Kaspersky for Business

KASPERSKY lab

カスペルスキー
サイバーセキュリティサービス

www.kaspersky.co.jp
#truecybersecurity

はじめに

毎日新しいサイバー攻撃が出現し、それぞれ異なる見かけと攻撃経路を持っています。

1 つのソリューションですべてを保護することは不可能です。しかし、ビッグデータの世界においても、危険が潜む可能性のある場所を知ることが、最新の脅威に対抗するための大きな力となります。

ビジネスマネージャーには、目下の脅威から組織を保護し、今後数年に待ち受ける危険を予測するという責任が課せられています。これには、スマートな方法で既知の脅威から業務を保護するだけでなく、一定の戦略的なセキュリティインテリジェンスが必要になりますが、これを社内で開発するだけのリソースを持っている企業はほとんどありません。

Kaspersky Lab は、事業に長期的な成功をもたらすには、長く続く関係が必要であると理解しています。

Kaspersky Lab は有益なビジネスパートナーとして、さまざまなチャネルを通じてお客様チームと常に最新情報を共有できるようにしています。幅広い提供手段を通じて、お客様のセキュリティオペレーションセンター（SOC）や IT セキュリティチームが、あらゆるオンライン脅威からいつでも組織を保護できる状態にあるように支援します。

カスペルスキー製品を使用していないお客様も、Kaspersky Lab のサイバーセキュリティサービスによるメリットを活用していただけます。

カスペルスキー
サイバーセキュリティサービス

- **カスペルスキー サイバー脅威インテリジェンス**
- **カスペルスキー 脅威ハンティング**
- **カスペルスキー セキュリティトレーニング**

他とは一線を画すセキュリティ

当社の DNA に組み込まれた世界有数のセキュリティインテリジェンスが、Kaspersky Lab のすべての行動に影響を及ぼし、市場でもっとも強力なアンチマルウェア保護の提供を可能にします。

Kaspersky Lab はテクノロジーを主眼に置いたセキュリティ専業ベンダーであり、CEO であるユージン・カスペルスキー（Eugene Kaspersky）を筆頭に、全社的にテクノロジーを重視しています。

Global Research & Analysis Team（GReAT）は、IT セキュリティエキスパートからなる精鋭集団であり、世界でもっとも危険なマルウェア脅威と標的型攻撃を多数発見するための道を開いてきました。

世界でもっとも評判の高いセキュリティ組織と警察機関（インターポール、ユーロポール、CERT、ロンドン市警察を含む）が、カスペルスキーの支援を積極的に求めてきました。

Kaspersky Lab は、中核をなす技術をすべて社内で開発し、完成させているため、その製品とインテリジェンスは必然的により信頼性が高く効率的です。

もっとも広く評価されている業界アナリスト（Gartner、Forrester Research、International Data Corporation（IDC）を含む）によって、Kaspersky Lab は、多数の主要なIT セキュリティカテゴリでリーダーとして評価されています。

130 を超える OEM（Microsoft、Cisco、Blue Coat、Juniper Networks、Alcatel Lucent を含む）がその製品およびサービスで、Kaspersky Labs のテクノロジーを使用しています。

カスペルスキー脅威インテリジェンス

絶えず進化し続ける IT セキュリティの脅威を追跡、分析、解釈、軽減する作業には、非常に大きな労力が必要です。あらゆるセクターの企業で、IT セキュリティの脅威に付随するリスクへの対処に必要な最新情報と適切なデータが不足しています。

カスペルスキー
サイバーセキュリティサービス

- **カスペルスキー**
  サイバー脅威インテリジェンス
  - 脅威データフィード
  - APT インテリジェンスレポート
  - オーダーメイドの脅威インテリジェンスレポート
  - カスペルスキー脅威インテリジェンスポータル
  - Kaspersky Cloud Sandbox
  - カスペルスキーフィッシング追跡
  - カスペルスキーボットネット追跡
- **カスペルスキー**
  脅威ハンティング
- **カスペルスキー**
  セキュリティトレーニング

Kaspersky Lab の脅威インテリジェンスサービスを利用することで、お客様は、世界有数の研究者とアナリストのチームが提供する、脅威を緩和するために必要なインテリジェンスにアクセスできます。

サイバーセキュリティのあらゆる側面に関する知識、経験、奥深い情報により、Kaspersky Lab は世界有数の警察機関および政府機関（インターポール、主要 CERT を含む）からパートナーとして信頼されています。このインテリジェンスを、お客様の組織で活用していただけます。

Kaspersky Lab が提供する脅威インテリジェンスサービスには以下が含まれます：

- 脅威データフィード
- APT インテリジェンスレポート
- オーダーメイドの脅威インテリジェンスレポート
- カスペルスキー脅威インテリジェンスポータル
- Kaspersky Cloud Sandbox
- カスペルスキーフィッシング追跡
- カスペルスキーボットネット追跡

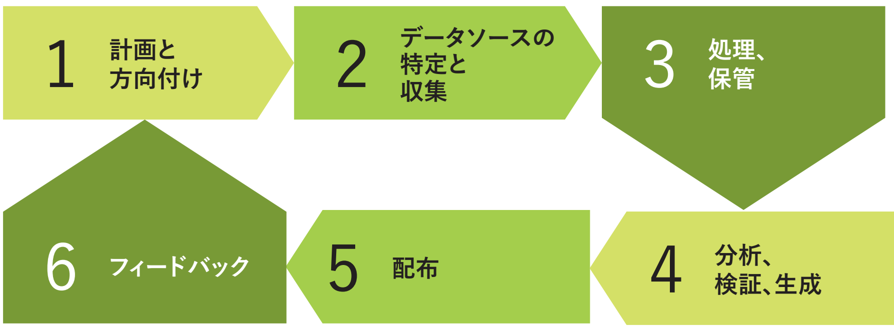
脅威データフィード

長年の実績があり信頼されたカスペルスキー脅威データフィードは、大規模セキュリティベンダーや大手企業により、**高品質のセキュリティ製品開発や自社ビジネスの保護に利用されています。**

サイバー攻撃は絶えず行われています。サイバー脅威は、**標的の防御を突破しようと**、頻度、複雑度、難読度において常に進化しています。現代の攻撃者は、標的のビジネスを中断させる、あるいはその顧客にダメージを与えるために、侵入するための複雑な**キルチェーン**、活動、およびカスタマイズされた**戦術**（**Tactics**）、**テクニック**（**Techniques**）、**手順**（**Procedures**）、**すなわち TTP を駆使しています。**

Kaspersky Lab は、**絶えず更新される**脅威データフィードを提供することで、**お客様やその顧客にサイバー脅威のリスクと**予想される影響について通知します。この情報により、**脅威を効果的に緩和**し、攻撃が始まる前でも**攻撃から保護**することができます。

