한국컴퓨터정보학회지
제22권 제1호, 2014. 6.

# KAIST 사이버보안연구센터

• 박재경(한국과학기술원 CSRC)

## I. 개요

### 1. 센터 설립 배경 및 추진방향

KAIST 사이버보안연구센터는 정보보호전문가 양성을 위해 국가에서 지정·인가한 체계적인 전문 교육, 훈련 기관 부재로 ITRC 사업 등을 통한 사이버 보안 관련 전문 연구 및 정보보호학과 신설을 추진하는데서 비롯되었다. 행정안전부 보고자료 설문조사에 의하면 국내 불균형 및 관리정책 미흡 등으로 우수 정보보호 인력의 82%가 해외진출을 고려하고 있는 것으로 조사되어 전문 인력의 해외유출이 심각한 것으로 확인되었다. 국가 정보보안의 중요성이 대두됨에 따라 지식경제부 분과위원회 등 국회에서 국가 사이버보안 전문 인력양성 필요성이 제기되었으며 청와대(정책실)에 국가차원의 '사이버보안연구소' 설립 필요성이 건의 되었다.

현재 KAIST 사이버보안연구센터는 글로벌 경쟁력을 갖춘 세계 최고의 정보보호, 고급 인력양성 및 차세대 사이버보안 신기술 개발을 통하여 Cyber World를 선도할 수 있는 강력한 사이버 방호 체제를 구축하고, 다음과 같은 목표를 가지고 국가의 안전보장 및 국가의 이익을 수호하는데 주력하고 있다.

- 사이버 보안 신기술 개발 및 연구 활동
- 악성코드 분석 서비스
- 정보보안 고급 인력 양성
- 사이버보안 교육실시

사이버 보안 신기술 개발 및 연구 활동은 신·변종 해킹 사전탐지 및 인공 지능형 첨단 신기술 개발 및 모바일(스마트폰)해킹 방어기술 개발 및 대응능력 연구, 침해사고 통제시스템 연구, 각종 해킹 프로그램 수법을 연구하고 있으며 악성코드 분석 서비스는 웹 사이트 비정상 정보 탐지시스템에 대한 안정화 및 고도화, 악성코드 분석 포털 서비스를 구축하여 악성코드를 미연에 탐지할 수 있도록 연구하고 있다. 정보보안 고급 인력 양성은 글로벌 수준의 고급 정보보호 전문가를 육성하여 국가 정보보안에 기여하고 있으며 사이버보안 교육을 통하여 사이버 공간에서의 위험 요인에 대한 인식을 제고하고 사이버보안 전문가로서 진출, 성장을 위한 최신 전문지식과 기술습득, 프레임 워크의 제시와 이를 위한 연수 프로그램의 운영을 통한 국가 사이버 인적 자원 확보에 기여를 목표로 하고 있다.

### 2. 주요 연혁

KAIST 사이버보안연구센터는 최근 3년간 공공기관과의 업무협정 체결 및 정보보호대학원을 통한 정보보호 전문가 양성, 악성코드 보고서를 발간하여 국가 정보보호에 기여하였다. 그 외 자세한 사항은 표 1 에 정의하였다.

