개인정보 취급 및 데이터 보호의 공통 고려사항을 반영한 AWS 사용

2016 년 12 월

(이 백서의 최신 버전은 https://aws.amazon.com/compliance/resources/를 참조하십시오.)

개요

본 문서는 고객이 AWS를 사용하여 개인정보가 포함된 콘텐츠를 저장하거나 처리하려고 할 때 개인정보 취급 및 데이터 보호에 관한 공통적인 고려사항을 제공합니다.

고객은 본 문서를 참조하여 다음을 이해할 수 있습니다.

- 고객이 보안 문제를 해결하고 콘텐츠를 암호화하는 방법을 비롯한 AWS 서비스 운영 방식
- 고객이 콘텐츠 및 기타 관련 고려사항을 저장할 때 선택할 수 있는 지리적 위치
- AWS 서비스에 저장된 콘텐츠를 관리하고 보호할 때 고객 및 AWS가 각기 수행하는 개별 역할

아시아 태평양 지역과 유럽 연합의 여러 국가에서 적용되는 개인정보 취급방침 및 데이터 보호 고려사항에 대해 더욱 구체적인 논의가 담긴 백서는 **http://aws.amazon.com/compliance/**에서 확인할 수 있습니다.

범위

본 백서는 AWS 고객이 개인정보가 포함된 콘텐츠를 저장하거나 처리하기 위해 AWS 서비스를 이용할 경우, 이와 관련된 개인정보 취급 및 데이터 보호에 관한 공통적인 요구 사항을 중점적으로 다룹니다. 또한 각 고객이 해결해야 할 다른 관련 고려사항도 다루고 있습니다. 예를 들어 고객은 산업별 요구 사항, 고객이 비즈니스를 수행하는 관할 법률 또는 고객이 제3자와 맺은 계약을 준수해야 합니다.

이 백서는 정보 제공 목적으로만 제공됩니다. 법률 자문서가 아니며 법률 자문으로 간주해서는 안 됩니다. 각 고객의 요구 사항이 다르므로 AWS는 고객이 개인정보 취급 및 데이터 보호 요구 사항의 이행에 대한 적절한 조언과 함께, 비즈니스와 관련된 법률 및 기타 요구 사항에 대해 적절한 조언을 얻을 것을 권장합니다.

이 백서에서 언급된 콘텐츠는 고객 또는 최종 사용자가 AWS 서비스를 사용하여 저장하거나 처리하는 소프트웨어(가상 컴퓨터 이미지 포함), 데이터, 텍스트, 오디오, 비디오, 이미지 및 기타 콘텐츠를 의미합니다. 예를 들어 고객의 콘텐츠에는 고객이 Amazon Simple Storage Service를 사용하여 저장하는 객체, Amazon Elastic Block Store 볼륨에 저장된 파일 또는

Amazon DynamoDB 데이터베이스 테이블의 콘텐츠가 포함됩니다. 이러한 콘텐츠에는 해당 고객, 최종 사용자 또는 제3자와 관련된 개인정보가 포함될 수 있지만 반드시 그런 것은 아닙니다. AWS 고객 계약 또는 AWS 서비스의 사용을 규정하는 당사와의 기타 관련 계약 조건이 고객 콘텐츠에 적용됩니다. 고객 콘텐츠에는 AWS 계정의 생성 또는 관리와 관련하여 고객이 제공한 데이터(예: 고객의 이름, 전화번호, 이메일 주소 및 청구 정보)가 포함되어 있지 않습니다. AWS에서는 이러한 정보를 계정 정보로써 참조하며 해당 정보는 AWS 개인정보 취급방침에 의해 관리됩니다.

고객 콘텐츠: 개인정보 취급방침 및 데이터 보호 관련 고려사항

콘텐츠를 저장하려는 모든 조직은 다음과 같이 실제 여러가지 사항을 고려해야 합니다.

- 콘텐츠가 안전합니까?
- 콘텐츠는 어디에 저장됩니까?
- 콘텐츠에 접근할 수 있는 사람은 누구입니까?
- 콘텐츠에 적용되는 법률 및 규정은 무엇이며 해당 법률 및 규정을 준수하는 데 필요한 사항은 무엇입니까?

이러한 고려사항은 새로운 내용이 아니며 클라우드에 한정된 내용도 아닙니다. 내부에서 호스팅 및 운영되는 시스템은 물론 기존의 제3자 호스팅 서비스와도 관련이 있습니다. 각 고려사항은 타사 장비 또는 타사 자체구축 서비스에 저장되며 타사 직원이 관리, 접근 또는 사용하는 콘텐츠와 관련이 있을 수 있습니다. AWS 서비스를 사용할 경우 각 AWS 고객은 다음에 대한 통제를 비롯하여 콘텐츠의 소유권 및 통제권을 보유합니다.

- AWS 서비스를 사용하여 저장하거나 처리하도록 선택하는 콘텐츠
- 콘텐츠 저장 및 처리를 위해 사용하는 AWS 서비스
- 콘텐츠가 저장되는 AWS 리전
- 마스킹, 익명 또는 암호화 처리 여부를 비롯한 콘텐츠의 형식, 구조 및 보안
- AWS 계정 및 콘텐츠에 대한 접근 권한을 가진 사람 및 해당 접근 권한의 부여, 관리 및 취소 방법

AWS 고객은 AWS 환경 내에서 소유권 및 통제권을 보유하기 때문에 AWS "책임 공유" 모델의 일부로서 해당 콘텐츠의 보안과 관련된 책임도 지게 됩니다. 이 책임 공유 모델은 개인정보 취급방침 및 데이터 보호 요구 사항에 따라 고객 및 AWS의 각 역할을 이해할 수 있는 기본

모델입니다. 개인정보 취급방침 및 데이터 보호 요구 사항은 고객이 AWS 서비스를 사용하여 저장하거나 처리하도록 선택한 콘텐츠에 적용될 수 있습니다.

클라우드 보안 관리에 대한 AWS 책임 공유 접근 방식

고객 콘텐츠가 보호됩니까?

