



CLOUD NATIVE SECURITY

本製品規約は、お客様と Rackspace との契約における他のあらゆる定めに加えて、お客様が Cloud Native Security Service Block を購入した際に適用されるものとします。

1. 追加定義規定

「アドオンサービス」は、本製品規約において定義されるとおりとします。

「AWS カスタマー契約」は、本製品規約において定義されるとおりとします。

「AWS パブリックセクターポリシー」は、本製品規約において定義されるとおりとします。

「AWS リージョン」とは、AWSが定義し、以下のURL（又は将来 Amazon が指定する後継の URL）にてご覧になれる地理的なリージョンを意味します：<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>。

「AWS サービス」は、本製品規約において定義されるとおりとします。

「CNS ツール」とは、AWS Security Hub、Amazon GuardDuty、及び IAM Access Analyzer、又は Rackspace が独自の裁量で決定する同等のツールを意味します。

「対象環境」とは、本サービスがサポートするリージョンにおいて Rackspace が提供する製品アカウントのセットで、導入プロセス中に文書化され、又はその後更新されたものを意味します。

「イベント」とは、最低レベル以上の緊急度がタグ付けされ、SIEM 及びその他の事前定義された関連ルールによって処理された、1つ以上の関連性のある検出を意味します。

「イベント手数料」とは、既定の請求サイクル内で処理されたイベントの総数に、お客様の適用されるサービスオーダーで特定される処理されたイベントごとのコストを乗じたものを意味します。

「イベント識別」とは、対象環境において識別された後、Rackspace SIEM を通じてイベントが完全に処理された時点の意味します。

「検出」とは、CNS ツールによって生成された、お客様の対象環境に関連する1つ以上のセキュリティ上の所見を意味します。

「GuardDuty」とは、現在以下の URL（Amazon ウェブサービスにより更新されることがあります）にて確認できる Amazon ウェブサービスの脅威検知サービスを意味します：<https://aws.amazon.com/guardduty/>。

「IAM Access Analyzer」とは、以下の URL（Amazon ウェブサービスにより更新されることがあります）にて確認できる Amazon ウェブサービスの ID 及びアクセス解析サービスを意味します：<https://aws.amazon.com/iam/features/analyze-access/>。



「最低緊急度レベル」とは、それ以下では Rackspace による監視、分析、及び検出に対する対応から除外される、特定の緊急度レベルを意味します。

「本製品規約」とは、Rackspace Optimizer+ の製品規約（現在は以下の URL にてご覧になれます：<https://www.rackspace.com/information/legal/optimizer>）を意味し、Rackspace によって更新されることがあります。

「製品アカウント」とは、本サービスの対象となる AWS アカウント、Azure サブスクリプション、及び／又は Google Cloud Platform プロジェクト（該当する場合）を意味します。

「リージョン」とは、AWS リージョン（該当する場合）を意味します。

「Runbook」とは、イベントを処理する際に Rackspace が従うべき、条件付けられた一連の手順、措置、及び情報を文書化したものを意味します。

「Security Hub」とは、現在以下の URL（Amazon ウェブサービスにより更新されることがあります）にて確認できる Amazon ウェブサービスのアラート集約及び自動化サービスを意味します：
<https://aws.amazon.com/security-hub/>。

「緊急度レベル」とは、「検出」に割り当てられたセキュリティ評価で、標準的な5つのカテゴリー（重要度の高いものから、重要・高・中・低・情報）のうちの1つに規格化されたものを意味します。

「SIEM」とは、Rackspace のセキュリティ専門家がお客様の対象環境を監視するために使用する、セキュリティ上の出来事及び事象の管理システムを意味します。

「サードパーティクラウド」とは、Amazon AWS、Microsoft Azure、及び／又は Google Cloud Platform（該当する場合）を意味します。

2. 本サービス

2.1. セットアップ、オンボーディング、継続的管理 Rackspace は、対象環境における CNS ツールの導入、設定、及び継続的な管理を行うものとします。CNS ツールは、相互に機能的に動作し、かつ、SIEM に情報を提供するように設定されます。