표 1. KAIST 사이버 보안 연구센터 주요 연혁

| | |
|---|---|
| 2013년 | |
| 9월 | 국방부 사이버사령부, “SIMon 엔진” 시범 설치 |
| 6월 | 병무청의 병역특례(전문 연구요원) 운용 |
| 4월 | 정부통합전산센터, “SIMon 엔진” 시범 설치 |
| 2월 | 정보보호대학원, 제1회 졸업생 배출(석사 5명) |
| 2월 | 주간 ‘악성코드 동향분석 보고서’ 발간 및 정기적 배포 |
| 1월 | 2012년도 연간 ‘악성코드 동향분석 보고서’ 발간 |
| 2012년 | |
| 11월 | 이스라엘 정부 초청, “Int'l Homeland Security Conference” 패널 발표 |
| 5월 | “SIMon 엔진”(웹페이지 비정상 정보 탐지 시스템) 개발 |
| 9월 | 정보보호대학원 국비 장학생 정원 확보(매년 25명) |
| 9월 | 경찰청과의 업무협정(MOU) 체결 |
| 2월 | 정보보호대학원 정규 인가 |
| 1월 | 중소기업중앙회와의 업무협정(MOU) 체결 |
| 1월 | ‘글로벌 사이버보안 기술연구 기관’ 고유사업 지정 |
| 2011년 | |
| 11월 | 한국인터넷진흥원과 업무협정(MOU) 체결 |
| 11월 | 국방과학연구소와 업무협정(MOU) 체결 |
| 11월 | 금융보안연구원과 업무협정(MOU) 체결 |
| 8월 | 정부통합전산센터와 업무협정(MOU) 체결 |
| 2월 | “KAIST 정보보호 대학원” 설립 및 제1회 신입생 입학 |
| 2월 | “KAIST 사이버보안연구센터” 설립 및 개소식 |
| 2010년 | |
| 12월 | ‘사이버보안 인력양성 및 연구 개발사업’ 수행기관 지정(3년) |

## 3. 조직도 및 인력운용

KAIST 사이버보안연구센터는 센터장을 중심으로 전략기획실, 기술개발실, 차세대보안연구실, 행정실, S+ 컨버전스 최고 경영자 과정, 위원회로 나뉘어져 있다.


그림 1. KAIST 사이버보안연구센터 조직도

전략기획실은 사이버보안 정책연구 및 사이버보안 교육 및 신규사업을 기획하고 있으며 기술 개발실은 신규 보안 기술 연구 및 통합보안장비 개발, 응용기반 제품 연구 및 개발을 하고 있다. 차세대보안 연구실은 지능형 사이버위협 대응기술 연구 및 악성코드 유포경유지 분석기술 연구와 대국민 보안 서비스를 제공함으로써 국가 정보보안에 기여하고 있다. s+ 컨버전스 최고 경영자 과정은 지속 가능 경영을 선도하는 최고 경영자 역할 및 모든 사업간의 기술 융합으로 새로운 패러다임을 제시 함으로써 불 확실한 미래 환경변화와 위기에 대처할 수 있는 창조적인 지식과 경영 전략을 교육한다.

각 연구실은 실장 및 연구원으로 구성되어 있으며 관련 이력사항 및 인원은 표 2 에 정의하였다.

표 2. 연구실 관련 정보

| 연구실 | 직책 | 이름 | 이력사항 | 인원 |
|---|---|---|---|---|
| 센터장 | | 주대준 | · KAIST대외부총장 역임<br>· 前)대통령실 경호처 경호차장<br>· 前)대통령경호실 행정본부장<br>· 前)대통령경호실 · 정보통신처장<br>· 前)청와대 전산실장<br>· KAIST 경영정보공학 박사 | |
| 부소장 | | 이광식 | · 대통령경호실 정보통신국장 역임 (이사관 퇴직)<br>· 前)대통령경호실 CIO 및 CSO<br>· 前)체신부, 국가안전보장회의, KT근무<br>· 광운대학교 정보통신공학 석사 | |
| 전략 기획실 | 실장 | 오익균 | · 前)대통령 비서실<br>· 전산정보실장, CIO 보좌관 역임<br>· 前)한국전산원 초고속국가망 연구실 정보서비스센터팀장<br>· 前)주)데이콤<br>· 충남대학교 컴퓨터공학 박사과정 | 황상기<br>윤관식 |
| 기술 개발실 | 실장 | 박재경 | · 한국컴퓨터정보학회 이사<br>· 前)어울림정보기술 연구소장<br>· 前)퓨처시스템 UTM개발부서장<br>· 홍익대학교 전자계산학 박사 | 박재필<br>정승일<br>김현우<br>오동엽 |

| | | | | |
|---|---|---|---|---|
| 차세대 보안 연구실 | 실장 | 최상용 | · 前)고용노동부<br>· 정보보호담당관<br>· 前)안행부 통합전산센터<br>· 해킹대응 및 분석담당<br>· 前)이글루시큐리티, SK인포섹<br>· 전남대학교 정보보호학 박사 | 한기문<br>정욱현<br>조호목<br>강익선<br>김대혁<br>김상원 |

# II. 본론

## 1. 각 실별 주요 활동

### 1.1 전략 기획실

전략 기획실은 사이버보안과 관련된 정책을 연구하고 교육을 통한 인재 양성 및 신규 사업을 기획하는 부서이다.

