The bridge to possible

Cisco Secure Cloud Insights

1. 概要

1.1 目的、対象者および範囲

本書では、Cisco® Secure Cloud Insights の価格、パッケージ構造、発注プロセスについて説明します。

対象者：本ガイドは、シスコのセールスチーム、シスコ スペシャライゼーションを取得済みのチャネルパートナー、シスコのお客様を対象にしています。

範囲：この発注ガイドでは、Cisco Secure Cloud Insights の価格設定と発注方法について説明します。

Cisco Secure 製品の詳細については、https://www.cisco.com/c/ja_jp/products/security/secure-cloud-insights/index.html を参照してください。

1.2 発注および見積ツール

ソリューションエキスパートの支援を受けることで、シスコフィールドおよびシスコ（製品 / シリーズ）スペシャライゼーション取得済みチャネルパートナーは、Cisco Unified Communications バンドルまたは従来の設計モデルを使用したソリューションの設計および見積を行えます。

Cisco Commerce では、案件と見積のアプリケーションを利用できます。これにより、スペシャライゼーションを取得済みのチャネルパートナーは、以下を含むシステムの見積を作成できます。

- 製品、必須モジュール、ソフトウェア
- 製品と設置場所に基づく自動生成サービス
- Cisco Capital® のカスタマイズ リース オプション（該当する場合）
- 設計マニュアル

目次

1. 概要

1.1 目的、対象者、および範囲
1.2 注文および見積もりツール
1.3 オーダー受付開始時期とお客様向け出荷開始（FCS）

2. Cisco Secure Cloud Insights

3. シスコ テクニカルサービス

4. 見積と発注のためのシスコツール

5. Cisco Capital ファイナンス

6. 付録

The bridge to possible

目次

1. 概要

1.1 目的、対象者、および範囲

1.2 注文および見積もりツール

1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)

2. Cisco Secure Cloud Insights

3. シスコ テクニカルサービス

4. 見積と発注のためのシスコツール

5. Cisco Capital ファイナンス

6. 付録

Cisco Commerce Experience の詳細については、https://apps.cisco.com/Commerce/home を参照してください。

Cisco Commerce には、ソリューションの見積、構成、発注に役立つツールがいくつか用意されており、これらを使用して、製品を構成したり、選択した製品ごとのリードタイムと価格を表示したりすることができます。また、さまざまな価格リストやサービス契約条項の下でのリードタイムおよび価格の変化を表示できます。発注の追跡も可能です。

次のシスコ製品とアプリケーションは、Cisco Estimates and Configurations Tool でサポートされています。

- Cisco Secure Analytics サブスクリプション (CSA-SUB) : トップレベルの Assemble to Order (ATO)
- Cisco Secure Insights (SCA-INS) : 課金製品 ID (PID)

Cisco Service Contract Center は、シスコ サービスのセールスチームおよびセールスパートナー向けに用意されており、サービスビジネスを簡単に運営、拡大させて利益を得るための統合ソリューションです。次のようなメリットがあります。

- サービス発注の見積と予約、サービス契約と更新の管理のすべてに、1 つのシンプルで使いやすいソリューションで対処できます。
- 管理上の問題の解決、ビジネス機会の検索、見積の作成にかかる時間を短縮できます。
- データの修正や検証に時間をかけずに、信頼できるデータを利用可能なため、ビジネスを拡大する業務に専念できます。
- パートナーが契約を作成して、それをプロアクティブに管理できます。

  参照先リンク : https://wwwin.cisco.com/CustAdv/globalops/wwsso/service.shtml

1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)

次に示す (製品 / シリーズ) の製品 / アプリケーションを発注する機能は、2021 年 11 月 2 日に有効になります。

- Cisco Secure Analytics : トップレベルの製品ファミリ
- Cisco Secure Cloud Insights : 請求可能なライセンス

上記すべての製品 / アプリケーションに、2021 年 11 月 2 日からのお客様向け出荷開始 (FCS) が予定されています。

The bridge to possible

目次

1. 概要

1.1 目的、対象者、および範囲

1.2 注文および見積もりツール

1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)

