국방부장관이 그 업무를 수행한다.

1. 제9조제4항의 규정에 의한 안전성 확인

2. 제11조제1항의 규정에 의한 경보 발령
3. 제12조제1항의 규정에 의한 사고통보
4. 제13조제1항의 규정에 의한 사고조사

② 국방부장관은 제1항의 규정에 의한 업무를 수행함에 있어 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

부칙 〈제00267호, 2010. 4.16〉

이 훈령은 발령한 날부터 시행한다.

부록 2. 국가사이버위기 관리법(안)

제1조(목적) 이 법은 국가차원에서 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 국가 역량을 결집하여 신속히 대처함으로써 국가의 안전보장과 이익보호에 이바지함을 목적으로 한다.

제2조(정의) ① 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “사이버공격”이라 함은 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 누출·훼손·왜곡전파 하는 모든 공격행위를 말한다.
2. “사이버위기”라 함은 사이버공격으로 인하여 국가·사회기능에 심각한 지장을 초래하거나 피해가 전국적으로 확산될 가능성이 있는 경우를 말한다.
3. “사이버위기경보”라 함은 사이버공격의 징후를 식별하거나 사이버위기발생이 예상되는 경우 그 위험 또는 위협수준에 부합되는 조치를 할 수 있도록 미리 정보를 제공하고 경고하는 것을 말한다.
4. “사이버위기관리”라 함은 사이버위기를 체계적으로 관리하기 위한 탐지·대응·사고조사·복구·훈련·경보발령 및 관계기관 간의 협조 등 국가차원의 모든 활동을 말한다.
5. “위기관리책임기관(이하 “책임기관”이라 한다)”이라 함은 사이버위기관리 업무를 행하는 다음 각 목의 기관을 말한다.
   가. 「대한민국헌법」, 「정부조직법」, 그 밖의 법령에 따라 설치된 국가기관과 지방자치단체 및 공공기관
   나. 「정보통신기반보호법」 제8조에 따른 주요정보통신기반시설을 관리하는 기관
   다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설사업자 및 제46조의3제1항제1호에 따른 주요정보통신서비스 제공자
   라. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관

6. “위기관리지원기관(이하 “지원기관”이라 한다)” 이라 함은 사이버공격에 대한 신속한 탐지·대응 및 사고조사·복구 등을 지원하는 다음 각 목의 기관 또는 업체를 말한다.
   가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원
   나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원
   다. 「소프트웨어산업진흥법」 제24조에 따라 소프트웨어사업자로 신고한 자 중 컴퓨터바이러스 백신소프트웨어를 제작 또는 판매하는 자
   라. 「정보통신기반보호법」 제17조에 따라 지정된 정보보호 컨설팅전문업체
   마. 지식경제부장관이 지정한 보안관제전문업체

② 이 법에서 사용하는 용어의 정의는 제1항에서 정하는 것을 제외하고는 「정보통신기반보호법」·「정보통신망 이용촉진 및 정보보호 등에 관한 법률」·「정보화촉진기본법」·「전기통신사업법」에서 정하는 바에 따른다.

제3조(다른 법률과의 관계) 사이버위기관리에 관하여 「재난 및 안전관리기본법」과 그 밖의 다른 법률에 우선하여 적용한다.

제4조(국가사이버안전센터의 설치) ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응과 사이버위기관리를 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 “안전센터”라 한다)를 둔다.

② 안전센터의 조직과 운영에 관한 사항은 국가정보원장이 정한다.

③ 국가정보원장은 제1항의 안전센터를 운영함에 있어 필요한 경우 제2조제1항제5호가목의 책임기관의 장에게 인력의 파견과 장비의 지원을 요청할 수 있다.

제5조(민·관 협의체의 구성) ① 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련정보를 상호 공유하기 위하여 민·관 협의체를 구성·운영할 수 있다.

② 제1항에 관하여 필요한 사항 등은 대통령령으로 정한다.

제6조(국가사이버위기 관리종합계획 수립 등) ① 국가정보원장은 대통령령으로 정하는 바에 따라 국가사이버위기 관리종합계획을 수립하고 이에 따라 위기관리기본지침(이하 “위기관리지침”이라 한다)을 작성하여 책임기관의 장에게 배포하여야 한다.

② 책임기관의 장은 제1항의 위기관리지침에 따라 세부지침을 수립·시행하여야 한다.

제7조(위기관리지침의 이행 확인 및 국회 보고) ① 중앙행정기관의 장은 소관 책임기관에 대하여 제6조제2항의 세부지침의 이행여부를 확인할 수 있다.

② 국가정보원장은 제2조제1항제5호가목의 책임기관에 대하여 제6조제2항의 세부지침의 이행여부를 점검·평가할 수 있고, 이를 제1항의 확인결과와 종합하여 매년 국회에 제출하여야 한다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회에 대한 점검·평가는 국회사무총장, 법원행정처장, 헌법재판소사무처장, 중앙선거관리위원회사무총장이 국가정보원장에게 요청한 경우에 한한다.

③ 제1항 및 제2항의 절차와 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제8조(보안관제센터의 설치) ① 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축·운영하거나 다음 각 호의 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 한다. 다만, 「정보통신기반보호법」 제16조에 따른 정보공유·분석센터는 보안관제센터로 본다.

1. 관계 중앙행정기관
2. 국가정보원
3. 제2조제1항제6호마목의 보안관제전문업체

② 책임기관의 장은 탐지된 사이버공격 정보를 즉시 관계 중앙행정기관의 장 및 국가정보원장에게 제공하여야 하며, 국가정보원장은 이를 종합·분석하여 대책을 수립·지원하여야 한다.

③ 누구든지 제2항에 따라 제공받은 정보에 대해서는 사이버위기관리를 위하여 필요한 범위에 한하여 정당하게 사용하여야 한다.

④ 보안관제센터의 구축·운영 및 보안관리 등에 관한 기준과 탐지된 사이버공격 정보의 제공에 관한 범위·절차·방법 등에 관한 사항은 대통령령으로 정한다.

제9조(대응 활동) ① 책임기관의 장은 사이버공격 정보를 탐지하여 사이버위기 발생 가능성을 조기에 차단·예방하는 등 피해를 최소화하기 위하여 신속한 대응조치를 취하여야 한다.

② 책임기관의 장이 제1항의 업무를 수행함에 있어 필요한 경우 관계 중앙행정기관의 장 및 국가정보원장에게 지원을 요청할 수 있다.

③ 관계 중앙행정기관의 장 및 국가정보원장은 제2항에 따른 지원을 요청받았을 때 신속한 대응이 이루어질 수 있도록 기술지원 등 필요한 조치를 하여야 한다.

④ 제3항에 따른 조치를 위하여 관계 중앙행정기관의 장 및 국가정보원장은 해당 지원기관의 장에게 필요한 지원을 요청할 수 있으며 이 경우 지원기관의 장에게 지원할 내용과 기간을 미리 통보하여야 한다.

⑤ 관계 중앙행정기관의 장 및 국가정보원장은 제4항에 따른 필요한 지원을 한 기관의 장에게 그 소요경비를 지원할 수 있으며, 소요경비의 지원절차·방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제10조(사고조사) ① 책임기관의 장은 사이버공격으로 인하여 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하고, 그 결과를 즉시 관계 중앙행정기관의 장 및 국가정보원장에게 통보하여야 한다.

② 국가정보원장은 제1항에 따른 사고조사결과가 미흡하거나 국가안보 및 이익에 중대한 영향을 미친다고 판단되는 경우 직접 그 사고조사를 실시할 수 있다.

③ 국가정보원장은 제2항에 따라 사고조사를 한 결과, 피해의 복구 및 확산방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

④ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사이버공격과 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

제11조(훈련) ① 정부는 사이버위기에 체계적이고 효율적으로 대응하기 위하여 훈련

을 실시하여야 한다.

② 제1항의 훈련은 매년 정기 또는 수시로 구분하여 실시할 수 있으며, 정기 훈련은 「비상대비자원관리법」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.

③ 제1항의 훈련 실시방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제12조(사이버위기경보의 발령) ① 국가정보원장은 사이버공격에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 제8조제2항에 따라 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있다.

② 책임기관의 장은 제1항에 따른 사이버위기경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 취하여야 한다.

③ 사이버위기경보 발령의 절차·기준 및 책임기관의 장의 조치 등에 관하여 필요한 사항은 대통령령으로 정한다.

제13조(사이버위기대책본부의 구성) ① 정부는 심각단계의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 조치를 취하기 위하여 국가역량을 결집한 사이버위기대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다.

② 대책본부의 장(이하 "대책본부장"이라 한다)은 국가정보원장으로 하며, 대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

③ 대책본부장은 제1항에 따른 대책본부를 구성·운영하기 위하여 책임기관 및 지원기관의 장에게 필요한 인력의 파견 및 장비의 제공을 요청할 수 있다. 이 경우 책임기관 및 지원기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

④ 대책본부장은 제3항에 따라 인력의 파견 및 장비의 제공을 한 기관의 장에게 그 소요경비를 지원할 수 있다.

제14조(연구개발) ① 중앙행정기관의 장 및 국가정보원장은 사이버위기관리에 필요한 기술개발과 기술수준의 향상을 위하여 필요한 시책을 추진할 수 있다.

② 국가정보원장은 제1항에 따라 연구소를 설립하거나, 다른 법령에 의하여 설립

된 기관을 전문기관으로 지정할 수 있다.

③ 사이버위기관리 기술의 연구개발에 관한 절차·방법 등 세부사항은 국가정보원장이 따로 정한다.

제15조(책임기관 간의 기술 이전) 사이버위기관리에 관하여 필요한 기술과 장비 등을 보유한 책임기관은 그러하지 아니한 책임기관에 대하여 기술의 이전 등 그 밖에 필요한 사항을 지원할 수 있다.

제16조(국제협력) 정부는 사이버위기관리에 관하여 국제기구·단체 및 외국과의 협력을 증진하기 위하여 다음 각 호의 업무를 수행할 수 있다.

1. 사이버위기관리를 위한 상호간 협력체계 구축
2. 사이버위기관리 기술에 관한 정보의 교류와 공동대응
3. 사이버위기관리 전담인력의 상호간 파견교육

제17조(비밀 엄수의 의무) 이 법에 따라 사이버위기관리 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.

제18조(포상 등) ① 책임기관의 장은 사이버위기관리와 관련하여 다음 각 호의 어느 하나에 해당하는 자에 대하여 포상하고, 예산의 범위에서 포상금을 지급할 수 있다.

1. 사이버공격 기도에 관한 정보를 제공한 자
2. 사이버공격을 가한 자를 신고한 자
3. 사이버공격의 탐지 및 대응·복구에 공이 많은 자

② 제1항에 따른 포상과 포상금 지급의 기준·방법과 절차, 구체적인 지급액 등 필요한 사항은 대통령령으로 정한다.

제19조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제10조제4항을 위반한 자

2. 제17조를 위반한 자

제20조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자는 2천만원 이하의 과태료에 처한다.

1. 제8조제1항을 위반한 자
2. 제12조제2항을 위반한 자

② 다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에 처한다.

1. 제9조제1항을 위반한 자
2. 제10조제3항을 위반한 자

③ 제1항 및 제2항에 따른 과태료는 대통령령이 정하는 바에 따라 국가정보원장이 부과·징수한다.

부 칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(보안관제전문업체에 대한 경과조치) 이 법 시행 당시 책임기관에 제8조제1항의 보안관제센터 업무를 제공하고 있는 업체는 이 법 시행일부터 6개월 내에 지식경제부장관에게 보안관제전문업체로 지정 받아야 한다.

부록 3. 사이버침해 사고 예방 및 대응 기법

제1절 악성코드 방지 대책

1. 악성코드 관리

가. 악성코드 관리 절차

악성코드[250]로 인한 피해를 최소화하기 위해 사용자와 정보보안담당관은 다음의 사항을 준수해야 한다.

① 비 인가된 소프트웨어 및 불법 소프트웨어 사용을 금지한다.

② 외부 네트워크나 매체로부터 파일이나 소프트웨어를 다운로드 받을 경우 백신 프로그램을 적용한 후 사용한다.

③ 백신 프로그램을 설치하고 정기적으로 업데이트를 수행한다.

④ 중요한 업무 프로세스를 지원하는 시스템의 소프트웨어 및 데이터는 주기적으로 점검하여 허가되지 않은 파일이나 수정사항 등이 있는지 조사한다.

⑤ 전자우편 첨부 파일에 대한 악성코드 감염여부를 점검한다.

⑥ 소프트웨어가 악성코드에 감염되는 것을 방지하기 위해 원본 소프트웨어는 쓰기 방지가 되어 있어야 한다.

⑦ 시스템의 악성코드 감염 시 즉각 정보보안담당관에게 통지한다.

⑧ 정보보안담당관은 악성코드 공격에 의한 피해를 복구하기 위한 적절한 백업, 복구계획을 수립한다.

⑨ 악성 소프트웨어와 관련된 정보(잡지, 바이러스[251] 백신 업체 등) 를 확인하

250) 악성코드 : 데이터를 파괴시킬 목적으로 암암리에 다른 프로그램에 삽입되어 파괴적이거나 침입적인 프로그램을 실행시키거나, 피해자의 데이터 보안성 또는 무결성을 손상시키는 프로그램을 가리킨다. 일반적으로, 악성 코드는 시스템의 사용자가 알지 못하는 상태에서 이러한 부정한 기능을 수행하기 위한 것이다. 악성 코드 공격은 바이러스, 트로이 목마, 웜, 이동 코드(mobile code), 블렌드(blended) 등 5가지 범주로 나뉘어질 수 있다.

251) 바이러스 : 자기 복제 즉, 자신의 복사본을 만드는 것과 복사본을 다른 파일, 프로그램 또는 컴퓨터에 배포하는 것을 목적으로 한다. 바이러스는 일반적으로 감염된 프로그램이 사용자의 상호작용(예를 들면, 파일 열기, 프로그램 실행, 첨부 파일 클릭)에 의해 실행되는 경우 호스트 프로그램에

는 절차를 수행한다.

⑩ 네트워크상의 파일 서버에 대한 관리책임을 명확히 하며, 주기적으로 점검하여 불법 소프트웨어 및 악성 소프트웨어(바이러스, 백도어 포함)에 대한 탐지를 수행한다.

⑪ 악성 소프트웨어에 대한 새로운 정보 및 보호 대책에 대해 사용자에게 주기적 혹은 수시로 공지를 수행한다.

나. 사고 예방

① 백신 프로그램을 이용한다. 백신 프로그램은 악성 코드의 위협을 퇴치하고 피해를 제한하는데 있어서 필수적이다. 이 소프트웨어는 모든 정보시스템에서 실행되어야 하며, 최신 위협이 제거될 수 있도록 지속적으로 최신 상태를 유지되어야 한다. 백신 프로그램은 다운로드 되고, 실행되는 각 파일에 대한 실시간 스캔뿐만 아니라 정기적인 시스템 스캔도 수행하도록 구성되어 있어야 한다. 또한, 감염된 파일을 복구하고 격리하도록 해야 한다. 백신 프로그램은 바이러스, 웜[252], 트로이 목마[253] 등을 찾아낼 뿐만 아니라 악의

삽입되고 전파된다. 바이러스는 다양한 목적을 갖는다. 즉, 일부는 성가시게 하는 장난을 위한 것인 반면, 다른 것은 파괴적인 목적을 갖는다. 일부 바이러스는 은밀한 파괴 기능을 수행하면서도 장난인 것처럼 보인다. 바이러스의 범주에는 파일 감염자 바이러스, 부트 섹터(boot sector) 바이러스, 매크로(macro) 바이러스, 바이러스 혹스(virus hoax) 등이 포함된다.

252) 웜은 피해자를 감염시키기 위한 호스트 프로그램을 필요로 하지 않는 완전한 자기 내장형 자가 복제 프로그램이다. 웜은 자체적으로 전파(self-propagating)되며, 바이러스와는 달리 기능적 복사를 완전하게 생성하며 사용자의 개입 없이도 스스로를 실행할 수 있다. 웜은 개방형 윈도우 공유 등과 같이 알려진 취약점과 구성 약점을 이용한다. 웜의 성격은 웜이 순식간에 전세계적으로 확산되도록 한다는 점이다. 웜의 예로는 Blaster 웜과 SQL Slammer 웜 등을 들 수 있다.

253) 그리스 신화의 목마로부터 명칭이 유래된 트로이 목마(Trojan horse)는 선의적인 것처럼 보이지만 실제로는 악의적인 목적을 숨기고 있는 프로그램이다. 일부 트로이 목마는 시스템 상의 기존 파일을 악성 버전으로 완전하게 대체하는 반면, 다른 트로이 목마는 정상적인 것(예를 들면, 다운로드가 가능한 게임)처럼 보이지만 실제로는 전혀 다른 것(예를 들면, 게임과 비밀번호 스니퍼)이다. 트로이 목마는 대개 유용한 기능을 수행하는 것처럼 보이기 때문에 탐지하기가 어렵다. 트로이 목마는 다음 3가지 모델 중 하나로 분류된다. 첫째, 원래 프로그램의 기능을 계속 수행하면서 추가적으로 별도의 악의적인 활동을 수행하는 것이다. 둘째, 원래 프로그램의 기능을 계속 수행하지만 악의적인 활동(예를 들면, 비밀번호를 수집하는 로그인 프로그램의 트로이 목마 버전)을 수행하거나 기타 악의적인 활동을 가장(예를 들면, 악의적인 특정 프로세스를 표시하지 않는 프로세스 목록 작성 프로그램(process listing

적인 컨텐츠 HTML, ActiveX, JavaScript 및 기타 유형의 악성 코드를 검사할 수 있어야 한다.

② 의심스러운 파일을 차단한다. 악성 코드와 관련되는 파일 확장자(예를 들면, .pif, .vbs)와 의심스러운 파일 확장자의 조합(예를 들면, .txt.vbs, .htm.exe)을 갖는 첨부 파일을 차단하도록 이메일 서버 및 클라이언트를 구성한다.

③ 파일 전송 기능을 가진 불필요한 프로그램의 사용을 제한한다. 이러한 예로는 peer-to-peer 파일, 음악 공유 프로그램, 인스턴트 메시징 소프트웨어, 대화방(IRC) 클라이언트 및 서버 등을 들 수 있다. 이러한 프로그램은 대개 사용자 사이에서 악성 코드를 확산시키는데 이용된다.

