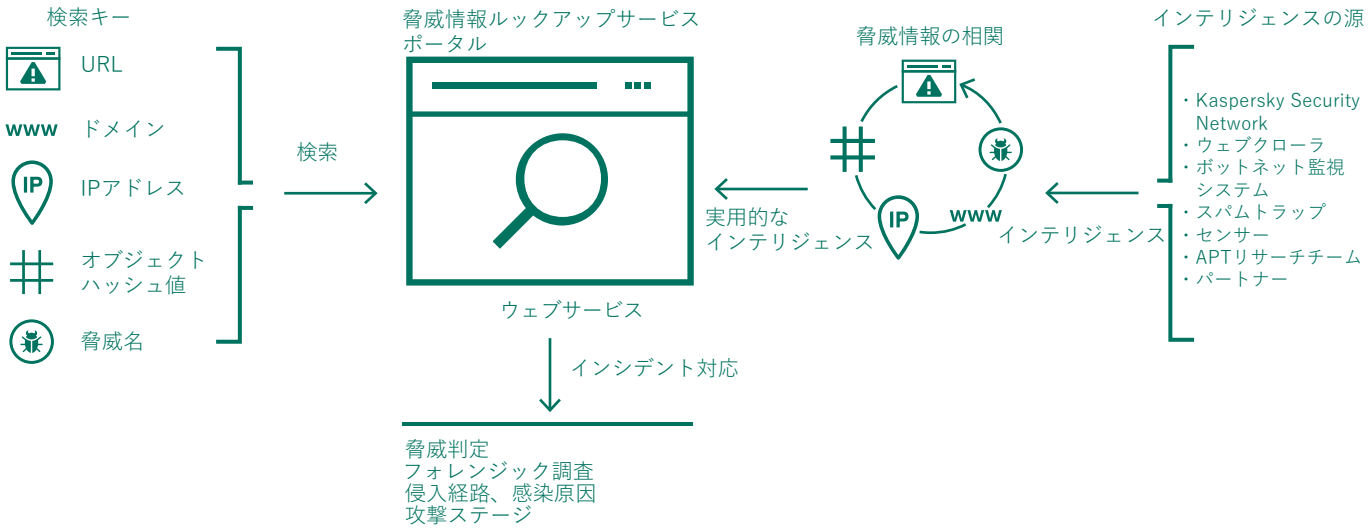
カスペルスキー
脅威情報ルックアップサービス

企業のSOC / CSIRT を強化・支援するインテリジェンスサービス

KASPERSKY lab

サイバー犯罪者の攻撃技術は急速に向上しており、攻撃を受けていることさえも気づかせない難読化・秘匿化の技術を使うなど、その攻撃手法は巧妙さを増す一方です。それは、最新のテクノロジーを駆使したセキュリティシステムをも打ち破ります。さらに、犯罪者はターゲットとした国・企業・組織毎に戦術(Tactics)・テクニック(Techniques)・手順(Procedure):TPPをカスタマイズすることで、標的に確実に侵入し、ビジネス・サービスの妨害、情報資産の奪取などの深刻な被害を与えます。

カスペルスキー脅威情報ルックアップサービスは、サイバー脅威に関して Kaspersky Lab が収集し蓄積し続けるすべてのデータとそれらの間にある相互関係を検索することのできるウェブサービスです。URL・ドメイン・IPアドレス・オブジェクトハッシュ値・脅威名をキーに、その脅威判定・統計的データ・ふるまいデータ・WHOISデータ・DNS データなどの関連する脅威情報を入手することができます。このような情報から企業のSOC・CSIRTは脅威に対するリスクと影響を把握するための調査と、脅威を回避・緩和させるための対処、感染の原因調査など一連のインシデント対応(インシデントレスポンス)が可能になります。カスペルスキーは常にアップデートされたグローバルな最新の脅威情報を提供することによって、組織の保護とインシデント対応の効率化と能力の強化を支援します。



特徴:

- **信頼できるインテリジェンス:** カスペルスキー脅威情報ルックアップサービスの主な特徴として、インテリジェンス情報の信頼性が高く、実用的な付加情報が付随していることが挙げられます。インテリジェンス情報の比類のない質の高さは最高水準の検知率と極めて低い誤検知率など常にトップの評価を獲得している第三者評価機関による比較テスト[1]において実証されています。
- **高いリアルタイム性:** カスペルスキーのインテリジェンス情報は、Kaspersky Security Network のサポートにより世界中から集められたレピュテーション情報・独自のセンサーをもとに、自動分析システムを通して「リアルタイム」で自動生成されています。
- **脅威ハンティング:** 脅威インテリジェンス情報から先を見越した防御・発見・対処を行うことで、攻撃の影響や被害を最小化することができるようになります。可能な限り早い段階から脅威情報ルックアップサービスを使って攻撃を追跡することで、早期に脅威を排除することが可能になります。脅威の発見が早いほど、企業・組織に与えるダメージも小さく、速やかに解消することができ、ビジネスを復旧させることができるようになります。
- **豊富なデータ:** サービスから提供される脅威インテリジェンスは、ハッシュ値・URL・IP・WHOIS・pDNS・GeoIP・ファイル属性・統計的データ・ふるまいデータ・ダウンロード-チェイン・タイムスタンプ・潜伏場所など、さまざまなデータタイプを幅広くカバーしています。組織が直面するセキュリティ脅威は広大な範囲に及びますが、こうした豊富なデータが提供されることで、その調査の効率化が可能になります。
- **いつでも利用できる:** インテリジェンス情報と脅威情報ルックアップサービスは耐障害性の高いインフラにて生成・監視されるため、いつでもどこからでも利用することができます。
- **セキュリティのエキスパートによる継続的な更新:** Kaspersky Lab に在籍する世界のセキュリティアナリスト、Global Research & Analysis Team (GReAT) の世界的に著名なエキスパート、最先端の研究開発チームなど、数百名に及ぶセキュリティ専門家が、価値ある脅威インテリジェンスの生成、更新に24時間365日尽力しています。

- **サンドボックス分析：**[2]疑わしいオブジェクトを分析する独自のクラウドサンドボックス環境を提供します。すべての動作を検証するとともに、未知の脅威を検知し、分かりやすいレポートを生成します。

- **データ、レポートのエクスポート：**検索結果から得られるインテリジェンス情報をIOC・OpenIOC・STIX・Yara・Snort・JSON・CSVフォーマットにエクスポートすることができるため、脅威インテリジェンスの利点を余すことなく活用できます。

- **使いやすいインターフェース、APIにも対応：**脅威情報ルックアップサービスは、ウェブインターフェース（ウェブブラウザー経由）だけでなく、RESTful API経由でアクセスすることもできます。

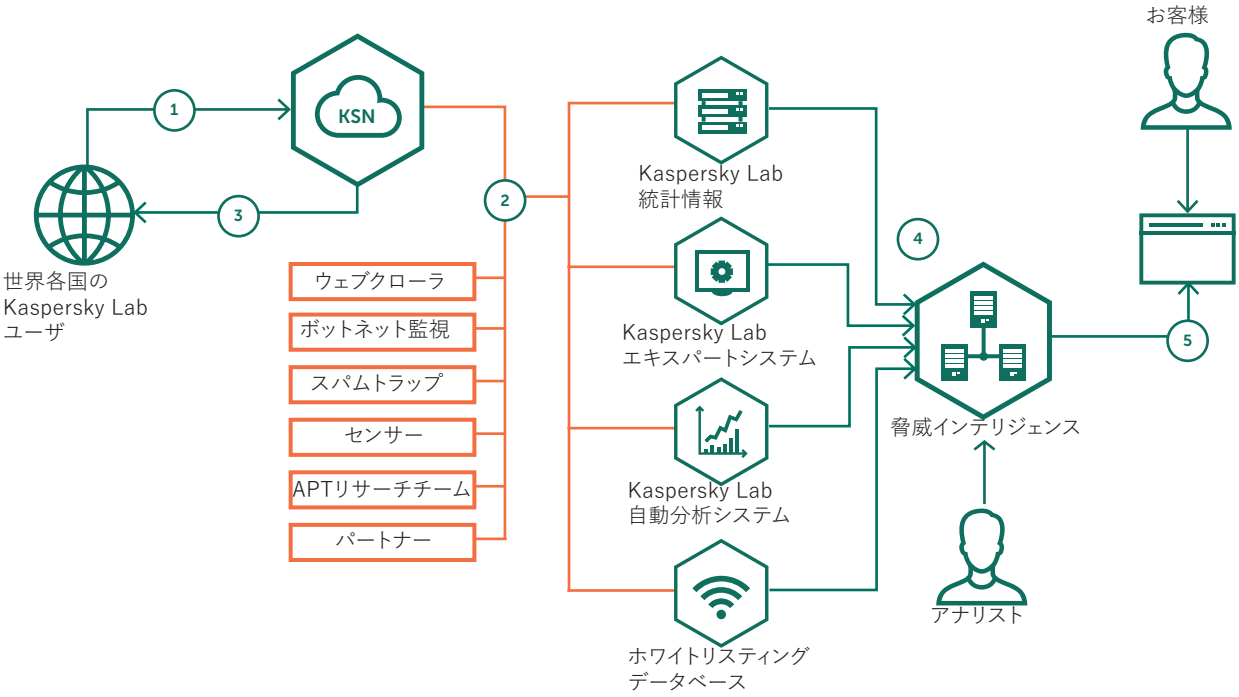
主な利点:

- **インシデント対応とフォレンジック解析の向上と加速：**お客様のSOC・CSIRT担当者は、脅威に関連する情報とグローバルな知見を入手することができるので、セキュリティシステムで検知された多くのイベントに対して優先順位を付け、それぞれに対して適切にかつ迅速に対処することが可能になります。インシデント対応の時間を最小限に抑え、サイバー犯罪者によって重要なシステムやデータに対して不正にアクセスされる前に、一連の攻撃を遮断するこができます。

- **脅威の兆候を詳細に検索：**既存のセキュリティシステムが検知できなかった脅威に対しても、SOC・CSIRTの担当者が発見した脅威の兆候をIPアドレス・URL・ドメイン・オブジェクトハッシュ値などをキーに検索することが出来ます。また、入手した未知のオブジェクトをサンドボックスに分析させることで、隠れた脅威を発見し、関連する脅威インテリジェンスからそのインシデントに対して適切に対応することができるようになります。

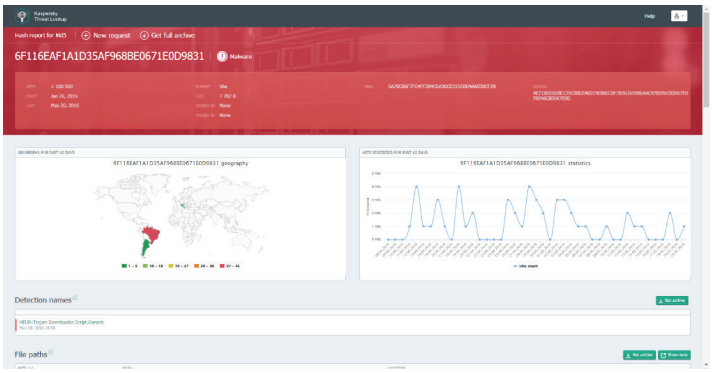
インテリジェンスのソース:

脅威インテリジェンスは、Kaspersky Security Network（KSN）、Kaspersy Lab独自のウェブクローラー、ボットネット監視サービス（ボットネットとそのターゲットおよび活動を 24 時間 365 日監視）、スパムトラップ、リサーチチーム、パートナー、および約 20 年をかけて Kaspersky Lab が収集した悪意あるオブジェクトに関するその他の過去データなど、信頼性の高い各種のソースから収集されています。収集された情報は、統計分析や Kaspersky Labのエキスパートシステム（サンドボックス、ヒューリスティックエンジン、類似性発見用ツール、動作プロファイリング、マシンラーニングなど）、アナリストによる検証、ホワイトリストなど、さまざまな技術を用いて、「リアルタイム」で分析されています。



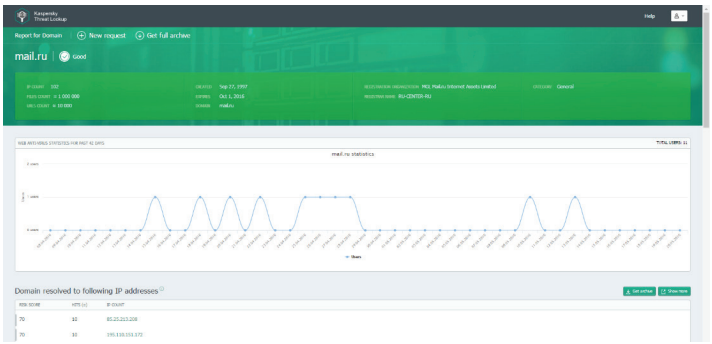
カスペルスキーのインテリジェンス情報は、現実の世界でリアルタイムに収集された脅威の解析結果で構成されています。

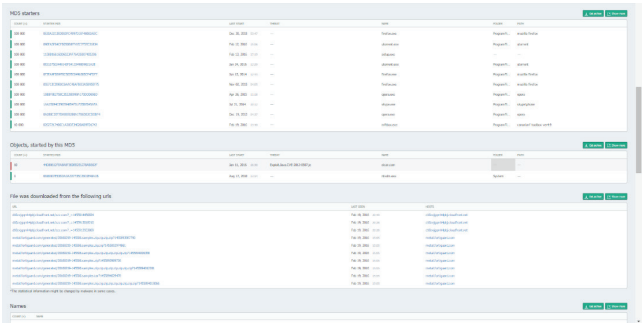
[1] http://www.kaspersky.com/top3
[2]. 2017年秋実装予定



