IBM Application Security on Cloud

ご利用条件 (以下「ToU」といいます。) は、本「IBM ご利用条件 – SaaS 特定オファリング条件」(以下「SaaS 特定オファリング条件」といいます。)、および以下の Web サイトでご覧いただける「IBM ご利用条件 – 一般条件」(以下「一般条件」といいます。) で構成されています (URL:http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/)。

「SaaS 特定オファリング条件」と「一般条件」の規定に矛盾がある場合、「SaaS 特定オファリング条件」が優先して適用されるものとします。「IBM SaaS」の注文、そのアクセスまたは利用により、お客様は「ToU」に同意したものとみなされます。

「ToU」には、「IBM パスポート・アドバンテージのご契約条件」、「IBM パスポート・アドバンテージ・エクスプレスのご契約条件」、または「IBM SaaS 特定オファリングのご契約条件」のうち該当する契約条件 (以下「本契約」といいます。) が適用され、これらと「ToU」を合わせて完全な合意として成立します。

1. IBM SaaS

以下の「IBM SaaS」オファリングに、これらの「SaaS 特定オファリング条件」が適用されます。

- IBM Application Security Analyzer
- IBM Application Security on Cloud Consulting Services

2. 課金単位

「IBM SaaS」は、「取引文書」に記載された以下の課金単位のいずれかに従って販売されます。

a. **「ジョブ」**は、「IBM SaaS」を取得する際の課金単位です。「ジョブ」は、それ以上分割することのできない、「IBM SaaS」内のオブジェクトで、それにかかわるすべてのサブプロセスを含む計算プロセスを表します。お客様は、お客様の「証書 (PoE)」または「取引文書」に定める課金期間中に「IBM SaaS」が処理または管理する「ジョブ」の総数をカバーするのに十分な使用許諾を取得しなければならないものとします。

b. **「アプリケーション・インスタンス」**は、「IBM SaaS」を取得する際の課金単位です。「IBM SaaS」に接続された「アプリケーション」の「インスタンス」ごとに、「アプリケーション・インスタンス」の使用許諾が必要となります。「アプリケーション」に複数のコンポーネントが含まれており、各コンポーネントが、異なる目的を果たす、別々のユーザー・ベースである、別々の接続を持っているなどといった場合には、かかる各コンポーネントは、個別の「アプリケーション」とみなされます。さらに、「アプリケーション」のテスト、開発、ステージング、および実稼働の各環境は、それぞれが「アプリケーション」の個別のインスタンスとみなされ、それぞれについて使用許諾を取得しなければならないものとします。1 つの環境に含まれる「アプリケーション」の複数の「インスタンス」は、それぞれが「アプリケーション」の個別のインスタンスとみなされ、それぞれについて使用許諾を取得しなければならないものとします。お客様は、お客様の「PoE」または「取引文書」に定める課金期間中に「IBM SaaS」に接続された「アプリケーション・インスタンス」の数をカバーするのに十分な使用許諾を取得しなければならないものとします。

本「IBM SaaS」においては、以下のとおりとします。

- 「動的テスト」の場合: 公開または非公開の URL 経由でアクセス可能な Web サイト。各「アプリケーション・インスタンス」には、単一ドメインで最大 1,000 ページからなる 1 つのサイトに対する資格を与えます。
- 「静的テスト」の場合: 単一のプログラム言語で実行可能なコード単位。各「アプリケーション・インスタンス」は、最大 1,000,000 行のコードをスキャンする資格を与えます。
- 「モバイル・テスト」の場合: モバイル・デバイス上で実行可能なバイナリー・コードの単位。各異種モバイル・プラットフォーム (例: iOS および Android) は異なる「アプリケーション・インスタンス」とみなされます。

c. **「インスタンス」**は、「IBM SaaS」を取得する際の課金単位です。「インスタンス」とは、「IBM SaaS」の特定の構成へのアクセスを意味します。お客様の「証書 (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利用することが可能な「IBM SaaS」の「インスタンス」ごとに十分な使用許諾を取得しなければならないものとします。

各「インスタンス」の使用許諾については、実行される「ジョブ」または「アプリケーション・インスタンス」 (接続される「アプリケーション」) の数量に制限はありません。ただし、同時に 30 を超える「ジョブ」を実行することはできません。

d. **「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、「IBM SaaS」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使用許諾を取得しなければならないものとします。