IT 인프라를 AWS로 이동하면 고객과 AWS 모두가 보안 운영 및 관리에 중요한 역할을 담당하므로 고객과 AWS 간에 책임 공유 모델이 형성됩니다. AWS는 호스트 운영 체제 및 가상화 계층부터 AWS 서비스가 운영되는 설비의 물리적 보안에 이르기까지 구성 요소를 운영하고 관리하고 통제합니다. 고객은 AWS에서 제공하는 보안 그룹 방화벽 및 기타 보안 관련 기능의 구성은 물론, 게스트 운영 체제(게스트 운영 체제에 대한 업데이트 및 보안 패치 포함) 및 관련 애플리케이션 소프트웨어의 관리를 책임집니다. 고객은 일반적으로 제3자(예: 인터넷 서비스 공급업체)로부터 받는 서비스를 통해 AWS 환경에 연결합니다. AWS는 이러한 연결을 제공하지 않으므로 AWS 환경에 대한 연결은 고객의 책임입니다. 따라서 고객은 이러한 연결의 보안 및 해당 시스템과 관련된 제3자의 보안 책임을 고려해야 합니다. 책임 공유 모델에서 고객과 AWS가 가지는 각 역할은 그림 1에 나와 있습니다.

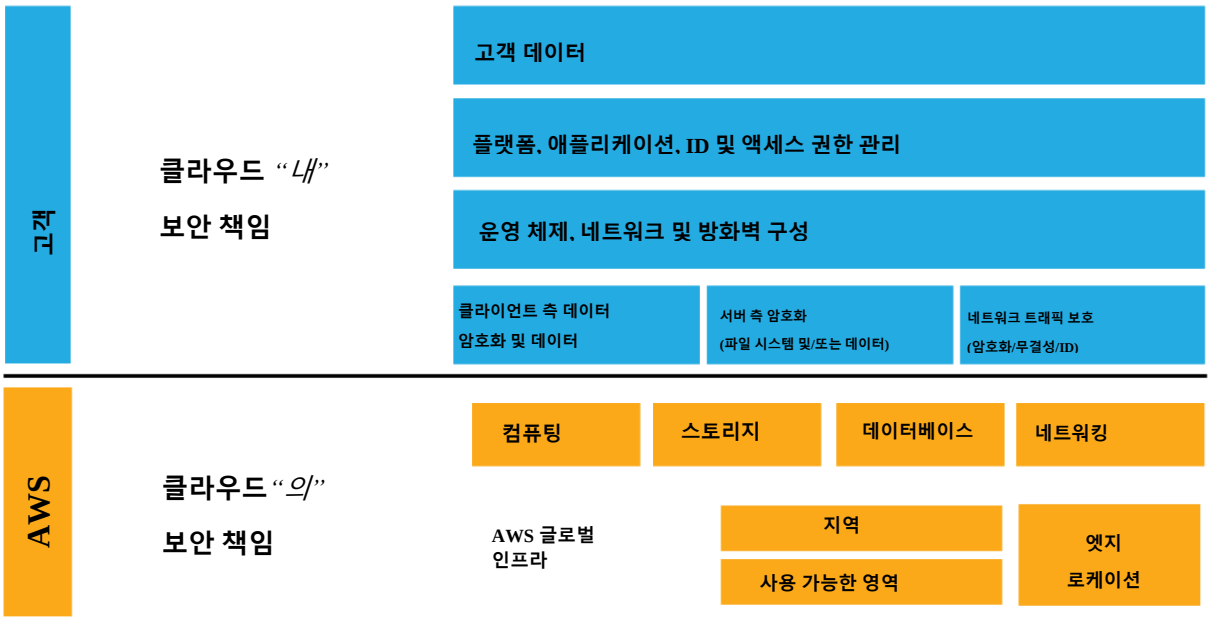

그림 1- 책임 공유 모델

책임 공유 모델이 고객 콘텐츠의 보안에 대해 가지는 의미는 무엇입니까?

클라우드 솔루션의 보안을 평가할 때 고객은 다음을 이해하고 구분해야 합니다.

- 클라우드 서비스 공급업체(AWS)가 구현하고 운영하는 보안 수단 – "클라우드***의*** 보안"
- AWS 서비스가 사용되는 고객 콘텐츠 및 애플리케이션의 보안과 관련하여 고객이 구현하고 운영하는 보안 수단 – "클라우드 내 보안."

AWS에서 클라우드***의*** 보안을 관리하는 반면, 클라우드 ***내*** 보안은 고객의 책임입니다. 고객이 현장 데이터 센터에서 구동되는 애플리케이션의 경우와 마찬가지로 고유의 콘텐츠, 플랫폼, 애플리케이션, 시스템 및 네트워크를 보호하기 위해 어떤 보안을 구현할지를 통제하기 때문입니다.

클라우드***의*** 보안 이해

AWS는 기본 클라우드 환경의 보안을 관리할 책임이 있습니다. AWS 클라우드 인프라는 가장 유연하고 안전한 클라우드 컴퓨팅 환경 중 하나로서 완벽한 고객 분리를 제공하는 동시에 최적의 가용성을 제공하도록 설계되었습니다. 또한 이 인프라는 확장성이 뛰어나고 안정성이 높은 플랫폼을 제공하므로 필요한 경우 고객은 애플리케이션과 콘텐츠를 광범위한 전 세계 규모로 빠르고 안전하게 배포할 수 있습니다.

AWS 서비스는 콘텐츠 유형이나 콘텐츠를 저장하는 리전과 상관없이 모든 고객에게 동일하게 높은 수준의 보안을 제공하기 때문에 콘텐츠의 영향을 받지 않습니다. 세계 최고 성능의 보안 수준을 자랑하는 AWS 데이터 센터는 첨단 전자 감시 및 다단계 접근 통제 시스템을 사용합니다. 데이터 센터에는 숙련된 보안 인력이 연중무휴로 근무하고 있으며 접근 권한은 최소 권한 기준으로 엄격하게 부여됩니다. 핵심 AWS 클라우드 인프라, 플랫폼 및 서비스에 기본 제공되는 모든 보안 수단의 전체 목록은 백서의 보안 프로세스[1] 개요를 참조하십시오.

