シマンテック™ インシデント レスポンス リテーナー サービス

サービス規定

2015 年 10 月 5 日

サービス概要

本サービス規定は、本サービス規定に含まれるシマンテックが提供する本サービスに関して、参照されることにより含まれる他の添付資料と共に、参照することにより本サービス規定が組み込まれるあらゆる契約（総称して「本契約」）の一部となります。本サービス規定は、お客様が2015年10月5日以降に購入した本サービスに対して適用されます。お客様が 2015 年 10 月 5 日より前に購入した本サービスについては、お客様の購入日に基づき、2015 年 4 月 6 日付または 2015 年 6 月 3 日付のサービス規定が適用されます。（同規定は、http://go.symantec.com/proserveterms で閲覧するか、またはシマンテックにお問い合わせ頂ければ提供致します。）

シマンテック™ インシデント レスポンス リテーナー サービスは、お客様のセキュリティ インシデントに効果的に対処するために必要とされる重要な能力を継続的に利用する機会を提供します。シマンテック™ インシデント レスポンス リテーナー サービスは、サブスクリプション文書および本サービス規定に従い、お客様が購入されたサービス提供内容に基づき、以下サービス（「**本サービス**」）の一つまたは組み合わせで構成されます。

1. **リテーナーサービス*:** スタンダード、エンタープライズ、およびアドバンスドエンタープライズのリテーナーサービスにバンドルされている当社推奨数の事前購入サービスデイおよび SLA オプションから成り、12、24 または 36 カ月の契約期間で利用可能（それぞれ「**リテーナーサービス**」）。
2. **カスタムリテーナーオプション*:** リテーナーサービスの組み合わせとは別に、 **24 時間**または **48 時間** SLA、および任意にサービスデイを組み合わせてカスタマイズされたリテーナー（「**カスタムリテーナーオプション**」）。カスタムリテーナーオプションは、単独のサービスオプションとして別途購入することもでき、またはお客様の既存のリテーナーサービス拡張のために購入することもできます。カスタムリテーナーオプションは、12、24、または 36 ケ月の契約期間で購入できます。**お客様の既存のリテーナーサービス拡張のためにカスタムリテーナーオプションを購入する場合、当該カスタムリテーナーオプションはかかるリテーナーサービスとともに終了するものとします。**
3. **追加サービスデイおよびレスポンス要員*:** リテーナーサービスまたはカスタムリテーナーオプションのお客様は、必要に応じてインシデント調査中に追加サービスデイおよび/または追加レスポンス要員を事前に購入することもできます。

* シマンテックが提供するすべてのサービスは、代金が支払われたサブスクリプション文書で記載されている**本地域**内で行われるものとします。

目次

シマンテック™ インシデント レスポンス リテーナー サービス

サービス規定

2015 年 10 月 5 日

テクニカル/ビジネスの機能および能力

サービスの特徴

インシデントレスポンス リテーナー サービスに関する本サービスの特徴は以下の通りとなります。

サービスの特徴	サービスの特徴の説明
サービスの管理	お客様には、お客様の業種または営業地域ならびにお客様のセキュリティ成熟度に基づき、シマンテックサービスマネージャーが割り当てられます。
365日24時間対応の電話および電子メールによるアクセス	お客様は、インシデントレスポンスアシスタンスの連絡先として、365 日 24 時間対応のシマンテックのインシデントレスポンス対応チームに電話連絡（「**インシデントレスポンスアシスタンスコール**」）頂けます。お客様は 365 日 24 時間いつでもインシデントレスポンス対応チームに電子メールでも連絡頂けます。
コールバック SLA	シマンテックのインシデントレスポンス対応チームは、シマンテックによるお客様のインシデントレスポンスアシスタンスコールの受信後 3 時間以内に折り返し連絡を行います。該当時間内にお客様のインシデントレスポンスアシスタンスコールへの折り返し連絡が行われない場合、シマンテックは、1 サービスクレジットをお客様のアカウントに付与します。
新種脅威レポート	シマンテックは、お客様のセキュリティ態勢に影響を及ぼす可能性のある新種の脅威に関する、シマンテック発行の新種脅威レポートを定期的にお客様に提供します。新種脅威レポートには、次のような内容が含まれます。（i）概要、（ii）技術的脅威詳細、（iii）攻撃ベクトル、（iv）検出能力および指標、（v）軽減措置および提案、および/または（vi）参照のための追加情報。
遠隔 SLA	シマンテックは、シマンテックへの連絡の受領後 12 通常営業時間内に遠隔サービス(以下「**遠隔サービス**」で定義)を開始します。シマンテックが該当時間内に遠隔評価を開始しない場合、シマンテックは、遅滞した各通常営業日につき 1 サービスクレジットをお客様のアカウントに付与します。
インシデント調査	シマンテックがインシデント調査期間中に実施する可能性のある事項は、以下の「**インシデント調査**」に規定されています。インシデント調査は、すでに代金が支払われたサブスクリプション文書に記載の本地域内にあるお客様の所在地において行われるものとします。
サービスデイ	▪ **スタンダード**では、12、24、または 36 カ月間につき、それぞれ **10**、**20**、または **30** サービスデイが含まれます。 ▪ **エンタープライズ**では、12、24、または 36 カ月間につき、それぞれ **30**、**60**、または **90** サービスデイが含まれます。 ▪ **アドバンストエンタープライズ**では、12、24、または 36 カ月間につき、それぞれ **60**、**120**、または **180** サービスデイが含まれます。 ▪ **カスタムリテーナーオプション**では、**12**、**24**、または **36** カ月間につき、それぞれ追加の **5**、**10**、または **15** サービスデイが含まれます。

