

IBM Payments Gateway

본 서비스 명세는 IBM 이 고객에게 제공하는 클라우드 서비스에 대해 설명합니다. 고객이란 클라우드 서비스의 대상 회사, 허가된 사용자 또는 수령자를 의미하며 이들을 포함합니다.

1. 클라우드 서비스

IBM 이 제공한 클라우드 서비스 오퍼링은 아래에 설명되어 있습니다. 관련 견적서와 라이선스 증서(PoE)는 별도의 거래서류로 제공됩니다.

IBM Payments Gateway

IBM Payments Gateway 는 개발, 사전 프로덕션 및 프로덕션 환경과의 연결성을 제공합니다. 다음 기능이 포함됩니다.

- 민감한 대금 지급 정보에 대한 보안을 제공하도록 설계된 스토리지 기능인 PCI(Payment Card Industry) 저장 장치
- 제 3 자 프로세서와의 대금 지급 트랜잭션에서 라우팅, 전환 및 처리를 수행하는 대금 지급 게이트웨이
- 콜센터, 신용 관리 및 back-office 대금 지급 작업에서 지급 추심 목적으로 설계된 웹 툴인 가상 터미널
- 보안 기능으로 설계된 인증
- 사기 방지 툴
- 보고서 생성 기능
- 문서

1.1 추가 서비스

고객은 다음 클라우드 서비스 Payment 오퍼링 중 최소 하나와 함께 IBM Payments Gateway 를 구입해야 합니다.

a. IBM Payments Gateway API Payment

다음 기능이 포함됩니다.

- 트랜잭션은 클라이언트 시스템과의 통합이 용이하도록 설계된 웹 서비스 세트로 구성되는 API 를 통해 전송됩니다. 해당 API 는 여러 국가와 통화 단위에서 은행과 처리자 간의 글로벌 대금 지급에 필요한 단일한 인터페이스를 제공합니다.

b. IBM Payments Gateway Hosted-Page Payment

다음 기능이 포함됩니다.

- 트랜잭션은 웹 사이트, 모바일 커머스 사이트, 스마트폰 앱, 콜센터 애플리케이션, back-office 콜렉션 시스템으로 통합되도록 설계된 대금 지급 추심 및 지급 관리 GUI 인 HPP(Hosted Payment Page)를 통해 전송됩니다. HPP(Hosted Payment Page)는 HTML 인라인 프레임(iframe)으로 전달되도록 설계되어 있습니다.

c. IBM Payments Gateway Advanced API Payment

다음 기능이 포함됩니다.

- 트랜잭션은 기본 스마트폰 애플리케이션에서 대금 지급 기능을 용이하게 개발할 수 있도록 설계된 JSON(JavaScript Object Notation) 인터페이스를 통해 전송됩니다.
- JSON 인터페이스는 JSON 형식으로 전달되는 데이터와 함께, 관련 URL 에서 HTTP 메소드를 사용하여 수행되는 대금 지급 API 세트를 제공합니다.

다음 IBM Payments Gateway 오퍼링을 선택적으로 구입할 수 있습니다.

d. IBM Payments Gateway Settlement

다음 기능이 포함됩니다.

- 트랜잭션은 결제를 완료할 수 있는 대금 지급 정보를 포함하여 판매자에서 구매자의 금융 기관으로 전송됩니다.

2. 보안 설명

2.1 보안 정책

IBM은 정보 보안 팀을 운영하며 IBM 직원에게 통지하는 개인 정보 보호 및 보안 정책도 유지 관리합니다. IBM 직원은 매년 개인정보 및 보안에 대한 교육을 이수해야 합니다. IBM 보안 정책은 업계 규정과 IBM 비즈니스 요구사항에 따라 매년 재평가됩니다. 보안 사고는 종합적인 사고 대응 절차에 따라 처리됩니다. IBM은 제한되고 감시되는 접근 지점을 포함하여 IBM 데이터 센터에서 권한이 부여된 직원에 대한 접근 권한을 제한하도록 작성된 물리적 보안 기준을 유지 관리합니다. 방문자는 입장 후에 등록하며 근무지 사이트에 있는 동안 안내자가 동행합니다.

