# IBM Security Trusteer Fraud Protection

이용 약관은 본 IBM 이용 약관 – SaaS 특정 오퍼링 조항(이하 "SaaS 특정 오퍼링 조항")과 IBM 이용 약관 – 일반 조항(이하 "일반 조항") 문서(URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/ 참조)로 구성됩니다.

조항이 상충하는 경우에는 SaaS 특정 오퍼링 조항이 일반 조항에 우선하여 적용됩니다. IBM SaaS 를 주문하거나 액세스하거나 사용함으로써 고객은 이용 약관에 동의하게 됩니다.

이용 약관에는 해당 IBM International Passport Advantage 계약, IBM International Passport Advantage Express 계약 또는 선택한 IBM SaaS 오퍼링에 관한 IBM 국제 계약(IBM International Agreement for Selected IBM SaaS Offerings)이 적용되며 이용 약관과 함께 완전한 계약을 구성합니다.

## 1. IBM SaaS

다음 IBM SaaS 오퍼링에는 본 SaaS 특정 오퍼링 조항이 적용됩니다.

### 1.1 Rapport IBM SaaS 오퍼링

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

### 1.2 Pinpoint IBM SaaS 오퍼링

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business

- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

### 1.3 Mobile IBM SaaS 오퍼링

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

## 2. 과금 체계

IBM SaaS 는 거래서류에 지정된 바와 같이 다음 중 하나의 과금 체계 하에서 판매됩니다.

a. **적격 참여자(Eligible Participant)** – IBM SaaS 구입 시 사용되는 측정 단위입니다. IBM SaaS 에서 관리하거나 추적하는 서비스 제공 프로그램에 참여할 수 있는 각 개인이나 법인을 적격 참여자라고 합니다. 고객의 거래서류에 명시된 측정 기간 동안 IBM SaaS 내에서 관리하거나 추적한 모든 적격 참여자를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

   IBM SaaS 에서 관리한 각 서비스 제공 프로그램을 개별적으로 분석한 후 모두 함께 추가합니다. 여러 서비스 제공 프로그램을 사용하는 개인이나 법인은 개별 권한이 필요합니다.

   해당 오퍼링의 경우 서비스 제공 프로그램에는 각 Business 또는 Retail 애플리케이션의 기본 로그인 페이지 및 관련 페이지를 포함한 고객의 단일한 Business 또는 Retail 애플리케이션이 포함되어 있습니다. 적격 참여자는 Business 또는 Retail 애플리케이션의 로그인 인증 정보를 보유하고 있는 고객의 최종 사용자입니다.

b. **클라이언트 디바이스(Client Device)** – IBM SaaS 구입 시 사용되는 측정 단위입니다. 클라이언트 디바이스란 일반적으로 서버라고 부르거나 서버에 의해 관리되는 다른 컴퓨터 시스템에서 명령, 프로시저 또는 애플리케이션 세트에 대한 실행을 요청하거나 수신하는 단일 사용자 컴퓨팅 디바이스 또는 특수 용도의 센서나 원격 측정 디바이스를 의미합니다. 다중 클라이언트 디바이스는 공통 서버에 대한 액세스를 공유할 수 있습니다. 클라이언트 디바이스는 일부 처리 기능을 갖추고 있거나 사용자가 작업을 수행할 수 있도록 프로그램화될 수 있습니다. 고객은 고객의 거래서류에 명시된 측정 기간 동안 IBM SaaS 를 실행하거나 IBM SaaS 에 데이터를 제공하거나 IBM SaaS 가 제공한 서비스를 이용하거나 IBM SaaS 에 달리 액세스하는 각 클라이언트 디바이스에 대한 권한을 취득해야 합니다.

## 3. 대금 및 청구

IBM SaaS 에 대한 청구 금액은 거래서류에 명시됩니다.

### 3.1 월 분할(Partial Month) 요금

거래서류에 명시된 월 분할 요금은 비례 배분하여 산정될 수 있습니다.

## 4. 준수 및 감사

IBM Security Trusteer Fraud Protection 오퍼링에 대한 액세스는 거래서류에 지정된 적격 참여자 또는 클라이언트 디바이스의 최대 수 범위로 제한됩니다. 고객은 적격 참여자 또는 클라이언트 디바이스의 수가 거래서류에 지정된 최대 수를 초과하지 않는지 확인해야 할 책임이 있습니다.

적격 참여자나 클라이언트 디바이스의 최대 수를 준수하는지 여부를 확인하기 위해 감사를 수행할 수 있습니다.

## 5. IBM SaaS 등록(Subscription) 기간 갱신 옵션

다음 중 하나를 선택하여 IBM SaaS 의 등록 기간 종료 시 갱신 여부를 고객의 거래서류에 명시합니다.

### 5.1 자동 갱신

고객의 거래서류에서 자동 갱신으로 명시한 경우 고객은 거래서류에 지정된 만료일보다 최소 90 일 이전에 고객의 IBM 영업 담당자 또는 IBM 비즈니스 파트너에게 서면 요청서를 통해 IBM SaaS 등록 기간을 해지할 수 있습니다. IBM 또는 IBM 비즈니스 파트너가 만료일까지 그러한 해지 통지를 수신하지 못하면 등록 기간은 1 년 또는 거래서류에 명시된 최초 등록 기간과 동일한 기간만큼 자동으로 갱신됩니다.

### 5.2 연속적 청구

거래서류에서 연속적 갱신으로 명시한 경우 고객은 계속해서 IBM SaaS 에 대한 액세스 권한을 가지며 연속적 기준에 따라 IBM SaaS 의 사용 대금이 청구됩니다. IBM SaaS 사용을 중단하고 연속적 청구 절차를 중지하려면 고객은 고객의 IBM SaaS 의 취소를 요청하는 90 일 사전 서면 통지를 IBM 이나 IBM 비즈니스 파트너에게 제공해야 합니다. 고객의 액세스가 취소되면 취소가 발효된 해당 월의 미지불된 액세스 대금이 고객에게 청구됩니다.

### 5.3 갱신

거래서류에서 고객의 갱신 유형을 "종료"로 지정한 경우에는 등록 기간이 만료되면 IBM SaaS 가 종료되며 IBM SaaS 에 대한 고객의 액세스 권한은 소멸됩니다. 종료 날짜 이후에도 IBM SaaS 를 계속 사용하려면 고객은 IBM 영업 담당자나 IBM 비즈니스 파트너에게 새로운 등록 기간을 구매하는 주문서를 접수해야 합니다.

## 6. 기술 지원

IBM SaaS 의 사용을 지원하기 위한 IBM SaaS 기술 지원을 고객과 고객의 적격 참여자에게 제공합니다.

표준 지원은 모든 오퍼링 등록에 포함되어 있습니다. Trusteer Rapport 의 추가 기능인 Trusteer Rapport Mandatory Service 에는 기본 Trusteer Rapport 등록의 프리미엄 지원이 선행 조건으로 포함됩니다.

IBM Security Trusteer Mobile SDK 오퍼링 및 IBM Security Trusteer Rapport Mandatory Service 오퍼링을 제외한, 각 IBM SaaS 오퍼링의 프리미엄 지원 등록 시 추가 요금이 부과됩니다.

**표준 지원:**

- 8AM-5PM 로컬 시간대 지원.
- 고객과 고객의 적격 참여자는 지원 티켓을 전자적으로 제출할 수 있습니다(Software as a Service [SaaS] Support Handbook 참조).
- 고객은 고객 지원 포털을 통해 알림사항, 문서, 사례 보고서, FAQ(http://www-01.ibm.com/software/security/trusteer/support/)를 확인할 수 있습니다.
- 지원 옵션과 세부사항은 IBM Software as a Service [SaaS] Support Handbook(http://www-01.ibm.com/software/support/handbook.html)에서 확인할 수 있습니다.

