Dropbox Business 보안

Dropbox 백서

Dropbox

목차

서론

오늘날 30만 이상의 기업과 조직이 콘텐츠 제작 통합 플랫폼으로 Dropbox Business를 이용하며 협업과 공유를 원활하게 진행하고 있습니다. Dropbox Business는 단순히 사용하기 쉬운 협업 도구일 뿐 아니라, 모든 데이터를 안전하게 보호해줍니다. 이에 Dropbox는 계정 관리자에게 정책의 기본 토대를 제공하고 필요에 따라 맞춤형으로 활용할 수 있는 상세한 기본 안내서를 제작했습니다. 이 백서에는 팀원들이 Dropbox Business를 창의적인 에너지를 발산할 수 있는 안전한 도구로 이용할 수 있도록 관리자가 이용 가능한 선택 사항과 백엔드 정책이 자세하게 설명되어 있습니다.

또한, 이 백서에서는 팀원들이 간편하게 아이디어를 공유할 수 있는 협업 공간 'Dropbox Paper'(또는 'Paper')의 보안에 관한 내용도 살펴볼 수 있습니다. Paper는 웹과 모바일에서 모두 이용 가능하며, 팀원들은 Paper를 통해 프로젝트를 관리하고, 문서를 만들어 공유하고, 실시간으로 피드백을 교환할 수 있습니다.

별도의 설명이 있지 않는 한 이 백서에 기술된 정보는 모든 Dropbox Business 제품(Standard, Advanced, Enterprise)과 Dropbox Education에 적용됩니다. Paper는 Dropbox Business와 Dropbox Education에서 제공되는 기능입니다.

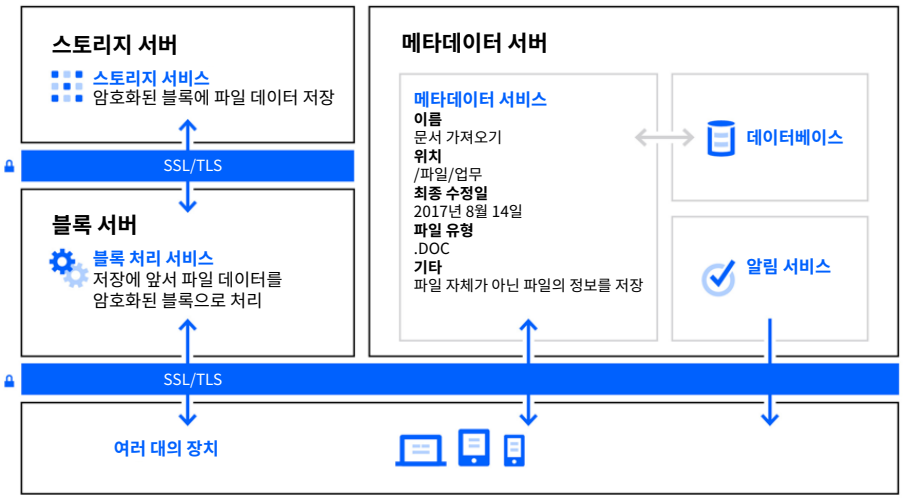
들여다보기

사용법이 간편한 Dropbox의 인터페이스는 이면에서 인프라스트럭처가 작동하며 빠르고 안정된 동기화, 공유, 협업 기능을 지원합니다. 이를 위해 Dropbox는 제품과 아키텍처를 지속적으로 향상해 데이터 전송 속도와 신뢰성을 높이고 끊임없는 IT 환경 변화에 대응하고 있습니다. 이 섹션에서는 데이터가 어떻게 전송되고, 저장되고, 안전하게 처리되는지 살펴볼 수 있습니다.

파일 인프라스트럭처

Dropbox 사용자는 데스크톱, 웹, 모바일 클라이언트 또는 Dropbox에 연동된 타사 애플리케이션을 통해 언제든지 파일과 폴더에 액세스할 수 있습니다. 모든 클라이언트는 안전한 서버에 연결되어 파일로의 액세스를 제공하고, 파일 공유 기능을 지원하며, 파일이 추가, 변경 또는 삭제됐을 때 연결된 장치를 업데이트해줍니다.

Dropbox의 파일 인프라스트럭처는 다음과 같이 구성되어 있습니다.



- **블록 서버**

  Dropbox는 기존의 암호화 기술의 한계를 넘어선 자체 보안 메커니즘으로 사용자들의 데이터를 보호합니다. 블록 서버는 Dropbox 애플리케이션에 있는 파일을 블록으로 나누어 암호화하고, 파일이 수정된 경우 변경된 블록만 동기화합니다. 새로운 파일이나 기존 파일에 변경 사항이 감지되면 애플리케이션이 블록 서버에 이를 통지하고, 블록 서버는 새롭게 생성되거나 변경된 파일 블록만 처리해 이를 스토리지 서버로 전송합니다. 이 서비스에 이용된 전송 중 데이터와 유휴 상태의 데이터 암호화에 관한 자세한 내용은 아래의 암호화 섹션에서 확인할 수 있습니다.

- **스토리지 서버**

  파일에 담긴 콘텐츠는 암호화된 블록으로 스토리지 서버에 저장됩니다. Dropbox 클라이언트는 파일 콘텐츠를 전송하기 전 파일을 블록으로 나누어 저장에 대비합니다. 스토리지 서버는 콘텐츠내용주소화기억장치(CAS) 역할을 하며 해시값을 기준으로 암호화된 파일 블록을 검색합니다.

- **메타데이터 서버**

  '메타데이터'로 불리는 사용자 데이터에 관한 기본 정보는 자체 스토리지 서비스에 개별적으로 보관되어 사용자 계정에 있는 모든 데이터의 지표 역할을 합니다. Dropbox 메타데이터는 데이터베이스 서비스에 저장되며, 필요에 따라 공유되고 복제되어 성능과 높은 가용성 요구사항을 충족합니다. 메타데이터에는 이메일 주소, 이름, 장치 이름 등 기본 계정과 사용자 정보에 관한 정보가 포함됩니다. 변경내용 기록, 복구, 동기화 등의 기능을 지원하는 파일 기본 정보(예: 파일 이름 및 유형)도 메타데이터에 포함됩니다.

- **알림 서비스**

  이 별도의 서비스는 Dropbox 계정에 변경 사항이 있는지를 감시하기 위한 것으로, 이 서비스에는 어떠한 파일이나 메타데이터도 저장되거나 전송되지 않습니다. 각 클라이언트는 롱 폴링 방식으로 알림 서비스에 연결되어 대기합니다. Dropbox 파일이 수정된 경우, 알림 서비스가 롱 폴링 연결을 종료해 관련 클라이언트에 변경 사항을 신호로 보냅니다. 연결이 종료된 후 클라이언트가 파일의 변경 사항을 동기화하려면 메타데이터 서버에 다시 연결되어야 합니다.

서로 다른 단계의 정보를 복수의 서비스에 분산하면 동기화 속도가 빨라지고, 안정성이 향상되며, 보안도 강화됩니다. 이러한 Dropbox 아키텍처의 기본적인 구조 덕분에 한 가지 서비스에 액세스해서는 파일을 재생성하는 것이 불가능합니다. 이 서비스에 이용된 암호화 종류에 관한 자세한 내용은 아래의 암호화 섹션에서 확인할 수 있습니다.

파일 데이터 저장

Dropbox는 기본적으로 파일 메타데이터(파일이 마지막으로 수정된 날짜와 시간 등)와 파일에 담긴 콘텐츠(파일 블록)의 2가지 데이터를 저장합니다. 파일 메타데이터는 Dropbox에 저장되고, 파일 블록은 Amazon Web Services(AWS)나 Magic Pocket 중 하나에 저장됩니다. Magic Pocket은 Dropbox의 내부 저장 시스템으로, 독점 소프트웨어와 하드웨어로 구성되어 있습니다. 이 시스템은 초기 단계에서부터 안정성과 보안을 염두에 두고 설계되었습니다. Magic Pocket과 AWS 모두 유휴 상태에서 파일 블록을 암호화하며, 높은 수준의 신뢰성 기준을 충족합니다. 더욱 자세한 내용은 아래의 신뢰성 섹션에서 확인할 수 있습니다.

파일 동기화

Dropbox는 업계가 인정하는 동종 최고의 파일 동기화 기능을 제공합니다. Dropbox의 동기화 방식은 파일의 빠르고 즉각적인 전송을 보장하며, 장소와 관계없이 모든 장치로 데이터에 액세스할 수 있습니다. Dropbox 동기화 기능은 회복력도 뛰어납니다. Dropbox 서비스로의 연결이 끊겼다가 복구된 경우, 클라이언트가 파일 전송을 자동으로 재개합니다. 파일이 완벽하게 동기화되거나 Dropbox 서비스의 인증을 받은 경우 파일은 로컬 클라이언트에만 업데이트됩니다. 데이터가 복수의 서버에 분산되어 저장되기 때문에 가외성이 보장되며 최종 사용자는 일관성 있는 동기화 기능을 경험할 수 있습니다.

- **델타 동기화**

  델타 동기화는 파일의 수정된 부분만 다운로드/업로드하는 동기화 방법입니다. Dropbox는 업로드된 파일을 암호화된 개별적인 블록에 저장한 후 변경 사항이 있는 블록만 업데이트합니다.

- **스트리밍 동기화**

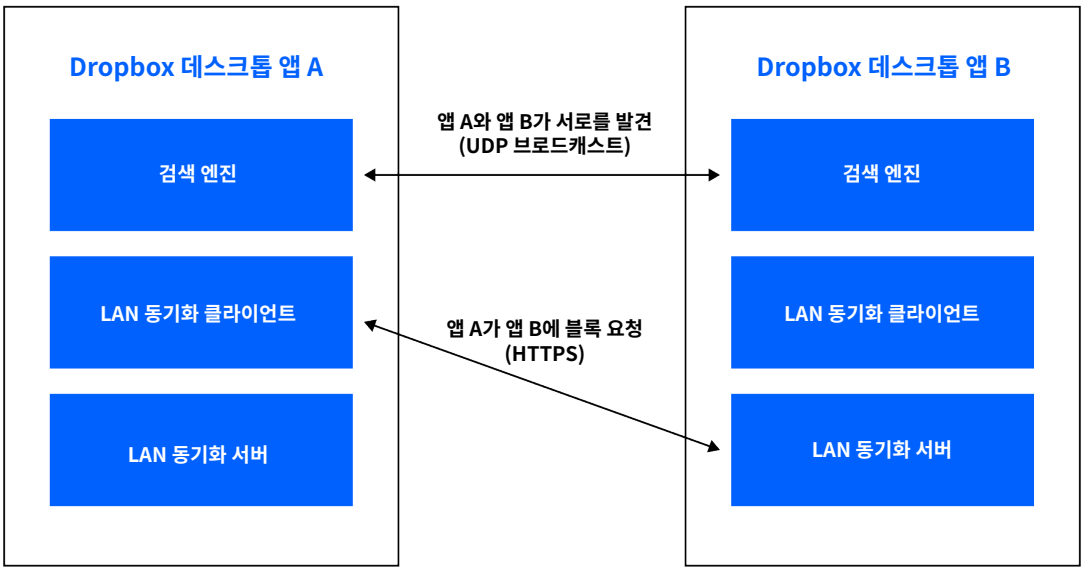
  스트리밍 동기화는 파일 업로드가 완료될 때까지 기다리지 않고 한쪽 장치에 모든 블록이 업로드되기 전에 다른 장치에 동기화된 블록의 다운로드를 시작하는 동기화 방법입니다. 동일한 Dropbox 계정에 컴퓨터 여러 대가 연결되어 있거나 여러 개의 계정이 한 개의 폴더를 공유할 경우 스트리밍 동기화가 자동으로 적용됩니다.

- LAN 동기화

  LAN 동기화가 활성화되면 동일한 근거리통신망(LAN)에 연결된 다른 컴퓨터의 신규 및 업데이트된 파일이 다운로드되기 시작합니다. 그 결과, Dropbox 서버에서 파일을 다운로드할 때보다 시간과 대역폭이 절약됩니다.

  아키텍처

  데스크톱 앱에서 실행되는 LAN 동기화 시스템은 검색 엔진과 서버, 클라이언트라는 3가지 주요 요소로 구성되어 있습니다. 검색 엔진은 네트워크에서 동기화할 컴퓨터를 검색하는 역할을 하며, 이때 동일한 개인용 또는 공유 Dropbox 폴더에 액세스가 허용된 컴퓨터만 검색 대상에 포함됩니다. 서버는 네트워크에 있는 다른 컴퓨터가 보낸 요청을 처리해 요청받은 파일 블록을 전송하고, 클라이언트는 네트워크에 파일 블록을 요청하는 역할을 합니다.



검색 엔진

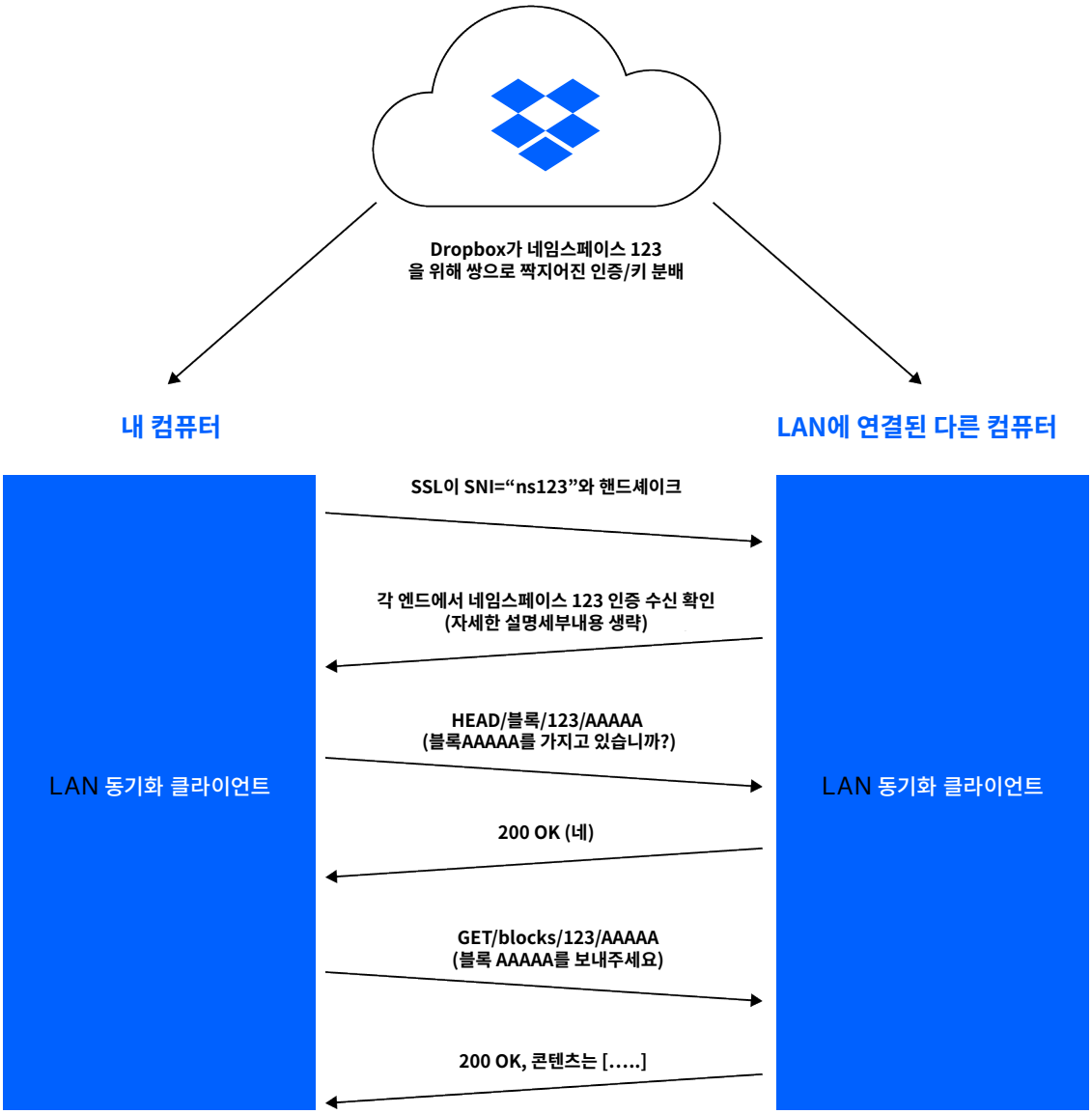
LAN에 연결된 각 컴퓨터는 LAN 동기화 전용 IANA인 포트 17500을 통해 주기적으로 UDP 동보 패킷을 송수신합니다. 동보 패킷에는 해당 컴퓨터의 프로토콜 버전과 지원되는 개인용 또는 공유 Dropbox 폴더, 서버 운영에 사용되는 TCP 포트(17500 포트가 지원되지 않을 경우 달라질 수 있음), 컴퓨터의 임의 식별자가 포함되어 있습니다. 패킷이 감지되면 컴퓨터의 IP 주소가 각 개인 또는 공유 폴더의 목록에 추가되며 잠재적인 타깃에 신호를 보냅니다.

