정 보 보 호 학 회 지
제25권 제2호, 2015. 4

한중일 침해사고 대응체계 비교에 관한 연구 – 사이버보안 법규, 대응기관, 대응절차를 중심으로

김 희 연*

요 약

국경을 넘나드는 사이버공격에 대한 효과적인 사이버보안 정책 수립을 위한 국가간 협력이 절실하다. 본 논문에서는 우리나라와 지리적으로 맞닿아 있는 중국 및 일본과 우리나라의 침해사고 대응 관련 법, 대응기관, 대응절차 등 국가별 침해사고 대응체계를 비교하고 효과적인 침해사고 대응체계 구축을 위한 초석을 마련하고자 한다. 우리나라 사이버보안 관련 법의 체계성에 중국 및 일본의 사이버보안 관련 정책의 유연성을 접합하고, 사이버보안 컨트롤타워를 성문화함으로써 인터넷 침해사고 대응의 효율성을 높일 수 있을 것이다.

Ⅰ. 서 론

컴퓨터 및 정보통신기술의 급속한 발전은, 사이버공간의 확대와 사이버공간에의 의존도 심화를 가져왔다. 이와 함께 컴퓨터를 이용한 사기 등의 범죄뿐만 아니라 사이버공간 자체에서의 범죄 및 인터넷 침해사고가 급격히 증가하고 있다. 인터넷 침해사고를 막기 위한 다양한 보안 기술이 발달하고 있지만, 사이버보안 정책도 기술의 발달에 발맞춰 수립되어야 한다.

사이버공간은 한 국가에 한정되는 것이 아니며 국경을 넘나드는 사이버공격이 이루어지고 있어, 효과적 사이버보안 정책 수립을 위한 국가 간의 협력이 절실한 시점이다. 이에 본 논문에서는 우리나라와 지리적으로 맞닿아 있는 중국 및 일본과 우리나라의 국가별 침해사고 대응체계를 비교하고, 보다 효과적인 침해사고 대응체계 구축을 위한 방안을 고찰하고자 한다.

Ⅱ. 국가별 침해사고 대응 관련 사이버보안 법규

2.1. 한국 침해사고 대응 관련 사이버보안 법규

우리나라의 사이버보안 기본법이라고 할 수 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법)에서는 사이버보안 정책과 관련된 세부적인 내용과 처벌에 관하여 규정하고 있으며, 그 정책의 실행과 관련된 절차나 조치들에 대해서는 동법 시행령에서 자세하게 정하고 있다. 중국 및 일본의 사이버보안 법률은 선언적·개괄적인 내용만 정하고 있다는 점에서 우리나라보다 상대적으로 유연하다고 할 수 있다.

또한 법상에서 ISP에의 차단요청에 대해 규정하고 있는 것은 우리나라뿐이다. 정보통신망법에서는 침해사고 발생시 접속경로 차단 요청 등에 대해 규정하고 있다. 그리고 정보통신망법에서는 침해사고 대응기관에 대해서도 명확히 규정한다.

2.1.1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률은 한국의 사이버보안 관련 기본법이다. 본 법에서는 해킹 및 악성프로그램 유포 등에 대한 처벌과, 침해사고 대응에 관하여 규정한다.

제47조의4에서는 정보통신망 이용자의 정보보호에 관하여 규정한다. 침해사고 발생으로 시스템, 망 등에 심각한 장애가 발생할 가능성이 있으면 주요정보통신서비스제공자(ISP)는 이용자의 정보통신망 접속을 일시적으로 제한할 수 있다.

제48조에서는 정보통신망 침해행위 등의 금지에 대해 규정한다. 정당한 접근권한 또는 허용된 접근권한을

* 한국인터넷진흥원(KISA) 인터넷침해대응본부 침해사고대응단 침해대응기획팀 김희연 (khy@kisa.or.kr)

넘는 정보통신망 침입행위와 컴퓨터 바이러스 등을 전달·유포하는 행위, DDoS공격 등을 금지한다.

제48조의2는 침해사고 대응 조치에 대해 규정한다. 침해사고 대응을 위하여 미래창조과학부와 한국인터넷진흥원은, 침해사고에 관한 정보의 수집·전파, 침해사고의 예보·경보, 침해사고에 대한 긴급조치 업무를 수행한다. 또한 동법 시행령 제56조에 따라 ISP에 대한 침해사고 확산 접속경로 차단 요청, 소프트웨어사업자에 대한 취약점 보완 프로그램 게재 요청, 언론사 및 ISP에 대한 침해사고 예보·경보의 전파, 국가 정보통신망 안전을 위한 침해사고 관련 정보 제공 등의 업무를 수행하고 있다.

2.1.2. 국가사이버안전관리규정

국가사이버안전관리규정은 2013년 9월 2일부터 시행(일부개정)되고 있는 국가정보원 소관의 대통령 훈령이다. 훈령은 하급 관청의 권한행사를 지휘하기 위해 발하는 명령으로서 법규의 성질을 갖지 않는다. 효과적인 사이버보안 정책을 위하여 본 규정을 입법화하려는 노력이 계속되고 있다.

본 규정은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다,

제8조는 국가정보원장이 국가사이버안전센터에 민·관·군 합동대응반을 설치 및 운영할 수 있음을 규정하고 있으며, 제11조는 국가정보원장이 공공분야에 대해 수준별 경보(관심, 주의. 경계, 심각 등)를 발령할 수 있음을 규정한다. 제13조는 '주의' 수준 이상의 경보 발령시 '범정부적 사이버위기 대책본부'를 구성·운영할 수 있음을 규정한다.

2.2. 중국 침해사고 대응 관련 사이버보안 법규

중국의 법규는 정보보호에 대해 개괄적으로 규정하고 있으며, 직접적으로 정보보호에 대해 규정하고 있는 관련법규는 주로 행정법규의 형식을 갖는다.

중국의 정보보호 관련 법률은 주로 컴퓨터 인터넷 운영질서·네트워크·정보시스템 안전측면에 집중되어 있고, 컴퓨터 자산 보호 및 컴퓨터 남용 범죄행위 관련 규정은 비교적 적은 편이다. 그리고 사이버범죄의 처벌에 대해서는 형법을 따른다. 중국은 우리나라처럼 침해사고 대응기관에 대해 법에서 명시하고 있다. 또한 중국은 침해사고 발생시 컴퓨터 작동 중단 명령으로 침해사고에 대해 강한 조치를 내릴 수 있음을 정하고 있다.

중국은 2015년 사이버보안 관련 기본법을 제정할 예정이다.

2.2.1. 법률

2.2.1.1. 형법(中華人民共和國刑法,)

중국은 사이버범죄를 사회에 존재하는 기존의 범죄형태의 하나로 파악하고 사이버범죄를 형법 해석으로 대처할 수 있다고 여겼다. 이에 1997년 중국 형법 전면개정시 제285조 '컴퓨터 정보시스템 불법침입죄'와, 제286조 '컴퓨터 정보시스템 파괴죄'의 두 조항만을 신설하였다.

제285조에서는 국가규정을 위반하고 국가사무·국방건설·첨단과학기술 영역의 컴퓨터 정보시스템을 침입하는 행위를 컴퓨터 정보시스템 불법침입죄로 규정한다. 제286조에서는 컴퓨터 정보시스템 기능 제거·개조·증가·간여 등으로 정상운행에 지장을 주는 행위, 데이터 및 응용절차의 제거·개조·조작 행위, 파괴성 프로그램 제작·전파행위 등 컴퓨터 시스템 정상운행에 영향을 주는 행위를 컴퓨터 정보시스템 파괴죄로 규정한다. 하지만 사이버범죄는 두 조항이 규정하는 범위에 포함되지 않는 경우가 많다.

제287조는 컴퓨터를 이용한 범죄에 관한 조항이다. 컴퓨터를 이용한 금융사기, 절도, 횡령, 공금횡령, 국가기밀 절취 혹은 기타 범죄를 형법 관련 규정에 따라 처벌한다고 규정한다. 본 조항의 형법에 따른 처벌 규정을 보아도, 중국이 사이버범죄를 형법으로 모두 규정할 수 있다고 여겼음을 알 수 있다.

중국에서는 모든 사이버범죄의 처벌에 형법을 적용한다. 전국인민대표회의 상무위원회 인터넷안전 보호에 관한 결정에서 사이버범죄의 유형들을 정하고 있지만, 그 처벌은 형법에 의한다.

