

## 퍼블릭 클라우드 서비스 이대로 좋은가

### 아마존 S3 & 드롭박스 들여다보기

시장조사기관인 IDG의 최근 조사결과 IT 인프라 시스템의 45% 이상이

클라우드로 시스템 환경을 전환했다고 한다. 그 중 퍼블릭 클라우드 서비스는

비용 절감과 쉽고 빠른 서비스 이용 등의 이점을 내세워 확산되는 추세다.

하지만 퍼블릭 클라우드가 기업의 IT 인프라 시스템으로 자리를 잡기엔 넘어야 할 산이 여전히 높다.

한국에서도 사용자가 많은 아마존 S3와 드롭박스 서비스가 안고 있는 과제를 알아보자.



### 빈번한 데이터 유출 사고 ‘보안 구멍 크다’

지난 한 해 동안 온라인에 접속된 아마존 S3(Amazon Simple Storage Service) 버킷<sup>1)</sup>을 통한 데이터 유출 사건이 끊이지 않았으며 이로 인해 수많은 기업의 고객 정보가 노출됐다. 액센추어, 부즈 알렌 해밀튼, 다운존스, 타임워너, 텔사, TSA, 베리존, 미국 국가지리정보국 등 굴지의 기업과 기관이 피해를 입었으며, 수익 건에 달하는 개인 정보가 외부에 그대로 공개됐다.

어떻게 이런 일이 가능했을까? 아마존 S3의 구조에서 단서를 찾을 수 있다. 사용자가 아마존 S3 클라우드 스토리지 버킷을 생성하면, 웹의 어디서나 데이터를 저장하고 검색할 수 있다. 데이터 유출의 대부분은 기업들이 퍼블릭 액세스가 허용된 상태의 아마존 S3 버킷 설정을 그대로 두었을 때 발생한다. 즉, S3 버킷이라는 명칭만 붙어 있으면 누구라도 인터넷에서 해당 콘텐츠에 접속해 다운로드할 수 있다는 말이다.

보안업체 스카이하이 네트워크스(Skyhigh Networks)에 따르면 전체 S3 버킷의 7%는 퍼블릭 액세스에 대해 아무런 제약이 없으며, 35%는 암호화되어 있지 않다고 한다. 이는 아마존 S3 에코시스템에서 가장 큰 문제이기도 하다. 상황을 더욱 악화시키는 것은 구멍 난 AWS 데이터셋을 살살이 뒤질 수 있는 툴이 웹에 널려 있다는 점이다. 노출 상태에 있는 S3 버킷을 찾아 내기가 그만큼 더 수월하다는 얘기다. 일례로, 버크해커(BuckHacker)는 노출된 S3 버킷을 가장 간편하게 검색할 수 있도록 해주는 검색엔진 툴이다.

#### 데이터 암호화가 능사는 아니다

암호화가 S3 데이터 침해를 예방하는 하나의 방법이 될 수도 있지만 실질적으로는 그렇지 못하다. 사람들은 데이터가 암호화되어 있으면 해당 데이터가 순식간에 유출되는 일은 일어나지 않을 것이라고 생각한다. 하지만 가장 간편하게 도입할 수 있는 암호화 접근 방법인 SSE(Server Side Encryption)만 해도 아마존 S3의 오픈 버킷 문제를 해결하지 못한다. 물론 SSE가 탑재된 아마존 S3는 사용자의 데이터가 데이터센터에 저장되기 전에 암호화를 수행한다. 하지만 데이터가 다운로드 되는 순간 자동으로 암호화가 해제된다. 따라서 암호화된 오픈 버킷 데이터가 암호화 상태로 저장된다 하더라도 일반 텍스트로 액세스가 가능하다는 얘기다.

Hitachi Content Platform(이하 HCP)과 같은 클라이언트를 통해 데이터를 암호화한 후 아마존 S3에 업로드하는 경우라면 얘기가 다르다. 클라이언트 측면에서 암호화가 보호받을 수 있기 때문이다. 이 경우 해당 클라이언트는 암호화 프로세스, 암호 키와 관련 톨 관리, 암호 키의 소유권을 유지한다. 또한 해당 버킷이 공개 상태로 전환된다 하더라도 콘텐츠의 암호화 상태는 그대로 유지된다.

#### HCP로 아마존 S3 버킷의 정보유출 완벽 차단

S3 데이터 유출을 방지하는 또 다른 방법은 HCP를 S3의 클라이언트로 동작하도록 하거나 하이브리드 접근 방식을 이용하는 것. HCP는 프라이빗 혹은 하이브리드 클라우드로 동작하도록 설계되어 있다. 퍼블릭 클라우드로 동작하는 시스템은 보편적인 수준의 보안 접근 방식을

1) 아마존 S3(Amazon Simple Storage Service) 버킷 : 아마존 웹 서비스에서 제공하는 온라인 스토리지 웹 서비스의 저장 공간





채용하므로 더 광범위한 공격에 노출될 수 있지만, 엔터프라이즈에 최적화 된 보안 방식을 적용할 수 있는 HCP에서는 이 리스크를 피해갈 수 있다. 시스템을 사내에서 직접 구동시키면 조직의 기밀 데이터가 돌발적으로 노출되는 리스크를 최소화할 수 있다. 이렇게 하면 유휴 데이터 및 실행 중인 데이터의 암호화 등 HCP가 제공하는 데이터 보호 서비스를 포함해 조직 내 방화벽, 접근 제어가 제공하는 보호까지도 활용할 수 있다. 물론 HCP의 모든 시큐리티 기능은 S3 버킷과 연동될 경우에도 여전히 유효하기 때문에, 아마존 S3 스토리지의 확장성과 저비용의 이점을 동시에 그대로 누릴 수 있다.

