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、世界各地の数百万人もの有志のユーザーから収集されたサイバーセキュリティ関連のデータ処理を行う、分散型の複合インフラストラクチャです。KSN は、すべてのユーザーとパートナーにインターネット経由で 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 は、弊社のセキュリティ製品の最も重要なコンポーネントの 1 つです。

未知の高度なサイバー脅威から保護

Kaspersky Lab のデータでは、毎日約 325,000 件の新規マルウェアサンプルがユーザー環境内で検知され、毎月 113,500 件のフィッシンググループ（フィッシングワイルドカード）がアンチフィッシングデータベースに登録されています。加えて、サイバー犯罪はその数が増加しているだけでなく、高度に進化し続けています。弊社の内部統計によると、ユーザーが日々遭遇する脅威のうち、既知のものはわずか 70%で、残りの 30%は追加の保護階層でのみ対応できる未知の高度な脅威です。そのため、従来型のシグネチャを使用した保護手法では十分とは言えず、大手セキュリティベンダー各社はいずれも、デバイスベースの技術とクラウド技術を組み合わせたハイブリッド型の保護手法を採用しています。

ハイブリッド型のアプローチでは、従来型の保護手法の強みを組み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提供します。このようなクラウド保護には以下の 3 つの利点があります。

- 検知率の向上
- 応答時間の短縮
- 誤検知の最小化

Kaspersky Security Network の基本原理

- KSN は、世界各地から受信したデータを自動解析し、新しいサイバー脅威をより効果的かつ迅速に検知し、デバイスのユーザビリティを妨げない形で保護することを目指します。
- KSN で処理される情報は、KSN への参加に同意したユーザーから送信された情報です。ユーザーが参加を希望しない場合や制限付きの利用を希望する場合は、カスペルスキー製品のインストール時に選択するか、またはインストール後の設定画面で選択できます[i]。
- KSN が受信するデータには、大半の国で法律上「個人情報」と見なされる、氏名、連絡先、その他の識別情報などは含まれず、データが特定の個人に結び付けられることはありません。取得する情報の種類について詳しくは、各カスペルスキー製品ドキュメントに含まれる「Kaspersky Security Network に関する声明」に記載されています。

- 弊社はこの情報を、現行の法定のセキュリティ要件および最高水準の業界基準に従って保護します。
- KSN からユーザーのデバイスに送信されるデータは完全に暗号化され、中間者攻撃から保護されます。

Kaspersky Security Network のワークフロー

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上の脅威に対する継続的で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アナリストが、さまざまな技術リソースを駆使して攻撃情報を分析します。

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値の有効性、ソースおよびプログラムの整合性の検証など、複数の要素から決定されます。Web サイトの安全性は、その企業の証明書、および Web ページの内容の解析を経て決定されます。

正規であると認識されたプログラムまたは Web サイトは、信頼できるアプリケーションまたは Web サイトのリスト（ホワイトリストデータベース）に登録されます。一方、悪意あるプログラムまたは Web サイトと判定されると、即座に弊社の緊急検知システム（Urgent Detection System：UDS）に通知され、KSN を通して全ユーザーに配信されます。

従来型のシグネチャデータベースでは、シグネチャを作成してアップロードするまでに数時間かかりますが、KSN ではサイバー攻撃が開始されてから数分のうちに、その攻撃に対する保護手段がユーザーに配信されます。KSN は、最新情報の分析により正規プログラムのリストを常時更新し、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サポートするとともに、シグネチャ型とヒューリスティック型検知の即時性を支えています。

KSN の特筆すべき機能として、クラウドベースのアンチスパムテクノロジーがあります。この技術により、ユーザーがローカルのアンチスパムフィルターを用意することなく、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することができます。

