概要資料

THREAT INTELLIGENCE

プロフェッショナルが厳選した、信頼性の高い
インテリジェンスフィードと分析レポート

Progress. Protected.

組織の脅威インテリジェンスに ESETを含める理由

現在の脅威動向やサイバー犯罪者が用いる手口を理解することは、極めて重要な知識上のアドバンテージとなります。この洞察により、組織は内部防御システムをより効果的に強化できます。高品質のインテリジェンスデータは、強力なサイバー脅威インテリジェンス（CTI）戦略の基盤です。

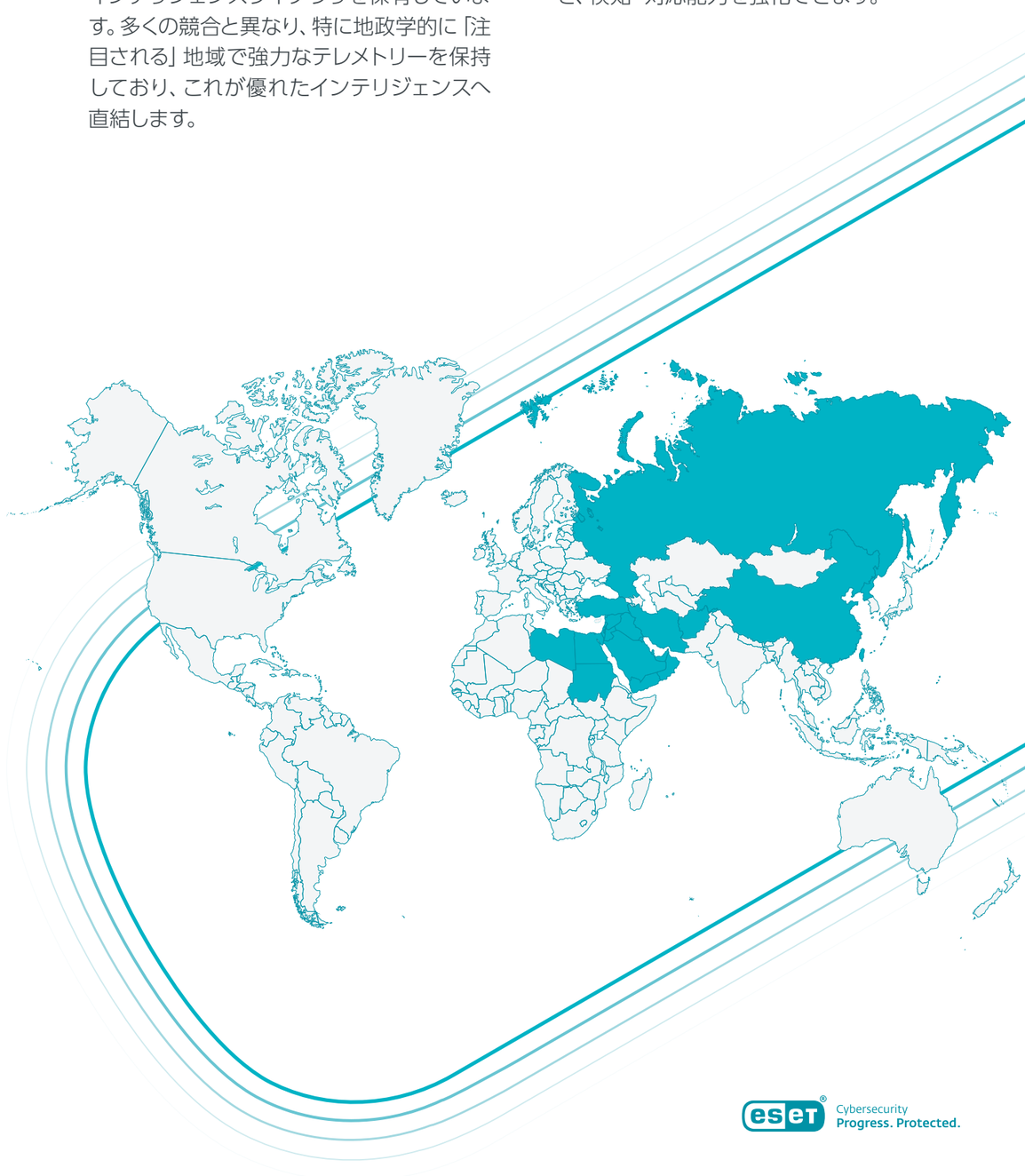
ESETは35年以上にわたり非公開企業として無借金経営を続け、継続的な成長を実現してきました。当社の成功はAIを活用した「予防ファースト」アプローチと人間の専門知識に支えられています。その中心となるのは、広範なR&Dネットワークと業界で高く評価される研究者たちが主導する独自のグローバル脅威インテリジェンスです。

