情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

미국과 프랑스 정부의 사이버조기 경보 체계

오 일 석*, 김 소 정*, 고 재 영*

요 약

정보보안 선진국인 미국과 프랑스 정부는 사이버위협을 국가안보에 대한 중대한 문제로 생각하고 국가 보안을 담당하는 기관(미국, 국토안보부/사이버보안실(NCSD); 프랑스, 중앙정보시스템보안국/프랑스 정부 CERT인 CERTA 및 정부 사이버보안운영센터(ITSOC))들로 하여금 사이버위협대응을 위한 정부의 경보체계를 구축·운영하도록 하고 있다. 이러한 미국과 프랑스 정부의 사이버조기 경보체계는 국가사이버안전센터를 중심으로 사이버보안 사각지대를 해소하고 최신 사이버위협 대응 기술을 확보하며 민관협력을 통하여 우리나라의 사이버조기 경보체계를 강화·발전시키는 데 좋은 참고자료가 될 것이다.

Ⅰ. 서 론

지난 2004년 말에 인도네시아에서 발생한 지진과 해일로 인해 피해는 사망자만 십만명이 넘고 수백만의 이재민을 발생시켰으며 도시 전체를 파괴한 인류 역사상의 대재앙 가운데 하나로 기록되었다. 이처럼 엄청난 피해를 야기 시킨 지진해일의 위험성을 알고 있었던 미국과 일본 등 선진국은 지진해일 경보체계를 구축하고 피해를 예방하기 위하여 준비하여 왔다. 그러나 인도네시아, 태국, 스리랑카, 인도 등의 국가는 이러한 경보체계를 구축하지 않아 피해를 더욱 확대하였다는 비난을 면치 못하고 있는 실정이다. 이처럼 자연재해를 비롯한 현대의 위협에 대한 경보체계의 구축은 그 피해의 예방과 대응을 마련하기 위하여 가장 중요하다고 할 것이다.

이러한 경보체계의 구축은 비단 물리적인 공간에서 뿐만 아니라 우리의 제2의 생활공간인 사이버 공간에서도 매우 중요한 위치를 차지하고 있다. 즉, 국가·사회의 주요기능이 정보통신시스템에 더욱 의존하고 있는 오늘날의 사회에서 사이버 공간의 위협에 대한 경보의 발령과 그에 따른 대응은 국가의 안위는 물론 국민의 생명과 재산을 보호하기 위한 기본적인 수단이라고 할 것이다. 이하에서는 정보보안 선진국인 미국과 프랑스의 사이버 위협에 대한 조기경보 체계를 살펴보기로 한다.

Ⅱ. 미국 정부의 사이버조기 경보 체계

1. 개요

미국 정부는 사이버위협에 대응하기 위하여 클린턴 행정부 시절 대통령지시지침63(Presidential Decision Directive 63)으로 주요기반보호정책 등 사이버보안의 기초를 확립하였다.[1] 나아가 미국은 2001년 911 테러 이후 사이버 보안의 중요성을 더욱 인식하게 되었다. 이에 따라 미국은 2002년에 자국내의 보안과 사이버보안을 총괄할 기구로 국토안보부를 설립하였으며,[2] 연방정보보안관리법(Federal Information Security Management Act: FISMA)을 통과시켜 연방 부처의 사이버보안 능력 향상의 기틀을 마련하였다.[3] 또한 2003년 2월에 "사이버보안을 위한 국가전략(National Strategy to Secure Cyberspace)"을 수립하여 국가차원의 사이버 보안 계획을 수립하였다.[4]

특히 미국 정부는 국토안보부의 정보분석기반보호국(Office of Information Analysis and Infrastructure Protection)으로 하여금 사이버 보안과 주요기반시설 보호를 담당하도록 하고 있다.[2] 이에 국토안보부 정보분석기반보호국은 사이버보안 강화를 위한 민간부문과 공공부문에 대한 국가차원의 중심적인 역할을 수행하기 위하여 2003년 6월에 국가 사이

* 국가보안기술연구소 정책연구실({lucas-oh, jskim, jykoh}@etri.re.kr)

버보안실(National Cyber Security Division)을 창설하였다.[5] 미국 정부는 국토안보부 NCSD로 하여금 "사이버보안을 위한 국가전략(National Strategy to Secure Cyberspace)"의 시행 및 조정을 담당하도록 하고 있다. 이와 더불어 미국 정부는 미국의 사이버위협 경보활동을 강화하는 동시에, NCSD로 하여금 US-CERT를 창설하여 사이버조기 경보 제공 등의 활동을 수행하도록 하고 있다.[6] 따라서 미국 국토안보부/NCSD의 사이버위협에 대한 활동과 사이버보안경보체계를 살펴봄으로써 미국 정부의 사이버조기 경보 체계를 파악할 수 있을 것이다.