프로토콜

실질적인 파일 블록은 HTTPS를 통해 전송됩니다. 각 컴퓨터는 엔드포인트로 HTTPS 서버를 작동합니다. 클라이언트는 복수의 피어에서 파일 블록의 존재 여부를 확인한 후 1개의 서버에서만 블록을 다운로드합니다.

Dropbox는 모든 데이터의 안전한 보관을 위해 해당 폴더의 인증을 받은 클라이언트만 파일 블록을 요청할 수 있게 합니다. 또한, Dropbox의 모든 개인용 또는 공유 폴더에 한 쌍의 SSL 키와 인증을 생성해 컴퓨터가 제어권이 없는 폴더의 서버 행세를 할 수 없게 합니다. 이러한 키와 인증은 Dropbox의 서버에서 폴더의 인증을 받은 컴퓨터로 분산되어 저장됩니다. 멤버십에 변화가 있을 때는(예: 공유 폴더에서 누군가가 삭제된 경우) 키와 인증이 순환 교대됩니다. Dropbox는 HTTPS에 연결된 양측이 동일한 인증서(Dropbox 또는 공유 폴더의 인증서)의 인증을 받도록 해 양측 모두가 인증을 받았다는 것을 증명합니다.

HTTPS에 연결할 때 Dropbox는 Server Name Indication(SNI)을 통해 서버에 어떤 개인용 Dropbox 또는 폴더가 연결을 시도 중인지 정보를 전송하며, 서버는 이 정보를 통해 어떤 인증서를 사용할 것인지 결정합니다.



서버/클라이언트

위에 설명된 프로토콜처럼 서버에는 사용 가능한 블록과 블록이 위치한 장소 정보가 필요합니다.

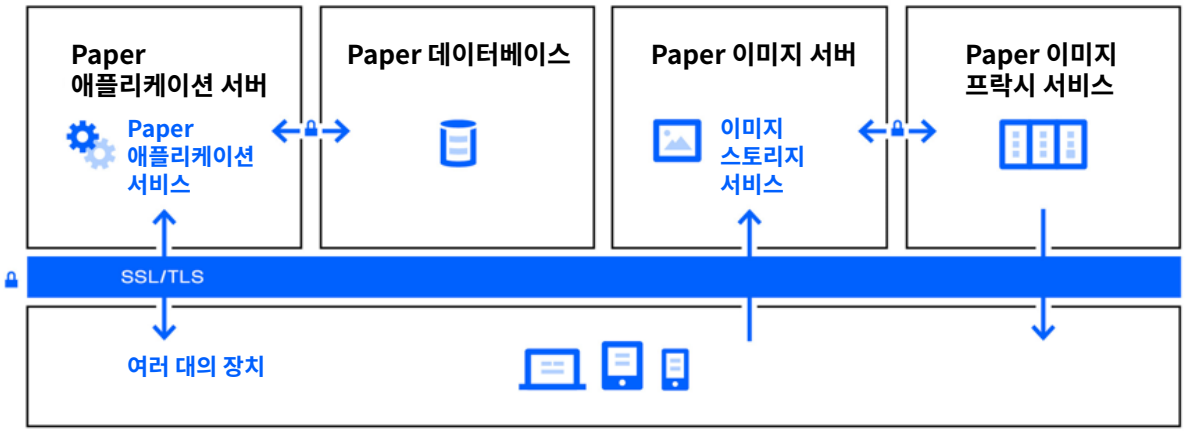
클라이언트는 검색 엔진의 검색 결과에 따라 각각의 개인용 Dropbox 폴더와 공유 폴더의 피어 목록을 보관합니다. LAN 동기화 시스템에 파일 블록 다운로드 요청이 전송되면 시스템은 해당 피어 목록에서 임의의 피어 샘플을 선택해 요청을 보내며, 블록을 보유한 피어 중 가장 먼저 응답한 피어에 블록을 요청합니다.

시간 지연을 막기 위해 Dropbox는 연결 풀을 통해 이미 시작된 연결을 다시 사용합니다. 필요할 때까지는 연결을 열지 않고, 연결을 연 후에는 다시 필요한 경우를 대비해 연결 상태를 유지합니다. 또한, 모든 피어에 연결할 수 있는 최대 허용치를 두어 그 수를 제한합니다.

파일 블록을 찾지 못했을 경우와 다운로드에 실패한 경우, 또는 연결이 너무 느린 경우에는 블록을 Dropbox 서버에서 다운로드합니다.

Paper 인프라스트럭처

Dropbox 사용자는 데스크톱, 웹, 모바일 클라이언트 또는 Dropbox Paper에 연결된 타사 애플리케이션을 통해 언제든지 Paper 문서에 액세스할 수 있습니다. 모든 클라이언트는 안전한 서버에 연결되어 Paper 문서에 액세스를 제공하고, 문서 공유 기능을 지원하며, 문서가 추가, 변경 또는 삭제됐을 때 연결된 장치를 업데이트합니다.



Dropbox Paper의 인프라스트럭처는 다음과 같이 구성되어 있습니다.

- **Paper 애플리케이션 서버**

  Paper 애플리케이션 서버는 사용자 요청을 처리하고, 수정된 Paper 문서의 변경 사항을 사용자에게 전송하며, 알림 서비스를 수행합니다. Paper 애플리케이션 서버가 사용자가 변경한 내용을 Paper 데이터베이스에 전송하면 변경 사항은 영구 저장소에 보관됩니다. Paper 애플리케이션 서버와 Paper 데이터베이스 간의 통신은 강력한 암호로 암호화됩니다.

- **Paper 데이터베이스**

  Paper 문서에 관한 특정한 메타데이터와 문서에 담긴 콘텐츠는 Paper 데이터베이스의 영구 저장소에서 암호화됩니다. 여기에는 Paper 댓글, 업무 등 문서에 담긴 콘텐츠뿐 아니라 제목, 문서를 공유한 회원, 권한, 폴더 연계 등 Paper 문서에 관한 정보가 포함됩니다. Paper 데이터베이스는 필요에 따라 공유되고 복제되어 성능과 높은 가용성 요구사항을 충족합니다.

- **Paper 이미지 서버**

  Paper 문서에 업로드된 이미지는 유휴 상태에서 Paper 이미지 서버에 저장되고 암호화됩니다. Paper 애플리케이션과 Paper 이미지 서버 간의 이미지 데이터 전송은 암호화된 세션을 통해 진행됩니다.

- **Paper 이미지 프락시 서비스**

  Paper 이미지 프락시 서비스는 Paper 문서에 업로드된 이미지와 임베딩된 하이퍼링크의 이미지 미리보기를 지원합니다. Paper 문서에 업로드된 이미지의 경우, Paper 이미지 프락시 서비스는 Paper 이미지 서버에 저장된 이미지 데이터를 암호화된 채널을 통해 불러옵니다. Paper 문서에 임베딩된 하이퍼링크의 경우, Paper 이미지 프락시 서비스는 원래의 링크에서 이미지 데이터를 불러와 소스 링크에 따라 HTTP 또는 HTTPS를 이용해 이미지 미리보기를 생성합니다.

Paper 문서 스토리지

Dropbox는 기본적으로 공유 권한 등 Paper 문서에 관한 정보와 사용자가 문서에 업로드한 콘텐츠를 저장합니다. 이러한 데이터는 통틀어 Paper 문서 데이터로 불리며, Paper 문서에 업로드된 이미지는 Paper 이미지 데이터로 불립니다. 각각의 문서 데이터와 이미지 데이터는 Amazon Web Services(AWS)에 저장되며, 유휴 상태에서 암호화됩니다. AWS는 높은 수준의 신뢰성 기준을 충족합니다. 더욱 자세한 내용은 아래의 신뢰성 섹션에서 확인할 수 있습니다.

신뢰성

스토리지 시스템은 신뢰할 수 있을 때만 그 가치를 발휘합니다. 이를 위해 Dropbox는 여러 단계의 중첩된 시스템으로 데이터 손실을 막고 가용성을 보장하도록 설계되었습니다.

파일 메타데이터

파일 메타데이터의 중복 사본은 기본적으로 N+2 가용성 모델의 데이터 센터 내부에 위치한 여러 개의 개별적인 장치에 분산되어 저장됩니다. 증분 백업은 1시간마다 수행되며, 전체 백업은 3일에 1번씩 수행됩니다. 메타데이터는 호스팅을 하는 서버에 저장된 후 미국 내 Dropbox에 의해 관리됩니다.

파일 블록

파일 블록의 중복 사본은 최소 2개의 서로 다른 지역에 독립적으로 저장되며 각 지역에서 안전하게 복제됩니다. (참고: 유럽 내 시설에 파일을 저장하도록 선택한 경우 파일 블록은 유럽 내에서만 복제됩니다. 더욱 자세한 내용은 아래의 데이터 센터 및 관리 서비스 제공업체 섹션에서 확인할 수 있습니다.) Magic Pocket과 AWS 모두 최소 99.999999999%의 연간 데이터 지속성을 유지합니다.

Dropbox는 아키텍처와 애플리케이션, 동기화 메커니즘을 결합해 사용자 데이터를 보호하고 데이터의 활용도를 높여줍니다. 드물게 서비스 사용이 불가능한 상황이 발생하더라도 사용자는 연결된 컴퓨터의 로컬 Dropbox 폴더에 동기화된 파일의 최신 사본에 액세스할 수 있습니다. Dropbox 데스크톱 클라이언트/로컬 폴더에 동기화된 파일 사본은 다운타임, 서비스 중단, 오프라인 시에도 하드 드라이브를 통해 액세스할 수 있습니다. 그사이 변경된 파일과 폴더는 서비스 또는 연결이 복구되는 즉시 Dropbox에 동기화됩니다.

Paper 문서

Paper 문서의 중복 사본은 N+1 가용성 모델의 데이터 센터 내부에 위치한 여러 개의 개별적인 장치에 분산되어 저장되며, 매일 문서 데이터의 전체 백업이 수행됩니다. Dropbox는 Paper 문서 스토리지로 최소 99.999999999%의 연간 데이터 지속성을 유지하는 미국 내 AWS 인프라스트럭처를 사용합니다. 드물게 서비스 사용이 불가능한 상황이 발생하더라도 사용자는 모바일 애플리케이션에서 오프라인 모드로 가장 최근에 동기화된 Paper 문서의 사본에 액세스할 수 있습니다.

사고 대응

Dropbox는 사고 대응에 관한 정책과 절차를 갖춰 서비스 가용성, 무결성, 보안, 개인정보 보호, 기밀성과 관련된 문제에 대응하고 있습니다. 사고 대응 절차의 일환으로 Dropbox의 사고대응팀은 다음과 같은 교육을 받습니다.

- 잠재적인 사고에 대한 경고에 신속하게 반응
- 사고의 심각도 결정
- 필요한 경우, 완화 및 억제 조치 실행
- 연관된 내외부 이해 당사자에게 연락(피해를 입은 고객에게 통보해 위반이나 사고 알림 계약 의무를 실행하고 관련된 법과 규정 준수하는 것 포함)
- 조사의 일환으로 관련 증거 수집 및 보존
- 사고 후 결과 기록 및 영구적인 사고 심각성 분류

Dropbox의 사고 대응 정책은 Dropbox가 준수하고 있는 SOC 2, ISO 27001, 기타 보안 평가에 따라 수립·검토됩니다.

업무 연속성

Dropbox는 업무연속성관리체계(BCMS)를 세워 어떻게 하면 사용자들에게 서비스를 지속적으로 제공하고 재개할 수 있는지, 그리고 비즈니스 운영에 필수적인 프로세스와 활동에 지장이 생긴 경우 기업으로서 어떻게 기능해야 하는지를 고심합니다. Dropbox는 다음과 같은 단계로 구성된 순환 프로세스를 운영하고 있습니다.

- **비즈니스 영향 및 위험성 평가**

  Dropbox는 최소 1년에 1번씩 비즈니스영향평가(BIA)를 실시해 Dropbox 운영에 필수적인 프로세스를 파악하고, 운영에 지장이 있을 시 잠재적인 영향을 가늠하고, 복구를 위해 우선적으로 처리해야 할 업무의 계획표를 작성하고, 주요 자회사와 공급업체를 파악합니다. 또한, 최소 1년에 1번씩 기업 전반에 걸쳐 위험성 평가를 시행합니다. 위험성 평가는 Dropbox 운영에 지장을 주는 사고의 위험성을 체계적으로 파악하고, 분석하고, 평가하는 것을 지원합니다. BIA와 위험성 평가를 통해 업무연속성계획(BCP)을 위한 완화 및 복구 전략과 업무 연속성 활동의 우선순위를 파악할 수 있습니다.

- **업무 연속성 계획**

  BIA를 통해 Dropbox의 연속성에 꼭 필요하다고 파악된 팀은 이 정보를 활용해 팀의 주요 프로세스에 필요한 BCP를 개발합니다. 이러한 계획은 응급상황이 발생할 시 프로세스를 재개하는 사람이 누구인지, 운영이 중단된 상황에서 다른 지점의 누가 팀의 프로세스를 인계하는지, 어떤 방법으로 연락을 해야 하는지를 확실하게 정립해줍니다. 또한, 계획을 실행해야 하는 경우와 그 방법, 연락처 및 회의 정보, 주요 앱, 복구 전략 등의 복구 계획과 기타 주요 정보를 중앙 집중화해 사고 발생에 대응할 수 있도록 도와줍니다. Dropbox의 연속성 계획은 Dropbox의 위기관리 및 사고대응팀의 바탕이 되는 위기관리계획(CMP)과 결합되어 있습니다.

- **계획의 테스트/실행**

  Dropbox는 업무 연속성 계획 중 일부 엄선된 원칙을 적어도 1년에 1번씩 테스트합니다. 이 테스트는 BCMS의 범위 및 목표와 맥락을 같이하며 적절한 시나리오를 바탕으로 합니다. 또한 명확하게 규정된 목표를 토대로 정교하게 설계되었습니다. 테스트는 모의훈련부터 실생활 속 사고를 재연한 대규모 시뮬레이션까지 다양한 범위를 다룹니다. 팀은 테스트의 결과와 실제 사고 경험에 따라 계획을 개선하고 향상해 문제를 해결하고 대응력을 강화합니다.

- **BCMS의 검토 및 승인**

  Dropbox신뢰 프로그램 검토의 일환으로 Dropbox의 경영진은 최소 1년에 1번씩 BCMS를 검토합니다

재해 복구

Dropbox는 Dropbox Business의 운영에 영향을 미치는 중대한 위기나 재해가 발생했을 때 정보 보안 요구 사항에 대응하기 위해 재해 복구 계획을 갖추고 있습니다. Dropbox 인프라스트럭처 팀이 매년 재해 복구 계획을 검토하며, 적어도 1년에 1번씩 특정 요소를 테스트합니다. 검토와 테스트를 통해 발견한 결과는 문제가 해결될 때까지 기록되고 추적됩니다.

Dropbox의 재해복구계획(DRP)에는 다음과 같은 재해의 내구성과 가용성을 다룹니다.

