Akamai Compliance Management

SSL 전송 및 가속 서비스 리스크 감소
PCI, ISO, FISMA, BITSM HIPAA 컴플라이언스 지원

사업시 규제를 준수하는데는 많은 일이 수반됩니다. Akamai Compliance Management는 비즈니스 애플리케이션과 웹사이트를 전달하는 과정에서 규제 준수에 필요한 툴과 문서를 제공합니다. 신용카드거래(PCI), 연방정보보안관리(FISMA), ISO 정보보호관리를 위한 실행지침(ISO 27001/27002), 금융서비스규제(BITS), 건강보험 이동 및 설명책임에 관한 법(HIPAA)[1*]에서 요구하는 규제를 보다 확실하게 준수할 수 있도록 합니다.

Akamai Compliance Management는 준법 이니셔티브를 간소화하는데 도움을 줍니다. Akamai는 자료의 전송이 비즈니스에서 요구되는 다양한 기준 준수에 부정적인 영향을 미치지 않도록 지원합니다. 또한, 지속적으로 새로운 규제 프레임워크를 받아들이며 고객의 PCI, FISMA, ISO, BITS, HIPAA 기준 및 규제준수 노력을 지원할 수 있는 모듈을 제공합니다.

PCI 모듈

신용카드 거래를 처리하는 모든 기업은 고객의 거래기록을 보호해야 할 책임이 있습니다. PCI 보안표준협의회(PCI Security Standards Council)는 신용카드 정보 보호를 위한 글로벌 표준인 PCI 데이터보안표준(PCI Data Security Standard, PCI DSS)를 정의했습니다. 이 표준은 신용카드 정보를 처리·저장·전송하는 모든 시스템을 포함하여 카드 거래와 관련된 모든 인프라를 다루고 있습니다. 이 표준을 위반하는 은행에게는 상당한 벌금이 부과됩니다.

글로벌 커머스 기업이나 온라인 스타트업이 웹을 효율적인 비즈니스 채널로 활용하려고 할 때 규제를 준수하지 않으면 상당한 문제에 직면하게 됩니다.

PCI 준수는 많은 관리와 비용이 들어가는 프로세스이고 경우에 따라 카드거래의 모든 인프라에 대한 독립 감사와 여러 단계에 걸친 인증 프로세스가 요구되는 경우도 있습니다. Akamai는 대표적인 글로벌 전자상거래업체의 대부분을 고객사로 두고 있고 SSL 네트워크의 PCI를 적극적으로 준수하고 있습니다. 결과적으로 전체 인프라에서 PCI 준수에 대해 사전인증을 받고 준수 요건 검증을 줄일 수 있습니다.

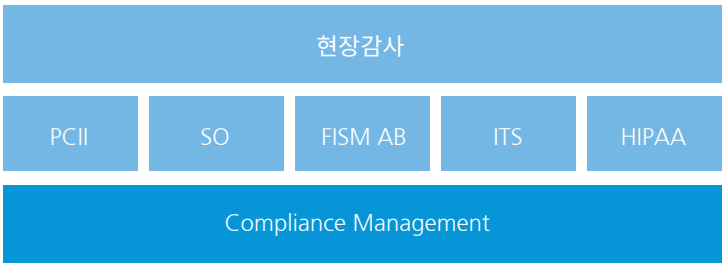
PCI 모듈 패키지 서비스, 지원, 보고, 문서작업, 서비스 조건은 네트워크를 이용하는 고객들이 PCI 준수 검증을 할 수 있도록 지원합니다.

PCI 모듈에 포함된 사항

아카마이 네트워크, 관리 인프라, 관련 프로세스 및 절차는 PCI 의 모범 사례(best practice) 보안 요건에 부합합니다. 이미 마련된 Akamai 인증은 전반적인 PCI 준수 프로세스를 단축시킬 수 있습니다.

PCI 모듈에는 다음 사항이 포함되어 있습니다.

- Akamai PCI 준수 인증서
- PCI 거래 약관(T&C)
- Akamai 분기별 SSL 네트워크 스캐닝 보고서 요약본



PCI 준수 문서

Akamai Compliance Management PCI는 Akamai의 결제카드산업 데이터 보안표준 준수와 관련된 정보를 제공합니다.

본 페이지는 가장 필요한 PCI 정보를 포함하고 있습니다.