**프리미엄 지원:**

- 모든 심각도 상태에 대한 24x7 지원.
- 고객이 지원 팀에 전화로 직접 연락할 수 있습니다.
- 고객과 고객의 적격 참여자는 지원 티켓을 전자적으로 제출할 수 있습니다(Software as a Service [SaaS] Support Handbook 참조).
- 고객은 고객 지원 포털을 통해 알림사항, 문서, 사례 보고서, FAQ(http://www-01.ibm.com/software/security/trusteer/support/)를 확인할 수 있습니다.
- 지원 옵션과 세부사항은 IBM Software as a Service [SaaS] Support Handbook(http://www-01.ibm.com/software/support/handbook.html)에서 확인할 수 있습니다.

# 7. IBM SaaS 오퍼링 추가 조항

## 7.1 Safe Harbor 준수

IBM 은 U.S. Department of Commerce 가 European Commission 과 함께 개발한 U.S. – EU Safe Harbor Framework 를 준수합니다. IBM Security Trusteer 제품은 IBM 의 EU-U.S. Safe Harbor 인증에 포함되어 있습니다. Safe Harbor 에 대한 자세한 정보와 Safe Harbor 회사 목록은 http://export.gov/safeharbor/에서 확인할 수 있습니다.

## 7.2 고객 연간 등록료 인상

IBM 은 IBM SaaS 의 등록료를 3%를 초과하지 않는 범위에서 IBM 이 정한 백분율로 12 개월마다 최대 한 번 조정할 수 있습니다. 조정한 등록료는 최초 적용 기간 시작일의 기준일에 발효됩니다. 등록료를 조정하더라도 IBM SaaS 에 대한 고객의 권한이나 IBM SaaS 에 적용되는 과금 체계는 변동이 없습니다. IBM 비즈니스 파트너는 IBM 과 독립된 조직이며 가격과 기간을 단독으로 결정합니다.

## 7.3 프리미엄 지원

고객은 고객이 프리미엄 지원 오퍼링에 등록한 IBM SaaS 오퍼링에 대해서만 프리미엄 지원을 제공받을 수 있습니다.

## 7.4 합법적 사용 및 동의

### 데이터 수집 및 처리 권한

본 IBM SaaS 는 고객이 고객의 보안 환경과 데이터를 개선할 수 있도록 지원하기 위해 설계되었습니다. IBM SaaS 는 IBM SaaS 오퍼링에 등록한 Business 또는 Retail 애플리케이션과 상호작동하는 적격 참여자와 클라이언트 디바이스로부터 정보를 수집합니다. 일부 국가(관할권)의 경우 IBM SaaS 는 개인 데이터로 간주될 수 있는 정보를 단독 또는 결합 형태로 수집합니다. 개인 데이터는 고객 대신 저장, 처리 또는 전송하도록 IBM 에 제공된 이름, 이메일 주소, 집주소, 전화번호 등 특정 개인을 식별할 수 있는 정보입니다.

데이터 수집 및 처리 규정은 IBM SaaS 의 기능을 개선하기 위해 업데이트될 수 있습니다. 필요에 따라 데이터 수집 및 처리 규정에 대해 자세하게 기술한 문서를 업데이트하며 고객이 요청하는 경우 이를 제공합니다. 고객은 IBM 이 본 이용 약관의 해외 전송 조항과 개인정보 보호 조항 및 이용 약관 일반 조항의 개인정보 보호 및 보안 조항에 따라 이러한 정보를 수집하고 처리할 수 있도록 권한을 부여합니다.

**IBM Security Trusteer Pinpoint 오퍼링의 경우:**

수집하는 데이터에는 사용자 IP 주소, 암호화 또는 단방향 해쉬된(hashed) 사용자 ID, 필터링되지 않은 경우 도메인 쿠키, 보안된 애플리케이션 및 피싱 사이트의 방문 기록, 지역 정보, 피싱 사이트에 입력한 신임 정보가 포함될 수 있습니다.

**IBM Security Trusteer Mobile SDK 오퍼링 및 IBM Security Trusteer Mobile Browser 오퍼링의 경우:**

수집하는 데이터에는 사용자 IP 주소, 암호화 또는 단방향 해쉬된(hashed) 사용자 ID, 지역정보, 보안된 애플리케이션의 방문 기록, SIM 카드 정보, 디바이스 이름, 고객과의 관계가 포함될 수 있습니다.

**IBM Security Trusteer Rapport 오퍼링의 경우:**

수집하는 데이터에는 사용자 IP 주소, 암호화 또는 단방향 해쉬된(hashed) 사용자 ID, 보안 이벤트, 고객 지원을 목적으로 IBM 에 접촉하기 위해 제공된 사용자 이름 및 이메일 주소, 고객의 소속 기관, 보안된 사이트에 입력한 암호화 비밀번호, 보안된 애플리케이션 및 피싱 사이트의 방문, 암호화된 대금지급 카드 번호, 의심되는 악성 프로그램, 유해 행위 또는 오작동에 대한 조사 목적으로 IBM 지원 인력이 원격으로 수집하는 파일 및 데이터가 포함될 수 있습니다.

**정보 주체로부터의 고지된 동의:**

IBM SaaS 의 사용에는 다양한 법률이나 규정이 적용될 수 있습니다. IBM SaaS 는 합법적인 목적과 방법으로만 사용해야 합니다. 고객은 적용되는 법률, 규정 또는 정책에 의거하여 IBM SaaS 를 사용하고 적용되는 법률, 규정 또는 정책을 준수할 모든 책임이 있다는 것에 동의합니다.

**IBM Security Trusteer Pinpoint 오퍼링 및 IBM Security Trusteer Mobile SDK 오퍼링의 경우:**

고객은 IBM SaaS 의 적법한 사용을 가능케 하고 IBM 이 IBM SaaS 를 통해 정보를 수집하고 처리하는 것을 허용하는 데 필요한 동의, 승인 또는 라이센스를 충분히 고지한 후에 획득하였거나 획득할 것에 동의합니다.

**IBM Security Trusteer Rapport 오퍼링 & IBM Security Trusteer Mobile Browser 오퍼링의 경우:**

고객은 최종 사용자 라이센스 계약(https://www.trusteer.com/support/end-user-license-agreement)에서 명시한 바와 같이 IBM SaaS 의 적법한 사용과 정보 수집 및 처리에 필요한 동의를 충분히 고지한 후에 획득하도록 IBM 에 권한을 부여합니다. 고객이 동의를 획득하기 위한 최종 사용자와의 접촉을 (IBM 이 아니라) 직접 수행하기로 결정한 경우, 고객은 IBM SaaS 를 적법하게 사용하도록 하고 IBM SaaS 를 통해 IBM 이 고객의 정보 처리자로서 정보를 수집하고 처리할 수 있도록 허용하는데 필요한 동의, 승인 또는 라이센스를 충분히 고지한 후에 획득하였거나 획득할 것에 동의합니다.

## 7.5 해외 전송

고객은 IBM 이 유럽 경제 지역(European Economic Area) 외부의 다음 국가와 적절한 보안 수준을 갖춘 것으로 유럽 연합 집행 기관(European Commission)에서 인정한 국가의 정보 처리자와 하위 처리자에게 개인 정보를 포함한 컨텐츠를 관련 법률 및 요건에 준하여 해외 전송하여 처리할 수 있다는 데 동의합니다: 미국.