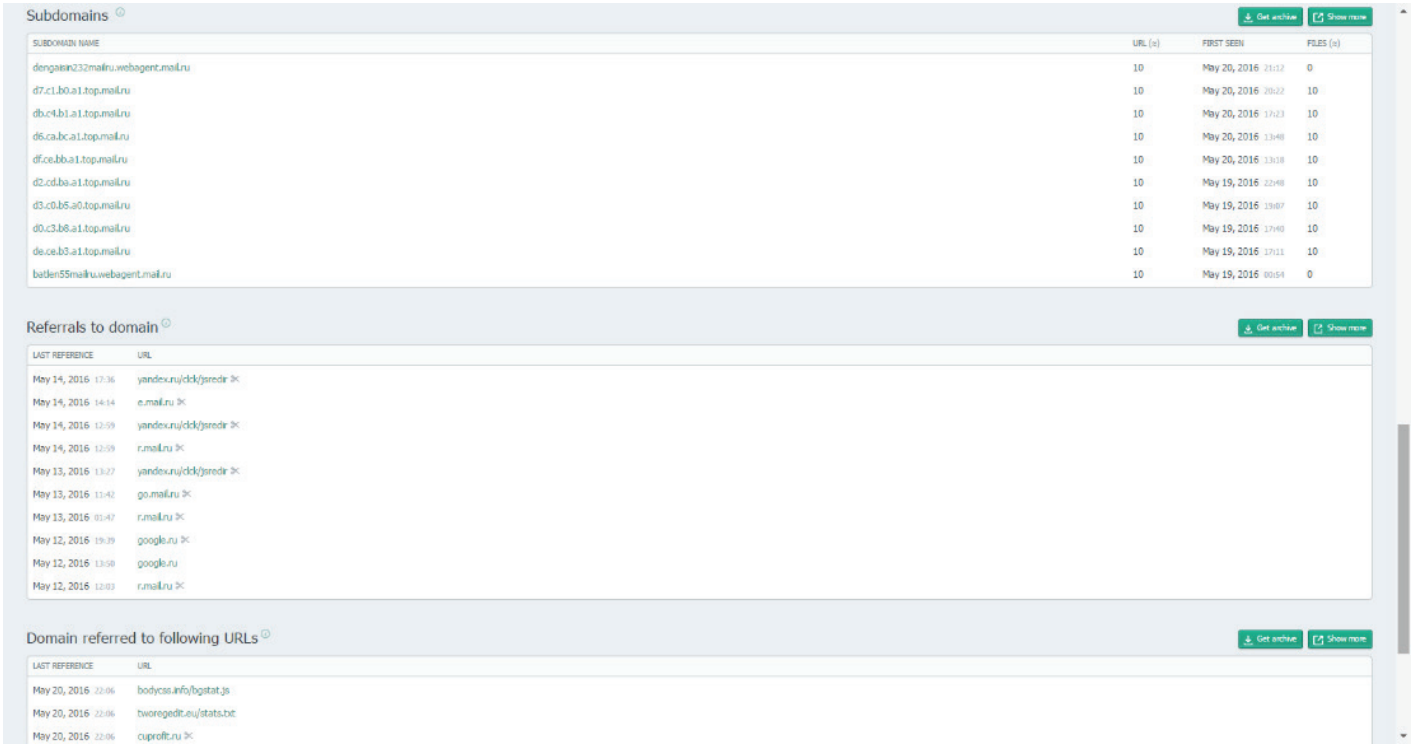
機能:

- **インターフェイス:** ウェブインターフェイスまたはRESTfulAPIを使用して検索することができます。
- **対応検索キー:** URL、IPアドレス、オブジェクトのハッシュ値
- **検索キーから得られるインテリジェンス情報:** キー情報の脅威判定（ブラック/ホワイト/グレー）、マルウェアの種類、検知日時、検知の地域分布や検知数の時間推移などの統計情報、マルウェアがホストされていたURL、マルウェアの通信先、オブジェクトの属性、マルウェアが潜伏しているフォルダーのパス　など
- **サンドボックスによる分析:** 未知のオブジェクトはサンドボックスにアップロードすることで、詳細な分析レポートを入手することができます。[2]





脅威情報ルックアップサービスはKaspersky Labが保有する膨大なホワイトリストとも連携しているので、正規のアプリケーション、悪意のない正規のURL、IPアドレスについても検索することができます。信頼できるオブジェクトの調査・解析にかかる時間を無駄にせず、インシデント対応を効率化します。



Kaspersky Lab のミッションは、あらゆる種類のサイバー脅威から世界を守ることです。これを実現し、インターネットの安全性を確保するためには、脅威インテリジェンスのリアルタイムの収集と共有が不可欠です。企業・組織のシステムと情報資産を効果的に保護し続けるための中核を成すのは、脅威情報へのタイムリーなアクセスです。カスペルスキー脅威情報検索サービスを使用すれば、このようなインテリジェンス情報をかつてないほど効率的かつ容易に入手することができます。

本サービスの詳細はKaspersky Labの地域代理店にお問い合わせいただくか、jp-sis@kaspersky.comまで電子メールにてお問い合わせください。

KASPERSKY lab
THE POWER OF PROTECTION

BD-KSIS_KTL-201701-001