# ENTERPRISE THREAT PROTECTOR

クラウドでの高度な脅威防御

エンタープライズ組織では、Direct Internet Access（DIA）、SaaS アプリケーション、クラウドサービス、モビリティ、モノのインターネット（IoT）の普及に伴い攻撃される対象（アタックサーフェス）が大幅に増加しているため、新たな課題に直面しています。マルウェア、フィッシング、データ窃盗などの高度な標的型脅威から組織とユーザーを守ることが、これまでとは比べものにならないほど難しくなっています。セキュリティを制御するポイントは複雑に入り組み、従来型（レガシー）ソリューションのセキュリティギャップも管理しなければなりません。Enterprise Threat Protector（ETP）は、セキュリティチームにとって他の従来型セキュリティソリューションのような複雑さ対応が不要で、ユーザーやデバイスがどこに位置していても、インターネットへの安全な接続を実現できる、セキュア・インターネット・ゲートウェイ（SIG）です。Enterprise Threat Protector には、インターネットやドメイン・ネーム・システム（DNS）のトラフィックに関する Akamai 独自のグローバルな知見に基づいた、リアルタイムの脅威インテリジェンスが搭載されています。

## ENTERPRISE THREAT PROTECTOR

Akamai Intelligent Edge Platform™ および Akamai のキャリアグレード再帰 DNS サービス上に構築されている Enterprise Threat Protector（ETP）は、導入や保守に特別なハードウェアを必要とせず、迅速に設定し簡単に展開できる SIG です。

Enterprise Threat Protector は、リアルタイムの Akamai Cloud Security Intelligence および Akamai の実績あるグローバル分散プラットフォームを活用し、マルウェア、ランサムウェア、フィッシング、DNS ベースのデータ窃盗などの標的型脅威を事前に識別し、ブロックします。セキュリティチームは、Akamai のポータルを使うことにより、インターネット接続場所に関係なく全社員に対して一元的に、セキュリティポリシーおよび利用規定（AUP）を数分で作成し展開し実行できます。

### 仕組み

Enterprise Threat Protector は、DNS、URL、インラインペイロード分析といった複数の防御層を使用して、パフォーマンスに影響を及ぼすことなく、最適なセキュリティを提供し、複雑さを軽減します。

**DNS 検査：**外部の再帰 DNS トラフィックを Enterprise Threat Protector にリダイレクトするだけで、リクエストされたすべてのドメインが、ドメインリスクをリアルタイムでスコアリングする Akamai の脅威インテリジェンスと照合されます。悪意のあるドメインやサービスに対するユーザーのアクセスは事前にブロックされ、安全なドメインやサービスへのリクエストは解決されます。こうした検証が IP 接続前に行われるため、脅威はセキュリティ・キル・チェーンの早い段階で阻止されます。さらに、DNS は、あらゆるポートおよびプロトコルにおいて有効であり、標準のウェブポートやプロトコルを使用しないマルウェアからも保護されます。また、ドメインをチェックすることで、ユーザーがアクセスしようとしているコンテンツの種類を判別し、そのコンテンツがエンタープライズの利用規定（AUP）に違反していればブロックすることも可能です。

**URL 検査：**Akamai の脅威インテリジェンスに基づいてリスクが高いとみなされたドメインは、自動的に Akamai Intelligent Edge Platform 上のクラウドプロキシに転送されます。リクエストされた URL は Akamai の URL 脅威インテリジェントと照合され、悪意のある URL は自動的にブロックされます。このプロキシは HTTP と HTTPS の両方の URL を検査します。

**インラインペイロード分析：**リスクの高い URL からの HTTP や HTTPS のペイロードは、高度な複数のマルウェア検出エンジンを使用して、リアルタイムでスキャンされます。これらのエンジンは、シグネチャ、シグネチャレス、機械学習など、さまざまなテクニックを利用し、実行可能ファイルやドキュメントファイルなど、悪意のある可能性のあるファイルや、リクエストされたウェブページに直接埋め込まれたその他のマルウェア（難読化されている悪意のある JavaScript など）に対する包括的なゼロデイ防御を提供します。

Enterprise Threat Protector は、ファイアウォールや SIEM、外部の脅威インテリジェンスフィードなど、他のセキュリティ製品やレポートツールと簡単に統合できるので、エンタープライズはセキュリティスタックのすべてのレイヤーで投資を最大限に活用できます。

さらに、管理対象のノートパソコンに軽量の Enterprise Security Connector を導入すれば、ノートパソコンがオフネットワークで使用される場合も、事前防御型のセキュリティレイヤーをすぐに追加できます。

