# Darktrace Enterprise Immune System の仮想化展開

## はじめに

Darktrace は AWS 環境内でクラウドベースのマスターアプライアンスをホスティングすることで、Enterprise Immune System を仮想化して展開しています。仮想化された構成では、顧客ネットワーク（物理または仮想）内のローカルプローブ、統合されたサードパーティサービス（SaaS またはクラウド等）、または Antigena Email 等の接続された Darktrace 製品からからデータを受け取ります。

## その仕組みは?

クラウドマスターアプライアンスは標準の物理アプライアンスと同じデータを取り込み解析しますが、ネットワークトラフィックは物理、仮想に関わらず、Darktrace vSensor を介して 2 つの暗号化モードのいずれかにより送信される必要があります。 プッシュトークンの使用は vSensor IP に対するインバウンドのファイアウォール例外を必要としないため、特に推奨されます。 vSensor はトラフィックミラーリングを使用する場合、スタンドアロン仮想マシンとして、あるいは最大 200 個までの osSensor エージェント（vSensor 1 個につき）とともに使用することができます。Darktrace osSensor は Windows またはサポートされる Linux ディストリビューションを実行するデバイス、ならびに Docker エンジンを実行する Linux 環境にインストールすることができます。

ネットワークトラフィックを処理し、送出することに加えて、vSensor は syslog 形式のログを取り込み Darktrace クラウドマスターに転送することができます。VPN と DHCP ログは貴重なデバイス追跡エンリッチメントを提供し、取り込まれたログデータからのカスタムイベントタイプは数多くのサードパーティ製ツールとの統合に使用できます。

クラウドベース展開では、Darktrace の可視性をサードパーティサービスおよび仮想化環境のマネジメントアクティビティにも広げる Darktrace の SaaS およびクラウドセキュリティ用モジュールもサポートされています。認証後、各モジュールは指定されたサービスの監査イベントデータを取得および解析し、「生活パターン」検知と異常検知をネットワークの外側にも拡大します。

## 自動対処

仮想化展開においては、vSensor ならびに osSensor エージェントを使って Antigena 自動対処をサポートしています。vSensor は Antigena Network のリセットアクションを直接実行することも、それぞれに関連づけられた osSensor（エージェントまたはコンテナ化による）に対応を指示することもできます。VPC トラフィックミラーリングを行う場合には、osSensor が自動アクションを実行する必要があります。

Darktrace Antigena Email は仮想化されたマスターとシームレスに統合されており、G Suite、Office 365 または Hybrid Exchange 環境に対して使用することができます。Antigena Email とクラウドでホスティングされたアプライアンスはデバイスのメタデータ、ネットワークおよびドメインの珍しさ、ならびに双方のプラットフォームで検知された脅威を共有し、組織全体に広範な保護を実現します。

## セキュリティ

それぞれの顧客に対して、希望する AWS リージョン内に、個別の、完全に分離されたインスタンスが提供されます。ネットワーク、クラウドおよび仮想環境内のローカルプローブから取り込まれたデータは、転送中に暗号化され関連づけられたアベイラビリティゾーンを出ることはありません。さらに、すべてのユーザーアカウントに対して二要素認証が徹底されます。

Darktrace のオペレーションならびにセキュリティプラクティスは ISO27001 認証を受けています。これには次が含まれます：

- 最小権限役割ベースのアクセス制御
- ソフトウェアおよびインフラに対する強力な最新の暗号化（TLS1.2、AES 256 GCM、SSHv2 Chacha-poly20）
- 社内および第三者のエキスパートによる定期的な侵入テスト
- 製造および開発環境に対する Darktrace Security Operations Center による 24 時間週 7 日、年中無休での監視
- 新入スタッフメンバーに対するバックグラウンドチェック、ならびに離職者に対するアカウントロックアウト

詳細な情報セキュリティポリシーについては Darktrace 担当者にお問い合わせください。

## 制限事項

- Darktrace は現在クラウドでの複数マスター展開を提供しておりません。
- Darktrace の仮想化マスター展開は Darktrace AWS クラウド以外でのホスティングを提供しておりません。
- セキュリティ上の理由から、クラウドでホスティングされたマスターは暗号化されていないデータを受け入れも取り込みもしません。ネットワークトラフィック、ログデータ、およびその他のタイプのデータは、認可されたモードで動作する vSensor 等のセキュアなチャネルを介して送信しなければなりません。