2.2.1.2. 전국인민대표회의 상무위원회 인터넷안전 보호에 관한 결정(全國人大常委會關于維護互聯网安全的決定)

중국 전국인민대표회의 및 그 상무위원회에서 공포하는 결의(決議), 결정(決定), 규정(規定), 판법(判法) 등은 '법'이라는 명칭을 사용하지는 않지만 법률과 동일한 효력을 가지며 법적 구속력을 갖는다. 본 결정은 형법상 규제되는 범위(형법 제285조, 제286조) 외에도 인터넷에서 실행되는 각종 범죄들을 사이버범죄의 범주에 두었다는 점에 의의가 있다.

본 결정에서는 사이버범죄를 다섯 가지로 분류한다. 네트워크 운행안전 방해범죄, 국가안보·사회안정을 해치는 범죄, 사회주의 시장경제 및 공공질서 관리를 해치는 범죄, 개인 신상·명예·재산 등 합법적 권리를 침해하는 범죄, 기타 사이버범죄가 그것이다.

본 결정의 제15조에서는 컴퓨터 바이러스나 사회 공공안전을 위협하는 데이터 확산을 방지·연구하는 업무는 공안부가 총괄한다고 명시한다. 그리고 제20조에서는 공안기관의 안전상황 개선 통지에 응하지 않은 경우, 컴퓨터 정보시스템 안전을 해치는 기타행위를 하는 경우 등에 공안기관이 경고조치나 컴퓨터 작동중단 명령을 내릴 수 있음을 규정하고 있다.

본 결정을 통해, 중국이 사이버범죄에 대해 '민사책임, 행정처분, 기율처분, 행정처벌, 치안관리처분, 형사책임 등이 일체가 되는 예방 타격시스템'을 구축하는 과정에 있다는 점을 알 수 있다.

2.2.1.3. 치안관리처벌법(中華人民共和國治安管理處罰法)

치안관리처벌법 제29조는, 국가규정을 위반하여 컴퓨터 정보 시스템에 침범하는 행위, 컴퓨터 정보 시스템 기능의 삭제·수정·증가·방해 등 시스템의 정상 작동을 막는 행위, 컴퓨터 시스템에 보전·처리되어 있는 프로그램 및 데이터의 삭제·수정, 고의적으로 컴퓨터 바이러스를 제작·전파하는 행위에 대한 행정 처벌에 대해 규정하고 있다.

2.2.2. 행정법규

2.2.2.1. 컴퓨터 정보시스템 안전보호조례(中華人民共和國計算机信息系統安全保護條例編輯)

컴퓨터 정보시스템 안전보호조례는 컴퓨터 정보시스템을 이용하여 국가 및 집단의 이익과 국민의 합법적 권리를 해치거나 컴퓨터 정보시스템의 안전을 해치는 행위를 금지하고 있다.

제15조는 컴퓨터 바이러스 등 사회 공공안전을 위협하는 데이터 확산을 방지·연구하는 업무를 공안부가 총괄적으로 관리한다고 규정한다.

제20조에서는 컴퓨터 정보시스템의 안전을 해치는 행위에 대해 공안기관이 경고조치를 하거나 컴퓨터 작동중단을 명할 수 있다고 규정한다.

제23조에서는 바이러스 등 컴퓨터 정보시스템 안전을 위협하는 데이터 반입행위를 금지한다.

2.2.2.2. 컴퓨터 네트워크의 인터넷 접속관리 잠정규정(中華人民共和國計算机信息网絡國際聯网管理暫行規定)

본 규정은 중화인민공화국 경내의 컴퓨터가 국제 교류를 위하여 외국의 컴퓨터 네트워크와 상호 연결되는 경우에 관련 단체나 기관이 따라야 하는 사항을 다룬다. 특히 중국내 컴퓨터 네트워크 운영활동에 대한 '접속제한정책'의 시행에 관하여 정하고 있다.

2.3. 일본 침해사고 대응 관련 사이버보안 법규

일본의 사이버보안 관련 법률은 사이버보안 정책의 기본적인 방향과 필요성에 대하여 선언적·개괄적으로 규정하고 있다. 그리고 구체적 내용은 ISPC 등 사이버보안 관련 부처에서 제시하는 정책에 의해 실현되고 있다.

침해사고 대응기관에 대해서 법에서 명시하고 있는 우리나라 및 중국과는 달리, 일본에서는 법에서 침해사고 대응기관을 명시하고 있지 않다. 하지만 새롭게 도입된 사이버보안 기본법에서는 '사이버보안 전략 본부'에 대해 법적으로 규정한다.

또한 침해사고에 대하여 접속경로 차단 요청, 컴퓨터 작동 중단 명령 등 강력한 조치를 내릴 수 있음을 법에

서 명시하고 있는 한국 및 중국과 달리, 일본에는 관련 규정이 없다. 일본에서는 접속관리자의 필요한 조치의무와 이에 대한 공안위원회의 지원에 대해서만 규정하고 있을 뿐, 명확한 침해사고 대응과 관련된 규정이 없다.

일본은 2015년 시행예정인 사이버보안 기본법을 제정하여, 사이버보안 관련 문제를 해결하기 위해 노력하고 있다.

2.3.1. 법률

2.3.1.1. 고도 정보통신 네트워크 사회형성 기본법(高度情報通信ネットワーク社會形成基本法)

고도 정보통신 네트워크 사회형성 기본법은 2000년 'e-Japan 구상'에 기초하여 제정된 일본 IT기본법으로, IT관련 기본원칙을 정하고 있다. 특히 제22조는 '고도 정보통신 네트워크 사회 형성에 관한 시책의 책정에 있어서는, 고도 정보통신 네트워크의 안정성 및 신뢰성 확보, 개인정보보호 및 기타 국민이 고도 정보통신 네트워크를 안심하고 이용할 수 있도록 하기 위해 필요한 조치가 취해져야 한다'고 정하면서, 정보보호정책을 마련할 것을 요구하고 있다.

2.3.1.2. 부정접속행위의 금지에 관한 법률(不正アクセス行爲の禁止等に關する法律)

부정접속행위의 금지에 관한 법률은, 해킹 등 침해행위를 방지하기 위해 1999년에 제정된 법률이다. 이 법은 부정접속행위를 금지하고, 이에 대한 벌칙과, 재발방지를 위한 공안위원회의 지원 조치 등을 정한다. 전기통신 회선을 통하여 이루어지는 컴퓨터에 의한 범죄 예방과, 접근 통제 기능에 의해 실현되는 통신에 대한 질서유지를 도모하여, 고도 정보 통신 사회의 건전한 발전에 기여하는 것을 목적으로 한다.

제3조부터 제8조에서는 부정접속행위 및 부정접속행위 조장 금지, 타인 식별 부호 부정취득행위 금지, 식별부호를 잘못 요청하는 행위 금지 등에 대하여 규정하고 있다.

제9조와 제10조에서는 공안위원회의 재발 방지를 위한 지원 조치에 대해 규정하고 있다. 공안위원회는 부정접속행위 방어를 위해 자료제공, 조언, 교육 등의 원조를 실시한다.

제11조, 제12조, 제13조는 벌칙 조항으로, 사이버범죄의 처벌에 대해 규정하고 있다. 정책에서 형벌까지 다루는 것은 법적 안정성을 침해하기 때문인 것으로 보인다.

본 법의 제3조에서는 '어느 누구도 부정 액세스 행위를 해서는 안된다'고만 규정하고 있으며, 세부적인 사항들은 ISPC에서 사이버보안에 초점을 맞추어 보안정책 강화 목적으로 제시한 전략인 사이버보안 전략에서 규정하고 있었다. 이에 최근 더더욱 급증하는 사이버 위협에 효과적으로 대응하기 위한 법안의 도입 필요성이 제기되었다.

2.3.1.3. 사이버보안 기본법(Cybersecurity Basic Act)

일본은 사이버보안의 중요성을 인식하고, 정부 주도의 사이버보안 체제를 강화하고자 사이버보안 기본법 제정을 추진하였다. 본 법안은 2014년 6월 11일 발의되어, 2014년 11월 6일 중의원 본회의에서 가결되었다.

사이버보안 기본법 제1조는 국가 차원의 지방 공공부처의 책임 등을 명확히 하고, 사이버보안 관련 정책의 기본사항을 정하기 위하여 '사이버보안 전략 본부'를 설치하여 고도 정보통신 네트워크 사회형성 기본법과 함께 사이버보안 관련 정책을 종합적·효과적으로 추진하는 것이 본 법의 목표임을 명시한다.