3. 料金および課金

「IBM SaaS」に対する料金は、「取引文書」に記載されます。

3.1 1 か月に満たない期間の料金

「取引文書」に記載された 1 か月に満たない期間の料金は、按分にて算定される場合があります。

3.2 超過料金

課金期間中の「IBM SaaS」の実際の利用が、「PoE」に記載された使用許諾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。

3.3 セットアップ料金

お客様は、「取引文書」に定めるとおり、セットアップの料金を請求されます。

4. 期間および更新オプション

「IBM SaaS」の期間は、「PoE」に記述されるとおり、「IBM SaaS」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、「IBM SaaS」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少なくとも 30 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、「IBM SaaS」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、「IBM SaaS」は、お客様が 30 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。「IBM SaaS」は、かかる 30 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。

5. テクニカル・サポート

「サブスクリプション期間」中、および IBM が「IBM SaaS」へのアクセスが利用可能になった旨をお客様に通知後、テクニカル・サポートオンライン・フォーラム経由で、お客様が「従量制課金」の料金を負担する期間中は標準サポートとして提供されます。「IBM SaaS」内から、お客様はサポート・チケットを送信したり、支援用チャット・セッションをオープンしたりできます。IBM は、テクニカル・サポートの連絡先情報ならびにその他情報およびプロセスを規定する IBM Software as a Service Support Handbook を提供します。

重要度	重要度の定義	目標応答時間	対象応答時間
1	**重大な事業影響/サービス・ダウン** 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	1 日 24 時間週 7 日

重要度	重要度の定義	目標応答時間	対象応答時間
2	**著しい事業影響** サービス事業機能またはサービスの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	月曜から金曜の営業時間
3	**軽度の事業影響** 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ないことを示す。	4 営業時間以内	月曜から金曜の営業時間
4	**最小の事業影響** 問い合わせまたは非技術的な依頼。	1 営業日以内	月曜から金曜の営業時間

5.1 お客様データへのアクセス

IBM は、当該サービスでの問題を診断する目的でお客様データにアクセスすることができ、当該サービスによりお客様のアプリケーションのスキャンを容易に行うことができます。IBM が当該データにアクセスするのは、IBM 製品もしくは IBM サービスに関する障害の修正、または、これらに対するサポート提供を目的とした場合のみとします。

6. 「IBM SaaS」オファリングの追加条件

セキュリティー・スキャンは、アプリケーションにおけるすべてのセキュリティー・リスクを特定することはできません。また、フェイルセーフ運用を必要とする危険な環境での使用のために設計されたものでも、それを意図したものでもありません。これには、航空機航行、航空管制システム、兵器システム、生命維持装置、核施設が含まれますが、これらに限定されるものではなく、セキュリティー・リスクを特定できなかったことが死亡や人身傷害、物的損害につながる可能性のあるその他のあらゆるアプリケーションが含まれます。セキュリティー・スキャンについては、中断やエラーのない運用が保証されていません。

「IBM SaaS」は、お客様が法規、規制、規格または慣行に基づく遵守義務を満たすために使用される場合があります。「サービス」が提供する指示、推奨使用法またはガイダンスは、法律上、会計上、またはその他の専門的な助言ではないため、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取得するようにしてください。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ものとします。「サービス」の使用は、あらゆる法規、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。

「IBM SaaS」は、お客様がスキャンすることを選択した Web サイトおよび Web またはモバイル・アプリケーション上で侵入テストおよび非侵入テストを実施します。特定の法律では、コンピューター・システムへの侵入またはアクセスの不正な試みを禁止しています。お客様は、IBM が本書に記載のとおりに「サービス」を実行することを許可し、「サービス」がお客様のコンピューター・システムへの許可アクセスとみなされることに同意します。IBM は、「サービス」を実行するのに必要と判断した場合には、この権限の付与について第三者に開示できます。

このテストの実行は、以下のような特定のリスクを伴いますが、これらに限定されるものではありません。

a. テスト中にアプリケーションを実行するお客様のコンピューター・システムは、停止またはクラッシュする可能性があり、その場合には、一時的にシステムが使用できなくなるか、またはデータの損失が生じます。

b. お客様のシステムのパフォーマンスおよびスループット、ならびに関連するルーターおよびファイアウォールのパフォーマンスおよびスループットが、テスト中に、一時的に低下する場合があります。

c. 過剰な量のログ・メッセージが生成され、ログ・ファイル・ディスク領域の過剰な消費につながる場合があります。

d. 脆弱性を精査した結果として、データが変更または削除される場合があります。

e. 侵入検知システムによってアラームが起動する場合があります。

f. テスト中の Web アプリケーションの電子メール機能によって電子メールが起動する場合があります。

g. 「IBM SaaS」はイベントを探すために監視中のネットワークのトラフィックを妨害する場合があります。

IBM から提供された、およびテストの対象である Web サイトまたはアプリケーションに関連する、サービス・レベル・アグリーメントの権利または救済は、テスト活動中は適用されません。