AWS는 고객의 보안을 유지하기 위해 경계 태세를 유지하며 무단 액세스에 대응하기 위한 정교한 기술 및 물리적 조치를 구현했습니다. 고객은 AWS SOC(서비스 조직 통제) 1, 2[2] 및 3[3]

[1] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
[2] http://aws.amazon.com/compliance/soc-faqs/
[3] http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

보고서, ISO 27001[4], 27017[5] 및 27018[6] 인증 및 PCI DSS[7] 규정 준수 보고서를 비롯한 AWS 인증 및 보고서를 통해 AWS 환경 내의 보안 통제 기능을 적절히 검증할 수 있습니다. 27018 인증은 AWS가 고객 콘텐츠의 개인정보 보호 문제를 구체적으로 해결하는 시스템을 적절히 갖추고 있음을 입증합니다. 이러한 보고서 및 인증은 독립적인 제3자 감사자에 의해 생성되며 AWS 보안 통제 기능의 설계 및 운영 효율성을 입증합니다. AWS 규정 준수 인증 및 보고서는 https://aws.amazon.com/compliance/contact에서 요청할 수 있습니다.

AWS 규정 준수 인증, 보고서, 모범 사례 및 표준 준수에 대한 자세한 내용은 AWS의 규정 준수 사이트에서 확인할 수 있습니다.

클라우드 *사*보안 이해

고객은 AWS 서비스를 사용할 때 콘텐츠의 소유권과 통제권을 보유합니다. AWS가 아니라 고객이 AWS 서비스를 사용하여 저장하거나 처리할 콘텐츠를 결정합니다. 고객이 AWS 클라우드에 저장할 콘텐츠를 결정하기 때문에 고객만이 AWS를 사용하여 저장하고 처리하는 콘텐츠의 적합한 보안 수준을 결정할 수 있습니다. 또한 고객은 사용하는 서비스는 물론, 필요한 자격 증명을 비롯하여 콘텐츠 및 서비스에 접근할 수 있는 권한을 부여할 대상을 완전히 통제할 수 있습니다. 고객은 콘텐츠(저장되었거나 전송 중인 상태) 암호화 여부, 사용하고자 하는 기타 보안 기능 및 도구를 비롯하여 환경을 구성하고 콘텐츠를 보호하는 방법을 통제합니다. 이러한 설정을 고객이 결정하고 통제하므로 AWS가 고객 구성 설정을 변경하지 않습니다. AWS 고객은 규정 준수 요구 사항을 충족하기 위해 보안 아키텍처를 자유롭게 설계할 수 있습니다. 이는 공급업체가 아키텍처를 결정하는 기존 호스팅 솔루션과의 핵심적인 차이점입니다. AWS를 통해 고객은 비즈니스 요구 사항에 따라 클라우드에서 보안 조치를 구현할 시기와 방법을 결정할 수 있습니다. 예를 들어 고객 콘텐츠를 보호하기 위해 고가용성 아키텍처가 필요한 경우 고객은 중복 시스템, 백업, 위치, 네트워크 상향링크 등을 추가하여 복원성이 뛰어난 고가용성 아키텍처를 만들 수 있습니다. 고객 콘텐츠에 대해 접근 제한이 필요한 경우 고객은 AWS를 통해 시스템 수준 및 데이터 수준의 암호화 모두에 대해 접근 권한 관리 통제 기능을 구현할 수 있습니다.

고객이 보안 AWS 환경을 설계, 구현, 운영하도록 지원하기 위해 AWS는 고객이 사용할 수 있는 다양한 보안 도구 및 기능을 제공합니다. 또한 고객은 다양한 제3자 보안 솔루션을 비롯한 보안 도구 및 통제 기능을 사용할 수도 있습니다. 고객은 AWS 서비스에서 정교한 ID 및 접근 관리 도구, 보안 기능, 암호화, 네트워크 보안 등 다양한 보안 기능, 도구 및 통제 기능을 활용하여

[4] http://aws.amazon.com/compliance/iso-27001-faqs/
[5] http://aws.amazon.com/compliance/iso-27017-faqs/
[6] http://aws.amazon.com/compliance/iso-27018-faqs/
[7] https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

콘텐츠를 보호하도록 구성할 수 있습니다. 고객이 콘텐츠 보안을 유지하기 위해 수행할 수 있는 단계로는 다음을 구현하는 작업이 포함됩니다.

- 강력한 암호 정책(사용자에게 적절한 권한을 할당하고 접근 키를 보호하기 위한 강력한 단계 실행)
- 적절한 방화벽 및 네트워크 세분화(데이터 손실 및 무단 접근 위험을 줄이기 위해 콘텐츠 암호화 및 적절한 시스템 설계)

AWS가 아닌 고객이 이러한 중요 요소를 통제하기 때문에 고객은 자체적으로 선택한 사항과 함께 AWS에 저장하는 콘텐츠나 게스트 운영 체제, 컴퓨팅 인스턴스의 애플리케이션, AWS 스토리지, 플랫폼, 데이터베이스 또는 기타 서비스에서 저장되고 처리되는 콘텐츠 등 AWS 인프라에 연결하는 콘텐츠의 보안을 책임집니다.

AWS는 AWS Key Management Service, AWS CloudTrail 등 액세스, 암호화 및 로깅 기능의 고급 세트를 제공하여 고객이 콘텐츠를 효과적으로 관리할 수 있도록 지원합니다. 고객이 기존 통제 프레임워크에 AWS 보안 통제 기능을 통합하고 조직의 AWS 서비스 사용에 대한 보안 평가를 설계하고 실행할 수 있도록 지원하기 위해 AWS는 보안, 거버넌스, 위험 및 규정 준수에 관한 여러 백서, 다양한 점검표, 모범 사례를 게시합니다. 또한 고객은 선호 사항에 따라 보안 평가를 자유롭게 설계하고 실행할 수 있으며, 해당 검사가 고객의 컴퓨팅 인스턴스로 제한되고 AWS 이용목적 제한방침을 위반하지 않는 한 클라우드 인프라 스캔을 수행 권한을 요청할 수 있습니다.

AWS 리전: 콘텐츠는 어디에 저장됩니까?

AWS 데이터 센터는 다양한 글로벌 지역의 클러스터에 구축됩니다. 특정 국가의 각 데이터 센터 클러스터를 '리전'이라고 합니다. 고객은 전 세계 16개의 AWS 리전에 액세스할 수 있습니다[8]. 고객은 단일 리전, 모든 리전 또는 임의의 리전 조합을 사용할 수 있습니다. 그림 2에 표시된 AWS 리전 위치는 다음과 같습니다.