④ 사용자가 의심스러운 첨부 파일 또는 알려지지 않은 발신지로부터 발송된 첨부 파일을 열어서는 안 되도록 교육을 강화한다. 사용자는 또한 발신자를 알고 있다고 해서 첨부 파일이 감염되지 않았다고 추측해서는 안된다. 발신자는 파일로부터 이메일 주소를 추출하여 악성 코드를 발송할 수 있는 악성 코드에 자신의 시스템이 감염되었다는 것을 알지 못할 수도 있다. 이러한 활동은 이메일이 그러한 이메일이 발송되었다는 것 조차도 모르는 신뢰할 수 있는 사람으로부터 발신된다는 인상을 준다. 사용자는 절대 열어서는 안 되는 파일 형식(예를 들면, .bat, .com, .exe, .pif, .vbs)에 대해서도 교육을 받아야 한다.

⑤ 윈도우 공유를 제거한다. 대부분의 웜은 윈도우를 실행하는 호스트 상의 안전하지 않은 공유를 통해 확산된다. 조직의 호스트 1 대가 웜에 감염되는 경우, 안전하지 않은 공유를 통해 기관 내부의 수 백 또는 수 천 대에 달하는 호스트에 급속하게 확산될 수 있다. 기관은 모든 호스트의 개방형 공유에 대해 일상적으로 검사하고, 시스템 소유자에게 공유를 적절하게 보호하도록 지시하여야 한다.

⑥ 악성 코드를 제한하기 위해 웹 브라우저 보안을 이용한다. 모든 웹 브라우저는 서명되지 않은(unsigned) ActiveX와 기타 이동 코드 전달 수단이 로컬

program)의 트로이 목마 버전)하기 위해 기능을 변경시키는 것이다. 셋째, 원래 프로그램의 기능을 완전하게 대체하는 악의적인 기능을 수행하는 것이다.

시스템에서 알지 못하는 사이에 다운로드되고 실행되지 않도록 구성된 보안 설정을 갖도록 한다.

⑦ 이메일 클라이언트가 더 안전하게 동작하도록 구성한다. 조직 전체의 이메일 클라이언트는 무의식 중에 감염이 이루어질 수 있는 행동을 피하도록 구성되어야 한다. 예를 들면, 이메일 클라이언트가 자동으로 첨부 파일을 실행해서는 안된다.

2. 불필요한 서비스를 제한

가. r 명령어의 사용

Telnet과 FTP를 사용 할 수 있으면, r 명령어의 사용을 금한다. 단, 업무상의 필요가 있는 경우, 정보보안담당관의 동의하에 다음과 같은 보안상의 제약 사항을 준수하여 운영한다.

① r 명령어의 사용을 위해서는 신뢰 관계에 있는 타 시스템의 보안을 같거나 높은 수준으로 유지할 수 있도록 한다.

② 신뢰할 수 있는 시스템은 목록을 만들어 유지하며, 그 수를 최소로 한다.

③ /.rhosts나 hosts.equiv와 hosts.lpd 등의 파일을 검사할 때 다음 사항을 따른다.

(가) .rhosts 및 hosts.equiv 파일의 권한은 600으로 한다.

(나) .rhosts 파일 내에 '+' 항목을 가지면 안된다.

(다) .rhosts의 경우 원칙적으로 Netgroup Option의 사용을 허용하지 않으며, 부득이한 경우 사용자 계정 이름이나 신뢰할 수 있는 시스템의 이름만을 가지도록 한다.

(라) 시스템관리자는 개인 사용자 홈 디렉토리의 .rhosts파일의 변조 유무 등에 대해 주간 단위로 점검한다.

나. 네트워크 서비스

① /etc/inetd.conf에서 사용하지 않거나 불필요한 서비스를 삭제한다.

(가) TFTP(trivial FTP)를 사용하지 않는다.

(나) fingerd를 사용하지 않는다.

(다) rexecd를 사용하지 않는다.

② portmapper에서 불필요한 서비스를 삭제한다.

다. NFS (네트워크 파일시스템)

① 가능하면 NFS를 사용하지 않는다.

② NFS를 사용하는 상대 시스템은 같은 정도로 보호되는 시스템으로 한정한다.

③ NFS를 사용하는 상대 시스템은 PC가 될 수 없다.

④ 침입차단시스템 정책설정 시 111, 2049 포트를 막아서 외부에서 NFS를 사용하지 못하도록 한다.

⑤ 구성 파일(exports나 dfstab 파일)에서 최소한의 디렉토리만 Export하도록 설정한다.

⑥ 쓰기가 필요 없는 파일시스템은 -ro 옵션을 사용하여 읽기 전용으로 Export 한다.

⑦ 구성 파일이 'localhost' 항목을 가지지 않도록 한다. 구성 파일 내의 호스트 이름은 도메인 이름을 붙여 사용하며, 구성 파일 내의 각 줄이 256 문자를 넘지 않도록 하여 외부의 모든 호스트를 신뢰하는 결과를 초래하지 않도록 한다.

⑧ 가능하면 Nosuid 옵션을 사용하여 Setuid 파일을 클라이언트에서 사용 못하게 한다.

⑨ 구성 파일의 변경 후 exportfs 를 실행하여 실효가 있도록 한다.

⑩ "showmount -e"를 사용하여 어떤 파일시스템이 개방되는지 확인하고, fsirand 을 전 파일시스템에 대해 실행한다.

라. NIS/YP(Network Information Service / Yellow Page)

① 가능하면 NIS를 사용하지 않거나 NIS+를 사용한다.

② SUN 기종은 portmap과 rpcbind를 새로 설치하여, 접속 할수 있는 시스템을 제한한다.

③ NIS Master Server의 /etc/passwd와 /etc/yp/passwd에 '+::0:0::' 항목을 넣어서는 안된다.

④ NIS Client들은 /etc/passwd에 +user,-user,-@netgroup을 사용하여 이용자를 최소한으로 선택한다.

마. Sendmail

① Sendmail은 주기적으로 가장 최신 패치를 적용해야 한다.

② Wizard 옵션을 지원하지 않는 Sendmail을 사용하거나, Wizard Option을 사용하지 않는다.

③ Debug 옵션을 지원하지 않는 Sendmail을 사용하거나, Debug Option을 사용하지 않는다.

④ aliases 파일에 postmaster의 Alias가 있는가 확인하고, 없으면 만들어 넣는다.

⑤ aliases 파일에서 "decode"나 "uudecode" alias를 제거한다.

⑥ aliases 파일에 정의되어 실행되는 모든 프로그램의 사용권한은 755, 소유주는 Root 가 되어야 한다.

⑦ aliases 파일의 변경 후에는 newaliases을 실행해야 하며, NIS를 사용한다면 NIS Map을 다시 만든다.

바. uucp

불필요한 경우 uucp 서비스를 사용하지 않는다. 단, 업무상의 필요가 있는 경우, 정보보안담당관의 동의하에 다음과 같은 보안상의 제약 사항을 준수하여 관리한다.

① 쉘을 가진 uucp 계정을 사용하지 않는다.

② uucp 계정에 비밀번호를 부여한다.

③ 연결되는 상대 시스템에 따라 다른 계정과 비밀번호를 부여한다.

④ uucp가 특정 디렉토리에서만 파일을 읽을 수 있도록 하며 사용할 수 있는 명령어를 제한한다.

⑤ uucp 홈디렉토리에 .rhosts 를 제거하고, L.cmds 는 소유주가 루트가 되도

록 한다.

⑥ uucp 소유주의 파일들이 완전히 개방되지 않도록 한다.

⑦ uucp 에서 실행할 수 있는 명령을 제한한다.

사. FTP

① 최신의 FTP 패치 버젼을 적용한다.

② SITE EXEC 명령을 가지지 않은 FTP나 SITE EXEC 명령을 실행하지 않도록 한다.

③ /etc/ftpusers에 루트와 uucp, bin, news, ingres, nobody등을 추가하여 루트, 디폴트 계정 및 비인가된 사용자의 FTP 사용을 금한다.

④ 필요시 inetd.conf에서 in.ftpd를 실행시킬 때 -l 옵션을 주어서 상세한 로그를 하도록 한다.

아. Anonymous FTP

대외적으로 중요한 서비스가 아닌 이상 Anonymous FTP를 사용하지 않는다. 단, 업무상의 필요가 있는 경우, 보안 관리자의 동의하에 다음과 같은 보안상의 제약 사항을 준수하여 운영한다.

① Anonymous FTP 에서 비밀번호는 RFC822 전자우편주소 형태로 받을 수 있도록 한다.

② ~ftp 디렉토리 내에 어떤 외부 기계의 디스크도 마운트하지 않는다.

③ ~ftp의 파일을 옮기거나 지울때 비밀번호 파일에서 ftp 계정을 지운다.

④ guest, anonymous 계정 사용자의 delete, overwrite, rename, chmod 및 umask 옵션을 없앤다.

⑤ 비밀번호 파일내의 ftp 계정의 비밀번호에 *를 넣거나 NP를 넣어서 비밀번호를 사용한 로그인을 금지하고 정상적인 쉘을 주지 않는다. (예) ftp:*:400:400:Anonymous FTP:/home/ftp:/bin/false

⑤ ~ftp/etc/passwd가 실제 비밀번호의 복사본을 가져서는 안되며, ~ftp/etc/group에 실제 /etc/group의 복사를 가져서는 안된다. 또한 ~ftp/.rhosts 와 ~ftp/.forward를 가져서는 안된다.

⑥ 어떤 경우라도 ftp 계정 소유의 파일과 디렉토리를 두지 않는다. ftp 사용자는 주어진 구역에서의 파일만 읽을 수 있도록 한다. 또한, 쓰기 가능한 디렉토리를 가져서는 안되며, 부득이한 경우 특정 시스템 사용자만이 쓸 수 있도록 하고 사용자와 디렉토리의 목록을 유지한다.

자. 스니핑(sniffing)에 대한 대책

① 다음과 같이 스니핑을 탐지한다.

(가) 보안 프로그램 등을 사용하여 네트워크 카드가 Promiscuous 모드에 있는가 확인한다.

(나) ifconfig 명령어로 확인한다.

(다) 열린 파일을 조사한다.

(라) 용량이 급격히 늘어나는 파일을 조사한다.

(마) ps 명령어로 수상한 이름의 Process를 찾는다.

(예 : a.out, in.telnetd, in.uucpd 등)

② 네트워크를 이동하는 정보에 관해서는 다음 사항을 따른다.

"메시지 보안은 다양한 유형의 네트워크를 거쳐 전산시스템 간에 발생하는 데이터의 교환, 전송을 보호하기 위한 것이며, 정보 보호 등급 2 이상의 데이터는 암호화된 형태로 전송함을 원칙으로 한다."

3. 악성 코드 관리 절차

가. 백신 프로그램 배포 및 설치

① 정보보안담당관은 악성코드를 예방 및 제거할 수 있는 최신 버전의 백신 프로그램을 배포한다.

② 정보보안담당관은 악성코드 관련 정보, 예방사항 및 점검에 관련된 사항을 사용자에게 공지하며 공지결과를 악성코드 공지일지에 기록한다.

③ 사용자는 현재 사용 중인 컴퓨터가 악성코드에 감염되었는지 확인할 수 있도록 백신 프로그램을 설치하고 주기적으로 업그레이드 한다.

나. 백신 프로그램의 실행

① 사용자는 디스켓 및 다운로드를 통해 외부에서 반입되는 파일은 사용 전 반드시 악성코드의 감염 여부를 검사하고 악성코드 발견 시 이를 완전히 제거 후 사용한다.

② 사용자는 전자우편 첨부 파일에 대한 악성코드 감염 여부를 검사하고 악성코드 발견 시 이를 완전히 제거 후 사용한다.

③ 사용자는 제3자에게 소프트웨어를 제공하기 전에 바이러스나 프로그램 오류 등이 있는지 검사하여야 한다.

④ 사용자는 주기적으로 백신 프로그램을 실행한다.

4. 감염 대책

가. 악성코드의 발견

① 컴퓨터가 악성코드에 감염되었을 경우 보안사고 및 대응 결과서를 기록하고 정보보안담당관에게 즉시 알려야 한다.

② 정보보안담당관은 악성코드 발견을 확인하고 적절한 조치를 취하며 그 결과를 보안사고 및 대응 결과서 및 악성코드 발견 및 조치대장에 기록한다.

나. 악성코드 감염 후 조치

① 시스템을 네트워크로부터 분리시키고 감염된 컴퓨터로부터 다른 컴퓨터로 파일을 복사하지 않는다.

② 데이터를 테이프나 디스켓에 복사한다.

③ 감염이 심각할 경우 포맷 프로그램을 사용하여 하드디스크를 낮은 수준(low-level)으로 포맷한다.

④ 쓰기 방지된 마스터 운영체제 디스켓으로 시스템을 재부팅한다.

⑤ 백신 프로그램을 시스템에 복사한다.

⑥ 쓰기 방지된 원본 마스터 디스켓으로 응용 소프트웨어를 재설치한다.

⑦ 백업된 데이터를 재설치한다.

다. 주기적 점검

정보보안담당관은 주기적으로 악성코드 점검을 수행하며 그 결과를 악성코드 점검 결과서로 문서화한다.

제2절 접근기록 관리

1. 접근기록 내용

가. 접근기록 내용

① 사용자가 사용한 명령들에 대한 로깅은 특히 필요한 서버에 대해서만 하고, 기타 서버들은 요약(summary)파일만 관리한다.

② 다음의 파일들은 기본적으로 로깅하여야 할 내용들이다.

(가) Log on/off

(나) File and object access

(다) User and Group management

(라) Security policy changes

(마) Restart, Shutdown

(바) Process Tracking

(사) Backup, Restore files and directories

나. 로그 관리

① 사용자나 이벤트 등의 감사 대상을 선택할 때 각 대상들의 적정성을 판단해야 한다.

② 로깅 파일이 수용치를 넘을 때에는 테이프 등에 보관한다. 이 때 주요 시스템의 로그기록은 1년 이상 보관한다.

③ 최소한 주간단위로 감사 로그 파일을 점검해야 한다.

④ 아래와 같은 비정상적인 행위에 대한 로그 파일은 주의 깊게 점검하고 로그 검토 결과서를 작성한다.

(가) 최종 로그인 사용자

(나) 로그인 실패

(다) 시스템 파일에 대한 접근 실패

(라) 정보보안과 관련되는 작업 수행에 대한 실패

(마) 관리자 특권이 있는 파일 또는 서비스 사용 시도

(바) 허가 안된 파일, 자원 또는 서비스의 사용 시도

⑤ 시스템의 로그 기록이 불법 수정이 되지 않도록 보호하거나, 불법 수정을 확인할 수 있는 방법을 마련해야 한다.

⑥ 주기적으로 저장 점검을 통해 감사 파일의 오버플로우를 예방해야 한다.

⑦ 로그기록을 검토하여 침입 또는 침입시도의 흔적 등 문제점이 있을 경우 침해사고 대응절차에 따라 정보보안담당관에게 보고하고 기술된 절차에 따라 조치하여야 한다.

2. 접근관리

가. 보안점검 절차

① 시스템관리자는 주기적으로 보안점검 체크리스트를 이용하여 보안점검을 수행한다.

② 보안점검 결과서를 매월 정보보안담당관에게 제출한다.

나. 자체 점검항목, 주기 및 수행자

주 기	항 목	수행자	취합/보고
1일 단위	– 악성코드 점검		
1주일 단위	– 침입차단시스템, 침입탐지시스템, 웹서버, 주요 서버의 로그 분석	시스템 관리자	
1개월 단위	– 로그 데이터 백업 – 웹서버 자체 스캐닝 점검 – 침입차단시스템, 게이트웨이, 라우터 자체 스캐닝 점검 – 주요 서버 취약성 점검 및 로그분석	시스템 관리자	정보보안담당관에게 보고
3개월 단위	– 사용자계정 및 권한의 재확인 – 파일과 디렉토리의 사용 권한 분석 – 최신 패치 이행 – 침입차단시스템, 서버 등 관리자 비밀번호 변경 – 전산 자산 내역 확인	시스템 관리자	정보보안담당관에게 보고

3. 시스템 침해사고 분석 절차

가. 로그 점검

① 사용하지 않는 IP 대역이나 비정상적인 행위를 하는 로그를 점검한다.

② 이벤트 표시기 등을 실행하여 시스템, 보안, 애플리케이션 로그를 점검한다.

③ 침입탐지시스템, 웹서버, 라우터를 운영하고 있다면 관련 로그도 점검하여야 한다.

나. 사용자 및 그룹 점검

① 도메인 사용자 관리자 등을 실행하여 불법적인 계정이나 그룹의 생성여부를 점검한다.

② 내장된 Guest 계정이 사용안함으로 되어 있는지 점검한다.

③ 모든 그룹에서 불법사용자를 점검한다. 특히 Administrators 그룹, Backup Operators 그룹이나 Power Users 그룹과 같이 특별 권한을 가지고 있는 그룹의 멤버들의 정당성을 확인한다.

④ 사용자와 그룹에 할당될 수 있는 권한은 27가지가 있으며 올바르게 할당되었는지 점검한다.

다. 비인가된 응용 프로그램 점검

① 비인가된 응용 프로그램이 실행되었는지 점검한다.

② 실행중인 불법서비스를 점검한다. 어떤 백도어 프로그램은 시스템 부팅시 시작되는 서비스로 설치되며, 이 백도어 서비스는 “서비스로 로그온 권한” 을 가진 사용자에 의해 실행된다. 자동으로 실행되는 서비스를 점검하고, 트로이 목마나 백도어 프로그램인지 점검한다.

라. 변경된 시스템 바이너리 파일 점검

① CD-ROM이나 기타 설치 매체에서 설치된 초기 시스템 바이너리 정보를 복사한 후 주기적으로 비교한다. 또한 백업 시 트로이 목마나 백도어 파일이 있는지 미리 점검한다.

② 트로이 목마 프로그램을 정상 프로그램과 같은 파일 사이즈, timestamp 로 조작이 가능하다. 이런 경우는 MD5, Tripwire나 기타 무결성 점검도구를 이용하여 트로이 목마 프로그램을 탐지할 수 있다. 이런 무결성 점검도구는 공격자에 의해 조작되지 않도록 안전하게 보관하여야 한다.

③ 백신프로그램을 이용하여 바이러스, 백도어, 트로이 목마 프로그램을 점검한다. 하지만 변종 프로그램이 지속적으로 나오기 때문에 주기적으로 최신버전으로 업데이트한다.

