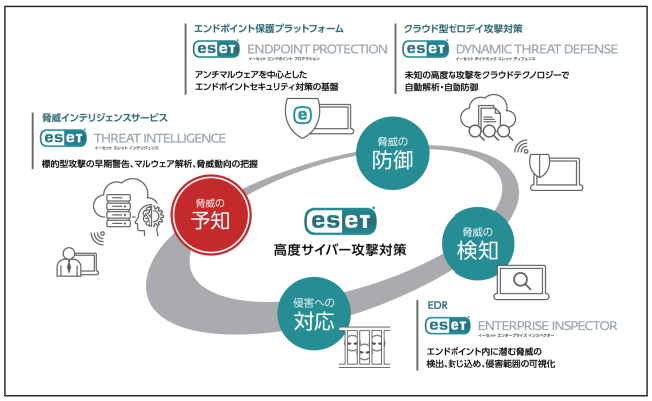
2019年11月11日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

ESETの高度サイバー攻撃対策ソリューションを強化
クラウド型脅威インテリジェンスサービスを発売

キヤノンマーケティングジャパン株式会社（代表取締役社長：坂田正弘、以下キヤノンMJ）は、近年の巧妙なサイバー攻撃への予防対策を可能にする脅威インテリジェンスサービス“ESET Threat Intelligence（イーセット スレット インテリジェンス）”を2020年1月下旬より発売します。
キヤノンMJは、サイバー攻撃の予知から防御、検知、対応までの包括的なセキュリティソリューションを展開し、エンドポイントセキュリティ事業で2021年に売上100億円を目指します。



高度サイバー攻撃対策　概念図

近年、企業や官公庁、研究機関などの組織を標的としたサイバー攻撃は増加し続けており、2019年9月の警察庁の調べ※1では上半期の標的型攻撃メールは2687件にのぼります。標的型攻撃や高度で持続的な脅威をもたらすAPT攻撃は、攻撃者の長期的な情報収集と緻密な戦略によりカスタマイズして繰り返し仕掛けられます。このように高度で執拗な攻撃には、攻撃の予兆をいち早く入手し速やかに予防的な対策を講じることが重要です。

キヤノンMJはこうした脅威に対応するため、標的型攻撃の予兆や個別の攻撃情報の予測などをレポートする脅威インテリジェンスサービス「ESET Threat Intelligence（以下ETI）」の提供を2020年1月より開始します。ETIは、マネージドセキュリティサービス事業者やSOCサービス事業者などのセキュリティサービスプロバイダーやCSIRTやSOCなどのセキュリティ対策部門を有する企業や組織向けのサービスです。

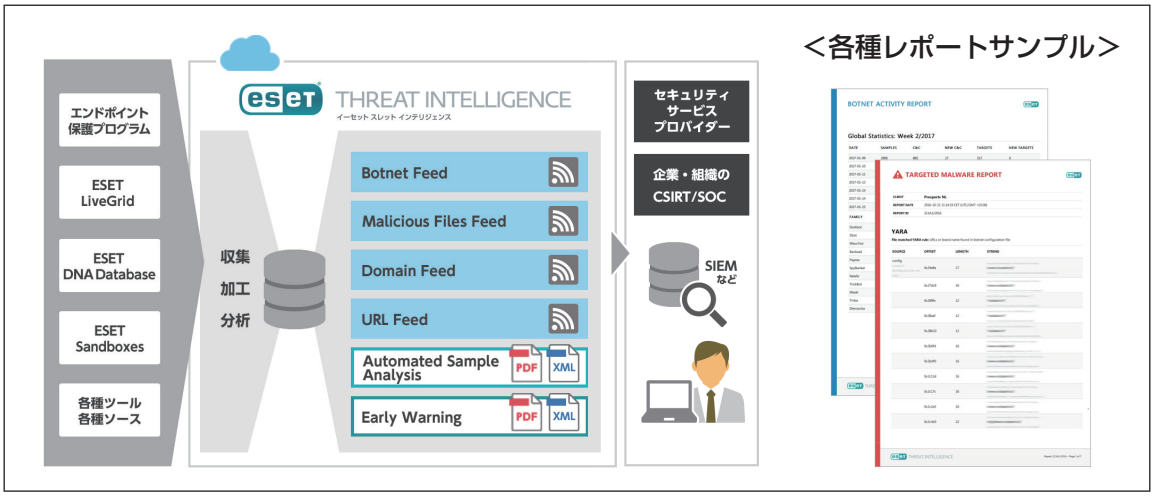
ETIは、ESET社が世界中の1億台以上の端末から収集、分析した脅威情報を6つのサービスとして展開します。ボットネットや悪質な疑いのあるファイル、URLなどの情報をSIEM※2などのシステムと連携可能なデータとして提供する「ETI Botnet Feed」「ETI Malicious Files Feed」「ETI Domain Feed」「ETI URL Feed」、予測される個別の攻撃の情報をレポートする「ETI Early Warning」、攻撃に使われたマルウェアなどを解析しインシデント調査に役立つ情報をレポートする「ETI Automated Sample Analysis」など、必要に応じてサービスを選択することが可能です。本サービスによりサイバー攻撃の予兆や攻撃手法の解析、世界で使われている攻撃ツールの検出状況などを把握し、「今は見えていない攻撃」や「将来発生しうる攻撃」を予測できるため事前にサイバーセキュリティ対策を講じ被害を最小限に抑えることが可能です。