- 내구성 재해는 다음의 항목 중 1개 이상으로 구성됩니다.
  - 메타데이터를 저장하는 기본 데이터 센터 또는 파일 블록을 저장하는 복수의 데이터 센터의 완전하거나 영구적인 상실
  - 메타데이터를 저장하는 데이터 센터 또는 파일 콘텐츠를 저장하는 복수의 데이터 센터에 보관된 데이터와의 통신 또는 처리 능력 상실
- 가용성 재해는 다음의 항목 중 1개 이상으로 구성됩니다.
  - 10일 이상 지속된 정전
  - 메타데이터를 저장하는 스토리지 서비스/데이터 센터 또는 파일 블록을 저장하는 복수의 스토리지 서비스/데이터 센터에 보관된 데이터와의 통신 또는 처리 능력 상실

Dropbox는 목표복구시간(RTO: 재해 발생 후 비즈니스 프로세스나 서비스를 복구하는 데 허용된 시간 및 서비스 수준)과 목표복구시점(RPO: 서비스 중단으로 손실된 데이터를 복구하는 데 허용된 최대 시간)을 분명하게 규정하고 있습니다. 또한, 적어도 1년에 1번씩 재해 복구 테스트를 시행해 실제복구시간(RTA)을 측정합니다.

Dropbox 사고 대응, 업무 연속성, 재해 복구 계획은 계획된 시간표에 따라 테스트되며, 중대한 조직상·환경적 변화가 발생할 시 달라질 수 있습니다.

데이터 센터 및 관리 서비스 제공업체

Dropbox의 기업 시스템과 생산 시스템은 미국 내 여러 곳에 흩어져 있는 외부 하청서비스 조직의 데이터 센터 및 관리 서비스 제공업체에 보관되어 있습니다. 하청서비스 조직 데이터 센터 SOC 보고서 및/또는 공급업체 보안 설문지, 계약상 의무는 보안 제어 보장을 위해 적어도 1년에 1번씩 검토됩니다. 이러한 외부 서비스 제공업체는 Dropbox 인프라스트럭처의 경계에서 물리적·환경적·운영상 보안 제어를 책임집니다. Dropbox는 외부 데이터 센터에 보관된 Dropbox 인프라스트럭처의 논리적 보안, 네트워크 보안, 애플리케이션 보안에 관한 책임을 집니다.

Dropbox의 데이터를 처리하고 저장하는 관리 서비스 제공업체 Amazon Web Services(AWS)는 내부 인프라스트럭처를 통해 제공된 Dropbox 서비스의 논리적 보안과 네트워크 보안을 책임집니다. 연결은 AWS의 디폴트 전체 차단 모드로 설정된 방화벽을 통해 보호되며, Dropbox는 제한된 수의 IP 주소와 직원들에게만 액세스를 허용합니다.

유럽 내 인프라스트럭처

Dropbox는 자격을 갖춘 제한된 고객들에게 유럽에 위치한 파일 블록 스토리지를 제공합니다. Dropbox의 인프라스트럭처는 독일 프랑크푸르트에 위치한 Amazon Web Services(AWS)에 의해 호스팅되며, 프랑크푸르트 지역 내에서 복제돼 가외성을 보장하고 데이터 손실을 방지합니다. 모든 고객의 메타데이터와 Paper 문서는 미국 내 저장됩니다.

제품 기능(보안, 제어, 가시성)

Dropbox는 IT 부서와 최종 사용자 모두가 업무와 데이터를 효율적으로 관리할 수 있도록 관리자 제어 기능과 가시성을 제공합니다. 아래는 관리자와 사용자가 이용할 수 있는 기능과 핵심적인 IT 프로세스 관리를 위한 타사 앱 통합 기능의 일부입니다.

참고: 이용 가능한 기능은 가입 요금제에 따라 다릅니다. 자세한 내용은 dropbox.com/business/plans를 참조하세요.

관리자를 위한 관리 기능

하나부터 열까지 모든 것이 똑같은 조직은 존재하지 않습니다. 그래서 Dropbox는 관리자가 팀의 환경과 특성에 따라 Dropbox Business를 맞춤형으로 설정할 수 있는 다양한 도구를 개발했습니다. 아래는 Dropbox Business 관리 콘솔에서 사용할 수 있는 제어 기능과 가시성 기능의 일부입니다.

제어

- **계층적 관리자 역할**

  Dropbox는 팀 관리의 효율성 향상을 위해 계층적 관리자 역할을 제공합니다. 계정 관리자는 세 종류의 액세스 레벨 중 하나를 할당받을 수 있습니다. 팀당 관리자의 수에는 제한이 없으며, 팀원이라면 누구나 관리자 역할을 맡을 수 있습니다.

  - **팀 관리자**
    팀 관리자는 팀의 보안 및 공유 권한을 설정하고, 관리자를 생성하고, 팀원을 관리할 수 있습니다. 팀 관리자에게는 이용 가능한 모든 관리 권한이 주어집니다. 팀 관리자만이 관리자 역할을 할당하거나 변경할 수 있어 Dropbox Business 계정에는 적어도 1명의 팀 관리자가 항상 있어야 합니다.

  - **사용자 관리자**
    사용자 관리자는 팀원 추가/삭제, 그룹 관리, 활동 피드 확인 등 대부분의 팀 관리 업무를 처리할 수 있습니다.

- **지원 관리자**
  지원 관리자는 삭제된 파일 복구나 2단계 인증에 실패해 계정에 액세스할 수 없는 팀원을 지원하는 일 등의 일반적인 서비스 요청을 처리할 수 있습니다. 또한, 관리자가 아닌 팀원의 비밀번호를 초기화하고 특정한 팀원의 활동 로그를 파일로 내보낼 수 있습니다.

- **사용자 프로비저닝 및 계정 관리 방법**

  - **이메일 초대장**
    Dropbox Business 관리 콘솔에 있는 도구로 관리자가 수동으로 이메일 초대장을 생성할 수 있습니다.

  - **Active Directory**
    Dropbox Business 관리자는 Dropbox의 Active Directory 커넥터 또는 외부 ID 공급업체를 통해 기존의 Active Directory에 있는 계정을 삭제하거나 새롭게 생성할 수 있습니다. 통합한 후에는 Active Directory를 이용해 회원을 관리할 수 있습니다.

  - **SSO(Single Sign-On)**
    SSO(Single Sign-On)는 팀원들이 중앙 ID 공급업체에 로그인해 Dropbox Business에 액세스하도록 하는 기능입니다. Dropbox의 SSO는 업계 표준인 SAML 2.0(Security Assertion Markup Language 2.0)을 사용하며, 인증을 신뢰할 수 있는 ID 공급업체에 맡기고 팀원들이 별도의 비밀번호 없이 Dropbox에 액세스할 수 있게 함으로써 업무 환경을 개선하고 보안을 강화해줍니다. Dropbox는 업계를 선도하는 ID 공급업체들과 파트너십을 맺어 사용자 프로비전 및 프로비전 해제를 자동화했습니다. 자세한 내용은 아래의 Dropbox Business API 통합 섹션을 참조하세요.

  - **API**
    고객은 Dropbox Business API를 이용해 맞춤형 사용자 프로비전과 계정 관리 솔루션을 구축할 수 있습니다. 자세한 내용은 아래의Dropbox Business API 통합 섹션을 참조하세요.

- **도메인 관리**

  Dropbox는 기업들이 사용자 온보딩 프로세스와 Dropbox 사용 제어 프로세스를 간소화하고 속도를 향상할 수 있도록 다양한 도구를 제공합니다.

  - **도메인 인증**
    기업이 자신의 도메인에 대한 소유권을 주장할 수 있고, 다른 도메인 관리 도구를 이용할 수 있습니다.

  - **초대 집행**
    관리자가 회사의 Dropbox 팀에 초대된 Dropbox 개인 사용자에게 팀 계정으로 이전하라고 요구하거나 개인용 계정에서 사용 중인 이메일 주소를 변경하라고 요구할 수 있습니다.

  - **도메인 정보**
    관리자가 Dropbox 개인용 계정으로 회사 이메일 주소를 사용 중인 사람 수 등의 주요 정보를 확인할 수 있습니다.

  - **계정 캡처**
    관리자가 회사 이메일 주소를 이용해 모든 Dropbox 사용자가 팀 계정에 합류하도록 강제하거나 개인용 계정에서 사용 중인 이메일 주소를 변경하라고 강제할 수 있습니다.

- **엔터프라이즈 설치 관리자**

  확장된 프로비저닝이 필요한 관리자는 Windows용 엔터프라이즈 설치 관리자를 이용해 Dropbox 데스크톱 클라이언트를 관리 소프트웨어 솔루션 및 배포 메커니즘을 통해 아무도 모르게 원격 설치할 수 있습니다.

- **2단계 인증 요구사항**

  관리자는 팀원 전체에 2단계 인증을 활성화할 것인지, 아니면 특정한 팀원들에게만 2단계 인증을 활성화할 것인지 선택할 수 있습니다. 팀이 SSO 구축을 통해 기타 다요인 인증의 요구사항도 충족할 수 있습니다.

- **비밀번호 제어**

  Education, Advanced, Enterprise 팀의 관리자는 팀원들이 강력하고 복잡한 비밀번호를 생성하도록 설정할 수 있습니다. 이 기능이 활성화되면 모든 웹 세션에서 팀원들의 계정이 로그아웃되고, 다시 로그인할 때는 새로운 비밀번호를 생성하라는 요청이 뜹니다. 기능에 내장된 도구가 사용자의 비밀번호를 흔히 사용되는 단어, 이름, 패턴, 숫자를 수집해 놓은 데이터베이터와 비교해 비밀번호의 강도를 분석합니다. 사용자가 흔한 비밀번호를 입력할 경우, 조금 더 독특하고 추측하기 어려운 비밀번호를 입력하라는 메시지가 표시됩니다. 관리자는 팀의 비밀번호와 개별적인 사용자의 비밀번호를 초기화할 수도 있습니다.

- **그룹**

  팀은 Dropbox를 사용 중인 팀원들의 목록을 생성하고 관리할 수 있습니다. 또한, 팀원들에게 특정한 폴더에 대한 액세스를 제공할 수 있습니다. Active Directory 커넥터로 Dropbox와 Active Directory 그룹을 동기화할 수도 있습니다.

  - **기업 관리 그룹**
    이 유형의 그룹은 관리자만이 회원을 생성하고, 삭제하고, 관리할 수 있습니다. 사용자가 직접 그룹 합류를 요청하거나 자의로 그룹을 떠나는 것은 가능하지 않습니다.

  - **사용자 관리 그룹**
    관리자는 사용자에게 그룹을 생성하고 관리할 권한을 줄 것인지 결정할 수 있습니다. 또한, 언제든지 사용자 관리 그룹을 기업 관리 그룹으로 변경해 그룹에 대한 통제력을 확보할 수 있습니다.

- **컴퓨터 복수 계정 제한**

  관리자는 팀원들이 별도의 Dropbox 계정으로 업무용 Dropbox 계정과 연결된 컴퓨터에 접속하는 것을 차단할 수 있습니다.

- **공유 권한**

  팀 관리자는 다음과 같이 팀의 공유 권한을 광범위하게 제어할 수 있습니다.

  - 팀원들이 파일과 폴더를 팀 외부의 사람들과 공유할 수 있는 권한
  - 팀원들이 팀 외부의 사람들이 소유한 폴더를 수정할 수 있는 권한
  - 팀원들이 생성한 공유 링크를 팀 외부의 사람들이 액세스할 수 있는 권한
  - 팀원들이 파일 요청을 생성하고 팀원 및/또는 팀 외부의 사람들로부터 파일을 수집할 수 있는 권한
  - 팀이 소유한 파일을 다른 사람들이 보고 댓글을 달 수 있는 권한
  - 팀원들이 Paper 문서와 Paper 폴더를 팀 외부에서 공유할 수 있는 권한

- **파일용 팀 폴더**

  관리자는 자동으로 그룹 및 다른 공동 작업자들에게 콘텐츠에 대한 적절한 액세스 레벨(보기 전용 또는 수정)을 부여하는 팀 폴더를 생성할 수 있습니다.

  - **세분화된 액세스 및 공유 제어**
    공유 제어는 회사 내외부의 관계자와 그룹이 허용된 특정한 폴더에만 액세스할 수 있도록 관리자가 최상위 또는 하위 폴더 레벨에서 멤버십과 권한을 관리하는 기능입니다.

  - **팀 폴더 관리 도구**
    관리자가 모든 팀 폴더를 볼 수 있고, 중심에서 공유 정책을 맞춤형으로 변경해 기밀문서가 잘못 공유되는 일을 방지할 수 있습니다.

- **Paper 문서용 공유 폴더**

  관리자는 자동으로 다른 공동 작업자들에게 콘텐츠에 관한 적절한 액세스 레벨(댓글 달기 또는 수정)을 부여하는 Paper 공유 폴더를 생성할 수 있습니다.

- **영구 삭제 권한**

  Dropbox Business 계정의 팀 관리자는 파일과 Paper 문서를 영구적으로 삭제할 수 있는 권한을 팀 관리자만 가지도록 한정할 수 있습니다.

- **웹 세션 제어**

  관리자는 팀원들의 dropbox.com 로그인 지속 시간을 제어할 수 있고, 모든 웹 세션 및/또는 유휴 세션의 지속 시간을 제한할 수 있습니다. 제한 시간이 지난 세션은 자동으로 로그아웃됩니다. 또한, 관리자는 개별 사용자의 웹 세션을 추적하거나 종료할 수 있습니다.

- **앱 액세스**

  관리자는 사용자 계정에 대한 타사 앱의 액세스를 확인하거나 철회할 수 있습니다.

- **장치 연결 해제**

  사용자 계정에 연결된 컴퓨터와 모바일 장치는 관리자가 관리 콘솔에서 연결을 해제하거나 사용자가 직접 개인 계정의 보안 설정에서 연결을 해제할 수 있습니다. 컴퓨터로 연결을 해제하면 인증 데이터가 삭제되며, 다음번에 컴퓨터가 온라인에 접속됐을 때 파일의 로컬 사본을 삭제할 것인지 선택할 수 있습니다(원격 삭제 참조). 모바일 장치의 경우, 연결을 해제하면 즐겨찾기에 추가된 파일과 캐시 데이터, 로그인 정보가 삭제됩니다. 또한, Paper 모바일 애플리케이션에서 오프라인 Paper 문서가 삭제됩니다. 2단계 인증이 활성화된 경우 장치 재연결 시 반드시 재인증을 받아야 합니다. 사용자 계정 설정 화면에서 장치가 연결됐을 때 자동으로 이메일 알림이 전송되도록 설정할 수 있습니다.

- **원격 삭제**

  직원이 팀을 떠나거나 장치를 분실했을 때 관리자가 원격으로 Dropbox 데이터와 파일의 로컬 사본을 삭제할 수 있습니다. 온라인에 접속해 Dropbox 애플리케이션을 실행하면 컴퓨터와 모바일 장치에서 파일이 삭제됩니다.

- **계정 이전**

  수동으로 또는 디렉터리 서비스를 통해 사용자 프로비전을 해제한 후, 관리자는 이전 팀원이 생성한 Paper 문서의 소유권과 파일을 팀 내 다른 사용자의 계정으로 이전할 수 있습니다. 계정 이전 기능은 사용자를 삭제하는 과정 또는 사용자 계정을 삭제한 후 아무 때나 이용할 수 있습니다.

- **일시 중단된 사용자 상태**

  관리자는 사용자의 계정 액세스를 비활성화하면서 계정 내 데이터를 보존하고 관계를 공유해 회사 정보를 안전하게 보호할 수 있습니다. 비활성화된 계정은 이후 관리자가 다시 활성화하거나 삭제할 수 있습니다.

- **사용자로 로그인**

  팀 관리자는 팀원으로 로그인할 수 있습니다. 관리자는 이 기능으로 팀원의 계정에 있는 파일과 폴더, Paper 문서에 직접 액세스해 콘텐츠를 수정하거나 팀원을 대표해 콘텐츠를 공유할 수 있고, 파일 레벨과 관련된 활동에 대한 감사를 수행할 수 있습니다. '사용자로 로그인' 활동은 팀의 활동 로그에 기록되며 관리자는 팀원들에게 이 활동에 대한 알림을 전송할지 여부를 결정할 수 있습니다.