## 7.6 개인 정보 보호

고객이 유럽 연합 회원국, 아이슬란드, 리히텐슈타인, 노르웨이 또는 스위스에서 개인 정보를 IBM SaaS 에 제공하거나 해당 국가 내에 적격 참여자 또는 클라이언트 디바이스가 있는 경우, 단독 관리자로서 고객은 개인 정보를 처리하는 처리자(EU Directive 95/46/EC 의 용어 정의 참조)로 IBM 을 지명합니다. IBM 은 IBM 이 공개한 IBM SaaS 관련 설명에 따라 IBM SaaS 를 제공하기 위해 필요한 범위 내에서만 그러한 개인 정보를 처리하며, 고객은 그러한 개인 정보의 처리는 고객의 지시대로라는 것에 동의합니다. IBM SaaS 의 일환으로 개인 정보를 보호하는 방법이나 처리하는 지역을 IBM 이 중대하게 변경하는 경우 IBM 은 합리적인 사전 통지를 제공합니다. 고객은 IBM 의 변경 통지일로부터 30 일 이내에 서면 통지서를 IBM 에 제출하여 해당 IBM SaaS 의 현재 등록 기간을 해지할 수 있습니다. 고객은 IBM 이 개인 정보를 포함한 컨텐츠를 다음 처리자 및 하위 처리자로 해외 전송하여 처리할 수 있다는 데 동의합니다.

| 처리자/하위 처리자 이름 | 역할(정보 처리자 또는 하위 처리자) | 장소* |
|---|---|---|
| IBM 계약 법인 | 처리자 | 거래서류에 명시된 바와 같음 |
| Amazon Web Services LLC | 하위 처리자 | 410 Terry Ave. N<br>Seattle, WA 98109<br>United States |
| Connectria Corp. | 하위 처리자 | 10845 Olive Blvd., Suite 300<br>St. Louis, MO 63141<br>United States |

| 처리자/하위 처리자 이름 | 역할(정보 처리자 또는 하위 처리자) | 장소* |
|---|---|---|
| IBM Israel Ltd. | 하위 처리자 | 94 Derech Em-Hamoshavot<br>49527 Petach-Tikva<br>Israel |
| IBM Corp | 하위 처리자 | 1 New Orchard Rd.<br>Armonk, NY 10504<br>United States |

고객은 IBM 이 IBM SaaS 제공에 필요하다고 판단하는 경우에 통지를 제공하여 이러한 국가 지역 목록을 변경할 수 있다는 데 동의합니다.

고객은 독일 데이터 센터를 통해 제공된 서비스의 경우, 프로비저닝 프로세스 과정에서 결정된 바와 같이 IBM 이 개인 정보를 포함한 컨텐츠를 다음 처리자 및 하위 처리자로 해외 전송하여 처리할 수 있다는 데 동의합니다.

| 처리자/하위 처리자 이름 | 역할(정보 처리자 또는 하위 처리자) | 장소* |
|---|---|---|
| IBM 계약 법인 | 처리자 | 거래서류에 명시된 바와 같음 |
| Amazon Web Services(Germany) | 하위 처리자 | Munich, Germany |
| IBM Israel Ltd. | 하위 처리자 | 94 Derech Em-Hamoshavot<br>49527 Petach-Tikva<br>Israel |

고객은 일본 데이터 센터를 통해 제공된 서비스의 경우 프로비저닝 프로세스 과정에서 판단한 바와 같이 IBM 이 개인 정보를 포함한 컨텐츠를 다음 처리자 및 하위 처리자로 해외 전송하여 처리할 수 있다는 데 동의합니다.

| 처리자/하위 처리자 이름 | 역할(정보 처리자 또는 하위 처리자) | 장소* |
|---|---|---|
| IBM 계약 법인 | 처리자 | 거래서류에 명시된 바와 같음 |
| Amazon Web Services(Japan) | 하위 처리자 | Tokyo, Japan |
| IBM Israel Ltd. | 하위 처리자 | 94 Derech Em-Hamoshavot<br>49527 Petach-Tikva<br>Israel |

* 위 표에 명시된 장소에는 처리자/하위 처리자의 회사 주소가 포함됩니다. 데이터 센터는 기재된 지역과 동일 국가에 소재합니다.

양 당사자 또는 관련 계열사는 선택 조항을 삭제하여 EC Decision 2010/87/EU 에 의거하여 그들의 상응하는 역할 안에서 수정되지 않은 별도의 표준 EU 모델 조항(Model Clause) 계약을 체결할 수 있습니다. 이러한 계약으로 인해 발생한 모든 분쟁이나 책임은 해당 계약이 계열사 간에 체결된 경우라도 본 계약의 조항에 의거해서 양 당사자 간에 발생한 분쟁이나 책임과 마찬가지로 양 당사자에 의해 처리됩니다.

# 부록 A

## 1. IBM SaaS 오퍼링

IBM 은 이러한 서비스를 독립형 서비스와 오퍼링, 또는 추가 서비스와 오퍼링으로 제공합니다. 주문한 특정 IBM SaaS 오퍼링을 고객의 라이센스 증서에 명시합니다.

### 1.1 Business 및 Retail 정의

IBM Security Trusteer 사기 방지 제품은 특정 유형의 애플리케이션에서 사용할 목적으로 라이센스가 부여됩니다. 애플리케이션은 Retail 유형 또는 Business 유형으로 정의됩니다. Retail 애플리케이션과 Business 애플리케이션에 대해 별개의 오퍼링을 사용할 수 있습니다.

- Retail 애플리케이션은 소비자 서비스를 위해 설계된 온라인 뱅킹 애플리케이션, 모바일 애플리케이션 또는 e-commerce 애플리케이션을 의미합니다. 고객의 정책은 특정 소규모 비즈니스를 리테일 액세스에 적합한 것으로 분류할 수 있습니다.
- Business 애플리케이션은 기업, 기관 또는 그와 동등한 법인 서비스를 위해 설계된 온라인 뱅킹 애플리케이션, 모바일 애플리케이션, e-commerce 애플리케이션 또는 Retail 범주에 속하지 않는 모든 애플리케이션을 의미합니다.

### 1.2 IBM SaaS 기본 등록(Subscription) 오퍼링

Business 오퍼링:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Retail 오퍼링:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

각 Business 및 Retail 오퍼링에 대해 추가 요금을 부담하여 사용할 수 있는 연관된 프리미엄 지원 제품이 제공됩니다(단, IBM Security Trusteer Mobile SDK 오퍼링은 제외).

### 1.3 IBM Security Trusteer Rapport 오퍼링의 추가 IBM SaaS 등록(Subcription) 오퍼링

IBM Security Trusteer Rapport for Business 에 사용 가능한 추가 오퍼링:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

IBM Security Trusteer Rapport for Retail 에 사용 가능한 추가 오퍼링:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

IBM Security Trusteer Rapport 오퍼링의 각 Business 및 Retail 추가 기능의 경우(IBM Security Trusteer Rapport Mandatory Service 추가 기능은 제외), 추가 요금을 부담하여 사용 가능한 연관된 프리미엄 지원 제품이 제공됩니다.

IBM Security Trusteer Rapport for Business 또는 IBM Security Trusteer Rapport for Retail 등록(Subscription)은 본 조항에 나열된 연관된 추가 IBM SaaS 등록 오퍼링의 선행 조건입니다.

### 1.4 IBM Security Trusteer Pinpoint Malware Detection 오퍼링의 추가 IBM SaaS 등록(Subscription) 오퍼링

IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 또는 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 에 사용 가능한 추가 오퍼링:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 에 사용 가능한 추가 오퍼링:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

본 조항에 나열된 각 추가 IBM SaaS 오퍼링에 대해 추가 요금을 부담하여 프리미엄 지원 등록(Subscription)을 사용할 수 있습니다.

IBM Security Trusteer Pinpoint Malware Detection for Business 오퍼링 또는 IBM Security Trusteer Pinpoint Malware Detection for Retail 오퍼링 등록(Subscription)은 본 조항에 나열된 연관된 추가 IBM SaaS 등록 오퍼링의 선행 조건입니다.