## ビジネス上のメリット

- **セキュリティ防御を改善。**最新かつ独自の脅威インテリジェンスに基づいて、マルウェアやランサムウェアのドロップサイト、マルウェア CnC（コマンド＆コントロール）サーバー、DNS データ窃盗およびフィッシングのドメインと URL に対するリクエストを事前にブロックします。
- **悪意のあるペイロードをブロックしてゼロデイ対策を改善。**リクエストされたファイルとウェブコンテンツをリアルタイムでスキャンすることにより、エンドポイントデバイスに脅威が到達して影響を及ぼす前に阻止します。
- **DIA パフォーマンスを強化。**疑わしいトラフィックのみプロキシ転送し、URL 検査とペイロード分析を行います。
- **面倒な作業もハードウェアも不要で、簡単に防御を追加。**ユーザーへのサービスを中断することなく、数分で設定・展開でき、迅速な拡張も可能な 100% クラウドベースのソリューションです。
- **VPN を使用せずに、オフネットワークのノートパソコンに対するリスクを軽減しセキュリティを強化。**軽量の Enterprise Client Connector を使用して、セキュリティポリシーと利用規定（AUP）両方を適用します。
- **セキュリティ管理の時間と複雑さを最小限に。**誤検出のセキュリティアラートや他のセキュリティ製品からのアラートを減らし、セキュリティポリシーやアップデートをどこからでも数秒で管理し、すべてのロケーションを保護します。
- **コンプライアンスや利用規定（AUP）を迅速かつ一元的に実施。**問題がある／不適切なドメインおよびコンテンツカテゴリーへのアクセスをブロックします。
- **DNS の耐障害性と信頼性を向上。**Akamai Intelligent Edge Platform を活用します。

# ENTERPRISE THREAT PROTECTOR

## AKAMAI CLOUD SECURITY INTELLIGENCE（CSI）

Enterprise Threat Protector には、脅威やそれによってエンタープライズが受けるリスクに関するリアルタイムインテリジェンスを提供する Akamai Cloud Security Intelligence が活用されています。

Akamai の脅威インテリジェンスは、クラウドがお客様のビジネスにもたらす現在の脅威や関連する脅威に対する防御を提供するとともに、セキュリティチームが調査しなければならない誤検出アラートの数を最小限に抑えるように設計されています。

この情報は、世界中のウェブトラフィックの 30% 近くを管理し、毎日最大 2.2 兆件の DNS クエリーを配信している Akamai Intelligent Edge Platform から常時収集されるデータに基づいて構築されます。Akamai のインテリジェンスは、多数の外部脅威フィードによってさらに強化されます。これらと結合されたデータセットは、挙動分析テクニック、機械学習、独自のアルゴリズムを使用して継続的に分析、整理されています。新たな脅威が確認されると、直ちに Enterprise Threat Protector サービスに追加され、リアルタイムの防御を提供します。

## AKAMAI INTELLIGENT EDGE PLATFORM

Enterprise Threat Protector サービスは、安全で信頼性が高く、高速な、キャリアグレードの Akamai Intelligent Edge Platform 上に構築されています。このプラットフォームは、世界中に分散されており、100% の可用性を保証する SLA を提供し、エンタープライズの再帰 DNS サービスにとって最適な信頼性を実現します。

## クラウドベースの管理ポータル

Enterprise Threat Protector の設定やその後の管理はすべて、クラウドベースの Akamai Luna ポータルから実行するため、いつでもどこにいても管理できます。

ポリシー管理も迅速かつ簡単です。変更内容は数分で世界中にプッシュされ、すべての拠点とユーザーを確実に保護できます。リアルタイムの E メール通知と定期的なレポートを設定すれば、重大なポリシーイベントの発生時にセキュリティチームに知らせることができます。これにより、潜在的な脅威を特定し解決する修復手段をただちに講じることができます。リアルタイムダッシュボードには、トラフィック、脅威、AUP イベントの概要が出力されます。個々のダッシュボード要素をドリルダウンすると、これらアクティビティの詳細情報を確認できます。こうした詳細情報は、セキュリティインシデントの分析や対処方法に関する貴重なリソースとなります。

すべてのポータル機能に、API でアクセスできます。また、データログを SIEM にエクスポートできるため、ご使用の他のセキュリティソリューションやレポーティングツールと Enterprise Threat Protector を、簡単かつ効果的に統合できます。

## 主な機能

- **Akamai によって分類される脅威：**1 日のウェブトラフィックの 15～30% という Akamai の可視性に基づく最新の脅威インテリジェンスが、Akamai の再帰 DNS クラウドへの 1 日 2.2 兆件の DNS リクエストと結合されます。
- **お客様による脅威分類：**お客様のセキュリティチームはデータを既存の脅威インテリジェンスフィードとすぐに統合できるので、セキュリティへの既存の投資からさらに大きな価値を得ることができます。
- **インライン・リアルタイム・ペイロード分析：**3 つの高度なマルウェア検出エンジンが、複雑で巧妙な脅威を識別してブロックし、ゼロデイ防御を強化します。
- **利用規定（AUP）：**エンタープライズの利用規定を実施し、アクセス可能なコンテンツカテゴリーとアクセス不可能なコンテンツカテゴリーを限定することで、コンプライアンスを実現します。
- **分析とレポート：**ダッシュボードでは、脅威イベントや AUP イベントだけでなく、エンタープライズウェブのすべてのアウトバウンドトラフィックに関する知見をリアルタイムでご覧になれます。
- **セキュリティの知見：**Akamai がその脅威インテリジェンスリストにドメインまたは URL を追加した理由がすぐにわかります。
- **ロギング：**トラフィックログは 30 日間保存され、CSV ファイルとして簡単にエクスポートできます。また SIEM へ統合して詳細な分析を行うこともできます。
- **DNSSEC：**Enterprise Threat Protector に送られるすべての DNS リクエストで、DNSSEC は有効です。