- 각 DSS 섹션의 요약과 세부내용의 링크를 나타낸 표
- 써드파티가 취합한 보고서
- Compliance Management PCI 조건
- Akamai 고객들이 PCI 준수를 위해 자주 필요로 하는 기타 아카마이 제품 관련 추가 정보
- 서비스 기본내용에 대한 간략한 답변을 보려면 Quick Facts 파일을 열어보시기 바랍니다.
- Compliance Management Knowledgebase를 검색해 보시기 바랍니다.

DSS 섹션번호 별 PCI 준수

다음 표는 Akamai가 PCI를 어떻게 준수하고 있는지 DSS 섹션 번호별로 정렬한 것입니다. 문서에 있는 링크는 DSS 섹션 번호 세부내용에 대한 준수를 설명하는 PDF 파일로 연결됩니다. 또는 표에 있는 모든 서류의 집파일을 다운로드 할 수 있습니다.

PCI DSS 섹션	PCI DSS 요건	Akamai 접근법	문서(PDF)
1	카드소지자 데이터를 보호하기 위해 방화벽을 설치 및 관리한다.	아카마이의 Secure CDN은 카드소지자의 데이터를 저장하지 않는 공개 접근이 가능한 서버로 구성되어 있습니다. Akamai가 소유한 TRIP 소프트웨어 라우터는 부하 분산장치의 기능을 하며 부적절한 연결을 줄여줍니다.	Secure CDN
2	시스템 비밀번호 또는 보안변수에 벤더가 제공한 디폴트 값을 사용하지 않는다.	Secure CDN의 모든 소프트웨어는 Akamai만을 위해 작성되었거나 수정 및 보호되어 있습니다. 네트워크에 대한 접근은 패스워드가 아닌 개별 SSH 키를 사용하는 특수 인증(Authgate) 프로그램에 의해 통제됩니다.	접근통제설명
3	저장된 카드소지자의 데이터를 보호한다.	Akamai는 카드소지자의 데이터를 저장하지 않습니다.	
4	오픈, 퍼블릭 트워크에서 카드소지자의 데이터 전송을 암호화한다.	Secure CDN은 퍼블릭 인터넷을 통해 전송되는 트래픽을 암호화합니다. 고객은 PCI 준수 가이드라인 내에서 자신만의 암호 변수를 설정할 수 있습니다.	PCI DSS 준수 환경설정 가이드
5	바이러스방지 소프트웨어 또는 프로그램을 사용하고 주기적으로 업데이트한다.	Secure CDN은 악성소프트웨어의 영향을 거의 받지 않는 운영체제인 리눅스를 사용하는 서버로 구성되어 있습니다.	PCI DSS 준수 환경설정 가이드

Akamai Compliance Management

- 포털에서 제공되는 환경설정 검증 툴
- PCI DSS에 따라 고객의 메타데이터가 구성되었는지 확인하는 서비스통합 툴 및 가이드라인
- PCI 사고 통지 및 대응 절차
- PCI 표준의 각 섹션에 대한 Akamai의 입장 요약, 뒷받침 할 수 있는 관련 서류에 대한 링크

ISO 모듈

정보보안에 관한 ISO 27001/27002 표준은 수백 가지의 통제, 통제 메커니즘, 모범사례에 대해 개략적으로 설명합니다. 이 표준은 조직 내 정보보안관리 시작, 이행, 유지, 개선을 위한 지침과 일반원칙을 정의하고 있습니다. 구조, 리스크 평가 및 관리, 보안정책, 정보보안조직, 자산관리, 인적자원보안, 물리적 보안, 통신 및 운영관리, 액세스 컨트롤, 정보보안사고관리, 비즈니스 연속성 및 준법에 대한 내용을 다루고 있습니다.

ISO 모듈에 포함된 사항

Akamai 네트워크, 경영 인프라, 관련 프로세스 및 절차는 ISO의 보안요건과 일치합니다. Akamai Compliance Management의 ISO 모듈은 전반적인 ISO 27001/27002 준수 프로세스를 가속시켜 줍니다. ISO 모듈에는 다음 내용이 포함되어 있습니다.