#### 1.1.1 사이버보안 정책 연구

현재 사이보안의 의미나 범위 등의 기준이 모호한 경우가 많은 상황에서 사이버보안의 표준을 정립하고, 거버넌스, 위험관리, 컴플라이언스 체계 확립을 위한 연구를 진행하고 있다. 또한 사이버보안 운영 절차 및 방법에 대한 가이드라인 개발과 기술 지원을 연구한다. 그리고 사이버보안 수준에 대한 측정 방법을 연구하고 있으며 국가 사이버 안보의 위협을 파악하기 위한 사이버보안 지수 수준 평가 모델을 연구하고 측정을 위한 관련 기술 개발을 추진한다. 정부부처, 공공기관의 사이버보안 지수 수준 측정을 통한 위험관리 및 보안강화 방안을 강구하고 있다. 그리고 국가 사이버보안 전략 지원과 관련하여 국내 사이보안 환경과 선진국 사이버보안 환경 분석을 통하여 개선 방향을 도출하고 조직, 법·제도, 예산, 인력, 기술 분야별 문제점 발견 및 개선 방안을 도출하고 있다. 또한 사이버보안 주요 피해 사례를 통하여 사이버보안 대응전략 개발을 지원한다.

#### 1.1.2 사이버보안 교육 아카데미

사이버안보 분야에서는 정부, 금융권, 산업계 인원(경영진) 및 현장 직원들에게 사이버보안 직무교육을 체계적으로 실시하여 지능적 사이버 테러와 해킹사고를 예방하고 국가 사이버안보의 수준을 제고한다.

전문 위탁 교육 분야에서는 사이버보안(정보보안 포함) 분야의 다양한 연구개발 및 해킹사고 대응경험이 풍부한 KAIST 전문 연구원과 정보보호대학원 교수진으로 강사를 구성한 전문 위탁 교육을 실시하고 있다.

교육 범위로는 첫 번째, 사이버보안 교육으로 사이버 업무의 안정성, 신뢰성 보장을 위한 보안 조치 대책에 대해 교육한다. 두 번째로 정보보호 교육으로는 전자정부, 전자금융, 산업기술, 개인정보 등 대민서비스 및 내부 정보보호 담당(실무 책임자) 직무 향상 교육이 있다. 세 번째로 국방부 직할부대 및 기관장(최고 경영자)을 위한 사이버보안 경영 정책 제안(Mentoring)으로 내부심사(Internal Audit)를 통해 조직 내 잠재된 보안위협 및 취약성 사전진단(대안제시)이 있다.

### 1.2 기술 개발실

기술 개발실은 신규 보안기술을 연구 하고 보안 기술을 이용하여 통합 보안 장비를 개발한다. 또한, 산학협력 개발 및 산업화를 진행하는 조직이다.

#### 1.2.1 신규 보안기술 연구

국가 사이버 공격의 주요 도구로 사용되는 악성코드를 탐지 및 차단하기 위하여 능동적이고 자동화된 기술을 연구하고 개발한다.

동적 분석 시스템 연구 개발은 웹 브라우저 애뮬레이터 분석의 한계를 해결하기 위한 동적 분석 시스템 개발하는 것이다. 에뮬레이터에서 분석 불가한 악성 의심 웹 페이지에 대한 재분석 기술을 연구하며 Windows 파일 시스템을 모니터링(파일 및 레지스트리 생성 및 변경 여부)하고 네트워크 데이터(Pcap), 행위 로그 저장하는 기술을 연구하며 개발한다.