마. 환경 설정 점검

WINS, DNS, IP 포워딩 같은 환경설정변경을 점검한다. 네트워드 환경설정 등록정보를 이용하거나 ipconfig /all 명령어를 이용하여 점검하고, 불필요한 네트워크 서비스가 실행중인지 점검하기 위해 "netstat -an" 명령어를 이용하여 의심스러운 호스트의 접근이나 연결대기중인 의심스러운 포트를 점검한다.

바. 비 인가된 공유자원 점검

명령 프롬프트에서 net share 명령어를 이용하여 점검하거나 서버관리자를 이용하여 점검한다. 공유폴더의 끝에 "$" 표시가 있으면 이는 Hidden Share이다. 즉, 불법 공유폴더와 NT의 디폴트나 공유폴더에 비 인가된 사용자가 연결되어 있는지 점검한다.

사. 기타 사항 점검

① 이상한 파일이나 숨겨진 파일을 찾는다. 비밀번호 크래킹 프로그램이나 다른 시스템의 비밀번호 파일이 있는지 점검하고, 탐색기(보기 → 폴더 옵션 → 보기 → 모든 파일 표시)를 이용하여 숨겨진 파일을 찾거나, "dir /ah" 명령어를 이용하여 점검한다.

② 파일 퍼미션 변경이나 레지스트리 키값의 변경을 점검한다. 리소스 킷의 xcacls.exe 프로그램을 이용하여 디렉토리별 파일들을 점검한다.

③ 사용자나 컴퓨터의 정책변화를 점검한다. 정책편집기 (poledit.exe) 에서 구성된 현재 정책의 복사본을 정리하여 변경되었는지 주기적으로 점검한다.

④ 시스템이 다른 도메인으로 변경되었는지 점검한다.

⑤ 한 시스템이 해킹을 당했다면 로컬 네트워크내의 모든 시스템을 점검한다.

4. 시스템 침해사고 대응 절차

가. 조사 기관 접촉

국가정보원의 국가사이버안전센터 또는 법적 제재 기관을 접촉하여 침입 분석 및 대응을 위한 사전 준비를 한다. 또한 단계별 작업 내용을 문서화하여 법적 대응 및 향후 발생할 수 있는 침해 사고 발생에 참고 자료로 활용할 수 있도록 한다.

나. 시스템 제어권 회복(네트워크로부터 분리)

① 네트워크로부터 해당 시스템을 분리한다. 침입 당한 시스템을 네트워크에서 분리하지 않을 경우 시스템 복구 작업이 침입자에 의해 원래 상태로 되돌아 갈 수 있고 계속적으로 다른 시스템들이 침해될 수 있으므로 해당 시스템을 네트워크에서 분리함으로써 완전한 시스템 제어권을 획득한 후 Local Administrator로 시스템 복구 작업을 시작한다.

② 침해 시스템에 대한 이미지를 복사한다. 침입을 분석하기 이전에 침해 시스템에 대한 백업을 수행하여 향후 법적 대응이나 혹은 시스템 복구 이전의 침해 상태로 되돌아갈 필요가 있을 경우에 대비한다.

다. 침입 분석

침해 사고 보고서를 작성하고 국가사이버안전센터에 연락한다. 또한 다른 Site에 대해서도 침입자의 공격이 있었음을 증명할 수 있는 증거를 찾은 경우 해당 기관에 연락한다.

라. 시스템 복구

① 침입자에 의해 사용된 시스템 취약점을 수정하고 변경된 정보를 복구 및 삭제하는 것으로는 보안상 완벽한 시스템을 유지하기에는 부적합하다. 관리자

가 신중하게 변경된 정보를 복구하고 침입자에 의해 설치된 백도어 등의 프로그램을 삭제하였다 하더라도 OS를 재설치하여 시스템을 재설정하는 것이 바람직하다.

② 시스템이 작동하는데 필요한 서비스나 업무상 반드시 필요한 서비스가 아니면 사용 중지시킨다.

③ 업체에서 제공하는 최근의 보안 패치(service packs/hotfixes)를 시스템에 적용한다.

④ 국가사이버안전센터 등 정보보안 관련 연구소에서 공시하는 보안 사항들을 시스템에 적용하고 향후 주기적으로 해당 기관의 공지 사항들을 참조하여 보안을 유지한다.

⑤ 백업에서 데이터를 복구할 경우 침해당하지 않은 시스템에서 데이터에 취약점이나 트로이 목마 프로그램은 없는지 확인 후 복구한다.

⑥ 시스템에서 Security Holes 이나 Configuration상의 보안 문제를 해결하고 보안 패치를 적용한 후에는 모든 사용자 계정에 대해서 비밀번호를 변경한다. 변경 시에는 추측하기 어려운 비밀번호를 설정하도록 하며 Account Policy에서 옵션들을 설정하여 보안을 강화하도록 한다.

마. 보안강화 및 보안정책 변경

시스템 및 네트워크에 대한 취약점 스캐닝 도구를 사용하여 보안상 취약성을 수시로 점검, 보완하고 사용자 계정, 사용자 권한, 파일시스템, 레지스트리 등에 보안강화를 위한 정책을 수립한다.

바. 네트워크 연결

복구된 시스템을 네트워크에 다시 연결하고 시스템 운영에 문제가 없는지 확인한다.

사. 시스템 모니터링

Event Viewer나 Network Monitor, Performance Monitor와 같은 툴을 사용하여 시스템 성능 및 침입 시도를 모니터링 한다.

부록 4. 전문가인식조사 응답 주요 내용

구분	질문 번호		응답 주요 내용
공공 1	1	0	– 들어 봤음. – 안전이라고 하면 공무원의 안전이라는 개념보다 국민들 입장에서 안전을 느껴야 되고 국민들은 전문성이 없기 때문에 그쪽에 있는 전문가들이 어떤 문제가 있고 그런 거에 대해서는 알려줄 수 있고 그 부분에 대해서 국민들이 안심할 수 있는 정도가 보호의 의미이다. – 70% 이상.
		1	– 사이버위기라고 그러면 예를 들어 전체적으로 사회조직체계들을 흔들 수 있는 수도가 중단된다든가 가장 작은 레벨이라면 컴퓨터사용이 안 되거나 금융거래가 안 되거나 이런 것, 그런 측면에서 보면 전문적으로 얘기하면 더 큰 게 많은데 국민들이 이해하는 측면에서 보면 그 정도. – 90%.
	2	0	– 대내는 인식의 부족. 대외는 해킹, 바이러스에 대해서 대응체계가 만들어져야 된다고 봄. – 정보의 시스템이 과거에는 학생들 공부, 오락하는데 한정이 되어 있었지만 지금은 사회 저변에 깔려서 연계가 되어 있으니 한 쪽이 문제가 생기면 전체가 다 무너짐.
		1	– 대외 : 홍보영상 제작. 침해를 할 수 있는 수칙도 제작해서 홍보함. 대내 : 상당히 높은 수준의 제도화를 준비하고 있음. 대외 : 해킹, 바이러스의 침해 등 상시적인 법리체계를 갖춰서 상시체계에서는 모니터링만 하고 있다가 집중대란이 발생할 때는 집중적으로 방어를 하는 시스템을 갖추고 있음. 침입자의 기술과 방어기술이 같이 진보를 하고 있음. 국제공조체제를 동원해서 이기도록 하는 노력을 함.
		2	– 이미 제도적으로 되어 있음. 개인적으로는 맞는 것은 아니라고 생각함. 왜냐하면 국민들의 의식이 중요함. 패널티를 완전히 높이든지, 의식수준을 높이는 것과 패널티를 높이는 것이 같이 가야 됨.
	3	0	– 침해는 높은 수준이나 방지하는 수준도 높음. 인터넷과 업무망을 물리적으로 구분해 놓음. 하지만 유출될 가능성은 낮음.
		1	– 내부자 소행이거나 다른 조직에 의해서 공개되는 거지 기술적으로 꺼내가는 경우는 거의 없음. 제도적인 인식부족임. 민간분야에서 일이 많이 생김.
		2	– 국가기밀이 높음. 민간부분의 개인정보유출은 많이 일어나고 있음.
		3	– 국가기관이 큼. 하지만 투자를 많이 해서 막고 있음.
	4	0	– 안전한 장치가 국민들의 표현의 자유나 언론을 침해 하지 않는 범위에서는 쓰는 게 맞다고 봄. 고려를 해 봐야 되는 부분임. 현실에서는 쓰는 게 조금 더 바람직함.

구분	질문 번호		응답 주요 내용
		1	– 같은 가치인데 건전한 인터넷 문화조성이 더 중요함. – 중요한 것을 지키기 위한 수단이 안전임.
	5	0	– 분리를 하면 경비가 많이 듦. 이 부분은 답이 없음. 어떤 부분은 통제를 해야 되고 어떤 부분은 분산을 해야 되기 때문에. – 중앙통제방식이 효과적임. 분리를 하면 정책기조가 다 다르기 때문에 대응이 안 됨.
		1	– 위와 상동.
		2	– 행안부, 국정원, 경찰청.
	6	0	– 가장 중요한 것은 위험의 분석, 정보입수. 가장 짧은 시간에의 원인분석. 분석된 체계에 따라서의 대응방식.
공공 2	1	0	– 사이버 상에서 안전하게 활동할 수 있는 의미. – 90%.
		1	– 들어봤음. – 그동안 사이버 편리함만 강조되었었는데 지금은 거기에 대한 부작용이 증가하는 추세. 효율성면에서 떨어지는, 편리한 것에 대해서 미처 생각하지 못하는 증상이라고 생각. – 위험성은 85% 정도.
	2	0	– 대내는 사람이라고 생각. 보완하는데 인적보완, 물적보완, 관리적 보완 중 사람의 보완이 가장 중요하다고 생각. – 대외는 기술적인 부분. 보완시스템 이런 부분이 기술적으로 많이 발달할 수 있는 부분. 네트워크도 보면 기술적인 부분. 위기라는 게 특정홈페이지에 들어갔을 때 동시에 대량으로 접속 등 기술이 발달하면 제한할 수 부분이니까 악의적이지는 않지만 특정사이트에 많이 접수를 해서 시스템을 다운시키는 등.
		1	– 사전예방 사후예방은 다 마련되어 있음. 사전예방은 기술적으로 사이버위협에 대응할 수 있는 장치, 장비, 그런 부분이 많이 구축. 완벽하지는 않음. 기술은 깨질 수 있는 부분이기 때문에 그런 부분을 염두에 둠. 지금은 완벽하다고 하지만 새로 기술이 나오면 위험한 입장. – 제도적으로는 국가에서도 많이 만들 수 있음. 단계별로. 금년도에 하려고 하는 상태.
		2	– 효과가 있다고 생각함. 그렇지만 형벌만 갖고는 수행을 못한다는 인식이 있음. 의식이 돼야지 처벌만 한다는 건 상책은 아니다. 사회적으로 궤도 부분이 많이 들어가야 된다. 이런 일을 하면 나쁘다는 인식을 심어주고 거기에 따라서 형벌이 가해진다는 부분이 들어가야지 어떤 긍정적인 계도를 통해서 인식이 된다는 하에서 나쁘다는 것을 주지시켜야 됨. 다른 사람의 주민등록번호를 이용한다는 게 옛날에는 큰일이었는데 지금은 개인정보보호법에 따라서 불법이라는 인식이 됐는데 옛날에는 많이 널려 있었다. 택배주소 등도 옛날에는 무심코 버렸는데 지금은 범죄에 악용되니까 하나의 정보로서 봐야 된다. 형벌도 중요하지만 같이 병행하는 부분이다. 형벌의 효과를 내고 그러면 사전에 계도 하고 인식시킨 다음에 적용해야 된다.

구분	질문 번호		응답 주요 내용
			– 복합적으로 해야 된다. – 형벌도 가볍게 줄 수 있고 세분화시켜야 된다. 가중처벌이나 심하게 처벌해야 되는 부분이 있다. 고의성의 유무. 내가 실수하는 부분은 가볍게, 고의적으로는 중벌로.
	3	0	– 높다고 생각함. 사이버 중에서는 보완을 해야 되는 입장에서는 큼. 남과 북이 서로 적대관계에 있기 때문에 그런 부분이 사이버 상에 많이 널려있다는 얘기. 편리함은 있지만 급한 사람 만나서 회담을 할 때는 불리한 부분이 많기 때문에 직원들을 공개를 하지 않음. 사이버침해에 대해서 침해율이 높습니다. 자료유출 되면 지금도 내부적으로 처벌을 많이 당함. – 기밀이라는 건 이쪽 국민이 봤을 때는 기밀이 아니다. 그 내용이 북으로 갔을 때는 다르다는 것임. – 사소한 것도 북에서는 중요하다. 침해의 가능성이 높다고 봄.
		1	– 마찬가지입니다. 이런 부분도 기술적인 부분은 인터넷상에 얻을 수 있는 부분이 많이 있음. 그런 부분이 조심을 하는 입장임. – 심지어 이메일도 공개를 하지 않음. 이메일을 통해서 정보를 잡기 때문에 공개를 하지 않음. 인터넷상에서 많이 유출이 됨. 개인정보는 동창회 같은 홈페이지에서 많이 유출이 됨.
		2	– 공공보다 민간 쪽이 더 많다고 생각함. 민간 쪽에서는 수익창출 등으로 어쩔 수 없다고 보는 입장인데 양자를 비교했을 때 공공 쪽이 높다는 생각을 함. 국가기관에서는 보완체계가 많이 발달이 되어 있으니까 민간부분에서는 회사차원이기 때문에 그렇다고 봄.
		3	– 공공분야가 크다고 생각함. 통일부는 더 함. 사이버 상에서도 보완은 아니지만 파급효과는 크다고 생각함.
	4	0	– 다른 경우다. 외국은 주민등록번호가 없다. 주민번호는 우리나라에만 있다. 주민번호에 정보가 상당히 많다. – 지금도 주민번호 외에 다른 걸로 많이 대체하고 있다. 인식의 차이다. 핸드폰의 경우 인증번호 등을 통해서 본인인증을 한다. 주민등록번호는 두 개를 비교했을 때는 덜 안전하다. 지금은 꼭 주민번호를 쓸 필요가 없다. 우리나라의 유일한 키가 주민번호이기 때문에 한번 유출되면 모든 것을 할 수 있다. – 다른 걸로 대체하는 것이 낫다고 생각한다. 메일이 더 안전하고 바람직하다.
		1	– 개인입장은 사이버안전이 중요하다는 입장이고 이용하는 국민의 입장에서 봤을 때는 건전한 인터넷문화가 중요하다는 입장이므로 양면성이 있다고 생각한다. 똑같은 사고가 났을 때 민간인이 낸 사고와 국가가 낸 사고는 가치가 다르다. 그런 면에서 안전성을 많이 얘기한다.
	5	0	– 비교하는 건 그렇고 두 개를 적절하게 하는 게 좋다고 봄. 국가사이버안전센터에서 이미 두 개가 같이 시행에 들어가 있음. – 강력한 건 중앙통제방식을 해야 됨.
		1	– 가장 바람직한 것은 중앙통제방식 하에 적정소관별 관리통제방식을 병합하는 것.

구분	질문 번호		응답 주요 내용
		2	– 국가정보원, 경찰청, 나머지는 똑같음.
	6	0	– 확산 방지. 피해 최소화. 외부로 유출되는 경로를 차단해야 됨. 홍보도 같이 공조를 해야 됨.
공공 3	1	0	– 들어봤다. – 인터넷 상에서의 보호방안. – 100%는 없을 거고, 80%는 돼야 안전하다고 생각.
		1	– 들어본 적이 있음. – 모든 사람들은 인터넷을 통해서 업무, 개인적인 볼 일도 보지만 본인의 의사와 관계없이 위해요인이 많음. 바이러스도 있고, 스파이웨어, 정보도 빼가려는 사람도 많고 거기에 대해서 인터넷 성격상 효율적인 대응체계는 어려운 점이 있다. 인터넷은 꼭 써야 되는데 거기에 대해서 안전한 방안이 체계적으로 되어 있지 않다. – 50% 넘어가면 위기임.
	2	0	– 사람이다. 사람이 없으면 이런 것도 없으니까. – 대내 : 위험성에 대해서 무감각하다. 경고, 교육도 하지만 자기가 당하기 전에는 못 느끼니까 보완수칙을 잘 안 지킴. – 대외 : 외교통상부는 타깃이 됨. 중국이나 북한 등 위협이 됨. DDoS 같은 것도 타깃이 됨. 중요하게 다뤄져야 됨.
		1	– 예방은 가장 큰 것은 정부기관에서 최초로 인터넷은 워낙 위험하고 효율적으로 대처가 어려워서 외교부는 보완이 필요한 자료를 많이 다루기 때문에 업무망과 인터넷망을 분리를 했습니다. 직원들이 업무PC, 인터넷PC를 분리해서 사용하고 있고, 사이버안전센터가 별도로 있음. 거기에 외부전문가들이 356일 24시간 보완등급제를 실시하고 PC는 점검도 함.
		2	– 효과는 잘 모르겠음. 처벌은 지금보다 더 엄격히 해야 된다고 봄. 이 피해가 굉장히 큼. 장난으로 할 수도 있지만 거기에 대해서 당하는 입장은 다름. 국가적으로도 전쟁도 사이버공간이 굉장히 중요하니까 잘 대비하는 것도 그렇지만 그것을 법을 어겨서 그런 짓을 저지르는 사람에 대해서는 엄격하게 처벌해야 함. – 잘못한 사람은 끝까지 추적을 해서 잡힌다는 것을 보여 줘야 됨. 반드시 본인이 큰 불이익을 받는다는 메시지를 분명히 줘야 함.
	3	0	– 대비는 많이 하고 있어서 높지는 않음. 기본적으로 업무를 다 분리를 해 놨음. 하지만 업무를 외부와 할 때는 인터넷을 하니까 결국 개개인이 보완스펙을 얼마나 지키느냐가 관건인데 이는 결국 사람임. 사람이 잘 모르거나 실수해서 유출될 가능성은 있음.
		1	– 개인정보가 유출이 되는지 다른 기관에서 모니터링도 하고 내부적으로도 홈페이지나 이런 곳에 올릴 수 없게 프로그램을 해 놨음. 실수로 올려도 스크린이 되고 있음. – 일반적으로는 지금도 굉장히 많음. 주민번호 뜨는 사이트도 많음.