- ISO 27001/27002 표준 조건
- 아마카이의 ISO 27001/27002 연례평가 요약본
- 사고대응절차
- ISO 27001/27002 표준의 각 섹션에 대한 Akamai의 입장 요약, 뒷받침 할 수 있는 관련 서류에 대한 링크

FISMA 모듈

연방정보보안관리법(Federal Information Security Management Act, FISMA)는 각 연방기관이 다른 기관, 하청업체 등에서 제공 또는 관리하는 자산을 포함하여 기관의 운영과 자산을 지원하는 정보시스템과 정보의 정보보안을 제공하는 전사적인 프로그램을 개발, 문서화, 이행하도록 요구합니다. 2009년 8월 연방표준기술연구소 NIST 특별 간행물 800-53에 따라 미국 국토안보부로부터 운영 허가를 받았습니다(Authorization to Operate, ATO).

FISMA는 정보 및 정보 시스템의 승인되지 않은 접근, 사용, 공개, 개입, 수정, 파괴가 가져올 수 있는 피해의 정도를 포함한 리스크를 주기적으로 평가할 것을 요구합니다. 조직별 각 정보시스템의 전체 생애주기 동안 정보보안이 관리될 수 있도록 리스크평가를 기반으로 한 정책, 절차서, 시험, 시정조치 계획 및 교육을 요구합니다.

ISO 컴플라이언스 문서

Akamai Compliance Management ISO는 Akamai가 ISO 표준을 어떻게 준수하고 있는지에 대한 정보를 제공합니다.

본 페이지는 반드시 필요로 하는 ISO 정보를 포함하고 있습니다.

- 각 ISO 섹션의 요약과 세부내용의 링크를 나타낸 표
- Compliance Management ISO 조건

추가정보

- 서비스 기본내용에 대한 간략한 답변을 보려면 ISO Quick Fact 파일을 열어보십시오.
- Compliance Management Knowledgebase를 검색하시기 바랍니다.

섹션 번호별 ISO 준수

다음 표는 Akamai가 ISO를 어떻게 준수하고 있는지 ISO 섹션 번호별로 정렬한 것입니다. 문서에 있는 링크는 ISO섹션 번호 세부내용에 대한 준수를 설명하는 PDF 파일로 연결됩니다. 또는 표에 있는 모든 서류의 집파일을 다운로드 할 수 있습니다.

ISO 섹션	ISO 요건	Akamai 접근법	문서(PDF)
5	보안정책	Akamai는 모든 직원들이 이용할 수 있는 보안정책을 관리합니다. 보안위반에 대한 처벌에는 해고가 포함됩니다.	안전 및 보안 Akamai 정보보안정책
6	정보보안조직	Akamai는 정보보안 고위관리자가 이끄는 정보보안 전담팀이 있습니다. Akamai의 부 법무자문위원이 최고정보보호 책임자입니다.	PII 정보보안 책임 Akamai 정보보안정책
7	자산관리	Akamai에 속한 물리적 자산은 데이터베이스로 추적할 수 있습니다. Akamai 자산 사용에 대한 규칙과 제한사항이 수립되어 있습니다.	전자_통신_정책 PDA
8	인적자원보호	Akamai 직원들은 직무를 수행하기 위해 필요한 접근권을 부여받으며 보안 및 윤리에 관한 교육을 매년 받습니다. Akamai는 신규고용시 신원조회를 진행하고 직원들이 퇴사하는 즉시 접근권을 철회합니다.	Akamai_신원_조회_정책 기본원칙 보안_인식
9	물리적 환경적 보안	Akamai가 배치한 네트워크는 퍼블릭 인터넷을 통해 접근가능하도록 설계되었습니다. 회사 시스템은 악성코드로부터 보호하기 위한 추가 보호장치를 가지고 있습니다. Akamai 사무실은 잠금상태이며 직원들만 접근할 수 있습니다.	Akamai_바이러스 방지_정책

FISMA 준수 문서

Akamai Compliance Management FISMA는 FISMA 보안 표준을 Akamai가 어떻게 준수하고 있는지에 대한 정보를 제공합니다.

본 페이지는 반드시 필요로 하는 ISO 정보를 포함하고 있습니다.

- 각 FISMA 섹션의 요약과 세부내용의 링크를 나타낸 표
- Compliance Management FISMA 조건

추가정보

- 서비스 기본내용에 대한 간략한 답변을 보려면 NIST Quick Fact 파일을 열어보십시오.
- Compliance Management Knowledgebase를 검색해 보시기 바랍니다.

NIST 800-53 섹션 번호별 FISMA 준수

다음 표는 Akamai가 FISMA를 어떻게 준수하고 있는지 NIST 800-53섹션 번호별로 정렬한 것입니다. 문서에 있는 링크는 NIST 800-53섹션 번호 세부내용에 대한 준수를 설명하는 PDF 파일로 연결됩니다. 또는 표에 있는 FISMA 서류의 집파일을 다운로드 할 수 있습니다.