### 1.5 기타 추가 IBM SaaS 등록(Subscription)

현재 사용이 가능하거나 개발 중에 있는, 본 이용 약관에 명시되지 않은 상기 기본 등록에 대한 추가 IBM SaaS 등록(Subscription)은 업데이트로 간주되지 않으며 별도로 라이센스를 부여받아야 합니다.

### 1.6 용어 정의

**계정 소유자(Account Holder)** – 클라이언트 인에이블링 소프트웨어를 설치하였고 최종 사용자 라이센스 계약("EULA")을 수락하였으며 고객이 IBM SaaS 오퍼링에 등록한 고객의 Retail 또는 Business 애플리케이션에서 최소 한 번 인증된 고객의 최종 사용자를 의미합니다.

**계정 소유자 클라이언트 소프트웨어(Account Holder Client Software)** – IBM Security Trusteer Rapport 클라이언트 인에이블링 소프트웨어, IBM Security Trusteer Mobile Browser 클라이언트 인에이블링 소프트웨어 또는 최종 사용자의 디바이스에 설치하도록 일부 IBM SaaS 등록에서 제공되는 기타 클라이언트 인에이블링 소프트웨어를 의미합니다.

**Trusteer Splash** – 사용 가능한 스플래시 템플리트에 따라 고객에게 제공된 스플래시를 의미합니다.

**랜딩 페이지(Landing Page)** – 고객 스플래시 및 다운로드 가능한 계정 소유자 클라이언트 소프트웨어와 함께 고객에게 제공되는 IBM 이 호스팅하는 페이지를 의미합니다.

## 2. IBM Security Trusteer Rapport 오퍼링

### 2.1 IBM Security Trusteer Rapport for Retail 및/또는 IBM Security Trusteer Rapport for Business(이하 "Trusteer Rapport")

Trusteer Rapport 는 피싱 및 MitB(Man-in-the-Browser) 악성 소프트웨어 공격을 방지하는 보호 계층(layer)을 제공합니다. IBM Security Trusteer Rapport 는 전세계 수천만의 엔드포인트 네트워크를 사용하여 전세계 조직에 대한 활성 피싱 및 악성 소프트웨어 공격에 대한 정보를 수집합니다. IBM

Security Trusteer Rapport 는 피싱 공격을 차단하고 MitB 악성 소프트웨어류의 설치 및 운영을 방지하기 위한 행위기반 알고리즘을 적용합니다.

본 IBM SaaS 오퍼링에는 적격 참여자 과금 체계가 적용됩니다. Business 오퍼링은 적격 참여자 10 명 단위의 팩으로 판매됩니다. Retail 오퍼링은 적격 참여자 100 명 단위의 팩으로 판매됩니다.

IBM SaaS 오퍼링은 다음을 포함합니다.

a. Trusteer Management Application(이하 "TMA"):

   TMA 는 고객(및 고객의 제한없는 수의 허가된 직원)이 다음을 수행할 수 있는 IBM Security Trusteer 클라우드 호스트 환경에서 제공됩니다. (i) 이벤트 데이터 보고 및 위험 평가 수신 (ii) 이벤트 데이터 보고 관련 정책의 확인, 구성 및 설정 (iii) EULA 에 따라 일반 사용자에게 라이센스를 부여하여 적격 참여자의 데스크탑 또는 디바이스(PC/MAC)에 다운로드하도록 제공한 클라이언트 인에이블링 소프트웨어(Trusteer Rapport 소프트웨어 스위트라고도 함)(이하 "계정 소유자 클라이언트 소프트웨어")의 무료 보기. 고객은 Trusteer Splash 또는 Rapport API 를 통해서만 계정 소유자 클라이언트 소프트웨어를 판매할 수 있으며 고객의 내부 비즈니스 운영 또는 고객 직원에 의한 사용(고객 직원의 개인적인 사용은 제외)을 위한 용도로는 계정 소유자 클라이언트 소프트웨어를 사용할 수 없습니다.

b. Web Script:

   IBM SaaS 오퍼링 액세스 또는 사용 목적의 웹 사이트 액세스 용도.

c. 이벤트 데이터:

   고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 IBM SaaS 에 등록한 Business 또는 Retail 애플리케이션과 계정 소유자 간의 온라인 상호작동의 결과로 계정 소유자 클라이언트 소프트웨어에서 생성된 이벤트 데이터를 수신할 수 있습니다. 이벤트 데이터는 EULA 를 승인하였고 고객의 Business 또는 Retail 애플리케이션에서 최소 한 번 인증된 적격 참여자의 (관련 디바이스에서 현재 실행 중인) 계정 소유자 클라이언트 소프트웨어에서 수신되며, 고객의 구성에는 사용자 ID 수집내용이 포함되어야 합니다.

d. Trusteer Splash:

   Trusteer Splash 마케팅 플랫폼은 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 및/또는 Retail 애플리케이션에 액세스하는 적격 참여자에게 계정 소유자 클라이언트 소프트웨어를 식별하고 판매합니다. 고객은 사용 가능한 스플래시 템플리트 중에서 선택할 수 있습니다. 사용자 정의된 스플래시에 대해서는 별도의 계약서 또는 작업명세서를 작성하여 계약을 체결할 수 있습니다.

고객은 TMA 와 관련해서, 그리고 Trusteer Splash 에만 사용하고, 계정 소유자 클라이언트 소프트웨어 또는 IBM 이 호스팅하는 랜딩 페이지와 IBM Security Trusteer 웹 사이트에 사용할 목적으로 고객의 상표, 로고 또는 아이콘을 제공하는 데 동의합니다. 제공된 고객의 상표, 로고 또는 아이콘은 광고 및 상표 사용에 관한 IBM 의 합리적인 정책에 따라 사용됩니다.

고객은 계정 소유자 클라이언트 소프트웨어의 필수 배치 유형을 이용하고자 하는 경우 IBM Security Trusteer Rapport Mandatory Service SaaS 오퍼링에 등록해야 합니다.

계정 소유자 클라이언트 소프트웨어의 필수 배치에는 다음을 포함합니다(단, 이에 한하지 않음) – 직접 또는 간접적으로 계정 소유자 클라이언트 소프트웨어를 적격 참여자(Eligible Participant)가 다운로드하도록 강제하는 메커니즘이나 방법, 또는 계정 소유자 클라이언트 소프트웨어의 필수 배치를 위한 라이센싱 요구사항을 IBM 이 생성하거나 승인하지 않은 바이패스하도록 생성된 방법, 도구, 절차, 계약 또는 메커니즘.

## 2.2 IBM Security Trusteer Rapport for Business 및/또는 IBM Security Trusteer Rapport for Retail 의 선택적 추가 IBM 오퍼링

IBM Security Trusteer Rapport 오퍼링에 대한 등록은 다음 추가 IBM SaaS 오퍼링 중 하나의 등록에 대한 선행 조건입니다. IBM SaaS 가 "for Business"로 지정된 경우, 취득된 추가 IBM SaaS 오퍼링도 "for Business"로 지정되어야 합니다. IBM SaaS 가 "for Retail"로 지정된 경우에는 취득된 추가 IBM SaaS 오퍼링도 "for Retail"로 지정되어야 합니다. 고객은 EULA 를 승인하였고 고객의 Business 및/또는 Retail

애플리케이션에서 최소 한 번 인증된 계정 소유자 클라이언트 소프트웨어를 실행 중인 적격 참여자로부터 이벤트 데이터를 수신하며, 고객의 구성에는 사용자 ID 수집내용이 포함되어야 합니다.

### 2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business 및/또는 IBM Security Trusteer Rapport Fraud Feeds for Retail

고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 특정 계정 소유자 데스크탑의 악성 소프트웨어 감염 및 기타 엔드포인트 취약점에 대한 이벤트 데이터를 수신할 수 있습니다.