2.2 접근 권한 통제

IBM 인증 스택은 중간 "게이트웨이"(gateway) 관리 호스트에 대한 이중(two-factor) 인증 방식을 사용합니다. 알려져 있는 손상된 인터넷 사이트 및 미국 통상 금지국의 사용자에 의한 접근을 방지하도록 IP 차단 기능을 사용할 수 있습니다. 고객 데이터에 대한 접근과 호스팅 환경 내외부로 데이터 전송은 모두 기록됩니다. 이 클라우드 서비스를 지원하는 IBM 데이터 센터 내부에서는 WIFI 사용이 금지됩니다.

클라우드 서비스에서는 IBM 네트워크와 고객의 네트워크 액세스 지점 간에 데이터가 전송되는 동안 콘텐츠를 암호화해야 합니다. 세부 암호화 방식은 고객과의 계약을 통해 특정되며, 암호화를 위해 IBM과 고객 사이트 모두에서 SSL 인증을 설치해야 합니다. 대금 지급 처리에 필요한 개인 정보만 수집합니다. 클라우드 서비스는 데이터 전송을 대기하는 정지 기간 동안 콘텐츠를 암호화합니다.

2.3 서비스 무결성 및 가용성

운영 체제, 애플리케이션 소프트웨어 및 방화벽 규칙에 대한 수정사항은 IBM 변경 관리 프로세스에 따라 처리됩니다. 방화벽 규칙의 변경사항은 구현하기 전에 IBM 보안 직원의 검토를 별도로 받습니다. IBM은 데이터 센터를 24x7 원칙으로 감시합니다. 허가된 관리자와 제 3자 벤더는 내외부 취약성 스캐닝을 정기적으로 실시하여 잠재적인 시스템 보안 문제를 발견하고 해결할 수 있도록 지원합니다. 모든 IBM 데이터 센터에는 악성 소프트웨어 감지 시스템(안티바이러스, 침입 감지, 취약성 스캐닝 및 침입 방지)이 사용됩니다. IBM 데이터 센터 서비스는 공용 네트워크에서 데이터를 전송하기 위해 다양한 정보 전달 프로토콜을 지원합니다. 예를 들면, HTTPS/SFTP/FTPS/S/MIME, site-to-site VPN이 있습니다. 오프 사이트 저장 목적의 백업 데이터는 전송되기 전에 암호화됩니다.

2.4 활동 로깅

IBM은 활동 로깅 용도로 구성된 시스템, 애플리케이션, 데이터 저장소, 미들웨어 및 네트워크 인프라스트럭처 디바이스의 활동 로그를 유지 관리합니다. 로그의 조작을 방지하고 중앙 집중적 분석, 경보 및 보고 기능을 수행할 수 있도록 활동 로깅은 중앙 로그 저장소에서 실시간으로 처리됩니다. 조작 방지를 위해 데이터는 서명됩니다. 이상 동작을 찾기 위해 정기 분석 보고서를 통해 로그를 실시간으로 분석합니다. 운영 직원(또는 그에 준하는)에게 이상 동작을 통지하고 필요한 경우 24x7 on-call 보안 전문가에게 문의합니다.

2.5 준수

IBM은 IBM 정보 보안 정책을 준수하도록 프로덕션 IBM Payments Gateway 데이터 센터에서 매년 업계 표준 ISAE3402 16 감사(또는 그와 동등한 감사)를 실시합니다. IBM의 매해 PCI DSS 인증에는 모든 IBM Payments Gateway 데이터 센터에서 외부 자격있는 보안 평가인 (Qualified Security Assessor)(Trustwave)에 의한 현장 감사가 포함됩니다. 요청이 있는 경우 AoC(Attestation of Compliance) 또는 준수 확인서(Compliance Letter)를 고객과 감사자에게 제공할 수 있습니다.

