# IBM Resilient Incident Response Platform On Cloud

本「サービス記述書」は IBM がお客様に提供する「クラウド・サービス」について規定するものです。お客様とは、会社、その許可ユーザーおよび「クラウド・サービス」の受領者を意味します。適用される「見積書」および「証書 (PoE)」は、別個の「取引文書」として提供されます。

## 1. クラウド・サービス

IBM Resilient Incident Response Platform on Cloud では通常、動的な行動計画 (マルウェアから DDoS、デバイスの紛失に至るまで) およびインシデントに対応するためのベスト・プラクティスを提供します。この知識ベースがお客様のチームを当該対応に導きます。また、お客様の独自の運用手順に合わせて構成できます。

インシデント対応チームは IBM Resilient Incident Response Platform on Cloud 内で直接、それぞれの対応を管理し、連携することができます。チケット発行システムおよびその他の汎用 IT ツールとは異なり、IBM Resilient Incident Response Platform は完全に構成が可能で、インシデント対応の為に作られています。ほぼ総合的な分析、カスタマイズ可能なダッシュボード、および堅固なレポート作成機能により、管理者は重要な情報へアクセスすることができます。

IBM Resilient Incident Response Platform は、さまざまな規模の複合的な組織向けに設計されており、複数の別個注文可能なバージョンで提供されます。

### 1.1 IBM Resilient Incident Response Platform Enterprise on Cloud

IBM Resilient Incident Response Platform Enterprise on Cloud は、大規模なエンタープライズの大型で多様なシステム用に設計された「クラウド・サービス」ソリューションです。組織やインシデント・タイプに合わせた対応計画、管理、および緩和の土台を提供します。ユーザーは、業界標準およびベスト・プラクティスに基づいてインシデント対応計画を作成し、解決までインシデントを追跡できます。「クラウド・サービス」は、組織にわたって一元的なコラボレーションを促進し、さまざまな利害関係者がインシデント対応の取り組みの一部としてそれぞれの役割やタスクを引き受けることができるようにします。インシデント・シミュレーションも実施して、チームが対応計画をテストし、ギャップを明らかにし、対応プロセスを改善できるようにします。標準装備されている、さまざまな外部の脅威に関するインテリジェンス・フィードとの統合機能により、インシデントと作成物の拡張を自動化できます。「クラウド・サービス」には、インシデント対応計画をさらに調整できるような、グローバル・データ・プライバシー違反通知の規制に関する知識ベースが含まれます。データを、既存のセキュリティー・システムや IT システムと同期させて、ほぼリアルタイムの情報を提供することもできます。カスタム開発を必要とすることなく、さまざまなタスクを「クラウド・サービス」内で自動化、簡素化、または微調整できます。本サービスについて、お客様は、少なくとも 1 つの「インスタンス」使用許諾および 1 つの「許可ユーザー」使用許諾を取得しなければなりません。

### 1.2 IBM Resilient Incident Response Platform Standard on Cloud

IBM Resilient Incident Response Platform Standard on Cloud は、中規模から小規模のエンタープライズのインシデント対応ニーズを満たせるように設計された「クラウド・サービス」ソリューションです。この製品は、IBM Resilient Incident Response Platform Enterprise on Cloud とほとんど同じ機能を提供します。ただし、お客様の使用が認められていない以下のフィーチャーおよび機能は除きます。プライバシー違反規制、オートメーション/オーケストレーション、脅威に関するインテリジェンス・フィード、カスタムの脅威フィード、および LDAP 統合。本サービスについて、お客様は、少なくとも 1 つの「インスタンス」使用許諾および 1 つの「許可ユーザー」使用許諾を取得しなければなりません。

### 1.3 オプション・サービス

#### 1.3.1 IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud

IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud は、お客様が社内の非実稼働活動のためにのみ使用できる IBM Resilient Incident Response Platform の別個のインスタンスです。これには、テスト、性能調整、障害診断、内部ベンチマーク、段階的な品質保証活動、および公

表済みのアプリケーション・プログラミング・インターフェースを使用した、「クラウド・サービス」に対して行われる、内部で使用する追加または拡張の開発が含まれますが、これらに限定されません。

## 1.4 リモート・サービス

以下の「リモート・サービス」は別個注文可能であり、それぞれ、すべての時間 (該当する場合) を使用したか否かに関係なく、購入から 90 日後に満了となります。

### 1.4.1 IBM Resilient Incident Response Platform Integration for Cloud

本オファリングでは、「クラウド・サービス」と関連するセキュリティー・システムおよび管理システムを事前に開発された統合を活用して結び付ける統合サービスを提供します。1 つのシステムに 1 つの統合のみが「エンゲージメント」単位でセットアップされます。本「リモート・サービス」でセットアップ用に利用できる統合は下記のとおりです。