제2조에서는 그동안 명확하게 법적 정의가 존재하지 않았던 '사이버보안'의 개념에 대해 최초로 법률적 정의를 내린다. 본 법률에 의하면 사이버보안이란, 전자적 방식·자기적 방식 등 타인이 인식할 수 없는 방식에 의해 기록·발송·전송 또는 수신된 정보의 누출·멸실·훼손의 방지 및 기타 당해 정보의 안전관리를 위해 필요한 조치와 정보 시스템 및 정보통신네트워크의 안전성 및 신뢰성의 확보를 위해 필요한 조치를 구비하여 그 상황이 적절히 유지·관리되도록 하는 것을 의미한다.

그리고 제3조에서는 사이버보안 정책의 기본이념에 대해 정하며, 제12조에서는 사이버보안 전략에서 정해야 할 사항에 대해 규정하고 있다. 또한 본 법안에서는 국가와 지방자치단체 등 관계자 책임, 국가에 의한 기본적 시책, 종합적·효과적 추진체계 등에 대해 정하고 있다.

2.3.2. 정부 사이버보안 정책(ISPC 발표)

2.3.2.1. 첫 번째 및 두 번째 정보보호 국가전략

2006년 2월, IT전략본부 정보보호정책회의(ISPC)는 ISPC를 중심으로 국가전반적 정보보호문제를 다룬 제1차 정보보호 기본계획을 책정하였다. 이는 국가차원의 정보보호 기본이념과 중점정책방향성을 제시하는 정보보호 중장기 계획으로 발표된 것이었다.

2006년 12월에는 'Secure Japan의 실현을 향한 대응평가 및 평가등급의 합리성을 가진 지속적 개선의 추진에 관한 안'이 제안되어 2007년에 확정 발표되었다. 그리고 제1차 정보보호 국가전략(2006~2008)의 실현성 제고를 위한 단기계획으로 'Secure Japan 07/08''이 발표 및 추진되었다.

2009년 2월에는 제2차 정보보호 국가전략을 마련하여 추진되었다. 이는 'IT시대의 강력한 '개인'과 '사회'의 확립을 위하여' 마련된 정책이었다.

2.3.2.2. 국가보호를 위한 정보보호전략

일본은 미국·한국 등에 나타난 대규모 사이버 공격 사례를 통해 기존의 정보보호 국가전략의 수정 필요성을 느꼈다. 그리고 2010년 7월 22일, 국가보호를 위한 정보보호전략(Information Security Strategy for Protecting the Nation)을 책정하여 추진하였다.

2.3.2.3. 사이버 보안 전략 2014 (サイバーセキュリティ戦略)

ICT 기술에 대한 의존성이 높은 일본은, 사이버보안 위협에 큰 위기감을 느끼고 보다 적극적인 대처의 필요성을 느끼게 되었다. 그리고 2013년 6월 10일, 사이버보안에 초점을 맞춰 보안 정책을 강화하기 위하여 '정보보호 국가전략'을 '사이버 보안전략'으로 수정하여 발표하였다.

2013년부터 2015년까지 3년간 추진되는 본 전략은 정부기관 및 주요 기반시설 사업자 등 사이버보안 주체들이 상호 연계를 통해 보안 수준을 향상시킴으로써 사이버공격 대응력을 강화하기 위해 필요한 각종 정책들을 마련하기 위한 것이다. 또한 2015년까지 강건하고 활력있는 사이버 공간 구축을 실현하고 글로벌 사이버보안 사업에서 일본이 선도적 위치에 오르기 위한 '사이버보안 입국(入國)을 실현하는 것을 목표로 한다.

사이버 보안전략 2014에서는 APT 공격 증가 등 사이버 환경의 변화를 인식하고 리스크 대응 및 기반을 분석하였다. 그리고 사이버 보안의 주요주체의 역할을 강화하고, 정보보호 연구개발 전략 향상을 위해 노력하였다. 또한 사이버보안 위협에 대한 대응전략을 체계화하였고 교육훈련 및 국제 공조를 강화하였다.

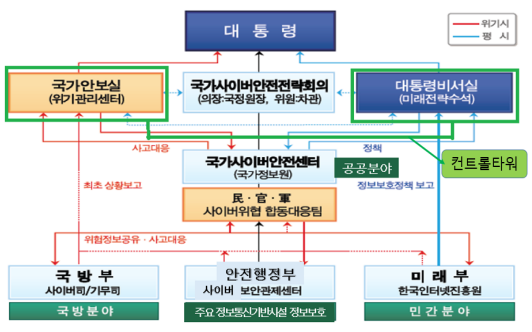
특히 사이버 보안전략 2014에서 화제가 되고 있는 정책은, 정보통신사업자에게 바이러스를 포함하고 있는 이메일 검출 등 통신내용을 분석할 수 있는 권한을 부여하고 있다는 점이다. APT공격이 주로 악성코드를 담은 이메일로 이루어진다는 점에 착안한 것이다. 그러나 이는 통신의 비밀을 침해한다는 논란을 가져오고 있다.

Ⅲ.국가별 침해사고 대응기관

3.1. 한국 침해사고 대응기관

우리나라의 사이버보안 대응기관들은 기반시설 보호, 국방분야, 공공분야, 민간분야 등 각 분야별로 정보보호 업무를 담당하고 있다. 주요 정보통신기반시설에 대한 정보보호는 안전행정부, 국방분야는 국방부 사이버사령부, 공공분야는 국가정보원, 민간분야는 미래창조과학부와 한국인터넷진흥원이 주관하고 있다.

사이버공격 등 위기상황 발생시 각급기관은 국가안보실(위기관리센터)과 국가정보원(국가사이버안전센터)에 동시 최초 상황보고를 하고 국가정보원은 사이버공격 피해 및 대응상황을 국가안보실을 통해 대통령에게 보고하게 된다.



〔그림 1〕 국가정보보호체계(국가정보보호백서(2014))

3.1.1. 국가안보실(위기관리센터)

국가안보실(위기관리센터)은 사이버공격 등 위기상황 발생시의 컨트롤타워로서 사이버위기 상황 보고·전파 및 대응활동을 총괄하는 역할을 수행하고 있다.

3.1.2. 대통령비서실(미래전략수석실)

대통령비서실(미래전략수석실)은 평시의 컨트롤타워로서 정보보호 관련 법·제도 정비, 정책 수립 등의 역할을 수행하고 있다.

3.1.3. 국가정보원

국가정보원은 국가정보원법, 정보통신기반보호법, 전자정부법, 국가정보화기본법 등에 의해 국가 정보보안 업무 기획·조정 및 보안정책 수립·시행 등 국가·공공분야에 대한 사이버보안 실무총괄 역할을 수행하고 있다.

국가정보원 국가사이버안전센터(NCSC, National Cyber Security Center)는 공공분야 사이버공격 예방 및 침해사고 조사를 하고 있으며, 사이버위협 정보를 수집·분석·배포하고 있다. 그리고 국가사이버전략회의를 운영하고 사이버안전기본계획을 수립한다.

NCSC에 설치된 국가사이버안전전략회의는 국가사이버안전체계 수립 및 개선, 국가사이버안전 관련 정책기관 간 역할조정, 대통령 지시사항 조치방안 심의 등의 업무를 맡는다. 전략회의의 의결사항은 국가안보실·미래전략수석실과 협의를 거쳐 최종적으로 대통령에게 보고된다.

NCSC에 설치되어 있는 민·관·군 사이버위협합동대응팀은 사이버위협에 대한 범국가차원의 체계적 대응체계를 유지하고 있다.

3.1.4. 국방부 사이버사령부

국방부 사이버사령부는 북한 7.7 DDoS공격을 계기로 2010년 1월 국방정보본부 산하에 창설되었고, 2011년 국방부 직속 사령부로 독립하였다.