2. Cisco Secure Cloud Insights

3. シスコ テクニカルサービス

4. 見積と発注のためのシスコツール

5. Cisco Capital ファイナンス

6. 付録

2. Cisco Secure Cloud Insights

Cisco Secure Cloud Insights® は、JupiterOne® とのパートナーシップによって市場投入されたクラウドネイティブ プラットフォームです。これにより、企業が持つきわめて変化の激しいサイバーアセットについて、詳細な分析情報を得られます。また、マルチクラウド環境（パブリッククラウドとプライベートクラウドの両方）に加え、オンプレミス インフラストラクチャが混在するハイブリッド環境を監視できます。Secure Cloud Insights は API 主導型であり、エージェントレス統合によって、組織のデジタル環境におけるエンティティ間の設定および相互作用のマッピングに必要なデータを取り込みます。こうした接続された豊富なデータセットを、事前作成された約 550 を超えるクエリを使用して調査し、使いやすい視覚的なグラフで表示できます。また、JupiterOne 独自のクエリ言語である J1QL で、ユーザー独自のクエリを簡単に作成することも可能です。作成したクエリは、セキュリティアラートに変換したり、既存のコンプライアンス ベンチマーク（SOC-2 など）の強化に利用したり、グループ化してカスタム標準を作成することもできます。

こうした強力な機能を利用してセキュリティとコンプライアンスのギャップを特定することで、アタックサーフェス（攻撃対象領域）の継続的な拡大によるリスクを大幅に緩和できます。また、セキュリティポスチャの継続的なモニタリング（クラウド セキュリティ ポスチャ管理（CSPM）を含むが、これに限定されない）も可能になります。関係性と相互作用を把握することにより、調査も迅速になり、脅威の封じ込めと対処も容易になります。さらに、アウトバウンド統合によって、アラートを、チケットシステム、電子メールエイリアス、メッセージング アプリケーション、パブリケーション / キューイングサービスにルーティングできます。カスタム API を介してコンテキストを他のサービスと共有することも可能です。この機能を活用して、Secure Cloud Analytics や Cisco SecureX™ といった他のシスコソリューションとの間でコンテキストを共有できます。

次の表に、Cisco Secure Cloud Insights の製品情報と価格を示します。

Cisco Secure Cloud Insights Software as a Service ライセンス

製品番号	説明	表示価格（米ドル）
CSA-SUB	Cisco Secure Analytics ファミリ製品	カテゴリのみのため 0 ドル
SCA-INS	Secure Cloud Insights	請求対象エンティティによって異なる
SVC-CSA-SUP-B	Cisco Secure Analytics ファミリの基本サポート	組み込まれているため 0 ドル

The bridge to possible

目次

1. 概要
1.1 目的、対象者、および範囲
1.2 注文および見積もりツール
1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)
2. Cisco Secure Cloud Insights
3. シスコ テクニカルサービス
4. 見積と発注のためのシスコツール
5. Cisco Capital ファイナンス
6. 付録

請求対象エンティティ

Cisco Secure Cloud Insights のライセンスは、請求対象エンティティで測定された、監視対象環境の規模またはボリュームに基づきます。エンティティとは、グラフデータベースに保存されているノードを指します。エンティティは通常、統合から取得しますが、アセットインベントリ Web アプリケーションまたは API（カスタムスクリプト）によって追加することもできます。

各エンティティは、組織のデジタル運用環境のオブジェクトを表します。たとえば、AWS EC2 インスタンス、RDS DB クラスタ、RDS DB インスタンス、IAM ロール、IAM ポリシー、ユーザーエンドポイント、ユーザーなどです。すべてのエンティティが請求対象カテゴリに加算されるわけではありません。詳細については、オンラインマニュアルを参照するか、付録の表を参照してください。