## 使用できるリージョン

Darktraceはクラウドベース展開を欧州（AWSリージョンeu-west-1またはeu-west-2）、米国（AWSリージョンca-central-1）、シンガポール（AWSリージョンap-southeast-1）、またはオーストラリア（AWSリージョンap-southeast-2）でのホスティングにより提供できます。お客様の組織がデータフローに対する地域または地理的な制限の対象となっているためにこれらのリージョンにおける使用が難しい場合には、そのことについてDarktraceの担当者にご相談ください。

クラウドでホスティングされたインスタンスからの受信トラフィックをホワイトリスト化したい場合、これらのリージョナルゾーンからの送信トラフィック（NAT）に使用される次のIPアドレス／ホスト名ペアをご確認ください。

| リージョン | IPアドレス | DNSエントリ |
|---|---|---|
| 米国 | 52.9.179.107 | cloud-nat-usw1.darktrace.com |
| カナダ | 15.223.16.1 | cloud-nat-cac1.darktrace.com |
| ヨーロッパ、中東、アフリカ（アイルランド） | 52.51.139.68 | cloud-nat-euw1.darktrace.com |
| ヨーロッパ、中東、アフリカ（UK） | 18.132.236.38 | cloud-nat-euw2.darktrace.com |
| アジア太平洋（シンガポール） | 52.220.237.248 | cloud-nat-apse1.darktrace.com |
| アジア太平洋（オーストラリア） | 3.24.26.120 | cloud-nat-apse2.darktrace.com |

## 設定および管理

クラウドマスターはDarktraceのオペレーションにより管理されます。この展開シナリオではマネジメントおよびシステムアドミニストレーションコンソールは使用できません。コンソールへのアクセスを必要とするような設定の変更またはプロセスの変更を行いたい場合、Darktraceのお客様担当者またはDarktraceサポート組織のメンバーに連絡して支援を受けてください。

Darktraceはトラフィック負荷に応じてインスタンスのスケーリングを管理します。

## ソフトウェアアップデート

Threat Visualizerソフトウェアは新しいバージョンが使用可能になると自動的に更新されます。可能な場合、更新は通常の業務時間外に適用されます。それが不可能な場合も、更新のプロセスはThreat Visualizerユーザーに対する混乱を最小限に抑えて実施されます。

## バックアップ

複数の短期スナップショットバックアップがローリングベースで行われ、災害復旧が必要となった場合も継続性が確保されています。

## アクセス

クラウドでホスティングされる環境には、"https://[region]-XXXX-01.cloud.darktrace.com" という形式の一意のホスト名でアクセスします。

このホスト名は変更できません。これがお客様で使用されている命名スキームに適合しない場合、System Configページでカスタム内部DNSレコードと対応するFQDN値を設定することも可能です。

二要素認証はすべてのユーザーアカウントに対してデフォルトで有効に設定されています。

## ネットワークの必要条件

ネットワークトラフィックの取り込みには、少なくとも1個のvSensorが暗号化モードでDarktraceマスターと通信することを承認されていなければなりません。

- プッシュトークンモード（推奨）では、vSensorはクラウドマスターに対して443番ポートから接続できる必要があります。
- プルモードでは、vSensor IPはクラウドマスターのロケーションからインバウンドで継続的に443番ポートにアクセス可能である必要があります。

## 別のプルモード構成

vSensor IPをクラウドマスターに直接露出することができない場合、複数のvSensorを1つの外部IPを持つカスタムプロキシの後ろ側に構成することも可能です。または、ネットワークファイアウォールの外側にあるサーバーを介してOpenVPNトンネルを使ってHTTPSトラフィックを任意のvSensorにプロキシすることも可能です。

さらに、ネットワーク上の制約または同じIPの背後に複数のvSensorが存在するなどの理由で443番ポートを使ったvSensorへのアクセスが不可能な場合、別の外部ポートを使用することもできますが、ファイアウォール内にこれに対応するNATルールが存在しこのトラフィックをvSensor内部IPの443番ポートにルートすることが条件となります。

