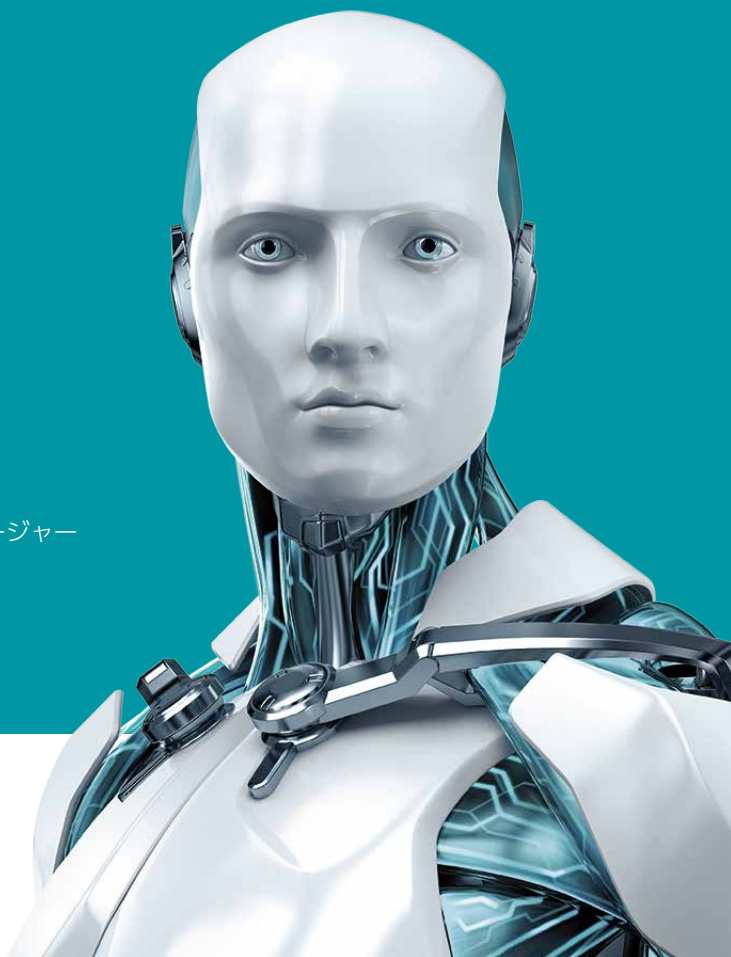
ESET TECHNOLOGY

多層型アプローチの概要とその有効性

著者：
Jakub Debski - 最高製品責任者（CPO）
Juraj Malcho - 最高技術責任者（CTO）
Peter Stančík - セキュリティリサーチ & アウェアネス担当マネージャー

ドキュメントバージョン：1.3



ENJOY SAFER TECHNOLOGY™

目次

本書の目的

本書では、基本的なウイルス対策をはるかに超える機能を提供するために、ESET がどのような方法で多層型テクノロジーを使用しているのかをまとめています。理解しやすいよう、特定の問題の解決にどのレイヤーが関係しているかや、それらがユーザーにどのようなメリットをもたらすかを説明しています。

次世代のセキュリティソリューション

定評のあるウイルス対策企業のほとんどは、ウイルスやマルウェアに悩まされている人々を助けたいという願いから誕生しており、そうした企業のテクノロジーは、セキュリティベンダーが対策を開始したばかりの幅広い脅威に対応するために進化しました。現在、ウイルス対策はコモディティビジネスだと受け取られています。そしてセキュリティは、（セキュリティが実際に何を意味するかが理解されているかどうかは不明ですが）誰もが共感できるテーマとなっています。最近では、「次世代」企業を自称する新しい企業（ESET が呼ぶところの「ポスト真実：客観的事実より感情に訴えかける」企業）が急増しています。このような企業は通常、マルウェア対策ソリューションの開発経験がほとんどありませんが、既存のベンダーを「過去の物」として排除しつつ、自社ソリューションを「革新的」だと売り込んでいます。しかし、その主張の多くは誤解を招くものであり、皮肉なことに、そうした企業の検出機能は通常、定評のあるベンダーから供給された検出エンジンに依存しています。なぜなら、現在市場に参入している数十社のソリューションプロバイダーのうち、独自のコア検出テクノロジーを開発できる経験と能力を備えているものはほとんどありません。ESET のテクノロジーはすべて独自のものであり、社内開発されています。

ただし、「既存のマルウェア対策業界の有効性を低下させている」と新規参入企業が主張する静的シグネチャによる単純な検出は、最新のセキュリティ製品が最新の脅威に対して展開している一連のテクノロジーのほんの一部に過ぎません。

複数の脅威に対抗する多層防御

現在もビジネスを継続している既存のマルウェア対策企業は、最新の脅威に対処するために進化することで市場シェアを維持しています。

現代の脅威は静的ではなく、2000 年代初期には脅威は大きく進化しました。1990 年代のテクノロジーをベースにしているだけでは、今日の脅威に効果的に対抗することはできません。現代のマルウェアとの戦いは、熟練した金銭目当ての攻撃者集団が相手のいたちごっこにほかなりません。そのため、セキュリティ企業が効果的なソリューションを提供するためには、最新のマルウェアの検出やブロックが可能なさまざまなレイヤーを追加して、積極的に製品を絶えず改良する必要があります。一カ所だけを保護する、あるいは 1 つの防御策を導入するだけでは不十分です。

それが、ESET がアンチウイルスベンダーから IT セキュリティ企業へと進化した理由の 1 つです。

複数の脅威、複数のプラットフォーム

最近では、マルウェアが実行されるプラットフォームは Microsoft オペレーティングシステムだけではありません。攻撃者は未開拓のプラットフォームとプロセスを掌握しようとしているため、攻撃対象は急速に変化しています。

- 制御して、悪意のあるアクティビティを実行させられるものはすべて、攻撃に使用される恐れがあります。
- 実行コードを実行して外部データを処理するものはすべて、悪意のあるデータに乗っ取られる恐れがあります。

Linux サーバーは以前から攻撃者にとって主要な標的であり（Operation Windigo、*Linux/Mumblehard*）、OS X を実行する Mac は過去最大のボットネットの 1 つのホストとなっており（*OSX/Flashback*）、スマートフォンは標的になりやすく（*Hesperbot*）、そしてルーターに対する攻撃は深刻な脅威になりつつあります（*Linux/Moose*）。ルートキットはハードウェアに迫りつつあり（ファームウェアへの攻撃、*UEFI rootkit* の使用）、仮想化によって新たな攻撃経路が誕生しています（Bluepill、VM エスケープの脆弱性）。また、Web ブラウザやその他のアプリケーションはオペレーティングシステムと同じくらい複雑化しており、そのスクリプトメカニズムが攻撃に悪用されるケースも増えています（*Win32/Theola*）。

さまざまな拡散経路

過去を振り返ってみると、世界初のマルウェアは、システム内で自己複製を行うプロセスとして登場しました。次に、PC から PC へと広がるファイル感染型やディスク感染型のウイルスが出現しました。インターネットがほぼ世界中で使用されるようになったことで、マルウェアが配布される方法も格段に増えました。

悪意のあるオブジェクトは、電子メールの添付ファイルやリンクとして送信されたり、Web ページからダウンロードされたり、ドキュメント内のスクリプトによってドロップされたり、リムーバブルデバイスで共有されたり、脆弱な認証機能やパスワードが悪用されてリモートで展開されたり、エクスプロイトによって実行されたり、あるいはソーシャルエンジニアリングの罠に掛かったエンドユーザーによってインストールされたりします。

マルウェアの設計

ティーンエイジャーがいたずらで、あるいは注目を集めようとしてマルウェアを作成していた時代は、とうに終わっています。今やマルウェアは金儲けや情報の窃取を目的に作成されており、犯罪者そして政府がマルウェア開発に多額の資金を投入しています。