구분	질문 번호		응답 주요 내용
		2	– 많이 대응이 돼서 중앙부처는 인터넷이 분리된 것으로 알고 있음. 기밀이 직접적으로 유출된 거는 별로 없다고 봄. 민간적으로는 아직도 유출될 가능성이 높다고 봄. – 민간은 국가기관처럼 차단된 게 아니기 때문에.
		3	– 국가기밀 중에서 유출되면 굉장히 피해가 크다고 봄. 민간 쪽은 금융같은 경우는 인터넷뱅킹 등등 뚫리면 그것도 만만찮게 크다고 보지만 국가기밀 유출쪽이 문제가 많이 됨.
	4	0	– 안전하다고 봐야 됨. 국가에서 운영하는 주민번호가 더 안전하다고 봄. – 메일주소는 내가 여러 군데 만들 수 있으니까. – 주민번호가 안전하기는 한데 유출될 가능성이 쉽고, 필요한 경우가 아니면 메일주소로, 추적을 하면 누구인지는 알아낼 수 있으니까. 메일이 더 바람직함.
		1	– 건전한 인터넷문화 조성이 중요하다고 보는데 현실적으로 가능할지. – 사람들이 건전하면 인터넷사용에 문제가 없는데 효과적인지는 모르겠다.
	5	0	– 병행이 돼야 됨. 인력이나 전문성 등 다 확보하기가 어렵기 때문에. 현재 체제가 좋은 것 같음. 지금은 국가정보원 사이버안전센터에서 효과적으로 하고 있다고 봄. 개인 PC가 문제가 많음. 스파이웨어 좀비 프로그램 등으로. 중앙통제방식은 아니지만 지금과 같이 국가사이버안전센터기관이 필요함.내부 개인의 PC까지 모니터링할 수 있어야 함.
		1	– 각 기관이 인력과 예산을 투입할 수 없기 때문에 중앙통제방식에 의존해야 되는 기관도 있고 그 기관의 필요성과 취약성, 비밀 취급하는 양 등을 봐서 사이버보완이 더 요구되는 기관은 그 기관에서 중심을 잡고 하는 게 맞을 거 같음.
		2	–국가정보원, 경찰청, 행안부.
	6	0	– 원인파악을 제대로 해서 차단이 돼야 됨.
공공 4	1	0	– 많이 신경을 쓰고 있음. 저희는 100% 활용.
		1	– 사소한 것까지 위기라고 봄. – 70%.
	2	0	– 내부에서 이뤄지는 것은 별로 없고 대외적으로 공격들이 많이 옴. 차단을 하려고 노력하고 시스템구축을 함. 내부에서 나가는 것을 방지하기 위해서 망분리 사업을 해 놨음. 사람들이 유출할 수 있어서 그런 것도 통제를 하고 있음. – 성격상 중요한 문서들이 많음. 국가기밀과 연관이 있음
		1	– 기술적인 것들은 예방하기 위해 시스템들이 구축이 되어 있음. 사람들의 인식에 따라서 자료 등이 나갈 수 있어서 매월 1회 전 직원 대상으로 PC점검을 함. 내부는 상관이 없

구분	질문 번호		응답 주요 내용
			는데 외부 쪽에 자료를 옮겨서 보내고 그런 것들을 보관하고 있다 보면 자료유출이 되니까 확인하고 발견되면 간단한 징계를 줌. 대응방안이 마련되어 있음.
		2	– 효과적일 수는 있음. 그러나 많은 반발이 따를 것임. 사용자들의 인식이 제일 중요함. – 벌당직 세우는 정도. 중요한 사안에 대한 문책은 처벌규정이 따로 있음. 승진의 불이익, 감봉 조치 등이 효과적임.
	3	0	– 국가기밀 자료는 외부유출은 한 건도 없었음. 일반적인 업무만 인터넷을 통해서 함.
		1	– 개인정보 등 유출될 가능성이 있음. 국정원에서 모니터링을 해서 정보를 줘서 관리를 하고 있음. 일반인 쪽은 다양하게 오픈 돼서 정보가 나갈 수 있지만 내부에서는 개인정보가 나갈 확률은 없음.
		2	– 국가기밀이 유출될 가능성은 시스템을 통한 것은 별로 없을 것 같음. 의도적인 것으로 해서 나갈 수는 있음. 기밀 정도는 대외비로 관련돼서 문서도 만들지 않음. – 민간분야에서의 정보유출은 가능성이 있음.
		3	– 국가기밀이 조금 더 크다고 생각함.
	4	0	– 안전한 것은 외국사례가 더 낫다. 우리는 불필요한 정보들이 많이 입력이 되기 때문에 유출될 확률이 높다
		1	– 건전한 인터넷문화 조성이 중요하다고 봄.
	5	0	– 거의 중앙통제방식이 좋을 것 같음. 국정원이 더 전문적인 지식을 갖고 있음.
		1	– 중앙통제방식이 바람직하다고 봄. 국정원. 서로 힘겨루기를 하지 않기 때문에.
		2	– 국정원, 행안부, 경찰청.
	6	0	– 모든 부처가 정보를 공유할 수 있는 그런 체계가 필요한 것 같음. 한 부처가 공격을 당하면 다른 부처도 당할 수 있으니까.
공공 5	1	0	– 들어봤음. – 인터넷 상에서 정보보호라고 이해함. – 90% 이상.
		1	– 위험으로부터 파생되는 침해 사고. – 50% 이상.
	2	0	– 사이버안전은 외부요인보다 내부적인 게 더 크다고 판단함. 내부적으로 관리자 부주의, 내부직원들의 의식수준 저하로 인해서 안전의 위협을 느낌. 의식수준향상과 보완강화 등 홍보교육을 시킴. – 우리의 개인정보, 문서 등이 유출되면 심각한 피해가 발생함. 사전에 위험요인을 차단

구분	질문 번호		응답 주요 내용
			하기 위해서 노력을 함.
		1	– 방송통신위원회에서는 2009년 12월에 사이버안전센터를 내부에다 마련해서 네트워크, 직원 PC점검을 실시간으로 함. 제도적으로는 국가사이버안전관련규정을 준용해서 내부적으로 정보보호지침훈령으로 만들어서 지켜야 될 것을 시행하고 있음.
		2	– 형벌을 마련해서 직원들에게 제재를 가하는 것도 좋은 방법이지만 그렇게 했을 때 직원에 대한 피해도 심각해서 사전적인 예방이 더 중요하다고 생각함. – 형벌은 중징계를 얘기하는데 기관장 경고 정도는 가능하다는 봄.
	3	0	– 국가방침에 따라서 2008년 말에 업무망하고 인터넷망을 분리함. 공격을 해 와도 국가기밀이 유출될 가능성은 낮다고 봄.
		1	– 낮다고 봄. 필터링시스템, 사전 시스템적인 보호장치도 있고, 직원들에게 개인정보가 있는 문서나 파일은 별도로 관리하기 때문에 사전적인 조치를 하고 있음. – 민간도 대기업은 정보유출에 대해서 잘 갖춰져 있지만 중소기업이나 영세기업들이 문제여서 방통위에서 지원을 마련하는 걸로 알고 있음. 국가기관은 낮고 예산투자가 낮기 때문에 낮다고 봄.
		2	– 위와 상동.
		3	– 국가기관은 안전을 지키고 있지만 민간분야는 그렇지 않아서 민간이 피해가 클 거라고 생각함. 국가는 보안서버를 이용하고 있는데 민간은 개인파일을 저장하는 서버가 보안서버가 아닌 경우가 많기 때문에. – 금전적으로 보면 공익성, 국가정보, 많이 유출되면 국가기밀 유출이 더 피해가 큼.
	4	0	– 외국사이트는 간단한 메일주소를 요구하는 게 더 안전하다고 생각함. 사업자들이 개인정보를 최소한으로 보유하기 때문에 우리나라처럼 다량으로 요구하는 것보다 피해가 적다고 생각함. – 개인정보를 최소한으로 요구하는 게 바람직하다고 봄. 개인정보의 노출이 덜 되기 때문에.
		1	– 사이버 안전성이 확보돼야 건전한 인터넷문화가 조성될 수 있음.
	5	0	– 적정소관별 분산관리방식이 더 효과적으로 봄. 중앙에서 강력하게 한다는 것은 기술적으로 한계가 있음. 국가정보원이 중심을 하고 그다음에 정보통합센터에서 거르고 단위기관인 정부부처에서 하고 삼단계 관제를 하므로 자꾸 필터링이 되는 게 안전함. 이게 바람직함.
		1	– 국가정보원, 방송통신위원회, 행정안전부.
		2	–

구분	질문 번호		응답 주요 내용
	6	0	– 인터넷 연결된 포트를 빨리 제거해서 접속 차단하는 게 가장 중요함. 바이러스가 전파되기 때문에 다른 사람에게 피해를 주니까 조속히 접속 차단한 다음에 보호책에 따른 상황보고를 한다든가 해야 됨.
공공 6	1	0	– 들어봤음. – 사이버안전은 인터넷공간을 통해서 국가의 중요정보를 외부의 침입으로부터 막아서 안전하게 한다는 뜻. 해커나 정상적이지 않는 사람들의 접속을 차단하는 것으로 알고 있음. – 100%
		1	– 들어봤음. – DDOS가 대표적인 사이버위기. 해커 등의 방법을 통해서 주요 기관통신망이 마비가 되는 것이 위기라고 표현을 함. – 4단계 중에 마지막 단계가 위기인데 50% 이상 시스템이 작동이 안 될 때 위기라고 표현함.
	2	0	– 대외 : 해커가 이런 곳에서 우리 중요정보를 빼가거나 시스템을 마비시켜서 업무를 하지 못하게 하는 것. 대내 : 개인정보가 유출되는 것. – 대외 : 국가기관망이 마비가 되면 모든 국가의 업무를 제대로 하지 못하기 때문. 국가의 대혼돈을 야기하기 때문에. 대내:심각한 질병정도라든지 이런 부분이 유출이 되면 사생활의 침해가 되기 때문에.
		1	– 기술적으로 완벽한 것은 없지만 방화벽 등이 사이버안전센터를 둬서 주요한 인터넷접점에 대해서 차단하고 사후관리를 할 수 있도록 하고 있음. 제도적으로는 국정원에서 사이버안전을 단계별로 나눠서 심각, 위기 등을 둬서 대응을 할 수 있도록 하고 있음.
		2	– 법은 있기 때문에 중벌로 한다고 해서 그게 효과가 더 있을 거라고 생각하지 않음. 범죄행위를 하려는 사람이 범죄형량이 높다고 해서 사형을 시킬 수 있는 것은 아니기 때문에 이런 부분에서 만약에 북한이 해킹을 하면 국내법으로 할 수도 없음. – 형량을 높이는 수밖에 없는데 제가 법률전문가가 아니라서 잘 모름. – 우리가 내부정보를 유출하는 경우에 징벌을 강화하면 효과가 있을 거라고 봄. 복지부에서는 인사규정 등을 만들어서 처벌을 강화하고 있음. 인사이동, 인사상 불이익뿐만 아니라 파직이라든지 할 수 있도록 구성되어 있고 그래서 효과는 있음. 대외적으로는 잘 모름.
	3	0	– 높다고 봄. 이유는 모든 정보가 PC나 서버에 저장되어 있어서 사이버공격을 통해서 빼갈 수 있기 때문에 유출가능성이 높다고 봄.
		1	– 개인정보 유출도 상당히 높다고 봄. 기관의 정보를 팔아먹고 하는 부분도 있어서 높음. – 개인정보의 필요성이 많으니까. 옛날에는 개인정보를 통해서 할 수 있는 게 별로 없었는데 요즘은 할 수 있는 게 많다. 예를 들면 병력 있는 사람이 보험을 들면 손해가 있으

구분	질문 번호		응답 주요 내용
			니 그런 걸 빼 낼 수 있음.
		2	– 민간분야 개인정보 유출가능성이 높다고 봄. 개인은 국가보다 상대적으로 낮음. 심각하게 보는 부분도 낮음. 정보보호에 대한 심각성이 차이가 남. 직원들의 태도나 도덕성.
		3	– 공공분야가 국가기밀을 많이 갖고 있기 때문에 사이버침해에 의해서는 유출가능성이 훨씬 높고 피해가 큼.
	4	0	– 외국은 주민번호가 없어서 메일주소 등을 통해서 확인을 하고 우리는 주민번호가 있으니 낮다고 본다. – 주민번호는 내부자가 유출해서 위험하고 해킹을 했을 때 주민번호가 더 빠져나가서 위험하지만 우리나라가 메일주소로 하는 경우는 좀 어렵다. 바람직한 것은 주민번호가 낫다. 메일주소가 나갔을 때 피해를 줄일 수 있는 건 낫다.
		1	– 건전한 인터넷 문화조성이 더 중요하다.
	5	0	– 두 개를 경유하고 있음. 국정원이 전체통제를 하고 그다음 파트별로 하는 게 맞다고 생각함. – 국정원.
		1	– 국정원. 국정원이 아니면 다른 곳에서 할 수 없음. 국가적인 문제기 때문에.
		2	– 국정원, 방송통신위원회, 행안부.
	6	0	– 각 사이버안전센터에게 빨리 통보를 하는 것. 거기서 각각 대응체계를 구축하고 두 번째 국민들에게 알려주는 것
공공 7	1	0	– 들어봤음. – 정보 통신, 보안. – 70%.
		1	– 들어봤음. – 정보통신 시설에 혼란을 야기 시켜서 관련된 주요 시설이나 기관들을 무기력하게 만드는 것. – 60%
	2	0	– 대내는 인적, 사람이 가장 중요하고, 대외는 시스템에 대한 안전성. 방화벽이라든지 특정한 망하고 일반적으로 쓰는 인터넷망하고 분리해서 사용하는 것. – 시스템이 완벽하게 분리되더라도 사람이 시스템을 운영하기 때문에 사람들이 가장 중요하다. – 외부로부터 들어오는 것이기 때문에 분리돼 방어할 수 있는 시스템의 물리적인 보안. – 대외적인 부분을 우선적으로 해야 함.

구분	질문 번호		응답 주요 내용
		1	– 어느 정도 마련돼 있다. 사전에 관련되는 부분은 네트워크 분리돼 있는 부분들, 인적요소들, 관련담당자들 교육이 마련돼 있다. – 제도적으로 마련돼 있다.
		2	– 사안의 중요성에 봤을 때 필요성도 있지만 불특정 다수로 움직이고, 젊은 친구들이기 때문 형벌적인 측면보다 계도적인 측면으로 강화하자. 사회적으로 이 부분에 대해서 인식이 부족하므로 시기상조다. – 신체구속보다는 계도, 교육, 사회봉사.
	3	0	– 낮은 상태다. 업무망 쪽하고 일반적 인터넷하고 분리됨.
		1	– 법에 의해서 통제를 받고 있고, 내부자 유출이 대부분이라 높지 않다.
		2	– 절대적으로 비교할 수 없다. 국가는 조직적이고 체계적으로 관리, 민간은 가지고 있는 특성에 따라 정부보다 강한 곳도 있지만 경제 투자를 요하기 때문에 민간 쪽은 상대적으로 취약하다고 볼 수 있다.
		3	– 국가 부분은 관리체계가 있기 때문에 일반적으로 누출된 부분은 중요한 부분이라고 보기 어렵다. 공공 쪽에서 그렇게 유출이 많다고 보지 않는다. 오히려 민간 같은 데는 개인정보 유출이라는 부분이 상대적으로 퇴직이나 이직 이런 부분에서 가능성이 있다. – 국가 전체적으로 보면 국가기밀 유출이 크다.
	4	0	– 공공IP 쪽으로 제도를 바꾸고 있기 때문에 정확한 메일주소가 한 사람이 하나만 가지고 있으면 정확할 수 있지만 다양하게 가지고 있을 수 있기 때문에 우리나라 방식이 훨씬 안전하고 바람직하다. – 메일만을 요구하면 메일 주소는 얼마든지 바뀔 수 있기 때문에 어느 정도 위험 부담을 감수하고 움직인다. 공공IP 쪽이 훨씬 안전하고 정확하게 개인의 부분이기 때문에 신뢰감을 높인다.
		1	– 안전이라는 부분은 후행하는 부분이기 때문에 기본적으로 인터넷문화가 건전하게 조성되면 여러 가지 부작용들이 해소될 것이다. 일단은 건전한 인터넷문화 조성이 우선되어야 한다.
	5	0	– 사회 전반에 확산돼 있기 때문에 강력한 중앙통제방식보다 각 분야별로 분산 관리하는 방식으로 하는 것이 효과적이다.
		1	– 사회가 다변화돼 있기 때문에 중앙통제방식은 바람직하지 않다.
		2	– 공공적인 측면 국가정보원이 처음, 행안부 전반적인 정보관리, 총괄 방통위, 숫자적으로 나와 있지 않기 때문에 국가적인 측면이고, 개인적인 측면에서 경찰청, 검찰청.
	6	0	– 개인한테 오는 경우 관련 시스템을 차단하는 것, 총괄하는 기관에 알리는 것, 전반적으

구분	질문 번호		응답 주요 내용
			로 확산되지 않도록 조치하는 것, 사이버센터에 알리는 것이 확산을 막는 방법.
공공 8	1	0	– 들어봤음. – 개인의 프라이버시, 비방, 사이버를 통해서 실생활에 공격이 나타나는 것을 포함한 말. – 90% 이상.
		1	– 있음. – 청소년이 현실하고 구분을 못해서 현실적응을 못하고, 정부를 비방하거나 특정인에 대해서 댓글로 자살을 하게 하거나, 해킹, 개인정보 빼돌리는 것. – 해킹은 10% 이내라도 위험하다고 할 수 있지만 사이버모욕, 게임중독은 70% 이상.
	2	0	– 해킹. – 우리나라 해킹, 바이러스, 대외적인 게 많은 것 같다. 중국에서 우리나라를 해킹 경유지로 쓰니까 시스템이 그만큼 취약하다. – 양적으로 질적으로 IT가 발전했지만 보안은 투자 수준이 낮다. 한번만 해킹 당해도 기밀이 누출될 수 있으니까 중요시해야 함.
		1	– 기술적, 제도적으로 잘 돼 있습니다. 사후대응도 해킹을 침해된 적이 없다. 바로 모니터링할 수 있는 사이버안전센터도 있다.
		2	– 기존 형법을 이용할 수 없는 부분은 형법을 보완을 한다. – 처벌 수위를 높인다고 효과는 없다. 조항으로 크게 해 중요하다는 인식을 주자. 단순히 있는 조항의 처벌의 강화하는 것은 효과가 없다. 제도적인 장치가 없는 부분은 체벌을 신설하자.
	3	0	– 국가기밀, 기업기밀을 빼돌리기 위해 전문적으로 양성하기 때문에 상당히 위험이 높다.
		1	– 시스템에 따라 다르다. 민간분야도 과거 사건으로 암호화 사업을 많이 하고 있다. 보안 투자를 못한 중소업체 쪽은 나아지지 않고 있다. 보안 시스템이 미약하기 때문에 유출될 가능성이 있다. – 대학교 쪽은 취약하다.
		2	– 민간 쪽이라고 생각한다. 개인과세정보는 인터넷 접속을 안 했다. 지자체는 많이 있지만 민간보다 공공 쪽이 국정원 주도로 매년 보안점검을 하기 때문에 평균적으로 잘 돼 있다. 민간은 분야가 넓기 때문에 편차가 많다.
		3	– 민간 쪽도 정부 부분 못지않게 중요한 부분이 많다. 국민을 통제하는 정보가 많다. 조금만 유출돼도 큰 피해가 올 수 있다. 외교문서, 동일한 사안을 가지고 유출하면 공공 쪽이 피해가 크다.
	4	0	– 외국이 안전하다. 왜냐하면 개인정보를 일체 요구하지 않습니다. 바람직한 것은 개인의 신분을 확인하는 절차는 어떤 형태로든 필요하다. 문제는 우리 i-PIN 도입을 했지만 활성화가 안 되고, 실명을 확인할 수 있는 지금보다는 적은 개인정보를 하는 것이 바람직하다.