- **QRadar との統合**

  この統合により、QRadar は自動または手動で「クラウド・サービス」に対する違反を新規インシデントとしてプッシュできるようになります。これには、メモ、終了イベント、および新規オフェンス・データの双方向同期が含まれます。

- **HP Arcsight との統合**

  この統合により、ArcSight ユーザーは手動または自動で「クラウド・サービス」に対する Arcsight イベントの詳細を新規インシデントとしてプッシュするか、既存のインシデントに生成物として追加できるようになります。

- **Splunk との統合**

  この統合により、Splunk はインシデントとして「クラウド・サービス」にアラートを自動的にプッシュできるようになります。お客様は、「クラウド・サービス」の Web インターフェースから Splunk 照会を直接実行することもできます。

- **ServiceNow との統合**

  この統合により、ServiceNow ユーザーは「クラウド・サービス」においてインシデントを作成すること、「クラウド・サービス」ユーザーは ServiceNow においてチケットを作成することができるようになります。チケットまたはインシデントの更新もシステム間で複製されます。

- **JIRA との統合**

  この統合により、JIRA ユーザーは JIRA チケットに基づいて「クラウド・サービス」においてインシデントを作成すること、「クラウド・サービス」ユーザーは JIRA においてチケットを作成することができるようになります。チケットまたはインシデントの更新もシステム間で複製されます。

### 1.4.2 IBM Resilient Incident Response Platform Design Session for Cloud

本サービスでは、お客様に代わって行う「クラウド・サービス」インスタンスの最適化を支援するためにコンサルティング・エンゲージメントが提供されます。IBM のコンサルタントがお客様と協力して、最大 3 つのインシデント・タイプに対応したお客様の既存のインシデント対応プロセスを同期化し、その時点の業界のベスト・プラクティスと「クラウド・サービス」の機能に基づいてそれらを改善し、かかるプロセスを実装するために「クラウド・サービス」をどのように構成すべきかについてお客様に助言をします。

## 2. セキュリティーの内容

本「クラウド・サービス」は、IBM の「IBM SaaS」に関する「Data Security and Privacy Principles」(http://www.ibm.com/cloud/data-security で入手可能) および本セクションの追加条件に従うものとします。IBM の「Data Security and Privacy Principles」が変更される場合であっても、それにより「クラウド・サービス」のセキュリティーのレベルが低下することはありません。

本「クラウド・サービス」は、個人情報またはセンシティブ個人情報などの規制対象コンテンツに関する特定のセキュリティー要件に則して設計されているものではありません。お客様は、お客様が「クラウド・サービス」に関連して使用するコンテンツのタイプについて、本「クラウド・サービス」がお客様のニーズを満たすものかどうか判断する責任を負います。

## 3. サービス・レベル・アグリーメント

IBM は、「PoE」に記載するとおり、「クラウド・サービス」に関して、以下の可用性のサービス・レベル・アグリーメント (以下「SLA」といいます。) を提供します。「SLA」は保証ではありません。「SLA」はお客様にのみ提供され、実稼働環境における使用に対してのみ適用されます。

### 3.1 可用性クレジット

お客様は、「クラウド・サービス」の可用性に影響を及ぼした事象について最初に知り得たときから 24 時間以内に、IBM テクニカル・サポート・ヘルプデスクに対して重要度 1 のサポート・チケットを記録しなければなりません。お客様は、あらゆる問題診断および解決に関して IBM を合理的な範囲で支援しなければなりません。

「SLA」の未達を申告するサポート・チケットは、契約月の末日から 3 営業日以内に提出しなければなりません。有効な「SLA」の申告に対する補償は、「クラウド・サービス」の実稼働システム処理が利用できない時間 (以下「ダウンタイム」といいます。) に基づいた「クラウド・サービス」の将来の請求に対するクレジットになります。「ダウンタイム」は、お客様が当該事象を報告した時点から「クラウド・サービス」が復元される時点までの間で計測され、次のものに関連する時間は含まれません。保守のための計画停止または発表された停止、IBM の支配の及ばない原因、お客様または第三者のコンテンツもしくはテクノロジーの問題または設計もしくは指示、サポート対象外のシステム構成およびプラットフォームまたはその他お客様による誤り、またはお客様に起因するセキュリティーに関する事故もしくはお客様によるセキュリティー・テスト。IBM は、下表のとおり、各契約月における「クラウド・サービス」の累積的な可用性に基づき、適用しうる最大の補償を適用します。各契約月の補償の合計額は、「クラウド・サービス」に対する年額料金の 1/12 の 10% を超えないものとします。