보안 전용 OS 연구 개발은 보안에 최적화된 리눅스 Kernel 기반의 OS를 개발하여 OSI 7 Layer 7계층(Network), 4계층(Transport)을 분석하고 3, 4 계층의 최적화된 IOCTL을 개발한다.

또한, 고성능 URL Filtering 엔진 연구는 커널 레벨의 URL Filtering 엔진 연구를 통해 빠른 처리 속도와 다양한 Protocol에 대응하는 엔진을 연구한다.

#### 1.2.2 통합 보안장비 개발

악성코드에 대한 고도화된 기술을 통해 이를 보안장비화 하며 향후 실제 네트워크에 사용하여 실시간으로 악성코드를 차단하고 네트워크를 안전하게 보호하기 위한 장비를 개발한

다. 현재 패킷 미러링을 이용한 악성링크 탐지 및 차단 시스템을 개발 중에 있다.

#### 1.2.3 산학협력 개발 및 산업화

KAIST 사이버 보안연구 센터를 통해 개발된 기술을 산업화하고 산학 협동을 통한 기술이전 추진한다.

### 1.3 차세대 보안 연구실

차세대 보안 연구실은 지능형 사이버 위협 대응 기술을 연구 및 개발하고, 이 기술들을 이용하여 대국민 보안 서비스를 제공하고자 하는 부서이다.

#### 1.3.1 지능형 사이버위협 대응기술 연구

차세대 보안 연구실에서 개발한 SIMon(Suspicious Information Monitoring system in website)은 40만개 이상의 웹사이트에 대해 실시간으로 모니터링하며 에뮬레이션 기반의 웹페이지에 대한 악성 여부를 분석하는 시스템이다. 현재 다양한 기관에서 운영되고 있다.

악성 웹페이지 분류기술 연구 및 악성코드 유포 방법을 분석한다. 정상 및 악성 웹페이지 분류를 위한 특정 인자 추출과 기계 학습 기반의 요과적인 분류 알고리즘을 연구한다. 그리고 능동적인 웹페이지 검사를 통해 신종 악성코드 유포방법에 대한 탐지 및 분석 기술을 연구 하고, 웹페이지를 이용한 악성코드 전파 방법으로 사용되는 취약점에 대한 자동 분석 및 분류 방법을 연구한다. APT와 같은 지능형 위협을 탐지 할 수 있는 기반 기술을 연구하고 있는데 장기간 IT인프라 데이터를 수집 및 분석하고 빅데이터 플랫폼을 활용한 기계 학습 기반 탐지 알고리즘을 연구한다.

#### 1.3.2 대국민 보안 서비스 제공

현재 악성 웹페이지 접속 차단 서비스를 준비 중이며 2014년 하반기에 예정되어 있다. SIMon이 분석한 데이터를 실시간 반영하여 악성코드 감영을 예방하는데 목적이 있다.

홈페이지 위변조 점검 및 웹사이트 모니터링 서비스 또한 2014년 하반기 제공을 위한 준비 중에 있으며, 중소기업/소상공인 대상 홈페이지에 대해 사이버 공격에 의한 폼페이지 위변조 여부를 실시간으로 감시하는 서비스와 관리 소관 웹사이트에 악성링크 포함 유무를 무료 점검할 예정이다.

보안동향보고서를 발간 중에 있으며 SIMon 데이터베이스를 활용하여 악성코드 유포추이 및 통계분석 정보와 국내외 보안이슈를 분석하여 제공하고 있다.

## 2. 기존 주요 실적

### 2.1 2013년 주요 사업실적

#### 2.1.1 웹페이지 비정상 정보 탐지시스템(SIMon) 연구개발 및 고도화

악성코드(Malware)로 인한 피해를 최소화하고 예방할 수 있는 능력 강화를 위한 악성코드 감염 이전(以前) 단계에서 악성코드 유포/경유지를 실시간 수집, 모니터링 및 분석하는 '웹페이지 비정상 정보 모니터링 시스템' (SIMon: Suspicious Information Monitoring System in Website) 연구 개발하였다.