お客様が、テスト中のアプリケーションの認証済みログイン資格情報を「サービス」に入力する場合、お客様は、テスト・アカウントの資格情報のみを入力し、実稼働ユーザーの資格情報を入力してはなりません。実稼働ユーザーの資格情報の使用は、「サービス」による個人データの送信につながる場合があります。

「IBM SaaS」は実稼働中の Web アプリケーションをスキャンできるように構成できます。お客様がスキャン・タイプを「実稼働」に設定した場合、このサービスは上記のリスクを軽減する方法でスキャンを実行するよう設計されます。ただし、状況によっては「IBM SaaS」により、テスト対象の実稼働場所やインフラストラクチャー内でパフォーマンスが低下したり、不安定になる場合があります。IBM は、実稼働場所をスキャンするために「IBM SaaS」を使用することの適合性に関して何等の保証あるいは表明をしません。

「サービス」がお客様の Web サイト、Web アプリケーション、モバイル・アプリケーションまたは技術環境に対して適切であるかどうか、もしくは安全であるかどうかについては、お客様が責任を持って判断します。

「IBM SaaS」は、モバイルおよび Web アプリケーションならびに Web サービスのセキュリティーおよびコンプライアンスに関する潜在的な各種問題を特定できるように設計されています。「クラウド・サービス」は脆弱性およびコンプライアンスに関するすべてのリスクをテストするわけではなく、また、セキュリティー攻撃に対する障壁の役目も果たしません。セキュリティーの脅威、規制および標準は変化し続けているため、「サービス」はかかる変更のすべてを反映できません。お客様の Web アプリケーション、システムおよび従業員のセキュリティーとコンプライアンス、救済措置については、お客様が一切の責任を負います。「サービス」によって提供される情報を使用するかどうかは、お客様の判断に一任されます。

特定の法律では、コンピューター・システムへの侵入またはアクセスの不正な試みを禁止しています。お客様は、お客様が所有する Web サイトおよびアプリケーション、またはお客様がスキャンする権利および権限を有する Web サイトおよびアプリケーション以外の Web サイトおよびアプリケーションをスキャンするために「サービス」を使用しないことを保証する責任を負います。

明確にするために付言しますが、「IBM ご利用条件 – 一般条件」のデータ保護の項に記載されているお客様のコンテンツには、「アプリケーション侵入テスト」中に IBM のアクセスが可能になる可能性のあるデータも含まれているものとみなされます。

6.1 第三者が所有するシステム

本書に基づいてテストの対象となる、第三者が所有するシステム (本規定においては、アプリケーションおよび IP アドレスが含まれますが、これらに限られません。) について、お客様は以下に同意します。

a. IBM が第三者システム上でテストを開始する前に、お客様は各システムの所有者から、IBM が当該システム上で「サービス」を提供することを許可した、および「テストの実行の許可 (Permission to Perform Testing)」という表題の項に規定された条件に当該所有者が同意したことを示す、署名済みの書簡を入手し、かかる許可のコピーを IBM に提供すること。

b. IBM のリモート・テストにより当該システムで特定されたリスク、エクスポージャー、および脆弱性をシステム所有者に伝える責任を負うこと。

c. IBM が必要と判断した、システム所有者と IBM 間の情報交換を手配し、促進すること。

お客様は以下に同意します。

- 本契約書に基づくテストの対象であるシステムの所有権に変更があった場合には、必ず IBM に即時通知すること。
- IBM の書面による事前同意なくお客様の「エンタープライズ」以外で、成果物を開示しないこと、および IBM が「サービス」を実行したことを開示しないこと。

- お客様が本項「第三者が所有するシステム」の要件をお客様が満たせなかったことに起因する第三者の請求により IBM が負担するあらゆる損失または負債について、および (a) 本書に基づくテストの対象であるシステムのセキュリティー・リスク、エクスポージャーまたは脆弱性をテストすること、(b) かかるテストの結果をお客様に提供すること、または (c) かかる結果のお客様による使用もしくは開示に起因する、IBM または IBM の従契約者もしくは代理人を相手に起こされた第三者の罰金または請求について、IBM を免責すること。