3. シスコ テクニカルサービス

Cisco Commerce の Cisco Secure Cloud Insights では、セキュリティ向け Cisco Software Support の基本サポートオプションを利用できます。このサービスには、購入したソフトウェア サブスクリプションの全期間でオンラインツールまたは電子メールによるサポートを受けられるなど、基本的なオンラインサポートが含まれています。シスコは、送信されたケースに対し、遅くとも翌営業日の標準営業時間内に応答します。

セキュリティ向け Cisco Software Support の詳細については、サービス内容の説明を参照してください。

表 1.　基本サービスの PID - トランザクション

サービス製品番号	説明	コスト
SVS-CSA-SUP-B	Cisco Secure Analytics 製品ファミリに組み込まれた基本ソフトウェアサポート	0 ドル

The bridge to possible

目次

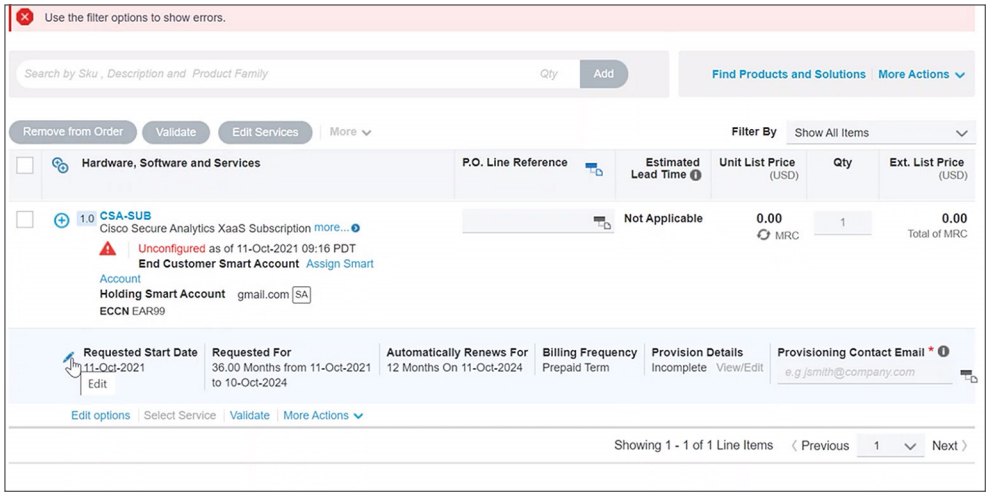
1. 概要
- 1.1 目的、対象者、および範囲
- 1.2 注文および見積もりツール
- 1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)

2. Cisco Secure Cloud Insights
3. シスコ テクニカルサービス
4. 見積と発注のためのシスコツール
5. Cisco Capital ファイナンス
6. 付録

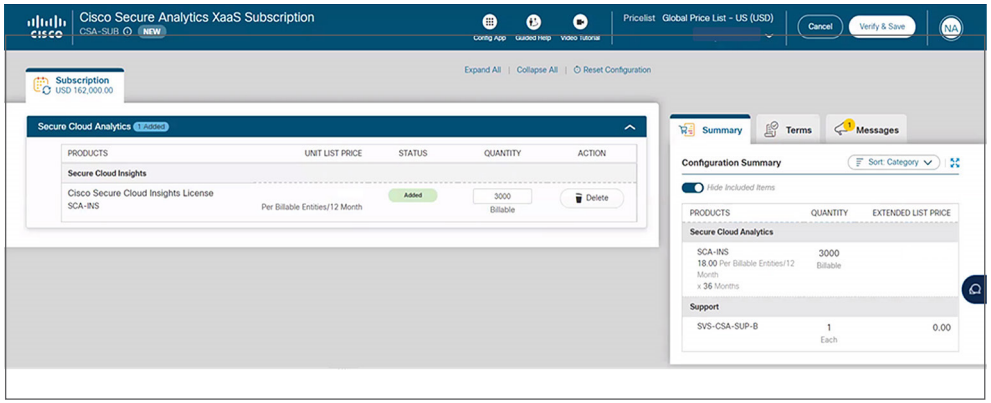
4. 見積と発注のためのシスコツール

このドキュメントの公開時点では、Cisco Secure Cloud Analytics は、シスコの Commerce Web サイトで個別に発注する場合にのみ利用でき、セキュリティ EA 購入プログラムへの追加は 2022 年に予定されています。発注手順は次のとおりです。