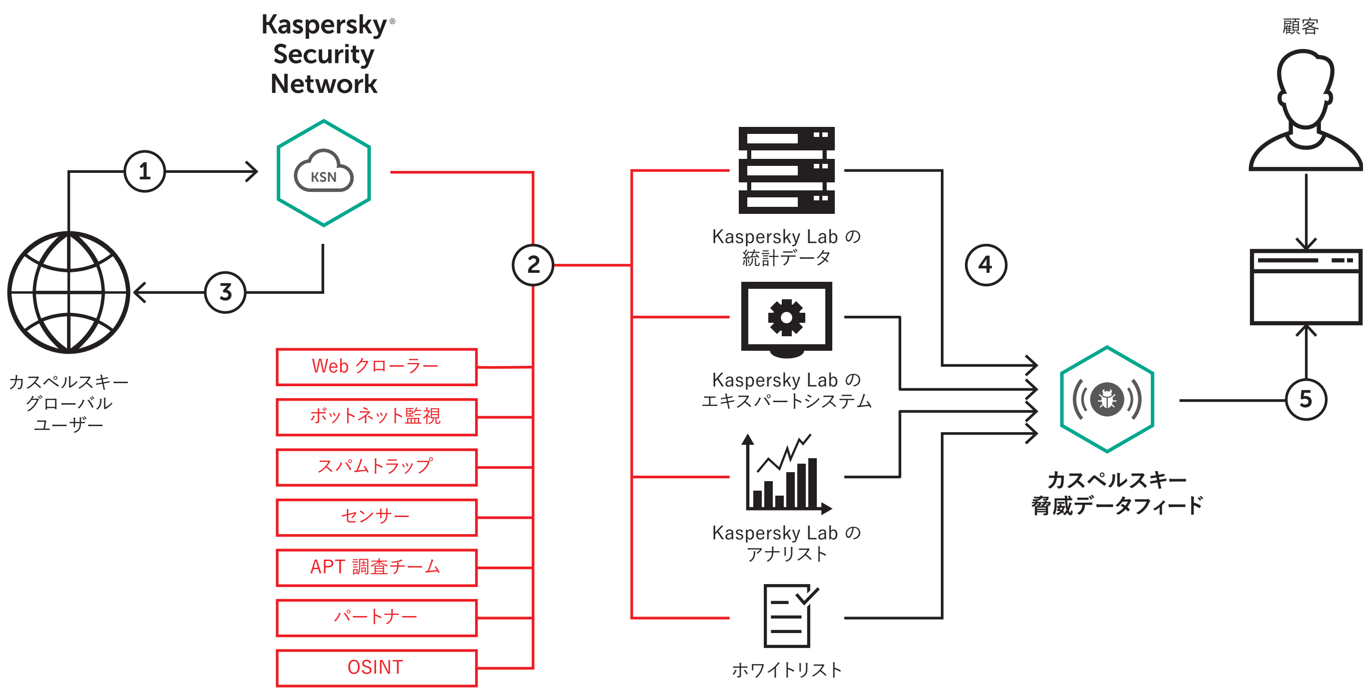
インテリジェンスのサイクル



データフィード

フィードの構成は以下のとおりです：

- **IP レピュテーションフィード** – 疑わしいホストや悪意のあるホストを対象とした IP アドレスとコンテキスト情報のセットです。
- **悪意のある URL およびフィッシング URL フィード** – 悪意のあるフィッシングリンクおよびフィッシングサイトを対象とします。
- **ボットネット C&C URL フィード** – デスクトップボットネット C&C サーバーおよび関連する悪意のあるオブジェクトを対象とします。
- **モバイルボットネット C&C URL フィード** – モバイルボットネット C&C サーバーを対象として、C&C と通信している感染したマシンを特定します。
- **ランサムウェア URL フィード** – ランサムウェアオブジェクトをホストするリンクまたはランサムウェアオブジェクトからアクセスされるリンクを対象とします。
- **APT IoC フィード**（APT インテリジェンスレポートのアクティブユーザーに対して提供）– APT 攻撃を実行するために利用される悪意のあるドメイン、ホスト、IP アドレス、ファイルと、関連ファイルやマルウェア群に関する YARA ルールを対象とします。
- **悪意のあるハッシュフィード** – もっとも危険かつ蔓延している新しいマルウェアを対象とします。
- **モバイル向けの悪意のあるハッシュフィード** – Android および iPhone モバイルプラットフォームに感染する悪意のあるオブジェクトの検知をサポートします。
- **P-SMS 型トロイの木馬フィード** – SMS メッセージの盗用、削除、応答や、モバイルユーザーへの高額請求を可能にする SMS 型トロイの木馬の検知をサポートします。
- **ホワイトリストデータフィード** – サードパーティの製品およびサービスについての正規ソフトウェアに関する体系的知識を提供します。
- **Kaspersky Transforms for Maltego** – Maltego ユーザーに対して、カスペルスキー脅威データフィードにアクセスするための一連の Transform を提供します。これにより、Kaspersky Lab から提供されるフィードと比較して、URL、ハッシュ値、IP アドレスの危険性を診断できます。また、この Transform により、オブジェクトのカテゴリを判断できるほか、そのオブジェクトに関する実用的なコンテキスト情報を提供できます。



カスペルスキー脅威データフィードには、実際の現場からリアルタイムに収集され徹底的に精査された脅威の兆候に関するデータが含まれています。

コンテキスト情報

各データフィード内のすべてのレコードに**実用的なコンテキスト情報**（脅威名、タイムスタンプ、地理位置情報、感染した Web リソースの解決済み IP アドレス、ハッシュ値、知名度など）が付加されます。コンテキスト情報によって「より広い視野」が得られ、その後の検証や、幅広いデータの利用法が可能になります。データをコンテキスト情報とともに考察することで、「**誰が**」、「**何を**」、「**どこで**」、「**いつ**」**という疑問**に答えることが簡単になり、その結果、攻撃者を特定して、**自社に固有の**タイムリーな意思決定を下して行動に移すことができます。

サービスの概要

- **誤検知**がいくつもあるデータフィードには価値がありません。そのため、十分に精査されたデータが配信されるように、フィードをリリースする前に大量のテストとフィルターを適用しています。
- データフィードは、世界中から収集された調査結果に基づいて、リアルタイムで自動的に生成されます（**Kaspersky Security Network** は、213 を超える国と地域の数千万エンドユーザーを対象として、インターネットの全トラフィックのうち、かなりの割合のトラフィックを把握しています）。そのため、高い**検知率**と精度を実現しています。
- すべてのフィードは耐障害性の高いインフラストラクチャによって生成、監視されており、**継続的可用性**を確保しています。
- データフィードによって、フィッシング、マルウェア、エクスプロイト、ボットネット C&C の URL、その他の悪意のあるコンテンツをホストするために使用されている **URL を即座に検知**できます。
- すべてのトラフィック種別（Web、メール、P2P、IM など）、あるいはモバイルプラットフォームを標的とした**マルウェア**も**すぐに検知**して特定できます。
- 単純な軽量の**配布**形式（**JSON、CSV、OpenIoC、STIX**）であり **HTTPS** や任意の配信手法によって配信されるため、フィードをセキュリティソリューションに容易に統合できます。
- 世界中の**セキュリティアナリスト**、世界的に著名な **GReAT チームや最先端の研究開発チームのセキュリティエキスパート**など、数百人に及ぶ専門家がこれらのフィードの生成に携わっています。セキュリティ担当者には、最高品質のデータから生成された重要情報とアラートが送られます。必要以上の兆候データや警告が大量に流入するリスクはありません。
- **実装のしやすさ**。Kaspersky Lab が提供する補助的なドキュメント、サンプル、技術専任のアカウントマネージャー、テクニカルサポートのすべてが一体となって、容易な統合を可能にします。

収集と処理

データフィードは、**Kaspersky Security Network** や当社独自の Web クローラーである**ボットネット監視サービス**（ボットネットおよびその標的とアクティビティを 24 時間 365 日監視するサービス）、スパムトラップ、調査チーム、パートナーなどの信頼性の高い異種混在のソースを融合して、そこから集積されます。

次に、集積されたすべてのデータがリアルタイムで慎重に調査され、複数の前処理手法によってふるい分けされます。その手法として、統計的な基準、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、マルチスキャナー、近似ツール、ふるまいプロファイリングなど）、アナリストによる検証、**ホワイトリスト**検証などが利用されます：

利点

- 絶えず更新される不正アクセスの痕跡（IOC）と実用的なコンテキスト情報によって SIEM、ファイアウォール、IPS/IDS、セキュリティプロキシ、DNS 解決、APT 対策などの**ネットワーク防御ソリューションを強化**することで、サイバー攻撃に関する知見を得て、攻撃者の意図、能力、標的についてより深く理解できるようになります。主要 SIEM（HP ArcSight、IBM QRadar、Splunk など）が完全にサポートされます。
- **周辺機器やエッジネットワーク機器のアンチマルウェア保護を強化**します（ルーター、ゲートウェイ、UTM アプライアンスなど）。
- 脅威に関連する有意義な情報と標的型攻撃の背景にあるグローバルな知見をお客様のセキュリティ / SOC チームに提供することで、**お客様のインシデント対応およびフォレンジック能力を改善、促進**します。ホストやネットワークでのセキュリティインシデントをより効率的かつ効果的に診断、分析し、未知の脅威に対する社内システムからのシグナルの優先順位を付けることで、インシデント対応の時間を最小限に抑え、重要なシステムやデータが不正アクセスを受ける前に、キルチェーンを遮断することができます。
- **サブスクリプション契約のある企業に対して脅威インテリジェンスを提供**します。新しいマルウェアやその他の悪意のある脅威について直接得た情報を活用して、**先手を打ってお客様の防御体制を強化し、侵害を防止**します。
- **標的型攻撃の緩和**に役立ちます。戦術的、戦略的脅威インテリジェンスを利用して、目の前の特定の脅威に対抗するために防御戦略を適応させることで、セキュリティ体制を強化できます。
- 脅威インテリジェンスを利用して、**ネットワークやデータセンターにホストされている悪意のあるコンテンツを検知**できます。
- 感染したマシンから**機密情報を含む資産や知的財産が外部に流出するのを防ぎます**。感染した資産を素早く検知することで、競争優位や事業機会の喪失を防ぎ、ブランドへの評価を維持します。
- コマンド & コントロールプロトコル、IP アドレス、悪意のある URL、ファイルハッシュ値などの脅威の兆候について詳細に調査し、さらに人間によって検証された脅威のコンテキスト情報を付加することで、攻撃に優先順位を付け、IT 支出やリソースの割り当てに関する意思決定を向上できるようにします。また、**ビジネスにとって極めて大きなリスクとなる脅威の緩和にお客様が集中できるようにサポート**します。
- 当社の専門知識とコンテキストに関する実用的なインテリジェンスを利用して、Web コンテンツフィルタリング、スパム / フィッシングブロックなどの**お客様の製品およびサービスが提供する保護機能を強化**できます。
- **MSSP として**、業界をリードする脅威インテリジェンスをお客様の顧客向けの高品質サービスとして提供することで、お客様のビジネスの成長に貢献します。**CERT として**、お客様のサイバー脅威の検知および特定能力を強化、拡張します。