2.6 보안 정책

IT 시스템 보안은 귀하 기업집단 내외부의 부적절한 액세스를 예방하고 감지하고 대응하여 시스템과 정보를 보호합니다. 부적절한 액세스는 정보의 변경, 파괴, 유출 또는 다른 사용자를 공격하는 귀하 시스템의 오용을 초래할 수 있습니다. 포괄적인 보안책에 대한 고려 없이 IT 시스템이나 제품을 완벽하게 보호할 수 있는 방법은 없으며 단일 제품이나 보안 조치가 부적절한 액세스를 예방하는 데 완전하게 효과적일 수는 없습니다. IBM 시스템과 제품은 포괄적인 보안책의 일부가 될 수 있도록 디자인됩니다. 포괄적인 보안책에는 필연적으로 추가 운영 절차가 포함될 수도 있고 효과적인 다른 시스템, 제품 또는 서비스가 필요할 수도 있습니다. IBM은 시스템과 제품이 제 3 자의 유해 제품이나 불법 제품으로부터 안전하다고 보증하지 않습니다.

2.7 개인 정보 보호

IBM과 고객은 각각 본 계약에 의거하여 IBM이 고객을 위해 저장하거나 처리한 개인 데이터(관련 정보 보호법에서 정의 됨)(이하 "고객 데이터")를 규제하는 적용되는 데이터 보호법 하의 각각의 의무사항을 준수해야 할 책임이 있습니다. 본 계약을 체결함으로써 고객은 IBM을 고객 데이터의 데이터 처리자로 지정합니다. 고객의 지시에 따른 정보 처리로 인해 IBM이 관련 개인 정보 보호법을 위반하게 하지 않도록 해야 한다는 것을 포함하여, 본 계약에 의거한 IBM의 고객 데이터 처리 목적과 방법을 결정할 책임은 전적으로 고객에게 있습니다. IBM과 고객은 각각 관련 정보 보호법을 준수하기 위해 상대방이 수행하는 조치를 살피고 있지 않는 것을 인정합니다. 본 계약의 어떠한 조항도 관련 정보 보호법을 준수하는 데 필요하다고 간주되는 조치를 IBM이나 고객이 수행하지 못하도록 금지하지 않습니다. 고객이 관련 정보 보호법을 준수하기 위해 추가 서비스나 다른 서비스를 요청하는 경우, 고객은 필요한 서비스가 별도의 계약 서비스 참여를 통해 전달되도록 요청할 수 있습니다. 고객은 본 계약에서 특정된 보안 조치가 관련 정보 보호법에서 요구하는 고객 데이터를 보호하기 위한 적절한 기술적 및 조직적 조치인지 판단할 책임이 전적으로 고객에게 있다는 것을 인정합니다. IBM은 본 계약에서 지정한 보호조치 외에 그리고 고객 데이터의 처리자로서 외에 고객 데이터에 대해 보호조치를 수행하거나 준수해야 할 필요는 없습니다; IBM은 본 계약에서 지정한 대로, 그리고 서비스를 수행하는 데 필요하거나 적절하다고 IBM이 합리적으로 간주하는 대로 고객 데이터를 처리합니다. 본 계약에 의거하여 IBM 또는 고객에 의한 고객 데이터의 해외 전송이 관련 정보 보호법을 준수하는지 판단할 책임은 전적으로 고객에게 있습니다.

3. SLA(Service Level Agreement)

IBM은 거래서류에 명시된 바와 같이 클라우드 서비스의 "서비스 레벨 계약"(이하 SLA)을 제공합니다. SLA는 보증이 아닙니다.