1. 最初に **CSA-SUB** カテゴリを検索して選択し、編集オプションをクリックします。



2. 発注情報はデフォルトで、現在利用可能な唯一のカテゴリである Secure Cloud Analytics にネストされた Secure Cloud Insights License **SCA-INS** に設定されます。
3. 発注する請求対象エンティティの数を入力します。**注：**最小発注数は 3,000 です。

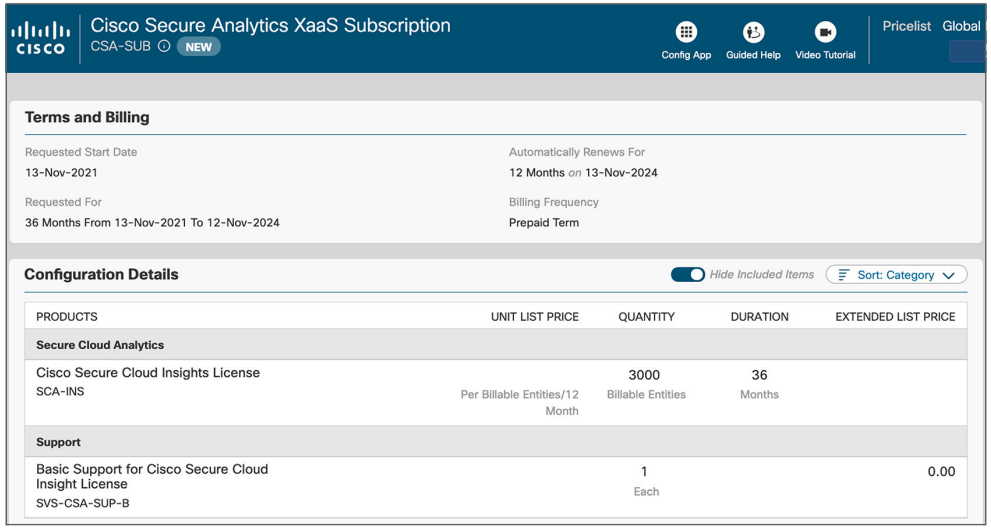


The bridge to possible

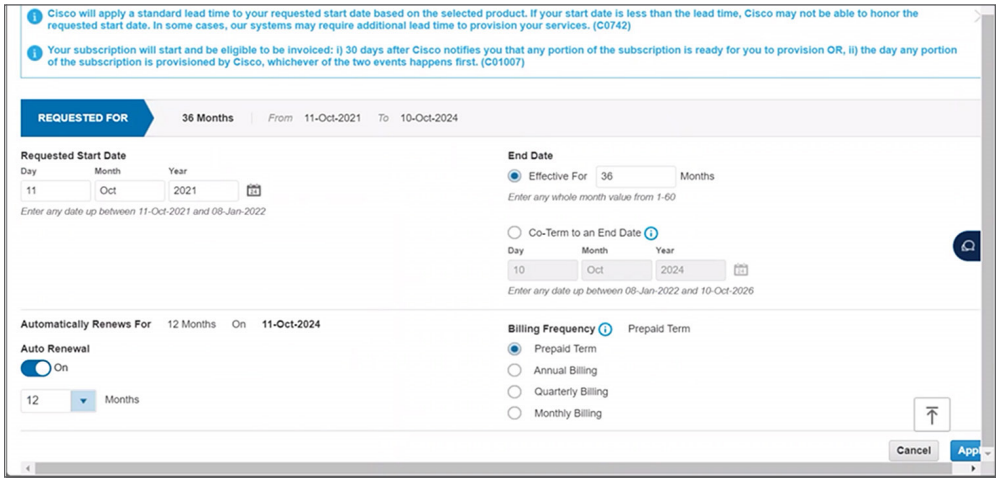
目次

1. 概要
   1.1 目的、対象者、および範囲
   1.2 注文および見積もりツール
   1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)
2. Cisco Secure Cloud Insights
3. シスコ テクニカルサービス
4. 見積と発注のためのシスコツール
5. Cisco Capital ファイナンス
6. 付録