サービスの特徴	リテーナーサービス			カスタムリテーナーオプション*	サービスの特徴の説明
	スタンダード	エンタープライズ	アドバンスドエンタープライズ		
現場出動 SLA	優先スケジュール設定	48 時間	24 時間	48 または 24 時間（お客様の購入に応じて）	インシデント調査レスポンス要員は、インシデント調査登録の後、該当する時間内にインシデント調査のためお客様の施設に「出発」します。「出発」とは、インシデント調査レスポンス要員がお客様の所在地への移動を開始したことを意味し、お客様の所在地はすでに代金が支払われたサブスクリプション文書に記載の**本地域内**に所在する**必要**があります。シマンテックが該当する時間内にインシデント調査レスポンス要員をお客様の施設に「出発」させない場合、シマンテックは、遅延した各通常営業日につき1 サービスクレジットをお客様のアカウントに付与します。「**優先スケジュール設定**」に関して、シマンテックはインシデント調査要員をインシデント調査登録後ただちに「出発」させるためにのみ最善を尽くします。

* お客様の既存のリテーナーサービスの拡張のためにカスタムリテーナーオプションを購入する場合、当該カスタムリテーナーオプションはかかるリテーナーサービスとともに終了するものとします。

リテーナーサービスまたはカスタムリテーナーオプションに追加して、お客様は以下のサービスの購入ができます。

サービスの特徴	サービスの特徴の説明
追加サービスデイ	お客様が、お客様のリテーナーサービスまたはカスタムリテーナーオプション（該当する場合）に含まれるサービスデイの追加をご希望の場合、セキュリティインシデントの前に **5**、**30**、または **60** サービスデイ単位の追加サービスデイを事前購入頂けます。お客様の所在地はすでに代金が支払われたサブスクリプション文書に記載の本地域内に所在する必要があります。事前に購入した追加サービスデイは、お客様のリテーナーサービスまたはカスタムリテーナーオプション（該当する場合）の期間と同時に終了します。
追加レスポンス要員	インシデント調査の間、追加インシデント調査レスポンス要員（「**追加レスポンス要員**」）の設定が推奨されるとシマンテックが判断する場合、お客様はかかる追加レスポンス要員の購入を選択することができます。1 追加レスポンス要員の購入により、お客様は **5** サービスデイの間インシデント調査のための 1 追加レスポンス要員の利用が可能となり、WAF（作業承認書）に反映されます。**追加レスポンス要員は購入日から 30 日以内に使用および提供されなければなりません。**

インシデント調査

インシデント調査の要請　お客様は、インシデント調査要請のため、シマンテックに連絡するものとします。シマンテックとお客様は、セキュリティインシデントの性質と種類に基づいて、適切な数と種類のレスポンス要員と必要なサービスデイについて合意するものとします。その後、シマンテックはお客様に対し、これらの合意内容を記載した作業承認書（WAF）を提出するものとし、お客様は、当該 WAF に記名押印または署名してシマンテックに返却しなければなりません（「**インシデント調査登録**」）。インシデント調査登録の日付は、シマンテックがお客様の記名押印または署名済みWAFを受領した日となります。インシデント調査登録後、シマンテックは、サービスレベル契約に従いお客様の所在地への移

動を開始および/または遠隔からのインシデント調査を実施します。シマンテックがインシデント調査期間中に実施する可能性のある事項の詳細は、以下に規定するとおりとなります。

お客様は、移動を伴う現場でのインシデント調査には少なくとも 3 サービスデイを要することを認識し、これに同意するものとします。お客様が当初の要請より長い期間を要すると判断した場合、お客様は、サービスデイの追加を要請できます。シマンテックは、お客様から要請を受けた後、お客様に対し、対応する WAF を提供します。お客様は、当該 WAF に記名押印または署名したうえで、シマンテックに返却しなければなりません。疑念を回避するために言及すると、お客様が要請した当該サービスデイの追加は、まずお客様の利用可能なサービスデイから差し引かれますが、お客様が利用可能なサービスデイをお持ちでない場合は、お客様が要請する当該追加分のサービスデイを購入することとなります。