3.1 용어 정의

- a. **서비스 크레딧** - 유효한 클레임에 대해 IBM이 제공하는 보상을 의미합니다. 서비스 크레딧은 IBM으로부터 직접 취득한 클라우드 서비스의 경우 추후 청구서에 대한 크레딧의 형식으로 적용됩니다. IBM 비즈니스 파트너로부터 클라우드 서비스를 취득한 경우 IBM은 고객이 직접 사용할 수 있는 리베이트를 제공합니다.
- b. **클레임** - 계약 월 동안 서비스 레벨이 충족되지 못하였다고 고객이 IBM에 제출하는 배상 청구를 의미합니다.
- c. **계약 월** - 해당 월 1일 12:00 AM(미 동부시)부터 해당 월 말일 11:59 PM(미 동부시)까지 측정된 클라우드 서비스 기간 동안의 각 역월(calendar month)을 의미합니다.
- d. **중지 시간** - 고객에게 사용 권한이 부여된 클라우드 서비스에 대한 프로덕션 시스템 처리가 이용 불가능한 기간의 시간을 의미합니다. 중지 시간에는 다음으로 인해 클라우드 서비스를 사용할 수 없는 기간은 포함되지 않습니다.
 - (1) 스케줄되거나 통지된 유지보수 목적의 가동 중단
 - (2) IBM의 통제권을 벗어난 이벤트 또는 원인(예: 자연 재해, 인터넷 중단, 긴급 유지보수 등);
 - (3) 고객이 클라우드 서비스와 함께 사용하는 콘텐츠, 설비, 애플리케이션, 또는 제 3 자의 소프트웨어, 하드웨어 또는 기타 기술의 문제점

- (4) 고객이 필수 시스템 구성과 지원되는 플랫폼을 준수하지 않거나 고객 시스템 관리, 명령 또는 프로그래밍의 오류.
 - (5) 고객이 야기한 보안 위반 행위나 고객이 수행한 보안 테스트, 또는
 - (6) 고객이 IBM 에게 제공하거나 고객을 대신한 제 3 자가 IBM 에 제공한 설계, 명세 또는 지침을 IBM 이 따른 경우.
- e. **이벤트** - 특정 상황 또는 여러 상황이 합쳐져서 결과적으로 SLA 에 부합되지 못하게 한 경우, 그러한 특정 상황 또는 여러 상황을 의미합니다.
- f. **응답 시간** - CheckoutStartSession 및/또는 CardAuthorize 웹 서비스가 IBM 시스템의 엔트리 포인트(entry point)에서 요청을 수신한 시점부터 IBM 웹 서비스 응답이 고객에게 전송된 시점까지 걸린 시간을 의미합니다.

3.2 서비스 크레딧

클레임을 제출하기 위해서는 이벤트가 클라우드 서비스의 사용에 영향을 준 것을 처음으로 인식한 시간으로부터의 24 시간 이내에 각 이벤트에 대해 각 이벤트의 심각도 1 지원 티켓(아래 기술 지원 조항에서 정의된 사항 참조)을 고객이 IBM 기술 지원 헬프 데스크에 로그(log)해야 합니다. 고객은 이벤트에 대한 필요한 정보를 모두 제공하고 진단과 해결을 위해 합리적인 범위 내에서 IBM 에 협력해야 합니다.

서비스 크레딧에 대한 클레임은 클레임이 발생한 계약 월의 말일 이후 삼(3) 영업일 이내에 제출되어야 합니다.

IBM 은 아래 표에서 관련 서비스 레벨에 해당하는 각 계약 월 동안의 총 중지 시간을 내부적으로 계산합니다. 서비스 크레딧은 중지 시간이 최초로 발생했다고 귀하가 보고한 시점부터 측정된 중지 시간의 기간을 기준으로 합니다.

- a. 고객이 웹 서비스, HPP(Hosted Payment Page) 및 가상 터미널 중지 시간 이벤트가 동시에 발생된 것으로 보고한 경우에는, IBM 은 중지 시간이 겹치는 기간을 단일 중지시간 기간으로 간주하며 별도의 두 개의 중지 시간의 기간으로 보지 않습니다.
- b. 고객이 CheckoutStartSession 및 CardAuthorize 웹 서비스 응답 시간 중지 시간 이벤트가 동시에 발생된 것으로 보고한 경우에는, IBM 은 응답 시간 중지 시간이 겹치는 기간을 단일 응답 시간 중지 시간 기간으로 간주하며 별도의 두 개의 응답 시간 중지 시간의 기간으로 보지 않습니다.

유효한 각 클레임의 경우, IBM 은 아래 표와 같이 각 계약 월 동안 달성한 서비스 레벨에 따라 적용 가능한 최대의 서비스 크레딧을 적용합니다. IBM 은 동일한 계약 월의 동일한 이벤트에 대해 여러 번의 크레딧을 제공할 책임이 없습니다.