2.2. Runbook Rackspace とお客様は、対象環境に関する情報、既知の IP ホワイトリスト又は IP 脅威、Rackspace が実行可能な改善措置、及び Rackspace がお客様に連絡をしようとする際のエスカレーションパスを含む、お客様固有の Runbook を共同で作成するものとします。お客様は、Runbook を作成しないことを選択することもでき（ただし、推奨はしません）、その場合、イベントに対して実行される全ての措置について、実行者はその実行前にお客様と共に検証をしなければなりません。

2.3. 監視、調査、改善 Rackspace のセキュリティ専門家は1日24時間、週7日、年間を通じて SIEM をモニタリングし、Rackspace はお客様の Runbook 及び第5.2条（該当する場合）に従って分析及び対処を行います。

3. AWS ライセンス お客様が Cloud Native Security を利用するためには、最低限、Fanatical Support for AWS Aviator / Navigator、Platform Essentials、又は Optimizer+ をご購入いただく必要があります。お客様による CNS ツールの利用は、AWS カスタマー契約に従うものとし、この契約は署名なくして有効であるものとします。お客様がパブリックセクターのお客様である場合、当該お客様による CNS ツールの利用は、AWS パブリックセクター・アクセスポリシーに従うものとし、このポリシーは署名なくして有効であるものとしま



す。お客様は、AWS サービス、AWS による AWS サービスの提供、管理、又は運用、及び AWS カスタマー契約もしくはパブリックセクター・アクセスポリシーにおける、又はお客様によるこれらへの違反に対する AWS の権利行使に起因又は関連する一切の責任から Rackspace を免責するものとします。CNS ツール及びその他の AWS サービスのライセンス及び再販売については、AWS カスタマー契約に従うものとします。

4. 最低緊急度レベル Security Hub で処理される全ての「検出」には、緊急度が設定されます。特定の最低緊急度レベル未満の緊急度の検出は、SIEM に送信されず、したがって Rackspace のイベント識別プロセス、モニタリング、及び対応から除外されます。最低緊急度レベルは、お客様が選択した本サービスの料金の計算方法によって異なります。

4.1. インフラストラクチャのパーセンテージベースの場合 お客様の料金が、基礎となる製品アカウントのインフラストラクチャ及び AWS マーケットプレイスの支出に対する割合として算出される場合、最低緊急度レベルは Rackspace が独占的に決定し、Rackspace だけがその合理的裁量をもってこれを変更できるものとします。

4.2. イベント単位ベースの場合 お客様の料金がイベント単位で算出される場合、お客様は、対象環境の最低緊急度レベルを定義づけることができます。お客様が選択した最低緊急度レベルは、最初に、適用されるサービスオーダーで特定されます。お客様は、Rackspace にチケットリクエストを提出することにより、最低緊急度レベルをより限定的なものに変更し、SIEM に送信される検出の数を制限することができます。お客様は、チケットリクエストにより最低緊急度レベルをより包括的なものにし、SIEM に送信される検出の数を増やすよう要求することもでき、Rackspace の明示的な同意によりかかる変更が行われます。お客様による最低緊急度レベルの変更要求は、Rackspace による承認後、最大14暦日後に有効となります。

5. サービス水準合意 (SLA)

5.1. 通知と更新 対象環境においてイベントが特定され、Rackspace SIEM で処理されると、Rackspace は、該当する緊急度レベル (Rackspace の合理的な裁量に基づき変更される場合があります) に基づき、以下の時間枠内で初動分析を開始するものとします。お客様は、イベント識別の際に最初の通知を受け取ります。お客様は、Rackspace がその独自の裁量により必要であると判断した場合には、イベントの状況についてその後の更新情報を受け取ることができます。

| 緊急度 | 分析開始時間 |
|-----|-------------|
| 重要 | イベント識別から30分 |
| 高 | イベント識別から60分 |
| 中 | イベント識別から4時間 |