### 2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business 및/또는 IBM Security Trusteer Rapport Phishing Protection for Retail

고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 의심되는 피싱이나 잠재적 사기 사이트에 대한 계정 소유자의 로그인 신임 정보의 제출과 관련한 이벤트 데이터 알림을 수신할 수 있습니다. 합법적인 온라인 애플리케이션(URL)은 피싱 사이트로 잘못 플래그(flag)될 수 있으며 IBM SaaS 는 계정 소유자에게 합법적인 사이트를 피싱 사이트로 경보를 제공할 수도 있습니다. 이 경우 고객은 IBM 에 이러한 오류를 통지해야 하고 IBM 은 오류를 정정해야 합니다. 해당 정정 조치는 이러한 오류에 대한 고객의 유일한 구제책입니다.

### 2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business 및/또는 IBM Security Trusteer Rapport Mandatory Service for Retail

고객은 Trusteer Splash 마케팅 플랫폼의 인스턴스를 사용하여 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 및/또는 Retail 애플리케이션에 액세스하는 적격 참여자의 계정 소유자 클라이언트 소프트웨어 다운로드를 관리할 수 있습니다.

IBM Security Trusteer Rapport Premium Support for Business 는 IBM Security Rapport Mandatory Service for Business 의 선행 조건입니다.

IBM Security Trusteer Rapport Premium Support for Retail 은 IBM Security Rapport Mandatory Service for Retail 의 선행 조건입니다.

고객은 고객이 IBM SaaS 에 등록한 Retail 또는 Business 애플리케이션에서 함께 사용할 목적으로 IBM Security Trusteer Rapport Mandatory Service 추가 기능을 주문하여 구성한 경우에만 해당 추가 기능을 구현할 수 있습니다.

## 3. IBM Security Trusteer Pinpoint 오퍼링

IBM Security Trusteer Pinpoint 는 또다른 보안 계층(layer)을 제공하도록 설계된 클라우드 기반 서비스로, 악성 소프트웨어, 피싱 및 계정 탈취 공격을 감지 및 보완하고자 하는 오퍼링입니다. Trusteer Pinpoint 는 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 및/또는 Retail 애플리케이션과 사기 방지 프로세스에 통합될 수 있습니다.

IBM SaaS 오퍼링은 다음을 포함합니다.

a. TMA:

   TMA 는 고객(및 고객의 제한없는 수의 허가된 직원)이 다음을 수행할 수 있는 IBM Security Trusteer 클라우드 호스트 환경에서 제공됩니다. (i) 이벤트 데이터 보고 및 위험 평가 수신 및 (ii) 보안 정책과 이벤트 데이터 보고 관련 정책의 확인, 구성 및 설정

b. Web Script 및/또는 API:

   IBM SaaS 액세스 또는 사용 목적의 웹 사이트 배치 용도.

### 3.1 IBM Security Trusteer Pinpoint Malware Detection 및 IBM Security Trusteer Pinpoint Criminal Detection

IBM Security Trusteer Pinpoint Malware Detection 오퍼링에서 악성 소프트웨어를 감지하거나 IBM Security Trusteer Pinpoint Criminal Detection 오퍼링에서 계정 탈취를 감지한 경우 고객은 Pinpoint Best Practies Guide 에 따라야 합니다. 악성 소프트웨어 또는 계정 탈취를 감지한 직후 적격 참여자의 사용 경험에 영향을 주어 다른 사용자가 IBM Security Trusteer Pinpoint 오퍼링을 사용하여 고객의 조치를 링크할 수 있는 방식(예: 악성 소프트웨어 또는 계정 탈취를 감지한 직후 알림, 메시지, 디바이스 차단 또는 Business 및/또는 Retail 애플리케이션 액세스 차단)으로는 IBM Security Trusteer Pinpoint

Malware Detection 오퍼링 또는 IBM Security Trusteer Pinpoint Criminal Detection 오퍼링을 사용하지 마십시오.

### 3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business 및/또는 IBM Security Trusteer Pinpoint Criminal Detection for Retail

디바이스 ID 를 사용하여 Business 또는 Retail 애플리케이션에 연결하는 브라우저에서 의심되는 계정 탈취 활동의 클라이언트리스(clientless) 감지, 피싱 감지 및 악성 소프트웨어 구동 신임 도용 감지. IBM Security Trusteer Pinpoint Criminal Detection 오퍼링은 또다른 보호 계층(layer)을 제공하며 계정 탈취 시도를 감지하고 (기본 브라우저나 고객 모바일 애플리케이션을 통해) Business 또는 Retail 애플리케이션에 액세스하는 브라우저 또는 모바일 디바이스의 위험 평가 점수를 고객에게 직접 전달합니다.

a. 이벤트 데이터:

   고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 및/또는 Retail 애플리케이션과 함께 적격 참여자의 온라인 상호작동의 결과로 생성된 이벤트 데이터를 수신하거나 백엔드 API 전달 모드를 통해 이벤트 데이터를 수신할 수 있습니다.

### 3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile 및/또는 IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) 오퍼링은 또 다른 보호막을 제공하기 위해 설계되었으며 불법적인 계정 액세스를 식별하고 고객에게 권장사항을 제공하여 계정 탈취와 부정한 행위로부터 보호하고자 하는 오퍼링입니다. 해당 IBM SaaS 오퍼링은 PPCD 모바일 API 를 사용하는 고객의 Business 및/또는 Retail 애플리케이션과 적격 참여자의 모바일 디바이스 양쪽에서 수신되는 정보를 수집합니다. IBM Security Trusteer PPCD Mobile 오퍼링은 적격 참여자의 모바일 디바이스와 관련된 복잡한 정보를 본 이용 약관에 명시된 IBM Security Trusteer 의 다른 IBM SaaS 오퍼링을 통해 통합된 기타 데이터 소스(실시간 악성 소프트웨어 감염 및 피싱 사고 등)와 상호 연관시키도록 설계되었습니다.

고객은 IBM Security Trusteer 의 클라우드 호스팅 환경에서 IBM Security Trusteer PPCD Mobile 오퍼링을 액세스하여 사용하고 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 또는 Retail 애플리케이션과 적격 참여자의 모바일 디바이스 간의 온라인 상호작동의 결과로 생성된 위험 평가 데이터를 해당 적격 참여자의 모바일 디바이스로부터 수신할 수 있습니다. 본 오퍼링의 목적상, "모바일 디바이스"에는 지원되는 휴대전화와 태블릿만 포함되며 PC 또는 MAC 은 포함되지 않습니다.

### 3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 및/또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 및/또는 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 및/또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Business 및/또는 Retail 애플리케이션에 연결하는 MitB(Man in the Browser) 파이낸셜 악성 소프트웨어 감염 브라우저에서 클라이언트리스 감지. IBM Security Trusteer Pinpoint Malware Detection 오퍼링은 또다른 보호 계층(layer)을 제공하며 MitB 파이낸셜 악성 소프트웨어 존재여부의 검사 및 경보 기능을 고객에게 제공하여 조직이 악성 소프트웨어 위험성에 따른 사기 방지 프로세스에 중점을 둘 수 있도록 합니다.

a. 이벤트 데이터:

   고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 고객의 Business 및/또는 Retail 애플리케이션과 함께 적격 참여자의 온라인 상호작동의 결과로 생성된 이벤트 데이터를 수신할 수 있습니다.

b. Advanced Edition:

   Business 및/또는 Retail 의 Advanced Edition 은 고객의 Business 및/또는 Retail 애플리케이션의 구조와 플로우에 맞게 조정되고 사용자 정의되며 고객에 대한 특정 위협 동향에 따라 사용자 정의될 수 있는, 추가적인 감지 및 보호 계층(layer)을 제공합니다. 이는 고객의 Business 및/또는 Retail 애플리케이션의 다양한 위치에서 통합될 수 있습니다.

