ATC 기술 변경 요약

1 기술변경의 배경 및 목적

IT 보안 서비스 환경은 매년 급격하게 변화하고 있다. 환경이 변하는 만큼 시장에서 요구하는 항목들도 함께 변화하며, 이런 변화에 맞춰 기술도 지속적으로 진화해야 한다. 지난 1단계(1~2차년) 및 3차년도에 연구 개발한 VMI 및 SecaaS 프레임워크는 여전히 혁신적이지만 시장에 출시될 시점과 현재 상황을 종합해 봤을 때, 추가적으로 보완할 수 있는 시스템의 연구 개발이 필요하다. 즉, 이미 클라우드 업무 환경이 도입되어 있는 잠재적 고객들도 도입할 수 있는 기술을 기획하여 기 연구 개발한 항목과 긍정적인 효과를 낼 수 있도록 하였다.

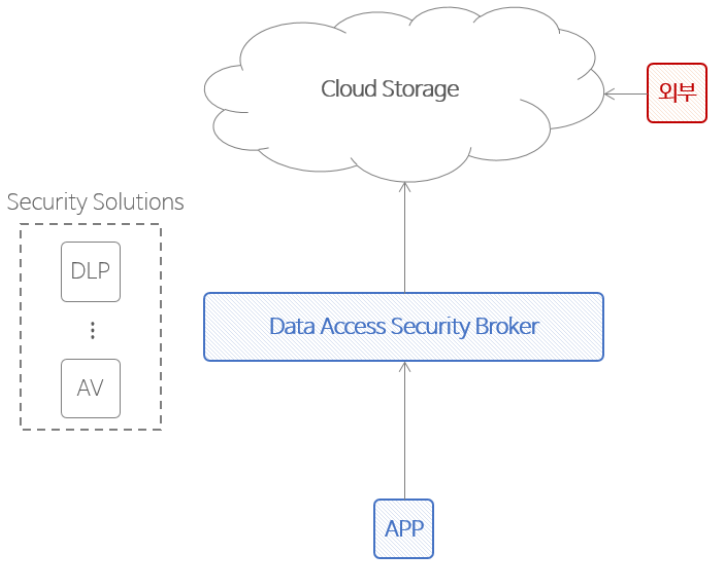
다음과 같은 네 가지 사유로 인해 기술 변경이 필요하다.

기업의 다양한 기존 환경과 연동되는 유연성

"모바일 보안 플랫폼"은 어떠한 클라우드 스토리지 환경과도 연동이 가능하며, 기업이 기존에 사용하던 보안 솔루션과의 연동을 통해 외부로 공유되는 파일에 대한 보안 검사, 그리고 스토리지로 유입되는 신규 파일에 대한 최소한의 안전성을 확보할 수 있다.

구글 드라이브(Google Drive), 마이크로소프트의 원 드라이브(One Drive), 드롭박스(Drop Box) 등과 같은 스토리지 서비스와의 연동 개발은 물론 표준 보안 브로커 API 및 프로토콜 개발을 통해 기존 Private 스토리지와의 연동도 가능하게 할 예정이다. 이미 다양한 보안 솔루션과 클라우드 혹은 On-premise 스토리지 서비스를 사용하고 있는 고객들이 새로운 모바일 보안 솔루션 도입을 위해 전체 시스템을 재 구축하는 비용을 절감할 수 있고, 기존의 환경을 최대한 활용하여 높은 투자 대비 수익률(ROI)을 실현할 수 있다.

또한 보안 브로커는 기 연구개발한 SecaaS에서 더욱더 발전된 형태로 다양한 보안 서비스를 연동하여 사용이 가능하며, 이를 통해 신규 보안 솔루션의 도입에도 적은 투자비용으로 모바일 보안 비즈니스 플랫폼 서비스와 연동이 가능하다.



[그림 1] 외부에서 클라우드 스토리지에 접속하는 위협

클라우드 스토리지 내의 모든 데이터는 암호화되어 있으며, 보안 비즈니스 플랫폼에서 제공하는 보안 브로커와 앱을 통하지 않으면 스토리지의 파일을 복호화 할 수 없다. 이에 외부에서 웹이나 기타 앱을 통해 데이터를 유출이 되더라도 파일을 복호화 할 수 없으므로 이러한 위협에서 안전하다.

글로벌 시장 진출의 용이성

모바일 보안 비즈니스 플랫폼은 다양한 환경에서 구동이 가능하게 개발할 예정이지만 1차적인 목표는 AWS(Amazon Web Service) 위에서 동작하도록 개발할 예정이다. AWS는 세계에서 가장 규모가 큰 클라우드 서비스 제공 플랫폼이며, 글로벌 시장 진출 시 많은 이점이 있다.

국내 AWS 위에서 개발된 모바일 보안 플랫폼을 타 국가 AWS에 이전하여 서비스를 하는데 매우 적은 금액 투자로 가능하다. 즉, AWS가 지원하는 다양한 국가에 빠르게 인프라를 구축하여 출시 시기(Time to Market)를 놓치지 않고, 진출할 수 있는 장점이 있다.