6.2 Cookie

お客様は、IBM が「IBM SaaS」の通常の運用およびサポートの一環として、トラッキングおよびその他の技術により、「IBM SaaS」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、「IBM SaaS」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、その他の IBM グループ会社およびその従契約者が、営業活動を行う地域において、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の範囲内で、収集した個人情報を以上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。

報告作業を含む「IBM SaaS」の一部として、IBM は、「IBM SaaS」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犯罪者情報の合法的な共有

6.3 Derived Benefit Locations

該当する場合、お客様が「IBM SaaS」に関する利益を享受しているとお客様が特定する所在地の税金が適用されます。IBM は、お客様が IBM に追加情報を提供する場合を除き、「IBM SaaS」の注文時に主要な Benefit Location として記載した事業所住所に基づいて税金を適用します。お客様は、当該情報を最新状態に保ち、変更があった場合には IBM に通知する責任を負うものとします。

6.4 個人情報および規制コンテンツおよびサービス

本「IBM SaaS」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即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「IBM SaaS」に関連して使用するコンテンツのタイプについて、本「IBM SaaS」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。

IBM は、米国連邦通信委員会 (以下、「FCC」といいます。) または州規制当局 (以下、「州監督機関」といいます。) によって規制されるサービスの提供者として運用しておらず、また FCC または「州監督機関」によって規制されるサービスを提供することを意図してもいません。FCC またはいずれかの「州監督機関」が、本書に基づいて IBM が提供するサービスに規制要件または義務を課す場合、IBM は以下のいずれか、または両方を行うことができます。(a) お客様の費用負担で製品の変更、交換、または代替を行う、(b) IBM に対するかかる要件または義務の適用を回避するために (例えば、第三者の電信電話会社からかかるサービスを取得するお客様の代理人として機能することによるなど) お客様へのサービス提供方法を変更する。

別紙 A

1. IBM Application Security on Cloud の概要

IBM Application Security on Cloud は、さまざまなアプリケーションについて、セキュリティーの脆弱性 (SQL インジェクション、クロスサイト・スクリプティング、およびデータ漏えい) を特定するための 1 つの場所をお客様に提供します。本サービスには、アプリケーションに対するセキュリティー・スキャンの多様な技法が含まれており、そのそれぞれは、該当するアプリケーションに含まれるセキュリティー問題を特定します。

IBM Application Security on Cloud は、以下の機能を提供します。

- セキュリティーの脆弱性を検出する、「モバイル・アプリケーション」のスキャン。これは、ダイナミック (ブラックボックス) およびインタラクティブ (グラスボックス) 手法のセキュリティー分析技術によって実行されます。
- セキュリティーの脆弱性を検出する、実稼働もしくは実稼働前の Web サイト、パブリック対応の、またはプライベート・ネットワーク上の Web サイトのスキャン。これは、ダイナミック (ブラックボックス) 手法のセキュリティー分析技術によって実行されます。
- セキュリティーの脆弱性を検出する、Web アプリケーションおよびデスクトップ・アプリケーション内のデータフローのスキャン。これは、スタティック (ホワイトボックス) 手法のセキュリティー分析技術によって実行されます。
- セキュリティーの脆弱性の詳細なレポート。これには、検出結果の大まかな要約、および開発者が従うことのできる修復ステップの両方が含まれます。
- さまざまな DevOps プラットフォームとの統合。

1.1 IBM Application Analyzer

IBM Application Analyzer は、「アプリケーション・インスタンス」単位、「ジョブ (スキャン)」単位、またはフル「インスタンス」として注文することができ、以下のスキャン・タイプを可能にします。

- 「動的アナライザー」 – DAST 技術により実稼働前 Web サイトまたは実稼働 Web サイトをテストします。
- 「モバイル・アナライザー」 – IAST 技術により iOS バイナリーまたは Android バイナリーをテストします。
- 「静的アナライザー」 – SAST 技術によりバイト・コードまたはソース・コードのデータをテストします。