Advanced Edition 은 최소 Retail 적격 참여자 10 만명 또는 Business 적격 참여자 1 만명(즉, Retail 적격 참여자 1000 명 단위 1000 팩 또는 Business 적격 참여자 10 명 단위 1000 팩)에 해당하는 최소 수량 한도로 고객에게 제공됩니다.

c. Standard Edition:

Business 또는 Retail 의 Standard Edition 은 본 이용 약관에 명시된 IBM SaaS 오퍼링의 핵심 기능을 제공하는 빠른 배치 솔루션입니다.

## 3.2 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 및/또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 및/또는 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 및/또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 의 선택적 추가 IBM SaaS 오퍼링

IBM Security Trusteer Rapport Remediation for Retail 오퍼링의 경우, IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 의 선행 조건이 있습니다.

IBM Security Trusteer Pinpoint Carbon Copy for Retail 의 경우, IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 또는 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 의 선행 조건이 있습니다. IBM Security Trusteer Pinpoint Carbon Copy for Business 의 경우, IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 또는 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 의 선행 조건이 있습니다.

### 3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business 및/또는 IBM Security Trusteer Pinpoint Carbon Copy for Retail

IBM Security Trusteer Pinpoint Carbon Copy 오퍼링은 고객이 IBM SaaS 오퍼링에 등록한 고객의 Retail 또는 Business 애플리케이션에 대한 피싱 공격으로 적격 참여자의 신임 정보가 훼손된 경우를 식별할 수 있는 모니터링 서비스와 또다른 보호 계층(layer)을 제공하도록 설계되었습니다.

### 3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail 은 IBM Security Trusteer Pinpoint Malware Detection 이벤트 데이터를 통해 MitB(man-in-the-browser) 악성 소프트웨어 감염을 감지한 경우 고객의 Retail 애플리케이션에 임시로 액세스하는 고객의 적격 참여자의 감염된 디바이스(PC/MAC)에서 MitB 악성 소프트웨어 감염을 조사하고 치료하며 차단하고 제거합니다. 고객은 고객 Retail 애플리케이션에서 실제로 실행 중인 IBM Security Trusteer Pinpoint Malware Detection 의 당시 유효한 등록을 보유하고 있어야 합니다. 고객은 고객의 Retail 애플리케이션에 액세스하는 적격 참여자와 관련해서 감염된 특정 디바이스(PC/MAC)를 임시로 조사하고 개선하기 위한 도구로만 해당 IBM SaaS 오퍼링을 사용할 수 있습니다. IBM Security Trusteer Rapport Remediation for Retail 은 관련 적격 참여자의 디바이스(PC/MAC)에서 실제로 실행되어야 하며 해당 적격 참여자는 EULA 를 승인해야 하고 고객의 Retail 애플리케이션에서 최소 한 번 인증되어야 하며 고객의 구성에는 사용자 ID 수집내용이 포함되어야 합니다. 즉, 본 IBM SaaS 오퍼링에는 Trusteer Splash 를 사용할 수 있는 권리는 포함되지 않으며  고객의 일반 적격 참여자 그룹에 기타 다른 방법으로 계정 소유자 클라이언트 소프트웨어를 판촉합니다.

# 4. IBM Security Trusteer Mobile 오퍼링

## 4.1 IBM Security Trusteer Mobile Browser for Business 및/또는 IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser 는 또다른 보호 계층(layer)을 추가하도록 설계되었으며 고객이 IBM SaaS 오퍼링에 등록한 고객의 Retail 또는 Business 애플리케이션에 액세스하는 적격 참여자의 모바일 디바이스에 대한 안전한 온라인 액세스, 모바일 디바이스의 위험 평가 및 피싱 방지를 제공하고자 하는 오퍼링입니다. 보안 Wi-Fi 감지는 Android 플랫폼에서만 가능합니다. 본 IBM SaaS 오퍼링의 목적상, 모바일 디바이스, 휴대전화 또는 태블릿은 포함되고 랩탑 PC 및 Mac 은 포함되지 않습니다.

TMA 를 통해 고객(및 제한없는 수의 허가된 직원)은, 적격 참여자가 (i) 최종 사용자 라이센스 계약("EULA")에 의거해서 일반 사용자에게 무료로 라이센스가 부여되어 적격 사용자의 모바일 디바이스에 다운로드하도록 제공된 애플리케이션인 계정 소유자 클라이언트 소프트웨어를 다운로드하였고 (ii) EULA 를 승인했으며 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 또는 Retail 애플리케이션에서 최소 한 번 인증된, 해당 적격 참여자의 디바이스와 관련된 이벤트 데이터, 분석 및 통계 정보를 수신할 수 있습니다. 고객은 Trusteer Splash 를 통해서만 계정 소유자 클라이언트 소프트웨어를 판매할 수 있으며 고객의 내부 비즈니스 운영 용도로는 계정 소유자 클라이언트 소프트웨어를 사용할 수 없습니다.

a. 이벤트 데이터:

   고객(및 제한없는 수의 허가된 직원)은 TMA 를 사용하여 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 또는 Retail 애플리케이션과 함께 모바일 디바이스 온라인 상호작동의 결과로 생성된 이벤트 데이터를 수신할 수 있습니다.

b. Trusteer Splash:

   Trusteer Splash 마케팅 플랫폼은 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 및/또는 Retail 애플리케이션에 액세스하는 적격 참여자에게 계정 소유자 클라이언트 소프트웨어를 식별하고 판매합니다. 고객은 사용 가능한 스플래시 템플리트(이하 "스플래시 템플리트") 중에서 선택할 수 있습니다. 사용자 정의된 스플래시에 대해서는 별도의 계약서 또는 작업명세서를 작성하여 계약을 체결할 수 있습니다.

고객은 TMA 와 관련해서, Trusteer Splash 에만 사용하고, 계정 소유자 클라이언트 소프트웨어, IBM 호스팅 랜딩 페이지 또는 IBM Security Trusteer 웹 사이트에 사용할 목적으로 고객의 상표, 로고 또는 아이콘을 제공하는 데 동의합니다. 제공된 고객의 상표, 로고 또는 아이콘은 광고 및 상표 사용에 관한 IBM 의 합리적인 정책에 따라 사용됩니다.

## 4.2 IBM Security Trusteer Mobile SDK for Business 및/또는 IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK 오퍼링은 고객이 IBM SaaS 오퍼링에 등록한 고객의 Business 및/또는 Retail 애플리케이션에 대한 안전한 웹 액세스, 디바이스의 위험 평가 및 피싱 방지를 제공하는 또다른 보호 계층(layer)을 추가하도록 설계되었습니다. 보안 Wi-Fi 감지는 Android 플랫폼에서만 가능합니다.

IBM Security Trusteer Mobile SDK 오퍼링에는 고객이 IBM SaaS 오퍼링에 등록한 고객의 보호된 독립형 iOS 또는 Android 모바일 애플리케이션에 내장되어 통합이 가능한 IBM Security Trusteer Mobile SDK 에서 생성한 고유 코드인 "재배포 가능 항목" 또는 "런타임 구성요소"와 함께, 문서, 프로그래밍 고유 소프트웨어 라이브러리 및 기타 관련 파일 및 항목이 포함된 소프트웨어 패키지(IBM Security Trusteer 모바일 라이브러리라고 함)인 고유 모바일 소프트웨어 개발자 킷(이하 "SDK")이 포함되어 있습니다(이하 "고객 통합 모바일 앱").