既に高度なCTIソリューションを導入している場合でも、ESETを統合することで卓越した価値が得られます。当社の包括的な脅威インテリジェンスフィード、APTレポート、eCrimeレポートによって、新たな脅威に常に先んじ、既存の防御を強化できます。

ESETの独自性の 高いテレメトリー

ESETは長年にわたるグローバル展開により、数百万のノードから収集した豊富で多様なインテリジェンスライブラリを保有しています。多くの競合と異なり、特に地政学的に「注目される」地域で強力なテレメトリーを保持しており、これが優れたインテリジェンスへ直結します。

ESETのテレメトリーを活用することで、高品質で行動可能な脅威インサイトにアクセスでき、検知・対応能力を強化できます。

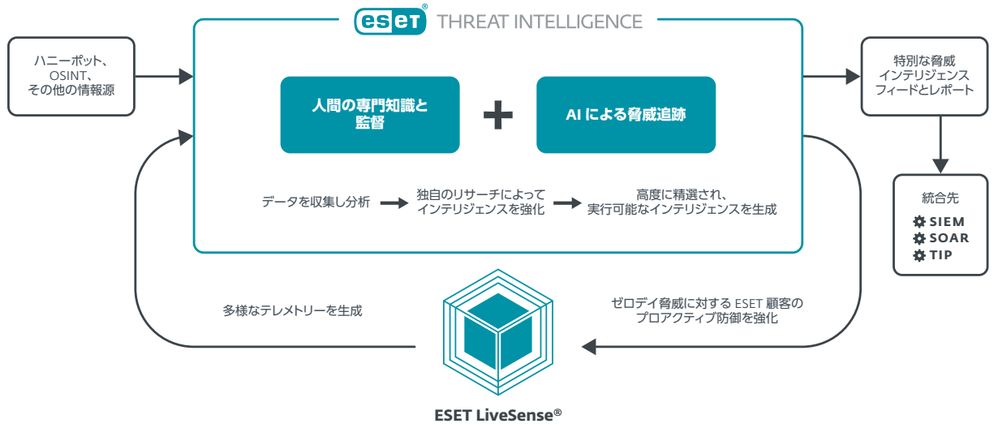


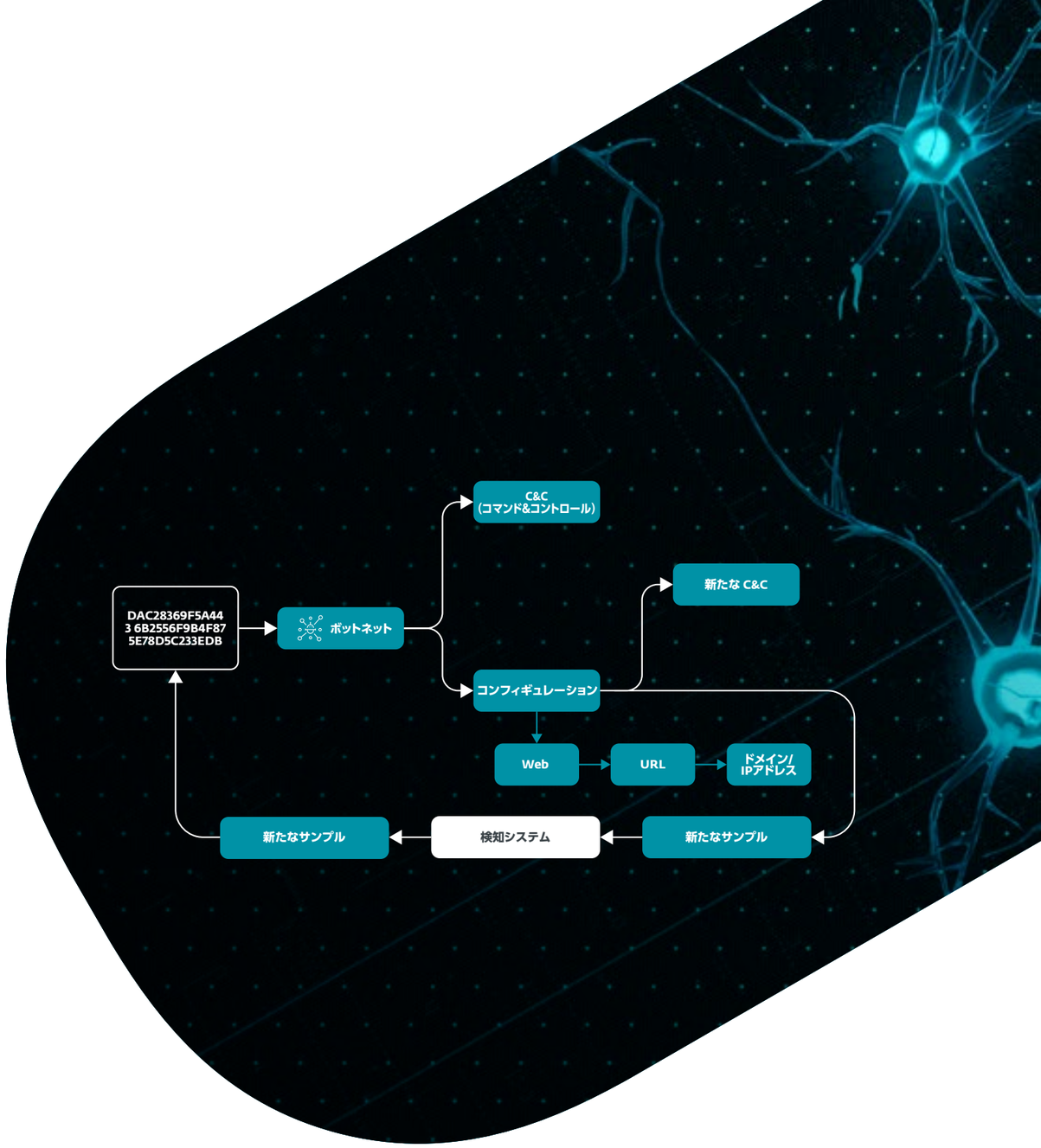
Cybersecurity
Progress. Protected.