2. 사이버위협 경보를 위한 미국 국토안보부/NCSD 주요활동

2.1 사이버위협대응훈련 실시

미국 "사이버 보안 국가전략"의 우선순위 과제 [4]는 국토안보부로 하여금 미국 정부의 사이버 공간에 대한 보안을 책임지도록 하고 있다. 미국 국토안보부는 사이버 침해사고 대응을 위한 절차와 대비태세에 대하여 평가해 왔다. 2003년 10월 국토안보부는 최초로 사이버에 중점을 둔 훈련 "Livewire"을 실시하였다. 동 훈련은 연방 정부 침해사고 대응 능력과 의사전달 경로(communication paths)에 대한 기준선을 제시하고 있다. 또한 동 훈련을 통하여 정부 부처간의 사이버위협에 대한 대응 절차와 능력 향상을 위하여 부처간 사이버 침해사고 관리 그룹(Cyber Interagency Incident Management Group: Cyber IIMG)을 창설하게 되었다.[7]

2.2 사이버침해사고 관리 그룹(Cyber IIMG)

사이버침해사고 관리 그룹은 사이버 공격과 위협에 대한 대응 및 복구를 위한 정부 내의 대비태세(preparedness)와 운영(operations)을 조정한다. 이 그룹에는 국토안보부, 백악관, 국가안전보장회의, 국토안보위원회(Homeland Security Council), 관리예산처(Office of Management and Budget: OMB), 법 집행 당국, 국방, 정보(intelligence) 및 기타 중요한 사이버 보안 시설(capability)을 관리하는 정부 부처의 고위 관리들로 구성된다. 이들 고위 관리들은 미국의 사이버 자산에 영향을 줄 수도 있는 사이버위협과 침해사고에 대하여 국가차원의 대응을 조정하고 분석하기 위한 향상된 능력을 제공하고 있다. 이들 고위 관리들은 자신들 부처의 소관사항에 대하여 중점적인 역할을 수행함과 동시에 사이버위협과 침해사고 대응에 있어 구체적인 행동을 취할 수 있는 필요한 법률적 권한을 보유하고 있다. Cyber IIMG는 사이버 위협과 침해사고의 대응에 있어 각 부처의 조정 강화를 위하여 정기적으로 회의를 개최하고 있으며 특별히 관심 있는 부분에 대하여는 회의 시 집중적으로 논의하고 있다.[7]

2.3 정부침해사고보안팀포럼(GFIRST)

Cyber IIMG에서의 조정이외에 국토안보부는 정부침해사고대응보안팀포럼(Government Forum of Incident Response and Security Teams: GFIRST)를 창설하였다. GFIRST는 정부 차원의 침해사고 대응 능력 강화를 위해 공동으로 노력하는 연방 침해사고 대응 및 정보보안 팀들의 연합체(consortium)이다. GFIRST는 정부가 소유하거나 운영하는 미국의 주요기반들의 보호책임을 담당하고 있는 사람들에게 보안에 중점을 둔 기술들을 제공하고 있다. GFIRST는 국방, 정보(intelligence) 및 법 집행 등을 포함한 연방 정부 부처 전체의 협력을 증진하고 있다. 국토안보부는 이미 Cyber IIMG와 GFIRST를 통하여 침해사고 대비태세 확립과 대응을 위한 정부 부처들 사이의 의사전달과 협력을 증진하는데 있어 상당한 결실을 보고 있다.[8]

2.4 Cyber Annex

국토안보부/NCSD는 백악관 및 다른 연방 부처와 협력하여 다양한 공격으로부터 국가를 보위하기 위하여 침해사고 대응 및 취약성 관리 개선을 위한 체계를 구축하고 있다. 국토안보부/NCSD는 사이버 공격이나 침해사고에 대한 정부의 대응절차를 기술한 Cyber Annex를 포함한 국가대응계획(National Response Plan)을 개발하고 있다. 특히, NCSD는 국가차원의 사이버 침해사고에 대한 신뢰할 수 있고 효과적인 관리체계를 보장하는 Cyber Annex를 개발하고 있다.[8]

2.5 연방컴퓨터침해사고대응센터(FedCIRC)