### 3.2 サービス・レベル

「契約月」における「クラウド・サービス」の可用性

| **「契約月」における可用性** | **補償<br>(申告の対象である「契約月」における<br>「月額サブスクリプション料金」* の割合)** |
|---|---|
| 99.5% | 2% |
| 98% | 5% |
| 96% | 10% |

*「クラウド・サービス」が IBM ビジネス・パートナーから取得されたものである場合、月額サブスクリプション料金は、申告の対象である「契約月」に対して有効な「クラウド・サービス」のその時点での最新の表示価格に基づいて計算され、それを 50% 割引した額となります。IBM は、直接お客様に払い戻します。

「可用性」は、以下のとおり算出されます。契約月における分単位の総時間数から、契約月における「ダウンタイム」の分単位の総時間数を差し引き、それを契約月における分単位の総時間数で除することにより算出され、結果はパーセントで表します。

例:「契約月」における「ダウンタイム」が合計 500 分である場合

| | |
|---|---|
| 30 日の「契約月」における合計 43,200 分<br>- 予定外の「ダウンタイム」500 分<br>= 42,700 分<br>_____<br>合計 43,200 分 | =「契約月」における 98.8% の可用性につき<br>2% の「可用性クレジット」 |

## 4. テクニカル・サポート

「クラウド・サービス」のテクニカル・サポートは、電子メール、オンライン・フォーラム、およびオンライン問題報告システムを介して提供されます。テクニカル・サポートは「クラウド・サービス」と

共に提供されるものであり、別個のオファリングとして提供されるものではありません。休日を除く、午前 9 時から午後 6 時 (東部標準時) の通常の営業時間中にテクニカル・サポートを利用できます。

| 重要度 | 重要度の定義 | サポート時間内の目標応答時間 |
|---|---|---|
| 1 | **重大な事業影響/サービス・ダウン**<br>事業上の重要な機能が作動不能である、または重要なインターフェースが機能しない状態。これは通常実稼働環境に適用され、サービスにアクセスできないことによって業務に重大な影響が生じることを示します。この状況は、即時に解決する必要があります。 | 1 時間以内 |
| 2 | **著しい事業影響**<br>利用中にサービスのフィーチャーまたは機能が著しく制限されているか、お客様が事業の最終期限に間に合わない危険にさらされている状態。 | 2 営業時間以内 |
| 3 | **軽度の事業影響**<br>サービスまたは機能を使用することができ、業務に重大な影響が表れていないことを示す。 | 4 営業時間以内 |
| 4 | **最小の事業影響**<br>問い合わせまたは非技術的な依頼。 | 1 営業日以内 |

## 5. エンタイトルメントおよび課金情報

### 5.1 課金単位

「クラウド・サービス」は、「取引文書」に記載された課金単位に基づいて提供されます。

a. **「インスタンス」**は、「クラウド・サービス」を取得する際の課金単位です。「インスタンス」とは、「クラウド・サービス」の特定の構成へのアクセスを意味します。お客様の「PoE」または「取引文書」に定める課金期間中にアクセスおよび使用が可能となる「クラウド・サービス」の各「インスタンス」に対する十分なエンタイトルメントを取得しなければならないものとします。

b. **「許可ユーザー」**は、「クラウド・サービス」を取得する際の課金単位です。お客様は、直接または間接のいかなる方法においても (例えば、多重化プログラム、デバイスまたはアプリケーション・サーバーを通じて)「クラウド・サービス」へのアクセスを与えられた特定の「許可ユーザー」ごとに、個別に専用のエンタイトルメントをいずれかの手段により取得しなければならないものとします。お客様の「PoE」または「取引文書」に定める課金期間中に「クラウド・サービス」へのアクセスを与えられた「許可ユーザー」の数をカバーするのに十分なエンタイトルメントを取得しなければならないものとします。

c. **「エンゲージメント」**は、サービスを取得する際の課金単位です。「エンゲージメント」は、「クラウド・サービス」に関連するプロフェッショナル・サービス、研修サービスまたはその両方のサービスで構成されます。それぞれの「エンゲージメント」をカバーするのに十分なエンタイトルメントを取得しなければならないものとします。