구분	질문 번호		응답 주요 내용
		1	– 둘 다 중요한데 원론적인 얘기는 문화를 조성하는 것이 맞지만 시간이 걸리고 안 될 수 있으니까 정책을 추진할 때는 병행을 하되 사이버안전 쪽에 예산투자를 더 많이 해야 한다.
	5	0	– 분산하는 게 맞다고 생각한다. 한쪽에서 하면 강력할 수 있고 효과적일 수 있지만 분야별로 그룹별로 중점 되는 사항이 다르기 때문에 획일적으로 하면 피해를 보는 그룹이 생긴다. 그룹에 맞게 분산관리가 더 낫다
		1	– 분산관리가 효과적이고 바람직하다고 생각한다. 효과성도 분산하는 게 효과적이다. 예산은 더 들어갈 수 있지만 사이버 효과를 보는 것이기 때문에 각 부서에 맞게 운영되는 게 바람직하다.
		2	– 사이버 침해 유형에 따라 다르다. 국정원, 경찰청, 국세청.
	6	0	– 발생하기 전이 중요하다. 모니터링해서 발생 징후를 감지한다. 전파가 제일 중요하다. 전파의 중요성은 해킹 같은 경우에는 순식간에 벌어지기 때문에 다른 쪽에 알려서 막는 게 중요하다. 감염 안 된 곳을 차단하는 것이 중요하다. 그 다음에 감염한 원인을 파악해서 조치를 취하는 게 맞다.
공공 9	1	0	– 사이버 상에서 정보를 유출하고 시스템을 마비시키는 공격. – 최소한 70~80% 돼야 한다.
		1	– 자주 듣습니다. – 정보 유출이라든지 공격. 시스템 마비시킨다. – 100% 들어맞게는 안 될 것 같고 50% 정도 범위에 들어가면 위기다.
	2	0	– 중요 국가 기반시설들이 위협을 받았을 때 큰 위협이다. – 공격이 네트워크에 들어오기 때문에 관리, 보안 소홀이 가장 큰 위협요인이다. – 국민의 안정적인 생활을 위협했을 때.
		1	– 제도적으로 마련돼 있다. 기술적으로 80~90%는 마련돼 있다. 그런데 DDoS 공격 같은 경우 관리적인 측면이 더 중요하다. 상황이 발생했을 때 신속한 대응을 할 수 있는 체계가 갖춰진 것이 중요하다. 80~90%는 갖춰져 있다. 관련 부서에서 자주 점검하고 공공기관의 경우 기본 체계는 갖춰져 있다.
		2	– 제도적으로 벌칙조항을 강화하고 있다. 형벌 강화도 할 필요는 있다. 민간기관들이 미흡해서 관련 기관에서 제도화하고 있으며 필요하다고 본다. – 처벌도 강화해야지만 처벌대상도 확대하면 효과가 있을 것이다. – 정보보안에 대한 처벌이 없거나 약해서 일반인 인식이 부족했다. – 단계적으로 벌금을 더 추가한다든지 구금이나 징역, 사회봉사활동 형사상의 형벌을 받게 한다.

구분	질문 번호		응답 주요 내용
	3	0	– 사이버상의 유출 가능성은 그렇게 높지 않다고 본다. 사이버에 의한 기밀유출보다 사람에 의한 관리적인 유출이 위험성이 크다. 관리 소홀. – 사이버 체계가 잘 갖춰져 있다.
		1	– 국가기밀보다 높다고 본다. – 개인정보에 대한 인식이 부족하고 개인정보에 대한 정의가 정확하지 않다. 정의가 광범위 하다. 개인정보가 많이 노출돼 있다. 별도의 보호할 수 있는 법과 제도화를 추진하는 과정에 있지만 아직까지 체계화될 필요가 있다.
		2	– 민간분야의 개인정보 유출 가능성이 훨씬 높다. – 국가는 체계가 갖춰져 있다, 보안면에서. 제도적 기술적인 부분이 갖춰져 있다. 민간분야는 너무 광범위하고 민간을 제도적으로 콘트롤 하기 어렵다.
		3	– 국가기밀 유출이 훨씬 크다. 개인정보유출도 대량일 경우에는 크겠지만 국가 안보상의 문제가 생기기 때문에 더 크다.
	4	0	– 외국의 경우가 안전하다. 개인정보가 요구가 안 될 경우 개인정보가 덜 들어가니까. – 주민등록번호를 쓰는 체계는 바람직하지 않다. 개인 신상이 너무 유출돼서.
		1	– 공공 부분에 있어서 사이버 안전성이 더 중요하다. 국가의 중요 정보이기 때문에 위협에 처할 수 있다.
	5	0	– 분산되는 거는 바람직하지 않다. 체계가 일관성 있게 특정 기관에서 중심돼서 분야별로 나뉘어야 한다. – 특정 부처는 언급은 곤란하다. 노코멘트. 실력 있는 기관에서 통제를 했으면 좋겠다.
		1	– 강력한 중앙통제하면서 그 아래 적정 소관별로 분임 있어서 하면 좋겠다. 기술이 압도적이고 제도적으로 잘 돼 있는 부처가 중앙이 돼서 하면 좋겠다. 혼합방식이 가장 좋으나 중앙방식이 낫다. – 한 개 기관에서 체계가 일관적으로 중앙통제방식이 좋겠다.
		2	– 국가정보원, 행정안전부, 방송통신위원회. 저희하고 직접적으로 관련 없다.
	6	0	– 상황 판단을 잘 해서 적정한 곳에 연락체계를 갖춰야 한다. 시스템적으로 할 수 없는 경우가 있기 때문에 상황에 따라 해결할 수 있는 전파를 빨리 하는 게 가장 중요하다. – 의사결정이 빨리 되고 응급 대처방법이 빨라진다.
공공 10	1	0	– 만날 듣고 있고, 시스템을 통한 안전은 전체적으로 다 사이버 안전이다. 사이버를 통해서 문제점이 하나도 안 생기는 게 안전이다. – 95%.
		1	– 보안시스템이 구축됐지만 새로운 위기가 항상 있다. – 조금이라는 의미로 보면 숫자가 낮은 거고, 현재 시스템에서 위험성 있다는 의미이면

구분	질문 번호		응답 주요 내용
			95~100% 항상 위험은 있다.
	2	0	– 대외적으로 사회가 갈수록 불안하고 통제범위를 임의로 정의할 수 없으니까 위협하는 요인이 증가한다. – 대내도 사회가 갈수록 불안해지고 일반 사이버 상에서 계층 간의 위압감이 생기고 적응을 못하고 경제적으로 떨어지니까 지하 쪽으로 관심을 가지고 정상적인 삶을 벗어나기 시작하고 새로운 기술도 개발된다. – 대외적으로 정치 불안, 국가 간의 이해관계도 따져지고 우리 같은 경우 북한 문제가 있을 것이다. – 내가 가진 것을 빼가는 거다. 그러니까 내가 공식적으로 내놓는 거와 상관없이 누군가가 나도 모르게 개인이고 국가고 다 가지고 가기 때문에 그런 측면에서 우리가 내놓는 것만 당연하게 갖고 갈 수 있는 상황이라면 별 문제가 없다.
		1	– 맞춰서 시스템을 구축하고 내부적으로 방침을 바꾸고 그런 식으로 준비돼 있습니다. 제도적으로 마련돼 있고 기술적 도입도 가급적 반영하려 하고 있다. – 효과적으로 하려고 필요성을 느끼고 완벽하게 하려고 함.
		2	– 형벌도 필요하지만 자기가 느껴서 할 수 있게끔 만들어줘야 된다. 형벌을 무겁게 한다고 효과적이지 않다. – 기본적인 피해를 준 범위에 맞춰서 형벌을 준다. 벌의 강화가 해결책이 아니다. 뉴욕처럼 청소를 하니까 범죄율이 줄었다 사회 시스템을 개선해야 된다. 체벌의 형식이 바뀌어야 한다.
	3	0	– 상대적으로 타 부처에 비해서 높지는 않다. 보안 쪽은 사이버 쪽보다 사람에 의한 유출 가능성이 있다고 생각한다. 높은 쪽의 기밀은 위에서 잘 보안이 되면 보안이 잘 될 것이다. – 시스템 잘 돼 있어서 역이용당해서 유출 가능성이 높을 것 같다.
		1	– 높을 것 같다. 모든 개인정보가 시스템으로 돼 있다. 개인정보가 시스템화 돼 있는데 시스템적인 오류나 취급자의 오류에 의해서 가능성은 있다.
		2	– 민간에서 개인정보 유출 가능성이 높다. 정부기관은 체계적으로 관리가 되지만 민간 같은 경우는 통제가 안 된다. – 국가기관은 보안 잘 돼 있지만 개인은 노출될 숫자가 많아서 가능성이 높다.
		3	– 파급효과를 전체 범위로 보면 국가가 큰 영향을 미치고 개인적인 거는 개인에게만 미친다.
	4	0	– 외국 사이트가 훨씬 안전하다. – 바람직한 것도 외국이다. 꼭 필요한 정보도 아닌데 받아 놓은 것은 잘못. 실명제보다 메일주소만 하는 것이 안전하다. 개인의 주민번호가 노출 안 되니까.

구분	질문 번호		응답 주요 내용
		1	– 사이버 안전성 확보가 돼서 사회가 안전하면 인터넷 문화도 자연적으로 따라온다.
	5	0	– 한 곳에서 강력하게 하는 게 괜찮은 거 같지만 실제는 안 된다. – 파트너가 계속 바뀌다 보니 책임 소재가 불분명하고 아쉬운 점이 생긴다.
		1	– 책임 소재도 불분명할 뿐만 아니라 조직이 다른 조직이 만들어지면 유대감이 그렇다. 예산절감 면은 좋은데 운영 면에서 아쉬운 점이 생긴다.
		2	– 국정원 전체적으로 계획을 세우고 다른 부처에서 기술작업, 행안부 지금 시스템을 운영하면서 그 분야 쪽에서, 방통위 관리하는데 약하다.
	6	0	– 규모라든가 사태파악. 위기의 종류, 원인 파악. 응급조치로는 네트워크 차단. 추가 피해가 안 생기니까.
공공 11	1	0	– 들어본 적 있음. – 인터넷상 통신을 통해서 이루어진 가상의 현실에서 보안에 어려운 부분이 있다. 개인정보유출 등 90% 이상은 취중해야 한다.
		1	– 있음. 초기의 단계에서는 해킹, 바이러스 유포, 시스템에 제약을 가할 수 있는 부분. 산업 전반까지 침투할 수 있는 국가적인 위기. – 90% 이상.
	2	0	– 해킹에 의해서 개인정보 탈취, DDoS 공격. 악성바이러스 유포. 좀비PC. – 개인정보가 유출될 수 있고, 정보 자원을 망가뜨릴 수 있고, 대외적으로 국가 보안, 경제 위협, 산업적인 혼란을 초래, 기관시설을 마비시킬 수 있음. 국가 마비.
		1	– 자체적으로 보안관제시스템 모니터링. 행안부 통합센터에서 관제를 함. 국정원에서 관제. 자체 관제시스템도 필요함. 2중, 3중으로 방어시스템을 보안정책을 시스템화한다. – 보안이 필요한 부분에 방화벽, 데이터베이스의 암호화 통제, IPS 침입 차단장비 시스템화.
		2	– 범법행위와 관련 없이 형벌 처벌은 강해야 된다. 사안에 따라 정상 참작은 가능하나 폭행, 살인에 못지않게 엄하게 다스려야 한다. – 재산적인 피해를 변상, 징역, 구속, 구금할 수 있음. 사형에 버금가는 중형으로
	3	0	– 보안 수준은 낮지 않고 높음. 완벽한 거는 없음. – 보안 시스템은 계속 새로운 것이 생길 수 있기 때문에 계속 연구해서 대비책을 세워야 된다. 국가 중요 시설은 보안을 철저히 한다. 유출될 빌미는 항상 있다.
		1	– 높다고 본다. 기관은 방비를 갖추지만 인적으로 유출. 보안시스템을 더 많이 갖춰야

구분	질문 번호		응답 주요 내용
			된다. 기술력은 항상 변화하기 때문에 침해 가능성이 있다.
		2	– 공공 분야에서 보안이 강하다. 민간 분야에서 대기업, 보안이 필요한 부분에서 강하다. 민간부분은 시스템화를 해야 되기 때문에 비용 부담, 유지 비용이 중소기업에서는 감당하기 쉽지 않다. – 민간 분야가 유출 가능성이 높다.
		3	– 국가기밀 유출은 국가 존립 자체를 위험에 빠뜨릴 수 있는 부분이기 때문에, 경제적으로는 민간분야에 피해가 크지만 국가적인 부분이라면 국가 자체의 존망이 문제가 될 수 있다. – 공공 분야가 크다고 볼 수 있다.
	4	0	– 주민번호를 요구하는 것은 문제가 있다. 메일 주소로 대체할 수 있는 것도 괜찮은 방법이다. 사이버 공간이라는 것은 사생활 피해를 주는 부분도 있지만 개인실명제는 바람직하지 않다. – 개인정보 노출 때문에 메일 주소가 바람직하다.
		1	– 사이버 안전성 확보가 더 중요하다. – 유출되지 않을 기밀이 유출될 때 오는 부작용이 더 크다.
	5	0	– 소관별로 분산 관리하는 게 좋다. 강력한 통제방식이 현실적으로 놓칠 수 있는 부분이 있다. 필요한 부분에서 특성을 부여해서 관리하는 적정소관별 분산관리가 적정하다.
		1	– 분산 관리되는 방식을 집중화해서 놓치지 않고 충분히 관리가 된다면 중앙통제방식이 효과적이지만 그게 쉽지 않기 때문에 분산관리가 중요하다. 정보시스템에서 관리하고 정보시스템에서도 이걸 관리하는 조직이 따로 필요하다. – 국가적으로 보면 국정원 소속에서 총괄하는 것.
		2	– 1. 국가정보원은 국가를 전부 다 할 수 있다. 2. 행정안전부가 국가 행정기관들의 총무부나 마찬가지니까. 3. 검찰청, 경찰청, 법무부 같은 순위로. 국방부도 같은 순위로. 하지만 특수 부분이기 때문에 전체적으로 적용하기에 무리다.
	6	0	– 시스템이 구축됐을 때 시스템에 경보 사항이 나온다. 관제센터에서 관리하다 이상 징후가 있다. 사이버 위기 대응에 대한 매뉴얼에 따라 움직이는 게 중요하다. 별도로 나올 때는 수행하고.
공공 1 2	1	0	– 들어봤음. – 정보 자산에 대해서 안전하게 보호하는 것. – 80%.
		1	– 들어봤음. – 현재 사이버 상에서 정보자산들이 침해되고 해킹당하는 빈도가 늘어나고 있음. 개인정보도 유출됨.

구분	질문 번호		응답 주요 내용
			– 80%.
	2	0	– 해킹, 네트워크 상에 침투해서 정보 자원을 빼가는 거. 대내 측면 네트워크 상에 침투하는 해킹을 대비해서 안전하게 유지하는 것. 네트워크를 마비시킴으로서 대국민 서비스가 안 되기 때문에 상당한 위협으로 작용한다. 대내적으로 정보 자원이 파괴되거나, 서비스 불가능. 대외적으로 국민이 서비스를 사용할 수 없다.
		1	– 제도적으로 정보보안기본지침이나 개인정보보호법으로 대응하는 방안. 기술적으로 정보보호시스템을 도입해서 침투를 미리 관제해서 사전차단, 사고 발행 후 재발방지를 위한 대책을 수립하는 부분을 준비하고 있으며 관제하고 있고 갖고 있다.
		2	– 징벌규정이 있으나 현행보다 무겁게 처벌하는 게 효과적이지 않다. 범죄라는 인식이 없다. 사이버 범죄에 대한 처벌을 홍보하고 국민이 인식한 후 처벌하는 방법이 좋다. 교육과 홍보를 먼저 하고 처벌이 뒤따라야 된다. – 교육하고 범죄를 일으킨 사람이 인식한 후에 처벌한다.
	3	0	– 과거보다 높아졌다. 사이버 침해 기술이 고도화됐다. 죄의식이 없어서 자기과시를 위해서 침투하는 경우가 있다. 범죄라는 것을 계속적으로 홍보하고 교육해야 한다.
		1	– 사이버공격, 침해뿐만 아니라 보안 인식이 부족해서 개인정보가 유출된다. 의도적으로 개인정보를 가져 가거나 목적성을 가지고 침투하기 때문에 높아지고 있다.
		2	– 민간 분야에서 유출 가능성이 훨씬 높다. 민간이 경각심이 적기 때문에 가능성이 높다.
		3	– 국가기밀 유출은 파급 효과가 크다. 그러나 제도적인 장치가 마련 있다. 그러나 실제로 어느 쪽이 높다고 할 수 없다. 민간에서 유출된 게 다시 공공으로 넘어온다. – 국가 쪽이 영향력은 크다.
	4	0	– 개인정보를 제공하지 않는 것이 안전하다. 필요 없는 개인정보는 받지 말고 정부에서도 과도한 개인정보를 수집하는 것을 없애야 한다. – 개인정보를 받지 않는 것이 바람직하다.
		1	– 인식과 교육, 홍보를 통해서 건전한 인터넷 문화를 조성하는 것이 먼저다. 이런 문화가 조성되면 사이버 범죄는 자동적으로 줄어든다.
	5	0	– 중앙통제방식이 훨씬 효과적이라고 생각한다. 국가가 일률적으로 시행하기 곤란하다. 각 기관별로 수준이 다르다. 결국은 분산방식으로 갈 수밖에 없다.