미국 의회는 2002년에 연방정보보안관리법(Federal Information Security Management Act of 2002: FISMA)을 통과시켜 연방 부처들로 하여금 자신들의 정보 자산과 주요기반보호에 노력하도록 하였다.[3] FISMA는 정보보안을 강화하고 취약성 감소의 효과를 극대화하기 위한 기본틀(framework)을 제시

하여 연방 부처들로 하여금 취약성을 감소시키고 사이버 위협에 대한 대비태세를 확립하도록 하는 것을 주요 골자로 하고 있다. FISMA는 사이버위협에 대응하기 위하여 연방 정부 부처가 정보보안을 위하여 노력할 방향을 보여주고 있으며, 연방 부처들로 하여금 각 부처의 사업 차원에서 보안 평가 및 보안 정책을 실행하도록 하고, 위험 및 취약성 관리 툴도 개발하도록 독려하고 있다.

FISMA는 연방 정보보안 침해사고 센터의 운영을 요구하고 있다[1]. 이에 따라 연방컴퓨터침해사고대응센터(Federal Computer Incident Response Center: FedCIRC)는 FISMA가 규정하고 있는 특정 기능을 수행하였다. 그러나 최근 이러한 기능들은 국토안보부/NCSD의 감시 기능(watch operations)으로 통합되었다. 국토안보부/NCSD는 관리예산처(OMB)와 협력하여 연방 정부에 영향을 줄 수 있는 사이버 사건들(Events)에 관하여 지속적으로 긴밀하게 연구하고 있다. 국토안보부/NCSD는 미국 정부의 사이버 공간 보안을 위한 중요하고 견고한 기초로서 FISMA의 실행을 지원하고 있다.[8]

3. 사이버 보안 경보 체계

3.1 미국 컴퓨터긴급대응팀(US-CERT)

미국 국토안보부/NCSD는 전반적인 사이버 보안 기능을 수행하는 기구로 미국 컴퓨터긴급대응팀(U.S. Computer Emergency Readiness Team: US-CERT)을 설립하였다. US-CERT는 국토안보부/NCSD와 공공 및 민간 부문의 협력의 산출물이다. 즉, US-CERT는 카네기멜론대학교의 컴퓨터긴급대응팀조정센터(Computer emergency Response Team Coordination Center: CERT/CC)와 국토안보부/NCSD가 공동으로 설립하였다.[6,9]

US-CERT는 전 국가적 조정 센터로서 공공 및 민간 침해사고 대응능력을 결집하여 모든 기반 영역의 정보 공유를 촉진하고 미국을 사이버 위협으로부터 보호하고 있다. US-CERT의 주요 목적은 시스템적인 대비, 조정 및 대응 체계를 구축하여 미국에 대한 사이버 공격과 침해사고에 대처하고 사이버에 기초한 물리적 공격을 무력화 하는 것이라고 한다.[8]

3.2 국가사이버경보시스템(NCAS)

US-CERT에 의하여 2004년 1월부터 운영되고 있는 국가사이버경보시스템(National Cyber Alert System: NCAS)은 취약성과 침해사고 관리 및 경보를 위한 매우 중요한 메커니즘이다.[10] NCAS는 사이버위협에 대한 정보를 적재 적시에 미 국민들에게 제공함으로써 이들이 자신들의 컴퓨터를 보호할 수 있도록 하는 운영 시스템이다. NCAS에 의하여 제공되는 정보들은 모든 컴퓨터 사용자들이 쉽게 이해할 수 있도록 작성되고 있으며 광범위한 인터넷 사용 실태를 반영하고 있다. 또한 NCAS는 사용자들을 위한 일반 가이드라인을 제공하고 있다. NCAS가 제공하는 정보는 미 국민들이 자신들의 컴퓨터를 보호하기 위하여 적절한 예방 조치를 취할 수 있도록 도와주고 있다.[8]

3.3 US-CERT의 NCAS를 통한 사이버조기 경보 제공 사례

US CERT가 NCAS를 통하여 사이버위협 경보를 제공하고 민관 협력을 통하여 취약성을 개선한 중요한 사례가 있다. US-CERT는 NCAS를 통하여 일반적인 정보를 제공하는 동시에, 특정 회사의 취약성(vendor-specific vulnerability) 또는 위협 정보를 파악하여, 가능한 경우 개별 회사와 직접 이 문제를 의논하고 있다. 최근 Cisco의 취약성 사례는 US-CERT가 어떻게 직접적으로 특정 회사 제품에 기초한 취약성에 대하여 민간 부문과 교류·협력하고 있는