기존 연구개발 품목은 Private 클라우드 기반으로 개발되어 신규 개발 기술에 비해서는 해외 진출에 있어서 더 많은 시간이 걸린다. 이에 신규 개발 플랫폼을 우선 AWS에서 개발 및 글로벌 시장 진출을 하고, 그 경험을 바탕으로 3차년도 개발 결과물인 VMI 및 SecaaS 프레임워크의 글로벌 시장 진출을 전략적으로 할 수 있다.

정량적 목표의 조기 달성

정량적 목표로 계획되었던 항목들 중 많은 항목들이 조기에 목표를 달성하였다. 이에 따라 기존 플랫폼의 경우 시장 진출 시에 고객의 요구에 맞게 개선해 나갈 예정이다. 단점인 Private 클라우드 기반(자체 플랫폼)의 약점을 보완하는 모바일 보안 플랫폼으로 기술을 개발하여 본 과제를 통해 개발한 두 항목 간의 부족한 부분을 서로 채울 수 있을 것으로 판단된다.

자체 플랫폼이 단점만은 아니지만 국내 경기가 좋지 않은 현재 성장하고 있는 글로벌 시장 진출을 위해 4~5차년도 개발 기술의 변경이 필요하다. 또한 VMI 및 SecaaS 플랫폼의 한계점을 극복 및 보완하여 글로벌 시장을 적극적으로 개척해 나갈 예정이다.

수익 모델의 다각화

메신저에 대한 감청 등으로 인해 보안이 강화된 메신저로 이동하는 사태가 있었다. 이를 통해 B2C 모델에서도 보안에 대한 인식의 변화가 있었으며, 개인 사용자들의 의식도 조금씩 변화되고 있다. 이에 기존에 B2B 모델만을 대상으로 하던 서비스에서 본 기술로 변경함으로써 B2C에 대한 수익모델도 전략적으로 고려하고 있다.

B2C 모델에서 반드시 상용화를 하지 않더라도, 많은 고객에게 공개하고 서비스 함으로써 과제를 통해 개발되는 플랫폼에 대한 홍보 및 보안에 대한 이미지 제고 등을 통해 부가적인 전략을 세울 수 있다.

이에 다양한 시장 공략이 가능하며 기존의 환경과도 유연하게 연동 및 활용이 가능하고, 글로벌 시장 진출을 위한 모바일 보안 비즈니스 플랫폼으로의 기술 변경이 필요하다.

본 기술 변경은 기존 플랫폼의 약점을 보완하고, 다양한 플랫폼과 서비스들을 연동할 수 있는 진보된 기술을 개발함으로써 기존 기술 대비 뛰어난 확장성과 사용자에게 높은 편의성 및 안정성, 보안성을 제공할 수 있다.

2 개발 항목 변경 내용

2.1 2단계 2차년도

개발항목	구분	주체	비고
불법변조, 비인가 조작 시도 탐지 기술	삭제	주관기관	- 네이티브 앱은 사용할 수 있는 플랫폼을 제한하게 됨 이제 모든 플랫폼에서 사용할 수 있도록 개발하여 본 항목 삭제
업무 전용 Android Image 개발	삭제	주관기관	- 내/외부 공유 보안, 유출 방지 등에 초점이 맞춰지면서 기술 개발의 필요성이 사라짐
Android 원격접속 기술 개발	삭제	주관기관	- VM에 접속하는 방식에서 실제 업무에 활용하는 파일에만 접근하는 방식으로 접근하여 개발 제외
모바일 DLP 기능 강화	변경	주관기관	- 요청 시만 결과를 리턴하는 응답형 DLP로 기술 변경 - 응답형 DLP 개발 항목으로 기술 변경
Android VM의 보안강화를 위한 Sandbox 위변조 탐지기술	변경	참여기관	- VM이 아닌 실 단말기에서 URL 등을 통해 악성 APK에 감염되는 것을 방지하는 형태로 보안을 강화하여 기술 변경
파일 외부 반출 보안 기능 강화	변경	참여기관	- 외부로 반출되는 파일에만 보안을 강화하던 기술에서 내/외부 공유(반출)에 대해 모두 통제하는 기술로 변경
보안 브로커 플랫폼 프로토타입	추가	주관기관	- 스토리지, 보안 서비스 및 보안 공유 플랫폼 연동 관리, 사용자 관리, 모바일 앱 보안 등을 관리하는 클라우드 기반 플랫폼
보안 파일 공유 플랫폼	추가	주관기관	- 문서 및 파일의 내/외부 공유에 대한 보안 강화 플랫폼 - 공유 레벨, 대상 설정 등으로 공유 등을 제한 할 수 있음
스토리지 파일 자체 암호화 기술	추가	주관기관	- 퍼블릭, 프라이빗 클라우드 스토리지에 저장되는 데이터를 서비스 제공자가 제공하는 암호화가 아닌 자체적 키로 암호화
파일관리 기술 및 문서뷰어	추가	주관기관	- 테넌트 사용자들이 클라우드 스토리지의 파일을 관리할 수 있도록 인터페이스 개발
파일 암호화 및 키 관리 연구	추가	참여기관	- 스토리지 데이터의 자체 암호화 시, 테넌트의 사용자 별로 다른 키를 이용하여 암호화하고 그 키를 관리하는 기술 연구
암호화 파일 검색 연구	추가	참여기관	- 암호화된 파일을 검색할 수 있는 효과적인 방안 연구 - 4차년도 참여기관에서 연구 후, 5차년도에 주관기관에서 구현
응답형 DLP	추가	주관기관	- 보안 브로커 플랫폼의 요청에 의해 기존 패킷 단위로 처리하던 DLP를 파일 단위로 처리하는 응답형 기술로 변경
스토리지 표준 API 프레임워크 연구	추가	참여기관	- 다양한 스토리지 서비스를 연동할 수 있는 표준 API 프레임워크를 연구하고, 5차년도에 주관기관에서 구현

