KASPERSKY lab

Kaspersky Security Network

クラウドベースのアンチウイルスネットワーク

Kaspersky Security Network（KSN）は、世界各国の数百万人もの有志のユーザーから収集、匿名化されたサイバーセキュリティ関連データの処理を行う、分散型のインフラストラクチャです。KSNはインターネットに接続するパートナー様やお客様にKaspersky Labのセキュリティインテリジェンスを提供し、最短の応答時間と最高レベルのプロテクションを実現します。KSNの機能は、Kaspersky Labのほとんどの個人向けおよび法人向け製品に組み込まれています。

KSNは新種のマルウェアに対しても、迅速な対応と高い検知力を誇り、抜群の保護能力を発揮します。KSNの目的は世界中のユーザーのセキュリティレベルを引き上げることです。既知の脅威を検知してブロックするだけに留まらず、オンライン上の攻撃ソースの場所を突き止めてブラックリストに登録するほか、Webサイトやアプリケーションのレピュテーションデータも提供します。つまり、KSNはKaspersky Labの高度な保護機能を実現するための最も重要なコンポーネントの1つであると言えます。

サイバー攻撃を迅速かつタイムリーに防御

ウイルス、ワーム、トロイの木馬といったマルウェアは、コンピューターの正常な動作とコンピューターに保存されたデータを脅かす主な脅威となっています。悪意あるソフトウェアの種類や攻撃範囲は絶えず拡大を続け、セキュリティ上の課題は増加の一途をたどっています。Kaspersky Labのデータによると、毎日約315,000件の新規サンプルがユーザー環境内で検知されています。マルウェアは新たな手口を用いてコンピューターシステムに侵入し、アクティビティを隠しながら、セキュリティソフトウェアを回避しています。従来型のマルウェア検知手法をスタンドアロンで使用しても、完全な保護が提供されることはもはや不可能です。

今日のIT社会は、コンピューターの安全性を確保するための新しく包括的なアプローチを求めています。そのアプローチには、従来型の防御技術の強みを組込みつつ、欠点を最小化し、グローバルな監視機能および新種の脅威に関する情報の継続的な更新機能を備える必要があります。そして、このようなアプローチはKSNを基盤にして実現されるものです。

Kaspersky Security Networkの基本原理

KSNでは、より安全なインターネット環境構築への協力に同意いただいたユーザーからマルウェア攻撃に関する情報を収集しています。取得したすべての情報は匿名化されます。Kaspersky Labで受信した情報はデータ種別に従って分類され、どのデータがどのユーザーから取得されたものかはトレースできません。Kaspersky Labは、現行法のセキュリティ要件に則り、収集したすべての情報を保護しています。

KSNの動作メカニズムは、複数の主要なプロセスから成り立っています。これには、ユーザーのコンピューターを狙う脅威に対する継続的かつ地理分散型のリアルタイムモニタリング、モニタリングデータの分析、保護対象のエンドポイントへの適切な情報と対策の提供などが含まれます。

専門的知識を持ったKaspersky Labの技術スタッフが攻撃情報を分析し、迅速かつ信頼性の高い方法で新出のマルウェアと正当なソフトウェアを識別します。プログラムの安全性は、ベンダーのデジタル署名とハッシュの有効性、ソースおよびプログラムの整合性の検証などの複数の要素に基づいて決定されます。正当であると認識されたプログラムは、信頼できるアプリケーションのリスト(ホワイトリスト)に登録されます。