4. 基本サポートのテクニカルサービス製品 ID、**SVS-CSA-SUP-B** (0 ドル) が発注に追加されます。



5. 必要に応じて、サブスクリプション期間と支払い期間を変更します。デフォルトでは 3 年のサブスクリプションが選択されますが、1 年と 5 年のサブスクリプションも利用できます。支払いオプションについても、月次、四半期ごと、年次、前払いから選択します。



6. これで、注文情報を保存して Cisco Commerce Web アカウントに追加する準備が整いました。

The bridge to possible

目次

1. 概要

1.1 目的、対象者、および範囲

1.2 注文および見積もりツール

1.3 オーダー受付開始時期とお客様向け出荷開始 (FCS)

2. Cisco Secure Cloud Insights

3. シスコ テクニカルサービス

4. 見積と発注のためのシスコツール

5. Cisco Capital ファイナンス

6. 付録

5. Cisco Capital ファイナンス

[[製品 / シリーズ]] がもたらす大きなメリットを考えると、[[機能]] の導入を考えたくなりますが、テクノロジーに投資するときには、新しいシステムを手頃な価格で調達できるかどうかが問題となります。その問題を解決するのが Cisco Capital です。シスコはお客様に最適なファイナンスソリューションを提供します。これによりお客様は、柔軟な返済によって支出とメリットを調整しキャッシュフローの問題を軽減することも、オペレーティングリースを選択して資本コストをゼロにすることもできます。

Cisco Capital を利用することで、必要とするテクノロジーを入手する際の障害を軽減または撤廃できます。総合的なソリューションであるファイナンスプログラムにより、パートナーとお客様は次のことが可能になります。

- ビジネス目標の達成
- 成長の加速
- 現行の戦略と将来的なニーズに適合するテクノロジーの獲得
- 競争力の維持

Cisco Capital は、投資資金の最適化、CapEx から OpEx への転換、キャッシュフローの管理など、お客様の財務目標達成を支援します。支払いが統一され、予想外の支払いが発生することもありません。シスコキャピタルは世界中の 100 を超える国で運営されているため、顧客やパートナーは地域を問わず、信頼のおける手段でシスコの製品やサービスを安全に利用することができます。

Cisco Capital ファイナンスの詳細については、次のリンクを参照してください。

- チャネルパートナー様の場合 : http://www.cisco.com/jp/go/capital/
- シスコの現場スタッフの場合 : http://wwwin.cisco.com/FinAdm/csc/

6. 付録

エンティティ	説明	請求対象
AccessKey	アクセス許可に使用されるキー（ssh-key、access-key、api-key/token、mfa-token/device など）	○
AccessPolicy	Host、Role、User、UserGroup、Service に割り当てられるアクセス制御のポリシー。	○
AccessRole	プリンシパル（ユーザー、グループ、サービスなど）にマッピングされるアクセス制御ロール。	○
Account	1 つのサービスまたは一連のサービスで使用される組織アカウント（AWS、Okta、Bitbucket Team、Google G-Suite アカウント、Apple Developer Account など）。各アカウントはサービスに接続される必要がある。	○
Application	ソフトウェア製品またはアプリケーション。	○
ApplicationEndpoint	アプリケーション エンドポイント。これは、要求を開始または受信するプログラムインターフェイス（API など）として機能する。	○
Assessment	HIPAA リスク評価などのコンプライアンス評価や、侵入テストなどの技術的アセスメントといった、評価を表すオブジェクト。各評価には、調査結果（脆弱性、リスクなど）が付随する。	○
Attacker	攻撃者または脅威アクター。	○
Backup	バックアップデータが含まれる特定のリポジトリまたはデータストア。	○
Certificate	SSL または S/MIME 証明書などのデジタル証明書。	○
Channel	Slack チャネルや、AWS SNS のトピックといった通信チャネル。	○
Cluster	コンピューティングまたはデータベースリソース / ワークロードのクラスタ。	○
CodeCommit	リポジトリへのコードコミット。コミット ID は、エンティティの _id プロパティにキャプチャされる。	×
CodeDeploy	コード展開のジョブ。	○
CodeModule	ソフトウェアモジュール。**npm モジュールや Java ライブラリ**など。	○
CodeRepo	ソースコードリポジトリ。CodeRepo は DataRepository でもあるため、DataRepository に必要なプロパティをすべて保持する必要がある。	○
CodeReview	コードレビューレコード。	○