HCP가 있다면 만약 해커들이 아마존이 사용하는 물리 인프라로의 액세스를 시도한다 해도 문제없다. S3 클라이언트로 사내에 직접 설치되거나 하이브리드 클라우드 형태로 설치된 HCP가 데이터를 암호화해 해커들의 데이터 액세스를 차단하는 것이다.

또한 아마존은 퍼블릭 클라우드 서비스이기 때문에 NSL(National Security Letter)<sup>2)</sup> 혹은 데이터에 대한 기타 증거 보존 통지를 받을 가능성이 늘 존재한다. 이 경우 사용자는 자신의 파일을 다른 곳에 보관해야 하고, 파일을 이동 저장한 지점이 또 다른 공격에 노출될 수 있다. HCP는 기업 내 직접 설치하거나 하이브리드 접근방식을 통해 아마존 S3 서비스의 클라이언트 역할을 수행하므로 아마존 S3 버킷의 정보 유출 가능성을 차단하는 최선의 방안이 될 것이다.

출처 Plugging Leaky Amazon S3 Buckets, <https://community.hds.com>, 2018년 2월



## 기업이 Dropbox 이용을 꺼리는 이유 ‘4가지’

드롭박스(Dropbox)는 파일 동기화와 공유 툴 서비스로 엄청난 성공을 거두었다. ‘USB 드라이브의 불편함을 개선한다’는 단순한 목적에서 시작된 드롭박스 서비스는 2018년 2월 현재, 등록 회원 5억 명, 일일 동기화 파일 12억 개 이상이라는 놀랄만한 성과를 거두면서 시장에서 자리를 굳혔다. 이러한 성공을 기반으로 지난 3월 미국 나스닥(NASDAQ) 시장에 상장됐다.

그러나 이런 드롭박스에도 어려움이 하나 있다. 일반 사용자에서 기업 사용자로 ‘고객 기반을 어떻게 옮길 것인가’이다. 기업 고객의 증가는 엄청난 매출 증가로 연결된다. 이는 기업 시장을 꾸준히 노크해온 이유이며, 드롭박스 입장에서 반드시 풀어야 할 숙제다.

조금 더 기능적인 질문을 해보자. 기업이 과연 파일 관리와 공유를 위해 또 다른 기술 사일로(Silo)를 필요로 할까? 지난 2009년 애플이 드롭박스 인수를 추진할 때 스티브 잡스는 “드롭박스는 제품이 아니라 기능일 뿐”이라고 일축했다. 맞는 말이다. 이미 탄탄히 자리 잡은 IT 기업과 스타트업 중에서 동기화와 공유 비즈니스를 주 사업으로 하는 기업이 얼마나 많으며, 이들 서비스 간 차별성을 찾기로 또 얼마나 어려운 일인가? 드롭박스와 다른 유사 서비스 사례에서 볼 수 있듯 진정한 차별성은 타깃 고객이 일반 소비자인가 아니면 기업인가에 달려 있다.

2018년에는 기업들 사이에서 이 문제가 더 부각되기 시작했다. 많은 기업들이 다양한 형태의 클라우드 서비스를 앞다투어 도입하면서 파일 공유가 기업 전체의 데이터 관리 전략의 일부로 자리 잡았다. 기업들이 원치 않는 게 하나 있다면 추가적인 관리를 필요로 하는 또 다른 데이터 사일로일 것이다.

올 초 드롭박스 CEO 드류 휴스턴은 드롭박스에 저장된 파일을 기업 서버에도 저장하는 직원들에 대해 “말도 안 되는 일”이라고 잘라 말했다. 100% 옳은 말이다. 실제로 말도 안 되는 일이다. 이렇게 하면서 또 모든 파일의 복사본을 이메일, 콘텐츠 관리 시스템, 클라우드 스토리지 서비스, 웹사이트, 사용자 디바이스 등에 추가한다면 어떨까. 파일 복제, 백업, 아카이브로 인해 수만 개에 달하는 동일 파일의 복사본이 곳곳에 널려 있게 될 것이다.

### 데이터 제어

기업들은 데이터를 완벽하게 제어하고, 기존 시스템에 간단히 통합 및 보완되는 것을 원한다. 또 다른 관리가 필요한 데이터 사일로는 원하지도, 필요하지도 않지만 프라이버시와 보안은 강화하고 싶어 한다.