1) FISMA 제3546조 연방컴퓨터침해사고대응센터
(a) (국토안보부 기반보호국) 국장은 다음 각호의 사항을 위하여 연방정보보안침해사고센터(Federal information security incident center)를 운영하여야 한다.
(1) 정보보안 침해사고(information security incidents)의 탐지와 처리에 관한 가이드라인을 포함하여, 보안 침해사고에 대하여 각 부처 정보 시스템의 운영자들에 대한 기술적 지원 제공
(2) 정보보안을 위협하는 침해사고에 대한 정보의 수집 및 분석
(3) 각 부처 정보시스템 운영자에 대하여 현재 및 잠재적 정보보안 위협과 취약성에 대한 정보의 제공
(4) 국립기술표준원(National Institute of Standard and Technology: NIST), 국가보안국(National Security Agency)를 포함하여 국가보안시스템(national security systems)을 운영하거나 통제하고 있는 부처 및 기관, 정보보안 침해사고 등에 관하여 대통령과 법률로부터 (권한과 책임을 위임받은) 부처 또는 기관들과의 협의(consult with)
(b) 국가보안시스템 - 국가보안시스템을 운영 또는 통제하는 각 부처는 정보보안 침해사고, 위협 및 취약성에 관한 정보를 법률과 대통령이 정한 바에 따라 발표되는 국가보안시스템을 위한 표준과 가이드라인에 의하여 연방 정보보안침해사고센터와 공유하여야 한다.

지를 잘 보여주고 있다.[7]

US-CERT는 Cisco 사로부터 자사의 인터넷운영시스템(Internet Operating System: IOS)과 단순네트워크관리프로토콜(Simple Network Management Protocol: SNMP)의 실행에 취약성이 있음을 통보받았다. 이 취약성은 다른 버전의 많은 IOS에 대하여 영향을 줄 수 있으며 지속적인 서비스 거부 공격(denial of service: DoS)으로 이어질 수도 있었다. Cisco의 대표자들은 이러한 취약성과 관련한 정보를 미국 전반적으로 제공하는 것에 대하여 US-CERT의 지원을 요청하였다. US-CERT는 즉각 이를 접수하고 이 문제에 대한 종합 경보 제공을 시작하였다. US-CERT는 NCAS를 통하여 사이버보안기술경보(Technical Cyber Security Alert)를 발령하고, 국토안보정보네트워크(Homeland Security Information Network: HSIN)와 미국 CERT 포털을 통하여 연방 정보보안책임관(the federal Chief Information Security Officers), 정보공유분석센터 및 주요기반 사용자와 운영자 등을 포함한 사이버 공동체에 이 사이버위협 경보를 제공하였다. 이러한 사례를 통하여 사이버조기 경보 제공의 중요성을 더욱 인식하게 된 미국 국토안보부/NCSD는 US-CERT와 사이버위협에 대한 경보 강화와 취약성의 발견과 감소를 위한 활동을 위하여 민관협력의 중요성을 크게 인식하여 US-CERT 협력 프로그램(US-CERT Partner Program)을 계획하게 되었다.[7]

3.4 US-CERT 민관협력 프로그램

국토안보부는 최근 미국의 사이버 보안 강화를 위한 종합적인 협력 프로그램 개발을 위하여 민간 부문과 밀접하게 협력하고 있다. US-CERT 민관협력 프로그램(US-CERT Partner Program)은 국토안보부, 기타 정부 부처, 학계 및 민간 부문의 공식적인 협력 체계를 구축하게 될 것이다. 이 프로그램은 사이버 보안에 대한 국가적 인식증대를 위한 공공 및 민간 부문의 협력에 중점을 둘 것이며 연방, 주 및 지방 정부와 학계 및 개별 기업들에 사이버 보안에 대한 조정을 실행할 것이다. 이 협력 프로그램은 미국 주요 기반과 인터넷의 사이버 보안을 강화하기 위한 공공과 민간 부문의 대비, 분석, 경보 및 대응 활동들에 대한 국가적 사이버 보안 조정의 초석이 될 것이다. 이 프로그램에는 정보공유분석센터를 포함한 주요기반 분야, 산업계 및 관련 기관, 연구기관 및 학계 등이 참석할 것이다.[8]

US-CERT Partner Program의 임무는 사이버 공격에 대한 예방, 인식, 대응 및 복구를 위한 국가적 능력을 실질적으로 향상시키는 것이다. 이러한 임무를 수행하기 위하여 US-CERT Partner Program은 사이버 위협과 취약성에 대한 예방, 예견, 탐지 및 대응 관련 정보를 공유하고, 미국의 주요 기반에 대한 사이버 보안을 강화하며 회원들에게 사이버 취약성, 악성 코드, 바이러스 등에 대한 식별, 분석 및 경보를 제공할 것이다.