2.2 2단계 3차년도

개발항목	구분	주체	비고
불법변조 탐지 기술 지원영역 확대	삭제	주관기관	- 네이티브 앱은 사용할 수 있는 플랫폼을 제한하게 됨 이제 모든 플랫폼에서 사용할 수 있도록 개발하여 본 항목 삭제
업무 전용 Android Image 개발	삭제	주관기관	- 안드로이드 VM 이미지의 개발이 많이 진행되었고, VM 이용 환경이 아닌 다양한 환경에 적용 가능한 기술로 변경
Android 원격접속 기술 개발	삭제	주관기관	- 스토리지 보안 브로커 플랫폼 중심으로 기술이 변경되면서 원격접속 기술 지원영역 확대 기술 없이 보안 강화 가능
모바일 DLP 기능 강화	삭제	주관기관	- 요청 시만 결과를 리턴하는 응답형 DLP로 기술 변경

			- 응답형 DLP 개발 항목으로 기술 변경
SecaaS 플랫폼 고도화 및 통합 작업	변경	참여기관	- SecaaS 플랫폼을 보안 브로커 플랫폼이 흡수하여 더 폭 넓고 다양한 환경에 적용 가능하도록 기술 개발 예정
Android VM의 보안강화를 위한 Sandbox 위변조 탐지기술	변경	참여기관	- VM이 아닌 실 단말기에서 URL 등을 통해 악성 APK에 감염되는 것을 방지하는 형태로 보안을 강화하여 기술 변경
보안 브로커 플랫폼 고도화	추가	주관기관	- MQTT 기술 적용으로 비동기 방식 처리를 통한 퍼포먼스 증대 시키고, 스토리지 데이터 암호화 통합 구현 등
스토리지 파일 자체 암호화 기술 고도화	추가	주관기관	- 4차년도에 연구된 사용자 별 암호화 키로 개별 암호화하고 키를 관리하는 기술 적용하여 개발
보안 파일 공유 플랫폼 고도화	추가	주관기관	- OTP(임시 비밀키), 공유를 위한 URL 취약성 제거, 공유 결재 시스템 등 전체적인 플랫폼 고도화
파일 관리 기술 및 문서 뷰어	추가	주관기관	- 테넌트 사용자들이 클라우드 스토리지의 파일을 관리할 수 있도록 인터페이스 개발 고도화
응답형 DLP	추가	주관기관	- 보안 브로커와 정책 등을 통합 구현하여 브로커 관리 콘솔에서 응답형 DLP 정책 등을 설정할 수 있도록 기술 개발

3 변경 전, 후의 비교

○ Low, ◐ Normal, ● High, X None

구분	변경 전	변경 후	비고
단말기 자원 소모	○	○	- 클라우드 상에서 중요 정보 보안 및 기타 보안 기능이 구현되어 있어 단말기 자원 소모가 매우 적음
지원 플랫폼의 수	○	●	- 웹 기반 포털을 제공하여 브라우저가 실행되는 거의 모든 플랫폼에서 동작 가능
분실 대비 보안성	●	●	- 중요 자료들은 클라우드 상에 저장되며 단말기 내 중요자료가 존재하지 않으므로 분실로 인한 보안 문제 원천 차단
단말기 내 중요 파일	X	X	- 중요 자료들은 클라우드 상에 저장되어 단말기 내 중요자료가 존재하지 않으므로 정보유출 원천 차단
보안 파일 공유 플랫폼	X	●	- Android VM의 도입으로 단말기 플랫폼, 버전 등에 관한 종속성이 낮아짐
서비스 연동 난이도	●	○	- 표준 API 프레임워크 등을 제공하여 클라우드 스토리지, 보안 서비스 등과 연동이 기존에 비해 구현하기가 쉬움
고객의 서비스 도입 난이도	●	○	- 고객이 기존 사용하던 클라우드 환경에도 손 쉽게 적용이 가능한 플랫폼으로 도입 난이도가 낮음
해외 서비스 난이도	●	○	- 우선 AWS 기반으로 기술을 개발하여 현지화 기간 및 서비스 배포 등이 해외 서비스 난이도가 기존에 비해 월등히 낮음
수익 모델의 다양성	○	●	- B2B, B2C 등 SaaS 형태 서비스, On-premise 등 다양한 수익(비즈니스) 모델 등 매우 다양한 수익 모델 적용 가능