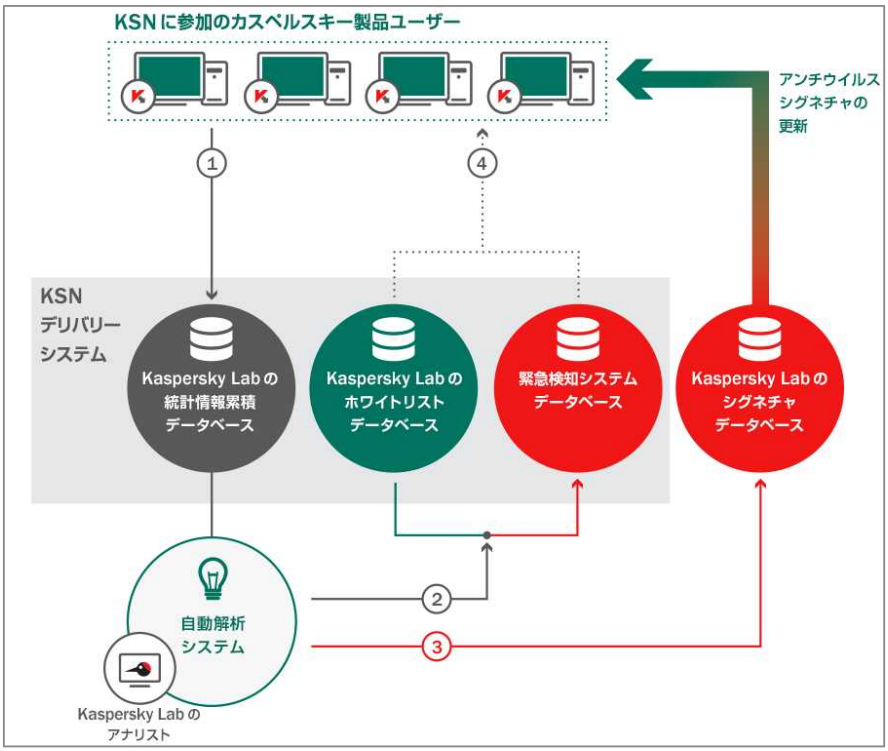
次の図は、カスペルスキー製品と KSN 間のインタラクションの基本原理を表しています。このインタラクションには 4 つのフェーズが存在します。

1. 脅威と不審なアクティビティに関する情報が、弊社のクラウドインフラストラクチャに送信されます。特定の一連のインジケーターに対応するレコードがデータベースに存在しない場合（たとえば、ヒューリスティック手法で検知された場合）は、自動解析システムでデータを解析します。このシステムは、弊社のリソースを利用するため、ユーザー側のデバイスのリソースに負荷をかけることはありません。システムで自動判定できない場合は、アナリストが手動でその情報を分析します。

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、詳細情報が緊急検知システム UDS のデータベースに登録され、最初の検知から数分で全ユーザーに情報が配信されます。同時に、正規と判定されたアプリケーションのデータは、ホワイトリストデータベースに登録されます。

3. 不審なコードまたは URL は、詳細な分析後にシステムまたはアナリストが危険度を判定し、その情報をシグネチャデータベースに登録します。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のユーザーが、既知のサイバー脅威（シグネチャデータベースに未登録のもの）に遭遇した場合は、製品から KSN に判定がリクエストされ、即時に結果が返されるため、確実性の高い保護が実現します。



個人ユーザー向け Kaspersky Security Network

クラウドベースのプロテクションによる一般的な利点以外にも、弊社の個人向け製品では、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統計情報を KSN から受信できます。