カスペルスキー APT インテリジェンスレポートのメリット:

- **専用アクセス:**最先端の脅威に関する技術的な情報を、公開前の調査段階で入手できます。
- **非公開の APT 情報:**注目を集めるすべての脅威が公開の対象となるわけではありません。被害を受けた組織やデータの機密性、脆弱性解消プロセスの性質、または関連する警察の活動が原因となって、公開されない脅威もあります。しかし、カスペルスキー APT インテリジェンスレポートの利用者には、すべての脅威が報告されます。
- **詳細な関連情報:**標準形式(OpenIOC、STIX など)で提供される不正アクセスの痕跡(IOC)の広範なリストを含む技術データに加えて、Yara ルールへのアクセスを提供します。
- **継続的な APT 活動の監視:**実用的なインテリジェンスに調査段階でアクセスできます(APT 分類、IOC、C&C インフラストラクチャに関する情報)。
- **異なる利用者層に合わせたコンテンツ:**各レポートには、関連する APT に関する情報をわかりやすくまとめた、経営陣向けのエグゼクティブサマリーが含まれています。また、エグゼクティブサマリーの後に APT の詳しい技術説明と関連する IOC および Yara ルールの情報が続きます。この情報から、セキュリティ調査チーム、マルウェアアナリスト、セキュリティエンジニア、ネットワークセキュリティアナリスト、APT 調査チームは、関連する脅威に対して高品質の保護を行うための実用的なアドバイスを得ることができます。
- **遡及的分析:**サブスクリプション期間中はずっと、以前に発行されたすべてのプライベートレポートにアクセスできます。
- **脅威インテリジェンスポータル:**最新の IoC を含むすべてのレポートが脅威インテリジェンスポータルまたは RESTful API から入手でき、お客様にとってシームレスなユーザーエクスペリエンスになっています。

注 - サブスクリプションの制限事項

本サービスのレポートに含まれる情報の機密性と固有性により、レポートのサブスクリプションは信用ある政府、公共団体、民間団体に限定することが義務付けられています。

APT インテリジェンスレポート

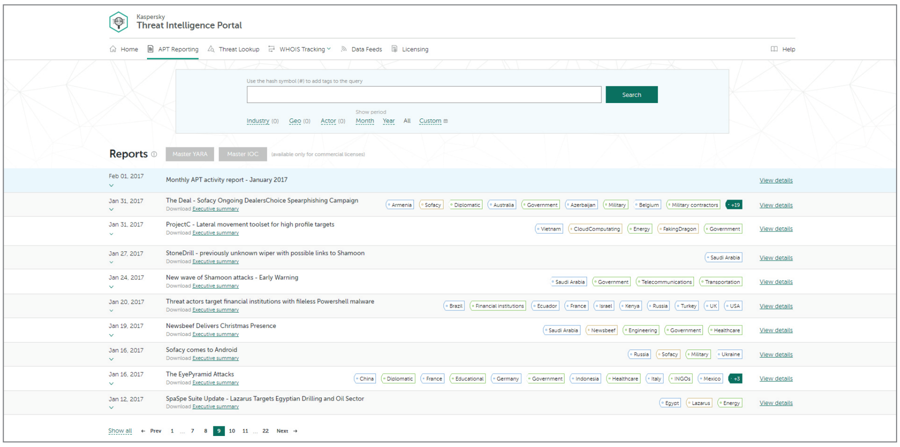
注目度の高いサイバースパイ活動の認識と知識を高める、包括的かつ実用的な Kaspersky Lab のレポート。

インテリジェンスレポートで提供される情報を活用すると、新しい脅威と脆弱性に素早く対応できるため、既知の経路からの攻撃をブロックし、先進の攻撃によるダメージを軽減し、セキュリティ戦略を強化することができます。

Kaspersky Lab はこれまで重大な APT 攻撃をいくつも発見してきましたが、発見されるすべての Advanced Persistent Threat が即座に報告されるわけではなく、多くは公表されないままになります。

カスペルスキー APT インテリジェンスレポートの利用者は、発見されたすべての APT に関して、幅広い形式で提供される完全な技術データを含むカスペルスキーの調査および発見結果に継続的にアクセスできます。これには、公開されることのない脅威もすべて含まれています。Kaspersky Lab が 2017 年の 1 年間に作成したレポートは実に 100 以上もあります。

Kaspersky Lab のエキスパートは、業界でもっとも高いスキルと実績を持つ APT 発見者であり、サイバー犯罪者グループが戦術を変更した場合は、ただちにお客様に警告を送ります。また、お客様は、企業のセキュリティ戦略にとって強力な研究および分析コンポーネントとなる、Kaspersky Lab の完全な APT レポートデータベースにアクセスできます。



オーダーメイドの脅威インテリジェンスレポート

お客様専用の脅威インテリジェンスレポート

組織に攻撃を仕掛けるためにもっとも有効な方法は何でしょうか。標的を絞った攻撃者は、どのような経路と情報を利用できるでしょうか。すでに攻撃が開始されているか、または攻撃の脅威にさらされつつあるでしょうか。

お客様専用のカスペルスキー脅威レポートは、これらの疑問に答えるだけにとどまりません。Kaspersky Lab のエキスパートが現在の攻撃状況を総合的につなぎ合わせて、悪用可能な弱点を特定し、過去 / 現在 / 将来の攻撃の痕跡を明らかにします。

お客様は提供される固有の情報を活用して、サイバー犯罪者の一番の標的として特定された領域を重視した防御戦略を策定し、迅速かつ正確な行動で侵入者を撃退し、攻撃が成功するリスクを最小限に抑えることができます。

オープンソースインテリジェンス(OSINT)や、Kaspersky Lab のエキスパートシステムおよびデータベースによる詳細分析、アンダーグラウンドのサイバー犯罪ネットワークに関する知識を使用して開発されたインテリジェンスレポートは、以下の領域を対象としています:

- **攻撃経路の識別:**外部から利用でき、攻撃の対象となりうるネットワーク上の重要コンポーネント(ATM、モバイル技術を使ったビデオ監視などのシステム、従業員のソーシャルネットワークプロファイルと個人用メールアカウントなど)を特定し、その状況を分析します。

- **マルウェアとサイバー攻撃の追跡分析**：お客様の組織を標的とするマルウェアサンプル（活動中 / 非活動中）、過去または現在のボットネット動作、ネットワークベースの疑わしい動作のすべてを識別、監視、分析します。

- **第三者による攻撃**：お客様の顧客、パートナー、サービス利用者を明確に標的とした脅威やボットネット動作がある場合、感染システムが攻撃に使用される可能性があるため、その痕跡を確認します。

- **情報漏洩**：アンダーグラウンドのオンラインフォーラムやコミュニティを慎重に監視することで、ハッカーがお客様を念頭に置いた攻撃計画を話し合っているか、たとえば不誠実な従業員が情報を売買しているかどうかを突き止めます。

- **現在の攻撃ステータス**：APT 攻撃は、何年にもわたって気付かれることなく継続される場合があります。お客様のインフラストラクチャに影響を与えている現在の攻撃を見つけた場合、有効な修正手順をアドバイスします。

クイックスタート - リソース不要の使いやすさ

パラメータとデータ形式がいったん決まったら、当サービスを使用し始めるためにインフラストラクチャを追加する必要はありません。

カスペルスキーのオーダーメイドの脅威レポートは、ネットワークリソースを含むリソースの整合性と可用性にまったく影響を与えません。

当サービスは、一度のプロジェクトとして、またはサブスクリプションに基づいて定期的（例：四半期ごと）に利用できます。

各国固有の脅威インテリジェンスレポート

国家のサイバーセキュリティは、そのすべての主要機関および組織の保護により成り立ちます。政府当局への APT（Advanced Persistent Threat）は国家の安全に影響を及ぼします。製造、輸送、通信、銀行、その他の中枢産業に対してサイバー攻撃が行われれば、財務的損失、製造工程での事故、ネットワーク通信障害、一般市民の不満など、国全体にとって大きなダメージになる可能性もあります。