検出されにくくなることを期待して、マルウェアはさまざまなコンパイラーとインタープリタ型言語を使用した、さまざまなプログラミング言語で記述されています。コードは、検出と分析を困難にする目的で、カスタマイズされたソフトウェアを使用して難読化され保護されています。不審なアクティビティを検出するように設計された動作監視を回避するため、また、削除を阻止してシステムの常駐するために、クリーンなプロセスにコードが注入されます。スクリプトは、アプリケーションコントロール技術を迂回するために使用され、メモリ内に潜むマルウェアはファイルベースのセキュリティをバイパスします。

保護機能をすり抜けるためには、攻撃者は何千種類もの大量のマルウェアをインターネットに送り込みます。マルウェアを少数のターゲットに配信して、セキュリティ企業の注目を集めないようにする、という方法もあります。検出を回避するために、正規の企業から盗まれた証明書を使用して、クリーンなソフトウェアコンポーネントを悪用したり、悪意のあるコードに署名したりします。そのため、不正なコードの検出は以前よりも難しくなっています。

また、ネットワークレベルでは、マルウェアが命令を送信し、感染先のシステムからデータを受信するために、ハードコードされた C&C サーバーを使用する頻度は下がっています。ピアツーピアネットワークを使用したボットネットの分散制御が一般的になっており、暗号化された通信が原因で攻撃の識別が困難になっています。ドメイン生成アルゴリズムは、既知の URL のブロックに基づいた検出の効果を低下させます。

評判の高い正規 Web サイトが乗っ取られることも、さらには正規の広告サービスが悪意のあるコンテンツを表示するために使用されることもあります。

重要

攻撃者が検出を回避する方法は多数あるため、単純な単層型ソリューションでは保護を提供するのに十分ではありません。ESET は、最高レベルのセキュリティを確保するためには、持続的でリアルタイムの多層防御が必要であると考えています。

ESET のコアテクノロジーがもたらすメリット

ESET のスキャンエンジンは ESET 製品の中心であり、その基盤テクノロジーは「昔ながらのアンチウイルス」から継承されたものですが、大幅に拡張および強化されており、最新の脅威に対応できるよう絶えず開発されています。

スキャンエンジンの目的は、潜在的マルウェアを特定し、検査したコードが悪意のあるものである可能性を自動的に判断することです。

長年、ESET のパフォーマンスはスマートアルゴリズムと手動で作成されたアセンブリコードに基づいており、製品に統合されたサンドボックステクノロジーを使用した詳細なコード分析が原因のパフォーマンスボトルネックに対処していました。しかし、このアプローチはすでに改善されています。現在、パフォーマンスを最大化するため、インタープリタ型エミュレーションと併せてバイナリ変換を使用しています。

製品にサンドボックスが内蔵されている場合、仮想化環境でプログラムを実行するには、コンピュータのハードウェアとソフトウェアのさまざまなコンポーネントをエミュレートする必要があります。これらのコンポーネントには、メモリ、ファイルシステム、オペレーティングシステム API、および CPU（中央処理装置）を含めることができます。

過去には、カスタムのアセンブリコードを使用して CPU がエミュレートされていました。ただし、それは「解釈されたコード」であるため、各命令を個別にエミュレートする必要がありました。バイナリ変換では、エミュレートされた命令を実際の CPU でネイティブに実行します。特にコード内のループの場合、これは何倍も速い方法です。複数のループを導入するのは、セキュリティ製品や研究者による分析を回避する対策が適用されているすべての実行ファイルに共通する手法です。

ESET 製品は、埋め込まれた悪意のあるコンポーネントを正確に検出するために、数百の異なるファイル形式（実行ファイル、インストーラ、スクリプト、アーカイブ、ドキュメント、バイトコード）を分析します。

次ページの図は、さまざまなコア ESET テクノロジーと、システムのライフサイクル中に脅威の検出やブロックを実行できるタイミングと方法の概要を示しています。

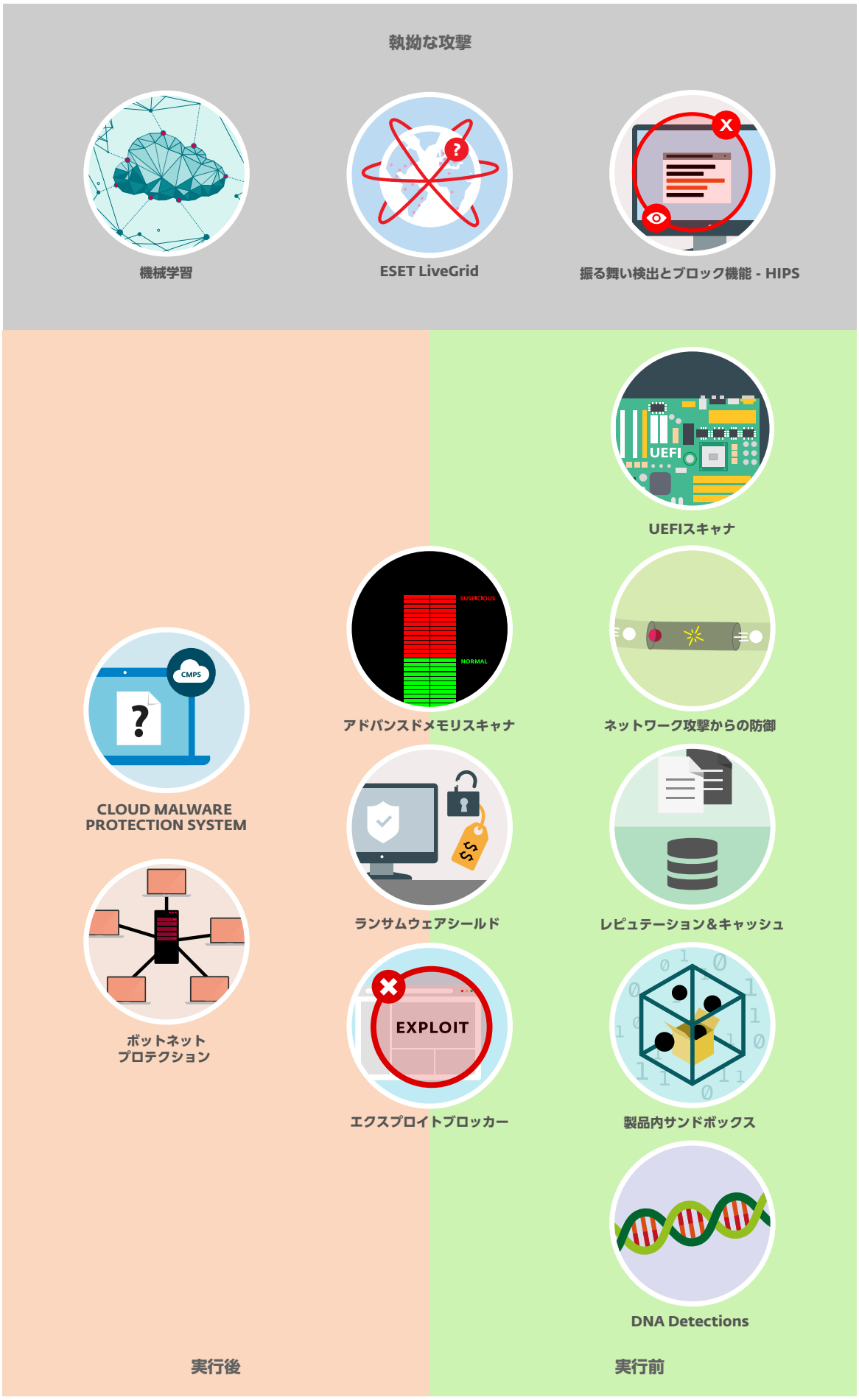
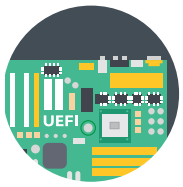