국방부 사이버사령부는 국방 사이버전의 기획·계획을 수립하고, 국방 사이버전을 시행한다. 그리고 사이버전문인력 육성 및 기술개발, 부대훈련을 하고 있다. 또한 유관기관과의 정보공유 및 협조체계 구축, 국방분야

〔그림 2〕 국방부 사이버사령부 체계

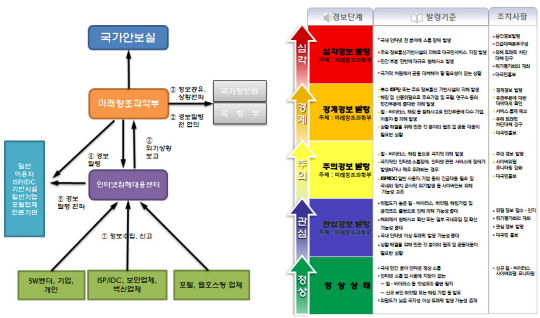
침해사고 예방 및 대응 등의 업무를 수행하고 있다.

3.1.5. 미래창조과학부

미래창조과학부는 민간 정보보호 및 정보보호 산업 업무를 총괄한다. 정보통신망법, 국가정보화기본법, 전자서명법, 정보통신기반보호법, 정보통신산업진흥법에 근거하여 정보보호업무를 수행한다.

미래창조과학부는 민간 정보보호 정책 수립·총괄·조정, 민간분야 주요정보통신기반시설 지정·권고·보호대책·보호지원·보호계획 등의 업무를 하고 있으며, 민간분야 침해사고 예방·대응체계 구축 및 운영, 사이버안보 대국민 홍보 업무도 맡고 있다. 또한 정보보호 산업·인력 육성과 정보보호 기술개발 등에도 힘쓰고 있다.

미래창조과학부 산하 한국인터넷진흥원(KISA) 인터넷침해대응센터(KISC(Korea Internet Security Center), KrCERT.CC)에서는 국내 인터넷 침해사고 사전예방 및 대응 업무를 맡고 있다. 종합상황실 운영을 통해 국내 주요통신사업자 및 보안관제업체와 연계하여 24시간 365일 인터넷 트래픽상의 이상징후를 모니터링한다. 또한 보안취약점 및 악성코드 등 보안위협에 대한 정보를 수집 및 분석하고 있다. 나아가 국내외 유관기관과의 상시적 정보공유를 통하여 신속하고 효과적인 공



〔그림 3〕 미래창조과학부 정보보호 업무 체계도

동대응을 하고 있다.

3.1.6. 안전행정부

안전행정부는 국가정보화기본법, 전자정부법, 개인정보보호법에 의해 소관 정보보호 및 개인정보보호정책 업무를 수행하며, 주요 정보통신기반시설에 대한 정보보호 업무를 하고 있다.

정보통합전산센터 및 17개 시·도 종합사이버보안관제센터를 통한 공동대응 및 유관기관과의 범정부적 공조체계 구축으로 국가기관의 사이버침해 대응 역량강화를 도모하고 있다.

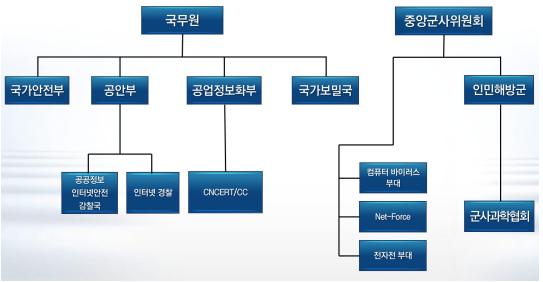
2007년 지식경제부(현 산업통상자원부)·국토해양부(현 국토교통부)·교육과학기술부(현 교육부)·보건복지가족부 등 4개 부처는 에너지·교통·교육·보건 등 국가 핵심전산망의 부문별 종합사이버보안관제센터를 구축하였다. 부문별 사이버보안관제센터는 국정원의 국가사이버안전센터(NCSC)와 연계하여 범정부차원의 종합사이버보안센터 체계를 갖추어 공동대응하고 있다.

〔표 1〕 종합사이버보안관제센터 운영 현황

기획재정부	기획재정 사이버안전센터	농림축산식품부	농림 사이버안전센터
미래창조과학부	미래창조과학 사이버안전센터	산업통상자원부	산업통상자원 사이버안전센터
	KISA		
교육부	교육 사이버안전센터	보건복지부	보건복지 사이버안전센터
	과학기술 정보보호센터		
외교부	외교 사이버안전센터	환경부	환경 사이버안전센터
통일부	통일 사이버안전센터	고용노동부	고용노동 사이버안전센터
법무부	대검찰청	여성가족부	
	법무 사이버안전센터		
국방부	사이버사령부	국토교통부	국토교통 사이버안전센터
안전행정부	**정부통합전산센터(대전/광주)**	해양수산부	해양수산 사이버안전센터
	지역정보개발원		
문화체육관광부	문화체육 사이버안전센터	금융위원회	증권 ISAC
			금융 ISAC
방송통신위원회	방송통신 사이버안전센터	관세청	관세청 관제센터
국가보안기술연구소	보안관제기술지원센터	기상청	기상 사이버안전센터
방위사업청	방위사업청 보안관제센터	특허청	특허청 관제센터
경찰청	경찰청 보안관제센터	국세청	국세청 사이버안전센터

3.2. 중국 침해사고 대응기관

중국은 정보기관과 공안을 중심으로 사이버테러 대응이 이루어지고 있다.



〔그림 4〕 중국 침해사고 대응기관 체계도

3.2.1. 국무원 국가안전부 (國務院 國家安全部)

국무원 국가안전부는 국가 암호 및 컴퓨터 보안정책 수립 등 사이버보안 업무를 총괄한다. 특히 전산망 관리 및 사이버 정보분석 업무를 담당한다.

국무원 국가안전부 내에서 사이버보안 담당 부처가 9국 기술정찰국이라는 주장과 16국 계산기관리국이라는 주장이 존재하는데, 외부에 명확히 밝혀진 바는 없다.

3.2.2. 국무원 공안부(公安部) 공공정보 인터넷안전 감찰국 (公共信息网絡安全監察)

공공정보 인터넷안전감찰국은 옛 사이버안전보위국(网絡違法犯罪擧報网站)이다. 이곳에서는 컴퓨터 바이러스 등 사회 공공안전을 위협하는 데이터 확산 방지 및 연구를 총괄한다. 유해 데이터의 예방·관리, 컴퓨터 정보시스템 안전보호업무 감독·검사·인증 업무를 행하고 있다. 그리고 공공정보 인터넷안전감찰국은 컴퓨터 및 네트워크 보안정책과 보안제품 개발에 관여하고 있으며, 컴퓨터 위법 범죄사건 조사, 암호화 절차 결정 등 국가기밀 보호에 핵심적 역할을 하고 있다.

1998년에는 인터넷 검열 프로그램인 만리방화벽(防火長城, Great Firewall, The Golden Shield Project)을 구축하기도 하였다. 그리고 Internet Crime Reporting Center를 구축하여 사이버범죄의 신고를 접수받아 빠른 대응을 위해 노력하고 있다.

3.2.3. 공업정보화부 침해사고 대응센터 CNCERT/CC

CNCERT/CC는 2002년 9월, 국무원 공업정보화부(工業和信息化部)에 신설되어 민간분야의 사이버 침해사고 조사 및 대응활동을 한다. 그리고 2004년 FIRST

(국제침해사고대응협의회)에 가입하여 국제협력을 통한 사이버보안 문제 해결을 위해 노력한다. 공업정보화부는 정보제공 및 공유 업무를 총괄 지도·감독하고 있으며, 실무는 공업정보화부 통신보장국이 담당한다.

CNCERT/CC는 공업정보화부의 위임을 받아 인터넷 보안정보를 수집·통합·분석·발표하고, 정보제공 참여자에게 인터넷 보안정보를 공유한다.

CNCERT/CC는 국가 취약점 데이터베이스(CNVD, China National Vulnerability Database)와 反네트워크 바이러스 연합(Anti Network-Virus Alliance of China)을 설립하여 ISP, 도메인네임 등록기관, 사이버보안 전문가 등의 업무 체제 확립을 통한 취약점 정보 교환, 바이러스 방지 및 처치, 사이버 정보 공유·기술 협력을 한다.

또한 컴퓨터 네트워크 감독·검사·예방·응급처리 등 안전 모니터링·경보·기술지원, 컴퓨터 네트워크 보안 사건 발생시 공동대처, 국제합작 및 교류 도모 등의 업무도 행하고 있다.