インシデント調査の特徴 シマンテックは、常にお客様のセキュリティインシデント、シマンテックが本サービスを提供するためのロジスティクス、およびお客様が利用可能かつ必要とするサービスデイの数を前提として、シマンテックがお客様から要請されたサービスデイに基づき当該活動を合理的に完了できる範囲において、お客様のプロジェクトマネージャとの調整に従い、以下に規定する一定の活動を実施するものとします。

情報収集およびプロジェクト調整:

- お客様と連携し、お客様のプロジェクトマネージャーを含めた、お客様のインシデントレスポンスチームに必要とされる人材を特定します。
- お客様のネットワーク図を検討し、既存のネットワークインフラストラクチャの設計を判定します。
- お客様の担当代表者およびお客様が指定した以下の責任者と現地面談を行います。
  - サーバー、クライアント、および遠隔システムの管理責任者（接続性と管理プロセスを判定するため）
  - インターネットゲートウェイセキュリティ責任者（情報セキュリティの保護、監視および緩和を提供するソリューションの利用可能性を判定するため）
  - 電子メールセキュリティ責任者（情報セキュリティの保護、監視および緩和を提供するソリューションの利用可能性を判定するため）、また、エンドポイントセキュリティソリューションの管理者（監視可能性を判定するため）
- 講じた措置および発見事項の取り扱いを書面化する手続きを確立します。
- お客様のプロジェクトマネージャーと調整し、必要な人材のスケジューリングと会議日程を設定します。

検出、データ収集および解析:

危殆化したお客様の情報システム資産について、以下の作業を含む評価を行います。

- 悪意のある活動の監視
- ネットワークパケットの捕捉と解析
- ログ収集および解析
- ライブシステムのアーチファクト収集
- 物理システムメモリ解析
- ディスク解析
- マルウェアサンプル収集
- 高度マルウェア解析（リバースエンジニアリングサービス）
- 収集した結果や危殆の兆候と、シマンテックのアナリストやシマンテックグローバルインテリジェンスネットワーク（GIN）との相互参照による、宣伝活動や悪意のある者との関連性の特定
- データ抽出技術の特定
- シマンテックが必要とみなすその他の解析

マルウェアアウトブレイク:

お客様がご利用中のシマンテック製品に応じて、シマンテックは以下を提供することもできます。

- 次の製品および製品間の危殆の兆候を分析ならびに比較：Symantec Endpoint Protection Manager、Symantec Data Loss Prevention、Symantec Critical Systems Protection、および Symantec Management Platform

- お客様への脅威の封じ込め・根絶推奨のために、アンチマルウェア保護機能から得られるログを検証し、現在の脅威情報を特定
- Symantec Endpoint Protection Manager 内でのポリシーおよび設定の調査
  - ウイルス対策およびスパイウェア対策の設定オプション
  - ウイルス事象の検出、スキャン、回復、および緩和設定
  - Advance Threat Detection Configuration
  - Application & Device の制御
  - ネットワーク脅威防御ファイアウォール
  - 侵入防止システム（IPS）設定オプション - ネットワークおよびブラウザ
  - Network Access Controlホストインテグリティ検査および救済措置のコンフィギュレーションオプション
  - 実行コンポーネントを使用したネットワークデバイスおよびネットワークサービスのNetwork Access Control統合設定（該当する場合）
  - Client Content Update （ライブアップデート）の設定
- シマンテックが必要とみなすその他の解析

封じ込め：

危殆化した情報システム資産の調査・解析を行い、以下の事項を支援するため、脅威の解析報告と短期的封じ込め計画を書面にて提供します。

- 悪質な活動の監視および/または停止
- 影響を受けたリソースの隔離
- 封じ込め計画実施に関する助言

根絶および復旧：

危殆化した情報システム資産の調査・解析を行い、脅威の根絶および復旧への戦略および推奨策を書面にて提供します。

遠隔サービス：

シマンテックは、ハードウェア、ソフトウェア、画像、メモリ、ネットワーク、ログ、その他のお客様のデータ（「**お客様データ**」）について、インシデント調査の間、一定の遠隔サービス（「**遠隔サービス**」）を行うことができるものとします。お客様は、シマンテックが行うかかる遠隔サービスには、次の条件が適用されるものとします。（a）お客様データの遠隔サービスは、インシデントレスポンス対応チームを通じてお客様が計画します。（b）お客様は、シマンテックに対するお客様データの（シマンテックと合意した媒体による）提供および遠隔調査終了後の当該お客様データのお客様への返却について、単独の費用負担のもとで全責任を負います。（c）お客様データは、お客様とインシデントレスポンス対応チームが合意した場所に、開封の有無が確認できる状態でシマンテックに提供されるものとする（該当する場合）。お客様は、シマンテックに送付物の配送追跡番号を提供し、配送に際しシマンテックの現物受領確認を必ず要求するものとします。遠隔サービスにおいて、「**シマンテック受領確認**」は、シマンテックによるお客様データの受領日とし、（d）シマンテックが行うすべての遠隔サービスは、通常の業務時間内においてのみ行うものとし、（e）シマンテックは、お客様のハードウェア内に記録されているお客様データ（アクセス可能か否か、読み込み可能か否かを問わない）に関して一切責任を負わないものとします。