これはSystem Configページでの vSensor IPを入力するときに"123.45.12.34:14677"の形式で指定しなければなりません。

これらの標準以外の構成については、Darktrace担当者が確認し設定を支援することができます。

## ログ転送

ネットワークトラフィックを処理し、送出することに加えて、vSensorはsyslog形式のログを取り込みDarktraceクラウドマスターに転送することができます。vSensorは暗号化されていないログおよびTLS/SSL暗号化されたログのどちらも受け入れます。暗号化されたログについては、vSensorはTCPトラフィックを6514番ポートで受け入れ、デフォルトで自己署名TLS/SSL証明書を使用します。お客様の証明書を使用する方法については、vSensor FAQを参照してください。

vSensorがネットワーク内にローカルに存在する場合、ログ入力データを暗号化せずに1514番ポート（UDPまたはTCP）に送る方法もあります。ただしこれはネットワーク境界の外側にあるvSensorには**推奨されません**。vSensorはネットワークトラフィックと対応するログエントリを同じ方法で送信しますので、プレーンテキストでvSensorに送信されるログは仮想プローブとマスター間で受け渡される際には暗号化されます。

パターンマッチングはDarktraceマスター上で設定され、vSensorに伝達されてそれ以降のログエントリに適用されます。照合（および破棄）はvSensorレベルで実行されます。有効な一致はそこからマスターに転送されます。

ログ入力についての詳しい説明は、Log Input GuideまたはDarktrace System Administration Guideを参照してください。

## クイックスタート ー ネットワークトラフィック

1. Darktrace がお客様の希望される AWS リージョン内でクラウドベースのマスターインスタンスをプロビジョンします。各リージョンに対する IP アドレスとホスト名については、「使用できるリージョン」のセクションをご覧ください。

2. アクセスとログインについての詳細を Darktrace 担当者から受け取り、インスタンスに最初にアクセスします。

   クラウドマスター運用では二要素認証がデフォルトで有効に設定されます。初回のアクセス時には QR コードが表示されます。Google Authenticator または Duo Security 等、お使いの二要素認証アプリを使ってこの QR コードをスキャンしてください。

3. 少なくとも 1 個の Darktrace vSensor を認可されたモードで設定し、クラウドマスターの System Config ページでこれを認証します。

   a. vSensor がプルモードに設定されている場合、対応するファイアウォールルールにおいてクラウドマスターのロケーションから vSensor IP に継続的なアクセスができるよう設定されていることを確認してください。

   b. vSensor がプッシュトークンモード（推奨）に設定されている場合、対応するファイアウォールルールにおいて vSensor からクラウドマスターのロケーションへ継続的なアクセスができるよう設定されていることを確認してください。

vSensor は仮想または物理ネットワーク 1、VPC パケットモニタリング環境、またはデバイスに直接インストールされた、またはコンテナ化された環境で運用されているホストベースの osSensor からのトラフィックを処理することができます。

4. さらにオプションで osSensor、SaaS およびクラウドセキュリティモジュールを展開することにより、広範なネットワーク環境に対する最大限の可視性を保証することができます。

5. すべての構成要素が正しく配備され、プローブがアクセス可能でありデータを処理していることを確認します。システムの状態やトラフィックについての詳しい情報は、System Status ならびに System Config ページから確認することができます。

   トラブルシューティング、仮想プローブ数の設定や追加モジュールの導入については Darktrace 担当者にご相談ください。

## クイックスタート ー SaaS の場合

1. Darktrace がお客様の希望される AWS リージョン内でクラウドベースのマスターインスタンスをプロビジョンし、必要な SaaS およびクラウドコネクタモジュールをプリインストールします。各リージョンに対する IP アドレスとホスト名については、「使用できるリージョン」のセクションをご覧ください。

2. アクセスとログインについての詳細を Darktrace 担当者から受け取り、インスタンスに最初にアクセスします。

   仮想化運用では二要素認証がデフォルトで有効に設定されます。初回のアクセス時には QR コードが表示されます。Google Authenticator または Duo Security 等、お使いの二要素認証アプリを使ってこの QR コードをスキャンしてください。

3. クラウドマスターの System Config ページの SaaS Connectors セクションを確認し、各モジュールに対して認証プロセスを実行します。

4. 認証が正しく行われ、コネクタモジュールがデータを取得できることを確認してください。コネクタサービスの状態については、System Config ページから詳細を確認することができます。

   トラブルシューティング、追加モジュールやネットワークトラフィックプローブの追加については Darktrace 担当者にご相談ください。

---

1 vSensor はデフォルトで仮想カーネルを使用していますが、これは限られた数のハードウェアドライバのみをサポートしています。カーネルを拡張して物理トラフィックをサポートする方法について、詳しくは vSensor FAQ を参照してください。