또한 US-CERT Partner Program은 민간 및 공공 분야의 사이버 이벤트(event) 대응을 조정 및 개선하고, 사이버위협 정보의 분석 및 정보 교류 증진을 위한 안전하고 신뢰성 있는 협력체계(Forum)을 구성하여 사이버 보안을 위한 국가적 실행사항(commitment)을 제공할 것이다. US-CERT Partner Program은 회원들에게 사이버 취약성, 악성 코드, 바이러스 등에 대한 식별, 분석 및 경보 제공을 위하여 미국의 국가 기반의 보호와 관련된 정보를 수집, 분석 및 제공을 위한 체제(mechanism)를 구축할 것이다. 회원들은 국토안보부의 전반적인 사이버 보안 대비를 위한 적절한 조치를 취하여야 할 것이며 이러한 노력의 결과로 취약성 관리가 개선되고 결과적으로 국가적 조직적 사이버 보안을 강화하게 될 것이다.[8]

Ⅲ. 프랑스 정부의 사이버조기 경보 체계

1. 개요

프랑스는 사이버 보안을 국가 안보의 문제로 인식하여 총리실 직속의 국방사무국(General Secretariat of National Defense: SGDN)으로 하여금 사이버 보안을 담당하도록 하고 있다.[11] 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 2001-693은 국방사무국내에 중앙정보시스템보안국(the 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.[12] 프랑스 사이버 보안 관련 국가적인 조직체계는 그림 1과 같다.

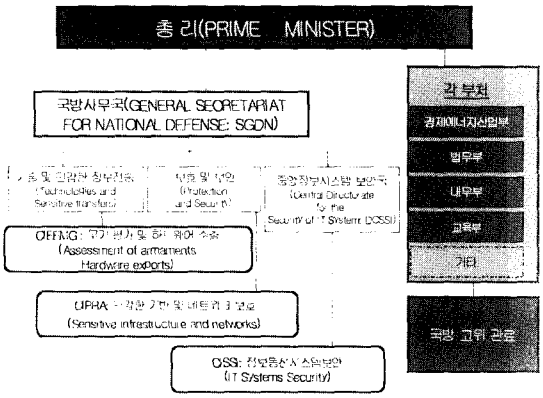


그림 1. 프랑스 정부 사이버 보안 관련 주요기구

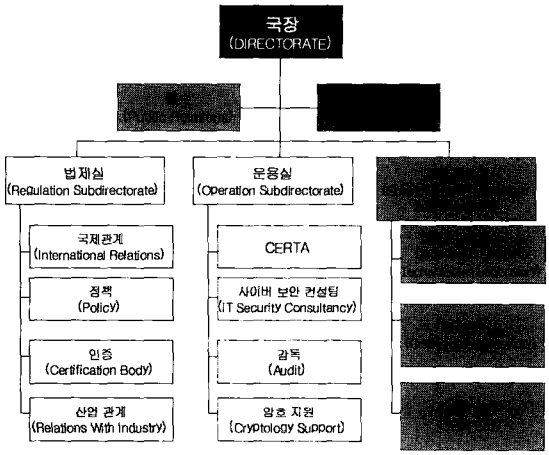


그림 2. 프랑스 DCSSI 조직도

2. 프랑스 정부의 사이버 보안 관련 주요기구

2.1 국방사무국(SGDN)

프랑스 국방사무국은 국내외 안보 문제에 관하여 책임을 부담하고 있다. 국방사무국은 프랑스 총리의 직접적인 명령을 받고 있으며 사이버보안 및 주요기반 보호와 관련된 정부 부처들의 활동을 조정하고 있다.[11] 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 국방사무국내에 중앙정보시스템보안국(the Central Directorate for Security of Information Systems: DCSSI)을 창설하도록 규정하고 있다.[15] 국방사무국은 국방 분야 및 민간 분야 관련 정보통신기술의 보안에 중점을 두면서 국방정책 및 보안정책의 과학·기술적 혁신에 대하여도 책임을 부담한다. 이와 관련하여 국방사무국은 DCSSI와 긴밀하게 협력하고 있다.[11]