高度マルウェア解析およびリバースエンジニアリング：

リバースマルウェア解析は、遠隔サービスの特殊なタイプとなります。お客様から提出されたマルウェアの高度解析は、静的、動的双方のマルウェア解析技術が含まれます。静的解析は、提出されたファイルの異なるリソースの解析および各コンポーネントの研究を含みます。どんなプログラムが実行しているのか理解するため、ファイルは逆アセンブラを使用して逆アセンブル（リバースエンジニアリング）されることもあります。ダイナミックマルウェア解析を行うこともあります。これは仮想マシンおよび/またはサンドボックス環境のいずれかを使用してエミュレートされたホストで実行され、これにより、シマンテックは、マルウェアの命令が CPU により処理され、ファイルシステムおよびメモリに影響を与え

る動作を逐一監視できます。マルウェア解析は、提出されたマルウェアサンプルの特質および動作、お客さまの環境に対する潜在的影響ならびに現在の感染を改善、ならびにさらなる感染または伝染から防御するために推奨される防御措置を詳細に記した書面報告書をもって終了します。

報告書およびプレゼンテーション:

シマンテックは、すべての活動の完了後、以下の各種項目を含む文書一式を交付します。

- **概要**
  - 背景
  - 初期所見
  - 初期攻撃事情説明
  - 危殆の範囲
  - 悪質なコード
  - 関連のハイプロファイルシステム
  - 封じ込め戦略
  - 提案の要旨
- **結論**
- **詳細な知見**
  - 技術的知見
  - 攻撃のタイムライン
  - 攻撃の分類区分
  - 判明したベクター
  - 判明した脅威の解析
- **提案**
  - インシデント固有の修復/緩和措置
  - 一般的提案
- **解析に使用したツールの一覧**
- **解析したシステムの一覧**

さらに、シマンテックは、要請に応じて、お客様が取締役会または社内管理部への状況説明に利用することを想定した、上記の報告書の内容を要約した提案書を提供します。

レディネス（事前準備）サービス

10 サービスデイ以上を購入したお客様は、該当期間中、当該年度期間に割り当てられた 5 サービスデイ以上を以下のレディネスサービスに交換できます。

レディネスサービスの提供は、シマンテック人材供給能力に依存します。レディネスサービスは、予定の 30 日以上前に、お客様とインシデントレスポンス対応チームでスケジュールを策定する必要があります。その後、シマンテックは、お客様に対し、レディネスサービスについて記載した対応する 作業承認書（WAF）を提出するものとし、お客様は、当該 WAF に記名押印または署名してシマンテックに返却する必要があります。サービスデイをレディネスサービスに交換する場合、各レディネスサービスのために必要とされるサービスデイの総数は、シマンテックの見積もりにより上下しますが、最低でも 5 サービスデイを必要とします。サービスデイを分割することは認められず、お客様に対するクレジット付与はありません。サービスレベル契約は、レディネスサービスには適用されません。

- **インシデントレスポンスレディネス評価** シマンテックは、オンサイトのワークショップを実施し、セキュリティインシデント検出時のお客様の対応能力を評価し、セキュリティインシデント時のお客様の役割および責任に関する現時点での定義を把握します。インシデントレスポンスレディネス評価は、シマンテックに対し、お客様特有の環境に基

づくインシデント調査を提供するのに役立つ重要な知見を提供し、シマンテックのインシデント調査中の対応時間と効率性を向上させるアドバイスをお客様に提供します。

- **インシデントレスポンス計画評価** インシデントレスポンス計画評価は、お客様の情報セキュリティインシデントレスポンス計画の徹底的な評価を含みます。シマンテックは、お客様と協力し、戦略的、運用上、および戦術的見地から、現在および将来のニーズを判断し、インシデントレスポンス計画が現在の運用状況を検査します。このアプローチにより、シマンテックは、お客様のインシデントレスポンス計画の全体的な検討を提供することを可能にします。お客様のインシデントレスポンスチーム、その他の社内および第三者間の連携関係も、それらの取り決めの有効性と効率性を判断するためにレビューされます。インシデントレスポンス計画評価は、通常 3 、4 週間にわたる一連のアンケート、ワークショップ、および面談と、3 、4 日間の現地調査を用いて実施されます。シマンテックは、現地訪問の最後に提示した提案措置とともに、評価スナップショットを提供します。

- **インシデントレスポンス計画策定** インシデントレスポンス計画は、セキュリティインシデントによる影響を最小限に抑え、インシデントの特定から解決までの期間を短縮するのに役立ちます。このため、インシデントレスポンス計画は、過去のインシデントの教訓を活かした継続的な改善プロセスを発展させ、セキュリティの有効性を全体として改善します。インシデントレスポンス計画は、セキュリティインシデントからの適時の復旧に欠かせない、過程と手続き、様々な関係者の役割と責任、コミュニケーションフロー、ならびに通知手順を書面化するものです。シマンテックは、お客様の組織的ニーズおよび固有の要件に合わせたインシデントレスポンス計画を作成するため、業界のベストプラクティスとともに、世界中のインシデントに対応した経験を活用します。