1.2 セットアップ・サービス

IBM Application Security on Cloud Consulting Services は、商品化された Application Analyzer 用のセットアップ・サービスです。「サービス」は IBM コンサルタントを活用して、アプリケーション・リスクのテストと管理についてガイダンスと支援を提供します。IBM Application Security on Cloud Consulting Services は、以下の特定サービスを要求して活用するために、以下に規定される数量で使用可能な「エンゲージメント」のブロックで購入されます。

a. **ファースト・スタート** [1 つの「エンゲージメント」単位を使用]

「ファースト・スタート」サービスでは、Application Security on Cloud のテスト・フィーチャーおよびリスク管理フィーチャーを活用するための専門知識とガイダンスを提供します。お客様が Application Security on Cloud ポータルへの正常なログインを確認後、IBM は、最大 2 時間の 2 名のアクティブな参加者による Web 会議を進行して、「IBM SaaS」の構成および機能の基本の AppSec について教育を提供します。これには、スキャン・タイプ、スキャンの実行、レポートの確認、および関連するツールおよびプラグインのインストールなどが含まれます。「ファースト・スタート」サービスは、(a) お客様の教育 Web セミナー、(b) 使用可能なツールおよびプラグインのインストー

ル、および (c) お客様の最初のスキャンをセットアップして実行するためのお客様への支援が完了した後に完了します。

b. **評価レビュー** [2 つの「エンゲージメント」単位を使用]

「評価レビュー」サービスは、テスト結果の確認において支援を提供します。これには、アプリケーションの脆弱性の修復を理解して優先順位を付けることが含まれます。IBM は、最大 1 時間の 2 名のアクティブな参加者による Web 会議を進行して、発見された脆弱性およびアプリケーションの全体的なセキュリティー・リスクの概要を提供し、発見されたアプリケーション・セキュリティーの脆弱性について詳細な話し合いを行います。これには、(1) 脆弱性をどのようにテストしたのか、(2) 脆弱性をどのように検出したのか、(3) 各脆弱性に関するリスクが何か、および (4) 脆弱性の修正に役立つ一般的なフィックスに関する推奨を提供することが含まれます。このレビューは、テスト結果のみに基づき、ソース・コード自体のレビューにはなりません。お客様はテスト結果を確認し、Web 会議前に、IBM に対してレビュー用のテスト結果を特定します。「評価レビュー」サービスは、Web 会議の完了後に完了します。

c. **スキャン代行** [4 つの「エンゲージメント」単位を使用]

「スキャン代行」サービスは、検出結果を確認するためにスキャンの構成と実行、結果の検証、およびレポートの概要報告を実施する IBM アプリケーション・セキュリティーの専門家を提供します。お客様は、スキャンの構成と実行、結果の検証、修復の優先順位付けに関する推奨、およびレポートの概要報告を実施するために IBM コンサルタントがお客様の ASoC 環境にアクセスすることを許可します。IBM は、最大 1 時間の 2 名のアクティブな参加者による Web 会議を進行して、発見された脆弱性およびアプリケーションの全体的なセキュリティー・リスクの概要を提供し、発見されたアプリケーション・セキュリティーの脆弱性について詳細な話し合いを行います。これには、(1) 脆弱性をどのようにテストしたのか、(2) 脆弱性をどのように検出したのか、(3) 各脆弱性に関するリスクが何か、および (4) 脆弱性の修正に役立つ一般的なフィックスに関する推奨を提供することが含まれます。要求された場合、初期スキャンの最大 30 日後に、IBM は、セキュリティー・フィックスを検証するためのみに、元のスキャン構成を利用して再スキャンを行います。新規機能をテストしたり、結果を検証したり、お客様に報告を提供したりしません。「スキャン代行」サービスは、初期スキャンの結果を確認するための Web 会議の完了後、または該当する場合には、お客様の要求に従った再スキャンおよびお客様への再スキャン・レポートの提供の完了後に、完了します。

d. **オンデマンド・アドバイザー** [7 つの「エンゲージメント」単位を使用]