国を標的としたマルウェアやハッカーの攻撃について、現在の攻撃対象領域と傾向を大まかに知っておくことで、サイバー犯罪者の第一の標的とされる領域を重視した防御戦略を策定し、迅速かつ正確な行動によって侵入者を撃退し、攻撃が成功するリスクを最小限に抑えることができます。

オープンソースインテリジェンス（OSINT）や、Kaspersky Lab のエキスパートシステムおよびデータベースによる詳細分析、アンダーグラウンドのサイバー犯罪ネットワークに関する知識を使用して作成された各国固有の脅威レポートは、以下の領域を対象としています：

- **攻撃経路の識別**：政府の脆弱なアプリケーション、通信機器、産業用制御システムのコンポーネント（SCADA、PLC など）、ATM など、外部からアクセス可能な国の重要 IT リソースを特定して、そのステータスを分析します。

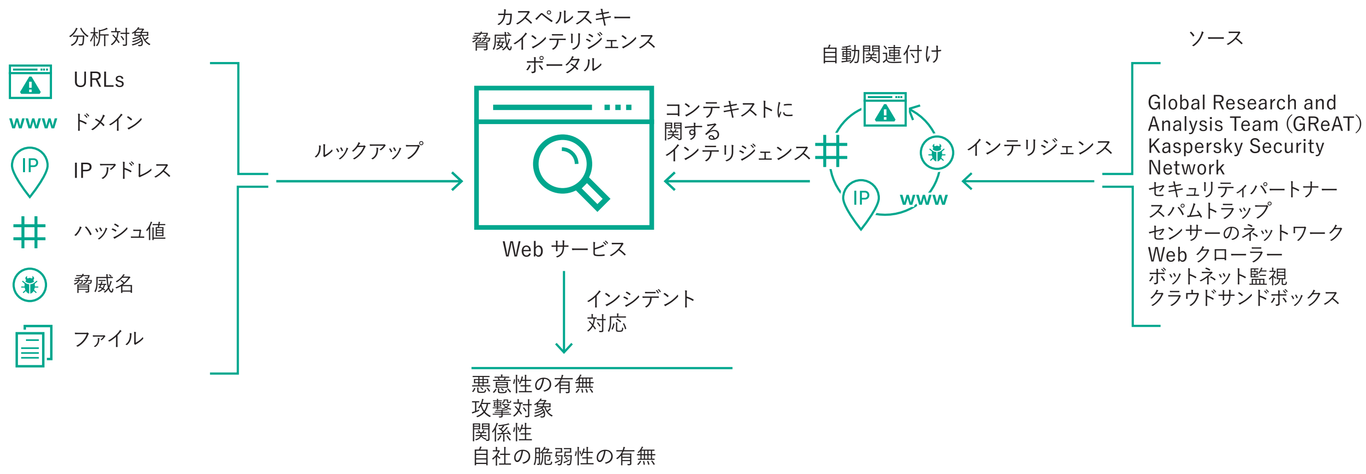
- **マルウェアとサイバー攻撃の追跡分析**：APT 活動、マルウェアサンプル（活動中 / 非活動中）、過去または現在のボットネット動作、国を標的としたその他の重大な脅威を、Kaspersky Lab 独自の内部監視リソースのデータに基づいて識別、分析します。

- **情報漏洩**：アンダーグラウンドのフォーラムやオンラインコミュニティを秘密裏に監視することで、ハッカーが特定組織を念頭に置いた攻撃計画を話し合っているかを突き止めます。また、標的の組織や機関にとってリスクになりうる、重大なアカウント侵害についても明らかにします（たとえば、不倫サイト「Ashley Madison」で情報が漏洩した政府職員のアカウント。この情報は脅迫に利用される恐れがあります）。

カスペルスキー脅威インテリジェンスレポートは、調査対象のネットワークリソースの整合性と可用性にまったく影響を与えません。このサービスは、ネットワークを阻害しない偵察手法と、オープンソースで入手できる情報の分析、およびアクセスが制限されているリソースに基づいています。

このサービスでは最終的に、それぞれの国営産業や国家機関にとって重大な脅威に関する説明、および詳しい技術分析結果に関する追加情報を含むレポートが提供されます。レポートは暗号化されたメールメッセージによって配信されます。

脅威インテリジェンスポータル



サービスの概要

- **信頼できるインテリジェンス**：カスペルスキー脅威インテリジェンスポータルの主な特徴として、脅威インテリジェンスデータの信頼性が高く、実用的なコンテキスト情報が付属していることが挙げられます。カスペルスキー製品はアンチマルウェアテスト[1] の分野でトップの評価を獲得しており、セキュリティインテリジェンスデータの比類のない質の高さが最高水準の検知率と極めて低い誤検知率によって実証されています。

- **脅威ハンティング**：先を見越した予防、検知、対処を行うことで、攻撃の影響や頻度を最小限に抑えることができます。可能な限り早期に攻撃を追跡し、積極的に排除します。脅威の発見が早いほど与えられるダメージも小さく、速やかに修復して、ネットワーク運用を通常状態に戻すことができます。

- **サンドボックス分析**：疑わしいオブジェクトを安全な環境内で実行することで未知の脅威を検知します。脅威のふるまいとアーチファクトの全体像をわかりやすいレポートで確認できます。

- **さまざまなエクスポートフォーマット**：不正アクセスの痕跡（IOC）や実用的なコンテキスト情報を、広範に利用され系統化された機械判読可能な共有フォーマット（STIX、OpenIOC、JSON、Yara、Snort のほか CSV にも対応）にエクスポートできるため、脅威インテリジェンスの十分な活用、運用ワークフローの自動化、SIEM などのセキュリティ管理システムへの統合が可能です。

- **使いやすい Web インターフェイス、RESTful API**：このサービスは、Web インターフェイス（Web ブラウザー）経由で手動モードで利用することも、簡潔な RESTful API 経由でアクセスすることもできます。

今日のサイバー犯罪に国境はなく、技術的な能力も急速に高まっており、サイバー犯罪者が闇の Web リソースを活用して標的を恐怖に陥れるなど、攻撃は巧妙になる一方です。サイバー脅威は、標的の防御を突破しようと次々と新たな試みが行われ、頻度、複雑度、難読度において常に進化しています。攻撃者は、標的のビジネスを中断させ、資産を窃取し、あるいはその顧客にダメージを与えるために、その活動において複雑なキルチェーン、およびカスタマイズされた戦術（Tactics）、テクニック（Techniques）、手順（Procedures）、すなわち TTP を駆使しています。

カスペルスキー脅威インテリジェンスポータルは、サイバー脅威に関して Kaspersky Lab が収集し続けているすべてのデータとそれらの間にある相互関係を単一の強力な Web サービスにまとめたものです。お客様のセキュリティチームに対して、影響を受ける前にサイバー攻撃を防止できるよう、可能な限り多くのデータを提供することを目的としています。URL、ドメイン、IP アドレス、ファイルハッシュ値、脅威名、統計的データまたはふるまいデータ、WHOIS データ、DNS データ、ファイル属性、地理位置情報データ、ダウンロードチェーン、タイムスタンプなどに関する最新の脅威インテリジェンスの詳細情報を取得できます。その結果、新しい脅威のグローバルな動向を把握し、組織の保護とインシデント対応能力の強化に役立てることができます。

カスペルスキー脅威インテリジェンスポータルによって提供される脅威インテリジェンスは耐障害性の高いインフラストラクチャによってリアルタイムで生成、監視されており、継続的可用性と一貫したパフォーマンスが確保されています。世界中のセキュリティアナリスト、世界的に著名な GReAT チームや最先端の研究開発チームのセキュリティエキスパートなど、数百人に及ぶ専門家が、実態に即した価値ある脅威インテリジェンスの生成に携わっています。