NIST 800-53 섹션	FISMA 요건	Akamai 접근법	문서(PDF)
AC	액세스 컨트롤	Akamai가 배치한 네트워크에 대한 접근은 엄격하게 통제되며 공식적인 승인이 필요합니다. 업무수행을 위해 접근이 필요한 Akamai 직원들에게만 접근이 허용됩니다. 모든 접근은 암호화된 연결을 통해 이루어집니다. 개발자들도 프로덕션 네트워크에는 접근할 수 없습니다.	구현된 네트워크 액세스
AT	인식 및 교육	Akamai는 신규고용 직원을 대상으로 보안에 대한 교육을 실시하고 연간 보안인식 캠페인을 실시합니다.	보안인식정책
AU	감사 및 책임성	경고관리 시스템은 Akamai가 배치한 네트워크를 실시간으로 감독하고 지속적으로 운영되는 아카마이 네트워크운영통제센터(NOCC)에 경고를 전송합니다. 조사목적으로 기록이 보관되며 조회보고 툴을 통해 기록에 접근할 수 있습니다.	경고관리 소프트웨어
CA	보안평가 및 승인	NIST 800-53을 준수하는 고객들은 규제를 준수하기 위해 Akamai와 협력합니다.	
CM	환경설정 관리	Akamai가 배치한 네트워크에 대한 변경은 일정한 단계를 거쳐 이루어집니다. 개발은 모범사례 가이드라인을 따라 이루어지며 싱글 릴리즈(릴리즈 이후 패치없이)로 개발되어야 합니다.	QA_SOGs 소프트웨어 개발 프로세스

Akamai Compliance Management

FISMA 모듈 패키지는 서비스, 문서, 서비스 조건을 제공하여 Akamai Intelligent Platform을 이용하는 고객들이 연방정보보안관리법의 모든 표준을 준수하는지 신속하게 검증할 수 있도록 해줍니다.

FISMA 모듈에 포함된 사항

Akamai 네트워크, 관리 인프라, 관련 프로세스와 절차는 연방정보시스템관리법과 NIST 특별 간행물 800-53에 명시된 보안요건에 부합합니다. Akamai Compliance Management의 FISMA 모듈은 전반적인 FISMA 준수 프로세스를 가속시켜 줍니다. FISMA 모듈에는 다음 내용이 포함되어 있습니다.

- 연방정보시스템관리법의 표준 조건
- 사고대응절차
- NIST 800-53 표준의 각 섹션에 대한 아카마이의 입장 요약, 뒷받침 할 수 있는 관련 서류에 대한 링크

BITS 모듈

BITS(www.bits.org)는 금융서비스 라운드테이블에 속한 세부 조직으로 미국의 100대 금융기관이 회원인 비영리 산업 컨소시엄입니다.

FISMA는 정보 및 정보 시스템의 승인되지 않은 접근, 사용, 공개, 개입, 수정, 파괴가 가져올 수 있는 피해의 정도를 포함한 리스크를 주기적으로 평가할 것을 요구합니다. 조직별 각 정보시스템의 전체 생애주기 동안 정보보안이 관리될 수 있도록 리스크 평가를 기반으로 한 정책, 절차서, 시험, 시정조치 계획 및 교육이 요구됩니다.

BITS 모듈 패키지는 서비스, 문서, 서비스 조건을 제공하여 아카마이 엣지 플랫폼을 이용하는 고객들이 BITS 자체진단 노력으로 만들어진 표준을 준수하는지 빠르게 검증할 수 있도록 해줍니다.

BITS 모듈에 포함된 사항

Akamai 네트워크, 경영 인프라, 관련 프로세스 및 절차는 BITS 표준이 명시한 보안요건과 일치합니다. Akamai Compliance Management의 BITS 모듈은 전반적인 BOTS 준수 프로세스를 가속시켜 줍니다. BITS 모듈에는 다음 내용이 포함되어 있습니다.