3.2.4. 국무원 국가보밀국(中華人民共和國的國家保密局)

국무원 국가보밀국은 보안감사, 보안정책수립 시달 및 통제감독을 담당한다. 국가보밀국은 국가보안과학기술연구소(Institute of National Security Science and Technology)를 운영하여, 전국비밀보호기술정책을 제정하고 기술의거를 제공 및 기획하며, 비밀보호업무를 수행하고 있다.

또한 국가보밀국은 공공기관 납품 제품평가·인증, 국가보안표준과 기술규범 연구·제정, 사이버보안기술검사, 예방제품·통신보안 검사제품 연구·개발, 자문서비스 제공 등의 업무도 수행한다.

국가보밀국은 '정보보안을 제외한' 국가 공공기관의 국가보안업무를 책임지고 있다고 알려져 있다. <국가정보연구>에 실린 "주요국의 사이버안전관련 법, 조직체계 비교 및 발전방안 연구"에 의하면 국가보밀국은 국가 기밀을 지키고 보안제품에 대해 관리하는 역할을 주로 하는 것으로 보인다. 따라서 침해대응기관으로서의 역할은 비교적 작은 것으로 보인다.

3.2.5. 중앙군사위원회

1997년 4월 중앙군사위원회 직속으로 컴퓨터 바이러스 부대가 창설되었으며, 2000년 2월 Net-Force가 창설되었다. 그리고 2008년 북경 등 4대 군구(軍區)에 전자전 부대가 창설되었다. 이들은 해킹기술을 개발하고 외국 정부기관의 자료를 획득하는 업무를 하고 있다.

2014년 5월에는 미국이 중국 인민해방군 61398부대 소속의 해커들을 기소하기도 하였다. 이후 기존의 61398부대의 능력을 능가하는 61486부대의 존재가 밝혀지기도 하였다.

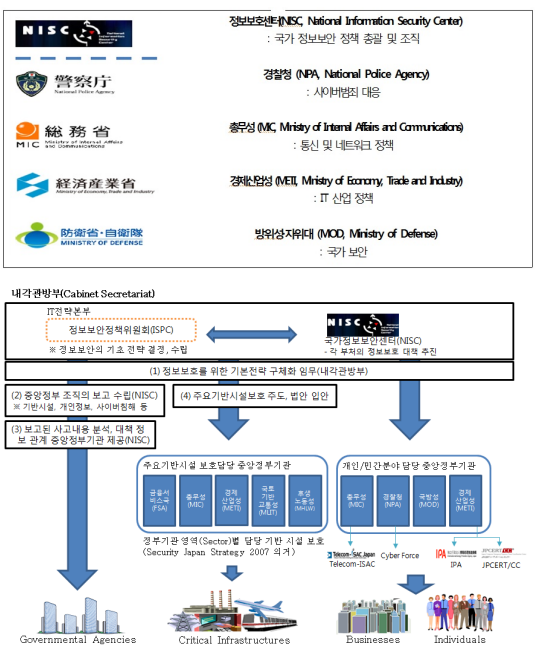
3.2.6. 인터넷 경찰 (网絡警察)

1998년 이후 중국 전역의 지방정부는 인터넷 범죄를 다루기 위해 자체적으로 인터넷 경찰을 수립하였다. 인터넷 경찰은 베이징시, 청두시, 항저우시, 광둥성 등 지방정부 공안국 산하에서 활동하고 있다.

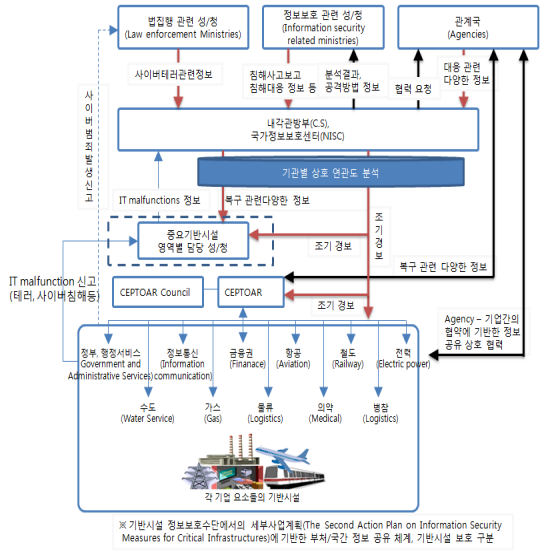
인터넷 경찰은 인터넷 사기·횡령 등 온라인 범죄를 다루고, 바이러스·네트워크 취약성 경고 등의 업무를 담당하고 있다.

3.3. 일본 침해사고 대응기관

일본은 '국가보호를 위한 정보보안전략' 등을 기반으로, 개인·공공·기반시설보호 등 모든 영역에서 내각관방



〔그림 5〕 일본 침해사고 대응기관 체계도



〔그림 6〕 일본 정보공유 및 중요기반시설 보고시스템

산하 국가정보보호센터(NISC)의 주도로 각 성·청(Ministries, Agencies)과 산하 정보기관이 정보보호 활동을 수행하고 있다.

대표적 일본 사이버보안 관련 부처인 정보보안정책회의(ISPC)와 정보보호센터(NISC)는 내각 관방 중심으로 관련 정부부처가 참여하는 범정부적 기구로서 국가단위의 통일적 대응을 도모하고 있다. 특히 NISC는 경찰청, 총무성, 경제산업성, 방위성·자위대의 네트워크 허브 역할을 한다.

각 성·청 간 정보공유, 중요기반시설 보고 시스템은 다음과 같이 이루어지고 있다. 민간기업의 기반시설이 테러(사이버테러 포함) 또는 IT malfunction(IT 기능저하)시 중요기반시설 영역별 담당 성·청에게 신고를 하도록 Action Plan으로 지정하고 있다. 신고를 접수한 담당 성·청은 NISC로 사고 관련 정보와 함께 복구정보(Recovery Information)를 제공한다. 그리고 산하기관과 협력하여 담당 영역에 대한 대응을 실시한다.

현재 일본은 민관 협력에도 힘을 쏟고 있는 것으로 보인다. 경찰청은 방위 및 첨단기술 관련 기업 간에 '사이버 인텔리전스 공유 네트워크'를 구축하였다. 총무성은 민관 정보공유분석센터(Telecom-ISAC)를 구축하였고, 경제산업성은 주요 인프라 관련 기업간에 사이버정보공유 이니셔티브(J-CSIP)를 구축하였다. 자위대·방위성은 방위관계 최고 책임자들에게 기업 정보보호와 민관협력을 요청하였다.

3.3.1. 정보보안정책위원회 (ISPC, Informs mation Security Policy Council)

정보보안정책위원회(ISPC)는 2005년 5월 내각 관방 IT전략본부(고도정보통신네트워크사회추진전략본부)에 설치되었으며 의장은 내각관방부 장관이, 사무국은 내각 관방 정보보호센터(NISC)가 맡고 있다. 내각 관방은 내각의 수장인 내각총리대신을 돕는 내각 소속 보조기관이다.

ISPC는 정부기관 사이버보안 업무를 총괄하며, 사이버테러 복구 및 대응지원 업무를 한다. 또한 ISPC는 전국가적 관점에서 정보보안관련 기본전략을 수립한다. 최근 ISPC는 기존의 '정보보호 국가전략'을 '사이버 보안전략'으로 수정하였는데, 이는 사이버보안에 초점을 맞춰 보안정책을 강화하기 위한 목적이다.

3.3.2. 정보보호센터 (NISC, National Information Security Center)

정보보호센터(NISC)는 2005년 4월 내각 관방 IT전략본부에 설치된 민·관 전문가로 구성된 기구이다. 총무성, 경제산업성, 경찰청, 방위성·자위대 등 각 부처에서 파견된 인사들을 중심으로 구성되어 있다. NISC는 ISPC에서 수립된 기본전략을 수행하는 기관이다.

NISC는 정보보안정책에 관한 중장기계획 및 연도계획의 입안, 정부기관 및 주요 인프라의 정보보안대책 수립, 정보보안정책에 관한 국제제휴 창구기능을 수행한다.

그리고 NISC는 각 영역별 모든 성·청 및 관계국의 정보를 취합·분석하여 관련 정보를 공유하고 상호의존도 분석을 통하여 침해사고와 연관된 성·청으로 조기경보를 발령한다.