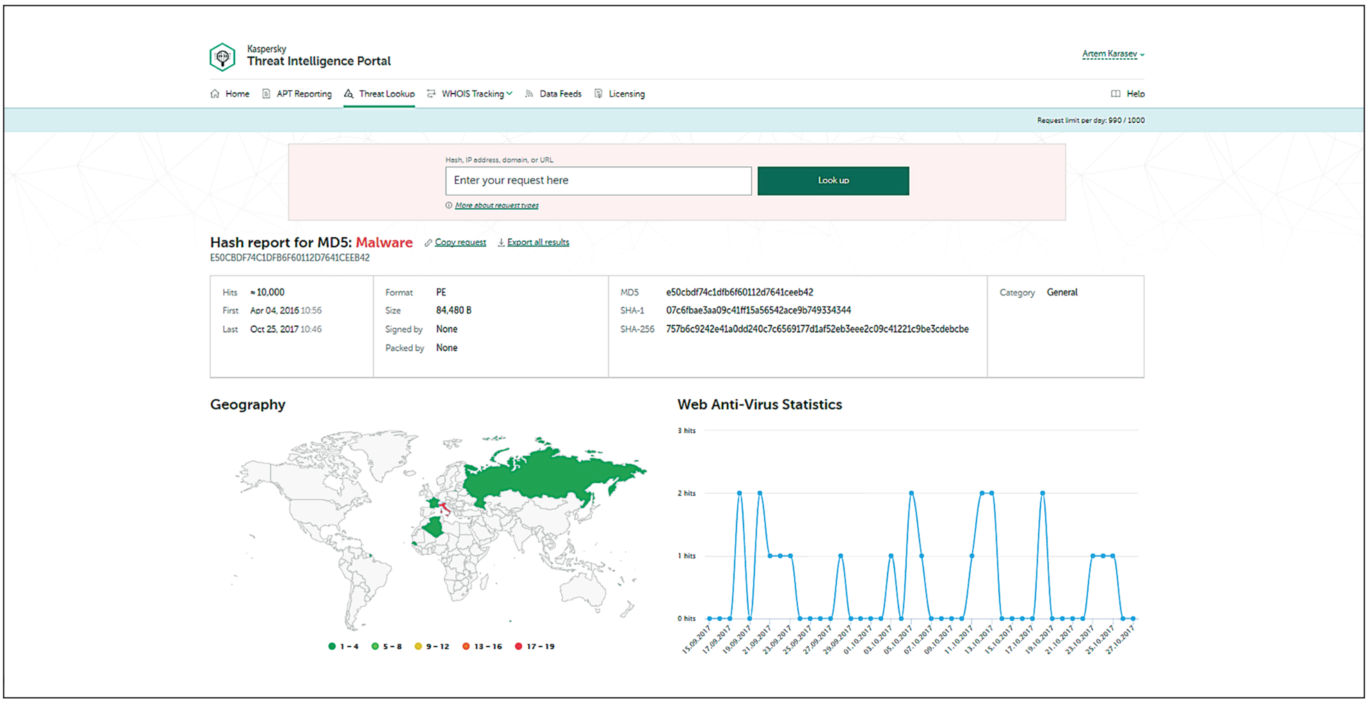
主な利点

- 脅威に関連する有意義な情報と標的型攻撃の背景にあるグローバルな知見をお客様のセキュリティ / SOC チームに提供することで、**お客様のインシデント対応およびフォレンジック能力を改善、促進**します。ホストやネットワークでのセキュリティインシデントをより効率的かつ効果的に診断、分析し、未知の脅威に対する社内システムからのシグナルの優先順位を付けることで、インシデント対応の時間を最小限に抑え、重要なシステムやデータが侵害される前に、キルチェーンを遮断することができます。

- IP アドレス、URL、ドメイン、ファイルハッシュ値などの**脅威の兆候について詳細に調査**し、さらに高度に検証された脅威のコンテキスト情報を付加することで、攻撃に優先順位を付け、スタッフやリソースの割り当てに関する意思決定を向上し、ビジネスにとって極めて大きなリスクとなる脅威の緩和に集中できるようにします。

- **標的型攻撃の緩和**：戦術的、戦略的脅威インテリジェンスを利用して、脅威に対抗するための防御戦略を適応させることで、セキュリティインフラストラクチャを強化できます。

1 https://www.kaspersky.co.jp/top3



このサービスでできること

- Web ベースのインターフェイスまたは RESTful API 経由で脅威の兆候を検索する
- オブジェクトを悪意のあるものとして扱うべき理由を理解する
- 検知されたオブジェクトは広範に拡散されているか、固有のものであるかを確認する
- 証明書、共通名、ファイルパス、関連 URL などの高度な詳細情報を調査し、新たな疑わしいオブジェクトを発見する

これらは一部の例に過ぎません。関連性が高く粒度の細かいインテリジェンスデータを集めた、この充実した持続的なソースを活用できる方法は無数にあります。

敵と味方を知ること。そして、悪意がないと立証されているファイル、URL、IP アドレスを見分けて、調査スピードを上げることが大切です。1 秒 1 秒が重大になるときに、信頼済みオブジェクトの分析のために時間を無駄にできません。

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。このため、また、インターネットを安全なものにするため、脅威インテリジェンスをリアルタイムで共有し、利用できるようにすることが不可欠です。データとネットワークを効果的に保護し続けるための中核を成すのは、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インテリジェンスポータルを利用すれば、このようなインテリジェンス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。

主な機能:

- ロード済み、実行済み DLL
- 作成された排他制御(ミューテックス)
- 変更、作成されたレジストリキー
- ドメイン名および IP アドレスによる外部接続
- HTTP、DNS のリクエストとレスポンス
- 実行済みファイルによって作成されたプロセス
- 作成、変更、削除されたファイル
- プロセスメモリダンプ、ネットワークトラフィックダンプ(PCAP)
- スクリーンショット
- 判明したすべての不正アクセスの痕跡(IOC)に関する詳細脅威インテリジェンスと実用的なコンテキスト情報
- RESTful API
- その他多数

主な利点:

- APT、標的型脅威、複雑な脅威の高度な検知
- 非常に効果的で複雑なインシデント調査を実行できるワークフロー
- コストのかかるアプライアンスの購入もシステムリソースに関する懸念も不要なスケーラビリティ
- 現行のセキュリティ対策とのシームレスな統合と自動化

クラウドサンドボックス

従来型のアンチウイルスツールだけで今日の標的型攻撃を予防することは不可能です。アンチウイルスエンジンは既知の脅威やその亜種を阻止することしかできず、豊富な知識を持つサイバー犯罪者はあらゆる手段を自在に利用して自動検知をすり抜けます。情報セキュリティインシデントによる損害が今も急増していることから、大きな損害が発生する前に、瞬時に脅威を検知して脅威に対して迅速に対応および対抗できることがますます重要になっています。

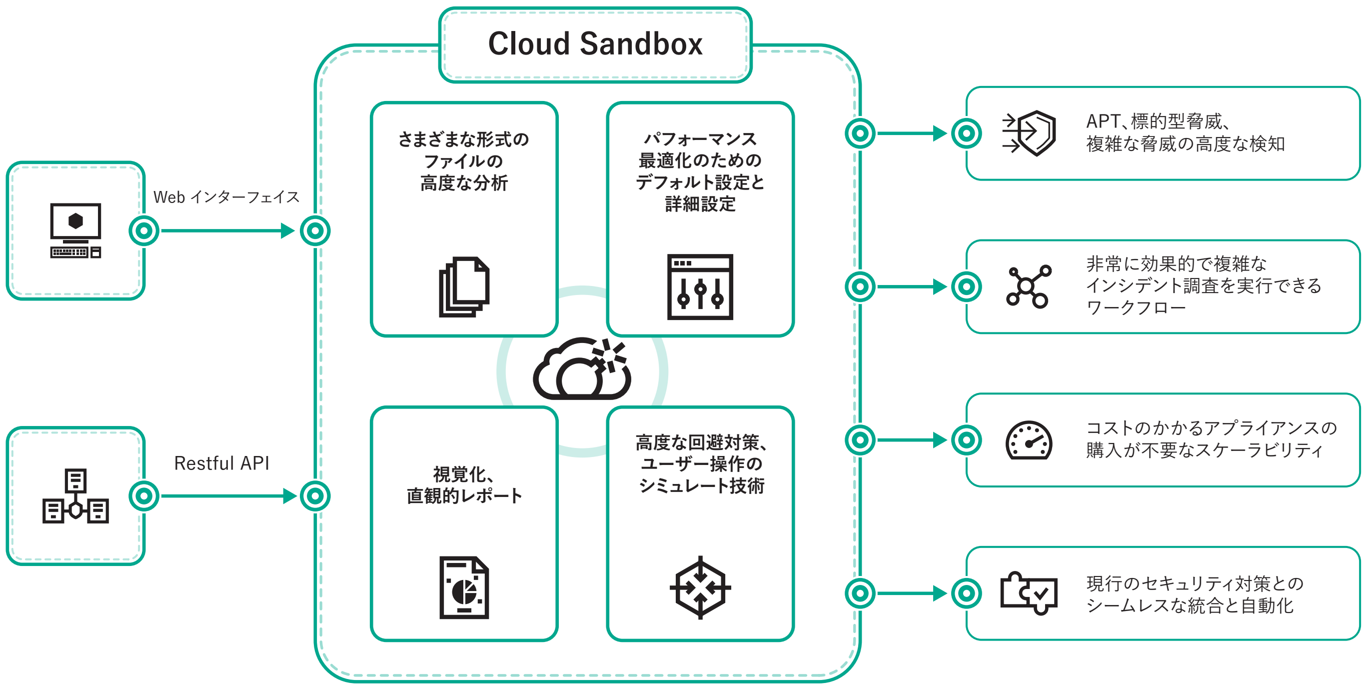
ファイルのふるまいに基づいてインテリジェントな判断を行うこと、およびそれと並行してプロセスメモリ、ネットワークアクティビティなどを分析することが、目標に合わせて洗練された現在の標的型脅威を理解する上で最適なアプローチです。統計的データには、つい最近に修正されたマルウェアに関する情報が含まれていない可能性があります。一方、サンドボックス技術は、ファイルサンプルの発生源を調査し、ふるまい分析に基づいて IOC を収集し、未知の悪意のあるオブジェクトを検知できる強力なツールとなります。