- **インシデントレスポンス机上訓練** シマンテックは、お客様の既存のインシデントレスポンス計画またはプロセスを検査および改善するため、机上演習（「**TTX**」（Tabletop Exercise））を用います。TTX は、実際にお客様の設備や人材を配置することなく、会議室において実施され、お客様の主要関係者がインシデントレスポンス計画またはプロセス、および特定のインシデントへの対応について話し合います。TTX の期間中、インシデントレスポンス計画またはプロセスにおけるギャップと弱点が判明する可能性があります。TTX の後、TTXを通じて明らかになったことインシデントレスポンスプロセスを改善するための計画についてブリーフィングが行われます。

- **インシデントレスポンストレーニング** シマンテックは、お客様のニーズを精査した上でインシデントレスポンストレーニングを開発し、セキュリティインシデントの当初の特定および封じ込めにおいてお客様を支援するインシデントレスポンストレーニングを提供します。インシデントレスポンストレーニングは、お客様の具体的な要請、社内のチーム構成、および具体的なセキュリティインシデントレスポンス対処要件に合わせて実施されます。インシデントレスポンストレーニングのテーマは、セキュリティ意識の向上、最新のセキュリティ動向、データ処理、揮発性データ収集またはその他の関連領域に及ぶことがあります。

- **高度脅威探索** シマンテックは、お客様の環境において以前発見されなかった障害（障害査定）および脅威活動の存在を発見するため、お客様のネットワークを捜索します（「**高度脅威探索**」）。シマンテックは、独自の探索法およびテクノロジーを使用してネットワークを捜索し、未発見のマルウェアから本格的な高度で永続的な脅威の活動に至るまで、潜在的脅威の存在を特定します。高度脅威探索は、シマンテック グローバルインテリジェンスネットワークの指標を含むシマンテックの膨大な情報リソース、ならびにシマンテックのアナリストの調査結果を使用します。シマンテックは、実施期間中に、まだ発見されていない潜在的な障害についてのより良い理解をお客様に対し提供すると共に、封じ込めおよび根絶のための提案を提供します。

旅費および滞在費用（T&E）

年間サブスクリプション料金には、旅費および滞在費用（「**T&E**」）は含まれませんが、本サービスの提供のために必要となることがあります。お客様は、該当する場合、サービスの履行過程で生じる妥当な T&E をシマンテックに支払います。T&E は、各 3 サービスデイごとに人員 1 人あたり **5,000 米ドル**（または米国外で発生した費用の場合、これに相当する現地通貨の金額）まで、または、大陸間移動を含む場合は **10,000 米ドル**まで、お客様の事前の承認を要しないも

のとします。シマンテックは、上記 T&E 該当額の払い戻しを受けるには、事前にお客様から書面による承認を得る必要があるものとします。シマンテックは、すべての T&E について、シマンテックの標準的業務慣行に従い、実費により請求書を発行するものとします。

お客様の責任

お客様は、本契約に従い、またはシマンテックの合理的な要請に従い、お客様が必要な情報を提供、または必要な行為を行った場合にのみ、シマンテックが該当する本サービスを実施することができることを認識し、これに同意します。お客様が以下のお客様の責任に関する規定を遵守しない場合、何らの制限なしに、以下に記述するように、シマンテックによる本サービスの提供が遅延し、損なわれ、または中断されることがあります。

- **プロジェクトマネージャー** お客様は、シマンテックがお客様の人材に適時に連絡・調整できるよう、本サービスに関連する問題の解決に関する取りまとめ役として「プロジェクトマネージャー」を指名します。お客様のプロジェクトマネージャーは、本サービスに関する意思決定を行うために必要な技術上および業務上の知識と権限を保有するものとします。さらに、お客様は、本サービス規定で定めた本サービスに従い、シマンテックを支援し協力する、適切な人数の熟練した適切な人材を配置するものとします。お客様は、要求された人材に関するエスカレーション情報/連絡先情報を提供するものとします。お客様は、そのインシデントレスポンス要員を特定し、その氏名をシマンテックに提供しなければなりません。

- **施設** お客様は、シマンテックの要請に応じて、シマンテックが本サービスの履行のために合理的に要求する、必要なすべての協力、情報、および支援を提供するものとします。これには、適切な渡航書類（就労許可、ビザ等）の手配および/もしくは取得、適切に設定されたコンピュータへのアクセス、無制限のネットワークの物理的接続性、ネットワーク監視ハードウェア、ソフトウェア製品、および適用されるパスワードのインストールに関する技術サポート要員の提供が含まれますが、これらに限定されません。さらに、お客様は、シマンテックの職員に対し、すべての建物、電話システム、インターネットアクセス、サーバー室、ワークステーションへの立ち入りと利用を許可するとともに、通常業務時間外における作業をお客様が求めた場合、当該領域へのアクセスに必要なすべての通行許可を提供するものとします。また、お客様は、サービスにかかる現地作業の間、会議、面接、および指導セッション用に適切な会議室施設への立ち入りを許可し、該当する場合、ネットワーク監視ハードウェアを設置するための技術サポート要員を提供するものとします。