지역 및 사용 가능한 영역 수

AWS GovCloud(2)

미국 서부
오리건(3),
캘리포니아 북부(3)

미국 동부
버지니아 북부(5),
오하이오(3)

캐나다
중부(2)

남미
상파울루(3)

유럽
아일랜드(3),
프랑크푸르트(2), 런던(2)

아시아 태평양
싱가포르(2),
시드니(3), 도쿄(3),
서울(2), 뭄바이(2)

중국
베이징(2)

새로운 지역(서비스 예정)

파리

닝샤

그림 2 – AWS 글로벌 리전

[8]AWS GovCloud(미국)는 미국 정부 기관 및 고객이 특정 규제 및 규정 준수 요구 사항을 충족하여 민감한 워크로드를 클라우드로 이동할 수 있도록 설계된 별도 AWS 리전입니다. AWS China(베이징)도 별도 AWS 리전입니다. AWS China(베이징) 리전을 이용하고자 하는 고객은 중국(베이징) 리전에만 적용되는 별도의 계정 자격 증명 세트를 등록해야 합니다.

AWS 고객이 콘텐츠와 서버를 저장할 AWS 리전을 선택합니다. 따라서 특정한 지리적 요구 사항을 가진 고객은 원하는 위치에 환경을 구축할 수 있습니다. 예를 들어 인도의 AWS 고객은 아시아 태평양(뭄바이) 리전에만 AWS 서비스를 배포하고 인도 내 원하는 위치에 콘텐츠를 저장하도록 선택할 수 있습니다. 이러한 선택을 한 후 고객이 콘텐츠를 이동하지 않는 한 해당 콘텐츠는 인도에 저장됩니다.

고객은 콘텐츠를 저장하고 처리하는 데 사용되는 리전을 항상 통제할 수 있습니다. AWS는 각 고객의 콘텐츠를 리전에 저장하고 처리하며, 고객이 선택한 서비스를 사용할 뿐이며, 법적으로 요구되지 않는 한 고객 콘텐츠를 이동하지 않습니다.

고객은 리전을 어떻게 선택할 수 있습니까?

고객이 AWS 관리 콘솔을 사용하거나 AWS API(Application Programming Interface)를 통해 요청하면 AWS 서비스를 사용하려는 특정 AWS 리전을 확인할 수 있습니다.

그림 3: AWS 글로벌 리전을 선택하면 AWS 관리 콘솔을 사용하여 AWS 스토리지 서비스로 콘텐츠를 업로드하거나 컴퓨팅 리소스를 프로비저닝할 때 고객에게 표시되는 AWS 리전 선택 메뉴의 예가 제공됩니다.

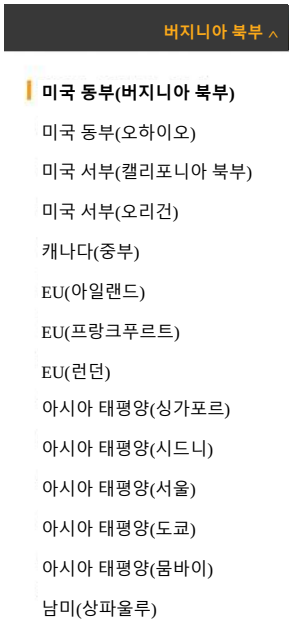

그림 3 – AWS 관리 콘솔에서 AWS 글로벌 리전 선택

또한 고객은 Amazon VPC(Virtual Private Cloud) 기능을 활용하여 컴퓨팅 리소스에 사용할 AWS 리전을 지정할 수도 있습니다. Amazon VPC를 통해 고객은 자체적으로 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 있는 AWS 클라우드의 격리된 비공개 섹션을 프로비저닝할 수 있습니다. 고객은 Amazon VPC를 사용하여 고객 소유의 데이터 센터에서 운영할 수 있는 기존 네트워크와 매우 유사한 가상 네트워크 토폴로지를 정의할 수 있습니다.

고객이 VPC에서 시작한 모든 컴퓨팅 및 기타 리소스는 고객이 지정한 AWS 리전에 저장됩니다. 예를 들어 아시아 태평양(시드니) 리전에 VPC를 만들고 고객의 데이터 센터에 다시 연결(VPN[9] 또는 Direct Connect[10]를 이용)하면 VPC에서 시작한 모든 컴퓨팅 리소스는 아시아 태평양(시드니) 리전에만 상주합니다. 이 옵션은 다른 AWS 리전에서도 활용할 수 있습니다.

국가 간 개인정보 전송

AWS 서비스를 사용할 때 고객은 개인정보를 포함한 콘텐츠를 국가 간에 전송할 수 있으며 이러한 전송에 적용되는 법적 요구 사항을 고려해야 합니다. AWS는 EU에서 유럽경제지역 외의 국가(예: 싱가포르)로 EU 규정에 명시된 내용에 따라 개인정보가 포함된 콘텐츠를 전송하는 AWS 고객에게 표준 계약 조항 2010/87/EU(대개 '모델 조항'이라고 지칭)를 포함하는 데이터 처리 부록을 제공합니다. AWS는 AWS 데이터 처리 계약 및 모델 조항의 제29조 작업반(Working Party)으로 알려진 EU 데이터 보호 당국의 승인을 받았습니다. AWS 고객은 유럽에 설립되었든 유럽경제지역에서 운영 중인 글로벌 회사든 상관없이 EU에서 승인한 AWS의 데이터 처리 부록 및 모델 조항을 통해 EU 규정을 완벽하게 준수하면서 AWS를 사용하여 글로벌 운영을 계속할 수 있습니다. 자세한 내용은 AWS EU 데이터 보호 FAQ를 참조하십시오. 고객이 AWS 데이터 처리 부록을 활용할 수 있는 방법에 대한 자세한 내용은 여기를 참조하십시오(로그인 필요).

고객 콘텐츠에 액세스할 수 있는 사람은 누구입니까?

콘텐츠에 대한 고객 통제

AWS를 사용하는 고객은 AWS 환경 내 콘텐츠에 대한 통제권을 유지하며 상실하지 않습니다. 고객은 다음을 수행할 수 있습니다.