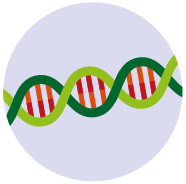
図1：ESET の保護レイヤー



UEFI スキャナ

ESET は、Unified Extensible Firmware Interface（UEFI）を保護する専用レイヤーをソリューションに追加した最初のインターネットセキュリティプロバイダーです。ESET の UEFI スキャナは UEFI 仕様に準拠し、プリブート環境のセキュリティをチェック・強化します。ファームウェア内の悪意のあるコンポーネントを検出し、ユーザーに報告するように設計されています。

UEFI は、1970 年代半ばからコンピュータに使用されていた Basic Input/Output System（BIOS）に代わる、デバイスのオペレーティングシステムとそのファームウェアの中間に位置するソフトウェアインタフェースの標準仕様です。UEFI はレイアウトが適切に文書化されているおかげで、分析および解析がしやすく、開発者はファームウェアの拡張機能を開発できるようになりました。しかし、マルウェア開発者や攻撃者にも UEFI を悪意のあるモジュールに感染させる機会を与えることにもなりました。



DNA Detections

検出タイプは、非常に特殊なハッシュ値（たとえば、特定の悪意のあるバイナリまたはマルウェアの特定のバージョンを対象として、統計を取ったりヒューリスティック検出したマルウェアの検出名をより正確なものに変更したりする上で有用なハッシュ値）から、**マルウェアの特性と属性まで多岐にわたります**。

従来のウイルス対策製品で使用されていたパターンマッチングは、簡単なコード改ざんや難読化技術の使用によって容易にバイパスできます。しかし、オブジェクトの動作を変更するのはそれほど簡単ではありません。

ESET DNA Detections は、この原理を活用するように設計されています。ESET は、コードを詳細に分析し、その動作を行っている「遺伝子」を抽出します。このような**動作遺伝子には、IOC（セキュリティ侵害の痕跡情報）よりもはるかに多くの情報が含まれており**、いわゆる「次世代」ソリューションはシグネチャ検出に「取って代わる優れた方法」だと主張しています。ESET の動作遺伝子は、DNA Detections の構築に使用されています。DNA Detections は、疑わしいコードが（ディスク上にあるか実行中のプロセスメモリ内にあるかどうかにかかわらず、）そのコードを評価する際に使用されます。

さらに、ESET のスキャンエンジンは、異常検出に使用される数多くの識別遺伝子を抽出します。正規のものと思われないものはすべて、潜在的に悪意のあるものだと判断されます。

調整可能なしきい値レベルと一致条件に応じて、DNA Detections は、特定の既知のマルウェアサンプル、既知のマルウェアファミリの新しい亜種、または悪意のある動作を示す遺伝子を含んだ初検出または未知のマルウェアを特定できます。つまり、**適切に作成された DNA 動作記述が 1 つあれば、関連する数万のマルウェア亜種を検出**し、既知のマルウェアや過去に確認されたマルウェアだけでなく、**新しい未知の亜種も** ESET のアンチウイルスソフトウェアで検出できます。

さらに、自動クラスター形成と悪意のあるサンプルセットへの機械学習アルゴリズムの適用により、ESET のスキャンエンジンによって検出される新しい悪意のある遺伝子と動作パターンを特定できます。このような遺伝子は、膨大なホワイトリストセットと簡単に照合できるため、誤検出が防止されます。

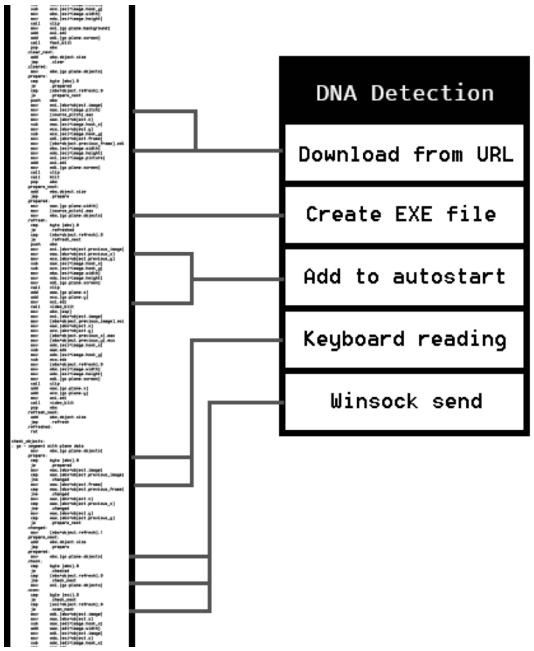


図 2：DNA Detections の例

機械学習

ESET は 1990 年代から脅威の検出とブロックに機械学習アルゴリズムを使用しています。また、1998 年にはすでにニューラルネットワークを製品に組み込みました。それ以来、この前途有望なテクノロジーを独自の多層型テクノロジー全体に実装してきました。

これには、機械学習に基づくモデルを使用して、クラウド接続の有無にかかわらず効果的に機能する DNA Detections が含まれます。機械学習アルゴリズムは、受信したサンプルを最初にソートして分類したり、想像上の「サイバーセキュリティマップ」に配置したりする際に不可欠な部分でもあります。

しかし、何よりも重要なのは、ESET が ESET Augur と呼ばれる独自の機械学習エンジンを開発したことです。ESET Augur は、ニューラルネットワーク（ディープラーニングや長期短期記憶など）と厳選された 6 つの分類アルゴリズム群を組み合わせて使用します。これにより、統合された出力が生成され、受信したサンプルを「クリーン」、「悪影響を及ぼす可能性がある」、または「悪意がある」と正しくラベル付けすることができます。

ESET Augur エンジンは、DNA、サンドボックス、メモリ分析などの他の保護テクノロジーや動作特性の抽出機能と連携するようにチューニングされているので、最高の検出率を実現し、誤検出を最小限に抑えます。

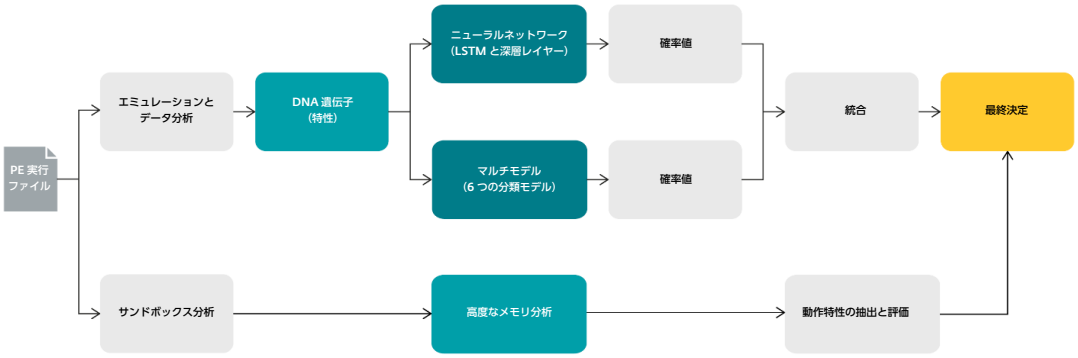


図 3：ESET の機械学習エンジン Augur の仕組み

ESET LiveGrid

クラウドシステムを使用して保護を提供する最も簡単な方法は、ハッシュを使用した正確なブラックリスト登録です。この方法はファイルと URL のどちらでも有効ですが、ブロックできるのはハッシュに正確に一致するオブジェクトに限られます。この制約があったことが、ファジーハッシュの発明につながりました。ファジーハッシュでは、オブジェクトのバイナリ類似性が考慮されます。これは、類似オブジェクトのハッシュは同じであるか類似しているためです。