2.2 중앙정보시스템보안국(DCSSI)

DCSSI는 프랑스 정부 특히 행정부(administration)와 주요기반의 정보시스템 보안과 정보화사회의 촉진과 발전을 위한 신뢰환경 구축을 2가지 주요한 목적으로 하고 있다. 이를 위하여 DCSSI는 사이버보안[2]에 관한 정부 정책을 수립하고, 사이버 보안을 위한 법률적 권한을 제공하며, 위기관리, 컨설팅, 감사(audit) 및 경보 등과 같은 정보기술보안을 위한 공적 서비스 제공 등의 임무를 수행하고 있다.[11] 또한 정보기술보안과 관련한 과학기술을 개발하고 사이버보안 교육·훈련 프로그램을 운영하고 있으며 사이버 보안 인식제고 임무도 수행하고 있다. 나아가 DCSSI는 정부 각 부처의 정보보안 관련 활동을 조정하고 있다. DCSSI는 그림 2와 같이 구성되어 있다.[12,15]

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.[12,15]

또한 DCSSI는 정보시스템보안(Security of Information Systems: SSI) 웹사이트를 운영하고 그 활동을 조정하고 있다. SSI 웹사이트는 프랑스 정부 CERT인 CERTA(Computer Emergency Response Team Administration)에 관한 정보를 제공할 뿐만아니라, 사이버 보안에 관련된 법규와 기술 정보를 제공하고 있으며, 평가인증(Evaluation-Certification)에 대한 일반적인 정보를 포함하여, 평가인증 방법론, 제품에 대한 정보도 제공하고 있다. 또한, 전자서명 및 암호 등에 관한 정보를 제공할 뿐

2) DCSSI 관부들은 정보기술보안(Information Technology Security: Infosec)이라고 하고 있으나 그 의미는 사이버 보안과 같다고 할 수 있다.

만 아니라 기술적 자문을 제공하고 있다. DCSSI는 프랑스의 다른 정부부처들에 대하여 정보보안에 대한 정보와 자문을 제공하고 있으며, 정보시스템 보안과 관련하여 국가적 법률 및 공공 서비스에 대한 지원을 하고 있다. 또한 DCSSI는 정보보안 분야에서 기술적 전문성을 확보하고 위협 평가 및 경보를 발령하고 있다. 아울러 프랑스 정부부처 공무원들에 대한 교육훈련센터도 운영하고 있다.[12,15]

3. 프랑스 정부의 사이버 조기 경보 체계

3.1 프랑스 정부 CERT(CERTA)

DCSSI가 운영하고 있는 프랑스 정부 CERT인 CERTA는 원래 "프랑스 정부의 컴퓨터 시스템 침입에 대한 활동을 강화하고 조정하기 위하여 프랑스 정부는 컴퓨터 공격을 탐지하고 관련 문제를 해결하기 위한 지원 및 경보팀의 창설을 결정한다"고 하는 1999년 1월 19일 CISI(Comite Interministeriel pour la Societe de l'Information) 결정에 의하여 창설되었으며, 1999년 10월 발족하였다. CERTA는 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.[13]

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. 즉, 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.[14,15]

3.2 프랑스 정부 사이버보안운영센터(ITSOC)

DCSSI가 운영하고 있는 사이버보안운영센터(IT Security Operation Center: ITSOC)는 사이버위협에 대한 프랑스 정부의 계획-VIGIPIRATE(IT 보안 측면) 및 PIRANET 계획을 조정하기 위하여

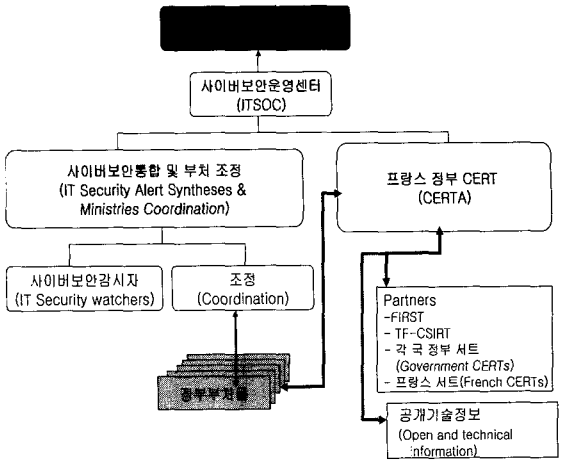


그림 3. DCSSI 사이버보안운영센터를 통한 사이버위협정보 제공

설립되었다.[12,14]

사이버보안운영센터는 기술적 활동, 조정 활동 및 커뮤니케이션 활동을 주요 임무로 수행하고 있다. 기술적 활동은 침해사고의 예방과 해결을 위한 기술적 전문지식과 관련된 활동으로 전반적인 보안 수준 향상을 위한 일반적인 조치(general measures)와 공격에 대한 특별한 기술적 조치(specific technical measures)들이 있다. 조정 활동을 통하여 효과적인 대응을 위한 공적인(Official) 활동을 주도하고 있다.