ATC 기술 변경 상세

1 변경 전, 후의 설계 구성 비교

1.1 변경 전 설계 구성

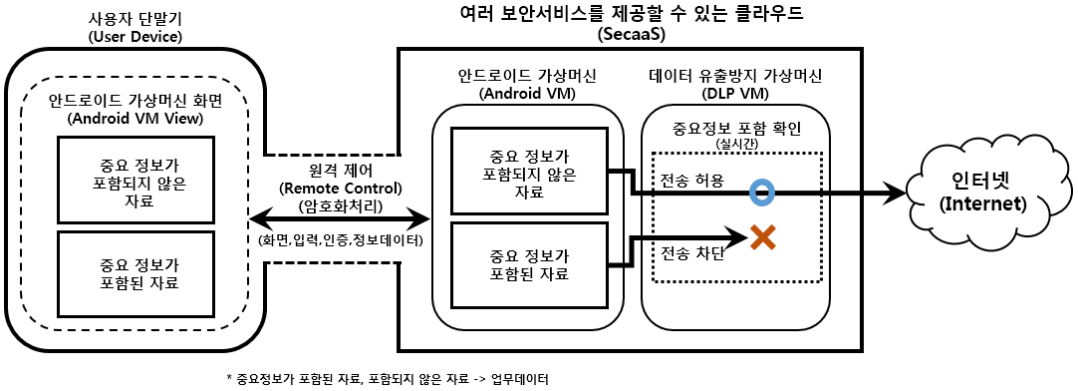


그림 2. 변경 전 구조

- SecaaS에 추가적으로 Android VM이 올라가게 되어 해당 VM을 업무영역으로써 사용하게 되고 중요자료가 저장될 수 있다.
- 사용자 단말기에서는 해당 Android VM을 원격제어 할 수 있으며 SecaaS와는 화면, 입력, 인증 단말 정보데이터만 주고받는다.
- 사용자 단말기에서 Android VM을 원격 제어하여 외부로 중요자료를 전송하려 할 시에 DLP VM에서 중요정보 포함여부를 실시간 적으로 검사하여 차단 또는 허용을 하게 된다.
- 사용자 단말기에는 어떠한 중요자료(업무데이터)도 저장 혹은 전송되지 않기에 어떠한 제한도 가하지 않는다.

변경 전의 경우에는 SecaaS 상에 DLP VM과 RAVM(원격 안드로이드 가상머신)도 같이 올라가게 된다. 해당 RAVM을 업무영역으로써 사용하고, 사용자 단말기는 개인영역으로 사용하는데 사용자 단말기에서 특정 앱 실행을 통해 SecaaS 상의 RAVM을 화면으로 원격 제어하게 된다. 단말기와 SecaaS 간에는 원격제어를 위한 정보들만 오갈 뿐, 중요파일이나 정보는 송수신되지 않게 된다. 또한, 실시간 적으로 고성능의 DLP 검사를 수행할 수 있다.