- **네트워크 제어 기능**

  Enterprise 요금제를 이용 중인 Dropbox Business 팀의 관리자는 회사 네트워크 내 Dropbox 사용을 Enterprise 팀으로만 한정할 수 있습니다. 이 기능을 회사 네트워크의 보안 서비스 공급업체와 통합해 특정한 레지스트리 키가 있는 컴퓨터로 로그인한 허용된 계정 외부에 존재하는 트래픽을 차단할 수 있습니다. 현재 Paper는 네트워크 제어 기능으로 관리할 수 없다는 점 참고하시기 바랍니다.

- **엔터프라이즈 모바일 관리 (EMM)**

  Enterprise 요금제를 이용 중인 Dropbox Business 팀의 관리자는 Dropbox와 외부 EMM 공급업체를 통합해 모바일 장치를 통한 팀원들의 Dropbox 사용에 대한 통제력을 강화할 수 있습니다. 관리자는 모바일 앱에서의 Dropbox Enterprise 계정 사용을 관리 중인 장치(회사에서 제공한 장치 및 개인 장치 포함)로 제한하고, 앱 사용 현황(남은 용량, 액세스한 위치 등)에 대한 가시성을 확보하고, 분실된 장치를 원격으로 삭제할 수 있습니다. Paper 모바일 앱은 EMM으로 관리할 수 없다는 점 참조하시기 바랍니다.

- **장치 승인**

  Advanced와 Enterprise 요금제를 이용 중인 Dropbox Education 및 Dropbox Business 팀의 관리자는 사용자 1명당 Dropbox에 동기화할 수 있는 장치의 수를 제한하고, 장치 승인의 주체가 사용자인지 관리자인지 선택할 수 있습니다. 또한, 관리자는 동기화할 수 있는 장치 수의 제한을 받지 않는 예외 사용자 목록을 생성할 수 있습니다. Paper 모바일 앱은 장치 승인에 포함되어 있지 않다는 점 참조하시기 바랍니다.

가시성

- **활동 피드**

  Dropbox Business는 사용자와 관리자의 활동을 팀의 활동 피드에 기록합니다. 이 활동은 관리 콘솔에서 액세스할 수 있습니다. 활동 피드는 관리자가 대상으로 삼은 계정이나 파일, Paper 문서 활동을 조사할 수 있는 유연한 필터 옵션을 제공합니다. 예를 들면, 관리자는 파일이나 Paper 문서의 전체 기록과 사용자의 활동을 볼 수 있고 특정한 기간에 있었던 팀 내 모든 활동을 볼 수 있습니다. 활동 피드는 CSV 형식의 다운로드 가능한 보고서로 내보낼 수 있고, 타사 파트너 솔루션을 통해 보안정보이벤트관리(SIEM) 제품 또는 기타 분석 도구로 직접 통합할 수도 있습니다. 활동 피드에 기록되는 활동은 다음과 같습니다.

- **로그인**
  Dropbox로의 로그인 및 로그인 실패
  - 로그인 시도 또는 로그인 시도 실패
  - 로그인 시도 실패 또는 SSO(Single Sign-On) 오류
  - 로그인 시도 실패 또는 EMM 오류
  - 로그아웃
  - 웹 세션의 IP 주소 변경
- **비밀번호**
  비밀번호 또는 2단계 인증 설정 변경. 관리자는 사용자의 실제 비밀번호를 볼 수 없습니다.
  - 변경되거나 초기화된 비밀번호
  - 2단계 인증의 활성화, 초기화 또는 비활성화
  - SMS 또는 모바일 앱 이용을 위해 2단계 인증 설정 또는 변경
  - 2단계 인증을 위해 백업 휴대전화 추가, 변경 또는 삭제
  - 2단계 인증을 위해 보안 키 추가 또는 삭제
- **멤버십**
  팀에 추가되거나 삭제된 회원
  - 팀원 초대
  - 팀 합류
  - 팀원 삭제
  - 팀원 계정 일시 중단 또는 일시 중단 해제
  - 삭제된 팀원 계정 복구
  - 계정 도메인에 따라 팀 합류 요청
  - 계정 도메인에 따라 팀 합류 요청 승인 또는 거절
  - 기존의 도메인 계정에 도메인 초대장 발송
  - 사용자가 계정 캡처에 응답해 팀 합류
  - 사용자가 계정 캡처에 응답해 팀 탈퇴
  - 팀원의 새로운 팀원 추천 차단 또는 차단 해제
  - 새로운 팀원 추천
- **앱**
  Dropbox 계정에 타사 앱 연결
  - 애플리케이션 승인 또는 삭제
  - 팀 애플리케이션 승인 또는 삭제

- **장치**
  Dropbox 계정에 컴퓨터 또는 모바일 장치 연결
  - 장치 연결 또는 연결 해제
  - 원격 삭제 기능으로 파일을 모두 삭제 또는 일부 파일 삭제 실패
  - 데스크톱 컴퓨터 또는 모바일 장치의 IP 주소 변경

- **관리자 활동**
  공유 폴더 권한 등의 관리 콘솔 설정 변경

  인증 및 SSO(Single Sign-On)
  - 팀원의 비밀번호 초기화
  - 모든 팀원의 비밀번호 초기화
  - 팀원의 2단계 인증 비활성화 차단 또는 차단 해제
  - SSO 활성화 또는 비활성화
  - 요청된 SSO를 통해 로그인
  - SSO URL 변경 또는 삭제
  - SSO 인증서 업데이트
  - SSO 계정 모드 변경

  멤버십
  - 계정 도메인에 따라 사용자의 합류 요청 차단 또는 차단 해제
  - 팀원 자격 요청 자동 승인 또는 관리자 직접 승인 설정

  팀원 계정 관리
  - 팀원 이름 변경
  - 팀원 이메일 주소 변경
  - 관리자 상태 정보 제공 또는 삭제, 또는 관리자 역할 변경
  - 팀원으로 로그인 또는 로그아웃
  - 삭제된 팀원 계정의 콘텐츠 이전 또는 삭제
  - 삭제된 팀원 계정의 콘텐츠 영구 삭제

  글로벌 공유 설정
  - 팀원들이 팀 외부 사람이 소유한 공유 폴더 추가하는 것 차단 또는 차단 해제
  - 팀원들이 팀 외부 사람과 폴더 공유하는 것 차단 또는 차단 해제
  - 팀원들이 팀 외부 사람과 폴더를 공유하기 전에 표시되는 경고 메시지 활성화
  - 팀 외부 사람의 공유 링크 확인 차단 또는 차단 해제
  - 공유 링크를 팀 전용으로 디폴트 설정

- 파일에 댓글 달기 차단 또는 차단 해제
- 팀원들의 파일 요청 차단 또는 차단 해제
- 공유 링크 페이지의 로고 추가, 변경 또는 삭제
- 팀원들이 팀 외부 사람과 Paper 문서 및 Paper 폴더 공유하는 것 차단 또는 차단 해제

파일용 팀 폴더 관리

- 팀 폴더 생성
- 팀 폴더 이름 변경
- 팀 폴더 보관 또는 보관 취소
- 팀 폴더 영구 삭제
- 팀 폴더를 공유 폴더로 다운그레이드

도메인 관리

- 도메인 인증 시도, 도메인 인증 성공, 또는 도메인 삭제
- Dropbox 지원팀의 도메인 인증 또는 삭제
- 도메인 초대장 발송 활성화 또는 비활성화
- '신규 사용자 자동 초대' 활성화 또는 비활성화
- 계정 캡처 모드 변경
- Dropbox 지원팀의 계정 캡처 승인 또는 철회

엔터프라이즈 모바일 관리 (EMM)

- 테스트 모드(선택 사항) 또는 배포 모드(필수)에 대한 EMM 활성화
- EMM 토큰 새로고침
- EMM 사용자 제외 목록에서 팀원 추가 또는 삭제
- EMM 비활성화
- EMM 사용 예외 목록 보고서 생성
- EMM 모바일 앱 사용 현황 보고서 생성

기타 팀 설정 변경

- 팀 합병
- 팀을 Dropbox Business로 업그레이드 또는 무료 버전으로 다운그레이드
- 팀 이름 변경
- 팀 활동 보고서 생성
- 팀원들이 컴퓨터 1대당 1개 이상의 계정 연결하는 것 차단 또는 차단 해제
- 모든 팀원 또는 관리자만 그룹 생성 허용

- 팀원들의 파일 영구 삭제 차단 또는 차단 해제
- 리셀러를 위한 Dropbox 지원 세션 시작 또는 종료

- **파일, 폴더, 링크 공유**
  보고서에 팀 외부 사람이 결부된 활동이 있는지 표시됩니다(해당될 경우).

  파일 공유

  - 팀원 또는 팀 외부 사람 추가 또는 삭제
  - 팀원 또는 팀 외부 사람의 권한 변경
  - 그룹 추가 또는 삭제
  - 사용자의 Dropbox에 공유 파일 추가
  - 파일 또는 폴더 초대를 통해 공유한 파일 콘텐츠 확인
  - 사용자의 Dropbox로 공유 콘텐츠 복사
  - 공유 콘텐츠 다운로드
  - 파일에 댓글 추가
  - 댓글 해결 또는 미해결
  - 댓글 삭제
  - 댓글 알림 구독 또는 구독 취소
  - 팀이 소유한 파일로의 초대 요청
  - 팀이 소유한 파일에 대한 액세스 요청
  - 파일 공유 해제

  폴더 공유

  - 새로운 공유 폴더 생성
  - 팀원, 팀 외부 사람, 그룹 추가 또는 삭제
  - 사용자의 Dropbox로 공유 폴더 추가, 또는 사용자가 직접 공유 폴더 액세스 삭제
  - 링크에서 공유 폴더 추가
  - 팀원 또는 팀 외부 사람의 권한 변경
  - 폴더 소유권을 다른 사용자에게 이전
  - 폴더 공유 해제
  - 공유 폴더 회원 자격 요청
  - 공유 폴더에 대한 액세스 요청
  - 회원 자격 요청한 사용자를 공유 폴더에 추가
  - 팀 외부 사람을 폴더에 추가하는 것 차단 또는 차단 해제
  - 모든 팀원 또는 관리자만 폴더에 구성원 추가 허용
  - 공유 폴더에 대한 그룹 액세스 변경

링크 공유

- 링크 생성 또는 삭제
- 링크에 담긴 콘텐츠를 링크를 전송받은 모든 사람 또는 팀원만 볼 수 있도록 설정
- 링크에 담긴 콘텐츠에 비밀번호 보호 설정
- 링크에 만료일 설정 또는 삭제
- 링크 확인
- 링크에 담긴 콘텐츠 다운로드
- 링크에 담긴 콘텐츠를 사용자의 Dropbox로 복사
- API 앱으로 파일 링크 생성
- 팀원, 팀 외부 사람, 그룹과 링크 공유
- 팀 외부 사람의 파일 링크 확인 차단 또는 차단 해제
- 앨범 공유

파일 요청

- 파일 요청 생성, 변경 또는 종료
- 파일 요청에 사용자 추가
- 파일 요청 마감 시한 추가 또는 삭제
- 파일 요청 폴더 변경
- 파일 요청을 통해 파일 수신

- **그룹**
  그룹 생성, 삭제 및 그룹 멤버십 정보
  - 그룹의 생성, 이름 변경, 이동 또는 삭제
  - 구성원 추가 또는 삭제
  - 그룹 구성원의 액세스 유형 변경
  - 그룹을 팀 관리 또는 관리자 관리로 변경
  - 그룹의 외부 ID 변경

- **파일 활동**
  개별적인 파일 및 폴더 활동
  - Dropbox에 파일 추가
  - 폴더 생성
  - 파일 확인
  - 파일 수정
  - 파일 다운로드
  - 파일 또는 폴더 복사

- 파일 또는 폴더 이동
- 파일 또는 폴더의 이름 변경
- 파일을 이전 버전으로 복구
- 파일의 변경 사항 복구
- 삭제된 파일 복구
- 파일 또는 폴더 삭제
- 파일 또는 폴더 영구 삭제

- **Paper 활동 로그**
  관리자는 활동 로그에 있는 Paper 활동의 유형을 선택하거나, 전체 활동 보고서를 다운로드할 수 있습니다. 기록되는 Paper 활동은 다음과 같습니다.

  - Paper 활성화 또는 비활성화
  - Paper 문서의 생성, 수정, 내보내기, 보관, 영구 삭제, 복구
  - Paper 문서 댓글 달기 및 댓글 해결
  - 팀원, 팀 외부 사람과 Paper 문서 공유 및 공유 해제
  - 팀원, 팀 외부 사람의 Paper 문서 액세스 요청
  - Paper 문서에서 팀원 및 팀 외부 사람 언급
  - 팀원 및 팀 외부 사람의 Paper 문서 확인
  - Paper 문서 팔로잉
  - Paper 문서에 대한 구성원 권한 변경(수정, 댓글 또는 보기 전용)
  - Paper 문서 외부 공유 정책 변경
  - Paper 폴더 생성, 보관, 영구 삭제
  - Paper 문서를 폴더에 추가 또는 폴더에서 삭제
  - Paper 폴더 이름 변경
  - Paper 문서 및 폴더 이전

- **기술 지원 ID 확인**

  Dropbox 지원팀이 문제를 해결하거나 계정 정보를 제공하기에 앞서 계정 관리자는 임의로 생성된 일회용 보안 코드를 제공해 본인의 신분을 확인해야 합니다. 이 PIN 코드는 관리 콘솔을 통해서만 생성할 수 있습니다.

사용자를 위한 관리 기능

Dropbox Business는 관리자를 위한 관리 기능뿐 아니라 최종 사용자가 자신의 계정과 데이터에 대한 보안을 강화할 수 있는 도구를 갖추고 있습니다. Dropbox의 다양한 사용자 인터페이스를 통해 아래에 설명된 인증, 복구, 로그인, 기타 보안 기능 등을 이용할 수 있습니다.

복구 및 버전 관리

Dropbox Business의 모든 고객에는 삭제된 파일과 Paper 문서는 물론 파일과 Paper 문서의 이전 버전을 복구하는 기능이 제공되어 중요한 데이터의 변경 사항을 추적하고 되돌리는 것이 가능합니다.

2단계 인증

이 강력한 보안 기능은 Dropbox 계정의 보안 계층을 한층 더 강화해줍니다. 2단계 인증이 활성화되면 Dropbox에 로그인할 때와 새로운 컴퓨터, 휴대전화, 태블릿을 Dropbox에 연결할 때 비밀번호와 별도의 6자리 보안 코드를 입력해야 합니다.

- 관리자는 팀원 전체에 2단계 인증을 활성화할 것인지, 아니면 특정한 팀원들에게만 2단계 인증을 활성화할 것인지 선택할 수 있습니다.
- 계정 관리자는 어떤 팀원이 2단계 인증을 활성화했는지 추적할 수 있습니다.
- Dropbox의 2단계 인증 코드는 시간 기반 일회용 비밀번호(TOTP)의 알고리즘 표준을 따르며, 문자메시지나 앱을 통해 전송됩니다.
- 문자메시지나 앱으로 보안 코드가 전송되지 않을 경우 16자리 일회용 긴급 백업 코드를 사용하거나, 보조 휴대전화 번호를 사용해 문자메시지로 백업 코드를 전송받을 수 있습니다.
- Dropbox는 생체인증 표준인 U2F(Universal Second Factor)를 지원해 6자리 코드 대신 USB 보안 키로도 사용자 인증을 할 수 있습니다.

사용자 계정 활동

모든 사용자는 계정 설정 화면에서 다음의 페이지를 확인해 자신의 계정 활동에 관한 최신 정보를 얻을 수 있습니다.

- **공유 페이지**

  공유 페이지에는 현재 사용자의 Dropbox에 있는 공유 폴더와 사용자가 추가할 수 있는 공유 폴더가 표시됩니다. 각 사용자는 폴더와 파일의 공유를 해제하거나 공유 권한을 설정할 수 있습니다(아래 참조).