5.2. 修復 イベント識別後、特定されたリスク又は脆弱性を是正するために対象環境の変更が必要な場合、Rackspace は、かかるリスク又は脆弱性に対処するための推奨アクションを作成し、お客様に提供するものとします。お客様が特定のアドオンサービスを購入した場合、特定されたリスク又は脆弱性を有する製品アカウントについて、Rackspace は、お客様の書面による承認を得て、又は許可されている場合は Runbook に従って、かかるリスク又は脆弱性に対処するための推奨措置に従って、これらの対象製品アカウントを修正することができます。修復のための適用されるアドオンサービスには、Manage & Operate 及び Aviator のサービスレベルである Fanatical Support for AWS が含まれます。明確化のために明記すると、お客様は、適用されるアドオンサービスの対象とならない製品アカウントに対する是正措置については単独で責任を負うものとします。お客様は、本条に従って行われるいかなる変更も、侵害者の排除又は侵害によるお客様の対象環境への損害の防止に有効でない場合があることを、認めます。

5.3. 救済措置 Rackspace が第5.1条に記載された SLA に違反した場合、お客様は、影響を受ける製品アカウントに適用される月額料金の100%を上限として、イベントごとに5%のクレジットを受け取ることができます。お客様は、クレジットの原因となったイベントから14暦日以内に、Rackspace のアカウントを通して申請をするものとし、これをしなければクレジットは喪失します。Rackspace は、30暦日以内に、申請を承認するか拒否するか、又は詳細な情報を求めるかの回答をお客様に連絡するものとし、承認された場合、クレジットは承認後のお客様の次の月次請求書に適用されるものとし、

5.4. クレジット救済の例外 お客様は、Rackspace が制御することのできない事由に起因する SLA の不履行については、クレジットを受け取る権利を有しません。お客様は、クレジットの原因となった事象の発生時にお客様が本契約（Rackspace に対する支払義務を含みます）に違反している場合、クレジットを受け取る権利を有しません。お客様は、お客様による本契約への違反が無ければクレジットの原因となる事象が発生しなかったような場合には、クレジットを受け取る権利を有しません。第5.1条に記載された SLA は、お客様の対象環境にのみ適用され、お客様の製品アカウントのエンドユーザ又は他の Rackspace サービスには適用されません。

6. お客様への要求事項

6.1. クラウドインフラストラクチャ お客様は、Rackspace による GuardDuty 及び Security Hub の展開のために、検出の集約及び Rackspace SIEM との統合に使用する、単一かつ専用の製品アカウントを提供する必要があります。お客様は、製品アカウントと連動したサードパーティクラウドサービスの使用に関連する全ての費用を負担とするものとし、

6.2. Rackspace の構成要件 お客様は、Rackspace が本サービスを提供するために必要なアクセス、モニタリング、及び関連する機能と特徴を有効にするために合理的に必要な製品アカウントへの全ての変更を行う権利を有することに同意するものとし、Rackspace は、本サービスの実装及び設定をお客様と調整するものとし、お客様が Rackspace との調整をしない場合、Rackspace はその合理的な裁量に基づき、最低緊急度レベル及び対象環境のモニタリングからなる初期設定を行います。

6.3. 最低限の設定義務 お客様は、常に Security Hub を有効にしておく必要があります。ただし、お客様は、Rackspace に書面によるチケットリクエストを提出することにより、その他の CNS ツールを任意に無効にすることができ、Rackspace は、第7.1条に従って、これらの CNS ツールを無効にします。

6.4. 新規の製品アカウント CNS ツールは、新規の製品アカウントにおいて自動的に有効化又は設定されるものではありません。お客様は、Rackspace に対して、新規に作成された製品アカウントにおいて CNS ツールを有効化し、本サービスを提供するよう要求することにつき単独で責任を負います。お客様は、Rackspace に対して書面でチケットリクエストを提出することにより、いつでもその対象環境のサイズの増加を要求できます。Rackspace がお客様からの要求を確認したのに引き続いて、追加の地域又は追加の製品アカウントにおける本サービスの有効化及び設定のスケジュールが、両者の間で相互に合意されるものとし、お客様の対象環境のサイズの縮小は、本契約の該当する終了規定に従って行わなければなりません。