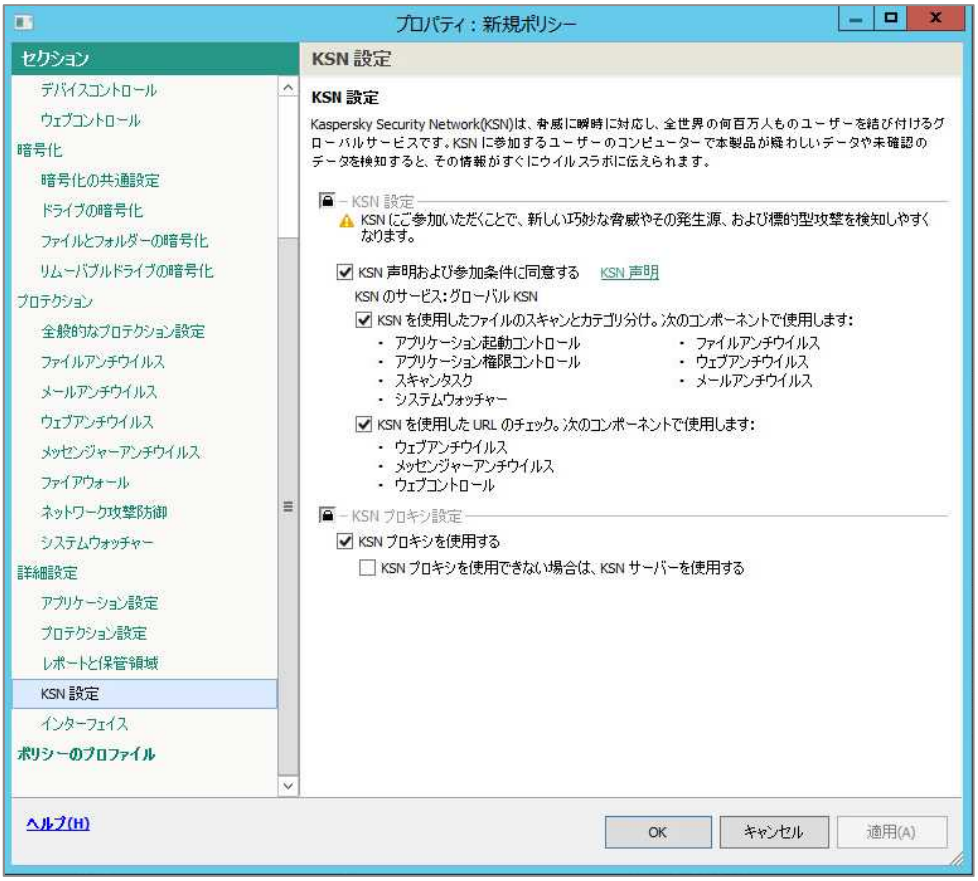
個人向け製品には、KSN からのデータを基に、実行ファイルのレピュテーションをチェックする機能も用意されています。クエリが送信されると、対象のファイルに関する判定（プログラムが正規か否か）、そのファイルが最初に出現した日付、国別のレピュテーションなどのデータが返されます。このようなレピュテーション評価技術を「危険ファイル診断」と呼んでいます。この機能により、ユーザーは未知のプログラムを起動する前に基本的なチェックを行うことができます。なお、この情報はユーザーがファイルを実行する際にも自動的に取得されます。

法人ユーザー向け Kaspersky Security Network

KSN は、法人向けの機能も数多く提供しています。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。正規と判定された既知のファイルは、たとえばゲーム、ビジネス用ソフトウェアなど自動的にカテゴリー分けされます。企業のシステム管理者は、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沿ったルールを容易に作成し、適用することができます。アプリケーションホワイトリストのデータベースを作成するためのデータは、400 社以上の主要なソフトウェアベンダーから提供され、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コントロールできます。システム管理者は、法人向け製品 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利用するかどうかを選択することができ、KSN へのデータ送信を無効化することも可能です。また、帯域幅の使用を低減するために KSN 内部プロキシをローカルネットワーク内にインストールし

て、KSN からのデータをキャッシュすることもできます。IT 部門は必要に応じて、KSN に送信されるトラフィックを常時監視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地のコンピューター上で利用されており、新出のサイバー脅威がどのように進化して広まっているか、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 の世界規模でのサイバー脅威の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、新しい脅威に迅速に対処することがより容易になります。

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、企業ユーザーのネットワークに甚大な損害を与える前に、それらを検出しブロックすることを可能にします。今日、そのような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安定して動作するためには必要不可欠と言えるでしょう。

[i] 各製品の使用許諾契約書をご参照ください