연구 개발 실적으로는 '웹페이지 비정상 정보 모니터링 시스템' 엔진 자체 개발하였고 4대 SIMon 에이전트 서버와 1대 SIMon 관리자 서버를 통하여 실시간으로 모니터링 하고 있다. 모니터링 대상은 약 42만개의 인터넷 홈페이지(도메인)이며 분석 결과는 악성코드 유포지 약 700여건, 악성코드 종류 약 400여종을 분석하였다. 탐지, 분석된 악성코드에 대한 중요 사항 및 내역, 예방책 등에 관하여 전파하기 위해 매주 '악성코드 주간동향보고서' (2013년 10월말 현재 42회) 발송하고 있으며 국가사이버침해 이벤트(3.20, 6.25 사이버테러 등)시 별도 보고서 발행하고 있다. 주요 배포처로는 정부, 공공기관, 정보보호업체 및 민간 정보보안 전문가 약 250여명 이다.

기대효과로는 페이지 비정상 정보 탐지시스템(SIMon)의 안정화 및 고도화 연구 개발과 SIMon 실시간 모니터링 대상 인터넷 홈페이지(도메인)의 규모/범위를 확대한다. 또한, SIMon 기술이전과 제품화를 통해 국내 정보보호산업 진흥에 기여하며 청와대, 국정원, KISA 등 핵심 기관에 주간 악성코드동향분석보고서 발송으로 국가 사이버안보 기여한다.

#### 2.1.2 능동형 통합보안시스템 (WebCure) 연구개발

인터넷주소 IP Filter(Version 5.1.2) 기능과 구조분석, 방화벽 엔진의 핵심기능 분석, Proxy 등의 부가기능 분석을 통해 최적화되고 안정적인 보안전용 운영체제(OS)가 탑재된 '능동형 통합보안 시스템' (WebCure) 연구 개발하였다.

연구 실적으로는 IP Filter(Version 5.1.2) 기능과 구조분석을 통해 리눅스 OS/URL(Uniform Resource Locator)

filtering 분석, 분석엔진/UI(User Interface) 개발하고 SIMon 및 F/W(Firmware) 연동, 내부 웹 서버 검사, 로그(log) 관리 등을 개발하였다.

기대효과로는 능동형 통합보안 시스템(WebCure) 설계 및 기술 개발로 솔루션에 대한 기능, 성능, UI 테스트를 통한 제품화를 연구하고 WebCure 기술 이전과 제품화를 통한 국내 정보보호 산업 진흥 및 국가사이버 안보 강화에 기여한다.

#### 2.1.3 사이버보안 정책연구 및 전문 인력 양성

국가 사이버 안보를 위한 공공정책의 효과적 수립을 위한 지원과 사이버보안 및 정보보호 관련 고급 전문 인력을 양성하기 위한 교육·훈련 프로그램 개발하였다.

연구개발 실적으로는 국가 사이버안보 콘트롤타워 역할 및 조직화 관련 공공정책 건의(기고 및 정책 관계자 인터뷰)하였고 한국인터넷거버넌스협의체(KIGA) 운영 지원과 사이버보안거버넌스분과(WG) 구성 및 활동 주관하였다. 또한, 행정기관, 정보통신 기반, 금융기관의 정보보호 직무담당자에 대한 교육·훈련 실시(약 450명)하였고 KAIST 정보보호대학원 석·박사 고급 전문 인력 배출을 위한 지원(석사 20명, 박사 5명) 하였다. 그리고 사이버보안/정보보호 분야 국제표준, 국가기술기준 등 중·고급자 보안교육 교재(5종)를 개발하였다.

기대효과로는 국가 사이버안보 공공정책 참여기회 확대 및 주요 안건에 대한 지속적 제언과 미래창조과학부/KISA 후원 국내·외 사이버보안 거버넌스 활성화를 위한 선도적이며 주도적인 활동을 한다. 이와 관련하여 UN 산하의 WFTP 2014 세계전기통신/ICT정책포럼(스위스 제네바) 한국대표단 참여 및 한국인터넷거버넌스협의회 운영위원회(8회), 사이버보안거버넌스분과위원회 구성 및 주관(2회) 한다. 추후 사이버보안연구센터 내 '사이버보안교육아카데미' 운영을 계획 중이다.