1.2 변경 후 설계 구성

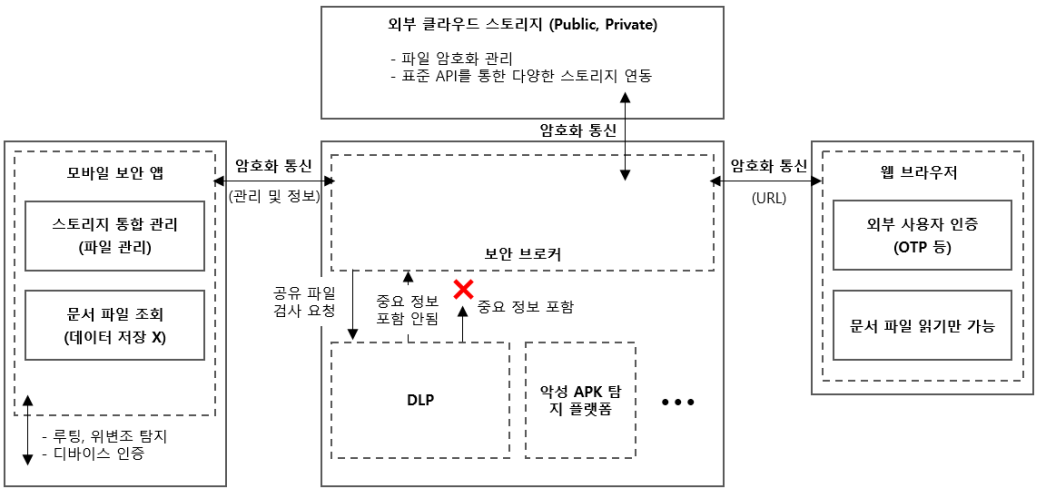


그림 3. 변경 후 구조

- 서비스 이용자는 보안 브로커를 통해 기존 클라우드 스토리지에 중요 자료를 저장할 수 있다. 보안 브로커를 통해 저장되는 모든 데이터는 서비스 이용자의 고유 암호화 키로 암호화 된다.
- 서비스 이용자는 웹 브라우저 혹은 모바일 앱을 통해 사용자 인증 등 보안 과정을 거쳐 서비스에 접속할 수 있다. 단말에서 접속하는 URL을 통해 설치되는 APK의 악성 여부를 점검하여 악성일 경우 알림을 제공하고, 서비스 이용을 제한할 수 있다.
- 단말에서 문서, 이미지 등을 확인할 경우 실 데이터는 클라우드 내에 안전하게 존재하고, 스트리밍 데이터만 표시되며 어떠한 정보도 단말에 저장되지 않는다.
- 문서를 공유하기 위해 사용자는 보안 공유 서비스를 이용할 수 있으며, 공유 레벨에 따라서 공유 받는 사람이 문서를 읽을 수만 있도록 할 수 있다.
- 또한 공유 시 테넌트 보안 관리자가 설정한 보안 서비스 정책에 따라 DLP로 공유 되는 데이터가 중요자료를 포함하고 있는지 점검하여 허용 혹은 차단할 수 있다.
- 서비스 이용자들은 다양한 스토리지를 보안 브로커에 등록하여 하나의 관리 앱 혹은 웹에서 쉽게 파일을 관리하고 공유할 수 있다.

보안 브로커를 포함하는 모든 서비스 플랫폼은 AWS 상에서 구현되고 동작하게 된다. 중요 파일이나 정보는 송수신되어 단말에 저장되지 않으며, 외부 사용자에게 공유 시에도 읽기 전용 모드를 제공하여 원본 중요 자료의 유출을 방지한다. 클라우드 스토리지에 저장되는 데이터는 모두 서비스를 이용하는 사용자의 개별 암호화 키로 암호화 되므로 클라우드 서비스 제공자 혹은 악의적 공격자에 의해 유출되더라도 안전하다. 또한 사용하는 다양한 클라우드 스토리지를 하나의 화면에서 관리할 수 있어 편의성 및 접근성을 극대화 하였으며, 자체 파일 암호화, 공유 보안과 읽기 전용 모드를 통해 높은 보안성을 제공할 수 있다.

2 개발 항목 변경 내용 상세

2.1 변경 항목

2.1.1 Android VM의 보안강화를 위한 Sandbox 위변조 탐지 기술 개발

개발항목	단계	년차	연구/개발 기술
클라우드 기반 악성 URL 분석 시스템	2	2	클라우드 환경에 분석 플랫폼 개발
		2	온라인 분석 서비스를 이용한 악성 URL 분석 기술
클라우드 기반 악성 APK 분석 시스템	2	2	클라우드 환경에 분석 플랫폼 개발
		2	악성 APK 정적 분석 기술
		2	악성 APK 동적 분석 기술
악성 URL 및 APK 분석 에이전트	2	3	악성 URL 및 APK 분석 에이전트 (안드로이드)
			SMS URL 크롤링 기술
			클라우드 분석 시스템 인터페이스

기술 대상이 VM에서 실 모바일 단말 및 클라우드 스토리지 보안으로 개선되면서 악성 APK를 탐지하는 기술의 명칭을 변경하였다. 또한 실 단말의 SMS, 메신저 등을 통해서 유통되는 URL 내에 포함된 APK를 감지하여 악성 여부를 판단하는 전체적인 분석 시스템을 세분화하여 개발 범위를 넓혔다. 악성 URL 및 APK 분석 시스템은 사용자의 에이전트로부터 얻어온 URL 정보와 APK 파일을 클라우드 시스템에 전송함으로서 시작된다. URL은 악성 URL 분석 시스템을 거쳐 온라인 분석 서비스를 사용해 분석을 하며, APK 파일은 악성 APK 분석 시스템을 거쳐 정적 분석과 동적 분석을 통해 결과를 리포트 형식으로 에이전트에 전달하여 사용자에게 해당 URL과 APK의 위험도를 알려줌으로서 보다 안전하게 사용할 수 있다.

2.1.2 파일 외부 반출 시스템

개발항목	단계	년차	연구/개발 기술
보안 파일 공유 플랫폼 프로토타입	2	2	URL 기반의 파일 공유 기술 및 인증 기술 개발
			공유 레벨 기술 개발: 완전 공유(반출, 다운로드), 읽기 전용 등
			공유 제한 기술 개발: URL 접근 횟수 및 기한 등 제한으로 URL 파기
			공유 결재 시스템 프로토타입 개발
보안 파일 공유 플랫폼 고도화		3	URL 기반 공유 보안 강화: OTP(임시 비밀키) 적용을 통한 인증
			URL 취약성 제거: 디렉토리 트레버셜, XSS 등
			공유 결재 시스템 개발
			알람 푸시 서버 기술 개발

파일 반출 시스템은 기존 업무영역에서 외부로 반출되는 파일에 대해 승인결재를 통해 완전 반출을 허용하는 시스템이다. 즉, 관리자가 파일의 내용을 보고 해당 파일의 반출 여부를 결정한다. 이 개발항목은 '2.3 추가항목' 중 '보안 파일 공유 플랫폼'에 통합하여 개발을 진행한다. 보안 파일 공유 플랫폼은 내외부 공유뿐만 아니라 외부 파일 반출에도 레벨을 설정하여 읽기만 가능하도록 할 수 있으며, 관리자의 결재 판단을 돕기 위해 공유/반출 요청 파일에 대한 DLP를 수행할 수 있다. 보안 파일 공유 플랫폼은 서비스 사용자가 내부 외부로 안전하게 파일을 공유 할 수 있도록 보안 URL, 인증 기술 등 다양한 보안 기술이 포함되어 있다. 또한 공유 시 관리자의 결재를 통해서 안전하게 반출 할 수 있다.