- BITS 표준 조건
- 사고대응절차
- BITS 표준의 각 섹션에 대한 Akamai의 입장 요약, 뒷받침 할 수 있는 관련 서류에 대한 링크

고객이 누릴 수 있는 혜택

- **리스크 감소**: Akamai SSL 네트워크의 사전 승인된 컴플라이언스 조건과 모범사례에 입각한 가이드라인을 통해 리스크 경감
- **네트워크 확장**: Akamai를 통해 컴플라이언스 노력 대비 보다 간편하게 네트워크 확장
- **신속성**: 사용하기 쉬운 검증도구와 문서화, Akamai SSL 네트워크의 사전인증을 통한 전체 컴플라이언스 프로세스 효율화·간소화
- **비용절감**: 완벽하게 준비된 준법관련 서류를 통해 엔드 투 엔드 네트워크 인프라에 대한 검토를 진행하는 과정에서의 부담 경감

BITS 준수 문서

Akamai Compliance Management BITS는 BITS 보안 표준을 Akamai가 어떻게 준수하고 있는지에 대한 정보를 제공합니다.

본 페이지는 반드시 필요한 BITS 정보를 포함하고 있습니다.

- 각 BITS 섹션의 요약과 세부내용의 링크를 나타낸 표
- Compliance Management BITS 조건

추가정보

- 서비스 기본내용에 대한 간략한 답변을 보려면 BITS Quick Fact 파일을 열어보십시오.
- Compliance Management Knowledgebase를 검색해 보시기 바랍니다.

BITS 준수

다음 표는 Akamai가 BITS를 어떻게 준수하고 있는지 BITS SIG 탭 번호별로 정렬한 것입니다. 문서에 있는 링크는 BITS SIG 탭 번호 세부내용에 대한 준수를 설명하는 PDF 파일로 연결됩니다. 또는 표에 있는 BITS 서류의 집파일을 다운로드 할 수 있습니다.

BITS SOG 탭	FISMA 요건	Akamai 접근법	문서(PDF)
A	리스크 관리	Akamai는 회사, 정보, 네트워크 보안에 대해 내부검토 및 리스크평가를 정기적으로 실시합니다. Akamai가 신규 서비스를 지속적으로 출시함에 따라 제품 설계·검토에 보안이 반영되어 있습니다. Akamai의 보안 전문가들은 정기적으로 여러 기능을 수행하는 팀을 만나 회사 및 네트워크 보안 문제에 대해 검토합니다.	취약점 관리 프로세스
B	보안정책	Akamai는 모든 직원들이 이용할 수 있는 보안정책을 관리합니다. 보안정책 위반에 대한 처벌에는 해고가 포함됩니다.	Akamai 정보보안정책 안전성 및 보안
C	조직보안	정보보안 이사는 Akamai의 보안 노력을 감독하는 역할을 하는 고위 경영진입니다. 정보보안 이사는 운영부사장에게 보고하며 Akamai 경영진 위원회와 월례 회의를 하여 현재 보안현황에 대해 검토합니다.	Akamai 정보보안정책 제3자를 위한 NDA 템플릿

Akamai Compliance Management

HIPAA 모듈

많은 보건의료 및 제약사, 비즈니스 파트너사들은 건강보험 이동 및 설명책임에 관한 법(HIPAA)과 HITECH와 같은 관련 규제를 준수해야 합니다. HIPAA, 건강정보, '프라이버시 규칙', '보안 규칙', HITECH에서는 보험회사가 보유하고 있는 개인의 건강정보를 연방차원에서 보호하고 정보에 대해 관련 환자들에게 권한을 줄 것을 요구하고 있습니다.

HIPAA와 관련 규제는 전자보호 건강정보의 기밀성, 무결성, 가용성을 보장하기 위해 사용할 수 있는 일련의 행정적, 물리적, 기술적 보호조치를 명시하고 있습니다. 전자보호건강정보의 보호에 관한 보안표준(이하 '보안규칙')은 특히 조직이 건강정보를 보호하기 위해 갖추어야 할 기술적, 비기술적 보호조치를 다루고 있습니다.

HIPAA 모듈 패키지는 서비스, 문서, 서비스 조건을 제공하여 아카마이 엣지 플랫폼을 이용하는 고객들이 미국 보건복지부가 시행하는 규정을 준수하는지 신속하게 검증할 수 있도록 합니다.

HIPAA 모듈에 포함된 사항

Akamai 네트워크, 관리 인프라, 관련 프로세스와 절차는 HIPAA와 관련 규정에 명시된 보안요건에 부합합니다. Akamai Compliance Management의 HIPAA 모듈은 전반적인 HIPAA 준수 프로세스를 가속합니다. HIPAA 모듈에는 다음 내용이 포함되어 있습니다.