行動につながる独自の強化インテリジェンス

脅威インテリジェンスは、単にインジケーターを収集してまとめることではありません。ESETでは高度な技術と専門知識を用い、インテリジェンスの加工・強化を行い、ビジネスに真の価値を提供します。

1. **包括的テレメトリー:** ESET LiveSenseによる多層防御技術から広範で深いデータを収集。
2. **多様な収集方法:** ハニーポッド、OSINT、センサー、ウェブクロール（クリア/ディープ）、脅威追跡など幅広いデータ取得源。
3. **高度な処理:** 収集データは強力なバックエンドとAIにより自動分類・分析。
4. **専門家による分析:** TIアナリストが脅威アクターの動機・TTPs・ツールを継続的に分析し、精度を向上。





サンプルの高度分析でインテリジェンスを強化テレメトリーで取得したサンプルは、
詳細な振る舞い分析および構造分析を実施。
これにより、追加の有用なインジケーターを抽出し、
脅威インテリジェンスをさらに強化します。

eset Cybersecurity Progress. Protected.

詳細な APT レポートにより高度なセキュリティを実現

組織のセキュリティ体制を強化するため、当社のAPTレポートは簡潔で実践的な言葉で書かれています。これらのレポートは、マルウェアキャンペーン、その配布手法、関与するアクターに関する詳細な洞察を提供します。さらに、当社のMISPサーバーおよびAIアドバイザーへアクセスできるほか、ESETのトップ脅威インテリジェンス専門家によるライブセッションを予約することも可能です。これらにより、包括的で実用的なインテリジェンスを得ることができます。

最高レベルのリサーチを、あなたの手元に

当社の研究チームは、受賞歴を持つ WeLiveSecurity ブログのおかげで、デジタルセキュリティ業界で広く知られています。チームが作成する優れた調査結果や APT アクティビティのサマリーに加えて、さらに詳細な情報も提供しています。また、ESET のお客様は、すべての WeLiveSecurity コンテンツを一般公開前に先行して閲覧できる特典を得られます。

行動につながる、精選されたコンテンツ

レポートは、「何が起きているのか、そしてなぜ起きているのか」を理解するための豊富なコンテキストを提供します。これにより、組織は今後起こりうる事態に事前に備えることができます。さらに重要なのは、当社の専門家が内容を分かりやすく伝えることを徹底している点です。

重大な意思決定を迅速に

これらすべての情報は、組織が重要な意思決定を行ううえで役立ち、デジタル犯罪との戦いにおいて戦略的な優位性をもたらします。インターネットの「闇側」で何が起きているのかを理解できるようになり、組織が迅速に内部対応の準備を進めるために必要な重要なコンテキストを提供します。