ESET によって、ファジーハッシュは次の段階へと進みました。ESET はデータのハッシュ化は実行しませんが、DNA Detections で説明されている動作のハッシュ化は実行します。DNA ハッシュを使用することで、マルウェアのさまざまな亜種を即座にブロックできます。右の図をご覧ください。

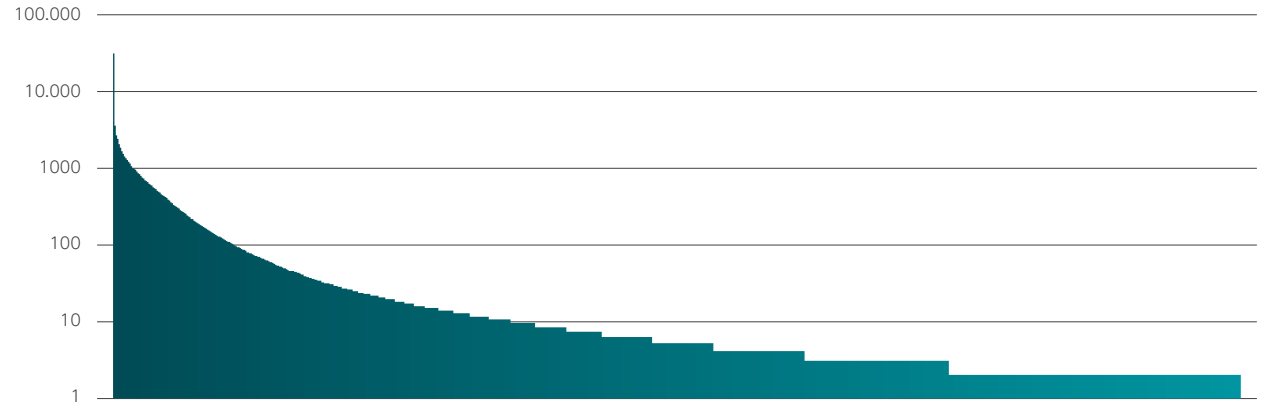


図 4：個々の DNA ハッシュ（x 軸）によって検出された一意のファイル（y 軸）の数。

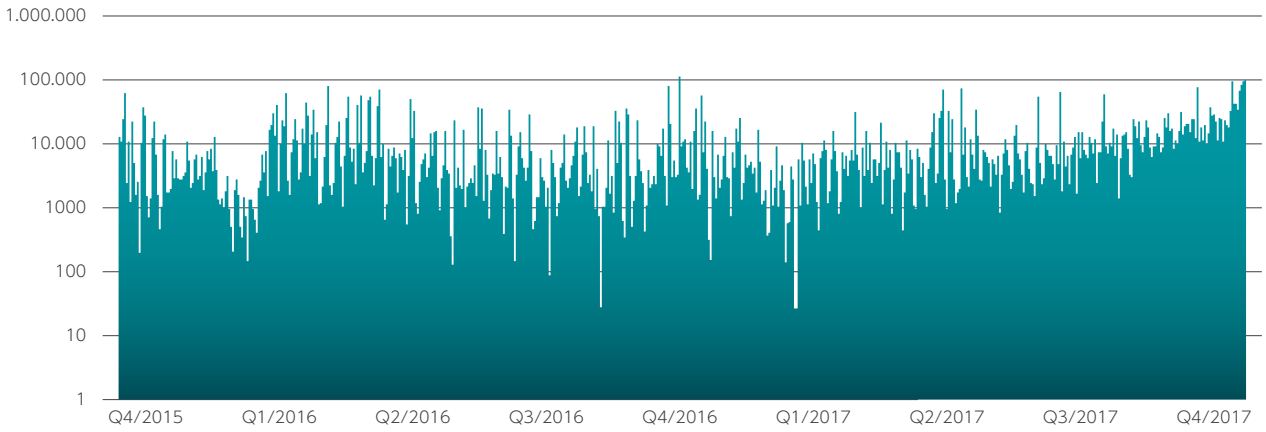


図 5：1 日あたりの DNA ハッシュ（x 軸）によって検出された一意のファイル（y 軸）の数。

Cloud Malware Protection System

ESET の Cloud Malware Protection System は、ESET のクラウドベースシステムである ESET LiveGrid に基づいたテクノロジーの 1 つです。未知の、悪意のある可能性のあるアプリケーションやその他の脅威を監視し、ESET LiveGrid フィードバックシステム経由で ESET クラウドに送信します。**収集したサンプルを、自動的にサンドボックス内で解析し動作を分析します。**悪意ある特性が確認された場合、自動的に検出されます。ESET ユーザーは、次回の検出エンジンの更新を待つことなく、ESET LiveGrid レピュテーションシステムを介して、自動検出されたマルウェアについて知ることができます。このメカニズムの所要時間は通常 20 分未満であるため、定期的な検出がユーザーのコンピュータ配信される前であっても、新たな脅威を効果的に検出できます。

ESET Cloud Malware Protection System の目的は、ユーザーにブラックリストを瞬時に提供することだけではありません。サンプル送信プロセスへの参加をユーザーが決定した場合、レピュテーションが疑わしい新しいサンプルが特定されるたびに、そのサンプルは ESET に送信され、詳細な分析にかけられます。ユーザーが Cloud Malware Protection System を最大限に活用するには、ESET LiveGrid フィードバックシステムも併せて有効にする必要があります。これにより、レピュテーションが疑わしい不審なサンプルを収集して、詳細な分析を行うことができます。

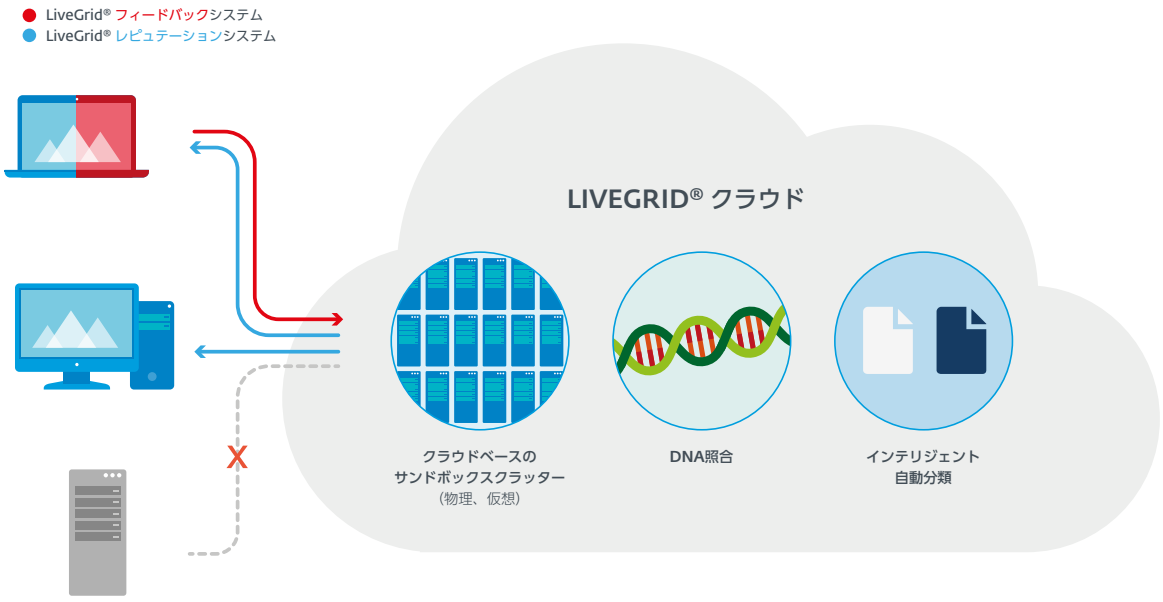


図 6：ESET Cloud Malware Protection System

レピュテーション&キャッシュ

ファイルや URL などのオブジェクトを検査する場合、ESET 製品はスキャンの実行前にローカルキャッシュ（ESET Endpoint Security ではローカルキャッシュに加えて **ESET 共有ローカルキャッシュ**）内に既知の悪意のあるオブジェクト、またはホワイトリストに登録されている無害なオブジェクトがないかを確認します。これにより、**スキャンのパフォーマンスが向上**します。