エンティティ	説明	請求対象
Configuration	Configuration には、Task、Deployment、Workload などのリソースを示す定義が含まれる。たとえば、aws_ecs_task_definition は Configuration に該当する。	○
Container	ソフトウェアの標準単位であり、これによって、コード、そのすべての依存関係、設定がパッケージ化される。	○
Control	セキュリティまたは IT 制御。Control は、ベンダー / サービス、人員 / チーム、プログラム / プロセス、自動化コード / スクリプト / 設定、システム / ホスト / デバイスによって実装できる。そのため、追加のクラスとして、Service（Okta SSO など）、Device（物理ファイアウォールなど）、HostAgent（Carbon Black CbDefense エージェントなど）に適用される可能性がある。また、Control は、セキュリティポリシー手順とコンプライアンス標準 / 要件にマッピングされる。	○
ControlPolicy	セキュリティ制御を管理（または適用、評価、監視）するルールが含まれる技術ポリシーまたは運用ポリシー。	○
CryptoKey	暗号キーなど、暗号化を行うために使用されるキー。	○
DataObject	aws-s3-object、sharepoint-document、source-code、またはディスク上のファイルといった個々のデータオブジェクト。正確なデータ型は、エンティティの _type プロパティに記述されている。	×
DataStore	データが保存される仮想リポジトリ（例：aws-s3-bucket、aws-rds-cluster、aws-dynamodb-table、bitbucket-repo、sharepoint-site、docker-registry）。正確なタイプは、エンティティの _type プロパティに記述されている。	○
Database	データベースのクラスタ / インスタンス。	○
Deployment	コード、アプリケーション、インフラストラクチャ、またはサービスの展開。たとえば、Kubernetes の展開など。自動スケーリンググループも展開と見なされる。	○
Device	サーバー、ノートパソコン、ワークステーション、スマートフォン、タブレット、ルータ、ファイアウォール、スイッチ、Wi-Fi アクセスポイント、USB ドライブなどの物理デバイスまたはメディア。正確なデータ型は、エンティティの _type プロパティに記述されている。	○
Directory	LDAP、Active Directory などのディレクトリ。	○
Disk	AWS EBS ボリュームなどのディスクストレージデバイス。	○
Document	ドキュメントまたはデータオブジェクト。	×
Domain	インターネットドメイン。	○
DomainRecord	ドメインゾーンの DNS レコード。	×