ESET アナリストとのコンタクト

APTレポートのPremiumパッケージをご利用のすべてのお客様は、月あたり最大4時間までESETのアナリストにコンタクトできます。これにより、特定のトピックをより詳細に議論したり、未解決の課題について専門家の支援を受けたりすることが可能になります。

ESET AI ADVISOR

ESET AI Advisorは、先進的な AI技術とAPT分析の専門知識を活用し、サイバー攻撃に対するオンデマンドのインサイトと防御策を提供します。チャットボットとして利用でき、セキュリティに関する問い合わせに対応するほか、APTの要約提供、IoCやTTPの整理、さらには迅速な脅威理解と対策に役立つYARAルールの生成も行います。

		APT Reports	APT Reports Advanced	APT Reports Ultimate
隔週アクティビティサマリー	対象となる APTグループの活動を要約したレポート(月 2 回)	✓	✓	✓
脅威分析レポート	主要脅威に関するカスタムまたは定期的な技術分析（年間約 30 回）	✓	✓	✓
月次概要	脅威のエグゼクティブサマリーを含む月次情報まとめ	✓	✓	✓
月次ダイジェスト	月内レポートや事象の索引とエグゼクティブサマリー	✓	✓	✓
WeLiveSecurity 先行アクセス	脅威レポートおよび特定のWeLiveSecurity記事への先行アクセス	✓	✓	✓
APT IOC フィード	レポートに基づく IOCを含む STIX/TAXII フィードへの完全アクセス	✓	✓	✓
MISP サーバーアクセス	レポートに含まれるすべての情報を保持する ESET MISPサーバーへの完全アクセス	✗	✓	✓
ESET AI Advisor	利用可能な APTレポートに基づく洞察やサマリーを提供する ESET AI アドバイザーへのアクセス	✗	✓	✓
アナリストとのコンタクト	MS Teamsやメールなどでのアナリストとのコンタクト（準備時間含め月 4 時間まで、翌月繰越なし）	✗	✗	✓

eset Cybersecurity
Progress. Protected.

サイバー犯罪へ先手を打つ：インジケーターからインテリジェンスへ

ESET Threat IntelligenceのeCrimeレポートは、ランサムウェアや、より広範なサイバー犯罪に関する深い洞察を提供します。攻撃者が使用するツール、インフラ、収益化戦略について、ESETのグローバルな研究とテレメトリーに基づく可視性を得ることができます。IoCの提示にとどまらず、プロアクティブな防御や戦略的な意思決定を強化するための、より広い文脈を備えた脅威インテリジェンスへとアクセスできます。

ESET eCrimeレポートが選ばれる理由

プロアクティブ防御

eCrimeグループそのものだけでなく、実際に攻撃を実行しているアフィリエイトに関するインテリジェンスも取得できます。彼らがどのように動き、次に何をしようとしているのかを把握することで、常に一歩先を行くことができます。

運用効率

実際のインシデントに基づいた明確で精選されたインサイトを活用し、ノイズを排除。これにより、脅威の検知が容易になり、対応の迅速化や、最も重要な領域にハンティングを集中させることが可能です。

独自の可視性

一般公開されている脅威フィードを超え、マネタイズ手法、インフラ、アフィリエイトの実際の挙動に関する深い洞察を得られます。これらはすべて、ESETのグローバルなテレメトリーと研究を基盤としています。

		eCrime Reports	eCrime Reports Advanced
アクティビティサマリー 月次	○ 最新のランサムウェアおよびインフォスティーラーのキャンペーンを明確で戦略的なインサイトとして要約 ○ ターゲット、攻撃の進行方法、失敗した点 ○ レジリエンス強化のための主要な教訓、IoC、ガイダンス	✓	✓
技術分析 随時	○ 特定の脅威アクター（例：FIN7）への詳細な分析 ○ 攻撃チェーン全体：初期アクセスからデータ窃取まで ○ 攻撃者の戦術、ツール、インフラ、MITRE ATT&CK®マッピング、IoC	✓	✓
月次ダイジェスト 月次	○ 最近のランサムウェア / インフォスティーラー活動に関するエグゼクティブ向け概要 ○ 主要トレンド、注目すべきインシデント、新たな脅威 ○ 経営層が複雑な技術要素なしにリスク評価や優先順位づけを行うのに役立つ	✓	✓
eCrimeフィード	○ ランサムウェアグループ、そのアフィリエイト、 ○ インフォスティーラーキャンペーンに関する新鮮で精選された IoC ○ 標準 STIX/TAXII 形式で提供	✓	✓
ESET AI Advisor	○ eCrime インサイトを用いて脅威関連質問に回答 ○ インシデントや攻撃者の行動を解釈する支援 ○ アナリストおよび意思決定者に対し、脅威インテリジェンスを即座に利用可能な形で提供	✗	✓
MISP サーバーアクセス	○ 精選された脅威インテリジェンスとの直接統合 ○ 自動 IoC 取り込みで防御を強化 ○ ワークフローを効率化し、検知速度向上とインシデント対応を支援	✗	✓