その後、**レピュテーションシステムに対して、オブジェクトレピュテーションのクエリ**（そのオブジェクトがすでに別の場所で確認され、悪意のあるオブジェクトか否かの分類が済んでいるかどうか）**が実行**されます。これにより、**スキャン効率が向上し、ユーザーとの迅速なマルウェア情報の共有が実現**します。

URL ブラックリストを適用して評判をチェックすることで、ユーザーが悪意のあるコンテンツやフィッシングサイトにアクセスするのを防止します。

振る舞い検出とブロック - HIPS

ESET の HIPS（ホストベースの侵入防止システム）はシステムアクティビティを監視し、事前定義されたルールセットに基づいて不審なシステム動作を認識します。このタイプのアクティビティが特定されると、HIPS の自己防衛メカニズムが、問題を起こすプログラムやプロセスの悪影響及ぼす可能性のあるアクティビティを阻止します。ユーザーは、デフォルトのルールセットの代わりにカスタムのユーザー定義ルールを設定できます。ただし、これにはアプリケーションおよびオペレーティングシステムに関する高度な知識が必要です。

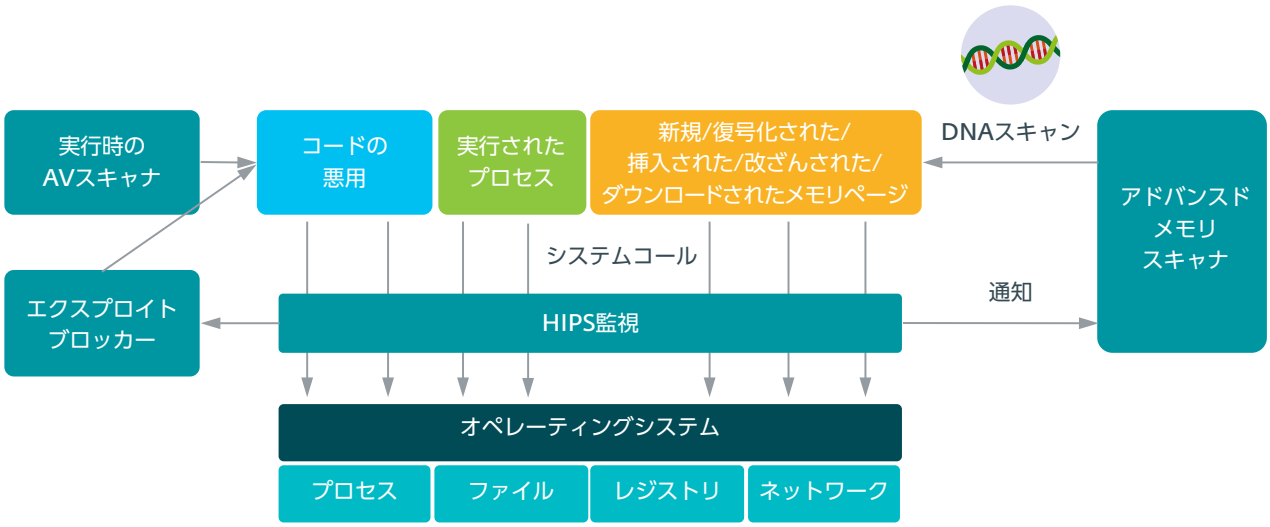
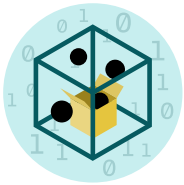


図 7：ESET の動作検出の仕組み



製品内サンドボックス

ESET の DNA 検出機能は 2 つに分割されています。そのおかげで、プロセス全体が理解しやすくなっています。この方法は、1995 年に最初のエミュレータが製品に導入された際に始まったもので、有名なゲーム Doom をこのエミュレータで実行することができました。目的は、DNA Detections で利用している動作メタデータを抽出することにあります。今日のマルウェアは難読化されていることが多く、可能な限り検出を回避しようとします。そこで ESET は、隠された動作の把握に取り組むことで、マルウェアの実際の動作を特定します。これにはバイナリ変換も使用しているため、マシンの速度が低下することはありません。

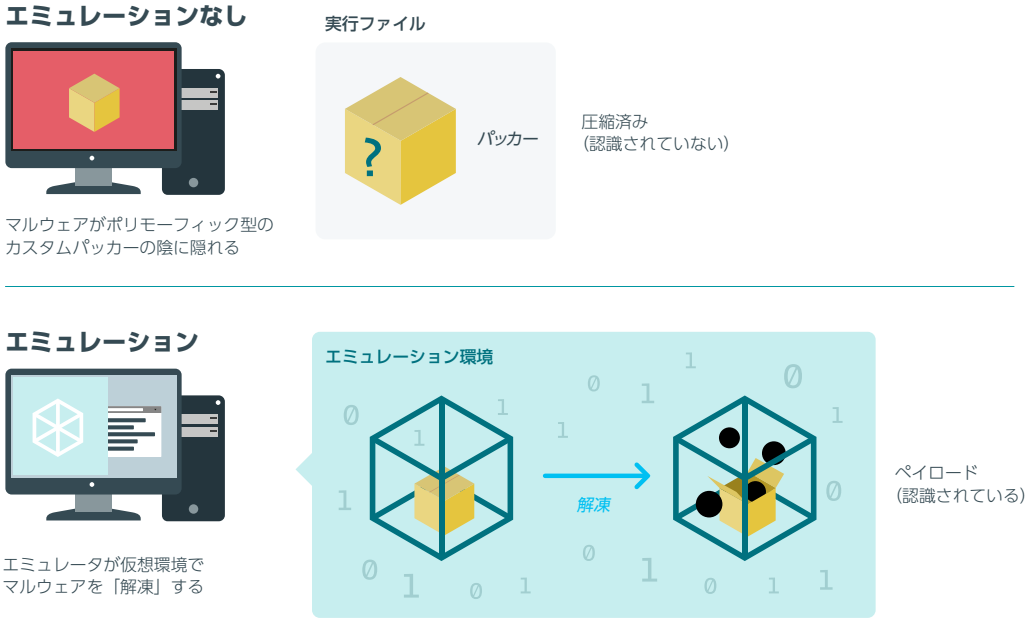
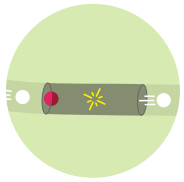
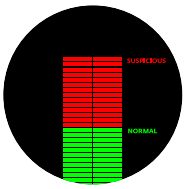


図 8：ESET が製品内サンドボックスを使用する理由



ネットワーク攻撃からの防御

ネットワーク攻撃からの防御は、**ファイアウォールテクノロジーの拡張機能であり、ネットワークレベルで既知の脆弱性の検出能力が強化**されます。*SMB*、*RPC*、*RDP* など、広く使用されているプロトコルによく見られる脆弱性を検出する機能を実装することにより、「マルウェアの拡散」、「ネットワーク実行攻撃」、および「パッチがリリース / 展開されていない脆弱性の悪用」に対する**保護を目的とした、重要なレイヤーが追加**されます。