- **파일 페이지**

  파일 페이지에는 사용자에게 공유된 파일과 각 파일로 공유된 데이터가 표시됩니다. 각 사용자는 파일에 대한 액세스를 삭제할 수 있습니다. Paper 문서 내 탐색 인터페이스에 있는 '나와 공유됨' 페이지로 이동하면 다른 사람이 본인과 공유한 Paper 문서를 확인할 수 있습니다.

- **링크 페이지**

  링크 페이지에는 사용자가 생성한 모든 활성화된 공유 링크와 각 링크의 생성일, 다른 사람이 사용자와 공유한 링크가 표시됩니다. 각 사용자는 링크를 비활성화하거나 권한을 변경할 수 있습니다(아래 참조).

- **이메일 알림**

  각 사용자는 새로운 장치나 앱이 자신의 Dropbox 계정으로 연결되면 이메일 알림이 전송되도록 설정할 수 있습니다.

사용자 계정 권한

- **연결된 장치**

  계정 보안 설정의 '장치' 섹션에는 사용자의 계정에 연결된 모든 컴퓨터와 모바일 장치가 표시됩니다. 또한, 각 컴퓨터의 IP 주소와 국가, 최근 활동 발생 시간이 표시됩니다. 각 사용자는 장치의 연결을 해제한 후 다음번에 컴퓨터가 온라인에 접속됐을 때 연결된 컴퓨터의 파일을 삭제할 것인지 선택할 수 있습니다.

- **활성화된 웹 세션**

  세션 섹션에는 현재 사용자 계정에 로그인되어 있는 모든 웹 브라우저가 표시됩니다. 또한, 각 브라우저의 IP 주소와 국가, 가장 최근 세션의 로그인 시간, 최근 활동 발생 시간이 표시됩니다. 각 사용자는 계정의 보안 설정에서 웹 세션을 원격으로 종료할 수 있습니다.

- **연결된 앱**

  '연결된 앱' 섹션에는 사용자의 계정에 액세스할 수 있는 모든 타사 앱과 각 앱에 허용된 액세스 레벨이 표시됩니다. 사용자는 타사 앱이 본인의 Dropbox에 액세스할 수 있는 권한을 철회할 수 있습니다.

모바일 보안

- **지문 스캔**

  Dropbox 모바일 앱을 열 때 iOS 장치는 Touch ID/Face ID, Android 장치는 지문으로 잠금 해제(해당될 경우) 기능을 활성화할 수 있습니다.

- **데이터 삭제**

  비밀번호 입력 오류 10회 이후 장치에서 모든 Dropbox 데이터를 삭제하는 기능을 활성화해 보안을 더욱 강화할 수 있습니다.

- **내부 스토리지 및 오프라인 파일**

  기본적으로 파일은 모바일 장치 내부의 스토리지에 저장되지 않습니다. Dropbox 모바일 클라이언트에는 개별적인 파일과 폴더를 장치에 오프라인 보기 전용으로 저장하는 기능이 있습니다. 모바일 또는 웹 인터페이스를 통해 Dropbox 계정에 연결된 장치가 해제되면 장치에 있는 파일과 폴더가 자동으로 장치의 내부 스토리지에서 삭제됩니다.

- **오프라인 Paper 문서**

  Dropbox 계정의 보안 페이지를 통해 Paper에 연결된 장치가 해제되면 사용자의 계정이 로그아웃되고 오프라인 Paper 문서가 자동으로 장치의 내부 스토리지에서 삭제됩니다.

공유 파일 및 폴더 권한

- **공유 파일에 대한 권한**

  공유 파일 소유자가 특정한 사용자의 액세스를 삭제하고, 파일에 댓글 달기 기능을 비활성화할 수 있습니다.

- **공유 폴더에 대한 권한**

  공유 폴더 소유자가 특정한 사용자의 폴더 액세스를 삭제하고, 특정한 사용자의 보기/수정 권한을 변경하고, 폴더 소유권을 이전할 수 있습니다. 또한, 팀의 글로벌 공유 권한에 따라 각 공유 폴더의 소유자가 폴더를 팀 외부 사람과 공유할 수 있는지, 수정 권한이 있는 구성원이 멤버십을 관리할 수 있는지, 그리고 링크를 폴더 외부의 사람과 공유할 수 있는지 제어할 수 있습니다.

- **공유 링크의 비밀번호**

  링크 소유자가 임의로 비밀번호를 설정해 공유 링크를 보호할 수 있습니다. 파일이나 폴더 데이터를 전송하기 전, 액세스 제어 단계에서 비밀번호가 올바르게 입력되었는지, 그리고 팀, 그룹, 폴더 ACL 등의 기타 요건이 충족되었는지를 확인합니다. 비밀번호가 올바르게 입력되고 기타 요건이 충족된 경우, 보안 쿠키가 사용자의 브라우저에 저장되어 입력한 비밀번호가 이미 확인을 거쳤음을 기억합니다.

- **공유 링크의 만료일**

  공유 링크에 만료일을 설정해 파일이나 폴더에 대한 임시 액세스를 제공할 수 있습니다.

Paper 문서 및 Paper 폴더 권한

- **Paper 문서 및 공유된 Paper 폴더에 대한 권한**

  Paper 문서나 공유된 Paper 폴더의 소유자가 특정한 사용자의 액세스를 삭제하고, Paper 문서를 수정하는 기능을 비활성화할 수 있습니다.

- **Paper 문서에 대한 권한**

  Paper 문서 소유자가 공유 패널에 등록된 특정한 사용자의 액세스를 삭제할 수 있습니다. Paper 문서 소유자와 수정 권한을 가진 구성원 모두 특정한 사용자의 보기/수정 권한과 문서의 연결 정책을 변경할 수 있습니다. 연결 정책은 문서를 열어볼 수 있는 사용자와 그들에게 부여된 권한을 규정합니다. 팀 전체에 적용되는 연결 정책 환경과 문서 공유 정책은 팀 관리자가 설정할 수 있습니다.

- **Paper 폴더에 대한 권한**

  폴더의 구성원인 팀원이 폴더의 공유 정책을 변경하고, 폴더에 추가된 특정한 사용자의 액세스를 삭제할 수 있습니다.

Dropbox Business API 통합

Dropbox Business API와 Dropbox 파트너를 통해 다양한 보안 도구를 추가해 데이터와 계정을 관리할 수 있습니다.

- **보안정보이벤트관리(SIEM) 및 분석**

  Dropbox Business 계정을 SIEM 및 분석 도구에 연결해 사용자 공유 현황과 로그인 시도, 관리자 활동 등을 모니터링하고 평가할 수 있습니다. 중앙 로그 관리 도구를 통해 직원들의 활동 로그와 보안 관련 데이터에 액세스하고 간편하게 관리하세요.

- **데이터손실방지(DLP)**

  이 도구는 파일 메타데이터와 콘텐츠를 자동으로 스캔해 Dropbox 계정에 중요한 변경 사항이 생기면 경고, 보고, 조치를 작동합니다. Dropbox Business 구축 시 회사 정책을 적용하면 규제 준수 요건을 충족하는 데 도움이 됩니다.

- **e디스커버리 및 소송 자료 보존**

  Dropbox Business 계정의 데이터에 관한 소송, 중재, 조사에 대응할 수 있습니다. e디스커버리 프로세스로 저장된 정보 중 관련 있는 것을 검색·수집하고 데이터를 보존해 업무상 시간과 비용을 절약하세요.

- **디지털저작권관리(DRM)**

  타사 콘텐츠 보호 도구를 추가해 직원의 계정에 저장된 데이터 중 중요하거나 저작권이 있는 데이터를 보호할 수 있습니다. 클라이언트 측 암호화, 워터마킹, 감사 추적, 액세스 철회, 사용자/장치 차단 등의 강력한 DRM 기능에 액세스하세요.

- **데이터 이전 및 사내 백업**

  기존의 서버나 클라우드 기반 솔루션에서 Dropbox로 데이터를 이전해 시간과 비용, 노력을 절약할 수 있습니다. Dropbox Business 계정에서 사내 서버로 백업을 자동화하세요.

- **ID 관리 및 SSO(Single Sign-On)**

  프로비전과 프로비전 해제 프로세스를 자동화하고 새로운 직원의 온보딩 속도를 향상할 수 있습니다. Dropbox Business를 기존의 ID 시스템과 통합해 관리를 간소화하고 보안을 강화하세요.

- **맞춤형 업무 흐름**

  Dropbox를 기존의 비즈니스 프로세스와 통합하는 사내 앱을 구축해 회사의 업무 흐름을 향상할 수 있습니다.

개발자들에게 Dropbox Business의 팀 기능에 대한 액세스를 부여하면 관리자가 팀 업무에 필수적인 애플리케이션을 구축하고 관리할 수 있습니다. Dropbox Business가 기존에 사용하던 타사 솔루션과 더욱 원활하게 통합되는 현재, 이러한 통합 기능은 특히 Enterprise 고객에게 유용하게 사용될 수 있습니다. Dropbox Business API에 관한 더욱 자세한 내용은 아래의 Dropbox용 앱 섹션을 참조하세요.

애플리케이션 보안

Dropbox 사용자 인터페이스

Dropbox 서비스는 다양한 인터페이스를 통해 활용하고 액세스할 수 있습니다. 각 서비스는 사용자 데이터를 처리하고 보호하는 동시에 간편한 액세스를 제공하는 보안 환경과 기능을 갖추고 있습니다.

- **웹**

  이 인터페이스는 현대의 모든 웹 브라우저를 통해 액세스할 수 있습니다. 사용자는 웹 인터페이스를 통해 파일을 업로드하고, 다운로드하고, 보고, 공유할 수 있으며, 컴퓨터에 깔린 기본 애플리케이션으로 기존의 로컬 버전 파일을 열어볼 수 있습니다.

- **데스크톱**

  Dropbox 데스크톱 애플리케이션은 파일을 로컬에 저장해 오프라인 액세스를 제공하는 강력한 동기화 클라이언트입니다. 이 애플리케이션은 Windows와 Mac, Linux 운영체제에서 실행되며 사용자에게 본인의 Dropbox 계정에 대한 전체 액세스를 제공합니다. 각 운영체제의 파일 브라우저에서 파일을 확인하고 공유할 수 있습니다.

- **모바일**

  Dropbox 앱은 iOS, Android, Windows, Kindle Fire 스마트폰과 태블릿에서 지원되어 이동 중에도 파일에 액세스하는 것이 가능합니다. 또한, 파일을 오프라인에서도 액세스할 수 있도록 설정할 수 있습니다.

- **API**

  Dropbox API는 검색, 수정, 파일 복구 등의 고급 기능에 대한 액세스와 Dropbox 계정에서 콘텐츠를 읽고 쓰는 유연한 방법을 제공합니다. API는 Dropbox Business 계정의 사용자 수명 주기를 관리하고, 모든 팀원에 작업을 수행하고, Dropbox Business 관리자 기능에 대한 액세스를 활성화하는 데 사용됩니다.

Paper 사용자 인터페이스

Paper 서비스는 다양한 인터페이스를 통해 활용하고 액세스할 수 있습니다. 각 서비스는 사용자 데이터를 처리하고 보호하는 동시에 간편한 액세스를 제공하는 보안 환경과 기능을 갖추고 있습니다.

- **웹**

  이 인터페이스는 현대의 모든 웹 브라우저를 통해 액세스할 수 있습니다. 사용자는 웹 인터페이스를 통해 Paper 문서를 생성하고, 보고, 수정하고, 다운로드하고, 공유할 수 있습니다.

- **모바일**

  Paper 모바일 애플리케이션은 iOS 및 Android 모바일 장치와 태블릿에서 지원되어 이동 중에도 Paper 문서에 액세스하는 것이 가능합니다. 모바일 애플리케이션은 기계어(iOS 또는 Android)가 내부의 웹뷰 브라우저를 감싸고 있는 형태의 하이브리드 애플리케이션입니다.

- **API**

  위에서 설명한 Dropbox API는 권한 관리, 압축 보관, 영구 삭제 등의 기능에 대한 지원을 포함해 Dropbox Paper에 있는 문서와 폴더를 관리하는 엔드포인트와 데이터 유형으로 구성됩니다.

암호화

전송 중 데이터

Dropbox는 데이터 전송 시 보안소켓계층(SSL)/전송계층보안(TLS) 프로토콜을 활용해 앱과 서버 간에 이동하는 데이터를 보호하며, 128비트 이상의 고급암호표준(AES) 알고리즘으로 보안이 강화된 안전한 터널을 생성합니다. Dropbox 클라이언트(현재 기준 데스크톱, 모바일, API, 웹)와 호스트된 서비스 간을 이동하는 파일 데이터는 SSL/TLS를 통해 암호화됩니다. 마찬가지로, Paper 클라이언트(현재 기준 모바일, API, 웹)와 호스트된 서비스 간을 이동하는 Paper 문서의 데이터도 SSL/TLS를 통해 암호화됩니다. 엔드포인트 보안을 위해 Dropbox는 (데스크톱과 모바일) 최신 브라우저를 제어하며, 강력한 암호를 사용해 완전 순방향 비밀성과 인증서 피닝을 지원합니다. 또한, 웹상에서 모든 인증 쿠키를 안전한 것으로 표시하고 활성화된 includeSubDomains로 HSTS(HTTP Strict Transport Security)를 활성화합니다.

참고: Dropbox는 취약성이 발견된 SSLv3 사용을 중단하고 TLS를 단독으로 사용합니다. TLS는 흔히 'SSL/TLS'로 통용되며, 이러한 이유로 이 백서에서는 TLS 대신 SSL/TLS라는 용어를 사용했습니다.

중간자 공격을 방지하기 위해 Dropbox 프런트엔드 서버 인증은 클라이언트가 보유한 공개 인증서를 통해 수행됩니다. 파일이나 Paper 문서를 전송하기 전에 연결이 암호화되어 Dropbox의 프런트엔드 서버로 안전하게 전송됩니다.

저장된 데이터

사용자가 업로드한 Dropbox 파일은 유휴 상태에서 256비트 고급암호표준(AES)을 통해 암호화됩니다. 파일은 개별적인 파일 블록으로 나뉘어 복수의 데이터 센터에 저장됩니다. 각 블록은 강력한 암호를 통해 분리되고 저장되며, 최신 버전에서 수정된 블록만 동기화됩니다. Paper 문서도 유휴 상태에서 256비트 고급암호표준(AES)을 통해 암호화되며. Paper 문서는 타사 시스템을 통해 복수의 가용 영역에 저장됩니다.

키 관리

Dropbox의 키 관리 인프라스트럭처는 키에 대한 직접적인 액세스를 최소한으로 제한해 운영상·기술적·절차상 보안을 유지하도록 설계되었습니다. 암호화 키의 생성과 교환, 저장은 분산 처리를 위해 여러 곳에 분배됩니다.

- **파일 암호화 키**

  Dropbox는 사용자를 대신해 파일 암호화를 관리하며 복잡성을 제거하고, 고급 제품 기능을 지원하며, 암호를 철저히 통제합니다. 파일 암호화 키는 생산 시스템 인프라스트럭처 보안 제어 장치와 보안 정책을 통해 생성·저장·보호됩니다.

- **내부 SSH 키**

  생산 시스템에 대한 액세스는 쌍으로 짝지어진 고유의 SSH 키를 통해 제한됩니다. 보안 정책과 절차는 SSH 키로 보호됩니다. 내부 시스템이 안전한 공개 키 교환 프로세스를 관리하고, 비공개 키는 안전하게 저장됩니다. 별도의 2차 인증 요소 없이는 내부 SSH 키를 생성 시스템에 액세스하는 데 사용할 수 없습니다.

- **키 분배**

  Dropbox는 운영에 필요한 시스템으로의 키 분배와 관리를 자동화하고 있습니다.

인증서 피닝

Dropbox는 대개의 경우 HPKP(HTTP Public Key Pinning) 사양을 지원하는 최신 브라우저와 Dropbox의 데스크톱 및 모바일 클라이언트에서 인증서 피닝을 합니다. 인증서 피닝은 연결하려는 서비스가 가짜가 아닌 진짜임을 보장하기 위해 실행하는 추가 점검입니다. Dropbox는 이 기능을 활용해 사용자 활동을 염탐하는 숙련된 해커의 다양한 루트를 방어합니다.