- HIPAA의 표준 조건
- 사고대응절차
- HIPAA의 '보안규칙' 섹션을 다룬 문서
- Akamai에 적용되는 '프라이버시 규칙'
- 각 섹션 별 Akamai의 입장 요약

HIPPA 준수 문서

Akamai Compliance Management HIPAA는 HIPAA 보안 표준을 Akamai가 어떻게 준수하고 있는지에 대한 정보를 제공합니다. 아래 표는 각 HIPAA 섹션에 대한 Akamai 문서 목록을 나타냅니다. 각 섹션에서는 다음과 같은 정보가 제공됩니다.

- 구현 정보
- Akamai의 접근법
- 추가정보에 대한 링크

HIPAA 문서의 집 파일을 다운로드 할 수도 있습니다.

건강보험개혁: 보안표준: 최종규칙

보건복지부, 68 연방등록부 8334, 45 CFR 파트 160, 162, 164, 2003년 2월 20일
문서에서는 "본 최종 규칙은 건강보험 이동 및 설명책임에 관한 법(HIPAA) 261~264 섹션 2-F에서 요구하는 내용을 모두 채택하고 있다"고 밝히고 있습니다. 또한 본 문서는 "보안 규칙"이라고도 불리며 보호된 건강정보를 포함한 전자 데이터를 다루는 방법을 다룹니다.

보다 상세한 내용은 Akamai HIPAA 준수(PDF)를 참조하십시오. HIPAA 문서 집파일을 다운받을 수도 있습니다.

섹션	문서(PDF)
164.308 (a)(1) (i) 표준: 보안관리 프로세스	취약점 관리 프로세스 ISO 27001 보고서 요약 Akamai 기술위기 및 사건관리 절차서 안전성 및 보안 경보관리소프트웨어 운영데이터를 테스트 네트워크에서 삭제
164.308 (a)표준: 주어진 보안책임	Akamai 정보보안정책
164.308 (a)(3) (i) 표준: 직원보안	구현된 네트워크 액세스 액세스 컨트롤 설명 Akamai 신원 조회 정책 자동화된 시스템에 대한 민감한 종료 프로세스
164.308 (a)(4) (i) 표준: 정보 접근관리	구현된 네트워크 액세스 액세스 컨트롤 설명 기밀성, 소유, 개인정보 보호

현장 감사 모듈

Akamai는 PCI, ISO, FISMA, BITS, HIPAA에 대한 현장감사 모듈을 제공합니다. 주어진 표준을 준수하는지 검증하기 위해 아카마이의 지원이 필요한 고객들은 Akamai InfoSec(정보보안팀)의 지원을 받을 수 있습니다. 감사는 5일 동안 매사추세츠 캠브리지에 있는 Akamai 사무실에서 고정비용으로 진행됩니다. Akamai InfoSec 팀은 고객과 함께 Akamai 서비스의 중요한 내용을 검증할 수 있는 가장 효과적인 방법을 찾고 맞춤형 관리를 설계합니다. 별도의 고객참여 계약을 통해 추가적인 지원을 받을 수도 있습니다.

[1] 이 서비스는 표준에 대한 준수를 보장하지 않지만 고객들이 자체적인 준법 프로그램을 지원하는 활동에 도움이 됩니다.

Akamai FASTER FORWARD

전세계 콘텐츠 전송 네트워크(CDN) 분야를 이끌고 있는 Akamai는 빠르고 안전하며 신뢰할 수 있는 인터넷 환경을 제공합니다. Akamai는 웹 성능, 모바일 성능, 클라우드 보안, 미디어 전송과 관련된 우수한 솔루션을 공급하고 있으며 이 과정에서 사용 기기나 장소에 상관없이 소비자, 기업, 엔터테인먼트 경험을 최적화하는 방법을 크게 바꿔놓고 있습니다. Akamai의 인터넷 전문가들과 솔루션이 어떻게 기업의 성장을 뒷받침하고 있는지 자세히 알아보려면 Akamai 홈페이지(www.akamail.co.kr) 혹은 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 Akamai(@Akamai)를 팔로우 하십시오.

Akamai는 미국 매사추세츠주 케임브리지에 본사를 두고 있으며 전세계 40여 개의 지사를 운영하고 있습니다. Akamai의 우수한 솔루션과 서비스를 사용하는 기업들은 전세계 고객들에게 우수한 웹 경험을 제공할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표번호는 02-2193-7200입니다.

2015년 4월 발행.