## AKAMAI エコシステム

Akamai Intelligent Edge Platform は、エンタープライズからクラウドまで全てを網羅し、お客様とそのビジネスを高速、スマート、セキュアなものにします。Akamai の包括的なソリューションは、統一されカスタマイズ可能な Luna Control Center がもたらす可視性と制御機能を通じて管理され、Professional Services のエキスパートによってサポートされています。こうしたエキスパートの支援により、お客様はソリューションを簡単に稼働できるとともに、戦略の進展に伴い、イノベーションのアイデアを得ることができます。

**Enterprise Threat Protector の詳細や無料トライアルのお申し込みについては、akamai.com/etp をご覧ください。**

Akamai

# ENTERPRISE THREAT PROTECTOR

| セキュリティ | Guest Wi-Fi | Intelligence | Advanced Threat |
|---|---|---|---|
| マルウェア、ランサムウェア、フィッシングの配信ドメインをブロック | | X | X |
| マルウェア CnC リクエストをブロック | | X | X |
| DNS ベースのデータ窃盗を特定 | | X | X |
| リスクの高いドメインをプロキシ経由させ、リクエストされた HTTP および HTTPS URL を検査 | | X | X |
| 複数のインラインマルウェア分析および検出エンジンを使用して、リスクの高い HTTP および HTTPS ペイロードのリアルタイムインライン分析を実行 | | | X |
| ファイル共有サイトからダウンロードされたファイルのリアルタイムインライン分析 | | | X |
| HTTP および HTTPS URL 検査用にカスタマイズされたドメインリストの作成 | | X | X |
| インラインペイロード分析用にカスタマイズされたドメインリストの作成 | | | X |
| 新しく発見された脅威の識別とアラートを目的としたお客様のトラフィックログのルックバック分析 | | X | X |
| 許可／拒否のカスタムリストの作成 | | X | X |
| 追加の脅威インテリジェントフィードの統合 | | X | X |
| カスタマイズ可能なエラーページ | X | X | X |
| 悪意のあるドメインおよび URL に関するインテリジェンスの獲得を目的とした Akamai 脅威データベースへのクエリー | | X | X |
| オフネットワークのノートパソコン（Windows および macOS）のセキュリティの強化 | | X | X |

| Acceptable Use Policy（利用規定／ AUP） | Guest Wi-Fi | Intelligence | Advanced Threat |
|---|---|---|---|
| オンネットワークおよびオフネットワークのユーザーに関する AUP 違反のモニタリングまたはブロック | X[1] | X | X |
| Google、Bing、YouTube に対するセーフサーチの強化 | X | X | X |

| レポート、モニタリング、管理 | Guest Wi-Fi | Intelligence | Advanced Threat |
|---|---|---|---|
| エンタープライズ全体のすべてのアクティビティをカスタマイズ可能なダッシュボードに表示 | X[2] | X | X |
| すべての脅威および AUP イベントの詳細な分析 | X[2] | X | X |
| オンボーディングされたすべてのトラフィックリクエストおよび脅威イベントと AUP イベントの完全なロギングおよび可視化 | X[2] | X | X |
| すべてのログのログ配信：ログは 30 日間保持され API を通じてエクスポート可能 | X[2] | X | X |
| 設定、カスタム・セキュリティ・リスト、およびイベントをオープン API で利用可能 | X[2] | X | X |
| SIEM などの他のセキュリティシステムとオープン API を通じて統合 | X | X | X |
| E メールベースのリアルタイムのセキュリティおよび AUP アラート | X[2] | X | X |
| 日次または週次の E メールレポートのスケジュール設定 | X | X | X |
| 管理者の委任 | X | X | X |

| AKAMAI INTELLIGENT EDGE PLATFORM ™ | Guest Wi-Fi | Intelligence | Advanced Threat |
|---|---|---|---|
| 再帰 DNS のお客様別専用 IPv4 および IPv6 VIP | X | X | X |
| 可用性 100% の SLA | X | X | X |
| 最適なパフォーマンスを実現する Anycast DNS ルーティング | X | X | X |
| DNSSEC の実施によるセキュリティの強化 | X | X | X |

| ENTERPRISE CONNECTOR | Guest Wi-Fi | Intelligence | Advanced Threat |
|---|---|---|---|
| Enterprise Client Connector によるオフネットワークのノートパソコン（Windows および OSX）の保護、およびオフネットワークとオンネットワークのイベントへのマシン名の報告 | | X | X |
| Enterprise Client Connector の自動更新 | | X | X |
| Enterprise Security Connector によるエンドポイントデバイスの IP アドレスおよびマシン名の識別 | | X | X |

1. ETP ゲスト Wi-Fi にはオフネットワークの AUP 実施は含まれません。
2. ETP ゲスト Wi-Fi にはセキュリティ制御は含まれません。そのため、AUP イベントとアクティビティを含むのはアラート、分析、ダッシュボード、ログのみです。