인증 데이터 보호

Dropbox는 사용자의 로그인 인증서를 보호하기 위해 해싱에 많은 노력을 기울입니다. 모든 패스워드는 업계 우수 사례에 발맞춰 임의로 생성된 고유의 일회성 솔트로 솔팅 처리되며, Dropbox는 반복 해싱을 사용해 계산 속도를 낮춥니다. 이러한 우수 사례는 무작위 대입 공격과 사전 공격, 레인보우 공격을 방어하는 데 유용하게 쓰입니다. Dropbox는 추가 예방을 위해 데이터베이스와 별도로 저장된 키로 해시를 암호화해 데이터베이스가 공격을 받았을 때도 비밀번호를 안전하게 보호합니다.

악성 소프트웨어 스캔

Dropbox는 악성 소프트웨어가 Dropbox의 공유 링크 기능에 침투할 수 없도록 설계된 자동 스캔 시스템을 개발했습니다. 이 시스템은 Dropbox 독점 기술과 업계 표준 바이러스 탐지 엔진을 모두 활용합니다.

Dropbox용 앱

DBX Platform은 Dropbox의 유연한 응용프로그램인터페이스(API)를 기반으로 애플리케이션을 제작하는 개발자들로 구성된 활발한 생태계입니다. 50만 이상의 개발자들이 생산성, 협업, 보안, 관리 등이 용이한 이 플랫폼을 활용해 애플리케이션과 서비스를 개발했습니다.

Dropbox API

Dropbox API는 Dropbox에서 콘텐츠를 읽고 쓸 수 있는 유연한 방식으로, 개발자는 이를 활용해 사용자에게 Dropbox 파일로의 인앱 액세스를 제공할 수 있습니다. 인증, 파일, 메타데이터 송수신, 공유 파일, 링크 주고받기, Paper 문서 및 Paper 폴더 공유, 파일 작업 등이 모두 Dropbox API를 통해 처리됩니다.

Dropbox API를 활용해 다음 중 하나의 권한을 가진 앱을 구축할 수 있습니다.

- **앱 폴더**

  앱 이름을 본딴 이 전용 폴더는 사용자 Dropbox의 Apps 폴더에 생성됩니다. 이 앱에는 Apps 폴더에만 적용되는 읽기 및 쓰기 액세스가 제공되며, 사용자는 폴더에 파일을 옮기는 방식으로 앱에 콘텐츠를 제공할 수 있습니다. 또한, 앱은 Chooser 또는 Saver를 통해 파일/폴더 액세스를 요청할 수 있습니다(아래 참조).

- **Full Dropbox**

  이 앱에는 사용자 Dropbox의 모든 파일과 폴더에 대한 액세스가 제공되며, Chooser 또는 Saver를 통해 파일/폴더 액세스를 요청할 수도 있습니다(아래 참조).

Chooser와 Saver

Chooser와 Saver를 활용하면 단 몇 줄의 코드로 Dropbox로의 간편한 액세스를 제공할 수 있습니다. Chooser는 Dropbox로부터 파일을 활성화하고, Saver는 사용자가 파일을 Dropbox에 파일을 바로 저장할 수 있도록 합니다. 본질적으로 Chooser와 Saver는 기존의 열기 및 저장하기 대화 상자를 대체하며, 앱의 액세스를 사용자가 일회성으로 선택한 파일 및/또는 폴더로만 제한합니다.

Dropbox는 업계 표준 인증 프로토콜인 OAuth를 통해 사용자가 자신의 계정 인증서를 노출하지 않고도 앱 계정 액세스를 승인할 수 있도록 합니다. Dropbox는 OAuth 2.0으로 API 요청 인증을 처리하며, 이러한 요청은 Dropbox의 웹사이트 또는 모바일 앱을 통해 인증됩니다.

Webhook

웹후크는 사용자의 Dropbox에 변경 사항이 있을 때 웹 앱에 실시간으로 알림을 전송하는 방식입니다. URI를 등록해 웹후크를 수신받을 수 있는 상태가 되면 앱에 등록된 사용자에 변경 사항이 있을 때마다 HTTP 요청이 해당 URI에 전송됩니다. Dropbox Business API를 이용하면(아래 설명 참조) 팀 멤버십에 변경 사항이 있을 때 알림을 생성하는 데도 웹후크를 사용할 수 있습니다. 많은 보안 앱이 관리자가 팀 활동을 추적하고 관리하는 데 웹후크를 사용합니다.

Dropbox Business API

Dropbox Business API를 이용하면 앱에서 모든 Dropbox Business 계정을 관리하고, 팀 내 모든 구성원에 Dropbox API 작업을 수행할 수 있습니다. Dropbox Business API는 앱에 Dropbox Business 관리자 기능에 대한 프로그래밍 액세스를 제공합니다.

Dropbox Business API는 Dropbox API 호출뿐 아니라 업무를 위해 특별히 고안된 추가적인 엔드포인트를 갖추고 있습니다. 여기에는 감사용 엔드포인트와 사용자 및 그룹 관리 엔드포인트가 포함됩니다.

앱 권한의 유형

Dropbox Business API 권한에는 팀과 사용자 데이터에 대한 다양한 수준의 액세스를 아우르는 4가지 유형이 있습니다. 개발자는 앱에 필요한 최소한의 권한에 대한 액세스만 요청해야 합니다.

- **팀 정보**

  팀에 통합 사용 데이터에 관한 정보

- **팀 감사**

  팀 정보 + 팀의 상세한 활동 로그

- **팀원 파일 액세스**

  팀 정보 및 감사 + 모든 팀원의 작업 수행 권한

- **팀원 관리**

  팀 정보 + 팀원을 추가, 편집, 삭제할 수 있는 권한

Dropbox API와 마찬가지로 Dropbox Business API는 OAuth 2.0으로 API 요청 인증을 처리합니다. Dropbox Business API OAuth 토큰은 계정 데이터에 대한 광범위한 액세스를 활성화할 수 있습니다. OAuth의 응답에는 추가적인 team_id 필드가 포함됩니다. 서버 측 OAuth 토큰의 보안을 철저히 유지하고, 불안정한 환경에서 캐시가 저장되거나 클라이언트 장치로 다운로드되지 않게 하는 일은 개발자의 책임입니다. 애플리케이션을 Dropbox Business 계정에 설치하려면 개발자가 OAuth 2.0 표준 방식을 통해 Dropbox Business 팀 관리자에게 명령을 내려야 합니다.

Dropbox API에 관한 더욱 자세한 내용은 dropbox.com/developers에서 확인하세요.

Dropbox 개발자 지침

Dropbox는 개발자들이 사용자의 개인정보를 보호하는 동시에 사용자 경험을 향상하는 API 앱을 제작할 수 있도록 다양한 지침과 사례를 제공합니다.

- **앱 키**

  개발자는 각각의 앱마다 고유의 Dropbox 앱 키를 사용해야 합니다. 앱이 DBX Platform을 통해 다른 개발자들이 사용할 수 있는 서비스나 소프트웨어를 제공할 경우, 각 개발자는 고유의 Dropbox 앱 키를 신청해야 합니다.

- **앱 권한**

  개발자는 앱에 허용되는 최소한의 특권만을 이용하도록 교육을 받습니다. 개발자가 배포 승인을 위해 앱을 제출하면 Dropbox는 앱이 제공하는 기능에 비해 불필요하게 광범위한 권한을 요청하지는 않는지 검토합니다.

- **앱 검토 프로세스**

  - **개발 상태**
    Dropbox API 앱이 개발되면, 앱에 개발 상태가 부여됩니다. 이 상태에서의 앱은 연결할 수 있는 Dropbox 사용자의 수가 500명이라는 점을 제외하면 다른 배포 상태의 앱과 동일하게 기능합니다. 앱을 연결한 사용자 수가 50명에 이르면 개발자는 2주 이내에 배포 상태를 신청하고 승인을 받아야 합니다. 그렇지 않으면 다른 사용자들의 앱 연결이 제한됩니다.

  - **배포 상태 및 승인**
    배포 상태 승인을 받으려면 앱이 DBX Platform 사용 시 금지되는 사항을 명시해 놓은 Dropbox 개발자 브랜딩 지침서와 이용 약관을 준수해야 합니다. DBX Platform 사용 시 금지되는 사항에는 IP 홍보, 저작권 침해, 파일 공유 네트워크 생성, 콘텐츠 불법 다운로드 등이 포함됩니다. 개발자는 앱을 제출해 심사를 받기 전에 먼저 앱의 기능에 관한 추가 정보를 제공하고 Dropbox API를 어떤 방식으로 활용했는지 설명해야 합니다. 앱이 배포 상태 승인을 받으면 무제한의 Dropbox 사용자가 앱을 연결할 수 있습니다.

API 파트너십

Dropbox는 많은 사람이 이용하는 소프트웨어와의 통합을 위해 다양한 파트너들과 긴밀하게 협력해 왔습니다. 타사 소프트웨어를 통합하면 원래 사용하던 기존의 인터페이스로 Dropbox에 보관된 데이터에 액세스할 수 있어 양쪽 서비스 사용자들의 경험이 더욱 원활해집니다.

- **모바일 및 웹용 Microsoft Office**

  Dropbox와 Microsoft Office를 통합하면 Dropbox에 저장된 Word, Excel, PowerPoint 파일을 열어보고 Office 모바일이나 웹 앱에서 파일을 수정할 수 있습니다. 또한, 파일의 변경 사항을 Dropbox에 바로 저장할 수 있습니다. 통합 후 Office 모바일 앱 또는 웹 앱에서 처음으로 Dropbox 파일을 열면 액세스 승인 여부를 묻는 메시지가 표시됩니다. 이후에 파일을 열 때는 연결 상태가 지속됩니다.

- **Adobe Acrobat과 Acrobat Reader**

  Dropbox에 Adobe Acrobat과 Acrobat Reader의 데스크톱 버전 및 모바일 버전(Android와 iOS)을 통합하면 Dropbox에 저장된 PDF를 보고, 편집하고, 공유할 수 있습니다. 통합 후 각 앱에서 처음으로 Dropbox 파일을 열면 액세스 승인 여부를 묻는 메시지가 표시됩니다. PDF 파일의 변경 사항은 Dropbox에 자동으로 저장됩니다.

- **AutoCAD**

  Dropbox와 Autodesk의 파트너십으로 전문가와 설계팀이 AutoCAD 데스크톱 애플리케이션을 떠나지 않고도 Dropbox에 저장된 AutoCAD 프로젝트 파일을 열어 작업을 진행할 수 있습니다. 변경 사항은 자동으로 Dropbox에 저장됩니다. 통합 후 AutoCAD 애플리케이션에서 처음으로 Dropbox 파일을 열면 액세스 승인 여부를 묻는 메시지가 표시됩니다.

네트워크 보안

Dropbox는 백엔드 네트워크의 보안을 철저히 유지합니다. Dropbox의 네트워크 보안 및 감시 기술은 여러 단계의 보호막과 방어막을 제공하도록 설계되었습니다. Dropbox는 방화벽과 네트워크 취약성 점검, 네트워크 보안 감시, 침입 탐지 시스템 등의 업계 표준 보호 기술을 적용해 악성이 아닌 적격 트래픽만 Dropbox의 인프라스트럭처에 접근할 수 있도록 합니다.

Dropbox의 내부 비공개 네트워크는 사용 현황과 위험 수준에 따라 세그먼트화됩니다. 주요 네트워크는 다음과 같습니다.

- 인터넷 방향 DMZ
- 우선순위 인프라스트럭처 DMZ
- 생산 네트워크
- 회사 네트워크

권한을 부여받은 IP 주소만이 생산 환경으로의 액세스가 허용되며 모든 엔드포인트에서 다요인 인증이 요구됩니다. 액세스 권한이 있는 IP 주소는 회사 네트워크 또는 승인된 Dropbox 직원의 것으로, Dropbox는 이러한 IP 주소를 분기별로 검토해 생산 환경의 보안을 유지합니다. IP 주소 변경에 대한 액세스는 권한을 부여받은 사람에게만 주어집니다.

생산 네트워크로 향하는 인터넷 트래픽은 여러 단계의 방화벽과 프락시로 보호됩니다.

내부 Dropbox 네트워크와 공공 인터넷 사이에는 엄격한 제한이 유지됩니다. 생산 네트워크를 오가는 인터넷 방향의 트래픽은 전용 프락시 서비스로 세심하게 통제되며, 그 결과 방화벽 제한 규정의 보호를 받습니다.

Dropbox는 정교한 도구로 Mac과 Windows 운영체제를 갖춘 노트북과 데스크톱 및 생산 시스템을 악성 이벤트로부터 감시합니다. 모든 보안 기록은 과학적 조사와 사고 대응을 위해 업계 표준 보존 정책을 따라 중앙에 저장됩니다.

Dropbox는 내부 보안팀과 외부 보안 전문가를 통해 정기적으로 네트워크 보안을 테스트하고 감사를 시행해 위험 요소를 파악하고 이를 경감합니다.

인터넷접속거점(POP)

Dropbox는 타사 콘텐츠전송네트워크(CDN)와 전 세계 20곳에 흩어져 있는 자체 호스팅 POP를 활용해 웹사이트 성능을 최적화합니다. 이 위치에서는 그 어떤 사용자 데이터도 캐시로 저장되지 않으며 전송 중인 모든 사용자 데이터는 SSL/TLS로 암호화됩니다. Dropbox가 호스팅하는 POP로의 물리적·논리적 액세스는 권한을 부여받은 Dropbox 직원에게만 주어집니다. Dropbox는 전송계층(TCP)과 응용계층(HTTP) 모두에 최적화를 수행합니다.

피어링(대등 접속)

Dropbox는 오픈 피어링 정책을 시행하고 있어 모든 고객이 Dropbox와 피어링을 할 수 있습니다. 자세한 내용은 dropbox.com/peering을 확인하세요.

취약성 관리

Dropbox의 보안팀은 정기적으로 자동/수동 애플리케이션 보안 테스트를 실시하고 타사 전문가들과 협력해 잠재적인 보안상 취약점과 버그를 파악하고 보완합니다.

이러한 테스트 결과는 보안팀 직원의 평가를 받으며, 보안팀의 평가에 따라 항목에 우선순위가 할당됩니다. Dropbox 정보 보안 관리 시스템의 필수 요소의 일환으로 테스트 결과 및 평가에 따른 권고사항은 Dropbox 경영진에 보고되고, 평가되며, 필요하다고 판단될 경우 적절한 조치가 취해집니다. 심각도가 높은 항목은 담당 보안 엔지니어가 기록하고, 추적하고, 해결합니다.

변경 관리

공식적인 변경 관리 정책은 생산 환경에 적용되기 전에 애플리케이션의 변경 사항이 승인을 받았는지 확인하기 위한 것으로, Dropbox 엔지니어링팀에 의해 개발되었습니다. 소스 코드의 변경은 Dropbox 애플리케이션과 서비스를 향상하고자 하는 개발자들이 주도합니다. 변경 사항은 버전 관리 시스템에 저장되며 자동화된 버전 관리(QA) 테스트 절차를 거쳐 보안 요건이 충족되었는지를 확인받아야 합니다. QA 절차의 성공적인 완료는 변경 사항의 적용으로 이어집니다. QA를 통과한 변경 사항은 자동으로 생산 환경에 적용됩니다. Dropbox의 소프트웨어개발수명주기(SDLC)에 따라 개발자는 안전한 코딩 지침을 준수하고, Dropbox의 QA와 수동 검토 프로세스를 통해 잠재적인 보안 문제에 대한 코드 변경을 검토해야 합니다

변경 사항이 배포 환경에 적용되면 Dropbox 엔지니어링팀 임원들에게 자동으로 경보가 발송되며 이러한 변경 사항은 기록되고 보관됩니다.