7. 免責及び制限

7.1. 最小デプロイ免責義務 お客様が CNS ツールを無効にした場合、Rackspace は、無効となった CNS ツールに本サービスが全部又は一部依存している限りは、本サービスの履行を免除され、無効となった CNS ツールを使用することにより検出又は防止されたかもしれないいかなる事象に起因す

る一切の責任を負わないものとします。

7.2. コンプライアンス免責事項 お客様は、法律及び規制上のコンプライアンス要件の遵守を支援するために本サービスを利用することができますが、一方で、本サービスがお客様の法律又は規制上のコンプライアンスのニーズを満たすことや、お客様のコンプライアンス要件を維持するために十分であることを、**Rackspace** が表明又は保証するものではないことを、認めるものとします。また、**Rackspace** は、本サービスが悪意のある攻撃によってもたらされる脅威を完全に軽減するのに十分であることや、又はそれが可能であることを、表明又は保証するものでもありません。お客様は、いかなるサービスも、インターネット接続に起因する機密性とセキュリティに対する固有のリスクを排除できないことを認めます。

7.3. 再販売の禁止 お客様は、本サービスを再販売してはなりません。ただし、お客様は、エンドユーザに対して対象環境のセキュリティについて表明することができますが、その表明は本契約において**Rackspace** が行ったものを超えないものとします。

7.4. 地域的な除外 **Rackspace** は、特定の地域において本サービスを提供できない場合があります。特定の地域における本サービスの利用可否についてのお問い合わせは、**Rackspace** のサポートまでご連絡ください。

8. 料金

8.1. セキュリティサービス お客様は、請求サイクルごとにお客様のサービス料金を決定するために、2つの料金体系から選択することができます。特に指定がない場合、自動的に第8.1条 (A) のオプションに登録されます。また、どちらの料金体系を選択したかにかかわらず、お客様にはセットアップ料金が請求されます。セットアップ料金は、お客様の適用されるサービスオーダーに記載されます。

(A). インフラストラクチャのパーセンテージベース デフォルトでは、本サービスの料金は、基礎となる製品アカウントのインフラストラクチャ及び **AWS** マーケットプレースの支出に対する割合から算出され、請求期間ごとにお客様に請求されます。適用されるパーセンテージは、お客様のサービスオーダーに記載されます。この料金体系は、全てのリージョンで利用できるとは限りません。

(B). イベント単位ベース あるいは、本サービスに対するお客様の料金が、イベントごとに算出される場合もあります。お客様が料金をイベント単位で支払うことを選択された場合、請求期間ごとに最低月額料金又はイベント料金のいずれかが請求されます。お客様は、最低月額料金が該当する請求サイクルのイベント料金を上回る場合のみ、請求を受けることとなります。最低月額料金及び処理されたイベントごとのコスト（イベント料金の算出に使われます）は、お客様の適用されるサービスオーダーに記載されます。

8.2. クラウドインフラストラクチャ CNS ツール及び本サービスを提供するために必要なサポートインストラクチャを含む、サードパーティクラウドサービスの追加料金は、サードパーティクラウドサービスに関するお客様の適用されるサービスオーダーに追加されるものとします。

9. 期間及び終了 本サービスの最初の有効期間は、適用されるサービスオーダーに定義されるとおりとし、お客様が署名した時点から開始されます。有効期間の終了後、本サービスは、以下の場合を除き、**90日**ずつ更新されます。(i) 本契約に別段の定めがある場合、(ii) 両当事者が更新期間に関する別途の契約を締結した場合、又は (iii) いずれかの当事者が期間満了の少なくとも**90日**前までに相手方に対し書面による解約通知を行った場合。