eset® Cybersecurity Progress. Protected.

明確で洗練されたデータフィード

ESET の独自テレメトリーによって、脅威状況の可視性を大幅に強化できます。当社は JSON や STIX 2.1 形式の高度に精選されたデータフィードを提供しており、SIEM、TIP、SOAR などのツールとシームレスに統合可能です。多くの TI ベンダーとは異なり、ESET はフィードの関連性を確保するために徹底したフィルタリングと評価を実施しています。これにより、必要な場合には既存のセキュリティシステムが自動的にアクションを実行でき、アナリストはグローバルな脅威情勢の包括的な把握が可能になります。

特長

- メタデータが豊富で詳細、かつ低い誤検知率を実現した精選データ
- 軽量・高関連性・重複排除済み・信頼度スコア付きのデータ
- ESET 研究者による高度なフィルタリングとインサイト
- 特にボットネットデータで市場をリード
- 適切に精選されているため、運用保守が容易
- リアルタイムで更新され、最新かつ重要度の高い IoC のみを提供

データフィードの種類

マルウェアデータフィード

新たに検出されたマルウェアサンプルに関するリアルタイムのインサイトを提供し、特性やIoCを含みます。ファイルハッシュ、タイムスタンプ、脅威タイプなどを通じ、悪意あるファイルを被害発生前にブロックできます。

ランサムウェアフィード

アクティブなランサムウェアファミリーと流通サンプルに関するリアルタイムデータを提供。侵害や高額な被害を防ぐためのプロアクティブなブロッキングが可能になります。

ボットネットフィード

ESETのボットネットトラッカーにより提供され、以下の3種類のサブフィードを含みます: これらは検出情報、ファイルハッシュ、最終通信時刻、ダウンロードファイル、IP、プロトコル、対象情報などを提供します。

APT IOC フィード

ESETの研究に基づく APT（高度持続的脅威）に関するインサイトを提供。内部MISPサーバーからエクスポートされ、APT レポートと連携しており、レポートの一部として、または単体フィードとして利用可能です。

望ましくないアプリ（不要アプリ・アドウェア）フィード

ESETは20年以上にわたる PUA（潜在的に迷惑なアプリ）分類の経験を持ち、精度と深みで他を圧倒します。アドウェアフィードでは、アクティブなアドウェアや類似の脅威に関するリアルタイムの洞察を提供し、影響が出る前にブロック可能です。

望ましくないアプリ（ツール悪用検知）フィード

攻撃者に悪用される正規ツール（例: RMM など）を追跡し、悪用を先回りして防ぎます。ノイズを抑えた低冗長データにより、効率よく脅威を把握できます。

Cybersecurity Progress. Protected.

ドメインフィード

悪意のあるドメインに関するデータを提供します。ドメイン名、IP アドレス、関連日時などを含み、ドメインは重大度に基づいてランク付けされます。これにより、リスクの高いドメインを優先的にブロックするなど、効果的に対応できます。

URL フィード

特定のURLを精選したフィードで、それぞれのURLとそのホスティングドメインに関する詳細情報を提供します。信頼性の高い情報のみを含み、検知理由も明確で人間が読みやすい形で説明されています。

IP フィード

悪意のある IP に関する実用的なデータを提供します。構造はドメインフィードや URLフィードと同様で、高危険度 IP のブロック、低リスク IP の監視、追加データを用いたさらなる調査などに活用できます。

Android 脅威フィード

流行している Android脅威とそのIoC（侵害指標）に関するリアルタイム情報を提供します。ESET のテレメトリーに基づき、ほぼリアルタイムで更新され、毎日重複が排除されます。

Android インフォスティーラーフィード

Android脅威フィードの中に含まれる専門特化フィードで、最新のインフォスティーラーに関するサンプルや関連データを提供します。アクティブなファミリーの可視化が可能で、被害が出る前にプロアクティブにブロックできます。