히타치 뱅타라(Hitachi Vantara)는 이 분야에서만큼은 충분한 전문성을 갖추고 있는 기업이다. 실제로 HCP는 고도의 유연성이 확보된 스토리지 시장에서 엔터프라이즈 파일에 대해 동기화와 공유 기능을 제공하는 몇 안 되는 솔루션 중 하나다. HCP Anywhere는 지난 3년 동안 100만 개의 기업 라이선스가 판매된 엔터프라이즈 파일 공유 솔루션이다.

2) NSL(National Security Letter) : 미국 연방수사국(FBI)이 기업에 사용자 정보를 요구할 때 법원 감독 없이 발행하는 비밀 서한으로, 안보상의 정당한 이유가 있을 경우 포털사이트, 서버 대여 기업이나 메일 서비스 업체 등으로 하여금 요구받은 자료 일체를 넘기도록 강제한다.

## 보안

드롭박스는 자사 서비스의 가장 큰 장점으로 보안 프로토콜을 내세우지만, 지난 몇 년 동안 드롭박스가 가장 골머리를 앓은 문제는 아마도 데이터 보안이 아닐까 싶다. 이미 퍼블릭 액세스가 가능하고, 고도의 가시성이 확보된 서비스라는 점에서 상당한 리스크를 안고 있다. 리걸 테크놀로지(Legal Technology)사 담당자는 “드롭박스는 앞으로도 계속 타깃이 될 것이고, 해커들이 얻을 수 있는 게 많은 만큼 늘 공격받게 될 것이다.”라고 강조했다.

보안과 사용의 편의성 부문이 서로 충돌을 일으키는 경우도 있다. 유휴 파일에 대해 암호화를 제공하면서도 동시에 특정 부분에서 취약하다는 점에 대해서는 드롭박스 스스로 인정하는 부분이다. 드롭박스 웹사이트에는 다음과 같은 문구가 있다.



파일 공유 툴이라면 그 종류가 무엇이든 보안 리스크에 민감할 수밖에 없다. 기업들이 정보 유출을 방지하기 위해 액세스, 가시성, 접근 제어 방안을 찾아나서는 이유다. 암호 키 관리는 기업의 핵심 요구사항이다. 드롭박스가 암호 키를 통제하는 한 드롭박스 내 파일에 대한 액세스 권한은 드롭박스가 갖고 있으며, 바로 이 지점에서 문제가 발생한다.

## 프라이버시

어떤 종류의 데이터 관리 전략이든 그 핵심은 데이터 통제다. ‘누가 어떤 데이터에 언제 액세스했냐’이다.

드롭박스가 스토리지 사용을 최적화하는 방법 중 하나는 사용자 전체에 대해 동일 파일의 중복을 제거하는 것이다. 수천 개에 달하는 동일한 파일을 드롭박스 인프라에 저장하지 않고, 한 번만 저장한 후 사용자가 개별 액세스할 수 있도록 한다. 많은 기업들이 스토리지 활용을 최적화하기 위해 이와 같은 기술을 사용하지만 드롭박스 같은 퍼블릭 클라우드 서비스라면 얘기가 달라진다. 프라이버시 부문에서는 취약성으로 돌변할 수 있기 때문이다. 저작권의 보호를 받는 콘텐츠를 저장하거나 공유할 생각이 없는 일반 사용자라면 문제가 되지 않을 수 있다. 그러나 기업 사용자라면 보안 및 프라이버시 정책면에서 문제가 될 수 있다.

## 유연성과 휴대성

기업이 중요하게 고려하는 또 다른 이슈 중 하나는 기업의 파일 동기화와 공유 데이터의 관리 방식이다. 프라이빗, 퍼블릭 및 하이브리드 클라우드가 발전하면서 유연성과 휴대성이 기업 데이터 전략 기획 수립의 핵심 이슈로 등장하기 시작했다. 앞서 언급한 것처럼 드롭박스의 파일 공유 툴은 일반적인 기업이 관리하는 데이터의 일부일 뿐이고, 기능적으로는 독립적인 관리가 필요한 또 다른 사일로드. 즉, 데이터 관리 자체가 또 다른 수준의 복잡성을 갖게 된다는 말이다.

이와 달리 HCP는 데이터가 사내에 저장될 뿐만 아니라, 하이브리드 클라우드로서 아마존, 구글, 마이크로소프트, S3 기반 서비스 등 다중 클라우드 서비스로 옮겨갈 수 있도록 한다. 유연성을 갖춘 중앙화된 콘텐츠 관리 서비스를 제공함으로써 비즈니스 요구사항과 예산의 변화에도 장기적인 데이터 관리 정책을 구현할 수 있게 된다.

궁극적으로 드롭박스의 모든 문제는 보안과 프라이버시를 포함해 데이터 제어, 데이터 관리 및 비용 통제에 관한 것이다. 그래서 또다시 기본 전제로 돌아갈 수밖에 없다. 드롭박스는 하나의 기능이지 솔루션이 아니다. 드롭박스는 실제로 일반 사용자에게는 환상적인 툴이지만 기업에게는 그다지 실용적이거나 합리적인 선택이 될 수 없다.

**출처** Reality check: Most enterprises aren't adopting Dropbox... and for good reasons, <https://community.hds.com>, 2018년 1월