- **情報** お客様は、シマンテックが常時（i）お客様の業務上および技術上の環境に関連する資料および人員、（ii）本サービスの提供に必要なソフトウェア設計文書、現在の設計図表、およびその他の情報、ならびに（iii）本サービスの完遂に必要なすべてのオペレーティングシステム、ネットワーク、およびコンピュータ環境にアクセスできるよう確保するものとします。当該アクセスには、必要に応じて、適宜、たとえば侵入評価を実施するための、関連アプリケーションに関するさまざまなユーザーアカウント（関連 IP アドレス、URL およびユーザー認証を含む）へのアクセスを含みます。

サービス固有の規定

サービス条件

- **サービス範囲に含まれないもの** 本サービス規定に明示的に記載のない事項は、範囲外であり、本サービスに含まれません。お客様は、本サービス、または本サービスの結果としてシマンテックが作成した提案および計画が、お客様のすべてのシステム上の脅威、脆弱性、マルウェア、悪意あるソフトウェア、もしくはその他の悪意のある脅威を特定、発見、封じ込め、もしくは根絶すること、またはそれらの脅威から復旧する結果をもたらすことを何ら確約または保証しないことを認め、了解し、承認するものとします。お客様は、シマンテックがかかる確約または保証をしているような表示を他者に対し表明しないことに同意するものとします。

- **サービスデイの失効** 本サービスおよびサービスデイは、本契約期間中に使用および提供されない場合、すべて失効するものとし、失効したまたは未使用の部分に関するお客様に対するクレジットの付与または返金は行いません。

- **オフサイト解析** お客様は、シマンテックに対し、本サービスに必要なお客様データのオフサイト解析を実施する権限を付与するものとします。したがって、お客様は、シマンテックが、コンピュータおよび設備をお客様のコンピュータネットワークに直接接続する必要が生じる場合があることを認識し、これに同意するものとします。お客様は、シマンテックがコンピュータおよび設備をお客様のコンピュータネットワークに直接接続することに明確に同意し、これに関する一切のリスクおよび責任を引き受けるものとし、シマンテックは、いかなる責任も負わないものとします。
- **サービス提供時間** お客様が365 日 24 時間の支援要請のアクセス（本サービスの特徴に記載）を有する場合を除き、すべての本サービスは、通常営業時間内に提供されます。ただし、インシデント調査は緊急ベースで提供され、またサービス提供時間に関する柔軟性が要請され、調整される必要があること認識しているため、本地域の該当する労働基準法を遵守すること、およびインシデント調査を提供する個々の人員が自由に選択できることを条件として、本サービスの提供を行うものとします。
- **除外次項** 以下に定めるサービス（「**訴訟サポートサービス**」）は、本サービスから明示的に除外されます。
    - 宣誓証言、事実証人証言、専門家・鑑定人証言、宣誓供述、宣言、供述、専門家の報告
    - 証拠開示手続（Discovery）申請、召喚状への対応
    - 電子証拠開示手続（eDiscovery）サービス
    - 主題に関連するその他の形式の訴訟サポート、訴訟手続への参加等のあらゆる法的手続に関係するもの（政府機関に関するものを含む）

訴訟サポートサービス　両当事者は、お客様が自身の弁護人の指示に基づき本サービスを求めることがある場合を認識しているものの、シマンテックが訴訟サポートサービスを実施することは、シマンテックまたはお客様の意図ではありません。ただし、シマンテックがその後訴訟サポートサービスを実施することを余儀なくされた場合、お客様とシマンテックは、当該訴訟サポートサービスが直接お客様または第三者によって求められたか否か、およびその他の条件に抵触するか否かにかかわらず、当該訴訟サポートサービスに対して、以下の規定が適用されることに同意するものとします。

- その時点で最新の時間単価が、訴訟サポートサービスを実施するすべてのシマンテック人員に対して適用されます。訴訟支援サービスの遂行に要する実時間は変動することがあるため、訴訟サポートサービスは、時間および費用ベースで提供されます。
- 両当事者は、訴訟サポートサービスの必要が生じた場合、本訴訟サポートサービス規定に定めた条件、および必要な追加的条件を、個別の契約書に誠実に書面化するものとします。
- 本訴訟サポートサービスの規定は、本契約の期間満了後または解除後にも存続するものとします。

秘匿特権　お客様が、必須連絡先情報フォームに法務責任者(General Counsel)の連絡先情報を記載したか、またはお客様の法務責任者の要請および指示により実施されることを確認する別途契約を締結した場合、シマンテックは、弁護士秘匿特権、弁護士の職務活動の成果物またはその他の該当する特権を合理的な範囲で保護します（本サービスが提供される国内法令で許容される範囲内に限ります）。シマンテックは、本サービスの過程でお客様に提供するあらゆる調査結果、報告書および文書について秘密情報として扱います。