セキュリティの防御をくぐり抜ける脅威に対する、先を見越した軽減対策

現代のマルウェアは、悪意のある動作の存在を知らせる可能性のあるコードを実行しないように、あらゆる策を講じています。標的のシステムに必要なパラメータが揃っていない場合、悪意のあるプログラムはほぼ確実に自らを破壊し、一切の痕跡を残しません。そのため、悪意のあるコードを実行するには、サンドボックス環境が通常のエンドユーザーのふるまいを正確に模倣できる必要があります。

カスペルスキークラウドサンドボックスは、(Kaspersky Security Network やその他の専有システムによって得られた)数ペタバイト規模の統計的データから収集した脅威インテリジェンス、ふるまい分析、信頼性の高い回避対策と、自動クリック、文書スクロール、ダミープロセスなどのユーザー操作のシミュレート技術を組み合わせたハイブリッドアプローチを採用しています。そのため、未知の脅威を検知するための最適なツールに仕上がっています。

このサービスは、当社のラボ内で 10 年以上にわたって進化を遂げてきたテクノロジーであるサンドボックスコンプレックスから直接開発されています。このテクノロジーは、Kaspersky Lab が 20 年間継続している脅威の研究によって判明したマルウェアのふるまいに関する全知識を取り込んでいます。当社が毎日 35 万件以上の新たな悪意のあるオブジェクトを検知して、業界をリードするセキュリティソリューションを提供できるのも、この知識があるからです。



脅威インテリジェンスポータルの一機能であるカスペルスキークラウドサンドボックスは、お客様の脅威インテリジェンスワークフローを完結させる最後のコンポーネントです。　ポータルが URL、ドメイン、IP アドレス、ファイルハッシュ値、脅威名、統計的データまたはふるまいデータ、WHOIS データ、DNS データなどに関する最新の脅威インテリジェンスの詳細情報を引き出すものであるのに対して、クラウドサンドボックスは、その知識を、分析対象サンプルによって生成された IOC に関連付けるものです。

このサービスによって、極めて効果的で複雑なインシデント調査を実施して、脅威の特性について即座に理解し、詳細情報を確認しながらそれぞれを結び付けて、相互に関連する脅威の兆候を明らかにすることができます。

インスペクションは、特に対象が多段階攻撃である場合に非常にリソースを消費する作業です。カスペルスキークラウドサンドボックスは、インシデント対応とフォレンジック分析のための理想的なツールであり、コストのかかるアプライアンスの購入もシステムリソースに関する懸念も不要で、自動的にファイルを処理できるスケーラビリティを備えています。

カスペルスキーフィッシング追跡のすべての通知は HTTPS 経由で配信されます。通知には、以下の情報が含まれます：

- フィッシング URL のスクリーンショット
- フィッシング URL のHTML コード
- 次のフィールドを含む JSON
  - フィッシング URL
  - フィッシング URL が標的としているブランドの名称
  - 初回発見時のタイムスタンプ
  - 直近発見時のタイムスタンプ
  - フィッシング URL の知名度
  - フィッシング URL の影響を受けたユーザーの地理位置情報
  - 窃取されたデータの種別（クレジットカード情報、銀行の認証情報、メール、ソーシャルネットワーク、個人情報など）
  - 攻撃の種別（アカウントをブロックする脅威、ファイルダウンロードの誘い、個人情報更新の依頼など）
  - フィッシング URL の解決済み IP アドレス
  - WHOIS データ
  - その他多数

フィッシング追跡

フィッシングや、特に標的となる人物を絞り込んだスピアフィッシングは、現在もっとも危険性が高く効果の大きいオンライン詐欺手法の 1 つです。偽の Web サイトでログイン名とパスワードを収集し、ユーザーのオンライン ID を乗っ取ります。その後、侵害されたメールアカウントやソーシャルネットワーキングプラットフォームを通じて、資金の窃取、スパムやマルウェアの拡散などを行います。サイバー犯罪グループにとっては強力な武器であり、攻撃の頻度はますます増え、その種類も多様化するばかりです。

また、攻撃対象となるのは金融機関だけではありません。オンライン小売店から ISP、政府機関に至るまで、誰もがスピアフィッシング攻撃を受けるリスクを負っています。企業ブランドが散りばめられた Web サイトの完全なコピー、あるいは会社役員から直接来たように見えるメールメッセージによって、ユーザーはあまりにも簡単に機密情報を提供しようという気になります。その結果、ユーザー自身が被害を受けるばかりか、企業にも多大なダメージが発生する可能性があります。

フィッシング攻撃がただ一度成功するだけで、その標的となった企業に大きな影響が及ぶこともあります。直接の損失のほかにも、侵害された Web サイトやアカウントの消去など、間接的なコストが大量に発生します。その中でも最悪の被害は、言うまでもなく、企業の評判が損なわれることです。オンラインサービスでのユーザーからの信頼が崩れたために、多数の顧客を失い、その後何年も信頼性の問題を抱えることになるでしょう。今日のサイバー犯罪に国境はなく、技術的な能力も急速に高まっており、サイバー犯罪者が闇の Web リソースを活用して標的を恐怖に陥れるなど、攻撃は巧妙になる一方です。サイバー脅威は、標的の防御を突破しようと次々と新たな試みが行われ、頻度、複雑度、難読度において常に進化しています。攻撃者は、標的のビジネスを中断させ、資産を窃取し、あるいはその顧客にダメージを与えるために、その活動において複雑なキルチェーン、およびカスタマイズされた戦術（Tactics）、テクニック（Techniques）、手順（Procedures）、すなわち TTP を駆使しています。

ソリューション – カスペルスキーフィッシング追跡サービス

このサービスは、お客様のブランドを標的としたフィッシングサイトの出現を、リアルタイムで積極的に追跡してアラートを出すものです。お客様に対して、フィッシングなど、お客様のビジネスに直接関連する詐欺行為について、関連性が高く正確で詳しい継続的レポートを提供します。このレポートには、ユーザーから認証情報、機密情報、金融情報、個人情報を窃取する侵入済みのマルウェアやフィッシング URL の情報が含まれます。このサービスでは、特定のトップレベルドメイン（TLD）や領域全体についても、フィッシングサイトの出現について監視します。