2.1.3 모바일 DLP 기능 강화

개발항목	단계	년차	연구/개발 기술
모바일 DLP	2	2	상세 정책 기반 선별적 패킷 우회 처리 기술 개발

			페이로드 정합성 판단 및 후처리 기술 개발
		3	프로토콜 분석 후처리 기술 고도화

2단계 1차년도까지 개발한 DLP 기술은 네트워크 패킷 기반 기술이었다. 이번 기술 변경에서 패킷 기반이 아닌 파일 기반의 응답형 DLP로 기술을 변경하였다. 응답형 DLP는 실제 내/외부 공유 및 파일 반출 시에 DLP를 체크함으로써 DLP가 사용하는 리소스의 양을 최소화 하여 유지 운영 비용을 절감할 수 있으며, 퍼포먼스 측면에서도 유리하다.

2.2 삭제 항목

2.2.1 업무 전용 Android Image 개발

개발항목	단계	년차	연구/개발 기술
Android Image	2	2	화면 워터마킹 기술 개발
			앱 사용시간 제어 등 MAM 기능 강화
		3	상위 버전을 지원하는 업무전용 Android Image 개발

2단계 1차년도까지 Adroid Image 개발이 매우 빠르게 수행되었고, 그 성과 또한 목표치들을 달성했다. 또한 기술 변경을 통해 가상 업무 영역 접속이 아닌 보안 브로커 접속을 통한 다양한 보안 서비스와 클라우드 스토리지를 사용할 수 있도록 되면서 Android Image 개발은 본 연구과제 개발항목에서 제외한다.

2.2.2 Android 원격접속 기술 개발

개발항목	단계	년차	연구/개발 기술
원격접속 기술	2	2	디바이스 화면 크기에 따른 적응적 화면 변경 기술 개발
		3	iOS 등으로 원격접속 기술 지원영역 확대

원격접속 기술 중 적응적 화면 변경 기술은 2단계 1차년에도 완료하였으며, iOS 등으로 원격 접속 기술 지원영역을 확대하는 것은 업무 전용 Android Image 개발과 마찬가지로 기술 변경으로 ATC 과제 외 영역에서 별도로 개발을 진행할 예정이다. 이에 본 과제의 개발항목에서 제외한다.

2.3 추가 항목

2.3.1 보안 브로커 플랫폼

개발항목	단계	년차	연구/개발 기술
보안 브로커 플랫폼 프로토타입	2	2	클라우드 스토리지 관리 기술 개발: AWS S3 대상
			다양한 보안 서비스 연동 및 관리 기술 개발
			보안 플랫폼 관리 콘솔 개발: 사용자, 정책 및 설정 관리 등
			모바일 인증 처리 프레임워크 등 백 엔드 기술 개발
			스토리지 표준 API 프레임워크 연구
보안 브로커 플랫폼 고도화		3	클라우드 스토리지 관리 기술 개발: 표준 API 프레임워크 (구글, 드롭박스 등)
			메시지 기반 처리 MQTT 기술 개발
			보안 플랫폼 관리 콘솔 개발: 대시보드 및 로그 추적, 고급 설정 등
			파일 암호화 기술 및 검색 플랫폼 구현 및 통합

보안 브로커 플랫폼은 SecaaS 프레임워크의 고도화된 버전으로 클라우드에서 동작한다. 또한 다른 클라우드 스토리지 서비스와 보안 서비스들과의 폭 넓은 연동이 가능하여 확장성 및 유연성이 매우 뛰어나다. 일반적으로 클라우드 스토리지를 사용할 때 자료 유출에 대한 위험을 자체 파일 암호화 기술로 보안을 강화하였으며, 다수의 클라우드를 관리할 수 있는 콘솔을 통해 통합 관리가 가능하다.

2.3.2 스토리지 파일 자체 암호화 기술

개발항목	단계	년차	연구/개발 기술
파일 암호화 기술	2	2	테넌트별 암호화 키 관리 기술 개발
			테넌트별 스토리지 파일 암호화 구현
암호화 기술 연구			파일 암호화 및 키 관리 연구
			암호화 파일 검색 연구
파일 암호화 기술 고도화		3	테넌트의 사용자별 암호화 키 관리
			테넌트의 사용자별 스토리지 파일 암호화 구현

클라우드에 저장되는 데이터의 안정성을 위해 서비스 프로바이더가 제공하는 암호화가 아닌 본 서비스에서 자체적으로 암호화하여 보안성을 높였다. 3차년도에는 각각의 사용자 별로 저장 데이터를 암호화를 하여 더욱 높은 보안성을 제공한다.