NISC는 2015년 '사이버 보안센터(Cyber Security Center)'라는 이름으로 역할과 기능을 확대할 예정이다. 중간목표는 2015년까지 정부기관과 주요 기반시설 서비스제공자 간 사이버보안 정보 공유 확대, 악성 소프트웨어 감염비율 최소화, 국제적 사고 협력 활동 강화에 있다. 그리고 장기목표는 2020년까지 정보보호 시장을 2배 이상 확대하고 보안 전문가 비율을 확대하는 것에 있다.

3.3.3. 사이버보안 전략 본부 (Cybersecurity Strategic Headquarters)

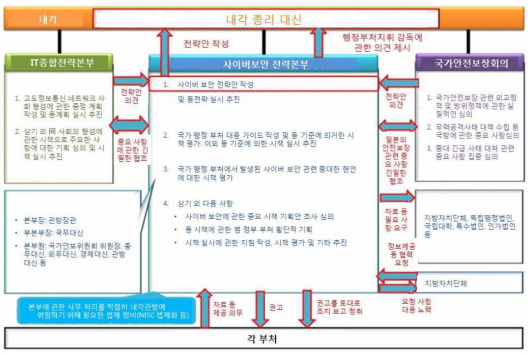
사이버보안 전략 본부는 사이버보안 관련 정책들을 효율적·종합적으로 집행하기 위하여, 2015년부터 시행될 사이버보안 기본법(Cybersecurity basic act)에 따라 설치될 예정이다.

사이버보안 전략 본부는 법적 근거를 바탕으로 민관 전체를 이끄는 사이버보안 관련 기관이라는 점에 가장 큰 의의가 있다. 사이버보안 전략 본부는 범 부처를 대상으로 한 사이버보안 정책의 사령탑 역할을 할 예정이며 민간 보안 전문가들을 기간제로 임용하여 전문성 향상을 꾀할 것이다.

사이버보안 전략 본부는 내각(Cabinet)에 설치되어 총리 직속으로 사이버보안을 다루게 된다, 기존의 내각관방 IT전략본부 산하의 ISPC가 사이버보안 전략 본부로 격상되는 것이다.

사이버보안 전략 본부는 사이버보안 전략안 작성 및 실시 추진, 국가 행정기관의 대책기준 작성 및 정책평가(감사 포함) 등의 정책을 추진한다. 그리고 국가 행정기관에 발생한 사이버보안 관련 중대 사고에 대한 정책평가(원인 규명을 위한 조사 등), 사이버보안 관련 중요 정책의 계획에 관한 조사심의, 부·성 횡단적 계획 및 관계행정기관의 경비·견적·방침·정책 실시 관련 지침 작성, 정책평가 등을 하며, 사이버보안 관련 정책들을 종합적으로 조정하게 된다.

사이버보안 전략 본부는 사이버보안 전략(CSS)등 주요사안에 대하여 내각관방 IT전략본부 및 국가안전보장회의(National Security Council)과 긴밀하게 협력할 예정이다.



〔그림 7〕 사이버보안 전략 본부 기능 및 권한 체계도

3.3.4. Cyber Force 및 사이버공격 특별 수사대

Cyber Force는 2001년 4월, 경찰청(NPA) 정보통신국에 창설되었다. Cyber Force는 R&D 연구를 위한 다양한 시설을 구비하고 교육 훈련을 하고 있다. 그리고 잠재적 미래 사이버 테러 및 유사 범죄에 대한 수사 지원을 하고 있다.

일본 전역 사이버포스의 지휘본부는 사이버포스 센터가 맡고 있다. 사이버포스 센터는 24시간 내내 인터넷 보안 모니터링, 관련 정보의 수집·부석, 각 지역 경찰이나 해외 치안정보기관과의 정보교환 업무를 수행한다.

2011년 8월 방위 및 첨단 기술 관련 기업 약 4천개 회사와 협력하여 '사이버 인텔리전스 정보 공유 네트워크'를 발족하였다.

'사이버공격 특별 수사대'는 사이버공격 대책 강화를 위해 2013년 4월 경찰청에 신설되었다. 전국 약 140명의 전담 수사관이 대책을 추진하는 체제가 구축되어 있다. 사이버공격 특별 수사대는 사이버공격에 대한 보안정보 수집·정리, 기타 사이버공격 경비·예방·수사 등의 업무를 통하여, 사이버공격으로부터 개인의 생명, 신체, 재산을 보호하고 공공 안전 및 질서를 유지한다.

3.3.5. 민·관 정보공유분석센터 (Telecom-ISAC)

Telecom-ISAC은 2011년 11일에 설치된 총무성 산하의 민관협력기관이다. Telecom-ISAC은 본래 2006년 총무성과 경제산업성의 공동산업으로 설치되었던 사이버 클린센터(CCC, Cyber Clean Center)를 통해 일반국민을 대상으로 악성봇에 관한 정보를 제공하고 ISP와 협력하여 봇 제거 툴 무료다운로드를 실시하고 있다.

또한 재해에 강한 전자자치체 연구 및 관측망 'nicter'를 통해 사이버공격 관측정보를 수집한다.

3.3.6. 정보처리추진기구 (IPA, Information-technology Promotion Agency)

정보처리추진기구(IPA)는 경제산업성 산하 기구로, 소프트웨어 웹 보안취약점 점검 및 관련사업을 시행하고 있다.

IPA는 1997년 1월, 'IT Security Center'를 설치하여 바이러스·부정접속대책 등 정보보안대책 강화·정비, 해

킹·웜바이러스 신고접수 및 취약점 정보 등을 게시해오고 있다.

2011년 10월 경제산업성은 '사이버정보공유이니시티브(J-CSIP)'를 구축하여 미쓰비시중공업, 히다찌제작소, 도시바 등 주요 인프라 관련 기업 중심으로 정보를 공유하고 있다.

2014년 5월 20일에는 '사이버 구조대(サイバーレスキュー隊, J-CRAT(Cyber Rescue and Advice Team against targeted attack of Japan))'를 신설하여 APT공격의 피해확대와 재발 방지, 조속한 대책방안 마련을 위해 노력하고 있다. 사이버 구조대는 공격을 탐지하지 못하고 피해에 노출된 조직과, 보안사고 상황 및 심각성을 인식하지 못하고 있는 조직을 적극 지원하고 있다. 사이버 공격에 대한 탐지와 조치지원, 조직의 피해발생 정도에 대한 조기파악 및 지원, 대책마련 조기착수를 지원하고 있다.

3.3.7. 일본 침해사고 대응센터 JPCERT/CC

1992년 자발적 조직으로 창설된 JPCERT/CC는 특정 정부기관이나 기업으로부터 독립된 중립적 조직으로서 경제산업성으로부터 재정적 지원을 받고 있다. JPCERT/CC는 인터넷 침해사고에 대해 사이트 보고·접수, 대응지원, 상황 파악, 범죄 수법 분석, 재발방지를 위한 대책검토 등의 업무를 수행한다.

2004년 7월부터 IPA와 JPCERT/CC는 경제산업성 고시에 기반하여 소프트웨어와 웹사이트 취약점 신고를 접수받아, 소프트웨어 개발자 및 웹사이트 운영자 등에게 통지하고 수정을 위해 필요한 조정을 행하고 있다.

그리고 1998년 FIRST(국제침해사고대응협의회)에 가입하여 국제협력을 통한 사이버보안 문제 해결을 위해 노력하고 있다.

3.3.8. 사이버 방위대

사이버 방위대는 2014년 3월 26일 신설된 방위성 직할 부대로, 육·해·공 자위대원 90여명으로 이루어져 있다.

사이버 방위대는 24시간 방위성과 자위대의 네트워크를 감시하고, 사이버 공격 발생시에 대응한다. 그리고 사이버 공격을 감행한 곳에 바이러스를 전송하는 등 반격 능력 보유 여부에 대한 검토가 이루어지는 중이다.

방위성 역시 방위관계기업 약 140개 회사의 최고책임자에게 기업 정보보호 및 민관협력에 관해 요청함으로써, 정보공유에 힘쓰고 있다.