エンティティ	説明	請求対象
DomainZone	インターネットドメインの DNS ゾーン。	○
Finding	セキュリティ調査の結果。脆弱性の問題、または単なる情報を示す場合がある。1 つの結果が、1 つ以上のリソースに影響を与えることもある。脆弱性と影響を受けたリソースエンティティとの IMPACTS 関係性が、結果の記録として機能する。IMPACTS 関係性には、「identifiedOn」、「remediatedOn」、「remediationDueOn」、「issueLink」 などのプロパティが含まれる。	×
Firewall	ネットワーク / ホスト / アプリケーションを保護するハードウェアまたはソフトウェア。	○
Framework	標準のコンプライアンスまたは技術的なセキュリティフレームワークを表すオブジェクト。	○
Function	仮想アプリケーションの関数たとえば、**awslambdafunction、azurefunction、googlecloud _function** など。	○
Gateway	ネットワークルータやアプリケーション ゲートウェイなど、システム / アプライアンスまたはソフトウェアサービスのゲートウェイ / プロキシ。	○
Group	定義済みの汎用エンティティグループ。Resource、User、Workload、DataRepository などのグループを表すことができる。	○
Host	ネットワークスタック全体を所有し、ワークロード環境として機能するコンピューティング インスタンス。通常、オペレーティングシステムを実行する。正確なホストタイプは、エンティティの _type プロパティに記述されている。ホストの UUID は、エンティティの _id プロパティにキャプチャされる。	○
HostAgent	ホスト / エンドポイントで実行されるソフトウェアエージェントまたはセンサー。	○
Image	システムのイメージ。たとえば、AWS AMI（Amazon Machine Image）など。	×
Incident	運用またはセキュリティ上のインシデント。	○
Internet	グラフ内のインターネットノード。インターネットノードは 1 つのみ存在する。	×
IpAddress	再割り当て可能な IpAddress リソースエンティティ。ホストに**設定済みの** IP アドレスに対して、エンティティを作成してはならない。これは、IP アドレスが再利用可能なリソース（例：AWS の Elastic IP アドレスオブジェクト）の場合にのみ使用する。	×
Key	ssh-key、access-key、api-key/token、pgp-key など。	○
Logs	アプリケーション、ネットワーク、システムログといった特定のリポジトリまたは宛先。	○
Module	ソフトウェアまたはハードウェアのモジュール。**npm モジュールや Java ライブラリ**など。	○

エンティティ	説明	請求対象
Network	aws-vpc、aws-subnet、cisco-meraki-vlan などのネットワーク。	○
NetworkEndpoint	ネットワークリソースに接続またはアクセスするためのネットワークエンドポイント。たとえば、NFS マウントのターゲットや、VPN エンドポイントなど。	○
NetworkInterface	再割り当て可能なソフトウェアデファインド ネットワーク インターフェイスのリソースエンティティ。ホストに**設定済みの**ネットワーク インターフェイスに対して、エンティティを作成してはならない。これは、ネットワーク インターフェイスが再利用可能なリソース（例：AWS の Elastic Network Interface オブジェクト）の場合にのみ使用する。	×
Organization	企業（JupiterOne など）や事業部門（HR など）などの組織。社内の組織にも、社外の組織にも使用できる。より具体的な Vendor というクラスもある。	○
PR	プル要求。	×
PasswordPolicy	パスワードポリシーは特定の Ruleset を表す。これは、デジタル環境全体で広く使用され、パスワードポリシーに固有のよく知られた特性（長さや複雑さなど）を持つため、個別に定義される。	○
Person	組織の従業員など、実際の人物を表すエンティティ。	○
Policy	文書化されたポリシードキュメント。	○
Procedure	手順と制御が文書化されたドキュメント。通常、Procedure には親 Policy が実装される。さらに、Control には Procedure が実装される。	○
Process	コンピューティングプロセス、つまり、1 つまたは複数のスレッドによって実行されているコンピュータプログラム / ソフトウェア アプリケーションのインスタンス。プログラムレベルの運用プロセス（Procedure）ではない。	○
Product	ソフトウェア製品など、組織が開発した製品。	○
Program	プログラム。たとえば、バグ報告報奨金や脆弱性開示プログラムなど。	○
Project	ソフトウェア開発プロジェクト。他の汎用プロジェクトにも使用できるが、定義済みプロパティはソフトウェア開発プロジェクト向け。	○
Queue	コンピューティングプロセスまたはデバイスのスケジューリングキュー。	○
Record	DNS レコード、正式な記録（例：Risk）、文書（例：Policy/Procedure）または参照先（例：Vulnerability/Weakness）。正確なレコードタイプは、エンティティの _type プロパティにキャプチャされる。	×