アドバンスド メモリスキャナ

アドバンスドメモリスキャナは、**難読化や暗号化**の多用という現代のマルウェアの問題を効果的に**解決する ESET 独自のテクノロジー**です。

ランタイムパッカーやコードプロテクターで使用されることの多いこれらのマルウェア保護技術は、エミュレーションやサンドボックスなどの解凍技術を採用した検出アプローチにおいて問題の原因となります。さらに、チェックにエミュレータを使用する場合でも、仮想 / 物理サンドボックスを使用する場合でも、分析中にマルウェアが「悪意のあるマルウェア」に分類される動作を示すという保証はありません。

マルウェアを難読化すれば、すべての実行パスの分析を不可能にすることができます。また、マルウェアはコードに条件付きトリガーや時間トリガーを含めることや、存続期間中に非常に高い頻繁で新しいコンポーネントをダウンロードすることが可能です。これらの問題に取り組むために、アドバンスドメモリスキャナは悪意のあるプロセスの動作を監視し、メモリ内でクローキングを解除した後にスキャンします。これにより、実行前または実行時のプロアクティブなコード分析の従来の機能が補完されます。

また、クリーンなプロセスであっても、悪用やコードインジェクションによって突然悪意のあるプロセスに変化する可能性があります。上記の理由から、分析を一度だけ実行するだけでは十分ではありません。常時監視が必要であり、この役割をアドバンスドメモリスキャナが担います。**プロセスが新しい実行ページからシステムコールを行うたびに、アドバンストメモリスキャナは ESET DNA Detections を使用して動作コード分析を実行します。**

コード分析は、標準の実行メモリだけでなく、マルウェア作成者が動的分析の妨害で使用する .NET MSIL（Microsoft Intermediate Language）コードに対しても実行されます。スマートキャッシュの実装のおかげで、アドバンストメモリスキャナにはオーバーヘッドがほとんどなく、処理速度が目立って低下することはありません。

アドバンスドメモリスキャナはエクスプロイトブロッカーとの連携に優れています。エクスプロイトブロッカーとは異なり、アドバンスドメモリスキャナは実行後に行われます。つまり、悪意のあるアクティビティがすでに発生している可能性があります。しかし、攻撃者が他の保護レイヤーをバイパスした場合には、**最終手段として保護チェーンに介入**します。

さらに、高度なマルウェアには新しい傾向が見られます。現在の悪意のあるコードの一部は、「メモリ内でのみ」動作するものがあり、これらは従来の方法で検出可能な常駐型コンポーネントをファイルシステムに持っている必要がありません。

当初、このようなマルウェアの出現場所は、稼働時間が長いサーバーに限られていました。というのも、サーバーシステムは数か月、あるいは数年間連続して稼働するため、悪意のあるプロセスは再起動に耐えて生き延びる必要もなく、無期限にメモリ内で存続できるためです。しかし、最近の企業に対する攻撃ではこの傾向に変化が現れてきており、エンドポイントもこの攻撃方法のターゲットになっています。**このような悪意のある攻撃を検出できるのはメモリスキャンだけであり、ESET のアドバンスドメモリスキャナを使用することで、この新しい傾向に対応できます。**

エクスプロイトブロッカー

ESET テクノロジーは、さまざまなレベルの多様な脆弱性から保護します。ESET のスキャンエンジンは、不正な形式のドキュメントファイルに見られるエクスプロイトをカバーし、ネットワーク攻撃からの防御は通信レベルを対象としていますが、エクスプロイトブロッカーはエクスプロイトプロセス自体をブロックします。

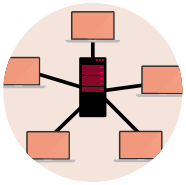
エクスプロイトブロッカーは、一般的に不正利用が可能なアプリケーション（ブラウザ、ドキュメントリーダー、電子メールクライアント、Flash、Java など）を監視し、特定の *CVE 識別子*を標的にするだけでなく、**その不正利用技術にも着目**しています。

各エクスプロイトはプロセスの実行における異常であり、ESET はエクスプロイト手法の存在を示す異常を探します。このテクノロジーは常に開発過程にあるため、新たな不正利用の手法をカバーできるよう、新たな検出方法が定期的に追加されています。トリガーされると、プロセスの動作が分析され、疑わしいと判断された場合には、**その脅威はマシン上で直ちにブロック**され、さらに攻撃関連のメタデータが ESET LiveGrid クラウドシステムに送信されます。この情報はさらに処理され、関連付けられます。これにより、**それまで未知であった脅威や「ゼロデイ」と呼ばれる攻撃を発見**でき、貴重な脅威インテリジェンスが ESET ラボに提供されます。

エクスプロイトブロッカーは、悪意のあるコード自体の分析に焦点を当てた検出手法とはまったく異なるテクノロジーを使用することにより、攻撃者に一歩近づいた別の保護層を追加します。

ランサムウェアシールド

ESET ランサムウェアシールドは、**恐喝型マルウェアとも呼ばれる脅威からユーザーを保護する追加レイヤー**です。このテクノロジーは、動作ベースおよびレピュテーションベースのヒューリスティックを使用して、実行されたすべてのアプリケーションを監視し、評価します。ランサムウェアに似た動作が特定されるか、マルウェアである可能性があるものが既存のファイルに不要な変更（暗号化など）を加えようとすると、アクティビティをブロックする権限を持つユーザーに通知されます。ランサムウェアシールドは、Cloud Malware Protection System、ネットワーク攻撃からの防御、DNA Detections などの他の ESET テクノロジーと共に、最高レベルのランサムウェア保護機能を提供するようにチューニングされています。



ボットネットプロテクション

作成者にとって変更コストが高額なマルウェアの要素の1つが、C&C サーバーとの通信です。

ESET のボットネットプロテクションは、ボットネットが使用する悪意のある通信を検出すると同時に、問題を起こすプロセスを特定することが実証されています。

ESET の Network Detections は、ボットネットプロテクションのテクノロジーを拡張することで、ネットワークトラフィック分析に関連する一般的な問題に対処します。これにより、**悪意のあるトラフィックをより高速かつ柔軟に検出**できます。Snort や Bro などの業界標準シグネチャを使用することで多くの攻撃を検出できますが、ESET Network Detections は中でもネットワークの脆弱性、エクスプロイトキット、および高度なマルウェアによる通信を対象とするように設計されています。

エンドポイントでネットワークトラフィック分析を実行できる機能には、さらなるメリットがあります。悪意のある通信を実行しているプロセスまたはモジュールを正確に特定すること、特定されたオブジェクトに対して措置を講じること、また場合によっては通信の暗号化をバイパスすることも可能です。

ボットネットトラッカー

サンプルまたはそのメモリダンプが ESET システムによって「ボットネット」として識別された場合、ESET ボットネットトラッカーに送信されます。ボットネットトラッカーは、マルウェアの亜種を特定し、ケースに応じて解凍ツール / 復号化ツールを使用して、C&C サーバーおよび暗号 / 通信キーに関する情報を抽出します。これらを取得した後は、さまざまなジオロケーションから偽の通信を開始します。抽出されたデータはすべて後処理され、URL のブロック、ペイロードの新しい検出機能の作成、ESET 脅威インテリジェンスのクライアントへの通知などにより、世界中の ESET ユーザーの保護に活用されます。