IBM Security Trusteer Mobile SDK for Retail 은 적격 참여자 100 명 단위의 팩이나 클라이언트 디바이스 100 대 단위의 팩으로 사용이 가능하며 IBM Security Trusteer Mobile SDK for Business 는 적격 참여자 10 명 단위의 팩 또는 클라이언트 디바이스 10 대 단위의 팩으로 사용 가능합니다.

고객(과 무제한의 고객의 허가된 직원)은 TMA 를 통해 이벤트 데이터 보고 및 위험 경향 평가를 수신할 수 있습니다. 고객은 고객 통합 모바일 앱을 통해 고객 통합 모바일 앱을 다운로드한 적격 참여자의 모바일 디바이스와 관련된 모바일 디바이스 정보와 위험 분석을 수신할 수 있으며 이를 통해 고객은 이러한 위험에 대한 완화 조치를 수행하는 사기 방지 정책을 구성할 수 있습니다. 본 오퍼링의 목적상, "모바일 디바이스"에는 지원되는 휴대전화와 태블릿만 포함되며 PC 또는 MAC 은 포함되지 않습니다.

고객은 다음을 수행할 수 있습니다.

a. 고객 통합 모바일 앱을 개발하기 위한 목적으로만 IBM Security Trusteer Mobile SDK 를 내부적으로 사용할 수 있습니다.

b. 고객 통합 모바일 앱에서 분리할 수 없는 방식으로 (오브젝트 코드 형식으로만) 재배포 가능 항목을 내장합니다. 재배포 가능 항목 중 본 라이센스에 따라 수정하거나 병합한 부분에는 본 이용 약관의 조항이 적용됩니다.

c. 다음을 전제 조건으로, 적격 참여자의 모바일 디바이스 또는 클라이언트 디바이스 홀더에 다운로드하도록 재배포 가능 항목을 마케팅하고 배포합니다.

- 본 계약에서 구체적으로 허용하는 경우를 제외하고, 고객은 (1) SDK 를 사용, 복사, 수정 또는 배포할 수 없으며 (2) 법률에서 계약상 면제하지 못하게 하고 구체적으로 허용하는 경우를 제외하고, SDK 를 리버스 어셈블, 리버스 컴파일, 달리 변환 또는 리버스 엔지니어링할 수 없고 (3) SDK 를 재라이센스 부여, 임대 또는 리스할 수 없고 (4) 재배포 가능 항목에 포함된 저작권 또는 통지 파일을 제거할 수 없고 (5) 원본 재배포 가능 파일/모듈과 동일한 경로 이름을 사용할 수 없으며 (6) IBM, IBM 라이센스 제공자 또는 판매자의 사전 서면 동의 없이 고객 통합 모바일 앱의 마케팅과 관련하여 IBM, IBM 의 라이센스 제공자 또는 판매자의 이름과 상표를 사용할 수 없습니다.
- 재배포 가능 항목은 고객 통합 모바일 앱(Client Integrated Mobile App)에서 분리할 수 없는 통합된 상태를 유지해야 합니다. 재배포 가능 항목은 오브젝트 코드 양식이어야 하고 SDK 및 관련 문서의 모든 지시사항과 명세를 준수해야 합니다. 고객 통합 모바일 앱에 관한 최종 사용자 라이센스 계약에서는 재배포 가능 항목을 i) 고객 통합 모바일 앱을 사용하기 위한 목적 외의 용도로 사용할 수 없으며 ii) 복사할 수 없으며(백업 용도는 제외) iii) 추가로 배포하거나 이전할 수 없으며 iv) 법률에서 계약상 면제하지 못하게 하고 구체적으로 허용하는 경우를 제외하고 리버스 어셈블, 리버스 컴파일 또는 달리 변환할 수 없다는 것을 최종 사용자에게 통지해야 합니다. 고객의 라이센스 계약은 최소한 본 계약 조항의 수준으로 IBM 을 보호해야 합니다.
- 고객의 지정 모바일 테스트 디바이스에 대한 유닛 테스트 및 내부 개발의 일환으로만 SDK 를 사용할 수 있습니다. 고객은 프로덕션 워크로드를 처리하거나 프로덕션 워크로드를 시뮬레이션하거나 코드, 애플리케이션 또는 시스템의 확장성을 테스트하는 용도로는 SDK 를 사용할 수 없습니다. 고객은 SDK 의 어떠한 부분도 기타 다른 용도를 위해서 사용할 수 없습니다.

고객은 고객 통합 모바일 앱 및 본 계약에서 허용한 대로 고객이 작성한 재배포 가능 항목의 수정사항에 대한 모든 기술 지원을 제공해야 할 책임이 있습니다.

고객은 IBM SaaS 오퍼링의 사용을 지원하기 위한 용도로만 재배포 가능 항목과 IBM Security Mobile SDK 를 설치하고 사용할 수 있습니다.

IBM 은 IBM Security Trusteer Mobile SDK 에서 제공한 모바일 도구(이하 "모바일 도구")로 작성된 샘플 애플리케이션이 Apple(iOS), Google(Android) 및 기타 모바일 운영 체제 플랫폼(이하 통칭하여 "모바일 OS 플랫폼")의 특정 버전에서 제대로 실행되는지 판별하기 위한 테스트를 수행하였습니다. 그러나 모바일 OS 플랫폼은 제 3 자가 제공하기 때문에 IBM 의 통제 대상이 아니며, IBM 에 대한 별도의 통지 없이 변경될 수 있습니다. 그러므로 상반되는 조항에도 불구하고, IBM 은 모바일 도구로 작성된 모든 애플리케이션이나 기타 결과물이 모든 모바일 OS 플랫폼이나 모바일 디바이스에서 제대로 실행되거나 상호 운영되거나 호환 가능하다고는 보증하지 않습니다.

고객은 고객의 IBM Security Trusteer Mobile SDK 사용이 본 이용 약관의 조항을 준수하는지 확인하기에 충분한 정도의 정확한 서면 기록, 시스템 도구 결과물 및 기타 시스템 정보를 작성하여 보관하고 IBM 및 관련 감사자에게 제공할 것에 동의합니다.

## 5. IBM SaaS Fraud Protection 오퍼링 배치

고객의 기본 등록에는 최초 일회성 설정, 구성, 스플래시 템플리트, 테스트 및 교육을 포함한 필수 설치와 초기 배치 활동이 포함됩니다.

추가 서비스에 대해서는 추가 요금을 부과하여 별도의 계약서를 작성하여 계약을 체결할 수 있습니다.

# 부록 B

IBM 은 IBM SaaS 에 관한 다음 가용성 서비스 레벨 계약(이하 "SLA")을 제공하며 이는 고객의 거래서류에 지정된 경우에 적용됩니다.

고객의 등록 기간 시작 당시 또는 등록 기간 갱신 당시의 유효한 SLA 버전이 적용됩니다. 고객은 SLA 가 고객에게 보증을 제공하는 것이 아님을 이해합니다.

## 1. 용어 정의

a. **허가된 담당자** – 본 SLA 에 따라 클레임을 제출할 수 있는 권한이 부여되어 있다고 고객이 IBM 에게 명시한 개인을 의미합니다.

b. **가용성 크레디트** – 유효한 클레임에 대해 IBM 이 제공하는 배상을 의미합니다. 가용성 크레디트는 IBM SaaS 등록료를 청구하는 추후 청구서에 대한 크레디트 또는 할인의 형식으로 적용됩니다.

c. **클레임** – 계약 월 동안 서비스 레벨에 부합하지 못하였다고 고객의 허가된 담당자가 본 SLA 에 따라 IBM 에 제출하는 배상 청구를 의미합니다.

d. **계약 월** – IBM SaaS 기간 동안의 각 월로, 해당 월 1 일 오전 12:00(GMT)부터 말일 오후 11:59(GMT)까지를 의미합니다.

e. **고객** – IBM 과의 IBM SaaS 계약에 따른 지불 의무를 포함하여 어떠한 중대한 의무도 불이행의 상태가 아닌 IBM 으로부터 직접 IBM SaaS 를 등록한 법인을 의미합니다.

f. **중지 시간** – 서비스에 대한 프로덕션 시스템 처리가 중지되고 해당 권한을 가진 모든 사용자가 서비스의 모든 부분을 전혀 이용할 수 없는 기간 시간을 의미합니다. 중지 시간에는 다음의 결과로 서비스를 사용할 수 없는 기간은 포함되지 않습니다.