- 콘텐츠의 위치(예: AWS에서 사용하는 스토리지의 유형 및 해당 스토리지의 지리적 위치(리전별)) 결정
- 마스킹, 익명 또는 암호화 처리 여부를 비롯한 콘텐츠의 형식, 구조 및 보안을 통제. AWS는 전송 또는 저장 중인 고객 콘텐츠에 대해 강력한 암호화를 구현할 수 있는

옵션을 제공하고, 고객에게 고유한 암호화 키를 관리하거나 선택한 제3자 암호화 메커니즘을 사용할 수 있는 옵션을 제공

- ID, 액세스 관리, 권한, 보안 자격 증명 등 기타 액세스 통제 관리

따라서 AWS 고객은 AWS에서 콘텐츠의 전체 수명 주기를 통제하고 콘텐츠 분류, 액세스 통제, 보존, 삭제 등 고유한 특정 요구 사항에 따라 콘텐츠를 관리할 수 있습니다.

고객 콘텐츠에 대한 AWS 액세스

AWS는 웹 사이트에 설명된 대로 컴퓨팅, 스토리지, 데이터베이스, 네트워킹 또는 기타 서비스를 각 고객에게 제공합니다. AWS 암호화 기능 사용, 고유한 암호화 키 관리, 고객이 직접 선택한 제3자 암호화 메커니즘 사용 등의 서비스를 사용할 때 콘텐츠를 암호화할 수 있는 다양한 옵션이 제공됩니다. AWS는 각 고객이 선택한 AWS 서비스를 해당 고객과 최종 사용자에게 제공하거나 합법적으로 요구되는 경우 이외의 어떤 목적으로도 고객 콘텐츠에 액세스하거나 해당 콘텐츠를 사용하지 않습니다. AWS는 마케팅이나 광고와 같은 다른 목적을 위해 고객 콘텐츠를 사용하거나 고객 콘텐츠에서 정보를 얻지 않습니다.

액세스에 대한 정부 권리

국내 및 외국 정부 기관에서 클라우드 서비스에 저장된 콘텐츠에 액세스할 수 있는 권리에 대한 문의가 종종 제기됩니다. 고객은 정부가 콘텐츠에 액세스할 수 있는지 여부와 그러한 상황 등 데이터 주권과 관련된 문제에 대해 혼란스러워할 때가 종종 있습니다. 콘텐츠가 저장된 관할권에 적용되는 현지 법률은 일부 고객에게는 중요한 고려사항입니다. 그러나 고객은 다른 관할지의 법률이 적용될 수 있는지 여부도 고려해야 합니다. 고객은 비즈니스와 운영에 관련 법률이 어떻게 적용되는지를 이해하기 위해 조언을 구해야 합니다.

---

[9] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
[10] http://aws.amazon.com/directconnect/

클라우드에 저장된 콘텐츠에 대해 액세스 권한을 요청할 수 있는 국내 또는 외국 정부의 권리에 관해 우려 사항이나 궁금한 사항이 있는 경우 관련 정부 기관에서 이미 고객에게 적용되는 법률에 따라 해당 콘텐츠에 대한 요청을 제기할 권리가 있음을 이해하는 것이 중요합니다. 예를 들어 X 국가에서 비즈니스를 운영하는 회사는 콘텐츠가 Y 국가에 저장되어 있더라도 정보에 대한 합법적 요청을 받을 수 있습니다. 일반적으로 법인의 데이터에 대한 액세스를 원하는 정부 기관은 클라우드 공급업체가 아닌 해당 법인에 직접 정보를 요청합니다.

대부분의 국가에는 법 집행 기관과 정부 보안 기관이 정보에 대한 액세스를 요구하도록 허용하는 법률이 있습니다. 사실, 대부분의 국가는 정보에 대한 적절한 법적 요청(예: 형법 조항과 관련)에 응답하여 다른 국가로 정보를 전송할 수 있는 절차(상호 법률 지원 조약 포함)를 갖추고 있습니다. 그러나 각 관련법에는 해당 법 집행 기관이 합당한 요청을 하기 위해 충족해야 하는 기준이 마련되어 있음을 기억해야 합니다. 예를 들어 액세스 권한을 요청하는 정부 기관은 당사자가 콘텐츠에 대한 액세스 권한을 제공해야 할 만한 합당한 이유가 있음을 입증해야 할 수 있으며 법원 명령이나 영장을 발급받아야 할 수도 있습니다.

많은 국가에서는 국외 적용을 취지로 하는 데이터 액세스 법을 보유하고 있습니다. 클라우드 서비스와 관련하여 언급되는 역외 적용 범위가 적용되는 미국 법률의 예로는 미국 애국자법(U.S. Patriot Act)이 있습니다. 애국자법은 정부가 국제 테러 및 기타 외국 정보 문제에 관한 조사와 관련하여 정보를 입수할 수 있도록 허용하는 다른 선진국의 법률과 유사합니다. 애국자법에 의거하여 문서를 요청할 경우 요청이 합법적인 수사와 관련되어 있음을 포함하여 요청이 법률을 준수한다는 사실을 입증하는 법원 명령을 항상 제공해야 합니다. 애국자법은 정보가 클라우드, 현장 데이터 센터 또는 물리적 레코드에 저장되어 있는지 여부와 상관없이, 그리고 회사가 세계적으로 통합되어 있거나 전 세계에서 운영되고 있는지와 상관없이 미국에서 운영되는 모든 회사에 일반적으로 적용됩니다. 즉, 미국에서 비즈니스를 운영하지만 미국 이외 지역에 본사를 두고 있거나 미국 이외의 지역에서도 비즈니스를 운영하는 회사는 비즈니스 운영으로 인해 애국자법의 적용을 받을 수 있습니다.

정부에 대한 액세스 권한 부여 관련 AWS 정책

AWS는 고객의 보안을 유지하기 위해 경계 태세를 유지하며, 소환장이나 법원 명령과 같이 법적으로 유효하고 구속력 있는 명령을 준수하기 위해 법적으로 요구되지 않는 한 또는 관련 법률에서 달리 요구하지 않는 한 미국이나 다른 정부의 요청에 따라 데이터를 공개하거나 이동하지 않습니다. 또한 AWS는 고객의 콘텐츠를 정부의 요구에 따라 공개하기 전 가능하다면 고객에 먼저 그 사실을 알리고 있습니다.다만, 법적으로 허용되지 않거나 고객의 AWS사용이

불법행위에 연관되어 있는 징후가 명백할 때는 제외합니다.