2.3.3 파일 관리 앱 및 문서 뷰어

개발항목	단계	년차	연구/개발 기술
파일 관리 기술 및 문서 뷰어	2	2	스토리지 파일 관리 기술 (모바일)
			문서 뷰어 연동
파일 관리 앱 확장 및 파일 관리 웹		3	스토리지 파일 관리 웹 포털
			워터마크 기술

안드로이드와 아이폰에서 클라우드 스토리지를 안전하게 관리할 수 있는 인터페이스를 제공한다. 또한 플랫폼에 영향을 받지 않는 웹 기반의 클라우드 스토리지 파일 관리 포털 기술을 개발한다.

2.3.4 응답형 DLP

개발항목	단계	년차	연구/개발 기술
DLP	2	2	패킷 처리 기반 DLP 기술을 파일 처리 기반 기술로 변경 개발
		3	보안 브로커와 정책 및 응답 공유를 위한 기술 개발

패킷 처리 기반의 DLP 기술을 파일 처리 기반으로 변경하여 개발하고, 이를 보안 브로커 서비스와 연동하여 파일의 내/외부 공유 시에 중요 정보 유무를 검사하여 차단 여부를 결정한다.

3 최종 개발 항목

3.1 주관기관

변경 전				변경 후			
개발항목	**단계**	**년차**	**연구/개발 기술**	**개발항목**	**단계**	**년차**	**연구/개발 기술**
모바일 장치 불법 변조 및 비인가 조작 방어 기술	2	2	불법변조, 비인가 조작 시도 탐지 중앙관리 기술 개발	사용자가 어떤 플랫폼에서나 서비스를 사용할 수 있도록 함. 이에 서비스 지원 대상에 많은 제약을 주는 네이티브 앱 개발 관련 항목은 삭제			
		3	개발기술 지원 영역 확대				
업무 전용 Android Image 개발	2	2	화면 워터마킹 기술 개발	업무 영역 VM 서비스를 클라우드 보안 브로커를 직접 서비스 방식으로 변경하여 "업무 전용 Android Image 개발" 공정 삭제			
		2	앱 사용시간 제어 등 MAM 기능 강화				
		3	상위 버전을 지원하는 업무전용 Android Image 개발				
Android 원격접속 기술 개발	2	2	적응적 화면 변경 기술 개발	업무 영역 VM 서비스를 클라우드 보안 브로커를 직접 서비스 방식으로 변경하여 "Android 원격접속 기술 개발" 공정 삭제			
		3	iOS 등으로 원격접속 기술 지원 영역 확대				
모바일 DLP 기능 강화	2	2	상세 정책 기반 선별적 패킷 우회 처리 기술 개발	**응답형 DLP**	2	2	패킷 처리 기반 기술을 파일 처리 기반으로 변경 개발
		2	페이로드 정합성 판단 및 후처리 기술 개발			3	보안 브로커와 정책 및 응답 공유를 위한 기술 개발
		3	프로토콜 분석 후처리 기술 고도화				
파일 외부 반출 시스템	2	2	보안 기능 강화	**보안 파일 공유 플랫폼**	2	2	URL 기반의 파일 공유 기술 및 인증 기술 개발
		3	서비스 고도화			2	공유 레벨 기술 개발: 완전 공유 (반출, 다운로드), 읽기 전용 등
						2	공유 제한 기술 개발: 접근 횟수 및 기한 등 제한으로 URL 파기
						2	공유 결재 시스템 프로토타입 개발
						3	URL 기반 공유 보안 강화: OTP (임시 비밀키) 적용을 통한 인증
						3	URL 취약성 제거: 디렉토리 트레버셜, XSS 등
						3	공유 결재 시스템 개발
						3	알람 푸시 서버 기술 개발
신규 추가 항목으로 변경 전 개발 항목에 없음				**보안 브로커 플랫폼**	2	2	클라우드 스토리지 관리 기술 개발: AWS S3 대상

			2	다양한 보안 서비스 연동 및 관리 기술 개발
			2	보안 플랫폼 관리 콘솔 개발: 사용자, 정책 및 설정 관리 등
			2	모바일 인증 처리 프레임워크 등 백 엔드 기술 개발
			3	클라우드 스토리지 관리 기술 개발: 표준 API 프레임워크 (구글, 드롭박스 등)
			3	메시지 기반 처리 MQTT 기술 개발
			3	보안 플랫폼 관리 콘솔 개발: 대시보드, 로그 추적, 고급 설정 등
			3	파일 암호화 기술 및 검색 플랫폼 구현 및 통합
신규 추가 항목으로 변경 전 개발 항목에 없음	**스토리지 파일 자체 암호화 기술**	2	2	테넌트별 암호화 키 관리 기술 개발
			2	테넌트별 스토리지 파일 암호화 구현
			3	테넌트의 사용자별 암호화 키 관리
			3	테넌트의 사용자별 스토리지 파일 암호화 구현
신규 추가 항목으로 변경 전 개발 항목에 없음	**파일 관리 기술 및 문서 뷰어**	2	2	스토리지 파일 관리 기술(모바일)
			2	문서 뷰어 연동
			3	스토리지 파일 관리 웹 포털
			3	워터마크 기술