「オンデマンド・アドバイザー」サービスは、最大 20 時間の IBM コンサルタントの時間を提供します。この時間は、「IBM SaaS」に関連する活動に対して使用可能です。IBM コンサルタントは、アプリケーション・セキュリティーの特定のトピックについて支援を行います。これには、プログラム管理、セキュリティー・テストの優先順位付け、修復戦略、ソース・コード分析およびソース・コード修復が含まれますが、これらに限定されません。IBM はお客様と協力して、プロジェクトの目標、関連テクノロジー、望ましいタイムライン、予想される成果物、および「オンデマンド・アドバイザー」サービスについて予想されるエンゲージメントの数を含む、特定のお客様の要件に合わせたプロジェクト・スケジュールを理解して作成します。お客様は、サービスを実行するために求められる必要なアプリケーション、システムおよび資料へのアクセスを提供しなければなりません。「オンデマンド・アドバイザー」サービスは、最大 20 時間のセキュリティー専門知識が実行された時点、またはプロジェクト・スケジュールもしくはプロジェクト・スケジュールで定義された文書化済みの成果物がお客様に提供された後で、完了します。

e. **アプリケーション侵入テスト**

3 つのオプションがあります。

(1) **コンプライアンス/エントリー・レベルのアプリケーション侵入テスト**は、最大 40 時間の「コンサルタント」の時間を含み、また「単一」ステップの論理的欠陥、および「簡易」バージョンのインジェクションの欠陥に重点を置きます。15 の「エンゲージメント」単位を利用します。

(2) **標準のアプリケーション侵入テスト**は、最大 60 時間の「コンサルタント」の時間を含み、また複数ステップのワークフローに関する「論理的」欠陥、「複合」バージョンのインジェクションの欠陥、および複合データ・タイプの「分析」を含むように重点を拡張します。21 の「エンゲージメント」単位を利用します。

(3) **拡張のアプリケーション侵入テスト**は、最大 80 時間の「コンサルタント」の時間を含み、また蓄積された実行可能ファイルの「リバース」エンジニアリング、カスタム・ネットワーク・プロトコルの「分解」、一般に使用可能なライブラリーおよびフレームワークの「詳細」分析を含むように重点を拡張します。27 の「エンゲージメント」単位を利用します。

アプリケーション侵入テスト・サービスでは IBM リソースを提供して、アプリケーションのテストおよび弱点の使用、テスト・レポートの提供、ならびに検出結果および関連リスクを説明するためのレポートの概要報告を実行します。

IBM は、最大 1 時間の 2 名のアクティブな参加者による、プロジェクトの開始コールを進行して、お客様の環境および組織を確認します。これには、アプリケーション・プラットフォーム、アーキテクチャー、フレームワーク、サポート・インフラストラクチャー、アプリケーションに関する既知のセキュリティー問題または懸念事項、予備テストのスケジュールおよび緊急連絡計画が含まれます。

IBM は、アプリケーション侵入テストを実行します。これには、一般的な脆弱性 (SQL インジェクションやクロスサイト・スクリプティングなど) の特定、既存のセキュリティー管理 (インプットの検証、認証、および許可など) の強みおよび弱みの評価、ビジネス・ロジックの適切な適用の確認、セキュア・プロトコルの適切な使用の検証、セッション処理の欠陥の特定、ならびにログイン、パスワード・リカバリー、パスワード・ポリシーに関する適切なセキュリティー管理、およびその他のユーザー管理機能の検証が含まれますが、これらに限定されません。検出結果は、「アプリケーション侵入テスト・レポート」で文書化されます。IBM は、最大 1 時間のレポートの概要報告のための Web 会議を進行します。「アプリケーション侵入テスト」サービスは、割り当てられたコンサルティング時間が使用され、Web 会議が実行され、最終の「アプリケーション侵入テスト・レポート」がお客様に提供された時点で完了します。

1.2.1 セットアップ・サービスに関する責任

IBM は以下を行うものとします。

- お客様が購入した「エンゲージメント」単位を使用して、「POE」ごとに「セットアップ・サービス」を提供する。
- 第 1.2 項に記載された完了基準が完了したときに「セットアップ・サービス」は完了している。

お客様は以下に同意します。

- 契約期間中にお客様が行った、すべての「エンゲージメント」要求に関連するすべての料金に対して責任を負うこと。
- ならびに購入した「エンゲージメント」単位は初期契約期間内に使用しなければならないこと、および契約期間の終了日までに未使用の場合には失効することに同意すること。
- サブスクリプションの終了日の 30 日前までにすべての「セットアップ・サービス」に対して正式要求を開始すること。

「セットアップ・サービス」の実行において、IBM はお客様からの情報および相応の協力を要求する場合があります。要求された情報や協力を適時にお客様が提供できない場合、IBM が決めたとおり、サービスによって要求される「エンゲージメント」単位料金、または該当するサービスの実行の遅延につながる可能性があります。

IBM がテストを正確に実行するために、お客様は、環境を準備し、テスト期間にわたって環境を維持することについて IBM の指示に従うことに同意します。