개인정보 취급 및 데이터 보호를 위한 공통 고려사항

많은 국가에서 개인정보의 보호를 위한 법률을 제정하고 있습니다. 하나의 포괄적인 데이터 보호법을 가자고 있는 국가들도 있고, 다양한 법률 및 규제를 통해 더욱 세부적인 방식으로 데이터 보호를 다루는 국가들도 있습니다. 법률 및 규제 요구사항이 국가별로 다를 수 있지만, 관할권 요구 사항, 산업별 요구 사항, 콘텐츠별 요구 사항 등 몇 가지 주요 데이터 보호법에 따라 공통적으로 고려해야 할 사항들이 있습니다. 이러한 고려사항은 개인정보의 일반적인 수명 주기에 따라 조정할 수 있습니다.

AWS를 사용하여 개인정보가 포함된 콘텐츠를 저장하고 처리할 때 고객이 개인정보 및 데이터 보호 요구 사항을 분석하고 해결할 수 있도록 하기 위해 아래와 같이 데이터 라이프 사이클의 다양한 단계를 논의하고 각 단계와 관련된 주요 고려사항을 확인하며 AWS 서비스 운영 방식에 대한 관련 정보를 제공합니다.

많은 데이터 보호법에서는 이용자가 개인정보와 상호 작용하는 방식, 그리고 개인정보에 대한 접근 및 통제 수준과 관련된 책임을 부여합니다. 일반적인 접근법 중 하나는 데이터 관리자, 데이터 처리자 및 데이터 주체를 구별하는 것입니다. 여러 관할권에서 사용되는 용어는 다를 수 있으며 일부 법률에서는 더 세심하게 구분합니다. AWS는 자사의 서비스가 여러 비즈니스 목적에 따라 다양한 상황에서 사용되며 AWS 서비스를 사용하여 저장되거나 처리되는 고객 콘텐츠에 포함된 개인정보의 데이터 수명 주기와 관련하여 여러 당사자가 있을 수 있다는 사실을 인식하고 있습니다. 복잡도를 낮추기 위해 아래 테이블의 지침에서는 AWS 서비스를 사용하여 고객 콘텐츠가 저장되거나 처리되는 상황에서 고객이 다음을 수행한다고 가정되어 있습니다.

- 최종 사용자 또는 기타 개인(데이터 주체)에게서 개인정보를 수집하고, 고객이 개인정보를 요구하고 사용할 목적을 결정함
- 개인정보에 접근하고 업데이트하며 사용할 수 있는 사람을 통제할 수 있는 권한을 가짐
- 관련 공개 및 동의 요구 사항을 준수하기 위해 필요한 경우 데이터 주체와의 의사소통을 비롯하여 개인정보와 관련된 개인(이 섹션에서는 데이터 주체로 언급됨)과의 관계를 관리함

따라서 콘텐츠를 통제하고, 콘텐츠를 접근할 수 있는 권한을 포함한 콘텐츠 처리와 관련한 의사를 결정한다는 점에서 고객은 데이터 통제권자와 유사한 역할을 수행합니다. 반면

AWS는 각 고객이 선택한 AWS 서비스를 해당 고객에게 제공하기 위해서만 고객 콘텐츠를 사용하고 다른 목적으로는 고객 콘텐츠를 사용하지 않기 때문에 데이터 처리자와 비슷한 역할을 수행합니다. '데이터 처리자' 및 '데이터 통제권자'라는 용어는 EU 법률에서 매우 다른 의미를 가지지만, 이 백서에서는 구체적인 EU 요구 사항을 다루지 않습니다. 데이터 통제권자 및 데이터 처리자와 관련된 EU 데이터 보호 요구 사항에 대한 지침이 필요한 고객은 EU 데이터 보호 백서[11]를 참조하시기 바랍니다.

고객이 제3자(개인정보의 관리자나 비즈니스 관계가 있는 다른 제3자)를 대신하고 3자의 지침을 따라 AWS 서비스를 사용하여 개인정보를 처리하는 경우, 이 테이블에 언급된 고객 책임 사항은 고객과 제3자 간에 공유되고 관리됩니다.

[11] http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf

데이터 수명 주기 단계	요약 및 예시	고려 사항
개인 정보 수집	개인 정보를 수집하기 전에 개인(데이터 주체)에게 알리거나 동의를 구하는 것이 적절하거나 필요할 수 있습니다. 여기에는 정보를 수집, 사용 또는 공개하는 목적에 대한 알림도 포함될 수 있습니다. 개인 정보를 수집 당하는 해당 개인에 대한 요구 사항이 있을 수 있습니다. 예를 들어, 개인 정보를 개인으로부터 직접 수집하는 대신 제3자 소스에서 수집하는 경우 요구 사항이 다를 수 있습니다. 유효한 목적 또는 합당한 목적이 있는 경우 개인 정보 수집이 허용될 수 있습니다.	**고객:** 고객은 정보주체로부터 언제, 어떻게, 왜 개인정보를 수집하는 지를 결정하고 통제해야 하며, AWS 서비스를 사용하여 저장하거나 처리하는 고객 콘텐츠에 해당 개인 정보가 포함되어야 할 지도결정해야 합니다. 또한 고객은 해당 데이터를 수집하는 목적을 관련정보주체에게 공개하고, 허용된 출처에서 데이터를 획득해야하며, 허용된 목적으로만 데이터를 사용하는지도 확인해야 할 필요가 있습니다. 고객과 AWS 간의 관계와 마찬가지로, AWS에 개인 정보가 저장되는 개인과 고객 간에도 관계가 있으며 따라서 고객은 개인 정보의 수집과 처리에 대해 해당 개인과 직접 소통할 수 있습니다. AWS가 아닌 고객은 개인 정보 수집에 대해 해당 개인에게 제공하는 알림 또는 해당 개인으로부터 고객이 받는 동의의 범위도 알고 있어야 합니다. **AWS:** AWS는 고객이 AWS를 사용하여 저장하고 처리하는 콘텐츠에 개인 정보가 포함되는 개인으로부터 개인 정보를 수집하지 않으며, AWS는 해당 개인과 연락하지 않습니다. 따라서 AWS는 이러한 상황에서 필수적인 동의를 받기 위해 관련 개인과 통신할 필요가 없으며 통신할 수도 없습니다. AWS에서는 각 고객이 선택한 AWS 서비스를 해당 고객에게 제공하는 데만 각 고객의 콘텐츠를 사용할 뿐 기타 목적을 위해 고객의 콘텐츠를 사용하지 않습니다.
개인 정보 사용 및 공개	개인 정보가 수집되는	**고객:** 고객은 개인 정보를 수집하는 이유, 개인 정보를 사용할 목적, 개인 정보를 사용할 수 있는 사람 및