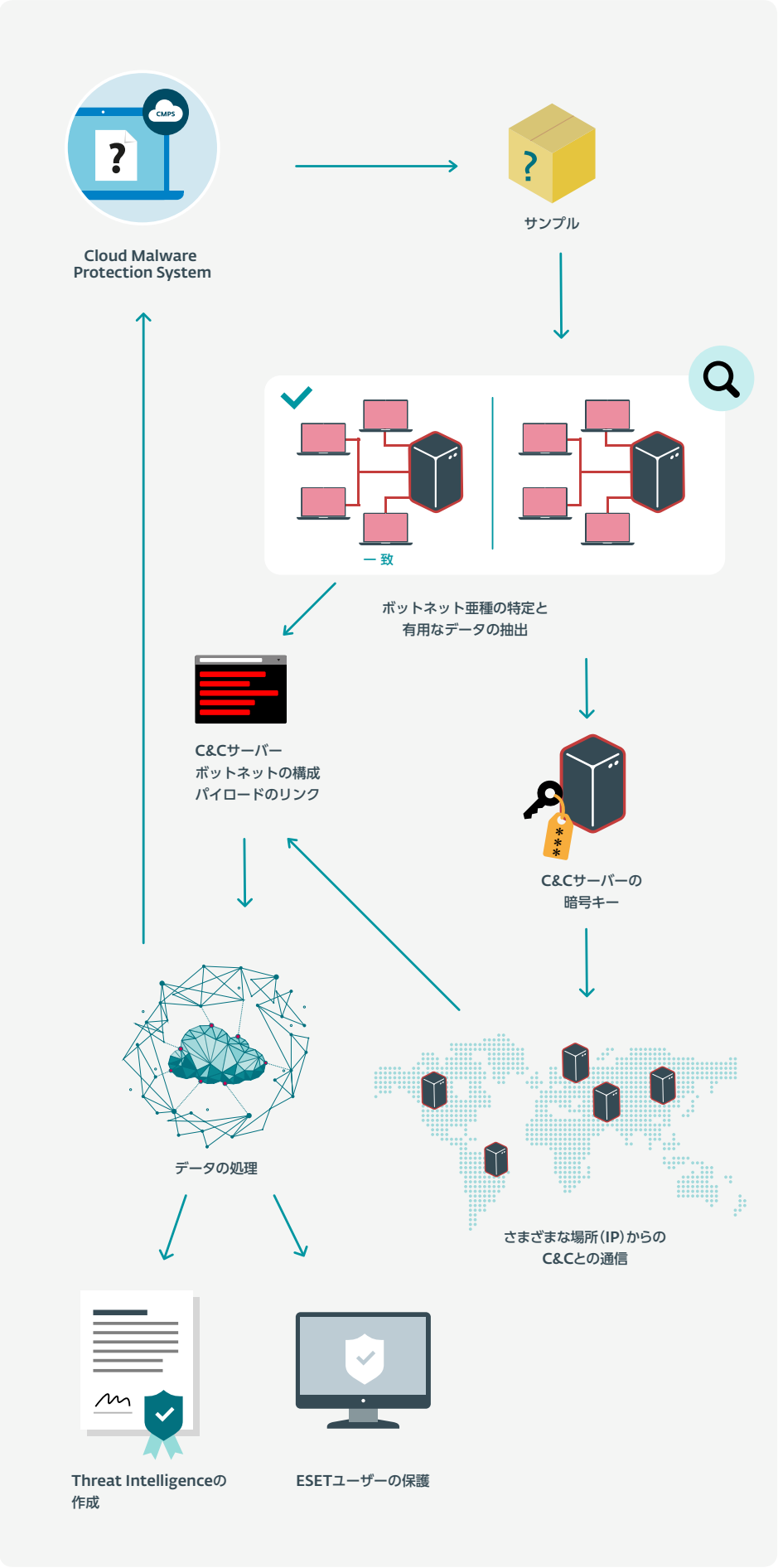


図 9：ESET ボットネットトラッカーの仕組み

Threat Intelligence

ESET Threat Intelligence（ETI）は、その多くが標的型かつステルス型である現代のサイバーセキュリティ脅威に企業が対処するのを支援します。このサービスは、1億個を超えるセンサーから収集された情報を提供することで、脅威環境の概要を企業に的確に伝え、攻撃が発生する前の予測と防止をサポートします。また、攻撃後のフェーズでは、インシデント診断の効果と効率の向上のためにデータを提供します。企業はこの ESET 独自の情報を活用することで、自社のセキュリティの強化だけでなく、エンドユーザーの保護も可能になります。ESET のシステムおよび専門家は、各企業のニーズに応じて、YARA ルールに基づいたボットネットと標的型マルウェアに関するカスタムレポートやフィッシングレポートを生成したり、既存の SIEM ツールへのシームレス統合が可能な STIX/TAXII 形式のリアルタイムデータフィードを提供したりできます。

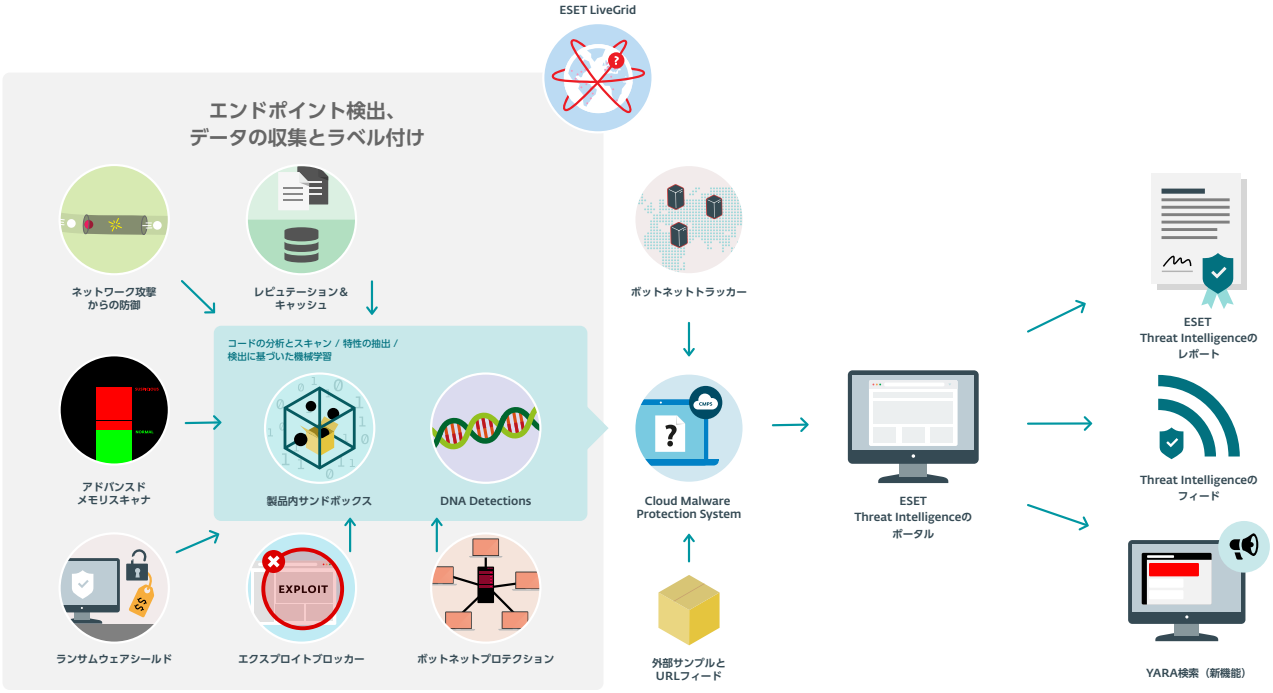


図 10：ESET のテクノロジーによって収集される Threat Intelligence

今日のリアクティブ保護とプロアクティブ保護の比較

DNA Detections はマルウェアファミリ全体の検出にも優れていまが、保護対象のユーザーに配布する必要があります。スキャンエンジン、ヒューリスティック、および最新の脅威をターゲットにした変更についても同様です。現在、ESET のクラウドベースの LiveGrid システムとの通信は、次のようなさまざまな理由から、最高レベルの保護を確保する上で欠かせません。