Ⅳ. 국가별 침해사고 대응절차

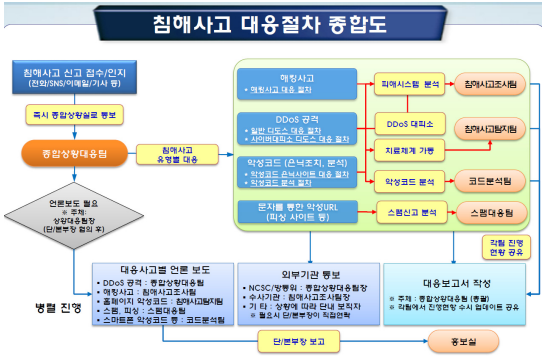
4.1. 한국 : 한국인터넷진흥원(KISA), KrCERT/CC(KISC)

한국의 민간분야 침해사고 대응은 정보통신망법 제52조 및 제48조의2 제1항에 의해 미래창조과학부 및 한국인터넷진흥원 관할이다. 그리고 KrCERT/CC는 한국인터넷진흥원 산하 침해사고대응부서에서 전담하고 있다. 한국인터넷진흥원의 침해사고 대응범위는 해킹, DDoS공격, 소프트웨어 취약점, 악성코드 은닉, 피싱 등이다.

한국의 침해사고 대응절차는 수집·탐지, 분석·협의, 전파·발령, 대응·복구의 네 단계로 이루어진다.

4.1.1. 수집·탐지

한국인터넷진흥원에서는 자체 운영 중인 탐지 시스템, 118콜센터, 사업자와의 정보공유 등을 통하여 침해



〔그림8〕 침해사고 대응절차 종합도 1

〔그림 9〕 침해사고 대응절차 종합도 2

사고 관련 정보를 수집한다. ISP의 경우 필요하다고 판단되는 경우 침해사고조사팀에서 증거를 수집한다.

홈페이지 내 악성코드 은닉 탐지시스템인 MC-Finder를 통하여 홈페이지를 통한 악성코드 유포 여부를 점검하고, 탐지된 사이트에 대해 악성코드를 차단 및 삭제하여 이용자 PC의 감염을 예방한다. 그리고 허니팟·허니넷으로 네트워크 전파형 악성코드를 수집·분석하고, 트래픽 모니터링을 통하여 동향을 파악한다.

4.1.2. 분석·협의

한국인터넷진흥원 취약점분석팀, 침해사고조사팀, 코드분석팀에서는 초동분석 후 필요시선차단 요청하고 상세분석을 실시한다.

사이버위협 및 침해사고정보 종합분석·공유시스템(CTAS, Cyber Threat Analysis & Share System), CTEX(Cyber Threat Expression), Hadoop Eco System, Elastic Search, MongoDB, R, Mahout 등으로 침해사고 분석이 이루어지고 있다.

침해사고 분석은 위협관리, 백신진단 및 행위분석, 종합 검색, 연관관계 및 유사도 분석, 위협알림의 차례로 이루어진다.

4.1.3. 전파·발령

ISP 등 정보제공 기관, 민간기업, 백신업체, 일반 인터넷 사용자, 방송·언론·주요 포털에 침해사고와 관련된 정보를 전파·발령한다.

4.1.4. 대응·복구

이 단계에서는 정보통신망법 제48조의2와 제49조의2 및 동법 시행령 제56조에 의하여 ISP, 도메인 등록대행자 등에 접속 차단 요청을 한다. 국내 사업자의 경우 직접 연락 후 조치 요청을 하며, 국외 사업자의 경우에는 내국인의 접속을 차단하도록 ISP에 요청한다.

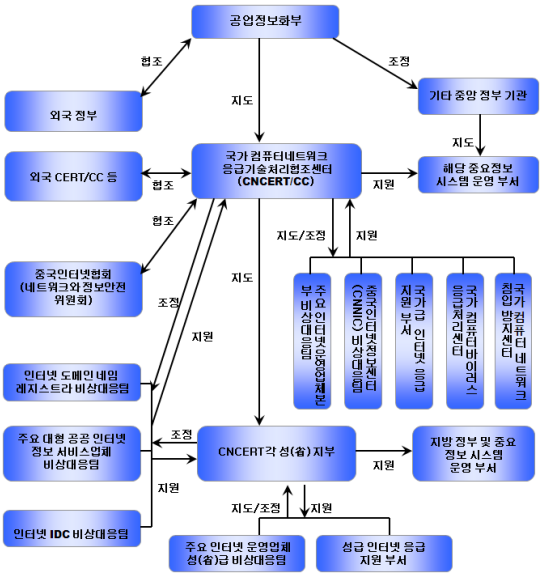
또한 사업자를 대상으로 한 기술인력 지원, 대국민 좀비PC 치료 전용 백신 제공 및 보안 취약점 공지문 게재 등의 업무를 수행한다.

4.2. 중국 : CNCERT/CC

중국의 CNCERT/CC는 2002년 9월 설립된 비정부·비영리 사이버 기술센터 및 침해사고대응팀이다. CNCERT/CC는 '주도적 방어·시기적절한 탐지·즉각적 대응·극대화된 복구' 가이드라인(guideline of "proactive prevention, timely detection, prompt response and maximized recovery)에 따라, 사이버보안 위협 방지·탐지·경고·조정 업무를 수행한다.

CNCERT/CC의 사고대응 범위는 악성코드, 변조, 백도어, 피싱, 취약점, 정보 파괴, 서비스거부 공격, 비정상적 도메인, 라우터 하이재킹, 무단 접근, 스팸, 복합적 사이버보안 사고 및 기타 사이버보안 사고 등이다.

중국의 침해사고 대응절차는, 신고(Report), 접수(Acceptance), 처리(Handling), 전파·발령(Feedback)의 네 단계로 이루어진다.



〔그림 10〕 중국 침해사고 대응절차

4.2.1. 신고 (Report)

CNCERT/CC는 기초 네트워크, 모바일 인터넷, IDC, 부가가치 비즈니스와 온라인 재정, 보안 등과 같은 필수적 정보시스템 등에 대한 사이버 공격을 모니터링한다.

그리고 CNCERT/CC에서는 24시간 내내 사이버보안 사고에 관한 신고를 받을 수 있는 메커니즘을 수립

하여 시행중이다. 기본통신서비스 사업자 및 국내외 사용자들의 웹사이트, 이메일, 핫라인, 팩스 등을 통하여 CNCERT/CC에게 침해사고를 신고할 수 있다.

4.2.2. 접수 (Acceptance)

접수된 사이버보안 위협에 대해 분석을 하고 분석된 정보에 관한 경고를 하는 단계이다. 다양한 경로를 통해 수집된 풍부한 데이터와 정보를 기반으로 침해사고를 탐지하여 사이버보안 트렌드를 분석한다.

CNCERT/CC는 정보를 접수·분석하여 중요상황을 공업정보화부 통신보장국에 신속히 보고한다. 그리고 침해사고들을 이미 발생한 사건정보와 발생예상되는 조기경보정보로 분류하고 정보등급 구분 기준을 정한다.

4.2.3. 처리 (Handling)

충분한 증거에 의해 침해사고가 사실이라는 것이 확인되면, CNCERT/CC는 즉각적 대응 메커니즘에 따라 긴급상황에 대처하게 된다.

국내외 ISP, 도메인 이름 등록자 및 사이버보안 서비스 업체들과 협력이 이루어진다. 기본통신서비스사업자, 인터넷도메인등록기관, 인터넷도메인등록서비스기관은 CNCERT/CC로부터 사이버보안 위협정보를 받은 후 가입자에게 통지하여 삭제하도록 하고 처리상황을 모니터링한다.

CNCERT/CC는 FIRST와 APCERT의 핵심멤버로서, 사이버보안 조직과 세계 CERT들과의 협력 메커니즘을 수립하여 침해사고를 처리하고 있다.

4.2.4. 전파·발령 (Feedback)

공업정보화부 통신보장국은 정보등급 구분 기준상 중대한 사고인 경우 통신보장국이 직접 또는 CNCERT/CC에 위탁하여 관련기관·관련자·인터넷 이용자 및 각 통신관리국에 신속히 전파한다.

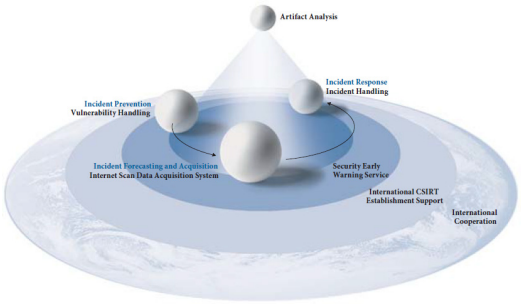
신고·접수·대응의 절차가 끝나면 CNCERT/CC는 신고에 대한 답변을 포함하여 신고자에게 피드백을 제공한다. 그리고 사이버보안 관련 통신 산업에 사이버보안 위협 정보를 경고·전파한다.

