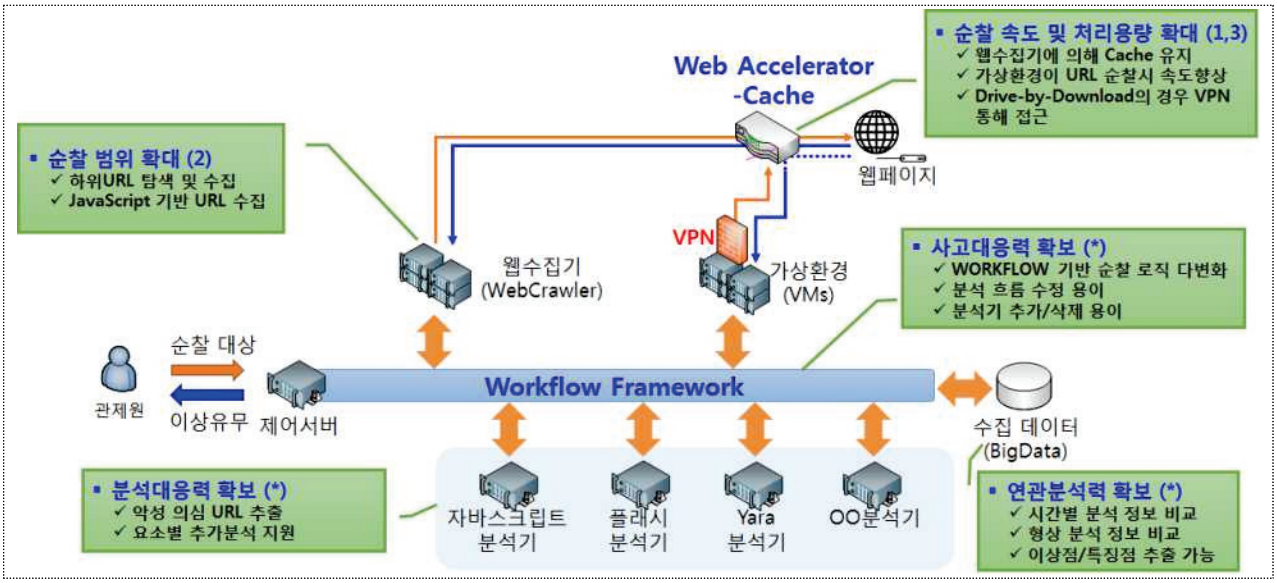
# 다중 분석기반 웹 악성코드 탐지 기술

| 기술키워드 | 웹 악성코드 탐지, 분석 Workflow | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 지식재산권 | 출원 1건 예정(대한민국) | | | | | | | | |
| 기술완성도 (TRL) | 기초 실험 | 개념 정립 | 기능 및 개념검증 | 연구실환경 테스트 | 시제품 제작 | 시제품 성능평가 | **시제품 신뢰성평가** | 시제품 인증 | 상용품 |

## 기술개요

- 다중 분석기반 웹 악성코드 탐지 기술
  - 웹리소스 수집, 자바스크립트 분석, Yara 분석 등 여러 기술들을 종합적으로 활용하여 입력된 Workflow에 따라 분석을 수행하고 분석된 내용을 종합 판단하여 웹 악성코드를 탐지하는 기술
  - 웹리소스 수집 속도, 분석 성능, 공격자에 대한 시스템 은닉성을 확보하기 위한 선택적 VPN 네트워크 라우팅 및 웹 리소스 캐싱 구조 적용

- 기술 구성도




## 기술성

- 독창성
  - 복합적인 분석기술을 활용하고 분석기술 및 로직 변경이 용이하여 운용성이 높고 캐싱과 VPN을 활용하여 성능과 시스템 은닉성을 확보함
- 범용성
  - 본 기술은 웹 악성코드 탐지 및 웹 서비스 보안 유지를 필요로 하는 곳에 범용적으로 적용가능
- 보안성
  - 지속적으로 변화하는 웹 공격에 신속한 대응을 위하여 Workflow, 분석 연동기술 적용

## 시장성

- 웹 악성코드 공격의 고도화 및 타겟형 공격의 증가
  - 웹 악성코드는 공격자에 의해 침투단계에서 지속적으로 사용되고 있음
  - 하위 URL이나 특정 그룹이 접속하는 페이지에 악성코드를 삽입, 난독화를 통하여 탐지를 우회함
  - 국내는 ActiveX, Non-ActiveX 등 웹 플러그인 형태의 소프트웨어를 이용한 공격 발생 증가
- 변화하는 웹 공격에 대한 탐지 필요성과 빠른 대응속도가 요구됨
  - 웹 서비스를 제공하는 기업의 웹 보안 유지를 위하여 활용될 수 있을 것으로 예상
  - 웹 악성코드 탐지 서비스를 제공하는 보안기업에 활용될 수 있을 것으로 예상

## 기술 응용 분야

- 웹 페이지에 삽입된 악성코드를 클라이언트 측에서 검출하기 위한 기관·기업
- 변화하는 웹 악성코드에 빠른 대응·탐지가 필요한 조직

## 기술개발 완료시기

- 2017년 12월 완료

## 관련 특허 등 지식재산권

- (국내 출원 예정) "(가칭) 다중 분석기반 웹 악성코드 탐지 장치"