구분	질문 번호		응답 주요 내용
		1	– 국가정보원에서 중앙집중방식으로 하고 있고 하는 것이 맞다. – 중앙통제방식이 바람직하다.
		2	– 국가정보원 정보보안 관련해서 가장 노력하고 있고, 행안부, 방통위.
	6	0	– 사고의 현상을 파악할 수 있는 자료를 확보하는 것. 자료를 통해서 왜 사고가 발생했는지 어떤 경로로 침투했는지 알 수 있다.
공공 13	1	0	– 저희가 하는 일이 사이버안전인데요 일단 인터넷상에서의 어떤 정보보 안전을 얘기하는 거겠죠 – 80% 이상은 되야 된다고 생각합니다.
		1	– 사이버위기 대응체계상에서 보면 4단계로 정의되고 있거든요 그래서 지금 관심, 주의, 경계 이런 형태로 올라가는데, 단계별로 되어 있습니다. – 3단계 정도 60% 정도가 되면 위기라고 해야 되겠죠. 5단계부터는 정상 관심 경계 이 부분은 기억이 안 나고 제일 위 단계는 심각입니다.
	2	0	– 대내적으로는 내부자 정보 유출로 봐야겠구요, 대외적으로는 사이버침해 어떤 해커들에 의한 사이버침해로 볼 수 있겠습니다. – 어차피 평상시에 일어나서는 안되는 일이거든요 이런 것들은 특히 내부자 정보유출 같은 경우는 누가 막을 수 있는 상황이 아니기 때문에 중요점은 상당히 높다고 할 수 있습니다.
		1	– 대내적인 내부자 정보 유출 같은 경우에는 직원의 의식 제고, 기호 그런 것들이 가장 중요하다고 보구요 그 다음 어떤 본인의 윤리적인 가치가 높아야 한다고 봐야 되겠죠. 기술적인 것보다는 어차피 기술은 정보 유출은 막을 수 없거든요 물론 부분적으로 usb로 직접 이식 이런 건 막을순 없겠지만 제도적으로 하는 것들이 더 크다고 볼 수 있겠습니다. – 대내나 대외 부분은 다 지금 절차상이라든지 제도적으로 많이 되어있습니다.
		2	– 일단 없는 것보다 있는 게 낫겠죠. 그리고 우리 같은 경우에도 내부적으로 서약서를 쓰게 되어 있고 법에 의해서 처벌을 받게 되어 있으니까 형량은 지금이 적절하다고 봅니다. – 정보통신망 법에 의하면 5년 이하의 징역이나 5천미만의 벌금을 처할 수 있게 되어 있으니까 그 정도면 될 거 같아요
	3	0	– 지금도 국가기밀이 유출된다고 판단이 되는데 각 분야별 정보 공유 체계가 좀 더 긴밀하게 돼야지만 유출 가능성을 낮출 수 있다고 생각합니다. 높다고 생각합니다. – 어차피 인터넷은 오픈공간이고 아마 장비를 가지고 막는다고 해도 질적인 부분을 계속 창과 방패에서 창을 막을 순 없거든요 어느 정도까지는 가능하겠지만 그런 것들이 너무 유기적으로 공유가 안되어 있어서 빨리 뭔가 대책을 만들어야 한다고 생각합니다.

구분	질문 번호		응답 주요 내용
		1	– 개인정보 유출 가능성도 항상 존재하고 있고, 국가기밀 유출만큼 높다고 생각한다. – 이것도 개인정보 유출이라고 하는 건 해커에 의한 부분보다도 내부 근무자들이 개인정보보호를 소홀히 했을 때 그때 문제점이 된다고 봅니다.
		2	– 국가보다는 민간부분이 상당히 좀 더 높겠죠 아무래도 국가는 정부예산으로 각종 아이피씨 정보보호 장비를 구축하고 있기 때문에 시간이 갈수록 격차는 더 크다고..
		3	– 공공분야가 아무래도 좀 더 크겠죠 국가적인 기밀들이 유출된다면 아무래도 우리나라는 좀 대북관계 문제도 있고 그래서 국가기관 유출 피해가 더 크다고 봅니다.
	4	0	– 아무래도 우리나라는 너무 많은 정보를 요구해요 외국처럼 메일주소만 필요하게 만들어 놓은거 보면 개인정보를 관리할 필요도 없고 간소화되면 아무래도 유출된다해도 피해가 적겠죠 너무 복잡합니다 우리나라는.. – 개인정보를 간략하게 해서 메일주소 정도나 할 수 있게 해야 될 거 같습니다. – 아무래도 복잡하면 관리기관이 그 개인정보를 관리해야 하는 부분도 있고, 그게 또 해커에 의해서 탈취가 되면 개인정보 유출되니까 지양이 되어야 할 거 같습니다.
		1	– 글쎄요, 뭐 건전한 인터넷문화 조성이 더 크다고 보구요 이게 지금 보면 악성댓글이랄지 이런 것들이 좀 어떤 위에서 나온 실명제를 도입을 해서 좀 많이 지양이 되야 된다고 생각합니다.
	5	0	– 지금도 이제 국정원 행안부 방통위 각 부처들이 나뉘어져서 사이버안전체계를 구축하고 있는데 제가 볼 때는 어차피 좀 국가정보원이랄지 전문기관에서 관장하는 것이 옳다고 봅니다 – 각 정부 부처들이 사이버체계 가짐으로써 인건비랄지 예산을 더 확보하고 힘을 다지려고 하는 그런 부분들이 크다보니 가장 중요한 컴맨도우가 있어서 그 기관에서 전체를 다 관장하는 그런 체계로 가는 게 옳다고 봅니다.
		1	– 위에서는 어떤 그 관장의 의미고, 밑에는 시설의 의미로 본다면 관장은 중앙에서 관장을 하지만, 시설부분은 각 부문별로 분리가 돼서 이걸을 청합하는 그런 관계로 시설을 구축하면 될 거 같아요 위는 논리적인 부분이고, 아래는 물리적인 부분인데 물리적인 부분은 분산해서 관리하는 그런 형태로 가는 게 좋다고 봅니다.
		2	– 1. 국가정보원 2. 방송통신위원회 3. 행안부
	6	0	– 사이버 안전관리체계가 명확히 구분이 되고, 어떤 의무가 부여가 된다 그러면 위기가 발생했을 때는 그런 어떤 대응체계, 대응 매뉴얼대로 각 부처들이 유관기관들 간의 유기적으로 업무를 수행할 수 있다면 더 빨리 초동조치가 가능하다고 봅니다.
공	1	0	– 인터넷이라는 게 많이 활성화가 되고 생활 깊숙이 아주 전반적으로 젖어들면서 일반적

구분	질문 번호		응답 주요 내용
공 14			으로 우리가 알고 있던 안전에 대한 개념이 사이버 쪽으로 확산이 된거죠. – 뭐 일반적으로 생각하는 안전, 치한 유지나 이런 정도 수준이 되지 않을까요 거기서도 100% 안전한 사회를 만들지는 못하는 것처럼 그걸 위해서 노력하는 것도 그것과 일맥상통하겠죠. 거기에서 말하는 안전도 막아보려고 안전을 유지하려고 하는 것일 뿐이지 100%는 아니기 때문에 70~80%정도 되지 않을까요.
		1	– 해킹 그 다음에 IT기술을 더한 사기, 피싱 여러 가지 IT기술을 통해서 일어날 수 있는 역기능들을 사이버 위기라고 하지 않을까요 – 뭐 이것도 70~80% 정도이지 않을까
	2	0	– 대내적인 것은 정보유출이 되겠고, 대외적은 외부에서 들어오는 해킹 시도나 디도스공격 – 당장은 돈과 관련이 될 수 있으니까요 돈과 레피테이션, 기관의 명예나 이런 것들과 직접적으로 관련이 있으니까요 금융사고도 그렇죠
		1	– 기술적 & 제도적으로 마련이 되어 있죠. 있습니다. 물론 100%는 아니지만.....
		2	– 법이라는 게 솔직히 없다는 얘기는 반대로 자율적으로 뭔가에 통제가 되야 된다는 전제를 하고 있는 건데 솔직히 자율적으로 뭔가를 하게 되면 항상 그에 따른 뭐가 안됐다 왜 그러느냐 반성, 이런 것들이 필요하고요. 자율적으로 했을 때는 항상 보면 통제가 100% 되지 않잖아요. 그런 부분들이 있기 때문에 역시 법이라는 것들이 여러 가지 것들을 법이 의무화하고 강제화하고 하는데 법만큼 중요하고 또 필요한 게 없다고 생각을 하구요. 그러다 보니까 제 생각으로는 법은 뭐 필요하다고 생각을 하는데 현행이 어떤지는 잘 모르겠어요. 근데 현행은 거의 미미한 수준이라고 생각하고 하고 있구요. 그렇다면 분명히 지금보다는 강화되어야 되지 않을까 생각을 하고 있습니다. – 쉽게 얘기해서 소프트웨어를 불법 복제 한다거나 이런 것들에 대해서 지금 처벌이 미약한 수준인데 중국처럼 무자비하게 할 필요는 없겠지만, 그렇더라도 사회적으로 사회적 구성원들이 공감대를 가질 수 있을 정도로는 높아져야 될 거 같고, 그렇다면 일반적으로 경제적인 피해를 입혔다라고 했을 때는 금액을 정확하게 산정을 하고 그 금액에 따라서 벌을 내리잖아요. 그 정도에 비례해서는 올라가야 되지 않을까 싶고, 그렇게 하려면 또 여러 가지 제반들을 측정할 수 있는 것들이 달리 마련돼야 되겠지만 결국은 그 정도 수준까지로 올라가야하지 않을까라는 생각이 드네요.
	3	0	– 높다고 생각한다. IT와 인터넷에 대한 순기능이 사회 다방면에 발전을 가져왔고, 그 만큼 기능도 클 것이다. 국가 기밀이라는 정보 상황에 엑세스할 수 있도록 편리하게 제공해오던 것들이 IT기술이기 때문에 여러 가지 방면에서 생각했을 때 가능성은 편리한 만큼이다.
		1	– 높다고 생각한다. 이것도 마찬가지이다. 눈에 보이지 않은 자산인데 물리적인 것뿐만 아니라 기술적인 방어대책 접근통제 이런 것들이 따라줘야 하는데 사회 전반적인 인프라가 구축되지 않아 시간이 해결해주겠지만 현재로서는 이런 가능성이 크다

구분	질문 번호		응답 주요 내용
		2	– 동인으로 따졌을 때 민간 쪽이 더 높다고 본다. 이해관계가 얽혀있고 실제로 정보의 환금성이라는 것을 따져봤을 때 많은 사람들이 생각을 가질 수 있게 원인 제공으로 되지 않나
		3	– 국가기밀 유출. 개인과 관련된 정보보단 국가과련 정보가 더 가치가 크다고 본다.
	4	0	– 안전한 것은 우리나라처럼 제한적으로나마 본인확인제를 실시하는 것이 더 안전하겠으나, 바람직한 건 답변하기가 어렵다. 우리는 과다한 개인정보를 요청하는 거 같아서 이러한 건 원치 않고 다른 사회적 안전망을 구축해서 이런 부분을 커버해 나가는 게 좋지 매 사이트마다 요구하는 것은 좋지 않다. 외국 사이트들도 위험이 좀 있겠지만 여러 가지 다른 대안이 복합적으로 얽혀서 서로가 서로를 커버할 수 있게 하는 것이 인터넷은 편리하고 실익을 가져가는 것 같다.
		1	– 건전한 인터넷문화 조성이 더 중요한 가치일 것 같다. 궁극적으로 추구해야 하는 가치인 것 같다. 이것을 위해 사이버 안전성도 필요하다
	5	0	– 전자에 대한 부분은 시행착오를 거쳐서 어렵다는 것을 알고 있고, 다뤄야 할 것이 많고, 그 후 2번째 방식으로 넘어와 좀 입증이 되지 않았나 한다. 전자는 실질적으로 효과를 나타내지 못했다.
		1	– 분산관리방식이 더 바람직하다. 5번 문제랑 같다
		2	– 국가정보원, 행정안전부, 법무부
	6	0	– 신고와 주변 파악. 피해 확산을 막기 위해서
공공 15	1	0	– 들어봤다. 완벽한 방어를 기준으로 하는 걸 의미한다. 60% 정도면 안전이라고 생각한다.
		1	– 들어봤다. 어느 정도의 치명적인 위험성이라고 이해한다. 경제적인 손실, 개인정보침해, 이런 것들이 사이버 위기라고 생각한다. – 공격받는 주체에 따라 다르지만 보통 30% 정도면 위험성이라고 생각한다.
	2	0	– 대내적인 것은 정보들을 노출시키는 내부직원이 기업정보 같은 걸 노출시키는 것이고 대외적인 것은 인터넷망을 통해서 정보를 빼가거나 서비스를 완전히 무력화 시키는 것이다. – 자본의 손실, 개인정보 침해 때문에 중요하게 다루어져야 한다.
		1	– 사전 예방방안은 문서화(제도적)되어 있는 것밖에 없고, 사후 대응방안은 기술적으로 많이 되어있는 것 같다.
		2	– 아니다. 효과적일 것 같지 않다. 보통은 이런 것들을 감수하고 그런 위협을 일으키고, 대부분 국내보다는 북한이나 중국에서 많이 이런 일들을 벌이니까 국내에서 형벌을 마련한다고 해도 효과적일 것 같지 않다.

구분	질문 번호		응답 주요 내용
	3	0	– 중간 정도 되는 것 같다. 왜냐하면 항상 새로운 기술이 나오니까 지금 보안수준이 높다고 해도 새로운 기술이 나오게 되면 쓸 수가 없고, 다시 낮아지고 순환되기 때문이다.
		1	– 높은 수준이다. 중소기업 같은 경우는 거의 보안체계가 마련되어 있지 않고, 대기업 같은 경우는 자본을 많이 들여 대응방안을 마련하지만, 중소기업 같은 경우는 하라고 해도 자본금이 적어서 못한다.
		2	– 개인정보 유출이 더 피해가 크다. 국가 기밀은 바꿀 수가 있지만 개인정보는 바꿀 수가 없어서 대응방안 자체가 존재하지 않는다. 군사작전 같은 건 바꾸면 되는데 개인정보는 일단 유출되면 바꿀 수 없기 때문에, 피해가 더 크다.
		3	– 공공분야가 더 심할 것이다. 질 자체가 다르다
	4	0	– 외국사이트가 안전하다고 생각한다. – 외국이 더 바람직하다. 왜냐하면 악성댓글이나 사이버 모욕같은 게 이걸 방지하기 위해서 인터넷 실명제와 제한적 본인확인제를 하는데, 이걸 하기 때문에 악성댓글이 발생하는 거라고 생각한다. 외국같은 경우는 익명으로 할 수 있지만, 우리나라는 무조건 실명으로 해야 되기 때문에 문제가 된다. 악성댓글을 받더라도 어차피 익명이라서 상관없다.
		1	– 사이버 안전성 확보가 중요한 가치인 것 같다. – 인터넷 문화 조성은 자연적으로 조성되는 거 같고, 사이버 안전성 확보는 국가차원에서 조치를 취해야겠다. 안전성이 확보되면 인터넷 문화 조성은 자연적으로 되는 것 같다.
	5	0	– 중앙통제방식이 효과적이다. 적정소관별 분산관리방식은 서로 간의 정보공유가 안 될 것 같고, 지금은 각각을 통제하는 기관이 따로 있어서 잘 되는 거 같다. – 현재 국정원에서 하고 있고, 국가 사이버 안전 센터에서 하는게 맞다. 사이버안전은 방송통신에만 국한되는 것이 아니고 전반적으로 해야 되기 때문에 보안을 담당하는 정부부처에서 하는 것이 맞다고 생각한다.
		1	– 중앙통제 방식이 바람직하고, 국정원에서 하는 것이 바람직하다. 통제가 가능할 것 같은데, 각 시 별로 사이버 안전정책이 구축되어 있는데, 이런 걸 통제하려면 정부에서 하는 게 맞는 것 같다.
		2	– 국가정보원, 행정안전부, 방송통신위원회
	6	0	– 전파이다. 위협이 발생했을 때 얼마나 빠르게 전파하고 대응하느냐가 중요하다
공공 1	1	0	– 대부분의 정보나 기업의 문서 처리 등이 인터넷으로 소통이 되고 있고 모든 정보에 대해서 기존의 인터넷이라는 자체적으로 개방성의 의미를 갖고 있고, 보안, 안전에 대한 체계가 개체되지 않으면 정보 유출의 가능성이 충분히 열려있고, 사이버안전이라 한다면 각 개인, 정보에 대한 보안 각 개인의 프라이버시, 국가 차원에서는 국가 보안과 밀접한 관

구분	질문 번호		응답 주요 내용
6			계를 가지고 있다. – 안전은 100%로 안전이 되어야 한다.
		1	– 사이버위기는 사이버 안전의 반대로 사용할 수 있다. 결국은 정보화의 역기능 중 하나이다. – 각 개인적인 프라이버시 측면에서는 조금이라도 침해가 된다면 위기라고 볼 수 있다. 정보 역시 유출, 노출, 침해 등 일어날 수 있다면 해킹들이 있다면 사이버 위기라고 볼 수 있다. – 1%의 위험도 있어서는 안 된다.
	2	0	– 국가적 측면에서 대외 대내적으로 DDoS공격이나 이런 것들이 상당히 많이 있어 대외적인 시스템 네트워크 안정성, 사이버 안전이라 한다면 결국은 7·7사태와 같은 DDoS를 대외적인 사이버 위협 요인이라 볼 수 있으며, 대내적으로 기업이나 대학이라고 본다면 대학내, 회사 내 각종 자산에 대한 정보시스템 등이 정보시스템을 물리적으로 또는 여러 가지 목적으로 공격하는 게 있을 수 있으며 단순히 정보를 끄집어내어 갈수도 있으며, 대내적인 위협요소로 볼 수 있으며, 각 개인의 측면은 개인의 pc나 개인의 스마트폰의 정보 등을 외부로 유출이 되었을 경우 개인적인 보안 위험이라고 볼 수 있다. – 국가, 기업, 개인 3가지로 볼 수 있다.
		1	– 상당히 많이 구축되어 있다. 제도적으로나 기술적으로 준비를 다 해놓고 있고, 제도적으로는 법적으로 확립이 되어 있으며, 기술적인 측면에서 본다면 대학이나 연구소 기업체에서 연구들을 많이 해오고 있다. 다만 문제점이 될 수 있는 것들은 새로운 장비나 서비스들이 나오므로 그것에 대한 기술은 선개발될 가능성이 없으므로 제도적으로 보안이 되어야 한다.
		2	– 정보화 사회가 개방이 되면서 유출되는 정보들은 더 많아질 수밖에 없으며, 따라서 기존의 법 제도적인 측면에서 본다면 점진적으로는 증가가 될 필요가 있다. – 사이버 위협 ,위기를 통해 기업, 개인이 받은 피해보다 더 높은 형량을 많이 줘야 한다.
	3	0	– 국가 기밀이 유출될 가능성은 내부적으로 있을 수도 있고, 가장 큰 요인은 사이버 요인이나 중국발 공격이나 제 3의 공격에 의해 있을수 있다.
		1	– 사이버 공격은 국가기밀을 유출하기 위해서 사용하는 기법이나 현상 등이고, 사이버 침해 는 개인 정보와 관련성이 높다. pc나 핸드폰으로 개인정보를 유출될 가능성이 상대적으로 높아질 것이다.
		2	– 국가 차원에서는 상당히 잘 대응하고 있고, 민간분야는 큰 대기업에서야 CSO보안 접문가가 중요 임원으로 배정되고, 기술적인 투자가 이루어져서 문제가 되지 않으며, 중소기업만 하더라도 보안에 대한 인식도가 높지 않아 개인정보가 상대적으로 유출될 가능성이 높다.
		3	– 사이버 공격은 주로 국가의 기관 등이 될 것이고, 그래서 국가의 공공기관이 더 피해가 클 것이다. 침해는 개인정보 유출에 관련성이 있을 것이다.