IBM 비즈니스 파트너로부터 클라우드 서비스를 취득한 경우, 서비스 크레딧은 클레임 대상이 되는 계약 월당시에 유효한 클라우드 서비스에 대한 정가의 월 등록 사용료를 기준으로 50% 할인되어 산정됩니다.

여하한 계약 월에 적용되는 서비스 크레딧의 총 금액은 클라우드 서비스의 연간 대금의 12 분의 1(1/12)의 10%를 초과할 수 없습니다.

3.3 서비스 레벨

IBM 웹 서비스, HPP(Hosted Payment Page) 및 가상 터미널 인터페이스는 계약 당월 중 시간의 최소 99.95%의 시간 동안 고객에게 제공됩니다.

가용률 (계약 월 동안)	서비스 크레딧(클레임 대상이 되는 계약 월의 월 등록(Subscription) 사용료의 %)
<99.95%	2%
< 99.80%	4%
< 99.60%	6%
< 99.30%	8%
< 99.00%	10%

백분율로 표시된 가용성은 계약 월에서 IBM 웹 서비스, HPP(Hosted Payment Page) 및 가상 터미널이 사용 가능하고 고객의 요청에 응답하는 총 시간(분)을 계약 월의 총 시간(분)으로 나눈 후 100 을 곱하여 계산합니다.

3.4 계약 월 동안의 IBM 웹 서비스 응답 시간

IBM 은 다음과 같이 두 가지 응답 시간 SLA 를 제공합니다.

3.4.1 IBM 웹 서비스 응답 시간 중간값

CheckoutStartSession 및 CardAuthorize 웹 서비스의 IBM 응답 시간 중간값은 100 밀리초 미만입니다.

특정 웹 서비스의 IBM 응답 시간은 웹 서비스 요청이 IBM 의 시스템에 대한 엔트리 포인트(entry point)에서 수신된 시점부터 IBM 웹 서비스 응답이 고객에게 전송된 시간까지 걸린 시간에서 IBM 시스템이 후속의 제 3 자 처리자 응답을 대기하는 데 걸린 여하한 시간을 제하여 측정합니다.

서비스 레벨 목표는 주어진 계약 월의 전체 웹 서비스 요청에서 CheckoutStartSession 및 CardAuthorize 웹 서비스에 대한 각 중간값으로 계산합니다.

응답 시간 중간값 (계약 월 동안)	서비스 크레딧(클레임 대상이 되는 계약 월의 월 등록(Subscription) 사용료의 %)
> 100 밀리초	2%
> 500 밀리초	6%
> 1 초	10%

3.4.2 IBM 웹 서비스 응답 시간 99%

CheckoutStartSession 및 CardAuthorize 웹 서비스의 99%는 IBM 응답 시간이 1 초 미만입니다.

IBM 응답 시간은 위에서 IBM 웹 서비스 응답 시간으로 정의된 방법과 동일하게 계산합니다.

서비스 레벨 목표는 주어진 역월의 전체 웹 서비스 요청에서 CheckoutStartSession 및 CardAuthorize 웹 서비스에 대한 각 99 백분위 수로 계산합니다.

응답 시간 99% (계약 월 동안)	서비스 크레딧(클레임 대상이 되는 계약 월의 월 등록(Subscription) 사용료의 %)
> 1 초	2%
> 5 초	6%
> 10 초	10%

3.5 SLA 에 대한 기타 정보

본 SLA 는 고객 회사에 제공되며 클라우드 서비스의 사용자의 청구나 베타 서비스나 시험 서비스에 대한 클레임에는 적용되지 않습니다. SLA 는 프로덕션 용도의 클라우드 서비스에만 적용됩니다. 테스트, 재해 복구, 품질 보증 또는 개발을 포함한(단, 이에 한하지 않음) 비프로덕션 환경에는 SLA 가 적용되지 않습니다. IBM 은 가용성 서비스 레벨 중단이 동일한 기간 동안에 기록된 경우 응답 시간 서비스 크레딧에 대한 클레임을 처리하지 않습니다.