### 2.2 2012년 주요 사업실적

#### 2.2.1 고급인력 양성

석·박사 과정 운영 및 인력양성, 커리큘럼 개발, S+ 컨버전스 AMP 최고경영자과정 운영 및 교재를 개발하였다.

실적으로는 인재양성을 위해 박사과정 9명과 석사과정 25명을 지원하였고 각종 교과과정 개발과 S+ 컨버전스 AMP 최고경영자과정으로 121명을 배출하였다. 또한, 사이버공격방어 실습교재 1종 "해킹의 비밀을 푸는 KEY15" 교재를 개발하였다.

기대 효과는 석사 5명을 배출하고 사이버보안 실무에 대한 능력을 향상시킨다.

#### 2.2.2 우수교수 초빙

정보(사이버)보안 실무가 가능한 전문 교수 인력을 확보하였다.

채용을 위한 최종 심사를 완료하여 '2013년 전반기 채용하였다. 일부 겸임교수에 대한 전임 교수로의 전환운용('2013년) 하였다.

기대효과로는 우수 교수 초빙으로 인한 정보보호대학원의 실무교육이 강화되었다.

#### 2.2.3 보안 분석 인프라 구축

인적 인프라 구축 및 분석, 서비스 강화를 위한 보고서, 책자를 발간하였다.

실적으로는 악성 코드 분석실 정상 운영 및 상시 분석인력 운용과 '주간 악성 코드 동향 분석 보고서' 연 52회, '연간 백서' 1회 발간하였다. 악성코드 분석체계 및 Explore DB 등록하였고, 논문으로 국제 7건(SCI 2건), 국내 7건으로 총 14편을 작성하였다. 또한, 각종 보고서를 발간(분석, 기술, 정책보고서 156건 작성)하였다.

기대 효과로는 악성코드 분석 보고서를 정부, 공공기관 및 관련기업 등에 배포하였고 Exploit-db 4건 게재, 1,000건 이상의 해외기관 다운로드를 통해 한국의 위상을 제고하였다.

## 3. 주요 업무추진 방향

### 3.1 사업 목적

국가 사이버안보 강국 실현을 위해, KAIST 소속 사이버보안연구센터는 공익성(公益性), 공공성(公共性)을 갖는 "글로벌 사이버보안 정책, 신기술 연구개발, 고급 교육.훈련" 전문기관으로 성장 발전하고자 한다.

정부출연 기관고유 연구사업은 정부, 공공, 군(軍), 민간(産業)이 갖는 제한적 여건을 극복하여 범(凡)국가적, 비(非)영리적, 중장기적, 고도화된 "사이버보안 및 정보보호 이슈" 연구개발을 수행하고자 한다.

### 3.2 사업의 필요성

2013년 발생한 정부/방송사/금융사에 대한 해킹사고는 국

내 인터넷 및 사이버공간에 전면적 사이버테러로 국가 경제, 사회, 행정, 매스컴에 치명적인 장애와 국민생활의 불편을 초래하였다.

사이버 테러는 단순한 해킹차원이 아니라 국가 사이버영토의 안보를 심각하게 위협하는 사이버전쟁, 사이버범죄로 더욱 고도화되고 지능화되어 정부, 민간, 학·연이 협력하는 범국가적 대응과 상설 모니터링 체계가 요구되고 있다.

### 3.2 사업 내용

#### 3.2.1 사이버보안 정책 연구

국가 사이버안보 전략 및 거버넌스 공공정책 연구와 국내, 국제 사이버보안 및 정보보호 관련 대외협력 및 교류를 통한 사이버보안을 연구한다.

#### 3.2.2 사이버보안 기반기술 연구 및 정보서비스

지능형 악성코드/해킹 징후탐지, 분석, 대응기술「SIMon」엔진 고도화와 글로벌 웹페이지(도메인) 확보 및 유포지/배포지 실시간 탐지 범위를 확대한다. 또한,「글로벌 악성코드(Malware) 동향 분석 보고서」발간 및 전파한다.