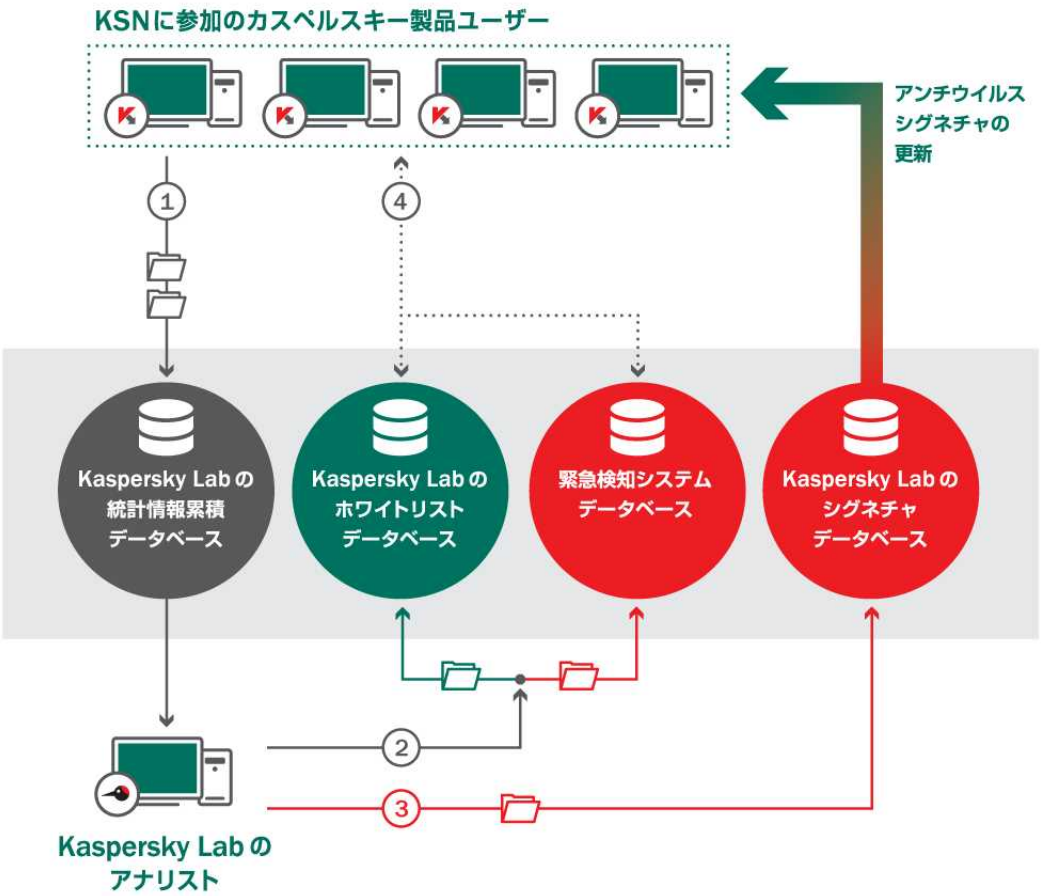
プログラムに対して必要な分析が完了し、マルウェアと判定されると、その情報は即座にKaspersky Labの緊急検知システムに通知され、KSN を通じて配信されます。そのためエンドポイントでは、マルウェアに対するシグネチャが作成されダウンロードされる前に保護策を講じることができます。このようにして、カスペルスキー製品ユーザーは、サイバー攻撃の数分後には、未知の脅威を食い止めるための情報を迅速に受信します。一方で、従来のシグネチャ型のデータベース更新では数時間もかかることになります。

ユーザーが起動したプログラムは、ホワイトリストおよび緊急検知システムリストと照合されます。その結果に従って、プログラムからコンピューターリソースへのアクセス権限を付与したり、プログラムの実行をブロックしたりします。KSNのテクノロジーは、これらのリストを更新し、最新の状態に保つという重要な役割を担うことにより、プログラムの実行を制御します。

もう 1 つ、KSNリソースを使用してプログラムの安全性を判断するテクノロジーがあります。それは、「Wisdom of the Crowd(WoC)」と呼ばれるレピュテーションテクノロジーで、他のKSNユーザーによるプログラムのレピュテーションに関する情報を提供するものです。

KSNは、シグネチャ型とヒューリスティック型の両方のマルウェア検知手法を支えるとともに、ホワイトリストおよびアプリケーションコントロール技術を採用しています。

KSNが提供するもう 1 つの効果的な保護技術である、クラウドベースのアンチスパムテクノロジーについても説明します。この技術はクラウドからの情報を利用して迷惑メールを検知しブロックします。そのため、ローカルのアンチスパムフィルタを必要としません。



上のフローチャートは、カスペルスキー製品とKSNとの間のインタラクションの基本原理を表しています。このインタラクションには3つのフェーズが存在します。

1. KSNの全参加者から取得したデータに基づいて検出された脅威と不審なアクティビティに関する統計情報は、Kaspersky Labのクラウドインフラストラクチャ内で処理されます。Kaspersky Labのデータベースに、関連するレコードが含まれていない場合（たとえば、ヒューリスティックによる検知が行われた場合）は、弊社のエキスパートがその情報をさらに深く解析します。
2. 悪意あるコードまたは悪意ある URLであることが判明した場合、その情報が緊急検知システムデータベースに追加され、最初の検知からわずか数分のうちに関連するカスペルスキー製品のすべてのユーザー（KSNの参加ユーザー以外にも）環境に反映されます。同時に、正当なアプリケーションに関するデータはホワイトリストデータベースに追加されます。
3. Kaspersky Labのエキスパートが不審なコードの分析を完了し、その危険性を診断したら、シグネチャデータベースに追記します。このデータベースは、カスペルスキー製品で保護された各コンピューターに定期的にダウンロードされます。
4. カスペルスキー製品ユーザーが既知のサイバー脅威に遭遇した場合は、製品からKSNに判定が依頼され、すぐに結果を得られます。