4. SLO(Service Level Objectives)

다음 SLO 는 목표치이며 고객에 대한 보증사항은 아닙니다. IBM 이 SLO 을 달성하지 못하더라도 환불, 크레딧 또는 구제책이 고객에게 제공되지는 않습니다.

서비스	목표
일괄처리 소요 시간	전체 트랜잭션 일괄처리의 90%는 수신 후 60 분 미만으로 처리 완료됩니다.
이메일 대응성	IBM 공유 지원 메일함에 전송된 이메일의 95%는 24 영업시간 이내에 답변이 제공됩니다.

서비스	목표
24x7 도움말 데스크 전화 응답 시간	IBM 24x7 도움말 데스크는 60 초 미만으로 전화 호출에 응답합니다.
보안 관리	<ul style="list-style-type: none"> ● IBM PCI-DSS 레벨 1 인증은 매년 최소 한 번 갱신됩니다. ● IBM 은 심각도가 높은 보안 취약점을 10 일 이내에 개선합니다. ● IBM 은 심각도가 낮은 보안 취약점을 30 일 이내에 개선합니다.
사전 프로덕션 시스템 가용성	<ul style="list-style-type: none"> ● 클라이언트 테스트 24x7 가능 ● 사전 프로덕션 시스템은 중앙 유럽의 정상 영업 시간 외에는 무인으로 운영됩니다. ● 사전 프로덕션 시스템의 사고는 기본적으로 심각도 3 으로 처리됩니다.

5. 기술 지원

클라우드 서비스에 대한 기술 지원은 이메일과 전화로 제공됩니다. 기술 지원의 일부로 IBM 이 제공하는 개선사항, 업데이트 및 기타 자료는 클라우드 서비스의 일부로 간주되며 이에 따라 본 서비스 명세가 적용됩니다. 기술 지원은 클라우드 서비스에 포함되며 별도의 오퍼링으로 제공되지 않습니다.

가용성 시간, 이메일 주소, 온라인 문제점 보고 시스템 및 기타 기술 지원 교신 방법과 절차에 대한 자세한 정보는 IBM Software as a Service Support Handbook 에 설명되어 있습니다.

심각도	심각도 정의	대응 시간 목표	대응 시간 범위
1	중대한 업무 영향/서비스 다운: 중대한 업무 기능이 작동 불가능하거나 중대한 인터페이스에 장애가 발생한 경우. 일반적으로 프로덕션 환경에 적용되며 서비스에 대한 액세스 불능으로 인해 운영에 중대한 영향을 끼치는 경우를 의미합니다. 이 경우 즉각적인 해결책을 제공해야 합니다.	15 분 이내에 고객에게 알림	24x7
2	상당한 업무 영향: 서비스 업무 기능이 사용에 있어 상당히 제한되거나 귀하가 업무 기한을 준수하지 못하게 됩니다.	15 분 이내에 고객에게 알림	월요일 - 금요일 현지 영업시간
3	사소한 업무 영향: 서비스 또는 기능을 이용할 수 있으며 운영에 대한 심각한 영향이 없는 것을 의미합니다.	알림 필요 없음	월요일 - 금요일 현지 영업시간
4	최소 업무 영향: 조사 또는 비기술적 요청.	알림 필요 없음	월요일 - 금요일 현지 영업시간

6. 권한 부여 및 대금 청구 정보

6.1 과금 체계

본 클라우드 서비스는 거래서류에 명시된 바와 같이 다음 과금 체계 하에서 제공됩니다.

- a. **인스턴스(Instance)** - 클라우드 서비스 구입 시 사용되는 측정 단위입니다. 하나의 인스턴스는 클라우드 서비스의 특정 구성에 대한 액세스를 의미합니다. 고객의 라이선스 증서나 거래서류에 명시된 측정 기간 동안 액세스하여 사용하도록 제공된 클라우드 서비스의 각 인스턴스에 대해 충분한 권한을 취득해야 합니다.
- b. **TE(Thousand Events)** - 클라우드 서비스 구입 시 사용되는 측정 단위입니다. TE 권한은 클라우드 서비스 사용과 관련된 특정 이벤트를 1000 개 단위로 측정하여 그 발생 횟수를 기준으로 합니다. TE 권한은 클라우드 서비스에서 고유하며 다른 클라우드 서비스 또는 이벤트 유형의 다른 TE 권한으로 이벤트 유형을 대체하거나 상호 교환하거나 통합될 수 없습니다. 라이선스 증서(PoE)나