	목적으로만 개인 정보를 사용하거나 공개하는 것이 적절하거나 필요할 수 있습니다. 따라서 고객이 AWS를 서비스 공급자로 사용할 것임을 개인(데이터 주체)에게 알려야 할 수 있습니다.	공개하는 사람 등을 결정하고 제어합니다. 고객은 허용된 목적으로만 정보가 사용되도록 확인해야 합니다. 고객이 AWS에 저장된 고객 콘텐츠에 개인 정보가 포함되도록 선택하는 경우, 고객은 콘텐츠의 형식과 구조, 익명화 또는 암호화 여부를 포함하여 권한 없는 사람에게 콘텐츠가 공개되지 않도록 보호하는 방법도 고객이 통제합니다. 고객은 AWS 서비스를 사용하여 개인 정보가 포함된 고객 콘텐츠를 저장하거나 처리하는지 여부를 알게 되며, 따라서 필요한 경우 AWS를 서비스 공급자로 사용한다는 점을 개인에게 알릴 수 있는 최적의 위치에 있습니다. **AWS:** AWS 각 고객이 선택한 AWS 서비스를 해당 고객에게 제공하기 위해서만 각 고객의 콘텐츠를 사용하며 기타 목적으로는 고객 콘텐츠를 사용하지 않습니다.
개인 정보 해외 이전	개인 정보를 해외로 이전하는 경우 고객이 개인 정보를 저장할 국가에 대해 개인(데이터 주체)에게 알리고 개인 정보를 해당 위치에 저장하기 위한 동의를 얻어야 할 수 있습니다. 개인 정보가 상주하는 관련 국가의 개인 정보	**고객:** 고객에게 지리적 또는 지역적 제약 조건이 있는 경우 고객은 요구 사항에 맞는 AWS 리전을 선택하여 제약 조건을 관리할 수 있으며 콘텐츠는 선택한 리전에 저장되고 처리됩니다. 고객은 개인 정보를 저장하거나 처리하는 위치를 개인에게 공개해야 하는지 여부를 고려하고 필요한 경우 관련 개인으로부터 해당 위치와 관련하여 필요한 동의를 받아야 합니다. 고객과 AWS 간의 관계와 마찬가지로, AWS에 개인 정보가 저장되는 개인과 고객 간에도 관계가 있으며 따라서 고객은 해당 문제에 대해 해당 개인과 직접 통신할 수 있습니다. **AWS:** AWS는 각 고객이 선택한 서비스를 사용하여 리전에서 고객 콘텐츠를 저장하고 처리할 뿐이며,

	보호 체계에서 제공되는 보호 조치도 고려해 보아야 합니다.	법적으로 필요한 경우 이외에는 고객 콘텐츠를 이동하지 않습니다. 고객이 둘 이상의 리전에 콘텐츠를 저장하거나 리전 간에 콘텐츠를 복사 또는 이동하도록 선택하는 경우, 이러한 결정은 전적으로 고객의 선택이며 고객은 콘텐츠가 어디에 저장되고 처리되든 상관없이 콘텐츠에 대한 유효한 제어 권한을 계속 유지합니다. **일반:** AWS는 ISO 27001인증을 획득하였으며[12]콘텐츠를 저장하는 지리적 리전에 관계없이 모든 고객에게 강력한 보안 기능을 제공합니다.
개인 정보 보안	개인 정보의 보안을 유지하기 위한 조치를 취하는 것이 중요합니다.	**고객:** 고객은 콘텐츠 및 콘텐츠에 포함된 개인 정보의 보안을 포함하여 클라우드 내부의 보안을 책임집니다. **AWS:** AWS는 기본 클라우드 환경 자체의 보안 관리를 책임집니다. 핵심 AWS 클라우드 인프라, 플랫폼 및 서비스에 내장된 모든 보안 조치의 전체 목록은 보안 프로세스 개요[13] 백서를 참조하십시오. 고객은 AWS SOC(Service Organization Control) 1, 2 및 3 보고서, ISO 27001, 27017 및 27018 인증, PCI-DSS 규정 준수 보고서 등의 AWS 인증 및 보고서를 통해 AWS 환경 내에 배치된 보안 제어 기능을 확인할 수 있습니다.
개인 정보 액세스 및 수정	개인(데이터 주체)은 개인 정보 수정 등의 목적으로 개인 정보에 액세스해야 할 수 있습니다.	**고객:** 고객은 AWS를 사용하여 저장되거나 처리되는 콘텐츠에 대한 제어 권한을 보유합니다(콘텐츠 보안 방법 및 해당 콘텐츠에 액세스하고 수정할 수 있는 사람에 대한 제어 포함). 또한 고객과 AWS 간의 관계와 마찬가지로, 고객은 AWS 서비스를 사용하여 저장되거나 처리되는 고객 콘텐츠에 개인 정보가 포함되는 개인과 관계가 있습니다. 따라서 AWS가 아닌 고객이 관련 개인과 협력하여 해당 개인에게 고객 콘텐츠에 포함된 개인 정보에 대한 액세스 권한과 수정 기능을 제공할 수 있습니다.

[12] https://aws.amazon.com/compliance/iso-27001-faqs/
[13] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