- **オフラインスキャンは主にリアクティブです**。現在の防衛機能は、お使いの製品に振る舞い検出を内蔵するというだけではありません。攻撃者が保護ツールを入手できる限り、防御側がシグネチャ、ヒューリスティック、または機械学習による分類ツールを使用しているかどうかは関係ありません。なぜなら、マルウェア作成者は使用されている検出テクノロジーを試し、マルウェアが検出されなくなるまで変更してからリリースすればよいからです。ESET LiveGrid であれば、このマルウェア戦略に対抗できます。
- **更新はリアルタイムではありません**。現在よりも頻繁に更新をリリースし、さらには数分ごとにユーザーにプッシュすることは可能です。では、もっと良い方法はないのでしょうか。答えは「YES」です。ESET LiveGrid は、必要に応じて情報を提供することにより、即時の保護を実現します。
- **マルウェアは検出を回避しようとします**。マルウェアの作成者、特にサイバースパイの場合、できるだけ長く検出を避けようとします。電子メールワームなどの大規模な配信とは対照的に、標的型攻撃は、1つのマルウェアを少数の標的、場合によっては1つの標的に展開します。ESET はこの事実を逆手に取ってマルウェア作成者に対抗します。人気がなく評判も良くないオブジェクトは、悪意がある可能性があると判断され、エンドポイントで詳細に分析されるか、LiveGrid フィードバックシステムを介して送信され詳細な自動分析を受けます。ESET LiveGrid レピュテーションシステムには、ファイル、ファイルの送信元、類似性、証明書、URL、および IP に関する情報が含まれています。

自動または手動でのサンプル処理

ESET は毎日数十万個のサンプルを受け取ります。これらのサンプルは、前処理とクラスタリングの後に自動、半自動、および手動で処理されます。**自動分析は、一連の仮想マシンと実マシン上で社内開発されたツールによって実行されます。**

分類は、実行中に抽出されたさまざまな属性を使用して、静的コード分析と動的コード分析、オペレーティングシステムに導入された変更、ネットワーク通信パターン、他のマルウェアサンプルとの類似性、DNA 機能、構造情報、および異常検出に従って実行されます。

すべての自動分類には次のような欠点があります。

- **分類のための識別機能の選択は簡単ではなく**、マルウェアの専門家である人間の知識が必要です。
- **機械学習分類ツールでは、人間の専門家が参加して**、学習に使用される入力を検証する必要があります。システムによって分類されたサンプルがシステムへの入力として使用される完全自動処理では、正のフィードバックループによって発生した雪だるま効果により、すぐに不安定になります。いわゆる「Garbage In, Garbage Out」（ゴミを入力しても、ゴミしか出力されない）の状態です。
- 機械学習アルゴリズムはデータを理解しません。また、**たとえ統計的に正しい情報であっても、有効であるとは限りません**。
- たとえば、機械学習では、クリーンなソフトウェアの新しいバージョンと不正なバージョンを区別できません。クリーンなアプリケーションにリンクされた修正プログラムとマルウェアで使用されるダウンローダーも区別できません。また、クリーンなソフトウェアコンポーネントが悪意のある目的で使用されていることを認識できません。

- 機械学習では、学習プロセスに新しいサンプルを追加すると誤検出が発生する可能性があり、誤検出を削除すると正検出の有効性が低下する可能性があります。
- 自動処理を実行することで、ESET LiveGrid を介した検出によって新たな脅威に即座に対応できますが、トップレベルの品質と検出率、および誤検出の最小化を保証するには、検出エンジニアによるサンプルの追加処理が重要になります。

レピュテーションサービス

ESET LiveGrid は、オブジェクトのレピュテーションも提供します。判定するのは、ファイル、証明書、URL、IP などのさまざまなエンティティのレピュテーションです。前述のように、レピュテーションを使用することで、新しい悪意のあるオブジェクトや感染源を特定できます。用途は上記以外にもあります。

スキャンのホワイトリスト作成

スキャンのホワイトリストを作成する機能により、スキャンエンジンがオブジェクトを検査する回数を減らすことができます。オブジェクトが変更されておらず、クリーンであることが確実であれば、スキャンを実行する必要は全くありません。この機能によってパフォーマンスは大幅に向上します。また、ESET 製品の存在も目立たなくなります。一切実行されないコードこそが最速のコードです。ESET のホワイトリストは、絶えず変化するソフトウェアの状況に常に適応します。

情報収集

ユーザーが統計情報を ESET LiveGrid に送信することを決定した場合、ESET はその情報を脅威のグローバルな追跡と監視に使用します。この情報は大量の調査データとなり、**ESET は最も緊急性が高く問題のあるケースに焦点を当て、マルウェアの傾向を観察し、保護テクノロジーの開発を計画し優先順位を決定することができます。**

FPS と IOC について

IOC（Indicators of Compromise：セキュリティ侵害の痕跡情報）は、現代の企業セキュリティにおいて非常に重要であると認識されていますが、「次世代」のセキュリティプロバイダーが主張しているように特別なものや高度なものとは言えません。以下の図は、最も一般的な IOC の内訳と、その根拠です。* ご覧のとおり、対象となる機能は非常に基本的なもので、4 分の 1 は既知の MD5、その次にファイル名などが続きます。これらの結果から、フォレンジックには有用ではあるものの、予防とブロックに適した方法ではないことは明らかです。皮肉なことに、「古い AV」で使用されているシグネチャベースの検出を「時代遅れ」だとして否定する「次世代」ベンダーの一部は、悪意のあるファイルやイベントを検出する最弱のシグネチャベースの方法であるにもかかわらず、IOC を高く評価しています。

* データソース：IOC Bucket、2015 年 4 月。IOC Bucket は、脅威インテリジェンスの共有方法をセキュリティコミュニティに提供することに特化した無料のコミュニティ主導型プラットフォームです。

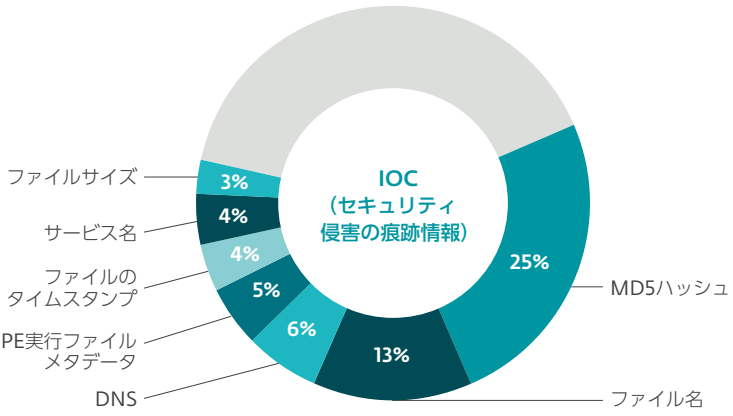


図 11：IOC Bucket による IOC の分析
（2015 年 4 月のサンプル）。

結論

セキュリティに特効薬は存在しません。動的で多くの場合、標的型である今日のマルウェアに対処するには、経験豊富な研究者が長年にわたり収集したペタバイトレベルの情報を活用する積極的でスマートなテクノロジーによる、多層型アプローチが必要です。20 年前、ESET は（従来型アプローチである）AV が不完全なソリューションであることを認識し、その時点で積極的なテクノロジーを ESET のスキャンエンジンに組み込み始めました。その後、サイバーキルチェーンのさまざまな段階で適用する保護層を段階的に実装していきました。

ESET は、25 年以上の研究に基づいて高水準の保護を提供できる数少ないセキュリティベンダーの 1 つです。そのため、ESET は常にマルウェアの一歩先を走り、標準の静的シグネチャの使用にとどまらずにテクノロジーを進化させ続けることが可能です。エンドポイントベースのテクノロジーとクラウド拡張テクノロジーの独自の組み合わせにより、マルウェアに対して最も高度なセキュリティを提供しています。

ENJOY SAFER TECHNOLOGY™