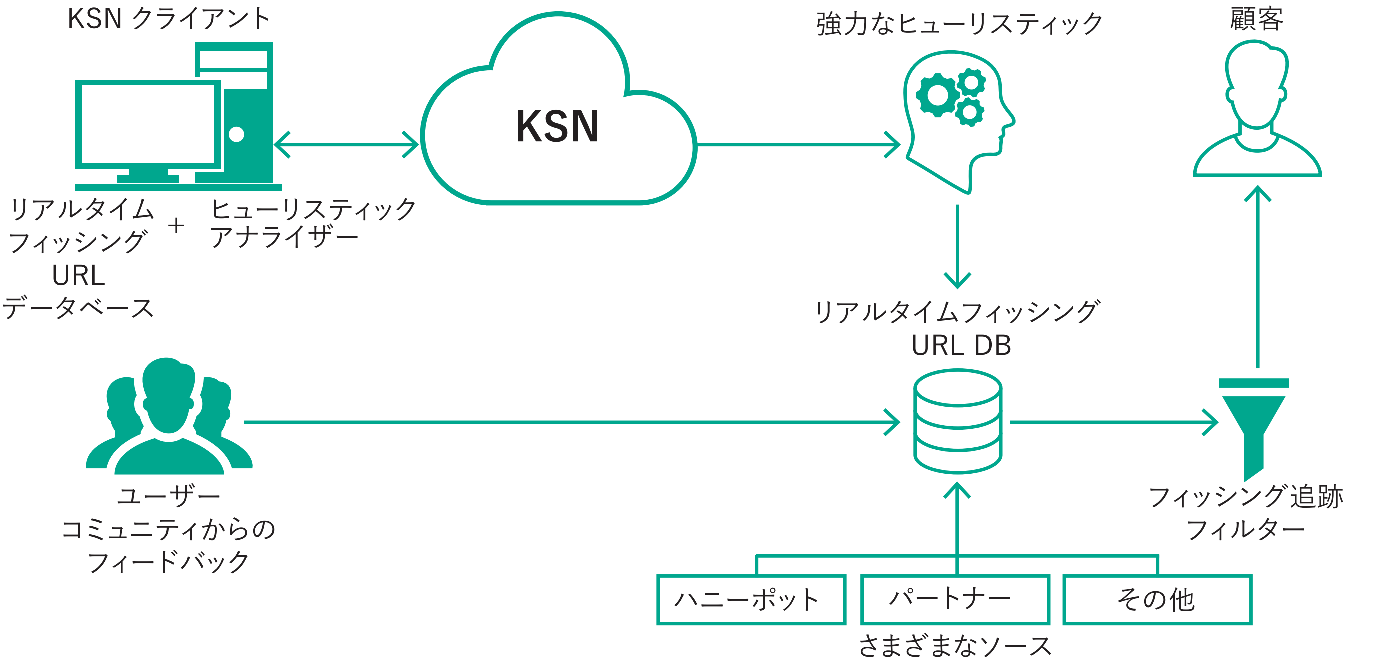
メール通知によって、お客様のブランド、企業名、または商標に対するフィッシングの脅威を継続的に確認できます。すべての通知に、巧妙化が増すフィッシング攻撃に関して、範囲が広く信頼できる高精度の情報が含まれており、動的に生成されるフィッシングドメインや URL、さらにはフィッシングの大発生にも素早く対応できるようになっています。受信する情報には、フィッシングサイト一覧とともに付加的なインテリジェンスも含まれているため、フィッシング攻撃に対してすぐに具体的な措置をとることができます。

専門家により検証されたこのようにタイムリーなインテリジェンスが付加されることで、お客様は迅速かつ正確に行動して、組織やユーザーに対するフィッシング攻撃の影響を緩和し、詐欺行為に対して先を見越した体制を築くことができます。

インテリジェンスのソース

カスペルスキーフィッシング追跡では、Kaspersky Security Network（KSN）、強力なヒューリスティックエンジン、メールハニーポット、Web クローラー、スパムトラップ、調査チーム、パートナー、当社が約 20 年にわたって収集してきた悪意のあるオブジェクトに関する履歴データなど、信頼性の高い異種混在のインテリジェンスソースからデータが融合されます。次に、集積されたデータがリアルタイムで十分に調査され、複数の前処理手法によってふるい分けされます。その手法として、統計的な基準、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、近似ツール、ふるまいプロファイリングなど）、コンテンツアナリストによる検証、ホワイトリスト検証ツールなどが利用されます。

世界中に配備されている Kaspersky Security Network と、Kaspersky Lab の検知テクノロジー、次々に実行されるテストやフィルターによって、あらゆるフィッシング攻撃や脅威を最大限まで検知し、極めて低い誤検知率も達成します。このことは、第三者機関によるテストによって継続的に確認されています*。



フィッシング攻撃についての早期警告

カスペルスキーフィッシング追跡サービスのサブスクリプションを登録することで、攻撃者に対抗するための強力な武器が得られます。お客様のブランド、オンラインサービス、または顧客を狙っている現在進行中または計画中のフィッシング攻撃について早期警告を受け取れるため、より実務に即した、正確で費用対効果に優れた方法でリソースを保護しリスクを緩和することができます。

先手必勝

重要な情報がリアルタイムで提供されるほか、高度な攻撃が計画中または進行中であることを示す悪意のある動作についても定期レポートによって報告されます。そのため、お客様を視界にとらえたサイバー犯罪者よりも、お客様の方が一歩先を行くことができます。

ユーザー向けのエクスペリエンスの強化

スピアフィッシングを行う攻撃者を把握し詳細を理解すれば、古いソフトウェアの廃止から SMS ベース認証の導入まで適切な保護措置を計画でき、お客様のオンラインユーザーが適切に保護されていると感じて安心できるようになります。

影響の最小化

フィッシングサイトの URL を把握することにより、そのサイトをホストしている ISP に通知できるため、そのサイトが取得した個人情報の今後の漏洩を防ぎ、攻撃を阻止することができます。

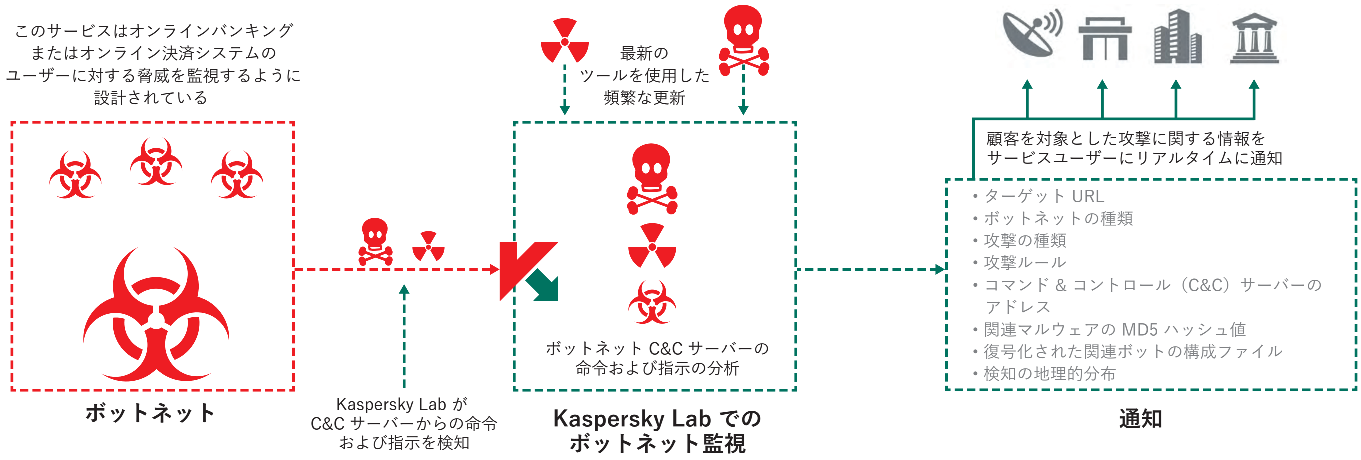
より良い情報の入手

このような関連性が高く正確な詳細情報が、「誤検知」も時間の浪費もなく提供されることから、現在および将来のセキュリティ戦略の情報を得てその戦略を強化するための新しい知見が得られます。そうすることで、お客様はオンライン詐欺に対して、十分な情報に基づいて先を見越した体制をとれるようになります。

* AV-Comparatives によるテストレポートはご要望に応じて提供いたします。

ボットネット追跡

顧客と評判を脅かすボットネットを特定するための、エキスパートによる監視および通知サービスです。



ユースケースおよびサービスのメリット

- オンラインユーザーを標的としたボットネットがもたらす脅威についての事前警告により、常に攻撃の一歩先を行くことができます。
- オンラインユーザーを狙うボットネットのコマンド & コントロールサーバーの URL 一覧を識別することで、CERT または警察機関に要請を送ってこれらをブロックすることができます。
- 攻撃の性質を理解することで、オンラインバンキングまたは決済キャビネットの機能を強化できます。
- オンラインユーザーの教育を通じて、攻撃に使用されるソーシャルエンジニアリングの認識と被害の防止を可能にします。

リアルタイムの情報提供による対策：

このサービスは、Kaspersky Lab が監視するボットネット内のキーワードを追跡して、一致したブランド名に関する情報を含む、個別化された通知をサブスクリプションとして提供します。通知はメールまたは RSS を介して、HTML あるいは JSON 形式で提供されます。通知に含まれる内容は以下のとおりです：

- **ターゲット URL** — ボットマルウェアは、ユーザーがターゲット組織の URL にアクセスするのを待ってから攻撃を開始するように設計されています。
- **ボットネットの種類** — 顧客のトランザクションを危険にさらすためにサイバー犯罪者が、どのようなマルウェアの脅威を利用しているのかを正確に識別します。例には、Zeus、SpyEye、Citadel が含まれます。
- **攻撃の種類** — サイバー犯罪者がマルウェアを使用する目的を特定します。例には、Web データインジェクション、画面ワイプ、ビデオキャプチャ、フィッシング URL への転送が含まれます。
- **攻撃ルール** — Web コードインジェクションでどのルールが使用されているかを特定します。例には、HTML リクエスト（GET または POST）、インジェクション前の Web ページのデータ、インジェクション後の Web ページのデータがあります。
- **コマンド & コントロール（C&C）サーバーのアドレス** — インターネットサービスプロバイダに問題のサーバーを通知して、迅速に脅威を解消できるようにします。
- **関連マルウェアの MD5 ハッシュ値** — マルウェアの検証に使用するハッシュサムを提供します。
- **復号化された関連ボットの構成ファイル** — ターゲット URL の完全なリストを特定します。
- **検出の地理的分布（上位 10か国）** — 世界中から取得したマルウェアサンプルの統計データを提供します。