補償　お客様は、過失の有無にかかわらず、お客様がシマンテックに本サービスの提供を依頼したインシデントに起因する申立、主張、請求、要求、令状またはその他の法的手続（政府機関が関連するものを含みます）に関連して発生するすべての損失、損害、責任、経費、費用および料金（合理的な範囲内での弁護士費用を含みます）ならびにシマンテック人員の時間料金（上述の訴訟サポートサービスに関する時間レートに基づきます）につき、シマンテックに完全に補償し、シマンテックを免責するものとします。

- **報告** お客様は、シマンテックが、本サービスを提供する過程において、データ侵害、ネットワーク侵入またはマルウェアの存在に気付くことがあること、ならびに当該問題によって、お客様が営業を行う 1つまたは複数の地域において、お客様が適用を受ける規制上の報告義務が生じることがあることを認め、これに同意します。したがって、お客

様は、かかるすべての報告要求について引き続き全責任を負い、シマンテックは、この点について一切責任を負わないものとします。

- **人員** シマンテックは、本サービスの提供に提供可能な熟練した適切な人材を配置する権利を保有します。シマンテックには、特定のシマンテック人員または第三者人員を提供する義務はありません。
- **アクセス権** お客様は、無線アクセスポイントへの未承認の侵入は、適用法令上禁止されることがあることを認識し、理解し、これに同意するものとします。お客様は、本契約に同意することにより、（i）シマンテックに対し、シマンテックが本サービスを提供するために該当するすべての同意および承認を受けた旨を明示的に確認し、（ii）シマンテックに対し本サービスを履行し、本サービスに関連するすべてのデータを利用および処理するための許可を付与し（承認されていない悪意あるコード（マルウェア）を含む既知の悪意ある通信パターンおよびトラフィックの証拠を検知するためにネットワークトラフィックをリアルタイムで解析すること、お客様のコンピュータネットワークに接続すること、本サービスの一環としてキャプチャーしたすべてのネットワークトラフィックをアーカイブ化し保管すること（お客様またはお客様のためもしくは客様とともに作業している他者がマルウェアおよびメタデータを保管することを含む）の同意を含みますが、これらに限定されません）、（iii）シマンテックによるかかるアクセスおよび処理が適用法令またはお客様が第三者に対し負担するその他の義務に違反しない旨を表明し、ならびに（iv）当該本サービスの執行に関する独自の責任と義務を承認するものとします。したがって、お客様は、自身がシマンテックが本サービスを履行する基礎をなすネットワーク、システム、IP アドレス、ソフトウェア、電子機器、コード、テンプレート、ツール、ポリシー、記録、作業文書、データおよび/またはコンピュータ（「**お客様システム**」）の所有者またはライセンシーであること、ならびに自身がシマンテックに対しお客様システム上で本サービスを提供することを指示する権限を有していることを表明および保証するものとします。お客様は、本サービスに関連して第三者から提起されるすべての訴えから、シマンテックを十分に保護し、シマンテックに損害が及ばないようにするものとします。
- **サービスの制限** 本サービスが履行される国の適用法令または規則により、本サービス（インシデント調査を含みますが、これに限定されません）の範囲が制限または変更されることがあります。

サービスレベル契約(SLA)

- サービスクレジットは、該当する本サービスの年間サブスクリプション料金の 2.5 パーセントに相当する金額となります。本サービス規定に基づいて付与される各サービスクレジットは、お客様によるサービスクレジットリクエストの提出後、該当するサービスの支払いに関するお客様の次回請求書に充当されるものとし、当該サービスの支払いに関する追加請求書がない場合は、支払いが行われるものとします。本サービス規定に矛盾する規定があったとしても、いかなる場合においても、シマンテックは、お客様が影響を受けた本サービスに関して支払うべき年間サブスクリプション料金の暦月当たり金額の 7.5 パーセントを超えてお客様に対しクレジットを付与することを義務付けられず、サービスクレジットを発行する期間中の年間累積最高限度額は、年間サブスクリプション料金の金額を超えないものとします。サービスレベル契約に定める、サービスクレジットの発行は、本サービスに関するシマンテックの唯一かつ排他的な義務であり、また、お客様の唯一かつ排他的な救済手段となります。
- 契約期間の同時終了のため 1 年未満の期間で提供されるカスタムリテーナーオプションまたは追加サービスデイに関し、カスタムリテーナーオプションの購入に支払われた費用は、サービスクレジットの対象となる範囲で、年間サブスクリプション料金が比例按分により計算されます。
- お客様がサービスレベル契約に基づいて救済を受ける権利があると判断する場合、お客様はサービスレベル契約違反の疑いが発生した月の最終日から10 通常営業日以内に、サービスクレジットリクエストを提出する必要があります。
- サービスクレジットリクエストは、すべて、シマンテックによる審査、確認が必要となります。
- シマンテックは、以下の場合、本サービス（サービスレベル契約の履行を含みます）のすべてまたは一部を履行できないことにつき責任を負いません。（i）戦争、ストライキ、暴動、犯罪、天災またはリソース不足を含む、シマンテックの合理的支配の及ばない予測できない状況または原因による場合、（ii）法律、規則または命令等の司法を含む法令により禁止される場合、（iii）本契約の条件に従いシマンテックが本サービスを停止する期間、（iv）お客様が