キヤノン MJ は、ESET 製品の中核であるアンチマルウェア・アンチウイルス製品「ESET Endpoint Protection シリーズ」、ゼロデイ攻撃などの未知の高度な脅威を防御するクラウドサービス「ESET Dynamic Threat Defense」、事後対策のための EDR 製品「ESET Enterprise Inspector」などの既存のソリューションに ETI を加えることで、サイバー攻撃の予知から防御、検知、対応まで包括的に対応できるセキュリティソリューションを提供します。さらに、コンサルティング、運用監視など新たなセキュリティサービスの強化を図ることで、2021 年にエンドポイントセキュリティ事業で売上 100 億円を目指します。

＜価格＞

サービス名	価格(税別)	発売日
ESET Threat Intelligence	個別見積	2020 年 1 月下旬

＜概要図＞



＜サービス概要＞

ETI Early Warning	顧客あるいは自社をターゲットとして準備中または進行中の潜在的な攻撃が見つかった場合にレポートします。特定のマルウェアファミリーやボットネットに関する世界的な活動状況についての情報も得られ、顧客／自社に対する攻撃の予兆を速やかに把握できます
ETI Automated Sample Analysis	指定したハッシュや手動でアップロードしたファイルを自動解析してその危険性をレポートします。攻撃に使われたマルウェアの動作に関する実用的な情報が得られ、事実に基づく意思決定やインシデント調査に役立ちます。
ETI Botnet Feed ETI Malicious Files Feed ETI Domain Feed ETI URL Feed	ボットネットに関する情報や、悪質な疑いのある実行ファイル、ドメイン、URL に関する情報を STIX 形式 /TAXII 手順で入手でき、SIEM 等と連携し活用できます。

＜主な特長＞

1）全世界 1 億台以上のセンサーから集められる最新の脅威情報

世界中に導入されている ESET エンドポイント保護プログラムから収集された脅威情報が集まるクラウドシステム「ESET LiveGrid」の情報を中心に、ESET 独自の脅威インテリジェンスを利用できます。

2）YARA によるカスタムルール

YARA ルール※3 の形態によるカスタムルールを作成し、顧客あるいは自社が必要とする固有の脅威情報を収集できます。ルールに合致した情報をレポートとして参照したり、API を介して外部システムへ連携したりできます。

3）ESET ユーザーでなくても利用可能

ETI はほかの ESET 製品を利用していなくても単独で利用できるサービスです。

※1 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf
警察庁 「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」
※2 セキュリティソフトの一つで、様々な機器やソフトウェアの動作状況の記録 (ログ) を一元的に蓄積・管理し、保安上の脅威となる事象をいち早く検知・分析するもの
※3 オープンソースのマルウェア検知・調査ツールである「YARA」で使用される記述形式

● 報道関係者のお問い合わせ先：キヤノンマーケティングジャパン株式会社
広報部　パブリックリレーションズグループ　03－6719－9093（直通）
● 法人のお客さま向け ESET ホームページ：https://eset-info.canon-its.jp/business/
● ニュースリリースホームページ：canon.jp/newsrelease