# 5. 개발 일정 및 역할 분담

## 5.1 개발 일정

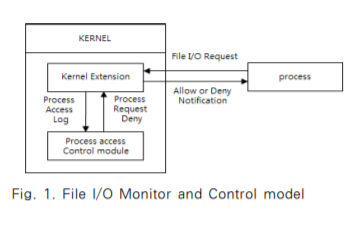
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5월 | | | 6월 | | | | | | 7월 | | | | | | | 8월 | | | | | | | | 9월 | | | | |
| 3주 | 4주 | 5주 | 1주 | 2주 | 3주 | 4주 | 5주 | | 1주 | | 2주 | | 3주 | 4주 | 5주 | 1주 | 2주 | | 3주 | 4주 | | 5주 | | 1주 | 2주 | 3주 | 4주 | 5주 |
| 관련 기술 공부 | | |  |  |  |  |  | |  | |  | |  |  |  |  |  | |  |  | |  | |  |  |  |  |  |
|  |  | 1. 분석용 가상환경 생성 | | |  |  |  | |  | |  | |  |  |  |  |  | |  |  | |  | |  |  |  |  |  |
|  |  | 2. 파일 I/O 모니터링 및 제어 모델 생성 | | | | | |  | |  | |  |  |  |  |  |  | |  |  | |  | |  |  |  |  |  |
|  |  |  |  | 2.파일 접근정보 송수신 모델 | | | | | | | | |  |  |  |  |  | |  |  | |  | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  | |  | | 중간 보고서 | | |  |  | |  |  | |  | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  | |  | |  |  |  | 3. 이상징후 탐지 모델 | | | | | |  | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  | |  | |  |  |  |  | 시스템 정확도 개선 및 추가기능 구현 | | | | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | |  | |  | |  |  |  |  |  |  | | |  | | 테스트 및 디버깅 | | | |  |  |
|  |  |  |  |  |  |  |  | |  | |  | |  |  |  |  |  | |  |  | |  | |  | 최종 발표/보고서 준비 | | | |

## 분석용 가상환경 생성 및 랜섬웨어 분석

* Sandbox, Emulator 혹은 Virtual Machine을 통해 샘플 랜섬웨어를 실행하고 분석할 수 있는 환경을 조성한다.

## 커널을 이용한 파일 I/O 모니터링 및 제어 모델(Monitor)

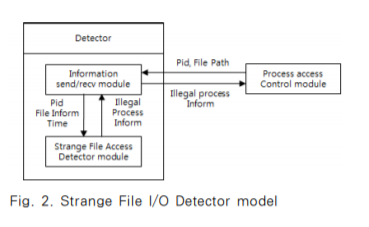
* 파일 I/O 모니터링 및 제어 모델 생성
* 파일 접근정보 송수신 모델



[그림 4]

## 비정상적 파일접근 탐지 모델(Detector)

* 파일 접근 정보 수신 및 파일 접근 명령 송신 모델
* 이상징후 탐지 모델



[그림 5]