- 계획된 시스템 중지 시간
- 불가항력
- 고객 또는 제 3 자 애플리케이션, 설비 또는 데이터와 관련한 문제
- 고객 또는 제 3 자의 조치 또는 부작위(고객의 비밀번호 또는 설비를 사용하여 IBM SaaS 에 액세스하는 개인 포함)
- 필수 시스템 구성 및 IBM SaaS 액세스를 위한 지원 플랫폼을 이용하지 않은 경우
- 고객이나 고객을 대신한 제 3 자가 제공한 설계, 명세 또는 지침을 IBM 이 따른 경우

g. **이벤트** – 특정 상황 또는 여러 상황이 합쳐져서 결과적으로 SLA 에 부합되지 못하게 한 경우, 그러한 특정 상황 또는 여러 상황을 의미합니다.

h. **불가항력** – 자연 재해, 테러, 노동 쟁의, 화재, 홍수, 지진, 폭동, 전쟁, 정부 조치, 명령 또는 제한 조치, 바이러스, 서비스 거부(DOS) 공격 및 기타 악의적 행위, 유틸리티 및 네트워크 연결 장애 또는 IBM 이 합리적으로 통제할 수 있는 영역 밖에 있는 IBM SaaS 비가용성의 기타 원인을 의미합니다.

i. **계획된 시스템 중지 시간** – 유지보수를 목적으로 IBM SaaS 의 계획된 중단을 의미합니다.

j. **서비스 레벨** – 본 SLA 에서 IBM 이 제공하는 서비스의 레벨을 측정하도록 아래와 같이 설정된 표준을 의미합니다.

## 2. 가용성 크레디트

a. 클레임을 제출할 수 있는 자격을 얻으려면 고객은 심각도 1 지원 문제 보고에 대한 IBM 절차에 따라 IBM 고객 지원 헬프 데스크에서 해당 IBM SaaS 에 대한 각 이벤트의 지원 티켓을 로그해야 합니다. 고객은 이벤트에 관한 모든 필요한 세부 정보를 제공하고 심각도 1 지원 티켓에 필요한 범위까지 이벤트에 대한 진단 및 해결을 위해 IBM 을 합리적으로 지원해야 합니다. 고객의 IBM SaaS 사용에 영향을 준 이벤트를 고객이 처음 인식하게 된 24 시간 이내에 해당 티켓을 로그해야 합니다.

b. 고객의 허가된 담당자는 클레임과 관련된 계약 월의 말일로부터 최소 영업일 3 일 이전에 가용성 크레디트에 대한 고객의 클레임을 제출해야 합니다.

c. 고객의 허가된 담당자는 모든 관련 이벤트 및 부합에 실패한 서비스 레벨의 상세 설명을 포함하되 이에 한하지 않는, 클레임과 관련한 모든 합리적인 상세 정보를 IBM 에 제공해야 합니다.

d. IBM 은 아래 표에서 관련 서비스 레벨에 해당하는 각 계약 월 동안의 총 중지 시간을 내부적으로 계산합니다. 가용성 크레디트는 고객이 중지 시간으로 인해 최초로 영향을 받았다고 고객이 보고한 시점부터 측정된 중지 시간의 기간을 기준으로 합니다. 고객이 애플리케이션 중지 시간 이벤트와 인바운드 데이터 처리 중지 시간 이벤트가 동시에 발생된 것으로 보고한 경우에는, IBM 은 중지 시간이 겹치는 기간을 중지 시간의 단일 기간으로 간주하며 두 개의 구별된 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 가용성 크레디트를 적용합니다. IBM 은 동일한 계약 월의 동일한 이벤트에 대해 여러 번의 가용성 크레디트를 제공할 책임이 없습니다.

e. 번들 서비스(단일 통합 가격의 함께 패키지되고 판매되는 개별 IBM SaaS)의 가용성 크레디트는 번들 서비스에 대하여 월별로 통합된 단일 가격을 기준으로 산출되며 각 개별 IBM SaaS 의 월별 등록료를 기준으로 하지 않습니다. 고객은 임의의 계약 월에 번들 중 하나의 개별 IBM SaaS 에 대해서만 클레임을 제출할 수 있으며 IBM 은 임의의 계약 월에 번들 중 둘 이상의 IBM SaaS 에 대해 가용성 크레디트를 제공해야 할 책임이 없습니다.

f. 고객이 IBM SaaS 및 SLA 확약을 이행하는 데 있어 IBM 에게 1 차 책임이 있는 리마케팅 거래의 유효한 IBM 리셀러로부터 IBM SaaS 를 구매한 경우, 가용성 크레디트는 클레임이 발생한 계약 월에 50% 할인이 제공된 IBM SaaS 에 대한 당시의 유효한 관계 SVP(Relationship Suggested Value Price, RSVP)를 기반으로 제공됩니다.

g. 어떠한 경우에도 계약 월에 적용되는 가용성 크레디트의 총 금액은 고객이 IBM 에 IBM SaaS 대가로 지불한 연간 대금의 12 분의 1(1/12)의 10%를 초과하지 않습니다.

h. IBM 은 IBM 의 레코드에서 사용 가능한 정보를 기반으로 클레임의 유효성을 검증하여 합리적인 판단을 하며 고객 레코드의 데이터와 충돌이 있을 경우 IBM 의 레코드가 우선하여 적용됩니다.

i. 본 SLA 에 따라 고객에게 제공되는 가용성 크레디트는 여하한 클레임과 관련하여 고객이 갖는 유일하고 배타적인 배상입니다.

## 3. 서비스 레벨

계약 당월 동안 IBM SaaS 가용성

| **달성한 서비스 레벨<br>(계약 월 동안)** | **가용성 크레디트<br>(클레임 대상이 되는 계약 월의 월 등록(Subscription) 사용료의 %)** |
|---|---|
| < 99.5% | 2% |
| < 98.0% | 5% |
| < 96.0% | 10% |

백분율로 표시된 "달성한 서비스 레벨"은 (a) 계약 월의 총 시간(분)에서 (b) 계약 월의 총 중지 시간(분)을 뺀 후 이를 (c) 계약 월의 총 시간(분)으로 나누어 산출합니다.

예: 계약 월의 총 중지 시간 250 분

| | |
|---|---|
| 계약 월 30 일 동안 총 43,200 분<br>- 중지 시간 250 분 = 42,950 분<br>_____<br>총 43,200 분 | = 계약 월 동안 달성한 서비스 레벨 99.4%에 대한 가용성 크레디트 2% |

## 3.1 제외사항

본 SLA 는 IBM 고객에게만 제공됩니다. 본 SLA 는 다음에 적용되지 않습니다.

- 베타 및 시범 운용 서비스.
- 테스트, 재해 복구, 품질 보증 또는 개발을 포함한(단, 이에 한하지 않음) 비 프로덕션 환경.
- IBM SaaS 에 대한 IBM 고객의 사용자, 게스트, 참여자 및 허가된 초청객이 제기한 클레임.
- 고객이 지불 의무 위반을 포함하여(단, 이에 한하지 않음) 이용 약관에 의거한 중대한 의무를 위반한 경우.