詐欺 URL フィード

詐欺サイトに関するリアルタイムデータを提供します。ECサイト詐欺、投資詐欺、出会い系詐欺、暗号資産詐欺などが含まれます。ESETの全URLソースに基づきほぼリアルタイムで生成され、24時間ごとに重複排除されます。

クリプト詐欺フィード

暗号資産関連の詐欺に関するリアルタイムデータ（ドメイン、URL、関連情報）を提供します。ESETの豊富なテレメトリーに基づき、早期で絞り込まれたインサイトにより、脅威を先回りしてブロックし、資産保護を可能にします。

悪意あるメール添付フィード

メールは攻撃の主要ターゲットです。このフィードは、ESETの広範なメールスキャンテレメトリーを基に、悪意あるメール添付に関するリアルタイムデータを提供します。

フィッシング URL フィード

ESETの専用データベースから、アクティブなフィッシング URLに関するリアルタイムのインテリジェンスを提供します。継続的に更新され、毎日重複が排除されるため、機密情報を盗む前に不正サイトを検知・ブロックできます。

スミッシングフィード

SMSを用いたフィッシング（Smishing）に関する、ドメイン・URL・関連インジケーターを含むタイムリーな情報を提供します。ESET のテレメトリーに基づき、ほぼリアルタイムで更新され、重複は毎日排除されます。

SMS 詐欺フィード

SMSを悪用した詐欺に対抗するため、悪意あるドメインや URLに関するリアルタイムデータを提供します。ESET のテレメトリーを基盤に、ほぼリアルタイムで更新および毎日の重複排除を行い、高度化する脅威の識別とブロックを支援します。

eCrime フィード

サイバー犯罪オペレーションおよびマルウェアを用いたeCrimeに関する、明確で行動可能なデータを提供します。ランサムウェアグループやそのアフィリエイト、インフォスティーラーキャンペーンなど、幅広い攻撃を継続的に監視し、組織が受動的対応からプロアクティブな防御へと移行できるよう支援します。

ESET Threat Intelligence の力を体感してみませんか？

営業担当にデモの実施についてご依頼ください。
ESET Threat Intelligence が組織にもたらす
比類ない価値 をぜひご確認ください。
お客様のサイバーセキュリティ防御をどのように
強化できるか、私たちがお見せします。

デモの依頼までは不要という段階でしたら、
ESET Threat Intelligence ポータルで
プレビューアカウントを作成し、
フィードや APT レポートをお試しください。

Cybersecurity Progress. Protected.

ESETについて

プロアクティブな防御。予防によるリスク最小化。

既知・未知のサイバー脅威――標的型攻撃、ゼロデイ脅威、ランサムウェア、フィッシングなど――に、常に一歩先んじるために。ESET は AI ネイティブの「予防ファースト」アプローチによって、AI の力と人間の専門知識を融合させ、シンプルで効果的な保護を提供します。

30年以上の自社グローバル脅威インテリジェンスに裏付けられた、科学的に磨かれた最高レベルのセキュリティを提供します。ESETの広範なR&Dネットワークは、業界で高く評価される研究者によって主導され、受賞歴のあるクラウドファーストのサイバーセキュリティプラットフォームを支えています。

ESETのソリューションは高いカスタマイズ性を備え、ローカルサポートに対応し、システムパフォーマンスへの影響も最小限です。

ESETの実績

10億以上
保護中のインターネットユーザー

50万以上
法人顧客

178
提供国

11
グローバル研究開発センター

導入顧客の一例

MITSUBISHI MOTORS
Drive your Ambition

2017 年から ESET を利用
9,500 台以上のデバイスを保護

BVB 09

2019 年から ESET を利用
1,200 台のデバイス &
2,700 のメールボックスを保護

Canon
Canon Marketing Japan Group

2016 年から ESET を利用
23,000 台以上のデバイスを保護

2008 年から
ISP セキュリティパートナー
2 百万以上のお客様をサポート

業界からの評価

SE LABS ®
AWARDS
Enterprise Endpoint (Windows)
WINNER 2025

Best Enterprise Endpoint Award、
Best Small Business Endpoint
Awardを受賞

Gartner
Peer Insights
Customers' Choice 2026

Gartner® Peer Insights™
「Voice of the Customer」
Endpoint Protection Platforms
レポート 2026 にて、
Customers' Choiceに選出

FROST & SULLIVAN

Frost Radar: Endpoint Security 2025 にて
成長とイノベーションに優れた
リーダー企業 として選出