3.2 참여기관

변경 전				변경 후			
개발항목	단계	년차	연구/개발 기술	개발항목	단계	년차	연구/개발 기술
Android VM의 보안강화를 위한 Sandbox 위 변조 탐지 기술 개발	2	2	Android VM 커널 변조 탐지 기능	**클라우드 기반 악성 URL 분석 시스템 개발**	2	2	클라우드 환경에 시스템 개발
		2	APP 크롤링 기능			2	온라인 분석 서비스를 이용한 악성 URL 분석 모듈 개발
		2	상태 정보 전송 APP 개발	**클라우드 기반 악성 APK 분석 시스템 개발**	2	2	클라우드 환경에 시스템 개발
		2	악성 URL, 변조 APK 확인 기능			2	악성 APK 정적 분석 모듈 개발
						2	악성 APK 동적 분석 모듈 개발
				악성 URL 및 APK 분석 에이전트	2	3	악성 URL 및 APK 분석 에이전트 (안드로이드)
						3	SMS URL 크롤링 기술 고도화
						3	분석 플랫폼과의 인터페이스 모듈 개발
신규 추가 항목으로 변경 전 개발 항목에 없음				**암호화 기술 연구**	2	2	사용자별 파일 암호화 및 키 관리 연구
						2	암호화 파일 검색 연구
						2	스토리지 표준 API 프레임워크 연구

4 기술 변경으로 인한 특장점

① 클라우드 스토리지의 보안성 극대화

클라우드 스토리지의 계정이 해킹 당하거나 스토리지 자체가 공격 당했을 때, 중요 데이터가 유출될 수 있다. 본 서비스를 통해서 보안 브로커를 통해 클라우드 스토리지를 관리할 경우 모든 데이터가 자체적인 암호화 기술과 사용자 개별적인 암호화 키를 통해 암호화 되어 높은 보안성을 제공한다. 계정 등 악의적인 공격으로 파일이 유출되더라도 복호화 할 수 없어 중요 자료의 유출이 최소화된다.

② 안전한 파일 내/외부 공유를 통한 자료유출방지

보다 안전한 파일 공유 플랫폼을 제공하고, URL로 유통시킴으로써 편의성 또한 높였다. 사용자는 내/외부에 자료를 공유할 경우 공유 기간 등 제한 조건을 설정할 수 있으며, 특정 대상에게만 공유가 가능하다. 또한 공유 상대방이 URL을 통해 접속할 경우 임시 발급 비밀키 등으로 인증 과정을 거치고, 다운로드 등이 불가능하도록 읽기 전용모드를 통해 자료 유출을 방지한다. 또한 공유 시에 워터마크 기능을 통해 카메라를 통한 유출 등 물리적인 대한 위협도 낮췄다. 또한 기본적으로 BYOD 단말에는 어떠한 정보도 남기지 않는다.

③ BYOD 플랫폼에 영향 받지 않는 업무 효율성

기본적으로 안드로이드와 아이폰을 지원하지만, 웹 기반 서비스도 제공하여 브라우저가 있는 환경이면 높은 보안의 클라우드 스토리지 관리 서비스를 이용할 수 있다. 어떤 플랫폼에서건 파일을 공유하고 관리할 수 있어 업무의 효율성을 높였다.

④ 다양한 스토리지의 통합 관리로 효율성 극대화

AWS 스토리지, 구글 드라이브, 드롭박스 등 지원되는 스토리지 서비스를 지속적으로 늘려감으로써 사용자는 여러 클라우드 스토리지를 하나의 화면에서 하나의 스토리지처럼 매우 쉽게 관리할 수 있다.

⑤ 다양한 보안 서비스 연동으로 보안성 강화

기본적으로 DLP 보안 서비스를 제공하여 자료유출에 대한 방지 기능을 제공하고, 악성 URL 및 APK 분석/탐지 보안 서비스를 통해 모바일 단말을 보다 안전하게 관리할 수 있다. 또한 표준 API 프레임워크의 제공으로 APT 솔루션 등 다양한 보안 서비스를 연동하여 높은 확장성을 제공하며, 이를 통해 보안을 강화할 수 있다.

⑥ 손쉬운 서비스 가입 및 사용에 따른 높은 접근성

프라이빗 환경에 구축하는 On-premise가 아닌 퍼블릭 클라우드에서 쉬운 가입을 통해 바로 서비스를 이용할 수 있으므로 기존의 구축 환경보다 매우 높은 접근성을 제공한다.

⑦ 다양한 비즈니스 모델을 통한 수익 창출의 기회 확대

기본적으로 서비스 대상을 B2B, B2C 모두로 확장할 수 있으며, 장기적으로 퍼블릭 서비스와 On-premise 등으로 다양한 구축 형태를 지원한다. 또한 각 요소 기술들에 대한 타사의 서비스와 연동을 통한 비즈니스 모델도 기대할 수 있다.

⑧ 해외 진출을 위한 준비 리소스 최소화

전 세계에서 서비스하고 있는 AWS 기반에서 운영되어 언어 지원과 현지화 작업 후, 바로 서비스가 가능하다. 엔지니어링, 고객지원 등의 서비스를 위해 현지에 직접 파견하지 않고도 AWS 상에서 지원이 가능하다. 이 외에도 해외에 인프라 구축이 불필요 한 점 등 해외 진출을 위한 리소스를 최소화하고, 전통적인 방식에 비해 쉽게 진출할 수 있다.