#### 3.2.3 사이버보안 솔루션 개발 및 산업화

네트워크 필터링을 통한 능동적 통합보안 시스템「WebCure」개발하고 웹 취약점/비정상 행위 탐지를 통한 보안 관리정보 솔루션 개발한다. 또한, 연구개발 솔루션의 민간, 산업체 기술이전 및 제품화를 연구한다.

#### 3.2.4 학술 및 R&D 목적의「허니넷(HoneyNet)」조성

사이버공격 유도와 감시를 통한 최신 해킹기법 예측 및 대응 연구를 진행하고 실효적 사이버보안 교육·훈련을 위한 기술 구현 및 가상 실습장을 구축 한다. 또한, 다변화 형태, 국가사회기반(영역)별 위협/취약점 테스트 베드를 구축 및 운영한다.

#### 3.2.5 사이버보안 고급인재 육성

「KAIST 정보보호대학원」지원을 통한 정보보호 고급인력 양성하고 국제표준/국가기술기준 특화된 중·고급 교육를 위한「사이버보안 아카데미」구축한다. 또한, 행정, 공공, 금융, 국방, 정보통신, 산업기반 보안전문가 대상의 직무교육을 실시한다.

### 3.3 기대효과 및 향후 계획 내용

차세대 사이버보안 신기술 개발 및 운용을 통한 국가사회 기반시설(전력, 통신, 교통, 방송, 원자력, 금융, 국방 등) 보호와 사이버 테러에 대한 선제적 대응 체계 구축

세계적 수준의 사이버보안 전문 인력 양성을 통한 국가 사이버보안 대응능력을 확보한다.

## III. 결론

KAIST 사이보안연구센터는 사이버공간에 유포되는 각종 악성코드를 신속하게 탐지, 차단하는 엔진(SIMon)을 자체 개발(특허 출원)하였으며, 이를 통해 300여 주요 국가기관 및 전문가들에게 주간동향보고서를 전파하고 있다.

또한 나날이 새롭게 나타나는 신·변종 악성코드 유형을 실시간 분석하여 웹 취약성, 악성코드 유포지를 탐지하고 예측하는 '지능형 선제적 사이버보안 종합 관제 체계'를 구축하고 있다.

KAIST 정보보호대학원과 함께 석·박사 고급 인재를 양성하고 있으며, 행정공무원 및 정보통신 기반시설 보안 담당자를 대상으로 한 사이버보안과 정보보호 교육을 정규 과정으로 실시함으로, 실시간 사이버 현장에서 겪는 침해사고 대응기술과 체험적인 대처 스킬(skill)들을 신속하게 전수하고 있다.

이러한 노력 가운데 안전행정부의 정부통합전산센터, 국방부의 사이버사령부, 청와대, 국가정보원 등 중요 국가기관의 요청과 검증을 통해, 저희 센터가 보유한 사이버보안의 핵심인 '악성코드 탐지 및 예측', '웹 취약점 분석 및 조치' 기술을 지원하고 있으며, 한국인터넷진흥원을 비롯한 산·학·연 협업적 공동 연구개발을 수행하고 있다.

지난 3년간 축적된 기술력과 노하우를 기반으로, 더욱 적극적이고 비중 높은 '국가 사이버안보 강화'에 기여하고, 글로벌한 사이버보안 신기술의 연구개발을 위해 한층 더 업그레이드된 '사이버보안 전문 연구기관'으로 성장 발전하는 기관이 되고자 노력하려 한다.

## 저자소개

박 재 경

1994: 동국대학교
컴퓨터공학과 공학사
1996: 홍익대학교
전자계산학과 이학석사.
2002: 홍익대학교
전자계산학과 이학박사
현 재: 학국과학기술원
사이버보안연구센터
책임연구원
관심분야: 네트워크 보안,
사이버 보안
Email: wildcur@kaist.ac.kr