		AWS: AWS는 각 고객이 선택한 AWS 서비스를 해당 고객에게 제공할 목적으로만 고객 콘텐츠를 사용하며, AWS 서비스를 사용하여 저장하거나 처리하는 고객 콘텐츠에 개인 정보가 포함되어 있는 개인에게 연락을 취하지 않습니다. 이상의 내용과 고객이 고객 콘텐츠에 대해 보유하는 제어 권한의 수준을 고려할 때, AWS는 이러한 상황에서 해당 개인에게 개인 정보에 대한 액세스 권한 또는 수정 기능을 제공할 필요가 없으며 제공할 수도 없습니다.
개인 정보의 품질 유지	개인 정보의 정확성과 무결성이 유지되고 있는지 확인해야 할 필요가 수있습니다.	**고객:** 고객이 AWS를 사용하여 개인 정보가 포함된 콘텐츠를 저장하거나 처리하도록 선택하는 경우, 고객은 해당 콘텐츠의 품질을 제어할 수 있으며 고객은 해당 콘텐츠에 대한 액세스 권한을 보유하고 콘텐츠를 수정할 수 있습니다. 따라서 고객은 고객 콘텐츠에 포함된 개인 정보가 정확하고 완전하며 오해의 소지가 없고 최신 상태로 유지되는지 확인하기 위해 필요한 모든 조치를 취해야 합니다. **AWS:** AWS의 SOC 1, Type 2 보고서에는 전송, 저장 및 처리를 포함한 모든 단계를 통해 데이터 무결성이 유지된다는 합당한 보장을 제공하는 컨트롤이 포함됩니다.
개인 정보 삭제 또는 익명화	일반적으로 개인 정보는 데이터 수집 목적에 합당한 필요 기간 이상으로 장기 보관해서는 안 되며, 일반적으로 관련 데이터 보존법에 따라 보존해야 합니다.	**고객:** 고객만이 AWS에 저장된 고객 콘텐츠에 포함된 개인 정보가 수집된 이유를 알고 있으며, 고객만이 합법적인 목적으로 더 이상 개인 정보를 보존할 필요가 없는 시기를 알고 있습니다. 고객은 더 이상 필요하지 않을 때 개인 정보를 삭제하거나 익명화해야 합니다. **AWS:** AWS 서비스에서는 고객이 콘텐츠를 삭제할 수 있습니다. 삭제 방법에 대한 설명은 http://aws.amazon.com/documentation 을 참조하십시오.

개인 정보 보호 위반

AWS를 사용하는 동안 고객이 콘텐츠에 대한 제어 권한을 유지한다는 점을 고려할 때, 고객은 자신의 환경을 모니터링하여 개인 정보 보호 침해가 있는지 확인하고 적용 법률에 따라 필요한 방식으로 규제 기관 및 관련 개인에게 알릴 책임이 있습니다. 고객만이 이 책임을 관리할 수 있습니다.

AWS보다는 고객이 이 책임을 관리할 최적의 위치에 있는 이유를 설명하기 위해 고객의 AWS 액세스 키를 예로 사용할 수 있습니다. 고객은 액세스 키를 제어하고, AWS 계정에 액세스할 권한이 있는 사람을 결정합니다. AWS는 액세스 키를 볼 수 없으며 계정에 로그인할 권한이 있는 사람과 권한이 없는 사람을 확인할 수 없습니다. 따라서 고객은 액세스 키의 사용, 오용, 배포 또는 분실을 모니터링할 책임이 있습니다.

일부 관할권에서는 개인이나 규제 기관에게 개인 정보에 대한 무단 액세스 또는 개인 정보의 공개에 대해 알리는 것이 필수이며, 필수 요건은 아니더라도 위험 완화를 위해 이렇게 하는 것이 최선인 경우가 있습니다. 개인에게 통지할 시간과 준수할 통지 프로세스를 결정하는 것은 고객입니다.

기타 법적 고려 사항

앞에서 설명한 바와 같이, 이 백서에서는 특정 개인 정보 또는 데이터 보호법에 대해 논의하지 않습니다. 고객은 산업별 요구 사항을 포함하여 고객에게 적용되는 특정 요구 사항을 고려해야 합니다. 개별 고객에게 적용되는 관련 개인 정보 및 데이터 보호 법률과 규제는고객이 비즈니스를 수행하는 위치, 고객이 사업을 운영하는 산업, 저장하려는 콘텐츠의 유형, 콘텐츠 생성 장소 또는 생성자, 콘텐츠 저장 위치 등 여러 요인에 따라 달라집니다.

개인 정보 보호 규제 의무가 우려되는 고객은 먼저 적용되는 요구 사항을 파악하고 이해한 다음 적절한 조언을 구해야 합니다.

마무리 인사

AWS에게 보안은 항상 최상위 우선 순위에 있습니다. AWS는 기업, 교육 기관, 정부 기관 등

190여 개국에서 1백만이 넘는 고객에게 서비스를 제공하고 있습니다. AWS 고객에는 금융 서비스 제공업체 및 의료 서비스 제공업체가 포함되어 있으며, AWS는 가장 민감한 정보를 믿고 맡길 수 있는 동료로 신뢰 받고 있습니다.

AWS 서비스는 솔루션을 구성하고 배포하는 방법의 유연성과 콘텐츠 저장 위치, 저장 방법, 액세스할 수 있는 사람 등을 포함하여 콘텐츠에 대한 제어를 고객에게 제공하도록 설계되었습니다. AWS 고객은 AWS에서 자신의 보안 애플리케이션을 구축하고 콘텐츠를 안전하게 저장할 수 있습니다.

추가 리소스

개인 정보 및 데이터 보호 요구 사항을 해결하는 방법을 자세히 알아보려면 AWS 웹 사이트에 게시된 위험, 규정 준수 및 보안 백서, 모범 사례, 체크리스트 및 지침을 읽어 보는 것이 좋습니다. 이 자료는 http://aws.amazon.com/compliance 및 http://aws.amazon.com/security 에서 찾아볼 수 있습니다. 이 문서의 작성 시점 현재, 다음 국가 또는 리전의 개인 정보 및 데이터 보호 고려 사항에 대한 구체적인 백서가 준비되어 있습니다.

호주[14]
유럽 연합[15]
말레이시아[16]
뉴질랜드[17]
싱가포르[18]

추가 정보

AWS는 고객이 고가용성의 효율적이고 안전한 애플리케이션을 AWS클라우드에 설계, 개발 및

[14] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf
[15] http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf
[16] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf
[17] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf
[18] http://d0.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf

운영하고 AWS서비스와 솔루션에 대해 능숙해질 수 있도록 트레닝을 제공합니다. 당사는 무료 강의 동영상, 자기주도 실험, 그리고 강의식 수업을 제공합니다. AWS트레이닝과 관련된 추가 정보는 http://aws.amazon.com/training/에서 확인할 수 있습니다.

AWS자격증은 AWS 기술을 사용해서 안전하고 안정적인 클라우드 기반 애플리케이션을 구축하는 모범사례와 연관된 기술적 역량과 지식을 증명해줍니다. AWS자격증에 대한 추가 정보는 http://aws.amazon.com/certification/에서 확인할 수 있습니다.

추가 정보가 필요한 경우 https://aws.amazon.com/contact-us/ 를 통해 AWS에게 문의하거나 AWS 어카운트 매니저(영업담당자)를 통해 문의해 주십시오.