エンティティ	説明	請求対象
Repository	リソースが含まれるリポジトリ。たとえばDocker コンテナイメージをホストする Docker コンテナ レジストリ リポジトリなど。	○
Requirement	セキュリティ、コンプライアンス、規制、設計に関する個々の要件。	○
Resource	割り当て可能な汎用リソース。リソースは通常、ホストまたはワークロードによって使用または接続されない限り、単独では機能しない。	○
Review	レビューレコード。	○
Risk	Assessment の結果として特定されたリスクを表すオブジェクト。リスクレジスタは、JupiterOne の Risk オブジェクトコレクションで構成される。Control は、リスクとの MITIGATES 関係性を持つ場合がある。	○
Root	グラフ内のルートノード。ルートノードは組織アカウントごとに 1 つのみ存在する。	○
Rule	運用または設定のコンプライアンスルール。多くの場合、これによって Ruleset が構成される。	○
Ruleset	運用または設定のコンプライアンス ルールセット。セキュリティ制御または IT システムを管理（または適用、評価、監視）するルールで構成される。	○
Scanner	システムの脆弱性、アプリケーションコード、またはネットワーク インフラストラクチャのスキャナ。	○
Section	コンプライアンスセクションなどのセクションを表すオブジェクト。	○
Service	ベンダーが提供するサービス。	○
Site	組織の物理的な拠点。Person（従業員）は通常、サイト（locatat **または workat**）との関係性を持つ。AWS リージョンの抽象リファレンスとしても使用される。	○
Standard	コンプライアンスや技術標準などの標準を表すオブジェクト。	○
Subscription	サービスまたはチャネルのサブスクリプション。	○
Task	コンピューティングタスク。たとえば、AWS のバッチジョブ、ECS タスクなど。	○
Team	複数のメンバー Person エンティティで構成されるチーム。たとえば、開発チームやセキュリティチームなど。	○
ThreatIntel	脅威インテリジェンスには、十分な専門知識を持ち、あらゆるソース情報にアクセスできる担当者が脆弱性リスク分析によって収集した情報がキャプチャされる。脅威インテリジェンスを利用すると、検出されたリスクが組織に与える影響を判断できる。	○

エンティティ	説明	請求対象
Training	セキュリティ意識の啓発やセキュア開発のトレーニングといったトレーニングモジュール。	○
User	特定のシステムやサービスにアクセスするためのユーザーアカウント / ログイン。たとえば、okta-user、aws-iam-user、ssh-user、ホスト上の local-user など。	○
UserGroup	ユーザーグループ。通常、Okta や Office365 のグループなど、何らかのタイプのアクセス制御に関連付けられる。UserGroup にアクセスポリシーが関連付けられている場合、UserGroup のすべてのメンバー User がポリシーを継承する。	○
Vault	キーリングなどの秘密キーの集合。	○
Vendor	ベンダーまたはサービスプロバイダーなどの外部組織。	○
Vulnerability	セキュリティの脆弱性（アプリケーション、システム、またはインフラストラクチャ）。1 つの脆弱性が複数の調査結果に関連し、複数のリソースに影響を与える可能性があります。脆弱性と影響を受けたリソースエンティティとの IMPACTS 関係性が、結果の記録として機能する。IMPACTS 関係性には、「identifiedOn」、「remediatedOn」、「remediationDueOn」、「issueLink」などのプロパティが含まれる。	○
Weakness	セキュリティの弱点	○
Workload	仮想コンピューティングのインスタンス。aws-ec2-instance、docker-container、aws-lambda-function、application-process、または vmware-instance がこれに該当する。正確なワークロードタイプは、エンティティの _type プロパティに記述されている。	○
[システム マッピング エンティティ]	_source='system-mapper' が設定されたエンティティ。	×
[システムの内部エンティティ]	_source='system-internal' が設定されたエンティティ。	×
[カスタム作成されたエンティティ]	カスタム定義の _class または _type を使用して作成されたエンティティ。	○