구분	질문 번호		응답 주요 내용
	4	0	– 안전이란 것을 봤을 때 개인정보가 유출되는 것을 봤을 때 이메일은 오픈되어 있는 정보지만 주민등록이나 주소나 그런 것들을 추가적으로 기입을 한다면 당연히 개인정보는 이메일보다 안전할 것이다. 이메일만 가지고 가입을 요구한다면 그 사람이 누구인지 인증을 못한다. – 바람직한 건 우리나라에서 하는 것이 보안상에 다 이유가 있어서 하는 것이다. 주민등록번호까지 확인해야하나 해서 제도까지 나와 있고, 전자상거래에서 공인 인증서까지 나와 있다. 따라서 바람직한 건 우리나라가 더 바람직한다.
		1	– 둘 다 중요하다. 건전한 인터넷문화 조성을 통해서 국민의 전체적인 의식이나 인식이 바뀐다면 당연히 사이버 안전성은 더 높아질 것이다. 아무래도 기술적 제도적으로 사이버 안전성이 우선적으로 확보된다.
	5	0	– 중앙집중이 됐을 경우 사이버 공격에 대상이 될 수 있고, 가장 바람직한건 분산처리 분산관리 방식이 더 바람직하다.
		1	– 분산관리방식
		2	– 국가정보원, 행정안전부, 방송통신위원회
	6	0	– 매뉴얼이 더 있어야 한다. 사전대응 방법 체계 등이 다 있어야 한다. 국가 기관 망에 대한 안전성을 확보해야한다.
공공 17	1	0	– 불순한 의도에 의해 외부의 정보 쪽에 이런 것의 침입이 있을 때 데이터를 구하기 위해서 쓰는 것 – 70%
		1	– 개인적인 것 보다는 기업이라던가. 국가에서 적용시켜야 한다. 위기가 현대전에서 물리적인 것 보다는 사이버 쪽으로 전산망을 마비시키는 그런 걸로 결부시켜서 이야기해야 한다. – 30%
	2	0	– 사이버 안전을 아무리 구축해도 개개인이 심각성을 잘 모르고 미리 대비를 안하면 아무리 대비를 철저히 해도 사람들의 인식이라던가. 습관처럼 해야 한다. – 사이버를 안전화 하려면 시스템을 1차적으로 구축해야 되고 2차적으로 지침을 만들어야 하고, 사용자들이 안 지키면 무용지물이 되기 때문에 맨 아래의 사람의 인식이 가장 중요하다.
		1	– 기술적으로 보면 행안부 필 제품들도 있고 제도적으로 보면 정부보안 지침들이 업데이트되고 보안 감사에서 지적을 하기 때문에 요즘에는 마련되어 있다고 생각을 한다.
		2	– 효과적이진 않다. 불순한 의도로 사용한다면 좀 더 안 걸리게 하지 표면적으로 형벌이 있다고 안 쓸 것 같지는 않다.

구분	질문 번호		응답 주요 내용
	3	0	– 높은 수준인 것 같다. 우리나라의 인프라가 잘 되어 있어 접근성이 좋아 안전불감증이 남아 있어도 높은 수준인거 같다.
		1	– 높은 것 같다. 홈페이지를 가입할 때 아이핀을 사용한다 해도 위험하고, 외국같은 경우에도 간단하게 이메일만 적으면 되고, 우리나라 같은 경우에는 회원 가입시 개인정보를 요구하고 그것에 대해 보안이 잘 되어 있는 것도 아니기 때문이다.
		2	– 개인정보 유출이 높을거 같다. 중요정보를 다루는 공공정부나 지자체에서 인프라망과 내부망을 분리해서 쓰고 있어 민간분야보다 적다고 생각한다.
		3	– 유출 리스크를 보면 국가기밀 쪽이다. – 민간 분야를 보면 금전적이거나 개인에 국한되어 있어 피해에 대한 후폭풍이나 리스크를 보면 국가 기밀이 유출됐을 때 국가기밀이 더 높아서.
	4	0	– 간단한 정보로 회원가입을 하는 게 안전하다고 본다 – 간단한 정보만 쓴다는것이 유출될 데이터 자체가 줄어들기 때문이다. 바람직한 건 보안체계가 갖추어진 상태에서 일정 부분에 대해 개인정보를 요구하는 게 더 바람직해 보인다.
		1	– 사이버 안전성이다. – 인식변화로는 일어날 수 없다. 기술적이나 제도적이 있어야 하고 개개인의 인식도 있어야 한다. 건전한 인터넷문화는 인식변화만 있다면 이루어질 수 있는 문제이기 때문이다.
	5	0	– 반반씩 섞여야 한다. – 강력한 중앙 통제 방식은 중앙에서 통제를 해야 하나 중앙이 뚫리면 걷잡을 수 없어 중앙통제방식으로 통제를 하며 개개별로 사이버 안전이나 이런 걸 구축해야지 보안이 될 것이다.
		1	– 5번이랑 같다.
		2	– 국가정보원, 행정안전부, 방송통신위원회
	6	0	– 차단이다. – 침입을 막기 위해서 차단이 가장 중요하고, 근원을 찾는 것도 중요하지만 데이터 유실이나 정보 유출을 가장 먼저 막고, 침입 근원을 찾는 게 중요하다.
민간 1	1	0	– 네, 사이버 안전이란게 우리가 보통 일반적으로 물리적인 부분에서 가상된 공간으로 인터넷이란 가상공간에서 이뤄지는 전반적인 내용 – 85~90% 안전하다고 생각한다.
		1	– 사이버 위기는 군대에서 듣는 전시상황이라고 생각하면 된다. 실제적으로는 보이지 않지만 실제 따지고 들어가다 보면 그 안에 보이지 않는 굉장한 피해가 있다. – 50% 정도 되면 위기라고 생각한다.

구분	질문 번호		응답 주요 내용
	2	0	– 네트워크를 위한다거나 보안장비들이 위에서 그 안에 있는 데이터, 데이터베이스에 있는 데이터를 추출하거나 파괴하거나 유출하는 큰 부분이다 (대내, 대외 마찬가지이다). – 1차 피해로 가는게 아니라 2차 피해로 가는데, 1차 피해는 직접적으로 그게 네트워크 망을 못 쓰게 하거나 실제 사용을 못하게 하는 직접적 피해를 오는데, 데이터 유출이나 기술자료 유출 이런 것들은 바로 나타나는 것이 아니라 나중에 나타나는 것이다.
		1	– 많이 되어 있다. 진행도 되고 있다. 기술적으로는 80–90%, 제도적으로 60% 정도 되어 있다. 공공기관 위주로 하고 있는데, 정보 보호 관리체계라든지 개인 정보 보호관리 체계라든지 이런 부분이 잘 되어 있다.
		2	– 효과적일 것이다. – 벌금형 형태가 좀더 강화되면 기업체나 정부들이 경각심을 가지고 좀 더 잘하지 않을까 싶다.
	3	0	– 높다. 우리나라는 정보통신이 잘 발달되어 있고, 인터넷 망이 잘 되어 있다. 망이 잘 되어있다는 말은 그만큼 망이 뚫릴 가능성이 높다는 말인데, 우리나라 자체가 대북관계도 있고, 사회적 대립관계도 있고, 망 자체 인프라가 좋다. 망이 좋은 만큼 그만큼 위험성도 많다.
		1	– 높다. 모바일적으로 많이 넘어가고 있고 고정된 데에서 이동하는 형태로 넘어가는 시간의 변화가 하나 있고, 이 데이터가 예전에는 크게 가치가 없었는데 지금은 개인 데이터가 돈으로 따질 수가 없어서 이런 걸 이용할 가능성이 높다.
		2	– 개인정보가 유출될 가능성이 높다. 그만큼 정부에서 하는 투자에 대한 부족한 부분이 있고, 관리적인 부분이 가장 크다.
		3	– 공공부분이 피해가 크다. 공공부분 관련된 부분은 정치적인 것, 전쟁관련된 것들 이런 거라서 한번 유출되면 피해가 크다.
	4	0	– 외국이 더 안전하다. 자료가 적으면 적을수록 나갈 수 있는 게 적기 때문이다. – 보는 관점에 따라 다른데, 관리자나 사업가들 사이에서는 정보가 많았으면 좋겠고 사용자 입장에서는 외국처럼 하는 게 좋다.
		1	– 사이버 안전성 확보이다. 안전성은 당장 대원해 줄 수 있는 체계를 마련하는 것 인프라를 먼저 해놓고 제도를 바꾸는 것이 맞는 것 같다.
	5	0	– 중앙통제방식이 더 좋다. 처음 할때는 컨트롤 관리를 해야하기 때문이다. – 국정원이랑 행정안전부 쪽에서 했으면 좋겠다. 실무적인 것은 행정 안전부에서 해야되는 것 같다. 실무적인 일은 행정 안전부고, 정책을 내리는 것은 국정원이라서 행정 안전부에서 해야된다.

구분	질문 번호		응답 주요 내용
		1	– 실행차원에서 중앙통제방식이 바람직하다고 생각한다.
		2	– 국정원, 행안부, 경찰청
	6	0	– 상황전파이다. 정확한 상황이 신속하게 전달되어야 한다.
민간 2	1	0	– 컴퓨터 네트워크 상에서 안전, 정보 보호나 그런 쪽으로 이해, 개념이 확대되 정보가 선을 따라가는 것뿐만 아니라 공간중으로 가는 것도 있으므로 그것에 대한 시큐리티도 중요하다.
		1	– 우리가 안전하게 시큐리티가 필요한 내용이 중요하다. 1%나 100%로 나누는 건 힘들고 정보의 내용으로 반드시 보안이 유지되어야 할 정보는 100%로 유출이 되면 안 되고, 사소한 것은 조금씩 되도 괜찮지 않나. – 사이버 위기는 아주 심각한다. 네트워크에 걸려있는 저장되어 있는 정보는 자기 정보가 아니라 하는 아주 위험한 위기이다. 정보에 따라서 1%도, 100%도 안 된다.
	2	0	– 해킹 같은 것이 중요하다. 지금 사회의 여러 가지 기반 시설들이 컴퓨터나 전자정보통신기기를 빼놓고 이야기 할 수 없기 때문에 정보통신기기라는 것이 전부 물려서 연동되어 있기 때문에 중요하게 다룰 수밖에 없다.
		1	– 상당 부분 되어 있다 제도적으로 관련된 기술기준을 만들어야 하고 기술적으로 소프트웨어 하드웨어적으로 정보 보호를 하기위한 대책들이 되어 있다. 이런 것들이 많은 사람들한테 쉽게 사용되려고 한다면.. 되어 있는 것 같다.
		2	– 강하게 처벌해야 한다. 지금 정보와 관련해서 범죄들이 줄어들면 지금 형벌로도 충분하며, 범죄들이 더 많아지면 더욱 강화해야 한다. 범죄발생률이라든지 비용을 계산해야 한다.
	3	0	– 정보통신기기 사용이 증가되는 만큼 유출될 가능성도 높아진다.
		1	– 마찬가지다.
		2	개인적 유출이 더 많을것이다..
		3	– 공공분야가 더 심할 것이다. 질 자체가 다르다.
	4	0	– 국가에서 하는게 더 안전하다. – 우리나라 제도가 더 바람직하다.
		1	– 둘 다 중요하다, 정보의 질과 관계가 있다. 중요한 정보가 들어있지 않고, 많은 구성원들이 자기의 의견을 논의하고 그런 정도의 정보의 질이라면, 인터넷 문화조성에 더 중요할 것이고, 인터넷 중에 국가기관과 연관되어 있으면 사이버 안전성이 더 중요할 것이다.
	5	0	– 중앙통제하면서 각 부처들에게 권한을 줘서 중앙에서 충분히 제어를 할 수 있어야 관리가 될 것이다. 정보통신망이라는 것 자체가 전부 연결되어 있기 때문에 어디 한군데에서 봐줘야 한다. 사이버 안전과 관련해서 제일 적극적이고 제일 전문성 있고 부처의 미션으로 본다면 국정원에서 해야 한다.

구분	질문 번호		응답 주요 내용
		1	– 효과적인 것이 바람직한 것이다.
		2	– 국가정보원, 행정안전부, 경찰청
	6	0	– 일단 사용자한테 알리는 것이 중요하고, 발생 원인을 제거하는 것, 제거하기 위해서 여러 가지 조치가 중요하다.
민간 3	1	0	– 여기서 말하는 사이버안전이란 외부자에 의한 침입이 불가능하고 그게 가장 크죠 외부에서의 침입이나 침투가 불가능하다고 말합니다. – 80%
		1	– 쉽게 말하면 뚫렸다는 얘기예요. 외부자에 의한 침입이나 흔적 같은 것이 남았을 경우에 위기라고 하는데 어쨌든 간에 위기라는 말을 쓰는 거 자체가 뚫리고 향후에도 또 한 번의 어떤 문제점이 생길 수 있을 때만이 위기라고 얘기하죠. – 한 60% 정도 위험성이 있죠.
	2	0	– 대내적으로는 직원들이 어떤 악의적인 생각으로 정보를 외부로 빼돌리는 경우, 내부자의 의한 정보가 유출이 되는 경우에 대내적으로 위험하다고 볼 수 있는 것이죠 대외적으로는 해커의 침입, DDOS 같은 것들이 위험하다고 볼 수 있죠. – 사이버상의 안전을 위협하기 때문에 중요하게 다뤄줘야 되겠죠. 가장 큰 거는 사이버안전이라고 하는 거는 결국에는 그 중요한 끝까지 올라가면 나라로 봤을 때 국보에 대한 정보가 유출이 되는 경우 피해금액이 수조원에 이를 정도로 굉장히 크고 일반 기업에서도 중요한 문서들이 몇천 억, 몇백 억에 달하는 금전적 손실이 크다고 봐야죠. 정보에 대한 유출이 가장 크겠죠.
		1	– 어느 정도는 있다고 봅니다. 제도는 모르겠는데 기술적으로는 일반기업이나 공공기관들이 방화벽부터 해가지고 통화보안장비, 각종 이메일관련된 것들 뭐 여러 가지로 기술적으로는 많이 도입을 하고 있어요. 제품들 같은 경우에도 실질적으로도 많이 맡고 있고.
		2	– 효과 있다 봅니다. 법적인 강력한 제도가 있다고 하면은 특히 민간 기업은 모르겠는데 일반 공공기관 같은 경우에는 그런 법적인 제도나 장치가 있다고 하면은 분명히 더 관심을 갖고 신경을 쓰겠죠. – 공공기관의 장이 구속되는 뭐 그 정도까지 갈 수 있겠죠. 최고는 벌금형
	3	0	– 높다고 생각은 안합니다. 기본적으로 사이버공격이나 이런 거에 대해서 우리나라도 어느정도 막을 수 있는 시스템이 다 되어 있고요 국가기밀이 유출되기 직전에 다 이미 포착을 하고 저희가 알고 있다고 보기 때문에 유출이 될 가능성은 희박하다고 봅니다.
		1	– 이거는 가능성이 높습니다. 개인정보를 다루고 있는 데들이 공공기관도 있지만 일반기업들도 굉장히 많이 다루고 있는데 일반기업들은 보안시스템이 굉장히 취약합니다.그렇기 때문에 가능성이 높다고 봐야죠.