또한, 커뮤니케이션 활동을 통하여 고위 관리(Authorities)들을 위한 사이버 보안 활동을 통합하고 있다. 즉, 신속한 조치나 결정이 취해 질 수 있도록 하며 일반 대중을 위하여 정보를 제공하고 관련 고위 관리들을 위하여 특별한 정보를 제공하는 것이다.[12,15]

DCSSI의 사이버보안운영센터는 프랑스 정부 CERT인 CERTA를 통하여 다양한 통로로 사이버위협정보와 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 사이버보안통합및부처조정을 통하여 파악한 사이버위협정보를 각급기관의 고위관리들에게 제공하고 있다.[15]

3.3 프랑스 정부 사이버보안위기관리체계

프랑스 정부는 '사이버보안 경보 및 위기관리'를 위

하여 4가지 단계를 수립하고 사이버보안경계계획(VIGIPIRATE IT Sec)과 PIRANET계획을 수립하였다. 즉, 프랑스 정부는 '사이버보안 경보 및 위기관리'에 관하여 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.[12,15]

아울러 PIRANET계획을 수립하여 예·경보를 실행하고, DCSSI의 ITSOC로 하여금 일반적 조치와 특별 체계를 수립하도록 하고 있으며 각 정부부처로 하여금 사이버보안과 자체 사이버보안 조치 및 체계를 정립하도록 하고 있다. 특히 프랑스 정부가 2004년 3월 10일 발표한 정부정보시스템보안강화계획(the State Information System Reinforcement Plan (2004-2007)은 경계수준 4단계와 5단계에 대응하기 위한 사이버보안경계계획과 PIRANET 계획의 실행을 위하여, 사이버 위협 대응을 위한 24시간 운영센터를 DCSSI를 포함하여 각 정부 부처에 설립하도록 하고 있다. 나아가, 사이버 위협 대응과 사이버보안 경보를 위하여 DCSSI의 ITSOC와 CERTA에 필요한 전문인력을 확보할 것을 요구하고 있다.[14,15]

또한, 프랑스 정부는 사이버보안 및 위기관리를 위하여 각 정부부처로 하여금 사이버보안 기능, 운영 및 24시간 감시센터 등을 포함한 사이버보안 경보디렉토리를 설정하고, 사이버조기 경보 및 대응을 위한 각 부처의 행위자와 행동요령에 관한 카드 작성을 포함한 가이드라인을 정립하도록 하고 있다. 또한 프랑스는 정부 각 부처로 하여금 DCSSI 산하의 ITSOC 및 CERTA와 유기적으로 협력하여 사이버위협 관련 정보를 교류하고, 사이버보안 경보를 제공받아 자체 사이버보안조치를 실행하도록 하고 있다. 또한 사이버보안 관련 최종 정책적 결정은 총리가 실행하도록 하고 이를 위한 각 종 정보의 제공 및 지원을 국방사무국 및 DCSSI가 수행하도록 하고 있다.[12,15]

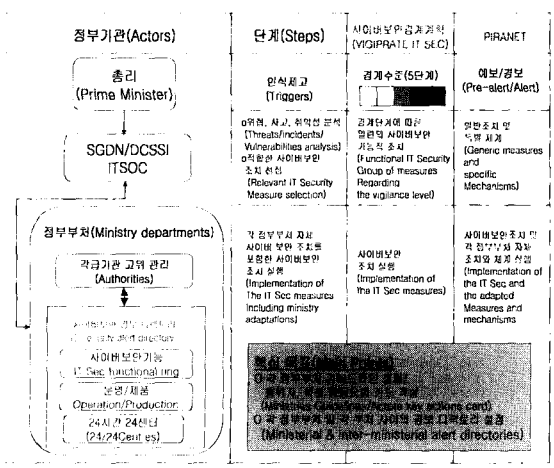


그림 4. 프랑스 정부의 사이버보안 경보 및 위기관리 체계

Ⅳ. 결 론

정보보안 선진국인 미국과 프랑스 정부는 사이버위협을 국가안보에 대한 중대한 문제로 생각하고 국가보안을 담당하는 기관들로 하여금 사이버위협대응을 위한 정부의 경보체계를 구축·운영하도록 하고 있다.