Dropbox 인프라스트럭처를 변경할 수 있는 권한은 승인된 Dropbox 직원에게만 주어집니다. Dropbox 보안팀은 인프라스트럭처의 보안을 유지하고, 서버와 방화벽, 기타 보안 관련 구성을 업계 기준에 맞춰 최신으로 유지하는 역할을 합니다. Dropbox는 주기적으로 방화벽 규정과 실서버에 액세스할 수 있는 직원들을 검토합니다.

스캔 및 보안 침투 테스트(내부 및 외부)

Dropbox의 보안팀은 정기적으로 자동화된 수동 애플리케이션 보안 테스트를 실시해 데스크톱, 웹(Dropbox 및 Paper), 모바일(Dropbox 및 Paper) 애플리케이션의 잠재적인 보안상 취약점과 버그를 파악하고 보완합니다.

또한, 타사 공급업체와 계약을 맺고 기업 환경과 생산 환경에 대한 보안 침투 및 취약성 테스트를 주기적으로 시행합니다. Dropbox는 타사 전문가들과 기타 업계 보안팀, 보안 연구 커뮤니티와 협력해 애플리케이션을 안전하게 보호합니다.

또한, Dropbox는 자동 분석 시스템을 통해 취약성 요인을 탐색합니다. 이러한 분석 시스템에는 자체적으로 개발한 시스템과 Dropbox의 특성에 맞춰 변경한 오픈 소스 시스템, 지속적인 자동 분석을 위해 고용한 외부 공급업체가 포함됩니다.

버그 현상금

Dropbox는 전문적인 기업과 협력해 침투 테스트와 자체 테스트를 시행할 뿐 아니라 광범위한 보안 관련 커뮤니티의 전문성을 빌어 버그 현상금 프로젝트(또는 보안 취약점 보상 프로그램)도 진행하고 있습니다. Dropbox의 버그 현상금 프로그램은 책임감을 가지고 소프트웨어의 버그를 신고하는 사람들에게 사례를 제공해 신고된 정보를 한 곳으로 집중합니다. 이러한 외부 커뮤니티의 참여는 Dropbox 보안팀이 애플리케이션을 더욱 철저하게 검토하는 계기로 작용해 보안 강화에 도움이 됩니다. Dropbox는 대응과 해결 시간뿐 아니라 사례금 영역에서도 업계 최고가 되기 위해 노력하고 있습니다.

Dropbox는 적격한 신고 요건과 Dropbox 애플리케이션, 버그 발견 및 보안 취약점의 신고를 촉진하고 사용자 보안을 향상하는 책임감 있는 공개 정책의 범위를 규정하고 있습니다. 정책에는 다음과 같은 지침이 포함됩니다.

- Dropbox에 보안 문제를 상세하게 전달해야 합니다
- 보안 문제를 대중에 공개하기 전에 Dropbox에 충분한 대응 시간을 줘야 합니다
- 계정 소유자의 승인 없이 사용자 데이터에 액세스하거나 데이터를 변경하면 안 됩니다
- Dropbox 서비스의 성능을 폄하하지 않아야 합니다(서비스 거부 포함)

보안 문제 신고는 HackerOne(hackerone.com/dropbox)에서 할 수 있습니다.

Dropbox 정보 보안

Dropbox는 정보 보안 관리 체계를 설립해 Dropbox의 신뢰 유지에 관한 목적과 방향, 원칙, 기본 규정을 명시해 놓고 있습니다. 고객과의 신뢰를 유지하려면 위험 요소를 평가하고 지속적으로 보안, 기밀성, 무결성, 가용성, Dropbox Business 시스템의 개인정보 보호 정책을 향상해야 합니다. Dropbox는 정기적으로 보안 정책을 업데이트·검토하고, 보안 관련 교육을 제공하며, 침투 테스트를 비롯해 애플리케이션과 네트워크 보안에 대한 테스트를 시행합니다. 또한, 보안 정책 준수 현황을 감사하고 내외부적으로 위험성 평가를 시행합니다.

Dropbox의 정책

Dropbox는 정보 보안, 개인정보 보호, 물리적 보안, 사고 대응, 업무 연속성, 논리적 액세스, 물리적 생산 액세스, 변경 관리, 영업 및 고객 경험을 아우르는 자세한 보안 정책을 마련해 놓았습니다. 이 정책은 적어도 1년에 1번씩 검토와 승인을 거치며 Dropbox 보안팀에 의해 집행됩니다. 모든 직원과 인턴, 하청업체는 업무를 시작하기에 앞서 필수 보안 교육을 받아야 하고, 정기적으로 보안 인식 교육을 받습니다.

- **정보 보안**

  장치 보안, 인증 요건, 데이터 및 시스템 보안, 사용자 정보 보호, 직원들의 자료 사용에 관한 지침 및 제한, 잠재적 문제 처리 등 사용자와 Dropbox 정보에 관련된 정책

- **사용자 정보 보호**

  개인정보 보호 정책 준수를 위해 Dropbox가 개인정보를 보호하고 처리할 때 따라야 할 요건

- **물리적 보안**

  인력과 시설의 보호를 위해 Dropbox가 안전한 환경을 유지하는 방식(아래의 물리적 보안 섹션 참조)

- **사고 대응**

  평가, 소통, 조사 절차 등 잠재적인 보안 사고에 대응할 때 따라야 할 요건

- **논리적 액세스**

  기업 환경, 생산 환경에 대한 액세스 등 Dropbox의 시스템, 사용자 정보, Dropbox 정보의 보안을 유지하기 위한 정책

- **물리적 생산 액세스**

  직원 경영 감사, 해고된 직원의 승인 철회 등 물리적 생산 네트워크 액세스를 제한하는 절차

- **변경 관리**

  승인된 개발자들이 시행하는 애플리케이션 소스 코드, 시스템 구성, 제품 릴리스 등 보안에 영향을 주는 코드 검토 및 변경 사항 관리에 관한 정책

- **영업 및 고객 경험**

  계정 보기, 지원 제공, 조치 시행과 관련된 지원팀의 사용자 메타데이터 액세스 정책

- **업무 연속성**

  계획에서부터 기록, 집행에 이르기까지 운영 중단 시 주요 업무 기능을 유지하고 복구하는 것에 관한 정책과 절차

- **위기 관리**

  주요 운영 기능이 중단되거나 전략 목표를 위협하는 전방위적 이벤트가 발생했을 때 Dropbox가 이를 처리하는 방법에 관한 정책과 절차

직원 정책 및 액세스

Dropbox의 직원은 입사 시 신원 조사를 완료하고 보안 정책 확인서와 기밀 유지 협약에 서명하고, 보안 교육을 받아야 합니다. 직무상 책임에 규정된 바에 따라 이러한 절차를 완료한 직원만이 기업 및 배포 환경에 대한 물리적·논리적 액세스를 제공받을 수 있습니다. 또한, 모든 직원은 연간 보안 교육을 받아야 하며, 정보성 이메일과 강연, 프레젠테이션, 인트라넷에 있는 자료를 통해 정기적인 보안 인식 교육을 받습니다.

직원들의 Dropbox 환경 액세스는 중앙 디렉터리에서 관리되며, 강력한 암호와 패스프레이즈 암호가 설정된 SSH 키, 2단계 인증, OTP 토큰을 거쳐 인증됩니다. 원격으로 액세스하려면 2단계 인증이 설정된 VPN을 사용해야 하고, 모든 특수한 액세스는 보안팀에 의해 검토·심사됩니다.

회사 네트워크와 생산 네트워크로의 액세스는 규정된 정책에 따라 엄격하게 제한됩니다. 예를 들어, 생산 네트워크에 대한 액세스는 SSH 키 기반 인증을 받아야 하며, 업무상 액세스가 필요한 엔지니어링팀만이 이 네트워크에 액세스할 수 있습니다. 방화벽 환경 설정은 소수의 관리자만이 액세스할 수 있고, 이들에 의해 철저하게 관리됩니다.

또한, Dropbox의 내부 정책에 따라 배포 환경과 기업 환경에 액세스하는 직원은 SSH 비공개 키의 생성 및 저장에 관한 우수 사례를 따라야 합니다.

데이터 센터, 서버 환경 설정 지원 프로그램, 실서버, 소스 코드 개발 지원 프로그램 등의 기타 리소스에 액세스하려면 관련 경영진의 명시적 승인을 받아야 합니다. 액세스 요청, 정당성, 승인에 관한 기록은 경영진에 의해 기록되며, 여기에 액세스하려면 관련 직원의 승인을 받아야 합니다.

Dropbox는 기술적 액세스 제어와 내부 정책을 적용해 직원들이 임의로 사용자 파일에 액세스하는 것을 금지하고, 사용자 계정에 관한 메타데이터와 기타 정보에 액세스하는 것을 제한합니다. 사용자의 개인정보 보호와 보안을 위해 사용자 파일이 저장된 환경으로의 액세스는 Dropbox의 핵심 서비스를 개발하는 소수의 엔지니어에게만 허용됩니다. 퇴사한 직원의 액세스는 퇴사 즉시 삭제됩니다.

기존의 인프라를 Dropbox와 통합하면 Dropbox가 데이터를 책임지고 보호한다는 점에서 안심할 수 있습니다. 더욱 자세한 내용은 아래의 개인정보 보호 섹션을 참조하세요.

물리적 보안

인프라스트럭처

생산 시스템이 위치한 하청서비스 시설로의 물리적 액세스는 직무상 역할 수행에 필요해 Dropbox로부터 승인을 받은 직원에게만 주어집니다. 생산 환경 시설로의 추가적인 액세스가 필요한 경우 해당 직원은 관련 경영진의 명시적 승인을 받아야 합니다.

액세스 요청, 정당성, 승인에 관한 기록은 경영진에 의해 기록되며, 여기에 액세스하려면 관련 직원의 승인을 받아야 합니다. 승인을 받은 후에는 권한이 있는 인프라스트럭처팀 직원이 해당 하청서비스 조직에 연락해 승인된 직원의 액세스를 요청합니다. 하청서비스 조직은 사용자 정보를 자체 시스템으로 입력한 후 승인된 Dropbox 직원에게 배지 액세스와 가능한 경우 생채 인증 액세스를 제공합니다. 액세스가 승인된 후에는 생산 환경 시설로의 액세스를 승인된 사람들에게만 제한하는 것에 대한 책임은 데이터 센터에 있습니다.

기업 사무실

- **물리적 보안**

  물리적 보안 정책을 집행하고 Dropbox 사무실의 보안을 감독하는 역할은 Dropbox의 물리적 보안팀이 담당합니다.

- **방문자 및 액세스 정책**

  공공 출입구와 로비 이외의 기업 시설에 대한 물리적 액세스는 승인된 Dropbox 직원과 Dropbox 직원과 동행하는 등록한 방문객으로 제한됩니다. Dropbox는 배지 액세스 시스템을 시행해 승인된 사람만 기업 시설 내 제한된 구역에 액세스하도록 허용하고 있습니다.

- **서버 액세스**

  기업 서버와 네트워크 장치가 있는 구역으로의 액세스는 배지 액세스 시스템을 통해 승인받은 고위직으로부터 권한을 부여받은 직원으로 제한됩니다. 기업 환경 및 생산 환경으로의 물리적 액세스를 승인받은 직원의 목록은 최소 분기별로 1번씩 검토됩니다.

규정 준수

기업에 적용될 수 있는 규정 준수 기준에는 여러 가지가 있습니다. Dropbox는 가장 흔히 통용되는 표준과 고객의 비즈니스나 산업에 특화된 규정 준수 방안을 결합해 기업의 규정 준수를 지원합니다.

ISO

국제표준화기구(ISO)는 세계 최고 수준의 정보 및 사회 안보 관련 표준을 개발해 조직들이 신뢰할 수 있고 혁신적인 제품과 서비스를 개발하는 것을 지원합니다. Dropbox는 네덜란드에 위치한 독립적인 외부 감사기관 EY CertifyPoint의 감사를 통해 데이터 센터와 시스템, 애플리케이션, 직원, 프로세스를 인증받았습니다. EY CertifyPoint는 Raad voor Accreditatie(네덜란드 인증 위원회)로부터 ISO 인가를 취득했습니다.

ISO 27001(정보 보안)

ISO 27001은 세계 최고의 정보보호관리체계(ISMS) 표준 인증으로 인정받고 있습니다. 이 인증에는 ISO 27002에 자세하게 설명된 보안 우수 사례도 포함되어 있습니다. Dropbox는 고객의 신뢰에 보답하기 위해 끊임없이 Dropbox의 물리적, 기술적, 법적 제어를 철저하게 관리하고 있습니다.

Dropbox Business와 Dropbox Education의 ISO 27001 인증 보기

ISO 27017(클라우드 보안)

ISO 27017은 프로비전과 클라우드 사용 관련 보안 통제에 대한 지침을 제공하는 클라우드 보안 부문 국제 표준 인증입니다. Dropbox의 공동 책임 안내서에 Dropbox와 고객이 함께 해결할 수 있는 보안, 개인정보 보호, 규정 준수 요건 중 일부가 설명되어 있습니다.

Dropbox Business와 Dropbox Education의 ISO 27017 인증 보기

ISO 27018 (클라우드 개인정보 및 데이터 보호)

ISO 27018은 Dropbox처럼 고객을 대신해 개인 정보를 처리하는 클라우드 서비스 공급업체에 적용되는 개인정보 및 데이터 보호 부문 국제 표준 인증입니다. 이 인증은 고객이 규제나 계약상에 관한 일반적 규정이나 문의에 대처할 수 있는 근거를 제시합니다.

Dropbox Business와 Dropbox Education의 ISO 27018 인증 보기

ISO 22301(업무 연속성)

ISO 22301은 잠재적인 위험을 최소화함으로써 운영이 중단됐을 때 비즈니스에 끼치는 영향을 줄이고, 운영 중단 시 이에 적절하게 대응하는 방법을 안내하는 업무 연속성 부문 국제 표준 인증입니다. Dropbox는 위기 상황 속에서 비즈니스 운영과 직원을 보호하기 위한 통합 위기관리 전략의 일환으로 업무연속성관리체계(BCMS)를 갖추고 있습니다.

Dropbox Business와 Dropbox Education의 ISO 22301 인증 보기

SOC

SOC 1, SOC 2, SOC 3으로 알려진 서비스조직통제(SOC) 보고서는 미국공인회계사협회(AICPA)가 조직 내에서 시행되는 내부 통제 신고를 위해 개발한 프레임워크입니다. Dropbox는 독립적인 외부 감사기관 Ernst & Young LLP의 감사를 통해 시스템과 애플리케이션, 직원, 프로세스에 대한 신뢰성을 입증받았습니다.

보안, 기밀성, 무결성, 가용성, 개인정보 보호에 대한 SOC 3

SOC 3 검증 보고서는 보안, 기밀성, 무결성, 가용성, 개인정보 보호로 구성된 5대 신뢰 서비스 원칙을 모두 다룹니다(TSP 섹션 100). Dropbox의 일반 사용 보고서는 SOC 2 보고서에 관한 종합적인 개요로, 실용적인 디자인과 운영상 통제에 관한 독립적인 외부 감사기관의 의견을 포함하고 있습니다.

Dropbox Business와 Dropbox Education의 SOC 3 검증 보기

보안, 기밀성, 무결성, 가용성, 개인정보 보호에 대한 SOC 2

SOC 2 보고서는 보안, 기밀성, 무결성, 가용성, 개인정보 보호로 구성된 5대 신뢰 서비스 원칙을 모두 다루며, 고객에게 통제에 관한 상세한 검증 결과를 제공합니다(TSP 섹션 100). SOC 2 보고서에는 Dropbox가 고객의 자료를 보호하기 위해 실행 중인 프로세스와 100개 이상의 통제 기능이 상세하게 설명되어 있습니다. 또한, 실용적인 디자인과 운영상 통제에 관한 독립적인 외부 감사기관의 의견에 더불어 감사기관의 테스트 절차와 각 통제 기능에 대한 감사 결과가 포함되어 있습니다. SOC 2 보고서(또는 SOC 2+ 보고서)에는 위에 언급된 ISO 국제 표준에 대한 Dropbox의 통제 현황을 감사한 결과도 설명되어 있어 고객에게 한층 강화된 투명성을 제공합니다. Dropbox Business와 Dropbox Education에 대한 SOC 2 검증 보고서는 요청 시 확인할 수 있습니다.