本契約に違反する場合（お客様が支払遅延に陥っている場合を含みますがそれに限りません）、または（v）シマンテック人員がお客様の国における作業の前に査証を取得する必要がある場合。

- サービスレベル契約に規定する救済手段は、サービスレベル契約に関する、契約上、不法行為上（過失を含みますが、これに限定されません）、その他の原因に基づく、お客様の唯一かつ排他的な救済手段となります。

定義

本サービス規定で使用される用語は、以下の意味を持ちます。本サービス規定で使用されているものの、定義されていない用語については、サブスクリプション文書における意味と同じ意味をもちます。

「年間サブスクリプション料金」とは、お客様がそのサブスクリプション文書で申し込んだ本サービスの対価として支払う年間料金を意味します。

「インシデント調査」とは、本サービス規定にさらに記載のあるとおり、特定のセキュリティインシデントの性質およびタイプに基づきシマンテックが行うインシデント調査を意味します。

「通常営業日」とは、通常営業時間からなる日を意味します。

「通常営業時間」とは、一般的に現地時間午前 9 時から午後 5 時 30 分まで（ただし、本サービスが履行される国において順守される、適用される法令上の休憩時間、土日および祝祭日を除きます）の通常の就業時間を意味します。

「遠隔評価」とは、本サービス規定にさらに記載のあるとおり、インシデント調査の間シマンテックが遠隔で行う評価を意味します。

「本地域」とは、以下のいずれかを意味するものとします。場合に応じ、（i）南北アメリカ大陸、（ii）ヨーロッパ・中東・アフリカ、（iii）アジア・太平洋、または（iv）日本

「サービスクレジット」とは、サービスクレジットリクエストが行われ、お客様にクレジットを支払うべきであるとシマンテックが審査、確認した後、お客様に返金またはお客様の次回請求書で相殺される金額を意味します。

「サービスクレジットリクエスト」とは、お客様がシマンテックに対して、お客様のサービスマネージャ宛ての電子メールにより提出する必要がある通知を意味します。

「サービスデイ」とは、シマンテック人員 1 名による、1 通常営業日を意味します。

「SLA」または**「サービスレベル契約」**とは、本サービス規定に規定された該当サービスレベルを意味します。

「サブスクリプション文書」とは、本サービスに関連するお客様の権利と義務をより詳細に定義する文書で、シマンテックの証明書またはシマンテックが発行した同等の文書、あるいは本サービスに付属、先行、追随するお客様とシマンテック間の書面による合意のうち、該当する 1 つ以上の文書を意味するものとします。

「シマンテック」とは、以下を意味するものとします。（i）**アメリカ**（ここでいう「アメリカ」とは、北、中央または南アメリカあるいはカリブ海にあるすべての国を意味します）でシマンテックが提供する本サービスについては、350 Ellis Street, Mountain View, CA 94043, USA に営業所を有する **Symantec Corporation**、（ii）**アジア太平洋**（ここでいう「アジア・太平洋」とは、オーストラリアおよびニュージーランドまたはアジア大陸にある国（カザフスタン、キルギスタン、ロシア、トルクメニスタン、ウズベキスタン、中東および日本を除く）を含めて太平洋諸島地域を意味します）でシマンテックが提供する本サービスについては、6 Temasek Boulevard, #11-01 Suntec Tower 4, Singapore 038986 に営業所を有する **Symantec Asia Pacific Pte Limited**、（iii）**日本**でシマンテックが提供する本サービスについては、〒107-0052　東京都港区赤坂1－11－44　赤坂インターシティに営業所を有する株式会社シマンテック、（iv）**ヨーロッパ・中東・アフリカ**（ここでいう「ヨーロッパ・中東・アフリカ」とは、アメリカおよびアジア・太平洋・日本以外にある世界の国を意味します）でシマンテックが提供する本サービスについては、Ballycoolin Business Park, Blanchardstown, Dublin 15, Ireland に営業所を有する **Symantec Limited**。

「期間」とは、該当するサブスクリプション文書に規定されたサービスのサブスクリプション期間を意味します。

「WAF」または**「作業承認書」**とは、シマンテックがお客様に対し提供する文書であって、それによりお客様がインシデント調査に関する場所、連絡先情報、T&E、追加のレスポンス要員、レディネスサービスおよび/またはサービスデイを承認、確認する文書等を意味します。

以上、サービス規定