그리고 정보보안과 관련하여 과학적인 방법과 독립적인 판단을 갖춘 표준 서비스를 제공하여 정부기관의 사업을 운영 지원한다. 또한 통신 네트워크의 표준을 정립하여 통신 네트워크 및 인터넷 보안 강화를 위해 힘쓰고 있다.

4.3. 일본 : JPCERT/CC

일본의 JPCERT/CC는 1992년 자발적 조직으로 창설되어, 이후 2004년 7월 경제산업성이 소프트웨어 및 기타 취약점 관련 정보 공개 기관으로 지정하였다.

일본의 침해사고 대응절차는, 침해사고 방지(Incident Prevention), 침해사고 예측 및 수집(Incident Forecasting and Acquisition), 침해사고 대응(Incidnet Response), 침해사고 분석(Artifact Analysis)의 네 단계로 이루어진다.



〔그림 11〕 일본 침해사고 대응절차

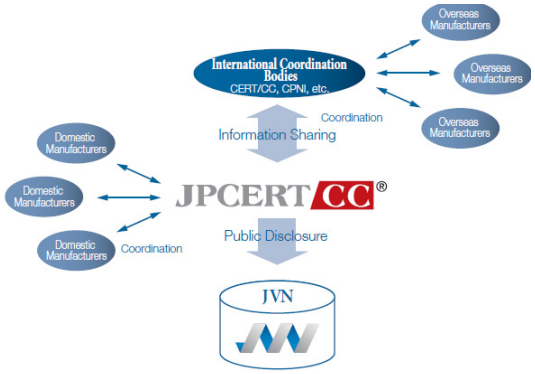
4.3.1. 침해사고 방지(Incident Prevention) - Vulnerability Handling

유사 침해사고를 막기 위하여 정확한 취약점 정보를 전파(publish)하는 단계이다. JPCERT/CC는 탐지된 취약점, 요청된 패치 및 해결책들을 제공한다.

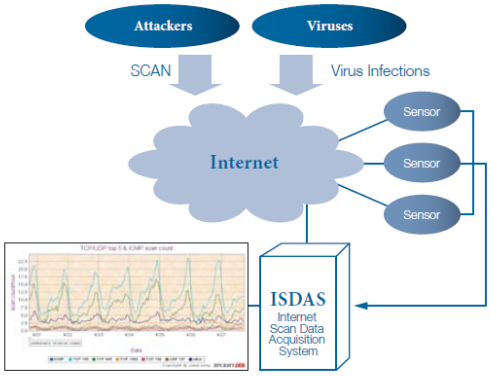
그리고 국제 CSIRTs 및 관련조직들과 함께 경보(advisory) 발령을 관리하여, 취약점 정보가 동시에 전파될 수 있도록 한다. 그리고 JPCERT/CC는 정보를 취약점 알림 포털 사이트인 JVN에 게재한다.

4.3.2. 침해사고 예측 수집(Incident Forecasting and Acquision) - Internet Scan Data Acquisition System (ISDAS)

보안 위협 및 사이버 공격에 쓰이는 봇 등 기술에 대



〔그림 12〕 침해사고 방지 단계



〔그림 13〕 침해사고 예측 수집 단계

한 정보를 수집·탐지·전파하려는 목적으로 침해사고 발생 포착을 위한 센서를 구축한다. 그리고 웜 감염 및 취약점들을 탐지하고, 네트워크 트래픽 정보를 평가·분석한다. 탐지된 데이터들은 분석되어 보안 공지 프로그램 제공에 사용되며 관련 조직 및 국제 CSIRTs와의 협력하에 분석된다.

4.3.3. 침해사고 대응(Incident Response) - Incident Handling

일본 국내외 CSIRTs와 협조하여 일하면서 JPCERT/CC는 침해사고에 관한 정보를 받고 필요에 의한 지원을 제공한다. 외국에서 탐지된 피싱사이트에 대한 정보가 입수되면, 그 나라의 CSIRT와 협조하여 사이트 차단을 요구한다. 그리고 침해사고에 관한 정보와 대책을 서로 교환 및 공유함으로써 미래의 침해사고를 방지한다.

4.3.4. 침해사고 분석 - 악성행위 분석(Artifact Analysis)

이 단계에서는 사이버공격에 사용되는 봇 등의 사물을 분석하고, 대응기술에 관한 연구를 수행한다. 그리고 분석결과물은 JPCERT/CC 활동의 기반이 되는 정보로 전파된다.

조기경보(Security Early Warning Service)를 통하여 주요 인프라시설 관련 조직들에 침해사고 대응 정보를 제공한다. 그리고 국내외 정보보안 관련 기관들의 효율적 침해사고 대응을 위해 다양한 지원을 제공한다.

〔그림 14〕 침해사고 대응 단계

Ⅴ. 결 론

우리나라가 정보통신망법 및 동법 시행령에서 사이버보안 정책에 관하여 상세히 규정하고 있는 반면, 중국은 행정법규를 통해, 일본은 정보보안 기본정책을 통해 침해사고에 대응하고 있다. 특히 중국은 정치사회체계상 정보제공 및 공유가 법률의 근거 없어도 정부의 가이드만으로 가능하다는 특징이 있다.

중국과 같이 하위법규로 규정하는 것은 보호범위와 집행효과에 문제가 발생할 수 있으며, 체계적이지 못하여 법을 집행하는 과정에서 문제가 생길 수 있다. 하지만 행정규칙 및 정부의 가이드라인을 통한 사이버보안 정책은 사이버공격 방법의 진화, 빠르게 변화하는 IT업계 등의 특성에 맞추어 침해사고에 대한 유연한 대응을 가져올 수 있다는 장점이 있다.

우리나라는 이미 정보통신망법 등 침해사고에 관해 체계적으로 정하고 있는 성문법이 존재한다. 따라서 이를 기반으로 구체적 사안에 대해서는 행정기관에 실질적 권한을 위임하여 유연한 침해사고 대응을 하는 방향으로

사이버보안 정책을 발전시켜나가는 것이 바람직하다.

또한 조사결과, 한중일 침해사고 대응기관들은 비슷한 업무의 분산으로 통일적·체계적인 침해사고 대응에 어려움을 겪어왔다는 점이 공통적으로 나타났다. 최근 일본이 「사이버보안 기본법」 제정을 통해 '사이버보안 전략 본부'를 컨트롤 타워로 법에서 명시한 것처럼, 우리나라도 실질적인 기능을 할 수 있는 사이버보안 컨트롤타워를 법에서 명시하여 인터넷 침해사고에 대한 효율적·통일적 대응을 해야 한다.

참 고 문 헌

[1] 국가정보원·미래창조과학부·방송통신위원회·안전행정부, *국가정보보호백서*, 2014.

[2] 권현준, "사이버 보안법제 선진화 방안 연구", *방송통신정책연구*, 11-진흥-라-02, 2011.

[3] 박세건, "중국정보안전입법모델연구", *경희법학*. 42권 3호, 2007.

[4] 민경식, "일본의 최근 정보보호정책 현황 및 시사점", *정보보호 Issue Report*, 2008.6.

[5] 백승흠(2009), "일본의 정보통신망 정부규제 및 자율규제 현황", *경원법학* 제2권 제2호, 2009.

[6] 이광형, "중국의 사이버범죄수사", *해외연수검사 논문*, 2007.

[7] 이연수 외 3인, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구", *국가정보연구* 제1권 2호, 2009.

[8] 이재호 외 3인 "중국의 정부체계 및 동향분석", 한국행정연구원, 2011,

[9] 정연수, "중국 사이버위협 정보공유 및 사고처리 메카니즘", 한중인터넷협력센터, 2014.

[10] KISA, "일본 정부의 사이버보안 강화 전략 분석", *Internet & Security Bimonthly* 3호, 2014.

[11] CNCERT/CC 홈페이지 http://www.cert.org.cn/

[12] JPCERT/CC 홈페이지 https://www.jpcert.or.jp/

〈저 자 소 개〉

김 희 연 (HEE YEON KIM)
정회원

2013년 8월 : 서울대학교 법과대학 법학부 졸업

2014년 9월~현재 : 서울대학교 법과대학 법학과 지식재산전공 석사과정

2014년 3월~12월 : 한국인터넷진흥원(KISA) 인터넷침해대응본부 침해사고대응단 침해대응기획팀 연구원

관심분야 : 정보보호 정책, 지식재산