SOC 1 / SSAE 18 / ISAE 3402 (구 SSAE 16 또는 SAS 70)

SOC 1 보고서는 Dropbox Business 또는 Dropbox Education을 기업 내부재무보고관리(ICFR) 프로그램의 핵심 요소로 여기는 고객에게 상세한 검증 결과를 제공합니다. 이 검증 결과는 특히 사베인스-옥슬리법(SOX)을 준수해야 하는 Dropbox 고객에게 유용합니다. 독립적인 외부 감사기관의 감사는 기존의 SSAE 16과 SAS 70을 대체하는 SSAE 18과 ISAE 3402, SAS 70에 따라 시행됩니다. Dropbox Business와 Dropbox Education에 대한 SOC 1 검증 보고서는요청 시 확인할 수 있습니다.

클라우드 시큐리티 얼라이언스: 보안, 신뢰, 보장 레지스트리(CSA STAR)

CSA의 보안, 신뢰, 보장 레지스트리(STAR)는 클라우드 서비스에 보안 보장 프로그램을 제공하는 무료 공개 레지스트리로, 이를 통해 현재 이용 중이거나 이용을 고려 중인 서비스 제공업체의 보안 현황을 확인할 수 있습니다.

Dropbox Business와 Dropbox Education은 CSA START 레벨 2 인증과 레벨 2 증명을 받았습니다. CSA START 레벨 2를 획득하려면 ISO 27001과 SOC 2 신뢰 서비스 원칙, CSA Cloud Controls Matrix(CCM) v.3.0.1의 요건에 따라 독립적인 외부 감사기관 EY CertifyPoint와(인증 부문) Ernst & Young LLP(증명 부문)의 평가를 거쳐야 합니다. Dropbox는 Dropbox Business와 Dropbox Education의 CSA STAR 레벨1 자체 평가도 완료했습니다. 이 자체 평가는 CCA 기준에 부합하는 Consensus Assessments Initiative Questionnaire(CAIQ)를 토대로 한 CSA의 까다로운 설문 조사로, 클라우드 서비스 이용 고객과 클라우드 보안 감사기관이 궁금해하는 300여 개의 질문에 답변을 제공해야 합니다.

CSA 웹사이트에서 CSA STAR 레벨 1 자체 평가와 레벨 2 인증 및 증명 보기

HIPAA/HITECH

Dropbox는 Dropbox Business 또는 Dropbox Education 고객이 Health Insurance Portability and Accountability Act(HIPAA)와 Health Information Technology for Economic and Clinical Health Act(HITECH) 규정 준수의 일환으로 Business Associate Agreement(BAA)를 필요로 할 경우 BBA를 작성하고 있습니다.

Dropbox는 Dropbox Business 또는 Dropbox Education을 통해 HIPAA/HITECH 보안 및 개인정보 보호 규정의 요건을 충족하려는 고객에게 HIPAA/HITECH 보안, 개인정보 보호, 개인정보 침해 통보 규정에 대한 Dropbox의 통제 현황에 더불어 다양한 내부 사례와 권장 사항을 제공합니다.

이와 같은 문서를 요청하거나 Dropbox Business 또는 Dropbox Education 구매에 대해 더욱 자세한 내용을 알고 싶다면 Dropbox 영업팀으로 문의할 수 있습니다. 현재 Dropbox Business나 Dropbox Education의 팀 관리자인 경우, 관리 콘솔 내 계정 페이지에서 전자 BAA를 작성할 수 있습니다. 더욱 자세한 내용은 HIPAA 시작하기 안내서를 참조하세요.

현재 Dropbox Paper를 사용하지 않는 미국 거주 고객만 관리 콘솔에서 전자 BAA를 작성할 수 있다는 점 참조하시기 바랍니다. Dropbox Paper에는 HIPAA/HITECH 지원이 제공되지 않습니다.

독일 BSI C5 증명 보고서

Cloud Computing Compliance Controls Catalog(C5)는 독일 연방정보보안청(BSI)이 클라우드 서비스 프로비전과 관련된 보안 통제 신고를 위해 개발한 프레임워크입니다. C5 증명은 조직이 정보 보안 사례를 입증해 BSI의 '클라우드 공급업체를 위한 보안 권장 사항'을 준수하도록 도와줍니다. C5는 ISO 27001, CSA STAR 등 현존하는 국제 보안 표준을 토대로 개발되었습니다. Dropbox는 독일에 위치한 독립적인 외부 감사기관 Ernst & Young GmbH로부터 시스템과 프로세스, 통제 기능을 인증받아 C5 증명 보고서를 취득했습니다. 외부 기관의 감사는 International Standard on Assurance Engagements No. 3000(ISAE 3000)에 따라 수행됩니다.

이 보고서에는 Dropbox의 시스템, 애플리케이션, 프로세스, 통제 기능뿐 아니라 외부 감사기관의 테스트 절차 및 각 통제 기능에 대한 감사 결과가 상세하게 설명되어 있습니다. Dropbox Business와 Dropbox Education에 대한 C5 보고서는 요청 시 확인할 수 있습니다.

Dropbox Paper는 C5 보고서 범위에 포함되어 있지 않은 점 참조하시기 바랍니다.

학생 및 아동(FERPA 및 COPPA)

Dropbox Business와 Dropbox Education의 고객은 미국 가족교육권리 및 개인정보법(FERPA)에 따른 공급업체의 의무를 준수하며 서비스를 이용할 수 있습니다. 부모로부터 서비스 이용에 관한 동의를 얻어야 하는 계약상 조항에 동의할 경우, 만 13세 이하의 학생들을 가르치는 교육기관도 어린이온라인사생활보호법(COPPA)을 준수하며 Dropbox Business 또는 Dropbox Education을 이용할 수 있습니다.

영국 디지털 마켓플레이스 G-클라우드

Dropbox Business는 영국 디지털 마켓플레이스 정부 클라우드 서비스 부문에 등록되어 있습니다. 영국 디지털 마켓플레이스 웹사이트에서 Dropbox Business Standard 요금제와 Dropbox Business Advanced 요금제, Dropbox Enterprise 요금제를 확인하세요.

Dropbox Paper는 영국 디지털 마켓플레이스 G-클라우드 목록에 포함되어 있지 않은 점 참조하시기 바랍니다.

PCI DSS

Dropbox는 지불카드보안표준(PCI DSS)을 준수하는 업체이지만, Dropbox Business와 Dropbox Education, Dropbox Paper는 신용카드 거래를 처리하거나 저장하지 않습니다. Dropbox의 업체 상태에 대한 PCI규정준수증명(AoC)은 요청 시 확인할 수 있습니다.

Dropbox Business와 Dropbox Education의 규정 준수에 관한 자세한 정보

Dropbox.com/business/trust/compliance 방문하기

개인정보 보호

많은 고객과 조직이 매일 Dropbox에서 중요한 업무를 처리합니다. 그리고 이러한 정보를 보호하고 비공개로 유지하는 것은 Dropbox의 책임입니다.

개인정보 보호 정책

Dropbox의 개인정보 보호 정책은 dropbox.com/privacy에서 확인할 수 있습니다. Dropbox의 개인정보 보호 정책과 업무 협약, 서비스 약관, 사용 제한 정책에는 다음과 같은 약관이 명시되어 있습니다.

- 수집하는 데이터의 유형과 데이터 수집 이유
- 정보 공유 대상
- 데이터 보호 방식 및 데이터 보관 기간
- 데이터를 저장하고 전송하는 장소
- 정책 변경 또는 고객 문의 절차

ISO 27018

Dropbox Business는 주요 클라우드 서비스 공급업체 중 최초로 개인정보 및 데이터 보호 부문 국제 표준인 ISO 27018 인증을 받은 업체 중 하나입니다. 2014년 8월에 발표된 ISO 27018은 개인정보 및 데이터 보호를 위해 특별히 설계되었습니다. 이 표준은 Dropbox가 조직의 정보를 사용하는 경우와 사용하지 않는 경우에 관한 다양한 요건을 제시합니다.

- **사용자 데이터에 대한 통제권은 조직이 갖고 있습니다.**

  Dropbox는 사용자가 제공한 개인 정보만을 사용해 사용자에 필요한 서비스를 제공합니다. 사용자는 필요에 따라 Dropbox에 있는 파일과 Paper 문서를 추가하고, 수정하고, 삭제할 수 있습니다.

- **Dropbox는 사용자의 데이터를 투명하게 사용합니다.**

  Dropbox는 사용자의 데이터가 어느 서버에 저장되어 있는지 투명하게 공개합니다. 사용자는 Dropbox와 협력하는 파트너가 누구인지 알 수 있고, 계정을 닫거나 파일/Paper 문서를 삭제했을 때 어떤 일이 생기는지 알 수 있습니다. 마지막으로, 이 중 하나라도 변경될 경우 Dropbox는 사용자에게 변경된 내용을 통보합니다.

- **사용자의 데이터가 안전하게 보호됩니다.**

  ISO 27018은 전 세계에서 가장 흔히 통용되는 정보 보안 표준인 ISO 27001을 보완합니다. Dropbox는 2014년 10월에 ISO 27001 인증을 취득했으며, ISO 27018에 명시된 암호화, 강력한 직원 액세스 제어 등의 보안 및 개인정보 보호 요건은 ISO 27001과 맥락을 같이합니다.

- **Dropbox의 운영 방식을 확인할 수 있습니다.**

  Dropbox는 ISO 27018 및 ISO 27001 규정 준수의 일환으로 매년 독립적인 외부 기관의 감사를 받아 인증을 유지할 것입니다. Dropbox의 ISO 27018 인증은 여기 에서 확인할 수 있습니다.

투명성

Dropbox는 사용자 정보에 관한 법률 집행 요청과 유사한 성격의 모든 요청을 처리하는 데 있어 투명성을 유지할 것을 약속합니다. Dropbox는 모든 데이터 요청을 면밀히 검토해 이러한 요청이 적법한 것인지 확인하며, 법이 허용하는 한 법률 집행 요청에 포함된 계정의 소유주에게 이 사실을 통보할 것을 약속합니다.

이러한 노력은 사용자의 개인정보와 데이터를 지키겠다는 Dropbox의 헌신을 명백히 보여줍니다. 이를 위해 Dropbox는 정부의 정보 요청에 대한 원칙을 세우고, 투명성 보고서를 꾸준히 관리하고 있습니다. 다음의 원칙은 정부의 정보 요청을 받았을 때와 이를 검토할 때, 이에 대응할 때 Dropbox가 따라야 할 행동을 규정합니다.

- **투명성 유지**

  Dropbox는 온라인 서비스가 정부로부터 받은 개인정보 요청 횟수와 유형을 공개하는 것을 허용해야 한다고 믿습니다. 또한, 정보 요청 대상에게 이 사실을 통보하는 것이 옳다고 생각합니다. 이러한 투명성은 사용자가 정부의 지나친 요청 사례와 패턴을 인지하도록 함으로써 사용자에게 권한을 부여합니다. Dropbox는 계속해서 이러한 요청에 관한 자세한 정보를 공개하고, 이 중요한 정보를 더 자세하게 제공할 권리를 지지할 것입니다.

- **광범위한 요청에 대한 투쟁**

  정부의 개인정보 요청은 특정한 인물과 적법한 조사로 제한되어야 합니다. Dropbox는 지나치게 광범위한 전면적인 요청을 거절할 것입니다.

- **모든 사용자 보호**

  거주지나 국적에 따라 가지각색의 보호를 제공하는 법은 낡은 법이며, 전 세계에 적용되는 온라인 서비스의 본질을 반영하지 못한 것입니다. Dropbox는 이러한 낡은 법의 개혁을 계속해서 지지할 것입니다.

- **신뢰할 수 있는 서비스 제공**

  정부는 온라인 서비스 공급업체에 백도어 프로그램을 설치하거나, 사용자 데이터를 입수하기 위해 업체의 인프라스트럭처를 침투해서는 안 됩니다. Dropbox는 계속해서 Dropbox의 시스템을 보호하고, 이러한 정부의 활동이 불법이라는 것이 법에 분명하게 명시될 수 있도록 노력할 것입니다.

Dropbox의 투명성 보고서는 dropbox.com/transparency에서 확인할 수 있습니다.

EU-미국 프라이버시 실드 및 스위스-미국 프라이버시 실드

Dropbox는 유럽연합과 유럽경제지역, 스위스에서 데이터를 전송할 때 사용자와 Dropbox 간에 맺은 계약서를 포함한 다양한 합법적 방법을 사용합니다. Dropbox는 유럽연합, 유럽경제지역, 스위스에서 미국으로 전송된 개인정보의 수집·사용·보관에 있어 미국 상무부의 규정에 따라 EU-미국 프라이버시 실드와 스위스-미국 프라이버시 실드를 준수합니다. Dropbox의 프라이버시 실드 인증은 www.privacyshield.gov/list에서 확인할 수 있습니다. 프라이버시 실드에 대해 더욱 자세한 내용을 알고 싶다면 www.privacyshield.gov을 참조하세요.

프라이버시 실드 원칙의 준수는 조직이 EU 데이터 보호 규정에 따라 충분한 개인정보 보호 정책을 제공하도록 보장합니다. Dropbox의 프라이버시 실드 준수와 관련된 고소 및 분쟁은 독립적인 외부 기관 JAMS가 조사와 해결을 담당합니다. 더욱 자세한 내용은 Dropbox의 개인정보 보호 정책(dropbox.com/privacy)을 참조하세요.

EU 개인정보 보호 규정(GDPR)

개인정보 보호 규정 2016/679(GDPR)은 유럽연합 내 거주자의 개인정보 처리에 관한 기존의 프레임워크를 대폭 수정한 유럽연합의 새로운 개인정보 보호 규정입니다. GDPR에는 Dropbox처럼 개인정보를 처리하는 기업에 적용되는 강력한 규정이 새롭게 도입되었습니다. GDPR은 기존의 EU 개인정보보호지침(EU Directive 95/46 EC)을 대체하며 2018년 5월 25일을 기점으로 시행됩니다. Dropbox는 다른 책임감 있는 기업과 마찬가지로 계속해서 자세한 GDPR 규정 준수 계획을 세우고 집행할 것이며, 2018년 5월 25일 이전에 모든 규정을 완벽하게 준수할 것입니다. 더욱 자세한 내용은 dropbox.com/security/GDPR를 참조하세요.

Dropbox의 개인정보 보호 사례와 정책에 관한 자세한 내용은 개인정보 및 데이터 보호 백서를 참조하세요.

Dropbox 신뢰 프로그램

신뢰는 Dropbox가 전 세계 수백만 고객과의 관계를 이루는 토대입니다. Dropbox는 고객의 신뢰를 소중히 여기며 사용자의 정보를 보호하는 것에 대한 책임을 중히 받아들입니다. 사용자의 신뢰에 보답하기 위해 우리는 보안과 규정 준수, 개인정보 보호에 중점을 두고 Dropbox를 구축했고, 앞으로도 같은 방향으로 성장해 나갈 것입니다.

Dropbox 신뢰 프로그램 정책은 환경적, 물리적, 사용자, 외부 업체, 관련 법률 및 규정, 계약상 요건, 이외에 시스템 보안과 기밀성, 무결성, 가용성, 개인정보 보호에 영향을 줄 수 있는 위험 요소를 다루는 위험성 평가 프로세스를 규정합니다. Dropbox는 이와 관련된 수행 평가를 최소 1년에 1번씩 시행하고 있습니다. Dropbox 신뢰 프로그램에 관한 자세한 내용은 dropbox.com/business/trust를 참조하세요.

요약

Dropbox Business는 조직에 필요한 규정 준수 인증과 보안 조치에 더불어 팀의 효율적인 협업을 지원하는 쉽고 간편한 도구를 제공합니다. Dropbox는 활발한 백엔드 인프라스트럭처와 맞춤형 정책을 결합한 다층적 접근 방식으로 필요에 따라 맞춤형으로 설계할 수 있는 강력한 솔루션을 제공합니다. Dropbox Business에 관한 자세한 내용은 Dropbox 영업팀(sales@dropbox.com)에 문의하세요.