カスペルスキーセキュリティトレーニング

絶えず増加と発展を続ける脅威に直面する企業にとって、サイバーセキュリティの教育は重要な手段です。IT セキュリティスタッフは、企業にとって効果的な脅威の管理および軽減戦略の主な要素となる高度なテクニックに精通する必要があります。

**カスペルスキー
サイバーセキュリティサービス**

**カスペルスキー
サイバー脅威インテリジェンス**

**カスペルスキー
脅威ハンティング**

**カスペルスキー
セキュリティトレーニング**

デジタルフォレンジック
マルウェア分析とリバース
エンジニアリング
高度なデジタルフォレンジック
高度なマルウェア分析とリバース
エンジニアリング
インシデント対応
Yara による効率的な脅威検知

サイバーセキュリティのテーマと技術に関する幅広いカリキュラムと、基本から専門家レベルまでにわたる評価を提供します。すべてのコースは、お客様の拠点で受講形式で行うか、または、可能な場合は Kaspersky Lab のローカルオフィスもしくは地域拠点で実施します。

コースは、理論的な講座とハンズオン「ラボ」の両方を含むように設計されています。各コースの終了時に、受講者の知識を確認するための評価が実施されます。

サービスのメリット

デジタルフォレンジック、高度なデジタルフォレンジック

社内のデジタルフォレンジックおよびインシデント対応チームの専門知識を強化します。これらのコースは、デジタルサイバー犯罪の痕跡調査や、攻撃のタイムラインおよび攻撃元の情報を復元するための各種データの分析において、実用的スキルを開発、強化し、経験不足を補うものになっています。このコースを受講することで、コンピューターインシデントを円滑に調査し、企業のセキュリティレベルを強化できるようになります。

マルウェア分析とリバースエンジニアリング、高度なマルウェア分析とリバースエンジニアリング

リバースエンジニアリングトレーニングは、悪意のある攻撃の調査を担当するインシデント対応グループを支援するものです。IT 部門の従業員およびシステム管理者向けのコースです。受講者は、悪意のあるソフトウェアの分析、不正アクセスの痕跡（IOC）の収集、感染したマシン上のマルウェアを検知するためのシグネチャの記述、感染した（または暗号化された）ファイルやドキュメントの復元について学習します。

インシデント対応

社内チームがインシデント対応プロセスの全段階を経験し、インシデントからの修復に必要となる包括的な知識が得られるコースです。

Yara による効率的な脅威検知

最も効果的な Yara ルールの記述方法、Yara ルールのテスト方法、未知の脅威を発見できるレベルにまで Yara ルールを改善する方法について学習します。

ハンズオン体験

大手セキュリティベンダーのグローバルエキスパートと一緒に作業し学習することで、受講者はサイバー犯罪を検出して阻止するための「もっとも困難な局面」での経験を学ぶことができます。

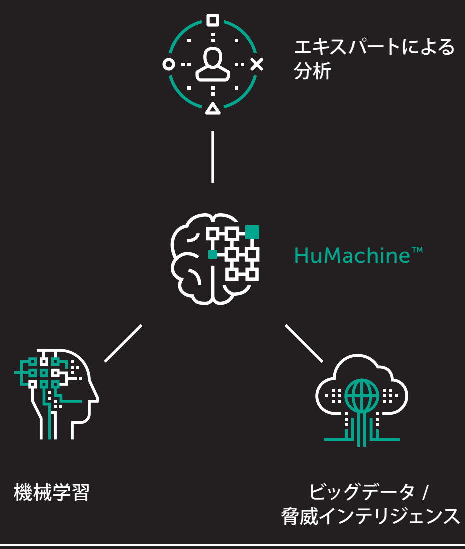
プログラムの説明

テーマ	期間	獲得スキル
デジタルフォレンジック		
• デジタルフォレンジックの紹介 • ライブ応答と形跡の収集 • Windows レジストリの内部 • Windows アーチファクトの分析 • ブラウザーのフォレンジック • メールの分析	5 日間	• デジタルフォレンジックラボの構築 • デジタル形跡の収集と正しい処理 • インシデントの再現とタイムスタンプの使用 • Windows OS 内のアーチファクトに基づく侵入形跡の発見 • ブラウザーおよびメール履歴の発見と分析 • デジタルフォレンジック用ツールおよび機器の活用
マルウェア分析とリバースエンジニアリング		
• マルウェア分析とリバースエンジニアリングの目標およびテクニック • Windows の内部処理、実行可能ファイル、x86 アセンブラ • 基本的な静的分析テクニック(文字列の抽出、インポート分析、 • PE エントリポイントの概要、自動解凍など) • 基本的な動的分析テクニック(デバッグ、監視ツール、トラフィックのインターセプトなど) • .NET、Visual Basic、Win64 ファイルの分析 • スクリプトと非 PE 分析テクニック(バッチファイル、Autoit、Python、Jscript、JavaScript、VBS)	5 日間	• マルウェア分析に適した安全な環境の構築:サンドボックスと必須ツールの導入 • Windows プログラム実行の原則の理解 • 悪意のあるオブジェクトの解凍、デバッグ、分析と機能の識別 • スクリプトマルウェア分析による悪意のあるサイトの検出 • 高速マルウェア分析の実施
高度なデジタルフォレンジック		
• 詳細な Windows フォレンジック • データの復元 • ネットワークとクラウドのフォレンジック • メモリフォレンジック • タイムライン分析 • 実際の標的型攻撃に対するフォレンジック手法	5 日間	• 詳細なファイルシステム分析の実施 • 削除済みファイルの復元 • ネットワークトラフィックの分析 • ダンプを使用した悪意のある動作の調査 • インシデントタイムラインの再現
高度なマルウェア分析とリバースエンジニアリング		
• マルウェア分析とリバースエンジニアリングの目標およびテクニック • 高度な静的分析テクニック(シェルコードの静的分析、PE ヘッダー、TEB、PEB の解析、異なるハッシュアルゴリズムによる関数のロード) • 高度な動的分析テクニック(PE 構造、手動の高度な解凍、実行可能ファイル全体を暗号化形式で保存している悪意のある圧縮ファイルの解凍) • APT リバースエンジニアリング(フィッシングメールから始まり可能な限り踏み込もうとする APT 攻撃シナリオが対象) • プロトコル分析(暗号化された C2 通信プロトコルの分析、トラフィックの復号化方法) • ルートキット、ブートキットの分析(Ida および VMWare を使ったブートセクターのデバッグ、2 つの仮想マシンを使ったカーネルデバッグ、ルートキットサンプルの分析)	5 日間	• リバースエンジニアリング対策技術(難読化、アンチデバッグ)を認識しながらのベストプラクティスに従ったリバースエンジニアリング • 高度なマルウェア分析の活用によるルートキットおよびブートキットの詳細分析 • さまざまな種類のファイルや Windows 以外のマルウェアに埋め込まれているエクスプロイト用シェルコードの分析
インシデント対応		
• インシデント対応入門 • 検知と一次分析 • デジタル分析 • 検知ルールの作成(YARA、Snort、Bro)	5 日間	• APT とその他の脅威を区別する • さまざまな攻撃者のテクニックと標的型攻撃の構造を理解する • 具体的な監視と検知の方法を適用する • インシデント対応ワークフローに従う • インシデントの時系列とロジックを再現する • 検知ルールとレポートを作成する
Yara による効率的な脅威検知		
• Yara 構文の概要 • 高速かつ効果的なルールを作成するためのコツ • Yara 生成ツール • Yara ルールの誤検知テスト • VT での新規未検知サンプルのハンティング • 効果的な検知のための Yara 内での外部モジュール活用 • アノマリ検索 • 多数の実例 • Yara スキル向上のための演習	2 日間	• 効果的な Yara ルールを作成する • Yara ルールをテストする • 未知の脅威を発見できるレベルにまで Yara ルールを改善する

Kaspersky Lab
Enterprise Cybersecurity：www.kaspersky.co.jp/enterprise/
サイバー脅威に関する最新情報：www.securelist.com
IT セキュリティに関する最新情報：business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.co.jp



PMM-1040-201812