구분	질문 번호		응답 주요 내용
		2	– 3번과 3–1번에서 이미 얘기함.
		3	– 당연히 민간분야가 개인 정보 유출이 크다고 봐야죠. 그게 아까 국가 쪽에는 나름 시스템이 잘 돼 있어요. 그리고 이미 공격이 되는 순간에 포착이 되기 때문에 다 알 수가 있는데 민간 쪽은 굉장히 취약하기 때문에 개인정보를 다루는 데들이 이런 시스템이 많지가 않아요. 쉽게 개인정보가 유출된다고 봐야죠.
	4	0	– 바람직한 거는 주민번호가 들어가는 게 사실은 바람직하다고 보죠 악성댓글이나 사이버 모욕 같은 것도 여기에도 나와 있지만은 실명제가 안되면은 인터넷상은 진짜 엉망이 되거든요 충분히 필요한데 주민등록번호를 사실 입력하므로 인해서 자기 정보가 유출될 수 있는 부분에 안전하지 않죠. 이걸 병합해서, 혼합해서 좀 더 다른 부분으로 아이핀제도가 도입이 되면 괜찮을 거 같습니다.
		1	– 다 중요한데.. 근데 뭐 기본적으로 건전한 인터넷문화가 조성되면은 사이버 안전성이 확보가 될 수 있는데..... 건전한 인터넷문화 조성이 더 나을 거 같아요. 그게 조성이 되고 하면은 충분히 인터넷 문화에 대해서 사람들이 많이 알고 하면은 이게 결국에는 사이버 안전성과 연결이 될 거라고 보기 때문에 건전한 인터넷 문화가 먼저 조성이 되는 기본 바탕 하에 사이버안전이 확보가 되야 더욱더 안전이 될 거 같거든요.
	5	0	– 아무래도 비용적인 부분에서는 중앙통제방식이 낫지 않을까 생각을 해요. 분산하면은 좀 좋은 관중도 있을 거 같은데 한 곳의 중앙에서 통제를 하는 게 좀 더 효과적이지 않을까 다 개별로 구축할 필요 없이 한 곳만 하고 관리를 하는 게 낫지 않을까 싶거든요. – 그래도 행안부가 낫지 않을까 싶거든요 우선 행안부가 정보보안, 사이버보안 이쪽 관련된 것들 여러 가지로 하고 잇고 부처 중에서도 행안부가 하는 게 국민의 생활과 밀접한 관계가 있다고 보거든요.
		1	– 중앙통제가 바람직하다 이유는 5번과 같은 맥락이고 또 과거에 사이버, 정보보안과 관련된 것은 행안부가 예전부터 많이 해왔던 부분도 있고, 방통위 부처가 너무 작고 국정원은 그런 거 같고 행안부가 제일 적당하다고 생각합니다.
		2	– 1. 방통위 2. 행안부 3. 국정원
	6	0	– 가장 중요한 것은 먼저 바로 국민한테 알려주는 게 가장 급선무겠죠 전 나라가 다 퍼질 수 있고 좀비pc 만드는 것도 있기 때문에 중요한 거는 현재 KISA를 통해서 빠른 시일 내에 우선은 일반 시민들한테 알릴 수 있었으면 좋겠구요. 그 전에 행안부나 국정원, KISA 정보 보안 관련된 사이버 보안 관련된 부처들이 회의를 바로 해서 문제점에 대해서 바로 지적하고 대응방안을 찾는 것도 중요하지 않을까, 알리는 게 가장 중요하지 않을까 싶습니다.
민간 4	1	0	– 의미적으로 봤을 때 '침해'의 요인이 될 수 있는 모든 가능성에 대한 보호라고 생각된다. 사이버 공간 내에서 '개인정보'를 포함한 수많은 2차적 3차적 정보에 대한 보호조치가 이에 포함되며 '데이터 통신' 및 '통신 전후 의 기록'에 대한 안전까지 보장할 수 있는 것을 의미한다고 생각한다. 크게 2가지로 보자면 사이버 공간 내에서 할

구분	질문 번호		응답 주요 내용
			수 있는 행위(과정)에 대한 안전과 그 행위를 하고자 할 항목 혹은 행위를 통해 얻은 부산물, 즉 데이터에 대한 안전이라고 생각된다. 사이버 안전은 이러한 과정 및 과정을 통해 얻거나 수정되는 데이터들에 대한 보호를 의미 한다고 생각된다.
		1	– ‘사이버 위기’ 시스템 및 네트워크를 통한 공격이 실제로 이루어지지 않았다 하더라도 공격 가능성이 있는 상태를 포함하여 실제로 공격이 이루어지고 그로 인한 피해를 받은 상태로 재공격의 위험성이 있는 상태를 사이버 위기라고 생각한다. 다시 정리하자면 공격 자체가 치명적이지 않다고 하더라도 공격받을 가능성 및 공격으로 인해 피해를 입을 가능성이 있는 것을 나타낸다고 생각한다. 작년에 있었던 DDoS 공격을 떠올리면 그 당시 외국 서버에서 한국으로 이어진 프록시 자체를 차단하여 외국계 주요 업체 등의 사이트를 포함하여 인터넷망 연결 자체가 안되기도 했었으니 그 위험성이 어느정도인지 또한 얼마나 치명적인 형태로 작용하는지는 이러한 예만 봐도 알 수 있을꺼라 생각된다.
	2	0	–
		1	– 기술적&제도적 제도적인 것은 잘 모르겠으나 기술적 요인에 대해서는 시스템 및 네트워크 감시, 트래픽 감시를 포함하여 사이버 상의 공격 및 위협을 감지하고 이를 통한 해당 IP 대역 및 트래픽을 차단함으로서 네트워크 관리를 용이하게 하고 안전성을 확보하는 도구가 있다. 이러한 도구들은 하드웨어적 경향을 띄고 있는 것들도 있으나 간단한 보안성을 지닌 소프트웨어 형태의 프리웨어로서 웹상에서 제공되고 있는 경우도 있으니 이를 활용하는 것도 좋은 것은 물론 암호화나 인증에 대한 키 값 관리 등 사전에 준비할 수 있는 많은 방법등이 있다. 사후시에는 먼저 공격에 대한 피해정도를 파악하고 변조된 데이터 및 로그 기록 등을 통한 포렌식 기술 등을 이용, 데이터 복구 및 증거 확보 작업 등을 통해 빠른 피해복구 과정을 체계적으로 구성해 놓는 것이 좋다.
		2	– 어느 정도 효과는 있을 것이라 생각된다. 위협요인 자체가 공격 대상으로 하여금 피해를 입힐 수 있기 때문에 그에 대한 대응 방안으로서 엄중한 형벌이 필요하리라 생각된다. 이는 위협 요인을 행하는 자체에 대한 경각심을 불러 일으키는 것은 물론 현행보다 더욱 무겁게 처벌함으로서 재범의 가능성 또한 배제할 수 있다.
	3	0	– 대체적으로 국가 기밀은 사이버 인터넷 공간에서 인트라넷 형태의 망을 이용하는 것으로 알고 있다. 법무기관 등의 공공 기관이 그러하며 내부적 네트워크망을 형성하여 내부적으로 데이터를 순환시키기 때문에 안전성에 있어서 내부적으로 접근하지 않는 한 외부적 공격에 의해 유출될 가능성이 적다고 볼 수 있다. 하지만 내부적으로 직접 접근한 공격자가 있다면 상황은 달라진다. 외부에서의 접근 가능성을 완전 배제하는 가정하에 내부에서의 사이버 공격에 있어서는 그 취약성이 두드러지게 드러난다. 중기업 및 대기업에서 제공하는 보안망에서도 위같은 가정하에 운영 및 몇몇 감시 도구와 로그 분석 등의 기본 망 형태로 구성되어 있는 경우가 많으며 기본적으로 인터넷에서 제공하는 보안 모듈조차 제공되고 있지 않는 경우가 많다. 이는 내부 망 자체에서는 무분별한 접근 가능성을 배제하고 있기 때문일 것이다.
		1	– 개인정보가 유출될 가능성이 높다. 일반적으로 대부분의 사이트가 ‘회원 가입’ 및 ‘개인정보 수정’ 혹은 부가적으로 내놓은 서비스 등에 있어서 사용자의 개인 정보를 요구하고 있다. 문제는 해당 사이트의 보안성이 높고 낮음에 상관없이 대부분의 사이트가

구분	질문 번호		응답 주요 내용
			개인정보를 요구한다는 점에 있다. 예를 들어 사용자가 주로 쓰는 아이디를 알고 있는 상태에서 사이버 공격을 행한다고 한다면 공격자는 해당 아이디를 이용하여 사용자가 가입한 사이트 등을 알 수가 있고 이에 대한 보안정도를 체크하여 공격 대상의 다른 여러 유형의 정보를 얻을 수 있다. 또한 보안 정도가 낮은 사이트에서 얻게 된 정보를 공격자가 이용한다면 보안도가 높은 사이트에 대해서도 공격 대상에 대한 개인 정보를 유출시킬 수도 있다. 더구나 사이버 공간은 하나의 거대한 소사이어티를 이루면서 남들과는 개별성을 이루기 위해 사용자의 개인정보를 공개적으로 드러낸 사이트 등도 많이 있다. 하지만 이에 대한 보안은 드러낸 정보에 비해 취약한 편이기 때문에 사이버 공격 또는 사이버 침해에 의하여 개인 정보가 유출될 가능성이 높다고 본다.
		2	– 민간분야에서의 개인정보가 유출될 가능성이 높은 것으로 알고있다. 물론 다소 차이는 있을 수 있으나 민간 정보의 접근성이 더 용이하고 보안 또한 더욱 뛰어난 경우가 많기 때문이다. 여기서 먼저 접근성을 보자면 공공기관의 경우 중요도가 높은 기밀 정보를 다루는 서버가 있으며 그에 대한 보안을 체계적으로 구성해 놓을 수 있으나 민간 분야의 경우 개인 정보가 특정 서버에만 머무르는 것이 아니라 개인의 취미나 특징적 요소, 혹은 관심사에 따라 다양한 민간분야에 같은 형태의 개인정보가 저장되어 있을 가능성이 크다. 또한 이런 접근성 말고도 공공분야의 경우 특정 보안협력업체 등과 연계되어 기밀 정보를 관리하거나 자체 규명된 보안 모듈을 둠으로서 정보를 보호하고 있으나 민간분야에서 체계적이고 구체적인 개인정보 관리는 몇몇 전문분야를 제외하곤 기대하기 힘들다.
		3	– 국가 기밀과 개인정보. 국가와 국민, 내가 보기에는 피해의 기준을 어떻게 잡느냐에 따라 피해의 크기가 어느 한쪽으로 기울 수 있을 것 같다. 국가적 피해와 국민의 피해. 예전 옥션과 이베이를 비롯 해킹을 통한 가입자들의 개인정보 유출사건이 떠오른다. 민간기업체의 손해 배상은 물론이거니와 기업의 이미지 또한 추락하여 해당 서비스를 제공했던 민간 기업으로 볼 때 막대한 데미지를 얻었던 것으로 기억한다. 이러한 한 예와 국내 반도체 기술을 외국으로 팔아넘겼던 과거 사례. 국민들 개개인이 입은 피해와 국가적 손실, 이 두가지 중에서 어떤 것이 더 피해가 크다고 할 수 있을까.
	4	0	–내가 알고 있기로는 인터넷 실명제, 혹은 제한적 본인 확인제를 가장하여 개인정보를 수집하려는 곳 또한 많이 있으며 대형 사이버 마켓 등에서도 이런 식으로 수집한 정보를 광고성 글, 스팸 등으로 이용하려는 곳이 있는 것을 종종 보아왔다. 하지만 문항에서 보이는 것과 마찬가지로 악성 댓글이나 사이버 테러 등의 공격을 방지하기 위해선 개인정보가 필요할 수 있다. 따라서 이 두 가지 경우에 생기는 문제점을 정리해보면 사용자가 누군지 알 수 있는 개별성을 띄고 있으면서도 '주민등록번호'처럼 중요도가 높은 정보가 아닌 중요도가 낮은 정보를 필요로 한다는 점에 있다. 즉 인증된 사용자임을 알 수 있는 그러면서도 중요도는 낮은 정보(알아도 쓸 수 없거나 쓰기 어려운 정보)가 필요하다는 것이다. 따라서 일부 사이트에서는 공인인증서를 이용한 가입도 있으나 PIN 값(개별성을 띄고 있으나 PIN을 보고 사용자를 바로 알기는 어려움) 등을 이용한 회원가입도 고려하고 있다. 따라서 이 같은 방식 더 바람직하다고 생각되며 여기에 'OTP'를 접목시켜 보안적 측면에서 기밀성과 무결성을 높이면 어떨까 하는 생각이 든다.
		1	– 내가 보기엔 사이버 안전성 확보라고 생각된다. 이는 '안전한 사이버 세계 확보 후 건전한 인터넷 문화를 조성하는가?' 와 '건전한 인터넷 문화를 조성한 후 사이버 안전성을 확보하는가?' 라고 우선순위를 두어 각각의 경우에 생길 수 있는 문제점에 대해 생각 및 판단해보면 보다 더 쉽게 답이 나올 것라고 생각된다. 물론 흉흉한 뉴스가 하루가 다르게 터져 나오고 있는 상황에서 '건전한 인터넷 문화' 또한 중요하다 하지 않을 수 없겠지만 실질적으로 보자면 사이버 안전성이 확보되지 않은 상태에서 건전한 인터넷

구분	질문 번호		응답 주요 내용
			문화 조성에 노력을 기울인다 한들 제대로 된 '건전한 인터넷 문화'가 조성되지 않을 가능성이 높다. (공격자에 의한 사이버 테러 등을 감안한다면) 이것은 '건전한 인터넷 문화를 조성하기 위해 사이버 안전성을 확보해야 할 필요성이 있다'라고도 해석될 수 있다. 따라서 건전한 인터넷 문화 조성 보다는 사이버 안전성 확보가 더 중요하다고 생각된다.
	5	0	– 그물망형 적정소관별 분산 관리 방식이 효과적이라고 생각한다. 강력한 중앙통제방식의 경우 간혹 DDoS Attack과 같은 형태의 사이버 테러라도 받게 될 시 문제가 커질 수도 있을 뿐더러 안전체계에 대한 명령 중 잘못된 경우라도 생길 시 중앙을 중심으로 전체적인 오류가 발생하게 될 수도 있다. 또한 통제 시스템이 특정하게 드러나게 되므로 자칫 사이버 침해의 주요 타겟이 될 수도 있다.
		1	– 위의 답안과 동일
		2	– 국가정보원, 행정안전부, 방송통신위원회
	6	0	–사이버 위기가 될 수 있는 공격 방법 및 이에 대한 초동조치 또한 각각 개별성을 띄고 있는 경우가 많아 뚜렷하게 대답하기 어렵지만 주요 공격 기법에 대한 초동조치로서 생각하자면 정보동결이라고 생각한다. 여기서 정보 동결은 말 그대로 정보에 대한 모든 접근 가능성을 끊어놓는 것으로 일종의 Interrupt라고 생각하면 될 것이다. 이는 공격자가 얻게 될 정보를 악용할 수 있는 가능성을 배제하기 위한 것으로 사이버 위기 발생 시 정보의 안전한 보호를 위해 필요하다고 생각된다. 가. 정보 동결 (정보의 접근 가능성 배제) 나. 발생한 사이버 위기상황에 대해 분석 다. 분석한 내용을 바탕으로 대응 방안 모색 라. 대응 방안을 통하여 같은 유형의 위기 발생 시 빠른 초동조치 (초동조치 유형에 따라 첫번째 항목이 바뀔 수 있음)
민간 5	1	0	– 들어봤음. – 인터넷 등 가상의 환경에서 받을 수 있는 개인, 기업, 국가의 피해 – % 표현 어려움, 실환경과 동일한 보호를 받아야 할 것 같음.
		1	– 들어봤음. – 사이버 테러, 인터넷 루머/비방/시위 및 서비스 차단/중지/위변조 등의 행위 – %로 표현하기 어려움.
	2	0	– DDoS 공격 및 주요 정보 해킹(유출) – 기업이나 국가의 주요 기능 마비 및 고객정보 오/남용 시킬 수 있음.
		1	– 대응 방안으로는 DDoS 방어 시스템 및 침해사고에 대한 대응 프로세스 있음. – 사전 예방방안은 상당히 어려우며, 국내 유/무선 ISP 및 국제적으로 사전 교류와 정보 교환을 통해 철저히 예방해야 함.
		2	– 현행보다 무겁게 처벌한다고 해서 보다 효과적일 것 같지는 않음(무게 형벌 대비 black market에서 얻는 이익이 클 것으로 보임)

구분	질문 번호		응답 주요 내용
			– 형벌보다는 전 국가적으로 홍보 및 문화 형성을 통해 사전 위협요인을 제거하는 것이 훨씬 효과적일 것임.
	3	0	– 국가기밀의 수준에 따라 다르겠지만, 높다고 생각함 (국가기밀을 다루는 인력에 대한 정보보호 마인드가 낮음)
		1	– 높다고 생각함. (아직 중/소 site의 경우 적절한 기술적/관리적 조치가 미흡한 실정임. 예를 들어 DB암호화 등도 아직 안된 곳이 많으며 기본적인 SQL injection 공격 등에 취약함)
		2	– 민간분야가 높다고 생각하며, 상대적으로 보안에 취약한 업체가 많음.
		3	– 국가 기밀 유출이 더 클 것임.(국가 위협과 직접적으로 연관)
	4	0	– 가입절차를 좀 더 간소화하여 되도록 개인정보 자체가 인터넷 등 open된 공간으로 정보 flow가 차단되어야 함. 오히려 외국의 경우 훨씬 안전하며 바람직하지 않나 생각됨
		1	– 질문자체가 모호함. 당연히 둘 다 중요함. 닭이 먼저냐, 알이 먼저냐 질문과 똑같음.
	5	0	– 안전체계 구축은 중앙통제방식으로 하고, 각 부서별 담당 조직을 두는 것이 효과적임. – 중앙통제방식이 사이버 문제등 긴급 대응 시 유리함. – 개인적인 의견으로는 대통령 직속이 사이버위협 관리 담당 부처를 신설하고 각 부처별 (국정원/행안부/방통위 등) 서로 co-work 할 수 있는 체계를 가져갔으면 함.
		1	– 5번 항목과 상동
		2	– 국방부, 국정원, 방송통신위원회
	6	0	– communication 및 사전대응 긴급 전파 및 대응 관리기관(민/관 관리기관, ISP 등) 사전 조치 이행 적용 =〉 현상 분석 및 해결안 도출

연구총서 10-07

사이버안전체계 구축에 관한 연구

발 행 / 2010년 12월
발행인 / 김일수
발행처 / 한국형사정책연구원
서울특별시 서초구 태봉로 114
(02)575-5285
등 록 / 1990. 3. 20. 제21-143호
인 쇄 / 디자인프리즘
(02)2264-1728
보고서 내용의 무단복제를 금함

정가 10,000원
ISBN 978-89-7366-846-5 93360