즉 미국은 국토안보부 사이버보안실을 중심으로 사이버위협대응 훈련을 실시하고 US-CERT와 국가사이버경보시스템(NCAS)를 구축·운영하고 있다.

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. 또한 2004년 3월에 정보시스템보안강화계획(2004-2007)을 수립하여 프랑스 정부의 사이버 위협 대응 능력 향상을 위해 노력하고 있다.

이러한 미국과 프랑스 정부의 사이버 위협 경보체계는 국가사이버안전센터를 중심으로 사이버보안 사각지대를 해소하고 최신 사이버위협 대응 기술을 확보하며 민관협력을 통하여 우리나라의 사이버 위협 경보체계를 강화·발전시키는데 좋은 참고자료가 될 것이다.

참 고 문 헌

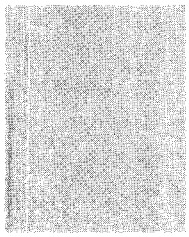
[1] 한국정보보호센터, 국외의 주요기반보호 정책 분석 연구, pp. 31-47, 1999년 12월

[2] 오일석외, 미국국토안보부 설립 대통령제안서 분석, 국가보안기술연구소, 2002년 12월

[3] 오일석 외, 미국 정보보안 관련 주요 법규, 국가보안기술연구소, 2003년 11월

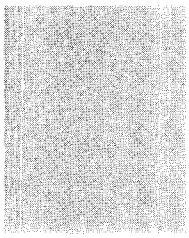
[4] 오일석 외, 미국 사이버공간보안 국가전략(초안), 국가보안기술연구소, 2003년 2월
[5] http://www.dhs.gov/dhspublic/display?content=916
[6] www. us-cert.gov
[7] http://www.us-cert.gov/policy/testimony_yoran_jun0204.html
[8] Amit Yoran, 미국 국토안보부 기반보호국 국가사이버보안실 실장, 미 하원, "정부개혁위원회" 소속 "기술, 정보정책, 정부 부처간 관계 및 센서스 소 위원회" 청문회 증언, 2004년 6월 4일 (http://reform.house.gov/UploadedFiles/Yoran%20Testimony%20Final1.pdf)
[9] www.cmu.edu/cmnews/031004/031004/031004_homesecurity.html
[10] http://www.us-cert.gov/cas/
[11] 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.
[12] http://www.ssi.gouv.fr
[13] http://www.certa.ssi.gouv.fr
[14] 프랑스 정부, 정보시스템보안강화계획(2004-2007), 2004년 3월 10일.
[15] 프랑스 DCSSI 간부들과의 인터뷰, 2004년 9월.

〈著 者 紹 介〉



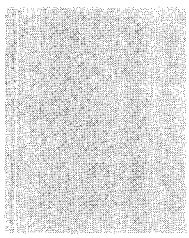
오 일 석 (Il Seok, Oh)
정회원

1994년 2월 : 한국외국대학교 영어과 졸업
1997년 2월 : 고려대학교 대학원 법학과 석사
1997년 3월~10월 : 고려대학교 비교법연구소 전임연구원
2001년 3월~현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 국내외 정보보호 정책 및 법/제도



김 소 정 (So Jeong, Kim)

1998년 8월 : 부산대학교 사학과 졸업
2001년 2월 : 경희대학교 GIP 동북아학과 석사
2005년 2월 : 고려대학교 정보보호대학원 정보보호학과 박사
2004년 5월~현재 : 국가보안기술연구소 연구원
〈관심분야〉 정보보호 정책 및 법/제도, 개인정보보호



고 재 영 (Jae Young, Koh)

1984년 2월 : 전북대학교 공과대학 전자공학과 졸업
1992년 8월 : 전북대학교 대학원 전자공학과 석사
1998년 8월 : 전북대학교 대학원 전자공학과 박사
1984년 3월~2000년 1월 : 국방과학연구소 선임연구원 전산보안팀장
2000년 2월~2004년 1월 : 국가보안기술연구소 책임연구원 응용기술연구부장
2004년 2월~현재 : 국가보안기술연구소 책임연구원 정책연구실장
〈관심분야〉 정보보호 정책, 정보통신망 보안, 정보보증