KSNを利用可能なプログラムリスト

KSNは、ほとんどのカスペルスキー製品（プログラム）でご利用いただけます。

個人ユーザー向け

- カスペルスキー インターネット セキュリティ (*1)
- カスペルスキー インターネット セキュリティ for Mac (*2)
- カスペルスキー インターネット セキュリティ for Android (*3)
- カスペルスキー アンチウイルス for Windows
- Kaspersky Security Browser for iOS

*1: カスペルスキー マルチプラットフォーム セキュリティに含まれるWindows向け保護プログラム

*2: カスペルスキー マルチプラットフォーム セキュリティに含まれるMac向け保護プログラム

*3: カスペルスキー マルチプラットフォーム セキュリティに含まれるAndroid向け保護プログラム

法人ユーザー向け

- Kaspersky Small Office Security
- Kaspersky Endpoint Security for Windows / Windows Server (*4)
- Kaspersky Endpoint Security for Mac (*5)
- Kaspersky Endpoint Security for Linux (*6)
- Kaspersky Security for Mobile (*7)
- Kaspersky Security for Virtualization
- Kaspersky Security for Linux Mail servers･

*4: Kaspersky Endpoint Security for Business に含まれるWindows向け保護プログラム

*5: Kaspersky Endpoint Security for Business に含まれるMac向け保護プログラム

*6: Kaspersky Endpoint Security for Business に含まれるLinux WS向け保護プログラム

*7: Kaspersky Endpoint Security for Business に含まれるMobile向け保護プログラム

KSNとカスペルスキー製品とのインタラクションの原理はどの製品もほぼ共通ですが、個人ユーザー向け製品と法人ユーザー向け製品では異なる機能が存在します。

個人ユーザー向けのクラウドベースの保護機能

クラウドベースのプロテクションで享受できる一般的な利点以外にも、個人ユーザー向け製品では、保護されたユーザーの数、ブロックされた悪意あるオブジェクトの数、処理された正当なデータの数などのKSNに関する統計情報を受信できます。

個人ユーザー向け製品では、KSNのデータをベースにして実行ファイルのレピュテーションをチェックするアプリケーションコントロール機能も提供されています。クエリが送信されると、問題のファイルに関する判定（プログラムが正当なものか否か）、そのファイルが最初に出現した日付、国別のレピュテーションなどのデータが返されます。この機能により、ユーザーは未知のプログラムを起動する前に基本的なチェックを行うことができます。ちなみに、このような情報はユーザーがファイルを実行しようとしたときにも自動的に取得されます。

法人ユーザー向けに強化されたクラウドセキュリティ

KSNでは、法人向け製品にも数多くの機能を提供しています。まず、クラウドベースのプロテクションテクノロジーでは、KSNから取得したデータを使用して、アプリケーションのホワイトリストを作成します。正当な既知のファイルは、たとえばゲーム、商用ソフトウェアというように、自動的にカテゴリーに分類されます。システム管理者は、これらのカテゴリーを利用して、ソフトウェアタイプごとにセキュリティポリシーに従ったルールを簡単に作成して適用することがきます。アプリケーションのホワイトリストを作成するためのデータは、300社以上の主要なソフトウェアベンダーからも提供され、クラウドソース化された情報と併せて利用されています。

法人ユーザー向けの管理ソリューションであるKaspersky Security Center では、KSNが企業内のエンドポイントをどのように保護するかを詳細に制御できます。管理者は、Kaspersky Endpoint Security for Businessの特定のモジュール内で、クラウドベースのプロテクションを有効化するか無効化するかを選択できます。また、帯域幅の使用を低減するために、Kaspersky Security CenterのKSNプロキシサービス機能を使用して、KSNからのデータをキャッシュすることも可能です。

Kaspersky Security Networkの利点

現在、KSNのテクノロジーは世界各国の何百万台ものコンピューター上で使用されており、新出のマルウェアがどのように出現して流通しているか、発生源はどこか、特定の期間に何回の攻撃が試行されたかなどの状況をグローバル規模かつ詳細に提供しています。KSNで実行する世界規模でのマルウェアモニタリングにより、発生源や攻撃対象の場所に関わらず新出の脅威に容易に対処することが可能になっています。

KSNは効果的でプロアクティブな防御機構の構築に役立ちます。新しい脅威が拡大し、お客様のITネットワークに甚大な損害を与える前に、検出しブロックすることを可能にします。プロアクティブな防御システムは、IT機器とそれらを支えるビジネスプロセスが中断することなく安定して動作するうえで必要不可欠です。

Kaspersky Lab
2014 年 6 月
株式会社カスペルスキー

PR-1009-201501