거래서류에 명시된 측정 기간 동안 발생한 모든 이벤트를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

- c. **이벤트** - 이 클라우드 서비스의 경우, 하나의 이벤트는 1000 개 단위로 계수된 마스터 트랜잭션을 의미합니다. 마스터 트랜잭션은 프로그램 외부의 애플리케이션에서 시작되거나(예: 비즈니스 뱅킹 웹 채널, 매뉴얼 메시지 입력 채널) 프로그램에서 이벤트에 의해 트리거되는(예: 반복적 대금 지급, 벌크 처리 시작 시간) 명령어 세트입니다. 마스터 트랜잭션은 다양한 처리 단계와 연계되어 외부 애플리케이션에 최종 명령이 전송되거나 처리 라이프사이클이 완료되면 종료되는 모든 이벤트와 업데이트를 포함하여 관련 비즈니스 활동 및 논리적 작업 단위를 관리합니다. 마스터 트랜잭션은 처리 라이프사이클 중에 기본 트랜잭션을 시작합니다.

6.2 월 분할(Partial Month) 요금

거래서류에 명시된 월 분할 요금은 비례 배분하여 산정될 수 있습니다.

6.3 추가 요금

측정 기간 동안 클라우드 서비스 실제 사용량이 라이선스 증서에 지정된 권한을 초과하면 거래서류에 지정된 대로 초과분에 대한 요금이 고객에게 부과됩니다.

7. 기간 및 갱신 옵션

7.1 기간

클라우드 서비스의 기간은 라이선스 증서에 명시된 바와 같이, IBM 이 고객에게 클라우드 서비스에 대한 고객의 액세스 권한에 대해 통지한 날부터 시작됩니다. 고객은 IBM 또는 고객의 IBM 비즈니스 파트너에게 연락하여 해당 기간 동안 고객의 클라우드 서비스의 사용 레벨을 상향 조정할 수 있으며 그러한 상향 조정은 거래서류를 통해 확정됩니다.

7.2 기간 갱신 옵션

다음 중 클라우드 서비스 기간 갱신에 적용되는 사항이 거래서류에 명시됩니다.

7.2.1 자동 갱신

자동 갱신의 경우, 기간 만료일에서 최소 90 일 이전에 고객이 서면 해지서를 제공하지 않는 한 클라우드 서비스는 거래서류에 지정된 기간(1 년 또는 만료되는 기간과 동일한 기간)만큼 자동으로 갱신됩니다.

7.2.2 연속적 청구

연속적 청구의 경우, 고객은 고객의 기간이 종료된 후에도 계속해서 클라우드 서비스에 대한 액세스 권한을 가지며 지속적으로 사용 대금이 청구됩니다. 클라우드 서비스의 사용을 중단하고 연속적 청구 절차를 중지하려면 고객은 고객의 클라우드 서비스의 취소를 요청하는 서면 통지를 90 일 전에 IBM 이나 고객의 IBM 비즈니스 파트너에게 제공해야 합니다. 취소되는 달의 말일까지의 미지불 액세스 대금이 고객에게 청구됩니다.

7.2.3 갱신

갱신 유형이 "종료"로 지정된 경우에는 클라우드 서비스는 기간의 종료 시 해지되며 고객의 액세스 권한도 종료됩니다. 기간 종료일 후에도 클라우드 서비스를 계속 사용하려면 고객은 새로운 등록 기간을 주문해야 합니다.

8. 일반조항

해당하는 경우, 세금은 클라우드 서비스의 혜택을 제공받는 사업장을 기준으로 부과됩니다. 고객이 IBM 에 추가 정보를 제공하지 않는 한, IBM 은 고객의 주문서에 기재된 비즈니스 주소에 따라 세금을 적용합니다. 고객은 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM 에 제공해야 할 책임이 있습니다.