### 5.2 超過料金

課金期間中の「クラウド・サービス」のお客様による実際の利用が、「PoE」に記載されたエンタイトルメントの範囲を超える場合には、お客様は、「取引文書」の記載に従い、その超過分について請求されます。

### 5.3 リモート・サービス料金

「リモート・サービス」は、「エンゲージメント」単位で購入するものとし、「取引文書」に記載された料金で請求されます。

## 6. 期間および更新オプション

「クラウド・サービス」の期間は、「PoE」に記述されるとおり、「クラウド・サービス」へのお客様のアクセスについて、IBM がお客様に通知した日に開始します。「PoE」には、「クラウド・サービス」が自動的に更新されるか、継続利用ベースで続行されるか、期間満了時に終了するかが記載されます。

自動更新の場合には、お客様が期間満了日の 90 日前までに書面により更新しないことを通知する場合を除き、「クラウド・サービス」は、「PoE」に定める期間につき自動更新されます。

継続利用の場合は、「クラウド・サービス」は、お客様が 90 日前までに書面により終了を通知するまで、月単位で継続利用することができます。「クラウド・サービス」は、かかる 90 日の期間後の暦月末日まで引き続き利用することができます。

## 7. 追加条件

### 7.1 共通事項

お客様は、IBM が広報活動またはマーケティングのコミュニケーションにおいて、お客様を「クラウド・サービス」の利用者として公に言及できることに同意します。

### 7.2 遵守性管理クラウド・サービス

「クラウド・サービス」は、お客様が法規、規格または慣行に基づく遵守義務を満たすことを支援するために使用することができます。お客様は、「クラウド・サービス」が提供するいかなる指示、提案する使用法、またはガイダンスも、法律上、会計上、またはその他の専門的な助言ではないことを了承して同意し、お客様はお客様自身で法律上またはその他の専門的な助言を得るものとします。お客様は、お客様とお客様の活動、アプリケーション、およびシステムがあらゆる適用法規、規格、および慣行に準拠していることを保証する責任を単独で負うことにも同意します。「クラウド・サービス」の使用は、法規、規格または慣行に適合することを保証するものではありません。

### 7.3 クラウド・サービスの合法的利用

「クラウド・サービス」は、お客様のセキュリティー環境およびデータの改善についてお客様を支援するように設計されています。「クラウド・サービス」の利用は、さまざまな法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。「クラウド・サービス」は、合法的目的かつ合法的方法による場合にのみ利用可能です。お客様は、適用される法律、規則、および方針に従って「クラウド・サービス」を利用することに同意し、それらを遵守する一切の責任を負うものとします。お客様は、「クラウド・サービス」の合法的な利用に必要なすべての同意、許可、またはライセンスを取得するか、取得済みであることを表明します。

### 7.4 セキュリティー・データ

報告作業を含む「クラウド・サービス」サービスの一部として、IBM は、「クラウド・サービス」から収集された情報を匿名化または集約したものを準備し、維持管理します (以下「セキュリティー・データ」といいます) 。「セキュリティー・データ」では、下記 (d) に定めるものを除いて、お客様も個人も特定することはありません。お客様は本書において、以下のみを目的として IBM が「セキュリティー・データ」を使用またはコピーできることにさらに同意します。

a. 「セキュリティー・データ」の公表または配布 (サイバーセキュリティーに関連する集計または分析など)

b. 製品やサービスの開発または拡張

c. 社内で、または第三者と共に実施する調査

d. 確認済みの第三者の攻撃者情報の合法的な共有

### 7.5 Cookie

お客様は、IBM が「クラウド・サービス」の通常の運用およびサポートの一部として、トラッキングおよびその他の技術により、「クラウド・サービス」の利用に関連してお客様 (お客様の従業員および従契約者) から個人情報を収集することがあることを認識し、これに同意するものとします。IBM によるこのような情報収集は、ユーザー・エクスペリエンスの向上またはお客様との対話の調整を目的とし、「ク

ラウド・サービス」の有効性について使用統計および情報を収集するために行うものです。お客様は、IBM およびその他の IBM グループ会社が、営業活動を行ういずれの地域においても、適用法に従い、IBM、その他の IBM グループ会社およびそれぞれの従契約者が収集した個人情報を上記の目的のために処理することができるよう、お客様が同意を取得すること、または取得済みであることを確認するものとします。IBM は、収集した個人情報へのアクセス、更新、修正または削除について、お客様の従業員および従契約者からの要求に従うものとします。